kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 AO Kaspersky Lab

목차

Kaspersky Security Center 15.1 도움말
새로운 기능
Kaspersky Security Center 정보
- 아키텍처
- 하드웨어 및 소프트웨어 요구 사항
  - 중앙 관리 서버 요구 사항
  - 웹 콘솔 요구 사항
  - 모바일 서버 요구 사항
  - 관리 콘솔 요구 사항
  - 네트워크 에이전트 요구 사항
- 호환되는 Kaspersky 애플리케이션 및 솔루션
- Kaspersky Security Center 15.1 라이센스 및 기능
- Kaspersky Security Center 구성 요소의 호환성 관련 정보
- Windows 기반 및 Linux 기반 Kaspersky Security Center 비교
- Kaspersky Security Center Cloud Console 정보

Kaspersky Security Center 15.1
- 기본 개념
  - 중앙 관리 서버
  - 중앙 관리 서버 계층 구조
  - 가상 중앙 관리 서버
  - 모바일 기기 서버
  - 웹 서버
  - 네트워크 에이전트
  - 관리 그룹
  - 관리 중인 기기
  - 미할당 기기
  - 관리자 워크스테이션
  - 관리 플러그인
  - 관리 웹 플러그인
  - 정책
  - 정책 프로필
  - 작업
  - 작업 범위
  - 로컬 애플리케이션 설정과 정책의 관계
  - 배포 지점
  - 연결 게이트웨이
- 주요 설치 시나리오
- Kaspersky Security Center의 사용 포트
- Kaspersky Security Center 작업용 인증서
  - Kaspersky Security Center 인증서 정보
  - 중앙 관리 서버 인증서 정보
  - Kaspersky Security Center에서 사용되는 사용자 지정 인증서 요구 사항
  - 시나리오: 사용자 지정 중앙 관리 서버 인증서 지정

klsetsrvcert 유틸리티를 사용하여 중앙 관리 서버 인증서 교체
klmover 유틸리티를 사용하여 네트워크 에이전트를 중앙 관리 서버에 연결
웹 서버 인증서 재발급
데이터 트래픽 및 포트 사용 스키마
LAN 내에 중앙 관리 서버 및 관리 중인 기기
LAN 내에 기본 중앙 관리 서버 및 두 개의 보조 중앙 관리 서버
LAN 내에 중앙 관리 서버 설치, 인터넷 망에 관리 중인 기기 운영, 역방향 프록시 사용 중
LAN 내에 중앙 관리 서버 설치, 인터넷 망에 관리 중인 기기 운영, 연결 게이트웨이 사용 중
DMZ 내에 중앙 관리 서버 설치, 인터넷 망에 관리 중인 기기 운영
Kaspersky Security Center 구성 요소와 보안 제품의 상호 작용: 자세한 정보
상호 작용 스키마에서 사용되는 표기법
중앙 관리 서버 및 DBMS
중앙 관리 서버 및 관리 콘솔
중앙 관리 서버 및 클라이언트 기기: 보안 제품 관리
배포 지점을 통해 클라이언트 기기에 있는 소프트웨어 업그레이드
중앙 관리 서버 계층 구조: 기본 중앙 관리 서버 및 보조 중앙 관리 서버
DMZ에 있는 보조 중앙 관리 서버와 중앙 관리 서버 계층
네트워크 세그먼트 및 클라이언트 기기에 연결 게이트웨이가 있는 중앙 관리 서버
중앙 관리 서버와 DMZ의 두 기기: 연결 게이트웨이와 클라이언트 기기
중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔
활성화 및 모바일 기기에 있는 보안 제품 관리
배포 모범 사례
강화 가이드
중앙 관리 서버 배포
연결 안전
계정 및 인증
중앙 관리 서버의 보호 관리
클라이언트 기기의 보호 관리
관리 중인 애플리케이션에 대한 보호 구성
중앙 관리 서버 점검
타사 시스템으로 이벤트 전송
타사 정보 시스템에 대한 보안 권장 사항
Kaspersky 보안 애플리케이션 사용 시 권장 사항
배포 준비
Kaspersky Security Center 배포 계획
일반적인 보호 시스템 배포 구성
조직 네트워크에 대한 Kaspersky Security Center 배포 계획에 대한 정보
기업 보호용 구조 선택
Kaspersky Security Center의 표준 구성
표준 구성: 단일 사무소
표준 구성: 자체 관리자가 운영하는 소수의 대규모 사무소
표준 구성: 다수의 소규모 원격 사무소
중앙 관리 서버용 DBMS 선택
Kaspersky Security Center 15.1 사용을 위한 MariaDB x64 서버 구성
Kaspersky Security Center 15.1 사용을 위한 MySQL x64 서버 구성
Kaspersky Security Center 15.1 사용을 위한 PostgreSQL 또는 Postgres Pro 서버 구성
Kaspersky Endpoint Security for Android를 사용하여 모바일 기기 관리

중앙 관리 서버에 대한 인터넷 접속 제공
인터넷 접속: 로컬 네트워크의 중앙 관리 서버
인터넷 접속: DMZ의 중앙 관리 서버
인터넷 접근: 연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용
배포 지점 정보
klnagent 서비스에 대한 파일 설명자 제한 늘리기
배포 지점의 개수 및 구성 계산
중앙 관리 서버 계층 구조
가상 중앙 관리 서버
Kaspersky Security Center의 제한 사항에 대한 정보
네트워크 부하
안티 바이러스 보호 시스템 최초 배포
안티 바이러스 데이터베이스 최초 업데이트
중앙 관리 서버와 클라이언트 동기화
안티 바이러스 데이터베이스 추가 업데이트
중앙 관리 서버를 통한 클라이언트 이벤트 처리
24시간 기준 트래픽
모바일 기기 관리 준비
iOS MDM 서버
표준 구성: DMZ에 위치한 Kaspersky Device Management for iOS
표준 구성: 조직 로컬 네트워크의 iOS MDM 서버
Kaspersky Endpoint Security for Android를 사용하여 모바일 기기 관리
중앙 관리 서버 성능에 대한 정보
중앙 관리 서버 연결 관련 제한 사항
중앙 관리 서버 성능 테스트 결과
KSN 프록시 서버 성능 테스트 결과
외부 서비스와의 상호 작용을 위한 네트워크 설정
네트워크 에이전트 및 보안 제품 배포
초기 배포
설치 관리자 구성
설치 패키지
MSI 속성 및 변환 파일
애플리케이션 원격 설치용 타사 도구를 사용한 배포
Kaspersky Security Center의 원격 설치 작업에 대한 정보
기기 이미지 캡처 및 복사를 통한 배포
잘못된 하드 드라이브 이미지 복사
Microsoft Windows의 그룹 정책을 사용하는 배포
Kaspersky Security Center의 원격 설치 작업을 통한 강제 배포
Kaspersky Security Center에서 만든 독립 실행형 패키지 실행
애플리케이션 수동 설치용 옵션
MST 파일 생성
네트워크 에이전트가 설치된 기기에 애플리케이션 원격 설치
원격 설치 작업에서 기기 다시 시작 관리
보안 제품의 설치 패키지에서 데이터베이스를 업데이트하는 작업의 적합성
Kaspersky Security Center의 애플리케이션 원격 설치 도구를 사용하여 관리 중인 기기에서 관련 실행 파일 실행
배포 모니터링

- 설치 관리자 구성
  - 일반 정보
  - 숨김 모드로 설치 (응답 파일 사용)
  - 숨김 모드로 네트워크 에이전트 설치(응답 파일 사용 안 함)
  - setup.exe를 통한 부분 설치 구성
  - 중앙 관리 서버 설치 파라미터
  - 네트워크 에이전트 설치 파라미터
- 가상 인프라
  - 가상 컴퓨터 부하를 줄이기 위한 팁
  - 동적 가상 컴퓨터 지원
  - 가상 컴퓨터 복사 지원
- 네트워크 에이전트가 설치된 기기의 파일 시스템 롤백 지원
- 애플리케이션 로컬 설치
  - 네트워크 에이전트 로컬 설치
  - 숨김 모드로 네트워크 에이전트 설치
  - 숨김 모드에서 Linux용 네트워크 에이전트 설치(응답 파일 사용)
  - 네트워크 에이전트 설치를 위해 폐쇄형 소프트웨어 환경 모드에서 Astra Linux를 실행하는 기기 준비
  - 대화식 모드로 Linux용 네트워크 에이전트 설치
  - 애플리케이션 관리 플러그인의 로컬 설치
  - 숨김 모드에서 애플리케이션 설치
  - 독립 실행형 패키지를 사용하여 애플리케이션 설치
  - 네트워크 에이전트 설치 패키지 설정
  - 개인정보취급방침 보기
- 모바일 기기 관리 시스템 배포
  - iOS MDM 프로토콜을 통해 관리 시스템 배포
    - iOS MDM 서버 설치
    - 숨김 모드로 iOS MDM 서버 설치
    - iOS MDM 서버 배포 시나리오
    - 간소화된 배포 구성
    - Kerberos 제한 위임(KCD)을 사용하는 배포 구성
    - APNs 인증서 받기
    - APNs 인증서 갱신
    - 예약 iOS MDM 서버 인증서 구성
    - iOS MDM 서버에 APNs 인증서 설치
    - Apple 푸시 알림 서비스 접근 구성
    - 모바일 기기에 공유 인증서 발급 및 설치
  - 관리 중인 기기 목록에 KES 기기 추가
  - KES 기기를 중앙 관리 서버에 연결
    - 중앙 관리 서버에 기기 직접 연결
    - Kerberos 제한 위임(KCD)을 사용하는 서버에 KES 기기를 연결하기 위한 구성
    - Firebase Cloud Messaging 사용
  - 공개 키 인프라와의 통합
  - Kaspersky Security Center 웹 서버

Kaspersky Security Center 설치
- 설치 준비
- DBMS 작업용 계정
  - SQL Server 작업을 위한 계정 구성(Windows 인증)
  - SQL Server 작업을 위한 계정 구성(SQL Server 인증)
  - MySQL 및 MariaDB 작업을 위한 계정 구성
  - MySQL 또는 MariaDB DBMS에서 공유 테이블스페이스의 데이터를 테이블당 파일 테이블스페이스로 이동
  - PostgreSQL 및 Postgres Pro 작업을 위한 계정 구성
- 시나리오: Microsoft SQL Server 인증
- 시나리오: MySQL 서버 인증
- 시나리오: PostgreSQL 서버 인증
- 중앙 관리 서버 설치 권장 사항
  - Failover 클러스터에 중앙 관리 서버 서비스용 계정 생성
  - 공유 폴더 정의
  - Active Directory 그룹 정책을 통해 중앙 관리 서버 도구를 사용하여 원격 설치
  - 독립 실행형 패키지에 대한 UNC 경로를 전달하여 원격 설치
  - 중앙 관리 서버 공유 폴더에서 업데이트
  - 운영 체제 이미지 설치
  - 중앙 관리 서버 주소 지정
- 표준 설치
  - 1단계. 라이센스 계약서 및 개인정보취급방침 검토
  - 2단계. 설치 방법 선택
  - 3단계. Kaspersky Security Center 웹 콘솔 설치
  - 4단계. 네트워크 크기 선택
  - 5단계. 데이터베이스 선택
  - 6단계. SQL 서버 구성
  - 7단계. 인증 모드 선택
  - 8단계. 하드 드라이브에 파일 압축 해제 및 설치
- 사용자 지정 설치
  - 1단계. 라이센스 계약서 및 개인정보취급방침 검토
  - 2단계. 설치 방법 선택
  - 3단계. 설치할 구성 요소 선택
  - 4단계. Kaspersky Security Center 웹 콘솔 설치
  - 5단계. 네트워크 크기 선택
  - 6단계. 데이터베이스 선택
  - 7단계. SQL 서버 구성
  - 8단계. 인증 모드 선택
  - 9단계. 중앙 관리 서버를 시작할 계정 선택
  - 10단계. Kaspersky Security Center 서비스를 실행하기 위한 계정 선택
  - 11단계. 공유 폴더 선택
  - 12단계. 중앙 관리 서버에 대한 연결 구성
  - 13단계. 중앙 관리 서버 주소 정의
  - 14단계. 모바일 기기 연결에 사용할 중앙 관리 서버 주소
  - 15단계. 애플리케이션 관리 플러그인 선택
  - 16단계. 하드 드라이브에 파일 압축 해제 및 설치

- Kaspersky Security Center 장애 조치 클러스터 배포
  - 시나리오: Kaspersky Security Center 장애 조치 클러스터 배포
  - Kaspersky Security Center 장애 조치 클러스터 정보
  - Kaspersky Security Center 장애 조치 클러스터용 파일 서버 준비
  - Kaspersky Security Center 장애 조치 클러스터용 노드 준비
  - Kaspersky Security Center 장애 조치 클러스터 노드에 Kaspersky Security Center 설치
  - 수동으로 클러스터 노드 시작 및 중지
- Windows Server 장애 조치 클러스터에 중앙 관리 서버 설치
  - 1단계. 라이센스 계약서 및 개인정보취급방침 검토
  - 2단계. 클러스터에서 설치 유형 선택
  - 3단계. 가상 중앙 관리 서버의 이름 지정
  - 4단계. 가상 중앙 관리 서버의 네트워크 세부 정보 지정
  - 5단계. 클러스터 그룹 지정
  - 6단계. 클러스터 데이터 스토리지 선택
  - 7단계. 원격 설치를 위한 계정 지정
  - 8단계. 설치할 구성 요소 선택
  - 9단계. 네트워크 크기 선택
  - 10단계. 데이터베이스 선택
  - 11단계. SQL 서버 구성
  - 12단계. 인증 모드 선택
  - 13단계. 중앙 관리 서버를 시작할 계정 선택
  - 14단계. Kaspersky Security Center 서비스를 실행하기 위한 계정 선택
  - 15단계. 공유 폴더 선택
  - 16단계. 중앙 관리 서버에 대한 연결 구성
  - 17단계. 중앙 관리 서버 주소 정의
  - 18단계. 모바일 기기 연결에 사용할 중앙 관리 서버 주소
  - 19단계. 하드 드라이브에 파일 압축 해제 및 설치
- 숨김 모드로 중앙 관리 서버 설치
- 관리자의 워크스테이션에 관리 콘솔 설치
- Kaspersky Security Center 설치 후 시스템 변경 사항
- 애플리케이션 제거

Kaspersky Security Center 업그레이드 정보

- 이전 버전에서 Kaspersky Security Center 업그레이드
- Kaspersky Security Center 장애 조치 클러스터 노드에 Kaspersky Security Center 업그레이드
- Microsoft 장애 조치 클러스터 노드에 Kaspersky Security Center 업그레이드

Kaspersky Security Center 초기 설정

- 강화 가이드
- 중앙 관리 서버 빠른 시작 마법사
  - 빠른 시작 마법사 정보
  - 중앙 관리 서버 빠른 시작 마법사 시작
  - 1단계. 프록시 서버 구성
  - 2단계. 애플리케이션 활성화 방법 선택
  - 3단계. 보호 영역 및 운영 체제 선택
  - 4단계. 관리 중인 애플리케이션에 대한 플러그인 선택
  - 5단계. 배포 패키지 다운로드 및 설치 패키지 생성
  - 6단계. Kaspersky Security Network 사용 구성
  - 7단계. 이메일 알림 구성

8단계. 업데이트 관리 구성
9단계. 초기 보호 구성 만들기
10단계. 모바일 기기 연결
11단계. 업데이트 다운로드
12단계. 기기 발견
13단계. 빠른 시작 마법사 닫기
중앙 관리 서버로의 관리 콘솔 연결 구성
중앙 관리 서버의 인터넷 액세스 설정 구성
이동 사용자 기기 연결
시나리오: 연결 게이트웨이를 통해 이동 사용자 기기 연결
시나리오: DMZ의 보조 중앙 관리 서버를 통해 부재 중 기기 연결
이동 사용자 기기 연결 정보
중앙 관리 서버에 외부 데스크톱 기기 연결
이동 사용자를 위한 연결 프로필 정보
이동 사용자에 대한 연결 프로필 만들기
다른 중앙 관리 서버로 네트워크 에이전트 전환 정보
네트워크 위치에 따른 네트워크 에이전트 전환 규칙 만들기
이벤트 알림
이벤트 알림 구성
테스트 알림
실행 파일을 실행하면 표시되는 이벤트 알림
TLS를 사용하여 통신 암호화
인터페이스 구성
네트워크에 연결된 기기 발견
시나리오: 네트워크에 연결된 기기 발견
미할당 기기
기기 발견
Windows 네트워크 검색
Active Directory 검색
IP 범위 검색
Zeroconf 폴링
Windows 도메인 작업. 도메인 설정 보기 및 변경
미할당 기기에 대한 보존 규칙 구성
IP 범위 작업
IP 범위 만들기
IP 범위 설정 보기 및 변경
Active Directory 그룹 작업. 그룹 설정 보기 및 수정
자동으로 기기를 관리 그룹으로 이동하는 규칙 만들기
클라이언트 기기에서 VDI 동적 모드 사용
네트워크 에이전트 설치 패키지의 속성에서 VDI 동적 모드 사용
VDI를 구성하는 기기 검색
VDI를 구성하는 기기를 관리 그룹으로 이동
장비 재고
새 기기에 대한 정보 추가
기업 기기를 정의하는 데 사용한 기준 구성
사용자 지정 필드 구성

- 라이센스
  - 라이센스 제한 초과 이벤트
  - 라이센스 정보
    - 라이센스 정보
    - 최종 사용자 라이센스 계약서 정보
    - 라이센스 인증서 정보
    - 라이센스 키 정보
    - 라이센스 키 파일 정보
    - 서브스크립션 정보
    - 활성화코드 정보
    - 최종 사용자 라이센스 계약서 동의 취소
  - 데이터 제공 정보
  - Kaspersky Security Center 라이센스 옵션
  - Kaspersky Security Center 및 관리 애플리케이션의 라이센스 기능
- Kaspersky 애플리케이션. 중앙 집중식 배포
  - 타사 보안 제품 교체
  - 원격 설치 작업을 사용하여 애플리케이션 설치
    - 선택한 기기에 애플리케이션 설치
    - 관리 그룹의 클라이언트 기기에 애플리케이션 설치
    - Active Directory 그룹 정책을 통해 애플리케이션 설치
    - macOS 기기에 애플리케이션 원격 설치
    - 보조 중앙 관리 서버에 애플리케이션 설치
  - 원격 설치 마법사를 사용하여 애플리케이션 설치
  - 관리 플러그인 작업
  - 보호 배포 리포트 보기
  - 애플리케이션 원격 제거
    - 관리 그룹의 클라이언트 기기에서 애플리케이션 원격 제거
    - 선택한 기기에서 애플리케이션 원격 제거
  - 설치 패키지 사용
    - 설치 패키지 만들기
    - 독립 실행형 설치 패키지 만들기
    - 사용자 지정 설치 패키지 만들기
    - 사용자 지정 설치 패키지의 속성 확인 및 편집
    - Kaspersky Security Center 배포 키트에서 네트워크 에이전트 설치 패키지 받기
    - 보조 중앙 관리 서버에 설치 패키지 배포
    - 배포 지점을 통해 설치 패키지 배포
    - Kaspersky Security Center에 애플리케이션 설치 결과 전송
    - 설치 패키지에 대한 KSN 프록시 서버 주소 정의
  - 최신 버전의 애플리케이션 가져오기
  - Windows 기기에서 원격 설치 준비
  - Linux 기기 준비 및 Linux 기기에 네트워크 에이전트 원격 설치
    - 네트워크 에이전트 설치를 위해 SUSE Linux Enterprise Server 15를 실행하는 기기 준비
  - 네트워크 에이전트 원격 설치를 위한 macOS 기기 준비
- Kaspersky 애플리케이션: 라이센싱 및 활성화
  - 관리 애플리케이션 라이센싱
  - 사용 중인 라이센스 키 정보 보기
  - 중앙 관리 서버 저장소에 라이센스 키 추가

- 중앙 관리 서버 라이센스 키 삭제
- 클라이언트 기기에 라이센스 키 배포
- 라이센스 키 자동 배포
- 라이센스 키 사용 리포트 만들기 및 보기
- 애플리케이션 라이센스 키에 대한 정보 보기
- 라이센스 키 파일 내보내기

네트워크 보호 구성

- 시나리오: 네트워크 보호 구성
- 정책 설정 및 전파: 기기 중심 방식
- 기기 중심 및 사용자 중심 보안 관리 방식 정보
- Kaspersky Endpoint Security 정책 수동 설정
  - 지능형 위협 보호 섹션의 정책 구성
  - 필수 위협 보호 섹션의 정책 구성
  - 일반 설정 섹션의 정책 구성
  - 이벤트 구성 섹션의 정책 구성
- Kaspersky Endpoint Security용 그룹 업데이트 작업 수동 설정
- Kaspersky Endpoint Security가 설치된 기기 검사를 위한 그룹 작업 수동 설정
- 취약점 및 필요한 업데이트 검색 작업 스케줄 지정
- 업데이트 설치 및 취약점 수정을 위한 그룹 작업 수동 설정
- 이벤트 저장소에 저장되는 최대 이벤트 수 설정
- 수정된 취약점에 대한 정보의 최대 보관 기간 설정
- 작업 관리
  - 작업 만들기
  - 중앙 관리 서버 작업 생성
  - 특정 기기 작업 만들기
  - 로컬 작업 만들기
  - 중첩된 그룹의 작업 영역에서 상속된 그룹 작업 표시
  - 작업이 실행되기 전에 자동으로 기기 켜기
  - 작업이 완료된 후 자동으로 기기 끄기
  - 작업 실행 시간 제한
  - 작업 내보내기
  - 작업 가져오기
  - 작업 변환
  - 수동으로 작업 시작 및 중지
  - 수동으로 작업 일시 중지 및 다시 시작
  - 작업 실행 감시
  - 중앙 관리 서버에 저장된 작업 실행 결과 보기
  - 작업 실행 결과에 대한 정보 필터링 구성
  - 작업 수정. 변경 사항 롤백
  - 작업 비교
  - 작업을 시작할 계정
  - 작업 실행 기록 내보내기
  - 작업 암호 변경 마법사
    - 1단계. 자격증명 지정
    - 2단계. 수행할 작업 선택
    - 3단계. 결과 확인
- 가상 중앙 관리 서버에 종속되는 관리 그룹의 계층 구조 생성

정책 및 정책 프로필
정책 프로필을 사용하는 정책 계층 구조
정책 계층 구조
정책 프로필
정책 설정 상속
정책 관리
정책 만들기
하위 그룹에 상속된 정책 표시
정책 활성
바이러스 급증 이벤트 시 자동으로 정책 활성화
이동 사용자 정책 적용
정책 수정. 변경 사항 롤백
정책 비교
정책 배포 상태 차트 보기
정책 삭제
정책 복사
정책 내보내기
정책 가져오기
정책 변환
정책 프로필 관리
정책 프로필 만들기
정책 프로필 수정
정책 프로필 삭제
정책 프로필 활성화 규칙 만들기
기기 이동 규칙
기기 이동 규칙 복제
소프트웨어 분류
클라이언트 조직의 기기에 애플리케이션을 설치하기 위한 필수 구성 요소
로컬 애플리케이션 설정 보기 및 편집
Kaspersky Security Center 및 관리 중인 애플리케이션 업데이트
시나리오: Kaspersky 데이터베이스 및 애플리케이션의 정기적 업데이트
Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 업데이트 정보
Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트 시 diff 파일 사용에 대한 정보
diff 파일 다운로드 기능 활성화
중앙 관리 서버 저장소 업데이트 다운로드 작업 생성
배포 지점의 저장소로 업데이트 다운로드 작업 생성
중앙 관리 서버 저장소 업데이트 다운로드 작업 구성
다운로드한 업데이트 검증
테스트 정책 및 보조 작업 구성
다운로드된 업데이트 보기
기기에서 Kaspersky Endpoint Security 업데이트 자동 설치
업데이트 다운로드의 오프라인 모델
업데이트 다운로드 오프라인 모델 활성 및 비활성
Kaspersky Security Center 구성 요소 자동 업데이트 및 패치
Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성/비활성

업데이트 자동 배포
클라이언트 기기에 업데이트 자동 배포
보조 중앙 관리 서버에 업데이트 자동 배포
배포 지점 자동 할당
수동으로 배포 지점 기기 할당
배포 지점 목록에서 기기 제거
배포 지점을 통해 업데이트 다운로드
저장소에서 소프트웨어 업데이트 삭제
클러스터 모드에서 Kaspersky 애플리케이션에 대한 패치 설치
클라이언트 기기에서 타사 애플리케이션 관리
타사 애플리케이션 정보
타사 소프트웨어 업데이트 설치
시나리오: 타사 소프트웨어 업데이트
타사 애플리케이션에 사용 가능한 업데이트에 대한 정보 보기
소프트웨어 업데이트 승인 및 거부
중앙 관리 서버로 Windows 업데이트의 업데이트 동기화
1단계. 트래픽 감소 여부 정의
2단계. 애플리케이션
3단계. 업데이트 카테고리
4단계. 업데이트 언어
5단계. 작업을 시작할 계정 선택
6단계. 작업 시작 스케줄 구성
7단계. 작업 이름 정의
8단계. 작업 생성 완료
기기에 수동으로 업데이트 설치
네트워크 에이전트 정책에 Windows 업데이트 구성
타사 소프트웨어 취약점 수정
시나리오: 타사 소프트웨어 취약점 찾기 및 수정
소프트웨어 취약점 찾기 및 수정 정보
소프트웨어 취약점 정보 보기
관리 중인 기기의 취약점 통계 보기
취약점이 있는지 애플리케이션 검사
애플리케이션의 취약점 수정
격리된 네트워크의 취약점 수정
시나리오: 격리된 네트워크에서 타사 소프트웨어 취약점 수정
격리된 네트워크에서 타사 소프트웨어 취약점 수정 정보
격리된 네트워크의 취약점을 수정하기 위해 인터넷 액세스를 사용하여 중앙 관리 서버 구성
격리된 네트워크의 취약점을 수정하도록 격리된 중앙 관리 서버 구성
격리된 네트워크에서 패치 관리 및 업데이트 설치
격리된 네트워크에서 패치를 전송하고 업데이트를 설치할 수 있는 옵션 비활성화
소프트웨어 취약점 무시
타사 소프트웨어의 취약점에 사용자 수정 선택
업데이트 설치에 대한 규칙
애플리케이션 그룹
애플리케이션 제어로 실행 파일 관리
클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기
Kaspersky Endpoint Security for Windows 정책용 애플리케이션 카테고리 생성

수동으로 추가된 컨텐츠가 있는 애플리케이션 카테고리 만들기
선택한 기기의 실행 파일을 포함하는 애플리케이션 카테고리 만들기
특정 폴더의 실행 파일을 포함하는 애플리케이션 카테고리 만들기
애플리케이션 카테고리에 이벤트 관련 실행 파일 추가
클라이언트 기기의 애플리케이션 시작 관리 구성
실행 파일에 적용된 시작 규칙의 통계 분석 결과 보기
자산 관리(소프트웨어) 보기
소프트웨어 인벤토리 시작 시간 변경
타사 애플리케이션의 라이센스 키 관리 정보
유료 애플리케이션 그룹 만들기
유료 애플리케이션 그룹의 라이센스 키 관리
실행 파일 인벤토리
실행 파일에 대한 정보 보기
모니터링 및 보고
시나리오: 모니터링 및 보고
관리 콘솔에서 표시등 및 기록된 이벤트 모니터링
리포트, 통계 및 알림 작업
리포트 작업
리포트 템플릿 만들기
리포트 템플릿 속성 보기 및 편집
리포트 템플릿의 확장 필터 형식
필터를 확장 형식으로 변환
확장 필터 구성
리포트 만들기 및 보기
리포트 저장
리포트 전달 작업 만들기
1단계. 작업 유형 선택
2단계. 리포트 유형 선택
3단계. 리포트에 대한 작업
4단계. 작업을 시작할 계정 선택
5단계. 작업 스케줄 구성
6단계. 작업 이름 정의
7단계. 작업 생성 완료
통계 관리
이벤트 알림 구성
SMTP 서버용 인증서 발급
이벤트 조회
이벤트 조회 보기
이벤트 조회 사용자정의
이벤트 조회 만들기
이벤트 조회를 텍스트 파일로 내보내기
조회에서 이벤트 삭제
사용자 요청에 따라 예외에 애플리케이션 추가
기기 조회
기기 조회 보기
기기 조회 구성
기기 조회 설정을 파일로 내보내기

기기 조회 만들기
가져온 설정에 따라 기기 조회 만들기
조회된 관리 그룹에서 기기 제거
애플리케이션 설치 및 제거 모니터링
Kaspersky Security Center 구성 요소의 이벤트
이벤트 유형 데이터 구조 설명
중앙 관리 서버 이벤트
중앙 관리 서버 심각 이벤트
중앙 관리 서버 기능 실패 이벤트
중앙 관리 서버 경고 이벤트
중앙 관리 서버 정보 이벤트
네트워크 에이전트 이벤트
네트워크 에이전트 기능 실패 이벤트
네트워크 에이전트 경고 이벤트
네트워크 에이전트 정보 이벤트
iOS MDM 서버 이벤트
iOS MDM 서버 기능 실패 이벤트
iOS MDM 서버 경고 이벤트
iOS MDM 서버 정보 이벤트
자주 등록된 이벤트 차단 중
자주 등록된 이벤트 차단 정보
자주 등록된 이벤트 차단 관리
자주 등록된 이벤트 차단 제거
자주 등록된 이벤트 목록을 파일로 내보내기
가상 컴퓨터의 상태 변경 사항 제어
시스템 레지스트리의 정보를 사용하여 안티 바이러스 보호 상태 모니터링
기기가 비활성 상태로 표시될 때 작업 보기 및 구성
Kaspersky 공지 비활성화
배포 지점 및 연결 게이트웨이 조정
배포 지점의 표준 구성: 단일 사무소
배포 지점의 표준 구성: 다수의 소규모 원격 사무소
배포 지점 역할을 할 관리 중인 기기 추가
완충 지대에서 Linux 기기를 게이트웨이로 연결
연결 게이트웨이를 통해 Linux 기기를 중앙 관리 서버에 연결
DMZ에 배포 지점으로 연결 게이트웨이 추가
배포 지점 자동 할당
배포 지점으로 선택한 기기에 네트워크 에이전트 로컬 설치 정보
배포 지점을 연결 게이트웨이로 사용 정보
배포 지점에서 검색되는 범위 목록에 IP 범위 추가
배포 지점을 연결 게이트웨이로 사용
기타 정기 작업
중앙 관리 서버 관리
중앙 관리 서버 계층 만들기 및 보조 중앙 관리 서버 추가
중앙 관리 서버에 연결 및 중앙 관리 서버 간 전환
중앙 관리 서버와 해당 개체에 대한 접근 권한
인터넷을 통한 중앙 관리 서버 연결 조건

- 중앙 관리 서버에 대한 암호화된 연결
  - 기기 연결 시 중앙 관리 서버 인증
  - 관리 콘솔 연결 시 중앙 관리 서버 인증
- 중앙 관리 서버에 연결할 IP 주소의 허용 목록 구성
- Klscflag 유틸리티를 사용하여 포트 13291 닫기
- 중앙 관리 서버에서 연결 끊는 방법
- 콘솔 트리에 중앙 관리 서버 추가
- 콘솔 트리에서 중앙 관리 서버 제거
- 콘솔 트리에 가상 중앙 관리 서버 추가
- 중앙 관리 서버 서비스 계정 변경. klsrvswch 유틸리티
- DBMS 자격증명 변경
- 중앙 관리 서버 공유 폴더 변경
- 중앙 관리 서버 노드의 문제 해결
- 중앙 관리 서버의 설정 보기 및 수정
  - 중앙 관리 서버의 일반 조정
  - 관리 콘솔 인터페이스 설정
  - 중앙 관리 서버에서의 이벤트 처리 및 저장소
  - 중앙 관리 서버로의 연결 로그 보기
  - 바이러스 급증 제어
  - 트래픽 제한
  - 웹 서버 구성
  - 내부 사용자 작업
- 중앙 관리 서버 설정 백업 및 복원
  - 파일 시스템 스냅샷을 사용하여 백업 시간 단축
  - 중앙 관리 서버가 설치된 기기가 작동하지 않음
  - 데이터베이스 또는 중앙 관리 서버의 설정이 손상됨
- 중앙 관리 서버 데이터의 백업 복사 및 복원
  - 중앙 관리 서버 데이터 백업 작업
  - 데이터 백업 및 복구 유틸리티(klbackup)
  - 대화식 모드에서 데이터 백업 및 복구
  - 숨김 모드에서 데이터 백업 및 복구
  - klbackup 유틸리티를 사용하여 다른 중앙 관리 서버에서 관리 중인 기기 전환
  - MySQL 또는 MariaDB 사용 시 중앙 관리 서버 데이터 백업 및 복원
  - 중앙 관리 서버 데이터의 백업 및 복원 최적화
- 다른 기기로 중앙 관리 서버 이동
- 여러 중앙 관리 서버 간의 충돌 방지

관리 그룹 관리

- 관리 그룹 생성
- 관리 그룹 이동
- 관리 그룹 삭제
- 관리 그룹의 구조 자동으로 만들기
- 관리 그룹에 있는 기기에 애플리케이션 자동 설치

클라이언트 기기 관리

- 클라이언트 기기를 중앙 관리 서버에 연결
- 클라이언트 기기를 중앙 관리 서버에 수동으로 연결. Klmover 유틸리티
- 클라이언트 기기와 중앙 관리 서버 간 연결 터널링

- 클라이언트 기기 데스크톱에 원격 연결
  - Windows 클라이언트 기기에 연결
  - macOS 클라이언트 기기에 연결
- Windows 데스크톱 공유를 통해 기기에 연결
- 클라이언트 기기 다시 시작 구성
- 원격 클라이언트 기기에서의 활동 감사
- 클라이언트 기기와 중앙 관리 서버 간 연결 상태 확인
  - 클라이언트 기기와 중앙 관리 서버 간 연결 상태 자동 확인
  - 클라이언트 기기와 중앙 관리 서버 간 연결 상태 수동 확인. Klnagchk 유틸리티
  - 기기와 중앙 관리 서버 간 연결 시간 확인 정보
- 중앙 관리 서버에서 클라이언트 기기 식별
- 관리 그룹로 기기 이동
- 클라이언트 기기의 중앙 관리 서버 변경
- 연결 게이트웨이를 통해 중앙 관리 서버에 연결된 기기를 다른 중앙 관리 서버로 이동
- 클러스터 및 서버 배열
- 클라이언트 기기 원격 켜기, 끄기 및 다시 시작
- 관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결 사용 정보
- 강제 동기화 정보
- 연결 스케줄 정보
- 기기 사용자에게 메시지 보내기
- Kaspersky Security for Virtualization 관리
- 기기 상태 전환 구성
- 기기 태그 및 할당된 태그 보기
  - 자동으로 기기 태그
  - 기기에 할당된 태그 보기 및 구성
- 클라이언트 기기 원격 진단. Kaspersky Security Center 원격 진단 유틸리티
  - 클라이언트 기기에 원격 진단 유틸리티 연결
  - 애플리케이션에 대한 덤프 파일 생성
  - 추적 로그 작동 및 중지, 추적 로그 파일 다운로드
  - 애플리케이션 설정 다운로드
  - 이벤트 로그 다운로드
  - 여러 진단 정보 항목 다운로드
  - 진단 시작 및 그 결과 다운로드
  - 애플리케이션 시작, 중지 및 다시 시작
- UEFI 보호 기기
- 관리 중인 기기 설정
- 일반 정책 설정
- 네트워크 에이전트 정책 설정

사용자 계정 관리

- 사용자 계정 작업
- 내부 사용자의 계정 추가
- 내부 사용자의 계정 편집
- 허용되는 암호 입력 시도 횟수 변경
- 내부 사용자 이름의 고유성을 확인하는 기능 구성
- 보안 그룹 추가
- 그룹에 사용자 추가

애플리케이션 기능에 대한 접근 권한 구성. 역할 기반 접근 제어
애플리케이션 기능에 대한 접근 권한
사전 정의된 사용자 역할
사용자 역할 추가
사용자 또는 보안 그룹에 역할 할당
사용자 및 그룹에 권한 할당
보조 중앙 관리 서버에 사용자 역할 전파
기기 소유자로 특정 사용자 지정
공지 메시지 배포
사용자 모바일 기기 목록 보기
사용자용 인증서 설치
사용자에게 발급된 인증서 목록 보기
가상 중앙 관리 서버의 관리자 정보
운영 체제와 애플리케이션의 원격 설치
운영 체제의 이미지 만들기
운영 체제 이미지 설치
KSN 프록시 서버 주소 구성
Windows 사전 설치 환경(WinPE)용 드라이버 추가
운영 체제 이미지가 있는 설치 패키지에 드라이버 추가
sysprep.exe 유틸리티 구성
새 네트워크 기기에 운영 체제 배포
클라이언트 기기에 운영 체제 배포
애플리케이션의 설치 패키지 만들기
애플리케이션 설치 패키지용 인증서 발급
클라이언트 기기에 애플리케이션 설치
개체 리비전 관리
개체 리비전 정보
리비전 내역 섹션 보기
개체 리비전 비교
개체 리비전 및 삭제된 개체 정보의 저장 기간 설정
개체 리비전 확인
개체 리비전을 파일에 저장
변경 사항 롤백
리비전 설명 추가
개체 삭제
개체 삭제
삭제된 개체에 대한 정보 보기
삭제된 개체 목록에서 영구적으로 개체 삭제
모바일 기기 매니지먼트
시나리오: 모바일 기기 관리 배포
iOS MDM 기기 관리를 위한 그룹 정책 정보
모바일 기기 매니지먼트 활성화
모바일 기기 관리 설정 수정
모바일 기기 매니지먼트 비활성화
모바일 기기용 명령 사용
모바일 기기 관리 명령
Firebase Cloud Messaging 사용

명령 보내기
명령 로그에서 명령 상태 보기
모바일 기기의 인증서 작업
인증서 설치 마법사 시작
1단계. 인증서 유형 선택
2단계. 기기 유형 선택
3단계. 사용자 선택
4단계. 인증서 경로 선택
5단계. 인증서에 태그 할당
6단계. 인증서 게시 설정 지정
7단계. 사용자 알림 방법 선택
8단계. 인증서 생성
인증서 발급 규칙 구성
공개 키 인프라와의 통합
Kerberos 제한된 위임 지원 작동
관리 중인 기기 목록에 iOS 모바일 기기 추가
관리 중인 기기 목록에 Android 모바일 기기 추가
iOS MDM 기기 관리
인증서로 iOS MDM 프로필 서명
구성 프로필 추가
기기에 구성 프로필 설치
기기에서 구성 프로필 제거
프로필에 대한 링크를 게시하여 새 기기 추가
관리자가 프로필을 설치하는 방식으로 새 모바일 기기 추가
프로비저닝 프로필 추가
기기에 프로비저닝 프로필 설치
기기에서 프로비저닝 프로필 제거
관리 애플리케이션 추가
모바일 기기에 앱 설치
기기에서 앱 제거
iOS MDM 모바일 기기에서 로밍 구성
iOS MDM 기기 정보 보기
관리에서 iOS MDM 기기 연결 끊기
기기에 명령 보내기
보낸 명령의 실행 상태 확인
KES 기기 관리
KES 기기용 모바일 애플리케이션 패키지 만들기
KES 기기의 인증서 기반 인증 활성
KES 기기 정보 보기
관리에서 KES 기기 연결 끊기
데이터 암호화 및 보호
암호화된 기기 목록 보기
암호화 이벤트 목록 보기
암호화 이벤트 목록을 텍스트 파일로 내보내기
암호화 리포트 만들기 및 보기
중앙 관리 서버 간 암호화 키 전송

데이터 저장소
저장소 개체 목록을 텍스트 파일로 내보내기
설치 패키지
저장소에 있는 파일의 주요 상태
스마트 학습 모드인 규칙 트리거링
적응형 이상 행위 제어 규칙을 사용하여 수행된 탐지 목록 보기
적응형 이상 행위 제어 규칙에서 예외 추가
1단계. 애플리케이션 선택
2단계. 하나 이상의 정책 선택
3단계. 하나 이상의 정책 처리
격리 및 백업 저장소
저장소 파일에 대한 원격 관리 작동
저장소에 보관된 파일의 속성 보기
저장소에서 파일 삭제
저장소에서 파일 복원
저장소에서 디스크로 파일 저장
격리 저장소의 파일 검사
처리 안 된 위협
처리 안 된 파일 치료
처리 안 된 파일을 디스크에 저장
"처리 안 된 위협" 폴더에서 파일 삭제
Kaspersky Security Network(KSN)
KSN 정보
Kaspersky Security Network에 대한 접근 설정
KSN 사용 및 중지
수락한 KSN 성명서 보기
KSN 프록시 서버 통계 확인
업데이트된 KSN 성명서 수락
Kaspersky Security Network로 더욱 향상된 보호 제공
배포 지점이 KSN 프록시 서버로 작동하는지 확인
온라인 도움말과 오프라인 도움말 간 전환
SIEM 시스템으로 이벤트 내보내기
SIEM 시스템으로 이벤트 내보내기 구성
시작하기 전에
Kaspersky Security Center의 이벤트 정보
이벤트 내보내기 정보
SIEM 시스템에서 이벤트 내보내기 구성 정보
Syslog 형식으로 SIEM 시스템으로 내보내기 위한 이벤트 표시
Syslog 형식으로 내보내기 위한 Kaspersky 애플리케이션의 이벤트 표시
Syslog 형식으로 내보낼 일반 이벤트 표시
Syslog 형식을 사용한 이벤트 내보내기 정보
CEF 및 LEEF 형식을 사용하여 이벤트 내보내기 정보
SIEM 시스템으로 이벤트를 내보내기 위한 Kaspersky Security Center 구성

데이터베이스에서 직접 이벤트 내보내기
klsql2 유틸리티를 사용하여 SQL 쿼리 생성
klsql2 유틸리티의 SQL 쿼리 예제
Kaspersky Security Center 데이터베이스 이름 확인
내보내기 결과 보기
SNMP를 사용하여 타사 애플리케이션에 통계 보내기
Kaspersky Security Center와 함께 사용할 SNMP 서비스 구성
SNMP 에이전트 및 개체 식별자
개체 식별자에서 문자열 카운터 이름 가져오기
SNMP에 대한 개체 식별자 값
문제 해결
클라우드 환경에서 작업
클라우드 환경에서 작업 정보
시나리오: 클라우드 환경용 배포
클라우드 환경에서 Kaspersky Security Center를 배포하기 위한 필수 구성 요소
클라우드 환경에 있는 중앙 관리 서버용 하드웨어 요구 사항
클라우드 환경의 라이센스 옵션
클라우드 환경에서 작업하기 위한 데이터베이스 옵션
Amazon Web Services 클라우드 환경 사용
Amazon Web Services 클라우드 환경에서의 작업 정보
Amazon EC2 인스턴스용 IAM 역할 및 IAM 사용자 계정 생성
Kaspersky Security Center 중앙 관리 서버에 AWS와 연동할 권한이 있는지 확인
중앙 관리 서버에 대한 IAM 역할 생성
Kaspersky Security Center와의 연동을 위한 IAM 사용자 계정 만들기
Amazon EC2 인스턴스에 애플리케이션 설치를 위한 IAM 역할 생성
Azure RDS 사용
Amazon RDS 인스턴스 생성
Amazon RDS 인스턴스용 옵션 그룹 생성
옵션 그룹 수정
Amazon RDS DB 인스턴스용 IAM 역할의 권한 수정
데이터베이스용 Amazon S3 버킷 준비
Amazon RDS로 데이터베이스 마이그레이션
Microsoft Azure 클라우드 환경에서 작업
Microsoft Azure에서 작업 수행 정보
서브스크립션, 애플리케이션 ID 및 암호 생성
Azure 애플리케이션 ID에 역할 할당
Microsoft Azure에 중앙 관리 서버 배포 및 데이터베이스 선택
Azure SQL 작업
Azure 스토리지 계정 생성
Azure SQL 데이터베이스 및 SQL Server 생성
Azure SQL로 데이터베이스 마이그레이션
Google 클라우드에서 작업
클라이언트 이메일, 프로젝트 ID, 개인 키 생성
Google Cloud SQL for MySQL 인스턴스로 작업
Kaspersky Security Center 연동을 위한 클라우드 환경에서의 클라이언트 기기 준비
클라우드 환경 구성에 필요한 설치 패키지 생성

- 클라우드 환경 구성
  - 클라우드 환경 구성 마법사 정보
  - 1단계. 애플리케이션 활성화 방법 선택
  - 2단계. 클라우드 환경 선택
  - 3단계. 클라우드 환경에서 인증
  - 4단계. 클라우드와의 동기화 구성 및 추가 작업 선택
  - 5단계. 클라우드 환경에서 Kaspersky Security Network 구성
  - 6단계. 클라우드 환경에서 이메일 알림 구성
  - 7단계. 클라우드 환경 보호를 위한 초기 구성 생성
  - 8단계. 설치 중에 운영 체제를 다시 시작해야 할 때의 작업 선택 (클라우드 환경의 경우)
  - 9단계. 중앙 관리 서버에서 업데이트 받기
- 구성 확인
- 클라우드 기기 그룹
- 네트워크 세그먼트 검색
  - 클라우드 세그먼트 검색에 대한 연결 추가
  - 클라우드 세그먼트 검색에 대한 연결 삭제
  - 검색 스케줄 구성
- 클라우드 환경의 기기에 애플리케이션 설치
- 클라우드 기기 속성 보기
- 클라우드와 동기화
- Yandex.Cloud에 Kaspersky Security Center 배포

부록

- 고급 옵션
  - Kaspersky Security Center 작동 자동화. klakaut utility
  - 사용자 지정 도구
  - 네트워크 에이전트 디스크 복제 모드
  - 운영 체제 이미지 생성을 위해 설치된 네트워크 에이전트로 참조 기기 준비
  - 파일 무결성 모니터에서 메시지 수신 구성
  - 중앙 관리 서버 점검
  - 공용 DNS 서버 접근
  - 사용자 알림 방법 창
  - 기기 조회 창
  - 새 개체 창의 이름 정의
- 관리 인터페이스 사용 기능
  - 콘솔 트리
  - 작업 영역에서 데이터를 업데이트하는 방법
  - 콘솔 트리를 탐색하는 방법
  - 작업 영역에서 개체 속성 창을 여는 방법
  - 작업 영역에서 개체 그룹을 선택하는 방법
  - 작업 영역에서 열 집합을 변경하는 방법
- 참조 정보
  - 마우스 오른쪽 메뉴 명령
  - 관리 중인 기기 목록. 열 설명
  - 기기, 작업 및 정책의 상태
  - 관리 콘솔의 파일 상태 아이콘

데이터 검색 및 내보내기
기기 찾기
기기 검색 설정
문자열 값에 마스크 사용
검색 필드에서 정규식 사용
대화상자에서 목록 내보내기
작업 설정
일반 작업 설정
중앙 관리 서버 저장소에 업데이트 다운로드 작업 설정
배포 지점의 저장소로 업데이트 다운로드 작업 설정
취약점 및 필요한 업데이트 검색 작업 설정
취약점 관련 업데이트를 설치하고 취약점 수정 작업 설정
글로벌 서브넷 목록
글로벌 서브넷 목록에 서브넷 추가
글로벌 서브넷 목록에서 서브넷 속성 보기 및 수정
Windows, Linux, macOS용 네트워크 에이전트 사용: 비교
Kaspersky Security Center 웹 콘솔
Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔의 배포 다이어그램
Kaspersky Security Center 웹 콘솔에서 사용되는 포트
Kaspersky Security Center 웹 콘솔 인터페이스
메인 메뉴의 섹션 고정 및 고정 해제
시나리오: Kaspersky Security Center 웹 콘솔의 설치 및 초기 설정
설치
Kaspersky Security Center 설치(표준 설치)
Kaspersky Security Center 웹 콘솔 설치
장애 조치 클러스터 노드에 설치된 중앙 관리 서버에 연결된 Kaspersky Security Center 웹 콘솔 설치
Kaspersky Security Center 웹 콘솔 업그레이드
Kaspersky Security Center 웹 콘솔 작업용 인증서
Kaspersky Security Center 웹 콘솔용 인증서 재발급
Kaspersky Security Center 웹 콘솔 인증서 교체
Kaspersky Security Center 웹 콘솔에서 신뢰하는 중앙 관리 서버에 대한 인증서 지정
PFX 인증서를 PEM 형식으로 변환
Kaspersky Security Center Windows에서 마이그레이션
Kaspersky Security Center Cloud Console로 마이그레이션
Kaspersky Next XDR Expert로 마이그레이션
Kaspersky Security Center Linux로 마이그레이션
중앙 관리 서버 데이터 백업을 사용하여 Kaspersky Security Center Linux로 마이그레이션
마이그레이션 마법사를 사용하여 Kaspersky Security Center Linux로 마이그레이션
Kaspersky Security Center Windows에서 그룹 개체 내보내기
Kaspersky Security Center Linux로 내보내기 파일 가져오기
관리 중인 기기를 Kaspersky Security Center Linux에서 관리하도록 전환
Kaspersky Security Center 웹 콘솔 로그인 및 로그아웃
Kaspersky Security Center 웹 콘솔의 ID 및 액세스 관리
ID 및 액세스 관리 정보
ID 및 액세스 관리 활성화: 시나리오
Kaspersky Security Center 웹 콘솔에서 ID 및 액세스 관리 구성
Kaspersky Security Center 웹 콘솔에 Kaspersky Industrial CyberSecurity for Networks 애플리케이션 등록

ID 및 액세스 관리의 토큰 수명 및 인증 시간 초과 값
IAM 인증서 다운로드 및 배포
ID 및 액세스 관리 비활성화
NTLM 및 Kerberos 프로토콜을 사용하여 도메인 인증 구성
중앙 관리 서버 구성
Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 연결 구성
중앙 관리 서버 연결 이벤트 로깅 기록
중앙 관리 서버의 인터넷 액세스 설정 구성
이벤트 저장소에 저장되는 최대 이벤트 수 설정
UEFI 보호 기기의 연결 설정
중앙 관리 서버 계층 만들기 및 보조 중앙 관리 서버 추가
보조 중앙 관리 서버의 목록 보기
중앙 관리 서버의 계층 구조 삭제
중앙 관리 서버 점검
인터페이스 구성
가상 중앙 관리 서버 관리
가상 중앙 관리 서버 만들기
가상 중앙 관리 서버 활성화 및 비활성화
가상 중앙 관리 서버의 관리자 정보
클라이언트 기기의 중앙 관리 서버 변경
가상 중앙 관리 서버 삭제
무단 수정으로부터 계정 보호 활성화
중앙 관리 서버 데이터의 백업 복사 및 복원
데이터 백업 작업 만들기
다른 기기로 중앙 관리 서버 이동
klscmodchk 및 integrity_checker 유틸리티를 사용하여 모듈 무결성 확인
Kaspersky Security Center 웹 콘솔 초기 설정
빠른 시작 마법사(Kaspersky Security Center 웹 콘솔)
1단계. 인터넷 연결 설정 지정
2단계. 필수 업데이트 다운로드 중
3단계. 확보할 자산 선택
4단계. 솔루션 암호화 선택
5단계. 관리 중인 애플리케이션용 플러그인 설치 구성
6단계. 선택한 플러그인 설치
7단계. 배포 패키지 다운로드 및 설치 패키지 생성
8단계. Kaspersky Security Network 구성
9단계. 애플리케이션 활성화 방법 선택
10단계. 타사 업데이트 관리 설정 지정
11단계. 기본 네트워크 보호 구성 만들기
12단계. 이메일 알림 구성
13단계. 네트워크 검색 수행
14단계. 빠른 시작 마법사 닫기
이동 사용자 기기 연결
시나리오: 연결 게이트웨이를 통해 이동 사용자 기기 연결
시나리오: DMZ의 보조 중앙 관리 서버를 통해 부재 중 기기 연결
이동 사용자 기기 연결 정보
중앙 관리 서버에 외부 데스크톱 기기 연결

이동 사용자를 위한 연결 프로필 정보
이동 사용자에 대한 연결 프로필 만들기
다른 중앙 관리 서버로 네트워크 에이전트 전환 정보
네트워크 위치에 따른 네트워크 에이전트 전환 규칙 만들기
보호 배포 마법사
1단계. 보호 배포 마법사 시작
2단계. 설치 패키지 선택
3단계. 키 파일 또는 활성화 코드 배포 방법 선택
4단계. 네트워크 에이전트 버전 선택
5단계. 기기 선택
6단계. 원격 설치 작업 설정 지정
7단계. 관리 다시 시작
8단계. 설치하기 전에 비-호환 애플리케이션 제거
9단계. 관리 중인 기기로 기기 이동
10단계. 기기에 접근할 수 있는 계정 선택
11단계. 설치 시작
Kaspersky Security Center 웹 콘솔을 통한 Kaspersky 애플리케이션 배포
시나리오: Kaspersky Security Center 웹 콘솔을 통한 Kaspersky 애플리케이션 배포
Kaspersky 애플리케이션용 플러그인 받기
Kaspersky 애플리케이션용 설치 패키지 다운로드 및 생성
사용자 지정 설치 패키지 데이터의 크기 제한 변경
Kaspersky 애플리케이션용 배포 패키지 다운로드
Kaspersky Endpoint Security가 성공적으로 배포되었는지 확인
독립 실행형 설치 패키지 만들기
독립 실행형 설치 패키지 목록 보기
사용자 지정 설치 패키지 만들기
보조 중앙 관리 서버에 설치 패키지 배포
원격 설치 작업을 사용하여 애플리케이션 설치
애플리케이션 원격 설치
Active Directory 그룹 정책을 통해 애플리케이션 설치
보조 중앙 관리 서버에 애플리케이션 설치
Unix 기기에서 원격 설치용 설정 지정
Kaspersky 애플리케이션 시작 및 중지.
모바일 기기 매니지먼트
타사 보안 제품 교체
네트워크에 연결된 기기 발견
시나리오: 네트워크에 연결된 기기 발견
기기 발견
Windows 네트워크 검색
IP 범위 검색
IP 범위 추가 및 수정
Zeroconf 폴링
도메인 컨트롤러 검색
도메인 컨트롤러에 대한 인증 및 연결
Samba 도메인 컨트롤러 구성
미할당 기기에 대한 보존 규칙 구성

장비 재고
새 기기에 대한 정보 추가
기업 기기를 정의하는 데 사용한 기준 구성
Kaspersky 애플리케이션: 라이센싱 및 활성화
관리 애플리케이션 라이센싱
중앙 관리 서버 저장소에 라이센스 키 추가
중앙 관리 서버 라이센스 키 추가
클라이언트 기기에 라이센스 키 배포
라이센스 키 자동 배포
사용 중인 라이센스 키 정보 보기
저장소에서 라이센스 키 삭제
최종 사용자 라이센스 계약서 동의 취소
Kaspersky 애플리케이션 라이선스 갱신
Kaspersky 마켓플레이스를 사용하여 Kaspersky 비즈니스 솔루션 선택
네트워크 보호 구성
시나리오: 네트워크 보호 구성
기기 중심 및 사용자 중심 보안 관리 방식 정보
정책 설정 및 전파: 기기 중심 방식
정책 설정 및 전파: 사용자 중심 접근 방식
네트워크 에이전트 정책 설정
운영 체제별 네트워크 에이전트 정책 설정 비교
네트워크 에이전트의 저자원 소비 모드 활성화 및 비활성화
Kaspersky Endpoint Security 정책 수동 설정
Kaspersky Security Network 구성
방화벽으로 보호되는 네트워크 목록 확인
네트워크 드라이브 검사 비활성화
중앙 관리 서버 메모리에서 소프트웨어 세부 정보 제외
워크스테이션에서 Kaspersky Endpoint Security for Windows 인터페이스에 대한 접근 구성
중앙 관리 서버 데이터베이스에 중요한 정책 이벤트 저장
Kaspersky Endpoint Security용 그룹 업데이트 작업 수동 설정
기기 제어에 의해 차단된 외부 기기에 대한 오프라인 접근 권한 부여
애플리케이션 또는 소프트웨어 업데이트 원격 제거
작업
작업 정보
작업 범위 정보
작업 만들기
수동으로 작업 시작
작업 목록 보기
일반 작업 설정
작업 내보내기
작업 가져오기
작업 암호 변경 마법사 시작
1단계. 자격증명 지정
2단계. 수행할 작업 선택
3단계. 결과 확인

- 스크립트 원격 실행 작업 생성
  - 스크립트 원격 실행 작업을 사용하여 기기에 애플리케이션 원격 설치
  - 스크립트 원격 실행 작업에 대한 알림 및 모니터링 구성
  - 스크립트 원격 실행 작업을 위한 압축 파일 준비
  - 매니페스트 파일을 기반으로 설치 패키지 생성
- 클라이언트 기기 관리
  - 관리 중인 기기 설정
  - 관리 그룹 생성
  - 관리 그룹에 수동으로 기기 추가
  - 관리 그룹에 수동으로 기기 또는 클러스터 이동
  - 기기 이동 규칙 생성
  - 기기 이동 규칙 복사
  - 기기 이동 규칙 조건
  - 클러스터 및 서버 배열 정보
  - 클러스터 또는 서버 배열 속성
  - 기기가 비활성 상태로 표시될 때 작업 보기 및 구성
  - 기기 상태 정보
  - 기기 상태 전환 구성
  - 클라이언트 기기 데스크톱에 원격 연결
  - Windows 데스크톱 공유를 통해 기기에 연결
  - 기기 조회
    - 기기 조회에서 기기 목록 보기
    - 기기 조회 만들기
    - 기기 조회 구성
    - 기기 조회에서 기기 목록 내보내기
    - 조회된 관리 그룹에서 기기 제거
  - 기기 태그
    - 기기 태그 만들기
    - 기기 태그 이름 바꾸기
    - 기기 태그 삭제
    - 태그가 할당된 기기 보기
    - 기기에 할당된 태그 보기
    - 수동으로 기기에 태그 지정
    - 기기에서 할당된 태그 제거
    - 자동으로 기기에 태그를 지정하는 규칙 보기
    - 자동으로 기기에 태그를 지정하는 규칙 편집
    - 자동으로 기기에 태그를 지정하는 규칙 생성
    - 기기 자동 태그 지정을 위한 규칙 실행
    - 자동으로 기기에 태그를 지정하는 규칙 삭제
    - Klscflag 유틸리티를 사용하여 기기 태그 관리
- 정책 및 정책 프로필
  - 활성 정책 및 정책 프로필 정보
  - 잠금 및 잠긴 설정 정보
  - 정책 상속 및 정책 프로필
    - 정책 계층 구조
    - 정책 계층 구조의 정책 프로필
    - 관리 중인 기기에서 설정을 구현하는 방법

- 정책 관리
  - 정책 목록 보기
  - 정책 만들기
  - 정책 수정
  - 일반 정책 설정
  - 정책 상속 옵션 활성화 및 비활성화
  - 정책 복사
  - 정책 이동
  - 정책 내보내기
  - 정책 가져오기
  - 정책 배포 상태 차트 보기
  - 정책 삭제
- 정책 프로필 관리
  - 정책 프로필 보기
  - 정책 프로필 우선 순위 변경
  - 정책 프로필 만들기
  - 정책 프로필 수정
  - 정책 프로필 복사
  - 정책 프로필 활성화 규칙 만들기
  - 정책 프로필 삭제
- 데이터 암호화 및 보호
  - 암호화된 드라이브 목록 보기
  - 암호화 이벤트 목록 보기
  - 암호화 리포트 만들기 및 보기
  - 오프라인 모드에서 암호화된 드라이브에 접근 권한 부여
- 사용자 및 사용자 역할
  - 사용자 역할 정보
  - 사용자 계정 및 세션 보기
  - 애플리케이션 기능에 대한 접근 권한 구성. 역할 기반 접근 제어
    - 애플리케이션 기능에 대한 접근 권한
    - 사전 정의된 사용자 역할
    - 특정 개체에 대한 액세스 권한 할당
    - 사용자 및 보안 그룹에 접근 권한 할당
  - 내부 사용자의 계정 추가
  - 보안 그룹 생성
  - 내부 사용자의 계정 편집
  - 보안 그룹 편집
  - 사용자 또는 보안 그룹에 역할 할당
  - 내부 보안 그룹에 사용자 계정 추가
  - 기기 소유자로 특정 사용자 지정
  - 모든 사용자에 대해 2단계 인증 구성
    - 2단계 인증 정보
    - 본인 계정의 2단계 인증 활성화(웹 콘솔)
    - 본인 계정의 2단계 인증 활성화(MMC 기반)
    - 모든 사용자의 필수 2단계 인증 활성화(웹 콘솔)
    - 모든 사용자의 2단계 인증 활성화(MMC 기반)
    - 사용자 계정의 2단계 인증 비활성화(웹 콘솔)

사용자 계정의 2단계 인증 비활성화(MMC 기반)
모든 사용자의 필수 2단계 인증 비활성화(웹 콘솔)
모든 사용자의 필수 2단계 인증 비활성화(MMC 기반)
2단계 인증에서 계정 제외(웹 콘솔)
2단계 인증에서 계정 제외(MMC 기반)
보안 코드 발행자 이름 편집(웹 콘솔)
보안 코드 발행자 이름 편집(MMC 기반)
본인 계정의 2단계 인증 구성(웹 콘솔)
본인 계정의 2단계 인증 구성(MMC 기반)
새 비밀 키 생성
신규 사용자가 스스로 2단계 인증을 설정하지 못하도록 금지
네트워크 에이전트 설치 후 사용자를 Linux 기기 소유자로 할당
사용자 또는 보안 그룹 삭제
사용자 계정의 암호 변경
사용자 역할 생성
사용자 역할 편집
사용자 역할의 범위 편집
사용자 역할 삭제
정책 프로필과 역할 연결
보조 중앙 관리 서버에 사용자 역할 전파
계정 암호 변경
로컬 관리자 권한 취소
개체 리비전 관리
개체를 이전 리비전으로 롤백
리비전 설명 추가
정책 리비전 보기 및 저장
개체 삭제
Kaspersky Security Network(KSN)
KSN 정보
KSN에 대한 액세스 설정
KSN 사용 활성화 및 비활성화
수락한 KSN 성명서 보기
업데이트된 KSN 성명서 수락
배포 지점이 KSN 프록시 서버로 작동하는지 확인
시나리오: Kaspersky Security Center 및 관리 중인 보안 제품 업그레이드
Kaspersky 데이터베이스 및 애플리케이션 업데이트
시나리오: Kaspersky 데이터베이스 및 애플리케이션의 정기적 업데이트
Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 업데이트 정보
중앙 관리 서버 저장소에 업데이트 다운로드 작업 생성
다운로드한 업데이트 검증
배포 지점의 저장소로 업데이트 다운로드 작업 생성
Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성/비활성
Kaspersky Endpoint Security for Windows 업데이트 자동 설치
소프트웨어 업데이트 승인 및 거부
중앙 관리 서버 업데이트
업데이트 다운로드 오프라인 모델 활성 및 비활성
오프라인 기기에서 Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트

웹 플러그인 백업 및 복원
배포 지점 및 연결 게이트웨이 조정
배포 지점의 표준 구성: 단일 사무소
배포 지점의 표준 구성: 다수의 소규모 원격 사무소
배포 지점 할당 정보
배포 지점 자동 할당
배포 지점 수동 할당
관리 그룹의 배포 지점 목록 수정
강제 동기화
푸시 서버 활성화
클라이언트 기기에서 타사 애플리케이션 관리
타사 소프트웨어 업데이트 설치
시나리오: 타사 소프트웨어 업데이트
타사 소프트웨어 업데이트 설치
취약점 및 필요한 업데이트 검색 작업 만들기
취약점 및 필요한 업데이트 검색 작업 설정
필수 업데이트 설치 및 취약점 수정 작업 만들기
업데이트 설치에 대한 규칙 추가
Windows Update 업데이트 설치 작업 만들기
사용 가능한 타사 소프트웨어 업데이트에 대한 정보 보기
사용 가능한 소프트웨어 업데이트 목록을 파일로 내보내기
타사 소프트웨어 업데이트 승인 및 거부
Windows 업데이트 동기화 수행 작업 만들기
타사 애플리케이션 자동 업데이트
타사 소프트웨어 취약점 수정
시나리오: 타사 소프트웨어 취약점 찾기 및 수정
소프트웨어 취약점 찾기 및 수정 정보
타사 소프트웨어 취약점 수정
취약점 수정 작업 생성
필수 업데이트 설치 및 취약점 수정 작업 만들기
업데이트 설치에 대한 규칙 추가
타사 소프트웨어의 취약점에 사용자 수정 선택
관리 중인 모든 기기에서 감지된 소프트웨어 취약점에 대한 정보 보기
선택된 관리 중인 기기에서 감지된 소프트웨어 취약점에 대한 정보 보기
관리 중인 기기의 취약점 통계 보기
소프트웨어 취약점 목록을 텍스트 파일로 내보내기
소프트웨어 취약점 무시
클라이언트 기기에서 실행되는 애플리케이션 관리
애플리케이션 제어로 실행 파일 관리
애플리케이션 제어 모드 및 카테고리
클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기
컨텐츠가 수동으로 추가된 애플리케이션 카테고리 만들기
선택한 기기의 실행 파일을 포함하는 애플리케이션 카테고리 만들기
선택한 폴더의 실행 파일을 포함하는 애플리케이션 카테고리 만들기
애플리케이션 카테고리 목록 보기

애플리케이션 카테고리에 이벤트 관련 실행 파일 추가
Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성
클라이언트 기기에 설치된 애플리케이션 목록 가져오기 및 보기
Kaspersky 데이터베이스의 타사 애플리케이션 설치 패키지 만들기
Kaspersky 데이터베이스에서 타사 애플리케이션의 설치 패키지 설정 보기 및 수정
Kaspersky 데이터베이스의 타사 애플리케이션 설치 패키지 설정
애플리케이션 태그
애플리케이션 태그 생성
애플리케이션 태그 이름 변경
애플리케이션에 태그 할당
애플리케이션에서 할당된 태그 제거
애플리케이션 태그 삭제
모니터링 및 보고
시나리오: 모니터링 및 보고
모니터링 및 리포팅 유형 정보
대시보드 및 위젯
대시보드 사용
대시보드에 위젯 추가
대시보드에서 위젯 숨기기
대시보드에서 위젯 이동
위젯 크기 또는 모양 변경
위젯 설정 변경
대시보드 전용 모드 정보
대시보드 전용 모드 구성
관리 및 보호 리포트
리포트 사용
리포트 템플릿 만들기
리포트 템플릿 속성 보기 및 편집
리포트를 파일로 내보내기
리포트 만들기 및 보기
리포트 전달 작업 만들기
리포트 템플릿 삭제
이벤트 및 이벤트 선택
Kaspersky Security Center 이벤트 정보
이벤트 조회 사용
이벤트 조회 만들기
이벤트 조회 편집
이벤트 조회 목록 보기
이벤트 조회 내보내기
이벤트 조회 가져오기
이벤트 세부 정보 보기
이벤트를 파일로 내보내기
이벤트에서 개체 내역 보기
이벤트 삭제
이벤트 조회 삭제
이벤트의 저장 기간 설정

Kaspersky Security Center 구성 요소의 이벤트
이벤트 유형 데이터 구조 설명
중앙 관리 서버 이벤트
중앙 관리 서버 심각 이벤트
중앙 관리 서버 기능 실패 이벤트
중앙 관리 서버 경고 이벤트
중앙 관리 서버 정보 이벤트
네트워크 에이전트 이벤트
네트워크 에이전트 기능 실패 이벤트
네트워크 에이전트 경고 이벤트
네트워크 에이전트 정보 이벤트
iOS MDM 서버 이벤트
iOS MDM 서버 기능 실패 이벤트
iOS MDM 서버 경고 이벤트
iOS MDM 서버 정보 이벤트
자주 등록된 이벤트 차단 중
자주 등록된 이벤트 차단 정보
자주 등록된 이벤트 차단 관리
자주 등록된 이벤트 차단 제거
Kaspersky Security for Microsoft Exchange Servers에서 이벤트 수신
알림 및 기기 상태
알림 사용
화면 알림 보기
기기 상태 정보
기기 상태 전환 구성
알림 전달 구성
실행 파일을 실행하면 표시되는 이벤트 알림
Kaspersky 공지
Kaspersky 관련 공지
Kaspersky 공지 설정 지정
Kaspersky 공지 비활성화
위협 탐지에 대한 정보 보기
Cloud Discovery
위젯으로 Cloud Discovery 활성화
대시보드에 Cloud Discovery 위젯 추가
클라우드 서비스 사용에 대한 정보 보기
클라우드 서비스의 위험도
원치 않는 클라우드 서비스에 대한 접근 차단
Kaspersky Security Center 웹 콘솔 활동 로깅
Kaspersky Security Center와 기타 솔루션 간의 통합
백그라운드 연결 설정
SIEM 시스템으로 이벤트 내보내기
SIEM 시스템으로 이벤트 내보내기 구성
시작하기 전에
Kaspersky Security Center의 이벤트 정보
이벤트 내보내기 정보
SIEM 시스템에서 이벤트 내보내기 구성 정보

Syslog 형식으로 SIEM 시스템으로 내보내기 위한 이벤트 표시
Syslog 형식으로 SIEM 시스템으로 내보내기 위한 이벤트 표시 정보
Syslog 형식으로 내보내기 위한 Kaspersky 애플리케이션의 이벤트 표시
Syslog 형식으로 내보낼 일반 이벤트 표시
CEF 및 LEEF 형식을 사용하여 이벤트 내보내기 정보
이벤트를 CEF 또는 LEEF 형식으로 변환
Syslog 형식을 사용한 이벤트 내보내기 정보
SIEM 시스템으로 이벤트를 내보내기 위한 Kaspersky Security Center 구성
데이터베이스에서 직접 이벤트 내보내기
klsql2 유틸리티를 사용하여 SQL 쿼리 생성
klsql2 유틸리티의 SQL 쿼리 예제
Kaspersky Security Center 데이터베이스 이름 확인
내보내기 결과 보기
클라우드 환경에서 Kaspersky Security Center 웹 콘솔 작동하기
Kaspersky Security Center 웹 콘솔의 클라우드 환경 구성
1단계. 필요한 플러그인 및 설치 패키지 확인
2단계. 애플리케이션 라이센싱
3단계. 클라우드 환경 및 권한 선택
4단계. 세그먼트 폴링, 클라우드와의 동기화 구성 및 추가 작업 선택
5단계. 정책 및 작업을 생성할 애플리케이션 선택
6단계. Kaspersky Security Center용 Kaspersky Security Network 구성
7단계. 초기 보호 구성 생성
Kaspersky Security Center 웹 콘솔을 통한 네트워크 세그먼트 검색
클라우드 세그먼트 검색에 대한 연결 추가
클라우드 세그먼트 검색에 대한 연결 삭제
Kaspersky Security Center 웹 콘솔을 통한 검색 스케줄 구성
Kaspersky Security Center 웹 콘솔을 통한 클라우드 세그먼트 검색 결과 보기
Kaspersky Security Center 웹 콘솔을 통한 클라우드 기기 속성 보기
클라우드와 동기화: 이동 규칙 구성
Azure 가상 컴퓨터에 애플리케이션 원격 설치
클라우드 DBMS를 사용하여 중앙 관리 서버 데이터 작업의 백업 생성
클라이언트 기기 원격 진단
원격 진단 창 열기
애플리케이션에 대한 추적 로그 활성화 및 비활성화
애플리케이션 추적 로그 파일 다운로드
추적 로그 파일 삭제
애플리케이션 설정 다운로드
이벤트 로그 다운로드
애플리케이션 시작, 중지, 다시 시작
Kaspersky Security Center 네트워크 에이전트의 원격 진단 실행 및 결과 다운로드
클라이언트 기기에서 애플리케이션 실행
애플리케이션에 대한 덤프 파일 생성
Linux 기반 클라이언트 기기에서 원격 진단 실행
격리 및 백업 저장소에서 파일 다운로드 및 삭제
격리 및 백업 저장소에서 파일 다운로드
Kaspersky Security Center 웹 콘솔 인터페이스의 언어 변경
API 참조 가이드

서비스 공급업체를 위한 모범 사례
Kaspersky Security Center 배포 계획
중앙 관리 서버에 대한 인터넷 접속 제공
Kaspersky Security Center 표준 구성
배포 지점 정보
중앙 관리 서버 계층 구조
가상 중앙 관리 서버
Kaspersky Endpoint Security for Android를 사용하여 모바일 기기 관리
배포 및 초기 설정
중앙 관리 서버 설치 권장 사항
Failover 클러스터에 중앙 관리 서버 서비스용 계정 생성
DBMS 선택
중앙 관리 서버 주소 지정
클라이언트 조직의 네트워크에 보호 구성
Kaspersky Endpoint Security 정책 수동 설정
지능형 위협 보호 섹션의 정책 구성
필수 위협 보호 섹션의 정책 구성
일반 설정 섹션의 정책 구성
이벤트 구성 섹션의 정책 구성
Kaspersky Endpoint Security용 그룹 업데이트 작업 수동 설정
Kaspersky Endpoint Security가 설치된 기기 검사를 위한 그룹 작업 수동 설정
취약점 및 필요한 업데이트 검색 작업 스케줄 지정
업데이트 설치 및 취약점 수정을 위한 그룹 작업 수동 설정
관리 그룹 구조 작성 및 배포 지점 할당
표준 MSP 클라이언트 구성: 단일 사무소
표준 MSP 클라이언트 구성: 다수의 소규모 원격 사무소
정책 프로필을 사용하는 정책 계층 구조
정책 계층 구조
정책 프로필
작업
기기 이동 규칙
소프트웨어 분류
멀티테넌트 애플리케이션 정보
중앙 관리 서버 설정 백업 및 복원
중앙 관리 서버가 설치된 기기가 작동하지 않음
데이터베이스 또는 중앙 관리 서버의 설정이 손상됨
네트워크 에이전트 및 보안 제품 배포
초기 배포
설치 관리자 구성
설치 패키지
MSI 속성 및 변환 파일
애플리케이션 원격 설치용 타사 도구를 사용한 배포
Kaspersky Security Center의 원격 설치 작업에 대한 일반 정보
Microsoft Windows의 그룹 정책을 사용하는 배포
Kaspersky Security Center의 원격 설치 작업을 통한 강제 배포
Kaspersky Security Center에서 만든 독립 실행형 패키지 실행
애플리케이션 수동 설치용 옵션

네트워크 에이전트가 설치된 기기에 애플리케이션 원격 설치
원격 설치 작업에서 기기 다시 시작 관리
안티 바이러스 애플리케이션의 설치 패키지에서 데이터베이스를 업데이트하는 작업의 적합성
호환되지 않는 타사 보안 애플리케이션 제거
명령 프롬프트를 사용하여 암호로 보호된 네트워크 에이전트 제거
Kaspersky Security Center의 애플리케이션 원격 설치 도구를 사용하여 관리 중인 기기에서 관련 실행 파일 실행
배포 모니터링
설치 관리자 구성
일반 정보
숨김 모드로 설치 (응답 파일 사용)
숨김 모드로 네트워크 에이전트 설치(응답 파일 사용 안 함)
setup.exe를 통한 부분 설치 구성
중앙 관리 서버 설치 파라미터
네트워크 에이전트 설치 설정
가상 인프라
가상 컴퓨터 부하를 줄이기 위한 팁
동적 가상 컴퓨터 지원
가상 컴퓨터 복사 지원
네트워크 에이전트가 설치된 기기의 파일 시스템 롤백 지원
이동 사용자를 위한 연결 프로필 정보
모바일 기기 관리 기능 배포
KES 기기를 중앙 관리 서버에 연결
중앙 관리 서버에 기기 직접 연결
Kerberos 제한 위임(KCD)을 사용하는 서버에 KES 기기를 연결하기 위한 구성
Firebase Cloud Messaging 사용
공개 키 인프라와의 통합
Kaspersky Security Center 웹 서버
기타 정기 작업
관리 콘솔에서 표시등 및 기록된 이벤트 모니터링
관리 중인 기기에 원격 접근
"중앙 관리 서버와 계속 연결 유지" 옵션을 사용하여 관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결 제공
기기와 중앙 관리 서버 간 연결 시간 확인 정보
강제 동기화 정보
터널링 정보
사이징 가이드
이 설명서 정보
Kaspersky Security Center의 제한 사항에 대한 정보
중앙 관리 서버에 대한 계산
중앙 관리 서버에 대한 하드웨어 리소스 계산
DBMS 및 중앙 관리 서버의 하드웨어 요구 사항
데이터베이스 공간 계산
디스크 공간 계산(취약점 및 패치 관리 기능 사용 유무)
중앙 관리 서버의 수 및 구성 계산
동적 가상 컴퓨터를 Kaspersky Security Center에 연결하기 위한 권장 사항

- 배포 지점 및 연결 게이트웨이에 대한 계산
  - 배포 지점의 요구 사항
  - 배포 지점의 개수 및 구성 계산
  - 연결 게이트웨이 수 계산
- 작업 및 정책에 대한 이벤트 정보 로깅
- 어떤 작업의 특정한 고려 사항 및 최적 설정
  - 기기 발견 빈도
  - 중앙 관리 서버 데이터 백업 작업 및 중앙 관리 서버 점검 작업
  - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업
  - 인벤토리 작업
- 중앙 관리 서버 및 보호 제품이 설치된 기기 간의 네트워크 부하 분산에 대한 세부 정보
  - 다양한 시나리오에서의 트래픽 사용량
  - 24시간 기준 평균 트래픽 사용

기술 지원 연락처
- 기술 지원을 받는 방법
- Kaspersky CompanyAccount를 통해 기술 지원 받기
- 중앙 관리 서버의 덤프 파일 받기

애플리케이션에 대한 정보 출처

용어집
- Amazon EC2 인스턴스
- AMI(Amazon 머신 이미지)
- AWS IAM 액세스 키
- AWS Management Console
- AWS 애플리케이션 프로그램 인터페이스(AWS API)
- Cloud Discovery
- DMZ(완충 지역)
- HTTPS
- IAM 사용자
- IAM 역할
- IAM(ID 및 접근 관리)
- iOS MDM 기기
- iOS MDM 서버
- iOS MDM 프로필
- JavaScript
- Kaspersky Private Security Network (KPSN)
- Kaspersky Security Center SHV(System Health Validator)
- Kaspersky Security Center 관리자
- Kaspersky Security Center 업그레이드
- Kaspersky Security Center 운영자
- Kaspersky Security Center 웹 서버
- Kaspersky Security Network(KSN)
- Kaspersky 업데이트 서버
- KES 기기
- Lightweight Nagent(LWNGT)
- MITM 공격
- SSL
- UEFI 보호 기기

Windows 서버 업데이트 서비스(WSUS)
가상 중앙 관리 서버
강제 설치
강화 가이드
공유 인증서
관리 그룹
관리 중인 기기
관리 콘솔
관리 플러그인
관리자 권한
관리자 워크스테이션
구성 프로필
그룹 작업
기기 소유자
내부 사용자 계정
네트워크 보호 상태
네트워크 안티 바이러스 보호
네트워크 에이전트
네트워크 위치 인식(NLA)
라이센스 기간
로컬 설치
로컬 작업
모바일 기기 서버
바이러스 급증 기준 임계값
배포 지점
백업 폴더
보호 상태
복원
브로드캐스트 도메인
비-호환 애플리케이션
사용 가능한 업데이트
서비스 공급업체 관리자
설치 패키지
수동 설치
악성 코드 급증
안티 바이러스 데이터베이스
안티 바이러스 보호 서비스 공급업체
애플리케이션 직접 관리
앱 마켓
업데이트
연결 게이트웨이
원격 설치
유료 애플리케이션 그룹
이벤트 심각도
이벤트 저장소
인증 에이전트
작업

- 작업 설정
- 정책
- 중앙 관리 서버
- 중앙 관리 서버 데이터 백업
- 중앙 관리 서버 데이터 복원
- 중앙 관리 서버 인증서
- 중앙 관리 서버 클라이언트(클라이언트 기기)
- 중앙 집중식 애플리케이션 관리
- 추가(또는 예비) 라이센스 키
- 취약점
- 클라우드 환경
- 클라이언트 관리자
- 키 파일
- 특정 기기 작업
- 패치 심각도
- 프로그램 설정
- 프로비저닝 프로필
- 홈 중앙 관리 서버
- 활성 라이센스 키

타사 코드 정보

상표 고지

알려진 문제

Kaspersky Security Center 15.1 도움말

	**새로운 기능** 최신 출시 애플리케이션의 새로운 기능에 대해 알아봅니다.		**네트워크 보호 구성** 조직의 보안을 관리합니다.
	**하드웨어 및 소프트웨어 요구 사항** 지원되는 운영 체제와 애플리케이션 버전을 확인합니다.		**Kaspersky 애플리케이션, 데이터베이스 및 소프트웨어 모듈 업데이트** 보호 시스템의 신뢰성을 유지합니다.
	**배포 및 초기 설정** 리소스 사용을 계획하고, 중앙 관리 서버를 설치하고, 클라이언트 기기에 네트워크 에이전트와 보안 제품을 설치하고, 관리 그룹에 기기를 통합합니다.		**모니터링 및 보고** 인프라, 보호 상태 및 통계를 확인합니다. Cloud Discovery를 사용하여 클라우드 서비스 접근을 관리합니다.
	**네트워크에 연결된 기기 발견** 조직 네트워크의 기존 기기와 새 기기를 발견합니다.		**타사 보안 제품 교체** 비-호환 애플리케이션을 제거하는 방법에 대해 알아봅니다.
	**Kaspersky 애플리케이션, 중앙 집중식 배포** Kaspersky 애플리케이션 배포.		**배포 지점 및 연결 게이트웨이 조정** 배포 지점을 구성합니다.
	**이전 버전에서 Kaspersky Security Center 업그레이드** 이전 버전에서 Kaspersky Security Center 15.1로 업그레이드합니다.		**서비스 공급업체를 위한 모범 사례(온라인 도움말에만 해당)** 애플리케이션을 배포, 구성 및 사용하는 방법에 대한 권장 사항을 제공하며 애플리케이션 작동 시에 일반적으로 발생하는 문제를 해결하는 방법을 설명합니다.
	**Kaspersky 애플리케이션, 라이센스 및 활성화** 몇 가지 단계를 수행하여 Kaspersky 애플리케이션을 활성화합니다.		**사이징 가이드(온라인 도움말만 해당)** 다양한 운영 조건에서 최적의 성능을 유지하기 위해 네트워크에 있는 기기 수, 네트워크 토폴로지 및 필요한 Kaspersky Security Center 기능을 고려하십시오.
	**SIEM 시스템으로 이벤트 내보내기** 분석을 위해 SIEM 시스템에 대한 이벤트 내보내기를 구성합니다.		**취약점 및 패치 관리** 타사 소프트웨어의 취약점을 찾고 수정합니다.
	**클라우드 환경에서 작업** 클라우드 환경(Amazon Web Services™, Microsoft Azure™, Google™ 클라우드 플랫폼)에서 Kaspersky Security Center를 배포합니다.		**자주 하는 질문 (영어로만 제공)** 일반적인 문제 해결 방법에 대한 지침을 확인할 수 있습니다.
	**Kaspersky Endpoint Security for Business 빠른 시작 가이드** Kaspersky Endpoint Security for Business 시작하기: 이 솔루션을 설치하고 구성합니다. 또한 Kaspersky Security Center의 기능 비교를 검토하여 가장 적절한 네트워크 보안 관리 방법을 선택할 수 있습니다.		

새로운 기능

Kaspersky Security Center 15.1 업데이트 2

Kaspersky Security Center 15.1 업데이트 2는 사용자와 테스트 팀이 보고한 문제의 수정에 중점을 둡니다.

- 이제 TXT 파일을 가져와 지정한 Linux 기반 관리 중인 기기의 범위에서 작업이 올바르게 실행됩니다.
- 이제 가상 중앙 관리 서버에서 생성한 원격 설치 작업을 사용하여 Kaspersky 애플리케이션을 설치하면 운영 체제 도구를 사용하여 해당 가상 중앙 관리 서버에서 관리하는 배포 지점을 통해서만 설치 패키지가 관리 중인 기기로 전송됩니다.
- 보조 서버의 인증서를 교체한 후 보조 중앙 관리 서버가 기본 중앙 관리 서버에 다시 연결하지 못하는 문제를 해결했습니다.
- TLS 연결에 영향을 미치는 문제를 해결했습니다.
- 사용자 로그인 중에 '잘못된 유형 변환' 오류가 여러 번 발생하는 문제가 해결되었습니다.
- 이제 Kaspersky Security Center 이메일로 이벤트 알림을 올바르게 전송합니다.
- 버전 14.2에서 15.1로 Kaspersky Security Center를 업데이트할 때 백업 복사본에 *업데이트* 폴더를 추가하여 문제를 해결했습니다.
- 이제 Kaspersky Security Center 웹 콘솔에 Kaspersky 애플리케이션 라이센스의 만료 날짜가 올바르게 표시됩니다.
- 이제 **모바일 기기 위치 확인** 및 **기기 위치 내역 가져오기** 명령이 올바르게 작동합니다.
- 모바일 인증서가 포함된 설치 패키지가 다운로드 1시간 후 또는 사용하지 않은 상태로 남아 있는 경우 24시간 후에 자동으로 삭제되지 않는 문제를 수정했습니다.
- 이제 특정 태그로 활성화된 정책 프로필이 설명에 해당 태그가 포함된 기기에 올바르게 적용됩니다.
- PostgreSQL 데이터베이스 오류 메시지가 이벤트 로그에 나타나는 문제가 수정되었습니다.
- 이제 2단계 인증에서 계정 제외가 올바르게 작동합니다.
- 신원 및 액세스 관리자를 활성화한 상태에서 도메인 인증을 사용할 때 Kaspersky Security Center 웹 콘솔에서 로그아웃하면 제대로 로그아웃되지 않는 문제가 수정되었습니다.
- 이제 관리 웹 플러그인을 업데이트할 때 필요한 플러그인 버전의 링크를 클릭하면 다운로드가 시작됩니다.
- 리포트에서 수정된 문제:
  - 위협 처리 및 업데이트 리포트에 대한 전달 작업을 생성하고 작업 스케줄을 **월별**로 설정하면 리포트에 데이터가 올바르게 채워집니다.
  - *애플리케이션 구성 요소 상태 리포트* 템플릿에서 구성 요소 이름으로 필터링이 올바르게 적용됩니다.
  - 이제 Kaspersky 애플리케이션이 설치되지 않은 기기만 표시하도록 *보호 배포 리포트*를 필터링할 수 있습니다. 이렇게 하면 애플리케이션을 설치할 기기의 수를 시각화하는 데 도움이 됩니다.

- **일반 기능: 기본 기능** 영역에서 **실행** 권한이 있는지 여부에 관계 없이 **Cloud Discovery** 위젯이 올바르게 표시됩니다.
- 저장 프로시저 및 데이터베이스 작업의 성능이 개선되었습니다.
- 존재하지 않는 사용자에게 연결된 만료된 인증서로 인해 모든 사용자의 갱신 프로세스가 중지되는 문제가 수정되었습니다.
- 적절한 인증서 처리에 영향을 미치는 문제가 해결되었습니다.
- 버전 14.2에서 15.1로 Kaspersky Security Center를 업그레이드한 후, 이제 관리 콘솔의 보조 가상 중앙 관리 서버에서 독립 실행형 설치 패키지 다운로드가 제대로 작동합니다.
- Kaspersky Security Center 웹 콘솔의 Kaspersky 애플리케이션 정책에서 Kaspersky Security Network(KSN) 사용을 활성화할 경우 다음 애플리케이션에 대해 KSN 선언문을 수락할 수 없는 문제가 해결되었습니다. Kaspersky Endpoint Security for Linux 버전 12.2 이하, Kaspersky Industrial CyberSecurity for Linux Nodes 버전 1.5 이하, Kaspersky Security for Virtualization Light Agent 버전 6.0 및 6.1, Kaspersky Embedded Systems Security for Linux 버전 3.3, Kaspersky Security for Windows Server 버전 11.0.1.897.
- Active Directory 도메인 그룹에 포함된 Linux 기반 기기에 정책 프로필이 적용되지 않는 문제가 수정되었습니다.
- 몇몇 2차 레벨 보조 중앙 관리 서버에서 기본 중앙 관리 서버로 연결을 시도하는 도중 발생하는 문제가 수정되었습니다.

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1에는 여러 새 기능과 개선 사항이 포함되어 있습니다.

- Cloud Discovery. Windows를 실행하는 관리 중인 기기에서 클라우드 서비스 사용 시도를 모니터링하고, 원치 않는 클라우드 서비스에 대한 접근을 차단할 수 있는 새로운 기능입니다. 이 기능은 Kaspersky Security Center 웹 콘솔 버전에서만 사용할 수 있습니다.
- 이제 도메인 컨트롤러 검색으로 Linux 기반 배포 지점을 통해 Samba 도메인 컨트롤러를 검색할 수 있습니다. 큰 도메인의 검색을 지원하도록 개선하였습니다.
- Linux 기반의 관리 중인 기기에서 원격 진단을 향상했습니다.
- macOS 기기의 확장 하드웨어 인벤토리. macOS 기기의 네트워크 에이전트는 MAC 주소 및 기기 일련번호를 중앙 관리 서버로 전송합니다.
- 이제 SIEM 시스템에 대한 연결을 확인할 수 있습니다.
- 내부 사용자의 최대 암호 길이가 256자로 증가했습니다.
- 이제 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux로 마이그레이션할 때 백업 복사본에서 중앙 관리 서버의 인증서 및 개인 키를 복원하여, Kaspersky Security Center Linux에서 관리하도록 관리 중인 기기를 전환할 수 있습니다.
- 클리너 도구나 klmover 유틸리티를 실행하여 암호가 걸려 있는 네트워크 에이전트를 제거할 때, 제거 암호를 입력하라는 메시지가 표시됩니다.
- 이제 Kaspersky Endpoint Security for Windows에서 Kaspersky Security for Windows Server로 업그레이드할 때 대상 기기를 다시 시작할 필요가 없습니다.

- Linux 기반 클라이언트 기기에 네트워크 에이전트를 설치하는 동안이나 설치한 후에 사용자를 기기 소유자로 할당할 수 있습니다.
- 이제 사용자 지정 스크립트로 관리 중인 기기에 소프트웨어 설치 시 원격 설치 관련 리포트를 수신할 수 있습니다.
- 관리 중인 기기에서 여러 사용자 지정 스크립트를 실행할 때 각 스크립트의 우선순위를 설정하여 실행 순서를 정의할 수 있습니다. 스크립트는 우선순위가 가장 높은 스크립트부터 가장 낮은 순으로 실행됩니다.
- 확장 정책 감사. 이제 정책 개정의 내용을 확인하고 정책 개정을 파일에 저장할 수 있습니다. 현재 이러한 기능은 중앙 관리 서버 정책 및 네트워크 에이전트 정책에서만 사용할 수 있습니다.
- 다음과 같은 사용자 경험을 개선했습니다.
  - **고정됨** 섹션에서 빠르게 접근할 수 있도록 Kaspersky Security Center 웹 콘솔의 섹션을 고정하여 메인 메뉴를 개인화하였습니다.
  - 표 작업을 최적화했습니다. 이제 각 표의 기본 보기에 가장 자주 사용되는 열이 포함됩니다. 또한 이제 현재 페이지 또는 전체 표에서 모든 항목을 선택하거나 전체 표에서 항목을 정렬할 수 있습니다.
  - 리포트 전달 구성이 개선되었습니다. 이제 리포트를 보낼 이메일 주소와 리포트 전달 스케줄을 최대 20개까지 지정할 수 있습니다.
- Linux 기반 관리 중인 기기의 계정에서 로컬 관리자 권한을 취소할 수 있습니다. 이를 통해 사용자 계정 보호를 한 단계 더 추가할 수 있습니다. 예를 들어 일회성 할당이 완료된 로컬 관리자 권한을 철회할 수 있습니다.
- 예를 들어 사용자가 로컬 계정 암호를 잊어버렸거나 스케줄에 따라 암호를 변경할 때, Linux 기반 관리 중인 기기에서 로컬 계정 암호를 변경할 수 있습니다.
- **사용자 인증서 관리** 하위 섹션에서 설치할 루트 인증서를 지정할 수 있습니다. 이러한 인증서는 웹사이트나 웹 서버 인증 확인 등의 작업에 사용할 수 있습니다.
- 이제 네트워크 공격 리포트에 공격 기기의 MAC 주소와 포트가 포함됩니다.
- 내부 사용자가 다음번에 Kaspersky Security Center 웹 콘솔에 로그인할 때 암호 변경을 강제하는 새로운 옵션이 추가되었습니다.
- 이제 이벤트를 CEF 또는 LEEF 형식으로 SIEM 시스템에 내보낼 때 상업용 라이센스를 확인하지 않습니다.
- Kaspersky 애플리케이션에서 다른 애플리케이션으로 마이그레이션할 때 현재 사용하는 애플리케이션이 암호로 보호 중이라면, 이제 원격 설치 작업에서 제거 암호를 지정할 수 있습니다.
- 이제 Exchange ActiveSync는 지원하지 않습니다.

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2에는 여러 새 기능과 개선 사항이 포함되어 있습니다.

- 새로운 강화 가이드가 출시되었습니다. 가이드를 주의 깊게 읽고 보안 권장 사항에 따라 Kaspersky Security Center 및 네트워크 인프라를 구성할 것을 권장합니다.

  또한 Kaspersky Security Center에 대한 최신 업데이트를 설치하십시오. 이 업데이트에는 사용자 계정의 2단계 인증 및 기타 개선 사항과 같은 인프라 보호 기능을 포함합니다.

- 이제 Kaspersky 서버에 대한 액세스가 자동 확인됩니다. 시스템 DNS를 사용하여 서버에 액세스할 수 없을 시, 애플리케이션이 공용 DNS를 사용합니다.
- 가상 중앙 관리 서버에 대한 사용자 권한은 기본 중앙 관리 서버와 별도로 언제든지 구성할 수 있습니다. 또한 기본 서버 사용자에게 가상 서버를 관리할 수 있는 권한을 할당할 수 있습니다.
- Kaspersky Security Center는 이제 다음 DBMS 작업을 지원합니다:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x(모든 버전)
  - Postgres Pro 14.x(모든 버전)
  - MariaDB 10.1, 10.4, 10.5
- Kaspersky Security Center 웹 콘솔을 사용하여 정책 및 작업을 파일로 내보낸 다음 정책 및 작업을 Kaspersky Security Center Windows 또는 Kaspersky Security Center Linux로 가져올 수 있습니다.
- 다음 작업에서 **프록시 서버 사용 안 함** 옵션이 제거되었습니다:
  - *중앙 관리 서버 저장소에 업데이트 다운로드*
  - *배포 지점의 저장소로 업데이트 다운로드*
- 클라우드 환경에서 클라이언트 기기 보호를 위해 Kaspersky Security for Windows Server 대신 Kaspersky Endpoint Security for Windows를 배포할 수 있습니다. 이 기능은 Kaspersky Endpoint Security 12.0 for Windows 릴리스 후에 사용할 수 있습니다.
- 이제 암호화 키 작업은 **일반 기능**: **암호화 키 관리** 기능 영역에 대한 액세스 권한으로 제한됩니다. Kaspersky Security Center 사용자는 이제 **읽기** 권한이 있을 시 암호화 키를 내보낼 수 있고 **쓰기** 권한이 있을 시 암호화 키를 가져올 수 있습니다.

Kaspersky Security Center 14

Kaspersky Security Center 14에는 여러 새 기능과 개선 사항이 포함되어 있습니다.

- 격리된 네트워크에서 타사 소프트웨어(Microsoft 소프트웨어)의 업데이트를 설치하고 취약점을 수정할 수 있습니다. 이러한 네트워크에는 인터넷 액세스가 없는 및 관리 중인 기기 및 중앙 관리 서버가 포함됩니다. 이러한 종류의 네트워크에서 취약점을 수정하려면 인터넷 액세스가 가능한 중앙 관리 서버를 사용하여 필수 업데이트를 다운로드한 다음, 격리된 중앙 관리 서버로 패치를 전송해야 합니다.
- macOS 기기에 이동 사용자를 위한 연결 프로필이 추가되었습니다. 연결 프로필을 사용하여 기기 위치에 따라 같거나 다른 중앙 관리 서버에 연결하도록 macOS 기기의 네트워크 에이전트 규칙을 구성할 수 있습니다.
- 이제 Microsoft Windows 10 IoT Enterprise를 실행하는 기기에 네트워크 에이전트를 설치할 수 있습니다.
- 이제 **위협 처리 리포트**에서 위협 목록을 필터링하여 Cloud Sandbox에서 탐지한 위협만 볼 수 있습니다.
- 이제 Kaspersky Security Center에서 관리 중인 애플리케이션으로 Kaspersky Industrial Cybersecurity for Linux Nodes 1.3을 지원합니다.

Kaspersky Security Center 웹 콘솔에는 여러 새 기능과 개선 사항이 있습니다:

- 네트워크를 관리하지 않지만 Kaspersky Security Center에서 네트워크 보호 통계를 보고자 하는 직원(최고 관리자 등)을 위해 대시보드 전용 모드를 구성할 수 있습니다. 사용자가 이 모드를 활성화하면 사전 정의된 위젯 세트가 있는 대시보드만 표시됩니다. 따라서 위젯에 지정된 통계(예: 관리되는 모든 기기의 보호 상태, 최근에 탐지된 위협 수 또는 네트워크에서 가장 빈번한 위협 목록)를 모니터링할 수 있습니다.
- 이제 Kaspersky Security Center 웹 콘솔이 Kaspersky Security for iOS를 보안 애플리케이션으로 지원합니다.
- 작업 속성에서 하위 그룹 및 보조 중앙 관리 서버(가상 서버 포함)에 작업을 적용할지 지정할 수 있습니다.
- 이제 Kaspersky Security Center에서 관리 중인 애플리케이션으로 Kaspersky Industrial Cybersecurity for Linux Nodes 1.3을 지원합니다.

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2에는 여러 새 기능과 개선 사항이 포함되어 있습니다.

- 이제 중앙 관리 서버, 관리 콘솔, Kaspersky Security Center 13.2 웹 콘솔 및 네트워크 에이전트를 다음 새 운영 체제에 설치할 수 있습니다(자세한 내용은 소프트웨어 요구 사항 참조).
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2(2021년 10월 업데이트)
  - Windows Server 2022
- MySQL 8.0을 데이터베이스로 사용할 수 있습니다.
- Kaspersky Security Center 장애 조치 클러스터 에 Kaspersky Security Center를 배포하여 Kaspersky Security Center의 고가용성을 제공할 수 있습니다.
- Kaspersky Security Center는 이제 IPv6 주소 및 IPv4 주소로 작동합니다. 중앙 관리 서버에서 IPv6 주소를 사용하는 기기가 있는 네트워크를 검색할 수 있습니다.

Kaspersky Security Center 13.2 웹 콘솔에는 여러 새 기능과 개선 사항이 포함되어 있습니다.

- 이제 Kaspersky Security Center 13.2 웹 콘솔을 통해 Android를 실행하는 모바일 기기 를 관리할 수 있습니다.
- Kaspersky 마켓플레이스는 새 메뉴 섹션으로 제공됩니다. Kaspersky Security Center 13.2 웹 콘솔을 통해 Kaspersky 애플리케이션을 검색할 수 있습니다.
- Kaspersky Security Center는 이제 다음 Kaspersky 애플리케이션을 지원합니다.
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1에는 여러 새 기능과 개선 사항이 포함되어 있습니다.

- SIEM 시스템과의 통합이 개선되었습니다. 이제 암호화된 채널(TLS)을 통해 SIEM 시스템으로 이벤트 내보내기를 할 수 있습니다. 이 기능은 Kaspersky Security Center 웹 콘솔 및 MMC 기반 관리 콘솔에서 사용할 수 있습니다.
- 이제 중앙 관리 서버용 패치를 배포 패키지로 받을 수 있으며 이후 버전의 업데이트에 사용할 수 있습니다.
- Kaspersky Endpoint Detection and Response Optimum에 대한 새 섹션인 **Alerts**가 Kaspersky Security Center 13.1 웹 콘솔에 추가되었습니다. Kaspersky Endpoint Detection and Response Optimum Optimum에서 탐지한 위협을 처리하기 위해 몇 가지 새로운 위젯도 추가되었습니다.
- Kaspersky Security Center 13.1 웹 콘솔에서 이제 Kaspersky 애플리케이션용 라이센스 만료에 대한 알림을 수신할 수 있습니다.
- Kaspersky Security Center 13.1 웹 콘솔에 대한 응답 시간이 단축되었습니다.

Kaspersky Security Center 13

Kaspersky Security Center 13 웹 콘솔에 다음과 같은 기능이 추가되었습니다.

- 2단계 인증이 구현되었습니다. 2단계 인증을 활성화하여 Kaspersky Security Center 13 웹 콘솔에 대한 무단 액세스 위험을 줄일 수 있습니다.
- NTLM 및 Kerberos 프로토콜(싱글 사인온)을 사용하여 도메인 인증을 구현했습니다. 싱글 사인온 기능을 사용하면 Windows 사용자가 회사 네트워크에 암호를 다시 입력하지 않아도 Kaspersky Security Center 13 웹 콘솔에서 보안 인증을 활성화할 수 있습니다.
- 이제 Kaspersky Managed Detection and Response와 함께 작동하도록 플러그인을 구성할 수 있습니다. 이 통합을 사용하여 인시던트를 보고 워크스테이션을 관리할 수 있습니다.
- 이제 중앙 관리 서버의 설치 마법사에서 Kaspersky Security Center 13 웹 콘솔에 대한 설정을 지정할 수 있습니다.
- 업데이트 및 패치의 새 릴리스에 대한 알림이 표시됩니다. 업데이트는 즉시 또는 나중에 언제든지 설치할 수 있습니다. 이제 Kaspersky Security Center 13 웹 콘솔을 통해 중앙 관리 서버용 패치를 설치할 수 있습니다.
- 표로 작업할 때 이제 열의 순서와 너비를 지정하고 데이터를 정렬하며 페이지 크기를 지정할 수 있습니다.
- 이제 이름을 클릭하여 보고서를 열 수 있습니다.
- Kaspersky Security Center 13 웹 콘솔이 이제 한국어로도 제공됩니다.
- 새로운 섹션인 Kaspersky 공지 사항은 **모니터링 및 보고** 메뉴에서 제공됩니다. 이 섹션에서는 사용 중인 Kaspersky Security Center 버전과 관리 중인 기기에 설치된 관리 애플리케이션에 대한 정보를 계속 제공합니다. Kaspersky Security Center는 오래된 공지를 제거하고 새로운 정보를 추가하여 섹션의 정보를 정기적으로 업데이트합니다. 그러나 원하는 경우 Kaspersky 공지 사항을 비활성화할 수 있습니다.
- 사용자 계정 설정 변경 후 추가 인증이 구현되었습니다. 무단 수정으로부터 사용자 계정을 보호할 수 있습니다. 이 옵션이 활성화된 경우 사용자 계정 설정을 수정하려면 수정 권한이 있는 사용자의 인증이 필요합니다.

Kaspersky Security Center 13에 다음 기능이 추가되었습니다.

- 2단계 인증이 구현되었습니다. 2단계 인증을 활성화하여 관리 콘솔에 대한 무단 액세스 위험을 줄일 수 있습니다. 이 옵션이 활성화된 경우 사용자 계정 설정을 수정하려면 수정 권한이 있는 사용자의 인증이 필요합니다. 이제 KES 기기에 대한 2단계 인증을 활성화하거나 비활성화할 수 있습니다.

- HTTP를 통해 중앙 관리 서버에 메시지를 보낼 수 있습니다. 이제 중앙 관리 서버의 OpenAPI 작업을 위한 참조 가이드와 Python 라이브러리를 사용할 수 있습니다.

- iOS MDM 서버 인증서가 만료된 후 관리되는 iOS 기기를 원활하게 전환될 수 있도록 iOS MDM 프로필에서 사용할 예비 인증서를 발급할 수 있습니다.

- 다중 테넌시 애플리케이션 폴더가 더 이상 관리 콘솔에 표시되지 않습니다.

Kaspersky Security Center 정보

이 섹션은 Kaspersky Security Center의 목적, 주요 기능 및 구성 요소, Kaspersky Security Center 구매 방법에 대한 정보를 포함합니다.

온라인 도움말에 제공된 정보는 애플리케이션과 함께 제공된 문서에 있는 정보와 다를 수 있습니다. 이 경우 온라인 도움말이 최신으로 간주됩니다. 애플리케이션 인터페이스에서 링크를 클릭하거나 문서에서 온라인 도움말 링크를 클릭하여 온라인 도움말로 이동할 수 있습니다. 온라인 도움말은 사전 통지 없이 업데이트될 수 있습니다. 필요한 경우 온라인 도움말과 오프라인 도움말 간을 전환할 수 있습니다.

Kaspersky Security Center는 조직 네트워크의 기본 관리 및 유지 관리 작업의 중앙 집중식 실행을 위해 설계되었습니다. 애플리케이션은 관리자가 조직의 네트워크 보안 수준에 대한 자세한 정보에 접근할 수 있도록 하여 Kaspersky 애플리케이션을 사용해 구축한 모든 보호 구성 요소를 구성할 수 있도록 허용합니다.

Kaspersky Security Center는 다양한 조직에서 기기 보호 업무를 맡은 회사 네트워크 관리자와 직원을 대상으로 개발된 애플리케이션입니다.

Kaspersky Security Center를 사용하면 다음을 수행할 수 있습니다:

- 조직의 네트워크 및 원격 지사나 클라이언트 조직의 네트워크를 관리하기 위해 중앙 관리 서버의 계층 구조 만들기.

  *클라이언트 조직*은 서비스 공급업체가 안티 바이러스 보호를 보장하는 대상 조직입니다.

- 클라이언트 기기를 통합적으로 관리하기 위해 관리 그룹의 계층 구조 만들기.
- Kaspersky 애플리케이션을 바탕으로 구축된 안티 바이러스 보호 시스템 관리.
- 운영 체제의 이미지를 만들어 네트워크에 있는 클라이언트 기기에 배포하고, Kaspersky 및 다른 소프트웨어 공급업체에 의해 애플리케이션의 원격 설치를 수행.
- 클라이언트 기기에 설치된 Kaspersky 및 기타 공급업체의 애플리케이션을 원격으로 관리. 업데이트 설치, 취약점 찾기 및 수정.
- Kaspersky 애플리케이션의 라이센스 키를 클라이언트 기기에 중앙 집중식으로 배포하고 사용을 모니터링하며 라이센스를 갱신.
- 애플리케이션과 기기의 작동에 관한 통계 및 리포트 수신.
- Kaspersky 애플리케이션 작동 중 발생한 심각 이벤트에 대한 알림 수신.
- 모바일 기기 관리.
- 기기의 하드 드라이브와 이동식 드라이브에 저장된 정보의 암호화 및 암호화된 데이터에 대한 사용자의 접근 관리.
- 조직의 네트워크에 연결된 하드웨어의 인벤토리 수행.
- 보안 제품에 의해 격리 저장소나 백업 저장소로 옮겨진 파일과 보안 제품별 처리가 연기된 파일을 중앙에서 관리.

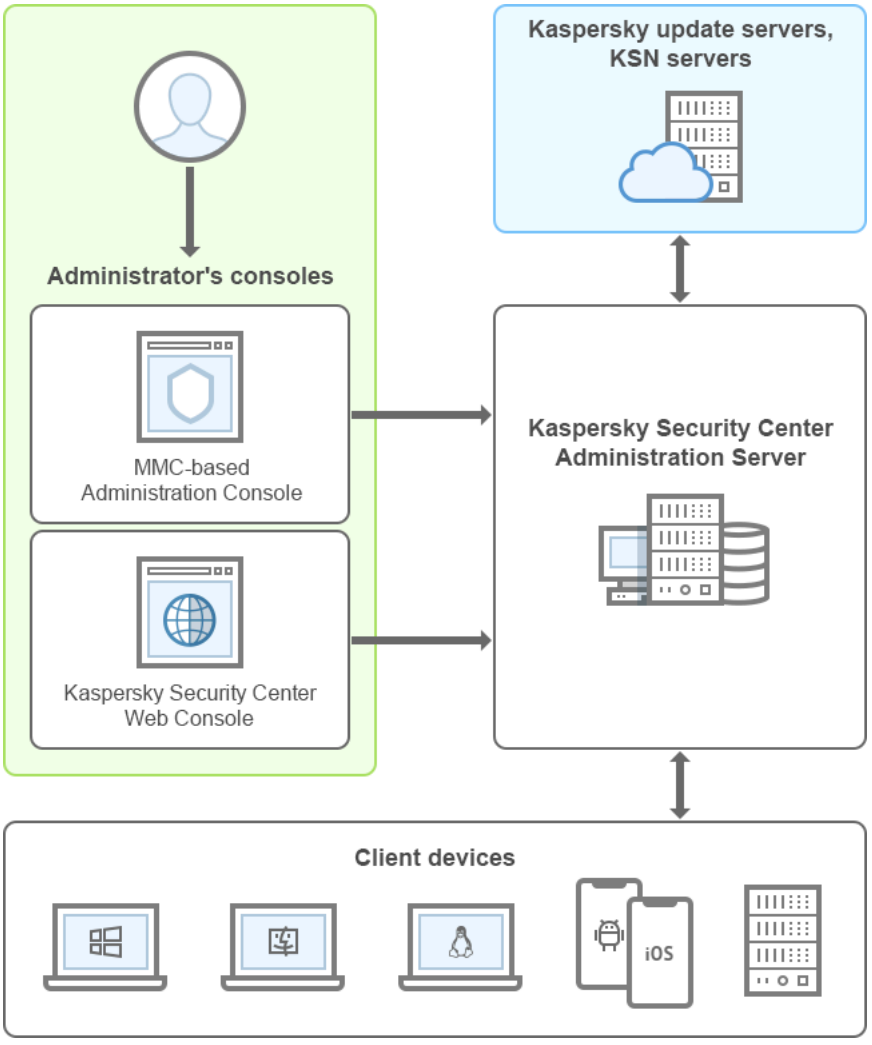
Kaspersky Security Center는 Kaspersky(https://www.kaspersky.com 등)나 파트너 회사를 통해 구매할 수 있습니다.

Kaspersky를 통해 Kaspersky Security Center를 구매했다면 당사 웹사이트에서 애플리케이션을 복사할 수 있습니다. 결제가 처리되고 나면 애플리케이션 활성화에 필요한 정보가 이메일로 전송됩니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)과 KSN 기능이 제공되지 않을 수도 있습니다.

아키텍처

이 섹션에서는 Kaspersky Security Center 구성 요소 및 구성 요소들 사이의 상호 작용에 대해 설명합니다.



Kaspersky Security Center 아키텍처

Kaspersky Security Center는 다음 기본 구성 요소로 구성됩니다:

- *관리 콘솔*(이하 *콘솔*). 중앙 관리 서버 및 네트워크 에이전트의 관리 서비스에 대한 사용자 인터페이스를 제공합니다. 관리 콘솔은 MMC(Microsoft Management Console)의 스냅인으로 구현됩니다. 관리 콘솔에서는 인터넷을 통해 중앙 관리 서버에 원격으로 연결할 수 있습니다.

- *Kaspersky Security Center 웹 콘솔*. Kaspersky Security Center가 관리하는 클라이언트 조직 네트워크의 보호 시스템을 생성하고 모니터링하기 위한 웹 인터페이스를 제공합니다.

- *Kaspersky Security Center 중앙 관리 서버*(이하 *서버*). 조직 네트워크에 설치된 애플리케이션과 해당 애플리케이션 관리에 대한 정보를 중앙 집중식으로 저장합니다.

- *Kaspersky 업데이트 서버*. Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다.
- *KSN 서버*. 포함된 Kaspersky 데이터베이스에 파일, 웹 리소스, 소프트웨어 평판 관련 정보가 지속적으로 업데이트되는 서버입니다. Kaspersky Security Network의 데이터를 사용하면 위협이 발생할 때 Kaspersky 애플리케이션의 처리 속도가 더욱 빨라지며 일부 보호 구성 요소의 성능이 개선되며, 정상적인 개체를 바이러스로 잘못 탐지할 가능성이 줄어듭니다.
- *클라이언트 기기*. Kaspersky Security Center에서 보호하는 고객사의 기기입니다. 보호해야 하는 각 기기에는 Kaspersky 보안 제품 중 하나가 설치되어 있어야 합니다.

하드웨어 및 소프트웨어 요구 사항

- 중앙 관리 서버 요구 사항
- 웹 콘솔 요구 사항
- 모바일 서버 요구 사항
- 관리 콘솔 요구 사항
- 네트워크 에이전트 요구 사항

중앙 관리 서버 요구 사항

최소 하드웨어 요구 사항:

- 처리 속도가 1 GHz 이상인 CPU. 64비트 운영 체제의 경우 최소 CPU 처리 속도는 1.4GHz입니다.
- RAM: 4 GB.
- 사용 가능한 디스크 공간: 10 GB. 취약점 및 패치 관리 사용 시, 최소 100GB 이상의 디스크 여유 공간이 필요합니다.

클라우드 환경에 배포하는 경우 중앙 관리 서버 및 데이터베이스 서버의 요구 사항은 물리적 중앙 관리 서버의 요구 사항과 동일합니다(관리하려는 기기 수에 따름).

소프트웨어 요구 사항:

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

지원되는 운영 체제는 다음과 같습니다:

> 운영 체제에서 프로세스 간 커뮤니케이션을 위해서는 루프백 인터페이스를 사용할 수 있어야 합니다.

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64비트
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core(설치 옵션)(LTSB) 64비트
- Windows Server 2019 Standard/Datacenter/Core 64비트
- Windows Server 2022 Standard/Datacenter/Core 64비트
- Windows Server 2025 Standard/Datacenter/Core 64비트
- Windows Storage Server 2019 64비트

지원되는 가상 플랫폼은 다음과 같습니다.

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 64비트
- Microsoft Hyper-V Server 2022 64비트
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

다음 데이터베이스 서버가 지원됩니다(다른 기기에 설치할 수 있음).

- Microsoft SQL Server 2016 (모든 에디션) 64비트
- Microsoft SQL Server 2017(모든 에디션) Windows/Linux 64비트
- Microsoft SQL Server 2019(모든 에디션) Windows/Linux 64비트(추가 작업 필요)
- Microsoft SQL Server 2022(모든 에디션) Windows/Linux 64비트
- MySQL 5.7 Community 32비트/64비트
- MySQL Standard Edition 8.0(릴리스 8.0.20 이상) 32비트/64비트
- MySQL Enterprise Edition 8.0(릴리스 8.0.20 이상) 32비트/64비트
- MariaDB 10.5(빌드 10.5.27 이상) 32비트/64비트

- MariaDB Galera Cluster 10.3 32비트/64비트 InnoDB 스토리지 엔진
- PostgreSQL 13.x 64비트
- PostgreSQL 14.x 64비트
- PostgreSQL 15.x 64비트
- Postgres Pro 13.x Windows/Linux 64비트
- Postgres Pro 14.x Windows/Linux 64비트

세부 사항 및 제한 사항은 DBMS 선택 주제를 참조하십시오.

SIEM 및 기타 정보 관리 시스템:

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

웹 콘솔 요구 사항

Kaspersky Security Center 웹 콘솔 서버

최소 하드웨어 요구 사항:

- CPU: 4코어, 2.5GHz 동작 주파수.
- RAM: 8 GB.
- 사용 가능한 디스크 공간: 40 GB.

중앙 관리 서버 인증서 요구 사항:

- 인증서 서명 알고리즘 SHA-2
- 최소 키 길이: 2048

인증서를 재발급해야 한다면 Kaspersky Security Center 기술 자료를 참조하십시오.

Kaspersky Security Center 웹 콘솔 서버 지원 운영 체제

운영 체제. Microsoft Windows(64비트 버전만) 운영 체제에서 프로세스 간 커뮤니케이션을 위해서는 루프백 인터페이스를 사용할 수 있어야 합니다.	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core(설치 옵션)(LTSB) Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019

가상화 플랫폼	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

클라이언트 기기

클라이언트 기기에서 브라우저만 있으면 Kaspersky Security Center 웹 콘솔을 사용할 수 있습니다.

최소 화면 해상도는 1366x768 픽셀입니다.

기기의 하드웨어 및 소프트웨어 요구 사항은 Kaspersky Security Center 웹 콘솔에 사용되는 브라우저의 요구 사항과 동일합니다.

브라우저:

- Google Chrome 128.0.6613.120 이상
- Microsoft Edge 128.0.2739.67 이상
- macOS의 Safari 17.6
- "Yandex" Browser 24.7.3.1081 이상
- Mozilla Firefox Extended Support Release 115.14.0 이상

모바일 서버 요구 사항

iOS 모바일 기기 관리(iOS MDM) 서버

하드웨어 요구 사항:

- 처리 속도가 1 GHz 이상인 CPU. 64비트 운영 체제의 경우 최소 CPU 처리 속도는 1.4GHz입니다.
- RAM: 2 GB.
- 사용 가능한 디스크 공간: 2 GB.

소프트웨어 요구 사항: Microsoft Windows(지원하는 운영 체제 버전은 중앙 관리 서버 요구 사항에서 정의됩니다).

관리 콘솔 요구 사항

하드웨어 요구 사항:

- 처리 속도가 1 GHz 이상인 CPU. 64비트 운영 체제의 경우 최소 CPU 처리 속도는 1.4GHz입니다.
- RAM: 512MB.
- 사용 가능한 디스크 공간: 1 GB.

소프트웨어 요구 사항:

- Microsoft Windows 운영 체제(운영 체제 지원 버전은 중앙 관리 서버의 요구 사항에 따라 결정됨).
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64비트
  - Windows Server 2016 Standard/Datacenter/Essentials(LTSB) 64비트
  - Windows Server 2019 Standard/Datacenter 64비트
  - Windows Server 2022 Standard/Datacenter 64비트
  - Windows Server 2025 Standard/Datacenter/Core 64비트
  - Windows Storage Server 2019 64비트
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- 다음에서 실행되는 Microsoft Internet Explorer 11.0:
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Storage Server 2019
- Microsoft Windows Server 2022 Standard에서 실행하는 Microsoft Edge

네트워크 에이전트 요구 사항

최소 하드웨어 요구 사항:

- 처리 속도가 1 GHz 이상인 CPU. 64비트 운영 체제의 경우 최소 CPU 처리 속도는 1.4GHz입니다.
- RAM: 512MB.
- 사용 가능한 디스크 공간: 1 GB.

Linux 기반 기기에 대한 소프트웨어 요구 사항: Perl 언어 인터프리터 버전 5.10 이상이 설치되어 있어야 합니다.

운영 체제. Microsoft Windows	Windows Embedded POSReady 2009 최신 서비스 팩 32비트 Windows Embedded 7 Standard 서비스 팩 1 32비트/64비트 Windows Embedded 8.1 Industry Pro 32비트/64비트 Windows 10 Enterprise 2015 LTSB 32비트/64비트 Windows 10 Enterprise 2016 LTSB 32비트/64비트 Windows 10 IoT Enterprise 2015 LTSB 32비트/64비트 Windows 10 IoT Enterprise 2016 LTSB 32비트/64비트 Windows 10 Enterprise 2019 LTSC 32비트/64비트 Windows 10 IoT Enterprise version 1703 32비트/64비트 Windows 10 IoT Enterprise version 1709 32비트/64비트 Windows 10 IoT Enterprise version 1803 32비트/64비트 Windows 10 IoT Enterprise version 1809 32비트/64비트 Windows 10 20H2 IoT Enterprise 32비트/64비트 Windows 10 21H2 IoT Enterprise 32비트/64비트 Windows 10 IoT Enterprise 32비트/64비트 Windows 10 IoT Enterprise version 1909 32비트/64비트 Windows 10 IoT Enterprise LTSC 2021 32비트/64비트 Windows 10 IoT Enterprise version 1607 32비트/64비트 Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32비트/64비트 Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64비트 Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64비트 Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64비트 Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64비트 Windows 8 Pro/Enterprise 32비트/64비트 Windows 8.1 Pro/Enterprise 32비트/64비트 Windows 7 Home/Pro/Enterprise/Ultimate with Service Pack 1 32비트/64비트 Microsoft Windows XP Professional + 서비스 팩 2 32비트/64비트(네트워크 에이전트 버전 10.5.1781에서만 지원, 기술 지원에 요청할 수 있음) Windows XP Professional 서비스 팩 3 이상 32비트(네트워크 에이전트 버전 14.0.0.20023에서 지원) 임베디드 시스템용 Windows XP Professional 서비스 팩 3 32비트(네트워크 에이전트 버전 14.0.0.20023에서 지원) Windows MultiPoint Server 2011 Standard/Premium 64비트 Windows Server 2003 SP1 32비트/64비트(네트워크 에이전트 버전 10.5.1781에서만 지원) Windows Server 2003 SP2 Standard/Enterprise 32비트/64비트(네트워크 에이전트 버전 10.5.1781에서만 지원) Windows Server 2003 R2 Standard/Enterprise + SP2 32비트/64비트(네트워크 에이전트 버전 10.5.1781에서만 지원) Windows Server 2008 Standard/Enterprise/Datacenter/Foundation 서비스 팩 2 32비트/64비트 Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation 서비스 팩 1 이상 64비트 Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64비트 Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64비트 Windows Server 2016 Standard/Datacenter/Essentials/Server Core(설치 옵션)(LTSB) 64비트 Windows Server 2019 Standard/Datacenter/Core 64비트 Windows Server 2019 RS5 Standard/Essentials 64비트

	Windows Server 2022 Standard/Datacenter/Core 64비트 Windows Server 2022 21H2 Standard/Datacenter 64비트 Windows Server 2025 Standard/Datacenter/Core 64비트 Windows Storage Server 2019 64비트

운영 체제. Linux	Debian GNU/Linux 10.x (Buster) 32비트/64비트 Debian GNU/Linux 11.x (Bullseye) 32비트/64비트 Debian GNU/Linux 12 (Bookworm) 32비트/64비트 Ubuntu Server 18.04 LTS (Bionic Beaver) 64비트 Ubuntu Server 20.04 LTS (Focal Fossa) 64비트 Ubuntu Server 22.04 LTS(Jammy Jellyfish) 64비트 Ubuntu Server 22.04 LTS ARM 64비트 Ubuntu Server 24.04 LTS(Noble Numbat) 64비트 CentOS 6.7 이상 32비트 CentOS 6.x (최대 6.6) 32비트/64비트 CentOS 7.x 64비트 CentOS Stream 8 64비트 CentOS Stream 9 64비트 CentOS Stream 9 ARM 64비트 Red Hat Enterprise Linux Server 6.x 32비트/64비트 Red Hat Enterprise Linux Server 7.x 64비트 Red Hat Enterprise Linux Server 8.x 64비트 Red Hat Enterprise Linux Server 9.x 64비트 SUSE Linux Enterprise Server 12(모든 서비스 팩) 64비트 SUSE Linux Enterprise Server 15 (모든 서비스 팩) 64비트 SUSE Linux Enterprise Server 15(모든 서비스 팩) ARM 64비트 openSUSE 15 64비트 EulerOS 2.0 SP10 64비트 EulerOS 2.0 SP10 ARM 64비트 Astra Linux Special Edition RUSB.10015-01(운영 업데이트 1.5) 64비트 Astra Linux Special Edition RUSB.10015-01(운영 업데이트 1.6) 64비트 Astra Linux Special Edition RUSB.10015-16(Release 1)(운영 업데이트 1.6) 64비트 Astra Linux Special Edition RUSB.10015-17(운영 업데이트 1.7.3) 64비트 Astra Linux Special Edition RUSB.10015-01(운영 업데이트 1.7) 64비트 Astra Linux Special Edition RUSB.10015-01(운영 업데이트 1.8) 64비트 Astra Linux Special Edition RUSB.10015-37(운영 업데이트 7.7) 64비트 Astra Linux Special Edition RUSB.10152-02(운영 업데이트 4.7) ARM 64비트 Astra Linux Common Edition (운영 업데이트 2.12) 64비트 ALT Workstation 10.1 64비트 ALT Server 10.1 64비트 ALT Education 10.1 64비트 ALT SP Server 10 32비트/64비트 ALT SP Server 10 ARM 64비트 ALT SP Workstation 10 32비트/64비트 ALT SP Workstation 10 ARM 64비트 ALT Server 10 64비트 ALT Server 10 ARM 64비트 ALT Workstation 10 32비트/64비트 ALT 8 SP Workstation(8.4) ARM 64비트 ALT 8 SP Server(8.4) ARM 64비트 ALT 8 SP Server(LKNV.11100-01) 32비트/64비트 ALT 8 SP Server(LKNV.11100-02) 32비트/64비트 ALT 8 SP Server(LKNV.11100-03) 32비트/64비트 ALT 8 SP Workstation (LKNV.11100-01) 32비트/64비트 ALT 8 SP Workstation (LKNV.11100-02) 32비트/64비트 ALT 8 SP Workstation (LKNV.11100-03) 32비트/64비트 Mageia 4 32비트 Oracle Linux 7 64비트 Oracle Linux 8 64비트 Oracle Linux 9 64비트 Linux Mint 20.x 64비트

	Linux Mint 21.1 이상 64비트 AlterOS 7.5 이상 64비트 GosLinux IC6/7.17 64비트 GosLinux IC6/7.2 64비트 SberOS 3.3.1 64비트 Platform V SberLinux OS Server(SLO) 8.8 64비트 Platform V SberLinux OS Server(SLO) 8.9.2 64비트 RED OS 7.3 ARM 64비트 RED OS 7.3 Server 64비트 RED OS 7.3 Certified Edition 64비트 RED OS 8 Certified Edition 64비트 ROSA Enterprise Linux Server 7.9 64비트 ROSA Enterprise Linux Desktop 7.9 64비트 ROSA COBALT 7.9 64비트 ROSA CHROME 12 64비트 AlmaLinux 8 이상 64비트 AlmaLinux 9 이상 64비트 Rocky Linux 8 이상 64비트 Rocky Linux 9 이상 64비트 Atlant, Alcyone 빌드, 버전 2022.02 64비트 MSVSPHERE 9.2 SERVER 64비트 MSVSPHERE 9.2 ARM 64비트 SynthesisM Server 8.6 64비트 SynthesisM Client 8.6 64비트 OSnova 2.10 64-bit Kylin 10 64비트 EMIAS 1.0 64비트 Amazon Linux 2 64비트 MosOS 15.4 Arbat 64비트 OS MES(Moscow Electronic School) 64비트
운영 체제. macOS	지원하는 운영 체제 목록은 Kaspersky Endpoint Security for Mac 도움말을 참조하십시오.

네트워크 에이전트의 경우 Intel과 마찬가지로 Apple Silicon(M1) 아키텍처도 지원됩니다.

지원되는 가상 플랫폼은 다음과 같습니다.

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM(커널 기반 가상 머신)

Microsoft Windows Server 2008 R2(서버 버전) 및 Microsoft Windows 7(데스크톱 버전)보다 오래된 Windows 버전에서 네트워크 에이전트는 다음 기능을 지원하지 않습니다.

- 업데이트 재번역(배포 지점에서 사용)
- KSN 프록시(배포 지점에서 사용)
- 취약점 검사 작업

Microsoft Windows 10 버전 RS4 또는 RS5를 실행하는 기기에서 Kaspersky Security Center가 대/소문자 구분이 활성화된 폴더에서 일부 취약점을 탐지하지 못할 수 있습니다.

Windows 7, Windows Server 2008 또는 Windows Server 2008 R2를 실행하는 기기에 네트워크 에이전트를 설치하기 전에 OS Windows용 보안 업데이트 KB3063858(Windows 7용 보안 업데이트(KB3063858)), x64 기반 시스템용 Windows 7용 보안 업데이트(KB3063858), Windows Server 2008용 보안 업데이트(KB3063858), Windows Server 2008 x64 버전용 보안 업데이트(KB3063858), Windows Server 2008 R2 x64 버전용 보안 업데이트(KB3063858)가 설치되었는지 확인하십시오.

Microsoft Windows XP에서는 네트워크 에이전트가 일부 동작을 올바르게 수행하지 않을 수 있습니다.

Microsoft Windows XP에서만 Network Agent for Windows XP를 설치하거나 업데이트할 수 있습니다. 지원하는 운영 체제 목록에 지원하는 Microsoft Windows XP 버전과 해당 버전의 네트워크 에이전트가 있습니다. 이 페이지에서 필요한 Microsoft Windows XP용 네트워크 에이전트 버전을 다운로드할 수 있습니다.

Kaspersky Security Center와 같은 버전의 네트워크 에이전트를 설치할 것을 권장합니다.

Kaspersky Security Center는 같거나 최신 버전의 네트워크 에이전트를 완벽히 지원합니다.

Network Agent for macOS는 이 운영 체제용 Kaspersky 보안 애플리케이션과 함께 제공됩니다.

호환되는 Kaspersky 애플리케이션 및 솔루션

Kaspersky Security Center는 현재 지원하는 모든 Kaspersky 애플리케이션 및 솔루션의 중앙 집중식 배포 및 관리를 지원합니다. 아래 표는 MMC 기반 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에서 지원하는 Kaspersky 애플리케이션 및 솔루션을 보여줍니다. 애리케이션 및 솔루션 버전을 찾으려면 제품 지원 수명 주기 웹페이지를 참조하십시오.

Kaspersky Security Center에서 지원하는 Kaspersky 애플리케이션 및 솔루션 목록

Kaspersky 애플리케이션 또는 솔루션의 이름	MMC 기반 관리 콘솔에서 지원	Kaspersky Security Center 웹 콘솔에서 지원
워크스테이션용		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓

Kaspersky 애플리케이션 또는 솔루션의 이름	MMC 기반 관리 콘솔에서 지원	Kaspersky Security Center 웹 콘솔에서 지원
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	–	✓
산업 솔루션용		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (중앙 집중식 배포는 지원되지 않음)	✓	✓
모바일 기기용		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	–	✓
파일 서버용		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
가상 환경용		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	–
메일 및 협업 서버용		
Kaspersky Security for Microsoft Exchange Servers	✓	–
표적 공격 탐지용		
Kaspersky Sandbox Server	–	✓
Kaspersky Endpoint Detection and Response Optimum	–	✓
Kaspersky Managed Detection and Response	–	✓
KasperskyOS 기기		
Kaspersky IoT Secure Gateway	–	✓
Kaspersky Thin Client	–	✓
평판 데이터베이스		
Kaspersky Private Security Network	–	✓

Kaspersky Security Center 15.1 라이센스 및 기능

Kaspersky Security Center에는 다음 기능에 대한 라이센스가 필요합니다.

아래 표에는 Kaspersky Security Center의 기능에 적용되는 라이센스가 표시됩니다.

Kaspersky Security Center 기능을 활성화하려면 중앙 관리 서버 라이센스 키를 추가하여 중앙 관리 서버를 활성화해야 합니다.

각 중앙 관리 서버에 대한 라이센스 키를 수동으로 추가해야 합니다.

라이센스 및 Kaspersky Security Center 기능

Kaspersky Security Center 기능	Kaspersky 취약점 및 패치 관리 표시	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
취약점 평가	✓	✓	✓	✓	✓	✓	✓
패치 관리	✓	–	✓	✓	–	✓	✓
역할 기반 접근 제어	✓	✓	✓	✓	✓	✓	✓
운영 체제와 애플리케이션의 설치	✓	–	✓	✓	–	✓	✓
모바일 기기 관리 (즉, 사용자의 iOS 및 Android 기기 관리)	✓	✓	✓	✓	–	–	✓
AWS, Microsoft Azure 또는 Google Cloud와 같은 클라우드 환경에서 작업하기 위한 클라우드 환경 구성	–	–	–	–	✓	✓	–
SIEM 시스템으로 이벤트 내보내기: Syslog	✓	✓	✓	✓	✓	✓	✓
SIEM 시스템으로 이벤트 내보내기: QRadar by IBM 및 ArcSight by Micro Focus	✓	✓	✓	✓	✓	✓	✓

Kaspersky Security Center 구성 요소의 호환성 관련 정보

아래 표에서 Kaspersky Security Center 구성 요소의 호환성에 대한 정보를 찾을 수 있습니다.

Kaspersky Security Center 구성 요소의 호환성

구성 요소	호환 항목
Kaspersky Security Center 15.1 중앙 관리 서버	• Kaspersky Security Center 15.1 관리 콘솔. • Kaspersky Security Center 15.1 웹 콘솔. • Kaspersky Security Center 네트워크 에이전트 버전: 16, 15.4, 15.1, 15, 14.2, 14.
Kaspersky Security Center 15.1 웹 콘솔	Kaspersky Security Center 중앙 관리 서버 버전: 15.1 및 14.2.
Kaspersky Security Center 15.1 기본 중앙 관리 서버	보조 중앙 관리 서버: • Kaspersky Security Center 14 Windows • Kaspersky Security Center 14.2 Windows • Kaspersky Security Center 15.1 Windows • Kaspersky Security Center 14.2 Linux • Kaspersky Security Center 15 Linux • Kaspersky Security Center 15.1 Linux

구성 요소	호환 항목
Kaspersky Security Center 15.1 보조 중앙 관리 서버	기본 중앙 관리 서버: • Kaspersky Security Center 14 Windows • Kaspersky Security Center 14.2 Windows • Kaspersky Security Center 15.1 Windows • Kaspersky Security Center 14.2 Linux • Kaspersky Security Center 15 Linux • Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 중앙 관리 서버와 Kaspersky Security Center 웹 콘솔의 최신 버전을 사용하는 것이 좋습니다. 그렇지 않으면 Kaspersky Security Center의 기능이 제한될 수 있습니다. Kaspersky Security Center 중앙 관리 서버와 Kaspersky Security Center 웹 콘솔을 독립적으로 설치하고 업그레이드할 수 있습니다. 이 경우에는 설치된 Kaspersky Security Center 웹 콘솔의 버전이 연결할 중앙 관리 서버 버전과 호환되는지 확인해야 합니다.

Kaspersky Security Center 웹 콘솔의 최신 버전과 Kaspersky Security Center의 이전 버전이 있는 상태에서 도메인 인증 중 오류가 발생하면, 오류 텍스트에 기본 메시지가 포함됩니다.

Windows 기반 및 Linux 기반 Kaspersky Security Center 비교

Kaspersky는 Windows와 Linux 두 가지 플랫폼을 위한 온프레미스 솔루션으로 Kaspersky Security Center를 제공합니다. Windows 기반 솔루션에서는 Windows 기기에 중앙 관리 서버를 설치하고, Linux 기반 솔루션에는 Linux 기기에 설치할 수 있도록 설계된 버전의 중앙 관리 서버가 있습니다. 이 온라인 도움말에는 Kaspersky Security Center Windows에 대한 정보가 포함되어 있습니다. Linux 기반 솔루션에 대한 자세한 내용은 Kaspersky Security Center Linux 온라인 도움말 을 참조하십시오.

아래 표에서 Windows 기반 솔루션 및 Linux 기반 솔루션 Kaspersky Security Center의 주요 기능을 비교할 수 있습니다.

Windows 기반 솔루션 및 Linux 기반 솔루션으로 작동하는 Kaspersky Security Center의 기능 비교

기능 또는 속성	Kaspersky Security Center	
	Windows 기반 솔루션	Linux 기반 솔루션
중앙 관리 서버		
데이터베이스 관리 시스템(DBMS) 위치	온프레미스	온프레미스 (Microsoft SQL은 지원하지 않음)
중앙 관리 서버를 설치할 운영 체제	Windows	Linux
중앙 관리 서버 계층 구조	✓	✓
가상 중앙 관리 서버 지원	✓	✓
SNMP를 사용하여 중앙 관리 서버 통계를 타사 애플리케이션에 전송	✓	2026년에 구현 예정
설치 패키지 및 기타 파일 게시를 위한 웹 서버	✓	✓
Windows Server 장애 조치 클러스터에 중앙 관리 서버 설치	✓	–
관리 콘솔		

기능 또는 속성	Kaspersky Security Center	
	Windows 기반 솔루션	Linux 기반 솔루션
관리 콘솔 유형	MMC 기반 및 웹 기반	웹 기반
웹 기반 관리 콘솔을 설치할 운영 체제	Windows 또는 Linux	Linux
도메인 인증을 사용하여 콘솔에 로그인	✓	✓ 버전 15.1~15.4에서는 싱글 사인온이 지원되지 않습니다
클라이언트 기기 및 관리 그룹 관리		
(중앙 관리 서버 1대당) 관리 중인 기기의 최대 수	100,000	50,000(PostgreSQL 및 Postgres Pro 포함)
네트워크 검색	✓	✓ 버전 16부터 FreeIPA 및 ALD Pro 도메인 컨트롤러가 지원됩니다
Windows, macOS 및 Linux로 관리 중인 기기 보호	✓	✓
모바일 기기 보호	✓ 모바일 기기의 기본 관리	✓ MDM 및 Kaspersky Secure Mobility Management 기능 사용(라이센스 사용)
가상 컴퓨터 보호 관리	✓	✓
퍼블릭 클라우드 인프라 보호	✓	—
클라이언트 기기 데스크톱에 원격 연결	✓	✓ 버전 15.3부터
데이터 암호화 및 보호	✓	✓ Kaspersky Endpoint Security for Windows 또는 Kaspersky Endpoint Security for Mac이 설치된 Windows 기반 관리 중인 기기 대상
Kaspersky Security Center 장애 조치 클러스터 배포	✓	✓
관리 그룹의 클러스터 및 서버 배열 지원	✓	✓
관리 그룹 계층 구조	✓	✓
DMZ에 배포 지점으로 연결 게이트웨이 추가	✓ (MMC 기반 관리 콘솔)	2026년에 구현 예정
사용자 작업		
사용자 계정 생성 및 관리	✓	✓
Kaspersky 애플리케이션 관리		
애플리케이션 정책	✓	✓
Kaspersky 애플리케이션용 작업	✓	✓
Kaspersky Security Network	✓	✓
KSN 프록시	✓	✓
Kaspersky Private Security Network	✓	✓
Kaspersky 애플리케이션용 라이센스 키의 중앙 집중식 배포	✓	✓
클라이언트 기기 원격 진단	✓	✓
Kaspersky 애플리케이션 자동 업데이트	✓	✓
적응형 이상 행위 제어 지원	✓	✓
기기 중심 보안 관리	✓	✓
사용자 중심 보안 관리	✓	✓
시스템 관리		

기능 또는 속성	Kaspersky Security Center	
	Windows 기반 솔루션	Linux 기반 솔루션
클라이언트 기기에 운영 체제 배포	✓	—
타사 라이센스 관리	✓	—
WSUS 서버로 이 중앙 관리 서버 사용	✓	✓ (패시브 Windows 업데이트 검색 모드만 해당)
클라이언트 기기에서 타사 애플리케이션 관리		
타사 소프트웨어 업데이트 설치 및 타사 소프트웨어 취약점 수정	✓	✓
모니터링, 보고 및 감사		
개체 리비전 관리	✓	✓
정책 리비전 비교	✓	2026년에 구현 예정
Kaspersky Endpoint Detection and Response Optimum에서 탐지한 경고 보기 및 작업	✓	✓
관리 중인 기기에서 발생한 이벤트에 대한 알림	✓	✓
정책 상태 및 작업 상태 모니터링	✓	✓
통합		
Kaspersky Managed Detection and Response와의 통합	✓	✓
SIEM 시스템과의 통합	✓	✓ (syslog만 사용)
CEF 및 LEEF 형식을 사용하여 이벤트 내보내기	✓	2026년에 구현 예정
Active directory, KASAP 및 Kaspersky TIP Sandbox를 통해 경고 집계 및 대응 작업 수행	—	✓ (버전 15.4부터) Kaspersky Next XDR Optimum 라이센스를 사용하여 중앙 관리 서버를 활성화한 다음, Kaspersky Next XDR Optimum 라이센스 키를 관리 중인 애플리케이션에 배포해야 합니다.

Kaspersky Security Center Cloud Console 정보

Kaspersky Security Center를 온프레미스 애플리케이션으로 사용하면 로컬 기기에 중앙 관리 서버를 포함한 Kaspersky Security Center를 설치해서 Microsoft Management Console 기반 관리 콘솔(Kaspersky Security Center Windows에서만 이용 가능) 또는 Kaspersky Security Center 웹 콘솔을 통해 네트워크 보안 시스템을 관리할 수 있습니다.

그러나 Kaspersky Security Center를 대신 클라우드 서비스로 사용할 수도 있습니다. 이 경우 Kaspersky 클라우드 환경에 Kaspersky Security Center를 설치하고 Kaspersky가 중앙 관리 서버에 대한 접근 권한을 부여합니다. Kaspersky Security Center Cloud Console이라는 클라우드 기반 관리 콘솔을 통해 네트워크 보안 시스템을 관리합니다. 이 콘솔에는 Kaspersky Security Center 웹 콘솔의 인터페이스와 유사한 인터페이스가 있습니다.

Kaspersky Security Center Cloud Console의 인터페이스 및 설명서는 다음 언어로 제공됩니다:

- 영어
- 프랑스어
- 독일어

- 이탈리아어
- 일본어
- 포르투갈어(브라질)
- 러시아어
- 중국어 간체
- 스페인어
- 스페인어 (라틴 아메리카)
- 중국어 번체

Kaspersky Security Center Cloud Console 정보 및 해당 기능 에 대한 자세한 내용은 Kaspersky Security Center Cloud Console 설명서 및 Kaspersky Endpoint Security for Business 설명서를 참조하십시오.

Kaspersky Security Center 15.1

이 섹션은 Kaspersky Security Center 15.1 사용에 대한 정보를 제공합니다.

온라인 도움말에 제공된 정보는 애플리케이션과 함께 제공된 문서에 있는 정보와 다를 수 있습니다. 이 경우 온라인 도움말이 최신으로 간주됩니다. 애플리케이션 인터페이스에서 링크를 클릭하거나 문서에서 온라인 도움말 링크를 클릭하여 온라인 도움말로 이동할 수 있습니다. 온라인 도움말은 사전 통지 없이 업데이트될 수 있습니다. 필요한 경우 온라인 도움말과 오프라인 도움말 간을 전환할 수 있습니다.

기본 개념

이 섹션에서는 Kaspersky Security Center와 관련된 기본적인 개념을 설명합니다.

중앙 관리 서버

Kaspersky Security Center 구성 요소를 사용하면 클라이언트 기기에 설치된 Kaspersky 애플리케이션을 원격으로 관리할 수 있습니다.

중앙 관리 서버 구성 요소가 설치된 기기를 *중앙 관리 서버*(이하 *서버*)라고 합니다. 중앙 관리 서버는 무단으로 접근할 수 없도록 보호(물리적 보호 포함)해야 합니다.

중앙 관리 서버는 다음과 같은 특성을 갖는 서비스로 기기에 설치됩니다:

- "Kaspersky Security Center 중앙 관리 서버" 이름 사용
- 운영 체제가 시작될 때 자동으로 시작하도록 설정
- 중앙 관리 서버를 설치할 때 선택한 **LocalSystem** 계정 또는 사용자 계정 사용

중앙 관리 서버는 다음과 같은 기능을 수행합니다:

- 관리 그룹 구조 저장
- 클라이언트 기기의 구성과 관련된 정보 저장
- 애플리케이션 배포 패키지의 저장소 구성
- 클라이언트 기기에 애플리케이션을 원격 설치 및 제거
- Kaspersky 애플리케이션의 애플리케이션 데이터베이스 및 소프트웨어 모듈 업데이트
- 클라이언트 기기에서 정책 및 작업 관리
- 클라이언트 기기에서 발생한 이벤트 관련 정보 저장
- Kaspersky 애플리케이션의 작동에 관한 리포트 생성

- 클라이언트 기기에 라이센스 키 배포 및 라이센스 키 관련 정보 저장
- 작업 진행에 대한 알림 전달(예: 클라이언트 기기의 바이러스 탐지)

애플리케이션 인터페이스에서 중앙 관리 서버 이름 지정

MMC 기반 관리 콘솔 및 Kaspersky Security Center 웹 콘솔의 인터페이스에서 중앙 관리 서버는 다음과 같은 이름을 가질 수 있습니다:

- 중앙 관리 서버 기기의 이름(예: "*기기 이름*" 또는 "중앙 관리 서버: *기기 이름*").
- 중앙 관리 서버 기기의 IP 주소(예: "*IP 주소*" 또는 "중앙 관리 서버: *IP 주소*").
- 보조 중앙 관리 서버 및 가상 중앙 관리 서버에는 가상 또는 보조 중앙 관리 서버를 기본 중앙 관리 서버에 연결할 때 지정하는 사용자 지정 이름이 있습니다.
- Linux 기기에 설치된 Kaspersky Security Center 웹 콘솔 사용 시, 애플리케이션이 사용자가 신뢰한다고 지정한 중앙 관리 서버의 이름을 응답 파일에 표시합니다.

Kaspersky Security Center 웹 콘솔 또는 관리 콘솔을 사용하여 중앙 관리 서버에 연결할 수 있습니다.

중앙 관리 서버 계층 구조

중앙 관리 서버는 계층 구조로 구성할 수 있습니다. 각 중앙 관리 서버에는 계층 구조의 서로 다른 중첩 레벨에 여러 개의 보조 중앙 관리 서버(*보조 서버*라고 함)가 있을 수 있습니다. 보조 서버의 중첩 레벨에는 제한이 없습니다. 기본 중앙 관리 서버의 관리 그룹에는 모든 보조 중앙 관리 서버의 클라이언트 기기가 포함됩니다. 따라서 여러 중앙 관리 서버가 네트워크의 분리 및 독립된 각 부분을 관리할 수 있고 해당 서버는 다시 기본 서버에 의해 관리됩니다.

가상 중앙 관리 서버 는 보조 중앙 관리 서버의 특수한 형태입니다.

중앙 관리 서버 계층 구조는 다음을 수행하는 데 사용할 수 있습니다:

- 중앙 관리 서버의 로드를 줄입니다(전체 네트워크에 설치된 단일 중앙 관리 서버와 비교).
- 인트라넷 트래픽을 줄이고 원격 지사와의 협업을 간소화합니다. 기본 중앙 관리 서버와 다른 지역에 있을 수도 있는 모든 네트워크 컴퓨터 간에 연결을 확립할 필요는 없습니다. 각 네트워크 세그먼트에 보조 중앙 관리 서버를 설치하고 보조 서버의 관리 그룹 사이에서 기기를 분산시킨 후, 고속 통신 채널을 통해 보조 서버와 기본 서버 간에 연결을 설정하는 것으로 충분합니다.
- 안티 바이러스 보안 관리자 사이에 책임을 분배합니다. 회사 네트워크의 바이러스 백신 보안 상태에 대한 중앙 집중식 관리와 감시 기능은 모두 그대로 유지됩니다.
- 서비스 공급업체를 통해 Kaspersky Security Center를 사용합니다. 서비스 공급업체는 Kaspersky Security Center와 Kaspersky Security Center 웹 콘솔만 설치하면 됩니다. 여러 조직에 있는 다수의 클라이언트 기기를 관리하기 위해, 서비스 공급업체는 중앙 관리 서버 계층 구조에 보조 중앙 관리 서버(가상 서버 포함)를 추가할 수 있습니다.

관리 그룹 계층 구조에 있는 각 기기는 하나의 중앙 관리 서버에만 연결할 수 있습니다. 사용자 기기와 중앙 관리 서버의 연결을 하나씩 감시해야 합니다. 네트워크 속성을 기준으로 여러 서버의 관리 그룹에서 기기 검색 기능을 사용하십시오.

가상 중앙 관리 서버

가상 중앙 관리 서버(또는 *가상 서버*라고도 함)는 클라이언트 조직 네트워크의 안티 바이러스 보호 시스템을 관리하기 위한 Kaspersky Security Center의 구성 요소입니다.

가상 중앙 관리 서버는 보조 중앙 관리 서버의 특수한 형태이며 실제 중앙 관리 서버와 비교하여 다음과 같은 제약이 따릅니다.

- 가상 중앙 관리 서버는 기본 중앙 관리 서버에서만 만들 수 있습니다.
- 가상 중앙 관리 서버는 작동 시 기본 중앙 관리 서버 데이터베이스를 사용합니다. 데이터 백업 및 복원 작업과 업데이트 검사 및 다운로드 작업은 가상 중앙 관리 서버에서 지원되지 않습니다.
- 가상 서버에서는 보조 중앙 관리 서버(가상 서버 포함) 만들기가 지원되지 않습니다.

그 외에도, 가상 중앙 관리 서버에는 다음과 같은 제한이 있습니다:

- 가상 중앙 관리 서버 속성 창의 섹션 수가 제한됩니다.
- 가상 중앙 관리 서버에서 관리하는 기기에 Kaspersky 애플리케이션을 원격으로 설치하려면, 가상 중앙 관리 서버와의 통신을 보장할 수 있도록 기기 중 하나에 네트워크 에이전트를 설치해야 합니다. 가상 중앙 관리 서버에 처음 연결할 때 배포 지점이 해당 기기에 자동으로 할당되어 클라이언트 기기와 가상 중앙 관리 서버 간 연결 게이트웨이 역할을 합니다.
- 가상 서버는 배포 지점을 사용하여 네트워크를 검색만 할 수 있습니다.
- 오작동하는 가상 서버를 다시 시작하려면 Kaspersky Security Center에서 기본 중앙 관리 서버 및 모든 가상 중앙 관리 서버를 다시 시작해야 합니다.
- 가상 서버에서 생성된 사용자에게는 중앙 관리 서버의 역할을 할당할 수 없습니다.

가상 중앙 관리 서버의 관리자는 해당 가상 서버에 대한 모든 권한을 보유합니다.

모바일 기기 서버

*모바일 기기 서버*는 관리 콘솔을 통해 모바일 기기에 대한 접근 및 관리 기능을 제공하는 Kaspersky Security Center의 한 구성 요소입니다. 모바일 기기 서버는 모바일 기기에 대한 정보를 수집하고 프로필을 저장합니다.

Kaspersky Security Center에는 iOS MDM 서버가 모바일 기기 서버로 포함됩니다. 이 모바일 기기 서버는 Apple® Push Notification(APNs) 서비스를 지원하는 모바일 기기를 관리하는 데 사용됩니다.

Kaspersky Security Center의 모바일 기기 서버는 다음 개체를 관리할 수 있도록 합니다:

- 개별 모바일 기기.
- 여러 모바일 기기.
- 서버 클러스터에 동시 연결된 여러 모바일 기기. 서버 클러스터에 연결한 후에는 이 클러스터에 설치된 모바일 기기 서버가 관리 콘솔에 단일 서버로 표시됩니다.

웹 서버

Kaspersky Security Center *웹 서버*(이후 *웹 서버*라고도 함)는 중앙 관리 서버와 함께 설치되는 Kaspersky Security Center의 한 구성 요소입니다. 웹 서버는 독립 실행형 설치 패키지, iOS MDM 프로필 및 공유 폴더의 파일을 네트워크를 통해 게시하도록 설계되었습니다.

독립 실행형 설치 패키지를 만들면 자동으로 웹 서버에 게시됩니다. 만들어진 독립 실행형 설치 패키지의 목록에 독립 실행형 패키지를 다운로드할 수 있는 링크가 표시됩니다. 필요할 경우 독립 실행형 패키지의 게시를 취소하거나 다시 웹 서버에 게시하도록 선택할 수 있습니다.

사용자의 모바일 기기에 대해 만든 iOS MDM 프로필 또한 자동으로 웹 서버에 게시됩니다. 게시된 프로필은 사용자 모바일 기기에 정상적으로 설치되는 즉시 웹 서버에서 자동으로 삭제됩니다.

공유 폴더는 중앙 관리 서버에 의해 기기가 관리되는 모든 사용자에게 제공될 정보 저장소로 사용됩니다. 공유 폴더에 직접 접근할 수 있는 권한이 없는 사용자에게 웹 서버를 통해 공유 폴더의 정보를 제공할 수 있습니다.

웹 서버를 통해 사용자에게 공유 폴더의 정보를 제공하기 위해서는 관리자가 "public"이라는 이름의 하위 폴더를 만들고 관련 정보를 복사해야 합니다.

정보 전송 링크의 구문은 다음과 같습니다:

`https://<웹 서버 이름>:<HTTPS 포트>/public/<개체>`

여기서:

- `<Web Server name>`은 Kaspersky Security Center 웹 서버의 이름입니다.
- `<HTTPS port>`는 관리자가 정의한 웹 서버의 HTTPS 포트입니다. 중앙 관리 서버의 속성 창, **웹 서버** 섹션에서 HTTPS 포트를 설정할 수 있습니다. 기본 포트 번호는 8061입니다.
- `<object>`는 사용자가 접근할 수 있는 하위 폴더 또는 파일입니다.

관리자는 이메일 등의 편리한 방법을 사용하여 새 링크를 전송할 수 있습니다.

사용자는 링크를 사용하여 요청된 정보를 로컬 기기로 다운로드할 수 있습니다.

네트워크 에이전트

중앙 관리 서버와 기기 간의 상호 작용은 Kaspersky Security Center의 *네트워크 에이전트* 구성 요소에 의해 수행됩니다. 네트워크 에이전트는 Kaspersky Security Center가 Kaspersky 애플리케이션을 관리하는 데 사용되는 모든 기기에 설치해야 합니다.

네트워크 에이전트는 다음과 같은 특성을 갖는 서비스로 기기에 설치됩니다:

- "Kaspersky Security Center 네트워크 에이전트" 이름
- 운영 체제가 시작될 때 자동으로 시작하도록 설정
- LocalSystem 계정 사용

네트워크 에이전트가 설치된 기기는 *관리 중인 기기* 또는 *기기*라고 합니다.

Windows, Linux 또는 Mac 기기에 네트워크 에이전트를 설치할 수 있습니다. 다음 경로 중 하나에서 구성 요소를 가져올 수 있습니다:

- 중앙 관리 서버 스토리지의 설치 패키지 (중앙 관리 서버가 설치되어 있어야 함)
- Kaspersky 웹 서버에 있는 설치 패키지

중앙 관리 서버를 설치하는 기기에는 네트워크 에이전트를 설치하지 않아도 됩니다. 네트워크 에이전트의 서버 버전이 중앙 관리 서버와 함께 자동으로 설치되기 때문입니다.

네트워크 에이전트가 시작하는 프로세스의 이름은 *klnagent.exe*입니다.

네트워크 에이전트는 관리 중인 기기를 중앙 관리 서버와 동기화합니다. 동기화 간격(*존재-알림 신호*라고도 함)은 관리 중인 기기 10,000개당 15분으로 설정하는 것이 좋습니다.

관리 그룹

관리 그룹(이후 *그룹*이라고도 함)은 Kaspersky Security Center 내의 기기를 하나의 단위로 관리하기 위해 특정 기준에 따라 통합된 관리 중인 기기의 논리적인 집합입니다.

관리 그룹 내의 모든 관리 중인 기기는 다음과 같이 작동하도록 구성됩니다:

- 동일한 애플리케이션 설정 사용(그룹 정책에서 지정).
- 지정된 설정의 그룹 작업을 만들어 모든 애플리케이션에 대한 공통 작동 모드를 사용합니다. 그룹 작업의 예로는 공통 설치 패키지 만들기 및 설치, 애플리케이션 데이터베이스 및 모듈 업데이트, 기기 수동 검사 작업, 실시간 보호 켜기 등이 있습니다.

관리 중인 기기는 하나의 관리 그룹에만 소속될 수 있습니다.

중앙 관리 서버와 그룹에 대해 원하는 중첩 수준의 계층 구조를 만들 수 있습니다. 하나의 계층 구조 레벨에는 보조 및 가상 중앙 관리 서버, 그룹 및 관리 중인 기기가 포함될 수 있습니다. 기기를 실제로 옮기지 않고도 그룹 간에 이동할 수 있습니다. 예를 들어 기업 내 작업자 직무가 경리에서 개발자로 변경되는 경우 해당 작업자의 기기를 경리 관리 그룹에서 개발자 관리 그룹으로 이동할 수 있습니다. 그리고 나면 해당 기기에는 개발자에게 필요한 애플리케이션 설정이 자동으로 수신됩니다.

관리 중인 기기

*관리 중인 기기*는 네트워크 에이전트가 설치된 Windows, Linux 또는 macOS를 실행하는 기기 또는 Kaspersky 보안 제품이 설치된 모바일 기기입니다. 이러한 기기에 설치된 애플리케이션용 작업과 정책을 만들어 해당 기기를 관리할 수 있습니다. 관리 중인 기기에서 리포트를 수집할 수도 있습니다.

모바일이 아닌 관리 중인 기기를 배포 지점과 연결 게이트웨이 기능을 하도록 지정할 수 있습니다.

각 기기는 중앙 관리 서버 하나를 통해서만 관리할 수 있습니다. 중앙 관리 서버 한 대는 모바일 기기를 포함하여 기기를 최대 10만 대까지 지원할 수 있습니다.

미할당 기기

*미할당 기기*는 어떤 관리 그룹에도 포함되지 않은 네트워크의 기기입니다. 미할당 기기에 특정 작업을 수행할 수 있습니다. 예, 관리 그룹으로 이동 또는 애플리케이션 설치.

네트워크에서 새로 발견되는 기기는 **미할당 기기** 관리 그룹에 추가됩니다. 발견된 기기가 다른 관리 그룹으로 자동 이동되도록 규칙을 구성할 수 있습니다.

관리자 워크스테이션

*관리자 워크스테이션*은 관리 콘솔을 설치했거나 사용자가 Kaspersky Security Center 웹 콘솔을 열기 위해 사용하는 기기입니다. 관리자는 클라이언트 기기에 설치된 Kaspersky 애플리케이션을 중앙 집중식으로 원격 관리하는 목적으로 이 기기를 사용할 수 있습니다.

기기에 관리 콘솔이 설치되면 해당 아이콘이 표시되고 이 아이콘을 사용하여 관리 콘솔을 실행할 수 있습니다. 해당 아이콘은 **시작 → 프로그램 → Kaspersky Security Center** 메뉴에 있습니다.

관리자 워크스테이션의 수에는 제한이 없습니다. 어느 관리자 워크스테이션에서나 네트워크에 있는 여러 중앙 관리 서버의 관리 그룹을 한꺼번에 관리할 수 있습니다. 관리자 워크스테이션을 계층 구조 레벨에 관계없이 모든 중앙 관리 서버(실제 서버 또는 가상 서버)에 연결할 수 있습니다.

또한 관리자 워크스테이션을 관리 그룹에 클라이언트 기기로 포함시킬 수 있습니다.

중앙 관리 서버의 관리 그룹 내에서 동일한 기기가 중앙 관리 서버 클라이언트, 중앙 관리 서버 또는 관리자 워크스테이션 기능을 수행할 수 있습니다.

관리 플러그인

Kaspersky 애플리케이션은 관리 콘솔에서 *관리 플러그인*이라는 전용 구성 요소를 통해 관리됩니다. Kaspersky Security Center를 통해 관리할 수 있는 각 Kaspersky 애플리케이션에는 관리 플러그인이 포함되어 있습니다.

애플리케이션 관리 플러그인을 사용하여 관리 콘솔에서 다음 작업을 수행할 수 있습니다:

- 애플리케이션 정책과 설정 만들기 및 편집, 애플리케이션 작업 설정.
- 애플리케이션 작업, 애플리케이션 이벤트 및 클라이언트 기기로부터 받은 애플리케이션 작동 통계 수집.

Kaspersky 기술 지원 웹페이지에서 관리 플러그인을 다운로드할 수 있습니다.

관리 웹 플러그인

특수 구성 요소인 *관리 웹 플러그인*은 Kaspersky Security Center 웹 콘솔을 통해 Kaspersky 소프트웨어를 원격으로 관리하는 데 사용됩니다. 여기서는 관리 웹 플러그인을 *관리 플러그인*이라고도 합니다. 관리 플러그인은 Kaspersky Security Center 웹 콘솔과 특정 Kaspersky 애플리케이션 간의 인터페이스입니다. 관리 플러그인을 사용하여 애플리케이션용 작업과 정책을 구성할 수 있습니다.

Kaspersky 웹페이지에서 관리 웹 플러그인을 다운로드할 수 있습니다.

관리 플러그인에서는 다음을 제공합니다:

- 애플리케이션 작업 및 설정을 생성하고 편집할 수 있는 인터페이스
- Kaspersky 애플리케이션과 기기의 원격/중앙 집중식 구성을 위해 정책 및 정책 프로필을 생성하고 편집할 수 있는 인터페이스
- 애플리케이션에서 생성하는 이벤트 전송
- 애플리케이션의 작동 데이터와 이벤트 및 클라이언트 기기에서 전달되는 통계를 표시하기 위한 Kaspersky Security Center 웹 콘솔 기능

정책

*정책*은 중앙 관리 그룹 및 그 하위 그룹에 적용되는 Kaspersky 애플리케이션 설정의 집합입니다. 관리 그룹의 기기에 여러 Kaspersky 애플리케이션을 설치할 수 있습니다. Kaspersky Security Center는 관리 그룹의 각 Kaspersky 애플리케이션에 대해 단일 정책을 제공합니다. 정책의 상태는 다음 중 하나입니다(아래 표 참조).

정책의 상태

상태	설명
활성	기기에 적용되는 현재 정책입니다. 각 관리 그룹의 Kaspersky 애플리케이션에는 하나의 정책만 활성화될 수 있습니다. 기기는 Kaspersky 애플리케이션에 대한 활성 정책의 설정 값을 적용합니다.
비활성	현재 기기에 적용되지 않은 정책입니다.
이동 사용자	이 옵션을 선택하면 기기가 회사 네트워크를 벗어나는 경우 정책이 활성화됩니다.

정책은 다음 규칙에 따라 작동합니다.

- 하나의 애플리케이션에 대해 서로 다른 값을 갖는 다중 정책을 구성할 수 있습니다.
- 현재 애플리케이션에 하나의 정책만 활성화될 수 있습니다.
- 특정 이벤트가 발생하면 비활성화된 정책을 활성화할 수 있습니다. 예를 들어 바이러스가 급증할 때 더 엄격한 안티 바이러스 보호 설정을 강제할 수 있습니다.
- 정책에는 하위 정책이 포함될 수 있습니다.

일반적으로 바이러스 공격과 같은 비상 상황에 대비하여 정책을 사용할 수 있습니다. 예를 들어, 플래시 드라이브를 통한 공격이 있는 경우 플래시 드라이브에 대한 액세스를 차단하는 정책을 활성화할 수 있습니다. 이 경우 현재 활성 정책은 자동으로 비활성화됩니다.

예를 들어 서로 다른 상황에서 여러 설정만 변경한다고 가정하는 경우와 같이 여러 정책을 유지하는 것을 방지하기 위해 정책 프로필을 사용할 수 있습니다.

*정책 프로필*은 정책의 설정 값을 대체하는 정책 설정 값으로 구성된 명명된 하위 집합입니다. 정책 프로필은 관리 중인 기기에 대한 유효 설정 구성에 영향을 줍니다. *유효 설정*은 현재 기기에 적용된 정책 설정, 정책 프로필 설정 및 로컬 애플리케이션 설정의 집합입니다.

정책 프로필은 다음 규칙에 따라 작동합니다.

- 정책 프로필은 특정 활성화 조건이 발생할 때 적용됩니다.
- 정책 프로필에는 정책 설정이 아닌 설정 값이 포함됩니다.
- 정책 프로필을 활성화하면 관리 중인 기기의 유효 정책 설정이 변경됩니다.
- 프로필에는 최대 100개의 정책 프로필이 포함될 수 있습니다.

정책 프로필

여러 관리 그룹용으로 단일 정책의 여러 인스턴스를 만들어야 하는 경우도 있고, 해당 정책의 설정을 중앙에서 수정하려는 경우도 있습니다. 이러한 인스턴스에서는 설정이 한두 가지만 다를 수도 있습니다. 기업의 모든 경리 직원이 같은 정책에 따라 업무를 처리하는데 상급 경리 직원만 플래시 드라이브를 사용할 수 있는 경우를 예로 들어 보겠습니다. 이 경우 관리 그룹 계층 구조를 통해서만 기기에 정책을 적용하는 방식은 불편할 수 있습니다.

Kaspersky Security Center에서는 단일 정책의 여러 인스턴스를 만들 필요 없이 *정책 프로필*을 만들면 됩니다. 정책 프로필은 단일 관리 그룹 내의 기기가 다른 정책 설정으로 실행될 수 있도록 하기 위해 필요합니다.

정책 프로필은 정책 설정의 명명된 하위 집합입니다. 이 하위 집합은 정책과 함께 대상 기기에 배포되며 *프로필 활성화 조건*이라는 특수 조건에서 정책을 보완합니다. 관리 중인 기기에서 활성 상태인 "기본" 정책과 다른 설정만 프로필에 포함됩니다. 프로필을 활성화하면 기기에서 초기에 활성화되었던 "기본" 정책의 설정이 수정됩니다. 이 수정 설정은 프로필에 지정된 값을 사용합니다.

작업

Kaspersky Security Center에서는 *작업*을 만들고 실행하여 기기에 설치된 Kaspersky 보안 제품을 관리할 수 있습니다. 작업은 애플리케이션을 설치, 실행 및 중단하고, 파일을 검사하며, 데이터베이스와 소프트웨어 모듈을 업데이트하고, 애플리케이션에 대해 기타 작업을 수행하는 데 필요합니다.

특정 애플리케이션용 관리 플러그인이 설치되어 있어야 해당 애플리케이션용 작업을 생성할 수 있습니다.

중앙 관리 서버와 기기에서 작업을 수행할 수 있습니다.

다음 작업이 중앙 관리 서버에서 수행됩니다:

- 리포트 자동 배포
- 중앙 관리 서버 저장소 업데이트 다운로드
- 중앙 관리 서버 데이터 백업
- 데이터베이스 유지 보수
- Windows 업데이트 동기화
- 참조 기기의 운영 체제(OS) 이미지에 따라 설치 패키지 만들기

기기에서 수행되는 작업 유형은 다음과 같습니다:

- *로컬 작업* - 특정 기기에서 수행되는 작업

  로컬 작업은 관리자가 관리 콘솔 도구를 사용하여 수정할 수도 있고, 원격 기기의 사용자가 보안 제품 인터페이스 등을 통해 수정할 수도 있습니다. 관리자와 관리 중인 기기 사용자가 로컬 작업을 동시에 수정한 경우에는 우선 순위가 더 높은 관리자가 수행한 변경 사항이 적용됩니다.

- *그룹 작업* - 특정 그룹의 모든 기기에서 수행되는 작업

  작업 속성에 별도로 지정된 경우가 아니면 그룹 작업은 선택한 그룹의 모든 하위 그룹에도 영향을 줍니다. 그룹 작업은 이 그룹이나 해당 하위 그룹에 배포한 보조 및 가상 중앙 관리 서버에 연결된 기기에도 선택적으로 적용됩니다.

- *글로벌 작업* - 그룹에 포함되어 있는지 여부에 관계없이 선택한 기기에서 수행되는 작업

각 애플리케이션에 대해 그룹 작업, 글로벌 작업 또는 로컬 작업을 원하는 수만큼 만들 수 있습니다.

작업 설정을 변경하고 작업 진행 상황을 확인하며, 해당 설정의 복사, 내보내기, 가져오기 및 삭제를 수행할 수 있습니다.

작업을 만든 애플리케이션이 실행 중인 경우에만 기기에서 작업이 시작됩니다.

작업의 결과는 중앙 관리 서버에 중앙 집중식으로 Microsoft Windows 이벤트 로그 및 Kaspersky Security Center 이벤트 로그에 저장되며, 각 기기에 로컬로도 동일하게 저장됩니다.

작업 설정에 기밀 데이터를 포함하지 마십시오. 예를 들어, 도메인 관리자 암호를 지정하지 마십시오.

작업 범위

*작업의 범위*는 작업이 수행되는 기기 세트입니다. 범위의 유형은 다음과 같습니다:

- *로컬 작업*의 경우 범위는 기기 자체입니다.
- *중앙 관리 서버 작업*의 경우 범위는 중앙 관리 서버입니다.
- *그룹 작업*의 경우 범위는 그룹에 포함된 기기 목록입니다.

*글로벌 작업*을 만들 때는 다음 방법을 사용하여 범위를 지정할 수 있습니다.

- 특정 기기를 수동으로 지정합니다.

  IP 주소(또는 IP 범위), NetBIOS 이름 또는 DNS 이름을 기기의 주소로 사용할 수 있습니다.

- 추가할 기기의 주소가 포함된 .txt 파일에서 기기의 목록을 가져옵니다(줄당 하나의 주소를 표시해야 함).

  파일에서 기기의 목록을 가져오거나 수동으로 작성할 경우 기기가 이름으로 식별되면, 중앙 관리 서버 데이터에 이미 정보가 입력된 기기만 목록에 포함됩니다. 또한 해당 기기가 연결될 때나 기기 발견 중에 정보가 입력된 상태여야 합니다.

- 기기 선택 지정.

시간이 지남에 따라 조회에 포함된 기기 집합이 변경되면 작업 범위도 변경됩니다. 기기에 설치되어 있는 소프트웨어를 비롯한 기기 특성과, 기기에 할당된 태그를 기준으로 기기를 조회할 수 있습니다. 기기 조회 방식은 가장 유연하게 작업 범위를 지정하는 방법입니다.

기기 선택 작업은 항상 중앙 관리 서버에서 스케줄에 따라 실행됩니다. 중앙 관리 서버에 연결되어 있지 않은 기기에서는 이러한 작업을 실행할 수 없습니다. 다른 방법을 사용하여 범위를 지정한 작업은 기기에서 직접 실행되므로 중앙 관리 서버에 대한 기기 연결을 사용하지 않습니다.

기기 선택을 통한 작업은 기기의 로컬 시간에 실행되는 대신 중앙 관리 서버의 로컬 시간에 실행됩니다. 다른 방법을 사용하여 범위를 지정한 작업은 기기의 로컬 시간에 실행됩니다.

로컬 애플리케이션 설정과 정책의 관계

정책을 사용하여 그룹의 모든 기기에 대해 동일한 애플리케이션 설정 값을 지정할 수 있습니다.

정책으로 지정된 설정 값은 로컬 애플리케이션 설정을 사용하여 그룹의 개별 기기에 대해 재정의할 수 있습니다. 사용자는 정책에서 수정을 허용한 설정 값, 즉 잠금 해제된 설정 값만 설정할 수 있습니다.

애플리케이션이 클라이언트 기기에서 사용하는 설정 값은 정책 내 해당 설정의 잠금 위치(🔒)에 의해 결정됩니다:

- 설정 수정이 잠긴 경우, 정책에 정의된 동일한 값이 모든 클라이언트 기기에서 사용됩니다.
- 설정 수정이 "잠금 해제"된 경우, 애플리케이션은 정책에서 지정된 값 대신 로컬 설정 값을 각 클라이언트 기기에서 사용합니다. 이 경우 로컬 애플리케이션 설정에서 설정을 변경할 수 있습니다.

이처럼 클라이언트 기기에서 작업이 실행될 때 애플리케이션은 다음 두 가지 방식으로 정의된 설정을 적용합니다:

- 정책에서 설정을 변경하지 못하도록 잠기지 않은 경우, 작업 설정 및 로컬 애플리케이션 설정 사용.
- 설정의 변경이 잠긴 경우 그룹 정책 사용.

로컬 애플리케이션 설정은 우선 정책 설정에 따라 정책이 적용된 후에 변경됩니다.

배포 지점

배포 지점(기존 업데이트 에이전트)은 네트워크 에이전트가 설치된 기기이며 업데이트 배포, 애플리케이션 원격 설치 및 연결된 기기에 대한 정보 수집에 활용됩니다. 배포 지점은 업데이트 배포 속도를 높이고 중앙 관리 서버의 리소스를 절약합니다.

배포 지점으로 사용되는 기기에 설치된 네트워크 에이전트의 기능과 사용 사례는 운영 체제에 따라 달라집니다.

배포 지점은 다음 기능을 수행할 수 있습니다:

- 중앙 관리 서버에서 받은 파일을 UDP를 사용한 멀티캐스팅 등의 방식으로 그룹 내 클라이언트 기기에 배포합니다.

배포 지점을 통해 전송할 수 있는 파일 목록은 다음과 같습니다.

- Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트
- 타사 소프트웨어 업데이트
- 설치 패키지
- 중앙 관리 서버를 WSUS 서버로 사용 시 Windows 업데이트

업데이트는 중앙 관리 서버 또는 Kaspersky 업데이트 서버에서 받을 수 있습니다. 후자의 경우에는 배포 지점에 대해 업데이트 작업이 생성되어야 합니다. macOS를 실행하는 배포 지점 기기는 Kaspersky 업데이트 서버에서 업데이트를 다운로드할 수 없습니다.

macOS를 실행하는 하나 이상의 기기가 *배포 지점의 저장소로 업데이트 다운로드 작업 범위*에 있는 경우 모든 Windows 기기에서 작업이 성공적으로 완료되어도 작업은 *실패* 상태로 완료됩니다.

기기에 할당된 모든 배포 지점에 문제가 발생하면 기기는 업데이트(안티 바이러스 데이터베이스 및 패치)와 설치 패키지를 수신하지 않습니다.

- UDP를 통한 멀티캐스팅을 사용하여 정책 및 그룹 작업을 배포합니다.
- 중앙 관리 서버에 대한 관리 그룹 내 기기의 연결 게이트웨이로 작동합니다.

  그룹 내 관리 중인 기기와 중앙 관리 서버 간의 직접 연결을 설정할 수 없으면 이 그룹의 중앙 관리 서버에 대한 연결 게이트웨이로 배포 지점을 사용할 수 있습니다. 이 경우 관리 중인 기기는 연결 게이트웨이에 연결되며 연결 게이트웨이는 중앙 관리 서버에 연결됩니다.

  연결 게이트웨이로 작동하는 배포 지점의 존재 여부에 따라 관리 중인 기기와 중앙 관리 서버 간의 직접 연결 옵션이 차단되지는 않습니다. 연결 게이트웨이는 사용할 수 없지만 중앙 관리 서버와의 직접 연결이 기술적으로 가능한 경우에는 관리 중인 기기가 중앙 관리 서버에 직접 연결됩니다.
- 네트워크를 검색해서 새로운 기기를 탐지하고 기존 기기에 대한 정보를 업데이트합니다. 배포 지점은 중앙 관리 서버의 기기 발견 방법을 똑같이 적용할 수 있습니다.
- 배포 지점 운영 체제의 도구를 사용하여 타사 소프트웨어 및 Kaspersky 애플리케이션의 원격 설치를 수행합니다. 배포 지점은 네트워크 에이전트 없이 클라이언트 기기에서 설치를 수행할 수 있습니다.

  이 기능을 사용하면 네트워크 에이전트 설치 패키지를 중앙 관리 서버가 직접 접근할 수 없는 네트워크에 있는 클라이언트 기기로 원격 전송할 수 있습니다.
- Kaspersky Security Network(KSN)에 참여하는 프록시 서버 역할 수행.

  배포 지점 측에서 KSN 프록시를 활성화하여 기기가 KSN 프록시 역할을 하도록 할 수 있습니다. 이때, KSN 프록시 서비스(ksnproxy)가 기기에서 실행됩니다.

파일은 HTTP(SSL 연결을 사용하는 경우 HTTPS)를 통해 중앙 관리 서버에서 배포 지점로 전송됩니다. HTTP 또는 HTTPS를 사용할 경우 트래픽 커팅이 가능하므로 SOAP에 비해 성능이 향상됩니다.

네트워크 에이전트가 설치된 기기에는 수동(관리자에 의해) 또는 자동(중앙 관리 서버에 의해)으로 배포 지점을 할당할 수 있습니다. 지정한 관리 그룹의 전체 배포 지점 목록은 배포 지점 목록에 대한 리포트에서 확인할 수 있습니다.

배포 지점의 범위는 에이전트가 관리자에 의해 할당된 관리 그룹 및 모든 포함 레벨의 하위 그룹입니다. 관리 그룹 계층 구조에 여러 배포 지점이 할당된 경우 관리 중인 기기의 네트워크 에이전트는 계층 구조의 가장 가까운 배포 지점에 연결합니다.

네트워크 위치는 배포 지점의 범위가 될 수 있습니다. 네트워크 위치는 배포 지점이 업데이트를 배포할 대상 기기를 수동으로 만들 때 사용합니다. 네트워크 위치는 Windows 운영 체제를 실행하는 기기에 대해서만 결정됩니다.

만일 배포 지점이 중앙 관리 서버에 의해 자동으로 할당된다면 관리 그룹이 아닌 브로드캐스트 도메인에 의해 할당됩니다. 이는 모든 브로드캐스트 도메인이 알려질 때 발생됩니다. 네트워크 에이전트는 동일 서브넷에 있는 다른 네트워크 에이전트와 메시지를 교환하고 자기 자신과 다른 네트워크 에이전트에 대한 정보를 중앙 관리 서버에 전송합니다. 중앙 관리 서버는 브로드캐스트 도메인으로 네트워크 에이전트 그룹화하기 위해 이러한 정보를 이용합니다. 관리 그룹에서 70% 이상의 네트워크 에이전트가 검색된 이후에 브로드캐스트 도메인이 중앙 관리 서버에 표시됩니다. 중앙 관리 서버는 두 시간마다 브로드캐스트 도메인을 검색합니다. 배포 지점이 브로드캐스트 도메인에 의해 할당된 후 관리 그룹에 의해 재할당될 수 없습니다.

관리자가 수동으로 배포 지점을 할당하는 경우 관리 그룹이나 네트워크 위치에 할당할 수 있습니다.

활성 연결 프로필을 가진 네트워크 에이전트는 브로드캐스트 도메인 탐지에 참여하지 않습니다.

Kaspersky Security Center는 각 네트워크 에이전트에 다른 주소와는 다른 고유의 IP 멀티캐스트 주소를 할당합니다. 그러면 IP 중복으로 인해 발생할 수 있는 네트워크 과부하 문제를 방지할 수 있습니다.

두 개 이상의 배포 지점이 하나의 네트워크 영역 또는 하나의 관리 그룹에 할당되면, 그 중 하나는 활성 배포 지점이 되고 나머지는 대기 배포 지점로 남게 됩니다. 활성 배포 지점은 중앙 관리 서버에서 직접 업데이트 및 설치 패키지를 다운로드하고 대기 배포 지점은 활성 배포 지점에서만 업데이트를 가져옵니다. 이런 경우, 일단 중앙 관리 서버로부터 파일이 다운로드되고 배포 지점 간에 파일이 배포됩니다. 만일 활성 배포 지점이 어떤 이유로 인해 동작을 하지 않는다면, 대기 배포 지점 중 하나가 활성됩니다. 중앙 관리 서버는 자동으로 배포 지점을 대기 상태로 할당합니다.

이 경우 배포 지점 상태(*활성*/*대기*)가 klnagchk 리포트에 확인란과 함께 표시됩니다.

배포 지점은 최소 4GB의 디스크 여유 공간이 필요합니다. 배포 지점의 디스크 여유 공간이 2GB 미만일 시, Kaspersky Security Center는 심각도 레벨이 *경고*인 보안 문제를 생성합니다. 이 보안 문제는 기기 속성의 **보안 문제** 섹션에 게시됩니다.

배포 지점로 할당된 기기에서 원격 설치 작업을 실행하려면 디스크 여유 공간이 추가로 필요합니다. 디스크 여유 공간의 양은 설치할 모든 설치 패키지의 총 크기보다 커야 합니다.

배포 지점로 할당된 기기에서 업데이트(패치) 작업과 취약점 수정 작업을 실행하려면 디스크 여유 공간이 추가로 필요합니다. 디스크 여유 공간의 양은 설치할 모든 패치의 총 크기 2배 이상이어야 합니다.

배포 지점 기능을 하는 기기는 무단으로 접근할 수 없도록 보호(물리적 보호 포함)해야 합니다.

연결 게이트웨이

*연결 게이트웨이*는 특수 모드에서 작동하는 네트워크 에이전트입니다. 연결 게이트웨이는 다른 네트워크 에이전트의 연결을 수락하고 서버와의 자체 연결을 통해 이를 중앙 관리 서버로 터널링합니다. 일반 네트워크 에이전트와 달리 연결 게이트웨이는 중앙 관리 서버에 대한 연결을 설정하지 않고 중앙 관리 서버의 연결을 기다립니다.

연결 게이트웨이는 최대 1만 대의 기기와 연결할 수 있습니다.

연결 게이트웨이는 다음 두 가지 옵션으로 사용할 수 있습니다.

- DMZ(완충 지역)에 연결 게이트웨이를 설치하는 것이 좋습니다. 이동 사용자 기기에 설치된 다른 네트워크 에이전트의 경우 연결 게이트웨이를 통해 중앙 관리 서버에 대한 연결을 특별히 구성해야 합니다.

  연결 게이트웨이는 네트워크 에이전트에서 중앙 관리 서버로 전송되는 데이터를 수정하거나 처리하지 않습니다. 또한 이 데이터를 버퍼에 쓰지 않으므로 네트워크 에이전트의 데이터를 수락하고 나중에 중앙 관리 서버로 전달할 수 없습니다. 네트워크 에이전트가 연결 게이트웨이를 통해 중앙 관리 서버에 연결을 시도하지만 연결 게이트웨이가 중앙 관리 서버에 연결할 수 없는 경우 네트워크 에이전트는 이를 중앙 관리 서버에 접근할 수 없는 것으로 인식합니다. 모든 데이터는 연결 게이트웨이가 아닌 네트워크 에이전트에 저장됩니다.

  연결 게이트웨이는 다른 연결 게이트웨이를 통해 중앙 관리 서버에 연결할 수 없습니다. 즉, 네트워크 에이전트는 동시에 연결 게이트웨이가 될 수 없고 연결 게이트웨이를 사용하여 중앙 관리 서버에 연결할 수 없습니다.

  모든 연결 게이트웨이는 중앙 관리 서버 속성의 배포 지점 목록에 포함됩니다.

- 네트워크 내에서 연결 게이트웨이를 사용할 수도 있습니다. 예를 들어, 자동으로 할당된 배포 지점도 자체 범위에서 연결 게이트웨이가 됩니다. 그러나 내부 네트워크 내에서 연결 게이트웨이는 많은 이점을 제공하지 않습니다. 중앙 관리 서버에서 수신하는 네트워크의 연결 수를 줄이지만 들어오는 데이터의 양을 줄이지는 않습니다. 연결 게이트웨이가 없어도 모든 기기를 중앙 관리 서버에 연결할 수 있습니다.

주요 설치 시나리오

이 시나리오에서는 중앙 관리 서버를 배포하고 네트워크 기기에 네트워크 에이전트 및 보안 애플리케이션을 설치하는 것을 안내합니다. 이 시나리오는 애플리케이션을 더 자세히 살펴 보고 추가 작업을 위해 애플리케이션을 설치할 때 사용할 수 있습니다.

Kaspersky Security Center의 설치 및 배포는 다음 단계로 구성됩니다.

1. 준비 작업
2. 중앙 관리 서버 기기에 Kaspersky Security Center 및 Kaspersky 보안 제품 설치
3. Kaspersky 보안 제품을 클라이언트 기기에 중앙 집중식 배포

클라우드 환경에 Kaspersky Security Center를 배포하고 서비스 공급업체를 위해 Kaspersky Security Center를 배포하는 방법은 해당 도움말 섹션에 설명되어 있습니다.

중앙 관리 서버 설치에 적어도 한 시간을 할당하고 전체 시나리오 완료를 위해 최소 하루 이상의 작업 시간을 할당할 것을 권장합니다. Kaspersky Security for Windows Server 또는 Kaspersky Endpoint Security 같은 보안 제품을 Kaspersky Security Center 중앙 관리 서버 역할을 할 기기에 설치하는 것도 권장합니다.

이 시나리오 단계를 완료하면 다음과 같은 방법으로 조직 네트워크에 보호 기능이 배포됩니다.

- 중앙 관리 서버에 대한 DBMS가 설치됩니다.
- Kaspersky Security Center 중앙 관리 서버가 설치됩니다.
- 필요한 모든 정책과 작업이 만들어지고 정책과 작업의 기본 설정이 지정됩니다.
- 보안 제품(예: Kaspersky Endpoint Security for Windows)과 네트워크 에이전트가 관리 중인 기기에 설치됩니다.
- 관리 그룹이 생성됩니다(계층 구조로 결합될 수 있음).

- 필요한 경우 모바일 기기 보호 기능이 배포됩니다.
- 필요한 경우 배포 지점이 할당됩니다.

Kaspersky Security Center 설치는 다음 단계로 진행됩니다:

준비 작업

1 필요한 파일 가져오기

Kaspersky Security Center용 라이센스 키(활성화코드) 또는 Kaspersky 보안 애플리케이션용 라이센스 키(활성화코드)가 있는지 확인합니다.

공급 업체로부터 받은 압축 파일을 압축 해제합니다. 이 아카이브에는 라이센스 키(키 파일)와 활성화 코드, 각 라이센스 키로 활성화될 수 있는 Kaspersky 애플리케이션 목록이 포함되어 있습니다.

먼저 Kaspersky Security Center를 사용해보려면 Kaspersky 웹 사이트에서 30일 무료 평가판을 받을 수 있습니다.

Kaspersky Security Center에 포함되지 않은 Kaspersky 보안 애플리케이션의 라이센스에 대한 자세한 정보는 해당 애플리케이션의 문서를 참조하십시오.

2 조직 보호를 위한 조직도 선택

Kaspersky Security Center 구성 요소에 대해 더 알아 보기. 조직에 가장 적합한 보호 구조와 네트워크 구성을 선택합니다. (네트워크가 분산되어 있다면,) 통신 채널 처리 성능과 네트워크 구성에 따라 사용할 중앙 관리 서버의 수와 여러 사무실에 중앙 관리 서버를 배포할 방법을 정의합니다.

다양한 운영 조건에서 최적의 성능을 유지하려면 네트워크에 있는 기기 수, 네트워크 토폴로지 및 필요한 Kaspersky Security Center 기능을 고려하십시오. (자세한 내용은 Kaspersky Security Center 사이징 가이드를 참조하십시오).

조직에서 중앙 관리 서버 계층 구조를 사용할지 여부를 정의합니다. 이렇게 하려면 모든 클라이언트 기기를 간편하게 단일 중앙 관리 서버로 관리할 수 있는지, 아니면 중앙 관리 서버의 계층 구조를 작성해야 하는지를 평가해야 합니다. 보호해야 하는 조직의 조직 구조와 동일한 중앙 관리 서버 계층 구조를 작성해야 할 수도 있습니다.

모바일 기기를 보호하려면 iOS MDM 서버 구성에 필요한 모든 필수 작업을 수행합니다.

중앙 관리 서버로 선택한 기기와 관리 콘솔 설치를 위해 선택한 기기가 모두 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인합니다.

3 사용자 지정 인증서 사용 준비

조직의 공개 키 인프라(PKI)에 따라 특정 인증 기관(CA)에서 발급한 사용자 지정 인증서를 사용해야 하는 경우 해당 인증서를 준비하고 모든 요구 사항을 충족하는지 확인합니다.

4 Kaspersky Security Center 라이센싱 준비

모바일 기기 관리, SIEM 시스템과 통합 또는 취약점 및 패치 관리를 지원하는 Kaspersky Security Center 버전을 사용하려면 애플리케이션 라이센스 적용을 위한 키 파일이나 활성화코드가 있는지 확인합니다.

5 관리 중인 보안 제품 라이센싱 준비

Kaspersky 보호 제품 배포 중에 Kaspersky Security Center를 통해 관리하려는 애플리케이션에 대한 활성 라이센스 키를 제공해야 합니다(관리 가능한 보안 애플리케이션 목록 참조). 보안 애플리케이션의 라이센싱에 대한 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.

6 중앙 관리 서버 및 DBMS의 하드웨어 구성 선택

네트워크에 있는 기기 개수를 고려하여 중앙 관리 서버 및 DBMS의 하드웨어 구성을 계획합니다.

7 DBMS 선택

DBMS 선택 시에는 이 중앙 관리 서버가 관리하는 관리 중인 기기의 수를 고려합니다. 네트워크에 10,000 대 미만의 기기가 있고 그 수를 늘릴 계획이 없다면, SQL Express 또는 MySQL과 같은 무료 DBMS를 선택하고 같은 기기에 중앙 관리 서버를 설치할 수 있습니다. 또는 최대 20,000개의 기기를 관리할 수 있는 MariaDB DBMS를 선택할 수도 있습니다. 네트워크에 10,000 대 이상의 기기가 있거나 그 수만큼 네트워크를 확장하려는 경우 유료 SQL DBMS를 선택하고 전용 기기에 DBMS를 설치하는 것이 좋습니다. 유료 DBMS는 여러 중앙 관리 서버에서 사용할 수 있으며 무료 DBMS는 하나의 서버에서만 사용할 수 있습니다.

SQL Server DBMS를 선택하면 데이터베이스에 저장된 데이터를 MySQL, MariaDB 또는 Azure SQL DBMS로 마이그레이션할 수 있습니다. 마이그레이션하려면 데이터를 백업하고 새 DBMS로 복원하십시오.

8 DBMS 설치 및 데이터베이스 생성

DBMS 작업에 필요한 계정에 대해 자세히 알아보고 DBMS를 설치합니다.

설치 전에 지원하는 DBMS를 선택합니다. PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL, MariaDB 등을 선택할 수 있습니다.

선택한 DBMS를 설치하는 방법에 대한 정보는 해당 설명서를 참조하십시오.

MariaDB, MySQL, PostgreSQL, Postgres Pro 설치 시, 권장 설정을 사용하여 DBMS가 제대로 작동하는지 확인하십시오.

DBMS의 설정은 중앙 관리 서버 설치 중에 필요하므로 적어서 보관해 둡니다. 이러한 설정으로는 SQL Server 이름, SQL Server에 연결하는 데 사용되는 포트 번호, SQL Server 접근용 계정 이름/암호가 있습니다.

> PostgreSQL 또는 Postgres Pro DBMS 설치 시, 슈퍼유저의 암호를 지정했는지 확인하십시오. 암호를 지정하지 않으면 중앙 관리 서버가 데이터베이스에 연결하지 못할 수 있습니다.

기본적으로 Kaspersky Security Center 설치 프로그램은 중앙 관리 서버 정보를 저장하기 위한 데이터베이스를 생성하지만 이 데이터베이스를 생성하지 않고 다른 데이터베이스를 대신 사용할 수 있습니다. 이 경우 데이터베이스를 미리 생성했으며 데이터베이스 이름을 알고 있어야 합니다. 또한 중앙 관리 서버가 이 데이터베이스에 액세스하는 데 사용할 계정에 데이터베이스에 대한 db_owner 역할이 있어야 합니다.

필요할 경우 더 자세한 내용 확인을 위해 사용자의 DBMS 관리자에게 문의해 주십시오.

9 포트 구성

선택한 보안 구조에 따라 구성 요소 간의 상호 작용을 위해 필요한 모든 포트가 열려 있는지 확인하십시오.

인터넷을 통해 중앙 관리 서버에 접근하는 기능을 제공해야 하는 경우 네트워크 구성에 따라 포트를 구성하고 연결 설정을 지정합니다.

10 계정 확인

Kaspersky Security Center 중앙 관리 서버의 성공적인 설치와 기기에 추가 보호 기능을 배포하는 데 필요한 모든 로컬 관리자 권한이 있는지 확인합니다. 클라이언트 기기에 대한 로컬 관리자 권한은 해당 기기에 네트워크 에이전트를 설치할 때 필요합니다. 네트워크 에이전트가 설치된 이후에는 기기의 관리자 권한을 가진 계정을 사용하지 않고도 기기에 원격으로 애플리케이션을 설치할 수 있습니다.

기본적으로 중앙 관리 서버 설치를 위해 선택된 기기에 Kaspersky Security Center 설치 프로그램은 중앙 관리 서버와 Kaspersky Security Center 서비스가 실행될 세 개의 로컬 계정을 만듭니다:

- KL-AK-*: 중앙 관리 서버 서비스 계정
- NT Service/KSC*: 중앙 관리 서버 풀의 기타 서비스용 계정
- KlPxeUser: 운영 체제 배포용 계정

중앙 관리 서버 서비스 및 기타 서비스에 대한 계정을 만드는 것을 선택할 수 있습니다. Failover 클러스터에 중앙 관리 서버를 설치할 계획이거나 다른 이유로 로컬 계정 대신 도메인 계정을 사용할 계획인 경우 도메인 계정과 같은 것 대신에 기존 계정을 사용합니다. 이 경우 중앙 관리 서버와 Kaspersky Security Center 서비스를 실행하기 위한 계정이 생성되고 다른 권한이 없는지, 또한 DBMS에 접근하는 데 필요한 모든 권한이 있는지 확인하시기 바랍니다. (Kaspersky Security Center를 통해 기기에운영 체제를 배포하려는 경우 계정 생성을 선택하지 마십시오.)

중앙 관리 서버 기기에 Kaspersky Security Center 및 Kaspersky 보안 제품 설치

1 중앙 관리 서버, 관리 콘솔, Kaspersky Security Center 웹 콘솔, 보안 제품 관리 플러그인 설치

Kaspersky 웹 사이트에서 Kaspersky Security Center를 다운로드하십시오. 전체 패키지, 웹 콘솔만 또는 관리 콘솔만 다운로드할 수 있습니다.

선택한 기기(또는 여러 기기, 여러 중앙 관리 서버를 사용해야 할 경우)에 중앙 관리 서버를 설치합니다. 중앙 관리 서버의 표준 또는 사용자 지정 설치를 선택할 수 있습니다. 관리 콘솔은 중앙 관리 서버와 함께 설치됩니다. 도메인 컨트롤러 대신 전용 서버에 중앙 관리 서버를 설치하는 것이 좋습니다.

소규모 영역에서 작동 방식을 테스트하는 등 Kaspersky Security Center를 시험적으로 사용해 보려는 경우 표준 설치를 선택하는 것이 좋습니다. 표준 설치 시에는 데이터베이스만 구성합니다. Kaspersky 애플리케이션에 대한 기본 관리 플러그인 세트만 설치할 수도 있습니다. Kaspersky Security Center로 작업을 이미 해 본 적이 있는 경우 표준 설치를 사용할 수도 있습니다. 즉, 사용자는 표준 설치 후 모든 관련 설정을 지정하는 방법을 알고 있기 때문입니다.

사용자 지정 설치는 공유 폴더 경로, 계정, 중앙 관리 서버 연결용 포트, 데이터베이스 설정 등의 Kaspersky Security Center 설정을 수정하고자 할 때 사용하기를 권장합니다. 사용자 지정 설치를 선택하는 경우 설치할 Kaspersky 관리 플러그인을 지정할 수 있습니다. 필요하다면 숨김 모드로 사용자 지정 설치를 시작할 수 있습니다.

관리 콘솔과 네트워크 에이전트의 서버 버전은 중앙 관리 서버와 함께 설치됩니다. 설치 중에 Kaspersky Security Center 웹 콘솔 설치를 선택할 수도 있습니다.

필요하다면, 관리자 워크스테이션에 별도로 관리 콘솔을 설치하거나 Kaspersky Security Center 웹 콘솔을 설치하여 네트워크를 통해 중앙 관리 서버를 관리할 수 있습니다.

2 초기 설치 및 라이센싱

중앙 관리 서버 설치가 완료되면 중앙 관리 서버에 처음 연결될 때 빠른 시작 마법사가 자동으로 시작됩니다. 기존 요구 사항에 따라 중앙 관리 서버의 초기 구성을 수행합니다. 초기 구성 단계 중에 마법사는 기본 설정을 사용하여 보호 기능을 배포하는 데 필요한 정책과 작업을 만듭니다. 그러나 기본 설정으로는 조직의 요구를 가장 효율적으로 충족하지 못할 수도 있습니다. 필요한 경우 정책과 작업의 설정을 편집할 수 있습니다(클라이언트 조직의 네트워크에 보호 구성, 시나리오: 네트워크 보호 구성).

기본 기능 이외의 기능을 사용하려는 경우 이 애플리케이션에 라이센스를 할당합니다. 빠른 시작 마법사의 단계 중 하나에서 이 작업을 수행할 수 있습니다.

3 중앙 관리 서버 설치 확인

이전 단계가 모두 완료되면 중앙 관리 서버가 설치되고 사용할 준비가 됩니다.

관리 콘솔이 실행 중인지 확인하고 관리 콘솔을 통해 중앙 관리 서버에 연결할 수 있는지 확인합니다. 또한 Kaspersky Endpoint Security에 대한 정책(콘솔 트리의 **작업** 폴더에 있음)과 함께 중앙 관리 서버 작업의 저장소에 대한 다운로드 업데이트를 사용할 수 있는지 확인하십시오(콘솔 트리의 **정책** 폴더에 있음).

점검이 완료되면 아래 단계를 진행합니다.

Kaspersky 보안 제품을 클라이언트 기기에 중앙 집중식 배포

1 네트워크에 연결된 기기 발견

이 단계는 빠른 시작 마법사의 한 부분입니다. 수동으로 기기 발견을 시작할 수도 있습니다. Kaspersky Security Center는 네트워크에서 탐지된 모든 기기의 주소와 이름을 수신합니다. 그러면 Kaspersky Security Center를 사용하여 탐지된 기기에 Kaspersky 애플리케이션 및 다른 공급업체의 소프트웨어를 설치할 수 있습니다. Kaspersky Security Center는 정기적으로 기기 발견을 시작합니다. 이는 기업 네트워크에 새 인스턴스가 있을 경우 자동으로 탐지한다는 뜻입니다.

2 네트워크에 연결된 기기에 네트워크 에이전트 및 보안 제품 설치

조직의 네트워크에 보호를 배포하려면(클라이언트 조직의 네트워크에 보호 구성, 시나리오: 네트워크 보호 구성) 기기 발견 중에 중앙 관리 서버에서 탐지한 기기에 네트워크 에이전트 및 보안 제품(예: Kaspersky Endpoint Security)을 설치해야 합니다.

보안 제품은 기기를 위협하는 바이러스 및/또는 기타 프로그램으로부터 기기를 보호합니다. 네트워크 에이전트는 기기와 중앙 관리 서버가 서로 통신하도록 합니다. 네트워크 에이전트 설정은 기본적으로 자동 구성됩니다.

원하는 경우 응답 파일을 포함하거나 응답 파일을 제외한 채로 숨김 모드에서 네트워크 에이전트를 설치할 수 있습니다.

네트워크에 연결된 기기에 보안 제품 및 네트워크 에이전트 설치를 시작하기 전에 해당 기기가 접근 가능한 상태인지(켜져 있는지) 확인하십시오. 사용자는 가상 컴퓨터와 실제 기기에 네트워크 에이전트를 설치할 수 있습니다.

보안 제품과 네트워크 에이전트는 원격으로 또는 로컬로 설치할 수 있습니다.

원격 설치 – 보호 배포 마법사를 사용하여 중앙 관리 서버가 조직 네트워크에서 탐지한 기기에 보안 제품(예: Kaspersky Endpoint Security for Windows) 및 네트워크 에이전트를 원격으로 설치할 수 있습니다. 일반적으로는 원격 설치 작업을 통해 대다수 기기에 보호 제품을 정상 배포할 수 있습니다. 그러나 기기가 꺼져 있거나 다른 이유로 접근할 수 없는 경우 일부 기기에서 오류가 반환될 수 있습니다. 이 경우 기기에 수동으로 연결하고 로컬 설치를 사용하는 것이 좋습니다.

로컬 설치 - 원격 설치 작업을 사용하여 보호 기능을 배포할 수 없는 네트워크 기기에서 사용됩니다. 이러한 기기에 보호 제품을 설치하려면 해당 기기에서 로컬로 실행할 수 있는 독립 실행형 설치 패키지를 만듭니다.

Linux 및 macOS 운영 체제를 실행하는 기기에 네트워크 에이전트를 설치하는 방법은 Kaspersky Endpoint Security for Linux 및 Kaspersky Endpoint Security for Mac 설명서에 설명되어 있습니다. Linux 및 macOS 운영 체제를 실행하는 기기는 Windows를 실행하는 기기보다 더 취약하나 보안 애플리케이션을 설치하는 것이 좋습니다.

설치 이후에 관리 중인 기기에 해당 보안 제품이 설치되었는지를 확인하십시오. Kaspersky 애플리케이션 버전 리포트를 실행하여 해당 결과를 확인합니다.

3 클라이언트 기기에 라이센스 키 배포

클라이언트 기기에서 관리 중인 보안 제품을 활성화하기 위해 해당 기기에 라이센스 키를 배포합니다.

4 모바일 기기 보호 구성

이 단계는 빠른 시작 마법사의 한 부분입니다.

기업 모바일 기기를 관리하려면 필요한 준비 단계를 수행하고 모바일 기기 관리를 배포하십시오.

5 관리 그룹 구조 생성

경우에 따라서는 네트워크 기기에 보호 기능을 가장 편리한 방식으로 배포하려면 조직 구조를 고려하여 전체 기기 풀을 관리 그룹으로 분할해야 할 수도 있습니다. 그룹 간에 기기를 배포하는 이동 규칙을 만들거나 기기를 수동으로 배포할 수 있습니다. 그리고 나면 관리 그룹에 대해 그룹 작업을 할당하고, 정책 범위를 정의하고, 배포 지점을 할당할 수 있습니다.

모든 관리 중인 기기가 적절한 관리 그룹에 올바르게 할당되었으며 네트워크에 미할당 기기가 더 이상 없는지 확인합니다.

6 배포 지점 할당

Kaspersky Security Center는 배포 지점을 관리 그룹에 자동으로 할당하지만 필요한 경우 수동으로 할당할 수 있습니다. 처리 속도가 낮은 채널을 통해 통신을 하는 기기 또는 기기 그룹에 대한 접근 권한을 중앙 관리 서버에 제공하기 위한 분산 구조가 포함된 네트워크와 대규모 네트워크에서는 중앙 관리 서버의 부하를 줄이기 위해 배포 지점을 사용하는 것이 좋습니다. Windows를 실행하는 기기와 Linux를 실행하는 기기를 배포 지점으로 사용할 수 있습니다.

Kaspersky Security Center의 사용 포트

아래 표에는 중앙 관리 서버와 클라이언트 기기에서 사용하는 기본 포트가 나와 있습니다. 원하는 경우 기본 포트 번호를 변경할 수 있습니다.

중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치한다면, 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(예: MySQL Server는 3306 포트, Microsoft SQL Server는 1433 포트, PostgreSQL 및 Postgres Pro는 5432 포트). 관련 정보는 DBMS 설명서를 참조하십시오.

중앙 관리 서버에서 사용하는 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
8060	klcsweb	TCP	게시된 설치 패키지를 클라이언트 기기로 전송	설치 패키지 게시 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 내 중앙 관리 서버 속성 창의 **웹 서버** 섹션에서 기본 포트 번호를 변경할 수 있습니다. 이 포트는 선택 사항입니다. 보안상의 이유로 8061 TCP 포트를 사용하는 것이 좋습니다.
8061	klcsweb	TCP (TLS)	게시된 설치 패키지를 클라이언트 기기로 전송	설치 패키지 게시 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 내 중앙 관리 서버 속성 창의 **웹 서버** 섹션에서 기본 포트 번호를 변경할 수 있습니다.
13000	klserver	TCP (TLS)	네트워크 에이전트와 보조 중앙 관리 서버로부터 연결을 수신합니다. 또한 기본 중앙 관리 서버에서의 연결을 수신하기 위해 보조 중앙 관리 서버에도 사용됩니다(예: 보조 중앙 관리 서버가 DMZ에 있는 경우)	클라이언트 기기 및 보조 중앙 관리 서버 관리 연결 포트를 구성할 때 네트워크 에이전트에서 연결을 수신하기 위한 기본 포트 번호를 변경할 수 있습니다. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 중앙 관리 서버의 계층 구조를 생성할 때 보조 중앙 관리 서버에서 연결을 수신하기 위한 기본 포트 번호를 변경할 수 있습니다.
13000	klserver	UDP	네트워크 에이전트에서 꺼진 기기에 대한 정보 수신	클라이언트 기기 관리 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 네트워크 에이전트 정책 설정에서 기본 포트 번호를 변경할 수 있습니다.
13291	klserver	TCP (TLS)	관리 콘솔에서 중앙 관리 서버로의 연결 구성 가져오기	중앙 관리 서버 관리 관리 콘솔의 중앙 관리 서버 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
13299	klserver	TCP (TLS)	Kaspersky Security Center 웹 콘솔에서 중앙 관리 서버로의 연결 수신; OpenAPI를 통한 중앙 관리 서버로의 연결 수신	Kaspersky Security Center 웹 콘솔, OpenAPI. 기본 포트 번호는 관리 콘솔의 중앙 관리 서버 속성 창(**중앙 관리 서버 연결 설정** 섹션 → **연결 포트** 하위 섹션)에서 변경하거나 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 중앙 관리 서버의 계층을 만들 때 변경할 수 있습니다.
14000	klserver	TCP	네트워크 에이전트에서 연결 수신	클라이언트 기기 관리 Kaspersky Security Center를 설치하는 동안 연결 포트를 구성하거나 클라이언트 기기를 중앙 관리 서버에 수동으로 연결할 때 기본 포트 번호를 변경할 수 있습니다. 이 포트는 선택 사항입니다. 보안상의 이유로 13000 TCP 포트를 사용하는 것이 좋습니다.

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
13111(KSN 프록시 서비스가 기기에서 실행되는 경우에만)	ksnproxy	TCP	관리 중인 기기에서 KSN 프록시 서버로의 요청 수신	KSN 프록시 서버 중앙 관리 서버 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
15111(KSN 프록시 서비스가 기기에서 실행되는 경우에만)	ksnproxy	UDP	관리 중인 기기에서 KSN 프록시 서버로의 요청 수신	KSN 프록시 서버 중앙 관리 서버 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
17000	klactprx	TCP (TLS)	관리 중인 기기에서 애플리케이션 활성화를 위한 연결 수신(모바일 기기는 제외)	모바일이 아닌 기기에서 활성화 코드로 Kaspersky 애플리케이션을 활성화하는 데 사용하는 활성화 프록시 서버입니다. 중앙 관리 서버 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
17100(모바일 기기를 관리하는 경우에만)	klactprx	TCP (TLS)	모바일 기기에서 애플리케이션 활성화를 위한 연결 수신	모바일 기기용 활성화 프록시 서버 중앙 관리 서버 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
19170	klserver	HTTPS (TLS)	klsctunnel 유틸리티를 사용하여 관리 중인 기기에 터널링 연결	Kaspersky Security Center 웹 콘솔을 사용하여 관리 중인 기기에 원격 연결 기본 포트 번호는 관리 콘솔의 중앙 관리 서버 속성 창(**중앙 관리 서버 연결 설정** 섹션 → **연결 포트** 하위 섹션 → **Kaspersky Security Center 웹 콘솔용 RDP 포트 열기** 옵션)에서만 변경할 수 있습니다.
13292(모바일 기기를 관리하는 경우에만)	klserver	TCP (TLS)	모바일 기기에서 연결 수신	모바일 기기 관리 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 중앙 관리 서버 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
13294(모바일 기기를 관리하는 경우에만)	klserver	TCP (TLS)	UEFI 보호 기기에서 연결 수신	UEFI 보호 클라이언트 기기 관리 기본 포트 번호는 모바일 기기를 연결할 때 변경하거나 나중에 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 중앙 관리 서버 속성 창(**중앙 관리 서버 연결 설정** 섹션 → **연결 포트** 하위 섹션)에서 변경할 수 있습니다.
13296	klserver	TCP (TLS)	Prometheus에 대한 Kaspersky Security Center 메트릭 게시	Prometheus에서 추가로 얻을 Kaspersky Security Center 메트릭을 게시합니다. 다음 링크를 통해 메트릭을 확인할 수 있습니다: https://<서버 주소>:13296/metrics. <서버 주소>에서 중앙 관리 서버의 IP 주소 또는 도메인 이름을 지정합니다. 관리 콘솔의 중앙 관리 서버 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
30522, 30523(localhost 인터페이스의 포트)	klnagent	TCP	FileTransferBridge 구성 요소를 사용하여 중앙 관리 서버에서 Kaspersky 애플리케이션 업데이트 수신	Kaspersky 애플리케이션 업데이트를 수신하는 중앙 관리 서버 기기입니다.

아래 표에는 iOS MDM 서버에서 열어야 하는 포트(모바일 기기에서 관리하는 경우에만)가 나와 있습니다.

iOS MDM 서버의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
443	kliosmdmservicesrv	TCP (TLS)	iOS 모바일 기기에서 연결 수신	모바일 기기 관리 iOS MDM 서버를 설치할 때 기본 포트 번호를 변경할 수 있습니다.

아래 표에는 Kaspersky Security Center 웹 콘솔 서버에서 사용하는 포트가 나와 있습니다. 중앙 관리 서버가 설치되어 있는 동일한 기기이거나 다른 기기일 수 있습니다.

Kaspersky Security Center 웹 콘솔 서버의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
8080	Node.js: 서버 측 JavaScript	TCP (TLS)	브라우저에서 Kaspersky Security Center 웹 콘솔로의 연결 수신	Kaspersky Security Center 웹 콘솔. Linux 플랫폼 또는 Windows를 실행하는 기기에 Kaspersky Security Center 웹 콘솔을 설치할 때는 기본 포트 번호를 변경할 수 있습니다. Linux ALT 운영 체제에 Kaspersky Security Center 웹 콘솔을 설치할 시, 운영 체제에서 포트 8080을 사용하므로 8080 이외의 포트 번호를 지정해야 합니다.

아래 표에는 네트워크 에이전트가 설치된 관리 중인 기기에서 사용하는 포트가 나와 있습니다.

네트워크 에이전트의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
15000	klnagent	UDP	중앙 관리 서버 또는 배포 지점에서 네트워크 에이전트로의 관리 신호	클라이언트 기기 관리 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 네트워크 에이전트 정책 설정에서 기본 포트 번호를 변경할 수 있습니다.
15000	klnagent	UDP 브로드캐스트	동일한 브로드캐스팅 도메인 내의 기타 네트워크 에이전트에 관한 데이터 가져오기(이 데이터는 이후 중앙 관리 서버로 전송됨)	업데이트 및 설치 패키지 전달
15001	klnagent	UDP	배포 지점에서 멀티캐스트 요청 수신(사용 중일 시)	배포 지점에서 업데이트 및 설치 패키지 수신. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 배포 지점 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
30522, 30523(localhost 인터페이스의 포트)	klnagent	TCP	FileTransferBridge 구성 요소를 사용하여 중앙 관리 서버에서 Kaspersky 애플리케이션 업데이트 수신	데이터베이스 업데이트 경로로 지정된 중앙 관리 서버에서 보내는 Kaspersky 애플리케이션 업데이트를 수신하는 관리 중인 기기.
161	klnagent	SNMP	네트워크로 연결된 기기 모니터링 및 검색.	기기 검색 가능성.

klnagent 프로세스는 엔드포인트 운영 체제의 동적 포트 범위에서 사용 가능한 포트를 요청할 수도 있습니다. 이러한 포트는 운영 체제에서 klnagent 프로세스에 자동 할당되므로, klnagent 프로세스가 다른 소프트웨어에서 사용하는 일부 포트를 사용할 수 있습니다. klnagent 프로세스가 해당 소프트웨어 작업에 영향을 미친다면, 이 소프트웨어의 포트 설정을 변경하거나 운영 체제의 기본 동적 포트 범위를 변경하여 영향을 받는 소프트웨어에서 사용하는 포트를 제외하십시오.

또한, Kaspersky Security Center와 타사 소프트웨어의 호환성에 대한 권장 사항은 참조용으로만 설명되며 새 버전의 타사 소프트웨어에는 적용되지 않을 수 있습니다. 설명된 포트 구성 권장 사항은 기술 지원 및 모범 사례의 경험을 기반으로 합니다.

아래 표에는 배포 지점 역할을 하는 네트워크 에이전트가 있는 관리 중인 기기에서 사용하는 포트가 나와 있습니다. 네트워크 에이전트에서 사용하는 포트 외에, 목록의 포트도 배포 지점 기기에서 사용됩니다(위 표 참조).

배포 지점으로 작동하는 네트워크 에이전트의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
13000	klnagent	TCP (TLS)	배포 지점이 DMZ의 연결 게이트웨이 역할을 할 때 네트워크 에이전트 및 Kaspersky Security Center로부터 연결을 수신합니다. 중앙 관리 서버가 설치된 기기를 배포 지점으로 지정하면 SSL 연결에 기본적으로 포트 13000 대신 포트 13001이 사용됩니다.	클라이언트 기기 관리, 업데이트 및 설치 패키지 전달. 자세한 내용은 중앙 관리 서버, 네트워크 세그먼트의 연결 게이트웨이 및 클라이언트 기기 항목을 참조하십시오. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 배포 지점 속성 창에서 기본 포트 번호를 변경할 수 있습니다.

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
13111(KSN 프록시 서비스가 기기에서 실행되는 경우에만)	ksnproxy	TCP	관리 중인 기기에서 KSN 프록시 서버로의 요청 수신	KSN 프록시 서버 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 배포 지점 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
15111(KSN 프록시 서비스가 기기에서 실행되는 경우에만)	ksnproxy	UDP	관리 중인 기기에서 KSN 프록시 서버로의 요청 수신	KSN 프록시 서버 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 배포 지점 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
17111(KSN 프록시 서비스가 기기에서 실행되는 경우에만)	ksnproxy	HTTPS	관리 중인 기기에서 KSN 프록시 서버로의 요청 수신	KSN 프록시 서버 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 배포 지점 속성 창에서 기본 포트 번호를 변경할 수 있습니다.
13295(배포 지점을 푸시 서버로 사용하는 경우에만)	klnagent	TCP (TLS)	클라이언트 기기에서 연결 수신	푸시 서버. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 배포 지점 속성 창에서 기본 포트 번호를 변경할 수 있습니다.

아래 표에는 도메인 컨트롤러 기기에서 사용하는 포트가 나와 있습니다.

도메인 컨트롤러 기기에서 사용하는 포트

포트 번호	프로토콜	포트 용도	범위
389	TCP 또는 UDP를 통한 LDAP	LDAP 서버에 연결	도메인 컨트롤러 검색
636	TLS를 통한 LDAP	LDAP 서버에 연결	도메인 컨트롤러 검색

Kaspersky Security Center 작업용 인증서

이 섹션에는 Kaspersky Security Center 인증서에 대한 정보와 중앙 관리 서버용 사용자 지정 인증서를 발급하는 방법이 설명되어 있습니다.

Kaspersky Security Center 인증서 정보

Kaspersky Security Center는 다음 유형의 인증서를 사용하여 애플리케이션 구성 요소 간 보안 상호 작용을 구현합니다.

- 중앙 관리 서버 인증서
- 모바일 인증서
- iOS MDM 서버 인증서
- Kaspersky Security Center 웹 서버 인증서
- Kaspersky Security Center 웹 콘솔 인증서

기본적으로 Kaspersky Security Center는 자체 서명된 인증서(즉, Kaspersky Security Center 자체적으로 발행한 인증서)를 사용하지만 조직의 네트워크 요구 사항을 보다 확실히 충족하고 보안 표준을 준수하기 위해 사용자 지정 인증서로 교체할 수도 있습니다. 중앙 관리 서버가 사용자 지정 인증서가 모든 해당 요구 사항을 준수하는지 검증하고 나면 이 인증서는 자체 서명된 인증서와 같은 기능 범위를 가정합니다. 유일한 차이점은 사용자 지정 인증서는 만료 시 자동으로 재발행되지 않는다는 점입니다. 인증서 유형에 따라 인증서를 klsetsrvcert 유틸리티 또는 관리 콘솔의 중앙 관리 서버 속성 섹션을 통해 사용자 지정 인증서로 교체할 수 있습니다. Klsetsrvcert 유틸리티를 사용하는 경우 다음 값 중 하나를 사용하여 인증서 유형을 지정해야 합니다.

- C—포트 13000 및 13291용 공통 인증서.
- CR—포트 13000 및 13291용 공통 예약 인증서.
- M—포트 13292용 모바일 인증서.
- MR—포트 13292용 모바일 예약 인증서.
- MCA—자동 생성된 사용자 인증서용 모바일 인증 기관.

klsetsrvcert 유틸리티를 다운로드할 필요가 없습니다. Kaspersky Security Center 배포 키트에 포함되어 있습니다. 이 유틸리티는 이전 Kaspersky Security Center 버전과 호환되지 않습니다.

중앙 관리 서버 인증서의 최대 유효 기간은 397일 이하여야 합니다.

중앙 관리 서버 인증서

중앙 관리 서버 인증서는 중앙 관리 서버 인증, 그리고 중앙 관리 서버와 관리 중인 기기의 네트워크 에이전트 간이나 기본 중앙 관리 서버와 보조 중앙 관리 서버 간의 보안 상호 작용에 필요합니다. 관리 콘솔을 중앙 관리 서버에 처음으로 연결할 때에는 현재 중앙 관리 서버 인증서 사용을 확인하라는 메시지가 표시됩니다. 이 확인은 중앙 관리 서버 인증서를 교체할 때마다, 중앙 관리 서버를 재설치할 때마다, 그리고 보조 중앙 관리 서버를 기본 중앙 관리 서버에 연결할 때에도 필요합니다. 이 인증서를 공통("C")이라고 합니다.

중앙 관리 서버 구성 요소가 설치되면 공통("C") 인증서가 자동 생성됩니다. 인증서는 두 부분으로 구성됩니다.

- klserver.cer 파일; 기본적으로 중앙 관리 서버 구성 요소가 설치된 기기의 C:\ProgramData\KasperskyLab\adminkit\1093\cert 폴더에 있습니다.
- Windows 보호 저장소에 있는 비밀 키입니다.

공통 예약("CR") 인증서도 있습니다. Kaspersky Security Center는 공통 인증서가 만료되기 90일 전에 이 인증서를 자동 생성합니다. 이후에는 이 공통 예약 인증서를 사용하여 중앙 관리 서버 인증서를 원활하게 교체합니다. 일반 인증서가 만료 되려고 할 때 예약 인증서는 관리 중인 기기에 설치된 네트워크 에이전트 인스턴스와의 연결을 유지하는 데 사용됩니다. 이를 위해 이전 공통 인증서가 만료되기 24시간 전에 공통 예약 인증서가 자동으로 새 공통 인증서가 됩니다.

중앙 관리 서버를 데이터 손실 없이 한 기기에서 다른 기기로 옮기기 위해 다른 중앙 관리 서버 설정과 별도로 중앙 관리 서버 인증서를 백업해 둘 수도 있습니다.

모바일 인증서

모바일 인증서("M")는 모바일 기기에서 중앙 관리 서버를 인증하는 데 필요합니다. 빠른 시작 마법사의 해당 단계에서 모바일 인증서 사용을 구성합니다.

또한, 'MR'(모바일 예약) 인증서도 있습니다. 이 인증서는 모바일 인증서의 원활한 교체에 사용됩니다. Kaspersky Security Center는 공통 인증서가 만료되기 60일 전에 이 인증서를 자동 생성합니다. 모바일 인증서가 만료되려고 할 때 모바일 예약 인증서는 관리 중인 모바일 기기에 설치된 네트워크 에이전트 인스턴스와의 연결을 유지하는 데 사용됩니다. 이를 위해 이전 모바일 인증서가 만료되기 24시간 전에 모바일 예약 인증서가 자동으로 새 모바일 인증서가 됩니다.

연결 시나리오에서 모바일 기기에서 클라이언트 인증서를 사용해야 한다면(양방향 SSL 인증이 필요한 연결), 자동 생성된 사용자 인증서("MCA")용 인증서 기관을 통해 인증서를 생성할 수 있습니다. 또한, 빠른 시작 마법사를 통해 다른 인증 기관에서 발행한 사용자 지정 클라이언트 인증서를 사용할 수 있고, 조직의 도메인 공개 키 인프라(PKI) 통합을 사용하여 도메인 인증 기관을 통해 클라이언트 인증서를 발행할 수 있습니다.

iOS MDM 서버 인증서

IOS MDM 서버 인증서는 iOS 운영 체제를 실행하는 모바일 기기에서 중앙 관리 서버를 인증하는 데 필요합니다. 이 기기와의 상호 작용은 네트워크 에이전트와 무관한 Apple 모바일 기기 관리(MDM)를 통해 수행됩니다. 대신, 클라이언트 인증서를 포함하고 있는 특수 iOS MDM 프로필을 각 기기에 설치하여 양방향 SSL 인증을 활성화할 수 있습니다.

또한, 빠른 시작 마법사를 통해 다른 인증 기관에서 발행한 사용자 지정 클라이언트 인증서를 사용할 수 있고, 조직의 도메인 공개 키 인프라(PKI) 통합을 사용하여 도메인 인증 기관을 통해 클라이언트 인증서를 발행할 수 있습니다.

이 iOS MDM 프로필을 다운로드하면 클라이언트 인증서가 iOS 기기로 전송됩니다. iOS MDM 서버 클라이언트 인증서는 관리 중인 각 iOS 기기마다 고유합니다. 모든 iOS MDM 서버 클라이언트 인증서는 자동 생성된 사용자 인증서("MCA")용 인증 기관을 통해 생성합니다.

Kaspersky Security Center 웹 서버 인증서

Kaspersky Security Center 관리 서버의 구성 요소인 Kaspersky Security Center 웹 서버(이하 웹 서버)는 특수 유형의 인증서를 사용합니다. 이 인증서는 나중에 관리 중인 기기에 다운로드하는 네트워크 에이전트 설치 패키지를 게시하고 iOS MDM 프로필, iOS 앱 및 Kaspersky Security for Mobile 설치 패키지를 게시하는 데 필요합니다. 이를 위해 웹 서버는 다양한 인증서를 사용할 수 있습니다.

모바일 기기 지원이 비활성화되어 있는 경우 웹 서버는 우선순위에 따라 다음 인증서 중 하나를 사용합니다.

1. 관리 콘솔을 통해 수동으로 지정한 사용자 지정 웹 서버 인증서
2. 공통 중앙 관리 서버 인증서("C")

모바일 기기 지원이 활성화되어 있는 경우 웹 서버는 우선순위에 따라 다음 인증서 중 하나를 사용합니다.

1. 관리 콘솔을 통해 수동으로 지정한 사용자 지정 웹 서버 인증서
2. 사용자 지정 모바일 인증서
3. 자체 서명된 모바일 인증서("M")
4. 공통 중앙 관리 서버 인증서("C")

Kaspersky Security Center 웹 콘솔 인증서

Kaspersky Security Center 웹 콘솔(이하 웹 콘솔) 서버에는 자체 인증서가 있습니다. 웹 사이트를 열면 브라우저에서 연결을 신뢰할 수 있는지 확인합니다. 웹 콘솔 인증서를 사용하면 웹 콘솔을 인증할 수 있으며 브라우저와 웹 콘솔 간의 트래픽을 암호화하는 데 사용됩니다.

웹 콘솔을 열면 브라우저에서 웹 콘솔에 대한 연결이 비공개가 아니며 웹 콘솔 인증서가 유효하지 않다고 알릴 수 있습니다. 이 경고는 웹 콘솔 인증서가 자체 서명되고 Kaspersky Security Center에서 자동으로 생성되기 때문에 표시됩니다. 이 경고를 없애려면 다음 작업 중 하나를 수행할 수 있습니다.

- 웹 콘솔 인증서를 사용자 지정 인증서로 교체합니다(권장 옵션). 사용자의 인프라에서 신뢰할 수 있고 사용자 지정 인증서의 요구 사항을 충족하는 인증서를 만듭니다.
- 웹 콘솔 인증서를 신뢰할 수 있는 브라우저 인증서 목록에 추가합니다. 사용자 지정 인증서를 만들 수 없는 경우에만 이 옵션을 사용하는 것이 좋습니다.

중앙 관리 서버 인증서 정보

*중앙 관리 서버 인증서*에 따라 연결 시 중앙 관리 서버 인증 및 기기와의 데이터 교환, 두 가지 작업이 수행됩니다. 또한 인증서는 기본 중앙 관리 서버를 보조 중앙 관리 서버에 연결할 때 인증에도 사용됩니다.

Kaspersky에서 발급한 인증서

중앙 관리 서버 인증서는 중앙 관리 서버 구성 요소 설치 시 자동 생성되며, %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder 폴더에 저장됩니다.

인증서를 중앙 관리 서버 12.2 또는 이전 버전에서 생성했다면 중앙 관리 서버 인증서의 유효 기간은 5년입니다. 그 외에는 인증서 유효 기간이 397일로 제한됩니다. 현재 인증서 만료 날짜 90일 전에 중앙 관리 서버가 예약 인증서 형식으로 새 인증서를 생성합니다. 그 후에는 만료 날짜 1일 전에 현재 인증서가 새 인증서로 자동 교체됩니다. 클라이언트 기기의 모든 네트워크 에이전트는 새 인증서를 사용하여 중앙 관리 서버를 인증하도록 자동으로 재구성됩니다.

사용자 지정 인증서

필요한 경우 중앙 관리 서버용 사용자 지정 인증서를 할당할 수 있습니다. 기업의 기존 PKI를 더 효율적으로 통합하려는 경우나 인증서 필드의 사용자 지정 구성을 사용하려는 경우를 예로 들 수 있습니다.

중앙 관리 서버 인증서의 최대 유효 기간은 397일 이하여야 합니다.

인증서를 교체하면 이전에 SSL을 통해 중앙 관리 서버에 연결했던 모든 네트워크 에이전트의 연결이 끊기며 "중앙 관리 서버 인증 오류"가 반환됩니다. 이러한 오류를 방지하려면 인증서 교체 후 연결을 복원해야 합니다.

중앙 관리 서버 인증서를 분실한 경우, 이를 복구하기 위해 중앙 관리 서버 구성 요소를 다시 설치하고 데이터를 복원해야 합니다.

다른 브라우저에서 Kaspersky Security Center 웹 콘솔을 열고 중앙 관리 서버 속성 창에서 중앙 관리 서버 인증서 파일을 다운로드하면 다운로드한 파일의 이름이 달라집니다.

Kaspersky Security Center에서 사용되는 사용자 지정 인증서 요구 사항

아래 표는 Kaspersky Security Center의 여러 구성 요소에 대해 지정된 사용자 지정 인증서의 요구 사항을 보여줍니다.

Kaspersky Security Center 인증서의 요구 사항

인증서 유형	요구 사항	메모
공통 인증서, 공통 예약 인증서("C", "CR")	최소 키 길이: 2048. 기본 제한: • 경로 길이 제한: 없음 키 사용: • 전자 서명 • 인증서 서명 • 키 암호화 • CRL 서명 확장 키 사용(옵션): 서버 인증, 클라이언트 인증. 인증서에는 중앙 관리 서버 루프백 주소가 포함된 유효한 주체 대체 이름(SAN)을 포함해야 합니다. • IPv4의 경우: 127.0.0.1 • IPv6의 경우: 0:0:0:0:0:0:0:1	확장 키 사용 매개 변수는 선택 사항입니다. 경로 길이 제한 값은 "없음" 및 그 외의 정수일 수 있지만, 단 "1" 이상이어야 합니다.
모바일 인증서, 모바일 예약 인증서("M", "MR")	최소 키 길이: 2048. 기본 제한: • CA: 참 • 경로 길이 제한: 없음 키 사용: • 전자 서명 • 인증서 서명 • 키 암호화 • CRL 서명 확장 키 사용(선택 사항): 서버 인증.	확장 키 사용 매개 변수는 선택 사항입니다. 공통 인증서의 경로 길이 제한 값이 "1" 이상인 경우 경로 길이 제한 값은 "없음" 및 그 외의 정수일 수 있습니다.
자동 생성된 사용자 인증서용 인증서 CA("MCA")	최소 키 길이: 2048. 기본 제한: • CA: 참 • 경로 길이 제한: 없음 키 사용: • 전자 서명 • 인증서 서명 • 키 암호화 • CRL 서명 확장 키 사용(옵션): 서버 인증, 클라이언트 인증.	확장 키 사용 매개 변수는 선택 사항입니다. 공통 인증서의 경로 길이 제한 값이 "1" 이상인 경우 경로 길이 제한 값은 "없음" 및 그 외의 정수일 수 있습니다.
웹 서버 인증서	확장 키 사용: 서버 인증. 인증서가 지정된 PKCS #12 / PEM 컨테이너에 공개 키의 전체 체인이 포함되어 있습니다. 인증서의 주체 대체 이름(SAN)이 있습니다. 즉, `subjectAltName` 필드의 값이 유효합니다. 인증서가 서버 인증서에 부과된 브라우저의 유효한 요구 사항 및 CA/Browser Forum 의 현재 기본 요구 사항을 충족합니다.	—
Kaspersky Security Center 웹 콘솔 인증서	인증서가 지정된 PEM 컨테이너에 공개 키의 전체 체인이 포함되어 있습니다. 인증서의 주체 대체 이름(SAN)이 있습니다. 즉, `subjectAltName` 필드의 값이 유효합니다. 인증서가 서버 인증서에 대한 브라우저의 유효한 요구 사항 및 CA/Browser Forum 의 현재 기본 요구 사항을 충족합니다.	암호화된 인증서는 Kaspersky Security Center 웹 콘솔에서 지원되지 않습니다.

시나리오: 사용자 지정 중앙 관리 서버 인증서 지정

예를 들어, 기업의 기존 공개 키 인프라(PKI)와의 더 나은 통합을 위해 또는 인증서 필드의 사용자 정의 구성을 위해 사용자 정의 중앙 관리 서버 인증서를 할당할 수 있습니다. 따라서 중앙 관리 서버를 설치한 직후, 그리고 빠른 시작 마법사가 완료되기 전에 인증서를 교체하면 유용합니다.

중앙 관리 서버 인증서의 최대 유효 기간은 397일 이하여야 합니다.

필수 구성 요소

다음 조건을 충족해야 합니다.

- 새 인증서는 PKCS#12 형식으로 만들어야 합니다(조직의 PKI 사용 등.).
- 새 인증서의 경우 아래 표에 나열된 요구 사항을 충족해야 합니다.

  아래 표에서 "CA: 참" 요구 사항을 확인하십시오. 새 인증서를 신뢰할 수 있는 인증 기관(CA)에서 발행해야 한다는 의미입니다. 또한 새 인증서는 전체 신뢰 체인과 개인 키를 포함해야 하며, 이는 확장자가 pfx 또는 p12인 파일에 저장되어야 합니다.

중앙 관리 서버 인증서에 대한 요구 사항

인증서 유형	요구 사항
공통 인증서, 공통 예약 인증서 ("C", "CR")	최소 키 길이: 2048. 기본 제한: • 경로 길이 제한: 없음 경로 길이 제한 값은 "없음" 및 그 외의 정수일 수 있지만, 단 "1" 이상이어야 합니다. 키 사용: • 전자 서명 • 인증서 서명 • 키 암호화 • CRL 서명 확장 키 사용(EKU): 서버 인증, 클라이언트 인증. EKU는 선택 사항이지만 인증서에 EKU가 포함되어 있는 경우 서버 및 클라이언트 인증 데이터를 EKU에 지정해야 합니다. 인증서에 유효한 주체 대체 이름(SAN)을 포함해야 합니다. `subjectAltName` 필드는 중앙 관리 서버 루프백 주소를 포함해야 합니다. • IPv4의 경우: 127.0.0.1 • IPv6의 경우: 0:0:0:0:0:0:0:1
모바일 인증서, 모바일 예약 인증서 ("M", "MR")	최소 키 길이: 2048. 기본 제한: • CA: 참 • 경로 길이 제한: 없음 공통 인증서의 경로 길이 제한 값이 "1" 이상인 경우 경로 길이 제한 값은 "없음" 및 그 외의 정수일 수 있습니다. 키 사용: • 전자 서명 • 인증서 서명 • 키 암호화 • CRL 서명 확장 키 사용(EKU): 서버 인증. EKU는 선택 사항이지만 인증서에 EKU가 포함되어 있는 경우 EKU에 서버 인증 데이터를 지정해야 합니다.

인증서 유형	요구 사항
자동 생성된 사용자 인증서용 인증서 CA("MCA")	최소 키 길이: 2048. 기본 제한: • CA: 참 • 경로 길이 제한: 없음 공통 인증서의 경로 길이 제한 값이 "1" 이상인 경우 경로 길이 제한 값은 "없음" 및 그 외의 정수일 수 있습니다. 키 사용: • 전자 서명 • 인증서 서명 • 키 암호화 • CRL 서명 확장 키 사용(EKU): 클라이언트 인증. EKU는 선택 사항이지만 인증서에 EKU가 포함되어 있는 경우 EKU에 클라이언트 인증 데이터를 지정해야 합니다.

공용 CA에서 발급한 인증서에는 인증서 서명 권한이 없습니다. 이러한 인증서를 사용하려면 네트워크의 배포 지점 또는 연결 게이트웨이에 네트워크 에이전트 버전 13 이상을 설치했는지 확인하십시오. 그렇지 않으면 서명 권한 없이 인증서를 사용할 수 없습니다.

단계

중앙 관리 서버 인증서 지정은 다음 단계로 진행됩니다.

1. **중앙 관리 서버 인증서 교체**

   이를 위해서는 명령줄 klsetsrvcert 유틸리티를 사용합니다.

2. **새 인증서 지정 및 중앙 관리 서버에 대한 네트워크 에이전트 연결 복원**

   인증서를 교체하면 이전에 SSL을 통해 중앙 관리 서버에 연결했던 모든 네트워크 에이전트의 연결이 끊기며 "중앙 관리 서버 인증 오류"가 반환됩니다. 새 인증서를 지정하고 연결을 복원하려면 klmover 유틸리티를 사용합니다.

3. **Kaspersky Security Center 웹 콘솔 설정에서 새 인증서 지정**

   인증서 교체 후 Kaspersky Security Center 웹 콘솔 설정에서 인증서를 지정합니다. 그렇지 않으면 Kaspersky Security Center 웹 콘솔에서 중앙 관리 서버에 연결할 수 없습니다.

결과

시나리오 마지막으로 중앙 관리 서버 인증서가 교체되고 관리 중인 기기의 네트워크 에이전트를 통해 서버가 인증됩니다.

klsetsrvcert 유틸리티를 사용하여 중앙 관리 서버 인증서 교체

중앙 관리 서버 인증서를 교체하려면 다음과 같이 하십시오:

명령줄에서 다음 명령을 실행합니다.

```
klsetsrvcert [-t <인증서 유형> {-i <새 인증서 경로> [-p <암호>] [-o <파라미터>] | -g <DNS 이름>}][-f <교체 시간>][-r <루트 인증서>][-l <로그 파일 경로>]
```

klsetsrvcert 유틸리티를 다운로드할 필요가 없습니다. Kaspersky Security Center 배포 키트에 포함되어 있습니다. 이전 Kaspersky Security Center 버전과 호환되지 않습니다.

klsetsrvcert 유틸리티 파라미터에 대한 설명은 아래 표에 나와 있습니다.

klsetsrvcert 유틸리티 파라미터의 값

파라미터	값
`-t <인증서 유형>`	교체할 인증서의 유형입니다. <인증서 유형> 매개변수의 가능한 값: • `C` – 포트 13000 및 13291에서 공통 인증서를 교체합니다. • `CR` – 포트 13000 및 13291에서 공통 예약 인증서를 교체합니다. • `M` – 포트 13292에서 모바일 기기용 인증서를 교체합니다. • `MR` – 포트 13292에서 모바일 예약 인증서를 교체합니다. • `MCA` – 자동 생성된 사용자 인증서용 모바일 클라이언트 CA.
`-f <교체 시간>`	"DD-MM-YYYY hh:mm" 형식(포트 13000 및 13291의 경우)을 사용하는 인증서 변경 일정입니다. 공통 인증서가 만료되기 전에 공통 인증서를 공통 예약 인증서로 교체하려면 이 파라미터를 사용하십시오. 관리 중인 기기가 새 인증서에서 중앙 관리 서버와 동기화되어야 하는 시간을 지정합니다.
`-i <새 인증서 경로>`	PKCS#12 형식의 인증서 및 비공개 키가 포함된 컨테이너(확장자가 .p12 또는 .pfx인 파일)입니다.
`-p <암호>`	p12 컨테이너를 보호하는 데 사용되는 암호입니다. 인증서와 개인 키가 컨테이너에 저장되므로 컨테이너로 파일을 해독하려면 암호가 필요합니다.
`-o <검증 매개변수>`	인증서 검증 파라미터(세미콜론으로 구분)입니다. 서명 권한 없이 사용자 지정 인증서를 사용하려면 klsetsrvcert 유틸리티에서 `-o NoCA` 를 지정하십시오. 이는 공용 CA에서 발급한 인증서에 유용합니다. 인증서 유형 C 또는 CR의 암호화 키 길이를 변경하려면 klsetsrvcert 유틸리티에서 `-o RsaKeyLen:<키 길이>`를 지정합니다. 여기서 <키 길이> 파라미터는 필요한 키 길이 값입니다. 그렇지 않으면 현재 인증서 키 길이가 사용됩니다.
`-g <DNS 이름>`	지정한 DNS 이름에 대해 새 인증서가 생성됩니다.
`-r <루트 인증서>`	PEM 형식의 신뢰할 수 있는 루트 인증서 기관 목록입니다.
`-l <로그 파일 경로>`	결과 출력 파일입니다. 기본적으로 출력은 표준 출력 스트림으로 리다이렉트됩니다.

예를 들어 사용자 지정 중앙 관리 서버 인증서를 지정하려면 다음 명령을 사용합니다.

```
klsetsrvcert -t C -i <새 인증서 경로> -p <암호> -o NoCA
```

인증서가 교체되면 SSL을 통해 중앙 관리 서버에 연결된 모든 네트워크 에이전트의 연결이 끊어집니다. 연결을 복원하려면 klmover 유틸리티 명령줄을 사용하십시오.

네트워크 에이전트 연결이 끊어지지 않도록 하려면 다음 명령을 사용합니다:

1. 새 인증서를 설치하려면,

   ```
   klsetsrvcert.exe -t CR -i <새 인증서 경로> -p <암호> -o NoCA
   ```

2. 새 인증서를 적용할 날짜를 지정하려면,

   ```
   klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
   ```

여기서 "DD-MM-YYYY hh:mm"은 현재 날짜보다 3~4주 뒤의 날짜입니다. 현재 인증서를 새 인증서로 변경하기 위해 시간 이동을 하여 새 인증서를 모든 네트워크 에이전트에 배포할 수 있습니다.

klmover 유틸리티를 사용하여 네트워크 에이전트를 중앙 관리 서버에 연결

명령줄 klsetsrvcert 유틸리티를 사용하여 중앙 관리 서버 인증서를 교체하고 나면 연결이 끊어졌으므로 네트워크 에이전트와 중앙 관리 서버 간에 SSL 연결을 설정해야 합니다.

새 중앙 관리 서버 인증서를 지정하고 연결 복원하기:

명령줄에서 다음 명령을 실행합니다.

```
klmover [-address <서버 주소>] [-pn <포트 번호>] [-ps <SSL 포트 번호>] [-nossl] [-cert <인증서 파일 경로>]
```

유틸리티를 실행하려면 관리자 권한이 필요합니다.

이 유틸리티는 네트워크 에이전트가 클라이언트 기기에 설치될 때 네트워크 에이전트 설치 폴더에 자동으로 복사됩니다.

침입자가 중앙 관리 서버의 제어권 밖으로 기기를 이동하는 것을 방지하려면 klmover 유틸리티 실행 시 암호 보호를 활성화하는 것이 좋습니다. 암호 보호를 활성화하려면 네트워크 에이전트 정책 설정에서 **제거 암호 사용** 옵션을 선택하세요.

klmover 유틸리티에는 로컬 관리자 권한이 필요합니다. 로컬 관리자 권한 없이 작동하는 기기는 klmover 유틸리티 실행을 위한 암호 보호를 생략할 수 있습니다.

제거 암호 사용 옵션을 활성화하면 클리너 도구(cleaner.exe)에 대한 암호 보호도 활성화됩니다.

연결 게이트웨이를 통해 중앙 관리 서버에 연결된 클라이언트 기기에는 klmover 유틸리티를 사용할 수 없습니다. 이러한 기기는 네트워크 에이전트를 재구성하거나 네트워크 에이전트를 다시 설치하고 연결 게이트웨이를 지정해야 합니다.

klmover 유틸리티 파라미터에 대한 설명은 아래 표에 나와 있습니다.

klsetsrvcert 유틸리티 파라미터의 값

파라미터	값
-address <서버 주소>	연결을 위한 중앙 관리 서버의 주소입니다. IP 주소, NetBIOS 이름 또는 DNS 이름을 지정할 수 있습니다.
-pn <포트 번호>	중앙 관리 서버에 암호화되지 않은 연결을 설정하는 데 사용되는 포트 번호입니다. 기본 포트 번호는 14000입니다.
-ps <SSL 포트 번호>	SSL 프로토콜을 사용하여 중앙 관리 서버에 암호화된 연결을 설정하는 데 사용되는 SSL 포트 번호입니다. 기본 포트 번호는 13000입니다.
-nossl	중앙 관리 서버에 암호화되지 않은 연결을 사용합니다. 키를 사용 중이지 않은 경우, 네트워크 에이전트는 암호화된 SSL 프로토콜을 사용해 중앙 관리 서버에 연결됩니다.

파라미터	값
`-cert <인증서 파일 경로>`	중앙 관리 서버에 대한 접근의 인증을 위해 지정된 인증서 파일을 사용합니다.
`-virtserv`	가상 중앙 관리 서버 이름.
`-cloningmode`	네트워크 에이전트 디스크 복제 모드. 다음 매개변수 중 하나를 사용하여 디스크 복제 모드를 구성합니다: • `-cloningmode` –디스크 복제 모드의 상태를 요청합니다. • `-cloningmode 1` –디스크 복제 모드를 활성화합니다. • `-cloningmode 0` –디스크 복제 모드를 비활성화합니다.
`-nauninstpwd <암호>`	이 파라미터를 사용하여 네트워크 에이전트 제거 암호를 지정합니다. 파라미터는 필수가 아닙니다.

예를 들어, 네트워크 에이전트를 중앙 관리 서버에 연결하려면 다음 명령을 실행합니다:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

웹 서버 인증서 재발급

Kaspersky Security Center에서 사용되는 웹 서버 인증서는 나중에 관리 중인 기기에 다운로드하는 네트워크 에이전트 설치 패키지를 게시하고 iOS MDM 프로필, iOS 앱 및 Kaspersky Endpoint Security for Mobile 설치 패키지를 게시하는 데 필요합니다. 현재 애플리케이션 구성에 따라 다양한 인증서가 웹 서버 인증서로 작동할 수 있습니다 (자세한 내용은 Kaspersky Security Center 인증서 정보 참조).

회사의 특정 보안 요구 사항을 충족하거나 애플리케이션 업그레이드를 시작하기 전에 관리 중인 기기의 지속적인 연결을 유지하려면 웹 서버 인증서 재발급이 필요할 수 있습니다. Kaspersky Security Center는 웹 서버 인증서를 재발급하는 방법은 두 가지이며 모바일 프로토콜(모바일 인증서)을 통해 모바일 기기를 연결하거나 관리하고 있는지 여부에 따라 방법이 선택할 수 있습니다.

중앙 관리 서버 속성 창의 **웹 서버** 섹션에서 사용자 지정 인증서를 웹 서버 인증서로 지정하지 않은 경우 모바일 인증서는 웹 서버 인증서로 작동합니다. 이 경우 웹 서버 인증서 재발급은 모바일 프로토콜 자체를 재발급하여 이루어집니다.

모바일 프로토콜을 통해 관리되는 모바일 기기가 없는 경우 웹 서버 인증서를 재발급하려면:

1. 콘솔 트리에서 관련 중앙 관리 서버의 이름을 마우스 오른쪽 버튼으로 클릭하고 마우스 오른쪽 메뉴에서**속성**를 선택합니다.
2. 중앙 관리 서버 속성 창이 열리면 왼쪽 창에서 **중앙 관리 서버 연결 설정** 섹션을 선택합니다.
3. 하위 섹션 목록에서 **인증서** 하위 섹션을 선택합니다.
4. Kaspersky Security Center에서 발급한 인증서를 계속 사용하려면 다음을 수행하십시오.
   a. 오른쪽 창에서, 설정의 **모바일 기기별 중앙 관리 서버 인증** 그룹에서 **중앙 관리 서버를 통해 발급된 인증서** 옵션을 선택한 후 **재발급** 버튼을 클릭합니다.
   b. **인증서 재발급** 창이 열리면 설정의 **연결 주소** 및 **활성화 기간** 그룹에서 관련 옵션을 선택한 후 **확인**을 클릭합니다.
   c. 확인 창에서 **예**를 클릭합니다.

또는 자체 사용자 지정 인증서를 사용하려는 경우 다음을 수행하십시오.

a. 사용자 지정 인증서가 Kaspersky Security Center의 요구 사항 및 Apple의 신뢰하는 인증서 요구 사항을 충족하는지 확인합니다. 필요한 경우 인증서를 수정하십시오.

b. **다른 인증서** 옵션을 선택하고 **찾기** 버튼을 클릭합니다.

c. **인증서** 창이 열리면 **인증서 유형** 필드에서 인증서 유형을 선택한 다음 인증서 위치 및 설정을 지정합니다.

- **PKCS #12 컨테이너**을(를) 선택한 경우 **찾기** 버튼(**인증서 파일** 필드 옆에 있는)을 클릭하고 하드 드라이브의 인증서 파일을 지정합니다. 인증서 파일이 암호로 보호된 경우 **암호(있을 경우)** 필드에 암호를 입력합니다.

- **X.509 인증서**을(를) 선택한 경우 **개인 키(.prk, .pem)** 버튼(**찾기** 필드 옆에 있는)을 클릭하고 하드 드라이브의 개인 키를 지정합니다. 개인 키가 암호로 보호되어 있는 경우**암호(있을 경우)** 필드에 암호를 입력합니다. 그런 다음 **찾기** 버튼(**공개 키(.cer)** 필드 옆에 있는)을 클릭하고 하드 드라이브의 개인 키를 지정합니다.

d. **인증서** 창에서 **확인**을 클릭합니다.

e. 확인 창에서 **예**를 클릭합니다.

웹 서버 인증서로 사용할 모바일 인증서가 재발급됩니다.

모바일 프로토콜을 통해 관리되는 모바일 기기가 있는 경우 웹 서버 인증서를 재발급하려면:

1. 사용자 지정 인증서를 생성하고 Kaspersky Security Center에서 사용할 수 있도록 준비합니다. 사용자 지정 인증서가 Kaspersky Security Center의 요구 사항 및 Apple의 신뢰하는 인증서 요구 사항을 충족하는지 확인합니다. 필요한 경우 인증서를 수정하십시오.

2. 콘솔 트리에서 관련 중앙 관리 서버의 이름을 마우스 오른쪽 버튼으로 클릭하고 마우스 오른쪽 메뉴에서**속성**를 선택합니다.

3. 중앙 관리 서버 속성 창이 열리면 왼쪽 창에서 **웹 서버** 섹션을 선택합니다.

4. **HTTPS 사용** 메뉴에서 **다른 인증서 지정** 옵션을 선택합니다.

5. **HTTPS 사용** 메뉴에서 **변경** 버튼을 클릭합니다.

6. **인증서** 창이 열리면 **인증서 유형** 필드에서 인증서 유형을 선택합니다.

- **PKCS #12 컨테이너**을(를) 선택한 경우 **찾기** 버튼(**인증서 파일** 필드 옆에 있는)을 클릭하고 하드 드라이브의 인증서 파일을 지정합니다. 인증서 파일이 암호로 보호된 경우 **암호(있을 경우)** 필드에 암호를 입력합니다.

- **X.509 인증서**을(를) 선택한 경우 **개인 키(.prk, .pem)** 버튼(**찾기** 필드 옆에 있는)을 클릭하고 하드 드라이브의 개인 키를 지정합니다. 개인 키가 암호로 보호되어 있는 경우**암호(있을 경우)** 필드에 암호를 입력합니다. 그런 다음 **찾기** 버튼(**공개 키(.cer)** 필드 옆에 있는)을 클릭하고 하드 드라이브의 개인 키를 지정합니다.

7. **인증서** 창에서 **확인**을 클릭합니다.

8. 필요한 경우 중앙 관리 서버 속성 창의**웹 서버 HTTPS 포트** 필드에서 웹 서버의 HTTPS 포트 번호를 변경합니다. **확인**을 누릅니다.

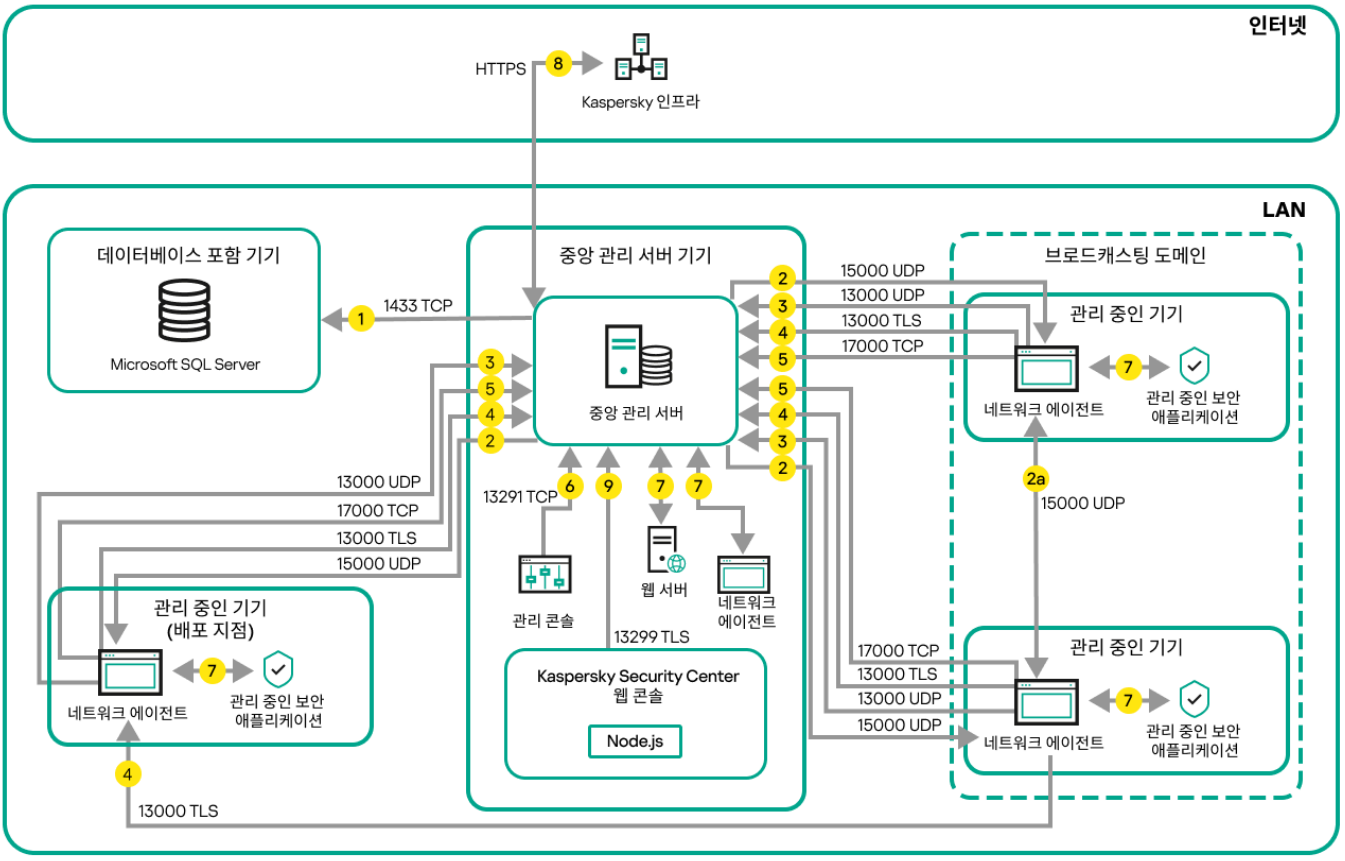
   웹 서버 인증서가 재발급됩니다.

데이터 트래픽 및 포트 사용 스키마

이 섹션에서는 다양한 구성으로 Kaspersky Security Center 구성 요소, 관리 중인 보안 제품 및 외부 서버 간의 데이터 트래픽에 대한 스키마를 제공합니다. 이 스키마는 로컬 기기에서 사용할 수 있어야 하는 포트 번호와 함께 제공됩니다.

LAN 내에 중앙 관리 서버 및 관리 중인 기기

아래 그림은 Kaspersky Security Center가 LAN(로컬 영역 네트워크)에만 배포된 경우 데이터의 트래픽을 보여 줍니다.



LAN(로컬 영역 네트워크)에 중앙 관리 서버 설치 및 관리 중인 기기 운영

그림에서는 관리 중인 기기가 서로 다른 방법으로 중앙 관리 서버에 연결되는 것을 보여 줍니다: 직접 또는 배포 지점 경유. 배포 지점은 업데이트 배포 시 중앙 관리 서버에서의 부하를 줄이고 네트워크 트래픽을 최적화합니다. 그러나 관리 중인 기기의 수가 충분히 많은 경우에만 배포 지점이 필요합니다. 만일 관리 중인 기기의 수가 작으면 모든 관리 중인 기기는 중앙 관리 서버에서 직접 업데이트를 받을 수 있습니다.

화살표는 트래픽 시작을 나타냅니다. 각 화살표는 연결을 시작하는 기기에서 호출을 "응답"하는 기기를 가리킵니다. 데이터 전송에 사용되는 포트 번호와 프로토콜 이름이 제공됩니다. 각 화살표에는 숫자 레이블이 있으며 해당 데이터 트래픽에 대한 자세한 내용은 다음과 같습니다:

1. 중앙 관리 서버는 데이터를 데이터베이스에 보냅니다. 중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치한다면 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(MySQL Server에서는 3306 포트, Microsoft SQL Server에서는 1433 포트 등). 관련 정보는 DBMS 설명서를 참조하십시오.

2. 중앙 관리 서버로부터의 통신 요청은 UDP 15000 포트를 통해 모바일 이외의 모든 관리 중인 기기로 전송됩니다.

   네트워크 에이전트들이 하나의 브로드캐스팅 도메인 내에서 서로 요청을 전송합니다. 그러면 데이터가 중앙 관리 서버로 전송되어 브로드캐스팅 도메인의 제한을 정의하고, 배포 지점을 자동 할당(이 옵션이 활성화되어 있는 경우)하는 데 사용됩니다.

   중앙 관리 서버가 관리 중인 기기에 직접 접근할 수 없다면, 중앙 관리 서버에서 이러한 기기로의 통신 요청이 직접 전송되지 않습니다.

3. 관리 중인 기기의 종료에 대한 정보는 UDP 13000 포트를 통해 네트워크 에이전트에서 중앙 관리 서버로 전송됩니다.

4. 중앙 관리 서버는 TLS 13000 포트를 통해 네트워크 에이전트 및 보조 중앙 관리 서버로부터 연결을 수신합니다.

   이전 버전의 Kaspersky Security Center를 사용했다면, 네트워크에 설치된 중앙 관리 서버는 TLS가 아닌 14000 포트를 통해 네트워크 에이전트 연결을 수신할 수 있습니다. 또한, Kaspersky Security Center는 13000 TLS 포트의 사용을 권장하지만 14000 포트를 통한 네트워크 에이전트 연결도 지원하고 있습니다.

   > 이전 버전의 Kaspersky Security Center에서는 배포 지점을 "업데이트 에이전트"라고 불렀습니다.

5. 관리 중인 기기(모바일 기기 제외)는 TCP 17000 포트를 통해 활성화를 요청합니다. 기기가 자체적으로 인터넷에 접근할 수 있을 시 이 작업이 필요하지 않습니다. 이때는 기기가 데이터를 인터넷의 Kaspersky 서버로 직접 전송합니다.

6. MMC 기반 관리 콘솔은 13291 포트를 통해 중앙 관리 서버로 데이터를 전송합니다. (관리 콘솔은 동일한 기기 또는 다른 기기에 설치될 수 있습니다.)

7. 단일 기기의 애플리케이션은 로컬 트래픽을 교환합니다(중앙 관리 서버 또는 관리 중인 기기). 외부 포트를 열 필요가 없습니다.

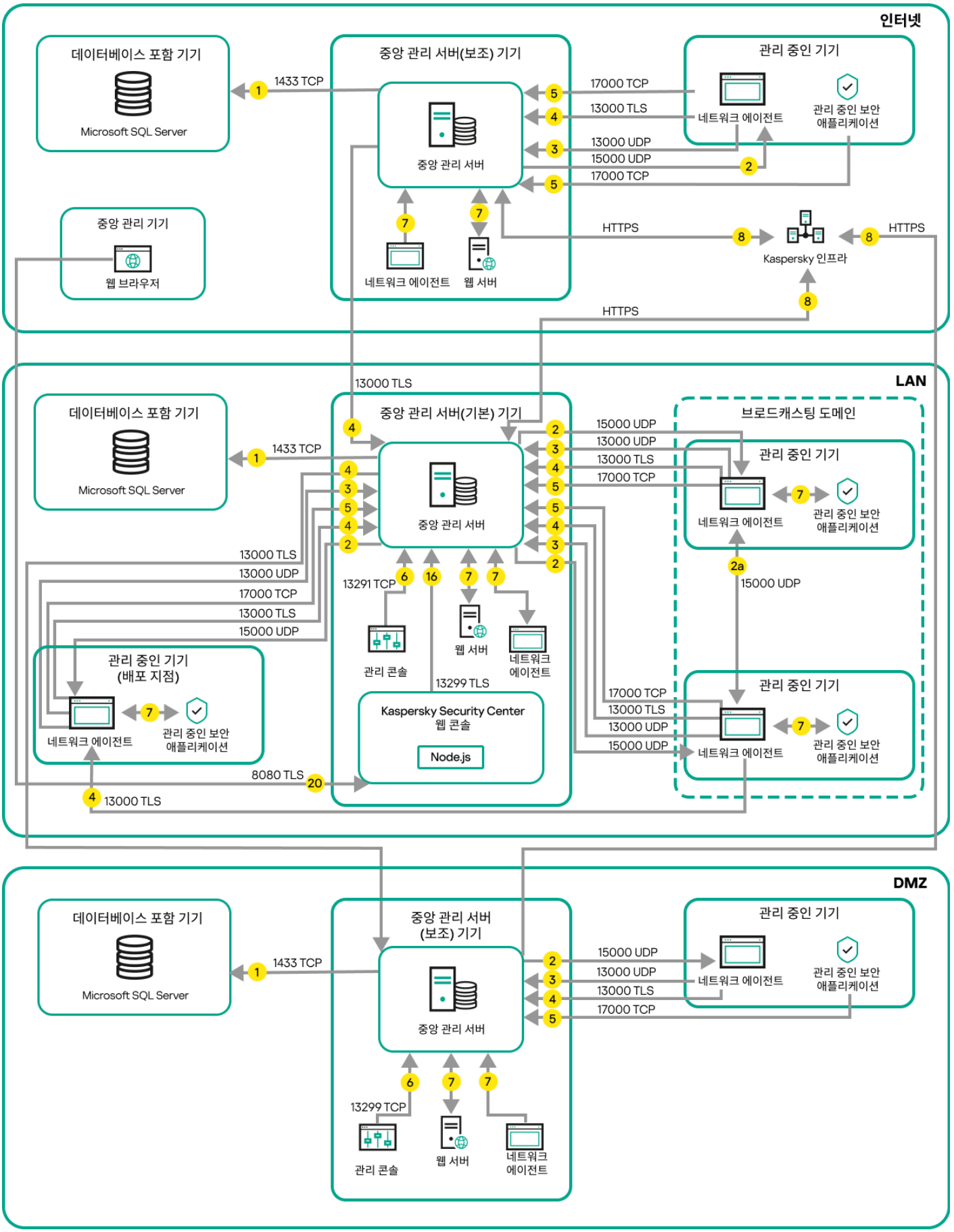
8. 중앙 관리 서버에서 KSN 데이터, 라이센스에 대한 정보 등 Kaspersky 서버로의 데이터와 애플리케이션 업데이트 및 안티 바이러스 데이터베이스 업데이트와 같은 Kaspersky 서버에서 중앙 관리 서버로의 데이터는 HTTPS 프로토콜을 통해 Kaspersky 서버로 전송됩니다.

   중앙 관리 서버가 인터넷에 접근하는 것을 원치 않는다면 이 데이터를 수동으로 관리해야 합니다.

9. Kaspersky Security Center 웹 콘솔 서버는 TLS 13299 포트를 통해 동일한 기기에 설치되거나 다른 기기에 설치될 수 있는 중앙 관리 서버로 데이터를 보냅니다.

LAN 내에 기본 중앙 관리 서버 및 두 개의 보조 중앙 관리 서버

아래 그림은 중앙 관리 서버의 계층을 보여 줍니다. 기본 중앙 관리 서버는 LAN(로컬 영역 네트워크)에 있습니다. 보조 중앙 관리 서버가 DMZ에 있고 다른 보조 중앙 관리 서버가 인터넷 망에 있습니다.



중앙 관리 서버 계층 구조: 기본 중앙 관리 서버 및 두 개의 보조 중앙 관리 서버

화살표는 트래픽 시작을 나타냅니다. 각 화살표는 연결을 시작하는 기기에서 호출을 "응답"하는 기기를 가리킵니다. 데이터 전송에 사용되는 포트 번호와 프로토콜 이름이 제공됩니다. 각 화살표에는 숫자 레이블이 있으며 해당 데이터 트래픽에 대한 자세한 내용은 다음과 같습니다:

1. 중앙 관리 서버는 데이터를 데이터베이스에 보냅니다. 중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치한다면 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(MySQL Server에서는 3306 포트, Microsoft SQL Server에서는 1433 포트 등). 관련 정보는 DBMS 설명서를 참조하십시오.

2. 중앙 관리 서버로부터의 통신 요청은 UDP 15000 포트를 통해 모바일 이외의 모든 관리 중인 기기로 전송됩니다.

   네트워크 에이전트들이 하나의 브로드캐스팅 도메인 내에서 서로 요청을 전송합니다. 그러면 데이터가 중앙 관리 서버로 전송되어 브로드캐스팅 도메인의 제한을 정의하고, 배포 지점을 자동 할당(이 옵션이 활성화되어 있는 경우)하는 데 사용됩니다.

   중앙 관리 서버가 관리 중인 기기에 직접 접근할 수 없다면, 중앙 관리 서버에서 이러한 기기로의 통신 요청이 직접 전송되지 않습니다.

3. 관리 중인 기기의 종료에 대한 정보는 UDP 13000 포트를 통해 네트워크 에이전트에서 중앙 관리 서버로 전송됩니다.

4. 중앙 관리 서버는 TLS 13000 포트를 통해 네트워크 에이전트 및 보조 중앙 관리 서버로부터 연결을 수신합니다.

   이전 버전의 Kaspersky Security Center를 사용했다면, 네트워크에 설치된 중앙 관리 서버는 TLS가 아닌 14000 포트를 통해 네트워크 에이전트 연결을 수신할 수 있습니다. 또한, Kaspersky Security Center는 13000 TLS 포트의 사용을 권장하지만 14000 포트를 통한 네트워크 에이전트 연결도 지원하고 있습니다.

   > 이전 버전의 Kaspersky Security Center에서는 배포 지점을 "업데이트 에이전트"라고 불렀습니다.

5. 관리 중인 기기(모바일 기기 제외)는 TCP 17000 포트를 통해 활성화를 요청합니다. 기기가 자체적으로 인터넷에 접근할 수 있을 시 이 작업이 필요하지 않습니다. 이때는 기기가 데이터를 인터넷의 Kaspersky 서버로 직접 전송합니다.

6. MMC 기반 관리 콘솔은 13291 포트를 통해 중앙 관리 서버로 데이터를 전송합니다. (관리 콘솔은 동일한 기기 또는 다른 기기에 설치될 수 있습니다.)

7. 단일 기기의 애플리케이션은 로컬 트래픽을 교환합니다(중앙 관리 서버 또는 관리 중인 기기). 외부 포트를 열 필요가 없습니다.

8. 중앙 관리 서버에서 KSN 데이터, 라이센스에 대한 정보 등 Kaspersky 서버로의 데이터와 애플리케이션 업데이트 및 안티 바이러스 데이터베이스 업데이트와 같은 Kaspersky 서버에서 중앙 관리 서버로의 데이터는 HTTPS 프로토콜을 통해 Kaspersky 서버로 전송됩니다.

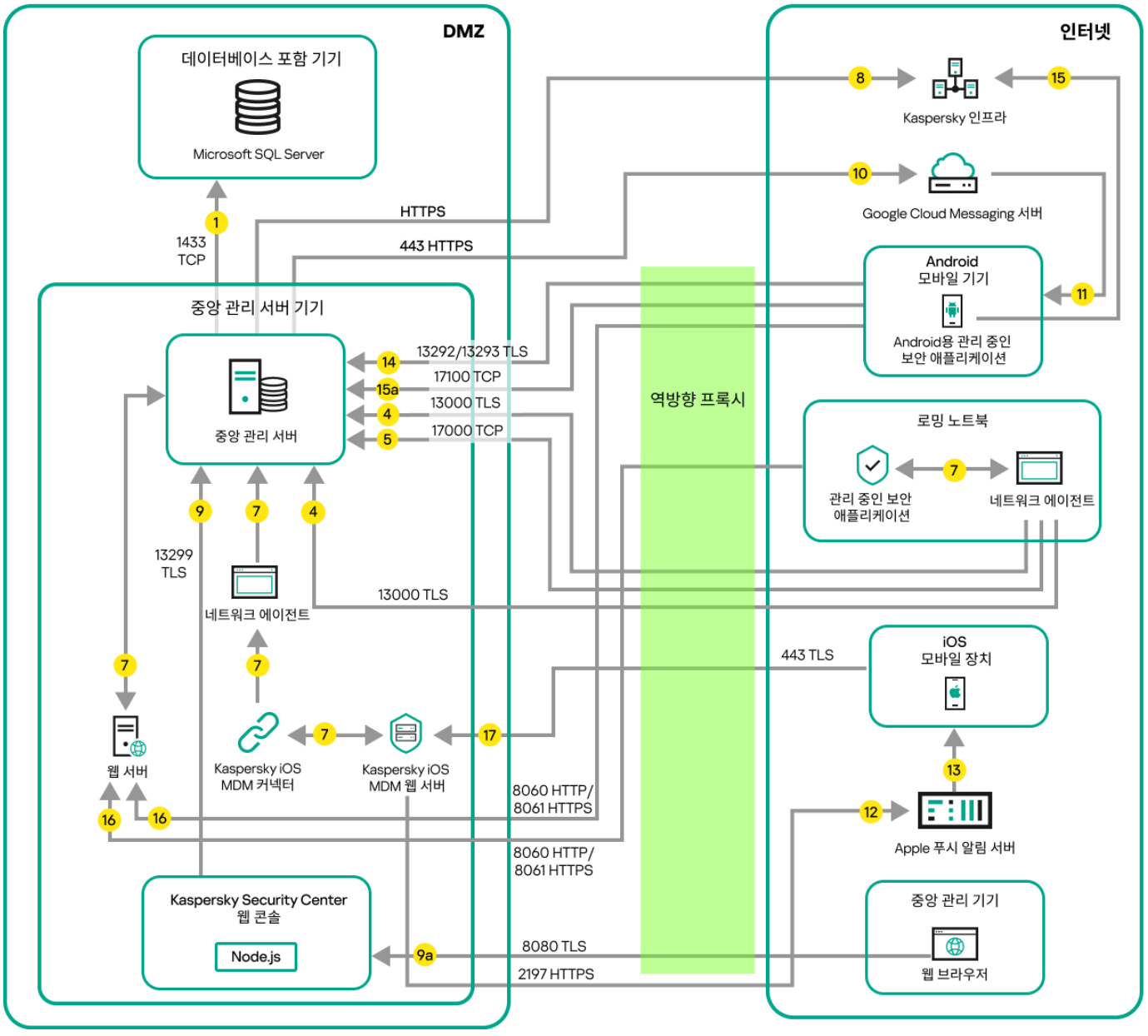
   중앙 관리 서버가 인터넷에 접근하는 것을 원치 않는다면 이 데이터를 수동으로 관리해야 합니다.

9. Kaspersky Security Center 웹 콘솔 서버는 TLS 13299 포트를 통해 같은 기기나 다른 기기에 설치할 수 있는 중앙 관리 서버로 데이터를 보냅니다.

   9a. 관리자의 별도 기기에 설치된 브라우저 데이터는 TLS 8080 포트를 통해 Kaspersky Security Center 웹 콘솔 서버로 전송됩니다. Kaspersky Security Center 웹 콘솔 서버는 중앙 관리 서버나 다른 장치에 설치할 수 있습니다.

LAN 내에 중앙 관리 서버 설치, 인터넷 망에 관리 중인 기기 운영, 역방향 프록시 사용 중

아래 그림은 중앙 관리 서버가 LAN(로컬 영역 네트워크) 내부에 있고 모바일 기기를 포함한 관리 중인 기기가 인터넷에 있는 경우 데이터의 트래픽을 보여줍니다. 이 그림에서는 선택한 역방향 프록시를 사용 중입니다. 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.



LAN 내에 중앙 관리 서버. 관리 중인 기기는 역방향 프록시를 통해 중앙 관리 서버에 연결

이 배포 계획은 모바일 기기가 중앙 관리 서버에 직접 연결되지 않도록 하고 DMZ 내의 연결 게이트웨이를 사용하지 않으려는 경우에 권장됩니다.

화살표는 트래픽 시작을 나타냅니다. 각 화살표는 연결을 시작하는 기기에서 호출을 "응답"하는 기기를 가리킵니다. 데이터 전송에 사용되는 포트 번호와 프로토콜 이름이 제공됩니다. 각 화살표에는 숫자 레이블이 있으며 해당 데이터 트래픽에 대한 자세한 내용은 다음과 같습니다:

1. 중앙 관리 서버는 데이터를 데이터베이스에 보냅니다. 중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치한다면 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(MySQL Server에서는 3306 포트, Microsoft SQL Server에서는 1433 포트 등). 관련 정보는 DBMS 설명서를 참조하십시오.

2. 중앙 관리 서버로부터의 통신 요청은 UDP 15000 포트를 통해 모바일 이외의 모든 관리 중인 기기로 전송됩니다.

   네트워크 에이전트들이 하나의 브로드캐스팅 도메인 내에서 서로 요청을 전송합니다. 그러면 데이터가 중앙 관리 서버로 전송되어 브로드캐스팅 도메인의 제한을 정의하고, 배포 지점을 자동 할당(이 옵션이 활성화되어 있는 경우)하는 데 사용됩니다.

   중앙 관리 서버가 관리 중인 기기에 직접 접근할 수 없다면, 중앙 관리 서버에서 이러한 기기로의 통신 요청이 직접 전송되지 않습니다.

3. 관리 중인 기기의 종료에 대한 정보는 UDP 13000 포트를 통해 네트워크 에이전트에서 중앙 관리 서버로 전송됩니다.

4. 중앙 관리 서버는 TLS 13000 포트를 통해 네트워크 에이전트 및 보조 중앙 관리 서버로부터 연결을 수신합니다.

   이전 버전의 Kaspersky Security Center를 사용했다면, 네트워크에 설치된 중앙 관리 서버는 TLS가 아닌 14000 포트를 통해 네트워크 에이전트 연결을 수신할 수 있습니다. 또한, Kaspersky Security Center는 13000 TLS 포트의 사용을 권장하지만 14000 포트를 통한 네트워크 에이전트 연결도 지원하고 있습니다.

   > 이전 버전의 Kaspersky Security Center에서는 배포 지점을 "업데이트 에이전트"라고 불렀습니다.

5. 관리 중인 기기(모바일 기기 제외)는 TCP 17000 포트를 통해 활성화를 요청합니다. 기기가 자체적으로 인터넷에 접근할 수 있을 시 이 작업이 필요하지 않습니다. 이때는 기기가 데이터를 인터넷의 Kaspersky 서버로 직접 전송합니다.

6. MMC 기반 관리 콘솔은 13291 포트를 통해 중앙 관리 서버로 데이터를 전송합니다. (관리 콘솔은 동일한 기기 또는 다른 기기에 설치될 수 있습니다.)

7. 단일 기기의 애플리케이션은 로컬 트래픽을 교환합니다(중앙 관리 서버 또는 관리 중인 기기). 외부 포트를 열 필요가 없습니다.

8. 중앙 관리 서버에서 KSN 데이터, 라이센스에 대한 정보 등 Kaspersky 서버로의 데이터와 애플리케이션 업데이트 및 안티 바이러스 데이터베이스 업데이트와 같은 Kaspersky 서버에서 중앙 관리 서버로의 데이터는 HTTPS 프로토콜을 통해 Kaspersky 서버로 전송됩니다.

   중앙 관리 서버가 인터넷에 접근하는 것을 원치 않는다면 이 데이터를 수동으로 관리해야 합니다.

9. Kaspersky Security Center 웹 콘솔 서버는 TLS 13299 포트를 통해 같은 기기나 다른 기기에 설치할 수 있는 중앙 관리 서버로 데이터를 보냅니다.

   9a. 관리자의 별도 기기에 설치된 브라우저 데이터는 TLS 8080 포트를 통해 Kaspersky Security Center 웹 콘솔 서버로 전송됩니다. Kaspersky Security Center 웹 콘솔 서버는 중앙 관리 서버나 다른 기기에 설치할 수 있습니다.

10. Android 모바일 기기만 해당: 중앙 관리 서버에서의 데이터는 Google 서버로 전송됩니다. 이 연결은 중앙 관리 서버에 연결하기 위해 Android 모바일 기기에 필요한 사항을 알리는 데 사용됩니다. 그런 다음 푸시 알림이 모바일 기기로 전송됩니다.

11. Android 모바일 기기만 해당: Google 서버에서의 푸시 알림이 해당 모바일 기기로 전송됩니다. 이 연결은 중앙 관리 서버에 연결하기 위해 모바일 기기에 필요한 사항을 알리는 데 사용됩니다.

12. IOS 모바일 기기만 해당: iOS MDM 서버에서의 데이터는 Apple 푸시 알림 서버로 전송됩니다. 그런 다음 푸시 알림이 모바일 기기로 전송됩니다.

13. IOS 모바일 기기만 해당: Apple 서버에서 모바일 기기로 알림을 푸시합니다. 이 연결은 중앙 관리 서버에 연결하기 위해 iOS 모바일 기기에 필요한 사항을 알리는 데 사용됩니다.

14. 모바일 기기만 해당: 관리 중인 애플리케이션의 데이터는 TLS 13292/13293 포트를 통해 직접 또는 역방향 프록시를 통해 중앙 관리 서버(또는 연결 게이트웨이로)로 전송됩니다.

15. 모바일 기기만 해당: 모바일 기기에서의 데이터는 Kaspersky 인프라로 전송됩니다.

    모바일 기기에 인터넷 접속이 없을 시, 데이터는 17100 포트를 통해 중앙 관리 서버로 전송되고 중앙 관리 서버는 이를 Kaspersky 인프라로 전송합니다. 다만, 이 시나리오는 매우 드물게 적용됩니다.

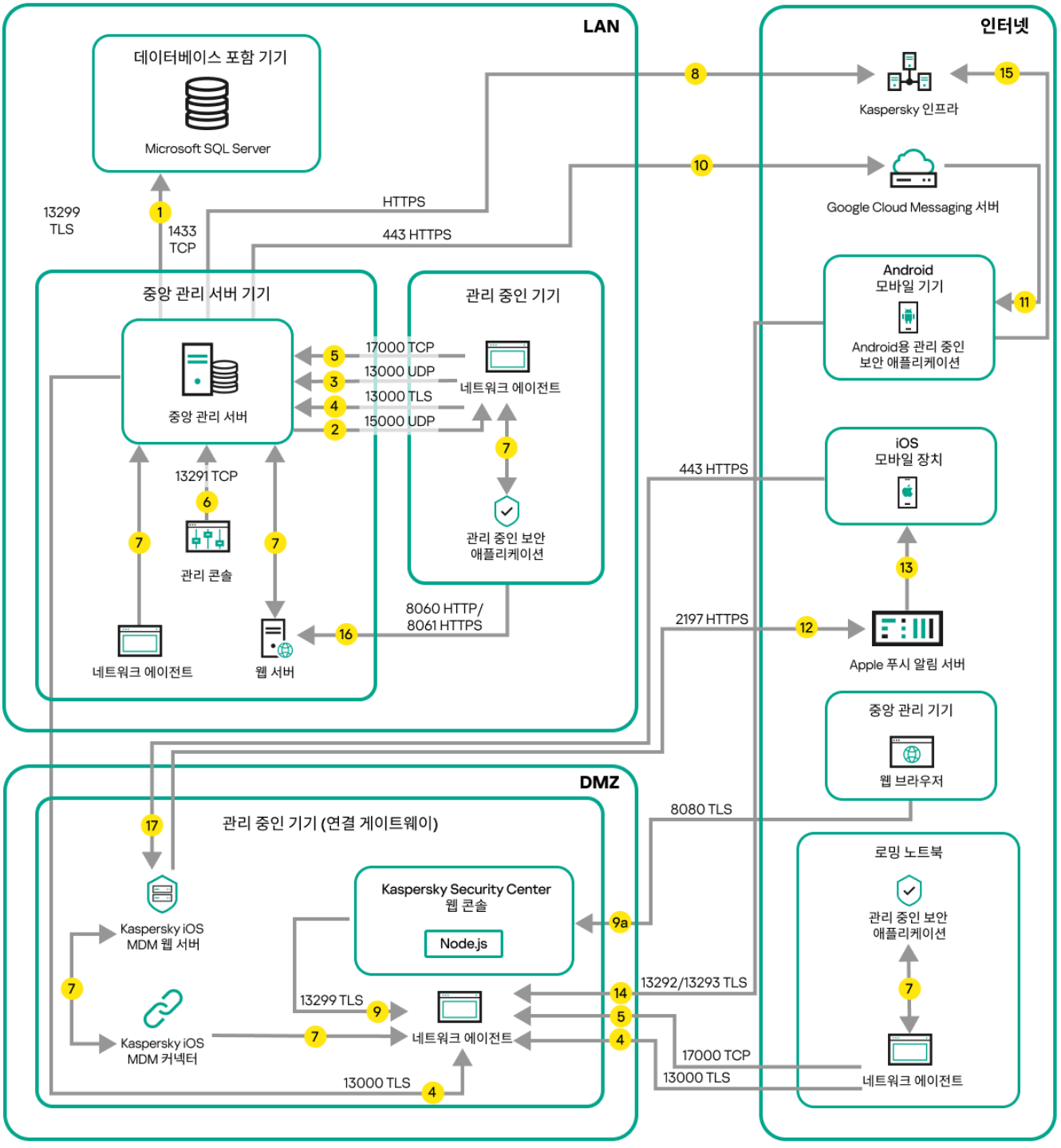
16. 모바일 기기를 포함한 관리 중인 기기의 패키지 요청은 중앙 관리 서버와 동일한 기기에 있는 웹 서버로 전송됩니다.

17. IOS 모바일 기기만 해당: 모바일 기기로부터의 데이터는 TLS 443 포트를 통해 중앙 관리 서버와 동일한 기기 또는 연결 게이트웨이에 있는 iOS MDM 서버로 전송됩니다.

LAN 내에 중앙 관리 서버 설치, 인터넷 망에 관리 중인 기기 운영, 연결 게이트웨이 사용 중

아래 그림은 중앙 관리 서버가 LAN(로컬 영역 네트워크) 내부에 있고 모바일 기기를 포함한 관리 중인 기기가 인터넷에 있는 경우 데이터의 트래픽을 보여줍니다. 연결 게이트웨이가 사용 중입니다.

이 배포 계획은 모바일 기기가 중앙 관리 서버를 직접 연결하지 않고 역방향 프록시 또는 기업 방화벽을 사용하지 않을 때 권장됩니다.



연결 게이트웨이를 통해 중앙 관리 서버에 연결된 관리 중인 모바일 기기

이 그림에서 관리 중인 기기는 DMZ에 있는 연결 게이트웨이를 통해 중앙 관리 서버에 연결됩니다. 사용 중인 역방향 프록시 또는 회사 방화벽이 없습니다.

화살표는 트래픽 시작을 나타냅니다. 각 화살표는 연결을 시작하는 기기에서 호출을 "응답"하는 기기를 가리킵니다. 데이터 전송에 사용되는 포트 번호와 프로토콜 이름이 제공됩니다. 각 화살표에는 숫자 레이블이 있으며 해당 데이터 트래픽에 대한 자세한 내용은 다음과 같습니다:

1. 중앙 관리 서버는 데이터를 데이터베이스에 보냅니다. 중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치한다면 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(MySQL Server에서는 3306 포트, Microsoft SQL Server에서는 1433 포트 등). 관련 정보는 DBMS 설명서를 참조하십시오.

2. 중앙 관리 서버로부터의 통신 요청은 UDP 15000 포트를 통해 모바일 이외의 모든 관리 중인 기기로 전송됩니다.

   네트워크 에이전트들이 하나의 브로드캐스팅 도메인 내에서 서로 요청을 전송합니다. 그러면 데이터가 중앙 관리 서버로 전송되어 브로드캐스팅 도메인의 제한을 정의하고, 배포 지점을 자동 할당(이 옵션이 활성화되어 있는 경우)하는 데 사용됩니다.

   중앙 관리 서버가 관리 중인 기기에 직접 접근할 수 없다면, 중앙 관리 서버에서 이러한 기기로의 통신 요청이 직접 전송되지 않습니다.

3. 관리 중인 기기의 종료에 대한 정보는 UDP 13000 포트를 통해 네트워크 에이전트에서 중앙 관리 서버로 전송됩니다.

4. 중앙 관리 서버는 TLS 13000 포트를 통해 네트워크 에이전트 및 보조 중앙 관리 서버로부터 연결을 수신합니다.

   이전 버전의 Kaspersky Security Center를 사용했다면, 네트워크에 설치된 중앙 관리 서버는 TLS가 아닌 14000 포트를 통해 네트워크 에이전트 연결을 수신할 수 있습니다. 또한, Kaspersky Security Center는 13000 TLS 포트의 사용을 권장하지만 14000 포트를 통한 네트워크 에이전트 연결도 지원하고 있습니다.

   > 이전 버전의 Kaspersky Security Center에서는 배포 지점을 "업데이트 에이전트"라고 불렀습니다.

   4a. DMZ의 연결 게이트웨이도 TLS 포트 13000을 통해 중앙 관리 서버에서 연결을 수신합니다. DMZ의 연결 게이트웨이는 중앙 관리 서버 포트에 도달할 수 없기 때문에 중앙 관리 서버는 연결 게이트웨이와의 영구적인 신호 연결을 생성하고 유지합니다. 신호 연결은 데이터 전송에 사용되지 않고, 네트워크 상호 작용으로 초대를 전송할 때에만 사용됩니다. 연결 게이트웨이가 서버에 연결해야 하는 경우에는 이 신호 연결을 통해 서버에 통지하고, 그러면 서버가 데이터 전송에 필요한 연결을 생성합니다.

   이동 사용자 기기 역시 TLS 포트 13000을 통해 연결 게이트웨이에 연결합니다.

5. 관리 중인 기기(모바일 기기 제외)는 TCP 17000 포트를 통해 활성화를 요청합니다. 기기가 자체적으로 인터넷에 접근할 수 있을 시 이 작업이 필요하지 않습니다. 이때는 기기가 데이터를 인터넷의 Kaspersky 서버로 직접 전송합니다.

6. MMC 기반 관리 콘솔은 13291 포트를 통해 중앙 관리 서버로 데이터를 전송합니다. (관리 콘솔은 동일한 기기 또는 다른 기기에 설치될 수 있습니다.)

7. 단일 기기의 애플리케이션은 로컬 트래픽을 교환합니다(중앙 관리 서버 또는 관리 중인 기기). 외부 포트를 열 필요가 없습니다.

8. 중앙 관리 서버에서 KSN 데이터, 라이센스에 대한 정보 등 Kaspersky 서버로의 데이터와 애플리케이션 업데이트 및 안티 바이러스 데이터베이스 업데이트와 같은 Kaspersky 서버에서 중앙 관리 서버로의 데이터는 HTTPS 프로토콜을 통해 Kaspersky 서버로 전송됩니다.

   중앙 관리 서버가 인터넷에 접근하는 것을 원치 않는다면 이 데이터를 수동으로 관리해야 합니다.

9. Kaspersky Security Center 웹 콘솔 서버는 TLS 13299 포트를 통해 같은 기기나 다른 기기에 설치할 수 있는 중앙 관리 서버로 데이터를 보냅니다.

   9a. 관리자의 별도 기기에 설치된 브라우저 데이터는 TLS 8080 포트를 통해 Kaspersky Security Center 웹 콘솔 서버로 전송됩니다. Kaspersky Security Center 웹 콘솔 서버는 중앙 관리 서버나 다른 기기에 설치할 수 있습니다.

10. Android 모바일 기기만 해당: 중앙 관리 서버에서의 데이터는 Google 서버로 전송됩니다. 이 연결은 중앙 관리 서버에 연결하기 위해 Android 모바일 기기에 필요한 사항을 알리는 데 사용됩니다. 그런 다음 푸시 알림이 모바일 기기로 전송됩니다.

11. Android 모바일 기기만 해당: Google 서버에서의 푸시 알림이 해당 모바일 기기로 전송됩니다. 이 연결은 중앙 관리 서버에 연결하기 위해 모바일 기기에 필요한 사항을 알리는 데 사용됩니다.

12. IOS 모바일 기기만 해당: iOS MDM 서버에서의 데이터는 Apple 푸시 알림 서버로 전송됩니다. 그런 다음 푸시 알림이 모바일 기기로 전송됩니다.

13. IOS 모바일 기기만 해당: Apple 서버에서 모바일 기기로 알림을 푸시합니다. 이 연결은 중앙 관리 서버에 연결하기 위해 iOS 모바일 기기에 필요한 사항을 알리는 데 사용됩니다.

14. 모바일 기기만 해당: 관리 중인 애플리케이션의 데이터는 TLS 13292/13293 포트를 통해 직접 또는 역방향 프록시를 통해 중앙 관리 서버(또는 연결 게이트웨이로)로 전송됩니다.

15. 모바일 기기만 해당: 모바일 기기에서의 데이터는 Kaspersky 인프라로 전송됩니다.

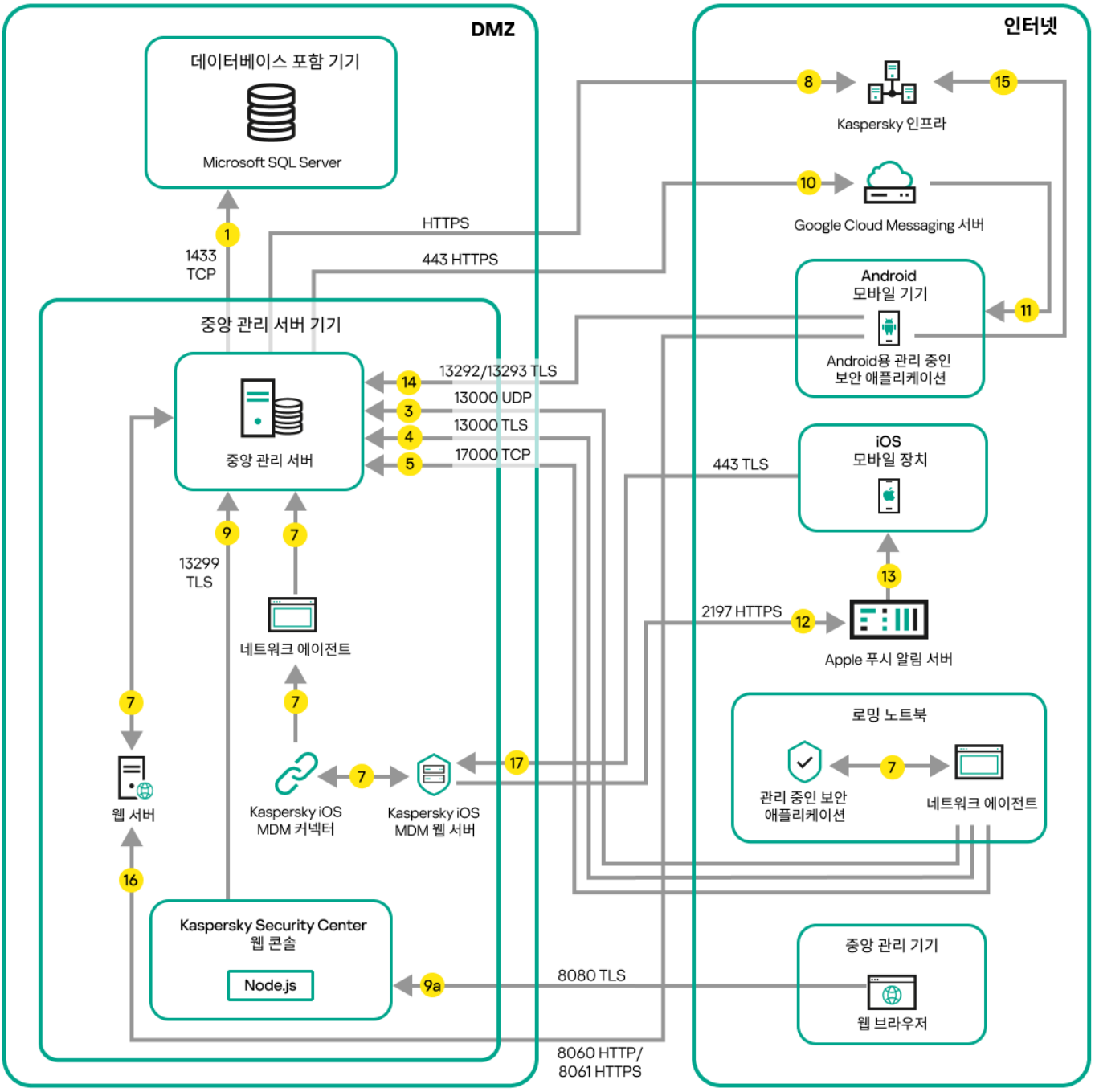
    > 모바일 기기에 인터넷 접속이 없을 시, 데이터는 17100 포트를 통해 중앙 관리 서버로 전송되고 중앙 관리 서버는 이를 Kaspersky 인프라로 전송합니다. 다만, 이 시나리오는 매우 드물게 적용됩니다.

16. 모바일 기기를 포함한 관리 중인 기기의 패키지 요청은 중앙 관리 서버와 동일한 기기에 있는 웹 서버로 전송됩니다.

17. IOS 모바일 기기만 해당: 모바일 기기로부터의 데이터는 TLS 443 포트를 통해 중앙 관리 서버와 동일한 기기 또는 연결 게이트웨이에 있는 iOS MDM 서버로 전송됩니다.

DMZ 내에 중앙 관리 서버 설치, 인터넷 망에 관리 중인 기기 운영

아래 그림은 중앙 관리 서버가 DMZ 내부에 있고 모바일 기기를 포함한 관리 중인 기기가 인터넷 망에 있을 때의 데이터 트래픽을 보여줍니다.



DMZ 내에 중앙 관리 서버 설치, 인터넷의 관리 중인 모바일 기기

이 그림에서는 사용 중인 연결 게이트웨이가 없습니다. 모바일 기기가 중앙 관리 서버에 직접 연결됩니다.

화살표는 트래픽 시작을 나타냅니다. 각 화살표는 연결을 시작하는 기기에서 호출을 "응답"하는 기기를 가리킵니다. 데이터 전송에 사용되는 포트 번호와 프로토콜 이름이 제공됩니다. 각 화살표에는 숫자 레이블이 있으며 해당 데이터 트래픽에 대한 자세한 내용은 다음과 같습니다:

1. 중앙 관리 서버는 데이터를 데이터베이스에 보냅니다. 중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치한다면 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(MySQL Server에서는 3306 포트, Microsoft SQL Server에서는 1433 포트 등). 관련 정보는 DBMS 설명서를 참조하십시오.

2. 중앙 관리 서버로부터의 통신 요청은 UDP 15000 포트를 통해 모바일 이외의 모든 관리 중인 기기로 전송됩니다.

   네트워크 에이전트들이 하나의 브로드캐스팅 도메인 내에서 서로 요청을 전송합니다. 그러면 데이터가 중앙 관리 서버로 전송되어 브로드캐스팅 도메인의 제한을 정의하고, 배포 지점을 자동 할당(이 옵션이 활성화되어 있는 경우)하는 데 사용됩니다.

   중앙 관리 서버가 관리 중인 기기에 직접 접근할 수 없다면, 중앙 관리 서버에서 이러한 기기로의 통신 요청이 직접 전송되지 않습니다.

3. 관리 중인 기기의 종료에 대한 정보는 UDP 13000 포트를 통해 네트워크 에이전트에서 중앙 관리 서버로 전송됩니다.

4. 중앙 관리 서버는 TLS 13000 포트를 통해 네트워크 에이전트 및 보조 중앙 관리 서버로부터 연결을 수신합니다.

   이전 버전의 Kaspersky Security Center를 사용했다면, 네트워크에 설치된 중앙 관리 서버는 TLS가 아닌 14000 포트를 통해 네트워크 에이전트 연결을 수신할 수 있습니다. 또한, Kaspersky Security Center는 13000 TLS 포트의 사용을 권장하지만 14000 포트를 통한 네트워크 에이전트 연결도 지원하고 있습니다.

   > 이전 버전의 Kaspersky Security Center에서는 배포 지점을 "업데이트 에이전트"라고 불렀습니다.

5. 관리 중인 기기(모바일 기기 제외)는 TCP 17000 포트를 통해 활성화를 요청합니다. 기기가 자체적으로 인터넷에 접근할 수 있을 시 이 작업이 필요하지 않습니다. 이때는 기기가 데이터를 인터넷의 Kaspersky 서버로 직접 전송합니다.

6. MMC 기반 관리 콘솔은 13291 포트를 통해 중앙 관리 서버로 데이터를 전송합니다. (관리 콘솔은 동일한 기기 또는 다른 기기에 설치될 수 있습니다.)

7. 단일 기기의 애플리케이션은 로컬 트래픽을 교환합니다(중앙 관리 서버 또는 관리 중인 기기). 외부 포트를 열 필요가 없습니다.

8. 중앙 관리 서버에서 KSN 데이터, 라이센스에 대한 정보 등 Kaspersky 서버로의 데이터와 애플리케이션 업데이트 및 안티 바이러스 데이터베이스 업데이트와 같은 Kaspersky 서버에서 중앙 관리 서버로의 데이터는 HTTPS 프로토콜을 통해 Kaspersky 서버로 전송됩니다.

   중앙 관리 서버가 인터넷에 접근하는 것을 원치 않는다면 이 데이터를 수동으로 관리해야 합니다.

9. Kaspersky Security Center 웹 콘솔 서버는 TLS 13299 포트를 통해 같은 기기나 다른 기기에 설치할 수 있는 중앙 관리 서버로 데이터를 보냅니다.

   9a. 관리자의 별도 기기에 설치된 브라우저 데이터는 TLS 8080 포트를 통해 Kaspersky Security Center 웹 콘솔 서버로 전송됩니다. Kaspersky Security Center 웹 콘솔 서버는 중앙 관리 서버나 다른 기기에 설치할 수 있습니다.

10. Android 모바일 기기만 해당: 중앙 관리 서버에서의 데이터는 Google 서버로 전송됩니다. 이 연결은 중앙 관리 서버에 연결하기 위해 Android 모바일 기기에 필요한 사항을 알리는 데 사용됩니다. 그런 다음 푸시 알림이 모바일 기기로 전송됩니다.

11. Android 모바일 기기만 해당: Google 서버에서의 푸시 알림이 해당 모바일 기기로 전송됩니다. 이 연결은 중앙 관리 서버에 연결하기 위해 모바일 기기에 필요한 사항을 알리는 데 사용됩니다.

12. IOS 모바일 기기만 해당: iOS MDM 서버에서의 데이터는 Apple 푸시 알림 서버로 전송됩니다. 그런 다음 푸시 알림이 모바일 기기로 전송됩니다.

13. IOS 모바일 기기만 해당: Apple 서버에서 모바일 기기로 알림을 푸시합니다. 이 연결은 중앙 관리 서버에 연결하기 위해 iOS 모바일 기기에 필요한 사항을 알리는 데 사용됩니다.

14. 모바일 기기만 해당: 관리 중인 애플리케이션의 데이터는 TLS 13292/13293 포트를 통해 직접 또는 역방향 프록시를 통해 중앙 관리 서버(또는 연결 게이트웨이로)로 전송됩니다.

15. 모바일 기기만 해당: 모바일 기기에서의 데이터는 Kaspersky 인프라로 전송됩니다.

    모바일 기기에 인터넷 접속이 없을 시, 데이터는 17100 포트를 통해 중앙 관리 서버로 전송되고 중앙 관리 서버는 이를 Kaspersky 인프라로 전송합니다. 다만, 이 시나리오는 매우 드물게 적용됩니다.

16. 모바일 기기를 포함한 관리 중인 기기의 패키지 요청은 중앙 관리 서버와 동일한 기기에 있는 웹 서버로 전송됩니다.

17. IOS 모바일 기기만 해당: 모바일 기기로부터의 데이터는 TLS 443 포트를 통해 중앙 관리 서버와 동일한 기기 또는 연결 게이트웨이에 있는 iOS MDM 서버로 전송됩니다.

Kaspersky Security Center 구성 요소와 보안 제품의 상호 작용: 자세한 정보

이 섹션에서는 Kaspersky Security Center 구성 요소와 관리 중인 보안 제품의 상호 작용을 위한 스키마를 제공합니다. 스키마는 이용 가능해야 하는 포트 번호와 해당 포트를 여는 프로세스 이름을 제공합니다.

상호 작용 스키마에서 사용되는 표기법

다음 표는 스키마에서 사용되는 규칙을 제공합니다.

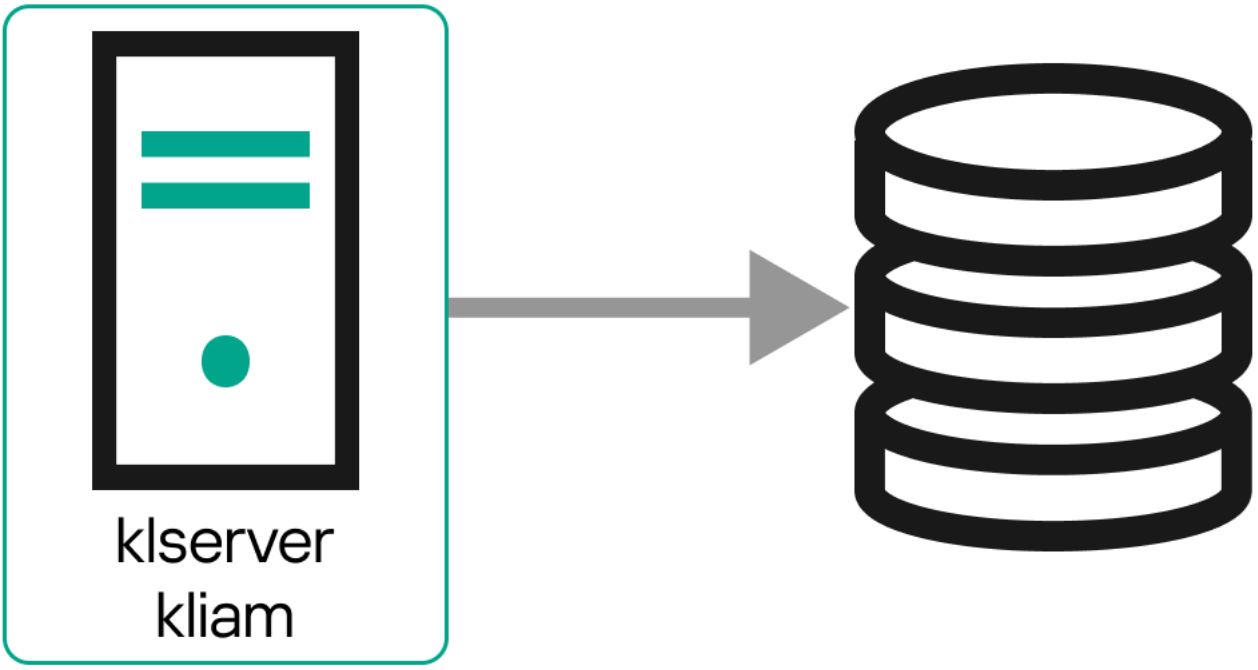
문서 표기법

아이콘	의미
	중앙 관리 서버
	보조 중앙 관리 서버
	DBMS

	클라이언트 기기(네트워크 에이전트 및 Kaspersky Endpoint Security 제품군의 애플리케이션이 설치되어 있거나 Kaspersky Security Center에서 관리 할 수 있는 다른 보안 제품이 설치되어 있음)
	연결 게이트웨이
	배포 지점
	Kaspersky Security for Mobile이 설치된 모바일 클라이언트 기기
	사용자 기기 찾기
	기기에서 실행 중인 프로세스와 포트 열기
	포트 및 그 번호
	TCP 트래픽(화살표 방향은 트래픽 이동 방향을 나타냅니다.)
	UDP 트래픽(화살표 방향은 트래픽 이동 방향을 나타냅니다.)
	COM 호출
	DBMS 트랜스포트
	DMZ 경계단

중앙 관리 서버 및 DBMS

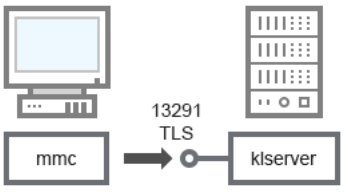
중앙 관리 서버의 데이터는 SQL Server, MySQL 또는 MariaDB 데이터베이스에 입력됩니다.



중앙 관리 서버 및 DBMS

중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치한다면 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(MySQL Server에서는 3306 포트, Microsoft SQL Server에서는 1433 포트 등). 관련 정보는 DBMS 설명서를 참조하십시오.

중앙 관리 서버 및 관리 콘솔



중앙 관리 서버 및 관리 콘솔

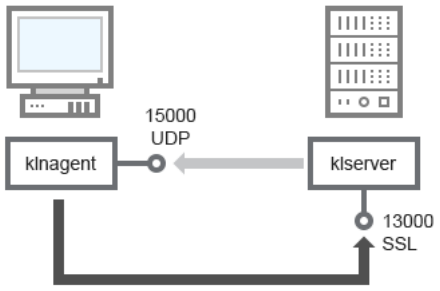
스키마 설명은 아래 표를 참조하십시오.

중앙 관리 서버 및 관리 콘솔(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS	포트 용도
중앙 관리 서버	13291	klserver	TCP	예	관리 콘솔에서 연결 수신

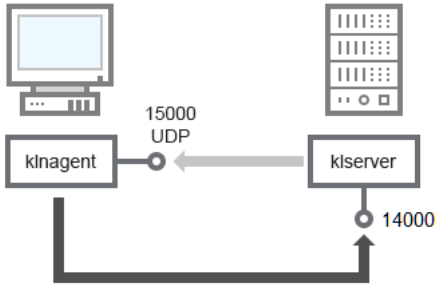
중앙 관리 서버 및 클라이언트 기기: 보안 제품 관리

중앙 관리 서버는 SSL 포트 13000을 통해 네트워크 에이전트 연결을 수신합니다(아래 그림 참조).



중앙 관리 서버 및 클라이언트 기기: 보안 제품 관리, 13000 포트를 통해 연결(권장)

이전 버전의 Kaspersky Security Center를 사용했다면, 네트워크에 설치된 중앙 관리 서버는 SSL이 아닌 14000 포트를 통해 네트워크 에이전트 연결을 수신할 수 있습니다(아래 그림 참조). 또한, Kaspersky Security Center 15.1는 13000 SSL 포트의 사용을 권장하지만 14000 포트를 통한 네트워크 에이전트 연결도 지원하고 있습니다.



중앙 관리 서버 및 클라이언트 기기: 보안 제품 관리, 14000 포트를 통해 연결(낮은 보안)

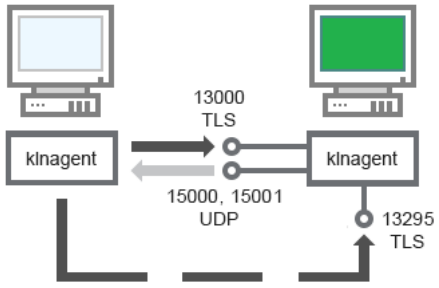
스키마에 대한 설명은 아래 표를 참조하십시오.

중앙 관리 서버 및 클라이언트 기기: 보안 제품 관리(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS(TCP에만 해당됨)	포트 용도
네트워크 에이전트	15000	klnagent	UDP	값 없음	네트워크 에이전트용 멀티캐스팅
중앙 관리 서버	13000	klserver	TCP	예	네트워크 에이전트에서 연결 수신
중앙 관리 서버	14000	klserver	TCP	아니요	네트워크 에이전트에서 연결 수신

배포 지점을 통해 클라이언트 기기에 있는 소프트웨어 업그레이드

클라이언트 기기는 포트 13000을 통해 배포 지점에 연결되며 포트 13295를 통해서도 배포 지점을 푸시 서버로 사용하는 경우, 배포 지점은 포트 15000을 통해 네트워크 에이전트에 멀티캐스트합니다(아래 그림 참조). 업데이트 및 설치 패키지는 15001 포트를 통해 배포 지점에서 수신됩니다.



배포 지점을 통해 클라이언트 기기에 있는 소프트웨어 업그레이드

스키마 설명은 아래 표를 참조하십시오.

배포 지점을 통한 소프트웨어 업그레이드(트래픽)

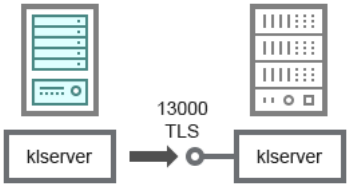
기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS(TCP에만 해당됨)	포트 용도
네트워크 에이전트	15000	klnagent	UDP	값 없음	네트워크 에이전트용 멀티캐스팅
네트워크 에이전트	15001	klnagent	UDP	값 없음	배포 지점에서 업데이트 및 설치 패키지 수신
배포 지점	13000	klnagent	TCP	예	네트워크 에이전트에서 연결 수신
배포 지점	13295	klnagent	TCP	예	클라이언트 기기에서 연결 수신(푸시 서버를 통해)

중앙 관리 서버 계층 구조: 기본 중앙 관리 서버 및 보조 중앙 관리 서버

스키마(아래 그림 참조)는 13000 포트를 사용하여 계층으로 결합된 중앙 관리 서버 간의 연동을 가능하게 하는 방법을 보여 줍니다.

두 개의 중앙 관리 서버를 하나의 계층으로 결합하는 경우 두 중앙 관리 서버 모두에서 13291 포트가 열려 있어야 합니다. 13291 포트를 통해 관리 콘솔이 해당 중앙 관리 서버와 연결합니다.

이후에 중앙 관리 서버가 계층으로 결합되면 기본 중앙 관리 서버에 연결된 관리 콘솔을 사용하여 두 서버를 모두 관리할 수 있습니다. 따라서 기본 중앙 관리 서버의 13291 포트에 대한 접근 가능성이 유일한 전제 조건입니다.



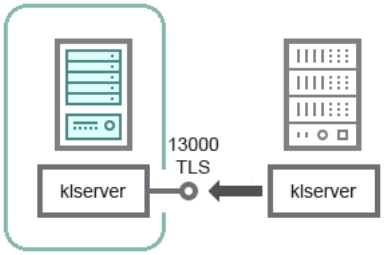
중앙 관리 서버 계층 구조: 기본 중앙 관리 서버 및 보조 중앙 관리 서버

스키마 설명은 아래 표를 참조하십시오.

중앙 관리 서버의 계층 구조(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS	포트 용도
기본 중앙 관리 서버	13000	klserver	TCP	예	보조 중앙 관리 서버에서 연결 수신

DMZ에 있는 보조 중앙 관리 서버와 중앙 관리 서버 계층



DMZ에 있는 보조 중앙 관리 서버와 중앙 관리 서버 계층

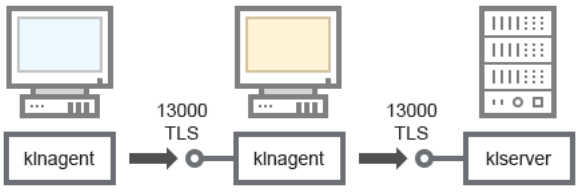
스키마는 DMZ에 있는 보조 중앙 관리 서버가 기본 중앙 관리 서버로부터 연결을 데이터를 수신하는 중앙 관리 서버의 계층 구조를 보여줍니다(스키마 설명은 아래 표 참조). 두 개의 중앙 관리 서버를 하나의 계층으로 결합하는 경우 두 중앙 관리 서버 모두에서 13291 포트가 열려 있어야 합니다. 13291 포트를 통해 관리 콘솔이 해당 중앙 관리 서버와 연결합니다.

이후에 중앙 관리 서버가 계층으로 결합되면 기본 중앙 관리 서버에 연결된 관리 콘솔을 사용하여 두 서버를 모두 관리할 수 있습니다. 따라서 기본 중앙 관리 서버의 13291 포트에 대한 접근 가능성이 유일한 전제 조건입니다.

DMZ에 있는 보조 중앙 관리 서버와 중앙 관리 서버 계층화(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS	포트 용도
보조 중앙 관리 서버	13000	klserver	TCP	예	기본 중앙 관리 서버에서 연결 수신

네트워크 세그먼트 및 클라이언트 기기에 연결 게이트웨이가 있는 중앙 관리 서버



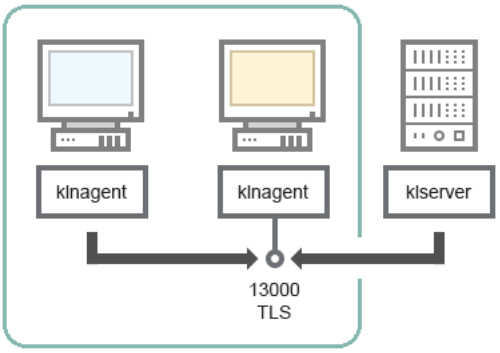
네트워크 세그먼트 및 클라이언트 기기에 연결 게이트웨이가 있는 중앙 관리 서버

스키마 설명은 아래 표를 참조하십시오.

네트워크 세그먼트 및 클라이언트 기기에 연결 게이트웨이가 있는 중앙 관리 서버(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS	포트 용도
중앙 관리 서버	13000	klserver	TCP	예	네트워크 에이전트에서 연결 수신
네트워크 에이전트	13000	klnagent	TCP	예	네트워크 에이전트에서 연결 수신

중앙 관리 서버와 DMZ의 두 기기: 연결 게이트웨이와 클라이언트 기기



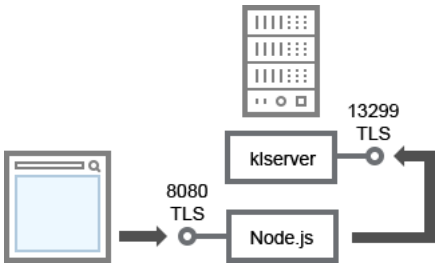
DMZ에 연결 게이트웨이와 클라이언트 기기가 있는 중앙 관리 서버

스키마 설명은 아래 표를 참조하십시오.

네트워크 세그먼트 및 클라이언트 기기에 연결 게이트웨이가 있는 중앙 관리 서버(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS	포트 용도
네트워크 에이전트	13000	klnagent	TCP	예	네트워크 에이전트에서 연결 수신

중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔



중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔

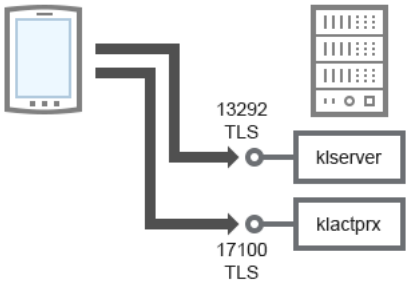
스키마 설명은 아래 표를 참조하십시오.

중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS	포트 용도
중앙 관리 서버	13299	klserver	TCP	예	OpenAPI를 통해 Kaspersky Security Center 웹 콘솔에서 중앙 관리 서버로의 연결 수신
Kaspersky Security Center 웹 콘솔 서버 또는 중앙 관리 서버	8080	Node.js: 서버 측 JavaScript	TCP	예	Kaspersky Security Center 웹 콘솔에서 연결 수신

Kaspersky Security Center 웹 콘솔은 중앙 관리 서버나 다른 기기에 설치할 수 있습니다.

활성화 및 모바일 기기에 있는 보안 제품 관리



활성화 및 모바일 기기에 있는 보안 제품 관리

스키마 설명은 아래 표를 참조하십시오.

활성화 및 모바일 기기에 있는 보안 제품 관리(트래픽)

기기	포트 번호	포트를 여는 프로세스의 이름	프로토콜	TLS	포트 용도
중앙 관리 서버	13292	klserver	TCP	예	관리 콘솔에서 중앙 관리 서버로의 연결 구성 가져오기
중앙 관리 서버	17100	klactprx	TCP	예	모바일 기기에서 애플리케이션 활성화를 위한 연결 수신

배포 모범 사례

Kaspersky Security Center는 배포 방식 애플리케이션입니다. Kaspersky Security Center는 다음과 같은 애플리케이션을 포함합니다:

- 중앙 관리 서버 – 조직의 기기를 관리하고 DBMS에 데이터를 저장하는 데 사용되는 핵심 구성 요소입니다.
- 관리 콘솔 – 관리자를 위한 기본적인 도구입니다. 관리 콘솔은 중앙 관리 서버와 함께 제공되지만 관리자가 실행하는 기기 한 대나 여러 대에 개별적으로 설치할 수도 있습니다.
- 네트워크 에이전트 – 기기에 설치된 보안 제품을 관리하고 해당 기기에 대한 정보를 받아 이를 중앙 관리 서버로 전송하도록 설계되었습니다. 네트워크 에이전트는 조직의 기기에 설치됩니다.

다음과 같은 방식으로 조직 네트워크에서 Kaspersky Security Center 배포를 수행합니다:

- 중앙 관리 서버 설치
- 관리자의 기기에 관리 콘솔 설치
- 기업 기기에 네트워크 에이전트 및 보안 제품 설치

강화 가이드

Kaspersky Security Center는 조직 네트워크의 기본 관리 및 유지 관리 작업의 중앙 집중식 실행을 위해 설계되었습니다. 이 애플리케이션은 조직의 세부 네트워크 보안 수준 정보에 대한 관리자 액세스를 제공합니다. Kaspersky Security Center Kaspersky 애플리케이션을 사용하여 구축한 모든 보호 구성 요소를 구성할 수 있습니다.

Kaspersky Security Center 중앙 관리 서버는 클라이언트 기기의 보호 관리에 대한 전체 액세스 권한이 있으며, 조직의 보안 시스템에서 가장 중요한 구성 요소입니다. 따라서 중앙 관리 서버에 대한 수준 높은 보호 방식이 필요합니다.

구성하기 전에, 중앙 관리 서버 데이터 백업 작업이나 klbackup 유틸리티를 사용하여 Kaspersky Security Center 중앙 관리 서버 백업 복사본을 생성하고 안전한 위치에 저장합니다.

강화 가이드는 보안 문제 발생 위험을 줄이기 위한 Kaspersky Security Center 및 해당 구성 요소 구성의 권장 사항 및 기능을 설명합니다.

강화 가이드는 다음 정보를 포함합니다:

- 중앙 관리 서버 아키텍처 선택
- 중앙 관리 서버에 대한 보안 연결 구성
- 중앙 관리 서버에 액세스하도록 계정 구성
- 중앙 관리 서버의 보호 관리
- 클라이언트 기기의 보호 관리
- 관리 중인 애플리케이션에 대한 보호 구성
- 중앙 관리 서버 점검
- 타사 애플리케이션으로 정보 전송
- 타사 정보 시스템에 대한 보안 권장 사항

중앙 관리 서버 배포

중앙 관리 서버 아키텍처

일반적으로 보호 기기의 위치, 인접 네트워크에서의 액세스, 데이터베이스 업데이트 전달 방식 등에 따라 중앙 집중식 관리 아키텍처의 선택이 달라집니다.

아키텍처 개발의 초기 단계에서 Kaspersky Security Center 구성 요소와 구성 요소 간의 상호 작용, 데이터 트래픽 및 포트 사용에 대한 스키마를 숙지할 것을 권장합니다.

이 정보를 기반으로 다음을 지정하는 아키텍처를 구성할 수 있습니다:

- 중앙 관리 서버 위치 및 네트워크 연결
- 관리자의 작업 공간 구성, 그리고 중앙 관리 서버에 연결하는 방법
- 네트워크 에이전트 및 보호 소프트웨어의 배포 방법
- 배포 지점 사용
- 가상 중앙 관리 서버 사용

- 중앙 관리 서버의 계층 구조 사용
- 안티 바이러스 데이터베이스 업데이트 구성
- 기타 정보 흐름

중앙 관리 서버 설치를 위한 기기 선택

조직 인프라의 전용 서버에 중앙 관리 서버를 설치할 것을 권장합니다. 서버에 다른 타사 소프트웨어가 설치되어 있지 않다면, 타사 소프트웨어 요구 사항에 무관하게 Kaspersky Security Center 요구 사항에 따라 보안 설정을 구성할 수 있습니다.

물리적 서버 또는 가상 서버에 중앙 관리 서버를 배포할 수 있습니다. 선택한 기기가 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인하십시오.

중앙 관리 서버 위치

중앙 관리 서버에서 관리하는 기기는 다음과 같이 찾을 수 있습니다:

- 근거리 통신망(LAN)에서
- 인터넷에서
- DMZ(완충 지역)에서

또한, 중앙 관리 서버는 산업, 기업, DMZ 세그먼트 등의 다른 세그먼트에 있을 수도 있습니다.

Kaspersky Security Center를 사용하여 격리된 네트워크 세그먼트의 보호를 관리한다면, DMZ(완충 지대) 세그먼트에 중앙 관리 서버를 배포할 것을 권장합니다. 이를 통해 네트워크 세분화를 적절하게 구성하고 보호된 세그먼트로의 트래픽 흐름을 최소화하면서 전체 관리 기능 및 업데이트 전달을 유지할 수 있습니다.

도메인 컨트롤러, 터미널 서버 또는 사용자 기기에 중앙 관리 서버 배포 제한

도메인 컨트롤러, 터미널 서버, 사용자 기기에 중앙 관리 서버를 설치하는 것은 권장하지 않습니다.

네트워크 키 노드를 기능적으로 분리하는 것을 권장합니다. 이 접근 방식을 사용하면 노드 오동작이나 손상 시에도 다른 시스템의 작동성을 유지할 수 있습니다. 또한, 각 노드에 대해 서로 다른 보안 정책을 생성할 수 있습니다.

예를 들어 도메인 컨트롤러에 일반적으로 적용되는 보안 제한에 따라 중앙 관리 서버의 성능이 크게 저하되고 일부 중앙 관리 서버 기능을 사용할 수 없게 될 수 있습니다. 침입자가 도메인 컨트롤러에 대한 액세스 권한을 얻으면 AD DS(Active Directory 도메인 서비스) 데이터베이스가 수정, 손상, 파괴될 수 있습니다. 또한 Active Directory에서 관리하는 모든 시스템과 계정이 손상될 수 있습니다.

중앙 관리 서버 설치 및 실행을 위한 계정

도메인 계정을 사용하여 중앙 관리 서버 데이터베이스에 액세스하지 않으려면 로컬 관리자 계정으로 중앙 관리 서버 설치를 실행할 것을 권장합니다. 필요한 계정 집합과 해당 권한은 선택한 DBMS 유형, DBMS 위치, 중앙 관리 서버 데이터베이스 생성 방법에 따라 다릅니다.

Kaspersky Security Center를 설치하는 동안 KLAdmins 및 KLOperators 그룹이 자동으로 만들어집니다. 이 그룹에는 중앙 관리 서버에 연결하고 중앙 관리 서버 개체를 사용할 수 있는 권한이 주어집니다.

Kaspersky Security Center 설치에 사용된 계정 유형에 따라 다음과 같이 KLAdmins 및 KLOperators 그룹이 만들어집니다:

- 도메인에 포함된 사용자 계정으로 애플리케이션을 설치했다면, 중앙 관리 서버를 포함하는 도메인과 중앙 관리 서버 기기에 그룹이 만들어집니다.
- 시스템 계정으로 애플리케이션을 설치했다면, 중앙 관리 서버 기기에만 그룹이 만들어집니다.

도메인에 KLAdmins 및 KLOperators 그룹을 생성하지 않고 결과적으로 **중앙 관리 서버를 관리할 수 있는 권한을 중앙 관리 서버 기기 외부의 계정에 제공**하려면, 로컬 계정으로 Kaspersky Security Center를 설치할 것을 권장합니다.

중앙 관리 서버 설치 시, 서비스로 중앙 관리 서버를 시작하는 데 사용할 계정을 선택합니다. 기본적으로 애플리케이션을 중앙 관리 서버 서비스(klserver 서비스)가 실행되는 KL-AK-*라는 로컬 계정을 만듭니다.

필요하다면 선택한 계정으로 중앙 관리 서버 서비스를 실행할 수 있습니다. 이 계정에 DBMS에 액세스하는 데 필요한 권한을 부여해야 합니다. 보안상의 이유로, 권한이 없는 계정을 사용하여 중앙 관리 서버 서비스를 실행하십시오.

잘못된 계정 설정을 사용하지 않으려면 계정을 자동 생성할 것을 권장합니다.

도메인에서 중앙 관리 서버 제외

중앙 관리 서버로 시스템 중요도가 높은 기기 그룹을 보호한다면, 중앙 관리 서버 기기를 도메인에 포함하지 않을 것을 권장합니다. 이를 통해 Kaspersky Security Center 관리 권한을 구별하고 도메인 계정이 손상되었을 때 중앙 관리 서버에 대한 액세스를 방지할 수 있습니다.

작업 그룹에 포함된 기기에 중앙 관리 서버를 설치한다면, 다음 중앙 관리 서버 작업 시나리오는 사용할 수 없습니다.

- Kaspersky Security Center 장애 조치 클러스터 사용
- Windows Server 장애 조치 클러스터 사용
- 별도의 기기에서 Windows용 SQL Server 사용

  중앙 관리 서버와 SQL Server가 같은 도메인 또는 신뢰할 수 있는 도메인에 있을 경우에만 별도의 기기에서 Windows용 SQL Server를 사용할 수 있습니다. 중앙 관리 서버, SQL Server 및 백업용 UNC 공유가 작업 그룹에 있을 경우 SQL Server와 공유 사이에 액세스 및 읽기-쓰기 권한을 안전하게 설정할 수 없습니다.
- Active Directory 그룹 정책을 통해 중앙 관리 서버 도구를 사용하여 원격 설치

Active Directory 도메인에서 중앙 관리 서버의 연결을 해제해야 한다면, Kaspersky Security Center 이름 변경 방법 주제의 단계를 따릅니다.

작업 그룹에 포함된 기기에 중앙 관리 서버를 설치해야 한다면, Kaspersky Security Center Windows 대신 Kaspersky Security Center Linux를 사용할 수도 있습니다.

연결 안전

TLS 사용

중앙 관리 서버에 대해 안전하지 않은 연결을 금지할 것을 권장합니다. 예를 들어 중앙 관리 서버 설정에서 HTTP를 사용하는 연결을 금지할 수 있습니다.

중앙 관리 서버의 여러 HTTP 포트는 기본적으로 닫혀 있습니다. 나머지 포트는 중앙 관리 서버 웹 서버(8060)에 사용됩니다. 이 포트는 중앙 관리 서버 기기의 방화벽 설정에 따라 제한될 수 있습니다.

엄격한 TLS 설정

버전 1.2 이상의 TLS 프로토콜을 사용하고, 안전하지 않은 암호화 알고리즘은 제한하거나 금지할 것을 권장합니다.

중앙 관리 서버에서 사용하는 암호화 프로토콜(TLS)을 구성할 수 있습니다. 중앙 관리 서버 버전 출시 시점에 안전한 데이터 전송 보장을 위해 기본적으로 암호화 프로토콜 설정이 구성되어 있습니다.

Windows 계정을 이용한 원격 인증 금지

LP_RestrictRemoteOsAuth 플래그를 사용하여 원격 주소에서 SSPI 연결을 금지할 수 있습니다. 이 플래그를 사용하면 로컬 또는 도메인 Windows 계정을 사용하여 중앙 관리 서버에서 원격 인증을 금지할 수 있습니다.

LP_RestrictRemoteOsAuth 플래그를 원격 주소로부터의 연결을 금지하는 모드로 전환하려면:

1. 관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

2. 명령줄에서 다음 명령을 실행하여 LP_RestrictRemoteOsAuth 플래그 값을 지정합니다.

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. 중앙 관리 서버 서비스를 다시 시작합니다.

중앙 관리 서버 기기에 설치된 Kaspersky Security Center 웹 콘솔 또는 관리 콘솔을 통해 원격 인증을 수행한다면, LP_RestrictRemoteOsAuth 플래그가 작동하지 않습니다.

중앙 관리 서버 데이터베이스에 대한 액세스 제한

중앙 관리 서버 데이터베이스에 대한 액세스를 제한할 것을 권장합니다. 예를 들어 중앙 관리 서버 기기에서만 액세스 권한을 부여합니다. 이렇게 하면 알려진 취약점을 통해 중앙 관리 서버 데이터베이스가 손상될 가능성이 줄어듭니다.

사용된 데이터베이스의 작동 지침에 따라 파라미터를 구성하고 방화벽에 닫힌 포트를 제공할 수 있습니다.

Microsoft SQL Server 인증

Kaspersky Security Center가 Microsoft SQL Server를 DBMS로 사용한다면, 데이터베이스와 주고받는 Kaspersky Security Center 데이터 및 데이터베이스에 저장된 데이터를 무단 액세스로부터 보호해야 합니다. 이를 위해 Kaspersky Security Center와 SQL Server간의 통신을 안전하게 보호해야 합니다. 안전한 통신을 제공하는 가장 안정적인 방법은 동일한 기기에 Kaspersky Security Center와 SQL Server를 설치하고 두 애플리케이션에 공유 메모리 메커니즘을 사용하는 것입니다. 그 외에는 SSL/TLS 인증서를 사용하여 SQL Server 인스턴스를 인증할 것을 권장합니다.

일반적으로 중앙 관리 서버는 다음 공급자를 통해 SQL Server의 주소를 지정할 수 있습니다.

- TCP/IP 또는 Named Pipes를 사용하는 SQLOLEDB

  이 공급자는 Windows 운영 체제에 설치되며 기본값으로 사용됩니다.

- TCP/IP, Named Pipes, Shared memory를 사용하는 MSOLEDBSQL

  이 공급자를 사용하려면 중앙 관리 서버가 설치된 기기에 이를 설치 한 후, 전역 환경 변수 `KLDBADO_UseMSOLEDBSQL`의 값을 `1`로 설정해야 합니다.

- TCP/IP, Named Pipes, Shared memory를 사용하는 MSOLEDBSQL19

  이 공급자를 사용하려면 중앙 관리 서버가 설치된 기기에 이를 설치 한 후, 전역 환경 변수 `KLDBADO_UseMSOLEDBSQL`의 값을 `1`로 설정하고 전역 환경 변수 `KLDBADO_ProviderName`의 값을 `MSOLEDBSQL19`로 설정해야 합니다.

또한 TCP/IP, Named Pipes, Shared memory를 사용하기 전에 필요한 프로토콜이 활성화되어 있는지 확인하십시오.

외부 DBMS와 보안 상호 작용

중앙 관리 서버(외부 DBMS) 설치 시 별도의 기기에 DBMS를 설치하면, 이 DBMS와의 안전한 상호 작용 및 인증을 위해 파라미터를 구성하는 것이 좋습니다. SSL 인증 구성에 대한 자세한 내용은 PostgreSQL 서버 인증 및 시나리오: MySQL 서버 인증을 참조하십시오.

중앙 관리 서버에 연결할 IP 주소의 허용 목록 구성

기본적으로 Kaspersky Security Center 사용자는 MMC 기반 관리 콘솔, Kaspersky Security Center 웹 콘솔 또는 OpenAPI 애플리케이션이 설치된 모든 기기에서 Kaspersky Security Center에 로그인할 수 있습니다. 사용자가 IP 주소가 허용된 기기에서만 연결할 수 있도록 중앙 관리 서버를 구성할 수 있습니다. 예를 들어 침입자가 허용 목록에 포함되지 않은 기기에 설치된 Kaspersky Security Center 웹 콘솔 서버를 통해 Kaspersky Security Center에 연결하려고 할 경우, Kaspersky Security Center에 로그인할 수 없습니다.

Kaspersky Security Center 웹 콘솔에 연결할 IP 주소의 허용 목록 구성

기본적으로 Kaspersky Security Center 사용자는 모든 기기에서 Kaspersky Security Center 웹 콘솔에 연결할 수 있습니다. Kaspersky Security Center 웹 콘솔이 설치된 기기에서 사용자는 허용된 IP 주소에서만 Kaspersky Security Center 웹 콘솔 에 연결할 수 있도록 방화벽(운영 체제 또는 타사 운영 체제에 내장된 방화벽)을 구성해야 합니다.

검색 중 도메인 컨트롤러 연결의 보안

중앙 관리 서버 또는 Linux 배포 지점은 LDAPS를 통해 도메인 컨트롤러에 연결하여 도메인을 검색합니다. 연결 시 인증서 확인은 기본적으로 불필요합니다. 인증서 확인을 강제 실행하려면 `KLNAG_LDAP_TLS_REQCERT` 플래그를 1로 설정합니다. 인증 기관(CA)에 대한 사용자 지정 경로를 지정하여 `KLNAG_LDAP_SSL_CACERT` 플래그를 사용하여 인증서 체인에 접근할 수도 있습니다.

계정 및 인증

아래 단계를 구성하기 전에 중앙 관리 서버 데이터 백업 작업 또는 klbackup 유틸리티를 사용하여 Kaspersky Security Center 중앙 관리 서버 백업 복사본을 생성한 다음 안전한 위치에 저장합니다.

중앙 관리 서버에서 2단계 인증 사용

Kaspersky Security Center는 RFC 6238 표준(TOTP: Time-Based One-Time Password 알고리즘)을 기반으로 Kaspersky Security Center 웹 콘솔 및 관리 콘솔 사용자를 위한 **2단계 인증**을 제공합니다.

사용자 계정에 2단계 인증이 활성화되면, Kaspersky Security Center 웹 콘솔 또는 관리 콘솔에 로그인할 때마다 사용자 이름, 암호, 추가 일회용 보안 코드를 입력해야 합니다. 계정에 도메인 인증을 사용하는 경우 추가 일회용 보안 코드만 입력하면 됩니다. 일회용 보안 코드를 받으려면 컴퓨터나 모바일 기기에 인증 앱을 설치해야 합니다.

RFC 6238 표준을 지원하는 소프트웨어 및 하드웨어 인증자(토큰)가 있습니다. 예를 들어 소프트웨어 인증자에는 Google Authenticator, Microsoft Authenticator, FreeOTP 등이 있습니다.

중앙 관리 서버 연결이 설정된 기기에는 인증 앱 설치를 권장하지 않습니다. 모바일 기기에 인증 앱을 설치할 수 있습니다.

신규 사용자가 2단계 인증을 설정하지 못하도록 제한

Kaspersky Security Center 웹 콘솔 접근 보안을 더욱 강화하기 위해 다음 조치를 수행할 수 있습니다.

신규 사용자가 2단계 인증을 설정하지 못하도록 제한.

이 옵션이 활성화되면 새 도메인 관리자 등 2단계 인증이 비활성화된 사용자는 직접 2단계 인증을 구성할 수 없습니다. 따라서 이러한 사용자는 이미 2단계 인증을 활성화한 다른 Kaspersky Security Center 관리자의 승인 없이는 중앙 관리 서버에서 인증을 받을 수 없으며 Kaspersky Security Center 웹 콘솔에 로그인할 수 없습니다.

운영 체제에 2단계 인증 사용

중앙 관리 서버 기기 인증에 토큰, 스마트카드 또는 기타 방법(가능할 시)을 통한 다단계 인증(MFA)을 사용할 것을 권장합니다.

관리자 암호 저장 제한

관리 콘솔을 사용한다면, 관리 서버 연결 대화 상자에 관리자 암호를 저장하는 것은 권장하지 않습니다.

Kaspersky Security Center 웹 콘솔을 사용한다면, 사용자 기기에 설치된 브라우저에 관리자 암호를 저장하는 것은 권장하지 않습니다.

내부 사용자 계정 인증

기본적으로 중앙 관리 서버의 내부 사용자 계정 암호는 다음 규칙을 따라야 합니다.

- 암호는 8자에서 256자 사이여야 합니다.
- 암호는 아래에 나와 있는 그룹 중 3개 이상의 문자를 포함해야 합니다:
  - 대문자(A-Z)
  - 소문자(a-z)
  - 숫자(0-9)
  - 특수 문자(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 암호는 공백, 유니코드 문자 또는 "." 및 "@"의 조합("."이 "@" 앞에 오는 경우)을 포함할 수 없습니다.

기본적으로 암호를 입력할 수 있는 최대 시도 횟수는 10회입니다. 암호 입력 시도 허용 횟수를 변경할 수 있습니다.

Kaspersky Security Center 사용자는 유효하지 않은 암호를 제한된 횟수만큼만 입력할 수 있습니다. 이 제한에 도달하면 사용자 계정은 1시간 동안 잠깁니다.

내부 사용자 계정의 암호 변경 옵션 구성

내부 사용자 계정의 암호 변경에 대해 다음 옵션을 구성하는 것이 좋습니다.

- 암호 순환 기간
- 암호 변경의 필요성에 대한 이전 경고 시간
- **첫 로그인 시 암호를 변경해야 합니다** 옵션의 값

무단 수정으로부터 계정 보호

중앙 관리 서버의 내부 사용자 계정을 무단으로 수정하지 못하도록 보호하려면 추가 옵션을 활성화하는 것이 좋습니다. 이 보호는 내부 사용자마다 하나씩 별도로 구성해야 합니다.

중앙 관리 서버 전용 관리 그룹

중앙 관리 서버 전용 관리 그룹 생성을 권장합니다. 이 그룹에 특별한 액세스 권한을 부여하고 특별한 보안 정책을 만듭니다.

중앙 관리 서버의 보안 수준을 의도적으로 낮추지 않으려면 전용 관리 그룹을 관리할 수 있는 계정 목록을 제한할 것을 권장합니다.

KLAdmins 및 KLOperators 그룹

Kaspersky Security Center를 설치하는 동안 KLAdmins 및 KLOperators 그룹이 자동으로 만들어집니다. KLAdmins 그룹에는 모든 액세스 권한이 부여됩니다. KLOperators 그룹에는 읽기 및 실행 권한만 부여됩니다. KLAdmins 그룹에 부여된 권한은 **잠겨** 있습니다.

KLAdmins 및 KLOperators 그룹을 보고 운영 체제의 표준 관리 도구를 사용하여 이 그룹을 변경할 수 있습니다.

중앙 관리 서버 작업을 위한 규정을 개발할 때, 정보 보안 전문가가 표준 작업을 수행하기 위해 전체 액세스 권한(및 KLAdmins 그룹에 포함)이 필요한지 결정해야 합니다.

대부분의 기본 관리 작업은 회사 부서(또는 동일한 부서의 다른 직원) 간에 분산될 수 있으며 결과적으로 서로 다른 계정 간에 분산될 수 있습니다. Kaspersky Security Center에서 관리 그룹 액세스 차별화를 설정할 수도 있습니다. 결과적으로 KLAdmins 그룹의 계정에 대한 권한 부여가 비정상적이며 인시던트로 간주할 수 있는 시나리오를 구현하는 것도 가능합니다.

Kaspersky Security Center를 시스템 계정으로 설치했다면 중앙 관리 서버 기기에서만 그룹이 생성됩니다. 이때는 Kaspersky Security Center 설치 중에 생성된 항목만 그룹에 포함하도록 할 것을 권장합니다. Kaspersky Security Center 설치 중에 자동 생성되는 KLAdmins 그룹(로컬 및/또는 도메인)에 그룹을 추가하는 것은 권장하지 않습니다. 이 그룹의 변경 권한도 제한해야 합니다. KLAdmins 그룹은 권한이 없는 단일 계정만 포함해야 합니다.

도메인 사용자 계정으로 설치를 진행했다면 중앙 관리 서버와 중앙 관리 서버가 포함된 도메인 모두에 KLAdmins 및 KLOperators 그룹이 생성됩니다. 로컬 계정 설치와 같은 유사한 접근 방식을 권장합니다.

기본 관리자 역할 구성원 자격 제한

주 관리자 역할 멤버 자격을 제한할 것을 권장합니다.

중앙 관리 서버 설치 후 기본 관리자 역할은 기본적으로 로컬 관리자 그룹 및 생성된 KLAdmins 그룹에 할당됩니다. 이는 관리에 유용하지만 보안 관점에서는 치명적입니다. 기본 관리자 역할의 권한은 광범위하므로 이 역할을 사용자에게 할당하는 것을 엄격하게 규제해야 합니다.

Kaspersky Security Center의 관리자 권한이 있는 사용자 목록에서 로컬 관리자를 제외할 수 있습니다. 기본 관리자 역할은 KLAdmins 그룹에서 제거할 수 없습니다. 중앙 관리 서버를 관리하는 데 사용할 계정을 KLAdmins 그룹에 포함할 수 있습니다.

도메인 인증을 사용한다면 Kaspersky Security Center에서 도메인 관리자 계정의 권한을 제한할 것을 권장합니다. 이러한 계정에는 기본적으로 기본 관리자 역할이 있습니다. 또한 도메인 관리자는 자신의 계정을 KLAdmins 그룹에 포함하여 주 관리자 역할을 얻을 수 있습니다. 이를 방지하기 위해 Kaspersky Security Center 보안 설정에서 Domain Admins 그룹을 추가한 다음 금지 규칙을 정의할 수 있습니다. 이러한 규칙은 허용 규칙보다 우선해야 합니다.

이미 구성된 권한 세트와 함께 미리 정의된 사용자 역할을 사용할 수도 있습니다.

애플리케이션 기능에 대한 접근 권한 구성

각 사용자 또는 사용자 그룹에 대해 Kaspersky Security Center의 기능에 대한 접근 권한을 유연하게 구성할 것을 권장합니다.

역할 기반 액세스 제어를 사용하면 사전 정의된 권한 집합이 있는 표준 사용자 역할을 생성하고 임무 범위에 따라 해당 역할을 사용자에게 할당할 수 있습니다.

역할 기반 액세스 제어 모델의 주요 이점:

- 관리 용이성
- 역할 계층
- 최소 권한 접근 방식
- 직무 분리

위치에 따라 특정 직원에게 기본 제공 역할을 할당하거나 완전히 새로운 역할을 만들 수 있습니다.

역할을 구성하는 동안, 중앙 관리 서버 기기의 보호 상태 변경 및 타사 소프트웨어의 원격 설치와 관련된 권한에 주의하십시오.

- 관리 그룹 관리.
- 중앙 관리 서버 작업.
- 원격 설치.
- 이벤트 저장 및 알림 전송을 위한 파라미터 변경.

  이 권한을 사용하면 이벤트가 발생할 때 중앙 관리 서버 기기에서 스크립트 또는 실행 가능한 모듈을 실행하는 알림을 설정할 수 있습니다.

애플리케이션 원격 설치를 위한 별도 계정

기본적인 접근 권한 차등화 외에도, 모든 계정(메인 관리자나 다른 특수 계정은 제외)에 대해 애플리케이션 원격 설치를 제한할 것을 권장합니다.

애플리케이션의 원격 설치를 위해 별도의 계정을 사용할 것을 권장합니다. 별도의 계정에 역할이나 권한을 할당할 수 있습니다.

Windows 권한이 있는 액세스 보안

권한 있는 액세스 보안 제공을 위한 Microsoft의 권장 사항을 고려할 것을 권장합니다. 이러한 권장 사항을 보려면 권한 있는 액세스 보안 문서로 이동하십시오.

PAW(Privileged Access Workstations) 구현은 핵심 권장 사항 중 하나입니다.

관리 서비스 계정(MSA) 또는 그룹 관리 서비스 계정(gMSA)을 사용하여 중앙 관리 서버 서비스 실행

Active Directory에는 서비스를 안전하게 실행하기 위한 MSA/gMSA(그룹 관리 서비스 계정)라는 특별한 계정 유형이 있습니다. Kaspersky Security Center는 MSA(관리 서비스 계정)와 gMSA(그룹 관리 서비스 계정)를 지원합니다. 이러한 유형의 계정이 사용자 도메인에서 사용되면 중앙 관리 서버 서비스용 계정으로 그 중 하나를 선택할 수 있습니다.

모든 사용자 및 사용자 작업에 대한 정기 감사

중앙 관리 서버 기기의 모든 사용자를 정기적으로 감사할 것을 권장합니다. 이를 통해 기기 손상과 관련된 특정 유형의 보안 위협에 대응할 수 있습니다.

또한 중앙 관리 서버에 대한 연결 및 연결 해제, 중앙 관리 서버에 오류가 발생한 연결, 개체 수정(리비전 관리를 지원하는 개체의 경우)과 같은 사용자 작업을 추적할 수 있습니다.

중앙 관리 서버의 보호 관리

중앙 관리 서버 보호 소프트웨어 선택

중앙 관리 서버 배포 유형 및 일반 보호 전략에 따라 중앙 관리 서버 기기를 보호할 애플리케이션을 선택합니다.

전용 기기에 중앙 관리 서버를 배포한다면, Kaspersky Endpoint Security 애플리케이션을 선택하여 중앙 관리 서버 기기를 보호하는 것이 좋습니다. 이를 통해 행동 분석 모듈 등 사용 가능한 모든 기술을 적용하여 중앙 관리 서버 기기를 보호할 수 있습니다.

인프라에 존재하고 이전에 다른 작업에 사용된 기기에 중앙 관리 서버를 설치했다면, 다음 보호 소프트웨어를 고려할 것을 권장합니다.

- Kaspersky Industrial CyberSecurity for Nodes. 산업 네트워크에 포함된 기기에 이 애플리케이션을 설치하는 것이 좋습니다. Kaspersky Industrial CyberSecurity for Nodes는 다양한 산업용 소프트웨어 제조업체와의 호환성 인증서를 보유한 애플리케이션입니다.

- 권장 보안 솔루션. 기기에 다른 소프트웨어와 함께 중앙 관리 서버를 설치했다면, 보안 솔루션의 호환성에 대한 해당 소프트웨어 공급업체의 권장 사항을 고려할 것을 권장합니다(보안 솔루션 선택에 대한 권장 사항이 이미 있을 수 있으며, 신뢰 영역을 구성해야 할 수도 있습니다).

보호 애플리케이션에 대한 별도의 보안 정책 생성

중앙 관리 서버 기기를 보호하는 애플리케이션에 대해 별도의 보안 정책을 만드는 것을 권장합니다. 이 정책은 클라이언트 기기에 대한 보안 정책과 달라야 합니다. 이렇게 하면 다른 기기의 보호 수준에 영향을 주지 않고 중앙 관리 서버에 가장 적합한 보안 설정을 지정할 수 있습니다.

기기를 그룹으로 나눈 후, 특별한 보안 정책을 만들 수 있는 별도의 그룹에 중앙 관리 서버 기기를 배치할 것을 권장합니다.

보호 모듈

중앙 관리 서버가 있는 기기에 설치한 타사 소프트웨어 공급업체의 특별한 권장 사항이 없다면, 사용 가능한 모든 보호 모듈을 활성화하고 구성할 것을 권장합니다(어느 정도 해당 보호 모듈의 작동을 확인한 후).

중앙 관리 서버 기기의 방화벽 구성

중앙 관리 서버 기기에서 관리자가 중앙 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 통해 중앙 관리 서버에 연결할 수 있는 기기 수를 제한하도록 방화벽을 구성할 것을 권장합니다.

기본적으로 중앙 관리 서버는 포트 13291을 사용하여 관리 콘솔에서 연결을 수신하고, 포트 13299를 사용하여 Kaspersky Security Center 웹 콘솔에서 연결을 수신합니다. 이러한 포트를 사용하여 중앙 관리 서버를 관리할 수 있는 기기 수를 제한할 것을 권장합니다.

클라이언트 기기의 보호 관리

설치 패키지에 라이센스 키 추가 제한

설치 패키지는 중앙 관리 서버 공유 폴더의 Packages 하위 폴더에 저장됩니다. 설치 패키지에 라이센스 키를 추가하면 설치 패키지의 저장소에 대한 공유 읽기 액세스 권한이 활성화되므로 라이센스 키가 손상될 수 있습니다.

라이센스 키 손상 방지를 위해 설치 패키지에 라이센스 키를 추가하지 않을 것을 권장합니다.

관리 중인 기기에 대한 라이센스 키 자동 배포, 관리 중인 애플리케이션 대한 라이센스 키 추가 작업을 통한 배포, 기기에 활성화 코드 또는 키 파일 수동 추가를 사용할 것을 권장합니다.

관리 그룹 간 기기 이동에 대한 자동 규칙

관리 그룹 간 기기 이동에 대한 자동 규칙 사용을 제한할 것을 권장합니다.

기기 이동에 자동 규칙을 사용하면, 이동된 기기에 재배치 전에 있던 것보다 더 많은 권한을 제공하는 정책이 전파될 수 있습니다.

또한, 클라이언트 기기를 다른 관리 그룹으로 이동하면 정책 설정이 전파될 수 있습니다. 이 정책 설정은 게스트 및 신뢰할 수 없는 기기에 배포하는 데 부적합할 수 있습니다.

이 권장 사항은 관리 그룹에 대한 일회성 초기 기기 할당에는 적용되지 않습니다.

배포 지점 및 연결 게이트웨이 보안 요구 사항

네트워크 에이전트가 설치된 기기는 배포 지점 역할을 할 수 있으며 다음 기능을 수행할 수 있습니다:

- 중앙 관리 서버에서 받은 업데이트 및 설치 패키지를 그룹 내의 클라이언트 기기에 배포합니다.
- 클라이언트 기기에서 타사 소프트웨어 및 Kaspersky 애플리케이션의 원격 설치를 수행합니다.
- 네트워크를 검색해서 새로운 기기를 탐지하고 기존 기기에 대한 정보를 업데이트합니다. 배포 지점은 중앙 관리 서버와 같은 기기 검색 방법을 사용할 수 있습니다.

다음에 사용되는 조직의 네트워크에 배포 지점 배치:

- 중앙 관리 서버의 부하 감소
- 트래픽 최적화
- 네트워크의 연결하기 어려운 부분에 있는 기기에 대한 중앙 관리 서버 액세스 제공

사용 가능한 기능을 고려하여 모든 유형의 무단 액세스(물리적 액세스 포함)로부터 배포 지점 역할을 하는 기기를 보호할 것을 권장합니다.

배포 지점 자동 할당 제한

관리를 간소화하고 네트워크 운용성을 유지하려면 배포 지점의 자동 할당을 사용할 것을 권장합니다. 그러나 산업 네트워크 및 소규모 네트워크는 배포 지점을 자동으로 할당하지 않을 것을 권장합니다. 원격 설치 작업을 추진하는 데 사용되는 계정의 개인 정보 등이 운영 체제를 통해 배포 지점으로 전송될 수 있기 때문입니다.

산업 네트워크 및 소규모 네트워크에서는 배포 지점으로 작동할 기기를 수동 할당할 수 있습니다.

배포 지점 활동에 대한 보고서도 볼 수 있습니다.

Kaspersky Security Center 사용자 기기에 대한 보안 요구 사항

Kaspersky Security Center 사용자의 기기에는 특수한 보안 요구 사항을 적용해야 합니다. 모든 유형의 무단 접근(물리적 접근 포함)으로부터 이러한 기기를 보호하는 것이 좋습니다.

Kaspersky Security Center 사용자 기기에는 다음이 포함됩니다.

- 사용자가 브라우저를 사용하여 Kaspersky Security Center 웹 콘솔에 연결하는 기기.
- 사용자가 MMC 기반 관리 콘솔을 사용하여 Kaspersky Security Center에 연결하는 기기.
- OpenAPI를 통해 중앙 관리 서버와 상호 작용하는 애플리케이션이 Kaspersky Security Center에 연결되는 기기.

Kaspersky Security Center 웹 콘솔이 설치된 기기의 보안 요구 사항

Kaspersky Security Center 웹 콘솔이 설치된 기기는 Kaspersky Security Center를 관리하는 데 사용되므로, 이러한 기기의 보안에는 특수한 요구 사항을 적용해야 합니다. 모든 유형의 무단 접근(물리적 접근 포함)으로부터 이러한 기기를 보호하는 것이 좋습니다.

관리 중인 애플리케이션에 대한 보호 구성

관리 중인 애플리케이션 정책

Kaspersky Security Center(네트워크 에이전트, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent 등)에서 사용 중인 애플리케이션 및 구성 요소 유형별로 정책을 생성할 것을 권장합니다. 이 정책은 모든 관리 중인 기기(루트 관리 그룹) 또는 구성된 이동 규칙에 따라 새 관리 중인 기기가 자동 이동되는 별도의 그룹에 적용해야 합니다.

보호 비활성화 및 애플리케이션 제거를 위한 암호 지정

침입자가 Kaspersky 보안 애플리케이션을 비활성화하지 못하도록, 보호 비활성화 및 Kaspersky 보안 애플리케이션 제거에 대한 암호 보호를 활성화할 것을 강력히 권장합니다. 예를 들어 Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Servers, 네트워크 에이전트 및 기타 Kaspersky 애플리케이션에 대한 암호를 설정할 수 있습니다. 암호 보호를 활성화한 후 "자물쇠"를 닫아 이러한 설정을 잠그는 것이 좋습니다.

클라이언트 기기를 중앙 관리 서버에 수동으로 연결하기 위한 암호 지정(klmover 유틸리티)

klmover 유틸리티를 사용하면 클라이언트 기기를 중앙 관리 서버에 수동으로 연결할 수 있습니다. 클라이언트 기기에 네트워크 에이전트를 설치할 때 이 유틸리티가 네트워크 에이전트 설치 폴더에 자동으로 복사됩니다.

침입자가 중앙 관리 서버의 제어권 밖으로 기기를 이동하는 것을 방지하려면 klmover 유틸리티 실행 시 암호 보호를 활성화하는 것이 좋습니다. 암호 보호를 활성화하려면 네트워크 에이전트 정책 설정에서 **제거 암호 사용** 옵션을 선택하세요.

klmover 유틸리티에는 로컬 관리자 권한이 필요합니다. 로컬 관리자 권한 없이 작동하는 기기는 klmover 유틸리티 실행을 위한 암호 보호를 생략할 수 있습니다.

제거 암호 사용 옵션을 활성화하면 클리너 도구(cleaner.exe)에 대한 암호 보호도 활성화됩니다.

Kaspersky Security Network 사용

관리 중인 애플리케이션의 모든 정책과 중앙 관리 서버 속성에서 KSN(Kaspersky Security Network) 사용을 활성화하고 KSN 진술문을 수락할 것을 권장합니다. 중앙 관리 서버를 업데이트하거나 업그레이드할 때, 업데이트된 KSN 진술문을 수락할 수 있습니다. 법률 또는 기타 규정에 따라 클라우드 서비스 사용이 금지된다면, KSN을 비활성화할 수 있습니다.

관리 중인 기기의 정기 검사

모든 기기 그룹에 대해 주기적으로 전체 기기 검사를 실행하는 작업을 생성할 것을 권장합니다.

새 기기 발견

기기 검색 설정을 적절하게 구성할 것을 권장합니다. Active Directory와 통합을 설정하고 새 기기 검색을 위한 IP 주소 범위를 지정하십시오.

보안을 위해 모든 새 기기를 포함하는 기본 관리 그룹과 이 그룹에 영향을 주는 기본 정책을 사용할 수 있습니다.

공유 폴더 선택

기존 공유 폴더(설치 패키지 배치 및 업데이트된 데이터베이스 저장 등에 사용)를 선택하여 Windows를 실행하는 기기에 중앙 관리 서버를 배포한다면, Everyone 그룹에 읽기 권한을, KLAdmins 그룹에 쓰기 권한을 부여할 것을 권장합니다.

중앙 관리 서버 점검

중앙 관리 서버 데이터 사본 백업

데이터 백업을 사용하면 데이터 손실 없이 중앙 관리 서버 데이터를 복원할 수 있습니다.

기본적으로 중앙 관리 서버 설치 후 데이터 백업 작업이 자동 생성되고 주기적으로 실행되어 적절한 디렉터리에 백업이 저장됩니다.

데이터 백업 작업의 설정은 다음과 같이 변경할 수 있습니다.

- 백업 빈도 증가
- 사본을 저장하기 위한 특수 디렉토리 지정
- 백업 복사본의 암호 변경

백업 복사본을 기본 디렉터리와 다른 특수 디렉터리에 저장할 시, 이 디렉터리에 대한 액세스 제어 목록(ACL)을 제한할 것을 권장합니다. 중앙 관리 서버 계정 및 중앙 관리 서버 데이터베이스의 계정에는 이 디렉토리에 대한 쓰기 액세스 권한이 있어야 합니다.

중앙 관리 서버 점검

중앙 관리 서버 점검은 해당 데이터베이스 크기를 줄이고 애플리케이션의 성능과 운영 신뢰성을 개선할 수 있도록 합니다. 중앙 관리 서버는 적어도 매주 한 번은 점검할 것을 권장합니다.

중앙 관리 서버 유지보수는 전용 작업을 통해 수행됩니다. 이 애플리케이션은 중앙 관리 서버 유지보수 시 다음 동작을 수행합니다.

- 오류가 있는지 데이터베이스 체크
- 데이터베이스 인덱스 재편성
- 데이터베이스 통계 업데이트
- 데이터베이스 줄임(필요 시)

운영 체제 업데이트 및 타사 소프트웨어 업데이트 설치

중앙 관리 서버 기기에 정기적으로 운영 체제 및 타사 소프트웨어용 소프트웨어 업데이트를 설치할 것을 권장합니다.

클라이언트 기기는 중앙 관리 서버에 계속 연결할 필요가 없으므로, 업데이트를 설치한 후 중앙 관리 서버 기기를 재부팅해도 안전합니다. 중앙 관리 서버 다운타임 동안 클라이언트 기기에 등록된 모든 이벤트는 연결이 복원된 후에 클라이언트 기기로 전송됩니다.

타사 시스템으로 이벤트 전송

모니터링 및 보고

보안 문제에 대한 적시 대응을 위해 모니터링 및 보고 기능을 구성할 것을 권장합니다.

SIEM 시스템으로 이벤트 내보내기

심각한 피해가 발생하기 전에 사고를 빠르게 감지하려면 SIEM 시스템에서 이벤트 내보내기를 사용할 것을 권장합니다.

감사 이벤트의 이메일 알림

Kaspersky Security Center에서는 관리 중인 기기에 설치된 중앙 관리 서버 및 Kaspersky 애플리케이션의 작동 중 발생한 이벤트 정보를 볼 수 있습니다. 긴급 상황에 적시에 대응하려면 게시하는 감사 이벤트, 중요 이벤트, 실패 이벤트 및 경고에 대한 알림을 보내도록 중앙 관리 서버를 구성할 것을 권장합니다.

이러한 이벤트는 시스템 내 이벤트인 만큼 이벤트 수가 적을 것으로 예상되므로, 메일링에 상당히 적합합니다.

중앙 관리 서버 기능 통계

보안 문제에 적시 대응할 수 있도록 SNMP(단순 네트워크 관리 프로토콜)를 사용하여 중앙 관리 서버 기능의 통계를 타사 애플리케이션으로 전송하도록 구성하는 것이 좋습니다.

타사 정보 시스템에 대한 보안 권장 사항

CIS 벤치마크의 보안 권장 사항

중앙 관리 서버 및 네트워크 에이전트가 지원하는 운영 체제, 가상화 플랫폼, 데이터베이스 서버 버전을 사용한다면, 인터넷 보안 센터(CIS)가 있을 시 최고의 정보 보안 방법을 적용하여 이러한 정보 시스템을 세부적으로 조정할 것을 권장합니다.

인터넷 보안 센터(CIS)는 정보 기술 분야의 보안을 개선하는 비영리 조직입니다. 특히 CIS는 CIS 제어, CIS 벤치마크 등의 안전 표준을 개발, 배포합니다. 이러한 표준은 정보 시스템의 보안을 보장하기 위한 권장 사항 및 사례입니다.

CIS 포털에는 중앙 관리 서버 및 네트워크 에이전트에서 지원하는 다음 정보 시스템 버전의 권장 사항이 포함되어 있습니다.

- 다음 제품군의 운영 체제:
  - 데스크톱용 Windows
  - 서버용 Windows
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware 가상화 플랫폼

- 데이터베이스 서버:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Astra Linux 운영 체제에 대한 보안 권장 사항

Astra Linux 운영 체제를 사용한다면, 해당 Astra Linux의 버전에 대해 Red Book의 보안 권장 사항을 따라야 합니다.

RED OS 운영 체제에 대한 보안 권장 사항

RED OS 운영 체제를 사용한다면 공식 RED OS 설명서에 설명된 관리자 설명서의 보안 권장 사항을 사용해야 합니다.

Kaspersky 보안 애플리케이션 사용 시 권장 사항

Kaspersky Endpoint Security for Windows에서 KLAdmin 암호 사용

컴퓨터 활용 능력 수준이 다른 여러 사용자가 Kaspersky Endpoint Security for Windows가 설치된 기기를 공유할 수 있습니다. 모든 사용자가 Kaspersky Endpoint Security for Windows 및 설정에 제한없이 접근할 수 있다면 전반적인 기기 보호 수준이 저하될 수 있습니다. 암호 보호를 사용하면 사용자에게 부여된 권한(애플리케이션 종료 권한 등)에 따라 사용자의 Kaspersky Endpoint Security for Windows 접근을 제한할 수 있습니다.

Kaspersky Endpoint Security for Windows 및 파라미터에 대한 접근을 제한하는 방법 중에는 KLAdmin 계정 사용도 있습니다. KLAdmin 계정은 Kaspersky Endpoint Security for Windows에 제한 없이 접근할 수 있는 관리자 계정입니다. KLAdmin 계정은 Kaspersky Endpoint Security for Windows에서 암호로 보호된 모든 동작을 수행할 권한이 있습니다. KLAdmin 계정에 대한 권한은 취소할 수 없습니다. Kaspersky Endpoint Security for Windows 정책의 속성에서 KLAdmin 계정의 암호를 설정할 수 있습니다. Kaspersky Endpoint Security for Windows 관리자는 KLAdmin 계정 암호를 안전하게 사용할 책임이 있습니다. 조직에 자체 암호 정책이 있다면 해당 정책의 지침을 따릅니다.

KLAdmin 암호 유출을 방지하고 조직을 보호할 수 있는 권장 사항은 다음과 같습니다.

- **일반적인 요구 사항**
  계정 이름의 일부나 전체를 암호로 사용하지 마십시오.
- **최소 암호 길이 요구 사항**
  10자 이상의 암호를 생성합니다.
- **여러 문자 유형 사용 요구**
  소문자와 대문자, 숫자, 특수 문자 등 다양한 카테고리의 문자를 포함하여 복합 암호를 설정합니다.

- **암호 만료 요구 사항**

  최소 암호 만료 날짜를 90일로 설정합니다. 새 암호는 마지막 24개의 암호와 같을 수 없습니다.

배포 준비

이 섹션에서는 Kaspersky Security Center를 배포하기 전에 수행해야 하는 단계를 설명합니다.

Kaspersky Security Center 배포 계획

이 섹션에서는 다음과 같은 기준에 따라 조직 네트워크에 Kaspersky Security Center 구성 요소를 배포하기 위한 가장 편리한 옵션 정보를 제공합니다:

- 총 기기 개수
- 조직/지역별로 분리된 단위(지역 사무소, 지사)
- 협채널을 통해 연결되는 개별 네트워크
- 중앙 관리 서버에 대한 인터넷 접속 필요

일반적인 보호 시스템 배포 구성

이 섹션에서는 Kaspersky Security Center를 사용하여 회사 네트워크에 보호 시스템을 배포하는 표준 구성을 설명합니다.

시스템은 모든 유형의 비인가 접근으로부터 보호되어야 합니다. 기기에 애플리케이션을 설치하기 전에 운영 체제용으로 제공되는 모든 보안 업데이트를 설치하고 중앙 관리 서버와 배포 지점을 물리적으로 보호하는 것이 좋습니다.

다음 배포 구성을 사용하면 Kaspersky Security Center를 사용하여 회사 네트워크에 보호 시스템을 배포할 수 있습니다:

- 다음 방법 중 하나로 Kaspersky Security Center를 통해 보호 시스템 배포:
  - 관리 콘솔을 통해
  - Kaspersky Security Center 웹 콘솔을 통해

  Kaspersky 애플리케이션은 Kaspersky Security Center를 사용하여 클라이언트 기기에 자동으로 설치되며, 설치가 완료되면 중앙 관리 서버에 자동으로 연결됩니다.

  기본 배포 구성은 관리 콘솔을 통해 보호 시스템을 배포하는 것입니다. Kaspersky Security Center 웹 콘솔을 사용하면 브라우저에서 Kaspersky 애플리케이션 설치를 시작할 수 있습니다.
- Kaspersky Security Center로 생성한 독립 실행형 설치 패키지를 사용하여 수동으로 보호 시스템 배포.

  클라이언트 기기와 관리자의 워크스테이션에 Kaspersky 애플리케이션을 수동으로 설치합니다; 네트워크 에이전트를 설치하는 동안 클라이언트 기기를 중앙 관리 서버에 연결하는 설정이 정의됩니다.

이 배포 방법은 원격 설치가 불가능한 경우에 권장됩니다.

Kaspersky Security Center에서는 Microsoft Active Directory® 그룹 정책을 사용하여 보호 시스템을 배포할 수 있습니다.

조직 네트워크에 대한 Kaspersky Security Center 배포 계획에 대한 정보

중앙 관리 서버 한 대는 기기를 최대 10만 대를 지원할 수 있습니다. 조직 네트워크의 총 기기 개수가 100,000만 대보다 많으면 해당 네트워크에 여러 중앙 관리 서버를 배포한 다음 중앙에서 편리하게 관리할 수 있도록 계층 구조로 결합해야 합니다.

자체 관리자가 있는 대규모 지역 사무소(지사)를 운영하는 조직의 경우 해당 사무소에 중앙 관리 서버를 배포하면 유용합니다. 이렇게 하지 않는 경우에는 해당 사무소를 낮은 스루풋 채널로 연결되는 분리된 네트워크로 간주해야 합니다. "표준 구성: 자체 관리자가 운영하는 소수의 대규모 사무소" 섹션을 참조하십시오.

협채널로 연결되는 분리된 네트워크를 사용할 때는 네트워크 에이전트 하나 또는 여러 개가 배포 지점로 작동하도록 할당하면 트래픽을 절약할 수 있습니다(배포 지점 수 계산표 참조). 이 경우 분리된 네트워크의 모든 기기가 해당 로컬 업데이트 센터에서 업데이트를 가져옵니다. 실제 배포 지점은 중앙 관리 서버(기본 시나리오)와 인터넷의 Kaspersky 서버에서 업데이트를 다운로드할 수 있습니다("표준 구성: 여러 소규모 원격 사무소" 섹션을 참조하십시오).

Kaspersky Security Center 표준 구성의 상세한 설명은 "Kaspersky Security Center의 표준 구성" 섹션에 나와 있습니다. 배포를 계획할 때는 조직의 구조에 따라 가장 적합한 표준 구성을 선택합니다.

배포 계획 단계에서는 중앙 관리 서버에 특수 인증서 X.509를 할당할지를 고려해야 합니다. 다음과 같은 경우 중앙 관리 서버에 X.509 인증서를 할당하면 유용할 수 있습니다. 아래 목록에 해당하는 경우 중 일부가 제시되어 있습니다:

- SSL 종료 프록시를 통해, 또는 역방향 프록시를 사용하기 위해 SSL(Secure Socket Layer) 트래픽 검사
- 조직의 PKI(공개 키 인프라)로 통합
- 인증서 필드의 필수 값 지정
- 인증서에 필요한 암호화 강도 제공

기업 보호용 구조 선택

기업의 보호 구조는 다음 요인에 따라 선택해야 합니다:

- 조직의 네트워크 토폴로지.
- 조직 구조.
- 네트워크 보호를 담당하는 직원 수 및 이들의 책임 할당.
- 보호 관리 구성 요소에 할당할 수 있는 하드웨어 리소스.

- 보호 구성 요소의 유지보수를 위해 할당할 수 있는 통신 채널의 처리 성능.
- 조직 네트워크에 대한 중요한 관리 작업을 실행하는 데 따른 시간 제한. 중요한 관리 작업에는 안티 바이러스 데이터베이스 배포 및 클라이언트 기기에 대한 정책 수정 등이 포함됩니다.

보호 구조를 선택할 때에는 먼저 중앙 집중식 보호 시스템 작동에 사용할 수 있는 네트워크 및 하드웨어 리소스를 평가하는 것이 좋습니다.

네트워크와 하드웨어 인프라를 분석하려면 다음 프로세스를 따르는 것이 좋습니다:

1. 보호 시스템이 배포되는 네트워크의 다음 설정을 정의합니다:
   - 네트워크 세그먼트 수.
   - 개별 네트워크 세그먼트 간 통신 채널의 속도.
   - 각 네트워크 세그먼트에 있는 관리 중인 기기의 수.
   - 보호 시스템의 작동을 유지하기 위해 할당할 수 있는 각 통신 채널의 처리 성능.
2. 모든 관리 중인 기기에 대한 주요 관리 작업을 실행하는 데 허용되는 최대 시간을 결정합니다.
3. 1단계와 2단계의 정보와 더불어 관리 시스템의 로드 테스트 데이터를 분석합니다. 분석 결과를 토대로 다음 질문에 답합니다:
   - 단일 중앙 관리 서버로 모든 클라이언트를 처리할 수 있습니까 아니면 계층 구조의 중앙 관리 서버가 필요합니까?
   - 2단계에서 지정한 시간 제한 내에 모든 클라이언트를 처리하려면 중앙 관리 서버에 어떤 하드웨어 구성이 필요합니까?
   - 통신 채널의 부하를 줄이기 위해 배포 지점을 사용해야 합니까?

위의 3가지 질문에 답하고 나면 허용되는 조직의 보호 시스템 구조를 결정할 수 있습니다.

조직 네트워크에서 다음과 같은 표준 보호 구조 중 하나를 사용할 수 있습니다:

- 단일 중앙 관리 서버. 모든 클라이언트 기기가 단일 중앙 관리 서버에 연결됩니다. 중앙 관리 서버를 배포 지점로 사용합니다.
- 단일 중앙 관리 서버와 여러 배포 지점. 모든 클라이언트 기기가 단일 중앙 관리 서버에 연결됩니다. 네트워크로 연결된 클라이언트 기기 중 일부가 배포 지점 역할을 합니다.
- 중앙 관리 서버의 계층 구조. 각 네트워크 세그먼트에 별도의 중앙 관리 서버가 하나씩 할당되어 중앙 관리 서버 계층 구조를 형성합니다. 기본 중앙 관리 서버가 배포 지점로 사용됩니다.
- 계층 구조의 중앙 관리 서버와 여러 배포 지점. 각 네트워크 세그먼트에 별도의 중앙 관리 서버가 하나씩 할당되어 중앙 관리 서버 계층 구조를 형성합니다. 네트워크로 연결된 클라이언트 기기 중 일부가 배포 지점 역할을 합니다.

Kaspersky Security Center의 표준 구성

이 섹션에서는 조직 네트워크에서 Kaspersky Security Center 구성 요소 배포에 사용되는 다음과 같은 표준 구성에 대해 설명합니다:

- 단일 사무소
- 각기 지역적으로 떨어진 곳에 위치하고 있으며 자체 관리자가 운영하는 소수의 대규모 사무소
- 각기 지역적으로 떨어진 곳에 위치한 여러 소규모 사무소

표준 구성: 단일 사무소

조직 네트워크에서 중앙 관리 서버를 하나 또는 여러 개 배포할 수 있습니다. 중앙 관리 서버 수는 사용 가능한 하드웨어 또는 관리 중인 기기의 총 수를 기준으로 선택할 수 있습니다.

중앙 관리 서버 한 대는 기기를 최대 100,000대까지 지원합니다. 조만간 관리 중인 기기의 수가 늘어날 가능성을 고려해야 합니다: 단일 중앙 관리 서버에 약간 더 적은 수의 기기를 연결하면 유용할 수 있습니다.

중앙 관리 서버에 대한 인터넷 접속이 필요한지에 따라 내부 네트워크나 DMZ에 중앙 관리 서버를 배포할 수 있습니다.

여러 서버를 사용하는 경우에는 서버를 계층 구조로 결합하는 것이 좋습니다. 중앙 관리 서버 계층 구조를 사용하면 정책 및 작업 중복을 방지할 수 있으며 전체 관리 중인 기기 집합을 단일 중앙 관리 서버에서 관리되는 것처럼 처리하여 기기 검색, 기기 조회 작성, 리포트 작성 등을 수행할 수 있습니다.

표준 구성: 자체 관리자가 운영하는 소수의 대규모 사무소

조직에 지리적으로 분리된 대형 사무소가 몇 개 있는 경우 각 사무소에 중앙 관리 서버를 배포하는 옵션을 고려해야 합니다. 사용 가능한 클라이언트 기기 및 하드웨어 수에 따라 사무소당 하나 이상의 중앙 관리 서버를 배포할 수 있습니다. 이 경우 각 사무소를 "표준 구성: 단일 사무소"로 볼 수 있습니다. 관리를 쉽게 하기 위해 모든 중앙 관리 서버를 계층 구조(다중 레벨 가능)로 결합하는 것이 좋습니다.

일부 직원이 기기(노트북)를 가지고 다른 사무실로 이동한다면 네트워크 에이전트 정책에서 네트워크 에이전트 연결 프로필을 생성합니다. 네트워크 에이전트 연결 프로필은 Windows 및 macOS 기기에서만 지원됩니다.

표준 구성: 다수의 소규모 원격 사무소

이 표준 구성은 본사 사무소 하나와 인터넷을 통해 본사 사무소와 통신할 수 있는 여러 소규모 원격 사무소를 제공합니다. 각 원격 사무소는 NAT(Network Address Translation)가 적용된 상태로 배치되어 서로 격리되기 때문에 두 원격 사무소 간에 연결을 설정할 수 없습니다.

중앙 관리 서버는 본사 사무소에 배포해야 하며, 기타 모든 사무소에는 배포 지점을 하나 이상 할당해야 합니다. 사무실이 인터넷을 통해 연결 시, 배포 지점에 대해 *배포 지점의 저장소로 업데이트 다운로드* 작업을 생성하면 유용할 수 있습니다. 그러면 배포 지점은 중앙 관리 서버가 아닌 Kaspersky 서버, 로컬, 네트워크 폴더에서 업데이트를 직접 다운로드합니다.

원격 사무소의 일부 기기가 중앙 관리 서버에 직접 접근할 수 없을 시(중앙 관리 서버 접근 기능이 인터넷을 통해 제공되는데 일부 기기가 인터넷에 접속할 수 없을 때 등)에는 배포 지점을 연결 게이트웨이 모드로 전환해야 합니다. 이 경우 원격 사무소에 있는 기기의 네트워크 에이전트는 추가 동기화를 위해 중앙 관리 서버에 연결되지만 직접 연결되지는 않으며 게이트웨이를 통해 연결됩니다.

중앙 관리 서버는 원격 사무소 네트워크를 검색하지 못할 가능성이 높으므로, 배포 지점이 이 기능을 수행하도록 하는 것이 좋습니다.

중앙 관리 서버는 NAT가 적용된 상태로 원격 사무소에 있는 관리 중인 기기의 15000 UDP 포트로 알림을 전송할 수 없습니다. 이 문제를 해결하려는 경우 배포 지점 역할을 하는 기기의 속성에서 중앙 관리 서버에 대한 지속적인 연결 모드(**중앙 관리 서버와 계속 연결 유지** 확인란)를 활성화할 수 있습니다. 전체 배포 지점 개수가 300개 미만일 경우 이 모드를 사용할 수 있습니다. 푸시 서버를 사용하여 관리 중인 기기와 중앙 관리 서버 간의 연결을 유지할 수 있습니다. 자세한 내용은 배포 지점을 푸시 서버로 사용 항목을 참조하십시오.

중앙 관리 서버용 DBMS 선택

중앙 관리 서버에서 사용할 데이터베이스 관리 시스템(DBMS)을 선택할 때는 중앙 관리 서버에서 관리하는 기기 개수를 고려해야 합니다.

아래 표에는 유효한 DBMS 옵션과 해당 옵션 사용 시의 권장 사항 및 제한 사항이 나와 있습니다.

DBMS에 대한 권장 사항 및 제한 사항

DBMS	권장 사항 및 제한 사항
SQL Server Express Edition 2016 이상	10,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 데이터베이스 오버플로 방지를 위해 이벤트 저장소의 최대 이벤트 수를 제한할 수 있습니다. 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오. 중앙 관리 서버와 다른 애플리케이션이 SQL Server Express Edition DBMS를 동시에 사용하도록 해서는 안 됩니다. **Windows 업데이트 동기화 수행** 작업에는 Microsoft SQL Express 데이터베이스를 지원하지 않습니다.
Express 2016 이상 이외의 로컬 SQL Server Edition	제한 없음
Express 2016 이상 이외의 원격 SQL Server Edition	두 기기가 같은 Windows® 도메인에 있는 경우에만 유효합니다. 기기의 도메인이 다른 경우에는 도메인 간에 양방향 신뢰 관계를 설정해야 합니다
로컬 또는 원격 MySQL 5.5, 5.6, 5.7 (MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5 버전은 더 이상 지원하지 않습니다.)	10,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.
로컬 또는 원격 MySQL 8.0.20 이상	50,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.
로컬 또는 원격 MariaDB(지원되는 버전 참조)	20,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.
PostgreSQL, Postgres Pro(지원하는 버전 참조)	50,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS 중 하나를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.

SQL Server 2019를 DBMS로 사용하고 CU12 이상의 누적 패치가 없는 경우 Kaspersky Security Center를 설치한 후에 다음을 수행해야 합니다.

1. SQL Management Studio를 사용하여 SQL Server에 연결합니다.
2. 다음 명령을 실행하십시오(데이터베이스에 다른 이름을 선택한 경우 KAV 대신 해당 이름을 사용하십시오).

```
USE KAV
```

```
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. SQL Server 2019 서비스를 다시 시작합니다.

그렇지 않으면 SQL Server 2019 사용 시 "이 쿼리를 실행하기 위한 리소스 풀 'internal'에 시스템 메모리가 부족합니다."와 같은 오류가 발생할 수 있습니다.

Kaspersky Security Center 15.1 사용을 위한 MariaDB x64 서버 구성

MariaDB x64 서버를 구성하여 Kaspersky Security Center와 공동 작업하려면 이 문서에 지정된 서버 파라미터를 제외하고 기본 서버 파라미터를 사용해야 합니다.

Kaspersky Security Center 15.1는 MariaDB DBMS를 지원합니다. 지원하는 MariaDB 버전에 대한 자세한 내용은 하드웨어 및 소프트웨어 요구 사항 섹션을 참조하십시오.

Kaspersky Security Center를 위해 MariaDB DBMS를 사용한다면, InnoDB 및 MEMORY 스토리지와 UTF-8 및 UCS-2 인코딩 지원을 활성화하십시오.

my.ini 파일에 대한 권장 설정

my.ini 파일 구성하기:

1. 텍스트 편집기에서 my.ini 파일을 엽니다.

2. My.ini 파일의 `[mysqld]` 섹션에 다음 줄을 추가합니다.

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<값은 예상 KAV 데이터베이스 크기의 80% 이상이어야 합니다>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

`innodb_buffer_pool_size` 값은 예상 KAV 데이터베이스 크기의 80% 이상이어야 합니다. 지정된 메모리는 서버 시작 시 할당됩니다. 데이터베이스 크기가 지정된 버퍼 크기보다 작다면, 필요한 메모리만 할당됩니다. MariaDB 10.4.3 이하를 사용한다면, 할당된 메모리의 실제 크기는 지정된 버퍼 크기보다 약 10% 큽니다.

파라미터값으로 `innodb_flush_log_at_trx_commit=0`을 사용하기를 권장합니다. "1" 또는 "2" 값은 MariaDB의 작동 속도에 부정적인 영향을 미치기 때문입니다. `innodb_file_per_table` 파라미터가 `1`로 설정되었는지 확인합니다.

MariaDB 10.1은 [mysqld] 섹션에 다음 줄을 추가로 입력합니다.

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

MariaDB 10.6은 [mysqld] 섹션에 다음 줄을 추가로 입력합니다.

```
optimizer_prune_level=0
optimizer_search_depth=8
```

기본적으로 옵티마이저 애드온 `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` 가 활성화됩니다. 이러한 애드온이 활성화되지 않은 경우 이를 활성화해야 합니다.

옵티마이저 애드온이 활성화되어 있는지 확인하려면 다음과 같이 하십시오:

1. MariaDB 클라이언트 콘솔에서 다음과 같은 명령을 실행합니다.

   ```
   SELECT @@optimizer_switch;
   ```

2. 출력에 다음과 같은 행이 포함되어 있는지 확인합니다.

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   이러한 행이 있고 `on` 값을 갖는 경우 옵티마이저 애드온이 활성화됩니다.

   이러한 행이 없거나 `off` 값을 갖는 경우 다음과 같이 해야 합니다.

   1. 텍스트 편집기에서 my.ini 파일을 엽니다.

   2. My.ini 파일의 `[mysqld]` 섹션에 다음 줄을 추가합니다.

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

애드온으로 `join_cache_incremental`, `join_cache_hash` 및 `join_cache_bka`가 활성화됩니다.

Kaspersky Security Center 15.1 사용을 위한 MySQL x64 서버 구성

MySQL x64 서버를 구성하여 Kaspersky Security Center와 공동 작업하려면 이 문서에 지정된 서버 파라미터를 제외하고 기본 서버 파라미터를 사용해야 합니다.

Kaspersky Security Center에 MySQL DBMS를 사용한다면, InnoDB 및 MEMORY 스토리지와 UTF-8 및 UCS-2 인코딩 지원을 활성화하십시오.

my.ini 파일에 대한 권장 설정

my.ini 파일 구성하기:

1. 텍스트 편집기에서 my.ini 파일을 엽니다.

2. My.ini 파일의 `[mysqld]` 섹션에 다음 줄을 추가합니다.

   ```
   sort_buffer_size=10M
   join_buffer_size=20M
   tmp_table_size=600M
   ```

```
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=<값은 예상 KAV 데이터베이스 크기의 80% 이상이어야 합니다>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0(서버가 대개 작은 트랜잭션을 사용)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

`innodb_buffer_pool_size` 값에 지정된 메모리는 서버 시작 시 할당됩니다. 데이터베이스 크기가 지정된 버퍼 크기보다 작다면, 필요한 메모리만 할당됩니다. 할당된 메모리의 실제 크기는 지정된 버퍼 크기보다 약 10% 큽니다. 자세한 내용은 MySQL 설명서를 참조하십시오.

파라미터값으로 `innodb_flush_log_at_trx_commit = 0`을 사용하기를 권장합니다. "1" 또는 "2" 값은 MySQL의 작동 속도에 부정적인 영향을 미치기 때문입니다. `innodb_file_per_table` 파라미터가 `1`로 설정되었는지 확인합니다.

Kaspersky Security Center 15.1 사용을 위한 PostgreSQL 또는 Postgres Pro 서버 구성

PostgreSQL 또는 Postgres Pro 서버를 구성하여 Kaspersky Security Center와 공동 작업하려면 이 문서에 지정된 서버 파라미터를 제외하고 기본 서버 파라미터를 사용해야 합니다.

Kaspersky Security Center 15.1는 PostgreSQL 및 Postgres Pro DBMS를 지원합니다. 해당 DBMS 중 하나를 사용 시, Kaspersky Security Center와의 DBMS 작업을 최적화하도록 DBMS 서버 매개변수를 구성하는 것을 고려하십시오.

구성 파일의 기본 경로는 `C:\Program Files\PostgreSQL\<버전>\data\postgresql.conf`입니다.

PostgreSQL 및 Postgres Pro에 대한 권장 매개변수:

- `shared_buffers` = DBMS가 설치된 기기 RAM 값의 25%

  RAM이 1GB 미만이면 기본값을 그대로 둡니다.
- `max_stack_depth = 2MB`
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

`standard_conforming_strings` 파라미터가 기본값인 `on`으로 설정되었는지 확인합니다. postgresql.conf 파일을 업데이트한 후 구성을 다시 로드하거나 서버를 다시 시작합니다. 자세한 내용은 PostgreSQL 설명서를 참조하십시오.

Postgres Pro 15.7 또는 Postgres Pro 15.7.1을 사용한다면 `enable_compound_index_stats` 파라미터를 비활성화합니다:

```
enable_compound_index_stats = off
```

PostgreSQL 및 Postgres Pro 서버 매개변수 및 매개변수 지정 방법에 대한 자세한 내용은 해당 DBMS 설명서를 참조하십시오.

PostgreSQL 및 Postgres Pro용 계정을 만들고 구성하는 방법에 대한 자세한 내용은 PostgreSQL 및 Postgres Pro 작업을 위한 계정 구성 항목을 참조하십시오.

Kaspersky Endpoint Security for Android를 사용하여 모바일 기기 관리

Kaspersky Endpoint Security for Android™가 설치된 모바일 기기(이하 KES 기기로 지칭함)는 중앙 관리 서버를 통해 관리됩니다. Kaspersky Security Center는 KES 기기 관리를 위해 다음 기능을 지원합니다:

- 모바일 기기를 클라이언트 기기로 취급:
  - 관리 그룹 멤버십
  - 상태, 이벤트 및 리포트 보기와 같은 모니터링
  - 로컬 설정 수정 및 Kaspersky Endpoint Security for Android용 정책 할당
- 중앙 집중식 모드로 명령 전송
- 원격으로 모바일 앱 패키지 설치

중앙 관리 서버는 TLS, TCP 포트 13292를 통해 KES 기기를 관리합니다.

중앙 관리 서버에 대한 인터넷 접속 제공

다음 경우, 중앙 관리 서버에 대한 인터넷 접속이 필요합니다:

- Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 정기 업데이트
- 타사 소프트웨어 업데이트

  기본적으로 중앙 관리 서버에서 Microsoft 소프트웨어 업데이트를 관리 중인 기기에 설치하는 경우 인터넷 연결이 필요하지 않습니다. 예를 들어 관리 중인 기기는 Microsoft Update 서버 또는 회사의 네트워크에 배포된 Microsoft WSUS(Windows Server Update Services)가 있는 Windows Server에서 직접 Microsoft 소프트웨어 업데이트를 다운로드할 수 있습니다. 다음 경우, 중앙 관리 서버를 인터넷에 연결해야 합니다:
  - WSUS 서버로 중앙 관리 서버 사용 시
  - Microsoft 소프트웨어 이외의 타사 소프트웨어 업데이트 설치
- 타사 소프트웨어 취약점 수정

  중앙 관리 서버가 다음 작업을 수행하려면 인터넷 연결이 필요합니다.
  - Microsoft 소프트웨어의 취약성에 대한 권장 수정 목록을 작성합니다. 이 목록은 Kaspersky 전문가가 생성하고 정기적으로 업데이트합니다.
  - Microsoft 소프트웨어가 아닌 타사 소프트웨어의 취약점을 수정합니다.
- 이동 사용자의 기기(노트북)를 관리하는 경우

- 원격 사무소의 기기를 관리하는 경우
- 원격 사무실에 있는 기본 또는 보조 중앙 관리 서버와 통신하는 경우
- 모바일 기기 관리

이 섹션에서는 인터넷을 통해 중앙 관리 서버에 접근하는 일반적인 방식에 대해 설명합니다. 각 사례는 중앙 관리 서버에 대해 인터넷 접속을 제공하는 방법을 중점적으로 설명하고 있으며, 중앙 관리 서버 전용 인증서가 필요할 수 있습니다.

인터넷 접속: 로컬 네트워크의 중앙 관리 서버

중앙 관리 서버가 조직의 내부 네트워크에 있는 경우 포트 포워딩을 통해 외부에서 중앙 관리 서버의 TCP 13000 포트에 접근할 수 있습니다. 모바일 기기 관리가 필요하다면 액세스 가능한 TCP 13292 포트를 만들 수 있습니다.

인터넷 접속: DMZ의 중앙 관리 서버

조직 네트워크의 DMZ에 있는 중앙 관리 서버는 조직의 내부 네트워크에 접근할 수 없습니다. 따라서 다음과 같은 제한이 적용됩니다:

- 중앙 관리 서버가 새로운 기기를 탐지할 수 없습니다.
- 중앙 관리 서버가 조직 내부 네트워크에서 기기 강제 설치를 통해 네트워크 에이전트 초기 배포를 수행할 수 없습니다.

이 제한은 네트워크 에이전트 초기 설치에만 적용됩니다. 설치되어 있는 네트워크 에이전트 또는 보안 제품의 추가 업그레이드는 중앙 관리 서버를 통해 수행할 수 있습니다. 그와 동시에 Microsoft® Active Directory®의 그룹 정책을 사용하는 등의 다른 방법으로 네트워크 에이전트 초기 배포를 수행할 수도 있습니다.

- 중앙 관리 서버가 포트 15000 UDP를 통해 관리 중인 기기로 알림을 전송할 수 없습니다. 그러나 알림 전송은 Kaspersky Security Center가 작동하는 데 반드시 필요한 기능은 아닙니다.
- 중앙 관리 서버가 Active Directory를 검색할 수 없습니다. 그러나 대부분의 경우에는 Active Directory 검색의 결과가 필요하지 않습니다.

위의 제한이 중요한 사항으로 확인되는 경우에는 조직 네트워크에 있는 배포 지점을 사용하여 제거할 수 있습니다:

- 네트워크 에이전트를 사용하지 않고 기기에서 초기 배포를 수행하려면 먼저 기기 중 하나에 네트워크 에이전트를 설치한 다음 배포 지점 상태를 할당합니다. 그러면 다른 기기의 네트워크 에이전트 초기 설치가 이 배포 지점을 통해 중앙 관리 서버에서 수행됩니다.
- 조직 내부 네트워크의 새로운 기기를 탐지하고 Active Directory를 검색하려면 배포 지점 중 하나에서 관련 기기 발견 방법을 작동시켜야 합니다.

조직 내부 네트워크에 있는 관리 중인 기기에 포트 15000 UDP로 알림이 올바르게 전송되도록 하려면 배포 지점이 전체 네트워크를 업데이트하도록 설정해야 합니다. 할당 된 배포 지점의 속성에서 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택합니다. 그러면 중앙 관리 서버와 배포 지점의 연결이 계속 설정된 상태로 유지되며, 배포 지점이 조직 내부 네트워크(IPv4 또는 IPv6 네트워크일 수 있음)에 있는 기기의 포트 15000 UDP로 알림을 전송할 수 있습니다.

인터넷 접근: 연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용

중앙 관리 서버가 조직 내부 네트워크에 있고, 해당 네트워크의 DMZ에는 역방향 연결을 사용하여 연결 게이트웨이로 실행 중인 네트워크 에이전트가 포함된 기기가 있는 경우가 있습니다(중앙 관리 서버가 네트워크 에이전트에 대한 연결을 설정함). 이때, 인터넷 접속이 가능하도록 하려면 다음 조건을 충족해야 합니다:

- DMZ에 있는 기기에 네트워크 에이전트를 설치해야 합니다. 네트워크 에이전트를 설치할 때 설치 마법사의 **연결 게이트웨이** 창에서 **연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용**를 선택합니다.
- 연결 게이트웨이가 설치된 기기를 배포 지점으로 추가해야 합니다. 연결 게이트웨이를 추가할 때에는 **배포 지점 추가** 창에서 **선택 → 주소로 DMZ에 있는 연결 게이트웨이 추가** 옵션을 선택합니다.
- 인터넷 연결을 사용하여 외부 데스크톱 기기를 중앙 관리 서버에 연결하려면 네트워크 에이전트용 설치 패키지를 수정해야 합니다. 생성된 설치 패키지의 속성에서 **고급 → 연결 게이트웨이를 통해 중앙 관리 서버에 연결** 옵션을 선택한 다음, 새로 생성된 연결 게이트웨이를 지정합니다.

DMZ에 있는 연결 게이트웨이의 경우 중앙 관리 서버는 중앙 관리 서버 인증서로 서명된 인증서를 만듭니다. 관리자는 중앙 관리 서버에 사용자 지정 인증서를 할당하려는 경우 DMZ에서 연결 게이트웨이를 만들기 전에 할당해야 합니다.

일부 직원이 로컬 네트워크나 인터넷을 통해 중앙 관리 서버에 연결할 수 있는 노트북을 사용 시, 네트워크 에이전트 정책에서 네트워크 에이전트용 전환 규칙을 만들면 유용할 수 있습니다.

배포 지점 정보

네트워크 에이전트가 설치된 기기를 배포 지점으로 사용할 수 있습니다. 이 모드에서 네트워크 에이전트는 다음 기능을 수행할 수 있습니다:

- 업데이트를 배포합니다(중앙 관리 서버 또는 Kaspersky 서버에서 업데이트를 가져올 수 있습니다). 후자의 경우 *배포 지점의 저장소로 업데이트 다운로드* 작업이 배포 지점 역할을 수행하는 기기에 만들어져야 합니다.
  - 다른 기기에 소프트웨어를 설치하고 네트워크 에이전트 초기 배포를 수행합니다.
  - 네트워크를 검색해서 새로운 기기를 탐지하고 기존 기기에 대한 정보를 업데이트합니다. 배포 지점은 중앙 관리 서버의 기기 발견 방법을 똑같이 적용할 수 있습니다.

조직 네트워크에서 배포 지점을 배포하는 목적은 다음과 같습니다:

- 중앙 관리 서버의 부하 감소.
- 트래픽 최적화.
- 조직 네트워크의 연결하기 어려운 위치에 있는 기기에 대한 중앙 관리 서버 접근 기능을 제공합니다. 중앙 관리 서버와 관련하여 NAT가 적용된 네트워크에서 배포 지점을 사용할 수 있으면 중앙 관리 서버가 다음 작업을 수행할 수 있습니다:
  - IPv4 또는 IPv6 네트워크의 UDP를 통해 기기로 알림 전송
  - IPv4 또는 IPv6 네트워크 검색
  - 초기 배포 수행
  - 푸시 서버로 작동

배포 지점은 관리 그룹용으로 할당됩니다. 이 경우 배포 지점의 범위에는 관리 그룹 및 모든 하위 그룹 내의 모든 기기가 포함됩니다. 그러나 배포 지점 역할을 하는 기기가 할당된 관리 그룹에 포함되어 있지 않을 수도 있습니다.

배포 지점을 연결 게이트웨이로 만들 수 있습니다. 이 경우에는 배포 지점 범위의 기기가 직접 중앙 관리 서버에 연결되는 것이 아니라 게이트웨이를 통해 연결됩니다. 중앙 관리 서버와 관리 중인 기기 사이에 직접 연결을 할 수 없는 경우 이 모드를 사용하는 것이 좋습니다.

Linux 기반 기기를 배포 지점으로 사용하면 klnagent 서비스에 대한 파일 설명자의 제한을 늘리는 것이 좋습니다. 배포 지점의 범위에 기기가 다수 포함되면, 열 수 있는 최대 파일 수의 기본값이 적용되어 부족할 수 있습니다.

klnagent 서비스에 대한 파일 설명자 제한 늘리기

Linux 기반 배포 지점의 범위에 기기가 많다면 열 수 있는 파일의 기본 제한(파일 설명자)만으로는 부족할 수 있습니다. klnagent 서비스에 대한 파일 설명자의 제한을 늘리면 이를 방지할 수 있습니다.

klnagent 서비스에 대한 파일 설명자의 제한을 늘리려면:

1. 배포 지점으로 사용되는 Linux 기반 기기에서 다음 명령을 실행합니다.

   ```
   systemctl edit klnagent64.service
   ```

2. `[Service]` 섹션의 `LimitNOFILE` 파라미터에서 파일 설명자의 하드 및 소프트 제한을 지정합니다.

   `LimitNOFILE=<소프트 리소스 제한>:<하드 리소스 제한>`

   예: `LimitNOFILE=32768:131072`. 파일 설명자의 소프트 제한은 하드 제한보다 작거나 같아야 합니다.

3. 다음 명령을 실행하여 파라미터가 올바르게 지정되었는지 확인합니다:

   ```
   systemd-analyze verify klnagent64.service
   ```

   파라미터를 잘못 지정하면 이 명령이 다음 오류 중 하나를 출력할 수 있습니다:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     이 오류가 발생하면 `LimitNOFILE` 줄의 기호를 잘못 지정한 것입니다. 입력한 줄을 확인 및 수정해야 합니다.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     입력한 파일 설명자의 소프트 제한이 하드 제한보다 크면 이 오류가 발생합니다. 입력한 줄을 확인하고 파일 설명자의 소프트 제한이 하드 제한보다 작거나 같은지 확인해야 합니다.

4. 다음 명령을 실행하여 systemd 프로세스를 다시 로드합니다.

   ```
   systemctl daemon-reload
   ```

5. 다음 명령을 실행하여 네트워크 에이전트 서비스를 다시 시작합니다.

   ```
   systemctl restart klnagent
   ```

6. 다음 명령을 실행하여 지정한 파라미터가 올바르게 적용되었는지 확인합니다.

   `less /proc/<NAgent 프로세스 ID>/limits`

   여기서 `<네트워크 에이전트 프로세스 ID>` 파라미터는 네트워크 에이전트 프로세스의 식별자입니다. 다음 명령을 실행하여 식별자를 가져올 수 있습니다.

   ```
   ps -ax | grep klnagent
   ```

Linux 기반 배포 지점은 열 수 있는 파일의 제한이 증가합니다.

배포 지점의 개수 및 구성 계산

네트워크에 포함된 클라이언트 기기가 많을수록 배포 지점도 더 많이 필요합니다. 배포 지점 자동 할당 기능을 중지하는 않는 것을 권장합니다. 배포 지점 자동 할당 기능이 활성되면 클라이언트 기기의 수가 매우 많으면 중앙 관리 서버는 배포 지점을 할당하고 그 구성을 정의합니다.

독점 할당된 배포 지점 사용

특정 기기를 배포 지점(예, 독점적으로 할당된 서버)로 사용하려는 경우 배포 지점의 자동 할당을 사용하지 않도록 선택할 수 있습니다. 이 경우 배포 지점을 할당할 기기에 사용 가능한 디스크 공간이 충분하고 정기적으로 종료되지 않으며 절전 모드가 해제되어 있는지 확인하십시오.

네트워크에 연결된 기기 수에 따라 단일 네트워크 세그먼트를 포함하는 네트워크에 할당된 배포 지점의 수

네트워크 세그먼트에 있는 클라이언트 기기의 수	배포 지점 개수
300대 이하	0(배포 지점 할당 안 함)
300대 이상	적합: (N/10,000 + 1), 권장: (N/5,000 + 2), 여기서 N은 네트워크에 연결된 기기 개수

네트워크에 연결된 기기 수에 따라 다중 네트워크 세그먼트를 포함하는 네트워크에 할당된 배포 지점의 수

네트워크 세그먼트당 클라이언트 기기의 수	배포 지점 개수
10대 이하	0(배포 지점 할당 안 함)
10~100대	1
100대 이상	적합: (N/10,000 + 1), 권장: (N/5,000 + 2), 여기서 N은 네트워크에 연결된 기기 개수

표준 클라이언트 기기(워크스테이션)를 배포 지점으로 사용

표준 클라이언트 기기(워크스테이션)를 배포 지점으로 사용하려는 경우에는 통신 채널과 중앙 관리 서버에 과도한 부하가 걸리지 않도록 아래 표에 나와 있는 것처럼 배포 지점을 할당하는 것이 좋습니다:

네트워크에 연결된 기기 수에 따라 단일 네트워크 세그먼트를 포함하는 네트워크에 배포 지점 기능을 수행하는 워크스테이션의 수

네트워크 세그먼트에 있는 클라이언트 기기의 수	배포 지점 개수
300대 이하	0(배포 지점 할당 안 함)
300대 이상	(N/300 + 1), 여기서 N은 네트워크에 연결된 기기 수를 뜻하지만 최소 3대의 배포 지점이 있어야합니다

네트워크에 연결된 기기 수에 따라 다중 네트워크 세그먼트를 포함하는 네트워크에 배포 지점 기능을 수행하는 워크스테이션의 수

네트워크 세그먼트당 클라이언트 기기의 수	배포 지점 개수
10대 이하	0(배포 지점 할당 안 함)
10~30대	1
31~300대	2
300대 이상	(N/300 + 1), 여기서 N은 네트워크에 연결된 기기 수를 뜻하지만 최소 3대의 배포 지점이 있어야합니다

배포 지점이 종료되거나 다른 원인으로는 사용할 수 없는 경우 이 배포 지점에 연결된 관리 중인 기기는 업데이트를 위해 중앙 관리 서버에 접근할 수 있습니다.

중앙 관리 서버 계층 구조

한 MSP에서 다수의 중앙 관리 서버를 실행할 수 있습니다. 개별 중앙 관리 서버를 여러 개 관리하려면 불편할 수도 있으므로 계층 구조를 적용할 수 있습니다. 두 중앙 관리 서버에 대한 "기본/보조" 구성에서는 다음 옵션을 제공합니다.

- 보조 중앙 관리 서버는 기본 중앙 관리 서버에서 정책과 작업을 상속하므로 설정이 중복되지 않습니다.
- 기본 중앙 관리 서버의 기기 조회 시 보조 중앙 관리 서버의 기기가 포함될 수 있습니다.
- 기본 중앙 관리 서버의 리포트에는 상세 정보를 비롯한 보조 중앙 관리 서버의 데이터가 포함될 수 있습니다.

기본 중앙 관리 서버는 위에 나열된 옵션 범위 내에서 가상이 아닌 보조 중앙 관리 서버에서만 데이터를 수신합니다. 이 제한은 기본 중앙 관리 서버와 데이터베이스를 공유하는 가상 중앙 관리 서버에는 적용되지 않습니다.

가상 중앙 관리 서버

실제 중앙 관리 서버를 기준으로 하여 보조 중앙 관리 서버와 비슷한 가상 중앙 관리 서버를 여러 개 만들 수 있습니다. 가상 중앙 관리 서버 모델은 ACL(접근 제어 목록)을 기반으로 하는 임의 접근 모델에 비해 기능성이 뛰어나며 보다 광범위한 격리 수준을 제공합니다. 각 가상 중앙 관리 서버는 정책 및 작업을 포함하는 할당된 기기에 대한 관리 그룹의 전용 구조 외에 자체 미할당 기기 그룹, 자체 리포트 세트, 선택한 기기와 이벤트, 설치 패키지, 이동 규칙 등도 제공합니다. 서비스 공급업체(xSP)는 가상 중앙 관리 서버의 기능 범위를 사용하여 고객을 최대한 격리할 수 있으며, 복잡한 워크플로를 수행하는 관리자가 여러 명인 대규모 조직에서도 해당 범위를 사용할 수 있습니다.

가상 중앙 관리 서버는 보조 중앙 관리 서버와 매우 비슷하지만 다음과 같은 점이 다릅니다:

- 가상 중앙 관리 서버에는 대부분의 글로벌 설정과 자체 TCP 포트가 없습니다.
- 가상 중앙 관리 서버에는 보조 중앙 관리 서버가 없습니다.
- 가상 중앙 관리 서버에는 다른 가상 중앙 관리 서버가 없습니다.
- 실제 중앙 관리 서버는 모든 가상 중앙 관리 서버의 기기, 그룹, 이벤트 및 관리 중인 기기에 있는 개체(격리의 항목, 자산 관리(소프트웨어) 등)를 확인합니다.
- 가상 중앙 관리 서버는 배포 지점이 연결된 네트워크만 검사할 수 있습니다.

Kaspersky Security Center의 제한 사항에 대한 정보

아래 표에는 Kaspersky Security Center 최신 버전의 제한 사항이 표시되어 있습니다.

Kaspersky Security Center 제한 사항

제한 유형	값
중앙 관리 서버당 관리 중인 기기의 최대 수	100,000
중앙 관리 서버와 계속 연결 유지 옵션이 선택된 기기의 최대 개수	300
관리 그룹의 최대 개수	10,000
저장할 이벤트의 최대 개수	45,000,000
최대 정책 개수	2 000
최대 작업 개수	2 000

제한 유형	값
총 Active Directory 개체(조직 단위, OU) 및 사용자의 계정, 기기, 보안 그룹) 개수의 최댓값	1,000,000
정책 내 프로필 개수의 최댓값	100
단일 기본 중앙 관리 서버의 보조 중앙 관리 서버 개수 최댓값	500
가상 중앙 관리 서버 개수의 최댓값	500
단일 배포 지점이 관리할 수 있는 최대 기기 수(배포 지점은 모바일이 아닌 기기만 관리할 수 있음)	10,000
단일 연결 게이트웨이를 사용할 수 있는 최대 기기 수	10,000, 모바일 기기 포함
중앙 관리 서버당 최대 모바일 기기 수	100,000 - 고정된 관리 중인 기기 수

네트워크 부하

이 섹션에는 주요 관리 작업을 수행하는 동안 클라이언트 기기와 중앙 관리 서버 간에 교환되는 네트워크 트래픽 양에 대한 정보가 들어 있습니다.

주요 부하 중 상당 부분은 다음 관리 시나리오를 진행하면서 발생합니다:

- 안티 바이러스 보호 시스템 최초 배포
- 안티 바이러스 데이터베이스 최초 업데이트
- 중앙 관리 서버와 클라이언트 기기 동기화
- 안티 바이러스 데이터베이스 정기 업데이트
- 중앙 관리 서버에 의한 클라이언트 기기 이벤트 처리

안티 바이러스 보호 시스템 최초 배포

이 섹션에서는 네트워크 에이전트 및 Kaspersky Endpoint Security for Windows를 클라이언트 기기에 설치한 후의 트래픽 양 값에 대한 정보를 제공합니다(아래 표 참조).

네트워크 에이전트는 강제 설치 방식으로 설치되어, 설치에 필요한 파일이 중앙 관리 서버에서 클라이언트 기기의 공유 폴더로 복사됩니다. 설치 후에는 네트워크 에이전트가 중앙 관리 서버에 대한 연결을 사용해서 Kaspersky Endpoint Security for Windows 배포 패키지를 검색합니다.

트래픽

시나리오	단일 클라이언트 기기용 네트워크 에이전트 설치	데이터베이스가 업데이트되는 단일 클라이언트 기기에 Kaspersky Endpoint Security for Windows 설치	네트워크 에이전트와 Kaspersky Endpoint Security for Windows의 동시 설치
클라이언트 기기에서 중앙 관리 서버로 발생하는 트래픽, KB	1638.4	7843.84	9707.52
중앙 관리 서버에서 클라이언트 기기로 발생하는 트래픽, KB	69,990.4	259,317.76	329,318.4
총 트래픽(단일 클라이언트 기기 기준), KB	71,628.8	267,161.6	339,025.92

클라이언트 기기에 네트워크 에이전트를 설치한 후에는 관리 그룹의 기기 중 하나를 배포 지점로 작동하도록 할당할 수 있습니다. 이 기기는 설치 패키지를 배포하는 데 사용됩니다. 이 경우 안티 바이러스 보호 초기 배포 중에 전송되는 트래픽 양은 IP 멀티캐스팅을 사용하는지 여부에 따라 크게 달라집니다.

IP 멀티캐스팅을 사용하는 경우에는 관리 그룹에서 실행 중인 모든 기기에 설치 패키지가 한 번 전송됩니다. 따라서 총 트래픽은 1/N로 감소합니다. 여기서 N은 관리 그룹에서 실행 중인 총 기기 수를 의미합니다. IP 멀티캐스팅을 사용하지 않을 경우 총 트래픽은 중앙 관리 서버에서 배포 패키지를 다운로드하는 것처럼 계산된 트래픽과 동일합니다. 그러나 이때는 패키지 소스가 중앙 관리 서버가 아닌 배포 지점입니다.

안티 바이러스 데이터베이스 최초 업데이트

안티 바이러스 데이터베이스의 최초 업데이트 중(클라이언트 기기에서 처음으로 데이터베이스 업데이트 작업을 시작) 트래픽 용량은 다음과 같습니다.

- 클라이언트 기기에서 중앙 관리 서버로 발생하는 트래픽: 1,8 MB.
- 중앙 관리 서버에서 클라이언트 기기로 발생하는 트래픽: 113 MB.
- 총 트래픽(단일 클라이언트 기기 기준): 114 MB.

데이터는 현재 사용 중인 안티 바이러스 데이터베이스 버전에 따라 약간 달라질 수 있습니다.

중앙 관리 서버와 클라이언트 동기화

이 시나리오는 클라이언트 기기와 중앙 관리 서버 간 집약적인 데이터 동기화가 발생할 경우 관리 시스템의 상태를 나타냅니다. 클라이언트 기기는 관리자가 정의한 간격으로 중앙 관리 서버에 연결됩니다. 중앙 관리 서버는 클라이언트 기기의 데이터 상태를 서버의 데이터 상태와 비교하여 마지막 클라이언트 기기 연결에 대한 정보를 데이터베이스에 기록하고 데이터를 동기화합니다.

이 섹션에서는 클라이언트를 중앙 관리 서버에 연결하는 경우 기본적인 관리 시나리오의 트래픽 값 정보를 제공합니다(아래 표 참조). 표의 데이터는 현재 사용 중인 안티 바이러스 데이터베이스 버전에 따라 약간 달라질 수 있습니다.

트래픽

시나리오	클라이언트 기기에서 중앙 관리 서버로 발생하는 트래픽, KB	중앙 관리 서버에서 클라이언트 기기로 발생하는 트래픽, KB	총 트래픽(단일 클라이언트 기기 기준), KB
클라이언트 기기에서 데이터베이스를 업데이트하기 전의 초기 동기화	699.44	568.42	1267.86
클라이언트 기기에서 데이터베이스를 업데이트한 후의 초기 동기화	735.8	4474.88	5210.68
클라이언트 기기와 중앙 관리 서버를 변경하지 않은 경우의 동기화	11.99	6.73	18.72
그룹 정책 설정 값이 변경된 후의 동기화	9.79	11.39	21.18
그룹 작업 설정 값이 변경된 후의 동기화	11.27	11.72	22.99
클라이언트 기기를 변경하지 않은 경우의 강제 동기화	77.59	99.45	177.04

전체 트래픽 양은 관리 그룹 내에서 IP 멀티캐스팅의 사용 여부에 따라 크게 달라집니다. IP 멀티캐스팅을 사용하는 경우 총 트래픽 양은 해당 그룹에 대해 약 N배 감소합니다. 여기서 N은 관리 그룹에 포함된 기기의 총 수입니다.

데이트 베이스 업데이트 전후로 초기 동기화 당시 트래픽의 양이 지정되는 경우는 다음과 같습니다:

- 클라이언트 기기에 네트워크 에이전트 및 보안 제품 설치
- 클라이언트 기기를 관리 그룹으로 이동
- 기본적으로 그룹용으로 만든 정책과 작업을 클라이언트 기기에 적용

이 표에는 Kaspersky Endpoint Security 정책 설정에 포함된 보호 설정 중 하나를 변경하는 경우의 트래픽 속도가 나와 있습니다. 다른 정책 설정의 데이터는 이 표에 나온 값과 차이가 있을 수 있습니다.

안티 바이러스 데이터베이스 추가 업데이트

이전 업데이트 20시간 후 안티 바이러스 데이터베이스 증분 업데이트를 수행하는 경우의 트래픽 용량은 다음과 같습니다.

- 클라이언트 기기에서 중앙 관리 서버로 발생하는 트래픽: 169 KB.
- 중앙 관리 서버에서 클라이언트 기기로 발생하는 트래픽: 16 MB.
- 총 트래픽(단일 클라이언트 기기 기준): 16.3 MB.

표의 데이터는 현재 사용 중인 안티 바이러스 데이터베이스 버전에 따라 약간 달라질 수 있습니다.

트래픽 양은 관리 그룹 내에서 IP 멀티캐스팅의 사용 여부에 따라 크게 달라집니다. IP 멀티캐스팅을 사용하는 경우 총 트래픽 양은 해당 그룹에 대해 약 N배 감소합니다. 여기서 N은 관리 그룹에 포함된 기기의 총 수입니다.

중앙 관리 서버를 통한 클라이언트 이벤트 처리

이 섹션에서는 클라이언트 기기에 "바이러스 탐지" 이벤트가 발생하여 이를 중앙 관리 서버로 전송하고 데이터베이스에 기록하는 경우의 트래픽 속도를 제공합니다(아래 그림 참조).

트래픽

시나리오	단일 "바이러스 탐지" 이벤트 발생 시 중앙 관리 서버로의 데이터 전송	9개의 "바이러스 탐지" 이벤트 발생 시 중앙 관리 서버로의 데이터 전송
클라이언트 기기에서 중앙 관리 서버로 발생하는 트래픽, KB	49.66	64.05
중앙 관리 서버에서 클라이언트 기기로 발생하는 트래픽, KB	28.64	31.97
총 트래픽(단일 클라이언트 기기 기준), KB	78.3	96.02

이 표의 데이터는 안티 바이러스 애플리케이션의 현재 버전과 정책에 정의되고 중앙 관리 서버 데이터베이스에 등록될 이벤트에 따라 약간 달라질 수 있습니다.

24시간 기준 트래픽

이 섹션에서는 클라이언트 기기와 중앙 관리 서버에 모두 데이터 변경 사항이 없는 상태에서 관리 시스템 활동의 24시간 기준 트래픽 속도에 대한 정보가 포함되어 있습니다(아래 표 참조).

이 표에 나온 데이터는 Kaspersky Security Center의 표준 설치를 수행하고 빠른 시작 마법사를 완료한 후의 네트워크 상태를 나타냅니다. 중앙 관리 서버와 클라이언트 기기의 동기화 주기는 20분이고 한 시간에 한 번 중앙 관리 서버 저장소로 업데이트가 다운로드되었습니다.

유휴 상태에서 24시간당 트래픽 속도

트래픽 흐름	값
클라이언트 기기에서 중앙 관리 서버로 발생하는 트래픽, KB	3235.84
중앙 관리 서버에서 클라이언트 기기로 발생하는 트래픽, KB	64,378.88
총 트래픽(단일 클라이언트 기기 기준), KB	67,614.72

모바일 기기 관리 준비

이 섹션에는 다음 정보를 제공합니다:

- 전용 iOS MDM 프로필을 iOS 기기에 설치해 관리하기 위한 목적으로 운영하는 iOS MDM 서버 정보
- Kaspersky Endpoint Security for Android를 설치해 모바일 기기를 관리하는 정보

iOS MDM 서버

iOS MDM 서버에서는 iOS 기기에 전용 iOS MDM 프로필을 설치하여 해당 기기를 관리할 수 있습니다. 지원되는 기능은 다음과 같습니다:

- 기기 잠금
- 암호 초기화
- 데이터 삭제
- 앱 설치 또는 제거
- VPN 설정, 이메일 설정, Wi-Fi 설정, 카메라 설정, 인증서 등의 고급 설정이 포함된 iOS MDM 프로필 사용

iOS MDM 서버는 해당 TLS 포트(기본적으로 포트 443)를 통해 모바일 기기로부터의 인바운드 연결을 수신하는 웹 서비스로, 네트워크 에이전트를 통해 Kaspersky Security Center에서 관리됩니다. 네트워크 에이전트는 iOS MDM 서버가 배포된 기기에 로컬로 설치됩니다.

관리자는 iOS MDM 서버를 배포할 때 다음 작업을 수행해야 합니다:

- 네트워크 에이전트에 중앙 관리 서버 접근 권한 제공
- 모바일 기기에 iOS MDM 서버의 TCP 포트 접근 권한 제공

이 섹션에서는 iOS MDM 서버의 두 가지 표준 구성에 대해 설명합니다.

표준 구성: DMZ에 위치한 Kaspersky Device Management for iOS

iOS MDM 서버가 인터넷 접속이 가능한 조직 로컬 네트워크의 DMZ에 있습니다. 이 방식의 특수한 기능은, 인터넷을 통해 기기에서 iOS MDM 웹 서비스에 접근할 때 문제가 발생하지 않는다는 것입니다.

iOS MDM 서버를 관리하려면 네트워크 에이전트를 로컬에 설치해야 하므로, 네트워크 에이전트와 중앙 관리 서버의 통신을 확인해야 합니다. 다음 방법 중 하나를 사용해 이를 구성할 수 있습니다:

- 중앙 관리 서버를 DMZ로 이동합니다.
- 연결 게이트웨이 사용:
  a. iOS MDM 서버가 배포된 기기에서 연결 게이트웨이를 통해 네트워크 에이전트를 중앙 관리 서버에 연결합니다.
  b. iOS MDM 서버가 배포된 기기에서 연결 게이트웨이 역할을 할 네트워크 에이전트를 할당합니다.

표준 구성: 조직 로컬 네트워크의 iOS MDM 서버

iOS MDM 서버가 조직의 내부 네트워크에 있는 구성입니다. 예를 들어 Kerberos 제한 위임을 지원하는 역방향 프록시에 iOS MDM 웹 서비스를 게시하여 외부 액세스를 위해 포트 443(기본 포트)을 활성화해야 합니다.

모든 표준 구성에서는 TCP 포트 2197을 통해 iOS MDM 서버용 Apple 웹 서비스(범위 17.0.0.0/8)에 접근할 수 있어야 합니다. 이 포트는 APNs이라는 전용 서비스를 통해 기기에 새 명령을 알리는 데 사용됩니다.

Kaspersky Endpoint Security for Android를 사용하여 모바일 기기 관리

Kaspersky Endpoint Security for Android™가 설치된 모바일 기기(이하 KES 기기로 지칭함)는 중앙 관리 서버를 통해 관리됩니다. Kaspersky Security Center는 KES 기기 관리를 위해 다음 기능을 지원합니다:

- 모바일 기기를 클라이언트 기기로 취급:
  - 관리 그룹 멤버십
  - 상태, 이벤트 및 리포트 보기와 같은 모니터링
  - 로컬 설정 수정 및 Kaspersky Endpoint Security for Android용 정책 할당
- 중앙 집중식 모드로 명령 전송
- 원격으로 모바일 앱 패키지 설치

중앙 관리 서버는 TLS, TCP 포트 13292를 통해 KES 기기를 관리합니다.

중앙 관리 서버 성능에 대한 정보

이 섹션에서는 다양한 하드웨어 구성으로 중앙 관리 서버의 성능을 테스트한 결과와, 중앙 관리 서버에 관리 중인 기기를 연결할 때의 제한에 대해 설명합니다.

중앙 관리 서버 연결 관련 제한 사항

중앙 관리 서버는 성능을 유지하면서 최대 기기 10만 대를 관리할 수 있도록 지원합니다.

성능 저하 없이 중앙 관리 서버에 연결하려는 경우 적용되는 제한 사항은 다음과 같습니다:

- 중앙 관리 서버 하나가 가상 중앙 관리 서버를 500개까지 지원할 수 있습니다.
- 기본 중앙 관리 서버는 세션을 동시에 1000개까지만 지원합니다.
- 가상 중앙 관리 서버는 세션을 동시에 1000개까지만 지원합니다.

중앙 관리 서버 성능 테스트 결과

중앙 관리 서버 성능 테스트 결과로 지정한 시간 동안 중앙 관리 서버가 동기화할 수 있는 최대 클라이언트 기기 수를 정의할 수 있었습니다. 이 정보는 네트워크에 안티 바이러스 보호 시스템을 배포하는 최적의 구성을 선택하는 데 사용됩니다.

아래 하드웨어 구성을 가진 기기를 테스트에서 사용했었습니다:

파라미터	값
CPU	Intel Xeon CPU E5630, 2.53GHz 클럭 속도, 2소켓, 8코어, 16논리 프로세서
RAM	26 GB
하드 드라이브	IBM ServeRAID M5014 SCSI 디스크, 487GB
운영 체제	Microsoft Windows Server 2019 Standard, 버전 10.0.17763, 빌드 17763
네트워크	QLogic BCM5709C 기가 비트 Ethernet(NDIS VBD Client)

SQL 서버 기기의 하드웨어 구성

파라미터	값
CPU	Intel Xeon CPU X5570, 2.93GHz 클럭 속도, 2소켓, 8코어, 16논리 프로세서
RAM	32 GB
하드 드라이브	Adaptec Array SCSI Disk Device, 2047 GB
운영 체제	Microsoft Windows Server 2019 Standard, 버전 10.0.17763, 빌드 17763
네트워크	Intel 82576 기가 비트

중앙 관리 서버에서는 500대의 가상 중앙 관리 서버 생성을 지원합니다.

동기화 주기는 관리 중인 기기 10,000대당 15분입니다(아래 표 참조).

중앙 관리 서버 부하 테스트 결과 요약

동기화 주기(분)	관리 중인 기기 수
15	10,000
30	20,000
45	30,000
60	40,000
75	50,000
90	60,000
105	70,000
120	80,000
135	90,000
150	100,000

중앙 관리 서버를 MySQL 또는 SQL Express 데이터베이스 서버에 연결할 경우 애플리케이션을 10000대 이상의 기기 관리에 사용하는 것은 권장되지 않습니다. MariaDB 데이터베이스 관리 시스템의 경우 관리 중인 기기의 최대 권장 수는 20,000대입니다.

KSN 프록시 서버 성능 테스트 결과

기업 네트워크에 클라이언트 기기가 많이 포함되어 있으며 이러한 기기가 KSN 프록시 서버로 중앙 관리 서버를 사용할 시, 중앙 관리 서버가 클라이언트 기기의 요청을 처리할 수 있도록 특정 요구 사항을 충족해야 합니다. 아래의 테스트 결과를 사용하여 네트워크의 중앙 관리 서버 부하를 평가하고 KSN 프록시 서비스가 정상적으로 작동하는 데 필요한 하드웨어 리소스를 계획할 수 있습니다.

아래 표는 중앙 관리 서버와 SQL 서버의 하드웨어 구성을 보여줍니다. 이 구성은 테스트에 사용되었습니다.

중앙 관리 서버 하드웨어 구성

파라미터	값
CPU	Intel Xeon CPU E5450, 3.00GHz 클럭 속도, 2소켓, 8코어, 16논리 프로세스
RAM	32 GB
운영 체제	Microsoft Windows Server 2016 Standard

SQL 서버 하드웨어 구성

파라미터	값
CPU	Intel Xeon CPU E5450, 3.00GHz 클럭 속도, 2소켓, 8코어, 16논리 프로세스
RAM	32 GB
운영 체제	Microsoft Windows Server 2019 Standard

아래 표에는 테스트 결과가 나와 있습니다.

KSN 프록시 서버 성능 테스트의 요약 결과

파라미터	값
초당 처리되는 최대 요청 수	4914
최대 CPU 사용률	36%

외부 서비스와의 상호 작용을 위한 네트워크 설정

Kaspersky Security Center 외부 서비스와 상호 작용하기 위해 다음 네트워크 설정을 사용합니다.

네트워크 설정	주소	설명
포트: 443 프로토콜: HTTPS	activation-v2.kaspersky.com	애플리케이션 활성화.
포트: 443 프로토콜: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 업데이트.
포트: 443 프로토콜: HTTPS	https://downloads.upd.kaspersky.com	• Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 업데이트. • Kaspersky 서버에 접근할 수 있는지 확인합니다. Kaspersky 데이터베이스 및 소프트웨어 모듈을 다운로드하기 전에 Kaspersky Security Center가 Kaspersky 서버에 액세스할 수 있는지 확인합니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다.

네트워크 설정	주소	설명
포트: 80 프로토콜: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 업데이트.
포트: 443 프로토콜: HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Kaspersky Security Network 사용.
포트: 443, 1443 프로토콜: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Kaspersky Security Network 사용.
포트: 443 프로토콜: HTTPS	click.kaspersky.com redirect.kaspersky.com	인터페이스에서 링크 사용.

네트워크 설정	주소	설명
포트: 80 프로토콜: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	이러한 서버는 공개 키 인프라(PKI)의 일부이며 Kaspersky 디지털 서명 인증서의 유효 상태 확인에 필요합니다. CRL은 해지된 인증서의 목록입니다. OCSP를 사용하면 특정 인증서의 상태를 실시간으로 요청할 수 있습니다. 이러한 서버는 디지털 인증서와의 상호 작용 보안 보장과 공격 방지에 도움이 됩니다.
포트: 443 프로토콜: HTTPS	https://ipm-klca.kaspersky.com	마케팅 공지.

Kaspersky Security Center Linux와 외부 서비스의 적절한 상호 작용을 위해 다음 권장 사항을 고려하십시오.
- 조직의 네트워크 장비 및 프록시 서버의 포트 443 및 1443에서 암호화되지 않은 네트워크 트래픽을 허용해야 합니다.
- 중앙 관리 서버가 Kaspersky 업데이트 서버 및 Kaspersky Security Network 서버와 상호 작용할 때 인증서 대체(MITM 공격)로 네트워크 트래픽 하이재킹을 방지해야 합니다.

klscflag 유틸리티를 사용하여 HTTP 또는 HTTPS 프로토콜을 통해 업데이트를 다운로드하려면:

1. 관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

2. HTTP 프로토콜을 통해 업데이트를 다운로드하려면 다음 명령 중 하나를 실행하십시오.

   - 중앙 관리 서버가 설치된 기기에서:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - 배포 지점에서:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   HTTPS 프로토콜을 통해 업데이트를 다운로드하려면 다음 명령 중 하나를 실행하십시오.

   - 중앙 관리 서버가 설치된 장치에서

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - 배포 지점에서:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

네트워크 에이전트 및 보안 제품 배포

조직의 기기를 관리하려면 각 기기에 네트워크 에이전트를 설치해야 합니다. 조직 기기에 분포된 Kaspersky Security Center를 배포할 때는 대개 해당 기기에 네트워크 에이전트를 먼저 설치합니다.

Microsoft Windows XP에서 네트워크 에이전트는 다음 동작을 올바르게 수행하지 못할 수 있습니다: Kaspersky 서버(배포 지점)에서 업데이트 직접 다운로드, KSN 프록시 서버 기능(배포 지점), 타사 취약점 탐지(취약점 및 패치 관리 사용 시).

초기 배포

조직의 기기를 관리하려면 기기마다 네트워크 에이전트를 설치해야 합니다.

Windows를 실행하는 관리 중인 기기에 네트워크 에이전트를 설치하는 방법은 다음과 같습니다.

- 애플리케이션 원격 설치용 타사 도구를 사용합니다.
- 운영 체제와 네트워크 에이전트가 설치된 관리자 하드 드라이브의 이미지를 복제하거나, Kaspersky Security Center에서 제공하는 디스크 이미지 처리용 도구를 사용하거나, 타사 도구를 사용합니다.
- Windows 그룹 정책을 사용하여 그룹 정책용 표준 Windows 관리 도구를 사용하거나, Kaspersky Security Center의 원격 설치 작업에서 해당하는 전용 옵션을 통해 자동 모드로 설치합니다.
- 강제 모드에서 Kaspersky Security Center의 원격 설치 작업을 통해 운영 체제 리소스를 사용합니다.
- 기기 사용자에게 Kaspersky Security Center에서 생성된 독립 실행형 패키지의 링크를 전송합니다. 독립 실행형 패키지는 선택한 애플리케이션의 배포 패키지를 포함하는 설정이 정의된 실행 모듈입니다.
- 기기에서 애플리케이션 설치 관리자를 실행하여 수동으로 수행합니다.

Linux를 실행하는 관리 중인 기기에 네트워크 에이전트를 최초 설치하는 방법은 다음과 같습니다.

- SSH를 통해 관리 중인 기기에 연결하고 원격 설치 작업을 실행합니다.
- 관리 중인 기기에서 패키지 설치를 실행합니다.

macOS를 실행하는 관리 중인 기기에 네트워크 에이전트를 최초 설치하는 방법은 다음과 같습니다.

- macOS 배포 지점에서 원격 설치 작업을 실행합니다.
- 기기 사용자에게 Kaspersky Security Center에서 생성된 독립 실행형 패키지의 링크를 전송합니다. 독립 실행형 패키지는 선택한 애플리케이션의 배포 패키지가 포함되어 있고 설정이 사전 정의된 실행 모듈입니다.

기기에 네트워크 에이전트를 설치한 후, 이 네트워크 에이전트를 통해 해당 기기에 Kaspersky 애플리케이션 원격 설치를 진행할 수 있습니다. 설치할 애플리케이션의 배포 패키지는 네트워크 에이전트와 중앙 관리 서버 간의 통신 채널을 통해 관리자가 정의한 설치 설정과 함께 전송됩니다. 릴레이 배포 노드, 즉 배포 지점, 멀티캐스트 전달 등을 사용하여 배포 패키지를 전송할 수 있습니다.

관리 네트워크에서 애플리케이션 배포를 위한 방법과 전략을 선택할 때는 다음과 같은 여러 가지 요인을 고려해야 합니다(일부만 제시됨).

- 조직의 네트워크 구성.
- 총 기기 개수.
- 조직 네트워크에서 Active Directory 도메인의 구성원이 아닌 기기의 유무 및 해당 기기에 대한 관리자 권한이 있는 통일 계정의 유무.
- 중앙 관리 서버와 기기 간의 채널 용량.

- 중앙 관리 서버와 원격 서브넷 간의 통신 유형 및 해당 서브넷의 네트워크 채널 용량.
- 배포 시작 시 원격 기기에 적용되는 보안 설정. 이러한 파라미터를 사용하면 관리 중인 기기에 대한 원격 연결을 설정하고 설치를 시작할 수 있습니다.

설치 관리자 구성

네트워크에서 Kaspersky 애플리케이션 배포를 시작하기 전에 애플리케이션 설치 중에 정의되는 설치 설정을 지정해야 합니다. 네트워크 에이전트를 설치할 때는 최소한 중앙 관리 서버 연결을 위한 주소를 지정해야 하며, 몇 가지 고급 설정도 필요할 수 있습니다. 선택한 설치 방법에 따라 각기 다른 방식으로 설정을 정의할 수 있습니다. 가장 단순한 방법(선택한 기기에서 수동 대화식 설치 수행)을 사용하는 경우에는 설치 관리자의 사용자 인터페이스에서 모든 관련 설정을 정의할 수 있습니다.

하지만 기기 그룹에서 숨김 모드로 애플리케이션을 설치할 때는 이러한 설정 정의 방법이 적절하지 않습니다. 일반적으로는 관리자가 중앙 집중식 모드에서 설정의 값을 지정해야 하며, 나중에 선택한 네트워크 연결 기기에서 숨김 모드로 설치를 수행할 때 이러한 값을 사용할 수 있습니다.

설치 패키지

애플리케이션 설치 설정을 정의하는 첫 번째 방법이자 기본 방법은 Kaspersky Security Center 도구와 대다수 타사 도구를 사용하는 모든 설치 방법에 적합한 범용 방법입니다. 이 방법을 사용할 때는 Kaspersky Security Center에서 애플리케이션 설치 패키지를 만듭니다.

다음과 같은 방법을 사용하여 설치 패키지를 생성합니다:

- 포함된 *설명자*(설치를 위한 규칙과 결과 분석 및 기타 정보를 포함하는 확장자가 .kud인 파일)를 기준으로 하여 지정한 배포 패키지에서 자동으로 생성
- 표준 또는 지원하는 애플리케이션에 대해서는 설치 프로그램의 실행 파일 또는 기본 형식(.msi, .deb, .rpm)의 설치 프로그램 사용

생성된 설치 패키지는 하위 폴더와 파일이 있는 폴더의 계층 구조로 구성됩니다. 설치 패키지에는 원본 배포 패키지 외에 편집 가능한 설정(설치를 완료하려면 운영 체제를 다시 시작해야 하는지 여부 등을 처리하기 위한 규칙과 설치 관리자의 설정 포함)과 부수적인 보조 모듈도 포함됩니다.

설치 패키지를 만들 때 관리 콘솔의 사용자 인터페이스에서 지원되는 개별 애플리케이션과 관련된 설치 설정의 값을 정의할 수 있습니다. Kaspersky Security Center 도구를 통해 애플리케이션 원격 설치를 수행할 때는 설치 패키지가 기기로 전송되므로, 애플리케이션의 설치 관리자를 실행하면 관리자가 정의한 모든 설정이 해당 애플리케이션에 제공됩니다. Kaspersky 애플리케이션 설치를 위해 타사 도구를 사용하는 경우에는 기기에서 전체 설치 패키지를 사용할 수 있는지, 즉 배포 패키지와 해당 설정을 사용할 수 있는지만 확인하면 됩니다. Kaspersky Security Center에서는 공유 폴더 내의 전용 하위 폴더에 설치 패키지를 만들어서 저장합니다.

> 설치 패키지 파라미터에서 권한 있는 사용자 계정의 세부정보를 입력하지 마십시오.

타사 도구를 통한 배포 전에 Kaspersky 애플리케이션에 이 구성 방법을 사용하는 방법에 대한 자세한 내용은 "Microsoft Windows의 그룹 정책을 사용하는 배포" 섹션을 참조하십시오.

Kaspersky Security Center를 설치한 직후에는 설치 패키지 몇 개가 자동으로 생성됩니다; 이러한 패키지는 Microsoft Windows용 보안 제품 패키지와 네트워크 에이전트 패키지를 포함하며 즉시 설치 가능합니다.

설치 패키지의 속성에서 애플리케이션의 라이센스 키를 설정할 수는 있지만, 이러한 라이센스 배포 방법은 사용하지 않는 것이 좋습니다. 속성에서 키를 설정하면 설치 패키지 읽기 권한을 쉽게 확보할 수 있기 때문입니다. 자동으로 배포되는 라이센스 키를 사용하거나 라이센스 키 설치 작업을 사용해야 합니다.

MSI 속성 및 변환 파일

Windows 플랫폼에서 설치를 구성하는 또 다른 방법은 MSI 속성 및 변환 파일을 정의하는 것입니다. 다음과 같은 경우에 이 방법을 적용할 수 있습니다:

- Windows 그룹 정책을 통해 설치할 때(일반 Microsoft 도구 또는 Windows 그룹 정책 처리용 기타 타사 도구 사용).
- Microsoft Installer 형식 설치 관리자 처리용 타사 도구를 사용하여 애플리케이션을 설치할 때.

애플리케이션 원격 설치용 타사 도구를 사용한 배포

Microsoft System Center 등의 애플리케이션 원격 설치용 도구가 조직에서 제공되는 경우에는 해당 도구를 사용하여 초기 배포를 수행하면 편리합니다.

이 경우 다음 작업을 수행해야 합니다:

- 사용할 배포 도구에 가장 적합한 설치 구성 방법을 선택합니다.
- 관리 콘솔 인터페이스를 통한 설치 패키지 설정 수정 작업과, 설치 패키지 데이터에서 애플리케이션 배포에 사용하도록 선택한 타사 도구의 작동을 동기화할 메커니즘을 정의합니다.
- 공유 폴더에서 설치를 수행할 때는 이 파일 리소스의 용량이 충분한지 확인해야 합니다.

Kaspersky Security Center의 원격 설치 작업에 대한 정보

Kaspersky Security Center에서는 애플리케이션 원격 설치를 위한 여러 가지 메커니즘을 제공합니다. 이러한 메커니즘은 원격 설치 작업(강제 설치, 하드 드라이브 이미지 복사를 통한 설치, Microsoft Windows 그룹 정책을 통한 설치)으로 구현됩니다. 지정한 관리 그룹과 특정 기기 또는 기기 조회에 모두 사용 가능한 원격 설치 작업을 만들 수 있습니다. 이러한 작업은 관리 콘솔의 **작업** 폴더에 표시됩니다. 작업을 만들 때는 해당 작업 내에서 설치할 설치 패키지(네트워크 에이전트 및/또는 기타 애플리케이션의 설치 패키지)를 선택할 수 있으며, 원격 설치 방법을 정의하는 특정 설정도 지정할 수 있습니다. 또한, 원격 설치 작업 생성과 결과 모니터링 기반의 원격 설치 마법사를 사용할 수도 있습니다.

관리 그룹에 대한 작업은 지정한 그룹에 포함되어 있는 기기와 해당 관리 그룹 내 모든 하위 그룹의 모든 기기에 영향을 줍니다. 작업에서 해당하는 설정을 작동하는 경우 그룹 또는 그룹의 하위 그룹에 포함된 보조 중앙 관리 서버의 기기에 대해 작업이 수행됩니다.

특정 기기에 대한 작업을 수행하면 작업이 시작될 때의 조회 컨텐츠에 따라 각 실행 시 클라이언트 기기 목록이 새로 고쳐집니다. 보조 중앙 관리 서버에 연결된 기기가 조회에 포함되는 경우에는 해당 기기에서도 작업이 실행됩니다. 이러한 설정 및 설치 방법에 대한 자세한 내용은 이 섹션의 뒷부분을 참조하십시오.

보조 중앙 관리 서버에 연결된 기기에서 원격 설치 작업이 정상적으로 작동하도록 하려면 전달 작업을 사용하여 작업에서 사용되는 설치 패키지를 해당하는 보조 중앙 관리 서버로 미리 전달해야 합니다.

기기 이미지 캡처 및 복사를 통한 배포

운영 체제 및 기타 소프트웨어도 설치(또는 재설치)해야 하는 기기에 네트워크 에이전트를 설치해야 한다면, 해당 기기의 이미지 캡처 및 복사 메커니즘을 사용할 수 있습니다.

하드 드라이브를 캡처 및 복사하여 배포를 수행하려면:

1. 운영 체제와 관련 소프트웨어(네트워크 에이전트 및 보안 제품 포함)가 설치되어 있는 참조 기기를 만듭니다.
2. 기기에서 참조 이미지를 캡처한 다음 Kaspersky Security Center의 전용 작업을 통해 새 기기에 해당 이미지를 배포합니다.

   디스크 이미지를 캡처하고 설치하려는 경우 조직에서 제공되는 타사 도구를 사용하거나, 취약점 및 패치 관리 라이센스에 따라 Kaspersky Security Center에서 제공하는 기능을 사용할 수 있습니다.

타사 도구를 사용하여 디스크 이미지를 처리하는 경우에는 참조 이미지에서 기기에 대한 배포를 수행할 때 Kaspersky Security Center에서 관리 중인 기기를 식별하는 데 사용하는 정보를 삭제해야 합니다. 이렇게 하지 않으면 중앙 관리 서버는 같은 이미지를 복사하여 생성한 기기를 올바르게 구분할 수 없습니다.

Kaspersky Security Center 도구를 사용하여 디스크 이미지를 캡처할 때는 이 문제가 자동으로 해결됩니다.

타사 도구를 사용하여 디스크 이미지 캡처

네트워크 에이전트가 설치된 기기의 이미지 캡처를 위해 타사 도구를 적용할 때는 다음 방법 중 하나를 사용합니다:

- 권장 방법. 참조 기기에 네트워크 에이전트를 설치할 때는, 네트워크 에이전트 서비스가 최초로 실행되기 전에 기기 이미지를 캡처합니다. 왜냐하면, 네트워크 에이전트가 중앙 관리 서버에 처음 연결할 때 기기를 식별하는 고유한 정보가 생성되기 때문입니다. 그 후에는 이미지 캡처 작업이 완료될 때까지 네트워크 에이전트 서비스를 실행하지 않는 것이 좋습니다.
- 참조 기기에서 네트워크 에이전트 서비스를 중지하고 -dupfix 키를 사용하여 klmover 유틸리티를 실행합니다. klmover 유틸리티는 네트워크 에이전트 설치 패키지에 포함되어 있습니다. 이미지 캡처 작업이 완료될 때까지는 네트워크 에이전트 서비스가 더 이상 실행되지 않도록 합니다.
- 이미지 배포 후 운영 체제가 처음 시작되면 대상 기기에서 네트워크 에이전트 서비스를 처음으로 실행하기 전에 -dupfix 키를 사용하여 klmover를 실행해야 합니다(필수 요구 사항). klmover 유틸리티는 네트워크 에이전트 설치 패키지에 포함되어 있습니다.
- 네트워크 에이전트 디스크 복제 모드를 사용합니다.

하드 드라이브 이미지가 잘못 복사되었다면 이 문제를 해결할 수 있습니다.

네트워크 에이전트가 설치되지 않은 기기의 이미지를 캡처할 수도 있습니다. 이렇게 하려면 대상 기기에서 이미지 배포를 수행한 다음 네트워크 에이전트를 배포합니다. 이 방법을 사용한다면 기기에서 독립 실행형 설치 패키지로 네트워크 폴더에 대한 액세스를 제공하십시오.

잘못된 하드 드라이브 이미지 복사

네트워크 에이전트가 설치된 하드 드라이브 이미지가 배포 규칙을 따르지 않고 복사되었다면, 일부 기기가 관리 콘솔에서 이름이 계속 변경되는 단일 아이콘으로 함께 표시될 수 있습니다.

다음 방법 중 하나를 사용해 이 문제를 해결할 수 있습니다:

- 네트워크 에이전트 제거

  가장 안정적인 방법입니다. 타사 도구를 사용하여 이미지에서 잘못 복사한 기기의 네트워크 에이전트를 제거한 후에 다시 설치해야 합니다. Kaspersky Security Center 도구를 통해 네트워크 에이전트를 제거할 수는 없습니다. 결함이 있는 기기가 관리 콘솔에서 모두 같은 아이콘으로 표시되므로, 중앙 관리 서버가 각 기기를 구분할 수 없기 때문입니다.

- "-dupfix" 키를 사용하여 klmover 유틸리티 실행

  이미지에서 잘못 복사한 결함이 있는 기기에 대해 타사 도구를 통해 "-dupfix" 키를 사용하여 네트워크 에이전트 설치 폴더에 있는 klmover 유틸리티를 실행합니다. Kaspersky Security Center 도구를 통해 이 유틸리티를 실행할 수는 없습니다. 결함이 있는 기기가 관리 콘솔에서 모두 같은 아이콘으로 표시되므로, 중앙 관리 서버가 각 기기를 구분할 수 없기 때문입니다.

  유틸리티를 실행하기 전에 결함이 있는 기기가 표시되었던 아이콘을 삭제합니다.

- 잘못 복사한 기기 탐지를 위한 규칙 강화.

  > 이 방법은 중앙 관리 서버와 네트워크 에이전트 버전 10 Service Pack 1 이상이 설치되어 있는 경우에만 적용됩니다.

  잘못 복사한 네트워크 에이전트를 탐지하기 위한 규칙을 강화하여 기기의 NetBIOS 이름을 변경하면 해당 네트워크 에이전트가 자동으로 "수정"되도록 해야 합니다. 이때 복사한 모든 기기의 NetBIOS 이름은 고유하다고 가정합니다.

  중앙 관리 서버가 설치된 기기에서는 아래에 나와 있는 레지스트리 파일을 레지스트리로 가져온 다음 중앙 관리 서버 서비스를 다시 시작해야 합니다.

  - 중앙 관리 서버가 설치된 기기에 32비트 운영 체제가 설치되어 있는 경우:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

  - 중앙 관리 서버가 설치된 기기에 64비트 운영 체제가 설치되어 있는 경우:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Microsoft Windows의 그룹 정책을 사용하는 배포

다음 조건이 충족되는 경우 Microsoft Windows 그룹 정책을 통해 네트워크 에이전트 초기 배포를 수행하는 것이 좋습니다:

- 이 기기는 Active Directory 도메인의 구성원입니다.
- 배포 구성에서 대상 기기에 대해 네트워크 에이전트 배포를 시작하기 전에 해당 기기의 다음 정기 다시 시작 시까지 기다리도록 허용하는 경우 또는 해당 기기에 Windows 그룹 정책을 강제로 적용할 수 있는 경우.

이 배포 구성은 다음과 같은 과정으로 진행됩니다:

- 공유 폴더(대상 기기의 LocalSystem 계정에 읽기 권한이 있는 폴더)에 Microsoft Installer 형식의 애플리케이션 배포 패키지(MSI 패키지)를 배치합니다.
- Active Directory 그룹 정책에서 배포 패키지용으로 설치 개체를 만듭니다.
- 대상 기기가 포함되는 조직 구성 단위(OU) 및 / 또는 보안 그룹을 지정하여 설치 범위를 설정합니다.
- 다음 번에 기기 사용자가 시스템에 로그인하기 전에 대상 기기가 도메인에 로그인하면 설치된 모든 애플리케이션에서 필요한 애플리케이션의 유무를 확인합니다. 애플리케이션을 찾을 수 없으면 정책에 지정된 리소스에서 배포 패키지를 다운로드하여 설치합니다.

이 배포 구성의 장점은 운영 체제가 로드되는 중에, 즉 사용자가 시스템에 로그인하기도 전에 할당된 애플리케이션이 대상 기기에 설치된다는 것입니다. 충분한 권한이 있는 사용자가 애플리케이션을 제거하더라도 다음 번에 운영 체제를 시작하면 애플리케이션이 다시 설치됩니다. 이 배포 구성의 단점은 추가 도구를 사용하지 않더라도 기기를 다시 시작할 때까지는 관리자가 그룹 정책에 대해 적용한 변경 사항이 적용되지 않는다는 것입니다.

네트워크 에이전트와 기타 애플리케이션의 개별 설치 관리자가 Windows Installer 형식이라면 그룹 정책을 사용하여 네트워크 에이전트와 기타 애플리케이션을 모두 설치할 수 있습니다.

이 배포 구성을 선택할 때는 Windows 그룹 정책을 적용한 후 기기에 복사할 파일을 가져올 파일 리소스에 대한 부하도 평가해야 합니다.

Kaspersky Security Center의 원격 설치 작업을 통해 Microsoft Windows 정책 처리

Microsoft Windows의 그룹 정책을 통해 애플리케이션을 설치하는 가장 간단한 방법은 Kaspersky Security Center의 원격 설치 작업 속성에서 **Active Directory 그룹 정책에 패키지 설치 지정** 옵션을 선택하는 것입니다. 이 경우 작업을 실행할 때 중앙 관리 서버가 다음 작업을 자동으로 수행합니다:

- Microsoft Windows의 그룹 정책에서 필요한 개체를 만듭니다.
- 전용 보안 그룹을 만들고 해당 그룹에 대상 기기를 포함한 다음 기기에 대해 선택한 애플리케이션 설치를 할당합니다. 작업을 실행할 때마다 실행 시점의 기기 풀에 따라 보안 그룹 집합이 업데이트됩니다.

이 기능이 작동하도록 하려면 작업 속성에서 Active Directory 그룹 정책에 대한 쓰기 권한이 있는 계정을 지정합니다.

같은 작업을 통해 네트워크 에이전트와 다른 애플리케이션을 모두 설치하려는 경우 **Active Directory 그룹 정책에 패키지 설치 지정** 옵션을 선택하면 애플리케이션이 Active Directory 정책에 네트워크 에이전트용 설치 개체만 만듭니다. 작업에서 선택한 두 번째 애플리케이션은 네트워크 에이전트가 기기에 설치되는 즉시 네트워크 에이전트의 도구를 통해 설치됩니다. Windows 그룹 정책을 통해 네트워크 에이전트 이외의 애플리케이션을 설치하려는 경우에는 네트워크 에이전트 패키지는 포함하지 않고 해당 설치 패키지 전용으로 설치 작업을 만들어야 합니다. Microsoft Windows 그룹 정책을 사용하여 모든 애플리케이션을 설치할 수 있는 것은 아닙니다. 이 기능에 대해 알아 보려면 애플리케이션 설치 방법에 대한 정보를 참조하십시오.

Kaspersky Security Center 도구를 사용하여 그룹 정책에서 필요한 개체를 만드는 경우에는 Kaspersky Security Center의 공유 폴더가 설치 패키지의 소스로 사용됩니다. 배포를 계획할 때는 이 폴더의 읽기 속도와 기기 개수, 그리고 설치할 배포 패키지의 크기 간 상관 관계를 파악해야 합니다. 고성능 전용 파일 저장소에 Kaspersky Security Center의 공유 폴더를 배치하면 유용할 수 있습니다.

Kaspersky Security Center를 통해 Windows 그룹 정책을 자동으로 만드는 방식은 쉽게 사용할 수 있을 뿐 아니라 다음과 같은 장점도 있습니다: 네트워크 에이전트 설치를 계획할 때 설치가 완료된 후 기기를 자동으로 이동할 Kaspersky Security Center 관리 그룹을 쉽게 지정할 수 있습니다. 원격 설치 작업의 설정 창이나 새 작업 마법사에서 이 그룹을 지정할 수 있습니다.

> Kaspersky Security Center를 통해 Windows 그룹 정책을 처리할 때는 보안 그룹을 만들어 그룹 정책 개체에 대해 기기를 지정할 수 있습니다. Kaspersky Security Center는 보안 그룹의 컨텐츠를 작업의 현재 기기 집합과 동기화합니다. 그룹 정책 처리를 위해 다른 도구를 사용할 때는 그룹 정책의 개체를 Active Directory의 선택한 OU와 직접 연결할 수 있습니다.

Microsoft Windows 정책을 통한 애플리케이션 무지원 설치

관리자는 자신을 대신하여 Windows 그룹 정책에서 설치를 수행하는 데 필요한 개체를 만들 수 있습니다. 이 경우 관리자는 Kaspersky Security Center의 공유 폴더에 저장된 패키지의 링크를 제공하거나, 전용 파일 서버에 해당 패키지를 업로드한 다음 패키지의 링크를 제공할 수 있습니다.

가능한 설치 시나리오는 다음과 같습니다:

- 관리자가 설치 패키지를 만들고 관리 콘솔에서 패키지의 속성을 설정합니다. 그룹 정책 개체가 Kaspersky Security Center의 공유 폴더에 저장된 이 패키지의 MSI 파일 링크를 제공합니다.
- 관리자가 설치 패키지를 만들고 관리 콘솔에서 패키지의 속성을 설정합니다. 그런 다음 이 패키지의 전체 EXEC 하위 폴더를 Kaspersky Security Center의 공유 폴더에서 조직의 전용 파일 리소스에 있는 폴더로 복사합니다. 그룹 정책 개체가 조직의 전용 파일 리소스에 있는 하위 폴더에 저장된 이 패키지의 MSI 파일 링크를 제공합니다.
- 관리자가 네트워크 에이전트의 패키지를 포함한 애플리케이션 배포 패키지를 인터넷에서 다운로드하여 조직의 전용 파일 리소스에 업로드합니다. 그룹 정책 개체가 조직의 전용 파일 리소스에 있는 하위 폴더에 저장된 이 패키지의 MSI 파일 링크를 제공합니다. MSI 속성을 구성하거나 MST 변환 파일을 구성하여 설치 설정을 정의합니다.

Kaspersky Security Center의 원격 설치 작업을 통한 강제 배포

네트워크 에이전트나 다른 애플리케이션의 초기 배포 수행을 위해, Kaspersky Security Center의 원격 설치 작업으로 선택한 설치 패키지를 강제 설치할 수 있습니다. 단, 기기마다 로컬 관리자 권한이 있는 사용자 계정이 있어야 합니다.

중앙 관리 서버가 기기에 직접 접근할 수 없을 때도 강제 설치를 적용할 수 있습니다: 기기가 격리된 네트워크에 있거나, 기기는 로컬 네트워크에 있고 중앙 관리 서버 항목은 DMZ에 있을 때를 예로 들 수 있습니다.

초기 배포 시 네트워크 에이전트가 설치되지 않습니다. 따라서 원격 설치 작업의 설정에서 네트워크 에이전트를 사용하여 애플리케이션 설치에 필요한 파일 배포를 선택할 수 없습니다. 중앙 관리 서버나 배포 지점을 통해서만 운영 체제 리소스를 사용하여 파일을 배포할 수 있습니다.

대상 기기에 대한 관리 권한이 있는 계정으로 중앙 관리 서버 서비스를 실행해야 합니다. 또는 원격 설치 작업의 설정에서 admin$ 공유에 접근 권한이 있는 계정을 지정할 수 있습니다.

> 기본적으로 원격 설치 작업은 중앙 관리 서버를 실행하는 계정의 자격 증명을 사용하여 기기에 적용됩니다. 이 계정이 원격 설치 작업 실행에 사용하는 계정이 아닌, admin$ 공유 접근에 사용하는 계정임을 분명히 해야 합니다. 설치가 LocalSystem 계정으로 수행됩니다.

대상 기기가 속하는 Kaspersky Security Center 관리 그룹을 선택하거나, 특정 기준에 따라 기기 조회를 만들어 목록으로 대상 기기를 명시적으로 지정할 수 있습니다. 설치 시작 시간은 작업 스케줄에 따라 정의됩니다. 작업 속성에서 **누락된 작업 실행** 설정을 활성화하면 대상 기기가 켜진 직후나 대상 관리 그룹으로 이동될 때 작업을 실행할 수 있습니다.

강제 설치 시에는 설치 패키지를 대상 기기로 전달하고, 파일을 각 대상 기기의 admin$ 리소스에 복사하고, 해당 기기에서 지원 서비스를 원격 등록합니다. 네트워크 상호 작용을 수행할 수 있도록 하는 Kaspersky Security Center 기능을 통해 대상 기기로 설치 패키지를 전달합니다. 이 경우 다음 조건이 충족되어야 합니다:

- 대상 기기는 중앙 관리 서버나 배포 지점 측에서 액세스할 수 있습니다.
- 네트워크에서 대상 기기에 대한 이름 해석이 정상 작동합니다.
- 대상 기기에서 관리 공유(admin$)가 작동하는 상태로 유지되어야 합니다.
- 대상 기기에서 다음 시스템 서비스가 실행 중입니다:
  - Server(LanmanServer)
    이 서비스는 기본적으로 실행 중입니다.
  - DCOM Server Process Launcher(DcomLaunch)
  - RPC Endpoint Mapper(RpcEptMapper)
  - Remote Procedure Call(RpcSs)
- Windows Management Instrumentation을 통한 원격 접근 활성화를 위해 TCP 445 포트가 대상 기기에서 열려 있습니다.
  또한, 원격 설치를 수행하기 전에 대상 기기의 운영 체제 유형을 결정하기 위해 TCP 포트 445를 확인합니다 (UDP 137을 사용할 수 없는 경우).

  > TCP 139, UDP 137, UDP 138은 이전 프로토콜에서 사용되며, 현재 애플리케이션에서는 이제 필요하지 않습니다.

  중앙 관리 서버와 배포 지점에서 대상 기기로 연결하려면, 방화벽에서 동적 아웃바운드 액세스 포트를 허용해야 합니다.
- 네트워크 에이전트 배포 중 Active Directory 도메인 정책 보안 설정이 NTLM 프로토콜의 동작을 제공할 수 있습니다.
- Microsoft Windows XP를 실행하는 대상 기기에서는 단순 파일 공유 모드를 중지합니다.

- 대상 기기에서, 접근 공유 및 보안 모델은 *클래식(로컬 사용자가 본인으로 인증)*으로 설정됩니다. 이는 *게스트 전용(로컬 유저가 게스트로 인증)*일 수 없습니다.

- 대상 기기가 도메인의 구성원이거나 대상 기기에서 관리자 권한이 있는 통일 계정을 미리 만들어야 합니다.

Windows Server 2003 이상 Active Directory 도메인에 가입되지 않은 기기에 네트워크 에이전트나 기타 애플리케이션을 배포하려면, 해당 기기에서 UAC를 비활성화해야 합니다. 원격 UAC는 로컬 관리 계정이 네트워크 에이전트나 다른 애플리케이션의 강제 배포에 필요한 admin$에 접근하지 못하는 이유 중 하나입니다. 원격 UAC를 중지해도 로컬 UAC에 영향을 주지 않습니다.

아직 Kaspersky Security Center 관리 그룹에 할당되지 않은 새 기기에 설치를 수행하는 중에 원격 설치 작업 속성을 열고 네트워크 에이전트를 설치한 후 기기를 이동할 관리 그룹을 지정할 수 있습니다.

그룹 작업을 만들 때는 각 그룹 작업이 선택한 그룹 내에 중첩된 모든 그룹의 모든 기기에 적용된다는 점을 기억하십시오. 그러므로 하위 그룹에 중복된 설치 작업을 포함하면 안 됩니다.

자동 설치를 활용하면 애플리케이션 강제 설치 작업을 간단히 생성할 수 있습니다. 이렇게 하려면 관리 그룹 속성을 열고 설치 패키지 목록을 연 다음 이 그룹의 기기에 설치해야 하는 패키지를 선택해야 합니다. 그러면 이 그룹과 모든 해당 하위 그룹의 모든 기기에 선택한 설치 패키지가 자동으로 설치됩니다. 패키지가 설치되는 시간 간격은 네트워크 처리 성능과 총 네트워크 연결 기기 개수에 따라 달라집니다.

대상 기기로 설치 패키지를 전달하는 동안 중앙 관리 서버의 부하를 줄이기 위해 설치 작업에서 배포 지점을 통한 설치를 선택할 수 있습니다. 이 설치 방법을 사용하면 배포 지점 역할을 하는 기기의 부하가 크게 증가합니다. 따라서 배포 지점의 요구 사항을 충족하는 기기를 선택하는 것이 좋습니다. 배포 지점을 사용한다면 배포 지점이 대상 기기를 호스팅하는 격리된 각 서브넷에 있는지 확인해야 합니다.

저용량 채널을 통해 중앙 관리 서버와 통신하는 서브넷의 기기에서 설치를 수행할 때 동일 서브넷의 기기 간에 더 광범위한 채널을 사용할 수 있는 경우에도 배포 지점을 로컬 설치 센터로 사용하는 방식이 유용할 수 있습니다.

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 폴더가 있는 파티션의 디스크 여유 공간은 설치되는 애플리케이션의 배포 패키지 총 크기보다 커야 합니다.

Kaspersky Security Center에서 만든 독립 실행형 패키지 실행

앞에서 설명한 네트워크 에이전트 및 기타 애플리케이션의 초기 배포 방법을 항상 구현할 수 있는 것은 아닙니다. 해당하는 모든 조건을 충족할 수는 없기 때문입니다. 이러한 경우에는 설치 패키지와 관리자가 준비한 관련 설치 설정을 함께 사용하여 Kaspersky Security Center를 통해 *독립 실행형 설치 패키지*라는 일반 실행 파일을 만들 수 있습니다. 독립 실행형 설치 패키지는 Kaspersky Security Center의 공유 폴더에 저장됩니다.

Kaspersky Security Center를 통해 공유 폴더 내의 이 파일에 대한 링크가 포함된 이메일 메시지를 선택한 사용자에게 전송하여 대화식 모드나 숨김 설치용 "-s" 키를 사용해 파일을 실행하라는 메시지를 표시할 수 있습니다. 독립 실행형 설치 패키지를 이메일 메시지에 첨부한 다음 Kaspersky Security Center의 공유 폴더 접근 권한이 없는 기기 사용자에게 전송할 수 있습니다. 관리자는 이동식 드라이브에 독립 실행형 패키지를 복사하여 관련 기기로 전송한 다음 나중에 실행할 수도 있습니다.

네트워크 에이전트 패키지나 보안 제품과 같은 기타 애플리케이션의 패키지 중 하나 또는 두 패키지에서 모두 독립 실행형 패키지를 만들 수 있습니다. 네트워크 에이전트와 기타 애플리케이션에서 모두 독립 실행형 패키지를 만든 경우에는 네트워크 에이전트를 사용하여 설치가 시작됩니다.

네트워크 에이전트를 사용하여 독립 실행형 패키지를 만들 때는 새 기기(관리 그룹에 미할당 기기)에서 네트워크 에이전트 설치가 완료되면 해당 기기를 자동으로 이동할 관리 그룹을 지정할 수 있습니다.

독립 실행형 패키지는 대화식 모드(기본값)로 실행하여 패키지에 포함된 애플리케이션의 설치 결과를 표시할 수도 있고, "-s" 키를 사용하여 실행하는 경우 숨김 모드로 실행할 수도 있습니다. 스크립트(예: 운영 체제 이미지를 배포한 후에 실행되도록 구성된 스크립트)에서 설치하려는 경우 숨김 모드를 사용할 수 있습니다. 숨김 모드에서 수행된 설치 결과는 프로세스의 반환 코드를 통해 확인할 수 있습니다.

독립 실행형 Linux용 네트워크 에이전트에는 nmap 유틸리티의 선택적인 종속성이 있습니다. nmap 유틸리티가 없거나 버전 6.0 이하인 경우 DHCP 검색 브로드캐스트 기능이 지원되지 않습니다.

애플리케이션 수동 설치용 옵션

관리자나 숙련된 사용자는 대화식 모드에서 수동으로 애플리케이션을 설치할 수 있습니다. 이때 원본 배포 패키지를 사용할 수도 있고, 원본 배포 패키지에서 생성되어 Kaspersky Security Center의 공유 폴더에 저장된 설치 패키지를 사용할 수도 있습니다. 기본적으로 설치 관리자는 대화식 모드로 실행되며 사용자에게 필요한 모든 값을 입력하라는 메시지를 표시합니다. 그러나 "-s" 키를 사용하여 설치 패키지 루트에서 setup.exe 프로세스를 실행할 때는 설치 관리자가 설치 패키지를 구성할 때 정의한 설정을 사용하여 숨김 모드로 실행됩니다.

Kaspersky Security Center의 공유 폴더에 저장된 설치 패키지의 루트에서 setup.exe를 실행할 때는 패키지가 먼저 임시 로컬 폴더에 복사된 후에 해당 로컬 폴더에서 애플리케이션 설치 관리자가 실행됩니다.

MST 파일 생성

MSI 패키지의 콘텐츠를 변환하고 사용자 지정 설정을 기존 MSI 파일에 적용하려면 MST 형식의 변환 파일을 만들어야 합니다. 이렇게 하려면 Windows SDK에 포함된 Orca.exe 편집기를 사용합니다.

MST 파일을 생성하려면:

1. Orca.exe 편집기를 실행합니다.
2. **파일** 탭으로 이동하고 메뉴에서 **열기**를 클릭합니다.
3. Kaspersky Network Agent.msi 파일을 선택합니다.
4. **변환** 탭으로 이동한 후 메뉴에서 **새 변환**을 선택합니다.
5. **표** 열에서 **속성**을 선택하고 다음 값을 기록합니다.
   - *EULA=1*
   - *SERVERADDRESS=<중앙 관리 서버 주소>*

   저장 버튼을 누릅니다.
6. **변환** 탭으로 이동한 후 메뉴에서 **변환 생성**을 선택합니다.
7. 창이 열리면 생성하는 변환 파일의 이름을 지정한 다음 **저장** 버튼을 클릭합니다.

MST 파일이 저장됩니다.

네트워크 에이전트가 설치된 기기에 애플리케이션 원격 설치

기본 중앙 관리 서버나 해당 보조 서버에 연결된 작동 가능한 네트워크 에이전트가 기기에 설치되어 있으면 해당 기기에서 네트워크 에이전트를 업그레이드할 수 있을 뿐 아니라 네트워크 에이전트를 통해 지원되는 애플리케이션을 설치, 업그레이드 또는 제거할 수도 있습니다.

원격 설치 작업의 속성에서 **네트워크 에이전트 이용** 옵션을 활성화할 수 있습니다.

이 옵션을 선택하면 관리자가 정의한 설치 설정이 포함된 설치 패키지가 네트워크 에이전트와 중앙 관리 서버 간의 통신 채널을 통해 대상 기기로 전송됩니다.

중앙 관리 서버의 부하를 최적화하고 중앙 관리 서버와 기기 간의 트래픽을 최소화하려는 경우 모든 원격 네트워크 또는 모든 브로드캐스팅 도메인에 배포 지점을 할당하면 유용합니다("배포 지점 정보" 및 "관리 그룹 구조 작성 및 배포 지점 할당" 섹션 참조). 이 경우 설치 패키지와 설치 관리자 설정은 배포 지점을 통해 중앙 관리 서버에서 대상 기기로 배포됩니다.

또한 설치 패키지 브로드캐스팅(멀티캐스트) 전송에 배포 지점을 사용할 수도 있습니다. 이렇게 하면 애플리케이션을 배포할 때 네트워크 트래픽을 크게 줄일 수 있습니다.

네트워크 에이전트와 중앙 관리 서버 간의 통신 채널을 통해 대상 기기로 설치 패키지를 전송할 때는 전송용으로 준비한 모든 설치 패키지가 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer 폴더에도 캐시됩니다. 다양한 유형의 대형 설치 패키지 여러 개를 사용하며 많은 수의 배포 지점을 작업에 포함하는 경우에는 이 폴더의 크기가 매우 커질 수 있습니다.

FTServer 폴더에서 파일을 수동으로 삭제할 수는 없습니다. 원본 설치 패키지를 삭제하면 해당하는 데이터가 FTServer 폴더에서 자동으로 삭제됩니다.

배포 지점에 의해 받은 데이터는 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp 폴더에 저장됩니다.

$FTCITmp 폴더에서 파일을 수동으로 삭제할 수는 없습니다. 이 폴더에서 데이터를 사용하는 작업이 완료되면 이 폴더의 컨텐츠가 자동으로 삭제됩니다.

설치 패키지는 중앙 관리 서버와 네트워크 에이전트 간의 통신 채널을 통해 네트워크 전송에 최적화된 형식으로 중간 저장소에서 배포되므로, 각 설치 패키지의 원래 폴더에 저장된 설치 패키지를 변경할 수는 없습니다. 해당 변경 사항은 중앙 관리 서버를 통해 자동으로 등록되지 않습니다. 설치 패키지의 파일은 수동으로 수정하지 않는 것이 좋지만, 수동으로 수정해야 한다면 관리 콘솔에서 설치 패키지의 설정을 편집해야 합니다. 관리 콘솔에서 설치 패키지의 설정을 편집하면 중앙 관리 서버가 대상 기기로 전송하기 위해 준비했던 캐시의 패키지 이미지를 업데이트합니다.

원격 설치 작업에서 기기 다시 시작 관리

특히 Windows에서는 애플리케이션 원격 설치를 완료하려면 기기를 다시 시작해야 하는 경우가 많습니다.

Kaspersky Security Center의 원격 설치 작업 사용 시, 새 작업 마법사 또는 생성된 작업의 속성 창(**운영 체제 다시 시작** 섹션)에서 Windows 기기를 다시 시작해야 할 때 수행할 작업을 선택할 수 있습니다:

- **기기 다시 시작 안 함**. 이 옵션을 선택하면 자동 다시 시작이 수행되지 않습니다. 설치를 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 설치 작업에 적합합니다.

- **기기 다시 시작**. 이 옵션을 선택하면 설치를 완료하기 위해 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 설치 작업에 유용합니다.

- **사용자 확인 후 실행**. 이 경우 클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. **사용자 확인 후 처리**는 사용자가 기기를 다시 시작할 가장 편리한 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합한 옵션입니다.

보안 제품의 설치 패키지에서 데이터베이스를 업데이트하는 작업의 적합성

보호 배포를 시작하기 전에 보안 제품 배포 패키지와 함께 제공된 안티 바이러스 데이터베이스(자동 패치 모듈 포함) 업데이트 가능성을 고려해야 합니다. 배포를 시작하기 전에 선택한 설치 패키지의 마우스 오른쪽 메뉴에서 해당하는 명령을 사용하는 등의 방법으로 애플리케이션의 설치 패키지에서 데이터베이스를 업데이트하면 유용합니다. 이렇게 하면 대상 기기에서 보호 배포를 완료하는 데 필요한 다시 시작 횟수를 줄일 수 있습니다.

Kaspersky Security Center의 애플리케이션 원격 설치 도구를 사용하여 관리 중인 기기에서 관련 실행 파일 실행

새 패키지 마법사를 사용하면 실행 파일을 선택하고 해당 파일에 대해 명령줄 설정을 정의할 수 있습니다. 이를 위해 선택한 파일 자체나 해당 파일이 저장된 전체 폴더를 설치 패키지에 추가할 수 있습니다. 그런 후에는 원격 설치 작업을 만들고 작성된 설치 패키지를 선택해야 합니다.

작업이 실행되는 동안 명령 프롬프트의 정의된 설정을 포함하는 지정된 실행 파일이 대상 기기에서 실행됩니다.

Microsoft Windows Installer(MSI) 형식의 설치 관리자를 사용하는 경우 Kaspersky Security Center에서 표준 도구를 통해 설치 결과를 분석합니다.

취약점 및 패치 관리 라이센스를 사용할 수 있는 경우에는 기업 환경에서 지원되는 애플리케이션용 설치 패키지를 만들 때 Kaspersky Security Center가 업데이트 가능 데이터베이스에 포함되어 있는 설치 결과 분석 내용과 설치를 위한 규칙도 사용합니다.

그렇지 않은 경우 실행 파일에 대한 기본 작업은 실행 중인 프로세스 및 모든 자식 프로세스가 완료될 때까지 대기합니다. 실행 중인 프로세스가 모두 완료되고 나면 초기 프로세스의 반환 코드에 관계없이 작업이 정상적으로 완료됩니다. 이 작업의 해당 동작을 변경하려면 작업을 만들기 전에 Kaspersky Security Center가 새로 작성된 설치 패키지의 폴더 및 하위 폴더에 생성한 .kud 파일을 수동으로 수정해야 합니다.

.kpd 파일은 ASCII 인코딩을 사용합니다. .kud 파일은 유니코드 인코딩을 사용합니다.

작업이 실행 중인 프로세스가 완료될 때까지 대기하지 않도록 하려면 [SetupProcessResult] 섹션에서 Wait 설정의 값을 0으로 설정합니다:

```
[SetupProcessResult]
Wait=0
```

작업이 Windows에서 실행 중인 프로세스만 완료될 때까지 대기하고 모든 자식 프로세스가 완료되기를 대기하지는 않도록 하려면 다음과 같이 [SetupProcessResult] 섹션에서 WaitJob 설정의 값을 0으로 설정합니다:

```
[SetupProcessResult]
WaitJob=0
```

작업이 완료되거나 실행 중인 프로세스의 반환 코드에 따라 오류를 반환하도록 하려면, 다음과 같이 오류 코드를 파일에 저장하는 실행 가능한 .bat 파일을 만듭니다.

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

그런 다음 새로 만든 설치 패키지의 폴더에 있는 Kaspersky Security Center가 생성한 .kud 파일을 수정합니다.

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

이 경우에는 목록에 포함된 코드 이외의 코드가 반환되면 오류가 반환됩니다.

작업 정상 완료 또는 오류에 대한 주석이 포함된 문자열을 작업 결과에 표시하려면 다음과 같이 [SetupProcessResult_SuccessCodes] 및 [SetupProcessResult_ErrorCodes] 섹션에 프로세스 반환 코드에 해당하는 오류의 간단한 설명을 입력합니다:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

작업 완료를 위해 기기를 다시 시작해야 하는 경우 Kaspersky Security Center 도구를 사용하여 기기 다시 시작을 관리하려면 다시 시작을 수행해야 함을 나타내는 프로세스의 반환 코드를 [SetupProcessResult_NeedReboot] 섹션에 포함합니다:

```
[SetupProcessResult_NeedReboot]
3010=
```

배포 모니터링

Kaspersky Security Center 배포를 모니터링하고 보안 제품과 네트워크 에이전트가 관리 중인 기기에 설치되었는지 확인하려면 **배포** 섹션의 표시등을 확인해야 합니다. 이 표시등은 관리 콘솔 기본 창의 중앙 관리 서버 노드 작업 영역에 있습니다. 표시등은 현재 배포 상태를 반영합니다. 네트워크 에이전트와 보안 제품이 설치된 기기의 수가 표시등 옆에 표시됩니다. 실행 중인 설치 작업이 있으면 여기서 해당 진행률을 모니터링할 수 있습니다. 설치 오류 발생 시에는 오류 수가 여기에 표시됩니다. 링크를 클릭하여 오류의 세부 정보를 확인할 수 있습니다.

그룹 탭에서 **관리 중인 기기** 폴더 작업 영역에 있는 배포 스키마를 사용할 수도 있습니다. 이 차트에는 배포 프로세스가 반영되어 네트워크 에이전트가 설치된/설치되지 않은 기기 또는 네트워크 에이전트와 보안 제품이 모두 설치된 기기의 수가 표시됩니다.

배포 진행률이나 특정 설치 작업의 동작에 대한 추가 세부 사항을 확인하려면 관련 원격 설치 작업의 결과 창을 엽니다: 작업을 오른쪽 클릭하고 마우스 오른쪽 메뉴에서 **결과**를 선택합니다. 그러면 창에 두 개의 목록이 표시됩니다: 위쪽 목록에는 기기의 작업 상태가 포함되어 있고, 아래쪽 목록에는 현재 위쪽 목록에서 선택한 기기의 작업 이벤트가 포함되어 있습니다.

배포 오류에 대한 정보는 중앙 관리 서버의 Kaspersky 이벤트 로그에 추가됩니다. 중앙 관리 서버 노드의 **이벤트** 탭에서 해당하는 이벤트 조회를 통해 오류에 대한 정보를 확인할 수도 있습니다.

설치 관리자 구성

이 섹션에서는 Kaspersky Security Center 설치 관리자의 파일과 설치 설정에 대한 정보, 그리고 중앙 관리 서버 및 네트워크 에이전트를 숨김 모드로 설치하기 위한 권장 방법을 제공합니다.

일반 정보

Kaspersky Security Center 15.1의 구성 요소(중앙 관리 서버, 네트워크 에이전트, 관리 콘솔) 설치 관리자는 Windows Installer 기술을 기반으로 작성되었습니다. 설치 관리자의 핵심 요소는 MSI 패키지입니다. 이 패키징 형식에서는 Windows Installer에서 제공하는 모든 이점: 확장성, 패칭 시스템 사용 가능성, 변환 시스템, 타사 솔루션을 통한 중앙 집중식 설치, 운영 체제에 대한 자동 등록 등을 사용할 수 있습니다.

숨김 모드로 설치 (응답 파일 사용)

중앙 관리 서버 및 네트워크 에이전트의 설치 관리자에는 응답 파일(ss_install.xml) 사용 기능이 포함되어 있습니다. 이 파일에는 사용자의 작업 없이 숨김 모드로 설치를 수행하기 위한 파라미터가 통합되어 있습니다. ss_install.xml 파일은 MSI 패키지와 같은 폴더에 있습니다; 숨김 모드로 설치하는 동안 이 파일이 자동으로 사용됩니다. 명령줄 키 "/s"로 숨김 설치 모드를 활성화할 수 있습니다.

실행 방법의 대략적인 예는 다음과 같습니다:

```
setup.exe /s
```

숨김 모드에서 설치 프로그램을 시작하기 전에 EULA(최종 사용자 라이센스 계약서)를 읽어 보십시오. Kaspersky Security Center 배포 키트에 EULA 텍스트가 있는 TXT 파일이 없다면 Kaspersky 웹사이트에서 다운로드할 수 있습니다.

ss_install.xml 파일은 Kaspersky Security Center 설치 관리자 파라미터의 내부 형식 인스턴스입니다. 배포 패키지에는 기본 파라미터가 들어 있는 ss_install.xml 파일이 포함됩니다.

ss_install.xml 파일을 수동으로 수정하지 마십시오. 관리 콘솔에서 설치 패키지의 파라미터를 편집할 때 Kaspersky Security Center의 도구를 통해 이 파일을 수정할 수 있습니다.

중앙 관리 서버 설치를 위한 응답 파일을 수정하려면:

1. Kaspersky Security Center 배포 패키지를 엽니다. 전체 패키지 EXE 파일 사용 시, 압축을 풉니다.
2. Server 폴더에서 명령줄을 열고 다음 명령을 실행합니다:

   ```
   setup.exe /r ss_install.xml
   ```

   Kaspersky Security Center 설치 프로그램이 시작됩니다.
3. 마법사의 단계를 따라 Kaspersky Security Center 설치를 구성하십시오.

   마법사를 완료하면 지정한 새 설정에 따라 응답 파일이 자동으로 수정됩니다.

숨김 모드로 네트워크 에이전트 설치(응답 파일 사용 안 함)

표준 방식으로 MSI 속성 값을 지정하여 단일 msi 패키지를 사용해 네트워크 에이전트를 설치할 수 있습니다. 이 경우 그룹 정책을 사용하여 네트워크 에이전트를 설치할 수 있습니다.

설치 패키지 Kaspersky Network Agent.msi의 이름을 바꾸지 마십시오. 이 패키지 이름을 바꾸면 네트워크 에이전트의 향후 업데이트 시 설치 오류가 발생할 수 있습니다.

응답 파일에 정의된 파라미터와 MSI 속성을 통해 정의하는 파라미터 간의 충돌을 방지하려는 경우 `DONT_USE_ANSWER_FILE=1` 속성을 설정하여 응답 파일을 중지할 수 있습니다. MSI 파일은 Kaspersky Security Center 배포 패키지의 Packages\NetAgent\exec 폴더에 있습니다. msi 패키지를 사용하여 네트워크 에이전트 설치 관리자를 실행하는 방식의 예는 다음과 같습니다.

숨김 모드에서 네트워크 에이전트를 설치하려면 최종 사용자 라이센스 계약서의 조항에 동의해야 합니다. 최종 사용자 라이센스 계약서의 조항을 모두 읽고 이해했으며, 이에 동의하는 경우에만 `EULA=1` 파라미터를 사용하십시오.

```
예:
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

응답 파일(확장자가 mst인 파일)을 미리 준비하여 msi 패키지의 파라미터 설정을 정의할 수도 있습니다. 이 명령은 다음과 같이 표시됩니다:

```
예:
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

단일 명령에서 여러 응답 파일을 지정할 수 있습니다.

Windows 설치 프로그램을 사용하여 네트워크 에이전트를 업그레이드하려면 다음 명령을 실행하십시오.

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

setup.exe를 통한 부분 설치 구성

setup.exe를 통해 애플리케이션 설치를 실행할 때는 MSI의 모든 속성 값을 MSI 패키지에 추가할 수 있습니다.

이 명령은 다음과 같이 표시됩니다:

예:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

중앙 관리 서버 설치 파라미터

아래 표에는 중앙 관리 서버를 설치할 때 구성할 수 있는 MSI 속성에 대한 설명이 나와 있습니다. EULA 및 PRIVACYPOLICY를 제외한 모든 파라미터는 선택 사항입니다.

숨김 모드의 중앙 관리 서버 설치 파라미터

MSI 속성	설명	사용 가능한 값
EULA	라이센스 계약서 조건에 동의(필수)	• 1 – 최종 사용자 라이센스 계약서의 조건을 모두 읽고 이해했으며, 이에 동의합니다. • 다른 값 및 값 없음 – 라이센스 계약서 조건에 동의하지 않음(설치가 수행되지 않음).
PRIVACYPOLICY	개인정보취급방침 조건에 동의(필수)	• 1 – 개인정보취급방침에 설명된 대로 제 데이터가 처리되고 전송(제3국으로의 전송 포함)되는 것을 알고 있으며 이에 동의합니다. 개인정보취급방침을 모두 읽고 이해했음을 확인합니다. • 다른 값 및 값 없음 - 개인정보취급방침 조건에 동의하지 않음(설치가 수행되지 않음).
INSTALLATIONMODETYPE	중앙 관리 서버 설치 유형	• 표준 • 사용자 지정
INSTALLDIR	애플리케이션 설치 폴더	문자열 값.
ADDLOCAL	쉼표로 구분된 설치할 구성 요소 목록	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 중앙 관리 서버를 적절히 설치하기 위한 최소한의 구성 요소 목록: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	네트워크 크기	• NRT_1_100—1대 ~ 100대. • NRT_100_1000—101~1000대. • NRT_GREATER_1000 - 기기 1000대 초과.
SRV_ACCOUNT_TYPE	중앙 관리 서버 서비스 동작을 위한 사용자를 지정하는 방식	• SrvAccountDefault – 사용자 계정이 자동으로 만들어짐. • SrvAccountUser - 사용자 계정을 수동으로 정의함.
SERVERACCOUNTNAME	서비스의 사용자 이름	문자열 값.
SERVERACCOUNTPWD	서비스의 사용자 암호	문자열 값.
DBTYPE	데이터베이스 유형	• MySQL – MySQL 또는 MariaDB 데이터베이스가 사용됩니다. • MSSQL – Microsoft SQL Server(SQL Express) 데이터베이스가 사용됩니다.
MYSQLSERVERNAME	MySQL 또는 MariaDB 서버의 전체 이름	문자열 값.
MYSQLSERVERPORT	MySQL 또는 MariaDB 서버에 연결할 포트 번호	숫자 값.
MYSQLDBNAME	MySQL 또는 MariaDB 서버 데이터베이스의 이름	문자열 값.
MYSQLACCOUNTNAME	MySQL 또는 MariaDB 서버 데이터베이스 연결을 위한 사용자 이름	문자열 값.

MSI 속성	설명	사용 가능한 값
MYSQLACCOUNTPWD	MySQL 또는 MariaDB 서버 데이터베이스 연결을 위한 사용자 암호	문자열 값.
MSSQLCONNECTIONTYPE	MSSQL 데이터베이스의 사용 유형	• InstallMSSEE – 패키지에서 설치 • ChooseExisting – 설치된 서버 사용
MSSQLSERVERNAME	SQL Server 인스턴스의 전체 이름	문자열 값.
MSSQLDBNAME	SQL Server 데이터베이스의 이름	문자열 값.
MSSQLAUTHTYPE	SQL Server 연결을 위한 인증 방법	• Windows • SQLServer
MSSQLACCOUNTNAME	SQLServer 모드에서 SQL Server에 연결하기 위한 사용자 이름	문자열 값.
MSSQLACCOUNTPWD	SQLServer 모드에서 SQL Server에 연결하기 위한 사용자 암호	문자열 값.

CREATE_SHARE_TYPE	공유 폴더를 지정하는 방법	• Create - 새 공유 폴더 만들기. 이 경우 다음 속성을 정의해야 합니다:
		  • SHARELOCALPATH – 로컬 폴더의 경로
		  • SHAREFOLDERNAME – 폴더의 네트워크 이름
		• Null – EXISTSHAREFOLDERNAME 속성이 지정되어야 함

EXISTSHAREFOLDERNAME	기존 공유 폴더의 전체 경로	문자열 값.
SERVERPORT	중앙 관리 서버에 연결할 포트 번호입니다	숫자 값.
SERVERSSLPORT	SSL을 이용해 중앙 관리 서버에 연결할 경우의 포트 번호	숫자 값.
SERVERADDRESS	중앙 관리 서버 주소	문자열 값.
SERVERCERT2048BITS	중앙 관리 서버 인증서용 키 길이(비트)	• 1 – 중앙 관리 서버 인증서용 키 길이는 2048비트입니다. • 0 – 중앙 관리 서버 인증서용 키 길이는 1024비트입니다. • 값이 지정되지 않았다면 중앙 관리 서버 인증서용 키 크기는 2048비트입니다.
MOBILESERVERADDRESS	모바일 기기 연결을 위한 중앙 관리 서버의 주소; MobileSupport 구성 요소를 선택하지 않은 경우 무시됨	문자열 값.

네트워크 에이전트 설치 파라미터

아래 표에는 네트워크 에이전트를 설치할 때 구성할 수 있는 MSI 속성에 대한 설명이 나와 있습니다. EULA 및 SERVERADDRESS를 제외한 모든 파라미터는 선택 사항입니다.

숨김 모드의 네트워크 에이전트 설치 파라미터

MSI 속성	설명	사용 가능한 값
EULA	라이센스 계약서 조건에 동의	• 1 – 이 최종 사용자 라이센스 계약서의 이용 약관을 모두 읽고 이해했으며 수락하는 것에 동의합니다. • 0 - 라이센스 계약서 조건에 동의하지 않음(설치가 수행되지 않음). • 값이 없는 경우 - 라이센스 계약서 조건에 동의하지 않음(설치가 수행되지 않음).
DONT_USE_ANSWER_FILE	응답 파일에서 설치 설정 읽기	• 1–사용 안 함. • 다른 값 또는 값이 없는 경우 - 읽기.
INSTALLDIR	네트워크 에이전트 설치 폴더 경로	문자열 값.
SERVERADDRESS	중앙 관리 서버 주소 (필수)	문자열 값.
SERVERPORT	중앙 관리 서버에 연결할 포트 수	숫자 값.

MSI 속성	설명	사용 가능한 값
SERVERSSLPORT	SSL 프로토콜을 사용하여 중앙 관리 서버에 암호화된 연결을 설정하기 위한 포트 번호	숫자 값.
USESSL	SSL 연결을 사용할지 여부	• 1 - 사용. • 다른 값 또는 값이 없는 경우 - 사용 안 함.
OPENUDPPORT	UDP 포트를 열지 여부	• 1 - 열기. • 다른 값 또는 값이 없는 경우 - 열지 않음.
UDPPORT	UDP 포트 번호	숫자 값.
USEPROXY	프록시 서버를 사용할지 여부. 호환성을 위해 네트워크 에이전트 설치 패키지 설정에서 프록시 연결 설정을 지정하지 않는 것이 좋습니다.	• 1 - 사용. • 다른 값 또는 값이 없는 경우 - 사용 안 함.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	프록시 서버에 연결할 프록시 주소 및 포트 번호	문자열 값.
PROXYLOGIN	프록시 서버에 연결할 계정	문자열 값.
PROXYPASSWORD	프록시 서버에 연결하기 위한 계정의 암호(설치 패키지 파라미터에 권한 있는 계정의 세부 정보를 입력하지 마십시오).	문자열 값.
GATEWAYMODE	연결 게이트웨이 사용 모드	• 0 - 연결 게이트웨이 사용 안 함. • 1 - 이 네트워크 에이전트를 연결 게이트웨이로 사용. • 2 - 연결 게이트웨이를 통해 중앙 관리 서버에 연결.
GATEWAYADDRESS	연결 게이트웨이 주소	문자열 값.
CERTSELECTION	인증서를 받는 방법	• GetOnFirstConnection - 중앙 관리 서버에서 인증서 수신. • GetExistent - 기존 인증서 선택. 이 옵션을 선택하는 경우 CERTFILE 속성을 정의해야 함.
CERTFILE	인증서 파일 경로	문자열 값.
VMVDI	VDI(가상 데스크톱 인프라) 동적 모드 사용	• 1 - 설정. • 0—활성화하지 않음. • 값이 없는 경우—활성화하지 않음.
VMOPTIMIZE	하이퍼바이저에 대한 네트워크 에이전트 설정 최적 여부 확인	• 1 - 설정. • 0—활성화하지 않음. • 값이 없는 경우—활성화하지 않음.
LAUNCHPROGRAM	설치 완료 후 네트워크 에이전트 서비스의 시작 여부. VMVDI=1이라면 파라미터를 무시합니다	• 1 - 시작. • 다른 값 또는 값이 없는 경우 - 시작 안 함.
NAGENTTAGS	네트워크 에이전트 태그 (응답 파일에 지정된 태그보다 우선임)	문자열 값.

가상 인프라

Kaspersky Security Center는 가상 컴퓨터 사용을 지원합니다. 각 가상 머신에 네트워크 에이전트 및 보안 제품을 설치할 수 있으며 하이퍼바이저 수준에서 가상 머신을 보호할 수도 있습니다. 첫 번째 경우 표준 보안 애플리케이션이나 Kaspersky Security for Virtualization Light Agent를 사용하여 가상 머신을 보호할 수 있습니다. 두 번째 경우에는 Kaspersky Security for Virtualization Agentless를 사용할 수 있습니다.

Kaspersky Security Center는 가상 머신을 이전 상태로 롤백할 수 있습니다.

가상 컴퓨터 부하를 줄이기 위한 팁

가상 컴퓨터에 네트워크 에이전트를 설치할 때는 가상 컴퓨터에 거의 사용되지 않을 것으로 보이는 일부 Kaspersky Security Center 기능을 중지하는 것이 좋습니다.

가상 컴퓨터 또는 가상 컴퓨터 생성용 템플릿에 네트워크 에이전트를 설치할 때는 다음 작업이 권장됩니다.

- 원격 설치를 실행하는 경우 네트워크 에이전트 설치 패키지의 속성 창에 있는 **고급** 섹션에서 **VDI 설정 최적화** 옵션을 선택합니다.
- 마법사를 통해 대화형 설치를 실행할 시, 마법사 창에서 **가상 인프라를 위해 네트워크 에이전트 설정 최적화** 옵션을 선택합니다.

이러한 옵션을 선택하면 네트워크 에이전트의 설정이 변경되어 정책을 적용하기 전까지는 다음 기능이 기본적으로 비활성화된 상태로 유지됩니다.

- 설치된 소프트웨어에 대한 정보 가져오기
- 하드웨어에 대한 정보 가져오기
- 탐지된 취약점에 대한 정보 가져오기
- 요구되는 업데이트에 대한 정보 가져오기

이러한 기능은 통합 소프트웨어 및 가상 하드웨어를 사용하므로 대개 가상 컴퓨터에서 필요하지 않습니다.

기능 중지는 취소가 가능합니다. 중지한 기능이 필요한 경우 네트워크 에이전트의 정책이나 네트워크 에이전트 로컬 설정을 통해 기능을 작동시킬 수 있습니다. 네트워크 에이전트의 로컬 설정은 관리 콘솔에서 관련 기기의 마우스 오른쪽 메뉴를 통해 제공됩니다.

동적 가상 컴퓨터 지원

Kaspersky Security Center는 동적 가상 컴퓨터를 지원합니다. 조직 네트워크에 가상 인프라가 배포되었다면 특정한 경우에 동적(임시) 가상 컴퓨터를 사용할 수 있습니다. 동적 VM은 관리자가 준비한 템플릿에 따라 고유한 이름으로 작성됩니다. 사용자가 필요한 시간 동안 VM에서 작업을 한 후 VM을 끄면 가상 인프라에서 해당 가상 컴퓨터가 제거됩니다. 조직 네트워크에 Kaspersky Security Center를 배포한 경우에는 네트워크 에이전트가 설치된 가상 컴퓨터가 중앙 관리 서버 데이터베이스에 추가됩니다. 가상 컴퓨터를 끈 후에는 중앙 관리 서버의 데이터베이스에서도 해당 항목을 제거해야 합니다.

가상 컴퓨터에서 항목 자동 제거 기능이 작동하도록 하려면 동적 가상 컴퓨터용 템플릿에 네트워크 에이전트를 설치할 때 **VDI에 대해 동적 모드 사용** 옵션을 선택합니다:

- 원격 설치 시: 네트워크 에이전트 설치 패키지의 속성 창(**고급** 섹션)
- 대화형 설치 시 - 네트워크 에이전트 설치 마법사

실제 기기에 네트워크 에이전트를 설치할 때는 **VDI에 대해 동적 모드 사용** 옵션을 선택하지 마십시오.

동적 가상 컴퓨터를 제거한 후 일정 시간 동안 중앙 관리 서버에 해당 가상 컴퓨터의 이벤트를 저장하려는 경우 중앙 관리 서버 속성 창의 **이벤트 저장소** 섹션에서 **기기가 삭제된 후 이벤트 저장** 옵션을 선택하고 이벤트의 최대 저장 기간을 일 단위로 지정합니다.

동적 가상 컴퓨터에서는 드라이브 암호화를 활성화하지 않는 것이 좋습니다.

가상 컴퓨터 복사 지원

네트워크 에이전트가 설치된 가상 컴퓨터를 복사하거나 네트워크 에이전트가 설치된 템플릿에서 가상 컴퓨터를 만드는 작업은 하드 드라이브 이미지를 캡처 및 복사하여 네트워크 에이전트를 배포하는 작업과 동일합니다. 대부분의 경우 가상 컴퓨터를 복사할 때 디스크 이미지 복사를 통해 네트워크 에이전트를 배포하는 경우와 동일한 단계를 수행해야 합니다.

그러나 아래의 두 가지 경우에서는 복사를 자동으로 탐지하는 네트워크 에이전트에 대해 설명합니다. 위에서 설명한 이유로 인해 "기기의 하드 드라이브 캡처 및 복사를 통한 배포"에서 설명하는 복잡한 작업은 수행하지 않아도 됩니다:

- 네트워크 에이전트를 설치할 때 **VDI에 대해 동적 모드 사용** 옵션을 선택함: 운영 체제를 다시 시작할 때마다 이 가상 컴퓨터가 복사되었는지 여부에 관계없이 새 기기로 인식됩니다.
- 다음 하이퍼바이저 중 하나를 사용 중임: VMware™, HyperV® 또는 Xen®: 네트워크 에이전트가 가상 하드웨어의 변경된 ID를 기준으로 가상 컴퓨터 복사를 탐지합니다.

가상 하드웨어의 변경 사항 분석 정보 신뢰도가 아주 높은 것은 아닙니다. 이 방법을 광범위하게 적용하기 전에 소규모 가상 컴퓨터 풀에서 현재 조직에서 사용되는 하이퍼바이저 버전에 대해 이 방법을 테스트해야 합니다.

네트워크 에이전트가 설치된 기기의 파일 시스템 롤백 지원

Kaspersky Security Center는 배포 방식 애플리케이션입니다. 네트워크 에이전트가 설치된 기기에서 파일 시스템을 이전 상태로 롤백하면 데이터 동기화가 해제되며 Kaspersky Security Center가 잘못된 방식으로 작동하게 됩니다.

다음과 같은 경우 파일 시스템 또는 파일 시스템의 일부분을 롤백할 수 있습니다:

- 하드 드라이브의 이미지를 복사할 때.
- 가상 인프라를 통해 가상 컴퓨터 상태를 복원할 때.
- 백업 복사본 또는 복구 지점에서 데이터를 복원할 때.

네트워크 에이전트가 설치된 기기의 타사 소프트웨어가 the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 폴더에 영향을 주는 시나리오는 Kaspersky Security Center의 심각한 시나리오뿐입니다. 그러므로 가능하면 항상 복구 절차에서 이 폴더를 제외해야 합니다.

일부 조직의 업무 규칙에서는 기기의 파일 시스템을 롤백하는 기능을 제공하기 때문에 Kaspersky Security Center 10 Maintenance Release 1부터는 네트워크 에이전트가 설치된 기기의 파일 시스템 롤백 지원이 추가되었습니다. 이 경우 중앙 관리 서버와 네트워크 에이전트가 버전 10 Maintenance Release 1 이상이어야 합니다. 이러한 기기는 탐지되는 경우 중앙 관리 서버에 자동으로 다시 연결되며 전체 데이터 정리 및 전체 동기화가 수행됩니다.

기본적으로 Kaspersky Security Center 15.1에서는 파일 시스템 롤백 탐지 지원이 활성화되어 있습니다.

네트워크 에이전트가 설치된 기기의 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 폴더는 가급적 롤백하지 않아야 합니다. 데이터의 전체 다시 동기화를 수행하려면 리소스가 많이 필요하기 때문입니다.

중앙 관리 서버가 설치된 기기에서는 시스템 상태를 절대 롤백해서는 안 됩니다. 중앙 관리 서버에서 사용하는 데이터베이스도 롤백하면 안 됩니다.

표준 klbackup 유틸리티를 통해서만 백업 복사본에서 중앙 관리 서버 상태를 복원할 수 있습니다.

애플리케이션 로컬 설치

이 섹션에서는 로컬 기기에만 설치 가능한 애플리케이션의 설치 절차를 설명합니다.

선택한 클라이언트 기기에 애플리케이션을 로컬 설치하려면 해당 기기에 대한 관리자 권한이 있어야 합니다.

선택한 클라이언트 기기에 애플리케이션을 로컬로 설치하려면 다음과 같이 하십시오:

1. 클라이언트 기기에 네트워크 에이전트를 설치하고 클라이언트 기기와 중앙 관리 서버 간의 연결을 설정합니다.
2. 이러한 애플리케이션의 설명서에 설명된 대로 기기에 필요한 애플리케이션을 설치합니다.
3. 관리자의 워크스테이션에 설치된 각 애플리케이션에 대한 관리 플러그인을 설치합니다.

Kaspersky Security Center는 독립 실행형 설치 패키지를 사용한 애플리케이션 로컬 설치 옵션도 지원합니다. Kaspersky Security Center는 모든 Kaspersky 애플리케이션 설치를 지원하지 않습니다.

네트워크 에이전트 로컬 설치

기기에 네트워크 에이전트를 로컬로 설치하려면 다음과 같이 하십시오:

1. 기기에서 인터넷에서 다운로드한 배포 패키지의 setup.exe 파일을 실행합니다. 자세한 내용은 다음 항목을 참조하십시오: Kaspersky Security Center 배포 키트에서 네트워크 에이전트 설치 패키지 가져오기.

   설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다.

2. 애플리케이션 선택 창에서 **Kaspersky Security Center 네트워크 에이전트만 설치** 링크를 클릭하여 네트워크 에이전트 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

   a. **중앙 관리 서버**

   포트

   네트워크 에이전트로부터 연결을 수신하기 위해 중앙 관리 서버에서 사용하는 비SSL 포트를 지정합니다.

   기본적으로 이 옵션은 14000으로 설정됩니다.

   SSL 포트

   네트워크 에이전트로부터 연결을 수신하기 위해 중앙 관리 서버에서 사용하는 SSL 포트를 지정합니다.

기본적으로 이 옵션은 13000으로 설정됩니다.

SSL을 사용해 중앙 관리 서버에 접속

이 확인란을 선택하면 SSL을 사용하여 보안 포트를 통해 중앙 관리 서버에 연결됩니다.

기본적으로 이 옵션은 켜져 있습니다.

네트워크 에이전트가 UDP 포트를 열도록 허용

이 옵션이 활성화되면 설치 프로그램은 클라이언트 기기를 관리하고 관련 정보를 수신하기 위해 중앙 관리 서버에서 사용하는 포트를 자동으로 엽니다.

기본적으로 이 옵션은 켜져 있습니다.

UDP 포트

중앙 관리 서버에서 클라이언트 기기를 관리하고 관련 정보를 수신하는 데 사용하는 포트를 구성할 수 있습니다.

기본적으로 이 옵션은 15000으로 설정됩니다.

b. **프록시 서버 구성**

프록시 서버 사용

이 옵션을 사용하면 프록시 서버 인증을 위한 자격 증명을 지정할 수 있습니다.

프록시 서버 인증에만 필요한 최소 권한이 있는 계정의 자격 증명을 지정하는 것이 좋습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

주소

포트

계정

프록시 서버에 대한 연결을 구성할 계정의 사용자 이름입니다.

프록시 서버 인증에만 필요한 최소 권한이 있는 계정의 자격 증명을 지정하는 것이 좋습니다.

암호

프록시 서버에 대한 연결을 구성할 계정의 암호입니다.

프록시 서버 인증에만 필요한 최소 권한이 있는 계정의 자격 증명을 지정하는 것이 좋습니다.

c. **연결 게이트웨이**

연결 게이트웨이 사용 안 함

연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용

이 옵션을 선택하여 중앙 관리 서버에 연결할 때 DMZ에서 네트워크 에이전트를 연결 게이트웨이로 사용하고, 이를 이용해 통신하고, 데이터 전송 중 네트워크 에이전트의 데이터를 안전하게 유지할 수 있습니다.

연결 게이트웨이를 통해 중앙 관리 서버에 연결

이 옵션을 선택한 다음 연결 게이트웨이 역할을 할 기기를 지정합니다.

d. **중앙 관리 서버 인증서**

e. **에이전트 태그**

f. **고급 설정**

승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치

이 옵션을 활성화된 상태로 유지하는 것이 좋습니다. 이 옵션을 선택 해제하면 Kaspersky Security Center 구성 요소에 대한 자동 업데이트 및 패치가 비활성화됩니다. 관리자는 정책을 사용하여 나중에 자동 업데이트 및 패치를 다시 활성할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

네트워크 에이전트 서비스 보호 사용

이 옵션이 활성화되면, 관리 중인 기기에 네트워크 에이전트를 설치한 후에 구성 요소를 제거하거나 재구성하려면 필요한 권한이 있어야 합니다. 네트워크 에이전트 서비스는 중지할 수 없습니다. 이 옵션은 도메인 컨트롤러에 영향을 주지 않습니다.

로컬 관리자 권한으로 작동하는 워크스테이션에서 네트워크 에이전트를 보호하려면 이 옵션을 활성화합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

VDI에 대해 동적 모드 사용

이 확인란을 선택하면 가상 컴퓨터에 설치된 네트워크 에이전트에 대해 VDI(가상 데스크톱 인프라) 동적 모드가 활성됩니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

VDI에 대한 Kaspersky Security Center 네트워크 에이전트 설정을 최적화합니다. 애플리케이션 및 하드웨어의 취약성 검색 및 인벤토리를 비활성화합니다. 네트워크 에이전트 정책을 통해 현재 설정을 편집할 수 있습니다.

이 확인란을 선택하면, 다음 기능이 네트워크 에이전트 설정에서 중지됩니다.

- 설치된 소프트웨어에 대한 정보 가져오기
- 하드웨어에 대한 정보 가져오기
- 탐지된 취약점에 대한 정보 가져오기
- 요구되는 업데이트에 대한 정보 가져오기

기본적으로 이 옵션은 비활성화되어 있습니다.

g. **애플리케이션 시작**

설치 마법사가 완료되면 네트워크 에이전트가 해당 기기에 설치됩니다.

Kaspersky Security Center 네트워크 에이전트 서비스의 속성을 보고 표준 Microsoft Windows 도구: 컴퓨터 관리\서비스를 사용하여 네트워크 에이전트 활동을 시작, 중지 및 감시할 수도 있습니다.

숨김 모드로 네트워크 에이전트 설치

네트워크 에이전트는 사용자가 설치 파라미터를 직접 입력할 필요 없는 숨김 모드로 설치할 수 있습니다. 숨김 모드 설치 시에는 네트워크 에이전트용 Windows Installer 패키지(MSI)를 사용합니다. MSI 파일은 Kaspersky Security Center 배포 패키지의 Packages\NetAgent\exec 폴더에 있습니다.

설치 패키지 Kaspersky Network Agent.msi의 이름을 바꾸지 마십시오. 이 패키지 이름을 바꾸면 네트워크 에이전트의 향후 업데이트 시 설치 오류가 발생할 수 있습니다.

MSI 패키지에서 네트워크 에이전트 설치는 숨김 모드에서만 가능하며 MSI 패키지를 통한 대화식 설치는 지원하지 않습니다.

로컬 기기에 숨김 모드로 네트워크 에이전트를 설치하려면:

1. 최종 사용자 라이센스 계약서를 읽어 보십시오. 최종 사용자 라이센스 계약서의 조건을 이해하고, 이에 동의하는 경우에만 아래 명령을 사용하십시오.

2. 다음 명령 실행

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   여기서 설치_파라미터는 공백으로 구분된 파라미터 및 해당 값 목록입니다(`PROP1=PROP1VAL PROP2=PROP2VAL`).

   파라미터 목록에 `EULA=1`을 포함해야 합니다. 그렇지 않으면 네트워크 에이전트가 설치되지 않습니다.

Kaspersky Security Center 및 원격 기기의 네트워크 에이전트에 대한 표준 연결 설정을 사용한다면 다음 명령을 실행합니다.

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx`는 로그 작성을 위한 키입니다. 로그는 네트워크 에이전트 설치 중에 생성되며 C:\windows\temp\nag_inst.log에 저장됩니다.

nag_inst.log 외에도 애플리케이션은 설치 로그를 포함하는 $klssinstlib.log 파일을 생성합니다. 이 파일은 %windir%\temp 또는 %temp% 폴더에 저장됩니다. 문제 해결을 위해 사용자 또는 Kaspersky 기술 지원 전문가에게 두 개의 로그 파일(nag_instlib.log 및 $klssinstlib.log)이 모두 필요할 수 있습니다.

중앙 관리 서버에 연결할 포트를 추가로 지정해야 하는 경우 다음 명령을 실행하십시오:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

`SERVERPORT` 파라미터는 중앙 관리 서버 연결용 포트의 번호에 해당합니다.

숨김 모드로 네트워크 에이전트를 설치할 때 사용할 수 있는 파라미터의 이름과 이용 가능한 값은 네트워크 에이전트 설치 파라미터 섹션에 나와 있습니다.

Windows 설치 프로그램을 사용하여 네트워크 에이전트를 업그레이드하려면 다음 명령을 실행하십시오.

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

숨김 모드에서 Linux용 네트워크 에이전트 설치(응답 파일 사용)

변수와 개별 값으로 이루어진 일련의 맞춤 설치 파라미터가 포함된 텍스트 파일인 응답 파일을 사용하여 Linux 기기에 네트워크 에이전트를 설치할 수 있습니다. 이 응답 파일을 사용하면 숨김 모드에서 설치를 실행할 수 있으므로 사용자가 개입할 필요가 없습니다.

숨김 모드에서 Linux에 네트워크 에이전트를 설치하려면

1. 해당하는 Linux 기기에 원격으로 설치할 준비를 합니다. 적절한 패키지 관리 시스템에서 네트워크 에이전트의 .deb 또는 .rpm 패키지를 사용하여 원격 설치 패키지를 다운로드하고 생성합니다.

2. SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면 insserv-compat 패키지를 먼저 설치 해서 네트워크 에이전트를 구성합니다.

   운영 체제 RED OS 7.3.4 이상이나 MSVSPHERE 9.2 이상을 사용하는 기기에 네트워크 에이전트를 설치한다면, 중앙 관리 서버가 올바르게 작동하려면 libxcrypt-compat 패키지를 설치해야 합니다.

3. 최종 사용자 라이센스 계약서를 읽어 보십시오. 최종 사용자 라이센스 계약서의 조건을 이해하고, 이에 동의하는 경우에만 아래 단계를 따르십시오.

4. 응답 파일(TXT 형식)을 생성합니다. 응답 파일에 변수 목록을 VARIABLE_NAME=variable_value 형식으로 한 줄에 변수 하나씩 추가합니다.

   응답 파일을 올바르게 사용하려면 다음과 같은 세 개의 필수 변수로 이루어진 최소 세트가 반드시 포함되어야 합니다.

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   더 구체적인 원격 설치 파라미터를 사용하려면 선택적 변수를 추가해도 됩니다. 다음 표에는 응답 파일에 포함될 수 있는 모든 변수가 나열되어 있습니다.

숨김 모드로 Linux에 네트워크 에이전트를 설치하는 데 파라미터로 사용되는 응답 파일의 변수

숨김 모드로 Linux에 네트워크 에이전트를 설치하는 데 파라미터로 사용되는 응답 파일의 변수

변수 이름	필요한 용량	설명	가능한 값
KLNAGENT_SERVER	예	FQDN(전체 주소 도메인 이름) 또는 IP 주소로 표시되는 중앙 관리 서버 이름을 포함합니다.	DNS 이름 또는 IP 주소입니다.

KLNAGENT_AUTOINSTALL	예	숨김 설치 모드를 활성화할지 정의합니다.	1 - 숨김 모드가 활성화됩니다. 설치 중 어떠한 작업에 대한 메시지도 사용자에게 표시되지 않습니다. 기타 - 숨김 모드가 비활성화됩니다. 설치 중 작업에 대한 메시지가 사용자에게 표시될 수 있습니다.
EULA_ACCEPTED	예	사용자가 네트워크 에이전트의 최종 사용자 라이센스 계약서(EULA)를 수락하는지 여부를 정의합니다. 누락될 경우 EULA를 수락하지 않는 것으로 해석될 수 있습니다.	1 – 이 최종 사용자 라이센스 계약서의 이용 약관을 모두 읽고 이해했으며 수락하는 것에 동의합니다. 다른 값 또는 지정되지 않음 – 라이센스 계약서 조건에 동의하지 않음(설치가 수행되지 않음).
KLNAGENT_PROXY_USE	아니요	중앙 관리 서버와의 연결에 프록시 설정을 사용할지 여부를 정의합니다. 기본값은 0입니다.	1 - 프록시 설정을 사용합니다. 기타 - 프록시 설정을 사용하지 않습니다.
KLNAGENT_PROXY_ADDR	아니요	중앙 관리 서버와의 연결에 사용할 프록시 서버의 주소를 정의합니다.	DNS 이름 또는 IP 주소입니다.
KLNAGENT_PROXY_LOGIN	아니요	프록시 서버에 로그인하는 데 사용할 사용자 이름을 정의합니다.	기존 사용자 이름이면 됩니다.
KLNAGENT_PROXY_PASSWORD	아니요	프록시 서버에 로그인하는 데 사용할 사용자 암호를 정의합니다.	운영 체제에서 암호 형식으로 허용되는 모든 영숫자 세트입니다.
KLNAGENT_VM_VDI	아니요	공적 가상 머신의 생성을 위해 이미지에 네트워크 에이전트를 설치할지 여부를 정의합니다.	1 - 네트워크 에이전트를 이미지에 설치하고, 이후에 이를 동적 가상 머신 생성에 사용합니다. 기타 - 설치 중 이미지를 사용하지 않습니다.
KLNAGENT_VM_OPTIMIZE	아니요	네트워크 에이전트 설정이 하이퍼바이저에 대해 최적인지 여부를 정의합니다.	1 - 하이퍼바이저에서 최적의 상태로 사용할 수 있도록 네트워크 에이전트의 기본 로컬 설정이 수정되었습니다.
KLNAGENT_TAGS	아니요	네트워크 에이전트 인스턴스에 할당된 태그를 나열합니다.	하나 이상의 태그 이름이 세미콜론으로 구분됩니다.
KLNAGENT_UDP_PORT	아니요	네트워크 에이전트에 사용되는 UDP 포트를 정의합니다. 기본값은 15000입니다.	기존 포트 번호면 됩니다.
KLNAGENT_PORT	아니요	네트워크 에이전트에 사용되는 비 TLS 포트를 정의합니다. 기본값은 14000입니다.	기존 포트 번호면 됩니다.
KLNAGENT_SSLPORT	아니요	네트워크 에이전트에 사용되는 TLS 포트를 정의합니다. 기본값은 13000입니다.	기존 포트 번호면 됩니다.
KLNAGENT_USESSL	아니요	연결에 전송 계층 보안(TLS)을 사용할지 여부를 정의합니다.	1(기본값) - TLS를 사용합니다. 기타 - TLS를 사용하지 않습니다.

KLNAGENT_GW_MODE	아니요	연결 게이트웨이 사용 여부를 정의합니다.	1(기본값) - 현재 설정을 수정하지 않습니다(최초 호출 시 연결 게이트웨이가 지정되지 않음). 2 - 연결 게이트웨이를 사용하지 않습니다. 3 - 연결 게이트웨이를 사용합니다. KLNAGENT_GW_ADDRESS가 필요합니다. 4 - 네트워크 에이전트 인스턴스를 DMZ(완충 지역)에서 연결 게이트웨이로 사용합니다. 서버 인증서가 필요합니다.
KLNAGENT_GW_ADDRESS	아니요	연결 게이트웨이의 주소를 정의합니다. 이 값은 KLNAGENT_GW_MODE=3인 경우에만 적용할 수 있습니다.	DNS 이름 또는 IP 주소입니다.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	아니요	네트워크 에이전트 설치 후 기기 소유자 유틸리티로 사용자 등록을 실행할 수 있습니다. 이 옵션이 꺼져 있으면 사용자는 기기 소유자 등록을 사용할 수 없습니다.	1—네트워크 에이전트 설치 후 기기 소유자 유틸리티로 사용자 등록이 실행됩니다. 기타—꺼져 있습니다.

5. 네트워크 에이전트 설치를 실행합니다. 응답 파일의 경로를 지정하는 KLAUTOANSWERS 환경 변수가 설치 명령에 전달됩니다. 다음 명령 중 하나를 실행합니다.

   - RPM 패키지에서 32비트 운영 체제로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
     `sudo KLAUTOANSWERS=<응답 파일 경로> yum install ./klnagent-<빌드 번호>.i386.rpm`
   - RPM 패키지에서 64비트 운영 체제로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
     `sudo KLAUTOANSWERS=<응답 파일 경로> yum install ./klnagent64-<빌드 번호>.x86_64.rpm`
   - RPM 패키지에서 Arm 아키텍처용 64비트 운영 체제로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
     `sudo KLAUTOANSWERS=<응답 파일 경로> yum install ./klnagent64-<빌드 번호>.aarch64.rpm`
   - DEB 패키지에서 32비트 운영 체제로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
     `sudo KLAUTOANSWERS=<응답 파일 경로> apt install ./klnagent_<빌드 번호>_i386.deb`
   - DEB 패키지에서 64비트 운영 체제로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
     `sudo KLAUTOANSWERS=<응답 파일 경로> apt install ./klnagent64_<빌드 번호>_amd64.deb`
   - DEB 패키지에서 Arm 아키텍처용 64비트 운영 체제로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
     `sudo KLAUTOANSWERS=<응답 파일 경로> apt install ./klnagent64_<빌드 번호>_arm64.deb`

   운영 체제 구성에 따라 rpm, dpkg 또는 dnf 패키지 관리자를 사용하여 네트워크 에이전트를 설치할 수도 있습니다.

Linux용 네트워크 에이전트 설치가 숨김 모드에서 시작됩니다. 설치 중 작업에 관한 메시지가 사용자에게 표시되지 않습니다.

네트워크 에이전트 설치를 위해 폐쇄형 소프트웨어 환경 모드에서 Astra Linux를 실행하는 기기 준비

폐쇄형 소프트웨어 환경 모드에서 Astra Linux를 실행하는 기기에 네트워크 에이전트를 설치하기 전에, 아래 지침에 있는 절차와 모든 Linux 기기에 대한 일반 준비 단계를 수행해야 합니다.

루트 권한이 있는 계정으로 이 지침에 제공된 명령을 실행합니다.

네트워크 에이전트 설치를 위해 폐쇄형 소프트웨어 환경 모드에서 Astra Linux를 실행하는 기기를 준비하려면:

1. `/etc/digsig/digsig_initramfs.conf` 파일을 열고 다음 설정을 지정합니다.

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 명령줄에서 다음 명령을 실행하여 호환성 패키지를 설치합니다.

   ```
   apt install astra-digsig-oldkeys
   ```

3. 애플리케이션 키용 디렉터리를 만듭니다.

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg 애플리케이션 키를 이전 단계에서 만든 디렉터리에 넣습니다.

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Kaspersky Security Center 배포 키트에 kaspersky_astra_pub_key.gpg 애플리케이션 키가 포함되어 있지 않다면 https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg 링크를 클릭하여 다운로드할 수 있습니다.

5. RAM 디스크를 업데이트합니다.

   ```
   update-initramfs -u -k all
   ```

   시스템을 재부팅합니다.

이제 Linux 기기에 네트워크 에이전트를 설치할 수 있습니다. 네트워크 에이전트를 원격, 대화식 모드 또는 숨김 모드로 설치할 수 있습니다.

대화식 모드로 Linux용 네트워크 에이전트 설치

이 문서에서는 설치 파라미터를 지정하여 대화식 모드로 Linux 기기에 네트워크 에이전트를 설치하는 방법을 단계별로 설명합니다. 또한 변수와 개별 값으로 이루어진 일련의 맞춤 설치 파라미터가 포함된 텍스트 파일인 응답 파일을 사용할 수 있습니다. 이 응답 파일을 사용하면 숨김 모드에서 설치를 실행할 수 있으므로 사용자가 개입할 필요가 없습니다.

운영 체제 RED OS 7.3.4 이상이나 MSVSPHERE 9.2 이상을 사용하는 기기에 네트워크 에이전트를 설치한다면, 중앙 관리 서버가 올바르게 작동하려면 libxcrypt-compat 패키지를 설치해야 합니다.

비대화식 모드로 네트워크 에이전트 설치:

1. 네트워크 에이전트 설치를 실행합니다. Linux 배포판에 따라 다음 명령 중 하나를 실행합니다.

   - RPM 패키지에서 32비트 운영 체제로 네트워크 에이전트를 설치하려면:

     `# yum -i klnagent-<빌드 번호>.i386.rpm`

   - RPM 패키지에서 64비트 운영 체제로 네트워크 에이전트를 설치:

     `# yum -i klnagent64-<빌드 번호>.x86_64.rpm`

   - Arm 아키텍처용 64비트 운영 체제의 RPM 패키지에서 네트워크 에이전트를 설치:

     `# yum -i klnagent64-<빌드 번호>.aarch64.rpm`

   - DEB 패키지에서 32비트 운영 체제에 네트워크 에이전트를 설치:

     `# apt install ./klnagent_<빌드 번호>_i386.deb`

   - DEB 패키지에서 64비트 운영 체제에 네트워크 에이전트를 설치:

     `# apt install ./klnagent64_<빌드 번호>_amd64.deb`

   - Arm 아키텍처용 64비트 운영 체제의 DEB 패키지에서 네트워크 에이전트를 설치:

     `# apt install ./klnagent64_<빌드 번호>_arm64.deb`

2. 네트워크 에이전트 구성을 실행합니다.

   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

3. 최종 사용자 라이센스 계약서(EULA)를 읽어 보십시오. 텍스트가 명령줄 창에 표시됩니다. 다음 텍스트 세그먼트를 보려면 스페이스 바를 누르십시오. 그런 다음 메시지가 표시되면 다음 값을 입력합니다.

   - EULA의 약관을 읽고 이에 동의하는 경우 `y`를 입력합니다.
   - EULA의 약관에 동의하지 않는 경우 `n`을 입력하십시오. 네트워크 에이전트를 사용하려면 EULA 약관에 동의해야 합니다.
   - `r`을 입력하여 EULA를 다시 표시합니다.

4. 중앙 관리 서버 DNS 이름 또는 IP 주소를 입력합니다.

5. 중앙 관리 서버 포트 번호를 입력합니다. 기본적으로 포트 14000이 사용됩니다.

6. 중앙 관리 서버 SSL 포트 번호를 입력합니다. 기본적으로 포트 13000이 사용됩니다.

7. 네트워크 에이전트와 중앙 관리 서버 간의 트래픽에 SSL 암호화를 사용하려면 `y`를 입력합니다. 그렇지 않으면 `n`을 입력합니다.

8. 다음 옵션 중 하나를 선택하여 네트워크 에이전트를 구성합니다.

   - `[1]` - 연결 게이트웨이를 구성하지 않습니다.

     사용자의 기기는 연결 게이트웨이로 작동하지 않으며 연결 게이트웨이를 통해 중앙 관리 서버에 연결하지 않습니다.

   - `[2]` - 연결 게이트웨이 사용 안 함.

     기기는 연결 게이트웨이를 통해 중앙 관리 서버에 연결하지 않습니다.

- [3] - 연결 게이트웨이로 중앙 관리 서버에 연결.
  기기는 연결 게이트웨이를 통해 중앙 관리 서버에 연결합니다.
- [4] - 연결 게이트웨이로 사용.
  기기가 연결 게이트웨이 역할을 합니다.

네트워크 에이전트는 Linux 기기에 설치됩니다.

애플리케이션 관리 플러그인의 로컬 설치

애플리케이션 관리 플러그인을 설치하려면 다음과 같이 하십시오:

관리 콘솔이 설치된 기기에서 애플리케이션 배포 패키지에 들어 있는 klcfginst.exe 실행 파일을 실행합니다.

Klcfginst.exe 파일은 Kaspersky Security Center를 통해 관리하는 모든 애플리케이션에 포함되어 있습니다. 설치는 마법사를 통해 이루어지므로 직접 설정을 구성할 필요가 없습니다.

숨김 모드에서 애플리케이션 설치

숨김 모드에서 애플리케이션을 설치하려면:

1. Kaspersky Security Center의 메인 창을 엽니다.
2. 콘솔 트리의 **원격 설치** 폴더에 있는 **설치 패키지** 하위 폴더에서 관련 애플리케이션의 설치 패키지를 선택하거나 이 애플리케이션에 대한 새 설치 패키지를 만듭니다.

   설치 패키지는 중앙 관리 서버의 공유 폴더 내 패키지 서비스 폴더에 저장됩니다. 별도 하위 폴더는 각 설치 패키지를 의미합니다.

3. 다음 방법 중 하나로 필수 설치 패키지가 저장된 폴더를 엽니다:
   - 중앙 관리 서버에서 관련 설치 패키지에 해당하는 폴더를 클라이언트 기기로 복사합니다. 그러면 클라이언트 기기에서 복사된 폴더가 열립니다.
   - 클라이언트 기기에서 필수 설치 패키지에 해당하는 중앙 관리 서버의 공유 폴더를 엽니다.

   Microsoft Windows Vista가 설치된 기기에 공유 폴더가 있는 경우 **사용자 계정 컨트롤: 관리 승인 모드에서 모든 관리자 실행** 설정에 **사용 안 함** 값을 설정해야 합니다(**시작 → 제어판 → 관리 → 로컬 보안 정책 → 보안 설정**).

4. 선택한 애플리케이션에 따라 다음 작업을 수행합니다:
   - Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers 및 Kaspersky Security Center의 경우, exec 하위 폴더를 열고 /s 키를 사용하여 실행 파일을 실행합니다(확장자가 .exe인 파일).
   - 기타 Kaspersky 애플리케이션의 경우에는 열린 폴더에서 /s 키를 사용하여 실행 파일을 실행합니다(확장자가 .exe인 파일).

EULA=1 및 PRIVACYPOLICY=1 키로 실행 파일을 실행하면 최종 사용자 라이센스 계약서 및 개인정보취급방침의 조건을 모두 읽고 이해했으며, 이에 동의한다는 의미입니다. 또한, 데이터가 개인정보취급방침의 설명대로 취급 및 전송(제삼국으로의 전송도 포함)될 수 있다는 점도 인지한 것으로 간주됩니다. 라이센스 계약서 및 개인정보취급방침 문구는 Kaspersky Security Center 배포 키트에 포함되어 있습니다. 애플리케이션을 설치하거나 이전 버전의 애플리케이션을 업데이트하려면 반드시 라이센스 계약서 및 개인정보취급방침 조건을 수락해야 합니다.

독립 실행형 패키지를 사용하여 애플리케이션 설치

Kaspersky Security Center에서는 애플리케이션의 독립 실행형 설치 패키지를 만들 수 있습니다. 독립 실행형 설치 패키지는 웹 서버에 저장하거나 이메일로 보내거나 다른 방법으로 클라이언트 기기에 전송할 수 있는 실행 파일입니다. 이렇게 수신된 파일을 클라이언트 기기에서 로컬로 실행하여 Kaspersky Security Center의 관여 없이 애플리케이션을 설치할 수 있습니다.

독립 실행형 Linux용 네트워크 에이전트에는 nmap 유틸리티의 선택적인 종속성이 있습니다. nmap 유틸리티가 없거나 버전 6.0 이하인 경우 DHCP 검색 브로드캐스트 기능이 지원되지 않습니다.

독립 실행형 설치 패키지를 사용하여 애플리케이션을 설치하려면 다음과 같이 하십시오:

1. 필요한 중앙 관리 서버에 연결합니다.
2. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
3. 작업 영역에서 필요한 애플리케이션의 설치 패키지를 선택합니다.
4. 다음 방법 중 하나로 독립 실행형 설치 패키지를 만드는 프로세스를 시작합니다:
   - 설치 패키지의 마우스 오른쪽 메뉴에서 **독립 실행형 설치 패키지 생성**를 선택합니다.
   - 설치 패키지의 작업 영역에 있는 **독립 실행형 설치 패키지 생성** 링크를 누릅니다.

   독립 실행형 설치 패키지 만들기 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
   마법사의 마지막 단계에서 독립 실행형 설치 패키지를 클라이언트 기기로 전송하는 방법을 하나 선택합니다.
5. 독립 실행형 설치 패키지를 클라이언트 기기로 전송합니다.
6. 클라이언트 기기에서 독립 실행형 설치 패키지를 실행합니다.

   애플리케이션이 독립 실행형 패키지에 지정된 설정으로 클라이언트 기기에 설치됩니다.

독립 실행형 설치 패키지를 만들면 자동으로 웹 서버에 게시됩니다. 만들어진 독립 실행형 설치 패키지의 목록에 독립 실행형 패키지를 다운로드할 수 있는 링크가 표시됩니다. 필요할 경우 선택한 독립 실행형 패키지의 게시를 취소하거나 다시 웹 서버에 게시할 수 있습니다. 독립 실행형 설치 패키지를 다운로드하는 데는 기본적으로 8060 포트가 사용됩니다.

네트워크 에이전트 설치 패키지 설정

네트워크 에이전트 설치 패키지를 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
   기본적으로 **원격 설치** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. 네트워크 에이전트 설치 패키지의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

네트워크 에이전트 설치 패키지 속성 창이 열립니다.

일반

일반 섹션에는 설치 패키지에 대한 일반 정보가 표시됩니다:

- 설치 패키지 이름
- 설치 패키지가 만들어진 애플리케이션의 이름 및 버전
- 설치 패키지 크기
- 설치 패키지를 만든 날짜
- 설치 패키지 폴더 경로

설정

이 섹션에는 설치 직후 네트워크 에이전트가 올바르게 작동하도록 하는 데 필요한 설정이 나와 있습니다. 이 섹션의 설정은 Windows를 실행 중인 기기에서만 사용 가능합니다.

대상 폴더 설정 그룹에서 네트워크 에이전트를 설치할 클라이언트 기기 폴더를 선택할 수 있습니다.

- **기본 폴더에 설치**

  이 옵션을 선택하면 네트워크 에이전트가 <드라이브>:\Program Files\Kaspersky Lab\NetworkAgent 폴더에 설치됩니다. 이 폴더가 없는 경우 자동으로 만들어집니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **지정한 폴더에 설치**

  이 옵션을 선택하면 네트워크 에이전트가 입력 필드에 지정된 필드에 설치됩니다.

다음 설정 그룹에서 네트워크 에이전트 원격 제거 작업을 위한 암호를 지정할 수 있습니다:

- **제거 암호 사용**

  이 확인란을 선택하면 **수정** 버튼을 눌러 제거 암호를 입력할 수 있습니다(Windows 운영 체제를 실행하는 기기의 네트워크 에이전트에만 사용 가능함).

기본적으로 이 옵션은 비활성화되어 있습니다.

- **상태**

  암호 상태입니다: **암호가 설정되었습니다** 또는 **암호가 설정되지 않았습니다**.

  기본적으로 이 암호는 설정되어 있지 않습니다.

- **무단 제거, 중지 또는 설정 변경을 하지 못하도록 네트워크 에이전트 서비스 보호**

  이 옵션이 활성화되면, 관리 중인 기기에 네트워크 에이전트를 설치한 후에 구성 요소를 제거하거나 재구성하려면 필요한 권한이 있어야 합니다. 네트워크 에이전트 서비스는 중지할 수 없습니다. 이 옵션은 도메인 컨트롤러에 영향을 주지 않습니다.

  로컬 관리자 권한으로 작동하는 워크스테이션에서 네트워크 에이전트를 보호하려면 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치**

  이 옵션을 사용하면 중앙 관리 서버, 네트워크 에이전트, 관리 콘솔, iOS MDM 서버용으로 다운로드한 모든 업데이트 및 패치가 자동 설치됩니다.

  이 확인란의 선택을 취소하면 다운로드한 모든 업데이트와 패치는 상태를 *승인됨*으로 변경해야 설치됩니다. *정의 안 됨* 상태의 업데이트와 패치는 설치되지 않습니다.

  기본적으로 이 옵션은 켜져 있습니다.

연결

이 섹션에서는 네트워크 에이전트와 중앙 관리 서버 간 연결을 구성할 수 있습니다. 연결을 설정하기 위해 SSL 또는 UDP 프로토콜을 사용할 수 있습니다. 연결을 구성하려면 다음 설정을 지정하십시오.

- **중앙 관리 서버**

  중앙 관리 서버가 설치된 기기의 주소.

- **포트**

  연결에 사용되는 포트 번호.

- **SSL 포트**

  SSL 프로토콜을 통한 연결에 사용되는 포트 번호입니다.

- **서버 인증서 사용**

  이 확인란을 선택하면 중앙 관리 서버에 대한 네트워크 에이전트 접근 권한 인증 시 **찾기** 버튼을 눌러 지정할 수 있는 인증서 파일이 사용됩니다.

이 확인란의 선택을 취소하면 **서버 주소** 필드에 지정된 주소에 네트워크 에이전트를 처음 연결할 때 중앙 관리 서버에서 인증서 파일이 수신됩니다.

중앙 관리 서버에 연결할 때 네트워크 에이전트가 중앙 관리 서버 인증서를 자동으로 수신하는 방식은 안전하지 않은 것으로 간주되므로 이 확인란의 선택을 취소하지 않는 것이 좋습니다.

기본적으로 이 확인란은 선택되어 있습니다.

- **SSL 사용**

  이 확인란을 선택하면 SSL을 사용하여 보안 포트를 통해 중앙 관리 서버에 연결됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 연결이 안전하게 유지되도록 이 옵션을 비활성화하지 않는 것이 좋습니다.

- **UDP 포트 사용**

  이 확인란을 선택하면 네트워크 에이전트가 UDP 포트를 통해 중앙 관리 서버에 연결됩니다. 이를 통해 클라이언트 기기를 관리하고 이에 대한 정보를 수신할 수 있습니다.

  UDP 포트는 네트워크 에이전트가 설치된 관리 중인 기기에서 열어야 합니다. 따라서 이 옵션을 비활성화하지 않는 것이 좋습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **UDP 포트 번호**

  이 필드에서 UDP 프로토콜을 통해 네트워크 에이전트에 중앙 관리 서버를 연결하기 위한 포트를 지정할 수 있습니다.

  기본 UDP 포트는 15000입니다.

- **Microsoft Windows 방화벽에 네트워크 에이전트 포트 열기**

  이 옵션을 사용하면 네트워크 에이전트에서 사용하는 포트가 Microsoft Windows 방화벽 제외 목록에 추가됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **프록시 서버 사용**

  이 옵션을 사용하면 프록시 서버 파라미터를 지정합니다:

  - **프록시 서버 주소**
  - **프록시 서버 포트**

  프록시 서버에 인증이 필요하면 **프록시 서버 인증** 옵션을 활성화하고 프록시 서버에 대한 연결이 설정되는 계정의 **사용자 이름**과 **암호**를 지정합니다. 프록시 서버 인증에만 필요한 최소 권한이 있는 계정의 자격 증명을 지정하는 것이 좋습니다.

호환성을 위해 네트워크 에이전트 설치 패키지 설정에서 프록시 연결 설정을 지정하지 않는 것이 좋습니다.

고급

고급 섹션에서는 연결 게이트웨이가 사용되는 방법을 구성할 수 있습니다. 이를 위해 다음 작업을 수행할 수 있습니다.

- 네트워크 에이전트를 DMZ(Demilitarized Zone)에서 연결 게이트웨이로 사용하여 중앙 관리 서버에 연결하고, 이를 이용해 통신하고, 데이터 전송 중 네트워크 에이전트의 데이터를 안전하게 유지할 수 있습니다.
- 중앙 관리 서버에 대한 연결 수를 줄이려면 연결 게이트웨이를 사용하여 중앙 관리 서버에 연결하십시오. 이 경우 **연결 게이트웨이 주소** 필드에 연결 게이트웨이 역할을 할 기기의 주소를 입력하십시오.
- 네트워크에 가상 머신이 포함된 경우 VDI(가상 데스크톱 인프라)에 대한 연결을 구성합니다. 이를 위해 다음을 수행하십시오.
  - **VDI에 대해 동적 모드 사용**

    이 확인란을 선택하면 가상 컴퓨터에 설치된 네트워크 에이전트에 대해 VDI(가상 데스크톱 인프라) 동적 모드가 활성됩니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **VDI 설정 최적화**

    이 확인란을 선택하면, 다음 기능이 네트워크 에이전트 설정에서 중지됩니다.
    - 설치된 소프트웨어에 대한 정보 가져오기
    - 하드웨어에 대한 정보 가져오기
    - 탐지된 취약점에 대한 정보 가져오기
    - 요구되는 업데이트에 대한 정보 가져오기

    기본적으로 이 옵션은 비활성화되어 있습니다.

- **네트워크 에이전트 설치 후 사용자 등록 유틸리티 실행 허용**

  이 옵션을 활성화하면 네트워크 에이전트 설치 후 기기 소유자 유틸리티로 사용자 등록이 실행됩니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

추가 구성 요소

이 섹션에서는 네트워크 에이전트와의 동시 설치를 위한 추가 구성 요소를 선택할 수 있습니다.

태그

태그 섹션에는 네트워크 에이전트 설치 후 클라이언트 기기에 추가할 수 있는 키워드(태그) 목록이 표시됩니다. 목록에서 태그를 추가 및 제거할 수 있으며 태그의 이름도 바꿀 수 있습니다.

태그 옆의 확인란을 선택하면 해당 태그가 네트워크 에이전트 설치 중에 관리 중인 기기에 자동으로 추가됩니다.

태그 옆의 확인란이 비어 있으면 해당 태그가 네트워크 에이전트 설치 중에 관리 중인 기기에 자동으로 추가되지 않습니다. 이 태그는 기기에 수동으로 추가할 수 있습니다.

목록에서 제거한 태그는 추가된 모든 기기에서 자동으로 제거됩니다.

리비전 내역

이 섹션에서 설치 패키지의 리비전 내역을 확인할 수 있습니다. 리비전을 비교/확인/파일에 저장하고 리비전 설명을 추가 및 편집할 수 있습니다.

아래 표에는 특정 운영 체제에 사용 가능한 네트워크 에이전트 설치 패키지 설정이 나와 있습니다.

네트워크 에이전트 설치 패키지 설정

속성 섹션	Windows	Mac	Linux
일반	✓	✓	✓
설정	✓	—	—
연결	✓	✓ (Microsoft Windows **방화벽에 네트워크 에이전트 포트 열기** 및 **프록시 서버 자동 탐지만 사용** 옵션 제외)	✓ (Microsoft Windows **방화벽에 네트워크 에이전트 포트 열기** 및 **프록시 서버 자동 탐지만 사용** 옵션 제외)
고급	✓	✓	✓
추가 구성 요소	✓	✓	✓
태그	✓	✓ (자동 태그 지정 규칙 제외)	✓ (자동 태그 지정 규칙 제외)
리비전 내역	✓	✓	✓

개인정보취급방침 보기

개인정보 취급방침은 https://www.kaspersky.com/products-and-services-privacy-policy 에서 온라인으로 확인할 수 있으며, 오프라인에서도 확인할 수 있습니다. 예를 들어 네트워크 에이전트를 설치하기 전에 개인정보취급방침을 확인할 수 있습니다.

오프라인으로 개인정보취급방침을 확인하는 방법:

1. Kaspersky Security Center 설치 프로그램을 시작합니다.
2. 설치 프로그램 창에서 **설치 패키지 추출** 링크로 이동합니다.
3. 열리는 목록에서 Kaspersky Security Center 네트워크 에이전트를 선택하고 **다음**을 클릭합니다.

   privacy_policy.txt 파일은 기기의 지정한 폴더에 있는 NetAgent 하위 폴더에 표시됩니다.

모바일 기기 관리 시스템 배포

이 섹션에는 iOS MDM 및 Kaspersky Endpoint Security 프로토콜을 통한 모바일 기기 관리 시스템 배포에 대한 설명이 나와 있습니다.

iOS MDM 프로토콜을 통해 관리 시스템 배포

Kaspersky Security Center에서는 iOS에서 실행되는 모바일 기기를 관리할 수 있습니다. iOS MDM 기기는 iOS MDM 서버에 연결되어 중앙 관리 서버를 통해 관리되는 iOS 모바일 기기입니다.

모바일 기기는 다음 단계를 통해 iOS MDM 서버에 연결됩니다.

1. 관리자가 iOS MDM 서버를 설치합니다.
2. 관리자는 Apple 푸시 알림 서비스(APNs) 인증서를 가져옵니다(APNs 인증서 받기, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   APNs 인증서는 중앙 관리 서버에서 APNs 서버에 연결하여 iOS MDM 기기에 푸시 알림을 전송할 수 있도록 합니다.
3. 관리자는 iOS MDM 서버에 APNs 인증서를 설치합니다.
4. iOS 모바일 기기 사용자의 경우 관리자는 iOS MDM 프로필을 생성합니다.

   iOS MDM 프로필에는 iOS 모바일 기기를 중앙 관리 서버에 연결하기 위한 설정 모음이 들어 있습니다.

iOS MDM 프로필이 설치되어 iOS MDM 모바일 기기가 중앙 관리 서버와 동기화되면 콘솔 트리의 **Mobile devices**의 하위 폴더인 **Mobile Device Management**에 기기가 표시됩니다.

iOS MDM 서버 설치

로컬 기기에 iOS MDM 서버를 설치하려면 다음과 같이 하십시오:

1. setup.exe 실행 파일을 실행합니다.

   설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다.

   애플리케이션 선택 창에서 **iOS MDM 서버 설치** 링크를 클릭하여 iOS MDM 서버 설치 마법사를 실행합니다.
2. 대상 폴더를 선택합니다.

   기본 폴더는 <디스크>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS입니다. 이 폴더가 없는 경우에는 설치를 진행하는 동안 자동으로 생성됩니다. **찾기** 버튼을 사용하여 대상 폴더를 변경할 수 있습니다.
3. 마법사의 **iOS MDM 서버에 연결하기 위한 설정을 지정해 주십시오** 창에 있는 **iOS MDM 서비스로 연결하는데 사용되는 외부 포트** 필드에서 모바일 기기를 iOS MDM 서비스에 연결하는 데 사용할 외부 포트를 지정합니다.

   모바일 기기는 APNs 서버와의 통신을 위해 외부 5223 포트를 사용합니다. 17.0.0.0/8 주소 범위와 연결이 가능하도록 5223 포트가 방화벽에서 열려 있는지 확인합니다.

   기본적으로 443 포트를 사용하여 iOS MDM 서버에 연결합니다. 다른 서비스 또는 애플리케이션에서 443 포트를 사용 중이라면 9443 포트 등을 사용하여 연결합니다.

   iOS MDM 서버는 APNs 서버로 알림을 보내기 위해 2197 외부 포트를 사용했습니다.

   APNs 서버는 부하 분산 모드로 실행됩니다. 모바일 기기에서 언제나 동일한 IP 주소에 연결하여 알림을 받지는 않습니다. 17.0.0.0/8 주소 범위는 Apple 용도로 사용하도록 예약되어 있으며 이 전체 범위를 방화벽 설정에서 허용되는 범위로 지정하는 것이 좋기 때문입니다.

4. 애플리케이션 구성 요소의 상호 작용을 위한 포트를 수동으로 구성하려는 경우 **로컬 포트 수동 설정** 옵션을 선택하고 다음 설정의 값을 지정합니다:

   - **네트워크 에이전트 연결 포트**. 네트워크 에이전트에 iOS MDM 서비스를 연결하기 위한 포트를 이 필드에 지정합니다. 기본 포트 번호는 9799입니다.

   - **iOS MDM 서비스에 연결하는 로컬 포트**. 네트워크 에이전트를 iOS MDM 서비스에 연결하기 위한 로컬 포트를 이 필드에 지정합니다. 기본 포트 번호는 9899입니다.

   기본 값을 사용하는 것이 좋습니다.

5. 마법사의 **모바일 기기 서버의 외부 주소** 창에 있는 **모바일 기기 서버에 대한 원격 연결용 웹 주소** 필드에서 iOS MDM 서버를 설치할 클라이언트 기기의 주소를 지정합니다.

   이 주소는 관리 중인 모바일 기기를 iOS MDM 서비스에 연결하는 데 사용됩니다. iOS MDM 기기 연결에 클라이언트 기기를 사용할 수 있어야 합니다.

   클라이언트 기기의 주소를 다음 형식으로 지정할 수 있습니다:

   - 기기 FQDN(예: mdm.example.com)

   - 기기 NetBIOS 이름

   URL 체계 또는 포트 번호를 주소 문자열에 추가하지 마십시오: 이 값은 자동으로 추가됩니다.

마법사가 완료되면 iOS MDM 서버가 로컬 기기에 설치됩니다. iOS MDM 서버가 콘솔 트리의 **모바일 기기 관리** 폴더에 표시됩니다.

숨김 모드로 iOS MDM 서버 설치

Kaspersky Security Center는 설치 설정을 대화식으로 입력하지 않고 숨김 모드에서 로컬 기기에 iOS MDM 서버를 설치하도록 허용합니다.

숨김 모드로 로컬 기기에 iOS MDM 서버를 설치하려면:

1. 최종 사용자 라이센스 계약서를 읽어 보십시오. 최종 사용자 라이센스 계약서의 조건을 이해하고, 이에 동의하는 경우에만 아래 명령을 사용하십시오.

2. 다음 명령을 실행합니다:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <setup_parameters>"
   ```

   여기서 설치_파라미터는 공백으로 구분된 설정 및 해당 값 목록입니다(`PROP1=PROP1VAL PROP2=PROP2VAL`). setup.exe 파일은 Kaspersky Security Center 배포 키트에 포함된 Server 폴더에 있습니다.

아래 표에는 숨김 모드로 iOS MDM 서버를 설치할 때 사용할 수 있는 파라미터의 이름과 가능한 값이 나와 있습니다. 파라미터는 편한 순서대로 지정될 수 있습니다.

파라미터 이름	파라미터 설명	사용 가능한 값
EULA	최종 사용자 라이센스 계약서 조건 동의. 이 파라미터는 필수입니다.	• 1 – 최종 사용자 라이센스 계약서의 조건을 모두 읽고 이해했으며, 이에 동의합니다. • 다른 값 및 값 없음 – 라이센스 계약서 조건에 동의하지 않음(설치가 수행되지 않음).
DONT_USE_ANSWER_FILE	iOS MDM 서버 설치 설정이 있는 XML 파일 사용 여부. XML 파일에는 설치 패키지에 포함되어 있거나 중앙 관리 서버에 저장되어 있습니다. 해당 파일로의 추가 경로를 지정할 필요는 없습니다. 이 파라미터는 필수입니다.	• 1 – 파라미터를 가진 XML 파일 사용 안 함. • 다른 값 또는 정의된 값 없음 – 파라미터를 가진 XML 파일 사용.
INSTALLDIR	iOS MDM 서버 설치 폴더. 이 파라미터는 선택 사항입니다.	문자열 값 예: `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	네트워크 에이전트에 iOS MDM 서비스를 연결하기 위한 로컬 포트. 기본 포트 번호는 9799입니다. 이 파라미터는 선택 사항입니다.	숫자 값.
LOCALSERVERPORT	iOS MDM 서비스에 네트워크 에이전트를 연결하기 위한 로컬 포트. 기본 포트 번호는 9899입니다. 이 파라미터는 선택 사항입니다.	숫자 값.
EXTERNALSERVERPORT	iOS MDM 서버에 기기를 연결하기 위한 포트. 기본 포트 번호는 443입니다. 이 파라미터는 선택 사항입니다.	숫자 값.
EXTERNAL_SERVER_URL	iOS MDM 서버가 설치될 클라이언트 기기의 외부 주소. 이 주소는 관리 중인 모바일 기기를 iOS MDM 서비스에 연결하는 데 사용됩니다. iOS MDM을 통한 연결에 클라이언트 기기를 사용할 수 있어야 합니다. 해당 주소는 URL 및 포트 번호는 포함하고 있지 않아야 하며, 해당 값은 추후 자동으로 추가됩니다. 이 파라미터는 선택 사항입니다.	• 기기 FQDN(예: mdm.example.com) • 기기 NetBIOS 이름 • 기기 IP 주소
WORKFOLDER	iOS MDM 서버 작업 폴더. 만일 작업 폴더가 지정되지 않았다면, 데이터는 기본 폴더에서 기록됩니다. 이 파라미터는 선택 사항입니다.	문자열 값 예: `WORKFOLDER=\"C:\work\"`
MTNCY	복수의 가상 서버에서 iOS MDM 서버 사용. 이 파라미터는 선택 사항입니다.	• 1 – 복수의 가상 중앙 관리 서버에서 iOS MDM 서버를 사용합니다. • 다른 값 또는 정의된 값 없음 – 복수의 가상 중앙 관리 서버에서 iOS MDM 서버를 사용하지 않습니다.

예:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

iOS MDM 서버 설치 파라미터는 "iOS MDM 서버 설치" 섹션에 자세히 나와 있습니다.

iOS MDM 서버 배포 시나리오

설치할 iOS MDM 서버의 복사본 수는 사용 가능한 하드웨어 또는 설치를 수행할 모바일 기기의 총 수를 기준으로 선택할 수 있습니다.

단일 Kaspersky Device Management for iOS 설치에 권장되는 모바일 기기의 최대 수는 5만 대입니다. 부하를 줄이려는 경우 iOS MDM 서버가 설치된 여러 서버 간에 전체 기기 풀을 분산시킬 수 있습니다.

사용자 인증서를 통해 iOS MDM 기기 인증을 수행합니다. 기기에 설치된 모든 프로필에는 기기 소유자의 인증서가 포함되어 있습니다. 그러므로 iOS MDM 서버에 사용 가능한 배포 구성은 다음의 두 가지입니다:

- 간소화된 구성
- Kerberos 제한 위임(KCD)을 사용하는 배포 구성

간소화된 배포 구성

간소화된 구성에 따라 iOS MDM 서버를 배포할 때는 모바일 기기가 iOS MDM 웹 서비스에 직접 연결합니다. 이 경우 중앙 관리 서버에서 발급한 사용자 인증서는 기기 인증용으로만 적용할 수 있습니다. 사용자 인증서를 공개키 인프라(PKI)와 통합할 수는 없습니다.

Kerberos 제한 위임(KCD)을 사용하는 배포 구성

KCD(Kerberos 제한 위임)와 함께 배포 체계를 사용하려면 다음 요구 사항을 충족해야 합니다.

- 중앙 관리 서버와 iOS MDM 서버는 조직의 내부 네트워크에 위치합니다.
- KCD를 지원하는 역방향 프록시가 사용 중입니다.

이 배포 구성에서는 다음과 같은 기능을 제공합니다:

- KCD를 지원하는 역방향 프록시와 통합
- 모바일 기기의 인증에 KCD 사용
- 사용자 인증서 적용을 위해 PKI와 통합하는 기능

이 배포 구성을 사용할 때는 다음 작업을 수행해야 합니다:

- 관리 콘솔의 iOS MDM 웹 서비스 설정에서 **Kerberos constrained delegation와의 호환성 보장** 확인란을 선택합니다.
- iOS MDM 웹 서비스용 인증서로는 역방향 프록시에 iOS MDM 웹 서비스를 게시할 때 정의한 사용자 지정된 인증서를 지정합니다.
- 도메인의 인증 기관(CA)에서 iOS 기기용 사용자 인증서를 발급해야 합니다. 도메인에 루트 CA가 여러 개 포함되어 있으면 역방향 프록시에 iOS MDM 웹 서비스를 게시할 때 지정한 CA에서 사용자 인증서를 발급해야 합니다.

  다음 방법 중 하나를 사용하여 사용자 인증서가 이 CA 발급 요구 사항을 준수함을 확인할 수 있습니다:

  - 새 iOS MDM 프로필 마법사와 인증서 설치 마법사에서 사용자 인증서를 지정합니다.
  - 중앙 관리 서버를 도메인 PKI와 통합하고 인증서 발급을 위한 규칙에서 해당하는 설정을 정의합니다:

    1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **인증서** 하위 폴더를 선택합니다.
    2. **인증서** 폴더의 작업 영역에서 **인증서 발급 규칙 구성** 버튼을 눌러 **인증서 발급 규칙** 창을 엽니다.
    3. **PKI와 통합** 섹션에서 공개키 인프라와의 통합을 구성합니다.
    4. **모바일 인증서 발급** 섹션에서 인증서의 소스를 지정합니다.

아래에는 다음 사항을 가정하고 Kerberos 제한 위임(KCD)을 설정하는 과정의 예가 나와 있습니다:

- iOS MDM 웹 서비스는 포트 443에서 실행됨.
- 역방향 프록시가 있는 기기의 이름은 firewall.mydom.local입니다.
- iOS MDM 웹 서비스가 설치된 기기의 이름은 iosmdm.mydom.local입니다.
- iOS MDM 웹 서비스의 외부 게시 이름은 iosmdm.mydom.global입니다.

http/iosmdm.mydom.local의 서비스 사용자 이름

도메인에서 iOS MDM 웹 서비스가 설치된 기기(iosmdm.mydom.local)의 서비스 사용자 이름(SPN)을 등록해야 합니다:

```
setspn -a http/iosmdm.mydom.local iosmdm
```

역방향 프록시(firewall.mydom.local)를 사용하여 기기의 도메인 속성 구성

트래픽을 위임하려면 SPN으로 정의된 서비스(http/iosmdm.mydom.local)가 역방향 프록시가 설치된 기기(firewall.mydom.local)를 신뢰하도록 설정합니다.

SPN으로 정의된 서비스(http/iosmdm.mydom.local)가 역방향 프록시가 설치된 기기를 신뢰하도록 설정하려면 관리자가 다음 작업을 수행해야 합니다:

1. Microsoft Management Console 스냅인 "Active Directory 사용자 및 컴퓨터"에서 역방향 프록시가 설치된 기기(firewall.mydom.local)를 선택합니다.
2. 기기 속성의 **위임** 탭에서 **지정한 서비스로만 위임하도록 이 컴퓨터 신뢰** 토글을 **모든 인증 프로토콜 사용**으로 설정합니다.
3. SPN(http/iosmdm.mydom.local)을 **이 계정이 위임된 자격증명을 제공할 수 있는 서비스** 목록에 추가합니다.

게시된 웹 서비스(iosmdm.mydom.global)용 특수(사용자 지정) 인증서

FQDN iosmdm.mydom.global의 iOS MDM 웹 서비스용으로 특수(사용자 지정) 인증서를 발급해야 하며, 관리 콘솔의 iOS MDM 웹 서비스 설정에서 기본 인증서가 해당 인증서로 교체됨을 지정해야 합니다.

인증서 컨테이너(확장자가 p12 또는 pfx인 파일)에는 루트 키 체인(공개키)도 포함되어야 합니다.

역방향 프록시에서 iOS MDM 웹 서비스 게시

역방향 프록시에서 모바일 기기로부터 iosmdm.mydom.global의 포트 443으로 전송되는 트래픽에 대해 FQDN(iosmdm.mydom.global)용으로 발급된 인증서를 사용하여 SPN(http/iosmdm.mydom.local)에서 KCD를 구성해야 합니다. 게시 작업과 게시된 웹 서비스는 같은 서버 인증서를 공유해야 합니다.

APNs 인증서 받기

APNs 인증서가 이미 있는 경우 새 인증서를 생성하는 대신 갱신 해 보십시오. 기존 APNs 인증서를 새로 생성한 인증서로 교체하면 중앙 관리 서버가 현재 연결되어 있는 iOS 모바일 기기의 관리 기능을 상실합니다.

APNs 인증서 마법사의 첫 단계에서 인증서 서명 요청(CSR)이 생성되면 해당 개인 키가 기기의 RAM에 저장됩니다. 따라서 모든 마법사 단계를 애플리케이션의 단일 세션 내에서 완료해야 합니다.

APNs 인증서를 받으려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기 서버** 하위 폴더를 선택합니다.
2. **모바일 기기 서버** 폴더의 작업 영역에서 iOS MDM 서버를 선택합니다.
3. IOS MDM 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   그러면 iOS MDM 서버의 속성 창이 열립니다.
4. IOS MDM 서버의 속성 창에서 **인증서** 섹션을 선택합니다.
5. **인증서** 섹션의 **Apple 푸시 알림 인증서** 설정 그룹에서 **새로 요청** 버튼을 누릅니다.
   APNs 인증서 수신 마법사가 시작되고 **새로 요청** 창이 열립니다.
6. 인증서 서명 요청(이하 CSR)을 만듭니다. 이를 위해 다음 작업을 수행합니다:
   a. **CSR 만들기** 버튼을 누릅니다.
   b. **CSR 만들기** 창이 열리면 요청의 이름과 회사 및 부서 이름, 도시, 지역 및 국가를 지정합니다.
   c. **저장** 버튼을 누르고 CSR을 저장할 파일의 이름을 지정합니다.

   인증서의 개인 키는 기기 메모리에 저장됩니다.
7. Kaspersky이 서명하도록 CompanyAccount를 사용하여 CSR이 저장된 파일을 전송합니다.

   모바일 기기 관리 기능을 사용할 수 있도록 하는 키를 CompanyAccount 포털에 업로드한 후에만 CSR의 서명이 가능합니다.

   온라인 요청이 처리되면 Kaspersky에서 서명한 CSR 파일을 받게 됩니다.
8. 임의의 Apple ID를 사용해 서명된 CSR 파일을 Apple Inc. 웹사이트로 보냅니다.

   개인 Apple ID를 사용하지 않는 것이 좋습니다. 회사에서 사용할 전용 Apple ID를 만듭니다. Apple ID를 만들었으면 직원의 사서함이 아닌 조직의 사서함에 연결합니다.

   Apple Inc.에서 CSR이 처리되면 APNs 인증서의 공개 키를 받게 됩니다. 해당 파일을 디스크에 저장합니다.

9. CSR을 생성할 때 만들어진 개인 키와 함께 APNs 인증서를 PFX 파일 형식으로 내보냅니다. 이렇게 하려면:

   a. **새 APNs 인증서 요청** 창에서 **CSR 완료** 버튼을 누릅니다.

   b. **열기** 창에서 CSR 처리 결과로 Apple Inc.에서 받은 인증서 공개 키가 들어 있는 파일을 선택하고 **열기** 버튼을 누릅니다.

   인증서 내보내기 프로세스가 시작됩니다.

   c. 다음 창에서 개인 키 암호를 입력하고 **확인**을 누릅니다.

   이 암호는 iOS MDM 서버에 APNs 인증서를 설치하는 데 사용됩니다.

   d. **APNs 인증서 저장** 창에서 APNs 인증서의 파일 이름을 지정하고 폴더를 선택한 후 **저장**을 누릅니다.

인증서의 개인 키와 공개 키가 결합되고 APNs 인증서가 PFX 형식으로 저장됩니다. 이후에 iOS MDM 서버에 APNs 인증서를 설치할 수 있습니다.

APNs 인증서 갱신

APNs 인증서를 갱신하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기 서버** 하위 폴더를 선택합니다.
2. **모바일 기기 서버** 폴더의 작업 영역에서 iOS MDM 서버를 선택합니다.
3. IOS MDM 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   그러면 iOS MDM 서버의 속성 창이 열립니다.
4. IOS MDM 서버의 속성 창에서 **인증서** 섹션을 선택합니다.
5. **인증서** 섹션의 **Apple 푸시 알림 인증서** 설정 그룹에서 **갱신** 버튼을 누릅니다.

   APNs 인증서 갱신 마법사가 시작되고 **APNs 인증서 갱신** 창이 열립니다.
6. 인증서 서명 요청(이하 CSR)을 만듭니다. 이를 위해 다음 작업을 수행합니다:

   a. **CSR 만들기** 버튼을 누릅니다.

   b. **CSR 만들기** 창이 열리면 요청의 이름과 회사 및 부서 이름, 도시, 지역 및 국가를 지정합니다.

   c. **저장** 버튼을 누르고 CSR을 저장할 파일의 이름을 지정합니다.

   인증서의 개인 키는 기기 메모리에 저장됩니다.
7. Kaspersky이 서명하도록 CompanyAccount를 사용하여 CSR이 저장된 파일을 전송합니다.

   > 모바일 기기 관리 기능을 사용할 수 있도록 하는 키를 CompanyAccount 포털에 업로드한 후에만 CSR의 서명이 가능합니다.

   온라인 요청이 처리되면 Kaspersky에서 서명한 CSR 파일을 받게 됩니다.
8. 임의의 Apple ID를 사용해 서명된 CSR 파일을 Apple Inc. 웹사이트로 보냅니다.

개인 Apple ID를 사용하지 않는 것이 좋습니다. 회사에서 사용할 전용 Apple ID를 만듭니다. Apple ID를 만들었으면 직원의 사서함이 아닌 조직의 사서함에 연결합니다.

Apple Inc.에서 CSR이 처리되면 APNs 인증서의 공개 키를 받게 됩니다. 해당 파일을 디스크에 저장합니다.

9. 인증서의 공개 키를 요청합니다. 이를 위해 다음 작업을 수행합니다:

   a. Apple Push 인증서 포털로 이동합니다. 이 포털에 로그인하려면 최초 인증서 요청 시 받은 Apple ID를 사용합니다.

   b. 인증서 목록에서 APSP 이름("APSP: <번호>" 형식)이 iOS MDM 서버에서 사용하는 인증서의 APSP 이름과 일치하는 인증서를 선택하고 **갱신** 버튼을 누릅니다.

   APNs 인증서가 갱신됩니다.

   c. 포털에서 생성된 인증서를 저장합니다.

10. CSR을 생성할 때 만들어진 개인 키와 함께 APNs 인증서를 PFX 파일 형식으로 내보냅니다. 이를 위해 다음 작업을 수행합니다:

   a. **APNs 인증서 갱신** 창에서 **CSR 완료** 버튼을 누릅니다.

   b. **열기** 창에서 CSR 처리 결과로 Apple Inc.에서 받은 인증서 공개 키가 들어 있는 파일을 선택하고 **열기** 버튼을 누릅니다.

   인증서 내보내기 프로세스가 시작됩니다.

   c. 다음 창에서 개인 키 암호를 입력하고 **확인**을 누릅니다.

   이 암호는 iOS MDM 서버에 APNs 인증서를 설치하는 데 사용됩니다.

   d. **APNs 인증서 갱신** 창이 열리면 APNs 인증서의 파일 이름을 지정하고 폴더를 선택한 후 **저장**을 누릅니다.

인증서의 개인 키와 공개 키가 결합되고 APNs 인증서가 PFX 형식으로 저장됩니다.

예약 iOS MDM 서버 인증서 구성

iOS MDM 서버 기능을 사용하면 예약 인증서를 발급할 수 있습니다. 이 인증서는 iOS MDM 서버 인증서가 만료된 후 관리되는 iOS 기기가 원활하게 전환될 수 있도록 iOS MDM 구성 프로필에 사용하기 위한 것입니다.

iOS MDM 서버가 Kaspersky에서 발급한 기본 인증서를 사용하는 경우 iOS MDM 서버 인증서가 만료되기 전에 예약 인증서를 발급하거나 자체 사용자 지정 인증서를 예약으로 지정할 수 있습니다. 기본적으로 예약 인증서는 iOS MDM 서버 인증서 만료 60일 전에 자동으로 발급됩니다. 예약 iOS MDM 서버 인증서는 iOS MDM 서버 인증서 만료 직후에 기본 인증서가 됩니다. 공개 키는 구성 프로필을 통해 관리 중인 모든 기기에 배포되므로 수동으로 전송할 필요가 없습니다.

iOS MDM 서버 예약 인증서를 발급하거나 사용자 지정 예약 인증서를 지정하려면:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기 서버** 하위 폴더를 선택합니다.

2. 모바일 기기 서버 목록에서 관련 iOS MDM 서버를 선택하고 오른쪽 창에서 **iOS MDM 서버 구성** 단추를 클릭합니다.

3. iOS MDM 서버 속성 창이 열리면 **인증서** 섹션을 선택합니다.

4. 설정의 **인증서 예약** 블록에서 다음 중 하나를 수행합니다:

   - 자체 서명된 인증서(즉, Kaspersky에서 발급한 인증서)를 계속 사용하려는 경우:

     a. **발급** 버튼을 누릅니다.

     b. **활성화 날짜** 창이 열리면 예약 인증서를 적용해야 하는 날짜에 대한 두 가지 옵션 중 하나를 선택합니다.

     - 현재 인증서 만료 시 예약 인증서를 적용하려면 **현재 인증서 만료 시** 옵션을 선택합니다.
     - 현재 인증서가 만료되기 전에 예약 인증서를 적용하려면 **특정 기간(일) 이후** 옵션을 선택합니다. 이 옵션 옆에 있는 입력 필드에서 예약 인증서가 현재 인증서를 대체해야 하는 기간을 지정합니다.

     > 지정하는 예약 인증서의 유효 기간은 현재 iOS MDM 서버 인증서의 유효 기간을 초과할 수 없습니다.

     c. **확인** 버튼을 누릅니다.

     예약 iOS MDM 서버 인증서가 발급됩니다.

   - 인증 기관에서 발급한 사용자 지정 인증서를 사용하려는 경우:

     a. **추가** 버튼을 누릅니다.

     b. 파일 탐색기 창이 열리면 기기에 저장된 *.PEM, *.PFX 또는 *.P12 형식의 인증서 파일을 지정한 다음 **열기** 버튼을 클릭합니다.

     사용자 지정 인증서는 예약 iOS MDM 서버 인증서로 지정됩니다.

예약 iOS MDM 서버 인증서가 지정되었습니다. 예약 인증서의 세부 정보는 **인증서 예약** 설정 블록에 표시됩니다(인증서 이름, 발행자 이름, 만료 날짜 및 예약 인증서를 적용해야 하는 경우 해당 날짜).

iOS MDM 서버에 APNs 인증서 설치

APNs 인증서를 받았으면 이를 iOS MDM 서버에 설치해야 합니다.

IOS MDM 서버에 APNs 인증서를 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기 서버** 하위 폴더를 선택합니다.
2. **모바일 기기 서버** 폴더의 작업 영역에서 iOS MDM 서버를 선택합니다.
3. IOS MDM 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   그러면 iOS MDM 서버의 속성 창이 열립니다.
4. IOS MDM 서버의 속성 창에서 **인증서** 섹션을 선택합니다.
5. **인증서** 섹션의 **Apple 푸시 알림 인증서** 설정 그룹에서 **설치** 버튼을 누릅니다.

6. APNs 인증서가 들어 있는 PFX 파일을 선택합니다.

7. APNs 인증서를 내보낼 때 지정했던 개인 키의 암호를 입력합니다.

APNs 인증서가 iOS MDM 서버에 설치됩니다. 인증서 상세 정보가 iOS MDM 서버 속성 창의 **인증서** 섹션에 표시됩니다.

Apple 푸시 알림 서비스 접근 구성

iOS MDM 웹 서비스가 정상적으로 작동하고 모바일 기기가 관리자의 명령에 제때 응답하도록 하려면 iOS MDM 서버 설정에서 Apple 푸시 알림 서비스 인증서(이하 APNs 인증서로 지칭함)를 지정해야 합니다.

iOS MDM 웹 서비스는 Apple 푸시 알림(이하 APNs으로 지칭함)과 통신하여 포트 2197(아웃바운드)를 통해 외부 주소 api.push.apple.com에 연결합니다. 따라서 iOS MDM 웹 서비스에는 17.0.0.0/8 주소 범위에 대한 포트 TCP 2197 접근 권한이 필요합니다. iOS 기기에는 17.0.0.0/8 주소 범위에 대한 포트 TCP 5223 접근 권한이 필요합니다.

프록시 서버를 통해 iOS MDM 웹 서비스 쪽에서 APNs에 접근하려는 경우에는 iOS MDM 웹 서비스가 설치된 기기에서 다음 작업을 수행해야 합니다:

1. 레지스트리에 다음 문자열을 추가합니다:

   - 32비트 운영 체제:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<프록시 호스트 이름>"
"ApnProxyPort"="<프록시 포트>"
"ApnProxyLogin"="<프록시 아이디>"
"ApnProxyPwd"="<프록시 암호>"
```

   - 64비트 운영 체제:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<프록시 호스트 이름>"
"ApnProxyPort"="<프록시 포트>"
"ApnProxyLogin"="<프록시 아이디>"
"ApnProxyPwd"="<프록시 암호>"
```

2. iOS MDM 웹 서비스를 재시작합니다.

모바일 기기에 공유 인증서 발급 및 설치

사용자에게 공유 인증서를 발급하려면 다음을 수행합니다:

1. 콘솔 트리의 **사용자 계정** 폴더에서 사용자 계정을 선택합니다.

2. 사용자 계정의 컨텍스트 메뉴에서 **인증서 설치**를 선택합니다.

그러면 인증서 설치 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

마법사를 마치면 인증서가 만들어져 사용자의 인증서 목록에 추가됩니다.

발급된 인증서를 사용자가 다운로드하고 이때 iOS MDM 프로필이 포함된 설치 패키지도 함께 다운로드됩니다.

모바일 기기가 iOS MDM 서버에 연결된 후 iOS MDM 프로필 설정은 사용자의 기기에 적용됩니다. 관리자는 연결 이후에 기기를 관리할 수 있게 됩니다.

iOS MDM 서버에 연결된 사용자의 모바일 기기는 **모바일 기기** 폴더에 표시되는데 이 폴더는 콘솔 트리 **모바일 기기 관리** 폴더의 하위 폴더입니다.

관리 중인 기기 목록에 KES 기기 추가

Google Play™로의 링크를 사용해 관리 중인 기기 목록에 사용자의 KES 기기를 추가하려면:

1. 콘솔 트리에서 **사용자 계정** 폴더를 선택합니다.

   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.

2. 관리 중인 기기 목록에 모바일 기기를 추가할 사용자 계정을 선택합니다.

3. 사용자 계정의 마우스 오른쪽 메뉴에서 **모바일 기기 추가**을 선택합니다.

   모바일 기기 연결 마법사가 시작됩니다. 마법사의 **인증서 소스** 창에서 중앙 관리 서버가 모바일 기기를 식별하기 위해 사용할 공유 인증서의 생성 방법을 지정해야 합니다. 다음 방법 중 하나를 사용해 공유 인증서를 지정할 수 있습니다:

   - 중앙 관리 서버 도구를 사용하여 자동으로 공유 인증서를 생성한 후 해당 인증서를 기기에 전달합니다.
   - 공유 인증서 파일을 지정합니다.

4. 마법사의 **기기 유형** 창에서 **Google Play로의 링크**을 선택합니다.

5. 마법사의 **사용자 알림 방법** 창에서 인증서 생성 시 모바일 기기 사용자 알림 설정을 정의합니다(SMS 메시지, 이메일, 마법사 완료 시 정보 표시 중 하나).

6. 마법사의 인증서 정보 패널에서 **마침** 버튼을 클릭해 마법사를 닫습니다.

마법사가 동작을 마친 후 사용자의 모바일 기기로 링크 및 QR 코드가 보내지며, 이를 통해 Google Play에서 Kaspersky Endpoint Security를 다운로드할 수 있습니다. 사용자는 해당 링크를 누르거나 QR 코드를 스캔하여 Google Play에 접속합니다. 그 이후 기기의 운영 체제가 Kaspersky Endpoint Security for Android 설치에 동의할 것인지를 물어봅니다. Kaspersky Endpoint Security for Android가 다운로드되고 설치된 후 모바일 기기는 중앙 관리 서버에 연결 및 공유 인증서를 다운로드합니다. 인증서가 모바일 기기에 설치된 이후에 콘솔 트리의 **모바일 기기 관리** 폴더의 하위 폴더인 **모바일 기기** 폴더에 후자가 표시됩니다.

만일 Kaspersky Endpoint Security for Android가 이미 기기에 설치되어 있다면, 사용자는 관리자에게 중앙 관리 서버 연결 설정을 물어본 후 독립적으로 해당 정보를 입력해야 합니다. 연결 설정이 정의된 이후에 모바일 기기는 중앙 관리 서버에 연결됩니다. 관리자는 해당 기기에 대한 공유 인증서를 발급하며 사용자에게 이메일이나 SMS 메시지로 인증서를 다운로드할 수 있는 아이디와 암호를 발송합니다. 이후 사용자는 공유 인증서를 다운로드하고 설치할 수 있습니다. 인증서가 모바일 기기에 설치된 이후에 콘솔 트리의 **모바일 기기 관리** 폴더의 하위 폴더인 **모바일 기기** 폴더에 후자가 표시됩니다. 이 경우 Kaspersky Endpoint Security for Android는 다운로드되지 않고 다시 설치되지 않습니다.

KES 기기를 중앙 관리 서버에 연결

중앙 관리 서버에 기기를 연결하는 데 사용하는 방법에 따라 KES 기기용 Kaspersky Device Management for iOS에 대해 두 가지 배포 구성을 사용할 수 있습니다:

- 기기를 중앙 관리 서버에 직접 연결하는 배포 구성
- Kerberos 제한 위임을 지원하는 역방향 프록시와 관련된 배포 방식

중앙 관리 서버에 기기 직접 연결

KES 기기는 중앙 관리 서버의 포트 13292에 직접 연결할 수 있습니다.

인증에 사용하는 방법에 따라 두 가지 옵션을 통해 중앙 관리 서버에 KES 기기를 연결할 수 있습니다:

- 사용자 인증서를 사용하여 기기 연결
- 사용자 인증서 없이 기기 연결

사용자 인증서를 사용하여 기기 연결

사용자 인증서를 사용하여 연결하는 기기는 중앙 관리 서버 도구를 통하여 해당 인증서가 할당된 사용자 계정과 연결됩니다.

이 경우 양방향 SSL 인증(상호 인증)이 사용됩니다. 중앙 관리 서버와 기기가 모두 인증서를 통해 인증됩니다.

사용자 인증서 없이 기기 연결

사용자 인증서 없이 연결하는 기기는 중앙 관리 서버의 사용자 계정과 연결되지 않습니다. 그러나 기기는 인증서를 수신하면 중앙 관리 서버 도구를 통하여 해당 인증서가 할당된 사용자와 연결됩니다.

해당 기기를 중앙 관리 서버에 연결할 때는 단방향 SSL 인증이 적용되므로, 중앙 관리 서버만 인증서를 통해 인증됩니다. 기기가 사용자 인증서를 가져오면 인증 유형이 양방향 SSL 인증 (상호 인증)으로 변경됩니다.

Kerberos 제한 위임(KCD)을 사용하는 서버에 KES 기기를 연결하기 위한 구성

Kerberos 제한 위임(KCD)을 사용하는 중앙 관리 서버에 KES 기기를 연결하기 위한 구성에서는 다음 기능이 제공됩니다:

- KCD를 지원하는 역방향 프록시와 통합.
- 모바일 기기 인증에 Kerberos 제한 위임(이하 KCD로 지칭함)을 사용하는 기능.
- 사용자 인증서를 적용하기 위해 공개키 인프라(이하 PKI로 지칭함)와 통합하는 기능.

이 연결 구성을 사용할 때는 다음 사항을 참고하십시오:

- 역방향 프록시에 대한 KES 기기 연결 유형은 "양방향 SSL 인증"이어야 합니다. 즉, 기기가 관련 사용자 인증서를 통해 역방향 프록시에 연결해야 합니다. 기기가 이와 같이 연결되도록 하려면 기기에 설치된 Kaspersky Endpoint Security for Android의 설치 패키지에 사용자 인증서를 통합해야 합니다. 이 KES 패키지는 이 기기(사용자) 전용으로 중앙 관리 서버에서 만든 것이어야 합니다.

- 모바일 프로토콜용 기본 서버 인증서 대신 특수(사용자 지정) 인증서를 지정해야 합니다:

  1. 중앙 관리 서버 속성 창의 **설정** 섹션에서 **모바일 기기용 포트 열기** 확인란을 선택하고 드롭다운 목록에서 **인증서 추가**를 선택합니다.

  2. 열리는 창에서 모바일 프로토콜에 대한 액세스 포인트를 중앙 관리 서버에 게시할 때 역방향 프록시에서 설정한 것과 같은 인증서를 지정합니다.

- 도메인의 인증 기관(CA)에서 KES 기기용 사용자 인증서를 발급해야 합니다. 도메인에 루트 CA가 여러 개 포함되어 있으면 역방향 프록시에서 게시할 때 설정했던 CA에서 사용자 인증서를 발급해야 합니다.

  다음 방법 중 하나를 사용하여 사용자 인증서가 위에서 설명한 요구 사항을 준수함을 확인할 수 있습니다:

  - 새 패키지 마법사와 인증서 설치 마법사에서 특수 사용자 인증서를 지정합니다.

  - 중앙 관리 서버를 도메인 PKI와 통합하고 인증서 발급을 위한 규칙에서 해당하는 설정을 정의합니다:

    1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **인증서** 하위 폴더를 선택합니다.

    2. **인증서** 폴더의 작업 영역에서 **인증서 발급 규칙 구성** 버튼을 눌러 **인증서 발급 규칙** 창을 엽니다.

    3. **PKI와 통합** 섹션에서 공개키 인프라와의 통합을 구성합니다.

    4. **모바일 인증서 발급** 섹션에서 인증서의 소스를 지정합니다.

아래에는 다음 사항을 가정하고 Kerberos 제한 위임(KCD)을 설정하는 과정의 예가 나와 있습니다:

- 중앙 관리 서버의 모바일 프로토콜에 대한 액세스 포인트가 13292 포트로 설정되어 있음.

- 역방향 프록시가 있는 기기의 이름은 firewall.mydom.local입니다.

- 중앙 관리 서버가 설치된 기기의 이름은 ksc.mydom.local임.

- 모바일 프로토콜에 대한 액세스 포인트의 외부 게시 이름은 kes4mob.mydom.global임.

중앙 관리 서버용 도메인 계정

중앙 관리 서버를 실행할 도메인 계정(예: KSCMobileSrvcUsr)을 만들어야 합니다. 중앙 관리 서버 서비스용 계정은 중앙 관리 서버를 실행할 때 지정하거나 klsrvswch 유틸리티를 통해 지정할 수 있습니다. klsrvswch 유틸리티는 중앙 관리 서버의 설치 폴더에 있습니다. 기본 설치 경로: <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

도메인 계정을 지정해야 하는 이유는 다음과 같습니다:

- KES 기기 관리용 기능은 중앙 관리 서버의 필수 요소입니다.

- Kerberos 제한 위임(KCD)이 올바르게 작동하도록 하려면 수신 쪽(중앙 관리 서버)을 도메인 계정으로 실행해야 합니다.

http/kes4mob.mydom.local의 서비스 사용자 이름

도메인의 KSCMobileSrvcUsr 계정에 중앙 관리 서버가 설치된 기기의 포트 13292에서 모바일 프로토콜 서비스를 게시하기 위한 SPN을 추가합니다. 중앙 관리 서버가 설치된 kes4mob.mydom.local 기기의 경우 이는 다음과 같이 표시됩니다:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

역방향 프록시(firewall.mydom.local)를 사용하여 기기의 도메인 속성 구성

트래픽을 위임하려면 SPN으로 정의된 서비스(http/kes4mob.mydom.local:13292)가 역방향 프록시가 설치된 기기(firewall.mydom.local)를 신뢰하도록 설정합니다.

SPN으로 정의된 서비스(http/kes4mob.mydom.local:13292)가 역방향 프록시가 설치된 기기를 신뢰하도록 설정하려면 관리자가 다음 작업을 수행해야 합니다:

1. Microsoft Management Console 스냅인 "Active Directory 사용자 및 컴퓨터"에서 역방향 프록시가 설치된 기기(firewall.mydom.local)를 선택합니다.
2. 기기 속성의 **위임** 탭에서 **지정한 서비스로만 위임하도록 이 컴퓨터 신뢰** 토글을 **모든 인증 프로토콜 사용**으로 설정합니다.
3. **이 계정이 위임된 자격증명을 제공할 수 있는 서비스** 목록에서 SPN http/kes4mob.mydom.local:13292를 추가합니다.

게시(kes4mob.mydom.global)용 특수(사용자 지정) 인증서

중앙 관리 서버의 모바일 프로토콜을 게시하려면 FQDN kes4mob.mydom.global용으로 특수(사용자 지정) 인증서를 발급하여 관리 콘솔 내 중앙 관리 서버의 모바일 프로토콜 설정에서 기본 서버 인증서 대신 해당 인증서를 지정해야 합니다. 이렇게 하려면 중앙 관리 서버의 속성 창 **설정** 섹션에서 **모바일 기기용 포트 열기** 확인란을 선택하고 드롭다운 목록에서 **인증서 추가**를 선택합니다.

서버 인증서 컨테이너(확장자가 p12 또는 pfx인 파일)에는 루트 키 체인(공개키)도 포함되어야 합니다.

역방향 프록시에서 게시 구성

역방향 프록시에서 모바일 기기 쪽으로부터 kes4mob.mydom.global의 포트 13292로 전송되는 트래픽에 대해 FQDN(kes4mob.mydom.global)용으로 발급된 서버 인증서를 사용하여 SPN(http/kes4mob.mydom.local:13292)에서 KCD를 구성해야 합니다. 게시 작업과 게시된 액세스 포인트(중앙 관리 서버의 포트 13292)는 같은 서버 인증서를 공유해야 합니다.

Firebase Cloud Messaging 사용

Android 운영 체제에 의해 관리되는 KES 기기에 적절히 명령을 전달하기 위해 Kaspersky Security Center는 푸시 알림 메커니즘을 사용합니다. Firebase 클라우드 메시지(이하 FCM)를 통해 KES 기기와 중앙 관리 서버 간에 푸시 알림을 교환합니다. Kaspersky Security Center 관리 콘솔에서 해당 서비스에 KES 기기를 연결하기 위해 Firebase Cloud Messaging 설정을 지정할 수 있습니다.

Firebase Cloud Messaging 설정을 가져오려면 Google 계정이 있어야 합니다.

FCM을 사용하도록 설정하려면 다음을 수행합니다:

1. 관리 콘솔에서 **모바일 기기 관리** 노드와 **모바일 기기** 폴더를 선택합니다.
2. **모바일 기기** 폴더의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 폴더 속성에서 **Firebase Cloud Messaging 설정** 섹션을 선택합니다.
4. **Firebase 프로젝트 번호** 필드에서 FCM 발신자 ID를 지정합니다.
5. **개인 키 파일(JSON 형식)** 필드에서 개인 키 파일을 선택합니다.

   중앙 관리 서버와의 다음 동기화에서 Android 운영 체제에 의해 관리되는 KES 기기는 Firebase Cloud Messaging에 연결됩니다.

기기 초기 설정으로 재설정 버튼을 클릭하여 Firebase Cloud Messaging의 설정을 편집할 수 있습니다.

다른 Firebase 프로젝트로 전환하면 FCM이 재개될 때까지 10분을 기다려야 합니다.

FCM 서비스는 다음 주소 범위에서 실행됩니다:

- KES 기기 쪽에서는 다음 주소의 포트 443(HTTPS), 5228(HTTPS), 5229(HTTPS) 및 5230(HTTPS) 접근 권한이 필요합니다:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Google의 ASN 15169에 나열된 모든 IP 주소
- 중앙 관리 서버 쪽에서는 다음 주소의 포트 443(HTTPS) 접근 권한이 필요합니다:
  - fcm.googleapis.com
  - Google의 ASN 15169에 나열된 모든 IP 주소

관리 콘솔의 중앙 관리 서버 속성에서 프록시 서버 설정(**고급/인터넷 연결 구성**)을 정의한 경우에는 FCM과의 통신에 해당 설정이 사용됩니다.

FCM 구성: 발신자 ID 및 개인 키 파일 가져오기

FCM을 구성하려면:

1. Google 포털에 등록합니다.
2. Firebase 콘솔로 이동합니다.

3. 다음 중 하나를 수행합니다:

   - 새 프로젝트를 생성하려면 **프로젝트 생성**을 클릭하고 화면의 지침을 따릅니다.
   - 기존 프로젝트를 엽니다.

4. 기어 아이콘을 클릭하고 **프로젝트 설정**을 선택합니다.
   프로젝트 설정 창이 열립니다.

5. **클라우드 메시지** 탭을 선택합니다.

6. **Firebase 클라우드 메시지 API(V1)** 섹션의 **발신자 ID** 필드에서 관련 발신자 ID를 검색합니다.

7. **서비스 계정** 탭을 선택하고 **새 개인 키 생성**을 클릭합니다.

8. 창이 열리면 **키 생성**을 클릭하여 개인 키 파일을 생성하고 다운로드합니다.

   이제 Firebase 클라우드 메시지가 구성되었습니다.

공개 키 인프라와의 통합

기본적으로는 중앙 관리 서버의 도메인 사용자 인증서 발급 과정을 간소화하기 위해 공개키 인프라(이하 PKI로 지칭함)와의 통합을 수행합니다.

관리자는 관리 콘솔에서 사용자에게 도메인 인증서를 할당할 수 있습니다. 다음 방법 중 하나를 사용해 이 할당을 수행할 수 있습니다:

- 인증서 설치 마법사에서 사용자에게 파일의 특수(사용자 지정) 인증서를 할당합니다.
- PKI와의 통합을 수행하고 특정 인증서 유형 또는 모든 인증서 유형의 인증서 소스 역할을 할 PKI 할당.

PKI와의 통합 설정은 **공개 키 인프라와 통합** 링크를 눌러 **모바일 기기 관리/인증서** 폴더의 작업 영역에서 사용할 수 있습니다.

도메인 사용자 인증서 발급을 위한 PKI와의 통합 관련 일반 원칙

관리 콘솔에서 **모바일 기기 관리/인증서** 폴더의 작업 영역에 있는 **공개 키 인프라와 통합** 링크를 클릭하여 중앙 관리 서버가 도메인 CA를 통해 도메인 사용자 인증서를 발급하는 데 사용하도록 할 도메인 계정(이하 PKI와의 통합을 수행하는 계정으로 지칭함)을 지정합니다.

이때 다음 사항을 참고하십시오:

- PKI와의 통합 설정을 사용하면 모든 인증서 유형의 기본 템플릿을 지정할 수 있습니다. **인증서 발급 규칙 구성** 버튼을 눌러 **모바일 기기 관리/인증서** 폴더의 작업 영역에서 제공되는 인증서 발급을 위한 규칙을 통해 모든 인증서 유형에 대해 개별 템플릿을 지정할 수 있습니다.
- 중앙 관리 서버가 설치된 기기에서 PKI와의 통합을 수행하는 계정의 인증서 저장소에 특수 등록 에이전트(EA) 인증서를 설치해야 합니다. 등록 에이전트(EA) 인증서는 도메인 CA(인증 기관)의 관리자가 발급합니다.

PKI와의 통합을 수행하는 계정은 다음 기준을 충족해야 합니다:

- 도메인 사용자여야 합니다.
- PKI와의 통합을 시작하는 중앙 관리 서버가 설치된 기기의 로컬 관리자여야 합니다.
- *서비스로 로그온*할 수 있는 권한이 있어야 합니다.
- 영구 사용자 프로필을 만들려면 중앙 관리 서버가 설치된 기기를 한 번 이상 이 계정으로 실행해야 합니다.

Kaspersky Security Center 웹 서버

Kaspersky Security Center 웹 서버(이후 웹 서버라고도 함)는 Kaspersky Security Center의 한 구성 요소입니다. 웹 서버는 독립 실행형 설치 패키지 게시, 모바일 기기용 독립 실행형 설치 패키지, iOS MDM 프로필 및 공유 폴더의 파일을 게시하도록 설계되었습니다.

만들어진 iOS MDM 프로필 및 설치 패키지는 웹 서버에 자동으로 게시되며 처음으로 다운로드하고 나면 제거됩니다. 관리자는 이메일 등의 편리한 방법을 사용하여 새 링크를 전송할 수 있습니다.

사용자는 이 링크를 눌러 요청된 정보를 모바일 기기로 다운로드할 수 있습니다.

웹 서버 설정

웹 서버를 미세 조정해야 하는 경우 관리 콘솔 웹 서버의 속성을 통해 HTTP용 포트(8060)와 HTTPS용 포트(8061)를 변경할 수 있습니다. 포트 변경 외에 HTTPS용 서버 인증서를 교체할 수 있으며 HTTP용 웹 서버의 FQDN도 변경할 수 있습니다.

Kaspersky Security Center 설치

이 섹션에서는 Kaspersky Security Center 구성 요소의 설치에 대해 설명합니다. 하나의 기기에만 로컬로 애플리케이션을 설치하려는 경우 두 가지 설치 옵션을 사용할 수 있습니다.

- **표준**. 기업 네트워크 내의 소규모 영역에서 작동 방식을 테스트하는 등 Kaspersky Security Center를 시험적으로 사용해 보려는 경우 이 옵션을 선택하는 것이 좋습니다. 표준 설치 시에는 데이터베이스만 구성합니다. Kaspersky 애플리케이션에 대한 기본 관리 플러그인 세트만 설치할 수도 있습니다. Kaspersky Security Center로 작업을 이미 해 본 적이 있는 경우 표준 설치를 사용할 수도 있습니다. 즉, 사용자는 표준 설치 후 모든 관련 설정을 지정하는 방법을 알고 있기 때문입니다.
- **사용자 지정**. 이 옵션은 공유 폴더 경로, 계정, 중앙 관리 서버 연결용 포트, 데이터베이스 설정 등의 Kaspersky Security Center 설정을 수정하고자 할 때 사용하기를 권장합니다. 사용자 지정 설치를 선택하는 경우 설치할 Kaspersky 관리 플러그인을 지정할 수 있습니다. 필요하다면 숨김 모드로 사용자 지정 설치를 시작할 수 있습니다.

네트워크에 중앙 관리 서버가 1대 이상 설치되어 있는 경우 강제 설치를 사용하는 원격 설치 작업을 통해 원격으로 다른 기기에 서버를 설치할 수 있습니다. 원격 설치 작업을 생성하는 경우, 중앙 관리 서버 설치 패키지인 ksc_<version_number>.<build number>_full_<localization language>.exe를 사용해야 합니다.

Kaspersky Security Center가 완전히 작동하는 데 필요한 모든 구성 요소를 설치하거나 이러한 구성 요소의 현재 버전을 업그레이드하려는 경우 이 패키지를 사용하십시오.

Kaspersky Security Center 장애 조치 클러스터를 배포하려면 클러스터의 모든 노드에 Kaspersky Security Center를 설치해야 합니다.

설치 준비

설치를 시작하기 전에 다음 작업을 수행하십시오.

- **하드웨어 및 소프트웨어 요구 사항 확인**

  기기의 하드웨어 및 소프트웨어가 중앙 관리 서버 및 관리 콘솔을 위한 요구 사항을 충족하는지 확인하십시오.

- **데이터베이스 관리 시스템(DBMS) 선택 및 설치**

  Kaspersky Security Center는 DBMS에서 관리하는 데이터베이스에 정보를 저장합니다. Kaspersky Security Center 이전에 네트워크에 DBMS를 설치합니다(DBMS 선택 방법 자세히 알아보기). PostgreSQL 또는 Postgres Pro DBMS 설치 시, 슈퍼유저의 암호를 지정하십시오. 암호를 지정하지 않으면 중앙 관리 서버가 데이터베이스에 연결하지 못할 수 있습니다.

  도메인 컨트롤러 대신 전용 서버에 중앙 관리 서버를 설치할 것을 권장합니다. RODC(읽기 전용 도메인 컨트롤러) 역할을 하는 서버에 Kaspersky Security Center를 설치하는 경우 Microsoft SQL Server(SQL Express)를 (동일한 기기에) 로컬로 설치해서는 안 됩니다. 이때, Microsoft SQL Server(SQL Express)를 (다른 장치에) 원격 설치하거나, DBMS를 로컬로 설치해야 한다면 MySQL, MariaDB, PostgreSQL 중 하나를 사용할 것을 권장합니다.

- **중앙 관리 서버, 네트워크 에이전트, 관리 콘솔용 폴더 준비**

  대/소문자 구분이 비활성화된 폴더에 중앙 관리 서버, 네트워크 에이전트, 관리 콘솔를 설치해야 합니다. 또한 중앙 관리 서버 공유 폴더 및 Kaspersky Security Center 숨겨진 폴더(%ALLUSERSPROFILE%\KasperskyLab\adminkit)에는 대/소문자 구분을 비활성화해야 합니다.

- **이전 네트워크 에이전트 제거**

  네트워크 에이전트의 서버 버전은 중앙 관리 서버가 설치된 기기에 설치됩니다. 중앙 관리 서버를 일반 버전의 네트워크 에이전트와는 함께 설치할 수 없습니다. 서버 버전의 네트워크 에이전트가 기기에 이미 설치되어 있을 경우 이를 제거하고 중앙 관리 서버의 설치를 다시 시작하십시오. 네트워크 에이전트의 서버 버전에 대한 자세한 내용은 Kaspersky Security Center 설치 후 시스템 변경 사항을 참조하십시오.

- **계정 확인**

  Kaspersky Security Center를 설치하려면 설치를 수행할 기기에 대한 관리자 권한이 필요합니다.

  Kaspersky Security Center는 관리 서비스 계정 및 그룹 관리 서비스 계정을 지원합니다. 이러한 유형의 계정을 도메인에서 사용하고 그중 하나를 중앙 관리 서버 서비스의 계정으로 지정하려면 먼저 중앙 관리 서버를 설치할 동일한 기기에 계정을 설치합니다. 로컬 기기에 관리 중인 서비스 계정을 설치하는 방법에 대한 자세한 내용은 공식 Microsoft 설명서를 참조하십시오.

DBMS 작업용 계정

중앙 관리 서버를 설치하고 작업하려면, 중앙 관리 서버 설치 프로그램(이하 설치 프로그램)을 실행할 Windows 계정, 중앙 관리 서버 서비스를 시작할 Windows 계정, 그리고 DBMS 접속을 위한 내부 DBMS 계정이 필요합니다. 새 계정을 만들거나 기존 계정을 사용할 수 있습니다. 이 모든 계정에는 특정 권한이 필요합니다. 필요한 계정 및 해당 권한 집합은 다음 기준에 따라 달라집니다:

- DBMS 유형:
  - Microsoft SQL 서버(Windows 인증과 SQL Server 인증 사용)
  - MySQL 또는 MariaDB
  - PostgreSQL 또는 Postgres Pro
- DBMS 위치:
  - **로컬 DBMS**. *로컬 DBMS*는 중앙 관리 서버와 동일한 기기에 설치된 DBMS입니다.
  - **원격 DBMS**. *원격 DBMS*는 다른 기기에 설치된 DBMS입니다.
- 중앙 관리 서버 데이터베이스 생성 방법:
  - **자동**. 중앙 관리 서버를 설치하는 동안 중앙 관리 서버 설치 프로그램(설치 프로그램)을 사용하여 중앙 관리 서버 데이터베이스(이하 서버 데이터베이스)를 자동 생성할 수 있습니다.
  - **수동**. 타사 애플리케이션(SQL Server Management Studio 등) 또는 스크립트를 사용하여 빈 데이터베이스를 생성할 수 있습니다. 그런 다음 중앙 관리 서버 설치 중에 이 데이터베이스를 서버 데이터베이스로 지정할 수 있습니다.

계정에 권한을 부여할 때는 최소 권한 원칙을 따르십시오. 즉, 필요한 작업을 수행할 수 있을 정도의 권한만 부여해야 합니다.

아래 표에는 중앙 관리 서버를 설치하고 시작하기 전에 계정에 부여해야 하는 시스템 권한 및 DBMS 권한에 대한 정보가 있습니다.

Windows 인증을 사용하는 Microsoft SQL Server

SQL Server를 DBMS로 선택하면 Windows 인증을 사용하여 SQL Server에 액세스할 수 있습니다. 설치 프로그램 실행에 사용되는 Windows 계정과 중앙 관리 서버 서비스 시작에 사용되는 Windows 계정에 대한 시스템 권한을 구성합니다. SQL Server에서 이 두 Windows 계정 모두에 대한 로그인을 만듭니다. 서버 데이터베이스의 생성 방법에 따라 아래 표에 설명된 대로 이러한 계정에 필요한 SQL Server 권한을 부여합니다. 계정 권한을 구성하는 방법에 대한 자세한 내용은 SQL Server 작업을 위한 계정 구성(Windows 인증)을 참조하십시오.

DBMS: Windows 인증 모드로 실행되는 Microsoft SQL Server(Express Edition 포함)

	자동 데이터베이스 생성(설치 프로그램)	수동 데이터베이스 생성(관리자)
설치 프로그램을 실행하는 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만. • 로컬 DBMS: 로컬 관리자 계정 또는 도메인 계정.	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만. • 로컬 DBMS: 로컬 관리자 계정 또는 도메인 계정.

설치 프로그램을 실행하는 계정에 대한 권한	• 시스템 권한: 로컬 관리자 권한.
	• SQL Server 권한:
	  • 서버 레벨 역할: sysadmin.
		• 시스템 권한: 로컬 관리자 권한.
		• SQL Server 권한:
		  • 서버 레벨 역할: public.
		  • 서버 데이터베이스의 데이터베이스 역할 구성원: db_owner, public.
		  • 서버 데이터베이스의 기본 스키마: dbo.

중앙 관리 서버 서비스 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만.
	• 로컬 DBMS:
	  • 관리자가 선택한 Windows 계정.
	  • 설치 프로그램이 자동 생성하는 KL-AK-* 형식의 계정.
		• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만.
		• 로컬 DBMS:
		  • 관리자가 선택한 Windows 계정.
		  • 설치 프로그램이 자동 생성하는 KL-AK-* 형식의 계정(이때, KL-AK-* 계정의 자동 생성은 권장하지 않습니다).

중앙 관리 서버 서비스 계정에 대한 권한	• 시스템 권한: 설치 프로그램이 할당한 필수 권한.
	• SQL Server 권한: 설치 프로그램이 할당한 필수 권한.
		• 시스템 권한: 설치 프로그램이 할당한 필수 권한.
		• SQL Server 권한:
		  • 서버 레벨 역할: public.
		  • 서버 데이터베이스의 데이터베이스 역할 구성원: db_owner, public.
		  • 서버 데이터베이스의 기본 스키마: dbo.

SQL Server 인증을 사용하는 Microsoft SQL Server

SQL Server를 DBMS로 선택하면 SQL Server 인증을 사용하여 SQL Server에 액세스할 수 있습니다. 설치 프로그램 실행에 사용되는 Windows 계정과 중앙 관리 서버 서비스 시작에 사용되는 Windows 계정에 대한 시스템 권한을 구성합니다. SQL Server에서 인증에 사용할 아이디와 암호를 생성합니다. 그런 다음 이 SQL Server 계정에 아래 표에 나열된 필수 권한을 부여합니다. 계정 권한 구성 방법에 대한 자세한 내용은 SQL Server 작업을 위한 계정 구성(SQL Server 인증)을 참조하십시오.

DBMS: SQL Server 인증(Express Edition 포함)을 사용하는 Microsoft SQL Server

	자동 데이터베이스 생성(설치 프로그램)	수동 데이터베이스 생성(관리자)
설치 프로그램을 실행하는 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만. • 로컬 DBMS: 로컬 관리자 계정 또는 도메인 계정.	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만. • 로컬 DBMS: 로컬 관리자 계정 또는 도메인 계정.
설치 프로그램을 실행하는 계정에 대한 권한	시스템 권한: 로컬 관리자 권한.	시스템 권한: 로컬 관리자 권한.

중앙 관리 서버 서비스 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만.
	• 로컬 DBMS:
	  • 관리자가 선택한 Windows 계정.
	  • 설치 프로그램이 자동 생성하는 KL-AK-* 형식의 계정.
		• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만.
		• 로컬 DBMS:
		  • 관리자가 선택한 Windows 사용자 계정.
		  • 설치 프로그램이 자동 생성하는 KL-AK-* 형식의 계정.

중앙 관리 서버 서비스 계정에 대한 권한	시스템 권한: 설치 프로그램이 할당한 필수 권한.	시스템 권한: 설치 프로그램이 할당한 필수 권한.

	자동 데이터베이스 생성(설치 프로그램)	수동 데이터베이스 생성(관리자)

SQL Server 인증에 사용되는 아이디 권한	데이터베이스를 생성하고 중앙 관리 서버를 설치하는 데 필요한 SQL Server 권한:
	• 서버 레벨 역할: public.
	• *마스터* 데이터베이스의 데이터베이스 역할 구성원: db_owner.
	• *마스터* 데이터베이스의 기본 스키마: dbo.
	• 권한:
	  • CONNECT ANY DATABASE
	  • CONNECT SQL
	  • CREATE ANY DATABASE
	  • VIEW ANY DATABASE
	  • 서버 상태 표시(**항상 켜기** 옵션 활성화 시)
	중앙 관리 서버 작업에 필요한 SQL Server 권한:
	• 서버 레벨 역할: public.
	• 서버 데이터베이스의 데이터베이스 역할 구성원: db_owner.
	• 서버 데이터베이스의 기본 스키마: dbo.
	• 권한:
	  • CONNECT SQL
	  • VIEW ANY DATABASE
	  • 서버 상태 표시(**항상 켜기** 옵션 활성화 시)
	  • VIEW ANY DEFINITION
		SQL Server 권한:
		• 서버 레벨 역할: public.
		• 서버 데이터베이스의 데이터베이스 역할 구성원: db_owner.
		• 서버 데이터베이스의 기본 스키마: dbo.
		• 권한:
		  • CONNECT SQL
		  • VIEW ANY DATABASE
		  • VIEW ANY DEFINITION

중앙 관리 서버 데이터 복구를 위한 SQL Server 권한 구성

백업에서 중앙 관리 서버 데이터를 복원하려면, 중앙 관리 서버 설치에 사용된 Windows 계정으로 klbackup 유틸리티를 실행하십시오. klbackup 유틸리티를 시작하기 전에 SQL Server에서 이 Windows 계정과 연결된 SQL Server 아이디에 대한 권한을 부여하십시오. SQL Server 권한은 중앙 관리 서버 버전에 따라 다릅니다. 버전 14.2 이상의 중앙 관리 서버에서는 sysadmin 서버 레벨 역할 또는 dbcreator 서버 레벨 역할을 부여할 수 있습니다.

중앙 관리 서버 데이터베이스 복구를 위한 SQL Server 권한

중앙 관리 서버 버전 14.2 이상	기타 중앙 관리 서버 버전

• SQL Server 권한:
  • 서버 레벨 역할: dbcreator.
• 권한:
  • VIEW ANY DEFINITION
klbackup 유틸리티를 시작하기 전에 KLSRV_SKIP_ADJUSTING_DBMS_ACCESS 서버 플래그를 지정하십시오. 관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다. 이후, 명령줄에서 다음 명령을 실행합니다.
`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL 및 MariaDB

MySQL 또는 MariaDB를 DBMS로 선택 시, DBMS 내부 계정을 만들고 이 계정에 아래 표에 나열된 필수 권한을 부여합니다. 설치 프로그램과 중앙 관리 서버 서비스는 이 내부 DBMS 계정을 사용하여 DBMS에 액세스합니다. 데이터베이스 생성 방법은 필요한 권한 집합에 영향을 미치지 않습니다. 계정 권한을 구성하는 방법에 대한 자세한 내용은 MySQL 및 MariaDB 작업을 위한 계정 구성을 참조하십시오.

DBMS: MySQL 및 MariaDB

	자동 또는 수동 데이터베이스 생성
설치 프로그램을 실행하는 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만. • 로컬 DBMS: 로컬 관리자 계정 또는 도메인 계정.
설치 프로그램을 실행하는 계정에 대한 권한	시스템 권한: 로컬 관리자 권한.

중앙 관리 서버 서비스 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만.
	• 로컬 DBMS:
	  • 관리자가 선택한 Windows 계정.
	  • 설치 프로그램이 자동 생성하는 KL-AK-* 형식의 계정.

중앙 관리 서버 서비스 계정에 대한 권한	시스템 권한: 설치 프로그램이 할당한 필수 권한.
DBMS 내부 계정의 권한	스키마 권한: • 중앙 관리 서버 데이터베이스: ALL(GRANT OPTION 제외). • 시스템 구성표(mysql 및 sys): SELECT, SHOW VIEW. • sys.table_exists 저장 프로시저: EXECUTE(MariaDB 10.5 이하를 DBMS로 사용한다면 EXECUTE 권한을 부여할 필요가 없습니다). 모든 구성표에 대한 전역 권한: PROCESS, SUPER.

데이터를 공유 테이블스페이스에서 테이블당 파일 테이블스페이스로 이동하는 방법에 대한 자세한 내용은 MySQL 및 MariaDB DBMS에서 공유 테이블스페이스의 데이터를 테이블당 파일 테이블스페이스로 이동을 참조하십시오.

중앙 관리 서버 데이터 복구 권한 구성

내부 DBMS 계정에 부여한 권한은 백업에서 중앙 관리 서버 데이터를 복원하기에 충분합니다. 복원을 시작하려면 중앙 관리 서버를 설치하는 데 사용된 Windows 계정으로 klbackup 유틸리티를 실행하십시오.

PostgreSQL 또는 Postgres Pro

PostgreSQL 또는 Postgres Pro를 DBMS로 선택하면 *Postgres* 사용자(기본 Postgres 역할)를 사용하거나 새로운 Postgres 역할(이하 역할)을 생성하여 DBMS에 접근할 수 있습니다. 서버 데이터베이스의 생성 방법에 따라 아래 표에 설명된 대로 역할에 필요한 권한을 부여합니다. 계정 권한을 구성하는 방법에 대한 자세한 내용은 PostgreSQL 또는 Postgres Pro 작업을 위한 계정 구성을 참조하십시오.

DBMS: PostgreSQL 또는 Postgres Pro

	자동 데이터베이스 생성	수동 데이터베이스 생성
설치 프로그램을 실행하는 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만. • 로컬 DBMS: 로컬 관리자 계정 또는 도메인 계정.	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만. • 로컬 DBMS: 로컬 관리자 계정 또는 도메인 계정.
설치 프로그램을 실행하는 계정에 대한 권한	시스템 권한: 로컬 관리자 권한.	시스템 권한: 로컬 관리자 권한.

중앙 관리 서버 서비스 계정	• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만.
	• 로컬 DBMS:
	  • 관리자가 선택한 Windows 계정.
	  • 설치 프로그램이 자동 생성하는 KL-AK-* 형식의 계정.
		• 원격 DBMS: DBMS가 설치된 원격 기기의 도메인 계정만.
		• 로컬 DBMS:
		  • 관리자가 선택한 Windows 계정.
		  • 설치 프로그램이 자동 생성하는 KL-AK-* 형식의 계정.

중앙 관리 서버 서비스 계정에 대한 권한	시스템 권한: 설치 프로그램이 할당한 필수 권한.	시스템 권한: 설치 프로그램이 할당한 필수 권한.

Postgres 역할의 권한	*Postgres* 사용자는 추가 권한이 필요하지 않습니다.	새 역할에 대한 권한: `CREATEDB`.	새 역할: • 중앙 관리 서버 데이터베이스에 대한 권한: `ALL`. • 공용 스키마의 모든 테이블에 대한 권한: `ALL`. • 공용 스키마의 모든 시퀀스에 대한 권한: `ALL`.

중앙 관리 서버 데이터 복구 권한 구성

백업에서 중앙 관리 서버 데이터를 복원하려면, 중앙 관리 서버 설치에 사용된 Windows 계정으로 klbackup 유틸리티를 실행하십시오. DBMS에 액세스하는 데 사용되는 Postgres 역할에는 중앙 관리 서버 데이터베이스에 대한 소유자 권한이 있어야 합니다.

SQL Server 작업을 위한 계정 구성(Windows 인증)

필수 구성 요소

계정에 권한을 할당하기 전에 다음 작업을 수행하십시오:

1. 로컬 관리자 계정으로 시스템에 로그인했는지 확인하십시오.
2. SQL Server 작업을 위한 환경을 설치합니다.
3. 중앙 관리 서버를 설치할 Windows 계정이 있는지 확인하십시오.
4. 중앙 관리 서버 서비스를 시작할 Windows 계정이 있는지 확인하십시오.
5. SQL Server에서 중앙 관리 서버 설치 프로그램(이하 설치 프로그램)을 실행하는 데 사용되는 Windows 계정에 대한 아이디를 만듭니다. 또한 중앙 관리 서버 서비스를 시작하는 데 사용되는 Windows 계정에 대한 아이디를 만듭니다.

SQL Server Management Studio 사용 시, 로그인 속성 창의 **일반** 페이지에서 **Windows 인증** 옵션을 선택합니다

별도의 Windows 도메인에 있는 기기에 중앙 관리 서버와 SQL Server를 설치하려면 작업 실행 및 정책 적용을 포함하여 중앙 관리 서버의 올바른 작동을 보장하기 위해 이러한 도메인에 양방향 신뢰 관계가 있어야 합니다. 다양한 DBMS 작업에 필요한 계정 및 계정 권한에 대한 자세한 내용은 DBMS 작업을 위한 계정을 참조하십시오.

중앙 관리 서버를 설치하도록 계정 구성(중앙 관리 서버 데이터베이스 자동 생성)

중앙 관리 서버 설치를 위한 계정을 구성하려면:

1. SQL Server에서 설치 관리자를 실행하는 데 사용되는 Windows 계정의 아이디에 sysadmin 서버 레벨 역할을 할당합니다.
2. 설치 프로그램을 실행하는 데 사용된 Windows 계정으로 시스템에 로그인합니다.
3. 중앙 관리 서버 설치 프로그램을 실행합니다.

   중앙 관리 서버 설정 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

4. 중앙 관리 서버 사용자 지정 설치 옵션을 선택합니다.

5. 중앙 관리 서버 데이터베이스를 저장하는 DBMS로서의 Microsoft SQL Server를 선택합니다.

6. Windows 계정을 통해 중앙 관리 서버와 SQL Server 간의 연결을 설정하려면 Microsoft Windows 인증 모드를 선택하십시오.

7. 중앙 관리 서버 서비스를 시작하는 데 사용할 Windows 계정을 지정합니다.

   이전에 SQL Server 아이디를 생성한 Windows 사용자 계정을 선택할 수 있습니다. 또는 설치 프로그램을 사용하여 KL-AK-* 형식으로 새 Windows 계정을 자동 생성할 수 있습니다. 이때, 설치 관리자는 이 계정에 대한 SQL Server 로그인을 자동으로 생성합니다. 계정 선택과 관계없이 설치 프로그램은 필요한 시스템 권한과 SQL Server 권한을 중앙 관리 서버 서비스 계정에 할당합니다.

설치가 완료되면 서버 데이터베이스가 생성되고 필요한 모든 시스템 권한과 SQL Server 권한이 중앙 관리 서버 서비스 계정에 할당됩니다. 중앙 관리 서버를 사용할 준비가 되었습니다.

중앙 관리 서버를 설치하기 위한 계정 구성(중앙 관리 서버 데이터베이스 수동 생성)

중앙 관리 서버 설치를 위한 계정을 구성하려면:

1. SQL Server에서 빈 데이터베이스를 만듭니다. 이 데이터베이스는 중앙 관리 서버 데이터베이스(이하 서버 데이터베이스)로 사용됩니다.

2. Windows 계정에 대해 생성된 두 SQL Server 로그인에 대해 공용 서버 레벨 역할을 지정하고 생성된 데이터베이스에 대한 매핑을 구성합니다:

   - 서버 레벨 역할: public
   - 데이터베이스 역할 구성원: db_owner, public
   - 기본 스키마: dbo

3. 설치 프로그램을 실행하는 데 사용된 Windows 계정으로 시스템에 로그인합니다.

4. 중앙 관리 서버 설치 프로그램을 실행합니다.

   중앙 관리 서버 설정 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

5. 중앙 관리 서버 사용자 지정 설치 옵션을 선택합니다.

6. 중앙 관리 서버 데이터베이스를 저장하는 DBMS로서의 Microsoft SQL Server를 선택합니다.

7. 생성된 데이터베이스의 이름을 중앙 관리 서버 데이터베이스 이름으로 지정합니다.

8. Windows 계정을 통해 중앙 관리 서버와 SQL Server 간의 연결을 설정하려면 Microsoft Windows 인증 모드를 선택하십시오.

9. 중앙 관리 서버 서비스를 시작하는 데 사용할 Windows 계정을 지정합니다.

   이전에 SQL Server 아이디를 생성하고 로그인 권한을 구성한 Windows 사용자 계정을 선택할 수 있습니다.

KL-AK-* 형식으로 새 Windows 계정 자동 생성은 권장하지 않습니다. 이때, 설치 프로그램은 SQL Server 계정을 생성 및 구성하지 않은 새 Windows 계정을 만듭니다. 중앙 관리 서버는 이 계정을 사용하여 중앙 관리 서버 서비스를 시작할 수 없습니다. KL-AK-* Windows 계정을 만들어야 한다면, 설치 후 관리 콘솔을 시작하지 마십시오. 다음을 수행합니다:

1. kladminserver 서비스를 중지합니다.
2. SQL Server에서 생성한 L-AK-* Windows 계정에 대해 SQL Server 로그인을 생성합니다.
3. 이 SQL Server 로그인에 대한 권한을 부여하고 생성된 데이터베이스에 대한 매핑을 구성합니다:
   - 서버 레벨 역할: public
   - 데이터베이스 역할 구성원: db_owner, public
   - 기본 스키마: dbo
4. kladminserver 서비스를 다시 시작한 다음 관리 콘솔을 실행합니다.

설치가 완료되면 중앙 관리 서버는 생성된 데이터베이스를 사용하여 서버 데이터를 저장합니다. 중앙 관리 서버를 사용할 준비가 되었습니다.

SQL Server 작업을 위한 계정 구성(SQL Server 인증)

필수 구성 요소

계정에 권한을 할당하기 전에 다음 작업을 수행하십시오:

1. 로컬 관리자 계정으로 시스템에 로그인했는지 확인하십시오.
2. SQL Server 작업을 위한 환경을 설치합니다.
3. 중앙 관리 서버를 설치할 Windows 계정이 있는지 확인하십시오.
4. 중앙 관리 서버 서비스를 시작할 Windows 계정이 있는지 확인하십시오.
5. SQL Server에서 SQL Server 인증 모드를 활성화합니다.

   SQL Server Management Studio를 사용 시, SQL Server 속성 창의 **보안** 페이지에서 **SQL Server 및 Windows 인증 모드** 옵션을 선택합니다.
6. SQL Server에서 아이디와 암호를 생성합니다. 중앙 관리 서버 설치 프로그램(이하 설치 프로그램) 및 중앙 관리 서버 서비스는 이 SQL Server 계정을 사용하여 SQL Server에 액세스합니다.

   SQL Server Management Studio 사용 시, 로그인 속성 창의 **일반** 페이지에서 **SQL Server 인증** 옵션을 선택합니다.

별도의 Windows 도메인에 있는 기기에 중앙 관리 서버와 SQL Server를 설치하려면 작업 실행 및 정책 적용을 포함하여 중앙 관리 서버의 올바른 작동을 보장하기 위해 이러한 도메인에 양방향 신뢰 관계가 있어야 합니다. 다양한 DBMS 작업에 필요한 계정 및 계정 권한에 대한 자세한 내용은 DBMS 작업을 위한 계정을 참조하십시오.

중앙 관리 서버를 설치하도록 계정 구성(중앙 관리 서버 데이터베이스 자동 생성)

중앙 관리 서버 설치를 위한 계정을 구성하려면:

1. SQL Server에서 SQL Server 계정을 기본 *마스터* 데이터베이스에 매핑합니다. *마스터* 데이터베이스는 중앙 관리 서버 데이터베이스(이하 서버 데이터베이스)의 템플릿입니다. *마스터* 데이터베이스는 설치 프로그램이 서버 데이터베이스를 생성할 때까지 매핑에 사용됩니다. SQL Server 계정에 다음 권한을 부여합니다:
   - 서버 레벨 역할: public
   - *마스터* 데이터베이스의 데이터베이스 역할 구성원: db_owner
   - *마스터* 데이터베이스의 기본 스키마: dbo
   - 권한:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. 설치 프로그램을 실행하는 데 사용된 Windows 계정으로 시스템에 로그인합니다.
3. 설치 프로그램을 실행합니다.
   중앙 관리 서버 설정 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
4. 중앙 관리 서버 사용자 지정 설치 옵션을 선택합니다.
5. 중앙 관리 서버 데이터베이스를 저장하는 DBMS로서의 Microsoft SQL Server를 선택합니다.
6. 중앙 관리 서버 데이터베이스 이름을 지정합니다.
7. 생성된 SQL Server 계정을 통해 중앙 관리 서버와 SQL Server 간의 연결을 설정하려면 SQL Server 인증 모드를 선택합니다. 그런 다음 SQL Server 계정 자격 증명을 지정합니다.
8. 중앙 관리 서버 서비스를 시작하는 데 사용할 Windows 계정을 지정합니다.
   기존 Windows 사용자 계정을 선택하거나 설치 프로그램을 사용하여 KL-AK-* 형식으로 새 Windows 계정을 생성할 수 있습니다. 계정 선택과 관계없이 설치 프로그램은 필요한 시스템 권한을 중앙 관리 서버 서비스 계정에 할당합니다.

설치가 완료되면 서버 데이터베이스가 생성되고 필요한 모든 시스템 권한이 중앙 관리 서버 서비스 계정에 할당됩니다. 중앙 관리 서버를 사용할 준비가 되었습니다.

중앙 관리 서버 설치 시 설치 프로그램이 서버 데이터베이스를 만들고 이 데이터베이스에 대한 매핑을 구성했으므로 *마스터* 데이터베이스에 대한 매핑을 취소할 수 있습니다.

자동 데이터베이스 생성에는 일반 중앙 관리 서버 작업보다 더 많은 권한이 필요하므로 일부 권한을 취소할 수 있습니다. SQL Server에서 SQL Server 계정을 선택하고 중앙 관리 서버 작업을 위해 다음 권한을 부여합니다:

- 서버 레벨 역할: public
- 서버 데이터베이스의 데이터베이스 역할 구성원: db_owner

- 서버 데이터베이스의 기본 스키마: dbo
- 권한:
  - CONNECT SQL
  - VIEW ANY DATABASE

중앙 관리 서버를 설치하기 위한 계정 구성(중앙 관리 서버 데이터베이스 수동 생성)

중앙 관리 서버 설치를 위한 계정을 구성하려면:

1. SQL Server에서 빈 데이터베이스를 만듭니다. 이 데이터베이스는 중앙 관리 서버 데이터베이스로 사용됩니다.
2. SQL Server에서 SQL Server 계정에 다음 권한을 부여합니다:
   - 서버 레벨 역할: public.
   - 생성한 데이터베이스의 데이터베이스 역할 구성원: db_owner.
   - 생성한 데이터베이스의 기본 스키마: dbo.
   - 권한:
     - CONNECT SQL
     - VIEW ANY DATABASE
3. 설치 프로그램을 실행하는 데 사용된 Windows 계정으로 시스템에 로그인합니다.
4. 설치 프로그램을 실행합니다.
   중앙 관리 서버 설정 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
5. 중앙 관리 서버 사용자 지정 설치 옵션을 선택합니다.
6. 중앙 관리 서버 데이터베이스를 저장하는 DBMS로서의 Microsoft SQL Server를 선택합니다.
7. 생성된 데이터베이스의 이름을 중앙 관리 서버 데이터베이스 이름으로 지정합니다.
8. 생성된 SQL Server 계정을 통해 중앙 관리 서버와 SQL Server 간의 연결을 설정하려면 SQL Server 인증 모드를 선택합니다. 그런 다음 SQL Server 계정 자격 증명을 지정합니다.
9. 중앙 관리 서버 서비스를 시작하는 데 사용할 Windows 계정을 지정합니다.
   기존 Windows 사용자 계정을 선택하거나 설치 프로그램을 사용하여 KL-AK-* 형식으로 새 Windows 계정을 생성할 수 있습니다. 계정 선택과 관계없이 설치 프로그램은 필요한 시스템 권한을 중앙 관리 서버 서비스 계정에 할당합니다.

설치가 완료되면 중앙 관리 서버는 생성된 데이터베이스를 사용하여 중앙 관리 서버 데이터를 저장합니다. 필요한 모든 시스템 권한이 중앙 관리 서버 서비스 계정에 할당됩니다. 중앙 관리 서버를 사용할 준비가 되었습니다.

MySQL 및 MariaDB 작업을 위한 계정 구성

필수 구성 요소

계정에 권한을 할당하기 전에 다음 작업을 수행하십시오:

1. 로컬 관리자 계정으로 시스템에 로그인했는지 확인하십시오.
2. MySQL 또는 MariaDB 작업을 위한 환경을 설치합니다.
3. 중앙 관리 서버를 설치할 Windows 계정이 있는지 확인하십시오.
4. 중앙 관리 서버 서비스를 시작할 Windows 계정이 있는지 확인하십시오.

중앙 관리 서버 설치에 대한 계정 구성

중앙 관리 서버 설치를 위한 계정을 구성하려면:

1. DBMS 설치 시 생성한 루트 계정으로 MySQL 또는 MariaDB 작업용 환경을 실행합니다.
2. 암호로 내부 DBMS 계정을 생성합니다. 중앙 관리 서버 설치 프로그램(이하 설치 프로그램) 및 중앙 관리 서버 서비스는 이 내부 DBMS 계정을 사용하여 DBMS에 액세스합니다. 이 계정에 다음 권한을 부여합니다:
   - 스키마 권한:
     - 중앙 관리 서버 데이터베이스: ALL(`GRANT OPTION` 제외)
     - 시스템 구성표(mysql 및 sys): `SELECT`, `SHOW VIEW`
     - sys.table_exists 저장 프로시저: `EXECUTE`
   - 모든 구성표에 대한 전역 권한: `PROCESS`, `SUPER`

   내부 DBMS 계정을 만들고 이 계정에 필요한 권한을 부여하려면 아래 스크립트를 실행합니다(이 스크립트에서 DBMS 로그인은 *KSCAdmin*이고 중앙 관리 서버 데이터베이스 이름은 *kav*입니다):

   ```
   /* KSCAdmin이라는 사용자 생성 */
   CREATE USER 'KSCAdmin'
   /* KSCAdmin의 암호 지정 */
   IDENTIFIED BY '<암호>';
   ```

   MySQL 8.0 이하를 DBMS로 사용 시, 해당 버전에서는 "Caching SHA2 암호" 인증을 지원하지 않습니다. 기본 인증을 "Caching SHA2 암호"에서 "MySQL 기본 암호"로 변경합니다.

   - "MySQL 기본 암호" 인증을 사용하는 DBMS 계정을 생성하려면 다음 명령을 실행합니다.

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<암호>';
     ```

   - 기존 DBMS 계정에 대한 인증을 변경하려면 다음 명령을 실행합니다.

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<암호>';
     ```

```
/* KSCAdmin에 권한 부여 */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

> MariaDB 10.5 이하를 DBMS로 사용 시, EXECUTE 권한을 부여할 필요가 없습니다. 이때는 스크립트에서 `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'` 명령을 제외합니다.

3. DBMS 계정에 부여된 권한 목록을 보려면 다음 스크립트를 실행합니다:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. 중앙 관리 서버 데이터베이스를 수동으로 만들려면 다음 스크립트를 실행합니다(이 스크립트에서 중앙 관리 서버 데이터베이스 이름은 *kav*입니다):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   DBMS 계정을 생성하는 스크립트에서 지정한 것과 같은 데이터베이스 이름을 사용합니다.

5. 설치 프로그램을 실행하는 데 사용된 Windows 계정으로 시스템에 로그인합니다.

6. 설치 프로그램을 실행합니다.

   중앙 관리 서버 설정 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

7. 중앙 관리 서버 사용자 지정 설치 옵션을 선택합니다.

8. 중앙 관리 서버 데이터베이스를 저장하는 DBMS로 MySQL 또는 MariaDB를 선택합니다.

9. 중앙 관리 서버 데이터베이스 이름을 지정합니다. 스크립트에서 지정하는 것과 같은 데이터베이스 이름을 사용합니다.

10. 스크립트로 생성한 DBMS 계정의 자격 증명을 지정합니다.

11. 중앙 관리 서버 서비스를 시작하는 데 사용할 Windows 계정을 지정합니다.

    기존 Windows 사용자 계정을 선택하거나 설치 프로그램을 사용하여 KL-AK-* 형식으로 새 Windows 계정을 자동 생성할 수 있습니다. 계정 선택과 관계없이 설치 프로그램은 필요한 시스템 권한을 중앙 관리 서버 서비스 계정에 할당합니다.

설치가 완료되면 중앙 관리 서버 데이터베이스가 생성되고 중앙 관리 서버를 사용할 수 있습니다.

MySQL 또는 MariaDB DBMS에서 공유 테이블스페이스의 데이터를 테이블당 파일 테이블스페이스로 이동

MySQL 및 MariaDB DBMS에서는 다음 방법에 따라 데이터를 저장할 수 있습니다.

- 모든 사용자 데이터베이스의 데이터가 단일 파일(보통 `ibdata1` 파일에)에 저장될 경우 공유 테이블스페이스로 저장합니다.
- 각 테이블에 대해 별도의 데이터 공간이 별도의 파일로 생성될 경우 테이블당 파일 테이블스페이스로 저장합니다.

공유 테이블 공간을 사용하면 테이블스페이스 조각화 위험이 증가합니다. `SHRINK` 작업은 수행할 수 없으므로 공유 테이블스페이스에 있는 파일이 디스크 공간의 최대 90% 정도를 차지할 수 있습니다. 이는 디스크 하위 시스템 성능에 부정적인 영향을 미칩니다. 따라서 테이블당 파일 테이블스페이스를 선택하는 것이 좋습니다.

이 문서에서는 공유 테이블스페이스에서 테이블당 파일 테이블스페이스로 데이터를 이동하는 방법을 설명합니다. 다른 애플리케이션에서도 MySQL 또는 MariaDB DBMS를 사용할 경우, 해당 애플리케이션의 데이터베이스를 테이블당 파일 테이블스페이스로 옮겨야 합니다.

> 중앙 관리 서버용 MySQL 또는 MariaDB DBMS를 사용하는 경우에만 이 절차를 수행하는 것이 좋습니다. 공유 테이블스페이스에서 테이블당 파일 테이블스페이스로 데이터를 옮기면 디스크 하위 시스템의 부하가 증가할 수 있습니다.

필수 구성 요소

시작하기 전에 다음을 확인하십시오.

- 데이터 백업 작업 또는 klbackup 유틸리티를 실행하여 중앙 관리 서버 데이터의 백업 복사본을 생성했습니다.
- MySQL 또는 MariaDB DBMS로 관리되는 데이터베이스(있을 경우)가 있는 다른 애플리케이션의 백업 복사본을 생성했습니다.
- DBMS가 설치된 기기에서 데이터베이스가 있는 파티션에 디스크 여유 공간이 있습니다.

필요한 디스크 공간은 현재 총 데이터베이스 크기(`ibdata1` 파일의 현재 크기)의 150%입니다.

프로세스

다음 방법에 따라 공유 테이블스페이스에서 테이블당 파일 테이블스페이스로 데이터를 옮길 수 있습니다.

1. Kaspersky Security Center 중앙 관리 서버 서비스 및 이 절차를 수행할 DBMS 인스턴스를 사용하는 기타 애플리케이션을 중지합니다.
2. DBMS 버전에 따라 DBMS에 수퍼유저로 로그인한 다음, 원하는 애플리케이션에서 `fix_tablespace.sql` 스크립트를 실행합니다.

   다음 링크를 클릭하여 `fix_tablespace.sql` 스크립트를 볼 수 있습니다.

MySQL 5.7 및 MariaDB 10.1 이상을 위한 스크립트 보기

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

MySQL 8.0 이상을 위한 스크립트 보기

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

스크립트 실행을 중지하면 안 됩니다.
DBMS 오류가 발생하지 않았지만 스크립트 실행을 종료한 경우 스크립트를 다시 실행하거나 이 절차의 단계 수행을 멈춘 다음, DBMS 서비스를 다시 시작하고 백업에서 중앙 관리 서버 데이터를 복원합니다.

3. my.cnf 파일의 `[mysqld]` 섹션에서 `innodb_file_per_table` 파라미터를 `1`로 설정합니다.
4. MySQL 또는 MariaDB 서비스를 재개합니다.
5. Kaspersky Security Center 중앙 관리 서버 서비스를 시작합니다.

데이터가 공유 테이블스페이스에서 테이블당 파일 테이블스페이스로 옮겨집니다.

PostgreSQL 및 Postgres Pro 작업을 위한 계정 구성

필수 구성 요소

계정에 권한을 할당하기 전에 다음 작업을 수행하십시오:

1. 로컬 관리자 계정으로 시스템에 로그인했는지 확인하십시오.
2. PostgreSQL 및 Postgres Pro 작업을 위한 환경을 설치합니다.
3. Kaspersky Security Center 15.1 사용을 위한 PostgreSQL 또는 Postgres Pro 구성.
4. 중앙 관리 서버를 설치할 Windows 계정이 있는지 확인하십시오.
5. 중앙 관리 서버 서비스를 시작할 Windows 계정이 있는지 확인하십시오.

중앙 관리 서버를 설치하도록 계정 구성(중앙 관리 서버 데이터베이스 자동 생성)

중앙 관리 서버 설치를 위한 계정을 구성하려면:

1. PostgreSQL 및 Postgres Pro 작업을 위한 환경을 실행합니다.
2. DBMS에 액세스하려면 Postgres 역할을 선택합니다. 다음 역할 중 하나를 사용할 수 있습니다:

   - *Postgres* 사용자(기본 Postgres 역할).

     Postgres 사용자를 사용 시, 추가 권한을 부여할 필요가 없습니다.

   - 새로운 Postgres 역할.

     새 Postgres 역할을 사용하려면 이 역할을 생성하고 CREATEDB 권한을 부여합니다. 이렇게 하려면 다음 스크립트를 실행합니다(이 스크립트에서 역할은 *KSCAdmin*입니다):

     `CREATE USER "KSCAdmin" WITH PASSWORD '<암호>' CREATEDB;`

     생성된 역할은 중앙 관리 서버 데이터베이스(이하 서버 데이터베이스)의 소유자로 사용됩니다.

3. 중앙 관리 서버 설치 프로그램(이하 설치 프로그램)을 실행하는 데 사용되는 Windows 계정으로 시스템에 로그인합니다.

4. 설치 프로그램을 실행합니다.
   중앙 관리 서버 설정 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

5. 중앙 관리 서버 사용자 지정 설치 옵션을 선택합니다.

6. 중앙 관리 서버 데이터베이스를 저장하는 DBMS로 PostgreSQL 또는 Postgres Pro를 선택합니다.

7. 서버 데이터베이스 이름을 지정합니다. 설치 프로그램이 서버 데이터베이스를 자동 생성합니다.

8. Postgres 역할의 자격 증명을 지정합니다.

9. 중앙 관리 서버 서비스를 시작하는 데 사용할 Windows 계정을 지정합니다.
   기존 Windows 사용자 계정을 선택하거나 설치 프로그램을 사용하여 KL-AK-* 형식으로 새 Windows 계정을 자동 생성할 수 있습니다. 계정 선택과 관계없이 설치 프로그램은 필요한 시스템 권한을 중앙 관리 서버 서비스 계정에 할당합니다.

설치가 완료되면 서버 데이터베이스가 자동 생성되고 중앙 관리 서버를 사용할 수 있습니다.

중앙 관리 서버를 설치하기 위한 계정 구성(중앙 관리 서버 데이터베이스 수동 생성)

중앙 관리 서버 설치를 위한 계정을 구성하려면:

1. Postgres 작업을 위한 환경을 실행합니다.

2. *Postgres* 데이터베이스에서 *Postgres* 사용자로 로그인합니다.

3. 새 Postgres 역할(이 예에서의 역할: *KSCAdmin*)을 만듭니다.

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '< 암호 >';
   ```

4. 중앙 관리 서버(이 예에서의 중앙 관리 서버 데이터베이스 이름: *KAV*)을 만듭니다.

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   > "새 인코딩(UTF8)이 템플릿 데이터베이스의 인코딩과 호환되지 않습니다." 오류가 발생하면 다음 명령을 사용하여 데이터베이스를 생성합니다.
   > ```
   > CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;
   > ```
   > 대신에
   > ```
   > CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   > ```

5. 중앙 관리 서버 데이터베이스의 역할에 모든 권한을 부여합니다.

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   > 역할에 중앙 관리 서버 데이터베이스에 대한 기본 CONNECT 및 TEMPORARY 권한이 있는지 확인해야 합니다.

6. 생성한 Postgres 역할에 다음 권한을 부여합니다:

   - 공용 스키마의 모든 테이블에 대한 권한: ALL
   - 공용 스키마의 모든 시퀀스에 대한 권한: ALL

이렇게 하려면 서버 데이터베이스의 *Postgres* 사용자로 로그인하고 다음 스크립트를 실행합니다(이 스크립트에서 역할은 *KSCAdmin*입니다):

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
```

7. 설치 프로그램을 실행하는 데 사용된 Windows 계정으로 시스템에 로그인합니다.
8. 중앙 관리 서버 설치 프로그램을 실행합니다.

   중앙 관리 서버 설정 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
9. 중앙 관리 서버 사용자 지정 설치 옵션을 선택합니다.
10. 중앙 관리 서버 데이터베이스를 저장하는 DBMS로 PostgreSQL 또는 Postgres Pro를 선택합니다.
11. 서버 데이터베이스 이름을 지정합니다. 스크립트에서 지정하는 것과 같은 데이터베이스 이름을 사용합니다. 데이터베이스 이름은 대소문자를 구분합니다.
12. Postgres 역할의 자격 증명을 지정합니다.
13. 중앙 관리 서버 서비스를 시작하는 데 사용할 Windows 계정을 지정합니다.

    기존 Windows 사용자 계정을 선택하거나 설치 프로그램을 사용하여 KL-AK-* 형식으로 새 Windows 계정을 자동 생성할 수 있습니다. 계정 선택과 관계없이 설치 프로그램은 필요한 시스템 권한을 중앙 관리 서버 서비스 계정에 할당합니다.

설치가 완료되면 중앙 관리 서버는 생성된 데이터베이스를 사용하여 중앙 관리 서버 데이터를 저장합니다. 중앙 관리 서버를 사용할 준비가 되었습니다.

시나리오: Microsoft SQL Server 인증

이 섹션의 정보는 Kaspersky Security Center uses 데이터베이스 관리 시스템으로 Microsoft SQL Server를 사용하는 Kaspersky Security Center의 구성에만 적용됩니다.

데이터베이스에서 또는 데이터베이스로 전송된 Kaspersky Security Center 데이터와 데이터베이스에 저장된 데이터를 무단 액세스로부터 보호하려면 Kaspersky Security Center와 SQL Server 사이의 통신에 보안을 적용해야 합니다. 안전한 통신을 제공하는 가장 안정적인 방법은 동일한 기기에 Kaspersky Security Center와 SQL Server를 설치하고 두 애플리케이션에 공유 메모리 메커니즘을 사용하는 것입니다. 다른 모든 경우에는 SSL 또는 TLS 인증서를 사용하여 SQL Server 인스턴스를 인증하는 것이 좋습니다. 신뢰할 수 있는 인증 기관(CA)의 인증서 또는 자체 서명 인증서를 사용할 수 있습니다. 자체 서명 인증서의 보호는 제한적이므로 신뢰할 수 있는 CA의 인증서를 사용하는 것이 좋습니다.

SQL Server 인증은 다음 단계로 진행됩니다.

1. **인증서 요구사항에 따라 SQL Server에 대한 자체 서명 SSL 또는 TLS 인증서 생성하기**

   SQL Server용 인증서가 이미 있는 경우 이 단계를 건너뜁니다.

   SSL 인증서는 2016 (13.x) 이전의 SQL Server 버전에만 적용됩니다. SQL Server 2016 (13.x) 이후 버전에는 TLS 인증서를 사용합니다.

   예를 들어, TLS 인증서를 생성하려면 PowerShell에 다음 명령을 입력하십시오.

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

명령에서 호스트가 도메인에 포함된 경우 SQL Server 호스트 이름을, 호스트가 도메인에 포함되지 않은 경우는 도메인의 *전체 주소 도메인 이름*(FQDN)을 SQL_HOST_NAME 대신 입력합니다. 같은 이름(호스트 이름 또는 FQDN)을 중앙 관리 서버 설치 마법사의 SQL Server 인스턴스 이름으로 지정해야 합니다.

2. **SQL Server 인스턴스에서 인증서 추가**

   이 단계의 지침은 SQL Server가 실행 중인 플랫폼에 따라 다릅니다. 자세한 내용은 공식 문서를 참조하십시오.

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   Failover 클러스터에서 인증서를 사용하려면 Failover 클러스터의 각 노드에 인증서를 설치해야 합니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.

3. **서비스 계정 권한 할당**

   SQL Server 서비스가 실행되는 서비스 계정에 비공개 키에 액세스할 수 있는 완전한 제어 권한이 있는지 확인하십시오. 자세한 내용은 Microsoft 설명서를 참조하십시오.

4. **Kaspersky Security Center의 신뢰할 수 있는 인증서 목록에 인증서 추가**

   중앙 관리 서버 기기에서 신뢰할 수 있는 인증서 목록에 인증서를 추가합니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.

5. **SQL Server 인스턴스와 Kaspersky Security Center 사이의 암호화된 연결 활성화**

   중앙 관리 서버 기기에서 `1` 값을 환경 변수 `KLDBADO_UseEncryption`으로 설정합니다. 예를 들어, Windows Server 2012 R2의 경우, **시스템 속성** 창의 **고급** 탭에서 **환경 변수**를 눌러 환경 변수를 변경할 수 있습니다. 새 변수를 추가하고 `KLDBADO_UseEncryption`으로 이름을 지정한 다음 `1` 값을 설정합니다.

6. **TLS 1.2 프로토콜 사용을 위한 추가 구성**

   TLS 1.2 프로토콜을 사용하는 경우, 추가로 다음을 수행합니다.

   - 설치된 SQL Server 버전이 64비트 애플리케이션인지 확인합니다.
   - 중앙 관리 서버에서 Microsoft OLE DB 드라이버를 설치합니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.
   - 중앙 관리 서버 기기에서 `1` 값을 환경 변수 `KLDBADO_UseMSOLEDBSQL`로 설정합니다. 예를 들어, Windows Server 2012 R2의 경우, **시스템 속성** 창의 **고급** 탭에서 **환경 변수**를 눌러 환경 변수를 변경할 수 있습니다. 새 변수를 추가하고 `KLDBADO_UseMSOLEDBSQL`로 이름을 지정한 다음 `1` 값을 설정합니다.

     OLE DB 드라이버 버전이 19 이상일 시, 값 `MSOLEDBSQL19`도 환경 변수 `KLDBADO_ProviderName`으로 설정합니다.

7. **이름이 지정된 SQL Server의 인스턴스에서 TCP/IP 프로토콜 사용 활성화**

   이름이 지정된 SQL Server 인스턴스를 사용할 경우 추가적으로 TCP/IP 프로토콜의 사용을 활성화하고 SQL Server 데이터베이스 엔진에 TCP/IP 포트 번호를 할당합니다. 중앙 관리 서버 설치 마법사에서 SQL Server 연결 구성 시, **SQL Server 인스턴스 이름** 필드에서 SQL Server 호스트 이름과 포트 번호를 지정합니다.

시나리오: MySQL 서버 인증

MySQL 서버를 인증하려면 TLS 인증서를 사용할 것을 권장합니다. 신뢰할 수 있는 인증 기관(CA)의 인증서 또는 자체 서명 인증서를 사용할 수 있습니다.

중앙 관리 서버는 MySQL에 대해 단방향 및 양방향 SSL 인증을 모두 지원합니다.

단방향 SSL 인증 활성화

MySQL에 대한 단방향 SSL 인증을 구성하려면 다음 단계를 따릅니다.

1 MySQL 서버에 대한 자체 서명 TLS 인증서 생성

PowerShell에서 인증서를 저장할 폴더로 디렉터리를 변경합니다. 다음 명령을 실행합니다.

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

이 명령은 현재 사용자의 인증서를 만들고 인증서를 PEM 형식으로 내보냅니다. 서버를 인증할 때는 내보낸 PEM 파일만 있으면 됩니다. Windows에서 생성한 인증서를 제거하려면 PowerShell에서 다음 명령을 실행합니다:

```
certmgr.msc
```

개인 → **인증서** 폴더에서 생성된 인증서를 찾아 삭제합니다.

2 서버 플래그 파일을 생성합니다

관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

klscflag 유틸리티를 사용하여 KLSRV_MYSQL_OPT_SSL_CA 서버 플래그를 생성하고 인증서의 경로를 값으로 지정합니다.

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <ca-cert.pem 경로> -t s
```

3. **데이터베이스를 구성합니다**

my.cnf 파일에 인증서를 지정합니다. 텍스트 편집기에서 my.cnf 파일을 열고 [mysqld] 섹션에 다음 줄을 추가합니다.

```
[mysqld]

ssl-ca="...\mysqlcerts\ca-cert.pem"

ssl-cert="...\mysqlcerts\server-cert.pem"

ssl-key="...\mysqlcerts\server-key.pem"
```

양방향 SSL 인증 활성화

MySQL에 대한 양방향 SSL 인증을 구성하려면 다음 단계를 따릅니다.

1. **서버 플래그 파일을 생성합니다**

관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

klscflag 유틸리티를 사용하여 서버 플래그를 생성하고 인증서 파일의 경로를 값으로 지정합니다.

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <경로 ca-cert.pem> -t s

klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <경로 server-cert.pem> -t s

klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <경로 server-key.pem> -t s
```

2. **암호를 지정합니다(선택사항)**

server-key.pem에 암호가 필요한 경우 KLSRV_MARIADB_OPT_TLS_PASPHRASE 플래그를 생성하고 암호를 값으로 지정합니다.

```
klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <암호> -t s
```

3. **데이터베이스를 구성합니다**

my.cnf 파일에 인증서를 지정합니다. 텍스트 편집기에서 my.cnf 파일을 열고 [mysqld] 섹션에 다음 줄을 추가합니다.

```
[mysqld]

ssl-ca="...\ca-cert.pem"

ssl-cert="...\server-cert.pem"

ssl-key="...\server-key.pem"
```

시나리오: PostgreSQL 서버 인증

PostgreSQL 서버를 인증하려면 TLS 인증서를 사용할 것을 권장합니다. 신뢰할 수 있는 인증 기관(CA)의 인증서 또는 자체 서명 인증서를 사용할 수 있습니다. 자체 서명 인증서의 보호는 제한적이므로 신뢰할 수 있는 CA의 인증서를 사용하십시오.

중앙 관리 서버는 PostgreSQL에 대해 단방향 및 양방향 SSL 인증을 모두 지원합니다.

PostgreSQL 서버 인증은 다음과 같은 단계로 진행됩니다.

1. **PostgreSQL 서버에 대한 인증서 생성**

   OpenSSL 기반 교차 플랫폼 유틸리티에서 다음 명령을 실행합니다.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **중앙 관리 서버에 대한 인증서 생성**

   다음 명령을 실행합니다. CN 값은 중앙 관리 서버를 대신하여 PostgreSQL에 연결하는 사용자의 이름과 일치해야 합니다. 사용자 이름은 기본적으로 postgres로 설정됩니다.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **클라이언트 인증서 인증 구성**

   pg_hba.conf를 다음과 같이 수정합니다:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   pg_hba.conf에 `host`로 시작하는 레코드가 포함되어 있지 않은지 확인합니다.

4. **PostgreSQL 인증서 지정**

   단방향 SSL 인증

   postgresql.conf를 다음과 같이 수정합니다(.crt 및 .key 파일에 대한 올바른 경로 지정).

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   양방향 SSL 인증

   postgresql.conf를 다음과 같이 수정합니다(.crt 및 .key 파일에 대한 올바른 경로 지정).

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_ca_file = '<postgres.crt>'
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

5. **PostgreSQL 데몬 다시 시작**

   다음 명령을 실행합니다:

   ```
   systemctl restart postgresql-14.service
   ```

6. **중앙 관리 서버에 대한 서버 플래그 지정**

단방향 SSL 인증

klscflag 유틸리티를 사용하여 KLSRV_POSTGRES_OPT_SSL_CA 서버 플래그를 생성하고 인증서의 경로를 값으로 지정합니다.

관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

다음 명령을 실행합니다:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt 경로> -t s
```

양방향 SSL 인증

klscflag 유틸리티를 사용하여 서버 플래그를 생성하고 인증서 파일의 경로를 값으로 지정합니다.

관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

다음 명령을 실행합니다.

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <psql.crt 경로> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <postgres.crt 경로> -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <postgres.key 경로> -t s
```

postgres.key에 암호가 필요한 경우 KLSRV_POSTGRES_OPT_TLS_PASPHRASE 플래그를 생성하고 암호를 값으로 지정합니다.

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <암호> -t s
```

7. **중앙 관리 서버 서비스 다시 시작**

중앙 관리 서버 설치 권장 사항

이 섹션에서는 중앙 관리 서버를 설치하는 권장 방법을 설명합니다. 또한 클라이언트 기기에서 네트워크 에이전트를 배포하기 위해 중앙 관리 서버 기기에서 공유 폴더를 사용하는 경우에 대해서도 설명합니다.

Failover 클러스터에 중앙 관리 서버 서비스용 계정 생성

기본적으로 설치 관리자는 중앙 관리 서버 서비스용으로 권한이 없는 계정을 자동으로 만듭니다. 이 동작은 일반 기기에 중앙 관리 서버를 설치할 때 활용하면 가장 편리합니다.

그러나 Failover 클러스터에 중앙 관리 서버를 설치하려면 다른 방법을 사용해야 합니다:

1. 중앙 관리 서버 서비스용으로 권한이 없는 도메인 계정을 만든 다음 KLAdmins 도메인 보안 그룹의 구성원으로 지정.
2. 중앙 관리 서버 설치 프로그램에 이 서비스를 위해 생성한 도메인 계정을 지정합니다.

공유 폴더 정의

중앙 관리 서버를 설치할 때는 공유 폴더의 위치를 지정할 수 있습니다. 설치 후에 중앙 관리 서버 속성에서 공유 폴더 위치를 지정할 수도 있습니다. 기본적으로 공유 폴더는 중앙 관리 서버가 설치된 기기에 만들어지며 **모든 사용자** 하위 그룹에 대한 읽기 권한을 포함합니다. 하지만 부하가 많거나 격리된 네트워크에서 접근해야 하는 등의 몇 가지 경우에는 전용 파일 리소스에 공유 폴더를 배치하면 유용합니다.

공유 폴더는 네트워크 에이전트 배포에서도 경우에 따라 사용됩니다.

> 공유 폴더에 대한 대/소문자 구분을 비활성화해야 합니다.

Active Directory 그룹 정책을 통해 중앙 관리 서버 도구를 사용하여 원격 설치

작업 그룹이 없는 Windows 도메인 내에 대상 기기가 있는 경우에는 Active Directory 그룹 정책을 통해 초기 배포(아직 관리되고 있지 않은 기기에 네트워크 에이전트 및 보안 제품 설치)를 수행해야 합니다. Kaspersky Security Center 원격 설치용 표준 작업을 사용하여 배포를 수행합니다. 네트워크의 규모가 큰 경우에는 중앙 관리 서버 기기의 디스크 하위 시스템에 대한 부하를 줄이기 위해 전용 파일 리소스에 공유 폴더를 배치하는 것이 유용합니다.

독립 실행형 패키지에 대한 UNC 경로를 전달하여 원격 설치

조직의 네트워크에 연결된 기기 사용자에게 로컬 관리자 권한이 있는 경우 사용할 수 있는 다른 초기 배포 방법은 독립 실행형 네트워크 에이전트를 만드는 것입니다. 또는 보안 제품과 "결합"된 네트워크 에이전트 패키지를 만들 수도 있습니다. 독립 실행형 패키지를 만든 후 공유 폴더에 저장된 해당 패키지의 링크를 사용자에게 전송합니다. 사용자가 링크를 클릭하면 설치가 시작됩니다.

중앙 관리 서버 공유 폴더에서 업데이트

안티 바이러스 업데이트 작업에서는 중앙 관리 서버의 공유 폴더에서 업데이트를 수행하도록 구성할 수 있습니다. 많은 수의 기기에 작업이 할당된 경우에는 전용 파일 리소스에 공유 폴더를 배치하면 유용합니다.

운영 체제 이미지 설치

운영 체제 이미지는 항상 공유 폴더를 통해 설치됩니다: 기기는 공유 폴더에서 운영 체제 이미지를 읽습니다. 많은 수의 조직 소유 기기에 대해 이미지 배포를 계획한 경우에는 전용 파일 리소스에 공유 폴더를 배치하면 유용합니다.

중앙 관리 서버 주소 지정

중앙 관리 서버를 설치할 때는 중앙 관리 서버의 주소를 지정할 수 있습니다. 이 주소는 네트워크 에이전트 설치 패키지를 만들 때 기본 주소로 사용됩니다.

중앙 관리 서버 주소로 다음을 지정할 수 있습니다.

- 중앙 관리 서버 기기의 NetBIOS 이름(기본적으로 이것으로 지정됨)
- 조직 네트워크에서 Domain Name System(DNS)이 구성되었으며 정상적으로 작동하는 경우에는 중앙 관리 서버 기기의 전체 주소 도메인 이름(FQDN)
- 중앙 관리 서버가 DMZ(완충 지역)에 설치된 경우에는 외부 주소

그리고 나면 관리 콘솔 도구를 사용하여 중앙 관리 서버의 주소를 변경할 수 있습니다. 이미 만들어진 네트워크 에이전트 설치 패키지에서는 주소가 자동으로 변경되지 않습니다.

표준 설치

표준 설치는 중앙 관리 서버 설치로, 애플리케이션 파일의 기본 경로를 사용하고 기본 플러그인 세트를 설치하며 모바일 기기 관리는 활성화하지 않습니다.

로컬 기기에 Kaspersky Security Center 중앙 관리 서버를 설치하려면 다음과 같이 하십시오:

ksc_<version number>.<build number>_full_<localization language>.exe 실행 파일을 실행합니다.

설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다. 애플리케이션 선택 창에서 **Kaspersky Security Center 중앙 관리 서버 설치** 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

1단계. 라이센스 계약서 및 개인정보취급방침 검토

설치 마법사의 이 단계에서, 사용자와 Kaspersky 사이에 적용되는 라이센스 계약서 및 개인 정보 취급 방침을 읽어보아야 합니다.

또한 Kaspersky Security Center 배포 키트에 포함된 애플리케이션 관리 플러그인에 대한 라이센스 계약서 및 개인정보취급방침을 확인하는 창이 표시될 수 있습니다.

라이센스 계약서 및 개인정보취급방침을 주의 깊게 읽어 주십시오. 라이센스 계약서 및 개인 정보 취급 방침의 모든 조건에 동의한다면, 적절한 확인란을 선택하여 확인하십시오.

두 개의 확인란을 모두 선택한 이후 기기에 애플리케이션을 계속 설치할 수 있습니다.

라이센스 계약서 또는 개인정보취급방침에 동의하지 않을 경우 **취소** 버튼을 눌러 애플리케이션 설치를 취소하십시오.

2단계. 설치 방법 선택

설치 유형 선택 창에서 **표준**을 선택합니다.

기업 네트워크 내의 소규모 영역에서 작동 방식을 테스트하는 등 Kaspersky Security Center를 시험적으로 사용해 보려는 경우 표준 설치를 선택하는 것이 좋습니다. 표준 설치 시에는 데이터베이스만 구성합니다. 중앙 관리 서버 설정은 지정하지 않으며, 개별 설정의 기본값이 사용됩니다. 표준 설치에서는 설치할 관리 플러그인을 선택할 수 없으며 기본 플러그인 세트만 설치됩니다. 표준 설치 중에는 모바일 기기용 설치 패키지가 만들어지지 않습니다. 하지만 나중에 관리 콘솔에서 이를 만들 수 있습니다.

3단계. Kaspersky Security Center 웹 콘솔 설치

이 단계는 64비트 운영 체제를 사용 중인 경우에만 표시됩니다. 그렇지 않으면, 32비트 운영 체제에서 Kaspersky Security Center 웹 콘솔이 작동하지 않아 이 단계가 표시되지 않습니다.

기본적으로 Kaspersky Security Center 웹 콘솔과 MMC 기반 관리 콘솔이 모두 설치됩니다.

Kaspersky Security Center 웹 콘솔만 설치하려면:

1. **다음 하나만 설치**를 선택합니다.
2. 드롭다운 목록에서 **웹 기반 콘솔**을 선택합니다.

Kaspersky Security Center 웹 콘솔 설치는 중앙 관리 서버 설치 완료 후 자동으로 시작됩니다.

MMC 기반 관리 콘솔만 설치하려면:

1. **다음 하나만 설치**를 선택합니다.
2. 드롭다운 목록에서 **MMC 기반 콘솔**을 선택합니다.

4단계. 네트워크 크기 선택

Kaspersky Security Center를 설치할 네트워크의 규모를 지정합니다. 마법사는 네트워크에 구성된 기기 수에 따라 애플리케이션 인터페이스 모양과 설치가 서로 일치하도록 구성합니다.

다음 표는 네트워크 규모에 따라 달라지는 애플리케이션 설치 설정 및 인터페이스 모양 설정을 목록화한 것입니다.

선택한 네트워크 규모에 따라 달라지는 설치 설정

설정	1~100대의 관리 중인 기기	101~1,000대의 관리 중인 기기	1,001~5,000대의 관리 중인 기기	5,000대 이상의 관리 중인 기기
콘솔 트리에 보조 및 가상 중앙 관리 서버의 노드 표시, 보조 및 가상 중앙 관리 서버와 관련된 모든 설정 표시(MMC 기반 관리 콘솔에서만 사용 가능)	사용 불가능	사용 불가능	사용 가능한 용량	사용 가능한 용량
중앙 관리 서버 및 관리 그룹의 속성 창에 **보안** 섹션 표시(MMC 기반 관리 콘솔에서만 사용 가능)	사용 불가능	사용 불가능	사용 가능한 용량	사용 가능한 용량
클라이언트 기기에서의 업데이트 작업 시작 시간을 임의 배포	사용 불가능	5분 간격	10분 간격	10분 간격

중앙 관리 서버를 MySQL 5.7 또는 SQL Express 데이터베이스 서버에 연결 시, 애플리케이션에서 관리하는 기기 수가 10,000대를 넘지 않을 것을 권장합니다. MariaDB 데이터베이스 관리 시스템의 경우 관리 중인 기기의 최대 권장 수는 20,000대입니다.

5단계. 데이터베이스 선택

마법사의 이 단계에서 중앙 관리 서버 데이터베이스를 저장하는 데 사용할 다음 DBMS(데이터베이스 관리 시스템) 중 하나를 선택합니다:

- **Microsoft SQL Server 또는 SQL Server Express**
- **MySQL 또는 MariaDB**
- **PostgreSQL 또는 Postgres Pro**

> 도메인 컨트롤러 대신 전용 서버에 중앙 관리 서버를 설치하는 것이 좋습니다. RODC(읽기 전용 도메인 컨트롤러) 역할을 하는 서버에 Kaspersky Security Center를 설치하는 경우 Microsoft SQL Server(SQL Express)를 (동일한 기기에) 로컬로 설치해서는 안 됩니다. 이때, Microsoft SQL Server(SQL Express)를 (다른 기기에) 원격 설치하거나, DBMS를 로컬로 설치해야 한다면 MySQL, MariaDB, PostgreSQL 중 하나를 사용할 것을 권장합니다.

중앙 관리 서버 데이터베이스 구조는 Kaspersky Security Center 설치 폴더에 있는 klakdb.chm 파일에서 제공됩니다. 이 파일은 Kaspersky 포털의 압축 파일(klakdb.zip)에서도 사용할 수 있습니다.

6단계. SQL 서버 구성

마법사의 이 단계에서 선택한 DBMS(데이터베이스 관리 시스템)에 따라 다음 연결 설정을 지정합니다:

- 이전 단계에서 **Microsoft SQL Server 또는 SQL Server Express**를 선택한 경우:
  - **SQL 서버 인스턴스 이름** 필드에 네트워크의 SQL Server 이름을 지정합니다. 네트워크에 설치된 모든 SQL Server 목록을 보려면 **찾기** 버튼을 클릭합니다. 이 필드는 기본적으로 비워져 있습니다.

    사용자 지정 포트를 통해 SQL Server에 연결할 경우 SQL Server와 함께 호스트 이름이 쉼표로 구분되는 포트 번호로 지정됩니다(예:

    ```
    SQL_Server_host_name,1433
    ```

    인증서를 사용하여 중앙 관리 서버와 SQL Server 사이의 통신 보호 시, **SQL 서버 인스턴스 이름** 필드에서 인증서 생성에 사용한 것과 동일한 호스트 이름을 지정합니다. 이름이 지정된 SQL Server 인스턴스를 사용할 경우 SQL Server와 함께 호스트 이름이 쉼표로 구분되는 포트 번호로 지정됩니다(예:

    ```
    SQL_Server_name,1433
    ```

    동일한 호스트에서 여러 SQL Server 인스턴스를 사용하는 경우 백슬래시로 구분되는 인스턴스 이름을 추가로 지정합니다(예:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    엔터프라이즈 네트워크의 SQL Server에 Always On 기능이 활성화되어 있다면, **SQL 서버 인스턴스 이름** 필드에서 가용성 그룹 수신기의 이름을 지정합니다. 중앙 관리 서버는 Always On 기능이 활성화된 경우에만 동기 커밋 가용성 모드를 지원합니다.
  - **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.

  이 단계에서 Kaspersky Security Center를 설치 중인 기기에 SQL Server를 설치하려고 한다면 이 설치를 중지하고 SQL Server 설치 후 다시 시작해야 합니다. 지원하는 SQL 서버 버전은 시스템 요구 사항에 기록되어 있습니다.

원격 기기에 SQL Server를 설치 시, Kaspersky Security Center 설치 마법사를 중지할 필요가 없습니다. SQL Server를 설치하고 Kaspersky Security Center 설치를 재개합니다.

- 이전 단계에서 **MySQL 또는 MariaDB**을 선택했다면:
  - **SQL 서버 인스턴스 이름** 필드에 DBMS 인스턴스 이름을 지정합니다. 이 이름은 기본적으로 Kaspersky Security Center를 설치할 기기의 IP 주소입니다.
  - **포트** 필드에 DBMS에 대한 중앙 관리 서버 연결용 포트를 지정합니다. 기본 포트 번호는 3306입니다.
  - **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.
- 이전 단계에서 **PostgreSQL 또는 Postgres Pro**를 선택했다면:
  - **PostgreSQL 또는 Postgres Pro Server** 필드에 DBMS 인스턴스 이름을 지정합니다. 이 이름은 기본적으로 Kaspersky Security Center를 설치할 기기의 IP 주소입니다.
  - **포트** 필드에 DBMS에 대한 중앙 관리 서버 연결용 포트를 지정합니다. 기본 포트 번호는 5432입니다.
  - **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.

7단계. 인증 모드 선택

중앙 관리 서버를 DBMS(데이터베이스 관리 시스템)에 연결하는 데 사용될 인증 모드를 결정합니다.

선택한 DBMS에 따라 다음 인증 모드를 선택할 수 있습니다:

- SQL Express 또는 Microsoft SQL Server의 경우 다음 옵션 중 하나를 선택합니다:
  - **Microsoft Windows 인증 모드**. 중앙 관리 서버를 시작한 계정을 사용하여 권한이 확인됩니다.
  - **SQL 서버 인증 모드**. 이 옵션을 선택하면 이 창에 지정된 계정을 사용하여 접근 권한을 확인합니다. **계정** 및 **암호** 필드를 입력합니다.

    입력한 암호를 보려면 **보기** 버튼을 길게 누릅니다.

  애플리케이션은 두 인증 모드에서 모두 데이터베이스를 사용할 수 있는지 확인합니다. 데이터베이스를 사용할 수 없으면 오류 메시지가 표시되며, 올바른 자격증명을 입력해야 합니다.

  중앙 관리 서버 데이터베이스가 다른 기기에 저장되어 있고 중앙 관리 서버 계정에 데이터베이스 서버 접근 권한이 없으면 중앙 관리 서버를 설치하거나 업그레이드하는 동안 SQL Server 인증 모드를 사용해야 합니다. 이것은 데이터베이스를 저장하는 기기가 도메인 외부에 있거나 중앙 관리 서버가 LocalSystem 계정 아래에 설치된 경우에 적용됩니다.

- MySQL, MariaDB, PostgreSQL, Postgres Pro은 계정과 암호를 지정합니다.

8단계. 하드 드라이브에 파일 압축 해제 및 설치

Kaspersky Security Center 구성 요소 설치에 대한 구성이 완료되었으면 하드 드라이브에 파일 설치를 시작할 수 있습니다.

설치에 추가 프로그램이 필요하다면 설치 마법사는 Kaspersky Security Center를 설치하기 전에 **필수 구성 요소 설치** 페이지에 이를 표시합니다. **다음** 버튼을 누르면 필수 프로그램이 자동으로 설치됩니다.

마지막 페이지에서 Kaspersky Security Center 사용을 위해 시작할 콘솔을 선택할 수 있습니다:

- **MMC 기반 관리 콘솔 시작**
- **Kaspersky Security Center 웹 콘솔 시작**

  이 옵션은 이전 단계 중 하나에서 Kaspersky Security Center 웹 콘솔을 설치하도록 선택했을 때만 사용할 수 있습니다.

마침을 눌러 Kaspersky Security Center 사용을 시작하지 않고 마법사를 닫을 수도 있습니다. 나중에 언제든지 작업을 시작할 수 있습니다.

관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 처음 시작할 때 애플리케이션 초기 설정을 수행할 수 있습니다.

설치 마법사가 완료되면 운영 체제가 설치된 하드 드라이브에 다음 애플리케이션 구성 요소가 설치됩니다:

- 중앙 관리 서버(서버 버전의 네트워크 에이전트와 함께 설치)
- Microsoft Management Console 기반 관리 콘솔
- Kaspersky Security Center 웹 콘솔(설치하도록 선택했을 시)
- 배포 키트에서 제공되는 애플리케이션 관리 플러그인

또한 Microsoft Windows Installer 4.5가 이전에 설치하지 않은 경우 설치됩니다.

사용자 지정 설치

사용자 지정 설치는 중앙 관리 서버를 설치하는 동안 설치하려는 구성 요소를 선택하고 설치되어야 하는 폴더를 지정하라는 메시지가 나타납니다.

이 설치 유형을 사용하면 데이터베이스 및 중앙 관리 서버를 구성할 수 있을 뿐만 아니라 표준 설치에 포함 안 된 구성 요소를 설치하거나 여러 Kaspersky 보안 제품을 위한 관리 플러그인을 설치할 수 있습니다. 또한, 모바일 기기 관리를 활성화할 수 있습니다.

로컬 기기에 Kaspersky Security Center 중앙 관리 서버를 설치하려면 다음과 같이 하십시오:

ksc_<version number>.<build number>_full_<localization language>.exe 실행 파일을 실행합니다.

설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다. 애플리케이션 선택 창에서 **Kaspersky Security Center 중앙 관리 서버 설치** 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

1단계. 라이센스 계약서 및 개인정보취급방침 검토

설치 마법사의 이 단계에서, 사용자와 Kaspersky 사이에 적용되는 라이센스 계약서 및 개인 정보 취급 방침을 읽어 보아야 합니다.

또한 Kaspersky Security Center 배포 키트에 포함된 애플리케이션 관리 플러그인에 대한 라이센스 계약서 및 개인정보취급방침을 확인하는 창이 표시될 수 있습니다.

라이센스 계약서 및 개인정보취급방침을 주의 깊게 읽어 주십시오. 라이센스 계약서 및 개인 정보 취급 방침의 모든 조건에 동의한다면, 적절한 확인란을 선택하여 확인하십시오.

두 개의 확인란을 모두 선택한 이후 기기에 애플리케이션을 계속 설치할 수 있습니다.

라이센스 계약서 또는 개인정보취급방침에 동의하지 않을 경우 **취소** 버튼을 눌러 애플리케이션 설치를 취소하십시오.

2단계. 설치 방법 선택

설치 유형 선택 창에서 **사용자 지정**을 지정합니다.

사용자 지정 설치에서는 공유 폴더 경로, 계정, 중앙 관리 서버 연결용 포트, 데이터베이스 설정 등의 Kaspersky Security Center 설정을 수정할 수 있습니다. 사용자 지정 설치를 선택하는 경우 설치할 Kaspersky 관리 플러그인을 지정할 수 있습니다. 사용자 지정 설치 중에는 해당하는 옵션을 활성하여 모바일 기기용 설치 패키지를 만들 수 있습니다.

3단계. 설치할 구성 요소 선택

설치할 Kaspersky Security Center 중앙 관리 서버의 구성 요소를 선택합니다:

- **모바일 기기 매니지먼트**. Kaspersky Security Center 설치 마법사 실행 시 모바일 기기용 설치 패키지를 만들어야 한다면 이 확인란을 선택합니다. 중앙 관리 서버 설치 이후에 관리 콘솔 도구를 사용하여 모바일 기기용 설치 패키지를 수동으로 만들 수도 있습니다.

- **SNMP 에이전트**. 이 구성 요소는 SNMP 프로토콜을 통한 중앙 관리 서버의 통계 정보 수집합니다. 이 구성 요소는 SNMP가 설치된 기기에 애플리케이션이 설치된 경우에 사용할 수 있습니다.

  Kaspersky Security Center가 설치되면 통계를 가져올 때 필요한 .mib 파일이 애플리케이션 설치 폴더의 SNMP 하위 폴더에 위치합니다.

네트워크 에이전트와 관리 콘솔은 구성 요소 목록에 표시되지 않습니다. 이러한 구성 요소는 자동으로 설치되며 설치를 취소할 수 없습니다.

이 단계에서는 중앙 관리 서버 구성 요소의 설치 폴더를 지정해야 합니다. 기본적으로 구성 요소는 <디스크>:\Program Files\Kaspersky Lab\Kaspersky Security Center에 설치됩니다. 이 폴더가 없는 경우 설치를 진행하는 동안 자동으로 생성됩니다. **찾기** 버튼을 사용하여 대상 폴더를 변경할 수 있습니다.

4단계. Kaspersky Security Center 웹 콘솔 설치

이 단계는 64비트 운영 체제를 사용 중인 경우에만 표시됩니다. 그렇지 않으면, 32비트 운영 체제에서 Kaspersky Security Center 웹 콘솔이 작동하지 않아 이 단계가 표시되지 않습니다.

기본적으로 Kaspersky Security Center 웹 콘솔과 MMC 기반 관리 콘솔이 모두 설치됩니다.

Kaspersky Security Center 웹 콘솔만 설치하려면:

1. **다음 하나만 설치**를 선택합니다.
2. 드롭다운 목록에서 **웹 기반 콘솔**을 선택합니다.

Kaspersky Security Center 웹 콘솔 설치는 중앙 관리 서버 설치 완료 후 자동으로 시작됩니다.

MMC 기반 관리 콘솔만 설치하려면:

1. **다음 하나만 설치**를 선택합니다.
2. 드롭다운 목록에서 **MMC 기반 콘솔**을 선택합니다.

5단계. 네트워크 크기 선택

Kaspersky Security Center를 설치할 네트워크의 규모를 지정합니다. 마법사는 네트워크에 구성된 기기 수에 따라 애플리케이션 인터페이스 모양과 설치가 서로 일치하도록 구성합니다.

다음 표는 네트워크 규모에 따라 달라지는 애플리케이션 설치 설정 및 인터페이스 모양 설정을 목록화한 것입니다.

선택한 네트워크 규모에 따라 달라지는 설치 설정

설정	1~100대의 관리 중인 기기	101~1,000대의 관리 중인 기기	1,001~5,000대의 관리 중인 기기	5,000대 이상의 관리 중인 기기
콘솔 트리에 보조 및 가상 중앙 관리 서버의 노드 표시, 보조 및 가상 중앙 관리 서버와 관련된 모든 설정 표시(MMC 기반 관리 콘솔에서만 사용 가능)	사용 불가능	사용 불가능	사용 가능한 용량	사용 가능한 용량
중앙 관리 서버 및 관리 그룹의 속성 창에 **보안** 섹션 표시(MMC 기반 관리 콘솔에서만 사용 가능)	사용 불가능	사용 불가능	사용 가능한 용량	사용 가능한 용량
클라이언트 기기에서의 업데이트 작업 시작 시간을 임의 배포	사용 불가능	5분 간격	10분 간격	10분 간격

중앙 관리 서버를 MySQL 5.7 또는 SQL Express 데이터베이스 서버에 연결 시, 애플리케이션에서 관리하는 기기 수가 10,000대를 넘지 않을 것을 권장합니다. MariaDB 데이터베이스 관리 시스템의 경우 관리 중인 기기의 최대 권장 수는 20,000대입니다.

6단계. 데이터베이스 선택

마법사의 이 단계에서 중앙 관리 서버 데이터베이스를 저장하는 데 사용할 다음 DBMS(데이터베이스 관리 시스템) 중 하나를 선택합니다:

- **Microsoft SQL Server 또는 SQL Server Express**
- **MySQL 또는 MariaDB**
- **PostgreSQL 또는 Postgres Pro**

> 도메인 컨트롤러 대신 전용 서버에 중앙 관리 서버를 설치하는 것이 좋습니다. RODC(읽기 전용 도메인 컨트롤러) 역할을 하는 서버에 Kaspersky Security Center를 설치하는 경우 Microsoft SQL Server(SQL Express)를 (동일한 기기에) 로컬로 설치해서는 안 됩니다. 이때, Microsoft SQL Server(SQL Express)를 (다른 기기에) 원격 설치하거나, DBMS를 로컬로 설치해야 한다면 MySQL, MariaDB, PostgreSQL 중 하나를 사용할 것을 권장합니다.

중앙 관리 서버 데이터베이스 구조는 Kaspersky Security Center 설치 폴더에 있는 klakdb.chm 파일에서 제공됩니다. 이 파일은 Kaspersky 포털의 압축 파일(klakdb.zip)에서도 사용할 수 있습니다.

7단계. SQL 서버 구성

마법사의 이 단계에서 선택한 DBMS(데이터베이스 관리 시스템)에 따라 다음 연결 설정을 지정합니다:

- 이전 단계에서 **Microsoft SQL Server 또는 SQL Server Express**를 선택한 경우:
  - **SQL 서버 인스턴스 이름** 필드에 네트워크의 SQL Server 이름을 지정합니다. 네트워크에 설치된 모든 SQL Server 목록을 보려면 **찾기** 버튼을 클릭합니다. 이 필드는 기본적으로 비워져 있습니다.

    사용자 지정 포트를 통해 SQL Server에 연결할 경우 SQL Server와 함께 호스트 이름이 쉼표로 구분되는 포트 번호로 지정됩니다(예:

    ```
    SQL_Server_host_name,1433
    ```

    인증서를 사용하여 중앙 관리 서버와 SQL Server 사이의 통신 보호 시, **SQL 서버 인스턴스 이름** 필드에서 인증서 생성에 사용한 것과 동일한 호스트 이름을 지정합니다. 이름이 지정된 SQL Server 인스턴스를 사용할 경우 SQL Server와 함께 호스트 이름이 쉼표로 구분되는 포트 번호로 지정됩니다(예:

    ```
    SQL_Server_name,1433
    ```

    동일한 호스트에서 여러 SQL Server 인스턴스를 사용하는 경우 백슬래시로 구분되는 인스턴스 이름을 추가로 지정합니다(예:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    엔터프라이즈 네트워크의 SQL Server에 Always On 기능이 활성화되어 있다면, **SQL 서버 인스턴스 이름** 필드에서 가용성 그룹 수신기의 이름을 지정합니다. 중앙 관리 서버는 Always On 기능이 활성화된 경우에만 동기 커밋 가용성 모드를 지원합니다.
  - **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.

  이 단계에서 Kaspersky Security Center를 설치 중인 기기에 SQL Server를 설치하려고 한다면 이 설치를 중지하고 SQL Server 설치 후 다시 시작해야 합니다. 지원하는 SQL 서버 버전은 시스템 요구 사항에 기록되어 있습니다.

원격 기기에 SQL Server를 설치 시, Kaspersky Security Center 설치 마법사를 중지할 필요가 없습니다. SQL Server를 설치하고 Kaspersky Security Center 설치를 재개합니다.

- 이전 단계에서 **MySQL 또는 MariaDB**을 선택했다면:
  - **SQL 서버 인스턴스 이름** 필드에 DBMS 인스턴스 이름을 지정합니다. 이 이름은 기본적으로 Kaspersky Security Center를 설치할 기기의 IP 주소입니다.
  - **포트** 필드에 DBMS에 대한 중앙 관리 서버 연결용 포트를 지정합니다. 기본 포트 번호는 3306입니다.
  - **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.
- 이전 단계에서 **PostgreSQL 또는 Postgres Pro**를 선택했다면:
  - **PostgreSQL 또는 Postgres Pro Server** 필드에 DBMS 인스턴스 이름을 지정합니다. 이 이름은 기본적으로 Kaspersky Security Center를 설치할 기기의 IP 주소입니다.
  - **포트** 필드에 DBMS에 대한 중앙 관리 서버 연결용 포트를 지정합니다. 기본 포트 번호는 5432입니다.
  - **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.

8단계. 인증 모드 선택

중앙 관리 서버를 DBMS(데이터베이스 관리 시스템)에 연결하는 데 사용될 인증 모드를 결정합니다.

선택한 DBMS에 따라 다음 인증 모드를 선택할 수 있습니다:

- SQL Express 또는 Microsoft SQL Server의 경우 다음 옵션 중 하나를 선택합니다:
  - **Microsoft Windows 인증 모드**. 중앙 관리 서버를 시작한 계정을 사용하여 권한이 확인됩니다.
  - **SQL 서버 인증 모드**. 이 옵션을 선택하면 이 창에 지정된 계정을 사용하여 접근 권한을 확인합니다. **계정** 및 **암호** 필드를 입력합니다.

    입력한 암호를 보려면 **보기** 버튼을 길게 누릅니다.

  애플리케이션은 두 인증 모드에서 모두 데이터베이스를 사용할 수 있는지 확인합니다. 데이터베이스를 사용할 수 없으면 오류 메시지가 표시되며, 올바른 자격증명을 입력해야 합니다.

  중앙 관리 서버 데이터베이스가 다른 기기에 저장되어 있고 중앙 관리 서버 계정에 데이터베이스 서버 접근 권한이 없으면 중앙 관리 서버를 설치하거나 업그레이드하는 동안 SQL Server 인증 모드를 사용해야 합니다. 이것은 데이터베이스를 저장하는 기기가 도메인 외부에 있거나 중앙 관리 서버가 LocalSystem 계정 아래에 설치된 경우에 적용됩니다.

- MySQL, MariaDB, PostgreSQL, Postgres Pro은 계정과 암호를 지정합니다.

9단계. 중앙 관리 서버를 시작할 계정 선택

서비스로 중앙 관리 서버를 시작하는 데 사용할 계정을 선택합니다.

- **자동으로 계정 생성**. 이 애플리케이션은 kladminserver 서비스를 실행하기 위해 KL-AK-*로 시작하는 계정을 만듭니다.

  공유 폴더와 DBMS를 중앙 관리 서버와 동일한 기기에서 운영할 계획이라면 이 옵션을 선택할 수 있습니다.

- **계정 선택**. 중앙 관리 서버 서비스(kladminserver)가 사용자가 선택한 계정을 사용해 실행됩니다.

  만일 다른 기기에 있는 SQL Express를 포함한 모든 버전의 SQL Server 인스턴스를 DBMS로 사용하려는 경우 및/또는 다른 기기에 있는 공유 폴더를 사용할 계획이라면 도메인 계정을 선택해야 합니다.

  Kaspersky Security Center는 MSA(관리 서비스 계정)와 gMSA(그룹 관리 서비스 계정)를 지원합니다. 이러한 유형의 계정이 사용자 도메인에서 사용되면 중앙 관리 서버 서비스용 계정으로 그 중 하나를 선택할 수 있습니다.

  MSA 또는 gMSA를 지정하기 전에 중앙 관리 서버를 설치할 동일한 기기에 계정을 설치해야 합니다. 계정이 아직 설치되지 않은 경우 중앙 관리 서버 설치를 취소하고 계정을 설치한 다음 중앙 관리 서버를 다시 설치하십시오. 로컬 기기에 관리 중인 서비스 계정을 설치하는 방법에 대한 자세한 내용은 공식 Microsoft 설명서를 참조하십시오.

  MSA 또는 gMSA를 지정하려면 다음을 수행하십시오.

  1. **찾기** 버튼을 누릅니다.
  2. 열리는 창에서 **개체 유형** 버튼을 누릅니다.
  3. **서비스 계정** 유형을 선택하고 **확인**을 누릅니다.
  4. 관련 계정을 선택하고 **확인**을 누릅니다.

선택한 계정에는 사용하려는 DBMS에 따라 다른 권한을 가지고 있어야 합니다.

보안 문제로 인해 중앙 관리 서버를 실행하는 계정에 이 권한을 할당하지 마십시오.

중앙 관리 서버 계정은 나중에 변경할 수 없습니다. 다른 중앙 관리 서버 계정을 사용하려면 장애 조치 클러스터를 다시 설치해야 합니다.

10단계. Kaspersky Security Center 서비스를 실행하기 위한 계정 선택

이 기기에서 Kaspersky Security Center 서비스를 실행하는 데 사용할 계정을 선택합니다:

- **자동으로 계정 생성**. Kaspersky Security Center는 kladmins 그룹에 소속된 KlScSvc라는 로컬 계정을 만듭니다. Kaspersky Security Center 서비스는 생성된 계정으로 실행됩니다.
- **계정 선택**. Kaspersky Security Center 서비스는 사용자가 선택한 계정으로 실행됩니다.

  예를 들어 리포트를 다른 기기에 있는 폴더에 저장하려는 경우 또는 조직의 보안 정책일 경우에는 도메인 계정을 선택해야 합니다. Failover 클러스터에 중앙 관리 서버를 설치하려는 경우에도 도메인 계정을 선택해야 할 수 있습니다.

보안 문제로 인해 이 서비스를 실행하는 계정에는 권한을 부여하지 마십시오.

KSN 프록시 서비스(ksnproxy), Kaspersky 활성화 프록시 서비스(klactprx) 및 Kaspersky 인증 포털 서비스(klwebsrv)는 선택한 계정으로 실행됩니다.

11단계. 공유 폴더 선택

다음 작업에 사용될 공유 폴더의 이름과 위치를 정의합니다:

- 애플리케이션의 원격 설치에 필요한 파일 저장(이러한 파일은 설치 패키지를 만드는 동안 중앙 관리 서버로 복사됨).
- 업데이트 경로에서 다운로드한 업데이트를 중앙 관리 서버에 저장.

파일 공유(읽기 전용)는 모든 사용자가 사용할 수 있습니다.

다음 옵션 중 하나를 선택하실 수 있습니다:

- **공유 폴더 만들기**. 새 폴더를 만듭니다. 텍스트 상자에 폴더 경로를 지정합니다.
- **기존 공유 폴더 선택**. 기존 공유 폴더를 하나 선택합니다.

공유 폴더는 설치에 사용된 기기의 로컬 폴더 또는 회사 네트워크에 있는 클라이언트 기기의 원격 디렉터리일 수 있습니다. **찾기** 버튼을 눌러 공유 폴더를 선택하거나 해당 필드에 UNC 경로(예: \\server\Share)를 직접 지정할 수도 있습니다.

기본적으로 설치 프로그램은 Kaspersky Security Center의 구성 요소가 포함된 애플리케이션 폴더에 KLSHARE 로컬 하위 폴더를 생성합니다.

필요하다면 나중에 공유 폴더를 정의할 수 있습니다.

12단계. 중앙 관리 서버에 대한 연결 구성

중앙 관리 서버에 대한 연결을 구성합니다:

- **Port**

  중앙 관리 서버에 연결하는 데 사용되는 포트 번호입니다.
  기본 포트 번호는 14000입니다.

- **SSL 포트**

  SSL(Secure Sockets Layer)을 통해 중앙 관리 서버에 안전하게 연결하는 데 사용되는 SSL 포트 번호입니다.
  기본 포트 번호는 13000입니다.

- **암호화 키 길이**

  암호화 키의 길이(1024비트 또는 2048비트)를 선택합니다.

  1024비트 암호화 키의 경우 CPU에 대한 부하는 더 적지만 기술 사양으로 인해 안정적인 암호화 기능을 제공하지 못하기 때문에 오래된 기술로 간주됩니다. 또한 1024비트 키를 사용하는 SSL 인증서와 기존 하드웨어가 호환되지 않을 가능성이 높습니다.

  2048비트 암호화 키는 최신 암호화 표준을 모두 충족합니다. 그러나 2048비트 암호화 키를 사용하는 경우 CPU에 대한 부하가 추가될 수 있습니다.

  기본적으로 **2048비트 (최고의 보안)**가 선택됩니다.

나중에 중앙 관리 서버에 연결하기 위한 파라미터를 다음과 같이 변경할 수도 있습니다.

- 중앙 관리 서버 속성의 **연결 포트** 섹션에서 포트 및 SSL 포트 번호를 변경할 수 있습니다. 중앙 관리 서버 연결 포트에 대한 자세한 내용은 Kaspersky Security Center에서 사용하는 포트를 참조하십시오.

- 중앙 관리 서버 인증서를 klsetsrvcert 유틸리티로 교체할 때 `-o RsaKeyLen:<키 길이>` 파라미터를 사용하여 암호화 키 길이를 변경할 수 있습니다.

13단계. 중앙 관리 서버 주소 정의

다음 방법 중 하나를 사용하여 중앙 관리 서버 주소를 지정합니다.

- **DNS 도메인 이름**. 이 방법은 네트워크에 DNS 서버가 포함되어 있고 클라이언트 기기가 이를 사용하여 중앙 관리 서버 주소를 수신할 수 있는 경우에 유용합니다.

- **NetBIOS 이름**. 이 방법은 클라이언트 기기가 NetBIOS 프로토콜을 통해 중앙 관리 서버 주소를 수신하거나 네트워크에 WINS 서버를 사용할 수 있는 경우에 유용합니다.

- **IP 주소**. 이 방법은 중앙 관리 서버에 큰 변화가 없는 정적 IP 주소가 있는 경우에 사용됩니다.

Kaspersky Security Center 장애 조치 클러스터의 액티브 노드에 Kaspersky Security Center를 설치하고, 클러스터 노드 준비 시 보조 네트워크 어댑터를 생성했다면, 이 어댑터의 IP 주소를 지정합니다. 생성하지 않았다면 사용 중인 타사 로드 밸런서의 IP 주소를 입력하십시오.

14단계. 모바일 기기 연결에 사용할 중앙 관리 서버 주소

설치 시 모바일 기기 매니지먼트를 선택했다면 이 설치 마법사를 사용할 수 있습니다.

모바일 기기 연결용 주소 창에서 로컬 네트워크 외부에 있는 모바일 기기 연결을 위한 중앙 관리 서버의 외부 주소를 지정하십시오. 중앙 관리 서버의 IP 주소 또는 DNS(Domain Name System)를 지정할 수 있습니다.

15단계. 애플리케이션 관리 플러그인 선택

Kaspersky Security Center와 함께 설치해야 하는 애플리케이션 관리 플러그인을 선택합니다.

검색이 쉽도록 플러그인이 보안 개체 유형에 따라 그룹으로 구분되어 있습니다.

16단계. 하드 드라이브에 파일 압축 해제 및 설치

Kaspersky Security Center 구성 요소 설치에 대한 구성이 완료되었으면 하드 드라이브에 파일 설치를 시작할 수 있습니다.

설치에 추가 프로그램이 필요하다면 설치 마법사는 Kaspersky Security Center를 설치하기 전에 **필수 구성 요소 설치** 페이지에 이를 표시합니다. **다음** 버튼을 누르면 필수 프로그램이 자동으로 설치됩니다.

마지막 페이지에서 Kaspersky Security Center 사용을 위해 시작할 콘솔을 선택할 수 있습니다:

- **MMC 기반 관리 콘솔 시작**
- **Kaspersky Security Center 웹 콘솔 시작**

  이 옵션은 이전 단계 중 하나에서 Kaspersky Security Center 웹 콘솔을 설치하도록 선택했을 때만 사용할 수 있습니다.

마침을 눌러 Kaspersky Security Center 사용을 시작하지 않고 마법사를 닫을 수도 있습니다. 나중에 언제든지 작업을 시작할 수 있습니다.

관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 처음 시작할 때 애플리케이션 초기 설정을 수행할 수 있습니다.

Kaspersky Security Center 장애 조치 클러스터 배포

이 섹션에는 Kaspersky Security Center 장애 조치 클러스터에 대한 일반 정보와 네트워크에서 Kaspersky Security Center 장애 조치 클러스터를 준비하고 배포하는 작업에 대한 지침이 모두 포함되어 있습니다.

시나리오: Kaspersky Security Center 장애 조치 클러스터 배포

Kaspersky Security Center 장애 조치 클러스터는 Kaspersky Security Center의 가용성을 높이고 장애 발생 시 중앙 관리 서버의 다운타임을 최소화합니다. 장애 조치 클러스터는 두 대의 컴퓨터에 설치된 두 개의 동일한 Kaspersky Security Center 인스턴스를 기반으로 작동합니다. 인스턴스 중 하나는 액티브 노드로 작동하고 다른 하나는 패시브 노드로 작동합니다. 액티브 노드는 클라이언트 기기의 보호를 관리하는 반면, 패시브 노드는 액티브 노드가 실패할 경우 액티브 노드의 모든 기능을 수행할 준비가 되어 있습니다. 장애가 발생하면 패시브 노드는 액티브 노드가 되고 액티브 노드는 패시브 노드가 됩니다.

필수 구성 요소

장애 조치 클러스터의 요구 사항을 충족하는 하드웨어가 있습니다.

단계

Kaspersky 애플리케이션 배포는 다음 단계로 진행됩니다.

1. **Kaspersky Security Center 서비스용 계정 생성**

   새 도메인 그룹을 만들고(이 시나리오에서는 이러한 그룹에 대해 'KLAdmins' 이름이 사용됨) 두 노드와 파일 서버의 그룹에 로컬 관리자 권한을 부여합니다. 그런 다음 두 개의 새 도메인 사용자 계정(이 시나리오에서는 이러한 계정에 대해 'ksc' 및 'rightless' 이름이 사용됨)을 만들고 계정을 KLAdmins 도메인 그룹에 추가합니다.

   Kaspersky Security Center를 설치할 사용자 계정을 이전에 생성된 KLAdmins 도메인 그룹에 추가합니다.

2. **파일 서버 준비**

   Kaspersky Security Center 장애 조치 클러스터의 구성 요소로 작동하도록 파일 서버를 준비합니다. 파일 서버가 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인하고 Kaspersky Security Center 데이터를 위한 두 개의 공유 폴더를 만들고 공유 폴더에 액세스할 수 있는 권한을 구성하십시오.

   방법 지침: Kaspersky Security Center 장애 조치 클러스터용 파일 서버 준비

3. **액티브 및 패시브 노드 준비**

   액티브 및 패시브 노드로 작동하도록 동일한 하드웨어 및 소프트웨어를 사용하는 두 대의 기기를 준비합니다.

   방법 지침: Kaspersky Security Center 장애 조치 클러스터용 노드 준비

4. **데이터베이스 관리 시스템(DBMS) 설치**

   지원되는 DBMS 중 하나를 선택하고, 전용 기기에 DBMS를 설치합니다. DBMS 설치 방법에 관한 정보는 해당 설명서를 참조하십시오.

5. **Kaspersky Security Center 설치**

   두 노드에 장애 조치 클러스터 모드로 Kaspersky Security Center를 설치합니다. 액티브 호스트로 설정하려는 기기에 Kaspersky Security Center를 먼저 설치한 다음, 패시브 호스트에도 이를 설치해야 합니다.

   또한 클러스터 노드가 아닌 별도의 기기에 Kaspersky Security Center 웹 콘솔을 설치해야 합니다.

   방법 지침: Kaspersky Security Center 장애 조치 클러스터 노드에 Kaspersky Security Center 설치

6 **장애 조치 클러스터 테스트**

장애 조치 클러스터를 올바르게 구성하고 제대로 작동하는지 확인하십시오. 예를 들어, 액티브 노드에서 Kaspersky Security Center 서비스(kladminserver, klnagent, ksnproxy, klactprx 또는 klwebsrv) 중 하나를 중지해 보면 됩니다. 서비스가 중지되면 보호 관리가 자동으로 패시브 노드로 전환되어야 합니다.

결과

Kaspersky Security Center 장애 조치 클러스터가 배포됩니다. 액티브 노드와 패시브 노드 간 전환을 일으키는 이벤트를 숙지해 두십시오.

Kaspersky Security Center 장애 조치 클러스터 정보

Kaspersky Security Center 장애 조치 클러스터는 Kaspersky Security Center의 가용성을 높이고 장애 발생 시 중앙 관리 서버의 다운타임을 최소화합니다. 장애 조치 클러스터는 두 대의 컴퓨터에 설치된 두 개의 동일한 Kaspersky Security Center 인스턴스를 기반으로 작동합니다. 인스턴스 중 하나는 액티브 노드로 작동하고 다른 하나는 패시브 노드로 작동합니다. 액티브 노드는 클라이언트 기기의 보호를 관리하는 반면, 패시브 노드는 액티브 노드가 실패할 경우 액티브 노드의 모든 기능을 수행할 준비가 되어 있습니다. 장애가 발생하면 패시브 노드는 액티브 노드가 되고 액티브 노드는 패시브 노드가 됩니다.

장애 조치 클러스터를 사용해도 사이징 가이드에 기반한 계산에는 영향을 미치지 않습니다.

문제를 해결하기 위해 Kaspersky 이벤트 로그 기능을 사용합니다.

전환 조건

장애 조치 클러스터는 액티브 노드에서 다음 이벤트 중 하나가 발생하는 경우 클라이언트 기기의 보호 관리를 액티브 노드에서 패시브 노드로 전환합니다.

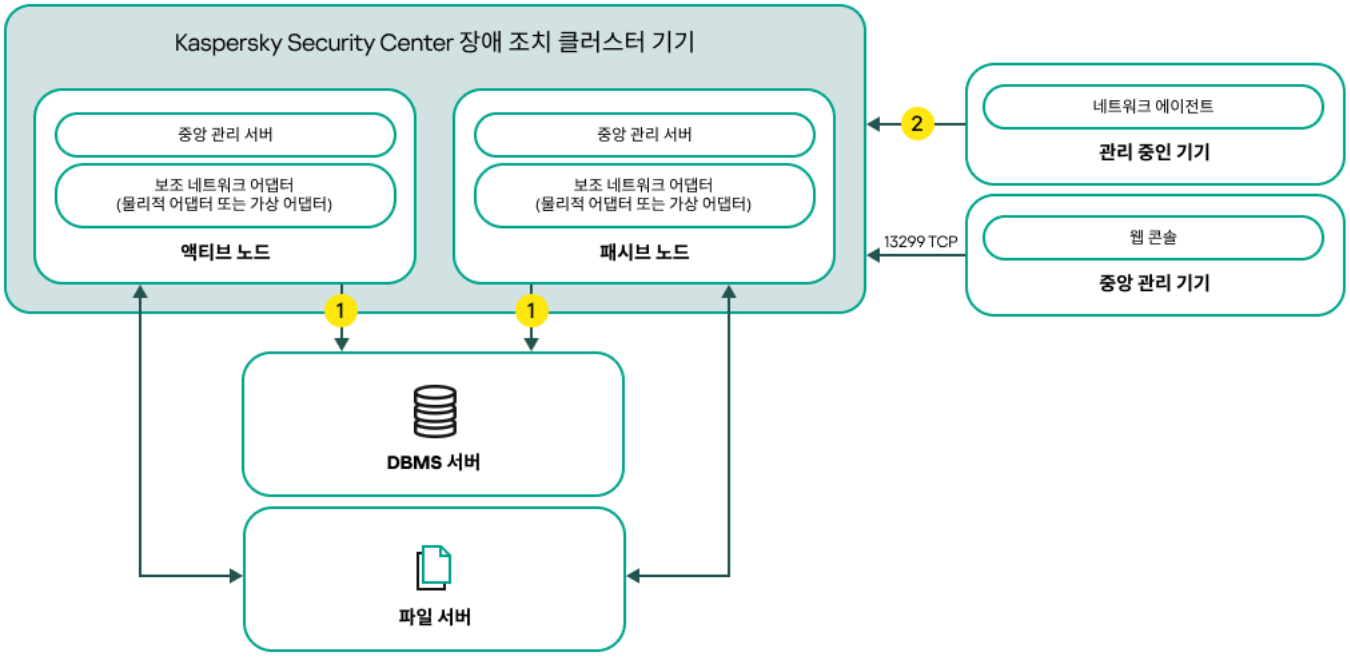
- 소프트웨어 또는 하드웨어 오류로 인해 액티브 노드가 손상되었습니다.
- 액티브 노드가 유지 관리 작업을 위해 일시적으로 중지되었습니다.
- Kaspersky Security Center 서비스(또는 프로세스) 중 하나 이상이 실패했거나 사용자가 의도적으로 종료했습니다. Kaspersky Security Center 서비스는 kladminserver, klnagent, klactprx 및 klwebsrv입니다.
- 액티브 노드와 파일 서버의 스토리지 간 네트워크 연결이 중단되거나 종료되었습니다.

Kaspersky Security Center 장애 조치 클러스터는 모든 Kaspersky Security Center 서비스를 자동으로 관리합니다. 서비스를 수동으로 다시 시작하지 마십시오.

배포 체계

다음 체계 중 하나를 선택하여 Kaspersky Security Center 장애 조치 클러스터를 배포할 수 있습니다.

- 보조 네트워크 어댑터를 사용하는 체계.
- 타사 로드 밸런서를 사용하는 체계.

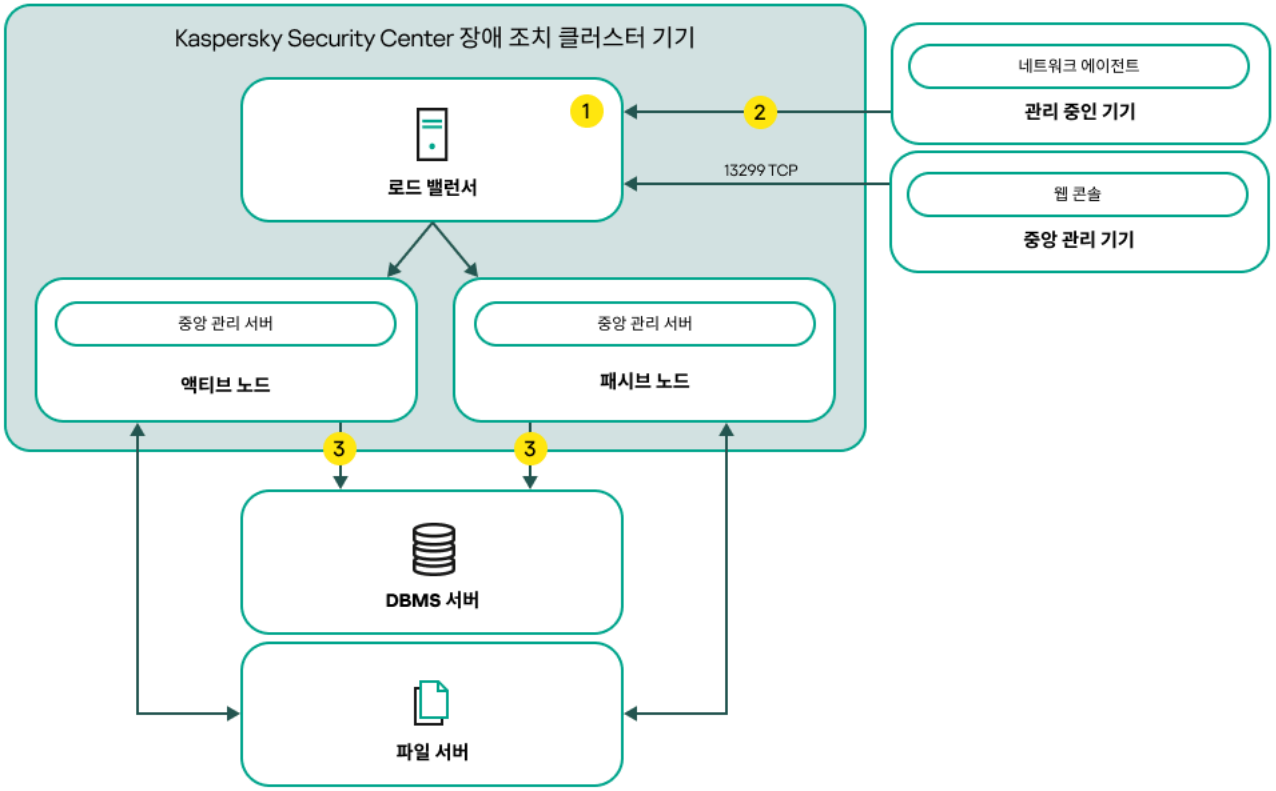


보조 네트워크 어댑터를 사용하는 체계

체계 범례:

1 중앙 관리 서버는 데이터를 데이터베이스에 보냅니다. 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(예: MySQL Server는 포트 3306, Microsoft SQL Server는 포트 1433). 관련 정보는 DBMS 설명서를 참조하십시오.

2 관리 중인 기기에서 TCP 13000, UDP 13000, TCP 17000 포트를 엽니다.



타사 로드 밸런서를 사용하는 체계

체계 범례:

1 로드 밸런서 기기에서 모든 중앙 관리 서버 포트(TCP 13000, UDP 13000, TCP 13299, TCP 17000)를 엽니다.

> 자동화 작업에 klakaut 유틸리티를 사용하려면 TCP 13291 포트도 열어야 합니다.

2 관리 중인 기기에서 TCP 13000, UDP 13000, TCP 17000 포트를 엽니다.

3 중앙 관리 서버는 데이터를 데이터베이스에 보냅니다. 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(예: MySQL Server는 포트 3306, Microsoft SQL Server는 포트 1433). 관련 정보는 DBMS 설명서를 참조하십시오.

Kaspersky Security Center 장애 조치 클러스터용 파일 서버 준비

파일 서버는 Kaspersky Security Center 장애 조치 클러스터의 필수 구성 요소입니다.

파일 서버를 준비하려면:

1. 파일 서버가 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인하십시오.
2. 파일 서버와 두 노드(액티브 및 패시브)가 동일한 도메인에 포함되어 있는지 또는 파일 서버가 도메인 컨트롤러인지 확인하십시오.
3. 파일 서버에서 두 개의 공유 폴더를 만듭니다. 그 중 하나는 장애 조치 클러스터 상태에 대한 정보를 유지하는 데 사용됩니다. 다른 하나는 Kaspersky Security Center의 데이터 및 설정을 저장하는 데 사용됩니다. Kaspersky Security Center 설치를 구성하는 동안 공유 폴더 경로를 지정합니다.

4. 다음 사용자 계정 및 그룹에 대해 생성된 공유 폴더에 전체 액세스 권한(공유 권한 및 NTFS 권한 모두)을 부여합니다.

   - 도메인 그룹 KLAdmins.
   - 사용자 계정 $<node1> 및 $<node2>. 여기서 <node1>과 <node2>는 액티브 노드와 패시브 노드의 기기 이름입니다.

파일 서버가 준비되었습니다. Kaspersky Security Center 장애 조치 클러스터를 배포하려면 이 시나리오의 추가 지침을 따르십시오.

Kaspersky Security Center 장애 조치 클러스터용 노드 준비

Kaspersky Security Center 장애 조치 클러스터의 액티브 노드와 패시브 노드 역할을 할 두 대의 기기를 준비합니다.

Kaspersky Security Center 장애 조치 클러스터용 노드를 준비하려면:

1. 하드웨어 및 소프트웨어 요구 사항을 충족하는 두 대의 기기가 있는지 확인합니다. 두 대의 기기는 장애 조치 클러스터의 액티브 노드와 패시브 노드 역할을 합니다.
2. 파일 서버와 두 노드가 동일한 도메인에 포함되어 있는지 확인하십시오.
3. 다음 중 하나를 수행합니다:

   - 각 노드에서 보조 네트워크 어댑터를 구성합니다.

     보조 네트워크 어댑터는 물리적 어댑터이거나 가상 어댑터일 수 있습니다. 물리적 네트워크 어댑터를 사용하려면, 표준 운영 체제 도구를 사용하여 어댑터를 연결하고 구성하십시오. 가상 네트워크 어댑터를 사용하려면 제삼자 소프트웨어를 사용하여 어댑터를 만드십시오.

     다음 조건이 충족되는지 확인하십시오.

     - 보조 네트워크 어댑터는 비활성화됩니다.

       비활성화된 상태로 보조 네트워크 어댑터를 생성하거나 생성 후 비활성화할 수 있습니다.

     - 두 노드의 보조 네트워크 어댑터는 IP 주소가 같습니다.

   - 타사 로드 밸런서를 사용합니다. 예를 들어 nginx 서버를 사용할 수 있습니다. 이 경우 다음을 수행하십시오.

     a. nginx가 설치된 전용 Linux 기반 기기를 제공합니다.

     b. 로드 밸런싱을 구성합니다. 액티브 노드를 메인 서버로, 패시브 노드를 백업 서버로 설정합니다.

     c. nginx 서버에서 모든 중앙 관리 서버 포트(TCP 13000, UDP 13000, TCP 13299, TCP 17000)를 엽니다.

     > 자동화 작업에 klakaut 유틸리티를 사용하려면 TCP 13291 포트도 열어야 합니다.

4. 노드와 파일 서버를 모두 다시 시작합니다.

5. 파일 서버 준비 단계 중에 생성한 두 개의 공유 폴더를 각 노드에 매핑합니다. 공유 폴더를 네트워크 드라이브로 매핑해야 합니다. 폴더를 매핑할 때 비어 있는 드라이브 문자를 선택할 수 있습니다. 공유 폴더에 액세스하려면 시나리오 1단계에서 생성한 사용자 계정의 자격 증명을 사용하십시오.

   노드가 준비되었습니다. Kaspersky Security Center 장애 조치 클러스터를 배포하려면 시나리오의 추가 지침에 따릅니다.

Kaspersky Security Center 장애 조치 클러스터 노드에 Kaspersky Security Center 설치

Kaspersky Security Center는 Kaspersky Security Center 장애 조치 클러스터의 두 노드에 별도로 설치됩니다. 먼저 액티브 노드에 애플리케이션을 설치한 다음 패시브 노드에 설치합니다. 설치할 때 액티브 노드와 패시브 노드를 선택합니다.

KLAdmins 도메인 그룹의 사용자만 모든 노드에 Kaspersky Security Center를 설치할 수 있습니다.

Kaspersky Security Center 장애 조치 클러스터의 액티브 노드에 Kaspersky Security Center를 설치하려면:

1. ksc_15.1_<빌드 번호>_full_<언어>.exe 실행 파일을 실행합니다.

   설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다. 애플리케이션 선택 창에서 **Kaspersky Security Center 중앙 관리 서버 설치** 설치 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

2. 라이센스 계약서 및 개인정보취급방침을 주의 깊게 읽어 주십시오. 라이센스 계약서 및 개인정보취급방침의 조건에 동의하면 **나는 다음 내용을 모두 읽고 이해했으며 수락하는 것에 동의합니다** 섹션의 확인란을 선택합니다:

   - **이 최종 사용자 라이센스 계약서의 이용 약관**
   - **데이터 처리에 대한 개인정보취급방침**

   두 개의 확인란을 모두 선택한 이후 기기에 애플리케이션을 계속 설치할 수 있습니다.

   라이센스 계약서 또는 개인정보취급방침에 동의하지 않을 경우 **취소** 버튼을 눌러 애플리케이션 설치를 취소하십시오.

3. **Kaspersky Security Center 장애 조치 클러스터의 기본 노드**를 선택하여 액티브 노드에 애플리케이션을 설치합니다.

4. **공유 폴더** 창에서 다음을 수행합니다.

   - **상태 공유** 및 **데이터 공유** 필드에서 준비 중에 파일 서버에서 생성한 공유 폴더의 경로를 지정합니다.
   - **상태 공유 드라이브** 및 **데이터 공유 드라이브** 필드에서 노드 준비 중에 공유 폴더를 매핑한 네트워크 드라이브를 선택합니다.
   - 보조 네트워크 어댑터를 통하거나 타사 로드 밸런서를 통하는 방법으로 클러스터 연결 모드를 선택합니다.

5. 3단계를 시작으로 사용자 지정 설치를 위한 기타 단계를 수행합니다.

> 클러스터 노드 준비 시 어댑터를 생성했다면 13단계에서 보조 네트워크 어댑터의 IP 주소를 지정합니다. 생성하지 않았다면 사용 중인 타사 로드 밸런서의 IP 주소를 입력하십시오.

Kaspersky Security Center가 액티브 노드에 설치됩니다.

Kaspersky Security Center 장애 조치 클러스터의 패시브 노드에 Kaspersky Security Center를 설치하려면:

1. ksc_15.1_<빌드 번호>_full_<언어>.exe 실행 파일을 실행합니다.

   설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다. 애플리케이션 선택 창에서 **Kaspersky Security Center 중앙 관리 서버 설치** 설치 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

2. 라이센스 계약서 및 개인정보취급방침을 주의 깊게 읽어 주십시오. 라이센스 계약서 및 개인정보취급방침의 조건에 동의하면 **나는 다음 내용을 모두 읽고 이해했으며 수락하는 것에 동의합니다** 섹션의 확인란을 선택합니다:

   - **이 최종 사용자 라이센스 계약서의 이용 약관**
   - **데이터 처리에 대한 개인정보취급방침**

   두 개의 확인란을 모두 선택한 이후 기기에 애플리케이션을 계속 설치할 수 있습니다.

   라이센스 계약서 또는 개인정보취급방침에 동의하지 않을 경우 **취소** 버튼을 눌러 애플리케이션 설치를 취소하십시오.

3. 애플리케이션을 패시브 노드에 설치하려면 **Kaspersky Security Center 장애 조치 클러스터의 보조 노드**를 선택합니다.

4. **공유 폴더** 창의 **상태 공유** 필드에서 준비 중에 파일 서버에서 생성한 클러스터 상태 관련 정보가 포함된 공유 폴더의 경로를 지정합니다.

5. **설치** 버튼을 누릅니다. 설치가 끝나면 **마침** 버튼을 클릭합니다.

Kaspersky Security Center가 패시브 노드에 설치됩니다. 이제 Kaspersky Security Center 장애 조치 클러스터를 테스트하여 올바르게 구성했는지, 클러스터가 제대로 작동하는지 확인할 수 있습니다.

수동으로 클러스터 노드 시작 및 중지

유지 관리를 위해 전체 Kaspersky Security Center 장애 조치 클러스터를 중지하거나 클러스터 노드 중 하나를 잠시 분리해야 할 수 있습니다. 이 경우 이 섹션의 지침을 따르십시오. 다른 수단을 사용하여 장애 조치 클러스터와 관련된 서비스 또는 프로세스를 시작하거나 중지하지 마십시오. 이로 인해 데이터가 손실될 수 있습니다.

유지 관리를 위해 전체 장애 조치 클러스터 시작 및 중지

전체 장애 조치 클러스터를 시작하거나 중지하려면:

1. 액티브 노드에서 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center로 이동합니다.
2. 명령줄을 열고 다음 명령 중 하나를 실행합니다.
   - 클러스터를 중지하려면 다음을 실행: `klfoc -stopcluster --stp klfoc`
   - 클러스터를 시작하려면 다음을 실행: `klfoc -startcluster --stp klfoc`

   실행하는 명령에 따라 장애 조치 클러스터가 시작되거나 중지됩니다.

노드 중 하나 유지 관리

노드 중 하나를 유지 관리하려면:

1. 액티브 노드에서 `klfoc -stopcluster --stp klfoc` 명령을 사용하여 장애 조치 클러스터를 중지합니다.
2. 유지 관리하려는 노드에서 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center로 이동합니다.
3. 명령줄을 열고 `detach_node.cmd` 명령을 실행하여 클러스터에서 노드를 분리합니다.
4. 액티브 노드에서 `klfoc -startcluster --stp klfoc` 명령을 사용하여 장애 조치 클러스터를 시작합니다.
5. 유지 관리 작업을 수행합니다.
6. 액티브 노드에서 `klfoc -stopcluster --stp klfoc` 명령을 사용하여 장애 조치 클러스터를 중지합니다.
7. 유지 관리한 노드에서 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center로 이동합니다.
8. 명령줄을 열고 `attach_node.cmd` 명령을 실행하여 클러스터에 노드를 연결합니다.
9. 액티브 노드에서 `klfoc -startcluster --stp klfoc` 명령을 사용하여 장애 조치 클러스터를 시작합니다.

   노드가 유지 관리를 마치고 장애 조치 클러스터에 연결됩니다.

Windows Server 장애 조치 클러스터에 중앙 관리 서버 설치

장애 조치 클러스터에 중앙 관리 서버를 설치하는 절차는 독립 실행형 기기의 표준 및 사용자 지정 설치 절차와 다릅니다.

클러스터의 공통 데이터 저장소가 포함된 노드에서 이 섹션에 설명된 절차를 수행합니다.

클러스터에 Kaspersky Security Center 중앙 관리 서버를 설치하려면 다음 단계를 따릅니다.

ksc_<version number>.<build number>_full_<localization language>.exe 실행 파일을 실행합니다.

설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다. 애플리케이션 선택 창에서 **Kaspersky Security Center 중앙 관리 서버 설치** 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

1단계. 라이센스 계약서 및 개인정보취급방침 검토

설치 마법사의 이 단계에서, 사용자와 Kaspersky 사이에 적용되는 라이센스 계약서 및 개인 정보 취급 방침을 읽어보아야 합니다.

또한 Kaspersky Security Center 배포 키트에 포함된 애플리케이션 관리 플러그인에 대한 라이센스 계약서 및 개인정보취급방침을 확인하는 창이 표시될 수 있습니다.

라이센스 계약서 및 개인정보취급방침을 주의 깊게 읽어 주십시오. 라이센스 계약서 및 개인 정보 취급 방침의 모든 조건에 동의한다면, 적절한 확인란을 선택하여 확인하십시오.

두 개의 확인란을 모두 선택한 이후 기기에 애플리케이션을 계속 설치할 수 있습니다.

라이센스 계약서 또는 개인정보취급방침에 동의하지 않을 경우 **취소** 버튼을 눌러 애플리케이션 설치를 취소하십시오.

2단계. 클러스터에서 설치 유형 선택

클러스터에서 설치 유형을 선택합니다.

- **클러스터 (모든 클러스터 노드에 설치)**

  이는 권장되는 옵션입니다. 이 옵션을 선택하면 중앙 관리 서버가 클러스터의 모든 노드에 동시에 설치됩니다.

  > 설치할 관리 콘솔 선택 단계에서 현재 클러스터 노드에 설치할 콘솔을 선택해야 합니다. 클러스터 노드에만 콘솔을 설치하면 노드 장애 시 중앙 관리 서버에 액세스할 수 없게 됩니다. 이 단계에서 모든 클러스터 노드에 설치할 MMC 기반 관리 콘솔을 선택할 것을 권장합니다. 중앙 관리 서버를 설치한 후 클러스터 노드가 아닌 별도의 기기에 Kaspersky Security Center 웹 콘솔을 설치하십시오. 이렇게 하면 클러스터 노드에 장애 발생 시 Kaspersky Security Center 웹 콘솔을 사용하여 중앙 관리 서버를 관리할 수 있습니다.

- **로컬 (이 기기에만 설치)**

  이 옵션을 선택하면 중앙 관리 서버는 독립 실행형 서버처럼 현재 노드에만 설치되며 중앙 관리 서버는 클러스터 인식 애플리케이션으로 작동하지 않습니다. 예를 들어 중앙 관리 서버에 내결함성이 필요하지 않은 경우 공유 스토리지 공간을 절약하기 위해 이 옵션을 선택할 수 있습니다. 현재 노드가 실패한 경우 다른 노드에 중앙 관리 서버를 설치하고 백업에서 중앙 관리 서버 상태를 복원해야 합니다.

추가 단계는 설치 방법 선택 단계부터 시작하여 표준 또는 사용자 지정 설치 방법을 사용할 때와 동일합니다.

3단계. 가상 중앙 관리 서버의 이름 지정

새 가상 중앙 관리 서버의 네트워크 이름을 지정합니다. 이 이름을 사용하여 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 중앙 관리 서버에 연결할 수 있습니다.

지정하는 이름은 클러스터 이름과 달라야 합니다.

4단계. 가상 중앙 관리 서버의 네트워크 세부 정보 지정

새 가상 중앙 관리 서버 인스턴스의 네트워크 세부 정보를 지정하려면 다음 단계를 따릅니다.

1. **사용할 네트워크**에서 현재 클러스터 노드가 연결된 도메인 네트워크를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 선택한 네트워크에서 DHCP를 사용하여 IP 주소를 할당하는 경우 **DHCP 사용** 옵션을 선택합니다.
   - 선택한 네트워크에서 DHCP를 사용하지 않는 경우 필요한 IP 주소를 지정하십시오.
     지정하는 IP 주소는 클러스터 IP 주소와 달라야 합니다.
3. **추가**를 클릭하여 지정된 설정을 적용합니다.

자동으로 할당되거나 지정된 IP 주소를 사용하여 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 중앙 관리 서버에 연결할 수 있습니다.

5단계. 클러스터 그룹 지정

클러스터 그룹은 모든 노드에 대한 공통 리소스를 포함하는 특수 장애 조치 클러스터 역할입니다. 두 가지 옵션이 있습니다.

- 새 클러스터 그룹 생성.
  이 옵션은 대부분의 경우에 권장됩니다. 새 클러스터 그룹에는 중앙 관리 서버 인스턴스와 관련된 모든 공통 리소스가 포함됩니다.
- 기존 클러스터 그룹 선택.
  기존 클러스터 그룹과 이미 연결된 공통 리소스를 사용하려면 이 옵션을 선택합니다. 예를 들어 기존 클러스터 그룹과 연결된 스토리지를 사용하고 새 클러스터 그룹에 사용할 수 있는 다른 스토리지가 없는 경우 이 옵션을 사용할 수 있습니다.

6단계. 클러스터 데이터 스토리지 선택

클러스터 데이터 스토리지를 선택하려면 다음 단계를 따릅니다.

1. **사용 가능한 저장소**에서 가상 중앙 관리 서버 인스턴스의 공통 리소스가 설치될 데이터 스토리지를 선택합니다.
2. 선택한 데이터 스토리지에 여러 볼륨이 포함된 경우 **디스크 드라이브의 사용 가능한 섹션**에서 필요한 볼륨을 선택합니다.
3. **설치 경로**에서 가상 중앙 관리 서버 인스턴스의 리소스를 설치할 공통 데이터 스토리지의 경로를 입력합니다.

데이터 스토리지가 선택됩니다.

7단계. 원격 설치를 위한 계정 지정

클러스터의 수동 노드에 가상 중앙 관리 서버 인스턴스를 원격 설치하는 데 사용할 사용자 이름과 암호를 지정합니다.

지정하는 계정에는 클러스터의 모든 노드에 대한 관리 권한이 부여되어야 합니다.

8단계. 설치할 구성 요소 선택

설치할 Kaspersky Security Center 중앙 관리 서버의 구성 요소를 선택합니다:

- **모바일 기기 매니지먼트**. Kaspersky Security Center 설치 마법사 실행 시 모바일 기기용 설치 패키지를 만들어야 한다면 이 확인란을 선택합니다. 중앙 관리 서버 설치 이후에 관리 콘솔 도구를 사용하여 모바일 기기용 설치 패키지를 수동으로 만들 수도 있습니다.

- **SNMP 에이전트**. 이 구성 요소는 SNMP 프로토콜을 통한 중앙 관리 서버의 통계 정보 수집합니다. 이 구성 요소는 SNMP가 설치된 기기에 애플리케이션이 설치된 경우에 사용할 수 있습니다.

  Kaspersky Security Center가 설치되면 통계를 가져올 때 필요한 .mib 파일이 애플리케이션 설치 폴더의 SNMP 하위 폴더에 위치합니다.

네트워크 에이전트와 관리 콘솔은 구성 요소 목록에 표시되지 않습니다. 이러한 구성 요소는 자동으로 설치되며 설치를 취소할 수 없습니다.

이 단계에서는 중앙 관리 서버 구성 요소의 설치 폴더를 지정해야 합니다. 기본적으로 구성 요소는 <디스크>:\Program Files\Kaspersky Lab\Kaspersky Security Center에 설치됩니다. 이 폴더가 없는 경우 설치를 진행하는 동안 자동으로 생성됩니다. **찾기** 버튼을 사용하여 대상 폴더를 변경할 수 있습니다.

9단계. 네트워크 크기 선택

Kaspersky Security Center를 설치할 네트워크의 규모를 지정합니다. 마법사는 네트워크에 구성된 기기 수에 따라 애플리케이션 인터페이스 모양과 설치가 서로 일치하도록 구성합니다.

다음 표는 네트워크 규모에 따라 달라지는 애플리케이션 설치 설정 및 인터페이스 모양 설정을 목록화한 것입니다.

선택한 네트워크 규모에 따라 달라지는 설치 설정

설정	1~100대의 관리 중인 기기	101~1,000대의 관리 중인 기기	1,001~5,000대의 관리 중인 기기	5,000대 이상의 관리 중인 기기
콘솔 트리에 보조 및 가상 중앙 관리 서버의 노드 표시, 보조 및 가상 중앙 관리 서버와 관련된 모든 설정 표시(MMC 기반 관리 콘솔에서만 사용 가능)	사용 불가능	사용 불가능	사용 가능한 용량	사용 가능한 용량
중앙 관리 서버 및 관리 그룹의 속성 창에 **보안** 섹션 표시(MMC 기반 관리 콘솔에서만 사용 가능)	사용 불가능	사용 불가능	사용 가능한 용량	사용 가능한 용량
클라이언트 기기에서의 업데이트 작업 시작 시간을 임의 배포	사용 불가능	5분 간격	10분 간격	10분 간격

중앙 관리 서버를 MySQL 5.7 또는 SQL Express 데이터베이스 서버에 연결 시, 애플리케이션에서 관리하는 기기 수가 10,000대를 넘지 않을 것을 권장합니다. MariaDB 데이터베이스 관리 시스템의 경우 관리 중인 기기의 최대 권장 수는 20,000대입니다.

10단계. 데이터베이스 선택

마법사의 이 단계에서 중앙 관리 서버 데이터베이스를 저장하는 데 사용할 다음 DBMS(데이터베이스 관리 시스템) 중 하나를 선택합니다:

- **Microsoft SQL Server 또는 SQL Server Express**
- **MySQL 또는 MariaDB**
- **PostgreSQL 또는 Postgres Pro**

도메인 컨트롤러 대신 전용 서버에 중앙 관리 서버를 설치하는 것이 좋습니다. RODC(읽기 전용 도메인 컨트롤러) 역할을 하는 서버에 Kaspersky Security Center를 설치하는 경우 Microsoft SQL Server(SQL Express)를 (동일한 기기에) 로컬로 설치해서는 안 됩니다. 이때, Microsoft SQL Server(SQL Express)를 (다른 기기에) 원격 설치하거나, DBMS를 로컬로 설치해야 한다면 MySQL, MariaDB, PostgreSQL 중 하나를 사용할 것을 권장합니다.

중앙 관리 서버 데이터베이스 구조는 Kaspersky Security Center 설치 폴더에 있는 klakdb.chm 파일에서 제공됩니다. 이 파일은 Kaspersky 포털의 압축 파일(klakdb.zip)에서도 사용할 수 있습니다.

11단계. SQL 서버 구성

마법사의 이 단계에서 선택한 DBMS(데이터베이스 관리 시스템)에 따라 다음 연결 설정을 지정합니다:

- 이전 단계에서 **Microsoft SQL Server 또는 SQL Server Express**를 선택한 경우:
  - **SQL 서버 인스턴스 이름** 필드에 네트워크의 SQL Server 이름을 지정합니다. 네트워크에 설치된 모든 SQL Server 목록을 보려면 **찾기** 버튼을 클릭합니다. 이 필드는 기본적으로 비워져 있습니다.

    사용자 지정 포트를 통해 SQL Server에 연결할 경우 SQL Server와 함께 호스트 이름이 쉼표로 구분되는 포트 번호로 지정됩니다(예:

    ```
    SQL_Server_host_name,1433
    ```

    인증서를 사용하여 중앙 관리 서버와 SQL Server 사이의 통신 보호 시, **SQL 서버 인스턴스 이름** 필드에서 인증서 생성에 사용한 것과 동일한 호스트 이름을 지정합니다. 이름이 지정된 SQL Server 인스턴스를 사용할 경우 SQL Server와 함께 호스트 이름이 쉼표로 구분되는 포트 번호로 지정됩니다(예:

    ```
    SQL_Server_name,1433
    ```

동일한 호스트에서 여러 SQL Server 인스턴스를 사용하는 경우 백슬래시로 구분되는 인스턴스 이름을 추가로 지정합니다(예:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

엔터프라이즈 네트워크의 SQL Server에 Always On 기능이 활성화되어 있다면, **SQL 서버 인스턴스 이름** 필드에서 가용성 그룹 수신기의 이름을 지정합니다. 중앙 관리 서버는 Always On 기능이 활성화된 경우에만 동기 커밋 가용성 모드를 지원합니다.

- **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.

이 단계에서 Kaspersky Security Center를 설치 중인 기기에 SQL Server를 설치하려고 한다면 이 설치를 중지하고 SQL Server 설치 후 다시 시작해야 합니다. 지원하는 SQL 서버 버전은 시스템 요구 사항에 기록되어 있습니다.

원격 기기에 SQL Server를 설치 시, Kaspersky Security Center 설치 마법사를 중지할 필요가 없습니다. SQL Server를 설치하고 Kaspersky Security Center 설치를 재개합니다.

- 이전 단계에서 **MySQL 또는 MariaDB**을 선택했다면:
  - **SQL 서버 인스턴스 이름** 필드에 DBMS 인스턴스 이름을 지정합니다. 이 이름은 기본적으로 Kaspersky Security Center를 설치할 기기의 IP 주소입니다.
  - **포트** 필드에 DBMS에 대한 중앙 관리 서버 연결용 포트를 지정합니다. 기본 포트 번호는 3306입니다.
  - **데이터베이스 이름** 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.
- 이전 단계에서 **PostgreSQL 또는 Postgres Pro**를 선택했다면:
  - **PostgreSQL 또는 Postgres Pro Server** 필드에 DBMS 인스턴스 이름을 지정합니다. 이 이름은 기본적으로 Kaspersky Security Center를 설치할 기기의 IP 주소입니다.
  - **포트** 필드에 DBMS에 대한 중앙 관리 서버 연결용 포트를 지정합니다. 기본 포트 번호는 5432입니다.

데이터베이스 이름 필드에 중앙 관리 서버 데이터 저장 용도로 만들어질 데이터베이스의 이름을 지정합니다. 기본값은 *KAV*입니다.

12단계. 인증 모드 선택

중앙 관리 서버를 DBMS(데이터베이스 관리 시스템)에 연결하는 데 사용될 인증 모드를 결정합니다.

선택한 DBMS에 따라 다음 인증 모드를 선택할 수 있습니다:

- SQL Express 또는 Microsoft SQL Server의 경우 다음 옵션 중 하나를 선택합니다:
  - **Microsoft Windows 인증 모드**. 중앙 관리 서버를 시작한 계정을 사용하여 권한이 확인됩니다.
  - **SQL 서버 인증 모드**. 이 옵션을 선택하면 이 창에 지정된 계정을 사용하여 접근 권한을 확인합니다. **계정** 및 **암호** 필드를 입력합니다.

    입력한 암호를 보려면 **보기** 버튼을 길게 누릅니다.

애플리케이션은 두 인증 모드에서 모두 데이터베이스를 사용할 수 있는지 확인합니다. 데이터베이스를 사용할 수 없으면 오류 메시지가 표시되며, 올바른 자격증명을 입력해야 합니다.

중앙 관리 서버 데이터베이스가 다른 기기에 저장되어 있고 중앙 관리 서버 계정에 데이터베이스 서버 접근 권한이 없으면 중앙 관리 서버를 설치하거나 업그레이드하는 동안 SQL Server 인증 모드를 사용해야 합니다. 이것은 데이터베이스를 저장하는 기기가 도메인 외부에 있거나 중앙 관리 서버가 LocalSystem 계정 아래에 설치된 경우에 적용됩니다.

MySQL, MariaDB, PostgreSQL, Postgres Pro은 계정과 암호를 지정합니다.

13단계. 중앙 관리 서버를 시작할 계정 선택

서비스로 중앙 관리 서버를 시작하는 데 사용할 계정을 선택합니다.

- **자동으로 계정 생성**. 이 애플리케이션은 kladminserver 서비스를 실행하기 위해 KL-AK-*로 시작하는 계정을 만듭니다.

  공유 폴더와 DBMS를 중앙 관리 서버와 동일한 기기에서 운영할 계획이라면 이 옵션을 선택할 수 있습니다.

- **계정 선택**. 중앙 관리 서버 서비스(kladminserver)가 사용자가 선택한 계정을 사용해 실행됩니다.

  만일 다른 기기에 있는 SQL Express를 포함한 모든 버전의 SQL Server 인스턴스를 DBMS로 사용하려는 경우 및/또는 다른 기기에 있는 공유 폴더를 사용할 계획이라면 도메인 계정을 선택해야 합니다.

  Kaspersky Security Center는 MSA(관리 서비스 계정)와 gMSA(그룹 관리 서비스 계정)를 지원합니다. 이러한 유형의 계정이 사용자 도메인에서 사용되면 중앙 관리 서버 서비스용 계정으로 그 중 하나를 선택할 수 있습니다.

  MSA 또는 gMSA를 지정하기 전에 중앙 관리 서버를 설치할 동일한 기기에 계정을 설치해야 합니다. 계정이 아직 설치되지 않은 경우 중앙 관리 서버 설치를 취소하고 계정을 설치한 다음 중앙 관리 서버를 다시 설치하십시오. 로컬 기기에 관리 중인 서비스 계정을 설치하는 방법에 대한 자세한 내용은 공식 Microsoft 설명서를 참조하십시오.

  MSA 또는 gMSA를 지정하려면 다음을 수행하십시오.

  1. **찾기** 버튼을 누릅니다.
  2. 열리는 창에서 **개체 유형** 버튼을 누릅니다.
  3. **서비스 계정** 유형을 선택하고 **확인**을 누릅니다.
  4. 관련 계정을 선택하고 **확인**을 누릅니다.

선택한 계정에는 사용하려는 DBMS에 따라 다른 권한을 가지고 있어야 합니다.

보안 문제로 인해 중앙 관리 서버를 실행하는 계정에 이 권한을 할당하지 마십시오.

중앙 관리 서버 계정은 나중에 변경할 수 없습니다. 다른 중앙 관리 서버 계정을 사용하려면 장애 조치 클러스터를 다시 설치해야 합니다.

14단계. Kaspersky Security Center 서비스를 실행하기 위한 계정 선택

이 기기에서 Kaspersky Security Center 서비스를 실행하는 데 사용할 계정을 선택합니다:

- **자동으로 계정 생성**. Kaspersky Security Center는 kladmins 그룹에 소속된 KlScSvc라는 로컬 계정을 만듭니다. Kaspersky Security Center 서비스는 생성된 계정으로 실행됩니다.
- **계정 선택**. Kaspersky Security Center 서비스는 사용자가 선택한 계정으로 실행됩니다.

  예를 들어 리포트를 다른 기기에 있는 폴더에 저장하려는 경우 또는 조직의 보안 정책일 경우에는 도메인 계정을 선택해야 합니다. Failover 클러스터에 중앙 관리 서버를 설치하려는 경우에도 도메인 계정을 선택해야 할 수 있습니다.

보안 문제로 인해 이 서비스를 실행하는 계정에는 권한을 부여하지 마십시오.

KSN 프록시 서비스(ksnproxy), Kaspersky 활성화 프록시 서비스(klactprx) 및 Kaspersky 인증 포털 서비스(klwebsrv)는 선택한 계정으로 실행됩니다.

15단계. 공유 폴더 선택

다음 작업에 사용될 공유 폴더의 이름과 위치를 정의합니다:

- 애플리케이션의 원격 설치에 필요한 파일 저장(이러한 파일은 설치 패키지를 만드는 동안 중앙 관리 서버로 복사됨).
- 업데이트 경로에서 다운로드한 업데이트를 중앙 관리 서버에 저장.

파일 공유(읽기 전용)는 모든 사용자가 사용할 수 있습니다.

다음 옵션 중 하나를 선택하실 수 있습니다:

- **공유 폴더 만들기**. 새 폴더를 만듭니다. 텍스트 상자에 폴더 경로를 지정합니다.
- **기존 공유 폴더 선택**. 기존 공유 폴더를 하나 선택합니다.

공유 폴더는 설치에 사용된 기기의 로컬 폴더 또는 회사 네트워크에 있는 클라이언트 기기의 원격 디렉터리일 수 있습니다. **찾기** 버튼을 눌러 공유 폴더를 선택하거나 해당 필드에 UNC 경로(예: \\server\Share)를 직접 지정할 수도 있습니다.

기본적으로 설치 프로그램은 Kaspersky Security Center의 구성 요소가 포함된 애플리케이션 폴더에 KLSHARE 로컬 하위 폴더를 생성합니다.

필요하다면 나중에 공유 폴더를 정의할 수 있습니다.

16단계. 중앙 관리 서버에 대한 연결 구성

중앙 관리 서버에 대한 연결을 구성합니다:

- **Port**

  중앙 관리 서버에 연결하는 데 사용되는 포트 번호입니다.
  기본 포트 번호는 14000입니다.

- **SSL 포트**

  SSL(Secure Sockets Layer)을 통해 중앙 관리 서버에 안전하게 연결하는 데 사용되는 SSL 포트 번호입니다.
  기본 포트 번호는 13000입니다.

- **암호화 키 길이**

  암호화 키의 길이(1024비트 또는 2048비트)를 선택합니다.

  1024비트 암호화 키의 경우 CPU에 대한 부하는 더 적지만 기술 사양으로 인해 안정적인 암호화 기능을 제공하지 못하기 때문에 오래된 기술로 간주됩니다. 또한 1024비트 키를 사용하는 SSL 인증서와 기존 하드웨어가 호환되지 않을 가능성이 높습니다.

  2048비트 암호화 키는 최신 암호화 표준을 모두 충족합니다. 그러나 2048비트 암호화 키를 사용하는 경우 CPU에 대한 부하가 추가될 수 있습니다.

  기본적으로 **2048비트 (최고의 보안)**가 선택됩니다.

나중에 중앙 관리 서버에 연결하기 위한 파라미터를 다음과 같이 변경할 수도 있습니다.

- 중앙 관리 서버 속성의 **연결 포트** 섹션에서 포트 및 SSL 포트 번호를 변경할 수 있습니다. 중앙 관리 서버 연결 포트에 대한 자세한 내용은 Kaspersky Security Center에서 사용하는 포트를 참조하십시오.

- 중앙 관리 서버 인증서를 klsetsrvcert 유틸리티로 교체할 때 `-o RsaKeyLen:<키 길이>` 파라미터를 사용하여 암호화 키 길이를 변경할 수 있습니다.

17단계. 중앙 관리 서버 주소 정의

중앙 관리 서버 주소를 지정하십시오. 다음 옵션 중 하나를 선택할 수 있습니다:

- **DNS 도메인 이름**. 이 방법은 네트워크에 DNS 서버가 포함되어 있고 클라이언트 기기가 이를 사용하여 중앙 관리 서버 주소를 수신할 수 있는 경우에 유용합니다.

- **NetBIOS 이름**. 이 방법은 클라이언트 기기가 NetBIOS 프로토콜을 통해 중앙 관리 서버 주소를 수신하거나 네트워크에 WINS 서버를 사용할 수 있는 경우에 유용합니다.

- **IP 주소**. 이 방법은 중앙 관리 서버에 큰 변화가 없는 정적 IP 주소가 있는 경우에 사용됩니다.

18단계. 모바일 기기 연결에 사용할 중앙 관리 서버 주소

설치 시 모바일 기기 매니지먼트를 선택했다면 이 설치 마법사를 사용할 수 있습니다.

모바일 기기 연결용 주소 창에서 로컬 네트워크 외부에 있는 모바일 기기 연결을 위한 중앙 관리 서버의 외부 주소를 지정하십시오. 중앙 관리 서버의 IP 주소 또는 DNS(Domain Name System)를 지정할 수 있습니다.

19단계. 하드 드라이브에 파일 압축 해제 및 설치

Kaspersky Security Center 구성 요소 설치에 대한 구성이 완료되었으면 하드 드라이브에 파일 설치를 시작할 수 있습니다.

설치에 추가 프로그램이 필요하다면 설치 마법사는 Kaspersky Security Center를 설치하기 전에 **필수 구성 요소 설치** 페이지에 이를 표시합니다. **다음** 버튼을 누르면 필수 프로그램이 자동으로 설치됩니다.

마지막 페이지에서 Kaspersky Security Center 사용을 위해 시작할 콘솔을 선택할 수 있습니다:

- **MMC 기반 관리 콘솔 시작**
- **Kaspersky Security Center 웹 콘솔 시작**

  이 옵션은 이전 단계 중 하나에서 Kaspersky Security Center 웹 콘솔을 설치하도록 선택했을 때만 사용할 수 있습니다.

마침을 눌러 Kaspersky Security Center 사용을 시작하지 않고 마법사를 닫을 수도 있습니다. 나중에 언제든지 작업을 시작할 수 있습니다.

관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 처음 시작할 때 애플리케이션 초기 설정을 수행할 수 있습니다.

숨김 모드로 중앙 관리 서버 설치

중앙 관리 서버는 사용자가 설치 설정을 직접 입력할 필요 없는 숨김 모드로 설치할 수 있습니다.

중앙 관리 서버를 숨김 모드로 로컬 기기에 설치하려면:

1. 최종 사용자 라이센스 계약서를 읽어 보십시오. 최종 사용자 라이센스 계약서의 조건을 이해하고, 이에 동의하는 경우에만 아래 명령을 사용하십시오.
2. 개인정보취급방침을 읽어보십시오. 데이터가 개인정보취급방침의 설명대로 취급 및 전송(제삼국으로의 전송도 포함)될 수 있다는 점을 이해하고, 이에 동의하는 경우에만 아래 명령을 사용하십시오.
3. 다음 명령 실행

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"
```

여기서 설치_파라미터는 공백으로 구분된 파라미터 및 해당 값 목록입니다(`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). setup.exe 파일은 Kaspersky Security Center 배포 키트에 포함된 Server 폴더에 있습니다.

아래 표에는 숨김 모드로 중앙 관리 서버를 설치할 때 사용할 수 있는 파라미터의 이름과 가능한 값이 나와 있습니다.

숨김 모드의 중앙 관리 서버 설치 파라미터

파라미터 이름	파라미터 설명	사용 가능한 값
EULA	라이센스 계약서 조건에 동의.	• 1 – 최종 사용자 라이센스 계약서의 조건을 모두 읽고 이해했으며, 이에 동의합니다. • 다른 값 및 값 없음 – 라이센스 계약서 조건에 동의하지 않음(설치가 수행되지 않음).
PRIVACYPOLICY	개인정보취급방침 조건에 동의.	• 1 – 개인정보취급방침에 설명된 대로 제 데이터가 처리되고 전송(제3국으로의 전송 포함)되는 것을 알고 있으며 이에 동의합니다. 개인정보취급방침을 모두 읽고 이해했음을 확인합니다. • 다른 값 및 값 없음 - 개인정보취급방침 조건에 동의하지 않음(설치가 수행되지 않음).
INSTALLATIONMODETYPE	중앙 관리 서버 설치 유형.	• 표준 – 표준 설치. • 사용자 지정 – 사용자 지정 설치.
INSTALLDIR	중앙 관리 서버 설치 폴더 경로.	문자열 값.
ADDLOCAL	설치할 중앙 관리 서버 구성 요소 목록(쉼표로 구분).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 중앙 관리 서버를 적절히 설치하기 위한 최소한의 구성 요소 목록: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.
NETRANGETYPE	네트워크 규모(네트워크 내 기기 수).	• NRT_1_100—1대 ~ 100대. • NRT_100_1000—101~1000대. • NRT_GREATER_1000 - 기기 1000대 초과.
SRV_ACCOUNT_TYPE	중앙 관리 서버를 서비스로 실행할 계정을 지정하는 모드.	• SrvAccountDefault – 계정이 자동으로 생성됩니다. • SrvAccountUser - 사용자 계정을 수동으로 정의됩니다. 이 경우 `SERVERACCOUNTNAME` 및 `SERVERACCOUNTPWD` 파라미터의 값을 지정해야 합니다.
SERVERACCOUNTNAME	중앙 관리 서버를 서비스로 실행할 계정 이름. 만일 SRV_ACCOUNT_TYPE=SrvAccountUser라면 파라미터 값을 지정해야 합니다.	문자열 값.
SERVERACCOUNTPWD	서비스로 중앙 관리 서버를 시작하는 데 사용할 계정의 암호. 만일 SRV_ACCOUNT_TYPE=SrvAccountUser라면 파라미터 값을 지정해야 합니다.	문자열 값.
SERVERCER	중앙 관리 서버 인증서용 키 길이(비트).	• 1 – 중앙 관리 서버 인증서용 키 길이는 2,048비트입니다. • 값 없음 - 중앙 관리 서버 인증서용 키 길이는 1024 비트입니다.
DBTYPE	중앙 관리 서버의 데이터베이스를 저장하기 위해 사용되는 데이터베이스의 유형입니다. 이 파라미터는 필수입니다.	• MySQL – MySQL 또는 MariaDB 데이터베이스가 사용됩니다. 이때, `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME`, `MYSQLACCOUNTPWD` 파라미터의 값을 지정해야 합니다. • MSSQL – Microsoft SQL Server(SQL Express) 데이터베이스가 사용됩니다. 이때, `MSSQLSERVERNAME`, `MSSQLDBNAME`, `MSSQLAUTHTYPE` 파라미터의 값을 지정해야 합니다. • POSTGRES - PostgreSQL 또는 Postgres Pro 데이터베이스를 사용합니다. 이때, `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME`, `POSTGRESACCOUNTPWD` 파라미터의 값을 지정해야 합니다.
MYSQLSERVERNAME	SQL Server의 전체 이름. DBTYPE=MySQL인 경우 파라미터 값을 지정해야 합니다.	문자열 값.

파라미터 이름	파라미터 설명	사용 가능한 값
MYSQLSERVERPORT	SQL Server에 연결할 포트 번호. DBTYPE=MySQL인 경우 파라미터 값을 지정해야 합니다.	숫자 값.
MYSQLDBNAME	중앙 관리 서버의 데이터를 저장하기 위해 생성되는 데이터베이스의 이름입니다. DBTYPE=MySQL인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
MYSQLACCOUNTNAME	데이터베이스에 연결할 계정의 이름. DBTYPE=MySQL인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
MYSQLACCOUNTPWD	데이터베이스에 연결할 계정의 암호. DBTYPE=MySQL인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
MSSQLSERVERNAME	SQL Server의 전체 이름. DBTYPE=MSSQL인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
MSSQLDBNAME	데이터베이스 이름. DBTYPE=MSSQL인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
MSSQLAUTHTYPE	SQL Server에 연결 시 사용할 인증 유형. DBTYPE=MSSQL일 시, 파라미터 값을 지정해야 합니다.	• Windows – Microsoft Windows 인증 모드. • SQLServer – SQL 서버 인증 모드. 이때, MSSQLACCOUNTNAME 및 MSSQLACCOUNTPWD 파라미터의 값을 지정해야 합니다.
MSSQLACCOUNTNAME	SQL Server에 연결할 계정의 이름. MSSQLAUTHTYPE=SQLServer인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
MSSQLACCOUNTPWD	SQL Server에 연결할 계정의 암호. MSSQLAUTHTYPE=SQLServer인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
CREATE_SHARE_TYPE	공유 폴더를 지정하는 방법.	• Create - 새 공유 폴더 만들기. 이때, SHARELOCALPATH 및 SHAREFOLDERNAME 파라미터의 값을 지정해야 합니다. • ChooseExisting – 기존 폴더를 선택합니다. 이때, EXISTSHAREFOLDERNAME 파라미터의 값을 지정해야 합니다.
SHARELOCALPATH	로컬 폴더의 전체 경로. 다음인 경우 파라미터 값을 지정해야 합니다 CREATE_SHARE_TYPE=Create	문자열 값.
SHAREFOLDERNAME	공유 폴더의 네트워크 이름. CREATE_SHARE_TYPE=Create인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
EXISTSHAREFOLDERNAME	기존 공유 폴더의 전체 경로. CREATE_SHARE_TYPE=ChooseExisting인 경우 파라미터 값을 지정해야 합니다.	문자열 값.
SERVERPORT	중앙 관리 서버에 연결할 포트 번호입니다.	숫자 값.
SERVERSSLPORT	SSL 프로토콜을 사용하여 중앙 관리 서버에 암호화된 연결을 설정하기 위한 포트 번호.	숫자 값.
SERVERADDRESS	중앙 관리 서버 주소.	문자열 값.
MOBILESERVERADDRESS	모바일 기기 연결에 사용할 중앙 관리 서버 주소.	문자열 값.

중앙 관리 서버 설치 파라미터에 대한 자세한 설명은 사용자 지정 설치 섹션을 참조하십시오.

관리자의 워크스테이션에 관리 콘솔 설치

관리자의 워크스테이션에 관리 콘솔을 별도로 설치하고 이 콘솔을 사용하여 네트워크를 통해 중앙 관리 서버를 관리할 수 있습니다.

관리자의 워크스테이션에 관리 콘솔을 설치하려면 다음과 같이 하십시오:

1. setup.exe 실행 파일을 실행합니다.

   설치할 Kaspersky 애플리케이션을 묻는 창이 열립니다.

2. 애플리케이션 선택 창에서 **Kaspersky Security Center 관리 콘솔만 설치** 링크를 클릭하여 관리 콘솔 설치 마법사를 실행합니다. 마법사의 지침을 따릅니다.

3. 대상 폴더를 선택합니다. 기본적으로 <디스크>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console이 대상 폴더로 설정됩니다. 이 폴더가 없는 경우에는 설치를 진행하는 동안 자동으로 생성됩니다. **찾기** 버튼을 사용하여 대상 폴더를 변경할 수 있습니다.

4. 설치 마법사의 마지막 단계에서 **시작** 버튼을 눌러 관리 콘솔 설치를 시작합니다.

   마법사가 작업을 완료하면 관리 콘솔이 관리자의 워크스테이션에 설치됩니다.

숨김 모드에서 관리자의 워크스테이션에 관리 콘솔을 설치하는 방법:

1. 최종 사용자 라이센스 계약서를 읽어 보십시오. 최종 사용자 라이센스 계약서의 조건을 이해하고, 이에 동의하는 경우에만 아래 명령을 사용하십시오.

2. Kaspersky Security Center 배포 키트의 `Distrib\Console` 폴더에서 다음 명령을 사용하여 setup.exe 파일을 실행합니다.

   ```
   setup.exe /s /v"EULA=1"
   ```

   관리 콘솔과 함께 `Distrib\Console\Plugins` 폴더에서 모든 관리 플러그인을 설치하려면 다음 명령을 실행하십시오.

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   관리 콘솔과 함께 `Distrib\Console\Plugins` 폴더에서 설치할 관리 플러그인을 지정하려면 '/p' 키 뒤에 플러그인을 지정하고 세미콜론으로 구분합니다.

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   여기서 `P1`, `P2`, `P3`은 `Distrib\Console\Plugins` 폴더의 플러그인 폴더 이름에 해당하는 플러그인 이름입니다. 예:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

   관리 콘솔 및 관리 플러그인(있는 경우)이 관리자 워크스테이션에 설치됩니다.

관리 콘솔이 설치되었으면 중앙 관리 서버에 연결해야 합니다. 이렇게 하려면, 관리 콘솔을 실행하고 열리는 창에서 중앙 관리 서버가 설치된 기기의 이름이나 IP 주소를 지정하고 연결에 사용된 사용자 계정의 설정도 지정합니다. 중앙 관리 서버에 연결되면 관리 콘솔을 사용하여 안티 바이러스 보호 시스템을 관리할 수 있습니다.

관리 콘솔은 표준 Microsoft Windows 추가/제거 툴을 사용하여 제거할 수 있습니다.

Kaspersky Security Center 설치 후 시스템 변경 사항

관리 콘솔 아이콘

기기에 관리 콘솔이 설치되면 해당 아이콘이 표시되고 이 아이콘을 사용하여 관리 콘솔을 실행할 수 있습니다. **시작 → 프로그램 → Kaspersky Security Center** 메뉴의 관리 콘솔에서 찾을 수 있습니다.

중앙 관리 서버 및 네트워크 에이전트 서비스

중앙 관리 서버와 네트워크 에이전트가 기기에 아래 나열된 속성과 함께 서비스로 설치됩니다. 또한 이 표에는 중앙 관리 서버 설치 후 기기에 적용되는 다른 서비스의 특성도 표시되어 있습니다.

Kaspersky Security Center 서비스 속성

구성 요소	서비스 이름	표시되는 서비스 이름	계정
중앙 관리 서버	kladminserver	Kaspersky Security Center 중앙 관리 서버	설치 중에 생성된 KL-AK-* 형식으로 된 사용자 정의 또는 전용 권한이 제한된 계정
네트워크 에이전트	klnagent	Kaspersky Security Center 네트워크 에이전트	로컬 시스템
Kaspersky Security Center 웹 콘솔에 접근하여 조직 인트라넷을 관리하기 위한 웹 서버	klwebsrv	Kaspersky 웹 서버	권한이 부여 안 된 전용 KlScSvc 계정
활성화 프록시 서버	klactprx	Kaspersky 활성화 프록시 서버	권한이 부여 안 된 전용 KlScSvc 계정
KSN 프록시 서버	ksnproxy	Kaspersky Security Network 프록시 서버	권한이 부여 안 된 전용 KlScSvc 계정

Kaspersky Security Center 장애 조치 클러스터 노드에 Kaspersky Security Center를 설치하면 klfocsvc_klfoc 서비스를 사용할 수 있게 됩니다. klnagent_klfoc 및 klfocsvc_klfoc 서비스는 로컬 시스템 계정으로 실행됩니다. kladminserver_klfoc 서비스는 'ksc' 계정으로, 다른 서비스는 'rightless' 계정으로 실행해야 합니다. 'ksc' 및 'rightless' 계정은 로컬 관리자 권한으로 KLAdmins 그룹에 추가해야 합니다. Kaspersky Security Center가 올바르게 작동하려면 서비스 실행에 'ksc' 및 'rightless' 계정만 사용해야 합니다. 같은 권한을 가진 다른 계정을 사용하는 것은 권장하지 않습니다. 아래 표는 Kaspersky Security Center 장애 조치 클러스터에 중앙 관리 서버를 설치한 후 기기에 적용되는 서비스 속성을 포함합니다.

Kaspersky Security Center 장애 조치 클러스터에 설치된 Kaspersky Security Center 서비스 속성

구성 요소	서비스 이름	표시되는 서비스 이름	계정
중앙 관리 서버	kladminserver_klfoc	Kaspersky Security Center 중앙 관리 서버	ksc
네트워크 에이전트	klnagent_klfoc	Kaspersky Security Center 네트워크 에이전트	로컬 시스템
Kaspersky Security Center 웹 콘솔에 접근하여 조직 인트라넷을 관리하기 위한 웹 서버	klwebsrv_klfoc	Kaspersky 웹 서버	rightless
활성화 프록시 서버	klactprx_klfoc	Kaspersky 활성화 프록시 서버	rightless
KSN 프록시 서버	ksnproxy_klfoc	Kaspersky Security Network 프록시 서버	rightless
Kaspersky Security Center 장애 조치 클러스터	klfocsvc_klfoc	Kaspersky Security Center 장애 조치 클러스터	로컬 시스템

Kaspersky Security Center 웹 콘솔 서비스

Kaspersky Security Center 웹 콘솔을 기기에 설치하면 다음 서비스가 배포됩니다(아래 표 참조):

Kaspersky Security Center 웹 콘솔 서비스

표시되는 서비스 이름	계정
Kaspersky Security Center 서비스 웹 콘솔	NT 서비스/KSCSvcWebConsole
Kaspersky Security Center 웹 콘솔	네트워크 서비스
Kaspersky Security Center 제품 플러그인 서버	NT 서비스/KSCWebConsolePlugin

Kaspersky Security Center Web Console Management Service	로컬 시스템
Kaspersky Security Center Web Console Message Queue	NT 서비스/KSCWebConsoleMessageQueue

네트워크 에이전트 서버 버전

네트워크 에이전트의 서버 버전은 중앙 관리 서버와 함께 운영하는 기기에 설치됩니다. 중앙 관리 서버의 일부 구성 요소인 서버 버전의 네트워크 에이전트는 중앙 관리 서버와 함께 설치되며 로컬에 설치된 중앙 관리 서버하고만 상호 작용할 수 있습니다. 중앙 관리 서버로 네트워크 에이전트 연결을 구성할 필요가 없습니다. 해당 구성 요소는 동일한 기기에 설치되기 때문에 구성은 자동으로 적용됩니다. 서버 버전의 네트워크 에이전트는 표준 네트워크 에이전트와 같은 속성으로 설치되며 동일한 애플리케이션 관리 기능을 수행합니다. 이 버전은 중앙 관리 서버의 클라이언트 기기가 속하는 관리 그룹의 정책에 의해 관리됩니다. 서버 버전의 네트워크 에이전트의 경우, 서버 변경 작업을 제외한 모든 작업은 중앙 관리 서버에 제공된 작업 범위에서 생성됩니다.

네트워크 에이전트는 이미 중앙 관리 서버가 설치된 기기에 별도로 설치할 수 없습니다.

중앙 관리 서버와 네트워크 에이전트의 각 서비스의 속성을 볼 수 있을 뿐만 아니라 표준 Microsoft Windows 관리 도구: 컴퓨터 관리\서비스를 사용하여 작동을 모니터링할 수 있습니다. Kaspersky 중앙 관리 서버 서비스의 활동에 관한 정보는 중앙 관리 서버가 설치된 기기의 별도 Kaspersky 이벤트 로그 분기 내의 Microsoft Windows 시스템 로그에 저장됩니다.

서비스를 수동으로 시작하거나 중지하지 말고 해당 서비스 설정의 서비스 계정을 변경하지 말고 그대로 둘 것을 권장합니다. 필요한 경우 klsrvswch 유틸리티를 사용하여 중앙 관리 서버 서비스 계정을 수정할 수 있습니다. 중앙 관리 서버 설치에 사용된 관리자 권한이 있는 계정으로 중앙 관리 서버 기기에서 klsrvswch 유틸리티를 시작해야 합니다.

사용자 계정 및 보안 그룹

중앙 관리 서버 설치 프로그램은 기본적으로 다음 계정을 생성합니다:

- KL-AK-*: 중앙 관리 서버 서비스 계정
- KlScSvc: 중앙 관리 서버 풀의 기타 서비스용 계정
- KlPxeUser: 운영 체제 배포용 계정

설치 프로그램을 실행하는 동안 중앙 관리 서버 서비스 및 기타 서비스에 대해 다른 계정을 선택하면 지정된 계정이 사용됩니다.

KLAdmins와 KLOperators로 명명된 로컬 보안 그룹이 각 권한과 함께 중앙 관리 서버가 설치된 기기에 자동으로 생성됩니다.

도메인 컨트롤러에 중앙 관리 서버를 설치하지 않는 것이 좋으나 도메인 컨트롤러에 중앙 관리 서버를 설치하는 경우 도메인 관리자 권한으로 설치 프로그램을 시작해야 합니다. 이 경우 설치 프로그램은 KLAdmins와 KLOperators로 명명된 도메인 보안 그룹을 자동으로 생성합니다. 도메인 컨트롤러가 아닌 기기에 중앙 관리 서버를 설치하는 경우에는 대신 로컬 관리자 권한으로 설치 프로그램을 시작해야 합니다. 이 경우 설치 프로그램은 KLAdmins와 KLOperators로 명명된 로컬 보안 그룹을 자동으로 생성합니다.

이메일 알림을 구성할 때 ESMTP 인증용 메일 서버 계정을 만들어야 할 수 있습니다.

애플리케이션 제거

Kaspersky Security Center는 표준 Microsoft Windows 추가/제거 툴을 사용하여 제거할 수 있습니다. 애플리케이션을 제거하려면 플러그인을 비롯한 모든 애플리케이션 구성 요소를 기기에서 제거하는 마법사를 시작해야 합니다. 마법사는 Kaspersky Security Center 사용을 중지한 이유를 묻는 설문 조사 웹 페이지를 기본 브라우저에서 열도록 합니다. 마법사를 진행하는 동안 공유 폴더(KLSHARE) 제거를 선택하지 않았다면 모든 관련 작업이 완료된 후에 이 폴더를 직접 삭제할 수 있습니다.

애플리케이션이 제거된 후 시스템의 임시 폴더에 파일 중 일부가 남아 있을 수 있습니다.

애플리케이션 제거 작업 생성 마법사가 중앙 관리 서버의 백업 복사본을 저장하라는 메시지가 표시됩니다.

Microsoft Windows 7 및 Microsoft Windows 2008에서 애플리케이션이 제거되면 애플리케이션 제거 작업 생성 마법사가 조기 종료될 수 있습니다. 운영 체제에서 UAC(사용자 계정 컨트롤)를 사용하지 않도록 설정하고 애플리케이션 제거를 다시 시작하면 이 현상이 나타나지 않습니다.

Kaspersky Security Center 업그레이드 정보

이 섹션은 이전 버전의 Kaspersky Security Center를 업그레이드하는 방법에 대한 정보를 포함합니다. Kaspersky Security Center의 설치 위치가 로컬인지 Kaspersky Security Center 장애 조치 클러스터 노드인지에 따라, Kaspersky Security Center 업그레이드 방법이 달라집니다.

업그레이이드 중에는 중앙 관리 서버와 다른 애플리케이션이 DBMS를 동시에 사용하도록 해서는 안 됩니다.

중앙 관리 서버를 버전 15.1로 업그레이드하면 네트워크 에이전트 버전 15 이하의 설치 패키지를 새로 생성할 수 없습니다. 그러나 이전에 만든 설치 패키지는 사용할 수 있습니다.

Kaspersky Security Center를 이전 버전에서 업그레이드하면, 지원하는 Kaspersky 애플리케이션에 설치한 모든 플러그인이 유지됩니다. 중앙 관리 서버 플러그인 및 네트워크 에이전트 플러그인은 자동 업그레이드됩니다(관리 콘솔 및 Kaspersky Security Center 웹 콘솔 모두).

이전 버전에서 Kaspersky Security Center 업그레이드

Kaspersky Security Center 및 관리 중인 보안 애플리케이션 업그레이드 주제에서 권장되는 업그레이드 준비 단계에 관해 설명합니다.

이전 버전의 중앙 관리 서버(버전 11 이상(11.0.0.1131b))가 설치된 기기에 중앙 관리 서버 15.1 버전을 설치할 수 있습니다. 15.1 버전으로 업그레이드할 때, 중앙 관리 서버의 모든 이전 버전 데이터 및 설정은 저장됩니다.

중앙 관리 서버 설치를 진행하는 동안 문제가 발생하면 업그레이드 전에 만든 중앙 관리 서버 데이터의 백업 복사본을 사용하여 중앙 관리 서버의 이전 버전을 복구할 수 있습니다.

네트워크에 새 버전의 중앙 관리 서버가 1대 이상 설치되어 있다면, 중앙 관리 서버 설치 패키지를 사용하는 원격 설치 작업을 사용하여 이 네트워크에 있는 다른 중앙 관리 서버를 업그레이드할 수 있습니다.

Kaspersky Security Center 장애 조치 클러스터를 배포했다면 해당 노드에서 Kaspersky Security Center를 업그레이드할 수도 있습니다.

이전 버전의 중앙 관리 서버를 15.1 버전으로 업그레이드하려면 다음과 같이 하십시오.

1. 버전 15.1에 대한 ksc_15.1_<build number>_full_<language>.exe 설치 파일을 실행합니다(이 파일은 Kaspersky 웹사이트에서 다운로드할 수 있습니다.)

2. 창이 열리면 **Kaspersky Security Center 설치** 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

3. 라이센스 계약서 및 개인정보취급방침을 읽어봅니다. 라이센스 계약서 및 개인정보취급방침의 조건에 동의하면 **나는 다음 내용을 모두 읽고 이해했으며 수락하는 것에 동의합니다** 섹션의 확인란을 선택합니다:

   - **이 최종 사용자 라이센스 계약서의 이용 약관**
   - **데이터 처리에 대한 개인정보취급방침**

   두 개의 확인란을 모두 선택한 이후 기기에 애플리케이션을 계속 설치할 수 있습니다. 설치 마법사에서 이전 버전의 중앙 관리 서버 데이터 백업을 만들라는 메시지를 표시합니다.

   Kaspersky Security Center는 이전 버전의 중앙 관리 서버에서 생성된 백업 복사본을 통한 데이터 복구를 지원합니다.

4. **중앙 관리 서버 데이터 백업** 창이 열리면 중앙 관리 서버 데이터의 백업 생성을 지정할 수 있습니다.

   klbackup 유틸리티가 백업을 생성합니다. 이 유틸리티는 배포 키트에 포함되어 있으며 Kaspersky Security Center 설치 폴더의 루트에서 찾을 수 있습니다.

5. 설치 마법사에 따라 중앙 관리 서버 버전 15.1를 설치합니다.

   Kaspersky Security Center 웹 콘솔 서비스가 과부하 상태라는 메시지가 나타나면 마법사 창에서 **무시** 버튼을 클릭합니다.

   설치 마법사를 중단하지 마십시오. 중앙 관리 서버 설치 단계에서 업그레이드를 취소하면 Kaspersky Security Center의 업그레이드된 버전에서 오류가 발생할 수 있습니다.

6. 기기에 이전 버전의 네트워크 에이전트가 설치되어 있으면 최신 버전의 네트워크 에이전트에 대한 원격 설치 작업을 만들어 실행합니다.

   Linux용 네트워크 에이전트를 Kaspersky Security Center와 같은 버전으로 업그레이드할 것을 권장합니다.

   원격 설치 작업을 완료하면 네트워크 에이전트 버전이 업그레이드됩니다.

Linux 기반 에셋에 대해 다음 명령을 실행하여 더 이상 필요하지 않은 종속성을 제거합니다.

- Debian 기반 에셋의 경우 다음 명령 중 하나를 실행합니다.
  - `apt-get -y autoremove`
  - `apt -y autoremove`
- RPM 기반 에셋의 경우 다음 명령 중 하나를 실행합니다.
  - `dnf autoremove`
  - `yum autoremove`

Kaspersky Security Center 장애 조치 클러스터 노드에 Kaspersky Security Center 업그레이드

이전 버전의 중앙 관리 서버(버전 13.2부터)가 설치된 모든 Kaspersky Security Center 장애 조치 클러스터 노드에 중앙 관리 서버 버전 15.1을 설치할 수 있습니다. 15.1 버전으로 업그레이드할 때, 중앙 관리 서버의 모든 이전 버전 데이터 및 설정은 저장됩니다.

이전에 기기에 Kaspersky Security Center를 로컬로 설치했다면, 해당 기기에서 Kaspersky Security Center를 업그레이드할 수도 있습니다.

Kaspersky Security Center 장애 조치 클러스터 노드에서 Kaspersky Security Center를 업그레이드하려면:

1. 클러스터의 액티브 노드에서 다음 작업을 수행합니다.
   a. ksc_15.1_<빌드 번호>_full_<언어>.exe 실행 파일을 실행합니다.
   업그레이드할 Kaspersky 애플리케이션을 선택하는 창이 열립니다. **Kaspersky Security Center 중앙 관리 서버 설치** 설치 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.
   b. 라이센스 계약서 및 개인정보취급방침을 읽어봅니다. 라이센스 계약서 및 개인정보취급방침의 조건에 동의하면 **나는 다음 내용을 모두 읽고 이해했으며 수락하는 것에 동의합니다** 섹션의 확인란을 선택합니다:
   - **이 최종 사용자 라이센스 계약서의 이용 약관**
   - **데이터 처리에 대한 개인정보취급방침**

   설치를 계속하려면 두 확인란을 모두 선택합니다.
   라이센스 계약서나 개인정보취급방침에 동의하지 않는다면 **취소** 버튼을 클릭하여 업그레이드를 취소하십시오.
2. Kaspersky Security Center 장애 조치 클러스터의 패시브 노드에서 액티브 노드와 같은 작업을 수행합니다.
3. 클러스터를 시작합니다 .

결과적으로 Kaspersky Security Center 장애 조치 클러스터 노드에 최신 버전의 중앙 관리 서버가 설치됩니다.

Microsoft 장애 조치 클러스터 노드에 Kaspersky Security Center 업그레이드

이전 버전의 중앙 관리 서버(버전 13.2부터)가 설치된 모든 Microsoft 장애 조치 클러스터 노드에 중앙 관리 서버 버전 15.1을 업그레이드할 수 있습니다. 15.1 버전으로 업그레이드할 때, 중앙 관리 서버의 모든 이전 버전 데이터 및 설정은 저장됩니다.

Microsoft 장애 조치 클러스터 노드에서 Kaspersky Security Center를 업그레이드하려면 클러스터의 아무 노드에서 다음 작업을 수행합니다.

1. ksc_15.1_<빌드 번호>_full_<언어>.exe 실행 파일을 실행합니다.

   업그레이드할 Kaspersky 애플리케이션을 선택하는 창이 열립니다. **Kaspersky Security Center 중앙 관리 서버 설치** 설치 링크를 눌러 중앙 관리 서버 설치 마법사를 시작합니다. 마법사의 지침을 따릅니다.

2. 라이센스 계약서 및 개인정보취급방침을 읽어봅니다. 라이센스 계약서 및 개인정보취급방침의 조건에 동의하면 **나는 다음 내용을 모두 읽고 이해했으며 수락하는 것에 동의합니다** 섹션의 확인란을 선택합니다:

   - **이 최종 사용자 라이센스 계약서의 이용 약관**
   - **데이터 처리에 대한 개인정보취급방침**

   설치를 계속하려면 두 확인란을 모두 선택합니다.

   라이센스 계약서나 개인정보취급방침에 동의하지 않는다면 **취소** 버튼을 클릭하여 업그레이드를 취소하십시오.

3. **클러스터에 대한 설치 유형** 창에서 **클러스터(모든 클러스터 노드에 설치)**를 선택합니다.

   그런 다음, 설치 프로그램은 클러스터의 모든 노드에서 중앙 관리 서버를 구성하고 업그레이드를 완료합니다. 업그레이드 중에는 중앙 관리 서버 설정을 변경할 수 없습니다.

결과적으로 Microsoft 장애 조치 클러스터 노드에 최신 버전의 중앙 관리 서버가 설치됩니다.

Kaspersky Security Center 초기 설정

이 섹션에서는 Kaspersky Security Center 설치 후에 초기 설정을 위해 수행해야 하는 단계를 설명합니다.

강화 가이드

강화 가이드는 Kaspersky Security Center를 설치 및 관리하는 전문가와 Kaspersky Security Center를 사용하는 조직에 기술 지원을 제공하는 전문가를 위한 자료입니다.

강화 가이드는 보안 문제 발생 위험을 줄이기 위한 Kaspersky Security Center 및 해당 구성 요소 구성의 권장 사항 및 기능을 설명합니다.

구성하기 전에, 중앙 관리 서버 데이터 백업 작업이나 klbackup 유틸리티를 사용하여 Kaspersky Security Center 중앙 관리 서버 백업 복사본을 생성하고 안전한 위치에 저장합니다.

강화 가이드는 다음 정보를 포함합니다.

- 중앙 관리 서버 아키텍처 선택
- 중앙 관리 서버에 대한 보안 연결 구성
- 중앙 관리 서버에 액세스하도록 계정 구성
- 중앙 관리 서버 및 클라이언트 기기의 보호 관리
- 관리 중인 애플리케이션에 대한 보호 구성
- 중앙 관리 서버 점검
- 타사 애플리케이션으로 정보 전송

중앙 관리 서버 작업을 시작하기 전에 Kaspersky Security Center가 짧은 버전의 강화 가이드를 읽으라는 메시지를 표시합니다.

강화 안내서를 읽었음을 확인하기 전에는 중앙 관리 서버를 사용할 수 없습니다.

강화 가이드를 읽으려면:

1. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 열고 콘솔에 로그인합니다. 콘솔은 강화 가이드의 현재 버전을 읽었다는 것을 확인했는지 검사합니다.

   강화 가이드를 아직 읽지 않았다면 창이 열리고 짧은 버전이 표시됩니다.

2. 다음 중 하나를 수행합니다:

   - 짧은 버전의 강화 가이드를 텍스트 문서로 보려면 **새 창에서 열기** 링크를 클릭합니다.
   - 강화 가이드의 전체 버전을 보려면 **온라인 도움말에서 보호 가이드 열기**를 클릭합니다.

3. 강화 가이드를 읽은 후 **보호 가이드를 모두 읽고 이해했음을 확인합니다** 확인란을 선택한 다음 **수락** 버튼을 클릭합니다.

이제 중앙 관리 서버로 작업할 수 있습니다.

강화 가이드의 새 버전이 나타나면 Kaspersky Security Center가 이를 읽어보라는 메시지를 표시합니다.

중앙 관리 서버 빠른 시작 마법사

이 섹션은 중앙 관리 서버 빠른 시작 마법사에 대한 정보를 제공합니다.

빠른 시작 마법사 정보

이 섹션은 중앙 관리 서버 빠른 시작 마법사에 대한 정보를 제공합니다.

중앙 관리 서버 빠른 시작 마법사를 사용하여 필요한 최소한의 작업 및 정책을 만들고, 최소 설정을 조정하고, 관리 중인 Kaspersky 애플리케이션의 플러그인을 다운로드 및 설치하고, 관리 중인 Kaspersky 애플리케이션의 설치 패키지를 만들 수 있습니다. 마법사가 실행 중일 때 애플리케이션을 다음과 같이 변경할 수 있습니다:

- 관리 중인 애플리케이션에 대한 플러그인을 다운로드하고 설치합니다. 빠른 시작 마법사가 완료되면 설치되어 있는 관리 플러그인 목록이 중앙 관리 서버 속성 창의 **고급 → 설치된 애플리케이션 관리 플러그인 세부 정보** 섹션에 표시됩니다.

- 관리 중인 Kaspersky 애플리케이션의 설치 패키지를 만듭니다. 빠른 시작 마법사가 완료되면 Windows용 네트워크 에이전트 및 관리 중인 Kaspersky 애플리케이션의 설치 패키지가 **중앙 관리 서버 → 고급 → 원격 설치 → 설치 패키지** 목록에 표시됩니다.

- 관리 그룹 내의 기기에 자동으로 배포될 수 있는 키 파일을 추가하거나 활성화코드를 입력합니다. 빠른 시작 마법사가 완료되면 라이센스 키에 관한 정보가 **중앙 관리 서버 → Kaspersky 라이센스** 목록과 중앙 관리 서버 속성 창의 **라이센스 키** 섹션에 표시됩니다.

- Kaspersky Security Network (KSN)와의 연동을 구성합니다.

- 중앙 관리 서버 및 관리되는 애플리케이션의 운영 중에 일어나는 이벤트를 알려주는 이메일 전달 기능을 설정합니다(성공적인 알림 전달을 위해서는 중앙 관리 서버 및 모든 수신 기기에 메신저 서비스가 실행되고 있어야 합니다). 빠른 시작 마법사가 완료되면 이메일 알림 설정이 중앙 관리 서버 속성 창의 **알림** 섹션에 표시됩니다.

- 기기에 설치된 애플리케이션의 업데이트 설정과 취약점 수정 설정을 조정합니다.

- 워크스테이션 및 서버용 보호 정책을 만들고 관리 중인 기기의 계층 구조 최상위 레벨에 대한 악성 코드 검사 작업, 업데이트 다운로드 작업 및 데이터 백업 작업을 만듭니다. 빠른 시작 마법사가 완료되면 생성된 작업이 **중앙 관리 서버 → 작업** 목록에 표시되고, 관리 중인 애플리케이션용 플러그인에 해당하는 정책이 **중앙 관리 서버 → 정책** 목록에 표시됩니다.

빠른 시작 마법사는 **관리 중인 기기** 그룹에 정책을 이미 만들지 않은 경우 Kaspersky Endpoint Security for Windows와 같은 관리 중인 애플리케이션에 대한 정책을 만듭니다. **관리 중인 기기** 그룹에 대하여 이름이 같은 작업이 존재하지 않는 경우 빠른 시작 마법사에서 작업을 만듭니다.

Kaspersky Security Center는 처음 시작한 후 빠른 시작 마법사를 실행하라는 메시지를 관리 콘솔에서 자동으로 표시합니다. 언제든지 수동으로 빠른 시작 마법사를 시작할 수도 있습니다.

중앙 관리 서버 빠른 시작 마법사 시작

애플리케이션은 중앙 관리 서버 설치 후 첫 연결 시 빠른 시작 마법사의 실행 여부를 자동으로 물어봅니다. 언제든지 수동으로 빠른 시작 마법사를 시작할 수도 있습니다.

빠른 시작 마법사를 수동으로 시작하려면:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.

2. 노드의 마우스 오른쪽 메뉴에서 **모든 작업 → 중앙 관리 서버 빠른 시작 마법사**를 선택합니다.

   마법사가 중앙 관리 서버의 초기 구성을 수행하라는 메시지를 표시합니다. 마법사의 지침을 따릅니다.

빠른 시작 마법사를 다시 시작하면 이전에 마법사를 실행하여 만들어진 작업과 정책을 다시 만들 수 없습니다.

1단계. 프록시 서버 구성

중앙 관리 서버의 인터넷 접속 설정을 지정합니다. Kaspersky Security Network를 사용하고, Kaspersky Security Center 및 관리 중인 Kaspersky 애플리케이션용 안티 바이러스 데이터베이스의 업데이트를 다운로드하려면 인터넷 접속을 구성해야 합니다.

인터넷에 연결할 때 프록시 서버를 사용하려면 **프록시 서버 사용** 옵션을 선택합니다. 이 옵션을 선택하면 설정을 입력하는 필드를 사용할 수 있게 됩니다. 프록시 서버 연결에 대해 다음 설정을 지정합니다.

- **주소**

  Kaspersky Security Center에서 인터넷 연결에 사용한 프록시 서버의 주소입니다.

- **포트 번호**

  Kaspersky Security Center 프록시 연결을 설정하는 데 사용되는 포트 번호입니다.

- **로컬 주소에서 프록시 서버 사용 안 함**

  로컬 네트워크에서 기기로 연결하는 데 프록시 서버가 사용되지 않습니다.

- **프록시 서버 인증**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.

  프록시 서버 사용 확인란을 선택하면 이 입력 필드를 사용할 수 있습니다.

- **사용자 이름**

  프록시 서버에 대한 연결을 구성할 사용자 계정입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

- **암호**

  프록시 서버 연결을 구성한 계정의 사용자가 설정한 암호입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

  입력한 암호를 보려면 **보기** 버튼을 필요한 시간 동안 누르고 있어야 합니다.

빠른 시작 마법사와는 별도로 나중에 인터넷 액세스를 구성할 수도 있습니다.

2단계. 애플리케이션 활성화 방법 선택

다음의 Kaspersky Security Center 활성화 옵션 중 하나를 선택합니다:

- **활성화코드 삽입**

  *활성화코드*는 20자의 숫자와 문자로 이루진 고유한 값입니다. Kaspersky Security Center를 활성화하는 키를 추가하기 위해 활성화코드를 입력합니다. Kaspersky Security Center 구매 후 지정한 이메일 주소를 통해 활성화코드를 받습니다.

  활성화 코드로 애플리케이션을 활성화하려면 Kaspersky 활성화 서버 연결을 위한 인터넷 액세스가 필요합니다.

  이 활성화 옵션을 선택했다면 **관리 중인 기기에 자동으로 라이센스 키 배포** 옵션을 활성화할 수 있습니다.

  이 옵션을 활성화하면 라이센스 키가 관리 중인 기기에 자동으로 배포됩니다.

  이 옵션을 비활성화하면 나중에 관리 콘솔 트리의 **Kaspersky 라이센스** 노드에서 관리 중인 기기로 라이센스 키를 배포할 수 있습니다.

  모종의이유로 활성화 코드 삽입을 통한 활성화에 실패할 경우 키 파일을 지정하여 애플리케이션을 활성화할 수 있습니다.

- **라이센스 키 파일 지정**

  *키 파일*은 Kaspersky에서 사용자에게 제공한 .key 확장자를 가진 파일입니다. 라이센스 키 파일은 애플리케이션을 활성화하는 키를 추가하기 위한 것입니다.

  키 파일을 가져오는 방법은 다음 섹션에서 설명합니다: 키 파일 정보.

  라이센스 키 파일을 사용하여 애플리케이션을 활성화할 때 Kaspersky 활성화 서버에 연결하지 않아도 됩니다.

  이 활성화 옵션을 선택했다면 **관리 중인 기기에 자동으로 라이센스 키 배포** 옵션을 활성화할 수 있습니다.

  이 옵션을 활성화하면 라이센스 키가 관리 중인 기기에 자동으로 배포됩니다.

  이 옵션을 비활성화하면 나중에 관리 콘솔 트리의 **Kaspersky 라이센스** 노드에서 관리 중인 기기로 라이센스 키를 배포할 수 있습니다.

- **애플리케이션 활성화 연기**

  애플리케이션이 기본 기능으로 작동하며 모바일 기기 관리와 취약점 및 패치 관리 기능은 제공되지 않습니다.

애플리케이션 활성화를 연기하도록 선택한 경우 나중에 언제든지 라이센스 키를 추가할 수 있습니다.

3단계. 보호 영역 및 운영 체제 선택

네트워크에서 사용 중인 보호 범위와 운영 체제를 선택합니다. 이러한 옵션을 선택할 때 네트워크 내 클라이언트 기기에 설치하기 위해 다운로드할 수 있는 Kaspersky 서버의 애플리케이션 관리 플러그인 및 배포 패키지에 대한 필터를 지정합니다. 옵션을 선택합니다.

- **영역**

  다음 보호 영역을 선택할 수 있습니다:

  - **워크스테이션**. 네트워크의 워크스테이션을 보호하려면 이 옵션을 선택합니다. 워크스테이션 옵션은 기본으로 선택되어 있습니다.
  - **파일 서버 및 스토리지**. 네트워크의 파일 서버를 보호하려면 이 옵션을 선택합니다.
  - **모바일 기기**. 회사 또는 회사 직원이 소유한 모바일 기기를 보호하려면 이 옵션을 선택합니다. 이 옵션을 선택하지만 모바일 기기 관리 기능이 있는 라이센스를 제공하지 않으면 모바일 기기 관리 기능이 있는 라이센스를 제공해야 한다는 내용의 메시지가 표시됩니다. 라이센스를 제공하지 않으면 모바일 기기 기능을 이용할 수 없습니다.
  - **가상화** 네트워크에서 가상 컴퓨터를 보호하려면 이 옵션을 선택합니다.
  - **Kaspersky 안티 스팸**. 조직에 있는 메일 서버를 스팸, 사기 및 악성 코드 전달로부터 보호하려면 이 옵션을 선택합니다.

- **운영 체제**

  다음 플랫폼을 선택할 수 있습니다:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - 기타

  지원하는 운영 체제에 대한 정보는 하드웨어 및 소프트웨어 요구사항을 참조하십시오.

빠른 시작 마법사와는 별도로 나중에 사용 가능한 패키지 목록에서 Kaspersky 애플리케이션 패키지를 선택할 수 있습니다. 필수 패키지 검색을 단순화하기 위해 다음 기준으로 사용 가능한 패키지 목록을 필터링할 수 있습니다:

- 보호구역
- 다운로드한 소프트웨어 유형(배포 패키지, 유틸리티, 플러그인, 웹 플러그인 중 하나)
- Kaspersky 애플리케이션 버전
- Kaspersky 애플리케이션의 현지화 언어

4단계. 관리 중인 애플리케이션에 대한 플러그인 선택

설치할 관리 중인 애플리케이션에 대한 플러그인을 선택합니다. Kaspersky 서버에 있는 플러그인 목록이 표시됩니다. 마법사의 이전 단계에서 선택한 옵션에 따라 목록이 필터링됩니다. 전체 목록에는 기본적으로 모든 언어의 플러그인이 포함됩니다. 특정 언어의 플러그인만 표시하려면 **표시: 관리 콘솔 현지화 언어 또는** 드롭다운 목록에서 언어를 선택합니다. 플러그인 목록에는 다음 열이 포함됩니다:

- **애플리케이션 이름**

  이전 단계에서 선택한 보호 영역 및 플랫폼에 따라 플러그인이 선택됩니다.

- **애플리케이션 버전**

  이 목록에는 Kaspersky 서버에 있는 모든 버전의 플러그인이 포함됩니다. 최신 버전의 플러그인이 기본으로 선택되어 있습니다.

- **현지화 언어**

  기본적으로 플러그인의 현지화 언어는 설치 시 선택한 Kaspersky Security Center 언어에 따라 정의됩니다. **표시: 관리 콘솔 현지화 언어 또는** 드롭다운 목록에서 다른 언어를 지정할 수 있습니다.

플러그인을 선택한 후 별도의 창에서 설치가 자동으로 시작됩니다. 일부 플러그인은 설치 과정에서 EULA의 조항에 동의해야 합니다. EULA의 본문을 읽고 **라이선스 계약서 조건에 동의합니다** 옵션을 선택하고 **설치** 버튼을 누릅니다. EULA의 조항에 동의하지 않으면 플러그인이 설치되지 않습니다.

설치가 완료되면 설치 창을 닫습니다.

빠른 시작 마법사와 별도로 나중에 관리 플러그인을 선택할 수도 있습니다.

5단계. 배포 패키지 다운로드 및 설치 패키지 생성

Kaspersky Endpoint Security for Windows에는 클라이언트 기기에 저장된 정보를 위한 암호화 도구가 포함되어 있습니다. 조직의 요구에 적합한 Kaspersky Endpoint Security for Windows의 배포 패키지를 다운로드하려면 조직의 클라이언트 기기가 있는 국가의 법률을 참조하십시오.

암호화 유형 창에서 다음 암호화 유형 중 하나를 선택합니다:

- 강력한 암호화(AES256). 이 암호화 유형은 256비트 키 길이를 사용합니다.
- 가벼운 암호화(AES56). 이 암호화 유형은 56비트 키 길이를 사용합니다.

암호화 유형 창은 **워크스테이션**을 보호 범위로, **Microsoft Windows**를 플랫폼으로 선택했을 때만 표시됩니다.

암호화 유형을 선택한 후 두 암호화 유형의 배포 패키지 목록이 표시됩니다. 선택한 암호화 유형의 배포 패키지가 목록에서 선택됩니다. 배포 패키지 언어는 Kaspersky Security Center 언어에 해당합니다. Kaspersky Security Center 언어에 대한 Kaspersky Endpoint Security for Windows 배포 패키지가 없으면 영어 배포 패키지가 선택됩니다.

이 목록에서 **표시: 관리 콘솔 현지화 언어 또는** 드롭다운 목록을 사용하여 배포 패키지 언어를 선택할 수 있습니다.

관리 중인 애플리케이션을 배포하려면 Kaspersky Security Center의 특정 최소 버전을 설치해야 할 수 있습니다.

이 목록에서 **암호화 유형** 창에서 선택한 것과 다른 암호화 유형의 배포 패키지를 선택할 수 있습니다. Kaspersky Endpoint Security for Windows 배포 패키지를 선택하면 구성 요소 및 플랫폼에 해당하는 배포 패키지의 다운로드가 시작됩니다. **다운로드 상태** 열에서 다운로드 진행 상황을 모니터링할 수 있습니다. 빠른 시작 마법사가 완료되면 Windows용 네트워크 에이전트 및 관리 중인 Kaspersky 애플리케이션의 설치 패키지가 **중앙 관리 서버 → 고급 → 원격 설치 → 설치 패키지** 목록에 표시됩니다.

일부 배포 패키지는 EULA에 동의해야 다운로드를 완료할 수 있습니다. **수락** 버튼을 클릭하면 EULA의 본문이 표시됩니다. 마법사의 다음 단계로 진행하려면 EULA의 약관 및 Kaspersky 개인 정보 취급 방침의 약관을 수락해야 합니다. EULA 및 Kaspersky 개인정보취급방침과 관련된 옵션을 선택하고 **모두 수락** 버튼을 누릅니다. 약관에 동의하지 않으면 패키지 다운로드가 취소됩니다.

EULA의 약관 및 Kaspersky 개인정보취급방침 약관에 동의하면 배포 패키지 다운로드가 계속됩니다. 다운로드가 완료되면 **설치 패키지 생성 완료** 상태가 표시됩니다. 나중에 설치 패키지를 사용하여 클라이언트 기기에 Kaspersky 애플리케이션을 배포할 수 있습니다.

빠른 시작 마법사와 별도로 수동으로 설치 패키지를 생성할 수 있습니다. 관리 콘솔 트리에서 **중앙 관리 서버 → 고급 → 원격 설치 → 설치 패키지**로 이동합니다.

6단계. Kaspersky Security Network 사용 구성

Kaspersky Security Network의 평판 데이터베이스를 사용하면 보안 위협에 대한 Kaspersky 애플리케이션의 대응 속도를 한층 개선할 수 있으며, 일부 보호 구성 요소의 성능이 향상되고, 오탐 위험이 줄어듭니다.

창에 표시된 KSN 진술문을 읽어 주십시오. Kaspersky Security Center 작동 관련 정보를 Kaspersky Security Network 기술 자료로 전달하기 위한 설정을 지정합니다. 다음 옵션 중 하나를 선택합니다:

- **Kaspersky Security Network 사용에 동의합니다**

  클라이언트 기기에 설치된 Kaspersky Security Center 및 관리 중인 애플리케이션은 작업 세부 정보를 Kaspersky Security Network로 자동 전송합니다. Kaspersky Security Network에 참여하면 바이러스 및 기타 위협 관련 정보가 포함된 데이터베이스를 보다 빠르게 업데이트할 수 있으므로 새로운 보안 위협에 더욱 신속하게 대응할 수 있습니다.

- **Kaspersky Security Network 사용에 동의하지 않습니다**

  Kaspersky Security Center 및 관리 중인 애플리케이션은 Kaspersky Security Network로 정보를 제공하지 않습니다.

  이 옵션을 선택하면 Kaspersky Security Network 사용이 비활성화됩니다.

Kaspersky Endpoint Security for Windows 플러그인을 다운로드했다면, KSN 진술문(Kaspersky Security Center에 대한 KSN 진술문과 Kaspersky Endpoint Security for Windows에 대한 KSN 진술문)이 모두 표시됩니다. 플러그인이 다운로드된 기타 관리 중인 Kaspersky 애플리케이션에 대한 KSN 성명서는 별도의 창에 표시되며, 각 문에 대해 개별적으로 동의(또는 거부)해야 합니다.

나중에 관리 콘솔의 중앙 관리 서버 속성 창에서 KSN(Kaspersky Security Network)에 대한 중앙 관리 서버 액세스를 설정할 수도 있습니다.

7단계. 이메일 알림 구성

관리 중인 기기에서 Kaspersky 애플리케이션 작동 시 등록된 이벤트에 대한 알림 전달을 구성할 수 있습니다. 이러한 설정은 중앙 관리 서버에서 기본 설정으로 사용됩니다.

Kaspersky 애플리케이션에서 발생하는 이벤트에 대한 알림 전달을 구성하려면 다음 설정을 사용합니다:

- **받는 사람(이메일 주소)**

  애플리케이션에서 알림을 보낼 사용자의 이메일 주소입니다. 주소를 하나 이상 입력할 수 있습니다. 주소를 한 개 이상 입력하고자 할 경우 각 주소를 세미콜론으로 구분하십시오.

- **SMTP 서버**

  조직의 메일 서버 주소 또는 주소들입니다.

  주소를 한 개 이상 입력하고자 할 경우 각 주소를 세미콜론으로 구분하십시오. 다음 값을 사용할 수 있습니다:

  - IPv4 또는 IPv6 주소
  - 기기의 Windows 네트워크 이름(NetBIOS 이름)
  - SMTP 서버의 DNS 이름

- **SMTP 서버 포트**

  SMTP 서버의 통신 포트 번호입니다. 여러 SMTP 서버를 사용한다면 지정된 통신 포트를 통해 이들에 대한 연결이 설정됩니다. 기본 포트 번호는 25입니다.

- **ESMTP 인증 사용**

  ESMTP 인증을 지원하도록 설정합니다. **사용자 이름** 및 **암호** 필드의 확인란을 선택하면 ESMTP 인증 설정을 지정할 수 있습니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

- **설정**

  다음 설정을 지정합니다:

  - **제목**(이메일 메시지의 제목)
  - **발신자 이메일 주소**
  - **SMTP 서버에 대한 TLS 설정**

  다음과 같이 SMTP 서버에 대한 TLS 설정을 지정할 수 있습니다.

TLS 사용을 비활성화하거나, SMTP 서버가 이 프로토콜을 지원하는 경우 TLS를 사용하거나 또는 TLS만 사용하도록 강제할 수 있습니다. TLS만 사용하도록 선택했다면, SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, TLS만 사용하도록 선택한 경우 SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

- 다음 SMTP 서버 인증서 파일을 찾습니다.

신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 중앙 관리 서버에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

- 다음과 같이 클라이언트 인증서 파일을 찾습니다.

신뢰할 수 있는 인증 기관과 같은 다양한 출처에서 수신된 인증서를 사용할 수 있습니다. 다음 인증서 유형 중 하나를 사용하여 인증서와 개인 키를 지정해야 합니다:

- X-509 인증서:

인증서가 있는 파일과 개인 키가 있는 파일을 지정해야 합니다. 이러한 파일은 순서에 관계없이 업로드할 수 있습니다. 두 파일이 모두 로딩되면 개인 키 복호화를 위한 암호를 지정합니다. 개인 키가 암호화되지 않았다면 암호가 빈 값을 가질 수 있습니다.

- pkcs12 컨테이너:

인증서와 개인 키가 포함 된 단일 파일을 업로드해야 합니다. 파일이 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

테스트 메시지 전송 버튼을 눌러 새 이메일 알림 설정을 테스트할 수 있습니다.

빠른 시작 마법사와는 별도로 나중에 이벤트 알림을 구성할 수도 있습니다.

8단계. 업데이트 관리 구성

클라이언트 기기에 설치된 애플리케이션의 업데이트 관리를 위한 설정을 구성합니다.

취약점 및 패치 관리 옵션이 있는 라이센스 키를 제공했을 때만 이러한 설정을 구성할 수 있습니다.

설정의 **업데이트 검색 및 설치** 그룹에서 Kaspersky Security Center 업데이트 검색 및 설치 모드를 선택할 수 있습니다.

- **필요한 업데이트 검색**

  취약점 및 필요한 업데이트 검색 작업이 없다면 자동 생성됩니다.
  이 옵션은 기본적으로 선택되어 있습니다.

- **타사 제품 업데이트 검색 및 설치**

  작업이 없는 경우 *취약점 및 필요한 업데이트 검색* 및 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 자동으로 생성됩니다.

설정의 **Windows 서버 업데이트 서비스** 그룹에서 업데이트 동기화 소스를 선택할 수 있습니다:

- **도메인 정책에 정의되어 있는 업데이트 경로 사용**

  클라이언트 기기는 도메인 정책 설정에 따라 Windows 업데이트 업데이트를 다운로드합니다. 네트워크 에이전트 정책은 없는 경우 자동으로 생성됩니다.

- **WSUS 서버로 이 중앙 관리 서버 사용**

  클라이언트 기기는 중앙 관리 서버에서 Windows 업데이트 업데이트를 다운로드합니다. *Windows 업데이트 동기화 수행* 작업 및 네트워크 에이전트 정책은 없는 경우 자동으로 생성됩니다.

취약성 및 필수 업데이트 검색 및 *필수 업데이트 설치 및 취약성 수정* 태스크를 빠른 시작 마법사와 별도로 생성할 수 있습니다. 중앙 관리 서버를 WSUS 서버로 사용하려면 *Windows 업데이트 동기화 수행* 작업을 만들고 네트워크 에이전트 정책에서 **WSUS 서버로 이 중앙 관리 서버 사용** 옵션을 선택합니다.

9단계. 초기 보호 구성 만들기

초기 보호 구성 창에는 만들어진 정책과 작업의 목록이 자동으로 표시됩니다. 다음과 같은 정책 및 작업이 생성됩니다:

- Kaspersky Security Center 네트워크 에이전트 정책
- 관리 플러그인이 이전에 설치된 관리 중인 Kaspersky 애플리케이션에 대한 정책
- 중앙 관리 서버 점검 작업
- 중앙 관리 서버 데이터 백업 작업
- 중앙 관리 서버 저장소에 업데이트 다운로드 작업
- 취약점 및 필요한 업데이트 검색 작업
- 업데이트 설치 작업

정책 및 작업 만들기가 완료될 때까지 기다린 후에 마법사의 다음 단계로 진행합니다.

정책 및 작업을 생성하는 동안 Kaspersky Endpoint Security for Windows 10 서비스 팩 1 이상에서 11.0.1까지에 대한 플러그인을 다운로드하여 설치한 경우 Kaspersky Endpoint Security for Windows의 신뢰할 수 있는 영역의 초기 구성에 대한 창이 열립니다. 애플리케이션에는 Kaspersky에서 확인한 공급 업체의 애플리케이션이 잘못 차단되지 않도록 검사에서 제외하기 위해 해당 공급업체를 신뢰할 수 있는 영역에 추가하라는 메시지가 표시됩니다. 지금 권장 제외 항목을 만들거나 콘솔 트리에서 **정책** → Kaspersky Endpoint Security 속성 메뉴 → **지능형 위협 보호** → **신뢰 구역** → **설정** → **추가**를 선택하여 나중에 제외 항목 목록을 만들 수도 있습니다. 검사 예외 목록은 애플리케이션 사용 시 언제든지 편집할 수 있습니다.

신뢰할 수 있는 영역에서는 Kaspersky Endpoint Security for Windows에 포함된 도구를 사용하여 작업을 수행할 수 있습니다. 암호화 작업 수행 방법 및 암호화 기능에 대한 자세한 설명은 Kaspersky Endpoint Security for Windows 온라인 도움말을 참조하십시오.

신뢰할 수 있는 영역 초기 구성을 완료하고 마법사로 돌아가려면 **확인**을 누릅니다.

다음을 누릅니다. 필요한 정책과 작업을 모두 만들고 나면 이 버튼을 사용할 수 있게 됩니다.

빠른 시작 마법사와 별도로 필요한 작업 및 정책을 나중에 생성할 수도 있습니다.

10단계. 모바일 기기 연결

이전에 마법사 설정에서 **모바일 기기** 보호 범위를 활성화했다면 관리 중인 조직의 기업 모바일 기기 연결을 위한 설정을 지정합니다. **모바일 기기** 보호 범위를 활성화하지 않았다면 이 단계를 건너뜁니다.

마법사의 이 단계에서 다음을 수행합니다:

- 모바일 기기 연결용 포트 구성
- 중앙 관리 서버 인증 구성
- 인증서 만들기 또는 관리
- 일반 유형 인증서 발급, 자동 업데이트 및 암호화 설정
- 모바일 기기용 이동 규칙 생성

모바일 기기 연결용 포트를 설정하려면 다음과 같이 하십시오:

1. **모바일 기기 연결** 필드 오른쪽에 있는 **구성** 버튼을 누릅니다.
2. 드롭다운 목록에서 **포트 구성**을 선택합니다.
   중앙 관리 서버 속성 창이 열리고 **추가 포트** 섹션이 표시됩니다.
3. **추가 포트** 섹션에서 다음과 같은 모바일 기기 연결 설정을 지정할 수 있습니다.

   - **활성화 프록시 서버용 SSL 포트**

     이 필드에는 Kaspersky 활성화 서버의 Kaspersky Endpoint Security for Windows 연결을 위한 SSL 포트 번호를 지정할 수 있습니다.
     기본 포트 번호는 17000입니다.

   - **모바일 기기용 포트 열기**

     모바일 기기가 라이센스 서버에 연결하는 데 사용하는 포트가 열립니다. 아래 필드에서 포트 번호와 기타 설정을 정의할 수 있습니다.
     기본적으로 이 옵션은 켜져 있습니다.

   - **모바일 기기 동기화용 포트**

     모바일 기기가 중앙 관리 서버에 연결하여 해당 서버와 데이터를 교환하는 데 사용하는 포트의 번호입니다. 기본 포트 번호는 13292입니다.
     포트 13292이 다른 용도로 사용되고 있으면 다른 포트를 할당할 수 있습니다.

   - **모바일 기기 활성화용 포트**

     Kaspersky Endpoint Security for Android와 Kaspersky의 활성화 서버 연결용 포트.

기본 포트 번호는 17100입니다.

- **UEFI 보호 기기 및 KasperskyOS 기기용 포트 열기**

  UEFI 보호 기기가 중앙 관리 서버에 연결할 수 있습니다.

- **UEFI 보호 기기 및 KasperskyOS 기기용 포트**

  UEFI 보호 기기 및 KasperskyOS 기기용 포트 열기 옵션을 활성화하는 경우 포트 번호를 변경할 수 있습니다. 기본 포트 번호는 13294입니다.

- **Prometheus용 포트 열기**

  Prometheus 풀 요청을 위한 포트입니다. 기본 포트 번호는 13296입니다.

4. 변경 내용을 저장하고 빠른 시작 마법사로 돌아가려면 **확인**을 클릭합니다.

모바일 기기의 중앙 관리 서버 인증과 중앙 관리 서버의 모바일 기기 인증을 구성해야 합니다. 필요하다면 빠른 시작 마법사와 별도로 나중에 인증을 구성할 수도 있습니다.

모바일 기기의 중앙 관리 서버 인증을 구성하려면 다음과 같이 하십시오:

1. **모바일 기기 연결** 필드 오른쪽에 있는 **구성** 버튼을 누릅니다.
2. 드롭다운 목록에서 **인증 구성**을 선택합니다.

   중앙 관리 서버 속성 창이 열리고 **인증서** 섹션이 표시됩니다.
3. 설정의 **모바일 기기별 중앙 관리 서버 인증** 그룹에서 모바일 기기에 대한 인증 옵션을 선택하고 설정의 **UEFI 보호 기기별 중앙 관리 서버 인증** 그룹에서 UEFI 보호 기기에 대한 인증 옵션을 선택합니다.

   중앙 관리 서버는 클라이언트 기기와 데이터를 교환할 때 인증서를 사용하여 인증을 합니다.

   기본적으로 중앙 관리 서버는 중앙 관리 서버 설치 시 만들어진 인증서를 사용합니다. 원하는 경우 새 인증서를 추가할 수 있습니다.

새 인증서를 추가(옵션)하려면 다음과 같이 하십시오:

1. **다른 인증서**를 선택합니다.

   찾기 버튼이 나타납니다.
2. **찾기** 버튼을 누릅니다.
3. 열리는 창에서 인증서 설정을 구성하십시오:

   - **인증서 유형**

     드롭다운 목록에서 다음과 같은 인증서 유형을 선택할 수 있습니다.

     - **X.509 인증서**. 이 옵션을 선택하면 다음과 같이 인증서의 개인 키 및 공개 인증서를 지정해야 합니

다.

- **개인 키(.prk, .pem)**. 이 필드에서 **찾기** 버튼을 클릭하여 PKCS #8(*.prk) 형식의 인증서 개인 키를 지정합니다.
- **공개 키(.cer)**. 이 필드에서 **찾기** 버튼을 클릭하여 PEM(*.cer) 형식의 공개 키를 지정합니다.

- **PKCS #12 컨테이너**. 이 옵션을 선택하면 **찾기** 버튼을 클릭해 **인증서 파일** 필드를 작성하여 P12 또는 PFX 형식의 인증서 파일을 지정할 수 있습니다.

- 활성화 시간:
  - **즉시**

    확인을 누르는 즉시 현재 인증서가 새 인증서로 교체됩니다.
    그러면 이전에 연결했던 모바일 기기가 중앙 관리 서버에 연결할 수 없게 됩니다.

  - **이 기간이 만료된 후(일)**

    이 옵션을 선택하면 예약 인증서가 생성됩니다. 현재 인증서는 지정된 기간(일)이 지나면 새 인증서로 교체됩니다. 예약 인증서의 유효 날짜가 **인증서** 섹션에 표시됩니다.
    재발행은 미리 계획하는 것이 좋습니다. 지정된 기간이 만료되기 전에 예약 인증서를 모바일 기기에 다운로드해야 합니다. 현재 인증서가 새 인증서로 교체되고 나면 이전에 연결했으나 예약 인증서가 없는 모바일 기기는 중앙 관리 서버에 연결할 수 없게 됩니다.

4. **속성** 버튼을 눌러 선택한 중앙 관리 서버 인증서의 설정을 볼 수 있습니다.

중앙 관리 서버를 통해 발급된 인증서를 재발급하려면 다음과 같이 하십시오:

1. **중앙 관리 서버를 통해 발급된 인증서**를 선택합니다.
2. **재발급** 버튼을 누릅니다.
3. 열리는 창에서 다음 설정을 구성하십시오:
   - 연결 주소:
     - **이전 연결 주소 사용**

       모바일 기기가 연결하는 중앙 관리 서버의 주소가 변경되지 않고 그대로 유지됩니다.
       이 옵션은 기본적으로 선택되어 있습니다.

     - **다음 연결 주소로 변경**

       모바일 기기가 다른 주소에 연결되도록 하려면 이 필드에서 해당 주소를 지정합니다.
       모바일 기기 연결용 주소가 변경된 경우 새 인증서를 발급해야 합니다. 연결된 모든 모바일 기기에서 이전 인증서는 무효화됩니다. 이전에 연결했던 기기는 중앙 관리 서버에 연결할 수 없으므로 관리되지 않는 상태가 됩니다.

- 활성화 시간:

  - **즉시**

    확인을 누르는 즉시 현재 인증서가 새 인증서로 교체됩니다.
    그러면 이전에 연결했던 모바일 기기가 중앙 관리 서버에 연결할 수 없게 됩니다.

  - **이 기간이 만료된 후(일)**

    이 옵션을 선택하면 예약 인증서가 생성됩니다. 현재 인증서는 지정된 기간(일)이 지나면 새 인증서로 교체됩니다. 예약 인증서의 유효 날짜가 **인증서** 섹션에 표시됩니다.
    재발행은 미리 계획하는 것이 좋습니다. 지정된 기간이 만료되기 전에 예약 인증서를 모바일 기기에 다운로드해야 합니다. 현재 인증서가 새 인증서로 교체되고 나면 이전에 연결했으나 예약 인증서가 없는 모바일 기기는 중앙 관리 서버에 연결할 수 없게 됩니다.

4. 변경 내용을 저장하고 **인증서** 창으로 돌아오려면 **확인**를 누릅니다.

5. 변경 내용을 저장하고 빠른 시작 마법사로 돌아가려면 **확인**을 클릭합니다.

중앙 관리 서버의 모바일 기기 식별용 일반 유형 인증서 발급, 자동 업데이트 및 암호화를 설정하려면 다음과 같이 하십시오:

1. **모바일 기기 인증** 필드 오른쪽에 있는 **구성** 버튼을 누릅니다.
   인증서 발급 규칙 창이 열리고 **모바일 인증서 발급** 섹션이 표시됩니다.

2. 필요한 경우 **발급 설정** 섹션에서 다음 설정을 지정합니다:

   - **인증서 유효 기간, 일**

     인증서 수명 기간(일)입니다. 인증서의 기본 수명은 365일입니다. 이 기간이 만료되면 모바일 기기는 중앙 관리 서버에 연결할 수 없습니다.

   - **인증서 소스**

     모바일 기기용 일반 유형 인증서의 경로를 선택합니다. 인증서는 중앙 관리 서버에서 발급될 수도 있고 수동으로 지정할 수도 있습니다.

     PKI와 통합 섹션에서 PKI(공개키 인프라)와의 통합을 구성한 경우에는 인증서 템플릿을 수정할 수 있습니다. 이 경우에는 다음과 같은 템플릿 조회 필드를 사용할 수 있습니다:

   - **기본 템플릿**

     기본 템플릿 아래의 외부 인증서 경로(인증 센터)에서 발급한 인증서를 사용합니다.
     기본적으로 이 옵션은 선택되어 있습니다.

   - **기타 템플릿**

     인증서를 발급하는 데 사용되는 템플릿을 선택합니다. 도메인에서 인증서 템플릿을 지정할 수 있습니다. **목록 새로 고침** 버튼을 누르면 인증서 템플릿의 목록을 업데이트합니다.

3. 필요한 경우 **자동 업데이트 설정** 섹션에서 인증서 자동 발급을 위한 다음 설정을 지정합니다:

   - **다음 기간 이내에 인증서가 만료되면 갱신(일)**

     중앙 관리 서버가 새 인증서를 발급하는 동안 현재 인증서가 만료될 때까지 남은 날짜. 예를 들어, 필드의 값이 4이면 중앙 관리 서버는 현재 인증서가 만료되기 4일 전에 새 인증서를 발급합니다. 기본값은 7입니다.

   - **가능하면 자동으로 인증서 재발급**

     다음 기간 이내에 인증서가 만료되면 갱신(일) 필드에 지정된 일수 동안 인증서를 자동으로 재발급하려면 이 옵션을 선택하십시오. 인증서가 수동으로 정의된 경우 자동으로 갱신할 수 없으며 활성화된 옵션이 작동하지 않습니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

   인증서는 인증 센터에서 자동으로 재발급됩니다.

4. 필요한 경우 **암호 보호** 설정 섹션에서 설치 중의 인증서 복호화를 위한 설정을 지정합니다.

   모바일 기기에 인증서가 설치되어 있는 경우 사용자에게 암호를 입력하라는 메시지를 표시하려면 **인증서 설치 시 암호 물어보기** 옵션을 선택합니다. 암호는 모바일 기기에 인증서를 설치할 때 한 번만 사용됩니다.

   암호는 중앙 관리 서버에서 자동으로 생성되어 지정한 이메일 주소로 전송됩니다. 사용자의 이메일 주소를 지정할 수도 있고, 다른 방법으로 사용자에게 암호를 전달하려는 경우에는 자신의 이메일 주소를 지정할 수도 있습니다.

   슬라이더를 사용하여 인증서 복호화 암호의 문자 수를 지정할 수 있습니다.

   독립 실행형 Kaspersky Endpoint Security for Android 설치 패키지의 공유 인증서를 보호하려는 등의 경우에는 암호 요청 옵션을 사용해야 합니다. 암호를 보호하면 침입자가 Kaspersky Security Center 웹 서버의 독립 실행형 설치 패키지를 도용하여 공유 인증서 접근 권한을 확보하는 상황을 방지할 수 있습니다.

   이 옵션이 비활성화되어 있으면 설치 중에 인증서가 자동으로 복호화되며 사용자에게 암호를 입력하라는 메시지가 표시되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

5. 변경 내용을 저장하고 빠른 시작 마법사 창으로 돌아가려면 **확인**을 클릭합니다.

   변경 내용을 저장하지 않고 빠른 시작 마법사로 돌아오려면 **취소** 버튼을 누릅니다.

선택한 관리 그룹으로 모바일 기기를 이동하는 기능을 사용하도록 설정하려면 다음과 같이 하십시오,

모바일 기기 자동 이동 필드에서 **모바일 기기용 이동 규칙 생성** 옵션을 선택합니다.

모바일 기기용 이동 규칙 생성 옵션을 선택하면 애플리케이션이 Android 및 iOS를 실행하는 기기를 **관리 중인 기기** 그룹으로 이동하는 이동 규칙을 자동으로 만듭니다.

- Kaspersky Endpoint Security for Android 및 모바일 인증서가 설치된 Android 운영 체제
- 공유 인증서가 있는 iOS MDM 프로필이 설치된 iOS 운영 체제

해당 규칙이 이미 있으면 애플리케이션은 규칙을 새로 만들지 않습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

Kaspersky은 Kaspersky Safe Browser를 더 이상 지원하지 않습니다.

11단계. 업데이트 다운로드

Kaspersky Security Center 및 관리 중인 Kaspersky 애플리케이션에 대한 안티 바이러스 데이터베이스 업데이트는 자동으로 다운로드됩니다. 업데이트는 Kaspersky 서버에서 다운로드됩니다.

빠른 시작 마법사와 별도로 업데이트를 다운로드하려면 *중앙 관리 서버의 저장소에 업데이트 다운로드*를 생성 및 구성합니다.

12단계. 기기 발견

네트워크 검색 창에는 중앙 관리 서버가 수행하는 네트워크 검색의 상태에 대한 정보가 표시됩니다.

창 아래쪽의 링크를 누르면 중앙 관리 서버가 탐지한 네트워크 기기를 확인하고 **기기 발견** 창 사용법과 관련한 지원을 받을 수 있습니다.

빠른 시작 마법사와는 별도로 네트워크를 나중에 검색할 수도 있습니다. 관리 콘솔을 사용하여 Windows 도메인, Active Directory, IP 범위, IPv6 네트워크의 검색을 구성합니다.

13단계. 빠른 시작 마법사 닫기

네트워크의 기기에서 안티 바이러스 애플리케이션 및/또는 네트워크 에이전트 자동 설치를 시작하려면 빠른 시작 마법사 완료 창에서 **원격 설치 마법사 실행** 옵션을 선택합니다.

마법사를 완료하려면 **마침** 버튼을 클릭합니다.

중앙 관리 서버로의 관리 콘솔 연결 구성

관리 콘솔은 SSL 포트 TCP 13291을 통해 관리 서버에 연결됩니다. klakaut 자동화 개체에서 같은 포트를 사용할 수 있습니다.

Port TCP 14000은 관리 콘솔, 배포 지점, 보조 중앙 관리 서버 및 klakaut 자동화 개체 연결 및 클라이언트 기기 데이터 검색에만 사용됩니다.

일반적으로 SSL 포트 TCP 13000은 DMZ의 네트워크 에이전트, 보조 중앙 관리 서버, 기본 중앙 관리 서버에서만 사용할 수 있습니다. SSL port 13000을 통해 관리 콘솔을 연결해야 하는 경우는 다음과 같습니다:

- SSL 포트 한 개를 관리 콘솔과 기타 활동 모두에 사용할 가능성이 있는 경우(클라이언트 기기 데이터 검색, 배포 지점 연결, 보조 중앙 관리 서버 연결).
- klakaut 자동화 개체가 중앙 관리 서버에 직접 연결되지 않고 DMZ의 배포 지점을 통해 연결 시.

13000 포트를 통한 관리 콘솔 연결을 허용하려면 다음과 같이 하십시오:

1. 중앙 관리 서버가 설치된 기기에서 시스템 레지스트리를 엽니다(예:로컬에서 **시작** → **실행** 메뉴의 regedit 명령 사용).
2. 다음 하이브로 이동합니다:
   - 32비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 64비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. LP_ConsoleMustUsePort13291 (DWORD) 키의 값으로 00000000을 설정합니다.

   이 키에 지정된 기본값은 1입니다.
4. 중앙 관리 서버 서비스를 다시 시작합니다.

그러면 13000 포트를 통해 관리 콘솔을 중앙 관리 서버에 연결할 수 있습니다.

중앙 관리 서버의 인터넷 액세스 설정 구성

Kaspersky Security Network를 사용하고, Kaspersky Security Center 및 관리 중인 Kaspersky 애플리케이션용 안티바이러스 데이터베이스의 업데이트를 다운로드하려면 인터넷 접속을 구성해야 합니다.

중앙 관리 서버의 인터넷 접속 설정을 지정하려면:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창에서 **고급** → **인터넷 연결 구성** 으로 이동합니다.
4. 인터넷에 연결할 때 프록시 서버를 사용하려면 **프록시 서버 사용** 옵션을 선택합니다. 이 옵션을 선택하면 설정을 입력하는 필드를 사용할 수 있게 됩니다. 프록시 서버 연결에 대해 다음 설정을 지정합니다.
   - **주소**

     Kaspersky Security Center에서 인터넷 연결에 사용한 프록시 서버의 주소입니다.
   - **포트 번호**

     Kaspersky Security Center 프록시 연결을 설정하는 데 사용되는 포트 번호입니다.
   - **로컬 주소에서 프록시 서버 사용 안 함**

     로컬 네트워크에서 기기로 연결하는 데 프록시 서버가 사용되지 않습니다.

- **프록시 서버 인증**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.

  프록시 서버 사용 확인란을 선택하면 이 입력 필드를 사용할 수 있습니다.

- **사용자 이름**

  프록시 서버에 대한 연결을 구성할 사용자 계정입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

- **암호**

  프록시 서버 연결을 구성한 계정의 사용자가 설정한 암호입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

  입력한 암호를 보려면 **보기** 버튼을 필요한 시간 동안 누르고 있어야 합니다.

빠른 시작 마법사를 사용하여 인터넷 액세스를 구성할 수도 있습니다.

이동 사용자 기기 연결

이 섹션은 이동 사용자 기기(즉, 기본 네트워크 외부에 있는 관리 중인 기기)를 중앙 관리 서버에 연결하는 방법을 설명합니다.

시나리오: 연결 게이트웨이를 통해 이동 사용자 기기 연결

이 시나리오는 기본 네트워크 외부에 있는 관리 중인 기기를 중앙 관리 서버에 연결하는 방법을 설명합니다.

필수 구성 요소

시나리오에는 다음과 같은 전제 조건이 필요합니다.

- 완충 지역(DMZ)이 조직 네트워크에 구성됩니다.
- Kaspersky Security Center 중앙 관리 서버가 회사 네트워크에 배포됩니다.

단계

이 시나리오는 단계적으로 진행됩니다.

1. **DMZ에서 클라이언트 기기 선택**

   이 기기는 연결 게이트웨이로 사용됩니다. 선택하는 기기가 연결 게이트웨이에 대한 요구 사항을 충족해야 합니다.

2. **연결 게이트웨이 역할에 네트워크 에이전트 설치**

선택한 기기에 네트워크 에이전트를 설치하려면 로컬 설치를 사용하는 것이 좋습니다.

기본적으로 설치 파일은 다음 위치에 있습니다. \\<server name>\KLSHARE\PkgInst\NetAgent_<version number>

네트워크 에이전트 설치 마법사의 **연결 게이트웨이** 창에서 **연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용**을 선택합니다. 이 모드는 동시에 연결 게이트웨이 역할을 활성화하고 네트워크 에이전트가 중앙 관리 서버에 대한 연결을 설정하지 않고 중앙 관리 서버에서 연결을 기다리도록 지시합니다.

또는 Linux 기기에 네트워크 에이전트를 설치하고 네트워크 에이전트를 연결 게이트웨이로 작동하도록 구성할 수 있지만 Linux 기기에서 실행되는 네트워크 에이전트의 제한 사항 목록에 주의를 기울이십시오.

3 연결 게이트웨이의 방화벽에서 연결 허용

중앙 관리 서버를 실제로 DMZ의 연결 게이트웨이에 연결할 수 있는지 확인하려면 중앙 관리 서버와 연결 게이트웨이 사이의 모든 방화벽에서 TCP 포트 13000에 대한 연결을 허용하십시오.

연결 게이트웨이가 인터넷상의 실제 IP 주소를 가지고 있지는 않지만 대신 NAT(Network Address Translation) 뒤에 있다면, NAT를 통해 연결을 전달하도록 규칙을 구성하십시오.

4 외부 기기에 대한 관리 그룹 생성

관리 중인 기기 그룹 아래에 새 그룹을 생성합니다. 이 새 그룹에는 외부 관리 중인 기기가 포함됩니다.

5 연결 게이트웨이를 중앙 관리 서버에 연결

구성한 연결 게이트웨이가 중앙 관리 서버의 연결을 기다리고 있습니다. 하지만 중앙 관리 서버에는 연결 게이트웨이 기기가 관리 중인 기기로 나열되지 않습니다. 이는 연결 게이트웨이가 중앙 관리 서버 연결을 설정하려고 하지 않았기 때문입니다. 따라서 특별한 절차를 통해 중앙 관리 서버가 연결 게이트웨이로의 연결을 초기화하도록 해야 합니다.

다음을 수행하십시오.

1. 연결 게이트웨이를 배포 지점으로 추가합니다.
2. 연결 게이트웨이를 **미할당 기기** 그룹에서 외부 기기용으로 생성한 그룹으로 이동합니다.

연결 게이트웨이가 연결되고 구성됩니다.

6 중앙 관리 서버에 외부 데스크톱 기기 연결

일반적으로 외부 데스크톱 기기는 경계 내부로 이동하지 않습니다. 따라서 네트워크 에이전트를 설치할 때 게이트웨이를 통해 중앙 관리 서버에 연결하도록 구성해야 합니다.

7 외부 데스크톱 기기에 대한 업데이트 설정

보안 애플리케이션의 업데이트가 중앙 관리 서버에서 다운로드되도록 구성된 경우 외부 기기는 연결 게이트웨이를 통해 업데이트를 다운로드하며, 여기에는 다음 두 가지 단점이 있습니다.

- 회사 인터넷 커뮤니케이션 채널의 대역폭을 차지하는 불필요한 트래픽입니다.
- 업데이트를 받는 가장 빠른 방법이 아닙니다. 외부 기기의 경우 Kaspersky 업데이트 서버에서 업데이트를 받는 것이 더 저렴하고 빠를 수 있습니다.

다음을 수행하십시오.

1. 모든 외부 기기를 이전에 만든 별도의 관리 그룹으로 이동합니다.
2. 업데이트 작업에서 외부 기기가 있는 그룹을 제외합니다.
3. 외부 기기가 있는 그룹에 대해 별도의 업데이트 작업을 생성합니다.

8. **이동 중인 랩톱을 중앙 관리 서버에 연결**

   이동 중인 랩톱은 때로는 네트워크 내에 있고 때로는 네트워크 외부에 있습니다. 효과적인 관리를 위해서는 위치에 따라 다르게 중앙 관리 서버에 연결해야 합니다. 트래픽을 효율적으로 사용하려면 위치에 따라 다른 소스에서 업데이트를 받아야 합니다.

   이동 사용자에 대한 규칙(연결 프로필 및 네트워크 위치 설명)을 구성해야 합니다. 각 규칙은 이동 중인 랩톱이 위치에 따라 연결해야 하는 중앙 관리 서버 인스턴스와 업데이트를 받아야 하는 중앙 관리 서버 인스턴스를 정의합니다.

시나리오: DMZ의 보조 중앙 관리 서버를 통해 부재 중 기기 연결

중앙 관리 서버에 기본 네트워크 외부에 있는 관리 중인 기기를 연결하려면 DMZ(Demilitarized Zone)에 있는 보조 중앙 관리 서버를 사용하면 됩니다.

필수 구성 요소

시작하기 전에 다음을 수행했는지 확인하십시오:

- DMZ가 조직 네트워크에 구성됩니다.
- Kaspersky Security Center 중앙 관리 서버가 조직의 내부 네트워크에 배포됩니다.

단계

이 시나리오는 단계적으로 진행됩니다.

1. **DMZ에서 클라이언트 기기 선택**

   DMZ에서 보조 중앙 관리 서버로 사용할 클라이언트 기기를 선택합니다.

2. **Kaspersky Security Center 중앙 관리 서버 설치**

   이 클라이언트 기기에 Kaspersky Security Center 중앙 관리 서버를 설치합니다.

3. **중앙 관리 서버의 계층 구조 생성**

   DMZ에 보조 중앙 관리 서버를 둔다면, 보조 중앙 관리 서버는 기본 중앙 관리 서버에서 연결을 받아야 합니다. 이렇게 하려면, 새 중앙 관리 서버를 보조로 추가하여 13000 포트를 통해 기본 중앙 관리 서버가 보조 중앙 관리 서버에 연결하도록 합니다. 두 개의 중앙 관리 서버를 하나의 계층으로 결합하는 경우 두 중앙 관리 서버 모두에서 13291 포트가 열려 있어야 합니다. 13291 포트를 통해 관리 콘솔을 해당 중앙 관리 서버와 연결합니다.

4. **외부의 관리 중인 기기를 보조 중앙 관리 서버에 연결**

   중앙 관리 서버와 기본 네트워크에 있는 관리 중인 기기 간에 연결이 설정되는 것과 같은 방식으로 외부에 있는 기기를 DMZ의 중앙 관리 서버에 연결할 수 있습니다. 외부의 관리 중인 기기가 13000 포트를 통해 연결을 시작합니다.

이동 사용자 기기 연결 정보

일부 관리 중인 기기는 항상 기본 네트워크 외부(예: 회사 지사의 기기, 다양한 판매 지점에 설치된 키오스크, ATM 및 터미널, 직원의 본사 기기)에 위치합니다. 일부 기기는 때때로 경계 밖으로 이동합니다(예: 지사 또는 고객 사무실을 방문하는 사용자의 랩톱).

계속 이동 사용자 기기의 보호를 모니터링하고 관리해야 합니다. 보호 상태에 대한 실제 정보를 수신하고 해당 기기의 보안 애플리케이션을 최신 상태로 유지해야 합니다. 예를 들어 이러한 기기가 기본 네트워크에서 떨어져있는 동안 떨어져 있는 동안 손상되면 기본 네트워크에 연결하는 즉시 위협을 전파하는 플랫폼이 될 수 있기 때문에 이는 중요합니다. 다음 두 가지 방법을 사용하여 이동 사용자 기기를 중앙 관리 서버에 연결할 수 있습니다.

- DMZ(완충 지역)의 연결 게이트웨이

  다음 데이터 트래픽 스키마를 참조하십시오. LAN의 중앙 관리 서버, 인터넷의 관리 중인 기기, 사용 중인 연결 게이트웨이.

- DMZ의 중앙 관리 서버

  다음 데이터 트래픽 스키마를 참조하십시오. DMZ의 중앙 관리 서버, 인터넷의 관리 중인 기기.

DMZ의 연결 게이트웨이

이동 사용자 기기를 중앙 관리 서버에 연결 시 권장되는 방법은 조직의 네트워크에 DMZ를 구성하고 DMZ에 연결 게이트웨이를 설치하는 것입니다. 외부 기기는 연결 게이트웨이에 연결되고 네트워크 내부의 중앙 관리 서버는 연결 게이트웨이를 통해 기기에 대한 연결을 시작합니다.

다른 방법에 비해 이 방법이 더 안전합니다.

- 네트워크 외부에서 중앙 관리 서버에 대한 액세스를 열 필요가 없습니다.
- 손상된 연결 게이트웨이가 네트워크 기기의 안전에 큰 위험이 되지 않습니다. 연결 게이트웨이는 자체적으로 아무것도 관리하지 않으며 연결을 설정하지도 않습니다.

또한 연결 게이트웨이에는 많은 하드웨어 리소스가 필요하지 않습니다.

그러나 이 방법에는 더 복잡한 구성 프로세스가 있습니다.

- 기기를 DMZ의 연결 게이트웨이로 사용하려면 네트워크 에이전트를 설치하고 이를 구체적인 방법으로 중앙 관리 서버에 연결해야 합니다.
- 모든 상황에서 중앙 관리 서버에 연결하는 데 동일한 주소를 사용할 수는 없습니다. 경계 외부에서 다른 주소(연결 게이트웨이 주소)는 물론 연결 게이트웨이를 통한 다른 연결 모드를 사용해야 합니다.
- 또한 다른 위치에 있는 랩톱에 대해 다른 연결 설정을 정의해야 합니다.

이전에 구성된 네트워크에 연결 게이트웨이를 추가하려면:

1. 연결 게이트웨이 모드에 네트워크 에이전트 설치.
2. 새로 추가된 연결 게이트웨이에 연결하려는 장치에 네트워크 에이전트를 다시 설치하십시오.

DMZ의 중앙 관리 서버

또 다른 방법은 DMZ에 단일 중앙 관리 서버를 설치하는 것입니다.

이 구성은 다른 방법보다 덜 안전합니다. 이때, 외부 랩톱을 관리하려면 중앙 관리 서버가 인터넷의 모든 주소에서의 연결을 허용해야 합니다. 그래도 여전히 내부 네트워크의 모든 기기를 관리하며 이러한 관리는 DMZ에서 이루어집니다. 따라서 완전히 손상된 서버는 이러한 이벤트가 발생할 가능성이 낮음에도 불구하고 엄청난 피해를 입힐 수 있습니다.

DMZ의 중앙 관리 서버가 내부 네트워크의 기기를 관리하지 않는 경우 위험이 상당히 낮아집니다. 예를 들어 서비스 공급업체는 이러한 구성을 사용하여 고객의 기기를 관리할 수 있습니다.

다음과 같은 경우 이 방법을 사용할 수 있습니다.

- 중앙 관리 서버 설치 및 구성에 익숙하고, 연결 게이트웨이를 설치 및 구성하는 다른 절차를 수행하지 않으려는 경우.
- 더 많은 기기를 관리해야 하는 경우. 중앙 관리 서버의 기기 지원 수는 최대 100,000대이며, 연결 게이트웨이는 최대 기기 10,000대를 지원할 수 있습니다.

이 솔루션에는 다음과 같은 어려움이 있을 수 있습니다.

- 중앙 관리 서버에는 더 많은 하드웨어 리소스와 하나 이상의 데이터베이스가 필요합니다.
- 기기에 대한 정보는 관련이 없는 두 개의 데이터베이스(네트워크 내부의 중앙 관리 서버 및 DMZ의 다른 중앙 관리 서버의 경우)에 저장되므로 모니터링이 복잡합니다.
- 모든 기기를 관리하려면 중앙 관리 서버를 계층 구조로 결합해야 하므로 모니터링뿐만 아니라 관리도 복잡합니다. 보조 중앙 관리 서버 인스턴스로 인해 관리 그룹의 가능한 구조에 제한이 발생합니다. 보조 중앙 관리 서버 인스턴스에 배포할 방법, 작업 및 정책을 결정해야 합니다.
- 외부의 DMZ에서 중앙 관리 서버를 사용하고 내부의 기본 중앙 관리 서버를 사용하도록 외부 기기를 구성하는 것은 게이트웨이를 통해 조건부 연결을 사용하도록 구성하는 것보다 간단하지 않습니다.
- 높은 보안 위험. 손상된 중앙 관리 서버 인스턴스는 관리 중인 랩톱을 쉽게 손상시킬 수 있습니다. 이러한 손상이 발생하면 해커는 랩톱 중 하나가 회사 네트워크로 돌아올 때까지 기다려야 로컬 영역 네트워크에 대한 공격을 계속할 수 있습니다.

중앙 관리 서버에 외부 데스크톱 기기 연결

항상 기본 네트워크 외부에 있는 데스크톱 기기(예: 회사 지사의 기기, 다양한 판매 지점에 설치된 키오스크, ATM 및 터미널, 직원의 본사 기기)는 중앙 관리 서버에 직접 연결할 수 없습니다. DMZ(완충 지역)에 설치된 연결 게이트웨이를 통해 중앙 관리 서버에 연결되어야 합니다. 이 구성은 해당 기기에 네트워크 에이전트를 설치할 때 설정됩니다.

중앙 관리 서버에 외부 데스크톱 기기를 연결하는 방법:

1. 네트워크 에이전트에 대한 새 설치 패키지를 생성합니다 .
2. 생성된 설치 패키지의 속성으로 이동하여 **고급** 섹션을 클릭한 다음 **연결 게이트웨이를 통해 중앙 관리 서버에 연결** 옵션을 선택합니다.

   연결 게이트웨이를 통해 중앙 관리 서버에 연결 설정은 **연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용** 설정과 호환되지 않습니다. 이 두 설정을 동시에 활성화할 수 없습니다.

3. **연결 게이트웨이 주소**에서 연결 게이트웨이의 공용 주소를 지정합니다.

   연결 게이트웨이가 NAT(Network Address Translation) 뒤에 있고 자체 공용 주소가 없는 경우 공용 주소에서 연결 게이트웨이의 내부 주소로 연결을 전달하도록 NAT 게이트웨이 규칙을 구성합니다.

4. 생성된 설치 패키지를 기반으로 독립 실행형 설치 패키지를 생성합니다.

5. 독립 실행형 설치 패키지를 전자적으로 또는 이동식 드라이브를 통해 대상 기기에 제공합니다.

6. 독립 실행형 패키지에서 네트워크 에이전트를 설치합니다.

외부 데스크톱 기기는 중앙 관리 서버에 연결됩니다.

이동 사용자를 위한 연결 프로필 정보

노트북(이하 "기기"로 지칭함)의 이동 사용자는 기업 네트워크의 기기 현재 위치에 따라 중앙 관리 서버 간을 전환하거나 중앙 관리 서버에 연결하는 방법을 변경해야 할 수 있습니다.

연결 프로필은 Windows 및 macOS를 실행 중인 기기에서만 지원됩니다.

단일 중앙 관리 서버의 여러 주소 사용

네트워크 에이전트가 설치된 기기는 조직의 인트라넷이나 인터넷에서 중앙 관리 서버에 연결할 수 있습니다. 이러한 상황에서는 네트워크 에이전트가 중앙 관리 서버에 연결하는 데 다른 주소를 사용해야 할 수 있습니다. 인터넷 연결에는 외부 중앙 관리 서버 주소를 사용하고, 내부 네트워크 연결에는 내부 중앙 관리 서버 주소를 사용할 수 있습니다.

이처럼 여러 중앙 관리 서버 주소를 사용하려면 인터넷에서 중앙 관리 서버에 연결하는 데 사용할 프로필을 네트워크 에이전트 정책에 추가해야 합니다. 정책 속성(**연결** 섹션, **연결 프로필** 하위 섹션)에서 프로필을 추가합니다. 프로필 만들기 창에서 **지정한 서버에서 업데이트만 다운로드** 옵션을 비활성화하고 **이 프로필에 지정된 중앙 관리 서버 설정과 연결 설정을 동기화** 옵션을 선택해야 합니다. 중앙 관리 서버에 접속할 때 연결 게이트웨이를 사용한다면(예, 인터넷 접속: 연결 게이트웨이로 DMZ에 있는 네트워크 에이전트에서 설명되어 있는 Kaspersky Security Center 구성), 해당 연결 프로필의 관련 필드에서 연결 게이트웨이 주소를 지정해야 합니다.

현재 네트워크에 따라 중앙 관리 서버 간 전환

조직이 각기 다른 중앙 관리 서버를 사용하는 여러 사무소를 운영하며 네트워크 에이전트가 설치된 기기 중 일부를 해당 사무소 간에 이동하는 경우에는 현재 기기가 있는 사무소 내 로컬 네트워크의 중앙 관리 서버에 네트워크 에이전트를 연결해야 합니다.

이 경우 원래 홈 중앙 관리 서버가 있는 본사 사무소를 제외한 각 사무소에 대해 네트워크 에이전트 정책의 속성에서 중앙 관리 서버 연결용 프로필을 만들어야 합니다. 연결 프로필에서 중앙 관리 서버 주소를 지정해야 하며 **지정한 서버에서 업데이트만 다운로드** 옵션을 활성화 또는 비활성화해야 합니다.

- 로컬 서버는 업데이트 다운로드용으로만 사용하고 홈 중앙 관리 서버와 네트워크 에이전트를 동기화해야 하는 경우 옵션을 선택합니다.
- 로컬 중앙 관리 서버를 통해서만 네트워크 에이전트를 관리해야 하는 경우 이 옵션을 비활성화합니다.

그 후에는 새로 만든 프로필로 전환할 조건을 설정해야 합니다: 본사 사무소를 제외한 각 사무소에 대해 조건을 하나 이상 설정합니다. 모든 조건은 사무소의 네트워크 환경과 관련된 항목을 탐지하는 데 사용됩니다. 조건이 참이면 해당 프로필이 활성화됩니다. 참인 조건이 없으면 네트워크 에이전트가 홈 중앙 관리 서버로 전환됩니다.

이동 사용자에 대한 연결 프로필 만들기

중앙 관리 서버 연결 프로필은 Windows 및 macOS를 실행 중인 기기에서만 사용 가능합니다.

이동 사용자에 대한 중앙 관리 서버 네트워크 에이전트 연결 프로필을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 중앙 관리 서버에 네트워크 에이전트를 연결하기 위한 프로필을 만들어야 하는 클라이언트 기기를 포함한 관리 그룹을 선택합니다.

2. 다음 중 하나를 수행합니다:

   - 그룹의 모든 기기에 대한 연결 프로필을 만들려면 **정책** 탭에서 그룹 작업 영역에 있는 네트워크 에이전트 정책을 선택합니다. 선택한 정책의 속성 창을 엽니다.

   - 그룹 내 한 기기의 연결 프로필을 만들려면 **기기** 탭에서 그룹 작업 영역에 있는 기기를 선택하고 다음 동작을 수행합니다.

     a. 선택한 기기의 속성 창을 엽니다.

     b. 기기 속성 창의 **애플리케이션** 섹션에서 네트워크 에이전트를 선택합니다.

     c. 네트워크 에이전트 속성 창을 엽니다.

3. 속성 창의 **연결성** 섹션에서 **연결 프로필** 하위 섹션을 선택합니다.

4. **중앙 관리 서버 연결 프로필** 설정 그룹에서 **추가** 버튼을 누릅니다.

   기본적으로 연결 프로필 목록에는 <오프라인 모드> 및 <홈 중앙 관리 서버> 프로필이 포함됩니다. 이러한 프로필은 편집하거나 제거할 수 없습니다.

   <오프라인 모드> 프로필에는 연결할 서버가 지정되어 있지 않습니다. 따라서 이 프로필로 전환하는 네트워크 에이전트는 클라이언트 기기에 설치되어 있는 애플리케이션에서 이동 사용자 정책을 사용하여 작업하는 동안 중앙 관리 서버에 연결을 시도하지 않습니다. 네트워크에서 기기 연결이 끊어진 경우 <오프라인 모드> 프로필을 사용할 수 있습니다.

   <홈 중앙 관리 서버> 프로필은 네트워크 에이전트 설치 시 선택한 중앙 관리 서버에 대한 연결을 지정합니다. 기기를 일정 시간 동안 외부 네트워크에서 실행하다가 홈 중앙 관리 서버에 다시 연결하면 <홈 중앙 관리 서버> 프로필이 적용됩니다.

5. **새 프로필** 창이 열리면 다음과 같이 연결 프로필을 구성합니다.

   - **프로필 이름**

     입력 필드에서 연결 프로필 이름을 보거나 변경할 수 있습니다.

   - **중앙 관리 서버**

     프로필 활성화 중에 클라이언트 기기가 연결해야 하는 중앙 관리 서버의 주소입니다.

- **포트**

  연결에 사용되는 포트 번호.

- **SSL 포트**

  SSL 프로토콜을 사용하는 경우 연결용 포트 번호입니다.

- **SSL 사용**

  이 옵션을 사용하면 SSL 프로토콜을 사용하여 보안 포트를 통해 연결됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 연결이 안전하게 유지되도록 이 옵션을 비활성화하지 않는 것이 좋습니다.

- **프록시 서버를 통한 연결 구성** 링크를 눌러 프록시 서버를 통한 연결을 구성합니다: 인터넷에 연결할 때 프록시 서버를 사용하려면 **프록시 서버 사용** 옵션을 선택합니다. 이 옵션을 선택하면 설정을 입력하는 필드를 사용할 수 있게 됩니다. 프록시 서버 연결에 대해 다음 설정을 지정합니다.

  - **프록시 서버 주소**

    Kaspersky Security Center에서 인터넷 연결에 사용한 프록시 서버의 주소입니다.

  - **포트 번호**

    Kaspersky Security Center 프록시 연결을 설정하는 데 사용되는 포트 번호입니다.

  - **프록시 서버 인증**

    이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.

    프록시 서버 사용 확인란을 선택하면 이 입력 필드를 사용할 수 있습니다.

  - **사용자 이름**(**프록시 서버 인증** 옵션을 선택하면 이 필드를 사용할 수 있습니다)

    프록시 서버에 대한 연결을 구성할 사용자 계정입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

  - **암호**(**프록시 서버 인증** 옵션을 선택하면 이 필드를 사용할 수 있습니다)

    프록시 서버 연결을 구성한 계정의 사용자가 설정한 암호입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

    입력한 암호를 보려면 **보기** 버튼을 필요한 시간 동안 누르고 있어야 합니다.

- **연결 게이트웨이 설정**

  클라이언트 기기가 중앙 관리 서버에 연결할 때 사용하는 게이트웨이의 주소입니다.

- **이동 사용자 모드 사용**

  이 옵션을 사용하면 이 프로필을 통해 연결하는 경우 클라이언트 기기에 설치된 애플리케이션은 이동 사용자 정책뿐만 아니라 이동 사용자 모드에 있는 기기를 위한 정책 프로필을 사용합니다. 애플리케이션에 대해 이동 사용자 정책이 정의되어 있지 않은 경우에는 활성 정책이 사용됩니다.

  이 옵션을 비활성화하면 애플리케이션에서 활성 정책을 사용합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **지정한 서버에서 업데이트만 다운로드**

  이 옵션을 사용하면 클라이언트 기기에 설치된 애플리케이션을 통해 업데이트를 다운로드하는 데에만 프로필이 사용됩니다. 다른 작업의 경우 네트워크 에이전트 설치 중 정의된 초기 연결 설정에 따라 중앙 관리 서버와의 연결이 설정됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **이 프로필에 지정된 중앙 관리 서버 설정과 연결 설정을 동기화**

  이 옵션을 사용하면 네트워크 에이전트는 프로필에 지정된 설정을 사용해 중앙 관리 서버에 연결합니다.

  이 옵션을 비활성화하면 네트워크 에이전트는 설치하는 동안 지정되었던 원본 설정을 사용해 중앙 관리 서버에 연결합니다.

  이 옵션은 **지정한 서버에서 업데이트만 다운로드** 옵션이 비어 있는 경우에 사용 가능합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

6. 클라이언트 기기에 설치된 애플리케이션이 이동 사용자 모드의 기기에 대해 정책 프로필을 사용하는 동시에, 중앙 관리 서버를 사용할 수 없는 경우 모든 연결 시도에서 이동 사용자 정책을 사용하도록 허용하려면 **중앙 관리 서버에 연결할 수 없으면 이동 사용자 모드 사용** 옵션을 선택합니다. 애플리케이션에 대해 이동 사용자 정책이 정의되어 있지 않은 경우에는 활성 정책이 사용됩니다.

그러면 이동 사용자에 대해 네트워크 에이전트를 중앙 관리 서버에 연결하는 프로필이 만들어집니다. 네트워크 에이전트가 이 프로필을 사용하여 중앙 관리 서버에 연결했다면 클라이언트 기기에 설치된 애플리케이션은 이동 사용자 정책 또는 이동 사용자 모드에 있는 기기를 위한 정책을 사용합니다.

다른 중앙 관리 서버로 네트워크 에이전트 전환 정보

중앙 관리 서버에 대한 네트워크 에이전트 연결의 초기 설정은 네트워크 에이전트가 설치될 때 정의됩니다. 네트워크 에이전트를 다른 중앙 관리 서버로 전환하려면 전환 규칙을 사용할 수 있습니다. 이 기능은 Windows 또는 macOS를 실행하는 기기에 설치된 네트워크 에이전트에서만 지원됩니다.

전환 규칙은 다음 네트워크 매개변수 변경 시 트리거할 수 있습니다.

- 기본 게이트웨이 주소.
- DHCP(Dynamic Host Configuration Protocol) 서버의 IP 주소.
- 서브넷의 DNS 접미사.
- 네트워크 DNS 서버의 IP 주소.
- Windows 도메인 접근성. 이 파라미터는 Windows를 실행하는 기기에서만 사용할 수 있습니다.

- 서브넷 주소 및 마스크.
- 네트워크 WINS 서버의 IP 주소. 이 파라미터는 Windows를 실행하는 기기에서만 사용할 수 있습니다.
- 클라이언트 기기의 DNS 또는 NetBIOS 이름.
- SSL 연결 주소 접근성.

네트워크 에이전트를 다른 중앙 관리 서버로 전환하는 규칙을 만들 시, 네트워크 에이전트에서 네트워크 설정의 변경 사항에 다음과 같이 대응합니다:

- 네트워크 설정이 작성된 규칙 중 하나와 일치하는 경우 네트워크 에이전트가 이 규칙에 지정된 중앙 관리 서버에 연결됩니다. 클라이언트 기기에 설치된 애플리케이션이 이동 사용자 정책으로 전환됩니다(규칙에 지정된 경우).
- 기존의 어떤 규칙도 적용할 수 없는 경우 네트워크 에이전트가 설치 시 정의된 중앙 관리 서버에 대한 기본 연결 설정으로 되돌아갑니다. 클라이언트 기기에 설치된 애플리케이션이 활성 정책으로 다시 전환됩니다.
- 중앙 관리 서버에 접근할 수 없는 경우 네트워크 에이전트는 이동 사용자 정책을 사용합니다.

> 네트워크 에이전트 정책 설정에서 **중앙 관리 서버에 연결할 수 없으면 이동 사용자 모드 사용** 옵션이 활성화되어 있는 경우에만 네트워크 에이전트가 이동 사용자 정책으로 전환합니다.

중앙 관리 서버에 대한 네트워크 에이전트 연결 설정은 연결 프로필에 저장됩니다. 연결 프로필에서는 클라이언트 기기를 이동 사용자 정책으로 전환하는 규칙을 만들 수 있을 뿐 아니라 업데이트 다운로드에만 사용되는 프로필을 구성할 수도 있습니다.

네트워크 위치에 따른 네트워크 에이전트 전환 규칙 만들기

> 네트워크 위치에 따른 네트워크 에이전트 전환은 Windows 및 macOS를 실행 중인 기기에서만 사용 가능합니다.

네트워크 설정이 변경되는 경우 중앙 관리 서버 간에 네트워크 에이전트를 전환하는 규칙을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 네트워크 위치 설명에 의해 네트워크 에이전트 전환 규칙을 만들어야 하는 기기를 포함한 관리 그룹을 선택합니다.
2. 다음 중 하나를 수행합니다:
   - 그룹의 모든 기기에 대한 규칙을 만들려면 **정책** 탭에서 그룹 작업 영역으로 이동하여 네트워크 에이전트 정책을 선택합니다. 선택한 정책의 속성 창을 엽니다.
   - 그룹에서 선택한 기기에 대한 규칙을 만들려면 그룹 작업 영역으로 이동한 후 **기기** 탭에서 기기를 선택하고 다음 동작을 수행합니다.
     a. 선택한 기기의 속성 창을 엽니다.
     b. 기기 속성 창의 **애플리케이션** 섹션에서 네트워크 에이전트를 선택합니다.
     c. 네트워크 에이전트 속성 창을 엽니다.

3. **속성** 창이 열리면 **연결성** 섹션에서 **연결 프로필** 하위 섹션을 선택합니다.

4. **네트워크 위치 설정** 섹션에서 **추가** 버튼을 클릭합니다.

5. **새로운 설명** 창이 열리면 네트워크 위치 설명 및 전환 규칙을 구성합니다. 다음과 같은 네트워크 위치 설명 설정을 지정합니다:

   - **네트워크 위치 설명 이름**

     네트워크 위치 설명의 이름은 255자를 초과할 수 없으며 ("*<>?\/:|).

   - **연결 프로필 사용**

     드롭다운 목록에서 네트워크 에이전트가 중앙 관리 서버에 연결하는 데 사용하는 연결 프로필을 지정할 수 있습니다. 네트워크 위치 설명 조건을 충족하면 이 프로필이 사용됩니다. 연결 프로필은 네트워크 에이전트의 중앙 관리 서버 연결을 위한 설정을 포함하며, 클라이언트 기기가 이동 사용자 정책으로 전환해야 하는 시기도 정의합니다. 이 정책은 업데이트를 다운로드하는 데에만 사용됩니다.

6. **전환 조건** 섹션에서 **추가** 버튼을 눌러 네트워크 위치 설명 조건 목록을 만듭니다.

   한 규칙의 조건은 논리 연산자 AND를 사용하여 결합됩니다. 네트워크 위치 설명에 따라 전환 규칙을 활성화하려면 모든 규칙 전환 조건이 충족되어야 합니다.

7. 드롭 다운 목록에서 클라이언트 기기가 연결된 네트워크 특성의 변경 사항에 해당하는 값을 선택할 수 있습니다:

   - **기본 연결 게이트웨이 주소** – 기본 네트워크 게이트웨이의 주소가 변경된 경우.
   - **DHCP 서버 주소** – 네트워크 DHCP(Dynamic Host Configuration Protocol) 서버의 IP 주소가 변경된 경우.
   - **DNS 도메인** - 서브넷의 DNS 접미사가 변경된 경우.
   - **DNS 서버 주소** – 네트워크 DNS 서버의 IP 주소가 변경된 경우.
   - **Windows 도메인 접근 가능성(Windows 전용)** – 클라이언트 기기가 연결된 Windows 도메인의 상태를 변경합니다. 이 설정은 Windows를 실행하는 기기에만 사용합니다.
   - **서브넷** – 서브넷 주소 및 마스크를 변경합니다.
   - **WINS 서버 주소(Windows 전용)** – 네트워크 WINS 서버의 IP 주소가 변경된 경우. 이 설정은 Windows를 실행하는 기기에만 사용합니다.
   - **이름 해석 가능성** - 클라이언트 기기의 DNS 또는 NetBIOS 이름이 변경되었습니다.
   - **SSL 연결 주소의 가용성** - 클라이언트 기기는 지정한 서버(이름:포트)와 SSL 연결을 설정할 수 있거나 설정할 수 없습니다(선택한 옵션에 따라 다름). 각 서버에 대해 SSL 인증서를 추가로 지정할 수 있습니다. 이 경우 네트워크 에이전트는 SSL 연결 기능은 물론 서버 인증서를 확인합니다. 인증서가 일치하지 않으면 연결이 실패합니다. 연결 주기는 1분에 1회입니다.

8. 열린 창에서 네트워크 에이전트가 다른 중앙 관리 서버로 전환되는 조건을 지정할 수 있습니다. 창 이름은 이전 단계에서 선택한 값에 따라 달라집니다. 전환 조건의 다음 설정을 지정합니다:

   - **값**

     이 필드에서는 만들고 있는 조건에 대한 값을 하나 이상 추가할 수 있습니다.

   - **위 목록의 값 중 하나 이상과 일치하는 경우**

     이 옵션을 선택하면 **값** 목록에 지정된 값 중 하나 이상과 일치하면 조건이 충족됩니다.
     기본적으로 이 옵션은 선택되어 있습니다.

   - **위 목록의 어떤 값과도 일치하지 않는 경우**

     이 옵션을 선택하면 값이 **값** 목록에 없는 경우 조건이 충족됩니다.

9. **새로운 설명** 창에서 **설명 사용** 옵션을 선택하여 새 네트워크 위치 설명을 사용하도록 설정합니다.

   네트워크 위치 설명에 의해 새 전환 규칙이 만들어지고, 조건이 충족될 때마다 네트워크 에이전트에서 규칙에 지정된 연결 프로필을 사용하여 중앙 관리 서버에 연결합니다.

네트워크 위치 설명은 목록에 표시되는 순서대로 네트워크 레이아웃과 일치하는지 확인됩니다. 네트워크와 일치하는 설명이 여러 개 있는 경우 첫 번째 규칙이 사용됩니다. **위로** 버튼(⬆) 및 **아래로** 버튼(⬇) 버튼을 사용하여 목록에서 규칙의 순서를 변경할 수 있습니다.

이벤트 알림

이 섹션에서는 클라이언트 기기의 이벤트에 대한 알림을 관리자에게 전달할 방법을 선택하고 이벤트 알림 설정을 구성하는 방법을 설명합니다.

또한 Eicar 테스트 바이러스를 사용하여 이벤트 알림 배포를 테스트하는 방법도 설명합니다.

이벤트 알림 구성

Kaspersky Security Center에서는 클라이언트 기기에서 발생하는 이벤트를 관리자에게 알리기 위한 방법을 선택하고 알림을 구성할 수 있습니다:

- 이메일. 이벤트가 발생하면 애플리케이션이 지정된 이메일 주소로 알림을 보냅니다. 알림 텍스트는 편집할 수 있습니다.
- SMS. 이벤트가 발생하면 애플리케이션이 지정된 전화 번호로 알림을 보냅니다. 메일 게이트웨이를 통해 SMS 알림을 보내도록 구성할 수 있습니다.
- 실행 파일. 기기에서 이벤트가 발생하면 관리자 워크스테이션에서 실행 파일이 시작됩니다. 관리자는 이 실행 파일을 사용하여 발생한 이벤트의 파라미터를 받을 수 있습니다.

클라이언트 기기에서 발생하는 이벤트의 알림을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **알림 구성 및 이벤트 내보내기** 링크를 누르고 드롭다운 목록에서 **알림 구성** 값을 선택합니다.
   그러면 **속성: 이벤트** 창이 열립니다.
4. **알림** 섹션에서 알림 방법을 선택(이메일, 문자 또는 실행 파일 실행)하고 알림 설정을 정의합니다:

- **이메일**

이메일 탭에서 이메일로 이벤트 알림을 구성할 수 있습니다.

받는 사람(이메일 주소) 필드에서 애플리케이션이 알림을 보낼 이메일 주소를 지정합니다. 이 필드에서 세미콜론으로 구분해 여러 주소를 지정할 수 있습니다.

SMTP 서버 필드에서 세미콜론으로 구분해 이메일 서버 주소를 지정합니다. 다음 값을 사용할 수 있습니다:

- IPv4 또는 IPv6 주소
- 기기의 Windows 네트워크 이름(NetBIOS 이름)
- SMTP 서버의 DNS 이름

SMTP 서버 포트 필드에서 SMTP 서버 통신 포트의 번호를 지정합니다. 기본 포트 번호는 25입니다.

DNS MX 룩업 사용 옵션을 활성화하면 SMTP 서버의 동일한 DNS 이름에 대해 IP 주소의 여러 MX 레코드를 사용할 수 있습니다. 동일한 DNS 이름에는 이메일 메시지 수신 우선 순위 값이 다른 여러 MX 레코드가 있을 수 있습니다. 중앙 관리 서버는 MX 레코드 우선 순위의 오름차순으로 SMTP 서버에 이메일 알림을 보내려고 시도합니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

> **DNS MX 룩업 사용** 옵션을 활성화하고 TLS 설정을 활성화하지 않는 경우에는 이메일 알림 전송을 위한 ㅜ가 보호 수단으로 서버 기기에 DNSSEC 설정을 사용하는 것이 좋습니다.

설정 링크를 눌러 추가 알림을 설정:

- 도메인 이름(이메일 메시지의 도메인 이름)
- 발신자 이메일 주소
- ESMTP 인증 설정

SMTP 서버에 대한 ESMTP 인증 옵션이 활성화된 경우 SMTP 서버에서 인증용 계정을 지정해야 합니다.

- SMTP 서버에 대한 TLS 설정:
  - **TLS 사용하지 않음**

    이메일 메시지 암호화를 비활성화하려는 경우 이 옵션을 선택할 수 있습니다.
  - **SMTP 서버에서 지원 시 TLS 사용**

    SMTP 서버에 대한 TLS 연결을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 TLS를 사용하지 않고 SMTP 서버에 연결합니다.
  - **항상 TLS 사용, 서버 인증서 유효성 확인**

TLS 인증 설정을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 SMTP 서버에 연결할 수 없습니다.

SMTP 서버와의 연결을 보다 잘 보호하려면 이 옵션을 사용하는 것이 좋습니다. 이 옵션을 선택하면 TLS 연결에 대한 인증 설정을 설정할 수 있습니다.

항상 TLS를 사용하고 서버 인증서의 유효성을 확인하십시오 값을 선택한 경우에는 SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

다음과 같이 SMTP 서버에 대한 TLS 설정을 지정할 수 있습니다.

- 다음 SMTP 서버 인증서 파일을 찾습니다.

신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 중앙 관리 서버에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

- 다음과 같이 클라이언트 인증서 파일을 찾습니다.

신뢰할 수 있는 인증 기관과 같은 다양한 출처에서 수신된 인증서를 사용할 수 있습니다. 다음 인증서 유형 중 하나를 사용하여 인증서와 개인 키를 지정해야 합니다:

- X-509 인증서:

인증서가 있는 파일과 개인 키가 있는 파일을 지정해야 합니다. 두 파일은 서로 의존하지 않으며 파일의 로딩 순서는 중요하지 않습니다. 두 파일이 모두 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

- pkcs12 컨테이너:

인증서와 개인 키가 포함 된 단일 파일을 업로드해야 합니다. 파일이 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

알림 메시지 필드는 이벤트가 일어날 때 애플리케이션이 보내는 해당 이벤트에 대한 정보의 표준 문구를 포함하고 있습니다. 이 문구에는 이벤트 이름, 기기 이름 및 도메인 이름과 같은 대체 파라미터가 포함됩니다. 해당 이벤트에 더 많은 관련 세부 사항을 포함하고 있는 다른 대체 파라미터를 추가해 메시지 문구를 편집할 수 있습니다. 필드의 오른쪽에 있는 버튼을 누르면 대체 파라미터 목록을 이용할 수 있습니다.

만일 알림 텍스트가 % 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 입력해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

테스트 메시지 전송 버튼을 눌러 알림을 올바르게 구성했는지 확인하십시오. 애플리케이션은 지정한 이메일 주소로 테스트 알림을 보내야 합니다.

- **SMS**

SMS 탭은 휴대폰으로 여러 이벤트에 대한 SMS 알림 전송 구성을 허용합니다. SMS 메시지는 메일 게이트웨이를 통해 전송됩니다.

받는 사람(이메일 주소) 필드에서 애플리케이션이 알림을 보낼 이메일 주소를 지정합니다. 이 필드에서 세미콜론으로 구분해 여러 주소를 지정할 수 있습니다. 지정한 이메일 주소와 연결된 전화 번호로 알림이 전달됩니다.

SMTP 서버 필드에서 세미콜론으로 구분해 이메일 서버 주소를 지정합니다. 다음 값을 사용할 수 있습니다:

- IPv4 또는 IPv6 주소
- 기기의 Windows 네트워크 이름(NetBIOS 이름)
- SMTP 서버의 DNS 이름

SMTP 서버 포트 필드에서 SMTP 서버 통신 포트의 번호를 지정합니다. 기본 포트 번호는 25입니다.

설정 링크를 눌러 추가 알림을 설정:

- 도메인 이름(이메일 메시지의 도메인 이름)
- 발신자 이메일 주소
- ESMTP 인증 설정

필요할 시 SMTP 서버에 대해 ESMTP 인증 옵션이 활성화된 경우 SMTP 서버에서 인증을 위한 계정을 지정할 수 있습니다.

- SMTP 서버에 대한 TLS 설정

TLS 사용을 비활성화하거나, SMTP 서버가 이 프로토콜을 지원하는 경우 TLS를 사용하거나 또는 TLS만 사용하도록 강제할 수 있습니다. TLS만 사용하도록 선택한 경우에는 SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, TLS만 사용하도록 선택한 경우 SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

- SMTP 서버 인증서 파일 찾아보기

신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 Kaspersky Security Center에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

인증서와 개인 키가 포함 된 단일 파일을 업로드해야 합니다. 파일이 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다. **알림 메시지** 필드는 이벤트가 발생할 때 애플리케이션이 보내는 해당 이벤트에 대한 정보의 표준 문구를 포함하고 있습니다. 이 문구에는 이벤트 이름, 기기 이름 및 도메인 이름과 같은 대체 파라미터가 포함됩니다. 해당 이벤트에 더 많은 관련 세부 사항을 포함하고 있는 다른 대체 파라미터를 추가해 메시지 문구를 편집할 수 있습니다. 필드의 오른쪽에 있는 버튼을 누르면 대체 파라미터 목록을 이용할 수 있습니다.

만일 알림 텍스트가 % 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 입력해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

Configure numeric limit of notifications 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

알림이 제대로 구성되었는지 확인하려면 **테스트 메시지 전송** 버튼을 클릭합니다. 애플리케이션은 지정한 수신자에게 테스트 알림을 보내야 합니다.

- **실행되는 실행 파일**

이 알림 방법을 선택하면 입력 필드에 이벤트가 발생할 때 시작되는 애플리케이션을 지정할 수 있습니다.

알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격에서 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

테스트 메시지 전송을 누르면 알림을 제대로 구성했는지 확인할 수 있습니다: 애플리케이션은 지정한 이메일 주소로 테스트 알림을 보냅니다.

5. **알림 메시지** 필드에서 이벤트가 발생할 때 애플리케이션이 보낼 문구를 입력합니다.

   이벤트 상세 정보(예: 이벤트 설명, 발생 시기 등)와 함께 대체 설정을 추가하기 위해 텍스트 필드의 오른쪽에 있는 드롭다운 목록을 사용할 수 있습니다.

   만일 알림 텍스트가 퍼센트(%) 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 지정해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

6. 알림이 제대로 구성되었는지 확인하려면 **테스트 메시지 전송** 버튼을 누릅니다.

   애플리케이션은 지정된 사용자에게 테스트 알림을 전송합니다.

7. **확인**을 눌러 변경을 저장합니다.

클라이언트 기기에서 발생하는 모든 이벤트에 새롭게 조정된 알림 설정이 적용됩니다.

중앙 관리 서버 설정, 정책 설정 또는 애플리케이션 설정의 **이벤트 구성** 섹션에서 특정 이벤트에 대한 알림 설정을 재정의할 수 있습니다.

테스트 알림

이벤트 알림의 배포 여부를 확인하기 위해 애플리케이션은 클라이언트 기기의 EICAR 테스트 "바이러스" 탐지 알림을 사용합니다.

이벤트 알림 배포를 확인하려면 다음과 같이 하십시오:

1. 클라이언트 기기에 대한 실시간 파일 시스템 보호 작업을 중지하고 EICAR 테스트 "바이러스"를 클라이언트 기기로 복사합니다. 이제 파일 시스템의 실시간 보호를 다시 활성화합니다.

2. 관리 그룹의 클라이언트 기기 또는 특정 기기(EICAR "바이러스"가 있는 기기 포함)에 대해 검사 작업을 실행합니다.

   검사 작업이 올바르게 구성된 경우 테스트 "바이러스"가 탐지됩니다. 알림이 올바르게 구성된 경우 바이러스가 탐지되었다는 알림이 표시됩니다.

   중앙 관리 서버 노드의 작업 영역에서 **이벤트** 탭을 보면 **최근 이벤트** 조회에 "바이러스" 탐지 기록이 표시됩니다.

EICAR 테스트 "바이러스"에는 기기에 피해를 줄 수 있는 코드가 포함되어 있지 않습니다. 그러나 대부분의 제조업체의 보안 제품은 이 파일을 바이러스로 식별합니다. 공식 EICAR 웹사이트에서 테스트 "바이러스"를 다운로드할 수 있습니다.

실행 파일을 실행하면 표시되는 이벤트 알림

Kaspersky Security Center는 실행 파일을 실행하여 클라이언트 기기의 이벤트에 대한 알림을 관리자에게 제공할 수 있습니다. 실행 파일은 관리자에게 전달할 이벤트 자리 표시자가 있는 다른 실행 파일을 반드시 포함해야 합니다(아래 표 참조).

이벤트를 설명하기 위한 자리 표시자

자리 표시자	자리 표시자 설명
%SEVERITY%	이벤트 심각도. 가능한 값: • **정보** • **경고** • **오류** • **심각**
%COMPUTER%	이벤트가 발생한 기기 이름. 기기 이름은 최대 256자입니다.
%DOMAIN%	이벤트가 발생한 기기 도메인 이름.
%EVENT%	이벤트 유형 이름. 이벤트 유형 이름은 최대 50자입니다.
%DESCR%	이벤트 설명. 설명은 최대 1,000자입니다.
%RISE_TIME%	이벤트 생성 시각.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	작업 이름. 작업 이름은 최대 100자입니다.
%KL_PRODUCT%	애플리케이션 이름.
%KL_VERSION%	애플리케이션 버전 번호.
%KLCSAK_EVENT_SEVERITY_NUM%	이벤트 심각도 번호. 가능한 값: • 1 – **정보** • 2 – **경고** • 3 – **오류** • 4 – **심각**
%HOST_IP%	이벤트가 발생한 기기 IP 주소.
%HOST_CONN_IP%	이벤트가 발생한 기기 연결 IP 주소.

예:
이벤트 알림은 script1.bat와 같은 실행 파일을 통해 전송됩니다. 이 파일 내에는 %COMPUTER% 자리 표시자가 시작된 script2.bat 등의 다른 실행 파일이 들어 있습니다. 이벤트가 발생하면 관리자 기기에서 script1.bat 파일이 실행됩니다. 그러면 %COMPUTER% 자리 표시자가 포함된 script2.bat 파일이 실행됩니다. 따라서 관리자는 이벤트가 발생한 기기의 이름을 수신합니다.

TLS를 사용하여 통신 암호화

조직의 기업 네트워크에서 취약점을 수정하려면 TLS 프로토콜을 사용하여 트래픽 암호화를 활성화할 수 있습니다. 중앙 관리 서버 및 iOS MDM 서버에서 TLS 암호화 프로토콜과 지원되는 암호 그룹을 활성화할 수 있습니다. Kaspersky Security Center는 TLS 프로토콜 버전 1.0, 1.1, 1.2, 1.3을 지원합니다. 필요한 암호화 프로토콜과 암호 그룹을 선택할 수 있습니다.

Kaspersky Security Center는 자체 서명된 인증서를 사용합니다. iOS 기기를 추가로 구성할 필요는 없습니다. 자체 인증서를 사용할 수도 있습니다. Kaspersky 전문가의 권장 사항에 따라 신뢰할 수 있는 인증 기관에서 발급한 인증서를 사용하는 것이 좋습니다.

중앙 관리 서버

중앙 관리 서버에서 허용되는 암호화 프로토콜 및 암호 그룹을 구성하려면:

1. 관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

2. SrvUseStrictSslSettings 플래그를 사용하여 중앙 관리 서버에서 허용되는 암호화 프로토콜 및 암호 그룹을 구성합니다. 다음 명령을 실행합니다:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <값> -t d
   ```

   SrvUseStrictSslSettings 플래그의 <value> 파라미터를 지정합니다.

   - 4 –TLS 1.2 및 TLS 1.3 프로토콜만 활성화됩니다. 또한 TLS_RSA_WITH_AES_256_GCM_SHA384가 포함된 암호 그룹이 활성화됩니다(이 암호 그룹은 이전 Kaspersky Security Center 버전의 하위 호환성을 위해 필요합니다). 이는 기본값입니다.

     TLS 1.2 프로토콜에서 지원하는 암호 그룹:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384(TLS_RSA_WITH_AES_256_GCM_SHA384를 사용한 암호 그룹)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     TLS 1.3 프로토콜에서 지원하는 암호 그룹:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5 –TLS 1.2 및 TLS 1.3 프로토콜만 활성화됩니다. TLS 1.2 및 TLS 1.3 프로토콜에서는 아래 나열된 특정 암호 그룹을 지원합니다.

     TLS 1.2 프로토콜에서 지원하는 암호 그룹:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

TLS 1.3 프로토콜에서 지원하는 암호 그룹:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

SrvUseStrictSslSettings 플래그의 파라미터 값으로 0, 1, 2, 3은 사용하지 않을 것을 권장합니다. 이러한 파라미터 값은 안전하지 않은 TLS 프로토콜 버전(TLS 1.0 및 TLS 1.1 프로토콜) 및 안전하지 않은 암호 그룹에 해당하며, 이전 Kaspersky Security Center 버전과의 호환성을 위해서만 사용됩니다.

3. 다음 Kaspersky Security Center 15.1 서비스를 다시 시작하십시오.
   - 중앙 관리 서버
   - 웹 서버
   - 활성화 프록시

TLS 프로토콜을 사용한 트래픽 암호화가 활성화됩니다.

KLTR_TLS12_ENABLED 및 KLTR_TLS13_ENABLED 플래그를 사용하여 각각 TLS 1.2 및 TLS 1.3 프로토콜 지원을 활성화할 수 있습니다. 이러한 플래그는 기본적으로 활성화되어 있습니다.

TLS 1.2 및 TLS 1.3 프로토콜 지원을 활성화하거나 비활성화하려면:

1. klscflag 유틸리티를 실행합니다.

   관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

2. 관리자 권한을 사용하여 Windows 명령 프롬프트에서 다음 명령 중 하나를 입력합니다.
   - TLS 1.2 프로토콜 지원을 활성화하거나 비활성화하려면 다음 명령을 사용합니다.

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <값> -t d
     ```

   - TLS 1.3 프로토콜 지원을 활성화하거나 비활성화하려면 다음 명령을 사용합니다.

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <값> -t d
     ```

   플래그의 <값> 파라미터를 지정합니다.

   - `1`–TLS 프로토콜 지원을 활성화합니다.
   - `0`–TLS 프로토콜 지원을 비활성화합니다.

iOS MDM 서버

iOS 기기와 iOS MDM 서버 간의 연결은 기본적으로 암호화됩니다.

iOS MDM 서버에서 허용되는 암호화 프로토콜 및 암호 그룹을 구성하려면 다음과 같이 하십시오:

1. iOS MDM 서버가 설치된 클라이언트 기기에서 시스템 레지스트리를 엽니다(예:로컬에서 **시작 → 실행** 메뉴의 regedit 명령 사용).
2. 다음 하이브로 이동합니다:
   - 32비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - 64비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. `StrictSslSettings` 이름으로 키를 만듭니다.
4. 키 유형으로 `DWORD`를 지정합니다.
5. 키 값 지정:
   - `2` - TLS 1.0, TLS 1.1, TLS 1.2 프로토콜이 활성화됩니다.
   - `3` - TLS 1.2 프로토콜만 활성화됩니다(기본값).
6. Kaspersky Security Center iOS MDM 서버 서비스를 다시 시작합니다.

인터페이스 구성

Kaspersky Security Center 인터페이스를 구성할 수 있습니다.

- 사용하는 기능에 따라 콘솔 트리, 작업 영역, 개체(폴더, 섹션) 창 속성에서 개체를 보이거나 숨기기.
- 메인 창의 요소를 보이거나 숨기기(예, 콘솔 트리, **처리** 및 **보기**와 같은 표준 메뉴 등).

현재 사용 중인 기능 세트에 따라 Kaspersky Security Center 인터페이스를 구성하려면:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 메인 애플리케이션 창의 메뉴 표시줄에서 **보기 → 인터페이스 구성**을 선택합니다.
3. 열리는 **인터페이스 구성** 창에서 다음과 같은 확인란을 사용하여 인터페이스 요소가 표시되는 방식을 구성합니다:
   - **취약점 및 패치 관리 표시**

     이 옵션을 사용하면 **원격 설치** 폴더에 **기기 이미지 배포** 하위 폴더가 표시되고, **저장소** 폴더에는 **하드웨어** 하위 폴더가 표시됩니다.

빠른 시작 마법사가 완료되지 않은 경우 이 옵션은 기본적으로 비활성화되어 있습니다. 이 옵션은 빠른 시작 마법사가 완료된 후 기본적으로 활성화됩니다.

이 옵션이 비활성화되면 시스템 관리 라이센스가 있어도 **RDP 세션 생성** 및 **Windows Desktop Sharing** 메뉴 항목을 사용할 수 없습니다.

- **데이터 암호화 및 보호 표시**

  이 옵션을 사용하면 콘솔 트리에서 **데이터 암호화 및 보호** 폴더를 표시합니다.
  기본적으로 이 옵션은 켜져 있습니다.

- **엔드포인트 제어 설정 표시**

  이 옵션을 사용하면 Kaspersky Endpoint Security for Windows 정책 속성 창의 **보안 제어** 섹션에 다음 하위 섹션이 표시됩니다:
  - **애플리케이션 제어**
  - **매체 제어**
  - **웹 제어**
  - **적응형 이상 행위 제어**

  이 옵션을 선택 해제하면 해당 하위 섹션이 **보안 제어** 섹션에 표시되지 않습니다.
  기본적으로 이 옵션은 켜져 있습니다.

- **모바일 기기 관리 표시**

  이 옵션을 사용하면 **모바일 기기 관리** 기능을 사용할 수 있습니다. 애플리케이션을 다시 시작하고 나면 **모바일 기기** 폴더가 콘솔 트리에 표시됩니다.
  기본적으로 이 옵션은 켜져 있습니다.

- **보조 중앙 관리 서버 표시**

  확인란을 선택하면 콘솔 트리에 관리 그룹 안에 있는 보조 및 가상 중앙 관리 서버의 노드가 표시됩니다. 보조 및 가상 중앙 관리 서버와 연결된 기능을 사용할 수 있습니다. 예를 들어, 보조 중앙 관리 서버의 애플리케이션 원격 설치를 위한 작업을 만들 수 있습니다.
  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **보안 설정 섹션 표시**

  이 확인란을 선택하면 **보안** 섹션이 중앙 관리 서버, 관리 그룹 및 기타 개체의 속성 창에 표시됩니다. 이 옵션을 사용하여 사용자 및 사용자 그룹에 개체 작업에 필요한 사용자 지정 권한을 제공할 수 있습니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

4. **확인**을 누릅니다.

변경 사항을 적용하려면 메인 애플리케이션 창을 닫고 이를 다시 열어야 합니다.

메인 애플리케이션 창에 있는 항목의 표시를 구성하려면:

1. 메인 애플리케이션 창의 메뉴 표시줄에서 **보기 → 구성**을 선택합니다.
2. 열리는 **보기 구성** 창에서 확인란을 사용하여 메인 창 요소의 표시를 구성합니다.
3. **확인**을 누릅니다.

네트워크에 연결된 기기 발견

이 섹션에서는 Kaspersky Security Center 설치 후에 수행해야 하는 단계를 설명합니다.

시나리오: 네트워크에 연결된 기기 발견

보안 제품을 설치하기 전에 기기 발견을 수행해야 합니다. 중앙 관리 서버는 검색된 기기에 대한 정보를 수신하고 정책을 통해 기기를 관리할 수 있도록 합니다. 네트워크에서 사용 가능한 기기 목록을 업데이트하려면 정기적인 네트워크 검색이 필요합니다.

네트워크 폴링을 시작하기 전에 SMB 프로토콜이 활성화되어 있는지 확인하십시오. 그렇지 않으면 Kaspersky Security Center가 폴링된 네트워크에서 기기를 검색할 수 없습니다. SMB 프로토콜을 활성화하려면 운영 체제에 대한 지침을 따르십시오.

네트워크 기기 발견은 다음 단계로 진행됩니다.

1. **기기 발견**

   빠른 시작 마법사는 초기 기기 발견 과정을 안내하며 컴퓨터, 태블릿 및 스마트폰과 같은 네트워크 기기를 찾는 데 도움이 됩니다. 기기 발견을 수동으로 수행할 수도 있습니다.

2. **예약된 검색 구성**

   주기적으로 사용하려는 검색 유형을 결정합니다. 원하는 유형을 활성화하고 검색 스케줄을 구성합니다. 네트워크 검색 빈도에 대한 권장 사항을 참조할 수 있습니다.

3. **발견된 기기를 관리 그룹에 추가하는 규칙 설정(선택 사항)**

   네트워크에 표시되는 새 기기는 정기 검색 중에 발견되어 **미할당 기기** 그룹에 자동으로 포함됩니다. 기기 이동 규칙을 설정하여 **관리 중인 기기** 그룹에 대한 기기 할당을 자동화할 수 있습니다. 보존 규칙을 구성할 수도 있습니다.

   3단계를 건너뛰면 새로 검색된 기기가 **미할당 기기** 그룹에 할당됩니다. 원하는 경우 이러한 기기를 수동으로 **관리 중인 기기** 그룹으로 이동할 수 있습니다. 기기를 수동으로 **관리 중인 기기** 그룹으로 이동하면, 각 기기 관련 정보를 분석하여 해당 기기를 관리 그룹으로 이동할지, 이동한다면 정확히 어느 그룹으로 이동할지 결정할 수 있습니다.

결과

시나리오를 완료하면 다음과 같은 결과를 얻을 수 있습니다:

- Kaspersky Security Center 중앙 관리 서버가 네트워크에 있는 기기를 발견하여 해당 기기와 관련된 정보를 제공합니다.
- 이후 검색이 설정되어 지정된 스케줄에 따라 수행됩니다.
- 새로 발견된 기기가 구성된 규칙에 따라 정렬됩니다. (규칙이 구성되어 있지 않으면 기기는 **미할당 기기** 그룹에 유지됩니다.)

미할당 기기

이 섹션에서는 회사 네트워크에서 관리 그룹에 포함되지 않은 기기를 관리하는 방법에 대해 설명합니다.

기기 발견

이 섹션에서는 Kaspersky Security Center에서 사용 가능한 기기 발견 유형에 대해 설명하고 각 유형 사용과 관련된 정보를 제공합니다.

중앙 관리 서버는 정기 검색을 통해 이 네트워크의 네트워크 및 기기 구조 관련 정보를 수신합니다. 정보는 중앙 관리 서버 데이터베이스에 기록됩니다. 중앙 관리 서버에서는 다음과 같은 유형의 검색을 사용할 수 있습니다:

- **Windows 네트워크 검색**. 중앙 관리 서버는 두 가지 종류의 Windows 네트워크 검색(빠른 검색과 전체 검색)을 수행할 수 있습니다. 빠른 검색 시 중앙 관리 서버는 모든 네트워크 도메인 및 작업 그룹에서 기기들의 NetBIOS 이름 목록 정보만 가져옵니다. 상세 검색 시에는 각 클라이언트 기기에서 운영 체제 이름, IP 주소, DNS 이름, NetBIOS 이름 정보 등 더 상세한 정보가 요청됩니다. 기본적으로는 빠른 검색과 전체 검색이 모두 활성화됩니다. 포트 UDP 137, UDP 138, TCP 139가 라우터에서 닫혀 있거나 방화벽에 의해 닫힌 경우 등에는 Windows 네트워크 검색에서 기기를 발견하지 못할 수 있습니다.
- **Active Directory 검색**. Active Directory 단위 구조와 Active Directory의 기기 DNS 이름에 대한 정보를 중앙 관리 서버가 가져옵니다. 기본적으로 이 검색 유형은 활성화됩니다. Active Directory를 사용하는 경우 Active Directory 검색을 사용하는 것이 좋습니다. 그렇지 않으면 중앙 관리 서버에서 기기를 발견하지 못합니다. Active Directory를 사용하는데 네트워크에 연결된 일부 기기가 구성원으로 목록에 표시되지 않는 경우에는 Active Directory 검색에서 해당 기기를 발견할 수 없습니다.
- **IP 범위 검색**. 중앙 관리 서버에서 ICMP 패킷 또는 NBNS 프로토콜을 사용하여 지정된 IP 범위를 검색하고 IP 범위 내 기기에 있는 전체 데이터 집합을 수집합니다. 기본적으로 이 검색 유형은 비활성화됩니다. Windows 네트워크 검색 및/또는 Active Directory 검색을 사용하는 경우에는 이 검색 유형을 사용하지 않는 것이 좋습니다.
- **Zeroconf 폴링** 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 IPv6 네트워크를 검색하는 배포 지점입니다. 기본적으로 이 검색 유형은 비활성화됩니다. 배포 지점에서 Linux를 실행하는 경우 제로 구성 검색을 사용할 수 있습니다.

기기 이동 규칙을 설정하고 활성화한 경우 새로 발견된 기기가 **관리 중인 기기** 그룹에 자동으로 포함됩니다. 이동 규칙을 활성화하지 않은 경우에는 새로 발견된 기기가 **미할당 기기** 그룹에 자동으로 포함됩니다.

각 유형에 대해 기기 발견 설정을 수정할 수 있습니다. 검색 스케줄을 수정하려는 경우나, 전체 도메인 포레스트를 검색할지 아니면 특정 도메인만 검색할지를 설정하려는 경우를 예로 들 수 있습니다.

네트워크 폴링을 시작하기 전에 SMB 프로토콜이 활성화되어 있는지 확인하십시오. 그렇지 않으면 Kaspersky Security Center가 폴링된 네트워크에서 기기를 검색할 수 없습니다. SMB 프로토콜을 활성화하려면 운영 체제에 대한 지침을 따르십시오.

Windows 네트워크 검색

Windows 네트워크 검색 정보

빠른 검색 시 중앙 관리 서버는 모든 네트워크 도메인 및 작업 그룹에서 기기들의 NetBIOS 이름 목록 정보만 가져옵니다. 전체 검색 시에는 각 클라이언트 기기로부터 다음 정보가 요청됩니다:

- 운영 체제 유형
- IP 주소
- DNS 이름
- NetBIOS 이름

빠른 검색과 전체 검색 시에는 다음 조건을 충족해야 합니다:

- 네트워크에서 포트 UDP 137/138, TCP 139, UDP 445, TCP 445를 사용할 수 있어야 합니다.
- SMB 프로토콜이 활성화되었습니다.
- Microsoft Computer Browser 서비스를 사용해야 하며, 중앙 관리 서버에서 기본 브라우저 컴퓨터가 활성화되어야 합니다.
- Microsoft Computer Browser 서비스를 사용해야 하며, 클라이언트 기기에서 기본 브라우저 컴퓨터가 활성화되어야 합니다.
  - 네트워크에 연결된 기기 수가 32대를 초과하지 않는 경우 기기 한 대 이상에서.
  - 네트워크에 연결된 32대 기기 각각에 대해 기기 한 대 이상에서.

빠른 검색을 한 번 이상 실행해야 전체 검색을 실행할 수 있습니다.

Windows 네트워크 검색에 대한 설정 보기 및 수정

Windows 네트워크 검색에 대한 설정을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 발견** 폴더, **도메인** 하위 폴더를 차례로 선택합니다.
   지금 검색 버튼을 눌러 **미할당 기기** 폴더에서 **기기 발견** 폴더로 이동할 수 있습니다.
   도메인 하위 폴더의 작업 영역에 기기 목록이 표시됩니다.
2. **지금 검색**을 누릅니다.

도메인 속성 창이 열립니다. 원하는 경우 Windows 네트워크 검색의 설정을 수정합니다:

- **Windows 네트워크 검색 활성화**

  이 옵션은 기본적으로 선택되어 있습니다. Active Directory 검색만 수행하면 충분하다고 생각되는 경우와 같이 Windows 네트워크 검색을 수행하지 않으려는 경우에는 이 옵션을 선택 취소할 수 있습니다.

- **빠른 검색 스케줄 설정**

  기본 기간은 15분입니다.

  빠른 검색 시 중앙 관리 서버는 모든 네트워크 도메인 및 작업 그룹에서 기기들의 NetBIOS 이름 목록 정보만 가져옵니다.

  이전 데이터는 다음 검색에서 수신된 데이터로 완전히 교체됩니다.

  다음과 같은 검색 스케줄 옵션을 사용할 수 있습니다:

  - **N일마다**

    검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.

    기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **N분마다**

    검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.

    기본적으로 검색은 현재 시스템 시간부터 5분마다 실행됩니다.

  - **요일별**

    검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

    기본적으로 검색은 매주 금요일 오후 6:00:00에 실행됩니다.

  - **매달 선택한 주간의 지정한 날짜**

    검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

    기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

  - **누락된 작업 실행**

    중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.

    이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.

    이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.

    기본적으로 이 옵션은 켜져 있습니다.

- **상세 검색 스케줄 설정**

  기본 기간은 1시간입니다. 이전 데이터는 다음 검색에서 수신된 데이터로 완전히 교체됩니다.

다음과 같은 검색 스케줄 옵션을 사용할 수 있습니다:

- **N일마다**

  검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.
  기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **N분마다**

  검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.
  기본적으로 검색은 현재 시스템 시간부터 5분마다 실행됩니다.

- **요일별**

  검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 검색은 매주 금요일 오후 6:00:00에 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

- **누락된 작업 실행**

  중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.
  이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.
  이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.
  기본적으로 이 옵션은 켜져 있습니다.

검색을 즉시 수행하려면 **지금 검색**를 누릅니다. 두 유형의 검색이 모두 시작됩니다.

가상 중앙 관리 서버에서는 배포 지점 속성 창의 **기기 발견** 섹션에서 Windows 네트워크의 검색 설정을 보고 편집할 수 있습니다.

Active Directory 검색

Active Directory를 사용하는 경우 Active Directory 검색을 사용하고, 그렇지 않은 경우에는 다른 검색 유형을 사용하는 것이 좋습니다. Active Directory를 사용하는데 네트워크에 연결된 일부 기기가 구성원으로 목록에 표시되지 않는 경우에는 Active Directory 검색에서 해당 기기를 발견할 수 없습니다.

Active Directory 검색 결과는 이후 검색 결과와 관계없이 30일 동안 중앙 관리 서버에 저장됩니다.

네트워크 폴링을 시작하기 전에 SMB 프로토콜이 활성화되어 있는지 확인하십시오. 그렇지 않으면 Kaspersky Security Center가 폴링된 네트워크에서 기기를 검색할 수 없습니다. SMB 프로토콜을 활성화하려면 운영 체제에 대한 지침을 따르십시오.

Active Directory 검색에 대한 설정 보기 및 수정

Active Directory 그룹의 검색 설정을 수정하고 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 발견** 폴더, **Active Directory** 하위 폴더를 차례로 선택합니다.
   또는 **지금 검색** 버튼을 눌러 **미할당 기기** 폴더에서 **기기 발견** 폴더로 이동할 수 있습니다.

2. **검색 구성**을 누릅니다.
   Active Directory 속성 창이 열립니다. 원하는 경우 Active Directory 그룹 검색의 설정을 수정합니다:

   - **Active Directory 검색 사용**

     이 옵션은 기본적으로 선택되어 있습니다. 그러나 Active Directory를 사용하지 않는 경우에는 검색에서 결과가 반환되지 않습니다. 이 경우에는 옵션 선택을 취소할 수 있습니다.

   - **검색 스케줄 설정**

     기본 기간은 1시간입니다.
     다음과 같은 검색 스케줄 옵션을 사용할 수 있습니다:

     - **N일마다**

       검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.
       기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

     - **N분마다**

       검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.
       기본적으로 검색은 현재 시스템 시간부터 5분마다 실행됩니다.

     - **요일별**

       검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
       기본적으로 검색은 매주 금요일 오후 6:00:00에 실행됩니다.

     - **매달 선택한 주간의 지정한 날짜**

       검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
       기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

- **누락된 작업 실행**

  중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.

  이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.

  이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **고급**

  검색할 Active Directory 도메인을 선택할 수 있습니다:

  - Kaspersky Security Center가 속한 Active Directory 도메인.
  - Kaspersky Security Center가 속한 도메인 포레스트.
  - Active Directory 도메인의 지정된 목록.

    이 옵션을 선택하면 검색 범위에 도메인을 추가할 수 있습니다:

    - **추가** 버튼을 누릅니다.
    - 해당하는 필드에서 도메인 컨트롤러의 주소와 해당 주소에 액세스하는 데 사용할 계정의 이름 및 암호를 지정합니다.
    - **확인**을 눌러 변경사항을 저장합니다.

    목록에서 도메인 컨트롤러 주소를 선택한 다음 **수정** 또는 **제거** 버튼을 눌러 주소를 수정하거나 제거할 수 있습니다.

  - **확인**을 눌러 변경사항을 저장합니다.

검색을 즉시 수행하려면 **지금 검색** 버튼을 누릅니다.

가상 중앙 관리 서버에서는 배포 지점 속성 창의 **기기 발견** 섹션에서 Active Directory 그룹의 검색 설정을 보고 편집할 수 있습니다.

IP 범위 검색

중앙 관리 서버에서 ICMP 패킷 또는 NBNS 프로토콜을 사용하여 지정된 IP 범위를 검색하고 IP 범위 내 기기에 있는 전체 데이터 집합을 수집합니다. 기본적으로 이 검색 유형은 비활성화됩니다.

Microsoft Active Directory 또는 Samba 도메인 컨트롤러 내의 모든 Linux 기반 호스트에 대해 `/etc/samba/smb.conf` 파일에서 `netbios name`과 `workgroup` 매개변수를 지정합니다. 그렇지 않으면 검색 결과에 중복 호스트가 포함될 수 있습니다.

네트워크 폴링을 시작하기 전에 SMB 프로토콜이 활성화되어 있는지 확인하십시오. 그렇지 않으면 Kaspersky Security Center가 폴링된 네트워크에서 기기를 검색할 수 없습니다. SMB 프로토콜을 활성화하려면 운영 체제에 대한 지침을 따르십시오.

IP 범위 검색에 대한 설정 보기 및 수정

IP 범위 그룹에 대한 검색 설정을 수정하고 보려면 다음과 같이 하십시오:

1. 콘솔 트리의 **기기 발견** 폴더에서 **IP 범위** 하위 폴더를 선택합니다.
   지금 검색를 눌러 **미할당 기기** 폴더에서 **기기 발견** 폴더로 이동할 수 있습니다.
2. 원하는 경우 **IP 범위** 하위 폴더에서 **서브넷 추가**을 눌러 검색할 IP 범위를 추가한 다음 **확인**을 누릅니다.
3. **검색 구성**을 누릅니다.
   IP 범위 속성 창이 열립니다. 원하는 경우 IP 범위 검색의 설정을 수정할 수 있습니다:

- **IP 범위 검색 사용**

  이 옵션은 기본적으로 선택되어 있지 않습니다. Windows 네트워크 검색 및/또는 Active Directory 검색을 사용하는 경우에는 이 검색 유형을 사용하지 않는 것이 좋습니다.

- **검색 스케줄 설정**

  기본 기간은 420분입니다. 이전 데이터는 다음 검색에서 수신된 데이터로 완전히 교체됩니다.
  다음과 같은 검색 스케줄 옵션을 사용할 수 있습니다:

  - **N일마다**

    검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.
    기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **N분마다**

    검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.
    기본적으로 검색은 현재 시스템 시간부터 5분마다 실행됩니다.

  - **요일별**

    검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
    기본적으로 검색은 매주 금요일 오후 6:00:00에 실행됩니다.

  - **매달 선택한 주간의 지정한 날짜**

    검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
    기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

  - **누락된 작업 실행**

    중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.
    이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.
    이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.

기본적으로 이 옵션은 켜져 있습니다.

검색을 즉시 수행하려면 **지금 검색**를 누릅니다. 이 버튼은 **IP 범위 검색 사용**을 선택한 경우에만 사용할 수 있습니다.

가상 중앙 관리 서버에서는 배포 지점 속성 창의 **기기 발견** 섹션에서 IP 범위 검색 설정을 보고 편집할 수 있습니다. IP 범위 검색 도중 탐지된 클라이언트 기기는 가상 중앙 관리 서버의 **도메인** 폴더에 표시됩니다.

Zeroconf 폴링

이 검색 유형은 Linux 기반 배포 지점에 대해서만 지원됩니다.

배포 지점에서 IPv6 주소를 사용하는 기기가 있는 네트워크를 검색할 수 있습니다. 이 경우 IP 범위를 지정하지 않고 배포 지점에서 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 전체 네트워크를 검색합니다. 제로 구성을 시작하려면 배포 지점에 avahi-browse 유틸리티를 설치해야 합니다.

제로 구성 검색을 활성화하려면 다음을 수행하십시오.

1. 콘솔 트리의 **기기 발견** 폴더에서 **IP 범위** 하위 폴더를 선택합니다.
   지금 검색를 눌러 **미할당 기기** 폴더에서 **기기 발견** 폴더로 이동할 수 있습니다.
2. **검색 구성**을 누릅니다.
3. IP 범위 속성 창이 열리면 **Zeroconf 기술로 검색 활성화**를 선택합니다.

그러면 배포 지점에서 네트워크를 검색하기 시작합니다. 이 경우 지정된 IP 범위가 무시됩니다.

Windows 도메인 작업. 도메인 설정 보기 및 변경

도메인 설정을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 발견** 폴더, **도메인** 하위 폴더를 차례로 선택합니다.
2. 다음 방법 중 하나로 도메인을 선택하고 해당 속성 창을 엽니다:
   - 도메인의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - **그룹 속성 표시** 링크를 누릅니다.

속성: <도메인 이름> 창이 열리고 이 창에서 선택한 도메인을 구성할 수 있습니다.

미할당 기기에 대한 보존 규칙 구성

Windows 네트워크 검색이 완료되면 발견된 기기가 미할당 기기 관리 그룹의 하위 그룹에 배치됩니다. 이 관리 그룹은 **고급 → 기기 발견 → 도메인**에 있습니다. **도메인** 폴더가 부모 그룹입니다. 이 폴더에는 네트워크 검색 중에 발견된 해당 도메인과 워크 그룹의 이름이 지정된 자식 그룹이 포함됩니다. 모바일 기기의 관리 그룹도 부모 그룹에 포함될 수 있습니다. 부모 그룹과 각 자식 그룹에 대해 미할당 기기의 보존 규칙을 구성할 수 있습니다. 보존 규칙은 네트워크 검색 설정에 따라 달라지지 않으며 네트워크 검색을 비활성화해도 작동합니다.

미할당 기기에 대한 보존 규칙을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **기기 발견** 폴더에서 다음 중 하나를 수행합니다:

   - 부모 그룹의 설정을 구성하려면 **도메인** 하위 폴더를 마우스 오른쪽 버튼으로 누르고 **속성**을 선택합니다.
     부모 그룹 속성 창이 열립니다.
   - 자식 그룹의 설정을 구성하려면 그룹 이름을 마우스 오른쪽 버튼으로 누르고 **속성**을 선택합니다.
     하위 그룹 속성 창이 열립니다.

2. **기기** 섹션에서 다음 설정을 지정합니다:

   - **기기가 다음 비활성 기간을 초과하면 그룹에서 기기 제거(일)**

     이 옵션을 활성화하면 기기가 그룹에서 자동으로 제거될 때까지의 시간 간격을 지정할 수 있습니다. 기본적으로 이 옵션은 자식 그룹에도 배포됩니다. 기본 기간은 7일입니다.

     기본적으로 이 옵션은 켜져 있습니다.

   - **부모 그룹에서 상속**

     이 옵션을 활성화하면 현재 그룹에 있는 기기의 보존 기간이 부모 그룹에서 상속되며 변경할 수 없습니다.

     이 옵션은 자식 그룹에만 사용할 수 있습니다.

     기본적으로 이 옵션은 켜져 있습니다.

   - **자식 그룹에 강제 상속**

     이 설정 값은 자식 그룹에 배포되지만 자식 그룹의 속성에서는 이러한 설정이 잠깁니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

변경 내용이 저장 및 적용됩니다.

IP 범위 작업

기존 IP 범위를 사용자 지정하고 새 IP 범위를 만들 수 있습니다.

IP 범위 만들기

IP 범위를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리의 **기기 발견** 폴더에서 **IP 범위** 하위 폴더를 선택합니다.
2. 폴더의 마우스 오른쪽 메뉴에서 **새로 만들기 → IP 범위**를 선택합니다.
3. **새 IP 범위** 창이 열리면 새 IP 범위를 설정합니다.

새 IP 범위가 **IP 범위** 폴더에 표시됩니다.

IP 범위 설정 보기 및 변경

IP 범위 설정을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **기기 발견** 폴더에서 **IP 범위** 하위 폴더를 선택합니다.
2. IP 범위를 선택하고 다음 방법 중 하나로 속성 창을 엽니다:
   - IP 범위의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - **그룹 속성 표시** 링크를 누릅니다.

속성: <IP 범위 이름> 창이 열리고 이 창에서 선택한 IP 범위의 속성을 구성할 수 있습니다.

Active Directory 그룹 작업. 그룹 설정 보기 및 수정

Active Directory 그룹의 설정을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 발견** 폴더, **Active Directory** 하위 폴더를 차례로 선택합니다.
2. Active Directory 그룹을 선택하고 다음 방법 중 하나로 속성 창을 엽니다:
   - IP 범위의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - **그룹 속성 표시** 링크를 누릅니다.

속성: <Active Directory 그룹 이름> 창이 열리고 이 창에서 선택한 Active Directory 그룹을 구성할 수 있습니다.

자동으로 기기를 관리 그룹으로 이동하는 규칙 만들기

회사 네트워크 검색에서 기기가 발견되는 즉시 자동으로 관리 그룹으로 이동하도록 구성할 수 있습니다.

자동으로 기기를 관리 그룹으로 이동하는 규칙을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **미할당 기기** 폴더를 선택합니다.
2. 이 폴더의 작업 영역에서 **규칙 구성**를 누릅니다.

   그러면 **속성: 미할당 기기** 창이 열립니다. **기기 이동** 섹션에서 자동으로 기기를 관리 그룹으로 이동하는 규칙을 구성합니다.

목록에서 첫 번째 적용 가능한 규칙(목록 위에서 아래로)이 기기에 적용됩니다.

클라이언트 기기에서 VDI 동적 모드 사용

가상 인프라는 임시 가상 컴퓨터를 사용해 기업 네트워크에 배포될 수 있습니다. Kaspersky Security Center는 임시 가상 컴퓨터를 탐지하고 중앙 관리 서버에 임시 가상 컴퓨터 정보를 추가합니다. 사용자가 임시 가상 컴퓨터 사용을 마친 후에 해당 컴퓨터는 가상 인프라에서 제거됩니다. 그러나 제거된 가상 컴퓨터에 대한 기록은 중앙 관리 서버 데이터베이스에 저장될 수 있습니다. 또한 존재하지 않는 가상 컴퓨터가 관리 콘솔에 표시될 수 있습니다.

존재하지 않는 가상 컴퓨터에 대한 정보가 저장되는 것을 막기 위해 Kaspersky Security Center는 VDI(가상 데스크톱 인프라)용 동적 모드를 지원합니다. 관리자는 임시 가상 컴퓨터에 설치할 네트워크 에이전트 설치 패키지의 속성에서 VDI용 동적 모드 지원을 사용할 수 있습니다.

임시 가상 컴퓨터 사용이 중지되면 네트워크 에이전트는 중앙 관리 서버에게 컴퓨터 사용이 중지되었다고 알립니다. 가상 컴퓨터가 성공적으로 중지되면 중앙 관리 서버에 연결된 기기 목록에서 제거됩니다. 가상 컴퓨터가 오류로 중지되고 네트워크 에이전트가 중지된 가상 컴퓨터에 대한 알림을 중앙 관리 서버에 보내지 않으면 백업 시나리오가 사용됩니다. 이 시나리오에서는 가상 컴퓨터가 중앙 관리 서버와 세 번 동기화 시도를 실패하면 중앙 관리 서버에 연결된 기기 목록에서 제거됩니다.

네트워크 에이전트 설치 패키지의 속성에서 VDI 동적 모드 사용

VDI 동적 모드를 사용하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
2. 네트워크 에이전트 설치 패키지의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   속성: Kaspersky Security Center 네트워크 에이전트 창이 열립니다.
3. **속성: Kaspersky Security Center 네트워크 에이전트 창**에서 **고급** 섹션을 선택합니다.
4. **고급** 섹션에서 **VDI에 대해 동적 모드 사용** 옵션을 선택합니다.

   네트워크 에이전트가 설치될 기기는 가상 VDI에 포함됩니다.

VDI를 구성하는 기기 검색

VDI를 구성하는 미할당 기기를 검색하려면 다음과 같이 하십시오.

1. **미할당 기기** 폴더의 마우스 오른쪽 메뉴에서 **검색**를 선택합니다.
   가상 데스크톱 인프라에 포함된 모든 기기의 목록을 보려면 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴에서 **검색**을 선택합니다.
2. **검색** 창의 **가상 컴퓨터** 탭에 있는 **가상 데스크톱 인프라 소속** 설정 그룹에서 **예**를 선택합니다.
3. **지금 찾기** 버튼을 누릅니다.

가상 데스크톱 인프라에 속하는 미할당 기기 목록이 표시됩니다.

VDI를 구성하는 기기를 관리 그룹으로 이동

VDI를 구성하는 기기를 관리 그룹으로 이동하려면 다음과 같이 하십시오:

1. **미할당 기기** 폴더의 작업 영역에서 **규칙 구성**를 누릅니다.
   그러면 **미할당 기기** 폴더의 속성 창이 열립니다.
2. **미할당 기기** 폴더의 속성 창에 있는 **기기 이동** 섹션에서 **추가** 버튼을 누릅니다.
   새 규칙 창이 열립니다.
3. **새 규칙** 창에서 **가상 컴퓨터** 섹션을 선택합니다.
4. **이것은 가상 컴퓨터입니다** 드롭다운 목록에서 **예**를 선택합니다.

기기를 관리 그룹으로 이동하는 규칙이 만들어집니다.

장비 재고

장비 재고를 관리하는 데 사용하는 하드웨어 목록(**저장소 → 하드웨어**)은 자동 및 수동의 두 가지 방식으로 채워집니다. 네트워크 폴링 후마다 감지된 모든 기기가 목록에 자동으로 추가되지만, 네트워크를 폴링하지 않으려는 경우에는 기기를 수동으로 추가할 수도 있습니다. 예를 들어 라우터, 프린터 또는 기기 하드웨어와 같은 다른 기기를 목록에 수동으로 추가할 수 있습니다.

기기의 속성에서 기기에 대한 자세한 정보를 보고 편집할 수 있습니다.

하드웨어 목록에는 다음 유형의 기기가 포함될 수 있습니다.

- 컴퓨터
- 모바일 기기
- 네트워크 기기
- 가상 기기

- OEM 구성 요소
- 컴퓨터 주변 기기
- 연결된 기기
- VoIP 폰
- 네트워크 저장소

관리자는 *기업 장비* 속성을 탐지된 기기에 할당할 수 있습니다. 이 특성은 기기의 속성에서 수동으로 할당되거나 관리자가 자동으로 할당할 특성의 기준을 지정할 수 있습니다. 이 경우 *기업 장비* 속성은 기기 유형별로 할당됩니다.

Kaspersky Security Center는 장비를 목록에서 제외할 수 있습니다. 이렇게 하려면 기기 속성에서 **제거된 기기** 옵션을 선택합니다. 기기는 장비 목록에 표시되지 않습니다.

관리자는 **하드웨어** 폴더에서 프로그램 가능 논리 컨트롤러(PLC)의 목록을 관리할 수 있습니다. PLC 목록 관리에 대한 자세한 내용은 *Kaspersky Industrial CyberSecurity for Nodes 사용자 설명서*에 나와 있습니다.

새 기기에 대한 정보 추가

네트워크의 새 기기에 대한 정보를 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **저장소** 폴더에서 **하드웨어** 하위 폴더를 선택합니다.
2. **하드웨어** 폴더의 작업 영역에서 **기기 추가** 버튼을 눌러 **새로운 기기** 창을 엽니다.
   새로운 기기 창이 열립니다.
3. **새로운 기기** 창의 **유형** 드롭다운 목록에서 추가하려는 기기 유형을 선택합니다.
4. **확인**를 누릅니다.
   기기 속성 창이 **일반** 섹션에 열립니다.
5. **일반** 섹션의 입력 필드에 기기의 데이터를 입력합니다. **일반** 섹션에는 다음과 같은 설정이 나와 있습니다:
   - **기업 기기**. 기기에 *기업* 속성을 지정하려면 이 확인란을 선택합니다. 이 특성을 사용하여 **하드웨어** 폴더에서 기기를 검색할 수 있습니다.
   - **제거된 기기**. **하드웨어** 폴더에서 기기의 목록에 기기를 표시하지 않으려면 이 확인란을 선택합니다.
6. **적용**을 누릅니다.

새 기기가 **하드웨어** 폴더의 작업 영역에 표시됩니다.

기업 기기를 정의하는 데 사용한 기준 구성

기업 기기의 탐지 기준을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **저장소** 폴더에서 **하드웨어** 하위 폴더를 선택합니다.
2. **하드웨어** 폴더 작업 공간에서 **추가 조치**버튼을 누르고 드롭다운 목록에서 **기업 기기에 대한 규칙 설정**.
   하드웨어 속성 창이 열립니다.
3. 하드웨어 속성 창의 **기업 기기** 섹션에서 *기업* 특성을 기기에 할당하는 방법을 선택합니다:
   - **수동으로 기업 기기 속성 설정**. *기업 하드웨어* 특성은 기기 속성 창의 **일반** 섹션에서 수동으로 기기에 할당합니다.
   - **자동으로 기업 기기 속성 설정**. **기기 유형별** 설정 블록에서 애플리케이션이 *기업* 특성을 자동으로 할당할 기기 유형을 지정합니다.

     이 옵션은 네트워크 폴링을 통해 추가된 기기에만 영향을 줍니다. 수동으로 추가한 기기의 경우 *기업* 특성을 수동으로 설정합니다.
4. **확인**을 누릅니다.

기업 기기에 대한 탐지 기준이 구성됩니다.

사용자 지정 필드 구성

기기의 사용자 지정 필드를 구성하려면 다음과 같이 진행합니다:

1. 콘솔 트리의 **저장소** 폴더에서 **하드웨어** 하위 폴더를 선택합니다.
2. **하드웨어** 폴더의 작업 영역에서 **추가 조치** 버튼을 누르고 드롭다운 목록에서 **사용자 지정 데이터 필드 구성**를 선택합니다.
   하드웨어 속성 창이 열립니다.
3. 하드웨어 속성 창에서 **사용자 지정 필드** 섹션을 선택하고 **추가** 버튼을 누릅니다.
   필드 추가 창이 열립니다.
4. **필드 추가** 창에서 하드웨어 속성에 표시되는 사용자 지정 필드의 이름을 지정합니다.
   고유한 이름으로 여러 사용자 지정 필드를 만들 수 있습니다.
5. **확인**을 누릅니다.

추가된 사용자 지정 필드는 하드웨어 속성의 **사용자 지정 필드** 섹션에 표시됩니다. 사용자 지정 필드를 사용하여 기기에 대한 특정 정보를 제공할 수 있습니다. 예를 들어, 하드웨어 구매에 대한 내부 주문 번호 등일 수 있습니다.

라이센스

이 섹션에는 Kaspersky Security Center 15.1 라이센싱과 관련된 일반 개념 정보가 나와 있습니다.

라이센스 제한 초과 이벤트

Kaspersky Security Center에서는 클라이언트 기기에 설치된 Kaspersky 애플리케이션에서 초과한 라이센스 제한 이벤트 정보를 볼 수 있습니다.

라이센스 제한이 초과되면 다음 규칙에 따라 이벤트 중요도를 정의합니다.

- 단일 라이센스하에 현재 사용 중인 유닛 수가 해당 라이센스로 적용 가능한 총 유닛 수의 90~100%에 도달하면 심각도가 **정보**인 이벤트가 게시됩니다.
- 단일 라이센스하에 현재 사용 중인 유닛 수가 해당 라이센스로 적용 가능한 총 유닛 수의 100~110%에 도달하면 심각도가 **경고**인 이벤트가 게시됩니다.
- 단일 라이센스하에 현재 사용 중인 유닛 수가 해당 라이센스로 적용 가능한 총 유닛 수의 110%를 초과하면 심각도가 **심각 이벤트**인 이벤트가 게시됩니다.

라이센스 정보

이 섹션에는 Kaspersky Security Center를 통해 관리되는 Kaspersky 애플리케이션의 라이센스에 대한 정보가 포함되어 있습니다.

라이센스 정보

*라이센스*는 서명한 라이센스 계약서(최종 사용자 라이센스 계약서)의 약관에 따라 정해진 기간에 Kaspersky Security Center를 사용할 수 있는 권한을 말합니다.

서비스 범위 및 유효 기간은 애플리케이션을 사용하는 라이센스 형태에 따라 달라집니다.

다음과 같은 라이센스 유형이 제공됩니다:

- *체험판*

  애플리케이션 체험을 위한 무료 라이센스입니다. 체험판 라이센스는 보통 사용 기간이 짧습니다.

  체험판 라이센스가 만료되면 모든 Kaspersky Security Center 기능이 중지됩니다. 애플리케이션을 계속 사용하려면 상업용 라이센스를 구매해야 합니다.

  평가판 라이센스로 애플리케이션을 사용할 수 있는 기간은 한 번뿐입니다.

- *상업용*

  유료 라이센스입니다.

상업용 라이센스가 만료되면 애플리케이션의 주요 기능이 비활성화됩니다. Kaspersky Security Center를 계속 사용하려면 상업용 라이센스를 갱신해야 합니다. 상업용 라이센스가 만료된 후에는 해당 애플리케이션을 계속 사용할 수 없으며 기기에서 해당 애플리케이션을 제거해야 합니다.

모든 위협에 대한 끊임없는 보호를 위해, 라이센스가 만료되기 전에 갱신할 것을 권장합니다.

최종 사용자 라이센스 계약서 정보

최종 사용자 라이센스 계약서(라이센스 계약서 또는 EULA)는 애플리케이션 사용 약관을 규정하고 있는 사용자와 AO Kaspersky Lab 간의 계약서입니다.

애플리케이션 사용을 시작하기 전에 라이센스 계약서를 자세히 확인하십시오.

Kaspersky Security Center 및 구성 요소(예: 네트워크 에이전트)마다 EULA가 존재합니다.

다음과 같은 때 Kaspersky Security Center의 최종 사용자 라이센스 계약서를 볼 수 있습니다.

- Kaspersky Security Center 설치 중.
- Kaspersky Security Center 배포 키트에 포함된 license.txt 문서 확인.
- Kaspersky Security Center 설치 폴더의 license.txt 문서 확인.
- Kaspersky 웹사이트에서 license.txt 파일 다운로드.

다음 방법을 통해 Windows용 네트워크 에이전트, Mac용 네트워크 에이전트, Linux용 네트워크 에이전트의 최종 사용자 라이센스 계약서를 볼 수 있습니다.

- Kaspersky 웹 서버에서 네트워크 에이전트 배포 패키지 다운로드 중.
- Windows용 네트워크 에이전트, Mac용 네트워크 에이전트, Linux용 네트워크 에이전트 설치 중.
- Windows용 네트워크 에이전트, Mac용 네트워크 에이전트, Linux용 네트워크 에이전트 배포 패키지에 포함되어 있는 license.txt 문서 확인.
- Windows용 네트워크 에이전트, Mac용 네트워크 에이전트, Linux용 네트워크 에이전트 설치 폴더에 포함되어 있는 license.txt 문서 확인.
- Kaspersky 웹사이트에서 license.txt 파일 다운로드.

애플리케이션을 설치할 때 최종 사용자 라이센스 계약서에 동의하면 최종 사용자 라이센스 계약서에 동의하는 것입니다. 라이센스 계약서의 조건을 수락하지 않을 경우 애플리케이션 설치를 취소하거나 애플리케이션 사용을 포기해야 합니다.

라이센스 인증서 정보

*라이센스 인증서*는 키 파일 또는 활성화 코드와 함께 받은 문서입니다.

라이센스 인증서에는 제공된 라이센스에 대한 아래와 같은 정보가 담겨 있습니다:

- 라이센스 ID 또는 주문 번호
- 라이센스가 부여된 사용자에 대한 정보
- 제공된 라이센스로 인증할 수 있는 애플리케이션에 대한 정보
- 라이센스 구매 수량 (예, 애플리케이션에 제공된 라이센스로 사용할 수 있는 기기 수)
- 라이센스 유효 기간 시작 날짜
- 라이센스 만료 날짜 또는 라이센스 기간
- 라이센스 유형

라이센스 키 정보

*라이센스 키*는 최종 사용자 라이센스 계약서의 약관에 따라 애플리케이션을 활성화한 다음 사용하기 위해 적용할 수 있는 비트 시퀀스입니다. Kaspersky 전문가가 라이센스 키를 생성합니다.

다음 방법 중 하나를 사용해 애플리케이션에 라이센스 키를 추가할 수 있습니다: *키 파일* 적용 또는 *활성화코드* 입력. 애플리케이션에 추가한 라이센스 키는 고유한 영숫자 문자열로 애플리케이션 인터페이스에 표시됩니다.

라이센스 계약서의 약관을 위반한 경우에는 Kaspersky에서 라이센스 키를 차단할 수 있습니다. 라이센스 키가 차단된 경우 애플리케이션을 사용하려면 다른 라이센스 키를 추가해야 합니다.

라이센스 키는 활성 라이센스 키 또는 추가(또는 예약) 라이센스 키일 수 있습니다.

*활성 라이센스 키*는 현재 애플리케이션에서 사용 중인 라이센스 키입니다. 체험판 라이센스나 상업용 라이센스용으로 활성 라이센스 키를 추가할 수 있습니다. 애플리케이션은 하나 이상의 활성 라이센스 키를 보유할 수 없습니다.

*추가(또는 예약) 라이센스 키*는 사용자에게 애플리케이션을 사용하기 위한 라이센스 키를 부여하지만 현재 사용하지는 않습니다. 현재 활성 라이센스 키와 연결된 라이센스가 만료되면 추가 라이센스 키가 자동으로 활성화됩니다. 활성 라이센스 키를 이미 추가한 경우에만 추가 라이센스 키를 추가할 수 있습니다.

체험판용 라이센스 키는 활성 라이센스 키로만 추가할 수 있습니다. 체험판용 라이센스 키는 추가 라이센스 키로 추가할 수 없습니다.

라이센스 키 파일 정보

*키 파일*은 Kaspersky에서 사용자에게 제공한 .key 확장자를 가진 파일입니다. 키 파일은 라이센스 키를 추가하여 애플리케이션을 활성화하는 데 사용됩니다.

Kaspersky Security Center를 구매하거나 Kaspersky Security Center 체험판을 요청하면 사용자가 제공한 이메일 주소로 키 파일이 수신됩니다.

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.

사용자의 키 파일을 복원하려면, 다음 순서 조치를 취해야 합니다:

- 라이센스 구매처로 문의.
- 이용 가능한 활성화 코드를 사용해 Kaspersky 웹사이트에서 키 파일을 받습니다.
- 다른 중앙 관리 서버에서 라이센스 키 파일을 내보냅니다.

서브스크립션 정보

*Kaspersky Security Center로의 서브스크립션*은 선택한 설정 하에서 애플리케이션을 사용하기 위한 주문입니다 (서브스크립션 만료 날짜, 보호되는 기기 개수). 서비스 공급 업체(예, 인터넷 공급 업체)를 통해 Kaspersky Security Center에 사용자의 서브스크립션을 등록할 수 있습니다. 수동 또는 자동 모드로 서브스크립션을 갱신할 수 있습니다; 또한, 이를 취소할 수 있습니다.

서브스크립션은 기간을 제한하거나(예, 1년) 또는 무기한(만료 날짜 없음)으로 정할 수 있습니다. 제한한 서브스크립션 만료 이후에도 Kaspersky Security Center를 계속 사용하려면 반드시 갱신해야 합니다. 만일 만기일 안에 서비스 공급 업체에게 선불이 완료되면 무기한 서브스크립션이 자동으로 갱신됩니다.

기간을 제한한 서브스크립션이 만료되면, 갱신을 위해 애플리케이션의 정상적인 작동을 허용케 하는 유예 기간이 주어질 수 있습니다. 유예 기간의 부여 여부와 그 기간은 서비스 공급 업체에 의해 정의됩니다.

서브스크립션으로 Kaspersky Security Center를 사용하려면 서비스 공급업체로부터 받은 활성화코드를 적용해야 합니다.

서브스크립션 만료 또는 서브스크립션 취소 시에만 Kaspersky Security Center에 다른 활성화코드를 적용시킬 수 있습니다.

서비스 공급 업체에 따라 서브스크립션 관리를 위한 조치들이 달라질 수 있습니다. 서비스 공급 업체는 서브스크립션 갱신을 위한 유예기간을 제공하지 않을 수 있으며, 기간 만료 후 애플리케이션의 기능은 작동하지 않습니다.

서브스크립션으로 구매한 활성화코드는 Kaspersky Security Center의 이전 버전을 활성화할 수 없습니다.

서브스크립션으로 애플리케이션을 사용 때, Kaspersky Security Center는 서브스크립션이 만료될 때까지 지정된 시간 간격 동안 자동으로 활성화 서버에 접속을 시도합니다. 이렇게 하면 서브스크립션 정보가 활성화 서버와 동기화됩니다. 시스템 DNS를 사용하여 서버에 접근할 수 없을 시, 애플리케이션이 공용 DNS 서버를 사용합니다. 서브스크립션은 서비스 공급 업체의 홈페이지에서 갱신할 수 있습니다.

Kaspersky Security Center가 활성화 서버에 접근할 때까지 기다리지 않고 서브스크립션 정보를 수동으로 업데이트할 수 있습니다. 이는 서브스크립션 설정 변경 등에 유용할 수 있습니다.

서브스크립션 정보를 수동으로 업데이트하려면:

1. 콘솔 트리에서 **Kaspersky 라이센스** 폴더를 선택합니다.
2. **추가 작업**을 클릭하고 드롭다운 목록에서 **라이센스 서버와 서브스크립션 설정 동기화**를 선택합니다.

   서브스크립션 정보가 활성화 서버에서 업데이트됩니다.

활성화코드 정보

*활성화코드*는 20자의 숫자와 문자로 이루진 고유한 값입니다. Kaspersky Security Center를 활성화하는 라이센스 키를 추가하기 위해 활성화코드를 입력합니다. Kaspersky Security Center 구매 후 또는 Kaspersky Security Center 체험판 주문 후 사용자가 지정한 이메일 주소로 온 활성화코드를 가져옵니다.

활성화 코드로 애플리케이션을 활성화하려면 Kaspersky 활성화 서버 연결을 위한 인터넷 액세스가 필요합니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다.

애플리케이션이 활성화코드를 사용해 활성화되었다면, 경우에 따라 해당 라이센스 키의 현재 상태를 확인하기 위해 애플리케이션이 Kaspersky 활성화 서버에 정기적으로 요청을 보냅니다. 요청을 보낼 수 있도록 인터넷 접속이 가능해야 합니다.

애플리케이션을 설치한 후 활성화 코드를 분실한 경우 라이선스를 구입한 Kaspersky 파트너에게 문의하십시오.

관리 애플리케이션 활성화에 키 파일을 사용할 수 없습니다.활성화 코드만 허용됩니다.

최종 사용자 라이센스 계약서 동의 취소

클라이언트 기기 보호를 중지하기로 결정한 경우 관리 중인 Kaspersky 애플리케이션을 제거하고 이 애플리케이션의 EULA(최종 사용자 라이센스 계약서)를 취소할 수 있습니다.

관리 중인 Kaspersky 애플리케이션의 EULA를 취소하려면 다음 절차를 따르십시오.

1. 콘솔 트리에서 **중앙 관리 서버** → **고급** → **동의한 EULA**를 선택합니다.

   설치 패키지 생성 시, seamless 업데이트 설치 시, 또는 Kaspersky Security for Mobile 배포 시 동의한 EULA 목록이 표시됩니다.

2. 목록에서 동의를 취소할 EULA를 선택합니다.

   EULA에 관하여 다음 속성을 볼 수 있습니다.

   - EULA에 동의한 날짜.
   - EULA에 동의한 사용자 이름.
   - EULA 약관 링크.
   - EULA에 연결된 개체 목록: 설치 패키지 이름, seamless 업데이트 이름, 모바일 앱 이름.

3. **EULA 취소** 버튼을 클릭합니다.

   열린 창에서 해당 EULA와 연관된 Kaspersky 애플리케이션을 제거해야 한다는 메시지가 표시됩니다.

4. 버튼을 눌러 취소를 확인하십시오.

   Kaspersky Security Center에서 설치 패키지(EULA를 취소하려는 관리 중인 Kaspersky 애플리케이션의 설치 패키지)가 삭제되었는지 확인합니다.

설치 패키지가 삭제된 관리 중인 Kaspersky 애플리케이션의 EULA만 취소할 수 있습니다.

EULA가 취소됩니다. 취소한 EULA는 **중앙 관리 서버 → 고급 → 동의한 EULA** 섹션의 목록에 표시되지 않습니다. EULA를 취소한 Kaspersky 애플리케이션으로는 클라이언트 기기를 보호할 수 없습니다.

데이터 제공 정보

타사에게 전송되는 데이터

소프트웨어의 모바일 기기 관리 기능을 사용하는 경우, Android 운영 체제를 실행하는 기기로 푸시 알림 메커니즘을 통해 명령을 적시에 전달하기 위해 Google Firebase Cloud Messaging 서비스를 사용합니다. 사용자가 Google Firebase Cloud Messaging 서비스를 사용하도록 구성한 경우, 사용자는 자동 모드에서 Google Firebase Cloud Messaging 서비스로 푸시 알림을 전송해야 하는 Kaspersky Endpoint Security for Android 애플리케이션의 설치 ID 정보를 제공한다는 데 동의한 것으로 간주됩니다.

사용자가 Google Firebase Cloud Messaging 서비스와의 정보 교환을 차단하려는 경우에는 Google Firebase Cloud Messaging 서비스의 사용 설정을 초기화해야 합니다.

소프트웨어의 모바일 기기 관리 기능을 사용하는 경우, iOS 운영 체제를 실행하는 기기로 푸시 알림 메커니즘을 통해 명령을 적시에 전달하기 위해 Apple Push Notification Service(APN)를 사용합니다. 사용자가 APNs 인증서를 iOS MDM 서버에 설치하고, iOS 모바일 기기를 소프트웨어에 연결하기 위한 설정 모음으로 iOS MDM 프로필을 생성하고, 이 프로필을 모바일 기기에 설치한 경우 사용자는 다음 정보를 자동 모드에서 APN에 제공한다는 데 동의한 것으로 간주됩니다.

- 토큰 - 기기의 푸시 토큰. 서버는 기기로 푸시 알림을 보낼 때 이 토큰을 사용합니다.
- PushMagic - 푸시 알림에 포함되어야 하는 문자열. 문자열 값은 기기에 의해 생성됩니다.

로컬에서 처리되는 데이터

Kaspersky Security Center는 조직 네트워크의 기본 관리 및 유지 관리 작업의 중앙 집중식 실행을 위해 설계되었습니다. Kaspersky Security Center는 관리자가 조직의 네트워크 보안 수준에 대한 자세한 정보에 접근할 수 있도록 합니다. Kaspersky Security Center를 사용하면 Kaspersky 애플리케이션에 기초한 모든 보호 구성 요소를 구성할 수 있습니다. Kaspersky Security Center는 다음과 같은 주요 기능을 수행합니다.

- 조직 네트워크에서 기기 및 해당 사용자 탐지
- 기기 관리를 위해 관리 그룹의 계층 구조 생성
- 기기에 Kaspersky 애플리케이션 설치
- 설치된 애플리케이션의 설정 및 작업 관리
- Kaspersky 및 타사 애플리케이션의 업데이트 관리, 취약점 발견 및 해결
- 기기에서 Kaspersky 애플리케이션 활성화
- 사용자 계정 관리
- 기기에서 Kaspersky 애플리케이션의 작업 관련 정보 확인
- 리포트 보기

Kaspersky Security Center는 주요 기능을 수행하기 위해 다음과 같은 정보를 수신, 저장, 처리할 수 있습니다.

- Windows 도메인, Active Directory, Samba 도메인 컨트롤러 검색이나 IP 범위 검색을 통해 수신한 조직 네트워크의 기기에 대한 정보입니다. 중앙 관리 서버는 독립적으로 데이터를 가져오거나, 배포 지점으로 작동하는 네트워크 에이전트에서 데이터를 받습니다.

- 조직 구성단위, 도메인, 사용자 및 그룹에 대한 Active Directory 및 Samba의 정보입니다. 중앙 관리 서버는 독립적으로 데이터를 가져오거나, 배포 지점으로 작동하는 네트워크 에이전트에서 데이터를 받습니다.

- 관리 중인 기기의 세부 정보. 네트워크 에이전트는 아래 나열된 데이터를 기기에서 중앙 관리 서버로 전송합니다. 사용자는 관리 콘솔 인터페이스 또는 Kaspersky Security Center 웹 콘솔 인터페이스에 기기의 표시 이름 및 설명을 입력합니다:

  - 기기 식별에 필요한 관리 중인 기기 및 구성 요소의 기술 사양: 기기 표시 이름 및 설명, Windows 도메인 이름 및 유형, Windows 환경의 기기 이름, DNS 도메인 및 DNS 이름, IPv4 주소, IPv6 주소, 네트워크 위치, MAC 주소, 일련 번호, 운영 체제 유형, 기기가 하이퍼바이저 유형 및 가상 컴퓨터인지 여부, 기기가 VDI에 속한 동적 가상 컴퓨터인지 여부.

  - 관리 중인 기기의 감사 및 특정 패치와 업데이트 적용 가능 여부의 결정에 필요한 관리 중인 기기 및 구성 요소의 기타 사양: Windows 업데이트 에이전트(WUA) 상태, 운영 체제 아키텍처, 운영 체제 공급사, 운영 체제 빌드 번호, 운영 체제 릴리즈 ID, 운영 체제 위치 폴더, 기기가 가상 컴퓨터인 경우 가상 컴퓨터 유형; 기기를 관리하는 가상 중앙 관리 서버의 이름; 클라우드 기기 데이트 (클라우드 리전, VPC, 클라우드 가용 영역, 클라우드 서브넷, 클라우드 배치 영역).

  - 관리 중인 기기에 대한 작업 세부 정보: 마지막 업데이트 날짜 및 시간, 기기가 네트워크에서 마지막으로 확인된 시간, 다시 시작 대기 상태, 기기를 켠 시간.

  - 기기 사용자 계정 및 작업 세션의 세부 정보.

- 관리 중인 기기에서 원격 진단을 실행하여 받은 데이터: 추적 파일, 시스템 정보, 기기에 설치된 Kaspersky 애플리케이션 세부 정보, 덤프 파일, 이벤트 로그, Kaspersky 기술 지원에서 받은 진단 스크립트 실행 결과.

- 기기가 배포 지점인 경우 배포 지점 작업 통계. 네트워크 에이전트는 기기에서 중앙 관리 서버로 데이터를 전송합니다.

- 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 입력한 배포 지점 설정.

- 모바일 기기를 중앙 관리 서버에 연결하는 데 필요한 데이터: 인증서, 모바일 연결 포트, 중앙 관리 서버 연결 주소. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- iOS MDM 프로토콜을 사용하여 전송된 모바일 기기의 세부 정보. 모바일 기기에서 중앙 관리 서버로 전송되는 데이터는 이하 목록과 같습니다.

  - 기기 식별에 필요한 관리 중인 모바일 기기와 해당 구성 요소의 기술 사양: 기기 이름, 모델, 운영 체제 이름 및 빌드 번호, 기기 모델 번호, IMEI 번호, UDID, MEID, 일련 번호, 메모리의 양, 모뎀 펌웨어 버전, 블루투스 MAC 주소, Wi-Fi MAC 주소, SIM 카드 세부 정보(SIM 카드 ID의 일부분인 ICCID).

  - 관리 중인 기기에서 사용하는 모바일 네트워크의 세부 정보: 모바일 네트워크 유형, 현재 사용하는 모바일 네트워크의 이름, 홈 모바일 네트워크의 이름, 모바일 네트워크 운영자 설정의 버전, 음성 로밍 및 데이터 로밍 상태, 홈 네트워크의 국가 코드, 거주 국가 코드, 현재 사용하는 네트워크의 국가 코드, 암호화 레벨.

  - 모바일 기기의 보안 설정: 암호 사용 및 암호의 정책 설정 준수 여부, 타사 애플리케이션 설치에 사용되는 구성 프로필 및 프로비저닝 프로필의 목록.

  - 중앙 관리 서버와의 마지막 동기화 날짜 및 기기 관리 상태.

- 기기에 설치된 Kaspersky 애플리케이션의 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다.
  - 관리 중인 기기에 설치되어 있는 Kaspersky 애플리케이션 설정: Kaspersky 애플리케이션 이름 및 버전, 상태, 실시간 보호 상태, 마지막 기기 검사 날짜와 시간, 탐지된 위협 수, 치료되지 않은 개체 수, 애플리케이션 구성 요소의 가용성 및 상태, 마지막 업데이트 시간 및 안티 바이러스 데이터베이스의 버전, Kaspersky 애플리케이션 설정 및 작업의 세부 정보, 활성 및 예약 라이센스 키 정보, 애플리케이션 설치 날짜 및 ID.
  - 애플리케이션 작동 통계: 관리 중인 기기의 Kaspersky 애플리케이션 구성 요소 상태 변경 및 애플리케이션 구성 요소가 시작한 작업의 성능 관련 이벤트.
  - Kaspersky 애플리케이션에 의해 정의된 기기 상태.
  - Kaspersky 애플리케이션에 의해 할당된 태그.
  - Kaspersky 애플리케이션용으로 설치된 업데이트와 적용 가능한 업데이트 세트.
- Kaspersky Security Center 구성 요소와 관리 중인 Kaspersky 애플리케이션의 이벤트에 포함된 데이터. 네트워크 에이전트는 기기에서 중앙 관리 서버로 데이터를 전송합니다.
- 이벤트 내보내기를 위한 Kaspersky Security Center와 SIEM 시스템의 통합에 필요한 데이터. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 정책 및 정책 프로필에 표시되어 있는 Kaspersky Security Center 구성 요소 및 관리 중인 Kaspersky 애플리케이션의 설정. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- Kaspersky Security Center 구성 요소 및 관리 중인 Kaspersky 애플리케이션의 작업 설정. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 취약점 및 패치 관리 기능을 통해 처리되는 데이터. 네트워크 에이전트는 아래 나열된 데이터를 기기에서 중앙 관리 서버로 전송합니다.
  - 관리 중인 기기(자산 관리(소프트웨어))에 설치된 애플리케이션 및 패치의 세부 정보.
  - 관리 중인 기기(자산 관리(하드웨어))에서 탐지된 하드웨어의 정보.

    Windows를 실행하는 기기에 네트워크 에이전트를 설치했다면 기기 하드웨어에 대한 다음 정보를 중앙 관리 서버로 전송합니다.
    - RAM
    - 대용량 스토리지 기기
    - 마더보드
    - CPU
    - 네트워크 어댑터
    - 모니터
    - 비디오 어댑터
    - 사운드 카드

Linux 또는 macOS 실행하는 장치에 네트워크 에이전트를 설치했다면, 운영 체제에서 해당 정보를 제공하는 경우 장치 하드웨어에 대한 다음 정보를 중앙 관리 서버로 전송합니다.

- 총 RAM 크기
- 대용량 저장 기기의 총 크기
- 마더보드
- CPU
- 네트워크 어댑터

- 관리 중인 기기에서 탐지된 타사 소프트웨어의 취약점 세부 정보.
- 관리 중인 기기에 설치된 타사 애플리케이션에 사용할 수 있는 업데이트 세부 정보.
- WSUS 기능이 발견한 Microsoft 업데이트 세부 정보.
- WSUS 기능이 발견한, 기기에 설치되어야 하는 Microsoft 업데이트 목록.

- 관리 중인 기기의 타사 소프트웨어 취약성을 수정하기 위해 격리된 중앙 관리 서버에서 업데이트를 다운로드하는 데 필요한 데이터입니다. 사용자는 중앙 관리 서버 klscflag 유틸리티를 사용하여 데이터를 입력하고 전송합니다.
- 클라우드 환경(Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud)에서 Kaspersky Security Center 작업에 필요한 데이터. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 애플리케이션의 사용자 카테고리. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 관리 중인 기기에서 애플리케이션 제어 기능으로 탐지된 실행 파일 목록. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.
- 백업 저장소에 보관된 파일의 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.
- 격리 저장소에 보관된 파일의 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.
- 자세한 분석을 위해 Kaspersky 전문가가 요청한 파일의 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.
- 적응형 이상 행위 제어 규칙의 상태 및 트리거링 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.
- 관리 중인 기기에 설치되어 있거나 이에 연결되어 매체 제어 기능에 의해 탐지된 외부 기기(메모리 기기, 정보 전송 도구, 정보 하드카피 도구, 연결 버스)의 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.

- 암호화된 기기 및 암호화 상태의 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다.

- 기기에서 Kaspersky 애플리케이션의 데이터 암호화 기능을 사용하여 발생한 데이터 암호화 오류의 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.

- 관리 중인 PLC(Programmable Logic Controller)의 목록. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.

- 위협 개발 체인 생성에 필요한 데이터. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.

- 조직의 직원이 클라우드 서비스에 접근하려는 시도에 대한 정보입니다. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 전체 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.

- Kaspersky Security Center를 Kaspersky Managed Detection and Response 서비스와 통합하는 데 필요한 데이터(Kaspersky Security Center 웹 콘솔 전용 플러그인 설치 필요): 통합 시작 토큰, 통합 토큰, 사용자 세션 토큰. 사용자가 Kaspersky Security Center 웹 콘솔 인터페이스에 통합 시작 토큰을 입력합니다. Kaspersky MDR 서비스에서 전용 플러그인을 통해 통합 토큰과 사용자 세션 토큰을 전송합니다.

- 입력한 활성화 코드 또는 지정된 키 파일의 세부 정보. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- 사용자 계정: 이름, 설명, 전체 이름, 이메일 주소, 기본 전화번호, 비밀번호, 중앙 관리 서버에서 생성한 비밀 키, 2단계 인증을 위한 일회성 비밀번호. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- ID 및 액세스 관리가 중앙 집중식 인증과 Kaspersky Security Center에 통합된 Kaspersky 애플리케이션 간에 SSO(싱글 사인온)를 제공하는 데 필요한 데이터: ID 및 액세스 관리 설치 및 구성 설정, ID 및 액세스 관리 사용자 세션, ID 및 액세스 관리 토큰, 클라이언트 애플리케이션 상태 및 리소스 서버 상태. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- 관리 개체의 리비전 내역. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- 사용자가 리비전을 만든 기기의 IP 주소입니다. IP 주소는 중앙 관리 서버에서 자동으로 정의합니다.

- 삭제된 관리 개체의 레지스트리. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- 파일에서 생성된 설치 패키지 및 설치 설정. 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- Kaspersky Security Center 웹 콘솔에서 Kaspersky의 공지 사항을 표시하는 데 필요한 데이터. 사용자가 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- Kaspersky Security Center 웹 콘솔에서 관리되는 애플리케이션의 플러그인 기능에 필요하며 일상적인 작업 중에 플러그인에 의해 중앙 관리 서버 데이터베이스에 저장되는 데이터. 데이터 제공에 대한 설명과 방법은 해당 애플리케이션의 도움말 파일에 제공됩니다.

- Kaspersky Security Center 웹 콘솔 사용자 설정: 현지화 언어 및 인터페이스 테마, 모니터링 패널 표시 설정, 알림 상태 정보(이미 읽음/아직 읽지 않음), 스프레드시트 열의 상태(표시/숨기기), 학습 모드 진도. 사용자가 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- Kaspersky Security Center 구성 요소 및 관리 중인 Kaspersky 애플리케이션에 대한 Kaspersky 이벤트 로그. Kaspersky 이벤트 로그는 각 기기에 저장되며, 절대 중앙 관리 서버로 전송되지 않습니다.
- 관리 중인 기기와 Kaspersky Security Center 구성 요소의 보안 연결을 위한 인증서. 사용자는 중앙 관리 서버 klsetsrvcert 유틸리티로 데이터를 입력합니다.
- 조직의 내부 웹 리소스에 대한 신뢰를 설정하기 위한 인증서입니다. 사용자가 Kaspersky Security Center 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- Amazon Web Services(AWS), Microsoft Azure, Google Cloud 및 Yandex.Cloud와 같은 클라우드 환경에서 Kaspersky Security Center를 운영하는 데 필요한 데이터. 중앙 관리 서버는 실행되는 가상 머신에서 데이터를 수신합니다.
- Kaspersky와 체결한 법적 계약 조건의 사용자 동의에 대한 정보.
- 사용자가 다음 구성 요소에 입력하는 중앙 관리 서버 데이터:
  - 관리 콘솔
  - Kaspersky Security Center 웹 콘솔
  - Klscflag 유틸리티 사용 시 명령줄 터미널
  - Klakaut 자동화 개체 및 Kaspersky Security Center OpenAPI를 통해 중앙 관리 서버와 상호 작용하는 구성 요소
- 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 인터페이스에서 입력하는 모든 데이터.

상기 나열된 데이터는 다음 방법 중 하나가 적용되면 Kaspersky Security Center에 표시될 수 있습니다.

- 사용자는 다음 구성 요소의 인터페이스에 데이터를 입력합니다.
  - 관리 콘솔
  - Kaspersky Security Center 웹 콘솔
  - Klscflag 유틸리티 사용 시 명령줄 터미널
  - Klakaut 자동화 개체 및 Kaspersky Security Center OpenAPI를 통해 중앙 관리 서버와 상호 작용하는 구성 요소
- 네트워크 에이전트는 자동으로 컴퓨터에서 데이터를 수신하고, 이를 중앙 관리 서버로 전송합니다.
- 네트워크 에이전트는 관리 중인 Kaspersky 애플리케이션이 가져온 데이터를 수신하고, 이를 중앙 관리 서버로 전송합니다. 관리 중인 Kaspersky 애플리케이션이 처리하는 데이터 목록은 해당 애플리케이션의 도움말 파일에 나와 있습니다.
- 중앙 관리 서버는 네트워크로 연결된 기기 정보를 독자적으로 얻거나 배포 지점 역할을 하는 네트워크 에이전트에서 받습니다.
- 데이터는 iOS MDM 프로토콜을 사용하여 모바일 기기에서 중앙 관리 서버로 전송됩니다.

목록에 나열된 데이터는 중앙 관리 서버 데이터베이스에 저장됩니다. 사용자 이름과 암호는 암호화된 형식으로 저장됩니다.

위에 명시된 모든 데이터는 Kaspersky Security Center 구성 요소의 덤프 파일, 추적 로그 파일 또는 로그 파일(예: 설치 프로그램 및 유틸리티에 의해 생성되는 로그 파일 등)을 통해서만 Kaspersky로 전송될 수 있습니다.

Kaspersky Security Center 구성 요소의 덤프 파일, 추적 로그 파일, 로그 파일에는 중앙 관리 서버, 네트워크 에이전트, 관리 콘솔, iOS MDM 서버, Kaspersky Security Center 웹 콘솔의 무작위 데이터가 포함됩니다. 이 파일에는 개인 데이터 및 민감한 데이터가 포함될 수 있습니다. 덤프 파일, 추적 로그 파일 및 로그 파일은 암호화되지 않은 형식으로 기기에 저장됩니다. 덤프 파일, 추적 로그 파일 및 로그 파일은 Kaspersky에 자동 전송되지 않습니다. 그러나 관리자는 Kaspersky Security Center 작업의 문제를 해결하기 위해 기술 지원에서 요청하는 경우 Kaspersky에 데이터를 수동으로 전송할 수 있습니다.

사용자는 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔의 링크로 이동하여 다음 데이터 자동 전송에 동의합니다:

- Kaspersky Security Center 코드
- Kaspersky Security Center 버전
- Kaspersky Security Center 현지화
- 라이센스 ID
- 라이센스 유형
- 파트너를 통해 라이센스를 구매했는지 여부

각 링크를 통해 제공되는 데이터 목록은 링크의 목적과 위치에 따라 다릅니다.

Kaspersky는 익명의 형식으로 수신한 데이터를 일반 통계 목적으로만 사용합니다. 요약 통계는 원래 수신한 정보를 바탕으로 자동 생성되며, 어떠한 개인 데이터 또는 기밀 데이터도 포함하지 않습니다. 새 데이터가 축적되는 즉시 이전 데이터는 지워집니다(연 1회). 요약 통계는 무기한 저장됩니다.

Kaspersky는 이렇게 받은 정보를 법률 및 해당 Kaspersky 규칙에 따라 보호합니다. 데이터가 보안 채널을 통해 전송됩니다.

Kaspersky Security Center 라이센스 옵션

Kaspersky Security Center 다음 모드에서 작동합니다.

- **라이센스 없음(기본 기능)**

  애플리케이션이 활성화되지 않았거나 상업용 라이센스가 만료되면 Kaspersky Security Center가 이 모드에서 작동합니다. 기업 네트워크를 보호하기 위한 Kaspersky 애플리케이션에 관리 콘솔의 기본 기능을 지원하는 Kaspersky Security Center가 포함되어 제공됩니다. Kaspersky 웹사이트에서 다운로드할 수도 있습니다.

- **상업용 라이센스**

  관리 콘솔의 기본 기능에 포함되지 않은 추가 기능은 상업용 라이센스를 구매해야 사용할 수 있습니다.

  중앙 관리 서버 속성 창에서 라이센스 키를 추가할 때에는 Kaspersky Security Center를 사용할 수 있게 해주는 라이센스 키를 추가합니다. 이 정보는 Kaspersky 웹 사이트에서 찾을 수 있습니다. 각 솔루션 웹 페이지에는 이 솔루션에 포함된 애플리케이션 목록이 있습니다. 중앙 관리 서버는 지원되지 않는 라이센스 키(Kaspersky Endpoint Security Cloud용 라이센스 키 등)를 허용할 수 있지만 이러한 라이센스 키는 관리 콘솔의 기본 기능 외에 새로운 기능을 제공하지 않습니다.

기능 또는 속성	Kaspersky Security Center 동작 모드	
	라이센스 없음	상업용 라이센스
관리 콘솔의 기본 기능 다음과 같은 기능을 사용할 수 있습니다: • 원격 사무소 또는 클라이언트 조직의 네트워크 관리를 위해 가상의 중앙 관리 서버 만들기. • 특정 기기들을 하나의 구성으로 관리하기 위해 관리 그룹의 계층 만들기. • 애플리케이션 원격 설치. • 클라이언트 기기에 설치된 애플리케이션의 중앙 집중식 구성. • 조직의 안티 바이러스 보안 상태 제어. • 사용자 역할 관리. • 애플리케이션 동작의 통계와 리포트, 심각 이벤트에 대한 알림. • 격리 저장소나 백업 저장소로 이동한 파일 및 처리가 연기된 파일에 대한 중앙 집중식 작업. • 암호화 및 데이터 보호 관리. • 기존 유료 애플리케이션 그룹 보기 및 편집. • 네트워크 검색에 의해 감지된 하드웨어 구성 요소 목록의 확인 및 편집. • 원격 설치에 사용할 운영 체제 이미지의 목록 보기.	✓	✓
취약점 및 패치 관리: 기본 기능 다음 작업에는 상업용 라이센스가 필요하지 않습니다. • *취약점 및 필요한 업데이트 검색* 작업 이 작업을 통해, Kaspersky Security Center는 관리 중인 기기에 설치된 타사 소프트웨어에 대해 감지된 취약점 및 필수 업데이트 목록을 받습니다. • *Windows Update 업데이트 설치* 작업 이 작업은 Windows Update 업데이트 설치에만 사용할 수 있습니다. 이 작업을 사용하려면 작업 설정에서 필요한 업데이트를 수동으로 지정해야 합니다. • *취약점 해결* 작업 *취약점 해결* 작업에서는 Microsoft 소프트웨어에 권장 수정을 사용하고 타사 소프트웨어에는 사용자 수정을 사용합니다. 이 작업을 사용하려면 작업 설정에서 취약점에 대한 사용자 픽스를 수동으로 지정해야 합니다.	✓	✓
취약점 및 패치 관리: 고급 기능 다음과 같은 기능을 사용할 수 있습니다: • 정의한 규칙에 따라 소프트웨어 업데이트를 자동으로 원격 설치하고 취약점을 수정합니다. • 관리 서버를 WSUS(Windows Server Update Services) 서버로 사용하여 중앙 집중식 모드에서 설정된 빈도로 기기의 Windows 업데이트 서비스에 대한 업데이트를 제공합니다.	—	✓

기능 또는 속성	Kaspersky Security Center 동작 모드	
	라이센스 없음	상업용 라이센스
MMC 기반 관리 콘솔의 모바일 기기 관리 기능 모바일 기기 관리 기능은 iOS MDM 및 Android 모바일 기기 관리에 사용됩니다. iOS MDM 기기에 다음 기능을 사용할 수 있습니다: • Kaspersky Security Center에 새 기기 추가. • 구성 프로필 만들기 및 편집, 모바일 기기에 구성 프로필 설치. • App Store®, 매니페스트 파일(.plist), 모바일 설치 패키지(.ipa)를 사용하여 모바일 기기에 애플리케이션 설치. • 모바일 기기 잠금, 모바일 기기 암호 재설정, 모바일 기기에서 모든 데이터 삭제를 포함하여 iOS MDM 기기에서 명령 실행. Android 기기에서 다음 기능을 사용할 수 있습니다: • Kaspersky Security Center에 새 기기 추가. • 정책을 통해 Kaspersky Endpoint Security for Android 관리. • 기기에서 명령 실행. 모바일 기기 관리 기능의 관리 단위는 모바일 기기입니다. 모바일 기기를 관리하려면 먼저 모바일 기기 서버에 연결해야 합니다.	—	✓ (중앙 관리 서버 속성에 라이센스 키를 추가해야 합니다.)
Kaspersky Security Center 웹 콘솔의 모바일 기기 보호 Kaspersky Security Center 웹 콘솔은 Android 및 iOS 모바일 기기를 관리할 수 있는 다음 기능을 제공합니다. • Kaspersky Security Center에 새 기기 추가. • 정책을 통해 Kaspersky Endpoint Security for Android 및 Kaspersky Security for iOS 관리. • 관련 프로토콜을 통해 모바일 기기에 명령을 보내고 명령을 실행합니다.	—	✓ (각 모바일 기기에 라이센스 키를 추가해야 합니다.)
시스템 관리 다음과 같은 기능을 사용할 수 있습니다: • 운영 체제 및 애플리케이션 설치. Kaspersky Security Center를 사용하면 운영 체제의 이미지를 만들어 네트워크에 있는 클라이언트 기기에 배포하고 Kaspersky 또는 다른 공급업체에 의해 애플리케이션의 원격 설치를 수행할 수 있습니다. 운영 체제의 이미지를 캡처하여 중앙 관리 서버에 해당 이미지를 전송할 수 있습니다. 운영 체제의 이러한 이미지는 중앙 관리 서버의 전용 폴더에 저장됩니다. 참조 기기의 운영 체제 이미지가 캡처된 다음 설치 패키지 만들기 작업을 통해 만들어집니다. 이미지를 사용해 아직 운영 체제가 설치되지 않은 새 네트워크 기기에 배포할 수 있습니다. 이 경우 Preboot eXecution Environment(PXE) 기술이 사용됩니다. • 유료 애플리케이션 관리. • 원격 데스크톱 연결이라고 하는 Microsoft® Windows® 구성 요소를 통해 클라이언트 기기에 연결하기 위한 원격 권한. • Windows 데스크톱 공유를 통해 클라이언트 기기에 원격 연결. • **Kaspersky 원격 데스크톱 세션 뷰어**를 통한 원격 연결.	—	✓

기능 또는 속성	Kaspersky Security Center 동작 모드	
	라이센스 없음	상업용 라이센스
클라우드 환경과 통합 Kaspersky Security Center는 실제 기기에서 작동할 뿐 아니라 클라우드 환경 구성 마법사와 같이 클라우드 환경에서 작업하기 위한 특수 기능도 제공합니다. Kaspersky Security Center는 다음 가상 컴퓨터와 연동됩니다. • Amazon EC2 인스턴스 • Microsoft Azure 가상 컴퓨터 • Google 클라우드 가상 컴퓨터 인스턴스 • Yandex.Cloud 가상 컴퓨터	—	✓
SIEM 시스템으로 이벤트 내보내기: Syslog 프로토콜 사용 Syslog 프로토콜을 사용하는 경우 Kaspersky Security Center 중앙 관리 서버 및 관리 중인 기기에 설치된 Kaspersky 애플리케이션에서 발생하는 모든 이벤트를 전달할 수 있습니다. Syslog 프로토콜은 표준 메시지 로깅 프로토콜입니다. SIEM 시스템으로 이벤트를 내보내는 데 사용할 수 있습니다.	✓	✓

Kaspersky Security Center 및 관리 애플리케이션의 라이센스 기능

중앙 관리 서버 및 관리 중인 애플리케이션의 라이센싱에는 다음 내용을 포함하고 있습니다:

- 취약점 및 패치 관리, 모바일 기기 관리, SIEM 시스템과의 통합을 활성화하려면, 중앙 관리 서버에 라이센스 키 파일 또는 유효한 활성화 코드를 추가할 수 있습니다. Kaspersky Security Center의 일부 기능은 활성 키 파일 또는 중앙 관리 서버에 추가된 유효한 활성화 코드에 따라서만 액세스 할 수 있습니다.
- 관리 중인 애플리케이션의 여러 활성화코드 및 키 파일을 중앙 관리 서버 저장소에 추가할 수 있습니다.

Kaspersky Security Center 라이센싱 정보

키 파일을 사용하여 라이센스가 필요한 기능(모바일 기기 관리 등)을 활성화하였으나 다른 유형의 라이센스가 필요한 기능(취약점 및 패치 관리 등)도 사용하고 싶다면, 서비스 제공 업체로부터 이 두 기능을 모두 활성화하는 키 파일을 구매하고 이 키 파일을 사용하여 중앙 관리 서버를 활성화해야 합니다.

관리 애플리케이션의 라이센싱 기능

관리 중인 애플리케이션을 라이센싱할 때 활성화코드 또는 키 파일을 자동으로 배포하거나 다른 편리한 방법으로 배포할 수 있습니다. 다음 방법을 사용하여 활성화코드 또는 키 파일을 배포할 수 있습니다:

- 자동 배포

  다른 관리 중인 애플리케이션을 사용하고 있으며 특정 키 파일 또는 활성화코드를 그 기기에 배포해야 하는 경우 해당 활성화코드 또는 키 파일을 배포하는 다른 방법을 선택합니다.

Kaspersky Security Center를 사용하면 기기에 사용 가능한 라이센스 키를 자동으로 배포할 수 있습니다. 예를 들어 세 개의 라이센스 키가 중앙 관리 서버 저장소에 저장됩니다. 라이센스 키 세 개 모두에 대하여 **관리 중인 기기에 자동으로 라이센스 키 배포** 확인란을 선택하였습니다. 그리고, Kaspersky 보안 제품(예, Kaspersky Endpoint Security for Windows)이 기업의 기기에 설치됩니다. 라이센스 키를 배포해야 하는 새 기기가 발견됩니다. 애플리케이션은 적용 가능한 라이센스 키를 결정합니다: 저장소에 추가된 라이센스 키 중 두 개(이름이 *Key_1*과 *Key_2*인 키)의 라이센스 키가 해당 기기에 적용할 수 있습니다. 이러한 라이센스 키 중 하나가 기기에 배포됩니다. 이 경우, 라이센스 키 자동 배포는 관리자가 시작한 작업이 아니기 때문에 적용 가능한 두 라이센스 키 중 어느 라이센스 키가 기기에 배포될지 예측할 수 없습니다.

라이센스 키가 배포되면, 해당 기기는 그 라이센스 키가 적용된 기기로 카운터됩니다. 라이센스 키가 배포된 기기 수가 라이센스 제한을 초과하지 않는지 확인해야 합니다. 기기 수가 라이센스 제한을 초과하면, 해당 라이센스로 적용할 수 없는 모든 기기에 대해 *심각* 상태가 할당됩니다.

- 관리 중인 애플리케이션의 설치 패키지에 키 파일 또는 활성화코드 추가

  설치 패키지를 사용하여 관리 중인을 설치하는 경우 이 설치 패키지 또는 애플리케이션의 정책에서 활성화코드 또는 키 파일을 지정할 수 있습니다. 라이센스 키는 기기와 중앙 관리 서버를 다음에 동기화할 때 관리 중인 기기에 배포됩니다.

- 관리 중인 애플리케이션에 대해 라이센스 키 추가 작업을 실행하여 배포

  만일 관리 중인 애플리케이션에 대해 라이센스 키 추가 작업을 한다면, 기기에 배포해야 하는 라이센스 키를 선택하고 관리 그룹 또는 기기 조회와 같은 여러 편리한 방법으로 대상 기기를 선택할 수 있습니다.

- 기기에 수동으로 활성화코드 또는 키 파일 추가

Kaspersky 애플리케이션. 중앙 집중식 배포

이 섹션에서는 Kaspersky 애플리케이션을 원격 설치하고 네트워크에 있는 기기에서 이러한 애플리케이션을 제거하는 방법을 설명합니다.

클라이언트 기기에 애플리케이션을 배포하기 전에 기기의 하드웨어 및 소프트웨어가 개별 요구 사항을 충족하는지 확인하십시오.

네트워크 에이전트는 중앙 관리 서버와 클라이언트 기기의 연결을 제공하는 구성 요소입니다. 그러므로 중앙 집중식 원격 제어 시스템에 연결할 각 클라이언트 기기에 네트워크 에이전트를 설치해야 합니다. 중앙 관리 서버가 설치된 기기는 그 중앙 관리 서버 버전의 네트워크 에이전트만 사용할 수 있습니다. 이 버전은 중앙 관리 서버의 일부로 포함되므로 함께 설치 및 제거됩니다. 따라서 해당 기기에 네트워크 에이전트를 설치할 필요가 없습니다.

네트워크 에이전트는 다른 애플리케이션과 마찬가지로 원격으로 또는 로컬로 설치할 수 있습니다. 관리 콘솔을 통해 보안 제품의 중앙 집중식 배포를 진행하는 동안 네트워크 에이전트를 해당 보안 제품과 함께 설치할 수 있습니다.

네트워크 에이전트는 작동하는 Kaspersky 애플리케이션에 따라 다를 수 있습니다. 네트워크 에이전트가 로컬에만 설치 가능한 경우도 있습니다(자세한 내용은 해당 애플리케이션의 설명서 참조). 클라이언트 기기에 네트워크 에이전트를 한 번만 설치하면 됩니다.

Kaspersky 애플리케이션은 관리 콘솔에서 관리 플러그인을 통해 관리됩니다. 따라서 Kaspersky Security Center를 통해 애플리케이션 관리 인터페이스에 접근하려면 해당 관리 플러그인이 관리자의 워크스테이션에 설치되어 있어야 합니다.

관리자 워크스테이션의 Kaspersky Security Center 메인 창에서 애플리케이션 원격 설치를 수행할 수 있습니다.

소프트웨어를 원격으로 설치하려면 원격 설치 작업을 만들어야 합니다.

생성된 원격 설치 작업은 해당 스케줄에 따라 시작됩니다. 이 작업을 직접 중지하여 설치 절차를 중단할 수 있습니다.

애플리케이션을 원격 설치하는 도중 오류가 반환되면 기기 준비 요구 사항이 충족되었는지 확인하십시오.

배포 리포트를 사용하여 네트워크에 있는 Kaspersky 애플리케이션의 원격 설치 진행 상태를 추적할 수 있습니다.

Kaspersky Security Center에 나열된 애플리케이션의 관리에 대한 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.

타사 보안 제품 교체

Kaspersky Security Center를 통해 Kaspersky 보안 제품을 설치할 때는 설치하는 애플리케이션과 호환되지 않는 타사 소프트웨어를 제거해야 할 수 있습니다. Kaspersky Security Center는 타사 애플리케이션을 제거하는 여러 가지 방법을 제공합니다.

인스톨러를 사용하여 비-호환 애플리케이션 제거

이 옵션은 Microsoft Management Console을 기반으로 하는 관리 콘솔에서만 사용할 수 있습니다.

비-호환 애플리케이션을 제거하는 인스톨러의 작업 방법은 다양한 설치 유형에서 지원됩니다. 보안 제품 설치 패키지의 속성 창(**비호환 애플리케이션** 섹션)에서 **비호환 애플리케이션 자동 제거** 옵션을 선택한 경우 해당 보안 제품을 설치하기 전에 모든 비-호환 애플리케이션이 자동으로 제거됩니다.

애플리케이션의 원격 설치를 구성할 때 비-호환 애플리케이션 제거

보안 제품의 원격 설치를 구성할 때 **비호환 애플리케이션 자동 제거** 옵션을 활성화할 수 있습니다. MMC(Microsoft Management Console) 기반 관리 콘솔의 원격 설치 마법사에서 이 옵션을 사용할 수 있습니다. Kaspersky Security Center 웹 콘솔의 보호 배포 마법사에서 이 옵션을 찾을 수 있습니다. 이 옵션을 사용하도록 설정하면 Kaspersky Security Center는 비-호환 애플리케이션을 제거한 후 보안 제품을 관리 중인 기기에 설치합니다.

방법 지침:

- 관리 콘솔: 원격 설치 마법사를 사용하여 비호환 애플리케이션 제거
- Kaspersky Security Center 웹 콘솔: 설치하기 전에 비-호환 애플리케이션 제거

전용 작업을 통해 비-호환 애플리케이션 제거

비-호환 애플리케이션을 제거하려면 **애플리케이션을 원격으로 제거** 작업을 사용합니다. 이 작업은 보안 제품 설치 작업 전에 기기에서 실행해야 합니다. 예를 들어 설치 작업 시 **애플리케이션을 원격으로 제거** 작업이 진행 중인 경우 **다른 작업 완료 시** 스케줄 유형을 선택할 수 있습니다.

이 제거 방법은 보안 제품 설치 관리자가 비-호환 애플리케이션을 올바르게 제거할 수 없는 경우에 적합합니다.

관리 콘솔 사용 지침: 작업 만들기.

원격 설치 작업을 사용하여 애플리케이션 설치

Kaspersky Security Center에서 원격 설치 작업을 사용해 기기에 원격으로 애플리케이션을 설치할 수 있습니다. 이런 작업은 전용 마법사를 통해 생성되어 기기에 할당됩니다. 빠르고 쉽게 작업을 할당하려면 다음 방법 중 하나로 마법사 창에서 기기(최대 1,000대 기기)를 지정합니다.

- **중앙 관리 서버가 발견한 기기 중에서 선택**. 이 경우 특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.
- **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**. 작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.
- **기기 선택 결과에 작업 할당**. 이 경우 이전에 만든 조회에 포함되는 기기에 작업이 할당됩니다. 사전 정의 조회 또는 직접 생성한 사용자 지정 조회를 지정할 수 있습니다.
- **관리 그룹에 작업 할당**. 이 경우 이전에 만든 관리 그룹에 포함된 기기 작업이 할당됩니다.

네트워크 에이전트를 설치하지 않은 클라이언트 기기에 애플리케이션 설치 시 문제 발생을 방지하려면 Kaspersky Security Center의 원격 설치 작업을 통한 강제 배포에 설명된 대로 설치를 진행해야 합니다.

선택한 기기에 애플리케이션 설치

선택한 기기에 애플리케이션을 설치하려면:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **작업 생성** 버튼을 눌러 작업 만들기를 실행합니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

   Kaspersky Security Center **중앙 관리 서버 노드**에 있는 새 작업 마법사의 **작업 유형 선택** 창에서 작업 유형으로 **애플리케이션 원격 설치**를 선택합니다.

   새 작업 마법사가 특정 기기에 선택한 애플리케이션의 원격 설치 작업을 만듭니다. 새롭게 생성된 작업은 **작업** 폴더의 작업 영역에 표시됩니다.
3. 이 작업을 직접 실행하거나 작업 설정에 지정된 스케줄에 따라 실행될 때까지 기다립니다.

원격 설치 작업이 완료되면 선택한 애플리케이션이 선택한 기기에 설치됩니다.

관리 그룹의 클라이언트 기기에 애플리케이션 설치

관리 그룹의 클라이언트 기기에 애플리케이션을 설치하려면 다음과 같이 하십시오:

1. 관련 관리 그룹을 제어하는 중앙 관리 서버에 연결합니다.
2. 콘솔 트리에서 관리 그룹을 선택합니다.
3. 그룹 작업 영역에서 **작업** 탭을 선택합니다.
4. **작업 생성** 버튼을 눌러 작업 만들기를 실행합니다.

새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

Kaspersky Security Center 중앙 관리 서버 노드에 있는 새 작업 마법사의 **작업 유형 선택** 창에서 작업 유형으로 **애플리케이션 원격 설치**를 선택합니다.

새 작업 마법사가 선택한 애플리케이션의 원격 설치 그룹 작업을 만듭니다. 새 작업이 **작업** 탭에 있는 관리 그룹의 작업 영역에 표시됩니다.

5. 이 작업을 직접 실행하거나 작업 설정에 지정된 스케줄에 따라 실행될 때까지 기다립니다.

원격 설치 작업이 완료되면 선택한 애플리케이션이 관리 그룹의 클라이언트 기기에 설치됩니다.

Active Directory 그룹 정책을 통해 애플리케이션 설치

Kaspersky Security Center에서는 Active Directory 그룹 정책을 사용하여 관리 중인 기기에 Kaspersky 애플리케이션을 설치할 수 있습니다.

네트워크 에이전트가 포함된 설치 패키지를 통해서만 Active Directory 그룹 정책을 사용하여 애플리케이션을 설치할 수 있습니다.

Active Directory 그룹 정책을 사용하여 애플리케이션을 설치하려면 다음과 같이 하십시오:

1. 원격 설치 마법사를 사용하여 애플리케이션 설치 구성을 시작합니다.
2. 원격 설치 마법사의 **원격 설치 작업 설정 정의** 창에서 **Active Directory 그룹 정책에 패키지 설치 지정** 옵션을 선택합니다.
3. 원격 설치 마법사의 **기기에 접근할 수 있는 계정 선택** 창에서 **계정 필요(네트워크 에이전트는 사용되지 않음)** 옵션을 선택합니다.
4. Kaspersky Security Center가 설치된 기기 또는 Group Policy Creator Owners 도메인 그룹에 포함된 계정에 관리자 권한을 가진 계정을 추가합니다.
5. 선택한 계정에 권한을 부여합니다.
   a. **제어판** → **관리 도구**로 이동하여 **그룹 정책 관리**를 엽니다.
   b. 필요한 도메인이 있는 노드를 클릭합니다.
   c. **위임** 섹션을 클릭합니다.
   d. **권한** 드롭다운 목록에서 **GPO 링크**를 선택합니다.
   e. **추가**를 클릭합니다.
   f. **사용자, 컴퓨터 또는 그룹 선택** 창이 열리면 필요한 계정을 선택합니다.
   g. **확인**을 클릭하여 **사용자, 컴퓨터 또는 그룹 선택** 창을 닫습니다.
   h. **그룹 및 사용자** 목록에서 방금 추가한 계정을 선택하고 **고급** → **고급**을 클릭합니다.
   i. **권한 항목** 목록에서 지금 추가한 계정을 두 번 클릭합니다.

j. 다음 권한을 부여합니다.

- **Group 개체 생성**
- **Group 개체 삭제**
- **그룹 정책 컨테이너 개체 만들기**
- **그룹 정책 컨테이너 개체 삭제**

k. **확인**을 눌러 변경을 저장합니다.

6. 마법사의 지시에 따라 기타 설정을 정의합니다.

7. 만들어진 원격 설치 작업을 수동으로 실행하거나 시작 스케줄을 기다립니다.

다음과 같은 원격 설치 시퀀스가 시작됩니다:

1. 작업이 실행될 때 지정된 집합의 모든 클라이언트 기기가 있는 각 도메인에 다음과 같은 개체가 만들어집니다:
   - **Kaspersky_AK{GUID}** 이름의 그룹 정책 개체(GPO).
   - GPO에 해당하는 보안 그룹. 이 보안 그룹에는 작업에 포함되는 클라이언트 기기가 있습니다. 보안 그룹 컨텐츠는 GPO의 범위를 정의합니다.
2. Kaspersky Security Center는 선택한 Kaspersky 애플리케이션의 공유 네트워크 폴더인 KLSHARE에서 클라이언트 기기에 해당 애플리케이션을 직접 설치합니다. Kaspersky Security Center 설치 폴더에 설치할 애플리케이션의 .msi 파일이 포함된 보조 하위 폴더가 만들어집니다.
3. 새 기기를 작업 범위에 추가하는 경우 해당 기기는 다음 작업 시작 시 보안 그룹에 추가됩니다. 작업 스케줄에서 **누락된 작업 실행** 옵션을 선택하면, 기기가 보안 그룹에 즉시 추가됩니다.
4. 기기를 작업 범위에서 삭제하는 경우 해당 기기는 다음 작업 시작 시 보안 그룹에서 삭제됩니다.
5. Active Directory에서 작업을 삭제하는 경우 GPO, GPO 링크 및 해당 보안 그룹도 삭제됩니다.

Active Directory를 사용하는 다른 설치 구성을 적용하려는 경우 필요한 설정을 수동으로 구성할 수 있습니다. 예를 들어, 이는 다음과 같은 경우에 필요할 수 있습니다:

- 안티 바이러스 보호 관리자에게 특정 도메인의 Active Directory를 변경할 권한이 없는 경우
- 원본 설치 패키지를 별도의 네트워크 리소스에 저장해야 하는 경우
- GPO를 특정 Active Directory 단위에 연결해야 하는 경우

Active Directory를 통해 다른 설치 구성을 사용할 수 있는 다음과 같은 옵션이 제공됩니다:

- Kaspersky Security Center 공유 폴더에서 직접 설치하려면, GPO 속성에서 필요한 애플리케이션의 설치 패키지 폴더에 있는 exec 하위 폴더의 msi 파일을 지정해야 합니다.
- 설치 패키지가 다른 네트워크 리소스에 있는 경우 전체 exec 폴더 컨텐츠를 복사해야 합니다. 해당 폴더에 확장자가 .msi인 파일 외에도 패키지가 만들어질 때 생성된 구성 파일이 포함되어 있기 때문입니다. 라이센스 키를 애플리케이션과 함께 설치하려면 라이센스 키 파일도 이 폴더로 복사해야 합니다.

macOS 기기에 애플리케이션 원격 설치

다음 방법에 따라 원격 설치 작업을 사용하여 macOS를 실행하는 기기에 애플리케이션을 설치합니다.

1. 설치 패키지와 .sh 설치 스크립트로 구성된 압축 파일을 만듭니다.
2. 새 작업 마법사에서 **다운로드하기 전에 운영 체제 유형 확인** 옵션을 비활성화합니다.

또는 **스크립트 원격 실행** 작업을 사용할 수 있습니다. 다음 문서에서는 스크립트 원격 실행 작업을 사용하여 기기에 애플리케이션 원격 설치 작업을 진행하기 위해 파일을 구성하는 방법을 설명합니다.

보조 중앙 관리 서버에 애플리케이션 설치

보조 중앙 관리 서버에 애플리케이션을 설치하려면:

1. 관련 보조 중앙 관리 서버를 제어하는 중앙 관리 서버에 연결합니다.
2. 설치되고 있는 애플리케이션에 대한 설치 패키지가 선택한 각 보조 중앙 관리 서버에 있는지 확인합니다. 설치 패키지가 어느 보조 서버에도 없는 경우 설치 패키지 배포 작업을 사용하여 배포합니다.
3. 다음 방법 중 하나로 보조 중앙 관리 서버에 애플리케이션 설치 작업을 만듭니다:
   - 선택한 관리 그룹에 보조 중앙 관리 서버에 대한 작업을 만들려면 이 그룹에 대한 원격 설치 그룹 작업을 만듭니다.
   - 특정 보조 중앙 관리 서버에 대한 작업을 만들려면 특정 기기에 대한 원격 설치 작업을 만듭니다.

   배포 작업 만들기 마법사가 시작되어 원격 설치 작업 만들기 과정을 안내합니다. 마법사의 지침을 따릅니다.

   Kaspersky Security Center 중앙 관리 서버 섹션에 있는 새 작업 마법사에 있는 **작업 유형 선택** 창의 **고급** 폴더를 열고 작업 유형으로 **보조 중앙 관리 서버에 애플리케이션 원격 설치**를 선택합니다.

   새 작업 마법사가 특정 보조 중앙 관리 서버에 선택한 애플리케이션의 원격 설치 작업을 만듭니다.
4. 이 작업을 직접 실행하거나 작업 설정에 지정된 스케줄에 따라 실행될 때까지 기다립니다.

원격 설치 작업이 완료되면 선택한 애플리케이션이 보조 중앙 관리 서버에 설치됩니다.

원격 설치 마법사를 사용하여 애플리케이션 설치

원격 설치 마법사를 사용하여 Kaspersky 애플리케이션을 설치할 수 있습니다. 원격 설치 마법사에서는 미리 만든 설치 패키지나 배포 패키지를 사용해 직접 애플리케이션을 원격 설치할 수 있습니다.

네트워크 에이전트가 설치되지 않은 클라이언트 기기에서 원격 설치 작업을 올바르게 수행하려면 다음 포트가 열려 있어야 합니다: TCP 139 및 445, UDP 137 및 138. 기본적으로 이러한 포트는 해당 도메인에 포함된 모든 기기에 열려 있습니다. 네트워크 오류가 있는 경우 Kaspersky Security Center 기술 자료를 참조하십시오.

원격 설치 마법사를 사용하여 선택한 기기에 애플리케이션을 설치하려면:

1. 콘솔 트리에서 **원격 설치** 폴더를 찾아서 **설치 패키지** 하위 폴더를 선택합니다.
2. 이 폴더의 작업 영역에서 설치해야 하는 애플리케이션의 설치 패키지를 선택합니다.
3. 설치 패키지의 마우스 오른쪽 메뉴에서 **애플리케이션 설치**을 선택합니다.
   원격 설치 마법사가 시작됩니다.
4. **설치할 기기 선택** 창에서는 애플리케이션이 설치되는 기기의 목록을 만들 수 있습니다:
   - **관리 중인 기기의 그룹에 설치**

     이 옵션을 선택하면 기기 그룹에 대해 원격 설치 작업이 만들어집니다.

   - **설치할 기기 선택**

     이 옵션을 선택하면 특정 기기에 대해 원격 설치 작업이 만들어집니다. 특정 기기에는 관리 그룹의 기기와 미할당 기기가 모두 포함됩니다.

5. **원격 설치 작업 설정 정의** 창에서는 애플리케이션의 원격 설치에 대한 설정을 지정합니다.
   강제 설치 패키지 다운로드 설정 그룹에서 애플리케이션 설치에 필요한 파일이 클라이언트 기기에 배포되는 방식을 지정합니다:
   - **네트워크 에이전트 이용**

     이 옵션을 활성화하면 이들 클라이언트 기기에 설치된 네트워크 에이전트에 의해 클라이언트 기기로 설치 패키지가 전송됩니다.

     이 옵션을 비활성화하면 클라이언트 기기의 운영 체제 도구를 사용해 설치 패키지를 전송합니다.

     네트워크 에이전트가 설치된 기기에 작업이 할당된 경우 옵션을 활성화하는 것이 좋습니다.

     기본적으로 이 옵션은 켜져 있습니다.

   - **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드**

     이 옵션을 사용하면 중앙 관리 서버를 통해 클라이언트 기기의 운영 체제 도구를 사용하여 파일을 클라이언트 기기로 전송합니다. 이 옵션은 클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않아도 활성화할 수 있지만, 이 경우 클라이언트 기기는 중앙 관리 서버와 같은 네트워크에 있어야 합니다.

     기본적으로 이 옵션은 켜져 있습니다.

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

     이 옵션을 활성화하면 배포 지점을 통해 운영 체제 도구를 사용하여 클라이언트 기기로 설치 패키지가 전송됩니다. 네트워크에 하나 이상의 배포 지점이 있어야 이 옵션을 선택할 수 있습니다.

     네트워크 에이전트 이용 옵션이 활성화된 경우 네트워크 에이전트 도구를 사용할 수 없는 경우에만 운영 체제 도구를 사용하여 파일을 전송합니다.

이 옵션은 기본적으로 가상 중앙 관리 서버에서 만들어진 원격 설치 작업에 대해 활성화됩니다.

기기에 할당된 모든 배포 지점에 문제가 발생하면 기기는 업데이트(안티 바이러스 데이터베이스 및 패치)와 설치 패키지를 수신하지 않습니다.

- **설치 시도 횟수**

  원격 설치 작업을 실행할 때 Kaspersky Security Center가 파라미터로 지정된 인스톨러 실행 횟수 이내에 관리 중인 기기에 애플리케이션을 설치하지 못하면, Kaspersky Security Center가 이 관리 중인 기기에 설치 패키지 전송을 중지하고 해당 기기에서 인스톨러를 더 이상 시작하지 않습니다.

  설치 시도 횟수 옵션을 사용하면 관리 중인 기기의 리소스를 절약하고 트래픽(설치 제거, MSI 파일 실행 및 오류 메시지)을 줄일 수 있습니다.

  작업 시작 시도를 반복하면 해당 기기에 설치를 방해하는 문제가 표시될 수 있습니다. 관리자는 지정된 설치 시도 횟수 내에서 문제를 해결하고(예: 충분한 디스크 공간을 할당하거나, 비-호환 애플리케이션을 제거하거나, 설치를 방해하는 다른 애플리케이션의 설정 수정 등) 작업을 다시 시작해야 합니다(수동 또는 스케줄).

  그럼에도 설치가 완료되지 않으면 문제를 해결할 수 없는 것으로 간주되고 추가적인 작업 시작은 리소스 및 트래픽의 불필요한 소비 측면에서 불필요한 것으로 간주됩니다.

  작업이 생성되면 시도 카운터가 `0`으로 설정됩니다. 기기에서 오류를 반환하면 인스톨러 실행 시 카운터 판독 값이 증가합니다.

  파라미터에서 지정한 시도 횟수를 초과했지만 기기가 애플리케이션을 설치할 준비가 되었다면, 설치 시도 횟수 파라미터 값을 높이고 애플리케이션 설치 작업을 시작할 수 있습니다. 또는 새 원격 설치 작업을 생성할 수 있습니다.

다른 중앙 관리 서버에서 관리하는 클라이언트 기기에 대해 수행할 작업을 정의합니다:

- **모든 기기에 설치**

  다른 중앙 관리 서버에서 관리하는 기기에도 애플리케이션이 설치됩니다.

  이 옵션은 기본적으로 선택되어 있습니다. 네트워크에 중앙 관리 서버가 하나라면 이 설정을 변경하지 않아도 됩니다.

- **이 중앙 관리 서버를 통해 관리되는 기기에만 설치**

  이 중앙 관리 서버에서 관리하는 기기에만 애플리케이션이 설치됩니다. 네트워크에 중앙 관리 서버가 여러 대 있고 해당 서버 간의 충돌을 방지하려는 경우 이 옵션을 선택합니다.

추가 설정을 지정합니다:

- **이미 설치한 애플리케이션은 설치하지 않음**

  이 옵션을 활성화하면 선택한 애플리케이션이 이 클라이언트 기기에 이미 설치된 경우 다시 설치되지 않습니다.

  이 옵션을 비활성화해도 애플리케이션이 설치됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **Active Directory 그룹 정책에 패키지 설치 지정**

  이 옵션을 활성화하면 Active Directory 그룹 정책을 통해 설치 패키지가 설치됩니다.
  이 옵션은 네트워크 에이전트 설치 패키지가 선택되어 있는 경우에 사용할 수 있습니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

6. **라이센스 키 선택** 창에서 라이센스 키와 배포 방법을 선택합니다:

   - **설치 패키지에 라이센스 키 추가 안 함(권장)**

     키가 호환되는 모든 기기에 자동으로 배포됩니다:
     - 키 속성에서 자동 배포가 켜 있을 경우.
     - **키 추가** 작업이 생성된 경우.

   - **설치 패키지에 라이센스 키 추가**

     키가 설치 패키지와 함께 기기에 배포됩니다.

     설치 패키지 저장소에 대한 읽기 권한은 공유되므로 이 방법을 사용하여 키를 배포하는 것은 권장하지 않습니다.

   설치 패키지에 라이센스 키가 포함되어 있지 않으면 **라이센스 키 선택** 창이 표시됩니다.
   설치 패키지에 라이센스 키가 포함되어 있는 경우 해당 라이센스 키의 세부 정보를 보여 주는 **라이센스 키 속성** 창이 표시됩니다.

7. **운영 체제 재시작 옵션 선택** 창에서 애플리케이션을 설치할 때 운영 체제를 다시 시작해야 하는 경우 기기를 다시 시작해야 하는지 여부를 지정합니다:

   - **기기 다시 시작 안 함**

     이 옵션을 선택하면 보안 제품 설치 후에 기기가 다시 시작되지 않습니다.

   - **기기 다시 시작**

     이 옵션을 선택하면 보안 제품 설치 후에 기기가 다시 시작됩니다.

   - **사용자 확인 후 처리**

     이 옵션을 선택하면 보안 제품을 설치한 후 기기를 다시 시작해야 한다는 알림이 사용자에게 표시됩니다. **수정** 링크를 사용하여 메시지 텍스트, 메시지 표시 기간 및 자동 다시 시작 시간을 수정할 수 있습니다.
     기본적으로 이 옵션은 선택되어 있습니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  이 옵션을 사용하면 다시 시작하기 전에 차단된 기기의 애플리케이션이 강제로 닫힙니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

8. **기기에 접근할 수 있는 계정 선택** 창에서 원격 설치 작업을 시작하는 데 사용할 계정을 추가할 수 있습니다:

   - **계정 필요 없음(네트워크 에이전트가 설치되어 있음)**

     이 옵션을 선택하면 애플리케이션 설치 프로그램을 실행할 계정을 지정하지 않아도 됩니다. 중앙 관리 서버가 실행 중인 계정에서 작업이 실행됩니다.
     클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않다면, 이 옵션은 이용할 수 없습니다.

   - **계정 필요(네트워크 에이전트는 사용되지 않음)**

     원격 설치 작업을 할당한 기기에 네트워크 에이전트가 설치되어 있지 않다면 이 옵션을 선택하십시오. 이때, 사용자 계정 또는 SSH 인증서를 지정하여 애플리케이션을 설치할 수 있습니다.

     - **로컬 계정**. 이 옵션을 선택했다면 애플리케이션 설치 프로그램을 실행할 계정을 지정합니다. **추가** 버튼을 클릭하고 **로컬 계정**을 선택한 다음 사용자 계정 자격 증명을 지정합니다.
       예를 들어 이 작업이 할당된 모든 기기에 필요한 모든 권한이 어떤 계정에도 없다면, 사용자 계정을 여러 개 지정할 수 있습니다. 이때, 작업 실행 시 추가한 모든 계정을 위에서부터 순서대로 사용합니다.

     - **SSH 인증서**. Linux 기반 클라이언트 기기에 애플리케이션을 설치한다면 사용자 계정 대신 SSH 인증서를 지정할 수 있습니다. **추가** 버튼을 클릭하고 **SSH 인증서**를 선택한 다음 인증서의 개인 및 공개 키를 지정합니다.
       개인 키를 생성하려면 ssh-keygen 유틸리티를 사용할 수 있습니다. Kaspersky Security Center는 개인 키의 PEM 형식을 지원하지만 ssh-keygen 유틸리티는 기본적으로 OPENSSH 형식으로 SSH 키를 생성합니다. Kaspersky Security Center에서는 OPENSSH 형식을 지원하지 않습니다. 지원되는 PEM 형식으로 개인 키를 생성하려면 ssh-keygen 명령에 -m PEM 옵션을 추가합니다. 예:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "< 사용자  이메일 >"
       ```

9. **설치 시작** 창에서 **다음** 버튼을 눌러 선택한 기기에 원격 설치 작업을 만들고 작업을 시작합니다.

   설치 시작 창에서 **원격 설치 마법사 완료 후 이 작업을 실행하지 않음** 옵션을 선택한 경우 원격 설치 작업이 시작되지 않습니다. 나중에 이 작업을 직접 시작할 수 있습니다. 작업 이름이 애플리케이션에 대한 설치 패키지의 이름에 대응합니다: **<설치 패키지 이름>의 설치**.

원격 설치 마법사를 사용하여 관리 그룹의 기기에 애플리케이션을 설치하려면:

1. 관련 관리 그룹을 제어하는 중앙 관리 서버에 연결합니다.
2. 콘솔 트리에서 관리 그룹을 선택합니다.
3. 그룹의 작업 영역에서 **처리 방법 수행** 버튼을 누르고 드롭다운 목록에서 **애플리케이션 설치**을 선택합니다.
   그러면 원격 설치 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
4. 마법사의 마지막 단계에서 **다음**을 눌러 선택한 기기에 원격 설치 작업을 만들고 실행합니다.

원격 설치 마법사가 완료되면 Kaspersky Security Center는 다음 동작을 수행합니다:

- 애플리케이션 설치를 위한 설치 패키지를 만듭니다(아직 만들지 않은 경우). 설치 패키지는 **원격 설치** 폴더에 있는 **설치 패키지** 하위 폴더에서 애플리케이션 이름 및 버전에 해당하는 이름 아래에 있습니다. 이 설치 패키지를 사용하여 나중에 애플리케이션을 설치할 수 있습니다.

- 특정 기기 또는 관리 그룹에 대한 원격 설치 작업을 만들고 시작합니다. 새로 생성된 원격 설치 작업은 **작업** 폴더에 저장되거나 생성된 관리 그룹의 작업에 추가됩니다. 나중에 이 작업을 직접 시작할 수 있습니다. 작업 이름이 애플리케이션에 대한 설치 패키지의 이름에 대응합니다: **<설치 패키지 이름>의 설치**.

관리 플러그인 작업

Kaspersky 애플리케이션은 관리 콘솔에서 관리 플러그인을 통해 관리합니다. Kaspersky Security Center를 통해 관리할 수 있는 각 Kaspersky 애플리케이션에는 관리 플러그인이 포함되어 있습니다. 애플리케이션 관리 플러그인을 사용하여 관리 콘솔에서 다음 작업을 수행할 수 있습니다.

- 애플리케이션 정책과 설정 생성 및 편집, 애플리케이션 작업 설정.

- 애플리케이션 작업, 애플리케이션 이벤트 및 클라이언트 기기로부터 받은 애플리케이션 작동 통계 수집.

설치된 플러그인 및 해당 버전 목록을 확인하려면:

1. 관리 콘솔 트리에서 **중앙 관리 서버 <서버_이름>**을 마우스 오른쪽 클릭하고 **속성**을 선택합니다.

2. **고급 → 설치된 애플리케이션 관리 플러그인 세부 정보**를 클릭합니다.

   오른쪽 창에 설치된 관리 플러그인 및 해당 버전 목록이 나타납니다.

Kaspersky Security Center 초기 설정 중에 중앙 관리 서버 빠른 시작 마법사를 실행할 때 관리되는 애플리케이션용 플러그인을 설치할 수 있습니다. 또한 관리 플러그인을 수동으로 설치할 수도 있습니다.

관리 플러그인을 수동으로 설치하려면:

1. Kaspersky 기술 지원 웹페이지에서 Kaspersky 애플리케이션용 관리 플러그인과 필요한 버전(Kaspersky Endpoint Security for Windows 12.6 등)을 다운로드합니다.

2. 관리 콘솔이 실행 중이라면 닫습니다.

3. 다운로드한 플러그인 파일의 압축을 풀고 klcfginst.msi 또는 klcfginst.exe 파일을 실행합니다. 마법사의 지침을 따릅니다.

4. 설치가 완료되면 관리 콘솔을 실행하고 이전 절차에 설명된 대로 플러그인이 설치된 플러그인 목록에 표시되는지 확인합니다.

관리 중인 애플리케이션 빠른 시작 마법사를 지원하는 관리 플러그인 설치 후 관리 콘솔을 실행하면 이 마법사가 자동으로 시작됩니다. 관리 중인 애플리케이션 빠른 시작 마법사의 단계를 통해 기본 Kaspersky 애플리케이션 정책 및 작업을 생성할 수 있습니다. 마법사는 초기 플러그인 설치 후 관리 콘솔을 실행하거나 아직 작업 및 정책이 생성되지 않은 Kaspersky 애플리케이션의 다른 버전과 호환되는 버전으로 관리 플러그인을 업데이트한 후에만 자동으로 시작됩니다. 관리 중인 애플리케이션 빠른 시작 마법사를 수동으로 시작할 수도 있습니다.

관리 중인 애플리케이션 빠른 시작 마법사를 수동으로 시작하려면 다음과 같이 하십시오.

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 중앙 관리 서버 노드의 마우스 오른쪽 메뉴에서 **모든 작업 → 관리 중인 애플리케이션 빠른 시작 마법사**를 선택합니다.
3. 관리 중인 애플리케이션 빠른 시작 마법사가 시작됩니다. 마법사 단계에 따라 기본 Kaspersky 애플리케이션 정책 및 작업을 생성합니다.

관리 플러그인을 제거하려면:

1. 관리 콘솔이 실행 중이라면 닫습니다.
2. Windows 레지스트리 편집기를 엽니다.
3. 다음 키를 찾습니다.
   - 32비트 시스템은 `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins`.
   - 64비트 시스템은 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins`.

   키는 설치된 관리 플러그인을 포함합니다. 각 플러그인에서 `DisplayName` 값은 플러그인 이름을, `UninstallString` 값은 플러그인 제거 명령을 포함합니다.
4. 제거하려는 플러그인의 키를 찾고 해당 `UninstallString` 값을 클립보드에 복사합니다.
5. 명령 문자열에 값을 붙여넣고 시스템 관리자 권한으로 실행합니다.

관리 플러그인 버전은 Kaspersky 관리 애플리케이션 버전보다 이전 버전일 수 없습니다. 기기에서 Kaspersky 애플리케이션을 업데이트한다면 같은 버전의 관리 플러그인을 설치해야 합니다.

이전 버전의 플러그인에서 생성된 정책을 열면 Kaspersky Security Network 진술문에 동의하라는 메시지가 표시됩니다.

Kaspersky Security Center 웹 콘솔을 제거하면 모든 관리 플러그인도 제거됩니다.

관리 중인 애플리케이션 버전보다 최신 버전의 플러그인에서 정책을 열어 저장하면 해당 정책이 업데이트되며, 이전 버전의 플러그인에서는 열 수 없습니다.

보호 배포 리포트 보기

보호 배포 리포트를 사용하여 보호 배포 진행 상태를 감시할 수 있습니다.

보호 배포 리포트를 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. **리포트** 폴더의 작업 영역에서 이름이 **보호 배포 리포트**인 리포트 템플릿을 선택합니다.

작업 영역 패널에 네트워크상의 모든 기기에 대한 보호 배포 정보가 포함된 리포트가 표시됩니다.

새 보호 배포 리포트를 작성하고 다음 사항에 대한 정보를 반드시 포함하는 데이터 유형을 지정할 수 있습니다:

- 관리 그룹에 대해
- 특정 기기에 대해
- 기기 조회에 대해
- 모든 기기에 대해

Kaspersky Security Center는 보안 제품이 설치되어 있고 실시간 보호가 설정되어 있으면 해당 기기에 보호 기능이 배포된 것으로 가정합니다.

애플리케이션 원격 제거

Kaspersky Security Center에서 원격 제거 작업을 통해 원격으로 기기에서 애플리케이션을 제거할 수 있습니다. 이런 작업은 전용 마법사를 통해 생성되어 기기에 할당됩니다. 기기에 쉽고 빠르게 작업을 할당하려면 다음 방법 중 하나로 마법사 창에서 기기를 지정합니다:

- **중앙 관리 서버가 발견한 기기 중에서 선택**. 이 경우 특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.
- **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**. 작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.
- **기기 선택 결과에 작업 할당**. 이 경우 이전에 만든 조회에 포함되는 기기에 작업이 할당됩니다. 사전 정의 조회 또는 직접 생성한 사용자 지정 조회를 지정할 수 있습니다.
- **관리 그룹에 작업 할당**. 이 경우 이전에 만든 관리 그룹에 포함된 기기 작업이 할당됩니다.

원격 제거 문제

타사 애플리케이션을 원격 제거할 때 관리자가 "이 기기에서 원격 제거가 경고와 함께 완료되었습니다. 제거할 애플리케이션이 설치되지 않았습니다"라는 경고를 접할 수 있습니다. 이 문제는 일반적으로 제거할 애플리케이션을 현재 로그인한 개별 사용자용으로만 설치했을 때 발생합니다. 해당 사용자가 로그인하지 않았다면 이 애플리케이션이 보이지 않으며 원격 제거할 수 없습니다.

이러한 동작은 같은 기기에서 여러 사용자가 사용하도록 설계된 애플리케이션과 다릅니다. 이러한 애플리케이션은 기기의 모든 사용자가 보고 접근할 수 있습니다.

Kaspersky Security Center 내에서 자산 관리(소프트웨어) 알고리즘은 개별 사용자용 애플리케이션과 복수 사용자용 애플리케이션을 다르게 처리합니다.

- 복수 사용자용 애플리케이션은 설치된 애플리케이션 목록에 실시간 최신 상태로 관리됩니다.
- 개별 사용자용 애플리케이션은 캐싱 메커니즘으로 모니터링됩니다.

  애플리케이션 탐지 시점에 사용자가 로그인한 상태였다면, Kaspersky Security Center는 해당 사용자의 애플리케이션에 대한 정보를 캐시합니다. 이후 사용자가 로그아웃한 후에도 Kaspersky Security Center는 캐시된 데이터에 따라 이러한 애플리케이션을 설치된 것으로 표시하지만, 해당 애플리케이션은 기기에서 보거나 접근할 수 없습니다.

이러한 불일치에 따라, Kaspersky Security Center가 캐시된 데이터를 기준으로 애플리케이션을 설치된 것으로 식별하더라도 사용자가 로그아웃한 상태에서는 애플리케이션에 액세스할 수 없으므로, 애플리케이션 제거 작업이 실패하는 상황이 발생할 수 있습니다.

캐시된 애플리케이션 데이터의 수명은 기본적으로 30일입니다. 관리자는 이 설정을 수정하여 캐시 기간을 줄이고, 기기에 표시되는 데이터와 실제 표시되는 애플리케이션의 불일치를 최소화할 수 있습니다.

캐시 수명을 1시간(3600초)으로 조정하려면 중앙 관리 서버에서 다음 명령을 실행합니다.

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

이 명령을 실행한 후 변경 사항을 적용하려면 중앙 관리 서버를 다시 시작하십시오.

설치한 애플리케이션에 관한 정보 출처

네트워크 에이전트는 다음 레지스트리 키에서 Windows 기기에 설치된 소프트웨어 정보를 검색합니다.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  모든 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  모든 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  현재 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  특정 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.

관리 그룹의 클라이언트 기기에서 애플리케이션 원격 제거

관리 그룹의 클라이언트 기기에서 애플리케이션을 원격으로 제거하려면 다음과 같이 하십시오:

1. 관련 관리 그룹을 제어하는 중앙 관리 서버에 연결합니다.
2. 콘솔 트리에서 관리 그룹을 선택합니다.
3. 그룹 작업 영역에서 **작업** 탭을 선택합니다.

4. **새 작업** 버튼을 눌러 작업 만들기를 실행합니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

   Kaspersky Security Center 중앙 관리 서버 노드에 있는 새 작업 마법사의 **작업 유형 선택** 창에서 **고급** 폴더를 열고 작업 유형으로 **애플리케이션 원격 제거**를 선택합니다.

   새 작업 마법사가 선택한 애플리케이션의 원격 제거 그룹 작업을 만듭니다. 새 작업이 **작업** 탭에 있는 관리 그룹의 작업 영역에 표시됩니다.

5. 이 작업을 직접 실행하거나 작업 설정에 지정된 스케줄에 따라 실행될 때까지 기다립니다.

원격 제거 작업이 완료되면 선택한 애플리케이션이 관리 그룹의 클라이언트 기기에서 제거됩니다.

선택한 기기에서 애플리케이션 원격 제거

선택한 기기에서 원격으로 애플리케이션을 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.

2. **새 작업**를 눌러 작업 만들기를 실행합니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

   Kaspersky Security Center 중앙 관리 서버 노드에 있는 새 작업 마법사의 **작업 유형 선택** 창에서 **고급** 폴더를 열고 작업 유형으로 **애플리케이션 원격 제거**를 선택합니다.

   새 작업 마법사가 특정 기기에서 선택한 애플리케이션의 원격 제거 작업을 만듭니다. 새롭게 생성된 작업은 **작업** 폴더의 작업 영역에 표시됩니다.

3. 이 작업을 직접 실행하거나 작업 설정에 지정된 스케줄에 따라 실행될 때까지 기다립니다.

원격 제거 작업이 완료되면 선택한 애플리케이션이 지정된 기기에서 제거됩니다.

설치 패키지 사용

원격 설치 작업을 만들 때 시스템은 소프트웨어 설치에 필요한 파라미터 집합이 들어 있는 설치 패키지를 사용합니다.

> 설치 패키지에는 키 파일을 포함할 수 있습니다. 키 파일이 포함된 설치 패키지를 공유하는 것은 권장하지 않습니다.

동일한 설치 패키지를 필요할 때마다 다시 사용할 수 있습니다.

중앙 관리 서버에서 생성한 설치 패키지는 콘솔 트리의 **설치 패키지** 하위 폴더인 **원격 설치** 폴더에 저장됩니다. 설치 패키지는 중앙 관리 서버의 지정한 공유 폴더 내 패키지라는 이름의 서비스 하위 폴더에 저장됩니다.

필요한 경우, **개체 삭제설치 패키지**설치 패키지 하위 폴더에서 설치 패키지를 삭제할 수 있습니다.

> 공유 폴더에서 설치 패키지의 컨텐츠를 수동으로 변경하지 마십시오. 필요한 경우, 설치 패키지의 복사본을 생성하여 목적에 맞게 변경하고 새 설치 작업을 생성할 수 있습니다.

설치 패키지 만들기

이 문서는 다음 유형의 설치 패키지 생성 절차를 설명합니다:

- Kaspersky 애플리케이션에 대한 설치 패키지를 생성합니다
- 지정된 실행 파일용 설치 패키지
- Kaspersky 데이터베이스의 애플리케이션용 설치 패키지

네트워크 에이전트 원격 설치용 설치 패키지를 수동으로 만들 필요는 없습니다. 이 패키지는 Kaspersky Security Center 설치를 진행하는 동안 자동으로 만들어져 **설치 패키지** 폴더에 저장됩니다. 네트워크 에이전트의 원격 설치를 위한 패키지가 삭제되었다면 Kaspersky Security Center 배포 패키지의 NetAgent 폴더에 있는 nagent.kud 파일을 선택하여 다시 만들 수 있습니다.

설치 패키지를 만들려면:

1. 필요한 중앙 관리 서버에 연결합니다.
2. 콘솔 트리에서 **고급 → 원격 설치 → 설치 패키지**로 이동합니다.
3. 다음 방법 중 하나로 새 설치 패키지 만들기를 시작합니다:
   - **설치 패키지** 폴더를 마우스 오른쪽 클릭한 후, 메뉴에서 **새로 만들기 → 설치 패키지**를 선택합니다.
   - 설치 패키지 목록의 빈 영역을 마우스 오른쪽 버튼으로 클릭한 다음 마우스 오른쪽 메뉴에서 **생성 → 설치 패키지**를 선택합니다.
   - 설치 패키지 목록 관리 섹션에 있는 **설치 패키지 생성**을 누릅니다.

   새 패키지 마법사가 시작됩니다.
4. 해당 아이콘을 클릭하여 다음 설치 패키지 유형 중 하나를 선택합니다:
   - Kaspersky 애플리케이션용 설치 패키지.
   - 지정된 실행 파일용 설치 패키지.
   - Kaspersky 데이터베이스의 애플리케이션용 설치 패키지.
5. 생성할 설치 패키지의 이름을 지정합니다.
   원하는 이름을 지정할 수 있습니다.
6. 다음 방법 중 하나로 설치 패키지를 생성할 애플리케이션이나 실행 파일을 선택합니다:
   - **찾아보기** 버튼을 클릭하고 표준 Windows **열기** 창에서 사용 가능한 디스크에 있는 필요한 애플리케이션의 배포 패키지를 선택합니다.
     이 옵션은 Kaspersky 애플리케이션이나 지정한 실행 파일용 설치 패키지 생성을 선택했을 때 적용할 수 있습니다.

- **찾아보기** 버튼을 누르고 **애플리케이션 선택** 창에서 필요한 애플리케이션의 배포 패키지를 선택합니다.

  이 옵션은 Kaspersky 데이터베이스의 애플리케이션용 설치 패키지 생성을 선택했을 때 적용됩니다.

중앙 관리 서버용 설치 패키지를 만들려면 sc.kud 파일을 선택합니다. sc.kud 파일은 Kaspersky Security Center 배포 패키지의 루트 폴더에 있습니다.

설치 패키지 파라미터에서 권한 있는 사용자 계정의 세부정보를 입력하지 마십시오.

7. 최종 사용자 라이센스 계약서와 개인 정보 취급 방침을 읽어 보십시오.

   애플리케이션 설치 패키지 생성 시, 해당 애플리케이션의 최종 사용자 라이센스 계약서 및 개인정보 취급방침을 확인하고 동의하라는 메시지가 표시될 수 있습니다.

   두 문서를 모두 읽어 보십시오. 라이센스 계약서 및 개인 정보 취급 방침의 모든 조건에 동의한다면, 해당 확인란을 선택하여 수락하십시오.

   기기에 애플리케이션이 계속 설치되고 설치 패키지 생성이 다시 시작됩니다.

   Kaspersky Endpoint Security for Mac용 설치 패키지를 만들 때는 라이센스 계약서 및 개인 정보 취급 방침의 언어를 선택할 수 있습니다.

8. 필요하다면 시스템 구성 요소의 자동 설치를 활성화합니다.

   Kaspersky 데이터베이스의 애플리케이션용 설치 패키지를 생성할 때는 필요한 시스템 구성 요소의 자동 설치를 활성화할 수 있습니다. 새 패키지 마법사가 선택한 애플리케이션에 대해 사용 가능한 시스템 구성 요소 목록을 표시합니다. 설치 패키지 속성에서 언제든지 이 목록을 확인할 수 있습니다.

   패치 설치 패키지를 생성한다면 이 패치 배포에 필요한 모든 시스템 구성 요소가 목록에 포함됩니다.

9. **마침** 버튼을 눌러 패키지 생성 프로세스를 완료합니다.

새 패키지 마법사가 완료되면 콘솔 트리에서 **설치 패키지** 폴더의 작업 영역에 새 설치 패키지가 표시됩니다.

독립 실행형 설치 패키지 만들기

조직의 사용자와 기기 사용자는 독립 실행형 설치 패키지를 사용하여 기기에 수동으로 애플리케이션을 설치할 수 있습니다.

독립 실행형 설치 패키지는 웹 서버 또는 공유 폴더에 저장하거나 다른 방법으로 클라이언트 기기에 전송할 수 있는 실행 파일(installer.exe)입니다. 독립 실행형 설치 패키지에 대한 링크를 이메일로 전송해도 됩니다. 사용자는 클라이언트 기기에서 Kaspersky Security Center의 관여 없이 수신된 파일을 로컬로 실행하여 애플리케이션을 설치할 수 있습니다.

허가 받지 않은 사람은 독립 실행형 설치 패키지를 사용할 수 없도록 하십시오.

Kaspersky 애플리케이션 및 Windows, macOS, Linux 플랫폼을 위한 타사 애플리케이션의 독립 실행형 설치 패키지를 생성할 수 있습니다. 타사 애플리케이션에 대한 독립 실행형 설치 패키지를 생성하려면 먼저 사용자 지정 설치 패키지를 생성해야 합니다.

독립 실행형 설치 패키지를 생성하는 데 사용되는 소스는 중앙 관리 서버에서 만든 목록에 있는 설치 패키지입니다.

독립 실행형 설치 패키지를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **중앙 관리 서버 → 고급 → 원격 설치 → 설치 패키지**를 선택합니다.

   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.

2. 설치 패키지 목록에서 독립 실행형 패키지를 만들 설치 패키지를 선택합니다.

3. 마우스 오른쪽 메뉴에서 **독립 실행형 설치 패키지 생성**을 선택합니다.

   독립 실행형 설치 패키지 만들기 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

4. 마법사의 첫 번째 페이지에서 Kaspersky 애플리케이션용 설치 패키지를 선택했고, 선택한 애플리케이션과 함께 네트워크 에이전트를 설치하려는 경우에는 **이 애플리케이션과 함께 네트워크 에이전트 설치** 옵션이 활성화됩니다.

   기본적으로 이 옵션은 켜져 있습니다. 기기의 네트워크 에이전트 설치 여부가 확실하지 않은 경우 이 옵션을 활성화하는 것이 좋습니다. 기기에 네트워크 에이전트가 이미 설치되어 있는 경우 네트워크 에이전트가 포함된 독립 실행형 설치 패키지를 설치하면 네트워크 에이전트가 최신 버전으로 업데이트됩니다.

   이 옵션을 비활성화하면 네트워크 에이전트가 기기에 설치되지 않고 기기가 관리되지 않습니다.

   선택한 애플리케이션에 대한 독립 실행형 설치 패키지가 중앙 관리 서버에 이미 존재한다면 마법사가 이를 알려줍니다. 이 경우 다음 작업 중 하나를 선택해야 합니다:

   - **독립 실행형 설치 패키지 생성**. 예를 들어, 새 애플리케이션 버전에 대한 독립 실행형 설치 패키지를 만들고자 하면서 이전 애플리케이션 버전에 대해 만든 독립 실행형 설치 패키지는 유지하려는 경우 이 옵션을 선택하십시오. 새로운 독립 실행형 설치 패키지는 다른 폴더에 있습니다.

   - **기존 독립 실행형 설치 패키지 사용**. 기존 독립 실행형 설치 패키지를 사용하려면 이 옵션을 선택합니다. 패키지 생성 프로세스가 시작되지 않습니다.

   - **기존의 독립 실행형 설치 패키지 다시 생성**. 동일한 애플리케이션에 대한 독립 실행형 설치 패키지를 다시 만들려면 이 옵션을 선택합니다. 독립 실행형 설치 패키지는 동일한 폴더에 있습니다.

5. 마법사의 다음 페이지에서 **미할당 기기를 이 관리 그룹으로 이동** 옵션을 선택하고 네트워크 에이전트 설치 후 클라이언트 기기를 이동할 관리 그룹을 지정합니다.

   기본적으로 기기는 **관리 중인 기기** 그룹으로 이동합니다.

   네트워크 에이전트 설치 후 클라이언트 기기를 관리 그룹으로 이동하지 않으려면 **기기를 이동하지 않음** 옵션을 선택합니다.

6. 마법사의 다음 페이지에서 독립 실행형 설치 패키지 생성 프로세스가 완료되면 독립 실행형 패키지 생성 결과 및 독립 실행형 패키지에 대한 경로가 표시됩니다.

   링크를 클릭하고 다음 중 하나를 수행할 수 있습니다:

   - 독립 실행형 설치 패키지가 있는 폴더를 엽니다.

   - 생성된 독립 실행형 설치 패키지에 대한 링크를 이메일로 전송합니다. 이 작업을 수행하려면 실행된 이메일 애플리케이션이 있어야 합니다.

   - 웹사이트에 링크를 게시하기 위한 HTML 코드를 샘플링합니다. TXT 파일이 생성되고 TXT 형식과 연결된 애플리케이션에서 열립니다. 이 파일에서 속성이 있는 HTML <a> 태그가 표시됩니다.

7. 마법사의 다음 페이지에서 독립 실행형 설치 패키지의 목록을 열려면 **독립 실행형 패키지 목록 열기** 옵션을 활성화합니다.

8. **마침** 버튼을 누릅니다.

   독립 실행형 설치 패키지 생성 마법사가 닫힙니다.

독립 실행형 설치 패키지가 만들어지고 중앙 관리 서버 공유 폴더의 PkgInst 하위 폴더에 배치됩니다. 설치 패키지 목록 위에 있는 **독립 실행형 패키지 목록 보기** 버튼을 눌러 독립 실행형 패키지의 목록을 볼 수 있습니다.

사용자 지정 설치 패키지 만들기

사용자 지정 설치 패키지를 사용하여 다음을 수행할 수 있습니다:

- 작업을 이용하는 방법 등으로 클라이언트 기기에 애플리케이션(예: 텍스트 편집기)을 설치합니다.
- 독립 실행형 설치 패키지를 만듭니다.

사용자 지정 설치 패키지는 일련의 파일이 있는 폴더입니다. 사용자 지정 설치 패키지 생성에 사용하는 소스는 *아카이브 파일*입니다. 아카이브 파일에는 사용자 지정 설치 패키지에 포함해야 하는 파일이 있습니다. 사용자 지정 설치 패키지를 만들면 명령줄 파라미터를 지정하여 숨김 모드로 애플리케이션을 설치하는 작업 등을 수행할 수 있습니다.

사용자 지정 설치 패키지를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **중앙 관리 서버 → 고급 → 원격 설치 → 설치 패키지**를 선택합니다.

   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.

2. 설치 패키지 목록 위에서 **설치 패키지 생성** 버튼을 누릅니다.

   새 패키지 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

3. 마법사의 첫 페이지에서 **지정한 실행 파일에 대한 설치 패키지를 생성합니다**을 선택합니다.

4. 마법사의 다음 페이지에서 사용자 지정 설치 패키지 이름을 지정합니다.

5. 마법사의 다음 페이지에서 **찾기** 버튼을 누르고 표준 Windows **열기** 창에서 사용 가능한 디스크에 있는 아카이브 파일을 선택하여 사용자 지정 설치 패키지를 만듭니다.

   ZIP, CAB, TAR 또는 TAR.GZ 아카이브를 업로드할 수 있습니다. SFX(자동 압축 풀림 아카이브) 파일에서는 설치 패키지를 만들 수 없습니다.

   파일은 Kaspersky Security Center 중앙 관리 서버로 다운로드됩니다.

6. 마법사의 다음 페이지에서 실행 파일의 명령줄 파라미터를 지정합니다.

   명령줄 파라미터를 지정하여 설치 패키지에서 애플리케이션을 숨김 모드로 설치할 수 있습니다. 명령줄 파라미터 지정은 선택 사항입니다.

   원하는 경우 다음 옵션을 구성하십시오.

   - **전체 폴더를 설치 패키지로 복사**

     실행 파일과 애플리케이션 설치에 필요한 추가 파일이 함께 있는 경우 이 옵션을 선택합니다. 이 옵션을 실행하기 전에 필요한 모든 파일이 동일한 폴더에 저장되어 있는지 확인합니다. 이 옵션을 실행하면 애플리케이션은 지정된 실행 파일을 포함하여 폴더의 전체 내용을 설치 패키지에 추가합니다.

- **Kaspersky Security Center에서 인식할 수 있는 권장 값을 사용해 애플리케이션 설정 변환**

  지정한 애플리케이션에 대한 정보가 Kaspersky 데이터베이스에 있는 경우 권장 설정으로 애플리케이션이 설치됩니다.

  실행 파일 명령줄 필드에 파라미터를 입력한 경우 권장 설정으로 다시 작성됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

  Kaspersky 데이터베이스는 Kaspersky 분석가에 의해 생성 및 유지 관리됩니다. 데이터베이스에 추가된 각 애플리케이션에 대해 Kaspersky 분석가는 최적의 설치 설정을 정의합니다. 클라이언트 기기에 애플리케이션을 원격으로 설치하기 위한 설정이 정의됩니다. 중앙 관리 서버 저장소 업데이트 다운로드 작업을 실행하면 데이터베이스가 자동으로 중앙 관리 서버에 업데이트됩니다.

사용자 지정 설치 패키지 생성 프로세스가 시작됩니다.

프로세스가 완료되면 마법사가 알려줍니다.

사용자 지정 설치 패키지가 만들어지지 않으면 적절한 메시지가 표시됩니다.

7. **마침** 버튼을 눌러 마법사를 닫습니다.

생성한 설치 패키지가 중앙 관리 서버 공유 폴더의 Packages 하위 폴더로 다운로드됩니다. 다운로드 후에 사용자 지정 설치 패키지가 설치 패키지 목록에 나타납니다.

중앙 관리 서버의 설치 패키지 목록에서 사용자 지정 설치 패키지 속성을 보고 편집할 수 있습니다.

사용자 지정 설치 패키지의 속성 확인 및 편집

사용자 지정 설치 패키지를 생성한 후에는 설치 패키지의 일반 정보를 보고, 속성 창에서 설치 설정을 지정할 수 있습니다.

사용자 지정 설치 패키지의 속성을 확인하고 편집하려면 다음 단계를 따르십시오.

1. 콘솔 트리에서 **중앙 관리 서버 → 고급 → 원격 설치 → 설치 패키지**를 선택합니다.
   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.
2. 설치 패키지의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   선택한 설치 패키지의 속성 창이 열립니다.
3. 다음 정보를 확인할 수 있습니다.
   - 설치 패키지 이름
   - 사용자 지정 설치 패키지에 포함된 애플리케이션 이름
   - 애플리케이션 버전
   - 설치 패키지를 만든 날짜
   - 중앙 관리 서버에서 사용자 지정 설치 패키지의 경로
   - 실행 파일 명령줄

4. 다음 설정을 지정합니다:

   - 설치 패키지 이름
   - **필요한 일반 시스템 구성 요소 설치**

     이 옵션을 활성화하면 업데이트를 설치하기 전에 애플리케이션은 업데이트 설치를 설치하기 위해 필요한 모든 일반 시스템 구성 요소(선결 조건)를 자동으로 설치합니다. 이러한 필수 구성 요소의 예로는 운영 체제 업데이트 등이 있습니다.

     이 옵션을 비활성화하는 경우에는 필수 구성 요소를 수동으로 설치해야 합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

     이 옵션은 설치 패키지에 추가된 애플리케이션을 Kaspersky Security Center에서 인식한 경우에만 사용할 수 있습니다.

   - **실행 파일 명령줄**

     애플리케이션에 숨김 설치를 위한 추가 파라미터가 필요한 경우 이 필드에 관련 파라미터를 지정합니다. 자세한 내용은 공급업체 설명서를 참조하십시오.

     다른 파라미터를 입력할 수도 있습니다.

     이 옵션은 Kaspersky 애플리케이션을 기반으로 생성되지 않은 패키지에만 사용할 수 있습니다.

5. **확인** 또는 **적용** 버튼을 클릭하여 변경 사항(있는 경우)을 저장합니다.

   새 설정이 저장됩니다.

Kaspersky Security Center 배포 키트에서 네트워크 에이전트 설치 패키지 받기

Kaspersky Security Center를 설치할 필요 없이 Kaspersky Security Center 배포 키트에서 네트워크 에이전트 설치 패키지를 받을 수 있습니다. 그런 다음 설치 패키지를 사용하여 클라이언트 기기에 네트워크 에이전트를 설치할 수 있습니다.

Kaspersky Security Center 배포 키트에서 네트워크 에이전트 설치 패키지를 얻으려면:

1. Kaspersky Security Center 배포 키트에서 ksc_<version number>.<build number>_full_<localization language>.exe 실행 파일을 실행합니다.
2. 창이 열리면 **설치 패키지 추출** 링크를 누릅니다.
3. 설치 패키지 목록에서 네트워크 에이전트 설치 패키지 옆의 확인란을 선택한 다음 **다음** 버튼을 누릅니다.
4. 필요한 경우 **찾기** 버튼을 눌러 설치 패키지를 추출할 위치로 표시된 폴더를 변경합니다.

5. **추출** 버튼을 누릅니다.
   애플리케이션이 네트워크 에이전트 설치 패키지를 추출합니다.

6. 프로세스가 완료되면 **닫기** 버튼을 누릅니다.

선택한 폴더에 네트워크 에이전트 설치 패키지를 추출합니다.

설치 패키지를 사용하여 다음 방법 중 하나로 네트워크 에이전트를 설치할 수 있습니다.

- 추출한 폴더의 setup.exe 파일을 실행하여 로컬로 설치
- 자동 설치를 통해 설치
- Microsoft Windows의 그룹 정책 사용

보조 중앙 관리 서버에 설치 패키지 배포

보조 중앙 관리 서버에 설치 패키지를 배포하려면:

1. 관련 보조 중앙 관리 서버를 제어하는 중앙 관리 서버에 연결합니다.
2. 다음 방법 중 하나로 보조 중앙 관리 서버에 설치 패키지 배포 작업을 만듭니다:
   - 선택한 관리 그룹에 보조 중앙 관리 서버를 만들려면 이 그룹에 대한 그룹 작업 만들기를 실행합니다.
   - 특정 보조 중앙 관리 서버에 대한 작업을 만들려면 특정 기기에 대한 작업 만들기를 실행합니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

   Kaspersky Security Center 중앙 관리 서버 노드에 있는 새 작업 마법사의 **작업 유형 선택** 창에서 **고급** 폴더에서 작업 유형으로 **설치 패키지 배포**를 선택합니다.

   새 작업 마법사가 특정 보조 중앙 관리 서버에 대한 선택한 설치 패키지 배포 작업을 만듭니다.
3. 이 작업을 직접 실행하거나 작업 설정에 지정된 스케줄에 따라 실행될 때까지 기다립니다.

선택한 설치 패키지가 특정 보조 중앙 관리 서버로 복사됩니다.

배포 지점을 통해 설치 패키지 배포

배포 지점을 사용하여 관리 그룹 내에 설치 패키지를 배포할 수 있습니다.

중앙 관리 서버에서 설치 패키지를 받았으면, 배포 지점은 자동으로 IP 멀티캐스팅을 통해 이를 각 클라이언트 기기에 배포합니다. 관리 그룹 내에서 새 설치 패키지의 IP 멀티캐스팅은 한 번 수행됩니다. 배포 시 클라이언트 기기와 기기 네트워크의 연결이 끊어졌을 경우 해당 클라이언트 기기에 설치된 네트워크 에이전트는 설치 작업이 시작될 때 배포 지점에서 관련 설치 패키지를 자동으로 다운로드합니다.

Kaspersky Security Center에 애플리케이션 설치 결과 전송

애플리케이션 설치 패키지를 만든 후에는 애플리케이션 설치 결과에 대한 모든 진단 정보가 Kaspersky Security Center로 전송되도록 구성할 수 있습니다. Kaspersky 애플리케이션 설치 패키지의 경우 애플리케이션 설치 결과에 대한 진단 정보 전송이 기본적으로 구성되어 있으며 별도의 구성이 필요 없습니다.

Kaspersky Security Center에 애플리케이션을 설치한 결과에 대한 진단 정보 전송을 구성하려면 다음과 같이 하십시오:

1. 선택한 애플리케이션에 대해 Kaspersky Security Center를 사용하여 생성된 설치 패키지의 폴더로 이동합니다. 이 폴더는 Kaspersky Security Center 설치를 진행하는 동안 지정한 공유 폴더에서 찾을 수 있습니다.

2. 확장자가 .kpd 또는 .kud인 파일을 편집용 프로그램(예: Microsoft Windows 메모장 사용)으로 엽니다.

   이 파일은 일반 구성 .ini 파일 형식입니다.

3. 이 파일에 다음 행을 추가합니다:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   이 명령은 설치 패키지가 생성된 애플리케이션의 설치가 완료될 때까지 Kaspersky Security Center가 대기했다가 설치 프로그램 반환 코드를 분석하도록 구성합니다. 진단 데이터 전송을 비활성해야 하는 경우 Wait 키의 값을 0으로 설정합니다.

4. 설치 성공 시의 반환 코드에 대한 설명을 추가합니다. 이렇게 하려면 이 파일에 다음 행을 추가합니다:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   …
   ```

   > 대괄호는 옵션 키가 포함됩니다.

   행 구문:

   - `<return code>`. 설치 프로그램 반환 코드에 해당하는 숫자입니다. 반환 코드는 임의의 숫자일 수 있습니다.
   - `<description>`. 설치 결과의 텍스트 설명입니다. 설명은 생략할 수 있습니다.

5. 설치 실패 시의 반환 코드에 대한 설명을 추가합니다. 이렇게 하려면 이 파일에 다음 행을 추가합니다:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   …
   ```

   이러한 행의 구문은 설치 성공 시의 반환 코드에 포함된 행의 구문과 동일합니다.

6. 모든 변경 사항을 저장하여 .kpd 또는 .kud 파일을 닫습니다.

그러면 사용자 정의 애플리케이션의 설치 결과에 관한 정보가 Kaspersky Security Center 로그에 등록되고 리포트 및 작업 로그의 이벤트 목록에 표시됩니다.

설치 패키지에 대한 KSN 프록시 서버 주소 정의

중앙 관리 서버의 주소 또는 도메인 변경 시, 설치 패키지에 대한 KSN 프록시 서버 주소를 정의할 수 있습니다.

설치 패키지에 대한 KSN 프록시 서버 주소를 정의하려면:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
2. 메뉴가 열리면 **속성**을 선택합니다.
3. 속성 창이 열리면 **일반** 하위 섹션을 선택합니다.
4. 속성 창의 **일반** 하위 섹션에서 KSN 프록시 서버의 주소를 입력합니다.

설치 패키지가 이 주소를 기본값으로 사용합니다.

최신 버전의 애플리케이션 가져오기

Kaspersky Security Center를 이용하면 Kaspersky 서버에 저장된 최신 버전의 회사 애플리케이션을 받을 수 있습니다.

Kaspersky 회서 애플리케이션의 최신 버전을 받으려면 다음과 같이 하십시오:

1. 다음 중 하나를 수행합니다:
   - 콘솔 트리에서 필요한 중앙 관리 서버의 이름으로 되어 있는 노드를 선택하고, **모니터링** 탭이 선택되어 있는지 확인한 다음, **배포** 섹션에서 **새로운 버전의 Kaspersky 애플리케이션이 있습니다** 링크를 클릭합니다.

     중앙 관리 서버가 Kaspersky 서버에서 새 버전의 회사 애플리케이션을 찾은 경우 **새로운 버전의 Kaspersky 애플리케이션이 있습니다** 링크가 표시됩니다.

   - 콘솔 트리에서 **고급 → 원격 설치 → 설치 패키지**를 선택하고, 작업 영역에서 **추가 조치**를 선택한 후 드롭다운 목록에서 **최신 Kaspersky 제품 버전 확인**을 선택합니다.

   최신 버전의 Kaspersky 애플리케이션 목록이 표시됩니다.
2. Kaspersky 애플리케이션 목록을 필터링하여 필요한 애플리케이션 검색을 단순화할 수 있습니다.

   현재 애플리케이션 버전 창 상단에서 **필터** 링크를 클릭하여 다음 기준에 따라 애플리케이션 목록을 필터링합니다:
   - **구성 요소**. 이 기준을 사용하여 네트워크에서 사용 중인 보호 영역별로 Kaspersky 애플리케이션 목록을 필터링합니다.
   - **다운로드되는 소프트웨어 유형**. 이 기준을 사용하여 애플리케이션 유형별로 Kaspersky 애플리케이션 목록을 필터링합니다.
   - **표시할 소프트웨어 제품 및 업데이트**. 특정 버전별로 사용 가능한 Kaspersky 애플리케이션을 표시하려면 이 기준을 사용하십시오.
   - **소프트웨어 및 업데이트에 대한 언어**. 특정 현지화 언어로 Kaspersky 애플리케이션을 표시하려면 이 기준을 사용하십시오.

   적용 버튼을 클릭하여 선택한 필터를 적용합니다.
3. 목록에서 필요한 애플리케이션을 선택합니다.

4. **배포 패키지 웹 주소** 문자열의 링크를 눌러 애플리케이션 배포 패키지를 다운로드합니다.

관리 중인 애플리케이션을 업데이트하려면 Kaspersky Security Center의 특정 최소 버전을 설치해야 할 수 있습니다. 이 버전이 현재 버전보다 최신 버전이면 이러한 업데이트가 표시되지만 승인할 수는 없습니다. 또한 Kaspersky Security Center를 업그레이드할 때까지 이러한 업데이트에서 설치 패키지를 생성 할 수 없습니다. Kaspersky Security Center 인스턴스를 필요한 최소 버전으로 업그레이드하라는 메시지가 표시됩니다.

선택한 애플리케이션에 대해 **애플리케이션을 다운로드하고 설치 패키지 생성** 버튼이 표시될 경우 이 버튼을 클릭하여 애플리케이션 배포 패키지를 다운로드하고 자동으로 설치 패키지를 만들 수 있습니다. Kaspersky Security Center는 애플리케이션 배포 패키지를 Kaspersky Security Center를 설치할 때 지정한 중앙 관리 서버의 공유 폴더로 로드합니다. 자동으로 만들어지는 설치 패키지는 콘솔 트리의 **원격 설치** 폴더에 있는 **설치 패키지** 하위 폴더에 표시됩니다.

현재 애플리케이션 버전 창이 닫힌 후 **배포** 섹션에서 **새로운 버전의 Kaspersky 애플리케이션이 있습니다** 링크가 사라집니다.

새 버전의 애플리케이션에 대한 설치 패키지를 만들고 콘솔 트리의 **원격 설치** 폴더에 있는 **설치 패키지** 하위 폴더에서 새로 만든 설치 패키지를 관리할 수 있습니다.

또한 **설치 패키지** 폴더의 작업 영역에 있는 **최신 Kaspersky 제품 버전 확인** 링크를 누르면 **현재 애플리케이션 버전** 창을 열 수 있습니다.

Windows 기기에서 원격 설치 준비

클라이언트 기기에 애플리케이션을 원격으로 설치하는 작업이 다음과 같은 이유로 오류를 반환할 수 있습니다:

- 작업이 이미 이 기기에 성공적으로 수행되었습니다.
  이 경우 이 작업을 다시 수행할 필요가 없습니다.
- 작업이 시작되었을 때 기기가 종료된 상태였습니다.
  이 때는 기기를 켜면 작업이 다시 시작됩니다.
- 클라이언트 기기에 설치된 네트워크 에이전트와 중앙 관리 서버가 서로 연결되지 않았습니다.
  문제의 원인을 파악하려면 클라이언트 기기의 원격 진단용으로 설계된 유틸리티(klactgui)를 사용하십시오.
- 기기에 네트워크 에이전트가 설치되어 있지 않으면 원격 설치 시 다음과 같은 문제가 발생할 수 있습니다.
  - 클라이언트 기기가 **단순 파일 공유 해제**를 사용하도록 설정되었습니다.
  - 서버 서비스가 클라이언트 기기에서 실행되고 있지 않습니다.
  - 필요한 포트가 클라이언트 기기에서 닫혀 있습니다.
  - 이 작업을 수행하는 데 사용된 계정에 충분한 권한이 없습니다.

네트워크 에이전트를 설치하지 않은 클라이언트 기기에 애플리케이션 설치 시 문제 발생을 방지하려면 Kaspersky Security Center의 원격 설치 작업을 통한 강제 배포에 설명된 대로 설치를 진행해야 합니다.

이전에는 기기에서 원격 설치를 준비할 때 riprep 유틸리티를 사용했었습니다. 이 운영 체제 구성 방법은 이제 잘 사용하지 않습니다. Windows XP 및 Windows Server 2003 R2 이상의 운영 체제에서는 riprep 유틸리티를 사용하지 않는 것이 좋습니다.

Linux 기기 준비 및 Linux 기기에 네트워크 에이전트 원격 설치

네트워크 에이전트 설치는 두 단계로 구성됩니다.

- Linux 기기 준비
- 네트워크 에이전트 원격 설치

Linux 기기 준비

네트워크 에이전트 원격 설치를 위한 Linux 기기를 준비하려면 다음과 같이 하십시오:

1. Linux용 네트워크 에이전트를 설치할 기기에서 지원되는 Linux 배포판 중 하나를 실행하는지 확인합니다.
2. 애플리케이션 인터페이스를 사용하거나 Kaspersky 웹사이트에서 네트워크 에이전트 설치 패키지를 다운로드합니다.
3. 대상 Linux 기기에 다음 소프트웨어가 설치되어 있는지 확인합니다:
   - Sudo(Ubuntu 10.04는 Sudo 버전 1.7.2p1 이상)
   - Perl 언어 인터프리터 버전 5.10 이상
   - ps 유틸리티
4. 기기 구성을 테스트합니다:
   a. PuTTY 등의 SSH 클라이언트를 통해 기기에 연결할 수 있는지 확인합니다.
      기기에 연결할 수 없는 경우 `/etc/ssh/sshd_config` 파일을 열고 다음 설정이 아래에 나와 있는 개별 값으로 지정되어 있는지 확인합니다:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      기기 연결에 문제가 없다면 /etc/ssh/sshd_config 파일을 수정하지 마십시오. 수정하면, 원격 설치 작업 실행 시 SSH 인증 실패가 발생할 수 있습니다.

      필요한 경우 파일을 저장하고 `sudo service ssh restart` 명령을 사용하여 SSH 서비스를 다시 시작합니다.

   b. Linux 기반 미할당 기기에서 TCP 포트 22가 열려 있고 접근 가능한지 확인합니다. Linux용 네트워크 에이전트를 성공적으로 설치하려면 TCP 포트 22를 사용할 수 있어야 합니다.

c. 기기를 연결하는 데 사용할 사용자 계정의 sudo 암호를 사용하지 않도록 설정합니다.

d. sudo에서 `visudo` 명령을 사용하여 sudoers 구성 파일을 엽니다.

연 파일 끝에 다음 줄을 추가합니다: <사용자 이름> `ALL = (ALL) NOPASSWD: ALL`. 이때, < 사용자 이름 >은 사용자 계정이며, SSH를 통해 해당 기기에 연결할 때 사용합니다. Astra Linux 운영 체제를 사용한다면 /etc/sudoers 파일에서 마지막 줄에 `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`을 추가합니다

e. sudoers를 저장하고 닫습니다.

f. SSH를 통해 기기에 다시 연결하여 Sudo 서비스가 암호 입력 메시지를 표시하지 않는 것을 확인합니다. 이 작업은 `sudo whoami` 명령으로 수행할 수 있습니다.

5. `/etc/systemd/logind.conf` 파일을 열고 다음 중 하나를 수행합니다.

- '아니요'를 KillUserProcesses 설정 값으로 지정합니다. `KillUserProcesses=no`.
- KillExcludeUsers 설정에 대해 원격 설치를 수행할 계정의 사용자 이름(예: `KillExcludeUsers=root`)을 입력합니다.

대상 기기가 Astra Linux를 실행 중이라면 `/home/`< 사용자 이름 >`/.bashrc export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` 문자열을 추가합니다. 여기서 < 사용자 이름 >은 SSH를 사용하는 기기 연결에 사용할 사용자 계정입니다.

변경된 설정을 적용하려면 Linux 기기를 다시 시작하거나 다음 명령을 실행합니다.

```
sudo systemctl restart systemd-logind.service
```

6. SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면 insserv-compat 패키지를 먼저 설치 해서 네트워크 에이전트를 구성합니다.

7. 폐쇄형 소프트웨어 환경 모드에서 실행되는 Astra Linux 운영체제가 있는 기기에 네트워크 에이전트를 설치하려면 추가 단계를 수행하여 Astra Linux 기기를 준비합니다.

8. 운영 체제 RED OS 7.3.4 이상이나 MSVSPHERE 9.2 이상을 사용하는 기기에 네트워크 에이전트를 설치한다면, 중앙 관리 서버가 올바르게 작동하려면 libxcrypt-compat 패키지를 설치해야 합니다.

네트워크 에이전트 원격 설치

Linux 기기에 네트워크 에이전트를 원격 설치하려면:

1. 설치 패키지를 다운로드하고 만듭니다:

a. 기기에 패키지를 설치하기 전에 이 패키지에 대한 모든 종속성(프로그램 및 라이브러리)이 설치되어 있는지 확인하십시오.

해당 패키지가 설치될 Linux 배포판에 대한 특정한 유틸리티를 사용하여 스스로 각 패키지의 종속성을 직접 볼 수 있습니다. 유틸리티에 대한 자세한 내용은 사용자의 운영 체제 설명서를 참조하십시오.

b. 원격 설치 패키지를 만들려면 다음 파일을 사용하십시오:

- klnagent.kpd
- akinstall.sh
- 네트워크 에이전트의 .deb 또는 .rpm 패키지

2. 다음 설정을 사용하여 원격 설치 작업을 생성합니다.

   - 새 작업 마법사의 **설정** 페이지에서 **중앙 관리 서버를 통해 운영 체제 리소스 사용** 확인란을 선택합니다. 다른 확인란은 모두 선택을 취소합니다.
   - **작업을 실행할 계정 선택** 페이지에서 SSH를 통한 기기 연결에 사용할 사용자 계정의 설정을 지정합니다.

3. 원격 설치 작업을 실행합니다. `su` 명령에 대한 옵션을 사용하여 환경을 보존합니다: `-m, -p, --preserve-environment`.

네트워크 에이전트 설치를 위해 SUSE Linux Enterprise Server 15를 실행하는 기기 준비

SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면

네트워크 에이전트를 설치하기 전에 다음 명령을 실행합니다.

```
sudo zypper install insserv-compat
```

이렇게 하면 insserv-compat 패키지를 설치하고 네트워크 에이전트를 적절하게 구성할 수 있습니다.

`rpm -q insserv-compat` 명령을 실행하여 패키지가 이미 설치되어 있는지 확인합니다.

네트워크에 SUSE Linux Enterprise Server 15를 실행하는 기기가 많이 포함되어 있는 경우 회사 인프라를 구성 및 관리하기 위한 특수 소프트웨어를 사용할 수 있습니다. 이 소프트웨어를 사용하면 필요한 모든 기기에 insserv-compat 패키지를 한 번에 자동으로 설치할 수 있습니다. 예를 들어 Puppet, Ansible, Chef를 사용하거나 직접 스크립트를 만드는 등 편리한 방법을 사용하면 됩니다.

기기에 SUSE Linux Enterprise용 GPG 서명 키가 없으면 다음 경고가 나타날 수 있습니다: `Package header is not signed!` 경고를 무시하려면 `i` 옵션을 선택합니다.

insserv-compat 패키지 설치 외에 Linux 기기가 완전히 준비되었는지 확인하십시오. 이후, 네트워크 에이전트를 배포 및 설치합니다.

네트워크 에이전트 원격 설치를 위한 macOS 기기 준비

네트워크 에이전트 원격 설치를 위한 macOS 기기를 준비하려면 다음과 같이 하십시오:

1. 대상 macOS 기기에 sudo가 설치되어 있는지 확인합니다.
2. 기기 구성을 테스트합니다:

   a. 클라이언트 기기에서 포트 22가 열려 있는지 확인합니다. 이렇게 하려면 **시스템 환경설정**에서 **공유** 패널을 연 다음 **원격 로그인** 확인란이 선택되어 있는지 확인합니다.

   포트 22를 통해서만 SSH(Secure Shell)를 통해 클라이언트 기기에 연결할 수 있습니다. 포트 번호는 변경할 수 없습니다.

   `ssh <기기_이름>` 명령을 사용하여 macOS 기기에 원격으로 로그인할 수 있습니다. **공유** 창에서 **액세스 허용 대상** 옵션을 사용하여 macOS 기기에 액세스가 허용되는 사용자의 범위를 설정할 수 있습니다.

b. 기기를 연결하는 데 사용할 사용자 계정의 sudo 암호를 사용하지 않도록 설정합니다.

터미널에서 `sudo visudo` 명령을 사용하여 sudoers 구성 파일을 엽니다. 연 파일의 사용자 권한 사양 항목에서 다음을 지정합니다. `username ALL = (ALL) NOPASSWD: ALL`. 이때 `username`은 사용자 계정을 나타내며, SSH를 사용한 기기 연결에 사용됩니다.

c. sudoers를 저장하고 닫습니다.

d. SSH를 통해 기기에 다시 연결하여 Sudo 서비스에서 암호를 입력하라는 메시지가 표시되지 않음을 확인합니다. 이는 `sudo whoami` 명령으로 수행할 수 있습니다.

3. 설치 패키지를 다운로드하고 만듭니다:

a. 다음 방법 중 하나를 사용하여 네트워크 에이전트 설치 패키지를 다운로드합니다.

- 콘솔 트리의 **원격 설치 → 설치 패키지**에서 컨텍스트 메뉴를 열고 **현재 애플리케이션 버전 표시**을 선택하여 사용 가능한 패키지 중 선택합니다.
- 기술 지원 웹사이트(https://support.kaspersky.com/)에서 관련 네트워크 에이전트 버전을 다운로드합니다.
- 기술 지원 전문가로부터 설치 패키지를 요청합니다.

b. 원격 설치 패키지를 만들려면 다음 파일을 사용하십시오:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. 다음 설정을 사용하여 원격 설치 작업을 만듭니다:

- 새 작업 마법사의 **설정** 페이지에서 **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드** 확인란을 선택합니다. 다른 확인란은 모두 선택을 취소합니다.
- **작업을 실행할 계정 선택** 페이지에서 SSH를 통한 기기 연결에 사용할 사용자 계정의 설정을 지정합니다.

클라이언트 기기는 생성된 관련 작업을 통해 네트워크 에이전트를 원격 설치할 준비가 됩니다.

Kaspersky 애플리케이션: 라이센싱 및 활성화

이 섹션에서는 관리 중인 Kaspersky 애플리케이션의 라이센스 키 처리와 관련된 Kaspersky Security Center의 기능에 대해 설명합니다.

Kaspersky Security Center에서는 중앙 집중식으로 클라이언트 기기에 Kaspersky 애플리케이션 라이센스 키를 배포하고 기기의 라이센스 키 사용을 감시하며 라이센스를 갱신할 수 있습니다.

Kaspersky Security Center를 사용하여 라이센스 키를 추가하는 경우, 라이센스 키 설정이 중앙 관리 서버에 저장됩니다. 이 정보를 기반으로 애플리케이션은 라이센스 키 사용에 관한 리포트를 생성하고 라이센스가 만료되거나 라이센스 키 속성에 의해 적용된 라이센스 제한을 초과하는 경우 관리자에게 이를 알립니다. 중앙 관리 서버 설정 내에서 라이센스 키 사용에 대한 알림을 구성할 수 있습니다.

관리 애플리케이션 라이센싱

관리 중인 기기에 설치된 Kaspersky 애플리케이션은 각 애플리케이션에 키 파일 또는 활성화코드를 적용하여 라이센스를 부여받아야 합니다. 키 파일 또는 활성화코드는 다음과 같은 방법으로 배포할 수 있습니다:

- 자동 배포
- 관리 중인 애플리케이션의 설치 패키지
- 관리 중인 애플리케이션에 대한 *라이센스 키 추가* 작업
- 관리 중인 애플리케이션의 수동 활성화

위에 방법 중 하나를 사용하여 새 활성 또는 예약 라이센스 키를 추가할 수 있습니다. Kaspersky 애플리케이션은 현재 활성 키를 사용하고 활성 키가 만료된 후 적용할 예약 키를 저장합니다. 라이센스 키를 추가할 애플리케이션이 키의 활성 또는 예약 여부를 정의합니다. 키 정의는 새 라이센스 키를 추가하는 방법에 따라 달라지지 않습니다.

자동 배포

다른 관리 중인 애플리케이션을 사용하고 있으며 특정 키 파일 또는 활성화코드를 그 기기에 배포해야 하는 경우 해당 활성화코드 또는 키 파일을 배포하는 다른 방법을 선택합니다.

Kaspersky Security Center를 사용하면 기기에 사용 가능한 라이센스 키를 자동으로 배포할 수 있습니다. 예를 들어 세 개의 라이센스 키가 중앙 관리 서버 저장소에 저장됩니다. 라이센스 키 세 개 모두에 대하여 **관리 중인 기기에 자동으로 라이센스 키 배포** 확인란을 선택하였습니다. 그리고, Kaspersky 보안 제품(예, Kaspersky Endpoint Security for Windows)이 기업의 기기에 설치됩니다. 라이센스 키를 배포해야 하는 새 기기가 발견됩니다. 애플리케이션은 적용 가능한 라이센스 키를 결정합니다. 저장소에 추가된 라이센스 키 중 두 개(이름이 *key_1*과 *key_2*인 키)의 라이센스 키가 해당 기기에 배포할 수 있습니다. 이러한 라이센스 키 중 하나가 기기에 배포됩니다. 이 경우, 라이센스 키 자동 배포는 관리자가 시작한 작업이 아니기 때문에 적용 가능한 두 라이센스 키 중 어느 라이센스 키가 기기에 배포될지 예측할 수 없습니다.

라이센스 키가 배포되면, 해당 기기는 그 라이센스 키가 적용된 기기로 카운터됩니다. 라이센스 키가 배포된 기기 수가 라이센스 제한을 초과하지 않는지 확인해야 합니다. 기기 수가 라이센스 제한을 초과하면, 해당 라이센스로 적용할 수 없는 모든 기기에 대해 *심각* 상태가 할당됩니다.

배포하기 전에 키 파일 또는 활성화코드를 중앙 관리 서버 저장소에 추가해야 합니다.

방법 지침:

- 관리 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 라이센스 키 자동 배포

  또는

- Kaspersky Security Center 웹 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 라이센스 키 자동 배포

다음 경우에는 자동 배포된 라이센스 키가 가상 중앙 관리 서버 저장소에 표시되지 않을 수 있습니다:

- 애플리케이션에 대한 라이센스 키가 유효하지 않습니다.
- 가상 중앙 관리 서버에 관리 중인 기기가 없습니다.
- 다른 가상 중앙 관리 서버에서 관리하는 기기에서 이미 해당 라이센스 키를 사용했으며 기기 수 제한에 도달했습니다.

관리 중인 애플리케이션의 설치 패키지에 키 파일 또는 활성화코드 추가

보안상의 이유로 이 옵션은 사용하지 않는 것이 좋습니다. 설치 패키지에 추가된 키 파일 또는 활성화코드에 문제가 생길 수 있습니다.

설치 패키지를 사용하여 관리 중인을 설치하는 경우 이 설치 패키지 또는 애플리케이션의 정책에서 활성화코드 또는 키 파일을 지정할 수 있습니다. 라이센스 키는 기기와 중앙 관리 서버를 다음에 동기화할 때 관리 중인 기기에 배포됩니다.

방법 지침:

- 관리 콘솔:
  - 설치 패키지 만들기
  - 클라이언트 기기에 애플리케이션 설치

  또는
- Kaspersky Security Center 웹 콘솔: 설치 패키지에 라이센스 키 추가

관리 중인 애플리케이션에 대해 라이센스 키 추가 작업을 실행하여 배포

만일 관리 중인 애플리케이션에 대해 *라이센스 키* 추가 작업을 한다면, 기기에 배포해야 하는 라이센스 키를 선택하고 관리 그룹 또는 기기 조회와 같은 여러 편리한 방법으로 대상 기기를 선택할 수 있습니다.

배포하기 전에 키 파일 또는 활성화코드를 중앙 관리 서버 저장소에 추가해야 합니다.

방법 지침:

- 관리 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 클라이언트 기기에 라이센스 키 배포

  또는

- Kaspersky Security Center 웹 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 클라이언트 기기에 라이센스 키 배포

기기에 수동으로 활성화코드 또는 키 파일 추가

애플리케이션 인터페이스에 제공된 도구를 사용하여 설치된 Kaspersky 애플리케이션을 로컬에서 활성화할 수 있습니다. 자세한 내용은 설치하려는 애플리케이션의 설명서를 참조하십시오.

사용 중인 라이센스 키 정보 보기

사용 중인 라이센스 키 정보를 보려면,

콘솔 트리에서 **Kaspersky 라이센스** 폴더를 선택합니다.

이 폴더의 작업 영역에 클라이언트 기기에서 사용 중인 라이센스 키 목록이 표시됩니다.

각 라이센스 키 옆에 사용 유형에 해당하는 아이콘이 표시됩니다:

-  —현재 사용 중인 라이센스 키에 관한 정보를 중앙 관리 서버에 연결된 클라이언트 기기에서 가져옵니다. 이 라이센스 키 파일은 중앙 관리 서버 외부에 저장됩니다.
-  —라이센스 키가 중앙 관리 서버 저장소에 저장됩니다. 이 라이센스 키에는 자동 배포가 사용되지 않습니다.
-  —라이센스 키가 중앙 관리 서버 저장소에 저장됩니다. 이 라이센스 키에는 자동 배포가 사용됩니다.

클라이언트 기기 속성 창의 **애플리케이션** 섹션을 열어 클라이언트 기기의 애플리케이션 활성화에 사용된 라이센스 키 정보를 볼 수 있습니다.

가상 중앙 관리 서버 라이센스 키의 최신 설정을 정의하기 위해 해당 중앙 관리 서버는 하루에 한 번 이상 Kaspersky 활성화 서버에 요청을 보냅니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다.

클라이언트 기기에서 라이센스 키를 수신하면 파일로 내보낼 수 없습니다.

중앙 관리 서버 저장소에 라이센스 키 추가

중앙 관리 서버 저장소에 라이센스 키를 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **Kaspersky 라이센스** 폴더를 선택합니다.
2. 다음 방법 중 하나를 사용하여 라이센스 키 추가 작업을 시작합니다:
   - 라이센스 키 목록의 컨텍스트 메뉴에서 **활성화 코드 또는 키 파일 추가**을 선택합니다.
   - 라이센스 키 목록의 작업 영역에서 **활성화 코드 또는 키 파일 추가** 링크를 누릅니다.
   - **활성화 코드 또는 키 파일 추가** 버튼을 누릅니다.

   라이센스 키 추가 마법사가 시작됩니다.
3. 활성화 코드를 사용하거나 키 파일을 사용하는 방법 중 중앙 관리 서버를 활성화하는 방법을 선택하십시오.
4. 활성화 코드 또는 키 파일을 지정합니다.
5. 네트워크에 해당 라이센스 키를 즉시 배포하려면 **관리 중인 기기에 자동으로 라이센스 키 배포** 옵션을 선택합니다. 이 옵션을 선택하지 않으면 나중에 수동으로 라이센스 키를 배포 할 수 있습니다.

   그러면 키 파일이 다운로드되고 라이센스 키 추가 마법사 가 완료됩니다. 이제 추가된 라이센스 키를 Kaspersky 라이센스 목록에서 볼 수 있습니다.

중앙 관리 서버 라이센스 키 삭제

중앙 관리 서버 라이센스 키를 삭제하려면 다음 절차를 따릅니다.

1. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창이 열리면 **라이센스 키** 섹션을 선택합니다.
3. **삭제** 버튼을 눌러 라이센스 키를 삭제합니다.

   이렇게 하면 라이센스 키가 삭제됩니다.

예약 라이센스 키가 추가된 경우, 기존 활성 라이센스 키가 삭제된 후에 예약 라이센스 키가 활성 라이센스 키로 자동 전환됩니다.

중앙 관리 서버의 활성 라이센스 키를 삭제하고 나면 취약점 및 패치 관리 및 모바일 기기 관리 기능을 사용할 수 없게 됩니다. 삭제된 라이센스 키를 다시 추가하거나 새 라이센스 키를 추가할 수 있습니다.

클라이언트 기기에 라이센스 키 배포

Kaspersky Security Center에서는 *라이센스 키 배포* 작업을 사용하여 클라이언트 기기에 라이센스 키를 배포할 수 있습니다.

배포 전에 중앙 관리 서버 저장소에 라이센스 키를 추가하십시오.

클라이언트 기기에 라이센스 키를 배포하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **Kaspersky 라이센스** 폴더를 선택합니다.
2. 라이센스 키 목록의 작업 영역에서 **관리 중인 기기에 자동으로 라이센스 키 배포** 버튼을 누릅니다.
   키 설치 작업 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. 애플리케이션 목록에서 작업을 만들 애플리케이션을 선택합니다.
4. 마법사의 **키 추가** 단계에서 다음 옵션 중 하나를 사용하여 라이센스 키를 추가합니다.
   - Kaspersky Security Center 저장소에서 **활성화 코드**를 추가하려면 활성화 코드 옵션을 선택하십시오.
     선택을 클릭합니다. 창이 열리면 활성화 코드를 선택하고 **확인**을 클릭합니다.
   - **키 파일 또는 키** 옵션을 선택하고 다음을 수행합니다.
     a. **선택**을 클릭합니다.
     b. 마우스 오른쪽 메뉴에서 다음 옵션 중 하나를 선택합니다.
     - **$SelectKeyIdDropdownOption1**.
       창이 열리면 기기에서 키 파일을 선택하고 **열기**를 클릭합니다.
     - **$SelectKeyIdDropdownOption2**.
       창이 열리면 Kaspersky Security Center 저장소에서 키를 선택한 다음 **확인**을 클릭합니다.
5. 활성 라이센스 키를 교체하려면 기본값인 **예비 키로 사용** 확인란을 선택 해제합니다.
   예를 들어 조직이 변경되어 다른 조직의 키가 기기에서 필요하거나 키가 재발급되어 새 라이센스가 현재 라이센스보다 빨리 만료되는 경우에 필요합니다. 오류를 방지하려면 **예비 키로 사용** 확인란을 선택 해제해야 합니다.
   Kaspersky Security Center Windows에 라이센스 키를 추가할 때 발생할 수 있는 문제와 이를 해결하는 방법에 대한 자세한 내용은 Kaspersky Security Center 기술 자료를 참조하십시오.
6. 라이센스 키 정보를 확인한 후 **다음**을 클릭합니다.

7. 마법사의 이 단계에서는 키 추가 작업을 할당할 기기를 선택합니다. 다음 방법 중 하나로 기기(최대 1,000대)를 추가할 수 있습니다.

   - **중앙 관리 서버가 발견한 기기 중에서 선택**. 이 경우 특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.
   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**. 작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.
   - **기기 선택 결과에 작업 할당**. 이 경우 이전에 만든 조회에 포함되는 기기에 작업이 할당됩니다. 사전 정의 조회 또는 직접 생성한 사용자 지정 조회를 지정할 수 있습니다.
   - **관리 그룹에 작업 할당**. 이 경우 이전에 만든 관리 그룹에 포함된 기기 작업이 할당됩니다.

8. 마법사의 **작업 스케줄 구성**에서 작업 시작 스케줄을 만들 수 있습니다.

   - **시작 스케줄**:
     - **한번만**

       작업은 지정한 날짜와 시간(기본값은 작업 생성일)에 한 번 실행됩니다.

     - **수동 시작**

       작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

       기본적으로 이 옵션은 선택되어 있습니다.

     - **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**

       저장소에 업데이트가 다운로드되고 나면 작업이 실행됩니다. 예를 들어 취약점 및 필요한 업데이트 검색 작업에 이 스케줄을 사용할 수 있습니다.

     - **바이러스 발생 시**

       바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:
       - 워크스테이션 및 파일 서버용 안티 바이러스
       - 경계 방어용 안티 바이러스
       - 메일 시스템용 안티 바이러스

       기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

       바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

     - **다른 작업 완료 시**

       다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

- 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
- 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
  기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
- 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

9. 마법사의 **작업 이름 정의** 단계에서 작업 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

10. 마법사의 **작업 생성 마침** 단계에서 **마침** 버튼을 눌러 마법사를 닫습니다.

    마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

키 설치 작업 생성 마법사를 통해 생성한 작업은 콘솔 트리의 **작업** 폴더에 저장된 특정 기기에 해당하는 작업입니다.

작업 생성 마법사를 통해 관리 그룹 및 클라이언트 기기에 대한 그룹 또는 로컬 라이센스 키 배포 작업을 만들 수도 있습니다.

라이센스 키 자동 배포

라이센스 키가 중앙 관리 서버의 라이센스 키 저장소에 있는 경우 Kaspersky Security Center에서 관리 중인 기기에 라이센스 키를 자동으로 배포할 수 있습니다. **미할당 기기** 폴더의 기기에는 라이센스 키 자동 배포가 적용되지 않습니다.

관리 중인 기기에 라이센스 키를 자동으로 배포하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **Kaspersky 라이센스** 폴더를 선택합니다.
2. 폴더 작업 영역에서 자동으로 기기에 배포하고자 하는 라이센스 키를 선택합니다.
3. 다음 방법 중 하나를 사용하여 선택한 라이센스 키의 속성 창을 엽니다:
   - 라이센스 키의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 선택한 라이센스 키의 정보 박스에서 **라이센스 키 속성 보기** 링크를 누릅니다.
4. 열린 라이센스 키 속성 창에서 **자동으로 라이센스 키 배포** 확인란을 선택합니다. 라이센스 키 속성 창을 닫습니다.

   라이센스 키는 모든 호환 기기에 자동으로 배포됩니다.

라이센스 키 배포는 네트워크 에이전트를 통해 수행됩니다. 애플리케이션에 대한 라이센스 키 배포 작업은 만들어지지 않습니다.

라이센스 키를 배포할 때는 기기 수에 대해 라이센스 제한을 고려합니다. (라이센스 제한은 라이센스 키의 속성에 설정되어 있습니다.) 라이센스 제한에 도달하면, 기기에 대한 이 라이센스 배포가 자동으로 중단됩니다.

가상 중앙 관리 서버가 해당 저장소와 중앙 관리 서버의 저장소에서 라이센스 키를 자동으로 배포합니다. 다음을 수행할 것을 권장합니다:

- *라이센스 키 추가* 작업을 사용하여 기기에 배포할 라이센스 키를 선택합니다.
- 가상 중앙 관리 서버 설정에서 **이 가상 중앙 관리 서버에서 소속된 기기로 라이센스 키 자동 배포 허용** 옵션을 비활성화하지 마십시오. 그렇지 않으면 가상 중앙 관리 서버가 중앙 관리 서버 저장소의 라이센스 키를 포함해 라이센스 키를 기기에 배포하지 않습니다.

라이센스 키 속성 창에서 **자동으로 라이센스 키 배포** 확인란을 선택하면 라이센스 키가 네트워크에 즉시 배포됩니다. 이 옵션을 선택하지 않으면 나중에 수동으로 라이센스 키를 배포 할 수 있습니다.

라이센스 키 사용 리포트 만들기 및 보기

클라이언트 기기에서 라이센스 키 사용 리포트를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. **라이센스 키 사용 리포트**라는 이름의 리포트 템플릿을 선택하거나 같은 유형의 새 리포트 템플릿을 만듭니다.

라이센스 키 사용 리포트의 작업 영역에 클라이언트 기기에서 사용 중인 활성 라이센스 키와 예약 라이센스 키에 대한 정보가 표시됩니다. 리포트에는 라이센스 키가 사용되는 기기 및 라이센스 키 속성에 지정된 제한 사항에 관한 정보도 포함됩니다.

애플리케이션 라이센스 키에 대한 정보 보기

Kaspersky 애플리케이션에 사용 중인 라이센스 키에 대해 알아보려면:

1. Kaspersky Security Center 콘솔 트리에서 **관리 중인 기기** 노드를 선택한 다음 **기기** 탭으로 이동합니다.
2. 마우스 오른쪽 버튼을 눌러 관련 기기의 마우스 오른쪽 메뉴를 열고 **속성**를 선택합니다.
3. 기기 속성 창이 열리면 **애플리케이션** 섹션을 선택합니다.
4. 애플리케이션 목록에서 라이센스 키를 내보내야 하는 애플리케이션을 선택하고 **속성** 버튼을 누릅니다.
5. 애플리케이션 속성 창이 열리면 **License keys** 섹션을 선택합니다.
   정보는 이 섹션의 작업 영역에 표시됩니다.

라이센스 키 파일 내보내기

실수로 삭제한 라이선스 키를 복원하려는 경우 다른 중앙 관리 서버의 라이선스 키 파일을 내보냅니다.

라이선스 키 파일을 내보내려면 **일반 기능: 키 관리** 기능 영역에서 **키 파일 내보내기** 권한이 있어야 합니다.

클라이언트 기기에서 라이선스 키를 수신하면 파일로 내보낼 수 없습니다.

라이선스 키를 내보내려면 다음을 수행합니다.

1. 콘솔 트리에서 **Kaspersky 라이센스** 폴더를 선택합니다.
2. 파일로 내보낼 라이선스 키를 목록에서 선택합니다.

3. 정보 상자가 열리면 **키 파일 내보내기** 링크를 클릭합니다.

4. 창이 열리면 라이선스 키 파일을 저장할 폴더의 경로를 지정하고, 파일 이름을 지정합니다. 그런 다음 **저장**을 클릭합니다.

.key 형식의 라이센스 키 파일이 선택한 폴더로 내보내집니다.

내보낸 파일의 라이센스 키가 활성화 코드로 중앙 관리 서버 저장소에 추가되었고, 내보낸 라이센스 키 파일을 다른 중앙 관리 서버의 저장소에 추가하려면 키 파일이 아닌 활성화 코드로 추가해야 합니다. 그렇지 않으면 오류가 발생합니다. 원하는 텍스트 편집기에서 내보낸 라이센스 키 파일을 연 다음, 활성화 코드를 복사합니다.

네트워크 보호 구성

이 섹션에는 정책 및 작업의 수동 구성, 사용자 역할, 관리 그룹 구조 및 작업 계층 구축에 대한 정보가 포함되어 있습니다.

시나리오: 네트워크 보호 구성

빠른 시작 마법사는 기본 설정을 통해 정책 및 작업을 만듭니다. 이러한 설정은 조직에 가장 적합하지 않을 수도 있고 조직에서 허용되지 않을 수도 있습니다. 따라서 네트워크에 필요한 경우 이러한 정책과 작업을 미세 조정하고 다른 정책과 작업을 만드는 것이 좋습니다.

필수 구성 요소

시작하기 전에 다음을 수행했는지 확인하십시오:

- Kaspersky Security Center 중앙 관리 서버 설치
- Kaspersky Security Center 웹 콘솔 설치(선택 사항)
- Kaspersky Security Center 주요 배포 시나리오 완료됨
- 빠른 시작 마법사 완료 또는 **관리 중인 기기** 관리 그룹에서 다음 정책과 작업을 수동으로 생성:
  - Kaspersky Endpoint Security 정책
  - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업
  - 네트워크 에이전트의 정책
  - *취약점 및 필요한 업데이트 검색* 작업

네트워크 보호 구성은 다음 단계로 진행됩니다:

1. **Kaspersky 애플리케이션 정책과 정책 프로필 설정 및 전파**

   관리 중인 기기에 설치되어 있는 Kaspersky 애플리케이션의 설정을 구성하고 전파하려는 경우 두 가지 보안 관리 방식, 즉 기기 중심 방식이나 사용자 중심 방식 중 하나를 사용할 수 있습니다. 이 두 방식을 조합하여 사용할 수도 있습니다. 기기 중심 보안 관리를 구현하려는 경우 Microsoft Management Console 기반 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 제공되는 도구를 사용할 수 있습니다. 사용자 중심 보안 관리는 Kaspersky Security Center 웹 콘솔을 통해서만 구현할 수 있습니다.

2. **Kaspersky 애플리케이션 원격 관리용 작업 구성**

   빠른 시작 마법사에서 생성된 작업을 확인하고 필요하다면 조정합니다.

   방법 지침:

   - 관리 콘솔:
     - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업 설정
     - 취약점 및 필요한 업데이트 검색 작업 스케줄 지정
   - Kaspersky Security Center 웹 콘솔:
     - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업 설정
     - 취약점 및 필요한 업데이트 검색 작업 설정

   필요한 경우 클라이언트 기기에 설치된 Kaspersky 애플리케이션을 관리하기 위한 추가 작업을 생성합니다.

3. **데이터베이스의 이벤트 부하 평가 및 제한**

   클라이언트 기기에서 관리 중인 애플리케이션 작업 중 발생하는 이벤트 정보가 전송되어 중앙 관리 서버 데이터베이스에 등록됩니다. 중앙 관리 서버의 부하를 줄이려면 데이터베이스에 저장할 수 있는 최대 이벤트 수를 평가 및 제한합니다.

   방법 지침:

   - 관리 콘솔: 최대 이벤트 수 설정
   - Kaspersky Security Center 웹 콘솔: 최대 이벤트 수 설정

결과

이 시나리오를 완료하면 중앙 관리 서버에서 수신하는 Kaspersky 애플리케이션, 작업 및 이벤트 구성을 통해 네트워크가 보호됩니다.

- Kaspersky 애플리케이션은 정책 및 정책 프로필에 따라 구성됩니다.
- 애플리케이션은 일련의 작업을 통해 관리됩니다.
- 데이터베이스에 저장할 수 있는 최대 이벤트 수가 설정됩니다.

네트워크 보호 구성이 완료되면 Kaspersky 데이터베이스 및 애플리케이션에 대한 정기 업데이트를 구성할 수 있습니다.

Kaspersky Sandbox에서 탐지한 위협에 대한 자동 대응을 구성하는 방법은 Kaspersky Sandbox 2.0 온라인 도움말을 참조하십시오.

정책 설정 및 전파: 기기 중심 방식

이 시나리오를 완료하면 정의한 애플리케이션 정책 및 정책 프로필에 따라 관리 중인 모든 기기에서 애플리케이션이 구성됩니다.

필수 구성 요소

시작하기 전에 Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔(옵션)을 설치했는지 확인하십시오. Kaspersky Security Center 웹 콘솔을 설치했다면 기기 중심 방식의 대안이나 추가 옵션으로 사용자 중심 보안 관리를 고려할 수도 있습니다.

단계

Kaspersky 애플리케이션의 기기 중심 관리 시나리오는 다음 단계로 구성됩니다:

1. **애플리케이션 정책 구성**

   관리 중인 기기에 설치되어 있는 각 Kaspersky 애플리케이션용 정책을 생성하여 애플리케이션의 설정 구성. 정책 세트는 클라이언트 기기로 전파됩니다.

   빠른 시작 마법사에서 네트워크 보호를 구성할 때 Kaspersky Security Center는 다음 애플리케이션을 위한 기본 정책을 생성합니다:

   - Kaspersky Endpoint Security for Windows - Windows 기반 클라이언트 기기용
   - Kaspersky Endpoint Security for Linux – Linux 기반 클라이언트 기기용

   이 마법사를 사용하여 구성 프로세스를 완료했다면, 이 애플리케이션용으로 새 정책을 생성할 필요가 없습니다. Kaspersky Endpoint Security 정책 수동 설정을 진행합니다.

   여러 중앙 관리 서버 및/또는 관리 그룹이 포함된 계층 구조가 있는 경우 보조 중앙 관리 서버와 자식 관리 그룹은 기본적으로 기본 중앙 관리 서버에서 정책을 상속합니다. 업스트림 정책에 구성된 설정을 수정할 수 없도록 자식 그룹과 보조 중앙 관리 서버의 상속을 강제 적용할 수 있습니다. 설정 중 일부만 강제로 상속되도록 하려는 경우 업스트림 정책에서 해당 설정을 잠글 수 있습니다. 잠금 해제된 나머지 설정은 다운스트림 정책에서 수정할 수 있습니다. 생성된 정책 계층 구조에서는 관리 그룹의 기기를 효율적으로 관리할 수 있습니다.

   방법 지침:

   - 관리 콘솔: 정책 만들기
   - Kaspersky Security Center 웹 콘솔: 정책 생성

2. **정책 프로필 생성(선택 사항)**

   단일 관리 그룹 내의 기기가 각기 다른 정책 설정으로 실행되도록 하려는 경우 해당 기기용 정책 프로필을 생성합니다. 정책 프로필은 정책 설정의 명명된 하위 집합입니다. 이 하위 집합은 정책과 함께 대상 기기에 배포되며 *프로필 활성화 조건*이라는 특수 조건에서 정책을 보완합니다. 관리 중인 기기에서 활성 상태인 "기본" 정책과 다른 설정만 프로필에 포함됩니다.

   프로필 활성화 조건을 사용하면 Active Directory의 특정 단위 또는 보안 그룹에 있거나, 특정 하드웨어 구성을 포함하거나, 특정 태그로 표시된 기기 등에 다른 정책 프로필을 적용할 수 있습니다. 태그를 사용하여 특정 기준을 충족하는 기기를 필터링합니다. 예를 들어 *Windows* 태그를 생성하여 Windows 운영 체제를 실행 중인 모든 기기를 이 태그로 표시한 다음 정책 프로필의 활성화 조건으로 이 태그를 지정할 수 있습니다. 그러면 Windows를 실행 중인 모든 기기에 설치된 Kaspersky 애플리케이션이 자체 정책 프로필을 통해 관리됩니다.

방법 지침:

- 관리 콘솔:
  - 정책 프로필 만들기
  - 정책 프로필 활성화 규칙 만들기
- Kaspersky Security Center 웹 콘솔:
  - 정책 프로필 만들기
  - 정책 프로필 활성화 규칙 만들기

3. **관리 중인 기기로 정책 및 정책 프로필 전파**

   기본적으로 중앙 관리 서버는 15분마다 관리 중인 기기와 자동으로 동기화됩니다. 자동 동기화를 사용하지 않고 강제 동기화 명령을 사용해 동기화를 수동으로 실행할 수 있습니다. 또한 정책 또는 정책 프로필을 생성 및 변경 시 동기화가 강제 실행됩니다. 동기화 중에 신규 또는 변경된 정책과 정책 프로필은 관리 중인 기기로 전파됩니다.

   Kaspersky Security Center 웹 콘솔을 사용한다면 정책과 정책 프로필이 기기로 전달되었는지 확인할 수 있습니다. Kaspersky Security Center는 기기 속성에 전달 날짜와 시간을 지정합니다.

   방법 지침:

   - 관리 콘솔: 강제 동기화
   - Kaspersky Security Center 웹 콘솔: 강제 동기화

결과

기기 중심 시나리오를 완료하면 Kaspersky 애플리케이션은 정책 계층 구조를 통해 지정 및 전파된 설정에 따라 구성됩니다.

구성된 애플리케이션 정책 및 정책 프로필은 관리 그룹에 추가하는 새 기기에 자동으로 적용됩니다.

기기 중심 및 사용자 중심 보안 관리 방식 정보

기기 기능 및 사용자 역할 측면에서 보안 설정을 관리할 수 있습니다. 기기 기능 측면의 관리 방식은 *기기 중심 보안 관리*이고 사용자 역할 측면의 관리 방식은 *사용자 중심 보안 관리*입니다. 기기마다 서로 다른 애플리케이션 설정을 적용하려는 경우 두 관리 유형 중 하나를 사용하거나 두 유형을 조합하여 사용할 수 있습니다. 기기 중심 보안 관리를 구현하려면 Microsoft Management Console 기반 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 제공되는 도구를 사용할 수 있습니다. 사용자 중심 보안 관리는 Kaspersky Security Center 웹 콘솔을 통해서만 구현할 수 있습니다.

기기 중심 보안 관리를 통해 기기별 기능에 따라 다양한 보안 제품 설정을 관리 중인 기기에 적용할 수 있습니다. 예를 들어, 다른 관리 그룹에 할당된 기기에 다른 설정을 적용할 수 있습니다. Active Directory에서의 기기 사용이나 하드웨어 사양에 따라 기기를 차별화할 수도 있습니다.

사용자 중심 보안 관리를 통해 사용자 역할에 따라 다른 보안 제품을 적용할 수 있습니다. 여러 개의 사용자 역할을 만들고, 각 사용자에게 적절한 사용자 역할을 할당하고, 서로 다른 역할의 사용자가 소유한 기기에 다양한 애플리케이션 설정을 정의할 수 있습니다. 경리 직원과 HR(인사) 전문가의 기기에 서로 다른 애플리케이션 설정을 적용하려는 경우를 예로 들 수 있습니다. 따라서 사용자 중심의 보안 관리를 구현할 때 각 부서(계정 부서 및 HR 부서)에는 Kaspersky 애플리케이션에 대한 고유한 설정 구성이 있습니다. 설정 구성은 사용자가 변경할 수 있는 애플리케이션 설정과 관리자가 강제로 설정하고 잠금 설정을 정의합니다.

사용자 중심 보안 관리를 사용하면 개별 사용자에게 특정 애플리케이션 설정을 적용할 수 있습니다. 회사 내의 특정 직원에게 고유한 역할이 지정되어 있거나, 특정인의 기기와 관련된 보안 문제를 모니터링하려는 경우 이러한 방식을 사용할 수 있습니다. 회사 내 역할에 따라 해당 직원이 애플리케이션 설정을 변경하는 권한을 확장하거나 제한할 수 있습니다. 예를 들어 지역 사무소에서 클라이언트 기기를 관리하는 시스템 관리자의 권한을 확장할 수 있습니다.

기기 중심 및 사용자 중심 보안 관리 방식을 조합하여 사용할 수도 있습니다. 예를 들어 각 관리 그룹용으로 특정 애플리케이션 정책을 구성한 다음 기업의 사용자 역할 하나 또는 여러 개에 대해 정책 프로필을 만들 수 있습니다. 이 경우 정책 및 정책 프로필은 다음 순서로 적용됩니다:

1. 기기 중심 보안 관리용으로 만든 정책이 적용됩니다.
2. 이러한 정책은 정책 프로필 우선 순위에 따라 정책 프로필을 통해 수정됩니다.
3. 사용자 역할과 연결된 정책 프로필을 통해 정책이 수정됩니다.

Kaspersky Endpoint Security 정책 수동 설정

이 섹션에서는 빠른 시작 마법사를 통해 생성한 Kaspersky Endpoint Security 정책의 권장 구성 방법을 설명합니다. 정책 속성 창에서 설정을 수행할 수 있습니다.

설정을 편집할 때는 워크스테이션에서 관련 설정의 값을 사용할 수 있도록 해당 설정 위에 있는 잠금 아이콘을 클릭해야 합니다.

지능형 위협 보호 섹션의 정책 구성

이 섹션에 나와 있는 설정의 전체 설명은 Kaspersky Endpoint Security for Windows 설명서를 참조하십시오.

지능형 위협 보호 섹션에서 Kaspersky Endpoint Security for Windows용 Kaspersky Security Network의 사용을 구성할 수 있습니다. 행동 탐지, 익스플로잇 방지, 호스트 침입 방지 및 치료 엔진과 같은 Kaspersky Endpoint Security for Windows 모듈을 구성할 수도 있습니다.

Kaspersky Security Network 하위 섹션에서 **Kaspersky Security Network** 옵션을 활성화하는 것이 좋습니다. 네트워크에서 트래픽을 재분배하고 최적화하려면 이 기능을 사용합니다. **Kaspersky Security Network** 옵션이 비활성화되었다면, 직접 KSN 서버 사용을 활성화할 수 있습니다.

필수 위협 보호 섹션의 정책 구성

이 섹션에 나와 있는 설정의 전체 설명은 Kaspersky Endpoint Security for Windows 설명서를 참조하십시오.

정책 속성 창의 **필수 위협 보호** 섹션에서 **방화벽** 및 **파일 위협 보호** 하위 섹션에 추가 설정을 지정하는 것이 좋습니다.

방화벽 하위 섹션에는 클라이언트 기기에서 애플리케이션의 네트워크 활동을 제어할 수 있는 설정이 포함되어 있습니다. 클라이언트 기기는 공용, 로컬, 신뢰 상태 중 하나가 할당된 네트워크를 사용합니다. 네트워크 상태에 따라 Kaspersky Endpoint Security는 기기에서 네트워크 활동을 허용하거나 거부할 수 있습니다. 조직에 새 네트워크를 추가할 때 적절한 네트워크 상태를 할당해야 합니다. 예를 들어 클라이언트 기기가 랩톱이라면 랩톱이 항상 로컬 네트워크에 연결되어 있는 것은 아니므로 이 기기는 공용 또는 신뢰하는 네트워크를 사용할 것을 권장합니다. **방화벽** 하위 섹션에서 조직에서 사용하는 네트워크에 상태를 올바르게 할당했는지 확인할 수 있습니다.

네트워크 목록을 확인하려면 다음을 수행합니다:

1. 정책 속성에서 애플리케이션 **필수 위협 보호** → **방화벽**으로 이동합니다.
2. **사용 가능한 네트워크** 섹션에서 **설정** 버튼을 클릭합니다.
3. **방화벽** 창이 열리면 **네트워크** 탭으로 이동하여 네트워크 목록을 확인합니다.

파일 위협 보호 하위 섹션에서 네트워크 드라이브 검사를 비활성화할 수 있습니다. 네트워크 드라이브 검사 시 네트워크 드라이브의 부하가 높아질 수 있습니다. 그러므로 파일 서버에서 간접 검사를 수행하는 것이 더 편리합니다.

네트워크 드라이브 검사를 중지하려면 다음을 수행합니다:

1. 정책 속성에서 **필수 위협 보호** → **파일 위협 보호**로 갑니다.
2. **보안 레벨** 섹션에서 **설정** 버튼을 클릭합니다.
3. **파일 위협 보호** 창이 열리면 **일반** 탭에서 **모든 네트워크 드라이브** 확인란 선택을 취소합니다.

일반 설정 섹션의 정책 구성

이 섹션에 나와 있는 설정의 전체 설명은 Kaspersky Endpoint Security for Windows 설명서를 참조하십시오.

정책 속성 창의 **일반 설정** 섹션에서 **리포트 및 저장소**와 **인터페이스** 하위 섹션에 추가 설정을 지정할 것을 권장합니다.

리포트 및 저장소 하위 섹션에서 **중앙 관리 서버로의 데이터 전송** 섹션으로 갑니다. **시작된 애플리케이션 정보** 확인란은 네트워크에 연결된 기기에 설치된 소프트웨어 모듈 전체의 모든 버전에 관한 정보를 중앙 관리 서버 데이터베이스에 저장할지 지정합니다. 이 확인란을 선택하면 정보 저장을 위해 Kaspersky Security Center 데이터베이스에서 상당한 디스크 공간(수십 GB)이 필요할 수 있습니다. 최상위 정책에서 **시작된 애플리케이션 정보** 확인란이 선택되어 있다면 선택 취소합니다.

관리 콘솔이 조직 네트워크의 위협 보호를 중앙 집중식 모드로 관리한다면, 워크스테이션에서 Kaspersky Endpoint Security for Windows 사용자 인터페이스 표시를 비활성화하십시오. 이렇게 하려면 **인터페이스** 하위 섹션에서 **사용자와의 상호 작용** 섹션으로 간 후 **사용자 인터페이스 표시 안 함** 옵션을 선택합니다.

워크스테이션에서 암호 보호를 활성화하려면 **인터페이스** 하위 섹션에서 **암호 보호** 섹션으로 간 후 **설정** 버튼을 클릭하고 **암호 보호 사용** 확인란을 선택합니다.

이벤트 구성 섹션의 정책 구성

이벤트 구성 섹션에서는 다음을 제외한 중앙 관리 서버의 모든 이벤트 저장을 중지해야 합니다:

- **심각** 이벤트 탭:
  - *애플리케이션 자동 시작이 비활성화되었습니다*
  - *접근 거부됨*
  - *애플리케이션 시작이 금지됨*
  - *치료 불가*
  - *최종 사용자 라이센스 계약서 위반*
  - *암호화 모듈을 로드할 수 없음*
  - *두 작업을 동시에 시작할 수 없음*
  - *활성 위협 탐지됨. 고급 치료 시작 필요*
  - *네트워크 공격이 탐지됨*
  - *일부 구성 요소가 업데이트되지 않았습니다*
  - *활성화 오류*
  - *휴대용 모드 활성화 오류*
  - *Kaspersky Security Center와 통신 오류*
  - *휴대용 모드 비활성화 오류*
  - *애플리케이션 구성 요소 변경 오류*
  - *파일 암호화/복호화 규칙 적용 오류*
  - *정책을 적용할 수 없음*
  - *프로세스 종료*
  - *네트워크 활동이 차단됨*
- **기능 실패** 탭: *잘못된 작업 설정. 설정이 적용되지 않음*

- **경고** 탭:
  - *자기 보호가 비활성화되었습니다*
  - *잘못된 예비 키*
  - *사용자가 암호화 정책을 거부함*
- **정보** 탭: *테스트 모드에서의 애플리케이션 시작이 차단됨*

Kaspersky Endpoint Security용 그룹 업데이트 작업 수동 설정

Kaspersky Endpoint Security 버전 10 이상에 대한 최적 및 권장 스케줄 옵션은 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후(자동으로 작업 시작 임의 지연 사용** 확인란을 선택한 경우)입니다.

Kaspersky Endpoint Security가 설치된 기기 검사를 위한 그룹 작업 수동 설정

빠른 시작 마법사에서 기기 검사를 위한 그룹 작업을 생성합니다. 기본적으로 작업에는 **금요일 오후 7시에 실행** 스케줄이 할당되고, 작업은 자동으로 임의 실행되며, **누락된 작업 실행** 확인란 선택은 취소되어 있습니다.

즉, 예를 들어 조직의 기기가 금요일 오후 6시 30분에 종료되면 기기 검사 작업은 실행되지 않습니다. 조직에서 채택한 회사 규칙에 따라 이 작업에 가장 편리한 스케줄을 설정해야 합니다.

취약점 및 필요한 업데이트 검색 작업 스케줄 지정

빠른 시작 마법사에서 네트워크 에이전트용 *취약점 및 필요한 업데이트 검색* 작업을 만듭니다. 기본적으로 작업에는 **화요일 오후 7시에 실행** 스케줄이 할당되고, 작업은 자동으로 임의 실행되며, **누락된 작업 실행** 확인란은 선택되어 있습니다.

이 시간에 모든 기기를 종료하는 조직의 회사 규칙이 제공되는 경우에는 기기가 다시 켜진 후(수요일 아침)에 *취약점 및 필요한 업데이트 검색* 작업이 실행됩니다. 취약점 검사가 수행되면 CPU와 디스크 하위 시스템의 부하가 증가할 수 있으므로, 이러한 방식의 활동은 바람직하지 않을 수도 있습니다. 조직에서 채택한 회사 규칙에 따라 이 작업에 가장 편리한 스케줄을 설정해야 합니다.

업데이트 설치 및 취약점 수정을 위한 그룹 작업 수동 설정

빠른 시작 마법사에서 네트워크 에이전트용으로 업데이트 설치 및 취약점 수정을 위한 그룹 작업을 생성합니다. 기본적으로 작업은 매일 오전 1시에 실행되도록 설정되고, 작업은 자동으로 임의 실행되며, **누락된 작업 실행** 옵션이 활성화되어 있지 않습니다.

야간에는 기기를 종료하는 조직의 회사 규칙이 제공되는 경우 업데이트 설치는 실행되지 않습니다. 조직에서 채택한 회사 규칙에 따라 취약점 검사 작업에 가장 편리한 스케줄을 설정해야 합니다. 또한 업데이트 설치 시에는 기기를 다시 시작해야 할 수 있습니다.

이벤트 저장소에 저장되는 최대 이벤트 수 설정

중앙 관리 서버 속성 창의 **이벤트 저장소** 섹션에서 이벤트 레코드 개수 및 레코드 저장 기간을 제한해 중앙 관리 서버 데이터베이스의 이벤트 저장 설정을 편집할 수 있습니다. 최대 이벤트 수를 지정하면 애플리케이션은 지정된 이벤트 수에 필요한 스토리지 공간의 대략적인 양을 계산합니다. 이 대략적인 계산 결과 값을 사용하여 디스크의 사용 가능한 공간이 데이터베이스 초과 상황을 방지하기에 충분한지 여부를 평가할 수 있습니다. 중앙 관리 서버 데이터베이스의 기본 용량은 400,000개 이벤트입니다. 데이터베이스의 최대 권장 용량은 4,500만개 이벤트입니다.

애플리케이션은 10분마다 데이터베이스를 확인합니다. 이벤트 수가 지정된 최댓값이나 10,000에 도달하면 애플리케이션은 지정된 최대 이벤트 수만 남도록 가장 오래된 이벤트를 삭제합니다.

중앙 관리 서버가 오래된 이벤트를 삭제할 때에는 새 이벤트를 데이터베이스에 저장할 수 없습니다. 이 기간 동안에는 거부된 이벤트 관련 정보가 Kaspersky 이벤트 로그에 기록됩니다. 새 이벤트는 대기열에 보관되었다가 삭제 작업이 완료되고 나면 데이터베이스에 저장됩니다.

중앙 관리 서버의 이벤트 저장소에 저장할 수 있는 이벤트 수를 제한하려면 다음과 같이 하십시오:

1. 중앙 관리 서버를 마우스 오른쪽으로 클릭한 다음 **속성**을 선택합니다.

   중앙 관리 서버 속성 창이 열립니다.

2. **이벤트 저장소** 섹션의 작업 영역에서 데이터베이스에 저장된 최대 이벤트 수를 지정합니다.

3. **확인**를 누릅니다.

또한, 모든 작업의 설정을 변경하여 작업 진행과 관련된 이벤트를 저장하거나 작업 실행 결과만 저장할 수 있습니다. 이렇게 하면 데이터베이스의 이벤트 수를 줄이고, 데이터베이스의 이벤트 테이블에 대한 분석과 관련된 시나리오의 실행 속도를 높이며 다량의 이벤트가 심각 이벤트를 덮어쓰는 위험을 줄일 수 있습니다.

수정된 취약점에 대한 정보의 최대 보관 기간 설정

관리 중인 기기에서 이미 수정된 취약성에 대한 정보를 데이터베이스에 보관하는 최대 기간을 설정하려면:

1. 중앙 관리 서버를 마우스 오른쪽으로 클릭한 다음 **속성**을 선택합니다.

   중앙 관리 서버 속성 창이 열립니다.

2. **이벤트 저장소** 섹션의 작업 영역에서 수정된 취약점에 대한 정보를 데이터베이스에 보관하는 최대 기간을 지정합니다.

   기본 저장 기간은 90일입니다.

3. **확인**를 누릅니다.

수정된 취약점에 대한 정보의 최대 보관 기간은 지정된 일수로 제한됩니다. 그 후 중앙 관리 서버 유지 관리 작업 시 데이터베이스에서 오래된 정보가 삭제됩니다.

작업 관리

Kaspersky Security Center에서는 다양한 작업을 만들고 실행하여 기기에 설치된 애플리케이션을 관리할 수 있습니다. 작업은 애플리케이션을 설치, 실행 및 중단하고, 파일을 검사하며, 데이터베이스와 소프트웨어 모듈을 업데이트하고, 애플리케이션에 대해 기타 작업을 수행하는 데 필요합니다.

또한 다음과 같은 유형으로 작업을 세분화할 수 있습니다:

- *그룹 작업*. 선택한 관리 그룹의 기기에서 수행되는 작업.
- *중앙 관리 서버 작업*. 중앙 관리 서버에서 수행되는 작업.
- *특정 기기 작업*. 관리 그룹에 포함되어 있는지 여부에 관계없이 선택한 기기에서 수행되는 작업.
- *로컬 작업*. 특정 기기에서 수행되는 작업.

애플리케이션 작업은 관리자 워크스테이션에 해당 애플리케이션의 관리 플러그인이 설치되어 있는 경우에만 만들 수 있습니다.

다음과 같은 방법을 사용하여 작업을 만들어야 할 기기(최대 1,000대)의 목록을 컴파일할 수 있습니다.

- 중앙 관리 서버에서 탐지된 네트워크 기기 선택.
- 기기 목록을 수동으로 지정. IP 주소(또는 IP 범위), NetBIOS 이름 또는 DNS 이름을 기기의 주소로 사용할 수 있습니다.
- 추가할 기기의 주소가 포함된 .txt 파일에서 기기의 목록을 가져옵니다(줄당 하나의 주소를 표시해야 함).

  파일에서 기기의 목록을 가져오거나 수동으로 작성할 경우 기기가 이름으로 식별되면 기기를 연결할 때 또는 기기 발견 과정에서 중앙 관리 서버 데이터에 이미 정보가 입력된 기기만 목록에 포함됩니다.

각 애플리케이션에 대해 그룹 작업, 특정 기기 작업 또는 로컬 작업을 원하는 수만큼 만들 수 있습니다.

네트워크 에이전트가 중앙 관리 서버에 연결되면, 기기에 설치된 애플리케이션과 Kaspersky Security Center 데이터베이스 간에 작업 정보의 교환이 이루어집니다.

작업 설정을 변경하고 작업 진행 상황을 확인하며, 해당 설정의 복사, 내보내기, 가져오기 및 삭제를 수행할 수 있습니다.

작업을 만든 애플리케이션이 실행 중인 경우에만 기기에서 작업이 시작됩니다. 애플리케이션이 실행되고 있지 않은 경우, 실행 중인 모든 작업이 취소됩니다.

완료된 작업의 결과는 중앙 관리 서버에 중앙 집중식으로 Microsoft Windows 및 Kaspersky Security Center의 이벤트 로그에 저장되며, 각 기기에 로컬로도 동일하게 저장됩니다.

작업 설정에 기밀 데이터를 포함하지 마십시오. 예를 들어, 도메인 관리자 암호를 지정하지 마십시오.

멀티테넌시가 지원되는 애플리케이션용 작업 관리 세부 정보

멀티테넌시가 지원되는 애플리케이션용 그룹 작업은 중앙 관리 서버 및 클라이언트 기기의 계층 구조에 따라 애플리케이션에 적용됩니다. 작업이 생성된 가상 중앙 관리 서버는 애플리케이션이 설치된 클라이언트 기기와 같은 관리 그룹이나 하위 레벨 관리 그룹에 있어야 합니다.

작업 실행 결과에 해당하는 이벤트에는 작업이 실행된 기기 관련 정보가 서비스 공급자 관리자에게 표시됩니다. 반면 테넌트 관리에는 **멀티테넌트 노드**가 표시됩니다.

작업 만들기

관리 콘솔에서 그룹 작업을 만들어야 하는 관리 그룹의 폴더 또는 **작업** 폴더의 작업 영역에서 직접 작업을 만들 수 있습니다.

관리 그룹의 폴더에서 그룹 작업을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 작업을 만들 관리 그룹을 선택합니다.
2. 그룹 작업 영역에서 **작업** 탭을 선택합니다.
3. **작업 생성** 버튼을 눌러 작업 만들기를 실행합니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

***작업** 폴더의 작업 영역에서 작업을 만들려면 다음과 같이 하십시오:*

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **마침** 버튼을 눌러 작업 만들기를 실행합니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

작업 설정에 기밀 데이터를 포함하지 마십시오. 예를 들어, 도메인 관리자 암호를 지정하지 마십시오.

중앙 관리 서버 작업 생성

중앙 관리 서버는 다음과 같은 작업을 수행합니다:

- 리포트 전달
- 중앙 관리 서버 저장소에 업데이트 다운로드
- 중앙 관리 서버 데이터 백업
- 중앙 관리 서버 점검
- Windows 업데이트 동기화 수행

- 참조 기기 OS 이미지에 설치 패키지 생성
- 원격으로 애플리케이션 설치
- 원격으로 애플리케이션 제거
- 설치 패키지 배포
- 보조 중앙 관리 서버에 원격으로 애플리케이션 설치

가상 중앙 관리 서버에서는 리포트 자동 전달 작업 및 참조 기기 OS 이미지를 기반으로 한 설치 패키지 만들기 작업만 할 수 있습니다. 가상 중앙 관리 서버의 저장소에는 기본 중앙 관리 서버로 다운로드된 업데이트가 표시됩니다. 가상 중앙 관리 서버의 데이터 백업은 기본 중앙 관리 서버의 데이터 백업과 함께 수행됩니다.

중앙 관리 서버 작업을 만들려면 다음과 같이 하십시오.

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. 다음 방법 중 하나로 작업을 시작합니다:
   - 콘솔 트리에 있는 **작업** 폴더의 마우스 오른쪽 메뉴에서 **새로 만들기 → 작업**을 선택합니다.
   - **작업** 폴더의 작업 영역에 있는 **작업 생성** 버튼을 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

중앙 관리 서버 저장소 업데이트 다운로드, Windows 업데이트 동기화 수행, 중앙 관리 서버 점검 및 *중앙 관리 서버 데이터 백업* 작업은 한 번만 만들 수 있습니다. *중앙 관리 서버 저장소 업데이트 다운로드*, *중앙 관리 서버 점검*, *중앙 관리 서버 데이터 백업*, *Windows 업데이트 동기화 수행* 작업이 이미 중앙 관리 서버에 만들어져 있다면 새 작업 마법사의 작업 유형 선택 창에 이들 작업이 표시되지 않습니다.

특정 기기 작업 만들기

Kaspersky Security Center에서는 특정 기기 작업을 만들 수 있습니다. 하나의 집합으로 연결된 기기는 여러 관리 그룹에 포함되거나 어떤 관리 그룹에도 포함되지 않을 수 있습니다. Kaspersky Security Center에서는 다음과 같은 주요 특정 기기 작업을 수행할 수 있습니다:

- 원격으로 애플리케이션 설치
- 공지 메시지 배포
- 중앙 관리 서버 변경
- 기기 관리
- 업데이트 검증
- 설치 패키지 배포

- 보조 중앙 관리 서버에 원격으로 애플리케이션 설치
- 원격으로 애플리케이션 제거

특정 기기 작업을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. 다음 방법 중 하나로 작업을 시작합니다:
   - 콘솔 트리에 있는 **작업** 폴더의 마우스 오른쪽 메뉴에서 **새로 만들기** → **작업**를 선택합니다.
   - **작업** 폴더의 작업 영역에 있는 **작업 생성** 버튼을 누릅니다.

새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

로컬 작업 만들기

기기의 로컬 작업을 만들려면 다음과 같이 하십시오:

1. 기기를 포함한 그룹의 작업 영역에서 **기기** 탭을 선택합니다.
2. **기기** 탭의 기기 목록에서 로컬 작업을 만들어야 하는 기기를 선택합니다.
3. 다음 방법 중 하나를 사용해 선택한 기기에 대한 작업 만들기를 시작합니다:
   - **처리 방법 수행** 버튼을 클릭하고 드롭다운 목록에서 **작업 생성**을 선택합니다.
   - 기기의 작업 영역에서 **작업 생성** 링크를 클릭합니다.
   - 다음과 같이 기기 속성을 사용합니다.
     a. 기기의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
     b. 기기 속성 창이 열리면 **작업** 섹션을 선택하고 **추가**를 누릅니다.

새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

로컬 작업을 만들고 구성하는 방법에 대한 자세한 설명은 해당 Kaspersky 애플리케이션 설명서에 나와 있습니다.

중첩된 그룹의 작업 영역에서 상속된 그룹 작업 표시

작업 영역에서 중첩된 그룹의 상속된 작업을 표시하려면 다음과 같이 하십시오:

1. 중첩된 그룹의 작업 영역에서 **작업** 탭을 선택합니다.
2. **작업** 탭의 작업 영역에서 **상속된 작업 보기** 버튼을 누릅니다.

그러면 상속된 작업이 다음과 같은 아이콘과 함께 작업 목록에 표시됩니다:

-  —기본 중앙 관리 서버에 생성한 그룹에서 상속 시.
-  —최상위 그룹에서 상속 시.

상속 모드가 활성화된 경우, 상속된 작업은 해당 작업이 만들어진 그룹에서만 편집할 수 있습니다. 작업을 상속하는 그룹에서는 상속된 작업을 편집할 수 없습니다.

작업이 실행되기 전에 자동으로 기기 켜기

Kaspersky Security Center는 꺼진 기기에서는 작업을 실행하지 않습니다. Wake-on-LAN 기능을 사용하여 작업을 시작하기 전에 이러한 기기를 자동으로 켜도록 Kaspersky Security Center를 구성할 수 있습니다.

작업을 시작하기 전에 기기를 자동으로 켜도록 구성하려면:

1. 작업 속성 창에서 **스케줄** 섹션을 선택합니다.
2. 기기에서 작업을 구성하려면 **고급** 링크를 클릭합니다.
3. **고급** 창이 열리면, **작업 시작 전에 Wake-on-LAN 기능으로 기기 켜기(분)** 확인란을 선택하고 시간 간격을 분 단위로 지정합니다.

결과적으로 Kaspersky Security Center는 작업을 시작하기 전에 지정된 시간(분) 동안 Wake-on-LAN 기능을 사용하여 기기를 켜고 기기에 운영 체제를 로드합니다. 작업이 완료된 후 기기 사용자가 시스템에 로그인하지 않으면 기기가 자동으로 종료됩니다. Kaspersky Security Center는 Wake-on-LAN 기능을 사용하여 켜진 기기만 자동으로 종료합니다.

Kaspersky Security Center는 WoL(Wake-on-LAN) 표준을 지원하는 기기에서만 운영 체제를 자동으로 시작할 수 있습니다.

작업이 완료된 후 자동으로 기기 끄기

Kaspersky Security Center에서 작업이 완료된 후에 자동으로 설정이 배포된 기기가 꺼지는 방식으로 작업 설정을 구성할 수 있습니다.

작업이 완료된 후 자동으로 기기를 끄려면 다음과 같이 진행합니다:

1. 작업 속성 창에서 **스케줄** 섹션을 선택합니다.
2. **고급** 링크를 눌러 기기에 대한 작업을 구성하는 창을 엽니다.
3. **고급** 창이 열리면 **작업 완료 후 기기 종료** 확인란을 선택합니다.

작업 실행 시간 제한

기기에서 작업이 실행되는 시간을 제한하려면 다음과 같이 하십시오:

1. 작업 속성 창에서 **스케줄** 섹션을 선택합니다.
2. **고급**를 눌러 클라이언트 기기에서 작업을 구성할 수 있는 창을 엽니다.
3. **고급** 창이 열리면 **작업이 다음 시간보다 오래 실행되면 중지(분)** 확인란을 선택하고 시간 간격을 분 단위로 지정합니다.

   그러면 지정된 시간이 경과된 후에도 기기에서의 작업이 아직 완료되지 않은 경우 Kaspersky Security Center가 작업을 자동으로 중단합니다.

작업 내보내기

그룹 작업 및 특정 기기 작업을 파일로 내보낼 수 있습니다. 중앙 관리 서버 작업은 내보낼 수 없습니다.

작업을 내보내려면 다음과 같이 하십시오:

1. 작업의 마우스 오른쪽 메뉴에서 **모든 작업 → 내보내기**를 선택합니다.
2. **다른 이름으로 저장** 창이 열리면 파일 이름 경로를 지정합니다.
3. **저장** 버튼을 누릅니다.

로컬 사용자의 권한은 내보내지지 않습니다.

작업 가져오기

그룹 작업 및 특정 기기 작업을 가져올 수 있습니다. 중앙 관리 서버 작업은 가져올 수 없습니다.

작업을 가져오려면 다음과 같이 하십시오:

1. 작업을 가져와야 하는 목록을 선택합니다:
   - 작업을 그룹 작업 목록으로 가져오려면 관련 관리 그룹의 작업 영역에서 **작업** 탭을 선택합니다.
   - 작업을 특정 기기 작업 목록으로 가져오려면 콘솔 트리에서 **작업** 폴더를 선택합니다.

2. 다음 옵션 중 하나를 선택하여 작업을 가져옵니다:

   - 작업 목록의 마우스 오른쪽 메뉴에서 **모든 작업** → **가져오기**를 선택합니다.
   - 작업 목록 관리 블록에서 **파일에서 작업 가져오기** 링크를 누릅니다.

3. 열리는 창에서 작업을 가져올 파일 경로를 지정합니다.

4. **열기** 버튼을 누릅니다.

   그러면 작업 목록에 그 작업이 나타납니다.

새로 가져온 작업의 이름이 기존 작업과 같다면, 가져온 작업의 이름은 **(<다음 시퀀스 번호>)** 인덱스로 확장됩니다(예: **(1)**, **(2)**).

작업 변환

Kaspersky Security Center를 사용하여 이전 버전 Kaspersky 애플리케이션의 작업을 동일한 애플리케이션 최신 버전의 작업으로 변환할 수 있습니다.

작업 변환이 가능한 애플리케이션은 다음과 같습니다:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

작업을 변환하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 작업을 변환할 중앙 관리 서버를 선택합니다.

2. 중앙 관리 서버 마우스 오른쪽 메뉴에서 **모든 작업** → **정책 및 작업 변환 마법사**를 선택합니다.

   정책 및 작업 일괄 변환 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

마법사가 작업을 완료하면 이전 버전 애플리케이션의 작업 설정을 사용하는 새로운 작업이 만들어집니다.

수동으로 작업 시작 및 중지

다음 방법 중 하나로 작업을 수동으로 시작하고 중지할 수 있습니다: 작업이 할당된 클라이언트 기기 속성 창이나 이 작업의 마우스 오른쪽 메뉴.

KLAdmins 그룹에 포함된 사용자만 클라이언트 기기의 마우스 오른쪽 메뉴에서 그룹 작업을 시작할 수 있습니다.

작업 속성 창의 마우스 오른쪽 메뉴에서 작업을 시작하거나 중지하려면 다음과 같이 하십시오:

1. 작업 목록에서 작업을 선택합니다.
2. 다음 방법 중 하나로 작업을 시작 및 중지합니다:
   - 작업의 컨텍스트 메뉴에서 **시작** 또는 **중지**를 선택합니다.
   - 작업 속성 창의 **일반** 섹션에서 **시작** 또는 **중지**을 누릅니다.

클라이언트 기기 속성 창의 마우스 오른쪽 메뉴에서 작업을 시작하거나 중지하려면 다음과 같이 하십시오:

1. 기기 목록에서 기기를 선택합니다.
2. 다음 방법 중 하나로 작업을 시작 및 중지합니다:
   - 기기의 마우스 오른쪽 메뉴에서 **모든 작업** → **작업 실행**를 선택합니다. 작업 목록에서 관련 작업을 선택합니다.

     작업이 할당된 기기 목록이 선택한 기기로 교체됩니다. 작업이 시작됩니다.
   - 기기 속성 창의 **작업** 섹션에서 시작 버튼() 또는 정지 버튼()을 누릅니다.

수동으로 작업 일시 중지 및 다시 시작

실행 중인 작업을 수동으로 일시 중지하거나 다시 시작하려면 다음과 같이 하십시오:

1. 작업 목록에서 작업을 선택합니다.
2. 다음 방법 중 하나를 사용하여 작업을 일시 중지하거나 다시 시작합니다:
   - 작업의 마우스 오른쪽 메뉴에서 **일시 중지** 또는 **다시 시작**을 선택합니다.
   - 작업 속성 창에서 **일반** 섹션을 선택하고 **일시 중지** 또는 **다시 시작**을 누릅니다.

작업 실행 감시

작업 실행을 감시하려면 다음과 같이 하십시오,

작업 속성 창에서 **일반** 섹션을 선택합니다.

일반 섹션의 중간 부분에 현재 작업 상태가 표시됩니다.

중앙 관리 서버에 저장된 작업 실행 결과 보기

Kaspersky Security Center에서는 그룹 작업, 특정 기기 작업 및 중앙 관리 서버 작업의 결과를 볼 수 있습니다.

작업 결과를 보려면 다음과 같이 하십시오:

1. 작업 속성 창에서 **일반** 섹션을 선택합니다.
2. **결과** 링크를 눌러 **작업 결과** 창을 엽니다.

보조 중앙 관리 서버에 대한 작업 결과를 보려면:

1. 작업 속성 창에서 **일반** 섹션을 선택합니다.
2. **결과** 링크를 눌러 **작업 결과** 창을 엽니다.
3. **보조 서버의 통계**를 클릭합니다.
4. **작업 결과** 창을 표시할 보조 서버를 선택합니다.

작업 실행 결과에 대한 정보 필터링 구성

Kaspersky Security Center에서는 그룹 작업, 특정 기기 및 중앙 관리 서버 작업의 결과에 관한 정보를 필터링할 수 있습니다. 로컬 작업에는 필터링을 사용할 수 없습니다.

작업 실행 결과에 대한 정보의 필터링을 필터링하려면 다음과 같이 하십시오:

1. 작업 속성 창에서 **일반** 섹션을 선택합니다.
2. **결과** 링크를 눌러 **작업 결과** 창을 엽니다.

   상단의 표에는 작업이 할당된 모든 기기 목록이 모두 포함되어 있습니다. 하단의 표에는 선택한 기기에서 수행한 작업 결과가 표시됩니다.
3. 관련 테이블을 오른쪽 클릭해서 마우스 오른쪽 메뉴를 열고 **필터**를 선택합니다.
4. **필터 설정** 창이 열리면 **이벤트**, **기기** 및 **시간** 섹션에서 필터 설정을 정의합니다. **확인**를 누릅니다.

   그러면 **작업 결과** 창에 필터에 지정된 설정을 충족하는 정보가 표시됩니다.

작업 수정. 변경 사항 롤백

작업을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **작업** 폴더의 작업 영역에서 작업을 선택하고 마우스 오른쪽 메뉴를 사용하여 작업 속성 창으로 이동합니다.

3. 적절히 변경합니다.

> **작업 제외 그룹** 섹션에서 작업을 적용하지 않을 하위 그룹 목록을 설정할 수 있습니다.

4. **적용**을 누릅니다.

   작업 변경 사항이 작업 속성 창의 **리비전 내역** 섹션에 저장됩니다.

필요한 경우 작업 변경 사항을 롤백할 수 있습니다.

작업 변경 사항을 롤백하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. 변경 사항을 롤백해야 하는 작업을 선택한 후 마우스 오른쪽 메뉴를 사용하여 작업 속성 창으로 이동합니다.
3. 작업 속성 창에서 **리비전 내역** 섹션을 선택합니다.
4. 작업 수정 목록에서 변경 사항을 롤백해야 하는 수정의 번호를 선택합니다.
5. **고급** 버튼을 누르고 드롭다운 목록에서 **롤백** 값을 선택합니다.

작업 비교

두 악성 코드 검사 작업을 비교하는 등 같은 유형의 여러 작업을 비교할 수는 있지만, 악성 코드 검사 작업과 업데이트 설치 작업을 비교할 수는 없습니다. 비교 후에는 작업에서 일치하는 설정과 서로 다른 설정이 표시된 리포트가 제공됩니다. 작업 비교 리포트는 인쇄하거나 파일로 저장할 수 있습니다. 회사 내의 각 단위에 같은 유형의 여러 작업이 할당된 경우 작업을 비교해야 할 수 있습니다. 예를 들어 회계 부서의 직원은 기기의 로컬 디스크에서만 악성 코드를 검사하는 반면, 영업 부서의 직원들은 고객과 정보를 교환하므로 로컬 디스크와 이메일을 모두 검사해야 할 수 있습니다. 모든 작업 설정을 확인하지 않더라도 작업만 비교하면 이러한 차이를 바로 확인할 수 있습니다.

> 같은 유형의 작업만 비교할 수 있습니다.

> 작업은 쌍으로만 비교할 수 있습니다.

작업 하나를 선택하여 다른 작업과 비교하거나, 작업 목록에서 원하는 두 작업을 비교하는 방식 중 하나로 작업을 비교할 수 있습니다.

작업 하나를 선택하여 다른 작업과 비교하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **작업** 폴더의 작업 영역에서 다른 작업과 비교해야 하는 작업을 선택합니다.
3. 작업의 마우스 오른쪽 메뉴에서 **모든 작업** → **다른 작업과 비교**를 선택합니다.

4. **작업 선택** 창에서 비교할 작업을 선택합니다.

5. **확인**를 누릅니다.

   두 작업을 비교하는 HTML 형식 리포트가 표시됩니다.

작업 목록에서 두 작업을 비교하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.

2. **작업** 폴더의 작업 목록에서 **SHIFT** 또는 **CTRL** 키를 눌러 같은 유형의 두 작업을 선택합니다.

3. 마우스 오른쪽 메뉴에서 **비교**를 선택합니다.

   선택한 작업을 비교하는 HTML 형식 리포트가 표시됩니다.

작업 비교 시에 암호가 다르면 작업 비교 리포트에 별표(******)가 표시됩니다.

작업 속성에서 암호를 변경한 경우 리비전 비교 리포트에 별표(******)가 표시됩니다.

작업을 시작할 계정

작업을 실행해야 할 계정을 지정할 수 있습니다.

예를 들어 수동 검사 작업을 수행하려면 검사할 개체에 대한 접근 권한이 필요하고, 업데이트 작업을 수행하려면 승인된 프록시 서버 사용자 권한이 필요합니다. 작업 실행 계정을 지정함으로써 필요한 접근 권한이 없는 사용자가 수동 검사 작업과 업데이트 작업을 실행하여 발생하는 문제를 방지할 수 있습니다.

네트워크 에이전트가 설치되어 있지 않거나 사용 가능하지 않은 경우 원격 설치/제거 작업이 실행되는 동안 지정된 계정을 사용하여 애플리케이션을 설치 및 제거하는데 필요한 파일을 클라이언트 기기에 다운로드합니다. 네트워크 에이전트가 설치되어 있고 사용 가능하며, 작업 설정에 따라 Microsoft Windows 유틸리티를 사용하여 공유 폴더에서만 파일 전달이 수행되는 경우 이 계정이 사용됩니다. 이 경우, 해당 계정은 기기에서 다음과 같은 권한을 가지고 있어야 합니다:

- 애플리케이션을 원격으로 시작할 수 있는 권한.
- Admin$ 리소스를 사용할 수 있는 권한.
- *서비스로 로그온*할 수 있는 권한.

네트워크 에이전트를 통해 파일이 기기로 전달되는 경우에는 이 계정이 사용되지 않습니다. 이 경우 **네트워크 에이전트**(**LocalSystem 계정**)에서 모든 파일 복사 및 설치 작업을 수행합니다.

작업 실행 기록 내보내기

작업에 문제가 발생하면 근본적인 이유를 조사해야 할 수도 있습니다. 이를 위해 작업 실행 기록을 내보내고 추가로 분석할 수 있습니다.

작업 실행 기록을 내보내려면:

1. 기기의 디렉터리에 빈 TXT 파일을 만듭니다.
   작업 실행 내역이 이 파일에 내보내 집니다.
2. 작업 결과 창을 엽니다.
3. 작업 결과 창 상단에서 문제가 발생한 기기를 선택합니다.
4. 선택한 기기의 실행 기록이 표시되는 작업 결과 창 하단에서 하나 이상의 이벤트를 선택합니다.
   여러 이벤트를 선택하려면 **Shift**나 **Ctrl** 키를 사용합니다.
5. 선택한 이벤트를 오른쪽 클릭해서 마우스 오른쪽 메뉴를 열고 **내보내기**를 선택합니다.
   이벤트 내보내기 마법사가 시작됩니다.
6. 마법사의 **파일 내보내기** 단계에서 **찾기** 버튼을 클릭한 다음, 작업 실행 기록을 내보내기 위해 만든 TXT 파일을 선택합니다.
   선택한 이벤트만 내보내려면 **선택한 이벤트만 내보내기** 옵션을 활성화합니다.
   작업 실행의 전체 기록(모든 이벤트)을 내보내려면 **선택한 이벤트만 내보내기** 옵션을 비활성화해야 합니다.
7. **다음** 버튼을 누릅니다.
8. 마법사의 **내보내기 형식** 단계에서 다음 옵션 중 하나를 활성화합니다.
   - **탭으로 구분한 유니코드 텍스트로 내보내기**
     내보낸 데이터가 여러 언어의 특수 문자와 부호를 포함하고, 내보낸 데이터가 있는 TXT 파일을 다른 애플리케이션에서 열 때 모든 문자가 정확하게 보존되도록 하려면 이 옵션을 활성화합니다.
   - **탭으로 구분한 텍스트로 내보내기**
     유니코드를 지원하지 않는 이전 시스템이나 애플리케이션과의 호환성을 유지하려면 이 옵션을 활성화합니다.
9. **다음** 버튼을 눌러 마법사를 완료합니다.

작업 실행 내역이 선택한 TXT 파일로 내보내집니다.

작업 암호 변경 마법사

로컬이 아닌 작업의 경우 작업을 실행해야 하는 계정을 지정할 수 있습니다. 계정은 작업 생성 중 또는 기존 작업의 속성에서 지정할 수 있습니다. 지정된 계정이 조직의 보안 지침에 따라 사용되는 경우 이 지침에 따라 암호를 한 번씩 변경해야 할 수도 있습니다. 계정 암호가 만료되어 새 암호를 설정하면 작업 속성에서 유효한 새 암호를 지정해 주기 전까지 작업이 시작되지 않습니다.

작업 암호 변경 마법사를 이용하면 해당 계정이 지정되어 있는 모든 작업에서 이전 암호를 새 암호로 자동 교체할 수 있습니다. 아니면, 각 작업의 속성에서 수동으로 교체할 수 있습니다.

작업 암호 변경 마법사를 시작하려면:

1. 콘솔 트리에서 **작업** 노드를 선택합니다.
2. 노드의 마우스 오른쪽 메뉴에서 **작업 암호 변경 마법사**를 선택합니다.

마법사의 지침을 따릅니다.

1단계. 자격증명 지정

계정 및 **암호** 필드에서 시스템(예: Active Directory)에서 현재 유효한 새 자격증명을 지정합니다. 마법사의 다음 단계로 넘어갈 때 Kaspersky Security Center가 지정된 계정 이름이 각 로컬이 아닌 작업의 속성에 있는 계정 이름과 일치하는지 확인합니다. 계정 이름이 일치하면 작업 속성의 암호가 새 암호로 자동 교체됩니다.

이전 암호(옵션) 필드를 작성하면 Kaspersky Security Center가 계정 이름과 이전 암호가 모두 발견된 작업에 대해서만 암호를 교체합니다. 교체는 자동으로 수행됩니다. 기타 다른 경우에는 마법사의 다음 단계에서 수행할 작업을 선택해야 합니다.

2단계. 수행할 작업 선택

마법사의 첫 단계에서 이전 암호를 지정하지 않았거나 지정한 이전 암호가 작업의 암호와 일치하지 않을 시, 검색된 작업에 대해 수행할 행동을 선택해야 합니다.

승인 필요 상태의 각 작업에 대해 작업 속성에서 암호를 제거할지, 또는 이를 새 암호로 교체할지 결정합니다. 암호 제거를 선택하면 작업은 기본 계정에서 실행되도록 전환됩니다.

3단계. 결과 확인

마법사의 마지막 단계에서 발견된 각 작업의 결과를 확인합니다. 마법사를 완료하려면 **마침** 버튼을 클릭합니다.

가상 중앙 관리 서버에 종속되는 관리 그룹의 계층 구조 생성

가상 중앙 관리 서버가 만들어지면 여기에 **관리 중인 기기**이라는 이름의 관리 그룹이 기본적으로 포함됩니다.

가상 중앙 관리 서버에 속한 관리 그룹의 계층 구조를 만드는 절차는 물리 중앙 관리 서버에 속한 관리 그룹의 계층 구조를 만드는 절차와 동일합니다.

보조 및 가상 중앙 관리 서버는 가상 중앙 관리 서버에 속하는 관리 그룹에 추가할 수 없습니다. 이는 가상 중앙 관리 서버의 제한 때문입니다.

정책 및 정책 프로필

Kaspersky Security Center 웹 콘솔에서는 Kaspersky 애플리케이션용 정책을 만들 수 있습니다. 이 섹션에서는 정책 및 정책 프로필을 설명하고 정책을 만들고 수정하기 위한 지침을 제공합니다.

정책 프로필을 사용하는 정책 계층 구조

이 섹션에서는 관리 그룹에 있는 기기에 정책을 적용하게 하는 방법에 대한 정보를 제공합니다. 이 섹션에서는 정책 프로필에 대한 정보도 제공합니다.

정책 계층 구조

Kaspersky Security Center에서는 정책을 사용해 여러 기기에 대해 단일 설정 모음을 정의합니다. 예를 들어 관리 그룹 G에 대해 정의된 애플리케이션 P의 정책 범위에는 그룹 G와 그 하위 그룹에 배포되었으며 애플리케이션 P가 설치된 관리 중인 기기가 포함됩니다. 단, 속성에서 **부모 그룹에서 상속** 확인란 선택을 취소한 하위 그룹은 제외됩니다.

정책은 로컬 설정과 달리 해당 설정 옆에 자물쇠 아이콘()이 있습니다. 설정이나 설정 그룹이 정책 속성에서 잠금 상태인 경우에는 먼저 유효 설정을 만들 때 이 설정이나 설정 그룹을 사용해야 하며, 둘째로는 해당 설정이나 설정 그룹을 다운스트림 정책에 기록해야 합니다.

기기에서 유효 설정을 만드는 과정은 다음과 같이 설명할 수 있습니다: 잠금 상태가 아닌 모든 설정의 값을 정책에서 가져온 다음 로컬 설정의 값으로 덮어씁니다. 그런 후에 생성된 모음을 정책에서 가져온 "잠금" 상태의 설정 값으로 덮어씁니다.

동일 애플리케이션의 정책은 관리 그룹 계층 구조를 통해 서로 영향을 줍니다: 업스트림 정책에 있는 잠금 상태의 설정은 다운스트림 정책의 동일 설정을 덮어씁니다.

이동 사용자를 위한 특수 정책이 있습니다. 이 정책은 이동 사용자 모드로 전환되는 기기에 적용됩니다. 이동 사용자 정책은 관리 그룹 계층 구조를 통해 다른 정책에 영향을 주지 않습니다.

정책 프로필

대부분의 상황에서는 관리 그룹 계층 구조만을 통해 기기에 정책을 적용하는 방식이 불편할 수 있습니다. 즉, 각 관리 그룹용으로 설정이 한두 개만 다른 단일 정책의 여러 인스턴스를 만들고 나중에 해당 정책의 컨텐츠를 동기화해야 할 수 있습니다.

이러한 문제를 방지하기 위해 Kaspersky Security Center는 *정책 프로필*을 지원합니다. 정책 프로필은 정책 설정의 명명된 하위 집합입니다. 이 하위 집합은 정책과 함께 대상 기기에 배포되며 *프로필 활성화 조건*이라는 특수 조건에서 정책을 보완합니다. 클라이언트 기기(컴퓨터 또는 모바일 기기)에서 활성 상태인 "기본" 정책과 다른 설정만 프로필에 포함됩니다. 프로필을 활성화하면 프로필 활성화 전에 기기에서 활성 상태였던 정책 설정이 수정됩니다. 해당 설정은 프로필에 지정된 값을 사용합니다.

현재 정책 프로필에 적용되는 제한은 다음과 같습니다:

- 프로필은 정책당 100개까지 포함할 수 있습니다.
- 정책 프로필은 다른 프로필을 포함할 수 없습니다.
- 정책 프로필은 알림 설정을 포함할 수 없습니다.

프로필의 컨텐츠

정책 프로필에는 다음과 같은 구성 요소가 포함됩니다:

- 이름. 이름이 같은 프로필은 공통 규칙에 따라 관리 그룹의 계층을 통해 서로 영향을 줍니다.
- 정책 설정의 하위 집합. 모든 설정을 포함하는 정책과 달리 프로필은 실제로 필요한 설정(잠금 상태의 설정)만 포함합니다.
- 활성화 조건은 기기 속성이 포함된 논리식입니다. 프로필은 프로필 활성화 조건이 참일 때만 활성화되어 정책을 보완합니다. 기타 모든 경우에는 프로필이 비활성 상태이며 무시됩니다. 이 논리식에 포함할 수 있는 기기 속성은 다음과 같습니다:
  - 이동 사용자 모드의 상태.
  - 네트워크 환경의 속성 – 네트워크 에이전트 연결에 대한 활성화 규칙의 이름.
  - 기기에서 지정된 태그의 유무.
  - Active Directory 단위에서의 기기 할당: 명시적(기기가 지정된 OU에 직접 포함되어 있음) 또는 암묵적(기기가 특정 중첩 레벨에서 지정된 OU 내에 있는 OU에 포함되어 있음).
  - Active Directory 보안 그룹에 있는 기기 구성원 (명시적 또는 암묵적).
  - Active Directory 보안 그룹에 있는 기기 소유자 구성원 (명시적 또는 암묵적).
- 프로필 중지 확인란. 중지된 프로필은 항상 무시되며, 해당 프로필의 개별 활성화 조건을 확인하지 않습니다.
- 프로필 우선 순위. 개별 프로필의 활성화 조건은 서로 독립적이므로 여러 프로필을 동시에 활성화할 수 있습니다. 활성 프로필에 겹치지 않는 설정 모음이 포함되어 있으면 문제가 발생하지 않습니다. 그러나 두 활성 프로필에 동일 설정의 서로 다른 값이 포함되어 있으면 프로필이 모호해집니다. 프로필 우선 순위를 활용하여 이와 같은 모호한 프로필을 방지할 수 있습니다: 모호한 변수의 값을 우선 순위가 더 높은 프로필(프로필 목록에서 순위가 더 높은 프로필)에서 가져옵니다.

정책이 계층 구조를 통해 서로 영향을 줄 때의 프로필 동작

이름이 같은 프로필은 정책 병합 규칙에 따라 병합됩니다. 업스트림 정책의 프로필이 다운스트림 정책의 프로필보다 우선 순위가 높습니다. 업스트림 정책에서 설정 편집이 금지된 경우, 즉 설정이 잠금 상태인 경우 다운스트림 정책은 업스트림 정책의 프로필 활성화 조건을 사용합니다. 업스트림 정책에서 설정 편집이 허용되는 경우에는 다운스트림 정책의 프로필 활성화 조건이 사용됩니다.

정책 프로필의 활성화 조건에는 **오프라인 상태인 기기** 속성이 포함될 수 있으므로 이동 사용자를 위한 정책의 기능은 프로필로 완전히 교체되며 더 이상 지원되지 않습니다.

이동 사용자를 위한 정책은 프로필을 포함할 수 있지만 해당 프로필은 기기가 이동 사용자 모드로 전환된 후에만 활성화할 수 있습니다.

정책 설정 상속

정책은 관리 그룹에 대해 지정됩니다. 정책 설정은 *상속*될 수 있습니다. 즉, 정책 설정이 지정된 관리 그룹의 하위 그룹(자식 그룹)이 해당 설정을 수신할 수 있습니다. 아래에서는 부모 그룹의 정책이 *부모 정책*으로도 지칭됩니다.

두 가지 상속 옵션을 활성화하거나 비활성화할 수 있습니다. **그 중 하나는 부모 정책의 설정 상속이고 다른 하나는 자식 정책에 설정 강제 상속입니다**:

- 자식 정책에 대해 **부모 정책의 설정 상속**을 활성화하고 부모 정책에서 일부 설정을 잠금 상태로 설정하면 자식 그룹에서 해당 설정을 변경할 수 없습니다. 하지만 부모 정책에서 잠금 상태가 아닌 설정은 변경할 수 있습니다.
- 자식 정책에 대해 **부모 정책의 설정 상속**을 비활성화하면 부모 정책에서 일부 설정이 잠금 상태이더라도 자식 그룹의 모든 설정을 변경할 수 있습니다.
- 부모 그룹에서 **자식 정책에 설정 강제 상속**을 활성화하면 각 자식 정책에 대해 **부모 정책의 설정 상속**이 활성화됩니다. 이 경우에는 모든 자식 정책에 대해 이 옵션을 비활성화할 수 없습니다. 부모 정책에서 잠겨 있는 모든 설정이 자식 그룹에서 강제로 상속되며 자식 그룹에서 이러한 설정을 변경할 수 없습니다.
- **관리 중인 기기** 그룹의 정책에서 **부모 정책의 설정 상속**은 어떤 설정에도 영향을 주지 않습니다. **관리 중인 기기** 그룹에는 어떤 업스트림 그룹도 없으므로 정책을 상속하지 않기 때문입니다.

기본적으로 새 정책에 대해서는 **부모 정책의 설정 상속** 옵션이 활성화됩니다.

정책에 프로필이 있으면 모든 자식 정책이 해당 프로필을 상속합니다.

정책 관리

클라이언트 기기에 설치된 애플리케이션은 정책 구성을 통해 중앙 집중식으로 구성됩니다.

관리 그룹에서 애플리케이션에 대해 만든 정책은 작업 영역의 **정책** 탭에 표시됩니다. 각 정책 이름 앞에는 상태를 나타내는 아이콘이 표시됩니다.

정책을 삭제하거나 취소해도 애플리케이션은 계속 정책에 지정된 설정을 사용하여 작동합니다. 이러한 설정은 이후에 수동으로 수정할 수 있습니다.

정책을 적용할 경우 기기가 상주 작업(실시간 보호 작업)을 실행 중이라면 새로운 설정 값으로 중단 없이 작동을 계속할 수 있습니다. 이미 시작된 정기적인 작업(수동 검사, 애플리케이션 데이터베이스 업데이트)이 있는 경우에는 값이 변경되지 않고 계속 실행됩니다. 다음번에 새로운 설정 값으로 실행됩니다.

멀티테넌시가 지원되는 애플리케이션용 정책은 하위 레벨 관리 그룹과 상위 레벨 관리 그룹에 모두 상속됩니다. 정책은 애플리케이션이 설치된 모든 클라이언트 기기로 전파됩니다.

중앙 관리 서버가 계층 구조로 되어 있는 경우, 보조 중앙 관리 서버가 기본 중앙 관리 서버에서 정책을 받아 클라이언트 기기에 배포합니다. 상속이 활성화되어 있는 경우 기본 중앙 관리 서버에서 정책 설정을 수정할 수 있습니다. 그러면 정책 설정에 대한 모든 변경 내용이 보조 중앙 관리 서버에 상속된 정책으로 배포됩니다.

기본과 보조 중앙 관리 서버 사이의 연결이 끊어지면 적용된 설정을 사용하여 보조 서버의 정책이 계속 시행됩니다. 이때 기본 중앙 관리 서버에서 수정된 정책 설정은 다시 연결된 이후 보조 중앙 관리 서버로 배포됩니다.

상속이 비활성화되어 있는 경우에는 기본 중앙 관리 서버와 관계없이 보조 중앙 관리 서버에서 독립적으로 정책 설정을 수정할 수 있습니다.

중앙 관리 서버와 클라이언트 기기 사이의 연결이 끊어지면 클라이언트 기기가 이동 사용자 정책(정의된 경우)으로 작업을 시작하거나, 다시 연결될 때까지 이전에 적용된 설정을 사용하여 정책을 계속 시행합니다.

보조 중앙 관리 서버에 정책을 배포한 결과는 기본 중앙 관리 서버 콘솔의 정책 속성 창에 표시됩니다.

클라이언트 기기에 정책을 배포한 결과는 해당 컴퓨터가 연결된 중앙 관리 서버의 정책 속성 창에 표시됩니다.

정책 설정에서 기밀 데이터를 사용하지 마십시오. 예를 들어, 도메인 관리자 암호를 지정하지 마십시오.

정책 만들기

관리 콘솔에서 정책을 만들어야 하는 관리 그룹의 폴더 또는 **정책** 폴더의 작업 영역에서 직접 정책을 만들 수 있습니다.

관리 그룹의 폴더에서 정책을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 정책을 만들 관리 그룹을 선택합니다.
2. 그룹의 작업 영역에서 **정책** 탭을 선택합니다.
3. **새 정책** 버튼을 눌러 새 정책 마법사를 실행합니다.

   새 정책 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

***정책** 폴더의 작업 영역에서 정책을 만들려면 다음과 같이 하십시오:*

1. 콘솔 트리에서 **정책** 폴더를 선택합니다.
2. **새 정책** 버튼을 눌러 새 정책 마법사를 실행합니다.

   새 정책 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

그룹의 한 애플리케이션에 대해 여러 정책을 만들 수 있지만 한 번에 하나의 정책만 활성 상태일 수 있습니다. 새 활성 정책을 만들면 이전의 활성 정책은 비활성화됩니다.

정책을 만들 때 애플리케이션의 올바른 작동에 필요한 최소 파라미터 집합을 지정할 수 있습니다. 다른 모든 값은 애플리케이션을 로컬에서 설치할 때 적용되는 기본값으로 설정됩니다. 정책은 만든 후에 변경할 수 있습니다.

정책 설정에서 기밀 데이터를 사용하지 마십시오. 예를 들어, 도메인 관리자 암호를 지정하지 마십시오.

정책을 적용한 후 변경되는 Kaspersky 애플리케이션 설정에 대한 내용은 해당 설명서에 자세히 설명되어 있습니다.

정책이 생성된 이후에 편집이 차단된 설정(잠금 아이콘 표시(🔒))은 이전에 해당 애플리케이션에서 지정된 설정과 상관없이 클라이언트 기기에 적용됩니다.

하위 그룹에 상속된 정책 표시

중첩된 관리 그룹에 대한 상속된 정책을 표시하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 상속된 정책을 표시해야 하는 관리 그룹을 선택합니다.
2. 선택한 그룹의 작업 영역에서 **정책** 탭을 엽니다.
3. 정책 목록의 마우스 오른쪽 메뉴에서 **보기 → 상속된 정책**을 선택합니다.

상속된 정책이 다음 아이콘과 함께 정책 목록에 표시됩니다:

-  —기본 중앙 관리 서버에 생성한 그룹에서 상속 시.
-  —최상위 그룹에서 상속 시.

설정 상속 모드가 활성화된 경우, 상속된 정책은 해당 정책이 만들어진 그룹에서만 수정할 수 있습니다. 이 정책을 상속하는 그룹에서는 상속된 정책을 수정할 수 없습니다.

정책 활성

선택한 그룹에 대해 정책을 활성화하려면 다음과 같이 하십시오:

1. 그룹의 작업 영역에 있는 **정책** 탭에서 활성화할 정책을 선택합니다.
2. 정책을 활성화하려면 다음 작업 중 하나를 수행합니다:
   - 정책의 마우스 오른쪽 메뉴에서 **활성 정책**을 선택합니다.
   - 정책 속성 창에서 **일반** 섹션을 열고 **정책 상태** 설정 그룹에서 **활성 정책**를 선택합니다.

선택한 관리 그룹에 대해 정책이 활성화됩니다.

정책이 많은 클라이언트 기기에 적용될 경우 일정 기간 중앙 관리 서버의 부하와 네트워크 트래픽이 모두 상당히 증가합니다.

바이러스 급증 이벤트 시 자동으로 정책 활성화

바이러스 급증 이벤트 시 정책이 자동으로 활성화되도록 하려면 다음과 같이 하십시오:

1. 중앙 관리 서버 속성 창에서 **바이러스 발생** 섹션을 엽니다.
2. **바이러스 발생 이벤트 발생 시 활성화할 정책 구성** 링크를 눌러 **정책 활성화** 창을 열고 바이러스 급증이 탐지될 때 활성화되는 정책의 선택한 목록에 정책을 추가합니다.

바이러스 급증 이벤트 시 특정 정책이 활성화된 경우, 수동 모드를 사용해야만 이전 정책으로 돌아갈 수 있습니다.

이동 사용자 정책 적용

이동 사용자 정책은 기업 네트워크의 연결이 끊어지는 경우 기기에 적용됩니다.

이동 사용자 정책을 적용하려면:

정책 속성 창에서 **일반** 섹션을 열고 **정책 상태** 설정 그룹에서 **이동 사용자 정책**를 선택합니다.

회사 네트워크에서 연결이 끊어지는 경우 이동 사용자 정책이 기기에 적용됩니다.

정책 수정. 변경 사항 롤백

정책을 수정하려면 다음 단계를 따릅니다.

1. 콘솔 트리에서 **정책** 폴더를 선택합니다.
2. **정책** 폴더의 작업 영역에서 정책을 선택하고 마우스 오른쪽 메뉴를 사용하여 정책 속성 창으로 이동합니다.
3. 적절히 변경합니다.
4. **적용**을 누릅니다.

정책 변경 사항이 정책 속성의 **리비전 내역** 섹션에 저장됩니다.

필요한 경우 정책 변경 사항을 롤백할 수 있습니다.

정책 변경 사항을 롤백하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **정책** 폴더를 선택합니다.
2. 변경 사항을 롤백해야 하는 정책을 선택한 후 마우스 오른쪽 메뉴를 사용하여 정책 속성 창으로 이동합니다.
3. 정책 속성 창에서 **리비전 내역** 섹션을 선택합니다.
4. 정책 수정 목록에서 변경 사항을 롤백해야 하는 리비전 번호를 선택합니다.
5. **고급** 버튼을 누르고 드롭다운 목록에서 **롤백** 값을 선택합니다.

정책 비교

단일 관리 애플리케이션의 두 정책을 비교할 수 있습니다. 비교 후에는 정책에서 일치하는 설정과 서로 다른 설정이 표시된 리포트가 만들어집니다. 예를 들어 여러 관리자가 각 사무소에서 단일 관리 애플리케이션용으로 여러 정책을 만든 경우나 단일 최상위 정책을 모든 지역 사무소에서 상속한 후 각 사무소용으로 수정한 경우에는 정책을 비교해야 합니다. 정책 하나를 선택하여 다른 정책과 비교하거나, 정책 목록에서 원하는 두 정책을 비교하는 방식 중 하나로 정책을 비교할 수 있습니다.

수정 기록에 현재 수정이 있는 정책만 비교할 수 있습니다.

한 정책을 다른 정책과 비교하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **정책** 폴더를 선택합니다.
2. **정책** 폴더의 작업 영역에서 다른 정책과 비교해야 하는 정책을 선택합니다.
3. 정책의 마우스 오른쪽 메뉴에서 **정책을 다른 정책과 비교**를 선택합니다.
4. **정책 선택** 창에서 이 정책과 비교해야 하는 정책을 선택합니다.
5. **확인**를 누릅니다.

   동일 애플리케이션에 대해 두 정책을 비교할 수 있는 HTML 형식 리포트가 표시됩니다.

정책 목록에서 두 정책을 비교하려면 다음과 같이 하십시오:

1. **정책** 폴더의 정책 목록에서 **SHIFT** 또는 **CTRL** 키를 사용하여 단일 관리 애플리케이션용 정책 두 개를 선택합니다.
2. 마우스 오른쪽 메뉴에서 **비교**를 선택합니다.

   동일 애플리케이션에 대해 두 정책을 비교할 수 있는 HTML 형식 리포트가 표시됩니다.

Kaspersky Endpoint Security for Windows의 정책 설정 비교 리포트에서는 정책 프로필 비교 세부 정보도 제공됩니다. 정책 프로필 비교 결과는 최소화할 수 있습니다. 해당 섹션을 최소화하려면 해당 섹션 이름 옆의 화살표 아이콘( )을 누릅니다.

정책 배포 상태 차트 보기

Kaspersky Security Center에서 각 기기의 정책 시행 결과를 볼 수 있습니다.

각 기기에서 정책 배포 상태를 보려면 다음 단계를 따릅니다.

1. 그룹 작업 공간의 **정책** 탭에서 배포 상태를 확인할 정책을 선택합니다.
   오른쪽 창의 차트는 정책 시행의 개요를 표시합니다.
2. **자세히**를 클릭합니다.
   정책 배포 결과 창이 열립니다.
   정책 시행 결과를 CSV 또는 TXT 파일로 내보낼 수 있습니다.

정책 삭제

정책을 삭제하려면:

1. 관리 그룹의 작업 영역에 있는 **정책** 탭에서 삭제할 정책을 선택합니다.
2. 다음 방법 중 하나로 정책을 삭제합니다:
   - 정책의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
   - 선택한 정책의 정보 박스에서 **정책 삭제** 링크를 누릅니다.

정책 복사

정책을 복사하려면 다음과 같이 하십시오:

1. 필요한 그룹의 작업 영역에 있는 **정책** 탭에서 정책을 선택합니다.
2. 정책의 마우스 오른쪽 메뉴에서 **복사**를 선택합니다.
3. 콘솔 트리에서 정책을 추가할 그룹을 선택합니다.
   정책이 복사된 원본 그룹에 해당 정책을 추가할 수도 있습니다.
4. 선택한 그룹에 대한 정책 목록의 마우스 오른쪽 메뉴에 있는 **정책** 탭에서 **붙여넣기**를 선택합니다.

그러면 모든 설정과 함께 정책이 복사되고, 정책이 복사된 그룹에 소속된 기기에 적용됩니다. 정책이 복사된 원본 그룹에 해당 정책을 붙여넣으면 정책 이름에 **(<순차적 번호>)** 색인이 자동으로 추가됩니다. 예: **(1)**, **(2)**.

활성 정책은 복사하는 동안 비활성됩니다. 필요한 경우 활성할 수 있습니다.

정책 내보내기

정책을 내보내려면 다음과 같이 하십시오:

1. 다음 방법 중 하나로 정책을 내보냅니다:
   - 정책의 마우스 오른쪽 메뉴에서 **모든 작업 → 내보내기**를 선택합니다.
   - 선택한 정책의 정보 상자에서 **파일로 정책 내보내기** 링크를 누릅니다.
2. **다른 이름으로 저장** 창이 열리면 정책 파일의 이름과 경로를 지정합니다. **저장** 버튼을 누릅니다.

정책 가져오기

정책을 가져오려면 다음과 같이 하십시오:

1. 관련 그룹의 작업 영역에 있는 **정책** 탭에서 다음과 같은 정책 가져오기 방법 중 하나를 선택합니다:
   - 정책 목록의 마우스 오른쪽 메뉴에서 **모든 작업** → **가져오기**를 선택합니다.
   - 정책 목록에 대한 관리 블록에서 **파일에서 정책 가져오기** 버튼을 누릅니다.
2. 열리는 창에서 정책을 가져올 파일 경로를 지정합니다. **열기** 버튼을 누릅니다.

가져온 정책이 정책 목록에 표시됩니다. 정책의 설정 및 프로필도 가져옵니다. 내보내기 중에 선택한 정책 상태에 관계없이 가져온 정책은 비활성 상태입니다. 정책 속성에서 정책 상태를 변경할 수 있습니다.

새로 가져온 정책의 이름이 기존 정책과 같다면, 가져온 정책의 이름은 **(<다음 시퀀스 번호>)** 인덱스로 확장됩니다(예: **(1)**, **(2)**).

정책 변환

Kaspersky Security Center는 이전 버전 Kaspersky 애플리케이션의 정책을 같은 애플리케이션 최신 버전의 정책으로 변환할 수 있습니다. 변환된 정책은 업데이트 전에 지정된 현재 관리자 설정을 유지하고 최신 버전 애플리케이션의 새 설정을 포함합니다. 정책이 최신 버전의 관리 중인 Kaspersky 애플리케이션으로 변환되면, 이전 버전의 애플리케이션 플러그인이 설치된 중앙 관리 서버에서 해당 정책을 열 수 없습니다. Kaspersky 애플리케이션용 관리 플러그인은 이러한 애플리케이션의 정책에 대해 변환이 가능한지 결정합니다. 지원하는 각 Kaspersky 애플리케이션의 정책 변환에 대한 정보는 다음 목록에서 관련 도움말을 참조하십시오:

- **워크스테이션용 Kaspersky 애플리케이션:**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial Cybersecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (중앙 집중식 배포는 지원되지 않음)

- **모바일 기기용 Kaspersky 애플리케이션:**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **파일 서버용 Kaspersky 애플리케이션:**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **가상 컴퓨터용 Kaspersky 애플리케이션:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless
- **메일 시스템 및 SharePoint/협업 서버용 Kaspersky 애플리케이션:**
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **표적 공격 탐지용 Kaspersky 애플리케이션:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **KasperskyOS 기기용 Kaspersky 애플리케이션:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (Kaspersky Thin Client용 플러그인)

정책을 변환하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 정책을 변환할 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버 마우스 오른쪽 메뉴에서 **모든 작업 → 정책 및 작업 변환 마법사**를 선택합니다.

   정책 및 작업 일괄 변환 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

마법사가 완료되면 현재 관리자의 정책 설정과 최신 버전 Kaspersky 애플리케이션의 새 설정을 사용하는 새 정책이 생성됩니다.

정책 프로필 관리

정책 프로필은 기기가 특정 활성화 규칙 조건이 충족되면 클라이언트 기기(컴퓨터 또는 모바일 기기)에서 활성화되는 정책 설정의 집합을 말합니다. 프로필을 활성화하면 프로필 활성화 전에 기기에서 활성 상태였던 정책 설정이 수정됩니다. 해당 설정은 프로필에 지정된 값을 사용합니다.

정책 프로필은 단일 관리 그룹 내의 기기가 다른 정책 설정으로 실행될 수 있도록 하기 위해 필요합니다. 예를 들어, 관리 그룹의 일부 기기에 대한 정책 설정을 수정해야 하는 상황이 발생할 수 있습니다. 이 경우 해당 정책의 정책 프로필을 구성할 수 있으므로 관리 그룹에서 선택한 기기에 대한 정책 설정을 편집할 수 있습니다. 예를 들어, 특정 정책은 사용자 관리 그룹의 모든 기기에 대해 GPS 네비게이션 소프트웨어 실행을 금지합니다. GPS 네비게이션 소프트웨어는 사용자 관리 그룹에 있는 하나의 기기, 특히 배달원으로 고용된 직원이 소유한 기기에 필요합니다. 해당 기기를 "배달원"으로 태그를 지정하고 정책 프로필을 다시 구성하여 나머지 모든 정책 설정을 유지하면서 GPS 네비게이션 소프트웨어를 "배달원"으로 태그가 지정된 기기에서만 실행할 수 있게 할 수 있습니다. 이 경우 "배달원"으로 태그가 지정된 기기가 사용자 관리 그룹에 나타나면 GPS 네비게이션 소프트웨어를 실행할 수 있습니다. "배달원" 태그가 지정되어 있지 않으면 사용자 관리 그룹의 다른 기기에서는 GPS 네비게이션 소프트웨어를 실행할 수 없습니다.

다음 정책에서만 프로필 기능이 지원됩니다:

- Kaspersky Endpoint Security for Windows 정책
- Kaspersky Endpoint Security for Mac 정책
- 10 Service Pack 1 버전에서부터 10 Service Pack 3 Maintenance Release 1 버전에 해당하는 Kaspersky 모바일 기기 관리 플러그인으로 만든 정책
- Kaspersky Device Management for iOS 플러그인으로 만든 정책
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows의 정책
- Kaspersky Security for Virtualization 5.1 Light Agent for Linux의 정책

정책 프로필을 사용하면 정책을 적용한 클라이언트 기기 관리를 간편하게 할 수 있습니다:

- 정책 프로필 설정은 정책 설정과 다를 수 있습니다.
- 몇 가지 설정만 다른 단일 정책의 여러 인스턴스를 유지 관리하고 수동으로 적용할 필요가 없습니다.
- 개별 이동 사용자 정책을 할당할 필요가 없습니다.
- 정책 프로필을 내보내고 가져올 수 있으며 기존 정책 프로필을 기반으로 새 정책 프로필을 만들 수도 있습니다.
- 하나의 정책에는 여러 개의 활성 정책 프로필이 있을 수 있습니다. 특정 기기에 적용되는 활성화 규칙을 충족하는 프로필만 해당 기기에 적용됩니다.
- 프로필은 정책 계층 구조를 따릅니다. 상속된 정책에는 상위 정책의 모든 프로필이 포함됩니다.

프로필 우선 순위

정책에 대해 생성된 프로필은 우선 순위의 내림차순으로 정렬됩니다. 예를 들어 프로필 X가 프로필 Y보다 프로필 목록에서 더 높으면 X는 프로필 Y보다 우선 순위가 더 높습니다. 하나의 기기에 여러 프로필을 동시에 적용할 수 있습니다. 프로필의 설정 값이 다른 경우 가장 우선 순위가 높은 프로필의 값이 기기에 적용됩니다.

프로필 활성화 규칙

활성화 규칙이 작동하면 정책 프로필이 클라이언트 기기에서 활성화됩니다. *활성화 규칙*은 조건이 일치할 경우 기기에 정책 프로필을 시작하는 조건 집합입니다. 활성화 규칙은 다음 조건을 포함할 수 있습니다:

- 클라이언트 기기에 설치된 네트워크 에이전트는 중앙 관리 서버 주소, 포트 번호 등의 지정된 연결 파라미터 세트를 사용하여 중앙 관리 서버에 연결합니다.
- 클라이언트 기기가 오프라인입니다.
- 클라이언트 기기에 지정한 태그가 할당되었습니다.
- 클라이언트 기기가 명시적으로(해당 기기가 지정된 단위에 있음) 또는 암시적으로(기기가 모든 중첩 수준에서 지정된 단위에 있음) 특정 Active Directory® 단위에 있거나 기기나 그 기기 소유자가 Active Directory의 보안 그룹에 있습니다.
- 클라이언트 기기는 지정된 소유자에게 속하거나 기기 소유자가 Kaspersky Security Center의 내부 보안 그룹에 포함되어 있습니다.
- 클라이언트 기기의 소유자에게 지정된 역할이 할당되었습니다.

관리 그룹의 계층 구조 내 정책

하위 관리 그룹에서 정책을 생성하면, 이 새 정책은 상위 그룹의 활성 정책의 모든 프로필을 상속합니다. 동일한 이름의 프로필은 병합됩니다. 상위 그룹의 정책 프로필이 더 높은 우선 순위를 갖습니다. 예를 들어 관리 그룹 *A*에서 정책 *P(A)*에 프로필 *X1*, *X2*, *X3*(우선 순위 내림차순)이 포함되어 있다고 가정해 보겠습니다. 그리고 그룹 *A*의 하위 그룹인 관리 그룹 *B*에서 프로필 *X2*, *X4*, *X5*가 포함된 정책 *P(B)*를 생성했다고 가정합니다. 그러면 *P(B)* 정책은 *P(A)* 정책을 사용하여 수정되므로 *P(B)* 정책의 프로필 목록은 다음과 같이 표시됩니다: *X1*, *X2*, *X3*, *X4*, *X5*(우선 순위 내림차순). 프로필 *X2*의 우선 순위는 정책 *P(B)*의 *X2* 및 정책 *P(A)*의 *X2* 초기 상태에 따라 달라집니다. *P(B)* 정책을 생성한 이후에는 *P(A)* 정책이 *B* 하위 그룹에 더 이상 표시되지 않습니다.

네트워크 에이전트를 시작하거나, 오프라인 모드를 사용 및 중지하거나, 클라이언트 기기에 대해 할당된 태그 목록을 편집하면 활성 정책이 다시 계산됩니다. 예를 들어, 기기의 RAM 크기가 증가되어 RAM 크기가 큰 기기에 적용되는 정책 프로필이 활성화되었습니다.

정책 프로필의 속성 및 제한

프로필에는 다음과 같은 속성이 있습니다:

- 비활성 정책의 프로필은 클라이언트 기기에 아무 영향을 주지 않습니다.
- 정책이 **이동 사용자 정책** 상태로 설정되면 기기가 회사 네트워크에서 분리될 때 정책의 프로필도 적용됩니다.
- 프로필은 실행 파일에 대한 정적 접근 분석을 지원하지 않습니다.
- 정책 프로필에는 이벤트 알림 설정이 포함될 수 없습니다.
- 15000 UDP 포트를 사용하여 기기에서 중앙 관리 서버에 연결되는 경우에는 태그를 기기에 할당한 이후 1분 이내에 해당 정책 프로필이 활성화됩니다.
- 정책 프로필 활성화 규칙을 만들 때 중앙 관리 서버에 대한 네트워크 에이전트 연결 규칙을 사용할 수 있습니다.

정책 프로필 만들기

프로필 만들기는 다음 애플리케이션의 정책에 대해서만 사용 가능합니다:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows 이상 버전
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Kaspersky 모바일 기기 관리 플러그인 버전 10 Service Pack 1 ~ 10 Service Pack 3 Maintenance Release 1
- Kaspersky Device Management for iOS 플러그인
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows 및 Linux

정책 프로필을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 정책 프로필을 만들 관리 그룹을 선택합니다.
2. 관리 그룹의 작업 영역에서 **정책** 탭을 선택합니다.
3. 정책을 선택하고 마우스 오른쪽 메뉴를 사용하여 정책 속성 창으로 전환합니다.
4. 정책 속성 창에서 **정책 프로필** 섹션을 열고 **추가** 버튼을 누릅니다.
   새 정책 프로필 마법사가 시작됩니다.
5. 마법사의 **정책 프로필 이름** 창에서 다음을 지정합니다:
   a. 정책 프로필 이름
      프로필 이름은 100자를 초과할 수 없습니다.
   b. 정책 프로필 상태(*활성됨* 또는 *비활성됨*)
      먼저 정책 프로필 활성화 설정 및 조건 작업을 완료한 후에 정책 프로필 비활성 설정을 만들고 사용하는 것이 좋습니다.
6. 새 정책 프로필 활성화 규칙 마법사를 시작하려면 **새 정책 프로필 마법사를 마친 후 정책 프로필 활성화 규칙 구성하기** 확인란을 선택합니다. 마법사의 안내를 따르십시오.
7. 정책 프로필 속성 창에서 필요한 방식으로 정책 프로필 설정을 편집합니다.
8. **확인**를 눌러 변경 사항을 저장합니다.
   프로필이 저장되었습니다. 이제 활성화 규칙을 충족하는 기기에서 프로필이 활성됩니다.

하나의 정책에 여러 개의 프로필을 만들 수 있습니다. 정책에 대해 생성된 프로필은 정책 속성의 **정책 프로필** 섹션에 표시됩니다. 정책 프로필을 수정하고 프로필 우선 순위를 변경할 수 있으며 프로필을 제거할 수도 있습니다.

정책 프로필 수정

정책 프로필 설정 편집

Kaspersky Endpoint Security for Windows의 정책에 대해서만 정책 프로필을 편집할 수 있습니다.

정책 프로필을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 정책 프로필을 수정해야 하는 관리 그룹을 선택합니다.
2. 그룹의 작업 영역에서 **정책** 탭을 선택합니다.
3. 정책을 선택하고 마우스 오른쪽 메뉴를 사용하여 정책 속성 창으로 전환합니다.
4. 정책 속성에서 **정책 프로필** 섹션을 엽니다.
   이 섹션에는 정책에 대해 생성된 프로필의 목록이 포함되어 있습니다. 프로필은 우선 순위에 따라 목록에 표시됩니다.
5. 정책 프로필을 선택하고 **속성** 버튼을 누릅니다.
6. 속성 창에서 프로필 구성:
   - 필요한 경우 **일반** 섹션에서 프로필 이름을 변경하고 **프로필 사용** 확인란을 사용하여 프로필을 사용하거나 중지합니다.
   - **활성화 규칙** 섹션에서 프로필 활성화 규칙을 편집합니다.
   - 해당 섹션에서 정책 설정을 편집합니다.
7. **확인**를 누릅니다.

수정한 설정은 기기가 중앙 관리 서버와 동기화되거나(정책 프로필이 활성 상태인 경우) 활성화 규칙을 만족해 시작한 이후에(정책 프로필이 비활성 상태인 경우)에 적용됩니다.

정책 프로필의 우선 순위 변경

정책 프로필의 우선 순위에 따라 클라이언트 기기의 프로필 활성화 순서가 정의됩니다. 동일한 활성화 규칙을 여러 정책 프로필에 대해 설정한 경우 우선 순위가 사용됩니다.

두 개의 정책 프로필이 생성되었다고 가정하겠습니다. *프로필 1*과 *프로필 2*입니다. 이 두 프로필에서는 단일 설정의 개별 값(*값 1* 및 *값 2*)이 서로 다릅니다. *프로필 1*의 우선 순위가 *프로필 2*보다 높습니다. 또한 *프로필 2*보다 우선 순위가 낮은 프로필도 있습니다. 이러한 프로필의 활성화 규칙은 동일합니다.

활성화 규칙이 작동하면 *프로필 1*이 활성화됩니다. 기기의 설정은 *값 1*을 가집니다. *프로필 1*을 삭제하면 *프로필 2*의 우선 순위가 가장 높아지므로 설정은 *값 2*를 사용합니다.

정책 프로필 목록에서 프로필은 개별 우선 순위에 따라 표시됩니다. 우선 순위가 가장 높은 프로필 순서대로 순위가 지정됩니다. 위쪽 화살표  와 아래쪽 화살표  를 사용하여 프로필의 우선 순위를 변경할 수 있습니다

정책 프로필 삭제

정책 프로필을 삭제하려면 다음 단계를 따릅니다.

1. 콘솔 트리에서 정책 프로필을 삭제할 관리 그룹을 선택합니다.
2. 관리 그룹의 작업 영역에서 **정책** 탭을 선택합니다.
3. 정책을 선택하고 마우스 오른쪽 메뉴를 사용하여 정책 속성 창으로 전환합니다.
4. Kaspersky Endpoint Security의 정책 속성에서 **정책 프로필** 섹션을 엽니다.
5. 삭제할 정책 프로필을 선택하고 **삭제** 버튼을 누릅니다.

정책 프로필이 삭제됩니다. 활성 상태는 기기에서 활성화 규칙을 만족해 시작하는 다른 정책 프로필이나 정책으로 전달됩니다.

정책 프로필 활성화 규칙 만들기

정책 프로필 활성화 규칙을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 정책 프로필 활성화 규칙을 만들 관리 그룹을 선택합니다.
2. 그룹의 작업 영역에서 **정책** 탭을 선택합니다.
3. 정책을 선택하고 마우스 오른쪽 메뉴를 사용하여 정책 속성 창으로 전환합니다.
4. 정책 속성 창에서 **정책 프로필** 섹션을 선택합니다.
5. 활성화 규칙을 만들어야 하는 정책 프로필을 선택하고 **속성** 버튼을 누릅니다.
   정책 프로필 속성 창이 열립니다.
   정책 프로필 목록이 비어 있으면 정책 프로필을 만들 수 있습니다.
6. **활성화 규칙** 섹션을 선택하고 **추가** 버튼을 누릅니다.
   새 정책 프로필 활성화 규칙 마법사가 시작됩니다.
7. **정책 프로필 활성화 규칙** 창에서 만들려는 정책 프로필을 활성화하려면 충족해야 하는 조건 옆의 확인란을 선택합니다.

   - **정책 프로필 활성화에 대한 일반 규칙**

     기기 오프라인 모드의 상태, 중앙 관리 서버 연결을 위한 규칙 및 기기에 할당된 태그에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다.

   - **Active Directory 이용에 대한 규칙**

     Active Directory OU(조직 구성 단위) 유무 또는 기기나 해당 소유자의 Active Directory 보안 그룹 구성원 자격에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다.

- **특정 기기 소유자에 대한 규칙**

  기기 소유자에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다.

- **하드웨어 사양에 대한 규칙**

  메모리의 크기와 논리 프로세서 수에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다.

마법사의 추가 페이지 수는 첫 번째 단계에서 선택하는 설정에 따라 달라집니다. 정책 프로필 활성화 규칙은 나중에 수정할 수 있습니다.

8. **일반 조건** 창에서 다음 설정을 지정합니다:

   - **오프라인 상태인 기기** 필드의 드롭다운 목록에서 네트워크의 기기 유무에 대한 조건을 지정합니다.

     - **예**

       기기가 외부 네트워크에 있어 중앙 관리 서버를 사용할 수 없습니다.

     - **아니요**

       기기가 네트워크에 있어 중앙 관리 서버를 사용할 수 있습니다.

     - **어떤 값도 선택되지 않았습니다.**

       기준이 적용되지 않습니다.

   - **기기가 지정된 네트워크 위치에 있음** 박스에서 드롭다운 목록을 사용하여 이 기기에서 중앙 관리 서버 규칙이 실행되거나 실행되지 않는 경우의 정책 프로필 활성화를 설정합니다.

     - **실행됨 / 실행되지 않음**

       정책 프로필 활성화의 조건입니다(규칙이 실행되는지 여부).

     - **규칙 이름**

       중앙 관리 서버 연결을 위한 기기의 네트워크 위치 설명입니다. 해당 조건이 충족되거나 충족되지 않아야 정책 프로필이 활성됩니다.

       중앙 관리 서버 연결을 위한 기기의 네트워크 위치 설명은 네트워크 에이전트 전환 규칙에서 만들거나 구성할 수 있습니다.

정책 프로필 활성화에 대한 일반 규칙 확인란을 선택하면 **일반 조건** 창이 표시됩니다.

9. **태그를 사용하는 조건** 창에서 다음 설정을 지정합니다:

   - **태그 목록**

     태그 목록에서 관련 태그 옆의 확인란을 선택하여 정책 프로필에 기기를 포함하는 규칙을 지정할 수 있습니다.

     목록에서 필드에 태그를 입력하고 **추가** 버튼을 눌러 새 태그를 목록에 추가할 수 있습니다.

     정책 프로필에는 설명에 선택한 태그가 모두 들어 있는 기기가 포함됩니다. 확인란이 비어 있으면 기준이 적용되지 않습니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

   - **지정한 태그가 없는 기기에 적용**

     선택한 태그를 반대로 적용해야 하는 경우 이 옵션을 선택합니다.

     이 옵션을 사용하면 정책 프로필에는 설명에 선택한 태그가 하나도 없는 기기가 포함됩니다. 이 옵션을 비활성화하면 기준이 적용되지 않습니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

   정책 프로필 활성화에 대한 일반 규칙 확인란을 선택하면 **태그를 사용하는 조건** 창이 표시됩니다.

10. **Active Directory를 이용하는 조건** 창에서 다음 설정을 지정합니다:

    - **Active Directory 보안 그룹에 소속된 기기 소유자의 멤버십**

      이 옵션을 사용하면 소유자가 지정한 보안 그룹의 구성원인 기기에서 정책 프로필이 활성화됩니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

    - **Active Directory 보안 그룹의 기기 구성원**

      이 옵션을 사용하면 기기에서 정책 프로필이 활성화됩니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

    - **Active Directory 조직 구성 단위의 기기 할당**

      이 옵션을 사용하면 지정한 Active Directory 조직 단위(OU)에 포함된 기기에서 정책 프로필이 활성화됩니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    Active Directory 이용에 대한 규칙 확인란을 선택하면 **Active Directory를 이용하는 조건** 창이 표시됩니다.

11. **기기 소유자를 이용하는 조건** 창에서 다음 설정을 지정합니다:

- **기기 소유자**

  이 옵션을 사용해 기기 소유자에 따라 기기에 대한 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

  - 기기는 지정한 소유자의 것입니다("=" 기호).
  - 기기는 지정한 소유자의 것이 아닙니다("#" 기호).

    이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. 옵션이 활성화되면 기기 소유자를 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **기기 소유자는 내부 보안 그룹에 소속되어 있습니다**

  이 옵션을 사용해 Kaspersky Security Center 내부 보안 그룹의 소유자에 따라 기기에 대한 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

  - 기기 소유자는 지정된 보안 그룹의 구성원입니다("=" 기호).
  - 기기 소유자는 지정된 보안 그룹의 구성원이 아닙니다("#" 기호).

    이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. Kaspersky Security Center의 보안 그룹을 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **기기 소유자의 특정 역할에 따라 정책 프로필 활성화**

  소유자의 역할에 따라 기기에 대한 프로필 활성화 규칙을 구성하고 활성하려면 이 옵션을 선택합니다. 역할은 기존 역할 목록에서 수동으로 추가합니다.

  이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다.

특정 기기 소유자에 대한 규칙에 대한 규칙 확인란을 선택하면 **기기 소유자를 이용하는 조건** 창이 표시됩니다.

12. **장비 사양을 이용하는 조건** 창에서 다음 설정을 지정합니다:

- **RAM 크기(MB)**

  이 옵션을 사용해 기기의 이용 가능한 RAM 크기에 따라 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

  - 기기 RAM 크기가 지정된 값보다 작습니다("<" 기호).
  - 기기 RAM 크기가 지정된 값보다 큽니다(">" 기호).

  이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. 기기의 RAM 볼륨을 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **논리 프로세서 개수**

  이 옵션을 사용해 기기의 논리 프로세서의 개수에 따라 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

  - 기기의 논리 프로세서의 개수는 지정한 값보다 작거나 같습니다("<" 기호).
  - 기기의 논리 프로세서의 개수는 지정한 값보다 크거나 같습니다(">" 기호).

  이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. 기기의 논리 프로세서 수를 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

하드웨어 사양에 대한 규칙 확인란을 선택하면 **장비 사양을 이용하는 조건** 창이 표시됩니다.

13. **정책 프로필 활성화 규칙 이름** 창의 **규칙 이름** 필드에 규칙 이름을 지정합니다.

그러면 프로필이 저장됩니다. 활성화 규칙이 실행되면 해당 프로필이 기기에서 활성화됩니다.

프로필용으로 만든 정책 프로필 활성화 규칙은 **활성화 규칙** 섹션의 정책 프로필 속성에 표시됩니다. 모든 정책 프로필 활성화 규칙은 수정하거나 제거할 수 있습니다.

여러 활성화 규칙을 동시에 실행할 수 있습니다.

기기 이동 규칙

*기기 이동 규칙*을 통해 관리 그룹에 기기를 자동 할당하도록 설정할 것을 권장합니다. 기기 이동 규칙은 세 가지 주요 부분으로 구성됩니다: 이 세 가지 부분은 이름, 실행 조건(기기 특성이 포함된 논리식), 그리고 대상 관리 그룹입니다. 기기 특성이 규칙 실행 조건을 충족하면 규칙이 기기를 대상 관리 그룹으로 이동합니다.

모든 기기 이동 규칙에는 우선 순위가 있습니다. 중앙 관리 서버는 우선순위의 오름차순으로 기기 특성이 각 규칙의 실행 조건을 충족하는지를 확인합니다. 기기 특성이 규칙의 실행 조건을 충족하는 경우 기기가 대상 그룹으로 이동되며 해당 기기에 대한 규칙 처리가 완료됩니다. 기기 특성이 여러 규칙의 조건을 충족하는 경우에는 우선 순위가 가장 높은 규칙(규칙 목록에서 순위가 가장 높은 규칙)의 대상 그룹으로 기기가 이동됩니다.

기기 이동 규칙은 묵시적으로 만들 수 있습니다. 예를 들어 원격 설치 작업 또는 설치 패키지의 속성에서 네트워크 에이전트를 기기에 설치한 후 기기를 이동해야 하는 관리 그룹을 지정할 수 있습니다. 또한 Kaspersky Security Center 관리자가 이동 규칙 목록에서 기기 이동 규칙을 명시적으로 만들 수도 있습니다. 이 목록은 관리 콘솔의 **미할당 기기** 그룹 속성에 있습니다.

기본적으로 기기 이동 규칙은 기기를 관리 그룹으로 할당할 때 처음 한 번 사용됩니다. 이 규칙은 **미할당 기기** 그룹의 기기를 한 번만 이동합니다. 기기가 이 규칙에 의해 한 번 이동된 경우 해당 기기를 **미할당 기기** 그룹에 수동으로 되돌려 놓더라도 규칙은 해당 기기를 다시 이동하지 않습니다. 이동 규칙은 이러한 방식으로 적용하는 것이 좋습니다.

일부 관리 그룹에 이미 할당된 기기를 이동할 수 있습니다. 이렇게 하려면 규칙의 속성에서 **관리 그룹에 속하지 않는 기기만 이동** 확인란의 선택을 취소합니다.

일부 관리 그룹에 이미 할당된 기기에 이동 규칙을 적용하면 중앙 관리 서버의 부하가 크게 증가합니다.

자동 생성된 이동 규칙의 속성에서는 **관리 그룹에 속하지 않는 기기만 이동** 확인란이 잠겨 있습니다. 이러한 규칙은 *원격으로 애플리케이션 설치* 작업을 추가하거나 독립 실행형 설치 패키지를 생성할 때 생성됩니다.

단일 기기에 반복적으로 적용되는 이동 규칙을 만들 수 있습니다.

하지만 기기에 특수 정책을 적용하거나, 특수 그룹 작업을 실행하거나, 특정 배포 지점을 통해 기기를 업데이트하는 등의 작업을 위해 단일 기기를 그룹 간에 반복적으로 이동하지 않는 것이 좋습니다.

이렇게 이동 시 중앙 관리 서버의 부하와 네트워크 트래픽이 지나치게 증가하므로, 이러한 시나리오는 지원하지 않습니다. 그리고 이러한 이동은 특히 접근 권한, 이벤트 및 리포트 측면에서 Kaspersky Security Center의 작동 원칙과도 충돌합니다. 정책 프로필, 기기 조회용 작업, 표준 시나리오에 따라 네트워크 에이전트 할당 등 다른 해결 방법을 찾아야 합니다.

기기 이동 규칙 복제

설정이 비슷한 기기 이동 규칙을 여러 개 생성해야 할 때는 기존 규칙을 복제한 다음 복제된 규칙의 설정을 변경할 수 있습니다. 예를 들어 IP 범위와 대상 그룹이 다른 동일 기기 이동 규칙이 여러 개 필요한 경우 이러한 방식이 유용합니다.

기기 이동 규칙을 복제하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. **미할당 기기** 폴더에서 **규칙 구성**를 누릅니다.
   속성: 미할당 기기 창이 열립니다.
3. **기기 이동** 섹션에서 복제할 기기 이동 규칙을 선택합니다.
4. **규칙 복제**를 누릅니다.

   선택한 기기 이동 규칙의 복제본이 목록 끝에 추가됩니다.

새 규칙은 비활성화된 상태로 생성됩니다. 언제든지 규칙을 편집하거나 활성화할 수 있습니다.

소프트웨어 분류

애플리케이션 실행을 모니터링하는 데 기본적으로 사용되는 도구는 *Kaspersky 카테고리*(이하 *KL 카테고리*로 지칭함)입니다. Kaspersky Security Center 관리자는 KL 카테고리를 사용하여 소프트웨어 분류를 간편하게 지원하고 관리 중인 기기로 전송되는 트래픽을 최소화할 수 있습니다.

기존 KL 카테고리로 분류할 수 없는 애플리케이션(예: 사용자 지정 방식으로 작성된 소프트웨어)에 대해서만 사용자 카테고리를 만들어야 합니다. 애플리케이션 설치 패키지(MSI) 또는 설치 패키지가 포함된 폴더를 기준으로 하여 사용자 카테고리를 만듭니다.

KL 카테고리를 통해 분류되지 않은 대량의 소프트웨어 모음을 사용할 수 있는 경우에는 자동으로 업데이트되는 카테고리를 만들면 유용할 수 있습니다. 그러면 배포 패키지가 포함된 폴더를 수정할 때마다 실행 파일의 체크섬이 해당 카테고리에 자동으로 추가됩니다.

문서, %windir%, %ProgramFiles% 및 %ProgramFiles(x86)% 폴더에 자동 업데이트되는 소프트웨어 범주를 생성하지 마십시오. 이러한 폴더의 파일 풀은 자주 변경되므로 중앙 관리 서버의 부하와 네트워크 트래픽이 증가합니다. 소프트웨어 모음이 저장되는 전용 폴더를 만들어 주기적으로 새 항목을 해당 폴더에 추가해야 합니다.

클라이언트 조직의 기기에 애플리케이션을 설치하기 위한 필수 구성 요소

클라이언트 조직의 기기에 애플리케이션을 원격으로 설치하는 과정은 회사 내.기기에 원격 설치하는 방법과 같습니다.

클라이언트 조직의 기기에 애플리케이션을 설치하려면 다음 동작을 수행해야 합니다:

- 클라이언트 조직의 기기에 처음으로 애플리케이션을 설치하기 전에 네트워크 에이전트를 먼저 설치합니다.

  네트워크 에이전트 설치 패키지를 Kaspersky Security Center의 서비스 공급업체에 구성할 때 설치 패키지의 속성 창에서 다음 설정을 조정합니다:

  - **연결** 섹션의 **중앙 관리 서버** 문자열에 배포 지점에 네트워크 에이전트를 로컬 설치하는 동안 지정되었던 동일한 가상 중앙 관리 서버의 주소를 지정합니다.
  - **고급** 섹션에서 **연결 게이트웨이를 통해 중앙 관리 서버에 연결** 확인란을 선택합니다. **연결 게이트웨이 주소** 문자열에 배포 지점 주소를 지정합니다. 기기 IP 주소 또는 Windows 네트워크상의 기기 이름을 사용할 수 있습니다.

- **배포 지점을 통해 대상 운영 체제의 관리 공유 폴더 이용**을 네트워크 에이전트 설치 패키지의 다운로드 모드로 선택합니다. 다음과 같이 다운로드 방법을 선택할 수 있습니다:
  - 원격 설치 작업을 사용하여 애플리케이션을 설치할 경우 다음 방법 중 하나로 다운로드 방식을 지정할 수 있습니다:
    - **설정** 창에서 원격 설치 작업을 만들 때 지정
    - **설정** 섹션의 원격 설치 작업 속성 창에서 지정
  - 원격 설치 마법사를 사용하여 애플리케이션을 설치할 경우 이 마법사의 **설정** 창에 있는 다운로드 방식을 선택해야 합니다.
- 배포 지점이 인증에 사용하는 계정은 모든 클라이언트 기기에 대한 Admin$ 리소스에 접근할 수 있어야 합니다.

로컬 애플리케이션 설정 보기 및 편집

Kaspersky Security Center 관리 시스템에서는 관리 콘솔을 통해 기기의 로컬 애플리케이션 설정을 원격으로 관리할 수 있습니다.

*로컬 애플리케이션 설정*은 기기에 적용되는 특정 애플리케이션 설정을 의미합니다. Kaspersky Security Center를 사용하여 관리 그룹에 포함된 기기에 로컬 애플리케이션 설정을 지정할 수 있습니다.

Kaspersky 애플리케이션 설정에 대한 자세한 설명은 해당 설명서에 나와 있습니다.

애플리케이션 로컬 설정을 보거나 변경하려면 다음과 같이 하십시오:

1. 관련 기기가 속한 그룹의 작업 영역에서 **기기** 탭을 선택합니다.
2. 기기 속성 창의 **애플리케이션** 섹션에서 관련 애플리케이션을 선택합니다.
3. 애플리케이션 이름을 두 번 누르거나 **속성** 버튼을 눌러 애플리케이션 속성 창을 엽니다.

   그러면 선택한 애플리케이션의 로컬 설정 창이 열려 해당 설정을 보고 편집할 수 있습니다.

그룹 정책으로 수정이 금지되지 않은 설정(정책에서 잠금 아이콘(🔒)으로 표시되지 않은 설정)의 값을 변경할 수 있습니다.

Kaspersky Security Center 및 관리 중인 애플리케이션 업데이트

이 섹션에서는 Kaspersky Security Center 및 관리 중인 애플리케이션을 업데이트하기 위해 수행해야 하는 단계를 설명합니다.

시나리오: Kaspersky 데이터베이스 및 애플리케이션의 정기적 업데이트

이 섹션에서는 Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션을 정기적으로 업데이트하는 시나리오를 제공합니다. 네트워크 보호 구성 시나리오를 완료한 후 중앙 관리 서버와 관리 중인 기기가 바이러스, 네트워크 공격 및 피싱 공격을 비롯한 다양한 위협으로부터 보호되도록 보호 시스템의 안정성을 유지해야 합니다.

네트워크 보호는 다음을 정기적으로 업데이트하여 최신 상태로 유지됩니다.

- Kaspersky 데이터베이스 및 소프트웨어 모듈
- Kaspersky Security Center 구성 요소 및 보안 제품을 포함하여 설치된 Kaspersky 애플리케이션

이 시나리오를 완료하면 다음을 확인할 수 있습니다.

- 네트워크는 Kaspersky Security Center 구성 요소 및 보안 제품 등의 최신 Kaspersky 소프트웨어로 보호됩니다.
- 네트워크 안전에 중요한 안티 바이러스 데이터베이스 및 기타 Kaspersky 데이터베이스는 항상 최신 상태로 유지됩니다.

필수 구성 요소

관리 중인 기기는 중앙 관리 서버에 연결되어 있어야 합니다. 연결되지 않은 경우 Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션을 수동으로 업데이트하거나 Kaspersky 업데이트 서버에서 직접 업데이트하는 것을 고려하십시오.

중앙 관리 서버는 인터넷에 연결되어 있어야 합니다.

시작하기 전에 다음을 수행했는지 확인하십시오:

1. Kaspersky 보안 제품을 Kaspersky Security Center 웹 콘솔을 통한 Kaspersky 애플리케이션 배포 시나리오에 따라 관리 중인 기기에 배포했습니다.
2. 모든 필수 정책, 정책 프로필 및 작업을 네트워크 보호 구성 시나리오에 따라 생성하고 구성했습니다.
3. 관리 중인 기기의 수 및 네트워크 토폴로지에 따라 적절한 양의 배포 지점을 할당했습니다.

Kaspersky 데이터베이스 및 애플리케이션 업데이트는 단계적으로 진행됩니다.

1. **업데이트 체계 선택**

   Kaspersky Security Center 구성 요소 및 보안 제품에 대한 업데이트를 설치하는 데 사용 할 수 있는 몇 가지 체계가 있습니다. 네트워크의 요구 사항을 가장 잘 충족하는 체계를 하나 또는 여러 개 선택하십시오.

2. **중앙 관리 서버 저장소 업데이트 다운로드 작업 생성**

   이 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동으로 생성합니다. 마법사를 실행하지 않았다면 지금 작업을 만듭니다.

   이 작업은 Kaspersky 업데이트 서버에서 중앙 관리 서버의 저장소로 업데이트를 다운로드하고 Kaspersky Security Center용 Kaspersky 데이터베이스 및 소프트웨어 모듈을 업데이트하는 데 필요합니다. 업데이트를 다운로드한 후 관리 중인 기기로 배포할 수 있습니다.

네트워크에 배포 지점이 할당되면 업데이트가 중앙 관리 서버 저장소에서 배포 지점의 저장소로 자동 다운로드됩니다. 이러한 경우 배포 지점 범위에 포함된 관리 중인 기기가 중앙 관리 서버 저장소 대신 배포 지점의 저장소에서 업데이트를 다운로드합니다.

방법 지침:

- 관리 콘솔: 중앙 관리 서버 저장소 업데이트 다운로드 작업 생성
- Kaspersky Security Center 웹 콘솔: 중앙 관리 서버 저장소 업데이트 다운로드 작업 생성

3. **배포 지점의 저장소로 업데이트 다운로드 작업 생성(선택 사항)**

기본적으로 업데이트는 중앙 관리 서버에서 배포 지점으로 다운로드됩니다. Kaspersky 업데이트 서버에서 직접 배포 지점으로 업데이트를 다운로드하도록 Kaspersky Security Center를 구성할 수 있습니다. 배포 지점과 Kaspersky 업데이트 서버 간의 트래픽에 비해 중앙 관리 서버와 배포 지점 간의 트래픽에서 더 많은 비용이 발생하거나 중앙 관리 서버에서 인터넷에 연결할 수 없는 경우 배포 지점의 저장소로 업데이트 다운로드 작업을 사용하는 것이 좋습니다.

네트워크에 배포 지점이 할당되어 있고 *배포 지점의 저장소로 업데이트 다운로드* 작업이 생성되면 배포 지점은 중앙 관리 서버 저장소가 아닌 Kaspersky 업데이트 서버에서 업데이트를 다운로드합니다.

방법 지침:

- 관리 콘솔: 배포 지점의 저장소로 업데이트 다운로드 작업 생성
- Kaspersky Security Center 웹 콘솔: 배포 지점의 저장소로 업데이트 다운로드 작업 생성

4. **배포 지점 구성**

네트워크에 배포 지점이 할당되어 있는 경우 모든 필수 배포 지점의 속성에서 **업데이트 배포** 옵션이 활성화되어 있는지 확인합니다. 배포 지점에 대해 이 옵션이 비활성화되어 있으면 배포 지점 범위에 포함된 기기가 중앙 관리 서버의 저장소에서 업데이트를 다운로드합니다.

관리 중인 기기가 배포 지점에서만 업데이트를 받도록 하려는 경우 네트워크 에이전트 정책에서 **배포 지점을 통해서만 파일 배포** 옵션을 활성화합니다.

5. **업데이트 다운로드 또는 diff 파일의 오프라인 모델을 사용하여 업데이트 프로세스 최적화(선택 사항)**

업데이트 다운로드의 오프라인 모델(기본적으로 활성화됨) 또는 diff 파일을 사용하여 업데이트 프로세스를 최적화할 수 있습니다. 이러한 두 기능은 동시에 작동할 수 없기 때문에 각 네트워크 세그먼트에 대해 활성화할 기능을 선택해야 합니다.

업데이트 다운로드의 오프라인 모델이 활성화된 경우 네트워크 에이전트는 보안 제품이 업데이트를 요청하기 전에 업데이트가 중앙 관리 서버 저장소로 다운로드되면 관리 중인 기기에 필요한 업데이트를 다운로드합니다. 이를 통해 업데이트 프로세스의 안정성이 향상됩니다. 이 기능을 사용하려면 네트워크 에이전트 정책에서 **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드(권장)** 옵션을 활성화합니다.

업데이트 다운로드의 오프라인 모델을 사용하지 않는 경우 diff 파일을 사용하여 중앙 관리 서버와 관리 중인 기기 간의 트래픽을 최적화할 수 있습니다. 이 기능이 활성화되면 중앙 관리 서버 또는 배포 지점에서 Kaspersky 데이터베이스 또는 소프트웨어 모듈의 전체 파일 대신 diff 파일을 다운로드합니다. 달라진 파일은 데이터베이스 또는 소프트웨어 모듈의 두 파일 버전 간 차이점을 설명합니다. 따라서 diff 파일은 전체 파일보다 적은 공간을 차지합니다. 이로 인해 중앙 관리 서버 또는 배포 지점과 관리 중인 기기 간의 트래픽이 감소합니다. 이 기능을 사용하려면 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업 및/또는 *배포 지점의 저장소로 업데이트 다운로드* 작업의 속성에서 **diff 파일 다운로드** 옵션을 활성화합니다.

방법 지침:

- Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트에 달라진 파일 사용
- 관리 콘솔: 업데이트 다운로드 오프라인 모델 활성 및 비활성
- Kaspersky Security Center 웹 콘솔: 업데이트 다운로드 오프라인 모델 활성 및 비활성

6 다운로드한 업데이트 검증(선택 사항)

다운로드한 업데이트를 설치하기 전에 *업데이트 검증* 작업을 통해 업데이트를 확인할 수 있습니다. 이 작업은 지정된 테스트 기기 모음에 대한 설정을 통해 구성된 기기 업데이트 작업 및 악성 코드 검사 작업을 순차적으로 실행합니다. 작업 결과가 나오면 중앙 관리 서버에서 나머지 기기에 대한 업데이트 배포를 시작하거나 차단합니다.

업데이트 검증 작업은 *중앙 관리 서버 저장소 업데이트 다운로드* 작업에 포함되어 수행됩니다. *중앙 관리 서버 저장소 업데이트 다운로드* 작업의 속성에서 관리 콘솔의 **배포하기 전에 업데이트 검증 절차 수행** 옵션 또는 Kaspersky Security Center 웹 콘솔의 **업데이트 검증 실행** 옵션을 활성화합니다.

방법 지침:

- 관리 콘솔: 다운로드한 업데이트 검증
- Kaspersky Security Center 웹 콘솔: 다운로드한 업데이트 검증

7 소프트웨어 업데이트 승인 및 거부

기본적으로 다운로드한 소프트웨어 업데이트는 *정의 안 됨* 상태입니다. 상태를 *승인됨* 또는 *거부됨*으로 변경할 수 있습니다. 승인된 업데이트는 항상 설치됩니다. 업데이트를 위해 최종 사용자 라이센스 계약서 약관을 검토하고 동의해야 하는 경우 먼저 약관에 동의해야 합니다. 그런 다음 업데이트를 관리 중인 기기로 배포할 수 있습니다. 정의되지 않은 업데이트는 네트워크 에이전트 정책 설정에 따라 네트워크 에이전트 및 다른 Kaspersky Security Center 구성 요소에만 설치할 수 있습니다. *거부됨* 상태로 설정한 업데이트는 기기에 설치되지 않습니다. 보안 제품에 대해 거부된 업데이트가 이전에 설치된 경우 Kaspersky Security Center는 모든 기기에서 업데이트 제거를 시도합니다.

업데이트 승인 및 거부는 네트워크 에이전트 및 Windows 기반 및 Linux 기반 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션에서만 사용할 수 있습니다. 중앙 관리 서버, Kaspersky Security Center 웹 콘솔 및 관리 웹 플러그인의 원활한 업데이트를 지원하지 않습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 업데이트 승인 및 거부
- Kaspersky Security Center 웹 콘솔: 소프트웨어 업데이트 승인 및 거부

8 Kaspersky Security Center 구성 요소 업데이트 및 패치 자동 설치 구성

네트워크 에이전트 및 다른 Kaspersky Security Center 구성 요소에 대해 다운로드한 업데이트 및 패치가 자동 설치됩니다. 네트워크 에이전트 속성에서 **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 옵션을 활성화된 상태로 두면 모든 업데이트가 저장소 하나 또는 여러 개로 다운로드된 후 자동으로 설치됩니다. 이 옵션을 비활성화하면, 다운로드되어 *정의 안 됨* 상태가 태그된 Kaspersky 패치는 그 상태를 *승인됨*으로 변경한 후에만 설치할 수 있습니다.

방법 지침:

- 관리 콘솔: Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성/비활성
- Kaspersky Security Center 웹 콘솔: Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성화/비활성화

9 중앙 관리 서버의 업데이트 설치

중앙 관리 서버의 소프트웨어 업데이트는 업데이트 상태에 따라 달라지지 않습니다. 이는 자동으로 설치되지 않으며 관리 콘솔의 **모니터링** 탭(**중앙 관리 서버** <서버 이름> → **모니터링**)이나 Kaspersky Security Center 웹 콘솔의 **알림** 섹션(**모니터링 및 보고 → 알림**)에서 관리자의 사전 승인을 받아야 합니다. 그 후 관리자는 명시적으로 업데이트 설치를 실행해야 합니다.

10 보안 제품에 대한 업데이트 자동 설치 구성

관리 중인 애플리케이션에 대한 *업데이트* 작업을 생성하여 안티 바이러스 데이터베이스를 포함한 애플리케이션, 소프트웨어 및 Kaspersky 데이터베이스에 대한 업데이트를 적시에 제공할 수 있습니다. 업데이트를 적시에 제공하려면 작업 스케줄 구성 시 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후** 옵션을 선택합니다.

네트워크에 IPv6 전용 기기가 포함되어 있고 이러한 기기에 설치된 보안 애플리케이션을 정기적으로 업데이트하려면, 관리 중인 기기에 중앙 관리 서버(13.2 버전 이상)와 네트워크 에이전트(13.2 버전 이상)가 설치되어 있어야 합니다.

기본적으로 Kaspersky Endpoint Security for Windows 및 Kaspersky Endpoint Security for Linux에 대한 업데이트는 업데이트 상태를 *승인됨*으로 변경한 후에만 설치됩니다. *업데이트* 작업에서 업데이트 설정을 변경할 수 있습니다.

업데이트를 위해 최종 사용자 라이센스 계약서 약관을 검토하고 동의해야 하는 경우 먼저 약관에 동의해야 합니다. 그런 다음 업데이트를 관리 중인 기기로 배포할 수 있습니다.

방법 지침:

- 관리 콘솔: 기기에서 Kaspersky Endpoint Security 업데이트 자동 설치
- Kaspersky Security Center 웹 콘솔: 기기에 Kaspersky Endpoint Security 업데이트 자동 설치

결과

시나리오가 완료되면 Kaspersky Security Center는 Kaspersky 데이터베이스를 업데이트하도록 구성되고 업데이트가 중앙 관리 서버의 저장소 또는 배포 지점의 저장소에 다운로드된 후 Kaspersky 애플리케이션을 설치합니다. 그런 다음 네트워크 상태 모니터링을 진행할 수 있습니다.

Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 업데이트 정보

중앙 관리 서버 및 관리 중인 기기의 보호가 최신 상태로 유지하려면 다음을 적시에 업데이트해야 합니다:

- Kaspersky 데이터베이스 및 소프트웨어 모듈

  Kaspersky 데이터베이스 및 소프트웨어 모듈을 다운로드하기 전에 Kaspersky Security Center가 Kaspersky 서버에 액세스할 수 있는지 확인합니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다. 안티 바이러스 데이터베이스가 업데이트되고 관리 중인 기기에 대한 보안 수준을 유지하는 데 필요합니다.

- Kaspersky Security Center 구성 요소 및 보안 제품을 포함하여 설치된 Kaspersky 애플리케이션

  Kaspersky Security Center를 사용하면 Windows 기반 및 Linux 기반 클라이언트 기기에 설치된 네트워크 에이전트 및 Kaspersky 애플리케이션을 자동으로 업데이트할 수 있습니다. 중앙 관리 서버, Kaspersky Security Center 웹 콘솔 및 관리 웹 플러그인의 원활한 업데이트를 지원하지 않습니다. 이 구성 요소를 업데이트하려면 Kaspersky 웹사이트에서 최신 버전을 다운로드한 다음 수동 설치합니다.

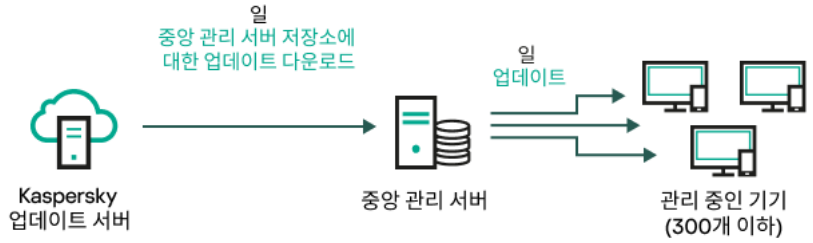
네트워크의 구성에 따라 다음과 같은 체계를 사용하여 필요한 업데이트를 관리 중인 기기로 다운로드하고 배포할 수 있습니다:

- 단일 작업 사용: *중앙 관리 서버 저장소에 업데이트 다운로드*
- 2개의 작업 사용:
  - *중앙 관리 서버 저장소에 업데이트 다운로드* 작업
  - *배포 지점의 저장소로 업데이트 다운로드* 작업

- 로컬 폴더, 공유 폴더 또는 FTP 서버를 통해 수동 업데이트
- Kaspersky 업데이트 서버에서 관리 중인 기기의 Kaspersky Endpoint Security로 직접 업데이트
- 중앙 관리 서버에 인터넷 연결이 없을 시, 로컬 또는 네트워크 폴더를 통해

중앙 관리 서버 저장소에 업데이트 다운로드 작업 사용

이 구성에서 Kaspersky Security Center는 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 통해 업데이트를 다운로드합니다. 단일 네트워크 세그먼트에 300대 미만의 관리 중인 기기가 있거나 각 네트워크 세그먼트에 10대 미만의 관리 중인 기기가 있는 소규모 네트워크에서는 업데이트가 중앙 관리 서버 저장소에서 직접 관리 중인 기기로 배포됩니다(아래 그림 참조).

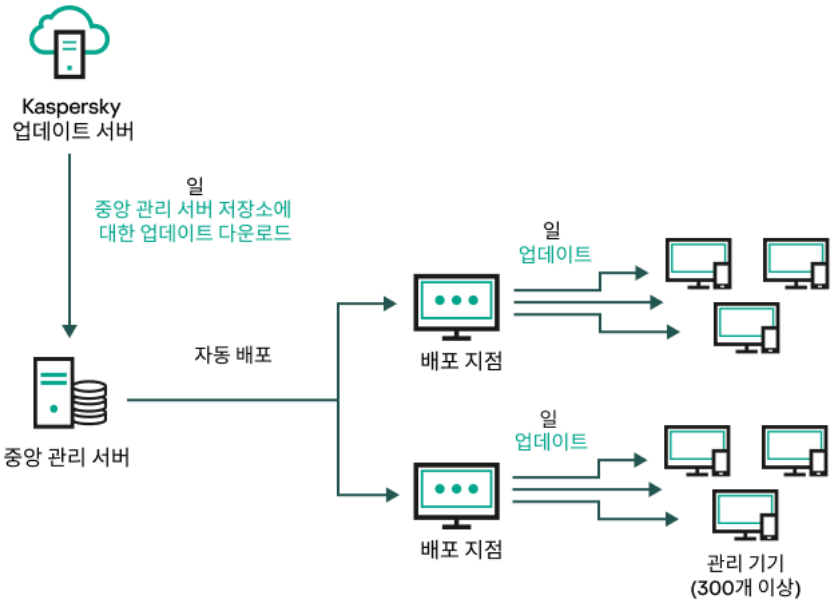


배포 지점이 없는 중앙 관리 서버 저장소에 업데이트 다운로드 작업을 사용하여 업데이트

기본적으로 중앙 관리 서버는 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버를 구성할 수 있습니다.

단일 네트워크 세그먼트에 300대 이상의 관리 중인 기기가 있거나 각 네트워크 세그먼트에 9대 이상의 관리 중인 기기가 있는 다중 네트워크 구성에서는 배포 지점을 사용하여 관리 중인 기기로 업데이트를 배포하는 것이 좋습니다(아래 그림 참조). 배포 지점은 중앙 관리 서버의 부하를 줄이고 중앙 관리 서버와 관리 중인 기기 간의 트래픽을 최적화합니다. 네트워크에 필요한 배포 지점의 수와 구성을 계산할 수 있습니다.

이 체계에서는 업데이트가 중앙 관리 서버 저장소에서 배포 지점의 저장소로 자동으로 다운로드됩니다. 배포 지점 범위에 포함된 관리 중인 기기가 중앙 관리 서버 저장소 대신 배포 지점의 저장소에서 업데이트를 다운로드합니다.



배포 지점이 있는 중앙 관리 서버 저장소에 업데이트 다운로드 작업을 사용하여 업데이트

중앙 관리 서버 저장소에 업데이트 다운로드 작업이 완료되면 다음과 같은 업데이트가 중앙 관리 서버 저장소로 다운로드됩니다.

- Kaspersky 데이터베이스 및 Kaspersky Security Center용 소프트웨어 모듈
  이러한 업데이트는 자동으로 설치됩니다.
- 관리 중인 기기에 설치된 보안 제품용 Kaspersky 데이터베이스 및 소프트웨어 모듈
  이러한 업데이트는 Kaspersky Endpoint Security for Windows 업데이트 작업을 통해 설치됩니다.
- 중앙 관리 서버용 업데이트:
  이 업데이트는 자동으로 설치되지 않습니다. 관리자는 업데이트 설치를 명시적으로 승인하고 실행해야 합니다.

  > 중앙 관리 서버에 패치를 설치하려면 로컬 관리자 권한이 필요합니다.

- Kaspersky Security Center의 구성 요소 업데이트
  기본적으로 이러한 업데이트는 자동으로 설치됩니다. 네트워크 에이전트 정책에서 설정을 변경할 수 있습니다.
- 보안 제품에 대한 업데이트
  기본적으로 Kaspersky Endpoint Security for Windows는 승인된 업데이트만 설치합니다(관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 통해 업데이트를 승인할 수 있습니다). 업데이트는 *업데이트* 작업을 통해 설치되며 이 작업의 속성에서 구성할 수 있습니다.

> 가상 중앙 관리 서버에서는 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 사용할 수 없습니다. 가상 중앙 관리 서버의 저장소에는 기본 중앙 관리 서버로 다운로드된 업데이트가 표시됩니다.

일련의 테스트 기기에서 작동 가능성과 오류를 확인하기 위한 업데이트를 구성할 수 있습니다. 검증에 성공하면 업데이트가 다른 관리 중인 기기에 배포됩니다.

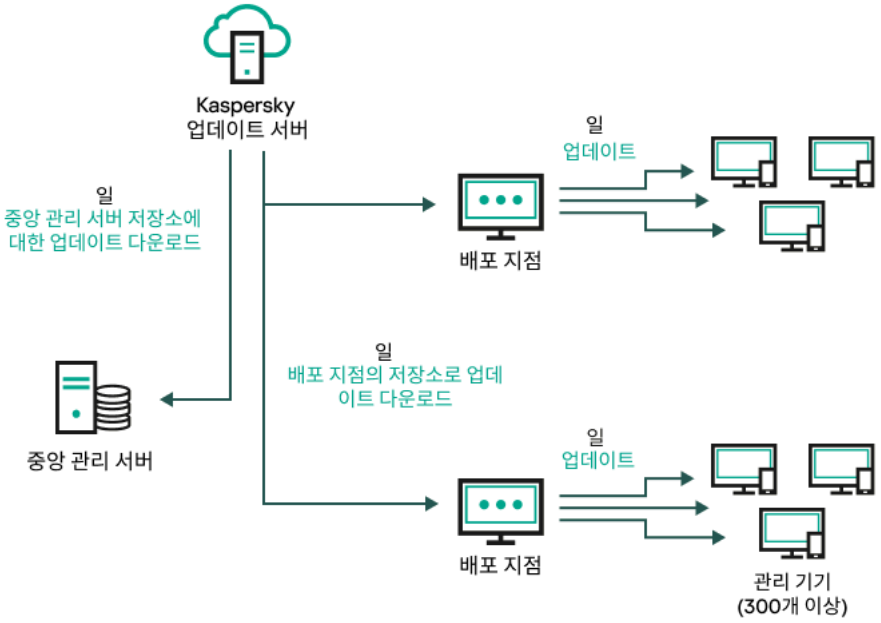
각 Kaspersky 애플리케이션은 중앙 관리 서버에서 필요한 업데이트를 요청합니다. 중앙 관리 서버는 이러한 요청을 집계하여 애플리케이션에 필요한 업데이트만 다운로드합니다. 그러므로 같은 업데이트가 여러 번 다운로드되지 않으며 불필요한 업데이트는 전혀 다운로드되지 않습니다. *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행할 때 Kaspersky 데이터베이스 및 소프트웨어 모듈의 관련 버전을 제대로 다운로드하기 위해 Kaspersky 업데이트 서버로 다음 정보를 중앙 관리 서버가 자동 전송합니다:

- 애플리케이션 ID 및 버전
- 애플리케이션 설치 ID
- 활성 키 ID
- *중앙 관리 서버 저장소 업데이트 다운로드* 작업 실행 ID

전송되는 정보에는 개인 정보 또는 기타 기밀 정보가 포함되지 않습니다. AO Kaspersky Lab은 법률로 규정된 요구 사항에 따라 정보를 보호합니다.

2개의 작업(중앙 관리 서버 저장소에 업데이트 다운로드 작업 및 배포 지점의 저장소로 업데이트 다운로드 작업) 사용

중앙 관리 서버 저장소 대신 Kaspersky 업데이트 서버에서 배포 지점의 저장소로 업데이트를 직접 다운로드할 수 있으며 이후 관리 중인 기기로 배포할 수 있습니다(아래 그림 참조). 배포 지점과 Kaspersky 업데이트 서버 간의 트래픽에 비해 중앙 관리 서버와 배포 지점 간의 트래픽에서 더 많은 비용이 발생하거나 중앙 관리 서버에서 인터넷에 연결할 수 없는 경우 배포 지점의 저장소로 업데이트 다운로드 작업을 사용하는 것이 좋습니다.



중앙 관리 서버 저장소에 업데이트 다운로드 작업 및 배포 지점의 저장소로 업데이트 다운로드 작업을 사용하여 업데이트

기본적으로 중앙 관리 서버 및 배포 지점은 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버 및 배포 지점을 구성할 수 있습니다.

이 구성을 구현하려면 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업과 함께 *배포 지점의 저장소로 업데이트 다운로드* 작업을 만듭니다. 그런 다음 배포 지점이 중앙 관리 서버 저장소가 아닌 Kaspersky 업데이트 서버에서 업데이트를 다운로드합니다.

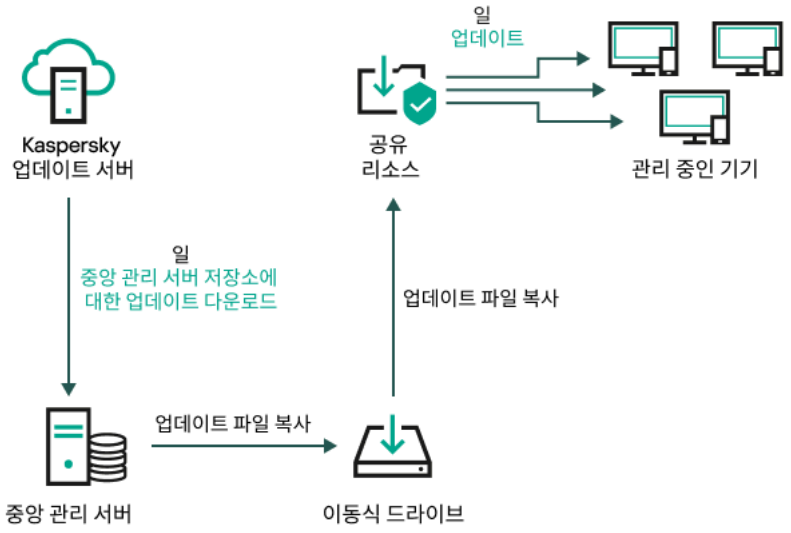
macOS를 실행하는 배포 지점 기기는 Kaspersky 업데이트 서버에서 업데이트를 다운로드할 수 없습니다.

macOS를 실행하는 하나 이상의 기기가 *배포 지점의 저장소로 업데이트 다운로드 작업 범위*에 있는 경우 모든 Windows 기기에서 작업이 성공적으로 완료되어도 작업은 *실패* 상태로 완료됩니다.

중앙 관리 서버 저장소에 업데이트 다운로드 작업 역시 이 체계에 필요합니다. 왜냐하면 이 작업은 Kaspersky Security Center용 Kaspersky 데이터베이스 및 소프트웨어 모듈을 다운로드하는 데 사용되기 때문입니다.

로컬 폴더, 공유 폴더 또는 FTP 서버를 통해 수동 업데이트

클라이언트 기기가 중앙 관리 서버에 연결되어 있지 않은 경우 로컬 폴더 또는 공유 리소스를 Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션을 업데이트하는 경로로 사용할 수 있습니다. 이 체계에서는 필요한 업데이트를 중앙 관리 서버 저장소에서 이동식 드라이브로 복사한 다음 Kaspersky Endpoint Security 설정에서 업데이트 경로로 지정된 로컬 폴더 또는 공유 리소스에 복사해야 합니다(아래 그림 참조).



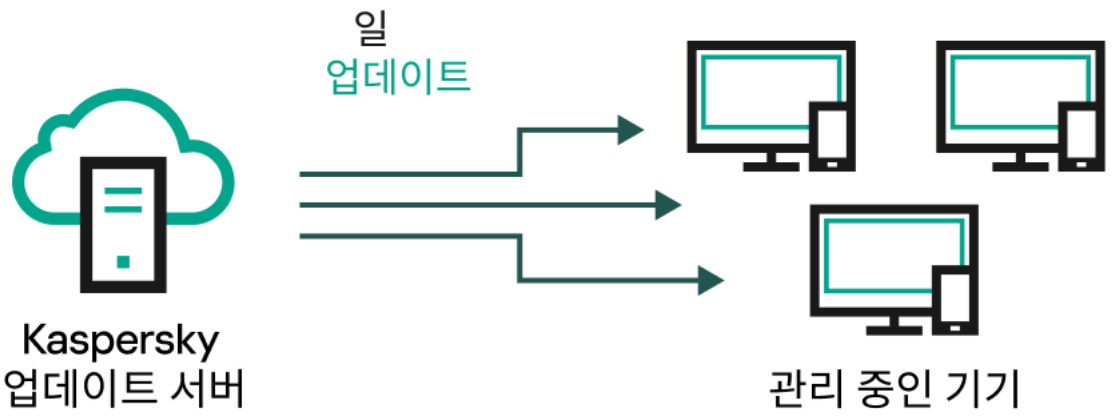
로컬 폴더, 공유 폴더 또는 FTP 서버를 통해 업데이트

Kaspersky Endpoint Security의 업데이트 소스에 대한 자세한 내용은 다음 도움말을 참조하십시오:

- Kaspersky Endpoint Security for Windows 도움말
- Kaspersky Endpoint Security for Linux 도움말

Kaspersky 업데이트 서버에서 관리 중인 기기의 Kaspersky Endpoint Security로 직접 업데이트

관리 중인 기기에서 Kaspersky Endpoint Security가 Kaspersky 업데이트 서버에서 직접 업데이트를 받도록 구성할 수 있습니다(아래 그림 참조).



Kaspersky 업데이트 서버에서 직접 보안 제품 업데이트

이 체계에서 보안 제품은 Kaspersky Security Center에서 제공하는 저장소를 사용하지 않습니다. Kaspersky 업데이트 서버에서 직접 업데이트를 받으려면 보안 제품 인터페이스에서 Kaspersky 업데이트 서버를 업데이트 경로로 지정합니다. 이러한 설정에 대한 자세한 내용은 다음 도움말을 참조하십시오:

- Kaspersky Endpoint Security for Windows 도움말
- Kaspersky Endpoint Security for Linux 도움말

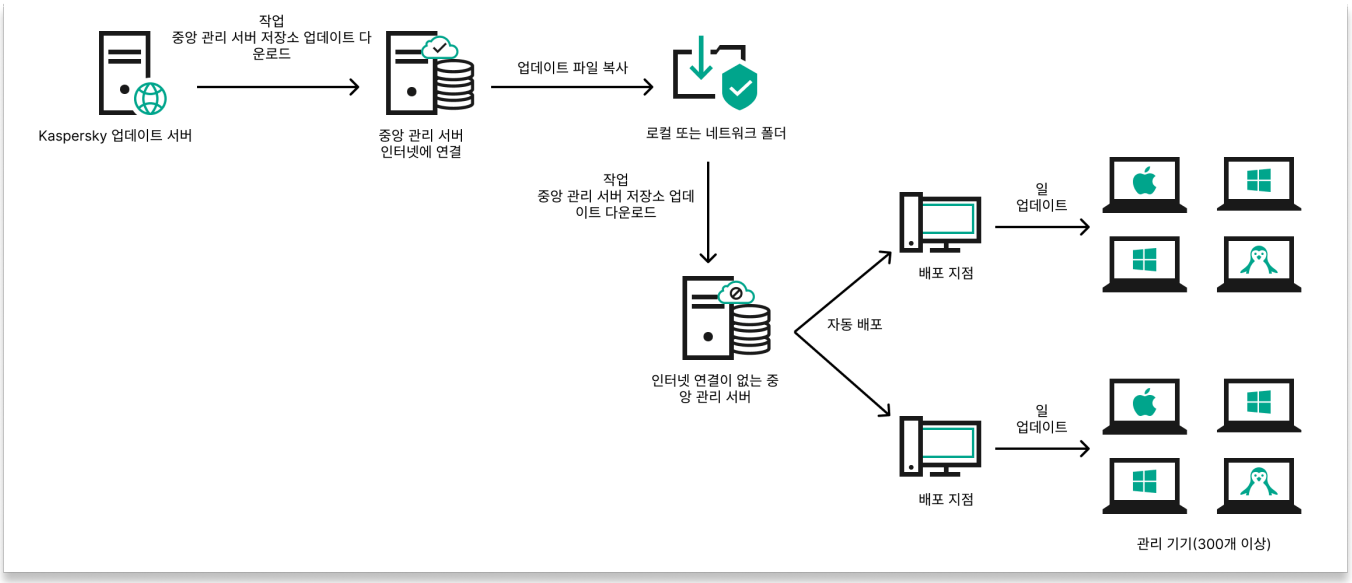
중앙 관리 서버에 인터넷 연결이 없을 시, 로컬 또는 네트워크 폴더를 통해

중앙 관리 서버가 인터넷에 연결되어 있지 않을 시, *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 구성하여 로컬 또는 네트워크 폴더에서 업데이트를 다운로드할 수 있습니다. 이때, 필요한 업데이트 파일을 지정된 폴더에 주기적으로 복사해야 합니다. 예를 들어 다음 경로 중 하나에서 필요한 업데이트 파일을 복사할 수 있습니다.

- 인터넷에 연결된 중앙 관리 서버(아래 그림 참조)

  중앙 관리 서버는 보안 애플리케이션에서 요청한 업데이트만 다운로드하므로 중앙 관리 서버에서 관리하는 보안 애플리케이션 집합(인터넷에 연결된 것과 연결되지 않은 것)이 일치해야 합니다.

  업데이트를 다운로드하는 데 사용하는 중앙 관리 서버의 버전이 13.2 이하일 시, *중앙 관리 서버 저장소에 업데이트 다운로드* 작업의 속성을 열고 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.



중앙 관리 서버에 인터넷 연결이 없을 시 로컬 또는 네트워크 폴더를 통해 업데이트

- Kaspersky 업데이트 유틸리티

  이 유틸리티는 이전 구성표를 사용하여 업데이트를 다운로드하므로, *중앙 관리 서버 저장소에 업데이트 다운로드* 작업의 속성을 열고 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.

Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트 시 diff 파일 사용에 대한 정보

Kaspersky Security Center는 Kaspersky 업데이트 서버에서 업데이트를 다운로드할 때 달라진 파일을 사용하여 트래픽을 최적화합니다. 네트워크의 다른 기기에서 업데이트를 가져오는 기기(중앙 관리 서버, 배포 지점 및 클라이언트 기기)의 달라진 파일 사용을 활성화할 수도 있습니다.

달라진 파일 다운로드 기능 정보

달라진 파일은 데이터베이스 또는 소프트웨어 모듈의 두 파일 버전 간 차이점을 설명합니다. 달라진 파일을 사용하면 회사 네트워크 내의 트래픽을 절약할 수 있습니다. 달라진 파일은 데이터베이스 및 소프트웨어 모듈의 전체 파일에 비해 공간을 적게 차지하기 때문입니다. 중앙 관리 서버 또는 배포 지점에서 *달라진 파일 다운로드* 기능을 활성화하면 해당 중앙 관리 서버 또는 배포 지점에 달라진 파일이 저장됩니다. 따라서 이 중앙 관리 서버 또는 배포 지점에서 업데이트를 가져오는 기기는 저장된 달라진 파일을 사용하여 데이터베이스 및 소프트웨어 모듈을 업데이트할 수 있습니다.

달라진 파일 사용을 최적화하려면 기기가 업데이트를 가져오는 중앙 관리 서버 또는 배포 지점의 업데이트 스케줄과 기기의 업데이트 스케줄을 동기화하는 것이 좋습니다. 하지만 기기가 업데이트를 가져오는 중앙 관리 서버 또는 배포 지점에 비해 기기의 업데이트 빈도가 낮아도 트래픽을 절약할 수 있습니다.

달라진 파일 다운로드 기능은 버전 11 이상의 중앙 관리 서버 및 배포 지점에서만 활성화할 수 있습니다. 이전 버전의 중앙 관리 서버 및 배포 지점에 달라진 파일을 저장하려면, 중앙 관리 서버 및 배포 지점을 버전 11 이상으로 업그레이드하십시오.

달라진 파일 다운로드 기능은 업데이트 다운로드의 오프라인 모델과 호환되지 않습니다. 즉, 업데이트 다운로드의 오프라인 모델을 사용하는 네트워크 에이전트는 이러한 네트워크 에이전트에 업데이트를 전달하는 중앙 관리 서버 또는 배포 지점에서 달라진 파일 다운로드 기능이 활성화되어 있어도 달라진 파일을 다운로드하지 않습니다.

배포 지점은 달라진 파일 자동 배포를 위해 IP 멀티캐스팅을 사용하지 않습니다.

diff 파일 다운로드 기능 활성화

필수 구성 요소

이 시나리오의 필수 구성 요소는 다음과 같습니다:

- 중앙 관리 서버와 배포 지점을 버전 11 이상으로 업그레이드합니다.
- 네트워크 에이전트 정책 설정에서 업데이트 다운로드의 오프라인 모델을 비활성화해야 합니다.

단계

1. **중앙 관리 서버에서 기능 활성화**

   중앙 관리 서버 저장소 업데이트 다운로드 작업 설정에서 이 기능을 활성화합니다.

2. **배포 지점에 대한 기능을 활성화하기**

   배포 지점의 저장소로 업데이트 다운로드 작업을 통해 업데이트를 받는 배포 지점에 기능을 사용하도록 설정합니다.

   중앙 관리 서버에서 업데이트를 받는 배포 지점에 기능을 사용하도록 설정합니다.

   네트워크 에이전트 정책 설정에서 이 기능을 활성화합니다. 배포 지점을 수동으로 할당하고 정책 설정을 재정의하려면 중앙 관리 서버 속성의 **배포 지점** 섹션에서 이 기능을 활성화합니다.

달라진 파일 다운로드 기능이 정상적으로 활성화되었는지 확인하려는 경우 시나리오를 수행하기 전과 수행한 후에 내부 트래픽을 측정하면 됩니다.

중앙 관리 서버 저장소 업데이트 다운로드 작업 생성

중앙 관리 서버의 *중앙 관리 서버 저장소로 업데이트 다운로드* 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동 생성합니다. *중앙 관리 서버 저장소 업데이트 다운로드* 작업은 하나만 만들 수 있습니다. 따라서 해당 작업이 중앙 관리 서버 작업 목록에서 제거되었을 때만 *중앙 관리 서버 저장소로 업데이트 다운로드* 작업을 만들 수 있습니다.

중앙 관리 서버 저장소 업데이트 다운로드 작업을 생성하려면 다음과 같이 합니다:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. 다음 방법 중 하나로 작업을 시작합니다:
   - 콘솔 트리에 있는 **작업** 폴더의 마우스 오른쪽 메뉴에서 **새로 만들기 → 작업**를 선택합니다.
   - **작업** 폴더의 작업 영역에서 **작업 생성** 버튼을 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. 마법사의 **작업 유형 선택** 페이지에서 **중앙 관리 서버 저장소 업데이트 다운로드**를 선택합니다.
4. 마법사의 **설정** 페이지에서 다음과 같이 작업 설정을 지정합니다:
   - **업데이트 경로**

     중앙 관리 서버의 업데이트 경로로 다음과 같은 리소스를 사용할 수 있습니다:

     - Kaspersky 업데이트 서버

       Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다. 기본적으로 중앙 관리 서버는 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버를 구성할 수 있습니다.

       기본적으로 선택됩니다.

     - 기본 중앙 관리 서버

       이 리소스는 보조 또는 가상 중앙 관리 서버용으로 생성한 작업에 적용됩니다.

     - 로컬 또는 네트워크 폴더

       최신 업데이트가 포함된 로컬 또는 네트워크 폴더입니다. 네트워크 폴더는 FTP/HTTP 서버이거나 SMB 공유일 수 있습니다. 네트워크 폴더 인증이 필요할 시, SMB 프로토콜만 지원합니다. 로컬 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다.

       업데이트 경로에 사용되는 FTP 또는 HTTP 서버나 네트워크 폴더는 Kaspersky 업데이트 서버 사용 시에 생성되는 구조와 일치하는 폴더 구조(업데이트 포함)를 포함해야 합니다.

- **기타 설정**:
  - **보조 중앙 관리 서버 강제 업데이트**

    이 옵션을 활성화하면 새 업데이트가 다운로드되는 즉시 중앙 관리 서버가 보조 중앙 관리 서버에서 업데이트 작업을 시작합니다. 업데이트 작업은 보조 중앙 관리 서버의 작업 속성에 구성된 업데이트 경로를 사용하여 시작됩니다.

    해당 옵션을 비활성화하면 보조 중앙 관리 서버의 업데이트 작업이 스케줄에 따라 시작됩니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **추가 폴더에 다운로드한 업데이트 복사**

    중앙 관리 서버에서 업데이트를 수신한 후 이를 지정된 폴더에 복사합니다. 네트워크에서 업데이트 배포를 수동으로 관리하려는 경우 이 옵션을 사용합니다.

    이 옵션을 사용할 수 있는 상황의 예로는, 조직 네트워크가 여러 독립 서브넷으로 구성되어 있으며 각 서브넷의 기기가 다른 서브넷에는 액세스할 수 없는 경우를 들 수 있습니다. 하지만 모든 서브넷의 기기는 공통 네트워크 공유에 액세스할 수 있습니다. 이 경우 서브넷 중 하나의 중앙 관리 서버가 Kaspersky 업데이트 서버에서 업데이트를 다운로드하도록 설정하고 이 옵션을 활성화한 다음 해당 네트워크 공유를 지정할 수 있습니다. 다른 중앙 관리 서버에 대한 저장소에 업데이트 다운로드 작업에서 업데이트 경로와 같은 네트워크 공유를 지정합니다.

    다운로드한 업데이트를 로컬 폴더에 복사하도록 선택한 경우, 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다. 폴더 경로는 기기의 운영 체제에 따라 달라집니다. 로컬 폴더는 Linux 기반 중앙 관리 서버에 있으므로 POSIX 형식의 경로(예: /path/to/dir)를 지정해야 합니다.

    Linux 기반 중앙 관리 서버에 있는 네트워크 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기에서 해당 네트워크 폴더를 미리 탑재해 접근할 수 있어야 합니다. 폴더 접근은 SMB 프로토콜을 통해 이루어집니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

    - **복사가 완료되기 전에 기기 및 보조 중앙 관리 서버로 강제 업데이트 안 함**

      메인 업데이트 폴더에서 추가 업데이트 폴더로 업데이트가 복사되어야만 클라이언트 기기와 보조 중앙 관리 서버의 업데이트 다운로드 작업이 시작됩니다.

      클라이언트 기기와 보조 중앙 관리 서버가 추가 네트워크 폴더에서 업데이트를 다운로드하는 경우 이 옵션을 활성화해야 합니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

  - **이전 구성표를 사용해 업데이트 다운로드**

    버전 14부터 Kaspersky Security Center 보안 센터는 새 체계를 사용하여 데이터베이스 및 소프트웨어 모듈 업데이트를 다운로드합니다. 애플리케이션이 새 구성을 사용하여 업데이트를 다운로드하려면 업데이트 소스에 새 구성과 호환되는 메타데이터가 포함된 업데이트 파일이 있어야 합니다. 업데이트 소스에 이전 구성과 호환되는 메타데이터가 있는 업데이트 파일이 포함된 경우 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다. 그렇지 않으면 업데이트 다운로드 작업이 실패합니다.

예를 들어 로컬 또는 네트워크 폴더가 업데이트 소스로 지정되고 이 폴더의 업데이트 파일이 다음 애플리케이션 중 하나에서 다운로드된 경우 이 옵션을 활성화해야 합니다.

- Kaspersky 업데이트 유틸리티

  이 유틸리티는 이전 구성을 사용하여 업데이트를 다운로드합니다.

- Kaspersky Security Center 13.2 또는 이전 버전

  예를 들어, 중앙 관리 서버 1은 인터넷에 연결되어 있지 않습니다. 이 경우 인터넷에 연결된 중앙 관리 서버 2를 사용하여 업데이트를 다운로드한 다음 로컬 또는 네트워크 폴더에 업데이트를 저장하여 중앙 관리 서버 1의 업데이트 소스로 사용할 수 있습니다. 중앙 관리 서버 2의 버전이 13.2 이하인 경우 중앙 관리 서버 1의 작업에서 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

5. 마법사의 **작업 스케줄 구성** 페이지에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

- **시작 스케줄:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

    작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

  - **N일마다**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

    기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **N주마다**

    작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

    기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

  - **N분마다**

    작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

    기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

  - **매일(서머타임 지원 안 함)**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

- **주별**

  이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.

  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

6. 마법사의 **작업 이름 정의** 페이지에서 만들 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

7. 마법사의 **작업 생성 마침** 페이지에서 **완료** 버튼을 눌러 마법사를 닫습니다.

   마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

마법사가 완료되면 작업 영역의 중앙 관리 서버 작업 목록에 **중앙 관리 서버 저장소 업데이트 다운로드**가 표시됩니다.

작업 생성 중에 지정하는 설정뿐 아니라 생성된 작업의 기타 속성도 변경할 수 있습니다.

중앙 관리 서버가 *중앙 관리 서버 저장소로업데이트 다운로드* 작업을 수행하면, 데이터베이스 및 소프트웨어 모듈이 해당하는 업데이트 경로에서 다운로드되어 중앙 관리 서버의 공유 폴더에 저장됩니다. 관리 그룹에 대해 이 작업을 만들면 지정한 관리 그룹에 포함되어 있는 네트워크 에이전트에만 작업이 적용됩니다.

업데이트가 중앙 관리 서버의 공유 폴더에서 클라이언트 기기와 보조 중앙 관리 서버로 배포됩니다.

배포 지점의 저장소로 업데이트 다운로드 작업 생성

macOS를 실행하는 배포 지점 기기는 Kaspersky 업데이트 서버에서 업데이트를 다운로드할 수 없습니다.

macOS를 실행하는 하나 이상의 기기가 *배포 지점의 저장소로 업데이트 다운로드 작업 범위*에 있는 경우 모든 Windows 기기에서 작업이 성공적으로 완료되어도 작업은 *실패* 상태로 완료됩니다.

관리 그룹에 대해 *배포 지점의 저장소로 업데이트 다운로드* 작업을 만들 수 있습니다. 이 작업은 지정한 관리 그룹에 포함된 배포 지점에 대해 실행됩니다.

예를 들어 배포 지점과 Kaspersky 업데이트 서버 간의 트래픽에 비해 중앙 관리 서버와 배포 지점 간의 트래픽에서 더 많은 비용이 발생하거나 중앙 관리 서버에서 인터넷에 연결할 수 없는 경우 이 작업을 사용할 수 있습니다. 배포 지점에서 프록시 서버를 사용하여 인터넷에 연결하는 경우 네트워크 에이전트 정책에서 해당 설정을 지정해야 합니다.

선택한 관리 그룹에 대한 배포 지점 저장소로 업데이트 다운로드 작업을 생성하려면 다음과 같이 하십시오.

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.

2. 이 폴더의 작업 영역에서 **새 작업** 버튼을 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

3. 마법사의 **작업 유형 선택** 페이지에서 **Kaspersky Security Center 중앙 관리 서버** 노드를 선택하고 **고급** 폴더를 확장한 다음 **배포 지점의 저장소로 업데이트 다운로드** 작업을 선택합니다.

4. 마법사의 **설정** 페이지에서 다음과 같이 작업 설정을 지정합니다:

   - **업데이트 경로**

     배포 지점의 업데이트 경로로 다음과 같은 리소스를 사용할 수 있습니다.

     - Kaspersky 업데이트 서버

       Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다.

이 옵션은 기본적으로 선택되어 있습니다.

- 로컬 또는 네트워크 폴더

  최신 업데이트가 포함된 로컬 또는 네트워크 폴더입니다. 네트워크 폴더는 FTP/HTTP 서버이거나 SMB 공유일 수 있습니다. 네트워크 폴더 인증이 필요할 시, SMB 프로토콜만 지원합니다. 로컬 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다.

  업데이트 경로에 사용되는 FTP 또는 HTTP 서버나 네트워크 폴더는 Kaspersky 업데이트 서버 사용 시에 생성되는 구조와 일치하는 폴더 구조(업데이트 포함)를 포함해야 합니다.

- **업데이트 저장 폴더**

  저장된 업데이트를 저장하기 위한 지정된 폴더의 경로입니다. 지정된 폴더 경로를 클립보드에 복사할 수 있습니다. 그룹 작업에 대해 지정된 폴더의 경로를 변경할 수 없습니다.

- **이전 구성표를 사용해 업데이트 다운로드**

  버전 14부터 Kaspersky Security Center 보안 센터는 새 체계를 사용하여 데이터베이스 및 소프트웨어 모듈 업데이트를 다운로드합니다. 애플리케이션이 새 구성을 사용하여 업데이트를 다운로드하려면 업데이트 소스에 새 구성과 호환되는 메타데이터가 있는 업데이트 파일이 포함되어 있어야 합니다. 업데이트 소스에 이전 구성과 호환되는 메타데이터가 있는 업데이트 파일이 포함된 경우 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다. 그렇지 않으면 업데이트 다운로드 작업이 실패합니다.

  예를 들어 로컬 또는 네트워크 폴더가 업데이트 소스로 지정되고 이 폴더의 업데이트 파일이 다음 애플리케이션 중 하나에서 다운로드된 경우 이 옵션을 활성화해야 합니다.

  - Kaspersky 업데이트 유틸리티

    이 유틸리티는 이전 구성을 사용하여 업데이트를 다운로드합니다.

  - Kaspersky Security Center 13.2 또는 이전 버전

    예를 들어 배포 지점은 로컬 또는 네트워크 폴더에서 업데이트를 가져오도록 구성됩니다. 이 경우 인터넷에 연결된 중앙 관리 서버를 사용하여 업데이트를 다운로드한 다음 배포 지점의 로컬 폴더에 업데이트를 저장할 수 있습니다. 중앙 관리 서버의 버전이 13.2 이하인 경우 *배포 지점 저장소에 업데이트 다운로드* 작업에서 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

5. 마법사의 **관리 그룹 선택** 페이지에서 **찾기**를 누르고 작업이 적용되는 관리 그룹을 선택합니다.

6. 마법사의 **작업 스케줄 구성** 페이지에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

   - **시작 스케줄:**

     작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

     - **N시간마다**

       작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

       작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

- **N일마다**

  작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

  기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **N주마다**

  작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

  기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

- **N분마다**

  작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

  기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

- **매일(서머타임 지원 안 함)**

  작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

  이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

  기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

- **주별**

  이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.

  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

7. 마법사의 **작업 이름 정의** 페이지에서 만들 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

8. 마법사의 **작업 생성 마침** 페이지에서 **완료** 버튼을 눌러 마법사를 닫습니다.

   마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

마법사의 작업이 완료되면 대상 관리 그룹의 네트워크 에이전트 작업 목록과 콘솔의 **작업** 작업 영역에 **배포 지점의 저장소로 업데이트 다운로드**가 표시됩니다.

작업 생성 중에 지정하는 설정뿐 아니라 생성된 작업의 기타 속성도 변경할 수 있습니다.

배포 지점의 저장소로 업데이트 강제 다운로드 작업을 수행하면 데이터베이스 및 소프트웨어 모듈용 업데이트가 업데이트 경로에서 다운로드되어 공유 폴더에 저장됩니다. 다운로드한 업데이트는 지정한 관리 그룹에 포함되어 있으며 업데이트 다운로드 작업이 명시적으로 설정되지 않은 배포 지점에만 사용됩니다.

중앙 관리 서버 속성 창의 **섹션** 창에서 **배포 지점**를 차례로 선택합니다. 각 배포 지점의 속성에 있는 **업데이트 경로** 섹션에서 업데이트 경로(**중앙 관리 서버에서 가져오기** 또는 **강제 업데이트 다운로드 작업 사용**)를 지정할 수 있습니다. 기본적으로는 수동이나 자동으로 할당된 배포 지점에 대해 **중앙 관리 서버에서 가져오기**가 선택됩니다. 이러한 배포 지점은 *배포 지점의 저장소로 업데이트 다운로드* 작업의 결과를 사용합니다.

각 배포 지점의 속성은 개별적으로 해당 배포 지점에 대해 설정된 네트워크 폴더를 지정합니다. 폴더 이름은 배포 지점마다 다를 수 있습니다. 그러므로 기기 그룹에 대해 작업을 만든 경우 작업 속성에서 네트워크 폴더를 변경하지 않는 것이 좋습니다.

기기에 대한 로컬 작업을 만드는 경우 *배포 지점의 저장소로 업데이트 다운로드* 작업의 속성에서 업데이트가 포함된 네트워크 폴더를 변경할 수 있습니다.

중앙 관리 서버 저장소 업데이트 다운로드 작업 구성

저장소 업데이트(중앙 관리 서버) 작업을 구성하려면 다음과 같이 합니다:

1. **작업** 콘솔 트리 폴더의 작업 영역에서 **중앙 관리 서버 저장소 업데이트 다운로드** 작업을 선택합니다.
2. 다음 방법 중 하나로 작업 속성 창을 엽니다:
   - 작업의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   - 선택한 작업의 정보 박스에서 **작업 구성** 링크를 누릅니다.

그러면 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업 속성 창이 열립니다. 이 창에서 중앙 관리 서버 저장소에 업데이트를 다운로드하는 방식을 구성할 수 있습니다.

다운로드한 업데이트 검증

관리 중인 기기에 업데이트를 설치하기 전에 먼저 *업데이트 검증* 작업을 통해 업데이트의 운용 가능성 및 오류를 확인할 수 있습니다. *업데이트 검증* 작업은 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업에 포함되어 자동으로 수행됩니다. 중앙 관리 서버는 경로에서 업데이트를 다운로드하고 임시 저장소에 이를 저장한 다음 *업데이트 검증* 작업을 실행합니다. 작업이 성공적으로 완료되면 업데이트가 임시 저장소에서 중앙 관리 서버의 공유 폴더(<Kaspersky Security Center 설치 폴더>\Share\Updates)로 복사됩니다. 이 중앙 관리 서버가 업데이트 경로인 모든 클라이언트 기기에 배포됩니다.

업데이트 검증 작업 결과에 임시 저장소에 있는 업데이트가 잘못된 것으로 나타나거나 *업데이트 검증* 작업이 완료되었으나 오류가 발생하면, 해당 업데이트는 공유 폴더로 복사되지 않습니다. 중앙 관리 서버에는 이전 업데이트 집합이 유지됩니다. 그러면 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후** 스케줄 유형이 포함된 작업이 시작되지 않습니다. 이러한 작업은 다음에 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업이 시작될 때 새 업데이트 검사가 성공적으로 완료되는 경우 수행됩니다.

한 대 이상의 테스트 기기에서 다음 조건 중 하나라도 충족되면 업데이트 집합이 잘못된 것으로 간주됩니다:

- 업데이트 작업 오류가 발생했습니다.
- 업데이트가 적용된 후 보안 제품의 실시간 보호 상태가 변경되었습니다.
- 수동 검사 작업 실행 중 감염된 개체가 탐지되었습니다.
- Kaspersky 애플리케이션에서 런타임 오류가 발생했습니다.

나열된 어떤 조건에도 해당하는 기기가 없다면, 업데이트 세트는 올바른 것으로 간주되며 *업데이트 검증* 작업은 성공적으로 완료된 것으로 간주됩니다.

업데이트 검증 작업 생성을 시작하기 전에 전제 조건을 수행하십시오.

1. 여러 테스트 기기가 있는 관리 그룹을 만듭니다. 업데이트를 확인하려면 이 그룹이 필요합니다.

   네트워크 전체에서 보호 수준을 가장 신뢰할 수 있고 가장 일반적인 애플리케이션 구성을 가진 기기를 사용하는 것이 좋습니다. 이 접근 방식은 검사 중 바이러스 탐지의 품질과 확률을 높이고 오탐지 위험을 최소화합니다. 테스트 기기에서 바이러스가 탐지되면 *업데이트 검증* 작업은 실패한 것으로 간주됩니다.

2. Kaspersky Security Center에서 지원하는 애플리케이션(Kaspersky Endpoint Security for Windows 또는 Kaspersky Security for Windows Server 등)에 대한 *업데이트 및 악성 코드 검사* 작업을 생성합니다. *업데이트 및 악성 코드 검사* 작업 생성 시, 테스트 기기로 관리 그룹을 지정합니다.

   업데이트 검증 작업은 테스트 기기에서 *업데이트* 및 *악성 코드 검사* 작업을 순차적으로 실행하여 모든 업데이트가 유효한지 확인합니다. 또한, *업데이트 검증* 작업 생성 시, *업데이트* 및 *악성 코드 검사* 작업을 지정해야 합니다.

3. *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 생성합니다.

다운로드한 업데이트를 클라이언트 기기로 배포하기 전에 Kaspersky Security Center에서 이를 검증하도록 하려면 다음과 같이 하십시오:

1. **작업** 폴더의 작업 영역에 있는 작업 목록에서 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 선택합니다.
2. 다음 방법 중 하나로 작업 속성 창을 엽니다:
   - 작업의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   - 선택한 작업의 정보 박스에서 **작업 구성** 링크를 누릅니다.
3. *업데이트 검증* 작업이 있다면 **찾기** 버튼을 누릅니다. 열리는 창에서 테스트 기기가 있는 관리 그룹의 *업데이트 검증* 작업을 선택합니다.
4. 이전에 *업데이트 검증* 작업을 생성하지 않았다면 **생성** 버튼을 누릅니다.
   업데이트 검증 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
5. **확인**을 눌러 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업의 속성 창을 닫습니다.

자동 업데이트 검증이 활성화됩니다. 이제 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행할 수 있으며 업데이트 검증부터 시작됩니다.

테스트 정책 및 보조 작업 구성

업데이트 검증 작업을 만들 때 중앙 관리 서버에서는 테스트 정책, 보조 업데이트 작업 및 수동 검사 작업을 생성합니다.

> 보조 그룹 업데이트 및 수동 검사 작업은 다소 시간이 소요됩니다. 이러한 작업은 *업데이트 검증* 작업이 실행되면 수행됩니다. *저장소로 업데이트 다운로드* 작업을 실행하는 동안 *업데이트 검증* 작업이 수행됩니다. *저장소로 업데이트 다운로드* 작업 기간에는 보조 그룹 업데이트와 수동 검사 작업이 포함됩니다.

테스트 정책 및 보조 작업의 설정을 변경할 수 있습니다.

테스트 정책 또는 보조 작업 설정을 변경하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 *업데이트 검증* 작업을 만들 그룹을 선택합니다.
2. 그룹 작업 영역에서 다음 탭 중 하나를 선택합니다:
   - **정책** 테스트 정책 설정을 편집하려는 경우.
   - **작업** 보조 작업 설정을 변경하려는 경우.

3. 탭 작업 영역에서 설정을 변경할 정책 또는 작업을 선택합니다.

4. 다음 방법 중 하나로 정책(작업) 속성 창을 엽니다:

   - 정책(작업)의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   - 선택한 정책(작업)의 정보 박스에서 **정책 구성**(**작업 구성**) 링크를 누릅니다.

업데이트가 올바른지 검증하기 위해 테스트 정책 및 보조 작업 수정 시 다음 제한을 적용합니다:

- 보조 작업 설정의 경우:
  - 중앙 관리 서버에 심각도가 **심각 이벤트** 및 **기능 실패**인 작업을 모두 저장합니다. 중앙 관리 서버에서 이러한 유형의 이벤트를 사용하여 애플리케이션의 작동을 분석합니다.
  - 중앙 관리 서버를 업데이트 경로로 사용합니다.
  - 작업 스케줄 유형을 지정합니다: **수동**.
- 테스트 정책 설정의 경우:
  - iChecker 및 iSwift 검사 가속화 기술 비활성화 (**필수 위협 보호 → 파일 위협 보호 → 설정 → 추가 → 검사 기술**).
  - **치료; 치료에 실패하는 경우 삭제/치료; 치료에 실패하는 경우 차단/차단**. (**필수 위협 보호 → 파일 위협 보호 → 위협 탐지 조치**).
- 테스트 정책 및 보조 작업 설정의 경우:

  소프트웨어 모듈에 업데이트를 설치한 후 기기를 다시 시작해야 하는 경우에는 즉시 다시 시작해야 합니다. 기기를 다시 시작하지 않으면 이러한 유형의 업데이트를 테스트할 수 없습니다. 일부 애플리케이션의 경우 컴퓨터를 다시 시작해야 하는 업데이트 설치가 금지되거나 먼저 사용자에게 확인 메시지를 표시하도록 구성될 수 있습니다. 테스트 정책 및 보조 작업의 설정에서는 이러한 제한을 중지해야 합니다.

다운로드된 업데이트 보기

다운로드된 업데이트 목록을 보려면 다음과 같이 하십시오,

콘솔 트리의 **저장소** 폴더에서 **Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트** 하위 폴더를 선택합니다.

Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트 폴더의 작업 영역에 중앙 관리 서버에 저장된 업데이트의 목록이 표시됩니다.

기기에서 Kaspersky Endpoint Security 업데이트 자동 설치

클라이언트 기기에 있는 Kaspersky Endpoint Security의 데이터베이스 및 소프트웨어 모듈에 대한 자동 업데이트를 구성할 수 있습니다.

기기에 있는 Kaspersky Endpoint Security에 대해 다운로드와 자동 업데이트 설치를 구성하려면:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. 다음 방법 중 하나로 **업데이트** 작업을 만듭니다:
   - 콘솔 트리에 있는 **작업** 폴더의 마우스 오른쪽 메뉴에서 **새로 만들기 → 작업**를 선택합니다.
   - **작업** 폴더의 작업 영역에 있는 **새 작업** 버튼을 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. 마법사의 **작업 유형 선택** 페이지에서, 작업 유형으로 **Kaspersky Endpoint Security**를 선택한 다음에 작업 하위 유형으로 **업데이트**를 선택합니다.
4. 마법사의 나머지 지침을 따릅니다.

   마법사를 완료한 후 Kaspersky Endpoint Security용 업데이트 작업이 생성됩니다. 새롭게 생성된 작업은 **작업** 폴더에서 작업 영역의 작업 목록에 표시됩니다.
5. **작업** 폴더의 작업 영역에서 생성한 업데이트 작업을 선택합니다.
6. 작업의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
7. 작업 속성 창이 열리면 **섹션** 창에서 **옵션**을 선택합니다.

   옵션 섹션에서 로컬 또는 모바일 모드로 업데이트 작업 설정을 정의할 수 있습니다:
   - **로컬 모드의 업데이트 설정**: 기기와 중앙 관리 서버 사이에 연결이 구성됩니다.
   - **모바일 모드의 업데이트 설정**: Kaspersky Security Center와 기기 사이에 연결이 설정되지 않습니다(예: 기기가 인터넷에 연결되지 않았을 때).
8. 업데이트 경로를 선택하려면, **설정** 버튼을 누릅니다.
9. 애플리케이션 데이터베이스와 함께 애플리케이션 모듈을 다운로드하고 설치하려면, **애플리케이션 모듈 업데이트 다운로드** 옵션을 선택합니다.

   확인란이 선택되어 있다면, Kaspersky Endpoint Security는 소프트웨어 모듈 업데이트가 있을 경우 이를 사용자에게 알리고 업데이트 작업을 실행할 때 업데이트 패키지 안에 소프트웨어 모듈 업데이트를 포함합니다. 업데이트 모듈 사용을 구성합니다:
   - **긴급 및 승인된 업데이트 설치**. 소프트웨어 모듈에 대한 업데이트가 이용 가능하면, Kaspersky Endpoint Security는 자동으로 *심각* 상태를 가진 것만 설치합니다; 나머지 업데이트는 관리자의 승인 이후에 설치됩니다.
   - **승인된 업데이트만 설치**. 소프트웨어 모듈 업데이트가 이용 가능하면, Kaspersky Endpoint Security는 해당 설치가 승인된 이후에 설치합니다; 애플리케이션 인터페이스를 사용해 로컬에서 설치되거나 Kaspersky Security Center를 통해 업데이트가 설치됩니다.

   소프트웨어 모듈 업데이트가 라이센스 계약서 및 개인정보취급방침의 조장에 대해 검토하고 수락을 요구한다면, 애플리케이션은 최종 사용자 라이센스 계약서 및 개인정보취급방침이 관리자에 의해 수락된 후 업데이트를 설치합니다.
10. **찾기** 버튼을 클릭하여 지정된 폴더에 다운로드 된 업데이트를 저장하기 위해 **폴더로 업데이트 복사** 옵션을 선택합니다.
11. **확인**을 누릅니다.

업데이트 작업을 실행할 때 애플리케이션은 Kaspersky 업데이트 서버로 요청을 보냅니다.

일부 업데이트는 최신 버전의 관리 플러그인 설치를 요구하기도 합니다.

업데이트 다운로드의 오프라인 모델

관리 중인 기기에 설치된 네트워크 에이전트는 가끔 업데이트를 받을 수 있는 중앙 관리 서버에 연결하지 못할 수 있습니다. 예를 들어, 네트워크 에이전트가 노트북에 설치되어 있어 인터넷 연결이 안되는 곳에 있거나 로컬 네트워크 접속이 불가능할 경우입니다. 또, 관리자가 기기의 네트워크 연결 시간을 제한하는 경우도 있습니다. 그런 경우, 네트워크 에이전트가 설치된 기기는 기존 스케줄에 따라 중앙 관리 서버에서 업데이트를 받지 못합니다. 네트워크 에이전트를 사용해 관리 중인 애플리케이션(Kaspersky Endpoint Security 등)의 업데이트를 구성했다면, 각각의 업데이트는 중앙 관리 서버로의 연결을 요구하게 됩니다. 네트워크 에이전트와 중앙 관리 서버와의 연결이 끊겨 있다면, 업데이트는 불가능합니다. 네트워크 에이전트가 지정된 스케줄에 따라 중앙 관리 서버에 연결되도록 네트워크 에이전트와 중앙 관리 서버 간의 연결을 구성할 수 있습니다. 최악의 경우, 연결이 안되는 동안 스케줄이 걸릴 경우 해당 데이터베이스는 업데이트되지 않습니다. 게다가 여러 관리 중인 애플리케이션이 업데이트를 받기 위해 중앙 관리 서버에 동시에 접속을 시도하면 문제가 발생할 수 있습니다. 이 경우에는 해당 중앙 관리 서버가 요청에 대한 응답이 중지될 수 있습니다(DDoS 공격에 당하는 것과 유사).

위에서 설명한 문제를 방지하려면 관리 중인 애플리케이션의 업데이트와 모듈에 대한 오프라인 다운로드 모드가 Kaspersky Security Center에 구현되어야 합니다. 이 모드는 일시적으로 중앙 관리 서버 통신 채널에 대한 접근이 원활하지 않은 경우에도 업데이트 배포 메커니즘을 제공합니다. 또한 이 모델을 사용하면 중앙 관리 서버의 부하도 감소합니다.

업데이트 다운로드의 오프라인 모델 작업 방법

중앙 관리 서버는 업데이트를 받을 때마다 네트워크 에이전트가 설치되어 있는 기기에서 관리 중인 애플리케이션에 대해 필요한 업데이트를 네트워크 에이전트에 통지합니다. 네트워크 에이전트가 업데이트 정보를 수신하면 중앙 관리 서버에서 미리 관련 파일을 다운로드합니다. 네트워크 에이전트와의 첫 연결에서, 중앙 관리 서버는 업데이트 다운로드를 시작합니다. 네트워크 에이전트가 모든 업데이트를 클라이언트 기기에 다운로드하고 나면 해당 기기의 애플리케이션이 업데이트를 사용할 수 있게 됩니다.

클라이언트 기기에 있는 관리 애플리케이션이 업데이트를 위해 네트워크 에이전트에 접근하면, 이 네트워크 에이전트는 모든 필요한 업데이트가 있는지 확인합니다. 업데이트가 해당 관리 중인 애플리케이션에 대한 것이고 중앙 관리 서버에서 25시간 이내에 받은 것이라면, 네트워크 에이전트는 중앙 관리 서버에 연결하지 않고 로컬 캐시에서 해당 업데이트를 관리 중인 애플리케이션에 공급합니다. 네트워크 에이전트가 클라이언트 기기의 애플리케이션에 업데이트를 제공하는데 업데이트를 위한 연결이 필요하지 않을 때는 중앙 관리 서버와의 연결이 설정되지 않을 수 있습니다.

중앙 관리 서버의 부하를 줄이기 위해, 기기에 설치된 네트워크 에이전트는 중앙 관리 서버에 연결하고 중앙 관리 서버에 의해 지정된 시간 간격 동안 임의의 순서로 업데이트를 다운로드합니다. 이 시간 간격은 업데이트를 다운로드하는 네트워크 에이전트가 설치된 기기의 개수와 해당 업데이트의 크기에 따라 달라집니다. 중앙 관리 서버의 부하를 줄이기 위해 배포 지점로 네트워크 에이전트를 사용할 수 있습니다.

업데이트 다운로드의 오프라인 모델이 비활성화되어 있으면 업데이트 다운로드 작업의 스케줄에 따라 업데이트가 배포됩니다.

기본적으로 업데이트 다운로드의 오프라인 모델은 활성되어 있습니다.

업데이트 다운로드 오프라인 모델은 관리 중인 애플리케이션을 통한 업데이트 가져오기 작업의 스케줄 유형이 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**로 선택되어 있는 관리 중인 기기에서만 사용됩니다. 나머지 관리 중인 기기의 경우에는 표준 구성을 사용하여 실시간 모드로 중앙 관리 서버에서 업데이트를 가져옵니다.

관리 중인 애플리케이션이 중앙 관리 서버가 아닌 Kaspersky 서버 또는 네트워크 폴더에서 업데이트를 가져오도록 설정되어 있으며 업데이트 다운로드 작업의 스케줄 유형이 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**로 선택되어 있는 경우 관련 관리 그룹의 네트워크 에이전트 정책 설정을 사용하여 업데이트 다운로드의 오프라인 모델을 중지하는 것이 좋습니다.

업데이트 다운로드 오프라인 모델 활성 및 비활성

업데이트 다운로드 오프라인 모델은 비활성하지 않는 것이 좋습니다. 이 모델을 비활성하면 기기로 업데이트를 전달하는 작업이 실패할 수 있습니다. 경우에 따라 Kaspersky 기술 지원 서비스 전문가가 **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드** 확인란 선택을 취소하는 것이 좋다는 지침을 제공할 수 있습니다. 이 경우 Kaspersky 애플리케이션용 업데이트 수신을 위한 작업을 설정했는지 확인해야 합니다.

관리 그룹의 업데이트 다운로드 오프라인 모델을 활성화하거나 비활성화하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 업데이트 다운로드 오프라인 모델을 활성해야 하는 관리 그룹을 선택합니다.
2. 그룹 작업 영역에서 **정책** 탭을 엽니다.
3. **정책** 탭에서 네트워크 에이전트 정책을 선택합니다.
4. 정책의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   네트워크 에이전트 정책의 속성 창을 엽니다.
5. **패치 및 업데이트 관리** 섹션을 선택합니다.
6. **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드(권장)** 확인란을 선택하거나 선택을 취소하여 업데이트 다운로드의 오프라인 모델을 활성화하거나 비활성화합니다.
   기본적으로 업데이트 다운로드의 오프라인 모델은 활성되어 있습니다.

업데이트 다운로드 오프라인 모델이 활성 또는 비활성됩니다.

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치

기본적으로 다음 애플리케이션 구성 요소용으로 다운로드된 모든 업데이트와 패치가 자동으로 설치됩니다:

- Windows용 네트워크 에이전트
- 관리 콘솔
- iOS MDM 서버

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치는 Windows를 실행 중인 기기에서만 사용 가능합니다. 이러한 구성 요소에 대해 자동 업데이트 및 패치를 비활성할 수 있습니다. 이 경우 다운로드된 업데이트와 패치는 해당 상태를 *승인됨*으로 변경해야 설치됩니다. *정의 안 됨* 상태의 업데이트와 패치는 설치되지 않습니다.

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성/비활성

Kaspersky Security Center 구성 요소용 업데이트 및 패치 자동 설치는 기기에 네트워크 에이전트를 설치할 때 기본적으로 활성됩니다. 네트워크 에이전트 설치 중에 업데이트 및 패치 자동 설치를 비활성할 수도 있고, 나중에 정책을 사용하여 자동 설치를 비활성할 수도 있습니다.

기기에서 네트워크 에이전트 로컬 설치를 수행하는 동안 Kaspersky Security Center 구성 요소의 자동 업데이트와 패치를 비활성하려면 다음과 같이 하십시오:

1. 기기에서 네트워크 에이전트 로컬 설치를 시작합니다.
2. **고급 설정** 단계에서 **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 확인란 선택을 취소합니다.
3. 마법사의 지침을 따릅니다.

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치가 비활성된 네트워크 에이전트가 기기에 설치됩니다. 정책을 사용하여 나중에 자동 업데이트 및 패치를 활성할 수 있습니다.

설치 패키지를 통해 기기에서 네트워크 에이전트 설치를 수행하는 동안 Kaspersky Security Center 구성 요소의 자동 업데이트와 패치를 비활성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **원격 설치** → **설치 패키지** 폴더를 선택합니다.
2. **Kaspersky Security Center 네트워크 에이전트<버전 번호>** 패키지의 마우스 오른쪽 메뉴에서 **속성**을(를) 선택합니다.
3. 설치 패키지 속성의 **설정** 섹션에서 **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 확인란 선택을 취소합니다.

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치가 비활성된 네트워크 에이전트가 이 패키지에서 설치됩니다. 정책을 사용하여 나중에 자동 업데이트 및 패치를 활성할 수 있습니다.

기기에 네트워크 에이전트를 설치하는 중에 이 확인란을 선택하거나 선택을 취소한 경우 나중에 네트워크 에이전트 정책을 사용하여 자동 업데이트를 활성하거나 비활성할 수 있습니다.

네트워크 에이전트 정책을 사용하여 Kaspersky Security Center 구성 요소의 자동 업데이트와 패치를 활성하거나 비활성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 자동 업데이트 및 패치를 활성 또는 비활성해야 하는 관리 그룹을 선택합니다.
2. 그룹 작업 영역에서 **정책** 탭을 엽니다.
3. **정책** 탭에서 네트워크 에이전트 정책을 선택합니다.
4. 정책의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   네트워크 에이전트 정책의 속성 창을 엽니다.
5. **패치 및 업데이트 관리** 섹션을 선택합니다.

6. **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 확인란을 선택하거나 선택을 취소하여 자동 업데이트 및 패치를 활성화하거나 비활성화합니다.

7. 이 확인란에 잠금을 설정합니다.

정책이 선택한 기기에 적용되고 해당 기기에서 Kaspersky Security Center 구성 요소 자동 업데이트 및 패치가 활성되거나 비활성됩니다.

업데이트 자동 배포

Kaspersky Security Center에서는 클라이언트 기기와 보조 중앙 관리 서버에 자동으로 업데이트를 배포하고 설치할 수 있습니다.

클라이언트 기기에 업데이트 자동 배포

업데이트가 중앙 관리 서버 저장소로 다운로드된 직후 클라이언트 기기에 선택한 애플리케이션의 업데이트를 자동으로 배포하려면 다음과 같이 하십시오:

1. 클라이언트 기기를 관리하는 중앙 관리 서버에 연결합니다.

2. 다음 방법 중 하나로 선택한 클라이언트 기기에 대한 업데이트 배포 작업을 만듭니다:

   - 선택한 관리 그룹에 속한 클라이언트 기기에 업데이트를 배포하려면 선택한 그룹에 대한 작업을 만듭니다.
   - 다른 관리 그룹에 속하거나 어떤 관리 그룹에도 속하지 않는 클라이언트 기기에 업데이트를 배포하려면 특정 기기에 대한 작업을 만듭니다.

   새 작업 마법사가 시작됩니다. 지침을 따르고 다음 작업을 수행하십시오:

   a. **작업 유형** 마법사 창에서 필요한 애플리케이션 노드에 있는 업데이트 배포 작업을 선택합니다.

      작업 유형 창에 표시되는 업데이트 배포 작업 이름은 이 작업을 만드는 대상 애플리케이션에 따라 달라집니다. 선택한 Kaspersky 애플리케이션의 업데이트 작업 이름에 대한 자세한 내용은 해당 설명서를 참조하십시오.

   b. **스케줄** 마법사 창의 **시작 스케줄** 필드에서 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**를 선택합니다.

   이제 중앙 관리 서버 저장소로 업데이트가 다운로드될 때마다 선택한 기기에 대해 만들어진 업데이트 배포 작업이 시작됩니다.

필요한 애플리케이션의 업데이트 배포 작업을 선택한 기기에 이미 만들었으면, **스케줄** 섹션의 작업 속성 창에서 클라이언트 기기로 업데이트를 자동 배포하기 위해 **시작 스케줄** 필드에서 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**를 시작 옵션을 선택합니다.

보조 중앙 관리 서버에 업데이트 자동 배포

업데이트가 기본 중앙 관리 서버 저장소로 다운로드된 직후 보조 중앙 관리 서버에 선택한 애플리케이션의 업데이트를 배포하려면 다음과 같이 하십시오:

1. 콘솔 트리의 기본 중앙 관리 서버 노드에서 **작업** 폴더를 선택합니다.
2. 작업 영역의 작업 목록에서 중앙 관리 서버의 중앙 관리 서버 저장소 업데이트 다운로드 작업을 선택합니다.
3. 다음 방법 중 하나로 선택한 작업의 **설정** 섹션을 엽니다:
   - 작업의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 선택한 작업의 정보 박스에서 **설정 편집** 링크를 누릅니다.
4. 작업 속성 창의 **설정** 섹션에서 **기타 설정** 하위 섹션을 선택한 다음 **구성** 링크를 누릅니다.
5. 열리는 **기타 설정** 창에서 **보조 중앙 관리 서버 강제 업데이트** 확인란을 선택합니다.
6. 중앙 관리 서버의 업데이트 다운로드 작업 설정에서 작업 속성 창의 **설정** 탭에 있는 **보조 중앙 관리 서버 강제 업데이트** 확인란을 선택합니다.

기본 중앙 관리 서버가 업데이트를 검색하면 스케줄에 관계 없이 보조 중앙 관리 서버에서 업데이트 다운로드 작업이 자동 시작됩니다.

기본 중앙 관리 서버는 보조 중앙 관리 서버에 설치된 애플리케이션에 따라 안티 바이러스 데이터베이스를 업데이트합니다. 기본 중앙 관리 서버에 추가 플러그인을 설치하거나 설치 패키지를 생성할 필요가 없습니다.

배포 지점 자동 할당

배포 지점을 자동으로 할당하는 것이 좋습니다. 그러면 Kaspersky Security Center는 배포 지점을 할당해야 하는 기기를 자체적으로 선택합니다.

배포 지점을 자동으로 할당하려면 다음 절차를 따르십시오.

1. 메인 애플리케이션 창을 엽니다.
2. 콘솔 트리에서 배포 지점을 자동으로 할당할 중앙 관리 서버 노드를 선택합니다.
3. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 클릭합니다.
4. 중앙 관리 서버 속성 창의 **섹션** 창에서 **배포 지점**를 차례로 선택합니다.

5. 창의 오른쪽에서 **배포 지점 자동 할당** 옵션을 선택합니다.

> 배포 지점 역할을 수행하는 기기를 자동으로 할당하면, 배포 지점을 수동으로 구성할 수 없으며 배포 지점 목록도 편집할 수 없습니다.

6. **확인**을 누릅니다.

중앙 관리 서버는 자동으로 배포 지점을 할당하고 구성합니다.

수동으로 배포 지점 기기 할당

Kaspersky Security Center를 사용하면 배포 지점 역할을 수행하는 기기를 할당할 수 있습니다.

배포 지점을 자동으로 할당하는 것이 좋습니다. 이 경우 Kaspersky Security Center는 배포 지점을 할당해야 하는 기기를 자체적으로 선택합니다. 그러나 어떠한 이유로 배포 지점을 자동으로 할당하지 않도록 해야 하는 경우(예, 배포 지점 전용 서버를 사용하고자 할 경우)에는 배포 지점 개수와 구성을 계산한 후에 배포 지점을 수동으로 할당할 수 있습니다.

배포 지점 기능을 하는 기기는 무단으로 접근할 수 없도록 보호(물리적 보호 포함)해야 합니다.

수동으로 배포 지점 역할을 수행하는 기기를 할당하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창에서 **배포 지점** 섹션을 선택하고 **추가** 버튼을 누릅니다. 이 버튼은 **수동으로 배포 지점 할당**을 선택한 경우에 사용할 수 있습니다.
   배포 지점 추가 창이 열립니다.
4. **배포 지점 추가** 창에서 다음 동작을 수행합니다:
   a. 배포 지점 역할을 수행하는 기기를 선택합니다(관리 그룹에서 선택 또는 기기의 IP 주소 지정). 기기를 선택할 때 배포 지점의 운영 특성과 배포 지점 역할을 수행하는 기기에 대한 요구 사항을 유의하십시오.
   b. 배포 지점이 업데이트를 배포할 특정 기기를 지정합니다. 관리 그룹 또는 네트워크 위치 설명을 지정할 수 있습니다.
5. **확인**를 누릅니다.
   추가한 배포 지점은 **배포 지점** 섹션의 배포 지점 목록에 표시됩니다.
6. 목록에서 새로 추가된 배포 지점을 선택하고 **속성** 버튼을 눌러 속성 창을 엽니다.
7. 속성 창에서 배포 지점 구성:

- **일반** 섹션에는 클라이언트 기기와 배포 지점 간의 상호 작용 설정이 포함되어 있습니다.
  - **SSL 포트**

    > SSL을 사용하는 클라이언트 기기와 배포 지점 간의 암호화된 연결용 SSL 포트의 번호입니다.
    > 기본적으로 포트 13000이 사용됩니다.

- **멀티캐스트 사용**

  이 옵션을 사용하면 IP 멀티캐스트를 사용하여 설치 패키지가 그룹의 클라이언트 기기에 자동으로 배포됩니다.

  IP 멀티캐스팅을 사용하면 설치 패키지에서 클라이언트 기기 그룹으로 애플리케이션을 설치하는 데 걸리는 시간은 줄어들지만 단일 클라이언트 기기로 애플리케이션을 설치하는 경우에는 설치 시간이 증가합니다.

- **IP 멀티캐스트 주소**

  멀티캐스팅에 사용할 IP 주소입니다. 224.0.0.0 – 239.255.255.255 범위의 IP 주소를 정의할 수 있습니다

  기본적으로 Kaspersky Security Center는 주어진 범위 내에서 고유한 IP 멀티캐스트 주소를 자동으로 할당합니다.

- **IP 멀티캐스트 포트 번호**

  IP 멀티캐스팅용 포트의 번호입니다.

  기본 포트 번호는 15001입니다. 중앙 관리 서버가 설치된 기기가 배포 지점으로 지정된 경우 기본적으로 포트 13001이 SSL 연결에 사용됩니다.

- **업데이트 배포**

  업데이트는 다음 소스에서 관리 중인 기기로 배포됩니다.

  - 이 옵션이 활성화된 경우 이 배포 지점입니다.
  - 이 옵션이 비활성화된 경우 다른 배포 지점, 중앙 관리 서버 또는 Kaspersky 업데이트 서버입니다.

  배포 지점을 사용하여 업데이트를 배포하면 다운로드 수가 줄어들기 때문에 트래픽을 절약할 수 있습니다. 또한 중앙 관리 서버의 로드를 줄이고 배포 지점 간에 부하를 재배치할 수 있습니다. 네트워크에 필요한 배포 지점의 수를 계산 하여 트래픽과 부하를 최적화할 수 있습니다.

  이 옵션을 비활성화하면 업데이트 다운로드 수와 중앙 관리 서버의 부하가 증가할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다.

- **설치 패키지 배포**

  설치 패키지는 다음 소스에서 관리 중인 기기로 배포됩니다.

  - 이 옵션이 활성화된 경우 이 배포 지점입니다.
  - 이 옵션이 비활성화된 경우 다른 배포 지점, 중앙 관리 서버 또는 Kaspersky 업데이트 서버입니다.

  배포 지점을 사용하여 설치 패키지를 배포하면 다운로드 수가 줄어들기 때문에 트래픽을 절약할 수 있습니다. 또한 중앙 관리 서버의 로드를 줄이고 배포 지점 간에 부하를 재배치할 수 있습니다. 네트워크에 필요한 배포 지점의 수를 계산 하여 트래픽과 부하를 최적화할 수 있습니다.

  이 옵션을 비활성화하면 설치 패키지 다운로드 수와 중앙 관리 서버의 부하가 증가할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다.

- **이 배포 지점을 푸시 서버로 사용하기**

  Kaspersky Security Center에서 배포 지점은 모바일 프로토콜을 통해 관리 중인 기기의 푸시 서버로 작동할 수 있습니다. 예를 들어, KasperskyOS 기기를 중앙 관리 서버에 강제로 동기화하려면 푸시 서버를 활성화해야 합니다. 푸시 서버에는 푸시 서버가 활성화된 배포 지점과 동일한 수준의 관리 중인 기기가 있습니다. 동일한 관리 그룹에 여러 배포 지점이 할당된 경우 각 배포 지점에서 푸시 서버를 활성화할 수 있습니다. 이 경우 중앙 관리 서버는 배포 지점 간의 로드 균형을 조정합니다.

  KasperskyOS가 설치된 기기를 관리하거나 관리할 계획이라면 배포 지점을 푸시 서버로 사용해야 합니다. 클라이언트 기기에 푸시 알림을 보내려면 배포 지점을 푸시 서버로 사용할 수도 있습니다.

- **푸시 서버 포트**

  클라이언트 기기가 연결에 사용할 배포 지점의 포트입니다. 기본적으로 포트 13295이 사용됩니다.

- **범위** 섹션에서는 배포 지점이 어느 범위까지 업데이트를 배포할 것인지 지정합니다(관리 그룹 및/또는 네트워크 위치).

- **KSN 프록시** 섹션에서는 애플리케이션이 배포 지점을 사용하여 관리 중인 기기에서 KSN 요청을 전달하도록 구성할 수 있습니다.

  - **배포 지점 측에서 KSN 프록시 기능 활성화**

    배포 지점으로 사용되는 기기에서 KSN 프록시 서비스가 실행됩니다. 네트워크에서 트래픽을 재분배하고 최적화하려면 이 기능을 사용합니다.

    배포 지점은 Kaspersky Security Network 진술문에 나열된 KSN 통계를 Kaspersky에 보냅니다.

    기본적으로 이 옵션은 비활성화되어 있습니다. 중앙 관리 서버 속성 창에서 **KSN 프록시 서버로 중앙 관리 서버 사용**과 **Kaspersky Security Network 사용에 동의합니다** 옵션이 활성화되어야만 이 옵션이 활성화됩니다.

    액티브-패시브 클러스터의 노드에 배포 지점을 할당하고 이 노드에 KSN 프록시 서버를 활성화할 수 있습니다.

  - **중앙 관리 서버에 KSN 요청 전달**

    배포 지점이 관리 중인 기기에서 중앙 관리 서버로 KSN 요청을 전달합니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근**

    배포 지점이 관리 중인 기기에서 KSN 클라우드 또는 KPSN으로 KSN 요청을 전달합니다. 배포 지점 자체에서 생성된 KSN 요청은 KSN 클라우드 또는 KPSN으로 직접 전송됩니다.

    네트워크 에이전트 버전 11 이하가 설치된 배포 지점은 KPSN에 직접 접근할 수 없습니다. KSN 요청을 KPSN으로 전송하도록 배포 지점을 재구성하면, 각 배포 지점에 대하여 **중앙 관리 서버에 KSN 요청 전달** 옵션을 활성화합니다.

    네트워크 에이전트 버전 12 이상이 설치된 배포 지점은 KPSN에 직접 접근할 수 있습니다.

- **사설 KPSN에 연결할 때 프록시 서버 설정 무시**

  배포 지점 속성 또는 네트워크 에이전트 정책에 프록시 서버 설정이 구성되어 있지만 네트워크 아키텍처에서 KPSN을 직접 사용해야 한다면 이 옵션을 활성화합니다. 이렇게 하지 않으면 관리 중인 애플리케이션의 요청을 KPSN으로 전송할 수 없습니다.

  이 옵션을 사용하려면 **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근** 옵션을 활성화해야 합니다.

- **TCP 포트**

  관리 중인 기기가 KSN 프록시 서버에 연결하는 데 사용할 TCP 포트의 번호입니다. 기본 포트 번호는 13111입니다.

- **UDP 포트**

  UDP 포트를 통해 네트워크 에이전트를 중앙 관리 서버에 연결하려면, **UDP 포트 사용** 옵션을 선택하고 **UDP 포트 번호**를 지정합니다. 기본적으로 이 옵션은 켜져 있습니다. 중앙 관리 서버에 연결하는 기본 UDP 포트는 15000입니다.

- **HTTPS 포트**

  HTTPS 포트를 통해 관리 중인 기기를 KSN 프록시 서버에 연결하려면, **HTTPS 사용** 옵션을 선택하고 **HTTPS 포트 번호**를 지정합니다. KSN 프록시 서버에 연결하는 기본 HTTPS 포트는 17111입니다.

- **기기 발견** 섹션에서 배포 지점에 의한 Windows 도메인, Active Directory 및 IP 범위의 검색을 구성합니다.

  - **Windows 도메인**

    Windows 도메인에 대해 기기 발견을 활성화하고 발견 스케줄을 설정할 수 있습니다.

  - **Active Directory**

    Active Directory에 대해 네트워크 검색을 활성화하고 검색 스케줄을 설정할 수 있습니다.

    Windows 배포 지점을 사용한다면 다음 옵션 중 하나를 선택할 수 있습니다.

    - **현재 Active Directory 도메인 검색**.
    - **Active Directory 도메인 포레스트 검색**.
    - **선택한 Active Directory 도메인만 검색**. 이 옵션을 선택하는 경우 Active Directory 도메인 하나 이상을 목록에 추가합니다.

    네트워크 에이전트 버전 15가 설치된 Linux 배포 지점을 사용하는 경우 주소 및 사용자 자격 증명을 지정한 Active Directory 도메인만 검색할 수 있습니다. 현재 Active Directory 도메인 및 Active Directory 도메인 포레스트에 대한 검색을 사용할 수 없습니다.

  - **IP 범위**

    IPv4 범위 및 IPv6 네트워크에 대해 기기 발견을 활성화할 수 있습니다.

    범위 검색 사용 옵션을 사용하는 경우 검사 범위를 추가하고 해당 범위에 대해 스케줄을 설정할 수 있습니다. 검사한 범위 목록에 IP 범위를 추가할 수 있습니다.

이 **Zeroconf을 사용하여 IPv6 네트워크 검색** 옵션을 활성화하면 배포 지점에서 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 IPv6 네트워크를 자동으로 검색합니다. 이 경우 배포 지점에서 전체 네트워크를 검색하기 때문에 지정된 IP 범위가 무시됩니다. 배포 지점에서 Linux를 실행 시, **Zeroconf을 사용하여 IPv6 네트워크 검색** 옵션을 사용할 수 있습니다. Zeroconf IPv6 검색을 사용하려면, 배포 지점에 avahi-browse 유틸리티를 설치해야 합니다.

- **고급** 섹션에서 배포된 데이터를 저장하기 위해 배포 지점이 사용할 폴더를 지정합니다.
  - **기본 폴더 사용**

    이 옵션을 선택하면 애플리케이션이 배포 지점의 네트워크 에이전트 설치 폴더를 사용합니다.

  - **지정한 폴더 사용**

    이 옵션을 선택하면 아래의 필드에서 폴더의 경로를 지정할 수 있습니다. 이 폴더는 배포 지점의 로컬 폴더일 수도 있고, 회사 네트워크에 있는 기기의 폴더일 수도 있습니다.

    배포 지점에서 네트워크 에이전트를 실행하는 데 사용되는 사용자 계정에는 지정한 폴더에 대한 읽기/쓰기 권한이 있어야 합니다.

선택한 기기는 배포 지점로 역할을 수행하게 됩니다.

Windows 운영 체제를 실행하는 기기만 해당 네트워크 위치를 확인할 수 있습니다. 다른 운영 체제를 실행하는 기기의 경우에는 네트워크 위치를 확인할 수 없습니다.

배포 지점 목록에서 기기 제거

배포 지점 목록에서 컴퓨터를 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **배포 지점** 섹션에서 배포 지점의 역할을 하는 기기를 선택하고 **제거** 버튼을 누릅니다.

   그러면 선택된 기기는 배포 지점 목록에서 제거되고 배포 지점의 역할을 하지 않게 됩니다.

배포 지점이 중앙 관리 서버에 의해 자동으로 할당된 경우에는 배포 지점 목록에서 해당 기기를 제거할 수 없습니다.

배포 지점을 통해 업데이트 다운로드

Kaspersky Security Center는 배포 지점이 중앙 관리 서버, Kaspersky 서버, 로컬 또는 네트워크 폴더에서 업데이트를 받을 수 있도록 허용합니다.

업데이트 경로를 지정할 필요가 없다면 관리 그룹에 대한 *배포 지점 저장소에 업데이트 다운로드* 작업을 사용하는 것이 좋습니다. 자세한 내용은 다음 항목을 참조하십시오: 배포 지점 저장소에 업데이트 다운로드 작업 생성.

배포 지점을 위해 업데이트 다운로드를 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **배포 지점** 섹션에서 그룹에 있는 클라이언트 기기로 업데이트를 전달하는 배포 지점을 선택합니다.
4. 선택한 배포 지점의 속성 창을 열려면 **속성** 버튼을 누릅니다.
5. 배포 지점 속성 창에서 **업데이트 경로** 섹션을 선택합니다.
6. 배포 지점을 위한 업데이트 경로를 선택하십시오:
   - 배포 지점이 중앙 관리 서버에서 업데이트를 받게 하려면, **중앙 관리 서버에서 가져오기**를 선택합니다:
     - **diff 파일 다운로드**

       이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

       기본적으로 이 옵션은 켜져 있습니다.
   - 배포 지점에서 작업을 사용하여 업데이트를 받게 하려면 **강제 업데이트 다운로드 작업 사용**를 선택합니다:
     - 해당 작업이 이미 기기에 있다면 **찾기** 버튼을 누르고 나타나는 목록에서 해당 작업을 선택하십시오.
     - 해당 작업이 아직 기기에 없다면 **새 작업** 버튼을 눌러 작업을 만듭니다. 새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

   배포 지점의 저장소로 업데이트 다운로드 작업은 로컬 작업입니다. 배포 지점의 역할을 수행하는 각 기기에 대해 새 작업을 생성해야 합니다.

배포 지점이 지정한 경로에서 업데이트를 가져오게 됩니다.

저장소에서 소프트웨어 업데이트 삭제

중앙 관리 서버 저장소에서 소프트웨어 업데이트를 삭제하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **소프트웨어 업데이트** 하위 폴더를 선택합니다.
2. **소프트웨어 업데이트** 폴더의 작업 영역에서 삭제할 업데이트를 선택합니다.
3. 기기의 마우스 오른쪽 메뉴에서 **업데이트 파일 삭제**를 선택합니다.

소프트웨어 업데이트가 중앙 관리 서버 저장소에서 삭제됩니다.

클러스터 모드에서 Kaspersky 애플리케이션에 대한 패치 설치

Kaspersky Security Center는 클러스터 모드의 Kaspersky 애플리케이션용 패치의 수동 설치만 지원합니다.

Kaspersky 애플리케이션의 패치를 설치하려면 다음과 같이 하십시오:

1. 각 클러스터 노드에 패치를 다운로드합니다.
2. 활성 노드에서 패치 설치를 실행합니다.
3. 패치가 정상적으로 설치될 때까지 기다립니다.
4. 클러스터의 모든 하위 노드에서 패치를 연속적으로 실행합니다.
   명령줄에서 패치를 실행하는 경우 `-CLUSTER_SECONDARY_NODE` 키를 사용합니다.
   그러면 패치가 클러스터의 모든 노드에 설치됩니다.
5. Kaspersky 클러스터 서비스를 수동으로 실행합니다.

클러스터의 모든 노드가 네트워크 에이전트가 설치된 기기로 관리 콘솔에 표시됩니다.

설치된 패치에 대한 자세한 내용은 Kaspersky 애플리케이션의 소프트웨어 모듈용 업데이트 버전에 대한 리포트 또는 **소프트웨어 업데이트** 폴더를 참조하십시오.

클라이언트 기기에서 타사 애플리케이션 관리

Kaspersky Security Center를 사용하면 클라이언트 기기에 설치된 Kaspersky 및 다른 공급업체의 애플리케이션을 관리할 수 있습니다.

관리자가 수행할 수 있는 작업은 다음과 같습니다.

- 특정 기준에 따라 애플리케이션 카테고리 만들기.
- 특수하게 생성된 규칙을 사용하여 애플리케이션 카테고리 관리.
- 기기에서 실행되는 애플리케이션 관리.
- 인벤토리 수행 및 기기에 설치된 소프트웨어 레지스트리 유지.
- 기기에 설치된 소프트웨어의 취약점 수정.
- Windows 업데이트 및 기타 소프트웨어 공급업체의 업데이트를 기기에 설치.
- 유료 애플리케이션 그룹의 라이센스 키 사용 모니터링.

타사 애플리케이션 정보

Kaspersky Security Center는 클라이언트 기기에 설치된 타사 소프트웨어를 업데이트하고 타사 소프트웨어의 취약점을 수정하는 데 도움을 줄 수 있습니다. Kaspersky Security Center는 타사 소프트웨어를 현재 버전에서 최신 버전으로만 업데이트할 수 있습니다.

타사 소프트웨어 목록은 변경될 수 있으며 유동적으로 업데이트됩니다. MMC 기반 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에서 사용 가능한 업데이트 목록 확인을 통해 Kaspersky Security Center로 사용자 기기에 설치된 타사 소프트웨어를 업데이트할 수 있는지 확인할 수 있습니다.

아래에 설명된 절차는 Kaspersky Security Center로 업데이트할 수 있는 타사 소프트웨어 목록을 확인하는 용도로만 사용됩니다. 작업을 시작하지 않고 관련 정보에 접근할 수 있는 단계가 이어집니다.

Kaspersky Security Center 웹 콘솔의 Kaspersky Security Center로 업데이트할 수 있는 타사 소프트웨어 목록을 보려면 다음 절차를 따르십시오.

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. 마법사의 **새 작업 설정** 단계에서 다음 설정을 지정합니다.
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Security Center**를 선택합니다.
   b. **작업 유형** 목록에서 **취약점 관련 업데이트를 설치하고 취약점 수정**을 선택합니다.
4. 마법사의 **작업 범위** 단계에서 **관리 중인 기기** 옵션을 선택합니다.
5. 마법사의 **업데이트 설치 규칙을 지정합니다** 단계에서 **추가** 버튼을 클릭합니다.
   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
6. 마법사의 **규칙 유형 선택** 단계에서 **타사 업데이트 규칙**을 선택합니다.
7. 마법사의 **일반 기준** 단계에서 **모든 업데이트 설치(거부된 것 제외)** 옵션을 선택한 후 **다음**을 클릭합니다.

타사 소프트웨어 목록이 표시됩니다.

MMC 기반 콘솔에서 Kaspersky Security Center로 업데이트할 수 있는 타사 소프트웨어 목록을 보려면 취약점 및 패치 관리 라이센스가 필요합니다. 라이센스가 없으면 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업을 이용할 수 없습니다.

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 선택합니다.
2. 작업 공간에서 **작업** 탭을 선택합니다.
3. **작업 생성** 버튼을 눌러 새 작업 마법사를 실행합니다. 마법사의 각 단계를 따릅니다.
4. 마법사의 **작업 유형 선택** 페이지에서 **취약점 관련 업데이트를 설치하고 취약점 수정**을 선택합니다.

5. 마법사의 **업데이트 설치 규칙을 지정합니다** 단계에서 **추가** 버튼을 클릭합니다.
   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

6. 마법사의 **규칙 유형 선택** 단계에서 **타사 업데이트 규칙**을 선택합니다.

7. 마법사의 **일반 기준** 단계에서 **모든 업데이트 설치(거부된 것 제외)** 옵션을 선택한 후 **다음**을 클릭합니다.

   타사 소프트웨어 목록이 표시됩니다.

타사 소프트웨어 업데이트 설치

Kaspersky Security Center를 사용하면 클라이언트 기기에 설치된 소프트웨어의 업데이트를 관리하고 필요한 업데이트를 설치해 Microsoft 애플리케이션과 다른 공급업체 제품의 취약점을 수정할 수 있습니다.

Kaspersky Security Center는 업데이트 검색 작업을 통해 업데이트를 검색하고 이를 업데이트 저장소에 다운로드합니다. 업데이트 검색이 완료되면 애플리케이션이 사용 가능한 업데이트와 해당 업데이트를 사용해 수정할 수 있는 애플리케이션의 취약점 정보를 관리자에게 제공합니다.

이용 가능한 Microsoft Windows 업데이트에 대한 정보는 Windows 업데이트 서비스에 의해 제공됩니다. 중앙 관리 서버를 Windows Server Update Services(WSUS) 서버로 사용할 수 있습니다. 중앙 관리 서버를WSUS 서버처럼 사용하려면 Windows 업데이트로 업데이트 동기화를 구성해야 합니다. Windows 업데이트로 데이터 동기화를 구성하면 중앙 관리 서버가 설정된 빈도에 따라 기기의 Windows 업데이트 서비스에 중앙 집중식 모드로 업데이트를 제공합니다.

네트워크 에이전트 정책을 통해 소프트웨어 업데이트를 관리할 수도 있습니다. 이렇게 하려면 네트워크 에이전트 정책을 만들고 소프트웨어 업데이트 기능을 새 정책 마법사의 해당 창에 구성해야 합니다.

관리자는 **애플리케이션 관리** 폴더 안에 구성되어 있는 **소프트웨어 업데이트** 하위 폴더에서 사용 가능한 업데이트 목록을 볼 수 있습니다. 이 폴더에는 기기에 배포할 수 있는 Microsoft 애플리케이션과 중앙 관리 서버가 검색한 기타 공급업체 제품의 업데이트 목록이 들어 있습니다. 관리자는 사용 가능한 업데이트 정보를 보고 나서 이를 기기에 설치할 수 있습니다.

Kaspersky Security Center는 애플리케이션의 이전 버전을 제거하고 새 버전으로 설치해 일부 애플리케이션을 업데이트합니다.

관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

기본 및 보조 중앙 관리 서버에 대한 **인터페이스 구성** 창에서 **취약점 및 패치 관리 표시** 옵션이 활성화되어 있는지 확인하십시오. 그렇지 않으면 업데이트 검색 작업이 WSUS 업데이트만 처리합니다.

취약점 및 패치 관리 기능을 사용하여 타사 소프트웨어 업데이트 설치 시, 보안상의 이유로 Kaspersky 기술을 사용해 악성 코드를 자동 검사합니다. 이러한 기술은 자동 파일 검사에 사용되며, 샌드박스 환경에서의 바이러스 검사, 정적 분석, 동적 분석, 행동 분석, 머신 러닝 등을 포함합니다.

Kaspersky 전문가는 취약점 및 패치 관리 기능으로 설치할 수 있는 타사 소프트웨어 업데이트에 대한 수동 분석을 수행하지 않습니다. 또한 Kaspersky 전문가는 이러한 업데이트에서 알려지거나 알려지지 않은 취약점이나 문서화되지 않은 기능을 검색하지 않으며, 위 단락에 지정된 유형 외에 다른 유형의 업데이트 분석도 수행하지 않습니다.

모든 기기에 업데이트를 설치하기 전에 테스트 설치를 수행하여 설치된 업데이트로 인해 기기의 애플리케이션 작동에 오류가 발생하지 않는지 확인합니다.

시나리오: 타사 소프트웨어 업데이트

이 섹션에서는 클라이언트 기기에 설치된 타사 소프트웨어의 업데이트 관련 시나리오를 제공합니다. 타사 소프트웨어에는 Microsoft 및 기타 소프트웨어 공급업체의 애플리케이션이 포함됩니다. Microsoft 애플리케이션 업데이트는 Windows Update 서비스에서 제공합니다.

필수 구성 요소

Microsoft 소프트웨어 이외의 타사 소프트웨어 업데이트를 설치하려면 중앙 관리 서버가 인터넷에 연결되어 있어야 합니다.

기본적으로 중앙 관리 서버에서 Microsoft 소프트웨어 업데이트를 관리 중인 기기에 설치하는 경우 인터넷 연결이 필요하지 않습니다. 예를 들어 관리 중인 기기는 Microsoft Update 서버 또는 회사의 네트워크에 배포된 Microsoft WSUS(Windows Server Update Services)가 있는 Windows Server에서 직접 Microsoft 소프트웨어 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버를 WSUS 서버로 사용하려면 중앙 관리 서버가 인터넷에 연결되어 있어야 합니다.

단계

타사 소프트웨어 업데이트는 다음과 같이 단계적으로 진행됩니다.

1. **필요한 업데이트 검색**

   관리 중인 기기에 필요한 타사 소프트웨어 업데이트를 찾으려면 *취약점 및 필요한 업데이트 검색* 작업을 실행합니다. 이 작업이 완료되면 Kaspersky Security Center는 작업 속성에서 지정한 기기에 설치된 타사 소프트웨어에 대하여 탐지된 취약점 및 필요한 업데이트의 목록을 받습니다.

   취약점 및 필요한 업데이트 검색 작업은 중앙 관리 서버 빠른 시작 마법사가 자동 생성합니다. 마법사를 실행하지 않았다면 지금 작업을 생성하거나 빠른 시작 마법사를 실행합니다.

   방법 지침:

   - 관리 콘솔: 애플리케이션 취약점 검사, 취약점 및 필요한 업데이트 검색 작업 스케줄 지정
   - Kaspersky Security Center 웹 콘솔: 취약점 및 필요한 업데이트 검색 작업 만들기, 취약점 및 필요한 업데이트 검색 작업 설정

2. **발견된 업데이트 목록 분석**

   소프트웨어 업데이트 목록을 확인하고 설치할 업데이트를 결정합니다. 각 업데이트에 대한 상세 정보를 확인하려면 목록에서 업데이트 이름을 누릅니다. 목록에 있는 각 업데이트에 대해 클라이언트 기기에서 업데이트 설치 관련 통계를 확인할 수도 있습니다.

   방법 지침:

   - 관리 콘솔: 사용 가능한 업데이트 관련 정보 보기
   - Kaspersky Security Center 웹 콘솔: 사용 가능한 타사 소프트웨어 업데이트 관련 정보 보기

3. **업데이트 설치 구성**

Kaspersky Security Center에서 타사 소프트웨어 업데이트 목록을 받으면 *필수 업데이트 설치 및 취약점 수정* 작업 또는 *Windows Update 업데이트 설치* 작업을 사용하여 클라이언트 기기에 업데이트를 설치할 수 있습니다. 이러한 작업 중 하나를 만듭니다. **작업** 탭 또는 **소프트웨어 업데이트** 목록을 사용하여 이러한 작업을 만들 수 있습니다.

필수 업데이트 설치 및 취약점 수정 작업은 Windows Update 서비스에서 제공하는 업데이트, 기타 공급업체 소프트웨어의 업데이트 등 Microsoft 애플리케이션 업데이트 설치에 사용됩니다. 이 작업은 취약점 및 패치 관리 기능에 대한 라이센스가 있을 때만 만들 수 있습니다.

Windows Update 업데이트 설치 작업에는 라이센스가 필요하지 않지만 Windows Update 업데이트를 설치하는 데만 사용할 수 있습니다.

소프트웨어 설치에 관한 EULA(최종 사용자 라이센스 계약서)에 동의해야 설치할 수 있는 소프트웨어 업데이트도 있습니다. EULA에 동의하지 않으면 소프트웨어 업데이트가 설치되지 않습니다.

스케줄에 따라 업데이트 설치 작업을 시작할 수 있습니다. 작업 스케줄을 지정할 때 업데이트 설치 작업은 *취약점 및 필요한 업데이트 검색* 작업이 완료된 후에 시작해야 합니다.

방법 지침:

- 관리 콘솔: 애플리케이션의 취약점 수정, 사용 가능한 업데이트 관련 정보 보기
- Kaspersky Security Center 웹 콘솔: 필수 업데이트 설치 및 취약점 수정 작업 생성, Windows Update 업데이트 설치 작업 생성, 사용 가능한 타사 소프트웨어 업데이트 관련 정보 보기

4 작업 스케줄 지정

업데이트 목록을 항상 최신 상태로 유지하기 위해 *취약점 및 필요한 업데이트 검색* 작업 스케줄을 지정하여 가끔 자동으로 실행합니다. 기본적으로 *취약점 및 필요한 업데이트 검색* 작업은 수동 시작으로 설정되어 있습니다.

사용자가 *필수 업데이트 설치 및 취약점 수정* 작업을 만든 경우 *취약점 및 필요한 업데이트 검색* 작업과 빈도가 같거나 적게 실행하도록 스케줄을 지정할 수 있습니다. *Windows Update 업데이트 설치* 작업의 스케줄을 지정할 때 이러한 작업의 경우 작업을 시작하기 전에 매번 업데이트 목록을 정해야 합니다.

작업 스케줄을 지정할 때는 *취약점 및 필요한 업데이트 검색* 작업이 완료된 후에 업데이트 설치 작업을 시작해야 합니다.

5 소프트웨어 업데이트 승인 및 거부(선택 사항)

필수 업데이트 설치 및 취약점 수정 작업을 만들었다면 작업 속성에서 업데이트 설치 관련 규칙을 지정할 수 있습니다. Windows Update 업데이트 설치 작업을 만들었다면 이 단계는 건너뛰십시오.

업데이트 상태가 *정의 안 됨*, *승인됨* 또는 *거부됨*인지에 따라 각 규칙에 대해 설치할 업데이트를 정의할 수 있습니다. 예를 들어, Windows Update 업데이트 설치만을 *승인됨* 상태인 사용자에게만 허용하려면 서버에 대한 특정 작업을 만들고 이 작업의 규칙을 설정하는 것이 좋습니다. 그런 다음 설치하고자 하는 업데이트에 대해 *승인됨* 상태를 수동으로 설정합니다. 이 경우 *정의 안 됨* 또는 *거부됨* 상태인 Windows Update 업데이트는 작업에서 지정한 서버에 설치되지 않습니다.

승인됨 상태를 사용하여 업데이트 설치를 관리하면 소량 업데이트에 효율적입니다. 여러 업데이트를 설치하려면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 구성할 수 있는 규칙을 사용하십시오. 규칙에 명시된 기준을 충족하지 않는 업데이트에 대해서만 *승인됨* 상태를 설정하는 것이 좋습니다. 대량의 업데이트를 수동으로 승인하면 중앙 관리 서버의 성능이 저하되어 결국 서버 과부하로 이어질 수 있습니다.

기본적으로 다운로드한 소프트웨어 업데이트는 *정의 안 됨* 상태입니다. **소프트웨어 업데이트** 목록(**동작 → 패치 관리 → 소프트웨어 업데이트**)에서 상태를 *승인됨* 또는 *거부됨*으로 변경할 수 있습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 업데이트 승인 및 거부
- Kaspersky Security Center 웹 콘솔: 타사 소프트웨어 업데이트 승인 및 거부

6 WSUS(Windows Server Update Services) 서버로 작동하도록 중앙 관리 서버 구성(선택 사항)

기본적으로 Windows Update 업데이트는 Microsoft 서버에서 관리 중인 기기로 다운로드됩니다. 중앙 관리 서버를 WSUS 서버로 사용하도록 이 설정을 변경할 수 있습니다. 이 경우, 중앙 관리 서버는 지정된 빈도로 Windows 업데이트와 업데이트 데이터를 동기화하고 중앙 집중식 모드로 클라이언트 기기에 Windows Update에 대한 업데이트를 제공합니다.

중앙 관리 서버를 WSUS 서버로 사용하려면 Windows 업데이트 동기화 수행 작업을 만들고 네트워크 에이전트 정책에서 **중앙 관리 서버를 WSUS 서버로 사용** 확인란을 선택합니다.

방법 지침:

- 관리 콘솔: 중앙 관리 서버와 Windows Update의 업데이트 동기화, 네트워크 에이전트 정책에서 Windows 업데이트 구성
- Kaspersky Security Center 웹 콘솔: Windows Update 동기화 수행 작업 생성

7. **업데이트 설치 작업 실행**

   필수 업데이트 설치 및 취약점 수정 작업 또는 *Windows Update 업데이트 설치* 작업을 시작합니다. 이러한 작업을 시작하면 관리 중인 기기에 업데이트가 다운로드되고 설치됩니다. 작업이 완료되면 작업 목록에서 상태가 *성공적으로 완료*인지 확인하십시오.

8. **타사 소프트웨어의 업데이트 설치 결과 관련 보고서 생성(선택 사항)**

   업데이트 설치에 관한 자세한 통계를 보려면 **타사 소프트웨어 업데이트 설치 결과 리포트**를 만듭니다.

   방법 지침:

   - 관리 콘솔: 리포트 만들기 및 보기
   - Kaspersky Security Center 웹 콘솔: 리포트 생성 및 보기

결과

필수 업데이트 설치 및 취약점 수정 작업을 만들고 구성했다면 업데이트가 관리 중인 기기에 자동으로 설치됩니다. 새 업데이트가 중앙 관리 서버 저장소에 다운로드되면 Kaspersky Security Center에서는 업데이트 규칙에 지정된 기준을 충족하는지 검사합니다. 기준을 충족하는 모든 새 업데이트는 다음 작업 실행 시 자동으로 설치됩니다.

Windows Update 업데이트 작업을 만들었다면 *Windows Update 업데이트* 작업 속성에 지정된 업데이트만 설치됩니다. 나중에 중앙 관리 서버 저장소에 다운로드된 새 업데이트를 설치하려면 기존 작업의 업데이트 목록에 필수 업데이트를 추가하거나 *Windows Update 업데이트* 작업을 새로 만들어야 합니다.

타사 애플리케이션에 사용 가능한 업데이트에 대한 정보 보기

클라이언트 기기에 설치된 타사 애플리케이션에 이용 가능한 업데이트 목록을 보려면 다음 단계를 따릅니다.

콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **소프트웨어 업데이트** 하위 폴더를 선택합니다.

폴더의 작업 영역에서 기기에 설치된 애플리케이션에 사용 가능한 업데이트 목록을 볼 수 있습니다.

업데이트의 속성을 보려면 다음과 같이 하십시오,

소프트웨어 업데이트 폴더의 작업 영역에서 해당 업데이트의 마우스 오른쪽 메뉴에 있는 **속성**를 선택합니다.

업데이트의 속성 창에서 볼 수 있는 정보는 다음과 같습니다:

- **일반** 섹션에서 다음과 같은 **승인 상태 업데이트**을 확인할 수 있습니다:
  - **정의 안 됨** - 업데이트 목록에서 업데이트를 사용할 수 있지만 설치가 승인되지 않았습니다.
  - **승인됨** - 업데이트 목록에서 업데이트를 사용할 수 있으며 설치가 승인되었습니다.
  - **거부됨** - 설치를 위해 업데이트가 거부되었습니다.
- **특성** 섹션에서 다음과 같은 **자동으로 설치됨** 필드의 값을 확인할 수 있습니다:
  - *필수 업데이트 설치 및 취약성 수정* 작업이 애플리케이션에 대한 업데이트를 설치할 수 있는 경우 **자동** 값이 표시됩니다. 이 작업을 통해 타사 소프트웨어 공급업체가 제공한 웹 주소에서 새 업데이트가 자동으로 설치됩니다.
  - Kaspersky Security Center에서 애플리케이션에 대한 업데이트를 자동으로 설치할 수 없는 경우 **수동 시작** 값이 표시됩니다. 업데이트를 수동으로 설치할 수 있습니다.

  Windows 애플리케이션 업데이트에 대한 **자동으로 설치됨** 필드는 표시되지 않습니다.
- 업데이트할 클라이언트 기기의 목록.
- 업데이트하기 전에 설치해야 할 시스템 구성 요소(필수 구성 요소)의 목록 (있을 경우)
- 업데이트로 수정되는 소프트웨어 취약점.

소프트웨어 업데이트 승인 및 거부

업데이트 설치 작업의 설정에서 설치할 업데이트에 대한 승인이 필요할 수 있습니다. 설치해야 하는 업데이트는 승인하고 설치하면 안 되는 업데이트는 거부할 수 있습니다.

예를 들어 업데이트가 기기 작동을 방해하지 않는지 테스트 환경에서 업데이트 설치를 먼저 확인한 후에만 클라이언트 기기에서 해당 업데이트 설치를 허용할 수 있습니다.

승인됨 상태를 사용하여 타사 업데이트 설치를 관리하면 소량 업데이트에 효율적입니다. 여러 타사 업데이트를 설치하려면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 구성할 수 있는 규칙을 사용하십시오. 규칙에 명시된 기준을 충족하지 않는 업데이트에 대해서만 *승인됨* 상태를 설정하는 것이 좋습니다. 대량의 업데이트를 수동으로 승인하면 중앙 관리 서버의 성능이 저하되어 결국 서버 과부하로 이어질 수 있습니다.

업데이트 하나 또는 여러 개를 승인하거나 거부하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **고급 → 애플리케이션 관리 → 소프트웨어 업데이트** 노드를 선택합니다.
2. **소프트웨어 업데이트** 폴더의 작업 영역에서 오른쪽 위에 있는 **새로 고침** 버튼을 누릅니다. 업데이트 목록이 나타납니다.
3. 승인하거나 거부할 업데이트를 선택합니다.

   선택한 개체의 정보 상자가 작업 영역 오른쪽에 표시됩니다.

4. **승인 상태 업데이트** 드롭다운 목록에서 **승인됨**를 선택하여 선택한 업데이트를 승인하거나 **거부됨**를 선택하여 선택한 업데이트를 거부합니다.

   기본값은 **정의 안 됨**입니다.

승인됨 상태를 설정한 업데이트는 설치 대기열에 배치됩니다.

거부됨 상태로 설정한 업데이트는 이전에 설치했던 모든 기기에서 제거됩니다(제거 가능할 시). 또한 앞으로 다른 기기에도 설치되지 않습니다.

Kaspersky 애플리케이션용 일부 업데이트는 제거할 수 없습니다. 이러한 업데이트에 대해 **거부됨** 상태를 설정하면, Kaspersky Security Center는 해당 업데이트를 이전에 설치했던 기기에서 업데이트를 제거하지 않습니다. 하지만 이러한 업데이트는 앞으로 다른 기기에 설치되지 않습니다. Kaspersky 애플리케이션용 업데이트를 제거할 수 없는 경우에는 이 속성이 업데이트 속성 창에 표시됩니다. **섹션** 창에서 **일반**을 선택하면 작업 영역의 **설치 요구 사항** 아래에 이 속성이 표시됩니다. 타사 소프트웨어 업데이트에 대해 **거부됨** 상태를 설정하면, 해당 업데이트 설치를 계획했으나 아직 설치하지는 않은 기기에 업데이트를 설치하지 않습니다. 그러나 업데이트를 이미 설치한 기기에서는 업데이트가 그대로 유지됩니다. 이러한 업데이트를 삭제해야 하는 경우 로컬에서 수동으로 삭제할 수 있습니다.

중앙 관리 서버로 Windows 업데이트의 업데이트 동기화

빠른 시작 마법사의 **업데이트 관리 설정** 창에서 **WSUS 서버로 이 중앙 관리 서버 사용**를 선택한 경우 Windows 업데이트 동기화 작업이 자동으로 생성됩니다. **작업** 폴더에서 작업을 실행할 수 있습니다. Microsoft 소프트웨어 업데이트 기능은 **Windows 업데이트 동기화 수행** 작업을 완료한 후에만 사용할 수 있습니다.

Microsoft 소프트웨어 업데이트는 10GB를 초과할 수 있습니다. 중앙 관리 서버 데이터베이스가 이러한 볼륨을 수용할 수 있는지 확인하십시오. 그렇지 않으면 **Windows 업데이트 동기화 수행** 작업이 실패합니다. **Windows 업데이트 동기화 수행** 작업에는 Microsoft SQL Express 데이터베이스를 지원하지 않습니다.

Windows 업데이트 동기화 수행 작업은 Microsoft 서버에서 메타데이터만 다운로드합니다. 네트워크에 WSUS 서버가 없으면 각 클라이언트 기기는 외부 서버에서 Microsoft 업데이트를 독립적으로 다운로드합니다.

중앙 관리 서버로 Windows 업데이트를 동기화하는 작업을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **소프트웨어 업데이트** 하위 폴더를 선택합니다.
2. **추가 조치** 버튼을 누르고 드롭다운 목록에서 **Windows 업데이트 동기화 구성**을 선택합니다.

   이 마법사는 **Windows 업데이트 동기화 수행** 작업을 만들어 **작업** 폴더에 표시합니다.

   이는 Windows 업데이트 센터 데이터 검색 작업 생성 마법사를 시작합니다. 마법사의 지침을 따릅니다.

또한 **작업 생성**를 눌러 **작업** 폴더에 Windows 업데이트 동기화 작업을 만들 수 있습니다.

Microsoft는 정기적으로 회사 서버에서 오래된 업데이트를 삭제하므로, 현재 제공하는 업데이트 수가 항상 20만에서 30만 사이입니다. 디스크 공간 사용량과 데이터베이스 크기를 줄이기 위해 Kaspersky Security Center는 Microsoft 업데이트 서버에 더는 존재하지 않는 오래된 업데이트를 삭제합니다.

Windows 업데이트 동기화 수행 작업을 실행하면 애플리케이션은 Microsoft 업데이트 서버에서 현재 업데이트 목록을 수신합니다. 그런 다음 Kaspersky Security Center는 오래된 업데이트 목록을 취합합니다. 다음 번 **취약점 및 필요한 업데이트 검색** 작업 시작 시 Kaspersky Security Center는 오래된 모든 업데이트에 플래그를 지정하고 해당 업데이트의 삭제 시간을 설정합니다. 다음 번 **Windows 업데이트 동기화 수행** 작업 시작 시 30일 전에 삭제 플래그가 지정된 모든 업데이트가 삭제됩니다. 또한 Kaspersky Security Center는 180일 전에 삭제 플래그가 지정된 오래된 업데이트를 확인한 다음 해당 이전 업데이트를 삭제합니다.

Windows 업데이트 동기화 수행 작업이 완료되고 오래된 업데이트가 삭제될 때 데이터베이스에 삭제된 업데이트 파일과 관련된 해시 코드와 함께 %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 파일(이전에 다운로드된 경우)과 연관된 파일이 남아 있을 수 있습니다. **중앙 관리 서버 점검** 작업을 실행하여 데이터베이스 및 해당 파일에서 오래된 레코드를 삭제할 수 있습니다.

1단계. 트래픽 감소 여부 정의

Kaspersky Security Center가 Microsoft Windows 업데이트 서버와 업데이트를 동기화할 때는 모든 파일에 대한 정보가 중앙 관리 서버 데이터베이스에 저장됩니다. 또한 Windows 업데이트 에이전트와 상호 작용하는 동안 업데이트에 필요한 모든 파일이 드라이브에도 다운로드됩니다. 특히 Kaspersky Security Center는 빠른 업데이트 파일에 대한 정보를 데이터베이스에 다운로드하여 필요할 때 다운로드합니다. 빠른 업데이트 파일을 다운로드하는 경우 드라이브의 사용 가능한 공간이 줄어듭니다.

디스크 공간 볼륨 감소를 방지하고 트래픽을 줄이려면 **Download express installation files** 옵션을 비활성화합니다.

이 옵션을 선택하면 작업 실행 시 빠른 업데이트 파일을 다운로드합니다. 기본적으로 이 옵션은 선택되어 있지 않습니다.

2단계. 애플리케이션

이 섹션에서는 업데이트를 다운로드할 애플리케이션을 선택할 수 있습니다.

모든 애플리케이션 확인란을 선택하면 모든 기존 애플리케이션 및 향후 출시될 수 있는 모든 애플리케이션에 대해 업데이트를 다운로드합니다.

기본적으로 **모든 애플리케이션** 확인란은 선택되어 있습니다.

3단계. 업데이트 카테고리

이 섹션에서는 중앙 관리 서버에 다운로드되는 업데이트 카테고리를 선택할 수 있습니다.

모든 카테고리 확인란을 선택하면 모든 기존 업데이트 카테고리 및 향후 표시될 수 있는 모든 카테고리에 대해 업데이트를 다운로드합니다.

기본적으로 **모든 카테고리** 확인란은 선택되어 있습니다.

4단계. 업데이트 언어

이 창에서는 중앙 관리 서버에 다운로드되는 업데이트의 현지화 언어를 선택할 수 있습니다. 업데이트의 현지화 언어 다운로드를 위한 다음 옵션 중 하나를 선택합니다:

- **새로운 언어를 포함해 모든 언어 다운로드**

  이 옵션을 선택하면 업데이트의 사용 가능한 모든 현지화 언어가 중앙 관리 서버에 다운로드됩니다. 기본적으로 이 옵션은 선택되어 있습니다.

- **선택한 언어만 다운로드**

  이 옵션을 선택하면 중앙 관리 서버에 다운로드할 언어를 업데이트의 현지화 언어 목록에서 선택할 수 있습니다.

5단계. 작업을 시작할 계정 선택

작업을 실행할 계정 선택 창에서 작업 실행 시 사용할 계정을 지정할 수 있습니다. 다음 옵션 중 하나를 선택합니다:

- **기본 계정**

  해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.
  기본적으로 이 옵션은 선택되어 있습니다.

- **계정 지정**

  계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

  - **계정**

    작업 실행에 사용되는 계정입니다.

  - **암호**

    작업을 실행할 계정의 암호입니다.

6단계. 작업 시작 스케줄 구성

작업 스케줄 구성 마법사 페이지에서는 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

- **시작 스케줄:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

    작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

  - **N일마다**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

    기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **N주마다**

    작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

    기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

  - **N분마다**

    작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

    기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

  - **매일(서머타임 지원 안 함)**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

    이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

    기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

  - **주별**

    이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **한번만**

  작업은 지정한 날짜와 시간(기본값은 작업 생성일)에 한 번 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:
  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.
  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

7단계. 작업 이름 정의

작업 이름 정의 창에서 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않아야 하며 특수 문자 (`"*<>?\:|`)를 사용할 수 없습니다. 기본값은 *Windows 업데이트 동기화 수행*입니다.

8단계. 작업 생성 완료

작업 생성 마침 창에서 **마침** 버튼을 눌러 마법사를 완료합니다.

마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

새로 만든 Windows 업데이트 동기화 작업이 콘솔 트리 **작업** 폴더의 작업 목록에 표시됩니다.

기기에 수동으로 업데이트 설치

빠른 시작 마법사의 **업데이트 관리 설정** 페이지에서 **타사 제품 업데이트 검색 및 설치** 및 설치를 선택하면 *필수 업데이트 설치 및 취약점 수정* 작업이 자동 생성됩니다. **작업** 탭의 **관리 중인 기기** 폴더에서 작업을 실행 또는 중지할 수 있습니다.

빠른 시작 마법사에서 **필요한 업데이트 검색**를 선택하면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 통해 클라이언트 기기에 소프트웨어 업데이트를 설치할 수 있습니다.

다음 중 원하는 작업을 수행할 수 있습니다:

- 업데이트 설치를 위한 작업을 만듭니다.
- 기존 업데이트 설치 작업에 업데이트 설치를 위한 규칙을 추가합니다.
- 기존 업데이트 설치 작업의 설정에서 업데이트 테스트 설치를 구성합니다.

> 관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

설치 작업을 만들어 업데이트 설치

다음 중 원하는 작업을 수행할 수 있습니다:

- 특정 업데이트 설치를 위한 작업을 만듭니다.
- 업데이트를 선택하고 해당 업데이트와 유사한 업데이트 설치를 위한 작업을 만듭니다.

특정 업데이트를 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **소프트웨어 업데이트** 하위 폴더를 선택합니다.
2. 작업 영역에서 설치할 업데이트를 선택합니다.

3. 다음을 수행합니다:

   - 목록에서 선택한 업데이트 중 하나를 마우스 오른쪽 버튼으로 누르고 **업데이트 설치 → 새 작업**를 선택합니다.
   - 선택한 업데이트의 정보 박스에서 **업데이트 설치(작업 생성)** 링크를 누릅니다.

4. 모든 이전 애플리케이션 업데이트 설치와 관련하여 표시되는 메시지에서 원하는 옵션을 선택합니다. 선택한 업데이트를 설치하는 데 필요한 경우 후속 애플리케이션 버전의 증분 방식 설치에 동의한다면 **예**를 누릅니다. 후속 버전을 설치하지 않고 애플리케이션을 단순하게 업데이트하려면 **아니오**를 누릅니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

   업데이트 설치 및 취약점 수정 작업 만들기 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

5. 마법사의 **운영 체제 재시작 옵션 선택** 페이지에서 작업 후 클라이언트 기기의 운영 체제를 재시작해야 할 때 수행할 작업을 선택합니다:

   - **기기 다시 시작 안 함**

     작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

   - **기기 다시 시작**

     이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

   - **사용자 확인 후 처리**

     클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

     기본적으로 이 옵션은 선택되어 있습니다.

     - **반복해서 물어보기(분)**

       이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

       기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

       이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

     - **다음 시간 이후에 재시작(분)**

       사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

       기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

6. 마법사의 **작업 스케줄 구성** 페이지에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

   - **시작 스케줄:**

     작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

     - **N시간마다**

       작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

       작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

     - **N일마다**

       작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

       기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

     - **N주마다**

       작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

       기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

     - **N분마다**

       작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

       기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

     - **매일(서머타임 지원 안 함)**

       작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

       이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

- **주별**

  이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

7. 마법사의 **작업 이름 정의** 페이지에서 만들 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

8. 마법사의 **작업 생성 마침** 페이지에서 **완료** 버튼을 눌러 마법사를 닫습니다.
   마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

마법사의 작업이 완료되면 **취약점 관련 업데이트를 설치하고 취약점 수정**이 **작업** 폴더에 표시됩니다.

업데이트를 설치하기 전에 *필수 업데이트 설치 및 취약점 수정* 작업 속성에서 시스템 구성 요소(필수 구성 요소)의 자동 설치를 활성화할 수 있습니다. 이 옵션이 설정되면 업데이트를 설치하기 전에 모든 필수 시스템 구성 요소가 설치됩니다. 필수 구성 요소의 목록은 업데이트 속성에서 확인할 수 있습니다.

필수 업데이트 설치 및 취약점 수정 작업의 속성에서 새 버전으로 애플리케이션을 업그레이드하는 업데이트 설치를 허용할 수 있습니다.

작업 설정에서 타사 업데이트 설치를 위한 규칙을 제공하는 경우 중앙 관리 서버는 공급 업체 웹사이트에서 모든 관련 업데이트를 다운로드합니다. 업데이트는 중앙 관리 서버 저장소에 저장된 후 해당하는 기기에 배포되어 설치됩니다.

작업 설정에서 Microsoft 업데이트 설치용 규칙을 제공하며 중앙 관리 서버가 WSUS 서버 역할을 하는 경우 중앙 관리 서버는 모든 관련 업데이트를 저장소에 다운로드한 다음 관리 중인 기기로 배포합니다. 네트워크에 WSUS 서버가 없으면 각 클라이언트 기기는 외부 서버에서 Microsoft 업데이트를 독립적으로 다운로드합니다.

특정 업데이트 및 유사한 업데이트를 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **소프트웨어 업데이트** 하위 폴더를 선택합니다.

2. 작업 영역에서 설치할 업데이트를 선택합니다.

3. **업데이트 설치 마법사 실행** 버튼을 누릅니다.
   업데이트 설치 마법사가 시작됩니다.

   > 업데이트 설치 마법사 기능은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

   마법사의 각 단계를 따릅니다.

4. **기존 업데이트 설치 작업 검색** 페이지에서 다음 설정을 지정합니다:

   - **이 업데이트를 설치하는 작업 검색**

     이 옵션이 활성화되어 있으면 업데이트 설치 마법사에서 선택한 업데이트를 설치하는 기존 작업을 검색합니다.

     이 옵션이 비활성화되어 있거나 검색에서 해당하는 작업이 검색되지 않으면 업데이트 설치 마법사에서 업데이트 설치를 위한 작업이나 규칙을 만들라는 메시지를 표시합니다.

     기본적으로 이 옵션은 켜져 있습니다.

   - **업데이트 설치 승인**

     선택한 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

5. 기존 업데이트 설치 작업을 검색하도록 선택하여 검색에서 일부 작업이 검색되는 경우 해당 작업의 속성을 확인하거나 작업을 수동으로 시작할 수 있습니다. 추가 조치는 필요하지 않습니다.

   그렇지 않으면 **새 업데이트 설치 작업** 버튼을 누릅니다.

6. 새 작업에 추가할 설치 규칙의 유형을 선택하고 **마침** 버튼을 누릅니다.

7. 모든 이전 애플리케이션 업데이트 설치와 관련하여 표시되는 메시지에서 원하는 옵션을 선택합니다. 선택한 업데이트를 설치하는 데 필요한 경우 후속 애플리케이션 버전의 증분 방식 설치에 동의한다면 **예**를 누릅니다. 후속 버전을 설치하지 않고 애플리케이션을 단순하게 업데이트하려면 **아니오**를 누릅니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

   업데이트 설치 및 취약점 수정 작업 만들기 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

8. 마법사의 **운영 체제 재시작 옵션 선택** 페이지에서 작업 후 클라이언트 기기의 운영 체제를 재시작해야 할 때 수행할 작업을 선택합니다:

   - **기기 다시 시작 안 함**

     작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

   - **기기 다시 시작**

     이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

   - **사용자 확인 후 처리**

     클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

     기본적으로 이 옵션은 선택되어 있습니다.

     - **반복해서 물어보기(분)**

       이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

       기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

       이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

     - **다음 시간 이후에 재시작(분)**

       사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

9. 마법사의 **이 작업이 할당되는 기기 선택** 페이지에서 다음 옵션 중 하나를 선택합니다.

- **중앙 관리 서버가 발견한 기기 중에서 선택**

  특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.

  예를 들어 미할당 기기에 네트워크 에이전트를 설치하는 작업에서 이 옵션을 사용할 수 있습니다.

- **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

  작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

  특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

- **기기 선택 결과에 작업 할당**

  기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

  예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

- **관리 그룹에 작업 할당**

  관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

  예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

  관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

10. 마법사의 **작업 스케줄 구성** 페이지에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

- **시작 스케줄:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

    작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

  - **N일마다**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

    기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **N주마다**

    작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

    기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

  - **N분마다**

    작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

    기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

  - **매일(서머타임 지원 안 함)**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

    이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

    기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

  - **주별**

    이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

  - **요일별**

    이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

    기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**(기본적으로 선택)

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.
  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

- 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
- 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
  기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
- 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

11. 마법사의 **작업 이름 정의** 페이지에서 만들 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

12. 마법사의 **작업 생성 마침** 페이지에서 **완료** 버튼을 눌러 마법사를 닫습니다.

    마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

마법사가 완료되면 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업이 생성되어 **작업** 폴더에 표시됩니다.

작업 생성 중에 지정하는 설정뿐 아니라 생성된 작업의 기타 속성도 변경할 수 있습니다.

새 버전의 애플리케이션으로 업그레이드할 경우 기기에서 종속 애플리케이션의 오작동이 발생할 수 있습니다.

기존 설치 작업에 규칙을 추가하여 업데이트 설치

기존 설치 작업에 규칙을 추가하여 업데이트를 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급 → 애플리케이션 관리** 폴더에서 **소프트웨어 업데이트** 하위 폴더를 선택합니다.
2. 작업 영역에서 설치할 업데이트를 선택합니다.
3. **업데이트 설치 마법사 실행** 버튼을 누릅니다.
   업데이트 설치 마법사가 시작됩니다.

   업데이트 설치 마법사 기능은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

   마법사의 각 단계를 따릅니다.
4. **기존 업데이트 설치 작업 검색** 페이지에서 다음 설정을 지정합니다:

   - **이 업데이트를 설치하는 작업 검색**

     이 옵션이 활성화되어 있으면 업데이트 설치 마법사에서 선택한 업데이트를 설치하는 기존 작업을 검색합니다.

     이 옵션이 비활성화되어 있거나 검색에서 해당하는 작업이 검색되지 않으면 업데이트 설치 마법사에서 업데이트 설치를 위한 작업이나 규칙을 만들라는 메시지를 표시합니다.

     기본적으로 이 옵션은 켜져 있습니다.

   - **업데이트 설치 승인**

     선택한 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

5. 기존 업데이트 설치 작업을 검색하도록 선택하여 검색에서 일부 작업이 검색되는 경우 해당 작업의 속성을 확인하거나 작업을 수동으로 시작할 수 있습니다. 추가 조치는 필요하지 않습니다.
   그렇지 않은 경우에는 **업데이트 설치 규칙 추가** 버튼을 누릅니다.
6. 규칙을 추가할 작업을 선택하고 **규칙 추가** 버튼을 누릅니다.
   기존 작업의 속성을 확인하거나, 작업을 수동으로 시작하거나, 새 작업을 만들 수도 있습니다.

7. 선택한 작업에 추가할 규칙의 유형을 선택하고 **마침** 버튼을 누릅니다.

8. 모든 이전 애플리케이션 업데이트 설치와 관련하여 표시되는 메시지에서 원하는 옵션을 선택합니다. 선택한 업데이트를 설치하는 데 필요한 경우 후속 애플리케이션 버전의 증분 방식 설치에 동의한다면 **예**를 누릅니다. 후속 버전을 설치하지 않고 애플리케이션을 단순하게 업데이트하려면 **아니오**를 누릅니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

업데이트 설치를 위한 새 규칙이 기존 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업에 추가됩니다.

업데이트에 대한 테스트 설치 구성

업데이트의 테스트 설치를 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 탭의 **관리 중인 기기** 폴더에 있는 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업을 선택합니다.

2. 작업의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.

   취약점 관련 업데이트를 설치하고 취약점 수정 작업의 속성 창이 열립니다.

3. 작업의 속성 창의 **테스트 설치** 섹션에서 테스트 설치에 사용할 수 있는 옵션 중 하나를 선택합니다:

   - **검사 안 함**. 업데이트의 테스트 설치를 수행하려면 이 옵션을 선택합니다.

   - **선택한 기기에서 검사 실행**. 선택한 기기에 테스트 업데이트를 설치하려면 이 옵션을 선택합니다. **추가** 버튼을 누르고 업데이트의 테스트 설치를 수행하려는 기기를 선택합니다.

   - **선택한 그룹의 모든 기기에서 검사 실행**. 기기 그룹에 테스트 업데이트를 설치하려면 이 옵션을 선택합니다. **테스트 그룹 지정** 필드에서 테스트 설치를 수행하려는 기기 그룹을 지정합니다.

   - **지정한 비율만큼 기기에서 검사 실행**. 대상 기기의 일부에 테스트 업데이트를 설치하려면 이 옵션을 선택합니다. **모든 대상 기기 대비 검증 테스트 기기 비율** 필드에 업데이트의 테스트 설치를 수행하려는 기기의 비율을 지정합니다.

4. **설치 지속 여부를 결정하는 데 걸리는 시간(시)** 필드에서 **검사 안 함** 외의 나머지 옵션을 선택한 다음 업데이트의 테스트 설치부터 모든 대상 기기에 업데이트 설치를 시작하기 전까지 경과되는 시간을 지정합니다.

네트워크 에이전트 정책에 Windows 업데이트 구성

네트워크 에이전트 정책에 Windows 업데이트를 구성하려면 다음을 수행하십시오:

1. 콘솔 트리에서 **관리 중인 기기**를 선택합니다.

2. 작업 영역에서 **정책** 탭을 선택합니다.

3. 네트워크 에이전트 정책을 선택합니다.

4. 정책의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.

   네트워크 에이전트 정책의 속성 창이 열립니다.

5. **섹션** 창에서 **소프트웨어 업데이트 및 취약점**를 선택합니다.

6. **WSUS 서버로 이 중앙 관리 서버 사용** 옵션을 선택해 Windows 업데이트를 다운하고 네트워크 에이전트를 통해 기기에 배포합니다.

   이 옵션이 선택 해제되어 있다면, Windows 업데이트는 중앙 관리 서버에 연결되지 않습니다. 이 경우 클라이언트 기기는 Microsoft 서버에서 직접 Windows 업데이트를 다운로드합니다.

7. 사용자가 Windows 업데이트를 사용하여 기기에 수동으로 설치할 수 있는 업데이트 세트를 선택합니다.

   Windows 10을 실행하는 기기에서 Windows 업데이트가 이미 해당 기기에 대한 업데이트를 찾은 경우 **사용자가 Windows 업데이트 설치를 관리하도록 허용** 아래에서 선택한 새 옵션은 앞서 검색된 업데이트가 설치된 후에만 적용됩니다.

   드롭다운 목록에서 항목을 선택합니다:

   - **사용자가 모든 적용 가능한 Windows 업데이트 패치를 설치할 수 있도록 허용**

     사용자가 기기에 적용 가능한 모든 Microsoft Windows 업데이트를 설치할 수 있습니다.

     업데이트 설치를 방해하고 싶지 않다면 옵션을 선택합니다.

     사용자가 Microsoft Windows 업데이트를 수동으로 설치할 때는 중앙 관리 서버가 아닌 Microsoft 서버에서 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버에서 이러한 업데이트를 아직 다운로드하지 않은 경우 Microsoft 서버에서 다운로드할 수 있습니다. Microsoft 서버에서 업데이트를 다운로드하면 트래픽이 추가로 발생합니다.

   - **사용자가 승인된 Windows 업데이트 패치만 설치할 수 있도록 허용**

     사용자가 기기에 적용 가능하며 관리자가 승인한 모든 Microsoft Windows 업데이트를 설치할 수 있습니다.

     예를 들어 업데이트가 기기 작동을 방해하지 않는지 테스트 환경에서 업데이트 설치를 먼저 확인한 후에만 클라이언트 기기에서 승인된 업데이트 설치를 허용할 수 있습니다.

     사용자가 Microsoft Windows 업데이트를 수동으로 설치할 때는 중앙 관리 서버가 아닌 Microsoft 서버에서 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버에서 이러한 업데이트를 아직 다운로드하지 않은 경우 Microsoft 서버에서 다운로드할 수 있습니다. Microsoft 서버에서 업데이트를 다운로드하면 트래픽이 추가로 발생합니다.

   - **사용자가 Windows 업데이트 패치를 설치하는 것을 허용 안 함**

     사용자가 기기에 Microsoft Windows 업데이트를 수동으로 설치할 수 없습니다. 해당하는 모든 업데이트는 관리자가 구성한 대로 설치됩니다.

     업데이트 설치를 중앙에서 관리하고 싶다면 이 옵션을 선택합니다.

     네트워크가 과부하되지 않도록 업데이트 스케줄을 최적화하려는 경우를 예로 들 수 있습니다. 사용자 생산성이 낮아지지 않도록 업무 시간 이후에 업데이트 스케줄을 지정할 수 있습니다.

8. Windows 업데이트 검색 모드 선택:

- **액티브**

  이 옵션을 선택하면 네트워크 에이전트에서 지원하는 중앙 관리 서버는 클라이언트 기기의 Windows 업데이트 에이전트에서 다음과 같은 업데이트 경로로 요청을 시작합니다: Windows 업데이트 서버 또는 WSUS. 그런 다음 네트워크 에이전트가 Windows 업데이트 에이전트에서 받은 정보를 중앙 관리 서버로 전달합니다.

  취약점 및 필요한 업데이트 검색 작업의 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션이 선택된 경우에만 이 옵션이 적용됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **패시브**

  이 옵션을 선택하면 네트워크 에이전트가 Windows 업데이트 에이전트와 업데이트 경로 간의 마지막 동기화 시 가져온 업데이트 관련 정보를 중앙 관리 서버에 주기적으로 전달합니다. 업데이트 경로와 Windows 업데이트 에이전트의 동기화가 수행되지 않으면 중앙 관리 서버의 업데이트 정보가 최신 상태를 유지할 수 없습니다.

  업데이트 경로의 메모리 캐시에서 업데이트를 받으려면 이 옵션을 선택합니다.

- **비활성화됨**

  이 옵션을 선택하면 중앙 관리 서버가 어떤 업데이트 관련 정보도 수집하지 않습니다.

  예를 들어, 로컬 기기에서 업데이트를 먼저 테스트하려면 이 옵션을 선택하십시오.

9. 실행 파일이 실행될 때 취약점을 검사하고 싶다면 **실행 파일 실행 시 취약점 검사** 옵션을 선택합니다.

10. 변경한 모든 설정에 대해 편집이 잠겨 있는지 확인하십시오. 그렇지 않으면 변경 사항이 적용되지 않습니다.

11. **적용**을 누릅니다.

타사 소프트웨어 취약점 수정

이 섹션에서는 관리 중인 기기에 설치된 소프트웨어의 취약점 수정과 관련된 Kaspersky Security Center의 기능을 설명합니다.

시나리오: 타사 소프트웨어 취약점 찾기 및 수정

이 섹션에서는 Windows를 실행하는 관리 중인 기기에서 취약점을 찾아 수정하는 시나리오를 제공합니다. 운영 체제 및 Microsoft 소프트웨어를 포함한 타사 소프트웨어에서 소프트웨어 취약점을 찾아 수정할 수 있습니다.

필수 구성 요소

- 조직에 Kaspersky Security Center가 배포되어 있습니다.
- 조직에 Windows를 실행하는 관리 중인 기기가 있습니다.

- 중앙 관리 서버가 다음 작업을 수행하려면 인터넷 연결이 필요합니다.
  - Microsoft 소프트웨어의 취약성에 대한 권장 수정 목록을 작성합니다. 이 목록은 Kaspersky 전문가가 생성하고 정기적으로 업데이트합니다.
  - Microsoft 소프트웨어가 아닌 타사 소프트웨어의 취약성을 수정합니다.

단계

소프트웨어 취약점 찾기 및 수정은 다음 단계로 진행됩니다:

1 관리 중인 기기에 설치된 소프트웨어의 취약점 검사

관리 중인 기기에 설치된 소프트웨어에서 취약점을 찾으려면 *취약점 및 필요한 업데이트 검색* 작업을 실행합니다. 이 작업이 완료되면 Kaspersky Security Center는 작업 속성에서 지정한 기기에 설치된 타사 소프트웨어에 대하여 탐지된 취약점 및 필요한 업데이트의 목록을 받습니다.

취약점 및 필요한 업데이트 검색 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동으로 생성합니다. 마법사를 실행하지 않았다면 지금 시작하거나 수동으로 작업을 만듭니다.

방법 지침:

- 관리 콘솔: 애플리케이션 취약점 검사, 취약점 및 필요한 업데이트 검색 작업 스케줄 지정
- Kaspersky Security Center 웹 콘솔: 취약점 및 필요한 업데이트 검색 작업 만들기, 취약점 및 필요한 업데이트 검색 작업 설정

2 탐지된 소프트웨어 취약점 목록 분석

소프트웨어 취약점 목록을 보고 수정할 취약점을 결정합니다. 각 취약점에 대한 자세한 정보를 보려면 목록에서 취약점 이름을 누릅니다. 목록의 각 취약점에 대해 관리 중인 기기의 취약점에 대한 통계를 볼 수도 있습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 취약점에 대한 정보 보기, 관리 중인 기기의 취약점 통계 보기
- Kaspersky Security Center 웹 콘솔: 소프트웨어 취약점 정보 보기, 관리 중인 기기의 취약점 통계 보기

3 취약점 수정 구성

소프트웨어 취약점이 탐지되면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업 또는 *취약점 해결* 작업을 사용하여 관리 중인 기기에서 소프트웨어 취약점을 수정할 수 있습니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 사용하여 관리 중인 기기에 설치된 Microsoft 소프트웨어를 포함한 타사 소프트웨어의 취약점에 대한 업데이트 및 수정을 수행합니다. 이 작업을 통해 여러 업데이트를 설치하고 특정 규칙에 따라 여러 취약점을 수정할 수 있습니다. 이 작업은 취약점 및 패치 관리 기능에 대한 라이센스가 있을 때만 만들 수 있습니다. 소프트웨어 취약점을 수정하기 위해 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업에서는 권장 소프트웨어 업데이트를 사용합니다.

취약점 해결 작업에는 취약점 및 패치 관리 기능에 대한 라이센스 옵션이 필요하지 않습니다. 이 작업을 사용하려면 작업 설정에 나열된 타사 소프트웨어의 취약점에 대한 사용자 수정을 수동으로 지정해야 합니다. *취약점 해결* 작업에서는 Microsoft 소프트웨어에 권장 수정을 사용하고 타사 소프트웨어에는 사용자 수정을 사용합니다.

취약점 수정 마법사를 시작하여 이러한 작업 중 하나를 자동으로 만들거나 수동으로 이러한 작업을 만들 수도 있습니다.

방법 지침:

- 관리 콘솔: 타사 소프트웨어의 취약점에 대한 사용자 수정 선택, 애플리케이션의 취약점 수정
- Kaspersky Security Center 웹 콘솔: 타사 소프트웨어의 취약점에 대한 사용자 수정 선택, 타사 소프트웨어의 취약점 수정, 필요한 업데이트 설치 및 취약점 수정 작업 만들기

4 작업 스케줄 지정

취약점 목록을 항상 최신 상태로 유지하기 위해 *취약점 및 필요한 업데이트 검색* 작업의 스케줄을 지정하여 가끔 자동으로 실행합니다. 권장하는 평균 빈도는 일주일에 한 번입니다.

사용자가 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 만든 경우 *취약점 및 필요한 업데이트 검색* 작업과 빈도가 같거나 적게 실행하도록 스케줄을 지정할 수 있습니다. *취약점 해결* 작업 예약 시 Microsoft 소프트웨어 수정을 선택하거나 작업을 시작하기 전에 매번 타사 소프트웨어의 사용자 수정을 지정해야 합니다.

작업의 스케줄을 지정할 때 *취약점 및 필요한 업데이트 검색* 작업이 완료된 후에 취약점 수정 작업을 시작해야 합니다.

5 소프트웨어 취약점 무시(선택 사항)

원하는 경우 모든 관리 중인 기기 또는 선택한 관리 중인 기기에서만 소프트웨어 취약점 수정을 무시할 수 있습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 취약점 무시
- Kaspersky Security Center 웹 콘솔: 소프트웨어 취약점 무시

6 취약점 수정 작업 실행

취약점 관련 업데이트를 설치하고 취약점 수정 작업 또는 *취약점 수정* 작업을 시작합니다. 작업이 완료되면 작업 목록에서 상태가 *성공적으로 완료*인지 확인하십시오.

7 소프트웨어 취약점 수정 결과에 대한 리포트 작성(선택 사항)

취약점 수정에 대한 자세한 통계를 보려면 취약점 리포트를 생성합니다. 이 리포트에는 수정되지 않은 소프트웨어 취약점에 대한 정보가 표시됩니다. 따라서 조직의 Microsoft 소프트웨어를 포함한 타사 소프트웨어의 취약점을 찾고 수정하는 방법에 대한 아이디어를 얻을 수 있습니다.

방법 지침:

- 관리 콘솔: 리포트 만들기 및 보기
- Kaspersky Security Center 웹 콘솔: 리포트 생성 및 보기

8 타사 소프트웨어의 취약점 발견 및 수정 구성 확인

다음을 수행했는지 확인합니다.

- 관리 중인 기기의 소프트웨어 취약점 목록을 구하고 검토했습니다.
- 원하는 경우 소프트웨어 취약점을 무시했습니다.
- 취약점을 수정하기 위한 작업을 구성했습니다.
- 소프트웨어 취약점을 찾아 수정하기 위한 작업이 순차적으로 시작되도록 작업 스케줄을 지정했습니다.
- 소프트웨어 취약점 수정 작업이 실행되었는지 확인했습니다.

결과

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 생성하고 구성한 경우 관리 중인 기기에서 취약점이 자동으로 수정됩니다. 작업이 실행될 때 사용 가능한 소프트웨어 업데이트의 목록을 작업 설정에 지정된 규칙과 연관시킵니다. 규칙의 기준을 충족하는 모든 소프트웨어 업데이트가 중앙 관리 서버 저장소에 다운로드되고 소프트웨어 취약점을 수정하기 위해 설치됩니다.

사용자가 *취약점 해결* 작업을 만든 경우 Microsoft 소프트웨어의 소프트웨어 취약점만 수정됩니다.

소프트웨어 취약점 찾기 및 수정 정보

Kaspersky Security Center는 Microsoft Windows 제품군 운영 체제를 실행하는 관리 중인 기기에서 소프트웨어 취약점을 탐지하고 수정합니다. 취약점은 운영 체제 및 Microsoft 소프트웨어를 포함한 타사 소프트웨어에서 탐지됩니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)과 KSN 기능이 제공되지 않을 수도 있습니다.

소프트웨어 취약점 찾기

소프트웨어 취약점을 찾기 위해 Kaspersky Security Center는 알려진 취약점 데이터베이스의 특성을 사용합니다. 이 데이터베이스는 Kaspersky 전문가가 만듭니다. 여기에는 취약점 설명, 취약점 탐지 날짜, 취약점 심각도와 같은 취약점에 대한 정보가 포함됩니다. 소프트웨어 취약점의 세부 정보는 Kaspersky 웹사이트에서 확인할 수 있습니다.

Kaspersky Security Center는 *취약점 및 필요한 업데이트 검색* 작업을 사용하여 소프트웨어 취약점을 찾습니다.

경우에 따라 다음 방법 중 하나로 Microsoft Windows 운영 체제에서 탐지한 취약점을 수정할 수 있습니다:

- OS용 업데이트 설치.
- OS를 최신 버전으로 업그레이드(예: Windows 10에서 Windows 11로).

이 시나리오에서 Kaspersky Security Center는 같은 취약점에 대해 두 개의 항목을 표시합니다.

소프트웨어 취약점 수정

소프트웨어 취약점을 해결하기 위해 Kaspersky Security Center는 소프트웨어 공급업체가 제공하는 소프트웨어 업데이트를 사용합니다. 소프트웨어 업데이트 메타데이터는 다음 작업을 실행한 결과로 중앙 관리 서버 저장소로 다운로드됩니다:

- *중앙 관리 서버 저장소에 업데이트 다운로드*. 이 작업은 Kaspersky 및 타사 소프트웨어의 업데이트 메타데이터를 다운로드하기 위한 것입니다. 이 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동으로 생성합니다. 중앙 관리 서버 저장소 작업에 대한 다운로드 업데이트를 수동으로 만들 수 있습니다.
- *Windows 업데이트 동기화 수행*. 이 작업은 Microsoft 소프트웨어용 업데이트 메타데이터를 다운로드하기 위한 것입니다.

취약점을 수정하기 위한 소프트웨어 업데이트는 전체 배포 패키지 또는 패치로 표시될 수 있습니다. 소프트웨어 취약점을 수정하는 소프트웨어 업데이트 이름은 *수정*입니다. *권장 수정*은 Kaspersky 전문가 설치가 권장되는 수정입니다. *사용자 수정*은 사용자 설치가 수동으로 지정되는 수정입니다. 사용자 수정을 설치하려면 이 수정이 포함된 설치 패키지를 만들어야 합니다.

취약점 및 패치 관리 기능이 있는 Kaspersky Security Center 라이센스가 있다면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 사용하여 소프트웨어 취약점을 수정할 수 있습니다. 이 작업은 권장 수정을 설치하여 여러 취약점을 자동으로 수정합니다. 이 작업에서는 여러 취약점을 수정하기 위해 특정 규칙을 수동으로 구성할 수 있습니다.

취약점 및 패치 관리 기능이 있는 Kaspersky Security Center 라이센스가 없다면 *취약점 해결* 작업을 사용하여 소프트웨어 취약점을 수정할 수 있습니다. 이 작업을 통해 Microsoft 소프트웨어에 대한 권장 수정과 타사 소프트웨어에 대한 사용자 수정을 설치하여 취약점을 수정할 수 있습니다.

취약점 및 패치 관리 기능을 사용하여 타사 소프트웨어 업데이트 설치 시, 보안상의 이유로 Kaspersky 기술을 사용해 악성 코드를 자동 검사합니다. 이러한 기술은 자동 파일 검사에 사용되며, 샌드박스 환경에서의 바이러스 검사, 정적 분석, 동적 분석, 행동 분석, 머신 러닝 등을 포함합니다.

Kaspersky 전문가는 취약점 및 패치 관리 기능으로 설치할 수 있는 타사 소프트웨어 업데이트에 대한 수동 분석을 수행하지 않습니다. 또한 Kaspersky 전문가는 이러한 업데이트에서 알려지거나 알려지지 않은 취약점이나 문서화되지 않은 기능을 검색하지 않으며, 위 단락에 지정된 유형 외에 다른 유형의 업데이트 분석도 수행하지 않습니다.

> 관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

일부 소프트웨어 취약점 수정에서 EULA(최종 사용자 라이센스 계약서) 동의가 요청되는 경우 설치 중인 소프트웨어의 EULA에 동의해야 합니다. EULA에 동의하지 않으면 소프트웨어 취약점이 수정되지 않습니다.

소프트웨어 취약점 정보 보기

클라이언트 기기에서 탐지된 취약점 목록을 보려면 다음과 같이 하십시오,

콘솔 트리의 **고급 → 애플리케이션 관리** 폴더에서 **소프트웨어 취약점** 하위 폴더를 선택합니다.

이 페이지에는 관리 중인 기기에서 탐지된 애플리케이션의 취약점의 목록이 표시됩니다.

선택한 취약점에 대한 정보를 얻으려면 다음과 같이 하십시오,

해당 취약점의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

해당 취약점의 속성 창이 열리고 다음과 같은 정보가 표시됩니다:

- 취약점이 탐지된 애플리케이션.
- 취약점이 탐지된 기기 목록.
- 취약점의 수정 여부에 대한 정보.

탐지된 모든 취약점에 대한 리포트를 보려면 다음과 같이 하십시오,

소프트웨어 취약점 폴더에서 **취약점 리포트 보기** 링크를 누릅니다.

기기에 설치된 애플리케이션의 취약점 리포트가 생성됩니다. **리포트** 탭을 열어서 관련 중앙 관리 서버의 이름으로 된 노드에서 이 리포트를 확인할 수 있습니다.

관리 중인 기기의 취약점 통계 보기

관리 중인 기기의 각 소프트웨어 취약점에 대한 통계를 볼 수 있습니다. 통계는 다이어그램으로 표시됩니다. 다이어그램에는 다음과 같은 상태와 함께 기기의 수가 표시됩니다:

- *무시: <기기의 수>*. 이 상태는 취약점 속성에서 취약점을 무시하는 옵션을 직접 설정했을 때 할당됩니다.
- *수정: <기기의 수>*. 이 상태는 취약점 수정 작업이 성공적으로 완료되었을 때만 할당됩니다.
- *수정 스케줄 지정: <기기의 수>*. 이 상태는 취약점을 수정하기 위한 작업을 만들었지만 아직 작업이 수행되지 않았을 때 할당됩니다.
- *패치 적용: <기기의 수>*. 이 상태는 취약점 수정을 위한 소프트웨어 업데이트를 수동으로 선택했지만 이 소프트웨어 업데이트로 취약점을 수정하지 못했을 때 할당됩니다.
- *수정 필요: <기기의 수>*. 이 상태는 취약점이 관리 중인 기기 중 일부에서만 수정되었으며, 관리 중인 다른 기기에서도 취약점을 수정해야 할 때 할당됩니다.

관리 중인 기기의 취약점 통계를 보려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **소프트웨어 취약점** 하위 폴더를 선택합니다.

   이 페이지에는 관리 중인 기기에서 탐지된 애플리케이션의 취약점의 목록이 표시됩니다.

2. 통계를 보려는 취약점을 선택합니다.

   선택한 개체로 작업하기 위한 블록에 취약점 상태 다이어그램이 표시됩니다. 상태를 클릭하면 선택한 상태의 취약점이 있는 기기의 목록이 열립니다.

취약점이 있는지 애플리케이션 검사

빠른 시작 마법사를 통해 애플리케이션을 구성하면 *취약점 검사* 작업이 자동 생성됩니다. **작업** 탭의 **관리 중인 기기** 폴더에서 작업을 볼 수 있습니다.

클라이언트 기기에 설치된 애플리케이션의 취약점 검사 작업을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **고급** → **애플리케이션 관리**를 선택한 다음 **소프트웨어 취약점** 하위 폴더를 선택합니다.

2. 작업 영역에서 **추가 조치** → **취약점 검사 구성**을 선택합니다.

   취약점 검사를 위한 작업이 이미 있으면 기존 작업을 선택한 상태에서 **관리 중인 기기** 폴더의 **작업** 탭이 표시됩니다. 그렇지 않은 경우에는 취약점 및 필요한 업데이트 검색 작업 생성 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

3. **작업 유형 선택** 창에서 **취약점 및 필요한 업데이트 검색**을 선택합니다.

4. 마법사의 **설정** 페이지에서 다음과 같이 작업 설정을 지정합니다:

- **Microsoft에서 작성한 취약점 및 업데이트 검색**

  취약점 및 업데이트를 검색할 때 Kaspersky Security Center는 현재 사용 가능한 Microsoft 업데이트 소스의 해당 Microsoft 업데이트에 대한 정보를 사용합니다.

  예를 들어 Microsoft 업데이트 및 타사 애플리케이션 업데이트에 대해 다양한 설정을 사용하는 다양한 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  선택 사항인 Microsoft Windows 업데이트에 대한 정보는 중앙 관리 서버로 전송되지 않습니다.

- **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트**

  관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결됩니다. 다음 서버는 Microsoft 업데이트의 소스로 작동할 수 있습니다.

  - Kaspersky Security Center 중앙 관리 서버(네트워크 에이전트 정책 설정 참조)
  - 조직의 네트워크에 Microsoft WSUS(Windows 서버 업데이트 서비스)가 배포된 Windows Server
  - Microsoft 업데이트 서버

  이 옵션을 활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결하여 해당하는 Microsoft Windows 업데이트 관련 정보를 새로 고칩니다.

  이 옵션을 비활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 이전에 Microsoft 업데이트 소스에서 받은 해당 Microsoft Windows 업데이트에 관한 정보를 사용합니다.

  Microsoft 업데이트 소스에 연결할 때는 리소스가 많이 사용될 수 있습니다. **소프트웨어 업데이트 및 취약점** 섹션에 있는 네트워크 에이전트 정책의 속성이나 다른 작업에서 이 업데이트 소스에 대한 정기 연결을 설정하는 경우 이 옵션을 비활성화할 수 있습니다. 이 옵션을 비활성화하고 싶지 않으면, 서버 과부하를 줄이기 위해 360분 내에 작업 시작 시간을 랜덤하게 지정하도록 작업 스케줄을 구성할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

다음 옵션 조합의 조합으로 네트워크 에이전트 정책 설정 업데이트를 받는 옵션을 정의합니다.

- 관리 중인 기기의 Windows 업데이트 에이전트는 *취약점 및 필요한 업데이트 검색* 작업의 속성에서 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화하고 네트워크 에이전트 정책 설정에서 **Windows 업데이트 검색 모드** 옵션을 **액티브**으로 설정했을 때만 업데이트 서버에 연결하여 업데이트를 가져옵니다.

- *취약점 검사* 작업을 수행할 때 네트워크 에이전트가 Microsoft Windows 업데이트 경로에 대한 연결 시작과 업데이트 다운로드가 필요하지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하는 동시에 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화된 상태로 유지해야 합니다. 이를 통해 리소스를 절약하고 이전에 받은 Windows 업데이트를 사용하여 취약점을 검사할 수 있습니다. 다른 방법으로 Microsoft Windows 업데이트 수신을 구성하는 경우 수동 모드를 사용할 수 있습니다. Microsoft Windows 업데이트 수신이 다른 방법으로 구성되지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하지 마십시오. 이 경우 업데이트 정보가 수신되지 않습니다.

- **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션의 상태(활성화 또는 비활성화)에 무관하게 **Windows 업데이트 검색 모드** 옵션이 **비활성화됨**로 설정되면 Kaspersky Security Center는 업데이트 정보를 요청하지 않습니다.

- **Kaspersky에서 작성한 타사 취약점 및 업데이트 검색**

  이 옵션을 활성화하면 Kaspersky Security Center는 **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정** 아래에 지정된 폴더와 Windows 레지스트리에서 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)에 필요한 업데이트와 취약점을 검색합니다. 지원되는 타사 애플리케이션의 전체 목록은 Kaspersky에서 관리합니다.

  이 옵션을 비활성화하면 Kaspersky Security Center는 타사 애플리케이션에 필요한 업데이트와 취약점을 검색하지 않습니다. 예를 들어 Microsoft Windows 업데이트 및 타사 애플리케이션 업데이트에 대해 다른 설정을 사용하는 다른 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정**

  Kaspersky Security Center가 취약점을 수정하고 업데이트를 설치해야 하는 타사 애플리케이션을 검색하는 폴더입니다. 시스템 변수를 사용할 수 있습니다.

  애플리케이션이 설치된 폴더를 지정합니다. 목록에는 기본적으로 대다수 애플리케이션이 설치된 시스템 폴더가 포함됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

  작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **고급 진단 파일의 최대 크기(MB)**

  기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

5. 마법사의 **작업 스케줄 구성** 페이지에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

   - **시작 스케줄:**

     작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

     - **N시간마다**

       작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

       작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

     - **N일마다**

       작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

       기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

     - **N주마다**

       작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

       기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

     - **N분마다**

       작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

       기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

     - **매일(서머타임 지원 안 함)**

       작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

       이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

       기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

- **주별**

  이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**

  저장소에 업데이트가 다운로드되고 나면 작업이 실행됩니다. 예를 들어 취약점 및 필요한 업데이트 검색 작업에 이 스케줄을 사용할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

6. 마법사의 **작업 이름 정의** 페이지에서 만들 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

7. 마법사의 **작업 생성 마침** 페이지에서 **완료** 버튼을 눌러 마법사를 닫습니다.

   마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

마법사의 작업이 완료되면 **취약점 및 필수 업데이트 검색** 작업이 **작업** 탭에 있는 **관리 중인 기기** 폴더의 작업 목록에 표시됩니다.

작업 생성 중에 지정하는 설정뿐 아니라 생성된 작업의 기타 속성도 변경할 수 있습니다.

취약점 및 필수 업데이트 검색 작업이 완료되면 기기에 설치되어 있는 애플리케이션에서 발견된 취약점 목록이 중앙 관리 서버에 표시됩니다. 또한 탐지된 취약점을 수정하는 데 필요한 모든 소프트웨어 업데이트도 표시됩니다.

0x80240033 "Windows 업데이트 에이전트 오류 80240033("라이센스 약관을 다운로드할 수 없습니다.")"가 발생하면 Windows 레지스트리를 통해 이 문제를 해결할 수 있습니다.

빠른 설치 파일 다운로드 옵션을 비활성화한 *Windows 업데이트 동기화 작업 수행* 및 *취약점 및 필수 업데이트 검색* 작업을 순차적으로 실행하면 중앙 관리 서버는 필요한 소프트웨어 업데이트 목록을 표시하지 않습니다. 필요한 소프트웨어 업데이트 목록을 보려면, *취약점 및 필수 업데이트 검색* 작업을 다시 실행해야 합니다.

네트워크 에이전트는 사용 가능한 Windows 업데이트 및 기타 Microsoft 제품 업데이트에 대한 정보를 Windows 업데이트 또는 중앙 관리 서버(중앙 관리 서버가 WSUS 서버 역할을 하는 경우)에서 수신합니다. 애플리케이션을 시작할 때(정책에서 해당 기능 제공 시)와 클라이언트 기기에서 *취약점 및 필수 업데이트 검색* 작업을 정기적으로 실행할 때마다 정보가 전송됩니다.

애플리케이션의 취약점 수정

빠른 시작 마법사의 **업데이트 관리 설정** 페이지에서 **타사 제품 업데이트 검색 및 설치**를 선택하면 *필수 업데이트 설치 및 취약점 수정* 작업이 자동 생성됩니다. 이 작업은 **관리 중인 기기** 폴더의 작업 영역에서 **작업** 탭에 표시됩니다.

그렇지 않은 경우에는 다음 중 원하는 작업을 수행할 수 있습니다:

- 사용 가능한 업데이트를 설치하여 취약점을 수정하는 작업을 만듭니다.
- 기존 취약점 수정 작업에 취약점 수정을 위한 규칙을 추가합니다.

관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

취약점 수정 작업을 만들어 취약점 수정

다음 중 원하는 작업을 수행할 수 있습니다:

- 특정 규칙을 충족하는 여러 취약점을 수정하는 작업을 만듭니다.
- 취약점 하나를 선택하고 해당 취약점과 유사한 취약점을 수정하는 작업을 만듭니다.

특정 규칙을 충족하는 취약점을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 취약점을 수정하려는 기기의 중앙 관리 서버를 선택합니다.
2. 메인 애플리케이션 창의 **보기** 메뉴에서 **인터페이스 구성**을 선택합니다.
3. 창이 열리면 **취약점 및 패치 관리 표시** 확인란을 선택한 다음 **확인**을 클릭합니다.
4. 애플리케이션 메시지 창에서 **확인**를 누릅니다.
5. 관리 콘솔을 다시 시작하면 변경 사항이 적용됩니다.
6. 콘솔 트리에서 **관리 중인 기기** 폴더를 선택합니다.
7. 작업 공간에서 **작업** 탭을 선택합니다.
8. **작업 생성** 버튼을 눌러 새 작업 마법사를 실행합니다. 마법사의 각 단계를 따릅니다.
9. 마법사의 **작업 유형 선택** 페이지에서 **필수 업데이트 설치 및 취약점 수정**을 선택합니다.

   작업이 표시되지 않으면 계정에 **시스템 관리**: **취약성 및 패치 관리** 기능 영역에 대한 **읽기**, **수정**, **실행** 권한이 있는지 확인하십시오. 이러한 액세스 권한이 없으면 *필요한 업데이트 설치 및 취약성 수정* 작업을 생성하고 구성할 수 없습니다.
10. 마법사의 **설정** 페이지에서 다음과 같이 작업 설정을 지정합니다:

    - **업데이트 설치 규칙을 지정합니다**

      이러한 규칙은 클라이언트 기기의 업데이트 설치에 적용됩니다. 규칙을 지정하지 않으면 작업이 수행되지 않습니다. 규칙을 사용하는 작업에 대한 정보는 업데이트 설치에 대한 규칙을 참조하십시오.

    - **기기 재시작 또는 종료 시 설치 시작**

      이 옵션을 활성화하면 기기가 다시 시작되거나 종료되기 전에 업데이트가 설치됩니다. 그렇지 않으면 업데이트는 스케줄에 따라 설치됩니다.

      업데이트 설치가 기기 성능에 영향을 줄 수 있는 경우 이 옵션을 사용합니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    - **필요한 일반 시스템 구성 요소 설치**

      이 옵션을 활성화하면 업데이트를 설치하기 전에 애플리케이션은 업데이트 설치를 설치하기 위해 필요한 모든 일반 시스템 구성 요소(선결 조건)를 자동으로 설치합니다. 이러한 필수 구성 요소의 예로는 운영 체제 업데이트 등이 있습니다.

      이 옵션을 비활성화하는 경우에는 필수 구성 요소를 수동으로 설치해야 합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 시 새 애플리케이션 버전의 설치 허용**

  이 옵션을 활성화하면 업데이트 시 소프트웨어 애플리케이션의 새 버전이 설치되는 경우 업데이트가 허용됩니다.

  이 옵션을 비활성화하면 소프트웨어가 업그레이드되지 않습니다. 그러면 소프트웨어의 새 버전을 수동으로 또는 다른 작업을 통해 설치할 수 있습니다. 예를 들어 새 소프트웨어 버전이 회사 인프라를 지원하지 않거나 테스트 인프라에서 업그레이드를 확인하려는 경우 이 옵션을 사용할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  애플리케이션을 업그레이드하면 클라이언트 기기에 설치된 종속 애플리케이션의 오작동이 발생할 수 있습니다.

- **업데이트를 기기에 다운로드만 하고 설치는 하지 않음**

  이 옵션을 활성화하면 애플리케이션은 기기에 업데이트를 다운로드하지만 자동으로 해당 업데이트를 설치하지는 않습니다. 그러면 다운로드한 업데이트를 수동으로 설치할 수 있습니다.

  Microsoft 업데이트는 시스템 Windows 저장소에 다운로드됩니다. 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트는 **업데이트 다운로드 경로** 필드에 지정된 폴더에 다운로드됩니다.

  이 옵션을 비활성화하면 업데이트가 기기에 자동으로 설치됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

  - **업데이트 다운로드 경로**

    이 폴더는 타사 애플리케이션(Kaspersky이 아닌 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트를 다운로드하는 데 사용됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

  작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **고급 진단 파일의 최대 크기(MB)**

  기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

11. 마법사의 **운영 체제 재시작 옵션 선택** 페이지에서 작업 후 클라이언트 기기의 운영 체제를 재시작해야 할 때 수행할 작업을 선택합니다:

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

  - **반복해서 물어보기(분)**

    이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

    기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

    이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

  - **다음 시간 이후에 재시작(분)**

    사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

    기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

12. 마법사의 **작업 스케줄 구성** 페이지에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

- **시작 스케줄:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

    작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

  - **N일마다**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

    기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **N주마다**

    작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

    기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

  - **N분마다**

    작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

    기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

  - **매일(서머타임 지원 안 함)**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

    이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

- **주별**

  이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

13. 마법사의 **작업 이름 정의** 페이지에서 만들 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

14. 마법사의 **작업 생성 마침** 페이지에서 **완료** 버튼을 눌러 마법사를 닫습니다.

    마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

마법사의 작업이 완료되면 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업이 생성되어 **작업** 폴더에 표시됩니다.

작업 생성 중에 지정하는 설정뿐 아니라 생성된 작업의 기타 속성도 변경할 수 있습니다.

작업 결과에 0x80240033 'Windows 업데이트 에이전트 오류 80240033("라이센스 약관을 다운로드할 수 없습니다.")' 오류가 포함되어 있는 경우 Windows 레지스트리를 통해 이 문제를 해결할 수 있습니다.

특정 취약점 및 유사한 취약점을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급 → 애플리케이션 관리** 폴더에서 **소프트웨어 취약점** 하위 폴더를 선택합니다.

2. 수정하고 싶은 취약점을 선택합니다.

3. **취약점 수정 마법사 실행** 버튼을 누릅니다.

   취약점 수정 마법사가 시작됩니다.

   취약점 수정 마법사 기능은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

   마법사의 각 단계를 따릅니다.

4. **기존 취약점 수정 작업 검색** 창에서 다음 파라미터를 지정합니다:

   - **이 취약점을 수정하는 작업만 표시**

     이 옵션이 활성화되어 있으면 취약점 수정 마법사에서 선택한 취약점을 수정하는 기존 작업을 검색합니다.

     이 옵션이 비활성화되어 있거나 검색에서 해당하는 작업이 검색되지 않으면 취약점 수정 마법사에는 취약점 수정을 위한 작업이나 규칙을 만들라는 메시지가 표시됩니다.

     이 옵션은 기본적으로 활성화되어 있습니다.

   - **이 취약점을 수정하는 업데이트 승인**

     취약점을 수정하는 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

5. 기존 취약점 수정 작업을 검색하도록 선택하여 검색에서 일부 작업이 검색되는 경우 해당 작업의 속성을 확인하거나 작업을 수동으로 시작할 수 있습니다. 추가 조치는 필요하지 않습니다.

   그렇지 않은 경우에는 **새 취약점 수정 작업** 버튼을 누릅니다.

6. 새 작업에 추가할 취약점 수정 규칙의 유형을 선택하고 **마침** 버튼을 누릅니다.

7. 모든 이전 애플리케이션 업데이트 설치와 관련하여 표시되는 메시지에서 원하는 옵션을 선택합니다. 선택한 업데이트를 설치하는 데 필요한 경우 후속 애플리케이션 버전의 증분 방식 설치에 동의한다면 **예**를 누릅니다. 후속 버전을 설치하지 않고 애플리케이션을 단순하게 업데이트하려면 **아니오**를 누릅니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

   업데이트 설치 및 취약점 수정 작업 만들기 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

8. 마법사의 **운영 체제 재시작 옵션 선택** 페이지에서 작업 후 클라이언트 기기의 운영 체제를 재시작해야 할 때 수행할 작업을 선택합니다:

   - **기기 다시 시작 안 함**

     작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

   - **기기 다시 시작**

     이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

   - **사용자 확인 후 처리**

     클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

     기본적으로 이 옵션은 선택되어 있습니다.

     - **반복해서 물어보기(분)**

       이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

       기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

       이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

     - **다음 시간 이후에 재시작(분)**

       사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

       기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

   - **잠긴 세션에서 애플리케이션 강제 종료**

     애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

9. 마법사의 **이 작업이 할당되는 기기 선택** 페이지에서 다음 옵션 중 하나를 선택합니다.

- **중앙 관리 서버가 발견한 기기 중에서 선택**

  특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.

  예를 들어 미할당 기기에 네트워크 에이전트를 설치하는 작업에서 이 옵션을 사용할 수 있습니다.

- **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

  작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

  특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

- **기기 선택 결과에 작업 할당**

  기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

  예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

- **관리 그룹에 작업 할당**

  관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

  예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

  관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

10. 마법사의 **작업 스케줄 구성** 페이지에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

- **시작 스케줄:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

    작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

- **N일마다**

  작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

  기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **N주마다**

  작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

  기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

- **N분마다**

  작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

  기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

- **매일(서머타임 지원 안 함)**

  작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

  이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

  기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

- **주별**

  이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.

  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

11. 마법사의 **작업 이름 정의** 페이지에서 만들 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

12. 마법사의 **작업 생성 마침** 페이지에서 **완료** 버튼을 눌러 마법사를 닫습니다.
    마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

마법사가 완료되면 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업이 생성되어 **작업** 폴더에 표시됩니다.

작업 생성 중에 지정하는 설정뿐 아니라 생성된 작업의 기타 속성도 변경할 수 있습니다.

기존 취약점 수정 작업에 규칙을 추가하여 취약점 수정

기존 취약점 수정 작업에 규칙을 추가하여 취약점을 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **소프트웨어 취약점** 하위 폴더를 선택합니다.

2. 수정하고 싶은 취약점을 선택합니다.

3. **취약점 수정 마법사 실행** 버튼을 누릅니다.
   취약점 수정 마법사가 시작됩니다.

   취약점 수정 마법사 기능은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

   마법사의 각 단계를 따릅니다.

4. **기존 취약점 수정 작업 검색** 창에서 다음 파라미터를 지정합니다:

   - **이 취약점을 수정하는 작업만 표시**

     이 옵션이 활성화되어 있으면 취약점 수정 마법사에서 선택한 취약점을 수정하는 기존 작업을 검색합니다.

     이 옵션이 비활성화되어 있거나 검색에서 해당하는 작업이 검색되지 않으면 취약점 수정 마법사에는 취약점 수정을 위한 작업이나 규칙을 만들라는 메시지가 표시됩니다.

     이 옵션은 기본적으로 활성화되어 있습니다.

   - **이 취약점을 수정하는 업데이트 승인**

     취약점을 수정하는 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

5. 기존 취약점 수정 작업을 검색하도록 선택하여 검색에서 일부 작업이 검색되는 경우 해당 작업의 속성을 확인하거나 작업을 수동으로 시작할 수 있습니다. 추가 조치는 필요하지 않습니다.

   그렇지 않은 경우에는 **기존 작업에 취약점 수정 규칙 추가** 버튼을 누릅니다.

6. 규칙을 추가할 작업을 선택하고 **규칙 추가** 버튼을 누릅니다.

   기존 작업의 속성을 확인하거나, 작업을 수동으로 시작하거나, 새 작업을 만들 수도 있습니다.

7. 선택한 작업에 추가할 규칙의 유형을 선택하고 **마침** 버튼을 누릅니다.

8. 모든 이전 애플리케이션 업데이트 설치와 관련하여 표시되는 메시지에서 원하는 옵션을 선택합니다. 선택한 업데이트를 설치하는 데 필요한 경우 후속 애플리케이션 버전의 증분 방식 설치에 동의한다면 **예**를 누릅니다. 후속 버전을 설치하지 않고 애플리케이션을 단순하게 업데이트하려면 **아니오**를 누릅니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

취약점 수정을 위한 새 규칙이 기존 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업에 추가됩니다.

격리된 네트워크의 취약점 수정

이 섹션에서는 인터넷 액세스가 없는 격리된 중앙 관리 서버에 연결된 관리 대상 기기에서 타사 소프트웨어 취약점을 수정하기 위해 수행할 수 있는 단계를 설명합니다.

시나리오: 격리된 네트워크에서 타사 소프트웨어 취약점 수정

격리된 네트워크에서 관리 중인 기기에 설치된 타사 소프트웨어의 업데이트를 설치하고 취약점을 수정할 수 있습니다. 이러한 네트워크에는 인터넷에 액세스가 없는 중앙 관리 서버 및 이에 연결된 관리 대상 기기가 포함됩니다. 이러한 네트워크의 취약점을 수정하려면 인터넷에 연결된 중앙 관리 서버가 필요합니다. 그런 다음 인터넷 액세스가 가능한 중앙 관리 서버를 사용하여 업데이트가 포함된 패치를 다운로드하고 패치를 격리된 중앙 관리 서버로 전송할 수 있습니다.

소프트웨어 공급업체에서 발행한 타사 소프트웨어 업데이트는 다운로드할 수 있지만 Kaspersky Security Center를 사용하여 격리된 중앙 관리 서버에서 Microsoft 소프트웨어 업데이트를 다운로드할 수는 없습니다.

격리된 네트워크에서 취약점을 수정하는 프로세스가 작동하는 방식을 알아보려면 이 프로세스의 설명 및 구성을 참조하십시오.

필수 구성 요소

시작하기 전에 다음을 먼저 진행해 주십시오.

1. 인터넷에 연결하고 패치를 다운로드하기 위해 기기 한 개를 할당합니다. 이 기기는 인터넷 액세스가 가능한 중앙 관리 서버로 계산됩니다.
2. 다음 기기에 Kaspersky Security Center 14 버전 이하를 설치 하십시오.
   - 인터넷 액세스가 가능한 중앙 관리 서버 역할을 하는 할당된 기기
   - 인터넷에서 격리된 중앙 관리 서버 역할을 하는 격리된 기기 (이하 격리된 중앙 관리 서버라고 함)
3. 모든 중앙 관리 서버에 업데이트 및 패치를 다운로드하고 저장하기 위한 충분한 디스크 공간이 있는지 확인합니다.

단계

격리된 중앙 관리 서버의 관리 대상 기기에 업데이트 설치 및 타사 소프트웨어 취약성 수정은 다음 단계로 구성됩니다.

1. **인터넷 액세스가 가능한 중앙 관리 서버 구성**

   인터넷 액세스가 가능한 중앙 관리 서버를 준비하여 필요한 타사 소프트웨어 업데이트에 대한 요청을 처리하고 패치를 다운로드합니다.

2. **격리된 중앙 관리 서버 구성**

   격리된 중앙 관리 서버를 준비하여 필요한 업데이트 목록을 형성하고 인터넷 액세스를 통해 중앙 관리 서버에서 다운로드한 패치를 처리할 수 있습니다. 구성 후에는 격리된 중앙 관리 서버가 인터넷에서 패치를 다운로드하려고 시도하지 않습니다. 대신 패치를 통해 업데이트를 받습니다.

3. **격리된 중앙 관리 서버의 패치 관리 및 업데이트 설치**

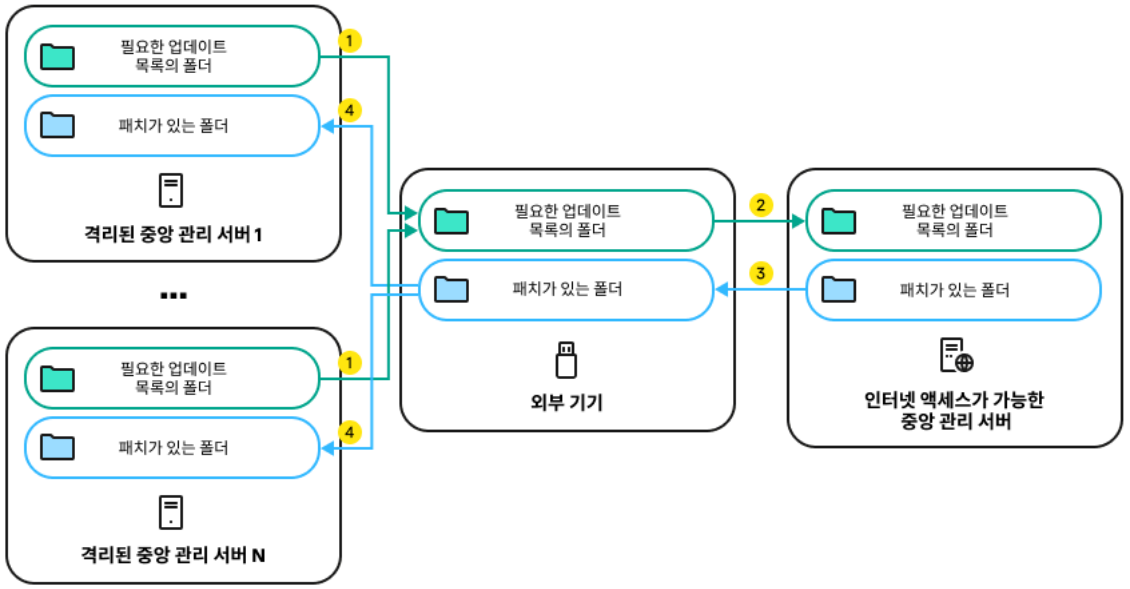
   서버 구성을 완료한 후 인터넷 액세스가 가능한 중앙 관리 서버와 격리된 중앙 관리 서버 간에 필요한 업데이트 목록 및 패치를 전송할 수 있습니다. 다음으로 패치의 업데이트는 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 사용하여 관리 중인 기기에 설치됩니다.

결과

따라서 타사 소프트웨어 업데이트가 격리된 중앙 관리 서버로 전송되고 Kaspersky Security Center를 통해 연결된 관리 대상 기기에 설치됩니다. 중앙 관리 서버는 한 번만 구성해도 되며 이후에는 필요한 만큼 업데이트할 수 있습니다(예: 하루에 한 번 또는 여러 번).

격리된 네트워크에서 타사 소프트웨어 취약점 수정 정보

격리된 네트워크에서 타사 소프트웨어 취약점을 수정하는 프로세스는 아래 그림에 설명되어 있습니다. 이 프로세스는 주기적으로 반복할 수 있습니다.



인터넷 액세스가 가능한 중앙 관리 서버와 격리된 중앙 관리 서버 간의 패치 및 필요한 업데이트 목록을 전송하는 프로세스

인터넷에서 격리된 모든 중앙 관리 서버(이하 격리된 중앙 관리 서버)는 이 중앙 관리 서버에 연결된 관리 기기에 설치해야 하는 업데이트 목록을 생성합니다. 필요한 업데이트 목록은 특정 폴더에 저장되며 이진 파일 집합을 제공합니다. 각 파일에는 필요한 업데이트가 있는 패치의 ID가 포함된 이름이 있습니다. 따라서 목록의 모든 파일이 특정 패치를 가리킵니다.

외부 기기를 사용하여 필요한 업데이트 목록을 격리된 중앙 관리 서버에서 인터넷 액세스가 가능한 할당된 중앙 관리 서버로 전송합니다. 그런 다음 할당된 중앙 관리 서버가 인터넷에서 패치를 다운로드하여 별도의 폴더에 넣습니다.

모든 패치가 다운로드되고 해당 패치용 특정 폴더에 있는 경우 필요한 업데이트 목록을 가져온 모든 격리된 중앙 관리 서버로 패치를 이동합니다. 격리된 중앙 관리 서버에서 패치를 위해 별도로 만든 폴더에 패치를 저장합니다. 따라서 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업은 패치를 실행하고 격리된 중앙 관리 서버의 관리 기기에 업데이트를 설치합니다.

격리된 네트워크의 취약점을 수정하기 위해 인터넷 액세스를 사용하여 중앙 관리 서버 구성

격리된 네트워크에서 업데이트를 사용하여 취약점 수정 및 패치 전송을 준비하려면 먼저 인터넷 액세스가 가능한 중앙 관리 서버를 구성한 다음 격리된 중앙 관리 서버를 구성합니다.

인터넷 액세스가 가능한 중앙 관리 서버를 구성하려면 다음을 수행합니다.

1. 중앙 관리 서버가 설치된 디스크에 다음과 같은 두 개의 폴더를 만듭니다.

   - 필요한 업데이트 목록의 폴더
   - 패치 폴더

   이 폴더의 이름은 원하는 대로 지정할 수 있습니다.

2. 운영 체제의 표준 관리 도구를 사용하여 생성된 폴더의 KLAdmins 그룹에 대한 수정 액세스 권한을 부여합니다.

3. klscflag 유틸리티를 사용하여 중앙 관리 서버 속성의 폴더에 대한 경로를 씁니다.

   관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

4. Windows 명령 프롬프트에서 다음 명령을 입력합니다.

   - 패치 폴더의 경로를 설정하려면 다음을 수행합니다.
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"
     ```
   - 필요한 업데이트 목록의 폴더 경로를 설정하려면 다음을 수행합니다.
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"
     ```

   예: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<패치용 폴더>"`

5. 필요하다면, klscflag 유틸리티를 사용하여 관리 중인 기기가 새 패치 요청을 확인할 빈도를 지정합니다.
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <값(초)>
   ```
   기본 값은 120 초입니다.

   예시: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. *취약점 및 필요한 업데이트 검색* 작업을 생성하여 관리 중인 기기에 설치된 타사 소프트웨어용 패치 정보를 얻은 후 작업 스케줄을 설정합니다.

7. *취약점 해결* 작업을 생성하여 취약점 수정에 사용되는 타사 소프트웨어용 패치를 지정한 다음 작업 스케줄을 설정합니다.

   지정된 일정보다 일찍 실행하려면 작업을 수동 실행하십시오. 작업 시작 순서가 중요합니다. *취약점 해결* 작업은 *취약점 및 필요한 업데이트 검색* 작업 완료 후에 실행해야 합니다.

8. 중앙 관리 서버 서비스를 다시 시작합니다.

이제 인터넷 액세스가 가능한 중앙 관리 서버가 업데이트를 다운로드하고 격리된 중앙 관리 서버에 전송할 수 있습니다. 취약점 수정을 시작하기 전에 격리된 중앙 관리 서버를 구성합니다.

격리된 네트워크의 취약점을 수정하도록 격리된 중앙 관리 서버 구성

인터넷 액세스가 가능한 중앙 관리 서버 구성을 완료한 후, 네트워크에서 격리된 모든 중앙 관리 서버를 준비하면 격리된 중앙 관리 서버에 연결된 관리 대상 기기에서 취약점을 수정하고 업데이트 설치할 수 있습니다.

격리된 중앙 관리 서버를 구성하려면 모든 중앙 관리 서버에서 다음 작업을 수행합니다.

1. 취약점 및 패치 관리(VAPM) 기능에 대한 라이센스 키를 활성화합니다.

2. 중앙 관리 서버가 설치된 디스크에 다음과 같은 두 개의 폴더를 만듭니다.

   - 필요한 업데이트 목록이 표시될 폴더
   - 패치 폴더

   이 폴더의 이름은 원하는 대로 지정할 수 있습니다.

3. 운영 체제의 표준 관리 도구를 사용하여 생성된 폴더의 KLAdmins 그룹에 대한 *수정* 액세스 권한을 부여합니다.

4. klscflag 유틸리티를 사용하여 중앙 관리 서버 속성의 폴더에 대한 경로를 씁니다.

   관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

5. Windows 명령 프롬프트에서 다음 명령을 입력합니다.

   - 패치 폴더의 경로를 설정하려면 다음을 수행합니다.
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<path to the folder>"`

   - 필요한 업데이트 목록의 폴더 경로를 설정하려면 다음을 수행합니다.
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<path to the folder>"`

   예: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<패치용 폴더>"`

6. 필요하다면, klscflag 유틸리티를 사용하여 격리된 중앙 관리 서버가 새 패치를 확인할 빈도를 지정합니다.
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <value in seconds>`

   기본 값은 120 초입니다.

   예시: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. 필요하다면, klscflag 유틸리티를 사용하여 패치의 SHA256 해시를 계산합니다.
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   이 명령을 입력하면 격리된 중앙 관리 서버로 전송하는 동안 패치가 수정되지 않았는지, 필요한 업데이트가 포함된 올바른 패치를 수신했는지 확인할 수 있습니다.

   기본적으로 Kaspersky Security Center는 패치의 SHA256 해시를 계산하지 않습니다. 이 옵션을 활성화하면 격리된 중앙 관리 서버가 패치를 수신한 후 Kaspersky Security Center가 해당 해시를 계산하고 획득한 값을 중앙 관리 서버 데이터베이스에 저장된 해시와 비교합니다. 계산된 해시가 데이터베이스의 해시와 일치하지 않으면 오류가 발생하며 잘못된 패치를 교체해야 합니다.

8. *취약점 및 필요한 업데이트 검색* 작업을 생성하여 관리 중인 기기에 설치된 타사 소프트웨어용 패치 정보를 얻은 후 작업 스케줄을 설정합니다.

9. *취약점 해결* 작업을 생성하여 취약점 수정에 사용되는 타사 소프트웨어용 패치를 지정한 다음 작업 스케줄을 설정합니다.

   지정된 일정보다 일찍 실행하려면 작업을 수동 실행하십시오. 작업 시작 순서가 중요합니다. *취약점 해결* 작업은 *취약점 및 필요한 업데이트 검색* 작업 완료 후에 실행해야 합니다.

10. 중앙 관리 서버 서비스를 다시 시작합니다.

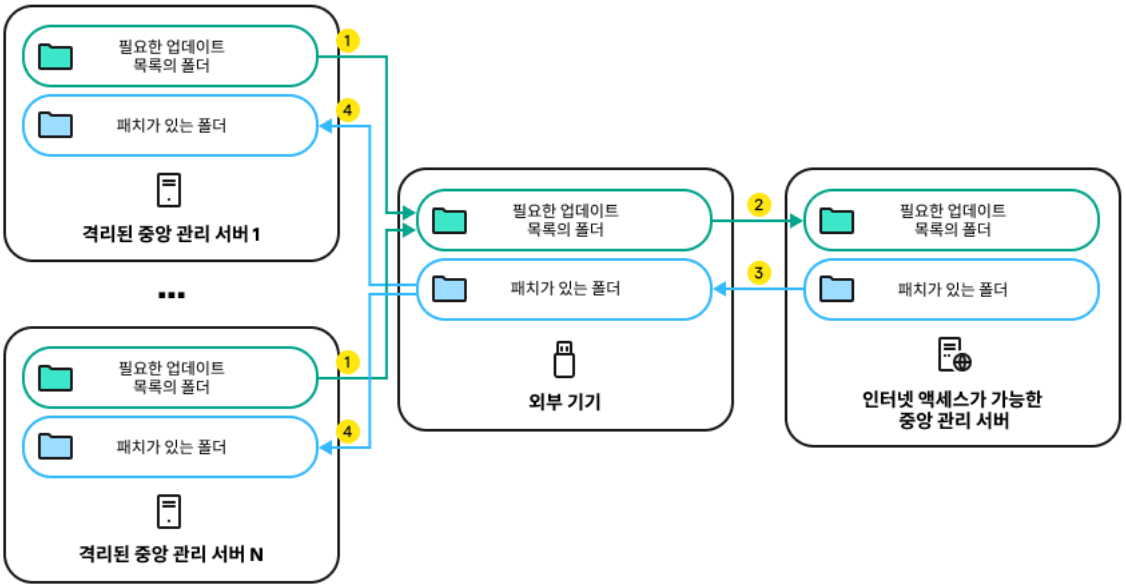
모든 중앙 관리 서버를 구성한 후 패치 및 필요한 업데이트 목록을 이동하고 격리된 네트워크에서 관리 중인 기기에 대한 타사 소프트웨어 취약점을 수정합니다.

격리된 네트워크에서 패치 관리 및 업데이트 설치

중앙 관리 서버 구성을 완료한 후, 업데이트가 포함된 패치를 인터넷 액세스가 가능한 중앙 관리 서버에서 격리된 중앙 관리 서버로 전송할 수 있습니다. 하루에 한 번 또는 여러 번 등 필요한 만큼 업데이트를 전송하고 설치할 수 있습니다.

중앙 관리 서버 간에 패치와 필요한 업데이트 목록을 전송하려면 이동식 드라이브와 같은 외부 기기가 필요합니다. 따라서 외부 기기에 업데이트 및 패치를 다운로드하고 저장하기 위해 충분한 디스크 공간이 있는지 확인하십시오.

아래 그림에는 패치 및 필요한 업데이트 목록을 전송하는 프로세스가 설명되어 있습니다.



인터넷 액세스가 가능한 중앙 관리 서버와 격리된 중앙 관리 서버 간의 패치 및 필요한 업데이트 목록을 전송하는 프로세스

격리된 중앙 관리 서버에 연결된 관리 기기에 업데이트를 설치하고 취약점을 수정하려면:

1. *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 아직 실행되고 있지 않은 경우 시작합니다.

2. 외부 기기를 격리된 중앙 관리 서버에 연결합니다.

3. 외부 기기에 필요한 업데이트 목록용 폴더 하나와 패치용 폴더 하나를 만듭니다. 이 폴더의 이름은 원하는 대로 지정할 수 있습니다.

   이전에 만든 폴더는 삭제하십시오.

4. 격리된 모든 중앙 관리 서버에서 필수 업데이트 목록을 복사하고 이 목록을 외부 기기의 필요한 업데이트 목록 폴더에 붙여넣습니다.

   결과적으로 격리된 모든 중앙 관리 서버에서 가져온 모든 목록을 하나의 폴더로 통합합니다. 따라서 이 폴더에는 격리된 모든 중앙 관리 서버에 필요한 패치 ID가 있는 이진 파일이 포함되어야 합니다.

5. 외부 기기를 인터넷 액세스가 가능한 중앙 관리 서버에 연결합니다.

6. 외부 기기에서 필요한 업데이트 목록을 복사하고 인터넷 액세스가 가능한 중앙 관리 서버의 필요한 업데이트 목록 폴더에 이 목록을 붙여넣습니다.

   필요한 모든 패치는 인터넷에서 중앙 관리 서버의 패치 폴더로 자동 다운로드됩니다. 몇 시간이 걸릴 수 있습니다.

7. 필요한 모든 패치가 다운로드되었는지 확인합니다. 이를 위해 다음 작업 중 하나를 수행할 수 있습니다.

   - 인터넷 액세스가 가능한 중앙 관리 서버의 패치 폴더를 확인합니다. 필요한 업데이트 목록에 지정된 모든 패치는 필요한 폴더에 다운로드해야 합니다. 적은 수의 패치가 필요한 경우 더 편리합니다.

   - 셸 스크립트와 같은 특수 스크립트를 준비합니다. 여러 패치를 받는 경우 모든 패치가 다운로드되었는지 직접 확인하기 어려울 수 있습니다. 이러한 경우 검사를 자동화하는 것이 좋습니다.

8. 인터넷 액세스가 가능한 중앙 관리 서버에서 패치를 복사하여 외부 기기의 해당 폴더에 붙여넣습니다.

9. 패치를 격리된 모든 중앙 관리 서버로 전송합니다. 패치를 지정 폴더에 넣습니다.

따라서 격리된 모든 중앙 관리 서버가 현재 중앙 관리 서버에 연결된 관리 대상 기기에 필요한 업데이트의 실제 목록을 생성합니다. 인터넷 액세스가 가능한 중앙 관리 서버가 필요한 업데이트 목록을 수신한 후 서버가 인터넷에서 업데이트가 포함된 패치를 다운로드합니다. 이러한 패치가 격리된 중앙 관리 서버에 표시되면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 패치를 처리합니다. 따라서 업데이트가 관리 중인 기기에 설치되고 타사 소프트웨어 취약점이 수정됩니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업이 실행 중일 때는 중앙 관리 서버 기기를 재부팅하거나 중 *중앙 관리 서버 데이터 백업* 작업을 실행하지 마십시오(재부팅의 원인이 됨). 그렇게 하면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 중단되고 업데이트가 설치되지 않습니다. 이 경우 작업을 수동으로 다시 시작하거나 구성된 일정에 따라 작업이 시작될 때까지 기다려야 합니다.

격리된 네트워크에서 패치를 전송하고 업데이트를 설치할 수 있는 옵션 비활성화

예를 들어 격리된 네트워크에서 하나 이상의 서버를 가져오기로 결정한 경우, 격리된 중앙 관리 서버에서 업데이트가 포함된 패치 전송을 비활성화할 수 있습니다. 따라서 패치 수와 다운로드 시간을 줄일 수 있습니다.

격리된 중앙 관리 서버에서 패치를 관리할 수 있는 옵션을 비활성화하려면 다음을 수행합니다.

1. 모든 중앙 관리 서버를 격리 해제하려면 인터넷 액세스가 가능한 중앙 관리 서버의 속성에서 패치 폴더의 경로와 필요한 업데이트 목록을 삭제합니다. 일부 중앙 관리 서버를 격리된 네트워크에서 유지하려면 이 단계를 건너뛰십시오.

   관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

   Windows 명령 프롬프트에서 다음 명령을 입력합니다.

   - 패치 폴더의 경로를 삭제하려면 다음을 수행합니다.
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - 필요한 업데이트 목록의 폴더 경로를 삭제하려면 다음을 수행합니다.
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. 이 중앙 관리 서버에서 폴더 경로를 삭제한 경우 중앙 관리 서버 서비스를 다시 시작하십시오.

3. 격리를 해제하려는 모든 중앙 관리 서버의 속성에서 패치 폴더의 경로와 필요한 업데이트 목록을 삭제합니다.

   관리자 권한을 사용하여 Windows 명령 프롬프트에서 다음 명령을 입력합니다.

   - 패치 폴더의 경로를 삭제하려면 다음을 수행합니다.
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - 필요한 업데이트 목록의 폴더 경로를 삭제하려면 다음을 수행합니다.
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. 폴더 경로를 삭제한 중앙 관리 서버의 서비스를 다시 시작하십시오.

따라서 인터넷 액세스가 가능한 중앙 관리 서버를 재구성한 경우 더 이상 Kaspersky Security Center를 통해 패치를 받을 수 없습니다. 예를 들어 일부 격리된 중앙 관리 서버만 재구성한 경우 격리된 네트워크에서 일부를 가져오면 나머지 격리된 중앙 관리 서버에 대한 패치만 받게 됩니다.

격리된 중앙 관리 서버의 취약점 수정을 비활성화한 후 나중에 다시 시작하려면 이 중앙 관리 서버와 인터넷 액세스가 가능한 중앙 관리 서버를 다시 구성해야 합니다.

소프트웨어 취약점 무시

수정할 소프트웨어 취약점을 무시할 수 있습니다. 소프트웨어 취약점을 무시하는 이유는 다음과 같은 것이 있을 수 있습니다:

- 해당 소프트웨어 취약점이 조직에 치명적이라고 생각하지 않습니다.
- 소프트웨어 취약점 수정이 취약점 수정이 필요한 소프트웨어와 관련된 데이터를 손상시킬 수 있다는 것을 이해합니다.
- 다른 방법을 사용하여 관리 중인 기기를 보호하기 때문에 소프트웨어 취약점이 조직의 네트워크에 위험하지 않다고 확신합니다.

모든 관리 중인 기기나 선택한 관리 중인 기기에서 소프트웨어 취약점을 무시할 수 있습니다.

모든 관리 중인 기기에서 소프트웨어 취약점을 무시하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급 → 애플리케이션 관리** 폴더에서 **소프트웨어 취약점** 하위 폴더를 선택합니다.

   폴더의 작업 영역에는 설치된 네트워크 에이전트가 기기에서 탐지한 애플리케이션의 취약점 목록이 표시됩니다.

2. 무시하고 싶은 취약점을 선택합니다.
3. 해당 취약점의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   취약점 속성 창이 열립니다.

4. **일반** 섹션에서 **취약점 무시** 옵션을 선택합니다.
5. **확인**를 누릅니다.

   소프트웨어 취약점 속성 창이 닫힙니다.

모든 관리 중인 기기에서 소프트웨어 취약점이 무시됩니다.

선택한 관리 중인 기기에서 소프트웨어 취약점을 무시하려면 다음과 같이 하십시오:

1. 선택한 관리 중인 기기의 속성 창을 열고 **소프트웨어 취약점** 섹션을 선택합니다.
2. 소프트웨어 취약점을 선택합니다.
3. 선택한 취약점을 무시합니다.

선택한 기기에서 소프트웨어 취약점이 무시됩니다.

무시한 소프트웨어 취약점은 *취약점 해결* 작업 또는 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 완료한 후에 수정되지 않습니다. 취약점 목록에서 필터를 사용하여 무시한 소프트웨어 취약점을 제외할 수 있습니다.

타사 소프트웨어의 취약점에 사용자 수정 선택

취약점 해결 작업을 사용하려면 작업 설정에 나열된 타사 소프트웨어의 취약점을 수정하기 위한 소프트웨어 업데이트를 수동으로 지정해야 합니다. *취약점 해결* 작업에서는 Microsoft 소프트웨어에 권장 수정을 사용하고 타사 소프트웨어에 사용자 수정을 사용합니다. *사용자 수정*은 관리자가 설치를 위해 수동으로 지정하는 취약점을 수정하기 위한 소프트웨어 업데이트입니다.

타사 소프트웨어의 취약점에 대한 사용자 수정을 선택하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급 → 애플리케이션 관리** 폴더에서 **소프트웨어 취약점** 하위 폴더를 선택합니다.

   폴더의 작업 영역에는 설치된 네트워크 에이전트가 기기에서 탐지한 애플리케이션의 취약점 목록이 표시됩니다.

2. 사용자 수정을 지정하려는 취약점을 선택합니다.

3. 해당 취약점의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   취약점 속성 창이 열립니다.

4. **사용자 수정 또는 기타 수정** 섹션에서 **추가** 버튼을 누릅니다.

   사용 가능한 설치 패키지 목록이 표시됩니다. 표시되는 설치 패키지의 목록은 **원격 설치 → 설치 패키지** 목록에 해당합니다. 선택한 취약점에 대한 사용자 수정이 포함된 설치 패키지를 만들지 않았다면 새 패키지 마법사를 시작하여 패키지를 만들 수 있습니다.

5. 타사 소프트웨어의 취약점에 대한 사용자 수정이 포함된 설치 패키지를 선택합니다.

6. **확인**를 누릅니다.

   소프트웨어 취약점에 대한 사용자 수정이 포함된 설치 패키지가 지정됩니다. *취약점 해결* 작업이 시작되면 설치 패키지가 설치되고 소프트웨어 취약점이 수정됩니다.

업데이트 설치에 대한 규칙

애플리케이션의 취약점을 수정할 때는 업데이트 설치를 위한 규칙을 지정해야 합니다. 이러한 규칙에 따라 설치할 업데이트와 수정할 취약점이 결정됩니다.

정확한 설정은 업데이트 규칙을 생성하는 대상(Microsoft 애플리케이션, 타사 애플리케이션(Kaspersky이 아닌 소프트웨어 공급 업체에서 만든 애플리케이션) 또는 모든 애플리케이션)에 따라 달라집니다. Microsoft 애플리케이션 또는 타사 애플리케이션용 규칙을 생성할 때는 업데이트를 설치할 특정 애플리케이션 및 애플리케이션 버전을 선택할 수 있습니다. 모든 애플리케이션용 규칙을 생성할 때는 설치할 특정 업데이트 및 업데이트 설치를 통해 수정할 취약점을 선택할 수 있습니다.

모든 애플리케이션의 업데이트를 위한 새 규칙을 생성하려면 다음과 같이 하십시오:

1. 새 작업 마법사의 **설정** 페이지에서 **추가** 버튼을 누릅니다.

   규칙 생성 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

2. **규칙 유형** 페이지에서 **모든 업데이트에 대한 규칙**를 선택합니다.

3. **일반 기준** 페이지에서 드롭다운 목록을 사용하여 다음 설정을 지정합니다:

- **설치할 업데이트 세트**

  클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.

  - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
  - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
  - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

- **다음 심각도와 같거나 높은 취약점만 수정**

  소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

  이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

  이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

4. **업데이트** 페이지에서 설치할 업데이트를 선택합니다:

- **적합한 모든 업데이트 설치**

  마법사의 **일반 기준** 페이지에 지정된 기준을 충족하는 모든 소프트웨어 업데이트를 설치합니다. 기본적으로 선택됩니다.

- **다음 목록의 업데이트만 설치**

  목록에서 수동으로 선택하는 소프트웨어 업데이트만 설치합니다. 이 목록에는 사용 가능한 모든 소프트웨어 업데이트가 포함되어 있습니다.

  예를 들어 테스트 환경에서 설치를 확인하거나 중요한 애플리케이션 또는 특정 애플리케이션만 업데이트하려는 등의 경우 특정 업데이트를 선택할 수 있습니다.

  - **선택된 업데이트를 설치하는 데 필요한 이전의 모든 애플리케이션 업데이트 자동 설치**

    선택한 업데이트를 설치하는 데 필요한 경우 중간 애플리케이션 버전 설치에 동의한다면 이 옵션을 활성화한 상태로 유지하십시오.

    이 옵션을 비활성화하면 애플리케이션의 선택한 버전만 설치됩니다. 후속 버전의 증분 방식 설치를 시도하지 않고 단순하게 애플리케이션을 업데이트하려면 이 옵션을 비활성화합니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

    기기에 설치되어 있는 애플리케이션 버전 3을 버전 5로 업데이트하려고 하는데 이 애플리케이션의 버전 5는 버전 4가 설치되어 있어야 설치 가능한 경우를 예로 들어 보겠습니다. 이 옵션을 활성화하면 소프트웨어는 먼저 버전 4를 선택한 후에 버전 5를 선택합니다. 이 옵션을 비활성화하면 소프트웨어가 애플리케이션을 업데이트하지 못합니다.

기본적으로 이 옵션은 켜져 있습니다.

5. **취약점** 페이지에서 선택한 업데이트를 설치하면 수정되는 취약점을 선택합니다:

   - **기타 기준과 일치하는 모든 취약점 수정**

     마법사의 **일반 기준** 페이지에 지정된 기준을 충족하는 모든 취약점을 수정합니다. 기본적으로 선택됩니다.

   - **다음 목록의 취약점만 수정**

     목록에서 수동으로 선택하는 취약점만 수정합니다. 이 목록에는 탐지된 모든 취약점이 포함되어 있습니다.

     예를 들어 테스트 환경에서 수정을 확인하거나 중요한 애플리케이션 또는 특정 애플리케이션의 취약점만 수정하려는 등의 경우 특정 취약점을 선택할 수 있습니다.

6. **이름** 페이지에서 만들 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 **설정** 섹션에서 나중에 이 이름을 변경할 수 있습니다.

규칙 생성 마법사의 작업이 완료되면 새 규칙이 생성되어 새 작업 마법사의 **업데이트 설치 규칙을 지정합니다** 필드에 표시됩니다.

Microsoft 애플리케이션의 업데이트를 위한 새 규칙을 생성하려면 다음과 같이 하십시오:

1. 새 작업 마법사의 **설정** 페이지에서 **추가** 버튼을 누릅니다.

   규칙 생성 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

2. **규칙 유형** 페이지에서 **Windows 업데이트 규칙**을 선택합니다.

3. **일반 기준** 페이지에서 다음 설정을 지정합니다:

   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.

     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

   - **다음 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

     이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **다음 MSRC 심각도와 같거나 높은 취약점만 수정**

  소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

  이 옵션을 활성화하면 업데이트는 MSRC(Microsoft Security Response Center)에서 설정한 심각도가 목록에서 선택한 값(**낮음**, **중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

  이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

4. **애플리케이션** 페이지에서 업데이트를 설치할 애플리케이션 및 애플리케이션 버전을 선택합니다. 기본적으로 모든 애플리케이션이 선택되어 있습니다.

5. **업데이트 카테고리** 페이지에서 설치할 업데이트의 카테고리를 선택합니다. 이러한 카테고리는 Microsoft 업데이트 카탈로그의 카테고리와 동일합니다. 기본적으로 모든 카테고리가 선택되어 있습니다.

6. **이름** 페이지에서 만들 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 **설정** 섹션에서 나중에 이 이름을 변경할 수 있습니다.

규칙 생성 마법사의 작업이 완료되면 새 규칙이 생성되어 새 작업 마법사의 **업데이트 설치 규칙을 지정합니다** 필드에 표시됩니다.

타사 애플리케이션의 업데이트를 위한 새 규칙을 생성하려면 다음과 같이 하십시오:

1. 새 작업 마법사의 **설정** 페이지에서 **추가** 버튼을 누릅니다.

   규칙 생성 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

2. **규칙 유형** 페이지에서 **타사 업데이트 규칙**을 선택합니다.

3. **일반 기준** 페이지에서 다음 설정을 지정합니다:

   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.

     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

   - **다음 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

4. **애플리케이션** 페이지에서 업데이트를 설치할 애플리케이션 및 애플리케이션 버전을 선택합니다. 기본적으로 모든 애플리케이션이 선택되어 있습니다.

5. **이름** 페이지에서 만들 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 **설정** 섹션에서 나중에 이 이름을 변경할 수 있습니다.

규칙 생성 마법사의 작업이 완료되면 새 규칙이 생성되어 새 작업 마법사의 **업데이트 설치 규칙을 지정합니다** 필드에 표시됩니다.

애플리케이션 그룹

이 섹션에는 기기에 설치된 애플리케이션 그룹을 관리하는 방법이 설명되어 있습니다.

애플리케이션 카테고리 만들기

Kaspersky Security Center를 사용하면 기기에 설치된 애플리케이션 카테고리를 만들 수 있습니다.

다음 방법 중 하나를 사용하여 애플리케이션 카테고리를 만들 수 있습니다:

- 관리자는 선택한 카테고리에 포함된 실행 파일이 있는 폴더를 지정합니다.
- 관리자는 선택한 카테고리에 포함할 실행 파일이 있는 기기를 지정합니다.
- 관리자는 선택한 카테고리에 애플리케이션을 포함시키는 데 사용할 기준을 설정합니다.

애플리케이션 카테고리가 만들어지면 관리자가 해당 애플리케이션 카테고리의 규칙을 설정할 수 있습니다. 규칙은 지정한 카테고리에 포함된 애플리케이션의 동작을 정의합니다. 예를 들어 카테고리에 포함된 애플리케이션의 시작을 차단 또는 허용합니다.

기기에서 실행되는 애플리케이션 관리

Kaspersky Security Center에서는 허용 목록 모드에서 기기의 애플리케이션 시작을 관리할 수 있습니다. 자세한 설명은 Kaspersky Endpoint Security for Windows 온라인 도움말을 참조하십시오. 허용 목록 모드가 선택된 기기에서는 지정된 카테고리에 포함된 애플리케이션만 시작할 수 있습니다. 관리자는 각 사용자에 대한 기기의 애플리케이션 실행 규칙에 적용된 통계 분석 결과를 볼 수 있습니다.

기기에 설치된 소프트웨어 인벤토리

Kaspersky Security Center를 통해 Windows와 Linux 운영 체제를 사용하는 기기에서 소프트웨어 인벤토리를 수행할 수 있습니다. 네트워크 에이전트는 기기에 설치된 애플리케이션 전체의 정보를 수집합니다. 인벤토리 중에 수집된 정보는 **자산 관리(소프트웨어)** 폴더의 작업 영역에 표시됩니다. 관리자는 애플리케이션의 버전과 제조업체 등 애플리케이션에 대한 상세 정보를 볼 수 있습니다.

단일 기기에서 수신하는 실행 파일의 수는 150,000개를 초과할 수 없습니다. 이 제한에 도달하면 Kaspersky Security Center는 새 파일을 수신할 수 없습니다.

유료 애플리케이션 관리

Kaspersky Security Center에서 유료 애플리케이션 그룹을 만들 수 있습니다. 유료 애플리케이션 그룹에는 관리자가 지정한 기준에 부합하는 애플리케이션이 들어 있습니다. 관리자는 유료 애플리케이션 그룹의 다음 기준을 지정할 수 있습니다:

- 애플리케이션 이름
- 애플리케이션 버전
- 제조업체
- 애플리케이션 태그

하나 이상의 기준을 충족하는 애플리케이션이 그룹에 자동으로 포함됩니다. 유료 애플리케이션 그룹을 만들려면 해당 그룹에 포함된 애플리케이션에 최소 하나 이상의 기준을 설정해야 합니다.

각 유료 애플리케이션 그룹에는 고유의 라이센스 키가 있습니다. 유료 애플리케이션 그룹의 라이센스 키는 해당 그룹에 포함된 애플리케이션의 최대 허용 설치 횟수를 정의합니다. 라이센스 키에 설정된 설치 제한 횟수를 초과하면 정보 이벤트가 중앙 관리 서버에 로그온됩니다. 관리자는 라이센스 키의 만료 날짜를 지정할 수 있습니다. 이 날짜가 다가오면 정보 이벤트가 중앙 관리 서버에 로그온됩니다.

실행 파일에 대한 정보 보기

Kaspersky Security Center는 운영 체제가 기기에 설치된 이후 기기에서 실행된 실행 파일의 모든 정보를 수집합니다. 실행 파일에 대한 정보는 **실행 파일** 폴더의 작업 영역에 있는 메인 애플리케이션 창에 표시됩니다.

애플리케이션 제어로 실행 파일 관리

애플리케이션 제어 구성 요소를 사용하여 사용자 기기에서 실행 파일의 시작을 허용하거나 차단할 수 있습니다. 애플리케이션 제어 구성 요소는 Windows 기반 및 Linux 기반 운영 체제를 지원합니다.

Linux 기반 운영 체제는 Kaspersky Endpoint Security 11.2 for Linux부터 애플리케이션 제어 구성 요소를 사용할 수 있습니다. 또한 이 구성 요소는 Kaspersky Embedded Systems Security for Windows 3.0 이상에서도 사용할 수 있습니다.

필수 구성 요소

- 조직에 Kaspersky Security Center가 배포되어 있습니다.
- Kaspersky Endpoint Security for Windows 또는 Kaspersky Endpoint Security for Linux의 정책이 생성되고 활성화됩니다.
- Kaspersky Embedded Systems Security for Windows 또는 Kaspersky Embedded Systems Security for Linux 정책이 생성되어 활성 상태입니다.

단계

애플리케이션 제어 사용 시나리오는 다음과 같은 단계로 진행됩니다.

1 클라이언트 기기에서 실행 파일 목록 구성 및 보기

이 단계는 관리 중인 기기에서 찾을 수 있는 실행 파일을 파악하는 데 도움이 됩니다. 실행 파일 목록을 보고 허용 및 금지되는 실행 파일 목록과 비교합니다. 실행 파일 사용에 관한 제한은 조직의 정보 보안 정책과 관련될 수 있습니다.

방법 지침:

- 관리 콘솔: 실행 파일 인벤토리
- Kaspersky Security Center 웹 콘솔: 클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기

2 조직에서 사용되는 실행 파일 카테고리 생성

관리 중인 기기에 저장된 실행 파일 목록을 분석합니다. 분석 결과를 바탕으로 실행 파일에 대한 카테고리를 생성합니다. 조직에서 사용하는 표준 실행 파일 집합을 포괄하는 "업무용 애플리케이션" 카테고리를 만드는 것이 좋습니다. 다양한 보안 그룹이 업무에 자체 실행 파일 집합을 사용한다면 보안 그룹마다 별도의 카테고리를 만들 수 있습니다.

방법 지침:

- 관리 콘솔: 콘텐츠가 수동으로 추가된 애플리케이션 카테고리 생성, 선택한 기기의 실행 파일을 포함한 애플리케이션 카테고리 생성, 특정 폴더의 실행 파일을 포함한 애플리케이션 카테고리 생성.
- Kaspersky Security Center 웹 콘솔: 콘텐츠가 수동으로 추가된 애플리케이션 카테고리 생성, 선택한 기기의 실행 파일을 포함한 애플리케이션 카테고리 생성, 특정 폴더의 실행 파일을 포함한 애플리케이션 카테고리 생성.

3 Kaspersky Endpoint Security 정책에서 애플리케이션 제어 구성

이전 단계에서 만든 카테고리를 사용하여 Kaspersky Endpoint Security 정책의 애플리케이션 제어 구성 요소를 구성합니다.

방법 지침:

- 관리 콘솔: 클라이언트 기기의 애플리케이션 시작 관리 구성
- Kaspersky Security Center 웹 콘솔: Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성

4 Kaspersky Embedded Systems Security 애플리케이션 정책에서 애플리케이션 제어 구성

생성한 카테고리를 사용하여 Kaspersky Embedded Systems Security for Windows 정책에서 애플리케이션 제어 구성 요소를 구성합니다. 애플리케이션 제어 구성 요소에 관한 자세한 내용은 Kaspersky Embedded Systems Security for Windows 도움말 이나 Kaspersky Embedded Systems Security for Linux 도움말 을 참조하십시오.

사용하는 규칙의 수가 많으면 정책을 불러올 때 오류가 발생할 수 있습니다. 다음 명령을 사용하여 최대 요청 크기를 바이트 단위로 늘릴 수 있습니다.

- JSON 요청:

```
klscflag -fset -pv ".core/.independent" -s KLLIM -n
LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
```

- HTTP 요청:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  여기서 `<max_request_size>`는 요청의 최대 바이트 크기입니다(예: `200000000`).

5. **테스트 모드에서 애플리케이션 제어 구성 요소 사용 설정**

   애플리케이션 제어 규칙으로 사용자의 업무에 필요한 실행 파일이 차단되지 않도록 하려면 애플리케이션 제어 규칙에 대한 테스트를 활성화하고 새 규칙 생성 이후 작업을 분석해 보는 것이 좋습니다. 테스트가 활성화되면 Kaspersky Endpoint Security for Windows나 Kaspersky Embedded Systems Security는 애플리케이션 제어 규칙으로 시작이 금지된 실행 파일을 차단하는 대신 중앙 관리 서버에 시작에 관한 알림을 전송합니다.

   애플리케이션 제어 규칙을 테스트할 때 다음 작업을 수행하는 것이 좋습니다.

   - 테스트 기간을 결정합니다. 테스트 기간은 며칠부터 두 달까지 다양합니다.
   - 애플리케이션 제어 동작의 테스트 결과 이벤트를 살펴봅니다.

   Kaspersky Security Center 웹 콘솔 사용 지침: Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성 요소 구성. 이 지침에 따라 구성 프로세스에서 **테스트 모드** 옵션을 활성화합니다.

6. **애플리케이션 제어 구성 요소의 카테고리 설정 변경**

   필요한 경우 애플리케이션 제어 설정을 변경합니다. 테스트 결과를 바탕으로 애플리케이션 제어 구성 요소 이벤트와 관련된 실행 파일을 컨텐츠가 수동으로 추가된 카테고리에 추가할 수 있습니다.

   방법 지침:

   - 관리 콘솔: 애플리케이션 카테고리에 이벤트 관련 실행 파일 추가
   - Kaspersky Security Center 웹 콘솔: 애플리케이션 카테고리에 이벤트 관련 실행 파일 추가

7. **동작 모드인 애플리케이션 제어 규칙 적용**

   애플리케이션 규칙을 테스트하고 카테고리의 구성이 완료된 후에는 동작 모드인 애플리케이션 제어 규칙을 적용할 수 있습니다.

   Kaspersky Security Center 웹 콘솔 사용 지침: Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성 요소 구성. 이 지침에 따라 구성 프로세스에서 **테스트 모드** 옵션을 비활성화합니다.

8. **애플리케이션 제어 구성 확인**

   다음을 수행했는지 확인합니다.

   - 실행 파일에 대한 카테고리 생성.
   - 카테고리로 애플리케이션 제어 구성.
   - 동작 모드인 애플리케이션 제어 규칙 적용.

결과

시나리오가 완료되면 관리 중인 기기에서 실행 파일 시작이 제어됩니다. 사용자는 조직에서 허용한 사용 파일만 실행할 수 있으며 조직에서 금지한 실행 파일은 실행할 수 없습니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기

다음 방법의 하나를 사용하여 클라이언트 기기에 저장된 실행 파일 목록을 얻을 수 있습니다.

- Kaspersky Endpoint Security 정책에서 애플리케이션 시작에 관한 알림 활성화.
- 인벤토리 작업 생성.

Kaspersky Endpoint Security 정책에서 애플리케이션 시작에 관한 알림 활성화

애플리케이션 시작에 대한 알림을 활성화하려면 다음을 수행합니다.

1. Kaspersky Endpoint Security 정책 설정을 열고 **일반 설정 → 리포트 및 저장소**로 갑니다.
2. **중앙 관리 서버로의 데이터 전송** 설정 그룹에서 **시작된 애플리케이션 정보** 확인란을 선택하고 변경 사항을 저장합니다.

   사용자가 실행 파일을 시작하려고 하면 해당 파일에 대한 정보가 클라이언트 기기의 실행 파일 목록에 추가됩니다. Kaspersky Endpoint Security는 이 정보를 네트워크 에이전트로 전송하고, 네트워크 에이전트는 이를 중앙 관리 서버로 전송합니다.

인벤토리 작업 생성

실행 파일 인벤토리 기능은 다음 애플리케이션에서 사용할 수 있습니다:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 버전 11.2 이상
- Kaspersky Security for Virtualization 4.0 Light Agent 및 이후 버전

설치된 애플리케이션에 대한 정보를 얻으면서 데이터베이스의 부하를 줄일 수 있습니다. 공간을 절약하려면 표준 소프트웨어 집합이 설치된 참조 기기에서 인벤토리 작업을 실행하는 것이 좋습니다. 권장 수는 1~3개입니다.

다음 데이터베이스를 사용한다면 인벤토리 작업을 실행하지 않는 것이 좋습니다: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB(모든 버전).

클라이언트 기기에 있는 실행 파일에 대한 인벤토리 작업을 만들려면:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **작업** 폴더의 작업 영역에서 **새 작업**버튼을 누릅니다.
   새 작업 마법사가 시작됩니다.
3. 마법사의 **작업 유형 선택** 창에서 작업 유형으로 **Kaspersky Endpoint Security**를 선택한 후 작업 하위 유형으로 **인벤토리**를 선택하고 **다음**을 누릅니다.
4. 마법사의 나머지 지침을 따릅니다.

   새 작업 마법사를 종료한 후 **인벤토리** 작업이 생성 및 구성됩니다. 원한다면 생성된 작업에 대한 설정을 변경할 수 있습니다. 그러면 작업 목록에 새로 생성된 작업이 나타납니다. 원한다면 생성된 작업에 대한 설정을 변경할 수 있습니다.

인벤토리 작업에 대한 자세한 설명은 다음 도움말을 참조하십시오:

- Kaspersky Endpoint Security for Windows 도움말
- Kaspersky Endpoint Security for Linux 도움말
- Kaspersky Security for Virtualization Light Agent

인벤토리 작업을 수행한 후 관리 중인 기기에 저장된 실행 파일 목록이 형성되고 이 목록을 확인할 수 있습니다.

인벤토리 중에 다음 형식의 실행 파일을 탐지할 수 있습니다(인벤토리 작업 속성에서 선택한 옵션에 따라 다름): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, HTML.

관리 중인 기기에 저장된 실행 파일 목록 보기

클라이언트 기기에 저장된 실행 파일 목록을 보려면 다음 단계를 따릅니다.

콘솔 트리에서 **고급** → **애플리케이션 관리** → **실행 파일**로 갑니다.

필요한 경우 관리 중인 기기에서 관리 콘솔이 설치된 기기로 실행 파일을 전송할 수 있습니다.

실행 파일을 보내려면:

1. 콘솔 트리에서 **고급** → **애플리케이션 관리** → **실행 파일**로 갑니다.
2. 관리 콘솔이 설치된 기기로 전송할 실행 파일의 링크를 클릭합니다.

3. 창이 열리면 **기기** 섹션으로 가서 실행 파일을 보내고자 하는 관리 중인 기기의 확인란을 선택합니다.

실행 파일을 보내기 전에 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택하여 관리 중인 기기가 중앙 관리 서버에 직접 연결되도록 합니다.

4. **보내기** 버튼을 클릭하고 대상 폴더를 선택한 다음 **확인**을 클릭합니다.

선택한 실행 파일이 관리 콘솔이 설치된 기기로 전송할 수 있도록 다운로드됩니다.

Kaspersky Endpoint Security for Windows 정책용 애플리케이션 카테고리 생성

Kaspersky Endpoint Security for Windows 정책의 **속성** 창과 **애플리케이션 카테고리** 폴더에서 Kaspersky Endpoint Security for Windows 정책용 애플리케이션 카테고리를 생성할 수 있습니다.

*애플리케이션 카테고리 폴더에서 Kaspersky Endpoint Security 정책용 **애플리케이션 카테고리**를 생성하려면 다음과 같이 하십시오:*

1. 콘솔 트리에서 **고급** → **애플리케이션 관리** → **애플리케이션 카테고리**를 선택합니다.
2. **애플리케이션 카테고리** 폴더의 작업 영역에서 **새 카테고리** 버튼을 누릅니다.
   새 카테고리 마법사가 시작됩니다.
3. **카테고리 유형** 페이지에서 사용자 카테고리 유형을 선택합니다:
   - **수동으로 추가된 컨텐츠가 있는 카테고리**. 생성 중인 카테고리에 실행 파일을 할당하는 데 사용할 기준을 지정합니다.
   - **자동으로 추가된 컨텐츠가 있는 카테고리**. 생성된 카테고리에 실행 파일을 자동으로 할당할 원본 폴더를 지정합니다.

     자동으로 콘텐츠가 추가되는 카테고리를 생성하는 경우 애플리케이션은 다음 파일 형식에 대한 인벤토리 작업을 수행합니다: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX 및 SCR.

   - **선택한 기기의 실행 파일이 포함된 카테고리**. 카테고리에 자동으로 할당되는 실행 파일을 포함하는 기기를 지정합니다.
4. 마법사의 지침을 따릅니다.

마법사가 완료되면 사용자 지정 애플리케이션 카테고리가 생성됩니다. **애플리케이션 카테고리** 폴더의 작업 영역에서 카테고리 목록을 사용하여 새로 만든 카테고리를 볼 수 있습니다.

애플리케이션 카테고리를 KLC 파일로 내보내려면 카테고리 이름을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 **내보내기**를 선택한 후, 열리는 창에서 파일 이름을 지정하고 **저장**을 클릭합니다.

정책 폴더에서 애플리케이션 카테고리를 생성할 수도 있습니다.

*Kaspersky Endpoint Security for Windows 정책의 **속성** 창에서 애플리케이션 카테고리를 생성하려면 다음과 같이 하십시오:*

1. 콘솔 트리에서 **정책** 폴더를 선택합니다.
2. **정책** 폴더의 작업 영역에서 카테고리를 생성할 Kaspersky Endpoint Security 정책을 선택합니다.
3. 마우스 오른쪽 버튼을 누르고 **속성**를 선택합니다.
4. **속성** 창이 열리면 왼쪽 **섹션** 창에서 **보안 제어 → 애플리케이션 제어**를 선택합니다.
5. **애플리케이션 제어** 섹션의 **제어 모드** 및 **작업** 드롭다운 목록에서 허용 목록 또는 거부 목록을 선택한 다음 **추가** 버튼을 누릅니다.
   카테고리 목록이 포함된 **애플리케이션 제어 규칙** 창이 열립니다.
6. **새로 만들기** 버튼을 누릅니다.
7. 새 카테고리의 이름을 입력하고 **확인**을 누릅니다.
   새 카테고리 마법사가 시작됩니다.
8. **카테고리 유형** 페이지에서 사용자 카테고리 유형을 선택합니다:
   - **수동으로 추가된 컨텐츠가 있는 카테고리**. 생성 중인 카테고리에 실행 파일을 할당하는 데 사용할 기준을 지정합니다.
   - **자동으로 추가된 컨텐츠가 있는 카테고리**. 생성된 카테고리에 실행 파일을 자동으로 할당할 원본 폴더를 지정합니다.

     자동으로 콘텐츠가 추가되는 카테고리를 생성하는 경우 애플리케이션은 다음 파일 형식에 대한 인벤토리 작업을 수행합니다: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX 및 SCR.

   - **선택한 기기의 실행 파일이 포함된 카테고리**. 카테고리에 자동으로 할당되는 실행 파일을 포함하는 기기를 지정합니다.
9. 마법사의 지침을 따릅니다.

마법사가 완료되면 사용자 지정 애플리케이션 카테고리가 생성됩니다. 카테고리 목록에서 새로 만든 카테고리를 확인할 수 있습니다.

애플리케이션 카테고리는 Kaspersky Endpoint Security for Windows에 포함된 애플리케이션 제어 구성 요소에 사용됩니다. 관리자는 애플리케이션 제어를 통해 클라이언트 기기의 애플리케이션 시작에 대한 제한을 적용할 수 있습니다. 예를 들어 지정한 카테고리의 애플리케이션 시작을 제한할 수 있습니다.

수동으로 추가된 컨텐츠가 있는 애플리케이션 카테고리 만들기

조직에서 시작을 허용 또는 차단할 실행 파일의 템플릿으로 기준 집합을 지정할 수 있습니다. 기준에 해당하는 실행 파일을 바탕으로 애플리케이션 카테고리를 만들고 애플리케이션 제어 구성 요소 구성에 사용할 수 있습니다.

수동으로 추가된 컨텐츠가 있는 애플리케이션 카테고리를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리의**고급** → **애플리케이션 관리** 폴더에서 **애플리케이션 카테고리** 하위 폴더를 선택합니다.
2. **새 카테고리** 버튼을 누릅니다.
   새 카테고리 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. **카테고리 유형** 마법사 페이지에서 사용자 카테고리 유형으로 **수동으로 추가된 콘텐츠가 있는 카테고리**를 선택합니다.
4. **애플리케이션 카테고리 이름 입력** 마법사 페이지에서 새 애플리케이션 카테고리 이름을 입력합니다.
5. **카테고리의 애플리케이션을 포함하는 조건 구성** 페이지에서 **추가** 버튼을 누릅니다.
6. 드롭다운 목록에서 관련 설정을 지정합니다:

   - **실행 파일 목록에서**

     이 옵션을 선택하면 클라이언트 기기의 실행 파일 목록을 사용하여 실행 파일을 선택하고 애플리케이션을 카테고리에 추가할 수 있습니다.

   - **시작 파일 속성**

     이 옵션을 선택하면 사용자 애플리케이션 카테고리에 추가할 실행 파일에 대한 상세한 데이터를 지정할 수 있습니다.

   - **폴더 내 파일의 메타데이터**

     실행 파일이 포함된 클라이언트 기기의 폴더를 지정합니다. 그러면 지정된 폴더에 포함된 실행 파일의 메타데이터가 중앙 관리 서버로 전송됩니다. 동일한 메타데이터가 포함된 실행 파일이 사용자 애플리케이션 카테고리에 추가됩니다.

   - **폴더 내 파일의 체크섬**

     이 옵션을 선택하면 클라이언트 기기에서 폴더를 선택하거나 만들 수 있습니다. 그러면 지정된 폴더에 있는 파일의 MD5 해시가 중앙 관리 서버로 전송됩니다. 지정된 폴더의 파일과 동일한 해시를 가진 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

   - **폴더의 파일에 대한 인증서**

     이 옵션을 선택하면 클라이언트 기기에서 인증서로 서명된 실행 파일을 포함하는 폴더를 지정할 수 있습니다. 실행 파일의 인증서는 읽혀진 다음 카테고리의 조건에 추가됩니다. 지정된 인증서에 따라 서명된 실행 파일은 사용자 카테고리에 추가됩니다.

   - **MSI 인스톨러 파일 메타데이터**

     이 옵션을 선택하면 사용자 카테고리에 애플리케이션을 추가하는 조건으로 MSI 설치 파일을 지정할 수 있습니다. 그러면 애플리케이션 설치 파일 메타데이터가 중앙 관리 서버로 전송됩니다. 지정된 MSI 설치 파일과 동일한 설치 파일 메타데이터를 가진 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

- **애플리케이션 MSI 인스톨러의 파일 체크섬**

  이 옵션을 선택하면 사용자 카테고리에 애플리케이션을 추가하는 조건으로 MSI 설치 파일을 지정할 수 있습니다. 그러면 애플리케이션 인스톨러의 해시가 중앙 관리 서버로 전송됩니다. MSI 설치 파일의 해시가 지정한 해시와 동일한 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

- **KL 카테고리에서**

  이 옵션을 선택하면 사용자 카테고리에 애플리케이션을 추가하는 조건으로 Kaspersky 애플리케이션 카테고리를 지정할 수 있습니다. 그러면 지정된 Kaspersky 카테고리의 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

- **애플리케이션 경로 지정(마스크 지원)**

  이 옵션을 선택하면 사용자 애플리케이션 카테고리에 추가할 실행 파일이 포함된 파일 경로 또는 폴더 경로를 클라이언트 기기에서 지정할 수 있습니다. *C:\path_to_exe**와 같은 정규식을 사용할 수 있습니다(예: *C:\Program Files\Internet Explorer**).

- **저장소에서 인증서 선택**

  이 옵션을 선택하면 저장소에서 인증서를 지정할 수 있습니다. 카테고리 조건은 지정된 인증서로 서명된 실행 파일에만 적용됩니다.

  인벤토리 작업을 생성 및 시작하거나 Kaspersky Endpoint Security 정책의 **시작된 애플리케이션 정보 체크박스를 선택하면** 저장소에 인증서가 추가됩니다. 두 작업을 모두 수행할 수 있습니다.

- **드라이브 유형**

  이 옵션을 선택하면 애플리케이션이 실행되는 미디어(모든 드라이브 또는 이동식 드라이브) 유형을 지정할 수 있습니다. 선택한 드라이브 유형에서 실행된 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

7. **애플리케이션 카테고리 생성** 페이지에서 서 **마침** 버튼을 클릭합니다.

Kaspersky Security Center는 디지털 서명된 파일의 메타데이터만 처리합니다. 디지털 시그니처가 없는 파일의 메타데이터를 기준으로 카테고리를 만들 수는 없습니다.

마법사가 완료되면 수동으로 추가한 컨텐츠가 있는 사용자 애플리케이션 카테고리가 만들어집니다. **애플리케이션 카테고리** 폴더의 작업 영역에서 카테고리 목록을 사용하여 새로 만든 카테고리를 볼 수 있습니다.

애플리케이션 카테고리를 KLC 파일로 내보내려면 카테고리 이름을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 **내보내기**를 선택한 후, 열리는 창에서 파일 이름을 지정하고 **저장**을 클릭합니다.

선택한 장치의 실행 파일을 포함하는 애플리케이션 카테고리 만들기

선택한 기기의 실행 파일을 허용하거나 차단할 실행 파일의 템플릿으로 사용할 수 있습니다. 선택한 기기의 실행 파일을 기반으로 애플리케이션 카테고리를 만들고 애플리케이션 제어 구성 요소 구성에서 사용할 수 있습니다.

기기에서 실행 파일 목록을 가져오려면 다음을 따릅니다.

1. Kaspersky Endpoint Security for Windows 또는 Kaspersky Endpoint Security for Linux의 정책이 생성되고 활성화되도록 해야 합니다. 정책에서 애플리케이션 제어 구성 요소를 활성화합니다.

2. 클라이언트 기기에 저장된 실행 파일 목록을 가져옵니다.

선택한 기기의 실행 파일을 포함하는 애플리케이션 카테고리를 만들려면 다음 단계를 따릅니다.

1. 콘솔 트리의**고급** → **애플리케이션 관리** 폴더에서 **애플리케이션 카테고리** 하위 폴더를 선택합니다.

2. **새 카테고리** 버튼을 누릅니다.

   새 카테고리 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

3. **카테고리 유형** 마법사 페이지에서 **선택한 기기의 실행 파일을 포함하는 카테고리**를 사용자 카테고리 유형으로 선택합니다.

4. **애플리케이션 카테고리 이름 입력** 마법사 페이지에서 새 애플리케이션 카테고리 이름을 입력합니다.

5. **설정** 마법사 페이지에서 **추가** 버튼을 클릭합니다.

6. 기기 또는 애플리케이션 카테고리를 만드는 데 사용할 실행 파일의 기기를 선택합니다.

7. 다음 설정을 지정합니다:

   - **해시 값 계산 알고리즘**

     네트워크의 기기에 설치된 보안 제품 버전에 따라 이 카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산용 알고리즘을 선택해야 합니다. 해시 함수로 계산된 해시 값에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다.

     SHA256은 암호화 해시 함수입니다. 해당 알고리즘에서 발견된 취약점이 없으므로 최근까지 가장 믿을 수 있는 암호화 함수로 간주되고 있습니다. SHA256 계산은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원됩니다. MD5 해시 계산 기능은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전의 모든 버전에서 지원됩니다.

     카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산의 옵션 선택합니다:

     - 네트워크에 설치된 보안 애플리케이션의 모든 인스턴스가 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이상일 시, **SHA256** 확인란을 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전인 경우 실행 파일의 SHA256 해시 기준에 따라 만든 카테고리를 추가하지 않는 것이 좋습니다. 이러한 카테고리를 추가하면 보안 제품 작동 시에 오류가 발생할 수 있습니다. 이 경우 카테고리의 파일에 대해 MD5 암호화 해시 함수를 사용할 수 있습니다.

     - Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전이 네트워크에 설치되었다면 **MD5 해시**를 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서는 실행 파일의 MD5 체크섬 기준을 기반으로 만든 카테고리를 추가할 수 없습니다. 이 경우 카테고리의 파일에 대해 SHA256암호화 해시 함수를 사용할 수 있습니다.

     네트워크의 다른 기기가 Kaspersky Endpoint Security 10의 이전 버전과 이후 버전을 모두 사용한다면 **SHA256** 확인란과 **MD5 해시** 확인란을 모두 선택합니다.

     이 카테고리에 있는 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원) 확인란은 기본적으로 선택되어 있습니다.

     이 카테고리에 있는 파일에 대해 MD5 계산 (Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전에서 지원) 확인란은 기본적으로 선택되어 있지 않습니다.

- **중앙 관리 서버 저장소와 데이터 동기화**

  중앙 관리 서버에서 지정된 폴더의 변경 사항을 주기적으로 확인하도록 하려면 이 옵션을 선택합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

  이 옵션을 활성화할 경우 지정된 폴더의 변경 사항을 확인할 기간(시간 단위)을 지정합니다. 기본적으로 검사 간격은 24시간입니다.

8. **필터** 마법사 페이지에서 다음 설정을 지정합니다:

   - **파일 유형**

     이 섹션에서는 애플리케이션 카테고리를 만드는 데 사용되는 파일 형식을 지정할 수 있습니다.

     모든 파일. 카테고리를 만들 때 모든 파일을 고려합니다. 기본적으로 이 옵션은 선택되어 있습니다.

     애플리케이션 카테고리 이외의 파일만. 카테고리를 만들 때 애플리케이션 카테고리 외부의 파일만 고려합니다.

   - **폴더**

     이 섹션에서는 선택된 기기의 폴더 중 애플리케이션 카테고리를 만드는 데 사용할 파일이 포함되어 있는 폴더를 지정할 수 있습니다.

     모든 폴더. 카테고리 생성 시 모든 폴더를 고려합니다. 기본적으로 이 옵션은 선택되어 있습니다.

     지정한 폴더. 카테고리 생성 시 지정된 폴더만 고려합니다. 이 옵션을 선택하면 폴더 경로를 지정해야 합니다.

9. **애플리케이션 카테고리 생성** 페이지에서 서 **마침** 버튼을 클릭합니다.

   마법사가 완료되면 사용자 애플리케이션 카테고리가 만들어집니다. **애플리케이션 카테고리** 폴더의 작업 영역에서 카테고리 목록을 사용하여 새로 만든 카테고리를 볼 수 있습니다.

애플리케이션 카테고리를 KLC 파일로 내보내려면 카테고리 이름을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 **내보내기**를 선택한 후, 열리는 창에서 파일 이름을 지정하고 **저장**을 클릭합니다.

특정 폴더의 실행 파일을 포함하는 애플리케이션 카테고리 만들기

선택한 폴더의 실행 파일을 조직에서 허용 또는 차단할 실행 파일의 표준으로 사용할 수 있습니다. 선택한 폴더의 실행 파일을 기준으로 애플리케이션 제어 구성 요소 구성에서 애플리케이션 카테고리를 만들고 사용할 수 있습니다.

특정 폴더에서 실행 파일을 포함하는 애플리케이션 카테고리를 만들려면:

1. 콘솔 트리의**고급** → **애플리케이션 관리** 폴더에서 **애플리케이션 카테고리** 하위 폴더를 선택합니다.

2. **새 카테고리** 버튼을 누릅니다.

   새 카테고리 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

3. **카테고리 유형** 마법사 페이지에서 **특정 폴더의 실행 파일을 포함하는 카테고리**를 사용자 카테고리 유형으로 선택합니다.

4. **애플리케이션 카테고리 이름 입력** 마법사 페이지에서 새 애플리케이션 카테고리 이름을 입력합니다.

5. **저장소 폴더** 마법사 페이지에서 **찾기** 버튼을 클릭합니다.

6. 실행 파일이 애플리케이션 카테고리 생성에 사용되는 폴더를 지정합니다.

7. 다음 설정을 정의합니다:

- **이 카테고리에 동적 링크 라이브러리(DLL) 포함**

  애플리케이션 카테고리에 동적-링크 라이브러리(DLL 형식의 파일)이 포함되고 시스템에서 실행 중인 이러한 라이브러리의 동작을 애플리케이션 제어 구성 요소가 기록합니다. 카테고리에 DLL 파일이 포함되면 Kaspersky Security Center의 성능이 저하될 수 있습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **이 카테고리에 스크립트 데이터 포함**

  애플리케이션 카테고리에 스크립트 데이터가 포함되며 웹 위협 보호 구성 요소에서 스크립트를 차단하지 않습니다. 카테고리에 스크립트 데이터가 포함되면 Kaspersky Security Center의 성능이 저하될 수 있습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **해시 값 계산 알고리즘**: **이 카테고리의 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원)** / **이 카테고리의 파일에 대해 MD5 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 서비스 팩 2 이전 버전에서 지원)**

  네트워크의 기기에 설치된 보안 제품 버전에 따라 이 카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산용 알고리즘을 선택해야 합니다. 해시 함수로 계산된 해시 값에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다.

  SHA256은 암호화 해시 함수입니다. 해당 알고리즘에서 발견된 취약점이 없으므로 최근까지 가장 믿을 수 있는 암호화 함수로 간주되고 있습니다. SHA256 계산은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원됩니다. MD5 해시 계산 기능은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전의 모든 버전에서 지원됩니다.

  카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산의 옵션 선택합니다:

  - 네트워크에 설치된 보안 애플리케이션의 모든 인스턴스가 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이상일 시, **SHA256** 확인란을 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전인 경우 실행 파일의 SHA256 해시 기준에 따라 만든 카테고리를 추가하지 않는 것이 좋습니다. 이러한 카테고리를 추가하면 보안 제품 작동 시에 오류가 발생할 수 있습니다. 이 경우 카테고리의 파일에 대해 MD5 암호화 해시 함수를 사용할 수 있습니다.

  - Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전이 네트워크에 설치되었다면 **MD5 해시**를 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서는 실행 파일의 MD5 체크섬 기준을 기반으로 만든 카테고리를 추가할 수 없습니다. 이 경우 카테고리의 파일에 대해 SHA256암호화 해시 함수를 사용할 수 있습니다.

  네트워크의 다른 기기가 Kaspersky Endpoint Security 10의 이전 버전과 이후 버전을 모두 사용한다면 **SHA256** 확인란과 **MD5 해시** 확인란을 모두 선택합니다.

  이 카테고리에 있는 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원) 확인란은 기본적으로 선택되어 있습니다.

  이 카테고리에 있는 파일에 대해 MD5 계산 (Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전에서 지원) 확인란은 기본적으로 선택되어 있지 않습니다.

- **폴더 내 변경 사항을 강제로 검사**

  이 옵션을 사용하면 애플리케이션이 정기적으로 폴더에 카테고리 컨텐츠 추가에 대한 변경 사항이 있는지 확인합니다. 확인란 옆에 있는 항목에서 확인 주기(시간)를 지정할 수 있습니다. 기본적으로 강제로 확인하는 시간 간격은 24시간입니다.

  이 옵션이 비활성화되어 있으면 애플리케이션이 해당 폴더에 대해 모든 확인을 강제로 시작하지 않습니다. 파일이 수정되거나 추가되거나 삭제되었다면 서버는 파일로의 접근을 시도합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

8. **애플리케이션 카테고리 생성** 페이지에서 서 **마침** 버튼을 클릭합니다.

   마법사가 완료되면 사용자 애플리케이션 카테고리가 만들어집니다. **애플리케이션 카테고리** 폴더의 작업 영역에서 카테고리 목록을 사용하여 새로 만든 카테고리를 볼 수 있습니다.

애플리케이션 카테고리를 KLC 파일로 내보내려면 카테고리 이름을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 **내보내기**를 선택한 후, 열리는 창에서 파일 이름을 지정하고 **저장**을 클릭합니다.

애플리케이션 카테고리에 이벤트 관련 실행 파일 추가

테스트 모드에서 **애플리케이션 시작이 금지됨** 및 **테스트 모드에서 애플리케이션 시작이 금지됨** 이벤트와 관련된 실행 파일을 수동으로 추가된 컨텐츠가 있는 기존 애플리케이션 카테고리나 새 애플리케이션 카테고리에 추가할 수 있습니다.

애플리케이션 제어 이벤트와 관련된 실행 파일을 애플리케이션 카테고리에 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **이벤트** 탭에서 필요한 이벤트를 선택합니다.
4. 선택한 이벤트 중 하나의 마우스 오른쪽 메뉴에서 **카테고리에 추가**를 선택합니다.
5. **이벤트와 관련된 실행 파일에 대한 조치** 창이 열리면 관련된 설정을 지정합니다:

   다음 중 하나를 선택합니다:

   - **새 애플리케이션 카테고리에 추가**

     새 애플리케이션 카테고리를 생성하려면 이 옵션을 선택합니다.

     확인 버튼을 눌러 사용자 카테고리 만들기 마법사를 시작합니다. 마법사가 완료되면 지정한 설정을 가진 카테고리가 생성됩니다.

     기본적으로 이 옵션은 선택되어 있지 않습니다.

   - **기존 애플리케이션 카테고리에 추가**

     기존 애플리케이션 카테고리에 규칙을 추가해야 한다면 이 옵션을 선택합니다. 애플리케이션 카테고리 목록에서 관련 카테고리를 선택합니다.

     이 옵션은 기본적으로 선택되어 있습니다.

규칙 유형 섹션에서 다음 설정 중 하나를 선택하십시오:

- **카테고리에 추가**

  애플리케이션 카테고리의 조건에 규칙을 추가해야 하는 경우 이 옵션을 선택합니다.

  이 옵션은 기본적으로 선택되어 있습니다.

- **제외에 추가하기 위한 규칙**

  애플리케이션 카테고리의 제외에 규칙을 추가하려면 이 옵션을 선택합니다.

파일 정보 유형 섹션에서 다음 설정 중 하나를 선택하십시오:

- **인증서 세부 정보(또는 인증서가 없는 파일에 대한 SHA256 해시 값)**

  파일은 인증서로 서명될 수 있습니다. 여러 파일이 동일한 인증서로 서명될 수 있습니다. 예를 들어 동일한 애플리케이션의 서로 다른 버전이 동일한 인증서로 서명되거나 동일한 제조사의 여러 애플리케이션이 동일한 인증서로 서명될 수 있습니다. 인증서를 선택할 때 여러 버전의 애플리케이션이나 동일한 제조사의 여러 애플리케이션이 카테고리에 포함될 수 있습니다.

  각 파일에는 고유한 SHA256 해시 함수가 있습니다. SHA256 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

  카테고리 규칙에 실행 파일의 인증서 세부 정보(또는 인증서가 없는 파일의 경우 SHA256 해시 함수)를 추가하려면 이 옵션을 선택합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **인증서 세부 정보(인증서가 없는 파일은 건너뛰게 됩니다)**

  파일은 인증서로 서명될 수 있습니다. 여러 파일이 동일한 인증서로 서명될 수 있습니다. 예를 들어 동일한 애플리케이션의 서로 다른 버전이 동일한 인증서로 서명되거나 동일한 제조사의 여러 애플리케이션이 동일한 인증서로 서명될 수 있습니다. 인증서를 선택할 때 여러 버전의 애플리케이션이나 동일한 제조사의 여러 애플리케이션이 카테고리에 포함될 수 있습니다.

  실행 파일의 인증서 세부 사항을 카테고리 규칙에 추가하려면 이 옵션을 선택합니다. 실행 파일에 인증서가 없으면 이 파일은 건너 뜁니다. 이 파일에 대한 정보는 카테고리에 추가되지 않습니다.

- **SHA256만(해시가 없는 파일은 건너뜀)**

  각 파일에는 고유한 SHA256 해시 함수가 있습니다. SHA256 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

  실행 파일의 SHA256 해시 함수의 세부 사항만 추가하려면 이 옵션을 선택합니다.

- **MD5만(Kaspersky Endpoint Security 10 Service Pack 1 for Windows 이전의 버전에서 지원)**

  각 파일에는 고유한 MD5 해시 함수가 있습니다. MD5 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

  실행 파일의 MD5 해시 함수의 세부 사항만 추가하려면 이 옵션을 선택합니다. MD5 해시 계산 기능은 Kaspersky Endpoint Security 10 Service Pack 1 for Windows 및 그 이전 버전에서 지원됩니다.

6. **확인**을 누릅니다.

클라이언트 기기의 애플리케이션 시작 관리 구성

애플리케이션을 분류하면 기기에서 실행되는 애플리케이션 관리를 최적화할 수 있습니다. 애플리케이션 카테고리를 만들고 정책에 대해 애플리케이션 제어를 구성하면 해당 정책이 적용되는 기기에서 지정한 카테고리의 애플리케이션만 시작되도록 할 수 있습니다. *Application_1*및 *Application_2*라는 이름의 애플리케이션이 포함된 카테고리를 만든 경우를 예로 들어보겠습니다. 이 카테고리를 정책에 추가하면 해당 정책이 적용되는 기기에서는 다음 두 애플리케이션만 시작될 수 있습니다: *Application_1*및 *Application_2*사용자가 해당 카테고리에 포함되지 않는 애플리케이션, 즉 *Application_3*을 시작하려고 시도하면 Application_3의 실행이 차단됩니다. 사용자에게는 애플리케이션 제어 규칙에 따라 *Application_3*의 시작이 차단되었다는 알림 상태가 표시됩니다. 특정 폴더에서 여러 기준에 따라 컨텐츠가 자동으로 추가되는 카테고리를 만들 수 있습니다. 이 경우에는 지정한 폴더의 파일이 해당 카테고리에 자동으로 추가됩니다. 애플리케이션 실행 파일은 지정한 폴더에 복사되어 자동으로 실행되며 해당 메트릭이 카테고리에 추가됩니다.

클라이언트 기기의 애플리케이션 시작 관리를 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **애플리케이션 카테고리** 하위 폴더를 선택합니다.

2. **애플리케이션 카테고리** 폴더의 작업 영역에서 시작되는 동안에 관리하려는 애플리케이션 카테고리를 만듭니다.

3. **관리 중인 기기** 폴더의 **정책** 탭에서 **새 정책** 버튼을 클릭하여 Kaspersky Endpoint Security for Windows에 대한 새로운 정책을 만들고 마법사의 지침을 따릅니다.

   해당 정책이 이미 존재하는 경우 이 단계를 건너뛸 수 있습니다. 정책 설정을 통해 지정된 카테고리에 애플리케이션 시작 관리를 구성할 수 있습니다. 새로 만들어진 정책이 **관리 중인 기기** 폴더의 **정책** 탭에 표시됩니다.

4. Kaspersky Endpoint Security for Windows에 대한 정책의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.

   Kaspersky Endpoint Security for Windows에 대한 정책 속성 창이 열립니다.

5. Kaspersky Endpoint Security for Windows 정책의 속성 창에 있는 **보안 제어** → **애플리케이션 제어** 섹션에서 **애플리케이션 제어** 확인란을 선택합니다.

6. **추가** 버튼을 누릅니다.

   애플리케이션 제어 규칙 창이 열립니다.

7. **애플리케이션 제어 규칙** 창의 **카테고리** 드롭다운 목록에서 시작 규칙을 적용할 애플리케이션 카테고리를 선택합니다. 선택한 애플리케이션 카테고리의 시작 규칙을 구성합니다.

   Kaspersky Endpoint Security 10 서비스 팩 2 이후 버전의 경우 실행 파일의 MD5 해시 기준에 따라 만든 카테고리는 표시되지 않습니다.

   Kaspersky Endpoint Security 10 Service Pack 2 이전 버전에서는 실행 파일의 SHA256 해시 기준에 따라 만든 카테고리를 추가하지 않는 것이 좋습니다. 애플리케이션 오류가 발생할 수 있기 때문입니다.

   제어 규칙을 구성하는 방법에 대한 상세 정보는 Kaspersky Endpoint Security for Windows 온라인 도움말에 나와 있습니다.

8. **확인**을 누릅니다.

사용자가 만든 규칙에 따라 지정한 카테고리에 포함된 기기에서 애플리케이션이 실행됩니다. Kaspersky Endpoint Security for Windows 정책의 속성 창에 있는 **애플리케이션 제어** 섹션에 새롭게 생성된 규칙이 표시됩니다.

실행 파일에 적용된 시작 규칙의 통계 분석 결과 보기

사용자의 실행이 금지된 실행 파일의 정보를 보려면 다음과 같이 하십시오:

1. 콘솔 트리의 **관리 중인 기기** 폴더에서 **정책** 탭을 선택합니다.
2. Kaspersky Endpoint Security for Windows에 대한 정책의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   애플리케이션 정책의 속성 창이 열립니다.
3. **섹션** 창에서 **보안 제어**를 선택하고 **애플리케이션 제어** 하위 섹션을 선택합니다.
4. **정적 분석** 버튼을 누릅니다.
   접근 권한 분석 목록 창이 열립니다. 창의 왼쪽에 Active Directory 데이터 기반 사용자 목록이 표시됩니다.
5. 목록에서 사용자를 선택합니다.
   창의 우편에 해당 사용자에게 할당된 애플리케이션의 카테고리가 표시됩니다.
6. 실행이 금지된 실행 파일을 보려면 **접근 권한 분석 목록** 창에서 **파일 보기** 버튼을 누릅니다.
   금지된 실행 파일의 목록이 표시된 창이 열립니다.
7. 카테고리에 포함된 실행 파일 목록을 보려면 애플리케이션 카테고리를 선택하고 **카테고리에서 파일 보기** 버튼을 누릅니다.
   창이 열리고 애플리케이션 카테고리에 포함된 실행 파일 목록이 표시됩니다.

자산 관리(소프트웨어) 보기

Kaspersky Security Center는 관리 중인 기기에 설치되는 모든 소프트웨어의 인벤토리를 수행합니다.

네트워크 에이전트는 Windows나 Linux 기기에 설치된 애플리케이션 목록을 수집하고 이를 중앙 관리 서버로 전송합니다. Windows 기반 클라이언트 기기에서는 네트워크 에이전트가 설치된 애플리케이션에 대한 정보 대부분을 Windows 레지스트리에서 받습니다. Linux 기반 클라이언트 기기에서는 패키지 관리자가 설치된 애플리케이션에 대한 정보를 네트워크 에이전트에 제공합니다.

클라이언트 기기에 설치된 애플리케이션의 레지스트리를 보려면 다음과 같이 하십시오,

콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **자산 관리(소프트웨어)** 하위 폴더를 선택합니다.

자산 관리(소프트웨어) 폴더의 작업 영역에는 클라이언트 기기와 중앙 관리 서버에 설치된 애플리케이션의 목록이 표시됩니다.

애플리케이션의 마우스 오른쪽 메뉴를 열고 **속성**을 선택하면 상세 정보를 확인할 수 있습니다. 애플리케이션 속성 창에는 해당 애플리케이션의 상세 정보와 애플리케이션의 실행 파일에 대한 정보를 비롯해 해당 애플리케이션이 설치된 기기 목록이 표시됩니다.

목록의 모든 애플리케이션의 마우스 오른쪽 메뉴에서 다음을 수행할 수 있습니다:

- 애플리케이션 카테고리에 이 애플리케이션 추가합니다.
- 애플리케이션에 태그를 할당합니다.

- 애플리케이션 목록을 CSV 파일 또는 TXT 파일로 내보냅니다.
- 애플리케이션 속성(예: 공급업체 이름, 버전 번호, 실행 파일 목록, 애플리케이션이 설치된 기기 목록, 사용 가능한 소프트웨어 업데이트 목록, 탐지된 소프트웨어 취약점 목록)을 봅니다.

특정 기준에 맞는 애플리케이션을 보기 위해 **자산 관리(소프트웨어)** 폴더의 작업 영역에 있는 필터링 필드를 사용할 수 있습니다.

선택한 기기의 속성 창에 있는 **자산 관리(소프트웨어)** 섹션에서 기기에 설치된 애플리케이션의 목록을 볼 수 있습니다.

설치된 애플리케이션에 대한 리포트 생성

자산 관리(소프트웨어) 작업 영역에서 **자산 관리(소프트웨어) 리포트 보기** 버튼을 눌러 각 애플리케이션이 설치된 기기의 수를 포함하여 설치된 애플리케이션에 대한 자세한 통계가 포함된 리포트를 생성할 수도 있습니다. **자산 관리(소프트웨어) 리포트** 페이지에서 열리는 이 리포트는 Kaspersky 애플리케이션과 타사 소프트웨어 모두에 대한 정보를 포함합니다. 클라이언트 기기에 설치된 Kaspersky 애플리케이션에만 대한 정보를 보려면 **요약** 목록에서 AO Kaspersky Lab을 선택합니다.

또한 보조 및 가상 중앙 관리 서버에 연결된 기기에 설치되어 있는 Kaspersky 애플리케이션 및 타사 소프트웨어에 대한 정보도 수집되어 기본 중앙 관리 서버의 자산 관리(소프트웨어)에 저장됩니다. 보조 및 가상 중앙 관리 서버에서 데이터를 추가한 후 **자산 관리(소프트웨어) 리포트 보기** 버튼을 눌러 **자산 관리(소프트웨어) 리포트** 페이지가 열리면 이 정보를 볼 수 있습니다.

자산 관리(소프트웨어) 리포트에 보조 및 가상 중앙 관리 서버의 정보를 추가하려면:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. **리포트** 탭에서 **자산 관리(소프트웨어) 리포트**를 선택합니다.
4. 리포트의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   속성: 자산 관리(소프트웨어) 리포트 창이 열립니다.
5. **중앙 관리 서버 계층 구조** 섹션에서 **보조 및 가상 중앙 관리 서버의 데이터 포함** 확인란을 선택합니다.
6. **확인**를 누릅니다.

보조 및 가상 중앙 관리 서버의 정보는 **자산 관리(소프트웨어) 리포트**에 포함됩니다.

소프트웨어 인벤토리 시작 시간 변경

Kaspersky Security Center는 Windows을 사용하는 관리 중인 클라이언트 기기에 설치되는 모든 소프트웨어의 인벤토리를 수행합니다.

네트워크 에이전트는 기기에 설치된 애플리케이션 목록을 수집하고 이를 중앙 관리 서버로 전송합니다. 네트워크 에이전트는 자동으로 Windows 레지스트리에서 설치된 애플리케이션에 대한 정보를 수집합니다.

기기 리소스를 절약하기 위해, 기본적으로 네트워크 에이전트는 네트워크 에이전트 서비스가 시작되고 10분 후에 설치된 애플리케이션에 대한 정보 수집을 시작합니다.

기기에 설치된 네트워크 에이전트 서비스가 실행된 이후에 지난 소프트웨어 인벤토리 시작 시간을 변경하려면:

1. 네트워크 에이전트가 설치된 기기에서 시스템 레지스트리를 엽니다(예: 로컬에서 **시작** → **실행** 메뉴의 regedit 명령 사용).
2. 다음 하이브로 이동합니다:
   - 32비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - 64비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. KLINV_INV_COLLECTOR_START_DELAY_SEC 키에서 두 번째 값을 설정합니다.
   기본 값은 600 초입니다.
4. 그리고, 네트워크 에이전트 서비스를 재시작합니다.

네트워크 에이전트 서비스가 실행된 이후에 지난 소프트웨어 인벤토리 시작 시간이 변경됩니다.

타사 애플리케이션의 라이센스 키 관리 정보

Kaspersky Security Center를 사용하면 관리 중인 기기에 설치된 타사 애플리케이션에 대한 라이센스 키 사용을 추적할 수 있습니다. 라이센스 키 사용을 추적할 수 있는 애플리케이션 목록은 자산 관리(소프트웨어)에서 가져옵니다. 각 라이센스 키에 대해 다음 제한 사항의 위반을 지정하고 추적할 수 있습니다.

- 이 라이센스 키를 사용하는 애플리케이션을 설치할 수 있는 최대 기기의 수입니다
- 라이센스 키의 만료 날짜입니다

Kaspersky Security Center는 실제 라이센스 키를 지정했는지 여부를 확인하지 않습니다. 지정한 제한 사항만 추적할 수 있습니다. 라이센스 키에 적용한 제한 사항 중 하나를 위반하면 중앙 관리 서버는 정보, 경고 또는 기능 실패 이벤트를 등록합니다.

라이센스 키는 애플리케이션 그룹에 바인딩됩니다. 애플리케이션 그룹은 기준 또는 여러 기준에 따라 결합하는 타사 애플리케이션 그룹입니다. 애플리케이션 이름, 버전, 공급업체 및 태그로 애플리케이션을 정의할 수 있습니다. 기준 중 하나 이상이 충족되면 애플리케이션이 그룹에 추가됩니다. 각 애플리케이션 그룹에 여러 라이센스 키를 바인딩할 수 있지만 각 라이센스 키는 단일 애플리케이션 그룹에만 바인딩할 수 있습니다.

라이센스 키 사용을 추적하는 데 사용할 수 있는 또 하나의 도구는 유료 애플리케이션 그룹의 상태 리포트입니다. 이 리포트는 다음을 포함하여 유료 애플리케이션 그룹의 현재 상태에 대한 정보를 제공합니다.

- 각 애플리케이션 그룹의 라이센스 키 설치 수
- 사용 중인 라이센스 키 및 비어있는 라이센스 키 수
- 관리 중인 기기에 설치된 유료 애플리케이션의 세부 목록

타사 애플리케이션의 라이센스 키 관리 도구는 **타사 라이센스 사용 관리** 하위 폴더(**고급** → **애플리케이션 관리** → **타사 라이센스 사용 관리**)에 있습니다. 이 하위 폴더에서 애플리케이션 그룹을 생성하고 라이센스 키를 추가하며, 유료 애플리케이션 그룹에 대한 상태 리포트를 생성할 수 있습니다.

타사 애플리케이션의 라이센스 키 관리 도구는 **인터페이스 구성** 창에서 취약점 및 패치 관리 옵션을 활성화한 경우에만 사용할 수 있습니다.

유료 애플리케이션 그룹 만들기

유료 애플리케이션 그룹을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **타사 라이센스 사용 관리** 하위 폴더를 선택합니다.
2. **유료 애플리케이션 그룹 추가** 버튼을 눌러 유료 애플리케이션 그룹 추가 마법사를 실행합니다.
   유료 애플리케이션 그룹 추가 마법사가 시작됩니다.
3. **유료 애플리케이션 그룹 세부 정보** 단계에서 애플리케이션 그룹에 포함할 애플리케이션을 지정하십시오.
   - **유료 애플리케이션 그룹 이름**
   - **구매 수량 위반 추적**

     애플리케이션 그룹의 라이센스 키에 적용한 제한 사항 중 하나를 위반하면 중앙 관리 서버는 정보, 경고 또는 기능 실패 이벤트를 등록합니다.

     - 정보 이벤트: **유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 곧 초과합니다(95% 이상 사용 중)**
     - 경고 이벤트: **유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 곧 초과합니다**
     - 기능 실패 이벤트: **유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 초과했습니다**

       이벤트는 명시된 조건이 충족될 때 한 번만 등록됩니다. 다음 번에는 설치 횟수가 정상 수준으로 돌아온 경우에만 동일한 이벤트를 등록할 수 있으며 그 후 다시 이벤트가 발생합니다. 이벤트는 시간당 한 번 이상 등록할 수 없습니다.
   - **이 유료 애플리케이션 그룹으로 탐지된 애플리케이션을 추가하기 위한 기준**

     애플리케이션 그룹에 포함할 애플리케이션을 정의하는 기준을 지정하십시오. 애플리케이션 이름, 버전, 공급업체 및 태그로 애플리케이션을 정의할 수 있습니다. 기준을 하나 이상 지정해야 합니다. 기준 중 하나 이상이 충족되면 애플리케이션이 그룹에 추가됩니다.
4. **기존 라이센스 키 정보 입력** 단계에서 추적할 라이센스 키를 지정합니다. **라이센스 구매 수량을 초과하면 제어** 옵션을 선택한 다음 라이센스 키를 추가합니다.
   a. **추가** 버튼을 누릅니다.
   b. 추가할 라이센스 키를 선택한 다음 **확인** 버튼을 클릭합니다. 필요한 라이센스 키가 목록에 없으면 **추가** 버튼을 클릭한 다음 라이센스 키 속성을 지정합니다.
5. **유료 애플리케이션 그룹 추가** 단계에서 **완료** 버튼을 클릭합니다.

유료 애플리케이션 그룹이 생성되어 **타사 라이센스 사용 관리** 폴더에 표시됩니다.

유료 애플리케이션 그룹의 라이센스 키 관리

유료 애플리케이션 그룹에 대한 라이센스 키를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **타사 라이센스 사용 관리** 하위 폴더를 선택합니다.
2. **타사 라이센스 사용 관리** 폴더의 작업 공간에서 **유료 애플리케이션의 라이센스 키 관리** 버튼을 누릅니다.
   유료 애플리케이션의 라이센스 키 관리 창이 열립니다.
3. **유료 애플리케이션의 라이센스 키 관리** 창에서 **추가** 버튼을 누릅니다.
   라이센스 키 창이 열립니다.
4. **라이센스 키** 창에 라이센스 키의 속성과 유료 애플리케이션 그룹에 부과된 라이센스 키의 제한을 지정합니다.
   - **이름**. 라이센스 키의 이름입니다.
   - **메모**. 선택된 라이센스 키에 대한 설명입니다.
   - **제한**. 이 라이센스 키를 사용하는 애플리케이션을 설치할 수 있는 기기의 수입니다.
   - **만료**. 라이센스 키의 만료 날짜입니다.

   생성된 라이센스 키가 **유료 애플리케이션의 라이센스 키 관리** 창에 표시됩니다.

유료 애플리케이션 그룹에 라이센스 키를 적용하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급** → **애플리케이션 관리** 폴더에서 **타사 라이센스 사용 관리** 하위 폴더를 선택합니다.
2. **타사 라이센스 사용 관리** 폴더에서 라이센스 키를 적용하려는 유료 애플리케이션 그룹을 선택합니다.
3. 유료 애플리케이션 그룹의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   이렇게 하면 유료 애플리케이션 그룹의 속성 창이 열립니다.
4. 유료 애플리케이션 그룹의 속성 창에 있는 **라이센스 키** 섹션에서 **라이센스 구매 수량을 초과하면 제어**를 선택합니다.
5. **추가** 버튼을 누릅니다.
   라이센스 키 선택 창이 열립니다.
6. **라이센스 키 선택** 창에서 유료 애플리케이션 그룹에 적용할 라이센스 키를 선택합니다.
7. **확인**을 누릅니다.

   유료 애플리케이션 그룹에 부과되며 라이센스 키에 지정되어 있는 제한은 선택한 유료 애플리케이션 그룹에도 적용됩니다.

실행 파일 인벤토리

관리 중인 기기에 저장된 실행 파일 목록을 확보할 수 있습니다. 실행 파일의 인벤토리에 인벤토리 작업을 생성해야 합니다.

실행 파일 인벤토리 기능은 다음 애플리케이션에서 사용할 수 있습니다:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent 및 이후 버전

단일 기기에서 수신하는 실행 파일의 수는 150,000개를 초과할 수 없습니다. 이 제한에 도달하면 Kaspersky Security Center는 새 파일을 수신할 수 없습니다.

시작하기 전에 Kaspersky Endpoint Security 정책 및 네트워크 에이전트 정책에서 애플리케이션 시작에 대한 알림을 활성화하면 데이터를 중앙 관리 서버로 전송할 수 있습니다.

애플리케이션 시작에 대한 알림을 활성화하려면 다음을 수행합니다.

- Kaspersky Endpoint Security 정책 설정을 열고 다음을 수행합니다.
  1. **일반 설정** → **보고서 및 저장소**로 이동합니다.
  2. **중앙 관리 서버로 데이터 전송** 섹션에서 **시작된 애플리케이션 정보** 확인란을 선택합니다.
  3. 변경 사항을 저장합니다.
- 네트워크 에이전트 정책 설정을 열고 다음을 수행합니다.
  1. **저장소** 섹션으로 이동합니다.
  2. **자산 관리(소프트웨어) 정보** 확인란을 선택합니다.
  3. 변경 사항을 저장합니다.

클라이언트 기기에 있는 실행 파일에 대한 인벤토리 작업을 만들려면:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **작업** 폴더의 작업 영역에서 **새 작업** 버튼을 누릅니다.
   새 작업 마법사가 시작됩니다.
3. 마법사의 **작업 유형 선택** 창에서 작업 유형으로 **Kaspersky Endpoint Security**를 선택한 후 작업 하위 유형으로 **인벤토리**를 선택하고 **다음**을 누릅니다.
4. 마법사의 나머지 지침을 따릅니다.

마법사를 완료한 후 Kaspersky Endpoint Security용 인벤토리 작업이 생성됩니다. 새롭게 생성된 작업은 **작업** 폴더에서 작업 영역의 작업 목록에 표시됩니다.

인벤토리 작업 동안 기기에서 탐지된 실행 파일 목록은 **실행 파일** 폴더의 작업 영역에 표시됩니다.

인벤토리 작업 동안 애플리케이션은 MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR 및 HTML 파일 형식의 실행 파일을 탐지합니다.

실행 파일에 대한 정보 보기

클라이언트 기기에 탐지된 모든 실행 파일 목록을 보려면 다음과 같이 하십시오,

콘솔 트리의 **애플리케이션 관리** 폴더에서 **실행 파일** 하위 폴더를 선택합니다.

실행 파일 폴더의 작업 영역에는 기기에서 실행하였거나 Kaspersky Endpoint Security for Windows의 인벤토리 작업 실행 시 탐지된 실행 파일 목록이 표시됩니다.

특정 기준을 충족하는 실행 파일의 상세 정보를 보려면 필터링을 사용할 수 있습니다.

실행 파일의 속성을 보려면 다음과 같이 하십시오,

파일의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

실행 파일에 대한 정보와 함께 해당 파일이 탐지된 기기의 목록이 표시된 창이 열립니다.

모니터링 및 보고

이 섹션에서는 Kaspersky Security Center의 모니터링 및 보고 기능에 대해 설명합니다. 이러한 기능을 통해 인프라, 보호 상태 및 통계의 개요를 확인할 수 있습니다.

Kaspersky Security Center 배포 후나 작동 중에 요구에 가장 적합하도록 모니터링 및 리포팅 기능을 구성할 수 있습니다.

- **표시등**

  관리 콘솔에서는 표시등을 확인하여 Kaspersky Security Center 및 관리 중인 기기의 현재 상태를 평가할 수 있습니다.

- **통계**

  보호 시스템 및 관리 중인 기기의 상태에 대한 통계는 사용자 지정 가능한 정보 패널에 표시됩니다.

- **리포트**

  리포트 기능을 사용하면 조직의 네트워크 보안에 대한 자세한 숫자 정보를 얻고, 이 정보를 파일에 저장하며, 이메일로 보내고, 인쇄할 수 있습니다.

- **이벤트**

이벤트 조회는 중앙 관리 서버 데이터베이스에서 선택한 이벤트를 미리 정의된 조회 항목을 사용해 화면에 그 결과를 보여 줍니다. 이러한 이벤트 세트는 다음 카테고리에 따라 그룹화됩니다:

- 심각도 기준 – **심각 이벤트**, **기능 실패**, **경고** 및 **정보 이벤트**
- 시간 기준 – **최근 이벤트**
- 유형 기준 - **사용자 개선 요청 사항** 및 **감사 이벤트**

구성을 위해 Kaspersky Security Center 웹 콘솔 인터페이스에서 사용할 수 있는 설정에 따라 사용자 지정 이벤트 조회를 생성하고 볼 수 있습니다.

시나리오: 모니터링 및 보고

이 섹션에서는 Kaspersky Security Center에서 모니터링 및 리포팅 기능을 구성하는 시나리오를 제공합니다.

필수 구성 요소

조직의 네트워크에 Kaspersky Security Center를 배포한 후 모니터링을 시작하고 기능에 대한 리포트를 생성할 수 있습니다.

단계

조직의 네트워크에서 모니터링 및 리포팅은 단계적으로 진행됩니다.

1. **기기 상태 전환 구성**

   특정 조건에 따라 기기 상태 할당을 정의하는 설정을 익힙니다. 이러한 설정을 변경하여 *심각* 또는 *경고* 심각도의 이벤트 수를 변경할 수 있습니다.

   기기 상태 전환을 구성할 경우 새로운 설정이 조직의 정보 보안 정책과 충돌하지 않고 조직 네트워크의 중요 보안 이벤트에 대해 적시에 대응할 수 있는지 확인합니다.

2. **클라이언트 기기에서 이벤트 알림 구성**

   조직의 필요에 따라 클라이언트 기기에서 이벤트 알림(이메일, SMS 또는 실행 파일 실행을 통해) 구성.

3. **바이러스 발생 이벤트에 대한 보안 네트워크 응답 변경**

   새로운 이벤트에 대한 네트워크의 응답을 조정하려면 중앙 관리 서버 속성에서 특정 임계값을 변경합니다. 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.

4. **통계 관리**

   조직의 필요에 따라 통계 표시를 구성합니다.

5. **조직 네트워크의 보안 상태 검토**

   조직 네트워크의 보안 상태를 검토하려면 다음 중 하나를 수행합니다.

   - **중앙 관리 서버** 노드의 작업 영역에 있는 **통계** 탭에서 **보호 상태** 이차 레벨 탭(페이지)을 열고 **실시간 보호 상태** 정보 패널을 검토합니다.
   - **보호 상태 리포트** 생성 및 검토.
   - **오류 리포트** 생성 및 검토.

6. **보호되지 않는 클라이언트 기기 위치 추적**

   보호되지 않는 클라이언트 기기를 찾으려면 **중앙 관리 서버** 노드의 작업 영역에 있는 **통계** 탭에서 **보호 상태** 이차 레벨 탭(페이지)을 열고 **네트워크에 연결된 새 기기의 탐지 내역** 정보 패널을 검토합니다. 또한 **보호 배포 리포트**도 생성하고 검토할 수 있습니다.

7. **클라이언트 기기의 보호 확인**

   클라이언트 기기의 보호를 확인하려면 **중앙 관리 서버** 노드의 작업 영역에 있는 **통계** 탭에서 **배포** 또는 **위협 통계** 이차 레벨 탭(페이지)를 열고 관련 정보 패널을 검토합니다. 또한 **심각 이벤트** 이벤트 조회도 시작하고 검토할 수 있습니다.

8. **데이터베이스의 이벤트 부하 평가 및 제한**

   관리 중인 애플리케이션 작업 중 발생하는 이벤트에 대한 정보는 클라이언트 기기에서 전송되어 중앙 관리 서버 데이터베이스에 등록됩니다. 중앙 관리 서버의 부하를 줄이려면 데이터베이스에 저장할 수 있는 최대 이벤트 수를 평가 및 제한합니다.

   데이터베이스의 이벤트 로드를 평가하려면 데이터베이스 공간을 계산합니다. 또한 최대 이벤트 수를 제한하여 데이터베이스 오버플로를 방지할 수도 있습니다.

9. **라이센스 정보 검토**

   라이선스 정보를 검토하려면 **중앙 관리 서버** 노드의 작업 영역에 있는 **통계** 탭에서 **배포** 이차 레벨 탭(페이지)을 열고 **라이센스 키 사용 현황** 정보 패널을 검토합니다. 또한 **라이센스 키 사용 리포트**도 생성하고 검토할 수 있습니다.

결과

시나리오가 완료되면 조직의 네트워크 보호에 대한 정보를 받게 되므로 추가 보호 작업을 계획할 수 있습니다.

관리 콘솔에서 표시등 및 기록된 이벤트 모니터링

관리 콘솔에서는 표시등을 확인하여 Kaspersky Security Center 및 관리 중인 기기의 현재 상태를 평가할 수 있습니다. 표시등은 **중앙 관리 서버** 노드 작업 영역의 **모니터링** 탭에 표시됩니다. 이 탭에서는 표시등과 기록된 이벤트가 포함된 6개 정보 패널이 제공됩니다. 표시등은 패널 왼쪽에 있는 색상이 지정된 세로 막대입니다. 표시등이 포함된 각 창은 Kaspersky Security Center의 특정 기능 범위에 해당합니다(아래 표 참조).

관리 콘솔의 표시등에 해당하는 범위

패널 이름	표시등 범위
배포	조직 네트워크에 있는 기기에 네트워크 에이전트 및 보안 제품 설치
관리 계획	관리 그룹의 구조. 네트워크 검사. 기기 이동 규칙
보호 설정	보안 애플리케이션 기능: 보호 상태, 악성 코드 검사
업데이트	업데이트 및 패치
모니터링	보호 상태
중앙 관리 서버	중앙 관리 서버 기능 및 속성

각 표시등은 5가지 색상 중 하나로 켜질 수 있습니다(아래 표 참조). 표시등의 색상은 Kaspersky Security Center의 현재 상태와 기록된 이벤트에 따라 달라집니다.

표시등의 색상 코드

상태	표시등 색상	표시등 색상의 의미
정보	녹색	관리자의 개입 필요 없음.
경고	노란색	관리자의 개입 필요.

상태	표시등 색상	표시등 색상의 의미
심각	빨간색	심각한 문제 발생. 문제를 해결하려면 관리자의 개입이 필요합니다.
정보	하늘색	관리 중인 기기 보안에 대한 실제 위협 또는 위협 가능성과 관련이 없는 이벤트가 기록됨.
정보	회색	이벤트 세부 정보를 사용할 수 없거나 아직 가져오지 않음.

관리자는 **모니터링** 탭의 모든 정보 패널에서 표시등 색을 녹색으로 유지해야 합니다.

정보 패널에는 표시등에 영향을 미치는 기록된 이벤트와 Kaspersky Security Center 상태도 표시됩니다(아래 표 참조).

기록된 이벤트의 이름, 설명 및 표시등 색상

표시등 색상	이벤트 유형 표시 이름	이벤트 유형	설명
빨간색	**라이센스가 만료된 기기: %1대**	IDS_AK_STATUS_LIC_EXPAIRED	이 유형의 이벤트는 상업용 라이센스가 만료되면 발생합니다. Kaspersky Security Center는 하루에 한 번 기기에서 라이센스 만료 상태를 확인합니다. 상업용 라이센스가 만료되면 Kaspersky Security Center에서는 기본 기능만 제공됩니다. Kaspersky Security Center를 계속 사용하려면 상업용 라이센스를 갱신하십시오.
빨간색	**보안 제품이 실행 중이지 않음: %1대**	IDS_AK_STATUS_AV_NOT_RUNNING	이 유형의 이벤트는 기기에 설치된 보안 애플리케이션이 실행되고 있지 않을 때 발생합니다. 기기에서 Kaspersky Endpoint Security가 실행 중인지 확인합니다.
빨간색	**보호가 비활성화됨: %1대**	IDS_AK_STATUS_RTP_NOT_RUNNING	이 유형의 이벤트는 기기의 보안 애플리케이션이 지정된 간격보다 오랫동안 비활성화되었을 때 발생합니다. 기기에서 실시간 보호의 현재 상태를 확인하고 필요한 모든 보호 구성 요소가 활성화되어 있는지 확인하십시오.
빨간색	**소프트웨어 취약점이 기기에서 탐지됨**	IDS_AK_STATUS_VULNERABILITIES_FOUND	이 유형의 이벤트는 *취약성 및 필수 업데이트 찾기* 작업으로 기기에 설치된 애플리케이션에서 지정된 심각도 수준의 취약성이 탐지되면 발생합니다. **애플리케이션 관리** 폴더의 **소프트웨어 업데이트** 하위 폴더에서 사용 가능한 업데이트 목록을 확인할 수 있습니다. 이 폴더에는 기기에 배포할 수 있는 Microsoft 애플리케이션과 중앙 관리 서버가 검색한 기타 소프트웨어 공급업체 제품의 업데이트 목록이 들어 있습니다. 사용 가능한 업데이트 정보를 확인한 후 기기에 설치합니다.
빨간색	**중앙 관리 서버에 심각 이벤트가 등록됨**	IDS_AK_STATUS_EVENTS_OCCURED	이 유형의 이벤트는 중앙 관리 서버의 심각 이벤트가 감지될 때 발생합니다. 중앙 관리 서버에 저장된 이벤트 목록을 확인한 다음 심각 이벤트를 하나씩 수정하십시오.
빨간색	**중앙 관리 서버에 오류 이벤트가 기록됨**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	이 유형의 이벤트는 예기치 않은 오류가 중앙 관리 서버 측에 기록될 때 발생합니다. 중앙 관리 서버에 저장된 이벤트 목록을 확인하고 오류를 하나씩 수정하십시오.
빨간색	**연결이 끊긴 기기: %1대**	IDS_AK_STATUS_ADM_LOST_CONTROL1	이 유형의 이벤트는 중앙 관리 서버와 기기 간의 연결이 끊어지면 발생합니다. 연결 해제된 기기 목록을 보고 다시 연결해 보십시오.
빨간색	**오랫동안 중앙 관리 서버에 연결 안 된 기기: %1대**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	이 유형의 이벤트는 기기가 꺼져서 지정된 시간 내에 중앙 관리 서버에 연결되지 않았을 때 발생합니다. 기기가 켜져 있고 네트워크 에이전트가 실행 중인지 확인하십시오.
빨간색	**'정상' 상태가 아닌 기기: %1대**	IDS_AK_STATUS_HOST_NOT_OK	이 유형의 이벤트는 중앙 관리 서버에 연결된 기기의 *정상* 상태가 *위험* 또는 *경고*로 변경되면 발생합니다. Kaspersky Security Center 원격 진단 유틸리티를 사용하여 문제를 해결할 수 있습니다.

표시등 색상	이벤트 유형 표시 이름	이벤트 유형	설명
빨간색	**데이터베이스가 오래된 기기: %1대**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	이 유형의 이벤트는 바이러스 백신 데이터베이스가 지정된 시간 내에 기기에서 업데이트되지 않았을 때 발생합니다. 지침에 따라 Kaspersky 데이터베이스를 업데이트합니다.
빨간색	**오랫동안 Windows 업데이트 패치를 검색하지 않은 기기: %1대**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	이 유형의 이벤트는 *Windows Update 동기화 수행* 작업이 지정된 시간 내에 실행되지 않았을 때 발생합니다. 지침에 따라 Windows 업데이트를 중앙 관리 서버와 동기화하십시오.
빨간색	**Kaspersky Security Center용 %1 플러그인을 설치해야 합니다**	IDS_AK_STATUS_PLUGINS_REQUIRED2	이 유형의 이벤트는 Kaspersky 애플리케이션용 추가 플러그인을 설치해야 할 때 발생합니다. Kaspersky 기술 지원 웹페이지에서 Kaspersky 애플리케이션에 필요한 관리 플러그인을 다운로드하고 설치합니다.

리포트, 통계 및 알림 작업

이 섹션에서는 Kaspersky Security Center에서 리포트와 통계를 사용하고 이벤트와 기기를 조회하는 방법 및 중앙 관리 서버 알림을 구성하는 방법에 대해 설명합니다.

리포트 작업

Kaspersky Security Center의 리포트에는 관리 중인 기기의 상태에 대한 정보가 포함되어 있습니다. 리포트는 중앙 관리 서버에 저장된 정보를 기반으로 생성됩니다. 다음과 같은 유형의 개체에 대해 리포트를 작성할 수 있습니다:

- 특정 설정에 따라 생성된 기기 조회.
- 관리 그룹.
- 여러 관리 그룹의 특정 기기.
- 네트워크에 있는 모든 기기 (배포 리포트에서).

애플리케이션은 표준 리포트 템플릿을 선택할 수 있습니다. 또한, 사용자정의 리포트 템플릿을 만들 수도 있습니다. 리포트는 메인 애플리케이션 창의 콘솔 트리의 **중앙 관리 서버** 폴더에 표시됩니다.

리포트 템플릿 만들기

리포트 템플릿을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. **새 리포트 템플릿** 버튼을 누릅니다.

   새 리포트 템플릿 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

마법사가 작업을 완료하면 새로 만들어진 리포트 템플릿이 콘솔 트리의 선택한 **중앙 관리 서버** 폴더에 추가됩니다. 이 템플릿을 사용하여 리포트를 만들고 볼 수 있습니다.

리포트 템플릿 속성 보기 및 편집

리포트 템플릿 이름 또는 리포트에 표시되는 필드와 같은 리포트 템플릿의 기본 속성을 확인하고 편집할 수 있습니다.

리포트 템플릿의 속성을 확인하고 편집하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. 리포트 템플릿 목록에서 필요한 리포트 템플릿을 선택합니다.
4. 선택한 리포트 템플릿의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   먼저 리포트를 생성한 다음 **리포트 템플릿 속성 열기** 버튼이나 **리포트 열 구성** 버튼을 눌러도 됩니다.
5. 창이 열리면 리포트 템플릿 속성을 편집합니다. 각 리포트의 속성에는 아래에서 설명하는 섹션 중 일부만 포함될 수도 있습니다.

   - **일반** 섹션:
     - 리포트 템플릿 이름
     - **표시되는 최대 항목 수**

       이 옵션을 활성화하면 상세 리포트 데이터가 포함된 표에 표시되는 항목 수가 지정된 값을 초과하지 않습니다.

       리포트 항목은 먼저 리포트 템플릿 속성의 **필드 → 상세 정보 필드**드 섹션에 지정된 규칙에 따라 정렬되며, 결과 항목 중 첫 번째 항목만 유지됩니다. 상세 리포트 데이터가 포함된 표의 제목에는 표시되는 항목 수, 그리고 다른 리포트 템플릿 설정과 일치하는 총 사용 가능 항목 수가 나타납니다.

       이 옵션을 비활성화하면 상세 리포트 데이터가 포함된 표에 사용 가능한 모든 항목이 표시됩니다. 이 옵션은 사용하도록 설정하는 것이 좋습니다. 표시되는 리포트 항목의 수를 제한하면 DBMS(데이터베이스 관리 시스템)의 부하가 감소하며 리포트를 생성하고 내보내는 데 걸리는 시간도 단축됩니다. 항목이 너무 많이 포함된 리포트도 있습니다. 이러한 리포트에서는 모든 항목을 읽고 분석하기가 어려울 수도 있습니다. 또한 이러한 리포트를 생성하는 과정에서 기기의 메모리가 소진될 수도 있으며, 그러면 리포트를 확인할 수 없습니다.

       기본적으로 이 옵션은 켜져 있습니다. 기본값은 1000입니다.

     - **프린트 최적화**

       리포트 출력은 인쇄용으로 최적화되며 내용을 더 쉽게 읽을 수 있도록 일부 값 사이에는 공백 문자가 추가됩니다.

       기본적으로 이 옵션은 켜져 있습니다.

   - **필드** 섹션.

     리포트에 표시할 필드와 이러한 필드의 순서를 선택하고 각 필드를 기준으로 리포트의 정보를 정렬 및 필터링해야 하는지 여부를 구성합니다.

   - **시간 간격** 섹션.

리포트 기간을 수정합니다. 사용 가능한 값은 다음과 같습니다:

- 지정한 두 날짜 사이
- 지정한 날짜에서 리포트 생성 날짜까지
- 리포트 생성 날짜에서 리포트 생성 날짜까지의 지정된 기간(일)을 뺀 기간

- **그룹**, **기기 조회** 또는 **기기** 섹션.

  리포트 생성 대상 클라이언트 기기 세트를 변경합니다. 리포트 템플릿 생성 중에 지정한 설정에 따라서는 이러한 섹션 중 하나만 표시될 수도 있습니다.

- **설정** 섹션.

  리포트의 설정을 변경합니다. 정확한 설정 세트는 특정 리포트에 따라 달라집니다.

- **보안** 섹션. **중앙 관리 서버에서 설정 상속**

  이 옵션을 활성화하면 리포트의 보안 설정이 중앙 관리 서버에서 상속됩니다.

  이 옵션을 비활성화하는 경우에는 리포트의 보안 설정을 구성할 수 있습니다. 리포트에 적용된 대로 사용자 또는 사용자 그룹에 역할을 할당하거나 사용자 또는 사용자 그룹에 권한을 할당할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  보안 섹션은 인터페이스 설정 창에서 **보안 설정 섹션 표시** 확인란을 선택하면 사용할 수 있습니다.

- **중앙 관리 서버 계층 구조** 섹션:

  - **보조 및 가상 중앙 관리 서버의 데이터 포함**

    이 옵션을 활성화하면 리포트 템플릿 생성 대상인 중앙 관리 서버에 속한 보조 및 가상 중앙 관리 서버의 정보가 리포트에 포함됩니다.

    현재 중앙 관리 서버의 데이터만 보려면 이 옵션을 비활성화합니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **최대 중첩 레벨**

    현재 중앙 관리 서버에서 지정한 값 이하의 중첩 레벨 아래에 있는 보조 및 가상 중앙 관리 서버의 데이터가 리포트에 포함됩니다.

    기본값은 1입니다. 트리의 하위 레벨에 있는 보조 중앙 관리 서버에서 정보를 가져와야 하는 경우 이 값을 변경할 수 있습니다.

  - **데이터 대기 시간 간격(분)**

    리포트 템플릿 생성 대상인 중앙 관리 서버가 리포트를 생성하기 전에 지정된 시간(분) 동안 보조 중앙 관리 서버의 데이터를 기다립니다. 이 기간이 끝날 때까지 보조 중앙 관리 서버에서 데이터가 수신되지 않아도 리포트는 실행됩니다. 리포트에는 실제 데이터가 아니라 캐시에서 가져온 데이터(**보조 중앙 관리 서버에서 데이터 캐시** 옵션 활성화 시) 또는 **N/A**(사용 불가)가 표시됩니다.

    기본값은 5분입니다.

- **보조 중앙 관리 서버에서 데이터 캐시**

  보조 중앙 관리 서버가 리포트 템플릿 생성 대상인 중앙 관리 서버에 데이터를 주기적으로 전송합니다. 전송된 데이터는 이 중앙 관리 서버에서 캐시에 저장됩니다.

  현재 중앙 관리 서버가 리포트를 생성하는 중에 보조 중앙 관리 서버에서 데이터를 수신할 수 없으면 리포트에는 캐시에서 가져온 데이터가 표시됩니다. 데이터가 캐시로 전송된 날짜도 표시됩니다.

  이 옵션을 활성화하면 최신 데이터를 가져올 수 없어도 보조 중앙 관리 서버에서 정보를 확인할 수 있습니다. 하지만 표시되는 데이터는 오래된 데이터일 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **캐시 업데이트 간격(시)**

  보조 중앙 관리 서버가 리포트 템플릿 생성 대상인 중앙 관리 서버에 데이터를 주기적으로 전송합니다. 이 기간을 시간 단위로 지정할 수 있습니다. 0시간을 지정하면 리포트 생성 시에만 데이터가 전송됩니다.

  기본값은 0입니다.

- **보조 중앙 관리 서버에서 자세한 정보 전송**

  생성된 리포트에서 상세 리포트 데이터가 포함된 표에 리포트 템플릿 생성 대상인 중앙 관리 서버의 보조 중앙 관리 서버 데이터가 포함됩니다.

  이 옵션을 활성화하면 리포트 생성 속도가 느려지며 중앙 관리 서버 간의 트래픽이 증가합니다. 그러나 리포트 하나에서 모든 데이터를 확인할 수 있습니다.

  이 옵션을 활성화하는 대신 상세 리포트 데이터를 분석하여 결함이 있는 보조 중앙 관리 서버를 탐지한 다음 결함이 있는 중앙 관리 서버에 대해서만 같은 리포트를 생성할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

리포트 템플릿의 확장 필터 형식

Kaspersky Security Center 15.1에서는 확장 필터 형식을 리포트 템플릿에 적용할 수 있습니다. 확장 필터 형식은 기본 형식에 비해 유연합니다. 일련의 필터를 사용하여 복잡한 필터링 조건을 만들고 아래에 나와 있는 것처럼 리포트 작성 중에 OR 논리 연산자를 사용하여 리포트에 적용할 수 있습니다:

필터[1](필드[1] AND 필드[2]... AND 필드[n]) OR 필터[2](필드[1] AND 필드[2]... AND 필드[n]) OR... 필터[n](필드[1] AND 필드[2]... AND 필드[n])

또한 확장 필터 형식을 사용하면 필터의 특정 필드에 대해 상대 시간 형식으로 시간 간격 값을 설정할 수 있습니다(예: "지난 N일 동안" 조건 사용). 가용성 및 시간 간격 조건 세트는 리포트 템플릿 유형에 따라 다릅니다.

필터를 확장 형식으로 변환

리포트 템플릿에 대한 확장 필터 형식은 Kaspersky Security Center 12 이상 버전에서만 지원됩니다. 기본 필터를 확장 형식으로 변환한 후에는 리포트 템플릿이 이전 버전의 Kaspersky Security Center가 설치된 네트워크의 중앙 관리 서버와 호환되지 않습니다. 이러한 중앙 관리 서버의 정보는 리포트에 대해 수신되지 않습니다.

리포트 템플릿 기본 필터를 확장 형식으로 변환하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. 리포트 템플릿 목록에서 필요한 리포트 템플릿을 선택합니다.
4. 선택한 리포트 템플릿의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
5. 속성 창이 열리면 **필드** 섹션을 선택합니다.
6. **상세 정보 필드** 탭에서 **필터 변환** 링크를 누릅니다.
7. 창이 열리면 **확인** 버튼을 누릅니다.

   확장 필터 형식으로 변환하면 적용된 리포트 템플릿은 되돌릴 수 없습니다. 실수로 **필터 변환** 링크를 누른 경우 리포트 템플릿 속성 창에서 **취소** 버튼을 눌러 변경 사항을 취소할 수 있습니다.

8. 변경 사항을 적용하려면 **확인** 버튼을 눌러 리포트 템플릿 속성 창을 닫습니다.

   리포트 템플릿 속성 창이 다시 열리면 새로 사용 가능한 **필터** 섹션이 표시됩니다. 이 섹션에서는 확장 필터 구성을 할 수 있습니다.

확장 필터 구성

리포트 템플릿 속성에서 확장 필터를 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. 리포트 템플릿 목록에서 이전에 확장 필터 형식으로 변환된 리포트 템플릿을 선택합니다.
4. 선택한 리포트 템플릿의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
5. 속성 창이 열리면 **필터** 섹션을 선택합니다.

   이전에 리포트 템플릿이 확장 필터 형식으로 변환되지 않은 경우 **필터** 섹션이 표시되지 않습니다.

   리포트 템플릿 속성 창의 **필터** 섹션에서 리포트에 적용된 필터의 목록을 검토하고 수정할 수 있습니다. 목록의 각 필터에는 고유의 이름이 있으며 리포트의 해당 필드에 대한 필터 집합을 나타냅니다.

6. 다음 방법 중 하나로 필터 설정 창을 엽니다:
   - 새 필터를 만들려면 **추가** 버튼을 누릅니다.
   - 기존 필터를 수정하려면 필요한 필터를 선택하고 **수정** 버튼을 누릅니다.
7. 창이 열리면 필터에 필요한 필드의 값을 선택하고 지정합니다.
8. **확인** 버튼을 눌러 변경 사항을 저장하고 창을 닫습니다.

   새 필터를 만드는 경우 **확인** 버튼을 누르기 전에 **필터 이름** 필드에 필터 이름을 지정해야 합니다.

9. **확인** 버튼을 눌러 리포트 템플릿 속성 창을 닫습니다.

   리포트 템플릿의 확장 필터가 구성됩니다. 이제 이 리포트 템플릿을 사용하여 리포트 작성을 할 수 있습니다.

리포트 만들기 및 보기

리포트를 만들고 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. 리포트 템플릿 목록에서 필요한 리포트 템플릿을 두 번 누릅니다.
   선택한 템플릿에 해당하는 리포트가 표시됩니다.

리포트에는 다음 데이터가 표시됩니다:

- 리포트 이름과 유형, 리포트에 대한 간략한 설명과 보고 기간, 리포트가 생성된 대상 기기 그룹에 대한 정보.
- 가장 대표적인 리포트 데이터를 보여 주는 그래픽 차트.
- 계산된 리포트 지표로 구성된 통합 테이블.
- 세부 리포트 데이터로 구성된 테이블.

리포트 저장

작성한 리포트를 저장하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. 리포트 템플릿 목록에서 필요한 리포트 템플릿을 선택합니다.
4. 선택한 리포트 템플릿의 컨텍스트 메뉴에서 **저장**을 선택합니다.

   그러면 리포트 저장 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

마법사를 마치면 리포트 파일을 저장한 폴더가 열립니다.

보고서를 XLS 파일로 저장하면 로고 및 데이터그램과 같은 모든 관련 이미지가 별도의 파일로 저장됩니다.

리포트 전달 작업 만들기

리포트를 이메일로 전송할 수 있습니다. Kaspersky Security Center에서는 리포트 전달 작업을 사용하여 리포트를 전달합니다.

하나의 리포트에 대한 전달 작업을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. 리포트 템플릿 목록에서 필요한 리포트 템플릿을 선택합니다.
4. 선택한 리포트 템플릿의 컨텍스트 메뉴에서 **리포트 전달**을 선택합니다.

   리포트 전달 작업 생성 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

여러 리포트의 전달 작업을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버 이름으로 된 노드에서 **작업** 폴더를 선택합니다.
2. **작업** 폴더의 작업 영역에서 **작업 생성** 버튼을 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

   새롭게 생성된 리포트 전달 작업이 콘솔 트리의 **작업** 폴더에 표시됩니다.

Kaspersky Security Center 설치 도중 이메일 설정을 지정했으면 리포트 전달 작업이 자동으로 만들어집니다.

1단계. 작업 유형 선택

작업 유형 선택 창의 작업 목록에서 **리포트 전달**를 작업 유형으로 선택합니다.

다음을 눌러 다음 단계로 진행합니다.

2단계. 리포트 유형 선택

리포트 유형 선택 창의 작업 만들기 템플릿 목록에서 리포트 유형을 선택합니다.

다음을 눌러 다음 단계로 진행합니다.

3단계. 리포트에 대한 작업

리포트에 적용할 처리 방법 창에서 다음 설정을 지정합니다:

- **이메일로 리포트 전송**

  이 옵션을 사용하면 애플리케이션이 리포트를 이메일로 전송합니다.

  이메일 알림 설정 링크를 눌러 이메일로 보내지는 리포트를 구성할 수 있습니다. 이 링크는 이 옵션을 활성화한 경우에 사용할 수 있습니다.

  이 옵션이 비활성화되어 있으면 애플리케이션은 리포트를 저장하기 위해 지정한 폴더에 이를 저장합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **공유 폴더에 리포트 저장**

  이 옵션을 사용하면 애플리케이션은 확인란 아래에 있는 필드에 명시된 폴더로 리포트를 저장합니다. 리포트를 공유 폴더에 저장하려면 폴더의 UNC 경로를 지정합니다. 이 경우 **작업을 실행할 계정 선택** 창에서 이 폴더 접근을 위한 사용자 계정과 암호를 지정해야 합니다.

이 옵션이 비활성화되어 있으면 애플리케이션은 리포트를 폴더에 저장하지 않고 대신 이메일로 보내게 됩니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **동일 유형의 이전 리포트 덮어쓰기**

  이 옵션을 사용하면, 매번 작업 시작 시 새 리포트 파일은 이전 작업 시작 시 리포트 폴더에 저장했던 파일을 덮어쓰기합니다.

  이 옵션이 비활성화되어 있으면 리포트 파일은 덮어쓰기되지 않습니다. 새 리포트 파일은 매번 작업 실행 시 리포트 폴더에 저장됩니다.

  이 확인란은 **폴더에 리포트 저장** 확인란이 선택되어 있는 경우에 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **공유 폴더에 접근하기 위한 계정 지정**

  이 옵션을 사용하면 리포트가 저장될 폴더의 계정을 지정할 수 있습니다. **리포트에 적용할 작ㅓㅂ** 창에서 **폴더에 리포트 저장** 설정으로 공유 폴더의 UNC 경로를 지정하는 경우에는 이 폴더 접근을 위한 사용자 계정과 암호를 지정해야 합니다.

  이 옵션이 비활성화되어 있으면 리포트는 중앙 관리 서버 계정으로 폴더에 저장됩니다.

  이 확인란은 **폴더에 리포트 저장** 확인란이 선택되어 있는 경우에 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

보고서를 XLS 파일로 저장하거나 보낼 때 로고 및 데이터그램과 같은 모든 관련 이미지는 별도의 파일로 저장됩니다.

다음을 눌러 다음 단계로 진행합니다.

4단계. 작업을 시작할 계정 선택

작업을 실행할 계정 선택 창에서 작업 실행 시 사용할 계정을 지정할 수 있습니다. 다음 옵션 중 하나를 선택합니다:

- **기본 계정**

  해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **계정 지정**

  계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

  - **계정**

    작업 실행에 사용되는 계정입니다.

- **암호**

  작업을 실행할 계정의 암호입니다.

다음을 눌러 다음 단계로 진행합니다.

5단계. 작업 스케줄 구성

작업 스케줄 구성 마법사 페이지에서는 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 구성합니다.

- **시작 스케줄:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

    작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

  - **N일마다**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

    기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **N주마다**

    작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

    기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

  - **N분마다**

    작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

    기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

  - **매일(서머타임 지원 안 함)**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

    이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

    기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

- **주별**

  이 작업은 매주 지정한 요일의 지정된 시간에 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

6단계. 작업 이름 정의

작업 이름 정의 창에서 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자(`"*<>?\:|`)를 사용할 수 없습니다.

다음을 눌러 다음 단계로 진행합니다.

7단계. 작업 생성 완료

작업 생성 마침 창에서 **마침** 버튼을 눌러 마법사를 완료합니다.

마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

통계 관리

보호 시스템 및 관리 중인 기기의 상태에 대한 통계는 사용자 지정 가능한 정보 패널에 표시됩니다. 통계는 **중앙 관리 서버** 노드 작업 영역의 **통계** 탭에 표시됩니다. 이 탭에는 여러 탭(페이지)이 포함되어 있습니다. 각각의 페이지에는 통계 정보 패널을 비롯하여 Kaspersky의 기업 관련 뉴스 및 기타 자료 링크가 표시됩니다. 통계 정보는 표나 차트(파이 또는 막대)로 정보 패널에 표시됩니다. 정보 패널의 데이터는 애플리케이션이 실행되는 동안 보호 애플리케이션의 현재 상태를 반영하여 업데이트됩니다.

통계 탭의 두 번째 수준 탭 집합, 각 탭 페이지의 정보 패널 수 및 정보 패널의 데이터 표시 모드를 변경할 수 있습니다.

***통계** 탭에 정보 패널이 있는 두 번째 수준의 새 탭을 추가하려면:*

1. **통계** 탭의 오른쪽 위에 있는 **사용자 지정 보기** 버튼을 누릅니다.

   통계 속성 창이 열립니다. 이 창에는 **통계** 탭에 현재 표시된 탭 페이지 목록이 있습니다. 이 창에서 **속성** 버튼을 눌러 탭에 있는 페이지의 표시 순서를 변경하고 페이지를 추가 및 제거하며 페이지 속성 구성을 진행할 수 있습니다.

2. **추가** 버튼을 누릅니다.

   이것은 새 페이지 속성 창을 엽니다.

3. 새 페이지 구성하기:

   - **일반** 섹션에서 페이지 이름을 지정합니다.
   - **정보 패널** 섹션에서 **추가** 버튼을 눌러 해당 페이지에서 표시되어야 하는 정보 패널을 추가합니다.

     패널에 대한 이름, 유형, 차트 유형을 비롯하여 차트 설정에 사용되는 데이터 등 추가한 정보 패널의 속성을 설정하려면 **정보 패널** 섹션에 있는 **속성** 버튼을 누릅니다.

4. **확인**를 누릅니다.

추가한 정보 패널이 있는 탭 페이지는 **통계** 탭에 나타납니다. 설정 아이콘( )을 눌러 바로 페이지 구성이나 해당 페이지의 선택한 정보 패널 구성을 진행할 수 있습니다.

이벤트 알림 구성

Kaspersky Security Center에서는 클라이언트 기기에서 발생하는 이벤트를 관리자에게 알리기 위한 방법을 선택하고 알림을 구성할 수 있습니다:

- 이메일. 이벤트가 발생하면 애플리케이션이 지정된 이메일 주소로 알림을 보냅니다. 알림 텍스트는 편집할 수 있습니다.
- SMS. 이벤트가 발생하면 애플리케이션이 지정된 전화 번호로 알림을 보냅니다. 메일 게이트웨이를 통해 SMS 알림을 보내도록 구성할 수 있습니다.
- 실행 파일. 기기에서 이벤트가 발생하면 관리자 워크스테이션에서 실행 파일이 시작됩니다. 관리자는 이 실행 파일을 사용하여 발생한 이벤트의 파라미터를 받을 수 있습니다.

클라이언트 기기에서 발생하는 이벤트의 알림을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **알림 구성 및 이벤트 내보내기** 링크를 누르고 드롭다운 목록에서 **알림 구성** 값을 선택합니다.
   그러면 **속성: 이벤트** 창이 열립니다.
4. **알림** 섹션에서 알림 방법을 선택(이메일, 문자 또는 실행 파일 실행)하고 알림 설정을 정의합니다:
   - **이메일**

     이메일 탭에서 이메일로 이벤트 알림을 구성할 수 있습니다.

     받는 사람(이메일 주소) 필드에서 애플리케이션이 알림을 보낼 이메일 주소를 지정합니다. 이 필드에서 세미콜론으로 구분해 여러 주소를 지정할 수 있습니다.

     SMTP 서버 필드에서 세미콜론으로 구분해 이메일 서버 주소를 지정합니다. 다음 값을 사용할 수 있습니다:
     - IPv4 또는 IPv6 주소
     - 기기의 Windows 네트워크 이름(NetBIOS 이름)
     - SMTP 서버의 DNS 이름

     SMTP 서버 포트 필드에서 SMTP 서버 통신 포트의 번호를 지정합니다. 기본 포트 번호는 25입니다.

     DNS MX 룩업 사용 옵션을 활성화하면 SMTP 서버의 동일한 DNS 이름에 대해 IP 주소의 여러 MX 레코드를 사용할 수 있습니다. 동일한 DNS 이름에는 이메일 메시지 수신 우선 순위 값이 다른 여러 MX 레코드가 있을 수 있습니다. 중앙 관리 서버는 MX 레코드 우선 순위의 오름차순으로 SMTP 서버에 이메일 알림을 보내려고 시도합니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

     DNS MX 룩업 사용 옵션을 활성화하고 TLS 설정을 활성화하지 않는 경우에는 이메일 알림 전송을 위한 ㅜ가 보호 수단으로 서버 기기에 DNSSEC 설정을 사용하는 것이 좋습니다.

설정 링크를 눌러 추가 알림을 설정:

- 도메인 이름(이메일 메시지의 도메인 이름)
- 발신자 이메일 주소
- ESMTP 인증 설정

SMTP 서버에 대한 ESMTP 인증 옵션이 활성화된 경우 SMTP 서버에서 인증용 계정을 지정해야 합니다.

- SMTP 서버에 대한 TLS 설정:
  - **TLS 사용하지 않음**

    이메일 메시지 암호화를 비활성화하려는 경우 이 옵션을 선택할 수 있습니다.
  - **SMTP 서버에서 지원 시 TLS 사용**

    SMTP 서버에 대한 TLS 연결을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 TLS를 사용하지 않고 SMTP 서버에 연결합니다.
  - **항상 TLS 사용, 서버 인증서 유효성 확인**

    TLS 인증 설정을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 SMTP 서버에 연결할 수 없습니다.

SMTP 서버와의 연결을 보다 잘 보호하려면 이 옵션을 사용하는 것이 좋습니다. 이 옵션을 선택하면 TLS 연결에 대한 인증 설정을 설정할 수 있습니다.

항상 TLS를 사용하고 서버 인증서의 유효성을 확인하십시오 값을 선택한 경우에는 SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

다음과 같이 SMTP 서버에 대한 TLS 설정을 지정할 수 있습니다.

- 다음 SMTP 서버 인증서 파일을 찾습니다.

신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 중앙 관리 서버에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

- 다음과 같이 클라이언트 인증서 파일을 찾습니다.

신뢰할 수 있는 인증 기관과 같은 다양한 출처에서 수신된 인증서를 사용할 수 있습니다. 다음 인증서 유형 중 하나를 사용하여 인증서와 개인 키를 지정해야 합니다:

- X-509 인증서:

인증서가 있는 파일과 개인 키가 있는 파일을 지정해야 합니다. 두 파일은 서로 의존하지 않으며 파일의 로딩 순서는 중요하지 않습니다. 두 파일이 모두 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

- pkcs12 컨테이너:

인증서와 개인 키가 포함 된 단일 파일을 업로드해야 합니다. 파일이 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

알림 메시지 필드는 이벤트가 일어날 때 애플리케이션이 보내는 해당 이벤트에 대한 정보의 표준 문구를 포함하고 있습니다. 이 문구에는 이벤트 이름, 기기 이름 및 도메인 이름과 같은 대체 파라미터가 포함됩니다. 해당 이벤트에 더 많은 관련 세부 사항을 포함하고 있는 다른 대체 파라미터를 추가해 메시지 문구를 편집할 수 있습니다. 필드의 오른쪽에 있는 버튼을 누르면 대체 파라미터 목록을 이용할 수 있습니다.

만일 알림 텍스트가 % 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 입력해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

테스트 메시지 전송 버튼을 눌러 알림을 올바르게 구성했는지 확인하십시오. 애플리케이션은 지정한 이메일 주소로 테스트 알림을 보내야 합니다.

- SMS

SMS 탭은 휴대폰으로 여러 이벤트에 대한 SMS 알림 전송 구성을 허용합니다. SMS 메시지는 메일 게이트웨이를 통해 전송됩니다.

받는 사람(이메일 주소) 필드에서 애플리케이션이 알림을 보낼 이메일 주소를 지정합니다. 이 필드에서 세미콜론으로 구분해 여러 주소를 지정할 수 있습니다. 지정한 이메일 주소와 연결된 전화 번호로 알림이 전달됩니다.

SMTP 서버 필드에서 세미콜론으로 구분해 이메일 서버 주소를 지정합니다. 다음 값을 사용할 수 있습니다:

- IPv4 또는 IPv6 주소
- 기기의 Windows 네트워크 이름(NetBIOS 이름)
- SMTP 서버의 DNS 이름

SMTP 서버 포트 필드에서 SMTP 서버 통신 포트의 번호를 지정합니다. 기본 포트 번호는 25입니다.

설정 링크를 눌러 추가 알림을 설정:

- 도메인 이름(이메일 메시지의 도메인 이름)
- 발신자 이메일 주소
- ESMTP 인증 설정

필요할 시 SMTP 서버에 대해 ESMTP 인증 옵션이 활성화된 경우 SMTP 서버에서 인증을 위한 계정을 지정할 수 있습니다.

- SMTP 서버에 대한 TLS 설정

TLS 사용을 비활성화하거나, SMTP 서버가 이 프로토콜을 지원하는 경우 TLS를 사용하거나 또는 TLS만 사용하도록 강제할 수 있습니다. TLS만 사용하도록 선택한 경우에는 SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, TLS만 사용하도록 선택한 경우 SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

- SMTP 서버 인증서 파일 찾아보기

신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 Kaspersky Security Center에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

인증서와 개인 키가 포함 된 단일 파일을 업로드해야 합니다. 파일이 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다. **알림 메시지** 필드는 이벤트가 발생할 때 애플리케이션이 보내는 해당 이벤트에 대한 정보의 표준 문구를 포함하고 있습니다. 이 문구에는 이벤트 이름, 기기 이름 및 도메인 이름과 같은 대체 파라미터가 포함됩니다. 해당 이벤트에 더 많은 관련 세부 사항을 포함하고 있는 다른 대체 파라미터를 추가해 메시지 문구를 편집할 수 있습니다. 필드의 오른쪽에 있는 버튼을 누르면 대체 파라미터 목록을 이용할 수 있습니다.

만일 알림 텍스트가 % 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 입력해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

Configure numeric limit of notifications 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

알림이 제대로 구성되었는지 확인하려면 **테스트 메시지 전송** 버튼을 클릭합니다. 애플리케이션은 지정한 수신자에게 테스트 알림을 보내야 합니다.

- **실행되는 실행 파일**

  이 알림 방법을 선택하면 입력 필드에 이벤트가 발생할 때 시작되는 애플리케이션을 지정할 수 있습니다.

  알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격에서 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

  테스트 메시지 전송을 누르면 알림을 제대로 구성했는지 확인할 수 있습니다: 애플리케이션은 지정한 이메일 주소로 테스트 알림을 보냅니다.

5. **알림 메시지** 필드에서 이벤트가 발생할 때 애플리케이션이 보낼 문구를 입력합니다.

   이벤트 상세 정보(예: 이벤트 설명, 발생 시기 등)와 함께 대체 설정을 추가하기 위해 텍스트 필드의 오른쪽에 있는 드롭다운 목록을 사용할 수 있습니다.

   만일 알림 텍스트가 퍼센트(%) 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 지정해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

6. 알림이 제대로 구성되었는지 확인하려면 **테스트 메시지 전송** 버튼을 누릅니다.

   애플리케이션은 지정된 사용자에게 테스트 알림을 전송합니다.

7. **확인**을 눌러 변경을 저장합니다.

클라이언트 기기에서 발생하는 모든 이벤트에 새롭게 조정된 알림 설정이 적용됩니다.

중앙 관리 서버 설정, 정책 설정 또는 애플리케이션 설정의 **이벤트 구성** 섹션에서 특정 이벤트에 대한 알림 설정을 재정의할 수 있습니다.

SMTP 서버용 인증서 발급

SMTP 서버용 인증서를 발급하려면:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **알림 구성 및 이벤트 내보내기** 링크를 누르고 드롭다운 목록에서 **알림 구성** 값을 선택합니다.

   이벤트 속성 창이 열립니다.

4. **이메일** 탭에서 **설정** 링크를 눌러 **설정** 창을 엽니다.

5. **설정** 창에서 **인증서 지정** 링크를 눌러 **서명용 인증서** 창을 엽니다.

6. **서명용 인증서** 창에서 **찾기** 버튼을 누릅니다.
   인증서 창이 열립니다.

7. **인증서 유형** 드롭다운 목록에서 인증서 유형을 공개 또는 개인으로 지정합니다.

   - 개인 인증서 유형(**PKCS #12 컨테이너**)을 선택하면 인증서 파일과 암호를 지정합니다.
   - 공개 인증서 유형(**X.509 인증서**)을 선택하는 경우:

     a. 개인 키 파일을 지정합니다(*.prk 또는 *.pem 확장자).

     b. 개인 키 암호를 지정합니다.

     c. 공개 키 파일을 지정합니다(*.cer 확장자).

8. **확인**를 누릅니다.

SMTP 서버용 인증서가 발급됩니다.

이벤트 조회

Kaspersky Security Center 동작과 관리 중인 애플리케이션에 있는 이벤트에 대한 정보는 Microsoft Windows 시스템 로그와 중앙 관리 서버 데이터베이스에 모두 저장됩니다. **이벤트** 탭의 **중앙 관리 서버** 노드의 작업 영역에서 중앙 관리 서버 데이터베이스의 정보를 볼 수 있습니다.

이벤트 탭의 정보는 이벤트 조회 목록으로 표시됩니다. 각 조회에는 특정 유형에 대한 이벤트만 들어 있습니다. 예를 들어, "기기 상태 심각" 섹션에는 기기 상태가 "심각"으로 기록된 것만 표시됩니다. 애플리케이션을 설치하면 **이벤트** 탭에 몇 가지 표준 이벤트 조회가 포함됩니다. 추가(사용자지정) 이벤트 조회를 만들거나 이벤트 정보를 파일로 내보낼 수 있습니다.

이벤트 조회 보기

이벤트 조회를 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.

2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.

3. **이벤트 선택** 드롭다운 목록에서 관련 이벤트 조회를 선택합니다.
   이 조회에 대한 이벤트를 계속 작업 영역에 표시하려면 조회 옆에 있는 별 아이콘(☆)을 클릭합니다.

작업 영역에 중앙 관리 서버에 저장되어 있는 선택한 유형의 이벤트 목록이 표시됩니다.

필요한 열에서 이벤트 목록의 정보를 오름차순 또는 내림차순으로 정렬할 수 있습니다.

이벤트 조회 사용자정의

이벤트 조회 사용자 지정하려면:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **이벤트** 탭에서 관련 이벤트 조회를 엽니다.
4. **선택 속성** 버튼을 누릅니다.

   열리는 이벤트 조회 속성 창에서 이벤트 조회를 구성할 수 있습니다.

이벤트 조회 만들기

이벤트 조회를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **새 선택 항목 생성** 버튼을 누릅니다.
4. 열리는 **새 이벤트 선택** 창에 새 이벤트 선택의 이름을 입력하고 **확인**을 누릅니다.

   사용자가 지정한 이름의 조회가 **이벤트 선택** 드롭다운 목록에 생성됩니다.

기본적으로 만들어진 이벤트 조회에는 중앙 관리 서버에 저장된 모든 이벤트가 포함됩니다. 조회에서 원하는 이벤트만 표시되도록 하려면 조회를 사용자 지정해야 합니다.

이벤트 조회를 텍스트 파일로 내보내기

이벤트 조회를 텍스트 파일로 내보내려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **가져오기/내보내기** 버튼을 누릅니다.
4. 드롭다운 목록에서 **이벤트를 파일로 내보내기**를 선택합니다.

   이벤트 내보내기 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

조회에서 이벤트 삭제

조회에서 이벤트를 삭제하려면:

1. 콘솔 트리에서 관련 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. 마우스의 **SHIFT** 또는 **CTRL** 키를 사용하여 삭제할 이벤트를 선택합니다.
4. 다음 방법 중 하나로 선택 이벤트를 삭제합니다:
   - 선택한 이벤트의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.

     마우스 오른쪽 메뉴에서 **모두 삭제** 항목을 선택하면, 삭제할 이벤트의 선택에 관계없이 표시된 모든 이벤트가 조회에서 삭제됩니다.
   - 해당 이벤트의 정보 박스에서 하나의 이벤트를 선택한 경우에는 **이벤트 삭제** 링크를 누르고, 여러 개를 선택한 경우에는 **이벤트 삭제** 링크를 누릅니다.

선택한 이벤트가 삭제됩니다.

사용자 요청에 따라 예외에 애플리케이션 추가

잘못 차단된 애플리케이션의 차단을 해제해 달라는 사용자 요청을 받으면 이러한 애플리케이션에 대해 적응형 보안 규칙에서 예외를 생성할 수 있습니다. 그러면 해당 애플리케이션이 사용자 기기에서 더 이상 차단되지 않습니다. 중앙 관리 서버의 **모니터링** 탭에서 사용자 요청 수를 추적할 수 있습니다.

사용자 요청에 따라 Kaspersky Endpoint Security에서 차단한 애플리케이션을 예외에 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 영역에서 **이벤트** 탭을 엽니다.
3. **이벤트 선택** 드롭다운 목록에서 **사용자 개선 요청 사항**를 선택합니다.
4. 예외에 추가할 애플리케이션이 포함된 하나 또는 여러 개의 사용자 요청을 마우스 오른쪽 버튼으로 누르고 **예외 추가**를 선택합니다.

   예외 추가 마법사가 시작됩니다. 해당 지침을 따릅니다.

선택한 애플리케이션은 중앙 관리 서버와 클라이언트 기기의 다음 동기화 이후에 콘솔 트리의 **저장소** 아래 **스마트 학습 상태에서 트리거된 규칙** 목록에서 제외되며 목록에 더 이상 표시되지 않습니다.

기기 조회

기기 상태에 대한 정보는 콘솔 트리의 **기기 선택** 폴더에 표시됩니다.

기기 선택 폴더의 정보는 기기 조회 목록으로 표시됩니다. 각 조회에는 특정 조건을 충족하는 기기가 포함됩니다. 예를 들어 **심각 상태의 기기** 조회에는 *심각* 상태의 기기만 포함됩니다. 애플리케이션을 설치하면, **기기 선택** 폴더에 몇 가지 표준 조회가 포함됩니다. 기기 조회를 추가로 만들거나 조회 설정을 파일로 내보내거나 다른 파일에서 가져온 설정으로 조회 항목을 만들 수 있습니다.

기기 조회 보기

기기 조회를 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 선택** 폴더를 선택합니다.
2. 폴더의 작업 영역에 있는 **다음 선택에 해당하는 기기 -** 목록에서 관련된 기기 조회 항목을 선택합니다.
3. **선택 실행** 버튼을 누릅니다.
4. **선택 결과** 탭을 클릭합니다.

작업 영역에 조회 기준을 만족하는 기기 목록이 표시됩니다.

필요한 열에서 기기 목록의 정보를 오름차순 또는 내림차순으로 정렬할 수 있습니다.

기기 조회 구성

기기 조회를 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 선택** 폴더를 선택합니다.
2. 작업 영역에서 **선택** 탭을 누른 다음 사용자 지정 조회 목록에서 관련 기기 조회 항목을 누릅니다.
3. **선택 속성** 버튼을 누릅니다.
4. 열리는 속성 창에서 다음 설정을 구성하십시오:
   - 일반 조회 속성.
   - 이 조회에 기기를 포함하려면 충족해야 하는 조건입니다. 조건 이름을 선택하고 **속성** 버튼을 눌러 조건을 구성할 수 있습니다.
   - 보안 설정.
5. **확인**를 누릅니다.

   설정이 적용되고 저장됩니다.

아래에서는 조회에 기기를 할당하기 위한 조건에 대해 설명합니다. OR 논리자를 이용한 조건: 조회에는 나열된 조건 중 하나 이상을 만족시키는 기기가 모두 포함됩니다.

일반

일반 섹션에서 조회 조건의 이름을 변경하고 조건이 반전되어야 하는지 여부를 지정할 수 있습니다.

선택 조건 반전

기본적으로 이 옵션은 비활성화되어 있습니다.

이 옵션을 활성화하면 지정된 선택 조건이 반대로 적용됩니다. 즉, 조건을 충족하지 않는 모든 기기가 조회에 포함됩니다.

다음 예는 반전 작업의 논리를 보여줍니다.

- **조건** : 사용자의 기기에 유형이 Linux이고 빌드 번호가 00.0.000인 운영 체제가 있습니다.
- **반전된 조건**: 사용자의 기기에 조건이 (Linux 유형 및 빌드 번호가 00.0.000) 아닌 운영 체제가 있으며, 이는 다음에 해당합니다.

  유형이 Linux가 아니거나 빌드 번호가 00.0.000이 아닌 운영 체제가 있습니다.

따라서 선택에는 예를 들어 Windows 유형과 빌드 번호 00.0.000 또는 Linux 유형과 빌드 번호 00.0.000 이외의 운영 체제가 있는 기기가 포함됩니다.

네트워크

네트워크 섹션에서는 네트워크 데이터에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

- **기기 이름 또는 IP 주소**

  기기의 Windows 네트워크 이름(NetBIOS 이름) 또는 IPv4 또는 IPv6 주소.

- **Windows 도메인**

  지정된 Windows 도메인에 포함된 모든 기기를 표시합니다.

- **관리 그룹**

  지정된 관리 그룹에 포함된 기기를 표시합니다.

- **설명**

  기기 속성 창의 텍스트: **일반** 섹션의 **설명** 필드.
  설명 필드에서 텍스트를 설명하기 위해 다음 문자를 사용할 수 있습니다.
  - 한 단어 내에서 찾으려면 다음과 같이 하십시오:
    - ***.** 임의 개수의 문자열을 대체합니다.

    예:
    Server 또는 **Server's** 라는 단어를 설명하려면 **Server***를 입력하면 됩니다.
    - **?.** 표시는 단일 문자를 대체합니다.

    예:
    Window, **Windows** 등의 단어를 설명하려는 경우 **Windo?**를 입력하면 됩니다.
    별표(*) 또는 물음표(?)는 쿼리의 첫 문자로 사용할 수 없습니다.

- 여러 단어를 찾으려면 다음과 같이 하십시오:
  - 공백. 나열된 단어의 어느 하나라도 설명에 포함된 모든 기기가 표시됩니다.

  예:

  설명에 **Secondary** 또는 **Virtual**이라는 단어가 포함된 문구를 찾으려면 쿼리에 **Secondary Virtual**을 입력하면 됩니다.

  - **+**. 단어 앞에 더하기 기호를 입력하면 모든 검색 결과에 해당 단어가 포함됩니다.

  예:

  Secondary 및 **Virtual**이 모두 포함된 문구를 찾으려면 **+Secondary+Virtual** 쿼리를 입력합니다.

  - **-**. 단어 앞에 빼기 기호를 입력하면 검색 결과에 해당 단어가 포함되지 않습니다.

  예:

  Secondary를 포함하고 **Virtual**은 포함하지 않는 문구를 찾으려면 **+Secondary-Virtual** 쿼리를 입력합니다.

  - **"<텍스트>"**. 따옴표에 둘러싸인 텍스트가 검색 결과의 텍스트에 포함됩니다.

  예:

  Secondary Server의 단어 조합을 포함하는 문구를 찾으려면 쿼리에 **"Secondary Server"**를 입력하면 됩니다.

- **IP 범위**

  이 옵션을 사용하면 관련 기기가 포함되어야 하는 IP 범위의 첫 IP 주소와 마지막 IP 주소를 입력할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

태그

태그 섹션에서는 이전에 관리 중인 기기 설명에 추가한 키워드(태그)를 기준으로 하여 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **하나 이상의 지정 태그가 일치하면 적용**

  이 옵션을 사용하면 검색 결과에는 선택한 태그 중 적어도 하나와 일치하는 설명이 있는 기기가 표시됩니다.

  이 옵션이 비활성화되어 있으면 검색 결과에는 모든 선택한 태그와 일치하는 설명이 있는 기기만 표시됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **태그를 포함해야 함**

  이 옵션을 선택하는 경우 설명에 선택한 태그가 포함되어 있는 기기가 검색 결과에 표시됩니다. 기기를 찾으려는 경우 문자 수에 관계 없이 임의의 문자열을 나타내는 별표를 사용할 수 있습니다.

기본적으로 이 옵션은 선택되어 있습니다.

- **태그를 제외해야 함**

  이 옵션을 선택하는 경우 설명에 선택한 태그가 포함되어 있지 않은 기기가 검색 결과에 표시됩니다. 기기를 찾으려는 경우 문자 수에 관계 없이 임의의 문자열을 나타내는 별표를 사용할 수 있습니다.

Active Directory

Active Directory 섹션에서는 Active Directory 데이터에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **기기가 Active Directory 조직 구성 단위에 있습니다**

  이 옵션을 사용하면 입력 필드에 지정한 Active Directory 조직 구성 단위의 기기가 조회에 포함됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **하위 조직 구성 단위까지 포함**

  이 옵션을 선택하면 지정한 도메인 조직 구성 단위의 모든 하위 조직 구성 단위에 있는 기기가 선택에 포함됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **이 기기는 Active Directory 그룹의 멤버입니다**

  이 옵션을 사용하면 입력 필드에 지정한 Active Directory 그룹의 기기가 조회에 포함됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

네트워크 활동

네트워크 활동 섹션에서는 네트워크 활동에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

- **이 기기는 배포 지점입니다**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 배포 지점 역할을 하는 기기가 조회에 포함됩니다.
  - **아니요**. 배포 지점 역할을 하는 기기가 조회에 포함되지 않습니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **중앙 관리 서버와 계속 연결 유지**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **활성화됨**. 조회에 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택한 기기가 포함됩니다.
  - **비활성화됨**. 조회에 **중앙 관리 서버와 계속 연결 유지** 확인란의 선택을 취소한 기기가 포함됩니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **연결 프로필이 전환됨**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 연결 프로필이 전환된 후 중앙 관리 서버에 연결된 기기가 조회에 포함됩니다.
  - **아니요**. 연결 프로필이 전환된 후 중앙 관리 서버에 연결된 기기가 조회에 포함되지 않습니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **마지막 중앙 관리 서버 연결**

  이 확인란을 이용해 중앙 관리 서버에 마지막으로 연결한 시간에 따라 기기를 검색하는 기준을 설정할 수 있습니다.

  이 확인란을 선택하면 입력 필드에서 클라이언트 기기에 설치된 네트워크 에이전트와 중앙 관리 서버 간에 마지막으로 연결이 설정된 기간(날짜 및 시간)을 지정할 수 있습니다. 지정된 간격 내에 있는 기기가 조회에 포함됩니다.

  이 확인란이 비어 있으면, 기준은 적용되지 않습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **네트워크 검색 중 탐지된 새 기기**

  지난 며칠 동안 네트워크 검색을 통해 탐지된 새 기기를 검색합니다.

  이 옵션을 사용하면 **탐지 기간(일)** 필드에 지정된 기간 동안 기기 발견에서 탐지된 새 기기만 선택에 포함됩니다.

  이 옵션이 비활성화되어 있으면 선택에는 기기 발견에서 탐지된 모든 기기가 포함됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **기기 존재 확인**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 애플리케이션이 현재 네트워크에서 표시되는 기기를 조회에 포함시킵니다.
  - **아니요**. 애플리케이션이 현재 네트워크에 표시되지 않는 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

애플리케이션 섹션에서는 선택한 관리 중인 애플리케이션에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **애플리케이션 이름**

  Kaspersky 애플리케이션 이름별로 검색 수행 시 조회에 포함될 기기의 기준을 드롭다운 목록에서 지정할 수 있습니다.

  이 목록에는 관리자의 워크스테이션에서 관리 플러그인이 설치된 애플리케이션 이름만 표시됩니다.

  애플리케이션을 선택하지 않았다면, 이 기준은 적용되지 않습니다.

- **애플리케이션 버전**

  Kaspersky 애플리케이션 버전 이름별로 검색 수행 시 조회에 포함될 기기의 기준을 입력 필드에서 지정할 수 있습니다.

  버전 번호가 지정되지 않으면 기준이 적용되지 않습니다.

- **긴급 업데이트 이름**

  입력 필드에서 애플리케이션 이름 또는 업데이트 패키지 번호로 검색 수행 시 조회에 포함될 기기의 기준을 지정할 수 있습니다.

  필드를 비워두면 기준이 적용되지 않습니다.

- **마지막 모듈 업데이트**

  이 설정을 사용해 기기에 설치된 애플리케이션 모듈의 마지막 업데이트 시간으로 기기를 검색하기 위한 기준을 설정할 수 있습니다.

  이 확인란을 선택하면 입력 필드에서 기기에 설치된 애플리케이션 모듈의 마지막 업데이트가 수행된 시간 간격(날짜와 시간)을 지정할 수 있습니다.

  이 확인란이 비어 있으면, 기준은 적용되지 않습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **Kaspersky Security Center로 기기를 관리 중입니다**

  드롭다운 목록에서는 Kaspersky Security Center를 통해 관리되는 기기를 조회에 포함할 수 있습니다:

  - **예**. 애플리케이션이 Kaspersky Security Center를 통해 관리 중인 기기를 조회에 포함합니다.
  - **아니요**. 애플리케이션이 Kaspersky Security Center를 통해 관리되지 않는 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **보안 제품이 설치되어 있음**

  드롭다운 목록에서는 보안 제품이 설치된 모든 기기를 조회에 포함할 수 있습니다:
  - **예**. 애플리케이션이 보안 제품이 설치된 모든 기기를 조회에 포함합니다.
  - **아니요**. 애플리케이션이 보안 제품이 설치되지 않은 모든 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

운영 체제

운영 체제 섹션에서는 운영 체제 유형에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

- **운영 체제 버전**

  확인란을 선택하면 목록에서 운영 체제를 선택할 수 있습니다. 지정한 운영 체제가 설치된 기기가 검색 결과에 포함됩니다.

- **운영 체제 비트 크기**

  드롭다운 목록에서 운영 체제의 아키텍처를 선택할 수 있습니다. 선택한 아키텍처(**알 수 없음**, **x86**, **AMD64** 또는 **IA64**)에 따라 이동 규칙이 기기에 적용되는 방법이 결정됩니다. 기본적으로 목록에서 선택된 옵션은 없기 때문에 운영 체제 아키텍처는 정의되지 않게 됩니다.

- **운영 체제 서비스 팩 버전**

  이 필드에서는 사용자 운영 체제의 패키지 버전을 *X.Y* 형식으로 지정할 수 있습니다. 지정한 버전에 따라 이동 규칙이 장치에 적용되는 방법이 결정됩니다. 기본적으로 버전 값은 지정되지 않습니다.

- **운영 체제 빌드**

  > 이 설정은 Windows 운영 체제에만 적용됩니다.

  운영 체제의 빌드 번호입니다. 선택한 운영 체제의 빌드 번호가 이 번호와 같아야 하는지 아니면 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 빌드 번호를 제외한 모든 빌드 번호를 검색하도록 구성할 수도 있습니다.

- **운영 체제 릴리즈 ID**

  > 이 설정은 Windows 운영 체제에만 적용됩니다.

  운영 체제의 릴리즈 식별자(ID)입니다. 선택한 운영 체제의 릴리즈 ID가 이 ID와 같아야 하는지 아니면 이전/이후 ID여야 하는지를 지정할 수 있습니다. 지정한 릴리즈 ID 번호를 제외한 모든 번호를 검색하도록 구성할 수도 있습니다.

기기 상태

기기 상태 섹션에서는 관리 중인 애플리케이션의 기기 상태 설명에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **기기 상태**

  정상, *심각* 또는 *경고* 기기 상태 중 하나를 선택할 수 있는 드롭다운 목록입니다.

- **기기 상태 설명**

  이 필드에서는 조건 옆의 확인란을 선택할 수 있습니다. 이러한 조건이 충족되면 *정상*, *심각* 또는 *경고* 상태 중 하나가 기기에 할당됩니다.

- **애플리케이션에서 정의된 기기 상태**

  실시간 보호 상태를 선택할 수 있는 드롭다운 목록입니다. 지정된 실시간 보호 상태의 기기가 조회에 포함됩니다.

보호 구성 요소

보호 구성 요소 섹션에서는 보호 상태에 따라 조회에 기기를 포함하기 위한 기준을 설정할 수 있습니다.

- **데이터베이스 배포 날짜**

  이 옵션을 선택하면 안티 바이러스 데이터베이스 배포 날짜를 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에 수행하려는 검색을 기반으로 기간을 설정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **마지막 검사**

  이 확인 옵션을 사용하면 마지막 악성 코드 검사 시간을 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에서 마지막 악성 코드 검사가 수행된 시간을 지정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **탐지된 위협 전체 개수**

  이 옵션을 사용하면 탐지된 바이러스 수를 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에 탐지된 바이러스 수에 대한 상한 및 하한 임계값을 설정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

자산 관리(소프트웨어) 섹션에서는 설치된 애플리케이션에 따라 기기 검색을 위한 기준을 설정할 수 있습니다.

- **애플리케이션 이름**

  애플리케이션을 선택할 수 있는 드롭다운 목록입니다. 지정된 애플리케이션이 설치된 기기가 조회에 포함됩니다.

- **애플리케이션 버전**

  선택한 애플리케이션의 버전을 지정할 수 있는 입력 필드입니다.

- **공급사**

  기기에 설치된 애플리케이션의 제조업체를 선택할 수 있는 드롭다운 목록입니다.

- **애플리케이션 상태**

  애플리케이션의 상태(*설치됨*, *설치 안 됨*)를 선택할 수 있는 드롭다운 목록입니다. 지정된 애플리케이션이 설치되어 있거나 설치되어 있지 않은 기기는 선택한 상태에 따라 조회에 포함됩니다.

- **업데이트로 찾기**

  이 옵션을 사용하면 관련 기기에 설치된 애플리케이션의 업데이트 세부 정보를 사용하여 검색이 수행됩니다. 확인란을 선택하면 **애플리케이션 이름**, **애플리케이션 버전** 및 **애플리케이션 상태** 필드가 각각 **업데이트 이름**, **업데이트 버전** 및 **상태**로 변경됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **비호환 보안 제품 이름**

  타사의 보안 제품을 선택할 수 있는 드롭다운 목록입니다. 검색 시 지정된 애플리케이션이 설치된 기기가 조회에 포함됩니다.

- **애플리케이션 태그**

  드롭다운 목록에서 애플리케이션 태그를 선택할 수 있습니다. 설명에 선택한 태그가 있는 애플리케이션이 설치된 모든 기기는 기기 조회에 포함됩니다.

- **지정한 태그가 없는 기기에 적용**

  이 옵션을 사용하면 선택에는 설명에 선택한 태그가 하나도 없는 기기가 포함됩니다.

  이 옵션을 비활성화하면 기준이 적용되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

자산 관리(하드웨어)

자산 관리(하드웨어) 섹션에서는 설치된 하드웨어에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **기기**

  드롭다운 목록에서 다음과 같은 유닛 유형을 선택할 수 있습니다. 이 유닛이 모든 기기가 검색 결과에 포함됩니다.

  이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **공급사**

  드롭다운 목록에서 유닛 제조업체의 이름을 선택할 수 있습니다. 이 유닛이 모든 기기가 검색 결과에 포함됩니다.

  이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **기기 이름**

  Windows 네트워크의 기기 이름. 지정된 이름을 가진 기기는 조회에 포함됩니다.

- **설명**

  기기 또는 하드웨어 유닛의 설명. 이 필드에서 지정된 설명에 해당하는 기기가 조회에 포함됩니다.

  모든 유형에서의 기기 설명은 해당 기기의 속성 창에 입력될 수 있습니다. 이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **기기 제조업체**

  기기 제조사 이름. 이 필드에서 지정된 제조업체가 만든 기기가 조회에 포함됩니다.

  기기의 속성 창에 제조사의 이름을 입력할 수 있습니다.

- **일련 번호**

  이 필드에서 지정된 일련번호를 가진 모든 하드웨어는 조회에 포함됩니다.

- **인벤토리 번호**

  이 필드에서 지정된 인벤토리 번호를 가진 기기는 조회에 포함됩니다.

- **사용자**

  이 필드에서 지정된 사용자의 모든 하드웨어는 조회에 포함됩니다.

- **위치**

  기기 또는 하드웨어의 위치(예, 본사 또는 지사). 이 필드에서 지정된 위치에 배포된 컴퓨터 또는 기타 기기는 조회에 포함됩니다.

  기기의 속성 창에서 모든 형식으로 기기의 위치를 설명할 수 있습니다.

- **CPU 주파수(MHz)**

  CPU 주파수 범위. 이러한 필드(포함)에 있는 주파수 범위와 일치하는 CPU를 가진 기기는 조회에 포함됩니다.

- **가상 CPU 코어**

  CPU에 있는 가상 코어의 숫자 범위. 이러한 필드(포함)에 있는 범위와 일치하는 CPU를 가진 기기는 조회에 포함됩니다.

- **하드 드라이브 용량(GB)**

  기기에 있는 하드 드라이브 용량 값의 범위입니다. 이러한 입력 필드(포함)에 있는 범위와 일치하는 하드 드라이브를 가진 기기는 조회에 포함됩니다.

- **RAM 크기(MB)**

  기기 RAM 크기에 대한 값 범위입니다. 이 입력 필드의 범위와 일치하는 RAM이 있는 기기(포괄적)가 선택 항목에 포함됩니다.

가상 컴퓨터

가상 컴퓨터 섹션에서는 기기가 가상 컴퓨터인지 아니면 가상 데스크톱 인프라(VDI)의 일부분인지에 따라 조회에 기기를 포함하기 위한 기준을 설정할 수 있습니다.

- **이것은 가상 컴퓨터입니다**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.

  - **중요하지 않음**.
  - **아니요**. 가상 컴퓨터가 아닌 기기를 찾습니다.
  - **예**. 가상 컴퓨터인 기기를 찾습니다.

- **가상 컴퓨터 유형**

  드롭다운 목록에서 가상 컴퓨터 제조업체를 선택할 수 있습니다.

  이것은 가상 컴퓨터입니다 드롭다운 목록에서 **예** 또는 **중요하지 않음** 값을 선택하면 이 드롭다운 목록을 사용할 수 있습니다.

- **가상 데스크톱 인프라 소속**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **중요하지 않음**.
  - **아니요**. VDI(Virtual Desktop Infrastructure)의 일부가 아닌 기기를 찾습니다.
  - **예**. VDI(가상 데스크톱 인프라)의 일부인 기기를 찾습니다.

취약점 및 업데이트

취약점 및 업데이트 섹션에서는 Windows 업데이트 경로에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

WUA가 중앙 관리 서버로 전환됨

드롭다운 목록에서 다음 검색 옵션 중 하나를 선택할 수 있습니다:
- **예**. 이 옵션을 선택하면 Windows 업데이트를 통해 중앙 관리 서버에서 업데이트를 받는 기기가 검색 결과에 포함됩니다.
- **아니요**. 이 옵션을 선택하면 Windows 업데이트를 통해 다른 경로에서 업데이트를 받는 기기가 결과에 포함됩니다.

사용자

사용자 섹션에서는 운영 체제에 로그인한 사용자 계정에 따라 조회에 기기를 포함하기 위한 기준을 설정할 수 있습니다.

- **시스템에 마지막으로 로그인한 사용자**

  이 옵션을 사용하면 **찾기** 버튼을 눌러 사용자 계정을 지정할 수 있습니다. 지정한 사용자가 시스템에 대해 마지막 로그온을 수행한 기기가 검색 결과에 포함됩니다.

- **시스템에 적어도 한 번 이상 로그인한 사용자**

  이 옵션을 사용하면 **찾기** 버튼을 눌러 사용자 계정을 지정할 수 있습니다. 지정한 사용자가 한 번 이상 시스템에 로그인한 기기가 검색 결과에 포함됩니다.

관리 중인 애플리케이션에서 발생한 문제점

관리 중인 애플리케이션에서 발생한 문제점 섹션에서는 관리 중인 애플리케이션이 탐지한 가능한 문제점 목록에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다. 조회한 문제 중 하나 이상이 존재하는 기기는 조회에 포함됩니다. 여러 애플리케이션에 해당되는 문제 하나를 조회할 경우 모든 목록에서 이 문제를 자동으로 조회하도록 할 수 있습니다.

기기 상태 설명

관리 중인 애플리케이션의 상태 설명에 대한 확인란을 선택할 수 있습니다. 이러한 상태 정보를 수신하면 해당 기기가 조회에 포함됩니다. 여러 애플리케이션에 해당되는 상태 하나를 조회할 경우 모든 목록에서 이 상태를 자동으로 조회하도록 할 수 있습니다.

관리 중인 애플리케이션의 구성 요소 상태

관리 중인 애플리케이션의 구성 요소 상태 섹션에서는 관리 중인 애플리케이션의 구성 요소 상태에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **데이터 유출 방지 상태**

  데이터 유출 방지 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **협업 서버 보호 상태**

  서버 협업 보호 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **메일 서버의 안티 바이러스 보호 상태**

  메일 서버 보호 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **Endpoint Sensor 상태**

  엔드포인트 센서 구성 요소 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)를 기준으로 기기를 검색합니다.

암호화

암호화 알고리즘

AES(Advanced Encryption Standard) 대칭 블록 암호화 알고리즘입니다. 드롭다운 목록에서 암호화 키 크기(56비트, 128비트, 192비트 또는 256비트)를 선택할 수 있습니다.

사용 가능한 값: *AES56*, *AES128*, *AES192* 및 *AES256*.

클라우드 세그먼트

클라우드 세그먼트 섹션에서는 개별 클라우드 세그먼트에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **기기가 클라우드 세그먼트에 있습니다**

  이 옵션을 사용하면 **찾기** 버튼을 눌러 검색할 세그먼트를 지정할 수 있습니다.

  자녀 개체 포함 옵션도 사용하는 경우 지정한 세그먼트의 모든 자녀 개체에서 검색이 실행됩니다.

  검색 결과에는 선택한 세그먼트의 기기만 포함됩니다.

- **API를 사용해 발견된 기기**

  드롭다운 목록에서 API 도구로 기기를 탐지할지 선택할 수 있습니다:

  - **AWS**. AWS API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 AWS 클라우드 환경에 있습니다.
  - **Azure**. Azure API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Azure 클라우드 환경에 있습니다.
  - **Google Cloud.** Google API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Google Cloud 환경에 있습니다.
  - **아니요**. AWS, Azure, Google API로 기기를 찾을 수 없으므로, 기기가 클라우드 환경 밖에 있거나 클라우드 환경 내에 있지만 어떠한 이유로 인해 API를 사용해 찾을 수 없습니다.
  - **값 없음**. 이 조건이 적용되지 않습니다.

애플리케이션 구성 요소

이 섹션에는 관리 콘솔에 해당 관리 플러그인이 설치되어 있는 애플리케이션 구성 요소 목록이 포함되어 있습니다.

애플리케이션 구성 요소 섹션에서는 선택한 애플리케이션을 지칭하는 구성 요소의 상태와 버전 번호에 따라 조회에 기기를 포함하기 위한 기준을 지정할 수 있습니다.

- **상태**

  애플리케이션이 중앙 관리 서버로 전송하는 구성 요소 상태에 따라 기기를 검색합니다. *기기에서 보내 온 데이터 없음*, *중지됨*, *시작 중*, *일시 중지됨*, *실행 중*, *오작동* 또는 *설치 안 됨* 상태 중 하나를 선택할 수 있습니다. 관리 중인 기기에 설치되어 있는 애플리케이션의 선택한 구성 요소 상태가 지정한 값이면 해당 기기가 기기 조회에 포함됩니다.

  애플리케이션에서 전송하는 상태:

  - *시작 중* - 구성 요소가 현재 초기화되고 있습니다.
  - *실행 중* - 구성 요소가 활성화되어 정상 작동하고 있습니다.
  - *일시 중지됨* - 구성 요소가 일시 중지되었습니다. 예를 들어 사용자가 관리 중인 애플리케이션에서 보호를 일시 중지했습니다.
  - *오작동* - 구성 요소 작동 중에 오류가 발생했습니다.
  - *중지됨* - 구성 요소가 비활성화되었으며 현재 작동하고 있지 않습니다.
  - *설치 안 됨* - 사용자가 애플리케이션의 사용자 지정 설치를 구성할 때 설치할 구성 요소를 선택하지 않았습니다.

  기기에서 보내 온 데이터 없음 상태는 다른 상태와 달리 애플리케이션에서 전송되지 않습니다. 이 옵션은 선택한 구성 요소 상태 관련 정보가 애플리케이션에 없음을 표시합니다. 예를 들어 선택한 구성 요소가 기기에 설치된 어떤 애플리케이션에도 속하지 않거나 기기가 꺼져 있으면 이 상태가 표시될 수 있습니다.

- **버전**

  목록에서 선택하는 구성 요소의 버전 번호에 따라 기기를 검색합니다. `3.4.1.0` 등의 버전 번호를 입력한 다음 선택한 구성 요소의 버전이 해당 번호와 같아야 하는지 아니면 그 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 버전을 제외한 모든 버전을 검색하도록 구성할 수도 있습니다.

기기 조회 설정을 파일로 내보내기

기기 조회 설정을 텍스트 파일로 내보내려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 선택** 폴더를 선택합니다.
2. 작업 영역의 **선택** 탭에서 사용자 지정 조회 목록에 있는 관련 기기 조회 항목을 클릭합니다.

   설정은 사용자가 만든 기기 조회에서만 내보낼 수 있습니다.

3. **선택 실행** 버튼을 누릅니다.
4. **선택 결과** 탭에서 **설정 내보내기** 버튼을 클릭합니다.
5. **다른 이름으로 저장** 창이 열리면 조회 설정 내보내기 파일의 이름을 지정하고 저장할 폴더를 선택한 후 **저장** 버튼을 누릅니다.

기기 조회 설정이 지정한 파일에 저장됩니다.

기기 조회 만들기

기기 조회를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 선택** 폴더를 선택합니다.
2. 폴더의 작업 영역에서 **고급**를 누르고 드롭다운 목록에서 **새 선택 항목 생성**을 선택합니다.
3. **새 기기 선택** 창이 열리면 새 조회의 이름을 입력하고 **확인**를 누릅니다.

입력한 이름의 새 폴더가 **기기 선택** 폴더의 콘솔 트리에 나타납니다. 기본적으로 새 기기 조회에는 조회가 만들어진 중앙 관리 서버의 관리 그룹에 포함된 모든 기기가 포함됩니다. 조회에서 특별히 관심이 있는 기기만 표시하려면 **선택 속성** 버튼을 눌러 조회를 구성합니다.

가져온 설정에 따라 기기 조회 만들기

가져온 설정에 따라 기기 조회를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 선택** 폴더를 선택합니다.
2. 폴더의 작업 영역에서 **고급** 버튼을 누르고 드롭다운 목록에서 **미리 만든 선택 파일에서 선택 항목 가져오기**를 선택합니다.
3. 열리는 창에서 조회 설정을 가져올 파일 경로를 지정합니다. **열기** 버튼을 누릅니다.

새 선택 항목이 **기기 선택** 폴더에 만들어집니다. 새 조회의 설정은 지정한 파일에서 가져옵니다.

새 선택라는 이름의 조회가 **기기 선택** 폴더에 이미 존재하면 **(<순차적 번호>)** 형식의 색인이 생성된 조회의 이름에 추가됩니다. 예: **(1)**, **(2)**.

조회된 관리 그룹에서 기기 제거

기기 조회를 설정할 때, 제거되어야 하는 기기를 관리 그룹으로 전환할 필요없이 이 조회에 있는 관리 그룹에서 기기를 제거할 수 있습니다.

관리 그룹에서 기기를 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 선택** 폴더를 선택합니다.
2. **Shift** 또는 **Ctrl** 키를 사용하여 삭제할 기기를 선택합니다.
3. 다음 방법 중 하나로 관리 그룹에서 선택한 기기를 제거합니다:
   - 선택한 기기의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
   - **처리 방법 수행** 버튼을 클릭하고 드롭다운 목록에서 **그룹에서 제거**를 선택합니다.

그러면 선택한 기기가 해당 관리 그룹에서 제거됩니다.

애플리케이션 설치 및 제거 모니터링

관리 중인 기기에서 특정 애플리케이션의 설치 또는 제거를 모니터링 할 수 있습니다(예: 특정 브라우저). 이 기능을 사용하기 위해 자산 관리(소프트웨어)에서 모니터링되는 애플리케이션의 목록에 애플리케이션을 추가할 수 있습니다. 모니터링되는 애플리케이션이 설치되거나 제거되면 네트워크 에이전트가 해당 이벤트를 게시합니다(**감시 중인 애플리케이션이 설치되었습니다** 또는 **감시 중인 애플리케이션이 제거되었습니다**). 이벤트 조회 또는 리포트 등을 사용하여 이러한 이벤트를 모니터링할 수 있습니다.

이러한 이벤트는 중앙 관리 서버 데이터베이스에 저장된 경우에만 모니터링할 수 있습니다.

모니터링되는 애플리케이션의 목록에 애플리케이션을 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **고급 → 애플리케이션 관리** 폴더에서 **자산 관리(소프트웨어)** 하위 폴더를 선택합니다.
2. 애플리케이션의 목록이 표시되면 위에 있는 **자산 관리(소프트웨어) 속성 창 표시** 버튼을 누릅니다.
3. **감시 중인 애플리케이션** 창이 표시되면 **추가** 버튼을 누릅니다.
4. **애플리케이션 이름 선택** 창이 표시되면 설치 또는 제거를 모니터링하려고 하는 자산 관리(소프트웨어)에서 애플리케이션을 선택합니다.
5. **애플리케이션 이름 선택** 창에서 **확인** 버튼을 누릅니다.

모니터링되는 애플리케이션의 목록을 구성하고 조직의 관리 중인 기기에 모니터링되는 애플리케이션을 설치하거나 제거한 후에는 예를 들어 최근 이벤트 이벤트 조회를 사용하여 각 이벤트를 모니터링할 수 있습니다.

Kaspersky Security Center 구성 요소의 이벤트

각 Kaspersky Security Center 구성 요소에는 자체 이벤트 유형 집합이 있습니다. 이 섹션에는 Kaspersky Security Center 중앙 관리 서버, 네트워크 에이전트, iOS MDM 서버에서 발생하는 이벤트 유형이 나열되어 있습니다. Kaspersky 애플리케이션에서 발생하는 이벤트의 유형은 이 섹션에 나열되지 않습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

이벤트 유형 데이터 구조 설명

각 이벤트 유형에 대해 표시 이름, 식별자(ID), 알파벳 코드, 설명 및 기본 저장 기간이 제공됩니다.

- **이벤트 유형 표시 이름**. 구성한 이벤트가 발생하면 Kaspersky Security Center에 이 텍스트가 표시됩니다.
- **이벤트 유형 ID**. 이벤트 분석용 타사 도구를 사용하여 이벤트를 처리할 때 이 숫자 코드를 사용합니다.
- **이벤트 유형**(알파벳 코드). Kaspersky Security Center 데이터베이스에서 제공되는 공용 보기를 사용하여 이벤트를 찾아서 처리할 때와 SIEM 시스템으로 이벤트를 내보낼 때 이 코드를 사용합니다.
- **설명**. 이 텍스트에는 이벤트가 발생한 상황과 그러한 경우에 수행할 수 있는 작업이 포함되어 있습니다.
- **기본 저장 기간**. 이벤트가 중앙 관리 서버 데이터베이스에 저장되며 중앙 관리 서버의 이벤트 목록에 표시되는 기간(일)입니다. 이 기간이 지나면 이벤트는 삭제됩니다. 이벤트 저장 기간 값이 0이면 해당 이벤트가 탐지되기는 하지만 중앙 관리 서버의 이벤트 목록에는 표시되지 않습니다. 운영 체제 이벤트 로그에 그러한 이벤트를 저장하도록 구성한 경우에는 해당 로그에서 이벤트를 확인할 수 있습니다.

  다음과 같이 이벤트의 저장 기간을 변경할 수 있습니다:

  - 관리 콘솔: 이벤트의 저장 기간 설정
  - Kaspersky Security Center 웹 콘솔: 이벤트의 저장 기간 설정

기타 데이터에는 다음 필드가 포함될 수 있습니다.

- **event_id**: 자동으로 생성되어 할당되는 데이터베이스 내 이벤트의 고유 번호를 **이벤트 유형 ID**와 혼동하지 마십시오.
- **task_id**: 이벤트를 발생시킨 작업의 ID(있는 경우)
- **심각도**: 다음 심각도 중 하나(심각도 오름차순):

  0) 잘못된 심각도

  1) 정보

  2) 경고

  3) 오류

  4) 심각

중앙 관리 서버 이벤트

이 섹션에는 중앙 관리 서버와 관련된 이벤트에 대한 정보가 있습니다.

중앙 관리 서버 심각 이벤트

표에는 **심각** 심각도를 가진 Kaspersky Security Center 중앙 관리 서버의 이벤트가 표시됩니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

관리 콘솔의 중앙 관리 서버 속성 창에서 포트를 지정했다면 **Kaspersky Security Center**가 모니터링 및 알림 시스템인 Prometheus에서 얻을 수 있는 메트릭과 심각 이벤트를 게시합니다. Prometheus는 메트릭과 심각 이벤트를 획득한 다음 각 이벤트에 대한 경고를 생성합니다.

```
// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"
```

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

중앙 관리 서버 심각 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
라이센스 제한을 초과했습니다	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Security Center는 하루에 한 번 라이센스 제한 초과 여부를 확인합니다. 이 유형의 이벤트는 중앙 관리 서버가 클라이언트 기기에 설치된 Kaspersky 애플리케이션에 의해 일부 라이센스가 그 제한이 초과되었음을 탐지하고 하나의 라이센스로 사용한 라이센스 수가 해당 라이센스에 적용된 총 구매 수의 110%를 초과하는 경우에 발생합니다. 이 이벤트가 발생하더라도 클라이언트 기기는 보호됩니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록을 살펴봅니다. 사용하지 않는 기기를 삭제합니다. • 추가 라이센스를 배포합니다(중앙 관리 서버에 유효한 활성화코드 또는 키 파일 추가). Kaspersky Security Center는 라이센스 구매 수량을 초과할 때 이벤트를 생성하는 규칙을 결정합니다.	180일
바이러스 발생	26(파일 위협 보호의 경우)	GNRL_EV_VIRUS_OUTBREAK	이 유형의 이벤트는 몇몇 관리 중인 기기에서 탐지된 악성 코드 개체 수가 짧은 기간 내에 임계값을 초과할 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 속성에서 임계값을 구성할 수 있습니다. • 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.	180일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
바이러스 발생	27(메일 위협 보호의 경우)	GNRL_EV_VIRUS_OUTBREAK	이 유형의 이벤트는 몇몇 관리 중인 기기에서 탐지된 악성 코드 개체 수가 짧은 기간 내에 임계값을 초과할 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 속성에서 임계값을 구성할 수 있습니다. • 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.	180일
바이러스 발생	28(방화벽의 경우)	GNRL_EV_VIRUS_OUTBREAK	이 유형의 이벤트는 몇몇 관리 중인 기기에서 탐지된 악성 코드 개체 수가 짧은 기간 내에 임계값을 초과할 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 속성에서 임계값을 구성할 수 있습니다. • 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.	180일
기기와의 연결이 끊어짐	4111	KLSRV_HOST_OUT_CONTROL	이 유형의 이벤트는 관리 중인 기기가 네트워크에는 나타나지만 특정 기간 동안 중앙 관리 서버에 연결되지 않은 경우에 발생합니다. 해당 기기에서 네트워크 에이전트의 정상 작동을 방해하는 것이 무엇인지 확인하십시오. 가능한 원인으로는 네트워크 문제 및 기기에서 네트워크 에이전트가 제거되었을 수 있습니다.	180일
기기 상태가 '심각'입니다	4113	KLSRV_HOST_STATUS_CRITICAL	이 유형의 이벤트는 관리 중인 기기가 *심각* 상태로 변한 경우 발생합니다. 기기 상태가 *심각*으로 변경되는 조건을 구성할 수 있습니다.	180일
키 파일이 거부 목록에 추가되었습니다	4124	KLSRV_LICENSE_BLACKLISTED	이 유형의 이벤트는 Kaspersky에서 사용자가 사용하는 활성화코드 또는 키 파일을 거부 목록에 추가한 경우 발생합니다. 자세한 내용은 기술 지원에 문의하십시오.	180일
기능 제한 모드	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	이 유형의 이벤트는 Kaspersky Security Center가 취약점 및 패치 관리 기능과 모바일 기기 관리 기능 없이 기본 기능으로 동작하려고 할 때 발생합니다. 다음은 이벤트의 원인 및 그에 대한 대응 방안입니다: • 라이센스 기간 만료됨. 이 경우 Kaspersky Security Center의 전체 기능 모드를 사용할 수 있는 라이센스를 추가합니다(유효한 활성화코드 또는 키 파일을 중앙 관리 서버에 추가). • 중앙 관리 서버가 라이센스 제한에 지정된 것보다 더 많은 기기를 관리함. 이 경우 중앙 관리 서버의 일부 기기를 다른 중앙 관리 서버의 관리 그룹으로 이동합니다(다른 중앙 관리 서버의 라이센스 제한에 여유가 있을 경우).	180일
라이센스가 곧 만료됩니다	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	이 유형의 이벤트는 상업용 라이센스 만료 날짜가 다가오면 발생합니다. Kaspersky Security Center는 하루에 한 번 라이센스 만료일이 얼마나 남았는지 확인합니다. 이러한 유형의 이벤트는 라이센스 만료 날짜로부터 30일, 15일, 5일, 1일 전에 게시됩니다. 일 수는 변경할 수 없습니다. 라이센스 만료 날짜 이전의 지정된 날짜에 중앙 관리 서버를 끄면 이벤트는 다음날까지 게시되지 않습니다. 상업용 라이센스가 만료되면 Kaspersky Security Center에서는 기본 기능만 제공됩니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 예약 라이센스 키가 중앙 관리 서버에 추가되었는지 확인합니다. • 서브스크립션을 사용하는 경우 갱신해야 합니다. 만기일까지 서비스 공급 업체에게 선불이 완료되면 무기한 서브스크립션이 자동으로 갱신됩니다.	180일
인증서가 만료되었습니다	4132	KLSRV_CERTIFICATE_EXPIRED	모바일 기기의 클라이언트 인증서가 만료되면 이 유형의 이벤트가 발생합니다.	180일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
중앙 관리 서버 인증서가 만료되었습니다.	6129	ServerCertificateExpired	모바일 기기 및 UEFI 기기의 중앙 관리 서버 인증서가 만료되면 이 유형의 이벤트가 발생합니다. 만료된 인증서를 업데이트해야 합니다.	180일
Kaspersky 애플리케이션 모듈 업데이트를 취소했습니다	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	이러한 유형의 이벤트는 Kaspersky 기술 지원 전문가가 seamless 업데이트를 철회한 경우(이 업데이트에 대해 *철회됨* 상태가 표시됨) 발생합니다. 새로운 버전으로 업데이트해야 할 경우를 예로 들 수 있습니다. 이 이벤트는 Kaspersky Security Center 패치와 관련이 있으며 관리 중인 Kaspersky 애플리케이션의 모듈과는 관련이 없습니다. 이 이벤트는 seamless 업데이트가 설치되지 않은 이유를 제공합니다.	180일
감사: SIEM으로 내보내기에 실패했습니다	5130	KLAUD_EV_SIEM_EXPORT_ERROR	이 유형의 이벤트는 SIEM 시스템 연결 오류로 인해 SIEM 시스템으로 이벤트를 내보내기에 실패할 때 발생합니다.	180일

중앙 관리 서버 기능 실패 이벤트

아래 표에는 심각도가 **기능 실패**인 Kaspersky Security Center 중앙 관리 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

중앙 관리 서버 기능 실패 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
런타임 오류	4125	KLSRV_RUNTIME_ERROR	이 유형의 이벤트는 알 수 없는 문제로 인해 발생합니다. 이러한 문제의 대부분은 DBMS 문제, 네트워크 문제 및 기타 소프트웨어 및 하드웨어 문제입니다. 이벤트에 대한 자세한 내용은 이벤트 설명에서 확인할 수 있습니다.	180일
유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 초과했습니다	4126	KLSRV_INVLICPROD_EXCEDED	중앙 관리 서버는 정기적으로(매시간) 이 유형의 이벤트를 생성합니다. 이 유형의 이벤트는 Kaspersky Security Center에서 타사 애플리케이션의 라이센스 키를 관리하고 설치된 개수가 타사 애플리케이션의 라이센스 키에서 설정한 제한을 초과하는 경우에 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록을 살펴봅니다. 애플리케이션이 사용되지 않는 기기에서 해당 타사 애플리케이션을 삭제합니다. • 타사 라이센스의 구매 수량을 늘립니다. 유료 애플리케이션 그룹 기능을 사용하여 타사 애플리케이션의 라이센스 키를 관리할 수 있습니다. 유료 애플리케이션 그룹에는 관리자가 지정한 기준에 부합하는 타사 애플리케이션이 들어 있습니다.	180일
클라우드 세그먼트를 검색하지 못했습니다	4143	KLSRV_KLCLOUD_SCAN_ERROR	이 유형의 이벤트는 중앙 관리 서버가 클라우드 환경에서 네트워크 세그먼트를 검색하지 못할 때 발생합니다. 이벤트 설명에서 세부 정보를 읽고 그에 따라 대응하십시오.	저장되지 않음

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
지정한 폴더로 업데이트 파일을 복사하지 못했습니다	4123	KLSRV_UPD_REPL_FAIL	이 유형의 이벤트는 소프트웨어 업데이트가 추가 공유 폴더에 복사될 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 해당 폴더에 접근하기 위해 사용하는 사용자 계정에 쓰기 권한이 있는지 확인합니다. • 해당 폴더의 사용자 이름 및/또는 암호가 변경되었는지 확인합니다. • 이 이벤트의 원인일 수 있는 인터넷 연결을 확인합니다. 지침에 따라 데이터베이스 및 소프트웨어 모듈을 업데이트합니다.	180일
하드 드라이브에 여유 공간이 없습니다	4107	KLSRV_DISK_FULL	이 유형의 이벤트는 중앙 관리 서버가 설치된 기기의 하드 드라이브에 여유 공간이 부족한 경우 발생합니다. 기기의 디스크 공간을 확보하십시오.	180일
공유 폴더를 사용할 수 없습니다	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	이 유형의 이벤트는 중앙 관리 서버의 공유 폴더를 사용할 수 없는 경우 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버(공유 폴더가 있는)가 켜져 있고 사용 가능한지 확인합니다. • 해당 폴더의 사용자 이름 또는 암호가 변경되었는지 확인합니다. • 네트워크 연결을 확인합니다.	180일
중앙 관리 서버 정보 데이터베이스를 이용할 수 없습니다	4109	KLSRV_DATABASE_UNAVAILABLE	이 유형의 이벤트는 중앙 관리 서버 데이터베이스를 사용할 수 없게 되면 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • SQL Server가 설치된 원격 서버를 사용할 수 있는지 확인합니다. • DBMS 로그를 보고 중앙 관리 서버 데이터베이스를 사용할 수 없는 이유를 확인합니다. 예를 들어 예방 차원의 유지 보수 때문에 SQL Server가 설치된 원격 서버를 사용할 수 없을 수 있습니다.	180일
중앙 관리 서버 데이터베이스 공간 부족	4110	KLSRV_DATABASE_FULL	이 유형의 이벤트는 중앙 관리 서버 데이터베이스에 사용 가능한 공간이 없을 때 발생합니다. 데이터베이스 용량이 꽉 차고 데이터베이스에 추가 기록이 불가능할 경우 중앙 관리 서버가 동작하지 않습니다. 다음은 사용하는 DBMS에 따라 이 이벤트의 원인 및 해당 이벤트에 대한 적절한 대응 방안입니다: • SQL Server Express Edition DBMS를 사용하는 경우: SQL Server Express 설명서에서 현재 사용하는 버전에 대한 데이터베이스 크기 제한을 검토합니다. 아마도 중앙 관리 서버 데이터베이스가 그 데이터베이스 크기 제한을 초과했을 수 있습니다. 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한합니다. 중앙 관리 서버 데이터베이스에 애플리케이션 제어 구성 요소가 보낸 이벤트가 매우 많을 수 있습니다. 이 경우 중앙 관리 서버 데이터베이스에서 애플리케이션 제어 이벤트 저장과 관련된 Kaspersky Endpoint Security for Windows 정책 설정을 변경할 수 있습니다. • SQL Server Express Edition 이외의 DBMS를 사용하는 경우: 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한하지 않습니다. 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다. DBMS 선택에 대한 정보를 검토합니다.	180일

중앙 관리 서버 경고 이벤트

표에는 심각도가 **경고**인 Kaspersky Security Center 중앙 관리 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

중앙 관리 서버 경고 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
자주 등록된 이벤트가 탐지되었습니다		KLSRV_EVENT_SPAM_EVENTS_DETECTED	이 유형의 이벤트는 중앙 관리 서버가 관리 중인 기기에서 자주 등록된 이벤트를 감지할 때 발생합니다. 자세한 내용은 다음 섹션을 참조하십시오: 자주 등록된 이벤트 차단.	90일
라이센스 제한을 초과했습니다	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center는 하루에 한 번 라이센스 제한 초과 여부를 확인합니다. 이 유형의 이벤트는 중앙 관리 서버가 클라이언트 기기에 설치된 Kaspersky 애플리케이션에 의해 일부 라이센스가 그 제한이 초과되었음을 탐지하고 하나의 라이센스로 사용한 라이센스 수가 해당 라이센스에 적용된 총 구매 수의 100%에서 110% 이내인 경우에 발생합니다. 이 이벤트가 발생하더라도 클라이언트 기기는 보호됩니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록을 살펴봅니다. 사용하지 않는 기기를 삭제합니다. • 추가 라이센스를 배포합니다(중앙 관리 서버에 유효한 활성화코드 또는 키 파일 추가). Kaspersky Security Center는 라이센스 구매 수량을 초과할 때 이벤트를 생성하는 규칙을 결정합니다.	90일
오랫동안 기기가 네트워크에 접속하지 않았습니다	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	이 유형의 이벤트는 관리 중인 기기가 일정 시간 동안 비활성 상태로 표시될 때 발생합니다. 대부분의 경우 관리 중인 기기가 해제될 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록에서 기기를 수동으로 제거하십시오. • 관리 콘솔을 사용하거나 Kaspersky Security Center 웹 콘솔을 사용하여 **오랫동안 기기가 네트워크에 접속하지 않았습니다** 이벤트가 생성된 후 시간 간격을 지정하십시오. • 관리 콘솔을 사용하거나 Kaspersky Security Center 웹 콘솔을 사용하여 그룹에서 기기가 자동으로 제거된 후 시간 간격을 지정하십시오.	90일
기기 이름 중복	4102	KLSRV_EVENT_HOSTS_CONFLICT	이 유형의 이벤트는 중앙 관리 서버가 둘 이상의 관리 중인 기기를 단일 기기로 간주할 때 발생합니다. 대부분의 경우 복제된 하드 드라이브가 관리 중인 기기의 소프트웨어 배포에 사용되었으며 참조 기기에서 네트워크 에이전트를 전용 디스크 복제 모드로 전환하지 않은 경우 발생합니다. 이 문제를 방지하려면 이 기기의 하드 드라이브를 복제하기 전에 참조 기기에서 네트워크 에이전트를 디스크 복제 모드로 전환하십시오.	90일
기기 상태가 '경고'입니다	4114	KLSRV_HOST_STATUS_WARNING	이 유형의 이벤트는 관리 중인 기기가 *경고* 상태로 변한 경우 발생합니다. 기기 상태가 *경고*로 변경되는 조건을 구성할 수 있습니다.	90일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 곧 초과합니다	4127	KLSRV_INVLICPROD_FILLED	이 유형의 이벤트는 유료 애플리케이션 그룹에 포함된 타사 애플리케이션의 설치 수가 라이센스 키 속성에서 지정된 최대 허용 값인 90%에 도달하는 경우 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 일부 관리 중인 기기에서 타사 애플리케이션을 사용하지 않는 경우 이러한 기기에서 애플리케이션을 삭제하십시오. • 조만간 타사 애플리케이션의 설치 수가 허용된 최대 값을 초과할 것으로 예상되는 경우 더 많은 기기에 대한 타사 라이센스를 미리 확보하는 것이 좋습니다. 유료 애플리케이션 그룹 기능을 사용하여 타사 애플리케이션의 라이센스 키를 관리할 수 있습니다.	90일
인증서를 요청했습니다	4133	KLSRV_CERTIFICATE_REQUESTED	이 유형의 이벤트는 모바일 기기 관리에 대한 인증서가 자동으로 재발급되지 않을 때 발생합니다. 이벤트에 대한 원인과 적절한 대응은 다음과 같을 수 있습니다. • **가능하면 자동으로 인증서 재발급** 옵션이 비활성화된 인증서에 대한 자동 재발급이 시작되었습니다. 이는 인증서 생성 중에 발생한 오류 때문일 수 있습니다. 인증서를 수동으로 재발급해야 할 수 있습니다. • 공개 키 인프라와 통합을 사용하는 경우 PKI와의 통합 및 인증서 발급에 사용되는 계정의 SAM-Account-Name 특성이 누락된 것이 원인일 수 있습니다. 계정 속성을 검토하십시오.	90일
인증서가 제거되었습니다	4134	KLSRV_CERTIFICATE_REMOVED	이 유형의 이벤트는 관리자가 모바일 기기 관리에 대한 모든 유형의 인증서(일반, 메일, VPN)를 제거할 때 발생합니다. 인증서를 제거한 후에는 이 인증서를 통해 연결된 모바일 기기를 중앙 관리 서버에 연결할 수 없습니다. 이 이벤트는 모바일 기기 관리와 관련된 오작동을 조사할 때 유용할 수 있습니다.	90일
인증서가 만료됩니다	6128	ServerCertificateExpiresSoon	모바일 기기 및 UEFI 기기의 중앙 관리 서버 인증서가 만료되면 이 유형의 이벤트가 발생합니다. 만료된 인증서를 업데이트해야 합니다.	90일
APNs 인증서가 만료되었습니다	4135	KLSRV_APN_CERTIFICATE_EXPIRED	이 유형의 이벤트는 APNs 인증서가 만료되는 경우 발생합니다. 수동으로 APNs 인증서를 갱신하고 iOS MDM 서버에 설치해야 합니다.	저장되지 않음
APNs 인증서가 곧 만료됩니다	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	이 유형의 이벤트는 APNs 인증서가 만료되기까지 남은 기간이 14일 미만인 경우 발생합니다. APNs 인증서가 만료되면 수동으로 APNs 인증서를 갱신하고 iOS MDM 서버에 설치해야 합니다. 만료 날짜 이전에 APNs 인증서 갱신을 예약하는 것이 좋습니다.	저장되지 않음
모바일 기기로의 FCM 메시지 전송 실패	4138	KLSRV_GCM_DEVICE_ERROR	이 유형의 이벤트는 모바일 기기 관리가 Android 운영 체제를 사용하는 관리 중인 모바일 기기에 대해 FCM (Firebase Cloud Messaging)를 사용하도록 구성되고 FCM 서버가 중앙 관리 서버에서 받은 일부 요청을 처리하지 못할 때 발생합니다. 이는 관리 중인 모바일 기기 중 일부에 푸시 알림이 수신되지 않음을 의미합니다. 이벤트 설명의 세부 정보에서 HTTP 코드를 읽고 그에 따라 대응하십시오. FCM 서버에서 수신한 HTTP 코드 및 관련 오류에 대한 자세한 내용은 Firebase 서비스 문서('다운스트림 메시지 오류 대응 코드')를 참조하십시오.	90일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
FCM 서버에 FCM 메시지를 전송할 때 HTTP 오류 발생	4139	KLSRV_GCM_HTTP_ERROR	이 유형의 이벤트는 모바일 기기 관리가 FCM (Firebase Cloud Messaging)를 사용하여 Android 운영 체제를 사용하는 관리 중인 모바일 기기를 연결하도록 모바일 기기 관리를 구성하고 FCM 서버가 200(OK) 이외의 HTTP 코드를 사용하여 중앙 관리 서버 요청으로 돌아갈 때 발생합니다. 이벤트에 대한 원인과 적절한 대응은 다음과 같을 수 있습니다. • FCM 서버 측의 문제입니다. 이벤트 설명의 세부 정보에서 HTTP 코드를 읽고 그에 따라 대응하십시오. FCM 서버에서 수신한 HTTP 코드 및 관련 오류에 대한 자세한 내용은 Firebase 서비스 문서('다운스트림 메시지 오류 대응 코드')를 참조하십시오. • 프록시 서버 측의 문제입니다(프록시 서버를 사용하는 경우). 이벤트 설명의 세부 정보에서 HTTP 코드를 읽고 그에 따라 대응하십시오.	90일
FCM 서버로 FCM 메시지 전송 실패	4140	KLSRV_GCM_GENERAL_ERROR	이 유형의 이벤트는 Firebase Cloud Messaging HTTP 프로토콜로 작업할 때 중앙 관리 서버 측의 예상치 못한 오류로 인해 발생합니다. 이벤트 설명에서 세부 정보를 읽고 그에 따라 대응하십시오. 문제에 대한 해결 방법을 스스로 찾을 수 없는 경우 Kaspersky 기술 지원에 문의하는 것이 좋습니다.	90일
하드 드라이브에 여유 공간이 부족합니다	4105	KLSRV_NO_SPACE_ON_VOLUMES	이 유형의 이벤트는 중앙 관리 서버가 설치된 기기의 디스크 공간이 부족한 경우 발생합니다. 기기의 디스크 공간을 확보하십시오.	90일
중앙 관리 서버 데이터베이스에 여유 공간이 거의 없습니다	4106	KLSRV_NO_SPACE_IN_DATABASE	이 유형의 이벤트는 중앙 관리 서버 데이터베이스의 공간이 너무 부족할 경우 발생합니다. 이 문제를 해결하지 않으면 중앙 관리 서버 데이터베이스가 곧 제한 용량에 도달하고 중앙 관리 서버가 정상 작동하지 않게 됩니다. 다음은 사용하는 DBMS에 따라 이 이벤트의 원인 및 해당 이벤트에 대한 적절한 대응 방안입니다. SQL Server Express Edition DBMS를 사용하는 경우: • SQL Server Express 설명서에서 현재 사용하는 버전에 대한 데이터베이스 크기 제한을 검토합니다. 아마도 중앙 관리 서버 데이터베이스가 곧 데이터베이스 크기 제한에 도달하려고 합니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한합니다. • 중앙 관리 서버 데이터베이스에 애플리케이션 제어 구성 요소가 보낸 이벤트가 매우 많을 수 있습니다. 이 경우 중앙 관리 서버 데이터베이스에서 애플리케이션 제어 이벤트 저장과 관련된 Kaspersky Endpoint Security for Windows 정책 설정을 변경할 수 있습니다. SQL Server Express Edition 이외의 DBMS를 사용하는 경우: • 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한하지 않습니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다. DBMS 선택에 대한 정보를 검토합니다.	90일
보조 중앙 관리 서버와의 연결이 중단되었습니다	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	이 유형의 이벤트는 보조 중앙 관리 서버에 대한 연결이 끊어지는 경우 발생합니다. 보조 중앙 관리 서버가 설치된 기기에서 Kaspersky 이벤트 로그를 읽고 그에 따라 대응하십시오.	90일
기본 중앙 관리 서버와의 연결이 중단되었습니다	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	이 유형의 이벤트는 기본 중앙 관리 서버에 대한 연결이 끊어지는 경우 발생합니다. 기본 중앙 관리 서버가 설치된 기기에서 Kaspersky 이벤트 로그를 읽고 그에 따라 대응하십시오.	90일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
새로운 Kaspersky 애플리케이션 모듈 업데이트가 등록되었습니다	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	이 유형의 이벤트는 중앙 관리 서버가 설치 승인이 필요한 관리 중인 기기에 설치된 Kaspersky 소프트웨어에 대한 새 업데이트를 등록하는 경우 발생합니다. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 사용하여 업데이트를 승인 또는 거부하십시오.	90일
데이터베이스의 이벤트 수 제한을 초과하여 이벤트 삭제가 시작되었습니다	4145	KLSRV_EVP_DB_TRUNCATING	이 유형의 이벤트는 중앙 관리 서버 데이터베이스가 제한 용량에 도달한 후 중앙 관리 서버 데이터베이스의 이전 이벤트를 삭제하기 시작한 경우에 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 데이터베이스에 저장되는 최대 이벤트 수를 변경합니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다.	저장되지 않음
데이터베이스의 이벤트 수 제한을 초과하여 이벤트가 삭제되었습니다	4146	KLSRV_EVP_DB_TRUNCATED	이 유형의 이벤트는 중앙 관리 서버 데이터베이스가 제한 용량에 도달한 후 중앙 관리 서버 데이터베이스의 이전 이벤트가 삭제된 경우에 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 데이터베이스에 저장되는 최대 허용 이벤트 수를 변경합니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다.	저장되지 않음
감사(SIEM 서버 테스트 연결 실패)	5120	KLAUD_EV_SIEM_TEST_FAILED	이 유형의 이벤트는 SIEM 서버에 대한 연결 테스트가 실패했을 때 발생합니다.	30일
인증서를 자동 발급하지 못했습니다		KLSRV_인증서_자동_발급_오류	이 이벤트는 모바일 기기(모바일 프로토콜에 따라 작동하는 기기)를 위한 클라이언트 인증서를 생성하는 동안 오류가 발생했을 때 일어납니다.	90일

중앙 관리 서버 정보 이벤트

표에는 심각도가 **정보**인 Kaspersky Security Center 중앙 관리 서버의 이벤트가 나와 있습니다.

중앙 관리 서버 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간	비고
현재 라이센스 키를 90% 이상 사용했습니다	4097	KLSRV_EV_LICENSE_CHECK_90	30일	
새 기기가 탐지되었습니다	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30일	
기기가 자동으로 그룹에 추가되었습니다	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30일	
기기가 규칙에 따라 그룹으로 자동 이동되었습니다	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30일	
기기가 네트워크에 오랫동안 접속하지 않아 그룹에서 삭제되었습니다	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30일	
유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 곧 초과합니다(95% 이상 사용 중)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30일	
분석을 위해 Kaspersky로 전송해야 할 파일이 있습니다	4131	KLSRV_APS_FILE_APPEARED	30일	
FCM 인스턴스 ID가 이 모바일 기기에서 변경되었습니다	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30일	
업데이트 파일이 지정한 폴더에 복사되었습니다	4122	KLSRV_UPD_REPL_OK	30일	

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간	비고
보조 중앙 관리 서버에 연결되었습니다	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30일	
기본 중앙 관리 서버에 연결되었습니다	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30일	
데이터베이스가 업데이트되었습니다	4144	KLSRV_UPD_BASES_UPDATED	30일	
감사: 중앙 관리 서버로의 연결이 확립되었습니다	4147	KLAUD_EV_SERVERCONNECT	30일	
감사: 개체가 수정되었습니다	4148	KLAUD_EV_OBJECTMODIFY	30일	이 이벤트는 다음 개체의 변경 사항을 추적합니다. • 관리 그룹 • 보안 그룹 • 사용자 • 패키지 • 작업 • 정책 • 서버 • 가상 서버
감사: 개체 상태가 변경되었습니다	4150	KLAUD_EV_TASK_STATE_CHANGED	30일	예를 들어 이 이벤트는 오류로 작업이 실패했을 때 발생합니다.
감사: 그룹 설정이 수정되었습니다	4149	KLAUD_EV_ADMGROUP_CHANGED	30일	
감사: 중앙 관리 서버와의 연결이 종료되었습니다	4151	KLAUD_EV_SERVERDISCONNECT	30일	
감사: 개체 속성이 수정되었습니다	4152	KLAUD_EV_OBJECTPROPMODIFIED	30일	이 이벤트는 다음 속성의 변경 사항을 추적합니다. • 사용자 • 라이센스 • 서버 • 가상 서버
감사: 사용자 권한이 수정되었습니다	4153	KLAUD_EV_OBJECTACLMODIFIED	30일	
감사: 중앙 관리 서버에서 암호화 키를 가져오거나 내보냈습니다	5100	KLAUD_EV_DPEKEYSEXPORT	30일	
감사(SIEM 서버 테스트 연결 성공)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30일	이 이벤트는 SIEM 서버에 대한 연결 테스트가 성공했을 때 발생합니다.
예약 인증서가 생성되었습니다		서버 예약 인증서 생성됨	30일	이 이벤트는 중앙 관리 서버 인증서를 생성하면 발생합니다.
인증서 갱신		서버 인증서 갱신됨	30일	이 이벤트는 중앙 관리 서버 인증서를 갱신하면 발생합니다.
인증서 자동 발급에 성공했습니다		KLSRV_인증서_자동_발급	30일	이 이벤트는 모바일 기기(모바일 프로토콜을 기반으로 작동하는 기기)용 인증서가 생성되었을 때 발생합니다.

예약 인증서가 생성되었습니다, **인증서 갱신** 및 **인증서 자동 발급에 성공했습니다** 이벤트는 모바일 기기 및 UEFI 기기용 중앙 관리 서버 인증서에 대해 이러한 이벤트에 해당하는 작업이 수행될 때만 중앙 관리 서버에서

자동으로 게시되며 관리 콘솔에 표시됩니다.

네트워크 에이전트 이벤트

이 섹션에는 네트워크 에이전트와 관련된 이벤트에 대한 정보가 있습니다.

네트워크 에이전트 기능 실패 이벤트

표에는 **기능 실패** 심각도가 포함된 Kaspersky Security Center 네트워크 에이전트 이벤트가 표시됩니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

네트워크 에이전트 기능 실패 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
업데이트 설치 오류	7702	KLNAG_EV_PATCH_INSTALL_ERROR	이 유형의 이벤트는 Kaspersky Security Center 구성 요소에 대한 자동 업데이트 및 패치에 실패한 경우에 발생합니다. 이 이벤트는 관리 중인 Kaspersky 애플리케이션의 업데이트와 관련이 없습니다. 이벤트 설명을 읽습니다. 중앙 관리 서버의 Windows 문제가 이 이벤트의 원인일 수 있습니다. 이벤트 설명에 Windows 구성 문제가 언급되어 있으면 이 문제를 해결하십시오.	30일
타사 소프트웨어 업데이트를 설치하지 못했습니다	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	이 유형의 이벤트는 취약점 및 패치 관리와 모바일 기기 관리 기능이 사용 중이고 타사 소프트웨어를 업데이트하지 못했을 때 발생합니다. 타사 소프트웨어에 대한 링크가 올바른지 확인합니다. 이벤트 설명을 읽습니다.	30일
Windows 업데이트 패치를 설치하지 못했습니다	7717	KLNAG_EV_WUA_INSTALL_ERROR	이 유형의 이벤트는 Windows 업데이트에 실패했을 때 발생합니다. 네트워크 에이전트 정책에서 Windows 업데이트 구성. 이벤트 설명을 읽습니다. Microsoft 기술 자료에서 오류를 찾습니다. 문제를 직접 해결할 수 없는 경우 Microsoft 기술 지원에 문의합니다.	30일
사용자 관리: 오류	7723	KLNAG_EV_USR_MNG_ERR	일반 경고 이벤트.	30일
Sudoers 파일을 참조값으로 복구하지 못했습니다	7726	KLNAG_EV_SUDOER_RESTORED_ERR	이벤트는 sudoers 파일 대체 오류 설명을 포함합니다.	30일
루트 인증서를 설치하지 못했습니다	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	이벤트는 인증서 설치 오류 설명을 포함합니다.	30일
루트 인증서를 제거하지 못했습니다	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	이벤트는 인증서 제거 오류 설명을 포함합니다.	30일

네트워크 에이전트 경고 이벤트

아래의 표에 **경고** 심각도를 가진 Kaspersky Security Center 네트워크 에이전트의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

네트워크 에이전트 경고 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간
소프트웨어 모듈 업데이트 설치 시 경고가 발생했습니다	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30일
타사 소프트웨어 업데이트 설치가 완료했지만 경고 메시지가 있습니다	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30일
타사 소프트웨어 업데이트 설치가 연기되었습니다	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30일
보안 문제가 발생했습니다	549	GNRL_EV_APP_INCIDENT_OCCURED	30일
KSN 프록시가 시작되었지만 KSN 이용 가능 여부를 확인하지 못했습니다	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30일
사용자 관리: 경고	7722	KLNAG_EV_USR_MNG_WRN	30일
찾은 Sudoers 파일이 참조값과 일치하지 않습니다	7724	KLNAG_EV_SUDOER_DIFFERENT	30일

네트워크 에이전트 정보 이벤트

아래 표에는 **정보** 심각도를 가진 Kaspersky Security Center 네트워크 에이전트의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

네트워크 에이전트 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간
소프트웨어 모듈 업데이트를 설치했습니다	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30일
소프트웨어 모듈 업데이트 설치를 시작했습니다	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30일
애플리케이션을 설치했습니다	7703	KLNAG_EV_INV_APP_INSTALLED	30일
애플리케이션을 제거했습니다	7704	KLNAG_EV_INV_APP_UNINSTALLED	30일
감시 중인 애플리케이션이 설치되었습니다	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30일
감시 중인 애플리케이션이 제거되었습니다	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30일
타사 애플리케이션이 설치되었습니다	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30일
새 기기가 추가되었습니다	7708	KLNAG_EV_DEVICE_ARRIVAL	30일
기기가 제거되었습니다	7709	KLNAG_EV_DEVICE_REMOVE	30일
새 기기가 탐지되었습니다	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30일
기기가 인증되었습니다	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30일
Windows Desktop Sharing: 파일을 읽음	7712	KLUSRLOG_EV_FILE_READ	30일
Windows Desktop Sharing: 파일을 수정함	7713	KLUSRLOG_EV_FILE_MODIFIED	30일
Windows Desktop Sharing: 애플리케이션을 시작함	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30일
Windows Desktop Sharing: 시작됨	7715	KLUSRLOG_EV_WDS_BEGIN	30일
Windows Desktop Sharing: 중지됨	7716	KLUSRLOG_EV_WDS_END	30일
타사 소프트웨어 업데이트가 설치되었습니다	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30일
타사 소프트웨어 업데이트 설치가 시작되었습니다	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30일
KSN 프록시가 시작되었습니다. KSN 이용 가능 여부 확인 성공	7719	KSNPROXY_STARTED_CON_CHK_OK	30일
KSN 프록시가 중지되었습니다	7720	KSNPROXY_STOPPED	30일

iOS MDM 서버 이벤트

이 섹션에는 iOS MDM 서버와 관련된 이벤트에 대한 정보가 있습니다.

iOS MDM 서버 기능 실패 이벤트

표에는 **기능 실패** 심각도를 가진 Kaspersky Security Center iOS MDM 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

iOS MDM 서버 기능 실패 이벤트

이벤트 유형 표시 이름	이벤트 유형	기본 저장 기간
프로필 목록 요청 실패	PROFILELIST_COMMAND_FAILED	30일
프로필 설치 실패	INSTALLPROFILE_COMMAND_FAILED	30일
프로필 삭제 실패	REMOVEPROFILE_COMMAND_FAILED	30일
프로비저닝 프로필 목록 요청 실패	PROVISIONINGPROFILELIST_COMMAND_FAILED	30일
프로비저닝 프로필 설치 실패	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30일
프로비저닝 프로필 삭제 실패	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30일
디지털 인증서 목록 요청 실패	CERTIFICATELIST_COMMAND_FAILED	30일
설치된 애플리케이션 목록 요청 실패	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30일
모바일 기기에 대한 일반 정보 요청 실패	DEVICEINFORMATION_COMMAND_FAILED	30일
보안 정보 요청 실패	SECURITYINFO_COMMAND_FAILED	30일
모바일 기기 잠금 실패	DEVICELOCK_COMMAND_FAILED	30일
암호 초기화 실패	CLEARPASSCODE_COMMAND_FAILED	30일
모바일 기기에서 데이터 삭제 실패	ERASEDEVICE_COMMAND_FAILED	30일
앱 설치 실패	INSTALLAPPLICATION_COMMAND_FAILED	30일
앱에 대한 교환 코드 설정 실패	APPLYREDEMPTIONCODE_COMMAND_FAILED	30일
관리 중인 앱 목록 요청 실패	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30일
관리 중인 앱 제거 실패	REMOVEAPPLICATION_COMMAND_FAILED	30일
로밍 설정 거부	SETROAMINGSETTINGS_COMMAND_FAILED	30일
앱 동작 중 오류 발생	PRODUCT_FAILURE	30일
명령 결과에 잘못된 데이터가 있습니다	MALFORMED_COMMAND	30일
푸시 알림 전송 실패	SEND_PUSH_NOTIFICATION_FAILED	30일
명령 전송 실패	SEND_COMMAND_FAILED	30일
기기를 찾을 수 없습니다	DEVICE_NOT_FOUND	30일

iOS MDM 서버 경고 이벤트

아래 표에는 **경고** 심각도를 가진 Kaspersky Security Center iOS MDM 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

iOS MDM 서버 경고 이벤트

이벤트 유형 표시 이름	이벤트 유형	기본 저장 기간
잠긴 모바일 기기로의 연결 시도가 탐지되었습니다	INACTICE_DEVICE_TRY_CONNECTED	30일
프로필이 삭제되었습니다	MDM_PROFILE_WAS_REMOVED	30일
클라이언트 인증서를 재사용하려는 시도가 탐지되었습니다	CLIENT_CERT_ALREADY_IN_USE	30일
비활성 기기가 탐지되었습니다	FOUND_INACTIVE_DEVICE	30일
교환 코드가 필요합니다	NEED_REDEMPTION_CODE	30일
정책에 포함된 프로필이 기기에서 제거되었습니다	UMDM_PROFILE_WAS_REMOVED	30일

iOS MDM 서버 정보 이벤트

표에는 **정보** 심각도를 가진 Kaspersky Security Center iOS MDM 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

iOS MDM 서버 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형	기본 저장 기간
새 모바일 기기가 연결되었습니다	NEW_DEVICE_CONNECTED	30일
프로필 목록을 성공적으로 요청했습니다	PROFILELIST_COMMAND_SUCCESSFULL	30일
프로필을 성공적으로 설치했습니다	INSTALLPROFILE_COMMAND_SUCCESSFULL	30일
프로필을 성공적으로 삭제했습니다	REMOVEPROFILE_COMMAND_SUCCESSFULL	30일
프로비저닝 프로필 목록을 성공적으로 요청했습니다	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30일
프로비저닝 프로필을 성공적으로 설치했습니다	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30일
프로비저닝 프로필을 성공적으로 제거했습니다	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30일
디지털 인증서 목록을 성공적으로 요청했습니다	CERTIFICATELIST_COMMAND_SUCCESSFULL	30일
설치된 애플리케이션 목록을 성공적으로 요청했습니다	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30일
모바일 기기에 대한 일반 정보를 성공적으로 요청했습니다	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30일
보안 정보를 성공적으로 요청했습니다	SECURITYINFO_COMMAND_SUCCESSFULL	30일
모바일 기기가 성공적으로 잠겼습니다	DEVICELOCK_COMMAND_SUCCESSFULL	30일
암호를 성공적으로 초기화했습니다	CLEARPASSCODE_COMMAND_SUCCESSFULL	30일
모바일 기기에서 데이터를 성공적으로 삭제했습니다	ERASEDEVICE_COMMAND_SUCCESSFULL	30일
앱을 성공적으로 설치했습니다	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30일
이 앱에 대해 교환 코드를 성공적으로 설정했습니다	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30일
관리 중인 앱 목록을 성공적으로 요청했습니다	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30일
관리 중인 앱을 성공적으로 제거했습니다	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30일
로밍 설정을 성공적으로 적용했습니다	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30일

자주 등록된 이벤트 차단 중

이 섹션에서는 자주 등록된 이벤트 차단 관리, 자주 등록된 이벤트 차단 제거 및 자주 등록된 이벤트 목록을 파일로 내보내기에 대한 정보를 제공합니다.

자주 등록된 이벤트 차단 정보

관리 중인 애플리케이션(예: Kaspersky Endpoint Security for Windows)이 하나 또는 여러 개의 관리 중인 기기에 설치된 경우 동일한 유형의 여러 이벤트를 중앙 관리 서버로 보낼 수 있습니다. 자주 등록된 이벤트를 수신하면 중앙 관리 서버의 데이터베이스에 과부하가 발생하고 다른 이벤트를 덮어 쓸 수 있습니다. 중앙 관리 서버는 수신된 모든 이벤트의 수가 데이터베이스에 지정된 제한을 초과하면 가장 자주 등록된 이벤트 차단을 시작합니다.

중앙 관리 서버에서는 자주 등록된 이벤트가 자동으로 수신되지 않도록 차단합니다. 자주 등록된 이벤트를 직접 차단하거나 차단할 이벤트를 선택할 수는 없습니다.

이벤트가 차단되었는지 확인하려면 이 이벤트가 중앙 관리 서버 속성의 **자주 등록된 이벤트 차단 중** 섹션에 존재하는지 확인하면 됩니다. 이벤트가 차단된 경우 다음을 수행할 수 있습니다:

- 데이터베이스 덮어 쓰기를 방지하려면 이러한 유형의 이벤트 수신을 계속 차단하면 됩니다.
- 예를 들어 자주 등록된 이벤트를 중앙 관리 서버로 전송하는 이유를 알아보려면 자주 등록된 이벤트의 차단을 해제 하고 이 유형의 이벤트를 계속 수신합니다.
- 자주 등록된 이벤트가 다시 차단될 때까지 계속 수신하려면 자주 등록된 이벤트 차단에서 제거하면 됩니다.

자주 등록된 이벤트 차단 관리

중앙 관리 서버에서는 자주 등록된 이벤트의 수신을 자동으로 차단하지만 차단을 중지하고 자주 등록된 이벤트를 계속 수신할 수 있습니다. 이전에 차단 해제한 자주 등록된 이벤트 수신을 차단할 수도 있습니다.

자주 등록된 이벤트 차단을 관리하려면:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창에서 **섹션** 창으로 이동한 다음 **자주 등록된 이벤트 차단 중**을 선택합니다.
3. **자주 등록된 이벤트 차단 중** 섹션에서:
   - 수신을 차단할 이벤트의 **이벤트 유형** 옵션을 선택합니다.
   - 수신을 계속할 이벤트의 **이벤트 유형** 옵션을 선택 취소합니다.
4. **적용** 버튼을 클릭합니다.
5. **확인** 버튼을 누릅니다.

중앙 관리 서버에서 **이벤트 유형** 옵션을 선택 취소한 자주 등록된 이벤트를 수신하고 **이벤트 유형** 옵션을 선택한 자주 등록된 이벤트의 수신은 차단합니다.

자주 등록된 이벤트 차단 제거

자주 등록된 이벤트에 대한 차단을 제거하고 중앙 관리 서버에서 이러한 유형의 자주 등록된 이벤트를 다시 차단할 때까지 수신하기 시작할 수 있습니다.

자주 등록된 이벤트의 차단을 해제하려면 다음을 수행합니다.

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창에서 **섹션** 창으로 이동한 다음 **자주 등록된 이벤트 차단 중**을 선택합니다.
3. **자주 등록된 이벤트 차단 중** 섹션에서 차단을 제거할 자주 등록된 이벤트의 행을 클릭합니다.
4. **삭제** 버튼을 누릅니다.

자주 등록된 이벤트가 자주 등록된 이벤트 목록에서 제거됩니다. 중앙 관리 서버에서 이 유형의 이벤트를 수신합니다.

자주 등록된 이벤트 목록을 파일로 내보내기

자주 등록된 이벤트 목록을 파일로 내보내려면:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창에서 **섹션** 창으로 이동한 다음 **자주 등록된 이벤트 차단 중**을 선택합니다.
3. **파일로 내보내기** 버튼을 누릅니다.
4. **다른 이름으로 저장** 창이 열리면 목록을 저장할 파일의 경로를 지정합니다.
5. **저장** 버튼을 누릅니다.

자주 등록된 이벤트 목록의 모든 레코드를 파일로 내보냅니다.

가상 컴퓨터의 상태 변경 사항 제어

중앙 관리 서버는 자산 관리(하드웨어) 및 설치된 애플리케이션의 목록, 관리 대상 애플리케이션, 작업 및 정책의 설정 등과 같은 관리 중인 기기의 상태 정보를 저장합니다. 가상 컴퓨터가 관리 중인 기기일 경우 사용자는 언제든지 이전에 만든 가상 컴퓨터의 스냅샷을 사용하여 상태를 복원할 수 있습니다. 중앙 관리 서버에 저장된 가상 컴퓨터의 상태에 대한 정보가 최신 정보와 다를 수 있습니다.

예를 들어 관리자가 오후 12시에 중앙 관리 서버의 보호 정책을 만들어 오후 12시 1분에 VM_1 가상 컴퓨터에서 실행을 시작했습니다. 오후 12시 30분에 VM_1 가상 컴퓨터의 사용자가 오전 11시에 생성된 스냅샷으로 가상 컴퓨터를 복원하여 상태가 변경되었습니다. 이때는 가상 컴퓨터에서 보호 정책의 실행이 중단됩니다. 그러나 중앙 관리 서버에 저장된 이전 정보에 따르면 VM_1 가상 컴퓨터에서 보호 정책이 계속 실행 중인 것으로 나옵니다.

Kaspersky Security Center를 통해 가상 컴퓨터의 상태에 관한 모든 변경 사항을 감시할 수 있습니다.

기기와의 동기화 후 항상 중앙 관리 서버는 고유 ID를 생성하여 기기와 중앙 관리 서버에서 보관합니다. 다음 동기화를 시작하기 전 중앙 관리 서버는 두 곳에서 보관되고 있는 이 ID의 값을 비교합니다. ID의 값이 일치하지 않을 경우 중앙 관리 서버는 가상 컴퓨터가 스냅샷에서 복원된 것으로 간주합니다. 중앙 관리 서버는 가상 컴퓨터에 활성화된 정책과 작업의 모든 설정을 재설정하고 최신 정책과 그룹 작업의 목록을 전송합니다.

시스템 레지스트리의 정보를 사용하여 안티 바이러스 보호 상태 모니터링

기기의 운영 체제에 따라 네트워크 에이전트를 통해 기록된 정보를 사용하여 클라이언트 기기에서 안티 바이러스 보호 상태를 모니터링하려면 다음과 같이 하십시오:

- Windows를 실행하는 기기에서:

  1. 클라이언트 기기의 시스템 레지스트리를 엽니다(예:로컬에서 **시작 → 실행** 메뉴의 regedit 명령 사용).
  2. 다음 하이브로 이동합니다:

     - 32비트 운영 체제:
       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState
     - 64비트 운영 체제:
       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     시스템 레지스트리에 클라이언트 기기의 안티 바이러스 보호 상태 정보가 표시됩니다.

- Linux를 실행하는 기기에서:

  - 정보는 /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/에 각 데이터 유형마다 하나씩 별도의 텍스트 파일에 첨부되어 있습니다.

- macOS를 실행하는 기기에서:

  - 정보는 /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/에서 각 데이터 유형마다 하나씩 별도의 텍스트 파일로 묶습니다.

안티 바이러스 보호 상태는 아래 표에 명시된 키 값에 해당합니다.

레지스트리 키 및 가능한 키 값

키(데이터 유형)	값	설명
`Protection_LastConnected (REG_SZ)`	DD-MM-YYYY HH-MM-SS	중앙 관리 서버에 마지막으로 연결한 날짜 및 시간(UTC 형식)
`Protection_AdmServer (REG_SZ)`	IP, DNS 이름 또는 NetBIOS 이름	기기를 관리하는 중앙 관리 서버의 이름
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	기기에 설치된 네트워크 에이전트의 빌드 번호

키(데이터 유형)	값	설명
Protection_NagentFullVersion (REG_SZ)	a.b.c.d(patch1; patch2; ...; patchN)	기기에 설치된 네트워크 에이전트 버전의 전체 번호(패치 포함)
Protection_HostId (REG_SZ)	기기 ID	기기의 ID
Protection_DynamicVM (REG_DWORD)	0 — 아니요 1 — 예	네트워크 에이전트가 동적 VDI 모드로 설치됩니다
Protection_AvInstalled (REG_DWORD)	0 — 아니요 1 — 예	보안 제품이 기기에 설치됩니다
Protection_AvRunning (REG_DWORD)	0 — 아니요 1 — 예	기기에서 실시간 보호가 활성화됩니다
Protection_HasRtp (REG_DWORD)	0 — 아니요 1 — 예	실시간 보호 구성 요소가 설치됩니다
Protection_RtpState (REG_DWORD)	실시간 보호 상태:	
	0	알 수 없음
	1	비활성됨
	2	일시 중지됨
	3	시작 중
	4	활성됨
	5	높은 보호 레벨로 활성화됨(최대 보호)
	6	낮은 보호 레벨로 활성화됨(최대 속도)
	7	기본(권장) 설정으로 활성화됨
	8	사용자 지정 설정으로 활성화됨
	9	작동 오류
Protection_LastFscan (REG_SZ)	DD-MM-YYYY HH-MM-SS	마지막 전체 검사를 수행한 날짜 및 시간(UTC 형식)
Protection_BasesDate (REG_SZ)	DD-MM-YYYY HH-MM-SS	애플리케이션 데이터베이스 배포 날짜 및 시간(UTC 형식)

기기가 비활성 상태로 표시될 때 작업 보기 및 구성

그룹 내의 클라이언트 기기가 비활성 상태인 경우 해당 상태에 대한 알림을 받을 수 있습니다. 이러한 기기를 자동으로 삭제할 수도 있습니다.

그룹의 기기가 비활성 상태로 표시될 때 작업을 보거나 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 관리 그룹의 이름을 마우스 오른쪽 버튼으로 누릅니다.
2. 책 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   그러면 관리 그룹 속성 창이 열립니다.
3. **속성** 창에서 **기기** 섹션으로 이동합니다.
4. 필요한 경우 다음 옵션을 활성화하거나 비활성화합니다:

   - **기기가 다음 비활성 기간을 초과하면 관리자에게 알림(일)**

     이 옵션을 활성화하면 관리자에게 비활성 기기 관련 알림이 수신됩니다. **너무 오랫동안 기기가 네트워크에 접속하지 않았습니다** 이벤트가 만들어질 때까지의 기간을 지정할 수 있습니다. 기본 기간은 7일입니다.

기본적으로 이 옵션은 켜져 있습니다.

- **기기가 다음 비활성 기간을 초과하면 그룹에서 기기 제거(일)**

  이 옵션을 활성화하면 기기가 그룹에서 자동으로 제거될 때까지의 시간 간격을 지정할 수 있습니다. 기본 기간은 60일입니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **부모 그룹에서 상속**

  이 섹션의 설정이 클라이언트 기기가 포함된 부모 그룹에서 상속됩니다. 이 옵션을 활성화하면 **네트워크에서의 기기 활동**의 설정이 변경되지 않도록 잠깁니다.

  이 옵션은 관리 그룹에 부모 그룹이 있는 경우에만 사용할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **자식 그룹에 강제 상속**

  이 설정 값은 자식 그룹에 배포되지만 자식 그룹의 속성에서는 이러한 설정이 잠깁니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

5. **확인**를 누릅니다.

   변경 내용이 저장 및 적용됩니다.

Kaspersky 공지 비활성화

Kaspersky Security Center 웹 콘솔에서 Kaspersky 공지 섹션(**모니터링 및 보고 → Kaspersky 공지**)에서는 사용 중인 Kaspersky Security Center 버전과 관리 중인 기기에 설치된 관리 애플리케이션에 대한 정보를 계속 제공합니다. Kaspersky 공지를 받고 싶지 않으면 이 기능을 비활성화할 수 있습니다.

Kaspersky 공지에는 보안 관련 공지와 마케팅 공지 등 두 가지 유형의 정보가 포함됩니다. 각 유형의 공지를 개별적으로 비활성화할 수 있습니다.

보안 관련 공지 비활성화하기:

1. 콘솔 트리에서 보안 관련 공지 사항을 비활성화할 중앙 관리 서버를 선택합니다.
2. 마우스 오른쪽 버튼을 클릭하고 표시되는 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창이 열리면 **Kaspersky 공지 사항** 섹션에서 **Kaspersky Security Center 웹 콘솔에서 Kaspersky 공지 사항 디스플레이 사용** 옵션을 비활성화합니다.
4. **확인**을 누릅니다.

   Kaspersky 공지가 비활성화됩니다.

마케팅 공지는 기본적으로 비활성화되어 있습니다. Kaspersky Security Network(KSN)를 활성화한 경우에만 마케팅 공지를 받을 수 있습니다. KSN을 비활성화하여 이러한 유형의 공지를 비활성화할 수 있습니다.

배포 지점 및 연결 게이트웨이 조정

Kaspersky Security Center의 관리 그룹 구조는 다음과 같은 기능을 수행합니다:

- 정책의 범위 설정

  *정책 프로필*을 사용하여 기기에서 관련 설정 모음을 적용할 수도 있습니다. 이때는 태그, Active Directory 조직 구성 단위의 기기 위치, Active Directory 보안 그룹의 구성원 자격 등을 사용하여 정책의 범위를 설정합니다.

- 그룹 작업의 범위 설정

  관리 그룹의 계층 구조를 기준으로 하지 않는 그룹 작업은 특정 방식으로 범위를 정의합니다: 즉, 이러한 작업의 경우에는 기기 조회용 작업과 특정 기기용 작업을 사용합니다.

- 기기, 가상 중앙 관리 서버 및 보조 중앙 관리 서버에 대한 접근 권한 설정

- 배포 지점 할당

관리 그룹의 구조를 작성할 때는 배포 지점을 가장 적절하게 할당할 수 있도록 조직 네트워크의 토폴로지를 고려해야 합니다. 배포 지점을 최적의 방식으로 배포하면 조직 네트워크의 트래픽을 절약할 수 있습니다.

조직 스키마와 네트워크 토폴로지에 따라 관리 그룹 구조에 다음 표준 구성을 적용할 수 있습니다:

- 단일 사무소

- 다수의 소규모 원격 사무소

배포 지점 기능을 하는 기기는 무단으로 접근할 수 없도록 보호(물리적 보호 포함)해야 합니다.

배포 지점의 표준 구성: 단일 사무소

표준 "단일 사무소" 구성에서는 모든 기기가 조직 네트워크에 있으므로 기기 간에 서로 "인식"할 수 있습니다. 조직 네트워크는 협채널을 통해 연결된 몇 개의 개별 요소(네트워크 또는 네트워크 세그먼트)로 구성될 수 있습니다.

관리 그룹 구조를 구성하는 데 사용할 수 있는 방법은 다음과 같습니다:

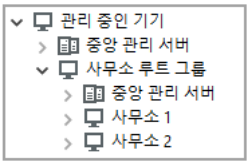
- 네트워크 토폴로지를 고려하여 관리 그룹 구조 구성. 관리 그룹의 구조가 정밀하게 네트워크 토폴로지를 반영하지 않을 수 있습니다. 네트워크의 각 부분과 특정 관리 그룹을 연결하는 걸로도 충분합니다. 배포 지점의 자동 할당을 사용할 수도 있고 수동으로 할당할 수도 있습니다.

- 네트워크 토폴로지를 고려하지 않고 관리 그룹 구조 구성. 이 경우 배포 지점의 자동 할당을 비활성하고 네트워크의 각 부분(예: **관리 중인 기기** 그룹)에서 하나 이상의 기기가 루트 관리 그룹의 배포 지점 역할을 하도록 직접 지정해야 합니다. 모든 배포 지점은 동일한 수준에 있으며 조직 네트워크의 모든 기기에 동일한 영역을 적용합니다. 이때, 각 네트워크 에이전트는 경로가 가장 짧은 배포 지점과 연결됩니다. 배포 지점 연결 경로는 tracert 유틸리티로 추적할 수 있습니다.

배포 지점의 표준 구성: 다수의 소규모 원격 사무소

이 표준 구성은 인터넷을 통해 본사 사무소와 통신할 수 있는 여러 소규모 원격 사무소를 제공합니다. 각 원격 사무소에는 NAT가 적용됩니다. 즉, 원격 사무소는 서로 격리되므로 사무소 간의 연결은 불가능합니다.

이 구성을 관리 그룹 구조에 반영해야 합니다: 각 원격 사무소에 대해 별도의 관리 그룹(아래 그림의 **사무소 1** 및 **사무소 2** 그룹)을 만들어야 합니다.



관리 그룹 구조에 포함된 원격 사무소

사무소에 해당하는 각 관리 그룹에는 배포 지점을 하나 이상 할당해야 합니다. 배포 지점은 원격 사무소의 기기여야 하며, 디스크에 여유 공간이 충분해야 합니다. 예를 들어 **사무소 1** 그룹에 배포된 기기는 **사무소 1** 관리 그룹에 할당된 배포 지점에 접근합니다.

일부 사용자가 노트북을 소지하고 사무소 간을 실제로 이동하는 경우에는 기존 배포 지점 외에 각 원격 사무소에서 둘 이상의 기기를 선택하여 상위 레벨 관리 그룹(위 그림에서는 **사무소 루트 그룹**)의 배포 지점 역할을 하도록 할당해야 합니다.

예: **사무소 1** 관리 그룹에 배포된 노트북이 **사무소 2** 관리 그룹에 해당하는 사무소로 실제로 이동되었습니다. 노트북이 이동된 후 네트워크 에이전트가 **사무소 1** 그룹에 할당된 배포 지점 접근을 시도하지만 해당 배포 지점은 사용할 수 없는 상태입니다. 그러면 네트워크 에이전트는 **사무소 루트 그룹**에 할당된 배포 지점에 대한 접근 시도를 시작합니다. 원격 사무소는 서로 격리되어 있으므로 **사무소 루트 그룹** 관리 그룹에 할당된 배포 지점 접근 시도는 네트워크 에이전트가 **사무소 2** 그룹의 배포 지점 접근을 시도할 때만 성공합니다. 즉, 노트북은 초기 사무소에 해당하는 관리 그룹에 그대로 유지되지만 해당 시점에 물리적으로 위치해 있는 사무소의 배포 지점을 사용합니다.

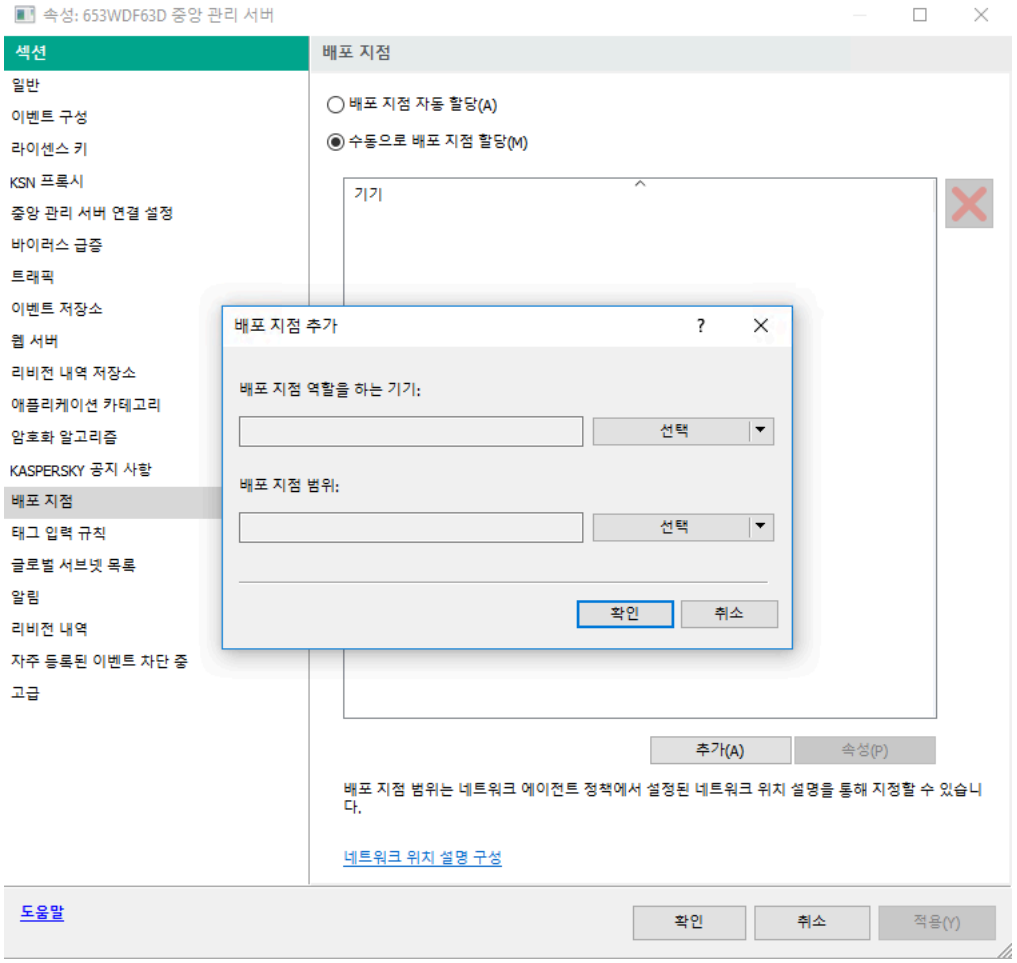
배포 지점 역할을 할 관리 중인 기기 추가

관리 그룹에 대한 배포 지점 역할을 수행하는 기기를 수동으로 할당할 수 있으며 관리 콘솔에서 연결 게이트웨이로 해당 기기를 구성할 수 있습니다.

기기를 관리 그룹의 배포 지점로 할당하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창에서 **배포 지점** 섹션을 선택합니다.
4. 창의 오른쪽에서 **수동으로 배포 지점 할당** 옵션을 선택합니다.

5. **추가** 버튼을 누릅니다.



배포 지점 수동 할당

배포 지점 추가 창이 열립니다.

6. **배포 지점 추가** 창에서 다음 동작을 수행합니다:

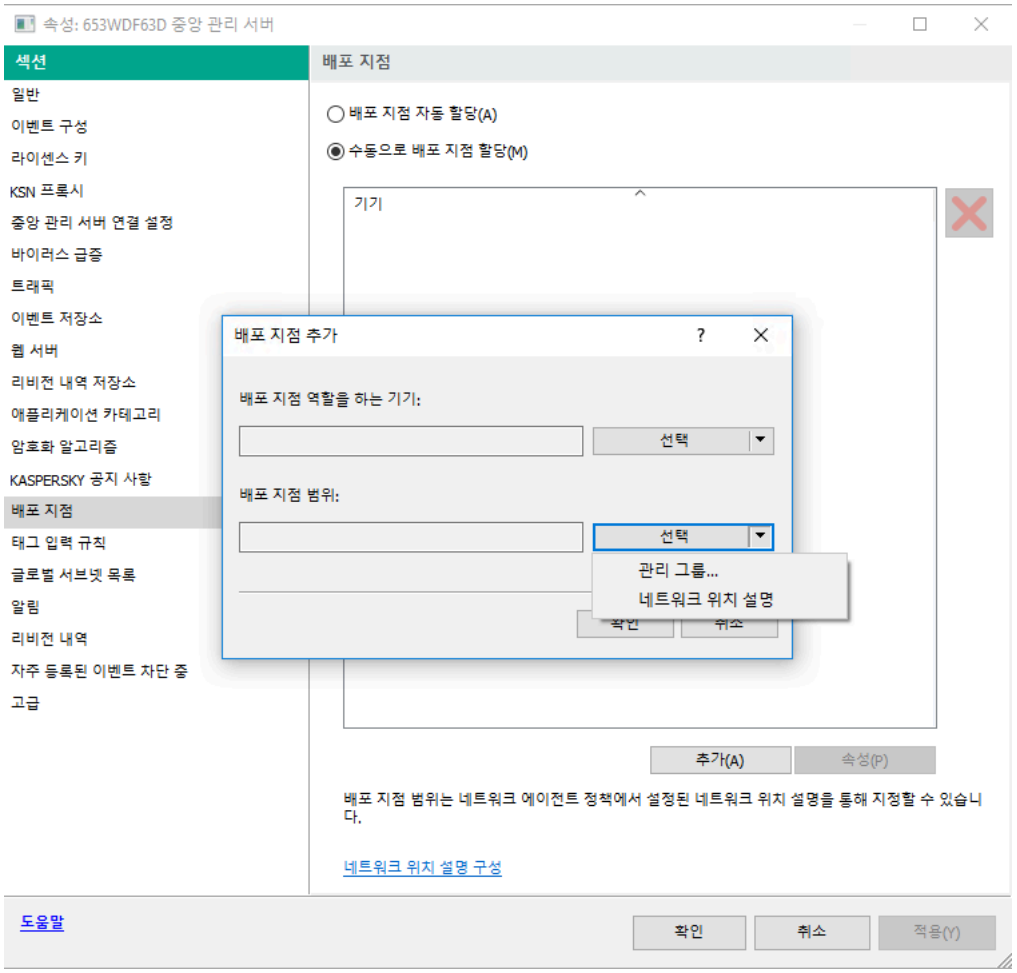
   a. **배포 지점 역할을 하는 기기**에서 **선택** 분할 버튼의 아래쪽 화살표(▾)를 클릭하고 **그룹에서 기기 추가** 옵션을 선택합니다.

   b. **기기 선택** 창이 열리면 배포 지점 역할을 할 기기를 선택합니다.

   c. **배포 지점 범위**에서 **선택** 분할 버튼의 아래쪽 화살표(▾)를 클릭합니다.

d. 배포 지점이 업데이트를 배포할 특정 기기를 지정합니다. 관리 그룹 또는 네트워크 위치 설명을 지정할 수 있습니다.

e. **확인**를 클릭하여 **배포 지점 추가** 창을 닫습니다.



배포 지점 범위 선택

추가한 배포 지점은 **배포 지점** 섹션의 배포 지점 목록에 표시됩니다.

가상 중앙 관리 서버에 연결하는 네트워크 에이전트를 가진 최초의 기기는 자동으로 배포 지점 역할을 수행하도록 할당되며 연결 게이트웨이로 구성됩니다.

완충 지대에서 Linux 기기를 게이트웨이로 연결

완충 지대(DMZ)에서 Linux 기기를 게이트웨이로 연결:

1. Linux 기기에 네트워크 에이전트를 다운로드하여 설치합니다.

2. 설치 후 스크립트를 실행하고 마법사를 따라 로컬 환경 구성을 설정합니다. 명령 프롬프트에서 다음 명령을 실행하십시오.

   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. 네트워크 에이전트 모드 지정 단계에서 **연결 게이트웨이로 사용** 옵션을 선택합니다.

4. MMC 기반 관리 콘솔에서 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

5. 중앙 관리 서버 속성 창이 열리면 **배포 지점** 섹션을 선택합니다.

6. **배포 지점** 창이 열리면 창 오른쪽에서:

   a. **수동으로 배포 지점 할당** 옵션을 선택합니다.

   b. **추가** 버튼을 누릅니다.

   배포 지점 추가 창이 열립니다.

7. **배포 지점 추가** 창에서 다음 동작을 수행합니다:

   a. **배포 지점 역할을 하는 기기**에서 **선택** 분할 버튼의 아래쪽 화살표(▾)를 클릭하고 **주소로 DMZ에 연결 게이트웨이 추가** 옵션을 선택합니다.

   b. **배포 지점 범위**에서 **선택** 분할 버튼의 아래쪽 화살표(▾)를 클릭합니다.

   c. 배포 지점이 업데이트를 배포할 특정 기기를 지정합니다. 관리 그룹을 지정할 수 있습니다.

   d. **확인**를 클릭하여 **배포 지점 추가** 창을 닫습니다.

8. 추가한 배포 지점은 **배포 지점** 섹션의 배포 지점 목록에 표시됩니다.

9. Kaspersky Security Center 연결이 성공적으로 구성되었는지 확인하려면 klnagchk 유틸리티를 실행하십시오. 명령 프롬프트에서 다음 명령 실행:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. 메인 애플리케이션 창에서 Kaspersky Security Center로 이동하여 기기를 검색합니다.

11. 창이 열리면 <기기 이름>을 클릭합니다.

12. 드롭다운 목록에서 **그룹으로 이동** 링크를 선택합니다.

13. **그룹 선택** 창이 열리면 **배포 지점** 링크를 클릭합니다.

14. **확인**을 누릅니다.

15. 명령 프롬프트에서 다음 명령을 실행하여 Linux 클라이언트에서 네트워크 에이전트 서비스를 다시 시작합니다.
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

DMZ에서 Linux 기기를 게이트웨이로 연결하는 작업이 완료되었습니다.

그런 다음 구성된 연결 게이트웨이를 통해 Linux 기기를 중앙 관리 서버에 연결할 수 있습니다. 기본 설치 시나리오를 완료한 후에만 이 절차를 따르십시오.

연결 게이트웨이를 통해 Linux 기기를 중앙 관리 서버에 연결

연결 게이트웨이를 사용하면 DMZ의 클라이언트 기기를 중앙 관리 서버에 연결할 수 있습니다. Windows 기반 및 Linux 기반 기기는 연결 게이트웨이 역할을 할 수 있습니다. 연결 게이트웨이를 연결하고 구성한 후 이 게이트웨이를 사용하여 Linux 기기를 중앙 관리 서버에 연결할 수 있습니다. 기본 설치 시나리오를 먼저 완료한 후에 다음 절차를 수행하십시오.

연결 게이트웨이를 통해 Linux 기기를 중앙 관리 서버에 연결하려면 이 기기에서 다음 작업을 수행하십시오.

1. Linux 기기에 네트워크 에이전트를 다운로드하여 설치합니다.

2. 명령 프롬프트에서 다음 명령을 실행하여 네트워크 에이전트 post-install 스크립트를 실행합니다.
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. 네트워크 에이전트 모드 지정 단계에서 **연결 게이트웨이를 사용하여 서버에 연결** 옵션을 선택한 후 연결 게이트웨이 주소를 입력합니다.

4. 명령 프롬프트에서 다음 명령을 사용하여 Kaspersky Security Center 및 연결 게이트웨이와의 연결을 확인합니다.
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   연결 게이트웨이의 주소가 출력에 표시됩니다.

연결 게이트웨이를 통해 Linux 기기를 중앙 관리 서버에 연결하는 작업이 완료되었습니다. 이 기기를 사용하여 배포를 업데이트하고 애플리케이션을 원격으로 설치하고 네트워크 기기에 대한 정보를 검색할 수 있습니다.

DMZ에 배포 지점으로 연결 게이트웨이 추가

연결 게이트웨이는 중앙 관리 서버로의 연결을 설정하기보다 중앙 관리 서버로부터의 연결을 기다립니다. 즉, 연결 게이트웨이를 DMZ의 기기에 설치한 직후에는 중앙 관리 서버에 이 기기가 관리 중인 기기로 나열되지 않습니다. 따라서 특별한 절차를 통해 중앙 관리 서버가 연결 게이트웨이로의 연결을 초기화하도록 해야 합니다.

연결 게이트웨이 기기를 배포 지점으로 추가하는 방법:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.

2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

3. 중앙 관리 서버 속성 창에서 **배포 지점** 섹션을 선택합니다.

4. 창의 오른쪽에서 **수동으로 배포 지점 할당** 옵션을 선택합니다.

5. **추가** 버튼을 누릅니다.
   배포 지점 추가 창이 열립니다.

6. **배포 지점 추가** 창에서 다음 동작을 수행합니다:

   a. **배포 지점 역할을 하는 기기**에서 **선택** 분할 버튼의 아래쪽 화살표(▾)를 클릭하고 **주소로 DMZ에 있는 연결 게이트웨이 추가** 옵션을 선택합니다.

   b. 열리는 **연결 게이트웨이 주소 입력** 창에서 연결 게이트웨이 의 IP 주소를 입력합니다(또는 이름으로 연결 게이트웨이에 액세스할 수 있는 경우 이름 입력).

   c. **배포 지점 범위**에서 **선택** 분할 버튼의 아래쪽 화살표(▾)를 클릭합니다.

   d. 배포 지점이 업데이트를 배포할 특정 기기를 지정합니다. 관리 그룹 또는 네트워크 위치 설명을 지정할 수 있습니다.
      외부 관리 중인 기기에 대해 별도 그룹을 생성하는 것이 좋습니다.

이 작업을 수행하고 나면 배포 지점 목록에 이름이 **연결 게이트웨이용 임시 항목**이라는 새 항목이 포함됩니다.

중앙 관리 서버는 사용자가 지정한 주소의 연결 게이트웨이에 거의 즉시 연결을 시도합니다. 성공하면 항목 이름이 연결 게이트웨이 기기의 이름으로 변경됩니다. 이 프로세스는 최대 5분이 소요됩니다.

연결 게이트웨이용 임시 항목이 이름이 지정된 항목으로 변환되는 동안 연결 게이트웨이는 **미할당 기기** 그룹에도 표시됩니다.

이전에 구성된 네트워크에 연결 게이트웨이를 추가하려면, 새로 추가된 연결 게이트웨이와 연결하려는 기기에 네트워크 에이전트를 다시 설치하십시오.

배포 지점 자동 할당

배포 지점을 자동으로 할당하는 것이 좋습니다. 그러면 Kaspersky Security Center는 배포 지점을 할당해야 하는 기기를 자체적으로 선택합니다.

배포 지점을 자동으로 할당하려면 다음 절차를 따르십시오.

1. 메인 애플리케이션 창을 엽니다.
2. 콘솔 트리에서 배포 지점을 자동으로 할당할 중앙 관리 서버 노드를 선택합니다.
3. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 클릭합니다.
4. 중앙 관리 서버 속성 창의 **섹션** 창에서 **배포 지점**를 차례로 선택합니다.
5. 창의 오른쪽에서 **배포 지점 자동 할당** 옵션을 선택합니다.

   배포 지점 역할을 수행하는 기기를 자동으로 할당하면, 배포 지점을 수동으로 구성할 수 없으며 배포 지점 목록도 편집할 수 없습니다.

6. **확인**을 누릅니다.

중앙 관리 서버는 자동으로 배포 지점을 할당하고 구성합니다.

배포 지점으로 선택한 기기에 네트워크 에이전트 로컬 설치 정보

배포 지점으로 선택된 기기를 가상 중앙 관리 서버에 직접 연결한 다음 연결 게이트웨이 역할을 할 수 있도록 하려면 해당 기기에 네트워크 에이전트를 로컬로 설치해야 합니다.

배포 지점 역할이 할당된 기기에 네트워크 에이전트를 로컬 설치하는 절차는 임의의 네트워크 기기에 네트워크 에이전트를 로컬 설치하는 절차와 동일합니다.

배포 지점로 선택한 기기는 다음 조건을 충족해야 합니다:

- 네트워크 에이전트 로컬 설치 중에 설치 마법사의 **중앙 관리 서버** 창에 있는 **서버 주소** 필드에서 기기를 관리하는 가상 중앙 관리 서버의 주소를 지정합니다. 기기 IP 주소 또는 Windows 네트워크상의 기기 이름을 사용할 수 있습니다.

  가상 중앙 관리 서버 주소에 <가상 서버가 속해 있는 물리적 중앙 관리 서버의 전체 주소>/<가상 중앙 관리 서버의 이름> 형식을 사용합니다.

- 해당 기기가 연결 게이트웨이 역할을 할 수 있도록 중앙 관리 서버와의 통신에 필요한 기기의 모든 포트를 개방합니다.

지정된 설정을 갖는 네트워크 에이전트를 기기에 설치한 후 Kaspersky Security Center는 다음 작업을 자동으로 수행합니다:

- 이 기기를 가상 중앙 관리 서버의 **관리 중인 기기** 그룹에 포함합니다.
- 이 기기가 가상 중앙 관리 서버의 **관리 중인 기기** 그룹의 배포 지점 역할을 하도록 할당합니다.

조직 네트워크 내에서 **관리 중인 기기** 그룹의 배포 지점 역할이 할당된 기기에 네트워크 에이전트를 로컬 설치해야 하며 이 설치만으로 충분합니다. 중첩된 관리 그룹에서 배포 지점 역할을 하는 기기에 네트워크 에이전트를 원격으로 설치할 수 있습니다. 이렇게 하려면 **관리 중인 기기** 그룹의 배포 지점을 연결 게이트웨이로 사용합니다.

배포 지점을 연결 게이트웨이로 사용 정보

중앙 관리 서버가 DMZ(완충 지역) 외부에 있으면 이 지역의 네트워크 에이전트가 중앙 관리 서버에 연결할 수 없습니다.

중앙 관리 서버를 네트워크 에이전트와 연결할 때는 배포 지점을 연결 게이트웨이로 사용할 수 있습니다. 배포 지점은 연결을 생성하기 위해 중앙 관리 서버에 대한 포트를 엽니다. 중앙 관리 서버는 시작 시 배포 지점에 연결하며 전체 세션 동안 이 연결을 유지합니다.

배포 지점은 중앙 관리 서버에서 신호를 받는 즉시 중앙 관리 서버에 대한 연결을 허용하기 위해 UDP 신호를 네트워크 에이전트로 보냅니다. 네트워크 에이전트는 해당 신호를 받으면 배포 지점에 연결하며, 그러면 네트워크 에이전트와 중앙 관리 서버 간에 정보가 교환됩니다. 정보 교환은 IPv4 또는 IPv6 네트워크를 통해 발생할 수 있습니다.

특별히 할당된 기기를 연결 게이트웨이로 사용하고 이 연결 게이트웨이로 최대 10,000대의 클라이언트 기기(모바일 기기 포함)를 담당하는 것이 좋습니다.

이전에 구성된 네트워크에 연결 게이트웨이를 추가하려면:

1. 연결 게이트웨이 모드에 네트워크 에이전트 설치.
2. 새로 추가된 연결 게이트웨이에 연결하려는 기기에 네트워크 에이전트를 다시 설치하십시오.

배포 지점에서 검색되는 범위 목록에 IP 범위 추가

배포 지점에서 검색되는 범위 목록에 IP 범위를 추가할 수 있습니다.

검색한 범위 목록에 IP 범위를 추가하려면 다음과 같이 하십시오.

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 기기의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창이 열리면 **배포 지점** 섹션을 선택합니다.
4. 목록에서 필요한 배포 지점을 선택하고 **속성**을 누릅니다.
5. 배포 지점 속성 창이 열리면 왼쪽 **섹션** 창에서 **기기 발견 → IP 범위**를 선택합니다.
6. **범위 검색 사용** 확인란을 선택합니다.
7. **추가** 버튼을 누릅니다.
   범위 검색 사용 확인란을 선택한 경우만 **추가** 버튼이 활성화됩니다.
   IP 범위 창이 열립니다.
8. **IP 범위** 창에서 새 IP 범위의 이름을 입력합니다(기본 이름: 새 범위).
9. **추가** 버튼을 누릅니다.
10. 다음 중 하나를 수행합니다:
    - 시작 및 종료 IP 주소를 사용하여 IP 범위를 지정합니다.
    - 주소 및 서브넷 마스크를 사용하여 IP 범위를 지정합니다.
    - **찾기**를 누르고 글로벌 서브넷 목록에서 서브넷을 추가합니다.
11. **확인**를 누릅니다.
12. **확인**를 눌러 지정한 이름의 새 범위를 추가합니다.

    새 범위가 검색한 범위 목록에 표시됩니다.

배포 지점을 연결 게이트웨이로 사용

Kaspersky Security Center에서 배포 지점은 모바일 프로토콜을 통해 관리 중인 기기 및 네트워크 에이전트를 통해 관리 중인 기기에 대한 푸시 서버로 작동될 수 있습니다. 예를 들어, KasperskyOS 기기를 중앙 관리 서버에 강제로 동기화하려면 푸시 서버를 활성화해야 합니다. 푸시 서버에는 푸시 서버가 활성화된 배포 지점과 동일한 수준의 관리 중인 기기가 있습니다. 동일한 관리 그룹에 여러 배포 지점이 할당된 경우 각 배포 지점에서 푸시 서버를 활성화할 수 있습니다. 이 경우 중앙 관리 서버는 배포 지점 간의 로드 균형을 조정합니다.

> 푸시 서버는 최대 50,000개의 동시 연결 로드를 지원합니다.

배포 지점을 푸시 서버로 사용하여 관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결을 유지할 수 있습니다. 로컬 작업 실행 및 중지, 관리 중인 애플리케이션에 대한 통계 수신 또는 터널 생성과 같은 일부 작업에는 지속적인 연결이 필요합니다. 배포 지점을 푸시 서버로 사용하는 경우 관리 중인 기기에서 **중앙 관리 서버와 계속 연결 유지** 옵션을 사용하거나 네트워크 에이전트의 UDP 포트로 패킷을 보냅니다.

배포 지점을 푸시 서버로 사용하려면 다음과 같이 하세요.

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 기기의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창이 열리면 **배포 지점** 섹션을 선택합니다.
4. 목록에서 필요한 배포 지점을 선택하고 **속성**을 누릅니다.
5. 배포 지점 속성 창이 열리면 **섹션** 패널의 **일반** 섹션에서 **이 배포 지점을 푸시 서버로 사용** 옵션을 선택합니다.
6. 푸시 서버 포트 번호, 즉 클라이언트 기기가 연결에 사용할 배포 지점의 포트를 지정합니다.
   기본적으로 포트 13295이 사용됩니다.
7. **확인** 버튼을 눌러 배포 지점 속성 창을 닫습니다.
8. 네트워크 에이전트 속성 창을 엽니다.
9. **연결성** 섹션에서 **네트워크** 하위 섹션으로 이동합니다.
10. **네트워크** 하위 섹션에서 **배포 지점을 사용하여 중앙 관리 서버에 강제 연결** 옵션을 선택합니다.
11. **OK** 버튼을 눌러 마법사를 닫습니다.

    배포 지점이 푸시 서버로 작동하기 시작합니다. 이제 클라이언트 기기에 푸시 알림을 보낼 수 있습니다.

KasperskyOS가 설치된 기기를 관리하거나 관리할 계획이라면 배포 지점을 푸시 서버로 사용해야 합니다. 클라이언트 기기에 푸시 알림을 보내려면 배포 지점을 푸시 서버로 사용할 수도 있습니다.

기타 정기 작업

이 섹션에서는 Kaspersky Security Center의 일상적인 작업에 대한 권장 사항을 제공합니다.

중앙 관리 서버 관리

이 섹션에서는 중앙 관리 서버를 처리하고 구성하는 방법에 대해 설명합니다.

중앙 관리 서버 계층 만들기 및 보조 중앙 관리 서버 추가

중앙 관리 서버를 보조 중앙 관리 서버로 추가하여 '기본/보조' 계층을 구축할 수 있습니다. 보조로 사용할 중앙 관리 서버가 관리 콘솔을 통해 연결할 수 있는지에 관계없이 보조 중앙 관리 서버를 추가할 수 있습니다.

두 개의 중앙 관리 서버를 하나의 계층으로 결합하는 경우 두 중앙 관리 서버 모두에서 13291 포트가 열려 있어야 합니다. 관리 콘솔에서 중앙 관리 서버로 연결을 수신하려면 13291 포트가 필요합니다.

중앙 관리 서버를 기본 중앙 관리 서버와 연동하여 보조로 연결

13000 포트를 통해 기본 중앙 관리 서버에 연결하여 중앙 관리 서버를 보조로 추가할 수 있습니다. 기본 중앙 관리 서버로 지정한 것과 보조 중앙 관리 서버 모두에서 TCP 13291 포트를 이용할 수 있도록 관리 콘솔이 설치된 기기가 필요합니다.

관리 콘솔을 통해 연결하여 사용할 수 있는 중앙 관리 서버를 보조 중앙 관리 서버로 추가하려면 다음을 수행하십시오:

1. 선정한 기본 중앙 관리 서버의 13000 포트가 보조 중앙 관리 서버에서 보내는 연결 데이터를 수신할 수 있는지 확인하십시오.
2. 이후 관리 콘솔을 사용하여 기본 중앙 관리 서버에 연결합니다.
3. 보조 중앙 관리 서버를 추가할 관리 그룹을 선택합니다.
4. 선택한 그룹의 **중앙 관리 서버** 노드의 작업 영역에서 **보조 중앙 관리 서버 추가** 링크를 누릅니다.

   보조 중앙 관리 서버 추가 마법사를 시작합니다.
5. 이 마법사의 첫 번째 단계(그룹에 추가되는 중앙 관리 서버의 주소 입력)에서 보조 중앙 관리 서버의 네트워크 이름을 입력합니다.
6. 마법사의 지침을 따릅니다.

'기본/보조' 계층이 구축됩니다. 보조 중앙 관리 서버가 기본 중앙 관리 서버로부터 연결 데이터를 수신하게 됩니다.

관리 콘솔이 설치된 기기가 없어 두 중앙 관리 서버 모두에서 TCP 13291 포트로 접근할 수 없더라도(보조 중앙 관리 서버가 원격 사무실에 있고 해당 사무실의 시스템 관리자가 보안상의 이유로 13291 포트에 대한 인터넷 접근을 열 수 없는 경우 등) 여전히 보조 중앙 관리 서버를 추가할 수 있습니다.

관리 콘솔을 통해 연결하여 사용할 수 없는 중앙 관리 서버를 보조 중앙 관리 서버로 추가하려면 다음을 수행하십시오:

1. 기본 중앙 관리 서버의 13000 포트가 보조 중앙 관리 서버에서 보내는 연결을 수신할 수 있는지 확인하십시오.
2. 기본 중앙 관리 서버의 인증서 파일을 플래시 드라이브와 같은 외부 기기에 복사해 보조 중앙 관리 서버가 있는 원격지 사무실의 시스템 관리자에게 보냅니다.

   중앙 관리 서버의 인증서 파일은 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer에 있습니다.
3. 보조 중앙 관리 서버의 인증서 파일을 플래시 드라이브와 같은 외부 기기에 복사합니다. 보조 중앙 관리 서버가 원격 사무실에 있는 경우 해당 사무실의 시스템 관리자에게 문의하여 인증서를 보내도록 요청하십시오.

   중앙 관리 서버의 인증서 파일은 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer에 있습니다.
4. 이후 관리 콘솔을 사용하여 기본 중앙 관리 서버에 연결합니다.
5. 보조 중앙 관리 서버를 추가할 관리 그룹을 선택합니다.
6. **중앙 관리 서버** 노드의 작업 영역에서 **보조 중앙 관리 서버 추가** 링크를 누릅니다.

   보조 중앙 관리 서버 추가 마법사를 시작합니다.
7. 마법사의 첫 번째 단계(주소 입력)에서 **보조 중앙 관리 서버 주소(선택 사항)** 필드를 비워 두십시오.

8. **보조 중앙 관리 서버 인증서 파일** 창에서 **찾기** 버튼을 누르고 저장한 보조 중앙 관리 서버의 인증서 파일을 선택합니다.

9. 마법사가 완료되면 관리 콘솔의 다른 인스턴스를 사용하여 지정한 보조 중앙 관리 서버에 연결합니다. 이 중앙 관리 서버가 원격 사무실에 있는 경우 해당 사무실의 시스템 관리자에게 문의하여 보조 중앙 관리 서버에 연결하고 추가 단계를 수행하도록 요청하십시오.

10. **중앙 관리 서버** 노드의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

11. 중앙 관리 서버 속성에서 **고급** 섹션으로 이동한 다음 **중앙 관리 서버 계층 구조** 하위 섹션으로 이동합니다.

12. **이 중앙 관리 서버는 계층 구조에서 보조임** 확인란을 선택합니다.

    입력 필드는 데이터 입력 및 편집에 사용할 수 있습니다.

13. **기본 중앙 관리 서버 주소** 필드에 향후 기본 중앙 관리 서버의 네트워크 이름을 입력합니다.

14. **찾기** 버튼을 클릭하여 제안된 기본 중앙 관리 서버의 인증서가 있는 이전에 저장한 파일을 선택합니다.

15. **확인**를 누릅니다.

'기본/보조' 계층이 구축됩니다. 관리 콘솔을 통해 보조 중앙 관리 서버에 연결할 수 있습니다. 보조 중앙 관리 서버가 기본 중앙 관리 서버로부터 연결 데이터를 수신하게 됩니다.

기본 중앙 관리 서버를 보조 중앙 관리 서버에 연결

새 중앙 관리 서버를 보조로 추가하여 기본 중앙 관리 서버가 13000 포트를 통해 보조 중앙 관리 서버에 연결할 수 있습니다. 이 방법은 DMZ에 보조 중앙 관리 서버를 구축하는 경우 사용하는 것이 좋습니다.

기본 중앙 관리 서버로 지정한 것과 보조 중앙 관리 서버 모두에서 TCP 13291 포트를 이용할 수 있도록 관리 콘솔이 설치된 기기가 필요합니다.

새 중앙 관리 서버를 보조로 추가하고 13000 포트를 통해 기본 중앙 관리 서버를 연결하려면 다음과 같이 진행합니다:

1. 보조 중앙 관리 서버의 13000 포트가 기본 중앙 관리 서버에서 보내는 연결 데이터를 수신할 수 있는지 확인하십시오.

2. 이후 관리 콘솔을 사용하여 기본 중앙 관리 서버에 연결합니다.

3. 보조 중앙 관리 서버를 추가할 관리 그룹을 선택합니다.

4. 관련된 관리 그룹의 **중앙 관리 서버** 노드의 작업 영역에서 **보조 중앙 관리 서버 추가** 링크를 누릅니다.

   보조 중앙 관리 서버 추가 마법사를 시작합니다.

5. 이 마법사의 첫 번째 단계(그룹에 추가되는 중앙 관리 서버의 주소 입력)에서 보조 중앙 관리 서버의 네트워크 이름을 입력하고 **DMZ에 있는 보조 중앙 관리 서버에 기본 중앙 관리 서버 연결** 확인란을 선택합니다.

6. 프록시 서버를 사용하여 보조 중앙 관리 서버에 연결한다면 마법사의 첫 번째 단계에서 **프록시 서버 사용** 확인란을 선택하고 연결 설정을 지정합니다.

7. 마법사의 지침을 따릅니다.

중앙 관리 서버의 계층이 생성됩니다. 보조 중앙 관리 서버가 기본 중앙 관리 서버로부터 연결 데이터를 수신하게 됩니다.

중앙 관리 서버에 연결 및 중앙 관리 서버 간 전환

Kaspersky Security Center를 시작하면 해당 애플리케이션에서 중앙 관리 서버에 연결을 시도합니다. 네트워크에 여러 개의 중앙 관리 서버가 있는 경우 애플리케이션은 이전 Kaspersky Security Center 세션 중에 연결했던 중앙 관리 서버를 요청합니다.

설치 후 처음 애플리케이션을 시작하는 경우에는 Kaspersky Security Center 설치 중에 지정된 중앙 관리 서버에 연결을 시도합니다.

중앙 관리 서버와의 연결이 설정되면 콘솔 트리에 해당 서버의 폴더 트리가 표시됩니다.

콘솔 트리에 여러 개의 중앙 관리 서버가 추가되어 있는 경우에는 서버 간에 전환을 할 수 있습니다.

관리 콘솔은 각 중앙 관리 서버와의 작업에 필요합니다. 새 중앙 관리 서버에 처음으로 연결하기 전에 관리 콘솔에서의 연결을 수신하기 위한 13291 포트가 열려 있으며 중앙 관리 서버와 다른 Kaspersky Security Center 구성 요소 간의 통신에 필요한 다른 모든 포트도 열려 있는지 확인하시기 바랍니다.

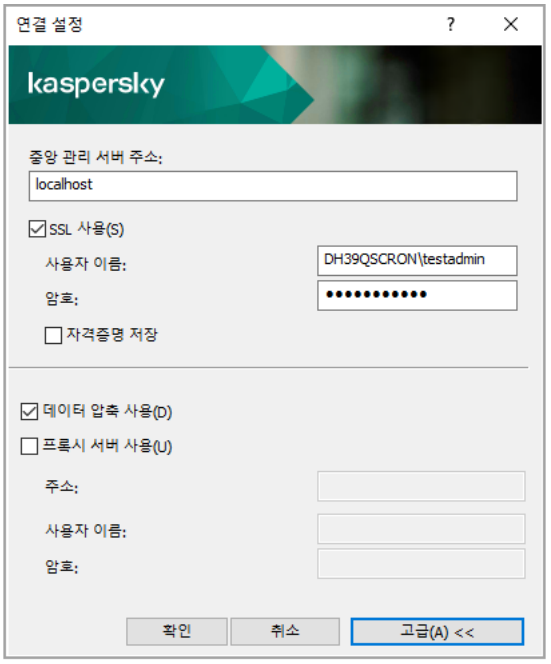
다른 중앙 관리 서버로 전환하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 컨텍스트 메뉴에서 **중앙 관리 서버에 연결**을 선택합니다.
3. **연결 설정** 창이 열리면 **중앙 관리 서버 주소** 필드에서 연결할 중앙 관리 서버의 이름을 지정합니다. Windows 네트워크의 IP 주소나 기기 이름을 중앙 관리 서버의 이름으로 지정할 수 있습니다. **고급** 버튼을 눌러 중앙 관리 서버와의 연결을 구성할 수 있습니다(아래 그림 참조).

   기본 포트 이외의 다른 포트를 통해 중앙 관리 서버에 연결하려면 **중앙 관리 서버 주소** 필드에 <중앙 관리 서버 이름>:<포트> 형식으로 값을 입력합니다.

   가상 중앙 관리 서버에 연결하려면 **중앙 관리 서버 주소** 필드에 <중앙 관리 서버 주소>/<가상 서버 이름> 형식으로 값을 입력합니다.

읽기 권한이 없는 사용자는 중앙 관리 서버에 대한 접근이 거부됩니다.



중앙 관리 서버에 연결하기

4. **확인**을 눌러 서버 간 전환을 완료합니다.

   중앙 관리 서버가 연결되면 콘솔 트리에서 해당 노드의 폴더 트리가 업데이트됩니다.

중앙 관리 서버와 해당 개체에 대한 접근 권한

Kaspersky Security Center를 설치하는 동안 **KLAdmins** 및 **KLOperators** 그룹이 자동으로 만들어집니다. 이 그룹에는 중앙 관리 서버에 연결하고 중앙 관리 서버 개체를 사용할 수 있는 권한이 주어집니다.

Kaspersky Security Center 설치에 사용된 계정 유형에 따라 다음과 같이 **KLAdmins** 및 **KLOperators** 그룹이 만들어집니다:

- 애플리케이션이 도메인에 포함된 사용자 계정으로 설치된 경우, 중앙 관리 서버를 포함하는 도메인과 중앙 관리 서버에 그룹이 만들어집니다.
- 애플리케이션이 시스템 계정으로 설치된 경우, 중앙 관리 서버에만 그룹이 만들어집니다.

운영 체제의 표준 관리 도구를 사용하여 **KLAdmins** 및 **KLOperators** 그룹을 확인하고 **KLAdmins** 및 **KLOperators** 그룹에 속한 사용자의 접근 권한을 수정할 수 있습니다.

KLAdmins 그룹에는 모든 접근 권한이 부여되고 **KLOperators** 그룹에는 읽기 및 실행 권한만 주어집니다. **KLAdmins** 그룹에 부여된 권한은 잠겨 있습니다.

KLAdmins 그룹에 속한 사용자를 *Kaspersky Security Center 관리자*라고 하고 **KLOperators** 그룹의 사용자를 *Kaspersky Security Center 운영자*라고 합니다.

Kaspersky Security Center 관리자 권한은 **KLAdmins** 그룹에 포함된 사용자 외에 중앙 관리 서버가 설치된 기기의 로컬 관리자에게도 제공됩니다.

Kaspersky Security Center 관리자 권한이 있는 사용자 목록에서 로컬 관리자를 제외할 수 있습니다.

Kaspersky Security Center 관리자가 시작한 모든 작업은 중앙 관리 서버 계정의 권한을 사용하여 수행됩니다.

네트워크의 각 중앙 관리 서버에 대해 개별적인 **KLAdmins** 그룹을 만들 수 있고, 이 그룹에는 이 중앙 관리 서버에 대한 필요한 권한만 주어집니다.

동일한 도메인에 속한 여러 기기가 서로 다른 중앙 관리 서버의 관리 그룹에 포함된 경우, 도메인 관리자가 모든 그룹에 대한 Kaspersky Security Center 관리자가 됩니다. **KLAdmins** 그룹은 이러한 관리 그룹에 대해 동일하며, 첫 중앙 관리 서버를 설치하는 과정에서 만들어집니다. Kaspersky Security Center 관리자가 시작한 모든 작업은 해당 작업이 시작된 중앙 관리 서버의 접근 권한을 사용하여 수행됩니다.

애플리케이션이 설치되면 Kaspersky Security Center 관리자는 다음을 수행할 수 있습니다:

- **KLOperators** 그룹에 부여된 권한 수정.
- Kaspersky Security Center의 기능에 접근할 수 있는 권한을 다른 보안 그룹 및 관리자의 워크스테이션에 등록된 개별 사용자에게 부여.
- 각 관리 그룹에 사용자 접근 권한 할당.

Kaspersky Security Center 관리자는 선택한 개체의 속성 창에 있는 **보안** 섹션에서 각 관리 그룹 또는 중앙 관리 서버의 다른 개체에 접근 권한을 할당할 수 있습니다.

중앙 관리 서버 작업의 이벤트 기록을 사용하여 사용자 활동을 추적할 수 있습니다. 이벤트 기록은 **중앙 관리 서버** 노드의 **이벤트** 탭에 나타납니다. 이러한 이벤트에는 심각도 **정보 이벤트**가 포함되어 있으며 이벤트 유형은 "**감사**"로 시작합니다.

인터넷을 통한 중앙 관리 서버 연결 조건

중앙 관리 서버가 회사 네트워크 외부에 위치하는 원격 서버인 경우 클라이언트 기기가 인터넷을 통해 중앙 관리 서버에 연결할 수 있습니다.

인터넷을 통해 기기를 중앙 관리 서버에 연결하려면 다음 조건을 충족해야 합니다:

- 원격 중앙 관리 서버는 외부 IP 주소를 가지고 있어야 하며 TCP 13000 포트가 수신되도록 열려 있어야 합니다(네트워크 에이전트 연결 용도). UDP 13000 포트도 열어 놓기를 권장합니다(기기 종료 알림 수신 용도).
- 네트워크 에이전트를 먼저 기기에 설치해야 합니다.
- 기기에 네트워크 에이전트를 설치할 때 원격 중앙 관리 서버의 외부 IP 주소를 지정해야 합니다. 설치 패키지를 사용하여 설치하는 경우 이 설치 패키지에 대한 속성의 **설정** 섹션에서 외부 IP 주소를 수동으로 지정합니다.
- 원격 중앙 관리 서버를 사용하여 기기의 애플리케이션 및 작업을 관리하려면 **일반** 섹션에 있는 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택해야 합니다. 확인란을 선택한 후 중앙 관리 서버가 원격 기기와 동기화될 때까지 기다립니다. 중앙 관리 서버와 지속적인 연결을 유지하는 클라이언트 기기의 수는 300대를 초과할 수 없습니다.

원격 중앙 관리 서버를 통해 시작되는 작업의 성능을 향상시키기 위해 기기에서 15000 포트를 열 수 있습니다. 이 경우, 작업을 실행하기 위해 기기와의 동기화가 완료될 때까지 기다리지 않고 중앙 관리 서버에서 15000 포트를 통해 네트워크 에이전트에 특수 패킷을 전송합니다.

중앙 관리 서버에 대한 암호화된 연결

클라이언트 기기와 중앙 관리 서버 간 데이터 교환 및 관리 콘솔과 중앙 관리 서버의 연결은 TLS(Transport Layer Security) 프로토콜을 사용하여 수행할 수 있습니다. TLS 프로토콜은 상호 작용하는 두 당사자를 식별하고 전송되는 데이터를 암호화하여 전송 중 변경되지 않도록 보호합니다. TLS 프로토콜은 공용 키를 사용하여 상호 작용하는 당사자를 인증하고 데이터를 암호화합니다.

기기 연결 시 중앙 관리 서버 인증

클라이언트 기기를 중앙 관리 서버에 처음 연결할 때 기기의 네트워크 에이전트는 중앙 관리 서버 인증서 사본을 다운로드하여 로컬에 저장합니다.

> 네트워크 에이전트를 기기에 로컬로 설치하는 경우, 중앙 관리 서버 인증서를 수동으로 선택할 수 있습니다.

다운로드한 인증서 사본은 이후 연결 시 중앙 관리 서버의 권한을 확인하는 데 사용됩니다.

이후 세션에서 네트워크 에이전트는 기기를 중앙 관리 서버에 연결할 때마다 중앙 관리 서버 인증서를 요청하고 이를 로컬 사본과 비교합니다. 사본이 일치하지 않으면 기기가 중앙 관리 서버에 접근할 수 없습니다.

관리 콘솔 연결 시 중앙 관리 서버 인증

중앙 관리 서버에 처음 연결할 때 관리 콘솔은 중앙 관리 서버 인증서를 요청하고 이 인증서를 관리자 워크스테이션에 로컬로 저장합니다. 그러면 관리 콘솔이 이 중앙 관리 서버에 연결을 시도할 때마다 인증서 사본을 기반으로 중앙 관리 서버가 확인됩니다.

중앙 관리 서버 인증서가 관리자 워크스테이션에 저장된 사본과 일치하지 않으면 관리 콘솔에서 지정된 이름을 가진 중앙 관리 서버와의 연결을 확인하고 새 인증서를 다운로드하라는 메시지가 표시됩니다. 연결이 설정되면 관리 콘솔이 새 중앙 관리 서버 인증서 사본을 저장하고, 해당 사본이 이후 중앙 관리 서버를 확인하는 데 사용됩니다.

중앙 관리 서버에 연결할 IP 주소의 허용 목록 구성

기본적으로 사용자는 Kaspersky Security Center 14 웹 콘솔(이하 웹 콘솔)을 열 수 있거나 MMC 기반 관리 콘솔이 설치된 모든 기기에서 Kaspersky Security Center에 로그인할 수 있습니다. 그러나 사용자가 허용된 IP 주소를 가진 기기에서만 연결할 수 있도록 중앙 관리 서버를 구성할 수 있습니다. 이 경우 침입자가 Kaspersky Security Center 계정을 도용하더라도 침입자의 기기 IP 주소가 허용 목록에 없으므로 Kaspersky Security Center에 로그인할 수 없습니다.

사용자가 Kaspersky Security Center에 로그인하거나 Kaspersky Security Center OpenAPI를 통해 중앙 관리 서버와 상호 작용하는 애플리케이션을 실행하는 경우 IP 주소를 확인합니다. 이때 사용자의 기기가 중앙 관리 서버와 연결을 시도합니다. 기기의 IP 주소가 허용 목록에 없으면 접근 거부 오류가 발생하고 KLAUD_EV_SERVERCONNECT 이벤트가 중앙 관리 서버와의 연결이 설정되지 않았음을 알립니다.

IP 주소 허용 목록 요구 사항

IP 주소는 다음 애플리케이션이 중앙 관리 서버에 연결을 시도할 때만 확인됩니다.

- 웹 콘솔 서버

  한재 기기에서 웹 콘솔에 로그인하고 웹 콘솔 서버가 다른 기기에 설치된 경우 운영 체제의 표준 수단을 사용하여 웹 콘솔 서버가 설치된 기기에 방화벽을 구성할 수 있습니다. 누군가 웹 콘솔에 로그인을 시도하면 방화벽이 침입자의 방해를 방지할 수 있습니다.

- 관리 콘솔

- Klakaut 자동화 개체를 통해 중앙 관리 서버와 상호 작용하는 애플리케이션

- Kaspersky Anti Targeted Attack Platform 또는 Kaspersky Security for Virtualization과 같은 OpenAPI를 통해 중앙 관리 서버와 상호 작용하는 애플리케이션

따라서 위에 나열된 애플리케이션이 설치된 기기의 주소를 지정합니다.

IPv4 및 IPv6 주소를 설정할 수 있습니다. IP 주소 범위를 지정할 수 없습니다.

IP 주소의 허용 목록을 설정하는 방법

이전에 허용 목록을 설정하지 않은 경우 아래 지침을 따르십시오.

Kaspersky Security Center에 로그인하기 위한 IP 주소 허용 목록을 구성하려면 다음을 수행합니다.

1. 중앙 관리 서버 기기에서 관리자 권한이 있는 계정으로 Windows 명령 프롬프트를 실행합니다.
2. 현재 디렉터리를 Kaspersky Security Center 설치 폴더(일반적으로 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center)로 변경합니다.
3. 관리자 권한을 사용하여 다음 명령을 입력합니다.
   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s
   ```
   위에 나열된 요구 사항을 충족하는 IP 주소를 지정합니다. 여러 IP 주소는 세미콜론으로 구분해야 합니다.

   하나의 기기만 중앙 관리 서버에 연결하도록 허용하는 방법의 예:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
   ```

   여러 기기를 중앙 관리 서버에 연결하도록 허용하는 방법의 예:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
   ```
4. 중앙 관리 서버 서비스를 다시 시작합니다.

중앙 관리 서버의 Kaspersky 이벤트 로그에서 IP 주소의 허용 목록이 구성되었는지 확인할 수 있습니다.

IP 주소의 허용 목록을 변경하는 방법

처음 설정할 때와 마찬가지로 허용 목록을 변경할 수 있습니다. 이를 위해 동일한 다음 명령을 실행하고 새 허용 목록을 지정합니다.

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP
addresses>" -t s
```

허용 목록에서 일부 IP 주소를 삭제하려면 다시 작성하십시오. 예를 들어 허용 목록에는 192.0.2.0; 198.51.100.0; 203.0.113.0 등의 IP 주소가 포함됩니다. 198.51.100.0 IP 주소를 삭제하려고 합니다. 이를 위해 명령 프롬프트에서 다음 명령을 입력합니다.

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

중앙 관리 서버 서비스를 반드시 다시 시작해야 합니다.

구성된 IP 주소 허용 목록 재설정하는 방법

이미 구성된 IP 주소 허용 목록을 재설정하려면 다음을 수행합니다.

1. 관리자 권한을 사용하여 명령 프롬프트에서 다음 명령을 입력합니다.
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. 중앙 관리 서버 서비스를 다시 시작합니다.

그 후에는 더 이상 IP 주소를 확인하지 않습니다.

Klscflag 유틸리티를 사용하여 포트 13291 닫기

중앙 관리 서버의 포트 13291은 중앙 관리 콘솔에서 연결을 수신하는 데 사용됩니다. 이 포트는 기본적으로 열려 있습니다. MMC 기반 중앙 관리 콘솔이나 klakaut 유틸리티를 사용하지 않으려면 klscflag 유틸리티를 사용하여 이 포트를 닫을 수 있습니다. 이 유틸리티는 KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN 매개변수의 값을 변경합니다.

포트 13291을 닫으려면 다음을 수행합니다.

1. 관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.
2. 명령줄에서 다음 명령을 실행합니다.
   ```
   klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -
   svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```
3. Kaspersky Security Center 중앙 관리 서버 서비스를 다시 시작합니다.

   포트 13291이 닫혀 있습니다.

포트 13291이 성공적으로 닫혔는지 확인하려면 다음을 수행합니다.

명령줄에서 다음 명령을 실행합니다.

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -
ss "|ss_type = \"SS_SETTINGS\";"
```

이 명령은 다음 결과를 반환합니다.

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T) false
```

`false` 값은 포트가 닫혀 있음을 의미합니다. 그렇지 않으면 `true` 값이 표시됩니다.

중앙 관리 서버에서 연결 끊는 방법

중앙 관리 서버에서 연결을 끊으려면 다음과 같이 하십시오:

1. 콘솔 트리에서 연결을 끊으려는 중앙 관리 서버에 해당하는 노드를 선택합니다.
2. 노드의 마우스 오른쪽 메뉴에서 **중앙 관리 서버에서 연결 끊기**를 선택합니다.

콘솔 트리에 중앙 관리 서버 추가

콘솔 트리에 중앙 관리 서버를 추가하려면 다음과 같이 하십시오:

1. Kaspersky Security Center 메인 창의 콘솔 트리에서 **Kaspersky Security Center** 노드를 선택합니다.
2. 노드의 마우스 오른쪽 메뉴에서 **새로 만들기 → 중앙 관리 서버**를 선택합니다.

   콘솔 트리에 **중앙 관리 서버 - <기기 이름>(연결 안 됨)** 노드가 만들어지고, 여기서 네트워크에 설치된 중앙 관리 서버에 연결할 수 있습니다.

콘솔 트리에서 중앙 관리 서버 제거

콘솔 트리에서 중앙 관리 서버를 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 제거하려는 중앙 관리 서버에 해당하는 노드를 선택합니다.
2. 노드의 마우스 오른쪽 메뉴에서 **제거**를 선택합니다.

콘솔 트리에 가상 중앙 관리 서버 추가

콘솔 트리에 가상 중앙 관리 서버를 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 가상 중앙 관리 서버를 만들어야 하는 중앙 관리 서버 이름이 있는 노드를 선택합니다.
2. 중앙 관리 서버 노드에서 **중앙 관리 서버** 폴더를 선택합니다.
3. **중앙 관리 서버** 폴더의 작업 영역에서 **가상 중앙 관리 서버 추가** 링크를 누릅니다.
   그러면 새 가상 중앙 관리 서버 마법사가 시작됩니다.
4. **가상 중앙 관리 서버 이름** 창에서 만들 가상 중앙 관리 서버의 이름을 지정합니다.
   가상 중앙 관리 서버 이름은 255자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

5. **가상 중앙 관리 서버에 기기를 연결하기 위한 주소 입력** 창에서 기기 연결 주소를 지정합니다.

   가상 중앙 관리 서버의 연결 주소는 기기가 해당 서버에 연결하는 데 사용하는 네트워크 주소입니다. 연결 주소는 실제 중앙 관리 서버의 네트워크 주소와 가상 중앙 관리 서버의 이름이 슬래시로 구분된 형식입니다. 가상 중앙 관리 서버의 이름은 자동으로 대체됩니다. 지정한 주소는 가상 중앙 관리 서버에서 네트워크 에이전트 설치 패키지의 기본 주소로 사용됩니다.

6. **가상 중앙 관리 서버의 관리자 계정 생성** 창에서 가상 서버 관리자 역할을 할 사용자를 목록에서 할당하거나 **생성** 버튼을 눌러 새 관리자 계정을 추가합니다.

   계정은 여러 개 지정할 수 있습니다.

콘솔 트리에 **중앙 관리 서버 - <가상 중앙 관리 서버의 이름>** 노드가 만들어집니다.

중앙 관리 서버 서비스 계정 변경. klsrvswch 유틸리티

Kaspersky Security Center를 설치할 때 중앙 관리 서버 서비스 계정을 변경해야 하는 경우 중앙 관리 서버 계정을 변경하도록 설계된 klsrvswch라는 유틸리티를 사용할 수 있습니다.

Kaspersky Security Center를 설치할 때 유틸리티가 애플리케이션 설치 폴더에 자동으로 복사됩니다.

유틸리티는 기본적으로 무제한 실행할 수 있습니다.

중앙 관리 서버 설치에 사용된 관리자 권한이 있는 계정으로 중앙 관리 서버 기기에서 klsrvswch 유틸리티를 시작해야 합니다.

klsrvswch 유틸리티는 계정 유형을 변경할 수 있도록 돕습니다. 예, 사용자가 로컬 계정을 사용한다면 이를 도메인 계정이나 관리 서비스 계정(및 그 반대)으로 변경할 수 있습니다. klsrvswch 유틸리티를 사용하면 계정 유형을 그룹 관리 서비스 계정(gMSA)으로 변경할 수 없습니다.

Windows Vista 이상의 Windows 버전에서는 중앙 관리 서버에 LocalSystem 계정을 사용할 수 없습니다. 이러한 Windows 버전에서는 **LocalSystem 계정** 옵션이 비활성화됩니다.

중앙 관리 서버 서비스 계정을 도메인 계정으로 변경하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 설치 폴더에서 klsrvswch 유틸리티를 실행합니다. 기본 설치 경로: <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   그러면 중앙 관리 서버 서비스 계정을 수정할 수 있는 마법사도 실행됩니다. 마법사의 지침을 따릅니다.

2. **중앙 관리 서버 서비스 계정** 창에서 **LocalSystem 계정**을 선택합니다.

   마법사가 작업을 마친 후 중앙 관리 서버 계정이 변경됩니다. 중앙 관리 서버 서비스가 *LocalSystem 계정* 및 그 자격 증명을 사용하여 시작됩니다.

Kaspersky Security Center가 올바르게 동작하려면 중앙 관리 서버 데이터베이스가 호스팅되는 리소스에 대한 관리자 권한이 중앙 관리 서버 서비스를 시작하는 데 사용되는 계정에 있어야 합니다.

중앙 관리 서버 서비스 계정을 사용자 계정 또는 관리 서비스 계정으로 변경하려면 다음과 같이 하십시오:

1. Kaspersky Security Center의 설치 폴더에서 klsrvswch 유틸리티를 실행합니다. 기본 설치 경로: <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
   그러면 중앙 관리 서버 서비스 계정을 수정할 수 있는 마법사도 실행됩니다. 마법사의 지침을 따릅니다.
2. **중앙 관리 서버 서비스 계정** 창에서 **사용자 지정 계정**을 선택합니다.
3. **지금 찾기** 버튼을 누릅니다.
   사용자 선택 창이 열립니다.
4. **사용자 선택** 창에서 **개체 유형** 버튼을 누릅니다.
5. 개체 유형 목록에서 사용자 계정을 사용하려는 경우 **사용자**를, 관리 서비스 계정을 사용하려는 경우 **서비스 계정**을 선택하고 **확인**을 누릅니다.
6. 개체 이름 필드에 계정 이름을 모두 또는 일부분 입력하고 **이름 확인**을 누릅니다.
7. 일치하는 이름 목록에서 필요한 이름을 선택하고 **확인**을 누릅니다.
8. **서비스 계정**을 선택한 경우 **계정 암호** 창에서 **암호** 및 **암호 확인** 필드를 비워 둡니다. **사용자**를 선택한 경우에는 사용자의 새 암호를 입력하고 확인합니다.

중앙 관리 서버 서비스 계정이 사용자가 선택한 계정으로 변경됩니다.

Windows 도구를 사용하여 사용자 계정 인증을 미리 인정하는 모드에서 Microsoft SQL Server를 사용할 경우 데이터베이스에 대한 접근 권한이 부여되어야 합니다. 이 사용자 계정은 Kaspersky Security Center 데이터베이스의 소유자여야 합니다. 기본적으로 dbo 구성표가 사용됩니다.

DBMS 자격증명 변경

예를 들어 보안을 위해 자격증명 순환을 수행하기 위해 DBMS 자격증명을 변경해야 하는 경우가 있습니다.

klsrvswch.exe를 사용하여 Windows 환경에서 DBMS 자격증명을 변경하려면:

1. Kaspersky Security Center의 설치 폴더에 있는 klsrvswch 유틸리티를 실행합니다. 기본 설치 경로: <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   중앙 관리 서버 설치에 사용된 관리자 권한이 있는 계정으로 중앙 관리 서버 기기에서 klsrvswch 유틸리티를 시작해야 합니다.

2. **DBMS 접근 자격증명 변경** 단계에 도달할 때까지 마법사의 **다음** 버튼을 클릭합니다.
3. 마법사의 **DBMS 접근 자격증명 변경** 단계에서 다음을 수행하십시오.

Windows 인증을 사용하는 경우 마법사의 **DBMS 접근 자격증명 변경** 단계는 건너뜁니다.

- **새 자격증명 적용** 옵션을 선택합니다.
- **계정** 필드에 새 계정 이름을 지정합니다.
- **비밀번호** 필드에 계정의 새 비밀번호를 지정합니다.
- **비밀번호 확인** 필드에 새 비밀번호를 지정합니다.

DBMS에 있는 계정의 자격증명을 지정해야 합니다.

4. **다음** 버튼을 클릭합니다.

마법사가 완료되면 DBMS 자격 증명이 변경됩니다.

klsrvswch 유틸리티는 SQL 인증을 위한 계정 암호를 변경하는 경우에만 사용할 수 있습니다. 인증 방법 변경은 지원하지 않습니다. 인증 방법을 변경하려면 관리 서버를 다시 설치하고 원하는 설정을 지정합니다.

중앙 관리 서버 공유 폴더 변경

중앙 관리 서버 설치 중에 중앙 관리 서버 공유 폴더가 지정됩니다. 중앙 관리 서버 속성에서 공유 폴더 위치를 변경할 수 있습니다.

공유 폴더를 변경하려면:

1. 네트워크 공유 폴더를 만들고 **Everyone** 하위 그룹에 대한 모든 제어 권한을 허용하도록 공유 및 폴더 구조에 대한 권한을 구성합니다.
2. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **섹션** 창에서 **고급**과 **중앙 관리 서버 공유 폴더**를 차례로 선택합니다.
4. **중앙 관리 서버 공유 폴더** 섹션에서 **변경** 버튼을 클릭합니다.
5. 공유 폴더로 사용할 폴더를 선택합니다.
6. **확인** 버튼을 눌러 중앙 관리 서버 속성 창을 닫습니다.
7. 공유 폴더로 선택한 폴더에 **Everyone** 하위 그룹에 대한 읽기 권한을 할당합니다.

중앙 관리 서버 노드의 문제 해결

관리 콘솔 왼쪽 창의 콘솔 트리에는 중앙 관리 서버의 노드가 포함되어 있습니다. 콘솔 트리에 중앙 관리 서버를 필요한 수만큼 추가할 수 있습니다.

콘솔 트리의 중앙 관리 서버 노드 목록은 Microsoft Management Console을 통해 .msc 파일의 섀도 복사본으로 저장됩니다. 이 파일의 섀도 복사본은 관리 콘솔이 설치된 기기의 %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ 폴더에 있습니다. 이 파일에는 각 중앙 관리 서버 노드에 대한 다음 정보가 포함됩니다:

- 중앙 관리 서버 주소
- 포트 번호
- TLS 사용 여부

  이 파라미터는 중앙 관리 서버에 관리 콘솔을 연결하는 데 사용되는 포트 번호에 따라 달라집니다.
- 사용자 이름
- 중앙 관리 서버 인증서

문제 해결

관리 콘솔이 중앙 관리 서버에 연결할 때는 로컬에 저장된 인증서를 중앙 관리 서버 인증서와 비교합니다. 인증서가 일치하지 않으면 관리 콘솔에서 오류가 생성됩니다. 예를 들어 중앙 관리 서버 인증서를 교체하면 인증서 불일치가 발생할 수 있습니다. 이 경우 콘솔에서 중앙 관리 서버 노드를 다시 만듭니다.

중앙 관리 서버 노드를 다시 만들려면 다음과 같이 하십시오:

1. Kaspersky Security Center 관리 콘솔 창을 닫습니다.
2. %USERPROFILE%\AppData\Roaming\Microsoft\MMC\에서 Kaspersky Security Center 15.1 파일을 삭제합니다.
3. Kaspersky Security Center 관리 콘솔을 실행합니다.

   중앙 관리 서버에 연결하여 기존 인증서를 수락하라는 메시지가 표시됩니다.
4. 다음 중 하나를 수행합니다:
   - **예** 버튼을 눌러 기존 인증서를 수락합니다.
   - 인증서를 지정하려면 **아니오** 버튼을 누른 다음 중앙 관리 서버를 인증하는 데 사용할 인증서 파일을 찾습니다.

인증서 문제가 해결됩니다. 관리 콘솔을 사용하여 중앙 관리 서버에 연결합니다.

중앙 관리 서버의 설정 보기 및 수정

중앙 관리 서버의 속성 창에서 해당 서버의 설정을 조정할 수 있습니다.

속성: 중앙 관리 서버 창을 열려면,

콘솔 트리에서 중앙 관리 서버 노드의 마우스 오른쪽 메뉴에 있는 **속성**을 선택합니다.

중앙 관리 서버의 일반 조정

중앙 관리 서버 속성 창의 **일반**, **중앙 관리 서버 연결 설정**, **이벤트 저장소** 및 **보안** 섹션에서 중앙 관리 서버의 일반 설정을 조정할 수 있습니다.

관리 콘솔 인터페이스에서 디스플레이가 비활성화되어 있다면 **보안** 섹션이 중앙 관리 서버에 나타나지 않을 수 있습니다.

*관리 콘솔에서 **보안** 섹션을 표시하려면 다음과 같이 하십시오:*

1. 콘솔 트리에서 원하는 중앙 관리 서버를 선택합니다.
2. 메인 애플리케이션 창의 **보기** 메뉴에서 **인터페이스 구성**를 선택합니다.
3. **인터페이스 구성** 창이 열리면, **보안 설정 섹션 표시** 확인란을 선택하고 **확인**을 누르십시오.
4. 애플리케이션 메시지 창에서 **확인**를 누릅니다.

   중앙 관리 서버 속성 창에 **보안** 섹션이 표시됩니다.

관리 콘솔 인터페이스 설정

관리 콘솔의 인터페이스 설정을 조정하여 다음 기능과 관련된 사용자 인터페이스 컨트롤을 표시하거나 숨길 수 있습니다:

- 취약점 및 패치 관리
- 데이터 암호화 및 보호
- 엔드포인트 제어 설정
- 모바일 기기 매니지먼트
- 보조 중앙 관리 서버
- 보안 설정 섹션

관리 콘솔 인터페이스 설정을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 원하는 중앙 관리 서버를 선택합니다.
2. 메인 애플리케이션 창의 **보기** 메뉴에서 **인터페이스 구성**을 선택합니다.
3. **인터페이스 구성** 창이 열리면 표시하고 싶은 기능 옆에 있는 확인란을 선택하고 **확인**를 누릅니다.
4. 애플리케이션 메시지 창에서 **확인**를 누릅니다.

   선택한 기능이 관리 콘솔 인터페이스에 표시됩니다.

중앙 관리 서버에서의 이벤트 처리 및 저장소

애플리케이션과 관리 중인 기기에서 운영 중 발생하는 이벤트 정보는 중앙 관리 서버 데이터베이스에 저장됩니다. 어떤 유형 및 심각도(*심각 이벤트*, *기능 실패*, *경고* 또는 *정보*)에 따라 각 이벤트가 기록됩니다. 이벤트가 일어나는 조건에 따라, 애플리케이션은 같은 유형의 이벤트에 다른 심각도를 할당할 수 있습니다.

중앙 관리 서버 속성 창의 **이벤트 구성** 섹션에서 이벤트에 할당된 유형과 심각도를 볼 수 있습니다. **이벤트 구성** 섹션에서 중앙 관리 서버에서의 이벤트 작업을 구성할 수도 있습니다:

- 중앙 관리 서버 및 기기와 중앙 관리 서버의 운영 체제에 있는 이벤트 로그에 이벤트 등록.
- 이벤트를 관리자에게 알리는 방법 (예, SMS 또는 이메일 메시지).

중앙 관리 서버 속성 창의 **이벤트 저장소** 섹션에서 이벤트 레코드 개수 및 레코드 저장 기간을 제한해 중앙 관리 서버 데이터베이스의 이벤트 저장 설정을 편집할 수 있습니다. 최대 이벤트 수를 지정하면 애플리케이션은 지정된 이벤트 수에 필요한 스토리지 공간의 대략적인 양을 계산합니다. 이 대략적인 계산 결과 값을 사용하여 디스크의 사용 가능한 공간이 데이터베이스 초과 상황을 방지하기에 충분한지 여부를 평가할 수 있습니다. 중앙 관리 서버 데이터베이스의 기본 용량은 400,000개 이벤트입니다. 데이터베이스의 최대 권장 용량은 4,500만개 이벤트입니다.

애플리케이션은 10분마다 데이터베이스를 확인합니다. 이벤트 수가 지정된 최댓값이나 10,000에 도달하면 애플리케이션은 지정된 최대 이벤트 수만 남도록 가장 오래된 이벤트를 삭제합니다.

중앙 관리 서버가 오래된 이벤트를 삭제할 때에는 새 이벤트를 데이터베이스에 저장할 수 없습니다. 이 기간 동안에는 거부된 이벤트 관련 정보가 Kaspersky 이벤트 로그에 기록됩니다. 새 이벤트는 대기열에 보관되었다가 삭제 작업이 완료되고 나면 데이터베이스에 저장됩니다.

모든 작업의 설정을 변경하여 작업 진행과 관련된 이벤트를 저장하거나 작업 실행 결과만 저장할 수 있습니다. 이렇게 하면 데이터베이스의 이벤트 수를 줄이고, 데이터베이스의 이벤트 테이블에 대한 분석과 관련된 시나리오의 실행 속도를 높이며 다량의 이벤트가 심각 이벤트를 덮어쓰는 위험을 줄일 수 있습니다.

중앙 관리 서버로의 연결 로그 보기

중앙 관리 서버가 작동하는 동안 중앙 관리 서버로의 연결 및 연결 시도 내역을 로그 파일에 저장할 수 있습니다. 이 파일의 정보를 통해 네트워크 인프라에서의 연결뿐 아니라 중앙 관리 서버에 무단으로 접근하려는 시도도 추적할 수 있습니다.

중앙 관리 서버와의 연결 이벤트를 기록하려면 다음 단계를 따릅니다.

1. 콘솔 트리에서 연결 이벤트를 기록하고 싶은 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 속성 창이 열리면 **중앙 관리 서버 연결 설정** 섹션에서 **연결 포트** 하위 섹션을 선택합니다.
4. **중앙 관리 서버 연결 이벤트 기록** 옵션을 활성화합니다.
5. **확인** 버튼을 눌러 중앙 관리 서버 속성 창을 닫습니다.

중앙 관리 서버와의 인바운드 연결, 인증 결과 및 SSL 오류와 관련된 모든 이후 이벤트가 %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog 파일에 저장됩니다.

바이러스 급증 제어

Kaspersky Security Center에서는 바이러스 급증의 신종 보안위협에 신속하게 대응할 수 있습니다. 바이러스 급증 위험은 기기의 바이러스 감시를 통해 평가됩니다.

바이러스 급증 위협에 대한 평가 규칙 및 발생 시 취할 조치를 구성할 수 있습니다. 이렇게 하려면 중앙 관리 서버의 속성 창에서 **바이러스 발생** 섹션을 사용합니다.

사용자는 중앙 관리 서버 속성 창의 **이벤트 구성** 섹션에 있는 *바이러스 급증* 이벤트 속성 창에서 *바이러스 급증* 이벤트에 대한 알림 절차를 지정할 수 있습니다.

바이러스 급증 이벤트는 보안 제품 작업에서 *악성 개체 탐지* 이벤트가 탐지될 때 생성됩니다. 따라서 바이러스 급증을 인식하기 위해 모든 *악성 개체 탐지* 이벤트에 관한 정보를 중앙 관리 서버에 저장해야 합니다.

보안 제품 정책에서 *악성 개체 탐지* 이벤트에 관한 정보를 저장하기 위한 설정을 지정할 수 있습니다.

악성 개체 탐지 이벤트를 계산할 때는 기본 중앙 관리 서버의 기기로부터 받은 정보만 고려됩니다. 즉, 보조 중앙 관리 서버에서 받은 정보는 고려되지 않습니다. *바이러스 급증* 이벤트 설정은 각 보조 서버에 대해 개별적으로 구성됩니다.

트래픽 제한

네트워크 내의 트래픽 양을 줄이기 위해 이 애플리케이션에서는 지정된 IP 범위 및 IP 서브넷에서 중앙 관리 서버로 데이터가 전송되는 속도를 제한하는 옵션을 제공합니다.

중앙 관리 서버 속성 창의 **트래픽** 섹션에서 트래픽 제한 규칙을 만들고 구성할 수 있습니다.

트래픽 제한 규칙을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 트래픽 제한 규칙을 만들기 원하는 중앙 관리 서버 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창에서 **트래픽** 섹션을 선택합니다.
4. **추가** 버튼을 누릅니다.
5. **새 규칙** 창에서 다음 설정을 지정합니다:

   트래픽을 제한하는 IP 범위 섹션에서 데이터 전송 속도를 제한할 범위 또는 서브넷을 정의하는 데 사용할 방법을 선택하고 선택한 방법의 설정 값을 입력합니다. 다음 방법 중 하나를 선택합니다:

   - **IP 주소 및 네트워크 마스크로 범위 지정**

     트래픽이 서브넷 설정에 따라 제한됩니다. 서브넷 주소와 서브넷 마스크를 지정하여 트래픽을 제한할 범위를 결정합니다.

     찾기를 눌러 글로벌 서브넷 목록에서 서브넷을 추가할 수도 있습니다.

- **시작 및 종료 IP 주소로 범위 지정**

  트래픽이 IP 주소의 범위에 따라 제한됩니다. **시작** 및 **종료** 입력 필드에서 IP 주소 범위를 지정합니다.
  이 옵션은 기본적으로 선택되어 있습니다.

트래픽 제한 섹션에서 다음과 같은 데이터 전송 속도 제한을 조정할 수 있습니다:

- **시간 간격**

  트래픽 제한이 강제 적용되는 기간입니다. 입력 필드에서 시간 간격의 경계를 지정할 수 있습니다.

- **제한 트래픽(KB/s)**

  중앙 관리 서버의 수신/발신 데이터에 대한 최대 전송 속도입니다. 트래픽 제한은 **제한 시간** 필드에 지정된 기간 내에서만 적용됩니다.

- **위 제한 시간 이외의 트래픽 제한(KB/s)**

  제한 시간 필드에 지정된 시간뿐 아니라 다른 시간에도 트래픽이 제한됩니다.
  기본적으로 이 확인란은 선택되어 있지 않습니다. 이 필드의 값은 **제한 트래픽(KB/s)** 필드의 값과 다를 수도 있습니다.

기본적으로 트래픽 제한 규칙은 파일 전송에 영향을 줍니다. 중앙 관리 서버와 네트워크 에이전트 또는 기본 중앙 관리 서버와 보조 중앙 관리 서버 간의 동기화에 의해 생성되는 트래픽에는 이러한 규칙이 적용되지 않습니다.

웹 서버 구성

웹 서버는 독립 실행형 설치 패키지, iOS MDM 프로필 및 공유 폴더의 파일을 게시하도록 설계되었습니다.

중앙 관리 서버의 속성 창의 **웹 서버** 섹션에서 웹 서버와 중앙 관리 서버의 연결 설정을 정의하고, 웹 서버 인증서를 설정할 수 있습니다.

내부 사용자 작업

내부 사용자 계정은 가상 중앙 관리 서버 작업에 사용됩니다. Kaspersky Security Center는 애플리케이션의 내부 사용자에게 실제 사용자의 권한을 부여합니다.

내부 사용자의 계정이 생성되어 Kaspersky Security Center 내에서만 사용됩니다. 내부 사용자에 대한 어떤 데이터도 운영 체제로 전송되지 않습니다. Kaspersky Security Center에서 내부 사용자를 인증합니다.

콘솔 트리의 **사용자 계정** 폴더에서 내부 사용자 계정을 구성할 수 있습니다.

중앙 관리 서버 설정 백업 및 복원

중앙 관리 서버와 해당 데이터베이스의 설정 백업은 백업 작업 및 klbackup 유틸리티를 통해 수행됩니다. 백업 복사본에는 인증서, 관리 중인 기기의 드라이브 암호화용 마스터 키, 다양한 라이센스용 키, 모든 컨텐츠/작업/정책 등이 들어 있는 관리 그룹의 구조와 같은 중앙 관리 서버와 관련된 모든 기본 설정 및 개체가 포함됩니다. 백업 복사본이 이 있으면 중앙 관리 서버의 동작을 최대한 빨리 복구할 수 있습니다(복구에는 약 10분~2시간이 소요됨). 백업 복사본이 이 있으면 중앙 관리 서버의 동작을 최대한 빨리 복구할 수 있습니다(복구에는 십여 분에서 몇 시간 소요).

백업 복사본을 사용할 수 없으면 오류 발생 시 인증서와 모든 중앙 관리 서버 설정이 손실되어 복구할 수 없게 될 수 있습니다. 그러면 Kaspersky Security Center를 처음부터 다시 구성해야 하며, 조직 네트워크에서 네트워크 에이전트 초기 배포를 다시 수행해야 합니다. 관리 중인 기기의 드라이브 암호화를 위한 모든 기본 키도 손실되므로 Kaspersky Endpoint Security가 설치된 기기에서 암호화된 데이터가 손실되어 복구할 수 없게 될 위험이 있습니다. 따라서, 표준 백업 작업을 사용하여 중앙 관리 서버를 정기적으로 백업해야 합니다.

빠른 시작 마법사에서는 중앙 관리 서버 설정에 대한 백업 작업을 만들어 매일 오전 4시에 실행되도록 설정합니다. 백업 복사본은 기본적으로 %ALLUSERSPROFILE%\Application Data\KasperskySC 폴더에 저장됩니다.

다른 기기에 설치된 Microsoft SQL Server 인스턴스를 DBMS로 사용하는 경우에는 UNC 경로를 지정하여 백업 작업을 수정해야 합니다. UNC 경로는 중앙 관리 서버 서비스와 SQL Server 서비스 둘 다에서 백업 복사본을 저장할 폴더로 작성 가능합니다. 이 요구 사항은 Microsoft SQL Server DBMS에 포함된 백업의 특수 기능과 연관된 것입니다.

Microsoft SQL Server의 로컬 인스턴스를 DBMS로 사용하는 경우에는 중앙 관리 서버와 함께 백업 복사본이 손상되지 않도록 보호하기 위해 전용 매체에 백업 복사본을 저장하는 방식도 권장합니다.

백업 복사본에는 중요한 데이터가 포함되므로 백업 작업 및 klbackup 유틸리티는 백업 복사본의 암호 보호 기능을 제공합니다. 백업 작업은 기본적으로 암호가 비어 있는 상태로 작성됩니다. 백업 작업의 속성에서 암호를 설정해야 합니다. 이 요구 사항을 무시하면 중앙 관리 서버 인증서의 모든 키, 라이센스용 키, 그리고 관리 중인 기기의 드라이브 암호화용 기본 키가 암호화되지 않은 상태로 유지되는 상황이 발생합니다.

정기적인 백업 외에도 중요한 변경(중앙 관리 서버 업그레이드 및 패치 설치 포함)을 수행하기 전에는 항상 백업 복사본을 만들어야 합니다.

Microsoft SQL Server를 DBMS로 사용하면 백업 복사본의 크기를 최소화할 수 있습니다. 이렇게 하려면 SQL Server 설정에서 **백업 압축** 옵션을 활성화합니다.

가장 최근에 설치되었으며 버전이 백업 복사본을 만든 인스턴스 이상인 작동 가능한 중앙 관리 서버 인스턴스에서 klbackup 유틸리티를 사용하여 백업 복사본 복원을 수행합니다.

복원을 수행할 중앙 관리 서버 인스턴스는 버전이 같거나 이후이고 유형이 같은 DBMS(같은 SQL Server 또는 MySQL 등)를 사용해야 합니다. 중앙 관리 서버의 버전은 원래 버전과 같을 수도 있고(패치가 원래 중앙 관리 서버와 동일하거나 그 이상임) 더 최신 버전일 수도 있습니다.

이 섹션에서는 중앙 관리 서버의 설정과 개체를 복원하기 위한 표준 시나리오에 대해 설명합니다.

파일 시스템 스냅샷을 사용하여 백업 시간 단축

Kaspersky Security Center 15.1에서는 백업하는 동안 중앙 관리 서버의 유휴 시간이 이전 버전에 비해 줄었습니다. 게다가 **데이터 백업에 파일 시스템 스냅샷 사용** 기능이 해당 작업 설정에 추가되었습니다. 이 기능은 klbackup 유틸리티를 사용할 때 추가적인 유휴 시간 단축을 가능하게 합니다. 즉, 백업 중에 디스크의 쉐도우 복사본을 생성하고(몇 초 소요) 동시에 데이터베이스를 복사합니다. klbackup 유틸리티를 통해 디스크의 쉐도우 복사본과 데이터베이스 복사본을 생성할 때 중앙 관리 서버 연결을 다시 시작할 수 있습니다.

다음 두 조건이 충족되는 경우에만 파일 시스템 스냅샷 기능을 사용할 수 있습니다:

- 중앙 관리 서버 공유 폴더와 %ALLUSERSPROFILE%\KasperskyLab 폴더가 같은 논리 디스크에 있으며 해당 중앙 관리 서버와 관련하여 로컬이어야 합니다.
- %ALLUSERSPROFILE%\KasperskyLab 폴더에는 수동으로 생성된 심볼 링크가 없어야 합니다.

이러한 조건 중 하나라도 충족되지 않으면 이 기능을 사용하지 마십시오. 그렇지 않으면 애플리케이션은 파일 시스템 스냅샷 생성 시도 시 오류 메시지를 반환합니다.

이 기능을 사용하려면 %ALLUSERSPROFILE% 폴더가 저장된 논리 디스크의 스냅샷을 만들 수 있는 사용 권한이 부여된 계정이 있어야 합니다. 중앙 관리 서버 서비스 계정에 이러한 사용 권한이 없다는 것을 알려 드립니다.

파일 시스템 스냅샷 기능을 사용하여 백업 시간을 단축하려면 다음과 같이 진행하시기 바랍니다:

1. **작업** 섹션에서 백업 작업을 선택합니다.
2. 책 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 열리는 작업 속성 창에서 **설정** 섹션을 선택합니다.
4. **데이터 백업에 파일 시스템 스냅샷 사용** 확인란을 선택합니다.
5. **사용자 이름** 및 **암호** 필드에 %ALLUSERSPROFILE% 폴더가 저장된 논리 디스크의 스냅샷을 만들 수 있는 권한이 있는 계정의 이름과 암호를 입력합니다.
6. **적용**을 누릅니다.

이제 백업 작업을 시작할 때마다 klbackup 유틸리티가 파일 시스템 스냅샷을 생성하여 작업 실행 동안 중앙 관리 서버의 유휴 시간을 단축됩니다.

중앙 관리 서버가 설치된 기기가 작동하지 않음

중앙 관리 서버가 설치된 기기가 오류로 인해 작동하지 않으면 다음 작업을 수행하는 것이 좋습니다:

- 새 중앙 관리 서버에 같은 주소를 할당해야 합니다. 네트워크 에이전트를 배포할 때 설정된 항목에 따라 NetBIOS 이름, FQDN 또는 고정 IP를 할당해야 합니다.
- 유형이 원래 DBMS와 같고 버전이 원래 DBMS 이상인 DBMS를 사용하여 중앙 관리 서버를 설치합니다. 패치가 원래 서버와 같거나 그 이상인 동일 버전의 서버 또는 최신 버전의 서버를 설치할 수 있습니다. 설치 후에는 마법사를 통해 초기 설정을 수행하지 않습니다.
- **시작** 메뉴에서 klbackup 유틸리티를 실행하여 복원을 수행합니다.

데이터베이스 또는 중앙 관리 서버의 설정이 손상됨

전원 서지 등이 발생한 이후 설정이나 데이터베이스가 손상되어 중앙 관리 서버가 작동하지 않는 경우에는 다음 복원 시나리오를 사용하는 것이 좋습니다:

1. 손상된 기기에서 파일 시스템을 검사합니다.
2. 작동하지 않는 중앙 관리 서버 버전을 제거합니다.
3. 유형이 원래 DBMS와 같고 버전이 원래 DBMS 이상인 DBMS를 사용하여 중앙 관리 서버를 다시 설치합니다. 패치가 원래 서버와 같거나 그 이상인 동일 버전의 서버 또는 최신 버전의 서버를 설치할 수 있습니다. 설치 후에는 마법사를 통해 초기 설정을 수행하지 않습니다.
4. **시작** 메뉴에서 klbackup 유틸리티를 실행하여 복원을 수행합니다.

klbackup 유틸리티를 사용하는 방식 이외의 방식으로 중앙 관리 서버를 복원하는 행위는 금지됩니다.

타사 소프트웨어를 통해 중앙 관리 서버 복원을 시도하면 배포된 애플리케이션 Kaspersky Security Center의 노드에서 데이터 동기화가 해제되며, 그러면 애플리케이션이 잘못된 방식으로 작동하게 됩니다.

중앙 관리 서버 데이터의 백업 복사 및 복원

데이터 백업을 사용하면 한 기기에서 다른 기기로 데이터 손실 없이 중앙 관리 서버를 이동할 수 있습니다. 백업을 통해, 중앙 관리 서버 데이터베이스를 다른 기기로 옮기거나 최신 버전의 Kaspersky Security Center로 업그레이드할 때 데이터를 복원할 수 있습니다. 또한 데이터 백업을 사용하여 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux의 관리 하로 중앙 관리 서버 데이터를 옮길 수 있습니다(Kaspersky Security Center Linux에서 Kaspersky Security Center Windows로 데이터를 옮기는 것은 지원하지 않습니다).

설치된 관리 플러그인은 백업되지 않습니다. 백업 복사본에서 중앙 관리 서버 데이터를 복원한 후, 관리 중인 애플리케이션용 플러그인을 다운로드하여 다시 설치해야 합니다.

중앙 관리 서버 데이터를 백업하기 전에 가상 중앙 관리 서버가 관리 그룹에 추가되어 있는지 확인합니다. 가상 중앙 관리 서버가 추가되었다면 백업 전에 이 가상 중앙 관리 서버에 관리자가 할당되어 있는지 확인합니다. 백업 후에는 가상 중앙 관리 서버에 관리자 액세스 권한을 부여할 수 없습니다. 관리자 계정 자격 증명을 상실하면 가상 관리자 서버에 새 관리자를 할당할 수 없습니다.

Kaspersky Security Center 장애 조치 클러스터를 백업하거나 복원하려면 유지 관리 작업을 위해 전체 클러스터를 중지한 다음, 백업 또는 복원이 완료되면 다시 시작해야 합니다.

다음 방법 중 하나를 사용하여 중앙 관리 서버 데이터의 백업 복사본을 만들 수 있습니다:

- 관리 콘솔을 사용하여 데이터 백업 작업을 만들고 실행합니다.
- 중앙 관리 서버가 설치된 기기에서 klbackup 유틸리티를 실행합니다. 이 유틸리티는 Kaspersky Security Center 배포 키트에 포함되어 있습니다. 중앙 관리 서버를 설치하면 이 유틸리티가 애플리케이션 설치 시 지정한 대상 폴더의 루트에 저장됩니다.

다음 데이터가 중앙 관리 서버의 백업 복사본에 저장됩니다.

- 중앙 관리 서버의 데이터베이스(중앙 관리 서버에 저장된 정책, 작업, 애플리케이션 설정, 이벤트).
- 관리 그룹 및 클라이언트 기기 구조에 관한 구성 세부사항.
- 원격 설치를 위한 애플리케이션의 배포 패키지 저장소.
- 중앙 관리 서버 인증서.
- *업데이트* 폴더의 내용.
  기본 폴더 경로는 C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\입니다

klbackup 유틸리티를 사용해야만 중앙 관리 서버 데이터를 복원할 수 있습니다. 가장 최근에 설치되었으며 버전이 백업 복사본을 만든 인스턴스 이상인 작동 가능한 중앙 관리 서버 인스턴스에서 복원을 수행해야 합니다.

중앙 관리 서버 데이터 백업 작업

중앙 관리 서버 데이터 백업 작업 생성

백업 작업은 중앙 관리 서버 작업이며, 빠른 시작 마법사로 생성합니다. 빠른 시작 마법사에서 만든 백업 작업이 삭제되었다면 수동으로 만들 수 있습니다.

중앙 관리 서버 데이터 백업 작업을 생성하려면:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. 다음 방법 중 하나로 작업을 시작합니다:
   - 콘솔 트리에 있는 **작업** 폴더의 마우스 오른쪽 메뉴에서 **새로 만들기 → 작업**를 선택합니다.
   - 작업 영역에서 **작업 생성** 버튼을 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다. 마법사의 **작업 유형 선택** 창에서 **중앙 관리 서버 데이터 백업**이라는 작업 유형을 선택합니다.

중앙 관리 서버 데이터 백업 작업은 하나의 복사본으로만 만들 수 있습니다. 중앙 관리 서버에 대한 중앙 관리 서버 데이터 백업 작업이 이미 만들어졌다면 중앙 관리 서버 백업 작업 생성 마법사의 작업 유형 선택 창에 이 작업이 표시되지 않습니다.

중앙 관리 서버 데이터 백업 작업 구성

백업 작업을 생성한 후 작업 설정을 구성할 수 있습니다.

중앙 관리 서버 데이터 백업 작업을 구성하려면:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **중앙 관리 서버 데이터 백업** 작업의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

중앙 관리 서버 데이터 백업 작업의 속성 창이 열립니다. 다음과 같은 속성을 사용할 수 있습니다.

- **일반**

  일반 섹션에서는 작업 이름을 지정하고, 작업 생성 날짜, 마지막 실행 날짜, 작업 시작 상태 및 작업 결과를 확인할 수 있습니다.

- **알림**

  알림 섹션에서 작업 실행 결과와 관련된 이벤트 저장 설정을 지정하고 작업 실행 결과에 대한 알림을 구성할 수 있습니다.

- **스케줄**

  스케줄 섹션에서 작업 시작 스케줄을 지정할 수 있습니다.

- **대상**

  대상 섹션에서 중앙 관리 서버 데이터의 백업 복사본을 저장할 폴더의 경로를 지정할 수 있습니다.

- **설정**

  필요 시 **설정** 섹션에서 백업 보호 암호와 백업 복사본 수를 설정할 수 있습니다.

  %ALLUSERSPROFILE% 폴더가 저장되어 있는 논리 디스크의 섀도 복사본을 생성하고 중앙 관리 서버 데이터베이스를 복사할 수도 있습니다. 이렇게 하려면 **데이터 백업 시 파일 시스템 스냅샷 사용** 옵션을 활성화한 다음, 스냅샷 생성 권한이 있는 계정의 이름과 암호를 지정해야 합니다.

- **보안**

  보안 섹션에서 사용자 및 그룹에 중앙 관리 서버에서 작업을 수행할 수 있는 권한을 부여할 수 있습니다. **중앙 관리 서버에서 설정 상속** 옵션을 사용하면 작업의 보안 설정이 중앙 관리 서버에서 상속됩니다.

  이 옵션을 비활성화하면 작업의 보안 설정을 구성할 수 있습니다. 작업에 적용된 대로 사용자 또는 사용자 그룹에 역할을 할당하거나 사용자 또는 사용자 그룹에 권한을 할당할 수 있습니다.

  기본적으로 **중앙 관리 서버에서 설정 상속** 옵션이 활성화되어 있습니다.

- **리비전 내역**

  리비전 내역 섹션에서 작업 수정 사항을 추적할 수 있습니다. 작업 변경 내용을 저장할 때마다 리비전이 만들어집니다.

데이터 백업 및 복구 유틸리티(klbackup)

Kaspersky Security Center 배포 키트의 일부인 klbackup 유틸리티를 사용하여 백업과 향후 복구를 위해 중앙 관리 서버 데이터를 복사할 수 있습니다.

klbackup 유틸리티는 다음 두 가지 모드 중 하나로 실행할 수 있습니다:

- 대화식
- 숨김

대화식 모드에서 데이터 백업 및 복구

대화식 모드에서 klbackup 유틸리티를 사용하여 만든 백업 복사본에서 중앙 관리 서버 데이터를 복원하면 오류가 발생할 수 있습니다. 중앙 관리 서버용 15.1.0.20748-pf2 패치를 설치한 후 **데이터베이스 마이그레이션** 옵션이 비활성화된 klbackup 유틸리티를 사용하여 백업 복사본을 생성할 경우, 이 복사본을 복원할 때 오류가 발생합니다(MySQL 및 MariaDB를 제외한 모든 DBMS에 적용됨). 중앙 관리 서버용 패치 15.1.0.20748-pf2가 설치되어 있는 상태에서 다른 DBMS로 마이그레이션하지 않고 백업 복사본을 만들려는 경우 데이터 백업 작업을 사용하거나, 명령줄에서 klbackup 유틸리티를 실행하십시오.

대화식 모드에서 중앙 관리 서버 데이터의 백업 복사본을 만들려면 다음과 같이 하십시오:

1. Kaspersky Security Center 설치 폴더에 있는 klbackup 유틸리티를 실행합니다.

   백업 및 복원 마법사가 시작됩니다.

2. 마법사의 첫 번째 창에서 **중앙 관리 서버 데이터 백업 실행**을 선택합니다.

   중앙 관리 서버 인증서만 백업 또는 복원 옵션을 선택하면 중앙 관리 서버 인증서 및 개인 키의 백업 복사본만 저장됩니다. 중앙 관리 서버 인증서와 개인 키 백업은 Kaspersky Security Center Windows의 중앙 관리 서버에서 Kaspersky Security Center Linux의 중앙 관리 서버로 마이그레이션을 수행할 때 유용할 수 있습니다. 또한 Kaspersky Security Center Linux 중앙 관리 서버 및 Kaspersky Security Center Windows 중앙 관리 서버 간에 관리 중인 기기를 마이그레이션할 수 있습니다. 자세한 내용은 klbackup 유틸리티를 사용하여 다른 중앙 관리 서버에서 관리 중인 기기 전환을 참조하십시오.

   다음을 누릅니다.

3. 마법사의 다음 창에서 다음 옵션을 지정합니다:

   - **백업 대상 폴더**
   - **데이터베이스 마이그레이션**

     현재 중앙 관리 서버 데이터를 Microsoft SQL Server 데이터베이스에 저장하고 있고 이를 MySQL 또는 MariaDB, PostgreSQL 또는 Postgres Pro, Azure SQL 중 하나로 마이그레이션해야 하는 경우 이 옵션을 활성화하십시오. 기본적으로 이 옵션은 비활성화되어 있습니다.

     - **MySQL/MariaDB 형식으로 마이그레이션**

       현재 SQL Server를 중앙 관리 서버용 DBMS로 사용 중이고 SQL Server에서 MySQL 또는 MariaDB DBMS로 데이터를 마이그레이션하려면 이 옵션을 활성화합니다. Kaspersky Security Center는 MySQL 및 MariaDB와 호환되는 백업을 생성합니다. 그런 다음 백업에서 MySQL 또는 MariaDB로 데이터를 복원할 수 있습니다.

     - **Postgres로 마이그레이션**

       현재 SQL Server를 중앙 관리 서버용 DBMS로 사용 중이고 SQL Server에서 PostgreSQL 또는 Postgres Pro DBMS로 데이터를 마이그레이션하는 경우 이 옵션을 활성화합니다. Kaspersky Security Center는 PostgreSQL 및 Postgres Pro와 호환되는 백업을 생성합니다. 이제 백업에서 PostgreSQL 또는 Postgres Pro로 데이터를 복원할 수 있습니다.

       이 옵션은 Kaspersky 기술 지원에 요청하여 중앙 관리 서버용 15.1.0.20748-pf2 패치를 설치하거나 Kaspersky Security Center Windows 버전 15.1.0.22239로 업데이트하는 경우에 사용할 수 있습니다.

- **Azure 형식으로 마이그레이션**

  현재 SQL Server를 중앙 관리 서버용 DBMS로 사용하고 SQL Server에서 Azure SQL DBMS로 데이터를 마이그레이션하려면 이 옵션을 활성화합니다. Kaspersky Security Center는 Azure SQL과 호환되는 백업을 생성합니다. 그런 다음 백업에서 Azure SQL로 데이터를 복원할 수 있습니다.

- **백업 대상 폴더의 이름에 현재 날짜 및 시간을 포함합니다**

- **백업 암호**

4. 백업을 시작하려면 **다음** 버튼을 클릭합니다.

5. AWS(Amazon Web Services) 또는 Microsoft Azure와 같은 클라우드 환경에서 데이터베이스를 사용 중이라면 **온라인 스토리지에 로그인** 창에서 다음 필드에 정보를 입력합니다.

   - AWS:

     - **S3 버킷 이름**

       백업용으로 생성한 S3 버킷의 이름입니다.

     - **액세스 키 ID**

       S3 버킷 스토리지 인스턴스 사용을 위해 IAM 사용자 계정을 만들 때 키 ID(영숫자 문자 시퀀스)가 제공됩니다.

       S3 버킷에서 RDS DB를 선택한 경우 이 필드를 사용할 수 있습니다.

     - **비밀 키**

       IAM 사용자 계정을 만들 때 액세스 키 ID와 함께 제공된 비밀 키입니다.

       비밀 키의 문자는 별표로 표시됩니다. 비밀 키 입력을 시작하면 **표시** 버튼이 나타납니다. 이 버튼을 필요한 시간 동안 누르고 있으면 입력한 문자가 표시됩니다.

       IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

   - Microsoft Azure:

     - **Azure 스토리지 계정 이름**

       Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

     - **Azure 서브스크립션 ID**

       Azure Portal에서 생성한 서브스크립션입니다.

     - **Azure 암호**

       애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

- **Azure 애플리케이션 ID**

  Azure Portal에서 생성한 애플리케이션 ID입니다.

  검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

- **Azure SQL 서버 이름**

  Azure SQL Server 속성에서 제공되는 이름 및 리소스 그룹입니다.

- **Azure SQL 서버 리소스 그룹**

  Azure SQL Server 속성에서 제공되는 이름 및 리소스 그룹입니다.

- **Azure 스토리지 액세스 키**

  스토리지 계정 속성의 접근 허용 키 섹션에서 제공됩니다. 원하는 어떤 키든 사용할 수 있습니다(key1 또는 key2).

대화식 모드에서 중앙 관리 서버 데이터를 복구하려면 다음과 같이 하십시오:

1. Kaspersky Security Center 설치 폴더에 있는 klbackup 유틸리티를 실행합니다. 유틸리티는 중앙 관리 서버를 설치할 때 사용한 것과 같은 계정으로 시작해야 합니다. 새로 설치된 중앙 관리 서버에서 유틸리티를 실행할 것을 권장합니다.

   백업 및 복원 마법사가 시작됩니다.

2. 마법사의 첫 번째 창에서 **중앙 관리 서버 데이터 복원**을 선택한 후, **다음**을 클릭합니다.

   중앙 관리 서버 인증서만 백업 또는 복원 옵션을 선택하면 중앙 관리 서버 인증서 및 개인 키만 복구됩니다.

   비활성 장애 조치 클러스터 노드에서 klbackup 유틸리티를 실행하면 옵션 중 하나를 선택하라는 메시지가 표시됩니다. 중앙 관리 서버 인증서를 지정하거나 중앙 관리 서버에서 자동으로 데이터를 검색합니다.

3. 마법사의 **복원 설정** 창에서:

   - 중앙 관리 서버 데이터의 백업 복사본이 있는 폴더를 지정합니다.

     AWS 또는 Azure와 같은 클라우드 환경에서 작업 중인 경우 스토리지 주소를 지정합니다. 파일 이름이 backup.zip인지 확인합니다.

   - 데이터를 백업했을 때 입력한 암호를 지정합니다.

     데이터를 복원할 때는 백업 중에 입력한 것과 같은 암호를 지정해야 합니다. 백업 후에 공유 폴더 경로가 변경된 경우, 복원되는 데이터를 사용하는 작업의 동작(복원 작업, 원격 설치 작업 등)이 잘 수행되는지 확인합니다. 필요한 경우 이러한 작업의 설정을 편집합니다. 데이터가 백업 파일에서 복원되는 동안 누구도 중앙 관리 서버의 공유 폴더에 접근해서는 안 됩니다. klbackup 유틸리티를 시작하는 계정에는 공유 폴더에 대한 모든 접근 권한이 있어야 합니다.

4. 데이터를 복구하려면 **다음** 버튼을 누릅니다.

숨김 모드에서 데이터 백업 및 복구

숨김 모드에서 중앙 관리 서버 데이터를 복구하거나 백업 복사본을 만들려면,

중앙 관리 서버가 설치된 기기의 명령줄에서 필요한 키 세트를 사용하여 klbackup을 실행합니다.

klbackup 유틸리티를 사용하면 네트워크 에이전트 플래그가 복원되지 않습니다. 수동으로 네트워크 에이전트 플래그를 구성해야 합니다.

복원을 수행할 중앙 관리 서버 인스턴스는 같은 유형의 DBMS를 사용해야 합니다. 중앙 관리 서버의 버전은 원래 버전과 같을 수도 있고(패치가 원래 중앙 관리 서버와 동일하거나 그 이상임) 더 최신 버전일 수도 있습니다.

유틸리티 명령줄 구문:

```
klbackup -path <backup path> [-linux_path <SQL Server 백업 경로>][-node_cert <인증서 경로>] [-logfile <로그 파일>] [-use_ts]|[-restore] [-password <암호>] [-cert_only] [-online] [-migrate postgres]
```

klbackup 유틸리티 명령줄에서 암호를 지정하지 않으면 유틸리티가 대화식으로 암호 입력을 요청합니다.

키에 대한 설명:

- `-path <백업 경로>` - 백업 폴더에 정보를 저장하거나, 백업 폴더의 데이터를 복구에 사용합니다(필수 파라미터).

  데이터베이스 서버 계정과 klbackup 유틸리티에 백업 폴더의 데이터를 변경할 수 있는 권한이 주어져야 합니다.

- `-linux_path <SQL Server 백업 경로>`—SQL Server on Linux에 대한 백업 데이터가 있는 폴더의 로컬 경로입니다.

  데이터베이스 서버 계정과 klbackup 유틸리티에 SQL Server 백업 폴더의 데이터를 변경할 수 있는 권한이 주어져야 합니다.

- `-node_cert <인증서 경로>` - 복구 후 비활성 장애 조치 클러스터 노드를 구성하기 위한 서버 인증서 파일입니다. 설정하지 않으면 서버에서 자동 검색됩니다.

  비활성 장애 조치 클러스터 노드에서 klbackup 유틸리티를 실행할 때 이 키를 사용하여 서버 인증서 경로를 지정합니다.

- `-logfile <로그 파일>`- 중앙 관리 서버 데이터의 백업 및 복구에 대한 리포트를 저장합니다.

- `-use_ts` - 데이터를 저장할 때 정보를 백업 폴더의 하위 폴더로 복사합니다. 이 하위 폴더의 이름은 현재 날짜와 UTC 기준 작업 시간을 포함하는 `klbackup YYYY-MM-DD # HH-MM-SS` 형식으로 되어 있습니다. 키가 지정되지 않으면 정보가 백업 폴더의 루트에 저장됩니다.

  이미 백업 복사본이 저장된 폴더에 정보를 저장하려고 하면 오류 메시지가 나타납니다. 정보가 업데이트되지 않습니다.

  `-use_ts` 키를 사용하면 중앙 관리 서버의 데이터 압축 파일을 유지 관리할 수 있습니다. 예를 들어 `-path` 키가 `C:\KLBackups` 폴더를 나타내면, `klbackup 2022/6/19 # 11-30-18` 폴더에는 2022년 6월 19일 오전 11시 30분 18초 당시의 중앙 관리 서버 상태 정보가 저장됩니다.

- `-restore` – 중앙 관리 서버 데이터를 복구합니다. 데이터 복구는 백업 폴더에 포함된 정보를 기반으로 수행됩니다. 키가 없으면 데이터가 백업 폴더에 백업됩니다.

- `-password <암호>` - 민감한 데이터를 보호하기 위한 암호입니다.

  잊어버린 암호는 복원할 수 없습니다. 암호 요구 사항이 없습니다. 암호 길이는 무제한이며 길이가 0(암호 없음)일 수도 있습니다.

  데이터를 복원할 때는 백업 중에 입력한 것과 같은 암호를 지정해야 합니다. 백업 후에 공유 폴더 경로가 변경된 경우, 복원되는 데이터를 사용하는 작업의 동작(복원 작업, 원격 설치 작업 등)이 잘 수행되는지 확인합니다. 필요한 경우 이러한 작업의 설정을 편집합니다. 데이터가 백업 파일에서 복원되는 동안 누구도 중앙 관리 서버의 공유 폴더에 접근해서는 안 됩니다. klbackup 유틸리티를 시작하는 계정에는 공유 폴더에 대한 모든 접근 권한이 있어야 합니다. 새로 설치된 중앙 관리 서버에서 유틸리티를 실행할 것을 권장합니다.

- `-cert_only` - 중앙 관리 서버의 인증서와 개인 키만 저장하거나 복구합니다.

  이 플래그는 Kaspersky Security Center Windows의 중앙 관리 서버에서 Kaspersky Security Center Linux의 중앙 관리 서버로 마이그레이션을 수행할 때 유용할 수 있습니다. 또한 Kaspersky Security Center Linux 중앙 관리 서버 및 Kaspersky Security Center Windows 중앙 관리 서버 간에 관리 중인 기기를 마이그레이션할 수 있습니다.

- `-online` - 볼륨 스냅샷을 생성하여 중앙 관리 서버의 오프라인 시간을 최소화하며 중앙 관리 서버 데이터를 백업합니다. 유틸리티를 사용하여 데이터를 복구하는 경우 이 옵션은 무시됩니다. 다른 DBMS로 마이그레이션하기 위한 백업을 생성할 경우에는 이 플래그를 사용하지 마십시오.

- `-archive 0` - 서버 데이터를 일반 파일로 유지합니다. 기본적으로(`-archive 1`) 서버 데이터는 압축 파일에 저장됩니다.

- `-migrate mysql` - MySQL과 호환되는 SQL Server 데이터베이스에 저장된 중앙 관리 서버 데이터의 백업을 생성합니다. 그런 다음 백업에서 MySQL로 데이터를 복원할 수 있습니다.

- `-migrate postgres` - PostgreSQL 및 Postgres Pro와 호환되는 SQL Server 데이터베이스에 저장된 중앙 관리 서버 데이터의 백업을 생성합니다. 백업의 데이터를 PostgreSQL 또는 Postgres Pro로 복원할 수 있습니다. 중앙 관리 서버 데이터 백업을 사용하여 Kaspersky Security Center Linux로 마이그레이션 수행 시, 이 플래그를 사용합니다.

  이 옵션은 Kaspersky 기술 지원에 요청하여 중앙 관리 서버용 15.1.0.20748-pf2 패치를 설치하거나 Kaspersky Security Center Windows 버전 15.1.0.22239로 업데이트하는 경우에 사용할 수 있습니다.

klbackup 유틸리티를 사용하여 다른 중앙 관리 서버에서 관리 중인 기기 전환

klbackup 유틸리티로 다른 중앙 관리 서버에서 관리 중인 기기를 전환할 수 있습니다. 마이그레이션을 수행할 때 klbackup 유틸리티를 사용하여 Kaspersky Security Center Windows 중앙 관리 서버를 Kaspersky Security Center Linux 중앙 관리 서버로 변경할 수 있습니다. 또한 Kaspersky Security Center Linux 중앙 관리 서버 및 Kaspersky Security Center Windows 중앙 관리 서버 간에 관리 중인 기기를 마이그레이션할 수 있습니다.

klbackup 유틸리티를 사용하여 다른 중앙 관리 서버에서 관리 중인 기기를 전환하려면:

1. 이전 기기에서 중앙 관리 서버 인증서와 개인 키의 백업 복사본을 생성합니다.

   다음 방법으로 백업 복사본을 생성할 수 있습니다.

   - klbackup 유틸리티 인터페이스 사용(Kaspersky Security Center Windows 중앙 관리 서버만 해당)

     Kaspersky Security Center 설치 폴더에 있는 klbackup 유틸리티를 실행한 후 **중앙 관리 서버 인증서만 백업 또는 복원** 옵션을 사용하여 백업을 생성합니다.

- 명령 프롬프트 사용(Kaspersky Security Center Windows 및 Kaspersky Security Center Linux 중앙 관리 서버 버전 15.1 이상)

  명령줄에서 `-cert_only` 키와 함께 klbackup 유틸리티를 실행하여 중앙 관리 서버 인증서와 개인 키의 백업 복사본을 만듭니다:

  `klbackup -path <중앙 관리 서버 인증서 백업 복사본 경로> -cert_only`

2. 이전 기기에서 중앙 관리 서버의 네트워크 연결을 해제합니다.

3. 다른 중앙 관리 서버가 있는 기기에 같은 주소를 할당합니다.

   새 중앙 관리 서버에 NetBIOS 이름, FQDN, 고정 IP 주소를 할당할 수 있습니다. 네트워크 에이전트 배포 시 네트워크 에이전트 설치 패키지에 설정된 중앙 관리 서버 주소에 따라 다릅니다. 또는 네트워크 에이전트가 연결할 중앙 관리 서버를 결정하는 연결 주소를 사용할 수 있습니다(이 주소는 관리 중인 기기에서 klnagchk 유틸리티를 사용하여 얻을 수 있습니다).

4. 다른 중앙 관리 서버가 있는 기기에서 백업 복사본에서 중앙 관리 서버 인증서와 개인 키를 복원합니다.

   다음 방법으로 백업 복사본을 복원할 수 있습니다.

   - klbackup 유틸리티 인터페이스 사용(Kaspersky Security Center Windows 중앙 관리 서버만 해당)

     klbackup 유틸리티를 실행한 후 **중앙 관리 서버 인증서만 백업 또는 복원** 옵션을 사용하여 백업을 복원합니다.

   - 명령 프롬프트 사용(Kaspersky Security Center Windows 및 Kaspersky Security Center Linux 중앙 관리 서버 버전 15.1 이상)

     명령줄에서 `-cert_only` 키와 함께 klbackup 유틸리티를 실행하여 중앙 관리 서버 인증서와 개인 키의 백업 복사본을 복원합니다.

     `klbackup -path <중앙 관리 서버 인증서 백업 복사본 경로> -restore -cert_only`

   관리 중인 기기는 다른 중앙 관리 서버에서 관리하게 됩니다. 이 중앙 관리 서버로 이동하여 관리 중인 기기가 네트워크에 표시되고 네트워크 에이전트가 설치되어 실행 중인지 확인합니다(**표시 여부**, **네트워크 에이전트가 설치됨**, **네트워크 에이전트가 실행 중**의 *예* 값).

MySQL 또는 MariaDB 사용 시 중앙 관리 서버 데이터 백업 및 복원

데이터 백업을 사용하여 Kaspersky Security Center Linux가 관리하도록 Kaspersky Security Center Windows에서 중앙 관리 서버 데이터를 마이그레이션할 수 있습니다. 중앙 관리 서버 데이터 백업을 사용한 마이그레이션은 지원하는 Kaspersky Security Center Windows 버전에서 Kaspersky Security Center Linux 15.2 이상으로의 마이그레이션에서만 지원합니다.

Kaspersky Security Center Windows 및 Kaspersky Security Center Linux에서 MySQL 또는 MariaDB를 DBMS로 사용한다면 `lower_case_table_names` 파라미터가 현재 및 새 DBMS와 일치해야 합니다. 그렇지 않으면 중앙 관리 서버 데이터가 잘못 마이그레이션됩니다.

Kaspersky Security Center Windows에서 중앙 관리 서버 데이터를 백업하기 전에 `lower_case_table_names` 파라미터값을 확인하십시오. 이전에 DBMS 설치 시 이 파라미터를 지정하지 않으면 기본 파라미터값이 사용됩니다. Windows용 `lower_case_table_names` 파라미터의 기본값은 `1`입니다.

Kaspersky Security Center Linux용 MySQL 또는 MariaDB를 설치할 때 MySQL 웹사이트의 지침을 참조하여 `lower_case_table_names` 파라미터를 Windows용 이 파라미터에 지정된 값과 같은 값으로 설정합니다. 이 파라미터를 지정하지 않으면 기본 파라미터값이 사용됩니다. Linux 기반 운영 체제에서 `lower_case_table_names` 파라미터의 기본값은 Windows용 기본값과 다릅니다.

MySQL 8.0을 설치하려면, 이 지침에 따라 `lower_case_table_names` 파라미터를 지정하는 방법이 통하지 않을 수 있습니다. 이때는 먼저 MySQL 5.7을 설치하고, 지침을 사용하여 `lower_case_table_names` 파라미터를 지정한 다음, MySQL 5.7을 MySQL 8.0으로 업그레이드해야 합니다. 현재 및 새 DBMS에 대한 `lower_case_table_names` 파라미터가 일치하지 않으면 중앙 관리 서버 데이터가 잘못 복원됩니다.

중앙 관리 서버 데이터의 백업 및 복원 최적화

중앙 관리 서버 데이터의 백업 및 복원을 최적화하기 위해 중앙 관리 서버의 다운타임을 줄이려면 다음 절차를 따르십시오.

- **데이터 백업에 파일 시스템 스냅샷 사용** 옵션을 활성화합니다.

  자세한 내용은 다음 글을 참조하십시오: 파일 시스템 스냅샷을 사용하여 백업 시간 단축.

- 다음 플래그를 구성합니다.

  관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

  - `KLSRV_BKP_FILES`—데이터베이스 파일을 2~32개의 작은 파일로 분할합니다. CPU가 DBMS 성능을 제한할 시 이를 통해 백업 및 복원 속도를 높일 수 있습니다.

    예:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
    ```

  - `KLSRV_BKP_BACKUP_EXTRA_PARS`—`COMPRESSION` 및 `MAXTRANSFERSIZE` 파라미터를 지정합니다. 파일 입출력으로 DBMS 성능이 제한될 시 이를 통해 백업 속도를 높일 수 있습니다.

    예:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
    MAXTRANSFERSIZE = 4194304"
    ```

  - `KLSRV_BKP_RESTORE_EXTRA_PARS`—`MAXTRANSFERSIZE` 매개변수를 지정합니다. 파일 입출력으로 DBMS 성능이 제한될 시 이를 통해 복원 속도를 높일 수 있습니다.

    예:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
    = 4194304"
    ```

  - `KLSRV_BKP_ONLINE_DB_BACKUP`—백업 중에 중앙 관리 서버 가동 중지 시간을 없앱니다. 다음 DBMS에서만 사용 가능합니다:

    - PostgreSQL, Postgres Pro.
    - 전체 복원 모델을 적용한 SQL Server. 자세한 내용은 SQL Server 설명서를 참조하십시오. `KLSRV_BKP_ONLINE_DB_BACKUP` 플래그를 활성화하면 SQL Server DBMS가 자동으로 전체 복구 모델로 전환됩니다.

    예:

    ```
    klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
    ```

다른 기기로 중앙 관리 서버 이동

새 기기에서 중앙 관리 서버 사용 시, 다음 방법 중 하나로 이동할 수 있습니다.

- 중앙 관리 서버와 데이터베이스 서버를 새 기기로 이동합니다(데이터베이스 서버는 새 기기에 중앙 관리 서버와 함께 설치하거나 다른 기기에 설치할 수 있습니다).
- 데이터베이스 서버를 이전 기기에 유지하고 중앙 관리 서버만 새 기기로 이동합니다.

새 기기로 중앙 관리 서버를 이동하려면:

1. 이전 기기에서 중앙 관리 서버 데이터의 백업을 만듭니다.

   이렇게 하려면 관리 콘솔을 통해 데이터 백업 작업을 실행하거나 klbackup 유틸리티를 실행합니다.

   > SQL Server를 중앙 관리 서버용 DBMS로 사용한다면 SQL Server에서 MySQL 또는 MariaDB DBMS로 데이터를 마이그레이션할 수 있습니다. 이렇게 하려면 대화형 모드에서 klbackup 유틸리티를 실행하여 데이터 백업을 만듭니다. 백업 및 복원 마법사의 **백업 설정** 창에서 **MySQL/MariaDB 형식으로 마이그레이션** 옵션을 활성화합니다. Kaspersky Security Center는 MySQL 및 MariaDB와 호환되는 백업을 생성합니다. 그런 다음 백업에서 MySQL 또는 MariaDB로 데이터를 복원할 수 있습니다.

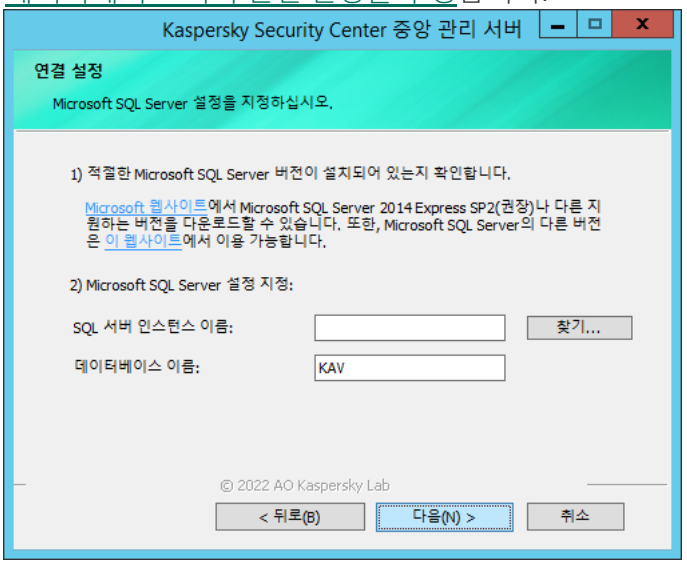
   > SQL Server에서 Azure SQL DBMS로 데이터를 마이그레이션하려면 **Azure 형식으로 마이그레이션** 옵션을 활성화할 수도 있습니다.

2. 이전 기기에서 중앙 관리 서버의 네트워크 연결을 해제합니다.
3. 중앙 관리 서버를 설치할 새 기기를 선택하십시오. 선택한 기기의 하드웨어 및 소프트웨어가 중앙 관리 서버, 관리 콘솔, 네트워크 에이전트의 요구 사항을 충족하는지 확인합니다. 또한 중앙 관리 서버에서 사용되는 포트를 사용할 수 있는지 확인하십시오.
4. 새 기기에 같은 주소를 할당합니다.

   새 중앙 관리 서버에 NetBIOS 이름, FQDN, 고정 IP 주소를 할당할 수 있습니다. 네트워크 에이전트 배포 시 네트워크 에이전트 설치 패키지에 설정된 중앙 관리 서버 주소에 따라 다릅니다. 또는 네트워크 에이전트가 연결할 중앙 관리 서버를 결정하는 연결 주소를 사용할 수 있습니다(이 주소는 관리 중인 기기에서 klnagchk 유틸리티를 사용하여 얻을 수 있습니다).
5. 필요하다면 다른 기기에 중앙 관리 서버가 사용할 데이터베이스 관리 시스템(DBMS)을 설치합니다.

   데이터베이스는 중앙 관리 서버가 설치된 새 기기에 설치하거나 다른 기기에 설치할 수 있습니다. 이 기기가 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인합니다. DBMS 선택 시, 중앙 관리 서버에서 다루는 기기의 수를 고려하십시오.
6. 새 기기에서 중앙 관리 서버 설치를 실행합니다.

7. 중앙 관리 서버를 설치할 때 데이터베이스 서버 연결 설정을 구성합니다.



Microsoft SQL Server용 연결 설정 창의 예

데이터베이스 서버를 찾아야 하는 위치에 따라 다음 중 하나를 수행합니다:

- **이전 기기에 데이터베이스 서버 유지**

  1. **SQL 서버 인스턴스 이름** 필드 옆에 있는 **찾기** 버튼을 클릭한 다음 표시되는 목록에서 이전 기기 이름을 선택합니다.

     새 중앙 관리 서버와 연결하려면 이전 기기를 사용할 수 있어야 합니다.

  2. **데이터베이스 이름** 필드에 이전 데이터베이스 이름을 입력합니다.

- **데이터베이스 서버를 새 기기로 이동**

  1. **SQL 서버 인스턴스 이름** 필드 옆에 있는 **찾기** 버튼을 클릭한 다음 표시되는 목록에서 기기 이름을 선택합니다.

  2. **데이터베이스 이름** 필드에 새 데이터베이스 이름을 입력합니다.

     새 데이터베이스 이름은 이전 기기의 데이터베이스 이름과 일치해야 합니다. 중앙 관리 서버 백업을 사용할 수 있도록 데이터베이스 이름이 같아야 합니다. 기본 데이터베이스 이름은 *KAV*입니다.

8. 설치가 완료되면 klbackup 유틸리티를 사용하여 새 기기에서 중앙 관리 서버 데이터를 복구합니다.

   이전 기기와 새 기기에서 SQL Server를 DBMS로 사용 시, 새 기기에 설치된 SQL Server 버전이 이전 기기에 설치된 SQL Server 버전과 같거나 더 최신 버전이어야 합니다. 그렇지 않으면 새 기기에서 중앙 관리 서버 데이터를 복구할 수 없습니다.

9. 관리 콘솔을 열고 중앙 관리 서버에 연결합니다.

10. 모든 관리 중인 기기가 중앙 관리 서버에 연결되어 있는지 확인합니다.

11. 이전 기기에서 중앙 관리 서버와 데이터베이스 서버를 제거합니다.

Kaspersky Security Center 웹 콘솔을 사용하여 중앙 관리 서버와 데이터베이스 서버를 다른 기기로 이동할 수도 있습니다.

여러 중앙 관리 서버 간의 충돌 방지

네트워크에 중앙 관리 서버가 둘 이상 있는 경우 해당 서버가 같은 클라이언트 기기를 확인할 수 있습니다. 이는 이미 다른 중앙 관리 서버에 의해 설치된 애플리케이션을 중앙 관리 서버가 다시 설치하는 등의 충돌을 발생시킬 수 있습니다. 다른 중앙 관리 서버에서 관리하는 기기에 애플리케이션이 설치되는 것을 방지하려면 *원격으로 애플리케이션 설치* 작업 속성에서 **이 중앙 관리 서버를 통해 관리되는 기기에만 설치** 옵션을 활성화해야 합니다.

이 중앙 관리 서버를 통해 관리되는 기기에만 설치 옵션을 활성화한 다음 *원격으로 애플리케이션 설치* 작업을 실행하면, 대상 기기가 다른 중앙 관리 서버에서 관리되는지 확인하기 위한 검사가 수행됩니다. 다른 중앙 관리 서버에서 관리 중인 기기의 경우 **다른 중앙 관리 서버에서 관리** 속성 값이 `true`로 설정됩니다. *원격으로 애플리케이션 설치* 작업은 이러한 기기에 적용되지 않습니다.

다른 중앙 관리 서버에서 관리 속성 값은 관리 중인 기기 목록 및 할당되지 않은 기기 목록의 **다른 중앙 관리 서버에서 관리** 열에 표시됩니다.

다음과 같은 용도로 **다른 중앙 관리 서버에서 관리** 속성을 기준으로 사용할 수도 있습니다:

- 기기 검색
- 기기 조회
- 기기 이동 규칙
- 자동 태그 입력 규칙

다른 중앙 관리 서버에서 관리 속성을 재설정하려면 다음 절차를 따르십시오.

1. Kaspersky Security Center 웹 콘솔의 메인 메뉴에서 **발견 및 배포 → 미할당 기기**로 이동합니다.
2. 필요한 기기를 선택한 다음 **다른 중앙 관리 서버로 관리 속성 해제** 버튼을 클릭합니다.

   다른 중앙 관리 서버에서 관리 속성이 초기화됩니다.

관리 그룹 관리

이 섹션에서는 관리 그룹을 관리하는 방법에 대해 설명합니다.

관리 그룹에 대해 다음과 같은 처리를 수행할 수 있습니다:

- 임의의 계층 구조 레벨에 속한 중첩된 그룹을 임의의 수만큼 관리 그룹에 추가.
- 관리 그룹에 기기 추가.
- 개별 기기 및 전체 그룹을 다른 그룹으로 이동하여 관리 그룹의 계층 구조 변경.
- 관리 그룹에서 중첩된 그룹 및 기기 제거.
- 관리 그룹에 보조 및 가상 중앙 관리 서버 추가.

- 중앙 관리 서버의 관리 그룹에서 다른 서버의 관리 그룹으로 기기 이동.
- 그룹에 포함된 기기에 자동으로 설치되는 Kaspersky 애플리케이션 정의.

관리하려는 관리 그룹이나 이러한 그룹이 속하는 중앙 관리 서버의 **관리 그룹 관리** 영역에서 **수정** 권한이 있는 경우에만 이러한 작업을 수행할 수 있습니다.

관리 그룹 생성

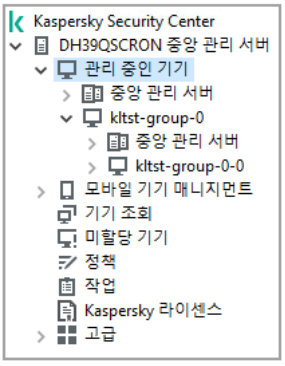
관리 그룹의 계층 구조는 Kaspersky Security Center 메인 애플리케이션 창의 **관리 중인 기기** 폴더에 만들어집니다. 관리 그룹은 콘솔 트리에 폴더로 표시됩니다(아래 그림 참조).

Kaspersky Security Center 설치 직후에 **관리 중인 기기** 폴더에는 빈 **중앙 관리 서버** 폴더만 있습니다.

> 사용자 인터페이스의 설정에 따라 콘솔 트리에 **중앙 관리 서버** 폴더가 표시되는지 여부가 결정됩니다. 이 폴더를 표시하려면 메뉴 바에서 **보기 → 인터페이스 구성**으로 이동한 다음 열리는 **인터페이스 구성** 창에서 **보조 중앙 관리 서버 표시** 확인란을 선택합니다.

관리 그룹의 계층 구조를 만들 때 **관리 중인 기기** 폴더에 기기와 가상 컴퓨터를 추가하고 중첩된 그룹도 함께 추가할 수 있습니다. 보조 중앙 관리 서버 및 가상 중앙 관리 서버를 **중앙 관리 서버** 폴더에 추가할 수 있습니다.

관리 중인 기기 폴더와 마찬가지로, 처음에는 이 그룹의 보조 및 가상 중앙 관리 서버와 함께 작업하기 위한 빈 **중앙 관리 서버** 폴더가 생성된 각 그룹에 포함됩니다. 이 그룹의 정책 및 작업에 관한 정보, 이 그룹에 포함된 기기에 관한 정보가 이 그룹의 작업 영역에 해당 이름으로 되어 있는 탭에 표시됩니다.



관리 그룹 계층 구조 보기

관리 그룹을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 확장합니다.
2. 기존 관리 그룹에 하위 그룹을 생성하려면 **관리 중인 기기** 폴더에서 새 관리 그룹을 포함할 그룹에 해당하는 하위 폴더를 선택합니다.

   가장 높은 레벨의 새 관리 그룹을 만드는 경우에는 이 단계를 건너뛸 수 있습니다.

3. 다음 방법 중 하나로 관리 그룹 만들기를 시작합니다:

   - 마우스 오른쪽 메뉴에서 **만들기 → 그룹** 명령을 사용합니다.
   - **기기** 탭에서 메인 애플리케이션 창의 작업 영역에 있는 **새 그룹** 버튼을 누릅니다.

4. 열리는 **그룹 이름** 창에 그룹 이름을 입력하고 **확인**을 누릅니다.

   지정한 이름의 새 관리 그룹 폴더가 콘솔 트리에 나타납니다.

애플리케이션은 Active Directory 구조 또는 도메인 네트워크의 구조에 기초하여 관리 그룹의 계층을 만들 수 있습니다. 또한, 텍스트 파일에서 그룹 구조를 만들 수 있습니다.

관리 그룹의 구조를 만들려면 아래와 같이 진행합니다:

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 선택합니다.
2. **관리 중인 기기** 폴더의 마우스 오른쪽 메뉴에서 **모든 작업 → 새 그룹 조직도**를 선택합니다.

   새 관리 그룹 구조 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

관리 그룹 이동

그룹의 계층 구조 내에서 중첩된 관리 그룹을 이동할 수 있습니다.

관리 그룹은 모든 중첩된 그룹, 보조 중앙 관리 서버, 기기, 그룹 정책 및 작업과 함께 이동합니다. 시스템이 관리 그룹의 계층 구조에서 새 위치에 해당하는 모든 설정을 그룹에 적용합니다.

그룹 이름은 계층 구조의 한 레벨 내에서 고유해야 합니다. 관리 그룹을 이동해가는 대상 폴더에 동일한 이름의 그룹이 이미 있으면 이동하는 관리 그룹의 이름을 변경해야 합니다. 이동하는 그룹의 이름을 변경하지 않으면 이동 후 해당 이름에 **(<순차적 번호>)** 형식의 색인이 자동으로 추가됩니다. 예: **(1)**, **(2)**.

관리 중인 기기 폴더는 관리 콘솔에 기본 제공되는 요소이므로 이름을 바꿀 수 없습니다.

그룹을 콘솔 트리의 다른 폴더로 이동하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 이동할 그룹을 선택합니다.
2. 다음 중 하나를 수행합니다:

   - 다음 방법으로 마우스 오른쪽 메뉴를 사용하여 그룹을 이동합니다:

     1. 그룹의 마우스 오른쪽 메뉴에서 **잘라내기**을 선택합니다.
     2. 선택한 그룹을 이동하려는 관리 그룹의 마우스 오른쪽 메뉴에서 **붙여넣기**를 선택합니다.

- 다음 방법으로 메인 애플리케이션 메뉴를 사용하여 그룹을 이동합니다:

  a. 메인 메뉴에서 **처리 → 잘라내기**을 선택합니다.

  b. 콘솔 트리에서 선택한 그룹을 이동하려는 관리 그룹을 선택합니다.

  c. 메인 메뉴에서 **처리 → 붙여넣기**를 선택합니다.

- 마우스를 사용하여 콘솔 트리에서 그룹을 다른 그룹으로 이동합니다.

관리 그룹 삭제

관리 그룹에 보조 중앙 관리 서버, 중첩된 그룹 또는 클라이언트 기기가 없고 해당 관리 그룹에 대해 만들어진 그룹 작업 또는 정책이 없는 경우 관리 그룹을 삭제할 수 있습니다.

관리 그룹을 삭제하려면 먼저 해당 그룹에서 모든 보조 중앙 관리 서버, 중첩된 그룹 및 클라이언트 기기를 삭제해야 합니다.

그룹을 삭제하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 관리 그룹을 선택합니다.
2. 다음 중 하나를 수행합니다:

   - 그룹의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
   - 메인 애플리케이션 메뉴에서 **처리 → 삭제**를 선택합니다.
   - **DELETE** 키를 누릅니다.

관리 그룹의 구조 자동으로 만들기

Kaspersky Security Center에서는 그룹 계층 구조 생성 마법사를 사용하여 관리 그룹의 구조를 생성할 수 있습니다.

이 마법사는 다음 데이터를 기반으로 관리 그룹의 구조를 만듭니다:

- Windows 도메인 및 작업 그룹 구조
- Active Directory 그룹 구조
- 관리자가 수동으로 만드는 텍스트 파일의 컨텐츠

텍스트 파일을 생성할 때는 다음 요구 사항을 충족해야 합니다:

- 새 그룹의 이름은 각각 새 행에 입력해야 하며 구분 기호는 줄 바꿈으로 시작해야 합니다. 빈 행은 무시됩니다.

  예:
  지사 1
  지사 2
  지사 3
  첫 번째 계층 구조 레벨의 세 그룹이 대상 그룹에 만들어집니다.

- 중첩 그룹의 이름은 슬래시(/)를 사용하여 입력해야 합니다.

  예:
  지사 1/국 1/부서 1/팀 1
  서로 중첩되는 네 개의 하위 그룹이 대상 그룹에 만들어집니다.

- 동일한 계층 구조 레벨의 중첩 그룹을 몇 개 만들려면 "그룹의 전체 경로"를 지정해야 합니다.

  예:
  지사 1/국 1/부서 1
  지사 1/국 2/부서 1
  지사 1/국 3/부서 1
  지사 1/국 4/부서 1
  첫 번째 계층 구조 레벨인 지사 1의 그룹 하나가 대상 그룹에 생성됩니다. 이 그룹에는 동일한 계층 구조 레벨에 속하는 4개의 중첩 그룹("국 1", "국 2", "국 3" 및 "국 4")이 포함되어 있습니다. 그리고 해당 그룹에는 각각 "부서 1" 그룹이 포함됩니다.

마법사를 통해 관리 그룹의 계층 구조를 만들더라도 네트워크 무결성에는 아무런 영향이 없으며 기존 그룹이 교체되는 대신 새 그룹이 추가됩니다. 클라이언트 기기를 관리 그룹으로 이동하면 **미할당 기기** 그룹에서 없어지기 때문에 관리 그룹에 다시 포함할 수 없습니다.

관리 그룹 구조를 만들 때 이유가 있어서(예: 기기 종료 또는 네트워크 연결 해제) 기기가 **미할당 기기** 그룹에 포함되어 있지 않으면 기기가 자동으로 관리 그룹으로 이동하지 않습니다. 마법사가 작업을 완료하면 관리 그룹에 기기를 수동으로 추가할 수 있습니다.

관리 그룹의 구조를 자동으로 만들려면 다음과 같이 하십시오:

1. **관리 중인 기기** 폴더를 콘솔 트리에서 선택합니다.
2. **관리 중인 기기** 폴더의 마우스 오른쪽 메뉴에서 **모든 작업 → 새 그룹 조직도**를 선택합니다.

   새 관리 그룹 구조 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

관리 그룹에 있는 기기에 애플리케이션 자동 설치

관리 그룹의 클라이언트 기기에 Kaspersky 애플리케이션을 자동 원격 설치하는 데 사용할 설치 패키지를 지정할 수 있습니다.

관리 그룹의 기기에서 애플리케이션의 자동 설치를 구성하려면:

1. 콘솔 트리에서 필요한 관리 그룹을 선택합니다.
2. 이 관리 그룹의 속성 창을 엽니다.

3. **섹션** 창에서 **자동 설치**를 선택하고 작업 영역에서 기기에 설치할 애플리케이션의 설치 패키지를 선택합니다.

4. **확인**를 누릅니다.

그룹 작업이 생성됩니다. 이러한 작업은 관리 그룹에 추가되는 즉시 클라이언트 기기에서 실행됩니다.

한 애플리케이션의 일부 설치 패키지가 자동 설치로 선택된 경우 설치 작업은 가장 최근 애플리케이션 버전을 대상으로만 생성됩니다.

클라이언트 기기 관리

이 섹션에는 클라이언트 기기 작업에 대한 정보가 포함되어 있습니다.

클라이언트 기기를 중앙 관리 서버에 연결

클라이언트 기기를 중앙 관리 서버에 연결할 때는 기기에 설치된 네트워크 에이전트를 사용합니다.

클라이언트 기기를 중앙 관리 서버에 연결하면 다음 작업이 수행됩니다:

- 자동 데이터 동기화:
  - 클라이언트 기기에 설치된 애플리케이션 목록 동기화.
  - 정책, 애플리케이션 설정, 작업 및 작업 설정 동기화.
- 애플리케이션 상태, 작업 실행 및 중앙 관리 서버별 애플리케이션 작동 통계에 관한 최신 정보 검색.
- 중앙 관리 서버에서 처리하도록 이벤트 정보 전달.

자동 데이터 동기화는 네트워크 에이전트 설정에 따라 주기적으로 수행됩니다(예:15분마다). 동기화 간격은 수동으로 지정할 수 있습니다.

이벤트에 관한 정보는 발생하는 즉시 중앙 관리 서버로 전달됩니다.

중앙 관리 서버가 회사 네트워크 외부에 위치하는 원격 서버인 경우 클라이언트 기기가 인터넷을 통해 중앙 관리 서버에 연결할 수 있습니다.

인터넷을 통해 기기를 중앙 관리 서버에 연결하려면 다음 조건을 충족해야 합니다:

- 원격 중앙 관리 서버는 외부 IP 주소를 가지고 있어야 하며 TCP 13000 포트가 수신되도록 열려 있어야 합니다(네트워크 에이전트 연결 용도). UDP 13000 포트도 열어 놓기를 권장합니다(기기 종료 알림 수신 용도).
- 네트워크 에이전트를 먼저 기기에 설치해야 합니다.

- 기기에 네트워크 에이전트를 설치할 때 원격 중앙 관리 서버의 외부 IP 주소를 지정해야 합니다. 설치 패키지를 사용하여 설치하는 경우 이 설치 패키지에 대한 속성의 **설정** 섹션에서 외부 IP 주소를 수동으로 지정합니다.

- 원격 중앙 관리 서버를 사용하여 기기의 애플리케이션 및 작업을 관리하려면 **일반** 섹션에 있는 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택해야 합니다. 확인란을 선택한 후 중앙 관리 서버가 원격 기기와 동기화될 때까지 기다립니다. 중앙 관리 서버와 지속적인 연결을 유지하는 클라이언트 기기의 수는 300대를 초과할 수 없습니다.

원격 중앙 관리 서버를 통해 시작되는 작업의 성능을 향상시키기 위해 기기에서 15000 포트를 열 수 있습니다. 이 경우, 작업을 실행하기 위해 기기와의 동기화가 완료될 때까지 기다리지 않고 중앙 관리 서버에서 15000 포트를 통해 네트워크 에이전트에 특수 패킷을 전송합니다.

모든 작업이 완료된 후에도 연결 상태가 유지되도록 Kaspersky Security Center에서 클라이언트 기기와 중앙 관리 서버 사이의 연결을 구성할 수 있습니다. 애플리케이션 상태를 실시간으로 모니터링해야 하고 어떤 이유(예: 연결이 방화벽으로 보호됨, 기기에서 포트를 열 수 없음, 클라이언트 기기의 IP 주소를 알 수 없음 등)로 인해 중앙 관리 서버에서 클라이언트로 연결을 설정할 수 없는 경우에 대비하여 중단 없는 연결은 반드시 필요합니다. **일반** 섹션의 기기 속성 창에서 클라이언트 기기와 중앙 관리 서버 간에 연결을 항상 유지하도록 설정할 수 있습니다.

가장 중요한 기기에 대해서만 연결을 항상 유지하도록 설정할 것을 권장합니다. 중앙 관리 서버에 의해 동시에 관리되는 총 연결의 개수는 300개로 제한되어 있습니다.

수동으로 동기화하는 경우, 시스템은 보조 연결 방법을 사용하며 중앙 관리 서버에서 해당 방법으로 연결을 시작합니다. 클라이언트 기기에서 연결을 확립하기 전에 사용자는 UDP 포트를 열어야 합니다. 중앙 관리 서버에서 클라이언트 기기의 UDP 포트로 연결 요청을 보냅니다. 그러면, 중앙 관리 서버의 인증서가 확인됩니다. 중앙 관리 서버 인증서가 클라이언트 기기에 저장된 인증서 사본과 일치할 경우 연결 수립이 시작됩니다.

애플리케이션 상태, 작업 실행 및 애플리케이션의 작동 통계에 관한 최신 정보를 얻기 위해 동기화를 수동으로 실행할 수도 있습니다.

클라이언트 기기를 중앙 관리 서버에 수동으로 연결. Klmover 유틸리티

클라이언트 기기를 중앙 관리 서버에 수동으로 연결해야 한다면, 해당 기기에서 klmover 유틸리티를 사용하면 됩니다.

클라이언트 기기에 네트워크 에이전트를 설치할 때 이 유틸리티가 네트워크 에이전트 설치 폴더에 자동으로 복사됩니다.

klmover 유틸리티를 사용하여 클라이언트 기기를 중앙 관리 서버에 수동으로 연결하려면 다음과 같이 하십시오:

기기의 명령줄에서 klmover 유틸리티를 시작합니다.

명령줄에서 시작할 때 klmover 유틸리티는 다음 처리(사용 중인 라이센스 키에 따라 다름)를 수행할 수 있습니다:

- 지정된 설정을 사용하여 네트워크 에이전트를 중앙 관리 서버에 연결합니다;

- 작업 결과를 이벤트 로그 파일에 기록하거나 화면에 표시합니다.

연결 게이트웨이를 통해 중앙 관리 서버에 연결된 클라이언트 기기에는 klmover 유틸리티를 사용할 수 없습니다. 이러한 기기는 네트워크 에이전트를 재구성하거나 네트워크 에이전트를 다시 설치하고 연결 게이트웨이를 지정해야 합니다.

유틸리티 명령줄 구문:

```
klmover [-logfile <파일 이름>] [-address <서버 주소>] [-pn <포트 번호>] [-ps <SSL 포트 번호>] [-nossl] [-cert <인증서 파일 경로>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

유틸리티를 실행하려면 관리자 권한이 필요합니다.

키에 대한 설명:

- `-logfile <파일 이름>` - 유틸리티 실행 결과를 로그 파일에 기록합니다.

  기본적으로 정보는 표준 출력 스트림(stdout)에 저장됩니다. 라이센스 키를 사용 중이지 않은 경우, 화면에 결과와 함께 오류 메시지가 표시됩니다.

- `-address <서버 주소>` - 연결할 중앙 관리 서버의 주소입니다.

  IP 주소, 기기의 NetBIOS 이름 또는 DNS 이름을 그 주소로 지정할 수 있습니다.

- `-pn <포트 번호>` - 중앙 관리 서버에 대한 암호화되지 않은 연결을 설정하는 데 사용되는 포트 번호입니다.

  기본 포트 번호는 14000입니다.

- `-ps <SSL 포트 번호>` - SSL을 사용하여 중앙 관리 서버에 대한 암호화된 연결을 설정하는 데 사용되는 SSL 포트 번호입니다.

  기본 포트 번호는 13000입니다.

- `-nossl` - 중앙 관리 서버에 암호화되지 않은 연결을 사용합니다.

  라이센스 키를 사용 중이지 않은 경우, 네트워크 에이전트는 암호화된 SSL 프로토콜을 사용해 중앙 관리 서버에 연결됩니다.

- `-cert <인증서 파일 경로>` - 중앙 관리 서버에 대한 접근을 인증하기 위해 지정된 인증서 파일을 사용합니다.

  라이센스 키를 사용 중이지 않은 경우, 네트워크 에이전트는 처음 중앙 관리 서버에 연결할 때 인증서를 수신합니다.

- `-silent` - 유틸리티를 숨김 모드로 실행합니다.

  라이센스 키를 사용하면 사용자 등록 시 로그온 스크립트에서 유틸리티가 시작되는 경우 등에 유용할 수 있습니다.

- `-dupfix` - 일반적인 방법(배포 패키지 사용)과 다른 방법(예: ISO 디스크 이미지에서 네트워크 에이전트 복구)으로 네트워크 에이전트가 설치된 경우 라이센스 키가 사용됩니다.

- `-virtserv`—가상 중앙 관리 서버 이름.

- `-cloningmode`—네트워크 에이전트 디스크 복제 모드.

  다음 매개변수 중 하나를 사용하여 디스크 복제 모드를 구성합니다:

  - `-cloningmode` –디스크 복제 모드의 상태를 요청합니다.
  - `-cloningmode 1` –디스크 복제 모드를 활성화합니다.
  - `-cloningmode 0` –디스크 복제 모드를 비활성화합니다.

- `-nauninstpwd <암호>` - 이 키는 네트워크 에이전트 제거 암호를 지정하는 데 사용합니다.

  이 키는 필수 사항이 아닙니다.

예를 들어, 네트워크 에이전트를 중앙 관리 서버에 연결하려면 다음 명령을 실행합니다:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

클라이언트 기기와 중앙 관리 서버 간 연결 터널링

Kaspersky Security Center에서는 중앙 관리 서버를 통해 관리 콘솔에서, 그리고 네트워크 에이전트를 통해 관리 중인 기기의 지정된 포트로 TCP 연결을 터널링할 수 있습니다. 터널링은 관리 콘솔과 대상 기기를 직접 연결할 수 없는 경우 기기의 클라이언트 애플리케이션을 관리 중인 기기의 TCP 포트에 설치된 관리 콘솔과 연결하는 데 사용됩니다.

예를 들어 기존 세션에 연결하고 새 원격 세션을 만들기 위한 용도로 원격 데스크톱에 연결하는 데 터널링을 사용할 수 있습니다.

외부 도구를 사용하여 터널링을 작동시킬 수도 있습니다. 예를 들어 관리자는 putty 유틸리티, VNC 클라이언트 및 기타 도구를 이러한 방식으로 실행할 수 있습니다.

원격 클라이언트 기기에 중앙 관리 서버와의 연결에 사용하는 포트가 제공되지 않을 경우 클라이언트 기기와 중앙 관리 서버 간 연결 터널링이 필요합니다. 다음과 같은 경우 기기의 포트를 사용하지 못할 수 있습니다:

- 원격 기기가 NAT 메커니즘을 사용하는 네트워크에 연결되어 있습니다.
- 원격 기기는 중앙 관리 서버와 같은 로컬 네트워크에 속하지만 해당 포트가 방화벽에 의해 닫혀 있습니다.

클라이언트 기기와 중앙 관리 서버 간 연결을 터널링하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 클라이언트 기기가 있는 관리 그룹을 선택합니다.
2. **기기** 탭에서 기기를 선택합니다.
3. 기기의 마우스 오른쪽 메뉴에서 **모든 작업 → 연결 터널링**을 선택합니다.
4. **연결 터널링** 창이 열리면 터널을 만듭니다.

클라이언트 기기 데스크톱에 원격 연결

관리자는 클라이언트 기기에 설치된 네트워크 에이전트를 통해 기기 데스크톱에 원격으로 접근할 수 있습니다.

클라이언트 기기의 TCP 및 UDP 포트가 폐쇄된 경우에도 네트워크 에이전트를 통해 기기에 원격으로 연결할 수 있습니다. 기기와 연결을 설정하면 관리자는 해당 컴퓨터에 저장된 정보에 대한 완전한 접근 권한을 얻어 컴퓨터에 설치된 애플리케이션을 관리할 수 있습니다.

이 섹션에서는 네트워크 에이전트를 통해 Windows 클라이언트 기기 및 macOS 클라이언트 기기에 대한 연결을 설정하는 방법을 설명합니다.

Windows 클라이언트 기기에 연결

다음 방법 중 하나를 통해 Windows 클라이언트 기기와의 원격 연결을 설정할 수 있습니다:

- 표준 Microsoft Windows 구성 요소인 원격 데스크톱 프로토콜 사용.

  원격 데스크톱에 대한 연결은 표준 Windows 유틸리티 mstsc.exe를 통해 해당 유틸리티에 대해 정의된 설정에 따라 이루어집니다.

- Windows 데스크톱 공유 기술 사용.

원격 데스크톱 연결을 사용하여 Windows 클라이언트 기기에 연결

사용자의 현재 원격 데스크톱 세션으로의 연결은 사용자의 인지없이 연결되었습니다. 일단 관리자가 세션에 연결하면, 기기 사용자는 추가 알림 없이 세션에서 연결이 끊깁니다.

원격 데스크톱 연결 구성 요소를 사용해서 클라이언트 기기 데스크톱에 원격으로 접속하려면 다음과 같이 하십시오:

1. 관리 콘솔 트리에서 원격으로 접속할 기기를 선택합니다.
2. 기기의 마우스 오른쪽 메뉴에서 **모든 작업 → 기기에 연결 → 새 RDP 세션**을 선택합니다.

   그러면 표준 Windows 유틸리티 mstsc.exe가 실행되어 원격 데스크톱에 대한 연결이 설정됩니다.
3. 유틸리티 대화 상자에 표시된 지침을 따릅니다.

기기에 연결된 후에는 Microsoft Windows의 원격 연결 창에서 해당 데스크톱을 사용할 수 있습니다.

Windows 데스크톱 공유를 통한 Windows 클라이언트 기기 연결

현재 활성화된 원격 데스크톱 세션에 연결하는 경우 해당 기기의 세션 사용자가 관리자로부터 연결 요청을 받게 됩니다. 기기의 원격 활동과 활동 결과는 Kaspersky Security Center에 의해 생성된 리포트에 저장되지 않습니다.

관리자는 세션을 운영 중인 사용자의 연결을 끊지 않고도 클라이언트 기기의 현재 세션에 연결할 수 있습니다. 이 경우 관리자와 기기의 세션 사용자가 데스크톱에 대한 접근을 공유하게 됩니다.

관리자가 원격 클라이언트 기기에서의 사용자 활동을 감사하도록 구성할 수 있습니다. 감사 중에 애플리케이션은 클라이언트 기기에서 관리자가 열거나 수정한 파일에 대한 정보를 저장합니다.

Windows 데스크톱 공유를 통해 클라이언트 기기의 데스크톱에 연결하려면 다음 조건이 충족되어야 합니다.

- 관리자 워크스테이션에 Microsoft Windows Vista 이상 버전이 설치되어 있어야 합니다. 중앙 관리 서버를 운영하는 기기의 운영 체제 유형이 Windows 데스크톱 공유를 사용한 연결을 제한하지 않아야 합니다.

  사용자의 Windows 에디션이 Windows 데스크톱 공유 기능을 포함하는지 확인하려면 Windows 레지스트리에 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 키가 있는지 확인하십시오.
- 클라이언트 기기에 Microsoft Windows Vista 이상 버전이 설치되어 있어야 합니다.
- Kaspersky Security Center는 취약점 및 패치 관리용 라이센스를 사용합니다.

Windows 데스크톱 공유 기술을 통해 클라이언트 기기의 데스크톱으로 연결하려면 다음과 같이 하십시오:

1. 관리 콘솔 트리에서 원격으로 접속할 기기를 선택합니다.
2. 기기의 컨텍스트 메뉴에서 **모든 작업** → **기기에 연결** → **Windows Desktop Sharing**를 선택합니다.
3. **원격 데스크톱 세션 선택** 창이 열리면 연결할 기기의 세션을 선택합니다.
   기기로 연결이 완료되면, 해당 기기의 바탕 화면을 **Kaspersky 원격 데스크톱 세션 뷰어** 창에서 이용 가능합니다.
4. 기기와의 상호 작용을 시작하려면 **Kaspersky 원격 데스크톱 세션 뷰어** 창의 메인 메뉴에서 **작업** → **대화식 모드**를 선택합니다.

Kaspersky 원격 데스크톱 세션 뷰어 유틸리티를 사용하려면 상업용 라이센스가 필요합니다.

macOS 클라이언트 기기에 연결

관리자는 VNC(Virtual Network Computing) 시스템을 사용하여 macOS 기기에 연결할 수 있습니다.

중앙 관리 서버 기기에 설치된 VNC 클라이언트를 통해 원격 데스크톱에 대한 연결이 설정됩니다. VNC 클라이언트는 키보드 및 마우스 제어를 클라이언트 기기에서 관리자로 전환합니다.

관리자가 원격 데스크톱에 연결할 때 사용자는 관리자로부터 알림이나 연결 요청을 받지 않습니다. 관리자는 이 세션에서 사용자의 연결을 유지한 채로 클라이언트 기기의 현재 세션에 연결할 수 있습니다.

VNC 클라이언트를 통해 클라이언트 macOS 기기의 데스크톱에 연결하려면 다음 조건을 충족해야 합니다:

- VNC 클라이언트는 중앙 관리 서버 기기에 설치됩니다.
- 클라이언트 기기에서 원격 로그인 및 원격 관리가 허용됩니다.
- 사용자가 macOS 운영 체제의 **공유** 설정에서 클라이언트 기기에 대한 관리자 액세스를 허용했습니다.

가상 네트워크 컴퓨팅 시스템을 통해 클라이언트 기기 데스크톱에 연결하려면:

1. 관리 콘솔 트리에서 원격으로 접속할 기기를 선택합니다.
2. 기기의 마우스 오른쪽 메뉴에서 **모든 작업** → **연결 터널링**을 선택합니다.
3. **연결 터널링** 창이 열리면 다음을 수행합니다:
   a. **1. 네트워크 포트** 섹션에서 연결해야 하는 기기의 네트워크 포트 번호를 지정합니다.
      기본적으로 포트 5900이 사용됩니다.
   b. **2. 터널링** 섹션에서 **터널 생성** 버튼을 클릭합니다.
   c. **3. 네트워크 설정** 섹션에서 **복사** 버튼을 클릭합니다.
4. VNC 클라이언트를 열고 복사한 네트워크 속성을 텍스트 필드에 붙여넣습니다. **Enter** 키를 누릅니다.

5. 창이 열리면 인증서 세부 정보를 확인합니다. 인증서 사용에 동의하면 **예** 버튼을 클릭합니다.

6. **인증** 창에서 클라이언트 기기의 자격 증명을 지정한 다음 **확인**을 클릭합니다.

Windows 데스크톱 공유를 통해 기기에 연결

Windows 데스크톱 공유를 통해 기기에 연결하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **기기** 탭에서 **관리 중인 기기** 폴더를 선택합니다.
   이 폴더의 작업 영역에 기기 목록이 표시됩니다.

2. 연결하려는 기기의 마우스 오른쪽 메뉴에서 **기기에 연결** → **Windows Desktop Sharing**을 선택합니다.
   원격 데스크톱 세션 선택 창이 열립니다.

3. **원격 데스크톱 세션 선택** 창에서 기기로의 연결에 대한 데스크톱 세션을 선택합니다.

4. **확인**을 누릅니다.

기기가 연결되었습니다.

클라이언트 기기 다시 시작 구성

Kaspersky Security Center 사용, 설치 또는 제거 시 기기를 다시 시작해야 합니다. Windows를 실행 중인 기기에서만 다시 시작 설정을 지정할 수 있습니다.

클라이언트 기기 다시 시작을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 재시작을 구성해야 하는 관리 그룹을 선택합니다.

2. 그룹의 작업 영역에서 **정책** 탭을 선택합니다.

3. 작업 영역 내 정책 목록에서 Kaspersky Security Center 네트워크 에이전트의 정책을 선택하고 해당 정책의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

4. 정책 속성 창에서 **관리 다시 시작** 섹션을 선택합니다.

5. 기기를 다시 시작해야 하는 경우 수행해야 하는 작업을 선택합니다:

   - 자동 다시 시작을 차단하려면 **운영 체제 다시 시작 안 함**을 선택합니다.
   - 자동 다시 시작을 허용하려면 **필요한 경우 운영 체제를 자동으로 다시 시작**를 선택합니다.
   - 사용자에게 운영 체제 다시 시작을 허용할지 묻도록 설정하려면 **사용자 확인 후 처리**을 선택합니다.

   해당하는 확인란 및 시간 설정을 선택하여 다시 시작 요청 빈도를 지정하고 기기의 차단된 세션에서 애플리케이션 강제 다시 시작 및 강제 닫기를 사용할 수 있습니다.

6. **확인**를 눌러 변경 사항을 저장하고 정책 속성 창을 닫습니다.

이제 기기를 다시 시작하는 작업이 구성됩니다.

원격 클라이언트 기기에서의 활동 감사

애플리케이션은 Windows 운영 체제를 사용하는 원격 클라이언트 기기에서의 관리자 활동을 감사합니다. 감사 중에 애플리케이션은 기기에서 관리자가 열거나 수정한 파일에 대한 정보를 저장합니다. 다음 조건이 충족되면 관리자 작업 감사를 사용할 수 있습니다:

- 취약점 및 패치 관리 라이센스를 사용 중.
- 관리자에게 원격 기기의 데스크톱에 대한 공유 접근 시작 권한이 있는 경우.

원격 클라이언트 기기에서의 활동을 감사하려면, 다음과 같이 하십시오:

1. 콘솔 트리에서 관리자 작업 감사를 구성해야 하는 관리 그룹을 선택합니다.
2. 그룹의 작업 영역에서 **정책** 탭을 선택합니다.
3. Kaspersky Security Center 네트워크 에이전트의 정책을 선택하고 해당 정책의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
4. 정책 속성 창에서 **Windows Desktop Sharing** 섹션을 선택합니다.
5. **감사 기능 사용** 확인란을 선택합니다.
6. **읽을 때 모니터링해야 하는 파일 마스크** 및 **변경될 때 모니터링해야 하는 파일 마스크** 목록에서 감사 중에 애플리케이션이 작업을 모니터링할 때 사용할 파일 마스크를 추가합니다.

   기본적으로 애플리케이션은 확장자가 .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt, .pdf인 파일에 대한 작업을 모니터링합니다.
7. **확인**를 눌러 변경 사항을 저장하고 정책 속성 창을 닫습니다.

그러면 원격 접속 시 사용자의 원격 기기에 대한 관리자 활동 감사가 구성됩니다.

원격 기기의 관리자 활동 기록은 다음 위치에 저장됩니다:

- 원격 기기의 이벤트 로그에 저장.
- 원격 기기의 네트워크 에이전트 폴더에 있는 syslog 확장자를 가진 파일에 저장(예, C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- Kaspersky Security Center의 이벤트 데이터베이스.

클라이언트 기기와 중앙 관리 서버 간 연결 상태 확인

Kaspersky Security Center에서는 클라이언트 기기와 중앙 관리 서버 간 연결을 자동 또는 수동으로 확인할 수 있습니다.

연결 자동 확인은 중앙 관리 서버에서 수행됩니다. 연결 수동 확인은 기기에서 수행됩니다.

클라이언트 기기와 중앙 관리 서버 간 연결 상태 자동 확인

클라이언트 기기와 중앙 관리 서버 간 연결 자동 확인을 시작하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 기기가 포함된 관리 그룹을 선택합니다.
2. 관리 그룹의 작업 영역에 있는 **기기** 탭에서 기기를 선택합니다.
3. 기기의 컨텍스트 메뉴에서 **기기 연결 가능성 확인**을 선택합니다.

기기의 연결 가능성에 대한 정보가 있는 창이 열립니다.

클라이언트 기기와 중앙 관리 서버 간 연결 상태 수동 확인. Klnagchk 유틸리티

klnagchk 유틸리티를 사용하여 클라이언트 기기와 중앙 관리 서버 사이의 연결 상태를 확인하고 연결 설정에 대한 자세한 정보를 볼 수 있습니다. klnagchk 유틸리티는 네트워크 에이전트 설치 폴더에 위치해 있습니다.

명령줄에서 시작할 때 klnagchk 유틸리티는 다음 처리(사용 중인 라이센스 키에 따라 다름)를 수행할 수 있습니다:

- 기기에 설치된 네트워크 에이전트와 중앙 관리 서버를 연결하는 데 사용하는 설정 값을 화면에 표시하거나 기록합니다.
- 네트워크 에이전트 통계(마지막 시작 이후의 통계 정보)와 유틸리티 작업 결과를 이벤트 로그 파일에 기록하거나 이 정보를 화면에 표시합니다.
- 네트워크 에이전트와 중앙 관리 서버의 연결을 시도합니다.

  연결에 실패하면 유틸리티가 ICMP 패킷을 전송하여 중앙 관리 서버가 설치된 기기의 상태를 확인합니다.

klnagchk 유틸리티를 사용하여 클라이언트 기기와 중앙 관리 서버 사이의 연결 상태를 확인하려면 다음과 같이 하십시오.

네트워크 에이전트가 설치된 기기에서 로컬 관리자 계정으로 명령줄을 사용해 klnagchk 유틸리티를 시작합니다.

유틸리티 명령줄 구문:

```
klnagchk [-logfile <파일 이름>] [-sp] [-savecert <인증서 파일 경로>] [-restart][-sendhb]
```

키에 대한 설명:

- `-logfile <파일 이름>` - 네트워크 에이전트와 중앙 관리 서버 사이의 연결 상태 값 및 유틸리티 작업 결과를 로그 파일에 기록합니다.

  기본적으로 정보는 표준 출력 스트림(stdout)에 저장됩니다. 라이센스 키를 사용 중이지 않은 경우, 화면에 설정 및 결과와 함께 오류 메시지가 표시됩니다.

- `-sp` - 프록시 서버에서 사용자 인증을 위한 암호를 표시합니다.

  프록시 서버를 통해 중앙 관리 서버에 연결했다면 이 키가 사용 중입니다.

- `-savecert <파일 이름>` - 지정된 파일에 중앙 관리 서버의 접근에 사용되는 인증서를 저장합니다.

- `-restart` - 유틸리티 작업이 완료된 후 네트워크 에이전트를 다시 시작합니다.
- `-sendhb` - 네트워크 에이전트와 중앙 관리 서버의 동기화를 시작합니다.

시작 후, klnagchk 유틸리티는 네트워크 에이전트의 구성 파일에 접근하고 연결 파라미터를 표시합니다. 이러한 매개변수는 네트워크 에이전트를 설치하는 동안 네트워크 에이전트 정책 설정에서 지정합니다.

- `Current device` - 클라이언트 기기의 Windows 네트워크 이름입니다.
- `Network Agent version` - 기기에 설치된 네트워크 에이전트 버전의 전체 번호입니다(패치 포함).
- `Administration Server address` - 중앙 관리 서버의 주소입니다.
- `Use SSL` - 중앙 관리 서버에 연결할 때 보안 연결 사용 여부를 나타내는 파라미터.
  가능한 값:
  - 0 - 보안 연결을 사용하지 않습니다.
  - 1 - 보안 연결이 사용됩니다.
- `Compress traffic` - 클라이언트 기기와 중앙 관리 서버 간의 트래픽 압축 여부를 나타내는 파라미터.
- `Numbers of the Administration Server SSL ports` - 보안 연결을 사용할 때 중앙 관리 서버와의 통신에 유효한 포트 수.
- `Numbers of the Administration Server ports` - 일반 연결을 사용할 때 중앙 관리 서버와의 통신에 유효한 포트 수.
- `Use proxy server` - 프록시 서버의 사용 여부를 나타내는 파라미터.
  가능한 값:
  - 0 - 프록시 서버를 사용하지 않습니다.
  - 1 - 프록시 서버가 사용됩니다.
- `Address` - 프록시 서버의 주소 및 포트로, 콜론으로 구분합니다. 이 매개변수는 프록시 서버를 사용할 때만 표시됩니다.
- `User name` - 프록시 서버에 접근하기 위한 사용자 이름입니다. 이 매개변수는 프록시 서버를 사용할 때만 표시됩니다.
- `Password` - 프록시 서버에 접근하기 위한 암호입니다. 이 매개변수는 프록시 서버를 사용할 때만 표시됩니다. 프록시 서버 암호를 표시하려면 명령에서 `sp` 키를 사용해야 합니다.
- `Administration Server certificate` - 클라이언트 기기에 중앙 관리 서버 인증서가 있는지를 나타내는 파라미터입니다. 예를 들어 네트워크 에이전트가 중앙 관리 서버에 성공적으로 연결한 적이 없다면 인증서가 없을 수 있습니다.
  가능한 값:
  - `not installed` - 클라이언트 기기에 중앙 관리 서버 인증서가 없습니다.
  - `available` - 클라이언트 기기에 중앙 관리 서버 인증서가 있습니다.

- `Open UDP port` - 네트워크 에이전트가 중앙 관리 서버의 동기화 요청을 수신하기 위해 UDP 포트 사용 여부를 나타내는 파라미터입니다.

  가능한 값:

  - `0` - 중앙 관리 서버의 동기화 요청 수신을 위한 UDP 포트가 닫힙니다.
  - `1` - 중앙 관리 서버의 동기화 요청을 수신하기 위한 UDP 포트가 열립니다.

- `Numbers of UDP ports` - 네트워크 에이전트에서 사용할 수 있는 UDP 포트의 수입니다.
- `Location name` - 기기의 네트워크 위치입니다.
- `State of network location` - 클라이언트 기기를 중앙 관리 서버 연결 프로필에서 다른 프로필로 전환 여부를 나타내는 파라미터입니다.

  가능한 값:

  - `Enabled` - 클라이언트 기기에서 중앙 관리 서버 연결 프로필을 전환할 수 있습니다.
  - `Disabled` - 클라이언트 기기에서 중앙 관리 서버 연결 프로필을 전환할 수 없습니다.

- `Profile to use` - 중앙 관리 서버용 연결 프로필입니다.
- `Condition` - 클라이언트 기기가 연결된 네트워크의 IP 주소 및 서브넷 마스크입니다.
- `Synchronization interval (min)` - 동기화 간의 표준 간격입니다.
- `Connection timeout (in seconds)` - 연결 시간 초과입니다.
- `Send / receive timeout (in seconds)` - 읽기-쓰기 작업의 연결 시간 초과입니다.
- `Device ID` - 네트워크에 있는 기기 식별자입니다. `Device ID`는 특정 중앙 관리 서버에서 관리하는 다른 클라이언트 기기와 구별됩니다.
- `Locations of connection gateways` - 연결 게이트웨이를 통해 클라이언트 기기를 중앙 관리 서버에 연결하기 위한 파라미터입니다.
- `Location of distribution points` - 배포 지점을 통해 클라이언트 기기를 중앙 관리 서버에 연결하기 위한 파라미터입니다.
- `Connection with server` - 연결 게이트웨이가 중앙 관리 서버에 계속 연결되어 있는지를 나타내는 파라미터입니다. 이 파라미터는 클라이언트 기기가 연결 게이트웨이로 작동할 때만 표시됩니다.

  가능한 값:

  - `active` - 연결 게이트웨이가 중앙 관리 서버에 계속 연결되어 있습니다.
  - `inactive` - 연결 게이트웨이가 중앙 관리 서버에 계속 연결되어 있지 않습니다.

- `Connection with server through connection gateway` - 연결 게이트웨이를 통한 중앙 관리 서버와의 연결이 올바르게 설정되었는지를 나타내는 파라미터입니다. 이 파라미터는 클라이언트 기기가 연결 게이트웨이로 작동할 때만 표시됩니다.

가능한 값:

- `active` - 연결 게이트웨이를 통한 중앙 관리 서버와의 연결이 올바르게 설정되었습니다.
- `inactive` - 연결 게이트웨이를 통한 중앙 관리 서버로의 연결이 잘못 설정되었습니다.

또한 klnagchk 유틸리티 출력에는 다음 행 중 하나가 포함될 수 있습니다.

- `Administration Server is installed on this device` - klnagchk 유틸리티가 중앙 관리 서버 기기에서 실행됩니다.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` - 네트워크 에이전트가 설치된 기기에서 klnagchk 유틸리티가 연결 게이트웨이 모드로 실행됩니다. 구성된 연결 게이트웨이가 중앙 관리 서버의 연결을 기다리고 있지만 기기가 관리 중인 기기로 나열되지 않습니다. 중앙 관리 서버가 연결 게이트웨이로의 연결을 초기화하도록 해야 합니다.
- `This device is a connection gateway` - 연결 게이트웨이로 작동하는 기기에서 klnagchk 유틸리티가 실행됩니다.
- `Acts as a distribution point` - 배포 지점으로 작동하는 기기에서 klnagchk 유틸리티가 실행됩니다.

klnagchk 유틸리티가 네트워크 에이전트 서비스 상태를 확인합니다. 서비스가 실행 중이 아니라면 유틸리티가 중지됩니다. 서비스가 실행 중이라면 이 유틸리티는 다음과 같은 연결 통계를 표시합니다.

- `Total number of synchronization requests` - 클라이언트 기기를 중앙 관리 서버에 연결하려는 시도 횟수입니다.
- `The number of successful synchronization request` - 클라이언트 기기와 중앙 관리 서버의 연결을 성공한 횟수입니다.
- `Total number of synchronizations` - 클라이언트 기기 설정과 중앙 관리 서버 설정의 동기화를 시도한 횟수입니다.
- `The number of successful synchronizations` - 클라이언트 기기 설정과 중앙 관리 서버의 동기화를 성공적으로 시도한 횟수입니다.
- `Date/time of the last request for synchronization` - 마지막으로 연결한 날짜와 시간입니다.

중앙 관리 서버와 네트워크 에이전트 간의 연결을 분석할 때는 `Total number of synchronization requests`와 `The number of successful synchronization request` 파라미터를 사용해야 합니다. 클라이언트 기기 설정은 중앙 관리 서버 설정을 변경했을 때만(예: 새 작업 추가 또는 정책 설정 수정) 중앙 관리 서버 설정과 동기화됩니다. 그렇지 않으면, `Total number of synchronizations` 및 `The number of successful synchronizations` 파라미터값이 변경되지 않습니다.

네트워크 에이전트와 중앙 관리 서버 연결 시 발생하는 문제를 해결하는 방법에 대한 자세한 내용은 Kaspersky Security Center FAQ를 참조하십시오.

기기와 중앙 관리 서버 간 연결 시간 확인 정보

기기를 종료하면 네트워크 에이전트가 중앙 관리 서버에 해당 이벤트를 알립니다. 관리 콘솔에서는 해당 기기가 종료된 것으로 표시됩니다. 그러나 네트워크 에이전트가 이러한 모든 이벤트를 중앙 관리 서버에 알릴 수는 없습니다. 따라서 중앙 관리 서버는 각 기기의 **중앙 관리 서버에 연결** 특성(이 특성의 값은 관리 콘솔의 기기 속성 **일반** 섹션에 표시됨)을 주기적으로 분석하여 네트워크 에이전트 현재 설정의 동기화 간격과 비교합니다. 연속하는 4회 이상의 동기화 간격 동안 응답하지 않은 기기는 종료된 것으로 표시됩니다.

중앙 관리 서버에서 클라이언트 기기 식별

클라이언트 기기는 이름으로 식별됩니다. 기기 이름은 중앙 관리 서버에 연결된 다른 모든 기기의 이름과 구별됩니다.

기기 이름은 Windows 네트워크가 검색되고 여기서 새 기기가 발견될 때, 또는 기기에 설치된 네트워크 에이전트가 중앙 관리 서버에 처음으로 연결될 때 중앙 관리 서버로 전송됩니다. 기본적으로 해당 이름은 Windows 네트워크에서의 기기 이름과 일치합니다(NetBIOS 이름). 같은 이름의 기기가 중앙 관리 서버에 이미 등록되어 있는 경우, 새 기기 이름에 순차적으로 숫자 색인이 추가됩니다. 예: **<이름>-1**, **<이름>-2**. 기기는 이 이름으로 관리 그룹에 추가됩니다.

관리 그룹로 기기 이동

소스 및 대상 관리 그룹이나 이러한 그룹이 속하는 중앙 관리 서버의 **관리 그룹 관리** 영역에서 **수정** 권한이 있을 때만 관리 그룹 간에 기기를 이동할 수 있습니다.

선택한 관리 그룹에 한 대 이상의 기기를 포함시키려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 확장합니다.
2. **관리 중인 기기** 폴더에서 클라이언트 기기를 포함할 그룹에 해당하는 하위 폴더를 선택합니다.
   관리 중인 기기 그룹에 기기를 포함시키려는 경우에는 이 단계를 건너뛸 수 있습니다.
3. 선택한 관리 그룹의 작업 영역에 있는 **기기** 탭에서 다음 방법 중 하나를 사용하여 그룹에 기기를 포함시키는 프로세스를 실행합니다:
   - 기기 목록이 있는 정보 박스에서 **그룹으로 기기 이동** 버튼을 눌러 그룹에 기기를 추가합니다
   - 기기 목록의 마우스 오른쪽 메뉴에서 **생성 → 기기**를 선택합니다

   기기 이동 마법사가 시작됩니다. 마법사의 지침에 따라 그룹에 기기를 이동할 방법을 선택하고 그룹에 포함시킬 기기 목록을 만듭니다.

   수동으로 기기 목록을 만들면 기기 주소로 IP 주소(또는 IP 범위), NetBIOS 이름 또는 DNS 이름을 사용할 수 있습니다. 기기에 연결할 때 또는 기기 발견 이후에 중앙 관리 서버 데이터베이스에 이미 정보가 이동된 기기만 수동으로 목록에 추가할 수 있습니다.

   기기 목록을 파일에서 가져오려면 추가할 기기 주소 목록이 포함된 TXT파일을 지정합니다. 주소는 각각 다른 줄에 지정해야 합니다.

마법사를 마치면 선택한 기기가 관리 그룹에 포함되고, 기기 목록에서 중앙 관리 서버에 의해 생성된 이름에 표시됩니다.

기기를 **미할당 기기** 폴더에서 관리 그룹의 폴더로 드래그하여 선택된 관리 그룹으로 이동할 수 있습니다.

클라이언트 기기의 중앙 관리 서버 변경

중앙 관리 서버 변경 작업을 사용하여 클라이언트 기기를 관리하는 중앙 관리 서버를 다른 서버로 변경할 수 있습니다.

클라이언트 기기를 관리하는 중앙 관리 서버를 다른 서버로 변경하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. 이 폴더의 작업 영역에서 **새 작업** 버튼을 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. 마법사의 **작업 유형 선택** 단계에서 **Kaspersky Security Center 중앙 관리 서버** 노드를 선택하고 **고급** 폴더를 확장한 다음, **중앙 관리 서버 변경** 작업을 선택합니다.
4. 열리는 창에서 **확인** 버튼을 클릭하여 클라이언트 기기에 대한 중앙 관리 서버 변경 조건에 동의함을 확인합니다.
5. 마법사의 **설정** 단계에서 선택한 기기를 관리하는 데 사용할 중앙 관리 서버를 선택합니다.

- **다른 기본 중앙 관리 서버로 변경**

  클라이언트 기기를 다른 기본 중앙 관리 서버로 이동하려면 다음 중앙 관리 서버 연결 설정을 지정합니다.

  1. **중앙 관리 서버** 필드에 새 기본 중앙 관리 서버의 주소를 지정합니다.
  2. **포트** 필드에 중앙 관리 서버에 연결할 포트 번호를 지정합니다.
     기본 포트 번호는 14000입니다.
  3. **SSL 포트** 필드에 기본 중앙 관리 서버의 SSL 포트 번호를 지정합니다.
     기본 포트 번호는 13000입니다.
  4. 필요하다면 **프록시 서버 사용** 확인란을 선택합니다.
     이 확인란을 선택 해제하면, 직접 연결을 통해 중앙 관리 서버에 기기를 연결합니다.
     이 확인란을 선택 해제하면, 프록시 서버 파라미터를 지정합니다.

     - **프록시 서버 주소**
     - **프록시 서버 포트**

     프록시 서버에 인증이 필요하다면 **사용자 이름** 및 **암호** 필드에 프록시 서버에 대한 연결이 설정된 계정의 자격 증명을 지정합니다. 프록시 서버 인증에만 필요한 최소 권한이 있는 계정의 자격 증명을 지정하는 것이 좋습니다.
  5. 필요한 경우 새로운 중앙 관리 서버 인증서를 업로드합니다.

- **이 기본 서버에서 다른 가상 서버로 변경**

  현재 기본 중앙 관리 서버의 가상 중앙 관리 서버로 클라이언트 기기를 이동하려면 이 옵션을 선택합니다. 이렇게 하려면 **가상 중앙 관리 서버 이름** 필드에 필요한 가상 중앙 관리 서버의 이름을 지정합니다.

필요하다면 네트워크 에이전트를 다시 시작하기 전의 대기 시간을 지정합니다.

6. 마법사의 이 단계에서는 작업이 할당될 기기를 선택합니다.

   - **중앙 관리 서버가 발견한 기기 중에서 선택**. 이 경우 특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.
   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**. 작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.
   - **기기 선택 결과에 작업 할당**. 이 경우 이전에 만든 조회에 포함되는 기기에 작업이 할당됩니다. 사전 정의 조회 또는 직접 생성한 사용자 지정 조회를 지정할 수 있습니다.
   - **관리 그룹에 작업 할당**. 이 경우 이전에 만든 관리 그룹에 포함된 기기 작업이 할당됩니다.

7. 마법사의 **작업을 실행할 계정 선택** 단계에서 계정 설정을 지정합니다.

   - **기본 계정**

     해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.
     기본적으로 이 옵션은 선택되어 있습니다.

   - **계정 지정**

     계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

     - **계정**

       작업 실행에 사용되는 계정입니다.

     - **암호**

       작업을 실행할 계정의 암호입니다.

8. 마법사의 **작업 스케줄 구성** 단계에서 작업 시작 스케줄을 만들 수 있습니다. 필요한 경우 다음 설정을 지정합니다:

- **시작 스케줄:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **매일(서머타임 지원 안 함)**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 이 스케줄에서는 DST(서머타임)를 준수할 수 없습니다. 즉, DST가 시작되거나 끝날 때 시간이 1시간 빨라지거나 느려져도 실제 작업 시작 시간은 변경되지 않습니다.

    이 스케줄은 사용하지 않는 것이 좋습니다. 이 스케줄은 Kaspersky Security Center 이전 버전과의 호환성을 유지하는 데 필요합니다.

    기본적으로 이 작업은 매일 현재 시스템 시간에 시작됩니다.

  - **요일별**

    이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

    기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

  - **월별**

    이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

    지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.

    기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

  - **한번만**

    작업은 지정한 날짜와 시간(기본값은 작업 생성일)에 한 번 실행됩니다.

  - **수동 시작**

    작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **즉시**

    해당 작업은 기기가 네트워크에서 표시되거나 기기가 작업 범위에 포함되는 즉시 실행됩니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

9. 마법사의 이 단계에서는 생성 중인 작업의 이름을 지정합니다.

10. 마법사의 **작업 생성 마침** 단계에서 **마침** 버튼을 눌러 마법사를 완료합니다.

    마법사가 완료되는 즉시 작업을 시작하려면 **마법사 종료 후 작업 실행** 확인란을 선택합니다.

작업이 완료되면 작업이 만들어진 클라이언트 기기가 작업 설정에 지정된 중앙 관리 서버의 관리를 받게 됩니다.

중앙 관리 서버가 암호화 및 데이터 보호를 지원하는 경우 *중앙 관리 서버 변경* 작업을 생성하면 경고가 표시됩니다. 경고의 내용은 기기에 암호화된 데이터가 저장되면 기기가 새로운 서버의 관리를 받게 된 후 사용자가 이전에 작업했던 암호화된 데이터에만 접근할 수 있다는 것입니다. 그 밖의 경우에는 암호화된 데이터에 접근할 수 없습니다. 암호화된 데이터에 대한 접근 권한이 없는 시나리오에 대한 자세한 설명은 Kaspersky Endpoint Security for Windows 도움말을 참조하십시오.

연결 게이트웨이를 통해 중앙 관리 서버에 연결된 기기를 다른 중앙 관리 서버로 이동

연결 게이트웨이를 통해 중앙 관리 서버에 연결된 기기를 다른 중앙 관리 서버로 이동할 수 있습니다. 예를 들어 기기에 다른 버전의 중앙 관리 서버를 설치하고 싶지만 시간을 들여서 네트워크 에이전트를 다시 설치하고 싶지는 않을 때 이 방법을 사용할 수 있습니다.

지침에 설명된 명령은 클라이언트 기기에서 관리자 권한이 있는 계정으로 실행해야 합니다.

연결 게이트웨이를 통해 연결된 기기를 다른 중앙 관리 서버로 이동하려면:

1. `-address <서버 주소>` 파라미터와 함께 klmover 유틸리티를 실행하여 새 중앙 관리 서버로 전환합니다.
2. `klnagchk -nagwait -tl 4` 명령을 실행합니다.
3. 다음 명령을 실행하여 새 연결 게이트웨이를 설정합니다:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<게이트웨이 IP 또는 이름>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`
     여기서 `<게이트웨이 IP 또는 이름>`은 인터넷에서 접근할 수 있는 연결 게이트웨이 주소입니다.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`
     `13000`은 연결 게이트웨이가 수신하는 TCP 포트의 번호입니다.
4. `klnagchk -restart -tl 4` 명령을 실행하여 네트워크 에이전트 서비스를 시작합니다.

기기가 새로운 중앙 관리 서버로 이동되고 새로 연결한 게이트웨이로 연결됩니다.

클러스터 및 서버 배열

Kaspersky Security Center는 클러스트 기술을 지원합니다. 네트워크 에이전트에서 클라이언트 기기에 설치된 애플리케이션이 서버 배열의 일부를 구성하는 한다는 정보를 중앙 관리 서버에 보내면 해당 기기가 클러스터 노드가 됩니다. 클러스터는 콘솔 트리의 **관리 중인 기기** 폴더에 서버 아이콘( )이 표시된 개별 개체로 추가됩니다.

클러스터의 몇몇 일반적인 특징은 다음과 같습니다:

- 클러스터와 모든 해당 노드는 항상 동일한 관리 그룹에 속합니다.
- 관리자가 클러스터 노드를 옮기려고 하면 노드는 원래 위치로 돌아갑니다.
- 관리자가 클러스터를 다른 그룹으로 옮기려고 하면 관련 모든 노드도 함께 옮겨집니다.

클라이언트 기기 원격 켜기, 끄기 및 다시 시작

Kaspersky Security Center에서는 클라이언트 기기를 원격으로 켜고 끄거나 다시 시작하여 관리할 수 있습니다.

클라이언트 기기를 원격 관리하려면 다음과 같이 하십시오:

1. 기기를 관리하는 중앙 관리 서버에 연결합니다.
2. 다음 방법 중 하나를 사용하여 기기 관리 작업을 만듭니다:
   - 선택한 관리 그룹에 포함된 기기를 켜거나 끄거나 다시 시작해야 하는 경우 선택된 그룹에 대한 작업을 만듭니다.
   - 여러 관리 그룹에 포함되어 있거나 어떤 관리 그룹에도 속하지 않은 기기를 켜거나 끄거나 다시 시작해야 하는 경우 특정 기기에 대한 작업을 만듭니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다. 새 작업 마법사의 **작업 유형 선택** 창에서 **Kaspersky Security Center** 노드를 선택하고 **고급** 폴더를 연 다음 **기기 관리** 작업을 선택합니다.
3. 만들어진 작업을 실행합니다.

   작업이 완료되면 선택된 기기에 대해 명령(켜기, 끄기 또는 다시 시작)이 실행됩니다.

관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결 사용 정보

Kaspersky Security Center에서는 기본적으로 관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결 기능이 제공되지 않습니다. 관리 중인 기기의 네트워크 에이전트는 주기적으로 연결을 설정하여 중앙 관리 서버와의 동기화를 수행합니다. 이러한 동기화 세션 간의 간격(기본값: 15분)은 네트워크 에이전트의 정책에서 정의되며 기본적으로 15분입니다. 정책을 강제 적용하려는 경우와 같이 이 간격보다 빨리 동기화해야 하는 경우에는 중앙 관리 서버가 네트워크 에이전트의 포트 UDP 15000으로 서명된 네트워크 패킷을 전송합니다. (중앙 관리 서버는 IPv4 또는 IPv6 네트워크를 통해 이 패킷을 전송할 수 있습니다.) 이유를 막론하고 중앙 관리 서버와 관리 그룹 간에 UDP를 통한 연결이 불가능한 경우에는 네트워크 에이전트와 중앙 관리 서버 간의 다음 정기 연결 시 동기화 간격 내에 동기화가 실행됩니다.

하지만 일부 작업은 네트워크 에이전트와 중앙 관리 서버 간을 미리 연결하지 않으면 수행할 수 없습니다. 로컬 작업 실행 및 중지, 관리 중인 애플리케이션에 대한 통계 수신, 터널 만들기 등의 작업이 포함됩니다. 이러한 작업을 수행하려면 관리 중인 기기에서 **중앙 관리 서버와 계속 연결 유지** 옵션을 활성화해야 합니다.

강제 동기화 정보

Kaspersky Security Center가 관리 중인 기기의 상태, 설정, 작업 및 정책을 자동으로 동기화하지만, 경우에 따라 관리자가 현재 시점에서 지정된 기기에 대해 동기화가 이미 수행되었는지를 정확히 파악해야 할 수도 있습니다.

관리 콘솔 내 관리 중인 기기의 마우스 오른쪽 메뉴에서 **모든 작업** 메뉴 항목에는 **강제 동기화** 명령이 포함되어 있습니다. Kaspersky Security Center 15.1에서 이 명령을 실행하면 중앙 관리 서버가 해당 기기에 연결을 시도합니다. 이 시도가 성공하면 강제 동기화가 수행됩니다. 그렇지 않은 경우에는 네트워크 에이전트와 중앙 관리 서버 간에 스케줄된 다음 연결 이후에만 강제 동기화가 수행됩니다.

연결 스케줄 정보

네트워크 에이전트 속성 창의 **연결성** 섹션에 있는 **연결 스케줄** 하위 섹션에서 네트워크 에이전트가 중앙 관리 서버에 데이터를 전송하는 시간 간격을 지정할 수 있습니다.

필요 시 연결. 이 옵션을 선택하면 네트워크 에이전트가 중앙 관리 서버로 데이터를 보내야 할 때 연결이 설정됩니다.

지정한 시간 간격에 연결. 이 옵션을 선택하면 네트워크 에이전트가 지정된 시간에 중앙 관리 서버와 연결됩니다. 여러 개의 연결 기간을 추가할 수 있습니다.

기기 사용자에게 메시지 보내기

기기 사용자에게 메시지를 보내려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 다음 방법 중 하나로 기기 사용자에게 메시지 발송 작업을 만듭니다:
   - 선택한 관리 그룹에 속한 클라이언트 기기의 사용자에게 메시지를 전송하려면 선택한 그룹에 대한 작업을 만듭니다.
   - 다른 관리 그룹에 속하거나 어떤 관리 그룹에도 속하지 않는 클라이언트 기기의 사용자에게 메시지를 전송하려면 특정 기기에 대한 작업을 만듭니다.

   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
3. 새 작업 마법사의 작업 유형 창에서 **Kaspersky Security Center 중앙 관리 서버** 노드를 선택한 후, **고급** 폴더를 열고 **사용자에게 메시지 전송** 작업을 선택합니다. 사용자에게 공지 메시지 배포 작업은 Windows를 실행 중인 기기에서만 사용 가능합니다. **사용자 계정** 폴더에서 해당 사용자의 마우스 오른쪽 메뉴를 사용해 메시지를 전송할 수도 있습니다.
4. 만들어진 작업을 실행합니다.

   작업이 완료되면 만들어진 메시지가 선택한 기기의 사용자에게 전송됩니다. 사용자에게 공지 메시지 배포 작업은 Windows를 실행 중인 기기에서만 사용 가능합니다. **사용자 계정** 폴더에서 해당 사용자의 마우스 오른쪽 메뉴를 사용해 메시지를 전송할 수도 있습니다.

Kaspersky Security for Virtualization 관리

Kaspersky Security Center는 중앙 관리 서버에 가상 컴퓨터를 연결할 수 있는 옵션을 지원합니다. 가상 컴퓨터는 Kaspersky Security for Virtualization이 보호합니다. 자세한 내용은 이 애플리케이션의 설명서를 참조하십시오.

기기 상태 전환 구성

조건을 변경하여 *심각* 또는 *경고* 상태를 기기에 할당할 수 있습니다.

기기 상태가 심각으로 변경되도록 설정하려면 다음과 같이 하십시오:

1. 다음 방법 중 하나로 속성 창을 엽니다:
   - **정책** 폴더에서 중앙 관리 서버 정책의 마우스 오른쪽 메뉴를 열고 **속성**를 선택합니다.
   - 관리 그룹의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
2. **속성** 창이 열리면 **섹션** 창에서 **기기 상태**를 선택합니다.

3. 오른쪽 창에 있는 **다음이 지정되면 심각으로 설정** 섹션에서 목록의 조건 옆에 있는 확인란을 선택합니다.

   부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

4. 선택한 조건의 이름을 두 번 클릭한 다음, 창이 열리면 해당 창에서 조건에 필요한 값을 설정합니다.

   다음과 같은 조건에는 값을 설정할 수 없습니다: 보안 제품이 설치 안 됨, 비호환 애플리케이션이 설치되어 있음, 소프트웨어 취약점이 탐지됨, 모바일 기기 설정이 정책과 일치하지 않음, 처리되지 않은 보안 문제가 있음, 애플리케이션에서 정의된 기기 상태, 기기와의 연결이 끊어짐, 보안 제품이 실행 중이지 않음, 라이센스 만료됨.

   재시작 필요 조건의 경우, 재시작 이유를 지정할 수 있습니다. 목록에서 모든 이유 옆에 있는 확인란을 선택하는 것이 좋습니다.

5. **확인**를 누릅니다.

지정한 조건이 충족되면 관리 중인 기기에 *심각* 상태가 할당됩니다.

기기 상태가 경고로 변경되도록 설정하려면 다음과 같이 하십시오:

1. 다음 방법 중 하나로 속성 창을 엽니다:

   - **정책** 폴더에서 중앙 관리 서버 정책의 마우스 오른쪽 메뉴를 열고 **속성**를 선택합니다.
   - 관리 그룹의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

2. **속성** 창이 열리면 **섹션** 창에서 **기기 상태**를 선택합니다.

3. 오른쪽 패널에 있는 **다음이 지정되면 경고로 설정** 섹션에서 목록의 조건 옆에 있는 확인란을 선택합니다.

   부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

4. 선택한 조건의 이름을 두 번 클릭한 다음, 창이 열리면 해당 창에서 조건에 필요한 값을 설정합니다.

   다음과 같은 조건에는 값을 설정할 수 없습니다: 보안 제품이 설치 안 됨, 비호환 애플리케이션이 설치되어 있음, 소프트웨어 취약점이 탐지됨, 모바일 기기 설정이 정책과 일치하지 않음, 처리되지 않은 보안 문제가 있음, 애플리케이션에서 정의된 기기 상태, 기기와의 연결이 끊어짐, 보안 제품이 실행 중이지 않음, 라이센스 만료됨.

   재시작 필요 조건의 경우, 재시작 이유를 지정할 수 있습니다. 목록에서 모든 이유 옆에 있는 확인란을 선택하는 것이 좋습니다.

5. **확인**를 누릅니다.

지정한 조건이 충족되면 관리 중인 기기에 *경고* 상태가 할당됩니다.

기기 태그 및 할당된 태그 보기

Kaspersky Security Center에서는 기기를 태그할 수 있습니다. *태그*는 기기 그룹화, 설명 또는 검색에 사용할 수 있는 기기의 ID입니다. 기기에 할당된 태그는 조회 만들기, 기기 검색 및 관리 그룹에 기기 배포 작업에 사용할 수 있습니다.

태그를 수동 또는 자동으로 할당할 수 있습니다. 개별 기기에 대해 태그를 할당해야 하는 경우 수동 태그를 사용할 수 있습니다. 수동 태그는 기기 속성에서 수행합니다. 자동 태그는 지정된 태그 규칙에 따라 중앙 관리 서버에서 수행합니다.

중앙 관리 서버의 속성에서 해당 서버가 관리하는 기기에 대한 자동 태그를 설정할 수 있습니다. 지정된 규칙을 충족하는 경우 기기에 자동으로 태그가 할당됩니다. 각 태그별로 해당하는 개별 규칙이 있습니다. 규칙은 기기의 네트워크 속성, 운영 체제, 기기에 설치된 애플리케이션 및 기타 기기 속성에 적용됩니다. 예를 들어 Windows를 실행하는 모든 기기에 *Win* 태그를 할당하는 규칙을 설정할 수 있습니다. 그런 다음 기기 조회를 만들 때 이 태그를 사용할 수 있습니다. 그러면 Windows를 실행하는 모든 기기를 손쉽게 분류하여 작업을 할당할 수 있습니다.

또한 관리 중인 기기의 정책 프로필 활성화 조건으로 태그를 사용할 수도 있습니다. 그러면 특정 태그가 할당된 기기에서만 특정 정책 프로필이 적용됩니다. 예를 들어 *Courier* 태그가 할당된 기기가 *사용자* 관리 그룹에 표시되고 *Courier* 태그에 해당하는 정책 프로필 활성화가 설정된 경우 *사용자* 그룹에 대해 생성된 정책은 이 기기에 적용되지 않지만 정책 프로필은 적용됩니다. 정책 프로필을 사용하면 정책에 의해 실행이 차단된 일부 애플리케이션을 이 기기에서 시작할 수 있습니다.

여러 개의 태그 규칙을 만들 수도 있습니다. 여러 개의 태그 규칙을 만들었는데 각 규칙의 조건이 동시에 충족되는 경우 한 기기에 여러 태그가 할당될 수 있습니다. 기기 속성에서 할당된 모든 태그의 목록을 볼 수 있습니다. 각 태그 규칙은 활성되거나 비활성될 수 있습니다. 하나의 규칙이 활성되면 중앙 관리 서버에서 관리하는 기기에 적용됩니다. 현재는 사용하지 않지만 나중에 필요할 수도 있는 규칙의 경우 제거할 필요가 없습니다. **규칙 사용** 확인란의 선택을 취소하면 됩니다. 그러면 규칙이 비활성화되고 **규칙 사용** 확인란이 다시 선택될 때까지 실행되지 않습니다. 일시적으로 태그 규칙 목록에서 특정 규칙을 제외하고 나중에 다시 포함시키려는 경우 해당 규칙을 비활성해야 합니다.

자동으로 기기 태그

중앙 관리 서버 속성 창에서 자동 태그 규칙을 만들고 편집할 수 있습니다.

기기에 자동으로 태그를 지정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 태그 규칙을 지정해야 하는 중앙 관리 서버의 이름이 있는 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창에서 **태그 입력 규칙** 섹션을 선택합니다.
4. **태그 입력 규칙** 섹션에서 **추가** 버튼을 누릅니다.
   새 규칙 창이 열립니다.
5. **새 규칙** 창에서 해당 규칙의 일반 속성을 구성합니다.
   - 규칙 이름을 지정합니다.
     규칙 이름은 255자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
   - **규칙 사용** 확인란을 사용하여 규칙을 사용하거나 중지합니다.
     기본적으로 **규칙 사용** 확인란은 선택되어 있습니다.
   - **태그** 필드에 태그 이름을 입력합니다.
     태그 이름은 255자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
6. **조건** 섹션에서, **추가** 버튼을 눌러 새로운 조건을 추가하거나 **속성**을 눌러 기존 조건을 편집하십시오.
   새 자동 태그 입력 규칙 조건 마법사 창이 열립니다.
7. **태그 할당 조건** 창에서 태그가 지정되려면 충족해야 하는 조건의 확인란을 선택합니다. 조건은 여러 개 선택할 수 있습니다.

8. 선택한 태그 입력 조건에 따라 마법사가 해당 조건 설정을 위한 창을 표시합니다. 다음 조건을 기준으로 하여 규칙 활성화를 설정합니다:

   - **기기 사용 또는 특정 네트워크와의 연결** - Windows 네트워크의 기기 이름, 도메인이나 IP 서브넷에 기기가 포함되는지 여부와 같은 기기의 네트워크 속성입니다.

     Kaspersky Security Center에 사용하는 데이터베이스에 대해 대소문자 구분 데이터 정렬이 설정되었다면, 기기 DNS 이름을 지정할 때 대소문자를 구분합니다. 그렇지 않으면 자동 태그 추가 규칙이 작동하지 않습니다.

   - **Active Directory** - Active Directory 조직 구성단위에 기기가 있는지 여부와 Active Directory 그룹에서의 기기 멤버십입니다.
   - **특정 애플리케이션** - 기기의 네트워크 에이전트 유무와 운영 체제 유형, 버전, 아키텍처입니다.
   - **가상 컴퓨터** - 특정 유형의 가상 컴퓨터에 기기가 포함되는지 여부입니다.
   - **자산 관리(소프트웨어)에 등록된 애플리케이션이 설치됨** - 기기에 다양한 공급업체의 애플리케이션이 설치되어 있는지 여부입니다.

9. 조건을 설정한 후 조건의 이름을 입력하고 마법사를 닫습니다.

   필요한 경우 규칙 하나에 여러 조건을 설정할 수 있습니다. 이 경우 기기가 조건 하나 이상을 충족하면 태그가 기기에 할당됩니다. 추가한 조건은 규칙 속성 창에 표시됩니다.

10. **새 규칙** 창에서 **확인**를 누른 다음 중앙 관리 서버 속성 창에서 **확인**를 누릅니다.

선택한 중앙 관리 서버를 통해 관리 중인 기기에서 새로 만든 규칙이 적용됩니다. 기기 설정이 규칙 조건을 충족하면 기기에 태그가 할당됩니다.

기기에 할당된 태그 보기 및 구성

기기에 할당된 모든 태그의 목록을 확인할 수 있을 뿐 아니라 기기 속성 창에서 자동 태그 규칙 설정을 진행할 수도 있습니다.

기기에 할당된 태그를 보고 설정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 엽니다.
2. **관리 중인 기기** 폴더의 작업 영역에서 할당된 태그를 보려는 기기를 선택합니다.
3. 모바일 기기의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
4. 기기 속성 창에서 **태그** 섹션을 선택합니다.

   선택한 기기에 할당된 태그 목록과 각 태그가 할당된 방식(수동으로 또는 규칙에 따라)이 표시됩니다.

5. 필요한 경우 다음 작업 중 하나를 수행합니다:

   - 태그 규칙 설정을 진행하려면 **자동 태그 입력 규칙 설정** 링크(Windows용만)를 누릅니다.
   - 태그 이름을 변경하려면 태그를 선택하고 **이름 바꾸기** 버튼을 누릅니다.

- 태그를 제거하려면 태그를 선택하고 **제거** 버튼을 누릅니다.
- 태그를 수동으로 추가하려면 **태그** 섹션 아래쪽의 필드 중 하나에 내용을 입력하고 **추가** 버튼을 누릅니다.

6. **태그** 섹션에서 변경을 수행한 경우 **적용** 버튼을 눌러 변경 내용을 적용합니다.
7. **확인**을 누릅니다.

기기 속성에서 태그를 제거하거나 이름을 변경한 경우 중앙 관리 서버 속성에서 설정한 태그 규칙에는 해당 변경 내용이 적용되지 않습니다. 즉, 해당 속성을 변경한 기기에만 변경 내용이 적용됩니다.

클라이언트 기기 원격 진단. Kaspersky Security Center 원격 진단 유틸리티

Kaspersky Security Center의 원격 진단용 유틸리티(이후 원격 진단 유틸리티라고 함)는 클라이언트 기기에서 다음과 같은 작업을 원격으로 수행할 수 있도록 설계되었습니다:

- 추적 로그 작동 및 중지, 추적 로그 레벨 변경, 추적 로그 파일 다운로드.
- 시스템 정보 및 애플리케이션 설정 다운로드.
- 이벤트 로그 다운로드.
- 애플리케이션에 대한 덤프 파일 생성.
- 진단 시작 및 진단 리포트 다운로드.
- 애플리케이션 시작 및 중지.

클라이언트 기기에서 다운로드한 이벤트 로그 및 진단 리포트를 사용하여 문제를 직접 해결할 수 있습니다. 또한 Kaspersky 기술 지원 전문가가 Kaspersky에서 추가 분석을 수행할 수 있도록 클라이언트 기기에서 추적 로그 파일, 덤프 파일, 이벤트 로그 및 진단 리포트를 다운로드하도록 요청할 수 있습니다.

원격 진단 유틸리티는 관리 콘솔과 함께 자동으로 기기에 설치됩니다.

클라이언트 기기에 원격 진단 유틸리티 연결

원격 진단 유틸리티를 클라이언트 기기에 연결하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 관리 그룹을 선택합니다.
2. 작업 영역의 **기기** 탭에서 기기의 마우스 오른쪽 메뉴를 열고 **사용자 지정 도구 → 원격 진단**를 선택합니다.
   원격 진단 유틸리티 메인 창이 열립니다.
3. 원격 진단 유틸리티 메인 창의 첫 번째 필드에서 기기에 연결하는 데 사용할 도구를 지정합니다:
   - **Microsoft Windows 네트워크를 사용하여 접근**.
   - **중앙 관리 서버를 사용하여 접근**.

4. 메인 유틸리티 창의 첫 번째 필드에서 **Microsoft Windows 네트워크를 사용하여 접근**를 선택한 경우 다음 처리를 수행합니다:

   - **기기** 필드에 연결해야 하는 기기의 주소를 지정합니다.

     IP 주소, NetBIOS 또는 DNS 이름을 기기 주소로 사용할 수 있습니다.

     기본값은 유틸리티가 시작되는 기기의 마우스 오른쪽 메뉴에 표시되는 주소입니다.

   - 다음과 같이 기기에 연결할 계정을 지정합니다:

     - **현재 사용자로 연결**(기본적으로 선택). 현재 사용자 계정을 사용하여 연결합니다.

     - **사용자 이름 및 암호를 사용하여 연결**. 제공된 사용자 계정을 사용하여 연결합니다. 필요한 계정의 **사용자 이름** 및 **암호**를 지정합니다.

     > 기기의 로컬 관리자 계정을 사용해야만 기기에 연결할 수 있습니다.

5. 메인 유틸리티 창의 첫 번째 필드에서 **중앙 관리 서버를 사용하여 접근**을 선택한 경우 다음 처리를 수행합니다:

   - **중앙 관리 서버** 필드에서 기기에 연결할 중앙 관리 서버의 주소를 지정합니다.

     IP 주소, NetBIOS 또는 DNS 이름을 서버 주소로 사용할 수 있습니다.

     기본값은 유틸리티가 실행되는 중앙 관리 서버의 주소입니다.

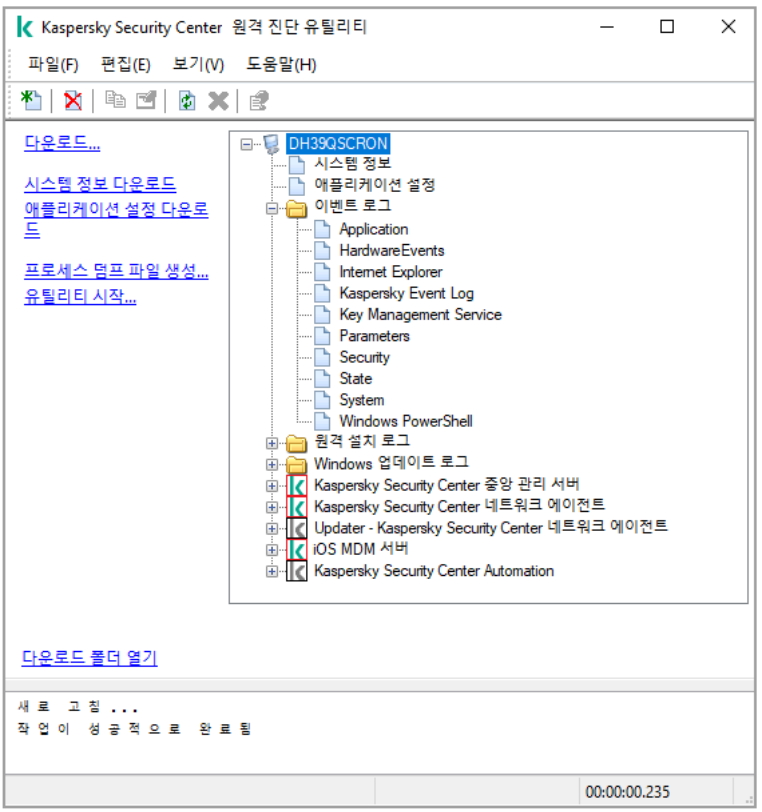
   - 필요한 경우 **SSL 사용**, **트래픽 압축** 및 **보조 중앙 관리 서버에 소속된 기기** 확인란을 선택합니다.

     보조 중앙 관리 서버에 소속된 기기 확인란을 선택한 경우 **보조 중앙 관리 서버에 소속된 기기** 필드에 **찾기** 버튼을 눌러 기기를 관리하는 보조 중앙 관리 서버의 이름을 입력할 수 있습니다.

6. 기기에 연결하려면 **로그인** 버튼을 누릅니다.

   > 계정의 2단계 인증이 활성화된 경우에는 2단계 인증을 사용하여 인증해야 합니다.

그러면 기기의 원격 진단 창이 열립니다(아래 그림 참조). 창 왼쪽에는 기기 진단 작동으로 연결되는 링크가 표시됩니다. 창 오른쪽에는 유틸리티에서 작동할 수 있는 기기의 개체 트리가 표시됩니다. 창 아래에는 유틸리티 작동의 진행 상황이 표시됩니다.



원격 진단 유틸리티. 원격 기기 진단 창

기기에서 다운로드한 파일은 원격 진단 유틸리티가 실행되는 기기의 바탕 화면에 저장됩니다.

애플리케이션에 대한 덤프 파일 생성

애플리케이션 덤프 파일을 사용하면 특정 시점에 클라이언트 기기에서 실행 중인 애플리케이션의 매개변수를 볼 수 있습니다. 이 파일에는 애플리케이션에 대해 로드된 모듈 정보도 포함되어 있습니다.

Linux 기반 기기에서 덤프 수집은 지원하지 않습니다.

원격 진단으로 덤프를 수집하려면 kldumper 유틸리티가 사용됩니다. 이 유틸리티는 기술 지원 전문가의 요청에 따라 Kaspersky 애플리케이션의 프로세스 덤프를 수집하도록 설계되었습니다. kldumper 유틸리티 사용을 위한 요구 사항에 대한 상세 정보는 Kaspersky Security Center 기술 자료를 참조하십시오.

애플리케이션에 대한 덤프 파일을 생성하려면:

1. **관리 중인 기기** 폴더 작업 공간의 **기기** 탭에서 필요한 기기의 마우스 오른쪽 메뉴를 열고 **사용자 지정 도구 → 원격 진단**을 선택합니다.

   Kaspersky Security Center 원격 진단 유틸리티 창이 열립니다.

2. 클라이언트 기기에 원격 진단 유틸리티에 연결합니다.

   그러면 기기의 원격 진단 창이 열립니다.

3. 창 왼쪽에서 **프로세스 덤프 파일 생성** 링크를 누릅니다.

4. **프로세스 덤프 파일 생성 중** 창이 열리면 덤프 파일을 생성할 애플리케이션의 실행 파일을 지정합니다.

5. **확인** 버튼을 누릅니다.

지정한 애플리케이션의 덤프 파일이 포함된 압축 파일이 다운로드됩니다.

지정한 애플리케이션을 클라이언트 기기에서 실행하고 있지 않다면 다운로드한 압축 파일에 포함된 "결과" 폴더는 비어 있게 됩니다.

지정한 애플리케이션은 실행 중이지만 오류가 발생하여 다운로드가 실패하거나 다운로드한 압축 파일에 포함된 "result" 폴더가 비어 있다면 Kaspersky Security Center 기술 자료를 참조하십시오.

추적 로그 작동 및 중지, 추적 로그 파일 다운로드

원격 기기에서 추적 로그를 작동하려면 다음과 같이 하십시오:

1. 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.

2. 기기의 개체 트리에서 추적 로그를 작성해야 하는 애플리케이션을 선택합니다.

> 기기가 중앙 관리 서버의 도구를 사용하여 연결했을 때만 자기 보호 기능이 있는 애플리케이션에 대해 추적 로그를 작동하거나 중지할 수 있습니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 생성하는 중에 네트워크 에이전트에 대한 추적 로그를 작동시킬 수도 있습니다. 이 경우에는 원격 진단 유틸리티에서 네트워크 에이전트에 대한 추적 로그가 비활성화되어 있어도 네트워크 에이전트가 추적 로그 정보를 씁니다.

3. 추적 로그를 작동하려면 다음과 같이 하십시오:

   a. 원격 진단 유틸리티 창 왼쪽에서 **추적 활성화**을 누릅니다.

   b. **추적 로그 레벨 선택** 창이 열리면 설정의 기본값을 유지하는 것이 좋습니다. 필요한 경우 기술 지원 전문가가 구성 프로세스를 안내합니다. 다음과 같은 설정을 사용할 수 있습니다:

   - **추적 로그 레벨**

     추적 로그 레벨은 추적 로그 파일에 포함되는 세부 정보의 양을 정의합니다.

   - **순환식 저장 모드 추적 로그**(Kaspersky Endpoint Security에만 사용 가능)

     추적 로그 파일 크기의 과도한 증가를 방지하기 위해 애플리케이션이 추적 로그 정보를 덮어씁니다. 추적 로그 정보를 저장하는 데 사용할 최대 파일 수와 각 파일의 최대 크기를 지정합니다. 최대 크기의 추적 로그 파일이 최대 수만큼 기록되면 새 추적 로그 파일을 기록할 수 있도록 가장 오래된 추적 로그 파일이 삭제됩니다.

   c. **확인**을 누릅니다.

4. Kaspersky Endpoint Security의 경우에는 기술 지원 전문가가 시스템 성능 관련 정보를 확인하기 위해 Xperf 추적 로그를 활성화하도록 요청할 수 있습니다.

Xperf 추적 로그를 작동하려면 다음과 같이 하십시오:

a. 원격 진단 유틸리티 창 왼쪽에서 **Xperf 추적 활성화**을 누릅니다.

b. **추적 로그 레벨 선택** 창이 열리면 기술 지원 전문가의 요청에 따라 다음 추적 로그 레벨 중 하나를 선택합니다.

- **Light 레벨**

  이 유형의 추적 로그 파일은 시스템과 관련된 최소한의 정보를 포함합니다.
  기본적으로 이 옵션은 선택되어 있습니다.

- **Deep 레벨**

  이 유형의 추적 로그 파일은 *Light* 유형의 추적 로그 파일에 비해 더 자세한 정보를 포함합니다. *Light* 유형의 추적 로그 파일만으로는 성능을 평가하기에 충분하지 않은 경우 기술 지원 전문가가 이 파일을 요청할 수 있습니다. *Deep* 추적 로그 파일에는 하드웨어, 운영 체제, 시작/완료한 프로세스와 애플리케이션 목록, 성능 평가에 사용되는 이벤트, Windows 시스템 평가 도구의 이벤트 관련 정보를 비롯하여 시스템에 대한 기술 정보가 포함됩니다.

c. 다음 추적 로그 유형 중 하나를 선택합니다:

- **기본 유형**

  Kaspersky Endpoint 보안 제품 작동 중에 추적 로그 정보가 수신됩니다.
  기본적으로 이 옵션은 선택되어 있습니다.

- **재시작 시 유형**

  관리 중인 기기에서 운영 체제가 시작될 때 추적 로그 정보가 수신됩니다. 기기를 켜고 나서 Kaspersky Endpoint Security를 시작하기 전에 시스템 성능에 영향을 주는 문제가 발생하는 경우 이 추적 로그 유형이 효과적입니다.

d. 추적 로그 파일 크기의 과도한 증가를 방지하기 위해 **순환식 저장 모드 추적 로그** 옵션을 활성화하라는 요청을 받을 수도 있습니다. 그런 후에는 추적 로그 파일의 최대 크기를 지정합니다. 파일이 최대 크기가 되면 새로운 정보가 가장 오래된 추적 로그 정보를 덮어씁니다.

e. **확인**을 누릅니다.

일부 경우에 추적 로그를 작동하려면 보안 제품 및 작업을 다시 시작해야 합니다.

원격 진단 유틸리티가 선택한 애플리케이션에 대한 추적 로그를 작동합니다.

애플리케이션의 추적 로그 파일을 다운로드하려면 다음과 같이 하십시오:

1. "클라이언트 기기에 원격 진단 유틸리티 연결"의 설명에 따라 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.
2. 애플리케이션 노드의 **추적 파일** 폴더에서 필요한 파일을 선택합니다.
3. 원격 진단 유틸리티 창 왼쪽에서 **전체 파일 다운로드**를 누릅니다.

대용량 파일의 경우 최신 추적 로그 파일의 부분만 다운로드할 수 있습니다.

강조 표시된 추적 로그 파일은 삭제할 수 있습니다. 추적 로그를 중지한 후에 파일을 삭제할 수 있습니다.

선택한 파일이 창 아래쪽에서 지정한 위치에 다운로드됩니다.

원격 기기에서 추적 로그를 중지하려면 다음과 같이 하십시오:

1. "클라이언트 기기에 원격 진단 유틸리티 연결"의 설명에 따라 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.
2. 기기 개체 트리에서 추적 로그를 중지할 애플리케이션을 선택합니다.

   기기가 중앙 관리 서버의 도구를 사용하여 연결된 경우에만 자기-보호 기능이 있는 애플리케이션에 대해 추적 로그를 작동하거나 중지할 수 있습니다.

3. 원격 진단 유틸리티 창 왼쪽에서 **추적 로그 중지**를 누릅니다.

원격 진단 유틸리티가 선택한 애플리케이션에 대한 추적 로그를 중지합니다.

애플리케이션 설정 다운로드

원격 기기에서 애플리케이션 설정을 다운로드하려면:

1. "클라이언트 기기에 원격 진단 유틸리티 연결"의 설명에 따라 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.
2. 원격 진단 유틸리티 창의 개체 트리에서 기기 이름이 지정된 최상위 노드를 선택합니다.
3. 원격 진단 유틸리티 창의 왼쪽에서 다음 옵션 중 필요한 작업을 선택합니다:

   - **시스템 정보 다운로드**
   - **애플리케이션 설정 다운로드**
   - **프로세스 덤프 파일 생성**

     이 링크를 누르면 열리는 창에서, 덤프 파일을 생성해야 하는 애플리케이션의 실행 파일을 지정합니다.
   - **유틸리티 시작**

     이 링크를 누르면 열리는 창에서, 시작하기 원하는 유틸리티의 실행 파일 및 그 실행 설정을 지정합니다.

그러면 선택한 유틸리티가 기기에 다운로드되고 실행됩니다.

이벤트 로그 다운로드

원격 기기에서 이벤트 로그를 다운로드하려면:

1. "클라이언트 기기에 원격 진단 유틸리티 연결"의 설명에 따라 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.
2. 기기 개체 트리의 **시스템 이벤트 로그** 폴더에서 관련 로그를 선택합니다.
3. 원격 진단 유틸리티 창의 왼쪽에서 **<이벤트 로그 이름> 이벤트 로그 다운로드** 링크를 눌러 선택한 로그를 다운로드합니다.

선택한 이벤트 로그가 아래쪽 창에서 지정한 위치에 다운로드됩니다.

여러 진단 정보 항목 다운로드

Kaspersky Security Center 원격 진단 유틸리티에서는 이벤트 로그, 시스템 정보, 추적 로그 파일 및 덤프 파일을 포함한 여러 진단 정보 항목을 다운로드할 수 있습니다.

원격 기기에서 진단 정보를 다운로드하려면:

1. "클라이언트 기기에 원격 진단 유틸리티 연결"의 설명에 따라 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.
2. 원격 진단 유틸리티 창 왼쪽에서 **다운로드**를 누릅니다.
3. 다운로드하려는 항목 옆에 있는 확인란을 선택합니다.
4. **시작**을 누릅니다.

선택한 모든 항목이 아래쪽 창에서 지정한 위치에 다운로드됩니다.

진단 시작 및 그 결과 다운로드

원격 기기에 있는 애플리케이션에 대한 진단을 시작하고 결과를 다운로드하려면 다음과 같이 하십시오:

1. "클라이언트 기기에 원격 진단 유틸리티 연결"의 설명에 따라 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.
2. 기기의 개체 트리에서 필요한 애플리케이션을 선택합니다.
3. 그런 다음 원격 진단 유틸리티 창의 왼쪽 부분에서 **진단 실행** 링크를 눌러 진단을 시작합니다.
   그러면 진단 리포트가 개체 트리에서 선택한 애플리케이션 노드에 표시됩니다.
4. 개체 트리에서 새로 생성된 진단 리포트를 선택하고 **다운로드 폴더 열기** 링크를 눌러 다운로드합니다.

선택한 리포트가 아래쪽 창에서 지정한 위치에 다운로드됩니다.

애플리케이션 시작, 중지 및 다시 시작

중앙 관리 서버 도구를 사용하여 기기에 연결한 경우 애플리케이션을 시작 또는 중지하거나 다시 시작하는 작업을 수행할 수 있습니다.

애플리케이션을 시작 또는 중지하거나 다시 시작하려면 다음과 같이 하십시오:

1. "클라이언트 기기에 원격 진단 유틸리티 연결"의 설명에 따라 원격 진단 유틸리티를 실행하고 필요한 기기에 연결합니다.
2. 기기의 개체 트리에서 필요한 애플리케이션을 선택합니다.
3. 원격 진단 유틸리티 창의 왼쪽에서 작업을 선택합니다:
   - **애플리케이션 중지**
   - **애플리케이션 다시 시작**
   - **애플리케이션 시작**

   선택한 처리에 따라 애플리케이션이 시작되거나 중지되거나 다시 시작됩니다.

UEFI 보호 기기

*UEFI 보호 기기*는 BIOS 수준에서 통합된 UEFI용 Kaspersky 솔루션 또는 애플리케이션이 설치된 기기입니다. 통합 보호 기능은 시스템이 시작되는 순간부터 기기 보안을 시작하며 통합 소프트웨어가 없는 기기에 대한 보호는 보안 제품이 시작된 이후에만 기능을 시작합니다. Kaspersky Security Center는 이러한 기기에 대한 관리를 지원합니다.

UEFI 보호 기기의 연결 설정을 수정하려면 다음과 같이 진행합니다:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창에서 **서버 연결 설정** → **추가 포트**를 선택합니다.
4. **추가 포트** 섹션에서 관련 설정을 수정합니다.
   - **UEFI 보호 기기 및 KasperskyOS 기기용 포트 열기**

     UEFI 보호 기기가 중앙 관리 서버에 연결할 수 있습니다.

   - **UEFI 보호 기기 및 KasperskyOS 기기용 포트**

     UEFI 보호 기기 및 KasperskyOS 기기용 포트 열기 옵션을 활성화하는 경우 포트 번호를 변경할 수 있습니다. 기본 포트 번호는 13294입니다.
5. **확인**를 누릅니다.

관리 중인 기기 설정

관리 중인 기기 설정을 보려면:

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 선택합니다.
2. 폴더의 작업 영역에서 기기를 선택합니다.
3. 기기의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.

선택한 기기의 속성 창이 열리고 **일반** 섹션이 선택됩니다.

일반

일반 섹션에는 클라이언트 기기에 대한 일반 정보가 표시됩니다. 정보는 클라이언트 기기와 중앙 관리 서버의 마지막 동기화 중에 수신된 데이터를 기준으로 제공됩니다:

- **이름**

  이 필드에서는 관리 그룹에 있는 클라이언트 기기의 이름을 보고 수정할 수 있습니다.

- **설명**

  이 필드에서는 클라이언트 기기에 대한 추가 설명을 입력할 수 있습니다.

- **Windows 도메인**

  기기가 포함된 Windows 도메인 또는 작업 그룹입니다.

- **NetBIOS 이름**

  클라이언트 기기의 Windows 네트워크 이름입니다.

- **DNS 이름**

  클라이언트 기기의 DNS 도메인 이름입니다.

- **IP 주소**

  기기 IP 주소.

- **그룹**

  클라이언트 기기가 포함된 관리 그룹입니다.

- **마지막 업데이트**

  기기에서 안티 바이러스 데이터베이스 또는 애플리케이션이 마지막으로 업데이트된 날짜입니다.

- **마지막 존재 확인**

  기기가 네트워크에 마지막으로 표시된 날짜와 시간입니다.

- **중앙 관리 서버에 연결**

  클라이언트 기기의 네트워크 에이전트가 중앙 관리 서버에 마지막으로 연결한 날짜와 시간입니다.

- **중앙 관리 서버와 계속 연결 유지**

  이 옵션이 활성화되면 관리 중인 기기와 중앙 관리 서버 사이에 지속적인 연결 이 유지됩니다. 해당 연결을 제공하는 푸시 서버를 사용 하지 않는다면 이 옵션을 사용하면 됩니다.

  이 옵션이 비활성화되어 있고 푸시 서버를 사용하지 않는 경우 관리 중인 기기가 데이터를 동기화하거나 정보를 전송하기 위해서만 중앙 관리 서버에 연결합니다.

  중앙 관리 서버와 계속 연결 유지 확인란을 선택한 상태에서 사용 가능한 기기의 최대 총 개수는 300입니다.

  이 옵션은 관리 중인 기기에서는 기본적으로 비활성화되어 있습니다. 이 옵션은 중앙 관리 서버가 설치된 기기에서 기본적으로 활성화되며 비활성화를 시도하더라도 활성화된 상태로 유지됩니다.

보호

보호 섹션에서는 클라이언트 기기의 현재 안티 바이러스 보호 상태에 대한 정보가 제공됩니다:

- **기기 상태**

  네트워크의 기기 활동과 기기의 안티 바이러스 보호 상태에 대해 관리자가 정의한 기준에 따라 할당된 클라이언트 기기의 상태입니다.

- **모든 문제**

  이 표에는 클라이언트 기기에 설치된 관리 중인 애플리케이션에서 탐지한 문제의 전체 목록이 포함되어 있습니다. 각 문제에는 해당 문제에 대해 기기에 할당하도록 애플리케이션이 제안하는 상태가 함께 표시됩니다.

- **실시간 보호**

  이 필드에서는 클라이언트 기기의 현재 실시간 보호 상태를 보여 줍니다.

  기기에서 상태가 변경되면 클라이언트 기기를 중앙 관리 서버와 동기화해야 기기 속성 창에 새 상태가 표시됩니다.

- **마지막 수동 검사 날짜**

  클라이언트 기기에서 마지막으로 악성 코드 검사를 수행한 날짜와 시간.

- **탐지된 위협 전체 개수**

  보안 애플리케이션 설치 이후(첫 번째 검사) 또는 위협 카운터를 마지막으로 초기화한 이후 클라이언트 기기에서 탐지된 전체 위협 수입니다.

- **처리 안 된 위협**

  클라이언트 기기에서 처리 안 된 파일의 개수입니다.

  모바일 기기의 처리 안 된 파일 수는 이 필드에서 무시됩니다.

- **디스크 암호화 상태**

  기기 로컬 드라이브의 현재 파일 암호화 상태입니다. 상태에 대한 설명은 Kaspersky Endpoint Security for Windows 도움말을 참조하십시오.

애플리케이션

애플리케이션 섹션에는 클라이언트 기기에 설치된 모든 Kaspersky 애플리케이션이 나열됩니다. 이 섹션에는 선택한 Kaspersky 애플리케이션(네트워크 에이전트 제외)을 시작 및 중지할 수 있는 시작 버튼( ) 및 중지 버튼( )이 있습니다. 이 버튼은 중앙 관리 서버의 수신 푸시 알림을 위해 관리 중인 기기에서 포트 15000 UDP를 사용할 수 있을 때 활성화됩니다. 관리 중인 기기를 푸시 알림에 사용할 수 없지만 중앙 관리 서버에 대한 연속 연결 모드가 활성화되어 있다면(**일반** 섹션에서 **중앙 관리 서버와 계속 연결 유지** 옵션 활성화), 시작 및 중지 버튼을 사용할 수 있습니다. 또한 **애플리케이션** 섹션에는 다음 버튼이 포함되어 있습니다:

- **이벤트**

  이 버튼을 누르면 애플리케이션을 실행할 때 클라이언트 기기에서 발생한 이벤트 목록과 이 애플리케이션의 작업 결과를 확인할 수 있습니다.

- **통계**

  이 버튼을 누르면 애플리케이션에 대한 현재 통계 정보를 볼 수 있습니다.

- **속성**

  이 버튼을 누르면 애플리케이션에 대한 정보를 확인하고 애플리케이션을 구성할 수 있습니다.

작업

작업 섹션에서는 기존 작업 목록 보기, 새 작업 만들기, 작업 제거, 작업 시작 및 중지, 작업 설정 수정, 실행 결과 보기 등의 클라이언트 기기 작업을 관리할 수 있습니다. 클라이언트를 중앙 관리 서버와 마지막으로 동기화할 때 받은 데이터를 기반으로 작업 목록이 제공됩니다. 중앙 관리 서버는 클라이언트 기기에서 작업 상태 세부 정보를 요청합니다.

시작(), 중지(), 제거() 버튼은 중앙 관리 서버의 수신 푸시 알림에 대해 관리 중인 기기에서 포트 15000 UDP를 사용할 수 있을 때 활성화됩니다. 관리 중인 기기를 푸시 알림에 사용할 수 없지만 중앙 관리 서버에 대한 연속 연결 모드가 활성화되어 있다면(**일반** 섹션에서 **중앙 관리 서버와 계속 연결 유지** 옵션 활성화) 시작, 중지, 제거 버튼을 사용할 수 있습니다.

연결할 수 없다면 작업 상태가 표시되지 않으며 버튼도 비활성화됩니다.

이벤트

이벤트 섹션에는 선택된 클라이언트 기기의 중앙 관리 서버에 기록된 이벤트가 표시됩니다.

기기 이벤트를 내보내기, 복사, 삭제할 수 있습니다.

태그

태그 섹션에서는 클라이언트 기기 검색을 위한 키워드 목록을 관리합니다: 기존 태그 목록 보기, 목록에서 태그 할당하기, 자동 태그 규칙 구성하기, 새 태그 추가하기, 오래된 태그 이름 변경하기, 태그 제거.

시스템 정보

일반 시스템 정보 섹션에서는 클라이언트 기기에 설치된 애플리케이션에 대한 정보를 제공합니다.

자산 관리(소프트웨어)

자산 관리(소프트웨어) 섹션에서는 클라이언트 기기에 설치된 애플리케이션의 레지스트리와 해당 업데이트를 볼 수 있으며 자산 관리(소프트웨어)의 표시 방식도 설정할 수 있습니다.

클라이언트 기기에 설치된 네트워크 에이전트가 중앙 관리 서버에 필요한 정보를 전송하는 경우 설치된 애플리케이션에 대한 정보가 제공됩니다. 네트워크 에이전트 또는 해당 정책의 속성 창에 있는 **저장소** 섹션에서 중앙 관리 서버로의 정보 전송을 구성할 수 있습니다.

- **호환되지 않는 보안 제품만 표시**

  이 옵션을 사용하면 애플리케이션 목록에 Kaspersky 애플리케이션과 호환되지 않는 보안 애플리케이션만 표시됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 표시**

  이 옵션을 활성화하면 애플리케이션 목록에 애플리케이션뿐만 아니라 해당 애플리케이션에 대해 설치된 업데이트 패키지까지 표시됩니다.

업데이트 목록을 표시하려면 100KB의 트래픽이 필요합니다. 목록을 닫았다가 다시 열면 100KB의 트래픽을 다시 소비해야 합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **파일로 내보내기**

  기기에 설치된 애플리케이션 목록을 CSV 파일 또는 TXT 파일로 내보내려면 이 버튼을 클릭합니다.

- **내역**

  이 버튼을 클릭하면 해당 기기에 대한 애플리케이션 설치 관련 이벤트를 볼 수 있습니다. 다음 정보가 표시됩니다:

  - 애플리케이션이 기기에 설치된 날짜와 시간
  - 애플리케이션 이름
  - 애플리케이션 버전

- **속성**

  기기에 설치된 애플리케이션 목록에서 선택한 애플리케이션의 속성을 보려면 이 버튼을 클릭합니다. 다음 정보가 표시됩니다:

  - 애플리케이션 이름
  - 애플리케이션 버전
  - 애플리케이션 공급업체

실행 파일

실행 파일 섹션에는 클라이언트 기기에서 발견된 실행 파일이 표시됩니다.

자산 관리(하드웨어)

자산 관리(하드웨어) 섹션에서는 클라이언트 기기에 설치된 하드웨어에 대한 정보를 확인할 수 있습니다. Windows 기기 및 Linux 기기에 대한 정보를 확인할 수 있습니다.

하드웨어 세부 정보를 가져오려는 Linux 기기에 lshw 유틸리티가 설치되어 있는지 확인합니다. 가상 머신에서 가져온 하드웨어 세부 정보는 사용된 하이퍼바이저에 따라 불완전할 수 있습니다.

Windows를 실행하는 기기에 네트워크 에이전트를 설치했다면 기기 하드웨어에 대한 다음 정보를 중앙 관리 서버로 전송합니다.

- RAM
- 대용량 스토리지 기기
- 마더보드

- CPU
- 네트워크 어댑터
- 모니터
- 비디오 어댑터
- 사운드 카드

Linux 또는 macOS 실행하는 장치에 네트워크 에이전트를 설치했다면, 운영 체제에서 해당 정보를 제공하는 경우 장치 하드웨어에 대한 다음 정보를 중앙 관리 서버로 전송합니다.

- 총 RAM 크기
- 대용량 저장 기기의 총 크기
- 마더보드
- CPU
- 네트워크 어댑터

세션

세션 섹션은 Windows 기기에서만 표시되며 선택한 클라이언트 기기에서 작업하는 사용자의 계정에 대한 정보와 클라이언트 기기 소유자에 대한 정보가 표시됩니다.

Active Directory 데이터를 바탕으로 도메인 사용자에 대한 정보가 생성됩니다. 로컬 사용자의 세부 정보는 클라이언트 기기에 설치된 Windows 보안 계정 관리자를 통해 제공됩니다.

- **기기 소유자**

  기기 소유자 필드에는 클라이언트 기기에 대해 특정 작업을 수행해야 할 때 관리자가 연락할 수 있는 사용자 이름이 표시됩니다.

  할당 및 **속성** 버튼을 사용하면 기기 소유자를 선택하고 기기 소유자로 지정된 사용자에 대한 정보를 확인할 수 있습니다.

  빨간 십자가 모양의 버튼을 사용하여 현재 기기 소유자를 삭제합니다.

목록에는 클라이언트 기기에서 작동하는 사용자 계정이 표시됩니다.

- **이름**

  Windows 네트워크의 기기 이름.

- **참가자 이름**

  해당 기기에서 시스템에 로그온한 사용자의 이름(도메인 또는 로컬).

- **계정**

  해당 기기에 로그온한 사용자의 계정.

- **이메일**

  사용자 이메일 주소.

- **전화**

  사용자 전화 번호.

보안 문제

보안 문제 탭에서는 클라이언트 기기에 대한 보안 문제를 보고, 편집, 생성할 수 있습니다. 보안 문제는 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션을 통해 관리자가 자동 또는 수동으로 생성할 수 있습니다. 예를 들어 어떤 사용자가 정기적으로 사용자의 이동식 드라이브에서 기기로 악성 프로그램을 옮기면 관리자는 보안 문제를 만들 수 있습니다. 관리자는 보안 문제 텍스트에 해당 케이스의 요약 설명과 권장하는 작업(사용자에 대해 취할 징계 조치 등)을 제공할 수 있으며 사용자 한 명 이상에 대한 링크를 추가할 수 있습니다.

필요한 작업을 모두 수행한 보안 문제는 *처리됨*으로 분류됩니다. 기기 상태를 *심각* 또는 *경고*로 변경하기 위한 조건으로 처리 안 된 보안 문제 유무를 선택할 수 있습니다.

이 섹션에는 기기에 대해 생성된 보안 문제의 목록이 포함되어 있습니다. 보안 문제는 심각도 레벨 및 유형을 기준으로 분류됩니다. 보안 문제 유형은 보안 문제를 생성하는 Kaspersky 애플리케이션이 정의합니다. **처리됨** 열에서 확인란을 선택하여 목록에서 처리된 보안 문제를 강조할 수 있습니다.

소프트웨어 취약점

소프트웨어 취약점 섹션에는 클라이언트 기기에 설치된 타사 애플리케이션의 취약점에 대한 정보가 들어 있습니다. 목록 위의 검색 필드를 사용하여 취약점을 이름으로 찾을 수 있습니다.

- **파일로 내보내기**

  파일로 내보내기 버튼을 눌러 취약점 목록을 파일에 저장합니다. 애플리케이션은 기본적으로 취약점 목록을 CSV 파일로 내보냅니다.

- **수정할 수 있는 취약점만 표시**

  이 옵션을 사용하면 패치를 사용하여 수정할 수 있는 취약점이 섹션에 표시됩니다.

  이 옵션이 비활성화되어 있으면 패치가 릴리즈되지 않은 취약점과 패치를 사용하여 수정할 수 있는 취약점이 모두 섹션에 표시됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **속성**

  목록에서 소프트웨어 취약점을 선택하고 **속성** 버튼을 눌러 선택한 소프트웨어 취약점의 속성을 별도의 창에서 볼 수 있습니다. 이 창에서 다음을 수행할 수 있습니다:

  - 이 관리 중인 기기에서 소프트웨어 취약점을 무시합니다(관리 콘솔에서 또는 Kaspersky Security Center 웹 콘솔에서).
  - 취약점에 대한 권장 수정 사항 목록을 봅니다.
  - 취약점 수정을 위한 소프트웨어 업데이트를 수동으로 지정합니다(관리 콘솔에서 또는 Kaspersky Security Center 웹 콘솔에서).
  - 취약점 인스턴스를 봅니다.
  - 취약점을 수정하기 위해 기존 작업의 목록을 보고 취약점을 수정하기 위한 새 작업을 만듭니다.

사용 가능한 업데이트

이 섹션에는 이 기기에 있지만 아직 설치되지 않은 소프트웨어 업데이트의 목록이 표시됩니다. 선택 사항인 Microsoft Windows 업데이트에 대한 정보는 중앙 관리 서버로 전송되지 않습니다.

- **설치된 업데이트 표시**

  이 옵션을 사용하면 클라이언트 기기에 이미 설치된 업데이트 및 설치되지 않은 업데이트가 모두 목록에 표시됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

활성 정책

이 섹션에는 현재 기기에 지정된 Kaspersky 애플리케이션 정책 목록이 표시됩니다.

- **파일로 내보내기**

  파일로 내보내기 버튼을 눌러 활성 정책의 목록을 파일에 저장할 수 있습니다. 애플리케이션은 기본적으로 정책 목록을 CSV 파일로 내보냅니다.

활성 정책 프로필

- **활성 정책 프로필**

  이 목록에서는 사용자가 클라이언트 기기에서 활성된 기존 정책 프로필에 대한 정보를 볼 수 있습니다. 정책 이름이나 정책 프로필 이름을 입력하여 목록에서 활성 정책 프로필을 찾을 수 있도록 목록 위에 검색바를 사용할 수 있습니다.

- **파일로 내보내기**

  파일로 내보내기 버튼을 눌러 활성 정책 프로필의 목록을 파일에 저장할 수 있습니다. 기본적으로 애플리케이션은 CSV 파일로 정책 프로필 목록을 내보냅니다.

배포 지점

이 섹션에서는 기기가 상호 작용하는 배포 지점의 목록을 제공합니다.

- **파일로 내보내기**

  기기가 상호 작용하는 배포 지점의 목록을 파일에 저장하려면 **파일로 내보내기** 버튼을 누릅니다. 애플리케이션은 기본적으로 기기 목록을 CSV 파일로 내보냅니다.

- **속성**

  기기가 상호 작용하는 배포 지점을 보고 구성하려면 **속성** 버튼을 누릅니다.

일반 정책 설정

일반

일반 섹션에서 정책 상태를 수정하고 정책 설정에 대한 상속을 지정할 수 있습니다:

- **정책 상태** 차단에서 정책 모드 중 하나를 선택할 수 있습니다:
  - **활성 정책**

    이 옵션을 선택하면 정책이 활성화됩니다.
    기본적으로 이 옵션은 선택되어 있습니다.

  - **이동 사용자 정책**

    이 옵션을 선택하면 기기가 회사 네트워크를 벗어나는 경우 정책이 활성화됩니다.

  - **비활성 정책**

    이 옵션을 선택하면 정책이 비활성화되지만 **정책** 폴더에는 계속 저장되어 있습니다. 필요한 경우 정책을 활성화할 수 있습니다.

- **설정 상속** 설정 그룹에서는 정책 상속을 구성할 수 있습니다:
  - **부모 정책의 설정 상속**

    이 옵션을 활성화하면 상위 그룹 정책에서 정책 설정 값이 상속되므로 이 값이 잠깁니다.

기본적으로 이 옵션은 켜져 있습니다.

- **자식 정책에 설정 강제 상속**

  이 옵션을 활성화하면 정책 변경 사항이 적용된 후 다음 작업이 수행됩니다.

  - 정책 설정의 값이 관리 하위 그룹의 정책, 즉 자식 정책에 배포됩니다.
  - 각 자식 정책의 속성 창에 있는 **일반** 섹션의 **설정 상속** 블록에서 **부모 정책의 설정 상속** 옵션은 자동으로 활성화됩니다.

  이 옵션을 활성화하면 자식 정책 설정이 잠깁니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

이벤트 구성

이벤트 구성 섹션에서는 이벤트 기록과 이벤트 알림을 구성할 수 있습니다. 이벤트는 심각도 레벨에 따라 다음 탭에 배포됩니다:

- **심각**

  심각 탭은 네트워크 에이전트 정책 속성에 표시되지 않습니다.

- **기능 실패**
- **경고**
- **정보**

각 탭에서 목록에는 이벤트 유형 및 중앙 관리 서버에 기본 이벤트가 저장되는 기간(일)이 표시됩니다. **속성**버튼을 눌러 이벤트 기록과 목록에서 선택된 이벤트에 대한 알림 설정을 지정할 수 있습니다. 기본적으로 전체 중앙 관리 서버에 대해 지정된 일반 알림 설정이 모든 이벤트 유형에 사용됩니다. 그러나 필요한 이벤트 유형에 대해 특정 설정을 변경할 수 있습니다.

예를 들어, **경고** 탭에서 **보안 문제가 발생했습니다** 이벤트 유형을 구성할 수 있습니다. 이러한 이벤트는 예를 들어, 배포 지점의 여유 디스크 공간 이 2GB 미만일 때 발생할 수 있습니다(애플리케이션을 설치하고 원격으로 업데이트를 다운로드하려면 최소 4GB 필요). **보안 문제가 발생했습니다** 이벤트를 구성하려면 이를 선택하고 **속성** 버튼을 클릭하십시오. 그런 다음 발생한 이벤트를 저장할 위치와 알림 방법을 지정할 수 있습니다.

네트워크 에이전트가 보안 문제를 감지한다면 관리 중인 기기의 설정을 사용하여 이 문제를 관리할 수 있습니다.

여러 이벤트 유형을 선택하려면 **SHIFT** 또는 **CTRL** 키를 사용하십시오; 모든 유형을 선택하려면 **모두 선택** 버튼을 사용하십시오.

네트워크 에이전트 정책 설정

네트워크 에이전트 정책을 구성하려면 다음을 수행하십시오:

1. 콘솔 트리에서 **정책** 폴더를 선택합니다.
2. 폴더의 작업 영역에서 네트워크 에이전트 정책을 선택합니다.
3. 정책의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.

   네트워크 에이전트 정책의 속성 창이 열립니다.

> 운영 체제의 유형에 따라 아래 설정이 어떻게 적용되는지 자세히 설명하는 비교표를 참조하십시오.

일반

일반 섹션에서 정책 상태를 수정하고 정책 설정에 대한 상속을 지정할 수 있습니다:

- **정책 상태** 차단에서 정책 모드 중 하나를 선택할 수 있습니다:
  - **활성 정책**

    이 옵션을 선택하면 정책이 활성화됩니다.
    기본적으로 이 옵션은 선택되어 있습니다.
  - **이동 사용자 정책**

    이 옵션을 선택하면 기기가 회사 네트워크를 벗어나는 경우 정책이 활성화됩니다.
  - **비활성 정책**

    이 옵션을 선택하면 정책이 비활성화되지만 **정책** 폴더에는 계속 저장되어 있습니다. 필요한 경우 정책을 활성화할 수 있습니다.
- **설정 상속** 설정 그룹에서는 정책 상속을 구성할 수 있습니다:
  - **부모 정책의 설정 상속**

    이 옵션을 활성화하면 상위 그룹 정책에서 정책 설정 값이 상속되므로 이 값이 잠깁니다.
    기본적으로 이 옵션은 켜져 있습니다.

- **자식 정책에 설정 강제 상속**

  이 옵션을 활성화하면 정책 변경 사항이 적용된 후 다음 작업이 수행됩니다.
  - 정책 설정의 값이 관리 하위 그룹의 정책, 즉 자식 정책에 배포됩니다.
  - 각 자식 정책의 속성 창에 있는 **일반** 섹션의 **설정 상속** 블록에서 **부모 정책의 설정 상속** 옵션은 자동으로 활성화됩니다.

  이 옵션을 활성화하면 자식 정책 설정이 잠깁니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

이벤트 구성

이벤트 구성 섹션에서는 이벤트 기록과 이벤트 알림을 구성할 수 있습니다. 이벤트는 심각도 레벨에 따라 다음 탭에 배포됩니다:

- **심각**

  심각 탭은 네트워크 에이전트 정책 속성에 표시되지 않습니다.
- **기능 실패**
- **경고**
- **정보**

각 탭에서 목록에는 이벤트 유형 및 중앙 관리 서버에 기본 이벤트가 저장되는 기간(일)이 표시됩니다. **속성**버튼을 눌러 이벤트 기록과 목록에서 선택된 이벤트에 대한 알림 설정을 지정할 수 있습니다. 기본적으로 전체 중앙 관리 서버에 대해 지정된 일반 알림 설정이 모든 이벤트 유형에 사용됩니다. 그러나 필요한 이벤트 유형에 대해 특정 설정을 변경할 수 있습니다.

예를 들어, **경고** 탭에서 **보안 문제가 발생했습니다** 이벤트 유형을 구성할 수 있습니다. 이러한 이벤트는 예를 들어, 배포 지점의 여유 디스크 공간 이 2GB 미만일 때 발생할 수 있습니다(애플리케이션을 설치하고 원격으로 업데이트를 다운로드하려면 최소 4GB 필요). **보안 문제가 발생했습니다** 이벤트를 구성하려면 이를 선택하고 **속성** 버튼을 클릭하십시오. 그런 다음 발생한 이벤트를 저장할 위치와 알림 방법을 지정할 수 있습니다.

네트워크 에이전트가 보안 문제를 감지한다면 관리 중인 기기의 설정을 사용하여 이 문제를 관리할 수 있습니다.

여러 이벤트 유형을 선택하려면 **SHIFT** 또는 **CTRL** 키를 사용하십시오; 모든 유형을 선택하려면 **모두 선택** 버튼을 사용하십시오.

설정

설정 섹션에서는 네트워크 에이전트 정책을 구성할 수 있습니다:

- **배포 지점을 통해서만 파일 배포**

  이 옵션을 선택하면 관리 중인 기기의 네트워크 에이전트가 배포 지점에서만 업데이트를 검색합니다.

이 옵션이 비어 있으면 관리 중인 기기의 네트워크 에이전트가 배포 지점 또는 중앙 관리 서버에서 업데이트를 수신합니다.

관리 중인 기기의 보안 애플리케이션은 각 보안 애플리케이션의 업데이트 작업에 설정된 경로에서 업데이트를 검색합니다. **배포 지점을 통해서만 파일 배포** 옵션을 선택하면 업데이트 작업에서 Kaspersky Security Center가 업데이트 경로로 설정되어 있는지 확인하시기 바랍니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **이벤트 큐 최대 크기(MB)**

  이 필드에는 드라이브에서 이벤트 큐가 차지할 수 있는 최대 공간을 지정할 수 있습니다.

  기본값은 2MB입니다.

- **기기의 정책 확장 데이터를 가져오도록 애플리케이션 허용**

  관리 중인 기기에 설치된 네트워크 에이전트는 적용된 보안 제품 정책에 대한 정보를 보안 제품(예: Kaspersky Endpoint Security for Windows)으로 전송합니다. 보안 제품 인터페이스에서 전송된 정보를 볼 수 있습니다.

  네트워크 에이전트는 다음 정보를 전송합니다:

  - 관리 중인 기기로 정책을 전달한 시간.
  - 관리 중인 기기로 정책을 전달할 때 적용된 활성 정책의 이름.
  - 관리 중인 기기로 정책을 전달할 때 적용된 이동 사용자 정책의 이름(Linux용 네트워크 에이전트에서는 사용 불가).
  - 관리 중인 기기로 정책을 전달할 때 관리 중인 기기가 포함된 관리 그룹의 이름 및 전체 경로.
  - 관리 중인 기기로 정책을 전달할 때 적용된 활성 정책 프로필의 목록과 이름, 우선순위.

  이 정보를 기기에 올바른 정책을 적용하는 데 사용하고 문제 해결 목적으로 사용할 수도 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **무단 제거, 중지 또는 설정 변경을 하지 못하도록 네트워크 에이전트 서비스 보호**

  이 옵션이 활성화되면, 관리 중인 기기에 네트워크 에이전트를 설치한 후에 구성 요소를 제거하거나 재구성하려면 필요한 권한이 있어야 합니다. 네트워크 에이전트 서비스는 중지할 수 없습니다. 이 옵션은 도메인 컨트롤러에 영향을 주지 않습니다.

  로컬 관리자 권한으로 작동하는 워크스테이션에서 네트워크 에이전트를 보호하려면 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **제거 암호 사용**

  이 확인란을 선택하면 **수정** 버튼을 눌러 klmover 유틸리티 및 네트워크 에이전트 원격 제거를 위한 암호를 지정할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

저장소

이 **저장소** 섹션에서 네트워크 에이전트가 중앙 관리 서버로 정보를 보낼 세부 개체 유형을 선택할 수 있습니다.

- **Windows 업데이트 패치 세부 정보**

  이 옵션을 사용하면 클라이언트 기기에 설치해야 하는 Microsoft Windows 업데이트 정보가 중앙 관리 서버로 전송됩니다.

  옵션이 비활성화되더라도 **사용 가능한 업데이트** 섹션의 기기 속성에 업데이트가 표시되는 경우가 있습니다. 예를 들어, 조직의 기기에 이 업데이트로 수정 가능한 취약점이 있다면 이러한 상황이 발생할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다. Windows에서만 사용할 수 있습니다.

  선택 사항인 Microsoft Windows 업데이트에 대한 정보는 중앙 관리 서버로 전송되지 않습니다.

- **소프트웨어 취약점 및 관련 업데이트 세부 정보**

  이 옵션을 활성화하면 관리 중인 기기에서 감지된 타사 소프트웨어(Microsoft 소프트웨어 포함)의 취약점에 관한 정보와 타사 취약점(Microsoft 소프트웨어 제외)을 수정할 수 있는 소프트웨어 업데이트 관련 정보가 중앙 관리 서버로 전송됩니다.

  이 옵션(**소프트웨어 취약점 및 관련 업데이트 세부 정보**)을 선택하면 네트워크 부하, 중앙 관리 서버 디스크 부하, 네트워크 에이전트 리소스 소비량이 증가합니다.

  기본적으로 이 옵션은 켜져 있습니다. Windows에서만 사용할 수 있습니다.

  Microsoft 소프트웨어의 소프트웨어 업데이트를 관리하려면 **Windows 업데이트 패치 세부 정보** 옵션을 사용합니다.

- **자산 관리(하드웨어) 정보**

  기기에 설치된 네트워크 에이전트는 기기 하드웨어에 관한 정보를 중앙 관리 서버로 전송합니다. 기기 속성에서 하드웨어 세부 정보를 볼 수 있습니다.

  하드웨어 세부 정보를 가져오려는 Linux 기기에 lshw 유틸리티가 설치되어 있는지 확인합니다. 가상 머신에서 가져온 하드웨어 세부 정보는 사용된 하이퍼바이저에 따라 불완전할 수 있습니다.

- **자산 관리(소프트웨어) 정보**

  이 옵션을 사용하면 클라이언트 기기에 설치된 애플리케이션 정보가 중앙 관리 서버로 전송됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **패치 정보 포함**

  클라이언트 기기에 설치된 애플리케이션의 패치에 대한 정보는 중앙 관리 서버로 전송됩니다. 이 옵션을 사용하면 중앙 관리 서버 및 DBMS의 부하가 증가하고 데이터베이스 크기가 증가할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다. Windows에서만 사용할 수 있습니다.

네트워크 에이전트 정책에서 이 섹션의 일부 설정에 대한 수정이 금지된 경우에는 해당 설정을 수정할 수 없습니다.

소프트웨어 업데이트 및 취약점

소프트웨어 업데이트 및 취약점 섹션에서는 Windows 업데이트의 검색 및 배포를 구성하고 실행 파일의 취약점 검사를 활성화할 수 있습니다.

- **WSUS 서버로 이 중앙 관리 서버 사용**

  이 옵션을 사용하면, Windows 업데이트는 중앙 관리 서버에서 다운로드됩니다. 중앙 관리 서버는 네트워크 에이전트를 통해 중앙 집중식 모드에서 클라이언트 기기의 Windows 업데이트로 다운받은 업데이트를 제공합니다.

  이 옵션이 비활성화되어 있으면 중앙 관리 서버는 Windows 업데이트 다운로드 용도로 사용되지 않습니다. 이 경우 클라이언트 기기는 스스로 Windows Update를 다운로드합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **사용자가 Windows 업데이트 설치를 관리하도록 허용** 아래에서 사용자가 Windows 업데이트를 사용하여 기기에 수동으로 설치할 수 있는 Windows 업데이트를 제한할 수 있습니다.

  Windows 10을 실행하는 기기에서 Windows 업데이트가 이미 해당 기기에 대한 업데이트를 찾은 경우 **사용자가 Windows 업데이트 설치를 관리하도록 허용** 아래에서 선택한 새 옵션은 앞서 검색된 업데이트가 설치된 후에만 적용됩니다.

  드롭다운 목록에서 항목을 선택합니다:

  - **사용자가 모든 적용 가능한 Windows 업데이트 패치를 설치할 수 있도록 허용**

    사용자가 기기에 적용 가능한 모든 Microsoft Windows 업데이트를 설치할 수 있습니다.

    업데이트 설치를 방해하고 싶지 않다면 옵션을 선택합니다.

    사용자가 Microsoft Windows 업데이트를 수동으로 설치할 때는 중앙 관리 서버가 아닌 Microsoft 서버에서 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버에서 이러한 업데이트를 아직 다운로드하지 않은 경우 Microsoft 서버에서 다운로드할 수 있습니다. Microsoft 서버에서 업데이트를 다운로드하면 트래픽이 추가로 발생합니다.

  - **사용자가 승인된 Windows 업데이트 패치만 설치할 수 있도록 허용**

    사용자가 기기에 적용 가능하며 관리자가 승인한 모든 Microsoft Windows 업데이트를 설치할 수 있습니다.

예를 들어 업데이트가 기기 작동을 방해하지 않는지 테스트 환경에서 업데이트 설치를 먼저 확인한 후에만 클라이언트 기기에서 승인된 업데이트 설치를 허용할 수 있습니다.

사용자가 Microsoft Windows 업데이트를 수동으로 설치할 때는 중앙 관리 서버가 아닌 Microsoft 서버에서 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버에서 이러한 업데이트를 아직 다운로드하지 않은 경우 Microsoft 서버에서 다운로드할 수 있습니다. Microsoft 서버에서 업데이트를 다운로드하면 트래픽이 추가로 발생합니다.

- **사용자가 Windows 업데이트 패치를 설치하는 것을 허용 안 함**

  사용자가 기기에 Microsoft Windows 업데이트를 수동으로 설치할 수 없습니다. 해당하는 모든 업데이트는 관리자가 구성한 대로 설치됩니다.

  업데이트 설치를 중앙에서 관리하고 싶다면 이 옵션을 선택합니다.

  네트워크가 과부하되지 않도록 업데이트 스케줄을 최적화하려는 경우를 예로 들 수 있습니다. 사용자 생산성이 낮아지지 않도록 업무 시간 이후에 업데이트 스케줄을 지정할 수 있습니다.

- **Windows 업데이트 검색 모드** 설정 그룹에서 업데이트 검색 모드를 선택할 수 있습니다:

  - **액티브**

    이 옵션을 선택하면 네트워크 에이전트에서 지원하는 중앙 관리 서버는 클라이언트 기기의 Windows 업데이트 에이전트에서 다음과 같은 업데이트 경로로 요청을 시작합니다: Windows 업데이트 서버 또는 WSUS. 그런 다음 네트워크 에이전트가 Windows 업데이트 에이전트에서 받은 정보를 중앙 관리 서버로 전달합니다.

    취약점 및 필요한 업데이트 검색 작업의 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션이 선택된 경우에만 이 옵션이 적용됩니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **패시브**

    이 옵션을 선택하면 네트워크 에이전트가 Windows 업데이트 에이전트와 업데이트 경로 간의 마지막 동기화 시 가져온 업데이트 관련 정보를 중앙 관리 서버에 주기적으로 전달합니다. 업데이트 경로와 Windows 업데이트 에이전트의 동기화가 수행되지 않으면 중앙 관리 서버의 업데이트 정보가 최신 상태를 유지할 수 없습니다.

    업데이트 경로의 메모리 캐시에서 업데이트를 받으려면 이 옵션을 선택합니다.

  - **비활성화됨**

    이 옵션을 선택하면 중앙 관리 서버가 어떤 업데이트 관련 정보도 수집하지 않습니다.

    예를 들어, 로컬 기기에서 업데이트를 먼저 테스트하려면 이 옵션을 선택하십시오.

- **실행 파일 실행 시 취약점 검사**

  이 옵션을 사용하면 실행 파일이 실행될 때 실행 파일의 취약점을 검사합니다.

  기본적으로 이 옵션은 켜져 있습니다.

관리 다시 시작

관리 다시 시작 섹션에서는 애플리케이션의 올바른 사용, 설치, 제거를 위해 관리 중인 기기의 운영 체제를 다시 시작해야 할 때 수행할 작업을 지정할 수 있습니다.

- **운영 체제 다시 시작 안 함**

  운영 체제가 다시 시작되지 않습니다.

- **필요한 경우 운영 체제를 자동으로 다시 시작**

  필요한 경우 운영 체제가 자동으로 다시 시작됩니다.

- **사용자 확인 후 처리**

  애플리케이션에서 운영 체제를 다시 시작할지를 사용자에게 묻습니다.
  기본적으로 이 옵션은 선택되어 있습니다.

  - **지정한 시간 간격마다 물어보기(분)**

    이 옵션을 사용하면 애플리케이션이 확인란 옆의 필드에 지정한 빈도로 운영 체제를 다시 시작하도록 허용할지를 사용자에게 묻습니다. 기본적으로 이 물어보는 주기는 5분입니다.

    이 옵션이 비활성화되어 있으면 애플리케이션이 반복적인 다시 시작을 허용할지를 사용자에게 묻지 않습니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **다음 시간 이후에 강제로 다시 시작(분)**

    이 옵션을 사용하면 애플리케이션은 사용자에게 운영 체제를 다시 시작할지 물은 후 확인란 옆의 필드에 지정한 시간 간격 만료 시 운영 체제를 강제로 다시 시작합니다.

    이 옵션이 비활성화되어 있으면 애플리케이션이 운영 체제를 강제로 다시 시작하지 않습니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **잠긴 세션에서 다음 시간 후 애플리케이션 강제 종료(분)**

    사용자 기기가 잠겨 있으면 애플리케이션은 지정된 비활성 기간이 지난 후 자동으로 또는 수동으로 강제 종료됩니다.

    이 옵션을 사용하면 입력 필드에 지정된 시간 간격 만료 시 애플리케이션이 잠긴 기기에서 강제 종료됩니다.

    이 옵션이 비활성화되어 있으면 애플리케이션이 잠긴 기기에서 종료되지 않습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

Windows 데스크톱 공유

Windows Desktop Sharing 섹션에서는 데스크톱 접근 권한 공유 시 원격 기기에서 수행할 관리자 작업 감사를 사용 및 구성할 수 있습니다.

- **감사 기능 사용**

  이 옵션을 활성화하면 원격 기기에서 관리자 작업 감사가 사용됩니다. 원격 기기의 관리자 활동 기록은 다음 위치에 저장됩니다:

  - 원격 기기의 이벤트 로그에 저장
  - 원격 기기의 네트워크 에이전트 설치 폴더에 있는 확장자가 syslog인 파일
  - Kaspersky Security Center의 이벤트 데이터베이스

  다음 조건이 충족되면 관리자 작업 감사를 사용할 수 있습니다:

  - 취약점 및 패치 관리 라이센스 사용 중
  - 관리자에게 원격 기기의 데스크톱에 대한 공유 접근 시작 권한이 있는 경우

  이 옵션 확인란이 비활성화되어 있으면 원격 기기에서 관리자 작업 감사가 사용되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **읽을 때 모니터링해야 하는 파일 마스크**

  목록에는 파일 마스크가 포함됩니다. 감사를 사용하는 경우 애플리케이션은 마스크와 일치하는 관리자의 읽기 파일을 모니터링하여 파일 읽기에 대한 정보를 저장합니다. 이 필드는 **감사 기능 사용** 확인란을 선택한 경우에 사용할 수 있습니다. 파일 마스크를 편집하고 목록에 새 마스크를 추가할 수 있습니다. 새 파일 마스크는 각각 목록의 새 줄에 지정해야 합니다.

  기본적으로 지정되는 파일 마스크는 *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf입니다.

- **변경될 때 모니터링해야 하는 파일 마스크**

  목록에는 원격 기기의 파일 마스크가 포함되어 있습니다. 감사를 사용하는 경우 애플리케이션은 마스크와 일치하는 파일에서 관리자가 수행하는 변경을 모니터링하여 해당 수정에 대한 정보를 저장합니다. 이 필드는 **감사 기능 사용** 확인란을 선택한 경우에 사용할 수 있습니다. 파일 마스크를 편집하고 목록에 새 마스크를 추가할 수 있습니다. 새 파일 마스크는 각각 목록의 새 줄에 지정해야 합니다.

  기본적으로 지정되는 파일 마스크는 *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf입니다.

패치 및 업데이트 관리

이 **패치 및 업데이트 관리** 섹션에서 업데이트 다운로드, 배포, 관리 중인 기기에서의 패치 설치를 구성할 수 있습니다.

- **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치**

  이 옵션을 활성화하면 *정의 안 됨* 상태의 Kaspersky 패치가 업데이트 서버에서 다운로드된 직후 자동으로 관리 중인 기기에 설치됩니다.

  이 옵션을 비활성화하면, 다운로드되어 *정의 안 됨* 상태가 태그된 Kaspersky 패치는 그 상태를 *승인됨*으로 변경한 후에만 설치할 수 있습니다.

기본적으로 이 옵션은 켜져 있습니다.

- **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드(권장)**

  이 옵션을 활성화하면 업데이트 다운로드의 오프라인 모델이 사용됩니다. 중앙 관리 서버는 업데이트를 받을 때마다 네트워크 에이전트가 설치되어 있는 기기에서 관리 중인 애플리케이션에 대해 필요한 업데이트를 네트워크 에이전트에 통지합니다. 네트워크 에이전트가 업데이트 정보를 수신하면 중앙 관리 서버에서 미리 관련 파일을 다운로드합니다. 네트워크 에이전트와의 첫 연결에서, 중앙 관리 서버는 업데이트 다운로드를 시작합니다. 네트워크 에이전트가 모든 업데이트를 클라이언트 기기에 다운로드하고 나면 해당 기기의 애플리케이션이 업데이트를 사용할 수 있게 됩니다.

  클라이언트 기기에 있는 관리 애플리케이션이 업데이트를 위해 네트워크 에이전트에 접근하면, 이 네트워크 에이전트는 모든 필요한 업데이트가 있는지 확인합니다. 업데이트가 해당 관리 중인 애플리케이션에 대한 것이고 중앙 관리 서버에서 25시간 이내에 받은 것이라면, 네트워크 에이전트는 중앙 관리 서버에 연결하지 않고 로컬 캐시에서 해당 업데이트를 관리 중인 애플리케이션에 공급합니다. 네트워크 에이전트가 클라이언트 기기의 애플리케이션에 업데이트를 제공하는데 업데이트를 위한 연결이 필요하지 않을 때는 중앙 관리 서버와의 연결이 설정되지 않을 수 있습니다.

  이 옵션을 비활성화하면 업데이트 다운로드의 오프라인 모델이 사용되지 않습니다. 업데이트는 업데이트 다운로드 작업 스케줄에 따라 배포됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

연결성

연결성 섹션에는 하위 섹션이 세 개 있습니다:

- **네트워크**
- **연결 프로필**(Windows 및 macOS만 해당됨)
- **연결 스케줄**

네트워크 하위 섹션에서 중앙 관리 서버에 대한 연결을 구성하고 UDP 포트의 사용을 설정하며 그 포트 번호를 지정할 수 있습니다. 다음과 같은 옵션을 사용할 수 있습니다.

- **중앙 관리 서버에 연결** 설정 그룹에서 중앙 관리 서버와의 연결을 구성하고 클라이언트 기기와 중앙 관리 서버 간의 동기화 시간 간격을 지정할 수 있습니다:
  - **네트워크 트래픽 압축**

    이 옵션을 사용하면 전송되는 정보의 양이 줄어들어 중앙 관리 서버의 로드가 감소하고, 결과적으로 네트워크 에이전트의 데이터 전송 속도가 빨라집니다.

    클라이언트 컴퓨터의 CPU 사용량이 증가할 수 있습니다.

    기본적으로 이 확인란은 선택되어 있습니다.

  - **Microsoft Windows 방화벽에 네트워크 에이전트 포트 열기**

    이 옵션을 사용하면 네트워크 에이전트의 작업에 필요한 포트가 Microsoft Windows 방화벽 예외 목록에 추가됩니다.

기본적으로 이 옵션은 켜져 있습니다.

- **SSL 사용**

  이 확인란을 선택하면 SSL을 사용하여 보안 포트를 통해 중앙 관리 서버에 연결됩니다.
  기본적으로 이 옵션은 켜져 있습니다.

- **기본 연결 설정에서 배포 지점(이용 가능할 경우)의 연결 게이트웨이 사용**

  이 옵션을 사용하면 관리 그룹 속성에 지정된 설정에 따라 배포 지점의 연결 게이트웨이가 사용됩니다.
  기본적으로 이 옵션은 켜져 있습니다.

- **UDP 포트 사용**

  UDP 포트를 통해 네트워크 에이전트를 중앙 관리 서버에 연결하려면, **UDP 포트 사용** 옵션을 선택하고 **UDP 포트 번호**를 지정합니다. 기본적으로 이 옵션은 켜져 있습니다. 중앙 관리 서버에 연결하는 기본 UDP 포트는 15000입니다.

- **UDP 포트 번호**

  이 필드에는 UDP 포트 번호를 입력할 수 있습니다. 기본 포트 번호는 15000입니다.
  십진법을 사용하여 기록합니다.
  클라이언트 기기가 Windows XP 서비스 팩 2를 실행하는 경우 내장 방화벽이 UDP 포트 15000을 차단합니다. 이 포트는 수동으로 열어야 합니다.

- **배포 지점을 사용하여 중앙 관리 서버에 강제 연결**

  배포 지점 설정 창에서 **이 배포 지점을 푸시 서버로 사용**옵션을 선택한 경우 이 옵션을 선택하십시오. 그렇지 않으면 배포 지점이 푸시 서버로 작동하지 않습니다.

연결 프로필 하위 섹션에서 네트워크 위치 설정을 지정하고 중앙 관리 서버에 대한 연결 프로필을 구성하며 중앙 관리 서버를 사용할 수 없을 때 이동 사용자 모드를 활성화할 수 있습니다.

- **네트워크 위치 설정**

  네트워크 위치 설정은 클라이언트 기기가 연결된 네트워크의 특성을 정의하고 해당 네트워크 특성이 변경될 때 하나의 중앙 관리 서버 연결 프로필에서 다른 중앙 관리 서버 연결 프로필로 전환하는 네트워크 에이전트에 대한 규칙을 지정합니다.

- **중앙 관리 서버 연결 프로필**

  이 섹션에서는 중앙 관리 서버로의 네트워크 에이전트 연결에 관한 프로필을 보고 추가할 수 있습니다. 이 섹션에서 다음 이벤트가 발생했을 때 다른 중앙 관리 서버로 네트워크 에이전트를 전환하는 규칙도 만들 수 있습니다:

  - 클라이언트 기기가 다른 로컬 네트워크에 연결될 때
  - 기기가 조직의 로컬 네트워크와의 연결이 끊길 때
  - 연결 게이트웨이 주소가 변경되거나 DNS 서버 주소가 수정될 때

  연결 프로필은 Windows 및 macOS를 실행 중인 기기에서만 지원됩니다.

- **중앙 관리 서버에 연결할 수 없으면 이동 사용자 모드 사용**

  이 옵션을 사용하면 이 프로필을 통해 연결하는 경우 클라이언트 기기에 설치된 애플리케이션은 이동 사용자 정책뿐만 아니라 이동 사용자 모드에 있는 기기를 위한 정책 프로필을 사용합니다. 애플리케이션에 대해 이동 사용자 정책이 정의되어 있지 않은 경우에는 활성 정책이 사용됩니다.

  이 옵션을 비활성화하면 애플리케이션에서 활성 정책을 사용합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

이 **연결 스케줄** 하위 섹션에서는 네트워크 에이전트가 중앙 관리 서버로 데이터를 보내는 시간 간격을 지정할 수 있습니다:

- **필요 시 연결**

  이 옵션을 선택하면 네트워크 에이전트가 중앙 관리 서버로 데이터를 보내야 할 때 연결이 설정됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **지정한 시간 간격에 연결**

  이 옵션을 선택하면 네트워크 에이전트가 지정된 시간에 중앙 관리 서버와 연결됩니다. 여러 개의 연결 기간을 추가할 수 있습니다.

배포 지점

배포 지점 섹션에는 하위 섹션이 네 개 있습니다:

- **네트워크 검색**
- **인터넷 연결 설정**
- **KSN 프록시**
- **업데이트**

네트워크 검색 하위 섹션에서는 네트워크 자동 검색을 구성할 수 있습니다. 세 가지 유형의 검색, 즉 네트워크 검색, IP 범위 검색, Active Directory 검색을 활성화 할 수 있습니다:

- **네트워크 검색 사용**

  이 옵션을 사용하면 중앙 관리 서버가 **빠른 검색 스케줄 설정** 및 **상세 검색 스케줄 설정** 링크를 눌러 구성한 스케줄에 따라 자동으로 네트워크를 검색합니다.

  이 옵션이 비활성화되면 중앙 관리 서버는 **네트워크 검색 주기(분)** 필드에 지정된 간격으로 네트워크를 검색합니다.

  10.2 버전 이전의 네트워크 에이전트의 기기 발견 간격은 **Windows 도메인의 검색 주기(분)**(빠른 Windows 네트워크 검색) 및 **네트워크 검색 주기(분)**(전체 Windows 네트워크 검색) 필드에서 구성할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **IP 범위 검색 사용**

  이 확인란을 선택하면 배포 지점이 **검색 스케줄 설정** 버튼을 눌러 구성한 스케줄에 따라 자동으로 IP 범위를 검색합니다.

  이 옵션이 비활성 상태라면 배포 지점이 IP 범위를 검색하지 않습니다.

  10.2 버전 이전의 네트워크 에이전트에서 IP 범위 검색 빈도는 **검색 주기(분)** 필드에서 구성할 수 있습니다. 이 필드는 옵션을 선택한 경우에 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **Zeroconf 폴링(Linux 플랫폼에서만 작동, 수동으로 지정된 IP 범위는 무시됨)을 사용합니다**

  이 옵션을 활성화하면 배포 지점에서 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 IPv6 기기가 있는 네트워크를 자동으로 검색합니다. 이 경우 배포 지점에서 전체 네트워크를 검색하기 때문에 활성화된 IP 범위 검색이 무시됩니다.

  제로 구성을 시작하려면 다음 조건이 충족되어야 합니다.

  - 배포 지점에서 Linux를 실행해야 합니다.
  - 배포 지점에 avahi-browse 유틸리티를 설치해야 합니다.

  이 옵션이 비활성화되어 있으면 배포 지점에서 IPv6 기기가 있는 네트워크를 검색하지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **Active Directory 검색 사용**

  이 확인란을 선택하면 배포 지점이 **검색 스케줄 설정** 링크를 눌러 구성한 스케줄에 따라 자동으로 Active Directory를 검색합니다.

  이 옵션이 비활성화되어 있으면 중앙 관리 서버가 Active Directory를 검색하지 않습니다.

  10.2 버전 이전의 네트워크 에이전트에 대한 Active Directory 검색 빈도는 **검색 주기(분)** 필드에서 구성할 수 있습니다. 이 필드는 이 옵션을 선택한 경우에 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

배포 지점에서 인터넷에 연결할 때 프록시 서버를 사용하는 경우 **인터넷 연결 설정** 하위 섹션에서 다음 설정을 지정할 수 있습니다:

- **프록시 서버 사용**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 연결을 구성할 수 있습니다.
  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **프록시 서버 주소**

  프록시 서버 주소입니다.

- **포트 번호**

  연결에 사용되는 포트 번호.

- **로컬 주소에서 프록시 서버 사용 안 함**

  이 옵션을 사용하면 로컬 네트워크에서 기기로 연결하는 데 프록시 서버가 사용되지 않습니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **프록시 서버 인증**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.
  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **사용자 이름**

  프록시 서버에 대한 연결을 구성할 사용자 계정입니다.

- **암호**

  작업을 실행할 계정의 암호입니다.

KSN 프록시 하위 섹션에서는 애플리케이션이 관리 중인 기기의 KSN 요청을 전달할 때 배포 지점을 사용하도록 구성할 수 있습니다:

- **배포 지점 측에서 KSN 프록시 기능 활성화**

  배포 지점으로 사용되는 기기에서 KSN 프록시 서비스가 실행됩니다. 네트워크에서 트래픽을 재분배하고 최적화하려면 이 기능을 사용합니다.
  배포 지점은 Kaspersky Security Network 진술문에 나열된 KSN 통계를 Kaspersky에 보냅니다.
  기본적으로 이 옵션은 비활성화되어 있습니다. 중앙 관리 서버 속성 창에서 **KSN 프록시 서버로 중앙 관리 서버 사용**과 **Kaspersky Security Network 사용에 동의합니다** 옵션이 활성화되어야만 이 옵션이 활성화됩니다.

액티브-패시브 클러스터의 노드에 배포 지점을 할당하고 이 노드에 KSN 프록시 서버를 활성화할 수 있습니다.

- **중앙 관리 서버에 KSN 요청 전달**

  배포 지점이 관리 중인 기기에서 중앙 관리 서버로 KSN 요청을 전달합니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근**

  배포 지점이 관리 중인 기기에서 KSN 클라우드 또는 KPSN으로 KSN 요청을 전달합니다. 배포 지점 자체에서 생성된 KSN 요청은 KSN 클라우드 또는 KPSN으로 직접 전송됩니다.

  네트워크 에이전트 버전 11 이하가 설치된 배포 지점은 KPSN에 직접 접근할 수 없습니다. KSN 요청을 KPSN으로 전송하도록 배포 지점을 재구성하면, 각 배포 지점에 대하여 **중앙 관리 서버에 KSN 요청 전달** 옵션을 활성화합니다.

  네트워크 에이전트 버전 12 이상이 설치된 배포 지점은 KPSN에 직접 접근할 수 있습니다.

- **TCP 포트**

  관리 중인 기기가 KSN 프록시 서버에 연결하는 데 사용할 TCP 포트의 번호입니다. 기본 포트 번호는 13111입니다.

- **UDP 포트 사용**

  UDP 포트를 통해 네트워크 에이전트를 중앙 관리 서버에 연결하려면, **UDP 포트 사용** 옵션을 선택하고 **UDP 포트 번호**를 지정합니다. 기본적으로 이 옵션은 켜져 있습니다. 중앙 관리 서버에 연결하는 기본 UDP 포트는 15000입니다.

업데이트 하위 섹션에서 **diff 파일 다운로드** 옵션을 활성화 또는 비활성화하여 네트워크 에이전트가 diff 파일을 다운로드할지 지정할 수 있습니다(기본적으로 이 옵션은 켜져 있습니다).

리비전 내역

리비전 내역 탭에서 네트워크 에이전트 정책 리비전을 확인할 수 있습니다. 리비전을 비교/확인할 수 있으며 파일에 리비전 저장, 리비전으로 롤백, 리비전 설명 추가/편집 등의 고급 작업을 수행할 수 있습니다.

사용자 계정 관리

이 섹션에서는 애플리케이션이 지원하는 사용자 계정 및 역할에 대한 정보를 제공합니다. 이 섹션에는 Kaspersky Security Center의 사용자에 대해 계정과 역할을 생성하는 방법에 대한 지침이 포함되어 있습니다.

Kaspersky Security Center를 통해 사용자 계정과 계정 그룹을 관리할 수 있습니다. 이 애플리케이션은 세 종류의 계정을 지원합니다.

- 조직 직원 계정. 중앙 관리 서버는 조직 도메인 컨트롤러를 검색할 때 해당 도메인 사용자들의 계정 데이터를 검색합니다.
- 로컬 사용자 계정. 관리 중인 기기의 로컬 계정 및 중앙 관리 서버가 설치된 기기의 로컬 계정을 포함합니다.
- Kaspersky Security Center 내부 사용자 계정. 내부 사용자의 계정을 생성할 수 있습니다. 이러한 계정은 Kaspersky Security Center 내부에서만 사용됩니다.

사용자 계정 작업

Kaspersky Security Center를 통해 사용자 계정과 계정 그룹을 관리할 수 있습니다. 이 애플리케이션은 두 종류의 계정을 지원합니다:

- 조직 직원 계정. 중앙 관리 서버는 조직 네트워크를 검색할 때 해당 사용자들의 계정 데이터를 검색합니다.
- 내부 사용자 계정. 이들 계정은 가상 중앙 관리 서버가 사용될 때 적용됩니다. 내부 사용자의 계정은 Kaspersky Security Center 내에서만 생성 및 사용됩니다.

다음 방법 중 하나로 사용자 계정 목록을 볼 수 있습니다.

- 콘솔 트리에서 **고급** → **사용자 계정**으로 이동합니다.
- 콘솔 트리에서 **관리 중인 기기** → **기기** 탭 → <기기 이름> 링크 → **세션** 섹션으로 이동합니다.
  세션 섹션에 Windows를 실행하는 기기의 활성 세션이 있는 사용자 계정이 표시됩니다.

다음 요구 사항을 충족하면 사용자 계정 목록이 올바르게 표시됩니다:

- 중앙 관리 서버와 같은 버전 이상의 네트워크 에이전트를 사용합니다.
- 도메인 사용자의 계정을 표시하기 위해 Active Directory 검색이 활성화됩니다.
- Windows를 실행하는 관리 중인 기기에서 **서버(LanmanServer)** 서비스가 실행됩니다.

사용자 계정과 계정 그룹에 다음 작업을 수행합니다:

- 역할을 사용해 애플리케이션 기능에 대한 사용자의 접근 권한을 구성합니다.
- 이메일 및 SMS를 사용해 사용자에게 메시지를 보냅니다.
- 사용자의 모바일 기기 목록 봅니다.
- 사용자의 모바일 기기에 인증서를 발급하고 설치합니다.
- 사용자에게 발급된 인증서 목록을 봅니다.
- 사용자 계정에 대한 2단계 인증을 비활성화하려면.

내부 사용자의 계정 추가

Kaspersky Security Center에 새 내부 사용자 계정을 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **사용자 계정** 폴더를 엽니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. 작업 영역에서 **사용자 추가** 버튼을 누릅니다.
3. **새 사용자** 창이 열리면 새 사용자 계정의 설정을 지정합니다:
   - 사용자 이름()

     사용자 이름을 입력할 때는 주의하십시오. 변경 사항을 저장한 후에는 이름을 변경할 수 없습니다.

   - **설명**
   - **전체 이름**
   - **메인 이메일**
   - **메인 전화**
   - Kaspersky Security Center에 대한 사용자 연결을 위한 **암호**
     암호는 다음 규칙을 따라야 합니다:
     - 암호는 8자에서 256자 사이여야 합니다.
     - 암호는 아래에 나와 있는 그룹 중 3개 이상의 문자를 포함해야 합니다:
       - 대문자(A-Z)
       - 소문자(a-z)
       - 숫자(0-9)
       - 특수 문자(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 암호는 공백, 유니코드 문자 또는 "." 및 "@"의 조합("."이 "@" 앞에 오는 경우)을 포함할 수 없습니다.

     입력한 암호를 보려면 **보기** 버튼을 길게 누릅니다.

     암호 입력 시도 횟수도 제한됩니다. 기본적으로 허용된 최대 암호 입력 시도 횟수는 10번입니다. "허용되는 암호 입력 시도 횟수 변경"의 설명에 따라 암호를 입력할 수 있는 시도 횟수를 변경할 수 있습니다.

지정한 암호 입력 시도 횟수를 초과하면, 해당 사용자 계정은 1시간 동안 차단됩니다. 사용자 계정 목록에서 차단된 계정의 사용자 아이콘()은 흐리게 표시됩니다(사용 불가). 암호 변경으로만 해당 사용자 계정을 잠금 해제할 수 있습니다.

- 필요한 경우 **계정 비활성화** 확인란을 선택하여 사용자의 애플리케이션 연결을 차단합니다. 계정을 미리 만들어 두고 나중에 활성화하려는 등의 경우 계정을 비활성화할 수 있습니다.
- 무단 수정으로부터 사용자 계정을 보호하는 추가 옵션을 활성화하려면 **계정 설정이 수정될 경우 암호 요청** 확인란을 선택합니다. 이 옵션이 활성화된 경우 사용자 계정 설정을 변경하려면 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한으로 사용자를 인증해야 합니다.

4. **확인**를 누릅니다.

사용자 계정 폴더의 작업 영역에 새로 생성된 사용자 계정이 표시됩니다.

내부 사용자의 계정 편집

Kaspersky Security Center에서 내부 사용자 계정을 편집하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **사용자 계정** 폴더를 엽니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. 작업 영역에서 편집할 내부 사용자 계정을 두 번 누릅니다.
3. **속성: <사용자 이름>** 창이 열리면 사용자 계정의 설정을 변경합니다:
   - **설명**
   - **전체 이름**
   - **메인 이메일**
   - **메인 전화**
   - Kaspersky Security Center에 대한 사용자 연결을 위한 **암호**
     암호는 다음 규칙을 따라야 합니다:
     - 암호는 8자에서 256자 사이여야 합니다.
     - 암호는 아래에 나와 있는 그룹 중 3개 이상의 문자를 포함해야 합니다:
       - 대문자(A-Z)
       - 소문자(a-z)
       - 숫자(0-9)
       - 특수 문자(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - 암호는 공백, 유니코드 문자 또는 "." 및 "@"의 조합("."이 "@" 앞에 오는 경우)을 포함할 수 없습니다.

     입력한 암호를 보려면 **보기** 버튼을 길게 누릅니다.

암호 입력 시도 횟수도 제한됩니다. 기본적으로 허용된 최대 암호 입력 시도 횟수는 10번입니다. "허용되는 암호 입력 시도 횟수 변경"의 설명에 따라 암호를 입력할 수 있는 시도 횟수를 변경할 수 있습니다.

지정한 암호 입력 시도 횟수를 초과하면, 해당 사용자 계정은 1시간 동안 차단됩니다. 사용자 계정 목록에서 차단된 계정의 사용자 아이콘()은 흐리게 표시됩니다(사용 불가). 암호 변경으로만 해당 사용자 계정을 잠금 해제할 수 있습니다.

- 필요한 경우 **계정 비활성화** 확인란을 선택하여 사용자의 애플리케이션 연결을 차단합니다. 예를 들어 직원이 퇴사한 후에 계정을 비활성화할 수 있습니다.
- 무단 수정으로부터 사용자 계정을 보호하는 추가 옵션을 활성화하려면 **계정 설정이 수정될 경우 암호 요청** 옵션을 선택합니다. 이 옵션이 활성화된 경우 사용자 계정 설정을 변경하려면 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한으로 사용자를 인증해야 합니다.

4. **확인**를 누릅니다.

사용자 계정 폴더의 작업 영역에 편집된 사용자 계정이 표시됩니다.

허용되는 암호 입력 시도 횟수 변경

Kaspersky Security Center 사용자는 유효하지 않은 암호를 제한된 횟수만큼만 입력할 수 있습니다. 이 제한에 도달하면 사용자 계정은 1시간 동안 잠깁니다.

기본적으로 암호를 입력할 수 있는 최대 시도 횟수는 10회입니다. 이 섹션의 설명에 따라 허용되는 암호 입력 횟수를 변경할 수 있습니다.

허용되는 암호 입력 시도 횟수를 변경하려면 다음과 같이 하십시오:

1. 중앙 관리 서버가 설치된 기기에서 시스템 레지스트리를 엽니다(예:로컬에서 **시작** → **실행** 메뉴의 regedit 명령 사용).
2. 다음 키로 이동합니다:
   - 32비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - 64비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. SrvSplPpcLogonAttempts 값이 없으면 생성합니다. 값 유형은 DWORD입니다.
   이 값은 Kaspersky Security Center를 설치한 후에 기본적으로 생성되지 않습니다.
4. SrvSplPpcLogonAttempts 값에서 필요한 시도 횟수를 지정합니다.
5. **확인**을 눌러 변경을 저장합니다.
6. 중앙 관리 서버 서비스를 다시 시작합니다.

허용되는 암호 입력 시도의 최대 횟수가 변경됩니다.

내부 사용자 이름의 고유성을 확인하는 기능 구성

Kaspersky Security Center 애플리케이션에 내부 사용자 이름을 추가할 때 이름의 고유성 여부를 확인하도록 구성할 수 있습니다. 내부 사용자 이름의 고유성 여부 확인은 사용자 계정이 만들어지는 가상 중앙 관리 서버 또는 기본 중앙 관리 서버에서만 수행되도록 하거나, 아니면 모든 가상 중앙 관리 서버 및 기본 중앙 관리 서버에서 수행되도록 설정할 수 있습니다. 기본적으로 모든 가상 중앙 관리 서버 및 기본 중앙 관리 서버에서 내부 사용자 이름의 고유성 여부가 확인됩니다.

가상 중앙 관리 서버 또는 기본 중앙 관리 서버에서 내부 사용자 이름의 고유성 여부가 확인되도록 설정하려면 다음과 같이 하십시오:

1. 중앙 관리 서버가 설치된 기기에서 시스템 레지스트리를 엽니다(예:로컬에서 **시작 → 실행** 메뉴의 regedit 명령 사용).
2. 다음 하이브로 이동합니다:
   - 32비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 64비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. LP_InterUserUniqVsScope (DWORD) 키에서 00000001 값을 입력합니다.

   이 키에 지정된 기본값은 0입니다.
4. 중앙 관리 서버 서비스를 다시 시작합니다.

내부 사용자가 만들어진 가상 중앙 관리 서버, 아니면 기본 중앙 관리 서버에서 내부 사용자가 만들어진 경우 기본 중앙 관리 서버에서만 이름의 고유성 여부가 확인됩니다.

모든 가상 중앙 관리 서버 및 기본 중앙 관리 서버에서 내부 사용자 이름을 확인하도록 설정하려면 다음과 같이 하십시오:

1. 중앙 관리 서버가 설치된 기기에서 시스템 레지스트리를 엽니다(예:로컬에서 **시작 → 실행** 메뉴의 regedit 명령 사용).
2. 다음 하이브로 이동합니다:
   - 64비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - 32비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. LP_InterUserUniqVsScope (DWORD) 키에서 00000000 값을 입력합니다.

   이 키에 지정된 기본값은 0입니다.
4. 중앙 관리 서버 서비스를 다시 시작합니다.

이러면 모든 가상 중앙 관리 서버와 기본 중앙 관리 서버에서 이름의 고유성 여부 확인이 수행됩니다.

보안 그룹 추가

보안 그룹(사용자 그룹)을 추가할 수 있고 유연하게 그룹 및 보안 그룹을 구성할 수 있으며 다양한 애플리케이션 기능에 접근하게 할 수 있습니다. 보안 그룹에는 용도별로 해당하는 이름을 할당할 수 있습니다. 예를 들어, 이름은 사용자가 사무실 내에 있는 곳 또는 사용자가 소속된 회사 부서 이름으로 정할 수 있습니다.

한 사용자가 여러 보안 그룹에 속할 수 있습니다. 가상 중앙 관리 서버에 의해 관리되고 있는 사용자 계정은 이 가상 서버 내에 있는 보안 그룹에만 소속될 수 있으며 이 가상 서버 내에서만 접근 권한을 가집니다.

보안 그룹을 추가하려면 다음과 같이 합니다:

1. 콘솔 트리에서 **사용자 계정** 폴더를 선택합니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. **보안 그룹 추가** 버튼을 누릅니다.
   보안 그룹 추가 창이 열립니다.
3. **보안 그룹 추가** 창의 **일반** 섹션에서 그룹 이름을 지정합니다.
   규칙 이름은 255자를 초과할 수 없으며 *, <, >, ?, \, :, |와 같은 특수 문자를 사용할 수 없습니다. 그룹 이름은 중복되지 않아야 합니다.
   설명 입력 필드에 그룹 설명을 입력할 수 있습니다. **설명** 필드 작성 여부는 선택 사항입니다.
4. **확인**를 누릅니다.

추가한 보안 그룹은 콘솔 트리의 **사용자 계정** 폴더에 나타납니다. 새로 생성된 그룹에 사용자를 추가할 수 있습니다.

그룹에 사용자 추가

그룹에 사용자를 추가하려면:

1. 콘솔 트리에서 **사용자 계정** 폴더를 선택합니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. 사용자 계정 및 그룹 목록에서 사용자를 추가하고 싶은 그룹을 선택합니다.
3. 그룹 속성 창에서 **그룹 사용자** 섹션을 선택하고 **추가** 버튼을 누릅니다.
   사용자 목록이 있는 창이 열립니다.
4. 목록에서 그룹에 추가하고 싶은 사용자를 선택합니다.
5. **확인**을 누릅니다.

사용자가 그룹에 추가되고 그룹 사용자 목록에 표시됩니다.

애플리케이션 기능에 대한 접근 권한 구성. 역할 기반 접근 제어

Kaspersky Security Center는 Kaspersky Security Center 및 관리 중인 Kaspersky 애플리케이션 기능에 대한 역할 기반 접근을 위한 기능을 제공합니다.

다음 방법 중 하나로 Kaspersky Security Center 사용자를 위한 애플리케이션 기능에 대한 접근 권한을 구성할 수 있습니다.

- 각 사용자 또는 사용자 그룹에 대해 개별적으로 권한 구성.
- 사전 정의된 권한 세트를 사용하여 표준 사용자 역할을 생성한 다음 사용자의 작업 범위에 따라 해당 역할을 사용자에게 할당합니다.

사용자 역할('역할'이라고도 함)은 Kaspersky Security Center 또는 관리 중인 Kaspersky 애플리케이션의 기능에 대한 사전 정의된 접근 권한 세트입니다. 사용자 또는 사용자 그룹에 역할을 할당할 수 있습니다.

사용자 역할 적용은 애플리케이션 기능에 대한 사용자 접근 권한을 구성하는 일상적인 절차를 간소화하고 줄이기 위한 것입니다. 역할 내의 접근 권한은 표준 작업 및 사용자의 작업 범위에 따라 구성됩니다.

사용자 역할에는 개별 용도에 해당하는 이름을 할당할 수 있습니다. 애플리케이션에서 역할을 수에 제한 없이 생성할 수 있습니다.

이미 구성된 권한 세트로 사전 정의된 사용자 역할을 사용하거나 새로운 역할을 만들고 필요한 권한을 직접 구성할 수 있습니다.

애플리케이션 기능에 대한 접근 권한

아래 표는 관련 작업, 리포트, 설정을 관리하고 관련 사용자 작업을 수행할 수 있는 접근 권한이 부여된 Kaspersky Security Center 기능을 보여줍니다.

표에 나열된 사용자 작업을 수행하려면 사용자는 작업 옆에 지정된 권한이 있어야 합니다.

읽기, **쓰기**, **실행** 권한은 모든 작업, 리포트 또는 설정에 적용됩니다. 이러한 권한 외에도 사용자는 작업, 리포트 또는 기기 조회에 대한 설정을 관리하려면 **기기 선택에 대한 동작 수행** 권한이 있어야 합니다.

> 테이블에 누락된 모든 작업, 리포트, 설정 및 설치 패키지는 **일반 기능: 기본 기능** 기능 영역에 속합니다.

애플리케이션 기능에 대한 접근 권한

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
일반 기능: 관리 그룹 관리	**쓰기**	• 관리 그룹에 기기 추가: **쓰기** • 관리 그룹에서 기기 삭제: **쓰기** • 다른 관리 그룹에 관리 그룹 추가: **쓰기** • 다른 관리 그룹에서 관리 그룹 삭제: **쓰기**	없음	없음	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
일반 기능: ACL에 상관없이 개체 접근	**읽기**	모든 개체에 대한 읽기 액세스 권한 가져오기: **읽기**	없음	없음	없음
일반 기능: 기본 기능	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 가상 서버에 대한 기기 이동 규칙(생성, 수정 또는 삭제): **쓰기**, **기기 선택에 대한 동작 수행** • 모바일(LWNGT) 프로토콜 사용자 지정 인증서 가져오기: **읽기** • 모바일(LWNGT) 프로토콜 사용자 지정 인증서 설정: **쓰기** • NLA 정의 네트워크 목록 가져오기: **읽기** • NLA 정의 네트워크 목록 추가, 수정 또는 삭제: **쓰기** • 그룹 접근 제어 목록 보기: **읽기** • Kaspersky 이벤트 로그 보기: **읽기** • BitLocker로 암호화된 하드 드라이브 액세스 복원을 위한 복구 키 보기: **실행**	• "중앙 관리 서버 저장소 업데이트 다운로드" • "리포트 전달" • "설치 패키지 배포" • "보조 중앙 관리 서버에 원격으로 애플리케이션 설치"	• "보호 상태 리포트" • "위협 처리 리포트" • "가장 자주 감염된 기기 리포트(상위 10대)" • "안티 바이러스 데이터베이스 업데이트 리포트" • "오류 리포트" • "네트워크 공격 리포트" • "설치된 메일 시스템 보호 애플리케이션 요약 리포트" • "설치된 경계 방어 애플리케이션 요약 리포트" • "설치된 애플리케이션 유형에 대한 요약 리포트" • "가장 많이 감염된 기기 리포트(상위 10대)" • "인시던트 리포트" • "이벤트 리포트" • "배포 지점 활동 리포트" • "보조 중앙 관리 서버 리포트" • "매체 제어 이벤트 리포트" • "취약점 리포트" • "금지한 애플리케이션에 대한 리포트" • "웹 제어 리포트" • "관리 중인 기기의 암호화 상태 리포트" • "대용량 스토리지 기기의 암호화 상태 리포트" • "파일 암호화 오류 리포트" • "암호화된 파일로의 접근 차단 리포트" • "암호화된 기기에 대한 접근 권한 리포트" • "유효한 사용자 권한에 대한 리포트" • "권한 리포트"	없음
일반 기능: 삭제된 개체	• **읽기** • **쓰기**	• 휴지통에서 삭제된 개체 보기: **읽기** • 휴지통에서 개체 삭제: **쓰기**	없음	없음	없음
일반 기능: 이벤트 처리	• **이벤트 삭제** • **이벤트 알림 설정 편집** • **이벤트 로그 기록 설정 편집** • **쓰기**	• 이벤트 등록 설정 변경: **이벤트 로그 기록 설정 편집** • 이벤트 알림 설정 변경: **이벤트 알림 설정 편집** • 이벤트 삭제: **이벤트 삭제**	없음	없음	설정: • 바이러스 급증 설정: 바이러스 급증 이벤트를 생성하는 데 필요한 바이러스 탐지 수 • 바이러스 급증 설

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
					정: 바이러스 탐지 평가 기간 • 데이터베이스에 저장되는 최대 이벤트 수 • 삭제된 기기에서 이벤트를 저장하는 기간
일반 기능: 중앙 관리 서버에서의 동작	• **읽기** • **쓰기** • **실행** • **개체 ACL 수정** • **기기 선택에 대한 동작 수행**	• 네트워크 에이전트 연결을 위한 중앙 관리 서버의 포트 지정: **쓰기** • 중앙 관리 서버에 실행된 활성화 프록시의 포트 지정: **쓰기** • 중앙 관리 서버에 실행된 모바일용 활성화 프록시의 포트 지정: **쓰기** • 독립형 패키지 배포를 위한 웹 서버의 포트 지정: **쓰기** • MDM 프로필 배포를 위한 웹 서버의 포트 지정: **쓰기** • Kaspersky Security Center 웹 콘솔을 통한 연결용 중앙 관리 서버 SSL 포트 지정: **쓰기** • 모바일 연결을 위한 중앙 관리 서버의 포트 지정: **쓰기** • 중앙 관리 서버 데이터베이스에 저장되는 최대 이벤트 수 변경: **쓰기** • 중앙 관리 서버에서 보낼 수 있는 최대 이벤트 수 지정: **쓰기** • 중앙 관리 서버에서 이벤트를 보낼 수 있는 기간 지정: **쓰기**	• "중앙 관리 서버 데이터 백업" • "데이터베이스 점검"	없음	없음
일반 기능: Kaspersky 애플리케이션 배포	• **Kaspersky 패치 관리** • **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	패치 설치 승인 또는 거부: **Kaspersky 패치 관리**	없음	• "가상 중앙 관리 서버의 라이센스 키 사용에 대한 보고" • "Kaspersky 소프트웨어 버전 리포트" • "비-호환 애플리케이션 리포트" • "Kaspersky 소프트웨어 모듈 업데이트 리포트" • "보호 배포 리포트"	설치 패키지: "Kaspersky"
일반 기능: 라이센스 키 관리	• **키 파일 내보내기** • **쓰기**	• 키 파일 내보내기: **키 파일 내보내기** • 중앙 관리 서버 라이센스 키 설정 수정: **쓰기**	없음	없음	없음
일반 기능: 강제 리포트 관리	• **읽기** • **쓰기**	• ACL에 상관없이 리포트 생성: **쓰기** • ACL에 상관없이 리포트 실행: **읽기**	없음	없음	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
일반 기능: 중앙 관리 서버 계층 구조	**중앙 관리 서버 계층 구조 구성**	보조 중앙 관리 서버 등록, 업데이트 또는 삭제: **중앙 관리 서버 계층 구조 구성**	없음	없음	없음
일반 기능: 사용자 권한	**개체 ACL 수정**	• 모든 개체의 보안 속성 변경: **개체 ACL 수정** • 사용자 역할 관리: **개체 ACL 수정** • 내부 사용자 관리: **개체 ACL 수정** • 보안 그룹 관리: **개체 ACL 수정** • 별칭 관리: **개체 ACL 수정**	없음	없음	없음
일반 기능: 가상 중앙 관리 서버	• **가상 중앙 관리 서버 관리** • **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 가상 중앙 관리 서버 목록 가져 오기: **읽기** • 가상 중앙 관리 서버에 대한 정보 가져오기: **읽기** • 가상 중앙 관리 서버 생성, 업데이트 또는 삭제: **가상 중앙 관리 서버 관리** • 가상 중앙 관리 서버를 다른 그룹으로 이동: **가상 중앙 관리 서버 관리** • 가상 중앙 관리 서버 권한 설정: **가상 중앙 관리 서버 관리**	없음	"타사 소프트웨어 업데이트 설치 결과 보고"	없음
일반 기능: 암호화 키 관리	• **읽기** • **쓰기**	• 암호화 키 내보내기: **읽기** • 암호화 키 가져오기: **쓰기**	없음	없음	없음
모바일 기기 관리: 일반	• **새 기기 연결** • **모바일 기기에 정보 명령만 보내기** • **모바일 기기에 명령 전송** • **인증서 관리** • **읽기** • **쓰기**	• 키 관리 서비스 복원 데이터 가져오기: **읽기** • 사용자 인증서 삭제: **인증서 관리** • 사용자 인증서 공개 부분 가져오기: **읽기** • 공개 키 인프라 활성화 여부 확인: **읽기** • 공개 키 인프라 계정 확인: **읽기** • 공개 키 인프라 템플릿 가져오기: **읽기** • 확장 키 사용 인증서로 공개 키 인프라 템플릿 가져오기: **읽기** • 공개 키 인프라 인증서 취소 여부 확인: **읽기** • 사용자 인증서 발급 설정 업데이트: **인증서 관리** • 사용자 인증서 발급 설정 가져오기: **읽기** • 애플리케이션 이름 및 버전별 패키지 가져오기: **읽기** • 사용자 인증서 설정 또는 취소: **인증서 관리** • 사용자 인증서 갱신: **인증서 관리** • 사용자 인증서 태그 설정: **인증서 관리** • MDM 설치 패키지 생성 실행, MDM 설치 패키지 생성 취소: **새 기기 연결**	없음	없음	없음
시스템 관리: 연결성	• **RDP 세션 시작** • **기존 RDP 세션에 연결**	• 데스크톱 공유 세션 생성: **RDP 세션 시작** • RDP 세션 생성: **기존**	없음	"기기 사용자에 대한 리포트"	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
	• **터널링 시작** • **기기에서 관리자의 워크스테이션에 파일 저장** • **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	**RDP 세션에 연결** • 터널 생성: **터널링 시작** • 컨텐츠 네트워크 목록 저장: **기기에서 관리자의 워크스테이션에 파일 저장**			
시스템 관리: 하드웨어 인벤토리	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 하드웨어 인벤토리 개체 가져오기 또는 내보내기: **읽기** • 하드웨어 인벤토리 개체 추가, 설정 또는 삭제: **쓰기**	없음	• "자산 관리(하드웨어) 리포트" • "하드웨어 자산 변경 사항 리포트" • "하드웨어 리포트"	없음
시스템 관리: 네트워크 접근 제어	• **읽기** • **쓰기**	• CISCO 설정 보기: **읽기** • CISCO 설정 변경: **쓰기**	없음	없음	없음
시스템 관리: 운영 체제 배포	• **PXE 서버 배포** • **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• PXE 서버 배포: **PXE 서버 배포** • PXE 서버 목록 보기: **읽기** • PXE 클라이언트에서 설치 프로세스 시작 또는 중지: **실행** • WinPE 드라이버 및 운영 체제 이미지 관리: **쓰기**	"참조 기기 OS 이미지에 설치 패키지 생성"	없음	설치 패키지: "OS 이미지"
시스템 관리: 취약점 및 패치 관리	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 타사 패치 속성 보기: **읽기** • 타사 패치 속성 변경: **쓰기**	• "Windows 업데이트 동기화 수행" • "Windows Update 업데이트 설치" • "취약점 수정" • "필요한 업데이트를 설치하고 취약점 수정"	"소프트웨어 업데이트 리포트"	없음
시스템 관리: 원격 설치	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 타사 취약점 및 패치 관리 기반 설치 패키지 속성 보기: **읽기** • 타사 취약점 및 패치 관리 기반 설치 패키지 속성 변경: **쓰기**	없음	없음	설치 패키지: • "사용자 지정 애플리케이션" • "VAPM 패키지"
시스템 관리: 소프트웨어 인벤토리	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	없음	없음	• "자산 관리(소프트웨어) 리포트" • "자산 관리(소프트웨어) 기록 리포트" • "유료 애플리케이션 그룹 상태에 대한 리포트" • "타사 소프트웨어 라이센스 키에 대한 리포트"	없음

사전 정의된 사용자 역할

Kaspersky Security Center 사용자에게 할당된 사용자 역할은 사용자에게 애플리케이션 기능에 대한 접근 권한 세트를 제공합니다.

가상 서버에서 생성된 사용자에게는 중앙 관리 서버의 역할을 할당할 수 없습니다.

미리 구성된 권한 세트로 사전 정의된 사용자 역할을 사용하거나 새로운 역할을 생성할 수 있습니다. 새 역할을 만들 경우, 직접 Kaspersky Security Center 기능에 대한 역할 범위를 설정하고 접근 권한을 할당해야 합니다. Kaspersky Security Center에서 사용할 수 있는 사전 정의된 사용자 역할 중 일부는 **감사관**, **보안 책임자**, **감독관** 등과 같은 특정 직책과 연관될 수 있습니다(이러한 역할은 Kaspersky Security Center 버전 11부터 제공). 이러한 역할의 접근 권한은 관련 직책의 표준 작업 및 직무 범위에 따라 미리 구성됩니다. 아래 표는 특정 직책과 역할이 어떻게 연관되는지 보여줍니다.

특정 직책별 역할의 예

역할	메모
감사관	로컬 관리자 권한(Linux에서는 루트)으로 네트워크 에이전트를 통해 중앙 관리 서버에 연결된 기기에서 모든 보기 작업과 생성된 작업의 실행을 허용합니다. 이 역할은 공식 업무 수행에 해당 역할이 필요한 사용자에게만 제한적으로 신중하게 할당하는 것이 좋습니다.
감독관	모든 보기 작업이 허용되며 다른 작업은 허용되지 않습니다. 조직의 IT 보안을 담당하는 보안 책임자 및 기타 관리자에게 이 역할을 할당할 수 있습니다.
보안 운영자	모든 보기 작업과 리포트 관리가 허용되며 **시스템 관리**: **연결성** 영역에 제한된 권한을 부여합니다. 조직의 IT 보안을 담당하는 운영자에게 이 역할을 할당할 수 있습니다.

아래 표는 미리 정의된 각 사용자 역할에 할당된 접근 권한을 보여줍니다.

미리 정의된 사용자 역할의 접근 권한

역할	설명

중앙 관리 서버 관리자	다음 기능 영역의 모든 작업을 허용합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **이벤트 처리**
	  • **중앙 관리 서버 계층 구조**
	  • **가상 중앙 관리 서버**
	• **시스템 관리**:
	  • **연결성**
	  • **하드웨어 인벤토리**
	  • **소프트웨어 인벤토리**
	일반 기능: 암호화 키 관리 기능 영역에 **읽기** 및 **쓰기** 권한을 부여합니다.

역할	설명

중앙 관리 서버 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **가상 중앙 관리 서버**
	• **시스템 관리**:
	  • **연결성**
	  • **하드웨어 인벤토리**
	  • **소프트웨어 인벤토리**

감사관	**일반 기능**에서 기능 영역에서의 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **삭제된 개체** • **강제 리포트 관리** 조직 감사를 수행하는 사용자에게 이 역할을 할당할 수 있습니다.

설치 관리자	다음 기능 영역의 모든 작업을 허용합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **Kaspersky 소프트웨어 배포**
	  • **라이센스 키 관리**
	• **시스템 관리**:
	  • **운영 체제 배포**
	  • **취약점 및 패치 관리**
	  • **원격 설치**
	  • **소프트웨어 인벤토리**
	일반 기능: 가상 중앙 관리 서버 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다.

설치 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **Kaspersky 소프트웨어 배포**(이 영역에 **Kaspersky 패치 관리** 권한도 부여)
	  • **가상 중앙 관리 서버**
	• **시스템 매니지먼트**:
	  • **운영 체제 배포**
	  • **취약점 및 패치 관리**
	  • **원격 설치**
	  • **소프트웨어 인벤토리**

Kaspersky Endpoint Security 관리자	다음 기능 영역의 모든 작업을 허용합니다. • **일반 기능: 기본 기능** • Kaspersky Endpoint Security 영역(모든 기능 포함) **일반 기능: 암호화 키 관리** 기능 영역에 **읽기** 및 **쓰기** 권한을 부여합니다.
Kaspersky Endpoint Security 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다. • **일반 기능: 기본 기능** • Kaspersky Endpoint Security 영역(모든 기능 포함)

역할	설명
메인 관리자	**일반 기능**에서 다음 영역을 *제외한* 기능 영역의 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **강제 리포트 관리** **일반 기능: 암호화 키 관리** 기능 영역에 **읽기** 및 **쓰기** 권한을 부여합니다.

메인 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다(해당하는 경우).
	• **일반 기능**:
	  • **기본 기능**
	  • **삭제된 개체**
	  • **중앙 관리 서버에서의 동작**
	  • **Kaspersky 애플리케이션 배포**
	  • **가상 중앙 관리 서버**
	• **모바일 기기 관리: 일반**
	• **시스템 관리**(모든 기능 포함)
	• Kaspersky Endpoint Security 영역(모든 기능 포함)

모바일 기기 관리 관리자	다음 기능 영역의 모든 작업을 허용합니다. • **일반 기능: 기본 기능** • **모바일 기기 매니지먼트: 일반**
모바일 기기 관리 운영자	**일반 기능**: **기본 기능** 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다. **모바일 기기 관리**: **일반**에서 **읽기** 및 **모바일 기기에 정보 명령만 보내기** 권한을 부여합니다.
보안 운영자	**일반 기능**의 다음 기능 영역에서 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **강제 리포트 관리** **시스템 관리: 연결성** 기능 영역에 **읽기**, **쓰기**, **실행**, **기기의 파일을 관리자 워크스테이션에 저장** 및 **기기 조회에 대한 동작 수행** 권한을 부여합니다. 조직의 IT 보안을 담당하는 운영자에게 이 역할을 할당할 수 있습니다.
셀프 서비스 포털 사용자	**모바일 기기 관리: 셀프 서비스 포털** 기능 영역의 모든 작업을 허용합니다. 이 기능은 Kaspersky Security Center 11 이상 버전에서 지원되지 않습니다.
감독관	**일반 기능**: **ACL에 상관없이 개체 접근** 및 **일반 기능**: **강제 리포트 관리** 기능 영역에 **읽기** 권한을 부여합니다. 조직의 IT 보안을 담당하는 보안 책임자 및 기타 관리자에게 이 역할을 할당할 수 있습니다.
취약점 및 패치 관리 관리자	**일반 기능**: **기본 기능** 및 **시스템 관리**(모든 기능 포함) 기능 영역의 모든 작업을 허용합니다.
취약점 및 패치 관리 운영자	**일반 기능**: **기본 기능** 및 **시스템 관리** (모든 기능 포함) 기능 영역에 **읽기 및 실행**(해당된다면) 권한을 부여합니다.

사용자 역할 추가

사용자 역할을 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **섹션** 창에서 **사용자 역할**를 선택하고 **추가** 버튼을 누릅니다.

사용자 역할 섹션은 **보안 설정 섹션 표시** 옵션이 활성화되어 있으면 사용할 수 있습니다.

4. **새 역할** 속성 창에서 역할을 구성합니다:

   - **섹션**에서 **일반**을 선택하고 역할의 이름을 지정합니다.
     역할 이름은 100자를 초과할 수 없습니다.
   - **권한** 섹션을 선택하고 애플리케이션 기능 옆의 **허락** 및 **거부** 확인란을 선택하여 권한 세트를 구성합니다.

   기본 중앙 관리 서버에서 작업하는 경우 **보조 중앙 관리 서버로 역할 목록 전달** 옵션을 활성화할 수 있습니다.

5. **확인**를 누릅니다.

역할이 추가됩니다.

중앙 관리 서버용으로 생성된 사용자 역할은 중앙 관리 서버 속성 창의 **사용자 역할** 섹션에 표시됩니다. 사용자 역할을 수정하고 삭제할 수 있을 뿐 아니라 선택한 사용자 또는 보안 그룹에 역할을 할당할 수 있습니다.

사용자 또는 보안 그룹에 역할 할당

사용자 또는 사용자 그룹에 역할을 할당하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창에서 **보안** 섹션을 선택합니다.

   보안 섹션은 인터페이스 설정 창에서 **보안 설정 섹션 표시** 확인란을 선택하면 사용할 수 있습니다.

4. **그룹 또는 사용자 이름** 필드에서 역할을 할당하려는 사용자 또는 사용자 그룹을 선택합니다.
   사용자 또는 그룹이 필드에 포함되어 있지 않으면 **추가** 버튼을 눌러 추가할 수 있습니다.
   추가 버튼을 눌러 사용자를 **추가**할 때 사용자 인증 유형(Microsoft Windows 또는 Kaspersky Security Center)을 선택할 수 있습니다. 가상 중앙 관리 서버 처리에 사용되는 내부 사용자 계정을 선택할 때는 Kaspersky Security Center 인증을 사용합니다.
5. **역할** 탭을 선택하고 **추가** 버튼을 누릅니다.
   사용자 역할 창이 열립니다. 이 창에는 생성된 사용자 역할이 표시됩니다.
6. **사용자 역할** 창에서 보안 그룹에 대한 역할을 선택합니다.
7. **확인**을 클릭합니다.

중앙 관리 서버 작업을 위한 권한 세트가 있는 역할이 사용자 또는 보안 그룹에 할당됩니다. 할당된 역할은 중앙 관리 서버 속성 창 **보안** 섹션의 **역할** 탭에 표시됩니다.

사용자 및 그룹에 권한 할당

사용자와 그룹에 중앙 관리 서버 및 관리 플러그인을 설치한 Kaspersky 프로그램(예: Kaspersky Endpoint Security for Windows)의 다른 기능을 사용할 권한을 제공할 수 있습니다.

사용자 또는 사용자 그룹에 권한을 할당하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 다음 중 하나를 수행합니다:
   - **중앙 관리 서버** 노드를 확장하고 필요한 중앙 관리 서버의 이름이 지정된 하위 폴더를 선택합니다.
   - 관리 그룹을 선택합니다.
2. 중앙 관리 서버 또는 관리 그룹의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창이나 관리 그룹 속성 창이 열리면 왼쪽 **섹션** 창에서 **보안**을 선택합니다.

   > **보안** 섹션은 인터페이스 설정 창에서 **보안 설정 섹션 표시** 확인란을 선택하면 사용할 수 있습니다.

4. **보안** 섹션의 **그룹 또는 사용자 이름** 목록에서 사용자나 그룹을 선택합니다.
5. 작업 영역 아래쪽 권한 목록의 **권한** 탭에서 사용자나 그룹의 권한 세트를 구성합니다:
   a. 더하기 기호(+)를 눌러 목록의 노드를 확장하고 권한에 액세스합니다.
   b. 원하는 권한 옆의 **허락** 및 **거부** 확인란을 선택합니다.
   예 1: **ACL에 상관없이 개체 접근** 노드 또는 **삭제된 개체** 노드를 확장하고 **읽기**를 선택합니다.
   예 2: **기본 기능** 노드를 확장하고 **쓰기**를 선택합니다.
6. 권한 세트를 구성한 후 **적용**를 누릅니다.

사용자나 사용자 그룹에 대한 권한 세트가 구성됩니다.

중앙 관리 서버 또는 관리 그룹의 권한은 다음 영역으로 구분됩니다:

- 일반 기능:
  - 관리 그룹 관리
  - ACL에 상관없이 개체 접근
  - 기본 기능
  - 삭제된 개체
  - 이벤트 처리
  - 중앙 관리 서버에서의 동작(중앙 관리 서버의 속성 창에만 있음)
  - Kaspersky 애플리케이션 배포
  - 라이센스 키 관리
  - 강제 리포트 관리
  - 서버 계층 구조

    - 사용자 권한
    - 가상 중앙 관리 서버
- 모바일 기기 관리:
    - 일반
- 시스템 관리:
    - 연결성
    - 하드웨어 인벤토리
    - 네트워크 접근 제어
    - 운영 체제 배포
    - 취약점 및 패치 관리
    - 원격 설치
    - 소프트웨어 인벤토리

권한에서 **허락**나 **거부**를 모두 선택하지 않으면 해당 권한은 *정의 안 됨*으로 간주되며 사용자에 대해 명시적으로 거부되거나 허락될 때까지는 거부됩니다.

사용자 권한은 다음 권한의 합입니다:

- 사용자의 고유 권한
- 이 사용자에게 할당된 모든 역할의 권한
- 사용자가 속한 모든 보안 그룹의 권한
- 사용자가 속한 보안 그룹에 할당된 모든 역할의 권한

이러한 권한 세트 중 하나 이상에서 권한 상태가 **거부**인 경우에는 다른 세트에서 해당 권한이 허용 또는 미정의 상태여도 사용자의 해당 권한 사용은 거부됩니다.

보조 중앙 관리 서버에 사용자 역할 전파

기본적으로 기본 및 보조 중앙 관리 서버의 사용자 역할 목록은 서로 독립적입니다. 기본 중앙 관리 서버에서 생성된 사용자 역할을 모든 보조 중앙 관리 서버에 자동으로 전파하도록 애플리케이션을 구성할 수 있습니다. 보조 중앙 관리 서버에서 자체 보조 중앙 관리 서버로 사용자 역할을 전파할 수도 있습니다.

기본 중앙 관리 서버에서 보조 중앙 관리 서버로 사용자 역할을 전파하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창을 엽니다.
2. 다음 중 하나를 수행합니다:
   - 콘솔 트리에서 중앙 관리 서버의 이름을 마우스 오른쪽 버튼으로 누르고 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 활성 중앙 관리 서버 정책이 있는 경우 **정책** 폴더의 작업 영역에서 이 정책을 마우스 오른쪽 버튼으로 누르고 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창이나 정책 설정 창의 **섹션** 창에서 **사용자 역할**을 선택합니다.

   사용자 역할 섹션은 **보안 설정 섹션 표시** 옵션이 활성화되어 있으면 사용할 수 있습니다.

4. **보조 중앙 관리 서버로 역할 목록 전달** 옵션을 활성화합니다.
5. **확인**을 누릅니다.

   애플리케이션이 기본 중앙 관리 서버에서 보조 중앙 관리 서버로 사용자 역할을 복사합니다.

보조 중앙 관리 서버로 역할 목록 전달 옵션이 활성화된 상태에서 전파하는 사용자 역할은 보조 중앙 관리 서버에서 편집하거나 삭제할 수 없습니다. 기본 중앙 관리 서버에서 새 역할을 생성하거나 기존 역할을 편집하면 변경 내용이 보조 중앙 관리 서버에 자동으로 복사됩니다. 기본 중앙 관리 서버에서 삭제하는 사용자 역할은 삭제 후에도 보조 중앙 관리 서버에 남아 있지만 편집되거나 삭제될 수 있습니다.

기본 중앙 관리 서버에서 보조 중앙 관리 서버로 전파되는 역할에는 자물쇠 아이콘()이 표시됩니다. 이러한 역할은 보조 중앙 관리 서버에서 편집할 수 없습니다.

기본 중앙 관리 서버에서 역할을 생성했는데 보조 중앙 관리 서버에 이름이 같은 역할이 있으면 새 역할은 이름에 ~~1, ~~2와 같은 색인(랜덤일 수 있음)이 추가되어 보조 중앙 관리 서버로 복사됩니다.

보조 중앙 관리 서버로 역할 목록 전달 옵션을 비활성화하면 모든 사용자 역할은 보조 중앙 관리 서버에 유지되지만 기본 중앙 관리 서버와의 역할과는 독립적인 역할이 됩니다. 독립적인 역할이 된 보조 중앙 관리 서버의 사용자 역할은 편집하거나 삭제할 수 있습니다.

기기 소유자로 특정 사용자 지정

특정 사용자에게 기기를 할당하기 위해 기기 소유자로 해당 사용자를 지정할 수 있습니다. 기기에 어떤 작업을 내려야 한다면(예, 소프트웨어 업그레이드), 관리자는 기기 소유자가 작업을 수행할 수 있도록 알림을 보낼 수 있습니다.

사용자를 기기의 소유자로 지정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 선택합니다.
2. 해당 폴더의 작업 영역에 있는 **기기** 탭에서 소유자를 지정해야 하는 기기를 선택합니다.
3. 기기의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
4. 기기 속성 창에서 **시스템 정보** → **세션**를 선택합니다.

5. **기기 소유자** 필드 옆에 있는 **할당** 버튼을 누릅니다.

6. **사용자 선택** 창에서 기기 소유자로 지정하고 싶은 사용자를 선택하고 **확인**를 누릅니다.

7. **확인**를 누릅니다.

기기 소유자가 지정되었습니다. 기본적으로 **기기 소유자** 필드는 Active Directory에서 가져온 값으로 채워지고 Active Directory 검색이 수행될 때마다 업데이트됩니다. **기기 소유자에 대한 리포트**에서 기기 소유자 목록을 확인할 수 있습니다. 새 리포트 템플릿 마법사를 이용해 리포트를 생성할 수 있습니다.

공지 메시지 배포

이메일로 사용자에게 메시지를 보내려면 다음과 같이 하십시오:

1. 콘솔 트리의 **사용자 계정** 폴더에서 사용자를 선택합니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.

2. 사용자의 마우스 오른쪽 메뉴에서 **이메일로 알림**을 선택합니다.

3. **메시지 배포** 창에서 관련 필드에 내용을 입력하고 **확인** 버튼을 누릅니다.

   그러면 사용자 속성에 지정된 이메일 주소로 메시지를 전송합니다.

이메일로 SMS 메시지를 보내려면 다음과 같이 하십시오:

1. 콘솔 트리의 **사용자 계정** 폴더에서 사용자를 선택합니다.

2. 사용자의 마우스 오른쪽 메뉴에서 **SMS 전송**을 선택합니다.

3. **SMS 문자** 창에서 관련 필드에 내용을 입력하고 **확인** 버튼을 누릅니다.

   그러면 사용자 속성에 지정된 번호의 모바일 기기로 메시지를 전송합니다.

사용자 모바일 기기 목록 보기

사용자의 모바일 기기 목록을 보려면, 다음과 같이 하십시오:

1. 콘솔 트리의 **사용자 계정** 폴더에서 사용자를 선택합니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.

2. 사용자 계정의 컨텍스트 메뉴에서 **속성**을 선택합니다.

3. 사용자 계정 속성 창에서 **모바일 기기** 섹션을 선택합니다.

모바일 기기 섹션에서 사용자 모바일 기기 목록 및 각 기기에 대한 정보를 확인할 수 있습니다. **파일로 내보내기** 버튼을 눌러 모바일 기기 목록을 파일에 저장할 수 있습니다.

사용자용 인증서 설치

사용자에 대해 세 가지 유형의 인증서를 설치할 수 있습니다:

- 사용자 모바일 기기를 식별하는 데 필요한 공유 인증서.
- 사용자 모바일 기기에서 회사 메일을 설정하는 데 필요한 메일 인증서.
- 사용자 모바일 기기에서 가상 사설망을 설정하는 데 필요한 VPN 인증서.

사용자에게 인증서를 발급한 후 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **사용자 계정** 폴더를 열고 사용자 계정을 선택합니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. 사용자 계정의 컨텍스트 메뉴에서 **인증서 설치**를 선택합니다.

그러면 인증서 설치 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

인증서 설치 마법사가 완료되면 사용자에 대해 인증서가 생성 및 설치됩니다. 설치된 사용자 인증서 목록을 확인하고 파일로 내보낼 수 있습니다.

사용자에게 발급된 인증서 목록 보기

사용자에게 발급된 모든 인증서의 목록을 보려면 다음과 같이 하십시오:

1. 콘솔 트리의 **사용자 계정** 폴더에서 사용자를 선택합니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. 사용자 계정의 컨텍스트 메뉴에서 **속성**을 선택합니다.
3. 사용자 계정 속성 창에서 **인증서** 섹션을 선택합니다.

인증서 섹션에서 사용자 인증서 목록 및 각 인증서에 대한 정보를 확인할 수 있습니다. **파일로 내보내기** 버튼을 눌러 인증서 목록을 파일에 저장할 수 있습니다.

가상 중앙 관리 서버의 관리자 정보

가상 중앙 관리 서버를 통해 관리되는 기업 네트워크의 관리자는 이 창에 지정된 사용자 계정으로 Kaspersky Security Center 웹 콘솔을 시작하여 안티 바이러스 보호의 세부 정보를 확인합니다.

필요한 경우 한 가상 서버에 여러 개의 관리자 계정을 만들 수 있습니다.

가상 서버에서 생성된 사용자에게는 중앙 관리 서버의 역할을 할당할 수 없습니다.

가상 중앙 관리 서버의 관리자는 Kaspersky Security Center의 내부 사용자입니다. 내부 사용자에 대한 어떤 데이터도 운영 체제로 전송되지 않습니다. Kaspersky Security Center에서 내부 사용자를 인증합니다.

운영 체제와 애플리케이션의 원격 설치

Kaspersky Security Center를 사용하면 운영 체제의 이미지를 만들어 네트워크에 있는 클라이언트 기기에 배포하고 Kaspersky 또는 다른 공급업체에 의해 애플리케이션의 원격 설치를 수행할 수 있습니다.

운영 체제의 이미지를 생성하려면 중앙 관리 서버에 Windows ADK 배포 도구 및 Windows ADK용 Windows PE 추가 기능 도구를 설치해야 합니다. Kaspersky Security Center 요구 사항을 충족하는 모든 버전의 Windows 운영 체제 이미지를 생성할 수 있습니다.

Kaspersky Security Center 64비트 버전의 Windows ADK 및 Windows PE를 지원하지 않습니다.

운영 체제의 이미지 캡처

Kaspersky Security Center는 대상 기기에서 운영 체제의 이미지를 캡처하여 중앙 관리 서버에 해당 이미지를 전송할 수 있습니다. 운영 체제의 이러한 이미지는 중앙 관리 서버의 전용 폴더에 저장됩니다. 참조 기기의 운영 체제 이미지가 캡처된 다음 설치 패키지 만들기 작업을 통해 만들어집니다.

운영 체제 이미지의 캡처 기능은 다음과 같은 특징을 가지고 있습니다:

- 중앙 관리 서버가 설치된 기기의 운영 체제 이미지는 캡처할 수 없습니다.
- 운영 체제 이미지를 캡처하는 동안 sysprep.exe 유틸리티가 참조 기기의 설정을 초기화합니다. 참조 기기의 설정을 초기화하려면 운영 체제 이미지 작업 생성 마법사의 **기기 상태 백업 복사본 생성(시간이 오래 걸림)** 확인란을 선택합니다.
- 이미지를 캡처하는 프로세스는 참조 기기의 재시작을 준비합니다.

새 기기에 운영 체제의 이미지 배포

이미지를 사용해 아직 운영 체제가 설치되지 않은 새 네트워크 기기에 배포할 수 있습니다. 이 경우 Preboot eXecution Environment(PXE) 기술이 사용됩니다. PXE 서버 역할을 할 네트워크 기기를 선택합니다. 이 기기는 다음 요구 사항을 충족해야 합니다:

- 네트워크 에이전트가 기기에 설치되어야 합니다.
- PXE 서버가 DHCP 서버와 동일한 포트를 사용하기 때문에 DHCP 서버가 해당 기기에 활성화되어 있지 않아야 합니다.
- 기기를 포함하는 네트워크 세그먼트에 다른 PXE 서버가 없어야 합니다.

운영 체제를 배포하려면 다음 조건이 충족되어야 합니다.

- 네트워크 카드가 기기에 장착되어 있어야 합니다.
- 기기가 네트워크에 연결되어 있어야 합니다.
- 기기를 부팅할 때 BIOS에서 네트워크 부팅 옵션을 선택해야 합니다.

운영 체제가 다음과 같이 배포됩니다:

1. 클라이언트 기기는 부팅 프로세스 중에 PXE 서버와의 연결을 설정합니다.
2. 클라이언트 기기가 Windows 사전 설치 환경(WinPE)으로 부팅됩니다.

   기기를 WinPE에 추가하려면 WinPE용 드라이버 모음을 구성해야 할 수 있습니다.

3. 클라이언트 기기가 중앙 관리 서버에 등록됩니다.
4. 관리자는 운영 체제 이미지가 있는 설치 패키지를 클라이언트 기기에 할당합니다.

   관리자는 필요한 드라이버를 운영 체제 이미지가 있는 설치 패키지에 추가할 수 있습니다. 또한 설치 중에 적용할 운영 체제 설정이 포함된 구성 파일(응답 파일)을 지정할 수 있습니다.

5. 운영 체제가 클라이언트 기기에 배포됩니다.

관리자는 아직 연결되지 않은 클라이언트 기기의 MAC 주소를 수동으로 지정하고 이를 운영 체제 이미지가 있는 설치 패키지에 할당할 수 있습니다. 선택한 클라이언트 기기가 PXE 서버에 연결되면 운영 체제가 해당 기기에 자동 설치됩니다.

다른 운영 체제가 이미 설치된 기기에 운영 체제 이미지 배포

다른 운영 체제가 이미 설치된 클라이언트 기기에 운영 체제 이미지를 배포하는 작업은 특정 기기에 대한 원격 설치 작업을 통해 수행됩니다.

운영 체제가 새로 설치됩니다. 모든 데이터가 삭제됩니다.

Kaspersky 및 다른 공급업체에 의한 애플리케이션 설치

관리자는 사용자가 지정한 애플리케이션을 포함해 모든 애플리케이션의 설치 패키지를 만들고 원격 설치 작업을 통해 클라이언트 기기에 해당 애플리케이션을 설치할 수 있습니다.

운영 체제의 이미지 만들기

참조 기기의 운영 체제 이미지 제거 작업을 사용하여 운영 체제의 이미지를 만들 수 있습니다.

운영 체제 이미지 만들기 작업을 생성하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
2. **설치 패키지 생성** 버튼을 눌러 새 패키지 마법사를 실행합니다.

3. 마법사의 **설치 패키지 유형 선택** 창에서 **운영 체제 이미지로 설치 패키지 생성** 버튼을 누릅니다.

4. 마법사의 지침을 따릅니다.

   마법사가 완료되면 **참조 기기의 OS 이미지에서 설치 패키지 생성**이라는 중앙 관리 서버 작업이 생성됩니다. **작업** 폴더에서 작업을 볼 수 있습니다.

참조 기기의 OS 이미지에서 설치 패키지 생성 작업이 완료되면 설치 패키지가 생성되어 PXE 서버 또는 원격 설치 작업을 통해 운영 체제를 클라이언트 기기에 배포할 수 있습니다. **설치 패키지** 폴더에서 설치 패키지를 볼 수 있습니다.

운영 체제 이미지 설치

Kaspersky Security Center에서는 조직 네트워크 내의 기기에 데스크톱 및 서버 기반 Windows® 운영 체제의 WIM 이미지를 배포할 수 있습니다.

다음과 같은 방법을 사용하면 Kaspersky Security Center 도구를 통해 배포할 수 있는 운영 체제 이미지를 가져올 수 있습니다:

- Windows 배포 패키지에 포함된 install.wim 파일에서 가져오기
- 참조 기기에서 이미지 캡처

다음과 같은 두 가지 방식의 운영 체제 이미지 배포가 지원됩니다:

- 운영 체제가 설치되지 않은 "초기" 상태의 기기에 배포
- Windows를 실행 중인 기기에 배포

Windows PE(Windows 사전 설치 환경)를 사용하여 운영 체제 이미지를 캡처하고 배포합니다. 모든 대상 기기가 올바르게 작동하려면 필요한 모든 드라이버를 WinPE에 추가해야 합니다. 일반적으로 네트워크 어댑터와 스토리지 컨트롤러 드라이버를 추가해야 합니다.

이미지 배포 및 캡처를 구현하려면 다음 요구 사항을 충족해야 합니다:

- Windows 자동 설치 키트(WAIK) 버전 2.0 이상 또는 Windows ADK용 Windows PE 추가 기능이 있는 Windows ADK를 중앙 관리 서버에 설치해야 합니다. Windows XP에서 이미지를 설치하거나 캡처할 수 있는 경우 WAIK를 설치해야 합니다.
- 대상 기기가 있는 네트워크에서 DHCP 서버를 사용할 수 있어야 합니다.
- 대상 기기가 있는 네트워크에서 중앙 관리 서버의 공유 폴더를 읽기용으로 열어야 합니다. 공유 폴더가 중앙 관리 서버가 설치된 곳에 있다면 접근 시 KlPxeUser 계정을 요구합니다(이 계정은 중앙 관리 서버 설치 프로그램을 실행하는 동안 자동으로 생성됩니다). 공유 폴더가 중앙 관리 서버 외부에 있는 경우에는 모든 사용자에 대해 접근 권한을 부여해야 합니다.

관리자는 설치할 운영 체제 이미지를 선택할 때 대상 기기의 CPU 아키텍처(x86 또는 x86-64)를 명시적으로 지정해야 합니다.

KSN 프록시 서버 주소 구성

기본적으로 중앙 관리 서버의 연결 이름이나 IP 주소는 KSN 프록시 서버 주소와 일치합니다. 중앙 관리 서버의 연결 이름이나 IP 주소를 변경 시, 호스트 기기와 KSN 간의 연결이 끊어지지 않도록 올바른 KSN 프록시 주소를 지정해야 합니다.

KSN 프록시 주소를 구성하려면:

1. 콘솔 트리에서 **고급 → 원격 설치 → 설치 패키지**로 이동합니다.
2. **설치 패키지**의 컨텍스트 메뉴에서 **속성**을 선택합니다.
3. 창이 열리면 **일반** 탭에서 새 KSN 프록시 서버 주소를 지정합니다.
4. **적용** 버튼을 클릭합니다.

이제 지정된 주소를 KSN 프록시 서버 주소로 사용합니다. **KSN 프록시 사용** 옵션을 활성화하여 네트워크의 트래픽을 최적화하는 것이 좋습니다.

Windows 사전 설치 환경(WinPE)용 드라이버 추가

Windows 사전 설치 환경(WinPE)용 드라이버를 추가하려면 다음과 같이 진행합니다:

1. 콘솔 트리의 **원격 설치** 폴더에서 **기기 이미지 배포** 하위 폴더를 선택합니다.
2. **기기 이미지 배포** 폴더 작업 공간에서 **추가 조치** 버튼을 누르고 드롭다운 목록에서 **Windows 사전 설치 환경(WinPE)에 대한 드라이버 구성**을 선택합니다.

   Windows 사전 설치 환경(WinPE) 드라이버 창이 열립니다.
3. **Windows 사전 설치 환경(WinPE) 드라이버** 창에서 **추가** 버튼을 누릅니다.

   드라이버 선택 창이 열립니다.
4. **드라이버 선택** 창의 목록에서 드라이버를 선택합니다.

   필요한 드라이버가 목록에 없으면 **추가** 버튼을 누르고 **드라이버 추가** 창이 열리면 이 창에서 드라이버 이름과 드라이버 배포 패키지 폴더를 지정합니다.

   찾기 버튼을 눌러 폴더를 선택할 수 있습니다.

   드라이버 추가 창에서 **확인**을 누릅니다.
5. **드라이버 선택** 창에서 **확인**을 누릅니다.

   드라이버가 중앙 관리 서버 저장소에 추가됩니다. 저장소에 추가되면 해당 드라이버가 **드라이버 선택** 창에 표시됩니다.
6. **Windows 사전 설치 환경(WinPE) 드라이버** 창에서 **확인**을 누릅니다.

그러면 드라이버가 Windows 사전 설치 환경(WinPE)에 추가됩니다.

운영 체제 이미지가 있는 설치 패키지에 드라이버 추가

운영 체제 이미지가 있는 설치 패키지에 드라이버를 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
2. 운영 체제 이미지가 있는 설치 패키지의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   설치 패키지 속성 창이 열립니다.
3. 설치 패키지 속성 창에서 **추가 드라이버** 섹션을 선택합니다.
4. **추가 드라이버** 섹션에서 **추가** 버튼을 누릅니다.
   드라이버 선택 창이 열립니다.
5. **드라이버 선택** 창에서 운영 체제 이미지가 있는 설치 패키지에 추가하려는 드라이버를 선택합니다.
   드라이버 선택 창의 **추가** 버튼을 눌러 중앙 관리 서버 저장소에 새 드라이버를 추가할 수 있습니다.
6. **확인**를 누릅니다.

추가된 드라이버가 운영 체제 이미지가 있는 설치 패키지 속성 창의 **추가 드라이버** 섹션에 표시됩니다.

sysprep.exe 유틸리티 구성

sysrep.exe 유틸리티는 기기에서 운영 체제 이미지를 생성할 수 있도록 준비하는 작업을 수행합니다.

sysprep.exe 유틸리티를 구성하려면:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
2. 운영 체제 이미지가 있는 설치 패키지의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   설치 패키지 속성 창이 열립니다.
3. 설치 패키지 속성 창에서 **sysprep.exe 설정** 섹션을 선택합니다.
4. **sysprep.exe 설정** 섹션에서 클라이언트 기기에 운영 체제를 배포할 때 사용할 구성 파일을 지정합니다:
   - **기본 구성 파일 사용**. 운영 체제 이미지를 캡처할 때 기본적으로 생성되는 응답 파일을 사용하려면 이 옵션을 선택합니다.
   - **메인 설정의 사용자 지정 값 지정**. 사용자 인터페이스를 통해 설정에 값을 지정하려면 이 옵션을 선택합니다.
   - **구성 파일 지정**. 사용자 지정 응답 파일을 사용하려면 이 옵션을 선택합니다.
5. 변경 사항을 적용하려면 **적용** 버튼을 누릅니다.

새 네트워크 기기에 운영 체제 배포

운영 체제가 아직 설치되지 않은 새 기기에 운영 체제를 배포하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **원격 설치** 폴더에서 **기기 이미지 배포** 하위 폴더를 선택합니다.

   인터페이스 구성 창에서 **취약점 및 패치 관리 표시** 옵션이 활성화되어 있는지 확인하십시오. 그렇지 않으면 **원격 설치** 폴더가 표시되지 않습니다.

2. **추가 조치** 버튼을 눌러 드롭다운 목록에서 **PXE 서버 목록 관리**를 선택합니다.

   PXE 서버 섹션에 **속성: 기기 이미지 배포** 창이 열립니다.

3. **PXE 서버** 섹션에서 **추가** 버튼을 누르고 **PXE 서버** 창이 열리면 PXE 서버로 사용할 기기를 선택합니다.

   추가한 기기가 PXE 서버 섹션에 표시됩니다. 생성된 WinPE 파일은 중앙 관리 서버에서 기기로 전송됩니다. 파일 전송 프로세스는 일반적으로 10분이 소요됩니다. 전송이 완료되면 표시되는 **상태** 값이 **시작하기**에서 **준비**으로 변경됩니다.

4. **PXE 서버** 섹션에서 PXE 서버를 선택하고 **속성** 버튼을 누릅니다.

5. 선택한 PXE 서버의 속성 창의 **PXE 서버 연결 설정** 탭에서 중앙 관리 서버와 PXE 서버 간의 연결을 구성합니다.

6. 운영 체제를 배포하려는 클라이언트 기기를 부팅합니다.

7. 클라이언트 기기의 BIOS에서 네크워크 부팅 설치 옵션을 선택합니다.

   클라이언트 기기가 PXE 서버에 연결되고 **기기 이미지 배포** 폴더의 작업 영역에 표시됩니다.

8. **처리** 섹션에서 **설치 패키지 지정** 링크를 눌러 선택한 기기에 운영 체제를 설치하는 데 사용할 설치 패키지를 선택합니다.

   선택한 기기에서 DiskPart 도구를 사용하여 사용 가능한 디스크를 확인하십시오. Windows PE 명령 프롬프트에서 `diskpart`를 입력하여 DiskPart 도구를 엽니다. `list disk`를 입력하여 디스크를 나열합니다.

   기기를 추가하고 설치 패키지를 여기에 할당하면 해당 기기에 운영 체제가 자동으로 배포되기 시작합니다.

9. 클라이언트 기기에 대한 운영 체제 배포를 취소하려면 **처리** 섹션의 **OS 이미지 설치 취소** 링크를 누릅니다.

MAC 주소로 기기를 추가하려면 다음과 같이 하십시오:

- **기기 이미지 배포** 폴더에서 **기기 MAC 주소 추가**를 눌러 **새로운 기기** 창을 열고 추가할 기기의 MAC 주소를 지정합니다.
- **기기 이미지 배포** 폴더에서 **파일에서 대상 기기의 MAC 주소 가져오기**을 누르고 운영 체제를 배포하려는 모든 기기의 MAC 주소의 목록이 포함된 파일을 선택합니다.

클라이언트 기기에 운영 체제 배포

다른 운영 체제가 이미 설치된 클라이언트 기기에 운영 체제를 배포하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **원격 설치** 폴더를 열고 **관리 중인 기기에 설치 패키지 배포(워크스테이션)** 링크를 눌러 보호 배포 마법사를 실행합니다.
2. 마법사의 **설치 패키지 선택** 창에서 운영 체제 이미지가 있는 설치 패키지를 지정합니다.
3. 마법사의 지침을 따릅니다.

마법사가 완료되면 클라이언트 기기에 운영 체제를 설치하는 원격 설치 작업이 생성됩니다. **작업** 폴더에서 작업을 시작 또는 중지할 수 있습니다.

애플리케이션의 설치 패키지 만들기

애플리케이션 설치 패키지를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
2. **설치 패키지 생성** 버튼을 눌러 새 패키지 마법사를 실행합니다.
3. 마법사의 **설치 패키지 유형 선택** 창에서 다음 버튼 중 하나를 누릅니다:

- **Kaspersky 애플리케이션에 대한 설치 패키지 생성**. Kaspersky 애플리케이션의 설치 패키지를 만들려면 이 옵션을 선택합니다.
- **지정한 실행 파일에 대한 설치 패키지를 생성합니다**. 실행 파일 형태의 서드 파티 애플리케이션에 대해 설치 패키지를 만들려면 이 옵션을 선택합니다. 일반적으로 실행 파일은 애플리케이션의 설정 파일입니다.
  - **전체 폴더를 설치 패키지로 복사**

    실행 파일과 애플리케이션 설치에 필요한 추가 파일이 함께 있는 경우 이 옵션을 선택합니다. 이 옵션을 실행하기 전에 필요한 모든 파일이 동일한 폴더에 저장되어 있는지 확인합니다. 이 옵션을 실행하면 애플리케이션은 지정된 실행 파일을 포함하여 폴더의 전체 내용을 설치 패키지에 추가합니다.

  - **설치 파라미터 지정**

    원격 설치에 성공하려면 대부분의 애플리케이션을 숨김 모드로 설치해야 합니다. 이 경우 숨김 설치 파라미터를 지정해야 합니다.

    설치 설정 구성:

    - **실행 파일 명령줄**

      애플리케이션에 숨김 설치를 위한 추가 파라미터가 필요한 경우 이 필드에 관련 파라미터를 지정합니다. 자세한 내용은 공급업체 설명서를 참조하십시오.

      다른 파라미터를 입력할 수도 있습니다.

    - **Kaspersky Security Center에서 인식할 수 있는 권장 값을 사용해 애플리케이션 설정 변환**

지정한 애플리케이션에 대한 정보가 Kaspersky 데이터베이스에 있는 경우 권장 설정으로 애플리케이션이 설치됩니다.

실행 파일 명령줄 필드에 파라미터를 입력한 경우 권장 설정으로 다시 작성됩니다.

기본적으로 이 옵션은 켜져 있습니다.

Kaspersky 데이터베이스는 Kaspersky 분석가에 의해 생성 및 유지 관리됩니다. 데이터베이스에 추가된 각 애플리케이션에 대해 Kaspersky 분석가는 최적의 설치 설정을 정의합니다. 클라이언트 기기에 애플리케이션을 원격으로 설치하기 위한 설정이 정의됩니다. 중앙 관리 서버 저장소 업데이트 다운로드 작업을 실행하면 데이터베이스가 자동으로 중앙 관리 서버에 업데이트됩니다.

- **Kaspersky 데이터베이스에서 설치 패키지를 만들 애플리케이션 선택**. Kaspersky 데이터베이스에서 필요한 서드 파티 애플리케이션을 선택하여 설치 패키지를 만들려면 이 옵션을 선택하십시오. 중앙 관리 서버 저장소 업데이트 다운로드 작업을 실행하면 데이터베이스가 자동으로 생성됩니다. 애플리케이션이 목록에 표시됩니다.

- **운영 체제 이미지로 설치 패키지 생성**. 참조 기기의 운영 체제 이미지로 설치 패키지를 만들려면 이 옵션을 선택합니다.

  마법사가 완료되면 **참조 기기의 OS 이미지에서 설치 패키지 생성**이라는 중앙 관리 서버 작업이 생성됩니다. 이 작업이 완료되면 설치 패키지가 생성되어 PXE 서버 또는 원격 설치 작업을 통해 운영 체제 이미지를 배포하는 데 사용할 수 있습니다.

4. 마법사의 지침을 따릅니다.

마법사 작업이 완료되면 클라이언트 기기에 애플리케이션을 설치하는 데 사용할 수 있는 설치 패키지가 만들어집니다. 콘솔 트리에서 **설치 패키지**를 선택하여 설치 패키지를 볼 수 있습니다.

애플리케이션 설치 패키지용 인증서 발급

애플리케이션 설치 패키지에 대한 인증서를 발급하려면:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.

   기본적으로 **원격 설치** 폴더는 **고급** 폴더의 하위 폴더입니다.

2. **설치 패키지** 폴더의 마우스 오른쪽 메뉴에서 **고급**를 선택합니다.

   설치 패키지 폴더의 속성 창을 열립니다.

3. **설치 패키지** 폴더의 속성 창에서 **독립 실행형 패키지 서명** 섹션을 선택합니다.

4. **독립 실행형 패키지 서명** 섹션에서 **지정** 버튼을 누릅니다.

   인증서 창.

5. **인증서 유형** 필드에서 인증서 유형을 공개 또는 개인으로 지정합니다.

   - **PKCS #12 컨테이너** 값이 선택되면 인증서 파일과 암호를 지정합니다.
   - **X.509 인증서** 값을 선택한 경우:

     a. 개인 키 파일을 지정합니다(*.prk 또는 *.pem 확장자).

     b. 개인 키 암호를 지정합니다.

     c. 공개 키 파일을 지정합니다(*.cer 확장자).

6. **확인**를 누릅니다.

애플리케이션 설치 패키지용 인증서가 발급됩니다.

클라이언트 기기에 애플리케이션 설치

클라이언트 기기에 애플리케이션을 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **원격 설치** 폴더를 열고 **관리 중인 기기에 설치 패키지 배포(워크스테이션)**를 눌러 보호 배포 마법사를 실행합니다.
2. 마법사의 **설치 패키지 선택** 창에서 설치하려는 애플리케이션의 설치 패키지를 지정합니다.
3. 마법사의 지침을 따릅니다.

마법사가 완료되면 클라이언트 기기에 애플리케이션을 설치하기 위해 원격 설치 작업이 생성됩니다. **작업** 폴더에서 작업을 시작 또는 중지할 수 있습니다.

보호 배포 마법사를 사용하여 Windows, Linux 및 macOS가 실행 중인 클라이언트 기기에 네트워크 에이전트를 설치할 수 있습니다.

Linux 운영 체제를 실행하는 기기에서 Kaspersky Security Center를 사용하여 64비트 보안 제품을 관리하려면 64비트 Linux용 네트워크 에이전트를 사용해야 합니다. 필요한 네트워크 에이전트는 기술 지원 웹사이트에서 필요한 버전을 다운로드할 수 있습니다.

Linux를 실행하는 기기에서 네트워크 에이전트를 원격 설치하기 전에 기기를 준비해야 합니다.

개체 리비전 관리

이 섹션에는 개체 리비전 관리에 대한 정보가 포함되어 있습니다. Kaspersky Security Center에서는 개체 수정 내용을 추적할 수 있습니다. 개체 변경 내용을 저장할 때마다 *리비전*이 만들어집니다. 각 리비전에는 번호가 있습니다.

리비전 관리를 지원하는 애플리케이션 개체는 다음과 같습니다:

- 중앙 관리 서버 속성
- 정책
- 작업
- 관리 그룹
- 사용자 계정
- 설치 패키지

개체 리비전에 대해 다음과 같은 작업을 수행할 수 있습니다:

- 선택한 리비전을 현재 리비전과 비교
- 선택한 리비전 비교
- 유형이 동일한 다른 개체의 선택한 리비전과 개체 비교
- 선택한 리비전 보기
- 개체에 대한 변경 내용을 선택한 리비전으로 롤백
- 리비전을 .txt 파일로 저장

리비전 관리를 지원하는 개체의 속성 창 **리비전 내역** 섹션에는 다음 세부 정보가 포함된 개체 리비전 목록이 표시됩니다.

- 개체 리비전 번호
- 개체가 변경된 날짜와 시간
- 개체를 변경한 사용자 이름
- 개체에 적용된 조치
- 개체 설정 변경 내용 관련 리비전 설명

개체 리비전 정보

개체 리비전에 대해 다음과 같은 작업을 수행할 수 있습니다:

- 선택한 리비전을 현재 리비전과 비교
- 선택한 리비전 비교
- 유형이 동일한 다른 개체의 선택한 리비전과 개체 비교
- 선택한 리비전 보기

- 개체에 대한 변경 내용을 선택한 리비전으로 롤백
- 리비전을 .txt 파일로 저장

리비전 관리를 지원하는 개체의 속성 창 **리비전 내역** 섹션에는 다음 세부 정보가 포함된 개체 리비전 목록이 표시됩니다.

- 개체 리비전 번호
- 개체가 변경된 날짜와 시간
- 개체를 변경한 사용자 이름
- 개체에 적용된 조치
- 개체 설정 변경 내용 관련 리비전 설명

리비전 내역 섹션 보기

개체 리비전을 현재 리비전과 비교하거나, 목록에서 선택한 여러 리비전을 비교하거나, 개체 리비전을 동일 유형의 다른 개체 리비전과 비교할 수 있습니다.

*개체의 **리비전 내역** 섹션을 보려면 다음과 같이 하십시오.*

1. 콘솔 트리에서 다음 개체 중 하나를 선택합니다:
   - **중앙 관리 서버** 노드
   - **정책** 폴더
   - **작업** 폴더
   - 관리 그룹의 폴더
   - **사용자 계정** 폴더
   - **삭제된 개체** 폴더
   - **원격 설치** 폴더에 중첩되는 **설치 패키지** 하위 폴더
2. 관련 개체의 위치에 따라 다음 작업 중 하나를 수행합니다:
   - 개체가 **중앙 관리 서버** 노드 또는 관리 그룹 노드에 있으면 해당 노드를 오른쪽 클릭하고 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   - 개체가 **정책**, **작업**, **사용자 계정**, **삭제된 개체** 또는 **설치 패키지** 폴더에 있는 경우 해당 폴더를 선택하고 해당 작업 영역에서 개체를 선택합니다.

   개체 속성 창이 열립니다.
3. 왼쪽 **섹션** 창에서 **리비전 내역**를 선택합니다.

   리비전 내역이 작업 영역에 표시됩니다.

개체 리비전 비교

개체 이전 리비전을 현재 리비전과 비교하거나, 목록에서 선택한 여러 리비전을 비교하거나, 개체 리비전을 동일 유형의 다른 개체 리비전과 비교할 수 있습니다.

개체 리비전을 비교하려면 다음과 같이 하십시오:

1. 개체를 선택하고 개체의 속성 창으로 이동합니다.
2. 속성 창에서 **리비전 내역** 섹션으로 이동합니다.
3. 작업 영역에서 개체 리비전 목록에서 비교할 리비전을 선택합니다.
   하나 이상의 개체 리비전을 선택하려면 **SHIFT** 및 **CTRL** 키를 사용합니다.
4. 다음 중 하나를 수행합니다:
   - **비교** 분할 버튼을 누르고 드롭다운 목록에서 값 하나를 선택합니다.
     - **현재 리비전과 비교**

       선택한 리비전을 현재 리비전과 비교하려면 이 옵션을 선택합니다.

     - **선택한 리비전 비교**

       선택한 두 리비전을 비교하려면 이 옵션을 선택합니다.

     - **다른 작업과 비교**

       작업 리비전을 사용하는 경우 선택한 리비전을 다른 작업의 리비전과 비교하려면 **다른 작업과 비교**를 선택합니다.
       정책 리비전을 사용하는 경우 선택한 리비전을 다른 정책의 리비전과 비교하려면 **다른 정책과 비교**를 선택합니다.

   - 리비전 이름을 두 번 누르고 리비전 속성 창이 열리면 다음 버튼 중 하나를 누릅니다:
     - **현재 항목과 비교**

       선택한 리비전을 현재 리비전과 비교하려면 이 버튼을 누릅니다.

     - **이전 항목과 비교**

       선택한 리비전을 이전 리비전과 비교하려면 이 버튼을 누릅니다.

리비전 비교 관련 정보가 포함된 HTML 형식 리포트가 기본 브라우저에서 표시됩니다.

이 리포트에서 리비전 설정이 포함된 일부 섹션을 최소화할 수 있습니다. 개체 리비전 설정이 포함된 섹션을 최소화하려면, 섹션 이름 옆에 있는 화살표 아이콘(▲)을 클릭합니다.

중앙 관리 서버 리비전에는 적용한 모든 변경 내용의 세부 정보가 포함됩니다. 단, 다음 영역의 세부 정보는 제외됩니다:

- **트래픽** 섹션
- **태그 입력 규칙** 섹션
- **알림** 섹션
- **배포 지점** 섹션
- **바이러스 발생** 섹션

  바이러스 급증 이벤트가 트리거되면 발생하는 정책 활성화 구성과 관련하여 **바이러스 발생** 섹션에서는 아무 정보도 기록되지 않습니다.

삭제된 개체 리비전을 기존 개체 리비전에 비교할 수는 있지만 기존 개체 리비전을 삭제된 개체 리비전에 비교할 수는 없습니다.

개체 리비전 및 삭제된 개체 정보의 저장 기간 설정

개체 리비전과 삭제된 개체 관련 정보의 저장 기간은 동일합니다. 기본 저장 기간은 90일입니다. 90일은 일반적인 프로그램 감사를 수행하기에 충분한 기간입니다.

삭제된 개체 영역에서 **수정** 권한이 있는 사용자만 저장 기간을 변경할 수 있습니다.

개체 리비전 및 삭제된 개체 관련 정보의 저장 기간을 변경하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 저장 기간을 변경하고 싶은 중앙 관리 서버를 선택합니다.
2. 마우스 오른쪽 버튼을 누른 다음 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창이 열리면 **리비전 내역 저장소** 섹션에서 원하는 저장 기간(일)을 입력합니다.
4. **확인**을 누릅니다.

   개체 리비전과 삭제된 개체 관련 정보는 입력한 기간(일) 동안 저장됩니다.

개체 리비전 확인

특정 기간 동안 개체가 수정된 내용을 확인해야 하는 경우 해당 개체의 리비전을 보면 됩니다.

개체 리비전을 보려면 다음과 같이 하십시오:

1. 개체의 **리비전 내역** 섹션으로 이동합니다.
2. 개체 리비전 목록에서 보기 원하는 설정의 리비전을 선택합니다.

3. 다음 중 하나를 수행합니다:

   - **리비전 보기** 버튼을 누릅니다.
   - 리비전 이름을 두 번 눌러 리비전 속성 창을 열고 **리비전 보기** 버튼을 누릅니다.

   선택한 개체 리비전 설정이 포함된 HTML 형식 리포트가 표시됩니다. 이 리포트에서 개체 리비전 설정이 포함된 일부 섹션을 최소화할 수 있습니다. 개체 리비전 설정이 포함된 섹션을 최소화하려면, 섹션 이름 옆에 있는 화살표 아이콘(▲)을 클릭합니다.

개체 리비전을 파일에 저장

개체 리비전을 이메일로 보내려는 등의 경우 텍스트 파일로 저장할 수 있습니다.

개체 리비전을 파일에 저장하려면 다음과 같이 하십시오:

1. 개체의 **리비전 내역** 섹션으로 이동합니다.
2. 개체의 리비전 목록에서 설정을 저장해야 하는 리비전을 선택합니다.
3. **고급** 버튼을 누르고 드롭다운 목록에서 **파일로 저장** 값을 선택합니다.

   그러면 리비전이 .txt 파일로 저장됩니다.

변경 사항 롤백

필요한 경우 개체에 이뤄진 변경 사항을 롤백할 수 있습니다. 정책의 설정을 특정 날짜의 상태로 되돌려야 하는 경우를 예로 들 수 있습니다.

개체에 이뤄진 변경 사항을 롤백하려면 다음과 같이 하십시오:

1. 개체의 **리비전 내역** 섹션으로 이동합니다.
2. 개체 리비전 목록에서 변경 사항을 롤백해야 하는 리비전 번호를 선택합니다.
3. **고급** 버튼을 누르고 드롭다운 목록에서 **롤백** 값을 선택합니다.

   그러면 개체가 선택한 리비전으로 롤백됩니다. 개체 리비전 목록에는 수행한 작업의 기록이 표시됩니다. 리비전 설명에는 개체를 되돌린 리비전의 번호에 대한 정보가 표시됩니다.

리비전 설명 추가

리비전의 설명을 추가하면 목록에서 리비전을 쉽게 검색할 수 있습니다.

리비전의 설명을 추가하려면 다음과 같이 하십시오:

1. 개체의 **리비전 내역** 섹션으로 이동합니다.
2. 개체 리비전 목록에서 설명을 추가하기 원하는 리비전을 선택합니다.
3. **설명** 버튼을 누릅니다.

4. **개체 리비전 설명** 창에서 리비전에 대한 설명을 추가할 수 있습니다.
   기본적으로 개체 리비전 설명은 비어 있습니다.

5. **확인**를 누릅니다.

개체 삭제

이 섹션에서는 개체 삭제에 대한 정보를 제공합니다.

다음과 같은 개체를 삭제할 수 있습니다:

- 정책
- 작업
- 설치 패키지
- 가상 중앙 관리 서버
- 사용자
- 보안 그룹
- 관리 그룹

개체를 삭제하려면:

1. Kaspersky Security Center 웹 콘솔에서 필요한 섹션을 연 다음 개체를 선택합니다.
2. 툴바에서 **삭제** 버튼을 클릭합니다.
3. 창이 열리면 **확인** 버튼을 눌러 사용자의 선택을 확인합니다.

   선택한 규칙이 삭제됩니다.

개체를 삭제해도 개체에 대한 정보는 데이터베이스에 유지됩니다. 삭제된 개체 관련 정보의 저장 기간은 개체 리비전의 저장 기간과 동일합니다(권장 저장 기간은 90일). **삭제된 개체** 권한 영역에서 **수정** 권한이 있어야 저장 기간을 변경할 수 있습니다.

클라이언트 기기 삭제 정보

관리 그룹에서 관리 중인 기기를 삭제하면 애플리케이션이 해당 기기를 미할당 기기 그룹으로 이동합니다. 기기를 삭제한 후에도 설치된 Kaspersky 애플리케이션(네트워크 에이전트 및 Kaspersky Endpoint Security 등의 보안 애플리케이션)은 기기에 남아 있습니다.

Kaspersky Security Center는 다음 규칙에 따라 미할당 기기 그룹의 기기를 처리합니다.

- 장치 이동 규칙을 설정했고 장치가 이동 규칙의 기준을 충족한다면, 장치는 규칙에 따라 자동으로 관리 그룹으로 이동됩니다.
- 기기는 미할당 기기 그룹에 저장되며 기기 보관 규칙에 따라 그룹에서 자동으로 제거됩니다.

기기 보관 규칙은 전체 디스크 암호화로 암호화된 하나 이상의 드라이브가 있는 기기에 영향을 주지 않습니다. 이러한 기기는 자동 삭제되지 않으며 수동으로만 삭제할 수 있습니다. 암호화된 드라이브가 있는 기기를 삭제해야 한다면, 먼저 드라이브를 복호화한 후 기기를 삭제하십시오.

암호화된 드라이브가 있는 기기를 삭제하면 드라이브 복호화에 필요한 데이터도 함께 삭제됩니다. 기기를 삭제할 때(미할당 기기**미할당 기기**관리 중인 기기**관리 중인 기기 위험을 이해했으며 선택한 기기를 삭제하겠습니다** 확인란을 선택하면 해당 데이터 삭제에 동의하는 것입니다.

드라이브를 복호화하려면 다음 조건을 충족해야 합니다.

- 드라이브 복호화에 필요한 데이터 복원을 위해 기기를 중앙 관리 서버에 다시 연결합니다.
- 기기 사용자가 복호화 암호를 기억합니다.
- 드라이브를 암호화하는 데 사용된 보안 애플리케이션(예 : Kaspersky Endpoint Security for Windows)이 여전히 기기에 설치되어 있습니다.

드라이브가 Kaspersky 디스크 암호화 기술로 암호화되었다면 FDERT 복원 유틸리티를 사용하여 데이터 복구를 시도할 수도 있습니다.

VDI에서 암호화된 드라이브가 있는 장치를 삭제하면 암호화된 드라이브에 있는 정보가 삭제됩니다.

미할당 기기 그룹에서 기기를 수동으로 삭제하면 애플리케이션이 목록에서 기기를 제거합니다. 기기 삭제 후에도 설치된 Kaspersky 애플리케이션(있다면)은 기기에 남아 있습니다. 이때, 기기가 여전히 중앙 관리 서버에 표시되고 일반 네트워크 폴링을 구성했다면 Kaspersky Security Center는 네트워크 폴링 중에 기기를 검색하여 미할당 기기 그룹에 다시 추가합니다. 따라서 기기가 중앙 관리 서버에 보이지 않을 때만 기기를 직접 삭제하는 것이 좋습니다.

개체 삭제

기본 기능 권한 카테고리의 수정 권한이 있는 경우, 정책, 작업, 설치 패키지, 내부 사용자, 내부 보안 그룹 등의 개체를 삭제할 수 있습니다(자세한 내용은 사용자 및 그룹에 권한 할당 문서 참조).

원격 설치 작업에 사용하는 설치 패키지는 삭제할 수 없습니다. 먼저 해당 작업을 중지해야 합니다. 관리 그룹의 자동 설치 작업에 대한 자세한 내용은 관리 그룹의 기기에 애플리케이션 자동 설치 문서를 참조하십시오.

개체를 삭제하려면:

1. 콘솔 트리의 필요한 폴더 작업 영역에서 개체를 선택합니다.
2. 다음 중 하나를 수행합니다:
   - 개체를 마우스 오른쪽 버튼으로 클릭하고 **삭제**를 선택합니다.
   - **DELETE** 키를 누릅니다.

개체가 삭제되며 개체에 대한 정보는 데이터베이스에 저장됩니다.

삭제된 개체에 대한 정보 보기

삭제된 개체에 대한 정보는 개체 리비전과 동일한 기간 동안 삭제된 개체 폴더에 저장됩니다(권장 저장 기간은 90일).

삭제된 개체 권한 영역에서 **읽기** 권한이 있는 사용자만 삭제된 개체 목록을 확인할 수 있습니다(자세한 내용은 사용자 및 그룹에 권한 할당 참조).

삭제된 개체 목록을 보려면 다음과 같이 하십시오,

콘솔 트리에서 **삭제된 개체**를 선택합니다. 기본적으로 **삭제된 개체**는 **고급** 폴더의 하위 폴더입니다.

삭제된 개체 권한 영역에서 읽기 권한이 없으면 **삭제된 개체** 폴더에 빈 목록이 표시됩니다.

삭제된 개체 폴더의 작업 영역에는 삭제된 개체와 관련된 다음 정보가 포함됩니다:

- **이름**. 개체 이름입니다.
- **유형**. 정책, 작업 또는 설치 패키지와 같은 개체 유형입니다.
- **시간**. 개체가 삭제된 시간입니다.
- **사용자**. 개체를 삭제한 사용자의 계정 이름입니다.

개체와 관련된 자세한 정보를 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **삭제된 개체**를 선택합니다. 기본적으로 **삭제된 개체**는 **고급** 폴더의 하위 폴더입니다.
2. **삭제된 개체** 작업 영역에서 원하는 개체를 선택합니다.
   선택한 개체에 대해 작업을 할 수 있는 상자가 작업 영역 오른쪽에 표시됩니다.
3. 다음 중 하나를 수행합니다:
   - 상자에서 **속성** 링크를 누릅니다.
   - 작업 영역에서 선택한 개체를 마우스 오른쪽 버튼으로 누르고 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.

   해당 개체의 속성 창이 열리고 다음과 같은 탭이 표시됩니다:
   - **일반**
   - **리비전 내역**

삭제된 개체 목록에서 영구적으로 개체 삭제

삭제된 개체 권한 영역에서 **수정** 권한이 있는 사용자만 삭제된 개체 목록에서 개체를 영구적으로 삭제할 수 있습니다(자세한 내용은 사용자 및 그룹에 권한 할당 참조).

삭제된 개체 목록에서 개체를 삭제하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 노드를 선택한 다음 **삭제된 개체** 폴더를 선택합니다.
2. 작업 영역에서 삭제할 개체를 선택합니다.
3. 다음 중 하나를 수행합니다:
   - **DELETE** 키를 누릅니다.
   - 선택한 개체의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
4. 확인 대화 상자에서 **예**를 누릅니다.

삭제된 개체 목록에서 개체가 영구적으로 삭제됩니다. 모든 리비전을 포함하여 이 개체에 대한 모든 정보가 데이터베이스에서 영구적으로 제거됩니다. 이 정보는 복원할 수 없습니다.

모바일 기기 매니지먼트

Kaspersky Security Center를 통해 모바일 기기 보호를 관리하려면 전용 라이센스가 필요한 모바일 기기 관리 기능을 사용하면 됩니다. 조직의 직원이 소유한 모바일 기기를 관리하려는 경우 모바일 기기 관리를 활성화해야 합니다.

이 섹션에서는 모바일 기기 관리를 활성화/구성/비활성화하는 지침을 제공합니다. 이 섹션에서는 중앙 관리 서버에 연결된 모바일 기기를 관리하는 방법에 대해서도 설명합니다.

Kaspersky Security for Mobile에 대한 자세한 내용은 *Kaspersky Security for Mobile 도움말*을 참조하십시오.

시나리오: 모바일 기기 관리 배포

이 섹션에서는 Kaspersky Security Center에서 모바일 기기 매니지먼트 기능을 구성하는 시나리오를 제공합니다.

필수 구성 요소

모바일 기기 매니지먼트 기능으로의 접근 권한을 부여하는 라이센스가 있는지 확인합니다.

단계

모바일 기기 매니지먼트 기능의 배포는 다음 단계로 진행됩니다:

1. **포트 준비**

   중앙 관리 서버에서 13292 포트를 사용할 수 있는지 확인합니다. 이 포트는 모바일 기기 연결 시 필요합니다. 또한 17100 포트를 사용할 수 있도록 설정할 수도 있습니다. 이 포트는 관리 중인 모바일 기기를 위한 활성화 프록시 서버 용도로만 필요합니다. 관리 중인 모바일 기기가 인터넷에 접속할 수 있다면 이 포트를 사용할 필요는 없습니다.

2. **모바일 기기 매니지먼트 활성화**

   중앙 관리 서버 빠른 시작 마법사를 실행할 때 또는 그 이후에 모바일 기기 관리를 활성화할 수 있습니다.

3. **외부 중앙 관리 서버 주소 지정**

   중앙 관리 서버 빠른 시작 마법사를 실행할 때 또는 그 이후에 외부 주소를 지정할 수 있습니다. 모바일 기기 매니지먼트를 설치 시 선택하지 않았고 설치 마법사에서 주소를 지정하지 않은 경우 설치 패키지 속성에서 외부 주소를 지정합니다.

4. **관리 중인 기기 그룹에 모바일 기기 추가**

   정책을 통해 관리할 수 있도록 모바일 기기를 관리 중인 기기 그룹에 추가합니다. 중앙 관리 서버 빠른 시작 마법사의 단계 중 하나에서 이동 규칙을 생성할 수 있습니다. 나중에 이동 규칙을 생성할 수도 있습니다. 이러한 규칙을 생성하지 않으면 모바일 기기를 관리 중인 기기 그룹에 수동으로 추가할 수 있습니다.

   모바일 기기를 관리 중인 기기 그룹에 직접 추가하거나 해당 기기에 대한 하위 그룹(또는 여러 하위 그룹)을 생성할 수 있습니다.

   이후 언제든지 모바일 기기 연결 마법사를 사용하여 새 모바일 기기를 중앙 관리 서버에 연결할 수 있습니다.

5. **모바일 기기용 정책 만들기**

   모바일 기기를 관리하려면 기기가 속한 그룹에 해당 기기에 대한 하나의 정책(또는 여러 정책)을 만듭니다. 이후 언제든지 이 정책의 설정을 변경할 수 있습니다.

결과

이 시나리오를 완료한 후에는 Kaspersky Security Center를 사용하여 Android 및 iOS 기기를 관리할 수 있습니다. 모바일 기기의 인증서를 사용하고 모바일 기기에 명령을 전송할 수 있습니다.

iOS MDM 기기 관리를 위한 그룹 정책 정보

iOS MDM 기기를 관리하면 Kaspersky Security Center 배포 키트에 포함된 Kaspersky Device Management for iOS 관리 플러그인을 사용할 수 있습니다. Kaspersky Device Management for iOS를 사용하면 iPhone® 구성 유틸리티를 사용하지 않고도 iOS MDM 기기의 구성 설정 지정을 위한 그룹 정책을 생성할 수 있습니다.

iOS MDM 기기 관리를 위한 그룹 정책은 관리자에게 다음 옵션을 제공합니다:

- 기기 암호 보안 설정 구성.
- 기기의 하드웨어 기능 사용 제한 및 모바일 앱 설치 및 제거 제한 구성.
- YouTube™, iTunes® Store, Safari와 같은 선 탑재된 모바일 앱의 사용에 대한 제한 구성.
- 특정 지역에 있는 기기에서 볼 수 있는 영화, TV 쇼 등의 미디어 컨텐츠에 대한 제한 구성.
- 프록시 서버(글로벌 HTTP 프록시)를 통한 인터넷 연결 구성.
- 사용자가 기업 애플리케이션 및 서비스를 이용하기 위해 사용하는 계정 구성(싱글 사인온(SSO) 기술).
- 모바일 기기에서 인터넷 사용 모니터링(웹사이트 방문).
- 다른 인증 메커니즘 및 네트워크 프로토콜을 사용한 무선 네트워크(Wi-Fi), 액세스 포인트(APNs), 가상 사설망(VPNs)의 구성.
- 스트리밍 사진, 음악 및 비디오에 대한 AirPlay® 기기로의 연결 설정 구성.
- 기기에서 무선으로 문서를 인쇄하기 위해 AirPrint™ 프린터로의 연결 설정 구성.

- 기기에서 회사 이메일을 사용하기 위해 Microsoft Exchange 서버 및 사용자 계정과의 동기화 구성.
- LDAP 디렉토리 서비스와의 동기화를 위해 사용자 자격증명 구성.
- 사용자가 기업의 캘린더 및 연락처 목록에 액세스 할 수 있게 CalDAV 및 CardDAV 서비스로의 연결을 위한 사용자 자격증명 구성.
- 사용자 기기의 iOS 인터페이스 설정(예: 폰트나 즐겨찾는 웹사이트 아이콘) 구성.
- 기기에 새로운 보안 인증서 추가.
- 기기가 인증 기관에서 인증서 자동 가져오기를 수행하기 위한 SCEP(Simple Certificate Enrollment Protocol) 서버 구성.
- 모바일 앱의 동작에 대한 사용자 지정 설정 추가.

iOS MDM 기기 관리 정책은 iOS MDM 서버(이하 "모바일 기기 서버")를 포함한 관리 그룹에 할당된다는 점이 특징입니다. 이 정책에 지정된 모든 설정은 모바일 기기 서버와 그 서버가 관리하는 모바일 기기에 우선 적용됩니다. 관리 그룹의 계층 구조의 경우에, 보조 모바일 기기 서버는 기본 모바일 기기 서버에서 모바일 기기로 이 정책 설정을 수신합니다.

Kaspersky Security Center 관리 콘솔에서 iOS MDM 기기 관리용 그룹 정책을 사용하는 방법에 대한 자세한 내용은 *Kaspersky Security for Mobile* 설명서를 참조하십시오.

모바일 기기 매니지먼트 활성화

모바일 기기를 관리하려면 모바일 기기 관리를 활성화하도록 설정해야 합니다. 빠른 시작 마법사에서 이 기능을 활성화하지 않았다면 나중에 활성화할 수 있습니다. 모바일 기기 관리에는 라이센스가 필요합니다.

기본 중앙 관리 서버에서만 모바일 기기 관리를 활성할 수 있습니다.

모바일 기기 관리를 활성화하려면:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 선택합니다.
2. 폴더의 작업 영역에서 **모바일 기기 관리 사용** 버튼을 누릅니다. 이전에 **모바일 기기 관리**를 활성화하지 않은 경우에만 이 버튼을 사용할 수 있습니다.

   중앙 관리 서버 빠른 시작 마법사의 **추가 구성 요소** 페이지가 표시됩니다.
3. 모바일 기기를 관리하려면 **모바일 기기 관리 사용**를 선택합니다.
4. **애플리케이션 활성화 방법 선택** 페이지에서 키 파일이나 활성화코드를 사용하여 애플리케이션을 활성화합니다.

   모바일 기기 관리 기능을 활성화할 때가지는 모바일 기기를 관리할 수 없습니다.
5. 인터넷에 연결할 때 프록시 서버를 사용하려는 경우 **인터넷에 접속하기 위한 프록시 서버 설정** 페이지에서 **프록시 서버 사용** 확인란을 선택합니다. 이 확인란을 선택하면 설정을 입력하는 필드를 사용할 수 있게 됩니다. 프록시 서버 연결에 대해 설정을 지정합니다.

6. **플러그인 및 설치 패키지에 대한 업데이트 확인** 페이지에서 다음 옵션 중 하나를 선택합니다:

   - **플러그인과 설치 패키지가 최신인지 여부를 확인합니다**

     최신 상태 확인을 시작합니다. 일부 플러그인이나 설치 패키지의 오래된 버전이 탐지되면, 마법사가 최신 버전을 다운로드하여 오래된 버전을 교체하라는 메시지를 표시합니다.

   - **확인 건너뛰기**

     플러그인 및 설치 패키지가 최신 상태인지를 확인하지 않고 작업을 계속합니다. 인터넷에 접속할 수 없거나 특정한 이유로 애플리케이션의 오래된 버전을 계속 사용하려는 등의 경우 이 옵션을 선택할 수 있습니다.

     플러그인 업데이트 확인을 건너뛰면 애플리케이션이 올바르지 않게 작동할 수도 있습니다.

7. **최신 플러그인 버전 이용 가능** 페이지에서 애플리케이션 버전에 필요한 언어의 최신 버전 플러그인을 다운로드하여 설치합니다. 플러그인 업데이트는 라이센스를 요구하지 않습니다.

   플러그인과 패키지를 설치하고 나면 애플리케이션은 모바일 기기의 정상 작동에 필요한 모든 플러그인이 설치되었는지 확인합니다. 일부 플러그인의 오래된 버전이 탐지되면, 마법사가 최신 버전을 다운로드하여 오래된 버전을 교체하라는 메시지를 표시합니다.

8. **모바일 기기 연결 설정** 페이지에서 중앙 관리 서버 포트를 설정합니다.

마법사가 완료되면 다음 변경 사항이 적용됩니다:

- Kaspersky Endpoint Security for Android 정책이 만들어집니다.
- Kaspersky Device Management for iOS 정책이 만들어집니다.
- 중앙 관리 서버에서 모바일 기기용 포트가 열립니다.

모바일 기기 관리 설정 수정

모바일 기기 지원을 활성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 선택합니다.
2. 폴더의 작업 영역에서 **모바일 기기용 연결 포트** 링크를 누릅니다.
   중앙 관리 서버 속성 창의 **추가 포트** 섹션이 표시됩니다.
3. **추가 포트** 섹션에서 관련 설정을 수정합니다.

   - **활성화 프록시 서버용 SSL 포트**

   - **모바일 기기용 포트 열기**

     모바일 기기가 라이센스 서버에 연결하는 데 사용하는 포트가 열립니다. 아래 필드에서 포트 번호와 기타 설정을 정의할 수 있습니다.

     기본적으로 이 옵션은 켜져 있습니다.

- **모바일 기기 동기화용 포트**

  모바일 기기가 중앙 관리 서버에 연결하여 해당 서버와 데이터를 교환하는 데 사용하는 포트의 번호입니다. 기본 포트 번호는 13292입니다.

  포트 13292이 다른 용도로 사용되고 있으면 다른 포트를 할당할 수 있습니다.

- **모바일 기기 활성화용 포트**

  Kaspersky Endpoint Security for Android와 Kaspersky의 활성화 서버 연결용 포트.

  기본 포트 번호는 17100입니다.

4. **확인**를 누릅니다.

모바일 기기 매니지먼트 비활성화

기본 중앙 관리 서버에서만 모바일 기기 관리를 비활성할 수 있습니다.

모바일 기기 관리를 비활성화하려면:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 선택합니다.
2. 이 폴더의 작업 영역에서 **추가 구성 요소 구성** 링크를 누릅니다.

   중앙 관리 서버 빠른 시작 마법사의 **추가 구성 요소** 페이지가 표시됩니다.
3. 모바일 기기를 더 이상 관리하지 않으려는 경우 **모바일 기기 관리 사용 안 함**를 선택합니다.
4. **확인**를 누릅니다.

   그러면 이전에 연결했던 모바일 기기가 중앙 관리 서버에 연결할 수 없게 됩니다. 모바일 기기 연결용 포트와 모바일 기기 활성화용 포트는 자동으로 닫힙니다.

   Kaspersky Endpoint Security for Android 및 Kaspersky Device Management for iOS용으로 생성된 정책은 삭제되지 않습니다. 인증서 발급 규칙은 수정되지 않습니다. 설치된 플러그인은 제거되지 않습니다. 모바일 기기용 이동 규칙은 삭제되지 않습니다.

관리 중인 모바일 기기에서 모바일 기기 관리를 다시 활성한 후에는 모바일 기기 관리에 필요한 모바일 앱을 다시 설치해야 할 수 있습니다.

모바일 기기용 명령 사용

이 섹션에는 Kaspersky Security Center가 지원하는 모바일 기기 관리용 명령에 대한 정보가 포함되어 있습니다. 이 섹션에서는 모바일 기기로 명령을 보내는 방법 및 명령 로그에서 명령 실행 상태를 확인하는 방법에 대한 지침이 제공됩니다.

모바일 기기 매니지먼트 명령

Kaspersky Security Center는 모바일 기기 관리를 위한 명령을 지원합니다.

이러한 명령은 원격 모바일 기기 관리에 사용됩니다. 예를 들어 모바일 기기를 분실한 경우 명령을 사용하여 기기에서 회사 데이터를 삭제할 수 있습니다.

명령을 사용할 수 있는 관리 모바일 기기의 유형은 다음과 같습니다:

- iOS MDM 기기
- Kaspersky Endpoint Security(KES) 기기

각 기기 유형은 전용 명령 세트를 지원합니다.

특정 명령에 대한 참고 사항

- 모든 기기 유형에 대해 **초기 설정으로 재설정** 명령이 정상적으로 실행되면 모든 데이터가 기기에서 삭제되며 기기 설정이 기본값으로 롤백됩니다.
- iOS MDM 기기에서 **기업 데이터 삭제** 명령을 성공적으로 실행한 이후에 모든 설치된 구성 프로필, 프로비저닝 프로필, iOS MDM 프로필 및 애플리케이션에 대해 **iOS MDM 프로필과 함께 제거** 확인란이 선택되었다면 기기에서 제거됩니다.
- KES 기기에서 **기업 데이터 삭제** 명령이 정상적으로 실행되면 모든 회사 데이터, 연락처의 항목, SMS 기록, 통화 기록, 일정, 인터넷 연결 설정 및 사용자 계정(Google™ 계정 제외)이 기기에서 삭제됩니다. KES 기기의 경우에는 메모리 카드의 데이터도 모두 삭제됩니다.
- KES 기기로 **위치 확인** 명령을 보내기 전에 조직 혹은 직원 소유의 분실 기기에 대한 승인된 검색에 이 명령을 사용하는지 여부를 확인해야 합니다. **위치 확인** 명령을 수신하는 모바일 기기는 잠겨 있지 않습니다.

모바일 기기용 명령 목록

다음 표에는 iOS MDM 기기에 대한 명령 세트가 나와 있습니다.

지원하는 모바일 기기 관리 명령: iOS MDM 기기

명령	명령 실행 결과
잠금	모바일 기기가 잠겨 있습니다.
잠금 해제	PIN으로 모바일 기기를 잠그는 것은 중지되었습니다. 이전에 지정한 PIN은 초기화되었습니다.
초기 설정으로 재설정	모든 데이터가 모바일 기기에서 삭제되고 설정이 공장 초기값으로 롤백됩니다.
기업 데이터 삭제	모든 설치된 구성 프로필, 프로비저닝 프로필, iOS MDM 프로필 및 애플리케이션에 대해 **iOS MDM 프로필과 함께 제거** 확인란이 선택되었다면 기기에서 제거됩니다.
기기 동기화	모바일 기기 데이터가 중앙 관리 서버와 동기화됩니다.
프로필 설치	구성 프로필이 모바일 기기에 설치됩니다.
프로필 제거	구성 프로필이 모바일 기기에서 삭제됩니다.
프로비저닝 프로필 설치	프로비저닝 프로필이 모바일 기기에 설치됩니다.

명령	명령 실행 결과
프로비저닝 프로필 제거	프로비저닝 프로필이 모바일 기기에서 삭제됩니다.
앱 설치	앱이 모바일 기기에 설치됩니다.
앱 제거	앱이 모바일 기기에서 제거됩니다.
교환 코드 입력	유료 앱용으로 입력한 교환 코드입니다.
로밍 구성	데이터 로밍 및 음성 로밍이 활성 또는 비활성됩니다.

다음 표에는 KES 기기에 대한 명령 세트가 나와 있습니다.

지원하는 모바일 기기 관리 명령: KES 기기

명령	명령 실행 결과
잠금	모바일 기기가 잠겨 있습니다.
잠금 해제	PIN으로 모바일 기기를 잠그는 것은 중지되었습니다. 이전에 지정한 PIN은 초기화되었습니다.
초기 설정으로 재설정	모든 데이터가 모바일 기기에서 삭제되고 설정이 공장 초기값으로 롤백됩니다.
기업 데이터 삭제	회사 데이터, 연락처의 항목, SMS 기록, 통과 기록, 달력, 인터넷 연결 설정, 사용자 계정(Google 계정 제외) 등이 삭제됩니다. 메모리 카드 데이터는 삭제되었습니다.
기기 동기화	모바일 기기 데이터가 중앙 관리 서버와 동기화됩니다.
기기 위치 확인	모바일 기기는 Google Maps™에 위치가 표시됩니다. 모바일 통신 사업자는 SMS 메시지 전송 및 인터넷 연결 제공 시 요금을 부과합니다.
전면 사진 촬영	모바일 기기가 잠겨 있습니다. 사진은 기기의 전면 카메라로 촬영되고 중앙 관리 서버에 저장됩니다. 사진은 명령 로그에서 볼 수 있습니다. 모바일 통신 사업자는 SMS 메시지 전송 및 인터넷 연결 제공 시 요금을 부과합니다.
경보음	모바일 기기에서 경보음이 울립니다.

Firebase Cloud Messaging 사용

Android 운영 체제에 의해 관리되는 KES 기기에 적절히 명령을 전달하기 위해 Kaspersky Security Center는 푸시 알림 메커니즘을 사용합니다. Firebase 클라우드 메시지(이하 FCM)를 통해 KES 기기와 중앙 관리 서버 간에 푸시 알림을 교환합니다. Kaspersky Security Center 관리 콘솔에서 해당 서비스에 KES 기기를 연결하기 위해 Firebase Cloud Messaging 설정을 지정할 수 있습니다.

Firebase Cloud Messaging 설정을 가져오려면 Google 계정이 있어야 합니다.

FCM을 사용하도록 설정하려면 다음을 수행합니다:

1. 관리 콘솔에서 **모바일 기기 관리** 노드와 **모바일 기기** 폴더를 선택합니다.
2. **모바일 기기** 폴더의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 폴더 속성에서 **Firebase Cloud Messaging 설정** 섹션을 선택합니다.
4. **Firebase 프로젝트 번호** 필드에서 FCM 발신자 ID를 지정합니다.
5. **개인 키 파일(JSON 형식)** 필드에서 개인 키 파일을 선택합니다.

중앙 관리 서버와의 다음 동기화에서 Android 운영 체제에 의해 관리되는 KES 기기는 Firebase Cloud Messaging에 연결됩니다.

기기 초기 설정으로 재설정 버튼을 클릭하여 Firebase Cloud Messaging의 설정을 편집할 수 있습니다.

명령 보내기

사용자 모바일 기기로 명령을 보내려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.
2. 명령을 보내야 하는 사용자 모바일 기기를 선택합니다.
3. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.
4. **모바일 기기 관리 명령** 창에서 모바일 기기로 보내야 하는 명령 이름이 지정된 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.
   선택한 명령에 따라 **명령 전송** 버튼을 누르면 애플리케이션의 고급 설정 창이 열릴 수 있습니다. 예를 들어 모바일 기기에서 프로비저닝 프로필을 삭제하는 명령을 보내면 모바일 기기에서 삭제해야 하는 프로비저닝 프로필을 선택하라는 메시지가 애플리케이션에 표시됩니다. 해당 창에서 명령의 고급 설정을 정의하고 선택을 확인합니다. 그리고 나면 모바일 기기로 명령이 전송됩니다.
   재전송 버튼을 눌러 사용자의 모바일 기기에 명령을 다시 보낼 수 있습니다.
   예약 목록에서 제거 버튼을 눌러 아직 실행되지 않은 명령의 실행을 취소할 수 있습니다.
   명령 로그 섹션에 모바일 기기로 보낸 명령이 각각의 실행 상태와 함께 표시됩니다. **새로 고침**를 눌러 명령 목록을 업데이트합니다.
5. **확인**를 눌러 **모바일 기기 관리 명령** 창을 닫습니다.

명령 로그에서 명령 상태 보기

애플리케이션은 모바일 기기로 전송된 모든 명령에 대한 정보를 명령 로그에 저장합니다. 명령 로그에는 각 명령이 모바일 기기로 전송된 날짜와 시간에 대한 정보, 명령의 상태 및 명령 실행 결과에 대한 상세 설명이 포함됩니다. 예를 들어 명령을 실행하지 못한 경우 로그에는 오류의 원인이 표시됩니다. 레코드는 최대 30일간 명령 로그에 저장됩니다.

모바일 기기로 전송된 명령은 다음 상태일 수 있습니다:

- *실행 중* – 명령이 모바일 기기로 전송되었습니다.
- *완료* – 명령 실행이 정상적으로 완료되었습니다.
- *오류 발생* – 명령 실행이 실패했습니다.
- *삭제* – 모바일 기기로 전송된 명령 큐에서 명령을 제거하는 중입니다.
- *삭제됨* – 모바일 기기로 전송된 명령 큐에서 명령이 성공적으로 제거되었습니다.
- *삭제 오류* – 모바일 기기로 전송된 명령 큐에서 명령을 제거할 수 없습니다.

애플리케이션은 각 모바일 기기에 대해 명령 로그를 유지 관리합니다.

모바일 기기로 전송된 명령의 로그를 확인하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.
2. 모바일 기기 목록에서 명령 로그를 확인할 기기를 선택합니다.
3. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.
   모바일 기기 관리 명령 창이 열립니다. **모바일 기기 관리 명령** 창의 섹션은 모바일 기기로 보낼 수 있는 명령에 해당합니다.
4. 필요한 명령이 포함된 섹션을 선택한 다음 **명령 로그** 섹션에서 명령 전송 및 실행 방법에 대한 정보를 확인합니다.

명령 로그 섹션에서는 모바일 기기로 전송된 명령의 목록과 해당 명령에 대한 상세 정보를 확인할 수 있습니다. **명령 보기** 필터를 사용하면 선택한 상태의 명령만 목록에 표시할 수 있습니다.

모바일 기기의 인증서 작업

이 섹션에는 모바일 기기의 인증서를 처리하는 방법에 대한 정보가 포함되어 있습니다.

모바일 기기용 루트 인증서의 만료 기간은 생성 후 700일로 고정됩니다. 예약 인증서는 만료 60일 전에 생성됩니다. 다음 명령을 사용하여 예약 인증서 생성 기간을 수정할 수 있습니다.

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <`시간 제한 (초)`>`

인증서 예약을 생성하는 기간은 모든 관리 중인 모바일 기기가 중앙 관리 서버와 동기화하고 인증서를 검색할 수 있을 만큼 충분히 길어야 합니다.

klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.

모바일 기기용 루트 인증서의 수동 갱신은 지원하지 않습니다.

인증서 설치 마법사 시작

사용자의 모바일 기기에 대해 다음 유형의 인증서를 설치할 수 있습니다:

- 모바일 기기 식별을 위한 공유 인증서
- 모바일 기기에서 회사 메일을 구성하기 위한 메일 인증서
- 모바일 기기에서 가상 사설망 접근을 구성하기 위한 VPN 인증서

사용자의 모바일 기기에 인증서를 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **인증서** 하위 폴더를 선택합니다.
2. **인증서** 폴더의 작업 영역에서 **인증서 추가** 링크를 눌러 인증서 설치 마법사를 실행합니다.

마법사의 지침을 따릅니다.

마법사가 완료되면 인증서가 생성되어 사용자 인증서 목록에 추가됩니다. 또한 사용자에게 모바일 기기에서 인증서를 다운로드하여 설치하기 위한 링크를 제공하는 알림이 전송됩니다. 모든 인증서 목록을 확인하고 파일로 내보낼 수 있습니다. 인증서를 삭제하고 다시 발급할 수 있으며 해당 속성을 볼 수도 있습니다.

1단계. 인증서 유형 선택

사용자의 모바일 기기에 설치해야 하는 인증서의 유형을 지정합니다:

- **모바일 인증서** - 모바일 기기 식별용.
- **메일 인증서** - 모바일 기기에 대한 기업 메일 구성용.
- **VPN 인증서** - 모바일 기기의 가상 사설망에 대한 접근 구성용.

2단계. 기기 유형 선택

이 창은 인증서 유형으로 **메일 인증서** 또는 **VPN 인증서**를 선택한 경우에만 표시됩니다.

기기에서 운영 체제의 유형을 지정합니다:

- **iOS MDM 장치**. iOS MDM 프로토콜을 사용하여 iOS MDM 서버에 연결된 모바일 기기에 인증서를 설치해야 하는 경우 이 옵션을 선택합니다.
- **Kaspersky Security for Mobile로 관리 중인 KES 기기**. KES 기기에 인증서를 설치해야 하는 경우 이 옵션을 선택합니다. 이 경우 인증서는 중앙 관리 서버에 연결할 때마다 사용자 식별에 사용됩니다.
- **사용자 인증서를 설치하지 않고 중앙 관리 서버에 연결된 KES 기기**. 인증서 인증 없이 KES 기기에 인증서를 설치해야 하는 경우 이 옵션을 선택합니다. 이때, 관리자가 마법사의 마지막 단계에 있는 **사용자 알림 방법** 창에서 중앙 관리 서버에 연결 시 사용할 사용자 인증 유형을 선택해야 합니다.

3단계. 사용자 선택

목록에서 인증서를 설치해야 하는 사용자, 보안 그룹 또는 Active Directory 보안 그룹을 선택합니다.

사용자 선택 창에서 Kaspersky Security Center 내부 사용자를 검색할 수 있습니다. **추가**를 눌러 내부 사용자를 추가할 수 있습니다.

4단계. 인증서 경로 선택

이 창에서는 중앙 관리 서버에서 모바일 기기를 식별하는 데 사용할 인증서 경로를 선택할 수 있습니다. 다음 방법 중 하나를 사용해 인증서를 지정할 수 있습니다:

- 중앙 관리 서버 도구를 이용해 자동으로 인증서를 생성한 후 해당 인증서를 기기에 전달합니다.
- 이전에 생성된 인증서 파일을 지정합니다. 이전 단계에서 여러 사용자를 선택한 경우 이 방법은 사용할 수 없습니다.

모바일 기기용 인증서 생성에 대한 알림을 사용자에게 보내야 하는 경우 **인증서 게시** 확인란을 선택합니다.

사용자의 모바일 기기가 이미 인증서를 사용하여 이전에 인증되어 새 인증서를 받기 위한 계정 이름과 암호를 지정할 필요가 없으면 **인증서 게시** 확인란의 선택을 해제합니다. 이 경우 **사용자 알림 방법** 창이 표시되지 않습니다.

5단계. 인증서에 태그 할당

기기 유형에서 **iOS MDM 장치**를 선택한 경우 **인증서 태그** 창이 표시됩니다.

드롭 다운 목록에서 사용자의 iOS MDM 기기 인증서에 태그를 지정할 수 있습니다. 태그가 할당된 인증서는 Kaspersky Device Management for iOS 정책 속성에서 이 태그에 대해 설정되는 특정 파라미터를 가질 수 있습니다.

드롭 다운 목록에서 *인증서 템플릿 1*, *인증서 템플릿 2* 또는 *인증서 템플릿 3* 태그를 선택하라는 메시지가 나타납니다. 다음 섹션에서 태그를 구성할 수 있습니다:

- **인증서 유형** 창에서 **메일 인증서**를 선택한 경우, 모바일 기기용 Exchange ActiveSync 계정 속성(**관리 중인 기기** → **정책** → Kaspersky Device Management for iOS 정책 속성 > **Exchange ActiveSync** 섹션 → **추가** →**고급**)에서 태그를 구성할 수 있습니다.
- **인증서 유형** 창에서 **VPN 인증서**를 선택한 경우, 모바일 기기용 VPN 속성(**관리 중인 기기** → **정책** → Kaspersky Device Management for iOS 정책 속성 → **VPN** 섹션 → **추가** → **고급**)에서 태그를 구성할 수 있습니다. VPN에 대해 L2TP, PPTP 또는 IPSec(Cisco™) 연결 유형을 선택한 경우 VPN 인증서에 사용되는 태그를 구성할 수 없습니다.

6단계. 인증서 게시 설정 지정

이 창에서는 다음 인증서 게시 설정을 지정할 수 있습니다:

- **새 인증서에 대해 사용자에게 알리지 않음**

  사용자 모바일 기기용 인증서 생성에 대해 사용자에게 알림을 보내지 않으려는 경우 이 옵션을 활성화합니다. 이 경우 **사용자 알림 방법** 창이 표시되지 않습니다.

  > 이 옵션은 Kaspersky Endpoint Security for Android가 설치된 기기에만 해당됩니다.

  예를 들어 사용자의 모바일 기기가 이미 인증서를 사용하여 이전에 인증되어서 새 인증서를 수신하기 위한 계정 이름과 암호를 지정할 필요가 없으면 이 옵션을 활성화할 수 있습니다.

- **단일 인증서로 다중 수신 하도록 기기 허용(Kaspersky Endpoint Security for Android가 설치된 기기만 해당)**

  인증서가 곧 만료되거나 대상 기기에서 인증서를 찾을 수 없을 때마다 Kaspersky Security Center에서 인증서를 자동으로 재전송하도록 하려면 이 옵션을 활성화합니다.

  인증서는 만료 날짜 며칠 전에 자동으로 재전송됩니다. 인증서 발급 규칙 창에서 기간(일)을 설정할 수 있습니다.

  기기에서 인증서를 찾을 수 없는 경우도 있습니다. 예를 들어 사용자가 기기에 Kaspersky 보안 제품을 다시 설치하거나 기기 설정 및 데이터를 공장 기본값으로 초기화하는 경우 이러한 상황이 발생할 수 있습니다. 이 경우 Kaspersky Security Center는 기기가 다음 번에 중앙 관리 서버에 연결을 시도할 때 기기 ID를 확인합니다. 기기의 ID가 인증서 발급 시의 ID와 같으면 애플리케이션이 기기에 인증서를 재전송합니다.

7단계. 사용자 알림 방법 선택

iOS MDM 장치를 기기 유형으로 선택한 경우 또는 **새 인증서에 대해 사용자에게 알리지 않음** 옵션을 선택한 경우 이 창이 표시되지 않습니다.

사용자 알림 방법 창에서 모바일 기기에 인증서를 설치하는 것에 관한 사용자 알림을 구성할 수 있습니다.

인증 방법 필드에서 사용자 인증 유형을 지정합니다:

- **자격증명(도메인 또는 별칭)**

  이 경우 사용자는 도메인 암호 또는 Kaspersky Security Center 내부 사용자의 암호를 사용하여 새 인증서를 받습니다.

- **일회용 암호**

  이 경우 사용자는 이메일 또는 SMS로 발송된 일회용 암호를 받게 됩니다. 새 인증서를 받으려면 이 암호를 입력해야 합니다.

  인증서 게시 설정 창에서 **단일 인증서로 기기 다중 수신 허용(모바일 기기의 경우 Kaspersky 보안 제품이 설치된 기기만 해당)** 옵션을 활성화(선택)한 경우 이 옵션은 **암호**로 변경됩니다.

- **암호**

  이 경우에는 사용자에게 인증서를 전송할 때마다 암호가 사용됩니다.

  인증서 게시 설정 창에서 **단일 인증서로 기기 다중 수신 허용(모바일 기기의 경우 Kaspersky 보안 제품이 설치된 기기만 해당)** 옵션을 비활성화(지우기)한 경우 이 옵션은 **일회용 암호**로 변경됩니다.

인증서 유형 창에서 **모바일 인증서**를 선택한 경우 또는 **사용자 인증서를 설치하지 않고 중앙 관리 서버에 연결된 KES 기기**을 기기 유형으로 선택한 경우 이 필드가 표시됩니다.

사용자 알림 옵션 선택:

- **마법사 완료 후 인증 암호 표시**

  이 옵션을 선택하면 인증서 설치 마법사의 마지막 단계에서 선택한 각 사용자에 대해 사용자 이름, SAM(보안 계정 관리자)의 사용자 이름, 인증서를 가져올 때 필요한 암호가 표시됩니다. 설치된 인증서에 대한 사용자 알림 구성을 사용할 수 없습니다.

  여러 사용자의 인증서를 추가할 때는 인증서 설치 마법사의 마지막 단계에서 **내보내기** 버튼을 눌러 제공된 인증서를 파일로 저장할 수 있습니다.

  > 인증서 설치 마법사의 **사용자 알림 방법** 단계에서 **자격증명(도메인 또는 별칭)**을 선택했다면 이 옵션을 사용할 수 없습니다.

- **새 인증서를 사용자에게 알림**

  이 옵션을 선택하면 새 인증서에 대한 사용자 알림을 구성할 수 있습니다.

  - **이메일**

    설정의 이 그룹에서 이메일 메시지를 사용하여 모바일 기기에 새 인증서 설치에 대한 사용자 알림을 구성할 수 있습니다. 이 알림 방법은 SMTP 서버를 사용했을 경우에만 이용할 수 있습니다.

    필요한 경우 **메시지 편집** 링크를 눌러 알림 메시지를 보거나 편집합니다.

  - **SMS**

    이 설정 그룹에서는 모바일 기기에서 SMS를 사용하여 인증서를 설치하는 작업과 관련된 사용자 알림을 구성할 수 있습니다. 이 알림 방법은 SMS 알림을 사용했을 경우에만 이용할 수 있습니다.

    필요한 경우 **메시지 편집** 링크를 눌러 알림 메시지를 보거나 편집합니다.

8단계. 인증서 생성

이 단계에서 인증서가 생성됩니다.

마침을 클릭하여 마법사를 종료할 수 있습니다.

인증서가 생성되며 **인증서** 폴더의 작업 영역에 있는 인증서 목록에 표시됩니다.

인증서 발급 규칙 구성

인증서는 중앙 관리 서버에서 기기 인증에 사용됩니다. 모든 관리 중인 모바일 기기에는 인증서가 있어야 합니다. 인증서 발급 방법을 구성할 수 있습니다.

인증서 발급 규칙을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **인증서** 하위 폴더를 선택합니다.
2. **인증서** 폴더의 작업 영역에서 **인증서 발급 규칙 구성** 버튼을 눌러 **인증서 발급 규칙** 창을 엽니다.
3. 인증서 유형의 이름이 지정된 섹션으로 이동합니다:
   모바일 인증서 발급 - 모바일 기기에 대한 인증서 발급을 구성합니다.
   메일 인증서 발급 – 메일 인증서 발급을 구성합니다.
   VPN 인증서 발급 –VPN 인증서 발급을 구성합니다.
4. **발급 설정** 섹션에서 인증서 발급을 구성합니다:
   - 수일 내로 인증서 기간을 지정합니다.
     모바일 기기용 인증서는 루트 인증서의 만료 날짜로 제한됩니다. 루트 인증서의 만료 날짜보다 인증서 기간을 지정하면 생성 시 인증서 기간이 자동으로 조정됩니다.
   - 인증서 소스를 선택합니다(**중앙 관리 서버** 또는 **인증서는 수동으로 지정됩니다**).
     중앙 관리 서버가 기본 인증서 경로로 선택됩니다.
   - 인증서 템플릿을 지정합니다(**기본 템플릿**, **기타 템플릿**).
     PKI와 통합 섹션에서 공개키 인프라와 통합이 활성화되어 있으면 템플릿을 구성할 수 있습니다.
5. **자동 업데이트 설정** 섹션에서 인증서 자동 업데이트를 구성합니다:
   - **다음 기간 이내에 인증서가 만료되면 갱신(일)** 필드에서 인증서를 갱신해야 하는 만료 전 기간(일)을 지정합니다.
   - 인증서 자동 업데이트를 활성화하려면 **가능하면 자동으로 인증서 재발급** 확인란을 선택합니다.
6. **암호 보호** 섹션에서 인증서를 복호화하기 위한 암호의 사용을 활성화하고 구성합니다.

   암호 보호는 모바일 인증서에만 사용할 수 있습니다.

   a. **인증서 설치 시 암호 물어보기** 확인란을 선택합니다.
   b. 슬라이더를 사용하여 암호화용 암호의 최대 기호 수를 정의합니다.
7. **확인**를 누릅니다.

공개 키 인프라와의 통합

사용자에 대한 도메인 인증서 발급을 간소화하려면 애플리케이션을 PKI(공개 키 인프라)와 통합해야 합니다. 통합 이후 인증서는 자동으로 발급됩니다.

Windows Server 2008 및 이후 버전에서 PKI 서버가 지원됩니다.

PKI와의 통합용 계정을 구성해야 합니다. 해당 계정은 다음 요구 사항을 충족해야 합니다:

- 중앙 관리 서버가 설치된 기기의 도메인 사용자 및 관리자여야 합니다.
- 중앙 관리 서버가 설치된 기기에 대한 SeServiceLogonRight 권한이 부여되어 있어야 합니다.

영구적인 사용자 프로필을 작성하려면, 중앙 관리 서버를 호스팅하는 기기에 구성된 사용자 계정으로 한 번 이상 로그인합니다. 중앙 관리 서버 기기의 이 사용자 인증서 저장소에 도메인 관리자가 제공한 에이전트 인증서 등록을 설치합니다.

공개 키 인프라와의 통합을 구성하려면:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **인증서** 하위 폴더를 선택합니다.
2. 작업 영역에서 **공개 키 인프라와 통합** 버튼을 눌러 **인증서 발급 규칙** 창의 **PKI와 통합** 섹션을 엽니다.
   인증서 발급 규칙 창의 **PKI와 통합** 섹션이 열립니다.
3. **PKI로 인증서 발급 통합** 확인란을 선택합니다.
4. **계정** 필드에서 공개 키 인프라와의 통합에 사용할 사용자 계정의 이름을 지정합니다.
5. **암호** 필드에 계정에 대한 도메인 암호를 입력합니다.
6. **PKI 시스템에서의 인증서 템플릿 이름** 목록에서 도메인 사용자에게 인증서를 발급하는 데 사용할 인증서 템플릿을 선택합니다.
   전용 서비스는 지정된 사용자 계정의 Kaspersky Security Center에서 실행됩니다. 이 서비스는 사용자의 도메인 인증서 발급을 담당합니다. 이 서비스는 인증서 템플릿 목록이 **목록 새로 고침** 버튼을 눌러 로딩되거나 인증서가 생성될 때 실행됩니다.
7. **확인**를 눌러 설정을 저장합니다.

통합 이후 인증서는 자동으로 발급됩니다.

Kerberos 제한된 위임 지원 작동

이 애플리케이션은 Kerberos 제한 위임의 사용을 지원합니다.

Kerberos 제한된 위임 지원 사용하려면:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 엽니다.
2. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기 서버** 하위 폴더를 선택합니다.
3. **모바일 기기 서버** 폴더의 작업 영역에서 iOS MDM 서버를 선택합니다.
4. iOS MDM 서버의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
5. iOS MDM 서버의 속성 창에서 **설정** 섹션을 선택합니다.
6. **설정** 섹션에서 **Kerberos constrained delegation와의 호환성 보장** 확인란을 선택합니다.
7. **확인**를 누릅니다.

관리 중인 기기 목록에 iOS 모바일 기기 추가

iOS 모바일 기기를 관리 중인 기기 목록에 추가하려면 기기에 공유 인증서를 전달하고 설치해야 합니다. 공유 인증서는 모바일 기기를 식별하기 위해 중앙 관리 서버에서 사용합니다. iOS 모바일 기기에 대한 공유 인증서는 iOS MDM 프로필 내에서 전달됩니다. 모바일 기기에 공유 인증서가 전달되고 설치되면 해당 기기가 관리 중인 기기 목록에 나타납니다.

Kaspersky은 Kaspersky Safe Browser를 더 이상 지원하지 않습니다.

모바일 장치 연결 마법사를 사용하여 사용자의 모바일 장치를 관리 중인 장치 목록에 추가할 수 있습니다.

공유 인증서를 사용하여 iOS 기기를 중앙 관리 서버에 연결하려면 다음과 같이 하십시오:

1. 다음 방법 중 하나로 모바일 기기 연결 마법사를 시작합니다:
   - **사용자 계정** 폴더에서 마우스 오른쪽 메뉴를 사용합니다:
     1. 콘솔 트리에서 **고급** 폴더를 확장하고 **사용자 계정** 하위 폴더를 선택합니다.
     2. **사용자 계정** 폴더의 작업 영역에서 관리 중인 기기 목록에 추가하려는 모바일 기기가 있는 사용자, 보안 그룹 또는 Active Directory 보안 그룹을 선택합니다.
     3. 마우스 오른쪽 버튼을 누르고 사용자 계정의 마우스 오른쪽 메뉴에서 **모바일 기기 추가**를 선택합니다.
        모바일 기기 연결 마법사가 시작됩니다.
   - **모바일 기기** 폴더의 작업 영역에서 **모바일 기기 추가** 버튼을 누릅니다:
     1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **모바일 기기** 하위 폴더를 선택합니다.
     2. **모바일 기기** 하위 폴더의 작업 영역에서 **모바일 기기 추가** 버튼을 누릅니다.
        모바일 장치 연결 마법사가 시작됩니다.
2. 마법사의 **운영 체제** 페이지에서 모바일 기기 운영 체제 유형으로 **iOS**를 선택합니다.
3. **iOS MDM 서버 선택** 페이지에서 iOS MDM 서버를 선택합니다.
4. **모바일 기기를 관리할 사용자 선택** 페이지에서 관리 중인 기기 목록에 추가하려는 모바일 기기가 있는 사용자, 보안 그룹, Active Directory 보안 그룹을 선택합니다.

   사용자 계정 폴더의 마우스 오른쪽 메뉴에서 **모바일 기기 추가**를 선택하여 마법사를 시작했다면 이 단계를 건너뜁니다.

   새 사용자 계정을 목록에 추가하려면 **추가** 버튼을 누르고 창이 열리면 사용자 계정 속성을 입력합니다. 사용자 계정 속성을 수정하거나 검토하려면 목록에서 사용자 계정을 선택하고 **속성** 버튼을 누릅니다.

5. 마법사의 **인증서 소스** 페이지에서 중앙 관리 서버가 모바일 기기 식별에 사용할 공유 인증서의 생성 방법을 지정합니다. 다음 방법 중 하나를 사용해 공유 인증서를 지정할 수 있습니다:

   - **중앙 관리 서버 도구를 통해 인증서 발급**

     이전에 만들지 않은 경우, 중앙 관리 서버 도구를 사용하여 새 인증서를 만들려면 이 옵션을 선택합니다.

     이 옵션을 선택하면 중앙 관리 서버에서 생성된 인증서로 iOS MDM 프로필이 자동 서명됩니다.

     이 옵션은 기본적으로 선택되어 있습니다.

   - **인증서 파일 지정**

     이전에 생성된 인증서 파일을 지정하려면 이 옵션을 선택합니다.

     이전 단계에서 여러 사용자를 선택한 경우 이 방법은 사용할 수 없습니다.

6. 마법사의 **사용자 알림 방법** 페이지에서 모바일 기기 사용자에게 SMS나 이메일로 인증서 생성 알림을 전달하기 위한 설정을 정의합니다:

   - **마법사에 QR 코드 표시**

     이 옵션을 선택하면 모바일 기기 연결 마법사의 마지막 단계에서 설치 패키지 링크가 표시됩니다.

     기기 연결에서 사용자를 여러 명 선택한 경우 이 옵션은 사용할 수 없습니다.

   - **사용자에게 QR 코드 전송**

     이 옵션을 선택하면 새 모바일 기기 연결에 대한 사용자 알림을 구성할 수 있습니다.

     이메일 주소 형식을 선택하고 추가 이메일 주소를 지정할 수 있으며 메시지 내용을 편집할 수 있습니다. SMS 메시지 전송을 위한 사용자 전화 번호 형식을 선택하고 추가 전화 번호를 지정하거나 SMS 메시지 내용을 편집할 수도 있습니다.

     SMTP 서버가 구성되지 않은 경우 이메일 메시지를 사용자에게 전송할 수 없습니다. SMS 알림이 구성되지 않은 경우 SMS 메시지를 사용자에게 전송할 수 없습니다.

7. **결과** 페이지에서 **마침**을 눌러 마법사를 닫습니다.

iOS MDM 프로필이 Kaspersky Security Center 웹 서버에 자동으로 게시됩니다. 모바일 기기 사용자는 웹 서버에서 iOS MDM 프로필을 다운로드할 수 있는 링크와 함께 알림을 받게 됩니다. 사용자가 링크를 누릅니다. 그 다음 모바일 기기의 운영 체제가 iOS MDM 프로필 설치에 동의할 것인지를 물어봅니다. 사용자가 iOS MDM 프로필을 설치하는 데 동의해야 iOS MDM 프로필을 모바일 기기에 다운로드할 수 있습니다. iOS MDM 프로필이 다운로드되어 모바일 기기가 중앙 관리 서버와 동기화되면 콘솔 트리에서 **모바일 기기 관리** 폴더의 하위 폴더인 **모바일 기기** 폴더에 기기가 표시됩니다.

링크를 이용해 사용자가 Kaspersky Security Center 웹 서버로의 진행을 허용하려면, 모바일 기기에서 8061 포트를 통한 중앙 관리 서버와의 연결이 가능해야 합니다.

관리 중인 기기 목록에 Android 모바일 기기 추가

관리 중인 기기 목록에 Android 모바일 기기를 추가하려면 반드시 Kaspersky Endpoint Security for Android와 공유 인증서를 모바일 기기에 전달하고 설치해야 합니다. 공유 인증서는 모바일 기기를 식별하기 위해 중앙 관리 서버에서 사용합니다. 모바일 기기에 공유 인증서가 전달되고 설치되면 해당 기기가 관리 중인 기기 목록에 나타납니다.

모바일 기기 연결 마법사를 사용하여 사용자의 모바일 기기를 관리 중인 기기 목록에 추가할 수 있습니다. 마법사는 공유 인증서 및 Kaspersky Endpoint Security for Android의 전달 및 설치 시 두 가지 옵션을 제공합니다:

- Google Play 링크 사용
- Kaspersky Security Center 웹 서버에서 생성된 링크 사용

  중앙 관리 서버에 배포하기 위해 저장된 Kaspersky Endpoint Security for Android 설치 패키지를 설치에 사용합니다

모바일 기기 연결 마법사 시작

모바일 기기 연결 마법사를 시작하려면 다음 중 하나를 수행합니다:

- **사용자 계정** 폴더에서 마우스 오른쪽 메뉴를 사용합니다:

  1. 콘솔 트리에서 **고급** 폴더를 확장하고 **사용자 계정** 하위 폴더를 선택합니다.
  2. **사용자 계정** 폴더의 작업 영역에서 관리 중인 기기 목록에 추가하려는 모바일 기기가 있는 사용자, 보안 그룹 또는 Active Directory 보안 그룹을 선택합니다.
  3. 마우스 오른쪽 버튼을 누르고 사용자 계정의 마우스 오른쪽 메뉴에서 **모바일 기기 추가**를 선택합니다.

     모바일 기기 연결 마법사가 시작됩니다.

- **모바일 기기** 폴더의 작업 영역에서 **모바일 기기 추가** 버튼을 누릅니다:

  1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **모바일 기기** 하위 폴더를 선택합니다.
  2. **모바일 기기** 하위 폴더의 작업 영역에서 **모바일 기기 추가** 버튼을 누릅니다.

     모바일 기기 연결 마법사가 시작됩니다.

Google Play 링크를 사용하여 Android 모바일 기기 추가

Google Play 링크를 사용하여 모바일 기기에 Kaspersky Endpoint Security for Android와 공유 인증서를 설치하려면 다음과 같이 하십시오:

1. 모바일 기기 연결 마법사를 시작합니다.
2. 마법사의 **운영 체제** 페이지에서 모바일 기기 운영 체제 유형으로 **Android**를 선택합니다.
3. 마법사의 **기기에서 Kaspersky Endpoint Security for Android를 설치하는 방법** 페이지에서 **Google Play에서 앱 다운로드**를 선택합니다.
4. 마법사의 **모바일 기기를 관리할 사용자 선택** 페이지에서 관리 중인 기기 목록에 추가하려는 모바일 기기가 있는 사용자, 보안 그룹, Active Directory 보안 그룹 중 하나를 선택합니다.

사용자 계정 폴더의 마우스 오른쪽 메뉴에서 **모바일 기기 추가**를 선택하여 마법사를 시작했다면 이 단계를 건너뜁니다.

새 사용자 계정을 목록에 추가하려면 **추가** 버튼을 누르고 창이 열리면 사용자 계정 속성을 입력합니다. 사용자 계정 속성을 수정하거나 검토하려면 목록에서 사용자 계정을 선택하고 **속성** 버튼을 누릅니다.

5. 마법사의 **인증서 소스** 페이지에서 중앙 관리 서버가 모바일 기기 식별에 사용할 공유 인증서의 생성 방법을 지정합니다. 다음 방법 중 하나를 사용해 공유 인증서를 지정할 수 있습니다:

   - **중앙 관리 서버 도구를 통해 인증서 발급**

     이전에 만들지 않은 경우, 중앙 관리 서버 도구를 사용하여 새 인증서를 만들려면 이 옵션을 선택합니다.

     이 옵션을 선택하면 중앙 관리 서버 도구를 사용하여 인증서가 자동으로 발급됩니다.

     이 옵션은 기본적으로 선택되어 있습니다.

   - **인증서 파일 지정**

     이전에 생성된 인증서 파일을 지정하려면 이 옵션을 선택합니다.

     이전 단계에서 여러 사용자를 선택한 경우 이 방법은 사용할 수 없습니다.

6. 마법사의 **사용자 알림 방법** 페이지에서 모바일 기기 사용자에게 SMS나 이메일로 인증서 생성 알림을 전달하기 위한 설정을 정의합니다:

   - **마법사에 QR 코드 표시**

     이 옵션을 선택하면 모바일 기기 연결 마법사의 마지막 단계에서 설치 패키지 링크가 표시됩니다.

     기기 연결에서 사용자를 여러 명 선택한 경우 이 옵션은 사용할 수 없습니다.

   - **사용자에게 QR 코드 전송**

     이 옵션을 선택하면 새 모바일 기기 연결에 대한 사용자 알림을 구성할 수 있습니다.

     이메일 주소 형식을 선택하고 추가 이메일 주소를 지정할 수 있으며 메시지 내용을 편집할 수 있습니다. SMS 메시지 전송을 위한 사용자 전화 번호 형식을 선택하고 추가 전화 번호를 지정하거나 SMS 메시지 내용을 편집할 수도 있습니다.

     SMTP 서버가 구성되지 않은 경우 이메일 메시지를 사용자에게 전송할 수 없습니다. SMS 알림이 구성되지 않은 경우 SMS 메시지를 사용자에게 전송할 수 없습니다.

7. **결과** 페이지에서 **마침**을 눌러 마법사를 닫습니다.

마법사가 완료된 후 Kaspersky Endpoint Security for Android를 다운로드할 수 있도록 사용자의 모바일 기기로 링크와 QR 코드가 전송됩니다. 사용자는 해당 링크를 클릭하거나 QR 코드를 스캔합니다. 그 다음 모바일 기기의 운영 체제가 Kaspersky Endpoint Security for Android 설치에 동의할 것인지를 물어봅니다. Kaspersky Endpoint Security for Android가 다운로드되고 설치된 후 모바일 기기는 중앙 관리 서버에 연결 및 공유 인증서를 다운로드합니다. 인증서가 모바일 기기에 설치된 이후에 콘솔 트리의 **모바일 기기 관리** 폴더의 하위 폴더인 **모바일 기기** 폴더에 후자가 표시됩니다.

Kaspersky Security Center 웹 서버의 링크를 사용하여 Android 모바일 기기 추가

중앙 관리 서버에 게시된 Kaspersky Endpoint Security for Android 설치 패키지를 설치에 사용합니다.

웹 서버의 링크를 사용하여 모바일 기기에 Kaspersky Endpoint Security for Android와 공유 인증서를 설치하려면 다음과 같이 하십시오:

1. 모바일 장치 연결 마법사를 시작합니다.
2. 마법사의 **운영 체제** 페이지에서 모바일 장치 운영 체제 유형으로 **Android**를 선택합니다.
3. 마법사의 **기기에서 Kaspersky Endpoint Security for Android를 설치하는 방법** 페이지에서 **Kaspersky Security Center에서 설치 패키지 앱 다운로드**을 선택합니다.

   아래에 나타나는 필드에서 설치 패키지를 선택하거나 **새로 생성**를 눌러 패키지를 새로 만듭니다.
4. 마법사의 **모바일 기기를 관리할 사용자 선택** 페이지에서 관리 중인 기기 목록에 추가하려는 모바일 기기가 있는 사용자, 보안 그룹, Active Directory 보안 그룹 중 하나를 선택합니다.

   사용자 계정 폴더의 마우스 오른쪽 메뉴에서 **모바일 기기 추가**를 선택하여 마법사를 시작했다면 이 단계를 건너뜁니다.

   새 사용자 계정을 목록에 추가하려면 **추가** 버튼을 누르고 창이 열리면 사용자 계정 속성을 입력합니다. 사용자 계정 속성을 수정하거나 검토하려면 목록에서 사용자 계정을 선택하고 **속성** 버튼을 누릅니다.
5. 마법사의 **인증서 소스** 페이지에서 중앙 관리 서버가 모바일 기기 식별에 사용할 공유 인증서의 생성 방법을 지정합니다. 다음 방법 중 하나를 사용해 공유 인증서를 지정할 수 있습니다:

   - **중앙 관리 서버 도구를 통해 인증서 발급**

     이전에 만들지 않은 경우, 중앙 관리 서버 도구를 사용하여 새 인증서를 만들려면 이 옵션을 선택합니다.

     이 옵션을 선택하면 중앙 관리 서버 도구를 사용하여 인증서가 자동으로 발급됩니다.

     이 옵션은 기본적으로 선택되어 있습니다.

   - **인증서 파일 지정**

     이전에 생성된 인증서 파일을 지정하려면 이 옵션을 선택합니다.

     이전 단계에서 여러 사용자를 선택한 경우 이 방법은 사용할 수 없습니다.
6. 마법사의 **사용자 알림 방법** 페이지에서 모바일 기기 사용자에게 SMS나 이메일로 인증서 생성 알림을 전달하기 위한 설정을 정의합니다:

   - **마법사에 QR 코드 표시**

     이 옵션을 선택하면 모바일 기기 연결 마법사의 마지막 단계에서 설치 패키지 링크가 표시됩니다.

     기기 연결에서 사용자를 여러 명 선택한 경우 이 옵션은 사용할 수 없습니다.

- **사용자에게 QR 코드 전송**

  이 옵션을 선택하면 새 모바일 기기 연결에 대한 사용자 알림을 구성할 수 있습니다.

  이메일 주소 형식을 선택하고 추가 이메일 주소를 지정할 수 있으며 메시지 내용을 편집할 수 있습니다. SMS 메시지 전송을 위한 사용자 전화 번호 형식을 선택하고 추가 전화 번호를 지정하거나 SMS 메시지 내용을 편집할 수도 있습니다.

  SMTP 서버가 구성되지 않은 경우 이메일 메시지를 사용자에게 전송할 수 없습니다. SMS 알림이 구성되지 않은 경우 SMS 메시지를 사용자에게 전송할 수 없습니다.

7. **결과** 페이지에서 **마침**을 눌러 마법사를 닫습니다.

Kaspersky Endpoint Security for Android의 모바일 앱 패키지가 Kaspersky Security Center 웹 서버에 자동으로 게시됩니다. 모바일 앱 패키지는 앱, 중앙 관리 서버로의 모바일 기기 연결 설정 및 인증서를 포함하고 있습니다. 모바일 기기는 웹 서버에서 패키지를 다운로드할 수 있는 링크가 있는 알림을 받습니다. 사용자가 링크를 누릅니다. 기기의 운영 체제에서 모바일 앱 패키지 설치에 동의할 것인지를 묻는 메시지를 표시합니다. 만일 사용자가 동의할 경우 모바일 기기에 패키지가 다운로드됩니다. 패키지가 다운로드되어 모바일 기기가 중앙 관리 서버와 동기화되면 콘솔 트리에서 **모바일 기기 관리** 폴더의 하위 폴더인 **모바일 기기** 폴더에 기기가 표시됩니다.

iOS MDM 기기 관리

이 섹션에는 Kaspersky Security Center를 통한 iOS MDM 기기 관리의 고급 기능이 나와있습니다. 이 애플리케이션은 다음과 같은 iOS MDM 기기 관리 기능을 지원합니다:

- 중앙 집중식 모드로 관리 iOS MDM 기기의 설정을 정의하고 구성 프로필을 통해 기기의 기능을 제한합니다. 구성 프로필을 추가하거나 수정하고 모바일 기기에 설치할 수 있습니다.
- 프로비저닝 프로필을 통해 앱 스토어에 없는 앱을 모바일 기기에 설치합니다. 예를 들어 프로비저닝 프로필을 사용해 자체 제작한 기업 앱을 사용자의 모바일 기기에 설치할 수 있습니다. 프로비저닝 프로필에는 앱과 모바일 기기에 대한 정보가 포함되어 있습니다.
- App Store를 통해 iOS MDM 기기에 앱을 설치합니다. iOS MDM 기기에 앱을 설치하기 전에 iOS MDM 서버에 해당 앱을 추가해야 합니다.

24시간마다 iOS MDM 서버와 데이터를 동기화하기 위해 모든 연결된 iOS MDM 기기로 푸시 알림을 보냅니다.

구성 프로필과 프로비저닝 프로필, 그리고 iOS MDM 기기에 설치된 앱에 대한 정보는 기기의 속성 창을 참조하십시오.

인증서로 iOS MDM 프로필 서명

인증서로 iOS MDM 프로필에 서명할 수 있습니다. 직접 발급한 인증서를 사용하거나 신뢰할 수 있는 인증 기관으로부터 인증서를 받을 수 있습니다.

iOS 기기는 서명하지 않은 프로필에 대한 고지 사항을 표시하며 프로필을 설치할 때 사용자에게 서명자를 신뢰하라는 메시지를 표시합니다.

인증서로 iOS MDM 프로필에 서명하려면 다음을 수행하십시오.

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
2. **모바일 기기** 폴더의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

3. 폴더의 속성 창에서 **iOS 장치용 연결 설정** 섹션을 선택합니다.

4. **인증서 파일 선택** 필드 아래에서 **찾기** 버튼을 누릅니다.
   인증서 창.

5. **인증서 유형** 필드에서 인증서 유형을 공개 또는 개인으로 지정합니다.

   - **PKCS #12 컨테이너** 값이 선택되면 인증서 파일과 암호를 지정합니다.
   - **X.509 인증서** 값을 선택한 경우:

     a. 개인 키 파일을 지정합니다(*.prk 또는 *.pem 확장자).

     b. 개인 키 암호를 지정합니다.

     c. 공개 키 파일을 지정합니다(*.cer 확장자).

6. **확인**를 누릅니다.

iOS MDM 프로필은 인증서로 서명됩니다.

구성 프로필 추가

구성 프로필을 생성하기 위해 Apple Inc. 웹 사이트에서 제공되는 Apple Configurator 2를 사용할 수 있습니다. Apple Configurator 2는 macOS를 실행하는 기기에서만 작동합니다. 이러한 기기를 사용할 수 없는 경우 관리 콘솔이 지원되는 기기에서 iPhone 구성 유틸리티를 대신 사용할 수 있습니다. 그러나 Apple Inc.에서는 더 이상 iPhone 구성 유틸리티를 지원하지 않습니다.

iPhone 구성 유틸리티를 사용하여 구성 프로필을 만들고 iOS MDM 서버에 추가하려면:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 선택합니다.

2. **모바일 기기 관리** 폴더의 작업 영역에서 **모바일 기기 서버** 하위 폴더를 선택합니다.

3. **모바일 기기 서버** 폴더의 작업 영역에서 iOS MDM 서버를 선택합니다.

4. iOS MDM 서버의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   모바일 기기 서버 속성 창이 열립니다.

5. iOS MDM 서버의 속성 창에서 **구성 프로필** 섹션을 선택합니다.

6. **구성 프로필** 섹션에서 **만들기** 버튼을 누릅니다.
   새 구성 프로필 창이 열립니다.

7. **새 구성 프로필** 창에서 프로필의 이름과 ID를 지정합니다.
   구성 프로필 ID는 고유해야 하며, 역순 DNS 형식(예: *com.companyname.identifier*)으로 값을 지정해야 합니다.

8. **확인**를 누릅니다.
   iPhone 구성 유틸리티가 설치되어 있으면 시작됩니다.

9. iPhone 구성 유틸리티에서 구성 프로필을 재구성합니다.

   프로필 설정에 대한 설명과 프로필 구성 방법에 대한 지침은 iPhone 구성 유틸리티에 함께 포함된 설명서를 참조하십시오.

   iPhone 구성 유틸리티를 사용해 프로필을 구성한 후에는 새 구성 프로필이 iOS MDM 서버 속성 창의 **구성 프로필** 섹션에 표시됩니다.

   수정 버튼을 눌러 구성 프로필을 수정할 수 있습니다.

   가져오기 버튼을 눌러 프로그램으로 구성 프로필을 로드할 수 있습니다.

   내보내기 버튼을 눌러 구성 프로필을 파일에 저장할 수 있습니다.

생성한 프로필은 iOS MDM 기기에 설치해야 합니다.

기기에 구성 프로필 설치

모바일 기기에 구성 프로필을 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.

   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.

2. 작업 영역에서 프로토콜 유형(*iOS MDM*)을 눌러 iOS MDM 기기를 필터링합니다.

3. 구성 프로필을 설치해야 하는 사용자의 모바일 기기를 선택합니다.

   여러 모바일 기기를 선택하여 프로필을 동시에 설치할 수 있습니다.

4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.

5. **모바일 기기 관리 명령** 창에서 **프로필 설치** 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.

   모바일 기기의 마우스 오른쪽 메뉴에서 **모든 명령**를 선택한 다음 **프로필 설치**을 선택하여 모바일 기기로 명령을 보낼 수도 있습니다.

   프로필 선택 창이 열리고 프로필 목록이 표시됩니다. 모바일 기기에 설치해야 하는 프로필을 목록에서 선택합니다. 여러 프로필을 선택하여 모바일 기기에 동시에 설치할 수 있습니다. 프로필 범위를 선택하려면 **SHIFT** 키를 사용합니다. 여러 프로필을 그룹으로 결합하려면 **CTRL** 키를 사용합니다.

6. **확인**를 눌러 모바일 기기로 명령을 보냅니다.

   명령이 실행되면 선택한 구성 프로필이 사용자 모바일 기기에 설치됩니다. 명령이 성공적으로 실행되면 명령 로그의 현재 상태가 *완료*로 표시됩니다.

   재전송 버튼을 눌러 사용자의 모바일 기기에 명령을 다시 보낼 수 있습니다.

   예약 목록에서 제거 버튼을 눌러 아직 실행되지 않은 명령의 실행을 취소할 수 있습니다.

   명령 로그 섹션에 모바일 기기로 보낸 명령이 각각의 실행 상태와 함께 표시됩니다. **새로 고침**를 눌러 명령 목록을 업데이트합니다.

7. **확인**를 눌러 **모바일 기기 매니지먼트 명령** 창을 닫습니다.

설치한 프로필을 확인하고 필요한 경우 제거할 수 있습니다.

기기에서 구성 프로필 제거

모바일 기기에서 구성 프로필을 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.
2. 작업 영역에서 **iOS MDM** 링크를 눌러 iOS MDM 기기를 필터링합니다.
3. 구성 프로필을 제거해야 하는 사용자의 모바일 기기를 선택합니다.
   여러 모바일 기기를 선택하여 프로필을 동시에 제거할 수 있습니다.
4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.
5. **모바일 기기 관리 명령** 창에서 **프로필 제거** 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.
   기기의 마우스 오른쪽 메뉴에서 **모든 명령**를 선택한 다음 **프로필 제거**을 선택하여 모바일 기기로 명령을 보낼 수도 있습니다.
   프로필 제거 창이 열리고 프로필 목록이 표시됩니다.
6. 모바일 기기에서 제거해야 하는 프로필을 목록에서 선택합니다. 여러 프로필을 선택하여 모바일 기기에서 동시에 제거할 수 있습니다. 프로필 범위를 선택하려면 **SHIFT** 키를 사용합니다. 여러 프로필을 그룹으로 결합하려면 **CTRL** 키를 사용합니다.
7. **확인**를 눌러 모바일 기기로 명령을 보냅니다.
   명령이 실행되면 선택한 구성 프로필이 사용자 모바일 기기에서 제거됩니다. 명령이 성공적으로 실행되면 현재 상태가 *완료*로 표시됩니다.
   재전송 버튼을 눌러 사용자의 모바일 기기에 명령을 다시 보낼 수 있습니다.
   예약 목록에서 제거 버튼을 눌러 아직 실행되지 않은 명령의 실행을 취소할 수 있습니다.
   명령 로그 섹션에 모바일 기기로 보낸 명령이 각각의 실행 상태와 함께 표시됩니다. **새로 고침**를 눌러 명령 목록을 업데이트합니다.
8. **확인**를 눌러 **모바일 기기 관리 명령** 창을 닫습니다.

프로필에 대한 링크를 게시하여 새 기기 추가

관리 콘솔에서 관리자가 인증서 설치 마법사를 사용하여 새 iOS MDM 프로필을 만듭니다. 마법사는 다음 작업을 수행합니다:

- iOS MDM 프로필이 웹 서버에 자동으로 게시됩니다.
- SMS 또는 이메일로 iOS MDM 프로필의 링크를 사용자에게 보냅니다. 링크를 받은 사용자는 모바일 기기에 iOS MDM 프로필을 설치합니다.
- 모바일 기기가 iOS MDM 서버에 연결됩니다.

Apple에서 보다 엄격한 보안 정책을 도입함에 따라, PKI(공개키 인프라)와의 통합이 활성된 중앙 관리 서버에 iOS 11을 실행하는 모바일 기기를 연결할 때는 TLS 1.1 및 TLS 1.2 프로토콜 버전을 설정해야 합니다.

관리자가 프로필을 설치하는 방식으로 새 모바일 기기 추가

모바일 기기에 iOS MDM 프로필을 설치하여 해당 기기를 iOS MDM 서버에 연결하려는 경우 관리자가 다음 작업을 수행해야 합니다:

1. 관리 콘솔에서 인증서 설치 마법사를 엽니다.
2. 마법사 창에서 **마법사 완료 후 인증서 보기** 확인란을 선택하여 새 iOS MDM 프로필을 만듭니다.
3. iOS MDM 프로필을 저장합니다.
4. Apple Configurator 유틸리티를 통해 사용자의 모바일 기기에 iOS MDM 프로필을 설치합니다.

   모바일 기기가 iOS MDM 서버에 연결됩니다.

Apple에서 보다 엄격한 보안 정책을 도입함에 따라, PKI(공개키 인프라)와의 통합이 활성된 중앙 관리 서버에 iOS 11을 실행하는 모바일 기기를 연결할 때는 TLS 1.1 및 TLS 1.2 프로토콜 버전을 설정해야 합니다.

프로비저닝 프로필 추가

iOS MDM 서버에 프로비저닝 프로필을 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 엽니다.
2. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기 서버** 하위 폴더를 선택합니다.
3. **모바일 기기 서버** 폴더의 작업 영역에서 iOS MDM 서버를 선택합니다.
4. iOS MDM 서버의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   모바일 기기 서버 속성 창이 열립니다.
5. **iOS MDM 서버**의 속성 창에서 **프로비저닝 프로필** 섹션을 선택합니다.
6. **프로비저닝 프로필** 속성 창에서 **가져오기** 버튼을 누르고 프로비저닝 프로필 파일의 경로를 지정합니다.

   프로필이 iOS MDM 서버 설정에 추가됩니다.

   내보내기 버튼을 눌러 프로비저닝 프로필을 파일에 저장할 수 있습니다.

iOS MDM 기기에서 가져온 프로비저닝 프로필을 설치할 수 있습니다.

기기에 프로비저닝 프로필 설치

모바일 기기에 프로비저닝 프로필을 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.

2. 작업 영역에서 프로토콜 유형(*iOS MDM*)을 눌러 iOS MDM 기기를 필터링합니다.

3. 프로비저닝 프로필을 설치해야 하는 사용자의 모바일 기기를 선택합니다.

   여러 모바일 기기를 선택하여 프로비저닝 프로필을 동시에 설치할 수 있습니다.

4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.

5. **모바일 기기 관리 명령** 창에서 **프로비저닝 프로필 설치** 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.

   모바일 기기의 마우스 오른쪽 메뉴에서 **모든 명령**를 선택한 다음 **프로비저닝 프로필 설치**를 선택하여 모바일 기기로 명령을 보낼 수도 있습니다.

   프로비저닝 프로필 선택 창이 열리고 프로비저닝 프로필 목록이 표시됩니다. 모바일 기기에 설치해야 하는 프로비저닝 프로필을 목록에서 선택합니다. 여러 프로비저닝 프로필을 선택하여 모바일 기기에 동시에 설치할 수 있습니다. 프로비저닝 프로필 범위를 선택하려면 **SHIFT** 키를 사용합니다. 여러 프로비저닝 프로필을 그룹으로 결합하려면 **CTRL** 키를 사용합니다.

6. **확인**를 눌러 모바일 기기로 명령을 보냅니다.

   명령이 실행되면 선택한 프로비저닝 프로필이 사용자 모바일 기기에 설치됩니다. 명령이 성공적으로 실행되면, 명령 로그의 현재 상태가 *완료*로 표시됩니다.

   재전송 버튼을 눌러 사용자의 모바일 기기에 명령을 다시 보낼 수 있습니다.

   예약 목록에서 제거 버튼을 눌러 아직 실행되지 않은 명령의 실행을 취소할 수 있습니다.

   명령 로그 섹션에 모바일 기기로 보낸 명령이 각각의 실행 상태와 함께 표시됩니다. **새로 고침**를 눌러 명령 목록을 업데이트합니다.

7. **확인**를 눌러 **모바일 기기 매니지먼트 명령** 창을 닫습니다.

설치한 프로필을 확인하고 필요한 경우 제거할 수 있습니다.

기기에서 프로비저닝 프로필 제거

모바일 기기에서 프로비저닝 프로필을 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.

   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.

2. 작업 영역에서 프로토콜 유형(*iOS MDM*)을 눌러 iOS MDM 기기를 필터링합니다.

3. 프로비저닝 프로필을 제거해야 하는 사용자의 모바일 기기를 선택합니다.

   여러 모바일 기기를 선택하여 프로비저닝 프로필을 동시에 제거할 수 있습니다.

4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.

5. **모바일 기기 관리 명령** 창에서 **프로비저닝 프로필 제거** 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.

   마우스 오른쪽 메뉴에서 **모든 명령**을 선택한 다음 **프로비저닝 프로필 제거**를 선택하여 모바일 기기로 명령을 보낼 수도 있습니다.

   프로비저닝 프로필 제거 창이 열리고 프로필 목록이 표시됩니다.

6. 모바일 기기에서 제거해야 하는 프로비저닝 프로필을 목록에서 선택합니다. 여러 프로비저닝 프로필을 선택하여 모바일 기기에서 동시에 제거할 수 있습니다. 프로비저닝 프로필 범위를 선택하려면 **SHIFT** 키를 사용합니다. 여러 프로비저닝 프로필을 그룹으로 결합하려면 **CTRL** 키를 사용합니다.

7. **확인**를 눌러 모바일 기기로 명령을 보냅니다.

명령이 실행되면 선택한 프로비저닝 프로필이 사용자 모바일 기기에서 제거됩니다. 삭제된 프로비저닝 프로필과 관련된 애플리케이션은 작동할 수 없습니다. 명령이 성공적으로 실행되면 현재 상태가 *완료*로 표시됩니다.

재전송 버튼을 눌러 사용자의 모바일 기기에 명령을 다시 보낼 수 있습니다.

예약 목록에서 제거 버튼을 눌러 아직 실행되지 않은 명령의 실행을 취소할 수 있습니다.

명령 로그 섹션에 모바일 기기로 보낸 명령이 각각의 실행 상태와 함께 표시됩니다. **새로 고침**를 눌러 명령 목록을 업데이트합니다.

8. **확인**를 눌러 **모바일 기기 관리 명령** 창을 닫습니다.

관리 애플리케이션 추가

iOS MDM 기기에 앱을 설치하기 전에 iOS MDM 서버에 해당 앱을 추가해야 합니다. Kaspersky Security Center를 통해 기기에 설치된 애플리케이션은 관리되는 것으로 간주됩니다. 관리 애플리케이션은 Kaspersky Security Center를 통해 원격으로 관리할 수 있습니다.

iOS MDM 서버에 관리 애플리케이션을 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 엽니다.
2. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기 서버** 하위 폴더를 선택합니다.
3. **모바일 기기 서버** 폴더의 작업 영역에서 iOS MDM 서버를 선택합니다.
4. iOS MDM 서버의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   그러면 iOS MDM 서버의 속성 창이 열립니다.
5. iOS MDM 서버의 속성 창에서 **관리 중인 애플리케이션** 섹션을 선택합니다.
6. **관리 중인 애플리케이션** 섹션에서 **추가** 버튼을 누릅니다.
   애플리케이션 추가 창이 열립니다.
7. **애플리케이션 추가** 창의 **앱 이름** 필드에 추가할 애플리케이션의 이름을 지정합니다.
8. **매니페스트 파일에 대한 Apple ID 또는 링크** 필드에 추가할 애플리케이션의 Apple ID를 지정하거나 애플리케이션 다운로드에 사용할 수 있는 매니페스트 파일 링크를 지정합니다.
9. 사용자의 모바일 기기에서 iOS MDM 프로필과 함께 관리 애플리케이션을 삭제하려면 **iOS MDM 프로필과 함께 제거** 확인란을 선택합니다.
10. iTunes를 통한 애플리케이션 데이터 백업을 차단하려면 **데이터 백업 차단** 확인란을 선택합니다.
11. **확인**를 누릅니다.

추가된 애플리케이션이 iOS MDM 서버의 속성 창에 있는 **관리 중인 애플리케이션** 섹션에 표시됩니다.

모바일 기기에 앱 설치

iOS MDM 모바일 기기에 앱을 설치하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.

   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.

2. 앱을 설치할 iOS MDM 기기를 선택합니다.

   애플리케이션을 동시에 설치할 여러 개의 모바일 기기를 선택할 수 있습니다.

3. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.

4. **모바일 기기 관리 명령** 창에서 **앱 설치** 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.

   모바일 기기의 마우스 오른쪽 메뉴에서 **모든 명령**를 선택한 다음 **앱 설치**를 선택하여 모바일 기기로 명령을 보낼 수도 있습니다.

   앱 선택 창이 열리고 프로필 목록이 표시됩니다. 모바일 기기에 설치해야 하는 애플리케이션을 목록에서 선택합니다. 여러 애플리케이션을 선택하여 모바일 기기에 동시에 설치할 수 있습니다. 앱의 범위를 선택하려면 **SHIFT** 키를 사용합니다. 앱을 그룹으로 통합하려면 **CTRL** 키를 사용합니다.

5. **확인**을 눌러 모바일 기기로 명령을 보냅니다.

   명령이 실행되면 선택된 애플리케이션이 사용자의 모바일 기기에 설치됩니다. 명령이 성공적으로 실행되면, 명령 로그의 현재 상태가 *완료*로 표시됩니다.

   재전송 버튼을 눌러 사용자의 모바일 기기에 명령을 다시 보낼 수 있습니다. **예약 목록에서 제거** 버튼을 눌러 아직 실행되지 않은 명령의 실행을 취소할 수 있습니다.

   명령 로그 섹션에 모바일 기기로 보낸 명령이 각각의 실행 상태와 함께 표시됩니다. **새로 고침**를 눌러 명령 목록을 업데이트합니다.

6. **확인**를 눌러 **모바일 기기 매니지먼트 명령** 창을 닫습니다.

설치된 애플리케이션에 대한 정보는 iOS MDM 모바일 기기의 속성에서 보여집니다. 명령 로그 또는 모바일 기기의 마우스 오른쪽 메뉴를 통해 모바일 기기에서 애플리케이션을 제거할 수 있습니다.

기기에서 앱 제거

모바일 기기에서 앱을 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.

   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.

2. 작업 영역에서 프로토콜 유형(*iOS MDM*)을 눌러 iOS MDM 기기를 필터링합니다.

3. 앱을 제거할 사용자의 모바일 기기를 선택합니다.

   앱을 동시에 제거할 모바일 기기를 여러 개 선택할 수 있습니다.

4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.

5. **모바일 기기 관리 명령** 창에서 **앱 제거** 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.

   모바일 기기의 마우스 오른쪽 메뉴에서 **모든 명령**을 선택한 다음 **앱 제거**를 선택하여 모바일 기기로 명령을 보낼 수도 있습니다.

앱 제거 창이 열려 애플리케이션 목록을 보여줍니다.

6. 모바일 기기에서 제거해야 하는 앱을 목록에서 선택합니다. 동시에 제거할 앱을 여러 개 선택할 수 있습니다. 앱의 범위를 선택하려면 **SHIFT** 키를 사용합니다. 앱을 그룹으로 통합하려면 **CTRL** 키를 사용합니다.

7. **확인**를 눌러 모바일 기기로 명령을 보냅니다.

   명령이 실행되면 선택된 앱이 사용자의 모바일 기기에서 제거됩니다. 명령이 성공적으로 실행되면 현재 상태가 *완료*로 표시됩니다.

   재전송 버튼을 눌러 사용자의 모바일 기기에 명령을 다시 보낼 수 있습니다.

   예약 목록에서 제거 버튼을 눌러 아직 실행되지 않은 명령의 실행을 취소할 수 있습니다.

   명령 로그 섹션에 모바일 기기로 보낸 명령이 각각의 실행 상태와 함께 표시됩니다. **새로 고침**를 눌러 명령 목록을 업데이트합니다.

8. **확인**를 눌러 **모바일 기기 관리 명령** 창을 닫습니다.

iOS MDM 모바일 기기에서 로밍 구성

로밍을 구성하려면 다음과 같이 진행합니다:

1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 엽니다.

2. **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.

   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.

3. 로밍을 구성해야 하는 사용자가 소유한 iOS MDM 기기를 선택합니다.

   로밍을 동시에 구성하려면 여러 개의 모바일 기기를 선택할 수 있습니다.

4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.

5. **모바일 기기 관리 명령** 창에서 **로밍 구성** 섹션으로 이동한 다음 **명령 전송** 버튼을 누릅니다.

   또한 기기의 마우스 오른쪽 메뉴에서 **모든 명령 → 로밍 구성**을 선택하여 모바일 기기로 명령을 보낼 수도 있습니다.

6. **로밍 설정** 창에서 다음 설정을 지정합니다:

   - **데이터 로밍 사용**

     이 옵션을 활성화하면 iOS MDM 모바일 기기에 대한 음성 로밍이 설정됩니다. iOS MDM 모바일 기기의 사용자가 로밍 시 인터넷을 탐색할 수 있습니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

선택한 기기에 대해 로밍이 구성됩니다.

iOS MDM 기기 정보 보기

iOS MDM 기기에 대한 정보를 보려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.
2. 작업 영역에서 **iOS MDM** 링크를 눌러 iOS MDM 기기를 필터링합니다.
3. 정보를 확인할 모바일 기기를 선택합니다.
4. 모바일 기기의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   iOS MDM 기기 속성 창이 열립니다.

모바일 기기의 속성 창에 연결된 iOS MDM 기기의 정보가 표시됩니다.

관리에서 iOS MDM 기기 연결 끊기

iOS MDM 서버에서 iOS MDM 기기의 연결을 끊으려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.
2. 작업 영역에서 **iOS MDM** 링크를 눌러 iOS MDM 기기를 필터링합니다.
3. 연결을 끊을 모바일 기기를 선택합니다.
4. 모바일 기기의 컨텍스트 메뉴에서 **삭제**를 선택합니다.

   iOS MDM 기기가 제거 목록에 표시됩니다. iOS MDM 서버의 데이터베이스에서 모바일 기기가 제거된 후 관리 중인 기기 목록에서 자동으로 제거됩니다. iOS MDM 서버 데이터베이스에서 1분 이내에 모바일 기기가 제거됩니다.

관리에서 iOS MDM 기기의 연결을 끊으면 모든 설치된 구성 프로필과 iOS MDM 프로필 및 **iOS MDM 프로필과 함께 제거** 옵션이 활성화된 애플리케이션이 모바일 기기에서 제거됩니다.

기기에 명령 보내기

iOS MDM 기기에 명령을 보내려면 다음 작업을 수행합니다:

1. 관리 콘솔에서 **모바일 기기 관리** 노드를 엽니다.
2. **모바일 기기** 폴더를 선택합니다.
3. **모바일 기기** 폴더에서 명령을 보내야 하는 모바일 기기를 선택합니다.
4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.
5. 표시되는 목록에서 모바일 기기로 보낼 명령을 선택합니다.

보낸 명령의 실행 상태 확인

모바일 기기로 전송된 명령의 실행 상태를 확인하려면 다음 작업을 수행해야 합니다:

1. 관리 콘솔에서 **모바일 기기 관리** 노드를 엽니다.
2. **모바일 기기** 폴더를 선택합니다.
3. **모바일 기기** 폴더에서 선택한 명령의 실행 상태를 확인해야 하는 모바일 기기를 선택합니다.
4. 모바일 기기의 마우스 오른쪽 메뉴에서 **명령 로그 보기**를 선택합니다.

KES 기기 관리

Kaspersky Security Center에서 다음과 같은 방법으로 KES 모바일 기기를 관리할 수 있습니다.

- 중앙에서 명령을 사용해 KES 기기 관리.
- KES 기기의 관리 설정에 대한 정보를 봅니다.
- 모바일 앱 패키지를 사용해 애플리케이션 설치.
- 관리에서 KES 기기 연결 끊기.

KES 기기용 모바일 애플리케이션 패키지 만들기

KES 기기용 모바일 앱 패키지를 만들려면 Kaspersky Endpoint Security for Android 기기 라이센스가 필요합니다.

모바일 애플리케이션 패키지를 만들려면 다음과 같이 하십시오:

1. 콘솔 트리의 **원격 설치** 폴더에서 **설치 패키지** 하위 폴더를 선택합니다.
   기본적으로 **원격 설치** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. **추가 조치** 버튼을 누르고 드롭다운 목록에서 **모바일 앱 패키지 관리**를 선택합니다.
3. **모바일 앱 패키지 관리** 창에서 **새로 생성** 버튼을 누릅니다.
4. 새 패키지 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

새로 생성된 모바일 애플리케이션 패키지가 **모바일 앱 패키지 관리** 창에 표시됩니다.

KES 기기의 인증서 기반 인증 활성

KES 기기의 인증서 기반 인증을 활성하려면:

1. 중앙 관리 서버가 설치된 클라이언트 기기에서 시스템 레지스트리를 엽니다(예:로컬에서 **시작** → **실행** 메뉴의 regedit 명령 사용).
2. 다음 하이브로 이동합니다:
   - 32비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - 64비트 운영 체제:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. LP_MobileMustUseTwoWayAuthOnPort13292 이름으로 키를 만듭니다.
4. 키 유형으로 REG_DWORD를 지정합니다.
5. 키 값은 1로 설정합니다.
6. 중앙 관리 서버 서비스를 다시 시작합니다.

중앙 관리 서버 서비스를 실행하면, 공유된 인증서를 이용한 KES 기기의 필수 인증서 기반 인증이 활성됩니다.

> 중앙 관리 서버로의 첫 KES 기기의 연결에서는 인증서를 요구하지 않습니다.

기본적으로 KES 기기의 인증서 기반 인증은 비활성되어 있습니다.

KES 기기 정보 보기

KES 기기 정보 보려면:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.
2. 작업 영역에서 프로토콜 유형(*KES*)을 기준으로 KES 기기를 필터링합니다.
3. 정보를 확인할 모바일 기기를 선택합니다.
4. 모바일 기기의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.

KES 기기의 속성 창이 열립니다.

모바일 기기의 속성 창에 연결된 KES 기기 정보가 표시됩니다.

관리에서 KES 기기 연결 끊기

관리에서 KES 기기를 연결 해제하려면, 사용자는 모바일 기기에서 네트워크 에이전트를 제거해야 합니다. 사용자가 네트워크 에이전트를 제거하면 모바일 기기 상세 정보가 중앙 관리 서버 데이터베이스에서 제거되므로 관리자가 관리 중인 기기 목록에서 해당 모바일 기기를 제거할 수 있습니다.

관리 중인 기기 목록에서 KES 기기를 제거하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **모바일 기기 관리** 폴더에서 **모바일 기기** 하위 폴더를 선택합니다.
   폴더 작업 영역에는 관리 중인 모바일 기기 목록이 표시됩니다.
2. 작업 영역에서 프로토콜 유형(*KES*)을 기준으로 KES 기기를 필터링합니다.
3. 관리에서 연결을 끊을 모바일 기기를 선택합니다.
4. 모바일 기기의 컨텍스트 메뉴에서 **삭제**를 선택합니다.

   모바일 기기는 관리 중인 기기 목록에서 제거됩니다.

   만일 모바일 기기에서 Kaspersky Endpoint Security for Android가 제거되지 않았다면, 해당 모바일 기기는 중앙 관리 서버와의 동기화 이후에 관리 중인 기기 목록에 다시 나타납니다.

데이터 암호화 및 보호

데이터 암호화는 노트북, 이동식 드라이브 또는 하드 드라이브를 도난 또는 분실한 경우 또는 승인되지 않은 사용자와 애플리케이션에서 접근하는 경우 원치 않는 유출 위험을 줄여줍니다.

Kaspersky Endpoint Security for Windows는 암호화 기능을 제공합니다. Kaspersky Endpoint Security for Windows는 기기와 이동식 드라이브의 로컬 드라이브에 저장된 파일 및 이동식 드라이브와 하드 드라이브 전체를 암호화합니다.

암호화 규칙은 Kaspersky Security Center의 정책 정의를 통해 구성됩니다. 정책 적용 시 기존 규칙에 따라 암호화 및 복호화가 수행됩니다.

사용자 인터페이스 설정에 의해 암호화 관리 기능의 사용 가능 여부가 결정됩니다.

관리자가 수행할 수 있는 작업은 다음과 같습니다.

- 기기의 로컬 드라이브에서 파일 암호화 또는 복호화 구성 및 수행.
- 이동식 드라이브에서 파일 암호화 구성 및 수행.
- 암호화된 파일에 대한 애플리케이션의 접근 규칙 만들기.
- 파일 암호화가 사용자 기기로 제한된 경우 암호화된 파일에 접근하기 위한 라이센스 키 파일을 만들어 사용자에게 전달.
- 하드 드라이브 암호화 구성 및 수행.

- 암호화된 하드 드라이브와 이동식 드라이브에 대한 사용자 접근 관리(인증 에이전트 계정 관리, 사용자에게 계정 이름과 암호 복구 요청에 대한 정보 및 암호화된 기기에 접근을 위한 접근 허용 키 전달).
- 암호화 상태 및 파일 암호화에 대한 리포트 보기.

이러한 작업은 Kaspersky Endpoint Security for Windows에 포함된 도구를 사용해 수행됩니다. 암호화 작업 수행 방법 및 암호화 기능에 대한 자세한 설명은 Kaspersky Endpoint Security for Windows 온라인 도움말을 참조하십시오.

Kaspersky Security Center는 macOS 운영 체제를 실행하는 기기에 암호화 관리 기능을 지원합니다. 암호화 기능을 지원하는 버전의 애플리케이션을 위한 Kaspersky Endpoint Security for Mac 도구를 사용해서 암호화를 구성할 수 있습니다. 암호화 작업 수행 방법 및 암호화 기능에 대한 자세한 설명은 *Kaspersky Endpoint Security for Mac의 관리자 설명서*를 참조하십시오.

암호화된 기기 목록 보기

암호화된 정보를 저장하는 기기 목록을 보려면 다음과 같이 하십시오:

1. 중앙 관리 서버의 콘솔 트리에서 **데이터 암호화 및 보호** 폴더를 선택합니다.
2. 다음 방법 중 하나를 사용하여 암호화된 기기 목록을 엽니다:
   - **암호화된 드라이브 관리** 섹션의 **암호화된 드라이브 목록으로 이동** 링크를 누릅니다.
   - **암호화된 드라이브** 폴더를 콘솔 트리에서 선택합니다.

암호화된 파일이 저장된 네트워크 기기 및 드라이브 레벨에서 암호화된 기기의 정보가 작업 영역에 표시됩니다. 기기의 정보가 복호화되면 기기가 목록에서 자동 제거됩니다.

필요한 열에서 기기 목록의 정보를 오름차순 또는 내림차순으로 정렬할 수 있습니다.

사용자 인터페이스의 설정에 따라 콘솔 트리에 **데이터 암호화 및 보호** 폴더가 표시되는지 여부가 결정됩니다.

암호화 이벤트 목록 보기

기기에서 데이터 암호화 또는 복호화 작업을 실행할 때 Kaspersky Endpoint Security for Windows는 Kaspersky Security Center에 다음과 같은 유형의 이벤트 정보를 전송합니다.

- 디스크 여유 공간이 부족하여 파일을 암호화 또는 복호화하거나 암호화된 압축 파일을 만들 수 없음.
- 라이센스 문제로 파일을 암호화 또는 복호화하거나 암호화된 압축 파일을 만들 수 없음.
- 접근 권한이 없어 파일을 암호화 또는 복호화하거나 암호화된 압축 파일을 만들 수 없음.
- 애플리케이션이 암호화된 파일에 접근 금지됨.
- 알 수 없는 오류.

기기의 데이터를 암호화할 때 발생한 이벤트 목록을 보려면 다음과 같이 하십시오:

1. 중앙 관리 서버의 콘솔 트리에서 **데이터 암호화 및 보호** 폴더를 선택합니다.
2. 다음 방법 중 하나를 사용하여 암호화 중 발생한 이벤트 목록을 엽니다:
   - **데이터 암호화 오류** 섹션에서 **이벤트 목록으로 이동** 링크를 누릅니다.
   - 콘솔 트리에서 **암호화된 드라이브** 폴더를 선택합니다.

기기에서 데이터를 암호화하는 동안 발생한 문제에 대한 정보가 작업 영역에 표시됩니다.

암호화 이벤트 목록에서 다음 작업을 수행할 수 있습니다:

- 필요한 열에서 데이터 레코드를 오름차순 또는 내림차순으로 정렬.
- 레코드의 빠른 검색 수행(임의 목록 필드의 하위 스트링과 텍스트 일치).
- 이벤트 목록을 텍스트 파일로 내보내기.

사용자 인터페이스의 설정에 따라 콘솔 트리에 **데이터 암호화 및 보호** 폴더가 표시되는지 여부가 결정됩니다.

암호화 이벤트 목록을 텍스트 파일로 내보내기

암호화 이벤트 목록을 텍스트 파일로 내보내려면 다음과 같이 하십시오:

1. 암호화 이벤트 목록을 만듭니다.
2. 이벤트 목록의 마우스 오른쪽 메뉴에서 **목록 내보내기**를 선택합니다.
   목록 내보내기 창이 열립니다.
3. **목록 내보내기** 창에서 이벤트 목록이 담긴 텍스트 파일 이름을 지정하고 이를 저장할 폴더를 선택한 다음 **저장** 버튼을 누릅니다.
   암호화 이벤트 목록이 지정한 파일에 저장됩니다.

암호화 리포트 만들기 및 보기

만들 수 있는 리포트는 다음과 같습니다.

- 관리 중인 기기의 암호화 상태 리포트. 이 리포트는 다양한 관리 중인 기기의 데이터 암호화에 대한 세부 정보를 제공합니다. 예를 들어 리포트에는 구성된 암호화 규칙이 있는 정책을 적용하는 기기 수가 표시됩니다. 또한 예를 들어 재부팅해야 하는 기기 수를 확인할 수 있습니다. 이 보고서에는 모든 기기의 암호화 기술 및 알고리즘에 대한 정보도 포함되어 있습니다.
- 대용량 스토리지 기기의 암호화 상태 리포트. 이 보고서에는 관리 중인 기기의 암호화 상태에 대한 보고서와 유사한 정보가 포함되어 있지만 대용량 저장 기기 및 이동식 드라이브에 대한 데이터만 제공합니다.
- 암호화된 드라이브로의 접근에 대한 권한 리포트. 이 보고서는 암호화된 드라이브에 액세스할 수 있는 사용자 계정을 보여줍니다.

- 파일 암호화 오류 리포트. 이 리포트에는 기기 데이터 암호화 또는 복호화 작업 실행 시 발생한 오류 정보가 담겨 있습니다.

- 암호화된 파일로의 접근 차단 리포트. 이 리포트에는 암호화된 파일로의 애플리케이션 접근 차단 관련 정보가 포함됩니다. 이 리포트는 권한이 없는 사용자나 애플리케이션이 암호화된 파일이나 드라이브에 액세스를 시도할 때 유용합니다.

기기 암호화 관련 리포트를 생성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **데이터 암호화 및 보호** 폴더를 선택합니다.

2. 다음 중 하나를 수행합니다:

   - 관리 중인 기기의 암호화 상태에 대한 리포트를 생성하려면 **대용량 스토리지 기기의 암호화 상태 리포트 보기** 링크를 누릅니다.

     아직 이 리포트를 구성하지 않았다면 새 리포트 템플릿 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

   - 대용량 저장 기기의 암호화 상태에 대한 리포트를 생성하려면 콘솔 트리에서 **암호화된 드라이브** 하위 폴더를 선택한 다음 **대용량 스토리지 기기의 암호화 상태 리포트 보기** 버튼을 누릅니다.

   리포트 생성이 시작됩니다. **중앙 관리 서버** 노드의 **리포트** 탭에 리포트가 나타납니다.

암호화된 기기에 대한 접근 권한 리포트를 생성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **데이터 암호화 및 보호** 폴더를 선택합니다.

2. 다음 중 하나를 수행합니다:

   - **암호화된 드라이브 관리** 섹션에서 **암호화된 드라이브로의 접근에 대한 권한 리포트** 링크를 클릭해 새 리포트 템플릿 마법사를 시작합니다.

   - **암호화된 드라이브** 하위 폴더를 선택한 다음 **암호화된 드라이브로의 접근에 대한 권한 리포트** 버튼을 클릭해 새 리포트 템플릿 마법사를 시작합니다.

3. 새 리포트 템플릿 마법사의 단계를 따릅니다.

   리포트 생성이 시작됩니다. **중앙 관리 서버** 노드의 **리포트** 탭에 리포트가 나타납니다.

파일 암호화 오류에 대한 리포트를 생성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **데이터 암호화 및 보호** 폴더를 선택합니다.

2. 다음 중 하나를 수행합니다:

   - **데이터 암호화 오류** 섹션의 **파일 암호화 오류 리포트 보기** 링크를 눌러 새 리포트 템플릿 마법사를 시작합니다.

   - **암호화 이벤트** 하위 폴더를 선택한 다음 **파일 암호화 오류 리포트** 링크를 눌러 새 리포트 템플릿 마법사를 실행합니다.

3. 새 리포트 템플릿 마법사의 단계를 따릅니다.

   리포트 생성이 시작됩니다. **중앙 관리 서버** 노드의 **리포트** 탭에 리포트가 나타납니다.

관리 중인 기기의 암호화 상태 리포트를 생성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. **새 리포트 템플릿** 버튼을 눌러 새 리포트 템플릿 마법사를 시작합니다.
4. 새 리포트 템플릿 마법사의 지침을 따릅니다. **리포트 템플릿 유형 선택** 창의 **기타** 섹션에서 **관리 중인 기기의 암호화 상태 리포트**를 선택합니다.

   새 리포트 템플릿 마법사가 종료되면 새 리포트 템플릿이 중앙 관리 서버 노드의 **리포트** 탭에 나타납니다.
5. **리포트** 탭의 관련된 중앙 관리 서버 노드에서 지침의 앞 단계에서 생성된 리포트 템플릿을 선택합니다.

리포트 생성이 시작됩니다. **중앙 관리 서버** 노드의 **리포트** 탭에 리포트가 나타납니다.

또한 중앙 관리 서버 노드의 **통계** 탭의 정보 패널을 확인하여 기기와 이동식 드라이브의 암호화 상태가 암호화 정책을 준수하는지 여부를 확인할 수 있습니다.

암호화된 파일에 대한 접근 권한 리포트를 생성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 이름을 가진 노드를 선택합니다.
2. 노드의 작업 공간에서 **리포트** 탭을 엽니다.
3. **새 리포트 템플릿** 버튼을 눌러 새 리포트 템플릿 마법사를 시작합니다.
4. 새 리포트 템플릿 마법사의 지침을 따릅니다. **리포트 템플릿 유형 선택** 창의 **기타** 섹션에서 **암호화된 파일로의 접근 차단 리포트**를 선택합니다.

   새 리포트 템플릿 마법사가 종료되면 새 리포트 템플릿이 **중앙 관리 서버** 노드의 **리포트** 탭에 나타납니다.
5. **중앙 관리 서버** 노드의 **리포트** 탭에서 지침의 앞 단계에서 생성된 리포트 템플릿을 선택합니다.

리포트 생성이 시작됩니다. **중앙 관리 서버** 노드의 **리포트** 탭에 리포트가 나타납니다.

중앙 관리 서버 간 암호화 키 전송

관리 중인 기기에서 데이터 암호화 기능을 활성화한 경우 암호화 키가 중앙 관리 서버에 저장됩니다. 암호화 키는 암호화된 데이터에 액세스하고 암호화 정책을 관리하는 데 사용됩니다.

다음과 같은 경우 암호화 키를 다른 중앙 관리 서버로 전송해야 합니다.

- 관리 중인 기기에서 네트워크 에이전트를 재구성하여 다른 중앙 관리 서버에 기기를 할당합니다. 이 기기에 암호화된 데이터가 포함되어 있으면 암호화 키를 대상 중앙 관리 서버로 전송해야 합니다. 그렇지 않으면 데이터를 해독할 수 없습니다.
- 중앙 관리 서버 S1에서 관리하는 기기 D1에 연결된 이동식 드라이브를 암호화한 다음 이 이동식 드라이브를 중앙 관리 서버 S2에서 관리하는 기기 D2에 연결합니다. 이동식 드라이브의 데이터에 액세스하려면 중앙 관리 서버 S1에서 중앙 관리 서버 S2로 암호화 키를 전송해야 합니다.
- 중앙 관리 서버 S1에서 관리하는 기기 D1의 파일을 암호화한 다음 중앙 관리 서버 S2에서 관리하는 기기 D2의 파일에 액세스하려고 합니다. 해당 파일에 액세스하려면 중앙 관리 서버 S1에서 중앙 관리 서버 S2로 암호화 키를 전송해야 합니다.

다음과 같은 방법으로 암호화 키를 전송할 수 있습니다.

- 암호화 키를 전송해야 하는 두 중앙 관리 서버의 속성에서 자동으로 **중앙 관리 서버의 계층 구조를 사용해 암호화 키 가져오기** 옵션을 활성화합니다. 중앙 관리 서버 중 하나에 대해 이 옵션을 비활성화하면 암호화 키를 자동으로 전송할 수 없습니다.

  중앙 관리 서버 속성의 **중앙 관리 서버의 계층 구조를 사용해 암호화 키 가져오기** 옵션을 활성화하면 중앙 관리 서버가 저장소에 저장된 모든 암호화 키를 계층 구조에서 한 단계 위에 있는 기본 중앙 관리 서버(있는 경우)로 전송합니다.

  암호화된 데이터에 액세스하려고 하면 중앙 관리 서버는 먼저 자체 저장소에서 암호화 키를 검색합니다. **중앙 관리 서버의 계층 구조를 사용해 암호화 키 가져오기** 옵션이 활성화되어 있고, 필요한 암호화 키가 저장소에서 발견되지 않은 경우에는 중앙 관리 서버가 기본 중앙 관리 서버(있는 경우)로 필요한 암호화 키를 제공해 달라는 요청을 추가로 전송합니다. 이 요청은 계층 구조의 최상위 레벨에 있는 서버까지 포함하여 모든 기본 중앙 관리 서버로 전송됩니다.

중앙 관리 서버의 계층 구조를 사용해 암호화 키 가져오기 옵션은 현재 웹 콘솔 인터페이스에서 사용할 수 없습니다. MMC 기반 관리 콘솔에 액세스할 수 없다면 기본 중앙 관리 서버를 사용하여 암호화된 기기를 관리하십시오.

- 하나의 중앙 관리 서버에서 다른 중앙 관리 서버로 암호화 키를 포함하고 있는 파일을 수동으로 내보내고 가져오기.

  암호화 키 내보내기 및 가져오기는 암호화 키 관리 기능에 포함된 작업입니다. 이러한 작업을 수행하려면 다음과 같이 Kaspersky Security Center 사용자의 기능에 대한 접근 권한을 구성합니다:

  - 보조 중앙 관리 서버에서 암호화 키를 내보내는 사용자에게 암호화 키 관리 기능에 대한 **읽기** 액세스 권한을 부여합니다.
  - 암호화 키를 대상 중앙 관리 서버로 가져오는 사용자에게 암호화 키 관리 기능에 대한 **쓰기** 액세스 권한을 부여합니다.

계층 구조 내 중앙 관리 서버 간에 자동으로 암호화 키를 전송하려면 다음 절차를 따르십시오.

1. 콘솔 트리에서 암호화 키의 자동 전송을 실행할 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 속성 창에서 **암호화 알고리즘** 섹션을 선택합니다.
4. **중앙 관리 서버의 계층 구조를 사용해 암호화 키 가져오기** 옵션을 활성화합니다.
5. **확인**을 눌러 변경을 적용합니다.

   암호화 키가 다음 동기화(존재-알림 신호) 시 기본 중앙 관리 서버로 전송됩니다(있는 경우). 또한 이 중앙 관리 서버는 요청에 따라 저장소에서 보조 중앙 관리 서버로 암호화 키를 제공합니다.

중앙 관리 서버 간 암호화 키를 수동으로 전송하려면 다음 절차를 따르십시오.

1. 중앙 관리 서버의 콘솔 트리에서 암호화 키를 전송할 보조 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 속성 창에서 **암호화 알고리즘** 섹션을 선택합니다.

4. **중앙 관리 서버에서 암호화 키 내보내기**을(를) 클릭합니다.

   서버에서 암호화 키를 내보내는 사용자에게 암호화 키 관리 기능에 대한 **읽기** 액세스 권한이 부여되었는지 확인합니다.

5. **암호화 키 내보내기** 창에서는 다음 절차를 따르십시오.

   - **찾기** 버튼을 클릭한 다음 파일을 저장할 위치를 지정합니다.
   - 무단 액세스로부터 파일을 보호하려면 암호를 지정하십시오.

     암호를 기억해 두십시오. 잊어버린 암호는 복원할 수 없습니다. 암호를 잊어버린 경우 내보내기 절차를 반복해야 합니다. 그러므로 암호를 기록해 두고 쉽게 참조할 수 있게 보관합니다.

6. 공유 폴더나 이동식 드라이브 등을 이용해 다른 중앙 관리 서버로 파일을 전송합니다.
7. 대상 중앙 관리 서버에서 Kaspersky Security Center 관리 콘솔이 실행 중인지 확인하십시오.
8. 중앙 관리 서버의 콘솔 트리에서 암호화 키를 전송할 대상 중앙 관리 서버를 선택합니다.
9. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
10. 속성 창에서 **암호화 알고리즘** 섹션을 선택합니다.
11. **중앙 관리 서버에서 암호화 키 가져오기**를 누릅니다.

    암호화 키를 서버로 가져오는 사용자에게 암호화 키 관리 기능에 대한 **쓰기** 액세스 권한이 부여되었는지 확인합니다.

12. **암호화 키 가져오기** 창에서는 다음 절차를 따르십시오.

    - **찾기** 버튼을 클릭한 다음 암호화 키를 포함하고 있는 파일을 선택합니다.
    - 암호를 지정합니다.

13. **확인**을 누릅니다.

    암호화 키가 대상 중앙 관리 서버로 전송됩니다.

데이터 저장소

이 섹션에서는 중앙 관리 서버에 저장되는 데이터 및 클라이언트 기기의 조건을 추적하고 추적 로그를 제공하는 데 사용되는 데이터에 대해 설명합니다.

콘솔 트리의 **저장소** 폴더에는 클라이언트 기기 상태를 추적하는 데 사용되는 데이터가 표시됩니다.

저장소 폴더에는 다음과 같은 개체가 포함됩니다:

- 클라이언트 기기로 배포된 중앙 관리 서버를 통해 다운로드된 업데이트
- 네트워크에서 탐지된 장비의 목록
- 클라이언트 기기에서 탐지된 라이센스 키

- 보안 제품에 의해 기기의 격리 저장소 폴더에 보관된 파일
- 클라이언트 기기의 백업 저장소에 보관된 파일
- 보안 제품이 나중에 검사하도록 연기된 파일

저장소 개체 목록을 텍스트 파일로 내보내기

저장소의 개체 목록을 텍스트 파일로 내보낼 수 있습니다.

저장소의 개체 목록을 텍스트 파일로 내보내려면 다음과 같이 하십시오:

1. 콘솔 트리의 **저장소** 폴더에서 관련 저장소의 하위 폴더를 선택합니다.
2. 저장소 하위 폴더에서 마우스 오른쪽 메뉴를 열고 **목록 내보내기**를 선택합니다.
   그러면 **목록 내보내기** 창이 열리고 해당 창에서 텍스트 파일 이름과 텍스트 파일이 배치되는 폴더의 경로를 지정할 수 있습니다.

설치 패키지

Kaspersky Security Center는 데이터 저장소에 Kaspersky 및 타사 공급업체의 애플리케이션 설치 패키지를 저장합니다.

*설치 패키지*는 애플리케이션 설치에 필요한 파일의 모음입니다. 설치 패키지에는 설치하려는 애플리케이션의 설치 설정과 초기 구성이 포함되어 있습니다.

클라이언트 기기에 애플리케이션을 설치하려면 해당 애플리케이션의 설치 패키지를 만들거나 기존 패키지를 사용해야 합니다. 만들어진 설치 패키지의 목록은 콘솔 트리의 **원격 설치** 폴더에 있는 **설치 패키지** 하위 폴더에 저장됩니다.

저장소에 있는 파일의 주요 상태

보안 제품은 기기에서 위협 요소가 될 수 있는 알려진 바이러스 및 기타 프로그램을 검사하고 파일에 감염 상태를 정의하며 저장소에 감염된 파일을 격리합니다.

예, 보안 제품은 다음과 같은 일을 할 수 있습니다:

- 삭제하기 전에 파일 복사본을 저장소에 백업
- 감염이 의심되는 파일을 저장소에서 격리

파일의 주요 상태는 아래 표에 나와 있습니다. 보안 제품의 각 도움말 시스템에서 파일에 수행할 작업에 대한 자세한 정보를 얻을 수 있습니다.

상태 이름	상태 설명
감염	해당 파일이 Kaspersky 안티 바이러스 데이터베이스에 있는 알려진 바이러스 또는 기타 악성 코드 정보에 해당하는 코드 섹션을 가지고 있습니다.
감염되지 않음	해당 파일에 알려진 바이러스 또는 기타 악성 코드가 탐지되지 않았습니다.
경고	해당 파일이 알려진 위협의 일부 코드와 부분적으로 일치하는 코드 조각을 포함하고 있습니다.
감염 의심	해당 파일이 알려진 악성 코드의 변종 코드이거나 아직 Kaspersky에 보고되지 않은 바이러스와 닮은 코드를 가지고 있습니다.
사용자가 폴더로 격리	해당 파일의 동작으로 인해 어떤 위협 요소가 포함되어 있는 것으로 추정되어 사용자가 파일을 수동으로 저장소로 옮겼습니다. 사용자는 최신 데이터베이스를 사용하여 위협이 있는지 해당 파일을 검사할 수 있습니다.
정상으로 재분석됨	Kaspersky 애플리케이션이 파일의 코드가 바이러스와 유사하기 때문에 감염 안 된 파일에 감염 상태를 정의했습니다. 이후 해당 파일이 최신 데이터베이스로 검사된 후 감염되지 않은 것으로 식별했습니다.
치료됨	해당 파일이 성공적으로 치료되었습니다.
삭제됨	처리 과정 중에 파일이 삭제되었습니다.
암호가 걸려 있음	해당 파일이 암호로 보호되어 있어 처리할 수 없습니다.

스마트 학습 모드인 규칙 트리거링

이 섹션에서는 클라이언트 기기에서 Kaspersky Endpoint Security for Windows의 적응형 이상 행위 제어 규칙을 통해 수행되는 탐지에 대해 설명합니다.

이러한 규칙은 클라이언트 기기의 이상 동작을 탐지하며 차단할 수 있습니다. 스마트 학습 모드에서 작동하는 규칙은 이상 동작을 탐지하며 모든 이상 동작 발생에 대한 리포트를 Kaspersky Security Center 중앙 관리 서버로 전송합니다. 이 정보는 **저장소** 폴더의 **스마트 학습 상태에서 트리거된 규칙** 하위 폴더에 목록으로 저장됩니다. 탐지가 정확함을 확인할 수도 있고, 이 유형의 동작이 앞으로는 이상 동작으로 간주되지 않도록 탐지를 예외로 추가할 수도 있습니다.

탐지에 대한 정보는 다른 이벤트와 함께 중앙 관리 서버의 이벤트 로그에 저장되며, 적응형 이상 행위 제어 리포트에도 저장됩니다.

적응형 이상 행위 제어, 규칙, 해당 모드 및 상태에 대한 자세한 내용은 Kaspersky Endpoint Security for Windows 도움말을 참조하십시오.

적응형 이상 행위 제어 규칙을 사용하여 수행된 탐지 목록 보기

적응형 이상 행위 제어 규칙을 사용하여 수행된 탐지 목록을 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버 노드를 선택합니다.
2. **스마트 학습 상태에서 트리거된 규칙** 하위 폴더를 선택합니다. 이 폴더는 기본적으로 **고급** → **저장소**의 하위 폴더입니다.

   목록에는 적응형 이상 행위 제어 규칙을 사용하여 수행된 탐지와 관련된 다음 정보가 표시됩니다:

   - **관리 그룹**

     기기가 속한 관리 그룹 이름입니다.

- **기기 이름**

  규칙이 적용된 클라이언트 기기의 이름입니다.

- **이름**

  적용된 규칙의 이름입니다.

- **상태**

  예외 중 - 관리자가 이 항목을 처리하여 규칙에 예외로 적용했습니다. 이 상태는 중앙 관리 서버와 클라이언트 기기의 다음 동기화 시까지 유지되며 동기화 후에는 목록에서 항목이 사라집니다.

  확인 중 - 관리자가 이 항목을 처리하여 확인했습니다. 이 상태는 중앙 관리 서버와 클라이언트 기기의 다음 동기화 시까지 유지되며 동기화 후에는 목록에서 항목이 사라집니다.

  비어 있음 - 관리자가 이 항목을 처리하지 않았습니다.

- **규칙이 트리거된 전체 횟수**

  휴리스틱 규칙/프로세스/클라이언트 기기 하나에서 탐지된 항목의 수입니다. 이 수는 Kaspersky Endpoint Security에서 계산됩니다.

- **사용자 이름**

  탐지가 생성된 프로세스를 실행한 클라이언트 기기 사용자의 이름입니다.

- **소스 프로세스 경로**

  소스 프로세스, 즉 작업을 수행하는 프로세스의 경로입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **소스 프로세스 해시**

  소스 프로세스 파일의 SHA256 해시입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **소스 개체 경로**

  프로세스를 시작한 개체의 경로입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **소스 개체 해시**

  소스 파일의 SHA256 해시입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **대상 프로세스 경로**

  대상 프로세스의 경로입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **대상 프로세스 해시**

  대상 파일의 SHA256 해시입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **대상 개체 경로**

  대상 개체의 경로입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **대상 개체 해시**

  대상 파일의 SHA256 해시입니다(자세한 내용은 Kaspersky Endpoint Security 도움말 참조).

- **처리됨**

  이상이 탐지된 날짜.

각 정보 요소의 속성을 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버 노드를 선택합니다.
2. **스마트 학습 상태에서 트리거된 규칙** 하위 폴더를 선택합니다. 이 폴더는 기본적으로 **고급** → **저장소**의 하위 폴더입니다.
3. **스마트 학습 상태에서 트리거된 규칙** 작업 영역에서 원하는 개체를 선택합니다.
4. 다음 중 하나를 수행합니다:
   - 화면 오른쪽에 표시되는 정보 상자에서 **속성** 링크를 누릅니다.
   - 오른쪽 클릭 후 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

   개체의 속성 창이 열리고 선택한 요소 관련 정보가 표시됩니다.

적응형 이상 행위 제어 규칙의 탐지 목록에서 요소를 확인하거나 예외에 추가할 수 있습니다.

요소를 확인하려면,

탐지 목록에서 요소를 하나 또는 여러 개 선택하고 **확인** 버튼을 누릅니다.

요소의 상태가 **확인 중**으로 변경됩니다.

요소를 확인하면 규칙에서 사용되는 통계에 해당 요소가 반영됩니다(자세한 내용은 Kaspersky Endpoint Security 11 for Windows 도움말 참조).

요소를 예외로 추가하려면,

탐지 목록에서 요소 하나 또는 여러 개를 오른쪽 클릭하고 마우스 오른쪽 메뉴에서 **예외에 추가**를 선택합니다.

예외 추가 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

거부하거나 확인하는 요소는 중앙 관리 서버와 클라이언트 기기의 다음 동기화 이후 탐지 목록에서 제외되며 더 이상 목록에 표시되지 않습니다.

적응형 이상 행위 제어 규칙에서 예외 추가

예외 추가 마법사로 Kaspersky Endpoint Security용 적응형 이상 행위 제어 규칙에 예외를 추가할 수 있습니다.

아래의 세 가지 절차 중 하나를 통해 마법사를 시작할 수 있습니다.

적응형 이상 행위 제어 노드를 통해 예외 추가 마법사를 시작하려면:

1. 콘솔 트리에서 필요한 중앙 관리 서버의 노드를 선택합니다.
2. **스마트 학습 상태에서 트리거된 규칙**를 선택합니다. 이 폴더는 기본적으로 **고급** → **저장소**의 하위 폴더입니다.
3. 작업 영역의 탐지 목록에서 요소 하나 또는 여러 개를 마우스 오른쪽 버튼으로 누르고 **예외에 추가**를 선택합니다.

   예외는 한 번에 1,000개까지 추가할 수 있습니다. 요소를 1,000개보다 많이 선택하여 예외에 추가하려고 하면 오류 메시지가 표시됩니다.

예외 추가 마법사가 시작됩니다.

콘솔 트리의 다른 노드에서 예외 추가 마법사를 시작할 수 있습니다:

- 예를 들어 중앙 관리 서버 메인 창의 **이벤트** 탭으로 이동한 다음 **사용자 개선 요청 사항** 옵션이나 **최근 이벤트** 옵션을 선택할 수 있습니다.
- **적응형 이상 행위 제어 규칙 상태 리포트**의 **탐지 수** 열을 선택해도 됩니다.

1단계. 애플리케이션 선택

Kaspersky Endpoint Security for Windows 버전이 하나뿐이며 적응형 이상 행위 제어 규칙을 지원하는 다른 애플리케이션은 없는 경우에는 이 단계를 건너뛰어도 됩니다.

예외 추가 마법사에는 관리 플러그인을 통해 해당 정책에 예외를 추가할 수 있는 Kaspersky 애플리케이션의 목록이 표시됩니다. 이 목록에서 애플리케이션을 선택하고 **다음**을 눌러 예외를 추가할 정책을 선택하는 작업을 계속 진행합니다.

2단계. 하나 이상의 정책 선택

마법사에 Kaspersky Endpoint Security용 정책과 정책 프로필의 목록이 표시됩니다.

예외를 추가할 정책과 프로필을 모두 선택하고 **다음**을 누릅니다.

3단계. 하나 이상의 정책 처리

정책이 처리되는 동안 마법사에 진행률 막대가 표시됩니다. **취소**를 눌러 정책 처리를 중단할 수 있습니다.

상속된 정책은 업데이트할 수 없습니다. 정책 수정 권한이 없어도 정책이 업데이트되지 않습니다.

모든 정책이 처리되거나 처리를 중단하면 리포트가 나타납니다. 이 리포트에는 정상적으로 업데이트된 정책(녹색 아이콘) 및 업데이트되지 않은 정책(빨간색 아이콘)이 표시됩니다.

이 단계가 마법사의 마지막 단계입니다. **마침**을 눌러 마법사를 닫습니다.

격리 및 백업 저장소

클라이언트 기기에 설치된 Kaspersky 안티 바이러스 애플리케이션은 컴퓨터 검사 중에 격리 저장소 또는 백업 저장소에 파일을 보관할 수 있습니다.

*격리*는 바이러스 감염이 의심되거나 탐지 시점에 치료할 수 없는 파일을 저장하는 특별한 저장소입니다.

*백업*는 치료 도중 삭제되거나 수정된 파일의 백업 복사본을 저장하기 위한 공간입니다.

Kaspersky Security Center는 해당 기기에서 Kaspersky 애플리케이션에 의해 격리 또는 백업 저장소에 보관된 파일의 요약 목록을 만듭니다. 클라이언트 기기의 네트워크 에이전트가 격리 및 백업 저장소의 파일에 대한 정보를 중앙 관리 서버로 전송합니다. 관리 콘솔을 사용하여 기기의 저장소에 있는 파일의 속성을 보고, 해당 저장소의 악성 코드 검사를 실행하고, 저장된 파일을 삭제할 수 있습니다. 파일 상태 아이콘에 대한 설명은 부록에 나와 있습니다.

Kaspersky Endpoint Security에서는 격리 저장소 및 백업 작업을 지원합니다.

Kaspersky Security Center는 저장소에서 중앙 관리 서버로 파일을 복사하지 않습니다. 모든 파일은 기기의 저장소에 저장됩니다. 저장소에 파일을 보관한 안티 바이러스 애플리케이션이 있는 기기에서만 파일을 복원할 수 있습니다.

저장소 파일에 대한 원격 관리 작동

기본적으로 클라이언트 기기의 저장소에 있는 파일은 관리할 수 없습니다.

클라이언트 기기의 저장소에 저장된 파일을 원격으로 관리하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 저장소에 있는 파일에 대한 원격 관리를 작동할 관리 그룹을 선택합니다.
2. 그룹 작업 영역에서 **정책** 탭을 엽니다.
3. **정책** 탭에서 기기의 저장소에 파일을 배치하는 보안 제품의 정책을 선택합니다.
4. 정책 설정 창의 **중앙 관리 서버로 데이터 전송** 설정 그룹에서 원격 관리를 작동할 저장소에 해당하는 확인란을 선택합니다.

   정책 속성 창에서 **중앙 관리 서버로 데이터 전송** 설정 그룹의 위치와 확인란의 이름은 현재 사용하고 있는 보안 제품에 따라 달라집니다.

저장소에 보관된 파일의 속성 보기

격리 또는 백업 저장소에 있는 파일의 속성을 보려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **저장소** 폴더, **격리** 또는 **백업** 하위 폴더를 차례로 선택합니다.
2. **격리** (**백업**) 폴더의 작업 영역에서 속성을 보려는 파일을 선택합니다.
3. 파일의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.

저장소에서 파일 삭제

격리 또는 백업 저장소에서 파일을 삭제하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **저장소** 폴더에서 **격리** 또는 **백업** 하위 폴더를 선택합니다.
2. **격리** (또는 **백업**) 폴더의 작업 영역에서 **Shift** 및 **Ctrl** 키를 사용하여 삭제할 파일을 선택합니다.
3. 다음 방법 중 하나로 파일을 삭제합니다:
   - 파일의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
   - 선택한 파일의 정보 박스에서 **삭제**(파일을 하나 삭제하려는 경우 **삭제**) 링크를 누릅니다.

그러면 클라이언트 기기의 저장소에 파일을 보관한 보안 제품이 해당 저장소에서 동일한 파일을 삭제합니다.

저장소에서 파일 복원

격리 또는 백업 저장소에서 파일을 복원하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **저장소** 폴더, **격리** 또는 **백업** 하위 폴더를 차례로 선택합니다.
2. **격리**(**백업**) 폴더의 작업 영역에서 **Shift** 및 **Ctrl** 키를 사용하여 복원할 파일을 선택합니다.
3. 다음 방법 중 하나로 파일 복원을 시작합니다:
   - 파일의 마우스 오른쪽 메뉴에서 **복원**을 선택합니다.
   - 선택한 작업의 정보 박스에서 **복원** 링크를 누릅니다.

그러면 클라이언트 기기의 저장소에 파일을 보관한 보안 제품이 원래 폴더로 동일한 파일을 복원합니다.

저장소에서 디스크로 파일 저장

Kaspersky Security Center에서는 보안 제품이 클라이언트 기기의 격리 저장소 또는 백업 저장소에 보관한 파일의 복사본을 디스크에 저장할 수 있습니다. 해당 파일은 Kaspersky Security Center가 설치된 기기의 지정된 폴더로 복사됩니다.

격리 또는 백업 저장소에서 하드 드라이브로 파일의 복사본을 저장하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **저장소** 폴더, **격리** 또는 **백업** 하위 폴더를 차례로 선택합니다.
2. **격리(백업)** 폴더의 작업 영역에서 하드 드라이브로 복사할 파일을 선택합니다.
3. 다음 방법 중 하나로 복사를 시작합니다:
   - 파일의 마우스 오른쪽 메뉴에서 **디스크로 저장**을 선택합니다.
   - 선택한 파일의 정보 박스에서 **디스크로 저장** 링크를 누릅니다.

그러면 클라이언트 기기의 격리 저장소에 보관된 보안 제품이 지정된 폴더로 파일 복사본을 저장합니다.

격리 저장소의 파일 검사

격리된 파일을 검사하려면:

1. 콘솔 트리에서 **저장소** 폴더와 **격리** 하위 폴더를 차례로 선택합니다.
2. **격리** 폴더의 작업 영역에서 **SHIFT** 및 **CTRL** 키를 사용하여 검사할 파일을 선택합니다.
3. 다음 방법으로 파일 검사를 시작합니다:
   - 파일의 마우스 오른쪽 메뉴에서 **검사**를 선택합니다.
   - 선택한 작업의 정보 박스에서 **검사** 링크를 누릅니다.

선택한 파일이 저장된 기기의 격리 저장소로 파일을 보낸 보안 제품에 대해 수동 검사 작업이 실행됩니다.

처리 안 된 위협

클라이언트 기기에서 탐지된 처리 안 된 파일에 대한 정보는 **저장소** 폴더의 **처리 안 된 위협** 하위 폴더에 저장됩니다.

보안 제품에 의해 연기된 처리 및 치료는 요청 시 또는 지정한 이벤트 발생 후에 수행됩니다. 사용자가 연기된 처리를 구성할 수 있습니다.

처리 안 된 파일 치료

처리 안 된 파일 치료를 시작하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **저장소** 폴더에서 **처리 안 된 위협** 하위 폴더를 선택합니다.
2. **처리 안 된 위협** 폴더의 작업 영역에서 치료할 파일을 선택합니다.

3. 다음 방법 중 하나로 파일 치료를 시작합니다:

   - 정책의 마우스 오른쪽 메뉴에서 **치료**를 선택합니다.
   - 선택한 작업의 정보 박스에서 **치료** 링크를 누릅니다.

   파일을 치료하려는 시도가 수행됩니다.

파일이 치료되면 클라이언트 기기에 설치된 보안 제품이 해당 파일을 원래 폴더로 복원합니다. 파일에 대한 레코드가 **처리 안 된 위협** 폴더의 목록에서 제거됩니다. 파일을 치료할 수 없으면 기기에 설치된 보안 제품이 해당 기기에서 파일을 삭제합니다. 파일에 대한 레코드가 **처리 안 된 위협** 폴더의 목록에서 제거됩니다.

> 파일 치료 및 삭제 기능은 설치된 보안 애플리케이션과 그 버전 및 설정에 따라 달라질 수 있습니다.

처리 안 된 파일을 디스크에 저장

Kaspersky Security Center에서는 클라이언트 기기에서 탐지된 처리 안 된 파일의 복사본을 디스크에 저장할 수 있습니다. 이는 애플리케이션에서 처리하거나 삭제한 파일을 말합니다. 해당 파일은 Kaspersky Security Center가 설치된 기기의 지정된 폴더로 복사됩니다.

관리 중인 기기의 Kaspersky Endpoint Security for Windows 저장소에 복사본을 저장했다면 치료 중에 삭제되거나 수정된 파일의 복사본만 저장할 수 있습니다.

탐지된 처리 안 된 파일의 복사본을 디스크에 저장하려면 다음과 같이 하십시오:

1. 콘솔 트리의 **저장소** 폴더에서 **처리 안 된 위협** 하위 폴더를 선택합니다.
2. **처리 안 된 위협** 폴더의 작업 영역에서 디스크로 복사할 파일을 선택합니다.
3. 다음 방법 중 하나로 복사를 시작합니다:

   - 파일의 마우스 오른쪽 메뉴에서 **디스크로 저장**을 선택합니다.
   - 선택한 파일의 정보 박스에서 **디스크로 저장** 링크를 누릅니다.

그러면 처리 안 된 파일이 탐지된 클라이언트 기기에 설치되어 있는 보안 제품이 지정된 폴더로 파일 복사본을 저장합니다.

"처리 안 된 위협" 폴더에서 파일 삭제

***처리 안 된 위협** 폴더에서 파일을 삭제하려면 다음과 같이 하십시오.*

1. 콘솔 트리의 **저장소** 폴더에서 **처리 안 된 위협** 하위 폴더를 선택합니다.
2. **처리 안 된 위협** 폴더의 작업 영역에서 **SHIFT** 및 **CTRL** 키를 사용하여 삭제할 파일을 선택합니다.

3. 다음 방법 중 하나로 파일을 삭제합니다:

- 파일의 마우스 오른쪽 메뉴에서 **삭제**를 선택합니다.
- 선택한 파일의 정보 박스에서 **삭제**(파일을 하나 삭제하려는 경우 **삭제**) 링크를 누릅니다.

그러면 클라이언트 기기의 저장소에 파일을 보관한 보안 제품이 해당 저장소에서 동일한 파일을 삭제합니다. 파일에 대한 레코드가 **처리 안 된 위협** 폴더의 목록에서 제거됩니다.

Kaspersky Security Network(KSN)

이 섹션에서는 KSN(Kaspersky Security Network)이라는 온라인 서비스 인프라를 사용하는 방법에 대한 설명이 제공됩니다. 해당 섹션에서는 KSN 관련 상세 정보와 KSN 사용 방법, KSN 접근을 구성하는 방법 및 KSN 프록시 서버 사용 통계를 확인하는 방법에 대한 지침이 제공됩니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)과 KSN 기능이 제공되지 않을 수도 있습니다.

KSN 정보

Kaspersky Security Network(KSN)은 파일, 웹 리소스 및 소프트웨어에 대한 정보가 포함된 Kaspersky의 온라인 기술 자료에 접속하도록 하는 온라인 서비스 인프라입니다. Kaspersky Security Network의 데이터를 사용하면 보안 위협이 발생할 때 Kaspersky 애플리케이션의 처리 속도가 더욱 빨라지며 일부 보호 구성 요소의 성능이 향상되고, 정상적인 개체를 바이러스로 탐지하는 위험은 줄어듭니다. KSN에서는 Kaspersky의 평판 데이터베이스를 사용하여 관리 중인 기기에 설치된 애플리케이션에 대한 정보를 검색할 수 있습니다.

Kaspersky Security Center는 다음 인프라 솔루션을 지원합니다:

- *KSN*은 Kaspersky Security Network와 정보를 교환할 수 있는 솔루션입니다. KSN에 참여하면 Kaspersky Security Center가 관리하는 클라이언트 기기에 설치된 Kaspersky 애플리케이션의 작동에 대한 정보를 Kaspersky에 자동 전송하는 데 동의하는 것입니다. 정보는 현재 구성된 KSN 접근 설정에 따라 전송됩니다. Kaspersky 분석가는 추가로 수신된 정보를 분석하여 Kaspersky Security Network의 평판 및 통계 데이터베이스에 포함합니다. Kaspersky Security Center는 기본적으로 이 솔루션을 사용합니다.
- *KPSN(Kaspersky Private Security Network)*은 Kaspersky 애플리케이션이 설치된 기기 사용자가 기기에서 Kaspersky Security Network으로 데이터를 보내지 않고도 글로벌 KSN의 평판 데이터베이스와 기타 통계 데이터에 접근할 수 있도록 하는 솔루션입니다. KPSN은 다음과 같은 이유로 Kaspersky Security Network에 참여할 수 없는 기업 고객용으로 제공됩니다:
  - 사용자 기기가 인터넷에 연결되어 있지 않습니다.
  - 국외 또는 기업 LAN 외부로의 데이터 전송이 법률이나 기업 보안 정책으로 금지되어 있습니다.

  중앙 관리 서버 속성 창의 **KSN 프록시 설정** 섹션에서 Kaspersky Private Security Network 진술문의 액세스 설정을 지정할 수 있습니다.

빠른 시작 마법사를 실행할 때 애플리케이션에서 KSN 참가 여부를 묻습니다. 애플리케이션을 사용할 때 언제든지 KSN 사용을 시작하거나 중지할 수 있습니다.

KSN을 활성화할 때 읽고 수락하는 KSN 성명서에 따라 KSN을 사용합니다. KSN 진술문이 업데이트되면, 중앙 관리 서버를 업데이트하거나 업그레이드할 때 표시됩니다. 업데이트된 KSN 성명서를 수락하거나 거부할 수 있습니다. 거부할 경우 이전에 수락한 이전 버전 KSN 성명서에 따라 KSN을 계속 사용합니다.

KSN이 활성화되면 Kaspersky Security Center가 KSN 서버에 액세스할 수 있는지 확인합니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다. 관리 중인 기기에 대한 보안 수준을 유지하는 데 필요합니다.

중앙 관리 서버를 통해 관리되는 클라이언트 기기는 KSN 프록시 서버를 통해 KSN과 상호 작용합니다. KSN 프록시는 다음 기능을 제공합니다:

- 클라이언트 기기에서 인터넷에 직접 접속할 수 없더라도 KSN으로 요청을 보내고, KSN에서 정보를 받아오고, KSN으로 정보를 전송할 수 있습니다.
- KSN 프록시 서버가 처리된 데이터를 캐시하므로 아웃바운드 채널의 부하 및 클라이언트 기기에서 요청한 정보를 기다리는 시간이 줄어듭니다.

중앙 관리 서버 속성 창의 **KSN 프록시 설정** 섹션에서 KSN 프록시 서버를 구성할 수 있습니다.

Kaspersky Security Network에 대한 접근 설정

중앙 관리 서버와 배포 지점에서 KSN(Kaspersky Security Network) 접근을 설정할 수 있습니다.

중앙 관리 서버의 KSN(Kaspersky Security Network) 접근을 설정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 KSN에 대한 접근을 구성해야 하는 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **섹션** 창에서 **KSN 프록시** → **KSN 프록시 설정**을 선택합니다.
4. 작업 영역에서 KSN 프록시 서비스를 사용하려면 **중앙 관리 서버를 프록시 서버로 사용** 옵션을 활성화합니다.

   데이터는 클라이언트 기기에서 활성 상태인 Kaspersky Endpoint Security 정책에 따라 해당 기기에서 KSN으로 전송됩니다. 이 확인란 선택을 취소하면 Kaspersky Security Center를 통해 중앙 관리 서버와 클라이언트 기기에서 KSN으로 데이터가 전송되지 않습니다. 그러나 클라이언트 기기는 해당 설정에 따라 KSN으로 직접 (Kaspersky Security Center를 바이패스) 데이터를 보낼 수 있습니다. 클라이언트 기기에 적용된 Kaspersky Endpoint Security for Windows 정책은 어떤 데이터가 해당 기기에서 KSN으로 직접(Kaspersky Security Center를 바이패스) 전송되는지를 결정합니다.
5. **Kaspersky Security Network 사용에 동의합니다** 옵션을 활성화합니다.

   이 옵션을 활성화하면 클라이언트 기기에서 패치 설치 결과에 대한 데이터를 Kaspersky에 보냅니다. 이 옵션을 활성화하는 경우, KSN 성명서 약관을 읽고 수락해야 합니다.

   Kaspersky Private Security Network 사용 시, **KPSN 구성** 옵션을 활성화하고 **KSN 프록시 설정 파일 선택** 버튼을 눌러 사설 KSN(확장자가 pkcs7, pem인 파일)의 설정을 다운로드합니다. 설정을 다운로드하면 인터페이스에 공급자의 이름과 연락처 및 KPSN 설정을 사용하여 파일을 생성한 날짜가 표시됩니다.

   KPSN을 사용하도록 설정하면 KSN 요청을 클라우드 KSN으로 직접 보내도록 구성된 배포 지점에 주의를 기울이십시오. 네트워크 에이전트 버전 11 및 이전 버전이 설치된 배포 지점은 계속해서 클라우드 KSN으로 KSN 요청을 보냅니다. KPSN으로 KSN 요청을 보내도록 배포 지점을 다시 구성하려면, 각 배포 지점에 대하여 **중앙 관리 서버에 KSN 요청 전달** 옵션을 활성화합니다. 배포 지점 속성 또는 네트워크 에이전트 정책에서 이 옵션을 활성화할 수 있습니다.

KPSN 구성 확인란을 선택하면 KPSN에 대한 세부 정보가 포함된 메시지가 나타납니다.

Kaspersky Security Center에서 **KPSN 구성** 옵션을 활성화하면 이들 애플리케이션은 KPSN 지원에 대한 정보를 받게 됩니다. 애플리케이션 설정 창에 있는 **지능형 위협 보호** 섹션의 **Kaspersky Security Network** 하위 섹션에 KSN 공급자가 KSN 또는 KPSN으로 표시됩니다.

Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 또는 Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent 이전 애플리케이션 버전을 사용할 시, KPSN을 실행하려면 KPSN을 사용하도록 설정하지 않은 보조 중앙 관리 서버를 사용하는 것이 좋습니다.

Kaspersky Security Center는 중앙 관리 서버 속성 창의 **KSN 프록시 → KSN 프록시 설정** 섹션에서 KPSN 구성 시, 통계 데이터를 Kaspersky Security Network에 전송하지 않습니다.

중앙 관리 서버 속성에 프록시 서버 설정이 구성되어 있는데 네트워크 아키텍처에서는 KPSN을 직접 사용해야 한다면, **사설 KPSN에 연결할 때 프록시 서버 설정 무시** 옵션을 활성화합니다. 이렇게 하지 않으면 관리 중인 애플리케이션의 요청을 KPSN으로 전송할 수 없습니다.

6. KSN 프록시 서비스에 대한 중앙 관리 서버 연결 구성:

   - **연결 설정**에서 **TCP 포트**에 대해 KSN 프록시 서버 연결에 사용할 TCP 포트 번호를 지정합니다. KSN 프록시 서버에 연결하는 기본 포트는 13111입니다.
   - UDP 포트를 통해 중앙 관리 서버를 KSN 프록시 서버에 연결하려면 **UDP 포트 사용** 옵션을 활성화하고 **UDP 포트**에 대한 포트 번호를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있으며 TCP 포트가 사용됩니다. 이 옵션이 활성화되어 있다면 UDP 포트 15111이 KSN 프록시 서버 연결에 기본으로 사용됩니다.
   - HTTPS 포트로 중앙 관리 서버를 KSN 프록시 서버에 연결하려면, **포트를 통해 HTTPS 사용** 옵션을 활성화하고 포트 번호를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있으며 TCP 포트가 사용됩니다. 이 옵션이 활성화되어 있다면 HTTPS 포트 17111이 KSN 프록시 서버 연결에 기본으로 사용됩니다.

7. **기본 중앙 관리 서버를 통해 보조 중앙 관리 서버와 KSN 연결** 옵션을 활성화합니다.

   이 옵션을 활성화하면 모든 계층 구조 레벨의 보조 중앙 관리 서버가 기본 중앙 관리 서버를 KSN 프록시 서버로 사용합니다. 이 옵션을 비활성화하면 보조 중앙 관리 서버에서 직접 KSN으로 연결합니다. 이 경우 관리 중인 기기는 보조 중앙 관리 서버를 KSN 프록시 서버로 사용합니다.

   보조 중앙 관리 서버 속성의 **KSN 프록시 설정** 섹션의 오른쪽 패널에서 **KSN 프록시 서버로 중앙 관리 서버 사용** 확인란이 선택되어 있으면 보조 중앙 관리 서버가 기본 중앙 관리 서버를 프록시 서버로 사용합니다.

8. **확인**를 누릅니다.

KSN 접근 설정이 저장됩니다.

중앙 관리 서버의 부하를 줄이려는 등의 경우, 배포 지점의 KSN 접근을 설정할 수도 있습니다. 그러면 KSN 프록시 서버 역할을 하는 배포 지점이 중앙 관리 서버를 사용하지 않고 관리 중인 기기에서 Kaspersky으로 KSN 요청을 직접 보냅니다.

배포 지점이 KSN(Kaspersky Security Network)에 접근하도록 설정하려면 다음과 같이 하십시오:

1. 배포 지점이 수동으로 할당되어 있는지 확인합니다.
2. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.

3. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
4. 중앙 관리 서버 속성 창에서 **배포 지점** 섹션을 선택합니다.
5. 목록에서 배포 지점을 선택하고 **속성** 버튼을 눌러 속성 창을 엽니다.
6. 배포 지점 속성 창의 **KSN 프록시** 섹션에서 **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근**을 선택합니다.
7. **확인**을 누릅니다.

배포 지점이 KSN 프록시 서버 역할을 합니다.

KSN 사용 및 중지

KSN을 사용하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 KSN을 활성화해야 하는 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **KSN 프록시** 섹션에서 **KSN 프록시 설정** 하위 섹션을 선택합니다.
4. **KSN 프록시 서버로 중앙 관리 서버 사용**를 선택합니다.

   KSN 프록시 서버가 활성됩니다.
5. **Kaspersky Security Network 사용에 동의합니다** 확인란을 선택합니다.

   KSN이 활성됩니다.

   이 확인란을 선택하면 클라이언트 기기에서 패치 설치 결과에 대한 데이터를 Kaspersky에 보냅니다. 이 확인란을 선택하는 경우 KSN 성명서를 확인하고 동의해야 합니다.
6. **확인**를 누릅니다.

KSN을 중지하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 KSN을 활성화해야 하는 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **KSN 프록시** 섹션에서 **KSN 프록시 설정** 하위 섹션을 선택합니다.
4. **프록시 서버로 중앙 관리 서버 사용** 확인란 선택을 취소하여 KSN 프록시 서비스를 비활성화하거나 **Kaspersky Security Network 사용에 동의합니다** 확인란 선택을 취소합니다.

   이 확인란을 선택 해제하면 클라이언트 기기에서 패치 설치 결과에 대한 데이터를 Kaspersky에 보내지 않습니다.

   KPSN을 사용 중인 경우 **KPSN 구성** 확인란 선택을 취소합니다.

   KSN이 비활성됩니다.
5. **확인**를 누릅니다.

수락한 KSN 성명서 보기

Kaspersky Security Network(KSN)를 활성화할 때 KSN 성명서를 읽고 수락해야 합니다. 수락한 KSN 성명서는 언제든지 볼 수 있습니다.

수락한 KSN 성명서를 보려면:

1. 콘솔 트리에서 KSN을 활성화한 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 중앙 관리 서버 속성 창의 **KSN 프록시** 섹션에서 **KSN 프록시 설정** 하위 섹션을 선택합니다.
4. **수락한 KSN 진술문 보기** 링크를 클릭합니다.

   열리는 창에서 수락한 KSN 성명서의 텍스트를 볼 수 있습니다.

KSN 프록시 서버 통계 확인

*KSN 프록시 서버*는 Kaspersky Security Network 인프라와 중앙 관리 서버에서 관리하는 클라이언트 기기 간의 상호 작용을 보장하는 서비스입니다.

KSN Proxy 서버는 다음 기능을 제공합니다:

- 클라이언트 기기에서 인터넷에 직접 접속할 수 없더라도 KSN으로 요청을 보내고 KSN으로 정보를 전송할 수 있습니다.
- KSN 프록시 서버가 처리된 데이터를 캐시하므로 아웃바운드 채널의 부하 및 클라이언트 기기에서 요청한 정보를 기다리는 시간이 줄어듭니다.

중앙 관리 서버 속성 창에서 KSN 프록시 서버를 구성하고 KSN 프록시 서버 사용에 대한 통계를 볼 수 있습니다.

KSN 프록시 서버의 통계를 확인하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 KSN 통계를 봐야 하는 중앙 관리 서버를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 관리 서버 속성 창의 **KSN 프록시** 섹션에서 **KSN 프록시 통계** 하위 섹션을 선택합니다.

   이 섹션에는 KSN 프록시 서버 작업에 대한 실제 통계(캐시 레코드, 캐시에서 처리된 패키지 및 수신된 패키지)가 표시됩니다. 또한 중앙 관리 서버가 KSN에 연결되어 있다면 해당 정보 메시지가 표시됩니다.

   필요한 경우 다음 추가 조치를 수행합니다:

   - KSN 프록시 서버 사용에 대한 통계를 업데이트하려면, **새로 고침**을 누릅니다.
   - **파일로 내보내기** 버튼을 눌러 CSV 파일로 통계를 내보냅니다.
   - **KSN 연결 확인** 버튼을 눌러 중앙 관리 서버가 현재 KSN에 연결되어 있는지를 확인합니다.
4. **확인** 버튼을 눌러 중앙 관리 서버 속성 창을 닫습니다.

업데이트된 KSN 성명서 수락

KSN을 활성화할 때 읽고 수락하는 KSN 성명서에 따라 KSN을 사용합니다. KSN 성명서가 업데이트되면 중앙 관리 서버를 업데이트하거나 업그레이드할 때 표시됩니다. 업데이트된 KSN 성명서를 수락하거나 거부할 수 있습니다. 거부할 경우 이전에 수락한 KSN 성명서 버전에 따라 KSN을 계속 사용합니다.

중앙 관리 서버를 업데이트하거나 업그레이드하면 업데이트된 KSN 성명서가 자동으로 표시됩니다. 업데이트된 KSN 성명서를 거부하더라도 나중에 보고 수락할 수 있습니다.

업데이트된 KSN 성명서를 보고 수락 또는 거부하기:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. **모니터링** 탭의 **모니터링** 섹션에서 **동의한 Kaspersky Security Network 진술문이 오래되었습니다** 링크를 누릅니다.

   KSN 성명서 창이 열립니다.
3. KSN 성명서를 주의깊게 읽고 결정을 내리십시오. 업데이트된 KSN 성명서를 수락하려면 **라이센스 계약서 조건에 동의합니다** 버튼을 누릅니다. 업데이트된 KSN 성명서를 거부하려면 **취소** 버튼을 누릅니다.

선택에 따라 KSN은 현재 또는 업데이트된 KSN 성명서의 약관을 계속 따릅니다. 중앙 관리 서버 속성에서 언제든지 수락한 KSN 성명서의 텍스트를 볼 수 있습니다.

Kaspersky Security Network로 더욱 향상된 보호 제공

Kaspersky은 Kaspersky Security Network를 통해 사용자에게 더욱 향상된 보호 기능을 제공합니다. 이 보호 방법은 지능형 지속 위협과 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.

배포 지점이 KSN 프록시 서버로 작동하는지 확인

배포 지점으로 작동하도록 할당된 관리 중인 기기에서 KSN 프록시 서버를 활성화할 수 있습니다. 관리 중인 기기는 기기에서 ksnproxy 서비스가 실행 중일 때 KSN 프록시로 작동합니다. 기기에서 로컬로 이 서비스를 확인하거나 켜거나 끌 수 있습니다.

Windows 기반 또는 Linux 기반 기기를 배포 지점으로 할당할 수 있습니다. 배포 지점 확인 방법은 이 배포 지점의 운영 체제에 따라 다릅니다.

Windows 기반 배포 지점이 KSN 프록시 서버로 작동하는지 확인하려면:

1. 배포 지점 기기의 Windows에서 **서비스**(**모든 프로그램 → 관리 도구 → 서비스**)를 엽니다.

2. 서비스 목록에서 ksnproxy 서비스가 실행되고 있는지 확인합니다.

   ksnproxy 서비스가 실행 중이면 기기의 네트워크 에이전트가 Kaspersky Security Network에 참여하고 배포 지점 범위에 포함된 관리 중인 기기에 대한 KSN 프록시 서버로 작동합니다.

원하는 경우 ksnproxy 서비스를 해제할 수 있습니다. 이 경우 배포 지점의 네트워크 에이전트는 Kaspersky Security Network에 참여하지 않게 됩니다. 이렇게 하려면 로컬 관리자 권한이 필요합니다.

Linux 기반 배포 지점이 KSN 프록시 서버로 작동하는지 확인하려면:

1. 배포 지점 기기에서, 실행 중인 프로세스 목록을 표시합니다.

2. 실행 중인 프로세스 목록에서 `/opt/kaspersky/ksc64/sbin/ksnproxy` 프로세스가 실행 중인지 확인합니다.

`/opt/kaspersky/ksc64/sbin/ksnproxy` 프로세스가 실행 중이면 기기의 네트워크 에이전트가 Kaspersky Security Network에 참여하고 배포 지점 범위에 포함된 관리 중인 기기에 대한 KSN 프록시 서버로 작동합니다.

온라인 도움말과 오프라인 도움말 간 전환

인터넷에 액세스할 수 없는 경우 오프라인 도움말을 사용할 수 있습니다.

온라인 도움말과 오프라인 도움말 간에 전환하는 방법:

1. Kaspersky Security Center 메인 창의 콘솔 트리에서 **Kaspersky Security Center 15.1**를 선택합니다.

2. **글로벌 인터페이스 설정** 링크를 클릭합니다.

   설정 창이 열립니다.

3. 설정 창에서 **오프라인 도움말 사용**을 클릭합니다.

4. **확인**을 누릅니다.

설정이 적용되고 저장됩니다. 원하는 경우 언제든지 설정을 다시 변경하고 온라인 도움말을 사용할 수 있습니다.

SIEM 시스템으로 이벤트 내보내기

이 섹션에서는 Kaspersky Security Center에서 등록한 이벤트를 외부 SIEM(Security Information and Event Management) 시스템으로 내보내는 방법을 설명합니다.

SIEM 시스템으로 이벤트 내보내기 구성

Kaspersky Security Center에서는 Syslog 형식을 사용하는 모든 SIEM 시스템으로 내보내기, LEEF 및 CEF 형식을 사용하는 QRadar, Splunk, ArcSight SIEM 시스템으로 내보내기 또는 Kaspersky Security Center 데이터베이스에서 직접 SIEM 시스템으로 이벤트 내보내기 중 하나의 방법으로 구성할 수 있습니다. 이 시나리오를 완료하면 중앙 관리 서버가 이벤트를 SIEM 시스템에 자동으로 전송합니다.

필수 구성 요소

Kaspersky Security Center에서 이벤트 구성 내보내기를 시작하기 전:

- 이벤트 내보내기 방법에 대해 자세히 알아보기.
- 시스템 설정 값이 있는지 확인합니다.

> 이 시나리오의 단계는 순서에 관계없이 수행할 수 있습니다.

SIEM 시스템에 대한 이벤트 내보내기 과정은 다음 단계로 구성됩니다:

- **Kaspersky Security Center에서 이벤트를 수신하도록 SIEM 시스템을 구성합니다.**

  방법 지침: SIEM 시스템에서 이벤트 내보내기 구성

- **SIEM 시스템으로 내보낼 이벤트를 선택하기:**

  방법 지침:

  - 관리 콘솔: Syslog 형식으로 내보낼 Kaspersky 애플리케이션의 이벤트 표시, Syslog 형식으로 내보낼 일반 이벤트 표시
  - Kaspersky Security Center 웹 콘솔: Syslog 형식으로 내보낼 Kaspersky 애플리케이션의 이벤트 표시, Syslog 형식으로 내보낼 일반 이벤트 표시

- **다음 중 하나의 방법을 사용하여 SIEM 시스템으로 이벤트 내보내기를 구성하기:**

  - TCP 프로토콜에서 TCP, UDP, TLS 중 하나 사용.

    방법 지침:

    - 관리 콘솔: SIEM 시스템으로 이벤트 내보내기 구성
    - Kaspersky Security Center 웹 콘솔: SIEM 시스템으로 이벤트 내보내기 구성

  - Kaspersky Security Center 데이터베이스에서 직접 이벤트 내보내기 사용(공용 보기 세트는 Kaspersky Security Center 데이터베이스에서 제공됩니다. 이러한 공용 보기에 대한 설명은 klakdb.chm 문서에서 확인할 수 있습니다).

결과

내보내기 원하는 이벤트를 선택한 경우에는 SIEM 시스템으로 이벤트 내보내기를 구성한 후 내보내기 결과를 볼 수 있습니다.

시작하기 전에

Kaspersky Security Center에서 이벤트 자동 내보내기를 설정할 때는 몇 가지 SIEM 시스템 설정을 지정해야 합니다. Kaspersky Security Center 설정을 준비하려면 이러한 설정을 미리 확인하는 것이 좋습니다.

SIEM 시스템으로의 이벤트 자동 전송을 올바르게 구성하려면 다음 설정을 확인해야 합니다:

- **SIEM 시스템 서버 주소**

  현재 사용 중인 SIEM 시스템이 설치된 서버의 IP 주소입니다. SIEM 시스템 설정에서 이 값을 확인하십시오.

- **SIEM 시스템 서버 포트**

  Kaspersky Security Center와 SIEM 시스템 서버 간의 연결을 설정하는 데 사용되는 포트 번호입니다. Kaspersky Security Center 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

- **프로토콜**

  Kaspersky Security Center에서 SIEM 시스템으로 메시지를 전송하는 데 사용되는 프로토콜입니다. Kaspersky Security Center 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

Kaspersky Security Center의 이벤트 정보

Kaspersky Security Center에서는 관리 중인 기기에 설치된 중앙 관리 서버 및 Kaspersky 애플리케이션의 작동 중 발생한 이벤트 정보를 볼 수 있습니다. 이벤트에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다. 이 정보를 외부 SIEM 시스템으로 내보낼 수 있습니다. 외부 SIEM 시스템으로 이벤트 정보를 내보내면 SIEM 시스템 관리자가 관리 중인 기기 또는 관리 그룹에서 발생하는 보안 시스템 이벤트에 신속하게 대응할 수 있습니다.

이벤트 유형

Kaspersky Security Center에는 다음과 같은 유형의 이벤트가 있습니다:

- 일반 이벤트. 이러한 이벤트는 모든 관리 중인 Kaspersky 애플리케이션에서 발생합니다. 일반 이벤트의 예로 바이러스 발생가 있습니다. 일반 이벤트에서는 구문과 의미를 엄격하게 정의합니다. 일반 이벤트는 리포트와 대시보드 등에 사용합니다.

- 관리 중인 Kaspersky 애플리케이션별 이벤트. 각 관리 중인 Kaspersky 애플리케이션에는 자체 이벤트 집합이 있습니다.

이벤트 소스

이벤트는 다음 애플리케이션에서 생성할 수 있습니다.

- Kaspersky Security Center 구성 요소:
  - 중앙 관리 서버
  - 네트워크 에이전트
  - iOS MDM 서버
- 관리 중인 Kaspersky 애플리케이션

  관리 중인 Kaspersky 애플리케이션에서 생성된 이벤트에 대한 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.

애플리케이션 정책의 **이벤트 구성** 탭에서 애플리케이션에서 생성할 수 있는 이벤트의 전체 목록을 볼 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 볼 수 있습니다.

이벤트의 중요성 수준

각 이벤트에는 고유한 심각도가 있습니다. 발생 조건에 따라 이벤트에는 여러 심각도가 할당될 수 있습니다. 네 가지 심각도가 있습니다.

- *심각 이벤트*는 데이터 손실, 운영상의 오작동, 심각한 오류 등을 초래할 수 있는 심각한 문제 발생을 나타내는 이벤트입니다.
- *기능 실패*는 애플리케이션 작동 중이나 절차 수행 중에 심각한 문제, 오류 또는 오작동이 발생했음을 나타내는 이벤트입니다.
- *경고*는 반드시 심각한 것은 아니지만 향후 문제 발생 가능성을 나타내는 이벤트입니다. 이벤트 발생 후 데이터나 기능 손실 없이 애플리케이션을 복원할 수 있는 경우 대부분의 이벤트는 경고로 지정됩니다.
- *정보* 이벤트는 정상적인 작업 완료, 적절한 애플리케이션 작동 또는 절차 완료에 대해 알리기 위해 발생하는 이벤트입니다.

각 이벤트에는 정의된 저장 기간이 있으며, 이 시간 동안 Kaspersky Security Center에서 이벤트를 보거나 수정할 수 있습니다. 정의된 저장 기간이 0이어서 기본적으로 중앙 관리 서버 데이터베이스에 저장되지 않는 이벤트도 있습니다. 1일 이상 중앙 관리 서버 데이터베이스에 저장되는 이벤트만 외부 시스템으로 내보낼 수 있습니다.

이벤트 내보내기 정보

조직 및 기술 레벨에서 보안 문제를 처리하고, 보안 모니터링 서비스를 제공하고, 여러 솔루션의 정보를 통합하는 중앙 집중식 시스템 내에서 이벤트 내보내기를 사용할 수 있습니다. 네트워크 하드웨어 및 애플리케이션이나 SOC(보안 운영 센터)에서 생성하는 보안 경고와 이벤트의 실시간 분석 기능을 제공하는 이러한 시스템을 SIEM 시스템이라고 합니다.

이러한 시스템은 네트워크, 보안, 서버, 데이터베이스, 애플리케이션 등의 여러 경로에서 데이터를 수집할 수 있습니다. 또한 SIEM 시스템은 심각 이벤트 누락을 방지할 수 있도록 모니터링된 데이터를 통합하는 기능도 제공합니다. 그리고 곧 발생할 것으로 예상되는 보안 문제를 관리자에게 알리기 위해 상관 관계가 지정된 이벤트와 경고의 자동 분석도 수행합니다. 경고는 대시보드를 통해 구현할 수도 있고 이메일 등의 타사 채널을 통해 전송할 수도 있습니다.

Kaspersky Security Center에서 외부 SIEM 시스템으로 이벤트를 내보내는 프로세스의 당사자는 이벤트 발신자(Kaspersky Security Center)와 이벤트 수신자(SIEM 시스템)입니다. 이벤트를 성공적으로 내보내려면 SIEM 시스템 및 Kaspersky Security Center 관리 콘솔에서 이를 구성해야 합니다. 구성 순서는 중요하지 않습니다. 즉, Kaspersky Security Center에서 이벤트 전송을 구성한 후에 SIEM 시스템의 이벤트 수신을 구성할 수도 있고 그 반대 순서로 구성할 수도 있습니다.

Kaspersky Security Center에서 이벤트를 보내는 방법

다음의 세 가지 방법으로 Kaspersky Security Center에서 외부 시스템으로 이벤트를 보낼 수 있습니다:

- Syslog 프로토콜을 통해 SIEM 시스템으로 이벤트 보내기

  Syslog 프로토콜을 사용하는 경우 Kaspersky Security Center 중앙 관리 서버 및 관리 중인 기기에 설치된 Kaspersky 애플리케이션에서 발생하는 모든 이벤트를 전달할 수 있습니다. Syslog 프로토콜은 표준 메시지 로깅 프로토콜입니다. SIEM 시스템으로 이벤트를 내보내는 데 사용할 수 있습니다.

  이를 위해 SIEM 시스템에 릴레이할 이벤트를 표시해야 합니다. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 이벤트를 표시할 수 있습니다. 표시된 이벤트만 SIEM 시스템으로 릴레이됩니다. 아무것도 표시하지 않으면 이벤트가 릴레이되지 않습니다.

- CEF 및 LEEF 프로토콜을 통해 QRadar, Splunk 및 ArcSight 시스템으로 이벤트 보내기

  CEF 및 LEEF 프로토콜을 사용하여 일반 이벤트를 내보낼 수 있습니다. CEF 및 LEEF 프로토콜을 통해 이벤트를 내보낼 때는 내보낼 특정 이벤트를 선택할 수 없습니다. 대신 모든 일반 이벤트가 내보내집니다. Kaspersky Security Center 이벤트를 CEF 및 LEEF 형식의 이벤트로 변환하려는 경우 siem_conversion_rules.xml file 파일을 사용해야 합니다. 이 파일에는 Kaspersky Security Center 이벤트 속성 목록과 CEF 및 LEEF 형식의 이벤트에 해당하는 속성이 포함되어 있습니다. 또한 siem_conversion_rules.xml 파일에는 이벤트에 해당하는 메시지를 생성하기 위한 규칙이 포함되어 있습니다. 이 파일은 Kaspersky Security Center 배포 키트에 포함되어 있습니다.

  Syslog 프로토콜과는 달리 CEF 및 LEEF 프로토콜은 범용 프로토콜이 아닙니다. CEF 및 LEEF는 QRadar, Splunk, ArcSight 등의 적합한 SIEM 시스템용 프로토콜입니다. 그러므로 이러한 프로토콜 중 하나를 통해 이벤트를 내보내도록 선택하는 경우에는 SIEM 시스템에서 필요한 파서를 사용합니다.

- Kaspersky Security Center 데이터베이스에서 SIEM 시스템으로 직접 보내기

  SQL 쿼리를 사용하여 데이터베이스 공용 보기에서 이벤트를 직접 받으려는 경우 이러한 이벤트 내보내기 방법을 사용할 수 있습니다. 쿼리 결과는 외부 시스템의 입력 데이터로 사용 가능한 XML 파일에 저장됩니다. 공용 보기에서 제공되는 이벤트만 데이터베이스에서 직접 내보낼 수 있습니다.

SIEM 시스템의 이벤트 수신

SIEM 시스템은 Kaspersky Security Center에서 이벤트를 받아서 올바르게 구문 분석해야 합니다. 따라서 SIEM 시스템을 적절하게 구성해야 합니다. 구성은 사용하는 특정 SIEM 시스템에 따라 달라집니다. 그러나 수신기와 파서 구성 등 모든 SIEM 시스템 구성에서 일반적으로 수행하는 여러 단계가 있습니다.

SIEM 시스템에서 이벤트 내보내기 구성 정보

Kaspersky Security Center에서 외부 SIEM 시스템으로 이벤트를 내보내는 프로세스의 당사자는 이벤트 발신자(Kaspersky Security Center)와 이벤트 수신자(SIEM 시스템)입니다. SIEM 시스템 및 Kaspersky Security Center 관리 콘솔에서 이벤트 내보내기를 구성해야 합니다.

SIEM 시스템에서 지정하는 설정은 사용하는 개별 시스템에 따라 달라집니다. 일반적으로는 모든 SIEM 시스템에서 수신자를 설정해야 하며 필요에 따라 수신된 이벤트를 구문 분석할 메시지 파서를 설정해야 합니다.

수신자 설정

Kaspersky Security Center에서 보낸 이벤트를 받으려면 SIEM 시스템에서 수신자를 설정해야 합니다. 일반적으로는 SIEM 시스템에서 다음 설정을 지정해야 합니다:

- **내보내기 프로토콜 또는 입력 유형**

  이는 메시지 전송 프로토콜입니다(예: UDP). 해당 프로토콜은 Kaspersky Security Center에서 지정한 프로토콜과 같아야 합니다.

- **Port**

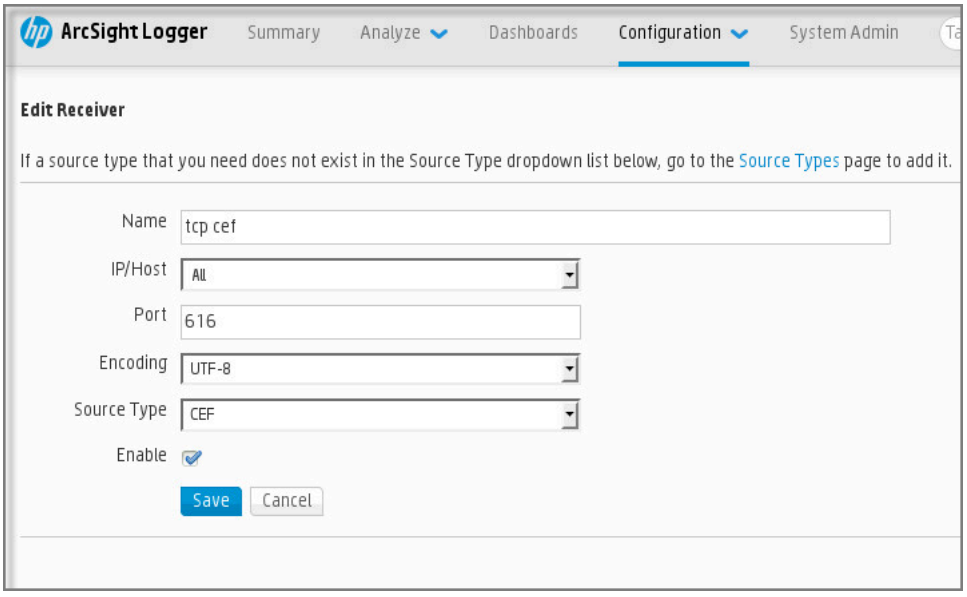
  Kaspersky Security Center 연결을 위한 포트 번호입니다. 이 포트는 Kaspersky Security Center에서 지정한 포트와 같아야 합니다.

- **메시지 프로토콜 또는 경로 유형**

  SIEM 시스템으로 이벤트를 내보내는 데 사용되는 프로토콜입니다. 다음의 표준 프로토콜 중 하나일 수 있습니다: Syslog, CEF 또는 LEEF. SIEM 시스템은 지정한 프로토콜에 따라 메시지 파서를 선택합니다.

사용하는 SIEM 시스템에 따라 몇 가지 추가 수신자 설정을 지정해야 할 수 있습니다.

아래 그림에는 ArcSight의 수신자 설정 화면이 나와 있습니다.



ArcSight의 수신자 설정

메시지 파서

내보낸 이벤트는 SIEM 시스템에 메시지로 전달됩니다. 이러한 메시지를 적절하게 구문 분석해야 SIEM 시스템에서 이벤트에 대한 정보를 사용할 수 있습니다. 메시지 파서는 SIEM 시스템의 일부로, 메시지 내용을 이벤트 ID, 심각도, 설명, 파라미터 등의 관련 필드로 분할하는 데 사용됩니다. 그러면 SIEM 시스템은 Kaspersky Security Center에서 받은 이벤트를 처리하여 SIEM 시스템 데이터베이스에 저장할 수 있습니다.

Syslog 형식으로 SIEM 시스템으로 내보내기 위한 이벤트 표시

이벤트 자동 내보내기를 사용하도록 설정한 후에는 외부 SIEM 시스템으로 내보낼 이벤트를 선택해야 합니다.

다음 조건 중 하나를 기준으로 하여 외부 시스템으로의 Syslog 형식 이벤트 내보내기를 구성할 수 있습니다.

- 일반 이벤트 표시. 이벤트 설정 또는 중앙 관리 서버 설정을 통해 정책에서 내보낼 이벤트를 표시하면 SIEM 시스템은 특정 정책을 통해 관리되는 모든 애플리케이션에서 발생한 표시된 이벤트를 수신하게 됩니다. 내보낸 이벤트를 정책에서 선택한 경우에는 이 정책을 통해 관리되는 개별 애플리케이션에 대해 이벤트를 재정의할 수 없습니다.

- 관리 애플리케이션에 대한 이벤트 표시. 관리 중인 기기에 설치된 개별 관리 애플리케이션에 대해 내보낼 이벤트를 선택하는 경우 SIEM 시스템은 해당 애플리케이션에서 발생한 이벤트만 수신하게 됩니다.

Syslog 형식으로 내보내기 위한 Kaspersky 애플리케이션의 이벤트 표시

관리 중인 기기에 설치된 개별 관리 애플리케이션에서 발생한 이벤트를 내보내려는 경우 해당 애플리케이션에 대해 내보낼 이벤트를 선택합니다. 정책에서 이전에 내보낸 이벤트를 선택한 경우에는 이 정책을 통해 관리되는 개별 애플리케이션에 대해 선택한 이벤트를 재정의할 수 없습니다.

개별 애플리케이션에 대해 내보낼 이벤트를 선택하려면 다음과 같이 하십시오.

1. Kaspersky Security Center 콘솔 트리에서 **관리 중인 기기** 노드를 선택한 다음 **기기** 탭으로 이동합니다.

2. 마우스 오른쪽 버튼을 눌러 관련 기기의 마우스 오른쪽 메뉴를 열고 **속성**를 선택합니다.

3. 기기 속성 창이 열리면 **애플리케이션** 섹션을 선택합니다.

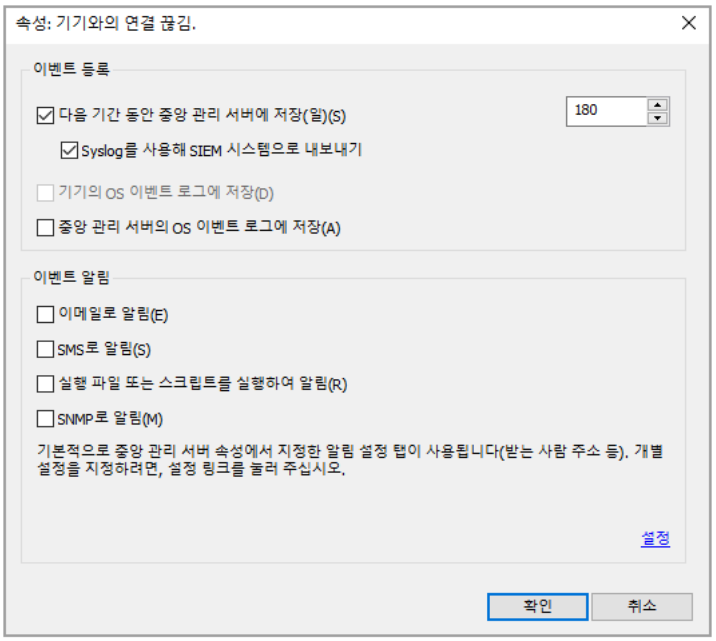
4. 애플리케이션 목록이 표시되면 이벤트를 내보내야 하는 애플리케이션을 선택하고 **속성** 버튼을 누릅니다.

5. 애플리케이션 속성 창에서 **이벤트 구성** 섹션을 선택합니다.

6. 이벤트 목록이 표시되면 SIEM 시스템으로 내보내야 하는 이벤트를 하나 이상 선택하고 **속성** 버튼을 누릅니다.

7. 이벤트 속성 창이 표시되면 **Syslog를 사용해 SIEM 시스템으로 내보내기** 확인란을 선택하여 선택한 이벤트 내보내기를 사용하도록 설정합니다. **Syslog를 사용해 SIEM 시스템으로 내보내기** 확인란의 선택을 해제하여 Syslog 형식으로 내보내기 위해 선택한 이벤트의 표시를 해제합니다.

정책에 이벤트 속성이 정의되어 있는 경우에는 이 창의 필드를 편집할 수 없습니다.



이벤트 속성 창

8. **확인**을 눌러 변경을 저장합니다.

9. 애플리케이션 속성 창과 기기 속성 창에서 **확인**를 누릅니다.

선택한 이벤트가 Syslog 형식을 통해 SIEM 시스템으로 전송됩니다. **Syslog를 사용해 SIEM 시스템으로 내보내기** 확인란의 선택을 취소한 이벤트는 SIEM 시스템으로 내보내지지 않습니다. 자동 내보내기를 사용하도록 설정하고 내보낼 이벤트를 선택한 직후에 내보내기가 시작됩니다. Kaspersky Security Center에서 이벤트를 받을 수 있도록 SIEM 시스템을 구성하십시오.

Syslog 형식으로 내보낼 일반 이벤트 표시

특정 정책을 통해 관리되는 모든 애플리케이션에서 발생한 이벤트를 내보내려는 경우 정책에서 내보낼 이벤트를 표시합니다. 이 경우 개별 관리 중인 기기에 대해 이벤트를 선택할 수는 없습니다.

SIEM 시스템으로 내보내기 위한 일반 이벤트 표시 방법:

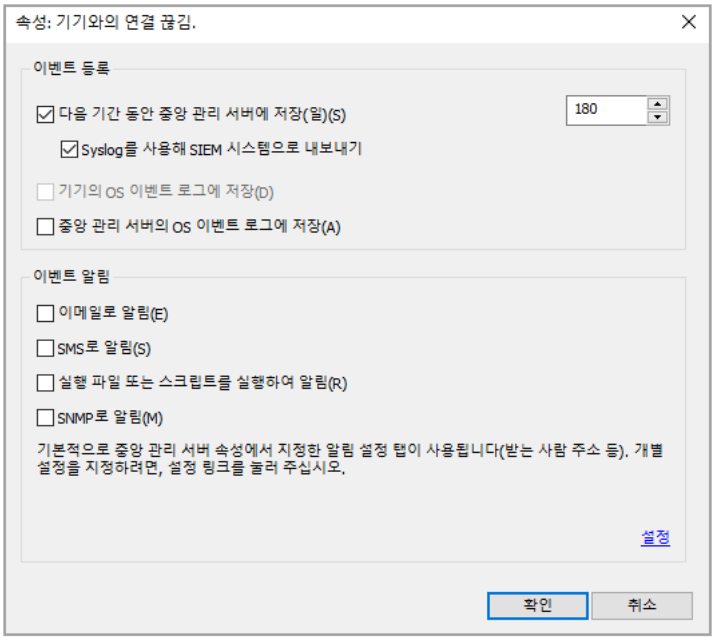
1. Kaspersky Security Center 콘솔 트리에서 **정책** 노드를 선택합니다.

2. 마우스 오른쪽 버튼을 눌러 관련 정책의 마우스 오른쪽 메뉴를 열고 **속성**를 선택합니다.

3. 정책 속성 창이 열리면 **이벤트 구성** 섹션을 선택합니다.

4. 이벤트 목록이 표시되면 SIEM 시스템으로 내보내야 하는 이벤트를 하나 이상 선택하고 **속성** 버튼을 누릅니다. 모든 이벤트를 선택해야 하는 경우 **모두 선택** 버튼을 누릅니다.

5. 이벤트 속성 창이 표시되면 **Syslog를 사용해 SIEM 시스템으로 내보내기** 확인란을 선택하여 선택한 이벤트 내보내기를 사용하도록 설정합니다. **Syslog를 사용해 SIEM 시스템으로 내보내기** 확인란의 선택을 해제하여 Syslog 형식으로 내보내기 위해 선택한 이벤트의 표시를 해제합니다.



중앙 관리 서버 이벤트 속성 창

6. **확인**을 눌러 변경을 저장합니다.

7. 정책 속성 창에서 **확인**를 누릅니다.

선택한 이벤트가 Syslog 형식을 통해 SIEM 시스템으로 전송됩니다. **Syslog를 사용해 SIEM 시스템으로 내보내기** 확인란의 선택을 취소한 이벤트는 SIEM 시스템으로 내보내지지 않습니다. 자동 내보내기를 사용하도록 설정하고 내보낼 이벤트를 선택한 직후에 내보내기가 시작됩니다. Kaspersky Security Center에서 이벤트를 받을 수 있도록 SIEM 시스템을 구성하십시오.

Syslog 형식을 사용한 이벤트 내보내기 정보

Syslog 형식을 사용하여 중앙 관리 서버 및 관리 중인 기기에 설치된 기타 Kaspersky 애플리케이션에서 발생하는 이벤트를 SIEM 시스템으로 내보낼 수 있습니다.

Syslog 프로토콜은 메시지 로깅용 표준 프로토콜입니다. 이 프로토콜을 사용하는 경우 메시지, 메시지를 저장하는 시스템, 그리고 메시지를 보고/분석하는 소프트웨어를 구분할 수 있습니다. 각 메시지에는 메시지를 생성하는 소프트웨어 유형을 나타내는 기능 코드 레이블이 지정되며 심각도가 할당됩니다.

Syslog 형식은 Internet Engineering Task Force(인터넷 표준)에서 게시한 RFC(Request for Comments) 문서를 통해 정의됩니다. Kaspersky Security Center에서 외부 시스템으로 이벤트를 내보낼 때는 RFC 5424 표준이 사용됩니다.

Kaspersky Security Center에서는 Syslog 형식을 사용한 외부 시스템으로의 이벤트 내보내기를 구성할 수 있습니다.

내보내기 프로세스에서는 다음의 두 단계를 수행합니다:

1. 자동 이벤트 내보내기를 사용하도록 설정. 이 단계에서는 SIEM 시스템으로 이벤트를 보내도록 Kaspersky Security Center를 구성합니다. 자동 내보내기를 사용하도록 설정한 직후에 Kaspersky Security Center가 이벤트 보내기를 시작합니다.

2. 외부 시스템으로 내보낼 이벤트 선택. 이 단계에서는 SIEM 시스템으로 내보낼 이벤트를 선택합니다.

CEF 및 LEEF 형식을 사용하여 이벤트 내보내기 정보

CEF 및 LEEF 프로토콜을 사용하여 SIEM 시스템 일반 이벤트와 함께 Kaspersky 애플리케이션에서 중앙 관리 서버로 전송한 이벤트로 내보낼 수 있습니다. 내보내기 이벤트 집합은 미리 정의되어 있으므로 내보낼 이벤트를 선택할 수는 없습니다. SIEM 시스템(QRadar, ArcSight 또는 Splunk)으로 이벤트를 보내기 전에, siem_conversion_rules.xml 파일에 지정된 규칙을 사용하여 Kaspersky Security Center 이벤트를 CEF 및 LEEF 형식의 이벤트로 해석해야 합니다.

사용하는 SIEM 시스템에 따라 내보내기 형식을 선택합니다. 아래 표에는 SIEM 시스템 및 해당 내보내기 형식이 나와 있습니다.

SIEM 시스템으로 이벤트 내보내기 형식

SIEM 시스템	내보내기 형식
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF(Log Event Extended Format)는 IBM Security QRadar SIEM용으로 사용자 지정된 이벤트 형식입니다. QRadar는 LEEF 이벤트를 통합, 식별 및 처리할 수 있습니다. LEEF 이벤트는 UTF-8 문자 인코딩을 사용해야 합니다. LEEF 프로토콜에 대한 세부 정보는 IBM Knowledge Center에서 확인할 수 있습니다.

- CEF(Common Event Format) - 서로 다른 여러 보안 및 네트워크 기기와 애플리케이션의 보안 관련 정보 상호 운용성을 개선하는 개방형 로그 관리 표준입니다. CEF에서는 공통 이벤트 로그 형식을 사용할 수 있으므로, 기업 관리 시스템에서 분석을 위해 데이터를 쉽게 통합하고 집계할 수 있습니다. CEF 이벤트는 UTF-8 문자 인코딩을 사용해야 합니다.

자동 내보내기 시에는 Kaspersky Security Center가 SIEM 시스템으로 일반 이벤트를 보냅니다. 이벤트 자동 내보내기를 사용하도록 설정한 직후에 내보내기가 시작됩니다. 이 섹션에서는 자동 이벤트 내보내기를 사용하도록 설정하는 방법을 자세히 설명합니다.

SIEM 시스템으로 이벤트를 내보내기 위한 Kaspersky Security Center 구성

Kaspersky Security Center에서 자동 이벤트 내보내기를 활성화시킬 수 있습니다.

일반 이벤트만 관리되는 애플리케이션에서 CEF 및 LEEF 형식을 통해 내보낼 수 없습니다. 이벤트를 CEF 및 LEEF 형식으로 변환하는 데 사용되는 해석 규칙은 Kaspersky Security Center 배포 키트에 포함된 siem_conversion_rules.xml 파일에 지정되어 있습니다. 애플리케이션 특정 이벤트는 관리되는 애플리케이션에서 CEF 및 LEEF 형식을 통해 내보낼 수 없습니다. 관리되는 애플리케이션의 정책을 사용하여 구성된 사용자 지정 이벤트 세트나 관리되는 애플리케이션의 이벤트를 내보내기해야 한다면 Syslog 형식을 통해 이벤트 내보냅니다.

자동 이벤트 내보내기 활성화:

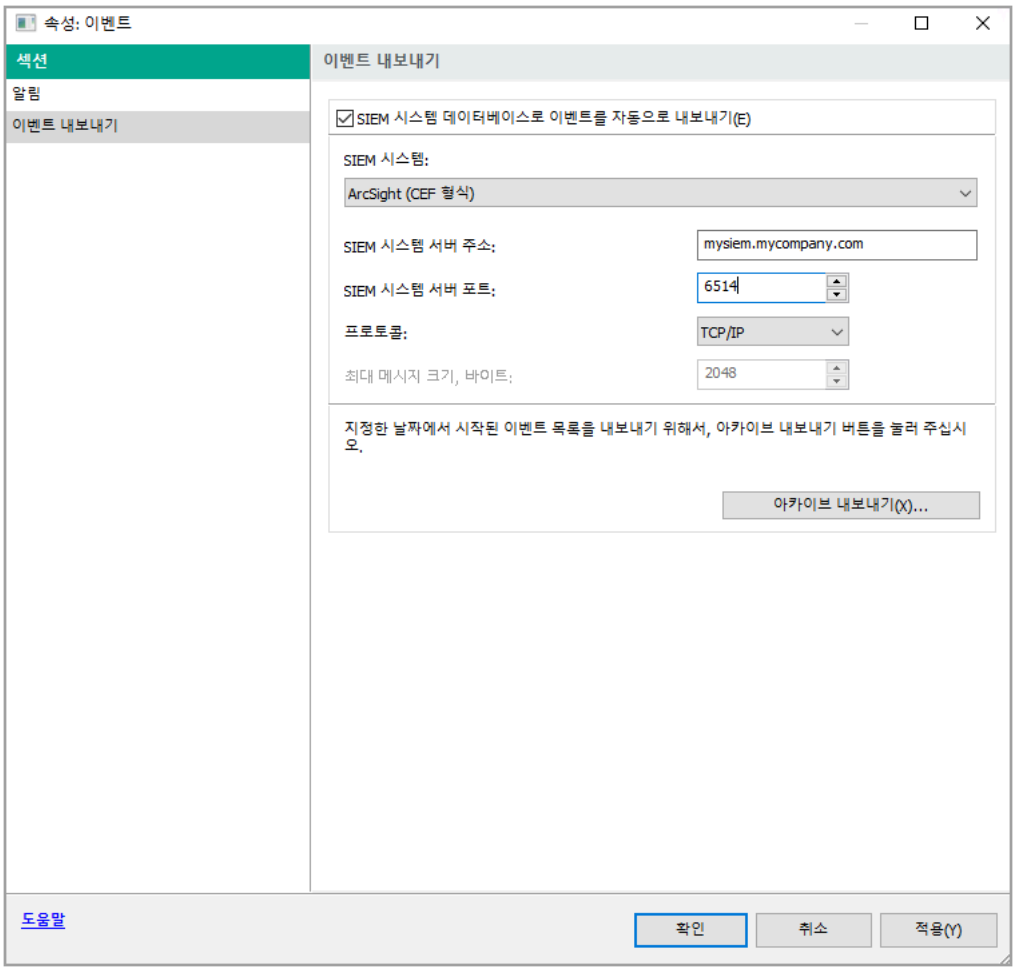
1. Kaspersky Security Center 콘솔 트리에서 이벤트를 내보낼 중앙 관리 서버를 선택합니다.

2. 선택한 중앙 관리 서버의 작업 영역에서 **이벤트** 탭을 누릅니다.

3. **알림 구성 및 이벤트 내보내기** 링크 옆의 드롭다운 화살표를 클릭하고, 드롭다운 목록에서 **SIEM 시스템으로 내보내기 구성**을 선택합니다.

   이벤트 속성 창이 열리고 **이벤트 내보내기** 섹션이 표시됩니다.

4. **이벤트 내보내기** 섹션에서 다음 내보내기 설정을 지정합니다.



이벤트 속성 창의 이벤트 내보내기 섹션

- **SIEM 시스템 데이터베이스로 이벤트를 자동으로 내보내기**

  SIEM 시스템으로의 이벤트 자동 내보내기를 사용하도록 설정하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 **이벤트 내보내기** 섹션의 모든 필드가 사용할 수 있도록 설정됩니다.

- **SIEM 시스템**

  SIEM 시스템을 선택하여 QRadar®(LEEF 형식), ArcSight(CEF 형식), Splunk®(CEF 형식), Syslog 형식(RFC 5424)와 같은 이벤트를 내보냅니다.

  Syslog 형식을 선택한다면 다음을 지정해야 합니다:

  최대 메시지 크기, 바이트

  SIEM 시스템으로 전달되는 메시지 하나의 최대 크기(바이트)를 지정합니다. 각 이벤트는 메시지 하나로 전달됩니다. 실제 메시지 길이가 지정된 값을 초과하면 메시지가 잘리며 데이터가 손실될 수 있습니다. 기본 크기는 2048바이트입니다. 이 필드는 **SIEM 시스템** 필드에서 Syslog 형식을 선택한 경우에만 사용할 수 있습니다.

- **SIEM 시스템 서버 주소**

  SIEM 시스템 서버 주소를 지정합니다. 주소는 DNS 또는 NetBIOS 이름이나 IP 주소로 지정할 수 있습니다.

- **SIEM 시스템 서버 포트**

  SIEM 시스템 서버 연결에 사용되는 포트 번호를 지정합니다. 이 포트 번호는 SIEM 시스템이 이벤트를 받는 데 사용하는 번호와 같아야 합니다. 자세한 내용은 SIEM 시스템 구성 섹션을 참조하십시오.

- **프로토콜**

  SIEM 시스템으로 메시지를 전송하는 데 사용할 프로토콜을 선택합니다. TCP, UDP 또는 TLS over TCP 프로토콜을 선택할 수 있습니다.

  TCP 프로토콜을 통해 TLS를 선택하면 다음과 같은 TLS 설정을 지정할 수 있습니다.

  - **SIEM 서버 인증**

    다음 방법 중 하나를 선택하여 SIEM 시스템 서버를 인증합니다:

    - **CA 인증서 사용**. 신뢰하는 인증 기관(CA)에서 인증서 목록이 포함된 파일을 수신하여 Kaspersky Security Center에 업로드할 수 있습니다. Kaspersky Security Center는 SIEM 시스템 서버의 인증서가 신뢰하는 인증 기관에서 서명한 것인지 확인합니다.

      신뢰하는 인증서를 추가하려면 **찾기** 버튼을 클릭한 다음 인증서를 업로드합니다.

      CA 인증서 사용 옵션을 선택하면 **서버 인증서의 대상 (선택 사항)** 필드에 대상 이름을 지정할 수 있습니다. *대상 이름*은 인증서가 수신되는 도메인 이름입니다. Kaspersky Security Center는 SIEM 시스템 서버의 도메인 이름이 SIEM 시스템 서버 인증서의 대상 이름과 일치하지 않는 경우 SIEM 시스템 서버에 연결할 수 없습니다. 그러나 SIEM 시스템 서버는 인증서에서 대상 이름이 변경되면 도메인 이름을 변경할 수 있습니다. 이렇게 하려면 **서버 인증서의 대상 (선택 사항)** 필드에 대상 이름을 지정합니다. 지정된 대상 이름이 SIEM 시스템 인증서의 대상 이름과 일치하면 Kaspersky Security Center가 SIEM 시스템 서버 인증서의 유효성을 검증합니다.

    - **서버 인증서의 SHA1 엄지손가락 지문을 사용**. Kaspersky Security Center에 대한 SIEM 시스템 인증서의 SHA-1 지문을 지정할 수 있습니다. SHA-1 지문을 추가하려면 옵션 아래의 필드에 입력합니다.

  - **클라이언트 인증**

클라이언트 인증의 경우 인증서를 삽입하거나 Kaspersky Security Center에서 생성할 수 있습니다.

- **인증서 삽입**. 신뢰할 수 있는 인증 기관(CA)과 같은 다양한 경로에서 수신된 인증서를 사용할 수 있습니다. 기존 인증서를 삽입하려면 **인증서 찾기** 버튼을 클릭합니다. **인증서** 창이 열리면 다음 인증서 유형 중 하나를 선택한 다음, 인증서와 해당 개인 키를 지정합니다:

  - **X.509 인증서**. **개인 키(*.prk, *.pem)** 필드에 개인 키가 있는 파일과 **인증서(*.cer)** 필드에 인증서가 있는 파일을 업로드합니다. 이렇게 하려면 해당 필드 오른쪽에 있는 **찾기** 버튼을 클릭한 다음 필요한 파일을 추가합니다. 두 파일은 서로 의존하지 않으며 파일의 로딩 순서는 중요하지 않습니다. 파일을 모두 업로드한 후 **암호** 필드에 개인 키 디코딩 암호를 지정합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

  - **PKCS #12 컨테이너**. **인증서 파일** 필드에 인증서와 개인 키가 포함된 단일 파일을 업로드합니다. 이렇게 하려면 필드 오른쪽에 있는 **찾기** 버튼을 클릭한 다음 필요한 파일을 추가합니다. 파일 업로드 후 **암호** 필드에 개인 키 디코딩 암호를 지정합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

- **키 생성**. Kaspersky Security Center에서 자체 서명 인증서를 생성할 수 있습니다. **인증서 생성** 버튼을 클릭한 다음 **제목** 필드에 대상 이름을 입력합니다. 이 대상 이름에 대해 클라이언트 인증서가 생성되고 이 인증서의 **클라이언트 인증서의 SHA1 엄지손가락 지문**의 SHA-1 지문 필드에 표시됩니다. 이에 따라 Kaspersky Security Center가 생성된 자체 서명 인증서를 저장하며, 인증서의 공개 부분 또는 SHA1 지문을 SIEM 시스템에 전달할 수 있습니다.

5. 이전의 특정 날짜 이후에 발생한 이벤트를 SIEM 시스템 데이터베이스로 내보내려면 **아카이브 내보내기** 버튼을 클릭하고 이벤트 내보내기 시작 날짜를 지정합니다. 기본적으로는 이벤트 내보내기를 사용하도록 설정한 직후에 내보내기가 시작됩니다.

6. SIEM 시스템 연결이 구성되었는지 확인하려면 **테스트 설정** 버튼을 클릭합니다.

   애플리케이션이 SIEM 시스템 서버와의 연결 설정 및 테스트 이벤트 전송을 시도합니다. 연결이 완료되지 않을 경우 오류 메시지가 표시됩니다. 연결이 완료될 경우 메시지가 표시되지 않습니다. 필요할 경우 **이벤트** 탭의 테스트 이벤트를 볼 수 있습니다.

7. **확인**를 누릅니다.

이벤트 자동 내보내기가 사용하도록 설정됩니다.

이벤트 자동 내보내기를 사용하도록 설정한 후에는 SIEM 시스템으로 내보낼 이벤트를 선택해야 합니다.

데이터베이스에서 직접 이벤트 내보내기

Kaspersky Security Center 인터페이스를 사용할 필요 없이 Kaspersky Security Center 데이터베이스에서 직접 이벤트를 가져올 수 있습니다. 공용 보기를 직접 쿼리하여 이벤트 데이터를 가져올 수도 있고, `기존 공용 보기를 기준으로 보기를 직접 만든 다음 주소를 지정해 필요한 데이터를 얻을 수도 있습니다.

공용 보기

Kaspersky Security Center 데이터베이스에서는 편의상 공용 보기 집합이 제공됩니다. 이러한 공용 보기의 설명은 klakdb.chm 문서에서 확인할 수 있습니다.

v_akpub_ev_event 공용 보기에는 데이터베이스의 이벤트 파라미터를 나타내는 필드 집합이 포함되어 있습니다. 기기, 애플리케이션, 사용자 등의 기타 Kaspersky Security Center 항목에 해당하는 공용 보기에 대한 정보도 klakdb.chm 문서에서 확인할 수 있습니다. 쿼리에서 이 정보를 사용할 수 있습니다.

이 섹션에는 klsql2 유틸리티를 통해 SQL 쿼리를 실행하는 지침과 쿼리 예제가 포함되어 있습니다.

SQL 쿼리 또는 데이터베이스 보기를 만들려는 경우 데이터베이스 작업을 위한 기타 프로그램도 사용할 수 있습니다. 인스턴스 이름, 데이터베이스 이름 등 Kaspersky Security Center 데이터베이스에 연결하는 데 필요한 파라미터를 확인하는 방법에 대한 정보는 해당 섹션에 나와 있습니다.

klsql2 유틸리티를 사용하여 SQL 쿼리 생성

이 문서에서는 klsql2 유틸리티를 다운로드하고 사용하는 방법과 이 유틸리티로 SQL 쿼리를 실행하는 방법을 설명합니다.

klsql2 유틸리티를 사용하려면:

1. Kaspersky Security Center의 설치 폴더에서 klsql2 유틸리티를 넣습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다. 이전 Kaspersky Security Center 버전용 klsql2 유틸리티 버전을 사용하지 마십시오.

2. 텍스트 편집기에서 .sql 확장자를 가진 파일을 생성하고 유틸리티와 같은 폴더에 파일을 넣습니다.

3. 생성된 .sql 파일에 원하는 SQL 쿼리를 입력한 다음 파일을 저장합니다.

4. Kaspersky Security Center 중앙 관리 서버를 설치한 기기의 명령줄에서 다음 명령을 입력하여 .sql 파일에서 SQL 쿼리를 실행한 다음 result.xml 파일에 결과를 저장합니다.
   ```
   klsql2 -i src.sql -u <사용자 이름> -p <암호> -o result.xml
   ```
   여기서 <사용자 이름> 및 <암호>는 데이터베이스에 대한 액세스 권한이 있는 사용자 계정의 자격 증명입니다.

5. 필요하다면 데이터베이스에 액세스할 수 있는 사용자 계정의 로그인 및 암호를 입력합니다.

6. 새로 작성된 result.xml 파일을 열어 SQL 쿼리 결과를 확인합니다.

.sql 파일을 편집하여 공용 보기에 대해 원하는 SQL 쿼리를 만들 수 있습니다. 그런 후에 명령줄에서 SQL 쿼리를 실행하고 결과를 파일에 저장하면 됩니다.

klsql2 유틸리티의 SQL 쿼리 예제

이 섹션에서는 klsql2 유틸리티를 통해 실행하는 SQL 쿼리의 예제를 제공합니다.

아래 그림에는 지난 7일 동안 기기에서 발생한 이벤트를 가져와서 발생 시간 순서대로 표시하는 과정이 나와 있습니다. 최신 데이터가 먼저 표시됩니다.

Microsoft SQL Server의 예:

```
SELECT
  /* 이벤트 식별자 */
  e.nId,

  /* 이벤트 발생 시간 */
  e.tmRiseTime,

  /* 이벤트 유형의 내부 이름 */
  e.strEventType,

  /* 이벤트의 표시 이름 */
  e.wstrEventTypeDisplayName,

  /* 이벤트의 표시 설명 */
  e.wstrDescription,

  /* 기기가 있는 그룹의 이름 */
  e.wstrGroupName,

  /* 이벤트가 발생한 기기의 표시되는 이름 */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* 이벤트가 발생한 기기의 IP 주소 */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

PostgreSQL의 예:

```
SELECT
  /* 이벤트 식별자 */
  "e"."nId",

  /* 이벤트 발생 시간 */
  "e"."tmRiseTime",

  /* 이벤트 유형의 내부 이름 */
  "e"."strEventType",

  /* 이벤트의 표시 이름*/
  "e"."wstrEventTypeDisplayName",

  /* 이벤트의 표시 설명 */
  "e"."wstrDescription",

  /* 이벤트의 표시 설명 */
  "e"."wstrGroupName",

  /* 이벤트가 발생한 기기의 표시되는 이름 */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* 이벤트가 발생한 기기의 IP 주소 */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 또는 MariaDB의 예:

```
SELECT

  /* 이벤트 식별자 */
  `e`.`nId`,

  /* 이벤트 발생 시간 */
  `e`.`tmRiseTime`,

  /* 이벤트 유형의 내부 이름 */
  `e`.`strEventType`,

  /* 이벤트의 표시 이름 */
  `e`.`wstrEventTypeDisplayName`,

  /* 이벤트의 표시 설명 */
  `e`.`wstrDescription`,

  /* 기기 그룹 이름 */
  `e`.`wstrGroupName`,

  /* 이벤트가 발생한 기기의 표시되는 이름 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* 이벤트가 발생한 기기의 IP 주소 */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Kaspersky Security Center 데이터베이스 이름 확인

예를 들어 SQL 쿼리를 보내고 SQL 스크립트 편집기에서 데이터베이스에 연결할 시, 데이터베이스 이름을 알면 도움이 될 수 있습니다.

Kaspersky Security Center 데이터베이스의 이름을 확인하려면 다음과 같이 하십시오:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창의 섹션 창에서 **고급**와 **현재 데이터베이스 세부 정보**를 차례로 선택합니다.
3. **현재 데이터베이스 세부 정보** 섹션에서 다음 데이터베이스 속성을 확인합니다(아래 그림 참조):

   - **인스턴스 이름**

     현재 Kaspersky Security Center DB 인스턴스의 이름입니다. 기본값은 *.\KAV_CS_ADMIN_KIT*입니다.

   - **데이터베이스 이름**

     Kaspersky Security Center SQL 데이터베이스의 이름입니다. 기본값은 *KAV*입니다.

- **Kaspersky Security Center 데이터베이스에 할당된 공간**

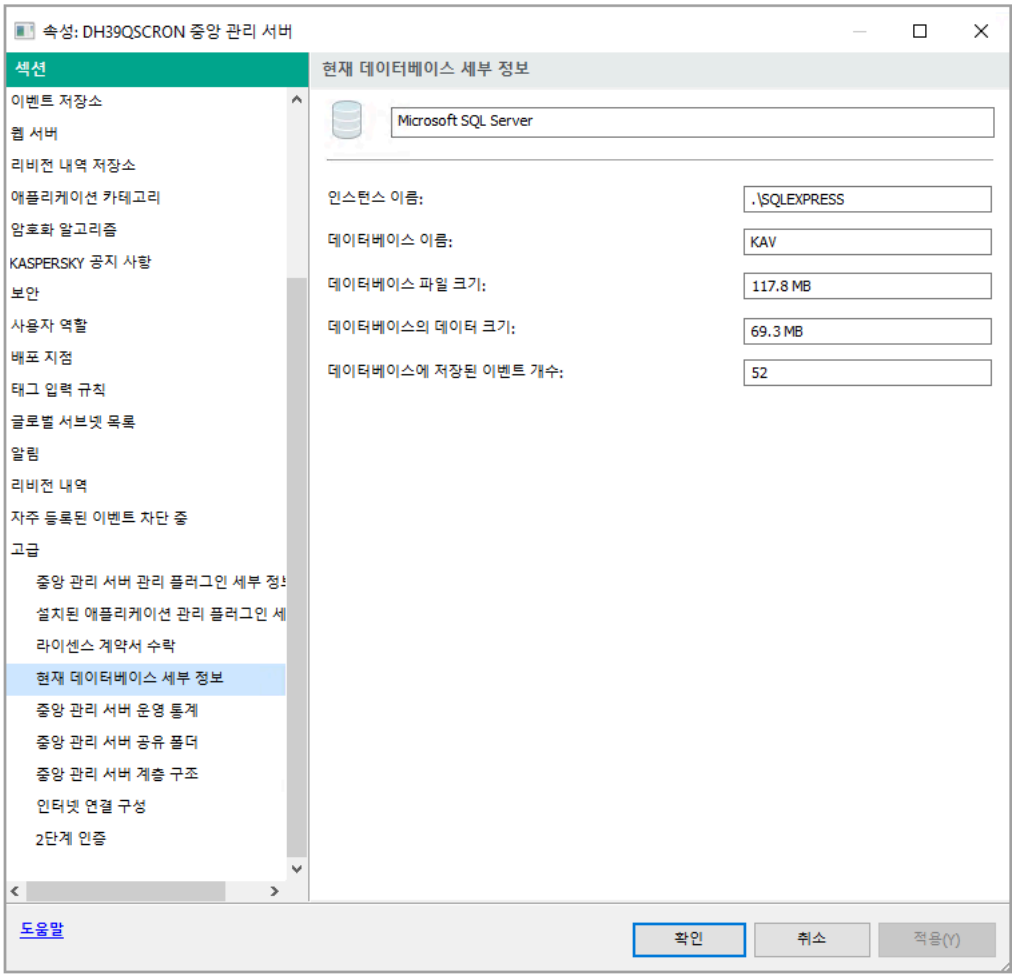
  데이터베이스 파일의 크기. 불필요한 데이터를 정리하려면 *중앙 관리 서버 점검* 작업을 사용하여 데이터베이스 압축을 구성합니다.

- **전체 데이터베이스의 데이터 크기**

  현재 DBMS에서 사용되는 실제 데이터의 크기입니다. 데이터베이스 크기가 한도 초과 문서에서는 DBMS를 진단하는 방법을 설명합니다.

- **데이터베이스에 저장된 이벤트 수**

  현재 DBMS에 저장된 이벤트의 수입니다. 자세한 내용은 이벤트 처리 및 저장소 문서를 참조하세요.



현재 중앙 관리 서버 데이터베이스에 대한 정보가 포함된 섹션입니다

4. **확인** 버튼을 눌러 중앙 관리 서버 속성 창을 닫습니다.

데이터베이스 이름을 사용하여 SQL 쿼리의 데이터베이스 주소를 지정합니다.

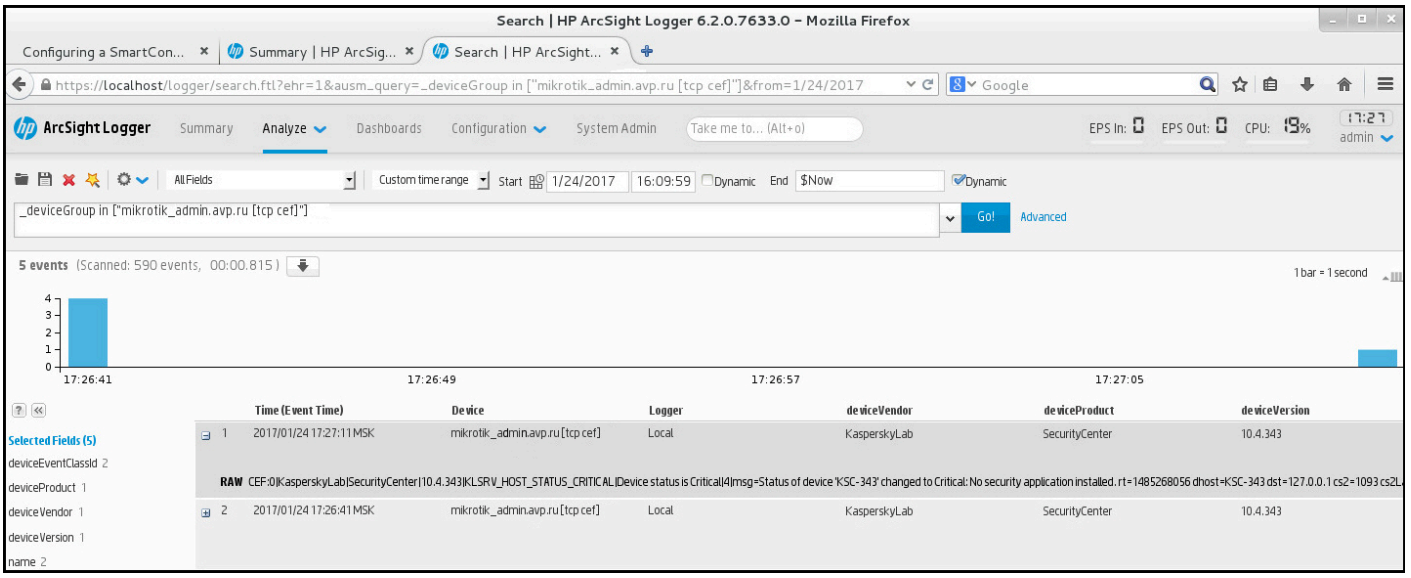
내보내기 결과 보기

이벤트 내보내기 절차가 정상적으로 완료되도록 제어할 수 있습니다. 이렇게 하려면 내보내기 이벤트가 포함된 메시지가 SIEM 시스템에서 수신되는지 확인합니다.

Kaspersky Security Center에서 보낸 이벤트가 SIEM 시스템에서 수신되어 적절하게 구문 분석되면 양쪽에서 모두 구성을 올바르게 수행한 것입니다. 그렇지 않은 경우에는 Kaspersky Security Center에서 지정한 설정을 SIEM 시스템의 구성과 대조하여 확인합니다.

아래 그림에는 ArcSight로 내보낸 이벤트가 나와 있습니다. 예를 들어 첫 번째 이벤트는 심각한 중앙 관리 서버 이벤트입니다: "*기기 상태가 위험입니다*".

SIEM 시스템에서의 내보내기 이벤트 표시 방식은 사용하는 SIEM 이벤트에 따라 다릅니다.



이벤트 예제

SNMP를 사용하여 타사 애플리케이션에 통계 보내기

이 섹션에서는 Windows에서 SNMP(Simple Network Management Protocol)를 사용하여 중앙 관리 서버에서 정보를 가져 오는 방법에 대해 설명합니다. Kaspersky Security Center에는 OID를 사용하여 중앙 관리 서버 성능 통계를 사이드 애플리케이션으로 전송하는 SNMP 에이전트가 포함되어 있습니다.

이 섹션에는 Kaspersky Security Center에 SNMP를 사용하는 동안 발생할 수 있는 문제 해결을 위한 정보도 포함되어 있습니다.

Kaspersky Security Center와 함께 사용할 SNMP 서비스 구성

이 섹션에서는 SNMP(간이 망 관리 프로토콜)를 사용하여 중앙 관리 서버에서 정보를 가져오도록 Windows에서 SNMP 서비스를 구성하는 방법에 대해 설명합니다.

SNMP 지원은 Windows에서 기본적으로 비활성화되어 있습니다.

Windows에서 SNMP 지원을 활성화하려면:

1. **제어판**으로 이동합니다.
2. **프로그램 추가/제거** 메뉴를 엽니다.
3. **Windows 기능 켜기 또는 끄기**를 클릭 합니다.

4. Windows 기능 목록에서 SNMP 기능으로 이동한 다음 **확인**을 클릭합니다.
5. **제어판 → 관리 도구 → 서비스**로 이동합니다.
6. **SNMP 서비스**를 선택하고 실행합니다.
7. 표준 UDP 포트에 대해 `netstat`로 테스트하여 listening이 작동하는지 확인합니다.

Windows에서는 SNMP 지원이 활성화되어 있습니다.

Windows에서 SNMP 서비스를 구성하려면:

1. 일반 또는 자동 설치 중에 Kaspersky Security Center의 **SNMP 에이전트** 구성 요소가 설치되었는지 확인합니다.
2. **SNMP 서비스** 및 **SNMP 트랩** Windows 서비스가 실행 중인지 확인합니다.
3. ManageEngine MIB 브라우저가 시스템에 설치되어 있는지 확인합니다.
4. **SNMP 서비스** 서비스 속성의 **보안** 탭에서 다음 권한이 있는 커뮤니티 두 개를 추가합니다.

커뮤니티	권한
`kaspersky`	알림
`public`	읽기 쓰기

5. **이 호스트에서 SNMP 패킷 수락** 필드에 ManageEngine MIB 브라우저가 설치된 기기의 IP 주소(예: 10.10.10.105)를 추가합니다.
6. **트랩** 탭에서 **커뮤니티 이름** 필드에 `kaspersky`를 입력합니다.
7. **OK**를 눌러 변경 사항을 저장하고 서비스 속성 창을 닫습니다.
8. ManageEngine MIB 브라우저의 Kaspersky Security Center 설치 폴더에서 adminkit.mib 파일을 로드합니다. 기본적으로 adminkit.mib 파일은 <Disk>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp 폴더에 있습니다.
9. ManageEngine MIB 브라우저 창의 **호스트** 필드에 Kaspersky Security Center 중앙 관리 서버가 설치된 기기의 IP 주소를 추가합니다.

SNMP 서비스는 간이 망 관리 프로토콜(SNMP)을 사용하여 중앙 관리 서버에서 정보를 가져오도록 구성됩니다.

SNMP 에이전트 및 개체 식별자

Kaspersky Security Center의 경우 SNMP 에이전트는 중앙 관리 서버 설치 중에 설치 프로그램에 의해 등록되는 동적 라이브러리 `klsnmpag.dll`로 구현됩니다. SNMP 에이전트는 `snmp.exe` 프로세스(Windows 서비스) 내에서 작동합니다. 타사 애플리케이션은 SNMP를 사용하여 중앙 관리 서버 성능에 대한 통계(카운터 형식으로 제공)를 받습니다.

각 카운터에는 고유한 *개체 식별자*(OID라고도 함)가 있습니다. 개체 식별자는 점으로 구분한 일련의 숫자입니다. 중앙 관리 서버의 개체 식별자는 1.3.6.1.4.1.23668.1093 접두사로 시작합니다. 카운터의 OID는 해당 접두사와 카운터를 설명하는 접미사를 연결한 것입니다. 예를 들어 OID 값이 1.3.6.1.4.1.23668.1093.1.1.4인 카운터에는 값이 1.1.4인 접미사가 있습니다.

Zabbix와 같은 SNMP 클라이언트를 사용하여 시스템 상태를 모니터링할 수 있습니다. 정보를 얻기 위해 정보에 해당하는 OID 값을 검색하고 해당 값을 SNMP 클라이언트에 입력할 수 있습니다. 그러면 SNMP 클라이언트는 시스템 상태를 나타내는 다른 값을 반환합니다.

카운터 및 카운터 유형 목록은 중앙 관리 서버에 있는 `adminkit.mib` 파일에 있습니다. *MIB*는 Management Information Base를 나타냅니다. 카운터 값을 요청하고 표시하도록 설계된 MIB 뷰어 애플리케이션을 통해 `.mib` 파일을 가져오고 구문 분석할 수 있습니다.

개체 식별자에서 문자열 카운터 이름 가져오기

정보를 타사 애플리케이션으로 전송하는 데 개체 식별자(OID)를 사용하려면 해당 OID에서 문자열 카운터 이름을 가져와야 합니다.

OID에서 문자열 카운터 이름을 가져오려면:

1. 중앙 관리 서버에 있는 `adminkit.mib` 파일을 텍스트 편집기에서 엽니다.
2. 첫 번째 값을 설명하는 네임스페이스를 찾습니다(왼쪽에서 오른쪽으로).
   예를 들어, 1.1.4 OID 접미사는 `"counters" (::= { kladminkit 1 })`가 됩니다.
3. 두 번째 값을 설명하는 네임스페이스를 찾습니다.
   예를 들어, 1.1.4 OID 접미사는 `counters 1`이 되며, 이는 `deployment`를 나타냅니다.
4. 세 번째 값을 설명하는 네임스페이스를 찾습니다.
   예를 들어, 1.1.4 OID 접미사는 `deployment 4`가 되며, 이는 `hostsWithAntivirus`를 나타냅니다.

문자열 카운터 이름은 이 값을 합한 것으로, 예를 들면 `<MIB base namespace>.counters.deployment.hostsWithAntivirus`이며, 이는 값이 1.3.6.1.4.1.23668.1093.1.1.4인 OID를 가리킵니다.

SNMP에 대한 개체 식별자 값

아래 표는 중앙 관리 서버 성능에 대한 정보를 타사 애플리케이션으로 전송하는 데 사용되는 개체 식별자(OID라고도 함)의 값과 설명입니다.

SNMP에 대한 개체 식별자 값 및 설명

개체 식별자 값	숫자 데이터 유형	OID	설명
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	배포 상태. 상태는 다음 중 하나일 수 있습니다. • **정보**. N 기기에 대한 라이센스가 더 이상 유효하지 않습니다. • **경고**. 다음 중 하나를 수행합니다: 중앙 관리 서버 그룹(N > M)의 총 N개의 기기에 Kaspersky 애플리케이션이 설치된 M대의 기기가 있습니다. 라이센스 L은 M일 후에 N 기기에서 만료됩니다. 애플리케이션 설치 작업 T가 N 기기에서 성공적으로 완료되었으며 M 기기를 재부팅해야 합니다. • **심각**. N 기기에 대한 라이센스가 만료되었습니다. • **확인**. 위의 어느 것도 없음.

개체 식별자 값	숫자 데이터 유형	OID	설명
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	[[deploymentStatus]] 상태는 중앙 관리 서버 그룹에 관리 중인 애플리케이션이 없는 기기가 너무 많이 포함되어 있음을 보여줍니다. 관리 중인 애플리케이션이 없는 기기가 몇 개 발견되면 값은 1이고 그렇지 않으면 0입니다.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	[[deploymentStatus]] 상태는 일부 기기에서 원격 설치 작업이 실패했음을 보여줍니다. 이러한 기기의 수는 hostsRemoteInstallFailed를 통해 얻을 수 있습니다.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	[[deploymentStatus]] 상태는 향후 7일간 라이센스가 만료되는 일부 기기가 있음을 보여줍니다. 이러한 기기의 수는 hostsLicenseExpiring을 통해 얻을 수 있습니다.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	[[deploymentStatus]] 상태는 라이센스가 만료된 일부 기기가 있음을 보여줍니다. 이러한 기기의 수는 hostsLicenseExpired를 통해 얻을 수 있습니다.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	중앙 관리 서버 그룹의 기기 수.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	관리 중인 애플리케이션이 있는, 중앙 관리 서버 그룹의 기기 수.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	원격 설치 작업이 실패한 기기 수.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	7 일 이내 만료되는 라이센스 키의 ID.
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	만료된 라이센스 키의 ID.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	라이센스 만료 전 남은 일수. 이 파라미터는 만료일까지 남은 시간이 7일 미만이면 라이센스 기간이 만료된 것으로 간주합니다. 만료 날짜가 7일 이상 남았다면 값은 0입니다.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	7 일 이내 곧 만료되는 라이센스가 있는 기기 수.
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	라이센스가 만료된 기기 수.
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	안티 바이러스 베이스의 현재 업데이트 상태입니다. 상태는 다음 중 하나일 수 있습니다. • **정보**. 중앙 관리 서버 또는 기기의 안티 바이러스 베이스가 1일 이상 업데이트되지 않았으며 애플리케이션 설치 후 1일이 지나지 않았습니다. • **경고**. 중앙 관리 서버 또는 기기의 안티 바이러스 베이스가 3일 이상 업데이트되지 않았습니다. 이 값은 그룹 설정에서 변경할 수 있습니다. • **심각**. 중앙 관리 서버 또는 기기의 안티 바이러스 베이스가 7일 이상 업데이트되지 않았습니다. 이 값은 그룹 설정에서 변경할 수 있습니다. • **확인**. 위의 어느 것도 없음.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	중앙 관리 서버가 오랫동안 업데이트되지 않았습니다. 긴 것으로 간주되는 시간은 updatesStatus에 지정됩니다.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	일부 기기가 오랫동안 업데이트되지 않았음을 나타냅니다(기본적으로 '**심각**'은 7일 이상, '**경고**'는 3일). 이러한 기기의 수는 hostsNotUpdated를 통해 얻을 수 있습니다.
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	중앙 관리 서버에서 바이러스 백신 기반이 마지막으로 업데이트된 시간입니다.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	안티 바이러스 베이스를 포함하고 오랫동안 업데이트되지 않는 기기의 수(기본적으로 **'심각'**은 7일 이상, **'경고'**는 3일). **심각** 업데이트 상태의 기기가 있다면 이러한 기기만 계산됩니다. updatesStatus를 통해 업데이트 상태를 가져올 수 있습니다.

개체 식별자 값	숫자 데이터 유형	OID	설명
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	실시간 보호의 상태. 다음 중 하나를 수행합니다: • **경고**. 다음 중 하나를 수행합니다: 중앙 관리 서버 그룹에 속한 기기에서 보안 위반이 감지되었습니다. 암호화 오류로 인해 일부 기기가 보호 상태를 변경했습니다. 전체 검사를 오랫동안 수행하지 않았습니다. • **심각**. 중앙 관리 서버 그룹의 일부 기기에서 안티바이러스 보호가 작동하지 않습니다. • **확인**. 위의 어느 것도 없음.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	일부 기기에서 보안 애플리케이션이 실행되지 않습니다. 이러한 기기의 수는 hostsAntivirusNotRunning을 통해 얻을 수 있습니다.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	일부 기기에서는 실시간 보호가 실행되지 않습니다. 이러한 기기의 수는 hostsRealtimeNotRunning을 통해 얻을 수 있습니다.
psRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.2.3	관리자가 설정한 레벨과 다른 실시간 보호 레벨을 가진 기기의 수
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	치료되지 않은 개체를 포함하는 기기입니다. 이러한 기기의 수는 hostsNotCuredObject를 통해 얻을 수 있습니다.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	일부 기기에서 위협이 발견되었습니다. 이러한 기기의 수는 hostsTooManyThreats를 통해 얻을 수 있습니다.
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	시스템의 이러스 발생 상태입니다. 특정 시간 동안 특정 양의 바이러스가 발견되면 값은 1이고 그렇지 않으면 0입니다. 바이러스의 양과 시간은 바이러스 공격 설정을 사용하여 중앙 관리 서버에서 지정됩니다.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	취약점이 탐지되었습니다.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	기기 보호 상태를 변경한 암호화 오류가 탐지되었습니다.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	일부 기기에서 취약점이 탐지되었습니다.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	장기간 전체 검사가 없는 기기가 탐지되었습니다.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	네트워크 에이전트가 다시 시작 후에만 시작되는 기기를 탐지했습니다.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	보안 제품이 실행되지 않는 기기 수.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	실시간 보호가 실행되지 않는 기기 수.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	실시간 보호 수준이 허용되지 않는 기기 수.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	치료되지 않은 개체를 포함하는 기기 수입니다.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	위협을 포함하는 기기 수.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	안티 바이러스 전체 검사의 상태는 다음 중 하나입니다. • **정보**. 애플리케이션 설치 후 7일 이내입니다. • **경고**. 애플리케이션 설치 후 7일 이상 바이러스 백신 전체 검사를 수행하지 않은 경우입니다. • **심각**. 애플리케이션 설치 후 14일 이상 바이러스 백신 전체 검사를 수행하지 않은 경우입니다. • **확인**. 위의 어느 것도 없음.

개체 식별자 값	숫자 데이터 유형	OID	설명
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	일정 시간 동안 검사되지 않은 기기 수. 이러한 기기의 수는 hostsNotScannedLately를 통해 얻을 수 있습니다. 시간은 fullScanStatus에 지정됩니다.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	일정 시간 동안 검색되지 않은 기기 수. 시간은 fullScanStatus에 지정됩니다.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	중앙 관리 서버의 논리 네트워크의 상태. 다음 중 하나를 수행합니다: • **경고**. 액세스할 수 없는 경고 상태의 기기가 있거나 중앙 관리 서버 그룹에 속하지 않는 기기가 있는 경우. • **심각**. 중앙 관리 서버에 의해 제어 권한이 상실된 기기가 있거나 위험 상태의 기기가 있으며 이 기기에 액세스할 수 없는 경우입니다. • **확인**. 위의 어느 것도 없음.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	일부 기기가 오랫동안 중앙 관리 서버에 연결되지 않았음을 나타냅니다(**경고** 상태 기기의 경우 7일 이상, **심각** 상태 기기의 경우 4일). 이러한 기기의 수는 hostsNotConnectedLongTime을 통해 얻을 수 있습니다.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	중앙 관리 서버에 의해 제어가 상실된 기기가 있습니다. 이러한 기기의 수는 hostsControlLost를 통해 얻을 수 있습니다.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	중앙 관리 서버 그룹에 속하지 않으며 중앙 관리 서버에서 찾은 기기 수.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	중앙 관리 서버의 그룹 수.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	오랫동안 중앙 관리 서버에 연결되지 않은 기기 수. 긴 것으로 간주되는 시간은 notConnectedLongTime에 지정됩니다.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	중앙 관리 서버에서 제어하지 않는 기기 수.
eventsStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.6.1	이벤트 하위 시스템의 상태는 다음 중 하나입니다. • **경고**. 다음 중 하나를 수행합니다: 중앙 관리 서버 그룹의 기기가 오랫동안 Windows 업데이트를 검색하지 않았습니다. 상태 문제가 있는 기기가 있습니다. • **심각**. 다음 중 하나를 수행합니다: 하나 이상의 기기에서 '심각' 이벤트가 있습니다. 하나 이상의 기기에서 '오류' 이벤트가 있습니다. 하나 이상의 기기에서 작업이 성공적으로 완료되지 않은 이벤트가 있습니다. 중앙 관리 서버 그룹의 기기가 오랫동안 Windows 업데이트를 검색하지 않았습니다. 상태 문제가 있는 기기가 있습니다. • **정보.** 다음 중 하나를 수행합니다: 모든 기기에서 마지막으로 전체 바이러스 검사를 수행한 지 일주일이 지나지 않았습니다. 원격 설치 작업이 완료되었으며 다시 시작할 기기가 없습니다. 마지막 중앙 관리 서버가 업데이트된 지 일주일이 지나지 않았습니다. 중앙 관리 서버가 장기간 업데이트되지 않았으며 현재 업데이트가 진행 중입니다. • **확인**. 위의 어느 것도 없음.
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	[[eventsStatus]] 상태는 중앙 관리 서버에 몇 가지 심각 이벤트가 있음을 보여줍니다. criticalEventsCount를 통해 이러한 이벤트 수를 얻을 수 있습니다. 기기에 하나 이상의 심각 이벤트가 있으면 값은 1이고 그렇지 않으면 0입니다.
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	중앙 관리 서버의 중요한 이벤트 수.

문제 해결

이 섹션에서는 SNMP 서비스를 사용하는 동안 발생할 수 있는 몇 가지 일반적인 문제에 대한 해결 방법을 설명합니다.

타사 애플리케이션은 SNMP 서비스에 연결할 수 없습니다.

Kaspersky Security Center와 함께 사용할 SNMP 서비스 구성 섹션에 설명된 대로 SNMP 서비스가 설치 및 구성되어 있는지 확인합니다.

SNMP 서비스가 작동하지만 타사 애플리케이션은 값을 가져올 수 없습니다.

SNMP 에이전트 추적 로그를 허용하고 비어 있지 않은 파일이 생성되었는지 확인합니다. 생성된 경우 SNMP 에이전트가 올바르게 등록되고 작동하고 있는 것입니다. 그런 다음 사이드 서비스 설정에서 SNMP 서비스의 연결을 허용하십시오. 사이드 서비스가 SNMP 에이전트와 동일한 호스트에서 작동하는 경우 IP 주소 목록에는 해당 호스트의 IP 주소 또는 `loopback 127.0.0.1`이 포함되어야 합니다.

에이전트와 통신하는 SNMP 서비스는 Windows에서 실행되어야 합니다. regedit를 사용하여 Windows 레지스트리에서 SNMP 에이전트에 대한 경로를 지정할 수 있습니다.

- Windows 10의 경우:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents

- Windows Vista 및 Windows Server 2008의 경우:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

regedit를 사용하여 SNMP 에이전트 추적 로그를 허용할 수도 있습니다.

- 32비트 운영 체제:

  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug

- 64비트 운영 체제:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb

  "TraceLevel"=dword:00000004

  "TraceDir"="C:\\"

값이 관리 콘솔의 상태와 일치하지 않습니다

중앙 관리 서버의 부하를 줄이기 위해 SNMP 에이전트에 대해 값 캐싱이 구현됩니다. 구현되는 캐시와 중앙 관리 서버에서 변경되는 값 사이의 대기 시간으로 인해 SNMP 에이전트가 반환한 값과 실제 값이 일치하지 않을 수 있습니다. 타사 애플리케이션으로 작업할 때는 가능한 지연 시간을 고려해야 합니다.

클라우드 환경에서 작업

이 섹션에서는 Amazon Web Services, Microsoft Azure 또는 Google 클라우드와 같은 클라우드 환경에서의 Kaspersky Security Center 배포 및 유지 관리에 대해 설명합니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)과 KSN 기능이 제공되지 않을 수도 있습니다.

클라우드 환경에서 작업 정보

Kaspersky Security Center 15.1은 실제 기기에서 작동할 뿐 아니라 클라우드 환경에서 작업하기 위한 특수 기능도 제공합니다. Kaspersky Security Center는 다음 가상 컴퓨터와 연동됩니다.

- Amazon EC2 인스턴스(이하 *인스턴스*). Amazon EC2 인스턴스는 AWS(Amazon Web Services) 플랫폼을 토대로 생성되는 가상 컴퓨터입니다. Kaspersky Security Center는 AWS *API*(애플리케이션 프로그래밍 인터페이스)를 사용합니다.
- Microsoft Azure 가상 컴퓨터. Kaspersky Security Center는 Azure API를 사용합니다.
- Google 클라우드 가상 컴퓨터 인스턴스. Kaspersky Security Center는 Google API를 사용합니다.

인스턴스 또는 가상 컴퓨터에 Kaspersky Security Center를 배포하면 클라우드 환경에서 기기 보호를 관리하고 클라우드 환경에서의 작업을 위한 Kaspersky Security Center의 특수 기능을 사용할 수 있습니다. 포함된 기능:

- 클라우드 환경에서 API 도구를 사용하여 기기를 검색합니다
- API 도구를 사용하여 클라우드 환경의 기기에 네트워크 에이전트 및 보안 제품을 설치합니다
- 특정 클라우드 세그먼트에 속하는지 여부에 따라 기기를 검색합니다

물리적인 서버보다 클라우드 서버를 더 쉽게 유지보수하고 서비스를 제공할 수 있는 등의 경우에는 Kaspersky Security Center 중앙 관리 서버가 배포되어 있는 인스턴스 또는 가상 컴퓨터를 사용하여 온프레미스 기기를 보호할 수도 있습니다. 이러한 경우 온프레미스 기기에 설치된 중앙 관리 서버를 사용할 때와 같은 방법으로 중앙 관리 서버를 사용합니다.

AWS의 유료 AMI(Amazon 머신 이미지) 또는 Azure의 월 종량제 요금이 청구되는 SKU에서 배포된 Kaspersky Security Center에서는 SIEM 시스템과의 통합을 비롯한 취약점 및 패치 관리가 자동 활성화되며 모바일 기기 관리는 활성화할 수 없습니다.

중앙 관리 서버는 관리 콘솔과 함께 설치됩니다. 중앙 관리 서버가 설치된 기기에는 Kaspersky Security for Windows Server도 자동으로 설치됩니다.

클라우드 환경 작업의 특성을 고려하여 클라우드 환경 구성 마법사를 사용하여 Kaspersky Security Center 구성할 수 있습니다.

시나리오: 클라우드 환경용 배포

이 섹션에서는 Amazon Web Services, Microsoft Azure, Google 클라우드와 같은 클라우드 환경에서 운영하기 위한 Kaspersky Security Center의 배포에 대해 설명합니다.

이 배포 시나리오를 완료한 이후에는 Kaspersky Security Center 중앙 관리 서버 및 관리 콘솔이 시작되어 기본 파라미터로 구성됩니다. Kaspersky Security Center에서 관리하는 안티 바이러스 보호 기능이 선택한 Amazon EC2 인스턴스 또는 Microsoft Azure 가상 컴퓨터에 배포됩니다. Kaspersky Security Center의 구성을 미세 조정하고, 복잡한 관리 그룹 구조를 만들고 그룹에 대해 여러 정책과 작업을 만들 수 있습니다.

클라우드 환경에서 작업을 위한 Kaspersky Security Center의 배포는 다음과 같이 구성됩니다.

1. 준비 작업
2. 중앙 관리 서버 배포
3. 보호해야 하는 가상 컴퓨터에 Kaspersky 안티 바이러스 애플리케이션 설치
4. 업데이트 다운로드 설정 구성
5. 기기 보호 상태에 대한 리포트 관리용 설정 구성

클라우드 환경 구성 마법사는 초기 구성 수행 용도입니다. 바로 사용할 수 있는 이미지에서 Kaspersky Security Center를 처음 배포할 때 자동으로 시작됩니다. 언제든지 마법사를 수동으로 시작할 수 있습니다. 또한 마법사가 수행하는 모든 작업을 수동으로 수행할 수 있습니다.

클라우드 환경에 Kaspersky Security Center 중앙 관리 서버를 배포하는 데 최소한 1시간을 할당하고, 클라우드 환경에 보호 제품을 배포하는 데 최소한 하루를 할당하는 것이 좋습니다.

클라우드 환경에서의 Kaspersky Security Center 배포는 다음 단계로 진행됩니다:

1. **클라우드 세그먼트 구성 계획**

   클라우드 환경에서 Kaspersky Security Center가 작동하는 방식을 알아봅니다. 중앙 관리 서버를 배포할 위치(클라우드 환경 내부 또는 외부)를 계획하고 얼마나 많은 클라우드 세그먼트를 보호할 것인지 결정합니다. 클라우드 환경 외부에 중앙 관리 서버를 배포하려는 경우 또는 5000대 이상의 기기를 보호하려는 경우 중앙 관리 서버를 수동으로 설치해야 합니다.

   Google 클라우드를 사용하려면 중앙 관리 서버만 수동으로 설치하면 됩니다.

2. **리소스 계획**

   배포에 필요한 모든 리소스가 확보되었는지 확인합니다.

3. **바로 사용할 수 있는 미리 준비된 이미지로 Kaspersky Security Center에 가입**

   AWS Marketplace에서 바로 사용할 수 있는 AMI 중 하나를 선택하거나 Azure Marketplace에서 사용 기반 월 요금이 청구되는 SKU를 선택하고, 필요한 경우 Marketplace 규칙에 따라 결제를 하거나 BYOL 모델을 사용하도록 선택한 다음 이미지를 사용하여 Amazon EC2 인스턴스 또는 Kaspersky Security Center가 설치된 Microsoft Azure 가상 컴퓨터를 배포합니다.

   이 단계는 클라우드 환경 내의 인스턴스 또는 가상 컴퓨터에 중앙 관리 서버를 배포할 계획이고 5000대 이하의 기기에 대해 보호 제품을 배포할 계획인 경우에만 필요합니다. 그렇지 않다면 이 단계가 필요하지 않으며 대신 중앙 관리 서버, 관리 콘솔 및 DBMS를 수동으로 설치해야 합니다.

   이 단계는 Google 클라우드에서는 사용할 수 없습니다.

4 DBMS의 위치 결정

DBMS의 위치를 결정합니다.

클라우드 환경 외부의 데이터베이스를 사용하려면 작동하는 데이터베이스가 있는지 확인합니다.

Amazon RDS(Relational Database Service)를 사용하려는 경우 AWS 클라우드 환경에서 RDS를 사용하여 데이터베이스를 생성합니다.

Microsoft Azure SQL DBMS를 사용하려는 경우 Microsoft Azure 클라우드 환경에서 Azure Database Service를 사용하여 데이터베이스를 생성합니다.

Google MySQL을 사용하려면 Google Cloud에서 데이터베이스를 생성합니다(자세한 내용은 https://cloud.google.com/sql/docs/mysql 참고).

5 선택한 기기에 수동으로 중앙 관리 서버 및 관리 콘솔(Microsoft Management Console 기반 및/또는 웹 기반 콘솔) 설치

Kaspersky Security Center에 대한 주요 설치 시나리오에서 설명한 대로 선택한 기기에 중앙 관리 서버, 관리 콘솔 및 DBMS를 설치합니다.

이 단계는 클라우드 환경 외부에 중앙 관리 서버를 배포하려는 경우 또는 5000대 이상의 기기에 대한 보호 제품을 배포하려는 경우에 필요합니다. 그런 다음 중앙 관리 서버가 하드웨어 요구 사항을 충족하는지 확인합니다. 그렇지 않으면 이 단계가 필요하지 않으며 AWS Marketplace, Azure Marketplace 또는 Google Cloud에서 미리 준비된 이미지 형태의 Kaspersky Security Center를 서브스크립션 구매하는 것으로도 충분합니다.

6 중앙 관리 서버에 클라우드 API와 연동할 수 있는 권한이 있는지 확인

AWS에서 AWS Management Console로 이동하고 IAM 역할 또는 IAM 사용자 계정을 생성합니다. 생성된 IAM 역할(또는 IAM 사용자 계정)을 통해 Kaspersky Security Center가 AWS API: 검색 클라우드 세그먼트와 연동하고 보호 제품을 배포할 수 있습니다.

Azure에서 암호를 사용하여 서브스크립션 및 애플리케이션 ID를 생성합니다. Kaspersky Security Center는 이러한 자격증명을 사용하여 Azure API: 검색 클라우드 세그먼트와 연동하고 보호 제품을 배포합니다.

Google Cloud에서 프로젝트를 등록하고 프로젝트 ID와 개인 키를 가져옵니다. Kaspersky Security Center는 이러한 자격 증명을 사용하여 Google API를 사용하는 클라우드 세그먼트를 검색합니다.

7 보호된 인스턴스에 대한 IAM 역할 생성(AWS에만 해당됨)

AWS Management Console에서 AWS에 대한 요청 실행 권한 집합을 정의하는 IAM 역할을 만듭니다. 새롭게 만들어진 이 역할은 이후에 새 인스턴스에 할당됩니다. Kaspersky Security Center를 사용하여 인스턴스에 보호 제품을 설치하려면 IAM 역할이 필요합니다.

8 Amazon Relational Database Service 또는 Microsoft Azure SQL을 사용하여 데이터베이스 준비

Amazon RDS(Relational Database Service)를 사용하려는 경우 데이터베이스 백업을 저장할 S3 버킷과 Amazon RDS DB 인스턴스를 생성합니다. 중앙 관리 서버가 설치된 것과 같은 EC2 인스턴스에 데이터베이스를 배치하려는 경우나 다른 위치에 데이터베이스를 배치하려는 경우에는 이 단계를 건너뛰어도 됩니다.

Microsoft Azure SQL을 사용하려는 경우 Microsoft Azure에서 스토리지 계정과 데이터베이스를 생성합니다.

Google MySQL을 사용하려면 Google Cloud에서 데이터베이스를 생성합니다(자세한 내용은 https://cloud.google.com/sql/docs/mysql 참고).

9 클라우드 환경 작업용 Kaspersky Security Center 라이센스 받기

Kaspersky Security Center가 클라우드 환경에서 작동하도록 라이센스를 부여받았는지 확인하고, 애플리케이션이 라이센스를 라이센스 저장소에 추가할 수 있도록 활성화코드 또는 키 파일을 제공합니다. 클라우드 환경 구성에서 이 단계를 완료할 수 있습니다.

이 단계는 BYOL 모델에 기초하여 무료로 바로 사용할 수 있는 AMI를 사용하여 설치된 Kaspersky Security Center를 사용하거나, AMI을 사용하지 않고 Kaspersky Security Center를 수동으로 설치하는 경우 필요합니다. 이 경우 Kaspersky Security Center를 활성화하려면 Kaspersky Security for Virtualization 또는 Kaspersky Hybrid Cloud Security용 라이센스가 필요합니다.

미리 준비된 이미지로 설치한 Kaspersky Security Center를 사용한다면 이 단계를 수행할 필요가 없으며, 클라우드 환경 구성 마법사에서 해당 창이 표시되지 않습니다.

10. **클라우드 환경에서 인증**

    Kaspersky Security Center가 필요한 권한을 사용하여 작동할 수 있도록 Kaspersky Security Center에 AWS, Azure 또는 Google Cloud 자격증명을 제공합니다. 클라우드 환경의 권한 부여 중에 이 단계를 완료할 수 있습니다.

11. **중앙 관리 서버가 클라우드 세그먼트의 기기에 대한 정보를 수신할 수 있도록 클라우드 세그먼트 검색**

    클라우드 세그먼트 검색을 시작합니다. AWS 환경에서 Kaspersky Security Center는 IAM 역할 또는 IAM 사용자의 권한에 따라 액세스할 수 있는 모든 인스턴스의 주소와 이름을 수신하게 됩니다. Microsoft Azure 환경에서 Kaspersky Security Center는 Reader 역할의 권한에 따라 액세스할 수 있는 모든 가상 컴퓨터의 주소와 이름을 수신하게 됩니다.

    그러면 Kaspersky Security Center를 사용하여 탐지된 인스턴스 또는 가상 컴퓨터에 Kaspersky 애플리케이션 및 다른 공급업체의 소프트웨어를 설치할 수 있습니다.

    Kaspersky Security Center는 검색을 정기적으로 시작하여 새 인스턴스 또는 가상 컴퓨터를 자동으로 탐지합니다.

12. **모든 네트워크 기기를 클라우드 관리 그룹에 추가**

    발견된 인스턴스 또는 가상 컴퓨터를 **관리 중인 기기\클라우드** 관리 그룹으로 이동하여 중앙 집중식 관리를 받을 수 있게 합니다. 기기에 설치되어 있는 운영 체제 등에 따라 하위 그룹에 기기를 할당하려는 경우에는 **관리 중인 기기\클라우드** 그룹 내에 여러 관리 그룹을 만들 수 있습니다. **관리 중인 기기\클라우드** 그룹 정기 검색 중에 탐지되는 모든 기기의 자동 이동을 활성할 수 있습니다.

13. **네트워크에 있는 기기를 중앙 관리 서버에 연결하기 위해 네트워크 에이전트 사용**

    클라우드 환경의 기기에 네트워크 에이전트를 설치합니다. 네트워크 에이전트는 기기와 중앙 관리 서버 간의 통신 기능을 제공하는 Kaspersky Security Center의 구성 요소입니다. 네트워크 에이전트 설정은 기본적으로 자동 구성됩니다.

    각 기기에 로컬로 네트워크 에이전트를 설치할 수 있습니다. Kaspersky Security Center를 사용하여 원격으로 기기에 네트워크 에이전트를 설치할 수도 있습니다. 또는 이 단계를 건너뛰고 최신 버전의 보안 제품과 함께 네트워크 에이전트를 설치할 수도 있습니다.

14. **네트워크 기기에 최신 버전의 보안 제품 설치**

    보안 제품을 설치할 기기를 선택한 다음 해당 기기에 최신 버전의 보안 제품을 설치하십시오. Kaspersky Security Center를 사용하여 중앙 관리 서버에 설치하거나 로컬에서 설치할 수 있습니다.

    이러한 프로그램의 설치 패키지를 수동으로 만들어야 할 수 있습니다.

    Kaspersky Endpoint Security for Linux는 Linux를 실행하는 인스턴스/가상 컴퓨터용입니다.

    Kaspersky Security for Windows Server는 Windows를 실행하는 인스턴스/가상 컴퓨터용입니다.

15. **업데이트 설정 구성**

클라우드 환경 구성을 시작할 때 **취약점 및 필수 업데이트 검색 작업**이 자동 생성됩니다. 작업을 수동으로 만들 수도 있습니다. 이 작업은 Kaspersky Security Center 도구를 사용하여 네트워크 기기에 나중에 설치할 필수 애플리케이션 업데이트를 자동으로 찾아서 다운로드합니다.

클라우드 환경 구성 마법사가 완료되고 나면 다음 단계를 수행하는 것이 좋습니다:

1. **리포트 관리 구성**

   중앙 관리 서버 노드의 작업 영역에 있는 **모니터링** 탭에서 리포트를 확인할 수 있습니다. 이메일로도 리포트를 받을 수 있습니다. **모니터링** 탭의 리포트는 기본적으로 사용할 수 있습니다. 이메일을 통한 리포트 수신을 구성하려면 리포트를 받아야 하는 이메일 주소를 지정한 다음 리포트 형식을 구성합니다.

결과

시나리오를 완료하면 초기 구성이 성공했는지 확인할 수 있습니다:

- 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 통해 중앙 관리 서버에 연결할 수 있습니다.
- 최신 버전의 Kaspersky 보안 제품이 관리 중인 기기에 설치되어 실행됩니다.
- Kaspersky Security Center에서 모든 관리 중인 기기에 대한 기본 정책과 작업을 생성됩니다.

클라우드 환경에서 Kaspersky Security Center를 배포하기 위한 필수 구성 요소

Amazon Web Services 또는 Microsoft Azure 클라우드 환경에서 Kaspersky Security Center 배포를 시작하기 전에 다음 항목이 있는지 확인합니다:

- 인터넷 접속
- 다음 계정 중 하나를 사용합니다.
  - Amazon Web Services 계정(AWS 작업용)
  - Microsoft 계정(Azure 작업용)
  - Google 계정(Google Cloud 작업용)
- 다음 중 하나를 수행합니다:
  - Kaspersky Security for Virtualization용 라이센스
  - Kaspersky Hybrid Cloud Security용 라이센스
  - 라이센스 구매 예산(Kaspersky Security for Virtualization 또는 Kaspersky Hybrid Cloud Security)
  - Azure Marketplace에서 바로 사용할 수 있는 이미지 구매 예산
- Kaspersky Endpoint Security for Linux 및 Kaspersky Security for Windows Server의 최신 버전 가이드

클라우드 환경에 있는 중앙 관리 서버용 하드웨어 요구 사항

클라우드 환경에 배포하는 경우 중앙 관리 서버 및 데이터베이스 서버의 요구 사항은 물리적 중앙 관리 서버의 요구 사항과 동일합니다(관리하려는 기기 수에 따름). 자세한 내용은 클라우드 환경 설명서를 참고하십시오.

클라우드 환경의 라이센스 옵션

클라우드 환경의 작업은 Kaspersky Security Center의 기본 기능 범위에 포함되지 않으므로 전용 라이센스가 필요합니다.

클라우드 환경에서 작업할 때는 두 가지 Kaspersky Security Center 라이센스 옵션을 사용할 수 있습니다:

- 유료 AMI(Amazon Web Services) 또는 사용량에 따라 월 요금이 청구되는 SKU(Microsoft Azure).

  이 옵션을 사용하는 경우 Kaspersky Security Center용 라이센스뿐 아니라 Kaspersky Endpoint Security for Linux 및 Kaspersky Security for Windows Server용 라이센스도 부여됩니다. 사용하는 클라우드 환경의 규칙에 따라 비용을 지불해야 합니다.

  이 모델에서는 중앙 관리 서버 하나당 클라이언트 기기를 200대까지 포함할 수 있습니다.

- BYOL(Bring Your Own License) 모델에 따라 관련 라이센스를 사용하는 무료 즉시 사용 가능 이미지.

  AWS 또는 Azure에서 Kaspersky Security Center 라이센스를 받으려면 다음 애플리케이션 중 하나의 라이센스가 있어야 합니다:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  BYOL 모델에서는 중앙 관리 서버 하나당 클라이언트 기기를 10만 대까지 포함할 수 있습니다. 또한 이 모델에서는 AWS, Azure 또는 Google 클라우드 환경 외부에서 기기를 관리할 수 있습니다.

  다음과 같은 경우 BYOL 모델을 선택할 수 있습니다:

  - 유효한 Kaspersky Security for Virtualization 라이센스를 이미 소유하고 있는 경우.
  - 유효한 Kaspersky Hybrid Cloud Security 라이센스를 이미 소유하고 있는 경우.
  - Kaspersky Security Center 배포 전에 즉시 라이센스를 구매하려는 경우.

  최초 설치 단계에서 Kaspersky Security Center가 활성화코드 또는 키 파일을 입력하라고 안내합니다.

  BYOL을 선택하는 경우 Azure Marketplace 또는 AWS Marketplace를 통해 Kaspersky Security Center 사용 요금을 결제할 필요가 없습니다.

두 경우 모두 취약점 및 패치 관리가 자동 활성화되며, 모바일 기기 관리는 활성화할 수 없습니다.

Kaspersky Hybrid Cloud Security용 라이센스를 사용하여 클라우드 환경 지원 기능을 활성화할 때 오류가 발생하면 해당 키 파일을 사용 합니다.

Kaspersky Security Center 서브스크립션에 가입하면 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 Kaspersky Security Center 중앙 관리 서버가 설치된 Microsoft Azure 가상 컴퓨터가 제공됩니다. Kaspersky Security for Windows Server 및 Kaspersky Endpoint Security for Linux용 설치 패키지는 중앙 관리 서버에서 제공됩니다. 클라우드 환경의 기기에 이러한 애플리케이션을 설치할 수 있습니다. 이러한 애플리케이션은 라이센스를 부여받지 않아도 됩니다.

관리 중인 기기가 1주일보다 이상 중앙 관리 서버에 표시되지 않으면 기기의 애플리케이션(Kaspersky Security for Windows Server 또는 Kaspersky Endpoint Security for Linux)이 기능 제한 모드로 전환됩니다. 애플리케이션을 다시 활성화하려면 애플리케이션이 설치된 기기가 중앙 관리 서버에 다시 표시되도록 해야 합니다.

클라우드 환경에서 작업하기 위한 데이터베이스 옵션

Kaspersky Security Center를 사용하려면 데이터베이스가 있어야 합니다. AWS, Microsoft Azure 또는 Google 클라우드에서 Kaspersky Security Center를 배포할 때는 다음의 세 가지 옵션을 사용할 수 있습니다.

- 중앙 관리 서버와 같은 기기에 로컬 데이터베이스를 생성합니다. Kaspersky Security Center에서는 관리 중인 기기를 5,000대까지 지원할 수 있는 SQL Server Express 데이터베이스가 제공됩니다. SQL Server Express Edition으로도 요구를 충분히 충족할 수 있으면 이 옵션을 선택합니다.

- AWS 클라우드 환경의 RDS(Relational Database Service) 또는 Microsoft Azure 클라우드 환경의 Azure Database Service를 사용하여 데이터베이스를 생성합니다. SQL Express 이외의 DBMS를 사용하려는 경우 이 옵션을 선택합니다. 데이터는 클라우드 환경 내로 전송되어 저장되며 추가 비용은 발생하지 않습니다. 실제 Kaspersky Security Center를 이미 사용 중이며 데이터베이스에 일부 데이터가 있는 경우 새 데이터베이스로 데이터를 전송할 수 있습니다.

  Google 클라우드 플랫폼에서 작업하는 경우에는 Cloud SQL for MySQL만 사용할 수 있습니다.

- 기존 데이터베이스 서버를 사용합니다. 데이터베이스 서버가 이미 있으며 Kaspersky Security Center에 해당 서버를 사용하려는 경우 이 옵션을 선택합니다. 이 서버가 클라우드 환경 외부에 있으면 데이터가 인터넷을 통해 전송되며, 그러면 추가 비용이 발생할 수 있습니다.

클라우드 환경의 Kaspersky Security Center 배포 절차에는 데이터베이스를 생성(선택)하는 특수 단계가 포함됩니다.

Amazon Web Services 클라우드 환경 사용

이 섹션에서는 Amazon Web Services에서 Kaspersky Security Center 사용을 준비하는 방법을 설명합니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Amazon Web Services 클라우드 환경에서의 작업 정보

AWS Marketplace에서 AMI(Amazon 머신 이미지) 형식으로 Kaspersky Security Center를 구매할 수 있습니다. AMI는 미리 구성된 가상 컴퓨터의 준비된 이미지입니다. 유료 AMI 또는 BYOL AMI을 구독할 수 있으며 해당 이미지에 따라 Kaspersky Security Center 중앙 관리 서버가 설치된 Amazon EC2 인스턴스를 만들 수 있습니다.

AWS 플랫폼을 사용하려면, 그리고 특히 AWS Marketplace에서 앱을 구매하고 인스턴스를 만들려면 Amazon Web Services 계정이 필요합니다. https://aws.amazon.com에서 무료 계정을 만들 수 있습니다. 기존 Amazon 계정을 사용해도 됩니다.

AWS Marketplace에서 제공되는 AMI 중 하나의 서브스크립션에 가입하면 즉시 사용 가능한 Kaspersky Security Center가 설치된 인스턴스가 제공됩니다. 즉, 애플리케이션을 직접 설치하지 않아도 됩니다. 이 경우 Kaspersky Security Center 중앙 관리 서버는 인스턴스에 설치되어 있으므로 사용자의 작업이 필요하지 않습니다. 설치 후에는 관리 콘솔을 시작하고 중앙 관리 서버에 연결하여 Kaspersky Security Center 사용을 시작할 수 있습니다.

AMI 및 AWS Marketplace의 작동 방식에 대한 자세한 내용은 AWS Marketplace 도움말 페이지를 참조하십시오. AWS 플랫폼 사용 및 인스턴스 사용 방법과 관련 개념에 대한 자세한 내용은 Amazon Web Services 설명서를 참조하십시오.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Amazon EC2 인스턴스용 IAM 역할 및 IAM 사용자 계정 생성

이 섹션에서는 중앙 관리 서버의 올바른 작동을 위해 수행해야 하는 작업에 대해 설명합니다. 여기에는 AWS IAM(ID 및 접근 관리) 역할 및 사용자 계정을 사용하는 작업이 포함됩니다. 또한 클라이언트 기기에 네트워크 에이전트를 설치한 다음 Kaspersky Security for Windows Server 및 Kaspersky Endpoint Security for Linux을 설치하려면 해당 기기에서 수행해야 하는 작업에 대해서도 설명합니다.

Kaspersky Security Center 중앙 관리 서버에 AWS와 연동할 권한이 있는지 확인

Amazon Web Services 클라우드 환경에서 동작하기 위한 표준은 AWS 서비스와 연동하려는 중앙 관리 서버 인스턴스에 특별한 IAM 역할이 할당되도록 규정하고 있습니다. IAM 역할은 AWS 서비스에 대한 요청 실행 권한 집합을 정의하는 IAM 엔티티입니다. IAM 역할은 클라우드 세그먼트 검색 및 인스턴스에 애플리케이션을 설치할 수 있는 권한을 제공합니다.

IAM 역할을 생성하여 중앙 관리 서버에 할당하면 Kaspersky Security Center에 추가 정보를 제공하지 않고도 이 역할을 사용하여 인스턴스에 보호 제품을 배포할 수 있습니다.

그러나 다음과 같은 경우 중앙 관리 서버에 대한 IAM 역할을 생성하지 않는 것이 좋습니다:

- 관리하려는 보호 제품이 설치된 기기가 Amazon Web Services 클라우드 환경 내의 EC2 인스턴스에 있지만 중앙 관리 서버가 그 클라우드 환경 외부에 있을 때입니다.
- 사용자의 클라우드 세그먼트뿐만 아니라 AWS의 다른 계정으로 생성된 다른 클라우드 세그먼트 내의 인스턴스의 보호 제품도 관리할 계획을 가지고 있을 수 있습니다. 이 경우 사용자의 클라우드 세그먼트 보호를 위해서만 IAM 역할이 필요합니다. 다른 클라우드 세그먼트를 보호하는 데 IAM 역할은 필요하지 않습니다.

이러한 경우 IAM 역할을 생성하는 대신 Kaspersky Security Center에서 AWS 서비스를 사용하기 위해 사용할 *IAM 사용자 계정*을 생성해야 합니다. 중앙 관리 서버 사용을 시작하기 전에 *AWS IAM 액세스 키*(이하 *IAM 액세스 키*로도 지칭됨)를 가진 IAM 사용자 계정을 만듭니다.

IAM 역할 또는 IAM 사용자 계정을 생성하려면 AWS Management Console이 필요합니다. AWS Management Console을 사용하려면 AWS 내 계정의 사용자 이름과 암호가 필요합니다.

중앙 관리 서버에 대한 IAM 역할 생성

중앙 관리 서버를 배포하기 전에 AWS Management Console에서 인스턴스에 애플리케이션을 설치하는 데 필요한 권한이 있는 IAM 역할을 만듭니다. 자세한 내용은 IAM 역할에 대한 AWS 도움말 섹션을 참조하십시오.

중앙 관리 서버에 대한 IAM 역할을 만들려면 다음과 같이 진행합니다:

1. AWS Management Console을 열고 AWS 계정으로 로그인합니다.
2. **역할** 섹션에서 다음 권한이 주어진 역할을 생성합니다:
   - **AmazonEC2ReadOnlyAccess** 옆, 클라우드 세그먼트 검색만 실행하고 AWS API를 사용하는 EC2 인스턴스에 애플리케이션을 설치할 계획이 없는 경우.
   - **AmazonEC2ReadOnlyAccess** 및 **AmazonSSMFullAccess** - 클라우드 세그먼트 검색을 실행하고 AWS API를 사용하는 EC2 인스턴스에 애플리케이션을 설치할 계획인 있는 경우. 이 경우에는 보호되는 EC2 인스턴스에 AmazonEC2RoleforSSM 권한을 가진 IAM 역할도 할당해야 합니다.

중앙 관리 서버로 사용할 EC2 인스턴스에 이 역할을 할당해야 합니다.

새로 생성된 역할은 중앙 관리 서버의 모든 애플리케이션에서 사용할 수 있습니다. 따라서 중앙 관리 서버에서 실행 중인 모든 애플리케이션은 클라우드 세그먼트를 검색하거나 클라우드 세그먼트 내의 EC2 인스턴스에 애플리케이션을 설치할 수 있습니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Kaspersky Security Center와의 연동을 위한 IAM 사용자 계정 만들기

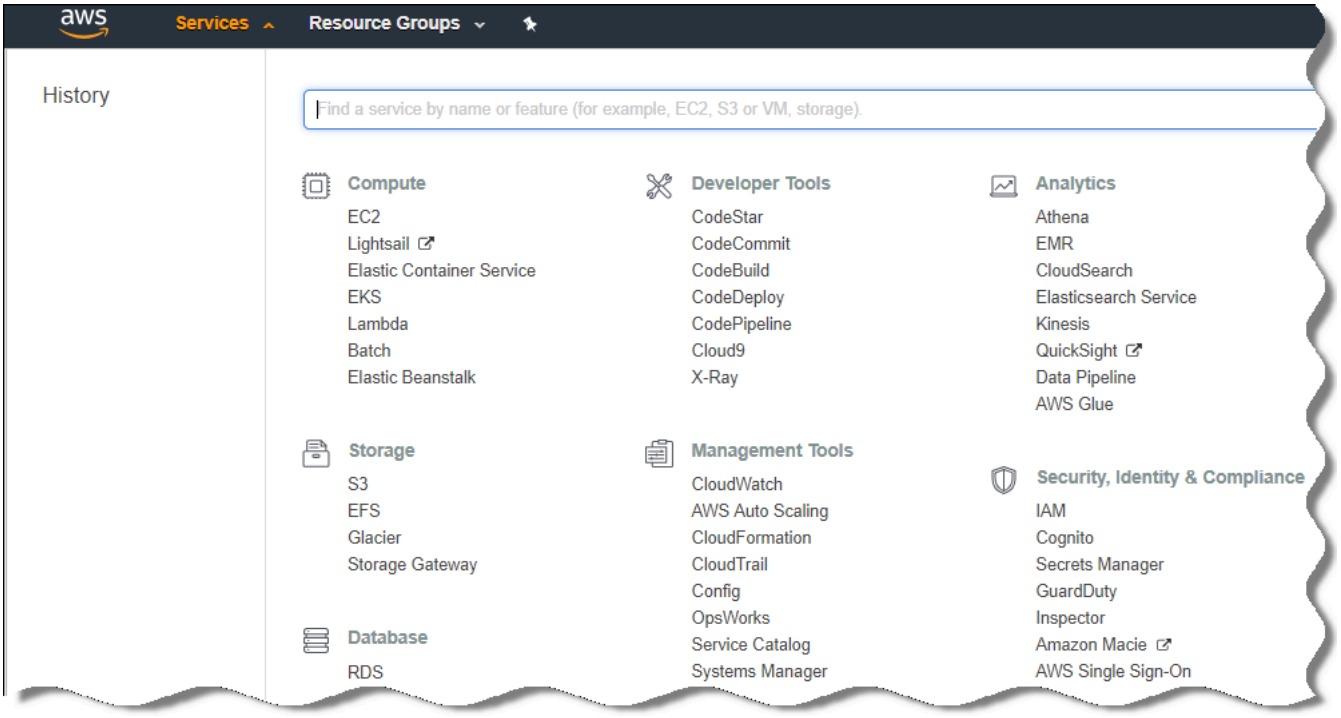
중앙 관리 서버에 인스턴스에 대한 기기 발견 및 애플리케이션 설치 권한이 있는 IAM 역할이 할당되지 않았다면 Kaspersky Security Center와의 연동 작업에 IAM 사용자 계정이 필요합니다. S3 버킷을 사용하는 경우 중앙 관리 서버 데이터 작업 백업용으로 같은 계정이나 다른 계정도 필요합니다. 필요한 모든 권한이 있는 IAM 사용자 계정 하나를 생성할 수도 있고 개별 사용자 계정 2개를 생성할 수도 있습니다.

초기 구성 중에 Kaspersky Security Center에 제공해야 할 *IAM 액세스 키*는 IAM 사용자를 위해 자동으로 생성됩니다. IAM 액세스 키는 액세스 키 ID와 비밀 키로 구성됩니다. IAM 서비스에 대한 자세한 내용은 다음 AWS 참조 페이지를 참조하십시오:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

필요한 권한을 가진 IAM 사용자 계정을 만들려면 다음과 같이 진행합니다:

1. AWS Management Console을 열고 사용자 계정으로 로그인합니다.
2. AWS 서비스 목록에서 아래 그림에 나와 있는 것처럼 **IAM**을 선택합니다.



AWS Management Console의 서비스 목록

사용자 이름 목록과 도구를 사용할 수 있는 메뉴가 포함된 창이 열립니다.

3. 사용자 계정과 관련된 콘솔 영역으로 이동하여 새 사용자 이름을 하나 이상 추가합니다.
4. 추가할 사용자에 대해 다음 AWS 속성을 지정합니다:
   - 액세스 유형:**프로그래밍 방식 액세스**.
   - 권한 경계가 설정되지 않습니다.
   - 권한:
     - **ReadOnlyAccess** - 클라우드 세그먼트 검색만 실행하고 AWS API를 사용하는 EC2 인스턴스에 애플리케이션을 설치할 계획이 없는 경우.
     - **ReadOnlyAccess** 및 **AmazonSSMFullAccess** - 클라우드 세그먼트 검색을 실행하고 AWS API를 사용하는 EC2 인스턴스에 애플리케이션을 설치할 계획인 있는 경우. 이 경우에는 보호되는 EC2 인스턴스에 AmazonEC2RoleforSSM 권한을 가진 IAM 역할도 할당해야 합니다.

     권한을 추가한 후 권한이 정확한지 확인합니다. 권한을 잘못 선택한 경우에는 이전 화면으로 돌아가서 다시 선택합니다.
5. 사용자 계정을 생성한 이후에 새로운 IAM 사용자의 IAM 액세스 키가 포함된 표가 나타납니다. 액세스 키 ID는 **액세스 키 ID** 열에 표시됩니다. 비밀 키는 **비밀 접근 허용 키** 열에 별표로 표시됩니다. 비밀 키를 보려면 **표시**를 누릅니다.

새로 생성된 계정은 AWS의 사용자 계정과 연관된 IAM 사용자 계정 목록에 표시됩니다.

클라우드 세그먼트에 Kaspersky Security Center를 배포할 때 IAM 사용자 계정을 사용하고 있음을 지정하고 Kaspersky Security Center에 액세스 키 ID와 비밀 접근 허용 키를 제공해야 합니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Amazon EC2 인스턴스에 애플리케이션 설치를 위한 IAM 역할 생성

Kaspersky Security Center를 사용하여 EC2 인스턴스에 보호 배포를 시작하기 전에 AWS Management Console에서 인스턴스에 애플리케이션을 설치하는 데 필요한 권한이 있는 IAM 역할을 만듭니다. 자세한 내용은 AWS 도움말 섹션, IAM 역할에 관한 AWS 도움말을 참조하십시오.

Kaspersky Security Center를 사용하여 보안 제품을 설치하려는 모든 EC2 인스턴스에 IAM 역할을 할당할 수 있도록 IAM 역할이 필요합니다. 인스턴스에 필요한 권한을 가진 IAM 역할을 지정하지 않으면 AWS API 도구를 사용하여 이 인스턴스에 애플리케이션을 설치할 때 오류가 발생합니다.

AWS Management Console을 사용하려면 AWS 내 계정의 사용자 이름과 암호가 필요합니다.

인스턴스에 애플리케이션을 설치하기 위한 IAM 역할을 생성하려면 다음과 같이 진행합니다:

1. AWS Management Console을 열고 AWS 계정으로 로그인합니다.
2. 왼쪽 메뉴에서 **역할**을 선택합니다.
3. **역할 만들기** 버튼을 누릅니다.
4. 나타나는 서비스 목록에서 **EC2**를 선택한 다음 **사용 사례 선택** 목록에서 **EC2**를 다시 선택합니다.
5. **다음: 권한** 버튼을 누릅니다.
6. 열리는 목록에서 **AmazonEC2RoleforSSM** 옆에 있는 확인란을 선택하십시오.
7. **다음: 검토** 버튼을 누릅니다.
8. IAM 역할에 대한 이름과 설명을 입력하고 **역할 생성** 버튼을 누릅니다.
   생성한 역할이 입력한 이름 및 설명이 포함된 역할 목록에 나타납니다.

이제부터는 새로 생성된 IAM 역할을 사용하여 Kaspersky Security Center를 통해 보호하려는 새 EC2 인스턴스를 생성하고 기존 인스턴스와 연결할 수 있습니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Azure RDS 사용

이 섹션에서는 Kaspersky Security Center용 Amazon RDS(Relational Database Service)의 데이터베이스를 준비하고, 옵션 그룹에 배치하고, RDS DB 사용을 위한 IAM 역할을 생성하고, 스토리지용 S3 버킷을 생성하고, 기존 데이터베이스를 RDS로 마이그레이션하기 위해 수행해야 하는 작업을 설명합니다.

Amazon RDS는 AWS 사용자가 AWS 클라우드 환경에서 관계형 데이터베이스를 설정, 작동 및 확장하는 데 사용할 수 있는 웹 서비스입니다. 원하는 경우 Amazon RDS DB를 통해 Kaspersky Security Center를 사용할 수 있습니다.

다음 데이터베이스로 작업할 수 있습니다.

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Amazon RDS 인스턴스 생성

Amazon RDS를 DBMS로 사용하려는 경우 Amazon RDS DB 인스턴스를 생성해야 합니다. 이 섹션에서는 SQL Express Edition 선택 방법을 설명합니다. Aurora MySQL 또는 Standard MySQL(5.7, 8.0 버전)을 사용하는 경우 이러한 엔진 중 하나를 선택해야 합니다.

Amazon RDS DB 인스턴스를 생성하려면 다음과 같이 하십시오:

1. https://console.aws.amazon.com 에서 AWS Management Console을 열고 사용자 계정으로 로그인합니다.
2. AWS 인터페이스를 사용하여 다음 설정으로 데이터베이스를 생성합니다:
   - 엔진: Microsoft SQL Server, SQL Express Edition
   - DB 엔진 버전: SQL Server 2014 12.00.5546.0v1
   - DB 인스턴스 클래스: db.t2.medium
   - 스토리지 유형: 범용
   - 할당된 스토리지: 최소 50GiB
   - 보안 그룹: Kaspersky Security Center 중앙 관리 서버가 포함된 EC2 인스턴스를 배치할 그룹

   RDS 인스턴스의 식별자, 사용자 이름 및 암호를 생성합니다.

   다른 모든 필드에서는 기본 설정을 그대로 두어도 됩니다. Amazon RDS 인스턴스를 사용자 지정하려는 경우에는 기본 설정을 변경합니다. 도움말을 확인하려면 AWS 정보 페이지를 참조하십시오.
3. 마지막 단계에서 AWS에 프로세스의 결과가 표시됩니다. Amazon RDS 인스턴스의 상세 정보를 확인하려면 **DB 인스턴스 상세 정보 보기**를 클릭합니다. 다음 작업을 계속 진행하려면 Amazon RDS 인스턴스용 옵션 그룹 생성을 시작합니다.

   새 Amazon RDS 인스턴스를 생성하는 작업은 몇 분 정도 걸릴 수 있습니다. 인스턴스가 생성되고 나면 해당 인스턴스를 통해 Kaspersky Security Center 데이터를 사용할 수 있습니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

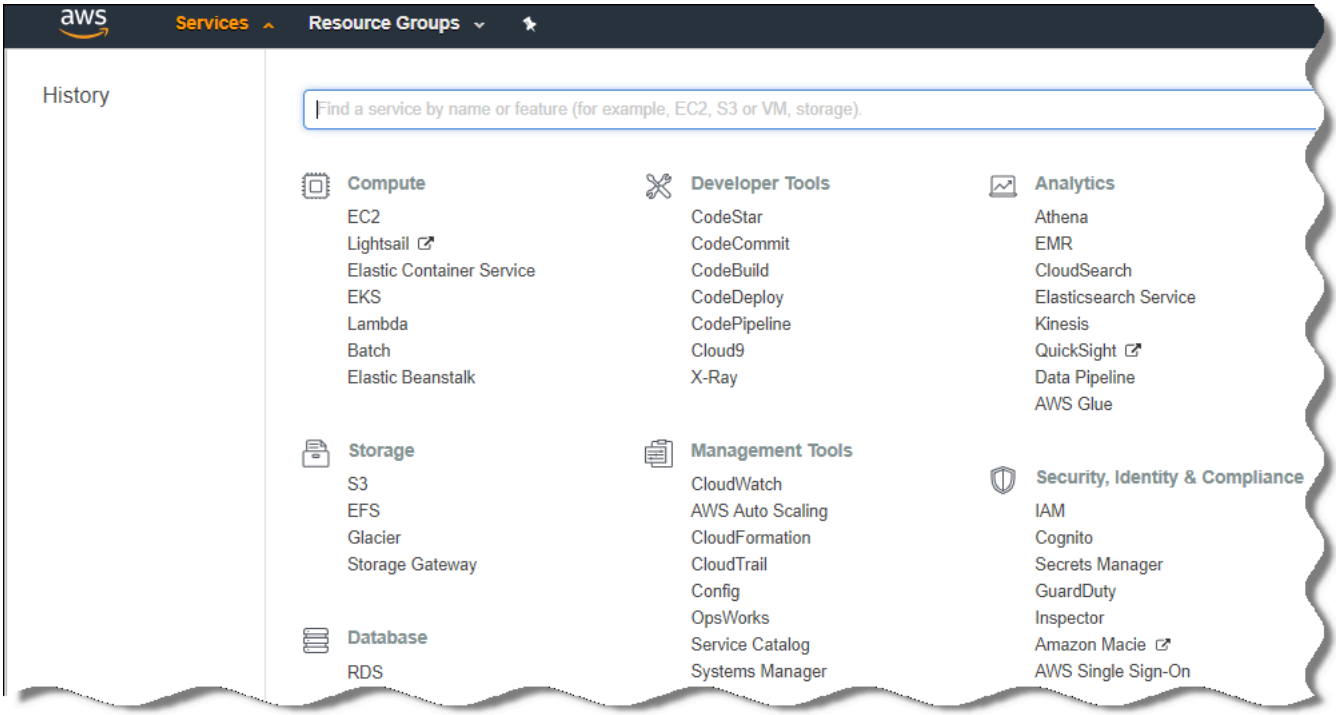
Amazon RDS 인스턴스용 옵션 그룹 생성

Amazon RDS 인스턴스는 옵션 그룹에 배치해야 합니다.

Amazon RDS 인스턴스용 옵션 그룹을 생성하려면 다음과 같이 하십시오:

1. AWS Management Console(https://console.aws.amazon.com)이 표시되어 있으며 계정이 로그인되어 있는지 확인합니다.

2. 메뉴 줄에서 **서비스**를 누릅니다.
   사용 가능한 서비스 목록이 나타납니다(아래 그림 참조).



AWS Management Console의 서비스 목록

3. 목록에서 **RDS**를 누릅니다.

4. 왼쪽 창에서 **옵션 그룹**을 누릅니다.

5. **그룹 만들기** 버튼을 누릅니다.

6. Amazon RDS 인스턴스 생성 단계에서 SQL Server를 선택한 경우 다음 설정으로 옵션 그룹을 생성합니다:

   - 엔진: SQLserver-ex
   - 주 엔진 버전: 12.00

   Amazon RDS 인스턴스 생성 단계에서 다른 SQL 데이터베이스를 선택한 경우에는 해당 엔진을 선택합니다.

작업이 생성되고 그룹 목록에 표시됩니다.

옵션 그룹을 생성한 후 Amazon RDS 인스턴스를 이 옵션 그룹에 배치합니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

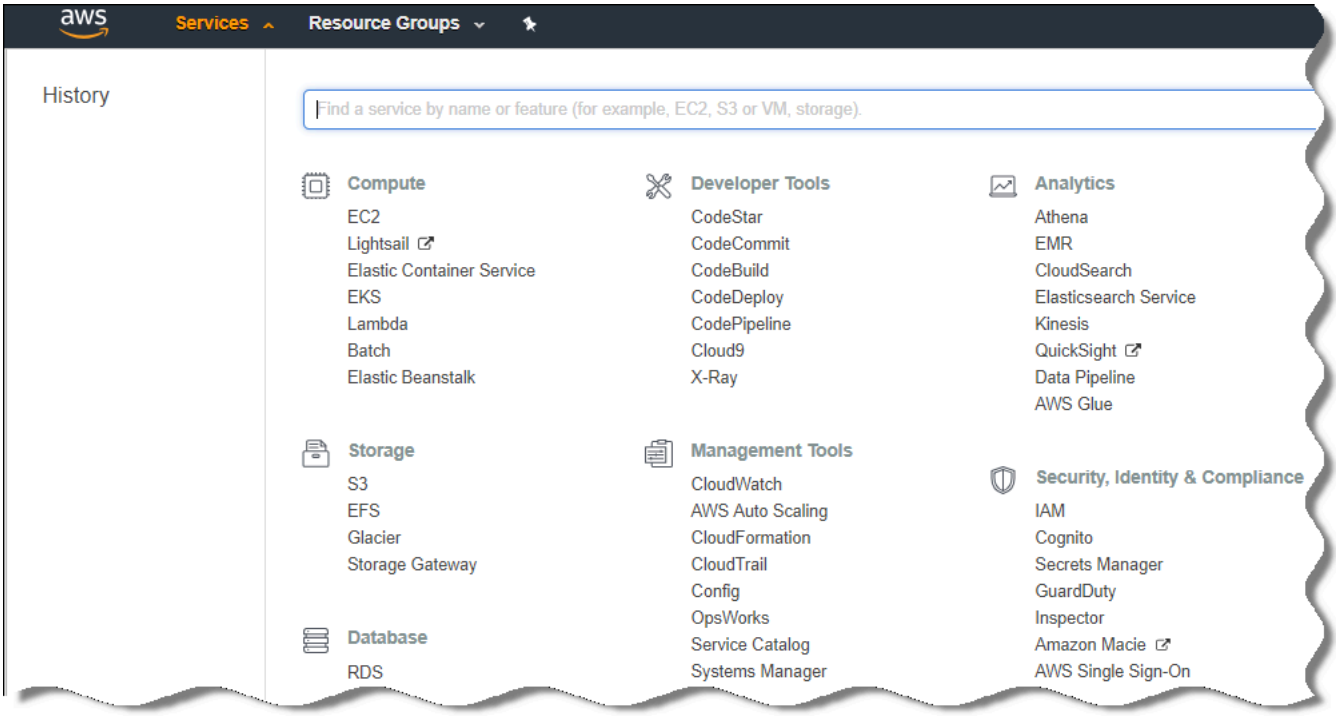
옵션 그룹 수정

Amazon RDS 인스턴스를 배치한 옵션 그룹의 기본 구성은 Kaspersky Security Center 데이터베이스를 사용하기에 충분하지 않습니다. 옵션을 옵션 그룹에 추가하고 데이터베이스 사용을 위한 새 IAM 역할을 생성해야 합니다.

옵션 그룹을 수정하고 새 IAM 역할을 생성하려면 다음과 같이 하십시오:

1. AWS Management Console(https://console.aws.amazon.com)이 표시되어 있으며 계정이 로그인되어 있는지 확인합니다.

2. 메뉴 줄에서 **서비스**를 누릅니다.
   사용 가능한 서비스 목록이 나타납니다(아래 그림 참조).



AWS Management Console의 서비스 목록

3. 목록에서 RDS를 선택합니다.

4. 왼쪽 창에서 **옵션 그룹**을 누릅니다.
   옵션 그룹 목록이 표시됩니다.

5. Amazon RDS 인스턴스를 배치한 옵션 그룹을 선택하고 **옵션 추가** 버튼을 누릅니다.
   옵션 추가 창이 열립니다.

6. IAM 역할 섹션에서 **새 역할 생성 /예** 옵션을 선택하고 새 IAM 역할의 이름을 입력합니다.
   기본 권한 세트를 사용하여 역할이 생성됩니다. 나중에 역할의 권한을 변경해야 합니다.

7. S3 버킷 섹션에서 다음 중 하나를 수행합니다:

   - 데이터 백업용 Amazon S3 버킷 인스턴스를 생성하지 않은 경우 **새 S3 버킷 생성** 링크를 선택하고 AWS 인터페이스를 사용하여 새 S3 버킷을 생성합니다.
   - 중앙 관리 서버 데이터 백업 작업용 Amazon S3 버킷 인스턴스를 이미 생성했다면 드롭다운 목록에서 S3 버킷을 선택합니다.

8. 페이지 아래쪽의 **옵션 추가** 버튼을 눌러 옵션 추가를 완료합니다.

옵션 그룹을 수정하고 RDS DB 사용을 위한 새 IAM 역할을 생성했습니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Amazon RDS DB 인스턴스용 IAM 역할의 권한 수정

옵션을 옵션 그룹에 추가한 후에는 Amazon RDS DB 인스턴스 사용을 위해 생성한 IAM 역할에 필요한 권한을 할당해야 합니다.

Amazon RDS DB 인스턴스 사용을 위해 생성한 IAM 역할에 필요한 권한을 할당하려면 다음과 같이 하십시오:

1. AWS Management Console(https://console.aws.amazon.com)이 표시되어 있으며 계정이 로그인되어 있는지 확인합니다.
2. 서비스 목록에서 **IAM**을 선택합니다.
   사용자 이름 목록과 도구를 사용할 수 있는 메뉴가 포함된 창이 열립니다.
3. 메뉴에서 **역할**을 선택합니다.
4. 작업 영역에 표시되는 IAM 역할 목록에서 옵션을 옵션 그룹에 추가할 때 생성한 역할을 선택합니다.
5. AWS 인터페이스를 사용하여 **sqlNativeBackup-<날짜>** 정책을 삭제합니다.
6. AWS 인터페이스를 사용하여 역할에 **AmazonS3FullAccess** 정책을 연결합니다.

IAM 역할에 Amazon RDS를 사용하는 데 필요한 권한이 할당됩니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

데이터베이스용 Amazon S3 버킷 준비

Amazon RDS(Relational Database System) 데이터베이스를 사용하려는 경우 데이터베이스의 일반 백업이 저장되는 Amazon S3(Simple Storage Service) 버킷 인스턴스를 생성해야 합니다. Amazon S3 및 S3 버킷에 대한 정보는 Amazon 도움말 페이지를 참조하십시오. Amazon S3 인스턴스 생성과 관련된 자세한 내용은 Amazon S3 도움말 페이지를 참조하십시오.

Amazon S3 버킷을 생성하려면 다음과 같이 하십시오:

1. AWS 관리 콘솔이 열려 있고 계정에 로그인되어 있는지 확인합니다.
2. AWS 서비스 목록에서 S3을 선택합니다.
3. 마법사의 지침에 따라 콘솔로 이동하여 버킷을 생성합니다.
4. 중앙 관리 서버가 있거나 중앙 관리 서버를 배치할 예정인 리전을 선택합니다.
5. 마법사가 완료되면 새 버킷이 버킷 목록에 나타나는지 확인합니다.

   새 S3 버킷이 생성되어 버킷 목록에 표시됩니다. 옵션을 옵션 그룹에 추가할 때 이 버킷을 지정해야 합니다. Kaspersky Security Center에서 *중앙 관리 서버 데이터 작업*의 백업을 생성할 때도 Kaspersky Security Center에 S3 버킷의 주소를 지정해야 합니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Amazon RDS로 데이터베이스 마이그레이션

실제 기기에서 Amazon RDS를 지원하는 Amazon S3 인스턴스로 Kaspersky Security Center 데이터베이스를 마이그레이션할 수 있습니다. 이렇게 하려면 RDS DB용 S3 버킷과 이 S3 버킷에 대한 AmazonS3FullAccess 권한이 있는 IAM 사용자 계정이 필요합니다.

데이터베이스 마이그레이션을 수행하려면 다음과 같이 하십시오:

1. RDS 인스턴스를 생성했는지 확인합니다(자세한 내용은 Amazon RDS 참조 페이지 참조).
2. 물리적 중앙 관리 서버(실제)에서 Kaspersky 백업 유틸리티를 실행하여 중앙 관리 서버 데이터를 백업합니다.
   파일 이름이 backup.zip인지 확인해야 합니다.
3. 중앙 관리 서버가 설치된 EC2 인스턴스에 backup.zip 파일을 복사합니다.

   중앙 관리 서버가 설치된 EC2 인스턴스에 디스크 공간이 충분한지 확인합니다. AWS 환경에서 데이터베이스 마이그레이션 프로세스를 처리할 수 있도록 인스턴스에 디스크 공간을 추가할 수 있습니다.

4. AWS 중앙 관리 서버에서 Kaspersky 백업 유틸리티를 대화식 모드로 다시 시작합니다.
   백업 및 복원 마법사가 시작됩니다.
5. **처리 방법 선택** 단계에서 **중앙 관리 서버 데이터 복원**를 선택하고 **다음**을 누릅니다.
6. **복원 설정** 단계에서 **백업 복사본 저장소 폴더** 옆의 **찾기** 버튼을 누릅니다.
7. **온라인 스토리지에 로그인** 창이 열리면 다음 필드에 내용을 입력하고 **확인**을 누릅니다:

   - **S3 버킷 이름**

     S3 버킷의 이름입니다.

- **백업 폴더**

  백업용 스토리지 폴더의 위치를 지정합니다.

- **액세스 키 ID**

  S3 버킷을 사용할 권한(AmazonS3FullAccess 권한)이 있는 IAM 사용자 소유의 AWS IAM 액세스 키 ID입니다.

- **비밀 키**

  S3 버킷을 사용할 권한(AmazonS3FullAccess 권한)이 있는 IAM 사용자 소유의 AWS IAM 비밀 키입니다.

8. **로컬 백업에서 마이그레이션** 옵션을 선택합니다. **찾기** 버튼이 사용 가능한 상태가 됩니다.

9. **찾기** 버튼을 클릭하여 backup.zip 파일을 복사한 AWS 중앙 관리 서버의 폴더를 선택합니다.

10. **다음**을 눌러 절차를 완료합니다.

    S3 버킷을 사용하여 RDS DB에 데이터가 복원됩니다. 나중에 AWS 환경에서 Kaspersky Security Center를 사용할 때 이 데이터베이스를 사용할 수 있습니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Microsoft Azure 클라우드 환경에서 작업

이 섹션에서는 Microsoft Azure에서 제공하는 클라우드 환경에서 Kaspersky Security Center를 배포하고 유지보수하는 과정을 설명하고, 이 클라우드 환경의 가상 컴퓨터에 보호 기능을 배포하는 방법을 자세히 설명합니다.

월 종량제 요금이 청구되는 SKU에서 배포된 Kaspersky Security Center에서는 취약점 및 패치 관리가 자동 활성화되며 모바일 기기 관리는 활성화할 수 없습니다.

Microsoft Azure에서 작업 수행 정보

Microsoft Azure 플랫폼을 사용하려면, 그리고 특히 Azure Marketplace에서 앱을 구매하고 가상 컴퓨터를 생성하려면 Azure 서브스크립션이 필요합니다. 중앙 관리 서버를 배포하기 전에 가상 컴퓨터에 애플리케이션을 설치하는 데 필요한 권한이 있는 Azure 애플리케이션 ID를 생성합니다.

Azure Marketplace에서 Kaspersky Security Center 이미지를 구매하는 경우 즉시 사용 가능한 Kaspersky Security Center 중앙 관리 서버와 함께 가상 컴퓨터를 배포할 수 있습니다. 가상 컴퓨터의 설정은 선택해야 하지만 애플리케이션 자체를 설치할 필요는 없습니다. 설치 후에는 관리 콘솔을 시작하고 중앙 관리 서버에 연결하여 Kaspersky Security Center 사용을 시작할 수 있습니다.

물리적인 서버보다 클라우드 서버를 더 쉽게 유지보수하고 서비스를 제공할 수 있는 등의 경우에는 Kaspersky Security Center 중앙 관리 서버가 배포되어 있는 Azure 가상 컴퓨터를 사용하여 온프레미스 기기를 보호할 수도 있습니다. 이러한 경우 온프레미스 기기에 설치된 중앙 관리 서버를 사용할 때와 같은 방법으로 중앙 관리 서버를 사용합니다. Azure API 도구를 사용하지 않으려는 경우 Azure 애플리케이션 ID가 필요하지 않습니다. 이 경우에는 Azure 서브스크립션만 있으면 됩니다.

서브스크립션, 애플리케이션 ID 및 암호 생성

Microsoft Azure 환경에서 Kaspersky Security Center를 사용하려면 Azure 서브스크립션, Azure 애플리케이션 ID 및 Azure 애플리케이션 암호가 필요합니다. 기존 서브스크립션이 이미 있으면 사용할 수 있습니다.

Azure 서브스크립션에서는 소유자에게 Microsoft Azure 플랫폼 관리 포털 및 Microsoft Azure 서비스 액세스 권한을 부여합니다. 소유자는 Microsoft Azure 플랫폼을 사용하여 Azure SQL, Azure Storage 등의 서비스를 관리할 수 있습니다.

Microsoft Azure 서브스크립션을 생성하려면,

https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription으로 가서 그곳의 지침을 따릅니다.

서브스크립션 생성과 관련된 자세한 내용은 Microsoft 웹사이트에서 제공됩니다. 제공되는 서브스크립션 ID는 나중에 애플리케이션 ID 및 암호와 함께 Kaspersky Security Center에 입력합니다.

Azure 애플리케이션 ID 및 암호를 생성하여 저장하려면 다음과 같이 하십시오:

1. https://portal.azure.com으로 이동하여 로그인되어 있는지 확인합니다.
2. 참조 페이지의 지침에 따라 애플리케이션 ID를 생성합니다.
3. 애플리케이션 설정의 **키** 섹션으로 이동합니다.
4. **키** 섹션의 **설명** 및 **만료** 필드에 내용을 입력하고 **값** 필드는 비워 둡니다.
5. **저장**을 누릅니다.

   저장을 누르면 **값** 필드에 긴 문자 시퀀스가 자동으로 입력됩니다. 이 시퀀스는 Azure 애플리케이션의 암호입니다(예: yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). 입력한 설명이 표시됩니다.
6. 나중에 애플리케이션 ID와 암호를 Kaspersky Security Center에 입력할 수 있도록 암호를 복사한 다음 저장합니다.

   암호는 생성 시에만 복사할 수 있습니다. 그 후에는 암호가 더 이상 표시되지 않으며 복원할 수 없습니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Azure 애플리케이션 ID에 역할 할당

기기 발견을 사용하여 가상 컴퓨터만 탐지하려는 경우 Azure 애플리케이션 ID에 Reader 역할이 있어야 합니다. 가상 컴퓨터를 탐지하고 가상 컴퓨터에 보호 기능도 배포하려는 경우에는 Azure 애플리케이션 ID에 Virtual Machine 참가자 역할이 있어야 합니다.

Microsoft 웹사이트의 지침에 따라 Azure 애플리케이션 ID에 역할을 할당하십시오.

Microsoft Azure에 중앙 관리 서버 배포 및 데이터베이스 선택

Microsoft Azure 환경에 중앙 관리 서버를 배포하려면 다음과 같이 하십시오:

1. 계정을 사용하여 Microsoft Azure에 로그인합니다.
2. Azure Portal로 이동합니다.
3. 왼쪽 창에서 녹색 더하기 기호를 누릅니다.
4. 메뉴의 검색 필드에 "Kaspersky Hybrid Cloud Security"를 입력합니다.

   Kaspersky Hybrid Cloud Security는 Kaspersky Security Center와 인스턴스 보호를 위한 보안 제품 2개가 조합된 제품입니다: Kaspersky Endpoint Security for Linux 및 Kaspersky Security for Windows Server.
5. 결과 목록에서 Kaspersky Hybrid Cloud Security 또는 Kaspersky Hybrid Cloud Security(BYOL)를 선택합니다.

   화면 오른쪽에 정보 패널이 나타납니다.
6. 정보를 확인한 후 정보 패널 끝에 있는 생성 버튼을 누릅니다.
7. 필요한 모든 필드에 내용을 입력합니다. 도구 설명을 사용하면 정보를 확인하고 지원을 받을 수 있습니다.
8. 크기 선택 시에는 별표가 있는 옵션 3개 중 하나를 선택합니다.

   대부분의 경우에는 8GB(기가바이트) RAM을 선택하면 충분합니다. 하지만 Azure에서는 언제든지 가상 컴퓨터의 RAM과 기타 리소스의 크기를 늘릴 수 있습니다.
9. 데이터베이스를 선택할 때는 계획에 따라 다음 중 하나를 선택합니다:

   - 로컬 - 중앙 관리 서버를 배포하려는 동일한 가상 컴퓨터에 있는 데이터 데이터베이스를 사용합니다. Kaspersky Security Center에서는 SQL Server Express 데이터베이스가 제공됩니다. SQL Server Express로도 요구를 충분히 충족할 수 있으면 이 옵션을 선택합니다.
   - 새로 만들기 - Azure 환경에서 새 RDS DB를 생성합니다. SQL Server Express 이외의 DBMS를 사용하려는 경우 이 옵션을 선택합니다. 데이터는 클라우드 환경으로 전송되어 저장되며 추가 비용은 발생하지 않습니다.
   - 기존 - 기존 데이터베이스 서버를 사용합니다. 이 경우에는 서버 위치를 지정해야 합니다. 이 서버가 Azure 환경 외부에 있으면 데이터가 인터넷을 통해 전송되며, 그러면 추가 비용이 발생할 수 있습니다.
10. 서브스크립션 ID를 입력할 때는 이전에 생성한 서브스크립션을 사용합니다.

배포 후에는 RDP를 사용하여 중앙 관리 서버에 연결할 수 있습니다. 관리 콘솔을 통해 중앙 관리 서버를 사용할 수 있습니다.

Azure SQL 작업

이 섹션에서는 Kaspersky Security Center용 Microsoft Azure 데이터베이스를 준비하고, Azure 스토리지 계정을 준비하고, 기존 데이터베이스를 Azure SQL로 마이그레이션하기 위해 수행해야 하는 작업을 설명합니다.

SQL 데이터베이스는 Microsoft Azure의 범용 관계형 데이터베이스 관리형 서비스입니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Azure 스토리지 계정 생성

Azure SQL 데이터베이스와 배포 스크립트를 사용할 수 있도록 Microsoft Azure에 스토리지 계정을 생성해야 합니다.

스토리지 계정을 생성하려면 다음과 같이 하십시오:

1. Azure Portal에 로그인합니다.
2. 왼쪽 창에서 **스토리지 계정**을 선택하여 **스토리지 계정** 창으로 이동합니다.
3. **스토리지 계정** 창에서 **추가** 버튼을 눌러 **스토리지 계정 만들기** 창으로 이동합니다.
4. 필요한 모든 필드에 정보를 입력하여 스토리지 계정을 만듭니다:
   - 위치: 중앙 관리 서버와 같은 위치여야 함.
   - 기타 필드: 기본값을 그대로 둘 수 있습니다.

   도구 설명을 사용하면 각 필드에 대한 정보를 확인할 수 있습니다.
   스토리지 계정이 생성되면 스토리지 계정 목록이 표시됩니다.
5. 스토리지 계정 목록에서 새로 만든 계정의 이름을 클릭하여 이 계정에 대한 정보를 확인합니다.
6. 이 스토리지 계정의 계정 이름, 리소스 그룹 및 접근 허용 키를 알고 있어야 합니다. Kaspersky Security Center를 사용하려면 이 정보가 필요합니다.

Azure 웹사이트에서 도움말을 참조할 수 있습니다.

스토리지 계정이 이미 있는 경우에는 해당 계정을 통해 Kaspersky Security Center를 사용할 수 있습니다.

Azure SQL 데이터베이스 및 SQL Server 생성

Azure 환경에는 SQL 데이터베이스와 SQL Server가 필요합니다.

Azure SQL 데이터베이스와 SQL Server를 생성하려면 다음과 같이 하십시오:

1. Azure 웹사이트의 지침을 따르십시오.

   Microsoft Azure에서 새 서버를 생성하라는 메시지가 표시되면 새 서버를 생성할 수 있습니다. Azure SQL Server가 이미 있는 경우에는 새 서버를 생성하지 않고 해당 서버를 Kaspersky Security Center용으로 사용할 수 있습니다.

2. SQL 데이터베이스 및 SQL Server를 생성한 후에는 해당 리소스 이름과 리소스 그룹을 확인해야 합니다:

   a. https://portal.azure.com으로 이동하여 로그인되어 있는지 확인합니다.

   b. 왼쪽 패널에서 **SQL 데이터베이스**를 하나 선택합니다.

   c. 데이터베이스 목록에서 데이터베이스의 이름을 누릅니다.
   속성 창이 열립니다.

   d. 데이터베이스의 이름이 리소스 이름입니다. 리소스 그룹 이름은 속성 창의 **개요** 섹션에 표시됩니다.

데이터베이스를 Azure SQL로 마이그레이션하려면 데이터베이스의 리소스 이름과 리소스 그룹이 필요합니다.

Azure SQL로 데이터베이스 마이그레이션

Azure 환경에 중앙 관리 서버를 배포한 후에는 실제 기기에서 Azure SQL로 Kaspersky Security Center 데이터베이스를 마이그레이션할 수 있습니다. 이렇게 하려면 Azure SQL 데이터베이스용 Azure 스토리지 계정이 필요합니다. 또한 중앙 관리 서버에 Microsoft SQL Server Data-Tier Application Framework(DacFx) 및 SQLSysCLRTypes도 있어야 합니다.

데이터베이스 마이그레이션을 수행하려면 다음과 같이 하십시오:

1. Azure 스토리지 계정을 생성했는지 확인합니다.

2. 중앙 관리 서버에 SQLSysCLRTypes 및 DacFx가 있는지 확인합니다.
   공식 Microsoft 웹 사이트에서 Microsoft SQL Server Data-Tier Application Framework(17.0.1 DacFx) 및 SQLSysCLRTypes(SQL Server 버전에 해당하는 버전 선택)를 다운로드할 수 있습니다.

3. 물리적 중앙 관리 서버(실제)에서 Kaspersky 백업 유틸리티를 실행하여 **Azure 형식으로 마이그레이션** 옵션을 활성화한 상태로 중앙 관리 서버 데이터를 백업합니다.

4. 백업 파일을 Azure 중앙 관리 서버에 복사합니다.

   > 중앙 관리 서버가 설치된 Azure 가상 컴퓨터에 디스크 공간이 충분한지 확인합니다. Azure 환경에서 데이터베이스 마이그레이션 프로세스를 처리할 수 있도록 가상 컴퓨터에 디스크 공간을 추가할 수 있습니다.

5. Microsoft Azure 환경에 있는 중앙 관리 서버에서 Kaspersky 백업 유틸리티를 대화식 모드로 다시 시작합니다.
   백업 및 복원 마법사가 시작됩니다.

6. **처리 방법 선택** 단계에서 **중앙 관리 서버 데이터 복원**를 선택하고 **다음**을 누릅니다.

7. **복원 설정** 단계에서 **백업 복사본 저장소 폴더** 옆의 **찾기** 버튼을 누릅니다.

8. **온라인 스토리지에 로그인** 창이 열리면 다음 필드에 내용을 입력하고 **확인**을 누릅니다:

   - **Azure 스토리지 계정 이름**

     > Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

- **백업 폴더**

  백업용 스토리지 폴더의 위치를 지정합니다.

- **Azure 서브스크립션 ID**

  Azure Portal에서 생성한 서브스크립션입니다.

- **Azure 애플리케이션 암호**

  애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

  암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

- **Azure 스토리지 액세스 키**

  스토리지 계정 속성의 접근 허용 키 섹션에서 제공됩니다. 원하는 어떤 키든 사용할 수 있습니다(key1 또는 key2).

- **Azure SQL 서버 이름**

  Azure SQL Server의 속성에서 제공됩니다.

- **Azure SQL 서버 리소스 그룹**

  Azure SQL Server의 속성에서 제공됩니다.

- **Azure 애플리케이션 ID**

  Azure Portal에서 생성한 애플리케이션 ID입니다.

  검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

9. **로컬 백업에서 마이그레이션** 옵션을 선택합니다.

   찾기 버튼이 사용 가능한 상태가 됩니다.

10. **찾기** 버튼을 눌러 백업 파일을 복사한 Azure 중앙 관리 서버의 폴더를 선택합니다.

11. **다음**을 눌러 절차를 완료합니다.

Azure 스토리지를 사용하여 Azure SQL 데이터베이스에 데이터가 복원됩니다. 나중에 Azure 환경에서 Kaspersky Security Center를 사용할 때 이 데이터베이스를 사용할 수 있습니다.

The addresses of web pages cited in this document are correct as of the Kaspersky Security Center release date.

Google 클라우드에서 작업

이 섹션에서는 Google에서 제공하는 클라우드 환경에서 Kaspersky Security Center 작업에 대한 정보를 제공합니다.

클라이언트 이메일, 프로젝트 ID, 개인 키 생성

Google API를 사용하여 Google 클라우드 플랫폼에서 Kaspersky Security Center로 작업할 수 있습니다. Google 계정이 필요합니다. 자세한 내용은 https://cloud.google.com 에서 Google 설명서를 참조하십시오.

Kaspersky Security Center를 생성하고 다음 자격 증명을 제공해야 합니다.

- **클라이언트 이메일**

  클라이언트 이메일은 Google Cloud에 프로젝트를 등록하는 데 사용한 이메일 주소입니다.

- **프로젝트 ID**

  프로젝트 ID는 Google Cloud에 프로젝트를 등록할 때 받은 ID입니다.

- **개인 키**

  개인 키는 Google Cloud에 프로젝트를 등록할 때 개인 키로 받은 문자열입니다. 실수가 생기지 않도록 이 문자열을 복사 후 붙여 넣으십시오.

Google Cloud SQL for MySQL 인스턴스로 작업

Google Cloud에서 데이터베이스를 만들고 이 데이터베이스를 Kaspersky Security Center에 사용할 수 있습니다.

Kaspersky Security Center는 MySQL 5.7 및 5.6과 호환됩니다. 다른 버전의 MySQL은 테스트되지 않았습니다.

MySQL 데이터베이스를 생성하고 구성하는 방법:

사용 중인 브라우저에서 https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen으로 이동하여 제공된 지침을 따르십시오.

MySQL 데이터베이스 구성 시 다음 플래그를 사용하십시오.

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300

- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

Kaspersky Security Center 연동을 위한 클라우드 환경에서의 클라이언트 기기 준비

중앙 관리 서버, 네트워크 에이전트 및 Kaspersky 보안 애플리케이션을 설치하려는 기기는 다음 조건을 충족해야 합니다:

- 보안 그룹의 구성은 다음 포트를 중앙 관리 서버에서 이용 가능하도록 해야 합니다(배포에 필요한 최소한의 포트):
  - 8060 HTTP - 중앙 관리 서버에서 보호된 인스턴스로 네트워크 에이전트 설치 패키지와 보안 제품 설치 패키지를 전송하는 용도
  - 8061 HTTPS - 중앙 관리 서버에서 보호된 인스턴스로 네트워크 에이전트 설치 패키지와 보안 제품 설치 패키지를 전송하는 용도
  - 13000 TCP - 보호된 인스턴스와 보조 중앙 관리 서버에서 SSL을 사용하는 기본 중앙 관리 서버로 전송하는 용도
  - 13000 UDP - 중앙 관리 서버로 인스턴스의 종료에 대한 정보를 전송하는 용도
  - 14000 TCP - 보호된 인스턴스와 보조 중앙 관리 서버에서 SSL을 사용하지 않는 기본 중앙 관리 서버로 전송하는 용도
  - 13291 - 관리 콘솔을 중앙 관리 서버에 연결할 때 사용하는 용도
  - 40080 - 배포 스크립트 작동에 필요

  AWS Management Console이나 Azure Portal에서 보안 그룹을 구성할 수 있습니다. 기본 구성이 아닌 다른 구성에서 Kaspersky Security Center를 사용하려는 경우 기술 자료 문서를 참조하십시오. 기본 구성이 아닌 구성의 예로는 관리 콘솔을 중앙 관리 서버 기기에 설치하는 대신 워크스테이션에 설치하는 경우나 KSN 프록시 서버를 사용하는 경우 등이 있습니다.
- 15000 UDP 포트는 해당 클라이언트 기기에서 이용 가능합니다(중앙 관리 서버와의 통신 요청을 수신할 때 필요).
- AWS 클라우드 환경:
  - AWS API를 사용할 계획이라면 IAM 역할은 이 애플리케이션이 해당 인스턴스에 설치될 때 설정됩니다.
  - 각 Amazon EC2 인스턴스에 시스템 관리자 에이전트(SSM 에이전트)가 설치되어 있으며 실행 중이어야 합니다.

- Kaspersky Security Center는 SSM 에이전트를 통해 매번 관리자에게 확인을 요청하지 않고 기기 및 기기 그룹에 애플리케이션을 자동으로 설치할 수 있습니다.

- 2016년 11월 이후의 AMI에서 배포되었으며 Windows 운영 체제를 실행 중인 인스턴스의 경우 SSM 에이전트가 설치되어 있으며 실행 중입니다. 기타 모든 기기에는 SSM 에이전트를 수동으로 설치해야 합니다. Windows 및 Linux 운영 체제를 실행 중인 기기에 SSM 에이전트를 설치하는 방법에 대한 자세한 내용은 AWS 도움말 페이지를 참조하십시오.

- Microsoft Azure 클라우드 환경:

  - 각 Azure 가상 컴퓨터에 Azure VM 에이전트가 설치되어 있으며 실행 중이어야 합니다.

    기본적으로는 Azure VM 에이전트와 함께 새 가상 컴퓨터가 생성되므로 가상 컴퓨터를 수동으로 설치하거나 활성화하지 않아도 됩니다. Windows 기기 및 Linux 기기의 Azure VM 에이전트 관련 세부 정보는 Microsoft 도움말 페이지를 참조하십시오.

  - Azure 애플리케이션 ID에는 다음과 같은 역할이 있습니다:

    - Reader(검색을 사용하여 가상 컴퓨터를 발견하는 데 필요함)

    - Virtual Machine 참가자(가상 컴퓨터에 보호 기능을 배포하는 데 필요함)

    - SQL Server Contributor(Microsoft Azure 환경에서 SQL 데이터베이스를 사용하는 데 필요함)

    이러한 모든 작업을 수행하려는 경우 Azure 애플리케이션 ID에 3개 역할을 모두 할당합니다.

클라우드 환경 구성에 필요한 설치 패키지 생성

다음 프로그램의 설치 패키지와 관리 플러그인이 있다면 Kaspersky Security Center에서 클라우드 환경 구성 마법사를 사용할 수 있습니다:

- Kaspersky Endpoint Security for Linux

- Kaspersky Endpoint Security for Windows

  > Kaspersky Endpoint Security for Windows 를 클라우드 환경에 배포하는 것은 Kaspersky Endpoint Security 12.0 for Windows가 출시된 이후에 사용할 수 있습니다.

- Kaspersky Security for Windows Server

이러한 설치 패키지는 보호하려는 인스턴스 또는 가상 머신에 애플리케이션을 설치하는 데 필요합니다. 이러한 설치 패키지가 없는 경우에는 만들어야 합니다. 그렇지 않으면 클라우드 환경 마법사가 작동하지 않습니다.

설치 패키지를 만들려면 다음을 수행합니다:

1. Kaspersky 웹 사이트에서 애플리케이션 및 플러그인 최신 버전을 다운로드합니다.

   - Kaspersky Security for Windows Server의 설치 프로그램과 관리 플러그인.

   - Kaspersky Endpoint Security for Linux의 설치 프로그램, 관리 플러그인, Kaspersky Endpoint Security for Linux를 통한 원격 설치용 파일.

2. 중앙 관리 서버가 설치될 인스턴스 또는 가상 머신에 모든 파일을 저장합니다.

3. 모든 패키지에서 파일을 추출합니다.

4. Kaspersky Security Center를 시작합니다.

5. 콘솔 트리에서 **고급** → **원격 설치** → **설치 패키지**로 이동한 다음 **설치 패키지 만들기**를 클릭합니다.

6. **Kaspersky 설치 패키지 만들기**를 선택합니다.

7. 패키지의 이름과 애플리케이션 설치 프로그램의 경로 <folder>\<file name>.kud를 지정하고 **다음**을 클릭합니다.

8. 최종 사용자 라이센스 계약서를 읽고 조건에 동의함을 확인하는 확인란을 선택한 후 **다음**을 클릭합니다.

설치 패키지가 중앙 관리 서버에 업로드되고 설치 패키지 목록에서 사용할 수 있습니다.

클라우드 환경 구성은 설치 패키지를 생성하고 중앙 관리 서버에 관리 플러그인을 설치하는 즉시 사용할 수 있습니다.

클라우드 환경 구성

클라우드 환경 구성 마법사를 사용하여 Kaspersky Security Center를 구성하려면 다음이 있어야 합니다:

- 클라우드 환경에 대한 특정 자격 증명:
  - 클라우드 세그먼트 검색 권한이 부여된 IAM 역할 또는 클라우드 세그먼트 검색 권한이 부여된 IAM 사용자 계정(Amazon Web Services 작업용)
  - Azure 애플리케이션 ID, 암호, 서브스크립션(Microsoft Azure 작업용)
  - Google 클라이언트 이메일, 프로젝트 ID, 비공개 키(Google Cloud 작업용)
- 설치 패키지:
  - Windows용 네트워크 에이전트
  - Linux용 네트워크 에이전트
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux용 웹 플러그인
- 다음 중 하나를 수행합니다:
  - Kaspersky Endpoint Security for Windows용 설치 패키지 및 웹 플러그인(권장)
  - Kaspersky Security for Windows Server용 설치 패키지 및 웹 플러그인

실제 클라이언트 기기의 보호만 관리하려는 등의 이유로 클라우드 환경 기능을 사용하지 않으려면, 클라우드 환경 구성 마법사를 종료하고 표준 중앙 관리 서버 빠른 시작 마법사를 수동으로 실행할 수 있습니다.

바로 사용할 수 있는 이미지에서 Kaspersky Security Center를 배포한다면 관리 콘솔을 통해 중앙 관리 서버에 처음 연결할 때 클라우드 환경 구성 작업이 자동 시작됩니다. 언제든지 수동으로도 클라우드 환경 구성 마법사를 시작할 수 있습니다.

클라우드 환경 구성 마법사를 수동으로 시작하려면:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 노드의 마우스 오른쪽 메뉴에서 **모든 작업 → 클라우드 환경 구성**을 선택합니다.

평균 작업 세션은 약 15분입니다.

클라우드 환경 구성 마법사 정보

클라우드 환경 구성 마법사에서는 클라우드 환경에서 작업하는 구체적인 방식을 고려하여 Kaspersky Security Center를 구성할 수 있습니다.

마법사는 다음 개체를 만듭니다:

- 기본 설정이 포함된 네트워크 에이전트 정책
- Kaspersky Endpoint Security for Linux용 정책
- Kaspersky Security for Windows Server용 정책
- 인스턴스용 관리 그룹 및 이 관리 그룹으로 인스턴스를 자동 이동하는 규칙
- 중앙 관리 서버 데이터 백업 작업
- Linux 및 Windows를 실행하는 기기에 보호 기능을 설치하기 위한 작업
- 각각의 관리 중인 기기에 대한 작업:
  - 빠른 악성 코드 검사
  - 업데이트 다운로드

BYOL 라이센스 옵션을 선택했다면, 클라우드 환경 구성 시 키 파일이나 활성화 코드를 사용하여 Kaspersky Security Center를 활성화하고 라이센스 스토리지에 키 파일 또는 활성화 코드를 저장합니다.

1단계. 애플리케이션 활성화 방법 선택

바로 사용할 수있는 AMI(AWS Marketplace) 중 하나 또는 사용량 기반 월별 청구 SKU(Azure Marketplace)에 가입되었다면 이 단계가 표시되지 않습니다. 이때, 마법사는 즉시 다음 단계로 진행합니다. 바로 사용할 수 있는 Google Cloud용 AMI는 구매할 수 없습니다.

Kaspersky Security Center에 대해 BYOL 라이센스 옵션을 선택했다면, 마법사가 애플리케이션 활성화 방법을 선택하라는 메시지를 표시합니다.

Kaspersky Security for Virtualization 또는 Kaspersky Hybrid Cloud Security용 활성화코드(또는 키 파일)를 사용하여 애플리케이션을 활성화합니다.

다음과 같은 방법으로 애플리케이션을 활성화할 수 있습니다:

- 활성화코드 입력.

  온라인 활성화가 시작됩니다. 이 프로세스에는 지정된 활성화코드 및 라이센스 키 파일의 검증 과정이 포함됩니다.

- 라이센스 키 파일 지정.

  애플리케이션은 키 파일을 확인하여 올바른 정보가 포함되어 있으면 키를 활성화하거나 다른 키 파일을 지정하라는 메시지를 표시합니다.

Kaspersky Security Center는 라이센스 키를 라이센스 저장소에 추가하고 관리 중인 기기에 자동으로 키 배포로 표시합니다.

Microsoft Windows의 표준 원격 데스크톱 연결 또는 유사한 애플리케이션을 사용하여 인스턴스에 연결하는 경우에는 원격 연결 속성에서 연결에 사용되는 실제 기기의 드라이브를 지정해야 합니다. 이렇게 하면 인스턴스에서 실제 기기의 파일에 접근할 수 있으며 키 파일을 선택하고 지정할 수 있습니다.

> 유료 AMI 또는 사용량 기반 월별 청구 SKU에서 배포된 Kaspersky Security Center를 사용할 때는 라이센스 저장소에 키 파일 및 활성화코드를 추가할 수 없습니다.

2단계. 클라우드 환경 선택

Kaspersky Security Center를 배포할 클라우드 환경을 AWS, Azure 또는 Google 클라우드 중에서 선택합니다.

3단계. 클라우드 환경에서 인증

AWS

AWS를 선택했다면 필요한 권한을 가진 IAM 역할을 지정하거나 AWS IAM 액세스 키를 가진 Kaspersky Security Center를 제공합니다. 클라우드 세그먼트 검색은 IAM 역할 또는 AWS IAM 액세스 키 없이는 불가능합니다.

추가적인 클라우드 세그먼트 검색에 사용할 연결에 대해 다음과 같은 설정을 지정합니다:

- **연결 이름**

  > 연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.
  >
  > 이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.
  >
  > 둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

- **AWS IAM 역할 사용**

  > 이미 AWS 서비스를 사용하기 위해 중앙 관리 서버에 대한 IAM 역할을 만들었다면 이 옵션을 선택합니다.

- **AWS IAM 사용자 계정 사용**

  필요한 권한을 가진 IAM 사용자 계정이 있고 키 ID와 비밀 키를 입력할 수 있다면 이 옵션을 선택합니다.

  - **액세스 키 ID**

    IAM 액세스 키 ID는 영숫자 문자 시퀀스입니다. IAM 사용자 계정을 만들 때 키 ID가 제공됩니다.

    IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

  - **비밀 키**

    IAM 사용자 계정을 만들 때 액세스 키 ID와 함께 제공된 비밀 키입니다.

    비밀 키의 문자는 별표로 표시됩니다. 비밀 키 입력을 시작하면 **표시** 버튼이 나타납니다. 이 버튼을 필요한 시간 동안 누르고 있으면 입력한 문자가 표시됩니다.

    IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

이 연결은 애플리케이션 설정에 저장됩니다. 클라우드 환경 구성에서는 단일 AWS IAM 액세스 키만 생성할 수 있습니다. 그런 다음 더 많은 연결을 지정하여 다른 클라우드 세그먼트를 관리할 수 있습니다.

Kaspersky Security Center를 통해 인스턴스에 애플리케이션을 설치하려면 IAM 역할(또는 입력하는 키와 연관된 계정을 가진 IAM 사용자)에 필요한 모든 권한이 있는지 확인해야 합니다.

Azure

Azure를 선택했다면 추가적인 클라우드 세그먼트 검색에 사용할 연결에 대해 다음과 같은 설정을 지정합니다:

- **연결 이름**

  연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.

  이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.

  둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

- **Azure 애플리케이션 ID**

  Azure Portal에서 생성한 애플리케이션 ID입니다.

  검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

- **Azure 서브스크립션 ID**

  Azure Portal에서 생성한 서브스크립션입니다.

- **Azure 애플리케이션 암호**

  애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

- **Azure 스토리지 계정 이름**

  Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

- **Azure 스토리지 액세스 키**

  Kaspersky Security Center에서 사용하기 위해 Azure 스토리지 계정을 생성할 때 제공된 암호(키)입니다.

  키는 "Azure 스토리지 계정 개요" 섹션의 "키" 하위 섹션에서 제공됩니다.

이 연결은 애플리케이션 설정에 저장됩니다.

Google Cloud

Google 클라우드를 선택한 경우 추가적인 클라우드 세그먼트 검색에 사용할 연결에 대해 다음과 같은 설정을 지정하십시오.

- **연결 이름**

  연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.

  이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.

  둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

- **클라이언트 이메일**

  클라이언트 이메일은 Google Cloud에 프로젝트를 등록하는 데 사용한 이메일 주소입니다.

- **프로젝트 ID**

  프로젝트 ID는 Google Cloud에 프로젝트를 등록할 때 받은 ID입니다.

- **개인 키**

  개인 키는 Google Cloud에 프로젝트를 등록할 때 개인 키로 받은 문자열입니다. 실수가 생기지 않도록 이 문자열을 복사 후 붙여 넣으십시오.

이 연결은 애플리케이션 설정에 저장됩니다.

4단계. 클라우드와의 동기화 구성 및 추가 작업 선택

이 단계에서는 클라우드 세그먼트 검색이 시작되며 특별한 인스턴스용 관리 그룹이 만들어집니다. 검색 중에 발견된 인스턴스는 이 그룹에 배치됩니다. 클라우드 세그먼트 검색 스케줄이 구성됩니다(기본적으로 5분마다).

클라우드와 동기화 자동 이동 규칙도 만들어집니다. 이 단계 후에는 클라우드 네트워크를 검사할 때마다 발견된 가상 기기가 **관리 중인 기기\클라우드** 그룹 내의 해당 하위 그룹으로 이동됩니다.

클라우드 세그먼트와 동기화 페이지에서 다음 설정을 구성할 수 있습니다:

- **클라우드 세그먼트와 관리 그룹 구조 동기화**

  이 옵션을 활성화하면 **클라우드** 그룹이 **관리 중인 기기** 그룹 내에 자동으로 만들어지고 클라우드 기기 발견이 시작됩니다. 각 클라우드 네트워크 검사 중에 탐지된 인스턴스 및 가상 컴퓨터는 클라우드 그룹에 배치됩니다. 이 그룹 내의 관리 하위 그룹 구조는 클라우드 세그먼트의 구조와 일치합니다. AWS에서는 구조에 가용 영역 및 배치 그룹이 표시되지 않으며 Azure에서는 구조에 서브넷이 표시되지 않습니다. 클라우드 환경의 인스턴스로 식별되지 않은 기기는 **미할당 기기** 그룹에 포함됩니다. 이 그룹 구조를 통해 그룹 설치 작업을 사용하여 인스턴스에 안티 바이러스 애플리케이션을 설치할 수 있으며 그룹별로 다른 정책을 설정할 수 있습니다.

  이 옵션을 비활성화하면 **클라우드** 그룹도 생성되며 클라우드 기기 발견도 시작됩니다. 하지만 클라우드 세그먼트 구조와 일치하는 하위 그룹이 그룹 내에 생성되지는 않습니다. 탐지된 모든 인스턴스는 **클라우드** 관리 그룹에 있으므로 목록 하나에 표시됩니다. Kaspersky Security Center 작업이 동기화를 요구한다면 **클라우드와 동기화** 규칙의 속성을 수정하고 그 규칙을 강제로 적용할 수 있습니다. 이 규칙을 적용하면 클라우드 그룹의 하위 그룹 구조가 클라우드 세그먼트의 구조와 일치하도록 변경됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **보호 배포**

  이 옵션을 선택하면 마법사가 인스턴스에 보안 제품을 설치하는 작업을 생성합니다. 마법사가 완료되면 클라우드 세그먼트의 기기에서 보호 배포 마법사가 자동 시작되며 ,해당 기기에 네트워크 에이전트 및 보안 제품을 설치할 수 있습니다.

  Kaspersky Security Center는 기본 도구를 사용하여 배포를 수행할 수 있습니다. EC2 인스턴스나 Azure 가상 컴퓨터에 애플리케이션을 설치할 권한이 없다면 **원격 설치** 작업을 수동으로 구성하고 필요한 권한이 있는 계정을 지정할 수 있습니다. 이 경우 AWS API 또는 Azure를 사용하여 검색된 기기에 대해서는 원격 설치 작업이 작동하지 않습니다. 이 작업은 Active Directory 검색, Windows 도메인 검색 또는 IP 범위 검색을 사용하여 검색된 기기에 대해서만 작동합니다.

  이 옵션을 선택하지 않으면 보호 배포 마법사가 시작되지 않으며 인스턴스에 보안 제품을 설치하는 작업이 생성되지 않습니다. 이 두 작업은 나중에 수동으로 수행할 수 있습니다.

Google 클라우드의 경우 Kaspersky Security Center 기본 도구로만 배포를 수행할 수 있습니다. Google 클라우드를 선택한 경우 **보호 배포** 옵션을 사용할 수 없습니다.

5단계. 클라우드 환경에서 Kaspersky Security Network 구성

Kaspersky Security Center 작동 관련 정보를 Kaspersky Security Network 기술 자료로 전달하기 위한 설정을 지정합니다. 다음 옵션 중 하나를 선택합니다:

- **Kaspersky Security Network 사용에 동의합니다.**

  클라이언트 기기에 설치된 Kaspersky Security Center 및 관리 중인 애플리케이션은 작업 세부 정보를 Kaspersky Security Network로 자동 전송합니다. Kaspersky Security Network에 참여하면 바이러스 및 기타 위협 관련 정보가 포함된 데이터베이스를 보다 빠르게 업데이트할 수 있으므로 새로운 보안 위협에 더욱 신속하게 대응할 수 있습니다.

- **Kaspersky Security Network 사용에 동의하지 않습니다.**

  Kaspersky Security Center 및 관리 중인 애플리케이션은 Kaspersky Security Network로 정보를 제공하지 않습니다.

  이 옵션을 선택하면 Kaspersky Security Network 사용이 비활성화됩니다.

Kaspersky Security Network에 참여하는 것이 좋습니다.

6단계. 클라우드 환경에서 이메일 알림 구성

가상 클라이언트 기기에서 Kaspersky 애플리케이션 작동 시 등록된 이벤트에 대한 알림 전달을 구성할 수 있습니다. 이러한 설정은 애플리케이션 정책에 대한 기본 설정으로 사용됩니다.

Kaspersky 애플리케이션에서 발생하는 이벤트에 대한 알림 전달을 구성하려면 다음 설정을 사용합니다:

- **받는 사람(이메일 주소)**

  애플리케이션에서 알림을 보낼 사용자의 이메일 주소입니다. 주소를 하나 이상 입력할 수 있습니다. 주소를 한 개 이상 입력하고자 할 경우 각 주소를 세미콜론으로 구분하십시오.

- **SMTP 서버**

  조직의 메일 서버 주소 또는 주소들입니다.

  주소를 한 개 이상 입력하고자 할 경우 각 주소를 세미콜론으로 구분하십시오. 다음 값을 사용할 수 있습니다:

  - IPv4 또는 IPv6 주소
  - 기기의 Windows 네트워크 이름(NetBIOS 이름)
  - SMTP 서버의 DNS 이름

- **SMTP 서버 포트**

  SMTP 서버의 통신 포트 번호입니다. 여러 SMTP 서버를 사용한다면 지정된 통신 포트를 통해 이들에 대한 연결이 설정됩니다. 기본 포트 번호는 25입니다.

- **ESMTP 인증 사용**

  ESMTP 인증을 지원하도록 설정합니다. **사용자 이름** 및 **암호** 필드의 확인란을 선택하면 ESMTP 인증 설정을 지정할 수 있습니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

테스트 메시지 전송 버튼을 눌러 새 이메일 알림 설정을 테스트할 수 있습니다. **받는 사람(이메일 주소)** 필드에 지정된 주소에서 테스트 메시지가 정상 수신된 경우에는 설정이 올바르게 구성된 것입니다.

7단계. 클라우드 환경 보호를 위한 초기 구성 생성

이 단계에서 Kaspersky Security Center는 정책과 작업을 자동으로 만듭니다. **초기 보호 구성** 창에는 애플리케이션이 만든 정책과 작업 목록이 표시됩니다.

AWS 클라우드 환경에서 RDS DB를 사용하는 경우에는 중앙 관리 서버 백업 작업을 생성할 때 Kaspersky Security Center에 IAM 액세스 키 쌍을 제공해야 합니다. 이 경우 다음 필드에 내용을 입력합니다:

- **S3 버킷 이름**

  백업용으로 생성한 S3 버킷의 이름입니다.

- **액세스 키 ID**

  S3 버킷 스토리지 인스턴스 사용을 위해 IAM 사용자 계정을 만들 때 키 ID(영숫자 문자 시퀀스)가 제공됩니다.

  S3 버킷에서 RDS DB를 선택한 경우 이 필드를 사용할 수 있습니다.

- **비밀 키**

  IAM 사용자 계정을 만들 때 액세스 키 ID와 함께 제공된 비밀 키입니다.

  비밀 키의 문자는 별표로 표시됩니다. 비밀 키 입력을 시작하면 **표시** 버튼이 나타납니다. 이 버튼을 필요한 시간 동안 누르고 있으면 입력한 문자가 표시됩니다.

  IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

Azure 클라우드 환경에서 Azure SQL 데이터베이스를 사용하는 경우에는 중앙 관리 서버 백업 작업을 생성할 때 Kaspersky Security Center에 Azure SQL Server 관련 정보를 제공해야 합니다. 이 경우 다음 필드에 내용을 입력합니다:

- **Azure 스토리지 계정 이름**

  Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

- **Azure 서브스크립션 ID**

  Azure Portal에서 생성한 서브스크립션입니다.

- **Azure 애플리케이션 암호**

  애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

  암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

- **Azure 애플리케이션 ID**

  Azure Portal에서 생성한 애플리케이션 ID입니다.

검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

- **Azure SQL 서버 이름**

  Azure SQL Server 속성에서 제공되는 이름 및 리소스 그룹입니다.

- **Azure SQL 서버 리소스 그룹**

  Azure SQL Server 속성에서 제공되는 이름 및 리소스 그룹입니다.

- **Azure 스토리지 액세스 키**

  스토리지 계정 속성의 접근 허용 키 섹션에서 제공됩니다. 원하는 어떤 키든 사용할 수 있습니다(key1 또는 key2).

중앙 관리 서버를 Google 클라우드에 배포하는 경우 백업 복사본을 저장할 폴더를 선택해야 합니다. 로컬 기기의 폴더 또는 가상 컴퓨터 인스턴스의 폴더를 선택하십시오.

최소 보호 구성에 필요한 정책과 작업을 모두 만들고 나면 **다음** 버튼을 사용할 수 있게 됩니다.

작업을 실행하려는 기기가 중앙 관리 서버에 표시되지 않는 경우에는 기기가 표시되어야 작업이 시작됩니다. 새 EC2 인스턴스 또는 새 Azure 가상 컴퓨터를 만드는 경우 해당 인스턴스나 컴퓨터가 중앙 관리 서버에 표시될 때까지 다소 시간이 걸릴 수 있습니다. 새로 만든 모든 기기에 네트워크 에이전트 및 보안 제품을 최대한 빨리 설치하려는 경우 **원격으로 애플리케이션 설치** 작업에 대해 **누락된 작업 실행** 옵션이 활성화되어 있는지 확인하십시오. 이렇게 하지 않으면 스케줄에 따라 작업을 시작할 때까지 새로 만든 인스턴스/가상 컴퓨터에 네트워크 에이전트 및 보안 제품이 설치되지 않습니다.

8단계. 설치 중에 운영 체제를 다시 시작해야 할 때의 작업 선택 (클라우드 환경의 경우)

이전에 **보호 배포**를 선택한 경우에는 대상 기기의 운영 체제를 다시 시작해야 할 때 수행할 작업을 선택해야 합니다. **보호 배포** 옵션을 선택하지 않은 경우에는 이 단계를 건너뜁니다.

애플리케이션 설치 중에 기기 운영 체제를 다시 시작해야 하는 경우 인스턴스를 다시 시작할지 여부를 선택합니다:

- **기기 다시 시작 안 함**

  이 옵션을 선택하면 보안 제품 설치 후에 기기가 다시 시작되지 않습니다.

- **기기 다시 시작**

  이 옵션을 선택하면 보안 제품 설치 후에 기기가 다시 시작됩니다.

다시 시작 전에 인스턴스에서 잠긴 세션의 모든 애플리케이션을 강제로 종료하려면 **애플리케이션 강제 종료** 확인란을 선택합니다. 이 확인란의 선택을 취소하는 경우에는 잠긴 인스턴스에서 실행 중인 모든 애플리케이션을 수동으로 종료해야 합니다.

9단계. 중앙 관리 서버에서 업데이트 받기

이 단계에서는 중앙 관리 서버의 정상적인 작동에 필요한 업데이트 다운로드 진행률을 확인할 수 있습니다. 다운로드가 완료될 때까지 기다리지 않고 **다음** 버튼을 누르면 마법사의 마지막 페이지로 진행할 수 있습니다.

마법사가 끝납니다.

구성 확인

클라우드 환경에서 작업할 수 있도록 Kaspersky Security Center 15.1이 올바르게 구성되었는지 확인하려면 다음과 같이 하십시오:

1. Kaspersky Security Center를 시작하여 관리 콘솔을 통해 중앙 관리 서버에 연결할 수 있는지 확인합니다.
2. 콘솔 트리에서 **관리 중인 기기\클라우드**를 선택합니다.
3. **관리 중인 기기\클라우드** 그룹에서 하위 그룹을 볼 때는 **기기** 탭에 해당 하위 그룹의 모든 기기가 표시되는지 확인하십시오.
   기기가 표시되지 않으면 수동으로 해당 클라우드 세그먼트를 검색하여 기기를 찾을 수 있습니다.
4. **정책** 탭에 다음 애플리케이션에 대한 활성 정책이 있는지 확인하십시오.
   - Kaspersky Security Center 네트워크 에이전트
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   정책이 목록에 없으면 수동으로 생성할 수 있습니다.
5. **작업** 탭에 다음 작업이 나열되는지 확인합니다.
   - **중앙 관리 서버 데이터 백업**
   - **Windows Server용 업데이트 작업**
   - **중앙 관리 서버 점검**
   - **중앙 관리 서버 저장소에 업데이트 다운로드**
   - **취약점 및 필요한 업데이트 검색**
   - **Windows용 보호 제품 설치**
   - **Linux용 보호 제품 설치**
   - **Windows Server용 빠른 검사 작업**

- **빠른 검사**
- **Linux용 업데이트 설치**

정책이 목록에 없으면 수동으로 생성할 수 있습니다.

Kaspersky Security Center 15.1은 클라우드 환경에서 작동하도록 적절하게 구성되었습니다.

클라우드 기기 그룹

클라우드 기기를 그룹으로 결합하여 관리할 수 있습니다. Kaspersky Security Center 초기 구성 단계에서는 **관리 중인 기기\클라우드** 관리 그룹이 기본적으로 생성되며 검색 중에 탐지된 클라우드 기기가 이 그룹에 배치됩니다.

동기화를 구성할 때 **클라우드 세그먼트와 관리 그룹 구조 동기화** 옵션을 선택한 경우 이 관리 그룹의 하위 그룹 구조는 클라우드 세그먼트의 구조와 동일합니다. (하지만 AWS에서는 구조에 가용 영역 및 배치 그룹이 표시되지 않으며 Microsoft Azure에서는 구조에 서브넷이 표시되지 않습니다.) 검색 중에 탐지되는 그룹 내의 빈 하위 그룹은 자동으로 삭제됩니다.

모든 기기나 특정 기기를 결합하여 관리 그룹을 수동으로 만들 수도 있습니다.

기본적으로 **관리 중인 기기\클라우드** 그룹은 **관리 중인 기기** 그룹에서 정책과 작업을 상속합니다. 해당하는 정책과 작업의 설정 속성에서 **편집 허용** 확인란을 선택한 경우 설정을 변경할 수 있습니다.

네트워크 세그먼트 검색

중앙 관리 서버는 AWS API, Azure API 또는 Google API 도구를 사용해 클라우드 세그먼트를 정기적으로 검색하여 네트워크의 구조 및 해당 네트워크의 기기에 대한 정보를 받습니다. Kaspersky Security Center는 이 정보를 사용하여 **미할당 기기** 및 **관리 중인 기기** 폴더의 컨텐츠를 업데이트합니다. 기기가 관리 그룹으로 자동으로 이동하도록 구성된 경우에는 발견된 기기가 관리 그룹에 포함됩니다.

중앙 관리 서버에서 클라우드 세그먼트를 검색할 수 있게 하려면, AWS의 경우 IAM 역할 또는 IAM 사용자 계정, Azure의 경우 애플리케이션 ID 및 암호 또는 Google 클라이언트 이메일, Google 프로젝트 ID 및 개인 키와 함께 제공되는 권한이 있어야 합니다.

연결을 추가하고 삭제할 수 있으며 각 클라우드 세그먼트에 대한 검색 일정을 설정할 수 있습니다.

클라우드 세그먼트 검색에 대한 연결 추가

이용 가능한 연결 목록에 클라우드 세그먼트 검색에 대한 연결을 추가하려면 아래와 같이 진행합니다:

1. 콘솔 트리에서 **기기 발견** → **클라우드** 노드를 선택합니다.
2. 이 창의 작업 영역에서 **검색 구성**을 누릅니다.
   클라우드 세그먼트 검색에 대해 사용할 수 있는 연결 목록이 포함된 속성 창이 열립니다.
3. **추가** 버튼을 누릅니다.
   연결 창이 열립니다.

4. 추가적인 클라우드 세그먼트 검색에 사용할 연결에 대해 클라우드 환경의 이름을 지정합니다.

클라우드 환경

EC2 인스턴스(또는 가상 컴퓨터)가 있는 환경은 AWS(Amazon Web Services), Microsoft Azure 또는 Google Cloud일 수 있습니다.

AWS를 선택한 경우 다음 설정을 지정하십시오.

- **연결 이름**

  연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.

  이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.

  둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

- **AWS IAM 역할 사용**

  이미 AWS 서비스를 사용하기 위해 중앙 관리 서버에 대한 IAM 역할을 만들었다면 이 옵션을 선택합니다.

- **AWS IAM 사용자 계정 사용**

  필요한 권한을 가진 IAM 사용자 계정이 있고 키 ID와 비밀 키를 입력할 수 있다면 이 옵션을 선택합니다.

  - **액세스 키 ID**

    IAM 액세스 키 ID는 영숫자 문자 시퀀스입니다. IAM 사용자 계정을 만들 때 키 ID가 제공됩니다.

    IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

  - **비밀 키**

    IAM 사용자 계정을 만들 때 액세스 키 ID와 함께 제공된 비밀 키입니다.

    비밀 키의 문자는 별표로 표시됩니다. 비밀 키 입력을 시작하면 **표시** 버튼이 나타납니다. 이 버튼을 필요한 시간 동안 누르고 있으면 입력한 문자가 표시됩니다.

    IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

클라우드 환경 구성 마법사에서는 AWS IAM 액세스 키를 하나만 지정할 수 있습니다. 그런 다음 더 많은 연결을 지정하여 다른 클라우드 세그먼트를 관리할 수 있습니다.

Azure를 선택한 경우 다음 설정을 지정하십시오.

- **연결 이름**

  연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.

  이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.

둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

- **Azure 애플리케이션 ID**

  Azure Portal에서 생성한 애플리케이션 ID입니다.

  검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

- **Azure 서브스크립션 ID**

  Azure Portal에서 생성한 서브스크립션입니다.

- **Azure 애플리케이션 암호**

  애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

  암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

- **Azure 스토리지 계정 이름**

  Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

- **Azure 스토리지 액세스 키**

  Kaspersky Security Center에서 사용하기 위해 Azure 스토리지 계정을 생성할 때 제공된 암호(키)입니다.

  키는 "Azure 스토리지 계정 개요" 섹션의 "키" 하위 섹션에서 제공됩니다.

Google 클라우드를 선택한 경우 다음 설정을 지정하십시오.

- **연결 이름**

  연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.

  이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.

  둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

- **클라이언트 이메일**

  클라이언트 이메일은 Google Cloud에 프로젝트를 등록하는 데 사용한 이메일 주소입니다.

- **프로젝트 ID**

  프로젝트 ID는 Google Cloud에 프로젝트를 등록할 때 받은 ID입니다.

- **개인 키**

  개인 키는 Google Cloud에 프로젝트를 등록할 때 개인 키로 받은 문자열입니다. 실수가 생기지 않도록 이 문자열을 복사 후 붙여 넣으십시오.

5. 원하는 경우 **검색 스케줄 설정**을 선택하고 기본 설정을 변경합니다.

   이 연결은 애플리케이션 설정에 저장됩니다.

새 클라우드 세그먼트를 처음으로 검색하고 나면 이 세그먼트에 해당하는 하위 그룹이 **관리 중인 기기\클라우드** 관리 그룹에 표시됩니다.

잘못된 자격증명을 지정하면 클라우드 세그먼트 검색 중에 인스턴스가 검색되지 않으며 **관리 중인 기기\클라우드** 관리 그룹에 새 하위 그룹이 표시되지 않습니다.

클라우드 세그먼트 검색에 대한 연결 삭제

특정 클라우드 세그먼트를 더 이상 검색할 필요가 없는 경우 그 세그먼트에 해당하는 연결을 사용 가능한 연결 목록에서 삭제할 수 있습니다. 클라우드 세그먼트 검색 권한이 다른 키를 가진 다른 AWS IAM 사용자에게로 이전된 경우 등에도 연결을 삭제할 수 있습니다.

연결을 삭제하려면 다음과 같이 진행합니다:

1. 콘솔 트리에서 **기기 발견** → **클라우드** 노드를 선택합니다.
2. 창의 작업 영역에서 **검색 구성**을 선택합니다.

   클라우드 세그먼트 검색에 대해 사용할 수 있는 연결 목록이 포함된 창이 열립니다.
3. 삭제할 연결을 선택하고 창 오른쪽의 **삭제** 버튼을 누릅니다.
4. 열리는 창에서 **확인** 버튼을 눌러 사용자의 선택을 다시 확인합니다.

사용 가능한 연결 목록에서 연결을 삭제하는 경우 관련 세그먼트를 내에 있는 기기가 해당 관리 그룹에서 자동으로 삭제됩니다.

검색 스케줄 구성

클라우드 세그먼트 검색은 스케줄에 따라 수행됩니다. 검색 빈도를 설정할 수 있습니다.

클라우드 환경 구성 설정에서 검색 빈도를 5분으로 자동 설정합니다. 언제든지 이 값을 변경하여 다른 스케줄을 설정할 수 있습니다. 그러나 검색 실행 빈도는 5분보다 더 짧게 구성하지 않는 것이 좋습니다. 빈도를 너무 짧게 구성하면 API 작업에서 오류가 발생할 수 있기 때문입니다.

클라우드 세그먼트 검색 스케줄을 구성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 발견 → 클라우드** 노드를 선택합니다.
2. 작업 영역에서 **검색 구성**을 누릅니다.
   클라우드 속성 창이 열립니다.
3. 목록에서 원하는 연결을 선택하고 **속성** 버튼을 누릅니다.
   연결 속성 창이 열립니다.
4. 속성 창에서 **검색 스케줄 설정** 링크를 누릅니다.
   스케줄 창이 열립니다.
5. 다음 설정을 정의합니다:

- **시작 스케줄**
  검색 스케줄 옵션:
  - **매 N일마다**

    검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.
    기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **매 N분마다**

    검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.
    기본적으로 검색은 현재 시스템 시간부터 5분마다 실행됩니다.

  - **요일별**

    검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
    기본적으로 검색은 매주 금요일 오후 6:00:00에 실행됩니다.

  - **매달 선택한 주간의 지정한 날짜**

    검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
    기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

- **누락된 작업 실행**

  중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.
  이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.
  이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.

기본적으로 이 옵션은 켜져 있습니다.

6. **확인**을 눌러 변경을 저장합니다.

검색 스케줄이 구성되어 저장됩니다.

클라우드 환경의 기기에 애플리케이션 설치

클라우드 환경의 기기에 Kaspersky Security for Windows Server(Windows용 기기) 및 Kaspersky Endpoint Security for Linux(Linux용 기기)와 같은 Kaspersky 애플리케이션을 설치할 수 있습니다.

보호 애플리케이션을 설치하려는 클라이언트 기기는 클라우드 환경의 Kaspersky Security Center 작동 요구 사항을 충족해야 합니다. AWS 인스턴스, Microsoft Azure 가상 컴퓨터 또는 Google 가상 컴퓨터 인스턴스에 애플리케이션을 설치하려면 유효한 라이센스가 있어야 합니다.

Kaspersky Security Center 15.1은 다음 시나리오를 지원합니다:

- API를 통해 클라이언트 기기를 검색하고 설치를 수행합니다. AWS 및 Azure 클라우드 환경의 경우 이 시나리오가 지원됩니다.
- Active Directory 검색, Windows 도메인 검색 또는 IP 범위 검색을 통해 클라이언트 기기를 검색하며 Kaspersky Security Center를 통해 설치를 수행합니다.
- Google API를 통해 클라이언트 기기를 검색하고 Kaspersky Security Center를 통해 설치를 수행합니다. Google 클라우드의 경우 이 시나리오만 지원됩니다.

그 외의 방법으로는 애플리케이션을 설치할 수 없습니다.

가상 기기에 애플리케이션을 설치하려면 설치 패키지를 사용합니다.

AWS API 또는 Azure API를 사용해 인스턴스에서 애플리케이션 원격 설치를 위한 작업을 만들려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **작업** 폴더를 선택합니다.
2. **새 작업** 버튼을 누릅니다.
   새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.
3. **작업 유형 선택** 페이지에서 **원격으로 애플리케이션 설치**를 작업 유형으로 선택합니다.
4. **기기 선택** 페이지의 **관리 중인 기기\클라우드** 그룹에서 관련 기기를 선택합니다.
5. 애플리케이션을 설치하려는 기기에 네트워크 에이전트가 아직 설치되어 있지 않으면 **작업을 실행할 계정 선택** 페이지에서 **계정 필요(네트워크 에이전트는 사용되지 않음)**를 선택하고 창 오른쪽에서 **추가** 버튼을 누릅니다. 나타나는 메뉴에서 다음 중 하나를 선택합니다:
   - **클라우드 계정**

     AWS의 인스턴스에 애플리케이션을 설치하려는 경우 필요한 권한이 있는 AWS IAM 액세스 키는 있지만 IAM 역할이 없으면 이 옵션을 선택합니다. Azure 환경의 기기에 애플리케이션을 설치하려는 경우에도 이 옵션을 선택합니다.

     창이 열리면 관련 기기에 애플리케이션을 설치할 권한을 부여하는 자격증명을 Kaspersky Security Center에 제공합니다.

클라우드 환경(AWS 또는 Azure)을 선택합니다.

계정 이름 필드에 이러한 자격증명의 이름을 입력합니다. 이 이름은 작업을 실행할 계정 목록에 표시됩니다.

AWS를 선택한 경우 지정한 기기에 애플리케이션을 설치할 권한이 있는 IAM 사용자 계정의 자격증명을 **액세스 키 ID** 및 **비밀 키** 필드에 입력합니다.

Azure를 선택한 경우 지정한 기기에 애플리케이션을 설치할 권한이 있는 Azure 계정의 자격증명을 **Azure 서브스크립션 ID** 및 **Azure 애플리케이션 암호** 필드에 입력합니다.

잘못된 자격증명을 지정하면 원격 설치 작업이 예정된 기기에서 해당 작업이 종료될 때 오류가 표시됩니다.

- **계정**

  Windows를 실행 중인 인스턴스의 경우, AWS 또는 Azure API 도구를 사용하여 애플리케이션을 설치하지 않으려면 이 옵션을 선택합니다. 이 경우 클라우드 세그먼트에 있는 기기가 필요한 조건을 충족하는지 확인하십시오. Kaspersky Security Center는 AWS API 또는 Azure API을 사용하지 않고 자체적으로 애플리케이션을 설치합니다.

  잘못된 데이터를 지정하면 원격 설치 작업이 예정된 기기에서 해당 작업이 종료될 때 오류가 표시됩니다.

- **IAM 역할**

  AWS 환경의 인스턴스에 애플리케이션을 설치하려는 경우 필요한 권한을 가진 IAM 역할이 있으면 이 옵션을 선택합니다.

  필요한 권한을 가진 IAM 역할이 없는데 이 옵션을 선택하면 원격 설치 작업이 예정된 기기에서 해당 작업이 종료될 때 오류가 표시됩니다.

- **SSH 인증서**

  Linux를 실행 중인 인스턴스에서는, AWS API 또는 Azure API 도구를 사용하여 애플리케이션을 설치하지 않으려면 이 옵션을 선택합니다. 이 경우 클라우드 세그먼트에 있는 기기가 필요한 조건을 충족하는지 확인하십시오. Kaspersky Security Center는 AWS API 또는 Azure API을 사용하지 않고 자체적으로 애플리케이션을 설치합니다.

  SSH 인증서의 개인 키를 지정하려면, ssh-keygen 유틸리티를 사용하여 생성할 수 있습니다. Kaspersky Security Center는 개인 키의 PEM 형식을 지원하지만 ssh-keygen 유틸리티는 기본적으로 OPENSSH 형식으로 SSH 키를 생성합니다. Kaspersky Security Center에서는 OPENSSH 형식을 지원하지 않습니다. 지원되는 PEM 형식으로 개인 키를 생성하려면 ssh-keygen 명령에 `-m PEM` 옵션을 추가합니다. 예:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< 사용자 이메일 >"
  ```

각각의 새 키에 대해 **추가** 버튼을 눌러 여러 자격증명을 제공할 수 있습니다. 클라우드 세그먼트마다 필요한 자격증명이 다른 경우에는 모든 세그먼트에 대해 자격증명을 입력합니다.

마법사가 완료되면 **작업** 폴더의 작업 영역에 있는 작업 목록에 애플리케이션 원격 설치를 위한 작업이 표시됩니다.

Microsoft Azure에서 가상 컴퓨터에 보안 제품을 원격으로 설치하면 이 가상 컴퓨터에 설치된 사용자 지정 스크립트 확장 프로그램이 삭제될 수 있습니다.

클라우드 기기 속성 보기

클라우드 기기의 속성을 보려면 다음과 같이 하십시오.

1. 콘솔 트리의 **기기 발견** → **클라우드** 노드에서 관련 인스턴스가 있는 그룹에 해당하는 하위 노드를 선택합니다.
   관련 가상 기기가 있는 그룹을 모르는 경우 검색 기능을 사용합니다.

   a. **관리 중인 기기** → **클라우드** 노드의 이름을 마우스 오른쪽 버튼으로 누른 다음 마우스 오른쪽 메뉴에서 **검색**을 선택합니다.

   b. 창이 열리면 검색을 수행합니다.
      설정된 기준을 충족하는 기기가 있으면 해당 이름과 세부 정보가 창 아래쪽에 표시됩니다.

2. 관련 노드의 이름을 마우스 오른쪽 버튼으로 누릅니다. 책 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
   열리는 창에 개체 속성이 표시됩니다.
   시스템 정보 → 일반 시스템 정보 섹션에는 클라우드 환경의 기기와 관련된 속성이 포함되어 있습니다.

   - **API를 사용해 발견된 기기**(**AWS**, **Azure** 또는 **Google Cloud**; API 도구를 사용해 기기를 발견할 수 없는 경우 **아니요** 값이 표시됩니다).
   - **클라우드 리전**.
   - **Cloud VPC**(AWS 및 Google Cloud 기기만 해당).
   - **클라우드 가용 영역**(AWS 및 Google Cloud 기기만 해당).
   - **클라우드 서브넷**.
   - **클라우드 배치 그룹**(이 단위는 인스턴스가 배치 그룹에 속하는 경우에만 표시되고 그렇지 않으면 표시되지 않음).

이 정보를 .csv 또는 .txt 파일로 내보내려면 **파일로 내보내기** 버튼을 누릅니다.

클라우드와 동기화

클라우드 환경 구성 동작을 수행하는 동안 클라우드와 동기화 규칙이 자동으로 만들어집니다. 이 규칙을 사용하면 각 검색에서 탐지된 인스턴스를 중앙 집중식 관리에서 사용할 수 있도록 **미할당 기기** 그룹에서 **관리 중인 기기\클라우드** 그룹으로 자동 이동할 수 있습니다. 이 규칙은 기본적으로 만들어진 후에 활성화됩니다. 언제든지 규칙을 비활성하거나 수정하거나 강제로 적용할 수 있습니다.

클라우드와 동기화 규칙 속성을 편집하거나 규칙을 강제로 적용하려면 아래와 같이 진행합니다.

1. 콘솔 트리에서 **기기 발견** 노드의 이름을 마우스 오른쪽 버튼으로 누릅니다.
2. 책 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. **속성** 창이 열리면 **섹션** 창에서 **기기 이동**을 선택합니다.

4. 작업 영역 내 기기 이동 규칙 목록에서 **클라우드와 동기화** 규칙을 선택하고 창 아래쪽의 **속성** 버튼을 누릅니다. 규칙 속성 창이 열립니다.

5. 필요한 경우 **클라우드 세그먼트** 설정 그룹에서 다음 설정을 지정합니다:

- **기기가 클라우드 세그먼트에 있습니다**

  선택한 클라우드 세그먼트에 있는 기기에만 이 규칙이 적용됩니다. 그렇지 않은 경우에는 검색된 모든 기기에 규칙이 적용됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **자식 개체 포함**

  선택한 세그먼트 및 모든 중첩 클라우드 하위 섹션에 있는 모든 기기에 규칙이 적용됩니다. 그렇지 않은 경우에는 루트 세그먼트에 있는 기기에만 규칙이 적용됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **중첩된 개체에서 관련 하위 그룹으로 기기 이동**

  이 옵션을 활성화하면 중첩된 개체의 기기가 개체 구조에 해당하는 하위 그룹으로 이동됩니다.

  이 옵션을 비활성화하면 중첩된 개체의 기기가 클라우드 하위 그룹 루트로 자동으로 이동되며 추가 분기는 설정되지 않습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  - **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성**

    이 옵션을 활성화하는 경우 **관리 중인 기기\클라우드** 그룹 구조에 기기가 포함된 섹션과 일치하는 하위 그룹이 없으면 Kaspersky Security Center에서 해당 하위 그룹을 생성합니다. 예를 들어 기기 발견 중에 새 서브넷이 발견되면 **관리 중인 기기\클라우드** 그룹 아래에 같은 이름의 새 그룹이 생성됩니다.

    이 옵션을 비활성화하면 Kaspersky Security Center에서 새 하위 그룹을 생성하지 않습니다. 예를 들어 네트워크 검색 중에 새 서브넷이 발견되어도 **관리 중인 기기\클라우드** 그룹 아래에 같은 이름의 새 그룹이 생성되지 않으며 서브넷의 기기는 **관리 중인 기기\클라우드** 그룹으로 이동됩니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **클라우드 세그먼트에서 일치하는 항목이 없는 하위 그룹 삭제**

    이 옵션을 활성화하면 애플리케이션이 기존 클라우드 개체와 일치하지 않는 모든 하위 그룹을 클라우드 그룹에서 삭제합니다.

    이 옵션을 비활성화하면 기존 클라우드 개체와 일치하지 않는 하위 그룹이 유지됩니다.

    기본적으로 이 옵션은 켜져 있습니다.

클라우드 환경 구성을 실행할 때 **클라우드와 동기화** 옵션을 활성화하면 해당 클라우드와 동기화 규칙에는 **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성**과 **클라우드 세그먼트에 일치하는 항목이 없는 하위 그룹은 삭제** 확인란이 선택됩니다.

클라우드와 동기화 옵션을 활성화하지 않은 경우 이러한 옵션이 비활성화(해제)된 상태로 클라우드와 동기화 규칙이 생성됩니다. Kaspersky Security Center를 사용하는 작업이 **관리 중인 기기\클라우드** 하위 그룹의 하위 그룹 구조가 클라우드 세그먼트의 구조와 일치해야 한다면, 규칙 속성에서 **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성**와 **클라우드 세그먼트에 일치하는 항목이 없는 하위 그룹은 삭제** 옵션을 선택하고 그 규칙을 강제로 적용합니다.

6. **API를 사용해 발견된 기기** 드롭다운 목록에서 다음 값 중 하나를 선택하십시오:
   - **AWS**. AWS API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 AWS 클라우드 환경에 있습니다.
   - **Azure**. Azure API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Azure 클라우드 환경에 있습니다.
   - **Google Cloud.** Google API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Google Cloud 환경에 있습니다.
   - **아니요**. AWS, Azure, Google API로 기기를 찾을 수 없으므로, 기기가 클라우드 환경 밖에 있거나 클라우드 환경 내에 있지만 어떠한 이유로 인해 API를 사용해 찾을 수 없습니다.
7. **값 없음**. 이 조건이 적용되지 않습니다. 필요한 경우 다른 섹션에서 기타 규칙 속성을 설정합니다.
8. 필요한 경우 창 아래에 있는 **강제 실행** 버튼을 눌러 규칙을 적용합니다.

   규칙 실행 마법사가 시작됩니다. 마법사의 지침을 따릅니다. 마법사가 완료되면 규칙이 실행되고 **관리 중인 기기\클라우드** 하위 그룹 내의 하위 그룹 구조가 클라우드 세그먼트 구조와 일치하게 됩니다.
9. **확인** 버튼을 누릅니다.

속성이 설정되어 저장됩니다.

클라우드와 동기화 규칙을 비활성하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **기기 발견** 노드의 이름을 마우스 오른쪽 버튼으로 누릅니다.
2. 책 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. **속성** 창이 열리면 **섹션** 창에서 **기기 이동**을 선택합니다.
4. 작업 영역의 기기 이동 규칙 목록에서 **클라우드와 동기화** 옵션을 비활성화(해제)하고 **확인**을 누릅니다.

그러면 규칙이 비활성화되어 더 이상 적용되지 않습니다.

Yandex.Cloud에 Kaspersky Security Center 배포

Yandex.Cloud에 Kaspersky Security Center를 배포할 수 있습니다. PPU(Pay-per-use) 모드만 사용할 수 있습니다. 클라우드 데이터베이스는 지원되지 않습니다.

Yandex.Cloud에서는 보안 제품에 대해 다음 배포 방법을 사용할 수 있습니다.

- Kaspersky Security Center의 기본 수단, 즉 *원격 설치* 작업을 통해(보안 프로그램 배포는 중앙 관리 서버와 보호할 가상 머신이 동일한 네트워크 세그먼트에 있는 경우에만 가능)
- 배포 스크립트를 통해

Yandex.Cloud에 Kaspersky Security Center를 배포하려면 Yandex.Cloud에 서비스 계정이 있어야 합니다. 이 계정에 marketplace.meteringAgent 권한을 부여하고 이 계정을 가상 머신과 연결해야 합니다(자세한 내용은 https://cloud.yandex.com/en 참조).

부록

이 섹션에서는 Kaspersky Security Center 사용과 관련한 다음과 같은 참조 정보 및 추가 사항을 제공합니다.

고급 옵션

이 섹션에서는 기기의 애플리케이션에 대한 중앙 집중식 관리 기능을 확대할 수 있도록 설계된 Kaspersky Security Center의 여러 가지 추가 옵션에 대해 설명합니다.

Kaspersky Security Center 작동 자동화. klakaut utility

klakaut 유틸리티를 사용하여 Kaspersky Security Center 작동을 자동화할 수 있습니다. klakaut 유틸리티 및 해당 유틸리티의 도움말 시스템은 Kaspersky Security Center 설치 폴더에 있습니다.

사용자 지정 도구

Kaspersky Security Center에서는 마우스 오른쪽 메뉴의 **사용자 지정 도구** 그룹을 통해 관리 콘솔에서 클라이언트 기기에 대해 활성화한 애플리케이션, 즉 *사용자 지정 도구*(이후 간단히 *도구*라고도 함)의 목록을 만들 수 있습니다. 목록의 각 도구는 별도의 메뉴 명령과 연결되며 관리 콘솔에서 해당 명령을 사용하여 도구에 해당하는 애플리케이션을 시작할 수 있습니다.

애플리케이션은 관리자 워크스테이션에서 시작됩니다. 원격 클라이언트 기기의 특성(예: NetBIOS 이름, DNS 이름 또는 IP 주소)을 명령줄 옵션으로 사용할 수 있습니다. 터널링을 통해 원격 기기에 대한 연결을 설정할 수 있습니다.

기본적으로 사용자 지정 도구의 기본 목록에는 각 클라이언트 기기에 대한 다음과 같은 서비스 프로그램이 들어 있습니다:

- **원격 진단** - Kaspersky Security Center의 원격 진단용 유틸리티.
- **원격 데스크톱** - 원격 데스크톱 연결이라는 표준 Microsoft Windows 구성 요소.
- **컴퓨터 관리** – 표준 Microsoft Windows 구성 요소.

사용자지정 도구를 추가 또는 제거하거나 설정을 편집하려면,

클라이언트 기기의 마우스 오른쪽 메뉴에서 **사용자 지정 도구 → 사용자 지정 도구 구성**를 선택합니다.

사용자 지정 도구 창이 열립니다. 이 창에서 사용자 지정 도구를 추가하거나 **추가** 및 **수정** 버튼을 사용하여 해당 설정을 편집할 수 있습니다. 사용자 정의 도구를 제거하려면 적십자 아이콘(❌)이 있는 제거 버튼을 클릭합니다.

네트워크 에이전트 디스크 복제 모드

참조 기기의 하드 드라이브를 복제하는 것은 새로운 기기에 소프트웨어를 설치하는 일반적인 방법입니다. 만일 네트워크 에이전트가 참조 기기의 하드 드라이브에서 표준 모드로 실행되고 있으면 다음과 같은 문제가 발생합니다:

네트워크 에이전트가 포함된 참조 기기의 디스크 이미지가 새로운 컴퓨터에 배포되면, 관리 콘솔에 하나의 컴퓨터 아이콘으로 나타납니다. 이 문제는 중앙 관리 서버가 관리 콘솔에서 아이콘으로 기기를 나타낼 때 필요한 고유한 내부 데이터가 복제되어 동일한 값을 새 기기가 가지고 있기 때문입니다.

복제 후 특별한 *네트워크 에이전트 디스크 복제 모드*를 사용하면 관리 콘솔에서 새 기기를 잘못 표시하는 문제를 막을 수 있습니다. 디스크를 복제해서 새로운 기기에 소프트웨어(네트워크 에이전트 포함)를 배포할 때 이 모드를 사용하시기 바랍니다.

디스크 복제 모드에서는 네트워크 에이전트가 계속 실행되지만, 중앙 관리 서버로는 연결하지 않습니다. 복제 모드를 종료할 때 관리 콘솔에서 중앙 관리 서버가 하나의 아이콘으로 여러 기기를 나타내게 만드는 내부 데이터를 네트워크 에이전트가 삭제합니다. 참조 기기 이미지 복제가 완료된 후 새로운 기기는 관리 콘솔에서 올바르게 표시됩니다(각각의 아이콘으로).

네트워크 에이전트 디스크 복제 모드 사용 시나리오

1. 관리자가 참조 기기에 네트워크 에이전트를 설치합니다.
2. 관리자가 klnagchk 유틸리티를 사용해 중앙 관리 서버로의 네트워크 에이전트 연결을 확인합니다.
3. 관리자가 네트워크 에이전트 디스크 복제 모드를 활성합니다.
4. 관리자가 기기에 소프트웨어 및 패치를 설치하고, 기기를 필요한 만큼 재시작합니다.
5. 관리자가 참조 기기의 하드 드라이브를 여러 기기에 복제합니다.
6. 각 복제된 컴퓨터는 다음 조건을 충족해야 합니다:
   a. 기기 이름은 변경되지 않아야 합니다.
   b. 기기가 재시작되어야 합니다.
   c. 디스크 복제 모드는 비활성되어야 합니다.

klmover 유틸리티를 이용한 디스크 복제 모드 활성 및 비활성

네트워크 에이전트 디스크 복제 모드를 활성화 또는 비활성화하려면:

1. 복제해야 할 네트워크 에이전트가 설치된 기기에 klmover 유틸리티를 실행합니다.
   klmover 유틸리티는 네트워크 에이전트 설치 폴더에 위치해 있습니다.
2. 디스크 복제 모드를 활성하려면 Windows 명령 프롬프트에서 다음 명령어를 입력합니다:
   ```
   klmover -cloningmode 1
   ```
   네트워크 에이전트는 디스크 복제 모드로 전환합니다.
3. 디스크 복제 모드의 현재 상태를 요청하려면, 명령 프롬프트에 다음 명령어를 입력합니다.

`klmover -cloningmode`

유틸리티 창이 디스크 복제 모드가 활성 유무를 표시합니다.

4. 디스크 복제 모드를 비활성하려면 유틸리티 명령줄에 다음 명령어를 입력합니다.

   `klmover -cloningmode 0`

운영 체제 이미지 생성을 위해 설치된 네트워크 에이전트로 참조 기기 준비

설치되어 있는 네트워크 에이전트로 참조 기기의 운영 체제 이미지를 생성한 다음, 이 이미지를 네트워크에 연결된 기기에 배포할 수 있습니다. 그 경우, 네트워크 에이전트가 아직 시작되지 않은 참조 기기의 운영 체제 이미지를 생성합니다. 운영 체제 이미지 생성 전에 참조 기기에서 네트워크 에이전트를 시작하는 경우 해당 참조 기기의 운영 체제 이미지로부터 배포된 기기를 중앙 관리 서버에서 식별하는 데 문제가 생길 수 있습니다.

운영 체제 이미지 생성을 위해 참조 기기를 준비하려면 다음 절차를 따르십시오.

1. Windows 운영 체제가 참조 기기에 설치되어 있는지 확인하고, 해당 기기에 필요한 다른 소프트웨어를 설치합니다.

2. 참조 기기의 Windows 네트워크 연결 설정에서 Kaspersky Security Center가 설치되어 있는 네트워크와 참조 기기의 연결을 끊습니다.

3. 참조 기기에서 setup.exe 파일을 사용하여 네트워크 에이전트의 로컬 설치를 시작합니다.

   Kaspersky Security Center 네트워크 에이전트 설치 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

4. 마법사의 **중앙 관리 서버** 페이지에서 중앙 관리 서버 IP 주소를 지정합니다.

   중앙 관리 서버의 정확한 주소를 모르면 localhost를 입력하십시오. 나중에 klmover 유틸리티와 `-address` 키를 사용하여 IP 주소를 변경할 수 있습니다.

5. 마법사의 **애플리케이션 시작** 페이지에서 **설치 중 애플리케이션 시작** 옵션을 비활성화합니다.

6. 네트워크 에이전트 설치가 완료되면 운영 체제 이미지 생성 전에 기기를 다시 시작하지 마십시오.

   기기를 다시 시작하는 경우 운영 체제 이미지 생성을 위한 참조 기기 준비의 전체 과정을 반복해야 합니다.

7. 참조 기기의 명령줄에서 sysprep utility를 시작하고 `sysprep.exe /generalize /oobe /shutdown` 명령을 실행합니다.

참조 기기가 운영 체제 이미지 생성 준비를 마쳤습니다.

파일 무결성 모니터에서 메시지 수신 구성

Kaspersky Security for Windows Server 또는 Kaspersky Security for Virtualization Light Agent와 같은 관리 중인 애플리케이션은 파일 무결성 모니터에서 Kaspersky Security Center로 메시지를 보냅니다. 또한, Kaspersky Security Center에서는 웹 서버, ATM 등 매우 중요한 시스템 구성요소의 변경 내용을 모니터링하고 해당 시스템의 무결성 위반 시 신속하게 대응할 수 있습니다. 이러한 작업을 위해 파일 무결성 모니터 구성요소에서 메시지를 받을 수 있습니다. 파일 무결성 모니터 구성요소를 사용하면 기기의 파일 시스템뿐 아니라 기기 레지스트리 하이브, 방화벽 상태, 연결된 하드웨어의 상태도 모니터링할 수 있습니다.

Kaspersky Security for Windows Server 또는 Kaspersky Security for Virtualization Light Agent를 사용하지 않고 파일 무결성 모니터 구성 요소의 메시지를 수신하도록 Kaspersky Security Center를 구성해야 합니다.

파일 무결성 모니터에서 메시지 수신을 구성하려면 다음과 같이 하십시오:

1. 중앙 관리 서버가 설치된 기기에서 시스템 레지스트리를 엽니다(예:로컬에서 **시작 → 실행** 메뉴의 regedit 명령 사용).

2. 다음 하이브로 이동합니다:

   - 32비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - 64비트 운영 체제:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. 키 만들기:

   - 처리된 이벤트 수를 계산할 기간을 지정하려면 KLSRV_EVP_FIM_PERIOD_SEC 키를 만듭니다. 다음 설정을 지정합니다:

     a. 키 이름으로 KLSRV_EVP_FIM_PERIOD_SEC 지정.

     b. 키 유형으로 DWORD를 지정합니다.

     c. 시간 간격 값 범위를 43200~172800초 사이로 지정합니다. 기본 시간 간격은 86400초입니다.

   - 지정한 시간 간격 동안 수신되는 이벤트 수를 제한하려면 KLSRV_EVP_FIM_LIMIT 키를 만듭니다. 다음 설정을 지정합니다:

     a. 키 이름으로 KLSRV_EVP_FIM_LIMIT를 지정합니다.

     b. 키 유형으로 DWORD를 지정합니다.

     c. 수신되는 이벤트의 값 범위를 2000~50000로 지정합니다. 기본 이벤트 수는 20000개입니다.

   - 특정 시간 간격까지의 정확도로 이벤트 수를 계산하려면 KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC 키를 만듭니다. 다음 설정을 지정합니다:

     a. 키 이름으로 KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC를 지정합니다.

     b. 키 유형으로 DWORD를 지정합니다.

     c. 값 범위를 120~600초 사이로 지정합니다. 기본 기간은 300초입니다.

   - 지정한 시간이 지난 후 애플리케이션이 해당 시간 간격 동안 처리된 이벤트 수가 지정된 제한보다 적은지 여부를 확인할 수 있도록 하려면 KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC 키를 만듭니다. 이벤트 수신 제한에 도달하면 이 확인이 수행됩니다. 이 조건이 충족되면 애플리케이션은 데이터베이스에 이벤트를 다시 저장하기 시작합니다. 다음 설정을 지정합니다:

     a. 키 이름으로 KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC를 지정합니다.

     b. 키 유형으로 DWORD를 지정합니다.

     c. 값 범위를 600~3600초로 지정합니다. 기본 시간 간격은 1800초입니다.

키를 만들지 않으면 기본값이 사용됩니다.

4. 중앙 관리 서버 서비스를 다시 시작합니다.

파일 무결성 모니터 구성 요소로부터의 이벤트 수신 제한이 구성됩니다. **가장 자주 트리거된 파일 무결성 모니터/시스템 무결성 모니터링의 상위 10개 규칙** 및 **파일 무결성 모니터/시스템 무결성 모니터링 규칙이 가장 자주 트리거되는 상위 10개 기기** 리포트에서 파일 무결성 모니터 구성요소의 결과를 확인할 수 있습니다.

중앙 관리 서버 점검

중앙 관리 서버 유지 관리를 통해 중앙 관리 서버 폴더의 공간을 확보하고 불필요한 개체를 삭제하여 데이터베이스의 크기를 줄일 수 있습니다. 이는 애플리케이션의 성능 및 작동 안정성 개선에 도움이 됩니다. 중앙 관리 서버 유지 관리는 최소 한 주에 한 번 수행하는 것이 좋습니다.

중앙 관리 서버는 전용 작업으로 유지 관리할 수 있습니다. 이 애플리케이션은 중앙 관리 서버 유지보수 시 다음 동작을 수행합니다.

- 저장소 폴더에서 불필요한 폴더와 파일을 삭제합니다.
- 표에서 불필요한 레코드(또는 "허상 포인터")를 삭제합니다.
- 캐시를 지웁니다.
- 데이터베이스 유지 관리(SQL Server 또는 PostgreSQL을 DBMS로 사용할 시):
  - 데이터베이스 오류를 확인합니다(SQL Server에서만 사용 가능).
  - 데이터베이스 인덱스 재편성.
  - 데이터베이스 통계 업데이트.
  - 데이터베이스 줄임(필요 시).

중앙 관리 서버 점검 작업을 생성하려면:

1. 콘솔 트리에서 *중앙 관리 서버 점검* 작업을 만들고자 하는 중앙 관리 서버 노드를 선택합니다.
2. **작업** 폴더를 선택합니다.
3. **작업** 폴더의 작업 영역에서 **새 작업** 버튼을 누릅니다.
   새 작업 마법사가 시작됩니다.
4. 마법사의 **작업 유형 선택** 창에서 **중앙 관리 서버 점검**을 작업 유형으로 선택하고 **다음**을 누릅니다.
5. 점검 중 중앙 관리 서버 데이터베이스를 줄이려면 마법사의 **설정** 창에서 **데이터베이스 축소** 확인란을 선택합니다.
6. 마법사의 나머지 지침을 따릅니다.

새롭게 생성된 작업은 **작업** 폴더에서 작업 영역의 작업 목록에 표시됩니다. 하나의 중앙 관리 서버에서는 하나의 *중앙 관리 서버 점검* 작업만 수행할 수 있습니다. 중앙 관리 서버를 위한 *중앙 관리 서버 점검* 작업이 이미 생성이 되었다면, 새로운 *중앙 관리 서버 점검* 작업을 만들 수 없습니다.

공용 DNS 서버 접근

시스템 DNS를 사용하여 Kaspersky 서버에 접근할 수 없다면 Kaspersky Security Center는 다음 순서로 다음 공용 DNS 서버를 사용할 수 있습니다.

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

애플리케이션이 DNS 서버에 대한 TCP/UDP 연결을 설정하므로, 이러한 DNS 서버에 대한 요청에는 도메인 주소와 중앙 관리 서버의 공용 IP 주소가 포함될 수 있습니다. Kaspersky Security Center가 공용 DNS 서버를 사용 시, 데이터 처리는 해당 서비스의 개인 정보 보호 정책에 따릅니다.

klscflag 유틸리티를 사용해 공용 DNS 사용을 구성하려면:

1. 관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다.
2. 공용 DNS 사용을 비활성화하려면 다음 명령을 실행합니다.

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. 공용 DNS 사용을 활성화하려면 다음 명령을 실행합니다.

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

사용자 알림 방법 창

사용자 알림 방법 창에서 모바일 기기에 인증서를 설치하는 것에 관한 사용자 알림을 구성할 수 있습니다.

- **마법사에 QR 코드 표시**. 이 옵션을 선택하면 모바일 기기 연결 마법사의 마지막 단계에서 설치 패키지 링크가 표시됩니다.
- **사용자에게 QR 코드 전송**. 이 옵션을 선택하면 기기 연결 시 사용자에게 알려 주는 설정을 지정할 수 있습니다.

설정의 **이메일** 그룹에서 이메일 메시지를 사용하여 모바일 기기에 새 인증서 설치에 대한 사용자 알림을 구성할 수 있습니다. 이 알림 방법은 SMTP 서버를 사용했을 경우에만 이용할 수 있습니다.

설정의 **SMS** 그룹에서 SMS를 사용하여 모바일 기기에 인증서 설치에 대한 사용자 알림을 구성할 수 있습니다. 이 알림 방법은 SMS 알림을 사용했을 경우에만 이용할 수 있습니다.

필요한 경우 설정의 **이메일** 및 **SMS** 그룹에서 **메시지 편집** 링크를 눌러 알림 메시지를 보거나 편집할 수 있습니다.

기기 조회 창

기기 선택 목록에서 조회를 선택합니다. 이 목록에는 사용자가 작성한 조회 항목과 사전 정의된 조회 항목이 포함되어 있습니다.

기기 선택 섹션의 작업 영역에서 기기 조회의 세부 정보를 볼 수 있습니다.

새 개체 창의 이름 정의

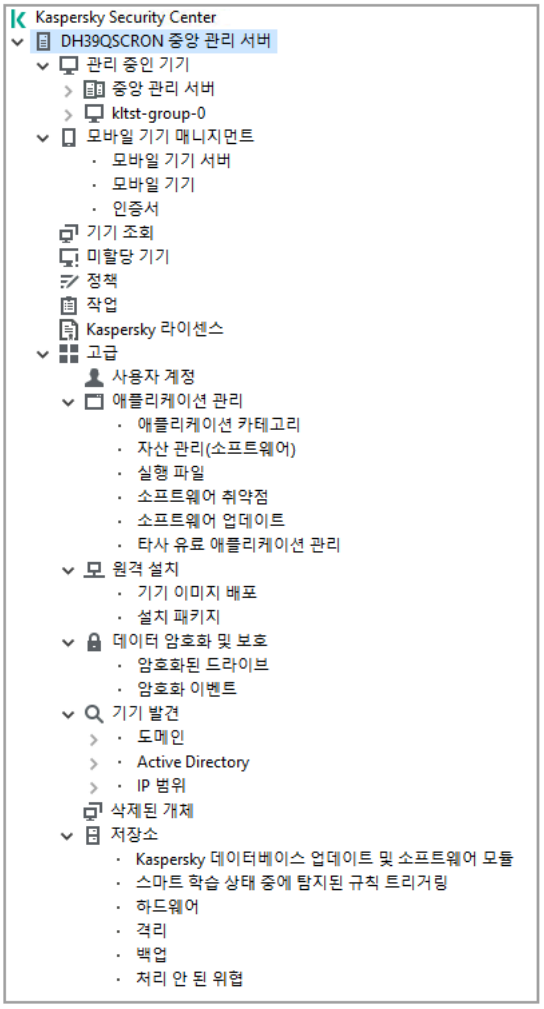
창에서 새로 생성된 개체의 이름을 지정하십시오. 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

관리 인터페이스 사용 기능

이 섹션에서는 Kaspersky Security Center의 메인 창에서 수행할 수 있는 처리에 대해 설명합니다.

콘솔 트리

콘솔 트리(아래 그림 참조)는 회사 네트워크 내 중앙 관리 서버의 계층 구조, 여기에 속한 관리 그룹의 구조 및 **저장소**나 **애플리케이션 관리** 폴더 등 애플리케이션의 기타 개체를 표시하도록 설계되었습니다. Kaspersky Security Center의 네임스페이스에는 설치 후 계층 구조에 포함된 중앙 관리 서버에 해당하는 서버 이름 등 여러 노드가 있을 수 있습니다.



콘솔 트리

중앙 관리 서버 노드

중앙 관리 서버 – <기기 이름> 노드는 선택한 중앙 관리 서버의 구성 체계를 보여주는 컨테이너입니다.

중앙 관리 서버 노드의 작업 영역에는 중앙 관리 서버에서 관리하는 애플리케이션 및 기기의 현재 상태에 대한 요약 정보를 담고 있습니다. 작업 영역에 있는 정보는 여러 탭에 분포됩니다:

- **모니터링**. 실시간 모드로 애플리케이션 운영과 클라이언트 기기의 현재 상태에 대한 정보를 표시합니다. 관리자를 위한 중요 메시지(취약점, 오류 또는 바이러스 탐지 등)는 특정 색으로 강조됩니다. 표준 관리자 작업(예: 클라이언트 기기에 보안 제품 설치 및 구성)과 다른 콘솔 트리 폴더로 이동과 같은 작업을 수행하기 위해 **모니터링** 탭에서 링크들을 사용할 수 있습니다.

- **통계**. 주제별로 그룹화된 차트를 포함하고 있습니다(보호 상태, 안티 바이러스 통계, 업데이트 등). 이 차트는 애플리케이션 운영 및 클라이언트 기기의 상태에 대한 현재 정보를 보여줍니다.

- **리포트**. 애플리케이션별로 만들 수 있는 리포트 템플릿이 있습니다. 이 탭에서 프리셋 템플릿을 사용해 리포트를 만들 수 있을 뿐만 아니라 사용자지정 리포트 템플릿도 만들 수 있습니다.

- **이벤트** 창이 열립니다. 애플리케이션 운영 중에 등록된 이벤트가 있습니다. 이 레코드는 읽기 편한 주제와 필터링을 사용해 배치되어 있습니다. 이 탭에서 자동으로 생성된 이벤트 조회 항목을 볼 수 있으며 사용자지정 조회도 만들 수 있습니다.

중앙 관리 서버 노드에 있는 폴더

중앙 관리 서버 – <기기 이름> 노드에는 다음과 같은 폴더가 포함됩니다:

- **관리 중인 기기**. 이 폴더는 관리 그룹의 구조, 그룹 정책 및 그룹 작업을 저장, 표시, 구성 및 수정하기 위한 폴더입니다.

- **모바일 기기 관리**. 이 폴더는 모바일 기기를 관리하기 위한 곳입니다. **모바일 기기 관리** 폴더에는 다음과 같은 하위 폴더가 포함됩니다:

  - **모바일 기기 서버**. iOS MDM 서버 관리용입니다.

  - **모바일 기기**. 모바일 기기, KES, iOS MDM 관리용입니다.

  - **인증서**. 모바일 기기의 인증서를 관리하기 위한 곳입니다.

- **기기 조회**. 이 폴더에서는 모든 관리 중인 기기 중에서 특정 조건(기기 조회)에 부합하는 기기를 빠르게 조회할 수 있습니다. 예를 들어, 보안 제품이 설치되지 않은 기기를 빠르게 선택하고 해당 기기의 목록을 볼 수 있습니다. 조회된 기기에 어떤 작업을 할당하는 조치를 진행할 수 있습니다. 프리셋 조회를 사용하거나 사용자지정 조회를 만들 수 있습니다.

- **미할당 기기**. 이 폴더에서는 관리 그룹에 포함 안 된 기기 목록을 확인할 수 있습니다. 미할당 기기에 특정 작업을 수행할 수 있습니다. 예, 관리 그룹으로 이동 또는 애플리케이션 설치.

- **정책**. 이 폴더에서 정책을 만들고 볼 수 있습니다.

- **작업**. 이 폴더에서 작업을 만들고 볼 수 있습니다.

- **Kaspersky 라이센스**. 이용 가능한 Kaspersky 애플리케이션용 라이센스 키 목록이 들어 있습니다. 이 폴더의 작업 영역에서 라이센스 키 저장소에 새 라이센스 키를 추가하고 관리 중인 기기에 라이센스 키를 배포하며 라이센스 키 사용 현황을 리포트로 볼 수 있습니다.

- **고급**. 이 폴더에서 애플리케이션 기능의 여러 그룹과 관련된 하위 폴더를 볼 수 있습니다.

고급 폴더. 콘솔 트리에 폴더 이동

고급 폴더에는 다음 하위 폴더가 들어 있습니다:

- **사용자 계정**. 이 폴더에는 네트워크 사용자 계정 목록이 들어 있습니다.

- **애플리케이션 관리**. 이 폴더는 기기에 설치된 애플리케이션을 관리하기 위한 폴더입니다. **애플리케이션 관리** 폴더에는 다음과 같은 하위 폴더가 포함됩니다:

  - **애플리케이션 카테고리**. 사용자 지정 애플리케이션 카테고리를 관리하는 데 사용됩니다.

  - **자산 관리(소프트웨어)**. 네트워크 에이전트가 설치된 기기에 있는 애플리케이션 목록이 들어 있습니다.

- **실행 파일**. 네트워크 에이전트가 설치된 클라이언트 기기에 저장되어 있는 실행 파일 목록이 들어 있습니다.
- **소프트웨어 취약점**. 네트워크 에이전트가 설치된 기기에 있는 애플리케이션의 취약점 목록이 들어 있습니다.
- **소프트웨어 업데이트**. 중앙 관리 서버에서 수신하여 기기에 배포할 수 있는 애플리케이션 업데이트 목록이 들어 있습니다.
- **타사 유료 애플리케이션 관리**. 유료 애플리케이션 그룹 목록이 들어 있습니다. 유료 애플리케이션 그룹을 사용하여 Kaspersky 애플리케이션이 아닌 타사 소프트웨어의 라이센스 사용 현황과 라이센스 제한 위반을 모니터할 수 있습니다.

- **원격 설치**. 이 폴더는 운영 체제와 애플리케이션의 원격 설치를 관리하기 위한 폴더입니다. **원격 설치** 폴더에는 다음과 같은 하위 폴더가 포함됩니다:
  - **기기 이미지 배포**. 기기에 운영 체제 이미지를 배포하기 위한 폴더입니다.
  - **설치 패키지**. 기기에 애플리케이션을 원격으로 설치하는 데 사용할 수 있는 설치 패키지 목록이 들어 있습니다.
- **데이터 암호화 및 보호**. 이 폴더는 드라이브와 이동식 드라이브의 데이터 암호화 절차를 관리하기 위한 폴더입니다.
- **네트워크 검색**. 이 폴더는 중앙 관리 서버가 설치된 네트워크를 표시합니다. 중앙 관리 서버는 회사 네트워크의 Windows 네트워크, IP 서브넷 및 Active Directory®를 정기적으로 검색하여 네트워크 구조 및 그 기기에 대한 정보를 수신합니다. 검색 결과는 **도메인**, **IP 범위** 및 **Active Directory**의 해당 폴더에 있는 작업 영역에 표시됩니다.
- **저장소**. 이 폴더는 기기의 상태 감시 및 유지 관리에 사용되는 개체 작업을 위한 폴더입니다. **저장소** 폴더에는 다음 하위 폴더가 포함됩니다:
  - **적응형 이상 탐지**. 클라이언트 기기에서 스마트 학습 모드로 Kaspersky Endpoint Security 규칙에 따라 적용되는 감지 목록이 들어 있습니다.
  - **Kaspersky 소프트웨어 업데이트 및 패치**. 중앙 관리 서버에서 받았으며 기기에 배포할 수 있는 업데이트 목록이 들어 있습니다.
  - **하드웨어**. 조직의 네트워크에 연결된 하드웨어 목록이 들어 있습니다.
  - **격리**. 기기에서 안티 바이러스 애플리케이션에 의해 격리 저장소로 이동된 개체의 목록이 들어 있습니다.
  - **백업**. 기기에서 악성 코드를 치료할 때 삭제 또는 수정된 파일의 백업 복사본 목록이 들어 있습니다.
  - **처리 안 된 파일**. 안티 바이러스 애플리케이션의 이후 검사에 할당된 파일의 목록이 들어 있습니다.

고급 폴더에 포함된 하위 폴더 집합을 변경할 수 있습니다. 자주 사용하는 하위 폴더는 **고급** 폴더에서 상위 레벨 그룹으로 이동할 수 있습니다. 자주 사용하지 않는 하위 폴더는 **고급** 폴더로 이동할 수 있습니다.

고급 폴더에서 하위 폴더를 이동하려면:

1. 콘솔 트리에서 **고급** 폴더로 옮기기 원하는 하위 폴더를 선택하십시오.
2. 하위 폴더의 마우스 오른쪽 메뉴에서 **보기 → 고급 폴더에서 이동**을 선택합니다.

고급 폴더의 작업 영역에서 **고급** 폴더에서 하위 폴더를 이동할 수 있습니다. 그렇게 하려면, 원하는 하위 폴더 이름 섹션에서 **고급 폴더에서 이동** 링크를 누르세요.

***고급** 폴더로 하위 폴더를 이동하려면:*

1. 콘솔 트리에서 **고급** 폴더로 옮겨야 하는 하위 폴더를 선택하십시오.
2. 하위 폴더의 마우스 오른쪽 메뉴에서 **보기 → 고급 폴더로 이동**을 선택합니다.

작업 영역에서 데이터를 업데이트하는 방법

Kaspersky Security Center에서는 기기 상태, 통계, 리포트 등의 작업 영역 데이터가 자동으로 업데이트되지 않습니다.

작업 영역의 데이터를 업데이트하려면 다음과 같이 하십시오:

- **F5** 키를 누릅니다.
- 콘솔 트리에 있는 개체의 마우스 오른쪽 메뉴에서 **새로 고침**를 선택합니다.
- 작업 영역에서 새로고침 아이콘()을 누릅니다.

콘솔 트리를 탐색하는 방법

다음과 같은 툴바 버튼을 사용하여 콘솔 트리를 탐색할 수 있습니다:

- —한 단계 뒤로.
- —한 단계 앞으로.
- —한 단계 위로.

작업 영역의 오른쪽 상단에 있는 탐색 체인을 사용할 수도 있습니다. 탐색 체인에는 콘솔 트리에서 현재 사용자가 있는 폴더에 대한 전체 경로가 들어 있습니다. 마지막 요소를 제외한 체인의 모든 요소는 콘솔 트리의 개체로 연결되는 링크입니다.

작업 영역에서 개체 속성 창을 여는 방법

개체 속성 창에서는 대부분의 관리 콘솔 개체의 속성을 변경할 수 있습니다.

작업 영역에 있는 개체의 속성 창을 열려면 다음과 같이 하십시오:

- 개체의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
- 개체를 선택하고 **ALT+ENTER** 키를 누릅니다.

작업　영역에서 개체 그룹을 선택하는 방법

작업　영역에서 개체 그룹을 선택할 수 있습니다. 작업　영역에서는 개체 그룹을 선택하여 예를 들면 나중에 작업을 만들 기기 집합을 만들 수 있습니다.

개체 범위를 선택하려면 다음과 같이 하십시오:

1. 범위의 첫 번째 개체를 선택하고 **SHIFT** 키를 누릅니다.
2. **SHIFT** 키를 누른 상태에서 범위의 마지막 개체를 선택합니다.

   이렇게 하면 범위가 선택됩니다.

개별 개체를 그룹화하려면 다음과 같이 하십시오:

1. 그룹에서 첫 번째 개체를 선택하고 **CTRL**을 누릅니다.
2. **CTRL** 키를 누른 상태에서 그룹에 포함할 다른 개체를 선택합니다.

   개체가 그룹화됩니다.

작업　영역에서 열 집합을 변경하는 방법

관리 콘솔에서는 작업　영역에 표시할 열 집합을 변경할 수 있습니다.

작업　영역에 표시되는 열 집합을 변경하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 열 집합을 변경할 개체를 누릅니다.
2. 폴더의 작업　영역에서 **열 추가/제거** 링크를 눌러 열 집합 구성을 위한 창을 엽니다.
3. **열 추가/제거** 창에서 표시할 열 집합을 지정합니다.

참조 정보

이 섹션의 표에는 관리 콘솔 개체의 마우스 오른쪽 메뉴와 콘솔 트리 개체 및 작업　영역 개체에 대한 요약 정보가 나와 있습니다.

마우스 오른쪽 메뉴 명령

이 섹션에는 관리 콘솔 개체와 해당하는 마우스 오른쪽 메뉴 항목이 나와 있습니다(아래 표 참조).

관리 콘솔 개체의 마우스 오른쪽 메뉴 항목

개체	메뉴 항목	메뉴 항목의 기능
마우스 오른쪽 메뉴의 일반 항목	**검색**	기기 검색 창을 엽니다.
	새로 고침	선택한 개체의 표시를 새로 고칩니다.
	목록 내보내기	현재 목록을 파일로 내보냅니다.
	속성	선택한 개체의 속성 창을 엽니다.
	보기 → 열 추가/제거	작업 영역에 있는 개체 표의 열을 추가하거나 제거합니다.
	보기 → 큰 아이콘	작업 영역의 개체를 큰 아이콘으로 표시합니다.
	보기 → 작은 아이콘	작업 영역의 개체를 작은 아이콘으로 표시합니다.
	보기 → 목록	작업 영역의 개체를 목록으로 표시합니다.
	보기 → 표	작업 영역의 개체를 표로 표시합니다.
	보기 → 구성	관리 콘솔 항목의 표시 방식을 구성합니다.
Kaspersky Security Center	**새로 만들기 → 중앙 관리 서버**	콘솔 트리에 중앙 관리 서버를 추가합니다.
<중앙 관리 서버 이름>	**중앙 관리 서버에 연결**	해당 중앙 관리 서버에 연결합니다.
	중앙 관리 서버에서 연결 끊기	해당 중앙 관리 서버에서 연결을 끊습니다.
관리 중인 기기	**애플리케이션 설치**	원격 설치 마법사를 시작합니다.
	보기 → 인터페이스 구성	인터페이스 요소의 표시 방식을 구성합니다.
	제거	콘솔 트리에서 중앙 관리 서버를 제거합니다.
	애플리케이션 설치	관리 그룹에 대한 원격 설치 마법사를 시작합니다.
	바이러스 카운터 초기화	관리 그룹에 포함된 기기의 바이러스 카운터를 초기화합니다.
	위협 처리 리포트 보기	관리 그룹에 포함된 기기의 위협 처리 리포트 및 바이러스 활동 리포트를 만듭니다.
	만들기 → 그룹	관리 그룹을 만듭니다.
	모든 작업 → 새 그룹 조직도	도메인 또는 Active Directory의 구조를 기반으로 관리 그룹 조직도를 만듭니다.
	모든 작업 → 메시지 표시	관리 그룹에 포함된 기기의 사용자에 대해 사용자를 위한 새 메시지를 시작합니다.
관리 중인 기기 → 중앙 관리 서버	**만들기 → 보조 중앙 관리 서버**	보조 중앙 관리 서버 추가 마법사를 시작합니다.
	New → 가상 중앙 관리 서버	새 가상 중앙 관리 서버 마법사를 시작합니다.
모바일 기기 관리 → 모바일 기기	**새로 만들기 → 모바일 기기**	사용자의 새 모바일 기기를 연결합니다.
모바일 기기 관리 → 인증서	**새로 만들기 → 인증서**	인증서를 만듭니다.
	만들기 → 모바일 기기	사용자의 새 모바일 기기를 연결합니다.
기기 선택	**새로 만들기 → 새 선택**	기기 조회를 생성합니다.
	모든 작업 → 가져오기	파일에서 조회 항목을 가져옵니다.
Kaspersky 라이센스	**활성화 코드 또는 키 파일 추가**	중앙 관리 서버 저장소에 라이센스 키를 추가합니다.
	애플리케이션 활성화	애플리케이션 활성화 작업 생성 마법사를 시작합니다.
	라이센스 키 사용 리포트	클라이언트 기기의 라이센스 키에 대한 리포트를 만들고 봅니다.
애플리케이션 관리 → 애플리케이션 카테고리	**만들기 → 카테고리**	애플리케이션 카테고리를 만듭니다.
애플리케이션 관리 → 자산 관리(소프트웨어)	**필터**	애플리케이션 목록에 대한 필터를 설정합니다.
	감시 중인 애플리케이션	애플리케이션 설치와 관련된 이벤트의 게시를 구성합니다.
	설치 안 된 애플리케이션 제거	네트워크 기기에 더 이상 설치되어 있지 않은 애플리케이션의 모든 상세 정보 목록을 제거합니다.

개체	메뉴 항목	메뉴 항목의 기능
애플리케이션 관리 → 소프트웨어 업데이트	**업데이트에 대한 라이센스 계약서 수락**	소프트웨어 업데이트에 대한 라이센스 계약서를 수락합니다.
애플리케이션 관리 → 타사 라이센스 사용 관리	**만들기 → 유료 애플리케이션 그룹**	유료 애플리케이션 그룹을 만듭니다.
원격 설치 → 설치 패키지	**현재 애플리케이션 버전 표시**	웹 서버에서 사용 가능한 최신 버전의 Kaspersky 애플리케이션 목록을 표시합니다.
	만들기 → 설치 패키지	설치 패키지를 만듭니다.
	모든 작업 → 데이터베이스 업데이트	설치 패키지의 애플리케이션 데이터베이스를 업데이트합니다.
	모든 작업 → 독립 실행형 패키지의 일반 목록 표시	설치 패키지에 대해 만들어진 독립 실행형 패키지의 목록을 봅니다.
기기 발견 → 도메인	**모든 작업 → 기기 활동**	네트워크 기기의 활동이 없을 경우 중앙 관리 서버의 대응을 설정합니다.
기기 발견 → IP 범위	**만들기 → IP 범위**	IP 범위를 만듭니다.
저장소 → Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트	**업데이트 다운로드**	중앙 관리 서버의 저장소 업데이트(중앙 관리 서버) 작업 속성 창을 엽니다.
	업데이트 다운로드 설정	중앙 관리 서버의 저장소 업데이트(중앙 관리 서버) 작업을 구성합니다.
	안티 바이러스 데이터베이스 사용 리포트	데이터베이스 버전에 대한 리포트를 만들고 봅니다.
	모든 작업 → 중앙 관리 서버 저장소 업데이트 지우기	중앙 관리 서버의 저장소 업데이트를 지웁니다.
저장소 → 하드웨어	**만들기 → 기기**	새 기기 만들기.

관리 중인 기기 목록. 열 설명

다음 표에는 관리 중인 기기 목록 열의 이름과 각각의 설명이 표시됩니다.

관리 중인 기기 목록 열의 설명

열 이름	값
이름	클라이언트 기기의 NetBIOS 이름. 기기 이름 아이콘에 대한 설명은 부록에 나와 있습니다.
운영 체제 유형	클라이언트 기기에 설치된 운영 체제 유형.
Windows 도메인	클라이언트 기기가 위치한 Windows 도메인 이름.
네트워크 에이전트가 설치됨	클라이언트 기기에서 수행한 네트워크 에이전트 설치 결과: *예*, *아니요*, *알 수 없음*.
네트워크 에이전트가 실행 중	네트워크 에이전트 작동 결과: *예*, *아니요*, *알 수 없음*.
실시간 보호	보안 제품이 설치됨: *예*, *아니요*, *알 수 없음*.
마지막 중앙 관리 서버 연결	클라이언트 기기가 중앙 관리 서버에 연결된 후 경과한 시간.
마지막 안티 바이러스 데이터베이스 업데이트	관리 중인 기기의 마지막 업데이트 이후 경과한 시간.
상태	클라이언트 기기의 현재 상태: *정상*, *심각 경고 중 하나*.

열 이름	값
상태 설명	클라이언트 기기의 상태가 *심각* 또는 *경고*로 변경되는 조건. 다음과 같은 조건에서는 기기의 상태가 *경고* 또는 *심각*으로 변경됩니다. • 보안 제품이 설치 안 됨. • 바이러스가 너무 많이 탐지됨. • 실시간 보호 레벨이 관리자가 설정한 레벨과 다름. • 오랫동안 악성 코드를 검사하지 않음. • 데이터베이스가 오래됨. • 오랫동안 중앙 관리 서버에 연결 안 됨. • 처리 안 된 위협이 탐지됨. • 재시작 필요. 기기를 다시 시작해야 하는 이유는 다음 중 하나일 수 있습니다. • 알 수 없는 이유로 재시작됨. • 재시작할 때까지 애플리케이션이 실행되지 않습니다. • 업데이트를 완료하려면 재시작이 필요합니다. 애플리케이션이 실행 중입니다. • 업데이트를 시작하려면 재시작해야 합니다. • 검사 또는 치료를 완료하려면 재시작해야 합니다. • 원격 설치/제거를 완료하려면 재시작해야 합니다. • 디스크의 데이터 암호화 완료. 기기 상태 전환 구성 시 이유를 설정할 수 있습니다. • 비호환 애플리케이션이 설치되어 있음. • 소프트웨어 취약점이 탐지됨. • 오랫동안 Windows 업데이트 패치를 검색하지 않았습니다. • 유효하지 않은 암호화 상태. • 모바일 기기 설정이 정책과 일치하지 않음. • 처리되지 않은 보안 문제가 있음. • 애플리케이션에서 정의된 기기 상태. • 기기 디스크 공간 부족. • 라이센스가 곧 만료됨. 다음 이유만으로 기기의 상태가 *심각*으로 변경되었습니다. • 라이센스 만료됨. • 기기와의 연결이 끊어짐. • 보호가 비활성화됨. • 보안 제품이 실행 중이지 않음. 클라이언트 기기의 관리되는 Kaspersky 애플리케이션이 목록에 상태 설명을 추가합니다. Kaspersky Security Center는 해당 클라이언트 기기에 설치된 관리되는 Kaspersky 애플리케이션으로부터 기기 상태 정보를 수신합니다. 관리되는 애플리케이션이 기기에 할당한 상태가 Kaspersky Security Center에서 할당한 상태 이외의 상태인 경우 관리 콘솔에 기기 보안이 가장 심각한 상태로 표시됩니다. 예를 들어 관리되는 애플리케이션이 기기에 *심각* 상태를 할당했는데 Kaspersky Security Center에서 *경고* 상태를 할당한 경우 관리 콘솔에는 해당 기기에 대해 *심각* 상태로 표시되고 관리되는 애플리케이션에서 보낸 해당 정보가 표시됩니다.
업데이트된 정보	클라이언트 기기가 마지막으로 중앙 관리 서버와 성공적으로 동기화한 후(즉, 마지막 네트워크 검사로부터) 경과한 시간.
DNS 이름	클라이언트 기기의 DNS 도메인 이름.
DNS 도메인	주요 DNS 접미사.
IP 주소	클라이언트 기기의 IP 주소. IPv4 주소를 사용하는 것이 좋습니다.
마지막 존재 확인	네트워크에서 클라이언트 기기의 존재가 확인된 기간.
마지막 전체 검사	사용자 요청에 따라 보안 제품이 마지막으로 수행한 클라이언트 기기 검사의 날짜와 시간.
탐지된 위협 전체 개수	발견된 위협의 수.
실시간 보호 상태	실시간 보호 상태: *시작 중, 실행 중, 실행 중 (최대 보호), 실행 중 (최고 속도), 실행 중 (권장), 실행 중 (사용자 지정 설정), 중지됨, 일시 중지됨, 실패.*
연결 IP 주소	Kaspersky Security Center 중앙 관리 서버 연결 시 사용하는 IP 주소.
네트워크 에이전트 버전	네트워크 에이전트의 버전.
애플리케이션 버전	클라이언트 기기에 설치된 보안 제품 버전.
배포된 안티 바이러스 데이터베이스	안티 바이러스 데이터베이스 버전.

열 이름	값
마지막 시스템 시작 시간	클라이언트 기기가 마지막으로 켜진 날짜 및 시간.
재시작 필요	클라이언트 기기를 다시 시작해야 합니다.
배포 지점	이 클라이언트 기기의 배포 지점 역할을 하는 기기의 이름.
설명	네트워크 검사 후 받은 클라이언트 기기에 대한 설명.
암호화 상태	클라이언트 기기의 데이터 암호화 상태.
WUA 상태	클라이언트 기기의 Windows 업데이트 에이전트 상태. *예*는 Windows 업데이트를 통해 중앙 관리 서버로부터 업데이트를 받는 클라이언트 기기에 해당합니다. *아니오*는 Windows 업데이트를 통해 다른 출처로부터 업데이트를 받는 클라이언트 기기에 해당합니다.
운영 체제 비트 크기	클라이언트 기기에 설치된 운영 체제의 비트 크기.
스팸 보호 상태	스팸 방지 구성 요소의 상태: *실행 중, 시작 중, 중지됨, 일시 중지됨, 실패, 알 수 없음*
데이터 유출 방지 상태	데이터 유출 방지 구성 요소의 상태: *실행 중, 시작 중, 중지됨, 일시 중지됨, 실패, 알 수 없음*
협업 서버 보호 상태	컨텐츠 필터링 구성 요소의 상태: *실행 중, 시작 중, 중지됨, 일시 중지됨, 실패, 알 수 없음*
메일 서버의 안티 바이러스 보호 상태	메일 서버 안티 바이러스 보호 구성 요소의 상태: *실행 중, 시작 중, 중지됨, 일시 중지됨, 실패, 알 수 없음*
Endpoint Sensor 상태	엔드포인트 Detection and Response 구성 요소의 상태: *실행 중, 시작 중, 중지됨, 일시 중지됨, 실패, 알 수 없음*
만든 날짜	<기기 이름> 아이콘이 생성된 시간. 이 속성은 다양한 이벤트를 서로 비교하는 데 사용됩니다.
가상 또는 보조 중앙 관리 서버 이름	가상 또는 보조 중앙 관리 서버 이름. 이 열은 다른 중앙 관리 서버의 기기가 포함된 목록에만 사용할 수 있습니다.
부모 그룹	<기기 이름> 아이콘이 있는 관리 그룹의 이름. 이 열은 다른 중앙 관리 서버의 기기가 포함된 목록에만 사용할 수 있습니다.
다른 중앙 관리 서버에서 관리	이 파라미터는 다음 값 중 하나를 가질 수 있습니다. • 기기에 보안 애플리케이션을 원격 설치하는 중 기기가 다른 중앙 관리 서버에 의해 관리 중인 것을 발견하는 경우 True입니다. • 그렇지 않으면 False입니다.
운영 체제 빌드	운영 체제의 빌드 번호입니다. 선택한 운영 체제의 빌드 번호가 이 번호와 같아야 하는지 아니면 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 빌드 번호를 제외한 모든 빌드 번호를 검색하도록 구성할 수도 있습니다.
운영 체제 릴리즈 ID	운영 체제의 릴리즈 식별자(ID)입니다. 선택한 운영 체제의 릴리즈 ID가 이 ID와 같아야 하는지 아니면 이전/이후 ID여야 하는지를 지정할 수 있습니다. 지정한 릴리즈 ID 번호를 제외한 모든 릴리즈 ID 번호를 검색하도록 구성할 수도 있습니다.

기기, 작업 및 정책의 상태

다음 표에는 콘솔 트리 및 중앙 관리 콘솔의 작업 영역에서 기기, 작업 및 정책 이름 옆에 표시되는 아이콘이 정리되어 있습니다. 이러한 아이콘은 개체의 상태를 정의합니다.

아이콘	상태
	워크스테이션용 운영 체제를 실행하고 시스템에서 검색되지만 관리 그룹에는 아직 포함되지 않은 기기.
	워크스테이션용 운영 체제를 실행하고 관리 그룹에 포함되어 있으며 *정상* 상태인 기기.
	워크스테이션용 운영 체제를 실행하고 관리 그룹에 포함되어 있으며 *경고* 상태인 기기.
	워크스테이션용 운영 체제를 실행하고 관리 그룹에 포함되어 있으며 *심각* 상태인 기기.
	워크스테이션용 운영 체제를 실행하고, 중앙 관리 서버와의 연결이 끊어진 관리 그룹에 포함되어 있는 기기.
	서버용 운영 체제를 실행하고 시스템에서 검색되지만 관리 그룹에는 아직 포함되지 않은 기기.
	서버용 운영 체제를 실행하고 관리 그룹에 포함되어 있으며 *정상* 상태인 기기.
	서버용 운영 체제를 실행하고 관리 그룹에 포함되어 있으며 *경고* 상태인 기기.
	서버용 운영 체제를 실행하고 관리 그룹에 포함되어 있으며 *심각* 상태인 기기.
	서버용 운영 체제를 실행하고, 중앙 관리 서버와의 연결이 끊어진 관리 그룹에 포함되어 있는 기기.
	네트워크에서 발견되었으며 관리 그룹에 포함 안 된 모바일 기기.
	*정상* 상태로 관리 그룹에 포함된 모바일 기기.
	*경고* 상태로 관리 그룹에 포함된 모바일 기기.
	*심각* 상태로 관리 그룹에 포함된 모바일 기기.
	중앙 관리 서버와의 연결이 끊겼으며 관리 그룹에 포함된 모바일 기기.
	UEFI 보호 기기가 네트워크에서 탐지되었지만 관리 그룹에 포함되지 않았습니다. UEFI 보호 기기가 네트워크에 있습니다.
	UEFI 보호 기기가 네트워크에서 탐지되었지만 관리 그룹에 포함되지 않았습니다. UEFI 보호 기기가 네트워크에 있지 않습니다.
	*정상* 상태로 관리 그룹에 포함된 UEFI 보호 기기. UEFI 보호 기기가 네트워크에 있습니다.
	*정상* 상태로 관리 그룹에 포함된 UEFI 보호 기기. UEFI 보호 기기가 네트워크에 있지 않습니다.
	*경고* 상태로 관리 그룹에 포함된 UEFI 보호 기기. UEFI 보호 기기가 네트워크에 있습니다.
	*경고* 상태로 관리 그룹에 포함된 UEFI 보호 기기. UEFI 보호 기기가 네트워크에 있지 않습니다.
	*심각* 상태로 관리 그룹에 포함된 UEFI 보호 기기. UEFI 보호 기기가 네트워크에 있습니다.
	*심각* 상태로 관리 그룹에 포함된 UEFI 보호 기기. UEFI 보호 기기가 네트워크에 있지 않습니다.
	활성 정책.
	비활성 정책.
	기본 중앙 관리 서버에서 생성된 그룹에서 상속된 활성 정책.
	최상위 그룹에서 상속된 활성 정책.
	*스케줄됨* 또는 *완료* 상태인 작업(그룹 작업, 중앙 관리 서버 작업 또는 특정 기기 작업).
	*실행 중* 상태인 작업(그룹 작업, 중앙 관리 서버 작업 또는 특정 기기 작업).
	*실패* 상태인 작업(그룹 작업, 중앙 관리 서버 작업 또는 특정 기기 작업).

	기본 중앙 관리 서버에서 생성된 그룹에서 상속된 작업.
	최상위 그룹에서 상속된 작업.

관리 콘솔의 파일 상태 아이콘

Kaspersky Security Center 관리 콘솔의 파일 관리가 용이하도록 파일 이름 옆에 아이콘이 표시됩니다(아래 테이블 참조). 각 아이콘은 클라이언트 기기의 관리되는 Kaspersky 애플리케이션이 파일에 할당한 상태를 나타냅니다. **격리**, **백업** 및 **처리 안 된 위협** 폴더의 작업 영역에 아이콘이 표시됩니다.

개체가 있는 클라이언트 기기에 설치된 Kaspersky Endpoint Security에서 개체에 상태를 할당합니다.

아이콘과 파일 상태 간 대응 관계

아이콘	상태
	파일이 *감염* 상태입니다.
	파일이 *경고* 또는 *감염 의심* 상태입니다.
	파일이 *사용자가 추가* 상태입니다.
	파일이 *오탐* 상태입니다.
	파일이 *치료됨* 상태입니다.
	파일이 *삭제됨* 상태입니다.
	파일이 **격리** 폴더에서 *감염되지 않음, 암호가 걸려 있음* 또는 *Kaspersky로 보내야 함* 상태임. 아이콘 옆에 상태 설명이 없는 경우 클라이언트 기기의 관리되는 Kaspersky 애플리케이션이 알려지지 않은 상태를 Kaspersky Security Center에 보고했다는 의미입니다.
	파일이 **백업** 폴더에서 *감염되지 않음, 암호가 걸려 있음* 또는 *Kaspersky로 보내야 함* 상태임. 아이콘 옆에 상태 설명이 없는 경우 클라이언트 기기의 관리되는 Kaspersky 애플리케이션이 알려지지 않은 상태를 Kaspersky Security Center에 보고했다는 의미입니다.
	**처리 안 된 위협** 폴더의 파일이 *감염되지 않음, 암호가 걸려 있음* 또는 *Kaspersky로 보내야 함* 상태입니다. 아이콘 옆에 상태 설명이 없는 경우 클라이언트 기기의 관리되는 Kaspersky 애플리케이션이 알려지지 않은 상태를 Kaspersky Security Center에 보고했다는 의미입니다.

데이터 검색 및 내보내기

이 섹션에는 데이터 검색 방법 및 데이터 내보내기에 대한 정보가 포함되어 있습니다.

기기 찾기

Kaspersky Security Center에서는 지정된 기준에 따라 기기를 찾을 수 있습니다. 검색 결과는 텍스트 파일로 저장할 수 있습니다.

검색 기능을 사용하면 다음과 같은 기기를 찾을 수 있습니다:

- 중앙 관리 서버 및 해당 보조 중앙 관리 서버의 관리 그룹에 있는 클라이언트 기기.
- 중앙 관리 서버 및 그 보조 중앙 관리 서버에서 관리하는 미할당 기기.

관리 그룹에 포함된 클라이언트 기기를 검색하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 관리 그룹 폴더를 선택합니다.
2. 관리 그룹 폴더의 마우스 오른쪽 메뉴에서 **검색**를 선택합니다.
3. **검색** 창의 탭에서 기기의 검색 기준을 지정하고 **지금 찾기** 버튼을 누릅니다.

   이제 지정한 검색 기준에 맞는 기기가 **검색** 창 하단의 표에 표시됩니다.

미할당 기기를 찾으려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **미할당 기기** 폴더를 선택합니다.
2. **미할당 기기** 폴더의 마우스 오른쪽 메뉴에서 **검색**를 선택합니다.
3. **검색** 창의 탭에서 기기의 검색 기준을 지정하고 **지금 찾기** 버튼을 누릅니다.

   이제 지정한 검색 기준에 맞는 기기가 **검색** 창 하단의 표에 표시됩니다.

관리 그룹에 포함되었는지 여부에 관계없이 기기를 검색하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **중앙 관리 서버** 노드를 선택합니다.
2. 노드의 마우스 오른쪽 메뉴에서 **검색**를 선택합니다.
3. **검색** 창의 탭에서 기기의 검색 기준을 지정하고 **지금 찾기** 버튼을 누릅니다.

   이제 지정한 검색 기준에 맞는 기기가 **검색** 창 하단의 표에 표시됩니다.

검색 창에서 우측 상단의 드롭다운 목록을 사용하여 관리 그룹과 보조 중앙 관리 서버를 검색할 수도 있습니다. **미할당 기기** 폴더에서 **검색** 창을 연 경우에는 관리 그룹 및 보조 중앙 관리 서버 검색 기능을 사용할 수 없습니다.

기기를 찾기 위해 **검색** 창의 필드에서 정규식을 사용할 수 있습니다.

다음 항목에서 **검색** 창의 전체 텍스트 검색을 사용할 수 있습니다:

- **네트워크** 탭의 **설명** 필드
- **하드웨어** 탭의 **기기**, **공급사** 및 **설명** 필드

기기 검색 설정

아래에서는 관리 중인 기기 검색에 사용되는 설정에 대해 설명합니다. 검색 결과는 창 하단에 표시됩니다.

네트워크

네트워크 탭에서는 네트워크 데이터로 기기를 검색할 때 사용할 기준을 지정할 수 있습니다.

- **기기 이름 또는 IP 주소**

  기기의 Windows 네트워크 이름(NetBIOS 이름) 또는 IPv4 또는 IPv6 주소.

- **Windows 도메인**

  지정된 Windows 도메인에 포함된 모든 기기를 표시합니다.

- **관리 그룹**

  지정된 관리 그룹에 포함된 기기를 표시합니다.

- **설명**

  기기 속성 창의 텍스트: **일반** 섹션의 **설명** 필드.
  설명 필드에서 텍스트를 설명하기 위해 다음 문자를 사용할 수 있습니다.

  - 한 단어 내에서 찾으려면 다음과 같이 하십시오:

    - *****. 임의 개수의 문자열을 대체합니다.

    예:
    Server 또는 **Server's** 라는 단어를 설명하려면 **Server***를 입력하면 됩니다.

    - **?.** 표시는 단일 문자를 대체합니다.

    예:
    Window, **Windows** 등의 단어를 설명하려는 경우 **Windo?**를 입력하면 됩니다.
    별표(*****) 또는 물음표(**?**)는 쿼리의 첫 문자로 사용할 수 없습니다.

  - 여러 단어를 찾으려면 다음과 같이 하십시오:

    - 공백. 나열된 단어의 어느 하나라도 설명에 포함된 모든 기기가 표시됩니다.

    예:
    설명에 **Secondary** 또는 **Virtual**이라는 단어가 포함된 문구를 찾으려면 쿼리에 **Secondary Virtual**을 입력하면 됩니다.

    - **+**. 단어 앞에 더하기 기호를 입력하면 모든 검색 결과에 해당 단어가 포함됩니다.

    예:
    Secondary 및 **Virtual**이 모두 포함된 문구를 찾으려면 **+Secondary+Virtual** 쿼리를 입력합니다.

    - **-**. 단어 앞에 빼기 기호를 입력하면 검색 결과에 해당 단어가 포함되지 않습니다.

    예:

Secondary를 포함하고 **Virtual**은 포함하지 않는 문구를 찾으려면 **+Secondary-Virtual** 쿼리를 입력합니다.

- **"<텍스트>"**. 따옴표에 둘러싸인 텍스트가 검색 결과의 텍스트에 포함됩니다.

예:

Secondary Server의 단어 조합을 포함하는 문구를 찾으려면 쿼리에 **"Secondary Server"**를 입력하면 됩니다.

- **IP 범위**

  이 옵션을 사용하면 관련 기기가 포함되어야 하는 IP 범위의 첫 IP 주소와 마지막 IP 주소를 입력할 수 있습니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **다른 중앙 관리 서버에서 관리**

  다음 값 중 하나를 선택합니다:
  - **예**. 다른 중앙 관리 서버에서 관리하는 클라이언트 기기만 고려합니다.
  - **아니요**. 같은 중앙 관리 서버에서 관리하는 클라이언트 기기만 고려합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

태그

태그 탭에서는 이전에 관리 중인 기기 설명에 추가한 키워드(태그)를 기준으로 하여 기기 검색을 구성할 수 있습니다.

- **하나 이상의 지정 태그가 일치하면 적용**

  이 옵션을 사용하면 검색 결과에는 선택한 태그 중 적어도 하나와 일치하는 설명이 있는 기기가 표시됩니다.
  이 옵션이 비활성화되어 있으면 검색 결과에는 모든 선택한 태그와 일치하는 설명이 있는 기기만 표시됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **태그를 포함해야 함**

  이 옵션을 선택하는 경우 설명에 선택한 태그가 포함되어 있는 기기가 검색 결과에 표시됩니다. 기기를 찾으려는 경우 문자 수에 관계 없이 임의의 문자열을 나타내는 별표를 사용할 수 있습니다.
  기본적으로 이 옵션은 선택되어 있습니다.

- **태그를 제외해야 함**

  이 옵션을 선택하는 경우 설명에 선택한 태그가 포함되어 있지 않은 기기가 검색 결과에 표시됩니다. 기기를 찾으려는 경우 문자 수에 관계 없이 임의의 문자열을 나타내는 별표를 사용할 수 있습니다.

Active Directory

Active Directory 탭에서 Active Directory OU(조직 구성 단위) 또는 그룹에서 기기를 검색하도록 지정할 수 있습니다. 지정된 Active Directory OU의 모든 하위 OU에 있는 기기를 선택 항목에 포함할 수도 있습니다. 기기를 선택하려면 다음 설정을 정의하십시오.

- **기기가 Active Directory 조직 구성 단위에 있습니다**

  이 옵션을 사용하면 입력 필드에 지정한 Active Directory 조직 구성 단위의 기기가 조회에 포함됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **하위 조직 구성 단위까지 포함**

  이 옵션을 선택하면 지정한 도메인 조직 구성 단위의 모든 하위 조직 구성 단위에 있는 기기가 선택에 포함됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **이 기기는 Active Directory 그룹의 멤버입니다**

  이 옵션을 사용하면 입력 필드에 지정한 Active Directory 그룹의 기기가 조회에 포함됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

네트워크 활동

네트워크 활동 탭에서는 네트워크 활동으로 기기를 검색할 때 사용할 기준을 지정할 수 있습니다.

- **이 기기는 배포 지점입니다**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 배포 지점 역할을 하는 기기가 조회에 포함됩니다.
  - **아니요**. 배포 지점 역할을 하는 기기가 조회에 포함되지 않습니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **중앙 관리 서버와 계속 연결 유지**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **활성화됨**. 조회에 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택한 기기가 포함됩니다.
  - **비활성화됨**. 조회에 **중앙 관리 서버와 계속 연결 유지** 확인란의 선택을 취소한 기기가 포함됩니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **연결 프로필이 전환됨**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 연결 프로필이 전환된 후 중앙 관리 서버에 연결된 기기가 조회에 포함됩니다.
  - **아니요**. 연결 프로필이 전환된 후 중앙 관리 서버에 연결된 기기가 조회에 포함되지 않습니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **마지막 중앙 관리 서버 연결**

  이 확인란을 이용해 중앙 관리 서버에 마지막으로 연결한 시간에 따라 기기를 검색하는 기준을 설정할 수 있습니다.

  이 확인란을 선택하면 입력 필드에서 클라이언트 기기에 설치된 네트워크 에이전트와 중앙 관리 서버 간에 마지막으로 연결이 설정된 기간(날짜 및 시간)을 지정할 수 있습니다. 지정된 간격 내에 있는 기기가 조회에 포함됩니다.

  이 확인란이 비어 있으면, 기준은 적용되지 않습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **네트워크 검색 중 탐지된 새 기기**

  지난 며칠 동안 네트워크 검색을 통해 탐지된 새 기기를 검색합니다.

  이 옵션을 사용하면 **탐지 기간(일)** 필드에 지정된 기간 동안 기기 발견에서 탐지된 새 기기만 선택에 포함됩니다.

  이 옵션이 비활성화되어 있으면 선택에는 기기 발견에서 탐지된 모든 기기가 포함됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **기기 존재 확인**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 애플리케이션이 현재 네트워크에서 표시되는 기기를 조회에 포함시킵니다.
  - **아니요**. 애플리케이션이 현재 네트워크에 표시되지 않는 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

애플리케이션

애플리케이션 탭에서는 선택한 관리 대상 애플리케이션으로 기기를 검색할 때 사용할 기준을 지정할 수 있습니다.

- **애플리케이션 이름**

  Kaspersky 애플리케이션 이름별로 검색 수행 시 조회에 포함될 기기의 기준을 드롭다운 목록에서 지정할 수 있습니다.

  이 목록에는 관리자의 워크스테이션에서 관리 플러그인이 설치된 애플리케이션 이름만 표시됩니다.

  애플리케이션을 선택하지 않았다면, 이 기준은 적용되지 않습니다.

- **애플리케이션 버전**

  Kaspersky 애플리케이션 버전 이름별로 검색 수행 시 조회에 포함될 기기의 기준을 입력 필드에서 지정할 수 있습니다.

  버전 번호가 지정되지 않으면 기준이 적용되지 않습니다.

- **긴급 업데이트 이름**

  입력 필드에서 애플리케이션 이름 또는 업데이트 패키지 번호로 검색 수행 시 조회에 포함될 기기의 기준을 지정할 수 있습니다.

  필드를 비워두면 기준이 적용되지 않습니다.

- **마지막 모듈 업데이트**

  이 설정을 사용해 기기에 설치된 애플리케이션 모듈의 마지막 업데이트 시간으로 기기를 검색하기 위한 기준을 설정할 수 있습니다.

  이 확인란을 선택하면 입력 필드에서 기기에 설치된 애플리케이션 모듈의 마지막 업데이트가 수행된 시간 간격(날짜와 시간)을 지정할 수 있습니다.

  이 확인란이 비어 있으면, 기준은 적용되지 않습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **Kaspersky Security Center로 기기를 관리 중입니다**

  드롭다운 목록에서는 Kaspersky Security Center를 통해 관리되는 기기를 조회에 포함할 수 있습니다:

  - **예**. 애플리케이션이 Kaspersky Security Center를 통해 관리 중인 기기를 조회에 포함합니다.
  - **아니요**. 애플리케이션이 Kaspersky Security Center를 통해 관리되지 않는 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **보안 제품이 설치되어 있음**

  드롭다운 목록에서는 보안 제품이 설치된 모든 기기를 조회에 포함할 수 있습니다:

  - **예**. 애플리케이션이 보안 제품이 설치된 모든 기기를 조회에 포함합니다.
  - **아니요**. 애플리케이션이 보안 제품이 설치되지 않은 모든 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

운영 체제

운영 체제 탭에서는 운영 체제(OS) 유형별로 기기를 찾는 다음과 같은 기준을 설정할 수 있습니다.

- **운영 체제 버전**

  확인란을 선택하면 목록에서 운영 체제를 선택할 수 있습니다. 지정한 운영 체제가 설치된 기기가 검색 결과에 포함됩니다.

- **운영 체제 비트 크기**

  드롭다운 목록에서 운영 체제의 아키텍처를 선택할 수 있습니다. 선택한 아키텍처(**알 수 없음**, **x86**, **AMD64** 또는 **IA64**)에 따라 이동 규칙이 기기에 적용되는 방법이 결정됩니다. 기본적으로 목록에서 선택된 옵션은 없기 때문에 운영 체제 아키텍처는 정의되지 않게 됩니다.

- **운영 체제 서비스 팩 버전**

  이 필드에서는 사용자 운영 체제의 패키지 버전을 *X.Y* 형식으로 지정할 수 있습니다. 지정한 버전에 따라 이동 규칙이 장치에 적용되는 방법이 결정됩니다. 기본적으로 버전 값은 지정되지 않습니다.

- **운영 체제 빌드**

  > 이 설정은 Windows 운영 체제에만 적용됩니다.

  운영 체제의 빌드 번호입니다. 선택한 운영 체제의 빌드 번호가 이 번호와 같아야 하는지 아니면 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 빌드 번호를 제외한 모든 빌드 번호를 검색하도록 구성할 수도 있습니다.

- **운영 체제 릴리즈 ID**

  > 이 설정은 Windows 운영 체제에만 적용됩니다.

  운영 체제의 릴리즈 식별자(ID)입니다. 선택한 운영 체제의 릴리즈 ID가 이 ID와 같아야 하는지 아니면 이전/이후 ID여야 하는지를 지정할 수 있습니다. 지정한 릴리즈 ID 번호를 제외한 모든 번호를 검색하도록 구성할 수도 있습니다.

기기 상태

기기 상태 탭에서는 관리 중인 애플리케이션의 기기 상태를 기준으로 하여 기기 검색을 위한 기준을 지정할 수 있습니다.

- **기기 상태**

  정상, *심각* 또는 *경고* 기기 상태 중 하나를 선택할 수 있는 드롭다운 목록입니다.

- **실시간 보호 상태**

  실시간 보호 상태를 선택할 수 있는 드롭다운 목록입니다. 지정된 실시간 보호 상태의 기기가 조회에 포함됩니다.

- **기기 상태 설명**

  이 필드에서는 조건 옆의 확인란을 선택할 수 있습니다. 이러한 조건이 충족되면 *정상*, *심각* 또는 *경고* 상태 중 하나가 기기에 할당됩니다.

- **애플리케이션에서 정의된 기기 상태**

  실시간 보호 상태를 선택할 수 있는 드롭다운 목록입니다. 지정된 실시간 보호 상태의 기기가 조회에 포함됩니다.

보호 구성 요소

보호 구성 요소 탭에서는 보호 상태를 기준으로 클라이언트 기기의 검색 기준을 설정할 수 있습니다.

- **데이터베이스 배포 날짜**

  이 옵션을 선택하면 안티 바이러스 데이터베이스 배포 날짜를 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에 수행하려는 검색을 기반으로 기간을 설정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **마지막 검사**

  이 확인 옵션을 사용하면 마지막 악성 코드 검사 시간을 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에서 마지막 악성 코드 검사가 수행된 시간을 지정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **탐지된 위협 전체 개수**

  이 옵션을 사용하면 탐지된 바이러스 수를 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에 탐지된 바이러스 수에 대한 상한 및 하한 임계값을 설정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

자산 관리(소프트웨어)

자산 관리(소프트웨어) 탭에서는 설치된 애플리케이션을 기준으로 기기 검색을 구성할 수 있습니다.

- **애플리케이션 이름**

  애플리케이션을 선택할 수 있는 드롭다운 목록입니다. 지정된 애플리케이션이 설치된 기기가 조회에 포함됩니다.

- **애플리케이션 버전**

  선택한 애플리케이션의 버전을 지정할 수 있는 입력 필드입니다.

- **공급사**

  기기에 설치된 애플리케이션의 제조업체를 선택할 수 있는 드롭다운 목록입니다.

- **애플리케이션 상태**

  애플리케이션의 상태(*설치됨*, *설치 안 됨*)를 선택할 수 있는 드롭다운 목록입니다. 지정된 애플리케이션이 설치되어 있거나 설치되어 있지 않은 기기는 선택한 상태에 따라 조회에 포함됩니다.

- **업데이트로 찾기**

  이 옵션을 사용하면 관련 기기에 설치된 애플리케이션의 업데이트 세부 정보를 사용하여 검색이 수행됩니다. 확인란을 선택하면 **애플리케이션 이름**, **애플리케이션 버전** 및 **애플리케이션 상태** 필드가 각각 **업데이트 이름**, **업데이트 버전** 및 **상태**로 변경됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **비호환 보안 제품 이름**

  타사의 보안 제품을 선택할 수 있는 드롭다운 목록입니다. 검색 시 지정된 애플리케이션이 설치된 기기가 조회에 포함됩니다.

- **애플리케이션 태그**

  드롭다운 목록에서 애플리케이션 태그를 선택할 수 있습니다. 설명에 선택한 태그가 있는 애플리케이션이 설치된 모든 기기는 기기 조회에 포함됩니다.

중앙 관리 서버 계층 구조

기기를 검색하는 동안 보조 중앙 관리 서버에 저장된 정보를 고려하고 싶으면 **중앙 관리 서버 계층 구조** 탭에서 **보조 중앙 관리 서버의 데이터 포함** 확인란을 선택합니다. 그리고 입력 필드에 기기를 검색하는 동안 정보를 고려할 보조 중앙 관리 서버의 중첩 레벨을 지정할 수 있습니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

가상 컴퓨터

가상 컴퓨터 탭에서는 검색할 기기가 가상 컴퓨터인지 아니면 가상 데스크톱 인프라(VDI)의 일부인지를 기준으로 기기 검색을 구성할 수 있습니다.

- **이것은 가상 컴퓨터입니다**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **중요하지 않음**.
  - **아니요**. 가상 컴퓨터가 아닌 기기를 찾습니다.
  - **예**. 가상 컴퓨터인 기기를 찾습니다.

- **가상 컴퓨터 유형**

  드롭다운 목록에서 가상 컴퓨터 제조업체를 선택할 수 있습니다.
  이것은 가상 컴퓨터입니다 드롭다운 목록에서 **예** 또는 **중요하지 않음** 값을 선택하면 이 드롭다운 목록을 사용할 수 있습니다.

- **가상 데스크톱 인프라 소속**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **중요하지 않음**.
  - **아니요**. VDI(Virtual Desktop Infrastructure)의 일부가 아닌 기기를 찾습니다.
  - **예**. VDI(가상 데스크톱 인프라)의 일부인 기기를 찾습니다.

하드웨어

하드웨어 탭에서는 하드웨어를 기준으로 클라이언트 기기 검색을 구성할 수 있습니다.

- **기기**

  드롭다운 목록에서 다음과 같은 유닛 유형을 선택할 수 있습니다. 이 유닛이 모든 기기가 검색 결과에 포함됩니다.
  이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **공급사**

  드롭다운 목록에서 유닛 제조업체의 이름을 선택할 수 있습니다. 이 유닛이 모든 기기가 검색 결과에 포함됩니다.
  이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **설명**

  기기 또는 하드웨어 유닛의 설명. 이 필드에서 지정된 설명에 해당하는 기기가 조회에 포함됩니다.

  모든 유형에서의 기기 설명은 해당 기기의 속성 창에 입력될 수 있습니다. 이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **인벤토리 번호**

  이 필드에서 지정된 인벤토리 번호를 가진 기기는 조회에 포함됩니다.

- **CPU 주파수(MHz)**

  CPU 주파수 범위. 이러한 필드(포함)에 있는 주파수 범위와 일치하는 CPU를 가진 기기는 조회에 포함됩니다.

- **가상 CPU 코어**

  CPU에 있는 가상 코어의 숫자 범위. 이러한 필드(포함)에 있는 범위와 일치하는 CPU를 가진 기기는 조회에 포함됩니다.

- **하드 드라이브 용량(GB)**

  기기에 있는 하드 드라이브 용량 값의 범위입니다. 이러한 입력 필드(포함)에 있는 범위와 일치하는 하드 드라이브를 가진 기기는 조회에 포함됩니다.

- **RAM 크기(MB)**

  기기 RAM 크기에 대한 값 범위입니다. 이 입력 필드의 범위와 일치하는 RAM이 있는 기기(포괄적)가 선택 항목에 포함됩니다.

취약점 및 업데이트

취약점 및 업데이트 탭에서는 Windows 업데이트 경로에 따라 기기 검색을 위한 기준을 설정할 수 있습니다.

- **WUA가 중앙 관리 서버로 전환됨**

  드롭다운 목록에서 다음 검색 옵션 중 하나를 선택할 수 있습니다:

  - **예**. 이 옵션을 선택하면 Windows 업데이트를 통해 중앙 관리 서버에서 업데이트를 받는 기기가 검색 결과에 포함됩니다.
  - **아니요**. 이 옵션을 선택하면 Windows 업데이트를 통해 다른 경로에서 업데이트를 받는 기기가 결과에 포함됩니다.

사용자

사용자 탭에서는 운영 체제에 로그인한 사용자 계정에 따라 기기 검색을 위한 기준을 설정할 수 있습니다.

- **시스템에 마지막으로 로그인한 사용자**

  이 옵션을 사용하면 **찾기** 버튼을 눌러 사용자 계정을 지정할 수 있습니다. 지정한 사용자가 시스템에 대해 마지막 로그온을 수행한 기기가 검색 결과에 포함됩니다.

- **시스템에 적어도 한 번 이상 로그인한 사용자**

  이 옵션을 사용하면 **찾기** 버튼을 눌러 사용자 계정을 지정할 수 있습니다. 지정한 사용자가 한 번 이상 시스템에 로그인한 기기가 검색 결과에 포함됩니다.

관리 중인 애플리케이션에서 발생한 문제점

관리 중인 애플리케이션에서 발생한 문제점 탭에서는 관리 중인 애플리케이션이 제공하는 상태 설명에 따라 기기 검색을 설정할 수 있습니다.

- **기기 상태 설명**

  관리 중인 애플리케이션의 상태 설명에 대한 확인란을 선택할 수 있습니다. 이러한 상태 정보를 수신하면 해당 기기가 조회에 포함됩니다. 여러 애플리케이션에 해당되는 상태 하나를 조회할 경우 모든 목록에서 이 상태를 자동으로 조회하도록 할 수 있습니다.

관리 중인 애플리케이션의 구성 요소 상태

관리 중인 애플리케이션의 구성 요소 상태 탭에서는 관리 중인 애플리케이션의 구성 요소 상태에 따라 기기 검색을 위한 기준을 설정할 수 있습니다.

- **데이터 유출 방지 상태**

  데이터 유출 방지 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **협업 서버 보호 상태**

  서버 협업 보호 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **메일 서버의 안티 바이러스 보호 상태**

  메일 서버 보호 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **Endpoint Sensor 상태**

  엔드포인트 센서 구성 요소 상태(*알 수 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)를 기준으로 기기를 검색합니다.

암호화

- **암호화**

  AES(Advanced Encryption Standard) 대칭 블록 암호화 알고리즘입니다. 드롭다운 목록에서 암호화 키 크기(56비트, 128비트, 192비트 또는 256비트)를 선택할 수 있습니다.

  사용 가능한 값: *AES56*, *AES128*, *AES192* 및 *AES256*.

클라우드 세그먼트

클라우드 세그먼트 탭에서는 기기가 특정 클라우드 세그먼트에 속하는지 여부를 기준으로 검색을 구성할 수 있습니다.

- **기기가 클라우드 세그먼트에 있습니다**

  이 옵션을 사용하면 **찾기** 버튼을 눌러 검색할 세그먼트를 지정할 수 있습니다.

  자녀 개체 포함 옵션도 사용하는 경우 지정한 세그먼트의 모든 자녀 개체에서 검색이 실행됩니다.

  검색 결과에는 선택한 세그먼트의 기기만 포함됩니다.

- **API를 사용해 발견된 기기**

  드롭다운 목록에서 API 도구로 기기를 탐지할지 선택할 수 있습니다:

  - **AWS**. AWS API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 AWS 클라우드 환경에 있습니다.
  - **Azure**. Azure API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Azure 클라우드 환경에 있습니다.
  - **Google Cloud.** Google API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Google Cloud 환경에 있습니다.
  - **아니요**. AWS, Azure, Google API로 기기를 찾을 수 없으므로, 기기가 클라우드 환경 밖에 있거나 클라우드 환경 내에 있지만 어떠한 이유로 인해 API를 사용해 찾을 수 없습니다.
  - **값 없음**. 이 조건이 적용되지 않습니다.

애플리케이션 구성 요소

이 섹션에는 관리 콘솔에 해당 관리 플러그인이 설치되어 있는 애플리케이션 구성 요소 목록이 포함되어 있습니다.

애플리케이션 구성 요소 섹션에서는 선택한 애플리케이션을 지칭하는 구성 요소의 상태와 버전 번호에 따라 조회에 기기를 포함하기 위한 기준을 지정할 수 있습니다.

- **상태**

  애플리케이션이 중앙 관리 서버로 전송하는 구성 요소 상태에 따라 기기를 검색합니다. *기기에서 보내 온 데이터 없음*, *중지됨*, *시작 중*, *일시 중지됨*, *실행 중*, *오작동* 또는 *설치 안 됨* 상태 중 하나를 선택할 수 있습니다. 관리 중인 기기에 설치되어 있는 애플리케이션의 선택한 구성 요소 상태가 지정한 값이면 해당 기기가 기기 조회에 포함됩니다.

  애플리케이션에서 전송하는 상태:

  - *시작 중* - 구성 요소가 현재 초기화되고 있습니다.
  - *실행 중* - 구성 요소가 활성화되어 정상 작동하고 있습니다.
  - *일시 중지됨* - 구성 요소가 일시 중지되었습니다. 예를 들어 사용자가 관리 중인 애플리케이션에서 보호를 일시 중지했습니다.
  - *오작동* - 구성 요소 작동 중에 오류가 발생했습니다.
  - *중지됨* - 구성 요소가 비활성화되었으며 현재 작동하고 있지 않습니다.
  - *설치 안 됨* - 사용자가 애플리케이션의 사용자 지정 설치를 구성할 때 설치할 구성 요소를 선택하지 않았습니다.

  기기에서 보내 온 데이터 없음 상태는 다른 상태와 달리 애플리케이션에서 전송되지 않습니다. 이 옵션은 선택한 구성 요소 상태 관련 정보가 애플리케이션에 없음을 표시합니다. 예를 들어 선택한 구성 요소가 기기에 설치된 어떤 애플리케이션에도 속하지 않거나 기기가 꺼져 있으면 이 상태가 표시될 수 있습니다.

- **버전**

  목록에서 선택하는 구성 요소의 버전 번호에 따라 기기를 검색합니다. `3.4.1.0` 등의 버전 번호를 입력한 다음 선택한 구성 요소의 버전이 해당 번호와 같아야 하는지 아니면 그 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 버전을 제외한 모든 버전을 검색하도록 구성할 수도 있습니다.

문자열 값에 마스크 사용

문자열 값에서 마스크를 사용할 수 있습니다. 마스크를 만들 때, 다음 규칙을 사용할 수 있습니다:

- 와일드카드 문자(*)는 모든 개수의 문자열을 의미합니다.
- 물음표(?) – 모든 한자리 문자.
- [<범위>] – 지정된 범위나 집합 내의 단일 문자.
  예: [0-9] - 모든 숫자. [Abcdef] - a, b, c, d, e, f에 해당하는 모든 문자.

검색 필드에서 정규식 사용

검색 필드에서 다음 정규식을 사용해 특정 단어 및 문자를 검색할 수 있습니다:

- *. 임의의 모든 문자열을 대체합니다. Server, Servers 또는 Server room 등의 단어를 검색하려면 검색 필드에 `Server*` 식을 입력합니다.
- ?. 표시는 단일 문자를 대체합니다. Word 또는 Ward 등의 단어를 검색하려면 검색 필드에 `W?rd` 식을 입력합니다.

  > 검색 필드에 있는 텍스트는 ? 물음표로 시작할 수 없습니다.

- [<범위>]. 지정된 범위나 집합 내의 단일 문자를 대체합니다. 숫자를 검색하려면 검색 필드에 `[0-9]` 식을 입력합니다. a, b, c, d, e, f 등의 문자 중 하나를 찾으려면 검색 필드에 `[abcdef]` 식을 입력합니다.

전체 텍스트 검색을 실행하려면 다음 정규식을 사용합니다:

- 공백. 나열된 단어의 어느 하나라도 설명에 포함된 모든 기기가 표시됩니다. 단어 "Secondary"나 "Virtual" 중 하나라도 포함하거나 둘 다 포함하는 문구를 검색하려면 검색 필드에 `Secondary Virtual` 정규식을 입력합니다.
- 더하기 기호 (+), AND 또는 &&. 단어 앞에 더하기 기호를 입력하면 모든 검색 결과에 해당 단어가 포함됩니다. "Secondary"와 "Virtual"을 둘 다 포함하는 문구를 검색하려면 검색 필드에 `+Secondary+Virtual`, `Secondary AND Virtual`, `Secondary && Virtual`과 같은 정규식을 입력합니다.
- OR 또는 ||. 두 단어 사이에 사용하는 경우 두 단어 중 하나를 텍스트에서 찾을 수 있음을 나타냅니다. "Secondary"와 "Virtual" 둘 중 하나를 포함하는 문구를 검색하려면 검색 필드에 `Secondary OR Virtual`, `Secondary || Virtual`과 같은 정규식을 입력합니다.
- 빼기 기호 (-). 단어 앞에 빼기 기호를 입력하면 검색 결과에 해당 단어가 포함되지 않습니다. Secondary 단어는 포함해야 하고 Virtual 단어는 포함하지 않아야 하는 구를 검색하려면 검색 필드에 `+Secondary-Virtual` 식을 입력해야 합니다.
- `"<` 일부 텍스트 `>"`. 따옴표에 둘러싸인 텍스트가 검색 결과의 텍스트에 포함됩니다. 보조 서버 단어 조합을 포함하는 구를 검색하려면 검색 필드에 `"` 보조 서버 `"` 문구를 입력합니다.

다음 필터링 블록에서 전체 텍스트 검색을 사용할 수 있습니다:

- 이벤트 목록 필터링 블록(**이벤트** 및 **설명** 열 기준).
- 사용자 계정 필터링 블록(**이름** 열 기준).
- **목록에 표시** 섹션에서 필터링 기준으로 **그룹화 안 됨**이 선택된 경우, 자산 관리(소프트웨어) 필터링 블록(**이름** 열 기준).

대화상자에서 목록 내보내기

대화상자에서 목록 내보내기애플리케이션 대화상자에서 텍스트 파일로 개체 목록을 내보내기할 수 있습니다.

개체 목록 내보내기는 **파일로 내보내기** 버튼이 있는 대화상자 섹션에서 가능합니다.

작업 설정

이 섹션에는 Kaspersky Security Center에서 수행되는 작업의 모든 설정이 나와 있습니다.

일반 작업 설정

이 섹션은 대부분의 작업을 보고 구성할 수 있는 설정을 포함합니다. 사용 가능한 설정 목록은 구성 중인 작업에 따라 다릅니다.

작업 생성 중에 지정하는 설정

작업을 생성할 때 다음과 같은 설정을 지정할 수 있습니다. 이러한 설정 중 일부는 생성된 작업의 속성에서 수정할 수도 있습니다.

- 운영 체제 다시 시작 설정:
  - **기기 다시 시작 안 함**

    작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

  - **기기 다시 시작**

    이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

  - **사용자 확인 후 처리**

    클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **반복해서 물어보기(분)**

    이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

    기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

    이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

- **다음 시간 이후에 재시작(분)**

  사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- 작업 스케줄 설정:

  스케줄의 종류는 작업에 따라 다를 수 있습니다.

  - **시작 스케줄 설정:**

    - **N시간마다**

      작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

      작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

    - **N일마다**

      작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

      기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

    - **N분마다**

      작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

      기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

    - **요일별**

      이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

      기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **한번만**

  작업은 지정한 날짜와 시간(기본값은 작업 생성일)에 한 번 실행됩니다.

- **즉시**

  작업은 해당 설정이 저장되는 즉시 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**

  저장소에 업데이트가 다운로드되고 나면 작업이 실행됩니다. 예를 들어 취약점 및 필요한 업데이트 검색 작업에 이 스케줄을 사용할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 임의 지연(분)**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

- 이 작업이 할당되는 기기:
  - **중앙 관리 서버가 발견한 기기 중에서 선택**

    특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.

    예를 들어 미할당 기기에 네트워크 에이전트를 설치하는 작업에서 이 옵션을 사용할 수 있습니다.

  - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

    작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

    특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

  - **기기 선택 결과에 작업 할당**

    기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

    예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

  - **관리 그룹에 작업 할당**

    관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

    예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

    관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

- 계정 설정:
  - **기본 계정**

    해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **계정 지정**

    계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

  - **계정**

    작업 실행에 사용되는 계정입니다.

- **암호**

  작업을 실행할 계정의 암호입니다.

대상 기기에 네트워크 에이전트가 설치되어 있지 않은 경우 대상 기기에서 admin$ 공유에 접근할 때 사용할 계정을 지정해야 합니다. 지정한 계정은 데이터를 기기로 복사하는 용도로만 사용됩니다. 대상 기기에 네트워크 에이전트를 설치하면 데이터가 네트워크 에이전트를 통해 복사되므로 작업 생성 시 계정을 지정할 필요가 없습니다.

작업 생성 후에 지정하는 설정

다음 설정은 작업을 생성한 후에만 지정할 수 있습니다.

- 그룹 작업 설정:

  - **하위 그룹에 배포**

    이 옵션은 그룹 작업 설정에서만 사용할 수 있습니다.
    이 옵션이 활성화되면 작업 범위 에 다음이 포함됩니다.
    - 작업을 생성하는 동안 선택한 관리 그룹입니다.
    - 관리 그룹은 그룹 계층 에서 모든 수준에 있는 선택된 관리 그룹에 종속됩니다.

    이 옵션이 비활성화되면 작업 범위에는 작업을 생성하는 동안 선택한 관리 그룹만 포함됩니다.
    기본적으로 이 옵션은 켜져 있습니다.

  - **보조 및 가상 중앙 관리 서버에 배포**

    이 옵션을 사용하면 기본 중앙 관리 서버에서 유효한 작업이 보조 중앙 관리 서버(가상 서버 포함)에도 적용됩니다. 동일한 유형의 작업이 보조 중앙 관리 서버에 이미 있는 경우 두 작업 모두 보조 중앙 관리 서버(기본 작업 및 기본 중앙 관리 서버에서 상속된 작업)에 적용됩니다.
    이 옵션은 **하위 그룹에 배포** 옵션이 활성화된 경우에만 사용할 수 있습니다.
    기본적으로 이 옵션은 비활성화되어 있습니다.

- 고급 스케줄 설정:

  - **작업 시작 전에 Wake-on-LAN 기능으로 기기 켜기(분)**

    작업이 시작되기 전 지정된 시간에 기기의 운영 체제가 시작됩니다. 기본 기간은 5분입니다.

    작업을 시작하려 할 때 꺼져 있는 기기를 포함하여 작업 범위의 모든 클라이언트 기기에서 작업을 실행하려는 경우 이 옵션을 활성화합니다.

    작업이 완료된 후 기기를 자동으로 끄려면 **작업 완료 후 기기 종료** 옵션을 활성화합니다. 이 옵션은 같은 창에서 찾을 수 있습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- **작업 완료 후 기기 종료**

  예를 들어 매주 금요일 업무 시간 후에 클라이언트 기기에 업데이트를 설치한 다음 주말 동안은 해당 기기를 꺼 두는 업데이트 설치 작업의 경우 이 옵션을 활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **작업이 다음 시간보다 오래 실행되면 중지(분)**

  작업 완료 여부에 관계없이 지정된 시간이 경과한 후 작업이 자동으로 중지됩니다.
  실행 시간이 너무 오래 걸리는 작업을 중단(중지)하려는 경우 이 옵션을 활성화합니다.
  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 작업 실행 시간은 120분입니다.

- 공지 설정:

  - **작업 기록 저장** 블록:

    - **다음 기간 동안 중앙 관리 서버에 저장(일)**

      작업 범위의 모든 클라이언트 기기에서 수행하는 작업 실행과 관련된 애플리케이션 이벤트가 지정된 기간(일) 동안 중앙 관리 서버에 저장됩니다. 이 기간이 지나면 중앙 관리 서버에서 해당 정보가 삭제됩니다.

      기본적으로 이 옵션은 켜져 있습니다.

    - **기기의 OS 이벤트 로그에 저장**

      작업 실행과 관련된 애플리케이션 이벤트가 각 클라이언트 기기의 Windows 이벤트 로그에 로컬로 저장됩니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    - **중앙 관리 서버의 OS 이벤트 로그에 저장**

      작업 범위의 모든 클라이언트 기기에서 수행하는 작업 실행과 관련된 애플리케이션 이벤트가 중앙 관리 서버 OS(운영 체제)의 Windows 이벤트 로그에 중앙 집중식으로 저장됩니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    - **모든 이벤트 저장**

      이 옵션을 선택하면 작업과 관련된 모든 이벤트가 이벤트 로그에 저장됩니다.

    - **작업 진행 상태와 관련된 이벤트 저장**

      이 옵션을 선택하면 작업 실행과 관련된 이벤트만 이벤트 로그에 저장됩니다.

    - **작업 실행 결과만 저장**

      이 옵션을 선택하면 작업 결과와 관련된 이벤트만 이벤트 로그에 저장됩니다.

- **작업 실행 결과를 관리자에게 알림**

  관리자가 작업 실행 결과에 대한 알림을 받는 방법(이메일, SMS, 실행 파일 실행)을 선택할 수 있습니다. 알림을 구성하려면 **설정** 링크를 누릅니다.

  기본적으로는 모든 알림 방법이 비활성화됩니다.

- **오류만 알림**

  이 옵션을 활성화하면 작업 실행 완료 시 오류가 발생할 때만 관리자에게 알림이 전송됩니다.

  이 옵션을 비활성화하면 작업 실행이 완료될 때마다 관리자에게 알림이 전송됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- 보안 설정
- 작업 범위 설정

  작업 범위가 결정되는 방법에 따라 다음과 같은 설정이 제공됩니다:

  - **기기**

    관리 그룹에 따라 작업 범위가 결정되는 경우 이 그룹을 볼 수 있습니다. 이 그룹에서는 변경을 수행할 수 없습니다. 하지만 **작업 제외 그룹**를 설정할 수 있습니다.

    기기 목록에 따라 작업 범위가 결정되는 경우에는 기기를 추가하고 제거하여 이 목록을 수정할 수 있습니다.

  - **기기 선택**

    작업이 적용되는 기기 조회를 변경할 수 있습니다.

  - **작업 제외 그룹**

    작업이 적용되지 않는 기기 그룹을 지정할 수 있습니다. 작업이 적용되는 관리 그룹의 하위 그룹만 제외할 수 있습니다.

- **리비전 내역**

중앙 관리 서버 저장소에 업데이트 다운로드 작업 설정

작업 생성 중에 지정하는 설정

작업을 생성할 때 다음과 같은 설정을 지정할 수 있습니다. 이러한 설정 중 일부는 생성된 작업의 속성에서 수정할 수도 있습니다.

- **업데이트 경로**

  중앙 관리 서버의 업데이트 경로로 다음과 같은 리소스를 사용할 수 있습니다:

  - Kaspersky 업데이트 서버

    Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다. 기본적으로 중앙 관리 서버는 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버를 구성할 수 있습니다.

    기본적으로 선택됩니다.

  - 기본 중앙 관리 서버

    이 리소스는 보조 또는 가상 중앙 관리 서버용으로 생성한 작업에 적용됩니다.

  - 로컬 또는 네트워크 폴더

    최신 업데이트가 포함된 로컬 또는 네트워크 폴더입니다. 네트워크 폴더는 FTP/HTTP 서버이거나 SMB 공유일 수 있습니다. 네트워크 폴더 인증이 필요할 시, SMB 프로토콜만 지원합니다. 로컬 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다.

    > 업데이트 경로에 사용되는 FTP 또는 HTTP 서버나 네트워크 폴더는 Kaspersky 업데이트 서버 사용 시에 생성되는 구조와 일치하는 폴더 구조(업데이트 포함)를 포함해야 합니다.

- **기타 설정**

  보조 중앙 관리 서버 강제 업데이트

  이 옵션을 활성화하면 새 업데이트가 다운로드되는 즉시 중앙 관리 서버가 보조 중앙 관리 서버에서 업데이트 작업을 시작합니다. 업데이트 작업은 보조 중앙 관리 서버의 작업 속성에 구성된 업데이트 경로를 사용하여 시작됩니다.

  해당 옵션을 비활성화하면 보조 중앙 관리 서버의 업데이트 작업이 스케줄에 따라 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

  추가 폴더에 다운로드한 업데이트 복사

  중앙 관리 서버에서 업데이트를 수신한 후 이를 지정된 폴더에 복사합니다. 네트워크에서 업데이트 배포를 수동으로 관리하려는 경우 이 옵션을 사용합니다.

이 옵션을 사용할 수 있는 상황의 예로는, 조직 네트워크가 여러 독립 서브넷으로 구성되어 있으며 각 서브넷의 기기가 다른 서브넷에는 액세스할 수 없는 경우를 들 수 있습니다. 하지만 모든 서브넷의 기기는 공통 네트워크 공유에 액세스할 수 있습니다. 이 경우 서브넷 중 하나의 중앙 관리 서버가 Kaspersky 업데이트 서버에서 업데이트를 다운로드하도록 설정하고 이 옵션을 활성화한 다음 해당 네트워크 공유를 지정할 수 있습니다. 다른 중앙 관리 서버에 대한 저장소에 업데이트 다운로드 작업에서 업데이트 경로와 같은 네트워크 공유를 지정합니다.

다운로드한 업데이트를 로컬 폴더에 복사하도록 선택한 경우, 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다. 폴더 경로는 기기의 운영 체제에 따라 달라집니다. 로컬 폴더는 Linux 기반 중앙 관리 서버에 있으므로 POSIX 형식의 경로(예: /path/to/dir)를 지정해야 합니다.

Linux 기반 중앙 관리 서버에 있는 네트워크 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기에서 해당 네트워크 폴더를 미리 탑재해 접근할 수 있어야 합니다. 폴더 접근은 SMB 프로토콜을 통해 이루어집니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

복사가 완료되기 전에 기기 및 보조 중앙 관리 서버로 강제 업데이트 안 함

메인 업데이트 폴더에서 추가 업데이트 폴더로 업데이트가 복사되어야만 클라이언트 기기와 보조 중앙 관리 서버의 업데이트 다운로드 작업이 시작됩니다.

클라이언트 기기와 보조 중앙 관리 서버가 추가 네트워크 폴더에서 업데이트를 다운로드하는 경우 이 옵션을 활성화해야 합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

작업 생성 후에 지정하는 설정

다음 설정은 작업을 생성한 후에만 지정할 수 있습니다.

- **설정** 섹션, **업데이트 내용** 블록

  diff 파일 다운로드

  이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 검증** 섹션

  배포하기 전에 업데이트 검증 절차 수행

  중앙 관리 서버가 업데이트 경로에서 업데이트를 다운로드하고 임시 저장소에 해당 업데이트를 저장한 다음, **업데이트 확인 작업** 필드에 정의된 작업을 실행합니다. 작업이 성공적으로 완료되면 임시 저장소에서 중앙 관리 서버의 공유 폴더로 업데이트가 복사되고, 중앙 관리 서버를 업데이트 경로로 설정한 모든 기기로 업데이트가 배포됩니다. 즉, 스케줄 유형이 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**인 작업이 시작됩니다. 업데이트를 저장소로 다운로드하는 작업은 *업데이트 검증* 작업이 완료된 후에만 완료됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

업데이트 확인 작업

이 작업은 중앙 관리 서버가 업데이트 경로 역할을 하는 모든 기기에 다운로드한 업데이트가 배포되기 전에 해당 업데이트를 확인합니다.

이 필드에서 이전에 생성된 *업데이트 검증* 작업을 지정할 수 있습니다. 또는 *새 업데이트 검증* 작업을 생성할 수 있습니다.

배포 지점의 저장소로 업데이트 다운로드 작업 설정

작업 생성 중에 지정하는 설정

작업을 생성할 때 다음과 같은 설정을 지정할 수 있습니다. 이러한 설정 중 일부는 생성된 작업의 속성에서 수정할 수도 있습니다.

- **업데이트 경로**

  배포 지점의 업데이트 경로로 다음과 같은 리소스를 사용할 수 있습니다.

  - Kaspersky 업데이트 서버

    Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다.

    이 옵션은 기본적으로 선택되어 있습니다.

  - 기본 중앙 관리 서버

    이 리소스는 보조 또는 가상 중앙 관리 서버용으로 생성한 작업에 적용됩니다.

  - 로컬 또는 네트워크 폴더

    최신 업데이트가 포함된 로컬 또는 네트워크 폴더입니다. 네트워크 폴더는 FTP/HTTP 서버이거나 SMB 공유일 수 있습니다. 네트워크 폴더 인증이 필요할 시, SMB 프로토콜만 지원합니다. 로컬 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다.

    업데이트 경로에 사용되는 FTP 또는 HTTP 서버나 네트워크 폴더는 Kaspersky 업데이트 서버 사용 시에 생성되는 구조와 일치하는 폴더 구조(업데이트 포함)를 포함해야 합니다.

- **기타 설정 → 업데이트 저장 폴더**

  저장된 업데이트를 저장하기 위한 지정된 폴더의 경로입니다. 지정된 폴더 경로를 클립보드에 복사할 수 있습니다. 그룹 작업에 대해 지정된 폴더의 경로를 변경할 수 없습니다.

작업 생성 후에 지정하는 설정

작업이 생성된 후에만 **업데이트 내용** 블록의 **설정** 섹션에서 다음 설정을 지정할 수 있습니다.

diff 파일 다운로드

이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

취약점 및 필요한 업데이트 검색 작업 설정

작업 생성 중에 지정하는 설정

작업을 생성할 때 다음과 같은 설정을 지정할 수 있습니다. 이러한 설정 중 일부는 생성된 작업의 속성에서 수정할 수도 있습니다.

- **Microsoft에서 작성한 취약점 및 업데이트 검색**

  취약점 및 업데이트를 검색할 때 Kaspersky Security Center는 현재 사용 가능한 Microsoft 업데이트 소스의 해당 Microsoft 업데이트에 대한 정보를 사용합니다.

  예를 들어 Microsoft 업데이트 및 타사 애플리케이션 업데이트에 대해 다양한 설정을 사용하는 다양한 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  선택 사항인 Microsoft Windows 업데이트에 대한 정보는 중앙 관리 서버로 전송되지 않습니다.

- **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트**

  관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결됩니다. 다음 서버는 Microsoft 업데이트의 소스로 작동할 수 있습니다.

  - Kaspersky Security Center 중앙 관리 서버(네트워크 에이전트 정책 설정 참조)
  - 조직의 네트워크에 Microsoft WSUS(Windows 서버 업데이트 서비스)가 배포된 Windows Server
  - Microsoft 업데이트 서버

  이 옵션을 활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결하여 해당하는 Microsoft Windows 업데이트 관련 정보를 새로 고칩니다.

  이 옵션을 비활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 이전에 Microsoft 업데이트 소스에서 받은 해당 Microsoft Windows 업데이트에 관한 정보를 사용합니다.

  Microsoft 업데이트 소스에 연결할 때는 리소스가 많이 사용될 수 있습니다. **소프트웨어 업데이트 및 취약점** 섹션에 있는 네트워크 에이전트 정책의 속성이나 다른 작업에서 이 업데이트 소스에 대한 정기 연결을 설정하는 경우 이 옵션을 비활성화할 수 있습니다. 이 옵션을 비활성화하고 싶지 않으면, 서버 과부하를 줄이기 위해 360분 내에 작업 시작 시간을 랜덤하게 지정하도록 작업 스케줄을 구성할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

다음 옵션 조합의 조합으로 네트워크 에이전트 정책 설정 업데이트를 받는 옵션을 정의합니다.

- 관리 중인 기기의 Windows 업데이트 에이전트는 *취약점 및 필요한 업데이트 검색* 작업의 속성에서 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화하고 네트워크 에이전트 정책 설정에서 **Windows 업데이트 검색 모드** 옵션을 **액티브**으로 설정했을 때만 업데이트 서버에 연결하여 업데이트를 가져옵니다.

- *취약점 검사* 작업을 수행할 때 네트워크 에이전트가 Microsoft Windows 업데이트 경로에 대한 연결 시작과 업데이트 다운로드가 필요하지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하는 동시에 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화된 상태로 유지해야 합니다. 이를 통해 리소스를 절약하고 이전에 받은 Windows 업데이트를 사용하여 취약점을 검사할 수 있습니다. 다른 방법으로 Microsoft Windows 업데이트 수신을 구성하는 경우 수동 모드를 사용할 수 있습니다. Microsoft Windows 업데이트 수신이 다른 방법으로 구성되지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하지 마십시오. 이 경우 업데이트 정보가 수신되지 않습니다.

- **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션의 상태(활성화 또는 비활성화)에 무관하게 **Windows 업데이트 검색 모드** 옵션이 **비활성화됨**로 설정되면 Kaspersky Security Center는 업데이트 정보를 요청하지 않습니다.

- **Kaspersky에서 작성한 타사 취약점 및 업데이트 검색**

  이 옵션을 활성화하면 Kaspersky Security Center는 **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정** 아래에 지정된 폴더와 Windows 레지스트리에서 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)에 필요한 업데이트와 취약점을 검색합니다. 지원되는 타사 애플리케이션의 전체 목록은 Kaspersky에서 관리합니다.

  이 옵션을 비활성화하면 Kaspersky Security Center는 타사 애플리케이션에 필요한 업데이트와 취약점을 검색하지 않습니다. 예를 들어 Microsoft Windows 업데이트 및 타사 애플리케이션 업데이트에 대해 다른 설정을 사용하는 다른 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  - **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정**

    Kaspersky Security Center가 취약점을 수정하고 업데이트를 설치해야 하는 타사 애플리케이션을 검색하는 폴더입니다. 시스템 변수를 사용할 수 있습니다.

    애플리케이션이 설치된 폴더를 지정합니다. 목록에는 기본적으로 대다수 애플리케이션이 설치된 시스템 폴더가 포함됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

  작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **고급 진단 파일의 최대 크기(MB)**

  기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업 설정

작업 생성 중에 지정하는 설정

작업을 생성할 때 다음과 같은 설정을 지정할 수 있습니다. 이러한 설정 중 일부는 생성된 작업의 속성에서 수정할 수도 있습니다.

- **업데이트 설치 규칙을 지정합니다**

  이러한 규칙은 클라이언트 기기의 업데이트 설치에 적용됩니다. 규칙을 지정하지 않으면 작업이 수행되지 않습니다. 규칙을 사용하는 작업에 대한 정보는 업데이트 설치에 대한 규칙을 참조하십시오.

- **기기 재시작 또는 종료 시 설치 시작**

  이 옵션을 활성화하면 기기가 다시 시작되거나 종료되기 전에 업데이트가 설치됩니다. 그렇지 않으면 업데이트는 스케줄에 따라 설치됩니다.

  업데이트 설치가 기기 성능에 영향을 줄 수 있는 경우 이 옵션을 사용합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **필요한 일반 시스템 구성 요소 설치**

  이 옵션을 활성화하면 업데이트를 설치하기 전에 애플리케이션은 업데이트 설치를 설치하기 위해 필요한 모든 일반 시스템 구성 요소(선결 조건)를 자동으로 설치합니다. 이러한 필수 구성 요소의 예로는 운영 체제 업데이트 등이 있습니다.

  이 옵션을 비활성화하는 경우에는 필수 구성 요소를 수동으로 설치해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 시 새 애플리케이션 버전의 설치 허용**

  이 옵션을 활성화하면 업데이트 시 소프트웨어 애플리케이션의 새 버전이 설치되는 경우 업데이트가 허용됩니다.

  이 옵션을 비활성화하면 소프트웨어가 업그레이드되지 않습니다. 그러면 소프트웨어의 새 버전을 수동으로 또는 다른 작업을 통해 설치할 수 있습니다. 예를 들어 새 소프트웨어 버전이 회사 인프라를 지원하지 않거나 테스트 인프라에서 업그레이드를 확인하려는 경우 이 옵션을 사용할 수 있습니다.

기본적으로 이 옵션은 켜져 있습니다.

애플리케이션을 업그레이드하면 클라이언트 기기에 설치된 종속 애플리케이션의 오작동이 발생할 수 있습니다.

- **업데이트를 기기에 다운로드만 하고 설치는 하지 않음**

  이 옵션을 활성화하면 애플리케이션은 기기에 업데이트를 다운로드하지만 자동으로 해당 업데이트를 설치하지는 않습니다. 그러면 다운로드한 업데이트를 수동으로 설치할 수 있습니다.

  Microsoft 업데이트는 시스템 Windows 저장소에 다운로드됩니다. 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트는 **업데이트 다운로드 경로** 필드에 지정된 폴더에 다운로드됩니다.

  이 옵션을 비활성화하면 업데이트가 기기에 자동으로 설치됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

  - **업데이트 다운로드 경로**

    이 폴더는 타사 애플리케이션(Kaspersky이 아닌 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트를 다운로드하는 데 사용됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

  작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

  - **고급 진단 파일의 최대 크기(MB)**

    기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

작업 생성 후에 지정하는 설정

아래 나열된 섹션 설정은 작업이 생성된 후에만 지정할 수 있습니다. 작업 설정에 대한 전체 설명은 일반 작업 설정을 참조하십시오.

- **일반**. 이 섹션에는 작업에 대한 일반 정보가 표시됩니다. 또한 *필요한 업데이트 설치 및 취약성 수정* 작업을 적용할 기기를 지정할 수 있습니다:

  - **하위 그룹에 배포**

    이 옵션은 그룹 작업 설정에서만 사용할 수 있습니다.

    이 옵션이 활성화되면 작업 범위 에 다음이 포함됩니다.

    - 작업을 생성하는 동안 선택한 관리 그룹입니다.
    - 관리 그룹은 그룹 계층 에서 모든 수준에 있는 선택된 관리 그룹에 종속됩니다.

    이 옵션이 비활성화되면 작업 범위에는 작업을 생성하는 동안 선택한 관리 그룹만 포함됩니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **보조 및 가상 중앙 관리 서버에 배포**

    이 옵션을 사용하면 기본 중앙 관리 서버에서 유효한 작업이 보조 중앙 관리 서버(가상 서버 포함)에도 적용됩니다. 동일한 유형의 작업이 보조 중앙 관리 서버에 이미 있는 경우 두 작업 모두 보조 중앙 관리 서버(기본 작업 및 기본 중앙 관리 서버에서 상속된 작업)에 적용됩니다.

    이 옵션은 **하위 그룹에 배포** 옵션이 활성화된 경우에만 사용할 수 있습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- 설치할 업데이트

  설치할 업데이트 섹션에서는 작업에서 설치되는 업데이트 목록을 확인할 수 있습니다. 적용된 작업 설정과 일치하는 업데이트만 표시됩니다.

- 업데이트 테스트 설치:

  - **검사 안 함**. 업데이트의 테스트 설치를 수행하려면 이 옵션을 선택합니다.
  - **선택한 기기에서 검사 실행**. 선택한 기기에 테스트 업데이트를 설치하려면 이 옵션을 선택합니다. **추가** 버튼을 누르고 업데이트의 테스트 설치를 수행하려는 기기를 선택합니다.
  - **선택한 그룹의 모든 기기에서 검사 실행**. 기기 그룹에 테스트 업데이트를 설치하려면 이 옵션을 선택합니다. **테스트 그룹 지정** 필드에서 테스트 설치를 수행하려는 기기 그룹을 지정합니다.
  - **지정한 비율만큼 기기에서 검사 실행**. 대상 기기의 일부에 테스트 업데이트를 설치하려면 이 옵션을 선택합니다. **모든 대상 기기 대비 검증 테스트 기기 비율** 필드에 업데이트의 테스트 설치를 수행하려는 기기의 비율을 지정합니다.

글로벌 서브넷 목록

이 섹션에서는 규칙에서 사용할 수 있는 글로벌 서브넷 목록에 대해 설명합니다.

네트워크의 서브넷 관련 정보를 저장하려는 경우 사용하는 각 중앙 관리 서버에 대해 글로벌 서브넷 목록을 설정할 수 있습니다. 이 목록에서는 {IP 주소, 마스크} 쌍과 일치하는 지사 등의 실제 단위를 설정할 수 있습니다. 네트워킹 규칙과 설정에서 이 목록의 서브넷을 사용할 수 있습니다.

글로벌 서브넷 목록에 서브넷 추가

글로벌 서브넷 목록에 서브넷을 설명과 함께 추가할 수 있습니다.

글로벌 서브넷 목록에 서브넷을 추가하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. **속성** 창이 열리면 **섹션** 창에서 **글로벌 서브넷 목록**를 선택합니다.
4. **추가** 버튼을 누릅니다.
   새 서브넷 창이 열립니다.
5. 다음 필드에 내용을 입력합니다:
   - **일반 설정**

     추가하는 서브넷의 서브넷 IP 주소입니다.
   - **서브넷 마스크**

     추가하는 서브넷의 서브넷 마스크입니다.
   - **이름**

     서브넷의 이름입니다. 이 이름은 글로벌 서브넷 목록 내에서 고유해야 합니다. 목록에 이미 있는 이름을 입력하면 색인이 추가됩니다. 예를 들면 다음과 같습니다: ~~1, ~~2
   - **설명**

     설명에는 이 서브넷이 있는 지사에 대한 몇 가지 추가 정보가 포함될 수 있습니다. 이 텍스트는 트래픽 제한 규칙 목록 등 해당 서브넷이 있는 모든 목록에 표시됩니다.

     이 필드는 필수 항목이 아니므로 비워 두어도 됩니다.
6. **확인**를 누릅니다.

서브넷 목록에 서브넷이 표시됩니다.

글로벌 서브넷 목록에서 서브넷 속성 보기 및 수정

글로벌 서브넷 목록에서 서브넷 속성을 보고 수정할 수 있습니다.

글로벌 서브넷 목록에서 서브넷 속성을 보거나 수정하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 필요한 중앙 관리 서버 노드를 선택합니다.
2. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. **속성** 창이 열리면 왼쪽 **섹션** 창에서 **글로벌 서브넷 목록**를 선택합니다.
4. 목록에서 원하는 서브넷을 선택합니다.
5. **속성** 버튼을 누릅니다.
   새 서브넷 창이 열립니다.
6. 필요한 경우 서브넷의 설정을 변경합니다.
7. **확인**를 누릅니다.

   변경을 한 경우 변경 내용이 저장됩니다.

Windows, Linux, macOS용 네트워크 에이전트 사용: 비교

네트워크 에이전트 사용은 기기의 운영 체제에 따라 달라집니다. 네트워크 에이전트 정책 및 설치 패키지 설정도 운영 체제에 따라 달라집니다. 아래 표는 Windows, macOS 및 Linux 운영 체제에서 사용할 수 있는 네트워크 에이전트 기능 및 사용 시나리오를 비교한 것입니다.

네트워크 에이전트 기능 비교

네트워크 에이전트 기능	Windows	Linux	macOS
설치			
Kaspersky Security Center 설치 후 네트워크 에이전트 설치 패키지 자동 생성	✓	–	–
Kaspersky Security Center의 원격 설치 작업에 포함된 특수 옵션을 사용하여 강제 모드로 설치	✓	✓	✓
기기 사용자에게 Kaspersky Security Center에서 생성된 독립 실행형 패키지의 링크를 전송해 설치	✓	✓	✓
Kaspersky Security Center에서 제공하는 디스크 이미지 처리용 도구를 사용하여 운영 체제와 네트워크 에이전트가 있는 관리자 하드 드라이브의 이미지를 복제해 설치	✓	–	–
제삼자 도구를 사용하여 운영 체제 및 네트워크 에이전트로 관리자 하드 드라이브의 이미지를 복제하여 설치	✓	✓	✓
애플리케이션 원격 설치용 타사 도구를 사용해 설치	✓	✓	✓
기기에서 애플리케이션 인스톨러를 실행하여 수동으로 설치	✓	✓	✓
숨김 모드로 네트워크 에이전트 설치	✓	✓	✓

네트워크 에이전트 기능	Windows	Linux	macOS
클라이언트 기기를 중앙 관리 서버에 수동으로 연결. klmover 유틸리티	✓	✓	✓
Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 설치	✓	✓	—
키 자동 배포	✓	✓	✓
강제 동기화	✓	✓	✓
배포 지점			
배포 지점으로 사용	✓	✓	✓
배포 지점 자동 할당	✓	✓ NLA(네트워크 위치 인식) 사용 안 함.	✓ NLA(네트워크 위치 인식) 사용 안 함.
네트워크 검색	✓ • Windows 네트워크 검색 • IP 범위 검색 • 도메인 컨트롤러 검색(Microsoft Active Directory)	✓ • IP 범위 검색 • Zeroconf 폴링 • 도메인 컨트롤러 검색(Microsoft Active Directory, Samba 4 Active Directory)	—
배포 지점 측에서 KSN 프록시 서비스 실행	✓	✓	—
Kaspersky 업데이트 서버를 통해 관리 중인 기기에 업데이트를 배포하는 배포 지점 저장소로 업데이트 다운로드	✓	✓	— Linux 또는 macOS를 실행하는 하나 이상의 기기가 배포 지점 작업의 저장소로 업데이트 다운로드 작업 범위에 있는 경우 모든 Windows 기기에서 작업이 성공적으로 완료되어도 작업은 실패 상태로 완료됩니다.
애플리케이션 설치 푸시	✓	제한됨: Linux 배포 지점을 사용하여 Windows 기기에서 푸시 설치를 수행할 수 없습니다.	제한됨: macOS 배포 지점을 사용하여 Windows 기기에서 푸시 설치를 수행할 수 없습니다.
푸시 서버로 사용	✓	✓	—
타사 애플리케이션 처리			
기기에 애플리케이션 원격 설치	✓	—	✓ 자세한 내용은 macOS 기기에 애플리케이션 원격 설치를 참조하십시오.
소프트웨어 업데이트	✓	—	—
네트워크 에이전트 정책에 운영 체제 업데이트 구성	✓	—	—
소프트웨어 취약점 정보 보기	✓	—	—
취약점이 있는지 애플리케이션 검사	✓	—	—
기기에 설치된 소프트웨어 인벤토리	✓	✓	—
가상 컴퓨터			
가상 컴퓨터에 네트워크 에이전트 설치	✓	✓	✓
VDI(가상 데스크톱 인프라) 설정 최적화	✓	✓	✓
동적 가상 컴퓨터 지원	✓	✓	✓
기타			
Windows 데스크톱 공유를 사용하여 원격 클라이언트 기기에서의 활동 감사	✓	—	—

네트워크 에이전트 기능	Windows	Linux	macOS
안티 바이러스 보호 상태 모니터링	✓	✓	✓
기기 다시 시작 관리	✓	–	–
파일 시스템 롤백 지원	✓	✓	✓
네트워크 에이전트를 연결 게이트웨이로 사용	✓	✓	✓
연결 관리자	✓	✓	✓
하나의 중앙 관리 서버에서 다른 중앙 관리 서버로 네트워크 에이전트 전환(네트워크 위치에 따라 자동 수행)	✓	–	✓
클라이언트 기기와 중앙 관리 서버 간 연결 상태 확인. klnagchk 유틸리티	✓	✓	✓
클라이언트 기기 데스크톱에 원격 연결	✓	–	✓ VNC(가상 네트워크 컴퓨팅) 시스템 사용
마이그레이션 마법사를 통한 독립 실행형 설치 패키지 다운로드	✓	✓	✓
Zeroconf 폴링	–	✓	–
클라이언트 기기의 하드웨어 정보 보기	✓	✓ Linux 기기의 하드웨어 정보는 해당 기기에 설치된 네트워크 에이전트가 중앙 관리 서버로 전송하며, 이는 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에 대한 관리 중인 기기 설정의 설명에 명시된 정보로 제한됩니다.	✓ macOS 기기의 하드웨어 정보는 해당 기기에 설치된 네트워크 에이전트가 중앙 관리 서버로 전송하며, 이는 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에 대한 관리 중인 기기 설정의 설명에 명시된 정보로 제한됩니다.

Kaspersky Security Center 웹 콘솔

Kaspersky Security Center 웹 콘솔(이하 Kaspersky Security Center 웹 콘솔이라고도 함)은 Kaspersky 애플리케이션을 통해 보호되는 네트워크의 보안 시스템 상태를 관리하는 웹 애플리케이션입니다.

이 애플리케이션을 사용하여 다음 작업을 수행할 수 있습니다.

- 조직의 보안 시스템 상태 관리.
- 네트워크에 있는 기기에 Kaspersky 애플리케이션 설치 및 설치된 애플리케이션 관리.
- 네트워크에 있는 기기용으로 생성된 정책 관리.
- 사용자 계정 관리.
- 기기에 설치된 애플리케이션용 작업 관리.
- 보안 시스템 상태에 대한 리포트 보기.
- 시스템 관리자 및 기타 IT 전문가에게 리포트 전달 관리.

하드웨어 및 소프트웨어 요구 사항에 대한 자세한 내용은 웹 콘솔 요구 사항을 참조하십시오.

Kaspersky Security Center 웹 콘솔은 중앙 관리 서버와 기기가 브라우저를 통해 상호 작용할 수 있도록 하는 웹 인터페이스를 제공합니다. 중앙 관리 서버는 기기에 설치된 Kaspersky 애플리케이션을 관리하기 위한 애플리케이션입니다. 중앙 관리 서버는 SSL(Secure Sockets Layer)로 보호되는 채널을 통해 네트워크의 기기에 연결합니다. 웹 브라우저를 사용하여 Kaspersky Security Center 웹 콘솔에 연결하면 브라우저에서 Kaspersky Security Center 웹 콘솔 서버와 연결을 확립합니다.

Kaspersky Security Center 웹 콘솔은 다음과 같이 작동합니다.

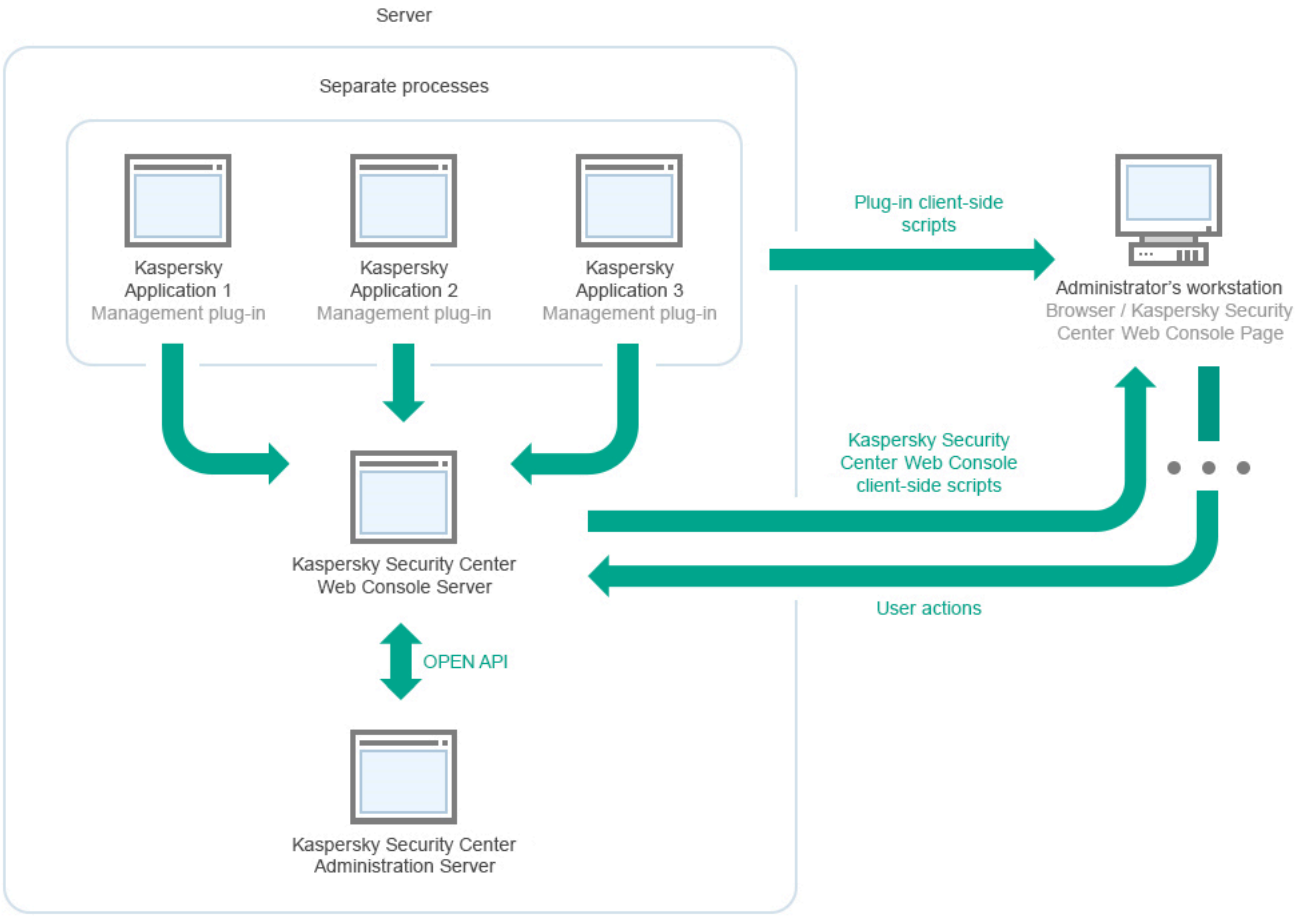
1. 브라우저를 사용하여 Kaspersky Security Center 웹 콘솔에 연결합니다. 그러면 웹 포털 인터페이스의 페이지가 표시됩니다.
2. 웹 포털 컨트롤을 사용하여 실행할 명령을 선택합니다. Kaspersky Security Center 웹 콘솔은 다음 작업을 수행합니다.
   - 기기 목록 보기와 같은 정보 수신에 사용되는 명령을 선택한 경우 Kaspersky Security Center 웹 콘솔은 중앙 관리 서버에 대한 정보 요청을 생성하고 필요한 데이터를 받은 다음 쉽게 확인할 수 있는 형식으로 해당 데이터를 브라우저에 보냅니다.
   - 애플리케이션 원격 설치와 같은 관리에 사용되는 명령을 선택한 경우에는 Kaspersky Security Center 웹 콘솔이 브라우저에서 명령을 받아 중앙 관리 서버에 보냅니다. 그런 다음 애플리케이션은 중앙 관리 서버에서 결과를 받아 쉽게 확인할 수 있는 형식으로 해당 결과를 브라우저에 보냅니다.

Kaspersky Security Center 웹 콘솔은 다중 언어 애플리케이션입니다. 애플리케이션을 다시 열지 않고도 언제든지 인터페이스 언어를 변경할 수 있습니다. Kaspersky Security Center 웹 콘솔을 Kaspersky Security Center와 함께 설치하면 Kaspersky Security Center 웹 콘솔에 설치 파일과 동일한 인터페이스 언어가 설정됩니다. Kaspersky Security Center 웹 콘솔만 설치하는 경우 애플리케이션에 운영 체제와 동일한 인터페이스 언어가 설정됩니다. Kaspersky Security Center 웹 콘솔에서 설치 파일 또는 운영 체제의 언어를 지원하지 않는 경우 기본적으로 영어가 설정됩니다.

Kaspersky Security Center 웹 콘솔에서는 모바일 기기 관리를 지원하지 않습니다. 그러나 Microsoft Management Console을 사용해 모바일 기기를 관리 그룹에 추가했다면 해당 기기가 Kaspersky Security Center 웹 콘솔에도 표시됩니다.

Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔의 배포 다이어그램

아래 그림은 Kaspersky Security 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔의 배포 다이어그램을 보여줍니다.



Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔의 배포 다이어그램

보호되는 기기에 설치된 Kaspersky 애플리케이션용 관리 플러그인(각 애플리케이션당 플러그인 하나)은 Kaspersky Security Center 웹 콘솔 서버와 함께 배포됩니다.

관리자는 워크스테이션에서 브라우저를 사용하여 Kaspersky Security Center 웹 콘솔에 접근합니다.

Kaspersky Security Center 웹 콘솔에서 특정 작업을 수행할 때 Kaspersky Security Center 웹 콘솔 서버는 OpenAPI를 통해 Kaspersky Security Center 중앙 관리 서버와 통신합니다. Kaspersky Security Center 웹 콘솔 서버는 Kaspersky Security Center 중앙 관리 서버에 필요한 정보를 요청하고 작업 결과를 Kaspersky Security Center 웹 콘솔에 표시합니다.

Kaspersky Security Center 웹 콘솔에서 사용되는 포트

아래 표에는 Kaspersky Security Center 웹 콘솔 서버(Kaspersky Security Center 웹 콘솔이라고도 함)가 설치된 기기에서 열어야 하는 포트가 나열되어 있습니다.

Kaspersky Security Center 웹 콘솔에서 사용되는 포트

포트 번호	서비스 이름	프로토콜	포트 용도	범위
2001	Kaspersky Security Center 제품 플러그인 서버	HTTPS	"Kaspersky Security Center 웹 콘솔 관리 서비스"의 요청 수신을 위해 관리 플러그인 프로세스에서 사용하는 API 포트	관리 플러그인의 node.exe 프로세스 실행
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTPS	같은 기기에서 실행 중인 "Kaspersky Security Center 웹 콘솔 관리 서비스"의 요청 수신을 위해 사용하는 API 포트	Kaspersky Security Center 웹 콘솔 구성 요소 업데이트
2005	Kaspersky Security Center 웹 콘솔	HTTPS	같은 기기에서 실행 중인 "Kaspersky Security Center 웹 콘솔 관리 서비스"의 요청 수신을 위해 사용하는 API 포트	Kaspersky Security Center 웹 콘솔의 node.exe 프로세스 실행
3333	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 인증 엔드포인트 포트	ID 및 접근 관리자
4004	Kaspersky OSMP Facade Service	HTTPS	OAuth2.0 ID 제공자 포트	ID 및 접근 관리자
4444	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 토큰 자체 검사 엔드포인트 포트	ID 및 접근 관리자
8200	—	HTTP	HashiCorp Vault를 통해 인증서를 생성하는 데 사용되는 API 포트(자세한 내용은 HashiCorp Vault 웹사이트 참조)	Kaspersky Security Center 웹 콘솔 설치 및 Kaspersky Security Center 웹 콘솔 구성 요소 업데이트
4150, 4151, 4152	Kaspersky Security Center Web Console Message Queue	HTTPS	Kaspersky Security Center 웹 콘솔과 관리 플러그인 프로세스 간 통신에 사용되는 메시지 브로커의 API 포트	Kaspersky Security Center 웹 콘솔과 관리 플러그인 간의 상호 작용

아래 표에는 Kaspersky Security Center 웹 콘솔 서버가 설치된 기기에서 열 필요가 없는 포트가 나열되어 있습니다. 그러나 Kaspersky Security Center 웹 콘솔은 이러한 포트를 ID 및 액세스 관리용으로 사용합니다.

Kaspersky Security Center 웹 콘솔에서 ID 및 액세스 관리용으로 사용하는 포트

포트 번호	서비스 이름	프로토콜	포트 용도	범위
4445	Kaspersky OSMP KAS Service	HTTPS	OAuth2.0 인증 엔드포인트 포트를 위해 Kaspersky Security Center 웹 콘솔로부터 구성을 수신하는 기본 ID 및 액세스 관리 포트(OAuth 2.0에 관한 자세한 정보는 OAuth 웹사이트 참조)	ID 및 접근 관리자
2444	Kaspersky OSMP Facade Service	HTTPS	ID 및 액세스 관리 구성용 포트	ID 및 접근 관리자
2445	Kaspersky OSMP Facade Service	HTTPS	"Kaspersky OSMP KAS Service"를 "Kaspersky OSMP Facade Service"에 연결하기 위한 포트	ID 및 접근 관리자

Kaspersky Security Center 웹 콘솔 인터페이스

Kaspersky Security Center는 Kaspersky Security Center 웹 콘솔 인터페이스로 관리합니다.

Kaspersky Security Center 웹 콘솔 창에는 다음 항목이 포함됩니다.

- 창 왼쪽의 메인 메뉴
- 창 오른쪽의 작업 영역

메인 메뉴

메인 메뉴는 다음 섹션으로 구성됩니다.

- **중앙 관리 서버**. 현재 연결된 중앙 관리 서버의 이름을 표시합니다. 설정 아이콘( )을 클릭하여 중앙 관리 서버 속성을 엽니다.
- **모니터링 및 보고**. 인프라, 보호 상태, 통계의 개요를 확인할 수 있습니다.
- **에셋(기기)**. 에셋에 대한 도구와 작업 및 Kaspersky 애플리케이션 정책이 포함되어 있습니다.
- **사용자 및 역할**. 사용자 및 역할을 관리하고, 사용자에게 역할을 할당하여 사용자 권한을 구성하고, 정책 프로필을 역할에 연결할 수 있습니다.
- **작업**. 애플리케이션 라이센스, 암호화된 드라이브 및 암호화 이벤트 확인 및 관리, 타사 애플리케이션 관리를 포함한 다양한 작업이 포함됩니다. 또한, 애플리케이션 저장소에 대한 접근 권한을 제공합니다.
- **발견 및 배포**. 네트워크를 검색하여 클라이언트 기기를 검색하고, 수동 또는 자동으로 관리 그룹에 기기를 배포할 수 있습니다. 이 섹션에는 빠른 시작 마법사 및 보호 배포 마법사도 포함되어 있습니다.
- **마켓플레이스**. Kaspersky 비즈니스 솔루션 전체 범위에 대한 정보가 포함되어 있으며, Kaspersky 웹사이트에서 필요한 솔루션을 선택한 후 해당 솔루션을 구매할 수 있습니다.
- **설정**. 웹 플러그인의 현재 상태를 백업하여 나중에 저장된 상태를 복원할 수 있습니다. 인터페이스 언어 또는 테마와 같이 인터페이스 모양과 관련된 개인 설정이 포함되어 있습니다.
- **계정 메뉴**. Kaspersky Security Center 도움말 링크를 포함합니다. 또한 Kaspersky Security Center에서 로그아웃하고 Kaspersky Security Center 웹 콘솔 버전과 설치된 관리 웹 플러그인 목록을 확인할 수 있습니다.

작업 공간

Kaspersky Security Center 웹 콘솔 인터페이스 창의 섹션에서 확인을 위해 선택한 정보가 작업 영역에 표시됩니다. 또한 정보 표시 방법 구성에 사용할 수 있는 제어 요소를 포함합니다.

메인 메뉴의 섹션 고정 및 고정 해제

Kaspersky Security Center 웹 콘솔의 섹션을 고정하여 즐겨찾기에 추가하고 메인 메뉴의 **고정됨** 섹션에서 빠르게 이용할 수 있습니다.

> 고정된 항목이 없으면 메인 메뉴에 **고정됨** 섹션이 표시되지 않습니다.

페이지만 표시하는 섹션을 고정할 수 있습니다. 예를 들어 **에셋(기기) → 관리 중인 기기**로 이동하면 기기의 표가 있는 페이지가 열립니다. 즉, **관리 중인 기기** 섹션을 고정할 수 있습니다. 메인 메뉴에서 섹션을 선택한 후에도 창 또는 항목이 표시되지 않는다면 해당 섹션을 고정할 수 없습니다.

섹션을 고정하려면:

1. 메인 메뉴에서 고정할 섹션 위로 마우스 커서를 이동합니다.
   고정 아이콘(📌)이 표시됩니다.
2. 고정 아이콘(📌)을 클릭합니다.

   섹션이 고정되고 **고정됨** 섹션에 표시됩니다.

즐겨찾기에서 항목을 고정 해제하여 제거할 수도 있습니다.

섹션을 고정 해제하려면:

1. 메인 메뉴에서 **고정됨** 섹션으로 이동합니다.
2. 고정을 해제할 섹션에 마우스 커서를 이동하고 고정 해제 아이콘(📌)을 클릭합니다.

   해당 섹션이 즐겨찾기에서 제거됩니다.

시나리오: Kaspersky Security Center 웹 콘솔의 설치 및 초기 설정

이 시나리오에서는 Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔을 설치하고, 빠른 시작 마법사를 사용하여 중앙 관리 서버 초기 설정을 수행하고, 보호 배포 마법사를 사용하여 관리 중인 기기에 Kaspersky 애플리케이션을 설치하는 방법을 설명합니다.

Kaspersky Security Center 웹 콘솔 설치 및 초기 설정은 다음과 같은 단계로 진행됩니다.

1. **DBMS(데이터베이스 관리 시스템) 설치**

   Kaspersky Security Center에서 사용할 DBMS를 설치하거나 기존 DBMS를 사용합니다.
   선택한 DBMS를 설치하는 방법에 대한 정보는 해당 설명서를 참조하십시오.

2. **중앙 관리 서버, 관리 콘솔, 네트워크 에이전트 설치**

   관리 콘솔과 네트워크 에이전트의 서버 버전은 중앙 관리 서버와 함께 설치됩니다.

   Kaspersky Security Center 중앙 관리 서버 설치 중에 Kaspersky Security Center 웹 콘솔을 같은 기기에 설치할지 지정할 수 있습니다. 같은 기기에 두 구성 요소를 모두 설치하기로 선택한 경우 Kaspersky Security Center 웹 콘솔이 자동으로 설치되므로 별도로 설치할 필요가 없습니다. Kaspersky Security Center 웹 콘솔을 다른 기기에 설치하려면, Kaspersky Security Center 중앙 관리 서버를 설치한 후 Kaspersky Security Center 웹 콘솔을 설치합니다.

3. **Kaspersky Security Center 웹 콘솔 설치**

   이전 단계에서 Kaspersky Security Center 중앙 관리 서버와 함께 Kaspersky Security Center 웹 콘솔을 설치하지 않았다면, 별도로 Kaspersky Security Center 웹 콘솔을 설치합니다. Kaspersky Security Center 웹 콘솔은 다른 기기나 중앙 관리 서버가 설치된 같은 기기에 설치할 수 있습니다.

4 초기 설정 수행

중앙 관리 서버 설치가 완료되면 중앙 관리 서버에 처음 연결될 때 빠른 시작 마법사가 자동으로 시작됩니다. 기존 요구 사항에 따라 중앙 관리 서버의 초기 구성을 수행합니다. 초기 구성 단계 중에 마법사는 기본 설정을 사용하여 보호 기능을 배포하는 데 필요한 정책과 작업을 만듭니다. 그러나 기본 설정으로는 조직의 요구를 가장 효율적으로 충족하지 못할 수도 있습니다. 필요한 경우 정책과 작업의 설정을 편집할 수 있습니다.

5 Kaspersky Security Center 라이센싱(선택 사항)

관리 콘솔을 지원하는 Kaspersky Security Center 기본 기능에는 라이센스가 필요하지 않습니다. 취약점 및 패치 관리, 모바일 기기 관리, SIEM 시스템과의 통합을 포함하여 하나 이상의 추가 기능을 사용하려면 상업용 라이센스가 필요합니다. 이러한 기능에 대한 키 파일 또는 활성화코드를 빠른 시작 마법사의 해당 단계에서나 수동으로 추가할 수 있습니다.

6 네트워크에 연결된 기기 발견

이 단계는 빠른 시작 마법사에서 처리됩니다. 기기를 수동으로 발견할 수도 있습니다. Kaspersky Security Center는 네트워크에서 탐지된 모든 기기의 주소와 이름을 수신합니다. 그러면 Kaspersky Security Center를 사용하여 탐지된 기기에 Kaspersky 애플리케이션 및 다른 공급업체의 소프트웨어를 설치할 수 있습니다. Kaspersky Security Center는 정기적으로 기기 발견을 시작합니다. 이는 네트워크에 새 인스턴스가 있을 경우 자동으로 탐지한다는 뜻입니다.

7 관리 그룹으로 기기 정렬

이 단계는 빠른 시작 마법사에서 처리되지만, 탐지된 기기를 그룹에 수동으로 이동할 수도 있습니다.

8 네트워크에 연결된 기기에 네트워크 에이전트 및 보안 제품 설치

기업 네트워크에 보호 기능을 배포한다는 것은 기기를 발견하는 동안 중앙 관리 서버가 탐지한 기기에 네트워크 에이전트 및 보안 제품(예: Kaspersky Endpoint Security for Windows)을 설치한다는 것입니다.

애플리케이션을 원격 설치하려면 보호 배포 마법사를 실행합니다.

보안 제품은 바이러스 및 위협을 가하는 기타 프로그램으로부터 기기를 보호합니다. 네트워크 에이전트는 기기와 중앙 관리 서버가 서로 통신하도록 합니다. 네트워크 에이전트 설정은 기본적으로 자동 구성됩니다.

네트워크에 연결된 기기에 보안 제품 및 네트워크 에이전트 설치를 시작하기 전에 해당 기기가 접근 가능한 상태인지(켜져 있는지) 확인하십시오.

9 클라이언트 기기에 라이센스 키 배포

클라이언트 기기에서 관리 중인 보안 제품을 활성화하기 위해 해당 기기에 라이센스 키를 배포합니다.

10 Kaspersky Security for Mobile 설치 (선택 사항)

회사 모바일 기기를 관리할 계획이라면 Kaspersky Security for Mobile 도움말의 지침에 따라 Kaspersky Endpoint Security for Android 배포에 대한 정보를 참조하십시오.

11 Kaspersky 애플리케이션 정책 구성

기기마다 서로 다른 애플리케이션 설정을 적용하려는 경우 기기 중심 보안 관리 및/또는 사용자 중심 보안 관리를 사용할 수 있습니다. 기기 중심 보안 관리는 정책과 작업을 사용하여 구현할 수 있습니다. 특정 조건을 충족하는 기기에만 작업을 적용할 수 있습니다. 기기 필터링용 조건을 설정하려면 기기 조회 및 태그를 사용합니다.

12 네트워크 보호 상태 모니터링

대시보드의 위젯을 사용하여 네트워크를 모니터링하고, Kaspersky 애플리케이션에서 리포트를 생성하고, 관리 중인 기기의 애플리케이션에서 수신된 이벤트 조회를 구성 및 확인하고, 알림 목록을 확인할 수 있습니다.

설치

이 섹션에서는 Kaspersky Security Center 및 Kaspersky Security Center 웹 콘솔 설치에 대해 설명합니다.

Kaspersky Security Center 설치(표준 설치)

이 절차에서는 Kaspersky Security Center를 설치하는 방법을 설명합니다. 설치 전에 데이터베이스 관리 시스템을 설치해야 합니다.

Kaspersky Security Center를 설치하려면 다음 단계를 따릅니다.

1. 관리 권한이 있는 계정으로 ksc_<빌드 번호>_full_<현지화 언어>.exe 실행 파일을 실행합니다.
2. 애플리케이션 조회 창이 열리면 **Kaspersky Security Center 설치**를 누릅니다.

   Kaspersky Security Center 중앙 관리 서버 설치 마법사가 시작됩니다.
3. 시작 페이지에서 **다음** 버튼을 사용해 마법사를 진행합니다.
4. Microsoft .NET Framework가 설치되어 있지 않으면 설치합니다.
5. 라이센스 계약서 및 개인정보취급방침의 조건에 동의합니다.
6. 설치 유형을 선택합니다. 평가용으로는 기본값인 **표준** 값을 그대로 유지하는 것이 좋습니다.
7. 같은 기기에 Kaspersky Security Center 웹 콘솔을 설치하려는 경우 **Kaspersky Security Center 웹 콘솔 설치** 확인란을 선택합니다.

   확인란 선택을 해제하면 나중에 같은 기기나 다른 기기에 별도로 Kaspersky Security Center 웹 콘솔을 설치할 수 있습니다.
8. 네트워크 크기를 선택합니다. 평가용으로는 기본값인 **네트워크에 100대 미만의 기기가 있음** 값을 그대로 유지하는 것이 좋습니다.
9. 이전에 설치한 데이터베이스 서버의 유형을 선택합니다.
10. 이전에 설치한 데이터베이스 서버에 대해 연결 파라미터를 지정합니다.
11. 이전에 설치한 데이터베이스 서버에 대해 인증 파라미터를 지정합니다.
12. **설치** 버튼을 눌러 설치를 시작합니다.
13. 설치가 정상적으로 완료되면, 마법사를 닫은 후 바로 관리 콘솔을 시작할지 선택합니다.

    Kaspersky Security Center 웹 콘솔을 열도록 선택하면 로그인 화면이 열립니다. 그러면 빠른 시작 마법사를 사용하여 중앙 관리 서버의 초기 구성을 수행할 수 있습니다.

    Kaspersky Security Center 웹 콘솔은 이미 설치된 경우에만 열 수 있습니다. Kaspersky Security Center 설치 중에 Kaspersky Security Center 웹 콘솔을 설치하거나 별도로 설치하지 않았다면 Kaspersky Security Center 웹 콘솔을 열 수 없습니다.

14. 관리 콘솔 창이 열리면 설치된 중앙 관리 서버를 누릅니다.

15. 중앙 관리 서버 인증서 창이 열리면 **예** 버튼을 눌러 계속 진행합니다.

    웹 기반 관리 콘솔에서 중앙 관리 서버 빠른 시작 마법사를 실행하지 않았다면 해당 마법사가 시작됩니다.

문제 해결

중앙 관리 서버 인증서 창이 열리지 않고 연결 오류가 표시되면 다음을 시도해 보십시오.

1. Windows에서 **서비스(제어판 → 관리 도구 → 서비스)**를 엽니다. Kaspersky Security Center 네트워크 에이전트 및 Kaspersky Security Center 중앙 관리 서버 서비스가 실행되고 있는지 확인합니다.

2. Windows에서 **이벤트 뷰어(제어판 → 관리 도구 → 이벤트 뷰어)**를 열고 **애플리케이션 및 서비스 로그 → Kaspersky 이벤트 로그**를 선택합니다. 로그에 오류가 없으며 **중앙 관리 서버 <버전 번호>가 실행되고 있음**과 같은 이벤트가 포함되어 있는지 확인합니다.

Kaspersky Security Center 웹 콘솔 설치

이 섹션에서는 Kaspersky Security Center 웹 콘솔 서버(또는 Kaspersky Security Center 웹 콘솔)를 별도로 설치하는 방법에 대해 설명합니다. 설치 전에 Kaspersky Security Center 중앙 관리 서버 및 DBMS를 설치해야 합니다. Kaspersky Security Center 웹 콘솔은 Kaspersky Security Center가 설치된 기기나 다른 기기에 설치할 수 있습니다.

Kaspersky Security Center 웹 콘솔을 설치하려면 다음 단계를 따릅니다.

1. 관리자 권한이 있는 계정으로 ksc-web-console-<version number>.<build number>.exe 실행 파일을 실행합니다.

   설치 마법사가 시작됩니다.

2. 설치 마법사의 언어를 선택합니다.

3. 시작 창에서 **다음**을 누릅니다.

4. **라이센스 계약서** 창에서 EULA(최종 사용자 라이센스 계약서)의 약관을 확인하고 해당 내용에 동의합니다. EULA에 동의하면 설치가 계속 진행되며, 동의하지 않으면 **다음** 버튼을 사용할 수 없습니다.

5. **대상 폴더** 창에서 Kaspersky Security Center 웹 콘솔을 설치할 폴더(기본값: %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console)를 선택합니다. 이 폴더가 없는 경우에는 설치를 진행하는 동안 자동으로 생성됩니다.

   찾기 버튼을 사용하여 대상 폴더를 변경할 수 있습니다.

6. **Kaspersky Security Center 웹 콘솔 연결 설정** 창에서 다음 정보를 지정합니다:

   - Kaspersky Security Center 웹 콘솔 주소(기본값: 127.0.0.1).

   - Kaspersky Security Center 웹 콘솔이 수신 연결에 사용할 포트, 즉 브라우저에서 Kaspersky Security Center 웹 콘솔에 접근 권한을 부여하는 포트(기본값: 8080).

   주소와 포트 번호는 그대로 유지하는 것이 좋습니다.

   원한다면 **테스트**를 클릭하여 선택한 포트를 사용할 수 있는지 확인할 수 있습니다.

   Kaspersky Security Center 웹 콘솔 활동 로그 기록을 활성화하려면 해당하는 옵션을 선택합니다. 이 옵션을 선택하지 않으면 Kaspersky Security Center 웹 콘솔 로그 파일이 생성되지 않습니다.

7. **계정 설정** 창에서 계정 이름과 암호를 지정합니다.

   기본 계정을 사용하는 것이 좋습니다.

8. **클라이언트 인증서** 창에서 다음 중 하나를 선택합니다:

   - **새 인증서 생성**. 브라우저 인증서가 없으면 이 옵션을 사용하는 것이 좋습니다.
   - **기존 인증서 선택**. 브라우저 인증서가 이미 있으면 이 옵션을 선택하고 인증서 경로를 지정할 수 있습니다.
   - 새 인증서 생성 선택 시, Kaspersky Security Center 웹 콘솔을 열면 브라우저에서 Kaspersky Security Center 웹 콘솔에 대한 연결이 비공개가 아니며 Kaspersky Security Center 웹 콘솔 인증서가 유효하지 않다고 알립니다. 이 경고는 Kaspersky Security Center 웹 콘솔 인증서가 Kaspersky Security Center에서 자체 서명되고 자동 생성되기 때문에 표시됩니다. 이 경고를 없애려면, 사용자의 인프라에서 신뢰할 수 있고 사용자 지정 인증서의 요구 사항을 충족하는 인증서를 만듭니다. 그런 다음 **클라이언트 인증서** 창에서 **기존 인증서 선택** 옵션을 선택한 다음 사용자 지정 인증서의 경로를 지정합니다.

   PFX 형식의 인증서는 Kaspersky Security Center 웹 콘솔에서 지원되지 않습니다. 이러한 인증서를 사용하려면 먼저 Windows용 OpenSSL과 같은 OpenSSL 기반 교차 플랫폼 유틸리티를 사용하여 지원되는 PEM 형식으로 변환해야 합니다.

9. **신뢰할 수 있는 중앙 관리 서버** 창에서 중앙 관리 서버가 목록에 있는지 확인한 후에 **다음**을 눌러 설치 프로그램의 마지막 창으로 이동합니다.

   새 중앙 관리 서버를 목록에 추가해야 한다면 **추가** 버튼을 클릭합니다. 열린 창에서 신뢰하는 새 중앙 관리 서버의 속성을 지정합니다:

   - **중앙 관리 서버 이름**

     Kaspersky Security Center 웹 콘솔의 로그인 창에 표시될 Kaspersky 중앙 관리 서버 이름입니다.

   - **중앙 관리 서버 주소**

     중앙 관리 서버를 설치하는 기기의 IP 주소입니다.

   - **중앙 관리 서버 포트**

     Kaspersky Security Center 웹 콘솔이 중앙 관리 서버에 연결하는 데 사용하는 OpenAPI 포트입니다(기본값은 13299).

   - **중앙 관리 서버 인증서**

     인증서 파일은 중앙 관리 서버가 설치된 기기에 저장됩니다. 중앙 관리 서버 인증서의 기본 경로:

     - Windows – %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
     - Linux의 경우—/var/opt/kaspersky/klnagent_srv/1093/cert/

     중앙 관리 서버가 설치된 기기에 Kaspersky Security Center 웹 콘솔을 설치한다면 위에 제공된 경로 중 하나를 사용하십시오. 그렇지 않으면 중앙 관리 서버가 설치된 기기에서 Kaspersky Security Center 웹 콘솔을 설치한 기기로 인증서 파일을 복사한 다음 인증서의 로컬 경로를 지정합니다.

10. **신원 및 접근 관리자(IAM)** 창에서 ID 및 액세스 관리(또는 IAM)를 설치하고 싶은지 지정하십시오. ID 및 액세스 관리를 설치하도록 선택한 경우 다음 포트 번호를 지정합니다.

    - **KAS 관리자 포트**. 기본적으로 포트 4445는 Kaspersky Security Center 웹 콘솔에서 OAuth2.0 인증 엔드포인트 포트를 위한 구성을 수신하는 데 사용됩니다.
    - **Facade 관리자 포트**. 기본적으로 포트 2444는 ID 및 액세스 관리 구성에 사용됩니다.
    - **Facade 인터랙션 포트**. 기본적으로 포트 2445는 Kaspersky OSMP KAS Service를 Kaspersky OSMP Facade Service에 연결하는 데 사용됩니다.

    원하는 경우 나중에 기본 포트 번호를 변경할 수 있습니다. 이후에 Kaspersky Security Center 웹 콘솔을 통해서는 변경할 수 없습니다.

11. 설치 프로그램의 마지막 창에서 **설치**를 눌러 설치를 시작합니다.

설치가 정상적으로 완료되면 바탕화면에 바로가기가 나타나고, Kaspersky Security Center 웹 콘솔에 로그인할 수 있습니다.

Microsoft Management Console 기반 관리 콘솔에서 중앙 관리 서버 빠른 시작 마법사를 실행하지 않았다면 해당 마법사가 시작됩니다.

문제 해결

브라우저에 URL을 입력해도 Kaspersky Security Center 웹 콘솔이 브라우저에 표시되지 않으면 다음을 시도해 보십시오:

1. Kaspersky Security Center 웹 콘솔이 설치된 기기의 올바른 호스트 이름이나 IP 주소를 지정했는지 확인합니다.
2. 작동하려는 기기에 Kaspersky Security Center 웹 콘솔이 설치된 기기 접근 권한이 있는지 확인합니다.
3. Kaspersky Security Center 웹 콘솔이 설치된 기기의 방화벽 설정이 포트 8080을 통한 수신 연결과 애플리케이션 node.exe에 대한 수신 연결을 허용하는지 확인합니다.
4. Windows에서 **서비스**를 엽니다. Kaspersky Security Center 웹 콘솔 서비스가 실행되고 있는지 확인합니다.
5. 관리 콘솔을 사용해 Kaspersky Security Center에 접근할 수 있는지 확인합니다.
6. Windows에서 **이벤트 뷰어**를 열고 **애플리케이션 및 서비스 로그 → Kaspersky 이벤트 로그**를 선택합니다. 로그에 오류가 없는지 확인합니다.

장애 조치 클러스터 노드에 설치된 중앙 관리 서버에 연결된 Kaspersky Security Center 웹 콘솔 설치

이 섹션에서는 Kaspersky Security Center 장애 조치 클러스터 노드 또는 Windows Server 장애 조치 클러스터 노드에 설치된 중앙 관리 서버에 연결되는 Kaspersky Security Center 웹 콘솔 서버(이하 Kaspersky Security Center 웹 콘솔이라고도 함)를 설치하는 방법을 설명합니다. Kaspersky Security Center 웹 콘솔을 설치하기 전에, Kaspersky Security Center 장애 조치 클러스터 노드 또는 Windows Server 장애 조치 클러스터 노드에 DBMS와 Kaspersky Security Center 중앙 관리 서버를 설치합니다.

Windows Server 장애 조치 클러스터 사용 시, 장애 조치 클러스터 노드에 Kaspersky Security Center 웹 콘솔 설치는 권장하지 않습니다. 노드 장애 발생 시, 중앙 관리 서버에 대한 접근 권한을 잃게 됩니다.

장애 조치 클러스터 노드에 설치된 중앙 관리 서버에 연결되는 Kaspersky Security Center 웹 콘솔을 설치하려면:

1. Kaspersky Security Center 웹 콘솔 설치 1~8단계를 수행합니다.
2. 9단계의 **신뢰할 수 있는 중앙 관리 서버** 창에서 **추가** 버튼을 클릭하여 장애 조치 클러스터를 신뢰하는 중앙 관리 서버로 추가합니다.

   열린 창에서 다음 속성을 지정합니다:

   - **중앙 관리 서버 이름**

     Kaspersky Security Center 웹 콘솔의 로그인 창에 표시될 클러스터 이름.

   - **중앙 관리 서버 주소**

     장애 조치 클러스터 유형에 따라 클러스터 주소를 지정합니다:

     - **Kaspersky Security Center 장애 조치 클러스터**. 클러스터 노드를 준비할 때 어댑터를 만들었다면 보조 네트워크 어댑터의 IP 주소를 클러스터 주소로 지정합니다. 생성하지 않았다면 사용 중인 타사 로드 밸런서의 IP 주소를 지정합니다.
     - **Windows Server 장애 조치 클러스터**. Windows Server 장애 조치 클러스터를 만들 때 받은 클러스터 주소를 지정합니다.

   - **중앙 관리 서버 포트**

     Kaspersky Security Center 웹 콘솔이 중앙 관리 서버에 연결하는 데 사용하는 OpenAPI 포트입니다(기본값은 13299).

   - **중앙 관리 서버 인증서**

     중앙 관리 서버 인증서는 Kaspersky Security Center 장애 조치 클러스터 또는 Windows Server 장애 조치 클러스터의 공유 데이터 저장소에 있습니다. 인증서 파일의 기본 경로: <공유 데이터 폴더>\1093\cert\klserver.cer. 공유 데이터 저장소에서 Kaspersky Security Center 웹 콘솔을 설치하는 기기로 인증서 파일을 복사합니다. 중앙 관리 서버 인증서의 로컬 경로를 지정합니다.
3. Kaspersky Security Center 웹 콘솔 기본 설치를 실행합니다.

설치가 완료되면 바탕화면에 바로가기가 나타나고, Kaspersky Security Center 웹 콘솔에 로그인할 수 있습니다.

Kaspersky Security Center 웹 콘솔 업그레이드

현재 설치된 인스턴스를 제거하지 않고 최신 버전의 Kaspersky Security Center 웹 콘솔을 사용하려는 경우 Kaspersky Security Center 웹 콘솔 설치 프로그램에서 제공되는 표준 업그레이드 절차를 사용하면 됩니다.

Kaspersky Security Center 웹 콘솔을 업그레이드하려면 다음 단계를 따릅니다.

1. 관리자 권한이 있는 계정으로 ksc-web-console-<version number>.<build number>.exe 설치 파일을 실행합니다. 여기에서 <build number>는 현재 설치된 인스턴스보다 숫자가 높은 Kaspersky Security Center 웹 콘솔 빌드를 나타냅니다.

2. 설치 마법사 창이 열리면 언어를 선택한 다음 **확인**을 누릅니다.

3. 시작 창에서 **업그레이드** 옵션을 선택하고 **다음**을 누릅니다.

4. **라이센스 계약서** 창에서 EULA(최종 사용자 라이센스 계약서)의 약관을 확인하고 해당 내용에 동의합니다. EULA에 동의하면 설치가 계속 진행되며, 동의하지 않으면 **다음** 버튼을 사용할 수 없습니다.

5. 설치가 완료될 때까지 설치 마법사의 단계를 진행합니다. 진행하면서 기존 설치 중 지정한 Kaspersky Security Center 웹 콘솔 설정을 수정할 수도 있습니다. **Kaspersky Security Center 웹 콘솔 수정 준비** 단계에 도달하면 **업그레이드** 버튼을 누릅니다. 새로운 설정이 적용될 때까지 기다렸다가 설치 마법사 다음 단계에서 **마침**를 누릅니다. **브라우저에서 Kaspersky Security Center 웹 콘솔 시작** 링크를 눌러 Kaspersky Security Center 웹 콘솔의 업그레이드된 인스턴스를 즉시 시작합니다.

   업그레이드 중 Kaspersky Security Center 웹 콘솔 설정 수정은 Kaspersky Security Center 웹 콘솔 버전 12.2 이상에서만 사용할 수 있습니다.

   Kaspersky Security Center 웹 콘솔 인스턴스가 업그레이드되었습니다.

Kaspersky Security Center 웹 콘솔 작업용 인증서

이 섹션에서는 Kaspersky Security Center 웹 콘솔에 대한 인증서를 발급 및 교체하는 방법과 서버가 Kaspersky Security Center 웹 콘솔과 상호 작용 시 중앙 관리 서버의 인증서를 갱신하는 방법에 대해 설명합니다.

Kaspersky Security Center 웹 콘솔용 인증서 재발급

대부분의 브라우저는 인증서의 유효 기간을 제한합니다. 이 제한에 부합하기 위해 Kaspersky Security Center 웹 콘솔 인증서의 유효 기간은 397일로 제한됩니다. 새로 자체 서명된 인증서를 수동으로 발행하여 인증 기관(CA)에서 받은 기존 인증서를 대체할 수 있습니다. 또는 만료된 Kaspersky Security Center 웹 콘솔 인증서를 재발급할 수도 있습니다.

Kaspersky Security Center 웹 콘솔에 대한 인증서 자동 재발급은 지원하지 않습니다. 만료된 인증서는 직접 재발급해야 합니다.

자체 서명된 인증서를 이미 사용하고 있는 경우 설치 프로그램의 표준 절차를 통해 Kaspersky Security Center 웹 콘솔을 업그레이드(**업그레이드** 옵션)하여 재발급할 수도 있습니다.

웹 콘솔을 열면 브라우저에서 웹 콘솔에 대한 연결이 비공개가 아니며 웹 콘솔 인증서가 유효하지 않다고 알릴 수 있습니다. 이 경고는 웹 콘솔 인증서가 자체 서명되고 Kaspersky Security Center에서 자동으로 생성되기 때문에 표시됩니다. 이 경고를 없애거나 방지하려면 다음 작업 중 하나를 수행할 수 있습니다.

- 재발급 시 사용자 지정 인증서를 지정하십시오(권장 옵션). 사용자의 인프라에서 신뢰할 수 있고 사용자 지정 인증서의 요구 사항을 충족하는 인증서를 만듭니다.
- 웹 콘솔 인증서 재발급 후 인증서를 신뢰할 수 있는 브라우저 인증서 목록에 추가합니다. 사용자 지정 인증서를 만들 수 없는 경우에만 이 옵션을 사용하는 것이 좋습니다.

Kaspersky Security Center 웹 콘솔을 처음 설치할 때 새 인증서를 발급하려면 다음 단계를 따릅니다.

1. Kaspersky Security Center 웹 콘솔 루틴 설치를 실행합니다.
2. 설치 마법사에서 **클라이언트 인증서** 단계에 도달하면 **새 인증서 생성** 옵션을 선택하고 **다음** 버튼을 누릅니다.
3. 설치가 완료될 때까지 설치 마법사의 나머지 단계를 진행합니다.

   Kaspersky Security Center 웹 콘솔에 대한 새 인증서가 397일의 유효 기간으로 발급됩니다.

만료된 Kaspersky Security Center 웹 콘솔 인증서를 재발급하려면 다음 단계를 따릅니다.

1. 관리자 권한이 있는 계정으로 ksc-web-console-<version number>.<build number>.exe 설치 파일을 실행합니다.
2. 설치 마법사 창이 열리면 언어를 선택한 다음 **확인**을 누릅니다.
3. 시작 창에서 **인증서 재발급** 옵션을 선택하고 **다음**을 누릅니다.
4. 다음 단계에서 Kaspersky Security Center 웹 콘솔 재구성이 완료될 때까지 기다린 다음 **마침**를 누릅니다.

   Kaspersky Security Center 웹 콘솔 인증서가 397일의 유효 기간으로 재발급됩니다.

ID 및 액세스 관리를 사용하는 경우 ID 및 액세스 관리가 사용하는 포트에 대해 모든 TLS 인증서를 다시 설치해야 합니다. Kaspersky Security Center 웹 콘솔은 인증서가 만료되면 알림을 표시합니다. 이 알림의 지침을 따라야 합니다.

Kaspersky Security Center 웹 콘솔 인증서 교체

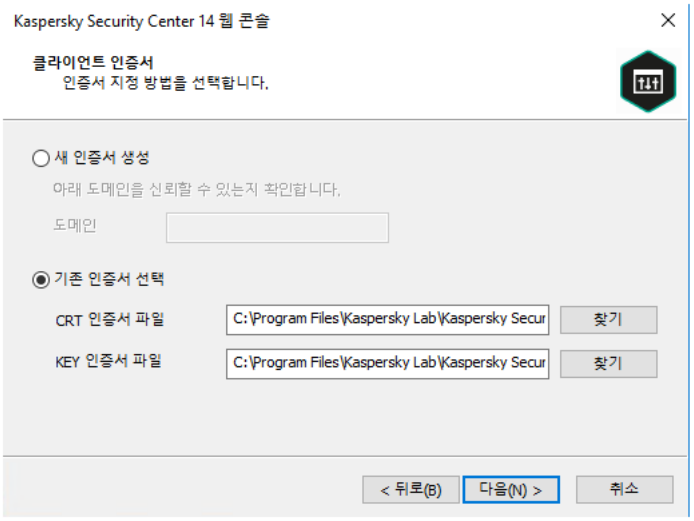
기본적으로 Kaspersky Security Center 웹 콘솔 서버를 설치하면 애플리케이션에 대한 브라우저 인증서가 자동 생성됩니다. 자동으로 생성된 인증서를 사용자 지정 인증서로 교체할 수 있습니다.

Kaspersky Security Center 웹 콘솔의 인증서를 사용자 지정 인증서로 교체하려면:

1. Kaspersky Security Center 웹 콘솔 서버가 설치된 기기에서 관리자 권한이 있는 계정으로 ksc-web-console-<버전 번호>.<빌드 번호>.exe 설치 파일을 실행합니다.

   설치 마법사가 시작됩니다.
2. 마법사 첫 페이지에서 **업그레이드** 옵션을 선택합니다.

3. **클라이언트 인증서** 페이지에서 **기존 인증서 선택** 옵션을 선택하고 사용자 지정 인증서의 경로를 지정합니다.



클라이언트 인증서 지정

4. 마법사의 마지막 페이지에서 **수정**을 눌러 새 설정을 적용합니다.
5. 애플리케이션 재구성이 성공적으로 완료되면 **마침** 버튼을 누릅니다.

Kaspersky Security Center 웹 콘솔이 지정된 인증서로 작동합니다.

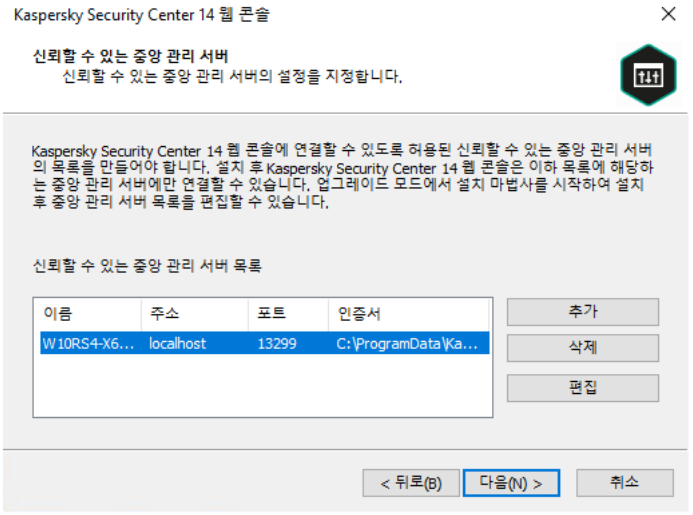
Kaspersky Security Center 웹 콘솔에서 신뢰하는 중앙 관리 서버에 대한 인증서 지정

기존 중앙 관리 서버 인증서는 인증서 만료일 전에 새 인증서로 자동 교체됩니다. 기존 중앙 관리 서버 인증서를 사용자 지정 인증서로 교체할 수도 있습니다. 인증서가 변경될 때마다 Kaspersky Security Center 웹 콘솔의 설정에서 새 인증서를 지정해야 합니다. 그렇지 않으면 Kaspersky Security Center 웹 콘솔에서 중앙 관리 서버에 연결할 수 없습니다.

중앙 관리 서버에 대한 새 인증서를 지정하려면 다음 단계를 따릅니다.

1. 중앙 관리 서버가 설치된 기기에서 인증서 파일을 예컨대 대용량 저장 기기로 복사합니다.
   기본적으로 인증서 파일은 다음 폴더에 저장됩니다.
   - Windows – %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Linux의 경우—/var/opt/kaspersky/klnagent_srv/1093/cert/
2. Kaspersky Security Center 웹 콘솔이 설치된 기기에서 인증서 파일을 로컬 폴더에 저장합니다.
3. 관리자 권한이 있는 계정으로 ksc-web-console-<version number>.<build number>.exe 설치 파일을 실행합니다.
   설치 마법사가 시작됩니다.
4. 첫 번째 마법사 페이지에서 **업그레이드** 옵션을 선택합니다.
   마법사의 지침을 따릅니다.

5. 마법사의 **신뢰할 수 있는 중앙 관리 서버** 페이지에서, 필요한 중앙 관리 서버를 선택하고 **편집** 버튼을 누릅니다.



신뢰할 수 있는 중앙 관리 서버 지정

6. **중앙 관리 서버 편집** 창이 열리면 **찾기** 버튼을 클릭하고 새 인증서 파일의 경로를 지정한 다음 **업데이트** 버튼을 클릭하여 변경 사항을 적용합니다.

7. 마법사의 **Kaspersky Security Center 웹 콘솔 수정 준비** 페이지에서 **업그레이드** 버튼을 클릭하여 업그레이드를 시작합니다.

8. 애플리케이션 재구성이 성공적으로 완료되면 **마침** 버튼을 누릅니다.

9. Kaspersky Security Center 웹 콘솔에 로그인합니다.

Kaspersky Security Center 웹 콘솔이 지정된 인증서로 작동합니다.

PFX 인증서를 PEM 형식으로 변환

Kaspersky Security Center 웹 콘솔에서 PFX 인증서를 사용하려면 먼저 아무 OpenSSL 기반 교차 플랫폼 유틸리티나 사용하여 해당 인증서를 PEM 형식으로 변환해야 합니다.

Windows 운영 체제에서 PFX 인증서를 PEM 형식으로 변환하려면:

1. OpenSSL 기반 교차 플랫폼 유틸리티에서 다음 명령을 실행합니다.

   `openssl pkcs12 -in <파일 이름.pfx> -clcerts -nokeys -out server.crt`

   `openssl pkcs12 -in <파일 이름.pfx> -nocerts -nodes -out key.pem`

   결과적으로 .crt 파일로 된 공개 키와 암호로 보호된 .pem 파일로 된 개인 키를 획득합니다.

2. .pfx 파일이 저장된 폴더에 .crt 및 .pem 파일이 생성되었는지 확인합니다.

3. .crt 또는 .pem 파일에 "Bag 속성"이 포함되어 있으면 아무 텍스트 편집기나 사용하여 이 속성을 삭제한 다음 파일을 저장합니다.

4. Windows 서비스를 다시 시작합니다.

5. Kaspersky Security Center 웹 콘솔은 암호로 보호된 인증서를 지원하지 않습니다. 따라서 OpenSSL 기반 교차 플랫폼 유틸리티에서 다음 명령을 실행하여 .pem 파일에서 암호를 제거하십시오.

   `openssl rsa -in key.pem -out key-without-passphrase.pem`

입력 및 출력 .pem 파일에 같은 이름을 사용하지 마십시오.

결과적으로 새 .pem 파일은 암호화되지 않습니다. 사용 시 암호를 입력할 필요가 없습니다.

.crt 및 .pem 파일을 사용할 준비가 되었으므로 Kaspersky Security Center 웹 콘솔 설치 프로그램에서 지정할 수 있습니다.

Linux 운영 체제에서 PFX 인증서를 PEM 형식으로 변환하려면:

1. OpenSSL 기반 교차 플랫폼 유틸리티에서 다음 명령을 실행합니다.

   ```
   openssl pkcs12 -in <파일 이름.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <파일 이름.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. 인증서 파일과 개인 키가 .pfx 파일이 저장된 디렉터리와 동일한 디렉터리에 생성되었는지 확인합니다.

3. Kaspersky Security Center 웹 콘솔은 암호로 보호된 인증서를 지원하지 않습니다. 따라서 OpenSSL 기반 교차 플랫폼 유틸리티에서 다음 명령을 실행하여 .pem 파일에서 암호를 제거하십시오.

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   입력 및 출력 .pem 파일에 같은 이름을 사용하지 마십시오.

   결과적으로 새 .pem 파일은 암호화되지 않습니다. 사용 시 암호를 입력할 필요가 없습니다.

.crt 및 .pem 파일을 사용할 준비가 되었으므로 Kaspersky Security Center 웹 콘솔 설치 프로그램에서 지정할 수 있습니다.

Kaspersky Security Center Windows에서 마이그레이션

이 섹션에서는 관리 중인 기기 및 관련 개체(정책, 작업, 그룹, 태그, 기타 개체)를 Kaspersky Security Center Windows에서 다음으로 마이그레이션하는 방법을 설명합니다:

- Kaspersky Security Center 클라우드 콘솔
- Kaspersky Security Center Linux

Kaspersky Security Center Cloud Console로 마이그레이션

Kaspersky Security Center 웹 콘솔에서 Kaspersky Security Center Cloud Console 로 마이그레이션을 수행할 수 있습니다. 그런 다음 Kaspersky 인프라에서 호스팅되는 중앙 관리 서버 및 데이터베이스 관리 시스템(DBMS)에 액세스할 수 있습니다. 물리적 서버나 DBMS가 필요하지 않습니다. 둘 다 Kaspersky 전문가가 유지 관리합니다.

Kaspersky Security Center Cloud Console의 제어 하에 Windows, Linux 또는 macOS 운영 체제를 실행하는 관리 중인 기기를 마이그레이션할 수 있습니다. 네트워크에 중앙 관리 서버 계층이 포함된 경우 Kaspersky Security Center Cloud Console에 저장할 수 있습니다. 또한 다음을 전송할 수 있습니다.

- 관리 중인 애플리케이션의 작업 및 정책
- 전역 작업
- 사용자 지정 기기 선택
- 관리 그룹 구조 및 포함된 기기
- 마이그레이션하는 기기에 할당된 태그

마이그레이션을 완료한 후 Kaspersky Security Center Cloud Console을 사용하여 기기를 관리할 수 있습니다. 동시에 전송된 개체가 보존되고 모든 관리 중인 기기에 네트워크 에이전트가 다시 설치됩니다.

마이그레이션 수행 방법 및 전제 조건 목록에 대한 자세한 내용은 *Kaspersky Security Center Cloud Console 도움말*을 참조하십시오.

Kaspersky Next XDR Expert로 마이그레이션

이 시나리오를 따라 Kaspersky Security Center Windows에서 Kaspersky Next XDR Expert로 관리 그룹 구조, 포함된 관리 중인 기기 및 기타 그룹 개체(정책, 작업, 전역 작업, 태그 및 기기 조회)를 전송할 수 있습니다.

제한사항:

- 마이그레이션은 Kaspersky Security Center 14.2 Windows에서 Kaspersky Next XDR Expert 버전 1.0 이상으로만 가능합니다.
- Kaspersky Security Center 웹 콘솔을 통해서만 이 시나리오를 수행할 수 있습니다.

단계

마이그레이션 시나리오는 다음 단계로 진행됩니다.

1. **마이그레이션 방법 선택**

   마이그레이션 마법사를 통해 Kaspersky Next XDR Expert로 마이그레이션합니다. 마이그레이션 마법사 단계는 Kaspersky Security Center Windows 및 Kaspersky Next XDR Expert 중앙 관리 서버의 계층 구조 배열 여부에 따라 달라집니다.

   - 중앙 관리 서버의 계층 구조를 사용한 마이그레이션

     Kaspersky Security Center Windows의 중앙 관리 서버가 Kaspersky Next XDR Expert의 중앙 관리 서버에 대한 보조 역할을 한다면, 이 옵션을 선택합니다. OSMP 콘솔 내에서 마이그레이션 프로세스를 관리하고 서버 간 전환을 수행합니다. 이 옵션을 선호한다면 중앙 관리 서버를 계층 구조로 배열하여 마이그레이션 절차를 단순화할 수 있습니다. 이렇게 하려면 마이그레이션을 시작하기 전에 계층 구조를 만드십시오.

- 내보내기 파일(ZIP 아카이브)을 사용한 마이그레이션

  Kaspersky Security Center Windows 및 Kaspersky Next XDR Expert의 중앙 관리 서버가 계층 구조로 정렬되지 않았다면 이 옵션을 선택합니다. Kaspersky Security Center Windows용 인스턴스와 OSMP 콘솔이라는 두 개의 콘솔을 사용하여 마이그레이션 프로세스를 관리합니다. 이때, Kaspersky Security Center Windows에서 내보내는 동안 생성하고 다운로드한 내보내기 파일을 사용하고, 이 파일을 Kaspersky Next XDR Expert로 가져옵니다.

2. **Kaspersky Security Center Windows에서 데이터 내보내기**

   Kaspersky Security Center Windows를 열고 마이그레이션 마법사를 실행합니다.

3. **Kaspersky Next XDR Expert로 데이터 가져오기**

   마이그레이션 마법사를 계속 진행하여 내보낸 데이터를 Kaspersky Next XDR Expert로 가져옵니다.

   서버가 계층 구조로 정렬되었다면, 같은 마법사 내에서 내보내기 완료 후 가져오기가 자동 시작됩니다. 서버가 계층 구조로 정렬되지 않았다면, Kaspersky Next XDR Expert로 전환한 후 마이그레이션 마법사를 계속 진행합니다.

4. **Kaspersky Security Center Windows에서 Kaspersky Next XDR Expert로 개체 및 설정을 수동 전송하기 위한 추가 작업 수행(선택 사항)**

   마이그레이션 마법사로 전송할 수 없는 개체와 설정도 전송할 방법이 있습니다. 예를 들어, 다음 절차를 추가로 수행할 수 있습니다.

   - 중앙 관리 서버의 전역 작업 구성
   - 네트워크 에이전트 정책 설정 구성
   - 애플리케이션의 설치 패키지 생성
   - 가상 서버 생성
   - 배포 지점 할당 및 구성
   - 기기 이동 규칙 구성
   - 기기 자동 태그 지정 규칙 구성
   - 애플리케이션 카테고리 생성

5. **가져온 관리 중인 기기를 Kaspersky Next XDR Expert에서 관리하도록 이동**

   마이그레이션을 완료하려면 가져온 관리 중인 기기를 Kaspersky Next XDR Expert에서 관리하도록 이동합니다. 다음 방법 중 하나를 사용할 수 있습니다:

   - Kaspersky Security Center 그룹 작업

     중앙 관리 서버 변경 작업으로 중앙 관리 서버를 특정 클라이언트 기기에 대한 다른 서버로 변경합니다.

   - klmover 유틸리티 사용

     klmover 유틸리티를 사용하여 새 중앙 관리 서버에 대한 연결 설정을 지정합니다.

   - 관리 중인 기기에 네트워크 에이전트 설치 또는 재설치

     새 네트워크 에이전트 설치 패키지를 생성하고 설치 패키지 속성에서 새 중앙 관리 서버에 대한 연결 설정을 지정합니다. 원격 설치 작업으로 가져온 관리 중인 기기에 설치 패키지로 네트워크 에이전트를 설치합니다.

     독립 실행형 설치 패키지를 생성하고 사용하여 네트워크 에이전트를 로컬로 설치할 수도 있습니다.

6. **네트워크 에이전트를 최신 버전으로 업데이트합니다**

   OSMP 콘솔과 같은 버전으로 네트워크 에이전트를 업그레이드할 것을 권장합니다.

7. **관리 중인 기기가 새 중앙 관리 서버에 표시되는지 확인합니다**

   Kaspersky Next XDR Expert 중앙 관리 서버에서 관리 중인 기기 목록(**에셋(기기)** → **관리 중인 기기**)을 열고 **표시 여부**, **네트워크 에이전트가 설치됨**, **마지막 중앙 관리 서버 연결** 열의 값을 확인합니다.

기타 데이터 마이그레이션 방법

마이그레이션 마법사 외에도 특정 작업 및 정책을 전송할 수 있습니다.

- Kaspersky Security Center Windows에서 작업 내보내기 후, Kaspersky Next XDR Expert로 작업을 가져옵니다.
- Kaspersky Security Center Windows에서 특정 정책을 내보낸 다음 Kaspersky Next XDR Expert로 정책을 가져옵니다. 선택한 정책과 함께 관련 정책 프로필을 내보내고 가져옵니다.

Kaspersky Security Center Linux로 마이그레이션

중앙 관리 서버 데이터 백업(klbackup 유틸리티 사용)과 마이그레이션 마법사를 사용하여 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux로 마이그레이션할 수 있습니다.

아래 표에서 중앙 관리 서버 데이터 백업과 마이그레이션 마법사를 사용한 마이그레이션의 주요 기능과 제한 사항을 비교하여 조직에 더 적합한 접근 방식을 결정할 수 있습니다.

파라미터	중앙 관리 서버 데이터 백업	마이그레이션 마법사
마이그레이션 프로세스	Kaspersky Security Center Windows 중앙 관리 서버 데이터의 전체 백업을 생성하고 Kaspersky Security Center Linux 중앙 관리 서버에서 복원	마이그레이션할 중앙 관리 서버 데이터 선택 및 내보내기, 이 데이터를 Kaspersky Security Center Linux 중앙 관리 서버로 가져오기, Kaspersky Security Center Linux가 관리하는 관리 중인 기기 전환
마이그레이션 방법의 특징	• 모든 중앙 관리 서버 데이터 마이그레이션 • 원하는 수의 관리 중인 기기 마이그레이션 • Kaspersky Security Center Windows 중앙 관리 서버 데이터의 전체 복사본을 가져와 Kaspersky Security Center Linux 중앙 관리 서버로 전송하는 데 사용됩니다	• 중앙 관리 서버 데이터의 부분적 마이그레이션 • 마이그레이션할 개체 선택이 가능합니다 • 마이그레이션할 관리 그룹 또는 하위 그룹에 포함할 수 있는 기기는 10,000개 이하입니다 • 마이그레이션 범위 내의 그룹 개체만 포함하여 중앙 관리 서버 데이터를 부분적으로 전송하는 데 사용됩니다. 마이그레이션 범위에 속하지 않는 그룹 개체는 직접 복원해야 합니다
마이그레이션 범위	관리 중인 기기 수에 제한 없이 중앙 관리 서버 데이터 전체 전송	• 관리 그룹 구조 • 관리 그룹에 포함된 관리 중인 기기(**10,000개 이하의 기기**) • 마이그레이션할 기기에 할당된 태그 • 네트워크 에이전트 및 관리 중인 애플리케이션의 글로벌 작업(중앙 관리 서버 제외) • 네트워크 에이전트 및 관리 중인 애플리케이션의 그룹 작업 • 관리 중인 애플리케이션의 정책 • 보고서 템플릿 • 사용자 역할 • 내부 사용자 및 보안 그룹 • 컨텐츠가 수동으로 추가된 사용자 지정 애플리케이션 카테고리 • 사용자 지정 기기 선택
마이그레이션되지 않는 범위	–	• 중앙 관리 서버의 전역 작업 • 중앙 관리 서버에 저장된 이벤트 • 원격 설치를 위한 애플리케이션의 배포 패키지 저장소 • 중앙 관리 서버 인증서 • 중앙 관리 서버 및 관리 중인 애플리케이션에서 사용하는 라이센스 키 • 가상 중앙 관리 서버 • 네트워크 에이전트 정책 설정 • 기기 이동 규칙 • 기기 자동 태그 지정 규칙 • 배포 지점 • 중앙 관리 서버에 저장된 Kaspersky 애플리케이션 설정
마이그레이션을 지원하는 Kaspersky Security Center 버전	• 지원되는 모든 Kaspersky Security Center Windows 버전 • Kaspersky Security Center Linux 버전 15.2 이상	• Kaspersky Security Center Windows 버전 14.2 이상 • Kaspersky Security Center Linux 버전 15 이상
서로 마이그레이션 가능한 DBMS	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro(패치가 설치된 Kaspersky Security Center Windows 버전 14.2 이상에서 Kaspersky Security Center Linux 버전 15.3 이상으로 마이그레이션하는 경우에만 해당) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro(Kaspersky Security Center Windows 15.1 이상에서 Kaspersky Security Center Linux 16 이상으로 마이그레이션하는 경우에만 해당)	지원되는 DBMS 간 제한 없는 마이그레이션

중앙 관리 서버 데이터 백업을 사용하여 Kaspersky Security Center Linux로 마이그레이션

데이터 백업을 사용하여 Kaspersky Security Center Windows 중앙 관리 서버 데이터를 Kaspersky Security Center Linux로 마이그레이션할 수 있습니다. 마이그레이션하기 전에 Kaspersky Security Center Linux에서 Kaspersky Security Center Windows의 필요 기능을 지원하는 지 확인하십시오.

제한사항:

- 다음과 같은 DBMS 간에 마이그레이션을 수행할 수 있습니다.
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Microsoft SQL Server, MySQL 또는 MariaDB 데이터베이스에 저장된 중앙 관리 서버 데이터를 MySQL 또는 MariaDB로 마이그레이션하는 작업은 Kaspersky Security Center Windows의 지원되는 모든 버전에서 Kaspersky Security Center Linux 버전 15.2 이상으로 마이그레이션하려는 경우에 지원됩니다.
- PostgreSQL 데이터베이스에 저장된 중앙 관리 서버 데이터를 PostgreSQL 또는 Postgres Pro 데이터베이스로 마이그레이션하는 작업은 Kaspersky Security Center Windows 버전 15.1 이상에서 Kaspersky Security Center Linux 버전 16 이상으로 마이그레이션하는 경우에 지원됩니다.
- Microsoft SQL Server 데이터베이스에 저장된 중앙 관리 서버 데이터를 PostgreSQL 또는 Postgres Pro로 마이그레이션하는 작업은 Kaspersky Security Center Windows 버전 14.2 이상에서 Kaspersky Security Center Linux 버전 15.3 이상으로 마이그레이션하는 경우에 지원됩니다.

  PostgreSQL 또는 Postgres Pro로 마이그레이션을 지원하려면, 다음 중 하나를 수행합니다.
  - Kaspersky Security Center Windows 중앙 관리 서버용 15.1.0.20748-pf2 패치를 설치합니다. 이 패치를 받으려면 Kaspersky 기술 지원팀에 문의하세요.
  - Kaspersky Security Center Windows를 버전 15.1.0.22239로 업데이트 합니다.
- Kaspersky Security Center Windows 및 Kaspersky Security Center Linux에서 MySQL 또는 MariaDB를 DBMS로 사용한다면 `lower_case_table_names` 파라미터가 현재 및 새 DBMS와 일치해야 합니다.

  데이터 백업을 생성하기 전에 `lower_case_table_names` 파라미터를 확인하십시오. 그런 다음 Kaspersky Security Center Linux용 MySQL 또는 MariaDB를 설치할 때 이 파라미터를 이 Windows용 파라미터에 지정된 값과 같은 값으로 설정해야 합니다.

단계

중앙 관리 서버 데이터 백업을 사용한 마이그레이션은 다음과 같은 단계로 진행됩니다.

1. **중앙 관리 서버에 로그인할 수 있는 관리자의 내부 사용자 계정을 보유하고 있는지 확인**

   관리자의 계정은 Kaspersky Security Center Linux 중앙 관리 서버에 로그인하는 데 사용됩니다. 이러한 계정이 없고 로컬 Windows 계정 또는 도메인 계정으로만 로그인한 경우, 백업을 복원한 후 Kaspersky Security Center Linux 중앙 관리 서버에 로그인할 수 없습니다. Kaspersky Security Center Linux 중앙 관리 서버는 로컬 Windows 계정을 사용한 로그인을 지원하지 않습니다. 도메인 계정으로 로그인할 수는 있지만, 중앙 관리 서버를 추가로 구성해야 할 수 있습니다.

   관리자의 계정이 없는 경우 kladduser 유틸리티를 사용하여 백업 복사본을 복원한 후 이러한 계정을 만들어야 합니다.

2 Kaspersky Security Center Windows 중앙 관리 서버 데이터의 최신 백업 복사본 만들기

Kaspersky Security Center Windows 및 Kaspersky Security Center Linux에 사용된 DBMS 유형에 따라 다음 중 한 가지 작업을 수행합니다.

- MySQL 또는 MariaDB 에서 MySQL 또는 MariaDB 로 마이그레이션하려는 경우: 중앙 관리 서버가 설치된 기기에서 klbackup 유틸리티 또는 데이터 백업 작업을 사용하여 백업 복사본을 만듭니다.
- PostgreSQL 간 또는 Postgres Pro 간 마이그레이션의 경우: 중앙 관리 서버가 설치된 기기에서 klbackup 유틸리티 또는 데이터 백업 작업을 사용하여 백업 복사본을 만듭니다.
- Microsoft SQL Server를 MySQL 또는 MariaDB로 마이그레이션하려는 경우: **MySQL/MariaDB 형식으로 마이그레이션** 옵션을 활성화한 상태에서 klbackup 유틸리티를 사용하여 백업 복사본을 만듭니다.
- Microsoft SQL Server에서 PostgreSQL 또는 Postgres Pro 로 마이그레이션하려는 경우:

  1. Kaspersky 기술 지원에 요청하여 중앙 관리 서버용 15.1.0.20748-pf2 패치를 설치하면 PostgreSQL 및 Postgres Pro로 마이그레이션을 지원할 수 있습니다.

     또는 Kaspersky Security Center Windows를 버전 15.1.0.22239 로 업데이트합니다.

  2. klbackup 유틸리티를 사용하여 백업 복사본을 만듭니다.

     명령줄에서 klbackup을 실행할 경우 `-migrate postgres` 플래그를 사용하십시오.

     klbackup 인터페이스를 사용할 경우 **Postgres 형식으로 마이그레이션** 옵션을 활성화하십시오.

백업 복사본을 만든 후 Kaspersky Security Center Windows 중앙 관리 서버를 네트워크에서 연결 해제합니다.

3 Kaspersky Security Center Linux 설치를 위한 새 기기 준비

마법사의 이 단계에서 다음을 수행합니다.

1. 중앙 관리 서버를 설치할 새 기기를 선택하십시오. 이 기기는 하드웨어 및 소프트웨어 요구 사항을 충족해야 합니다. 또한 중앙 관리 서버에서 사용되는 포트를 사용할 수 있는지 확인하십시오.
2. 새 기기에 같은 주소를 할당합니다.

   새 중앙 관리 서버에 NetBIOS 이름, FQDN, 고정 IP 주소를 할당할 수 있습니다. 네트워크 에이전트 배포 시 네트워크 에이전트 설치 패키지에 설정된 중앙 관리 서버 주소에 따라 다릅니다. 또는 네트워크 에이전트가 연결할 중앙 관리 서버를 결정하는 연결 주소를 사용할 수 있습니다(이 주소는 관리 중인 기기에서 klnagchk 유틸리티를 사용하여 얻을 수 있습니다).

4 DBMS 설치 및 구성

마법사의 이 단계에서 다음을 수행합니다.

1. 최적의 성능을 제공하는 DBMS 유형을 선택합니다. 네트워크로 연결된 기기의 수, 네트워크 토폴로지, 네트워크의 작업량을 고려합니다. 지원하는 DBMS 중 하나를 선택할 수 있습니다.
2. 백업을 생성할 때 선택한 DBMS 유형에 따라 DBMS를 설치합니다. 선택한 DBMS를 설치하는 방법에 대한 정보는 해당 설명서를 참조하십시오.

   > 새 데이터베이스 버전은 현재 버전보다 낮을 수 없습니다.

3. Kaspersky Security Center Linux와 작업하기 위한 DBMS 서버 구성.

5 Kaspersky Security Center Linux 설치

새 기기에 Kaspersky Security Center Linux를 설치합니다.

설치 중에 생성된 관리자의 내부 사용자 계정 및 백업에서 중앙 관리 서버 데이터를 복원하기 전에 생성된 다른 개체(그룹, 정책, 작업, 사용자)는 복원 이후 손실됩니다. 이러한 개체는 백업에 포함된 개체로 대체됩니다.

6 백업 복사본에서 중앙 관리 서버 데이터 복원

마법사의 이 단계에서 다음을 수행합니다.

1. klbackup 유틸리티를 사용하여 새 기기에서 중앙 관리 서버 데이터를 복원합니다.

2. Kaspersky Security Center Windows 중앙 관리 서버에 로그인할 당시 관리자의 내부 사용자 계정을 보유하지 않은 상태였고 로컬 Windows 계정 또는 도메인 계정을 사용한 경우, kladduser 유틸리티를 사용하여 다음과 같이 관리자 계정을 생성하십시오.

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   `<password>` 매개변수는 다음과 같은 요구 사항을 충족합니다.

   - 사용자 암호는 8자 미만이거나 256자를 초과할 수 없습니다.
   - 암호는 아래에 나와 있는 그룹 중 3개 이상의 문자를 포함해야 합니다:
     - 대문자(A-Z)
     - 소문자(a-z)
     - 숫자(0-9)
     - 특수 문자(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7 Kaspersky Security Center 웹 콘솔 서버 설치 및 중앙 관리 서버 구성

마법사의 이 단계에서 다음을 수행합니다.

1. Kaspersky Security Center 웹 콘솔을 설치합니다.

   이전에 Kaspersky Security Center 웹 콘솔을 설치했다면, 같은 응답 파일로 다시 설치합니다.

   관리자의 내부 사용자 계정으로 Kaspersky Security Center 웹 콘솔에 로그인합니다.

   데이터 초기화 프로세스는 일반적으로 중앙 관리 서버 데이터 복원 후 최대 15분 정도 소요되지만 시간은 하드웨어 성능과 중앙 관리 서버 데이터 크기에 따라 다릅니다. 이 시간 동안에는 Kaspersky Security Center 웹 콘솔에 연결하지 못하며 오류가 표시될 수 있습니다.

2. 데이터베이스의 데이터 초기화가 완료되면 중앙 관리 서버의 기본 기능이 제대로 작동하는지 확인합니다. 중앙 관리 서버가 관리 중인 기기와 동기화하고 중앙 관리 서버 데이터가 복구되는지 확인합니다.

3. 도메인 컨트롤러를 검색하여 도메인 구조, 사용자 계정, 보안 그룹, 도메인에 포함된 기기의 DNS 이름에 rhks한 정보를 복원합니다.

4. 필요하다면 이전 기기에서 중앙 관리 서버와 데이터베이스 서버를 제거합니다.

   같은 네트워크에 같은 연결 주소와 중앙 관리 서버 인증서를 사용하는 중앙 관리 서버가 여러 대 있어서는 안 됩니다.

관리자는 Kaspersky Security Center Linux에서 지원하는 기능을 고려하여 Kaspersky Security Center Windows에 있었던 중앙 관리 서버 데이터 및 관리 중인 기기에 접근할 수 있습니다.

마이그레이션 마법사를 사용하여 Kaspersky Security Center Linux로 마이그레이션

이 시나리오를 따라 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux로 관리 그룹 구조, 포함된 관리 중인 기기 및 기타 그룹 개체(정책, 작업, 전역 작업, 태그 및 기기 조회)를 전송할 수 있습니다. 마이그레이션하기 전에 Kaspersky Security Center Linux에서 Kaspersky Security Center Windows의 필요 기능을 지원하는 지 확인하십시오.

제한사항:

- Kaspersky Security Center Windows 14.2 버전 이상에서 Kaspersky Security Center Linux 버전 15 이상으로의 마이그레이션만 가능합니다.
- Kaspersky Security Center 웹 콘솔을 통해서만 이 시나리오를 수행할 수 있습니다.

단계

마이그레이션 시나리오는 다음 단계로 진행됩니다.

1. **마이그레이션 방법 선택**

   마이그레이션 마법사를 통해 Kaspersky Security Center Linux로 마이그레이션합니다. 마이그레이션 마법사 단계는 Kaspersky Security Center Windows 및 Kaspersky Security Center Linux의 중앙 관리 서버가 계층 구조로 배열되어 있는지에 따라 달라집니다.

   - 중앙 관리 서버의 계층 구조를 사용한 마이그레이션

     Kaspersky Security Center Windows의 중앙 관리 서버가 Kaspersky Security Center Linux의 중앙 관리 서버에 대한 보조 역할을 할 시, 이 옵션을 선택합니다. Kaspersky Security Center 웹 콘솔의 단일 인스턴스 내에서 마이그레이션 프로세스를 관리하고 서버를 전환합니다. 이 옵션을 선호한다면 중앙 관리 서버를 계층 구조로 배열하여 마이그레이션 절차를 단순화할 수 있습니다. 이렇게 하려면 마이그레이션을 시작하기 전에 계층 구조를 만드십시오.

   - 내보내기 파일(ZIP 아카이브)을 사용한 마이그레이션

     Kaspersky Security Center Windows 및 Kaspersky Security Center Linux의 중앙 관리 서버가 계층 구조로 정렬되지 않았다면 이 옵션을 선택합니다. Kaspersky Security Center 웹 콘솔의 두 인스턴스(Kaspersky Security Center Windows용 인스턴스와 Kaspersky Security Center Linux용 인스턴스)로 마이그레이션 프로세스를 관리합니다. 이때, Kaspersky Security Center Windows에서 내보내는 동안 생성하고 다운로드한 내보내기 파일을 사용하고 이 파일을 Kaspersky Security Center Linux로 가져옵니다.

2. **Kaspersky Security Center Windows 중앙 관리 서버의 인증서 및 개인 키 백업(옵션 단계)**

   백업 복사본에서 중앙 관리 서버의 인증서와 개인 키를 복원하여, 관리 중인 기기를 Kaspersky Security Center Linux의 중앙 관리 서버가 관리하도록 할 수 있습니다. 이때는, Kaspersky Security Center Windows 중앙 관리 서버의 인증서 및 개인 키를 백업합니다. 그 후에 6단계에서 인증서와 개인 키를 복원합니다.

3. **Kaspersky Security Center Windows에서 데이터 내보내기**

   Kaspersky Security Center Windows를 열고 마이그레이션 마법사를 실행합니다.

4 Kaspersky Security Center Linux로 데이터 가져오기

마이그레이션 마법사를 계속 진행하여 내보낸 데이터를 Kaspersky Security Center Linux로 가져옵니다. 서버가 계층 구조로 정렬되었다면, 같은 마법사 내에서 내보내기 완료 후 가져오기가 자동 시작됩니다. 서버가 계층 구조로 정렬되지 않았다면, Kaspersky Security Center Linux로 전환한 후 마이그레이션 마법사를 계속 진행합니다.

5 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux로 개체 및 설정을 수동 전송하기 위한 추가 작업 수행(선택적 단계)

마이그레이션 마법사로 전송할 수 없는 개체와 설정도 전송할 방법이 있습니다. 예를 들어, 다음 절차를 추가로 수행할 수 있습니다.

- 중앙 관리 서버 및 관리 중인 애플리케이션에서 사용하는 라이센스 키 전송
- 중앙 관리 서버의 전역 작업 구성
- 네트워크 에이전트 정책 설정 구성
- 애플리케이션의 설치 패키지 생성
- 가상 서버 생성
- 배포 지점 할당 및 구성
- 기기 이동 규칙 구성
- 기기 자동 태그 지정 규칙 구성
- 애플리케이션 카테고리 생성

6 가져온 관리 중인 기기를 Kaspersky Security Center Linux에서 관리하도록 이동

마이그레이션을 완료하려면 가져온 관리 중인 기기를 Kaspersky Security Center Linux에서 관리하도록 이동합니다. 다음 방법 중 하나를 사용할 수 있습니다:

- klmover 유틸리티 사용

  klmover 유틸리티를 사용하여 새 중앙 관리 서버에 대한 연결 설정을 지정합니다.

- *중앙 관리 서버 변경* 작업을 통해

  중앙 관리 서버 변경 작업을 생성하고, 가져온 관리 중인 기기, 새 중앙 관리 서버, 기타 작업 설정을 지정합니다. 그런 다음 작업을 실행하여 관리 중인 기기를 Kaspersky Security Center Linux의 중앙 관리 서버가 관리하도록 합니다.

- 관리 중인 기기에서 네트워크 에이전트 제거(이미 설치했다면) 후 추가 설치를 통해

  새 네트워크 에이전트 설치 패키지를 생성하고 설치 패키지 속성에서 새 중앙 관리 서버에 대한 연결 설정을 지정합니다. 가져온 관리 중인 기기에서 네트워크 에이전트를 제거한 후, 원격 설치 작업으로 가져온 관리 중인 기기에 설치 패키지를 사용해 네트워크 에이전트를 설치합니다. 독립 실행형 설치 패키지를 생성하고 사용하여 네트워크 에이전트를 로컬로 설치할 수도 있습니다. 자세한 내용은 관리 중인 기기를 Kaspersky Security Center Linux에서 관리하도록 전환을 참조하십시오.

- 백업 복사본에서 중앙 관리 서버의 인증서 및 개인 키 복원을 통해(Kaspersky Security Center Linux 15.1 이상으로 마이그레이션할 때만)

  Kaspersky Security Center Linux의 중앙 관리 서버가 설치된 기기에 Kaspersky Security Center Windows의 중앙 관리 서버와 같은 네트워크 주소를 할당합니다. klbackup 유틸리티를 `-cert_only` 파라미터와 함께 실행하여 2단계에서 저장한 백업 복사본에서 중앙 관리 서버 인증서 및 개인 키를 복원합니다. 명령줄에서 다음 명령을 실행합니다: `/opt/kaspersky/ksc64/sbin/klbackup -path <중앙 관리 서버 인증서의 백업 복사본 경로> -restore -cert_only` 자세한 내용은 klbackup 유틸리티를 사용하여 다른 중앙 관리 서버에서 관리 중인 기기 전환을 참조하십시오.

7. **네트워크 에이전트를 최신 버전으로 업데이트합니다**

   Kaspersky Security Center와 같은 버전으로 Linux용 네트워크 에이전트를 업그레이드할 것을 권장합니다.

8. **관리 중인 기기가 새 중앙 관리 서버에 표시되는지 확인합니다**

   Kaspersky Security Center Linux 중앙 관리 서버에서 관리 중인 기기 목록(**에셋(기기)** → **관리 중인 기기**)을 열고 **표시 여부**, **네트워크 에이전트가 설치됨**, **마지막 중앙 관리 서버 연결** 열의 값을 확인합니다.

기타 데이터 마이그레이션 방법

마이그레이션 마법사 외에도 특정 작업 및 정책을 전송할 수 있습니다.

- Kaspersky Security Center Windows에서 작업 내보내기 후, Kaspersky Security Center Linux로 작업을 가져옵니다.
- Kaspersky Security Center Windows에서 특정 정책을 내보낸 다음 Kaspersky Security Center Linux로 정책을 가져옵니다. 선택한 정책과 함께 관련 정책 프로필을 내보내고 가져옵니다.

Kaspersky Security Center Windows에서 그룹 개체 내보내기

관리 중인 기기 및 기타 그룹 개체를 포함하는 관리 그룹 구조를 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux로 마이그레이션하려면 먼저 내보낼 데이터를 선택하고 내보내기 파일을 생성해야 합니다. 내보내기 파일에는 마이그레이션하려는 모든 그룹 개체에 대한 정보가 포함되어 있습니다. 이 내보내기 파일은 그 다음 Kaspersky Security Center Linux로 가져오기에 사용됩니다.

다음 개체를 내보낼 수 있습니다:

- 관리 중인 애플리케이션의 작업 및 정책
- 전역 작업
- 사용자 지정 기기 선택
- 관리 그룹 구조 및 포함된 기기
- 마이그레이션하는 기기에 할당된 태그

가져오기를 시작하기 전에 Kaspersky Security Center Linux로의 마이그레이션에 대한 일반 정보를 읽어 보십시오. Kaspersky Security Center Windows 및 Kaspersky Security Center Linux의 중앙 관리 서버 계층을 사용하거나 사용하지 않는 마이그레이션 방법을 선택합니다.

마이그레이션 마법사를 통해 관리 중인 기기 및 관련 그룹 개체를 내보내려면:

1. Kaspersky Security Center Windows 및 Kaspersky Security Center Linux 중앙 관리 서버의 계층 구조 배열 여부에 따라 다음 중 하나를 수행합니다.

   - 서버가 계층 구조로 정렬되었다면, Kaspersky Security Center 웹 콘솔을 열고 Kaspersky Security Center Windows의 서버로 전환합니다.

   - 서버가 계층 구조로 정렬되지 않았다면 Kaspersky Security Center Windows에 연결된 Kaspersky Security Center 웹 콘솔을 엽니다.

2. 메인 메뉴에서 **동작** → **마이그레이션**으로 이동합니다.

3. 데이터와 설정을 전송할 위치를 선택하여 마법사를 시작하고 해당 단계를 따릅니다.

   - 데이터와 설정을 Kaspersky Security Center 클라우드 콘솔로 전송하려면 **Kaspersky Security Center Cloud Console로 마이그레이션**을 선택합니다.

   - 데이터와 설정을 Kaspersky Security Center Linux 또는 Kaspersky Next XDR Expert로 전송하려면 **Kaspersky Security Center Linux 또는 Open Single Management Platform으로 마이그레이션**을 선택합니다.

4. 내보낼 관리 그룹이나 하위 그룹을 선택합니다. 선택한 관리 그룹 또는 하위 그룹에 포함될 기기가 10,000개 이하인지 확인합니다.

5. 작업 및 정책을 내보낼 관리 중인 애플리케이션을 선택합니다. Kaspersky Security Center Linux에서 지원하는 애플리케이션만 선택하십시오. 지원되지 않는 애플리케이션의 개체는 계속 내보내지만 작동하지 않습니다.

6. 왼쪽에 있는 링크를 사용하여 글로벌 작업, 기기, 내보낼 리포트를 선택합니다. **그룹 개체** 링크를 사용하면 내보내기에서 사용자 지정 역할, 내부 사용자 및 보안 그룹, 사용자 지정 애플리케이션 카테고리를 제외할 수 있습니다.

내보내기 파일(ZIP 아카이브)이 생성됩니다. 중앙 관리 서버 계층 지원을 사용하여 마이그레이션을 수행하는지에 따라 내보내기 파일이 다음과 같이 저장됩니다.

- 서버가 계층 구조로 배열되었다면 내보내기 파일은 Kaspersky Security Center 웹 콘솔 서버의 임시 폴더에 저장됩니다.

- 서버가 계층 구조로 정렬되지 않았다면, 내보내기 파일이 기기에 다운로드됩니다.

중앙 관리 서버 계층 구조를 지원하는 마이그레이션에서는, 내보내기가 성공한 후 가져오기가 자동 시작됩니다. 중앙 관리 서버 계층 구조를 지원하지 않는 마이그레이션에서는 저장된 내보내기 파일을 Kaspersky Security Center Linux로 직접 가져올 수 있습니다.

Kaspersky Security Center Linux로 내보내기 파일 가져오기

Kaspersky Security Center Windows에서 내보낸 관리 중인 기기, 개체 및 해당 설정에 대한 정보를 전송하려면 작업 영역에 배포된 Kaspersky Security Center Linux나 Kaspersky Next XDR Expert로 가져와야 합니다.

마이그레이션 마법사를 통해 관리 중인 기기 및 관련 그룹 개체를 가져오려면:

1. Kaspersky Security Center Windows 및 Kaspersky Security Center Linux 중앙 관리 서버의 계층 구조 배열 여부에 따라 다음 중 하나를 수행합니다.

   - 서버가 계층 구조로 정렬되어 있으면 내보내기가 완료된 후 마이그레이션 마법사의 다음 단계로 진행하십시오. 이 마법사 내에서 성공적으로 내보내기가 완료되면 가져오기가 자동으로 시작됩니다(이 지침의 2단계 참조).

   - 서버가 계층 구조로 정렬되지 않았다면:

     a. Kaspersky Security Center Linux나 Kaspersky Next XDR Expert에 연결된 Kaspersky Security Center 웹 콘솔을 엽니다.

     b. 메인 메뉴에서 **동작 → 마이그레이션**으로 이동합니다.

     c. Kaspersky Security Center Windows에서 내보내기 시 생성하고 다운로드한 내보내기 파일(ZIP 아카이브)을 선택합니다. 내보내기 파일 업로드가 시작됩니다.

2. 내보내기 파일이 성공적으로 업로드되면 가져오기를 계속할 수 있습니다. 다른 내보내기 파일을 지정하려면 **변경** 링크를 클릭한 다음 필요한 파일을 선택합니다.

3. Kaspersky Security Center Linux 관리 그룹의 전체 계층 구조가 표시됩니다.

   내보낸 관리 그룹의 개체(관리 중인 기기, 정책, 작업 및 기타 그룹 개체)를 복원해야 하는 대상 관리 그룹 옆의 확인란을 선택합니다.

4. 그룹 개체 가져오기가 시작됩니다. 가져오는 동안에는 마이그레이션 마법사를 최소화하거나 다른 작업을 동시에 수행할 수 없습니다. 개체 목록의 모든 항목 옆에 있는 새로고침 아이콘(🔄)이 녹색 확인 표시(✓)로 바뀌고 가져오기가 완료될 때까지 기다립니다.

5. 가져오기가 완료되면 기기 세부 정보 등의 내보낸 관리 그룹 구조가 선택한 대상 관리 그룹 아래에 나타납니다. 복원하는 개체의 이름이 기존 개체의 이름과 동일한 경우 복원된 개체에 증분 접미사가 추가됩니다.

> 마이그레이션된 작업에서 작업 실행에 사용된 계정의 세부 정보가 지정되었다면, 작업을 열고 가져오기를 완료한 후 암호를 다시 입력해야 합니다.

가져오기가 오류와 함께 완료되면 다음 중 하나를 수행할 수 있습니다.

- 중앙 관리 서버 계층 구조를 지원하는 마이그레이션에서는 내보내기 파일 가져오기를 다시 시작할 수 있습니다.

- 중앙 관리 서버 계층 지원 없이 마이그레이션하려면 마이그레이션 마법사를 시작하여 다른 내보내기 파일을 선택한 다음 다시 가져올 수 있습니다.

내보내기 범위에 포함된 그룹 개체를 Kaspersky Security Center Linux로 성공적으로 가져왔는지 확인할 수 있습니다. 이렇게 하려면 **에셋(기기)** 섹션으로 이동하여 가져온 개체가 해당 하위 섹션에 나타나는지 확인합니다.

가져온 관리 중인 기기는 **관리 중인 기기** 하위 섹션에 표시되지만 네트워크에서 보이지 않으며 네트워크 에이전트가 설치되어 실행되지 않습니다(**표시 여부**, **네트워크 에이전트가 설치됨** 및 **네트워크 에이전트가 실행 중** 열의 *없음* 값).

마이그레이션을 완료하려면 관리 중인 기기를 Kaspersky Security Center Linux의 관리 대상으로 전환해야 합니다.

관리 중인 기기를 Kaspersky Security Center Linux에서 관리하도록 전환

관리 중인 기기, 개체 및 해당 설정에 대한 정보를 Kaspersky Security Center Linux로 성공적으로 가져온 후에는 관리 중인 기기를 Kaspersky Security Center Linux에서 관리하도록 전환하여 마이그레이션을 완료해야 합니다.

관리 중인 기기를 Kaspersky Security Center Linux로 이동하는 방법에는 다음이 있습니다.

- klmover 유틸리티 사용.
- *중앙 관리 서버 변경* 작업 사용.
- 백업 복사본에서 중앙 관리 서버의 인증서 및 개인 키 복원(Kaspersky Security Center Linux 15.1 이상으로 마이그레이션할 때만).

  자세한 내용은 기본 마이그레이션 시나리오 6단계를 참조하십시오.
- 원격 설치 작업으로 관리 중인 기기에 네트워크 에이전트 설치.

네트워크 에이전트를 설치하여 관리 중인 기기를 Kaspersky Security Center Linux에서 관리하도록 전환하려면:

1. Kaspersky Security Center Linux의 관리로 전환될 가져온 관리 중인 기기에서 네트워크 에이전트를 제거합니다.
2. Kaspersky Security Center Windows의 중앙 관리 서버로 전환합니다.
3. **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동하여 네트워크 에이전트의 기존 설치 패키지 속성을 엽니다.

   네트워크 에이전트의 설치 패키지가 패키지 목록에 없으면 새로 다운로드합니다.

   독립 실행형 설치 패키지를 생성하고 사용하여 네트워크 에이전트를 로컬로 설치할 수도 있습니다.
4. **설정** 탭에서 **연결** 섹션을 선택합니다. Kaspersky Security Center Linux 중앙 관리 서버의 연결 설정을 지정합니다.
5. 가져온 관리 중인 기기에 대한 원격 설치 작업을 생성한 다음 재구성된 네트워크 에이전트 설치 패키지를 지정합니다.

   Kaspersky Security Center Windows의 중앙 관리 서버 또는 배포 지점 역할을 하는 Windows 기반 기기를 통해 네트워크 에이전트를 설치할 수 있습니다. 중앙 관리 서버를 사용한다면 **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드** 옵션을 활성화합니다. 배포 지점을 사용한다면 **배포 지점에서 대상 운영 체제의 관리 공유 폴더로 다운로드** 옵션을 활성화합니다.
6. 원격 설치 작업을 실행합니다.

원격 설치 작업이 성공적으로 완료되면 Kaspersky Security Center Linux의 중앙 관리 서버로 이동하여 관리 중인 기기가 네트워크에 표시되고 네트워크 에이전트가 설치되어 실행 중인지 확인합니다(**표시 여부**, **네트워크 에이전트가 설치됨**, 및 **네트워크 에이전트가 실행 중**의 *예* 값).

Kaspersky Security Center 웹 콘솔 로그인 및 로그아웃

중앙 관리 서버와 웹 콘솔 서버를 설치한 후 Kaspersky Security Center 웹 콘솔에 로그인할 수 있습니다. 그러려면 설치 중에 지정한 포트 번호와 중앙 관리 서버의 웹 주소를 알고 있어야 합니다(기본 포트 번호는 8080). 그리고 브라우저에서 JavaScript가 활성화되어 있어야 합니다.

다음 방법을 사용하여 Kaspersky Security Center 웹 콘솔에 로그인할 수 있습니다.

- 도메인 인증 사용

  이 방법을 선택했다면 도메인 컨트롤러 검색이 활성화되었고 도메인 사용자가 중앙 관리 서버에 추가되었는지 확인하십시오.

- 도메인 사용자 이름과 암호 지정
- 관리자의 사용자 이름과 암호 지정

Kaspersky Security Center 웹 콘솔에 로그인하는 데 사용할 사용자 계정에 역할이 할당되어 있어야 합니다. 로그인하기 전에 도메인 또는 내부 사용자 계정에 역할이 할당되었는지 확인하십시오. 그렇지 않으면 로그인 오류가 발생합니다.

도메인 인증을 사용하여 로그인

도메인 인증을 사용하여 Kaspersky Security Center 웹 콘솔에 로그인하려면:

1. 브라우저에서 https://<Kaspersky Security Center 웹 콘솔 주소>:<포트 번호>로 이동합니다.
   로그인 페이지가 표시됩니다.
2. 신뢰할 수 있는 서버를 여러 개 추가한 경우 중앙 관리 서버 목록에서 연결할 중앙 관리 서버를 선택합니다.
   단일 중앙 관리 서버만 추가했다면 중앙 관리 서버 목록이 표시되지 않습니다.
3. 다음 중 하나를 수행합니다:
   - **도메인 인증 사용** 버튼을 클릭합니다.
   - 하나 이상의 가상 중앙 관리 서버가 생성된 서버에서 도메인 인증을 사용해 가상 서버에 로그인하려면:
     a. **가상 서버 옵션 표시**을 클릭합니다.
     b. 가상 서버 생성 시 지정한 가상 중앙 관리 서버 이름을 입력합니다.
     c. **도메인 인증 사용** 버튼을 클릭합니다.
4. 계정에 2단계 인증을 활성화했다면, 모바일 기기의 인증 앱에서 생성한 보안 코드를 입력합니다.
   필요하다면 로그인 페이지로 돌아갈 수 있습니다.

로그인하고 나면 마지막으로 사용한 언어와 테마가 적용된 대시보드가 표시됩니다. Kaspersky Security Center 웹 콘솔을 탐색하고 웹 콘솔을 통해 Kaspersky Security Center로 작업할 수 있습니다.

관리자의 사용자 이름과 암호를 지정하여 로그인

관리자의 사용자 이름과 암호를 지정하여 Kaspersky Security Center 웹 콘솔에 로그인하려면:

1. 브라우저에서 https://<Kaspersky Security Center 웹 콘솔 주소>:<포트 번호>로 이동합니다.
   로그인 페이지가 표시됩니다.

2. 신뢰할 수 있는 서버를 여러 개 추가한 경우 중앙 관리 서버 목록에서 연결할 중앙 관리 서버를 선택합니다.
   단일 중앙 관리 서버만 추가했다면 중앙 관리 서버 목록이 표시되지 않습니다.

3. 다음 중 하나를 수행합니다:

   - 도메인 사용자 계정으로 중앙 관리 서버에 로그인하려면 다음을 수행합니다.

     a. 도메인 사용자의 사용자 이름과 암호를 입력합니다.
        다음 형식 중 하나로 도메인 사용자의 사용자 이름을 입력할 수 있습니다.

        - 사용자 이름`@dns.domain`
        - `NTDOMAIN\`사용자 이름

     b. **로그인** 버튼을 클릭합니다.

     > 도메인 사용자 계정으로 로그인하기 전에 도메인 컨트롤러를 검색하여 도메인 사용자 목록을 얻으십시오.

   - 중앙 관리 서버에 로그인하려면:

     a. 로컬 관리자의 사용자 이름과 암호를 입력합니다.

     b. **로그인** 버튼을 클릭합니다.

   - 하나 이상의 가상 중앙 관리 서버가 생성된 서버에서 가상 서버에 로그인하려면:

     a. **가상 서버 옵션 표시**을 클릭합니다.

     b. 가상 서버 생성 시 지정한 가상 중앙 관리 서버 이름을 입력합니다.

     c. 가상 중앙 관리 서버에 대한 권한이 있는 관리자의 사용자 이름과 암호를 입력합니다.

     d. **로그인** 버튼을 클릭합니다.

4. 계정에 2단계 인증을 활성화했다면, 모바일 기기의 인증 앱에서 생성한 보안 코드를 입력합니다.
   필요하다면 로그인 페이지로 돌아갈 수 있습니다.

5. 계정에 강제 암호 변경을 설정했거나 암호가 만료되었다면, 암호 변경 창이 표시됩니다. Kaspersky Security Center 웹 콘솔 로그인을 위한 새 암호를 설정합니다.

로그인하고 나면 마지막으로 사용한 언어와 테마가 적용된 대시보드가 표시됩니다. Kaspersky Security Center 웹 콘솔을 탐색하고 웹 콘솔을 통해 Kaspersky Security Center로 작업할 수 있습니다.

로그아웃

Kaspersky Security Center 웹 콘솔에서 로그아웃하려면:

메인 메뉴에서 계정 설정으로 이동하여 **로그아웃**를 선택합니다.

Kaspersky Security Center 웹 콘솔이 닫히고 로그인 페이지가 표시됩니다.

Kaspersky Security Center 웹 콘솔의 ID 및 액세스 관리

이 섹션에서는 ID 및 액세스 관리(IAM이라고도 함)에 대한 정보를 제공합니다.

ID 및 액세스 관리 정보

ID 및 액세스 관리(또는 IAM이라고도 함)는 Kaspersky Security Center 웹 콘솔과 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스 간에 SSO(싱글 사인온)를 사용할 수 있게 해주는 Kaspersky Security Center 웹 콘솔 구성요소입니다. IAM은 OAuth 2.0 프로토콜을 사용하여 Kaspersky Security Center 웹 콘솔에서 Kaspersky Industrial CyberSecurity for Networks의 인증을 보장합니다.

이때, Kaspersky Security Center 웹 콘솔을 통해 액세스할 수 있는 Kaspersky Industrial CyberSecurity for Networks는 *리소스 서버*로 참조되고, Kaspersky Security Center 웹 콘솔 및 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스는 *OAuth 2.0 클라이언트*로 참조됩니다. 리소스 서버는 여러 사용자와 연동되고 인증이 필요한 프로그램입니다. 클라이언트는 리소스 서버에서의 인증을 위해 *토큰*을 사용합니다. 토큰은 고유한 바이트 시퀀스입니다. 토큰은 만료되면 자동으로 재발급됩니다. IAM은 여러 OAuth 2.0 클라이언트에 대해 단일 인증 서버 역할을 합니다.

Kaspersky Security Center 웹 콘솔 설치 시 IAM을 설치할 수 있습니다. Kaspersky Security Center 웹 콘솔 설정에서 나중에 언제든지 활성화할 수 있습니다. Kaspersky Industrial CyberSecurity 서버 또는 Kaspersky Industrial CyberSecurity 웹 인터페이스를 같은 중앙 관리 서버에서 관리하는 기기에 설치하면, IAM이 이 프로그램을 감지하고 Kaspersky Security Center 웹 콘솔에 이를 알리는 알림을 표시합니다. Kaspersky Industrial CyberSecurity for Networks를 등록한 후 나중에 Kaspersky Security Center 웹 콘솔과 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스 모두에 SSO를 사용할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서 로그아웃하면 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스의 세션도 종료되므로 Kaspersky Security Center 웹 콘솔에 다시 로그인해야 합니다.

ID 및 액세스 관리 활성화: 시나리오

필수 구성 요소

시작하기 전에 Kaspersky Industrial CyberSecurity for Networks 버전 3.1 이상에 액세스할 수 있는지 확인하십시오.

단계

ID 및 액세스 관리(IAM이라고도 함) 활성화는 단계적으로 진행됩니다.

1. **필요한 포트 확인**

   Kaspersky Security Center 웹 콘솔이 설치된 기기에서 포트 3333, 4004, 4444가 열려 있는지 확인합니다. 이러한 포트는 OAuth 2.0을 사용하는 데 필요합니다. 필요하다면 Kaspersky Security Center 웹 콘솔 설정 창에서 기본 포트 번호를 변경할 수 있습니다.

   Kaspersky Security Center 웹 콘솔은 포트 3333, 4004, 4444 외에도 다양한 목적을 위해 포트 4445, 2444, 2445를 사용합니다.

2. **ID 및 액세스 관리 설치**

   Kaspersky Security Center 웹 콘솔 설치 중에 ID 및 액세스 관리를 설치할지 지정합니다. 설치하지 않았다면 Kaspersky Security Center 웹 콘솔 설치 마법사를 다시 실행합니다.

3. **ID 및 액세스 관리 구성**

   Kaspersky Security Center 웹 콘솔 설정 창에서 **신원 및 접근 관리자(IAM)** 토글 버튼이 활성화되어 있는지 확인합니다. 또한 Kaspersky Security Center 웹 콘솔이 설치된 기기의 DNS 이름을 지정합니다. 클라이언트 애플리케이션이 이 기기에 연결됩니다.

4. **토큰 설정 지정**

   Kaspersky Security Center 웹 콘솔 설정 창에서 ID 및 액세스 관리가 사용할 토큰의 수명과 인증 시간 초과 값을 지정합니다. 기본값을 사용하거나 필요에 따라 고유한 값을 지정할 수 있습니다.

5. **인증서 부여**

   중앙 관리 서버에서 생성한 인증서를 사용하려면 Kaspersky Security Center 웹 콘솔 설정 창에서 IAM에서 사용하는 포트의 루트 인증서를 다운로드하여 Kaspersky Security Center 웹 콘솔 사용자의 워크스테이션에 배포합니다. 그렇지 않으면 Kaspersky Security Center 웹 콘솔에 연결하려고 할 때 사용자의 브라우저에 오류 메시지가 표시됩니다.

6. **Kaspersky Industrial CyberSecurity for Networks 서버 및 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스 등록**

   IAM이 설치되면 Kaspersky Security Center 웹 콘솔에 Industrial CyberSecurity for Networks 서버(또는 여러 서버)와 하나 이상의 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스가 등록 대기 중이라는 메시지가 표시됩니다. Kaspersky Industrial CyberSecurity for Networks 서버(또는 여러 서버) 및 웹 인터페이스(또는 여러 웹 인터페이스)를 등록하려면 이 메시지를 누르십시오.

결과

이 시나리오를 완료하면 SSO 및 IAM을 Kaspersky Industrial CyberSecurity for Networks 및 Kaspersky Security Center 웹 콘솔에 사용할 수 있습니다.

Kaspersky Security Center 웹 콘솔에서 ID 및 액세스 관리 구성

필요에 따라 ID 및 액세스 관리를 구성하려면 다음을 수행합니다.

1. 메인 메뉴에서 **설정** → **신원 및 접근 관리자**로 이동합니다.
2. **신원 및 접근 관리자** 섹션에서 ID 및 액세스 관리가 활성화되어 있는지 확인합니다.
3. **설정** 행의 **신원 및 접근 관리자 기기의 네트워크 이름** 링크를 클릭합니다.
4. ID 및 액세스 관리를 설치한 기기의 DNS 이름을 지정합니다. 클라이언트 애플리케이션이 이 기기에 연결됩니다.
5. 원한다면 관련 설정 그룹에 있는 **설정** 링크를 클릭해 기본 토큰 설정, 인증서 설정 및 포트 번호를 변경하십시오.

ID 및 액세스 관리가 활성화되어 필요에 따라 작동합니다.

Kaspersky Security Center 웹 콘솔에 Kaspersky Industrial CyberSecurity for Networks 애플리케이션 등록

Kaspersky Security Center 웹 콘솔을 통해 Kaspersky Industrial CyberSecurity for Networks 애플리케이션을 사용하기 시작하려면 먼저 Kaspersky Security Center 웹 콘솔에 등록해야 합니다.

Kaspersky Industrial CyberSecurity for Networks 애플리케이션을 등록하려면:

1. 다음이 완료되었는지 확인하십시오.

   - Kaspersky Industrial CyberSecurity for Networks 웹 플러그인을 다운로드하여 설치했습니다.

     하지만 Kaspersky Industrial CyberSecurity for Networks 서버가 중앙 관리 서버와 동기화될 때까지 기다렸다가 나중에 해도 됩니다.

   - 싱글 사인온(SSO) 기술 사용 준비 시나리오를 완료했습니다.

   - Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스에서 필요한 설정은 Kaspersky Security Center 페이지에 나와 있습니다. 자세한 내용은 Kaspersky Industrial CyberSecurity for Networks 온라인 도움말을 참조하십시오.

   - Kaspersky Security Center 웹 콘솔에 관리자 계정으로 로그인되어 있습니다.

   - IAM이 구성되어 있습니다.

2. Kaspersky Industrial CyberSecurity for Networks 서버가 설치되어 있는 기기를 미할당 기기 그룹에서 관리 중인 기기 그룹으로 이동합니다.

   a. 메인 메뉴에서 **발견 및 배포** → **미할당 기기**로 이동합니다.

   b. Kaspersky Industrial CyberSecurity for Networks 서버가 설치된 기기 옆의 확인란을 선택합니다.

   c. **소속 그룹 변경** 버튼을 누릅니다.

   d. 관리 그룹 계층에서 관리 중인 기기 그룹 옆에 있는 확인란을 선택합니다.

   e. **이동** 버튼을 누릅니다.

3. Kaspersky Industrial CyberSecurity for Networks 서버가 설치된 기기의 속성으로 이동합니다.

4. 기기 속성 페이지의 **일반** 섹션에서 **중앙 관리 서버와 계속 연결 유지** 옵션을 선택한 다음, **저장** 버튼을 누릅니다.

5. 기기 속성 페이지에서 **애플리케이션** 섹션을 선택합니다.

6. **애플리케이션** 섹션에서 Kaspersky 네트워크 에이전트를 선택합니다.

7. 애플리케이션의 현재 상태가 *중지됨*인 경우 *실행 중*으로 바뀔 때까지 기다립니다.

   최대 15분 정도 걸릴 수 있습니다. Kaspersky Industrial CyberSecurity for Networks 웹 플러그인을 아직 설치하지 않은 경우 지금 기다리는 동안 설치할 수 있습니다.

8. 메인 메뉴에서 **설정** → **신원 및 접근 관리자**로 이동합니다.

   등록 요청 필드에 보류 중인 요청이 하나 표시됩니다.

9. **등록 요청** 필드 아래의 **설정** 링크를 누릅니다.

10. 등록된 클라이언트 목록이 열리면 상태가 *보류 중*인 Kaspersky Industrial CyberSecurity for Networks 서버의 이름 옆에 있는 확인란을 선택한 다음, **승인** 버튼을 누릅니다.

    Kaspersky Industrial CyberSecurity for Networks 서버를 등록하지 않으려면 거부 버튼을 누르고, 나중에 이 목록으로 돌아갈 수 있습니다.

    승인 버튼을 누르고 나면 상태가 *승인됨*으로, 그리고 다시 *준비됨*으로 바뀝니다. 상태가 변경되지 않으면 새로 고침 버튼을 누르면 됩니다.

11. 등록된 클라이언트 목록을 닫고 **등록된 클라이언트** 필드의 값이 증가했는지 확인합니다.

12. 대시보드에 Kaspersky Industrial CyberSecurity for Networks 위젯을 추가하려면:

    a. 메인 메뉴에서 **모니터링 및 보고** → **대시보드**로 이동합니다.

    b. 대시보드에서 **웹 위젯 추가 또는 복원** 버튼을 누릅니다.

    c. 위젯 메뉴가 열리면 **Other**를 선택합니다.

    d. Kaspersky Industrial CyberSecurity for Networks 위젯을 선택합니다.

    이제 위젯의 링크를 사용하여 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스로 이동할 수 있습니다.

등록 절차를 완료하고 나면 새 버튼, **Kaspersky Security Center**가 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스의 로그인 페이지에 나타납니다. 이 버튼을 눌러서 Kaspersky Security Center 자격 증명으로 Kaspersky Industrial CyberSecurity for Networks 웹 인터페이스에 로그인할 수 있습니다.

ID 및 액세스 관리의 토큰 수명 및 인증 시간 초과 값

ID 및 액세스 관리(IAM이라고도 함)를 구성할 때 토큰 수명 및 인증 시간 초과 값에 대한 설정을 지정해야 합니다. 기본 설정은 보안 표준과 서버 부하를 모두 반영하도록 설계되었습니다. 그러나 조직의 정책에 따라 이러한 설정을 변경할 수 있습니다.

IAM은 토큰이 만료되려고 할 때 자동으로 토큰을 재발급합니다.

아래 표에는 기본 토큰 수명 설정이 나와 있습니다.

토큰 수명 설정

토큰	기본 수명(초)	설명
ID 토큰(id_token)	86400	OAuth 2.0 클라이언트(즉, Kaspersky Security Center 웹 콘솔 또는 Kaspersky Industrial CyberSecurity 콘솔)에서 사용하는 ID 토큰입니다. IAM은 사용자에 대한 정보가 포함된 ID 토큰(즉, 사용자 프로필)을 클라이언트로 보냅니다.
접근 토큰(access_token)	86400	IAM으로 식별된 리소스 소유자를 대신하여 리소스 서버에 액세스하기 위해 OAuth 2.0 클라이언트에서 사용하는 액세스 토큰입니다.
새로 고침 토큰(refresh_token)	172800	OAuth 2.0 클라이언트는 이 토큰을 사용하여 ID 토큰과 액세스 토큰을 재발급합니다.

아래 표에는 auth_code 및 login_consent_request에 대한 시간 초과 값이 나와 있습니다.

설정	연결 시간 제한 (초)	설명
인증 코드(auth_code)	3600	토큰에 대한 코드를 교환하는 시간 초과. OAuth 2.0 클라이언트는 이 코드를 리소스 서버에 보내고 그 대가로 액세스 토큰을 받습니다.
로그인 동의 요청 시간 초과 (login_consent_request)	3600	사용자 권한을 OAuth 2.0 클라이언트에 위임하는 시간 초과.

토큰에 대한 자세한 내용은 OAuth 웹사이트를 참조하십시오.

탐지된 마우스 또는 키보드 활동이 없는 클라이언트에 대해 시간 초과를 구성하려면 다음을 따릅니다.

1. Kaspersky Security Center 웹 콘솔의 설치 폴더에서 config.json 파일을 찾아 엽니다. 파일에는 유휴 클라이언트의 시간 초과를 구성하는 파라미터가 포함되어 있습니다.
2. `clientIdleTimeout` 파라미터를 사용하여 비활성 클라이언트가 경고 팝업을 표시할 때까지의 시간을 밀리초 단위로 지정합니다.
3. `clientLogoutTimeout` 파라미터를 사용하여 비활성 클라이언트에 대한 IAM 인증이 종료되는 시간을 밀리초 단위로 지정합니다. `clientLogoutTimeout`는 `clientIdleTimeout` 이후부터 순차적으로 내려갑니다.

IAM 인증서 다운로드 및 배포

기본적으로 ID 및 액세스 관리는 중앙 관리 서버에서 생성한 인증서를 사용하여 브라우저에 Kaspersky Security Center 웹 콘솔에 대한 액세스 권한을 부여합니다. 그러나 원하는 경우 사용자 지정 인증서를 사용할 수 있습니다. 어떤 인증서를 사용하든 Kaspersky Security Center 웹 콘솔 사용자가 Kaspersky Security Center 웹 콘솔에 액세스하는 모든 워크스테이션이 이 인증서를 신뢰하는지 확인해야 합니다.

인증서를 다운로드하고 배포하려면:

1. 메인 메뉴에서 **설정 → 신원 및 접근 관리자**로 이동합니다.
2. 각 인증서에 대해 관련 설정 그룹 아래의 **설정** 링크를 클릭하고, 다음 중 하나를 수행합니다.
   - Kaspersky Security Center 웹 콘솔을 설치하는 동안 중앙 관리 서버에서 생성한 인증서를 사용하려면:
     1. 인증서 속성 창이 열리면 **중앙 관리 서버에서 생성된 인증서**를 선택합니다.
     2. **다운로드** 버튼을 눌러 인증서를 다운로드합니다.
     3. 다운로드한 인증서를 Kaspersky Security Center 웹 콘솔 사용자가 Kaspersky Security Center 웹 콘솔에 액세스하는 모든 워크스테이션에 배포합니다.
   - 사용하려는 인증서가 있는 경우:
     1. 인증서 속성 창이 열리면 **사용자 지정 TLS 인증서**를 선택합니다.
     2. 인증서 파일과 개인 키를 선택합니다.
     3. **확인** 버튼을 누릅니다.
     4. 사용자가 Kaspersky Security Center 웹 콘솔 또는 Kaspersky Industrial CyberSecurity 콘솔에 액세스하는 모든 워크스테이션에 인증서를 배포합니다.

인증서는 사용자에게 Kaspersky Security Center 웹 콘솔 및 Kaspersky Industrial CyberSecurity 콘솔에 대한 액세스 권한을 부여합니다.

모든 인증서를 적시에 재발급해야 합니다. 중앙 관리 서버에서 생성한 인증서는 수동으로 다시 생성해야 합니다. Kaspersky Security Center 웹 콘솔 설치 프로그램을 통해 생성된 인증서는 설치 프로그램을 사용하여 다시 생성해야 합니다.

ID 및 액세스 관리 비활성화

필요한 경우 ID 및 액세스 관리(IAM이라고도 함)를 비활성화할 수 있습니다.

IAM을 중지하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **설정** → **통합** 섹션으로 이동합니다.
2. **신원 및 접근 관리자** 섹션에서 **신원 및 접근 관리자** 토글 버튼을 사용 안 함으로 전환합니다.

   나중에 언제든지 IAM을 활성화할 수 있습니다.

설치 프로그램을 통해 Kaspersky Security Center 웹 콘솔을 업데이트하고 IAM을 설치하지 않겠다고 지정하면, Kaspersky Security Center 웹 콘솔이 업그레이드되고 IAM은 설치되지 않습니다. Kaspersky Industrial CyberSecurity for Networks와의 통합에 대한 모든 정보는 물론, IAM 구성 파일 및 로그 파일도 기기에서 삭제됩니다.

NTLM 및 Kerberos 프로토콜을 사용하여 도메인 인증 구성

Kaspersky Security Center 15.1을 통해 NTLM 및 Kerberos 프로토콜을 사용하여 OpenAPI에서 도메인 인증을 사용할 수 있습니다. 도메인 인증을 사용하면 Windows 사용자가 회사 네트워크에 암호를 다시 입력할 필요 없이(싱글 사인온) Kaspersky Security Center 웹 콘솔에서 보안 인증을 활성화할 수 있습니다.

Kerberos 프로토콜을 통한 OpenAPI의 도메인 인증에는 다음과 같은 제한이 있습니다.

- Kaspersky Security Center 웹 콘솔 사용자는 Kerberos 프로토콜을 사용하여 Active Directory에서 인증되어야 합니다. 사용자는 유효한 Kerberos Ticket Granting Ticket(TGT라고도 함)을 가지고 있어야 합니다. 도메인에 인증하면 TGT가 자동으로 발급됩니다.
- 브라우저에서 Kerberos 인증을 구성해야 합니다. 자세한 내용은 사용 중인 브라우저의 설명서를 참조하십시오.

Kerberos 프로토콜을 사용하여 도메인 인증을 사용하려면 네트워크가 다음 조건을 충족해야 합니다.

- 중앙 관리 서버는 도메인 계정 이름으로 실행해야 합니다.
- Kaspersky Security Center 웹 콘솔 서버는 중앙 관리 서버가 설치되어 있는 동일한 기기에 설치해야 합니다.

- 중앙 관리 서버 계정용으로 다음 서비스 사용자 이름(SPN)을 지정해야 합니다.
  - "http/<server.fqnd.name>"
  - "http/<server>"

  여기에서 <server>는 중앙 관리 서버 기기의 네트워크 이름입니다. <server.fqnd.name>은 중앙 관리 서버 기기의 FQDN 이름입니다.
- 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에 연결할 때 중앙 관리 서버 주소는 서비스 사용자 이름(SPN)이 등록된 주소로 정확히 지정해야 합니다. <server.fqnd.name> 또는 <server>로 지정할 수 있습니다.
- 암호 없이 로그인하려면 Kaspersky Security Center 웹 콘솔로 열리는 브라우저 프로세스가 도메인 계정에서 실행되어야 합니다.

Kerberos 및 NTLM 프로토콜은 Kaspersky Security Center 15.1용 OpenAPI에서만 지원됩니다. Kaspersky Security Center Linux용 OpenAPI에서는 지원되지 않습니다.

중앙 관리 서버 구성

이 섹션에서는 Kaspersky Security Center 중앙 관리 서버의 구성 프로세스 및 속성에 대해 설명합니다.

Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 연결 구성

중앙 관리 서버의 연결 포트를 설정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **연결 포트** 섹션을 선택합니다.

선택한 서버의 주요 연결 설정이 애플리케이션에 표시됩니다.

Kaspersky Security Center 웹 콘솔은 SSL 포트 TCP 13299를 통해 관리 서버에 연결됩니다. klakaut 자동화 개체에서 같은 포트를 사용할 수 있습니다.

포트 TCP 14000은 Kaspersky Security Center 웹 콘솔, 배포 지점, 보조 중앙 관리 서버, klakaut 자동화 개체 연결 및 클라이언트 기기 데이터 검색에만 사용됩니다.

일반적으로 SSL 포트 TCP 13000은 DMZ의 네트워크 에이전트, 보조 중앙 관리 서버, 기본 중앙 관리 서버에서만 사용할 수 있습니다. SSL 포트 13000을 통해 Kaspersky Security Center 웹 콘솔을 연결해야 할 때도 있습니다.

- SSL 포트 한 개를 Kaspersky Security Center 웹 콘솔과 기타 활동 모두에 사용할 가능성이 있을 때(클라이언트 기기 데이터 검색, 배포 지점 연결, 보조 중앙 관리 서버 연결).
- klakaut 자동화 개체가 중앙 관리 서버에 직접 연결되지 않고 DMZ의 배포 지점을 통해 연결된 경우.

중앙 관리 서버 연결 이벤트 로깅 기록

중앙 관리 서버가 작동하는 동안 중앙 관리 서버로의 연결 및 연결 시도 내역을 로그 파일에 저장할 수 있습니다. 이 파일의 정보를 통해 네트워크 인프라 내의 연결뿐 아니라 서버에 무단으로 접근하려는 시도도 추적할 수 있습니다.

중앙 관리 서버와의 연결 이벤트를 기록하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **연결 포트** 섹션을 선택합니다.
3. **중앙 관리 서버 연결 이벤트 기록** 옵션을 활성화합니다.

   중앙 관리 서버와의 인바운드 연결, 인증 결과 및 SSL 오류와 관련된 모든 이후 이벤트가 %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog 파일에 저장됩니다.

중앙 관리 서버의 인터넷 액세스 설정 구성

Kaspersky Security Network를 사용하고, Kaspersky Security Center 및 관리 중인 Kaspersky 애플리케이션용 안티바이러스 데이터베이스의 업데이트를 다운로드하려면 인터넷 접속을 구성해야 합니다.

중앙 관리 서버의 인터넷 접속 설정을 지정하려면:

1. 메인 메뉴에서 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **인터넷 연결 구성** 섹션을 선택합니다.
3. 인터넷에 연결할 때 프록시 서버를 사용하려면 **프록시 서버 사용** 옵션을 활성화합니다. 이 옵션을 활성화하면 설정을 입력하는 필드를 사용할 수 있습니다. 프록시 서버 연결에 대해 다음 설정을 지정합니다.

   - **주소**

     Kaspersky Security Center에서 인터넷 연결에 사용한 프록시 서버의 주소입니다.

   - **포트 번호**

     Kaspersky Security Center 프록시 연결을 설정하는 데 사용되는 포트 번호입니다.

   - **로컬 주소에서 프록시 서버 사용 안 함**

     로컬 네트워크에서 기기로 연결하는 데 프록시 서버가 사용되지 않습니다.

- **프록시 서버 인증**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.

  프록시 서버 사용 확인란을 선택하면 이 입력 필드를 사용할 수 있습니다.

- **사용자 이름**

  프록시 서버에 대한 연결을 구성할 사용자 계정입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

- **암호**

  프록시 서버 연결을 구성한 계정의 사용자가 설정한 암호입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

  입력한 암호를 보려면 **보기** 버튼을 필요한 시간 동안 누르고 있어야 합니다.

빠른 시작 마법사를 사용하여 인터넷 액세스를 구성할 수도 있습니다.

이벤트 저장소에 저장되는 최대 이벤트 수 설정

중앙 관리 서버 속성 창의 **이벤트 저장소** 섹션에서 이벤트 레코드 개수 및 레코드 저장 기간을 제한해 중앙 관리 서버 데이터베이스의 이벤트 저장 설정을 편집할 수 있습니다. 최대 이벤트 수를 지정하면 애플리케이션은 지정된 이벤트 수에 필요한 스토리지 공간의 대략적인 양을 계산합니다. 이 대략적인 계산 결과 값을 사용하여 디스크의 사용 가능한 공간이 데이터베이스 초과 상황을 방지하기에 충분한지 여부를 평가할 수 있습니다. 중앙 관리 서버 데이터베이스의 기본 용량은 400,000개 이벤트입니다. 데이터베이스의 최대 권장 용량은 4,500만개 이벤트입니다.

애플리케이션은 10분마다 데이터베이스를 확인합니다. 이벤트 수가 지정된 최댓값이나 10,000에 도달하면 애플리케이션은 지정된 최대 이벤트 수만 남도록 가장 오래된 이벤트를 삭제합니다.

중앙 관리 서버가 오래된 이벤트를 삭제할 때에는 새 이벤트를 데이터베이스에 저장할 수 없습니다. 이 기간 동안에는 거부된 이벤트 관련 정보가 Kaspersky 이벤트 로그에 기록됩니다. 새 이벤트는 대기열에 보관되었다가 삭제 작업이 완료되고 나면 데이터베이스에 저장됩니다.

중앙 관리 서버의 이벤트 저장소에 저장할 수 있는 이벤트 수를 제한하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.

   중앙 관리 서버 속성 창이 열립니다.

2. **일반** 탭에서 **이벤트 저장소** 섹션을 선택합니다. 데이터베이스에 저장되는 최대 이벤트 수를 지정합니다.

3. **저장** 버튼을 누릅니다.

추가로 다음 작업을 수행할 수 있습니다.

- 모든 작업의 설정을 변경하여 작업 진행과 관련된 이벤트를 저장하거나 작업 실행 결과만 저장할 수 있습니다.
- 관리 중인 기기에 설치된 중앙 관리 서버, 네트워크 에이전트 및 Kaspersky 애플리케이션 이벤트의 저장 기간을 줄이거나 중지합니다.

이렇게 하면 데이터베이스의 이벤트 수를 줄이고, 데이터베이스의 이벤트 테이블에 대한 분석과 관련된 시나리오의 실행 속도를 높이며 다량의 이벤트가 심각 이벤트를 덮어쓰는 위험을 줄일 수 있습니다.

UEFI 보호 기기의 연결 설정

*UEFI 보호 기기*는 BIOS 수준에서 통합된 UEFI용 Kaspersky 솔루션 또는 애플리케이션이 설치된 기기입니다. 통합 보호 기능은 시스템이 시작되는 순간부터 기기 보안을 시작하며 통합 소프트웨어가 없는 기기에 대한 보호는 보안 제품이 시작된 이후에만 기능을 시작합니다. Kaspersky Security Center는 이러한 기기에 대한 관리를 지원합니다.

UEFI 보호 기기의 연결 설정을 수정하려면 다음과 같이 진행합니다:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **추가 포트** 섹션을 선택합니다.
3. 관련 설정을 수정합니다.
   - **UEFI 보호 기기 및 KasperskyOS 기기용 포트 열기**

     UEFI 보호 기기가 중앙 관리 서버에 연결할 수 있습니다.
   - **UEFI 보호 기기 및 KasperskyOS 기기용 포트**

     UEFI 보호 기기 및 KasperskyOS 기기용 포트 열기 옵션을 활성화하는 경우 포트 번호를 변경할 수 있습니다. 기본 포트 번호는 13294입니다.
4. **저장** 버튼을 누릅니다.

이제 UEFI 보호 기기를 중앙 관리 서버에 연결할 수 있습니다.

중앙 관리 서버 계층 만들기 및 보조 중앙 관리 서버 추가

보조 중앙 관리 서버 추가(향후 기본 중앙 관리 서버에서 수행)

중앙 관리 서버를 보조 중앙 관리 서버로 추가하여 '기본/보조' 계층을 구축할 수 있습니다.

Kaspersky Security Center 웹 콘솔을 통해 연결하여 사용할 수 있는 보조 중앙 관리 서버를 추가하려면 다음 단계를 따릅니다.

1. 향후 기본 중앙 관리 서버의 13000 포트가 보조 중앙 관리 서버에서 보내는 연결 데이터를 수신할 수 있는지 확인하십시오.
2. 향후 기본 중앙 관리 서버에서 설정 아이콘( )을 누릅니다.
3. 속성 페이지가 열리면 **중앙 관리 서버** 탭을 누릅니다.
4. 중앙 관리 서버를 추가하려는 관리 그룹 이름 옆의 확인란을 선택합니다.

5. 메뉴 줄에서 **보조 중앙 관리 서버 연결**을 누릅니다.
   보조 중앙 관리 서버 추가 마법사를 시작합니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

6. 다음 필드에 내용을 입력합니다:

   - **DMZ에 있는 보조 중앙 관리 서버에 기본 중앙 관리 서버 연결**

     보조 중앙 관리 서버가 DMZ(완충 지역)에 있는 경우 이 옵션을 선택합니다.
     이 옵션을 선택하면 **보조 서버 주소** 파라미터를 지정해야 합니다.
     이 옵션을 선택하면 기본 중앙 관리 서버가 보조 중앙 관리 서버에 대한 연결을 시작합니다. 그렇지 않으면 보조 중앙 관리 서버가 주 중앙 관리 서버에 대한 연결을 시작합니다.

   - **보조 중앙 관리 서버 표시 이름**

     계층 구조에서 보조 중앙 관리 서버가 표시되는 이름을 지정합니다. 원하는 경우 IP 주소를 이름으로 입력하거나 '그룹 1의 보조 서버'와 같은 이름을 사용할 수 있습니다.

   - **보조 중앙 관리 서버 주소(선택 사항)**

     보조 중앙 관리 서버의 IP 주소 또는 도메인 이름을 지정합니다.
     이 매개변수는 **DMZ에서 기본 중앙 관리 서버를 보조 중앙 관리 서버에 연결** 옵션을 활성화했을 때 필요합니다.

   - **중앙 관리 서버 SSL 포트**

     기본 중앙 관리 서버의 SSL 포트 번호를 지정합니다. 기본 포트 번호는 13000입니다.

   - **중앙 관리 서버 API 포트**

     OpenAPI를 통해 연결을 수신하는 데 사용할 기본 중앙 관리 서버의 포트 번호를 지정합니다. 기본 포트 번호는 13299입니다.

7. 보조 중앙 관리 서버용 인증서를 지정합니다. **보조 서버 주소** 파라미터를 지정했다면 **보조 중앙 관리 서버**에서 가져오기 버튼을 클릭하여 인증서를 가져올 수 있습니다. **인증서 파일 찾아보기** 버튼을 누르고 인증서 파일을 찾을 수도 있습니다.

8. 연결 설정을 지정합니다:

   - 향후 기본 중앙 관리 서버의 주소를 입력합니다.

   - 향후 보조 중앙 관리 서버에서 프록시 서버를 사용한다면, 프록시 서버 주소와 사용자 자격 증명을 입력하여 프록시 서버에 연결합니다.

9. 향후 보조 중앙 관리 서버에 대한 액세스 권한이 있는 사용자의 자격 증명을 입력합니다.

10. 2단계 인증을 활성화하고 구성했다면 인증 앱에서 생성한 보안 코드를 지정합니다.
    이 계정에 대해 2단계 인증을 활성화했다면, 향후 보조 서버에서만 계층을 생성할 수 있습니다(아래 지침 참조).

연결 설정이 올바르면 향후 보조 서버와의 연결이 설정되고 "기본/보조" 계층 구조가 구축됩니다. 연결 실패 시,

연결 설정을 확인하거나 향후 보조 서버의 인증서를 수동으로 지정하십시오.

기본 및 보조 중앙 관리 서버 간의 연결은 포트 13000을 통해 설정됩니다. 기본 중앙 관리 서버의 작업과 정책이 수신되어 적용됩니다. 보조 중앙 관리 서버가 기본 중앙 관리 서버에서 추가된 관리 그룹에 표시됩니다.

보조 중앙 관리 서버 추가(향후 보조 중앙 관리 서버에서 수행)

향후 보조 중앙 관리 서버가 일시적으로 연결이 끊겼거나 연결할 수 없는 등의 상태여서 해당 서버에 연결할 수 없더라도 보조 중앙 관리 서버를 추가할 수 있습니다.

Kaspersky Security Center 웹 콘솔을 통해 연결하여 사용할 수 없는 중앙 관리 서버를 보조 중앙 관리 서버로 추가하려면 다음 단계를 따릅니다.

1. 향후 기본 중앙 관리 서버 인증서 파일을 향후 보조 중앙 관리 서버를 둘 사무실의 시스템 관리자에게 보냅니다(플래시 드라이브와 같은 외부 기기에 파일을 쓰거나 이메일 등으로 보낼 수 있습니다).

   인증서 파일은 향후 기본 중앙 관리 서버(%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer)에 있습니다.

2. 향후 보조 중앙 관리 서버를 담당하는 시스템 관리자에게 다음 작업을 수행하도록 합니다.

   a. 설정 아이콘( )을 누릅니다.

   b. 속성 페이지가 열리면 **일반** 탭의 **중앙 관리 서버 계층 구조** 섹션으로 이동합니다.

   c. **이 중앙 관리 서버는 계층 구조에서 보조임** 확인란을 선택합니다.

   d. **기본 중앙 관리 서버 주소** 필드에 향후 기본 중앙 관리 서버의 네트워크 이름을 입력합니다.

   e. **찾기**를 눌러 이전에 저장한 향후 기본 중앙 관리 서버의 인증서 파일을 선택합니다.

   f. 필요하다면 **DMZ에 있는 보조 중앙 관리 서버에 기본 중앙 관리 서버 연결** 확인란을 선택합니다.

   g. 향후 보조 중앙 관리 서버에 대한 연결을 프록시 서버를 통해 수행하는 경우 **프록시 서버 사용** 옵션을 선택하고 연결 설정을 지정합니다.

   h. **저장**을 누릅니다.

'기본/보조' 계층이 구축됩니다. 기본 중앙 관리 서버는 포트 13000을 통해 보조 중앙 관리 서버에서 보내는 연결을 시작합니다. 기본 중앙 관리 서버의 작업과 정책이 수신되어 적용됩니다. 보조 중앙 관리 서버가 기본 중앙 관리 서버에서 추가된 관리 그룹에 표시됩니다.

보조 중앙 관리 서버의 목록 보기

보조 중앙 관리 서버(가상 중앙 관리 서버 포함) 목록을 확인하려면 다음 단계를 따릅니다.

메인 메뉴에서, 설정 아이콘( ) 옆에 있는 중앙 관리 서버의 이름을 누릅니다.

보조 중앙 관리 서버(가상 중앙 관리 서버 포함)의 드롭다운 목록이 표시됩니다.

이름을 눌러 이러한 중앙 관리 서버로 이동할 수 있습니다.

관리 그룹도 표시되지만 회색으로 표시되어 이 메뉴에서 관리할 수 없습니다.

Kaspersky Security Center 웹 콘솔에서 기본 중앙 관리 서버에 연결되어 있고 보조 중앙 관리 서버에서 관리하는 가상 중앙 관리 서버에 연결할 수 없을 시, 다음 방법의 하나를 사용할 수 있습니다:

- **기존 Kaspersky Security Center 웹 콘솔 설치를 수정하여 보조 서버를 신뢰하는 중앙 관리 서버 목록에 추가합니다.** 그러면 Kaspersky Security Center 웹 콘솔에서 가상 중앙 관리 서버에 연결할 수 있습니다.

  1. Kaspersky Security Center 웹 콘솔이 설치된 기기에서 관리자 권한이 있는 계정으로 ksc-web-console-<버전 번호>.<빌드 번호>.exe 설치 파일을 실행합니다.

     설치 마법사가 시작됩니다. **다음** 버튼으로 마법사를 진행합니다.
  2. **업그레이드** 옵션을 선택합니다.
  3. **수정 유형** 단계에서 **연결 설정 편집** 옵션을 선택합니다.
  4. **신뢰할 수 있는 중앙 관리 서버** 단계에서 필요한 보조 관리 서버를 추가합니다.
  5. 마지막 단계에서 **수정**을 눌러 새 설정을 적용합니다.
  6. 애플리케이션 재구성이 성공적으로 완료되면 **마침** 버튼을 누릅니다.

- Kaspersky Security Center 웹 콘솔을 사용하여 가상 서버가 생성된 보조 중앙 관리 서버에 직접 연결합니다. 그런 다음 Kaspersky Security Center 웹 콘솔에서 가상 중앙 관리 서버로 전환할 수 있습니다.
- MMC 기반 중앙 관리 콘솔을 사용하여 가상 서버에 직접 연결합니다.

중앙 관리 서버의 계층 구조 삭제

중앙 관리 서버의 계층을 더 이상 원하지 않는 경우 이 계층에서 연결을 끊을 수 있습니다.

중앙 관리 서버의 계층을 삭제하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 기본 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
2. 페이지가 열리면 **중앙 관리 서버** 탭으로 이동합니다.
3. 보조 중앙 관리 서버를 삭제할 관리 그룹에서 보조 중앙 관리 서버를 선택합니다.
4. 메뉴 줄에서 **삭제**를 누릅니다.
5. 창이 열리면 **확인**을 눌러 보조 중앙 관리 서버를 삭제를 확인합니다.

이전 기본 중앙 관리 서버와 이전 보조 중앙 관리 서버는 이제 서로 독립적입니다. 계층이 더 이상 존재하지 않습니다.

중앙 관리 서버 점검

중앙 관리 서버 유지 관리를 통해 중앙 관리 서버 폴더의 공간을 확보하고 불필요한 개체를 삭제하여 데이터베이스의 크기를 줄일 수 있습니다. 이는 애플리케이션의 성능 및 작동 안정성 개선에 도움이 됩니다. 적어도 매주마다 중앙 관리 서버를 유지보수하시기 바랍니다.

중앙 관리 서버 유지보수는 전용 작업을 통해 수행됩니다. 이 애플리케이션은 중앙 관리 서버 유지보수 시 다음 동작을 수행합니다.

- 저장소 폴더에서 불필요한 폴더와 파일을 삭제합니다.
- 표에서 불필요한 레코드(또는 "허상 포인터")를 삭제합니다.
- 캐시를 지웁니다.
- 데이터베이스 유지 관리(SQL Server 또는 PostgreSQL을 DBMS로 사용할 시):
  - 데이터베이스 오류를 확인합니다(SQL Server에서만 사용 가능).
  - 데이터베이스 인덱스 재편성.
  - 데이터베이스 통계 업데이트.
  - 데이터베이스 줄임(필요 시).

중앙 관리 서버 점검 작업은 Kaspersky Security Center를 설치하면 자동으로 생성됩니다. 중앙 관리 서버 점검 작업이 삭제된 경우 수동으로 만들 수 있습니다.

중앙 관리 서버 점검 작업을 만들려면 다음과 같이 하십시오.

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가** 버튼을 클릭합니다.
   새 작업 마법사가 시작됩니다.
3. 마법사의 **새 작업 설정** 창에서 **중앙 관리 서버 점검**을 작업 유형으로 선택하고 **다음**을 누릅니다.
4. 마법사의 나머지 지침을 따릅니다.

그러면 작업 목록에 새로 생성된 작업이 나타납니다. 하나의 중앙 관리 서버에서는 하나의 중앙 관리 서버 점검 작업만이 수행됩니다. 중앙 관리 서버를 위한 중앙 관리 서버 점검 작업이 이미 생성이 되었다면, 새로운 중앙 관리 서버 점검 작업을 만들 수 없습니다.

인터페이스 구성

사용 중인 기능에 따라 섹션과 인터페이스 구성 요소를 표시하고 숨기도록 Kaspersky Security Center 웹 콘솔 인터페이스를 구성할 수 있습니다.

현재 사용 중인 기능 세트에 따라 Kaspersky Security Center 웹 콘솔 인터페이스를 구성하려면 다음 단계를 따릅니다:

1. 메인 메뉴에서 계정 설정으로 이동하여 **인터페이스 옵션**을 선택합니다.
2. **인터페이스 옵션** 창이 열리면 필요한 옵션을 활성화 또는 비활성화합니다.
3. **저장**을 누릅니다.

그 후, 콘솔이 활성화된 옵션에 따라 기본 메뉴에 섹션을 표시합니다. 예를 들어, **EDR 경고 표시**를 활성화하면 메인 메뉴에 **모니터링 및 보고 → 경고** 섹션이 나타납니다.

가상 중앙 관리 서버 관리

이 섹션에서는 가상 중앙 관리 서버를 관리하는 다음 방법에 대해 설명합니다.

- 가상 중앙 관리 서버 만들기
- 가상 중앙 관리 서버 활성화 및 비활성화
- 가상 중앙 관리 서버에 관리자 할당
- 클라이언트 기기의 중앙 관리 서버 변경
- 가상 중앙 관리 서버 삭제

가상 중앙 관리 서버 만들기

가상 중앙 관리 서버를 생성하여 관리 그룹에 추가할 수 있습니다.

가상 중앙 관리 서버를 만들면 사용자 목록과 기본 중앙 관리 서버의 모든 사용자 권한을 상속합니다. 사용자에게 기본 서버에 대한 액세스 권한이 있다면 이 사용자는 가상 서버에 대한 액세스 권한도 가집니다. 생성 후 서버에 대한 액세스 권한을 독립적으로 구성합니다.

가상 중앙 관리 서버를 생성하여 추가하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
2. 페이지가 열리면 **중앙 관리 서버** 탭으로 이동합니다.
3. 가상 중앙 관리 서버를 추가할 관리 그룹을 선택합니다.
   가상 중앙 관리 서버는 선택한 그룹(하위 그룹 포함)의 기기를 관리합니다.
4. 메뉴 줄에서 **새 가상 중앙 관리 서버**를 누릅니다.

5. 페이지가 열리면 새 가상 중앙 관리 서버의 속성을 정의합니다.

   - **가상 중앙 관리 서버 이름**.
   - **중앙 관리 서버 연결 주소**
     중앙 관리 서버의 이름이나 IP 주소를 지정할 수 있습니다.

6. 사용자 목록에서 가상 중앙 관리 서버 관리자를 선택합니다. 원하는 경우 기존 계정 중 하나를 편집한 다음 관리자 역할을 할당하거나 새 사용자 계정을 생성할 수 있습니다.

7. **저장**을 누릅니다.

새 가상 중앙 관리 서버가 생성되어 관리 그룹에 추가되며 **중앙 관리 서버** 탭에 표시됩니다.

Kaspersky Security Center 웹 콘솔에서 기본 중앙 관리 서버에 연결되어 있고 보조 중앙 관리 서버에서 관리하는 가상 중앙 관리 서버에 연결할 수 없을 시, 다음 방법의 하나를 사용할 수 있습니다:

- **기존 Kaspersky Security Center 웹 콘솔 설치를 수정하여 보조 서버를 신뢰하는 중앙 관리 서버 목록에 추가합니다.** 그러면 Kaspersky Security Center 웹 콘솔에서 가상 중앙 관리 서버에 연결할 수 있습니다.

  1. Kaspersky Security Center 웹 콘솔이 설치된 기기에서 관리자 권한이 있는 계정으로 ksc-web-console-<버전 번호>.<빌드 번호>.exe 설치 파일을 실행합니다.
     설치 마법사가 시작됩니다. **다음** 버튼으로 마법사를 진행합니다.
  2. **업그레이드** 옵션을 선택합니다.
  3. **수정 유형** 단계에서 **연결 설정 편집** 옵션을 선택합니다.
  4. **신뢰할 수 있는 중앙 관리 서버** 단계에서 필요한 보조 관리 서버를 추가합니다.
  5. 마지막 단계에서 **수정**을 눌러 새 설정을 적용합니다.
  6. 애플리케이션 재구성이 성공적으로 완료되면 **마침** 버튼을 누릅니다.

- Kaspersky Security Center 웹 콘솔을 사용하여 가상 서버가 생성된 보조 중앙 관리 서버에 직접 연결합니다. 그런 다음 Kaspersky Security Center 웹 콘솔에서 가상 중앙 관리 서버로 전환할 수 있습니다.
- MMC 기반 중앙 관리 콘솔을 사용하여 가상 서버에 직접 연결합니다.

가상 중앙 관리 서버 활성화 및 비활성화

새 가상 중앙 관리 서버를 만들면 기본적으로 활성화됩니다. 언제든지 다시 비활성화하거나 활성화할 수 있습니다. 가상 중앙 관리 서버의 비활성화 또는 활성화는 실제 중앙 관리 서버를 켜거나 끄는 것과 같습니다.

가상 중앙 관리 서버를 활성화 또는 비활성화하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
2. 페이지가 열리면 **중앙 관리 서버** 탭으로 이동합니다.

3. 활성화하거나 비활성화할 가상 중앙 관리 서버를 선택합니다.

4. 메뉴 줄에서 **가상 중앙 관리 서버 활성화/비활성화** 버튼을 누릅니다.

가상 중앙 관리 서버 상태는 이전 상태에 따라 활성화 또는 비활성화로 변경됩니다. 업데이트된 상태가 중앙 관리 서버 이름 옆에 표시됩니다.

가상 중앙 관리 서버의 관리자 정보

조직에서 가상 중앙 관리 서버를 사용 시, 각 가상 중앙 관리 서버에 전담 관리자를 할당할 수 있습니다. 예를 들어 조직의 별도 사무실이나 부서를 관리하기 위해 가상 중앙 관리 서버를 만들거나, MSP 공급자이고 가상 중앙 관리 서버를 통해 테넌트를 관리한다면 이 기능이 유용할 수 있습니다.

가상 중앙 관리 서버를 만들면 사용자 목록과 기본 중앙 관리 서버의 모든 사용자 권한을 상속합니다. 사용자에게 기본 서버에 대한 액세스 권한이 있다면 이 사용자는 가상 서버에 대한 액세스 권한도 가집니다. 생성 후 서버에 대한 액세스 권한을 독립적으로 구성합니다. 가상 중앙 관리 서버에만 관리자를 지정하려면 관리자에게 기본 중앙 관리 서버에 대한 액세스 권한이 없는지 확인하십시오.

가상 중앙 관리 서버에 대한 관리자 액세스 권한을 부여하여 가상 중앙 관리 서버의 관리자를 할당합니다. 다음 방법 중 하나로 필요한 접근 권한을 부여할 수 있습니다:

- 관리자의 액세스 권한을 수동으로 구성
- 관리자에 대해 하나 이상의 사용자 역할 할당

Kaspersky Security Center 웹 콘솔에 로그인하려면, 가상 중앙 관리 서버의 관리자가 가상 중앙 관리 서버 이름, 사용자 이름, 암호를 지정합니다. Kaspersky Security Center 웹 콘솔은 관리자를 인증하고 관리자에게 액세스 권한이 있는 가상 중앙 관리 서버를 엽니다. 관리자는 중앙 관리 서버를 전환할 수 없습니다.

필수 구성 요소

시작하기 전에 다음 전제 조건을 충족하는지 확인하십시오:

- 가상 중앙 관리 서버가 생성됩니다.
- 기본 중앙 관리 서버에서 가상 중앙 관리 서버에 할당할 관리자 계정을 생성했습니다.
- **일반 기능 → 사용자 권한** 기능 영역에 **개체 ACL 수정** 권한이 있습니다.

수동으로 액세스 권한 구성

가상 중앙 관리 서버의 관리자를 지정하려면:

1. 기본 메뉴에서 필요한 가상 중앙 관리 서버로 전환합니다:

   a. 현재 중앙 관리 서버 이름 오른쪽의 펼침 단추 아이콘( )을 클릭합니다.

   b. 필요한 중앙 관리 서버를 선택합니다.

2. 메인 메뉴에서 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.

3. **접근 권한** 탭에서 **추가** 버튼을 클릭합니다.
   기본 중앙 관리 서버와 현재 가상 중앙 관리 서버의 사용자 통합 목록이 열립니다.

4. 사용자 목록에서 가상 중앙 관리 서버에 할당할 관리자 계정을 선택한 다음 **확인** 버튼을 클릭합니다.
   애플리케이션은 선택한 사용자를 **접근 권한** 탭의 사용자 목록에 추가합니다.

5. 추가된 계정 옆의 확인란을 선택한 다음 **접근 권한** 버튼을 클릭합니다.

6. 가상 중앙 관리 서버에서 관리자에게 부여할 권한을 구성합니다.
   인증에 성공하려면 최소한 관리자에게 다음 권한이 있어야 합니다:

   - **일반 기능** → **기본 기능** 기능 영역의 **읽기** 권한
   - **일반 기능** → **가상 중앙 관리 서버** 기능 영역의 **읽기** 권한

애플리케이션은 수정된 사용자 권한을 관리자 계정에 저장합니다.

사용자 역할을 할당하여 액세스 권한 구성

또는, 사용자 역할을 통해 가상 중앙 관리 서버 관리자에게 액세스 권한을 부여할 수 있습니다. 예를 들어 같은 가상 중앙 관리 서버에 여러 관리자를 할당할 때 유용할 수 있습니다. 이때, 여러 관리자에 대해 같은 사용자 권한을 구성하는 대신 관리자의 계정에 하나 이상의 같은 사용자 역할을 할당할 수 있습니다.

사용자 역할을 할당하여 가상 중앙 관리 서버의 관리자를 할당하려면:

1. 기본 중앙 관리 서버에서 새 사용자 역할을 만든 다음 가상 중앙 관리 서버에서 관리자에게 필요한 모든 필수 액세스 권한을 지정합니다. 예를 들어 여러 기능 영역에 대한 액세스를 분리하려면 여러 역할을 만들 수 있습니다.

2. 기본 메뉴에서 필요한 가상 중앙 관리 서버로 전환합니다:

   a. 현재 중앙 관리 서버 이름 오른쪽의 펼침 단추 아이콘(›)을 클릭합니다.

   b. 필요한 중앙 관리 서버를 선택합니다.

3. 새 역할 또는 여러 역할을 관리자 계정에 할당합니다.

애플리케이션은 관리자 계정에 역할을 할당합니다.

개체 수준에서 액세스 권한 구성

기능 영역 수준에서 액세스 권한을 할당하는 것 외에도 가상 중앙 관리 서버의 특정 개체에 대한 액세스를 구성할 수 있습니다(예: 특정 관리 그룹 또는 작업에 대한 액세스 구성). 이렇게 하려면 가상 중앙 관리 서버로 전환한 다음 개체 속성에서 액세스 권한을 구성합니다.

클라이언트 기기의 중앙 관리 서버 변경

중앙 관리 서버 변경 작업을 사용하여 클라이언트 기기를 관리하는 중앙 관리 서버를 다른 서버로 변경할 수 있습니다. 작업이 완료되면 선택한 클라이언트 기기가 지정한 중앙 관리 서버의 관리하에 놓이게 됩니다.

연결 게이트웨이를 통해 중앙 관리 서버에 연결된 클라이언트 기기에는 *중앙 관리 서버 변경* 작업을 사용할 수 없습니다. 이러한 기기는 네트워크 에이전트를 재구성하거나 네트워크 에이전트를 다시 설치하고 연결 게이트웨이를 지정해야 합니다.

클라이언트 기기를 관리하는 중앙 관리 서버를 다른 서버로 변경하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. 마법사의 **새 작업 설정** 단계에서 다음 설정을 지정합니다.
   a. **애플리케이션** 드롭다운 목록에서 **Kaspersky Security Center**를 선택합니다.
   b. **작업 유형** 필드에서 **중앙 관리 서버 변경**을 선택합니다.
   c. **작업 이름** 필드에서 만들고 있는 작업의 이름을 지정합니다.
   작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
   d. 이 작업이 할당되는 기기를 선택합니다.
   - **관리 그룹에 작업 할당**

     관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

     예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

     관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

     작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

     특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

   - **기기 선택 결과에 작업 할당**

     기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

4. 마법사의 **작업 범위** 단계에서 관리 그룹, 특정 주소가 있는 기기 또는 기기 선택을 지정합니다.

5. 마법사의 이 단계에서는 클라이언트 기기에 대한 중앙 관리 서버 변경 조건에 동의하는지 확인합니다.

6. 마법사의 이 단계에서는 선택한 기기의 관리에 사용할 중앙 관리 서버를 선택합니다.

- **다른 기본 중앙 관리 서버로 변경**

  클라이언트 기기를 다른 기본 중앙 관리 서버로 이동하려면 다음 중앙 관리 서버 연결 설정을 지정합니다.

  1. **중앙 관리 서버 주소** 필드에 새 기본 중앙 관리 서버의 주소를 지정합니다.
  2. **포트 번호** 필드에 중앙 관리 서버에 연결할 포트 번호를 지정합니다.
     기본 포트 번호는 14000입니다.
  3. **SSL 포트** 필드에 기본 중앙 관리 서버의 SSL 포트 번호를 지정합니다.
     기본 포트 번호는 13000입니다.
  4. 필요한 경우 **프록시 서버 사용** 옵션을 활성화합니다.
     이 옵션을 비활성화하면, 직접 연결을 통해 중앙 관리 서버에 기기를 연결합니다.
     이 옵션을 사용하면 프록시 서버 파라미터를 지정합니다:
     - **프록시 서버 주소**
     - **프록시 서버 포트**

     프록시 서버에 인증이 필요한 경우 **사용자 이름** 및 **암호** 필드에서 프록시 서버에 대한 연결이 설정된 계정의 자격 증명을 지정합니다. 프록시 서버 인증에만 필요한 최소 권한이 있는 계정의 자격 증명을 지정하는 것이 좋습니다.
  5. 필요한 경우 새로운 중앙 관리 서버 인증서를 업로드합니다.

- **이 기본 서버에서 다른 가상 서버로 변경**

  현재 기본 중앙 관리 서버의 가상 중앙 관리 서버로 클라이언트 기기를 이동하려면 이 옵션을 선택합니다. 이렇게 하려면 **가상 중앙 관리 서버 이름** 드롭다운 목록에서 필요한 가상 중앙 관리 서버를 선택합니다.

7. 마법사의 **작업을 실행할 계정 선택** 단계에서 계정 설정을 지정합니다.

- **기본 계정**

  해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.
  기본적으로 이 옵션은 선택되어 있습니다.

- **계정 지정**

  계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

  - **계정**

    작업 실행에 사용되는 계정입니다.

  - **암호**

    작업을 실행할 계정의 암호입니다.

8. 기본 작업 설정을 변경하려면 마법사의 **작업 생성 마침** 단계에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다.

   이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

9. **마침** 버튼을 누릅니다.

   그러면 작업이 생성되고 작업 목록에 표시됩니다.

10. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

11. 기본 작업 설정을 변경하려면 작업 속성 창에서 필요에 맞게 일반 작업 설정을 지정합니다.

12. **저장** 버튼을 누릅니다.

    작업이 생성 및 구성됩니다.

13. 만들어진 작업을 실행합니다.

작업이 완료되면 작업이 만들어진 클라이언트 기기가 작업 설정에 지정된 중앙 관리 서버의 관리를 받게 됩니다.

가상 중앙 관리 서버 삭제

가상 중앙 관리 서버를 삭제하면 정책 및 작업을 포함하여 중앙 관리 서버에서 생성된 모든 개체가 삭제됩니다. 가상 중앙 관리 서버가 관리하는 그룹의 관리 대상 기기가 관리 그룹에서 삭제됩니다. Kaspersky Security Center에서 관리 중인 기기를 반환하려면 네트워크 폴링을 실행한 다음 발견된 기기를 미할당 기기 그룹에서 관리 그룹으로 이동합니다.

가상 중앙 관리 서버를 삭제하려면 다음을 수행합니다.

1. 메인 메뉴에서 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.

2. 페이지가 열리면 **중앙 관리 서버** 탭으로 이동합니다.

3. 삭제할 가상 중앙 관리 서버를 선택합니다.

4. 메뉴 줄에서 **삭제** 버튼을 누릅니다.

가상 중앙 관리 서버가 삭제됩니다.

무단 수정으로부터 계정 보호 활성화

무단 수정으로부터 사용자 계정을 보호하는 추가 옵션을 활성화할 수 있습니다. 이 옵션이 활성화된 경우 사용자 계정 설정을 수정하려면 수정 권한이 있는 사용자의 인증이 필요합니다.

무단 수정으로부터 계정 보호를 활성화 또는 비활성화하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. 무단 수정으로부터 계정 보호를 지정할 내부 사용자 계정의 이름을 클릭합니다.
3. 사용자 설정 창이 열리면 **계정 보호** 탭을 선택합니다.
4. **계정 보호** 탭에서 계정 설정이 변경되거나 수정될 때마다 자격증명을 요청하고자 하는 경우 **사용자 계정 수정 권한을 확인하는 인증 요청** 옵션을 선택합니다. 다른 방법으로는 **사용자가 추가 인증 없이 이 계정을 수정할 수 있도록 허용** 옵션을 선택합니다.
5. **저장** 버튼을 누릅니다.

무단 수정으로부터 계정 보호가 사용자 계정에 대해 활성화됩니다.

중앙 관리 서버 데이터의 백업 복사 및 복원

데이터 백업을 사용하면 한 기기에서 다른 기기로 데이터 손실 없이 중앙 관리 서버를 이동할 수 있습니다. 백업을 통해, 중앙 관리 서버 데이터베이스를 다른 기기로 옮기거나 최신 버전의 Kaspersky Security Center로 업그레이드할 때 데이터를 복원할 수 있습니다. 또한 데이터 백업을 사용하여 Kaspersky Security Center Windows에서 Kaspersky Security Center Linux의 관리 하로 중앙 관리 서버 데이터를 옮길 수 있습니다(Kaspersky Security Center Linux에서 Kaspersky Security Center Windows로 데이터를 옮기는 것은 지원하지 않습니다).

설치된 관리 플러그인은 백업되지 않습니다. 백업 복사본에서 중앙 관리 서버 데이터를 복원한 후, 관리 중인 애플리케이션용 플러그인을 다운로드하여 다시 설치해야 합니다.

중앙 관리 서버 데이터를 백업하기 전에 가상 중앙 관리 서버가 관리 그룹에 추가되어 있는지 확인합니다. 가상 중앙 관리 서버가 추가되었다면 백업 전에 이 가상 중앙 관리 서버에 관리자가 할당되어 있는지 확인합니다. 백업 후에는 가상 중앙 관리 서버에 관리자 액세스 권한을 부여할 수 없습니다. 관리자 계정 자격 증명을 상실하면 가상 관리자 서버에 새 관리자를 할당할 수 없습니다.

Kaspersky Security Center 장애 조치 클러스터를 백업하거나 복원하려면 유지 관리 작업을 위해 전체 클러스터를 중지한 다음, 백업 또는 복원이 완료되면 다시 시작해야 합니다.

다음 방법 중 하나를 사용하여 중앙 관리 서버 데이터의 백업 복사본을 만들 수 있습니다:

- 관리 콘솔을 사용하여 데이터 백업 작업을 만들고 실행합니다.
- 중앙 관리 서버가 설치된 기기에서 klbackup 유틸리티를 실행합니다. 이 유틸리티는 Kaspersky Security Center 배포 키트에 포함되어 있습니다. 중앙 관리 서버를 설치하면 이 유틸리티가 애플리케이션 설치 시 지정한 대상 폴더의 루트에 저장됩니다.

다음 데이터가 중앙 관리 서버의 백업 복사본에 저장됩니다.

- 중앙 관리 서버의 데이터베이스(중앙 관리 서버에 저장된 정책, 작업, 애플리케이션 설정, 이벤트).
- 관리 그룹 및 클라이언트 기기 구조에 관한 구성 세부사항.
- 원격 설치를 위한 애플리케이션의 배포 패키지 저장소.
- 중앙 관리 서버 인증서.
- *업데이트* 폴더의 내용.

  기본 폴더 경로는 C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\입니다

klbackup 유틸리티를 사용해야만 중앙 관리 서버 데이터를 복원할 수 있습니다. 가장 최근에 설치되었으며 버전이 백업 복사본을 만든 인스턴스 이상인 작동 가능한 중앙 관리 서버 인스턴스에서 복원을 수행해야 합니다.

데이터 백업 작업 만들기

백업 작업은 중앙 관리 서버 작업이며 빠른 시작 마법사에 의해 만들어집니다. 빠른 시작 마법사에서 만든 백업 작업이 삭제되었다면 수동으로 만들 수 있습니다.

중앙 관리 서버 데이터 백업 작업을 만들려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가** 버튼을 클릭합니다.

   새 작업 마법사가 시작됩니다.
3. 마법사의 **새 작업 설정** 창에서 **중앙 관리 서버 데이터 백업**이라는 작업 유형을 선택합니다.
4. 마법사의 나머지 지침을 따릅니다.

중앙 관리 서버 데이터 백업 작업은 하나의 복사본으로만 만들 수 있습니다. 중앙 관리 서버에 대한 중앙 관리 서버 데이터 백업 작업이 이미 만들어졌다면 중앙 관리 서버 백업 작업 생성 마법사의 작업 유형 선택 창에 이 작업이 표시되지 않습니다.

중앙 관리 서버 데이터 백업 작업을 구성하려면:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동한 다음 **중앙 관리 서버 데이터 백업** 작업을 선택합니다.
2. **중앙 관리 서버 데이터 백업** 작업을 클릭합니다.

   작업 속성 창이 열립니다.

3. 필요하다면 원하는 일반 작업 설정을 지정합니다.

4. **애플리케이션 설정** 섹션에서 중앙 관리 서버 데이터의 백업 복사본 저장을 위한 폴더 경로를 지정하고 백업 보호 암호를 설정하며, 백업 복사본 수를 설정합니다.

5. 변경 사항을 적용하려면 **저장**을 클릭합니다.

중앙 관리 서버 데이터 백업 작업이 구성됩니다.

다른 기기로 중앙 관리 서버 이동

새 기기에서 중앙 관리 서버 사용 시, 다음 방법 중 하나로 이동할 수 있습니다.

- 중앙 관리 서버와 데이터베이스 서버를 새 기기로 이동합니다(데이터베이스 서버는 새 기기에 중앙 관리 서버와 함께 설치하거나 다른 기기에 설치할 수 있습니다).
- 데이터베이스 서버를 이전 기기에 유지하고 중앙 관리 서버만 새 기기로 이동합니다.

중앙 관리 서버와 데이터베이스 서버를 새 기기로 이동하려면:

1. 이전 기기에서 중앙 관리 서버 데이터의 백업을 만듭니다.

   이렇게 하려면 Kaspersky Security Center 웹 콘솔을 통해 데이터 백업 작업을 실행하거나 klbackup 유틸리티를 실행합니다.

   > SQL Server를 중앙 관리 서버용 DBMS로 사용한다면 SQL Server에서 MySQL 또는 MariaDB DBMS로 데이터를 마이그레이션할 수 있습니다. 이렇게 하려면 대화형 모드에서 klbackup 유틸리티를 실행하여 데이터 백업을 만듭니다. 백업 및 복원 마법사의 **백업 설정** 창에서 **MySQL/MariaDB 형식으로 마이그레이션** 옵션을 활성화합니다. Kaspersky Security Center는 MySQL 및 MariaDB와 호환되는 백업을 생성합니다. 그런 다음 백업에서 MySQL 또는 MariaDB로 데이터를 복원할 수 있습니다.

   > SQL Server에서 Azure SQL DBMS로 데이터를 마이그레이션하려면 **Azure 형식으로 마이그레이션** 옵션을 활성화할 수도 있습니다.

2. 이전 기기에서 중앙 관리 서버의 네트워크 연결을 해제합니다.

3. 중앙 관리 서버를 설치할 새 기기를 선택하십시오. 선택한 기기의 하드웨어 및 소프트웨어가 중앙 관리 서버, Kaspersky Security Center 웹 콘솔, 네트워크 에이전트의 요구 사항을 충족하는지 확인합니다. 또한 중앙 관리 서버에서 사용되는 포트를 사용할 수 있는지 확인하십시오.

4. 새 기기에 같은 주소를 할당합니다.

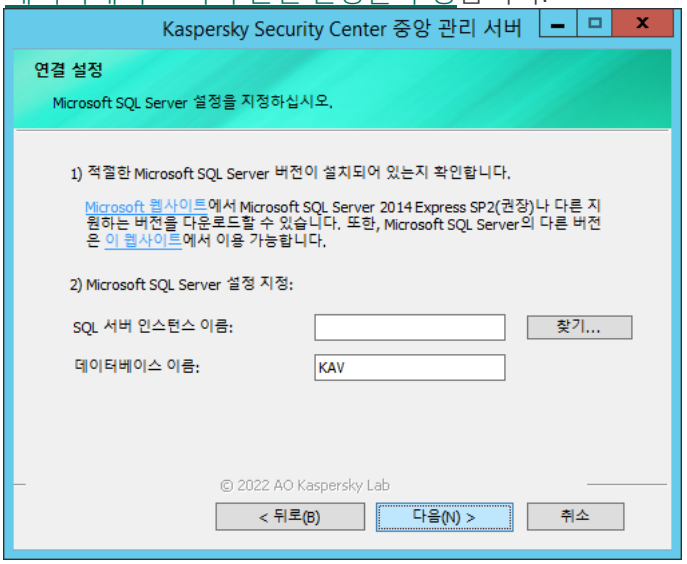
   새 중앙 관리 서버에 NetBIOS 이름, FQDN, 고정 IP 주소를 할당할 수 있습니다. 네트워크 에이전트 배포 시 네트워크 에이전트 설치 패키지에 설정된 중앙 관리 서버 주소에 따라 다릅니다. 또는 네트워크 에이전트가 연결할 중앙 관리 서버를 결정하는 연결 주소를 사용할 수 있습니다(이 주소는 관리 중인 기기에서 klnagchk 유틸리티를 사용하여 얻을 수 있습니다).

5. 필요하다면 다른 기기에 중앙 관리 서버가 사용할 데이터베이스 관리 시스템(DBMS)을 설치합니다.

   데이터베이스는 중앙 관리 서버가 설치된 새 기기에 설치하거나 다른 기기에 설치할 수 있습니다. 이 기기가 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인합니다. DBMS 선택 시, 중앙 관리 서버에서 다루는 기기의 수를 고려하십시오.

6. 새 기기에서 중앙 관리 서버 설치를 실행합니다.

7. 중앙 관리 서버를 설치할 때 데이터베이스 서버 연결 설정을 구성합니다.



Microsoft SQL Server용 연결 설정 창의 예

데이터베이스 서버를 찾아야 하는 위치에 따라 다음 중 하나를 수행합니다:

- **이전 기기에 데이터베이스 서버 유지**

  1. **SQL 서버 인스턴스 이름** 필드 옆에 있는 **찾기** 버튼을 클릭한 다음 표시되는 목록에서 이전 기기 이름을 선택합니다.

     새 중앙 관리 서버와 연결하려면 이전 기기를 사용할 수 있어야 합니다.

  2. **데이터베이스 이름** 필드에 이전 데이터베이스 이름을 입력합니다.

- **데이터베이스 서버를 새 기기로 이동**

  1. **SQL 서버 인스턴스 이름** 필드 옆에 있는 **찾기** 버튼을 클릭한 다음 표시되는 목록에서 기기 이름을 선택합니다.

  2. **데이터베이스 이름** 필드에 새 데이터베이스 이름을 입력합니다.

     새 데이터베이스 이름은 이전 기기의 데이터베이스 이름과 일치해야 합니다. 중앙 관리 서버 백업을 사용할 수 있도록 데이터베이스 이름이 같아야 합니다. 기본 데이터베이스 이름은 *KAV*입니다.

8. 설치가 완료되면 klbackup 유틸리티를 사용하여 새 기기에서 중앙 관리 서버 데이터를 복구합니다.

이전 기기와 새 기기에서 SQL Server를 DBMS로 사용 시, 새 기기에 설치된 SQL Server 버전이 이전 기기에 설치된 SQL Server 버전과 같거나 더 최신 버전이어야 합니다. 그렇지 않으면 새 기기에서 중앙 관리 서버 데이터를 복구할 수 없습니다.

9. Kaspersky Security Center 웹 콘솔을 열고 중앙 관리 서버에 연결합니다.

10. 모든 관리 중인 기기가 중앙 관리 서버에 연결되어 있는지 확인합니다.

11. 이전 기기에서 중앙 관리 서버와 데이터베이스 서버를 제거합니다.

관리 콘솔을 사용하여 중앙 관리 서버와 데이터베이스 서버를 다른 기기로 이동할 수도 있습니다.

klscmodchk 및 integrity_checker 유틸리티를 사용하여 모듈 무결성 확인

Kaspersky Security Center는 동적 링크 라이브러리, 실행 파일, 구성 파일, 인터페이스 파일 형태의 여러 바이너리 모듈을 포함합니다. 침입자는 하나 이상의 실행 모듈 또는 애플리케이션 파일을 악성 코드가 포함된 다른 파일로 교체할 수 있습니다. 모듈 및 파일 대체를 방지하기 위해 Kaspersky Security Center는 klscmodchk 및 integrity_checker 유틸리티를 사용하여 구성 요소 무결성 검사를 지원합니다. 이러한 유틸리티는 모듈과 파일의 무단 변경이나 손상을 검사합니다. 모듈 또는 애플리케이션 파일에 잘못된 체크섬이 포함되어 있으면 손상된 것으로 간주합니다.

klscmodchk 유틸리티는 다음 Kaspersky Security Center 구성 요소에 대한 무결성 검사를 수행합니다.

- 중앙 관리 서버
- 네트워크 에이전트
- 매니페스트 파일이 포함된 관리 콘솔용 관리 플러그인

integrity_checker 유틸리티는 다음 Kaspersky Security Center 구성 요소에 대한 무결성 검사를 수행합니다.

- 중앙 관리 서버
- 네트워크 에이전트
- Kaspersky Security Center 웹 콘솔

두 유틸리티 모두 Kaspersky Security Center 빌드의 일부이자 설치 폴더에 있는 kl_file_integrity_manifest.xml 매니페스트 파일을 기반으로 모듈 무결성을 검사합니다. 구성 요소 매니페스트 파일은 Kaspersky Security Center 구성 요소의 올바른 작동을 위해 무결성이 보장되어야 하는 파일을 포함하고 있습니다. 매니페스트 파일 자체의 무결성도 검사합니다.

kl_file_integrity_manifest.xml 매니페스트 파일은 가급적 수정하지 마십시오. 수정 시 디지털 서명이 무효화되어 무결성 검사에 실패할 수 있기 때문입니다.

Kaspersky Security Center 구성 요소의 무결성을 검사하려면 다음 명령 중 하나를 실행합니다.

- `$ klscmodchk [ 파라미터 ]`

  klscmodchk 유틸리티는 `--verbose` 매개변수를 사용하여 integrity_checker 유틸리티를 실행하고 모듈의 무결성을 검사합니다.

klscmodchk 유틸리티 매개변수

- `-logfile <log_file_path>` - 로그를 기록할 디스크상의 파일 경로를 지정합니다. 기본적으로 정보는 콘솔에 출력됩니다.
- `-chkplugins` - 매니페스트 파일을 포함하는 설치된 관리 콘솔용 관리 플러그인 모듈의 무결성을 확인합니다. 기본적으로 관리 플러그인은 선택되어 있지 않습니다.
- `-verbose` - 무결성 검사 중에 확장된 정보를 출력합니다.

- `$ integrity_checker [` 파라미터 `] <manifest_file_path>`

  integrity_checker 유틸리티 매개변수

  - `--help` - integrity_checker 유틸리티 도움말을 표시합니다.
  - `--version` - integrity_checker 유틸리티 버전을 표시합니다.
  - `--verbose` - 유틸리티 작업 정보를 표시합니다. 무결성 검사를 수행할 때는 명령에서 이 매개변수를 사용하면 됩니다.

각 매니페스트의 파일 검사 결과는 다음 형식으로 매니페스트 파일 이름 옆에 표시됩니다.

- SUCCEEDED - 파일 무결성이 확인되었습니다(반환 코드 0).
- FAILED - 파일 무결성이 확인되지 않았습니다(0이 아닌 반환 코드).

애플리케이션 시작 시 무결성 검사를 자동으로 시작하도록 구성할 수도 있습니다. 자동 무결성 검사는 기본적으로 비활성화되어 있습니다.

자동 무결성 검사를 활성화하려면:

1. 중앙 관리 서버가 설치된 기기의 Windows 명령 프롬프트에 다음 명령을 입력합니다.

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. 기기를 다시 시작합니다.

   자동 무결성 검사가 활성화됩니다.

다음번에 Kaspersky Security Center를 실행하면 klscmodchk 유틸리티가 중앙 관리 서버와 함께 실행되고, 모듈 무결성 검사가 시작됩니다. 무결성 검사 결과는 Kaspersky 이벤트 로그에 작성됩니다.

Kaspersky Security Center 웹 콘솔 초기 설정

이 섹션에서는 Kaspersky Security Center 웹 콘솔 설치 후에 초기 설정을 위해 수행해야 하는 단계를 설명합니다.

빠른 시작 마법사(Kaspersky Security Center 웹 콘솔)

이 섹션은 중앙 관리 서버 빠른 시작 마법사에 대한 정보를 제공합니다.

마법사에는 인터넷 액세스가 필요합니다. 중앙 관리 서버에 인터넷 액세스가 없다면, Kaspersky Security Center 웹 콘솔 인터페이스를 통해 마법사의 모든 단계를 수동으로 수행하는 것을 권장합니다.

Kaspersky Security Center를 사용하면 보안 위협으로부터 네트워크를 보호를 위해 중앙 집중화된 관리 시스템을 구축하는 데 필요한 최소 설정을 조정할 수 있습니다. 이 구성은 빠른 시작 마법사를 사용하여 수행합니다. 마법사가 실행 중일 때 애플리케이션을 다음과 같이 변경할 수 있습니다:

- 관리 그룹 내의 기기에 자동으로 배포될 수 있는 키 파일을 추가하거나 활성화코드를 입력합니다.
- Kaspersky Security Network(KSN)와의 연동을 구성합니다. KSN의 사용을 허용했다면, 마법사에서 KSN과 기기 사이의 연결을 보장하는 KSN 프록시 서버 서비스를 사용합니다.
- 중앙 관리 서버 및 관리되는 애플리케이션의 운영 중에 일어나는 이벤트를 알려주는 이메일 전달 기능을 설정합니다(성공적인 알림 전달을 위해서는 중앙 관리 서버 및 모든 수신 기기에 메신저 서비스가 실행되고 있어야 합니다).
- 워크스테이션 및 서버용 보호 정책을 만들고 관리 중인 기기의 계층 구조 최상위 레벨에 대한 악성 코드 검사 작업, 업데이트 다운로드 작업 및 데이터 백업 작업을 만듭니다.

  빠른 시작 마법사는 **관리 중인 기기** 폴더에 정책이 없는 애플리케이션에 대해서만 정책을 만듭니다. 관리 중인 기기 계층 구조의 가장 높은 레벨에 같은 이름의 작업이 이미 생성되어 있다면, 빠른 시작 마법사가 작업을 생성하지 않습니다.

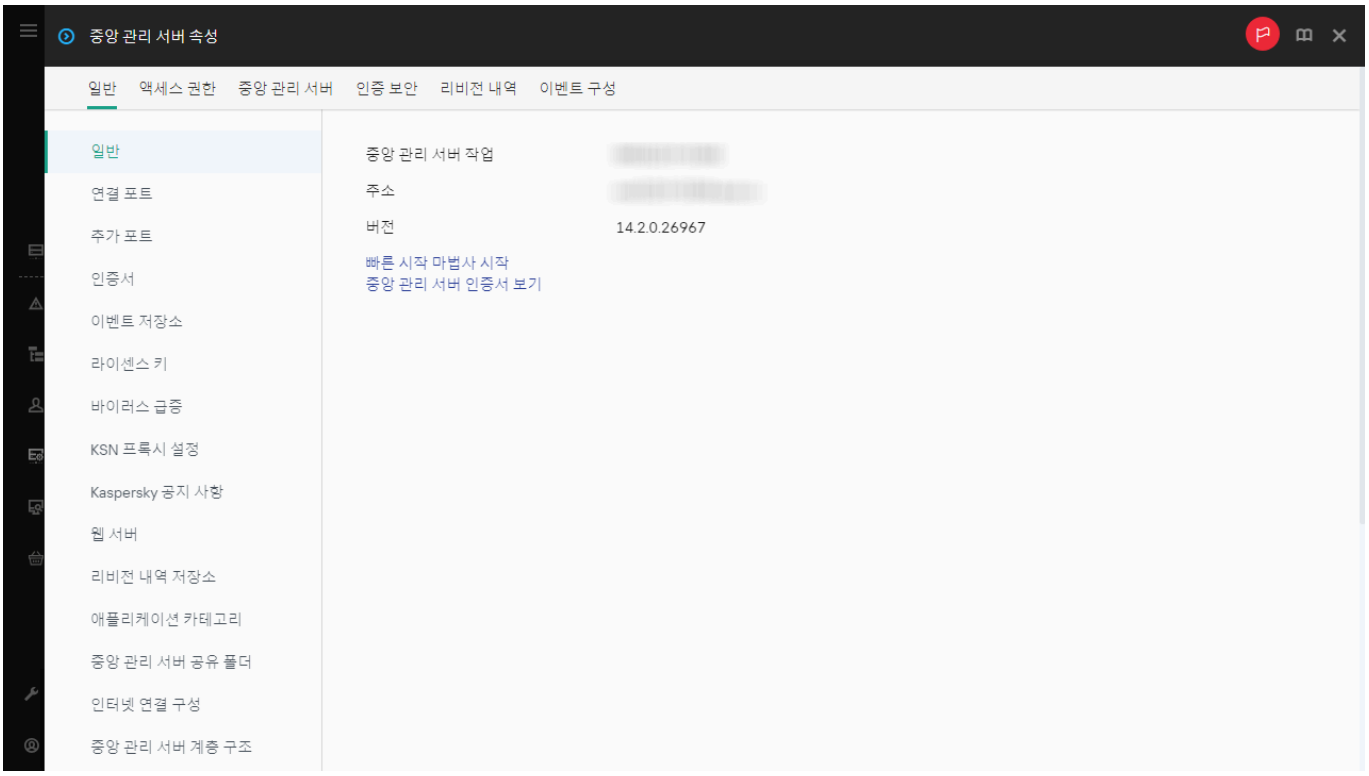
애플리케이션은 중앙 관리 서버 설치 후 첫 연결 시 빠른 시작 마법사의 실행 여부를 자동으로 물어봅니다. 언제든지 수동으로 빠른 시작 마법사를 시작할 수도 있습니다.

빠른 시작 마법사를 수동으로 시작하려면:

1. 메인 메뉴에서 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.

   중앙 관리 서버 속성 창이 열립니다.

2. **일반** 탭에서 **일반** 섹션을 선택합니다.



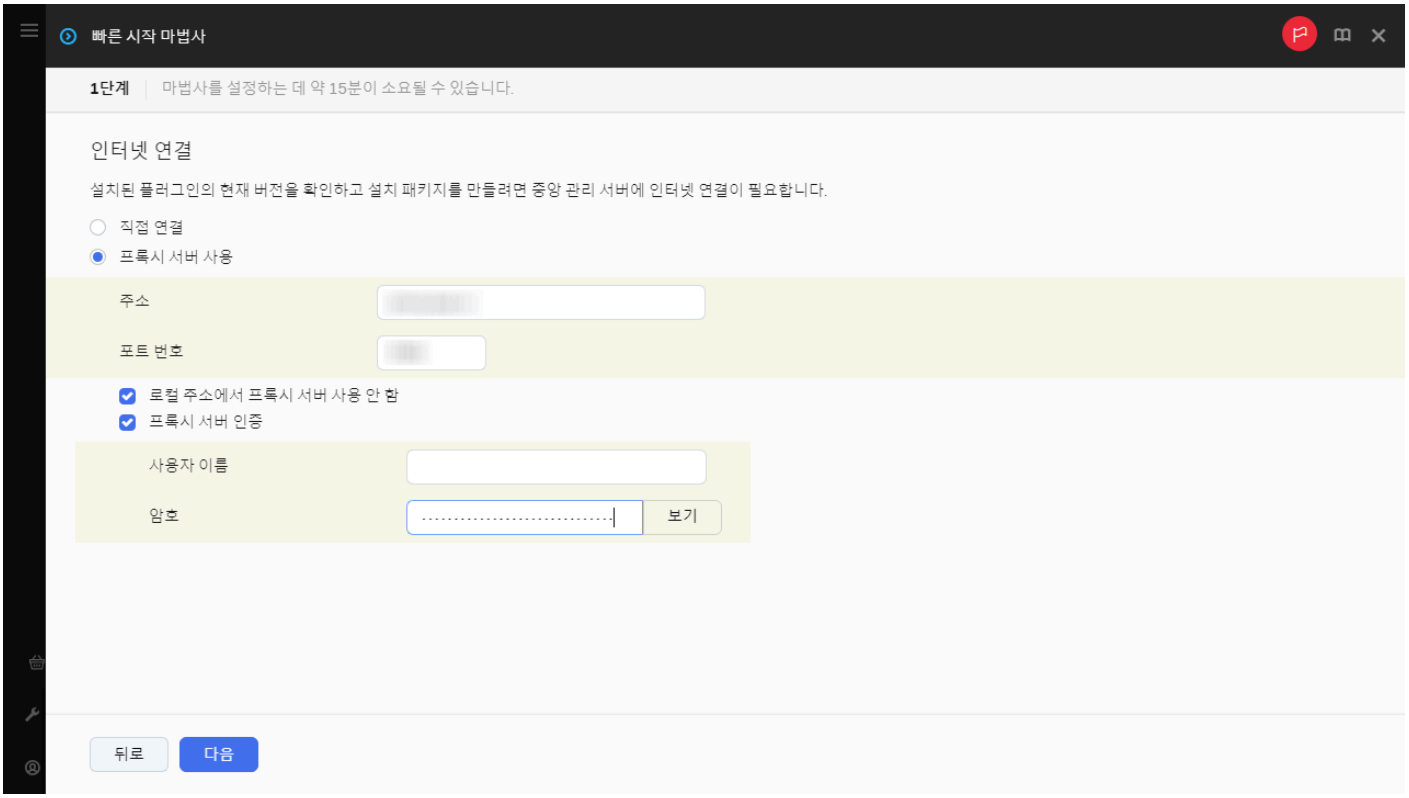
중앙 관리 서버 속성 창

3. **빠른 시작 마법사 시작**을 누릅니다.

마법사가 중앙 관리 서버의 초기 구성을 수행하라는 메시지를 표시합니다. 마법사의 지침을 따릅니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

1단계. 인터넷 연결 설정 지정

중앙 관리 서버의 인터넷 접속 설정을 지정합니다. Kaspersky Security Network를 사용하고, Kaspersky Security Center 및 관리 중인 Kaspersky 애플리케이션용 안티 바이러스 데이터베이스의 업데이트를 다운로드하려면 인터넷 접속을 구성해야 합니다.



인터넷 연결 설정

인터넷에 연결할 때 프록시 서버를 사용하려면 **프록시 서버 사용** 옵션을 활성화합니다. 이 옵션을 활성화하면 설정을 입력하는 필드를 사용할 수 있습니다. 프록시 서버 연결에 대해 다음 설정을 지정합니다.

- **주소**

  Kaspersky Security Center에서 인터넷 연결에 사용한 프록시 서버의 주소입니다.

- **포트 번호**

  Kaspersky Security Center 프록시 연결을 설정하는 데 사용되는 포트 번호입니다.

- **로컬 주소에서 프록시 서버 사용 안 함**

  로컬 네트워크에서 기기로 연결하는 데 프록시 서버가 사용되지 않습니다.

- **프록시 서버 인증**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.
  프록시 서버 사용 확인란을 선택하면 이 입력 필드를 사용할 수 있습니다.

- **사용자 이름**

  프록시 서버에 대한 연결을 구성할 사용자 계정입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

- **암호**

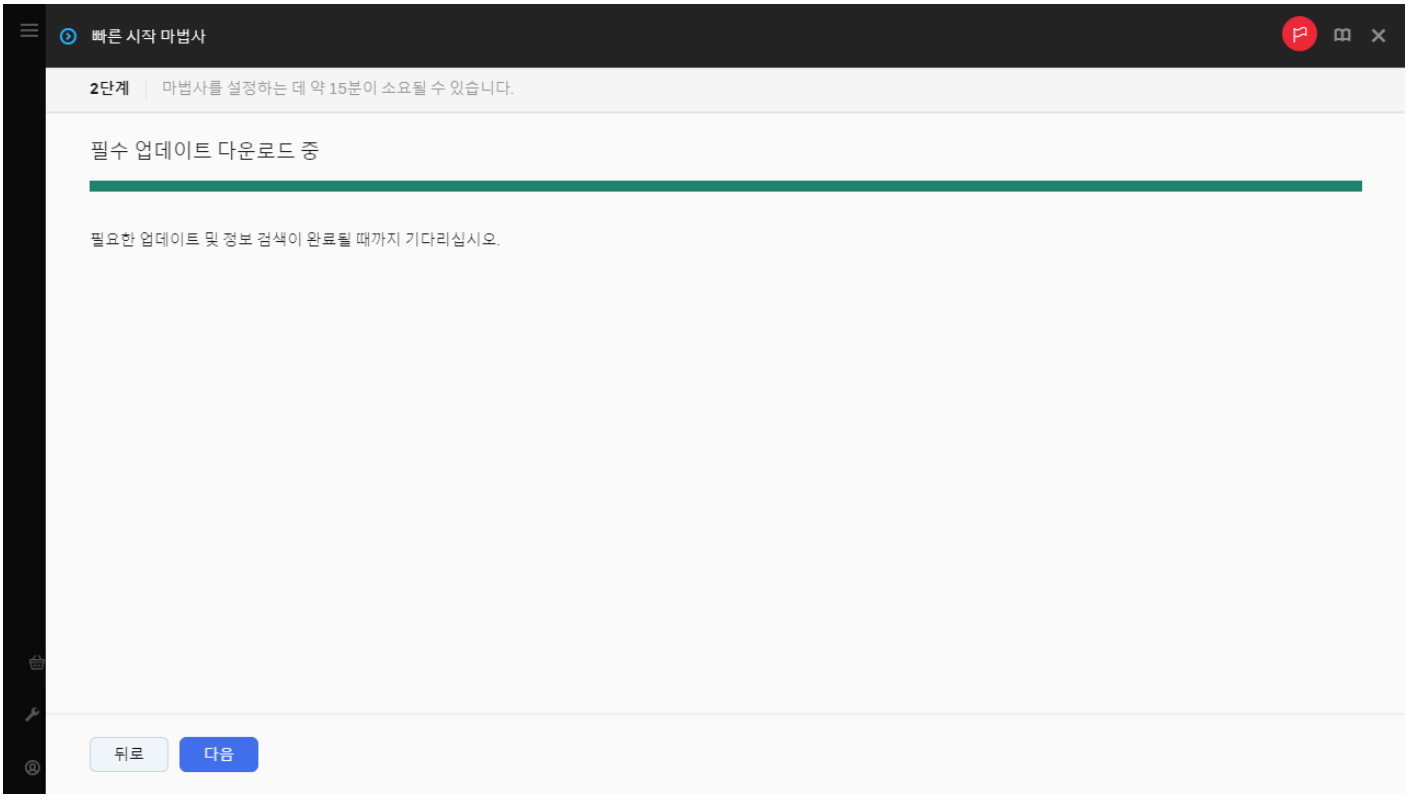
  프록시 서버 연결을 구성한 계정의 사용자가 설정한 암호입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

  입력한 암호를 보려면 **보기** 버튼을 필요한 시간 동안 누르고 있어야 합니다.

빠른 시작 마법사와는 별도로 나중에 인터넷 액세스를 구성할 수도 있습니다.

2단계. 필수 업데이트 다운로드 중

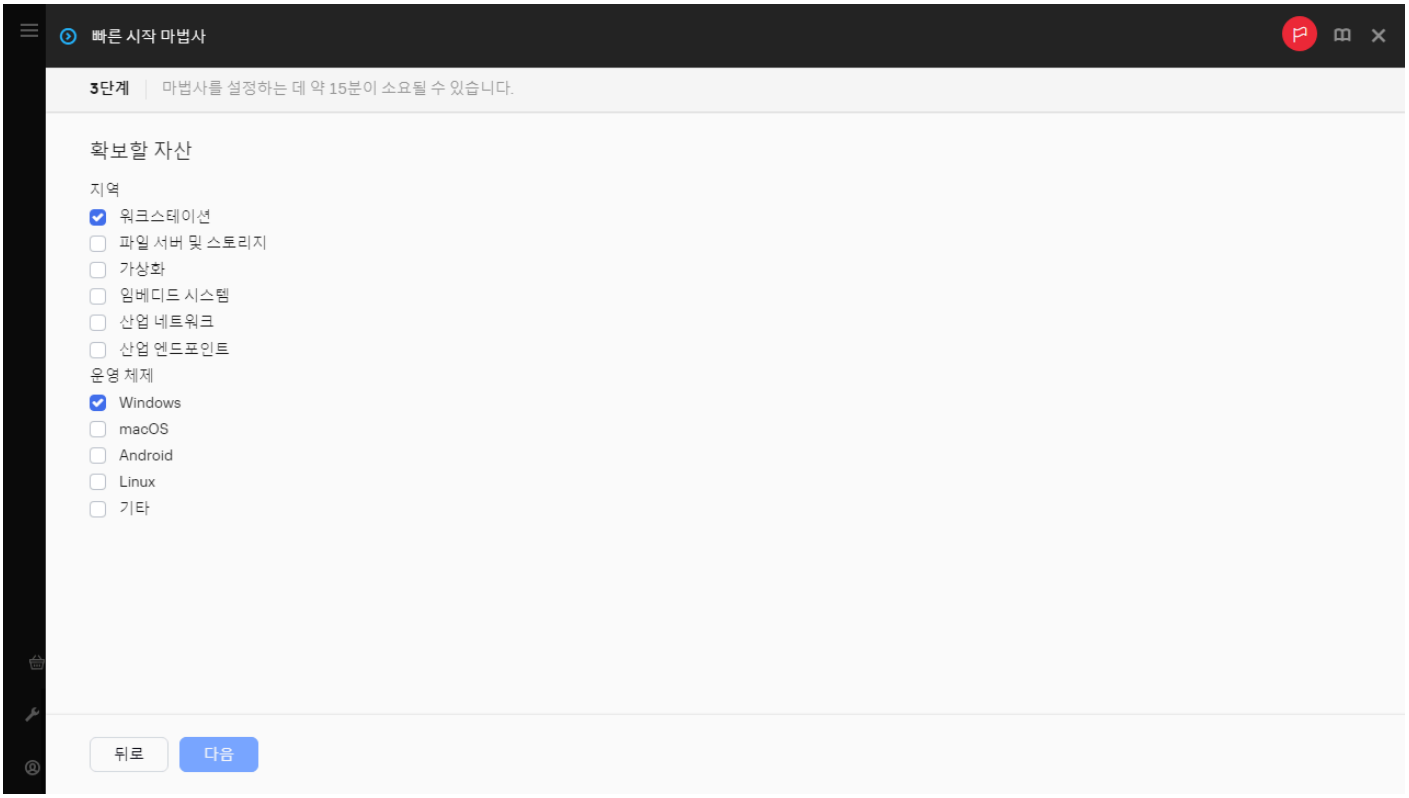
필수 업데이트 Kaspersky 서버에서 자동으로 다운로드됩니다.



필수 업데이트 다운로드 중

3단계. 확보할 자산 선택

네트워크에서 사용 중인 보호 범위와 운영 체제를 선택합니다. 이러한 옵션을 선택할 때 네트워크 내 클라이언트 기기에 설치하기 위해 다운로드할 수 있는 Kaspersky 서버의 애플리케이션 관리 플러그인 및 배포 패키지에 대한 필터를 지정합니다.



확보할 자산 선택

옵션을 선택합니다.

- **영역**

  다음 보호 영역을 선택할 수 있습니다:

  - **워크스테이션**. 네트워크의 워크스테이션을 보호하려면 이 옵션을 선택합니다. 워크스테이션 옵션은 기본으로 선택되어 있습니다.
  - **파일 서버 및 스토리지**. 네트워크의 파일 서버를 보호하려면 이 옵션을 선택합니다.
  - **모바일 기기**. 회사 또는 회사 직원이 소유한 모바일 기기를 보호하려면 이 옵션을 선택합니다. 이 옵션을 선택하지만 모바일 기기 관리 기능이 있는 라이센스를 제공하지 않으면 모바일 기기 관리 기능이 있는 라이센스를 제공해야 한다는 내용의 메시지가 표시됩니다. 라이센스를 제공하지 않으면 모바일 기기 기능을 이용할 수 없습니다.
  - **가상화** 네트워크에서 가상 컴퓨터를 보호하려면 이 옵션을 선택합니다.
  - **Kaspersky 안티 스팸**. 조직에 있는 메일 서버를 스팸, 사기 및 악성 코드 전달로부터 보호하려면 이 옵션을 선택합니다.
  - **임베디드 시스템** ATM(Automated Teller Machine)과 같은 Windows 기반 임베디드 시스템을 보호하려면 이 옵션을 선택합니다.

- **산업 네트워크** 산업용 네트워크 전체와 Kaspersky 애플리케이션으로 보호되는 네트워크 엔드포인트에서 보안 데이터를 모니터링하려면 이 옵션을 선택합니다.
- **산업 엔드포인트** 산업 네트워크 내의 개별 노드를 보호하려면 이 옵션을 선택합니다.

- **운영 체제**

  다음 플랫폼을 선택할 수 있습니다:
  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - 기타

  지원되는 운영 체제에 대한 정보는 Kaspersky Security Center 웹 콘솔의 하드웨어 및 소프트웨어 요구 사항을 참조하십시오.

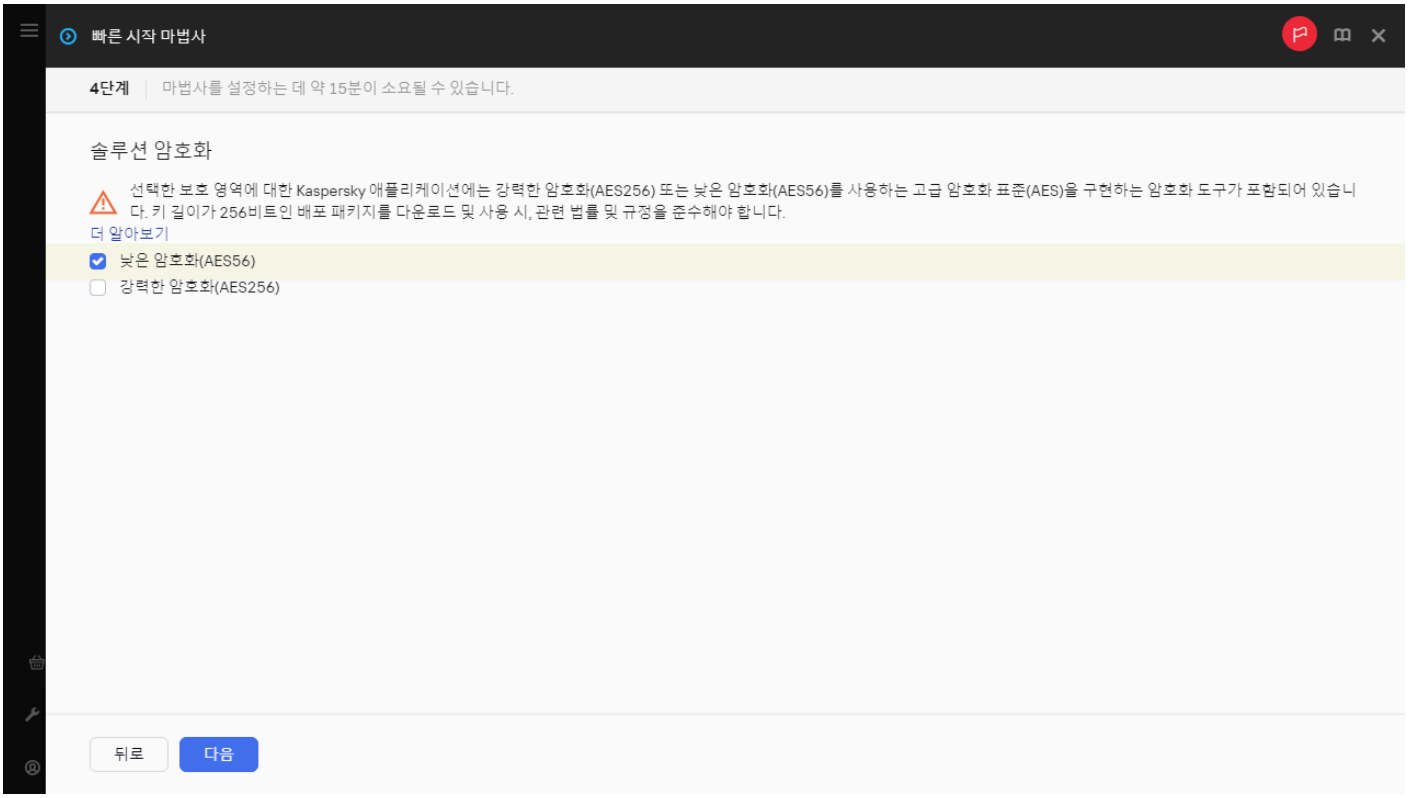
빠른 시작 마법사와는 별도로 나중에 사용 가능한 패키지 목록에서 Kaspersky 애플리케이션 패키지를 선택할 수 있습니다. 필수 패키지 검색을 단순화하기 위해 다양한 기준으로 사용 가능한 패키지 목록을 필터링할 수 있습니다.

4단계. 솔루션 암호화 선택

솔루션 암호화 창은 **워크스테이션**을 보호 범위로 선택했을 때만 표시됩니다.

Kaspersky Endpoint Security for Windows에는 Windows 기반의 클라이언트 기기에 저장된 정보를 위한 암호화 도구가 포함되어 있습니다. 이 암호화 도구에는 256비트 또는 56비트 키 길이로 구현된 AES(Advanced Encryption Standard)가 있습니다.

키 길이가 256비트인 배포 패키지를 다운로드해서 사용할 때는 해당하는 법률 및 규정을 준수해야 합니다. 조직의 요구에 적합한 Kaspersky Endpoint Security for Windows의 배포 패키지를 다운로드하려면, 조직의 클라이언트 기기가 있는 국가의 법률을 참조하십시오.



솔루션 암호화 선택

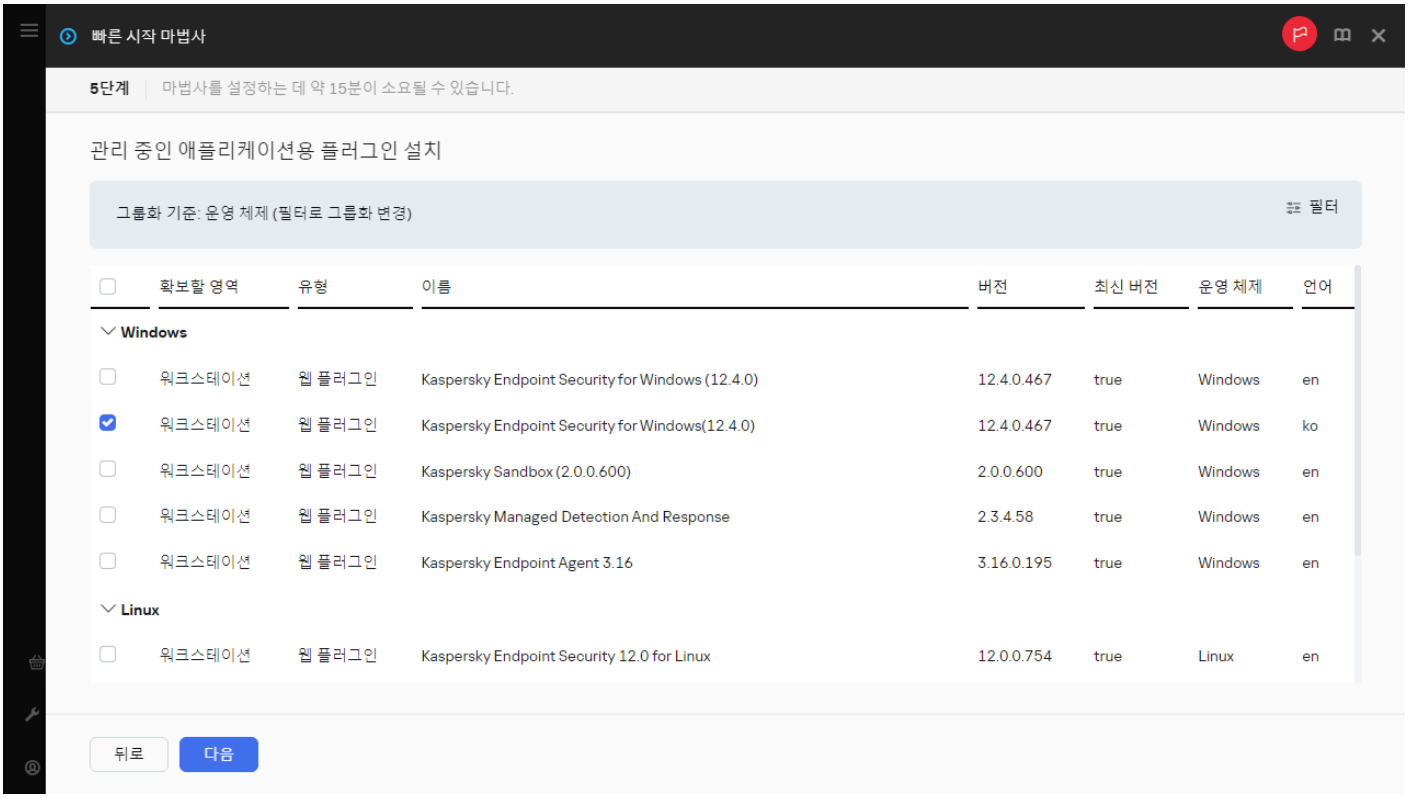
솔루션 암호화 창에서 다음 암호화 유형 중 하나를 선택합니다:

- 가벼운 암호화. 이 암호화 유형은 56비트 키 길이를 사용합니다.
- 강한 암호화. 이 암호화 유형은 256비트 키 길이를 사용합니다.

나중에 빠른 시작 마법사와 별도로, 필요한 암호화 유형이 포함된 Kaspersky Endpoint Security for Windows 배포 패키지를 선택할 수 있습니다.

5단계. 관리 중인 애플리케이션용 플러그인 설치 구성

설치할 관리 중인 애플리케이션에 대한 플러그인을 선택합니다. Kaspersky 서버에 있는 플러그인 목록이 표시됩니다. 마법사의 이전 단계에서 선택한 옵션에 따라 목록이 필터링됩니다. 전체 목록에는 기본적으로 모든 언어의 플러그인이 포함됩니다. 특정 언어의 플러그인만 표시하려면 필터를 사용합니다.



관리 중인 애플리케이션용 플러그인 설치

플러그인 목록에는 다음 열이 포함됩니다:

- **확보할 영역**

  보안을 위해 선택한 영역이 이 열에 표시됩니다.

- **유형**

  플러그인 유형이 이 열에 표시됩니다.

- **이름**

  이전 단계에서 선택한 보호 영역 및 플랫폼에 따라 플러그인이 선택됩니다.

- **버전**

  이 목록에는 Kaspersky 서버에 있는 모든 버전의 플러그인이 포함됩니다. 최신 버전의 플러그인이 기본으로 선택되어 있습니다.

- **최신 버전**

  이 열은 플러그인 버전이 최신인지 나타냅니다. **true** 값이 표시되면 해당 플러그인이 최신 버전입니다. **false** 값이 표시되면 해당 플러그인에 최신 버전이 있는 것입니다.

- **운영 체제**

  이 열에는 플러그인 운영 체제가 표시됩니다.

- **언어**

  기본적으로 플러그인의 현지화 언어는 설치 시 선택한 Kaspersky Security Center 언어에 따라 정의됩니다. **표시: 관리 콘솔 현지화 언어 또는** 드롭다운 목록에서 다른 언어를 지정할 수 있습니다.

플러그인을 선택한 다음 **다음**을(를) 눌러 설치를 시작합니다.

빠른 시작 마법사와 별도로 Kaspersky 애플리케이션용 관리 플러그인을 수동으로 설치할 수 있습니다.

빠른 시작 마법사는 선택한 플러그인을 자동 설치합니다. 일부 플러그인은 설치 과정에서 EULA의 조항에 동의해야 합니다. 표시된 EULA의 본문을 읽고 **Kaspersky Security Network 사용에 동의합니다** 확인란을 선택하고 **설치** 버튼을 누릅니다. EULA의 조항에 동의하지 않으면 플러그인이 설치되지 않습니다.

선택한 플러그인을 모두 설치하면, 빠른 시작 마법사가 다음 단계로 자동 이동합니다.

6단계. 선택한 플러그인 설치

빠른 시작 마법사가 이전 단계에서 사용자가 선택한 플러그인을 자동 설치합니다. 일부 플러그인은 설치 과정에서 EULA의 조항에 동의해야 합니다. 표시된 EULA의 본문을 읽고 **Kaspersky Security Network 사용에 동의합니다** 확인란을 선택하고 **설치** 버튼을 누릅니다. EULA의 조항에 동의하지 않으면 플러그인이 설치되지 않습니다.

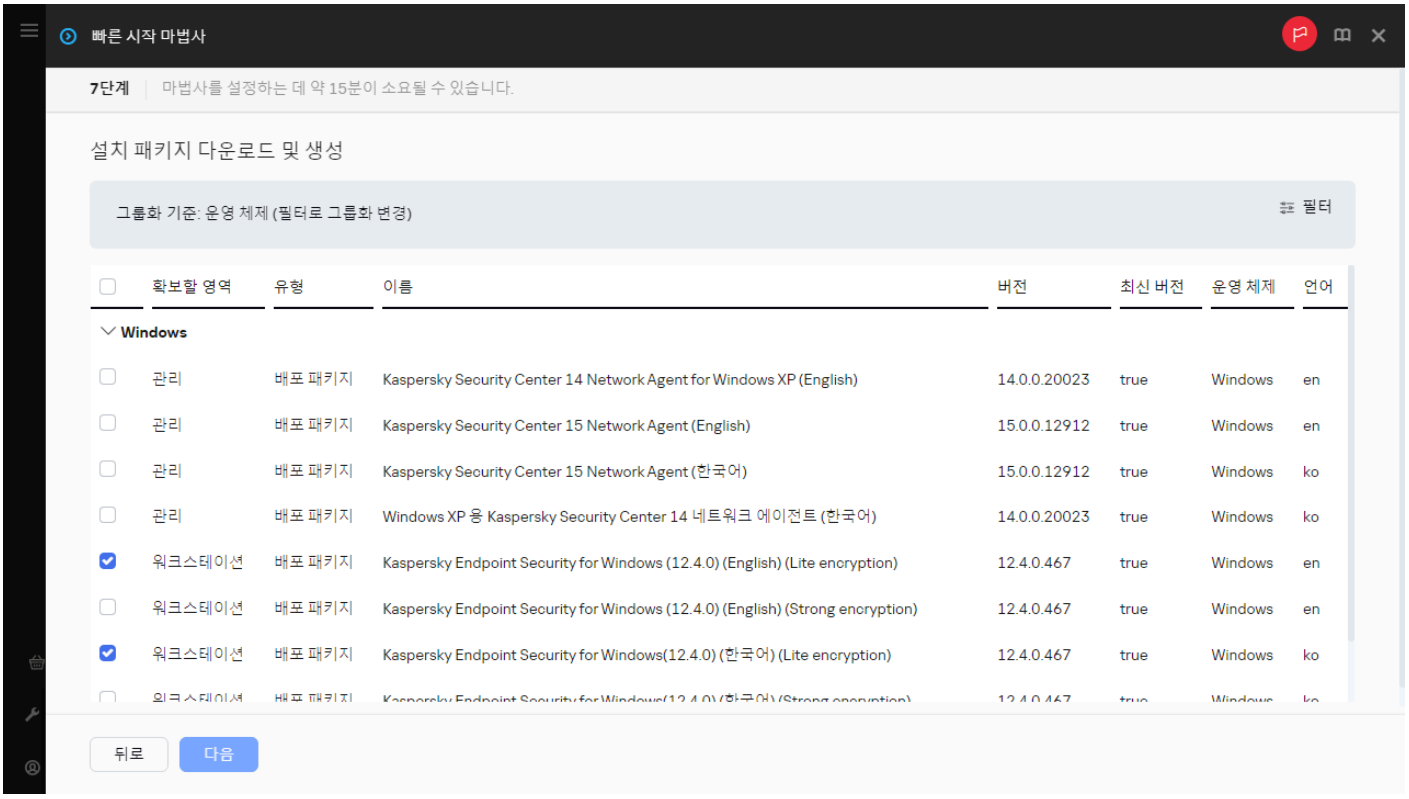
선택한 플러그인을 모두 설치하면, 빠른 시작 마법사가 다음 단계로 자동 이동합니다.

7단계. 배포 패키지 다운로드 및 설치 패키지 생성

다운로드할 배포 패키지를 선택합니다.

관리 중인 애플리케이션을 배포하려면 Kaspersky Security Center의 특정 최소 버전을 설치해야 할 수 있습니다.

Kaspersky Endpoint Security for Windows를 위한 암호화 유형을 선택한 후 두 암호화 유형의 배포 패키지 목록이 표시됩니다. 선택한 암호화 유형의 배포 패키지가 목록에서 선택됩니다. 모든 암호화 유형의 배포 패키지를 선택할 수 있습니다. 배포 패키지 언어는 Kaspersky Security Center 언어에 해당합니다. Kaspersky Security Center 언어에 대한 Kaspersky Endpoint Security for Windows 배포 패키지가 없으면 영어 배포 패키지가 선택됩니다.



배포 패키지 다운로드 및 설치 패키지 생성

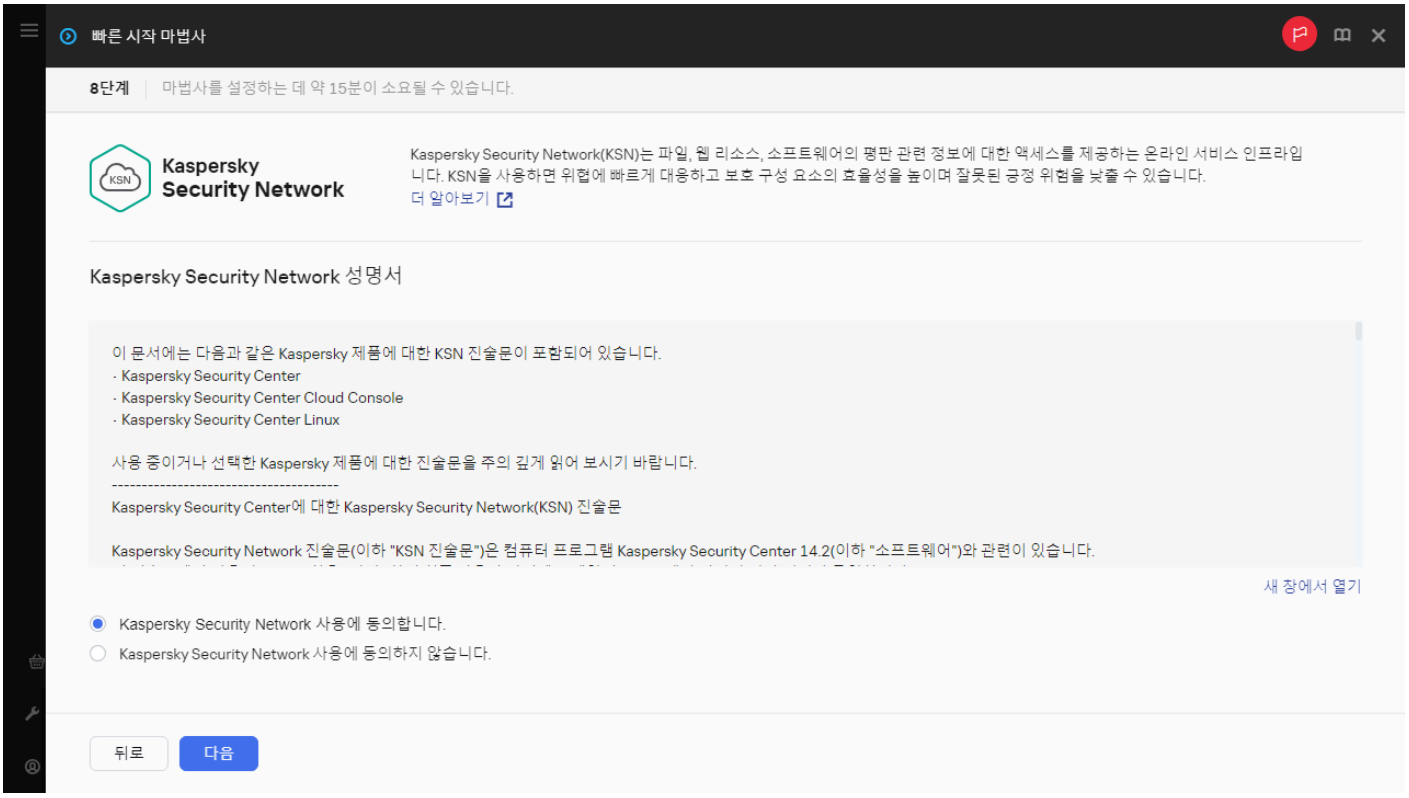
일부 배포 패키지는 EULA에 동의해야 다운로드를 완료할 수 있습니다. **수락** 버튼을 클릭하면 EULA의 본문이 표시됩니다. 마법사의 다음 단계로 진행하려면 EULA의 약관 및 Kaspersky 개인 정보 취급 방침의 약관을 수락해야 합니다. 약관에 동의하지 않으면 패키지 다운로드가 취소됩니다.

EULA의 약관 및 Kaspersky 개인정보취급방침 약관에 동의하면 배포 패키지 다운로드가 계속됩니다. 나중에 설치 패키지를 사용하여 클라이언트 기기에 Kaspersky 애플리케이션을 배포할 수 있습니다.

빠른 시작 마법사와 별도로 배포 패키지를 다운로드하고 나중에 설치 패키지를 생성할 수 있습니다.

8단계. Kaspersky Security Network 구성

Kaspersky Security Center 작동 관련 정보를 Kaspersky Security Network 기술 자료로 전달하기 위한 설정을 지정합니다.



Kaspersky Security Network 구성

다음 옵션 중 하나를 선택합니다:

- **Kaspersky Security Network 사용에 동의합니다**

  클라이언트 기기에 설치된 Kaspersky Security Center 및 관리 중인 애플리케이션은 작업 세부 정보를 Kaspersky Security Network로 자동 전송합니다. Kaspersky Security Network에 참여하면 바이러스 및 기타 위협 관련 정보가 포함된 데이터베이스를 보다 빠르게 업데이트할 수 있으므로 새로운 보안 위협에 더욱 신속하게 대응할 수 있습니다.

- **Kaspersky Security Network 사용에 동의하지 않습니다**

  Kaspersky Security Center 및 관리 중인 애플리케이션은 Kaspersky Security Network로 정보를 제공하지 않습니다.

  이 옵션을 선택하면 Kaspersky Security Network 사용이 비활성화됩니다.

나중에 빠른 시작 마법사와 별도로 KSN(Kaspersky Security Network)에 대한 액세스를 설정할 수 있습니다.

9단계. 애플리케이션 활성화 방법 선택

다음의 Kaspersky Security Center 활성화 옵션 중 하나를 선택합니다:

- **활성화코드 입력**

  *활성화코드*는 20자의 숫자와 문자로 이루진 고유한 값입니다. Kaspersky Security Center를 활성화하는 키를 추가하기 위해 활성화코드를 입력합니다. Kaspersky Security Center 구매 후 지정한 이메일 주소를 통해 활성화코드를 받습니다.

  활성화 코드로 애플리케이션을 활성화하려면 Kaspersky 활성화 서버 연결을 위한 인터넷 액세스가 필요합니다.

  이 활성화 옵션을 선택했다면 **관리 중인 기기에 자동으로 라이센스 키 배포** 옵션을 활성화할 수 있습니다.

  이 옵션을 활성화하면 라이센스 키가 관리 중인 기기에 자동으로 배포됩니다.

  이 옵션을 비활성화하면 나중에 관리 콘솔 트리의 **Kaspersky 라이센스** 노드에서 관리 중인 기기로 라이센스 키를 배포할 수 있습니다.

- **라이센스 키 파일 지정**

  *키 파일*은 Kaspersky에서 사용자에게 제공한 .key 확장자를 가진 파일입니다. 라이센스 키 파일은 애플리케이션을 활성화하는 키를 추가하기 위한 것입니다.

  키 파일을 가져오는 방법은 다음 섹션에서 설명합니다: 키 파일 정보.

  라이센스 키 파일을 사용하여 애플리케이션을 활성화할 때 Kaspersky 활성화 서버에 연결하지 않아도 됩니다.

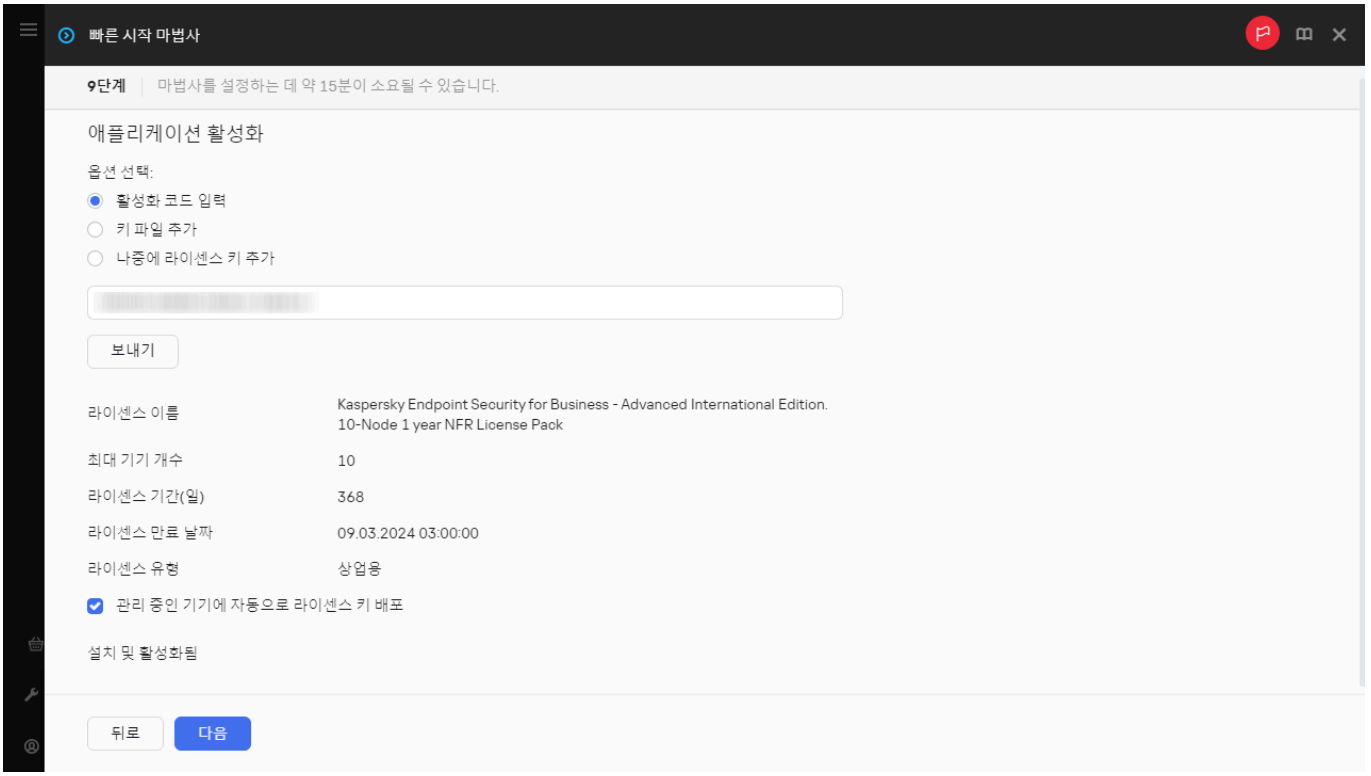
  이 활성화 옵션을 선택했다면 **관리 중인 기기에 자동으로 라이센스 키 배포** 옵션을 활성화할 수 있습니다.

  이 옵션을 활성화하면 라이센스 키가 관리 중인 기기에 자동으로 배포됩니다.

  이 옵션을 비활성화하면 나중에 관리 콘솔 트리의 **Kaspersky 라이센스** 노드에서 관리 중인 기기로 라이센스 키를 배포할 수 있습니다.

- **애플리케이션 활성화 연기**

  애플리케이션이 기본 기능으로 작동하며 모바일 기기 관리와 취약점 및 패치 관리 기능은 제공되지 않습니다.



애플리케이션 활성화 방법 선택

애플리케이션 활성화를 연기하도록 선택한 경우 **동작** → **라이센스**를 선택하여 나중에 언제든지 라이센스 키를 추가할 수 있습니다.

유료 AMI 또는 사용량 기반 월별 청구 SKU에서 배포된 Kaspersky Security Center를 사용할 때는 키 파일을 지정하거나 코드를 입력할 수 없습니다.

10단계. 타사 업데이트 관리 설정 지정

취약점 및 패치 관리 라이센스가 없고 *취약점 및 필요한 업데이트 검색* 작업이 이미 존재한다면, 이 단계가 표시되지 않습니다.



타사 업데이트 관리 설정

타사 소프트웨어 업데이트의 경우 다음 옵션 중 하나를 선택합니다.

- **필요한 업데이트 검색**

  취약점 및 필요한 업데이트 검색 작업이 없다면 자동 생성됩니다.
  이 옵션은 기본적으로 선택되어 있습니다.

- **타사 제품 업데이트 검색 및 설치**

  작업이 없는 경우 *취약점 및 필요한 업데이트 검색* 및 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 자동으로 생성됩니다.

  이 옵션은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

Windows Update 업데이트의 경우 다음 옵션 중 하나를 선택합니다.

- **도메인 정책에서 정의된 업데이트 경로 사용**

  클라이언트 기기는 도메인 정책 설정에 따라 Windows 업데이트 업데이트를 다운로드합니다. 네트워크 에이전트 정책은 없는 경우 자동으로 생성됩니다.

- **WSUS 서버로 이 중앙 관리 서버 사용**

  클라이언트 기기는 중앙 관리 서버에서 Windows 업데이트 업데이트를 다운로드합니다. *Windows 업데이트 동기화 수행* 작업 및 네트워크 에이전트 정책은 없는 경우 자동으로 생성됩니다.

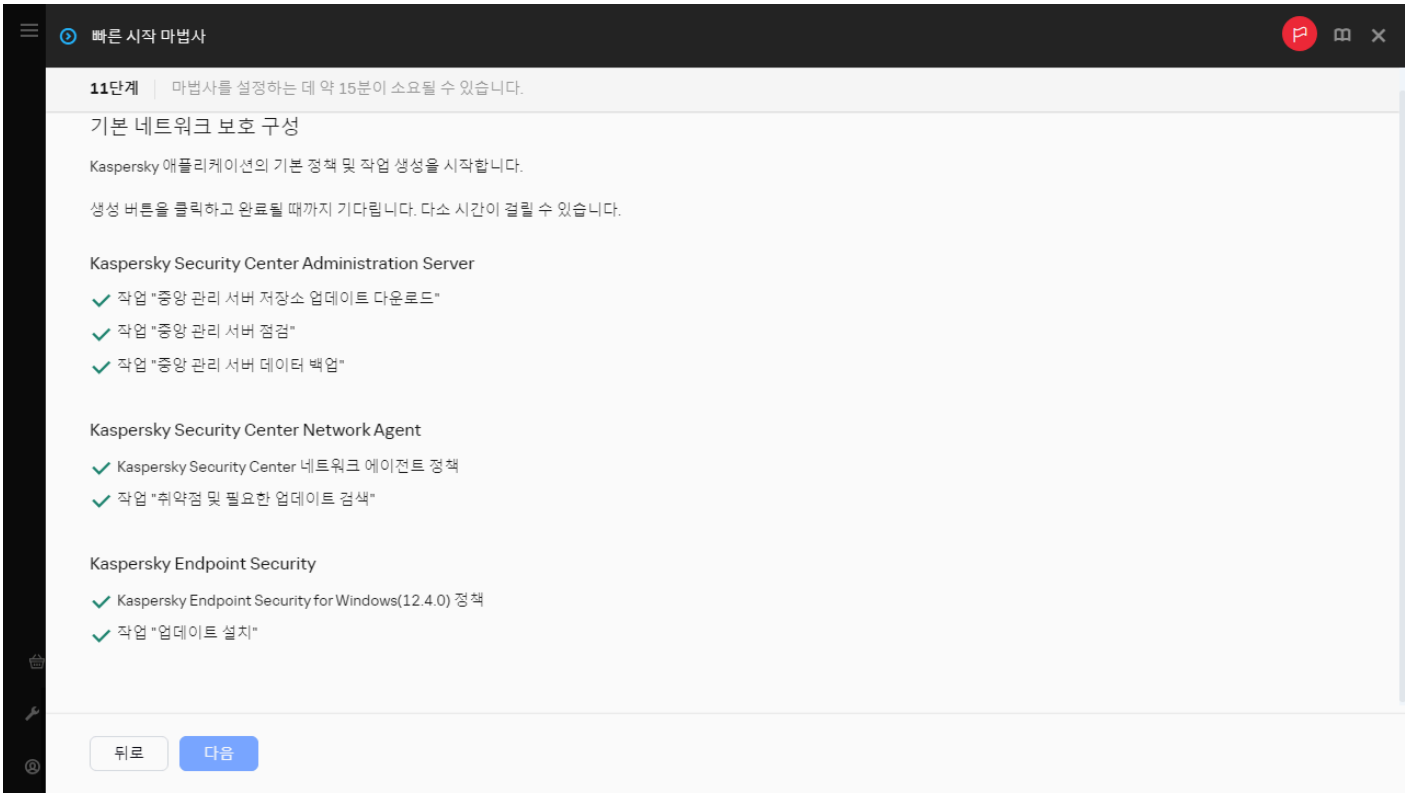
  이 옵션은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

취약성 및 필수 업데이트 검색 및 *필수 업데이트 설치 및 취약성 수정* 태스크를 빠른 시작 마법사와 별도로 생성할 수 있습니다. 중앙 관리 서버를 WSUS 서버로 사용하려면 *Windows 업데이트 동기화 수행* 작업을 만들고 네트워크 에이전트 정책에서 **WSUS 서버로 이 중앙 관리 서버 사용** 옵션을 선택합니다.

11단계. 기본 네트워크 보호 구성 만들기

만들어진 정책 및 작업 목록을 확인할 수 있습니다.

정책 및 작업 만들기가 완료될 때까지 기다린 후에 마법사의 다음 단계로 진행합니다.

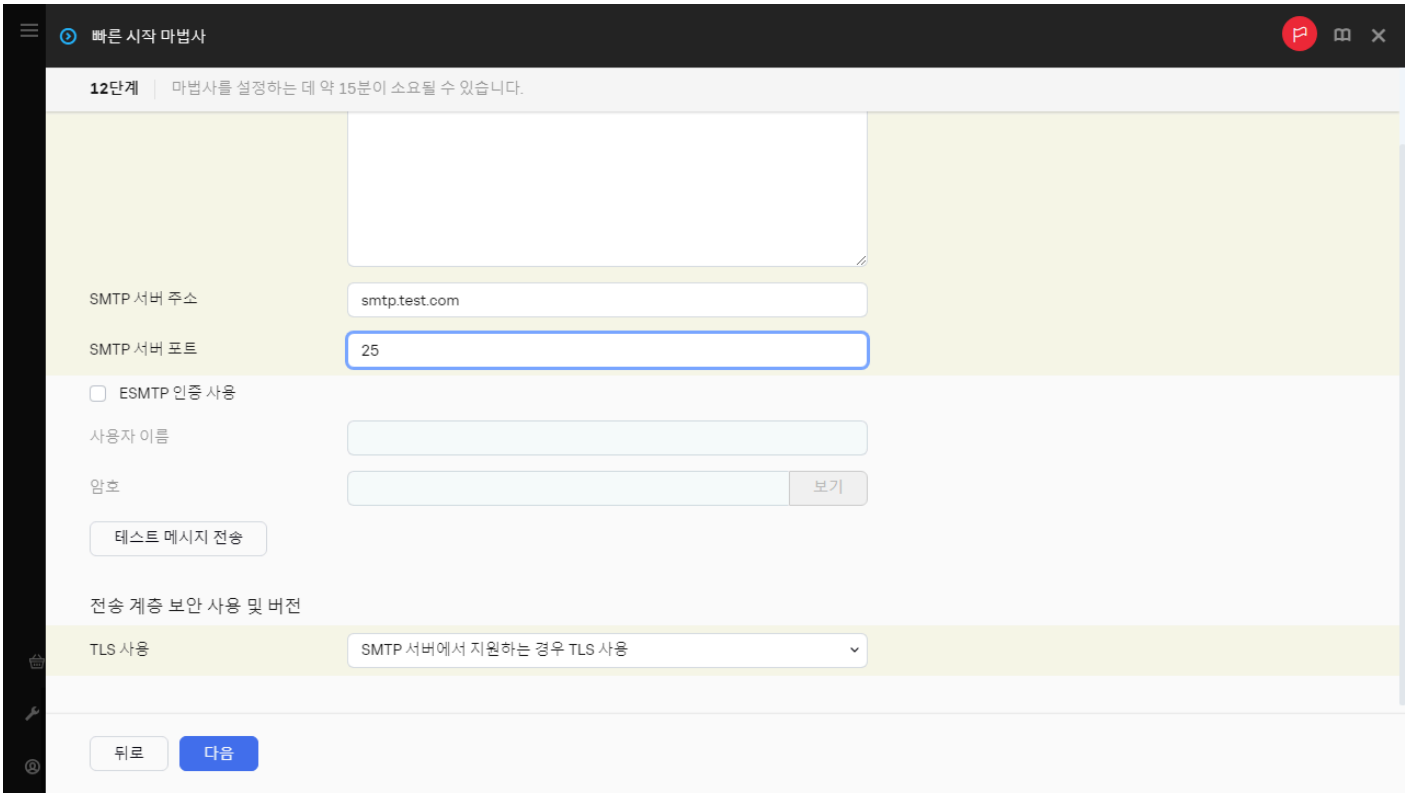


기본 네트워크 보호 구성 만들기

빠른 시작 마법사와 별도로 필요한 작업 및 정책을 나중에 생성할 수 있습니다.

12단계. 이메일 알림 구성

클라이언트 기기에서 Kaspersky 애플리케이션 작동 시 등록된 이벤트에 대한 알림 전달을 구성할 수 있습니다. 이러한 설정은 애플리케이션 정책에 대한 기본 설정으로 사용됩니다.



이메일 알림 구성

Kaspersky 애플리케이션에서 발생하는 이벤트에 대한 알림 전달을 구성하려면 다음 설정을 사용합니다:

- **받는 사람(이메일 주소)**

  애플리케이션에서 알림을 보낼 사용자의 이메일 주소입니다. 주소를 하나 이상 입력할 수 있습니다. 주소를 한 개 이상 입력하고자 할 경우 각 주소를 세미콜론으로 구분하십시오.

- **SMTP 서버 주소**

  조직의 메일 서버 주소 또는 주소들입니다.

  주소를 한 개 이상 입력하고자 할 경우 각 주소를 세미콜론으로 구분하십시오. 다음 값을 사용할 수 있습니다:

  - IPv4 또는 IPv6 주소
  - 기기의 Windows 네트워크 이름(NetBIOS 이름)
  - SMTP 서버의 DNS 이름

- **SMTP 서버 포트**

  SMTP 서버의 통신 포트 번호입니다. 여러 SMTP 서버를 사용한다면 지정된 통신 포트를 통해 이들에 대한 연결이 설정됩니다. 기본 포트 번호는 25입니다.

- **ESMTP 인증 사용**

  ESMTP 인증을 지원하도록 설정합니다. **사용자 이름** 및 **암호** 필드의 확인란을 선택하면 ESMTP 인증 설정을 지정할 수 있습니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

- **TLS 사용**

  다음과 같이 SMTP 서버와의 연결에 대한 TLS 설정을 지정할 수 있습니다.

  - **TLS 사용 안 함**

    이메일 메시지 암호화를 비활성화하려는 경우 이 옵션을 선택할 수 있습니다.

  - **SMTP 서버에서 지원하는 경우 TLS 사용**

    SMTP 서버에 대한 TLS 연결을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 TLS를 사용하지 않고 SMTP 서버에 연결합니다.

  - **항상 TLS를 사용하고 서버 인증서의 유효성을 확인합니다**

    TLS 인증 설정을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 SMTP 서버에 연결할 수 없습니다.

    SMTP 서버와의 연결을 보다 잘 보호하려면 이 옵션을 사용하는 것이 좋습니다. 이 옵션을 선택하면 TLS 연결에 대한 인증 설정을 설정할 수 있습니다.

    항상 TLS를 사용하고 서버 인증서의 유효성을 확인합니다 값을 선택한 경우에는 SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

  다음과 같이 **인증서 지정** 링크를 클릭하여 TLS 연결용 인증서를 지정할 수 있습니다.

  - 다음 SMTP 서버 인증서 파일을 찾습니다.

    신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 중앙 관리 서버에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

  - 다음과 같이 클라이언트 인증서 파일을 찾습니다.

    신뢰할 수 있는 인증 기관과 같은 다양한 출처에서 수신된 인증서를 사용할 수 있습니다. 다음 인증서 유형 중 하나를 사용하여 인증서와 개인 키를 지정해야 합니다:

    - X-509 인증서:

      인증서가 있는 파일과 개인 키가 있는 파일을 지정해야 합니다. 두 파일은 서로 의존하지 않으며 파일의 로딩 순서는 중요하지 않습니다. 두 파일이 모두 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

- pkcs12 컨테이너:

  인증서와 개인 키가 포함 된 단일 파일을 업로드해야 합니다. 파일이 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

테스트 메시지 전송 버튼을 눌러 새 이메일 알림 설정을 테스트할 수 있습니다.

빠른 시작 마법사와는 별도로 나중에 이벤트 알림을 구성할 수 있습니다.

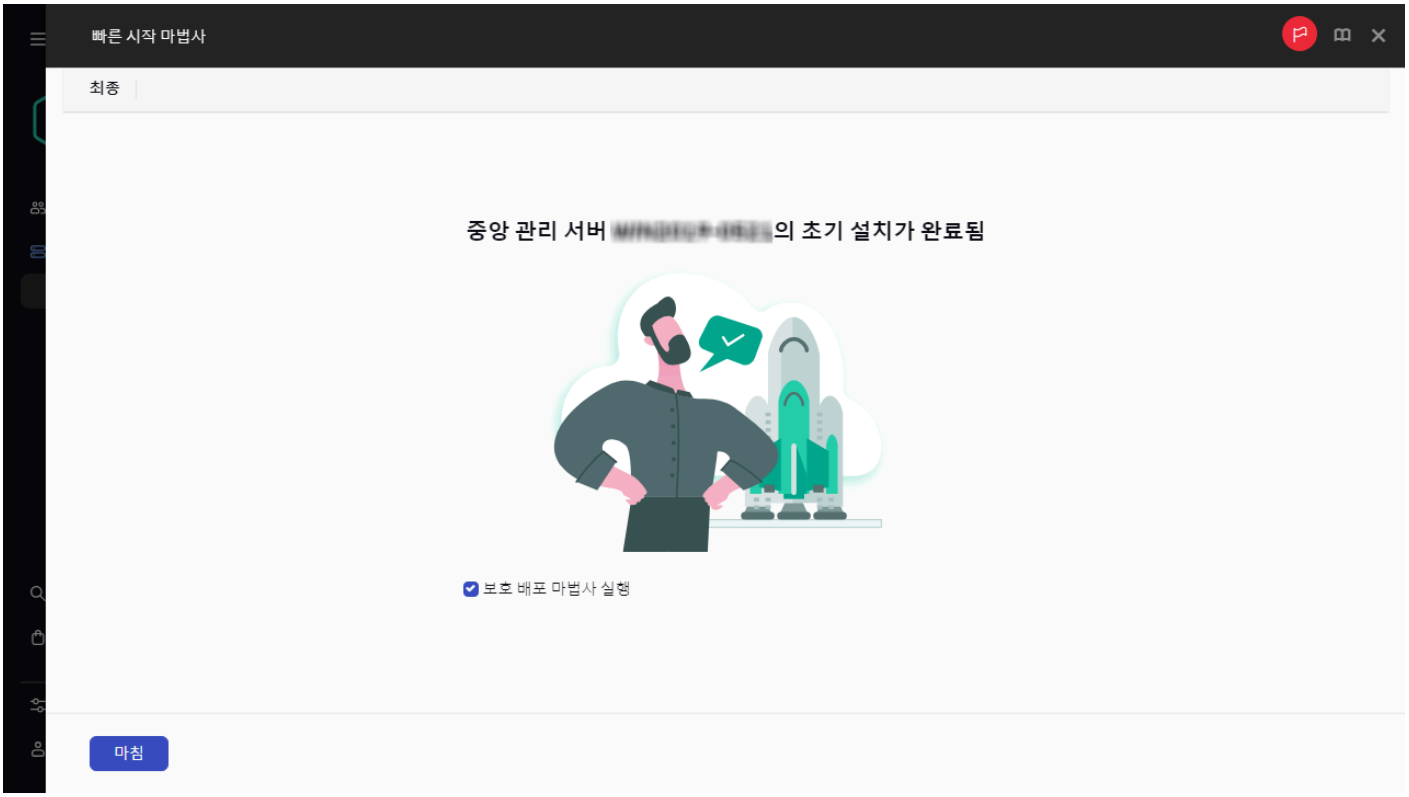
13단계. 네트워크 검색 수행

중앙 관리 서버는 초기 검색을 수행합니다. 검색 중에 진행률 막대가 표시됩니다. 검색이 완료되면 **검색된 기기 보기** 링크를 사용할 수 있습니다. 이 링크를 누르면 중앙 관리 서버에서 감지한 네트워크 기기를 확인할 수 있습니다. 빠른 시작 마법사로 돌아가려면 **Escape** 키를 누릅니다.

빠른 시작 마법사와는 별도로 네트워크를 나중에 검색할 수도 있습니다. Kaspersky Security Center 웹 콘솔을 사용하여 도메인 컨트롤러, Windows 도메인, IP 범위, IPv6 네트워크의 검색을 구성합니다.

14단계. 빠른 시작 마법사 닫기

네트워크의 기기에서 안티 바이러스 애플리케이션 또는 네트워크 에이전트의 자동 설치를 시작하려면 빠른 시작 마법사 완료 페이지에서 **보호 배포 마법사 실행** 확인란을 선택합니다.



빠른 시작 마법사의 마지막 단계

마법사를 닫으려면 **마침** 버튼을 누릅니다.

이동 사용자 기기 연결

이 섹션은 이동 사용자 기기(즉, 기본 네트워크 외부에 있는 관리 중인 기기)를 중앙 관리 서버에 연결하는 방법을 설명합니다.

시나리오: 연결 게이트웨이를 통해 이동 사용자 기기 연결

이 시나리오는 기본 네트워크 외부에 있는 관리 중인 기기를 중앙 관리 서버에 연결하는 방법을 설명합니다.

필수 구성 요소

시나리오에는 다음과 같은 전제 조건이 필요합니다.

- 완충 지역(DMZ)이 조직 네트워크에 구성됩니다.
- Kaspersky Security Center 중앙 관리 서버가 회사 네트워크에 배포됩니다.

단계

이 시나리오는 단계적으로 진행됩니다.

1. **DMZ에서 클라이언트 기기 선택**

   이 기기는 연결 게이트웨이로 사용됩니다. 선택하는 기기가 연결 게이트웨이에 대한 요구 사항을 충족해야 합니다.

2. **연결 게이트웨이 역할에 네트워크 에이전트 설치**

   선택한 기기에 네트워크 에이전트를 설치하려면 로컬 설치를 사용하는 것이 좋습니다.

   기본적으로 설치 파일은 다음 위치에 있습니다. \\<server name>\KLSHARE\PkgInst\NetAgent_<version number>

   네트워크 에이전트 설치 마법사의 **연결 게이트웨이** 창에서 **연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용**을 선택합니다. 이 모드는 동시에 연결 게이트웨이 역할을 활성화하고 네트워크 에이전트가 중앙 관리 서버에 대한 연결을 설정하지 않고 중앙 관리 서버에서 연결을 기다리도록 지시합니다.

   또는 Linux 기기에 네트워크 에이전트를 설치하고 네트워크 에이전트를 연결 게이트웨이로 작동하도록 구성할 수 있지만 Linux 기기에서 실행되는 네트워크 에이전트의 제한 사항 목록에 주의를 기울이십시오.

3. **연결 게이트웨이의 방화벽에서 연결 허용**

   중앙 관리 서버를 실제로 DMZ의 연결 게이트웨이에 연결할 수 있는지 확인하려면 중앙 관리 서버와 연결 게이트웨이 사이의 모든 방화벽에서 TCP 포트 13000에 대한 연결을 허용하십시오.

   연결 게이트웨이가 인터넷상의 실제 IP 주소를 가지고 있지는 않지만 대신 NAT(Network Address Translation) 뒤에 있다면, NAT를 통해 연결을 전달하도록 규칙을 구성하십시오.

4. **외부 기기에 대한 관리 그룹 생성**

   관리 중인 기기 그룹 아래에 새 그룹을 생성합니다. 이 새 그룹에는 외부 관리 중인 기기가 포함됩니다.

5. **연결 게이트웨이를 중앙 관리 서버에 연결**

구성한 연결 게이트웨이가 중앙 관리 서버의 연결을 기다리고 있습니다. 하지만 중앙 관리 서버에는 연결 게이트웨이 기기가 관리 중인 기기로 나열되지 않습니다. 이는 연결 게이트웨이가 중앙 관리 서버 연결을 설정하려고 하지 않았기 때문입니다. 따라서 특별한 절차를 통해 중앙 관리 서버가 연결 게이트웨이로의 연결을 초기화하도록 해야 합니다.

다음을 수행하십시오.

1. 연결 게이트웨이를 배포 지점으로 추가합니다.
2. 연결 게이트웨이를 **미할당 기기** 그룹에서 외부 기기용으로 생성한 그룹으로 이동합니다.

연결 게이트웨이가 연결되고 구성됩니다.

6 중앙 관리 서버에 외부 데스크톱 기기 연결

일반적으로 외부 데스크톱 기기는 경계 내부로 이동하지 않습니다. 따라서 네트워크 에이전트를 설치할 때 게이트웨이를 통해 중앙 관리 서버에 연결하도록 구성해야 합니다.

7 외부 데스크톱 기기에 대한 업데이트 설정

보안 애플리케이션의 업데이트가 중앙 관리 서버에서 다운로드되도록 구성된 경우 외부 기기는 연결 게이트웨이를 통해 업데이트를 다운로드하며, 여기에는 다음 두 가지 단점이 있습니다.

- 회사 인터넷 커뮤니케이션 채널의 대역폭을 차지하는 불필요한 트래픽입니다.
- 업데이트를 받는 가장 빠른 방법이 아닙니다. 외부 기기의 경우 Kaspersky 업데이트 서버에서 업데이트를 받는 것이 더 저렴하고 빠를 수 있습니다.

다음을 수행하십시오.

1. 모든 외부 기기를 이전에 만든 별도의 관리 그룹으로 이동합니다.
2. 업데이트 작업에서 외부 기기가 있는 그룹을 제외합니다.
3. 외부 기기가 있는 그룹에 대해 별도의 업데이트 작업을 생성합니다.

8 이동 중인 랩톱을 중앙 관리 서버에 연결

이동 중인 랩톱은 때로는 네트워크 내에 있고 때로는 네트워크 외부에 있습니다. 효과적인 관리를 위해서는 위치에 따라 다르게 중앙 관리 서버에 연결해야 합니다. 트래픽을 효율적으로 사용하려면 위치에 따라 다른 소스에서 업데이트를 받아야 합니다.

이동 사용자에 대한 규칙(연결 프로필 및 네트워크 위치 설명)을 구성해야 합니다. 각 규칙은 이동 중인 랩톱이 위치에 따라 연결해야 하는 중앙 관리 서버 인스턴스와 업데이트를 받아야 하는 중앙 관리 서버 인스턴스를 정의합니다.

시나리오: DMZ의 보조 중앙 관리 서버를 통해 부재 중 기기 연결

중앙 관리 서버에 기본 네트워크 외부에 있는 관리 중인 기기를 연결하려면 DMZ(Demilitarized Zone)에 있는 보조 중앙 관리 서버를 사용하면 됩니다.

필수 구성 요소

시작하기 전에 다음을 수행했는지 확인하십시오:

- DMZ가 조직 네트워크에 구성됩니다.
- Kaspersky Security Center 중앙 관리 서버가 조직의 내부 네트워크에 배포됩니다.

단계

이 시나리오는 단계적으로 진행됩니다.

1. **DMZ에서 클라이언트 기기 선택**

   DMZ에서 보조 중앙 관리 서버로 사용할 클라이언트 기기를 선택합니다.

2. **Kaspersky Security Center 중앙 관리 서버 설치**

   이 클라이언트 기기에 Kaspersky Security Center 중앙 관리 서버를 설치합니다.

3. **중앙 관리 서버의 계층 구조 생성**

   DMZ에 보조 중앙 관리 서버를 둔다면, 보조 중앙 관리 서버는 기본 중앙 관리 서버에서 연결을 받아야 합니다. 이렇게 하려면, 새 중앙 관리 서버를 보조로 추가하여 13000 포트를 통해 기본 중앙 관리 서버가 보조 중앙 관리 서버에 연결하도록 합니다. 두 개의 중앙 관리 서버를 하나의 계층으로 결합할 때는 두 중앙 관리 서버 모두에서 13299 포트가 열려 있어야 합니다. 13299 포트를 통해 Kaspersky Security Center 웹 콘솔이 해당 중앙 관리 서버와 연결합니다.

4. **외부의 관리 중인 기기를 보조 중앙 관리 서버에 연결**

   중앙 관리 서버와 기본 네트워크에 있는 관리 중인 기기 간에 연결이 설정되는 것과 같은 방식으로 외부에 있는 기기를 DMZ의 중앙 관리 서버에 연결할 수 있습니다. 외부의 관리 중인 기기가 13000 포트를 통해 연결을 시작합니다.

이동 사용자 기기 연결 정보

일부 관리 중인 기기는 항상 기본 네트워크 외부(예: 회사 지사의 기기, 다양한 판매 지점에 설치된 키오스크, ATM 및 터미널, 직원의 본사 기기)에 위치합니다. 일부 기기는 때때로 경계 밖으로 이동합니다(예: 지사 또는 고객 사무실을 방문하는 사용자의 랩톱).

계속 이동 사용자 기기의 보호를 모니터링하고 관리해야 합니다. 보호 상태에 대한 실제 정보를 수신하고 해당 기기의 보안 애플리케이션을 최신 상태로 유지해야 합니다. 예를 들어 이러한 기기가 기본 네트워크에서 떨어져있는 동안 떨어져 있는 동안 손상되면 기본 네트워크에 연결하는 즉시 위협을 전파하는 플랫폼이 될 수 있기 때문에 이는 중요합니다. 다음 두 가지 방법을 사용하여 이동 사용자 기기를 중앙 관리 서버에 연결할 수 있습니다.

- DMZ(완충 지역)의 연결 게이트웨이

  다음 데이터 트래픽 스키마를 참조하십시오. LAN의 중앙 관리 서버, 인터넷의 관리 중인 기기, 사용 중인 연결 게이트웨이.

- DMZ의 중앙 관리 서버

  다음 데이터 트래픽 스키마를 참조하십시오. DMZ의 중앙 관리 서버, 인터넷의 관리 중인 기기.

DMZ의 연결 게이트웨이

이동 사용자 기기를 중앙 관리 서버에 연결 시 권장되는 방법은 조직의 네트워크에 DMZ를 구성하고 DMZ에 연결 게이트웨이를 설치하는 것입니다. 외부 기기는 연결 게이트웨이에 연결되고 네트워크 내부의 중앙 관리 서버는 연결 게이트웨이를 통해 기기에 대한 연결을 시작합니다.

다른 방법에 비해 이 방법이 더 안전합니다.

- 네트워크 외부에서 중앙 관리 서버에 대한 액세스를 열 필요가 없습니다.
- 손상된 연결 게이트웨이가 네트워크 기기의 안전에 큰 위험이 되지 않습니다. 연결 게이트웨이는 자체적으로 아무것도 관리하지 않으며 연결을 설정하지도 않습니다.

또한 연결 게이트웨이에는 많은 하드웨어 리소스가 필요하지 않습니다.

그러나 이 방법에는 더 복잡한 구성 프로세스가 있습니다.

- 기기를 DMZ의 연결 게이트웨이로 사용하려면 네트워크 에이전트를 설치하고 이를 구체적인 방법으로 중앙 관리 서버에 연결해야 합니다.
- 모든 상황에서 중앙 관리 서버에 연결하는 데 동일한 주소를 사용할 수는 없습니다. 경계 외부에서 다른 주소(연결 게이트웨이 주소)는 물론 연결 게이트웨이를 통한 다른 연결 모드를 사용해야 합니다.
- 또한 다른 위치에 있는 랩톱에 대해 다른 연결 설정을 정의해야 합니다.

이전에 구성된 네트워크에 연결 게이트웨이를 추가하려면:

1. 연결 게이트웨이 모드에 네트워크 에이전트 설치.
2. 새로 추가된 연결 게이트웨이에 연결하려는 장치에 네트워크 에이전트를 다시 설치하십시오.

DMZ의 중앙 관리 서버

또 다른 방법은 DMZ에 단일 중앙 관리 서버를 설치하는 것입니다.

이 구성은 다른 방법보다 덜 안전합니다. 이때, 외부 랩톱을 관리하려면 중앙 관리 서버가 인터넷의 모든 주소에서의 연결을 허용해야 합니다. 그래도 여전히 내부 네트워크의 모든 기기를 관리하며 이러한 관리는 DMZ에서 이루어집니다. 따라서 완전히 손상된 서버는 이러한 이벤트가 발생할 가능성이 낮음에도 불구하고 엄청난 피해를 입힐 수 있습니다.

DMZ의 중앙 관리 서버가 내부 네트워크의 기기를 관리하지 않는 경우 위험이 상당히 낮아집니다. 예를 들어 서비스 공급업체는 이러한 구성을 사용하여 고객의 기기를 관리할 수 있습니다.

다음과 같은 경우 이 방법을 사용할 수 있습니다.

- 중앙 관리 서버 설치 및 구성에 익숙하고, 연결 게이트웨이를 설치 및 구성하는 다른 절차를 수행하지 않으려는 경우.
- 더 많은 기기를 관리해야 하는 경우. 중앙 관리 서버의 기기 지원 수는 최대 100,000대이며, 연결 게이트웨이는 최대 기기 10,000대를 지원할 수 있습니다.

이 솔루션에는 다음과 같은 어려움이 있을 수 있습니다.

- 중앙 관리 서버에는 더 많은 하드웨어 리소스와 하나 이상의 데이터베이스가 필요합니다.
- 기기에 대한 정보는 관련이 없는 두 개의 데이터베이스(네트워크 내부의 중앙 관리 서버 및 DMZ의 다른 중앙 관리 서버의 경우)에 저장되므로 모니터링이 복잡합니다.
- 모든 기기를 관리하려면 중앙 관리 서버를 계층 구조로 결합해야 하므로 모니터링뿐만 아니라 관리도 복잡합니다. 보조 중앙 관리 서버 인스턴스로 인해 관리 그룹의 가능한 구조에 제한이 발생합니다. 보조 중앙 관리 서버 인스턴스에 배포할 방법, 작업 및 정책을 결정해야 합니다.
- 외부의 DMZ에서 중앙 관리 서버를 사용하고 내부의 기본 중앙 관리 서버를 사용하도록 외부 기기를 구성하는 것은 게이트웨이를 통해 조건부 연결을 사용하도록 구성하는 것보다 간단하지 않습니다.
- 높은 보안 위험. 손상된 중앙 관리 서버 인스턴스는 관리 중인 랩톱을 쉽게 손상시킬 수 있습니다. 이러한 손상이 발생하면 해커는 랩톱 중 하나가 회사 네트워크로 돌아올 때까지 기다려야 로컬 영역 네트워크에 대한 공격을 계속할 수 있습니다.

중앙 관리 서버에 외부 데스크톱 기기 연결

항상 기본 네트워크 외부에 있는 데스크톱 기기(예: 회사 지사의 기기, 다양한 판매 지점에 설치된 키오스크, ATM 및 터미널, 직원의 본사 기기)는 중앙 관리 서버에 직접 연결할 수 없습니다. DMZ(완충 지역)에 설치된 연결 게이트웨이를 통해 중앙 관리 서버에 연결되어야 합니다. 이 구성은 해당 기기에 네트워크 에이전트를 설치할 때 설정됩니다.

중앙 관리 서버에 외부 데스크톱 기기를 연결하는 방법:

1. 네트워크 에이전트에 대한 새 설치 패키지를 생성합니다.
2. 생성된 설치 패키지의 속성을 열고 **설정** → **고급**로 이동한 다음, **연결 게이트웨이를 통해 중앙 관리 서버에 연결** 옵션을 선택합니다.

   연결 게이트웨이를 통해 중앙 관리 서버에 연결 설정은 **연결 게이트웨이로 DMZ에 있는 네트워크 에이전트 사용** 설정과 호환되지 않습니다. 이 두 설정을 동시에 활성화할 수 없습니다.

3. **연결 게이트웨이 주소** 필드에서 연결 게이트웨이의 공용 주소를 지정합니다.

   연결 게이트웨이가 NAT(Network Address Translation) 뒤에 있고 자체 공용 주소가 없는 경우 공용 주소에서 연결 게이트웨이의 내부 주소로 연결을 전달하도록 NAT 게이트웨이 규칙을 구성합니다.

4. 생성된 설치 패키지를 기반으로 독립 실행형 설치 패키지를 생성합니다.
5. 독립 실행형 설치 패키지를 전자적으로 또는 이동식 드라이브를 통해 대상 기기에 제공합니다.
6. 독립 실행형 패키지에서 네트워크 에이전트를 설치합니다.

외부 데스크톱 기기는 중앙 관리 서버에 연결됩니다.

이동 사용자를 위한 연결 프로필 정보

노트북(이하 "기기"로 지칭함)의 이동 사용자는 기업 네트워크의 기기 현재 위치에 따라 중앙 관리 서버 간을 전환하거나 중앙 관리 서버에 연결하는 방법을 변경해야 할 수 있습니다.

연결 프로필은 Windows 및 macOS를 실행 중인 기기에서만 지원됩니다.

단일 중앙 관리 서버의 여러 주소 사용

네트워크 에이전트가 설치된 기기는 조직의 인트라넷이나 인터넷에서 중앙 관리 서버에 연결할 수 있습니다. 이러한 상황에서는 네트워크 에이전트가 중앙 관리 서버에 연결하는 데 다른 주소를 사용해야 할 수 있습니다. 인터넷 연결에는 외부 중앙 관리 서버 주소를 사용하고, 내부 네트워크 연결에는 내부 중앙 관리 서버 주소를 사용할 수 있습니다.

이렇게 하려면, 네트워크 에이전트 정책 속성(**애플리케이션 설정 → 연결성 → 연결 프로필 → 중앙 관리 서버 연결 프로필** 섹션)에서 인터넷에서 중앙 관리 서버에 연결하기 위한 프로필을 추가합니다. 프로필 만들기 창에서**지정한 서버에서 업데이트만 다운로드** 옵션을 비활성화하고 **이 프로필에 지정된 중앙 관리 서버 설정과 연결 설정을 동기화** 옵션을 선택해야 합니다. 중앙 관리 서버에 접속할 때 연결 게이트웨이를 사용한다면(예, 인터넷 접속: 연결 게이트웨이로 DMZ에 있는 네트워크 에이전트에서 설명되어 있는 Kaspersky Security Center 구성), 해당 연결 프로필의 관련 필드에서 연결 게이트웨이 주소를 지정해야 합니다.

현재 네트워크에 따라 중앙 관리 서버 간 전환

조직이 각기 다른 중앙 관리 서버를 사용하는 여러 사무소를 운영하며 네트워크 에이전트가 설치된 기기 중 일부를 해당 사무소 간에 이동하는 경우에는 현재 기기가 있는 사무소 내 로컬 네트워크의 중앙 관리 서버에 네트워크 에이전트를 연결해야 합니다.

이 경우 원래 홈 중앙 관리 서버가 있는 본사 사무소를 제외한 각 사무소에 대해 네트워크 에이전트 정책의 속성에서 중앙 관리 서버 연결용 프로필을 만들어야 합니다. 연결 프로필에서 중앙 관리 서버 주소를 지정해야 하며 **지정한 서버에서 업데이트만 다운로드** 옵션을 활성화 또는 비활성화해야 합니다.

- 로컬 서버는 업데이트 다운로드용으로만 사용하고 홈 중앙 관리 서버와 네트워크 에이전트를 동기화해야 하는 경우 옵션을 선택합니다.
- 로컬 중앙 관리 서버를 통해서만 네트워크 에이전트를 관리해야 하는 경우 이 옵션을 비활성화합니다.

그 후에는 새로 만든 프로필로 전환할 조건을 설정해야 합니다: 본사 사무소를 제외한 각 사무소에 대해 조건을 하나 이상 설정합니다. 모든 조건은 사무소의 네트워크 환경과 관련된 항목을 탐지하는 데 사용됩니다. 조건이 참이면 해당 프로필이 활성화됩니다. 참인 조건이 없으면 네트워크 에이전트가 홈 중앙 관리 서버로 전환됩니다.

이동 사용자에 대한 연결 프로필 만들기

중앙 관리 서버 연결 프로필은 Windows 및 macOS를 실행 중인 기기에서만 사용 가능합니다.

이동 사용자에 대한 중앙 관리 서버 네트워크 에이전트 연결 프로필을 만들려면 다음과 같이 하십시오:

1. 관리 중인 기기 그룹에 대한 연결 프로필을 생성하려면 이 그룹의 네트워크 에이전트 정책을 엽니다. 이를 위해 다음 작업을 수행합니다.

   a. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**이동합니다.

   b. 현재 경로 링크를 누릅니다.

   c. 열리는 창에서 필요한 관리 그룹을 선택합니다.
   이후에 현재 경로가 변경됩니다.

   d. 관리 중인 기기 그룹에 대한 네트워크 에이전트 정책을 추가합니다. 이미 만든 경우 네트워크 에이전트 정책 이름을 눌러 정책 속성을 엽니다.

2. 특정 관리 대상 기기에 대한 연결 프로필을 만들려면 다음을 수행합니다.

   a. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.

   b. 관리 중인 기기의 이름을 누릅니다.

   c. 관리 중인 기기 속성 창이 열리면 **애플리케이션** 탭을 누릅니다.

   d. 선택한 관리 중인 기기에만 적용되는 네트워크 에이전트 정책의 이름을 누릅니다.

3. 열리는 속성 창에서 **애플리케이션 설정 → 연결성 → 연결 프로필로 이동합니다.**

4. **중앙 관리 서버 연결 프로필** 설정 그룹에서 **추가** 버튼을 클릭합니다.
   기본적으로 연결 프로필 목록에는 <오프라인 모드> 및 <홈 중앙 관리 서버> 프로필이 포함됩니다. 이러한 프로필은 편집하거나 제거할 수 없습니다.
   <오프라인 모드> 프로필에는 연결할 서버가 지정되어 있지 않습니다. 따라서 이 프로필로 전환하는 네트워크 에이전트는 클라이언트 기기에 설치되어 있는 애플리케이션에서 이동 사용자 정책을 사용하여 작업하는 동안 중앙 관리 서버에 연결을 시도하지 않습니다. 네트워크에서 기기 연결이 끊어진 경우 <오프라인 모드> 프로필을 사용할 수 있습니다.
   <홈 중앙 관리 서버> 프로필은 네트워크 에이전트 설치 시 선택한 중앙 관리 서버에 대한 연결을 지정합니다. 기기를 일정 시간 동안 외부 네트워크에서 실행하다가 홈 중앙 관리 서버에 다시 연결하면 <홈 중앙 관리 서버> 프로필이 적용됩니다.

5. 새 프로필 창이 열리면 다음과 같이 **프로필 구성**.

   - **프로필 이름**

     입력 필드에서 연결 프로필 이름을 보거나 변경할 수 있습니다.

   - **중앙 관리 서버 주소**

     프로필 활성화 중에 클라이언트 기기가 연결해야 하는 중앙 관리 서버의 주소입니다.

   - **포트 번호**

     연결에 사용되는 포트 번호.

- **SSL 포트**

  SSL 프로토콜을 사용하는 경우 연결용 포트 번호입니다.

- **SSL 연결 사용**

  이 옵션을 사용하면 SSL 프로토콜을 사용하여 보안 포트를 통해 연결됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 연결이 안전하게 유지되도록 이 옵션을 비활성화하지 않는 것이 좋습니다.

- 인터넷에 연결할 때 프록시 서버를 사용하려면 **프록시 서버 사용** 옵션을 선택합니다. 이 옵션을 선택하면 설정을 입력하는 필드를 사용할 수 있게 됩니다. 프록시 서버 연결에 대해 다음 설정을 지정합니다.

  - **주소**

    Kaspersky Security Center에서 인터넷 연결에 사용한 프록시 서버의 주소입니다.

  - **포트 번호**

    Kaspersky Security Center 프록시 연결을 설정하는 데 사용되는 포트 번호입니다.

  - **프록시 서버 인증**

    이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.

  - **사용자 이름**

    프록시 서버에 대한 연결을 구성할 사용자 계정입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

  - **암호**

    프록시 서버 연결을 구성한 계정의 사용자가 설정한 암호입니다(이 필드는 **프록시 서버 인증** 확인란을 선택한 경우 사용할 수 있음).

    입력한 암호를 보려면 **보기** 버튼을 필요한 시간 동안 누르고 있어야 합니다.

- **연결 게이트웨이 주소**

  클라이언트 기기가 중앙 관리 서버에 연결할 때 사용하는 게이트웨이의 주소입니다.

- **중앙 관리 서버에 연결할 수 없으면 이동 사용자 모드 사용**

  클라이언트 기기에 설치된 애플리케이션이 중앙 관리 서버를 사용할 수 없는 경우 모든 연결 시도에서 이동 사용자 모드의 정책 프로필과 이동 사용자 정책을 사용할 수 있도록 허용하려면 이 확인란을 선택합니다. 애플리케이션에 대해 이동 사용자 정책이 정의되어 있지 않은 경우에는 활성 정책이 사용됩니다.

  이 옵션을 비활성화하면 애플리케이션에서 활성 정책을 사용합니다.

기본적으로 이 확인란은 선택되어 있지 않습니다.

- **지정한 서버에서 업데이트만 다운로드**

  이 옵션을 사용하면 클라이언트 기기에 설치된 애플리케이션을 통해 업데이트를 다운로드하는 데에만 프로필이 사용됩니다. 다른 작업의 경우 네트워크 에이전트 설치 중 정의된 초기 연결 설정에 따라 중앙 관리 서버와의 연결이 설정됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **이 프로필에 지정된 중앙 관리 서버 설정과 연결 설정을 동기화**

  이 옵션을 사용하면 네트워크 에이전트는 프로필에 지정된 설정을 사용해 중앙 관리 서버에 연결합니다.

  이 옵션을 비활성화하면 네트워크 에이전트는 설치하는 동안 지정되었던 원본 설정을 사용해 중앙 관리 서버에 연결합니다.

  이 옵션은 지정한 서버에서 **지정한 서버에서 업데이트만 다운로드** 옵션이 비어 있는 경우에 사용 가능합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

그러면 이동 사용자에 대해 네트워크 에이전트를 중앙 관리 서버에 연결하는 프로필이 만들어집니다. 네트워크 에이전트가 이 프로필을 사용하여 중앙 관리 서버에 연결했다면 클라이언트 기기에 설치된 애플리케이션은 이동 사용자 정책 또는 이동 사용자 모드에 있는 기기를 위한 정책을 사용합니다.

다른 중앙 관리 서버로 네트워크 에이전트 전환 정보

Kaspersky Security Center에서는 다음과 같은 네트워크 설정이 변경된 경우 클라이언트 기기의 네트워크 에이전트를 다른 중앙 관리 서버로 전환하는 옵션을 제공합니다:

- **DHCP 서버 주소 조건** – 네트워크 DHCP(Dynamic Host Configuration Protocol) 서버의 IP 주소가 변경된 경우.
- **기본 연결 게이트웨이 주소 조건** –기본 네트워크 게이트웨이의 주소가 변경된 경우.
- **DNS 도메인 조건** - 서브넷의 DNS 접미사가 변경된 경우.
- **DNS 서버 주소 조건** –네트워크 DNS 서버의 IP 주소가 변경된 경우.
- **WINS 서버 주소 조건** –네트워크 WINS 서버의 IP 주소가 변경된 경우. 이 설정은 Windows를 실행하는 기기에서만 사용할 수 있습니다.
- **이름 해석 가능성 조건**-클라이언트 기기의 DNS 또는 NetBIOS 이름이 변경되었습니다.
- **서브넷 조건** –서브넷 주소 및 마스크를 변경합니다.
- **Windows 도메인 접근 가능성 조건**– 클라이언트 기기가 연결된 Windows 도메인의 상태를 변경합니다. 이 설정은 Windows를 실행하는 기기에서만 사용할 수 있습니다.
- **SSL 연결 주소 접근 가능성 조건**-클라이언트 기기는 지정한 서버(이름:포트)와 SSL 연결을 설정할 수 있거나 설정할 수 없습니다(선택한 옵션에 따라 다름). 연결 시 발생하는 높은 부하와 빈번한 네트워크 에이전트 요청을 처리할 수 있는 소프트웨어가 설치된 전용 서버를 사용해야 합니다. 중앙 관리 서버의 포트를 지정하지 마십시오. 각 서버에 대해 SSL 인증서를 추가로 지정할 수 있습니다. 이 경우 네트워크 에이전트는 SSL 연결 기능은 물론 서버 인증서를 확인합니다. 인증서가 일치하지 않으면 연결이 실패합니다.

이 기능은 Windows 또는 macOS를 실행하는 기기에 설치된 네트워크 에이전트에서만 지원됩니다.

중앙 관리 서버에 대한 네트워크 에이전트 연결의 초기 설정은 네트워크 에이전트가 설치될 때 정의됩니다. 이후에는 네트워크 에이전트를 다른 중앙 관리 서버로 전환하는 규칙을 만든 경우 네트워크 에이전트에서 다음과 같이 네트워크 설정의 변경 사항에 대응합니다:

- 네트워크 설정이 작성된 규칙 중 하나와 일치하는 경우 네트워크 에이전트가 이 규칙에 지정된 중앙 관리 서버에 연결됩니다. 클라이언트 기기에 설치된 애플리케이션이 이동 사용자 정책으로 전환됩니다(규칙에 지정된 경우).
- 기존의 어떤 규칙도 적용할 수 없는 경우 네트워크 에이전트가 설치 시 정의된 중앙 관리 서버에 대한 기본 연결 설정으로 되돌아갑니다. 클라이언트 기기에 설치된 애플리케이션이 활성 정책으로 다시 전환됩니다.
- 중앙 관리 서버에 접근할 수 없는 경우 네트워크 에이전트는 이동 사용자 정책을 사용합니다.

> 네트워크 에이전트 정책 설정에서 **중앙 관리 서버에 연결할 수 없으면 이동 사용자 모드 사용** 옵션이 활성화되어 있는 경우에만 네트워크 에이전트가 이동 사용자 정책으로 전환합니다.

중앙 관리 서버에 대한 네트워크 에이전트 연결 설정은 연결 프로필에 저장됩니다. 연결 프로필에서는 클라이언트 기기를 이동 사용자 정책으로 전환하는 규칙을 만들 수 있을 뿐 아니라 업데이트 다운로드에만 사용되는 프로필을 구성할 수도 있습니다.

네트워크 위치에 따른 네트워크 에이전트 전환 규칙 만들기

> 네트워크 위치에 따른 네트워크 에이전트 전환은 Windows 및 macOS를 실행 중인 기기에서만 사용 가능합니다.

네트워크 설정이 변경되는 경우 중앙 관리 서버 간에 네트워크 에이전트를 전환하는 규칙을 만들려면 다음과 같이 하십시오:

1. 관리 중인 기기 그룹에 대한 규칙을 생성하려면 이 그룹의 네트워크 에이전트 정책을 엽니다. 이를 위해 다음 작업을 수행합니다.
   a. 메인 메뉴에서 **에셋(기기)** → **정책 및 프로필**이동합니다.
   b. 현재 경로 링크를 누릅니다.
   c. 열리는 창에서 필요한 관리 그룹을 선택합니다.
      이후에 현재 경로가 변경됩니다.
   d. 관리 중인 기기 그룹에 대한 네트워크 에이전트 정책을 추가합니다. 이미 만든 경우 네트워크 에이전트 정책 이름을 눌러 정책 속성을 엽니다.
2. 특정 관리 대상 기기에 대한 규칙을 생성하려면 다음을 수행합니다.
   a. 메인 메뉴에서 **에셋(기기)** → **관리 중인 기기**로 이동합니다.
   b. 관리 중인 기기의 이름을 누릅니다.

c. 관리 중인 기기 속성 창이 열리면 **애플리케이션** 탭을 누릅니다.

d. 선택한 관리 중인 기기에만 적용되는 네트워크 에이전트 정책의 이름을 누릅니다.

3. 열리는 속성 창에서 **애플리케이션 설정 → 연결성 → 연결 프로필로 이동합니다.**

4. **네트워크 위치 설정** 섹션에서 **추가** 버튼을 클릭합니다.

5. 속성 창이 열리면 네트워크 위치 설명 및 전환 규칙을 구성합니다. 다음과 같은 네트워크 위치 설명 설정을 지정합니다:

- **설명**

  네트워크 위치 설명의 이름은 255자를 초과할 수 없으며 ("*<>?\/:|).

- **연결 프로필 사용**

  드롭다운 목록에서 네트워크 에이전트가 중앙 관리 서버에 연결하는 데 사용하는 연결 프로필을 지정할 수 있습니다. 네트워크 위치 설명 조건을 충족하면 이 프로필이 사용됩니다. 연결 프로필은 네트워크 에이전트의 중앙 관리 서버 연결을 위한 설정을 포함하며, 클라이언트 기기가 이동 사용자 정책으로 전환해야 하는 시기도 정의합니다. 이 정책은 업데이트를 다운로드하는 데에만 사용됩니다.

- **설명 사용**

  새 네트워크 위치 설명을 사용하려면 이 확인란을 선택합니다.

6. 네트워크 에이전트 전환 규칙에 대한 다음 조건을 선택합니다.

- **DHCP 서버 주소 조건** – 네트워크 DHCP(Dynamic Host Configuration Protocol) 서버의 IP 주소가 변경된 경우.
- **기본 연결 게이트웨이 주소 조건** –기본 네트워크 게이트웨이의 주소가 변경된 경우.
- **DNS 도메인 조건** - 서브넷의 DNS 접미사가 변경된 경우.
- **DNS 서버 주소 조건** –네트워크 DNS 서버의 IP 주소가 변경된 경우.
- **WINS 서버 주소 조건** –네트워크 WINS 서버의 IP 주소가 변경된 경우. 이 설정은 Windows를 실행하는 기기에서만 사용할 수 있습니다.
- **이름 해석 가능성 조건**-클라이언트 기기의 DNS 또는 NetBIOS 이름이 변경되었습니다.
- **서브넷 조건** –서브넷 주소 및 마스크를 변경합니다.
- **Windows 도메인 접근 가능성 조건**– 클라이언트 기기가 연결된 Windows 도메인의 상태를 변경합니다. 이 설정은 Windows를 실행하는 기기에서만 사용할 수 있습니다.
- **SSL 연결 주소 접근 가능성 조건**-클라이언트 기기는 지정한 서버(이름:포트)와 SSL 연결을 설정할 수 있거나 설정할 수 없습니다(선택한 옵션에 따라 다름). 각 서버에 대해 SSL 인증서를 추가로 지정할 수 있습니다. 이 경우 네트워크 에이전트는 SSL 연결 기능은 물론 서버 인증서를 확인합니다. 인증서가 일치하지 않으면 연결이 실패합니다.

한 규칙의 조건은 논리 연산자 AND를 사용하여 결합됩니다. 네트워크 위치 설명에 따라 전환 규칙을 활성화하려면 모든 규칙 전환 조건이 충족되어야 합니다.

7. 조건 섹션에서 네트워크 에이전트를 다른 중앙 관리 서버로 전환해야 하는 시기를 지정합니다. 이를 위해 **추가** 버튼을 누른 후 조건 값을 설정합니다.

   또한 **위 목록의 값 중 하나 이상과 일치하는 경우** 옵션은 기본적으로 활성화되어 있습니다. 지정된 모든 값으로 조건을 충족하기 위해 이 옵션을 비활성화할 수 있습니다.

8. 변경 사항을 저장합니다.

네트워크 위치 설명에 의해 새 전환 규칙이 만들어지고, 조건이 충족될 때마다 네트워크 에이전트에서 규칙에 지정된 연결 프로필을 사용하여 중앙 관리 서버에 연결합니다.

보호 배포 마법사

Kaspersky 애플리케이션을 설치하려면 보호 배포 마법사를 사용할 수 있습니다. 보호 배포 마법사에서는 미리 만든 설치 패키지를 통해 또는 배포 패키지에서 직접 애플리케이션을 원격 설치할 수 있습니다.

보호 배포 마법사는 다음 작업을 수행합니다:

- 애플리케이션 설치를 위한 설치 패키지를 다운로드합니다(아직 만들지 않은 경우). 설치 패키지는 다음 위치에 있습니다. **발견 및 배포 → 배포 및 할당 → 설치 패키지** 이 설치 패키지를 사용하여 나중에 애플리케이션을 설치할 수 있습니다.
- 특정 기기 또는 관리 그룹에 대한 원격 설치 작업을 만들고 시작합니다. 새로 생성된 원격 설치 작업은 **작업** 섹션에 저장됩니다. 나중에 이 작업을 직접 시작할 수 있습니다. 작업 유형은 다음과 같습니다. **원격으로 애플리케이션 설치**.

SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면 insserv-compat 패키지를 먼저 설치 해서 네트워크 에이전트를 구성합니다.

1단계. 보호 배포 마법사 시작

보호 배포 마법사를 수동으로 시작하려면,

메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 보호 배포 마법사**를 누릅니다.

보호 배포 마법사 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

2단계. 설치 패키지 선택

설치하려는 애플리케이션의 설치 패키지를 선택합니다.

필요한 애플리케이션의 설치 패키지가 목록에 없으면 **추가** 버튼을 누른 다음 목록에서 애플리케이션을 선택합니다.

3단계. 키 파일 또는 활성화 코드 배포 방법 선택

키 파일 또는 활성화코드 배포 방법을 선택합니다.

- **설치 패키지에 라이센스 키 추가 안 함**

  키가 호환되는 모든 기기에 자동으로 배포됩니다:
  - 키 속성에서 자동 배포가 켜 있을 경우.
  - **키 추가** 작업이 생성된 경우.

- **설치 패키지에 라이센스 키 추가**

  키가 설치 패키지와 함께 기기에 배포됩니다.

  설치 패키지 저장소에 대한 읽기 권한은 공유되므로 이 방법을 사용하여 키를 배포하는 것은 권장하지 않습니다.

설치 패키지에 키 파일이나 활성화 코드가 이미 포함되어 있으면 이 창이 표시되기는 하지만 창에는 라이센스 키 정보만 표시됩니다.

4단계. 네트워크 에이전트 버전 선택

네트워크 에이전트가 아닌 애플리케이션의 설치 패키지를 선택한 경우 애플리케이션을 Kaspersky Security Center 중앙 관리 서버와 연결하는 네트워크 에이전트도 설치해야 합니다.

최신 버전의 네트워크 에이전트를 선택합니다.

5단계. 기기 선택

애플리케이션을 설치할 기기의 목록을 지정합니다.

- **관리 중인 기기에 설치**

  이 옵션을 선택하면 기기 그룹에 대해 원격 설치 작업이 만들어집니다.

- **설치할 기기 선택**

  기기 조회에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

6단계. 원격 설치 작업 설정 지정

원격 설치 작업 설정 페이지에서 애플리케이션의 원격 설치에 대한 설정을 지정합니다.

강제 설치 패키지 다운로드 설정 그룹에서 애플리케이션 설치에 필요한 파일이 클라이언트 기기에 배포되는 방식을 지정합니다:

- **네트워크 에이전트 이용**

  이 옵션을 활성화하면 이들 클라이언트 기기에 설치된 네트워크 에이전트에 의해 클라이언트 기기로 설치 패키지가 전송됩니다.

  이 옵션을 비활성화하면 클라이언트 기기의 운영 체제 도구를 사용해 설치 패키지를 전송합니다.

  네트워크 에이전트가 설치된 기기에 작업이 할당된 경우 옵션을 활성화하는 것이 좋습니다.

  기본적으로 이 옵션은 켜져 있습니다.

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

  이 옵션을 활성화하면 배포 지점을 통해 운영 체제 도구를 사용하여 클라이언트 기기로 설치 패키지가 전송됩니다. 네트워크에 하나 이상의 배포 지점이 있어야 이 옵션을 선택할 수 있습니다.

  네트워크 에이전트 이용 옵션이 활성화된 경우 네트워크 에이전트 도구를 사용할 수 없는 경우에만 운영 체제 도구를 사용하여 파일을 전송합니다.

  이 옵션은 기본적으로 가상 중앙 관리 서버에서 만들어진 원격 설치 작업에 대해 활성화됩니다.

  > 기기에 할당된 모든 배포 지점에 문제가 발생하면 기기는 업데이트(안티 바이러스 데이터베이스 및 패치)와 설치 패키지를 수신하지 않습니다.

- **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드**

  이 옵션을 사용하면 중앙 관리 서버를 통해 클라이언트 기기의 운영 체제 도구를 사용하여 파일을 클라이언트 기기로 전송합니다. 이 옵션은 클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않아도 활성화할 수 있지만, 이 경우 클라이언트 기기는 중앙 관리 서버와 같은 네트워크에 있어야 합니다.

  기본적으로 이 옵션은 켜져 있습니다.

추가 설정을 지정합니다:

- **이미 설치한 애플리케이션은 설치하지 않음**

  이 옵션을 활성화하면 선택한 애플리케이션이 이 클라이언트 기기에 이미 설치된 경우 다시 설치되지 않습니다.

  이 옵션을 비활성화해도 애플리케이션이 설치됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **Active Directory 그룹 정책에 패키지 설치 지정**

  이 옵션을 활성화하면 Active Directory 그룹 정책을 통해 설치 패키지가 설치됩니다.
  이 옵션은 네트워크 에이전트 설치 패키지가 선택되어 있는 경우에 사용할 수 있습니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

7단계. 관리 다시 시작

애플리케이션을 설치할 때 운영 체제를 다시 설치해야 하는 경우 수행할 작업을 지정합니다.

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.
  기본적으로 이 옵션은 선택되어 있습니다.

  - **반복해서 물어보기(분)**

    이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.
    기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.
    이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

  - **다음 시간 이후에 재시작(분)**

    사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.
    기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

8단계. 설치하기 전에 비-호환 애플리케이션 제거

배포하는 애플리케이션이 다른 일부 애플리케이션과 호환되지 않는 것으로 확인된 경우에만 이 단계가 표시됩니다.

배포하는 애플리케이션과 호환되지 않는 애플리케이션을 Kaspersky Security Center에서 자동으로 제거하도록 하려면 이 옵션을 선택합니다.

호환되지 않는 애플리케이션 목록도 표시됩니다.

이 옵션을 선택하지 않으면 호환되지 않는 애플리케이션이 없는 기기에만 애플리케이션이 설치됩니다.

9단계. 관리 중인 기기로 기기 이동

네트워크 에이전트 설치가 끝난 기기가 이동될 관리 그룹을 지정합니다.

- **기기를 이동하지 않음**

  기기가 현재 포함되어 있는 그룹에 유지됩니다. 그룹에 배치되지 않은 기기는 미할당 상태로 유지됩니다.

- **미할당 기기를 그룹으로 이동**

  기기가 선택한 관리 그룹으로 이동됩니다.

기기를 이동하지 않음 옵션은 기본적으로 선택되어 있습니다. 보안상의 이유로 기기를 수동으로 이동해야 할 수 있습니다.

10단계. 기기에 접근할 수 있는 계정 선택

필요한 경우 원격 설치 작업을 시작하는 데 사용할 계정을 추가합니다.

- **계정 필요 없음(네트워크 에이전트가 설치되어 있음)**

  이 옵션을 선택하면 애플리케이션 설치 프로그램을 실행할 계정을 지정하지 않아도 됩니다. 중앙 관리 서버가 실행 중인 계정에서 작업이 실행됩니다.

  클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않다면, 이 옵션은 이용할 수 없습니다.

- **계정 필요(네트워크 에이전트는 사용되지 않음)**

  원격 설치 작업을 할당한 기기에 네트워크 에이전트가 설치되어 있지 않다면 이 옵션을 선택하십시오. 이 때, 사용자 계정 또는 SSH 인증서를 지정하여 애플리케이션을 설치할 수 있습니다.

  - **로컬 계정**. 이 옵션을 선택했다면 애플리케이션 설치 프로그램을 실행할 계정을 지정합니다. **추가** 버튼을 클릭하고 **로컬 계정**을 선택한 다음 사용자 계정 자격 증명을 지정합니다.

    예를 들어 이 작업이 할당된 모든 기기에 필요한 모든 권한이 어떤 계정에도 없다면, 사용자 계정을 여러 개 지정할 수 있습니다. 이때, 작업 실행 시 추가한 모든 계정을 위에서부터 순서대로 사용합니다.

  - **SSH 인증서**. Linux 기반 클라이언트 기기에 애플리케이션을 설치한다면 사용자 계정 대신 SSH 인증서를 지정할 수 있습니다. **추가** 버튼을 클릭하고 **SSH 인증서**를 선택한 다음 인증서의 개인 및 공개 키를 지정합니다.

    개인 키를 생성하려면 ssh-keygen 유틸리티를 사용할 수 있습니다. Kaspersky Security Center는 개인 키의 PEM 형식을 지원하지만 ssh-keygen 유틸리티는 기본적으로 OPENSSH 형식으로 SSH 키를 생성합니다. Kaspersky Security Center에서는 OPENSSH 형식을 지원하지 않습니다. 지원되는 PEM 형식으로 개인 키를 생성하려면 ssh-keygen 명령에 -m PEM 옵션을 추가합니다. 예:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< 사용자 이메일 >"
    ```

11단계. 설치 시작

이 페이지가 마법사의 마지막 단계입니다. 이 단계에서는 **원격 설치 작업**이 정상적으로 생성되어 구성되었습니다.

마법사 종료 후 작업 실행 옵션은 기본으로 선택되어 있습니다. 이 옵션을 선택하면 마법사를 완료한 직후에 **원격 설치 작업**이 시작됩니다. 이 옵션을 선택하지 않으면 **원격 설치 작업**이 시작되지 않습니다. 나중에 이 작업을 직접 시작할 수 있습니다.

확인을 클릭하여 보호 배포 마법사의 마지막 단계를 완료합니다.

Kaspersky Security Center 웹 콘솔을 통한 Kaspersky 애플리케이션 배포

이 섹션에서는 Kaspersky Security Center 웹 콘솔을 통해 조직의 클라이언트 기기에 Kaspersky 애플리케이션을 배포하는 방법에 대해 설명합니다.

시나리오: Kaspersky Security Center 웹 콘솔을 통한 Kaspersky 애플리케이션 배포

이 시나리오는 Kaspersky Security Center 웹 콘솔을 통해 Kaspersky 애플리케이션을 배포하는 방법을 설명합니다. 빠른 시작 마법사 및 보호 배포 마법사를 사용하거나 필요한 모든 단계를 수동으로 완료할 수도 있습니다.

Kaspersky Security Center 웹 콘솔을 사용하여 배포할 수 있는 애플리케이션은 다음과 같습니다:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

단계

Kaspersky 애플리케이션 배포는 다음 단계로 진행됩니다.

1. **애플리케이션용 관리 플러그인 다운로드**

   이 단계는 빠른 시작 마법사에서 처리됩니다. 마법사를 실행하지 않으려는 경우 Kaspersky Endpoint Security for Windows용 플러그인을 수동으로 다운로드합니다.

   회사 모바일 기기를 관리할 계획이라면 Kaspersky Security for Mobile 도움말의 지침에 따라 Kaspersky Endpoint Security for Android용 관리 플러그인을 다운로드하여 설치하십시오.

2. **설치 패키지 다운로드 및 생성**

   이 단계는 빠른 시작 마법사에서 처리됩니다.

   빠른 시작 마법사에서는 관리 플러그인과 함께 설치 패키지를 다운로드할 수 있습니다. 마법사를 실행할 때 이 옵션을 선택하지 않았거나 마법사 자체를 실행하지 않았다면, 패키지를 수동으로 다운로드해야 합니다.

   일부 기기(예: 원격 직원의 기기)에 Kaspersky Security Center를 통해 Kaspersky 애플리케이션을 설치할 수 없는 경우 애플리케이션에 대한 독립 실행형 설치 패키지를 생성할 수 없습니다. 독립 실행형 패키지를 사용하여 Kaspersky 애플리케이션을 설치하는 경우 원격 설치 작업을 생성 및 실행할 필요가 없으며 Kaspersky Endpoint Security for Windows를 위한 작업을 생성 및 구성할 필요도 없습니다.

3. **원격 설치 작업 생성, 구성 및 실행**

   Kaspersky Endpoint Security for Windows에서, 이 단계는 빠른 시작 마법사가 완료되고 나면 자동 시작되는 보호 배포 마법사의 일부분입니다. 보호 배포 마법사를 실행하지 않으려면, 이 작업을 수동으로 생성한 다음 수동으로 구성해야 합니다.

   서로 다른 관리 그룹이나 기기 조회용으로 여러 원격 설치 작업을 수동으로 생성할 수도 있습니다. 이러한 작업에서 한 애플리케이션의 다른 버전을 배포할 수 있습니다.

   네트워크의 모든 기기가 발견되었는지 확인한 후 원격 설치 작업(여러 작업 가능)을 실행합니다.

Linux 기반 에셋에 nmap 유틸리티를 설치합니다. 이 유틸리티는 네트워크 위치 인식 기능을 활성화하는 데 필요합니다.

SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면 insserv-compat 패키지를 먼저 설치 해서 네트워크 에이전트를 구성합니다.

운영 체제 RED OS 7.3.4 이상이나 MSVSPHERE 9.2 이상을 사용하는 기기에 네트워크 에이전트를 설치한다면, 중앙 관리 서버가 올바르게 작동하려면 libxcrypt-compat 패키지를 설치해야 합니다.

4. **관리 중인 애플리케이션에 대한 작업 생성 및 구성**

   Kaspersky Endpoint Security for Windows의 *업데이트 설치 작업*을 구성해야 합니다.

   이 단계는 빠른 시작 마법사의 일부분이며, 작업은 기본 설정을 사용하여 자동 생성 및 구성됩니다. 마법사를 실행하지 않았다면, 이러한 작업을 수동으로 생성한 다음 구성해야 합니다. 빠른 시작 마법사를 사용한다면 작업을 위한 스케줄이 요구 사항을 충족하는지 확인합니다(기본적으로 작업의 시작 스케줄은 **수동**으로 설정되지만 다른 옵션을 선택할 수도 있습니다).

   기본 작업은 Kaspersky 애플리케이션마다 다를 수 있습니다. 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.

   생성하는 각 작업의 스케줄이 요구 사항을 충족하는지 확인합니다.

5. **Kaspersky Security for Mobile 설치 (선택 사항)**

   회사 모바일 기기를 관리할 계획이라면 Kaspersky Security for Mobile 도움말의 지침에 따라 Kaspersky Endpoint Security for Android 배포에 대한 정보를 참조하십시오.

6. **정책 만들기**

   각 애플리케이션에 대한 정책을 수동으로, 또는 (Kaspersky Endpoint Security for Windows에서는) 빠른 시작 마법사를 통해 생성합니다. 정책의 기본 설정을 사용할 수 있으며, 언제든지 필요에 따라 정책의 기본 설정을 수정할 수도 있습니다.

7. **결과 확인**

   배포가 성공적으로 완료되었는지 확인합니다. 각 애플리케이션에 대한 정책 및 작업이 있으며, 이러한 애플리케이션은 관리 중인 기기에 설치됩니다.

결과

시나리오를 완료하면 다음과 같은 결과를 얻을 수 있습니다:

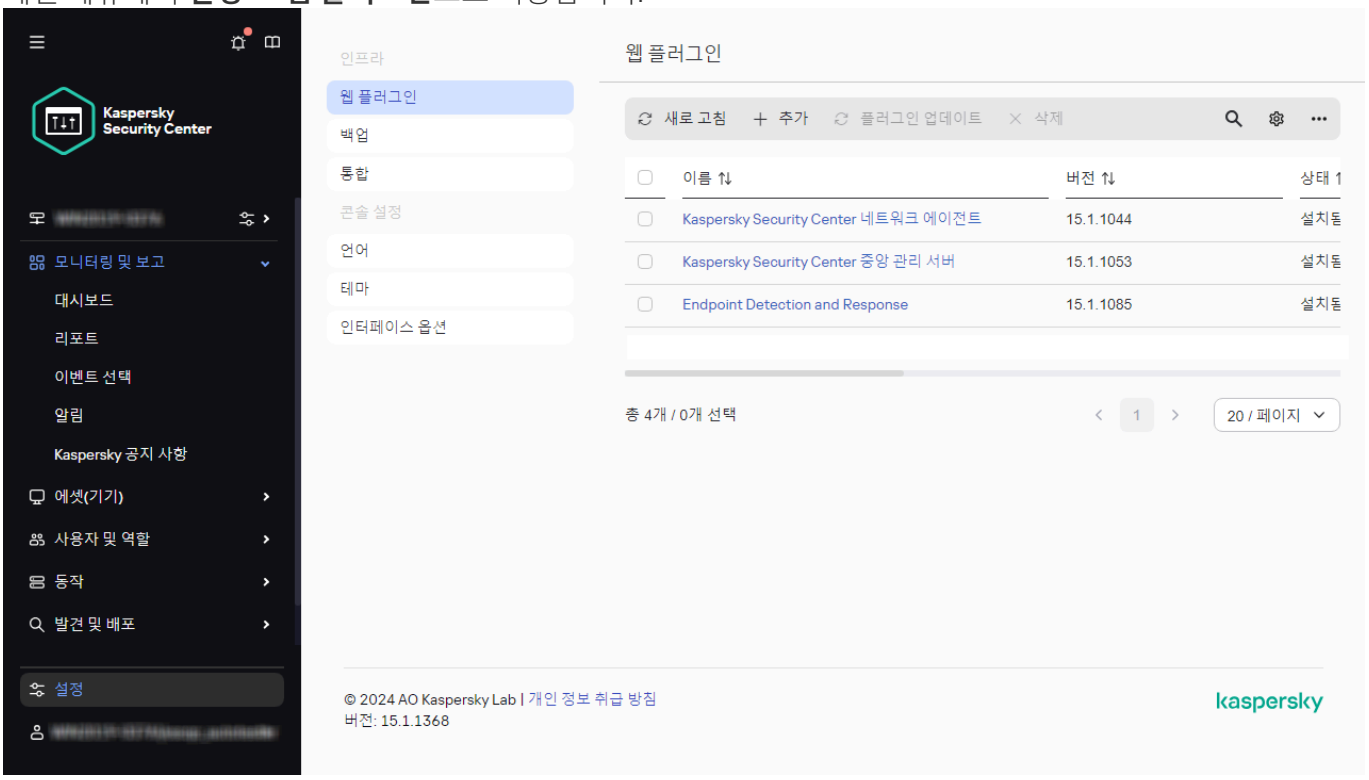
- 선택한 애플리케이션에 필요한 모든 정책 및 작업이 생성됩니다.
- 작업 스케줄은 필요에 따라 구성됩니다.
- 선택한 클라이언트 기기에 선택한 응용 프로그램이 배포되거나 배포 스케줄이 설정됩니다.

Kaspersky 애플리케이션용 플러그인 받기

Kaspersky Endpoint Security for Windows와 같은 Kaspersky 애플리케이션을 배포하려면 애플리케이션용 관리 플러그인을 다운로드해야 합니다.

Kaspersky 애플리케이션용 관리 플러그인을 다운로드하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **설정** → **웹 플러그인**으로 이동합니다.



설치된 웹 플러그인 목록

2. 창이 열리면 **추가**를 누릅니다.
   사용 가능한 플러그인 목록이 표시됩니다.

3. 사용 가능한 플러그인 목록에서 다운로드할 플러그인(예: Kaspersky Endpoint Security 11 for Windows) 이름을 눌러 해당 플러그인을 선택합니다.
   플러그인 설명 페이지가 표시됩니다.

4. 플러그인 설명 페이지에서 **플러그인 설치**를 누릅니다.

5. 설치가 완료되면 **확인**를 누릅니다.

관리 플러그인이 기본 구성으로 다운로드되어 관리 플러그인 목록에 표시됩니다.

플러그인을 추가하고 파일에서 다운로드한 플러그인을 업데이트할 수 있습니다. 관리 플러그인 및 웹 관리 플러그인을 Kaspersky 기술 지원 웹페이지에서 다운로드합니다.

파일에서 플러그인을 다운로드하거나 업데이트하려면 다음을 수행하십시오.

1. 메인 메뉴에서 **설정** → **웹 플러그인**으로 이동합니다.

2. 다음 중 하나를 수행합니다:

   - 파일에서 플러그인을 다운로드하려면 **파일에서 추가**를 클릭합니다.
   - 파일에서 플러그인 업데이트를 다운로드하려면 **파일에서 업데이트**를 클릭합니다.

3. 파일 및 파일 서명을 지정합니다.

4. 지정된 파일을 다운로드합니다.

관리 플러그인이 파일에서 다운로드되어 관리 플러그인 목록에 표시됩니다.

Kaspersky 애플리케이션용 설치 패키지 다운로드 및 생성

중앙 관리 서버가 인터넷에 접근할 수 있는 경우 Kaspersky 웹 서버에서 Kaspersky 애플리케이션용 설치 패키지를 생성할 수 있습니다.

Kaspersky 애플리케이션용 설치 패키지를 다운로드하고 생성하려면

1. 다음 중 하나를 수행합니다:

   - 메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동합니다.
   - 메인 메뉴에서 **동작 → 저장소 → 설치 패키지**로 이동합니다.

   화면 알림 목록에서 새로운 Kaspersky 애플리케이션용 패키지에 대한 알림을 확인할 수도 있습니다. 새 패키지에 대한 알림이 있는 경우 알림 옆에 있는 링크를 누르고 사용 가능한 설치 패키지 목록으로 이동할 수 있습니다.

   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.

2. **추가**를 누릅니다.

   새 패키지 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

3. **Kaspersky 애플리케이션에 대한 설치 패키지 생성**을 선택합니다.

   Kaspersky 웹 서버에서 사용 가능한 설치 패키지 목록이 표시됩니다. 목록에는 현재 버전의 Kaspersky Security Center와 호환되는 애플리케이션에 대한 설치 패키지만 포함됩니다.

4. Kaspersky Endpoint Security for Windows(11.1.0)와 같은 설치 패키지의 이름을 누릅니다.

   설치 패키지 관련 정보가 포함된 창이 열립니다.

   > 해당 법률 및 규정을 준수한다면 강력한 암호화를 구현하는 암호화 도구가 포함된 설치 패키지를 다운로드하여 사용할 수 있습니다. 조직의 요구에 적합한 Kaspersky Endpoint Security for Windows의 설치 패키지를 다운로드하려면 조직의 클라이언트 기기가 있는 국가의 법률을 참조하십시오.

5. 정보를 확인하고 **다운로드하고 설치 패키지 생성** 버튼을 누릅니다.

   배포 패키지를 설치 패키지로 변환할 수 없는 경우 **다운로드하고 설치 패키지 생성** 대신 **배포 패키지 다운로드** 버튼이 표시됩니다.

   설치 패키지가 중앙 관리 서버로 다운로드됩니다. 마법사의 창을 닫거나 지침의 다음 단계를 진행할 수 있습니다. 마법사 창을 닫으면 다운로드 프로세스가 백그라운드 모드에서 계속됩니다.

   설치 패키지 다운로드 프로세스를 추적하려면 다음 단계를 따릅니다.

   a. 메인 메뉴에서 **동작 → 저장소 → 설치 패키지 → 진행 중()**으로 이동합니다.

   b. 표의 **다운로드 진행** 열 및 **다운로드 상태** 열에서 작업 진행 상황을 추적합니다.

프로세스가 완료되면 설치 패키지가 **다운로드됨** 탭의 목록에 추가됩니다. 다운로드 프로세스가 중지되고 다운로드 상태가 **EULA 수락**으로 전환되면 설치 패키지 이름을 누르고 지침의 다음 단계를 진행합니다.

선택한 배포 패키지에 포함된 데이터 크기가 현재 제한을 초과하면 오류 메시지가 표시됩니다. 제한 값을 변경한 다음 설치 패키지 생성을 진행할 수 있습니다.

6. 일부 Kaspersky 애플리케이션의 경우 다운로드 프로세스 중에 **EULA 표시** 버튼이 표시됩니다. 이 버튼이 표시되면 다음을 수행합니다.

   a. **EULA 표시** 버튼을 눌러 EULA(최종 사용자 라이센스 계약서)를 확인합니다.

   b. 화면에 표시된 EULA를 읽고 **수락**를 누릅니다.

   EULA에 동의하면 다운로드가 계속 진행됩니다. **거부**를 누르면 다운로드가 중지됩니다.

7. 다운로드가 완료되면 **닫기** 버튼을 누릅니다.

선택한 설치 패키지가 중앙 관리 서버 공유 폴더의 패키지 하위 폴더로 다운로드됩니다. 다운로드 후에 설치 패키지가 설치 패키지 목록에 표시됩니다.

사용자 지정 설치 패키지 데이터의 크기 제한 변경

사용자 지정 설치 패키지를 만드는 동안에는 압축을 푼 데이터의 총 크기가 제한됩니다. 기본 제한은 1 GB입니다.

현재 제한을 초과하는 데이터가 포함된 압축 파일을 업로드하려고 하면 오류 메시지가 표시됩니다. 대용량 배포 패키지에서 설치 패키지를 만들 때는 이 제한 값을 늘려야 할 수 있습니다.

사용자 지정 설치 패키지 크기의 제한 값을 변경하려면 다음 단계를 따릅니다.

1. 중앙 관리 서버 기기에서 중앙 관리 서버 설치에 사용된 계정으로 명령 프롬프트를 실행합니다.

2. 현재 디렉터리를 Kaspersky Security Center 설치 폴더(일반적으로 <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center)로 변경합니다.

3. 관리 서버 설치 유형에 따라 관리자 권한을 사용하여 다음 명령 중 하나를 입력합니다:

   - 일반 로컬 설치:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <바이트 수>
     ```

   - Kaspersky Security Center 장애 조치 클러스터에 설치:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <바이트 수> --stp klfoc
     ```

   - Windows Server 장애 조치 클러스터에 설치:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <바이트 수> --stp cluster
     ```

   여기서 <바이트 수>는 16진수 또는 10진수 형식의 바이트 수입니다.

   예를 들어, 필요한 제한이 2GB인 경우 진수 값 2147483648 또는 진수 값 0x80000000을 지정할 수 있습니다. 이 때, 중앙 관리 서버의 로컬 설치를 위해 다음 명령을 사용할 수 있습니다:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

사용자 지정 설치 패키지 데이터의 크기 제한이 변경되었습니다.

Kaspersky 애플리케이션용 배포 패키지 다운로드

Kaspersky Security Center 웹 콘솔에서 Kaspersky 애플리케이션용 배포 패키지를 다운로드하고 저장할 수 있습니다. Kaspersky Security Center를 사용하지 않고 배포 패키지를 사용하여 애플리케이션을 수동으로 설치할 수 있습니다.

Kaspersky 애플리케이션용 배포 패키지를 다운로드하고 저장하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → Kaspersky 애플리케이션 → 현재 애플리케이션 버전**으로 이동합니다.

   사용 가능한 배포 패키지, 플러그인 및 패치 목록이 열립니다. Kaspersky Security Center는 현재 버전과 호환되는 항목만 표시합니다.

2. 목록에서 다운로드할 패키지 이름을 누릅니다.

   패키지에 대한 설명이 열립니다.

3. 설명을 읽고 **다운로드하고 설치 패키지 생성** 버튼을 누릅니다.

   배포 패키지를 설치 패키지로 변환할 수 없는 경우 **다운로드하고 설치 패키지 생성** 대신 **배포 패키지 다운로드** 버튼이 표시됩니다.

   설치 패키지가 중앙 관리 서버로 다운로드됩니다.

선택한 설치 또는 배포 패키지가 중앙 관리 서버 공유 폴더의 **패키지** 하위 폴더로 다운로드됩니다. 다운로드 후에 설치 패키지가 설치 패키지 목록에 표시됩니다.

Kaspersky Endpoint Security가 성공적으로 배포되었는지 확인

Kaspersky Endpoint Security와 같은 Kaspersky 애플리케이션을 올바르게 배포했는지 확인하려면 다음 단계를 따릅니다.

1. Kaspersky Security Center 웹 콘솔을 사용하여 다음이 있는지 확인합니다:

   - Kaspersky Endpoint Security 및/또는 사용하는 기타 보안 제품에 대한 정책.
   - Kaspersky Endpoint Security for Windows 작업: *빠른 검사* 작업 및 *업데이트 설치* 작업(Kaspersky Endpoint Security for Windows 사용 시).
   - 사용하는 기타 보안 제품 작업.

2. 설치용으로 선택한 관리 중인 기기 중 하나에서 다음 사항을 확인합니다.

   - Kaspersky Endpoint Security 또는 다른 Kaspersky 보안 제품이 설치되어 있습니다.
   - Kaspersky Endpoint Security에서 파일 위협 보호, 웹 위협 보호 및 메일 위협 보호 설정이 해당 기기용으로 생성한 정책과 일치합니다.
   - Kaspersky Endpoint Security 서비스는 수동으로 중지하고 시작할 수 있습니다.
   - 그룹 작업은 수동으로 중지하고 시작할 수 있습니다.

독립 실행형 설치 패키지 만들기

조직의 사용자와 기기 사용자는 독립 실행형 설치 패키지를 사용하여 기기에 수동으로 애플리케이션을 설치할 수 있습니다.

독립 실행형 설치 패키지는 웹 서버 또는 공유 폴더에 저장하거나, 이메일로 보내거나, 다른 방법으로 클라이언트 기기에 전송할 수 있는 실행 파일(Installer.exe)입니다. 사용자는 클라이언트 기기에서 Kaspersky Security Center의 관여 없이 수신된 파일을 로컬로 실행하여 애플리케이션을 설치할 수 있습니다. Kaspersky 애플리케이션 및 Windows, macOS, Linux 플랫폼을 위한 타사 애플리케이션의 독립 실행형 설치 패키지를 생성할 수 있습니다. 타사 애플리케이션에 대한 독립 실행형 설치 패키지를 생성하려면 사용자 지정 설치 패키지를 생성해야 합니다.

허가 받지 않은 사람은 독립 실행형 설치 패키지를 사용할 수 없도록 하십시오.

독립 실행형 설치 패키지를 만들려면 다음과 같이 하십시오:

1. 다음 중 하나를 수행합니다:

   - 메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동합니다.
   - 메인 메뉴에서 **동작 → 저장소 → 설치 패키지**로 이동합니다.

   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.

2. 설치 패키지 목록에서 설치 패키지를 선택하고 목록 위에서 **배포** 버튼을 누릅니다.

3. **독립 실행형 패키지 사용** 옵션을 선택합니다.

   독립 실행형 설치 패키지 만들기 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

4. 설치된 애플리케이션과 네트워크 에이전트를 함께 설치하려면 **이 애플리케이션과 함께 네트워크 에이전트 설치** 옵션이 활성화되어 있는지 확인합니다.

   독립 실행형 설치 패키지를 생성하는 애플리케이션에 따라 옵션이 표시됩니다.

   기본적으로 이 옵션은 켜져 있습니다. 기기의 네트워크 에이전트 설치 여부가 확실하지 않은 경우 이 옵션을 활성화하는 것이 좋습니다. 기기에 네트워크 에이전트가 이미 설치되어 있는 경우 네트워크 에이전트가 포함된 독립 실행형 설치 패키지를 설치하면 네트워크 에이전트가 최신 버전으로 업데이트됩니다.

   이 옵션을 비활성화하면 네트워크 에이전트가 기기에 설치되지 않고 기기가 관리되지 않습니다.

   선택한 애플리케이션에 대한 독립 실행형 설치 패키지가 중앙 관리 서버에 이미 존재한다면 마법사가 이를 알려줍니다. 이 경우 다음 작업 중 하나를 선택해야 합니다:

   - **독립 실행형 설치 패키지 생성**. 예를 들어, 새 애플리케이션 버전에 대한 독립 실행형 설치 패키지를 만들고자 하면서 이전 애플리케이션 버전에 대해 만든 독립 실행형 설치 패키지는 유지하려는 경우 이 옵션을 선택하십시오. 새로운 독립 실행형 설치 패키지는 다른 폴더에 있습니다.
   - **기존 독립 실행형 설치 패키지 사용**. 기존 독립 실행형 설치 패키지를 사용하려면 이 옵션을 선택합니다. 패키지 생성 프로세스가 시작되지 않습니다.
   - **기존의 독립 실행형 설치 패키지 다시 생성**. 동일한 애플리케이션에 대한 독립 실행형 설치 패키지를 다시 만들려면 이 옵션을 선택합니다. 독립 실행형 설치 패키지는 동일한 폴더에 있습니다.

5. **관리 중인 기기 목록으로 이동** 단계에는 **기기를 이동하지 않음** 옵션이 기본적으로 활성화되어 있습니다. 네트워크 에이전트 설치 후 클라이언트 기기를 관리 그룹으로 이동하지 않으려면 이 옵션을 선택한 상태 그대로 두십시오.

   네트워크 에이전트 설치 후 클라이언트 기기를 이동하려면 **미할당 기기를 이 관리 그룹으로 이동** 옵션을 선택하고 클라이언트 기기를 이동하려는 관리 그룹을 지정합니다. 기본적으로 기기는 **관리 중인 기기** 그룹으로 이동합니다.

6. 독립 실행형 설치 패키지 생성 프로세스가 완료되면, **완료** 버튼을 클릭합니다.

   Stand-alone Installation Package Creation Wizard가 닫힙니다.

독립 실행형 설치 패키지가 만들어지고 중앙 관리 서버 공유 폴더의 PkgInst 하위 폴더에 배치됩니다. 설치 패키지 목록 위에 있는 **독립 실행형 패키지 목록 보기** 버튼을 눌러 독립 실행형 패키지의 목록을 볼 수 있습니다.

독립 실행형 설치 패키지 목록 보기

독립 실행형 설치 패키지 목록과 각 독립 실행형 설치 패키지의 속성을 확인할 수 있습니다.

모든 설치 패키지의 독립 실행형 설치 패키지 목록을 보려면 다음 단계를 따릅니다.

목록 위에서 **독립 실행형 패키지 목록 보기** 버튼을 누릅니다.

독립 실행형 설치 패키지 목록에 다음과 같은 속성이 표시됩니다:

- **패키지 이름**. 패키지에 포함된 애플리케이션 이름과 애플리케이션 버전으로 자동 구성되는 독립 실행형 설치 패키지 이름입니다.
- **애플리케이션 이름**. 독립 실행형 설치 패키지에 포함된 애플리케이션 이름입니다.
- **애플리케이션 버전**.
- **네트워크 에이전트 설치 패키지 이름**. 이 속성은 네트워크 에이전트가 독립 실행형 설치 패키지에 포함된 경우에만 표시됩니다.
- **네트워크 에이전트 버전**. 이 속성은 네트워크 에이전트가 독립 실행형 설치 패키지에 포함된 경우에만 표시됩니다.
- **크기**. 파일 크기(MB)입니다.
- **그룹**. 네트워크 에이전트 설치 후 클라이언트 기기가 이동되는 그룹의 이름입니다.
- **만든 날짜**. 독립 실행형 설치 패키지 생성 날짜 및 시간입니다.
- **수정됨**. 독립 실행형 설치 패키지 수정 날짜 및 시간입니다.
- **경로**. 독립 실행형 설치 패키지가 위치한 폴더의 전체 경로입니다.
- **웹 주소**. 독립 실행형 설치 패키지 위치의 웹 주소입니다.
- **파일 해시**. 이 속성은 독립 실행형 설치 패키지가 제3자에 의해 변경되지 않았으며 생성 후 사용자에게 전송된 것과 동일한 파일이 사용자에게 있음을 인증하는 데 사용됩니다.

특정 설치 패키지의 독립 실행형 설치 패키지 목록을 보려면 다음 단계를 따릅니다.

목록에서 설치 패키지를 선택하고 목록 위에서 **독립 실행형 패키지 목록 보기** 버튼을 누릅니다.

독립 실행형 설치 패키지 목록에서 다음을 수행할 수 있습니다:

- **게시** 버튼을 눌러 웹 서버에서 독립 실행형 설치 패키지를 게시합니다. 게시된 독립 실행형 설치 패키지는 독립 실행형 설치 패키지 링크를 받은 사용자가 다운로드할 수 있습니다.
- **게시 취소** 버튼을 눌러 웹 서버에서 독립 실행형 설치 패키지의 게시를 취소합니다. 게시되지 않은 독립 실행형 설치 패키지는 관리자와 다른 관리자만 다운로드할 수 있습니다.
- **다운로드** 버튼을 눌러 독립 실행형 설치 패키지를 기기에 다운로드합니다.
- **이메일로 전송** 버튼을 눌러 독립 실행형 설치 패키지 링크가 포함된 이메일을 전송합니다.
- **제거** 버튼을 눌러 독립 실행형 설치 패키지를 제거합니다.

사용자 지정 설치 패키지 만들기

사용자 지정 설치 패키지를 사용하여 다음을 수행할 수 있습니다:

- 작업을 이용하는 방법 등으로 클라이언트 기기에 애플리케이션(예: 텍스트 편집기)을 설치합니다.
- 독립 실행형 설치 패키지를 만듭니다.

사용자 지정 설치 패키지는 일련의 파일이 있는 폴더입니다. 사용자 지정 설치 패키지 생성에 사용하는 소스는 *아카이브 파일*입니다. 아카이브 파일에는 사용자 지정 설치 패키지에 포함해야 하는 파일이 있습니다. 사용자 지정 설치 패키지를 만들면서 명령줄 파라미터를 지정하여 숨김 모드로 애플리케이션을 설치하는 작업 등을 수행할 수 있습니다.

VAPM(취약점 및 패치 관리) 기능에 대한 활성 라이센스 키가 있다면, 관련 사용자 지정 설치 패키지에 대한 기본 설치 설정을 전환하고 Kaspersky 전문가가 권장하는 값을 사용할 수 있습니다. 설정은 관련 실행 파일이 타사 애플리케이션의 Kaspersky 데이터베이스에 포함된 경우에만 사용자 지정 설치 패키지 생성 중에 자동으로 전환됩니다.

사용자 지정 설치 패키지를 만들려면 다음과 같이 하십시오:

1. 다음 중 하나를 수행합니다:
   - 메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동합니다.
   - 메인 메뉴에서 **동작 → 저장소 → 설치 패키지**로 이동합니다.

   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.
2. **추가**를 누릅니다.
   새 패키지 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. **파일에서 설치 패키지 생성**을 선택합니다.

4. 패키지 이름을 지정하고 **찾기** 버튼을 누릅니다.

   브라우저에서 표준 Windows **열기** 창이 열리면 파일을 선택하여 설치 패키지를 만들 수 있습니다.

5. 사용 가능한 디스크에 있는 아카이브 파일을 선택합니다.

   ZIP, CAB, TAR 또는 TAR.GZ 아카이브 파일을 업로드할 수 있습니다. SFX(자동 압축 풀림 아카이브) 파일에서는 설치 패키지를 만들 수 없습니다.

   > 패키지 설치 중 설정을 전환하려면 **마법사가 완료된 후 Kaspersky Security Center 에서 인식할 수 있는 애플리케이션에 대해 설정을 권장 값으로 전환** 확인란이 선택되어 있는지 확인하고 **다음**을 누릅니다.

   Kaspersky Security Center 중앙 관리 서버로 파일 업로드가 시작됩니다.

   > 권장 설치 설정 사용을 활성화한 경우 Kaspersky Security Center 15.1는 실행 파일이 타사 애플리케이션의 Kaspersky 데이터베이스에 포함되어 있는지 확인합니다. 확인에 성공하면 파일이 인식되었음을 알리는 알림이 표시됩니다. 설정이 전환되고 사용자 지정 설치 패키지가 생성됩니다. 추가 조치는 필요하지 않습니다. **마침** 버튼을 눌러 마법사를 닫습니다.

6. 선택한 아카이브 파일에서 추출된 파일의 목록에서 파일을 선택하고 실행 파일의 명령줄 파라미터를 지정합니다.

   명령줄 파라미터를 지정하여 설치 패키지에서 애플리케이션을 숨김 모드로 설치할 수 있습니다. 명령줄 파라미터 지정은 선택 사항입니다.

   설치 패키지 생성 프로세스가 시작됩니다.

   프로세스가 완료되면 마법사가 알려줍니다.

   설치 패키지가 만들어지지 않으면 적절한 메시지가 표시됩니다.

7. **마침** 버튼을 눌러 마법사를 닫습니다.

   생성한 설치 패키지가 중앙 관리 서버 공유 폴더의 Packages 하위 폴더로 다운로드됩니다. 다운로드 후에 설치 패키지가 설치 패키지 목록에 나타납니다.

중앙 관리 서버에서 사용 가능한 설치 패키지의 목록에서 사용자 지정 설치 패키지 이름이 있는 링크를 누르면 다음을 수행할 수 있습니다:

- 설치 패키지의 다음 속성을 봅니다:
  - **이름**. 사용자 지정 설치 패키지 이름.
  - **출처**. 애플리케이션 공급업체 이름.
  - **애플리케이션**. 사용자 지정 설치 패키지에 포함된 애플리케이션 이름.
  - **버전**. 애플리케이션 버전.
  - **언어**. 사용자 지정 설치 패키지에 포함된 애플리케이션의 언어.
  - **크기(MB)**. 설치 패키지의 크기.
  - **운영 체제**. 설치 패키지의 대상 운영 체제 유형.
  - **만든 날짜**. 설치 패키지 생성 날짜.

- **수정됨**. 설치 패키지 수정 날짜.
- **유형**. 설치 패키지의 유형.

- 패키지 이름과 명령줄 파라미터를 변경합니다. 이 기능은 Kaspersky 애플리케이션을 기반으로 만들지 않은 패키지에만 사용할 수 있습니다.

패키지 설치 설정을 사용자 지정 패키지 생성 프로세스의 권장 값으로 전환한 경우 사용자 지정 설치 패키지 속성의 **설정** 탭에 **설정** 및 **설치 절차**의 두 가지 추가 섹션이 나타날 수 있습니다.

설정 섹션에는 다음과 같이 표에 나타난 속성이 포함됩니다.

- **이름**. 이 열에는 설치 파라미터에 할당된 이름이 표시됩니다.
- **유형**. 이 열에는 설치 파라미터의 유형이 표시됩니다.
- **값**. 이 열에는 설치 파라미터에 의해 정의된 데이터의 유형이 표시됩니다(부울, 파일 경로, 숫자, 경로, 문자열).

설치 절차 섹션에는 사용자 지정 설치 패키지에 포함된 업데이트의 다음 속성을 설명하는 표가 포함됩니다.

- **이름**. 업데이트 이름입니다.
- **설명**. 업데이트에 대한 설명입니다.
- **소스**. Microsoft 또는 다른 타사 개발자가 릴리스했는지 여부를 가리키는 업데이트 소스입니다.
- **유형**. 드라이버용인지 또는 애플리케이션용인지를 가리키는 업데이트 유형입니다.
- **카테고리**. Microsoft 업데이트에 대해 표시되는 WSUS(Windows Server 업데이트 서비스) 카테고리(중요 업데이트, 정의 업데이트, 드라이버, 기능 팩, 보안 업데이트, 서비스 팩, 도구, 업데이트 롤업, 업데이트 또는 업그레이드)입니다.
- **MSRC에 따른 심각도**. MSRC(Microsoft Security Response Center)에서 정의한 업데이트의 심각도입니다.
- **심각도**. Kaspersky에서 정의한 업데이트의 심각도입니다.
- **패치 심각도(Kaspersky 애플리케이션용 패치)**. Kaspersky 애플리케이션용인 경우 패치의 심각도입니다.
- **기술 자료 문서**. 업데이트를 설명하는 기술 자료 문서의 식별자(ID)입니다.
- **보안 공지 문서**. 업데이트를 설명하는 보안 게시판의 ID입니다.
- **설치하도록 할당 안 됨**. 업데이트가 설치하도록 할당 안 됨 상태인지 여부를 표시합니다.
- **설치 대상**. 업데이트가 설치 대상 상태인지 여부를 표시합니다.
- **설치 중**. 업데이트가 설치 중 상태인지 여부를 표시합니다.
- **설치됨**. 업데이트가 설치됨 상태인지 여부를 표시합니다.
- **실패**. 업데이트가 실패 상태인지 여부를 표시합니다.
- **재부팅 필요**. 업데이트가 재시작 필요함 상태인지 여부를 표시합니다.

- **등록됨**. 업데이트가 등록된 날짜와 시간을 표시합니다.
- **대화식 모드로 설치됨**. 업데이트를 설치하는 동안 사용자와의 상호 작용이 필요한지 여부를 표시합니다.
- **철회됨**. 업데이트가 철회된 날짜와 시간을 표시합니다.
- **업데이트 승인 상태**. 업데이트 설치 승인 여부를 표시합니다.
- **리비전**. 업데이트의 현재 리비전 번호를 표시합니다.
- **업데이트 ID**. 업데이트 ID를 표시합니다.
- **애플리케이션 버전**. 애플리케이션이 업데이트될 버전 번호를 표시합니다.
- **대체됨**. 업데이트를 대체할 수 있는 다른 업데이트를 표시합니다.
- **대체 중**. 업데이트로 대체할 수 있는 다른 업데이트를 표시합니다.
- **라이센스 계약서 약관 동의 필요**. 업데이트 시 EULA(최종 사용자 라이센스 계약서) 약관에 동의해야 하는지 여부를 표시합니다.
- **공급업체**. 업데이트 공급업체의 이름을 표시합니다.
- **제품군**. 업데이트가 속한 애플리케이션 제품군의 이름을 표시합니다.
- **애플리케이션**. 업데이트가 속한 애플리케이션의 이름을 표시합니다.
- **언어**. 업데이트 현지화 언어를 표시합니다.
- **설치하도록 할당 안 됨(새 버전)**. 업데이트가 설치하도록 할당 안 됨(새 버전) 상태인지 여부를 표시합니다.
- **필수 구성 요소를 설치해야 함**. 업데이트가 필수 구성 요소 설치 필요 상태인지 여부를 표시합니다.
- **다운로드 모드**. 업데이트 다운로드 모드를 표시합니다.
- **패치**. 업데이트가 패치인지 여부를 표시합니다.
- **설치 안 됨**. 업데이트가 설치 안 됨 상태인지 여부를 표시합니다.

보조 중앙 관리 서버에 설치 패키지 배포

Kaspersky Security Center를 사용하면 Kaspersky 애플리케이션 및 타사 애플리케이션용 설치 패키지를 생성 하고 설치 패키지를 클라이언트 기기에 배포하고 패키지에서 애플리케이션을 설치할 수 있습니다. 기본 중앙 관리 서버의 로드 최적화를 위해, 보조 중앙 관리 서버에 설치 패키지를 배포할 수 있습니다. 그런 다음 보조 서버가 패키지를 클라이언트 기기로 전송하면 클라이언트 기기에서 애플리케이션의 원격 설치를 수행할 수 있습니다.

보조 중앙 관리 서버에 설치 패키지를 배포하려면:

1. 보조 중앙 관리 서버가 기본 중앙 관리 서버에 연결되어 있어야 합니다.
2. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**로 이동합니다.
   작업 목록이 표시됩니다.

3. **추가** 버튼을 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

4. **새 작업 설정** 페이지의 **애플리케이션** 드롭다운 목록에서 **Kaspersky Security Center**를 선택합니다. 그런 다음, **작업 유형** 드롭다운 목록에서 **설치 패키지 배포(동기화)**를 선택하고 작업 이름을 지정합니다.

5. **작업 범위** 페이지에서 다음 방법 중 하나로 작업이 할당된 기기를 선택합니다:

   - 특정 관리 그룹의 모든 보조 중앙 관리 서버에 대한 작업을 생성하려면, 이 그룹을 선택하고 그룹 작업을 생성합니다.
   - 특정 보조 중앙 관리 서버에 대한 작업을 생성하려면, 해당 서버를 선택하고 해당 서버에 대한 작업을 만듭니다.

6. **배포된 설치 패키지** 페이지에서, 보조 중앙 관리 서버에 복사할 설치 패키지를 선택합니다.

7. 이 계정으로 *설치 패키지 배포* 작업을 실행할 계정을 지정합니다. 사용자의 계정을 사용하며 **기본 계정** 옵션을 활성화된 상태로 둘 수 있습니다. 또는 필요한 액세스 권한이 있는 다른 계정으로 작업을 실행하도록 지정할 수 있습니다. 이를 위해 **계정 지정** 옵션을 선택한 다음 해당 계정의 자격 증명을 입력합니다.

8. **작업 생성 마침** 페이지에서, **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화하여 작업 속성 창을 열고 기본 작업 설정을 수정할 수 있습니다. 혹은 나중에 언제든지 작업 설정을 구성할 수 있습니다.

9. **마침** 버튼을 누릅니다.

   설치 패키지를 보조 중앙 관리 서버에 배포하기 위해 생성된 작업이 작업 목록에 표시됩니다.

10. 이 작업을 수동으로 실행하거나, 작업 설정에 지정한 스케줄에 따라 실행될 때까지 기다립니다.

    작업이 완료되면 선택한 설치 패키지가 지정한 보조 중앙 관리 서버로 복사됩니다.

원격 설치 작업을 사용하여 애플리케이션 설치

Kaspersky Security Center에서 원격 설치 작업을 사용해 기기에 원격으로 애플리케이션을 설치할 수 있습니다. 이런 작업은 전용 마법사를 통해 생성되어 기기에 할당됩니다. 빠르고 쉽게 작업을 할당하려면 다음 방법 중 하나로 마법사 창에서 기기(최대 1,000대 기기)를 지정합니다.

- **중앙 관리 서버가 발견한 기기 중에서 선택**. 이 경우 특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.
- **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**. 작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.
- **기기 선택 결과에 작업 할당**. 이 경우 이전에 만든 조회에 포함되는 기기에 작업이 할당됩니다. 사전 정의 조회 또는 직접 생성한 사용자 지정 조회를 지정할 수 있습니다.
- **관리 그룹에 작업 할당**. 이 경우 이전에 만든 관리 그룹에 포함된 기기 작업이 할당됩니다.

네트워크 에이전트를 설치하지 않은 클라이언트 기기에 애플리케이션 설치 시 문제 발생을 방지하려면 Kaspersky Security Center의 원격 설치 작업을 통한 강제 배포에 설명된 대로 설치를 진행해야 합니다.

애플리케이션 원격 설치

이 섹션에는 관리 그룹, 특정 IP 주소가 있는 기기, 선택한 관리 중인 기기에 애플리케이션을 원격 설치하는 방법에 대한 정보가 포함되어 있습니다.

특정 기기에 애플리케이션을 설치하려면:

1. 메인 메뉴에서 **에셋(기기) → 작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다.
3. **작업 유형** 필드에서 **원격으로 애플리케이션 설치**를 선택합니다.
4. 다음 옵션 중 하나를 선택합니다:

   - **관리 그룹에 작업 할당**

     관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

     예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

     관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

     작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

     특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

   - **기기 선택 결과에 작업 할당**

     기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

     예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

   지정된 기기에 대해 *애플리케이션 원격 설치* 작업이 생성됩니다. **관리 그룹에 작업 할당** 옵션 선택 시, 작업은 그룹 1입니다.
5. **작업 범위** 단계에서 관리 그룹, 특정 주소가 있는 기기 또는 기기 선택을 지정합니다.
   사용 가능한 설정은 이전 단계에서 선택한 옵션에 따라 다릅니다.

6. **설치 패키지** 단계에서 다음 설정을 지정합니다.

- **설치 패키지 선택** 필드에서 설치하려는 애플리케이션의 설치 패키지를 선택합니다.
- **강제 설치 패키지 다운로드** 설정 그룹에서 애플리케이션 설치에 필요한 파일이 클라이언트 기기에 배포되는 방식을 지정할 수 있습니다.
  - **네트워크 에이전트 이용**

    이 옵션을 활성화하면 이들 클라이언트 기기에 설치된 네트워크 에이전트에 의해 클라이언트 기기로 설치 패키지가 전송됩니다.

    이 옵션을 비활성화하면 클라이언트 기기의 운영 체제 도구를 사용해 설치 패키지를 전송합니다.

    네트워크 에이전트가 설치된 기기에 작업이 할당된 경우 옵션을 활성화하는 것이 좋습니다.

    기본적으로 이 옵션은 켜져 있습니다.

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

    이 옵션을 활성화하면 배포 지점을 통해 운영 체제 도구를 사용하여 클라이언트 기기로 설치 패키지가 전송됩니다. 네트워크에 하나 이상의 배포 지점이 있어야 이 옵션을 선택할 수 있습니다.

    네트워크 에이전트 이용 옵션이 활성화된 경우 네트워크 에이전트 도구를 사용할 수 없는 경우에만 운영 체제 도구를 사용하여 파일을 전송합니다.

    이 옵션은 기본적으로 가상 중앙 관리 서버에서 만들어진 원격 설치 작업에 대해 활성화됩니다.

    기기에 할당된 모든 배포 지점에 문제가 발생하면 기기는 업데이트(안티 바이러스 데이터베이스 및 패치)와 설치 패키지를 수신하지 않습니다.

  - **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드**

    이 옵션을 사용하면 중앙 관리 서버를 통해 클라이언트 기기의 운영 체제 도구를 사용하여 파일을 클라이언트 기기로 전송합니다. 이 옵션은 클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않아도 활성화할 수 있지만, 이 경우 클라이언트 기기는 중앙 관리 서버와 같은 네트워크에 있어야 합니다.

    기본적으로 이 옵션은 켜져 있습니다.

- **최대 동시 다운로드 수** 필드에서 중앙 관리 서버가 동시에 파일을 전송할 수 있는 클라이언트 기기의 최대 허용 수를 지정합니다.
- **최대 설치 시도 횟수** 필드에서 허용할 최대 설치 프로그램 실행 횟수를 지정합니다.

  매개변수에 지정한 시도 횟수를 초과하면 Kaspersky Security Center가 기기에서 설치 프로그램을 시작하지 않습니다. *애플리케이션 원격 설치* 작업을 다시 시작하려면 **최대 설치 시도 횟수** 매개변수의 값을 늘린 후 작업을 시작합니다. 또는 새 *애플리케이션 원격 설치* 작업을 생성할 수 있습니다.

- Kaspersky 애플리케이션에서 다른 애플리케이션으로 마이그레이션할 때 현재 사용하는 애플리케이션이 암호로 보호되어 있다면 **현재 Kaspersky 애플리케이션 제거에 필요한 암호** 필드에 암호를 입력합니다. 마이그레이션하는 동안 현재 사용 중인 Kaspersky 애플리케이션이 제거됩니다.

  현재 Kaspersky 애플리케이션 제거에 필요한 암호 필드는 **강제 설치 패키지 다운로드** 설정 그룹에서 **네트워크 에이전트 이용** 옵션을 선택했을 때만 사용할 수 있습니다.

애플리케이션 원격 설치 작업을 사용하여 Kaspersky Endpoint Security for Windows를 설치할 때 Kaspersky Security for Windows Server에서 Kaspersky Endpoint Security for Windows로의 마이그레이션 시나리오에서만 제거 암호를 사용할 수 있습니다. 다른 구성 요소 설치 시 제거 암호를 사용하면 설치 오류가 발생할 수 있습니다.

마이그레이션 시나리오를 성공적으로 완료하려면 다음 사전 요구 사항이 충족되는지 확인하십시오.

- Kaspersky Security Center Network Agent 14.2 for Windows 이상을 사용하고 있습니다.
- Windows를 실행하는 기기에 애플리케이션을 설치합니다.

- 추가 설정 정의:
  - **이미 설치한 애플리케이션은 설치하지 않음**

    이 옵션을 활성화하면 선택한 애플리케이션이 이 클라이언트 기기에 이미 설치된 경우 다시 설치되지 않습니다.

    이 옵션을 비활성화해도 애플리케이션이 설치됩니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **다운로드하기 전에 운영 체제 유형 확인**

    클라이언트 기기에 파일을 전송하기 전에 Kaspersky Security Center는 설치 유틸리티 설정을 클라이언트 기기의 운영 체제에 적용할 수 있는지 확인합니다. 설정을 적용할 수 없다면, Kaspersky Security Center는 파일을 전송하지 않고 애플리케이션도 설치하지 않습니다. 예를 들어, 다양한 운영 체제를 실행하는 기기가 포함된 관리 그룹의 기기에 일부 애플리케이션을 설치하려면, 관리 그룹에 설치 작업을 할당하고 이 옵션을 활성화하여 필요한 운영 체제 이외의 운영 체제를 실행하는 기기를 건너뜁니다.

    미할당 기기에 네트워크 에이전트를 원격 설치하면 Kaspersky Security Center 또는 배포 지점이 **다운로드하기 전에 운영 체제 유형 확인**에 상관없이 기기의 운영 체제 유형을 자동으로 결정합니다.

  - **Active Directory 그룹 정책에 패키지 설치 지정**

    이 옵션을 활성화하면 Active Directory 그룹 정책을 통해 설치 패키지가 설치됩니다.

    이 옵션은 네트워크 에이전트 설치 패키지가 선택되어 있는 경우에 사용할 수 있습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **실행 중인 애플리케이션의 종료 여부를 사용자에게 물어 보기**

    애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

    이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

    이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- 애플리케이션을 설치할 기기를 선택합니다.

  - **모든 기기에 설치**

    다른 중앙 관리 서버에서 관리하는 기기에도 애플리케이션이 설치됩니다.

    이 옵션은 기본적으로 선택되어 있습니다. 네트워크에 중앙 관리 서버가 하나라면 이 설정을 변경하지 않아도 됩니다.

  - **이 중앙 관리 서버를 통해 관리되는 기기에만 설치**

    이 중앙 관리 서버에서 관리하는 기기에만 애플리케이션이 설치됩니다. 네트워크에 중앙 관리 서버가 여러 대 있고 해당 서버 간의 충돌을 방지하려는 경우 이 옵션을 선택합니다.

- 설치가 끝난 기기를 이동할 관리 그룹을 지정합니다.

  - **기기를 이동하지 않음**

    기기가 현재 포함되어 있는 그룹에 유지됩니다. 그룹에 배치되지 않은 기기는 미할당 상태로 유지됩니다.

  - **미할당 기기를 선택한 그룹으로 이동(단일 그룹만 선택할 수 있음)**

    기기가 선택한 관리 그룹으로 이동됩니다.

  기본적으로 **기기를 이동하지 않음** 옵션이 선택됩니다. 보안상의 이유로 기기를 수동으로 이동해야 할 수 있습니다.

7. 마법사의 이 단계에서는 애플리케이션 설치 시 기기를 다시 시작해야 하는지 지정합니다.

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

기본적으로 이 옵션은 선택되어 있습니다.

- **반복해서 물어보기(분)**

  이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

  이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

- **다음 시간 이후에 재시작(분)**

  사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

8. 필요하다면 **기기에 접근할 수 있는 계정 선택** 단계에서 *애플리케이션 원격 설치* 작업을 시작하는 데 사용할 계정을 추가합니다.

- **계정 필요 없음(네트워크 에이전트가 설치되어 있음)**

  이 옵션을 선택하면 애플리케이션 설치 프로그램을 실행할 계정을 지정하지 않아도 됩니다. 중앙 관리 서버가 실행 중인 계정에서 작업이 실행됩니다.

  클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않다면, 이 옵션은 이용할 수 없습니다.

- **계정 필요(네트워크 에이전트는 사용되지 않음)**

  원격 설치 작업을 할당한 기기에 네트워크 에이전트가 설치되어 있지 않다면 이 옵션을 선택하십시오. 이때, 사용자 계정 또는 SSH 인증서를 지정하여 애플리케이션을 설치할 수 있습니다.

  - **로컬 계정**. 이 옵션을 선택했다면 애플리케이션 설치 프로그램을 실행할 계정을 지정합니다. **추가** 버튼을 클릭하고 **로컬 계정**을 선택한 다음 사용자 계정 자격 증명을 지정합니다.

    예를 들어 이 작업이 할당된 모든 기기에 필요한 모든 권한이 어떤 계정에도 없다면, 사용자 계정을 여러 개 지정할 수 있습니다. 이때, 작업 실행 시 추가한 모든 계정을 위에서부터 순서대로 사용합니다.

- **SSH 인증서**. Linux 기반 클라이언트 기기에 애플리케이션을 설치한다면 사용자 계정 대신 SSH 인증서를 지정할 수 있습니다. **추가** 버튼을 클릭하고 **SSH 인증서**를 선택한 다음 인증서의 개인 및 공개 키를 지정합니다.

  개인 키를 생성하려면 ssh-keygen 유틸리티를 사용할 수 있습니다. Kaspersky Security Center는 개인 키의 PEM 형식을 지원하지만 ssh-keygen 유틸리티는 기본적으로 OPENSSH 형식으로 SSH 키를 생성합니다. Kaspersky Security Center에서는 OPENSSH 형식을 지원하지 않습니다. 지원되는 PEM 형식으로 개인 키를 생성하려면 ssh-keygen 명령에 -m PEM 옵션을 추가합니다. 예:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< 사용자 이메일 >"
  ```

9. **작업 생성 마침** 단계에서 **마침** 버튼을 클릭하여 작업을 생성하고 마법사를 종료합니다.

   생성이 완료되면 작업 세부 정보 열기 옵션을 활성화하면 작업 설정 창이 열립니다. 필요하다면 이 창에서 작업 매개변수를 확인하고 수정하거나 작업 시작 일정을 구성할 수 있습니다.

10. 작업 목록에서 생성한 작업을 선택한 다음 **시작**을 클릭합니다.

    또는 작업 설정에서 지정한 일정에 따라 작업이 시작될 때까지 기다립니다.

원격 설치 작업이 완료되면 선택한 애플리케이션이 지정된 기기에 설치됩니다.

Active Directory 그룹 정책을 통해 애플리케이션 설치

Kaspersky Security Center에서는 Active Directory 그룹 정책을 사용하여 관리 중인 기기에 Kaspersky 애플리케이션을 설치할 수 있습니다.

네트워크 에이전트가 포함된 설치 패키지를 통해서만 Active Directory 그룹 정책을 사용하여 애플리케이션을 설치할 수 있습니다.

Active Directory 그룹 정책을 사용하여 애플리케이션을 설치하려면:

1. 보호 배포 마법사를 실행합니다. 마법사의 지침을 따릅니다.

2. 보호 배포 마법사의 **원격 설치 작업 설정** 페이지에서 **Active Directory 그룹 정책에 패키지 설치 지정** 옵션을 활성화합니다.

3. **기기에 접근할 수 있는 계정 선택** 페이지에서 **계정 필요(네트워크 에이전트는 사용되지 않음)** 옵션을 선택합니다.

4. Kaspersky Security Center가 설치된 기기 또는 Group Policy Creator Owners 도메인 그룹에 포함된 계정에 관리자 권한을 가진 계정을 추가합니다.

5. 선택한 계정에 권한을 부여합니다.

   a. **제어판 → 관리 도구**로 이동하여 **그룹 정책 관리**를 엽니다.

   b. 필요한 도메인이 있는 노드를 클릭합니다.

   c. **위임** 섹션을 클릭합니다.

   d. **권한** 드롭다운 목록에서 **GPO 링크**를 선택합니다.

   e. **추가**를 클릭합니다.

f. **사용자, 컴퓨터 또는 그룹 선택** 창이 열리면 필요한 계정을 선택합니다.

g. **확인**을 클릭하여 **사용자, 컴퓨터 또는 그룹 선택** 창을 닫습니다.

h. **그룹 및 사용자** 목록에서 방금 추가한 계정을 선택하고 **고급** → **고급**을 클릭합니다.

i. **권한 항목** 목록에서 지금 추가한 계정을 두 번 클릭합니다.

j. 다음 권한을 부여합니다.

- **Group 개체 생성**
- **Group 개체 삭제**
- **그룹 정책 컨테이너 개체 만들기**
- **그룹 정책 컨테이너 개체 삭제**

k. **확인**을 눌러 변경을 저장합니다.

6. 마법사의 지시에 따라 기타 설정을 정의합니다.

7. 만들어진 원격 설치 작업을 수동으로 실행하거나 시작 스케줄을 기다립니다.

다음과 같은 원격 설치 시퀀스가 시작됩니다:

1. 작업이 실행될 때 지정된 집합의 모든 클라이언트 기기가 있는 각 도메인에 다음과 같은 개체가 만들어집니다:
   - **Kaspersky_AK{GUID}** 이름의 그룹 정책 개체(GPO).
   - GPO에 해당하는 보안 그룹. 이 보안 그룹에는 작업에 포함되는 클라이언트 기기가 있습니다. 보안 그룹 컨텐츠는 GPO의 범위를 정의합니다.
2. Kaspersky Security Center는 선택한 Kaspersky 애플리케이션의 공유 네트워크 폴더인 KLSHARE에서 클라이언트 기기에 해당 애플리케이션을 직접 설치합니다. Kaspersky Security Center 설치 폴더에 설치할 애플리케이션의 .msi 파일이 포함된 보조 하위 폴더가 만들어집니다.
3. 새 기기를 작업 범위에 추가하는 경우 해당 기기는 다음 작업 시작 시 보안 그룹에 추가됩니다. 작업 스케줄에서 **누락된 작업 실행** 옵션을 선택하면, 기기가 보안 그룹에 즉시 추가됩니다.
4. 기기를 작업 범위에서 삭제하는 경우 해당 기기는 다음 작업 시작 시 보안 그룹에서 삭제됩니다.
5. Active Directory에서 작업을 삭제하는 경우 GPO, GPO 링크 및 해당 보안 그룹도 삭제됩니다.

Active Directory를 사용하는 다른 설치 구성을 적용하려는 경우 필요한 설정을 수동으로 구성할 수 있습니다. 예를 들어, 이는 다음과 같은 경우에 필요할 수 있습니다:

- 안티 바이러스 보호 관리자에게 특정 도메인의 Active Directory를 변경할 권한이 없는 경우
- 원본 설치 패키지를 별도의 네트워크 리소스에 저장해야 하는 경우
- GPO를 특정 Active Directory 단위에 연결해야 하는 경우

Active Directory를 통해 다른 설치 구성을 사용할 수 있는 다음과 같은 옵션이 제공됩니다:

- Kaspersky Security Center 공유 폴더에서 직접 설치하려면, GPO 속성에서 필요한 애플리케이션의 설치 패키지 폴더에 있는 exec 하위 폴더의 msi 파일을 지정해야 합니다.
- 설치 패키지가 다른 네트워크 리소스에 있는 경우 전체 exec 폴더 컨텐츠를 복사해야 합니다. 해당 폴더에 확장자가 .msi인 파일 외에도 패키지가 만들어질 때 생성된 구성 파일이 포함되어 있기 때문입니다. 라이센스 키를 애플리케이션과 함께 설치하려면 라이센스 키 파일도 이 폴더로 복사해야 합니다.

보조 중앙 관리 서버에 애플리케이션 설치

보조 중앙 관리 서버에 애플리케이션을 설치하려면:

1. 관련 보조 중앙 관리 서버를 제어하는 중앙 관리 서버에 연결합니다.
2. 설치되고 있는 애플리케이션에 대한 설치 패키지가 선택한 각 보조 중앙 관리 서버에 있는지 확인합니다. 보조 서버에서 설치 패키지를 찾을 수 없다면 배포합니다. 이를 위해 **설치 패키지 배포(동기화)** 작업 유형으로 작업을 생성합니다.
3. 보조 중앙 관리 서버에 애플리케이션 원격 설치를 위한 작업을 생성합니다. **보조 중앙 관리 서버에 원격으로 애플리케이션 설치** 작업 유형을 선택합니다.

   새 작업 마법사는 마법사에서 선택한 애플리케이션을 특정 보조 중앙 관리 서버에 원격 설치하기 위한 작업을 생성합니다.
4. 이 작업을 직접 실행하거나, 작업 설정에 지정한 스케줄에 따라 실행될 때까지 기다립니다.

원격 설치 작업이 완료되면 선택한 애플리케이션이 보조 중앙 관리 서버에 설치됩니다.

Unix 기기에서 원격 설치용 설정 지정

원격 설치 작업을 사용하여 Unix 기기에 애플리케이션을 설치할 때 작업에 대한 Unix 관련 설정을 지정할 수 있습니다. 이러한 설정은 작업을 생성한 다음 작업 속성에서 사용할 수 있습니다.

원격 설치 작업에 대한 Unix 관련 설정 지정하기:

1. 메인 메뉴에서 **에셋(기기)** → **작업**로 이동합니다.
2. Unix 관련 설정을 지정할 원격 설치 작업의 이름을 누릅니다.

   작업 속성 창이 열립니다.
3. **애플리케이션 설정** → **Unix 관련 설정**으로 이동합니다.

4. 다음 설정을 지정합니다:

- **루트 계정의 암호 설정(SSH를 통한 배포에만 해당)**

  암호를 지정하지 않고 sudo 명령을 대상 기기에 사용할 수 없다면, 이 옵션을 선택한 다음, 루트 계정의 암호를 지정합니다. Kaspersky Security Center는 암호화된 형식으로 암호를 대상 기기에 전송하고, 암호를 복호화한 다음, 지정된 암호로 루트 계정을 대신하여 설치 절차를 시작합니다.

  Kaspersky Security Center는 계정 또는 지정된 암호를 사용하여 SSH 연결을 생성하지 않습니다.

- **대상 기기에 대한 실행 권한이 있는 임시 폴더의 경로 지정(SSH를 통한 배포에만 해당)**

  대상 기기의 /tmp 디렉토리에 실행 권한이 없는 경우, 이 옵션을 선택한 다음, 실행 권한이 있는 디렉토리 경로를 지정합니다. Kaspersky Security Center는 지정된 디렉토리를 SSH를 통해 액세스하기 위한 임시 디렉토리로 사용합니다. 애플리케이션은 설치 패키지를 디렉토리에 배치하고 설치 절차를 실행합니다.

5. **저장** 버튼을 누릅니다.

지정된 작업 설정이 저장됩니다.

Kaspersky 애플리케이션 시작 및 중지.

관리 중인 기기에서 Kaspersky 애플리케이션을 시작 및 중지하기 위해 *애플리케이션 시작 또는 중지* 작업을 사용할 수 있습니다.

애플리케이션 시작 또는 중지 작업을 생성하려면:

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.

   새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. **애플리케이션** 드롭다운 목록에서 작업을 생성하려는 애플리케이션을 선택합니다.

   이전에 Kaspersky 애플리케이션에 대한 관리 웹 플러그인을 추가했다면 해당 애플리케이션이 목록에 표시됩니다.
4. **작업 유형** 목록에서 **애플리케이션 활성화** 작업을 선택합니다.
5. **작업 이름** 필드에 새 작업의 이름을 지정합니다.

   작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
6. 이 작업을 할당할 기기를 선택합니다.
7. **애플리케이션** 창에서 다음을 수행합니다.

- 작업을 생성할 애플리케이션 이름 옆의 확인란을 선택합니다.
- **애플리케이션 시작** 또는 **애플리케이션 중지** 옵션을 선택합니다.

8. 기본 작업 설정을 수정하려면 **생성이 완료되면 작업 세부 정보 열기** 단계에서 **작업 생성 마침** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

9. **마침** 버튼을 누릅니다.

   그러면 작업이 생성되고 작업 목록에 표시됩니다.

10. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

11. 작업 속성 창에서 필요에 따라 일반 작업 설정을 지정한 후 설정을 저장합니다.

    작업이 생성 및 구성됩니다.

작업을 실행하려면 작업 목록에서 작업을 선택하고 **시작** 버튼을 클릭합니다.

모바일 기기 매니지먼트

Kaspersky Security Center를 통해 모바일 기기 보호를 관리하려면 전용 라이센스가 필요한 모바일 기기 매니지먼트 기능을 사용하면 됩니다. 조직의 직원이 소유한 모바일 기기를 관리하려면 모바일 기기 관리를 활성화하고 구성해야 합니다.

모바일 기기 관리를 통해 직원의 Android 기기를 관리할 수 있습니다. 기기에 설치된 Kaspersky Endpoint Security for Android 모바일 앱이 보호 기능을 제공합니다. 이 모바일 앱은 위협을 제기하는 웹 위협, 바이러스 및 기타 프로그램으로부터 모바일 기기를 보호합니다. Kaspersky Security Center 웹 콘솔을 통한 중앙 집중식 관리 시, Kaspersky Security Center 웹 콘솔이 설치된 기기에 다음 웹 관리 플러그인을 설치해야 합니다:

- Kaspersky Security for Mobile Plug-in
- Kaspersky Endpoint Security for Android 플러그인

모바일 기기의 보호 배포 및 관리에 대한 자세한 내용은 Kaspersky Security for Mobile 도움말을 참조하십시오.

Kaspersky Security Center 웹 콘솔에서 모바일 기기 관리 설정 수정

모바일 기기 매니지먼트 설정을 수정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘()을 누릅니다.

   중앙 관리 서버 속성 창이 열립니다.

2. **일반** 탭에서 **추가 포트** 섹션을 선택합니다.

3. 관련 설정을 수정합니다.

   - **모바일 기기용 포트 열기**

     이 토글 스위치를 활성화하면 중앙 관리 서버에서 모바일 기기용 포트가 열립니다.
     모바일 기기 관리 구성 요소를 설치했을 때만 모바일 기기용 포트를 사용할 수 있습니다.
     이 토글 스위치를 비활성화하면 중앙 관리 서버에서 모바일 기기용 포트를 사용하지 않습니다.
     기본적으로 이 토글 스위치는 비활성화되어 있습니다.

- **모바일 기기 동기화용 포트**

  중앙 관리 서버와 모바일 기기 연결에 사용되는 포트 번호. 기본 포트 번호는 13292입니다.
  십진법을 사용하여 기록합니다.

- **모바일 기기 활성화용 포트**

  Kaspersky Endpoint Security for Android와 Kaspersky의 활성화 서버 연결용 포트.
  기본 포트 번호는 17100입니다.

4. **저장** 버튼을 누릅니다.

이제 모바일 기기를 중앙 관리 서버에 연결할 수 있습니다.

타사 보안 제품 교체

Kaspersky Security Center를 통해 Kaspersky 보안 제품을 설치할 때는 설치하는 애플리케이션과 호환되지 않는 타사 소프트웨어를 제거해야 할 수 있습니다. Kaspersky Security Center는 타사 애플리케이션을 제거하는 여러 가지 방법을 제공합니다.

인스톨러를 사용하여 비-호환 애플리케이션 제거

이 옵션은 Microsoft Management Console을 기반으로 하는 관리 콘솔에서만 사용할 수 있습니다.

비-호환 애플리케이션을 제거하는 인스톨러의 작업 방법은 다양한 설치 유형에서 지원됩니다. 보안 제품 설치 패키지의 속성 창(**비호환 애플리케이션** 섹션)에서 **비호환 애플리케이션 자동 제거** 옵션을 선택한 경우 해당 보안 제품을 설치하기 전에 모든 비-호환 애플리케이션이 자동으로 제거됩니다.

애플리케이션의 원격 설치를 구성할 때 비-호환 애플리케이션 제거

보안 제품의 원격 설치를 구성할 때 **비호환 애플리케이션 자동 제거** 옵션을 활성화할 수 있습니다. MMC(Microsoft Management Console) 기반 관리 콘솔의 원격 설치 마법사에서 이 옵션을 사용할 수 있습니다. Kaspersky Security Center 웹 콘솔의 보호 배포 마법사에서 이 옵션을 찾을 수 있습니다. 이 옵션을 사용하도록 설정하면 Kaspersky Security Center는 비-호환 애플리케이션을 제거한 후 보안 제품을 관리 중인 기기에 설치합니다.

방법 지침:

- 관리 콘솔: 원격 설치 마법사를 사용하여 비호환 애플리케이션 제거
- Kaspersky Security Center 웹 콘솔: 설치하기 전에 비-호환 애플리케이션 제거

전용 작업을 통해 비-호환 애플리케이션 제거

비-호환 애플리케이션을 제거하려면 **애플리케이션을 원격으로 제거** 작업을 사용합니다. 이 작업은 보안 제품 설치 작업 전에 기기에서 실행해야 합니다. 예를 들어 설치 작업 시 **애플리케이션을 원격으로 제거** 작업이 진행 중인 경우 **다른 작업 완료 시** 스케줄 유형을 선택할 수 있습니다.

이 제거 방법은 보안 제품 설치 관리자가 비-호환 애플리케이션을 올바르게 제거할 수 없는 경우에 적합합니다.

관리 콘솔 사용 지침: 작업 만들기.

네트워크에 연결된 기기 발견

이 섹션에서는 네트워크에 연결된 기기의 검색 및 발견에 관해 설명합니다.

Kaspersky Security Center에서는 지정된 기준에 따라 기기를 찾을 수 있습니다. 검색 결과는 텍스트 파일에 저장할 수 있습니다.

검색 및 발견 기능을 사용하면 다음과 같은 기기를 찾을 수 있습니다.

- Kaspersky Security Center 중앙 관리 서버 및 해당 보조 중앙 관리 서버의 관리 그룹에 있는 관리 중인 기기.
- Kaspersky Security Center 중앙 관리 서버 및 그 보조 중앙 관리 서버에서 관리 중인 미할당 기기.

시나리오: 네트워크에 연결된 기기 발견

보안 제품을 설치하기 전에 기기 발견을 수행해야 합니다. 중앙 관리 서버는 검색된 기기에 대한 정보를 수신하고 정책을 통해 기기를 관리할 수 있도록 합니다. 네트워크에서 사용 가능한 기기 목록을 업데이트하려면 정기적인 네트워크 검색이 필요합니다.

네트워크 폴링을 시작하기 전에 SMB 프로토콜이 활성화되어 있는지 확인하십시오. 그렇지 않으면 Kaspersky Security Center가 폴링된 네트워크에서 기기를 검색할 수 없습니다. SMB 프로토콜을 활성화하려면 운영 체제에 대한 지침을 따르십시오.

네트워크 기기 발견은 다음 단계로 진행됩니다.

1. **기기 발견**

   빠른 시작 마법사는 초기 기기 발견 과정을 안내하며 컴퓨터, 태블릿 및 스마트폰과 같은 네트워크 기기를 찾는 데 도움이 됩니다. 기기 발견을 수동으로 수행할 수도 있습니다.

2. **예약된 검색 구성**

   주기적으로 사용하려는 검색 유형을 결정합니다. 원하는 유형을 활성화하고 검색 스케줄을 구성합니다. 네트워크 검색 빈도에 대한 권장 사항을 참조할 수 있습니다.

3. **발견된 기기를 관리 그룹에 추가하는 규칙 설정(선택 사항)**

   네트워크에 표시되는 새 기기는 정기 검색 중에 발견되어 **미할당 기기** 그룹에 자동으로 포함됩니다. 기기 이동 규칙을 설정하여 **관리 중인 기기** 그룹에 대한 기기 할당을 자동화할 수 있습니다. 보존 규칙을 구성할 수도 있습니다.

   3단계를 건너뛰면 새로 검색된 기기가 **미할당 기기** 그룹에 할당됩니다. 원하는 경우 이러한 기기를 수동으로 **관리 중인 기기** 그룹으로 이동할 수 있습니다. 기기를 수동으로 **관리 중인 기기** 그룹으로 이동하면, 각 기기 관련 정보를 분석하여 해당 기기를 관리 그룹으로 이동할지, 이동한다면 정확히 어느 그룹으로 이동할지 결정할 수 있습니다.

결과

시나리오를 완료하면 다음과 같은 결과를 얻을 수 있습니다:

- Kaspersky Security Center 중앙 관리 서버가 네트워크에 있는 기기를 발견하여 해당 기기와 관련된 정보를 제공합니다.
- 이후 검색이 설정되어 지정된 스케줄에 따라 수행됩니다.
- 새로 검색한 기기는 구성한 규칙에 따라 정렬됩니다(규칙을 구성하지 않았다면, 기기가 **미할당 기기** 그룹에 남습니다).

기기 발견

이 섹션에서는 Kaspersky Security Center에서 사용 가능한 기기 발견 유형에 대해 설명하고 각 유형 사용과 관련된 정보를 제공합니다.

중앙 관리 서버는 정기 검색을 통해 이 네트워크의 네트워크 및 기기 구조 관련 정보를 수신합니다. 정보는 중앙 관리 서버 데이터베이스에 기록됩니다. 중앙 관리 서버에서는 다음과 같은 유형의 검색을 사용할 수 있습니다:

- **Windows 네트워크 검색**. 중앙 관리 서버는 두 가지 종류의 Windows 네트워크 검색(빠른 검색과 전체 검색)을 수행할 수 있습니다. 빠른 검색 시 중앙 관리 서버는 모든 네트워크 도메인 및 작업 그룹에서 기기들의 NetBIOS 이름 목록 정보만 가져옵니다. 상세 검색 시에는 각 클라이언트 기기에서 운영 체제 이름, IP 주소, DNS 이름, NetBIOS 이름 정보 등 더 상세한 정보가 요청됩니다. 기본적으로는 빠른 검색과 전체 검색이 모두 활성화됩니다. 포트 UDP 137, UDP 138, TCP 139가 라우터에서 닫혀 있거나 방화벽에 의해 닫힌 경우 등에는 Windows 네트워크 검색에서 기기를 발견하지 못할 수 있습니다.
- **도메인 컨트롤러 검색**. 중앙 관리 서버 또는 배포 지점은 도메인 구조에 대한 정보와 도메인에 포함된 기기의 DNS 이름에 대한 정보를 검색합니다. 기본적으로 이 검색 유형은 활성화됩니다. 네트워크로 연결된 모든 기기가 도메인 소속이라면 도메인 컨트롤러 검색을 사용할 것을 권장합니다. 네트워크로 연결된 기기 중 일부가 도메인에 포함되어 있지 않으면 도메인 컨트롤러 검색으로 이러한 기기를 검색할 수 없습니다.
- **IP 범위 검색**. 중앙 관리 서버에서 ICMP 패킷 또는 NBNS 프로토콜을 사용하여 지정된 IP 범위를 검색하고 IP 범위 내 기기에 있는 전체 데이터 집합을 수집합니다. 기본적으로 이 검색 유형은 비활성화됩니다. Windows 네트워크 검색 및/또는 Active Directory 검색을 사용하는 경우에는 이 검색 유형을 사용하지 않는 것이 좋습니다.
- **Zeroconf 폴링** 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 IPv6 네트워크를 검색하는 배포 지점입니다. 기본적으로 이 검색 유형은 비활성화됩니다. 배포 지점에서 Linux를 실행하는 경우 제로 구성 검색을 사용할 수 있습니다.

기기 이동 규칙을 설정하고 활성화한 경우 새로 발견된 기기가 **관리 중인 기기** 그룹에 자동으로 포함됩니다. 이동 규칙을 활성화하지 않은 경우에는 새로 발견된 기기가 **미할당 기기** 그룹에 자동으로 포함됩니다.

각 유형에 대해 기기 발견 설정을 수정할 수 있습니다. 검색 스케줄을 수정하려는 경우나, 전체 도메인 포레스트를 검색할지 아니면 특정 도메인만 검색할지를 설정하려는 경우를 예로 들 수 있습니다.

네트워크 폴링을 시작하기 전에 SMB 프로토콜이 활성화되어 있는지 확인하십시오. 그렇지 않으면 Kaspersky Security Center가 폴링된 네트워크에서 기기를 검색할 수 없습니다. SMB 프로토콜을 활성화하려면 운영 체제에 대한 지침을 따르십시오.

Windows 네트워크 검색

Windows 네트워크 검색 정보

빠른 검색 시 중앙 관리 서버는 모든 네트워크 도메인 및 작업 그룹에서 기기들의 NetBIOS 이름 목록 정보만 가져옵니다. 전체 검색 시에는 각 클라이언트 기기로부터 다음 정보가 요청됩니다:

- 운영 체제 유형
- IP 주소
- DNS 이름
- NetBIOS 이름

빠른 검색과 전체 검색 시에는 다음 조건을 충족해야 합니다:

- 네트워크에서 포트 UDP 137/138, TCP 139, UDP 445, TCP 445를 사용할 수 있어야 합니다.
- SMB 프로토콜이 활성화되었습니다.
- Microsoft Computer Browser 서비스를 사용해야 하며, 중앙 관리 서버에서 기본 브라우저 컴퓨터가 활성화되어야 합니다.
- Microsoft Computer Browser 서비스를 사용해야 하며, 클라이언트 기기에서 기본 브라우저 컴퓨터가 활성화되어야 합니다.
  - 네트워크에 연결된 기기 수가 32대를 초과하지 않는 경우 기기 한 대 이상에서.
  - 네트워크에 연결된 32대 기기 각각에 대해 기기 한 대 이상에서.

빠른 검색을 한 번 이상 실행해야 전체 검색을 실행할 수 있습니다.

Windows 네트워크 검색에 대한 설정 보기 및 수정

Windows 네트워크 검색 속성을 수정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **발견 및 배포 → 발견 → Windows 도메인**로 이동합니다.
2. **속성** 버튼을 누릅니다.
   Windows 도메인 속성 창이 열립니다.
3. **Windows 네트워크 검색 활성화** 토글 버튼을 사용하여 Windows 네트워크 검색 검색을 활성화하거나 비활성화합니다.
4. 검색 스케줄을 구성합니다. 기본적으로 빠른 검색은 15분마다 실행되고 전체 검색은 60분마다 실행됩니다.

검색 스케줄 옵션:

- **N일마다**

  검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.
  기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **N분마다**

  검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.

- **요일별**

  검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

- **누락된 작업 실행**

  중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.
  이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.
  이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

5. Windows 네트워크 검색 속성을 저장합니다.

속성이 저장되고 발견된 모든 Windows 도메인 및 작업 그룹에 적용됩니다.

수동으로 검색 실행

검색을 즉시 실행하려면

빠른 검색 시작 또는 **전체 검색 시작**을 누릅니다.

검색이 완료되면 도메인 이름 옆에 있는 확인란을 선택하고 **기기** 버튼을 눌러 **Windows 도메인** 페이지에서 발견된 기기 목록을 확인할 수 있습니다.

IP 범위 검색

Kaspersky Security Center는 처음에는 설치된 기기의 네트워크 설정에서 검색을 위한 IP 범위를 가져옵니다. 기기 주소가 192.168.0.1이고 서브넷 마스크가 255.255.255.0이면 Kaspersky Security Center는 검색 주소 목록에 192.168.0.0/24 네트워크를 자동으로 포함합니다. Kaspersky Security Center는 192.168.0.1~192.168.0.254 범위의 모든 주소를 검색합니다.

Microsoft Active Directory 또는 Samba 도메인 컨트롤러 내의 모든 Linux 기반 호스트에 대해 `/etc/samba/smb.conf` 파일에서 `netbios name`과 `workgroup` 매개변수를 지정합니다. 그렇지 않으면 검색 결과에 중복 호스트가 포함될 수 있습니다.

Kaspersky Security Center는 역순 DNS 룩업 또는 NBNS 프로토콜을 사용하여 IP 범위를 검색할 수 있습니다.

- **역순 DNS 룩업**

  Kaspersky Security Center에서는 표준 DNS 요청을 사용하여 모든 IP 주소에 대해 지정된 범위에서 DNS 이름으로의 역방향 이름 해석 수행을 시도합니다. 이 작업이 정상적으로 수행되면 서버는 수신된 이름으로 `ICMP ECHO REQUEST`(ping 명령과 같음)를 전송합니다. 기기가 응답하면 해당 기기에 대한 정보가 Kaspersky Security Center 데이터베이스에 추가됩니다. 역방향 이름 해석은 네트워크 프린터나 라우터와 같이 IP 주소는 있을 수 있지만 컴퓨터는 아닌 네트워크 기기를 제외하는 데 필요합니다.

  이 검색 방법에서는 올바르게 구성된 로컬 DNS 서비스를 사용합니다. 그리고 역방향 룩업 영역도 있어야 합니다. Active Directory가 사용되는 네트워크에서는 이러한 영역이 자동으로 유지 관리됩니다. 하지만 이러한 네트워크에서는 IP 서브넷 검색을 수행해도 Active Directory 검색보다 자세한 정보가 제공되지는 않습니다. 또한 소규모 네트워크의 관리자는 역방향 룩업 영역을 구성하지 않는 경우가 많습니다. 대다수 네트워크 서비스의 작업에서는 해당 영역이 필요하지 않기 때문입니다. 이러한 모든 이유로 인해 IP 서브넷 검색은 기본적으로 비활성화됩니다.

- **NBNS 프로토콜**

  네트워크에서 역순 이름 확인이 불가능하다면, Kaspersky Security Center가 NBNS 프로토콜을 사용하여 IP 주소 범위를 검색합니다. IP 주소에 대한 요청이 NetBIOS 이름을 반환하면 이 기기에 대한 정보가 Kaspersky Security Center 데이터베이스에 추가됩니다.

네트워크 폴링을 시작하기 전에 SMB 프로토콜이 활성화되어 있는지 확인하십시오. 그렇지 않으면 Kaspersky Security Center가 폴링된 네트워크에서 기기를 검색할 수 없습니다. SMB 프로토콜을 활성화하려면 운영 체제에 대한 지침을 따르십시오.

IP 범위 검색에 대한 설정 보기 및 수정

IP 범위 검색 속성을 보고 수정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **발견 및 배포 → 발견 → IP 범위**으로 이동합니다.
2. **속성** 버튼을 누릅니다.

   IP 검색 속성 창이 열립니다.
3. **검색 허용** 토글 버튼을 사용하여 IP 검색을 활성화하거나 비활성화합니다.
4. 검색 스케줄을 구성합니다. 기본적으로 IP 검색은 420분(7시간)마다 실행됩니다.

   검색 간격을 지정할 때는 이 설정이 IP 주소 유효 기간 파라미터의 값을 초과하지 않는지 확인하십시오. IP 주소 유효 기간 동안 검색을 통해 확인되지 않은 IP 주소는 검색 결과에서 자동으로 제거됩니다. 기본적으로 검색 결과의 유효 시간은 24시간입니다. DHCP(Dynamic Host Configuration Protocol)를 사용하여 할당되는 동적 IP 주소가 24시간마다 변경되기 때문입니다.

   검색 스케줄 옵션:

   - **N일마다**

     검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.

     기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **N분마다**

  검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.

- **요일별**

  검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

- **누락된 작업 실행**

  중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.

  이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.

  이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

5. **저장** 버튼을 누릅니다.

   속성이 저장되고 모든 IP 범위에 적용됩니다.

수동으로 검색 실행

검색을 즉시 실행하려면

폴링 시작을 누릅니다.

IP 범위 추가 및 수정

Kaspersky Security Center는 처음에는 설치된 기기의 네트워크 설정에서 검색을 위한 IP 범위를 가져옵니다. 기기 주소가 192.168.0.1이고 서브넷 마스크가 255.255.255.0이면 Kaspersky Security Center는 검색 주소 목록에 192.168.0.0/24 네트워크를 자동으로 포함합니다. Kaspersky Security Center는 192.168.0.1~192.168.0.254 범위의 모든 주소를 검색합니다. 자동으로 정의된 IP 범위를 수정하거나 사용자 지정 IP 범위를 추가할 수 있습니다.

IPv4 주소에 대해서만 범위를 생성할 수 있습니다. 제로 구성 검색을 활성화하면 Kaspersky Security Center가 전체 네트워크를 폴링합니다.

새 IP 범위를 추가하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **발견 및 배포** → **발견** → **IP 범위**로 이동합니다.

2. 새 IP 범위를 추가하려면 **추가** 버튼을 누릅니다.

3. 열리는 창에서 다음 설정을 구성하십시오:

- **IP 범위 이름**

  IP 범위의 이름입니다. '192.168.0.0/24'와 같은 IP 범위 자체를 이름으로 지정할 수 있습니다.

- **IP 간격 또는 서브넷 주소 및 마스크**

  시작 및 끝 IP 주소나 서브넷 주소와 서브넷 마스크를 지정하여 IP 범위를 설정합니다. **찾기** 버튼을 눌러 기존 IP 범위 중 하나를 선택할 수도 있습니다.

- **IP 주소 수명(시간)**

  이 파라미터를 지정할 때는 검색 스케줄에 설정된 검색 간격을 초과하는지 확인합니다. IP 주소 유효 기간 동안 검색을 통해 확인되지 않은 IP 주소는 검색 결과에서 자동으로 제거됩니다. 기본적으로 검색 결과의 유효 시간은 24시간입니다. DHCP(Dynamic Host Configuration Protocol)를 사용하여 할당되는 동적 IP 주소가 24시간마다 변경되기 때문입니다.

4. 추가한 서브넷 또는 간격을 검색하려는 경우 **IP 범위 검색 사용**를 선택합니다. 그렇지 않으면 추가한 서브넷 또는 간격이 검색되지 않습니다.

5. **저장** 버튼을 누릅니다.

새 IP 범위가 IP 범위 목록에 추가됩니다.

폴링 시작 버튼을 사용하여 각 IP 범위의 검색을 개별적으로 실행할 수 있습니다. 검색이 완료되면 **기기** 버튼을 사용하여 발견된 기기 목록을 확인할 수 있습니다. 기본적으로 검색 결과의 유효 시간(IP 주소 유효 기간 설정과 같음)은 24시간입니다.

기존 IP 범위에 서브넷을 추가하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **발견 및 배포** → **발견** → **IP 범위**로 이동합니다.

2. 서브넷을 추가할 IP 범위의 이름을 누릅니다.

3. 창이 열리면 **추가**를 누릅니다.

4. 주소와 마스크를 사용하거나 IP 범위의 첫 번째 및 마지막 IP 주소를 사용하여 서브넷을 지정합니다. 또는 **찾기** 버튼을 눌러 기존 서브넷을 추가합니다.

5. **저장** 버튼을 누릅니다.

   새 서브넷이 IP 범위에 추가됩니다.

6. **저장** 버튼을 누릅니다.

IP 범위의 새 설정이 저장됩니다.

서브넷은 필요한 수만큼 추가할 수 있습니다. 이름이 지정된 IP 범위는 겹칠 수 없지만 IP 범위 내에서 이름이 지정되지 않은 서브넷에는 이러한 제한이 없습니다. 모든 IP 범위에 대해 검색을 독립적으로 활성화 및 비활성화할 수 있습니다.

Zeroconf 폴링

이 검색 유형은 Linux 기반 배포 지점에 대해서만 지원됩니다.

배포 지점에서 IPv6 주소를 사용하는 기기가 있는 네트워크를 검색할 수 있습니다. 이 경우 IP 범위를 지정하지 않고 배포 지점에서 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 전체 네트워크를 검색합니다. 제로 구성을 시작하려면 배포 지점에 avahi-browse 유틸리티를 설치해야 합니다.

IPv6 네트워크 검색을 활성화하려면:

1. 메인 메뉴에서 **발견 및 배포 → 발견 → IP 범위**로 이동합니다.
2. **속성** 버튼을 누릅니다.
3. 열리는 창에서 **Zeroconf을 사용하여 IPv6 네트워크 검색** 토글 버튼을 켭니다.

그러면 배포 지점에서 네트워크를 검색하기 시작합니다. 이 경우 지정된 IP 범위가 무시됩니다.

도메인 컨트롤러 검색

Kaspersky Security Center는 Microsoft Active Directory 도메인 컨트롤러 및 Samba 도메인 컨트롤러의 검색을 지원합니다.

Kaspersky Security Center에서는 Linux 배포 지점을 통해서만 Samba 도메인 컨트롤러를 검색할 수 있습니다. Samba 도메인 컨트롤러에서는 Samba 4가 Active Directory 도메인 컨트롤러로 사용됩니다.

도메인 컨트롤러를 검색하면, 중앙 관리 서버 또는 배포 지점이 도메인에 포함된 기기의 도메인 구조, 사용자 계정, 보안 그룹, DNS 이름에 대한 정보를 검색합니다.

네트워크로 연결된 모든 기기가 도메인 소속이라면 도메인 컨트롤러 검색을 사용할 것을 권장합니다. 네트워크로 연결된 기기 중 일부가 도메인에 포함되어 있지 않으면 도메인 컨트롤러 검색으로 이러한 기기를 검색할 수 없습니다.

필수 구성 요소

도메인 컨트롤러를 검색하기 전에 방화벽 또는 프록시 서버를 통한 도메인 컨트롤러에 대한 연결을 허용하는지 확인하십시오. 또한 도메인 컨트롤러에서 다음 프로토콜이 활성화되었는지 확인합니다.

- LDAP(Lightweight Directory Access Protocol)
- SASL(Simple Authentication and Security Layer)

  이 프로토콜은 SASL 인증을 사용하여 도메인 컨트롤러에 대한 연결이 설정된 경우에 사용됩니다. 중앙 관리 서버 및 배포 지점은 DIGEST-MD5 메커니즘만 지원합니다.
- 보안 소켓 계층을 통한 경량 디렉토리 엑세스 프로토콜(LDAP)

  이 프로토콜은 암호화된 연결을 통해 도메인 컨트롤러에 연결해야 하는 경우 사용됩니다.

도메인 컨트롤러 기기에서 다음 포트를 사용할 수 있는지 확인합니다.

- LDAP 프로토콜 및 단순 인증용 389(SASL 포함)
- LDAPS 프로토콜용 636

Microsoft Active Directory 또는 Samba 도메인 컨트롤러 내의 모든 Linux 기반 호스트에 대해 `/etc/samba/smb.conf` 파일에서 `netbios name` 및 `workgroup` 파라미터를 지정해야 합니다. 그렇지 않으면 검색 결과에 중복 호스트가 포함될 수 있습니다.

Microsoft 활성 디렉토리 도메인에 여러 도메인 컨트롤러가 있는 경우, 도메인 검색 과정에서 특정 컨트롤러를 선택하는 것은 지원되지 않습니다. 처음으로 탐지된 도메인 컨트롤러와의 연결이 설정됩니다. Microsoft 활성 디렉토리 도메인에서 올바르게 인증하려면, 인증서의 주체 대체 이름(SAN) 필드에 해당 도메인에 포함된 모든 도메인 컨트롤러의 주소와 Microsoft 활성 디렉토리 도메인의 NetBIOS 이름이 포함되어야 합니다.

중앙 관리 서버를 사용한 도메인 컨트롤러 검색

중앙 관리 서버를 사용하여 Microsoft Active Directory 도메인 컨트롤러만 검색할 수 있습니다.

중앙 관리 서버를 사용하여 도메인 컨트롤러를 검색하려면:

1. 메인 메뉴에서 **발견 및 배포 → 발견 → 도메인 컨트롤러**로 이동합니다.
2. **검색 설정**을 클릭합니다.
   도메인 컨트롤러 검색 설정 창이 열립니다.
3. **도메인 컨트롤러 검색 활성화** 옵션을 선택합니다.
4. **고급 설정** 섹션에서 검색 범위를 지정합니다.
   - **현재 도메인 검색**
     Kaspersky Security Center가 속한 도메인을 검색하려면 이 옵션을 선택합니다.
   - **전체 도메인 포레스트 검색**
     Kaspersky Security Center가 속한 도메인 포레스트를 검색하려면 이 옵션을 선택합니다.
   - **지정한 도메인 검색**
     지정된 주소와 사용자 자격 증명을 사용하여 도메인을 검색하려면 이 옵션을 선택합니다.
5. 필요한 경우 검색 스케줄을 지정합니다. 기본 기간은 1시간입니다. 이전 데이터는 다음 검색에서 수신된 데이터로 완전히 교체됩니다.
   다음과 같은 검색 스케줄 옵션을 사용할 수 있습니다:
   - **N일마다**
     검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.
     기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **N분마다**

  검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.

- **요일별**

  검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

- **누락된 작업 실행**

  중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.

  이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.

  이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

도메인의 보안 그룹에서 사용자 계정을 변경하면 이러한 변경 사항은 도메인 컨트롤러를 검색하고 1시간 후에 Kaspersky Security Center에 표시됩니다.

6. 변경 사항을 적용하려면 **저장**을 클릭합니다.

7. 검색을 즉시 수행하려면 **폴링 시작** 버튼을 클릭합니다.

배포 지점을 사용한 도메인 컨트롤러 검색

배포 지점을 사용하여 Microsoft Active Directory 도메인 컨트롤러 및 Samba 도메인 컨트롤러를 검색할 수도 있습니다. Windows 또는 Linux 기반 관리 중인 기기는 배포 지점 역할을 할 수 있습니다.

Linux 배포 지점은 Microsoft Active Directory 도메인 컨트롤러 및 Samba 도메인 컨트롤러의 검색을 지원합니다.
Windows 배포 지점은 Microsoft Active Directory 도메인 컨트롤러의 검색만 지원합니다.
Mac 배포 지점을 사용한 검색은 지원되지 않습니다.

배포 지점을 사용하여 도메인 컨트롤러 검색을 구성하려면:

1. 배포 지점 속성을 엽니다.

2. **도메인 컨트롤러 검색** 섹션을 선택합니다.

3. **도메인 컨트롤러 검색 활성화** 옵션을 선택합니다.

4. 검색하려는 도메인 컨트롤러를 선택합니다.

Linux 배포 지점을 사용한다면 **지정한 도메인 검색** 섹션에서 **추가**를 클릭하고 도메인 컨트롤러의 주소와 사용자 자격 증명을 지정합니다.

Windows 배포 지점을 사용한다면 다음 옵션 중 하나를 선택할 수 있습니다.

- **현재 도메인 검색**
- **전체 도메인 포레스트 검색**
- **지정한 도메인 검색**

5. 필요하다면 **검색 스케줄 설정** 버튼을 클릭하여 검색 스케줄 옵션을 지정합니다.

   검색은 지정된 스케줄에 따라서만 시작됩니다. 검색을 수동으로 시작할 수는 없습니다.

검색이 완료되면 도메인 구조가 **도메인 컨트롤러** 섹션에 표시됩니다.

기기 이동 규칙을 설정하고 활성화한 경우 새로 발견된 기기가 **관리 중인 기기** 그룹에 자동으로 포함됩니다. 이동 규칙을 활성화하지 않은 경우에는 새로 발견된 기기가 **미할당 기기** 그룹에 자동으로 포함됩니다.

검색된 사용자 계정은 Kaspersky Security Center 웹 콘솔에서 도메인 인증에 사용될 수 있습니다.

도메인 컨트롤러에 대한 인증 및 연결

도메인 검색 시 도메인 컨트롤러 인증 및 연결

Linux 배포 지점으로 도메인 컨트롤러 검색 시, 도메인 컨트롤러에 대한 초기 연결 구성을 위해 배포 지점이 연결 프로토콜을 식별합니다. 이 프로토콜은 도메인 컨트롤러에 대한 모든 향후 연결에 사용됩니다. 도메인 컨트롤러에 대한 초기 연결 설정 시 네트워크 에이전트 플래(`KLNAG_LDAP_TLS_REQCERT` 및 `KLNAG_LDAP_SSL_CACERT`)를 사용하여 연결 옵션을 변경할 수 있습니다. 이 문서에서 설명된 것처럼 klscflag를 사용하여 네트워크 에이전트 플래그를 구성할 수 있습니다.

도메인 컨트롤러에 대한 초기 연결은 다음과 같이 진행됩니다.

1. Linux 배포 지점은 LDAPS를 통해 도메인 컨트롤러에 연결을 시도합니다.

   인증서 확인은 기본적으로 불필요합니다. 인증서를 확인하려면 `KLNAG_LDAP_TLS_REQCERT` 플래그를 1로 설정합니다.

   `KLNAG_LDAP_TLS_REQCERT` 플래그의 가능한 값:

   - `0` - 인증서가 요청되지만 제공되지 않거나 인증서 확인에 실패하면 TLS 연결이 여전히 성공적으로 생성된 것으로 간주됩니다(기본값).
   - `1` - LDAP 서버 인증서에 대한 엄격한 인증이 필요합니다.

   `KLNAG_LDAP_SSL_CACERT` 플래그를 지정하지 않으면, 인증서 체인 액세스 시 인증 기관(CA)에 대한 OS 종속 경로가 기본값으로 사용됩니다. 사용자 정의 경로를 지정하려면 `KLNAG_LDAP_SSL_CACERT` 플래그를 사용합니다.

2. LDAPS 연결에 실패하면 Linux 배포 지점은 SASL(DIGEST-MD5)을 사용하여 암호화되지 않은 TCP 연결을 통해 도메인 컨트롤러에 연결을 시도합니다.

플래그 구성

klscflag 유틸리티를 사용하여 플래그를 구성할 수 있습니다.

Linux 배포 지점에서 명령줄을 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. 기본적으로 Linux 배포 지점에서 klscflag 유틸리티는 /opt/kaspersky/ksc64/sbin에 있습니다.

예를 들어 다음 명령은 인증서 확인을 시행합니다.

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Samba 도메인 컨트롤러 구성

Kaspersky Security Center는 Samba 4에서만 실행되는 Linux 도메인 컨트롤러를 지원합니다.

Samba 도메인 컨트롤러는 Microsoft Active Directory 도메인 컨트롤러와 같은 스키마 확장을 지원합니다. Samba 4 스키마 확장을 사용하면 Samba 도메인 컨트롤러와 Microsoft Active Directory 도메인 컨트롤러의 완전한 호환성을 활성화할 수 있습니다. 이는 선택 사항입니다.

Microsoft Active Directory 도메인 컨트롤러와 Samba 도메인 컨트롤러의 완전한 호환성을 활성화할 것을 권장합니다. 이렇게 하면 Kaspersky Security Center와 Samba 도메인 컨트롤러 간의 올바른 상호 작용이 보장됩니다.

Microsoft Active Directory 도메인 컨트롤러와 Samba 도메인 컨트롤러의 완전한 호환성을 활성화하려면 다음을 수행합니다.

1. RFC2307 스키마 확장을 사용하려면 다음 명령을 실행합니다.

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Samba 도메인 컨트롤러에서 스키마 업데이트를 활성화합니다. 이렇게 하려면 `/etc/samba/smb.conf` 파일에 다음 행을 추가합니다.

   ```
   dsdb:schema update allowed = true
   ```

   스키마 업데이트가 오류와 함께 완료되면 스키마 마스터 역할을 하는 도메인 컨트롤러의 전체 복원을 수행해야 합니다.

Samba 도메인 컨트롤러 내의 모든 Linux 기반 호스트에 대해 `/etc/samba/smb.conf` 파일에서 `netbios name`과 `workgroup` 매개변수를 지정합니다. 그렇지 않으면 검색 결과에 중복 호스트가 포함될 수 있습니다.

미할당 기기에 대한 보존 규칙 구성

Windows 네트워크 검색이 완료되면 발견된 기기가 미할당 기기 관리 그룹의 하위 그룹에 배치됩니다. 이 관리 그룹은 **발견 및 배포 → 발견 → Windows 도메인**에 있습니다. **Windows 도메인** 폴더가 부모 그룹입니다. 이 폴더에는 검색 중에 발견된 해당 도메인과 작업 그룹의 이름이 지정된 자식 그룹이 포함됩니다. 모바일 기기의 관리 그룹도 부모 그룹에 포함될 수 있습니다. 부모 그룹과 각 자식 그룹에 대해 미할당 기기의 보존 규칙을 구성할 수 있습니다. 보존 규칙은 기기 발견 설정에 따라 달라지지 않으며 기기 발견을 비활성화해도 작동합니다.

기기 보관 규칙은 전체 디스크 암호화로 암호화된 하나 이상의 드라이브가 있는 기기에 영향을 주지 않습니다. 이러한 기기는 자동 삭제되지 않으며 수동으로만 삭제할 수 있습니다. 암호화된 드라이브가 있는 기기를 삭제하려면, 먼저 드라이브를 복호화한 후 기기를 삭제하십시오.

미할당 기기에 대한 보존 규칙을 구성하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **발견 및 배포** → **발견** → **Windows 도메인**로 이동합니다.
2. 다음 중 하나를 수행합니다:
   - 부모 그룹의 설정을 구성하려면 **속성** 버튼을 누릅니다.
     Windows 도메인 속성 창이 열립니다.
   - 자식 그룹의 설정을 구성하려면 그룹 이름을 누릅니다.
     하위 그룹 속성 창이 열립니다.
3. 다음 설정을 정의합니다:
   - **기기가 다음 비활성 기간을 초과하면 그룹에서 기기 제거(일)**

     이 옵션을 활성화하면 기기가 그룹에서 자동으로 제거될 때까지의 시간 간격을 지정할 수 있습니다. 기본적으로 이 옵션은 자식 그룹에도 배포됩니다. 기본 기간은 7일입니다.
     기본적으로 이 옵션은 켜져 있습니다.
   - **부모 그룹에서 상속**

     이 옵션을 활성화하면 현재 그룹에 있는 기기의 보존 기간이 부모 그룹에서 상속되며 변경할 수 없습니다.
     이 옵션은 자식 그룹에만 사용할 수 있습니다.
     기본적으로 이 옵션은 켜져 있습니다.
   - **자식 그룹에 강제 상속**

     이 설정 값은 자식 그룹에 배포되지만 자식 그룹의 속성에서는 이러한 설정이 잠깁니다.
     기본적으로 이 옵션은 비활성화되어 있습니다.
4. **수락** 버튼을 누릅니다.

변경 내용이 저장 및 적용됩니다.

장비 재고

장비 재고를 관리하는 데 사용하는 하드웨어 목록(**동작** → **저장소** → **하드웨어**)은 자동 및 수동이라는 두 가지 방식으로 채워집니다. 네트워크 폴링 후마다 감지된 모든 기기가 목록에 자동으로 추가되지만, 네트워크를 폴링하지 않으려는 경우에는 기기를 수동으로 추가할 수도 있습니다. 예를 들어 라우터, 프린터 또는 기기 하드웨어와 같은 다른 기기를 목록에 수동으로 추가할 수 있습니다.

기기의 속성에서 기기에 대한 자세한 정보를 보고 편집할 수 있습니다.

하드웨어 목록에는 다음 유형의 기기가 포함될 수 있습니다.

- 컴퓨터
- 모바일 기기
- 네트워크 기기
- 가상 기기
- OEM 구성 요소
- 컴퓨터 주변 기기
- 연결된 기기
- VoIP 폰
- 네트워크 저장소

관리자는 *기업 장비* 속성을 탐지된 기기에 할당할 수 있습니다. 이 특성은 기기의 속성에서 수동으로 할당되거나 관리자가 자동으로 할당할 특성의 기준을 지정할 수 있습니다. 이 경우 *기업 장비* 속성은 기기 유형별로 할당됩니다.

Kaspersky Security Center는 장비를 목록에서 제외할 수 있습니다. 이렇게 하려면 기기 속성에서 **쓰기 금지** 옵션을 선택합니다. 기기는 장비 목록에 표시되지 않습니다.

관리자는 **하드웨어** 폴더에서 프로그램 가능 논리 컨트롤러(PLC)의 목록을 관리할 수 있습니다. PLC 목록 관리에 대한 자세한 내용은 *Kaspersky Industrial CyberSecurity for Nodes 사용자 설명서*에 나와 있습니다.

새 기기에 대한 정보 추가

네트워크의 새 기기에 대한 정보를 추가하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작** → **저장소** → **하드웨어**로 이동합니다.
2. **추가** 버튼을 클릭하여 **새로운 기기** 창을 엽니다.
3. **새로운 기기** 창의 **기기 유형** 드롭다운 목록에서 추가하려는 기기 유형을 선택합니다.
4. **확인**를 누릅니다.
   기기 속성 창이 **일반** 섹션에 열립니다.
5. **일반** 섹션의 입력 필드에 기기의 데이터를 입력합니다. **일반** 섹션에는 다음과 같은 설정이 나와 있습니다:
   - **기업 기기**. 기기에 *기업* 속성을 지정하려면 이 확인란을 선택합니다. 이 특성을 사용하여 **하드웨어** 폴더에서 기기를 검색할 수 있습니다.
   - **쓰기 금지**. **하드웨어** 폴더에서 기기의 목록에 기기를 표시하지 않으려면 이 확인란을 선택합니다.
6. **적용**을 누릅니다.

새 기기가 **하드웨어** 페이지의 작업 영역에 표시됩니다.

기업 기기를 정의하는 데 사용한 기준 구성

기업 기기의 탐지 기준을 구성하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 저장소 → 하드웨어**로 이동합니다.
2. **하드웨어** 페이지 상단에서 **기업 기기에 대한 규칙 설정** 링크를 클릭합니다.
   기업 기기에 대한 규칙 설정 패널이 호출됩니다.
3. **기업 기기에 대한 규칙 설정** 패널에서 **자동으로 기업 기기 속성 설정**을 활성화합니다. *기업* 속성을 자동으로 할당할 기기 유형을 지정합니다.

   이 옵션은 네트워크 폴링을 통해 추가된 기기에만 영향을 줍니다. 수동으로 추가한 기기의 경우 *기업* 특성을 수동으로 설정합니다.

4. **확인**을 누릅니다.

기업 기기에 대한 탐지 기준이 구성됩니다.

Kaspersky 애플리케이션: 라이센싱 및 활성화

이 섹션에서는 관리 중인 Kaspersky 애플리케이션의 라이센스 키 처리와 관련된 Kaspersky Security Center의 기능에 대해 설명합니다.

Kaspersky Security Center에서는 중앙 집중식으로 클라이언트 기기에 Kaspersky 애플리케이션 라이센스 키를 배포하고 기기의 라이센스 키 사용을 감시하며 라이센스를 갱신할 수 있습니다.

Kaspersky Security Center를 사용하여 라이센스 키를 추가하는 경우, 라이센스 키 설정이 중앙 관리 서버에 저장됩니다. 이 정보를 기반으로 애플리케이션은 라이센스 키 사용에 관한 리포트를 생성하고 라이센스가 만료되거나 라이센스 키 속성에 의해 적용된 라이센스 제한을 초과하는 경우 관리자에게 이를 알립니다. 중앙 관리 서버 설정 내에서 라이센스 키 사용에 대한 알림을 구성할 수 있습니다.

관리 애플리케이션 라이센싱

관리 중인 기기에 설치된 Kaspersky 애플리케이션은 각 애플리케이션에 키 파일 또는 활성화코드를 적용하여 라이센스를 부여받아야 합니다. 키 파일 또는 활성화코드는 다음과 같은 방법으로 배포할 수 있습니다:

- 자동 배포
- 관리 중인 애플리케이션의 설치 패키지
- 관리 중인 애플리케이션에 대한 *라이센스 키 추가* 작업
- 관리 중인 애플리케이션의 수동 활성화

위에 방법 중 하나를 사용하여 새 활성 또는 예약 라이센스 키를 추가할 수 있습니다. Kaspersky 애플리케이션은 현재 활성 키를 사용하고 활성 키가 만료된 후 적용할 예약 키를 저장합니다. 라이센스 키를 추가할 애플리케이션이 키의 활성 또는 예약 여부를 정의합니다. 키 정의는 새 라이센스 키를 추가하는 방법에 따라 달라지지 않습니다.

자동 배포

다른 관리 중인 애플리케이션을 사용하고 있으며 특정 키 파일 또는 활성화코드를 그 기기에 배포해야 하는 경우 해당 활성화코드 또는 키 파일을 배포하는 다른 방법을 선택합니다.

Kaspersky Security Center를 사용하면 기기에 사용 가능한 라이센스 키를 자동으로 배포할 수 있습니다. 예를 들어 세 개의 라이센스 키가 중앙 관리 서버 저장소에 저장됩니다. 라이센스 키 세 개 모두에 대하여 **관리 중인 기기에 자동으로 라이센스 키 배포** 확인란을 선택하였습니다. 그리고, Kaspersky 보안 제품(예, Kaspersky Endpoint Security for Windows)이 기업의 기기에 설치됩니다. 라이센스 키를 배포해야 하는 새 기기가 발견됩니다. 애플리케이션은 적용 가능한 라이센스 키를 결정합니다. 저장소에 추가된 라이센스 키 중 두 개(이름이 *key_1*과 *key_2*인 키)의 라이센스 키가 해당 기기에 배포할 수 있습니다. 이러한 라이센스 키 중 하나가 기기에 배포됩니다. 이 경우, 라이센스 키 자동 배포는 관리자가 시작한 작업이 아니기 때문에 적용 가능한 두 라이센스 키 중 어느 라이센스 키가 기기에 배포될지 예측할 수 없습니다.

라이센스 키가 배포되면, 해당 기기는 그 라이센스 키가 적용된 기기로 카운터됩니다. 라이센스 키가 배포된 기기 수가 라이센스 제한을 초과하지 않는지 확인해야 합니다. 기기 수가 라이센스 제한을 초과하면, 해당 라이센스로 적용할 수 없는 모든 기기에 대해 *심각* 상태가 할당됩니다.

배포하기 전에 키 파일 또는 활성화코드를 중앙 관리 서버 저장소에 추가해야 합니다.

방법 지침:

- 관리 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 라이센스 키 자동 배포

  또는
- Kaspersky Security Center 웹 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 라이센스 키 자동 배포

다음 경우에는 자동 배포된 라이센스 키가 가상 중앙 관리 서버 저장소에 표시되지 않을 수 있습니다:

- 애플리케이션에 대한 라이센스 키가 유효하지 않습니다.
- 가상 중앙 관리 서버에 관리 중인 기기가 없습니다.
- 다른 가상 중앙 관리 서버에서 관리하는 기기에서 이미 해당 라이센스 키를 사용했으며 기기 수 제한에 도달했습니다.

관리 중인 애플리케이션의 설치 패키지에 키 파일 또는 활성화코드 추가

보안상의 이유로 이 옵션은 사용하지 않는 것이 좋습니다. 설치 패키지에 추가된 키 파일 또는 활성화코드에 문제가 생길 수 있습니다.

설치 패키지를 사용하여 관리 중인을 설치하는 경우 이 설치 패키지 또는 애플리케이션의 정책에서 활성화코드 또는 키 파일을 지정할 수 있습니다. 라이센스 키는 기기와 중앙 관리 서버를 다음에 동기화할 때 관리 중인 기기에 배포됩니다.

방법 지침:

- 관리 콘솔:
  - 설치 패키지 만들기
  - 클라이언트 기기에 애플리케이션 설치

  또는
- Kaspersky Security Center 웹 콘솔: 설치 패키지에 라이센스 키 추가

관리 중인 애플리케이션에 대해 라이센스 키 추가 작업을 실행하여 배포

만일 관리 중인 애플리케이션에 대해 *라이센스 키* 추가 작업을 한다면, 기기에 배포해야 하는 라이센스 키를 선택하고 관리 그룹 또는 기기 조회와 같은 여러 편리한 방법으로 대상 기기를 선택할 수 있습니다.

배포하기 전에 키 파일 또는 활성화코드를 중앙 관리 서버 저장소에 추가해야 합니다.

방법 지침:

- 관리 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 클라이언트 기기에 라이센스 키 배포

  또는
- Kaspersky Security Center 웹 콘솔:
  - 중앙 관리 서버 저장소에 라이센스 키 추가
  - 클라이언트 기기에 라이센스 키 배포

기기에 수동으로 활성화코드 또는 키 파일 추가

애플리케이션 인터페이스에 제공된 도구를 사용하여 설치된 Kaspersky 애플리케이션을 로컬에서 활성화할 수 있습니다. 자세한 내용은 설치하려는 애플리케이션의 설명서를 참조하십시오.

중앙 관리 서버 저장소에 라이센스 키 추가

중앙 관리 서버 저장소에 라이센스 키를 추가하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 라이센스 → Kaspersky 라이센스** 로 이동합니다.
2. **추가** 버튼을 누릅니다.
3. 다음 중 추가할 항목을 선택하십시오.
   - **키 파일 추가**
     키 파일 선택 버튼을 누르고 추가하려는 키 파일을 검색합니다.
   - **활성화 코드 입력**
     텍스트 필드에서 활성화코드를 지정하고 **보내기** 버튼을 누릅니다.
4. **닫기** 버튼을 누릅니다.

라이센스 키 하나 또는 여러 개가 중앙 관리 서버 저장소에 추가됩니다.

중앙 관리 서버 라이센스 키 추가

중앙 관리 서버 라이센스 키를 추가하려면:

1. 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창이 열리면 **라이센스 키** 섹션을 선택합니다.
3. **활성 라이센스 키** 섹션에서 **편집** 버튼을 클릭합니다.
4. 창이 열리면 **추가** 버튼을 클릭하여 라이센스 키를 추가합니다.
   라이센스 키 추가 마법사가 시작됩니다.

마법사가 완료되면 해당 라이선스에 따라 관리 콘솔에 기능이 표시되는지 확인할 수 있습니다.

클라이언트 기기에 라이센스 키 배포

Kaspersky Security Center 웹 콘솔에서는 **애플리케이션 활성화** 작업을 사용하거나 자동으로 클라이언트 기기에 라이센스 키를 배포할 수 있습니다. 이 작업을 사용하여 특정 기기 그룹에 키를 배포할 수 있습니다. 작업을 통해 라이선스 키를 배포할 때는 기기 수에 대한 라이선스 제한은 고려되지 않습니다. 자동 키 배포를 사용하여 라이센스 제한에 도달 시 라이센스 키 배포를 자동으로 중지합니다.

라이센스 키 자동 배포를 활성화한 경우 해당 키를 클라이언트 기기에 배포하기 위해 **애플리케이션 활성화** 작업을 생성하지 마십시오. 빈번한 동기화로 인해 중앙 관리 서버의 부하가 증가합니다.

배포 전에 중앙 관리 서버 저장소에 라이센스 키를 추가하십시오.

***애플리케이션 활성화** 작업으로 클라이언트 기기에 라이센스 키를 배포하려면 다음을 따르십시오.*

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. **애플리케이션** 드롭다운 목록에서 라이센스 키를 추가하려는 애플리케이션을 선택합니다.
4. **작업 유형** 목록에서 **애플리케이션 활성화** 작업을 선택합니다.
5. **작업 이름** 필드에 새 작업의 이름을 지정합니다.
6. 이 작업이 할당되는 기기를 선택합니다.
7. 마법사의 **라이센스 키 선택** 단계에서 **키 추가** 링크를 클릭하여 라이센스 키를 추가합니다.
8. 키 추가 창에서 다음 옵션 중 하나를 사용하여 라이센스 키를 추가합니다.

   애플리케이션 활성화 작업을 생성하기 전에 중앙 관리 서버 저장소에 라이센스 키를 추가하지 않았을 때만 라이센스 키를 추가해야 합니다.

   - **활성화 코드 입력** 옵션을 선택하여 활성화 코드를 입력한 후 다음을 수행합니다.

     a. 활성화 코드를 지정한 후 **보내기** 버튼을 클릭합니다.
     키 추가 창에 라이센스 키 정보가 나타납니다.

     b. **저장** 버튼을 누릅니다.

     라이선스 키를 관리 중인 기기에 자동 배포하려면 **관리 중인 기기에 자동으로 라이센스 키 배포** 옵션을 활성화합니다.

     키 추가 창이 닫힙니다.

   - **키 파일 추가** 옵션을 선택하여 키 파일을 추가하고 다음을 수행합니다.

     a. **키 파일 선택** 버튼을 클릭합니다.

     b. 창이 열리면 키 파일을 선택한 다음 **열기** 버튼을 클릭합니다.
     라이센스 키 추가 창에 라이센스 키 정보가 나타납니다.

     c. **저장** 버튼을 누릅니다.

     라이선스 키를 관리 중인 기기에 자동 배포하려면 **관리 중인 기기에 자동으로 라이센스 키 배포** 옵션을 활성화합니다.

     키 추가 창이 닫힙니다.

9. 키 테이블에서 라이선스 키를 선택합니다.

10. 마법사의 **라이센스 정보** 단계에서 활성 라이센스 키를 교체하려면 기본 선택된 **예비 키로 사용** 확인란을 선택 해제합니다.

    예를 들어 조직이 변경되어 다른 조직의 키가 기기에서 필요하거나 키가 재발급되어 새 라이센스가 현재 라이센스보다 빨리 만료되는 경우에 필요합니다. 오류를 방지하려면 **예비 키로 사용** 확인란을 선택 해제해야 합니다.

    Kaspersky Security Center에 라이센스 키를 추가할 때 발생할 수 있는 문제와 이를 해결하는 방법에 대한 자세한 내용은 Kaspersky Security Center 기술 자료를 참조하십시오.

11. 마법사의 **작업 생성 마침** 단계에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화하면 기본 작업 설정을 수정할 수 있습니다.

    이 옵션을 활성화하지 않으면 작업이 기본 설정으로 생성됩니다. 나중에 기본 설정을 수정할 수 있습니다.

12. **마침** 버튼을 누릅니다.

    마법사가 작업을 생성합니다. **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화하면 작업 속성 창이 자동으로 열립니다. 이 창에서는 일반 작업 설정을 지정할 수 있으며, 필요하다면 작업 생성 중에 지정된 설정을 변경할 수 있습니다.

    > 작업 목록에서 생성된 작업 이름을 클릭하여 작업 속성 창을 열 수도 있습니다.

    작업이 생성 및 구성되고 작업 목록에 표시됩니다.

13. 작업을 실행하려면 작업 목록에서 작업을 선택하고 **시작** 버튼을 누릅니다.

    작업 속성 창의 **스케줄** 탭에서 작업 시작 일정을 설정할 수도 있습니다.

    스케줄된 시작 설정에 대한 자세한 설명은 일반 작업 설정을 참조하십시오.

작업이 완료되면 라이선스 키가 선택한 기기에 배포됩니다.

라이센스 키 자동 배포

라이센스 키가 중앙 관리 서버의 라이센스 키 저장소에 있는 경우 Kaspersky Security Center에서 관리 중인 기기에 라이센스 키를 자동으로 배포할 수 있습니다.

관리 중인 기기에 라이센스 키를 자동으로 배포하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 라이센스 → Kaspersky 라이센스** 로 이동합니다.
2. 자동으로 배포하려고 하는 라이센스 키의 이름을 누릅니다.
3. 열린 라이센스 키 속성 창에서 **관리 중인 기기에 자동으로 라이센스 키 배포** 확인란을 선택합니다.
4. **저장** 버튼을 누릅니다.

라이센스 키는 모든 호환 기기에 자동으로 배포됩니다.

라이센스 키 배포는 네트워크 에이전트를 통해 수행됩니다. 애플리케이션에 대한 라이센스 키 배포 작업은 만들어지지 않습니다.

라이센스 키를 자동 배포할 때는 기기 수에 대해 라이센스 제한을 고려합니다. 라이센스 제한은 라이센스 키의 속성에 설정되어 있습니다. 만일 라이센스 구매 수량에 도달하면, 기기로의 이 라이센스 키 배포는 자동으로 중단됩니다.

다음 경우에는 자동 배포된 라이센스 키가 가상 중앙 관리 서버 저장소에 표시되지 않을 수 있습니다:

- 애플리케이션에 대한 라이센스 키가 유효하지 않습니다.
- 가상 중앙 관리 서버에 관리 중인 기기가 없습니다.
- 다른 가상 중앙 관리 서버에서 관리하는 기기에서 이미 해당 라이센스 키를 사용했으며 기기 수 제한에 도달했습니다.

가상 중앙 관리 서버가 해당 저장소와 중앙 관리 서버의 저장소에서 라이센스 키를 자동으로 배포합니다. 다음을 수행할 것을 권장합니다:

- *라이센스 키 추가* 작업을 사용하여 기기에 배포할 라이센스 키를 선택합니다.
- 가상 중앙 관리 서버 설정에서 **이 가상 중앙 관리 서버에서 소속된 기기로 라이센스 키 자동 배포 허용** 옵션을 비활성화하지 마십시오. 그렇지 않으면 가상 중앙 관리 서버가 중앙 관리 서버 저장소의 라이센스 키를 포함해 라이센스 키를 기기에 배포하지 않습니다.

라이센스 키 속성 창에서 **관리 중인 기기에 자동으로 라이센스 키 배포** 확인란을 선택하면 라이센스 키가 네트워크에 즉시 배포됩니다. 이 옵션을 선택하지 않으면 나중에 이 작업을 사용하여 라이센스 키를 배포할 수 있습니다.

기본 중앙 관리 서버에 구성된 라이센스 키의 자동 배포는 가상이 아닌 보조 중앙 관리 서버에서 관리 중인 기기로 확장되지 않습니다.

사용 중인 라이센스 키 정보 보기

중앙 관리 서버 저장소에 추가된 라이센스 키 목록을 보려면 다음 단계를 따릅니다.

메인 메뉴에서 **동작 → 라이센스 → Kaspersky 라이센스** 로 이동합니다.

표시된 목록에는 중앙 관리 서버 저장소에 추가된 키 파일 및 활성화코드가 포함되어 있습니다.

라이센스 키에 대한 자세한 정보를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 라이센스 → Kaspersky 라이센스** 로 이동합니다.
2. 필요한 라이센스 키의 이름을 누릅니다.

라이센스 키 속성 창이 열리면 다음을 확인할 수 있습니다.

- **일반** 탭 - 라이센스 키에 대한 기본 정보
- **기기** 탭 - 설치된 Kaspersky 애플리케이션의 활성화에 라이센스 키가 사용된 클라이언트 기기 목록

특정 클라이언트 기기에 배포된 라이센스 키를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기** 로 이동합니다.
2. 필요한 기기의 이름을 누릅니다.
3. 기기 속성 창이 열리면 **애플리케이션** 탭을 선택합니다.

4. 라이센스 키에 대한 정보를 보려는 애플리케이션의 이름을 누릅니다.

5. 애플리케이션 속성 창이 열리면 **일반** 탭을 누른 다음 **라이센스** 섹션을 엽니다.

활성 및 예약 라이센스 키에 대한 기본 정보가 표시됩니다.

가상 중앙 관리 서버 라이센스 키의 최신 설정을 정의하기 위해 해당 중앙 관리 서버는 하루에 한 번 이상 Kaspersky 활성화 서버에 요청을 보냅니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다.

저장소에서 라이센스 키 삭제

취약점 및 패치 관리 또는 모바일 기기 관리와 같은 중앙 관리 서버의 추가 기능에 대한 활성 라이센스 키를 삭제하면 해당 기능을 사용할 수 없습니다. 예약 라이센스 키가 추가된 경우, 기존 활성 라이센스 키가 삭제된 후에 예약 라이센스 키가 활성 라이센스 키로 자동 전환됩니다.

관리 중인 기기에 배포된 활성 라이센스 키를 삭제하면 애플리케이션이 관리 중인 기기에서 계속 작동합니다.

중앙 관리 서버 저장소에서 키 파일 또는 활성화코드를 삭제하려면 다음 단계를 따릅니다.

1. 삭제하려는 키 파일이나 활성화 코드를 중앙 관리 서버에서 사용하고 있는지 확인하십시오. 중앙 관리 서버에서 사용 중이라면, 키를 삭제할 수 없습니다. 확인하려면:

   a. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.

   b. **일반** 탭에서 **라이센스 키** 섹션을 선택합니다.

   c. 열린 섹션에서 필요한 키 파일 또는 활성화 코드가 표시되면 **활성 라이센스 키 제거** 버튼을 클릭한 다음 작업을 확인합니다. 이제 중앙 관리 서버는 삭제된 라이센스 키를 사용하지 않지만 키는 중앙 관리 서버 저장소에 남아 있습니다. 필요한 키 파일이나 활성화 코드가 표시되지 않는다면, 중앙 관리 서버에서 이를 사용하지 않습니다.

2. 메인 메뉴에서 **동작** → **라이센스** → **Kaspersky 라이센스**로 이동합니다.

3. 필요한 키 파일 또는 활성화 코드를 선택한 다음 **삭제** 버튼을 클릭합니다.

선택한 키 파일 또는 활성화 코드가 저장소에서 삭제됩니다.

삭제된 라이센스 키를 다시 추가하거나 새 라이센스 키를 추가할 수 있습니다.

최종 사용자 라이센스 계약서 동의 취소

일부 클라이언트 기기의 보호를 중지하기로 결정한 경우 관리 중인 모든 Kaspersky 애플리케이션에 대한 EULA(최종 사용자 라이센스 계약서)를 취소할 수 있습니다. EULA를 취소하기 전에 선택한 애플리케이션을 제거해야 합니다.

가상 중앙 관리 서버에서 승인된 EULA는 가상 중앙 관리 서버 또는 기본 중앙 관리 서버에서 취소할 수 있습니다. 기본 Administration Server에서 승인된 EULA는 기본 Administration Server에서만 취소할 수 있습니다.

관리 중인 Kaspersky 애플리케이션의 EULA를 취소하려면 다음 절차를 따르십시오.

1. 중앙 관리 서버 속성 창을 열고 **일반**탭에서 **최종 사용자 라이센스 계약서** 섹션을 선택합니다.

   설치 패키지 생성 시, seamless 업데이트 설치 시, 또는 Kaspersky Security for Mobile 배포 시 동의한 EULA 목록이 표시됩니다.

2. 목록에서 동의를 취소할 EULA를 선택합니다.

   EULA에 관하여 다음 속성을 볼 수 있습니다.

   - EULA에 동의한 날짜.
   - EULA에 동의한 사용자 이름.

3. EULA의 동의 날짜를 눌러 다음 데이터를 표시하는 속성 창을 엽니다.

   - EULA에 동의한 사용자 이름.
   - EULA에 동의한 날짜.
   - EULA의 고유 식별자(UID).
   - EULA의 전문.
   - EULA에 연결된 개체(설치 패키지, seamless 업데이트, 모바일 앱) 목록과 해당 이름 및 유형.

4. EULA 속성 창 하단에서 **라이센스 계약서 취소** 버튼을 누릅니다.

   > EULA가 취소되지 않도록 하는 개체(설치 패키지 및 해당 작업)가 있는 경우 해당 알림이 표시됩니다. 이러한 개체를 삭제할 때까지 취소를 진행할 수 없습니다.

   열린 창에서 해당 EULA와 연관된 Kaspersky 애플리케이션을 먼저 제거해야 한다는 메시지가 표시됩니다.

5. 버튼을 눌러 취소를 확인하십시오.

EULA가 취소됩니다. **최종 사용자 라이센스 계약서** 섹션의 라이센스 계약서 목록에 더 이상 표시되지 않습니다. EULA 속성 창이 닫힙니다. 애플리케이션이 더 이상 설치되지 않습니다.

Kaspersky 애플리케이션 라이선스 갱신

만료되었거나 만료 예정인(30일 이내) Kaspersky 애플리케이션 라이센스를 갱신할 수 있습니다.

만료된 라이센스 또는 만료 예정인 라이센스를 갱신하려면 다음과 같이 하세요.

1. 다음 중 하나를 수행합니다.

   - 메인 메뉴에서 **동작 → 라이센스 → Kaspersky 라이센스**으로 이동합니다.
   - 메인 메뉴에서 **모니터링 및 보고 → 대시보드**로 이동한 다음 알림 옆에 있는 **만료되는 라이센스 보기** 링크를 클릭합니다.

   라이센스를 보고 갱신할 수 있는 **Kaspersky 라이센스** 창이 열립니다.

2. 필요한 라이센스 옆의 **라이센스 갱신** 링크를 클릭합니다.

   라이센스 갱신 링크를 클릭하면 Kaspersky Security Center의 버전, 사용 중인 현지화, 소프트웨어 라이센스 ID(즉, 갱신하려는 라이센스의 ID) 및 파트너 회사를 통해 라이센스를 구매했는지 여부에 대한 정보를 Kaspersky에 전송하는 데 동의한 것으로 간주됩니다.

3. 라이센스 갱신 서비스 창이 열리면 지침에 따라 라이센스를 갱신합니다.

   라이센스가 갱신됩니다.

라이센스가 만료되려고 하면 Kaspersky Security Center 웹 콘솔에서 다음 스케줄에 따라 알림이 표시됩니다:

- 만료 30일 전
- 만료 7일 전
- 만료 3일 전
- 만료 24시간 전
- 라이센스가 만료된 때

Kaspersky Marketplace를 사용하여 Kaspersky 비즈니스 솔루션 선택

마켓플레이스는 메인 메뉴의 한 섹션으로 Kaspersky 비즈니스 솔루션의 전체 제품군을 보고 필요한 솔루션을 선택하고 Kaspersky 웹사이트에서 구매를 진행할 수 있는 곳입니다. 필터를 사용하여 조직과 정보 보안 시스템의 요구 사항에 맞는 솔루션만 볼 수 있습니다. 솔루션을 선택하면 Kaspersky Security Center에서 해당 솔루션에 대해 자세히 알아볼 수 있도록 Kaspersky 웹사이트의 관련 웹페이지로 리디렉션합니다. 각 웹 페이지에서 구매를 진행하거나 구매 프로세스에 대한 안내를 확인할 수 있습니다.

마켓플레이스 섹션에서는 다음 기준을 사용하여 Kaspersky 솔루션을 필터링할 수 있습니다.

- 보호하려는 기기(엔드포인트, 서버 및 기타 유형의 에셋) 수:
  - 50~250
  - 250–1000
  - 1,000대 이상
- 조직 정보 보안 팀의 성숙도:
  - **기초**

    이 수준은 IT 팀만 있는 기업에 일반적입니다. 가능한 최대 위협 수가 자동으로 차단됩니다.
  - **최적**

    이 수준은 IT 팀 내에 특정 IT 보안 기능이 있는 기업에 일반적입니다. 이 수준의 기업에게는 일반적인 위협과 기존 예방 메커니즘을 우회하는 위협에 대응할 수 있는 솔루션이 필요합니다.

- **전문**

  이 수준은 복잡하고 분산된 IT 환경을 가진 기업에 일반적입니다. IT 보안 팀이 성숙하거나 회사에 SOC(보안 운영 센터) 팀이 있습니다. 필요한 솔루션을 통해 기업은 복잡한 위협과 표적 공격에 대응할 수 있습니다.

- 보호하려는 자산 유형:
  - **엔드포인트**: 직원의 워크스테이션, 물리적 머신 및 가상 머신, 임베디드 시스템
  - **서버**: 물리적 서버 및 가상 서버
  - **클라우드**: 퍼블릭, 프라이빗 또는 하이브리드 클라우드 환경, 클라우드 서비스
  - **네트워크**: 근거리통신망, IT인프라
  - **서비스**: Kaspersky에서 제공하는 보안 관련 서비스

Kaspersky 비즈니스 솔루션을 찾고 구매하려면:

1. 메인 메뉴에서 **마켓플레이스**로 이동합니다.

   기본적으로 이 섹션에는 구매 가능한 모든 Kaspersky 비즈니스 솔루션이 표시됩니다.

2. 조직에 적합한 솔루션만 보려면 필터에서 필요한 값을 선택하십시오.

3. 구매를 원하거나 자세히 알고 싶은 솔루션을 클릭하십시오.

   해당 솔루션 웹페이지로 리디렉션됩니다. 화면의 지시에 따라 구매를 진행할 수 있습니다.

네트워크 보호 구성

이 섹션에는 정책 및 작업의 수동 구성, 사용자 역할, 관리 그룹 구조 및 작업 계층 구축에 대한 정보가 포함되어 있습니다.

시나리오: 네트워크 보호 구성

빠른 시작 마법사는 기본 설정을 통해 정책 및 작업을 만듭니다. 이러한 설정은 조직에 가장 적합하지 않을 수도 있고 조직에서 허용되지 않을 수도 있습니다. 따라서 네트워크에 필요한 경우 이러한 정책과 작업을 미세 조정하고 다른 정책과 작업을 만드는 것이 좋습니다.

필수 구성 요소

시작하기 전에 다음을 수행했는지 확인하십시오:

- Kaspersky Security Center 중앙 관리 서버 설치
- Kaspersky Security Center 웹 콘솔 설치(선택 사항)
- Kaspersky Security Center 주요 배포 시나리오 완료됨

- 빠른 시작 마법사 완료 또는 **관리 중인 기기** 관리 그룹에서 다음 정책과 작업을 수동으로 생성:
  - Kaspersky Endpoint Security 정책
  - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업
  - 네트워크 에이전트의 정책
  - *취약점 및 필요한 업데이트 검색* 작업

네트워크 보호 구성은 다음 단계로 진행됩니다:

1. **Kaspersky 애플리케이션 정책과 정책 프로필 설정 및 전파**

   관리 중인 기기에 설치되어 있는 Kaspersky 애플리케이션의 설정을 구성하고 전파하려는 경우 두 가지 보안 관리 방식, 즉 기기 중심 방식이나 사용자 중심 방식 중 하나를 사용할 수 있습니다. 이 두 방식을 조합하여 사용할 수도 있습니다. 기기 중심 보안 관리를 구현하려는 경우 Microsoft Management Console 기반 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 제공되는 도구를 사용할 수 있습니다. 사용자 중심 보안 관리는 Kaspersky Security Center 웹 콘솔을 통해서만 구현할 수 있습니다.

2. **Kaspersky 애플리케이션 원격 관리용 작업 구성**

   빠른 시작 마법사에서 생성된 작업을 확인하고 필요하다면 조정합니다.

   방법 지침:

   - 관리 콘솔:
     - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업 설정
     - 취약점 및 필요한 업데이트 검색 작업 스케줄 지정
   - Kaspersky Security Center 웹 콘솔:
     - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업 설정
     - 취약점 및 필요한 업데이트 검색 작업 설정

   필요한 경우 클라이언트 기기에 설치된 Kaspersky 애플리케이션을 관리하기 위한 추가 작업을 생성합니다.

3. **데이터베이스의 이벤트 부하 평가 및 제한**

   클라이언트 기기에서 관리 중인 애플리케이션 작업 중 발생하는 이벤트 정보가 전송되어 중앙 관리 서버 데이터베이스에 등록됩니다. 중앙 관리 서버의 부하를 줄이려면 데이터베이스에 저장할 수 있는 최대 이벤트 수를 평가 및 제한합니다.

   방법 지침:

   - 관리 콘솔: 최대 이벤트 수 설정
   - Kaspersky Security Center 웹 콘솔: 최대 이벤트 수 설정

결과

이 시나리오를 완료하면 중앙 관리 서버에서 수신하는 Kaspersky 애플리케이션, 작업 및 이벤트 구성을 통해 네트워크가 보호됩니다.

- Kaspersky 애플리케이션은 정책 및 정책 프로필에 따라 구성됩니다.
- 애플리케이션은 일련의 작업을 통해 관리됩니다.
- 데이터베이스에 저장할 수 있는 최대 이벤트 수가 설정됩니다.

네트워크 보호 구성이 완료되면 Kaspersky 데이터베이스 및 애플리케이션에 대한 정기 업데이트를 구성할 수 있습니다.

Kaspersky Sandbox에서 탐지한 위협에 대한 자동 대응을 구성하는 방법은 Kaspersky Sandbox 2.0 온라인 도움말을 참조하십시오.

기기 중심 및 사용자 중심 보안 관리 방식 정보

기기 기능 및 사용자 역할 측면에서 보안 설정을 관리할 수 있습니다. 기기 기능 측면의 관리 방식은 *기기 중심 보안 관리*이고 사용자 역할 측면의 관리 방식은 *사용자 중심 보안 관리*입니다. 기기마다 서로 다른 애플리케이션 설정을 적용하려는 경우 두 관리 유형 중 하나를 사용하거나 두 유형을 조합하여 사용할 수 있습니다. 기기 중심 보안 관리를 구현하려면 Microsoft Management Console 기반 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 제공되는 도구를 사용할 수 있습니다. 사용자 중심 보안 관리는 Kaspersky Security Center 웹 콘솔을 통해서만 구현할 수 있습니다.

기기 중심 보안 관리를 통해 기기별 기능에 따라 다양한 보안 제품 설정을 관리 중인 기기에 적용할 수 있습니다. 예를 들어, 다른 관리 그룹에 할당된 기기에 다른 설정을 적용할 수 있습니다. Active Directory에서의 기기 사용이나 하드웨어 사양에 따라 기기를 차별화할 수도 있습니다.

사용자 중심 보안 관리를 통해 사용자 역할에 따라 다른 보안 제품을 적용할 수 있습니다. 여러 개의 사용자 역할을 만들고, 각 사용자에게 적절한 사용자 역할을 할당하고, 서로 다른 역할의 사용자가 소유한 기기에 다양한 애플리케이션 설정을 정의할 수 있습니다. 경리 직원과 HR(인사) 전문가의 기기에 서로 다른 애플리케이션 설정을 적용하려는 경우를 예로 들 수 있습니다. 따라서 사용자 중심의 보안 관리를 구현할 때 각 부서(계정 부서 및 HR 부서)에는 Kaspersky 애플리케이션에 대한 고유한 설정 구성이 있습니다. 설정 구성은 사용자가 변경할 수 있는 애플리케이션 설정과 관리자가 강제로 설정하고 잠금 설정을 정의합니다.

사용자 중심 보안 관리를 사용하면 개별 사용자에게 특정 애플리케이션 설정을 적용할 수 있습니다. 회사 내의 특정 직원에게 고유한 역할이 지정되어 있거나, 특정인의 기기와 관련된 보안 문제를 모니터링하려는 경우 이러한 방식을 사용할 수 있습니다. 회사 내 역할에 따라 해당 직원이 애플리케이션 설정을 변경하는 권한을 확장하거나 제한할 수 있습니다. 예를 들어 지역 사무소에서 클라이언트 기기를 관리하는 시스템 관리자의 권한을 확장할 수 있습니다.

기기 중심 및 사용자 중심 보안 관리 방식을 조합하여 사용할 수도 있습니다. 예를 들어 각 관리 그룹용으로 특정 애플리케이션 정책을 구성한 다음 기업의 사용자 역할 하나 또는 여러 개에 대해 정책 프로필을 만들 수 있습니다. 이 경우 정책 및 정책 프로필은 다음 순서로 적용됩니다:

1. 기기 중심 보안 관리용으로 만든 정책이 적용됩니다.
2. 이러한 정책은 정책 프로필 우선 순위에 따라 정책 프로필을 통해 수정됩니다.
3. 사용자 역할과 연결된 정책 프로필을 통해 정책이 수정됩니다.

정책 설정 및 전파: 기기 중심 방식

이 시나리오를 완료하면 정의한 애플리케이션 정책 및 정책 프로필에 따라 관리 중인 모든 기기에서 애플리케이션이 구성됩니다.

필수 구성 요소

시작하기 전에 Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔(옵션)을 설치했는지 확인하십시오. Kaspersky Security Center 웹 콘솔을 설치했다면 기기 중심 방식의 대안이나 추가 옵션으로 사용자 중심 보안 관리를 고려할 수도 있습니다.

단계

Kaspersky 애플리케이션의 기기 중심 관리 시나리오는 다음 단계로 구성됩니다:

1. **애플리케이션 정책 구성**

   관리 중인 기기에 설치되어 있는 각 Kaspersky 애플리케이션용 정책을 생성하여 애플리케이션의 설정 구성. 정책 세트는 클라이언트 기기로 전파됩니다.

   빠른 시작 마법사에서 네트워크 보호를 구성할 때 Kaspersky Security Center는 다음 애플리케이션을 위한 기본 정책을 생성합니다:

   - Kaspersky Endpoint Security for Windows - Windows 기반 클라이언트 기기용
   - Kaspersky Endpoint Security for Linux – Linux 기반 클라이언트 기기용

   이 마법사를 사용하여 구성 프로세스를 완료했다면, 이 애플리케이션용으로 새 정책을 생성할 필요가 없습니다. Kaspersky Endpoint Security 정책 수동 설정을 진행합니다.

   여러 중앙 관리 서버 및/또는 관리 그룹이 포함된 계층 구조가 있는 경우 보조 중앙 관리 서버와 자식 관리 그룹은 기본적으로 기본 중앙 관리 서버에서 정책을 상속합니다. 업스트림 정책에 구성된 설정을 수정할 수 없도록 자식 그룹과 보조 중앙 관리 서버의 상속을 강제 적용할 수 있습니다. 설정 중 일부만 강제로 상속되도록 하려는 경우 업스트림 정책에서 해당 설정을 잠글 수 있습니다. 잠금 해제된 나머지 설정은 다운스트림 정책에서 수정할 수 있습니다. 생성된 정책 계층 구조에서는 관리 그룹의 기기를 효율적으로 관리할 수 있습니다.

   방법 지침:

   - 관리 콘솔: 정책 만들기
   - Kaspersky Security Center 웹 콘솔: 정책 생성

2. **정책 프로필 생성(선택 사항)**

   단일 관리 그룹 내의 기기가 각기 다른 정책 설정으로 실행되도록 하려는 경우 해당 기기용 정책 프로필을 생성합니다. 정책 프로필은 정책 설정의 명명된 하위 집합입니다. 이 하위 집합은 정책과 함께 대상 기기에 배포되며 *프로필 활성화 조건*이라는 특수 조건에서 정책을 보완합니다. 관리 중인 기기에서 활성 상태인 "기본" 정책과 다른 설정만 프로필에 포함됩니다.

   프로필 활성화 조건을 사용하면 Active Directory의 특정 단위 또는 보안 그룹에 있거나, 특정 하드웨어 구성을 포함하거나, 특정 태그로 표시된 기기 등에 다른 정책 프로필을 적용할 수 있습니다. 태그를 사용하여 특정 기준을 충족하는 기기를 필터링합니다. 예를 들어 *Windows* 태그를 생성하여 Windows 운영 체제를 실행 중인 모든 기기를 이 태그로 표시한 다음 정책 프로필의 활성화 조건으로 이 태그를 지정할 수 있습니다. 그러면 Windows를 실행 중인 모든 기기에 설치된 Kaspersky 애플리케이션이 자체 정책 프로필을 통해 관리됩니다.

방법 지침:

- 관리 콘솔:
  - 정책 프로필 만들기
  - 정책 프로필 활성화 규칙 만들기
- Kaspersky Security Center 웹 콘솔:
  - 정책 프로필 만들기
  - 정책 프로필 활성화 규칙 만들기

3. **관리 중인 기기로 정책 및 정책 프로필 전파**

   기본적으로 중앙 관리 서버는 15분마다 관리 중인 기기와 자동으로 동기화됩니다. 자동 동기화를 사용하지 않고 강제 동기화 명령을 사용해 동기화를 수동으로 실행할 수 있습니다. 또한 정책 또는 정책 프로필을 생성 및 변경 시 동기화가 강제 실행됩니다. 동기화 중에 신규 또는 변경된 정책과 정책 프로필은 관리 중인 기기로 전파됩니다.

   Kaspersky Security Center 웹 콘솔을 사용한다면 정책과 정책 프로필이 기기로 전달되었는지 확인할 수 있습니다. Kaspersky Security Center는 기기 속성에 전달 날짜와 시간을 지정합니다.

   방법 지침:

   - 관리 콘솔: 강제 동기화
   - Kaspersky Security Center 웹 콘솔: 강제 동기화

결과

기기 중심 시나리오를 완료하면 Kaspersky 애플리케이션은 정책 계층 구조를 통해 지정 및 전파된 설정에 따라 구성됩니다.

구성된 애플리케이션 정책 및 정책 프로필은 관리 그룹에 추가하는 새 기기에 자동으로 적용됩니다.

정책 설정 및 전파: 사용자 중심 접근 방식

이 섹션에서는 관리 중인 기기에 설치된 Kaspersky 애플리케이션의 중앙 집중식 구성을 위한 사용자 중심 방식의 시나리오에 대해 설명합니다. 이 시나리오를 완료하면 정의한 애플리케이션 정책 및 정책 프로필에 따라 관리 중인 모든 기기에서 애플리케이션이 구성됩니다.

> 이 시나리오는 Kaspersky Security Center 웹 콘솔 버전 13 이상을 통해 구현할 수 있습니다.

필수 구성 요소

시작하기 전에 Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 웹 콘솔을 설치했으며 기본 설치 시나리오를 완료했는지 확인합니다. 또한 사용자 중심 접근 방식의 대안 또는 추가 옵션으로 기기 중심 보안 관리를 고려할 수도 있습니다. 두 가지 관리 접근 방식에 대해 자세히 알아보십시오.

프로세스

Kaspersky 애플리케이션의 사용자 중심 관리 시나리오는 다음 단계로 구성됩니다.

1. **애플리케이션 정책 구성**

   관리 중인 기기에 설치되어 있는 각 Kaspersky 애플리케이션용 정책을 생성하여 애플리케이션의 설정 구성. 정책 세트는 클라이언트 기기로 전파됩니다.

   빠른 시작 마법사에서 네트워크 보호 구성 시, Kaspersky Security Center는 Kaspersky Endpoint Security용 기본 정책을 생성합니다. 이 마법사를 사용하여 구성 프로세스를 완료했다면, 이 애플리케이션용으로 새 정책을 생성할 필요가 없습니다. Kaspersky Endpoint Security 정책 수동 설정 진행.

   여러 중앙 관리 서버 및/또는 관리 그룹이 포함된 계층 구조가 있는 경우 보조 중앙 관리 서버와 자식 관리 그룹은 기본적으로 기본 중앙 관리 서버에서 정책을 상속합니다. 업스트림 정책에 구성된 설정을 수정할 수 없도록 자식 그룹과 보조 중앙 관리 서버의 상속을 강제 적용할 수 있습니다. 설정 중 일부만 강제로 상속되도록 하려는 경우 업스트림 정책에서 해당 설정을 잠글 수 있습니다. 잠금 해제된 나머지 설정은 다운스트림 정책에서 수정할 수 있습니다. 생성된 정책 계층 구조에서는 관리 그룹의 기기를 효율적으로 관리할 수 있습니다.

   방법 지침: 정책 만들기

2. **기기의 소유자 지정**

   해당하는 사용자에게 관리 중인 기기를 할당합니다.

   방법 지침: 기기 소유자로 특정 사용자 지정

3. **기업의 일반적인 사용자 역할 정의**

   기업 직원들은 일반적으로 다양한 종류의 작업을 수행합니다. 모든 직원을 해당 역할에 따라 구분해야 합니다. 예를 들어 부서, 직종, 직무 등을 기준으로 직원을 구분할 수 있습니다. 그 후에는 각 그룹에 대해 사용자 역할을 생성해야 합니다. 각 사용자 역할에는 해당 역할별 애플리케이션 설정을 포함하는 자체 정책 프로필이 포함됩니다.

4. **사용자 역할 생성**

   이전 단계에서 정의한 각 직원 그룹에 대해 사용자 역할을 생성하고 구성하거나 미리 정의된 사용자 역할을 사용합니다. 사용자 역할에는 애플리케이션 기능 접근 권한 세트가 포함됩니다.

   방법 지침: 사용자 역할 생성

5. **각 사용자 역할의 범위 정의**

   생성된 각 사용자 역할에 대해 사용자 및/또는 보안 그룹과 관리 그룹을 정의합니다. 사용자 역할과 연결된 설정은 이 역할이 지정된 사용자 소유의 기기가 이 역할과 연결된 그룹(자식 그룹 포함)에 속하는 경우에만 해당 기기에 적용됩니다.

   방법 지침: 사용자 역할의 범위 편집

6. **정책 프로필 만들기**

   기업의 각 사용자 역할용 정책 프로필을 생성합니다. 정책 프로필은 각 사용자의 역할에 따라 사용자 기기에 설치된 애플리케이션에 적용되는 설정을 정의합니다.

   방법 지침: 정책 프로필 만들기

7. **정책 프로필과 사용자 역할 연결**

   생성된 정책 프로필을 사용자 역할과 연결합니다. 그리고 나면 지정된 역할의 사용자에 대해 정책 프로필이 활성화됩니다. 정책 프로필에 구성된 설정은 사용자 기기에 설치된 Kaspersky 애플리케이션에 적용됩니다.

   방법 지침: 정책 프로필과 역할 연결

8. **관리 중인 기기로 정책 및 정책 프로필 전파**

기본적으로 중앙 관리 서버는 15분마다 관리 중인 기기와 자동으로 동기화됩니다. 동기화 중에 신규 또는 변경된 정책과 정책 프로필은 관리 중인 기기로 전파됩니다. 자동 동기화를 사용하지 않고 강제 동기화 명령을 사용해 동기화를 수동으로 실행할 수 있습니다. 동기화가 완료되면 정책과 정책 프로필이 설치된 Kaspersky 애플리케이션으로 전달되어 적용됩니다.

정책 및 정책 프로필이 기기에 전달되었는지 여부를 확인할 수 있습니다. Kaspersky Security Center는 기기 속성에 전달 날짜와 시간을 지정합니다.

방법 지침: 강제 동기화

결과

사용자 중심 시나리오를 완료하면 Kaspersky 애플리케이션은 정책 계층 구조 및 정책 프로필을 통해 지정 및 전파된 설정에 따라 구성됩니다.

새 사용자의 경우 새 계정을 생성하고 생성된 사용자 역할 중 하나를 사용자에게 할당한 다음 사용자에게 기기를 할당해야 합니다. 구성된 애플리케이션 정책 및 정책 프로필은 이 사용자의 기기에 자동으로 적용됩니다.

네트워크 에이전트 정책 설정

네트워크 에이전트 정책을 구성하려면 다음을 수행하십시오:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**이동합니다.
2. 네트워크 에이전트 정책의 이름을 클릭합니다.
   네트워크 에이전트 정책의 속성 창이 열립니다.

운영 체제의 유형에 따라 아래 설정이 어떻게 적용되는지 자세히 설명하는 비교표를 참조하십시오.

일반

이 탭에서는 정책 상태를 수정하고 정책 설정에 대한 상속을 지정할 수 있습니다.

- **정책 상태** 아래에서 다음 정책 모드 중 하나를 선택할 수 있습니다.
  - **액티브**

    이 옵션을 선택하면 정책이 활성화됩니다.
    기본적으로 이 옵션은 선택되어 있습니다.
  - **비활성**

    이 옵션을 선택하면 정책이 비활성화되지만 **정책** 폴더에는 계속 저장되어 있습니다. 필요한 경우 정책을 활성화할 수 있습니다.

- **설정 상속** 설정 그룹에서는 정책 상속을 구성할 수 있습니다:
  - **부모 정책의 설정 상속**

    이 옵션을 활성화하면 상위 그룹 정책에서 정책 설정 값이 상속되므로 이 값이 잠깁니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **자식 정책에 설정 강제 상속**

    이 옵션을 활성화하면 정책 변경 사항이 적용된 후 다음 작업이 수행됩니다.
    - 정책 설정의 값이 관리 하위 그룹의 정책, 즉 자식 정책에 배포됩니다.
    - 각 자식 정책의 속성 창에 있는 **일반** 섹션의 **설정 상속** 블록에서 **부모 정책의 설정 상속** 옵션은 자동으로 활성화됩니다.

    이 옵션을 활성화하면 자식 정책 설정이 잠깁니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

이벤트 구성

이 탭에서는 이벤트 기록과 이벤트 알림을 구성할 수 있습니다. 이벤트는 다음 **이벤트 구성** 탭에 있는 다음 섹션에서 심각도에 따라 배포됩니다.

- **기능 실패**
- **경고**
- **정보**

각 섹션에서 이벤트 유형 목록에는 이벤트 유형 및 중앙 관리 서버에 기본 이벤트가 저장되는 기간(일)이 표시됩니다. 이벤트 유형을 눌러 이벤트 기록과 목록에서 선택된 이벤트에 대한 알림 설정을 지정할 수 있습니다. 기본적으로 전체 중앙 관리 서버에 대해 지정된 일반 알림 설정이 모든 이벤트 유형에 사용됩니다. 그러나 필요한 이벤트 유형에 대해 특정 설정을 변경할 수 있습니다.

예를 들어, **경고** 섹션에서 **보안 문제가 발생했습니다** 이벤트 유형을 구성할 수 있습니다. 이러한 이벤트는 예를 들어, 배포 지점의 여유 디스크 공간 이 2GB 미만일 때 발생할 수 있습니다(애플리케이션을 설치하고 원격으로 업데이트를 다운로드하려면 최소 4GB 필요). **보안 문제가 발생했습니다** 이벤트를 구성하려면 이를 누른 다음, 발생한 이벤트를 저장할 위치와 알림 방법을 지정하면 됩니다.

네트워크 에이전트가 보안 문제를 감지한다면 관리 중인 장치의 설정을 사용하여 이 문제를 관리할 수 있습니다.

설정

설정 섹션에서는 네트워크 에이전트 정책을 구성할 수 있습니다:

- **배포 지점을 통해서만 파일 배포**

  이 옵션을 선택하면 관리 중인 기기의 네트워크 에이전트가 배포 지점에서만 업데이트를 검색합니다.
  이 옵션이 비어 있으면 관리 중인 기기의 네트워크 에이전트가 배포 지점 또는 중앙 관리 서버에서 업데이트를 수신합니다.

  > 관리 중인 기기의 보안 애플리케이션은 각 보안 애플리케이션의 업데이트 작업에 설정된 경로에서 업데이트를 검색합니다. **배포 지점을 통해서만 파일 배포** 옵션을 선택하면 업데이트 작업에서 Kaspersky Security Center가 업데이트 경로로 설정되어 있는지 확인하시기 바랍니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **이벤트 큐 최대 크기(MB)**

  이 필드에는 드라이브에서 이벤트 큐가 차지할 수 있는 최대 공간을 지정할 수 있습니다.
  기본값은 2MB입니다.

- **기기의 정책 확장 데이터를 가져오도록 애플리케이션 허용**

  관리 중인 기기에 설치된 네트워크 에이전트는 적용된 보안 제품 정책에 대한 정보를 보안 제품(예: Kaspersky Endpoint Security for Windows)으로 전송합니다. 보안 제품 인터페이스에서 전송된 정보를 볼 수 있습니다.

  네트워크 에이전트는 다음 정보를 전송합니다:

  - 관리 중인 기기로 정책을 전달한 시간.
  - 관리 중인 기기로 정책을 전달할 때 적용된 활성 정책의 이름.
  - 관리 중인 기기로 정책을 전달할 때 적용된 이동 사용자 정책의 이름(Linux용 네트워크 에이전트에서는 사용 불가).
  - 관리 중인 기기로 정책을 전달할 때 관리 중인 기기가 포함된 관리 그룹의 이름 및 전체 경로.
  - 관리 중인 기기로 정책을 전달할 때 적용된 활성 정책 프로필의 목록과 이름, 우선순위.

  이 정보를 기기에 올바른 정책을 적용하는 데 사용하고 문제 해결 목적으로 사용할 수도 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **무단 제거, 중지 또는 설정 변경을 하지 못하도록 네트워크 에이전트 서비스 보호**

  이 옵션이 활성화되면, 관리 중인 기기에 네트워크 에이전트를 설치한 후에 구성 요소를 제거하거나 재구성하려면 필요한 권한이 있어야 합니다. 네트워크 에이전트 서비스는 중지할 수 없습니다. 이 옵션은 도메인 컨트롤러에 영향을 주지 않습니다.

  로컬 관리자 권한으로 작동하는 워크스테이션에서 네트워크 에이전트를 보호하려면 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **제거 암호 사용**

  이 확인란을 선택하면 **수정** 버튼을 눌러 klmover 유틸리티 및 네트워크 에이전트 원격 제거를 위한 암호를 지정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

저장소

이 **저장소** 섹션에서 네트워크 에이전트로부터 중앙 관리 서버로 정보가 보내질 세부 개체 유형을 선택할 수 있습니다. 네트워크 에이전트 정책에서 이 섹션의 일부 설정에 대한 수정이 금지된 경우에는 해당 설정을 수정할 수 없습니다.

- **자산 관리(소프트웨어) 정보**

  이 옵션을 사용하면 클라이언트 기기에 설치된 애플리케이션 정보가 중앙 관리 서버로 전송됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **패치 정보 포함**

  클라이언트 기기에 설치된 애플리케이션의 패치에 대한 정보는 중앙 관리 서버로 전송됩니다. 이 옵션을 사용하면 중앙 관리 서버 및 DBMS의 부하가 증가하고 데이터베이스 크기가 증가할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다. Windows에서만 사용할 수 있습니다.

- **Windows 업데이트 패치 세부 정보**

  이 옵션을 사용하면 클라이언트 기기에 설치해야 하는 Microsoft Windows 업데이트 정보가 중앙 관리 서버로 전송됩니다.

  옵션이 비활성화되더라도 **사용 가능한 업데이트** 섹션의 기기 속성에 업데이트가 표시되는 경우가 있습니다. 예를 들어, 조직의 기기에 이 업데이트로 수정 가능한 취약점이 있다면 이러한 상황이 발생할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다. Windows에서만 사용할 수 있습니다.

  선택 사항인 Microsoft Windows 업데이트에 대한 정보는 중앙 관리 서버로 전송되지 않습니다.

- **소프트웨어 취약점 및 관련 업데이트 세부 정보**

  이 옵션을 활성화하면 관리 중인 기기에서 감지된 타사 소프트웨어(Microsoft 소프트웨어 포함)의 취약점에 관한 정보와 타사 취약점(Microsoft 소프트웨어 제외)을 수정할 수 있는 소프트웨어 업데이트 관련 정보가 중앙 관리 서버로 전송됩니다.

이 옵션(**소프트웨어 취약점 및 관련 업데이트 세부 정보**)을 선택하면 네트워크 부하, 중앙 관리 서버 디스크 부하, 네트워크 에이전트 리소스 소비량이 증가합니다.

기본적으로 이 옵션은 켜져 있습니다. Windows에서만 사용할 수 있습니다.

Microsoft 소프트웨어의 소프트웨어 업데이트를 관리하려면 **Windows 업데이트 패치 세부 정보** 옵션을 사용합니다.

- **자산 관리(하드웨어) 정보**

  기기에 설치된 네트워크 에이전트는 기기 하드웨어에 관한 정보를 중앙 관리 서버로 전송합니다. 기기 속성에서 하드웨어 세부 정보를 볼 수 있습니다.

  하드웨어 세부 정보를 가져오려는 Linux 기기에 lshw 유틸리티가 설치되어 있는지 확인합니다. 가상 머신에서 가져온 하드웨어 세부 정보는 사용된 하이퍼바이저에 따라 불완전할 수 있습니다.

소프트웨어 업데이트 및 취약점

소프트웨어 업데이트 및 취약점 섹션에서는 Windows 업데이트의 검색 및 배포를 구성하고 실행 파일의 취약점 검사를 활성화할 수 있습니다.

- **WSUS 서버로 이 중앙 관리 서버 사용**

  이 옵션을 사용하면, Windows 업데이트는 중앙 관리 서버에서 다운로드됩니다. 중앙 관리 서버는 네트워크 에이전트를 통해 중앙 집중식 모드에서 클라이언트 기기의 Windows 업데이트로 다운받은 업데이트를 제공합니다.

  이 옵션이 비활성화되어 있으면 중앙 관리 서버는 Windows 업데이트 다운로드 용도로 사용되지 않습니다. 이 경우 클라이언트 기기는 스스로 Windows Update를 다운로드합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- 사용자가 Windows 업데이트를 사용하여 기기에 수동으로 설치할 수 있는 Windows업데이트를 제한할 수 있습니다.

  Windows 10을 실행하는 기기에서 Windows 업데이트가 이미 해당 기기에 대한 업데이트를 찾은 경우 **사용자가 Windows 업데이트 설치를 관리하도록 허용** 아래에서 선택한 새 옵션은 앞서 검색된 업데이트가 설치된 후에만 적용됩니다.

  드롭다운 목록에서 항목을 선택합니다:

  - **사용자가 모든 적용 가능한 Windows 업데이트 패치를 설치할 수 있도록 허용**

    사용자가 기기에 적용 가능한 모든 Microsoft Windows 업데이트를 설치할 수 있습니다.

    업데이트 설치를 방해하고 싶지 않다면 옵션을 선택합니다.

    사용자가 Microsoft Windows 업데이트를 수동으로 설치할 때는 중앙 관리 서버가 아닌 Microsoft 서버에서 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버에서 이러한 업데이트를 아직 다운로드하지 않은 경우 Microsoft 서버에서 다운로드할 수 있습니다. Microsoft 서버에서 업데이트를 다운로드하면 트래픽이 추가로 발생합니다.

- **사용자가 승인된 Windows 업데이트 패치만 설치할 수 있도록 허용**

  사용자가 기기에 적용 가능하며 관리자가 승인한 모든 Microsoft Windows 업데이트를 설치할 수 있습니다.

  예를 들어 업데이트가 기기 작동을 방해하지 않는지 테스트 환경에서 업데이트 설치를 먼저 확인한 후에만 클라이언트 기기에서 승인된 업데이트 설치를 허용할 수 있습니다.

  사용자가 Microsoft Windows 업데이트를 수동으로 설치할 때는 중앙 관리 서버가 아닌 Microsoft 서버에서 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버에서 이러한 업데이트를 아직 다운로드하지 않은 경우 Microsoft 서버에서 다운로드할 수 있습니다. Microsoft 서버에서 업데이트를 다운로드하면 트래픽이 추가로 발생합니다.

- **사용자가 Windows 업데이트 패치를 설치하는 것을 허용 안 함**

  사용자가 기기에 Microsoft Windows 업데이트를 수동으로 설치할 수 없습니다. 해당하는 모든 업데이트는 관리자가 구성한 대로 설치됩니다.

  업데이트 설치를 중앙에서 관리하고 싶다면 이 옵션을 선택합니다.

  네트워크가 과부하되지 않도록 업데이트 스케줄을 최적화하려는 경우를 예로 들 수 있습니다. 사용자 생산성이 낮아지지 않도록 업무 시간 이후에 업데이트 스케줄을 지정할 수 있습니다.

- **Windows 업데이트 검색 모드** 설정 그룹에서 업데이트 검색 모드를 선택할 수 있습니다:

  - **액티브**

    이 옵션을 선택하면 네트워크 에이전트에서 지원하는 중앙 관리 서버는 클라이언트 기기의 Windows 업데이트 에이전트에서 다음과 같은 업데이트 경로로 요청을 시작합니다: Windows 업데이트 서버 또는 WSUS. 그런 다음 네트워크 에이전트가 Windows 업데이트 에이전트에서 받은 정보를 중앙 관리 서버로 전달합니다.

    취약점 및 필요한 업데이트 검색 작업의 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션이 선택된 경우에만 이 옵션이 적용됩니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **패시브**

    이 옵션을 선택하면 네트워크 에이전트가 Windows 업데이트 에이전트와 업데이트 경로 간의 마지막 동기화 시 가져온 업데이트 관련 정보를 중앙 관리 서버에 주기적으로 전달합니다. 업데이트 경로와 Windows 업데이트 에이전트의 동기화가 수행되지 않으면 중앙 관리 서버의 업데이트 정보가 최신 상태를 유지할 수 없습니다.

    업데이트 경로의 메모리 캐시에서 업데이트를 받으려면 이 옵션을 선택합니다.

  - **비활성화됨**

    이 옵션을 선택하면 중앙 관리 서버가 어떤 업데이트 관련 정보도 수집하지 않습니다.

    예를 들어, 로컬 기기에서 업데이트를 먼저 테스트하려면 이 옵션을 선택하십시오.

- **실행 파일 실행 시 취약점 검사**

  이 옵션을 사용하면 실행 파일이 실행될 때 실행 파일의 취약점을 검사합니다.

  기본적으로 이 옵션은 켜져 있습니다.

관리 다시 시작

관리 다시 시작 섹션에서는 애플리케이션의 올바른 사용, 설치, 제거를 위해 관리 중인 기기의 운영 체제를 다시 시작해야 할 때 수행할 작업을 지정할 수 있습니다.

- **운영 체제 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **필요한 경우 운영 체제를 자동으로 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

  - **지정한 시간 간격마다 물어보기(분)**

    이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

    기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

    이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

  - **다음 시간 이후에 강제로 다시 시작(분)**

    사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

    기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

Windows Desktop Sharing

Windows Desktop Sharing 섹션에서는 데스크톱 접근 권한 공유 시 원격 기기에서 수행할 관리자 작업 감사를 사용 및 구성할 수 있습니다.

- **감사 기능 사용**

  이 옵션을 활성화하면 원격 기기에서 관리자 작업 감사가 사용됩니다. 원격 기기의 관리자 활동 기록은 다음 위치에 저장됩니다:

  - 원격 기기의 이벤트 로그에 저장
  - 원격 기기의 네트워크 에이전트 설치 폴더에 있는 확장자가 syslog인 파일
  - Kaspersky Security Center의 이벤트 데이터베이스

  다음 조건이 충족되면 관리자 작업 감사를 사용할 수 있습니다:

  - 취약점 및 패치 관리 라이센스 사용 중
  - 관리자에게 원격 기기의 데스크톱에 대한 공유 접근 시작 권한이 있는 경우

  이 옵션 확인란이 비활성화되어 있으면 원격 기기에서 관리자 작업 감사가 사용되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **읽을 때 모니터링해야 하는 파일 마스크**

  목록에는 파일 마스크가 포함됩니다. 감사를 사용하는 경우 애플리케이션은 마스크와 일치하는 관리자의 읽기 파일을 모니터링하여 파일 읽기에 대한 정보를 저장합니다. 이 필드는 **감사 기능 사용** 확인란을 선택한 경우에 사용할 수 있습니다. 파일 마스크를 편집하고 목록에 새 마스크를 추가할 수 있습니다. 새 파일 마스크는 각각 목록의 새 줄에 지정해야 합니다.

  기본적으로 지정되는 파일 마스크는 *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf입니다.

- **변경될 때 모니터링해야 하는 파일 마스크**

  목록에는 원격 기기의 파일 마스크가 포함되어 있습니다. 감사를 사용하는 경우 애플리케이션은 마스크와 일치하는 파일에서 관리자가 수행하는 변경을 모니터링하여 해당 수정에 대한 정보를 저장합니다. 이 필드는 **감사 기능 사용** 확인란을 선택한 경우에 사용할 수 있습니다. 파일 마스크를 편집하고 목록에 새 마스크를 추가할 수 있습니다. 새 파일 마스크는 각각 목록의 새 줄에 지정해야 합니다.

  기본적으로 지정되는 파일 마스크는 *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf입니다.

패치 및 업데이트 관리

이 **패치 및 업데이트 관리** 섹션에서 업데이트 다운로드, 배포, 관리 중인 기기에서의 패치 설치를 구성할 수 있습니다.

- **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치**

  이 옵션을 활성화하면 *정의 안 됨* 상태의 Kaspersky 패치가 업데이트 서버에서 다운로드된 직후 자동으로 관리 중인 기기에 설치됩니다.

  이 옵션을 비활성화하면, 다운로드되어 *정의 안 됨* 상태가 태그된 Kaspersky 패치는 그 상태를 *승인됨*으로 변경한 후에만 설치할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드(권장)**

  이 옵션을 활성화하면 업데이트 다운로드의 오프라인 모델이 사용됩니다. 중앙 관리 서버는 업데이트를 받을 때마다 네트워크 에이전트가 설치되어 있는 기기에서 관리 중인 애플리케이션에 대해 필요한 업데이트를 네트워크 에이전트에 통지합니다. 네트워크 에이전트가 업데이트 정보를 수신하면 중앙 관리 서버에서 미리 관련 파일을 다운로드합니다. 네트워크 에이전트와의 첫 연결에서, 중앙 관리 서버는 업데이트 다운로드를 시작합니다. 네트워크 에이전트가 모든 업데이트를 클라이언트 기기에 다운로드하고 나면 해당 기기의 애플리케이션이 업데이트를 사용할 수 있게 됩니다.

  클라이언트 기기에 있는 관리 애플리케이션이 업데이트를 위해 네트워크 에이전트에 접근하면, 이 네트워크 에이전트는 모든 필요한 업데이트가 있는지 확인합니다. 업데이트가 해당 관리 중인 애플리케이션에 대한 것이고 중앙 관리 서버에서 25시간 이내에 받은 것이라면, 네트워크 에이전트는 중앙 관리 서버에 연결하지 않고 로컬 캐시에서 해당 업데이트를 관리 중인 애플리케이션에 공급합니다. 네트워크 에이전트가 클라이언트 기기의 애플리케이션에 업데이트를 제공하는데 업데이트를 위한 연결이 필요하지 않을 때는 중앙 관리 서버와의 연결이 설정되지 않을 수 있습니다.

  이 옵션을 비활성화하면 업데이트 다운로드의 오프라인 모델이 사용되지 않습니다. 업데이트는 업데이트 다운로드 작업 스케줄에 따라 배포됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

연결성

연결성 섹션에는 세 가지의 하위 섹션이 있습니다:

- **네트워크**
- **연결 프로필**
- **연결 스케줄**

네트워크 하위 섹션에서 중앙 관리 서버에 대한 연결을 구성하고 UDP 포트의 사용을 설정하며 UDP 포트 번호를 지정할 수 있습니다.

- **중앙 관리 서버에 연결** 설정 그룹에서 중앙 관리 서버와의 연결을 구성하고 클라이언트 기기와 중앙 관리 서버 간의 동기화 시간 간격을 지정할 수 있습니다:
  - **동기화 주기(분)**

    네트워크 에이전트는 관리 중인 기기를 중앙 관리 서버와 동기화합니다. 동기화 간격(존재-알림 신호라고도 함)은 관리 중인 기기 10,000개당 15분으로 설정하는 것이 좋습니다.

동기화 간격을 15분 미만으로 설정하면 15분마다 동기화가 수행됩니다. 동기화 간격을 15분 이상으로 설정하면 지정된 동기화 간격으로 동기화를 수행합니다.

- **네트워크 트래픽 압축**

  이 옵션을 사용하면 전송되는 정보의 양이 줄어들어 중앙 관리 서버의 로드가 감소하고, 결과적으로 네트워크 에이전트의 데이터 전송 속도가 빨라집니다.

  클라이언트 컴퓨터의 CPU 사용량이 증가할 수 있습니다.

  기본적으로 이 확인란은 선택되어 있습니다.

- **Microsoft Windows 방화벽에 네트워크 에이전트 포트 열기**

  이 옵션을 사용하면 네트워크 에이전트 및 중앙 관리 서버의 작업에 필요한 포트가 Microsoft Windows 방화벽 예외 목록에 추가됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **SSL 연결 사용**

  이 확인란을 선택하면 SSL을 사용하여 보안 포트를 통해 중앙 관리 서버에 연결됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **기본 연결 설정에서 배포 지점(이용 가능 시)의 연결 게이트웨이 사용**

  이 옵션을 사용하면 관리 그룹 속성에 지정된 설정에 따라 배포 지점의 연결 게이트웨이가 사용됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **UDP 포트 사용**

  UDP 포트를 통해 네트워크 에이전트를 중앙 관리 서버에 연결하려면, **UDP 포트 사용** 옵션을 선택하고 **UDP 포트 번호**를 지정합니다. 기본적으로 이 옵션은 켜져 있습니다. 중앙 관리 서버에 연결하는 기본 UDP 포트는 15000입니다.

- **UDP 포트 번호**

  이 필드에는 UDP 포트 번호를 입력할 수 있습니다. 기본 포트 번호는 15000입니다.

  십진법을 사용하여 기록합니다.

  클라이언트 기기가 Windows XP 서비스 팩 2를 실행하는 경우 내장 방화벽이 UDP 포트 15000을 차단합니다. 이 포트는 수동으로 열어야 합니다.

- **배포 지점을 사용하여 중앙 관리 서버에 강제로 연결**

  배포 지점 설정 창에서 **이 배포 지점을 푸시 서버로 사용**옵션을 선택한 경우 이 옵션을 선택하십시오. 그렇지 않으면 배포 지점이 푸시 서버로 작동하지 않습니다.

연결 프로필 하위 섹션에서 네트워크 위치 설정을 지정하고, 중앙 관리 서버를 사용할 수 없을 시 이동 사용자 모드를 활성화할 수 있습니다.

- **네트워크 위치 설정**

  네트워크 위치 설정은 클라이언트 기기가 연결된 네트워크의 특성을 정의하고 해당 네트워크 특성이 변경될 때 하나의 중앙 관리 서버 연결 프로필에서 다른 중앙 관리 서버 연결 프로필로 전환하는 네트워크 에이전트에 대한 규칙을 지정합니다.

- **중앙 관리 서버 연결 프로필**

  이 섹션에서는 중앙 관리 서버로의 네트워크 에이전트 연결에 관한 프로필을 보고 추가할 수 있습니다. 이 섹션에서 다음 이벤트가 발생했을 때 다른 중앙 관리 서버로 네트워크 에이전트를 전환하는 규칙도 만들 수 있습니다:

  - 클라이언트 기기가 다른 로컬 네트워크에 연결될 때
  - 기기가 조직의 로컬 네트워크와의 연결이 끊길 때
  - 연결 게이트웨이 주소가 변경되거나 DNS 서버 주소가 수정될 때

  연결 프로필은 Windows 및 macOS를 실행 중인 기기에서만 지원됩니다.

- **중앙 관리 서버에 연결할 수 없으면 이동 사용자 모드 사용**

  이 옵션을 사용하면 이 프로필을 통해 연결하는 경우 클라이언트 기기에 설치된 애플리케이션은 이동 사용자 정책뿐만 아니라 이동 사용자 모드에 있는 기기를 위한 정책 프로필을 사용합니다. 애플리케이션에 대해 이동 사용자 정책이 정의되어 있지 않은 경우에는 활성 정책이 사용됩니다.

  이 옵션을 비활성화하면 애플리케이션에서 활성 정책을 사용합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

이 **연결 스케줄** 하위 섹션에서는 네트워크 에이전트가 중앙 관리 서버로 데이터를 보내는 시간 간격을 지정할 수 있습니다:

- **필요 시 연결**

  이 옵션을 선택하면 네트워크 에이전트가 중앙 관리 서버로 데이터를 보내야 할 때 연결이 설정됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **지정한 시간 간격에 연결**

  이 옵션을 선택하면 네트워크 에이전트가 지정된 시간에 중앙 관리 서버와 연결됩니다. 여러 개의 연결 기간을 추가할 수 있습니다.

배포 지점별 네트워크 폴링

배포 지점별 네트워크 폴링 하위 섹션에서는 네트워크 자동 검색을 구성할 수 있습니다. 다음 옵션을 사용하여 검색을 활성화하고 다음과 같이 빈도를 설정할 수 있습니다.

- **Windows 네트워크**

  이 옵션을 사용하면 중앙 관리 서버가 **빠른 검색 스케줄 설정** 및 **상세 검색 스케줄 설정** 링크를 눌러 구성한 스케줄에 따라 자동으로 네트워크를 검색합니다.

  이 옵션이 비활성화되면 중앙 관리 서버는 **네트워크 검색 주기(분)** 필드에 지정된 간격으로 네트워크를 검색합니다.

  10.2 버전 이전의 네트워크 에이전트의 기기 발견 간격은 **Windows 도메인의 검색 주기(분)**(빠른 Windows 네트워크 검색) 및 **네트워크 검색 주기(분)**(전체 Windows 네트워크 검색) 필드에서 구성할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **Zeroconf**

  이 옵션을 활성화하면 배포 지점에서 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 IPv6 기기가 있는 네트워크를 자동으로 검색합니다. 이 경우 배포 지점에서 전체 네트워크를 검색하기 때문에 활성화된 IP 범위 검색이 무시됩니다.

  제로 구성을 시작하려면 다음 조건이 충족되어야 합니다.

  - 배포 지점에서 Linux를 실행해야 합니다.
  - 배포 지점에 avahi-browse 유틸리티를 설치해야 합니다.

  이 옵션이 비활성화되어 있으면 배포 지점에서 IPv6 기기가 있는 네트워크를 검색하지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **IP 범위**

  이 확인란을 선택하면 배포 지점이 **검색 스케줄 설정** 버튼을 눌러 구성한 스케줄에 따라 자동으로 IP 범위를 검색합니다.

  이 옵션이 비활성 상태라면 배포 지점이 IP 범위를 검색하지 않습니다.

  10.2 버전 이전의 네트워크 에이전트에서 IP 범위 검색 빈도는 **검색 주기(분)** 필드에서 구성할 수 있습니다. 이 필드는 옵션을 선택한 경우에 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **도메인 컨트롤러**

  이 확인란을 선택하면 배포 지점이 **검색 스케줄 설정** 링크를 눌러 구성한 스케줄에 따라 자동으로 Active Directory를 검색합니다.

  이 옵션이 비활성화되어 있으면 중앙 관리 서버가 Active Directory를 검색하지 않습니다.

  10.2 버전 이전의 네트워크 에이전트에 대한 Active Directory 검색 빈도는 **검색 주기(분)** 필드에서 구성할 수 있습니다. 이 필드는 이 옵션을 선택한 경우에 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

이 옵션을 활성화하면 배포 지점이 **검색 스케줄 설정** 버튼을 클릭하여 구성한 일정에 따라 자동으로 도메인 컨트롤러를 검색합니다.

이 옵션이 비활성화되면 배포 지점이 도메인 컨트롤러를 검색하지 않습니다.

10.2 버전 이전의 네트워크 에이전트에 대한 도메인 컨트롤러 검색 빈도는 **검색 주기(분)** 필드에서 구성할 수 있습니다. 이 필드는 이 옵션을 선택한 경우에 사용할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

배포 지점에 대한 네트워크 설정

배포 지점에서 인터넷에 연결할 때 프록시 서버를 사용하는 경우 **배포 지점에 대한 네트워크 설정** 섹션에서 다음 설정을 지정할 수 있습니다.

- **프록시 서버 사용**
- **주소**
- **포트 번호**
- **로컬 주소에서 프록시 서버 사용 안 함**

  이 옵션을 사용하면 로컬 네트워크에서 기기로 연결하는 데 프록시 서버가 사용되지 않습니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **프록시 서버 인증**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.
  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **사용자 이름**
- **암호**

KSN 프록시(배포 지점)

KSN 프록시(배포 지점) 섹션에서는 애플리케이션이 배포 지점을 사용하여 관리 중인 기기에서 Kaspersky Security Network(KSN) 요청을 전달하도록 구성할 수 있습니다:

- **배포 지점 측에서 KSN 프록시 기능 활성화**

  배포 지점으로 사용되는 기기에서 KSN 프록시 서비스가 실행됩니다. 네트워크에서 트래픽을 재분배하고 최적화하려면 이 기능을 사용합니다.

  배포 지점은 Kaspersky Security Network 진술문에 나열된 KSN 통계를 Kaspersky에 보냅니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 중앙 관리 서버 속성 창에서 **KSN 프록시 서버로 중앙 관리 서버 사용**과 **Kaspersky Security Network 사용에 동의합니다** 옵션이 활성화되어야만 이 옵션이 활성화됩니다.

액티브-패시브 클러스터의 노드에 배포 지점을 할당하고 이 노드에 KSN 프록시 서버를 활성화할 수 있습니다.

- **중앙 관리 서버에 KSN 요청 전달**

  배포 지점이 관리 중인 기기에서 중앙 관리 서버로 KSN 요청을 전달합니다.
  기본적으로 이 옵션은 켜져 있습니다.

- **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근**

  배포 지점이 관리 중인 기기에서 KSN 클라우드 또는 KPSN으로 KSN 요청을 전달합니다. 배포 지점 자체에서 생성된 KSN 요청은 KSN 클라우드 또는 KPSN으로 직접 전송됩니다.
  네트워크 에이전트 버전 11 이하가 설치된 배포 지점은 KPSN에 직접 접근할 수 없습니다. KSN 요청을 KPSN으로 전송하도록 배포 지점을 재구성하면, 각 배포 지점에 대하여 **중앙 관리 서버에 KSN 요청 전달** 옵션을 활성화합니다.
  네트워크 에이전트 버전 12 이상이 설치된 배포 지점은 KPSN에 직접 접근할 수 있습니다.

- **포트**

  관리 중인 기기가 KSN 프록시 서버에 연결하는 데 사용할 TCP 포트의 번호입니다. 기본 포트 번호는 13111입니다.

- **UDP 포트**

  UDP 포트를 통해 네트워크 에이전트를 중앙 관리 서버에 연결하려면, **UDP 포트 사용** 옵션을 선택하고 **UDP 포트 번호**를 지정합니다. 기본적으로 이 옵션은 켜져 있습니다. 중앙 관리 서버에 연결하는 기본 UDP 포트는 15000입니다.

업데이트(배포 지점)

업데이트(배포 지점) 섹션에서 diff 파일 다운로드 기능을 활성화하면 배포 지점이 Kaspersky 업데이트 서버에서 diff 파일 형식으로 업데이트됩니다.

로컬 계정 관리(Linux만)

로컬 계정 관리(Linux만) 섹션에는 다음 세 하위 섹션이 포함됩니다.

- **사용자 인증서 관리**
- **해당 로컬 관리 그룹 추가 또는 수정**
- **참조 파일을 업로드하여 사용자 기기의 sudoers 파일 변경을 방지합니다**

사용자 인증서 관리 하위 섹션에서 설치할 루트 인증서를 지정할 수 있습니다. 이러한 인증서는 웹사이트나 웹 서버 인증 확인 등의 작업에 사용할 수 있습니다.

- **루트 인증서 설치**

  이 옵션을 사용하면 표에 추가된 인증서가 지정된 기기에 설치됩니다.
  이 옵션을 사용하지 않으면 지정된 기기에 인증서를 설치하지 않습니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **추가**

  이 버튼을 클릭하면 인증서 추가 창이 열립니다.
  인증서는 10MB를 넘을 수 없습니다.
  Kaspersky Security Center는 CER, CRT, CERT, PEM, KEY 확장자의 인증서를 지원합니다.

해당 로컬 관리 그룹 추가 또는 수정 하위 섹션에서 로컬 관리 그룹을 관리할 수 있습니다. 이러한 그룹은 예를 들어 로컬 관리자 권한을 취소할 때 사용합니다. **권한이 있는 기기 사용자에 대한 리포트(Linux만)**를 사용하여 권한 있는 사용자 계정 목록을 확인할 수도 있습니다.

- **추가**

  이 버튼을 클릭하면 로컬 관리자 그룹 추가 창이 열립니다.

- **편집**

  이 버튼을 클릭하면 로컬 관리자 그룹 편집 창이 열립니다.
  이 버튼은 로컬 관리자 그룹 옆의 확인란을 선택하면 사용할 수 있습니다.

- **삭제**

  이 버튼을 클릭하면 선택한 로컬 관리자 그룹을 표에서 삭제합니다.
  이 버튼은 로컬 관리자 그룹 옆의 확인란을 선택하면 사용할 수 있습니다.

참조 파일을 업로드하여 사용자 기기의 sudoers 파일 변경을 방지합니다 하위 섹션에서 sudoers 파일 제어를 구성할 수 있습니다. 권한 그룹 및 기기 사용자는 기기의 sudoers 파일로 정의합니다. sudoers 파일은 `/etc/sudoers`에 있습니다. 참조 sudoers 파일을 업로드하여 sudoers 파일이 변경되지 않도록 보호할 수 있습니다. 이렇게 하면 sudoers 파일의 원치 않는 변경을 방지할 수 있습니다.

잘못된 참조 sudoers 파일을 업로드하면 사용자 기기에 오류가 발생할 수 있습니다.

- **sudoers 파일 제어**

  이 옵션을 사용하면 sudoers 파일이 현재 참조 sudoers 파일로 대체됩니다.

  이 옵션을 중지하면 sudoers 파일은 변경되지 않은 상태로 유지됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **참조 sudoers 파일**

  이 필드에는 업로드된 참조 sudoers 파일의 이름이 표시됩니다.

- **업로드**

  이 버튼을 클릭하면 참조 sudoers 파일을 업로드할 수 있는 창이 열립니다.

- **현재 참조 sudoers 파일**

  이 버튼을 클릭하면 현재 sudoers 파일의 내용이 표시됩니다.

리비전 내역

이 탭에서는 정책 리비전 목록을 확인하고 필요한 경우 정책 변경 사항을 롤백할 수 있습니다.

운영 체제별 네트워크 에이전트 정책 설정 비교

아래 표에는 관리 콘솔 및 Kaspersky Security Center 웹 콘솔에서 특정 운영 체제에 맞게 네트워크 에이전트를 구성하는 데 사용할 수 있는 네트워크 에이전트 정책 설정이 나와 있습니다.

네트워크 에이전트 정책 설정: 운영 체제별 비교

정책 섹션	Windows	macOS	Linux
일반	✓	✓	✓
이벤트 구성	✓	✓	✓
설정	✓	✓	✓ 다음과 같은 옵션을 사용할 수 있습니다. • **배포 지점을 통해서만 파일 배포** • **이벤트 큐 최대 크기(MB)** • **기기의 정책 확장 데이터를 가져오도록 애플리케이션 허용**
저장소	✓	✓ **자산 관리(하드웨어) 정보** 옵션을 사용할 수 있습니다.	✓ 다음과 같은 옵션을 사용할 수 있습니다. • **자산 관리(소프트웨어) 정보** • **자산 관리(하드웨어) 정보**
소프트웨어 업데이트 및 취약점	✓	—	—
관리 다시 시작	✓	—	—
Windows Desktop Sharing	✓	—	—
패치 및 업데이트 관리	✓	—	—
연결성 → 네트워크	✓	✓	✓ **Microsoft Windows 방화벽에 네트워크 에이전트 포트 열기** 옵션은 제외합니다.
연결성 → 연결 프로필	✓	✓	—
연결성 → 연결 스케줄	✓	✓	✓

정책 섹션	Windows	macOS	Linux
배포 지점별 네트워크 폴링	✓ **Windows 네트워크**, **IP 범위**, **도메인 컨트롤러** 옵션만 사용할 수 있습니다.	—	✓ 다음과 같은 옵션을 사용할 수 있습니다. • **Zeroconf** • **IP 범위** • **도메인 컨트롤러**
배포 지점에 대한 네트워크 설정	✓	✓	✓
KSN 프록시(배포 지점)	✓	—	✓
업데이트(배포 지점)	✓	—	✓
리비전 내역	✓	✓	✓

네트워크 에이전트의 저자원 소비 모드 활성화 및 비활성화

저자원 소비 모드를 사용하면 클라이언트 기기에 설치된 네트워크 에이전트의 RAM 사용량을 제한할 수 있습니다. 기본적으로 저자원 소비 모드는 비활성화되어 있습니다.

저자원 소비 모드에서 다음 기능은 수행할 수 없습니다.

- 네트워크 에이전트를 배포 지점 역할을 하도록 할당할 수 없습니다(수동 또는 자동).
- 네트워크 에이전트는 네트워크 에이전트의 상태에 대한 정보를 별도의 텍스트 파일에 기록하지 않습니다.
- 네트워크 에이전트는 업데이트 다운로드의 오프라인 모델을 지원하지 않습니다.
- 다음 구성 요소 및 프로세스는 비활성화됩니다.
  - 타사 업데이트 및 취약점에 대한 정보 입수.
  - 배포 지점 측에서 KSN 프록시 실행.
  - 배포 지점 저장소에 업데이트 업로드.
  - DNS 서버 차단을 우회합니다.
  - 사용 가능한 디스크 공간 정보를 가져오는 중입니다.

저자원 소비 모드를 비활성화한 후 구성 요소 및 프로세스가 다시 작동합니다.

저자원 소비 모드를 활성화하려면 다음을 따르십시오.

1. 클라이언트 기기의 명령줄에서 다음 명령을 실행합니다.

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. 그리고, 네트워크 에이전트를 재시작합니다.

3. 저자원 소비 모드가 활성화되어 있는지 확인하려면 Windows에서 **이벤트 뷰어**를 열고 **애플리케이션 및 서비스 로그 → Kaspersky 이벤트 로그**를 선택합니다.

   로그에 **Kaspersky Security Center 네트워크 에이전트가 저자원 소비 모드로 작동 중** 등의 이벤트가 포함되어 있는지 확인하십시오.

저자원 소비 모드 모드가 활성화됩니다.

저자원 소비 모드 모드를 비활성화하려면 다음을 따르십시오.

1. 클라이언트 기기의 명령줄에서 다음 명령을 실행합니다.

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. 그리고, 네트워크 에이전트를 재시작합니다.

3. 저자원 소비 모드가 비활성화되어 있는지 확인하려면 Windows에서 **이벤트 뷰어**를 열고 **애플리케이션 및 서비스 로그 → Kaspersky 이벤트 로그**를 선택합니다.

   마지막 klnagent 이벤트에 **Kaspersky Security Center 네트워크 에이전트가 저자원 소비 모드로 작동 중** 메시지가 포함되지 않는지 확인합니다.

저자원 소비 모드 모드가 비활성화됩니다.

원격 *스크립트 원격 실행* 작업을 사용하여 원격으로 저자원 소비 모드를 활성화할 수도 있습니다.

Kaspersky Endpoint Security 정책 수동 설정

이 섹션에서는 Kaspersky Endpoint Security 정책 구성 방법에 대한 권장 사항을 제공합니다. 정책 속성 창에서 설정을 수행할 수 있습니다. 설정 편집 시, 관련 설정 그룹 오른쪽에 있는 잠금 아이콘을 클릭하여 지정된 값을 워크스테이션에 적용합니다.

Kaspersky Security Network 구성

KSN(Kaspersky Security Network)은 파일, 웹 리소스, 소프트웨어의 평판 정보가 포함된 클라우드 서비스 인프라입니다. Kaspersky Security Network를 사용하면 Kaspersky Endpoint Security for Windows가 다양한 종류의 위협에 더 빠르게 대응하고, 보호 구성 요소의 성능을 개선하며, 오탐 가능성을 줄일 수 있습니다. Kaspersky Security Network에 대한 자세한 내용은 Kaspersky Endpoint Security for Windows 도움말을 참조하십시오.

권장 KSN 설정을 지정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.

2. Kaspersky Endpoint Security for Windows의 정책을 클릭합니다.

   선택한 정책의 속성 창이 열립니다.

3. 정책 속성에서 **애플리케이션 설정 → 지능형 위협 보호 → Kaspersky Security Network**로 이동합니다.

4. **Kaspersky Security Network** 옵션을 활성화했는지 확인합니다. 네트워크에서 트래픽을 재분배하고 최적화하려면 이 기능을 사용합니다.

   > Managed Detection and Response를 사용한다면, 배포 지점에 **Kaspersky Security Network** 옵션을 활성화하고 확장 KSN 모드를 활성화해야 합니다.

5. KSN 프록시 서비스를 사용할 수 없다면, KSN 서버를 활성화합니다. KSN 서버는 Kaspersky에 있을 수도 있고 (KSN 사용 시) 타사에 있을 수도 있습니다(KPSN 사용 시).

6. **확인**를 누릅니다.

권장 KSN 설정이 지정됩니다.

방화벽으로 보호되는 네트워크 목록 확인

Kaspersky Endpoint Security for Windows Firewall이 모든 네트워크를 보호하는지 확인합니다. 기본적으로 방화벽은 다음 연결 유형으로 네트워크를 보호합니다:

- **공용 네트워크**. 보안 애플리케이션, 방화벽, 필터는 이러한 네트워크의 기기를 보호하지 않습니다.
- **로컬 네트워크**. 이 네트워크의 기기에 대해서는 파일 및 프린터에 대한 액세스가 제한됩니다.
- **신뢰하는 네트워크**. 이러한 네트워크의 기기는 공격과 파일 및 데이터에 대한 무단 액세스로부터 보호됩니다.

사용자 정의 네트워크를 구성했다면 방화벽이 네트워크를 보호하는지 확인합니다. 이를 위해, Kaspersky Endpoint Security for Windows 정책 속성에서 네트워크 목록을 확인하십시오. 목록에 모든 네트워크가 포함되지 않을 수도 있습니다.

방화벽에 대한 자세한 내용은 Kaspersky Endpoint Security for Windows 도움말을 참조하십시오.

네트워크 목록을 확인하려면 다음을 수행합니다:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. Kaspersky Endpoint Security for Windows의 정책을 클릭합니다.
   선택한 정책의 속성 창이 열립니다.
3. 정책 속성에서 **애플리케이션 설정 → 필수 위협 보호 → 방화벽**으로 이동합니다.
4. **사용 가능한 네트워크** 아래에서 **네트워크 설정** 링크를 클릭합니다.
   네트워크 연결 창이 열립니다. 이 창에는 네트워크 목록이 표시됩니다.
5. 목록에 누락된 네트워크가 있으면 추가합니다.

네트워크 드라이브 검사 비활성화

Kaspersky Endpoint Security for Windows 네트워크 드라이브 검사 시, 상당한 부하가 발생할 수 있습니다. 파일 서버에서 간접 검사를 수행하는 것이 더 편리합니다.

Kaspersky Endpoint Security for Windows 정책 속성에서 네트워크 드라이브 검사를 중지할 수 있습니다. 이 정책 속성에 관한 설명은 Kaspersky Endpoint Security for Windows 설명서를 참조하십시오.

네트워크 드라이브 검사를 중지하려면 다음을 수행합니다:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. Kaspersky Endpoint Security for Windows의 정책을 클릭합니다.
   선택한 정책의 속성 창이 열립니다.
3. 정책 속성에서 **애플리케이션 설정 → 필수 위협 보호 → 파일 위협 보호**로 갑니다.
4. **보호 범위**에서 **모든 네트워크 드라이브** 옵션을 비활성화합니다.
5. **확인**을 누릅니다.

네트워크 드라이브 검색이 비활성화됩니다.

중앙 관리 서버 메모리에서 소프트웨어 세부 정보 제외

중앙 관리 서버가 네트워크 기기에서 시작되는 소프트웨어 모듈에 대한 정보를 저장하지 않는 것을 권장합니다. 이렇게 하면 중앙 관리 서버의 메모리 오버런을 방지할 수 있습니다.

Kaspersky Endpoint Security for Windows 정책 속성에서 이 정보 저장을 비활성화할 수 있습니다.

설치된 소프트웨어 모듈에 대한 정보 저장을 비활성화하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. Kaspersky Endpoint Security for Windows의 정책을 클릭합니다.
   선택한 정책의 속성 창이 열립니다.
3. 정책 속성에서 **애플리케이션 설정 → 일반 설정 → 리포트 및 저장소**로 이동합니다.
4. **중앙 관리 서버로의 데이터 전송**에서 최상위 정책의 **시작된 애플리케이션 정보** 확인란이 선택되어 있다면 선택 해제합니다.
   이 확인란을 선택하면 네트워크에 연결된 기기에 설치되어 있는 모든 소프트웨어 모듈의 모든 버전에 대한 정보가 중앙 관리 서버 데이터베이스에 저장됩니다. 이 정보를 저장하려면 Kaspersky Security Center 데이터베이스에서 수십 GB에 달하는 매우 많은 양의 디스크 공간이 필요할 수 있습니다.

설치된 소프트웨어 모듈에 대한 정보는 더 이상 중앙 관리 서버 데이터베이스에 저장되지 않습니다.

워크스테이션에서 Kaspersky Endpoint Security for Windows 인터페이스에 대한 접근 구성

Kaspersky Security Center를 통해 중앙 집중식 모드로 조직 네트워크의 위협 보호를 관리해야 한다면, 아래 설명된 대로 Kaspersky Endpoint Security for Windows 정책 속성에서 인터페이스 설정을 지정하십시오. 결과적으로 워크스테이션에서 Kaspersky Endpoint Security for Windows에 대한 무단 접근과 Kaspersky Endpoint Security for Windows 설정 변경을 방지할 수 있습니다.

이 정책 속성에 관한 설명은 Kaspersky Endpoint Security for Windows 설명서를 참조하십시오.

권장 인터페이스 설정을 지정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. Kaspersky Endpoint Security for Windows의 정책을 클릭합니다.
   선택한 정책의 속성 창이 열립니다.
3. 정책 속성에서 **애플리케이션 설정 → 일반 설정 → 인터페이스**로 이동합니다.
4. **사용자와의 상호 작용**에서 **사용자 인터페이스 표시 안 함** 옵션을 선택합니다. 이렇게 하면 워크스테이션에서 Kaspersky Endpoint Security for Windows 사용자 인터페이스 표시가 비활성화되어 사용자가 Kaspersky Endpoint Security for Windows 설정을 변경할 수 없습니다.
5. **암호 보호**에서 토글 스위치를 활성화합니다. 이렇게 하면 워크스테이션의 Kaspersky Endpoint Security for Windows 설정에서 무단 변경이나 의도치 않은 변경 위험이 감소합니다.

Kaspersky Endpoint Security for Windows의 인터페이스에 대한 권장 설정이 지정됩니다.

중앙 관리 서버 데이터베이스에 중요한 정책 이벤트 저장

중앙 관리 서버 데이터베이스 오버플로를 방지하려면 중요한 이벤트만 데이터베이스에 저장하는 것이 좋습니다.

중앙 관리 서버 데이터베이스에서 중요한 이벤트 등록을 구성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. Kaspersky Endpoint Security for Windows의 정책을 클릭합니다.
   선택한 정책의 속성 창이 열립니다.
3. 정책 속성에서 **이벤트 구성** 탭을 엽니다.
4. **심각** 섹션에서 **이벤트 추가**를 누르고 다음 이벤트 옆에 있는 확인란만 선택합니다.
   - *최종 사용자 라이센스 계약서 위반*
   - *애플리케이션 자동 시작이 비활성화되었습니다*
   - *활성화 오류*
   - *활성 위협 탐지됨. 고급 치료 시작 필요*
   - *치료 불가*
   - *이전에 열린 위험한 링크가 탐지됨*
   - *프로세스 종료*
   - *네트워크 활동이 차단됨*
   - *네트워크 공격이 탐지됨*

- *애플리케이션 시작이 금지됨*
- *접근 거부됨(로컬 기반)*
- *접근 거부됨(KSN)*
- *로컬 업데이트 오류*
- *두 작업을 동시에 시작할 수 없음*
- *Kaspersky Security Center와 통신 오류*
- *일부 구성 요소가 업데이트되지 않았습니다*
- *파일 암호화/복호화 규칙 적용 오류*
- *휴대용 모드 활성화 오류*
- *휴대용 모드 비활성화 오류*
- *암호화 모듈을 로드할 수 없음*
- *정책을 적용할 수 없음*
- *애플리케이션 구성 요소 변경 오류*

5. **확인**를 누릅니다.
6. **기능 실패** 섹션에서 **이벤트 추가**를 클릭하고 *작업 설정이 잘못되었습니다. 설정이 적용되지 않았습니다.* 이벤트 옆의 확인란을 선택합니다.
7. **확인**를 누릅니다.
8. **경고** 섹션에서 **이벤트 추가**를 누르고 다음 이벤트 옆에 있는 확인란만 선택합니다.
   - *자기 보호가 비활성화되었습니다*
   - *보호 구성 요소가 비활성화되었습니다*
   - *잘못된 예비 키*
   - *침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어가 탐지되었습니다(로컬 기반)*
   - *침입자에게 악용되어 사용자의 컴퓨터나 개인 데이터를 손상할 수 있는 합법적인 소프트웨어가 탐지되었습니다(KSN)*
   - *개체 삭제됨*
   - *개체 치료됨*
   - *사용자가 암호화 정책을 거부함*
   - *관리자가 Kaspersky Anti Targeted Attack Platform 서버의 격리 저장소에서 파일을 복원했습니다*

- *관리자가 파일을 Kaspersky Anti Targeted Attack Platform 서버로 격리했습니다*
- *관리자에게 애플리케이션 시작 차단 메시지 보내기*
- *관리자에게 장치 접근 차단 메시지 보내기*
- *관리자에게 웹 페이지 접근 차단 메시지 보내기*

9. **확인**를 누릅니다.
10. **정보** 섹션에서 **이벤트 추가**를 누르고 다음 이벤트 옆에 있는 확인란만 선택합니다.
    - *개체 백업 복사본 생성됨*
    - *테스트 모드에서의 애플리케이션 시작이 차단됨*
11. **확인**를 누릅니다.

중앙 관리 서버 데이터베이스의 중요한 이벤트 등록이 구성됨

Kaspersky Endpoint Security용 그룹 업데이트 작업 수동 설정

Kaspersky Endpoint Security에서 권장되는 최적의 스케줄 옵션은 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후** 및 **자동으로 작업 시작 임의 지연 사용** 확인란 선택하는 경우입니다.

매체 제어에 의해 차단된 외부 기기에 대한 오프라인 접근 권한 부여

Kaspersky Endpoint Security for Windows 정책의 매체 제어 구성 요소에서 클라이언트 기기에 설치되어 있거나 연결된 외부 기기(예: 하드 드라이브, 카메라, Wi-Fi 모듈)에 대한 사용자 접근 권한을 관리할 수 있습니다. 이렇게 하면 이러한 외부 기기가 연결되어 있을 때 클라이언트 기기를 감염으로부터 보호하거나 데이터 손실 또는 유출을 방지할 수 있습니다.

매체 제어에 의해 차단된 외부 기기에 대해 임시 접근 권한을 부여해야 하지만 기기를 신뢰할 수 있는 기기 목록에는 추가할 수 없는 경우 외부 기기에 대한 임시 오프라인 접근 권한을 부여하면 됩니다. 오프라인 접근 권한이란, 클라이언트 기기가 네트워크에 접근할 수 없다는 의미입니다.

> 기기 제어가 차단한 외부 기기에 오프라인 접근을 허용하려면, Kaspersky Endpoint Security for Windows 정책 설정의 **애플리케이션 설정 → 보안 제어 → 장치 제어** 섹션에서 **임시 접근 요청 허용** 옵션을 활성화해야 합니다.

매체 제어에 의해 차단된 외부 기기에 대한 오프라인 접근 권한 부여는 다음 단계를 따라 이루어집니다.

1. Kaspersky Endpoint Security for Windows 대화 창에서 차단된 외부 기기에 접근하고자 하는 기기 사용자는 접근 권한 요청 파일을 생성하여 Kaspersky Security Center 관리자에게 전송합니다.

2. 이 요청을 받은 Kaspersky Security Center 관리자는 접근 허용 키 파일을 만들어서 기기 사용자에게 전송합니다.

3. Kaspersky Endpoint Security for Windows 대화 창에서 기기 사용자는 접근 허용 키 파일을 활성화하고 외부 기기에 대한 임시 접근 권한을 획득합니다.

매체 제어에 의해 차단된 외부 기기에 대한 임시 접근 권한을 부여하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.

   관리 중인 기기 목록이 표시됩니다.

2. 목록에서 기기 제어로 차단된 외부 기기에 대한 접근 권한을 요청하는 사용자 기기를 선택합니다.

   하나의 기기만 선택할 수 있습니다.

3. 관리 중인 기기 목록 위에 있는 생략 부호 버튼(...)을 클릭한 다음 **오프라인 모드인 기기에 접근 권한 부여** 버튼을 클릭합니다.

4. **애플리케이션 설정** 창이 열리면 **장치 제어** 섹션에서 **찾기** 버튼을 클릭합니다.

5. 사용자로부터 받은 접근 권한 요청 파일을 선택한 후 **열기** 버튼을 클릭합니다. 파일은 AKEY 형식이어야 합니다.

   사용자가 접근 권한을 요청한 잠긴 기기의 세부 정보가 표시됩니다.

6. **접근 지속 시간** 설정의 값을 지정합니다.

   이 설정은 잠긴 기기에 대해 사용자 접근 권한을 부여하는 시간의 길이를 정의합니다. 기본값은 접근 권한 요청 파일 생성 시 사용자가 지정한 값입니다.

7. 기기에서 액세스 키를 활성화할 수 있는 기간을 지정합니다.

   이 설정은 사용자가 제공된 접근 허용 키로 차단된 기기에 대한 접근 권한을 활성화할 수 있는 기간을 정의합니다.

8. **저장** 버튼을 누릅니다.

   그러면 Microsoft Windows의 표준 **접근 허용 키 저장** 창이 열립니다.

9. 차단된 기기에 대한 접근 허용 키가 포함된 파일을 저장할 대상 폴더를 선택합니다.

10. **저장** 버튼을 누릅니다.

그러면 접근 허용 키 파일을 사용자에게 보내고 사용자가 Kaspersky Endpoint Security for Windows 대화 창에서 이 파일을 활성화하면 사용자는 일정 기간 동안 차단된 기기에 임시로 접근할 수 있게 됩니다.

애플리케이션 또는 소프트웨어 업데이트 원격 제거

선택한 기기에서 애플리케이션 또는 소프트웨어 업데이트를 원격으로 제거하려면 다음 단계를 따르십시오.

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼으로 마법사를 진행합니다.
3. Kaspersky Security Center 애플리케이션의 경우 **애플리케이션을 원격으로 제거** 작업 유형을 선택합니다.
4. 만들고 있는 작업의 이름을 지정합니다.
   작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
5. 이 작업이 할당되는 기기를 선택합니다.
6. 제거할 소프트웨어 종류를 선택한 다음 제거할 애플리케이션, 업데이트 또는 패치를 구체적으로 선택합니다.

   - **관리 중인 애플리케이션 제거**

     Kaspersky 애플리케이션 목록이 표시됩니다. 제거할 애플리케이션을 선택합니다.

   - **비호환 애플리케이션 제거**

     Kaspersky 보안 제품 또는 Kaspersky Security Center와 호환되지 않는 애플리케이션 목록이 표시됩니다. 제거할 애플리케이션 옆에 있는 확인란을 선택합니다.

   - **자산 관리(소프트웨어)에서 애플리케이션 설치 제거**

     기본적으로 네트워크 에이전트는 관리 중인 기기에 설치된 애플리케이션에 대한 중앙 관리 서버 정보를 전송합니다. 설치된 애플리케이션 목록은 자산 관리(소프트웨어)에 저장됩니다.

     자산 관리(소프트웨어)에서 애플리케이션을 선택하려면 다음 단계를 따르십시오.

     a. **제거할 애플리케이션** 필드를 누른 다음 제거할 애플리케이션을 선택합니다.

        Kaspersky Security Center 네트워크 에이전트를 선택하면, 작업 실행 시 *완료됨* 상태가 제거 프로세스 시작을 나타냅니다. Kaspersky Security Center 네트워크 에이전트를 제거해도 상태는 변경되지 않습니다. 작업이 실패하면 상태가 *실패*로 변경됩니다.

b. 제거 옵션을 지정합니다.

- **제거 모드**

  애플리케이션 제거 방법을 선택합니다.

  - **제거 명령을 자동으로 정의**

    애플리케이션에 애플리케이션 공급업체에서 정의한 제거 명령이 있는 경우 Kaspersky Security Center는 이 명령을 사용합니다. 이 옵션은 선택하는 것이 좋습니다.

  - **제거 명령 지정**

    애플리케이션 제거 명령을 지정하려면 이 옵션을 선택합니다.

    > 먼저, **제거 명령을 자동으로 정의** 옵션을 사용하여 애플리케이션을 제거해 보는 것이 좋습니다. 자동으로 정의된 명령을 통한 제거가 실패하면 사용자의 명령을 사용합니다.

    필드에 설치 명령을 입력하고 다음 옵션을 지정합니다.

    기본 명령이 자동 감지되지 않는 경우에만 이 제거 명령 사용

    > Kaspersky Security Center는 선택한 애플리케이션에 애플리케이션 공급업체가 정의한 제거 명령이 있는지를 확인합니다. 명령이 발견되면 Kaspersky Security Center는 **애플리케이션 제거 명령** 필드에 지정된 명령 대신 이 명령을 사용합니다.
    >
    > 이 옵션은 활성화하는 것이 좋습니다.

- **애플리케이션 제거 성공 후 재시작 필요**

  애플리케이션을 성공적으로 제거한 후 관리 중인 기기의 운영 체제를 다시 시작해야 하는 경우 운영 체제는 자동으로 다시 시작됩니다.

- **지정한 애플리케이션 업데이트, 패치 또는 타사 애플리케이션 제거**

  업데이트, 패치, 타사 애플리케이션 목록이 표시됩니다. 제거할 항목을 선택합니다.

  표시된 목록은 애플리케이션 및 업데이트의 일반적인 목록이며 관리 중인 기기에 설치된 애플리케이션 및 업데이트와 일치하지 않습니다. 항목을 선택하기 전에 관리 중인 기기에 설치된 애플리케이션 또는 업데이트가 작업 범위에 정의되어 있는지 확인하는 것이 좋습니다. 속성 창을 통해 애플리케이션 또는 업데이트가 설치되는 기기 목록을 확인할 수 있습니다.

  기기 목록을 확인하려면 다음 단계를 따르십시오.

  a. 애플리케이션 또는 업데이트의 이름을 누릅니다.

  속성 창이 열립니다.

  b. **기기** 섹션을 엽니다.

  기기 속성 창에서도 설치된 애플리케이션 및 업데이트의 목록을 확인할 수 있습니다.

7. 클라이언트 기기에서 제거 유틸리티를 다운로드하는 방법을 지정합니다.

- **네트워크 에이전트 이용**

  파일은 클라이언트 기기에 설치된 네트워크 에이전트에 의해 클라이언트 기기로 전달됩니다.

  이 옵션이 비활성화되어 있으면 파일은 Microsoft Windows 도구를 사용하여 전달됩니다.

  네트워크 에이전트가 설치되어 있는 기기에 작업이 할당된 경우 이 옵션을 활성화하는 것이 좋습니다.

- **중앙 관리 서버에서 대상 운영 체제의 관리 공유 폴더로 다운로드**

  파일은 중앙 관리 서버 운영 체제 도구를 사용하여 클라이언트 기기로 전송됩니다. 이 옵션은 클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않아도 활성화할 수 있지만, 이 경우 클라이언트 기기는 중앙 관리 서버와 같은 네트워크에 있어야 합니다.

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

  파일은 운영 체제 도구를 사용하여 배포 지점을 통해 클라이언트 기기로 전송됩니다. 네트워크에 하나 이상의 배포 지점이 있어야 이 옵션을 활성화할 수 있습니다.

  네트워크 에이전트 이용 옵션이 활성화된 경우 파일은 네트워크 에이전트 도구를 사용할 수 없는 경우에만 운영 체제 도구로 전달됩니다.

- **최대 동시 다운로드 수**

  중앙 관리 서버에서 동시에 파일을 전송할 수 있도록 허용되는 클라이언트 기기의 최대 수입니다. 이 숫자가 클수록 애플리케이션이 제거되는 속도는 빨라지지만 중앙 관리 서버의 부하도 커집니다.

- **최대 제거 시도 횟수**

  애플리케이션을 원격으로 제거 작업을 실행할 때 Kaspersky Security Center가 파라미터로 지정된 설치 프로그램 실행 횟수 이내에 관리 중인 기기에 애플리케이션을 제거하지 못하면, Kaspersky Security Center가 이 관리 중인 기기에 제거 유틸리티 전송을 중지하고 해당 기기에서 설치 프로그램을 더 이상 시작하지 않습니다.

  최대 제거 시도 횟수 파라미터를 사용하면 관리 중인 기기의 리소스를 절약하고 트래픽(설치 제거, MSI 파일 실행 및 오류 메시지)을 줄일 수 있습니다.

  작업 시작 시도를 반복하면 해당 기기에 제거를 방해하는 문제가 표시될 수 있습니다. 관리자는 지정된 제거 시도 횟수 내에 문제를 해결하고 작업을 다시 시작(수동으로 또는 스케줄에 따라)해야 합니다.

  그런데도 제거가 완료되지 않으면 문제를 해결할 수 없는 것으로 간주되고 추가적인 작업 시작은 리소스 및 트래픽의 불필요한 소비 측면에서 불필요한 것으로 간주됩니다.

  작업이 생성되면 시도 횟수 카운터가 `0`으로 설정됩니다. 기기에서 오류를 반환하면 인스톨러 실행 시 카운터 판독 값이 증가합니다.

  파라미터에서 지정된 시도 횟수가 초과되었지만 기기가 애플리케이션을 제거할 준비가 된 경우 **최대 제거 시도 횟수** 파라미터값을 높이고 애플리케이션 제거 작업을 시작할 수 있습니다. 또는 새 *애플리케이션을 원격으로 제거* 작업을 생성할 수 있습니다.

- **다운로드하기 전에 운영 체제 유형 확인**

  클라이언트 기기에 파일을 전송하기 전에 Kaspersky Security Center는 설치 유틸리티 설정을 클라이언트 기기의 운영 체제에 적용할 수 있는지 확인합니다. 설정을 적용할 수 없다면, Kaspersky Security Center는 파일을 전송하지 않고 애플리케이션도 설치하지 않습니다. 예를 들어, 다양한 운영 체제를 실행하는 기기가 포함된 관리 그룹의 기기에 일부 애플리케이션을 설치하려면, 관리 그룹에 설치 작업을 할당하고 이 옵션을 활성화하여 필요한 운영 체제 이외의 운영 체제를 실행하는 기기를 건너뜁니다.

  미할당 기기에 네트워크 에이전트를 원격 설치하면 Kaspersky Security Center 또는 배포 지점이 **다운로드하기 전에 운영 체제 유형 확인**에 상관없이 기기의 운영 체제 유형을 자동으로 결정합니다.

- **제거 암호 사용**

  이전 단계에서 **관리 중인 애플리케이션 제거**를 선택한 다음 **제거할 애플리케이션** 필드에 Kaspersky Security Center 네트워크 에이전트를 지정했다면 이 파라미터가 표시됩니다.

  이전에 네트워크 에이전트 정책 설정에서 네트워크 에이전트 원격 제거를 위한 암호를 설정했다면 **제거 암호 사용** 확인란을 선택한 다음 **암호** 필드에 제거 암호를 입력하십시오. 네트워크 에이전트 원격 제거를 위한 암호를 설정하지 않았다면 확인란을 선택하지 마십시오.

8. 운영 체제 다시 시작 설정을 지정합니다.

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **반복해서 물어보기(분)**

  이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

  이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

- **다음 시간 이후에 재시작(분)**

  사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

9. 필요한 경우 원격 제거 작업을 시작하는 데 사용할 계정을 추가합니다.

- **계정 필요 없음(네트워크 에이전트가 설치되어 있음)**

  이 옵션을 선택하면 애플리케이션 설치 프로그램을 실행할 계정을 지정하지 않아도 됩니다. 중앙 관리 서버가 실행 중인 계정에서 작업이 실행됩니다.

  클라이언트 기기에 네트워크 에이전트가 설치되어 있지 않다면, 이 옵션은 이용할 수 없습니다.

- **계정 필요(네트워크 에이전트는 사용되지 않음)**

  애플리케이션 원격 제거 작업을 할당한 기기에 네트워크 에이전트가 설치되어 있지 않다면 이 옵션을 선택합니다. 이때, 사용자 계정 또는 SSH 인증서를 지정하여 애플리케이션을 제거할 수 있습니다.

  - **로컬 계정**. 이 옵션을 선택했다면 애플리케이션 설치 프로그램을 실행할 계정을 지정합니다. **추가** 버튼을 클릭하고 **로컬 계정**을 선택한 다음 사용자 계정 자격 증명을 지정합니다.

    예를 들어 이 작업이 할당된 모든 기기에 필요한 모든 권한이 어떤 계정에도 없다면, 사용자 계정을 여러 개 지정할 수 있습니다. 이때, 작업 실행 시 추가한 모든 계정을 위에서부터 순서대로 사용합니다.

  - **SSH 인증서**. Linux 기반 클라이언트 기기에서 애플리케이션을 제거한다면 사용자 계정 대신 SSH 인증서를 지정할 수 있습니다. **추가** 버튼을 클릭하고 **SSH 인증서**를 선택한 다음 인증서의 개인 및 공개 키를 지정합니다.

    개인 키를 생성하려면 ssh-keygen 유틸리티를 사용할 수 있습니다. Kaspersky Security Center는 개인 키의 PEM 형식을 지원하지만 ssh-keygen 유틸리티는 기본적으로 OPENSSH 형식으로 SSH 키를 생성합니다. Kaspersky Security Center에서는 OPENSSH 형식을 지원하지 않습니다. 지원되는 PEM 형식으로 개인 키를 생성하려면 ssh-keygen 명령에 -m PEM 옵션을 추가합니다.

    예:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< 사용자 이메일 >"
    ```

10. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

11. **마침** 버튼을 누릅니다.

    그러면 작업이 생성되고 작업 목록에 표시됩니다.

12. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

13. 작업 속성 창에서 일반 작업 설정을 지정합니다.

14. **저장** 버튼을 누릅니다.

15. 이 작업을 직접 실행하거나 작업 설정에 지정된 스케줄에 따라 실행될 때까지 기다립니다.

    원격 제거 작업이 완료되면 선택한 애플리케이션이 지정된 기기에서 제거됩니다.

원격 설치 제거 문제

가끔 타사 애플리케이션 원격 제거가 "이 기기에서 원격 제거가 경고와 함께 끝났습니다. 제거할 애플리케이션이 설치되지 않았습니다"라는 경고와 함께 끝날 수 있습니다. 이 문제는 제거하려는 애플리케이션을 이미 제거했거나 개별 사용자를 대상으로만 설치했을 때 발생합니다. 개별 사용자용으로 설치한 애플리케이션(또는 사용자별 애플리케이션)은 해당 사용자가 로그인하지 않으면 보이지 않고 원격 제거할 수도 없습니다.

이는 같은 기기에서 여러 사용자가 사용할 수 있는 애플리케이션(또는 기기별 애플리케이션)과는 반대입니다. 기기별 애플리케이션은 기기의 모든 사용자가 보고 접근할 수 있습니다.

따라서 사용자별 애플리케이션은 해당 사용자가 로그인했을 때만 제거할 수 있습니다.

설치한 애플리케이션에 관한 정보 출처

네트워크 에이전트는 다음 레지스트리 키에서 Windows 기기에 설치된 소프트웨어 정보를 검색합니다.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  모든 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  모든 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  현재 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  특정 사용자를 위해 설치된 애플리케이션에 관한 정보가 들어 있습니다.

작업

이 섹션에서는 Kaspersky Security Center에서 사용하는 작업을 설명합니다.

작업 정보

Kaspersky Security Center에서는 *작업*을 만들고 실행하여 기기에 설치된 Kaspersky 보안 제품을 관리할 수 있습니다. 작업은 애플리케이션을 설치, 실행 및 중단하고, 파일을 검사하며, 데이터베이스와 소프트웨어 모듈을 업데이트하고, 애플리케이션에 대해 기타 작업을 수행하는 데 필요합니다.

Kaspersky Security Center 웹 콘솔 서버에 특정 애플리케이션용 관리 플러그인이 설치되어 있어야 Kaspersky Security Center 웹 콘솔을 사용하여 해당 애플리케이션용 작업을 생성할 수 있습니다.

중앙 관리 서버와 기기에서 작업을 수행할 수 있습니다.

중앙 관리 서버에서 수행되는 작업은 다음과 같습니다.

- 리포트 자동 배포
- 저장소 업데이트 다운로드
- 중앙 관리 서버 데이터 백업
- 데이터베이스 유지 보수

기기에서 수행되는 작업 유형은 다음과 같습니다:

- *로컬 작업* - 특정 기기에서 수행되는 작업

  로컬 작업은 관리자가 관리 콘솔 도구를 사용하여 수정할 수도 있고, 원격 기기의 사용자가 보안 제품 인터페이스 등을 통해 수정할 수도 있습니다. 관리자와 관리 중인 기기 사용자가 로컬 작업을 동시에 수정한 경우에는 우선 순위가 더 높은 관리자가 수행한 변경 사항이 적용됩니다.

- *그룹 작업* - 특정 그룹의 모든 기기에서 수행되는 작업

  작업 속성에 별도로 지정된 경우가 아니면 그룹 작업은 선택한 그룹의 모든 하위 그룹에도 영향을 줍니다. 그룹 작업은 이 그룹이나 해당 하위 그룹에 배포한 보조 및 가상 중앙 관리 서버에 연결된 기기에도 선택적으로 적용됩니다.

- *글로벌 작업* - 그룹에 포함되어 있는지 여부에 관계없이 선택한 기기에서 수행되는 작업.

각 애플리케이션에 대해 그룹 작업, 글로벌 작업 또는 로컬 작업을 원하는 수만큼 만들 수 있습니다.

작업 설정을 변경하고 작업 진행 상황을 확인하며, 해당 설정의 복사, 내보내기, 가져오기 및 삭제를 수행할 수 있습니다.

작업을 만든 애플리케이션이 실행 중인 경우에만 기기에서 작업이 시작됩니다.

작업 실행 결과는 각 기기의 운영 체제 이벤트 로그, 중앙 관리 서버의 운영 체제 이벤트 로그, 중앙 관리 서버 데이터베이스에 저장됩니다.

작업 설정에 기밀 데이터를 포함하지 마십시오. 예를 들어, 도메인 관리자 암호를 지정하지 마십시오.

작업 범위 정보

*작업의 범위*는 작업이 수행되는 기기 세트입니다. 범위의 유형은 다음과 같습니다:

- *로컬 작업*의 경우 범위는 기기 자체입니다.
- *중앙 관리 서버 작업*의 경우 범위는 중앙 관리 서버입니다.
- *그룹 작업*의 경우 범위는 그룹에 포함된 기기 목록입니다.

*글로벌 작업*을 만들 때는 다음 방법을 사용하여 범위를 지정할 수 있습니다.

- 특정 기기를 수동으로 지정합니다.

  IP 주소(또는 IP 범위), NetBIOS 이름 또는 DNS 이름을 기기의 주소로 사용할 수 있습니다.

- 추가할 기기의 주소가 포함된 .txt 파일에서 기기의 목록을 가져옵니다(줄당 하나의 주소를 표시해야 함).

  파일에서 기기의 목록을 가져오거나 수동으로 작성할 경우 기기가 이름으로 식별되면, 중앙 관리 서버 데이터에 이미 정보가 입력된 기기만 목록에 포함됩니다. 또한 해당 기기가 연결될 때나 기기 발견 중에 정보가 입력된 상태여야 합니다.

- 기기 선택 지정.

  시간이 지남에 따라 조회에 포함된 기기 집합이 변경되면 작업 범위도 변경됩니다. 기기에 설치되어 있는 소프트웨어를 비롯한 기기 특성과, 기기에 할당된 태그를 기준으로 기기를 조회할 수 있습니다. 기기 조회 방식은 가장 유연하게 작업 범위를 지정하는 방법입니다.

  기기 선택 작업은 항상 중앙 관리 서버에서 스케줄에 따라 실행됩니다. 중앙 관리 서버에 연결되어 있지 않은 기기에서는 이러한 작업을 실행할 수 없습니다. 다른 방법을 사용하여 범위를 지정한 작업은 기기에서 직접 실행되므로 중앙 관리 서버에 대한 기기 연결을 사용하지 않습니다.

기기 선택을 통한 작업은 기기의 로컬 시간에 실행되는 대신 중앙 관리 서버의 로컬 시간에 실행됩니다. 다른 방법을 사용하여 범위를 지정한 작업은 기기의 로컬 시간에 실행됩니다.

작업 만들기

작업을 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **작업**로 이동합니다.
2. **추가**를 누릅니다.

   새 작업 마법사가 시작됩니다. 해당 지침을 따릅니다.
3. 기본 작업 설정을 수정하려면 **생성이 완료되면 작업 세부 정보 열기** 페이지에서 **작업 생성 마침** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.
4. **마침** 버튼을 누릅니다.

그러면 작업이 생성되고 작업 목록에 표시됩니다.

선택한 기기에 할당된 새 작업을 생성하려면:

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.

   관리 중인 기기 목록이 표시됩니다.

2. 관리 중인 기기 목록에서 작업을 실행할 기기 옆의 확인란을 선택합니다. 검색 및 필터링 기능을 사용하여 필요한 기기를 찾을 수 있습니다.

3. **작업 실행** 버튼을 클릭하고 **새 작업 추가**을 선택합니다.

   새 작업 마법사가 시작됩니다.

   마법사의 첫 번째 단계에서 작업 범위에 포함하도록 선택한 기기를 제거할 수 있습니다. 마법사의 지침을 따릅니다.

4. **마침** 버튼을 누릅니다.

선택한 기기에 대한 작업이 생성됩니다.

수동으로 작업 시작

애플리케이션은 각 작업 속성에 지정된 스케줄 설정에 따라 작업을 시작합니다. 언제든 수동으로 작업 목록의 작업을 시작할 수 있습니다. 또는 **관리 중인 기기** 목록에서 기기를 선택한 다음 해당 기기에 대한 기존 작업을 시작할 수 있습니다.

작업을 수동으로 시작하려면 다음 단계를 따릅니다.

1. 메인 애플리케이션 창에서 **에셋(기기) → 작업**로 이동합니다.

2. 작업 목록에서 시작할 작업 옆에 있는 확인란을 선택합니다.

3. **시작** 버튼을 누릅니다.

작업이 시작됩니다. **상태** 열 또는 **결과** 버튼을 눌러 작업 상태를 확인할 수 있습니다.

작업 목록 보기

Kaspersky Security Center에서 생성된 작업 목록을 볼 수 있습니다.

작업 목록을 보려면 다음을 수행합니다.

메인 애플리케이션 창에서 **에셋(기기) → 작업**로 이동합니다.

작업 목록이 표시됩니다. 작업은 관련된 애플리케이션 이름별로 그룹화됩니다. 예를 들어 *애플리케이션을 원격으로 제거* 작업은 중앙 관리 서버와 관련이 있고 *취약점 및 필요한 업데이트 검색* 작업은 네트워크 에이전트를 나타냅니다.

작업 속성을 보려면

작업 이름을 누릅니다.

작업 속성 창이 여러 이름이 지정된 탭으로 표시됩니다. 예를 들어, **작업 유형**이 **일반** 탭에 표시되고 **스케줄** 탭에는 작업 스케줄이 표시됩니다.

일반 작업 설정

이 섹션은 대부분의 작업을 보고 구성할 수 있는 설정을 포함합니다. 사용 가능한 설정 목록은 구성 중인 작업에 따라 다릅니다.

작업 생성 중에 지정하는 설정

작업을 생성할 때 다음과 같은 설정을 지정할 수 있습니다. 이러한 설정 중 일부는 생성된 작업의 속성에서 수정할 수도 있습니다.

- 운영 체제 다시 시작 설정:
  - **기기 다시 시작 안 함**

    작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

  - **기기 다시 시작**

    이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

  - **사용자 확인 후 처리**

    클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **반복해서 물어보기(분)**

    이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

    기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

    이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

  - **다음 시간 이후에 재시작(분)**

    사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- 작업 스케줄 설정:

  스케줄의 종류는 작업에 따라 다를 수 있습니다.

  - **작업 시작 설정:**

    - **N시간마다**

      작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

      작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

    - **N일마다**

      작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.

      기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

    - **N분마다**

      작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.

      기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

    - **요일별**

      이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.

      기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

    - **월별**

      이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

      지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.

기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **한번만**

  작업은 지정한 날짜와 시간(기본값은 작업 생성일)에 한 번 실행됩니다.

- **즉시**

  작업은 해당 설정이 저장되는 즉시 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**

  저장소에 업데이트가 다운로드되고 나면 작업이 실행됩니다. 예를 들어 취약점 및 필요한 업데이트 검색 작업에 이 스케줄을 사용할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 자동 임의 지연**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

- 이 작업이 할당되는 기기:
  - **중앙 관리 서버가 발견한 기기 중에서 선택**

    특정 기기에 작업이 할당됩니다. 이 특정 기기에는 관리 그룹에 속하는 기기와 미할당 기기가 포함될 수 있습니다.

    예를 들어 미할당 기기에 네트워크 에이전트를 설치하는 작업에서 이 옵션을 사용할 수 있습니다.

  - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

    작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

    특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

  - **기기 선택 결과에 작업 할당**

    기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

    예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

  - **관리 그룹에 작업 할당**

    관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

    예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

    관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

- 계정 설정:
  - **기본 계정**

    해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **계정 지정**

    계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

  - **계정**

    작업 실행에 사용되는 계정입니다.

- **암호**

  작업을 실행할 계정의 암호입니다.

작업 생성 후에 지정하는 설정

다음 설정은 작업을 생성한 후에만 지정할 수 있습니다.

- 그룹 작업 설정:
  - **하위 그룹에 배포**

    이 옵션은 그룹 작업 설정에서만 사용할 수 있습니다.

    이 옵션이 활성화되면 작업 범위 에 다음이 포함됩니다.
    - 작업을 생성하는 동안 선택한 관리 그룹입니다.
    - 관리 그룹은 그룹 계층에서 모든 수준에 있는 선택된 관리 그룹에 종속됩니다.

    이 옵션이 비활성화되면 작업 범위에는 작업을 생성하는 동안 선택한 관리 그룹만 포함됩니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **보조 및 가상 중앙 관리 서버에 배포**

    이 옵션을 사용하면 기본 중앙 관리 서버에서 유효한 작업이 보조 중앙 관리 서버(가상 서버 포함)에도 적용됩니다. 동일한 유형의 작업이 보조 중앙 관리 서버에 이미 있는 경우 두 작업 모두 보조 중앙 관리 서버(기본 작업 및 기본 중앙 관리 서버에서 상속된 작업)에 적용됩니다.

    이 옵션은 **하위 그룹에 배포** 옵션이 활성화된 경우에만 사용할 수 있습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- 고급 스케줄 설정:
  - **작업 시작 전에 Wake-on-LAN 기능으로 기기 켜기**

    작업이 시작되기 전 지정된 시간에 기기의 운영 체제가 시작됩니다. 기본 기간은 5분입니다.

    작업을 시작하려 할 때 꺼져 있는 기기를 포함하여 작업 범위의 모든 클라이언트 기기에서 작업을 실행하려는 경우 이 옵션을 활성화합니다.

    작업이 완료된 후 기기를 자동으로 끄려면 **작업 완료 후 기기 종료** 옵션을 활성화합니다. 이 옵션은 같은 창에서 찾을 수 있습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **작업 완료 후 기기 종료**

    예를 들어 매주 금요일 업무 시간 후에 클라이언트 기기에 업데이트를 설치한 다음 주말 동안은 해당 기기를 꺼 두는 업데이트 설치 작업의 경우 이 옵션을 활성화할 수 있습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- **작업이 다음 시간보다 오래 실행되면 중지**

  작업 완료 여부에 관계없이 지정된 시간이 경과한 후 작업이 자동으로 중지됩니다.
  실행 시간이 너무 오래 걸리는 작업을 중단(중지)하려는 경우 이 옵션을 활성화합니다.
  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 작업 실행 시간은 120분입니다.

- 공지 설정:

  - **작업 기록 저장** 블록:

    - **다음 기간만큼 중앙 관리 서버에 저장(일)**

      작업 범위의 모든 클라이언트 기기에서 수행하는 작업 실행과 관련된 애플리케이션 이벤트가 지정된 기간(일) 동안 중앙 관리 서버에 저장됩니다. 이 기간이 지나면 중앙 관리 서버에서 해당 정보가 삭제됩니다.

      기본적으로 이 옵션은 켜져 있습니다.

    - **기기의 OS 이벤트 로그에 저장**

      작업 실행과 관련된 애플리케이션 이벤트가 각 클라이언트 기기의 Windows 이벤트 로그에 로컬로 저장됩니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    - **중앙 관리 서버의 OS 이벤트 로그에 저장**

      작업 범위의 모든 클라이언트 기기에서 수행하는 작업 실행과 관련된 애플리케이션 이벤트가 중앙 관리 서버 OS(운영 체제)의 Windows 이벤트 로그에 중앙 집중식으로 저장됩니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    - **모든 이벤트 저장**

      이 옵션을 선택하면 작업과 관련된 모든 이벤트가 이벤트 로그에 저장됩니다.

    - **작업 진행 상태와 관련된 이벤트 저장**

      이 옵션을 선택하면 작업 실행과 관련된 이벤트만 이벤트 로그에 저장됩니다.

    - **작업 실행 결과만 저장**

      이 옵션을 선택하면 작업 결과와 관련된 이벤트만 이벤트 로그에 저장됩니다.

  - **작업 실행 결과를 관리자에게 알림**

    관리자가 작업 실행 결과에 대한 알림을 받는 방법(이메일, SMS, 실행 파일 실행)을 선택할 수 있습니다. 알림을 구성하려면 **설정** 링크를 누릅니다.

    기본적으로는 모든 알림 방법이 비활성화됩니다.

- **오류만 알림**

  이 옵션을 활성화하면 작업 실행 완료 시 오류가 발생할 때만 관리자에게 알림이 전송됩니다.

  이 옵션을 비활성화하면 작업 실행이 완료될 때마다 관리자에게 알림이 전송됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- 보안 설정.
- 작업 범위 설정.

  작업 범위가 결정되는 방법에 따라 다음과 같은 설정이 제공됩니다:

  - **기기**

    관리 그룹에 따라 작업 범위가 결정되는 경우 이 그룹을 볼 수 있습니다. 이 그룹에서는 변경을 수행할 수 없습니다. 하지만 **작업 제외 그룹**를 설정할 수 있습니다.

    기기 목록에 따라 작업 범위가 결정되는 경우에는 기기를 추가하고 제거하여 이 목록을 수정할 수 있습니다.

  - **기기 조회**

    작업이 적용되는 기기 조회를 변경할 수 있습니다.

  - **작업 제외 그룹**

    작업이 적용되지 않는 기기 그룹을 지정할 수 있습니다. 작업이 적용되는 관리 그룹의 하위 그룹만 제외할 수 있습니다.

- **리비전 내역**.

작업 내보내기

Kaspersky Security Center를 사용하면 작업 및 해당 설정을 KLT 파일에 저장할 수 있습니다. 이 KLT 파일을 사용하여 저장된 작업을 Kaspersky Security Center Windows 및 Kaspersky Security Center Linux로 가져올 수 있습니다.

작업을 내보내려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기)** → **작업**로 이동합니다.
2. 내보내려는 작업 옆의 확인란을 선택합니다.

   동시에 여러 작업을 내보낼 수는 없습니다. 둘 이상의 작업을 선택하면 **내보내기** 버튼이 비활성화됩니다. 중앙 관리 서버 작업 또한 내보낼 수 없습니다.
3. **내보내기** 버튼을 클릭합니다.
4. **다른 이름으로 저장** 창이 열리면 작업 파일의 이름과 경로를 지정합니다. **저장** 버튼을 클릭합니다.

   다른 이름으로 저장 창은 Google Chrome, Microsoft Edge, Opera를 사용 시에만 표시됩니다. 다른 브라우저 사용 시, 작업 파일이 **다운로드** 폴더에 자동으로 저장됩니다.

작업 가져오기

Kaspersky Security Center를 사용하면 KLT 파일에서 작업을 가져올 수 있습니다. KLT 파일에는 내보낸 작업과 해당 설정이 포함되어 있습니다.

작업을 가져오려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **가져오기** 버튼을 클릭합니다.
3. **찾기** 버튼을 클릭하여 가져오려는 작업 파일을 선택합니다.
4. 열린 창에서 KLT 작업 파일의 경로를 지정한 후 **열기** 버튼을 클릭합니다. 작업 파일은 하나만 선택할 수 있습니다.

   작업 처리가 시작됩니다.
5. 작업이 성공적으로 처리된 후 작업을 할당할 기기를 선택합니다. 이렇게 하려면 다음 옵션 중 하나를 선택합니다:

   - **관리 그룹에 작업 할당**

     관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

     예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

     관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

     작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

     특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

   - **기기 선택 결과에 작업 할당**

     기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

     예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.
6. 작업 범위를 지정합니다.
7. **완료** 버튼을 클릭해 작업 가져오기를 완료합니다.

가져오기 결과가 포함된 알림이 표시됩니다. 작업을 성공적으로 가져왔다면 **자세히** 링크를 클릭하여 작업 속성을 볼 수 있습니다.

가져오기에 성공하면 작업이 작업 목록에 표시됩니다. 작업 설정 및 일정도 가져옵니다. 일정에 따라 작업이 시작됩니다.

새로 가져온 작업의 이름이 기존 작업과 같다면, 가져온 작업의 이름은 **(<다음 시퀀스 번호>)** 인덱스로 확장됩니다(예: **(1)**, **(2)**).

작업 암호 변경 마법사 시작

로컬이 아닌 작업의 경우 작업을 실행해야 하는 계정을 지정할 수 있습니다. 계정은 작업 생성 중 또는 기존 작업의 속성에서 지정할 수 있습니다. 지정된 계정이 조직의 보안 지침에 따라 사용되는 경우 이 지침에 따라 암호를 한 번씩 변경해야 할 수도 있습니다. 계정 암호가 만료되어 새 암호를 설정하면 작업 속성에서 유효한 새 암호를 지정해 주기 전까지 작업이 시작되지 않습니다.

작업 암호 변경 마법사를 이용하면 해당 계정이 지정되어 있는 모든 작업에서 이전 암호를 새 암호로 자동 교체할 수 있습니다. 아니면 각 작업의 속성에서 수동으로 암호를 교체해도 됩니다.

작업 암호 변경 마법사를 시작하려면:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **작업 시작을 위한 계정 자격 증명 관리**를 클릭합니다.

   마법사의 지침을 따릅니다.

1단계. 자격증명 지정

시스템(예: Active Directory)에서 현재 유효한 새 자격증명을 지정합니다. 마법사의 다음 단계로 넘어갈 때 Kaspersky Security Center가 지정된 계정 이름이 각 로컬이 아닌 작업의 속성에 있는 계정 이름과 일치하는지 확인합니다. 계정 이름이 일치하면 작업 속성의 암호가 새 암호로 자동 교체됩니다.

새 계정을 지정하려면 옵션을 선택합니다.

- **현재 계정 사용**

  마법사에서는 Kaspersky Security Center 웹 콘솔에 현재 로그인한 계정의 이름을 사용합니다. 그런 다음 **작업에 사용할 현재 암호** 필드에서 계정 암호를 수동으로 지정합니다.

- **다른 계정 지정**

  작업을 시작해야 하는 계정 이름을 지정합니다. 그런 다음 **작업에 사용할 현재 암호** 필드에서 계정 암호를 지정합니다.

이전 암호(선택 사항, 현재 암호로 바꾸려는 경우) 필드를 작성하면 Kaspersky Security Center가 계정 이름과 이전 암호가 모두 발견된 작업에 대해서만 암호를 교체합니다. 교체는 자동으로 수행됩니다. 기타 다른 경우에는 마법사의 다음 단계에서 수행할 작업을 선택해야 합니다.

2단계. 수행할 작업 선택

마법사의 첫 단계에서 이전 암호를 지정하지 않았거나 지정한 이전 암호가 작업 속성의 암호와 일치하지 않는 경우 검색된 작업에 대해 취할 행동을 선택해야 합니다.

작업에 대한 행동을 선택하려면 다음 단계를 따릅니다.

1. 행동을 선택할 작업 옆에 있는 확인란을 선택합니다.
2. 다음 중 하나를 선택합니다.
   - 작업 속성에서 암호를 제거하려면 **자격 증명 삭제**를 누릅니다.
     작업이 기본 계정으로 실행되도록 전환됩니다.
   - 암호를 새 암호로 바꾸려면 **이전 암호가 잘못되었거나 제공되지 않은 경우에도 암호 강제 변경**을 누릅니다.
   - 암호 변경을 취소하려면 **선택된 작업 없음**을 클릭합니다.

선택한 행동은 마법사의 다음 단계로 이동한 후에 적용됩니다.

3단계. 결과 확인

마법사의 마지막 단계에서 발견된 작업의 결과를 확인합니다. 마법사를 완료하려면 **마침** 버튼을 클릭합니다.

스크립트 원격 실행 작업 생성

스크립트 원격 실행 작업을 생성하여 클라이언트 기기에서 설치 패키지를 실행하고 애플리케이션을 원격으로 설치할 수 있습니다.

설치 패키지에는 클라이언트 기기에서 실행하기 위한 스크립트 세트와 manifest.json 파일이 포함된 ZIP 압축 파일이 포함되어 있습니다. 이 문서에서 이러한 유형의 설치 패키지를 생성하는 방법에 대해 자세히 알아보십시오.

이 작업은 Linux용 네트워크 에이전트가 설치된 기기에서만 시작해야 합니다.

스크립트 원격 실행 작업을 시작하려면:

1. **새 작업 마법사**로 이동하여 **스크립트 원격 실행** 작업 유형을 선택합니다.
2. 작업 이름을 입력하고 작업을 할당할 기기를 선택합니다. **다음** 버튼을 클릭합니다.
3. 원격 실행을 위해 manifest.json 파일이 포함된 ZIP 압축 파일 기반의 설치 패키지를 선택합니다.
   작업이 이미 완료된 기기에서 다시 실행하지 않으려면 **이미 이 작업을 완료한 기기에서는 시작하지 않음** 옵션을 켭니다.
4. 작업을 실행할 계정을 선택합니다.
   기본 계정을 선택하면 네트워크 에이전트(루트 계정)가 작업을 수행합니다.

스크립트 원격 실행 작업이 시작되면 이 작업에 할당된 계정을 변경할 수 없습니다. 작업이 할당된 계정을 변경하려면 작업 설정에서 작업을 중지하고 올바른 계정 세부 정보로 작업을 다시 생성하십시오.

5. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

6. **마침** 버튼을 클릭합니다.

   스크립트 원격 실행 작업이 생성되고 작업 목록에 표시됩니다.

스크립트 원격 실행 작업에서 데이터를 수신하면 네트워크 에이전트는 관리자와 작업 설정에서 지정된 사용자를 제외한 모든 사용자에 대해 수신된 데이터의 접근을 제한합니다.

스크립트 원격 실행 작업을 사용하여 기기에 애플리케이션 원격 설치

스크립트 원격 실행 작업을 사용하면 사용자 지정 설치 패키지를 생성하여 클라이언트 기기에 애플리케이션을 원격 설치할 수 있습니다.

이 문서에서 해당 작업을 위해 압축 파일을 준비하는 방법을 알아보십시오.

클라이언트 기기에 애플리케이션을 원격 설치하기 위한 설치 패키지를 생성하려면 해당 작업을 업로드할 압축 파일에 다음 파일이 포함되어 있어야 합니다.

- <패키지 이름>.deb
- **install.sh**

```
sudo apt-get install <패키지 이름>.deb
```

- **manifest.json**

애플리케이션 원격 설치를 위한 JSON 스키마

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<필요하면 인수를 입력합니다>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
```

```
}
```

배열 설명

1. version - 매니페스트 파일 및 작업의 버전입니다.
   현재 허용 가능한 값은 1입니다.

2. actions 배열의 요소에 따라 작업에서 실행되는 스크립트의 구성과 순서가 결정됩니다.
   스크립트의 실행 순서는 배열에서 요소의 색인(장소)에 해당합니다.

3. actions 배열의 각 요소에 대해 다음 요소가 정의됩니다.

   a. type - 스크립트에서 실행 가능한 명령의 유형입니다. 현재 이 값은 항상 `execute` 입니다.

   b. path - 압축 파일에 있는 스크립트 파일의 경로입니다.

   c. args - 실행 명령의 일부로 스크립트에 전달되는 인수입니다.

   d. results - 작업 결과에 따라 추가 동작을 정의하는 배열입니다.

      1. code - 스크립트를 반환하는 값입니다.

      2. next - 다음에 완료해야 하는 작업입니다. `continue` 동작은 다음 스크립트(actions 배열의 요소)를 실행하기 위해 진행합니다. `break` 동작은 작업을 중지합니다.

   e. default_next - 스크립트가 results에 포함되지 않은 값을 반환할 경우의 처리 방법입니다.

스크립트 원격 실행 작업이 시작되면 네트워크 에이전트는 애플리케이션과 설치 패키지를 클라이언트 기기에 업로드합니다. 클라이언트 기기가 설치 패키지를 수신하면 이 기기의 네트워크 에이전트가 manifest.json 파일을 분석하고 결과에 따라 스크립트 및 작업의 실행 순서를 정의한 후 실행을 시작합니다.

스크립트 원격 실행 작업이 완료되면 애플리케이션이 클라이언트 기기에 설치됩니다.

스크립트 원격 실행 작업에 대한 알림 및 모니터링 구성

스크립트 원격 실행 작업에 대한 모니터링, 이벤트 저장 동작 및 알림을 구성할 수 있습니다.

스크립트 원격 실행 상태를 보려면 다음과 같이 하십시오.

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
   작업 목록이 표시됩니다.

2. 작업을 선택하고 **기기 내역**을 클릭합니다.
   작업 진행률이 표시됩니다.

이벤트 저장 동작을 구성하려면:

1. 작업 목록에서 작업을 클릭하고 **설정** 탭으로 이동합니다.

2. **알림** 섹션에서 **설정** 버튼을 클릭합니다.

3. 작업 완료 후 애플리케이션이 작동하는 방식에 대해 다음 옵션 중 하나를 선택합니다.

   - **모든 이벤트 저장**.
   - **작업 진행 상태와 관련된 이벤트 저장**.
   - **작업 실행 결과만 저장**.
     이벤트는 **기기 내역** 및 **이벤트 저장소**에 저장됩니다.
     기본적으로 작업 실행 결과만 저장됩니다.

     > **모든 이벤트 저장**을 선택하면 작업 실행 결과만 저장됩니다.

4. 중앙 관리 서버 데이터베이스에 이벤트를 유지하거나 중앙 관리 서버 또는 기기의 이벤트 로그에 이벤트를 유지하려면 해당 옵션을 켭니다.

이 문서에서 알림 구성에 대해 자세히 알아보십시오.

스크립트 원격 실행 작업을 위한 압축 파일 준비

manifest.json 파일을 기반으로 *스크립트 원격 실행* 작업의 압축 파일은 다음 요구 사항을 충족해야 합니다.

- 압축 파일 형식: ZIP.
- 총 용량: 1GB 이하.
- 압축 파일에 있는 파일 및 폴더의 수에는 제한이 없습니다.
- 압축 파일의 매니페스트 파일은 아래의 스키마와 일치해야 하며 이름은 manifest.json이어야 합니다. 스키마는 기기에서 작업을 실행하는 동안에만 유효합니다.

  매니페스트 파일의 JSON 스키마 및 배열 설명

  JSON 스키마

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
```

```
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

매니페스트 파일의 예제

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
```

```
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- 압축 파일은 다음과 같이 구성되어야 합니다.

  `manifest.json`

  `<file1>`

  `<file2>`

  `<folder1>/<file3>`

  `<folder2>/<folder3>/<file4>`

  `...`

  `<fileX>`

  manifest.json은 작업에 대한 매니페스트 파일입니다.

  `<file1>, ...., <fileX>`는 실행할 스크립트가 있는 파일 집합입니다.

매니페스트 파일을 기반으로 설치 패키지 생성

매니페스트 파일을 기반으로 설치 패키지를 생성하려면:

1. 다음 중 하나를 수행합니다:

   - 메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동합니다.
   - 메인 메뉴에서 **동작 → 저장소 → 설치 패키지**로 이동합니다.

   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.

2. **추가**를 누릅니다.
   새 패키지 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

3. **manifest.jason 파일이 있는 ZIP 압축파일 기반의 스크립트 원격 실행 작업 설치 패키지를 생성합니다**을 선택합니다

4. 패키지 이름을 지정하고 **찾기** 버튼을 클릭합니다.
   브라우저에서 표준 Windows **열기** 창이 열리면 파일을 선택하여 설치 패키지를 만들 수 있습니다.

5. 사용 가능한 디스크에 있는 아카이브 파일을 선택합니다. 이 문서에서 해당 작업을 위해 압축 파일을 준비하는 방법을 알아보십시오.
   파일이 Kaspersky Security Center 중앙 관리 서버에 업로드됩니다.
   설치 패키지 생성 프로세스가 시작됩니다.
   프로세스가 완료되면 마법사가 알려줍니다.
   설치 패키지가 만들어지지 않으면 적절한 메시지가 표시됩니다.

6. **마침** 버튼을 눌러 마법사를 닫습니다.

   생성한 설치 패키지가 중앙 관리 서버 공유 폴더의 Packages 하위 폴더로 다운로드됩니다. 다운로드 후에 설치 패키지가 설치 패키지 목록에 나타납니다.

중앙 관리 서버에서 사용 가능한 설치 패키지 목록에서 사용자 지정 설치 패키지 이름이 있는 링크를 누르면 다음을 수행할 수 있습니다.

- 설치 패키지의 다음 속성을 봅니다:
  - **이름.** 사용자 지정 설치 패키지 이름.
  - **출처.** 애플리케이션 공급업체 이름.
  - **버전.** 애플리케이션 버전.
  - **만든 날짜.** 설치 패키지 생성 날짜.

- **수정됨.** 설치 패키지 수정 날짜.
- **경로.** 중앙 관리 서버에서 사용자 지정 설치 패키지의 경로.

- 패키지 이름과 명령줄 파라미터를 변경합니다. 이 기능은 Kaspersky 애플리케이션을 기반으로 만들지 않은 패키지에만 사용할 수 있습니다.

클라이언트 기기 관리

Kaspersky Security Center에서는 클라이언트 기기를 관리할 수 있습니다.

- 클러스터 및 서버 배열을 포함하여 관리 중인 기기의 설정과 상태를 확인합니다.
- 배포 지점을 구성합니다.
- 작업 관리.

관리 그룹에서 여러 클라이언트 기기를 한 세트로 결합하여 하나의 단위로 관리할 수 있습니다. 클라이언트 기기는 하나의 관리 그룹에만 포함할 수 있습니다. **규칙 조건**에 따라 기기를 그룹에 자동 할당할 수 있습니다.

- 기기 이동 규칙 생성.
- 기기 이동 규칙 복사.
- 기기 이동 규칙 조건.

기기 선택으로 조건에 따라 기기를 필터링할 수 있습니다. 기기에 태그를 지정하여 조회를 생성하고, 기기를 검색하고, 관리 그룹에서 기기를 배포할 수 있습니다.

관리 중인 기기 설정

관리 중인 기기 설정을 보려면:

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
   관리 중인 기기 목록이 표시됩니다.
2. 관리 중인 기기 목록에서 필수 기기의 이름이 포함된 링크를 누릅니다.

선택한 기기의 속성 창이 표시됩니다.

설정의 주요 그룹을 나타내는 속성 창의 상단 부분에 다음 탭이 표시됩니다.

- **일반**

  이 탭은 다음 섹션으로 구성됩니다:
  - **일반** 섹션에는 클라이언트 기기에 대한 일반 정보가 표시됩니다. 정보는 클라이언트 기기와 중앙 관리 서버의 마지막 동기화 중에 수신된 데이터를 기준으로 제공됩니다:
    - **이름**

이 필드에서는 관리 그룹에 있는 클라이언트 기기의 이름을 보고 수정할 수 있습니다.

- **설명**

  이 필드에서는 클라이언트 기기에 대한 추가 설명을 입력할 수 있습니다.

- **기기 상태**

  네트워크의 기기 활동과 기기의 안티 바이러스 보호 상태에 대해 관리자가 정의한 기준에 따라 할당된 클라이언트 기기의 상태입니다.

- **전체 그룹 이름**

  클라이언트 기기가 포함된 관리 그룹입니다.

- **마지막 안티 바이러스 데이터베이스 업데이트**

  기기에서 안티 바이러스 데이터베이스 또는 애플리케이션이 마지막으로 업데이트된 날짜입니다.

- **중앙 관리 서버에 연결**

  클라이언트 기기의 네트워크 에이전트가 중앙 관리 서버에 마지막으로 연결한 날짜와 시간입니다.

- **마지막 존재 확인**

  기기가 네트워크에 마지막으로 표시된 날짜와 시간입니다.

- **네트워크 에이전트 버전**

  설치된 네트워크 에이전트 버전.

- **만든 날짜**

  Kaspersky Security Center 내에서 기기 생성 날짜.

- **기기 소유자**

  기기 제조사 이름. **기기 소유자 관리** 링크를 클릭하여 사용자를 기기 소유자로 할당하거나 제거할 수 있습니다.

- **중앙 관리 서버와 계속 연결 유지**

이 옵션이 활성화되면 관리 중인 기기와 중앙 관리 서버 사이에 지속적인 연결 이 유지됩니다. 해당 연결을 제공하는 푸시 서버를 사용 하지 않는다면 이 옵션을 사용하면 됩니다.

이 옵션이 비활성화되어 있고 푸시 서버를 사용하지 않는 경우 관리 중인 기기가 데이터를 동기화하거나 정보를 전송하기 위해서만 중앙 관리 서버에 연결합니다.

중앙 관리 서버와 계속 연결 유지 확인란을 선택한 상태에서 사용 가능한 기기의 최대 총 개수는 300입니다.

이 옵션은 관리 중인 기기에서는 기본적으로 비활성화되어 있습니다. 이 옵션은 중앙 관리 서버가 설치된 기기에서 기본적으로 활성화되며 비활성화를 시도하더라도 활성화된 상태로 유지됩니다.

- **네트워크** 섹션에 클라이언트 기기의 네트워크 속성에 대한 다음 정보가 표시됩니다.
  - **IP 주소**

    기기 IP 주소.

  - **Windows 도메인**

    기기가 포함된 Windows 도메인 또는 작업 그룹입니다.

  - **DNS 이름**

    클라이언트 기기의 DNS 도메인 이름입니다.

  - **NetBIOS 이름**

    클라이언트 기기의 Windows 네트워크 이름입니다.

  - **IPv6 주소**
- **시스템** 섹션은 클라이언트 기기에 설치된 운영 체제에 대한 정보를 제공합니다:
  - **운영 체제**
  - **CPU 아키텍처**
  - **기기 이름**
  - **가상 컴퓨터 유형**

    가상 머신 제조업체.

  - **VDI의 일부인 동적 가상 머신**

    이 행은 클라이언트 기기가 VDI의 일부인 동적 가상 머신인지 표시합니다.

- **보호** 섹션에서는 클라이언트 기기의 현재 안티 바이러스 보호 상태에 대한 다음 정보가 제공됩니다.
  - **표시 여부**

    클라이언트 기기의 가시성 상태.

  - **기기 상태**

    네트워크의 기기 활동과 기기의 안티 바이러스 보호 상태에 대해 관리자가 정의한 기준에 따라 할당된 클라이언트 기기의 상태입니다.

  - **상태 설명**

    클라이언트 기기 보호 및 중앙 관리 서버 연결 상태.

  - **보호 상태**

    이 필드에서는 클라이언트 기기의 현재 실시간 보호 상태를 보여 줍니다.

    기기에서 상태가 변경되면 클라이언트 기기를 중앙 관리 서버와 동기화해야 기기 속성 창에 새 상태가 표시됩니다.

  - **마지막 전체 검사**

    클라이언트 기기에서 마지막으로 악성 코드 검사를 수행한 날짜와 시간.

  - **바이러스 탐지**

    보안 애플리케이션 설치 이후(첫 번째 검사) 또는 위협 카운터를 마지막으로 초기화한 이후 클라이언트 기기에서 탐지된 전체 위협 수입니다.

  - **치료하지 못한 개체**

    클라이언트 기기에서 처리 안 된 파일의 개수입니다.

    모바일 기기의 처리 안 된 파일 수는 이 필드에서 무시됩니다.

  - **디스크 암호화 상태**

    기기 로컬 드라이브의 현재 파일 암호화 상태입니다. 상태에 대한 설명은 Kaspersky Endpoint Security for Windows 도움말을 참조하십시오.

- **애플리케이션에서 정의된 기기 상태** 섹션은 기기에 설치된 관리 중인 애플리케이션에서 정의한 기기 상태에 대한 정보를 제공합니다. 이 기기 상태는 Kaspersky Security Center의 정의와 다를 수 있습니다.

- **애플리케이션**

  이 탭에는 클라이언트 기기에 설치된 모든 Kaspersky 애플리케이션이 표시됩니다. 이 탭의 **시작** 및 **중지** 버튼으로, 선택한 Kaspersky 애플리케이션(네트워크 에이전트 제외)을 시작 및 중지할 수 있습니다. 이 버튼은 관리 중인 기기에서 중앙 관리 서버의 수신 푸시 알림에 포트 15000 UDP 를 사용할 수 있을 때 사용할 수 있습니다. 관리 중인 기기를 푸시 알림에 사용할 수 없지만 중앙 관리 서버에 대한 연속 연결 모드가 활성화되어 있다면(**일반** 섹션에서 **중앙 관리 서버와 계속 연결 유지** 옵션 활성화), **시작** 및 **중지** 버튼을 사용할 수 있습니다. 그렇지 않으면, 애플리케이션을 시작하거나 중지하려고 할 때 오류 메시지가 표시됩니다. 애플리케이션 이름을 눌러 애플리케이션에 대한 일반적인 정보, 기기에서 발생한 이벤트의 목록, 애플리케이션 설정을 확인할 수 있습니다.

- **활성 정책 및 정책 프로필**

  이 탭에는 관리 중인 기기에서 현재 배정된 정책 및 정책 프로필이 나열됩니다.

- **작업**

  작업 섹션에서는 기존 작업 목록 보기, 새 작업 만들기, 작업 제거, 작업 시작 및 중지, 작업 설정 수정, 실행 결과 보기 등의 클라이언트 기기 작업을 관리할 수 있습니다. 클라이언트를 중앙 관리 서버와 마지막으로 동기화할 때 받은 데이터를 기반으로 작업 목록이 제공됩니다. 중앙 관리 서버는 클라이언트 기기에서 작업 상태 세부 정보를 요청합니다. 중앙 관리 서버의 푸시 알림 수신을 위해 관리 중인 기기에서 포트 15000 UDP를 사용할 수 있다면, 작업 상태가 표시되고 작업 관리 버튼을 사용할 수 있습니다. 푸시 서버가 관리 중인 기기에 연결할 수 없지만 중앙 관리 서버에 대한 연속 연결 모드가 활성화되면(**일반** 섹션에서 **중앙 관리 서버와 계속 연결 유지** 옵션 활성화), 작업이 있는 동작도 사용할 수 있습니다.

  연결할 수 없다면 상태가 표시되지 않으며 버튼도 비활성화됩니다.

- **이벤트**

  이벤트 섹션에는 선택된 클라이언트 기기의 중앙 관리 서버에 기록된 이벤트가 표시됩니다.

  기기 이벤트를 내보내기, 복사, 삭제할 수 있습니다.

- **보안 문제**

  보안 문제 탭에서는 클라이언트 기기에 대한 보안 문제를 보고, 편집, 생성할 수 있습니다. 보안 문제는 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션을 통해 관리자가 자동 또는 수동으로 생성할 수 있습니다. 예를 들어 어떤 사용자가 정기적으로 사용자의 이동식 드라이브에서 기기로 악성 프로그램을 옮기면 관리자는 보안 문제를 만들 수 있습니다. 관리자는 보안 문제 텍스트에 해당 케이스의 요약 설명과 권장하는 작업(사용자에 대해 취할 징계 조치 등)을 제공할 수 있으며 사용자 한 명 이상에 대한 링크를 추가할 수 있습니다.

  필요한 작업을 모두 수행한 보안 문제는 *처리됨*으로 분류됩니다. 기기 상태를 *심각* 또는 *경고*로 변경하기 위한 조건으로 처리 안 된 보안 문제 유무를 선택할 수 있습니다.

  이 섹션에는 기기에 대해 생성된 보안 문제의 목록이 포함되어 있습니다. 보안 문제는 심각도 레벨 및 유형을 기준으로 분류됩니다. 보안 문제 유형은 보안 문제를 생성하는 Kaspersky 애플리케이션이 정의합니다. **처리됨** 열에서 확인란을 선택하여 목록에서 처리된 보안 문제를 강조할 수 있습니다.

- **태그**

  태그 섹션에서는 클라이언트 기기 검색을 위한 키워드 목록을 관리합니다: 기존 태그 목록 보기, 목록에서 태그 할당하기, 자동 태그 규칙 구성하기, 새 태그 추가하기, 오래된 태그 이름 변경하기, 태그 제거.

- **고급**

  이 탭은 다음 섹션으로 구성됩니다:

  - **자산 관리(소프트웨어)**. 이 섹션에서는 클라이언트 기기에 설치된 애플리케이션의 레지스트리와 해당 업데이트를 볼 수 있으며, 자산 관리(소프트웨어)의 표시 방식도 설정할 수 있습니다.

    클라이언트 기기에 설치된 네트워크 에이전트가 중앙 관리 서버에 필요한 정보를 전송하는 경우 설치된 애플리케이션에 대한 정보가 제공됩니다. 네트워크 에이전트 또는 해당 정책의 속성 창에 있는 **저장소** 섹션에서 중앙 관리 서버로의 정보 전송을 구성할 수 있습니다.

    애플리케이션 이름을 누르면 애플리케이션 세부 정보와 애플리케이션에 대해 설치된 업데이트 패키지 목록이 포함된 창이 열립니다.

  - **실행 파일**. 이 섹션에는 클라이언트 기기에서 발견된 실행 파일이 표시됩니다.

  - **배포 지점**. 이 섹션에서는 기기가 상호 작용하는 배포 지점의 목록을 제공합니다.

    - **파일로 내보내기**

      기기가 상호 작용하는 배포 지점의 목록을 파일에 저장하려면 **파일로 내보내기** 버튼을 누릅니다. 애플리케이션은 기본적으로 기기 목록을 CSV 파일로 내보냅니다.

    - **속성**

      기기가 상호 작용하는 배포 지점을 보고 구성하려면 **속성** 버튼을 누릅니다.

  - **자산 관리(하드웨어)**. 이 섹션에서는 클라이언트 기기에 설치된 하드웨어에 대한 정보를 확인할 수 있습니다.

    Windows를 실행하는 기기에 네트워크 에이전트를 설치했다면 기기 하드웨어에 대한 다음 정보를 중앙 관리 서버로 전송합니다.

    - RAM
    - 대용량 스토리지 기기
    - 마더보드
    - CPU
    - 네트워크 어댑터
    - 모니터
    - 비디오 어댑터
    - 사운드 카드

    Linux 또는 macOS 실행하는 장치에 네트워크 에이전트를 설치했다면, 운영 체제에서 해당 정보를 제공하는 경우 장치 하드웨어에 대한 다음 정보를 중앙 관리 서버로 전송합니다.

    - 총 RAM 크기
    - 대용량 저장 기기의 총 크기

- 마더보드
- CPU
- 네트워크 어댑터

- **사용 가능한 업데이트**. 이 섹션에는 이 기기에 있지만 아직 설치되지 않은 소프트웨어 업데이트의 목록이 표시됩니다.

- **소프트웨어 취약점**. 이 섹션에는 클라이언트 기기에 설치된 타사 애플리케이션의 취약점에 대한 정보가 들어 있습니다.

  파일에 취약점을 저장하려면 저장할 취약점 옆에 있는 확인란을 선택하고 **CSV로 내보내기** 버튼 또는 **TXT로 내보내기** 버튼을 누릅니다.

  이 섹션에는 다음 설정이 포함되어 있습니다:

  - **수정할 수 있는 취약점만 표시**

    이 옵션을 사용하면 패치를 사용하여 수정할 수 있는 취약점이 섹션에 표시됩니다.

    이 옵션이 비활성화되어 있으면 패치가 릴리즈되지 않은 취약점과 패치를 사용하여 수정할 수 있는 취약점이 모두 섹션에 표시됩니다.

    기본적으로 이 옵션은 켜져 있습니다.

  - **취약점 속성**

    선택한 소프트웨어 취약점의 속성을 별도의 창에서 보려면 목록에서 소프트웨어 취약점을 누릅니다. 이 창에서 다음을 수행할 수 있습니다:

    - 이 관리 중인 기기에서 소프트웨어 취약점을 무시합니다(관리 콘솔에서 또는 Kaspersky Security Center 웹 콘솔에서).
    - 취약점에 대한 권장 수정 사항 목록을 봅니다.
    - 취약점 수정을 위한 소프트웨어 업데이트를 수동으로 지정합니다(관리 콘솔에서 또는 Kaspersky Security Center 웹 콘솔에서).
    - 취약점 인스턴스를 봅니다.
    - 취약점을 수정하기 위해 기존 작업의 목록을 보고 취약점을 수정하기 위한 새 작업을 만듭니다.

- **원격 진단**. 이 섹션에서는 클라이언트 기기의 원격 진단을 수행할 수 있습니다.

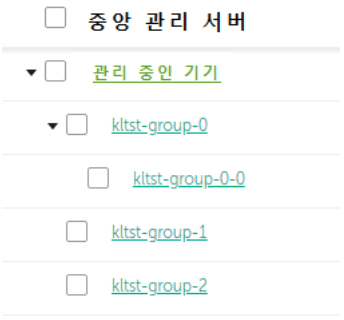
PostgreSQL, MariaDB, MySQL DBMS를 사용한다면 **이벤트** 탭의 선택한 클라이언트 기기에 대한 이벤트 목록이 완전하지 않을 수 있습니다. 이 문제는 DBMS에 저장된 이벤트가 매우 많을 때 발생합니다. 다음 작업 중 하나로 표시할 이벤트 수를 늘릴 수 있습니다:

- 불필요한 이벤트 제거.
- 불필요한 이벤트의 저장 기간 단축.

기기의 중앙 관리 서버에 기록된 이벤트의 전체 목록을 보려면 리포트를 사용하십시오.

관리 그룹 생성

Kaspersky Security Center 설치 직후 관리 그룹의 계층 구조에는 **관리 중인 기기**라는 관리 그룹 하나만 포함됩니다. 관리 그룹의 계층 구조를 만들 때 **관리 중인 기기** 그룹에 가상 컴퓨터 등의 기기를 추가하고 중첩된 그룹도 함께 추가할 수 있습니다(아래 그림 참조).



관리 그룹 계층 구조 보기

관리 그룹을 만들려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기)** → **그룹 계층 구조**로 이동합니다.
2. 관리 그룹 구조에서 새 관리 그룹을 포함할 관리 그룹을 선택합니다.
3. **추가** 버튼을 클릭합니다.
4. **새 관리 그룹의 이름** 창이 열리면 그룹 이름을 입력하고 **추가** 버튼을 클릭합니다.

   지정한 이름의 새 관리 그룹 폴더가 관리 그룹의 계층 구조에 나타납니다.

애플리케이션은 Active Directory 구조 또는 도메인 네트워크의 구조에 기초하여 관리 그룹의 계층을 만들 수 있습니다. 또한, 텍스트 파일에서 그룹 구조를 만들 수 있습니다.

관리 그룹의 구조를 만들려면 아래와 같이 진행합니다:

1. 메인 메뉴에서 **에셋(기기)** → **그룹 계층 구조**로 이동합니다.
2. **가져오기** 버튼을 누릅니다.

   새 관리 그룹 구조 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

관리 그룹에 수동으로 기기 추가

기기 이동 규칙을 만들어서 자동으로 또는 한 관리 그룹에서 다른 관리 그룹으로 기기를 이동해서 수동으로, 아니면 선택한 관리 그룹에 기기를 추가해서 기기를 관리 그룹으로 이동할 수 있습니다. 이 섹션에서는 관리 그룹에 기기를 수동으로 추가하는 방법에 대해 설명합니다.

선택한 관리 그룹에 한 대 이상의 기기를 포함시키려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
2. 목록 위에서 **현재 경로:** `<current path>` 링크를 누릅니다.
3. 창이 열리면 기기에 추가하려는 관리 그룹을 선택합니다.
4. **기기 추가** 버튼을 클릭합니다.
   기기 이동 마법사가 시작됩니다.
5. 관리 그룹에 추가할 기기 목록을 만듭니다.

   > 기기에 연결할 때 또는 기기 발견 이후에 중앙 관리 서버 데이터베이스에 이미 정보가 추가된 기기만 목록에 추가할 수 있습니다.

   다음 중 목록에 기기를 추가할 방법을 선택합니다.

   - **기기 추가** 버튼을 누르고 다음 방법 중 하나로 기기를 지정합니다.
     - 중앙 관리 서버에서 감지한 기기 목록에서 기기를 선택합니다.
     - 기기 IP 주소 또는 IP 범위를 지정합니다.

       > IP 범위에는 1,048,576개의 주소만 포함될 수 있습니다.

     - 기기의 NetBIOS 이름 또는 DNS 이름을 지정합니다.

       > 기기 이름 필드에는 공백, 백스페이스 문자, 또는 , \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %와 같이 금지되는 문자가 포함되어서는 안 됩니다.

   - **파일에서 기기 가져오기** 버튼을 눌러 .txt 파일에서 기기 목록을 가져옵니다. 각 기기 주소 또는 이름은 별도의 줄에 지정해야 합니다.

     > 파일에는 공백, 백스페이스 문자, 또는 , \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %와 같이 금지되는 문자가 포함되어서는 안 됩니다.

6. 관리 그룹에 추가할 기기 목록을 봅니다. 기기를 추가하거나 제거하여 목록을 편집할 수 있습니다.
7. 목록이 올바른지 확인한 후 **다음** 버튼을 클릭합니다.

   마법사가 기기 목록을 처리하고 결과를 표시합니다. 성공적으로 처리된 기기는 관리 그룹에 추가되고 기기 목록의 중앙 관리 서버에서 생성한 이름 아래에 표시됩니다.

관리 그룹에 수동으로 기기 또는 클러스터 이동

한 관리 그룹에서 다른 관리 그룹으로 또는 미할당 기기 그룹에서 관리 그룹으로 기기를 이동할 수 있습니다.

한 관리 그룹에서 다른 관리 그룹으로 클러스터 또는 서버 배열을 이동할 수도 있습니다. 클러스터와 해당 노드가 항상 같은 관리 그룹에 속하므로, 클러스터 또는 서버 배열을 다른 그룹으로 이동하면 노드도 전부 함께 이동됩니다. **기기** 탭에서 단일 클러스터 노드를 선택하면 **소속 그룹 변경** 버튼을 사용할 수 없게 됩니다.

선택한 관리 그룹으로 두 대 이상의 기기 또는 클러스터를 이동하려면 다음 단계를 따릅니다.

1. 기기를 이동할 관리 그룹을 엽니다. 이렇게 하려면 다음 중 하나를 수행하십시오.

   - 관리 그룹을 열려면 기본 메뉴에서 **에셋(기기) → 관리 중인 기기** 로 이동하고 **현재 경로** 필드에서 경로 링크를 클릭한 다음 열리는 왼쪽 창에서 관리 그룹을 선택합니다.

   - **미할당 기기** 그룹을 열려면 메인 메뉴에서 **발견 및 배포 → 미할당 기기**로 이동합니다.

2. 관리 그룹이 클러스터 또는 서버 어레이를 포함하면 **관리 중인 기기** 섹션이 **기기** 탭과 **클러스터 및 서버 배열** 탭으로 나뉩니다. 이동하려는 개체의 탭을 엽니다.

3. 다른 그룹으로 이동하려는 기기 또는 클러스터 옆에 있는 확인란을 선택합니다.

4. **소속 그룹 변경** 버튼을 클릭합니다.

5. 관리 그룹의 계층 구조에서 선택한 기기 또는 클러스터를 이동할 관리 그룹 옆의 확인란을 선택합니다.

6. **이동** 버튼을 누릅니다.

   선택한 기기 또는 클러스터가 선택한 관리 그룹으로 이동됩니다.

기기 이동 규칙 생성

관리 그룹에 기기를 자동 할당하는 기기 이동 규칙을 설정할 수 있습니다.

이동 규칙을 생성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 이동 규칙** 탭으로 이동합니다.

2. **추가**를 누릅니다.

3. 창이 열리면 **일반** 탭에서 다음 정보를 지정합니다.

   - **규칙 이름**

     새 규칙의 이름을 입력합니다.

     규칙을 복사하는 경우 새 규칙에는 소스 규칙과 같은 이름이 지정되지만 () 형식의 색인이 이름에 추가됩니다. 예: (1).

   - **관리 그룹**

     기기를 자동으로 이동할 관리 그룹을 선택합니다.

   - **활성 규칙**

     이 옵션을 활성화하면 규칙이 저장한 후에 활성화되어 작동하기 시작합니다.

이 옵션을 비활성화하면 규칙이 생성은 되지만 활성화되지는 않습니다. 이 옵션을 활성화할 때까지는 규칙이 작동하지 않습니다.

- **관리 그룹에 속하지 않는 기기만 이동**

  이 옵션을 활성화하면 미할당 기기만 선택한 그룹으로 이동됩니다.

  이 옵션을 비활성화하면 다른 관리 그룹에 이미 속해 있는 기기와 미할당 기기가 모두 선택한 그룹으로 이동됩니다.

- **규칙 적용**

  다음 옵션 중 하나를 선택할 수 있습니다:

  - **기기별로 한 번 실행**

    기준과 일치하는 각 기기에 대해 규칙이 한 번 적용됩니다.

  - **기기별로 한 번 실행한 후 네트워크 에이전트를 재설치할 때마다 실행**

    기준과 일치하는 각 기기에 대해 네트워크 에이전트를 해당 기기에 다시 설치할 때만 규칙이 한 번 적용됩니다.

  - **지속적으로 규칙 적용**

    중앙 관리 서버가 자동으로 설정되는 스케줄에 따라 규칙이 적용됩니다(대개 몇 시간마다).

4. **규칙 조건** 탭에서 기기를 관리 그룹으로 이동하는 기준을 하나 이상 지정합니다.

5. **저장**을 클릭합니다.

이동 규칙이 생성됩니다. 생성된 규칙은 이동 규칙 목록에 표시됩니다.

목록에서의 위치가 높을수록 규칙의 우선순위가 높아집니다. 이동 규칙의 우선순위를 높이거나 낮추려면 마우스를 사용하여 목록에서 각 규칙을 위 또는 아래로 이동합니다.

지속적으로 규칙 적용 옵션을 선택하면 우선 순위 설정에 상관없이 이동 규칙이 적용됩니다. 이러한 규칙은 중앙 관리 서버에서 자동 설정하는 스케줄에 따라 적용됩니다.

기기 특성이 여러 규칙의 조건을 충족하는 경우에는 우선 순위가 가장 높은 규칙(규칙 목록에서 순위가 가장 높은 규칙)의 대상 그룹으로 기기가 이동됩니다.

기기 이동 규칙 복사

예를 들어, 서로 다른 대상 관리 그룹에 동일한 여러 규칙을 적용하려는 경우 이동 규칙을 복사할 수 있습니다.

기존 이동 규칙을 복사하려면 다음 단계를 따릅니다.

1. 다음 중 하나를 수행합니다:

   - 메인 메뉴에서 **에셋(기기)** → **이동 규칙** 탭으로 이동합니다.
   - 메인 메뉴에서 **발견 및 배포** → **배포 및 할당** → **이동 규칙**으로 이동합니다.

   이동 규칙 목록이 표시됩니다.

2. 복사할 규칙 옆의 확인란을 선택합니다.
3. **복사**를 클릭합니다.
4. 창이 열리면 **일반** 탭에서 다음 정보를 변경하거나, 설정을 변경하지 않고 규칙을 복사만 하려는 경우 변경을 수행하지 않습니다.

   - **규칙 이름**

     새 규칙의 이름을 입력합니다.

     규칙을 복사하는 경우 새 규칙에는 소스 규칙과 같은 이름이 지정되지만 () 형식의 색인이 이름에 추가됩니다. 예: (1).

   - **관리 그룹**

     기기를 자동으로 이동할 관리 그룹을 선택합니다.

   - **활성 규칙**

     이 옵션을 활성화하면 규칙이 저장한 후에 활성화되어 작동하기 시작합니다.

     이 옵션을 비활성화하면 규칙이 생성은 되지만 활성화되지는 않습니다. 이 옵션을 활성화할 때까지는 규칙이 작동하지 않습니다.

   - **관리 그룹에 속하지 않는 기기만 이동**

     이 옵션을 활성화하면 미할당 기기만 선택한 그룹으로 이동됩니다.

     이 옵션을 비활성화하면 다른 관리 그룹에 이미 속해 있는 기기와 미할당 기기가 모두 선택한 그룹으로 이동됩니다.

   - **규칙 적용**

     다음 옵션 중 하나를 선택할 수 있습니다:

     - **기기별로 한 번 실행**

       기준과 일치하는 각 기기에 대해 규칙이 한 번 적용됩니다.

     - **기기별로 한 번 실행한 후 네트워크 에이전트를 재설치할 때마다 실행**

       기준과 일치하는 각 기기에 대해 네트워크 에이전트를 해당 기기에 다시 설치할 때만 규칙이 한 번 적용됩니다.

- **지속적으로 규칙 적용**
  중앙 관리 서버가 자동으로 설정되는 스케줄에 따라 규칙이 적용됩니다(대개 몇 시간마다).

5. **규칙 조건** 탭에서 자동 이동할 기기에 관한 기준을 하나 이상 지정합니다.
6. **저장**를 누릅니다.

새 이동 규칙이 생성됩니다. 생성된 규칙은 이동 규칙 목록에 표시됩니다.

기기 이동 규칙 조건

클라이언트 기기를 관리 그룹으로 이동하는 규칙을 생성하거나 복사할 때 **규칙 조건** 탭에서 기기 이동 조건을 설정합니다. 이동할 기기 결정 시 다음 기준을 사용할 수 있습니다.

- 클라이언트 기기에 할당된 태그.
- 네트워크 매개변수. 예를 들어, 지정된 범위에 IP 주소가 해당하는 기기를 이동할 수 있습니다.
- 네트워크 에이전트 또는 중앙 관리 서버와 같은 클라이언트 기기에 설치된 관리 애플리케이션.
- 클라이언트 기기인 가상 컴퓨터.
- 클라이언트 기기가 있는 Active Directory 조직 구성 단위(OU)에 대한 정보입니다.
- 클라이언트 기기가 있는 클라우드 세그먼트에 대한 정보입니다.

아래에서 기기 이동 규칙에서 이 정보를 지정하는 방법에 관한 설명을 확인할 수 있습니다.

규칙에 여러 조건을 지정하면 AND 논리 연산자가 동작하여 모든 조건이 동시 적용됩니다. 옵션을 선택하지 않거나 일부 필드를 비워두면 해당 조건이 적용되지 않습니다.

태그 탭

이 탭에서는 이전에 클라이언트 기기 설명에 추가한 기기 태그를 기준으로 기기 이동 규칙을 구성할 수 있습니다. 이렇게 하려면 필요한 태그를 선택합니다. 또한 다음 옵션을 활성화할 수 있습니다.

- **지정한 태그가 없는 기기에 적용**

  이 옵션을 활성화하면 지정된 태그가 있는 모든 기기가 기기 이동 규칙에서 제외됩니다. 이 옵션을 비활성화하면 선택한 모든 태그가 있는 기기에 기기 이동 규칙이 적용됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **하나 이상의 지정 태그가 일치하면 적용**

  이 옵션을 활성화하면 선택된 태그 중 하나 이상이 있는 클라이언트 기기에 기기 이동 규칙이 적용됩니다. 이 옵션을 비활성화하면 선택한 모든 태그가 있는 기기에 기기 이동 규칙이 적용됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

네트워크 탭

이 탭에서 기기 이동 규칙이 고려하는 기기의 네트워크 데이터를 지정할 수 있습니다.

- **Windows 네트워크상의 기기 이름**

  장치의 Windows 네트워크 이름(NetBIOS 이름) 또는 IPv4 또는 IPv6 주소.

- **Windows 도메인**

  기기 이동 규칙은 지정된 Windows 도메인에 포함된 모든 기기에 적용됩니다.

- **기기의 DNS 이름**

  이동하려는 클라이언트 기기의 DNS 도메인 이름입니다. 네트워크가 DNS 서버를 포함한다면 이 필드를 입력합니다.

  Kaspersky Security Center에 사용하는 데이터베이스에 대해 대소문자 구분 데이터 정렬이 설정되었다면, 기기 DNS 이름을 지정할 때 대소문자를 구분합니다. 그렇지 않으면 장치 이동 규칙이 작동하지 않습니다.

- **DNS 도메인**

  기기 이동 규칙은 지정된 기본 DNS 접미사에 포함된 모든 기기에 적용됩니다. 네트워크가 DNS 서버를 포함한다면 이 필드를 입력합니다.

- **IP 범위**

  이 옵션을 사용하면 관련 기기가 포함되어야 하는 IP 범위의 첫 IP 주소와 마지막 IP 주소를 입력할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **중앙 관리 서버에 연결할 IP 주소**

  이 옵션을 활성화하면 클라이언트 기기가 중앙 관리 서버에 연결되는 IP 주소를 설정할 수 있습니다. 이렇게 하려면 필요한 IP 주소를 모두 포함하도록 IP 범위를 지정합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **IP 범위에 있는 기기**

  이 옵션을 활성화하면 **IP 범위** 섹션에서 이전에 추가한 IP 범위를 선택할 수 있습니다. 선택한 IP 범위에 해당 기기가 포함되어야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **연결 프로필이 변경됨**

  다음 값 중 하나를 선택합니다:
  - **예**. 연결 프로필이 변경된 클라이언트 기기에만 기기 이동 규칙이 적용됩니다.
  - **아니요**. 기기 이동 규칙은 연결 프로필이 변경되지 않은 클라이언트 기기에만 적용됩니다.
  - **어떤 값도 선택되지 않았습니다**. 조건이 적용되지 않습니다.

- **다른 중앙 관리 서버에서 관리**

  다음 값 중 하나를 선택합니다:
  - **예**. 다른 중앙 관리 서버에서 관리하는 클라이언트 기기에만 기기 이동 규칙이 적용됩니다. 이 서버는 기기 이동 규칙을 구성하는 서버와 다릅니다.
  - **아니요**. 현재 중앙 관리 서버에서 관리하는 클라이언트 기기에만 기기 이동 규칙이 적용됩니다.
  - **어떤 값도 선택되지 않았습니다**. 조건이 적용되지 않습니다.

애플리케이션 탭

이 탭에서는 클라이언트 기기에 설치된 관리 중인 애플리케이션 및 운영 체제를 기반으로 기기 이동 규칙을 구성할 수 있습니다.

- **네트워크 에이전트가 설치됨**

  다음 값 중 하나를 선택합니다:
  - **예**. 네트워크 에이전트가 설치된 클라이언트 기기에만 기기 이동 규칙이 적용됩니다.
  - **아니요**. 네트워크 에이전트가 설치되지 않은 클라이언트 기기에만 기기 이동 규칙이 적용됩니다.
  - **어떤 값도 선택되지 않았습니다**. 조건이 적용되지 않습니다.

- **애플리케이션**

  클라이언트 기기에 기기 이동 규칙을 적용하기 위해 기기에 어떤 관리 중인 애플리케이션을 설치할지 지정합니다. 예를 들어, **Kaspersky Security Center 15.1 네트워크 에이전트** 또는 **Kaspersky Security Center 15.1 중앙 관리 서버**를 선택할 수 있습니다.

  관리 중인 애플리케이션을 선택하지 않으면 조건이 적용되지 않습니다.

- **운영 체제 버전**

  운영 체제 버전에 따라 클라이언트 기기를 선택할 수 있습니다. 이를 위해 클라이언트 기기에 설치해야 하는 운영 체제를 지정합니다. 이에 따라, 선택한 운영 체제를 사용하는 클라이언트 기기에 기기 이동 규칙이 적용됩니다.

  이 옵션을 활성화하지 않으면 조건이 적용되지 않습니다. 이 옵션은 기본으로 비활성화되어 있습니다.

- **운영 체제 비트 크기**

  운영 체제 비트 크기에 따라 클라이언트 기기를 선택할 수 있습니다. **운영 체제 비트 크기** 필드에서 다음 값 중 하나를 선택할 수 있습니다.

  - **알 수 없음**
  - **x86**
  - **AMD64**
  - **IA64**

  클라이언트 기기의 운영 체제 비트 크기를 확인하려면:

  1. 메인 메뉴에서 **에셋(기기)** → **관리 중인 기기**로 이동합니다.
  2. 오른쪽의 **열 설정** 버튼( )을 클릭합니다.
  3. **운영 체제 비트 크기** 옵션을 선택한 후 **저장** 버튼을 클릭합니다.
     그 후에는 관리 중인 모든 기기에 대해 운영 체제 비트 크기가 표시됩니다.

- **운영 체제 서비스 팩 버전**

  이 필드에서는 사용자 운영 체제의 패키지 버전을 *X.Y* 형식으로 지정할 수 있습니다. 지정한 버전에 따라 이동 규칙이 장치에 적용되는 방법이 결정됩니다. 기본적으로 버전 값은 지정되지 않습니다.

- **사용자 인증서**

  다음 값 중 하나를 선택합니다:

  - **설치됨**. 모바일 인증서가 있는 모바일 기기에만 기기 이동 규칙이 적용됩니다.
  - **설치 안 됨** 모바일 인증서가 없는 모바일 기기에만 기기 이동 규칙이 적용됩니다.
  - **어떤 값도 선택되지 않았습니다**. 조건이 적용되지 않습니다.

- **운영 체제 빌드**

  이 설정은 Windows 운영 체제에만 적용됩니다.

  선택한 운영 체제의 빌드 번호가 이 번호와 같아야 하는지 아니면 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 빌드 번호를 제외한 모든 빌드 번호에 대해 기기 이동 규칙을 구성할 수도 있습니다.

- **운영 체제 릴리스 번호**

  이 설정은 Windows 운영 체제에만 적용됩니다.

선택한 운영 체제의 릴리즈 번호가 이 번호와 같거나 이전/이후의 번호여야 하는지 지정할 수 있습니다. 지정된 번호를 제외한 모든 릴리즈 번호에 대해 기기 이동 규칙을 구성할 수도 있습니다.

가상 컴퓨터 탭

이 탭에서는 클라이언트 기기가 가상 컴퓨터인지 VDI(가상 데스크톱 인프라)에 속하는지에 따라 기기 이동 규칙을 구성할 수 있습니다.

- **이것은 가상 컴퓨터입니다**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **N/A**. 조건이 적용되지 않습니다.
  - **아니요**. 가상 컴퓨터가 아닌 기기를 이동합니다.
  - **예**. 가상 컴퓨터인 기기를 이동합니다.

- **가상 컴퓨터 유형**

- **가상 데스크톱 인프라 소속**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **N/A**. 조건이 적용되지 않습니다.
  - **아니요**. VDI에 속하지 않는 기기를 이동합니다.
  - **예**. VDI에 속하는 기기를 이동합니다.

도메인 컨트롤러 탭

이 탭에서 도메인 조직 구성단위에 포함된 기기를 이동해야 한다는 것을 지정할 수 있습니다. 지정된 도메인 조직 구성단위의 모든 하위 조직 구성단위에서 기기를 이동할 수도 있습니다.

- **기기가 다음 조직 구성 단위에 포함되어 있습니다**

  이 옵션을 사용하면 기기 이동 규칙이 옵션 아래 목록에 지정된 도메인 조직 구성단위의 기기에 적용됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **하위 조직 구성 단위까지 포함**

  이 옵션을 선택하면 지정한 도메인 조직 구성 단위의 모든 하위 조직 구성 단위에 있는 기기가 선택에 포함됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **자식 구성 단위에서 해당하는 하위 그룹으로 기기 이동**

- **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성**
- **도메인에 존재하지 않는 하위 그룹 삭제**
- **기기가 다음 도메인 보안 그룹에 포함되어 있습니다**

  이 옵션을 사용하면 기기 이동 규칙이 옵션 아래 목록에 지정된 도메인 보안 그룹의 기기에 적용됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

클라우드 세그먼트 탭

이 탭에서 특정 클라우드 세그먼트에 속하는 기기를 이동해야 한다는 것을 지정할 수 있습니다:

- **기기가 클라우드 세그먼트에 있습니다**

  이 옵션을 선택하면 클라우드 세그먼트에 속한 클라이언트 기기에 기기 이동 규칙이 적용됩니다. 옵션 아래 목록에서 서브넷까지 필요한 클라우드 세그먼트를 선택할 수 있습니다.
  이 옵션은 기본으로 비활성화되어 있습니다.

- **자식 개체 포함**

  이 옵션을 선택하면 선택한 클라우드 세그먼트뿐만 아니라 이 세그먼트의 하위 개체에도 기기 이동 규칙이 적용됩니다.
  이 옵션은 기본으로 비활성화되어 있습니다.

- **중첩된 개체에서 해당하는 하위 그룹으로 기기 이동**
- **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성**
- **클라우드 세그먼트에 일치하는 항목이 없는 하위 그룹 삭제**
- **API를 사용해 발견된 기기**

  드롭다운 목록에서 API 도구로 장치를 탐지할지 선택할 수 있습니다:
  - **AWS**. AWS API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 AWS 클라우드 환경에 있습니다.
  - **Azure**. Azure API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Azure 클라우드 환경에 있습니다.
  - **Google Cloud.** Google API를 사용하여 기기를 발견했으므로, 해당 기기는 명확히 Google Cloud 환경에 있습니다.
  - **아니요**. AWS, Azure, Google API로 기기를 찾을 수 없으므로, 기기가 클라우드 환경 밖에 있거나 클라우드 환경 내에 있지만 어떠한 이유로 인해 API를 사용해 찾을 수 없습니다.
  - **값 없음**. 이 조건이 적용되지 않습니다.

클러스터 및 서버 배열 정보

Kaspersky Security Center는 클러스트 기술을 지원합니다. 네트워크 에이전트에서 클라이언트 기기에 설치된 애플리케이션이 서버 배열의 일부를 구성하는 한다는 정보를 중앙 관리 서버에 보내면 해당 기기가 클러스터 노드가 됩니다.

관리 그룹이 클러스터 또는 서버 배열을 포함하면 **관리 중인 기기** 페이지에는 개별 기기 탭과 클러스터 및 서버 배열 탭이 표시됩니다. 관리 기기가 클러스터 노드로 감지되면 클러스터가 **클러스터 및 서버 배열** 탭에 개별 개체로 추가됩니다.

클러스터 또는 서버 배열 노드는 다른 관리 중인 기기와 함께 **기기** 탭에 나열됩니다. 노드의 속성을 개별 기기로 보고 다른 작업을 수행할 수 있지만 클러스터 노드를 삭제하거나 클러스터와 별도로 다른 관리 그룹으로 이동할 수는 없습니다. 클러스터는 전체 단위로만 삭제하거나 이동할 수 있습니다.

클러스터 또는 서버 배열로 다음 작업을 수행할 수 있습니다.

- 속성 보기
- 클러스터 또는 서버 배열을 다른 관리 그룹으로 이동

  클러스터와 해당 노드가 항상 같은 관리 그룹에 속하므로, 클러스터 또는 서버 배열을 다른 그룹으로 이동하면 노드도 전부 함께 이동됩니다.

- 삭제

  클러스터 또는 서버 배열이 조직 네트워크에 더는 존재하지 않을 때만 클러스터 또는 서버 배열을 삭제하는 것이 좋습니다. 클러스터가 여전히 네트워크에 표시되고 네트워크 에이전트와 Kaspersky 보안 애플리케이션이 여전히 클러스터 노드에 설치되어 있다면 Kaspersky Security Center는 삭제된 클러스터와 해당 노드를 자동으로 관리 중인 기기 목록에 다시 반환합니다.

클러스터 또는 서버 배열 속성

클러스터 또는 서버 배열의 설정을 보려면:

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기 → 클러스터 및 서버 배열**로 이동합니다.

   클러스터 및 서버 배열 목록이 표시됩니다.

2. 필요한 클러스터 또는 서버 배열의 이름을 클릭합니다.

선택한 클러스터 또는 서버 배열의 속성 창이 표시됩니다.

일반

일반 섹션에는 클러스터 또는 서버 배열에 대한 일반 정보가 표시됩니다. 정보는 클러스터 노드와 중앙 관리 서버의 마지막 동기화 중에 수신된 데이터를 기준으로 제공됩니다.

- **이름**
- **설명**

- **Windows 도메인**

  클러스터 또는 서버 배열을 포함하는 Windows 도메인 또는 작업 그룹.

- **NetBIOS 이름**

  클러스터 또는 서버 배열의 Windows 네트워크 이름입니다.

- **DNS 이름**

  클러스터 또는 서버 배열의 DNS 도메인 이름입니다.

작업

작업 탭에서는 기존 작업 목록 보기, 새 작업 만들기, 작업 제거, 작업 시작 및 중지, 작업 설정 수정, 실행 결과 보기 등 클러스터 또는 서버 배열에 할당된 작업을 관리할 수 있습니다. 나열된 작업은 클러스터 노드에 설치된 Kaspersky 보안 애플리케이션과 관련이 있습니다. Kaspersky Security Center는 클러스터 노드에서 작업 목록 및 작업 상태 세부 정보를 수신합니다. 연결할 수 없다면 상태가 표시되지 않습니다.

노드

이 탭은 클러스터 또는 서버 배열에 포함된 노드 목록을 표시합니다. 노드 이름을 클릭하여 기기 속성 창을 볼 수 있습니다.

Kaspersky 애플리케이션

속성 창에는 클러스터 노드에 설치된 Kaspersky 보안 애플리케이션과 관련된 정보 및 설정이 있는 추가 탭이 포함될 수도 있습니다.

기기가 비활성 상태로 표시될 때 작업 보기 및 구성

그룹 내의 클라이언트 기기가 비활성 상태인 경우 해당 상태에 대한 알림을 받을 수 있습니다. 이러한 기기를 자동으로 삭제할 수도 있습니다.

그룹의 기기가 비활성 상태로 표시될 때 작업을 보거나 구성하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 그룹 계층 구조**로 이동합니다.
2. 필요한 관리 그룹의 이름을 누릅니다.
   관리 그룹 속성 창이 열립니다.
3. 속성 창에서 **설정** 탭으로 이동합니다.

4. **상속** 섹션에서 다음 옵션을 활성화하거나 비활성화합니다.

- **부모 그룹에서 상속**

  이 섹션의 설정이 클라이언트 기기가 포함된 부모 그룹에서 상속됩니다. 이 옵션을 활성화하면 **네트워크에서의 기기 활동**의 설정이 변경되지 않도록 잠깁니다.

  이 옵션은 관리 그룹에 부모 그룹이 있는 경우에만 사용할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **자식 그룹에서 설정 상속 강제 실행**

  이 설정 값은 자식 그룹에 배포되지만 자식 그룹의 속성에서는 이러한 설정이 잠깁니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

5. **기기 활동** 섹션에서 다음 옵션을 활성화하거나 비활성화합니다.

- **기기가 다음 비활성 기간을 초과하면 관리자에게 알림(일)**

  이 옵션을 활성화하면 관리자에게 비활성 기기 관련 알림이 수신됩니다. **너무 오랫동안 기기가 네트워크에 접속하지 않았습니다** 이벤트가 만들어질 때까지의 기간을 지정할 수 있습니다. 기본 기간은 7일입니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **기기가 다음 비활성 기간을 초과하면 그룹에서 기기 제거(일)**

  이 옵션을 활성화하면 기기가 그룹에서 자동으로 제거될 때까지의 시간 간격을 지정할 수 있습니다. 기본 기간은 60일입니다.

  기본적으로 이 옵션은 켜져 있습니다.

6. **저장**을 누릅니다.

변경 내용이 저장 및 적용됩니다.

기기 상태 정보

Kaspersky Security Center는 관리 중인 기기마다 상태를 할당합니다. 특정 상태는 사용자가 정의한 조건이 충족되는지 여부에 따라 달라집니다. 기기에 상태를 할당할 때 Kaspersky Security Center에서 네트워크에 있는 기기의 가시성 플래그를 고려하는 경우가 있습니다(아래 표 참조). 예를 들어, *데이터베이스가 오래됨* 조건이 충족되어서 관리 중인 기기에 *심각* 상태가 할당되었고 나중에 기기의 가시성 플래그가 설정되었다면 기기에는 *확인* 상태가 할당됩니다. Kaspersky Security Center에서 2시간 내에 네트워크의 기기를 찾지 못하면 기기의 가시성 플래그가 *확인되지 않음*으로 설정됩니다.

상태는 다음과 같습니다.

- *심각* 또는 *심각/존재 확인*
- *경고* 또는 *경고/존재 확인*
- *확인* 또는 *확인/존재 확인*

아래 표에는 기기에 *심각* 또는 *경고* 상태를 할당하기 위해 충족해야 하는 기본 조건과 가능한 모든 값이 나와 있습니다.

기기에 상태를 할당하기 위한 조건

조건	조건 설명	사용 가능한 값
보안 제품이 설치 안 됨	기기에 네트워크 에이전트는 설치되어 있는데 보안 제품은 설치되어 있지 않습니다.	• 토글 버튼이 켜져 있습니다. • 토글 버튼이 꺼져 있습니다.
바이러스가 너무 많이 탐지됨	*악성 코드 검사* 작업 등의 바이러스 탐지 작업을 통해 기기에서 일부 바이러스가 발견되었으며, 발견된 바이러스 수가 지정된 값을 초과합니다.	0개 이상
실시간 보호 레벨이 관리자가 설정한 레벨과 다름	기기가 네트워크에 연결되었지만 실시간 보호 레벨이 조건에서 기기 상태에 대해 관리자가 설정한 레벨과 다릅니다.	• 중지됨 • 일시 중지됨 • 실행 중
오랫동안 악성 코드를 검사하지 않음	기기가 네트워크에 표시되며 보안 제품이 기기에 설치되어 있지만, *악성 코드 검사* 작업과 로컬 검사 작업이 지정된 시간 간격보다 오랫동안 실행되지 않았습니다. 이 조건은 중앙 관리 서버 데이터베이스에 추가된 지 7일 이상이 지난 기기에만 해당됩니다.	1일 이상
데이터베이스가 오래됨	기기가 네트워크에 표시되며 보안 제품이 기기에 설치되어 있지만 지정된 시간 간격보다 오랫동안 이 기기에서 안티 바이러스 데이터베이스가 업데이트되지 않았습니다. 이 조건은 중앙 관리 서버 데이터베이스에 추가된 지 1일 이상이 지난 기기에만 해당됩니다.	1일 이상
오랫동안 중앙 관리 서버에 연결 안 됨	네트워크 에이전트가 기기에 설치되었지만 기기가 꺼져 있어 지정된 시간 간격보다 오랫동안 중앙 관리 서버에 연결되지 않았습니다.	1일 이상
처리 안 된 위협이 탐지됨	**처리 안 된 위협** 폴더의 처리되지 않은 개체 수가 지정된 값을 초과합니다.	항목 0개 이상
재시작 필요	기기가 네트워크에 표시되지만 선택한 이유 중 하나로 인해 애플리케이션이 지정된 시간 간격보다 오랫동안 기기 다시 시작을 요구합니다.	0분 이상
비호환 애플리케이션이 설치되어 있음	기기가 네트워크에 표시되지만 네트워크 에이전트를 통해 수행된 소프트웨어 인벤토리에서 기기에 호환되지 않는 애플리케이션이 설치되어 있음을 탐지했습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
소프트웨어 취약점이 탐지됨	기기가 네트워크에 표시되며 네트워크 에이전트가 기기에 설치되어 있지만 *취약점 및 필요한 업데이트 검색* 작업을 통해 기기에 설치된 애플리케이션에서 지정된 심각도의 취약점이 탐지되었습니다.	• 심각 • 높음 • 중간 • 취약점을 수정할 수 없으면 무시 • 설치용 업데이트가 할당되어 있으면 무시
라이센스 만료됨	기기가 네트워크에 표시되지만 라이센스가 만료되었습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
라이센스가 곧 만료됨	기기가 네트워크에 표시되지만 기기에서 지정한 기간(일) 이내에 라이센스가 만료됩니다.	0대 이하

조건	조건 설명	사용 가능한 값
오랫동안 Windows 업데이트 패치를 검색하지 않음	기기가 네트워크에 표시되지만 *Windows 업데이트 동기화 수행* 작업이 지정된 시간 간격보다 오랫동안 실행되지 않았습니다.	1일 이상
유효하지 않은 암호화 상태	기기에 네트워크 에이전트가 설치되어 있는데 기기 암호화 결과가 지정된 값과 같습니다.	• 사용자의 거부로 인해 정책을 준수하지 않습니다(외부 기기에만 해당됨). • 오류로 인해 정책을 준수하지 않습니다. • 정책 적용 시 기기를 다시 시작해야 합니다. • 암호화 정책을 지정하지 않았습니다. • 지원되지 않습니다. • 정책 적용 시.
모바일 기기 설정이 정책과 일치하지 않음	모바일 기기 설정이 규정 준수 규칙 확인 중에 Kaspersky Endpoint Security for Android 정책에서 지정한 설정과 다릅니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
처리되지 않은 보안 문제가 있음	기기에서 처리되지 않은 일부 보안 문제가 발견되었습니다. 보안 문제는 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션을 통해 자동 또는 수동으로 관리자에 의해 생성될 수 있습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
애플리케이션에서 정의된 기기 상태	관리 애플리케이션이 기기 상태를 정의합니다. 관리 중인 기기는 Kaspersky Security Center 설정과 상관없이 관리 중인 애플리케이션에서 정의한 상태를 가질 수 있습니다. 이후 해당 상태가 Kaspersky Security Center에서 정의한 상태 중 하나를 반환하면, 중앙 관리 서버는 관리 중인 애플리케이션에서 반환한 상태와 중앙 관리 서버에서 할당한 상태 중 가장 심각한 상태를 관리 중인 기기에 할당합니다. 관리 중인 애플리케이션에서 정의한 상태에는 관리 중인 애플리케이션에서 전송한 설명이 있습니다. 관리 중인 기기 목록 , **상태 설명** 열에서 설명을 확인할 수 있습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
기기 디스크 공간 부족	기기의 사용 가능한 디스크 공간이 지정된 값보다 작거나 기기를 중앙 관리 서버와 동기화할 수 없습니다. 기기가 중앙 관리 서버와 성공적으로 동기화되고 기기의 사용 가능한 여유 공간이 지정된 값보다 크거나 같으면 *심각* 또는 *경고* 상태가 *정상* 상태로 변경됩니다.	0MB 이상.
기기와의 연결이 끊어짐	기기를 발견하는 동안 기기가 네트워크에 연결된 것으로 인식되었지만 중앙 관리 서버와의 동기화 시도가 3회 이상 실패했습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
보호가 비활성화됨	기기가 네트워크에 연결되었지만 기기의 보안 제품이 지정된 시간 간격보다 오랫동안 작동 중지된 상태로 유지되었습니다. 이때 보안 애플리케이션의 상태는 *정지* 또는 *실패*로 표시되며, 이는 *시작 중*, *실행 중*, *일시 중지*와는 다릅니다.	0분 이상
보안 제품이 실행 중이지 않음	기기가 네트워크에 표시되며 기기에 보안 제품이 설치는 되어 있지만 실행되고 있지는 않습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.

Kaspersky Security Center에서는 지정한 조건이 충족되면 관리 그룹의 기기 상태를 자동으로 전환하도록 설정할 수 있습니다. 지정한 조건이 충족되면 클라이언트 기기에는 *심각* 또는 *경고* 상태 중 하나가 할당됩니다. 지정한 조건이 충족되지 않으면 클라이언트 기기에 *확인* 상태가 할당됩니다.

서로 다른 상태는 한 조건의 서로 다른 값을 나타낼 수 있습니다. 예를 들어 기본적으로 **데이터베이스가 오래됨** 조건 값이 **3일 이상**이면 클라이언트 기기에 *경고* 상태가 할당되고 값이 **7일 이상이면** *심각* 상태가 할당됩니다.

Kaspersky Security Center를 이전 버전에서 업그레이드하면 *심각* 또는 *경고*로 상태를 할당하기 위한 **데이터베이스가 오래됨** 조건의 값이 변경되지 않습니다.

기기 상태 전환 구성

조건을 변경하여 *심각* 또는 *경고* 상태를 기기에 할당할 수 있습니다.

기기 상태가 심각으로 변경되도록 설정하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 그룹 계층 구조**로 이동합니다.
2. 그룹 목록이 열리면 기기 상태 전환을 변경할 그룹 이름이 있는 링크를 누릅니다.
3. 속성 창이 열리면 **기기 상태** 탭을 선택합니다.
4. 왼쪽 창에서 **심각**을 선택합니다.
5. 오른쪽 창의 **지정되었다면 심각으로 설정** 섹션에서 기기 전환 조건을 *심각* 상태로 활성화합니다.

   > 부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

6. 목록에서 조건 옆에 있는 라디오 버튼을 선택합니다.
7. 목록의 왼쪽 상단에서 **편집** 버튼을 누릅니다.
8. 선택한 조건에 필요한 값을 설정합니다.
   모든 조건에 대해 값을 설정할 수 있는 것은 아닙니다.
9. **확인**를 누릅니다.

   지정한 조건이 충족되면 관리 중인 기기에 *심각* 상태가 할당됩니다.

기기 상태가 경고로 변경되도록 설정하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 그룹 계층 구조**로 이동합니다.
2. 그룹 목록이 열리면 기기 상태 전환을 변경할 그룹 이름이 있는 링크를 누릅니다.
3. 속성 창이 열리면 **기기 상태** 탭을 선택합니다.
4. 왼쪽 창에서 **경고**를 선택합니다.
5. 오른쪽 창의 **지정되었다면 경고로 설정** 섹션에서 기기 전환 조건을 *경고* 상태로 활성화합니다.

   > 부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

6. 목록에서 조건 옆에 있는 라디오 버튼을 선택합니다.
7. 목록의 왼쪽 상단에서 **편집** 버튼을 누릅니다.

8. 선택한 조건에 필요한 값을 설정합니다.

   모든 조건에 대해 값을 설정할 수 있는 것은 아닙니다.

9. **확인**를 누릅니다.

지정한 조건이 충족되면 관리 중인 기기에 *경고* 상태가 할당됩니다.

클라이언트 기기 데스크톱에 원격 연결

관리자는 클라이언트 기기에 설치된 네트워크 에이전트를 통해 기기 데스크톱에 원격으로 접근할 수 있습니다. 클라이언트 기기의 TCP 및 UDP 포트가 폐쇄된 경우에도 네트워크 에이전트를 통해 기기에 원격으로 연결할 수 있습니다.

기기와 연결을 설정하면 관리자는 해당 컴퓨터에 저장된 정보에 대한 완전한 접근 권한을 얻어 컴퓨터에 설치된 애플리케이션을 관리할 수 있습니다.

관리 중인 대상 기기의 운영 체제 설정에서 원격 연결이 허용되어야 합니다. 예를 들어 Windows 10에서는 이 옵션을 **이 컴퓨터에 대한 원격 지원 연결 허용**이라고 합니다(이 옵션은 **제어판 → 시스템 및 보안 → 시스템 → 원격 설정**에서 찾을 수 있음). 취약점 및 패치 관리 기능에 대한 라이센스가 있다면 관리 중인 기기에 대한 연결을 설정할 때 이 옵션을 강제로 활성화할 수 있습니다. 라이센스가 없는 경우 관리 중인 대상 기기에서 로컬로 이 옵션을 활성화합니다. 이 옵션을 비활성화하면 원격으로 연결할 수 없습니다.

기기에 대한 원격 연결을 설정하려면 두 가지 유틸리티가 필요합니다.

- klsctunnel이라는 Kaspersky 유틸리티. 이 유틸리티는 관리자 워크스테이션에 저장되어야 합니다. 이 유틸리티를 사용하여 클라이언트 기기와 중앙 관리 서버 간의 연결을 터널링합니다.

  Kaspersky Security Center에서는 중앙 관리 서버를 통해 관리 콘솔에서, 그리고 네트워크 에이전트를 통해 관리 중인 기기의 지정된 포트로 TCP 연결을 터널링할 수 있습니다. 터널링은 관리 콘솔과 대상 기기를 직접 연결할 수 없는 경우 기기의 클라이언트 애플리케이션을 관리 중인 기기의 TCP 포트에 설치된 관리 콘솔과 연결하는 데 사용됩니다.

  원격 클라이언트 기기에 중앙 관리 서버와의 연결에 사용하는 포트가 제공되지 않을 경우 클라이언트 기기와 중앙 관리 서버 간 연결 터널링이 필요합니다. 다음과 같은 경우 기기의 포트를 사용하지 못할 수 있습니다:

  - 원격 기기가 NAT 메커니즘을 사용하는 네트워크에 연결되어 있습니다.
  - 원격 기기는 중앙 관리 서버와 같은 로컬 네트워크에 속하지만 해당 포트가 방화벽에 의해 닫혀 있습니다.

- 원격 데스크톱 연결이라는 표준 Microsoft Windows 구성 요소. 원격 데스크톱에 대한 연결은 표준 Windows 유틸리티 mstsc.exe를 통해 해당 유틸리티에 대해 정의된 설정에 따라 이루어집니다.

  사용자의 현재 원격 데스크톱 세션으로의 연결은 사용자의 인지없이 연결되었습니다. 일단 관리자가 세션에 연결하면, 기기 사용자는 추가 알림 없이 세션에서 연결이 끊깁니다.

클라이언트 기기 데스크톱에 연결하려면:

1. MMC 기반 관리 콘솔에서 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창이 열리면 **중앙 관리 서버 연결 설정 → 연결 포트**로 이동합니다.
3. **Kaspersky Security Center 웹 콘솔용 RDP 포트 열기** 옵션이 활성화되어 있는지 확인합니다.
4. Kaspersky Security Center 웹 콘솔에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.

5. 관리 중인 기기 목록 위의 **현재 경로** 필드에서 경로 링크를 클릭합니다.

6. 열리는 왼쪽 창에서 액세스하려는 기기가 포함된 관리 그룹을 선택합니다.

7. 접근 권한을 얻으려는 기기의 이름 옆에 있는 확인란을 선택합니다.

8. **원격 데스크톱에 연결** 버튼을 누릅니다.
   원격 데스크톱(Windows 전용) 창이 열립니다.

9. **관리 중인 기기에서 원격 데스크톱 연결 허용** 옵션을 활성화합니다. 이 경우 관리 중인 기기의 운영 체제 설정에서 현재 원격 연결이 금지되어 있어도 연결이 설정됩니다.

   이 옵션은 취약점 및 패치 관리 기능에 대한 라이센스가 있을 때만 사용할 수 있습니다.

10. **다운로드** 버튼을 눌러 klsctunnel 유틸리티를 다운로드합니다.

11. **클립보드로 복사** 버튼을 눌러 텍스트 필드에서 텍스트를 복사합니다. 이 텍스트는 중앙 관리 서버와 관리 중인 기기 간의 연결을 설정하는 데 필요한 설정을 포함하는 BLOB(Binary Large Object)입니다.

    BLOB는 3분 동안 유효합니다. 만료된 경우 원격 데스크톱(Windows 전용) 창을 다시 열어 새 BLOB를 생성합니다.

12. klsctunnel 유틸리티를 실행합니다.
    유틸리티 창이 열립니다.

13. 복사한 텍스트를 텍스트 필드에 붙여 넣습니다.

14. 프록시 서버를 사용하는 경우 **프록시 서버 사용** 확인란을 선택한 다음 프록시 서버 연결 설정을 지정합니다.

15. **포트 열기** 버튼을 누릅니다.
    원격 데스크톱 연결 로그인 창이 열립니다.

16. 현재 Kaspersky Security Center 웹 콘솔에서 로그인한 계정의 자격 증명을 지정합니다.

17. **연결** 버튼을 누릅니다.

기기에 연결된 후에는 Microsoft Windows의 원격 연결 창에서 해당 데스크톱을 사용할 수 있습니다.

Windows 데스크톱 공유를 통해 기기에 연결

관리자는 클라이언트 기기에 설치된 네트워크 에이전트를 통해 기기 데스크톱에 원격으로 접근할 수 있습니다. 클라이언트 기기의 TCP 및 UDP 포트가 폐쇄된 경우에도 네트워크 에이전트를 통해 기기에 원격으로 연결할 수 있습니다.

관리자는 세션을 운영 중인 사용자의 연결을 끊지 않고도 클라이언트 기기의 현재 세션에 연결할 수 있습니다. 이 경우 관리자와 기기의 세션 사용자가 데스크톱에 대한 접근을 공유하게 됩니다.

기기에 대한 원격 연결을 설정하려면 두 가지 유틸리티가 필요합니다.

- klsctunnel이라는 Kaspersky 유틸리티. 이 유틸리티는 관리자 워크스테이션에 저장되어야 합니다. 이 유틸리티를 사용하여 클라이언트 기기와 중앙 관리 서버 간의 연결을 터널링합니다.

  Kaspersky Security Center에서는 중앙 관리 서버를 통해 관리 콘솔에서, 그리고 네트워크 에이전트를 통해 관리 중인 기기의 지정된 포트로 TCP 연결을 터널링할 수 있습니다. 터널링은 관리 콘솔과 대상 기기를 직접 연결할 수 없는 경우 기기의 클라이언트 애플리케이션을 관리 중인 기기의 TCP 포트에 설치된 관리 콘솔과 연결하는 데 사용됩니다.

  원격 클라이언트 기기에 중앙 관리 서버와의 연결에 사용하는 포트가 제공되지 않을 경우 클라이언트 기기와 중앙 관리 서버 간 연결 터널링이 필요합니다. 다음과 같은 경우 기기의 포트를 사용하지 못할 수 있습니다:

  - 원격 기기가 NAT 메커니즘을 사용하는 네트워크에 연결되어 있습니다.
  - 원격 기기는 중앙 관리 서버와 같은 로컬 네트워크에 속하지만 해당 포트가 방화벽에 의해 닫혀 있습니다.

- Windows 데스크톱 공유. 현재 활성화된 원격 데스크톱 세션에 연결하는 경우 해당 기기의 세션 사용자가 관리자로부터 연결 요청을 받게 됩니다. 기기의 원격 활동과 활동 결과는 Kaspersky Security Center에 의해 생성된 리포트에 저장되지 않습니다.

  관리자가 원격 클라이언트 기기에서의 사용자 활동을 감사하도록 구성할 수 있습니다. 감사 중에 애플리케이션은 클라이언트 기기에서 관리자가 열거나 수정한 파일에 대한 정보를 저장합니다.

Windows 데스크톱 공유를 통해 클라이언트 기기의 데스크톱에 연결하려면 다음 조건이 충족되어야 합니다.

- 관리자 워크스테이션에 Microsoft Windows Vista 이상 버전이 설치되어 있어야 합니다. 중앙 관리 서버를 운영하는 기기의 운영 체제 유형이 Windows 데스크톱 공유를 사용한 연결을 제한하지 않아야 합니다.

  사용자의 Windows 에디션이 Windows 데스크톱 공유 기능을 포함하는지 확인하려면 Windows 레지스트리에 CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} 키가 있는지 확인하십시오.

- 클라이언트 기기에 Microsoft Windows Vista 이상 버전이 설치되어 있어야 합니다.

- Kaspersky Security Center는 취약점 및 패치 관리용 라이센스를 사용합니다.

Windows 데스크톱 공유 기술을 통해 클라이언트 기기의 데스크톱으로 연결하려면 다음과 같이 하십시오:

1. MMC 기반 관리 콘솔에서 중앙 관리 서버의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창이 열리면 **중앙 관리 서버 연결 설정 → 연결 포트**로 이동합니다.
3. **Kaspersky Security Center 웹 콘솔용 RDP 포트 열기** 옵션이 활성화되어 있는지 확인합니다.
4. Kaspersky Security Center 웹 콘솔에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
5. 관리 중인 기기 목록 위의 **현재 경로** 필드에서 경로 링크를 클릭합니다.
6. 열리는 왼쪽 창에서 액세스하려는 기기가 포함된 관리 그룹을 선택합니다.
7. 접근 권한을 얻으려는 기기의 이름 옆에 있는 확인란을 선택합니다.
8. **Windows Desktop Sharing** 버튼을 누릅니다.

   Windows Desktop Sharing 마법사가 열립니다.
9. **다운로드** 버튼을 눌러 klsctunnel 유틸리티를 다운로드하고 다운로드 프로세스가 완료될 때까지 기다립니다.

   klsctunnel 유틸리티가 이미 있는 경우 이 단계를 건너 뜁니다.

10. **다음** 버튼을 누릅니다.

11. 연결하려는 기기에서 세션을 선택한 다음 **다음** 버튼을 누릅니다.

12. 대상 기기에서 대화 상자가 열리면 사용자는 데스크톱 공유 세션을 허용해야 합니다. 그렇지 않으면 세션이 불가능합니다.

    기기 사용자가 데스크톱 공유 세션을 확인하면 마법사의 다음 페이지가 열립니다.

13. **클립보드로 복사** 버튼을 눌러 텍스트 필드에서 텍스트를 복사합니다. 이 텍스트는 중앙 관리 서버와 관리 중인 기기 간의 연결을 설정하는 데 필요한 설정을 포함하는 BLOB(Binary Large Object)입니다.

    BLOB는 3분 동안 유효합니다. 만료된 경우 새 BLOB를 생성합니다.

14. klsctunnel 유틸리티를 실행합니다.

    유틸리티 창이 열립니다.

15. 복사한 텍스트를 텍스트 필드에 붙여 넣습니다.

16. 프록시 서버를 사용하는 경우 **프록시 서버 사용** 확인란을 선택한 다음 프록시 서버 연결 설정을 지정합니다.

17. **포트 열기** 버튼을 누릅니다.

    새 창에서 데스크톱 공유가 시작됩니다. 기기와 상호 작용하려면 창의 왼쪽 상단에서 메뉴 아이콘( )을 누른 다음 **대화식 모드**를 선택합니다.

기기 조회

*기기 조회*는 특정 조건에 따라 기기를 필터링하는 도구입니다. 기기 조회를 사용하면 여러 기기를 관리할 수 있습니다. 예를 들어 해당 기기와 관련된 리포트만 확인하거나 모든 기기를 다른 그룹으로 이동할 수 있습니다.

Kaspersky Security Center에서는 폭넓은 *사전 정의 조회*(**심각 상태의 기기**, **보호가 비활성화됨**, **처리 안 된 위협이 탐지됨** 등)를 제공합니다. 미리 정의된 조회는 삭제할 수 없습니다. 추가 *사용자 정의 조회*를 만들고 구성할 수도 있습니다.

사용자 정의 조회에서는 검색 범위를 설정하고 모든 기기, 관리 중인 기기 또는 미할당 기기를 선택할 수 있습니다. 검색 파라미터는 조건에서 지정됩니다. 기기 선택에서는 검색 파라미터가 서로 다른 여러 조건을 생성할 수 있습니다. 예를 들어 두 조건을 생성하여 각각 다른 IP 범위를 지정할 수 있습니다. 여러 조건을 지정하면 조회에는 조건 중 하나라도 충족하는 기기가 표시됩니다. 반면 한 조건 내의 검색 파라미터는 겹쳐서 적용됩니다. 한 조건에서 IP 범위와 설치된 애플리케이션 이름을 모두 지정하는 경우 애플리케이션이 설치되어 있고 IP 주소가 지정된 범위에 속하는 기기만 표시됩니다.

기기 조회에서 기기 목록 보기

Kaspersky Security Center를 사용하면 기기 조회에서 기기 목록을 볼 수 있습니다.

기기 조회에서 기기 목록을 보려면:

1. 메인 메뉴에서 **에셋(기기) → 기기 선택** 또는 **발견 및 배포 → 기기 선택** 섹션으로 이동합니다.
2. 조회 목록에서 기기 조회 이름을 누릅니다.
   이 페이지에는 기기 조회에 포함된 기기에 대한 정보가 있는 테이블이 표시됩니다.
3. 기기 테이블의 데이터를 다음과 같이 그룹화하고 필터링할 수 있습니다.
   - 설정 아이콘( )을 클릭하고, 테이블에 표시할 열을 선택합니다.
   - 필터 아이콘( )을 클릭하고, 호출된 메뉴에서 필터 기준을 지정하고 적용합니다.
     필터링된 기기 테이블이 표시됩니다.

기기 선택에서 하나 또는 여러 기기를 선택하고 **새 작업** 버튼을 클릭하여 이러한 기기에 적용될 작업을 생성할 수 있습니다.

기기 선택에서 선택한 기기를 다른 관리 그룹으로 이동하려면 **소속 그룹 변경** 버튼을 클릭한 후 대상 관리 그룹을 선택합니다.

기기 조회 만들기

기기 조회를 만들려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 기기 선택**로 이동합니다.
   기기 조회 목록이 포함된 페이지가 표시됩니다.
2. **추가** 버튼을 누릅니다.
   기기 선택 설정 창이 열립니다.
3. 새 조회 이름을 입력합니다.
4. 기기 선택에 포함할 기기가 포함된 그룹을 지정합니다.
   - **모든 기기 검색**: 선택 기준을 충족하고 **관리 중인 기기** 또는 **미할당 기기** 그룹에 포함된 기기를 검색합니다.
   - **관리 중인 기기 검색**: 선택 기준을 충족하고 **관리 중인 기기** 그룹에 포함된 기기를 검색합니다.
   - **미할당 기기 검색**: 선택 기준을 충족하고 **미할당 기기** 그룹에 포함된 기기를 검색합니다.

   보조 중앙 관리 서버의 데이터 포함 확인란을 활성화하여 선택 기준을 충족하고 보조 중앙 관리 서버에서 관리하는 기기 검색을 활성화할 수 있습니다.
5. **추가** 버튼을 누릅니다.
6. 열리는 창에서 이 조회에 기기를 포함하기 위해 충족해야 할 조건을 지정한 다음 **확인** 버튼을 누릅니다.
7. **저장** 버튼을 누릅니다.

기기 조회가 생성되어 기기 조회 목록에 추가됩니다.

기기 조회 구성

기기 조회를 구성하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기)** → **기기 선택**로 이동합니다.
   기기 조회 목록이 포함된 페이지가 표시됩니다.
2. 관련 사용자 지정 기기 선택을 선택하고 **속성** 버튼을 클릭합니다.
   기기 선택 설정 창이 열립니다.
3. **일반** 탭에서 **새 조건** 링크를 클릭합니다.
4. 이 조회에 기기를 포함할 때 충족해야 하는 조건을 지정합니다.
5. **저장** 버튼을 누릅니다.

   설정이 적용되고 저장됩니다.

아래에서는 조회에 기기를 할당하기 위한 조건에 대해 설명합니다. OR 논리자를 이용한 조건: 조회에는 나열된 조건 중 하나 이상을 만족시키는 기기가 모두 포함됩니다.

일반

일반 섹션에서 조회 조건의 이름을 변경하고 조건이 반전되어야 하는지 여부를 지정할 수 있습니다.

선택 조건 반전

기본적으로 이 옵션은 비활성화되어 있습니다.

이 옵션을 활성화하면 지정된 선택 조건이 반대로 적용됩니다. 즉, 조건을 충족하지 않는 모든 기기가 조회에 포함됩니다.

다음 예는 반전 작업의 논리를 보여줍니다.

- **조건** : 사용자의 기기에 유형이 Linux이고 빌드 번호가 00.0.000인 운영 체제가 있습니다.
- **반전된 조건**: 사용자의 기기에 조건이 (Linux 유형 및 빌드 번호가 00.0.000) 아닌 운영 체제가 있으며, 이는 다음에 해당합니다.
  유형이 Linux가 아니거나 빌드 번호가 00.0.000이 아닌 운영 체제가 있습니다.

따라서 선택에는 예를 들어 Windows 유형과 빌드 번호 00.0.000 또는 Linux 유형과 빌드 번호 00.0.000 이외의 운영 체제가 있는 기기가 포함됩니다.

네트워크 인프라

네트워크 하위 섹션에서는 네트워크 데이터에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

- **기기 이름**

  기기의 Windows 네트워크 이름(NetBIOS 이름) 또는 IPv4 또는 IPv6 주소.

- **도메인**

  지정된 Windows 도메인에 포함된 모든 기기를 표시합니다.

- **관리 그룹**

  지정된 관리 그룹에 포함된 기기를 표시합니다.

- **설명**

  기기 속성 창의 텍스트: **일반** 섹션의 **설명** 필드.
  설명 필드에서 텍스트를 설명하기 위해 다음 문자를 사용할 수 있습니다.

  - 한 단어 내에서 찾으려면 다음과 같이 하십시오:

    - ***.** 임의 개수의 문자열을 대체합니다.

    예:
    Server 또는 **Server's** 라는 단어를 설명하려면 **Server***를 입력하면 됩니다.

    - **?.** 표시는 단일 문자를 대체합니다.

    예:
    Window, **Windows** 등의 단어를 설명하려는 경우 **Windo?**를 입력하면 됩니다.
    별표(*****) 또는 물음표(**?**)는 쿼리의 첫 문자로 사용할 수 없습니다.

  - 여러 단어를 찾으려면 다음과 같이 하십시오:

    - 공백. 나열된 단어의 어느 하나라도 설명에 포함된 모든 기기가 표시됩니다.

    예:
    설명에 **Secondary** 또는 **Virtual**이라는 단어가 포함된 문구를 찾으려면 쿼리에 **Secondary Virtual**을 입력하면 됩니다.

    - **+**. 단어 앞에 더하기 기호를 입력하면 모든 검색 결과에 해당 단어가 포함됩니다.

    예:
    Secondary 및 **Virtual**이 모두 포함된 문구를 찾으려면 **+Secondary+Virtual** 쿼리를 입력합니다.

    - **-**. 단어 앞에 빼기 기호를 입력하면 검색 결과에 해당 단어가 포함되지 않습니다.

    예:

Secondary를 포함하고 **Virtual**은 포함하지 않는 문구를 찾으려면 **+Secondary-Virtual** 쿼리를 입력합니다.

- **"<텍스트>"**. 따옴표에 둘러싸인 텍스트가 검색 결과의 텍스트에 포함됩니다.

예:

Secondary Server의 단어 조합을 포함하는 문구를 찾으려면 쿼리에 **"Secondary Server"**를 입력하면 됩니다.

- **IP 범위**

이 옵션을 사용하면 관련 기기가 포함되어야 하는 IP 범위의 첫 IP 주소와 마지막 IP 주소를 입력할 수 있습니다.
기본적으로 이 옵션은 비활성화되어 있습니다.

- **다른 중앙 관리 서버에서 관리**

다음 값 중 하나를 선택합니다:

- **예**. 다른 중앙 관리 서버에서 관리하는 클라이언트 기기에만 기기 이동 규칙이 적용됩니다. 이 서버는 기기 이동 규칙을 구성하는 서버와 다릅니다.
- **아니요**. 현재 중앙 관리 서버에서 관리하는 클라이언트 기기에만 기기 이동 규칙이 적용됩니다.
- **어떤 값도 선택되지 않았습니다**. 조건이 적용되지 않습니다.

도메인 컨트롤러 하위 섹션에서는 도메인 구성원을 기반으로 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **기기가 도메인 조직 구성 단위에 있습니다**

이 옵션을 사용하면 입력 필드에 지정한 도메인 조직 구성단위의 기기가 조회에 포함됩니다.
기본적으로 이 옵션은 비활성화되어 있습니다.

- **이 기기는 도메인 보안 그룹의 구성원입니다**

이 옵션을 사용하면 입력 필드에 지정한 도메인 보안 그룹의 기기가 조회에 포함됩니다.
기본적으로 이 옵션은 비활성화되어 있습니다.

네트워크 활동 하위 섹션에서는 네트워크 활동에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

- **배포 지점으로 역할 수행**

검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:

- **예**. 배포 지점 역할을 하는 기기가 조회에 포함됩니다.
- **아니요**. 배포 지점 역할을 하는 기기가 조회에 포함되지 않습니다.
- **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **중앙 관리 서버와 계속 연결 유지**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **활성화됨**. 조회에 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택한 기기가 포함됩니다.
  - **비활성화됨**. 조회에 **중앙 관리 서버와 계속 연결 유지** 확인란의 선택을 취소한 기기가 포함됩니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **연결 프로필이 전환됨**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 연결 프로필이 전환된 후 중앙 관리 서버에 연결된 기기가 조회에 포함됩니다.
  - **아니요**. 연결 프로필이 전환된 후 중앙 관리 서버에 연결된 기기가 조회에 포함되지 않습니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **마지막 중앙 관리 서버 연결**

  이 확인란을 이용해 중앙 관리 서버에 마지막으로 연결한 시간에 따라 기기를 검색하는 기준을 설정할 수 있습니다.

  이 확인란을 선택하면 입력 필드에서 클라이언트 기기에 설치된 네트워크 에이전트와 중앙 관리 서버 간에 마지막으로 연결이 설정된 기간(날짜 및 시간)을 지정할 수 있습니다. 지정된 간격 내에 있는 기기가 조회에 포함됩니다.

  이 확인란이 비어 있으면, 기준은 적용되지 않습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **네트워크 검색 중 탐지된 새 기기**

  지난 며칠 동안 네트워크 검색을 통해 탐지된 새 기기를 검색합니다.

  이 옵션을 사용하면 **탐지 기간(일)** 필드에 지정된 기간 동안 기기 발견에서 탐지된 새 기기만 선택에 포함됩니다.

  이 옵션이 비활성화되어 있으면 선택에는 기기 발견에서 탐지된 모든 기기가 포함됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **기기 존재 확인**

  검색을 수행할 때 조회에 기기를 포함하는 기준을 드롭다운 목록에서 설정할 수 있습니다:
  - **예**. 애플리케이션이 현재 네트워크에서 표시되는 기기를 조회에 포함시킵니다.
  - **아니요**. 애플리케이션이 현재 네트워크에 표시되지 않는 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

클라우드 세그먼트 하위 섹션에서는 개별 클라우드 세그먼트에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **기기가 클라우드 세그먼트에 있습니다**

  이 옵션이 활성화되면 AWS, Azure 및 Google 클라우드 세그먼트에서 기기를 선택할 수 있습니다.
  자식 개체 포함 옵션도 활성화되었다면, 선택한 세그먼트의 모든 자녀 개체에서 검색이 실행됩니다.
  검색 결과에는 선택한 세그먼트의 기기만 포함됩니다.

- **API를 사용해 발견된 기기**

  드롭다운 목록에서 API 도구로 기기를 탐지할지 선택할 수 있습니다:

  - **예**. AWS, Azure 또는 Google API를 사용하여 기기를 감지합니다.
  - **아니요**. AWS, Azure 또는 Google API를 사용하여 기기를 감지할 수 없습니다. 즉, 기기가 클라우드 환경 외부에 있거나, 클라우드 환경에 있지만 API를 사용하여 감지할 수 없습니다.
  - 값 없음. 이 조건이 적용되지 않습니다.

기기 상태

관리 중인 기기 상태 하위 섹션에서는 관리 중인 애플리케이션의 기기 상태 설명에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **기기 상태**

  정상, *심각* 또는 *경고* 기기 상태 중 하나를 선택할 수 있는 드롭다운 목록입니다.

- **실시간 보호 상태**

  실시간 보호 상태를 선택할 수 있는 드롭다운 목록입니다. 지정된 실시간 보호 상태의 기기가 조회에 포함됩니다.

- **기기 상태 설명**

  이 필드에서는 조건 옆의 확인란을 선택할 수 있습니다. 이러한 조건이 충족되면 *정상*, *심각* 또는 *경고* 상태 중 하나가 기기에 할당됩니다.

관리 중인 애플리케이션의 구성 요소 상태 하위 섹션에서는 관리 중인 애플리케이션의 구성 요소 상태에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **데이터 유출 방지 상태**

  데이터 유출 방지 상태(*알 수 없음*, *중지됨*, *시작 중*, *일시 중지됨*, *실행 중*, *실패*)에 따라 기기를 검색합니다.

- **협업 서버 보호 상태**

  서버 협업 보호 상태(*알 수 없음*, *중지됨*, *시작 중*, *일시 중지됨*, *실행 중*, *실패*)에 따라 기기를 검색합니다.

- **메일 서버의 안티 바이러스 보호 상태**

  메일 서버 보호 상태(*알 수 없음*, *중지됨*, *시작 중*, *일시 중지됨*, *실행 중*, *실패*)에 따라 기기를 검색합니다.

- **Endpoint Sensor 상태**

  엔드포인트 센서 구성 요소 상태(*알 수 없음*, *중지됨*, *시작 중*, *일시 중지됨*, *실행 중*, *실패*)를 기준으로 기기를 검색합니다.

관리 중인 애플리케이션에서 발생한 문제점 하위 섹션에서는 관리 중인 애플리케이션이 탐지한 가능한 문제점 목록에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다. 조회한 문제 중 하나 이상이 존재하는 기기는 조회에 포함됩니다. 여러 애플리케이션에 해당되는 문제 하나를 조회할 경우 모든 목록에서 이 문제를 자동으로 조회하도록 할 수 있습니다.

관리 중인 애플리케이션의 상태 설명에 대한 확인란을 선택할 수 있습니다. 이러한 상태 정보를 수신하면 해당 기기가 조회에 포함됩니다. 여러 애플리케이션에 해당되는 상태 하나를 조회할 경우 모든 목록에서 이 상태를 자동으로 조회하도록 할 수 있습니다.

시스템 세부 정보

운영 체제 섹션에서는 운영 체제 유형에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

- **플랫폼 유형**

  확인란을 선택하면 목록에서 운영 체제를 선택할 수 있습니다. 지정한 운영 체제가 설치된 기기가 검색 결과에 포함됩니다.

- **운영 체제 서비스 팩 버전**

  이 필드에서는 사용자 운영 체제의 패키지 버전을 *X.Y* 형식으로 지정할 수 있습니다. 지정한 버전에 따라 이동 규칙이 장치에 적용되는 방법이 결정됩니다. 기본적으로 버전 값은 지정되지 않습니다.

- **운영 체제 비트 크기**

  드롭다운 목록에서 운영 체제의 아키텍처를 선택할 수 있습니다. 선택한 아키텍처(**알 수 없음**, **x86**, **AMD64** 또는 **IA64**)에 따라 이동 규칙이 기기에 적용되는 방법이 결정됩니다. 기본적으로 목록에서 선택된 옵션은 없기 때문에 운영 체제 아키텍처는 정의되지 않게 됩니다.

- **운영 체제 빌드**

  이 설정은 Windows 운영 체제에만 적용됩니다.

운영 체제의 빌드 번호입니다. 선택한 운영 체제의 빌드 번호가 이 번호와 같아야 하는지 아니면 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 빌드 번호를 제외한 모든 빌드 번호를 검색하도록 구성할 수도 있습니다.

- **운영 체제 릴리스 번호**

  이 설정은 Windows 운영 체제에만 적용됩니다.

  운영 체제의 릴리즈 식별자(ID)입니다. 선택한 운영 체제의 릴리즈 ID가 이 ID와 같아야 하는지 아니면 이전/이후 ID여야 하는지를 지정할 수 있습니다. 지정한 릴리즈 ID 번호를 제외한 모든 번호를 검색하도록 구성할 수도 있습니다.

가상 컴퓨터 섹션에서는 기기가 가상 컴퓨터인지 아니면 가상 데스크톱 인프라(VDI)의 일부분인지에 따라 조회에 기기를 포함하기 위한 기준을 설정할 수 있습니다.

- **이것은 가상 컴퓨터입니다**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **정의 안 됨**.
  - **아니요**. 가상 컴퓨터가 아닌 기기를 찾습니다.
  - **예**. 가상 컴퓨터인 기기를 찾습니다.

- **가상 컴퓨터 유형**

  드롭다운 목록에서 가상 컴퓨터 제조업체를 선택할 수 있습니다.
  이것은 가상 컴퓨터입니다 드롭다운 목록에서 **예** 또는 **중요하지 않음** 값을 선택하면 이 드롭다운 목록을 사용할 수 있습니다.

- **가상 데스크톱 인프라 소속**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **정의 안 됨**.
  - **아니요**. VDI(Virtual Desktop Infrastructure)의 일부가 아닌 기기를 찾습니다.
  - **예**. VDI(가상 데스크톱 인프라)의 일부인 기기를 찾습니다.

자산 관리(하드웨어) 섹션에서는 설치된 하드웨어에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

하드웨어 세부 정보를 가져오려는 Linux 기기에 lshw 유틸리티가 설치되어 있는지 확인합니다. 가상 머신에서 가져온 하드웨어 세부 정보는 사용된 하이퍼바이저에 따라 불완전할 수 있습니다.

- **기기**

  드롭다운 목록에서 다음과 같은 유닛 유형을 선택할 수 있습니다. 이 유닛이 모든 기기가 검색 결과에 포함됩니다.

  이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **공급사**

  드롭다운 목록에서 유닛 제조업체의 이름을 선택할 수 있습니다. 이 유닛이 모든 기기가 검색 결과에 포함됩니다.

  이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **기기 이름**

  Windows 네트워크의 기기 이름. 지정된 이름을 가진 기기는 조회에 포함됩니다.

- **설명**

  기기 또는 하드웨어 유닛의 설명. 이 필드에서 지정된 설명에 해당하는 기기가 조회에 포함됩니다.

  모든 유형에서의 기기 설명은 해당 기기의 속성 창에 입력될 수 있습니다. 이 필드에서는 전체 텍스트 검색이 지원됩니다.

- **기기 제조업체**

  기기 제조사 이름. 이 필드에서 지정된 제조업체가 만든 기기가 조회에 포함됩니다.

  기기의 속성 창에 제조사의 이름을 입력할 수 있습니다.

- **일련 번호**

  이 필드에서 지정된 일련번호를 가진 모든 하드웨어는 조회에 포함됩니다.

- **인벤토리 번호**

  이 필드에서 지정된 인벤토리 번호를 가진 기기는 조회에 포함됩니다.

- **사용자**

  이 필드에서 지정된 사용자의 모든 하드웨어는 조회에 포함됩니다.

- **위치**

  기기 또는 하드웨어의 위치(예, 본사 또는 지사). 이 필드에서 지정된 위치에 배포된 컴퓨터 또는 기타 기기는 조회에 포함됩니다.

  기기의 속성 창에서 모든 형식으로 기기의 위치를 설명할 수 있습니다.

- **CPU 클럭 속도(MHz) 최소**

  CPU의 최소 클럭 속도입니다. 입력 필드(포함)에 지정된 클럭 속도 범위와 일치하는 CPU가 있는 기기가 조회 항목에 포함됩니다.

- **CPU 클럭 속도(MHz) 최대**

  CPU의 최대 클럭 속도입니다. 입력 필드(포함)에 지정된 클럭 속도 범위와 일치하는 CPU가 있는 기기가 조회 항목에 포함됩니다.

- **가상 CPU 코어 수, 최소**

  최소 가상 CPU 코어의 수입니다. 입력 필드에 지정된 가상 코어 수 범위(포함)와 일치하는 CPU가 있는 기기가 조회 항목에 포함됩니다.

- **가상 CPU 코어 수, 최대**

  최대 가상 CPU 코어의 수입니다. 입력 필드에 지정된 가상 코어 수 범위(포함)와 일치하는 CPU가 있는 기기가 조회 항목에 포함됩니다.

- **하드 드라이브 용량(GB), 최소**

  기기에 있는 하드 드라이브의 최소 볼륨입니다. 이러한 입력 필드(포함)에 있는 범위와 일치하는 하드 드라이브를 가진 기기가 조회에 포함됩니다.

- **하드 드라이브 용량(GB), 최대**

  기기에 있는 하드 드라이브의 최대 볼륨입니다. 이러한 입력 필드(포함)에 있는 범위와 일치하는 하드 드라이브를 가진 기기가 조회에 포함됩니다.

- **RAM 크기(MB), 최소**

  기기 RAM의 최소 크기입니다. 입력 필드에 지정된 크기 범위(포함)와 일치하는 RAM이 있는 기기가 선택 항목에 포함됩니다.

- **RAM 크기(MB)**

  기기 RAM의 최대 크기입니다. 입력 필드에 지정된 크기 범위(포함)와 일치하는 RAM이 있는 기기가 선택 항목에 포함됩니다.

타사 소프트웨어 세부 정보

자산 관리(소프트웨어) 섹션에서는 설치된 애플리케이션에 따라 기기 검색 기준을 설정할 수 있습니다.

- **애플리케이션 이름**

  애플리케이션을 선택할 수 있는 드롭다운 목록입니다. 지정된 애플리케이션이 설치된 기기가 조회에 포함됩니다.

- **애플리케이션 버전**

  선택한 애플리케이션의 버전을 지정할 수 있는 입력 필드입니다.

- **공급사**

  기기에 설치된 애플리케이션의 제조업체를 선택할 수 있는 드롭다운 목록입니다.

- **애플리케이션 상태**

  애플리케이션의 상태(*설치됨*, *설치 안 됨*)를 선택할 수 있는 드롭다운 목록입니다. 지정된 애플리케이션이 설치되어 있거나 설치되어 있지 않은 기기는 선택한 상태에 따라 조회에 포함됩니다.

- **업데이트로 찾기**

  이 옵션을 사용하면 관련 기기에 설치된 애플리케이션의 업데이트 세부 정보를 사용하여 검색이 수행됩니다. 확인란을 선택하면 **애플리케이션 이름**, **애플리케이션 버전** 및 **애플리케이션 상태** 필드가 각각 **업데이트 이름**, **업데이트 버전** 및 **상태**로 변경됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **호환되지 않는 보안 애플리케이션 이름**

  타사의 보안 제품을 선택할 수 있는 드롭다운 목록입니다. 검색 시 지정된 애플리케이션이 설치된 기기가 조회에 포함됩니다.

- **애플리케이션 태그**

  드롭다운 목록에서 애플리케이션 태그를 선택할 수 있습니다. 설명에 선택한 태그가 있는 애플리케이션이 설치된 모든 기기는 기기 조회에 포함됩니다.

- **지정한 태그가 없는 기기에 적용**

  이 옵션을 사용하면 선택에는 설명에 선택한 태그가 하나도 없는 기기가 포함됩니다.

  이 옵션을 비활성화하면 기준이 적용되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

취약점 및 업데이트 하위 섹션에서는 Windows 업데이트 경로에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

WUA가 중앙 관리 서버로 전환됨

드롭다운 목록에서 다음 검색 옵션 중 하나를 선택할 수 있습니다:

- **예**. 이 옵션을 선택하면 Windows 업데이트를 통해 중앙 관리 서버에서 업데이트를 받는 기기가 검색 결과에 포함됩니다.
- **아니요**. 이 옵션을 선택하면 Windows 업데이트를 통해 다른 경로에서 업데이트를 받는 기기가 결과에 포함됩니다.

Kaspersky 애플리케이션 세부 정보

Kaspersky 애플리케이션 하위 섹션에서는 선택한 관리 중인 애플리케이션에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

- **애플리케이션 이름**

  Kaspersky 애플리케이션 이름별로 검색 수행 시 조회에 포함될 기기의 기준을 드롭다운 목록에서 지정할 수 있습니다.

  이 목록에는 관리자의 워크스테이션에서 관리 플러그인이 설치된 애플리케이션 이름만 표시됩니다.

  애플리케이션을 선택하지 않았다면, 이 기준은 적용되지 않습니다.

- **애플리케이션 버전**

  Kaspersky 애플리케이션 버전 이름별로 검색 수행 시 조회에 포함될 기기의 기준을 입력 필드에서 지정할 수 있습니다.

  버전 번호가 지정되지 않으면 기준이 적용되지 않습니다.

- **긴급 업데이트 이름**

  애플리케이션의 상태(*설치됨*, *설치 안 됨*)를 선택할 수 있는 드롭다운 목록입니다. 지정된 애플리케이션이 설치되어 있거나 설치되어 있지 않은 기기는 선택한 상태에 따라 조회에 포함됩니다.

  입력 필드에서 애플리케이션 이름 또는 업데이트 패키지 번호로 검색 수행 시 조회에 포함될 기기의 기준을 지정할 수 있습니다.

  필드를 비워두면 기준이 적용되지 않습니다.

- **모듈의 마지막 업데이트 기간을 선택합니다**

  이 설정을 사용해 기기에 설치된 애플리케이션 모듈의 마지막 업데이트 시간으로 기기를 검색하기 위한 기준을 설정할 수 있습니다.

  이 확인란을 선택하면 입력 필드에서 기기에 설치된 애플리케이션 모듈의 마지막 업데이트가 수행된 시간 간격(날짜와 시간)을 지정할 수 있습니다.

  이 확인란이 비어 있으면, 기준은 적용되지 않습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **중앙 관리 서버로 기기를 관리 중입니다**

  드롭다운 목록에서는 Kaspersky Security Center를 통해 관리되는 기기를 조회에 포함할 수 있습니다:
  - **예**. 애플리케이션이 Kaspersky Security Center를 통해 관리 중인 기기를 조회에 포함합니다.
  - **아니요**. 애플리케이션이 Kaspersky Security Center를 통해 관리되지 않는 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

- **보안 제품이 설치되어 있음**

  드롭다운 목록에서는 보안 제품이 설치된 모든 기기를 조회에 포함할 수 있습니다:
  - **예**. 애플리케이션이 보안 제품이 설치된 모든 기기를 조회에 포함합니다.
  - **아니요**. 애플리케이션이 보안 제품이 설치되지 않은 모든 기기를 조회에 포함합니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

안티 바이러스 보호 하위 섹션에서는 보호 상태에 따라 조회에 기기를 포함하기 위한 기준을 설정할 수 있습니다.

- **데이터베이스 배포 날짜**

  이 옵션을 선택하면 안티 바이러스 데이터베이스 배포 날짜를 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에 수행하려는 검색을 기반으로 기간을 설정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **데이터베이스 레코드 수**

  이 옵션을 사용하면 데이터베이스 레코드 수를 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에 안티 바이러스 데이터베이스 레코드의 상한 및 하한 임계값을 설정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **마지막 검사**

  이 확인 옵션을 사용하면 마지막 악성 코드 검사 시간을 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에서 마지막 악성 코드 검사가 수행된 시간을 지정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **위협이 탐지됨**

  이 옵션을 사용하면 탐지된 바이러스 수를 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에 탐지된 바이러스 수에 대한 상한 및 하한 임계값을 설정할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

암호화 하위 섹션에서는 선택한 암호화 알고리즘에 따라 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

암호화 알고리즘

AES(Advanced Encryption Standard) 대칭 블록 암호화 알고리즘입니다. 드롭다운 목록에서 암호화 키 크기(56비트, 128비트, 192비트 또는 256비트)를 선택할 수 있습니다.

사용 가능한 값: *AES56*, *AES128*, *AES192* 및 *AES256*.

애플리케이션 구성 요소 하위 섹션에는 Kaspersky Security Center 웹 콘솔에 해당 관리 플러그인이 설치된 애플리케이션의 구성 요소 목록이 포함되어 있습니다.

애플리케이션 구성 요소 하위 섹션에서는 선택한 애플리케이션을 지칭하는 구성 요소의 상태와 버전 번호에 따라 조회에 기기를 포함하기 위한 기준을 지정할 수 있습니다.

- **상태**

  애플리케이션이 중앙 관리 서버로 전송하는 구성 요소 상태에 따라 기기를 검색합니다. *N/A*, *중지됨*, *일시 중지됨*, *시작 중*, *실행 중*, *실패*, *설치되지 않음*, *라이센스에서 지원하지 않음* 등의 상태 중 하나를 선택할 수 있습니다. 관리 중인 기기에 설치되어 있는 애플리케이션의 선택한 구성 요소 상태가 지정한 값이면 해당 기기가 기기 조회에 포함됩니다.

  애플리케이션에서 전송하는 상태:

  - *중지됨* - 구성 요소가 비활성화되었으며 현재 작동하고 있지 않습니다.
  - *일시 중지됨* - 구성 요소가 일시 중지되었습니다. 예를 들어 사용자가 관리 중인 애플리케이션에서 보호를 일시 중지했습니다.
  - *시작 중* - 구성 요소가 현재 초기화되고 있습니다.
  - *실행 중* - 구성 요소가 활성화되어 정상 작동하고 있습니다.
  - *오작동* - 구성 요소 작동 중에 오류가 발생했습니다.
  - *설치 안 됨* - 사용자가 애플리케이션의 사용자 지정 설치를 구성할 때 설치할 구성 요소를 선택하지 않았습니다.
  - *라이센스에서 지원하지 않음* - 선택한 구성 요소에 라이센스가 적용되지 않습니다.

  다른 상태와 달리 애플리케이션은 *N/A* 상태를 전송하지 않습니다. 이 옵션은 선택한 구성 요소 상태 관련 정보가 애플리케이션에 없음을 표시합니다. 예를 들어 선택한 구성 요소가 기기에 설치된 어떤 애플리케이션에도 속하지 않거나 기기가 꺼져 있으면 이 상태가 표시될 수 있습니다.

- **버전**

  목록에서 선택하는 구성 요소의 버전 번호에 따라 기기를 검색합니다. `3.4.1.0` 등의 버전 번호를 입력한 다음 선택한 구성 요소의 버전이 해당 번호와 같아야 하는지 아니면 그 이전/이후 번호여야 하는지를 지정할 수 있습니다. 지정한 버전을 제외한 모든 버전을 검색하도록 구성할 수도 있습니다.

태그

태그 섹션에서는 이전에 관리 중인 기기 설명에 추가한 키워드(태그)를 기준으로 하여 조회에 기기를 포함하기 위한 기준을 구성할 수 있습니다.

하나 이상의 지정 태그가 일치하면 적용

이 옵션을 사용하면 검색 결과에는 선택한 태그 중 적어도 하나와 일치하는 설명이 있는 기기가 표시됩니다.

이 옵션이 비활성화되어 있으면 검색 결과에는 모든 선택한 태그와 일치하는 설명이 있는 기기만 표시됩니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

기준에 태그를 추가하려면 **추가** 버튼을 클릭하고 **태그** 입력 필드를 클릭하여 태그를 선택합니다. 기기 선택에서 선택한 태그가 있는 기기를 포함할지 또는 제외할지 지정합니다.

- **이 태그가 있는 모든 기기**

  이 옵션을 선택하는 경우 설명에 선택한 태그가 포함되어 있는 기기가 검색 결과에 표시됩니다. 기기를 찾으려는 경우 문자 수에 관계 없이 임의의 문자열을 나타내는 별표를 사용할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **이 태그가 없는 모든 기기**

  이 옵션을 선택하는 경우 설명에 선택한 태그가 포함되어 있지 않은 기기가 검색 결과에 표시됩니다. 기기를 찾으려는 경우 문자 수에 관계 없이 임의의 문자열을 나타내는 별표를 사용할 수 있습니다.

사용자

사용자 섹션에서는 운영 체제에 로그인한 사용자 계정에 따라 조회에 기기를 포함하기 위한 기준을 설정할 수 있습니다.

- **시스템에 마지막으로 로그인한 사용자**

  이 옵션을 활성화하면 기준을 구성하기 위한 사용자 계정을 선택할 수 있습니다. 선택한 사용자가 시스템에 마지막으로 로그인한 기기가 검색 결과에 포함됩니다.

- **시스템에 적어도 한 번 이상 로그인한 사용자**

  이 옵션을 사용하면 **찾기** 버튼을 눌러 사용자 계정을 지정할 수 있습니다. 지정한 사용자가 한 번 이상 시스템에 로그인한 기기가 검색 결과에 포함됩니다.

기기 조회에서 기기 목록 내보내기

Kaspersky Security Center의 기기 조회에서 기기에 대한 정보를 저장하거나 CSV 또는 TXT 파일로 내보낼 수 있습니다.

기기 조회에서 기기 목록을 보려면:

1. 기기 조회에서 기기가 있는 테이블을 엽니다.
2. 다음 방법 중 하나를 사용하여 내보낼 기기를 선택하십시오.
   - 특정 기기를 선택하려면 해당 기기 옆에 있는 확인란을 선택합니다.
   - 현재 테이블 페이지에서 모든 기기를 선택하려면 기기 테이블 머리글의 확인란을 선택한 다음 **현재 페이지에서 모두 선택** 확인란을 선택합니다.
   - 테이블에서 모든 기기를 선택하려면 기기 테이블 머리글에서 확인란을 선택한 다음 **모두 선택** 확인란을 선택합니다.
3. **CSV로 내보내기** 또는 **TXT로 내보내기** 버튼을 클릭합니다. 표에 포함된 조회 기기에 대한 모든 정보를 내보냅니다.

기기 테이블에 필터 기준을 적용했다면, 표시된 열에서 필터링된 데이터만 내보내 집니다.

조회된 관리 그룹에서 기기 제거

기기 조회를 설정할 때, 제거되어야 하는 기기를 관리 그룹으로 전환할 필요없이 이 조회에 있는 관리 그룹에서 기기를 제거할 수 있습니다.

관리 그룹에서 기기를 제거하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 기기 선택** 또는 **발견 및 배포 → 기기 선택**로 갑니다.
2. 조회 목록에서 기기 조회 이름을 누릅니다.
   이 페이지에는 기기 조회에 포함된 기기에 대한 정보가 있는 테이블이 표시됩니다.
3. 제거할 기기를 선택하고 **삭제**를 클릭합니다.
   그러면 선택한 기기가 해당 관리 그룹에서 제거됩니다.

기기 태그

Kaspersky Security Center에서는 기기를 *태그*할 수 있습니다. 태그는 기기 그룹화, 설명, 검색 등에 사용할 수 있는 기기의 레이블입니다. 기기에 할당된 태그는 조회 만들기, 기기 검색 및 관리 그룹에 기기 배포 작업에 사용할 수 있습니다.

태그를 수동 또는 자동으로 할당할 수 있습니다. 개별 기기에 태그를 지정하려면 수동 태그 지정을 사용할 수 있습니다. Kaspersky Security Center는 다음 중 한 가지 방식으로 자동 태그 지정을 수행합니다.

- 지정된 태그 지정 규칙을 따릅니다.
- 애플리케이션으로 수행합니다.

동일한 태그를 할당하기 위해 다른 태그 지정 방법을 사용하는 것은 권장하지 않습니다. 예를 들어 규칙에 따라 태그가 할당된 경우 이 태그를 기기에 직접 할당하지 않는 것을 권장합니다.

규칙에 따라 태그가 할당되면, 지정된 규칙이 충족되었을 때 기기에 자동으로 태그가 지정됩니다. 각 태그별로 해당하는 개별 규칙이 있습니다. 규칙은 기기의 네트워크 속성, 운영 체제, 기기에 설치된 애플리케이션 및 기타 기기 속성에 적용됩니다. 예를 들어 물리적 컴퓨터, Amazon EC2 인스턴스 및 Microsoft Azure 가상 컴퓨터로 구성된 하이브리드 인프라가 있는 경우 모든 Microsoft Azure 가상 컴퓨터에 `[Azure]` 태그를 할당하는 규칙을 설정할 수 있습니다. 그런 다음 기기 조회를 만들 때 이 태그를 사용할 수 있습니다. 그러면 모든 Microsoft Azure 가상 컴퓨터를 손쉽게 분류하고 작업을 할당할 수 있습니다.

자동 태그 입력 규칙은 태그당 한 개만 추가할 수 있습니다. 같은 태그에 대해 새 규칙을 생성할 경우 이전 규칙이 대체됩니다.

다음과 같은 경우 기기에서 태그가 자동으로 제거됩니다.

- 태그를 할당하는 규칙의 조건을 기기가 더 이상 충족하지 않는 경우.
- 태그를 할당하는 규칙이 비활성화되거나 삭제된 경우.

각 중앙 관리 서버의 태그 목록과 규칙 목록은 기본 중앙 관리 서버 또는 종속 가상 중앙 관리 서버를 비롯한 기타 모든 중앙 관리 서버와는 독립적입니다. 규칙은 규칙이 생성된 중앙 관리 서버의 기기에만 적용됩니다.

기기 태그 만들기

기기 태그를 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **태그** → **기기 태그**로 이동합니다.
2. **추가**를 누릅니다.
   새 태그 창이 열립니다.
3. **태그** 필드에 태그 이름을 입력합니다.
4. **저장**을 눌러 변경 사항을 저장합니다.

   기기 태그 목록에 새 태그가 표시됩니다.

기기 태그 이름 바꾸기

기기 태그 이름을 바꾸려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 태그 → 기기 태그**로 이동합니다.
2. 이름을 바꿀 태그의 이름을 누릅니다.
   태그 속성 창이 열립니다.
3. **태그** 필드에서 태그 이름을 변경합니다.
4. **저장** 눌러 변경 사항을 저장합니다.

업데이트된 태그가 기기 태그 목록에 표시됩니다.

기기 태그 삭제

기기 태그를 삭제하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 태그 → 기기 태그**로 이동합니다.
2. 목록에서 삭제할 기기 태그를 선택합니다.
3. **삭제** 버튼을 누릅니다.
4. 창이 열리면 **예**를 누릅니다.

기기 태그가 삭제됩니다. 삭제된 태그는 할당되었던 모든 기기에서 자동으로 제거됩니다.

> 삭제한 태그는 자동 태그 추가 규칙에서 자동으로 제거되지 않습니다. 삭제된 태그는 기기가 태그를 할당하는 규칙의 조건을 먼저 충족해야 새 기기에 할당됩니다.

> 삭제된 태그가 애플리케이션 또는 네트워크 에이전트가 기기에 할당한 태그라면, 기기에서 자동 제거되지 않습니다. 이러한 태그를 제거하려면 klscflag 유틸리티를 사용하십시오.

태그가 할당된 기기 보기

태그가 할당된 기기를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 태그 → 기기 태그**로 이동합니다.
2. 할당된 기기를 확인하려는 태그 옆의 **기기 보기** 링크를 누릅니다.
   관리 중인 기기 링크를 클릭한 태그로 기기가 필터링된 기본 메뉴의 **기기 보기** 섹션으로 리다이렉트됩니다.
3. 기기 태그 목록으로 돌아가려면 브라우저의 **뒤로** 버튼을 누릅니다.

태그가 할당된 기기를 확인한 후 새 태그를 생성하여 할당하거나 기존 태그를 다른 기기에 할당할 수 있습니다. 이 경우 태그로 필터링을 제거하고 기기를 선택한 다음 태그를 할당해야 합니다.

기기에 할당된 태그 보기

기기에 할당된 태그를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **관리 중인 기기** 로 이동합니다.
2. 태그를 보려는 기기의 이름을 누릅니다.
3. 기기 속성 창이 열리면 **태그** 탭을 선택합니다.

   선택한 기기에 할당되어 있는 태그의 목록이 표시됩니다. **태그 할당 방식** 열에서 태그가 할당된 방법을 확인할 수 있습니다.

도구 모음에서 다음을 수행할 수 있습니다.

- 기기에 다른 태그를 할당합니다.
- 이미 할당된 태그를 제거합니다.
- 중앙 관리 서버의 모든 기기 태그를 볼 수 있습니다.

할당된 태그는 기기에서 로컬로 볼 수 없습니다.

수동으로 기기에 태그 지정

기기에 수동으로 태그를 할당하려면 다음 단계를 따릅니다.

1. 다른 태그를 할당할 기기에 할당된 태그를 확인합니다.
2. **추가**를 누릅니다.
3. 창이 열리면 다음 중 하나를 수행합니다.
   - 새 태그를 생성하여 할당하려면 **새 태그 생성**을 선택한 다음 새 태그의 이름을 지정합니다.
   - 기존 태그를 선택하려면 **기존 태그 할당**을 선택하고 드롭다운 목록에서 필요한 태그를 선택합니다.
4. **확인**을 눌러 변경을 적용합니다.
5. **저장**을 눌러 변경 사항을 저장합니다.

   선택한 태그가 기기에 할당됩니다.

기기에서 할당된 태그 제거

기기에서 태그를 제거하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기** 로 이동합니다.
2. 태그를 보려는 기기의 이름을 누릅니다.
3. 기기 속성 창이 열리면 **태그** 탭을 선택합니다.
4. 제거할 태그 옆에 있는 확인란을 선택합니다.
5. 목록 상단에서 **태그 할당을 해제하시겠습니까?** 버튼을 클릭합니다.
6. 창이 열리면 **예**를 누릅니다.

   태그가 기기에서 제거됩니다.

미할당 기기 태그는 삭제되지 않습니다. 원하는 경우 태그를 수동으로 삭제할 수 있습니다.

애플리케이션 또는 네트워크 에이전트가 기기에 할당한 태그는 수동으로 제거할 수 없습니다. 이러한 태그를 제거하려면 klscflag 유틸리티를 사용하십시오.

자동으로 기기에 태그를 지정하는 규칙 보기

자동으로 기기에 태그를 지정하는 규칙을 보려면

다음을 수행합니다:

- 메인 메뉴에서 **에셋(기기) → 태그 → 자동 태그 입력 규칙**로 이동합니다.
- 메인 메뉴에서 **에셋(기기) → 태그 → 기기 태그**로 이동한 다음 **자동 태그 입력 규칙 설정** 링크를 클릭합니다.
- 기기에 할당된 태그를 확인한 다음 **설정** 버튼을 누릅니다.

자동으로 기기에 태그를 지정하는 규칙 목록이 나타납니다.

자동으로 기기에 태그를 지정하는 규칙 편집

자동으로 기기에 태그를 지정하는 규칙을 편집하려면 다음 단계를 따릅니다.

1. 자동으로 기기에 태그를 지정하는 규칙을 확인합니다.
2. 편집할 규칙의 이름을 누릅니다.
   규칙 설정 창이 열립니다.

3. 해당 규칙의 일반 속성을 편집합니다.

    a. **규칙 이름** 필드에서 규칙 이름을 변경합니다.
    이름은 256자를 초과할 수 없습니다.

    b. 다음을 수행합니다:

    - 토글 버튼을 **규칙 활성화됨**으로 전환하여 규칙을 활성화합니다.
    - 토글 버튼을 **규칙 비활성화됨**으로 전환하여 규칙을 비활성화합니다.

4. 다음을 수행합니다:

- 새 조건을 추가하려면 **추가** 버튼을 누르고 열리는 창에서 새 조건 설정을 지정합니다.
- 기존 조건을 편집하려면 편집할 조건의 이름을 누르고 조건 설정을 편집합니다.
- 조건을 삭제하려면 삭제할 조건 이름 옆의 확인란을 선택하고 **삭제**를 누릅니다.

5. 규칙 설정 창에서 **확인**을 누릅니다.

6. **저장**을 눌러 변경 사항을 저장합니다.

편집한 규칙이 목록에 표시됩니다.

자동으로 기기에 태그를 지정하는 규칙 생성

자동으로 기기에 태그를 지정하는 규칙을 생성하려면 다음 단계를 따릅니다.

1. 자동으로 기기에 태그를 지정하는 규칙을 확인합니다.

2. **추가**를 누릅니다.
새 규칙 설정 창이 열립니다.

3. 해당 규칙의 일반 속성을 구성합니다.

    a. **규칙 이름** 필드에 새 규칙 이름을 입력합니다.
    이름은 256자를 초과할 수 없습니다.

    b. 다음 중 하나를 수행합니다:

    - 토글 버튼을 **규칙 활성화됨**으로 전환하여 규칙을 활성화합니다.
    - 토글 버튼을 **규칙 비활성화됨**으로 전환하여 규칙을 비활성화합니다.

    c. **태그** 필드에 새 기기 태그 이름을 입력하거나 목록에서 기존 기기 태그 중 하나를 선택합니다.
    이름은 256자를 초과할 수 없습니다.

4. 조건 섹션에서 **추가** 버튼을 눌러 새 조건을 추가합니다.
새 조건 설정 창이 열립니다.

5. 조건 이름을 입력합니다.
이름은 256자를 초과할 수 없습니다. 이름은 규칙 내에서 고유해야 합니다.

6. 다음 조건에 따라 규칙 활성화를 설정합니다. 조건은 여러 개 선택할 수 있습니다.

   - **네트워크** - Windows 네트워크의 기기 이름, 도메인이나 IP 서브넷에 기기가 포함되는지 여부와 같은 기기의 네트워크 속성입니다.

     Kaspersky Security Center에 사용하는 데이터베이스에 대해 대소문자 구분 데이터 정렬이 설정되었다면, 장치 DNS 이름을 지정할 때 대소문자를 구분합니다. 그렇지 않으면 자동 태그 추가 규칙이 작동하지 않습니다.

   - **애플리케이션** - 기기의 네트워크 에이전트 유무와 운영 체제 유형, 버전, 아키텍처입니다.
   - **가상 컴퓨터** - 기기가 특정 유형의 가상 컴퓨터에 속합니다.
   - **도메인 컨트롤러** - Active Directory 조직 구성 단위에 기기가 있는지 여부와 Active Directory 그룹의 기기 멤버십입니다.
   - **자산 관리(소프트웨어)** - 기기에 다양한 공급업체의 애플리케이션이 설치되어 있는지 여부입니다.

7. **확인**을 눌러 변경을 저장합니다.

   필요한 경우 규칙 하나에 여러 조건을 설정할 수 있습니다. 이 경우 기기가 조건 하나 이상을 충족하면 태그가 기기에 할당됩니다.

8. **저장**을 눌러 변경 사항을 저장합니다.

   선택한 중앙 관리 서버를 통해 관리 중인 기기에서 새로 만든 규칙이 적용됩니다. 기기 설정이 규칙 조건을 충족하면 기기에 태그가 할당됩니다.

나중에 규칙은 다음과 같은 경우 적용됩니다.

- 서버 워크로드에 따라 자동/주기적으로
- 규칙을 편집한 후
- 규칙을 수동으로 실행할 때
- 중앙 관리 서버가 규칙 조건을 충족하는 기기 설정 또는 이런 기기를 포함하는 그룹 설정의 변경 사항을 탐지한 후

여러 개의 태그 규칙을 만들 수도 있습니다. 여러 개의 태그 규칙을 만들었는데 각 규칙의 조건이 동시에 충족되는 경우 한 기기에 여러 태그가 할당될 수 있습니다. 기기 속성에서 할당된 모든 태그의 목록을 볼 수 있습니다.

기기 자동 태그 지정을 위한 규칙 실행

규칙을 실행하면 해당 규칙의 속성에 지정된 태그가 동일 규칙의 속성에 지정된 조건을 충족하는 기기에 할당됩니다. 활성 규칙만 실행할 수 있습니다.

자동으로 기기에 태그를 지정하는 규칙을 실행하려면 다음 단계를 따릅니다.

1. 자동으로 기기에 태그를 지정하는 규칙을 확인합니다.
2. 실행할 활성 규칙 옆의 확인란을 선택합니다.
3. **규칙 실행** 버튼을 누릅니다.

선택한 규칙이 실행됩니다.

자동으로 기기에 태그를 지정하는 규칙 삭제

자동으로 기기에 태그를 지정하는 규칙을 삭제하려면 다음 단계를 따릅니다.

1. 자동으로 기기에 태그를 지정하는 규칙을 확인합니다.
2. 삭제할 규칙 옆의 확인란을 선택합니다.
3. **삭제**를 누릅니다.
4. 창이 열리면 **삭제**를 누릅니다.

선택한 규칙이 삭제됩니다. 이 규칙의 속성에 지정된 태그가 할당되었던 모든 기기에서 할당 취소됩니다.

> 미할당 기기 태그는 삭제되지 않습니다. 원하는 경우 태그를 수동으로 삭제할 수 있습니다.

Klscflag 유틸리티를 사용하여 기기 태그 관리

태그 세트를 기기에 할당하려면 태그를 할당하려는 클라이언트 기기에서 klscflag 유틸리티를 실행해야 합니다.

klscflag 유틸리티는 기기에 할당된 기존 태그를 덮어씁니다. 즉, 명령에서 원하는 태그 세트를 지정하여 새로운 태그를 추가하거나 태그를 제거할 수 있습니다. 이 유틸리티에는 개별 태그를 추가하거나 제거하기 위한 별도의 명령이 없습니다. 대신, 전체 태그 세트를 수정할 수 있습니다.

> klscflag 같은 명령어에서 태그 이름을 지정할 때는 모두 대문자로 작성하는 등 일관된 대소문자 접근 방식을 사용하는 것이 좋습니다. 모두 대문자를 사용하면 DBMS 구성에 따라 대소문자만 다른 태그로 인해 발생할 수 있는 잠재적인 문제를 방지하는 데 도움이 됩니다.

klscflag 유틸리티를 사용하여 기기에 태그를 할당하려면:

1. 관리자 권한을 사용하여 Windows 명령 프롬프트를 실행한 후 klscflag 유틸리티를 사용하여 현재 디렉터리를 해당 디렉터리로 변경합니다. klscflag 유틸리티는 네트워크 에이전트가 설치된 폴더에 있습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\NetworkAgent입니다.
2. 다음 명령 중 하나를 실행합니다.
   - 태그 세트 할당

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" 태그명 1\",\" 태그명 2\",\" 태그명 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

여기에서 [\" 태그명 1\",\" 태그명 2\",\" 태그명 3\"]은 기기에 할당하려는 태그 목록입니다.

대괄호 안을 비워두면 기기에서 모든 태그가 제거됩니다.

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

- 기존 태그 세트에 새 태그 지정

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" 새로운 태그명\",\" 태그명 1\",\" 태그명 2\",\" 태그명 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

여기에서 새로운 태그명은 기기에 할당하려는 태그의 이름이고 태그명 1, 태그명 2, 태그명 3은 기기에 이미 할당된 태그의 이름입니다.

- 기기에 이미 할당된 다른 태그를 제거하지 않고 특정 태그만 제거하려면 업데이트된 태그 세트를 사용하여 명령을 실행합니다.

  예를 들어, 현재 태그가 태그명 1, 태그명 2, 태그명 3이고 태그명 2를 제거하고 싶다면 다음 명령을 실행합니다.

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" 태그명 1\",\" 태그명 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

3. 그리고, 네트워크 에이전트 서비스를 재시작합니다.

   klscflag 유틸리티는 기기에 지정된 태그를 할당합니다.

4. klscflag 유틸리티가 지정된 태그를 제대로 할당했는지 확인하려는 경우, 기기에 할당된 태그를 봅니다.

또는 기기 태그를 수동으로 할당할 수 있습니다.

정책 및 정책 프로필

Kaspersky Security Center 웹 콘솔에서는 Kaspersky 애플리케이션용 정책을 만들 수 있습니다. 이 섹션에서는 정책 및 정책 프로필을 설명하고 정책을 만들고 수정하기 위한 지침을 제공합니다.

활성 정책 및 정책 프로필 정보

*정책*은 중앙 관리 그룹 및 그 하위 그룹에 적용되는 Kaspersky 애플리케이션 설정의 집합입니다. 관리 그룹의 기기에 여러 Kaspersky 애플리케이션을 설치할 수 있습니다. Kaspersky Security Center는 관리 그룹의 각 Kaspersky 애플리케이션에 대해 단일 정책을 제공합니다. 정책의 상태는 다음 중 하나입니다(아래 표 참조).

정책의 상태

상태	설명
활성	기기에 적용되는 현재 정책입니다. 각 관리 그룹의 Kaspersky 애플리케이션에는 하나의 정책만 활성화될 수 있습니다. 기기는 Kaspersky 애플리케이션에 대한 활성 정책의 설정 값을 적용합니다.
비활성	현재 기기에 적용되지 않은 정책입니다.
이동 사용자	이 옵션을 선택하면 기기가 회사 네트워크를 벗어나는 경우 정책이 활성화됩니다.

정책은 다음 규칙에 따라 작동합니다.

- 하나의 애플리케이션에 대해 서로 다른 값을 갖는 다중 정책을 구성할 수 있습니다.
- 현재 애플리케이션에 하나의 정책만 활성화될 수 있습니다.
- 특정 이벤트가 발생하면 비활성화된 정책을 활성화할 수 있습니다. 예를 들어 바이러스가 급증할 때 더 엄격한 안티 바이러스 보호 설정을 강제할 수 있습니다.
- 정책에는 하위 정책이 포함될 수 있습니다.

일반적으로 바이러스 공격과 같은 비상 상황에 대비하여 정책을 사용할 수 있습니다. 예를 들어, 플래시 드라이브를 통한 공격이 있는 경우 플래시 드라이브에 대한 액세스를 차단하는 정책을 활성화할 수 있습니다. 이 경우 현재 활성 정책은 자동으로 비활성화됩니다.

예를 들어 서로 다른 상황에서 여러 설정만 변경한다고 가정하는 경우와 같이 여러 정책을 유지하는 것을 방지하기 위해 정책 프로필을 사용할 수 있습니다.

*정책 프로필*은 정책의 설정 값을 대체하는 정책 설정 값으로 구성된 명명된 하위 집합입니다. 정책 프로필은 관리 중인 기기에 대한 유효 설정 구성에 영향을 줍니다. *유효 설정*은 현재 기기에 적용된 정책 설정, 정책 프로필 설정 및 로컬 애플리케이션 설정의 집합입니다.

정책 프로필은 다음 규칙에 따라 작동합니다.

- 정책 프로필은 특정 활성화 조건이 발생할 때 적용됩니다.
- 정책 프로필에는 정책 설정이 아닌 설정 값이 포함됩니다.
- 정책 프로필을 활성화하면 관리 중인 기기의 유효 정책 설정이 변경됩니다.
- 프로필에는 최대 100개의 정책 프로필이 포함될 수 있습니다.

잠금 및 잠긴 설정 정보

각 정책 설정에는 잠금 버튼 아이콘(🔓)이 있습니다. 아래 표는 잠금 버튼 상태를 보여줍니다.

잠금 버튼 상태

상태	설명
정의 안 됨	설정 옆에 열린 자물쇠가 표시되고 토글 버튼이 비활성화되어 있으면 해당 설정이 정책에 지정되지 않은 것입니다. 사용자는 관리 중인 애플리케이션 인터페이스에서 이러한 설정을 변경할 수 있습니다. 이러한 유형의 설정을 *잠금 해제*라고 합니다.
강제 실행	설정 옆에 잠긴 자물쇠가 표시되고 토글 버튼이 활성화된 경우 해당 설정은 정책이 강제 실행되는 기기에 적용됩니다. 사용자는 관리 중인 애플리케이션 인터페이스에서 이러한 설정의 값을 수정할 수 없습니다. 이러한 유형의 설정을 *잠김*이라고 합니다.

관리 중인 기기에 적용하려는 정책 설정에 대해서는 잠금을 설정하는 것이 좋습니다. 잠금 해제된 정책 설정은 관리 중인 기기의 Kaspersky 애플리케이션 설정에서 재할당할 수 있습니다.

잠금 버튼을 사용하여 다음 작업을 수행할 수 있습니다.

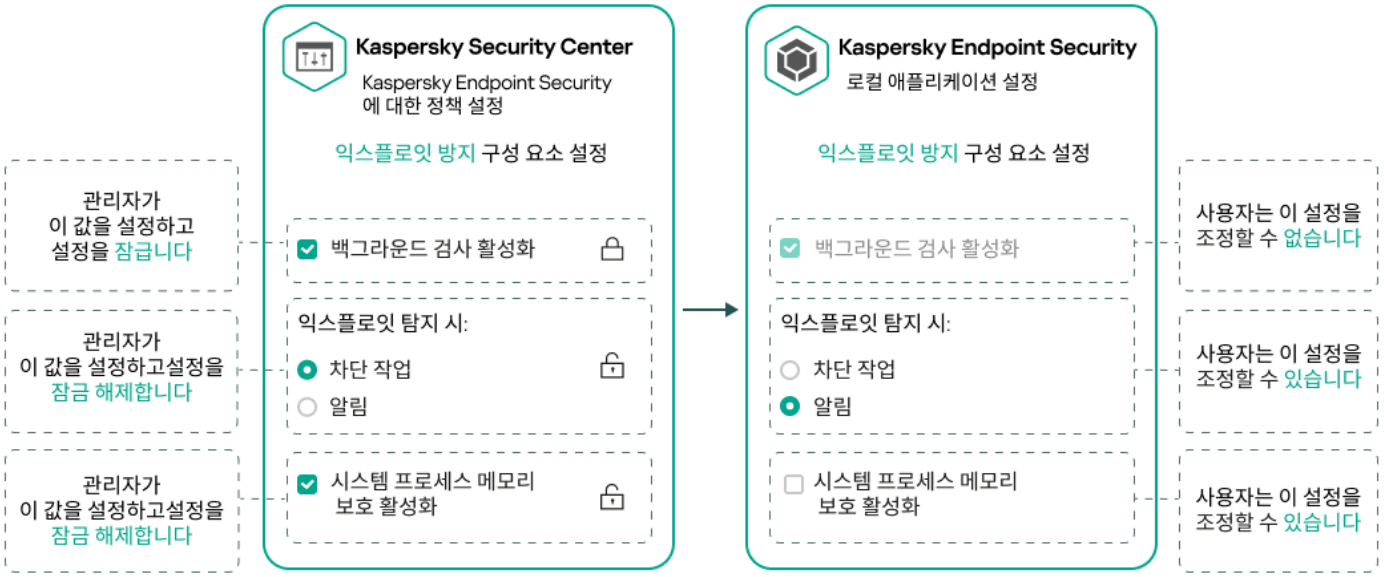
- 관리 하위 그룹 정책에 대한 잠금 설정
- 관리 중인 기기에서 Kaspersky 애플리케이션 잠금 설정

따라서 잠금 설정은 관리 중인 기기에서 유효 설정을 구현하는 데 사용됩니다.

유효 설정 구현 프로세스에는 다음 작업이 포함됩니다.

- 관리 중인 기기에서 Kaspersky 애플리케이션의 설정 값을 적용합니다.
- 관리 중인 기기에서 정책의 잠긴 설정 값을 적용합니다.

정책 및 관리 중인 Kaspersky 애플리케이션은 같은 설정을 포함합니다. 정책 설정을 구성하면 Kaspersky 애플리케이션 설정을 통해 관리 중인 기기의 값을 변경할 수 있습니다. 관리 중인 기기에서는 잠긴 설정을 조정할 수 없습니다(아래 그림 참조).



잠금 및 Kaspersky 애플리케이션 설정

정책 상속 및 정책 프로필

이 섹션은 정책 및 정책 프로필의 계층 및 상속에 대한 정보를 제공합니다.

정책 계층 구조

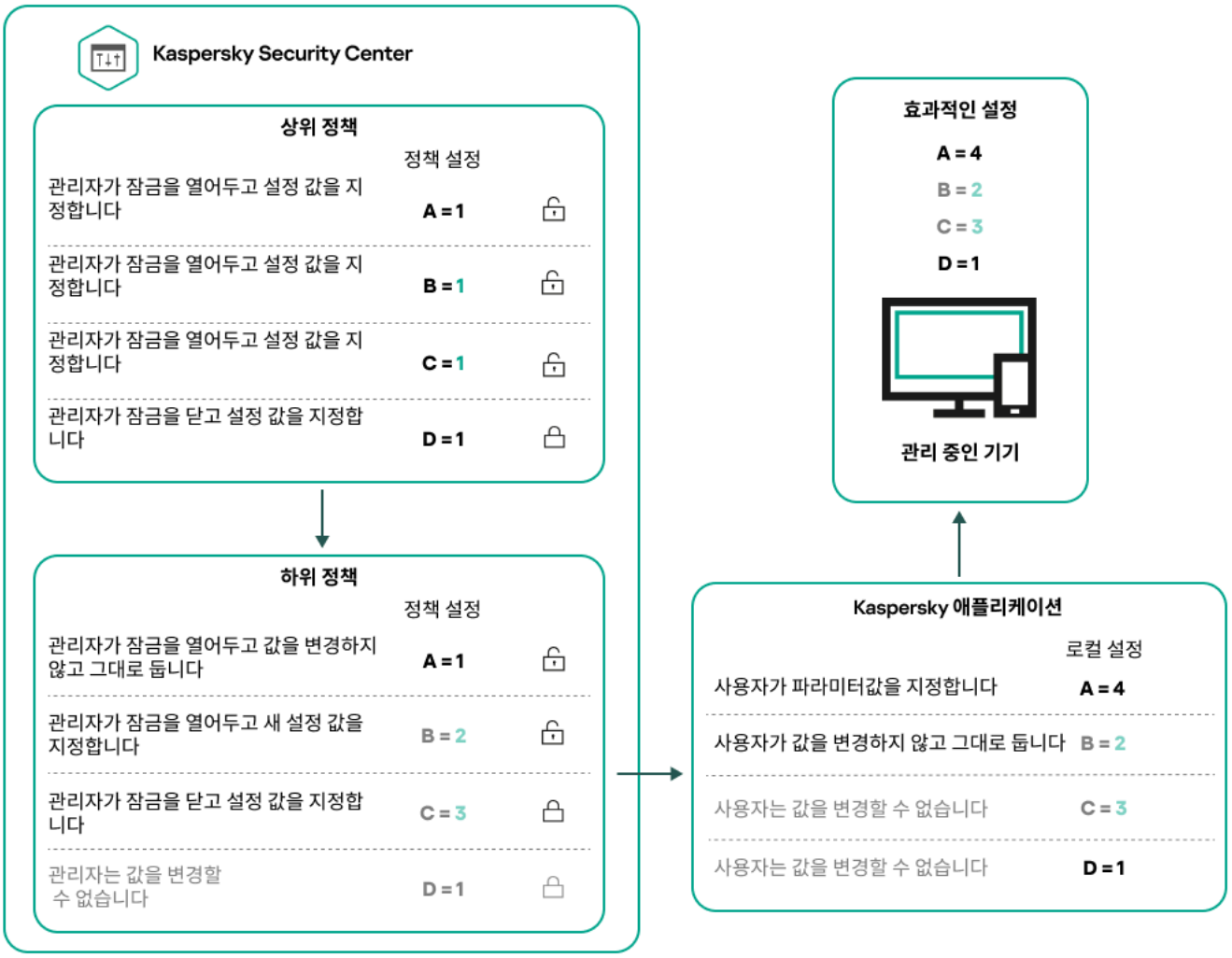
기기마다 다른 설정이 필요한 경우 기기를 관리 그룹으로 구성할 수 있습니다.

단일 관리 그룹에 대한 정책을 지정할 수 있습니다. 정책 설정은 *상속*될 수 있습니다. 상속이란 상위(부모) 관리 그룹의 하위 그룹(자식 그룹)의 정책 설정 값을 수신하는 것을 의미합니다.

아래에서는 부모 그룹의 정책이 *부모 정책*으로도 지칭됩니다. 하위 그룹(자식 그룹)의 정책은 *자식 정책*으로도 지칭됩니다.

기본적으로 중앙 관리 서버에는 하나 이상의 관리 중인 기기 그룹이 있습니다. 사용자 지정 그룹을 생성하려는 경우 관리 중인 기기 그룹 내에서 하위 그룹(자식 그룹)으로 생성됩니다.

동일한 애플리케이션의 정책은 관리 그룹의 계층 구조에 따라 서로 작용합니다. 상위(부모) 관리 그룹의 정책에서 잠긴 설정은 하위 그룹의 정책 설정 값을 다시 할당합니다(아래 그림 참조).

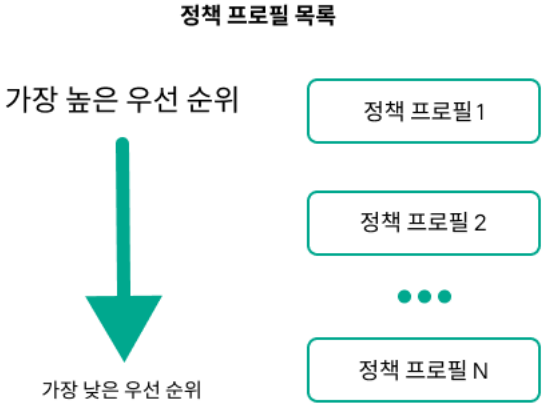


정책 계층 구조

정책 계층 구조의 정책 프로필

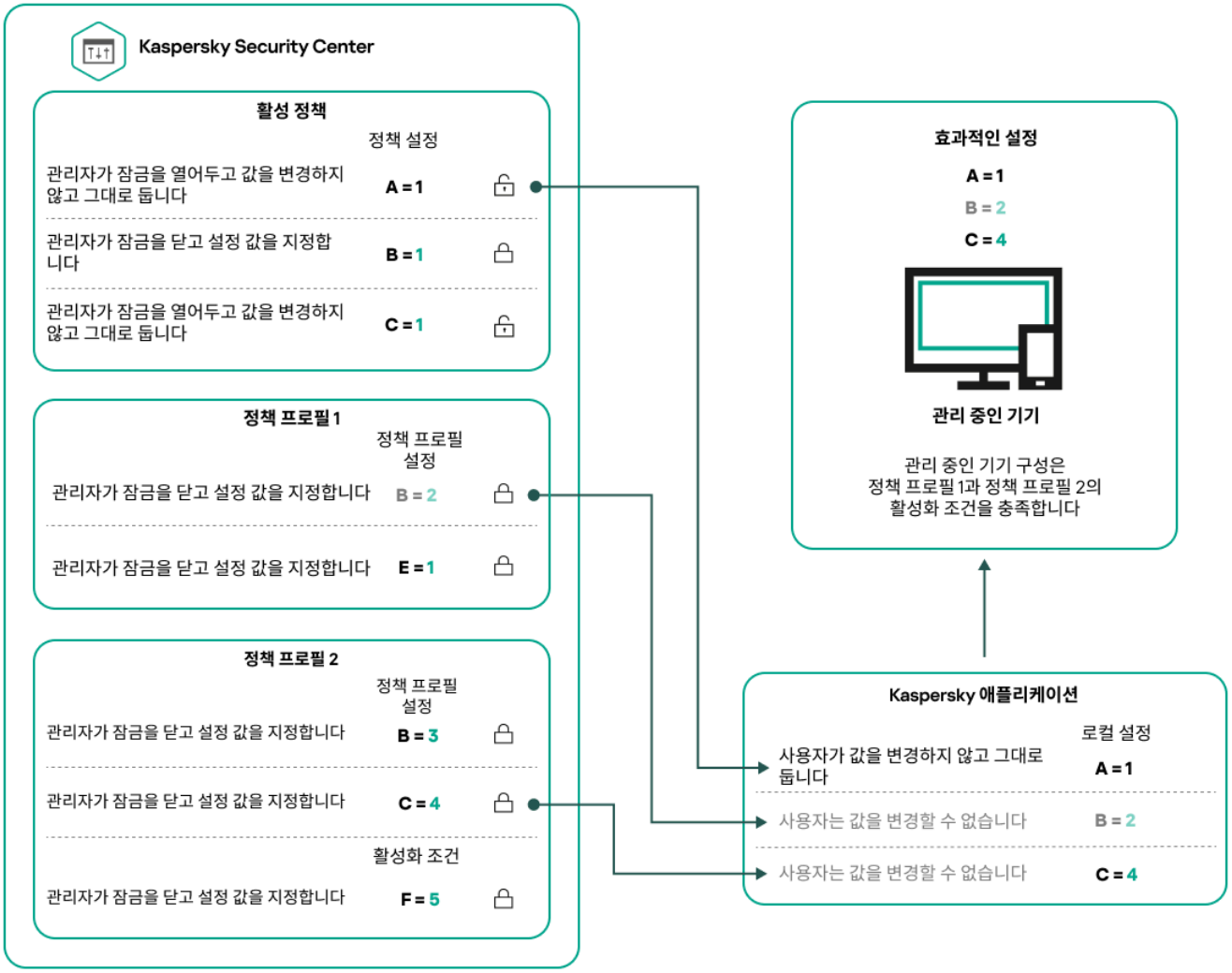
정책 프로필에는 다음과 같은 우선 순위 할당 조건이 있습니다.

- 정책 프로필 목록에서 프로필의 위치는 우선 순위를 나타냅니다. 정책 프로필 우선 순위를 변경할 수 있습니다. 목록에서 가장 높은 위치는 가장 높은 우선 순위를 나타냅니다(아래 그림 참조).



정책 프로필의 우선 순위 정의

- 정책 프로필의 활성화 조건은 서로 의존하지 않습니다. 여러 정책 프로필을 동시에 활성화할 수 있습니다. 여러 정책 프로필이 동일한 설정에 영향을 미치는 경우 기기는 우선 순위가 가장 높은 정책 프로필에서 설정 값을 가져옵니다(아래 그림 참조).

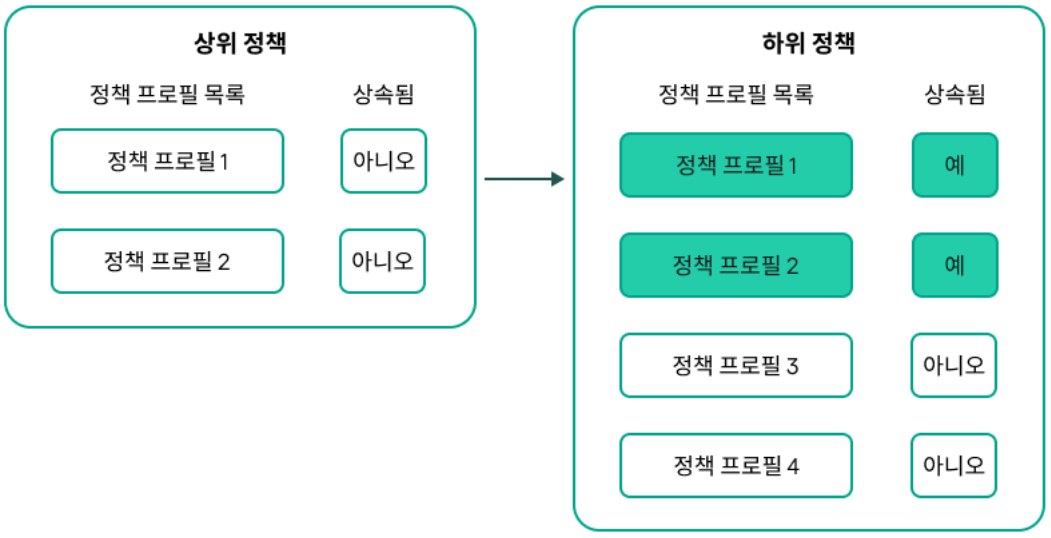


관리 중인 기기 구성은 여러 정책 프로필의 활성화 조건을 충족합니다.

상속 계층 구조의 정책 프로필

다른 계층 구조 수준 정책의 정책 프로필은 다음 조건을 준수합니다.

- 하위 정책은 상위 정책의 정책 프로필을 상속합니다. 상위 정책에서 상속된 정책 프로필은 원래 정책 프로필의 수준보다 높은 우선 순위를 얻습니다.
- 상속된 정책 프로필의 우선 순위는 변경할 수 없습니다(아래 그림 참조).

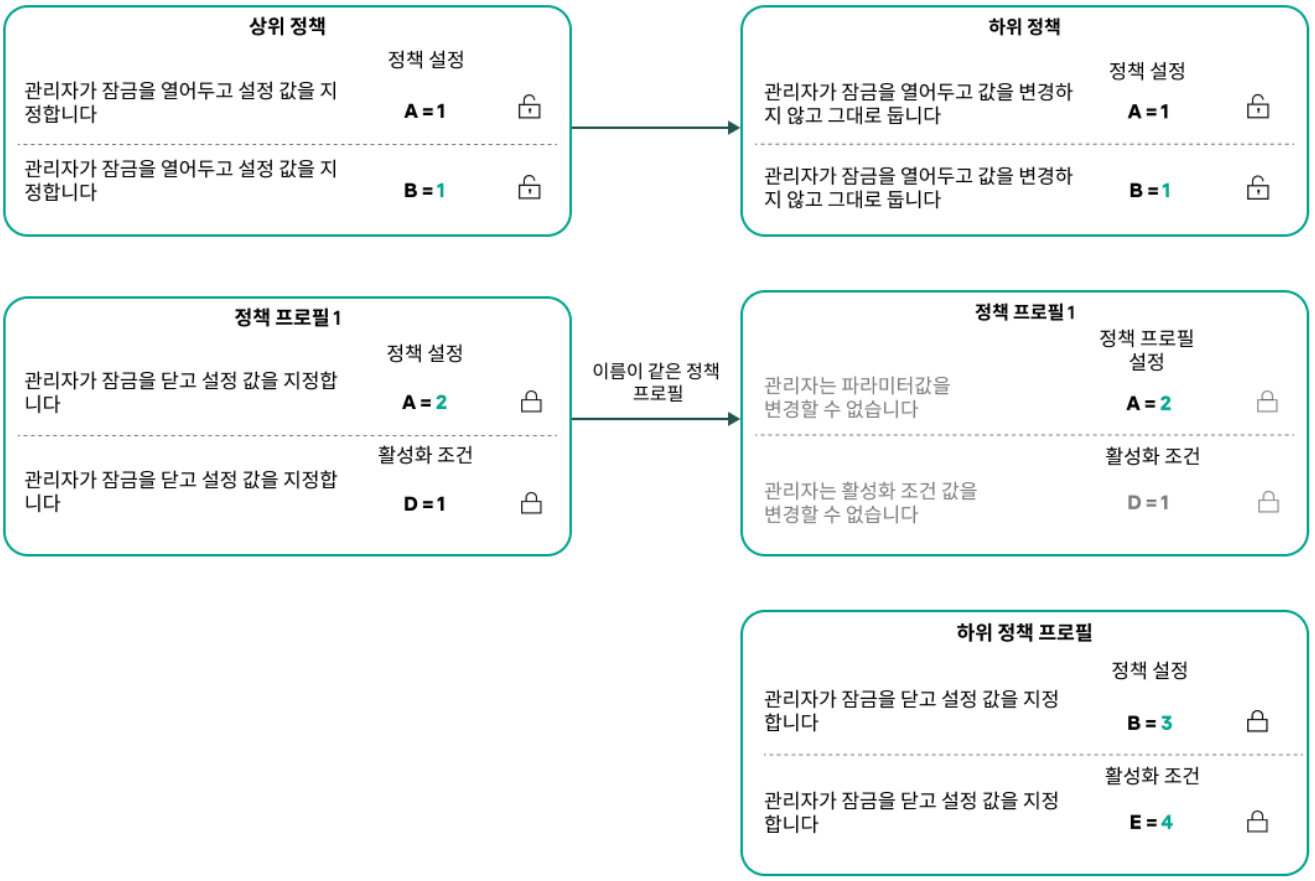


정책 프로필 상속

이름이 같은 정책 프로필

서로 다른 계층 구조 수준에 동일한 이름을 가진 정책이 두 개 있는 경우 이러한 정책은 다음 규칙에 따라 작동합니다.

- 잠긴 설정 및 상위 정책 프로필의 프로필 활성화 조건은 하위 정책 프로필의 설정 및 프로필 활성화 조건을 변경합니다(아래 그림 참조).



자식 프로필은 부모 정책 프로필의 설정 값을 상속합니다.

- 잠금 해제된 설정 및 상위 정책 프로필의 프로필 활성화 조건은 하위 정책 프로필의 설정 및 프로필 활성화 조건을 변경하지 않습니다.

관리 중인 기기에서 설정을 구현하는 방법

관리 중인 기기에서 유효 설정을 구현하는 방법은 다음과 같습니다.

- 잠겨 있지 않은 모든 설정의 값은 정책에서 가져옵니다.
- 그런 다음 관리 애플리케이션 설정 값으로 덮어씁니다.
- 그런 다음 유효 정책의 잠긴 설정 값이 적용됩니다. 잠긴 설정 값은 잠금 해제된 유효 설정 값을 변경합니다.

정책 관리

이 섹션에서는 정책 관리에 대해 설명하고 정책 목록 보기, 정책 만들기, 정책 수정, 정책 복사, 정책 이동, 강제 동기화, 정책 배포 상태 차트 보기 및 정책 삭제에 대한 정보를 제공합니다.

정책 목록 보기

중앙 관리 서버나 관리 그룹용으로 생성된 정책 목록을 확인할 수 있습니다.

정책 목록을 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 그룹 계층 구조**로 이동합니다.
2. 관리 그룹 구조에서 정책 목록을 보려는 관리 그룹을 선택합니다.

   정책 목록이 표 형식으로 표시됩니다. 정책이 없으면 표는 비어 있습니다. 표의 열을 표시 또는 숨기거나, 열 순서를 변경하거나, 지정한 값이 포함된 줄만 표시하거나, 검색을 사용할 수 있습니다.

정책 만들기

정책을 만들 수도 있고 기존 정책을 수정 및 삭제할 수도 있습니다.

정책을 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 정책을 생성할 관리 그룹을 선택합니다:
   - 루트 그룹.
     이 때는 다음 단계로 진행할 수 있습니다.
   - 하위 그룹:
     a. 창 상단에서 현재 경로 링크를 클릭합니다.
     b. 패널이 열리면 필요한 하위 그룹의 이름이 있는 링크를 클릭합니다.

     선택한 하위 그룹에 따라 현재 경로가 변경됩니다.
3. **추가**를 누릅니다.
   애플리케이션 선택 창이 열립니다.
4. 정책을 생성할 애플리케이션을 선택합니다.
5. **다음**을 누릅니다.
   일반 탭이 선택된 상태로 새 정책 설정 창이 열립니다.
6. 원하는 경우 정책의 기본 이름, 기본 상태 및 기본 상속 설정을 변경합니다.
7. **애플리케이션 설정** 탭을 누릅니다.
   또는 **저장**을 누르고 종료할 수도 있습니다. 정책이 정책 목록에 표시되며, 나중에 정책 설정을 편집할 수 있습니다.
8. **애플리케이션 설정** 탭의 왼쪽 창에서 원하는 카테고리를 선택하고 오른쪽의 결과 창에서 정책의 설정을 편집합니다. 각 카테고리(섹션)의 정책 설정을 편집할 수 있습니다.

설정 세트는 정책을 만드는 애플리케이션에 따라 다릅니다. 자세한 내용은 다음을 참조하십시오.

- 중앙 관리 서버 구성
- 네트워크 에이전트 정책 설정
- Kaspersky Endpoint Security for Windows 문서

다른 보안 제품 설정에 대한 자세한 내용은 해당 애플리케이션에 대한 문서를 참조하십시오.
설정을 편집할 때는 **취소**를 눌러 마지막 작업을 취소할 수 있습니다.

9. **저장**을 눌러 정책을 저장합니다.

정책 목록에 정책이 표시됩니다.

정책 수정

정책을 수정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 수정할 정책을 누릅니다.
정책 설정 창이 열립니다.
3. 일반 설정 및 정책을 생성하는 애플리케이션의 설정을 지정합니다. 자세한 내용은 다음을 참조하십시오.
   - 중앙 관리 서버 구성
   - 네트워크 에이전트 정책 설정
   - Kaspersky Endpoint Security for Windows 문서

   다른 보안 제품 설정에 대한 자세한 내용은 해당 애플리케이션에 대한 문서를 참조하십시오.
4. **저장**을 누릅니다.

정책 변경 사항이 정책 속성에 저장되고 **리비전 내역** 섹션에 표시됩니다.

일반 정책 설정

일반

일반 탭에서 정책 상태를 수정하고 정책 설정에 대한 상속을 지정할 수 있습니다.

- **정책 상태** 차단에서 정책 모드 중 하나를 선택할 수 있습니다:
  - **액티브**

    이 옵션을 선택하면 정책이 활성화됩니다.

기본적으로 이 옵션은 선택되어 있습니다.

- **이동 사용자**

  이 옵션을 선택하면 기기가 회사 네트워크를 벗어나는 경우 정책이 활성화됩니다.

- **비활성**

  이 옵션을 선택하면 정책이 비활성화되지만 **정책** 폴더에는 계속 저장되어 있습니다. 필요한 경우 정책을 활성화할 수 있습니다.

- **설정 상속** 설정 그룹에서는 정책 상속을 구성할 수 있습니다:

  - **부모 정책의 설정 상속**

    이 옵션을 활성화하면 상위 그룹 정책에서 정책 설정 값이 상속되므로 이 값이 잠깁니다.
    기본적으로 이 옵션은 켜져 있습니다.

  - **자식 정책에 설정 강제 상속**

    이 옵션을 활성화하면 정책 변경 사항이 적용된 후 다음 작업이 수행됩니다.
    - 정책 설정의 값이 관리 하위 그룹의 정책, 즉 자식 정책에 배포됩니다.
    - 각 자식 정책의 속성 창에 있는 **일반** 섹션의 **설정 상속** 블록에서 **부모 정책의 설정 상속** 옵션은 자동으로 활성화됩니다.

    이 옵션을 활성화하면 자식 정책 설정이 잠깁니다.
    기본적으로 이 옵션은 비활성화되어 있습니다.

이벤트 구성

이벤트 구성 탭에서는 이벤트 기록과 이벤트 알림을 구성할 수 있습니다. 이벤트는 심각도 레벨에 따라 다음 탭에 배포됩니다:

- **심각**

  심각 섹션은 네트워크 에이전트 정책 속성에 표시되지 않습니다.

- **기능 실패**
- **경고**
- **정보**

각 섹션에서 목록에는 이벤트 유형 및 중앙 관리 서버에 기본 이벤트가 저장되는 기간(일)이 표시됩니다. 이벤트 유형을 누르면 다음 설정을 지정할 수 있습니다.

- **이벤트 등록**

이벤트를 저장할 기간(일)을 지정하고 이벤트 저장 위치를 선택할 수 있습니다.

- **Syslog를 사용해 SIEM 시스템으로 내보내기**
- **기기의 OS 이벤트 로그에 저장**
- **중앙 관리 서버의 OS 이벤트 로그에 저장**

- **이벤트 알림**
  다음 방식 중 하나로 이벤트 관련 알림을 받을지 여부를 선택할 수 있습니다.
  - **이메일로 알림**
  - **SMS로 알림**
  - **실행 파일 또는 스크립트를 실행하여 알림**
  - **SNMP로 알림**

  기본적으로 중앙 관리 서버 속성 탭에서 지정한 받는 사람 주소 등의 알림 설정이 사용됩니다. 원하는 경우 **이메일**, **SMS** 및 **실행되는 실행 파일** 탭에서 이러한 설정을 변경할 수 있습니다.

리비전 내역

리비전 내역 탭에서는 정책 리비전 목록을 확인하고 필요한 경우 정책 변경 사항을 롤백할 수 있습니다.

정책 상속 옵션 활성화 및 비활성화

정책에서 상속 옵션을 활성화 또는 비활성화하려면 다음 단계를 따릅니다.

1. 필요한 정책을 엽니다.
2. **일반** 탭을 엽니다.
3. 정책 상속을 활성화 또는 비활성화합니다.
   - 자식 정책에 대해 **부모 정책의 설정 상속**을 활성화하고 관리자가 부모 정책에서 일부 설정을 잠금 상태로 설정하면 자식 정책에서 해당 설정을 변경할 수 없습니다.
   - 자식 정책에 대해 **부모 정책의 설정 상속**을 비활성화하면 부모 정책에서 일부 설정이 잠금 상태이더라도 자식 그룹의 모든 설정을 변경할 수 있습니다.
   - 부모 그룹에서 **자식 정책에 설정 강제 상속**을 활성화하면 각 자식 정책에 대한 **부모 정책의 설정 상속** 옵션이 활성화됩니다. 이 경우에는 모든 자식 정책에 대해 이 옵션을 비활성화할 수 없습니다. 부모 정책에서 잠겨 있는 모든 설정이 자식 그룹에서 강제로 상속되며 자식 그룹에서 이러한 설정을 변경할 수 없습니다.
4. **저장** 버튼을 눌러 변경 사항을 저장하거나 **취소** 버튼을 눌러 변경 사항을 거부합니다.

기본적으로 **부모 정책의 설정 상속** 옵션은 새 정책에 대해 활성화되어 있습니다.

정책에 프로필이 있으면 모든 자식 정책이 해당 프로필을 상속합니다.

정책 복사

관리 그룹 간에 정책을 복사할 수 있습니다.

다른 관리 그룹으로 정책을 복사하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 복사하려는 정책(여러 정책 선택 가능) 옆에 있는 확인란을 선택합니다.
3. **복사** 버튼을 누릅니다.
   화면 오른쪽에 관리 그룹 트리가 나타납니다.
4. 트리에서 대상 그룹(해당 정책 또는 여러 정책을 복사하려는 그룹)을 선택합니다.
5. 화면 아래쪽의 **복사** 버튼을 누릅니다.
6. **확인**을 눌러 동작을 허용합니다.

정책이 모든 프로필과 함께 대상 그룹에 복사됩니다. 대상 그룹의 복사된 각 정책 상태는 **비활성**가 됩니다. 언제든지 상태를 **액티브**으로 변경할 수 있습니다.

새로 이동한 정책과 이름이 동일한 정책이 이미 대상 그룹에 있는 경우 가져온 정책의 이름에 (<순차적 번호>) 색인이 추가됩니다. 예: (1).

정책 이동

관리 그룹 간에 정책을 이동할 수 있습니다. 그룹은 삭제하되 해당 정책은 다른 그룹에 사용하려는 경우를 예로 들 수 있습니다. 이 경우 이전 그룹에서 새 그룹으로 정책을 이동한 후에 이전 그룹을 삭제하고 싶을 수 있습니다.

> 정책을 다른 관리 그룹으로 이동하면 해당 정책의 리비전 기록이 삭제됩니다. **리비전 내역** 탭에는 가장 최근 변경 사항에 대한 정보만 표시됩니다.

다른 관리 그룹으로 정책을 이동하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 이동하려는 정책(여러 정책 선택 가능) 옆에 있는 확인란을 선택합니다.
3. **이동** 버튼을 누릅니다.
   화면 오른쪽에 관리 그룹 트리가 나타납니다.
4. 트리에서 대상 그룹(해당 정책 또는 여러 정책을 이동하려는 그룹)을 선택합니다.
5. 화면 아래쪽의 **이동** 버튼을 누릅니다.
6. **확인**을 눌러 동작을 허용합니다.

소스 그룹에서 상속되지 않는 정책은 모든 프로필과 함께 대상 그룹으로 이동됩니다. 대상 그룹의 정책 상태는 **비활성**입니다. 언제든지 상태를 **액티브**으로 변경할 수 있습니다.

소스 그룹에서 상속되는 정책은 소스 그룹에 유지됩니다. 이 정책은 모든 프로필과 함께 대상 그룹에 복사됩니다. 대상 그룹의 정책 상태는 **비활성**입니다. 언제든지 상태를 **액티브**으로 변경할 수 있습니다.

새로 이동한 정책과 이름이 동일한 정책이 이미 대상 그룹에 있는 경우 가져온 정책의 이름에 (<순차적 번호>) 색인이 추가됩니다. 예: (1).

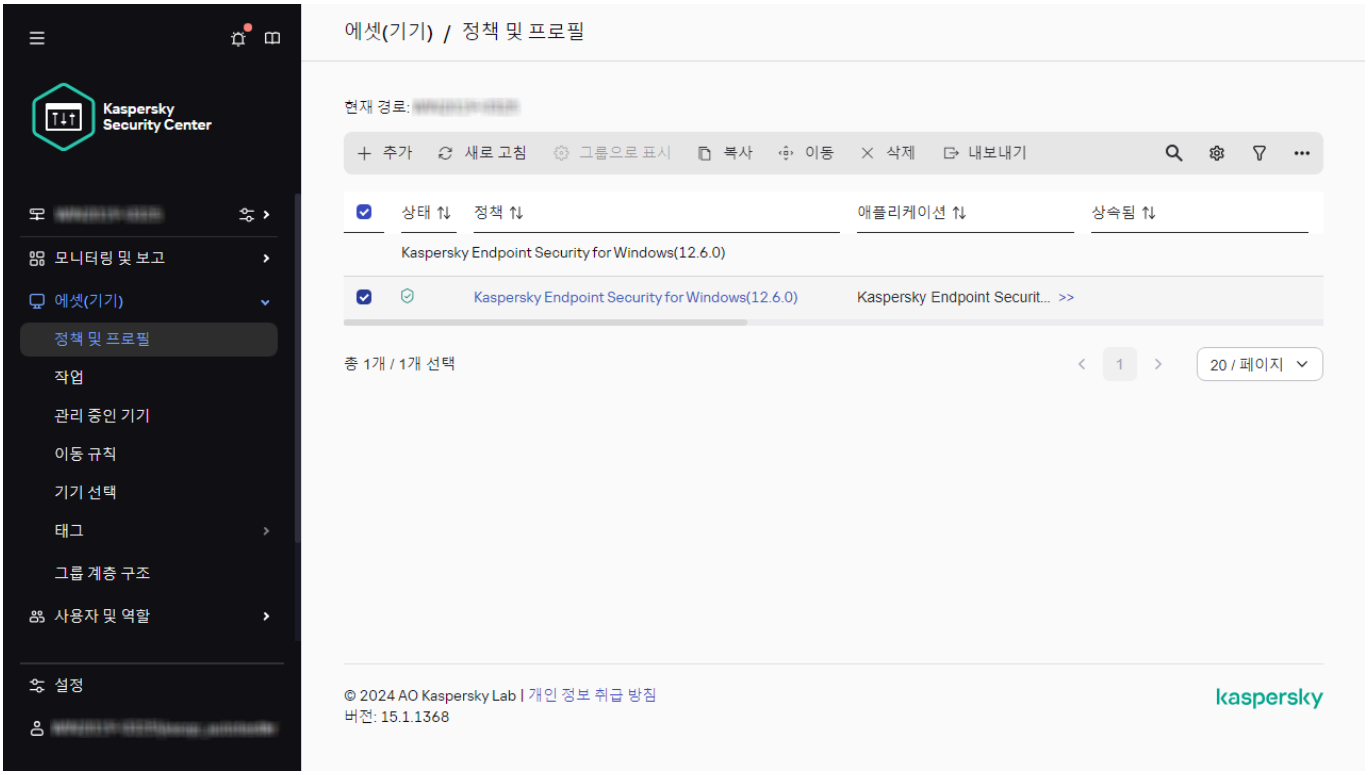
정책 내보내기

Kaspersky Security Center를 사용하면 정책, 정책 설정, 정책 프로필을 KLP 파일에 저장할 수 있습니다. 이 KLP 파일을 사용하여 Kaspersky Security Center Windows 및 Kaspersky Security Center Linux로 저장된 정책을 가져올 수 있습니다.

정책을 내보내려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기)** → **정책 및 프로필**로 이동합니다.
2. 내보내려는 정책 옆에 있는 확인란을 선택합니다.

   동시에 여러 정책을 내보낼 수는 없습니다. 둘 이상의 정책을 선택하면 **내보내기** 버튼이 비활성화됩니다.



3. **내보내기** 버튼을 클릭합니다.
4. **다른 이름으로 저장** 창이 열리면 정책 파일의 이름과 경로를 지정합니다. **저장** 버튼을 클릭합니다.

   다른 이름으로 저장 창은 Google Chrome, Microsoft Edge, Opera를 사용 시에만 표시됩니다. 다른 브라우저 사용 시, 정책 파일이 **다운로드** 폴더에 자동으로 저장됩니다.

정책 가져오기

Kaspersky Security Center를 사용하면 KLP 파일에서 정책을 가져올 수 있습니다. KLP 파일에는 내보낸 정책, 정책 설정 및 정책 프로필이 포함되어 있습니다.

정책을 가져오려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. **가져오기** 버튼을 클릭합니다.
3. 가져오려는 정책 파일을 선택하려면 **찾기** 버튼을 클릭합니다.
4. 열린 창에서 KLP 정책 파일의 경로를 지정한 후 **열기** 버튼을 클릭합니다. 정책 파일은 하나만 선택할 수 있습니다.
   정책 처리가 시작됩니다.
5. 정책을 성공적으로 처리한 후 정책을 적용할 관리 그룹을 선택합니다.
6. **완료** 버튼을 눌러 정책 가져오기를 완료합니다.

가져오기 결과가 포함된 알림이 표시됩니다. 정책을 성공적으로 가져오면 **자세히** 링크를 클릭하여 정책 속성을 볼 수 있습니다.

가져오기에 성공하면 정책이 정책 목록에 표시됩니다. 정책의 설정 및 프로필도 가져옵니다. 내보내기 중에 선택한 정책 상태에 관계없이 가져온 정책은 비활성 상태입니다. 정책 속성에서 정책 상태를 변경할 수 있습니다.

새로 가져온 정책의 이름이 기존 정책과 같다면, 가져온 정책의 이름은 **(<다음 시퀀스 번호>)** 인덱스로 확장됩니다(예: **(1)**, **(2)**).

정책 배포 상태 차트 보기

Kaspersky Security Center의 정책 배포 상태 차트에서 각 기기의 정책 적용 상태를 볼 수 있습니다.

각 기기에서 정책 배포 상태를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 기기의 배포 상태를 보려는 정책 이름 옆에 있는 확인란을 선택합니다.
3. 표시되는 메뉴에서 **배포** 링크를 선택합니다.
   <정책 이름> 배포 결과 창이 열립니다.
4. 열리는 **<정책 이름> 배포 결과** 창에 정책의 **상태 설명**이 표시됩니다.

정책 배포 결과와 함께 목록에 표시되는 결과의 수를 변경할 수 있습니다. 기본 기기 수는 100000개입니다.

정책 배포 결과와 함께 목록에 표시되는 기기 수를 변경하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 계정 설정으로 이동하여 **인터페이스 옵션**을 선택합니다.
2. **정책 배포 결과에 표시되는 기기 수 제한**에 기기 수를 입력합니다(최대 100000개).
   기본적으로 이 숫자는 5000으로 설정되어 있습니다.
3. **저장**을 누릅니다.
   설정이 저장 및 적용됩니다.

정책 삭제

더 이상 필요하지 않은 정책은 삭제할 수 있습니다. 지정한 관리 그룹에서 상속되지 않는 정책만 삭제할 수 있습니다. 상속되는 정책은 해당 정책의 생성 대상 상위 그룹에서만 삭제할 수 있습니다.

정책을 삭제하려면:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 삭제할 정책 옆의 확인란을 선택하고 **삭제**를 누릅니다.
   상속된 정책을 선택하면 **삭제** 버튼이 흐리게 표시되어 사용할 수 없는 상태가 됩니다.
3. **확인**을 눌러 동작을 허용합니다.

정책이 모든 프로필과 함께 삭제됩니다.

정책 프로필 관리

이 섹션에서는 정책 프로필 관리에 대해 설명하고 정책 프로필 보기, 정책 프로필 우선 순위 변경, 정책 프로필 만들기, 정책 프로필 수정, 정책 프로필 복사, 정책 프로필 활성화 규칙 만들기 및 정책 프로필 삭제에 대해 설명합니다.

정책 프로필 보기

정책의 프로필을 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 프로필을 보려는 정책의 이름을 누릅니다.
   일반 탭이 선택된 상태로 정책 속성 창이 열립니다.
3. **정책 프로필** 탭을 엽니다.

정책 프로필 목록이 테이블 형태로 나타납니다. 정책에 프로필이 없으면 빈 표가 나타납니다.

정책 프로필 우선 순위 변경

정책 프로필 우선 순위를 변경하려면 다음 단계를 따릅니다.

1. 원하는 정책의 프로필 목록으로 이동합니다.
   정책 프로필 목록이 나타납니다.
2. **정책 프로필** 탭에서 우선 순위를 변경할 정책 프로필 옆의 확인란을 선택합니다.

3. **우선 순위 지정** 또는 **우선 순위 해제**를 눌러 목록에서 정책 프로필의 새 위치를 설정합니다.
   목록에서 위쪽에 있는 정책 프로필일수록 우선 순위가 높습니다.

4. **저장** 버튼을 누릅니다.

선택한 정책 프로필의 우선 순위가 변경되어 적용됩니다.

정책 프로필 만들기

정책 프로필을 만들려면 다음과 같이 하십시오:

1. 원하는 정책의 프로필 목록으로 이동합니다.
   정책 프로필 목록이 나타납니다. 정책에 프로필이 없으면 빈 표가 나타납니다.

2. **추가**를 누릅니다.

3. 원하는 경우 프로필의 기본 이름 및 기본 상속 설정을 변경합니다.

4. **애플리케이션 설정** 탭을 누릅니다.
   또는 **저장**을 누르고 종료할 수도 있습니다. 생성한 프로필이 정책 프로필 목록에 나타나며, 나중에 프로필 설정을 편집할 수 있습니다.

5. **애플리케이션 설정** 탭의 왼쪽 창에서 원하는 카테고리를 선택하고 오른쪽의 결과 창에서 프로필 설정을 편집합니다. 각 카테고리(섹션)의 정책 프로필 설정을 편집할 수 있습니다.
   설정을 편집할 때는 **취소**를 눌러 마지막 작업을 취소할 수 있습니다.

6. **저장**을 눌러 프로필을 저장합니다.

프로필이 정책 프로필 목록에 표시됩니다.

정책 프로필 수정

Kaspersky Endpoint Security for Windows의 정책에 대해서만 정책 프로필을 편집할 수 있습니다.

정책 프로필을 수정하려면 다음과 같이 하십시오:

1. 원하는 정책의 프로필 목록으로 이동합니다.
   정책 프로필 목록이 나타납니다.

2. **정책 프로필** 탭에서 수정할 정책 프로필을 누릅니다.
   정책 프로필 속성 창이 열립니다.

3. 속성 창에서 프로필 구성:

   - 필요한 경우 **일반** 탭에서 프로필 이름을 변경하고 프로필을 활성화하거나 비활성화합니다.
   - 프로필 활성화 규칙을 편집합니다.
   - 애플리케이션 설정을 편집합니다.

   보안 제품의 설정 관련 세부 정보는 해당 애플리케이션의 설명서를 참조하십시오.

4. **저장**을 누릅니다.

수정한 설정은 기기가 중앙 관리 서버와 동기화되거나(정책 프로필이 활성 상태인 경우) 활성화 규칙을 만족해 시작한 이후에(정책 프로필이 비활성 상태인 경우)에 적용됩니다.

정책 프로필 복사

서로 다른 정책에 동일한 프로필을 적용하려는 등의 경우 현재 정책이나 다른 정책에 정책 프로필을 복사할 수 있습니다. 몇 가지 설정만 다른 프로필을 두 개 이상 적용하려는 경우에도 복사를 사용할 수 있습니다.

정책 프로필을 복사하려면 다음 단계를 따릅니다.

1. 원하는 정책의 프로필 목록으로 이동합니다.
   정책 프로필 목록이 나타납니다. 정책에 프로필이 없으면 빈 표가 나타납니다.
2. **정책 프로필** 탭에서 복사할 정책 프로필을 선택합니다.
3. **복사**를 클릭합니다.
4. 창이 열리면 프로필을 복사하려는 정책을 선택합니다.
   같은 정책이나 지정한 정책에 정책 프로필을 복사할 수 있습니다.
5. **복사**를 클릭합니다.

   정책 프로필이 선택한 정책에 복사됩니다. 새로 복사된 프로필에는 가장 낮은 우선 순위가 지정됩니다. 같은 정책에 프로필을 복사하면 새로 복사된 프로필의 이름은 () 색인이 추가되어 확장됩니다. 예: (1), (2).

나중에 프로필의 이름과 우선 순위를 비롯한 프로필 설정을 변경할 수 있습니다. 이 경우 원래 정책 프로필은 변경되지 않습니다.

정책 프로필 활성화 규칙 만들기

정책 프로필 활성화 규칙을 만들려면 다음과 같이 하십시오:

1. 원하는 정책의 프로필 목록으로 이동합니다.
   정책 프로필 목록이 나타납니다.
2. **정책 프로필** 탭에서 활성화 규칙을 생성해야 하는 정책 프로필을 누릅니다.
   정책 프로필 목록이 비어 있으면 정책 프로필을 만들 수 있습니다.

3. **활성화 규칙** 탭에서 **추가** 버튼을 누릅니다.
   정책 프로필 활성화 규칙이 있는 창이 열립니다.

4. 규칙의 이름을 지정합니다.

5. 만들려는 정책 프로필을 활성화하려면 충족해야 하는 조건 옆의 확인란을 선택합니다.

- **정책 프로필 활성화에 대한 일반 규칙**

  기기 오프라인 모드의 상태, 중앙 관리 서버 연결을 위한 규칙 및 기기에 할당된 태그에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다.

  이 옵션에 대해 다음 단계에서 아래 정보를 지정합니다.

  - **기기 상태**

    네트워크의 기기 유무에 대한 조건을 정의합니다.
    - **온라인** - 기기가 네트워크에 있어 중앙 관리 서버를 사용할 수 있습니다.
    - **오프라인** - 기기가 외부 네트워크에 있어 중앙 관리 서버를 사용할 수 없습니다.
    - **N/A** - 기준이 적용되지 않습니다.

  - **중앙 관리 서버 연결을 위한 규칙이 이 기기에서 활성화됨**

    정책 프로필 활성화 조건(규칙 실행 여부)과 규칙 이름을 선택합니다.
    이 규칙은 중앙 관리 서버 연결을 위한 기기의 네트워크 위치를 정의합니다. 해당 조건이 충족되거나 충족되지 않아야 정책 프로필이 활성됩니다.
    중앙 관리 서버 연결을 위한 기기의 네트워크 위치 설명은 네트워크 에이전트 전환 규칙에서 만들거나 구성할 수 있습니다.

- **특정 기기 소유자에 대한 규칙**
  이 옵션에 대해 다음 단계에서 아래 정보를 지정합니다.

  - **기기 소유자**

    이 옵션을 사용해 기기 소유자에 따라 기기에 대한 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

    - 기기는 지정한 소유자의 것입니다("=" 기호).
    - 기기는 지정한 소유자의 것이 아닙니다("#" 기호).
      이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. 옵션이 활성화되면 기기 소유자를 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **기기 소유자는 내부 보안 그룹에 포함되어 있습니다**

  이 옵션을 사용해 Kaspersky Security Center 내부 보안 그룹의 소유자에 따라 기기에 대한 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

  - 기기 소유자는 지정된 보안 그룹의 구성원입니다("=" 기호).
  - 기기 소유자는 지정된 보안 그룹의 구성원이 아닙니다("#" 기호).

    이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. Kaspersky Security Center의 보안 그룹을 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **하드웨어 사양에 대한 규칙**

  메모리의 크기와 논리 프로세서 수에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다.

  이 옵션에 대해 다음 단계에서 아래 정보를 지정합니다.

  - **RAM 크기(MB)**

    이 옵션을 사용해 기기의 이용 가능한 RAM 크기에 따라 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

    - 기기 RAM 크기가 지정된 값보다 작습니다("<" 기호).
    - 기기 RAM 크기가 지정된 값보다 큽니다(">" 기호).

    이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. 기기의 RAM 볼륨을 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

  - **논리 프로세서 개수**

    이 옵션을 사용해 기기의 논리 프로세서의 개수에 따라 프로필 활성화 규칙을 구성하고 활성화할 수 있습니다. 이 확인란 아래의 드롭다운 목록에서 프로필 활성화를 위한 기준을 선택할 수 있습니다.

    - 기기의 논리 프로세서의 개수는 지정한 값보다 작거나 같습니다("<" 기호).
    - 기기의 논리 프로세서의 개수는 지정한 값보다 크거나 같습니다(">" 기호).

    이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다. 기기의 논리 프로세서 수를 지정할 수 있습니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

- **역할 할당을 위한 규칙**

  이 옵션에 대해 다음 단계에서 아래 정보를 지정합니다.

  기기 소유자의 특정 역할에 따라 정책 프로필 활성화

  소유자의 역할에 따라 기기에 대한 프로필 활성화 규칙을 구성하고 활성하려면 이 옵션을 선택합니다. 역할은 기존 역할 목록에서 수동으로 추가합니다.

이 옵션을 활성화하면 구성된 기준에 따라 기기에서 프로필이 활성됩니다.

- **태그 사용에 대한 규칙**

  기기에 할당된 태그에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다. 선택한 태그가 있는 기기나 없는 기기에 대해 정책 프로필을 활성화할 수 있습니다.

  이 옵션에 대해 다음 단계에서 아래 정보를 지정합니다.

  - **태그**

    태그 목록에서 관련 태그 옆의 확인란을 선택하여 정책 프로필에 기기를 포함하는 규칙을 지정할 수 있습니다.

    목록에서 필드에 태그를 입력하고 **추가** 버튼을 눌러 새 태그를 목록에 추가할 수 있습니다.

    정책 프로필에는 설명에 선택한 태그가 모두 들어 있는 기기가 포함됩니다. 확인란이 비어 있으면 기준이 적용되지 않습니다. 기본적으로 이 확인란은 선택되어 있지 않습니다.

  - **지정한 태그가 없는 기기에 적용**

    선택한 태그를 반대로 적용해야 하는 경우 이 옵션을 선택합니다.

    이 옵션을 사용하면 정책 프로필에는 설명에 선택한 태그가 하나도 없는 기기가 포함됩니다. 이 옵션을 비활성화하면 기준이 적용되지 않습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- **Active Directory 이용에 대한 규칙**

  Active Directory OU(조직 구성 단위) 유무 또는 기기나 해당 소유자의 Active Directory 보안 그룹 구성원 자격에 따라 기기에서 정책 프로필 활성화 규칙을 설정하려면 이 확인란을 선택합니다.

  이 옵션에 대해 다음 단계에서 아래 정보를 지정합니다.

  - **Active Directory 보안 그룹에 소속된 기기 소유자의 멤버십**

    이 옵션을 사용하면 소유자가 지정한 보안 그룹의 구성원인 기기에서 정책 프로필이 활성화됩니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

  - **Active Directory 보안 그룹의 기기 구성원**

    이 옵션을 사용하면 기기에서 정책 프로필이 활성화됩니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

  - **Active Directory 조직 구성 단위의 기기 할당**

    이 옵션을 사용하면 지정한 Active Directory 조직 단위(OU)에 포함된 기기에서 정책 프로필이 활성화됩니다. 이 옵션이 비활성화되면 프로필 활성화 기준이 적용되지 않습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

마법사에서 추가로 표시되는 페이지의 수는 첫 번째 단계에서 선택하는 설정에 따라 달라집니다. 정책 프로필 활성화 규칙은 나중에 수정할 수 있습니다.

6. 구성된 파라미터 목록을 확인합니다. 목록이 정확하면 **생성**을 누릅니다.

그러면 프로필이 저장됩니다. 활성화 규칙이 실행되면 해당 프로필이 기기에서 활성화됩니다.

프로필용으로 만든 정책 활성화 규칙은 **활성화 규칙** 탭의 정책 프로필 속성에 표시됩니다. 모든 정책 프로필 활성화 규칙은 수정하거나 제거할 수 있습니다.

여러 활성화 규칙을 동시에 실행할 수 있습니다.

정책 프로필 삭제

정책 프로필을 삭제하려면 다음 단계를 따릅니다.

1. 원하는 정책의 프로필 목록으로 이동합니다.
   정책 프로필 목록이 나타납니다.

2. **정책 프로필** 탭에서 삭제할 정책 프로필 옆의 확인란을 선택하고 **삭제**를 누릅니다.

3. 창이 열리면 **삭제**를 누릅니다.

정책 프로필이 삭제됩니다. 정책이 하위 레벨 그룹에서 상속될 시, 프로필이 해당 그룹에 유지되지만 해당 그룹의 정책 프로필이 됩니다. 이는 하위 레벨 그룹의 기기에 설치된 관리 중인 애플리케이션의 설정이 크게 변경되지 않도록 하기 위한 것입니다.

데이터 암호화 및 보호

데이터 암호화는 노트북 또는 하드 드라이브를 도난 또는 분실했을 때, 혹은 승인되지 않은 사용자와 애플리케이션에서 접근할 때 원치 않는 유출 위험을 줄여줍니다.

암호화를 지원하는 Kaspersky 애플리케이션은 다음과 같습니다:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

사용자 인터페이스 설정을 사용하여 암호화 관리 기능과 관련된 인터페이스 구성 요소 중 일부를 표시하거나 숨길 수 있습니다.

VDI에서는 암호화를 활성화하지 않는 것이 좋습니다.

Kaspersky Endpoint Security for Windows의 데이터 암호화

다음 유형의 암호화를 관리할 수 있습니다:

- 서버용 Windows 운영 체제를 실행하는 기기의 BitLocker 드라이브 암호화
- 워크스테이션용 Windows 운영 체제를 실행하는 기기의 Kaspersky 디스크 암호화

Kaspersky Endpoint Security for Windows의 이러한 구성 요소를 사용하여 예를 들어 암호화를 활성화 또는 비활성화하거나, 암호화된 드라이브 목록을 보거나, 암호화에 대한 리포트를 생성하고 볼 수 있습니다.

Kaspersky Security Center에서 Kaspersky Endpoint Security for Windows 정책을 정의하여 암호화를 구성합니다. Kaspersky Endpoint Security for Windows는 활성 정책에 따라 암호화 및 복호화를 수행합니다. 규칙 구성 방법 및 암호화 기능에 대한 자세한 설명은 Kaspersky Endpoint Security for Windows 도움말을 참조하십시오.

Kaspersky Endpoint Security for Mac에서 데이터 암호화

macOS를 실행하는 기기에서는 FileVault 암호화를 사용할 수 있습니다. Kaspersky Endpoint Security for Mac을 사용하는 동안 이 암호화를 활성화 또는 비활성화할 수 있습니다.

Kaspersky Security Center에서 Kaspersky Endpoint Security for Mac의 정책을 정의하여 암호화를 구성합니다. Kaspersky Endpoint Security for Mac은 활성 정책에 따라 암호화 및 복호화를 수행합니다. 암호화 기능에 대한 자세한 설명은 Kaspersky Endpoint Security for Mac 온라인 도움말을 참조하십시오.

암호화된 드라이브 목록 보기

Kaspersky Security Center에서 암호화된 드라이브 및 드라이브 수준에서 암호화된 기기에 대한 세부 정보를 볼 수 있습니다. 기기의 정보가 복호화된 후 드라이브는 목록에서 자동으로 제거됩니다.

암호화된 드라이브 목록을 보려면 다음 단계를 따릅니다.

메인 메뉴에서 **동작 → 데이터 암호화 및 보호 → 암호화된 드라이브**로 이동합니다.

섹션이 메뉴에 없으면 숨겨져 있다는 뜻입니다. 사용자 인터페이스 설정에서 **데이터 암호화 및 보호 표시** 옵션을 활성화하여 섹션을 표시합니다.

암호화된 드라이브 목록을 CSV 또는 TXT 파일로 내보낼 수 있습니다. 이렇게 하려면 **CSV로 내보내기** 또는 **TXT로 내보내기** 버튼을 클릭합니다.

암호화 이벤트 목록 보기

기기에서 데이터 암호화 또는 복호화 작업을 실행할 때 Kaspersky Endpoint Security for Windows는 Kaspersky Security Center에 다음과 같은 유형의 이벤트 정보를 전송합니다.

- 디스크 여유 공간이 부족하여 파일을 암호화 또는 복호화하거나 암호화된 압축 파일을 만들 수 없습니다.
- 라이센스 문제로 파일을 암호화 또는 복호화하거나 암호화된 압축 파일을 만들 수 없습니다.
- 접근 권한이 없어 파일을 암호화 또는 복호화하거나 암호화된 압축 파일을 만들 수 없습니다.

- 애플리케이션이 암호화된 파일에 접근 금지됨.
- 알 수 없는 오류.

기기의 데이터를 암호화할 때 발생한 이벤트 목록을 보려면,

메인 메뉴에서 **동작 → 데이터 암호화 및 보호 → 암호화 이벤트**로 이동합니다.

섹션이 메뉴에 없으면 숨겨져 있다는 뜻입니다. 사용자 인터페이스 설정에서 **데이터 암호화 및 보호 표시** 옵션을 활성화하여 섹션을 표시합니다.

암호화된 드라이브 목록을 CSV 또는 TXT 파일로 내보낼 수 있습니다. 이렇게 하려면 **CSV로 내보내기** 또는 **TXT로 내보내기** 버튼을 클릭합니다.

또는 모든 관리 중인 기기에 대한 암호화 이벤트 목록을 검토할 수 있습니다.

관리 중인 기기의 암호화 이벤트를 보려면:

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
2. 관리 중인 기기의 이름을 클릭합니다.
3. **일반** 탭에서 **보호** 섹션으로 갑니다.
4. **데이터 암호화 오류 보기** 링크를 클릭합니다.

암호화 리포트 만들기 및 보기

만들 수 있는 리포트는 다음과 같습니다.

- 관리 중인 기기의 암호화 상태 리포트. 이 리포트는 다양한 관리 중인 기기의 데이터 암호화에 대한 세부 정보를 제공합니다. 예를 들어 리포트에는 구성된 암호화 규칙이 있는 정책을 적용하는 기기 수가 표시됩니다. 또한 예를 들어 재부팅해야 하는 기기 수를 확인할 수 있습니다. 이 보고서에는 모든 기기의 암호화 기술 및 알고리즘에 대한 정보도 포함되어 있습니다.
- 대용량 스토리지 기기의 암호화 상태 리포트. 이 보고서에는 관리 중인 기기의 암호화 상태에 대한 보고서와 유사한 정보가 포함되어 있지만 대용량 저장 기기 및 이동식 드라이브에 대한 데이터만 제공합니다.
- 암호화된 드라이브로의 접근에 대한 권한 리포트. 이 보고서는 암호화된 드라이브에 액세스할 수 있는 사용자 계정을 보여줍니다.
- 파일 암호화 오류 리포트. 이 리포트에는 기기 데이터 암호화 또는 복호화 작업 실행 시 발생한 오류 정보가 담겨 있습니다.
- 암호화된 파일로의 접근 차단 리포트. 이 리포트에는 암호화된 파일로의 애플리케이션 접근 차단 관련 정보가 포함됩니다. 이 리포트는 권한이 없는 사용자나 애플리케이션이 암호화된 파일이나 드라이브에 액세스를 시도할 때 유용합니다.

모니터링 및 보고 → 리포트 섹션에서 리포트를 생성할 수 있습니다. 또는, **동작 → 데이터 암호화 및 보호** 섹션에서 다음 암호화 리포트를 생성할 수 있습니다.

- 대용량 스토리지 기기의 암호화 상태 리포트
- 암호화된 드라이브로의 접근에 대한 권한 리포트
- 파일 암호화 오류 리포트

***데이터 암호화 및 보호** 섹션에서 암호화 리포트를 생성하려면:*

1. 인터페이스 옵션에서 **데이터 암호화 및 보호 표시** 옵션을 활성화했는지 확인합니다.
2. 정책 속성에서 **이벤트 구성** 탭을 엽니다.
3. **심각** 섹션에서 **이벤트 추가**를 클릭하고 *파일 암호화/복호화 규칙 적용 오류* 이벤트 옆에 있는 확인란을 선택합니다.
4. **확인**을 클릭합니다.
5. 메인 메뉴에서 **동작 → 데이터 암호화 및 보호**로 이동합니다.
6. 다음 섹션 중 하나를 엽니다:
   - **암호화된 드라이브** 는 대용량 저장 기기의 암호화 상태에 대한 리포트 또는 암호화된 드라이브로의 접근에 대한 권한 리포트를 생성합니다.
   - **암호화 이벤트**가 파일 암호화 오류에 관한 리포트를 생성합니다.
7. 생성할 리포트의 이름을 클릭합니다.

리포트 생성이 시작됩니다.

오프라인 모드에서 암호화된 드라이브에 접근 권한 부여

예를 들어, Kaspersky Endpoint Security for Windows가 관리 중인 기기에 설치되지 않은 경우 사용자는 암호화된 기기에 대한 접근 권한을 요청할 수 있습니다. 요청을 수신한 후 접근 허용 키 파일을 만들어 사용자에게 보낼 수 있습니다. Kaspersky Endpoint Security for Windows 도움말에서 모든 사용 사례와 세부 지침을 확인할 수 있습니다.

오프라인 모드에서 암호화된 드라이브에 접근 권한을 부여하려면 다음 단계를 따릅니다.

1. 사용자로부터 액세스 요청 파일(FDERTC 확장자가 있는 파일)을 가져옵니다. Kaspersky Endpoint Security for Windows 도움말의 지침을 따라 Kaspersky Endpoint Security for Windows에서 파일을 생성합니다.
2. 메인 메뉴에서 **동작 → 데이터 암호화 및 보호 → 암호화된 드라이브**로 이동합니다.
   암호화된 드라이브 목록이 나타납니다.
3. 사용자가 접근 권한을 요청한 드라이브를 선택합니다.
4. **오프라인 모드인 기기에 접근 권한 부여** 버튼을 누릅니다.

5. 창이 열리면 선택한 드라이브를 암호화하는 데 사용된 Kaspersky 애플리케이션에 해당하는 플러그인을 선택합니다.

> Kaspersky Security Center 웹 콘솔에서 지원하지 않는 Kaspersky 애플리케이션으로 드라이브를 암호화했다면, Microsoft Management Console 기반 관리 콘솔을 사용하여 오프라인 접근 권한을 부여하십시오.

6. Kaspersky Endpoint Security for Windows 도움말에 제공된 지침을 따릅니다(섹션 끝에 있는 확장 블록 참조).

그후, 사용자는 수신된 파일을 사용하여 암호화된 드라이브에 접근하고 드라이브에 저장된 데이터를 읽을 수 있습니다.

사용자 및 사용자 역할

이 섹션에서는 사용자 및 사용자 역할에 대해 설명하며 사용자와 사용자 역할을 생성/수정하고, 사용자에게 역할과 그룹을 할당하고, 정책 프로필을 역할과 연결하는 지침을 제공합니다.

사용자 역할 정보

*역할*이라고도 하는 *사용자 역할*은 권한 세트가 포함된 개체입니다. 사용자 기기에 설치된 Kaspersky 애플리케이션의 설정과 역할을 연결할 수 있습니다. 관리 그룹이나 중앙 관리 서버 계층 구조의 모든 레벨 또는 특정 개체 레벨에서 사용자 세트 또는 보안 그룹 세트에 역할을 할당할 수 있습니다.

> 가상 중앙 관리 서버가 포함된 중앙 관리 서버 계층을 통해 기기 관리 시, 물리적 중앙 관리 서버에서만 사용자 역할을 생성, 수정, 삭제할 수 있습니다. 그런 다음 가상 서버를 포함하여 보조 중앙 관리 서버에 사용자 역할을 전파할 수 있습니다.

사용자 역할을 정책 프로필과 연결할 수 있습니다. 역할이 할당된 사용자에게는 직무를 수행하는 데 필요한 보안 설정이 제공됩니다.

특정 관리 그룹의 기기 사용자와 사용자 역할을 연결할 수 있습니다.

사용자 역할 범위

*사용자 역할 범위*는 사용자와 관리 그룹의 조합입니다. 사용자 역할과 연결된 설정은 이 역할이 지정된 사용자 소유의 기기가 이 역할과 연결된 그룹(자식 그룹 포함)에 속하는 경우에만 해당 기기에 적용됩니다.

역할 사용 시의 이점

역할을 사용하는 경우 각각의 관리 중인 기기 또는 사용자에 대해 개별적으로 보안 설정을 지정하지 않아도 된다는 이점이 있습니다. 회사의 사용자와 기기 수는 매우 많을 수 있지만 다른 보안 설정을 사용해야 하는 직무의 수는 그보다 훨씬 적습니다.

정책 프로필을 사용하는 경우와의 차이점

정책 프로필은 각 Kaspersky 애플리케이션에 대해 별도로 생성된 정책의 속성입니다. 각 애플리케이션용으로 생성되는 여러 정책 프로필에는 역할이 연결됩니다. 그러므로 역할을 사용하면 특정 사용자 유형 관련 설정을 한 곳에서 통합하여 관리할 수 있습니다.

사용자 계정 및 세션 보기

Kaspersky Security Center를 통해 사용자 계정과 계정 그룹을 관리할 수 있습니다. 이 애플리케이션은 두 종류의 계정을 지원합니다:

- 조직 직원 계정. 중앙 관리 서버는 조직 네트워크를 검색할 때 해당 사용자들의 계정 데이터를 검색합니다.
- 내부 사용자 계정. 이들 계정은 가상 중앙 관리 서버가 사용될 때 적용됩니다. 내부 사용자의 계정은 Kaspersky Security Center내에서만 생성 및 사용됩니다.

다음 방법 중 하나로 사용자 계정 및 세션 목록을 볼 수 있습니다.

- 메인 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동합니다.
- 메인 메뉴에서 **에셋(기기)** → **관리 중인 기기** → <기기 이름> 링크 → **일반** 탭 → **일반** 섹션 → **세션** 블록으로 갑니다.

  세션 섹션에 Windows를 실행하는 기기의 활성 세션이 있는 사용자 계정이 표시됩니다.

다음 요구 사항을 충족하면 사용자 계정 및 세션 목록이 올바르게 표시됩니다.

- 중앙 관리 서버와 같은 버전 이상의 네트워크 에이전트를 사용합니다.
- 도메인 사용자의 계정을 표시하기 위해 Active Directory 검색이 활성화됩니다.
- Windows를 실행하는 관리 중인 기기에서 **서버(LanmanServer)** 서비스가 실행됩니다.

애플리케이션 기능에 대한 접근 권한 구성. 역할 기반 접근 제어

Kaspersky Security Center는 Kaspersky Security Center 및 관리 중인 Kaspersky 애플리케이션 기능에 대한 역할 기반 접근을 위한 기능을 제공합니다.

다음 방법 중 하나로 Kaspersky Security Center 사용자를 위한 애플리케이션 기능에 대한 접근 권한을 구성할 수 있습니다.

- 각 사용자 또는 사용자 그룹에 대해 개별적으로 권한 구성.
- 사전 정의된 권한 세트를 사용하여 표준 사용자 역할을 생성한 다음 사용자의 작업 범위에 따라 해당 역할을 사용자에게 할당합니다.

사용자 역할 적용은 애플리케이션 기능에 대한 사용자 접근 권한을 구성하는 일상적인 절차를 간소화하고 줄이기 위한 것입니다. 역할 내의 접근 권한은 표준 작업 및 사용자의 작업 범위에 따라 구성됩니다.

사용자 역할에는 개별 용도에 해당하는 이름을 할당할 수 있습니다. 애플리케이션에서 역할을 수에 제한 없이 생성할 수 있습니다.

이미 구성된 권한 세트로 사전 정의된 사용자 역할을 사용하거나 새로운 역할을 만들고 필요한 권한을 직접 구성할 수 있습니다.

애플리케이션 기능에 대한 접근 권한

아래 표는 관련 작업, 리포트, 설정을 관리하고 관련 사용자 작업을 수행할 수 있는 접근 권한이 부여된 Kaspersky Security Center 기능을 보여줍니다.

표에 나열된 사용자 작업을 수행하려면 사용자는 작업 옆에 지정된 권한이 있어야 합니다.

읽기, **쓰기** 및 **실행** 권한은 모든 작업, 리포트 또는 설정에 적용됩니다. 이러한 권한 외에도 사용자는 작업, 리포트 또는 기기 조회에 대한 설정을 관리하려면 **기기 선택에 대한 동작 수행** 권한이 있어야 합니다.

> 테이블에 누락된 모든 작업, 리포트, 설정 및 설치 패키지는 **일반 기능: 기본 기능** 기능 영역에 속합니다.

애플리케이션 기능에 대한 접근 권한

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
일반 기능: **관리 그룹 관리**	**쓰기**	• 관리 그룹에 기기 추가: **쓰기** • 관리 그룹에서 기기 삭제: **쓰기** • 다른 관리 그룹에 관리 그룹 추가: **쓰기** • 다른 관리 그룹에서 관리 그룹 삭제: **쓰기**	없음	없음	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
일반 기능: ACL에 상관없이 개체 접근	**읽기**	모든 개체에 대한 읽기 액세스 권한 가져오기: **읽기**	없음	없음	**일반 기능: ACL에 상관없이 개체 접근** 기능 영역은 감사를 위한 것입니다. 이 기능 영역에 대한 **읽기**권한이 부여되면 사용자는 모든 개체에 대한 전체 **읽기** 권한을 얻고 네트워크 에이전트를 통해 중앙 관리 서버에 연결된 기기 중에서 로컬 관리자 권한(Linux에서는 루트)으로 생성된 작업을 실행할 수 있습니다. 이러한 권한은 공식 업무 수행이 필요한 사용자에게만 제한적으로 신중하게 부여하는 것이 좋습니다. 특정 개체에 대한 읽기 접근을 금지하는 다른 권한과 상관없이 접근이 허용됩니다.
일반 기능: 기본 기능	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 가상 서버에 대한 기기 이동 규칙(생성, 수정 또는 삭제): **쓰기**, **기기 선택에 대한 동작 수행** • 모바일(LWNGT) 프로토콜 사용자 지정 인증서 가져오기: **읽기** • 모바일(LWNGT) 프로토콜 사용자 지정 인증서 설정: **쓰기** • NLA 정의 네트워크 목록 가져오기: **읽기** • NLA 정의 네트워크 목록 추가, 수정 또는 삭제: **쓰기** • 그룹 접근 제어 목록 보기: **읽기** • Kaspersky 이벤트 로그 보기: **읽기** • BitLocker로 암호화된 하드 드라이브 액세스 복원을 위한 복구 키 보기: **실행**	• "중앙 관리 서버 저장소 업데이트 다운로드" • "리포트 전달" • "설치 패키지 배포" • "보조 중앙 관리 서버에 원격으로 애플리케이션 설치"	• "보호 상태 리포트" • "위협 처리 리포트" • "가장 자주 감염된 기기 리포트(상위 10대)" • "안티 바이러스 데이터베이스 업데이트 리포트" • "오류 리포트" • "네트워크 공격 리포트" • "설치된 메일 시스템 보호 애플리케이션 요약 리포트" • "설치된 경계 방어 애플리케이션 요약 리포트" • "설치된 애플리케이션 유형에 대한 요약 리포트" • "가장 많이 감염된 기기 리포트(상위 10대)" • "인시던트 리포트" • "이벤트 리포트" • "배포 지점 활동 리포트" • "보조 중앙 관리 서버 리포트" • "매체 제어 이벤트 리포트" • "취약점 리포트" • "금지한 애플리케이션에 대한 리포트" • "웹 제어 리포트" • "관리 중인 기기의 암호화 상태 리포트" • "대용량 스토리지 기기의 암호화 상태 리포트" • "파일 암호화 오류 리포트"	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
				• "암호화된 파일로의 접근 차단 리포트" • "암호화된 기기에 대한 접근 권한 리포트" • "유효한 사용자 권한에 대한 리포트" • "권한 리포트"	
일반 기능: **삭제된 개체**	• **읽기** • **쓰기**	• 휴지통에서 삭제된 개체 보기: **읽기** • 휴지통에서 개체 삭제: **쓰기**	없음	없음	없음
일반 기능: **이벤트 처리**	• **이벤트 삭제** • **이벤트 알림 설정 편집** • **이벤트 로그 기록 설정 편집** • **쓰기**	• 이벤트 등록 설정 변경: **이벤트 로그 기록 설정 편집** • 이벤트 알림 설정 변경: **이벤트 알림 설정 편집** • 이벤트 삭제: **이벤트 삭제**	없음	없음	설정: • 바이러스 급증 설정: 바이러스 급증 이벤트를 생성하는 데 필요한 바이러스 탐지 수 • 바이러스 급증 설정: 바이러스 탐지 평가 기간 • 데이터베이스에 저장되는 최대 이벤트 수 • 삭제된 기기에서 이벤트를 저장하는 기간
일반 기능: **중앙 관리 서버에서의 동작**	• **읽기** • **쓰기** • **실행** • **개체 ACL 수정** • **기기 선택에 대한 동작 수행**	• 네트워크 에이전트 연결을 위한 중앙 관리 서버의 포트 지정: **쓰기** • 중앙 관리 서버에 실행된 활성화 프록시의 포트 지정: **쓰기** • 중앙 관리 서버에 실행된 모바일용 활성화 프록시의 포트 지정: **쓰기** • 독립형 패키지 배포를 위한 웹 서버의 포트 지정: **쓰기** • MDM 프로필 배포를 위한 웹 서버의 포트 지정: **쓰기** • Kaspersky Security Center 웹 콘솔을 통한 연결용 중앙 관리 서버 SSL 포트 지정: **쓰기** • 모바일 연결을 위한 중앙 관리 서버의 포트 지정: **쓰기** • 중앙 관리 서버 데이터베이스에 저장되는 최대 이벤트 수 변경: **쓰기** • 중앙 관리 서버에서 보낼 수 있는 최대 이벤트 수 지정: **쓰기** • 중앙 관리 서버에서 이벤트를 보낼 수 있는 기간 지정: **쓰기**	• "중앙 관리 서버 데이터 백업" • "데이터베이스 점검"	없음	없음
일반 기능: **Kaspersky 애플리케이션 배포**	• **Kaspersky 패치 관리** • **읽기** • **쓰기**	패치 설치 승인 또는 거부: **Kaspersky 패치 관리**	없음	• "가상 중앙 관리 서버의 라이센스 키 사용에 대한 보고"	설치 패키지: "Kaspersky"

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
	• **실행** • **기기 선택에 대한 동작 수행**			• "Kaspersky 소프트웨어 버전 리포트" • "비-호환 애플리케이션 리포트" • "Kaspersky 소프트웨어 모듈 업데이트 리포트" • "보호 배포 리포트"	
일반 기능: **라이센스 키 관리**	• **키 파일 내보내기** • **쓰기**	• 키 파일 내보내기: **키 파일 내보내기** • 중앙 관리 서버 라이센스 키 설정 수정: **쓰기**	없음	없음	없음
일반 기능: **강제 리포트 관리**	• **읽기** • **쓰기**	• ACL에 상관없이 리포트 생성: **쓰기** • ACL에 상관없이 리포트 실행: **읽기**	없음	없음	없음
일반 기능: **중앙 관리 서버 계층 구조**	**중앙 관리 서버 계층 구조 구성**	보조 중앙 관리 서버 등록, 업데이트 또는 삭제: **중앙 관리 서버 계층 구조 구성**	없음	없음	없음
일반 기능: **사용자 권한**	**개체 ACL 수정**	• 모든 개체의 보안 속성 변경: **개체 ACL 수정** • 사용자 역할 관리: **개체 ACL 수정** • 내부 사용자 관리: **개체 ACL 수정** • 보안 그룹 관리: **개체 ACL 수정** • 별칭 관리: **개체 ACL 수정**	없음	없음	없음
일반 기능 가상 중앙 관리 서버	• **가상 중앙 관리 서버 관리** • **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 가상 중앙 관리 서버 목록 가져 오기: **읽기** • 가상 중앙 관리 서버에 대한 정보 가져오기: **읽기** • 가상 중앙 관리 서버 생성, 업데이트 또는 삭제: **가상 중앙 관리 서버 관리** • 가상 중앙 관리 서버를 다른 그룹으로 이동: **가상 중앙 관리 서버 관리** • 가상 중앙 관리 서버 권한 설정: **가상 중앙 관리 서버 관리**	없음	"타사 소프트웨어 업데이트 설치 결과 보고"	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
일반 기능: 암호화 키 관리	**쓰기**	암호화 키 가져오기: **쓰기**	없음	없음	없음
모바일 기기 관리: 일반	• **새 기기 연결** • **모바일 기기에 정보 명령만 보내기** • **모바일 기기에 명령 전송** • **인증서 관리** • **읽기** • **쓰기**	• 키 관리 서비스 복원 데이터 가져오기: **읽기** • 사용자 인증서 삭제: **인증서 관리** • 사용자 인증서 공개 부분 가져오기: **읽기** • 공개 키 인프라 활성화 여부 확인: **읽기** • 공개 키 인프라 계정 확인: **읽기** • 공개 키 인프라 템플릿 가져오기: **읽기** • 확장 키 사용 인증서로 공개 키 인프라 템플릿 가져오기: **읽기** • 공개 키 인프라 인증서 취소 여부 확인: **읽기** • 사용자 인증서 발급 설정 업데이트: **인증서 관리** • 사용자 인증서 발급 설정 가져오기: **읽기** • 애플리케이션 이름 및 버전별 패키지 가져오기: **읽기** • 사용자 인증서 설정 또는 취소: **인증서 관리** • 사용자 인증서 갱신: **인증서 관리** • 사용자 인증서 태그 설정: **인증서 관리** • MDM 설치 패키지 생성 실행, MDM 설치 패키지 생성 취소: **새 기기 연결**	없음	없음	없음
시스템 관리: 연결성	• **RDP 세션 시작** • **기존 RDP 세션에 연결** • **터널링 시작** • **기기에서 관리자의 워크스테이션에 파일 저장** • **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 데스크톱 공유 세션 생성: **RDP 세션 시작** • RDP 세션 생성: **기존 RDP 세션에 연결** • 터널 생성: **터널링 시작** • 컨텐츠 네트워크 목록 저장: **기기에서 관리자의 워크스테이션에 파일 저장**	없음	"기기 사용자에 대한 리포트"	없음
시스템 관리: 하드웨어 인벤토리	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 하드웨어 인벤토리 개체 가져오기 또는 내보내기: **읽기** • 하드웨어 인벤토리 개체 추가, 설정 또는 삭제: **쓰기**	없음	• "자산 관리(하드웨어) 리포트" • "하드웨어 자산 변경 사항 리포트" • "하드웨어 리포트"	없음
시스템 관리:	• **읽기**	• CISCO 설정 보기:	없음	없음	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
네트워크 접근 제어	• **쓰기**	**읽기** • CISCO 설정 변경: **쓰기**			
시스템 관리: 운영 체제 배포	• **PXE 서버 배포** • **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• PXE 서버 배포: **PXE 서버 배포** • PXE 서버 목록 보기: **읽기** • PXE 클라이언트에서 설치 프로세스 시작 또는 중지: **실행** • WinPE 드라이버 및 운영 체제 이미지 관리: **쓰기**	"참조 기기 OS 이미지에 설치 패키지 생성"	없음	설치 패키지: "OS 이미지"
시스템 관리: 취약점 및 패치 관리	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 타사 패치 속성 보기: **읽기** • 타사 패치 속성 변경: **쓰기**	• "Windows 업데이트 동기화 수행" • "Windows Update 업데이트 설치" • "취약점 수정" • "필요한 업데이트를 설치하고 취약점 수정"	"소프트웨어 업데이트 리포트"	없음
시스템 관리: 원격 설치	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	• 타사 취약점 및 패치 관리 기반 설치 패키지 속성 보기: **읽기** • 타사 취약점 및 패치 관리 기반 설치 패키지 속성 변경: **쓰기**	없음	없음	설치 패키지: • "사용자 지정 애플리케이션" • "VAPM 패키지"
시스템 관리: 소프트웨어 인벤토리	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	없음	없음	• "자산 관리(소프트웨어) 리포트" • "자산 관리(소프트웨어) 기록 리포트" • "유료 애플리케이션 그룹 상태에 대한 리포트" • "타사 소프트웨어 라이센스 키에 대한 리포트"	없음
시스템 관리: 스크립트 원격 실행	• **읽기** • **쓰기** • **실행** • **기기 선택에 대한 동작 수행**	사용자가 작업 속성을 볼 수 있습니다: **읽기** 사용자가 설치 패키지를 생성, 삭제, 수정할 수 있습니다: **쓰기** 사용자가 작업을 실행할 수 있습니다: **쓰기**. 클라이언트 Linux 기기에서 스크립트는 루트 권한으로 실행됩니다. 사용자가 작업을 실행하거나 실행을 예약할 수 있습니다: **실행**	"스크립트 원격 실행"	없음	없음

기능 영역	권한	사용자 작업: 작업을 수행하는 데 필요한 권한	작업	리포트	기타
		사용자가 선택한 기기에서 작업을 실행할 수 있습니다: **기기 선택에 대한 동작 수행**			

사전 정의된 사용자 역할

Kaspersky Security Center 사용자에게 할당된 사용자 역할은 사용자에게 애플리케이션 기능에 대한 접근 권한 세트를 제공합니다.

가상 서버에서 생성된 사용자에게는 중앙 관리 서버의 역할을 할당할 수 없습니다.

미리 구성된 권한 세트로 사전 정의된 사용자 역할을 사용하거나 새로운 역할을 생성할 수 있습니다. 새 역할을 만들 경우, 직접 Kaspersky Security Center 기능에 대한 역할 범위를 설정하고 접근 권한을 할당해야 합니다. Kaspersky Security Center에서 사용할 수 있는 사전 정의된 사용자 역할 중 일부는 **감사관**, **보안 책임자**, **감독관** 등과 같은 특정 직책과 연관될 수 있습니다(이러한 역할은 Kaspersky Security Center 버전 11부터 제공). 이러한 역할의 접근 권한은 관련 직책의 표준 작업 및 직무 범위에 따라 미리 구성됩니다. 아래 표는 특정 직책과 역할이 어떻게 연관되는지 보여줍니다.

특정 직책별 역할의 예

역할	메모
감사관	로컬 관리자 권한(Linux에서는 루트)으로 네트워크 에이전트를 통해 중앙 관리 서버에 연결된 기기에서 모든 보기 작업과 생성된 작업의 실행을 허용합니다. 이 역할은 공식 업무 수행에 해당 역할이 필요한 사용자에게만 제한적으로 신중하게 할당하는 것이 좋습니다.
감독관	모든 보기 작업이 허용되며 다른 작업은 허용되지 않습니다. 조직의 IT 보안을 담당하는 보안 책임자 및 기타 관리자에게 이 역할을 할당할 수 있습니다.
보안 운영자	모든 보기 작업과 리포트 관리가 허용되며 **시스템 관리**: **연결성** 영역에 제한된 권한을 부여합니다. 조직의 IT 보안을 담당하는 운영자에게 이 역할을 할당할 수 있습니다.

아래 표는 미리 정의된 각 사용자 역할에 할당된 접근 권한을 보여줍니다.

미리 정의된 사용자 역할의 접근 권한

역할	설명

중앙 관리 서버 관리자	다음 기능 영역의 모든 작업을 허용합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **이벤트 처리**
	  • **중앙 관리 서버 계층 구조**
	  • **가상 중앙 관리 서버**
	• **시스템 관리**:
	  • **연결성**
	  • **하드웨어 인벤토리**
	  • **소프트웨어 인벤토리**
	일반 기능: 암호화 키 관리 기능 영역에 **읽기** 및 **쓰기** 권한을 부여합니다.

역할	설명

중앙 관리 서버 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **가상 중앙 관리 서버**
	• **시스템 관리**:
	  • **연결성**
	  • **하드웨어 인벤토리**
	  • **소프트웨어 인벤토리**

감사관	**일반 기능**에서 기능 영역에서의 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **삭제된 개체** • **강제 리포트 관리** 조직 감사를 수행하는 사용자에게 이 역할을 할당할 수 있습니다.

설치 관리자	다음 기능 영역의 모든 작업을 허용합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **Kaspersky 소프트웨어 배포**
	  • **라이센스 키 관리**
	• **시스템 관리**:
	  • **운영 체제 배포**
	  • **취약점 및 패치 관리**
	  • **원격 설치**
	  • **소프트웨어 인벤토리**
	일반 기능: 가상 중앙 관리 서버 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다.

설치 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다.
	• **일반 기능**:
	  • **기본 기능**
	  • **Kaspersky 소프트웨어 배포**(이 영역에 **Kaspersky 패치 관리** 권한도 부여)
	  • **가상 중앙 관리 서버**
	• **시스템 매니지먼트**:
	  • **운영 체제 배포**
	  • **취약점 및 패치 관리**
	  • **원격 설치**
	  • **소프트웨어 인벤토리**

Kaspersky Endpoint Security 관리자	다음 기능 영역의 모든 작업을 허용합니다. • **일반 기능: 기본 기능** • Kaspersky Endpoint Security 영역(모든 기능 포함) **일반 기능: 암호화 키 관리** 기능 영역에 **읽기** 및 **쓰기** 권한을 부여합니다.
Kaspersky Endpoint Security 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다. • **일반 기능: 기본 기능** • Kaspersky Endpoint Security 영역(모든 기능 포함)

역할	설명
메인 관리자	**일반 기능**에서 다음 영역을 *제외한* 기능 영역의 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **강제 리포트 관리** **일반 기능: 암호화 키 관리** 기능 영역에 **읽기** 및 **쓰기** 권한을 부여합니다.

메인 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다(해당하는 경우).
	• **일반 기능**:
	  • **기본 기능**
	  • **삭제된 개체**
	  • **중앙 관리 서버에서의 동작**
	  • **Kaspersky 애플리케이션 배포**
	  • **가상 중앙 관리 서버**
	• **모바일 기기 관리: 일반**
	• **시스템 관리**(모든 기능 포함)
	• Kaspersky Endpoint Security 영역(모든 기능 포함)

모바일 기기 관리 관리자	다음 기능 영역의 모든 작업을 허용합니다. • **일반 기능: 기본 기능** • **모바일 기기 매니지먼트: 일반**
모바일 기기 관리 운영자	**일반 기능**: **기본 기능** 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다. **모바일 기기 관리**: **일반**에서 **읽기** 및 **모바일 기기에 정보 명령만 보내기** 권한을 부여합니다.
보안 운영자	**일반 기능**의 다음 기능 영역에서 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **강제 리포트 관리** **시스템 관리: 연결성** 기능 영역에 **읽기**, **쓰기**, **실행**, **기기의 파일을 관리자 워크스테이션에 저장** 및 **기기 조회에 대한 동작 수행** 권한을 부여합니다. 조직의 IT 보안을 담당하는 운영자에게 이 역할을 할당할 수 있습니다.
셀프 서비스 포털 사용자	**모바일 기기 관리: 셀프 서비스 포털** 기능 영역의 모든 작업을 허용합니다. 이 기능은 Kaspersky Security Center 11 이상 버전에서 지원되지 않습니다.
감독관	**일반 기능**: **ACL에 상관없이 개체 접근** 및 **일반 기능**: **강제 리포트 관리** 기능 영역에 **읽기** 권한을 부여합니다. 조직의 IT 보안을 담당하는 보안 책임자 및 기타 관리자에게 이 역할을 할당할 수 있습니다.
취약점 및 패치 관리 관리자	**일반 기능**: **기본 기능** 및 **시스템 관리**(모든 기능 포함) 기능 영역의 모든 작업을 허용합니다.
취약점 및 패치 관리 운영자	**일반 기능**: **기본 기능** 및 **시스템 관리** (모든 기능 포함) 기능 영역에 **읽기 및 실행**(해당된다면) 권한을 부여합니다.

특정 개체에 대한 액세스 권한 할당

서버 레벨에서 액세스 권한을 할당하는 것 외에도 특정 작업 등 특정 개체에 대한 접근을 구성할 수 있습니다. 애플리케이션을 통해 다음 개체 유형에 대한 액세스 권한을 지정할 수 있습니다:

- 관리 그룹
- 작업
- 리포트
- 기기 조회
- 이벤트 조회

특정 개체에 대한 액세스 권한을 할당하려면:

1. 개체 유형에 따라 메인 메뉴에서 해당 섹션으로 이동합니다:
   - **에셋(기기) → 그룹 계층 구조**
   - **에셋(기기) → 작업**
   - **모니터링 및 보고 → 리포트**
   - **에셋(기기) → 기기 선택**
   - **모니터링 및 보고 → 이벤트 선택**
2. 액세스 권한을 구성하려는 개체의 속성을 엽니다.

   관리 그룹 또는 작업의 속성 창을 열려면 개체 이름을 클릭합니다. 도구 모음의 버튼을 사용하여 다른 개체의 속성을 열 수 있습니다.
3. 속성 창에서 **접근 권한** 섹션을 엽니다.

   사용자 목록이 열립니다. 나열된 사용자 및 보안 그룹은 개체에 대한 액세스 권한을 가집니다. 기본적으로 관리 그룹 또는 서버 계층 사용 시, 목록 및 액세스 권한은 상위 관리 그룹 또는 기본 서버에서 상속됩니다.
4. 목록을 수정하려면 **사용자 지정 권한 사용** 옵션을 활성화합니다.
5. 액세스 권한 구성:
   - **추가** 및 **삭제** 버튼을 사용하여 목록을 수정합니다.
   - 사용자 또는 보안 그룹에 대한 액세스 권한을 지정합니다. 다음 중 하나를 수행합니다:
     - 접근 권한을 수동으로 지정하려면 사용자 또는 보안 그룹을 선택하고 **접근 권한** 버튼을 클릭한 후 접근 권한을 지정합니다.
     - 사용자 또는 보안 그룹에 사용자 역할을 할당하려면 사용자 또는 보안 그룹을 선택하고 **역할** 버튼을 클릭한 다음 할당할 역할을 선택합니다.
6. **저장** 버튼을 클릭합니다.

개체에 대한 액세스 권한이 구성됩니다.

사용자 및 보안 그룹에 접근 권한 할당

사용자 및 보안 그룹에 중앙 관리 서버의 다양한 기능(Kaspersky Endpoint Security for Linux 등)에 대한 접근 권한을 부여할 수 있습니다.

사용자나 보안 그룹에 접근 권한을 할당하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.

   중앙 관리 서버 속성 창이 열립니다.
2. **접근 권한** 탭에서 권한을 할당할 사용자 또는 보안 그룹 이름 옆의 확인란을 선택하고 **접근 권한**을 클릭합니다.

   여러 사용자 또는 보안 그룹을 동시에 선택할 수는 없습니다. 둘 이상을 선택하면 **접근 권한** 버튼이 비활성화됩니다.

3. 사용자 또는 그룹에 대한 권한 집합을 구성합니다.

   a. 중앙 관리 서버 또는 기타 Kaspersky 애플리케이션 기능이 있는 노드를 확장합니다.

   b. 원하는 기능 또는 접근 권한 옆에 있는 **허락** 또는 **거부** 확인란을 선택합니다.

   예 1: **애플리케이션 통합** 노드 옆에 있는 **허용** 확인란을 선택하여 사용자 또는 그룹의 애플리케이션 통합 기능(**읽기**, **쓰기** 및 **실행**)에 사용 가능한 모든 접근 권한을 부여합니다.

   예 2: **암호화 키 관리** 노드를 확장한 다음 **쓰기** 권한 옆에 있는 **허용** 확인란을 선택하여 사용자 또는 그룹의 암호화 키 관리 기능에 대한 **쓰기** 접근 권한을 부여합니다.

4. 접근 권한 집합을 구성한 후 **확인**을 클릭합니다.

사용자나 사용자 그룹에 대한 권한 세트가 구성됩니다.

중앙 관리 서버 또는 관리 그룹의 권한은 다음 영역으로 구분됩니다:

- 일반 기능:
  - 관리 그룹 관리
  - ACL에 상관없이 개체 접근
  - 기본 기능
  - 삭제된 개체
  - 암호화 키 관리
  - 이벤트 처리
  - 중앙 관리 서버에서의 동작(중앙 관리 서버의 속성 창에만 있음)
  - 기기 태그
  - Kaspersky 애플리케이션 배포
  - 라이센스 키 관리
  - 애플리케이션 통합
  - 강제 리포트 관리
  - 중앙 관리 서버 계층 구조
  - 사용자 권한
  - 가상 중앙 관리 서버
- 모바일 기기 관리:
  - 일반
  - 셀프 서비스 포털

- 시스템 관리:
  - 연결성
  - 스크립트 원격 실행
  - 하드웨어 인벤토리
  - 네트워크 접근 제어
  - 운영 체제 배포
  - 취약점 및 패치 관리
  - 원격 설치
  - 소프트웨어 인벤토리

접근 권한에서 **허락**이나 **거부**를 모두 선택하지 않으면 접근 권한은 *정의 안 됨*으로 간주되며 사용자에 대해 명시적으로 거부되거나 허락될 때까지는 거부됩니다.

사용자 권한은 다음 권한의 합입니다:

- 사용자의 고유 권한
- 이 사용자에게 할당된 모든 역할의 권한
- 사용자가 속한 모든 보안 그룹의 권한
- 사용자가 속한 보안 그룹에 할당된 모든 역할의 권한

이러한 권한 세트 중 하나 이상에서 권한 상태가 **거부**인 경우에는 다른 세트에서 해당 권한이 허용 또는 미정의 상태여도 사용자의 해당 권한 사용은 거부됩니다.

또한 사용자 역할 범위에 사용자 및 보안 그룹을 추가하여 중앙 관리 서버의 다양한 기능을 사용할 수 있습니다. 사용자 역할이 지정된 사용자 소유의 기기가 이 역할과 연결된 그룹(자식 그룹 포함)에 속할 때만 사용자 역할과 연결된 설정이 해당 기기에만 적용됩니다.

내부 사용자의 계정 추가

사용자 계정을 추가하려면 일반 기능: 사용자 권한 기능 영역에서 계정에 개체 ACL 수정 권한이 있는지 확인합니다.

Kaspersky Security Center에 새 내부 사용자 계정을 추가하려면 다음과 같이 하십시오:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 탭을 선택합니다.
2. **추가**를 누릅니다.

3. **사용자 추가** 창이 열리면 새 사용자 계정의 설정을 지정합니다.

- **이름**
- **암호**
  암호는 다음 규칙을 따라야 합니다:
  - 암호는 8자에서 256자 사이여야 합니다.
  - 암호는 아래에 나와 있는 그룹 중 3개 이상의 문자를 포함해야 합니다:
    - 대문자(A-Z)
    - 소문자(a-z)
    - 숫자(0-9)
    - 특수 문자(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - 암호는 공백, 유니코드 문자 또는 "." 및 "@"의 조합("."이 "@" 앞에 오는 경우)을 포함할 수 없습니다.

  입력한 암호를 보려면 을(를) 클릭합니다.
  첫 로그인 시 암호를 변경해야 합니다 옵션을 사용하여 첫 사용자 인증 시 암호 변경을 강제할 수 있습니다.

4. 변경 사항을 저장하여 새 사용자 계정 생성을 완료합니다.

새 사용자 계정이 사용자 목록에 추가됩니다.

Kaspersky Security Center 웹 콘솔에서 생성된 내부 사용자 계정으로 로그인하려면 계정에 역할을 할당해야 합니다. 로그인하기 전에 내부 사용자 계정에 역할이 할당되어 있는지 확인합니다. 그렇지 않으면 로그인 오류가 발생합니다.

보안 그룹 생성

보안 그룹을 추가하려면:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **그룹** 탭을 선택합니다.
2. **추가**를 누릅니다.
3. **보안 그룹 생성** 창이 열리면 새 보안 그룹에 대해 다음 설정을 지정합니다.
   - **그룹 이름**
   - **설명**
4. **저장**을 눌러 변경 사항을 저장합니다.

새 보안 그룹이 그룹 목록에 추가됩니다.

내부 사용자의 계정 편집

사용자 계정을 편집하려면 일반 기능: 사용자 권한 기능 영역에서 계정에 개체 ACL 수정 권한이 있는지 확인합니다.

Kaspersky Security Center에서 내부 사용자 계정을 편집하려면 다음과 같이 하십시오:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 탭을 선택합니다.
2. 편집할 사용자 계정의 이름을 누릅니다.
3. 사용자 설정 창이 열리면 **일반** 탭에서 사용자 계정의 설정을 변경합니다.

- **사용자 상태**

  필요한 경우 토글 버튼을 **비활성화됨**으로 전환하여 사용자의 애플리케이션 연결을 차단합니다. 예를 들어 직원이 퇴사한 후에 계정을 비활성화할 수 있습니다.

- **이름**
- **전체 이름**
- **설명**
- **이메일 주소**
- **메인 전화**
- **암호**

  필요하다면 다음과 같이 Kaspersky Security Center에 사용자 연결을 위한 새 암호를 설정할 수 있습니다.

  a. **암호 변경** 버튼을 클릭하고 사용자 계정의 새 암호를 설정합니다.
  암호는 다음 규칙을 따라야 합니다:

  - 암호는 8자에서 256자 사이여야 합니다.
  - 암호는 아래에 나와 있는 그룹 중 3개 이상의 문자를 포함해야 합니다:
    - 대문자(A-Z)
    - 소문자(a-z)
    - 숫자(0-9)
    - 특수 문자(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - 암호는 공백, 유니코드 문자 또는 "." 및 "@"의 조합("."이 "@" 앞에 오는 경우)을 포함할 수 없습니다.

입력한 암호를 보려면 을(를) 클릭합니다.

b. 필요하다면 **첫 로그인 시 암호를 변경해야 합니다** 옵션을 사용하여 다음 사용자 인증 시 암호 변경을 강제할 수 있습니다.

c. 사용자 계정의 무단 수정을 방지 중이라면, 이 계정의 변경 권한이 있는지 확인해야 합니다. **계정 보호** 창의 일반 기능: 사용자 권한 기능 영역에서 개체 ACL 수정 권한이 있는 계정의 자격 증명을 지정합니다.

4. **인증 보안** 탭에서 이 계정에 대한 보안 설정을 지정할 수 있습니다.

5. **그룹** 탭에서 보안 그룹에 사용자를 추가할 수 있습니다.

6. **기기** 탭에서는 사용자에게 기기를 할당할 수 있습니다.

7. **역할** 탭에서는 사용자에게 역할을 할당할 수 있습니다.

8. 변경 사항을 저장하고 사용자 계정 편집을 완료합니다.

업데이트된 사용자 계정이 사용자 목록에 표시됩니다.

보안 그룹 편집

보안 그룹을 편집하려면:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **그룹** 탭을 선택합니다.

2. 편집할 보안 그룹의 이름을 누릅니다.

3. 그룹 설정 창이 열리면 보안 그룹의 설정을 변경합니다.

- **일반** 탭에서 **이름** 및 **설명** 설정을 변경할 수 있습니다. 이러한 설정은 내부 보안 그룹에만 사용할 수 있습니다.
- **사용자** 탭에서 보안 그룹에 사용자를 추가할 수 있습니다. 이 설정은 내부 사용자 및 내부 보안 그룹에만 사용할 수 있습니다.
- **역할** 탭에서는 보안 그룹에 역할을 할당할 수 있습니다.

4. **저장**을 눌러 변경 사항을 저장합니다.

변경 사항이 보안 그룹에 적용됩니다.

사용자 또는 보안 그룹에 역할 할당

사용자 또는 보안 그룹에 역할을 할당하려면:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 또는 **그룹** 탭을 선택합니다.
2. 역할을 할당할 사용자 또는 보안 그룹의 이름을 선택합니다.
   이름은 여러 개를 선택할 수 있습니다.
3. 메뉴 줄에서 **역할 할당** 버튼을 클릭합니다.
   역할 할당 마법사가 시작됩니다.
4. 마법사의 지시를 따릅니다. 선택한 사용자 또는 보안 그룹에 할당할 역할을 선택한 다음 역할 범위를 선택합니다.
   사용자 역할 범위는 사용자와 관리 그룹의 조합입니다. 사용자 역할과 연결된 설정은 이 역할이 지정된 사용자 소유의 기기가 이 역할과 연결된 그룹(자식 그룹 포함)에 속하는 경우에만 해당 기기에 적용됩니다.

중앙 관리 서버 처리를 위한 권한 집합이 포함된 역할이 해당 사용자 또는 보안 그룹에 할당됩니다. 사용자 또는 보안 그룹 목록에서 **역할 할당됨** 열에 확인란이 나타납니다.

가상 서버에서 생성된 사용자에게는 중앙 관리 서버의 역할을 할당할 수 없습니다.

내부 보안 그룹에 사용자 계정 추가

내부 보안 그룹에는 내부 사용자 계정만 추가할 수 있습니다.

내부 보안 그룹에 사용자 계정을 추가하려면:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 탭을 선택합니다.
2. 보안 그룹에 추가할 보안 사용자 계정 옆의 확인란을 선택합니다.
3. **그룹 할당** 버튼을 누릅니다.
4. **그룹 할당** 창이 열리면 사용자 계정을 추가할 보안 그룹을 선택합니다.
5. **저장** 버튼을 클릭합니다.

사용자 계정이 해당 보안 그룹에 추가됩니다. 그룹 설정을 사용하여 보안 그룹에 내부 사용자를 추가할 수도 있습니다.

기기 소유자로 특정 사용자 지정

사용자를 모바일 기기 소유자로 지정하는 방법은 Kaspersky Secure Mobility Management 도움말을 참조하십시오.

기기 소유자로 특정 사용자를 지정하려면 다음 단계를 따릅니다.

1. 가상 중앙 관리 서버에 연결된 기기의 소유자를 할당하려면, 먼저 가상 중앙 관리 서버로 전환합니다:

   a. 메인 메뉴에서 현재 중앙 관리 서버 이름 오른쪽의 펼침 단추 아이콘(▸)을 클릭합니다.

   b. 필요한 중앙 관리 서버를 선택합니다.

2. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 탭을 선택합니다.
   사용자 목록이 열립니다. 현재 가상 중앙 관리 서버에 연결되어 있다면, 목록에는 현재 가상 중앙 관리 서버 및 기본 중앙 관리 서버의 사용자가 포함됩니다.

3. 기기 소유자로 지정할 사용자 계정의 이름을 누릅니다.

4. 사용자 설정 창이 열리면 **기기** 탭을 누릅니다.

5. **추가**를 누릅니다.

6. 기기 목록에서 사용자에게 할당할 기기를 선택합니다.

7. **확인**를 누릅니다.

   선택한 기기가 사용자에게 할당된 기기 목록에 추가됩니다.

에셋(기기) → **관리 중인 기기**에서 할당할 기기 이름을 누른 다음 기기 소유자 관리 **기기 소유자 관리** 링크를 눌러 같은 작업을 수행할 수 있습니다.

모든 사용자에 대해 2단계 인증 구성

이 시나리오에서는 모든 사용자에 대해 2단계 인증을 활성화하는 방법과 2단계 인증에서 사용자 계정을 제외하는 방법을 설명합니다. 다른 사용자에 대해 활성화하기 전에 본인 계정에 2단계 인증을 활성화하지 않은 경우 애플리케이션에서 본인 계정에 2단계 인증을 활성화하는 창이 먼저 열립니다. 이 시나리오에서는 본인 계정에 대해 2단계 인증을 활성화하는 방법도 설명합니다.

> 본인 계정에 2단계 인증을 활성화했다면 모든 사용자에 대해 2단계 인증을 활성화하는 단계로 진행할 수 있습니다.

필수 구성 요소

시작하기 전에:

- 다른 사용자 계정의 보안 설정을 수정하려면 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한이 사용자 계정에 있어야 합니다.
- 중앙 관리 서버의 다른 사용자가 자신의 기기에 인증 앱을 설치했는지 확인합니다.

단계

모든 사용자에 대해 2단계 인증을 활성화하는 과정은 다음 단계로 진행됩니다.

1. **기기에 인증 앱 설치**

   다음과 같이 시간 기반 일회용 암호 알고리즘(TOTP)을 지원하는 모든 애플리케이션을 설치할 수 있습니다.

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA

   사용하려는 인증 앱을 Kaspersky Security Center가 지원하는지 확인하려면 모든 사용자 또는 특정 사용자에 대해 2단계 인증을 활성화합니다.

   단계 중 하나에서 인증 앱이 생성한 보안 코드를 입력하라고 합니다. 성공하면 Kaspersky Security Center가 선택한 인증기를 지원합니다.

   > 중앙 관리 서버 연결이 설정된 기기에는 인증 앱 설치를 권장하지 않습니다.

2. **인증 앱 시간을 중앙 관리 서버가 설치된 기기의 시간과 동기화**

   인증 앱이 있는 기기의 시간과 중앙 관리 서버가 있는 기기의 시간이 외부 시간 소스를 사용하여 UTC로 동기화되었는지 확인합니다. 그렇지 않으면 인증 및 2단계 인증 활성화 시 오류가 발생할 수 있습니다.

3. **계정에 대한 2단계 인증 활성화 및 계정의 비밀 키 받기**

   방법 지침:

   - MMC 기반 관리 콘솔: 본인 계정에 대해 2단계 인증 활성화
   - Kaspersky Security Center 웹 콘솔: 본인 계정에 대해 2단계 인증 활성화

   본인 계정에 2단계 인증을 활성화한 후 모든 사용자에 대해 2단계 인증을 활성화할 수 있습니다.

4. **모든 사용자에 대한 2단계 인증 활성화**

   2단계 인증이 활성화된 사용자는 이를 사용하여 중앙 관리 서버에 로그인해야 합니다.

   방법 지침:

   - MMC 기반 관리 콘솔: 모든 사용자에 대해 2단계 인증 활성화
   - Kaspersky Security Center 웹 콘솔: 모든 사용자에 대해 2단계 인증 활성화

5. **보안 코드 발행자 이름 편집**

   이름이 유사한 여러 중앙 관리 서버가 있는 경우 서로 다른 중앙 관리 서버를 보다 정확하게 구별할 수 있도록 보안 코드 발행자 이름을 변경해야 할 수 있습니다.

방법 지침:

- MMC 기반 관리 콘솔의 경우: 보안 코드 발행자 이름 편집
- Kaspersky Security Center 웹 콘솔: 보안 코드 발행자 이름 편집

6. **2단계 인증을 활성화할 필요가 없는 사용자 계정 제외**

   필요한 경우 2단계 인증에서 사용자를 제외합니다. 계정이 제외된 사용자는 중앙 관리 서버에 로그인하기 위해 2단계 인증을 사용할 필요가 없습니다.

   방법 지침:

   - MMC 기반 관리 콘솔: 2단계 인증에서 계정 제외
   - Kaspersky Security Center 웹 콘솔: 2단계 인증에서 계정 제외

7. **본인 계정에 대한 2단계 인증 구성**

   사용자가 2단계 인증에서 제외되지 않았고 해당 계정에 대해 2단계 인증을 아직 구성하지 않았다면, Kaspersky Security Center에 로그인할 때 열리는 창에서 이를 구성해야 합니다. 그렇지 않으면 보유 권한에 따라 중앙 관리 서버에 접근할 수 없습니다.

   방법 지침:

   - MMC 기반 관리 콘솔: 본인 계정에 대해 2단계 인증 구성
   - Kaspersky Security Center 웹 콘솔: 본인 계정에 대해 2단계 인증 구성

결과

이 시나리오를 완료하면:

- 계정에 대한 2단계 인증이 활성화됩니다.
- 제외된 사용자 계정을 제외하고 모든 중앙 관리 서버 사용자 계정에 2단계 인증이 활성화됩니다.

2단계 인증 정보

계정에 대해 2단계 인증을 활성화했다면 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에 로그인할 때 사용자 이름과 암호 외에 일회용 보안 코드가 필요합니다. 도메인 인증을 활성화하면 사용자는 일회용 보안 코드만 입력하면 됩니다.

2단계 인증을 사용하려면 모바일 기기나 컴퓨터에 일회용 보안 코드를 생성하는 인증 앱을 설치하십시오. 다음과 같이 시간 기반 일회용 암호 알고리즘(TOTP)을 지원하는 모든 애플리케이션을 사용할 수 있습니다.

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex ID

- Avanpost Authenticator
- Aladdin 2FA

사용하려는 인증 앱을 Kaspersky Security Center가 지원하는지 확인하려면 모든 사용자 또는 특정 사용자에 대해 2단계 인증을 활성화합니다.

단계 중 하나에서 인증 앱이 생성한 보안 코드를 입력하라고 합니다. 성공하면 Kaspersky Security Center가 선택한 인증기를 지원합니다.

> 비밀 키 또는 QR 코드를 저장하고 안전한 곳에 보관하는 것을 권장드립니다. 이는 모바일 기기 분실 시 Kaspersky Security Center 웹 콘솔에 대한 액세스 복원에 도움이 됩니다.

Kaspersky Security Center 사용을 보호하기 위해 본인 계정의 2단계 인증을 활성화하고 모든 사용자의 2단계 인증도 활성화할 수 있습니다.

> 2단계 인증에서 계정을 제외할 수 있습니다. 이는 인증을 위한 보안 코드를 받을 수 없는 서비스 계정에 필요할 수 있습니다.

규칙 및 제한 사항

모든 사용자에 대해 2단계 인증을 활성화하고 특정 사용자에 대해 2단계 인증을 비활성화하려면:

- **일반 기능: 사용자 권한** 기능 영역에 개체 ACL 수정 권한이 있는지 확인합니다.
- 사용자 계정에 대한 2단계 인증을 활성화합니다.

모든 사용자에 대해 2단계 인증을 비활성화하려면:

- **일반 기능: 사용자 권한** 기능 영역에 개체 ACL 수정 권한이 있는지 확인합니다.
- 2단계 인증을 사용하여 Kaspersky Security Center 웹 콘솔에 로그인합니다.

> Kaspersky Security Center 13 이상 버전에서 중앙 관리 서버의 사용자 계정에 대해 2단계 인증이 활성화된 경우 사용자는 버전이 12, 12.1 또는 12.2인 Kaspersky Security Center 웹 콘솔에는 로그인할 수 없습니다.

비밀 키 재발급

모든 사용자는 2단계 인증에 사용된 비밀 키를 재발급할 수 있습니다. 사용자가 재발급된 비밀 키로 중앙 관리 서버에 로그인하면 사용자 계정에 대해 새 비밀 키가 저장됩니다. 사용자가 새 비밀 키를 잘못 입력하면 새 비밀 키가 저장되지 않고 현재 비밀 키가 유지됩니다.

보안 코드에는 *발행자 이름*이라는 식별자가 있습니다. 보안 코드 발행자 이름은 인증 앱에서 중앙 관리 서버의 식별자로 사용됩니다. 보안 코드 발행자 이름에는 중앙 관리 서버의 이름과 동일한 기본값이 있습니다. 보안 코드 발행자 이름을 변경할 수 있습니다. 보안 코드 발행자 이름을 변경하면 새 비밀 키를 발행하여 인증 앱에 전달해야 합니다.

본인 계정의 2단계 인증 활성화(웹 콘솔)

자신의 계정에 대해서만 2단계 인증을 활성화할 수 있습니다.

본인 계정에 2단계 인증을 활성화하기 전에 모바일 기기에 인증 앱을 설치했는지 확인하십시오. 인증 앱에서 설정된 시간이 중앙 관리 서버를 설치한 기기에 설정된 시간으로 동기화되었는지 확인하십시오.

사용자 계정에 대한 2단계 인증 활성화하기:

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. 계정 이름을 누릅니다.
3. 사용자 설정 창이 열리면 **인증 보안** 탭을 선택합니다.
4. **인증 보안** 탭에서 다음을 수행합니다:
   a. **사용자 이름, 암호 및 보안 코드 요청(2단계 인증)** 옵션을 선택합니다. **저장** 버튼을 누릅니다.
   b. 2단계 인증 창이 열리면 **2단계 인증 설정 방법 보기**를 클릭합니다.
      인증 앱에 비밀 키를 입력하거나 **QR 코드 보기**를 클릭하고 모바일 기기의 인증 애플리케이션으로 QR 코드를 스캔하여 일회성 보안 코드를 받습니다.
   c. 2단계 인증 창이 열리면 인증 앱에서 생성한 보안 코드를 지정한 다음 **확인 및 적용** 버튼을 클릭합니다.
5. **저장** 버튼을 누릅니다.

계정에 대한 2단계 인증이 활성화됩니다.

본인 계정의 2단계 인증 활성화(MMC 기반)

본인 계정에 2단계 인증을 활성화하기 전에 모바일 기기에 인증 앱을 설치했는지 확인하십시오. 인증 앱에 설정된 시간과 중앙 관리 서버의 시간을 동기화해야 합니다.

본인 계정에 대한 2단계 인증을 활성화하려면:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창에서 **섹션** 창으로 이동한 다음 **고급** 및 **2단계 인증**을 차례로 선택합니다.
3. **2단계 인증** 섹션에서 **설정** 버튼을 클릭합니다.

   계정에 대해 이미 2단계 인증이 활성화된 경우 **설정** 버튼을 클릭하면 2단계 인증을 재구성할 수 있도록 비밀 키가 재설정됩니다.

   2단계 인증 속성 창이 열리면 비밀 키가 표시됩니다.

4. 일회용 보안 코드를 받으려면 인증 앱에 비밀 키를 입력합니다. 인증 앱에서 수동으로 비밀 키를 지정하거나 사용자 모바일 기기의 인증 앱에서 QR 코드를 스캔할 수 있습니다.

5. 인증 앱에서 생성된 보안 코드를 지정한 다음 **확인** 버튼을 클릭하여 2단계 인증 속성 창을 종료합니다.

6. **적용** 버튼을 클릭합니다.

7. **확인** 버튼을 누릅니다.

본인 계정에 대한 2단계 인증이 활성화되었습니다.

모든 사용자의 필수 2단계 인증 활성화(웹 콘솔)

계정의 **일반 기능: 사용자 권한** 기능 영역에 개체 ACL 수정 권한이 있고 2단계 인증을 사용하여 인증된 경우 중앙 관리 서버의 모든 사용자에 대해 2단계 인증을 활성화할 수 있습니다.

모든 사용자에 대해 2단계 인증을 활성화하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.

2. 속성 창의 **인증 보안** 탭에서 **모든 사용자에 대한 2단계 인증** 옵션의 토글 버튼을 활성화된 위치로 전환합니다.

3. 본인 계정에 2단계 인증을 활성화하지 않았다면, 애플리케이션에서 본인 계정에 2단계 인증을 활성화하는 창이 열립니다.

   a. 2단계 인증 창에서 **2단계 인증 설정 방법 보기**를 클릭합니다.

   b. 인증 애플리케이션에 비밀 키를 직접 입력하거나 **QR 코드 보기**를 클릭하고 모바일 기기의 인증 애플리케이션으로 QR 코드를 스캔하여 일회성 보안 코드를 받습니다.

   c. 2단계 인증 창이 열리면 인증 애플리케이션에서 생성한 보안 코드를 지정한 다음 **확인 및 적용** 버튼을 클릭합니다.

모든 사용자에게 대해 2단계 인증이 활성화되었습니다. 이제 2단계 인증에서 제외된 사용자를 제외하고, 모든 사용자에 대한 2단계 인증 활성화 이후 추가된 사용자를 포함하여 중앙 관리 서버의 사용자들은 계정에 2단계 인증을 구성해야 합니다.

모든 사용자의 2단계 인증 활성화(MMC 기반)

계정의 **일반 기능: 사용자 권한** 기능 영역에 개체 ACL 수정 권한이 있고 2단계 인증을 사용하여 인증된 경우 중앙 관리 서버의 모든 사용자에 대해 2단계 인증을 활성화할 수 있습니다.

모든 사용자에 대해 2단계 인증을 활성화하려면:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.

2. 중앙 관리 서버 속성 창의 **섹션** 창에서 **고급**와 **2단계 인증**을 차례로 선택합니다.

3. **필수로 설정** 버튼을 클릭하여 모든 사용자에 대해 2단계 인증을 활성화합니다.

4. 본인 계정에 2단계 인증을 활성화하지 않았다면, 애플리케이션에서 본인 계정에 2단계 인증을 활성화하는 창이 열립니다.

   a. 일회용 보안 코드를 받으려면 인증 앱에 비밀 키를 입력합니다. 인증 앱에 비밀 키를 수동으로 지정하거나 모바일 기기의 인증 앱으로 QR 코드를 스캔하여 일회성 보안 코드를 받을 수 있습니다.

   b. 인증 앱에서 생성된 보안 코드를 지정한 다음 **확인** 버튼을 클릭하여 2단계 인증 속성 창을 종료합니다.

5. **2단계 인증** 섹션에서 **적용** 버튼을 클릭하고 **확인** 버튼을 클릭합니다.

모든 사용자에게 대해 2단계 인증이 활성화되었습니다. 이제 계정이 2단계 인증에서 제외된 사용자를 제외하고, 이 옵션 활성화 이후 추가된 사용자를 포함하여 중앙 관리 서버의 모든 사용자는 계정에 2단계 인증을 구성해야 합니다.

사용자 계정의 2단계 인증 비활성화(웹 콘솔)

본인 및 다른 사용자의 계정에 2단계 인증을 비활성화할 수 있습니다.

> 계정의 일반 기능: 사용자 권한 기능 영역에 **개체 ACL 수정** 권한이 있고 2단계 인증을 사용하여 인증된 경우 모든 사용자의 계정에 대해 2단계 인증을 비활성화할 수 있습니다.

사용자 계정에 대한 2단계 인증을 비활성화하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.

2. 2단계 인증을 비활성화할 내부 사용자 계정의 이름을 클릭합니다. 본인의 계정일 수도 있고 다른 사용자의 계정일 수도 있습니다.

3. 사용자 설정 창이 열리면 **계정 보호** 탭을 선택합니다.

4. 사용자 계정에 대한 2단계 인증을 비활성화하려면 **계정 보호** 탭에서 **사용자 이름과 암호만 요청** 옵션을 선택합니다.

5. **저장** 버튼을 누릅니다.

사용자 계정에 대한 2단계 인증이 비활성화되었습니다.

> 2단계 인증을 사용하여 Kaspersky Security Center 웹 콘솔에 로그인할 수 없는 사용자의 접근을 복원하려면 이 사용자 계정에 대한 2단계 인증을 비활성화한 후 위에서 설명한 것처럼 **사용자 이름과 암호만 요청** 옵션을 선택합니다. 그런 다음 2단계 인증을 비활성화한 사용자 계정으로 Kaspersky Security Center 웹 콘솔에 로그인한 후 다시 인증을 활성화합니다.

사용자 계정의 2단계 인증 비활성화(MMC 기반)

사용자 계정에 대한 2단계 인증을 비활성화하려면 다음과 같이 하십시오:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창의 **섹션** 창에서 **고급 2단계 인증**을 차례로 선택합니다.
3. **2단계 인증** 섹션에서 **비활성화** 버튼을 클릭합니다.
4. **적용** 버튼을 클릭합니다.
5. **확인** 버튼을 누릅니다.

계정에 대한 2단계 인증이 비활성화되었습니다.

다른 사용자 계정의 2단계 인증을 비활성화할 수 있습니다. 예를 들어 사용자의 모바일 기기가 분실 또는 파손된 경우 보호 기능을 제공합니다.

계정의 일반 기능: 사용자 권한 기능 영역에 **개체 ACL 수정** 권한이 있고 2단계 인증을 사용하여 인증된 경우에만 모든 사용자의 계정에 대해 2단계 인증을 비활성화할 수 있습니다. 아래 단계에 따라 본인 계정에도 2단계 인증을 비활성화할 수 있습니다.

사용자 계정에 대한 2단계 인증을 비활성화하려면 다음과 같이 하십시오:

1. 콘솔 트리에서 **사용자 계정** 폴더를 엽니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
2. 작업 영역에서 2단계 인증을 비활성화할 사용자 계정을 두 번 클릭합니다.
   2단계 인증이 활성화된 모든 사용자 계정의 경우 **2단계 인증 필요함** 열이 **예**로 설정됩니다.
3. **속성: <user name>** 창이 열리면 **2단계 인증** 섹션을 선택합니다.
4. **2단계 인증** 섹션에서 다음 옵션을 선택합니다.
   - 모든 사용자에 대해 2단계 인증을 비활성화하려면 **비활성화** 버튼을 클릭합니다.
   - 이 사용자 계정을 2단계 인증에서 제외하려면 **사용자 이름과 암호만으로도 인증을 통할 수 있음** 옵션을 선택합니다.
5. **적용** 버튼을 클릭합니다.
6. **확인** 버튼을 누릅니다.

사용자 계정에 대한 2단계 인증이 비활성화되었습니다.

2단계 확인을 사용하여 관리 콘솔에 로그인할 수 없는 사용자의 접근을 복원하려면 이 사용자 계정에 대한 2단계 확인을 비활성화하고 위에서 설명한 **2단계 인증**에서 **사용자 이름과 암호만으로도 인증을 통할 수 있음** 옵션을 선택합니다. 그런 다음 2단계 인증을 비활성화한 사용자 계정으로 관리 콘솔에 로그인한 후 다시 인증을 활성화합니다.

모든 사용자의 필수 2단계 인증 비활성화(웹 콘솔)

계정에 대해 필수 2단계 인증이 활성화되어 있고 계정의 일반 기능: 사용자 권한 기능 영역에서 **개체 ACL 수정** 권한이 있다면, 모든 사용자에 대해 2단계 인증을 비활성화할 수 있습니다. 자신의 계정에 대해 2단계 인증이 활성화되어 있지 않은 경우 모든 사용자에 대해 비활성화하기 전에 자신의 계정에 대해 2단계 인증을 먼저 활성화해야 합니다.

모든 사용자에 대해 2단계 인증을 비활성화하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. 속성 창의 **인증 보안** 탭에서 **모든 사용자에 대한 2단계 인증** 옵션의 토글 버튼을 비활성화된 위치로 전환합니다.

모든 사용자에 대해 2단계 인증이 비활성화됩니다. 이전에 2단계 인증을 별도로 활성화했던 특정 계정에는 모든 사용자에 대해 2단계 인증을 중지해도 적용되지 않습니다.

모든 사용자의 필수 2단계 인증 비활성화(MMC 기반)

일반 기능: 사용자 권한 기능 영역에 **개체 ACL 수정** 권한이 있고 2단계 인증을 사용하여 인증된 경우 중앙 관리 서버의 모든 사용자에 대해 필수 2단계 인증을 비활성화할 수 있습니다.

모든 사용자에 대해 2단계 인증을 비활성화하려면:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.
2. 중앙 관리 서버 속성 창의 **섹션** 창에서 **고급**와 **2단계 인증**을 차례로 선택합니다.
3. **선택 사항으로 설정** 버튼을 클릭하여 모든 사용자에 대한 2단계 인증을 비활성화합니다.
4. **2단계 인증** 섹션에서 **적용** 버튼을 클릭합니다.
5. **2단계 인증** 섹션에서 **확인** 튼을 클릭합니다.

모든 사용자에 대해 2단계 인증이 비활성화됩니다. 이전에 2단계 인증을 별도로 활성화했던 특정 계정에는 모든 사용자에 대해 2단계 인증을 중지해도 적용되지 않습니다.

2단계 인증에서 계정 제외(웹 콘솔)

사용자에게 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한이 있는 경우 2단계 인증에서 사용자 계정을 제외할 수 있습니다.

모든 사용자에 대한 2단계 인증 목록에서 사용자 계정이 제외된 경우 해당 사용자는 2단계 인증을 사용하지 않아도 됩니다.

> 인증 시 보안 코드를 전달할 수 없는 서비스 계정의 경우 2단계 인증에서 계정을 제외해야 할 수 있습니다.

2단계 인증에서 일부 사용자 계정을 제외하려는 경우 다음과 같이 하십시오.

1. Active Directory 계정을 제외하려면 먼저 Microsoft Active Directory 도메인 컨트롤러 검색을 수행해야 중앙 관리 서버 사용자 목록을 새로 고칠 수 있습니다.
2. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
3. 속성 창의 **인증 보안** 탭에 있는 2단계 인증 제외 표에서 **추가** 버튼을 누릅니다.
4. 창이 열리면 다음과 같이 합니다.
   a. 제외할 사용자 계정을 선택합니다.
   b. **확인** 버튼을 누릅니다.

선택한 사용자 계정은 2단계 인증에서 제외됩니다.

2단계 인증에서 계정 제외(MMC 기반)

계정에 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한이 있는 경우 2단계 인증에서 계정을 제외할 수 있습니다.

사용자 계정이 2단계 인증에서 제외되면, 2단계 인증을 사용하지 않고도 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에 로그인할 수 있습니다.

> 인증 시 보안 코드를 전달할 수 없는 서비스 계정의 경우 2단계 인증에서 계정을 제외해야 할 수 있습니다.

2단계 인증에서 사용자 계정을 제외하려면:

1. Active Directory 계정을 제외하려면 Active Directory 폴링을 수행하여 중앙 관리 서버 사용자 목록을 새로 고칩니다.
2. 콘솔 트리에서 **사용자 계정** 폴더를 엽니다.
   기본적으로 **사용자 계정** 폴더는 **고급** 폴더의 하위 폴더입니다.
3. 작업 영역에서 2단계 인증에서 제외할 사용자 계정을 두 번 클릭합니다.
4. **속성: <user name>** 창이 열리면 **2단계 인증** 섹션을 선택합니다.

5. 섹션이 열리면 **사용자 이름과 암호만으로도 인증을 통할 수 있음** 옵션을 선택합니다.

6. **2단계 인증** 섹션에서 **적용** 버튼을 클릭하고 **확인** 버튼을 클릭합니다.

이 사용자 계정은 2단계 인증에서 제외됩니다. 사용자 계정 목록에서 제외된 계정을 확인할 수 있습니다.

보안 코드 발행자 이름 편집(웹 콘솔)

서로 다른 중앙 관리 서버에 대한 여러 식별자(발행자라고 함)가 있을 수 있습니다. 예를 들어 중앙 관리 서버에서 다른 중앙 관리 서버의 보안 코드 발행자와 유사한 이름을 사용하고 있는 경우 보안 코드 발행자의 이름을 변경할 수 있습니다. 기본적으로 보안 코드 발행자의 이름은 중앙 관리 서버의 이름과 동일합니다.

보안 코드 발행자 이름을 변경한 후에는 새 비밀 키를 재발급하여 인증 앱에 전달해야 합니다.

보안 코드 발행자의 새 이름을 지정하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.

2. 사용자 설정 창이 열리면 **계정 보호** 탭을 선택합니다.

3. **계정 보호** 탭에서 **편집** 링크를 누릅니다.
   보안 코드 발행자 편집 섹션이 열립니다.

4. 새 보안 코드 발행자 이름을 지정합니다.

5. **확인** 버튼을 누릅니다.

중앙 관리 서버에 대한 새 보안 코드 발행자 이름이 지정됩니다.

보안 코드 발행자 이름 편집(MMC 기반)

서로 다른 중앙 관리 서버에 대한 여러 식별자(발행자라고 함)가 있을 수 있습니다. 예를 들어 중앙 관리 서버에서 다른 중앙 관리 서버의 보안 코드 발행자와 유사한 이름을 사용하고 있는 경우 보안 코드 발행자의 이름을 변경할 수 있습니다. 기본적으로 보안 코드 발행자의 이름은 중앙 관리 서버의 이름과 동일합니다.

보안 코드 발행자 이름을 변경한 후에는 새 비밀 키를 재발급하여 인증 앱에 전달해야 합니다.

보안 코드 발행자의 새 이름을 지정하려면:

1. Kaspersky Security Center 콘솔 트리에서 **중앙 관리 서버** 폴더의 마우스 오른쪽 메뉴를 열고 **속성**을 선택합니다.

2. 중앙 관리 서버 속성 창의 **섹션** 창에서 **고급**와 **2단계 인증**을 차례로 선택합니다.

3. **보안 코드 발행자** 필드에서 새 보안 코드 발행자 이름을 지정합니다.

4. **2단계 인증** 섹션에서 **적용** 버튼을 클릭합니다.

5. **2단계 인증** 섹션에서 **확인** 튼을 클릭합니다.

중앙 관리 서버에 대한 새 보안 코드 발행자 이름이 지정됩니다.

본인 계정의 2단계 인증 구성(웹 콘솔)

2단계 인증을 활성화한 후 처음으로 Kaspersky Security Center에 로그인하면 자신의 계정에 대한 2단계 인증을 구성하는 창이 열립니다.

본인 계정에 2단계 인증을 구성하기 전에 모바일 기기에 인증 앱을 설치했는지 확인하십시오.

인증 앱이 있는 기기의 시간과 중앙 관리 서버가 있는 기기의 시간이 외부 시간 소스를 사용하여 UTC로 동기화되었는지 확인합니다.

본인 계정에 대한 2단계 인증을 구성하려면:

1. 모바일 기기의 인증 앱으로 일회용 보안 코드를 생성합니다. 이렇게 하려면 다음 중 하나를 수행합니다.

   - 인증 앱에 비밀 키를 직접 입력합니다.
   - **QR 코드 보기**를 클릭하고 인증 앱을 사용하여 QR 코드를 스캔합니다.

   모바일 기기에 보안 코드가 표시됩니다.

2. 2단계 인증 구성 창이 열리면 인증 앱에서 생성한 보안 코드를 입력한 다음 **확인 및 적용** 버튼을 클릭합니다.

   계정에 대한 2단계 인증을 구성했습니다. 귀하는 귀하의 권한에 따라 중앙 관리 서버에 접근할 수 있습니다.

본인 계정의 2단계 인증 구성(MMC-기반)

2단계 인증을 활성화한 후 처음으로 Kaspersky Security Center에 로그인하면 자신의 계정에 대한 2단계 인증을 구성하는 창이 열립니다.

본인 계정에 2단계 인증을 구성하기 전에 모바일 기기에 인증 앱을 설치했는지 확인하십시오. 인증 앱이 있는 기기의 시간과 중앙 관리 서버가 있는 기기의 시간이 외부 시간 소스를 사용하여 UTC로 동기화되었는지 확인합니다.

본인 계정에 대한 2단계 인증을 구성하려면:

1. 모바일 기기의 인증 앱으로 일회용 보안 코드를 생성합니다. 이렇게 하려면 다음 중 하나를 수행합니다.

   - 인증 앱에 비밀 키를 직접 입력합니다.
   - 인증 앱을 사용하여 QR 코드를 스캔합니다.

모바일 기기에 보안 코드가 표시됩니다.

2. **2단계 인증 설정** 창이 열리면 인증 앱에서 생성한 보안 코드를 지정한 다음 **확인** 버튼을 클릭합니다.

계정에 대한 2단계 인증을 구성했습니다. 귀하는 귀하의 권한에 따라 중앙 관리 서버에 접근할 수 있습니다.

새 비밀 키 생성

2단계 인증을 사용하여 인증된 경우에만 계정에 대한 2단계 인증용 새 비밀 키를 생성할 수 있습니다.

사용자 계정에 대한 새 비밀 키 생성하기:

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. 2단계 인증용 새 비밀 키를 생성하려는 사용자 계정의 이름을 누릅니다.
3. 사용자 설정 창이 열리면 **계정 보호** 탭을 선택합니다.
4. **계정 보호** 탭에서 **새 비밀 키 생성** 링크를 누릅니다.
5. 2단계 인증 창이 열리면 인증 앱에서 생성한 새 보안 키를 지정합니다.
6. **확인 및 적용** 버튼을 클릭합니다.

사용자의 새 비밀 키가 생성됩니다.

모바일 기기 분실 시 다른 모바일 기기에 인증 앱을 설치하고 새 비밀 키를 생성하여 Kaspersky Security Center 웹 콘솔에 대한 접근 권한을 복원할 수 있습니다.

신규 사용자가 스스로 2단계 인증을 설정하지 못하도록 금지

Kaspersky Security Center 웹 콘솔 접근 보안을 더욱 개선하기 위해 신규 사용자가 스스로 2단계 인증을 설정하지 못하도록 금지할 수 있습니다.

이 옵션이 활성화되면 새 도메인 관리자 등 2단계 인증이 비활성화된 사용자는 직접 2단계 인증을 구성할 수 없습니다. 따라서 이러한 사용자는 이미 2단계 인증을 활성화한 다른 Kaspersky Security Center 관리자의 승인 없이는 중앙 관리 서버에서 인증을 받을 수 없으며 Kaspersky Security Center 웹 콘솔에 로그인할 수 없습니다.

이 옵션은 모든 사용자에 대해 2단계 인증이 활성화되면 사용할 수 있습니다.

신규 사용자가 스스로 2단계 인증을 설정하지 못하도록 하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. 속성 창의 **인증 보안** 탭에서 **신규 사용자가 2단계 인증을 설정하지 못하도록 제한** 토글 버튼을 활성화 위치로 전환합니다.

이 옵션은 2단계 인증 제외에 추가된 사용자 계정에는 영향을 주지 않습니다.

2단계 인증이 비활성화된 사용자에게 Kaspersky Security Center 웹 콘솔 접근 권한을 부여하려면 **신규 사용자가 2단계 인증을 설정하지 못하도록 제한** 옵션을 일시적으로 끄고 사용자에게 2단계 인증을 활성화하도록 요청한 다음 옵션을 다시 켜십시오.

네트워크 에이전트 설치 후 사용자를 Linux 기기 소유자로 할당

사용자를 Linux 기기 소유자로 등록하도록 허용하려면:

1. Kaspersky Security Center 웹 콘솔에서 **발견 및 배포** → **배포 및 할당** → **설치 패키지**로 이동합니다.
   설치 패키지 목록이 열립니다.
2. 네트워크 에이전트 설치 패키지를 클릭합니다.
   설치 패키지의 속성 창이 열립니다.
3. 설치 패키지 속성 창에서 **설정** → **고급**을 클릭합니다.
4. **기기 소유자로 사용자 등록(Linux만)** 섹션에서 **네트워크 에이전트 설치 후 사용자 등록 유틸리티 실행 허용**을 켜고 **저장**을 클릭합니다.

사용자를 기기 소유자로 등록하는 유틸리티는 클라이언트 기기에서 명령줄로 실행할 수 있습니다.

클라이언트 기기에서 사용자를 Linux 기기 소유자로 등록하려면:

1. 클라이언트 기기의 명령줄에서 다음 명령을 실행합니다:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```
2. 메시지가 표시되면 로그인과 암호를 입력합니다.
   네트워크 에이전트의 응답 파일 또는 설치 패키지에 아이디와 암호가 포함된다면, 클라이언트 기기의 명령줄에서 다음 명령을 실행합니다:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

사용자가 내부 보안 그룹에 포함된다면 로그인에 사용자 이름을 포함해야 합니다.

사용자가 Active Directory 보안 그룹에 포함된다면 로그인에 사용자 이름과 도메인 이름을 포함해야 합니다.

사용자에 대해 2단계 인증이 켜져 있으면 앱에서 시간 기반 일회성 암호(TOTP)를 입력해야 합니다.

사용자가 기기 소유자로 등록됩니다.

사용자 또는 보안 그룹 삭제

내부 사용자 또는 내부 보안 그룹만 삭제할 수 있습니다.

사용자 또는 보안 그룹을 삭제하려면 다음 단계를 따릅니다.

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 또는 **그룹** 탭을 선택합니다.
2. 삭제할 사용자 또는 보안 그룹 옆의 확인란을 선택합니다.

3. **삭제**를 클릭합니다.

4. 확인 창이 열리면 **확인**를 누릅니다.

   사용자 또는 보안 그룹이 삭제됩니다.

사용자 계정의 암호 변경

현재 암호가 곧 만료되거나 더 안전한 암호로 변경하고자 한다면, 자신의 계정이나 다른 사용자 계정의 암호를 변경해야 할 수 있습니다.

암호는 다음 규칙을 따라야 합니다:

- 암호는 8자에서 256자 사이여야 합니다.
- 암호는 아래에 나와 있는 그룹 중 3개 이상의 문자를 포함해야 합니다:
  - 대문자(A-Z)
  - 소문자(a-z)
  - 숫자(0-9)
  - 특수 문자(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- 암호는 공백, 유니코드 문자 또는 "." 및 "@"의 조합("."이 "@" 앞에 오는 경우)을 포함할 수 없습니다.

자신의 계정 암호 변경

계정 암호를 편집하려면:

1. 메인 메뉴에서 계정 설정으로 이동하여 **암호 변경**을 선택합니다.

2. 현재 암호를 입력한 다음 Kaspersky Security Center 연결을 위한 새 암호를 지정합니다.
   입력한 암호를 보려면 을(를) 클릭합니다.

3. 계정의 무단 수정을 방지 중이라면, 이 계정의 변경 권한이 있는지 확인해야 합니다. **계정 보호** 창의 일반 기능: 사용자 권한 기능 영역에서 본인의 계정이나 개체 ACL 수정 권한이 있는 계정의 자격 증명을 지정합니다.

4. 이전 단계에서 사용한 계정에 2단계 인증을 활성화했다면 모바일 기기의 인증 앱에서 생성한 보안 코드를 입력합니다.

내부 사용자 계정의 암호 변경

내부 사용자 계정의 암호를 편집하려면:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 탭을 선택합니다.

2. 편집할 사용자 계정의 이름을 누릅니다.

3. 사용자 설정 창이 열리면 **일반** 탭에서 **암호 변경** 버튼을 클릭합니다.

4. Kaspersky Security Center에 사용자를 연결하기 위한 새 암호를 설정합니다.
   입력한 암호를 보려면 을(를) 클릭합니다.

5. 필요하다면 **첫 로그인 시 암호를 변경해야 합니다** 옵션을 사용하여 다음 사용자 인증 시 암호 변경을 강제할 수 있습니다.

6. 사용자 계정의 무단 수정을 방지 중이라면, 이 계정의 변경 권한이 있는지 확인해야 합니다. **계정 보호** 창의 일반 기능: 사용자 권한 기능 영역에서 개체 ACL 수정 권한이 있는 계정의 자격 증명을 지정합니다.

7. 이전 단계에서 사용한 계정에 2단계 인증을 활성화했다면 모바일 기기의 인증 앱에서 생성한 보안 코드를 입력합니다.

서버 플래그를 사용하여 암호 변경 옵션 구성

klscflag 유틸리티에서 다음 명령으로 암호 변경을 구성할 수 있습니다:

- 암호 순환 기간 구성(`LP_SplPwdChangePeriodDays` 플래그)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <순환_기간>
  ```

  <순환_기간>는 사용자 암호가 만료되는 기간의 일수입니다. 가능한 값: 0~730. 파라미터 값이 0이면 암호를 교체하지 않습니다.

- 암호 변경의 필요성에 대한 이전 경고 시간 구성(`LP_SplPwdChangeNotificationHours` 플래그)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <경고_시간>
  ```

  <경고_시간>는 사용자 암호 만료까지 남은 시간입니다. 이 시간에 암호를 변경해야 한다는 알림이 표시됩니다. 가능한 값: 0~17520. 파라미터 값이 0이면 경고 시간은 암호 순환 기간의 25%입니다.

- **첫 로그인 시 암호를 변경해야 합니다** 옵션의 기본값 지정(`LP_SplPwdForceChange` 플래그)

  ```
  klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <값>
  ```

  <값> 플래그의 가능한 값:

  `1`—**첫 로그인 시 암호를 변경해야 합니다** 옵션이 활성화됨.

  `0`—**첫 로그인 시 암호를 변경해야 합니다** 옵션이 비활성화됨.

현재 플래그 값을 보려면 다음 명령을 실행합니다:

```
klscflag.exe -fget -pv .core/.independent -s KLLIM -n <플래그> -t d
```

<플래그>는 `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours`, `LP_SplPwdForceChange` 중 하나의 플래그입니다.

사용자 역할 생성

사용자 역할을 생성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할** → **역할**로 이동합니다.

2. **추가**를 누릅니다.

3. **새 역할 이름** 창이 열리면 새 역할의 이름을 입력합니다.

4. **확인**을 눌러 변경을 적용합니다.

5. 역할 속성 창이 열리면 역할의 설정을 변경합니다.

   - **일반** 탭에서 역할 이름을 편집합니다.
     미리 정의된 역할의 이름은 편집할 수 없습니다.
   - **설정** 탭에서 역할과 연결된 정책과 프로필 및 역할 범위를 편집합니다.
   - **접근 권한** 탭에서 Kaspersky 애플리케이션 접근 권한을 편집합니다.

6. **저장**을 눌러 변경 사항을 저장합니다.

새 역할이 사용자 역할 목록에 표시됩니다.

사용자 역할 편집

사용자 역할을 편집하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할** → **역할**로 이동합니다.

2. 편집할 역할의 이름을 누릅니다.

3. 역할 속성 창이 열리면 역할의 설정을 변경합니다.

   - **일반** 탭에서 역할 이름을 편집합니다.
     미리 정의된 역할의 이름은 편집할 수 없습니다.
   - **설정** 탭에서 역할과 연결된 정책과 프로필 및 역할 범위를 편집합니다.
   - **접근 권한** 탭에서 Kaspersky 애플리케이션 접근 권한을 편집합니다.

4. **저장**을 눌러 변경 사항을 저장합니다.

업데이트된 역할이 사용자 역할 목록에 표시됩니다.

사용자 역할의 범위 편집

*사용자 역할 범위*는 사용자와 관리 그룹의 조합입니다. 사용자 역할과 연결된 설정은 이 역할이 지정된 사용자 소유의 기기가 이 역할과 연결된 그룹(자식 그룹 포함)에 속하는 경우에만 해당 기기에 적용됩니다.

사용자 역할 범위에 사용자, 보안 그룹 및 관리 그룹을 추가하려는 경우 다음 방법 중 하나를 사용할 수 있습니다.

방법 1:

1. 기본 메뉴에서 **사용자 및 역할** → **사용자 및 그룹**으로 이동한 다음 **사용자** 또는 **그룹** 탭을 선택합니다.

2. 사용자 역할 범위에 추가할 사용자 또는 보안 그룹 옆의 확인란을 선택합니다.

3. **역할 할당** 버튼을 누릅니다.
   역할 할당 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

4. **역할 선택** 단계에서 할당할 사용자 역할을 선택합니다.

5. **범위 정의** 단계에서 사용자 역할 범위에 추가할 관리 그룹을 선택합니다.

6. **역할 할당** 버튼을 클릭하여 마법사를 닫습니다.

선택한 사용자 또는 보안 그룹과 선택한 관리 그룹이 사용자 역할의 범위에 추가됩니다.

방법 2:

1. 메인 메뉴에서 **사용자 및 역할** → **역할**로 이동합니다.

2. 범위를 정의할 역할의 이름을 누릅니다.

3. 역할 속성 창이 열리면 **설정** 탭을 선택합니다.

4. **역할 범위** 섹션에서 **추가**를 누릅니다.
   역할 할당 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

5. **범위 정의** 단계에서 사용자 역할 범위에 추가할 관리 그룹을 선택합니다.

6. **사용자 선택** 단계에서 사용자 역할 범위에 추가할 사용자 및 보안 그룹을 선택합니다.

7. **역할 할당** 버튼을 클릭하여 마법사를 닫습니다.

8. **닫기** 버튼(✕)을 눌러 역할 속성 창을 닫습니다.

선택한 사용자 또는 보안 그룹과 선택한 관리 그룹이 사용자 역할의 범위에 추가됩니다.

방법 3:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.

2. **접근 권한** 탭에서 사용자 역할 범위에 추가할 사용자나 보안 그룹 이름 옆의 확인란을 선택하고 **역할** 버튼을 클릭합니다.
   여러 사용자 또는 보안 그룹을 동시에 선택할 수는 없습니다. 하나 이상 선택하면 **역할** 버튼이 비활성화됩니다.

3. **역할** 창에서 할당할 사용자 역할을 선택한 후 변경 사항을 적용하고 저장합니다.
   선택한 사용자나 보안 그룹이 사용자 역할 범위에 추가됩니다.

사용자 역할 삭제

사용자 역할을 삭제하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할** → **역할**로 이동합니다.

2. 삭제할 역할 이름 옆의 확인란을 선택합니다.

3. **삭제**를 클릭합니다.

4. 확인 창이 열리면 **확인**를 누릅니다.

사용자 역할이 삭제됩니다.

정책 프로필과 역할 연결

사용자 역할을 정책 프로필과 연결할 수 있습니다. 이 경우 해당 정책 프로필의 활성화 규칙은 역할을 기준으로 합니다. 즉, 지정된 역할의 사용자에 대해 정책 프로필이 활성화됩니다.

예를 들어, 특정 정책은 관리 그룹의 모든 기기에 대해 GPS 내비게이션 소프트웨어 실행을 금지합니다. GPS 내비게이션 소프트웨어는 사용자 관리 그룹에 있는 하나의 기기, 특히 배달원이 소유한 기기에 필요합니다. 이 경우 기기 소유자에게 '배달원' 역할을 할당한 다음 소유자에게 '배달원' 역할이 할당된 기기에서만 GPS 내비게이션 소프트웨어 실행을 허용하는 정책 프로필을 만들 수 있습니다. 기타 정책 설정은 모두 보존됩니다. '배달원' 역할의 사용자만 GPS 내비게이션 소프트웨어를 실행할 수 있습니다. 나중에 다른 작업자에게 '배달원' 역할이 할당되면 새 작업자도 조직 기기에서 내비게이션 소프트웨어를 실행할 수 있습니다. 같은 관리 그룹의 다른 기기에서는 GPS 내비게이션 소프트웨어 실행이 계속 차단됩니다.

역할을 정책 프로필과 연결하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할** → **역할**로 이동합니다.

2. 정책 프로필과 연결할 역할의 이름을 누릅니다.
   일반 탭이 선택된 상태로 역할 속성 창이 열립니다.

3. **설정** 탭을 선택하고 아래쪽의 **정책 및 프로필** 섹션으로 스크롤합니다.

4. **편집**을 클릭합니다.

5. 다음과 같이 역할을 각 프로필에 연결합니다.

   - **기존 정책 프로필** - 필요한 정책 이름 옆의 펼침 단추 아이콘(>)을 누른 다음 역할을 연결할 프로필 옆의 확인란을 선택합니다.

   - **새 정책 프로필**:

     a. 프로필을 만들 정책 옆의 확인란을 선택합니다.

     b. **새 정책 프로필**을 클릭합니다.

     c. 새 프로필의 이름을 지정하고 프로필 설정을 구성합니다.

     d. **저장** 버튼을 누릅니다.

     e. 새 프로필 옆에 있는 확인란을 선택합니다.

6. **역할에 할당**을 누릅니다.

프로필이 역할에 연결되고 역할 속성에 표시됩니다. 소유자에게 해당 역할이 할당된 모든 기기에 프로필이 자동으로 적용됩니다.

보조 중앙 관리 서버에 사용자 역할 전파

기본적으로 기본 및 보조 중앙 관리 서버의 사용자 역할 목록은 서로 독립적입니다. 기본 중앙 관리 서버에서 생성된 사용자 역할을 모든 보조 중앙 관리 서버에 자동으로 전파하도록 애플리케이션을 구성할 수 있습니다. 보조 중앙 관리 서버에서 자체 보조 중앙 관리 서버로 사용자 역할을 전파할 수도 있습니다.

기본 중앙 관리 서버에서 보조 중앙 관리 서버로 사용자 역할을 전파하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   일반 탭이 선택된 상태로 중앙 관리 서버 속성 창이 열립니다.
2. **중앙 관리 서버 계층 구조** 섹션으로 이동합니다.
3. **보조 중앙 관리 서버로 역할 목록 전달** 옵션을 활성화한 다음 **저장** 버튼을 클릭합니다.

   애플리케이션이 기본 중앙 관리 서버에서 보조 중앙 관리 서버로 사용자 역할을 복사합니다.

보조 중앙 관리 서버로 역할 목록 전달 옵션이 활성화된 상태에서 전파하는 사용자 역할은 보조 중앙 관리 서버에서 편집하거나 삭제할 수 없습니다. 기본 중앙 관리 서버에서 새 역할을 생성하거나 기존 역할을 편집하면 변경 내용이 보조 중앙 관리 서버에 자동으로 복사됩니다. 기본 중앙 관리 서버에서 삭제하는 사용자 역할은 삭제 후에도 보조 중앙 관리 서버에 남아 있지만 편집되거나 삭제될 수 있습니다.

기본 중앙 관리 서버에서 보조 중앙 관리 서버로 전파되는 역할에는 녹색 체크 확인 표시(✓)가 표시됩니다. 이러한 역할은 보조 중앙 관리 서버에서 편집할 수 없습니다.

기본 중앙 관리 서버에서 역할을 생성했는데 보조 중앙 관리 서버에 이름이 같은 역할이 있으면 새 역할은 이름에 ~~1, ~~2와 같은 색인(랜덤일 수 있음)이 추가되어 보조 중앙 관리 서버로 복사됩니다.

보조 중앙 관리 서버로 역할 목록 전달 옵션을 비활성화하면 모든 사용자 역할은 보조 중앙 관리 서버에 유지되지만 기본 중앙 관리 서버와의 역할과는 독립적인 역할이 됩니다. 독립적인 역할이 된 보조 중앙 관리 서버의 사용자 역할은 편집하거나 삭제할 수 있습니다.

계정 암호 변경

예를 들어 사용자가 로컬 계정 암호를 잊어버렸거나 스케줄된 암호 변경을 수행하기 위해 로컬 계정 암호를 변경할 수 있습니다.

사용자가 계정에 로그인하지 않았어도 암호 변경이 적용됩니다. 로컬 루트 계정의 암호를 변경할 수도 있습니다.

> 이 작업은 Linux 기기에서만 수행할 수 있습니다.

특정 기기에서 로컬 계정 암호를 변경하려면:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다.
3. **작업 유형** 필드에서 **계정 암호 변경(Linux만)**을 선택합니다.

4. 다음 옵션 중 하나를 선택합니다:

- **관리 그룹에 작업 할당**

  관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

  예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

  관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

- **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

  작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

  특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

- **기기 선택 결과에 작업 할당**

  기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

  예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

지정한 기기에 대해 *계정 암호 변경(Linux만 해당)* 작업이 생성됩니다. **관리 그룹에 작업 할당** 옵션 선택 시, 작업은 그룹 1입니다.

5. **작업 범위** 단계에서 관리 그룹, 특정 주소가 있는 기기 또는 기기 선택을 지정합니다.

   사용 가능한 설정은 이전 단계에서 선택한 옵션에 따라 다릅니다.

6. **계정 이름과 신규 암호 입력** 단계에서 다음 설정을 지정합니다.

   - **계정 이름** 필드에서 암호를 변경할 계정의 이름을 지정합니다.
   - **새 암호** 필드에 이전 필드에서 지정한 계정에 설정할 암호를 지정합니다.

     입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.
   - 필요하다면 **일회용 암호로 설정(첫 로그인 후 사용자가 암호를 변경해야 함)** 확인란을 선택합니다.

     - **일회용 암호로 설정(첫 로그인 후 사용자가 암호를 변경해야 함)**

       이 확인란을 선택하면 최초 로그인 시 새 암호를 설정하라는 메시지가 표시됩니다.

       이 확인란을 선택 취소하면 최초 로그인 후 새 암호를 설정하라는 메시지가 표시되지 않습니다.

       기본적으로 이 확인란은 선택되어 있지 않습니다.

7. **작업 생성 마침** 단계에서 **마침** 버튼을 클릭하여 작업을 생성하고 마법사를 종료합니다.

   생성이 완료되면 작업 세부 정보 열기 옵션을 활성화하면 작업 설정 창이 열립니다. 필요하다면 이 창에서 작업 매개변수를 확인하고 수정하거나 작업 시작 일정을 구성할 수 있습니다.

8. 작업 목록에서 생성한 작업을 선택한 다음 **시작**을 클릭합니다.
   또는 작업 설정에서 지정한 일정에 따라 작업이 시작될 때까지 기다립니다.

계정 암호 변경 작업이 완료되면 지정된 기기에서 지정된 로컬 계정의 암호가 변경됩니다.

계정 암호 변경 작업이 올바르게 작동하려면 사용자 기기에서 SELinux를 비활성화해야 합니다.

로컬 관리자 권한 취소

계정에서 로컬 관리자 권한을 철회할 수 있습니다. 이를 통해 사용자 계정 보호를 한 단계 더 추가할 수 있습니다. 예를 들어 일회성 할당이 완료된 로컬 관리자 권한을 철회할 수 있습니다.

이 작업이 실행되면 지정된 로컬 계정이 로컬 관리자 그룹에 속하는지 확인합니다. 이러한 그룹은 네트워크 에이전트 정책 설정에서 정의합니다. 네트워크 에이전트 정책 설정에서 로컬 관리자 그룹 목록을 사용자 지정할 수 있습니다. **권한이 있는 기기 사용자에 대한 리포트(Linux만)**를 사용하여 권한 있는 사용자 계정 목록을 확인할 수도 있습니다.

이 작업은 Linux 기기에서만 수행할 수 있습니다.

특정 기기에 대한 로컬 관리자 권한을 철회하려면 다음을 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다.
3. **작업 유형** 필드에서 **로컬 관리자 권한 취소(Linux만)**를 선택합니다.
4. 다음 옵션 중 하나를 선택합니다:

   - **관리 그룹에 작업 할당**

     관리 그룹에 포함되는 기기에 작업이 할당됩니다. 기존 그룹 중 하나를 지정하거나 새 그룹을 생성할 수 있습니다.

     예를 들어 특정 관리 그룹에 포함된 기기 관련 메시지를 사용자에게 보내는 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

     관리 그룹에 할당한 작업은 해당 그룹의 보안 설정을 따르므로, 작업 속성 창에 **보안** 탭이 표시되지 않습니다.

   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

     작업을 할당할 기기의 NetBIOS 이름, DNS 이름, IP 주소 및 IP 서브넷을 지정할 수 있습니다.

     특정 서브넷에 대해 작업을 제외하려는 경우 이 옵션을 사용할 수 있습니다. 경리 직원의 기기에 특정 애플리케이션을 설치하거나 감염이 의심되는 서브넷의 기기를 검사하려는 경우를 예로 들 수 있습니다.

   - **기기 선택 결과에 작업 할당**

     기기 선택에 포함되는 기기에 작업이 할당됩니다. 기존 조회 중 하나를 지정할 수 있습니다.

예를 들어 특정 운영 체제 버전이 설치된 기기에서 작업을 실행하려는 경우 이 옵션을 사용할 수 있습니다.

지정한 기기에 대해 *로컬 관리자 권한 취소(Linux만 해당)* 작업이 생성됩니다. **관리 그룹에 작업 할당** 옵션 선택 시, 작업은 그룹 1입니다.

5. **작업 범위** 단계에서 관리 그룹, 특정 주소가 있는 기기 또는 기기 선택을 지정합니다.
   사용 가능한 설정은 이전 단계에서 선택한 옵션에 따라 다릅니다.

6. 마법사의 이 단계에서 다음 설정을 지정합니다.

   - **운영 모드** 설정 그룹에서 운영 모드를 선택합니다.

     - **목록의 계정에서 로컬 관리자 권한 취소**

       이 옵션을 선택하면 지정한 로컬 계정에서 로컬 관리자 권한이 취소됩니다.
       기본적으로 이 옵션은 선택되어 있습니다.

     - **로컬 관리자 권한 취소에서 목록의 계정을 제외**

       이 옵션을 선택하면 지정된 로컬 계정을 제외한 모든 로컬 계정에서 로컬 관리자 권한이 취소됩니다.
       기본적으로 이 옵션은 선택되어 있지 않습니다.

   - 로컬 계정을 지정합니다.

     - **추가**를 누릅니다.

     - 창이 열리면 다음을 수행합니다.

       - **계정 이름** 필드에서 로컬 계정의 이름을 지정합니다.

       - **계정 처리** 설정 그룹(**목록의 계정에서 로컬 관리자 권한 취소** 옵션 선택 시에만 사용 가능)에서 작업을 선택합니다.

       - **계정 유지**

         이 옵션을 선택하면 로컬 관리자 권한 취소 후에도 로컬 계정이 삭제되지 않습니다.
         기본적으로 이 옵션은 선택되어 있습니다.

       - **계정 삭제**

         이 옵션을 선택하면 로컬 관리자 권한 여부에 관계없이 로컬 계정이 삭제됩니다.
         기본적으로 이 옵션은 선택되어 있지 않습니다.

7. **작업 생성 마침** 단계에서 **마침** 버튼을 클릭하여 작업을 생성하고 마법사를 종료합니다.
   생성이 완료되면 작업 세부 정보 열기 옵션을 활성화하면 작업 설정 창이 열립니다. 필요하다면 이 창에서 작업 매개변수를 확인하고 수정하거나 작업 시작 일정을 구성할 수 있습니다.

8. 작업 목록에서 생성한 작업을 선택한 다음 **시작**을 클릭합니다.
   또는 작업 설정에서 지정한 일정에 따라 작업이 시작될 때까지 기다립니다.

로컬 관리자 권한 취소 작업이 완료되면 지정된 기기의 지정된 로컬 계정에서 로컬 관리자 권한이 취소됩니다.

개체 리비전 관리

이 섹션에는 개체 리비전 관리에 대한 정보가 포함되어 있습니다. Kaspersky Security Center에서는 개체 수정 내용을 추적할 수 있습니다. 개체 변경 내용을 저장할 때마다 *리비전*이 만들어집니다. 각 리비전에는 번호가 있습니다.

리비전 관리를 지원하는 애플리케이션 개체는 다음과 같습니다:

- 중앙 관리 서버 속성
- 정책
- 작업
- 관리 그룹
- 사용자 계정
- 설치 패키지

개체 리비전에 대해 다음과 같은 작업을 수행할 수 있습니다:

- 선택한 리비전 보기(정책에만 사용 가능)
- 선택한 개체에 대한 리비전을 롤백
- 리비전을 JSON 파일로 저장(정책에만 사용 가능)

리비전 관리를 지원하는 개체의 속성 창 **리비전 내역** 섹션에는 다음 세부 정보가 포함된 개체 리비전 목록이 표시됩니다.

- **리비전** - 개체 리비전 번호.
- **시간** - 개체가 변경된 날짜와 시간.
- **사용자** - 개체를 변경한 사용자 이름.
- **사용자 기기 IP 주소** - 개체가 수정된 기기의 IP 주소.
- **웹 콘솔 IP 주소** - 개체가 수정된 Kaspersky Security Center 웹 콘솔의 IP 주소.
- **처리** - 개체에 실행한 조치.
- **설명** - 개체 설정 변경 사항 관련 리비전 설명.
  기본적으로 개체 리비전 설명은 비어 있습니다. 리비전에 설명을 추가하려면, 관련 리비전을 선택하고 **설명 편집** 버튼을 클릭합니다. 창이 열리면 리비전 관한 설명 텍스트를 입력합니다.

개체를 이전 리비전으로 롤백

필요한 경우 개체에 이뤄진 변경 사항을 롤백할 수 있습니다. 정책의 설정을 특정 날짜의 상태로 되돌려야 하는 경우를 예로 들 수 있습니다.

개체에 이뤄진 변경 사항을 롤백하려면 다음과 같이 하십시오:

1. 개체 속성 창에서 **리비전 내역** 탭을 엽니다.
2. 개체 리비전 목록에서 변경 사항을 롤백하려는 리비전을 선택합니다.
3. **롤백** 버튼을 클릭합니다.
4. **확인**을 눌러 동작을 허용합니다.

   그러면 개체가 선택한 리비전으로 롤백됩니다. 개체 리비전 목록에는 수행한 작업의 기록이 표시됩니다. 리비전 설명에는 개체를 되돌린 리비전의 번호에 대한 정보가 표시됩니다.

롤백 작업은 정책 및 작업 개체에만 사용할 수 있습니다.

리비전 설명 추가

Kaspersky Security Center에서는 개체 수정 내용을 추적할 수 있습니다. 개체 변경 내용을 저장할 때마다 리비전이 만들어집니다. 각 리비전에는 번호가 있습니다.

리비전의 설명을 추가하면 목록에서 리비전을 쉽게 검색할 수 있습니다.

리비전의 설명을 추가하려면 다음과 같이 하십시오:

1. 개체 속성 창에서 **리비전 내역** 탭을 엽니다.
2. 개체 리비전 목록에서 설명을 추가하기 원하는 리비전을 선택합니다.
3. **설명 편집** 버튼을 누릅니다.
   설명 창이 열립니다.
4. **설명** 창에서 리비전에 관한 설명 텍스트를 입력합니다.
   기본적으로 개체 리비전 설명은 비어 있습니다.
5. 개정 설명을 저장합니다.

개체의 리비전에 대한 설명이 추가됩니다.

정책 리비전 보기 및 저장

Kaspersky Security Center를 사용하면 특정 기간 내 정책에 어떤 수정 사항이 적용되었는지 확인할 수 있으며 이러한 수정 사항에 대한 정보를 파일에 저장할 수 있습니다.

해당 관리 웹 플러그인이 이 기능을 지원한다면 정책 리비전을 확인하고 저장할 수 있습니다.

정책 리비전을 확인하려면 다음을 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **정책 및 프로필**로 이동합니다.
2. 확인할 버전의 정책을 클릭한 다음 **리비전 내역** 섹션으로 이동합니다.
3. 리비전 내역 목록에서 확인할 정책의 번호를 클릭합니다.

   리비전 크기가 10 MB를 초과하면 Kaspersky Security Center 웹 콘솔을 사용하여 확인할 수 없습니다. 선택한 리비전을 JSON 파일에 저장하라는 메시지가 표시됩니다.

   리비전 크기가 10MB를 초과하지 않으면 선택한 정책 리비전의 설정이 포함된 HTML 형식 리포트가 표시됩니다. 리포트는 팝업 창으로 표시되므로 브라우저에서 팝업이 허용되는지 확인하십시오.

정책 리비전을 JSON 파일에 저장하려면:

정책 리비전 목록에서 저장할 리비전을 선택한 다음 **파일로 저장**을 클릭합니다.

리비전이 JSON 파일에 저장됩니다.

개체 삭제

이 섹션에서는 개체 삭제에 대한 정보를 제공합니다.

다음과 같은 개체를 삭제할 수 있습니다:

- 정책
- 작업
- 설치 패키지
- 가상 중앙 관리 서버
- 사용자
- 보안 그룹
- 관리 그룹

개체를 삭제하려면:

1. Kaspersky Security Center 웹 콘솔에서 필요한 섹션을 연 다음 개체를 선택합니다.
2. 툴바에서 **삭제** 버튼을 클릭합니다.
3. 창이 열리면 **확인** 버튼을 눌러 사용자의 선택을 확인합니다.

   선택한 규칙이 삭제됩니다.

개체를 삭제해도 개체에 대한 정보는 데이터베이스에 유지됩니다. 삭제된 개체 관련 정보의 저장 기간은 개체 리비전의 저장 기간과 동일합니다(권장 저장 기간은 90일). **삭제된 개체** 권한 영역에서 **수정** 권한이 있어야 저장 기간을 변경할 수 있습니다.

클라이언트 기기 삭제 정보

관리 그룹에서 관리 중인 기기를 삭제하면 애플리케이션이 해당 기기를 미할당 기기 그룹으로 이동합니다. 기기를 삭제한 후에도 설치된 Kaspersky 애플리케이션(네트워크 에이전트 및 Kaspersky Endpoint Security 등의 보안 애플리케이션)은 기기에 남아 있습니다.

Kaspersky Security Center는 다음 규칙에 따라 미할당 기기 그룹의 기기를 처리합니다.

- 장치 이동 규칙을 설정했고 장치가 이동 규칙의 기준을 충족한다면, 장치는 규칙에 따라 자동으로 관리 그룹으로 이동됩니다.
- 기기는 미할당 기기 그룹에 저장되며 기기 보관 규칙에 따라 그룹에서 자동으로 제거됩니다.

  기기 보관 규칙은 전체 디스크 암호화로 암호화된 하나 이상의 드라이브가 있는 기기에 영향을 주지 않습니다. 이러한 기기는 자동 삭제되지 않으며 수동으로만 삭제할 수 있습니다. 암호화된 드라이브가 있는 기기를 삭제해야 한다면, 먼저 드라이브를 복호화한 후 기기를 삭제하십시오.

  > 암호화된 드라이브가 있는 기기를 삭제하면 드라이브 복호화에 필요한 데이터도 함께 삭제됩니다. 기기를 삭제할 때(미할당 기기**미할당 기기**관리 중인 기기**관리 중인 기기 위험을 이해했으며 선택한 기기를 삭제하겠습니다** 확인란을 선택하면 해당 데이터 삭제에 동의하는 것입니다.

  드라이브를 복호화하려면 다음 조건을 충족해야 합니다.

  - 드라이브 복호화에 필요한 데이터 복원을 위해 기기를 중앙 관리 서버에 다시 연결합니다.
  - 기기 사용자가 복호화 암호를 기억합니다.
  - 드라이브를 암호화하는 데 사용된 보안 애플리케이션(예 : Kaspersky Endpoint Security for Windows)이 여전히 기기에 설치되어 있습니다.

  드라이브가 Kaspersky 디스크 암호화 기술로 암호화되었다면 FDERT 복원 유틸리티를 사용하여 데이터 복구를 시도할 수도 있습니다.

> VDI에서 암호화된 드라이브가 있는 장치를 삭제하면 암호화된 드라이브에 있는 정보가 삭제됩니다.

미할당 기기 그룹에서 기기를 수동으로 삭제하면 애플리케이션이 목록에서 기기를 제거합니다. 기기 삭제 후에도 설치된 Kaspersky 애플리케이션(있다면)은 기기에 남아 있습니다. 이때, 기기가 여전히 중앙 관리 서버에 표시되고 일반 네트워크 폴링을 구성했다면 Kaspersky Security Center는 네트워크 폴링 중에 기기를 검색하여 미할당 기기 그룹에 다시 추가합니다. 따라서 기기가 중앙 관리 서버에 보이지 않을 때만 기기를 직접 삭제하는 것이 좋습니다.

Kaspersky Security Network(KSN)

이 섹션에서는 KSN(Kaspersky Security Network)이라는 온라인 서비스 인프라를 사용하는 방법에 대한 설명이 제공됩니다. 해당 섹션에서는 KSN 관련 상세 정보와 KSN 사용 방법, KSN 접근을 구성하는 방법 및 KSN 프록시 서버 사용 통계를 확인하는 방법에 대한 지침이 제공됩니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)과 KSN 기능이 제공되지 않을 수도 있습니다.

KSN 정보

Kaspersky Security Network(KSN)은 파일, 웹 리소스 및 소프트웨어에 대한 정보가 포함된 Kaspersky의 온라인 기술 자료에 접속하도록 하는 온라인 서비스 인프라입니다. Kaspersky Security Network의 데이터를 사용하면 보안 위협이 발생할 때 Kaspersky 애플리케이션의 처리 속도가 더욱 빨라지며 일부 보호 구성 요소의 성능이 향상되고, 정상적인 개체를 바이러스로 탐지하는 위험은 줄어듭니다. KSN에서는 Kaspersky의 평판 데이터베이스를 사용하여 관리 중인 기기에 설치된 애플리케이션에 대한 정보를 검색할 수 있습니다.

Kaspersky Security Center는 다음 인프라 솔루션을 지원합니다:

- *KSN*은 Kaspersky Security Network와 정보를 교환할 수 있는 솔루션입니다. KSN에 참여하면 Kaspersky Security Center가 관리하는 클라이언트 기기에 설치된 Kaspersky 애플리케이션의 작동에 대한 정보를 Kaspersky에 자동 전송하는 데 동의하는 것입니다. 정보는 현재 구성된 KSN 접근 설정에 따라 전송됩니다. Kaspersky 분석가는 추가로 수신된 정보를 분석하여 Kaspersky Security Network의 평판 및 통계 데이터베이스에 포함합니다. Kaspersky Security Center는 기본적으로 이 솔루션을 사용합니다.

- *KPSN(Kaspersky Private Security Network)*은 Kaspersky 애플리케이션이 설치된 기기 사용자가 기기에서 Kaspersky Security Network으로 데이터를 보내지 않고도 글로벌 KSN의 평판 데이터베이스와 기타 통계 데이터에 접근할 수 있도록 하는 솔루션입니다. KPSN은 다음과 같은 이유로 Kaspersky Security Network에 참여할 수 없는 기업 고객용으로 제공됩니다:

  - 사용자 기기가 인터넷에 연결되어 있지 않습니다.
  - 국외 또는 기업 LAN 외부로의 데이터 전송이 법률이나 기업 보안 정책으로 금지되어 있습니다.

  중앙 관리 서버 속성 창의 **KSN 프록시 설정** 섹션에서 Kaspersky Private Security Network 진술문의 액세스 설정을 지정할 수 있습니다.

빠른 시작 마법사를 실행할 때 애플리케이션에서 KSN 참가 여부를 묻습니다. 애플리케이션을 사용할 때 언제든지 KSN 사용을 시작하거나 중지할 수 있습니다.

KSN을 활성화할 때 읽고 수락하는 KSN 성명서에 따라 KSN을 사용합니다. KSN 진술문이 업데이트되면, 중앙 관리 서버를 업데이트하거나 업그레이드할 때 표시됩니다. 업데이트된 KSN 성명서를 수락하거나 거부할 수 있습니다. 거부할 경우 이전에 수락한 이전 버전 KSN 성명서에 따라 KSN을 계속 사용합니다.

KSN이 활성화되면 Kaspersky Security Center가 KSN 서버에 액세스할 수 있는지 확인합니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다. 관리 중인 기기에 대한 보안 수준을 유지하는 데 필요합니다.

중앙 관리 서버를 통해 관리되는 클라이언트 기기는 KSN 프록시 서버를 통해 KSN과 상호 작용합니다. KSN 프록시는 다음 기능을 제공합니다:

- 클라이언트 기기에서 인터넷에 직접 접속할 수 없더라도 KSN으로 요청을 보내고, KSN에서 정보를 받아오고, KSN으로 정보를 전송할 수 있습니다.
- KSN 프록시 서버가 처리된 데이터를 캐시하므로 아웃바운드 채널의 부하 및 클라이언트 기기에서 요청한 정보를 기다리는 시간이 줄어듭니다.

중앙 관리 서버 속성 창의 **KSN 프록시 설정** 섹션에서 KSN 프록시 서버를 구성할 수 있습니다.

KSN에 대한 액세스 설정

중앙 관리 서버와 배포 지점에서 KSN(Kaspersky Security Network) 접근을 설정할 수 있습니다.

중앙 관리 서버의 KSN 접근을 설정하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **KSN 프록시 설정** 섹션을 선택합니다.
3. 토글 버튼을 **중앙 관리 서버에서 KSN 프록시 활성화 활성화됨** 위치로 전환합니다.
   이 옵션을 사용하면 KSN 프록시 서버가 KSN으로 데이터를 전송하여 Kaspersky Security Center 구성 요소의 효율성과 Kaspersky 애플리케이션의 성능을 개선합니다. 데이터는 클라이언트 기기에서 활성 상태인 Kaspersky Endpoint Security 정책에 따라 해당 기기에서 KSN으로 전송됩니다. 이 토글 버튼을 비활성화하면 중앙 관리 서버와 클라이언트 기기에서 Kaspersky Security Center를 통해 KSN으로 데이터를 전송하지 않습니다. 그러나 클라이언트 기기는 해당 설정에 따라 KSN으로 직접(Kaspersky Security Center를 바이패스) 데이터를 보낼 수 있습니다. 클라이언트 기기에서 활성화된 Kaspersky Endpoint Security 정책은 해당 기기에서 KSN으로 어떤 데이터를 직접 전송하는지(Kaspersky Security Center 우회) 결정합니다.
4. 토글 버튼을 **Kaspersky Security Network 사용 활성화됨** 위치로 전환합니다.
   이 옵션을 활성화하면 클라이언트 기기에서 패치 설치 결과에 대한 데이터를 Kaspersky에 보냅니다. 이 옵션을 활성화하는 경우, KSN 성명서 약관을 읽고 수락해야 합니다.
   KPSN 사용 시, 토글 버튼을 **Kaspersky Private Security Network 사용 활성화됨**위치로 전환하고 **KSN 프록시 설정 파일 선택** 버튼을 눌러 KPSN(확장자가 pkcs7, pem인 파일)의 설정을 다운로드합니다. 설정을 다운로드하면 인터페이스에 공급자의 이름과 연락처 및 KPSN 설정을 사용하여 파일을 생성한 날짜가 표시됩니다.

   > KPSN을 사용하도록 설정하면 KSN 요청을 클라우드 KSN으로 직접 보내도록 구성된 배포 지점에 주의를 기울이십시오. 네트워크 에이전트 버전 11 및 이전 버전이 설치된 배포 지점은 계속해서 클라우드 KSN으로 KSN 요청을 보냅니다. KPSN으로 KSN 요청을 보내도록 배포 지점을 다시 구성하려면, 각 배포 지점에 대하여 **중앙 관리 서버에 KSN 요청 전달** 옵션을 활성화합니다. 배포 지점 속성 또는 네트워크 에이전트 정책에서 이 옵션을 활성화할 수 있습니다.

   토글 버튼을 **Kaspersky Private Security Network 사용 활성화됨** 위치로 전환하면 KPSN에 대한 세부 정보가 포함된 메시지가 나타납니다.

KPSN을 지원하는 Kaspersky 애플리케이션은 다음과 같습니다:

- Kaspersky Security Center
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

Kaspersky Security Center에서 KPSN을 활성화하면 이러한 애플리케이션은 KPSN 지원에 대한 정보를 받게 됩니다. 애플리케이션 설정 창에 있는 **지능형 위협 보호** 섹션의 **Kaspersky Security Network** 하위 섹션에 KSN 공급자가 KSN 또는 KPSN으로 표시됩니다.

Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 또는 Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent 이전 애플리케이션 버전을 사용할 시, KPSN을 실행하려면 KPSN을 사용하도록 설정하지 않은 보조 중앙 관리 서버를 사용하는 것이 좋습니다.

Kaspersky Security Center는 중앙 관리 서버 속성 창의 **KSN 프록시 설정** 섹션에서 KPSN이 구성된 경우 통계 데이터를 Kaspersky Security Network에 전송하지 않습니다.

5. 중앙 관리 서버 속성에 프록시 서버 설정이 구성되어 있는데 네트워크 아키텍처에서는 KPSN을 직접 사용해야 한다면, **KPSN에 연결할 때 프록시 서버 설정 무시** 옵션을 활성화합니다. 이렇게 하지 않으면 관리 중인 애플리케이션의 요청을 KPSN으로 전송할 수 없습니다.

6. KSN 프록시 서비스에 대한 중앙 관리 서버 연결 구성:

   - **연결 설정**에서 **TCP 포트**에 대해 KSN 프록시 서버 연결에 사용할 TCP 포트 번호를 지정합니다. KSN 프록시 서버에 연결하는 기본 포트는 13111입니다.
   - UDP 포트를 통해 중앙 관리 서버를 KSN 프록시 서버에 연결하려면 **UDP 포트 사용** 옵션을 활성화하고 **UDP 포트**에 대한 포트 번호를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있으며 TCP 포트가 사용됩니다. 이 옵션이 활성화되어 있다면 UDP 포트 15111이 KSN 프록시 서버 연결에 기본으로 사용됩니다.
   - 중앙 관리 서버를 HTTPS 포트를 통해 KSN 프록시 서버에 연결해야 한다면 **HTTPS 사용** 옵션을 활성화한 다음, **포트를 통해 HTTPS 사용**에 포트 번호를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있으며 TCP 포트가 사용됩니다. 이 옵션이 활성화되어 있다면 HTTPS 포트 17111이 KSN 프록시 서버 연결에 기본으로 사용됩니다.

7. 토글 버튼을 **기본 중앙 관리 서버를 통해 보조 중앙 관리 서버와 KSN 연결 활성화됨** 위치로 전환합니다.

   이 옵션을 활성화하면 보조 중앙 관리 서버가 기본 중앙 관리 서버를 KSN 프록시 서버로 사용합니다. 이 옵션을 비활성화하면 보조 중앙 관리 서버에서 직접 KSN으로 연결합니다. 이 경우 관리 중인 기기는 보조 중앙 관리 서버를 KSN 프록시 서버로 사용합니다.

   보조 중앙 관리 서버 속성의 **KSN 프록시 설정** 섹션의 오른쪽 패널에서 토글 버튼이 **중앙 관리 서버에서 KSN 프록시 활성화 활성화됨** 위치로 전환되어 있으면 보조 중앙 관리 서버가 기본 중앙 관리 서버를 프록시 서버로 사용합니다.

8. **저장** 버튼을 누릅니다.

KSN 접근 설정이 저장됩니다.

중앙 관리 서버의 부하를 줄이려는 등의 경우, 배포 지점의 KSN 접근을 설정할 수도 있습니다. 그러면 KSN 프록시 서버 역할을 하는 배포 지점이 중앙 관리 서버를 사용하지 않고 관리 중인 기기에서 Kaspersky으로 KSN 요청을 직접 보냅니다.

배포 지점이 KSN(Kaspersky Security Network)에 접근하도록 설정하려면 다음과 같이 하십시오:

1. 배포 지점이 수동으로 할당되어 있는지 확인합니다.
2. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
3. **일반** 탭에서 **배포 지점** 섹션을 선택합니다.
4. 배포 지점의 이름을 누르면 속성 창이 열립니다.
5. 배포 지점 속성 창의 **KSN 프록시** 섹션에서 **배포 지점 측에서 KSN 프록시 기능 활성화** 옵션을 활성화한 다음, **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근** 옵션을 활성화합니다.
6. **확인**를 누릅니다.

배포 지점이 KSN 프록시 서버 역할을 합니다.

KSN 사용 활성화 및 비활성화

KSN을 사용하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **KSN 프록시 설정** 섹션을 선택합니다.
3. 토글 버튼을 **중앙 관리 서버에서 KSN 프록시 활성화 활성화됨** 위치로 전환합니다.

KSN 프록시 서버를 활성화하고 KSN에 데이터를 전송하여 Kaspersky Security Center 구성 요소의 효율성과 Kaspersky 애플리케이션의 성능을 개선합니다.

1. 사용 중인 KSN 인프라 솔루션에 따라 해당 토글 버튼을 활성화합니다.
   - 글로벌 KSN을 사용한다면 토글 버튼을 **Kaspersky Security Network 사용 활성화됨** 위치로 전환합니다.
     이제 KSN으로 데이터를 전송할 수 있습니다. 이 옵션을 활성화하려면, KSN 진술문 약관을 읽고 수락해야 합니다.
   - KPSN 사용 시, 토글 버튼을 **Kaspersky Private Security Network 사용 활성화됨** 위치로 전환하고 **KSN 프록시 설정 파일 선택** 버튼을 클릭해 KPSN(확장자가 pkcs7, pem인 파일)의 설정을 다운로드합니다. 설정을 다운로드하면 인터페이스에 공급자의 이름과 연락처 및 KPSN 설정을 사용하여 파일을 생성한 날짜가 표시됩니다.
     토글 버튼을 **Kaspersky Private Security Network 사용 활성화됨** 위치로 전환하면 KPSN 관련 세부 정보 메시지가 나타납니다.
2. **저장** 버튼을 클릭합니다.

KSN 사용을 중지하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **KSN 프록시 설정** 섹션을 선택합니다.
3. KSN 프록시 서비스를 비활성화하려면 토글 버튼을 **중앙 관리 서버에서 KSN 프록시 활성화 비활성화됨** 위치로 전환합니다.
4. **저장** 버튼을 누릅니다.

수락한 KSN 성명서 보기

Kaspersky Security Network(KSN)를 활성화할 때 KSN 성명서를 읽고 수락해야 합니다. 수락한 KSN 성명서는 언제든지 볼 수 있습니다.

수락한 KSN 성명서를 보려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **KSN 프록시 설정** 섹션을 선택합니다.
3. **Kaspersky Security Network 진술문 보기** 링크를 누릅니다.

   열리는 창에서 수락한 KSN 성명서의 텍스트를 볼 수 있습니다.

업데이트된 KSN 성명서 수락

KSN을 활성화할 때 읽고 수락하는 KSN 성명서에 따라 KSN을 사용합니다. KSN 진술문이 업데이트되면, 중앙 관리 서버를 업데이트하거나 업그레이드할 때 표시됩니다. 업데이트된 KSN 성명서를 수락하거나 거부할 수 있습니다. 거부 시, 이전에 수락한 KSN 진술문 버전에 따라 KSN을 계속 사용합니다.

중앙 관리 서버를 업그레이드하면 업데이트된 KSN 진술문이 자동으로 표시됩니다. 업데이트된 KSN 진술문을 거부하더라도 나중에 보고 수락할 수 있습니다.

업데이트된 KSN 성명서를 보고 수락 또는 거부하기:

1. 메인 애플리케이션 창의 오른쪽 상단에 있는 **알림 보기** 링크를 누릅니다.
   알림 창이 열립니다.
2. **업데이트된 KSN 진술문 보기** 링크를 클릭합니다.
   Kaspersky Security Network 진술문 업데이트 창이 열립니다.

3. KSN 진술문을 주의깊게 읽고 다음 버튼 중 하나를 눌러 결정을 내리십시오:

- **업데이트된 KSN 성명서를 수락합니다.**
- **이전 성명서 하에 KSN을 사용합니다.**

선택에 따라 KSN은 현재 또는 업데이트된 KSN 성명서의 약관을 계속 따릅니다. 중앙 관리 서버 속성에서 언제든지 수락한 KSN 성명서의 텍스트를 볼 수 있습니다.

배포 지점이 KSN 프록시 서버로 작동하는지 확인

배포 지점으로 작동하도록 할당된 관리 중인 기기에서 KSN 프록시 서버를 활성화할 수 있습니다. 관리 중인 기기는 기기에서 ksnproxy 서비스가 실행 중일 때 KSN 프록시로 작동합니다. 기기에서 로컬로 이 서비스를 확인하거나 켜거나 끌 수 있습니다.

Windows 기반 또는 Linux 기반 기기를 배포 지점으로 할당할 수 있습니다. 배포 지점 확인 방법은 이 배포 지점의 운영 체제에 따라 다릅니다.

Windows 기반 배포 지점이 KSN 프록시 서버로 작동하는지 확인하려면:

1. 배포 지점 기기의 Windows에서 **서비스(모든 프로그램 → 관리 도구 → 서비스)**를 엽니다.
2. 서비스 목록에서 ksnproxy 서비스가 실행되고 있는지 확인합니다.

   ksnproxy 서비스가 실행 중이면 기기의 네트워크 에이전트가 Kaspersky Security Network에 참여하고 배포 지점 범위에 포함된 관리 중인 기기에 대한 KSN 프록시 서버로 작동합니다.

   원하는 경우 ksnproxy 서비스를 해제할 수 있습니다. 이 경우 배포 지점의 네트워크 에이전트는 Kaspersky Security Network에 참여하지 않게 됩니다. 이렇게 하려면 로컬 관리자 권한이 필요합니다.

Linux 기반 배포 지점이 KSN 프록시 서버로 작동하는지 확인하려면:

1. 배포 지점 기기에서, 실행 중인 프로세스 목록을 표시합니다.
2. 실행 중인 프로세스 목록에서 `/opt/kaspersky/ksc64/sbin/ksnproxy` 프로세스가 실행 중인지 확인합니다.

`/opt/kaspersky/ksc64/sbin/ksnproxy` 프로세스가 실행 중이면 기기의 네트워크 에이전트가 Kaspersky Security Network에 참여하고 배포 지점 범위에 포함된 관리 중인 기기에 대한 KSN 프록시 서버로 작동합니다.

시나리오: Kaspersky Security Center 및 관리 중인 보안 제품 업그레이드

이 섹션에서는 Kaspersky Security Center 및 관리 중인 보안 제품을 업그레이드하는 주요 시나리오를 간단하게 설명합니다.

Kaspersky Security Center 및 관리 중인 보안 제품 업그레이드는 단계적으로 진행됩니다.

1. **하드웨어 및 소프트웨어 요구 사항 확인**

   하드웨어가 요구 사항을 충족하는지 확인하고 필요한 업데이트를 설치합니다.

2. **리소스 계획**

   데이터베이스가 차지하는 디스크 공간을 평가합니다. 중앙 관리 서버 설정 및 데이터베이스의 백업 복사본을 저장할 디스크 공간이 충분한지 확인합니다.

3. **Kaspersky Security Center용 설치 프로그램 파일 가져오기**

   현재 버전의 Kaspersky Security Center용 실행 파일을 가져와서 중앙 관리 서버로 사용할 기기에 저장합니다. 사용하려는 Kaspersky Security Center 버전의 릴리스 정보를 확인합니다.

4. **이전 버전의 백업 복사본 생성**

   데이터 백업 및 복구 유틸리티를 사용하여 중앙 관리 서버 데이터의 백업 복사본을 생성합니다. 백업 작업을 생성할 수도 있습니다.

   설치된 플러그인 목록을 내보낼 것을 권장합니다.

5. **설치 프로그램 실행**

   Kaspersky Security Center의 최신 버전에 대한 실행 파일을 실행합니다. 이 파일을 실행할 때 백업 복사본이 있음을 지정하고 해당 위치를 지정합니다. 데이터가 백업에서 복원됩니다.

6. **관리 중인 애플리케이션 업그레이드**

   최신 버전을 사용할 수 있는 경우 애플리케이션을 업그레이드할 수 있습니다. 지원되는 Kaspersky 애플리케이션 목록을 확인하고 사용 중인 Kaspersky Security Center 버전이 이 애플리케이션과 호환되는지 확인합니다. 그런 다음 릴리스 정보의 설명에 따라 애플리케이션 업그레이드를 수행합니다.

결과

업그레이드 시나리오가 완료되면 새 버전의 중앙 관리 서버가 Microsoft Management Console에 성공적으로 설치되었는지 확인합니다. **도움말** → **Kaspersky Security Center 정보**를 누릅니다. 버전이 표시됩니다.

Kaspersky Security Center 웹 콘솔에서 새 버전의 중앙 관리 서버를 사용하고 있는지 확인하려면, 화면 상단에서 중앙 관리 서버 이름 옆에 있는 설정 아이콘( )을 클릭합니다. 중앙 관리 서버 속성 창이 열리면 **일반** 탭에서 **일반** 섹션을 선택합니다. 버전이 표시됩니다.

중앙 관리 서버 데이터를 복구하려면, 대화형 모드에서 데이터 백업 및 복구 주제에 설명된 단계를 따르십시오.

관리 중인 보안 제품을 업그레이드한 경우 관리 중인 기기에 올바르게 설치되었는지 확인합니다. 자세한 내용은 이 애플리케이션의 문서를 참조하십시오.

Kaspersky 데이터베이스 및 애플리케이션 업데이트

이 섹션에서는 다음을 정기적으로 업데이트하기 위해 수행해야 하는 단계에 대해 설명합니다.

- Kaspersky 데이터베이스 및 소프트웨어 모듈
- Kaspersky Security Center 구성 요소 및 보안 제품을 포함하여 설치된 Kaspersky 애플리케이션

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)과 KSN 기능이 제공되지 않을 수도 있습니다.

시나리오: Kaspersky 데이터베이스 및 애플리케이션의 정기적 업데이트

이 섹션에서는 Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션을 정기적으로 업데이트하는 시나리오를 제공합니다. 네트워크 보호 구성 시나리오를 완료한 후 중앙 관리 서버와 관리 중인 기기가 바이러스, 네트워크 공격 및 피싱 공격을 비롯한 다양한 위협으로부터 보호되도록 보호 시스템의 안정성을 유지해야 합니다.

네트워크 보호는 다음을 정기적으로 업데이트하여 최신 상태로 유지됩니다.

- Kaspersky 데이터베이스 및 소프트웨어 모듈
- Kaspersky Security Center 구성 요소 및 보안 제품을 포함하여 설치된 Kaspersky 애플리케이션

이 시나리오를 완료하면 다음을 확인할 수 있습니다.

- 네트워크는 Kaspersky Security Center 구성 요소 및 보안 제품 등의 최신 Kaspersky 소프트웨어로 보호됩니다.
- 네트워크 안전에 중요한 안티 바이러스 데이터베이스 및 기타 Kaspersky 데이터베이스는 항상 최신 상태로 유지됩니다.

필수 구성 요소

관리 중인 기기는 중앙 관리 서버에 연결되어 있어야 합니다. 연결되지 않은 경우 Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션을 수동으로 업데이트하거나 Kaspersky 업데이트 서버에서 직접 업데이트하는 것을 고려하십시오.

중앙 관리 서버는 인터넷에 연결되어 있어야 합니다.

시작하기 전에 다음을 수행했는지 확인하십시오:

1. Kaspersky 보안 제품을 Kaspersky Security Center 웹 콘솔을 통한 Kaspersky 애플리케이션 배포 시나리오에 따라 관리 중인 기기에 배포했습니다.
2. 모든 필수 정책, 정책 프로필 및 작업을 네트워크 보호 구성 시나리오에 따라 생성하고 구성했습니다.
3. 관리 중인 기기의 수 및 네트워크 토폴로지에 따라 적절한 양의 배포 지점을 할당했습니다.

Kaspersky 데이터베이스 및 애플리케이션 업데이트는 단계적으로 진행됩니다.

1. **업데이트 체계 선택**

   Kaspersky Security Center 구성 요소 및 보안 제품에 대한 업데이트를 설치하는 데 사용 할 수 있는 몇 가지 체계가 있습니다. 네트워크의 요구 사항을 가장 잘 충족하는 체계를 하나 또는 여러 개 선택하십시오.

2. **중앙 관리 서버 저장소 업데이트 다운로드 작업 생성**

   이 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동으로 생성합니다. 마법사를 실행하지 않았다면 지금 작업을 만듭니다.

   이 작업은 Kaspersky 업데이트 서버에서 중앙 관리 서버의 저장소로 업데이트를 다운로드하고 Kaspersky Security Center용 Kaspersky 데이터베이스 및 소프트웨어 모듈을 업데이트하는 데 필요합니다. 업데이트를 다운로드한 후 관리 중인 기기로 배포할 수 있습니다.

네트워크에 배포 지점이 할당되면 업데이트가 중앙 관리 서버 저장소에서 배포 지점의 저장소로 자동 다운로드됩니다. 이러한 경우 배포 지점 범위에 포함된 관리 중인 기기가 중앙 관리 서버 저장소 대신 배포 지점의 저장소에서 업데이트를 다운로드합니다.

방법 지침:

- 관리 콘솔: 중앙 관리 서버 저장소 업데이트 다운로드 작업 생성
- Kaspersky Security Center 웹 콘솔: 중앙 관리 서버 저장소 업데이트 다운로드 작업 생성

3. **배포 지점의 저장소로 업데이트 다운로드 작업 생성(선택 사항)**

기본적으로 업데이트는 중앙 관리 서버에서 배포 지점으로 다운로드됩니다. Kaspersky 업데이트 서버에서 직접 배포 지점으로 업데이트를 다운로드하도록 Kaspersky Security Center를 구성할 수 있습니다. 배포 지점과 Kaspersky 업데이트 서버 간의 트래픽에 비해 중앙 관리 서버와 배포 지점 간의 트래픽에서 더 많은 비용이 발생하거나 중앙 관리 서버에서 인터넷에 연결할 수 없는 경우 배포 지점의 저장소로 업데이트 다운로드 작업을 사용하는 것이 좋습니다.

네트워크에 배포 지점이 할당되어 있고 *배포 지점의 저장소로 업데이트 다운로드* 작업이 생성되면 배포 지점은 중앙 관리 서버 저장소가 아닌 Kaspersky 업데이트 서버에서 업데이트를 다운로드합니다.

방법 지침:

- 관리 콘솔: 배포 지점의 저장소로 업데이트 다운로드 작업 생성
- Kaspersky Security Center 웹 콘솔: 배포 지점의 저장소로 업데이트 다운로드 작업 생성

4. **배포 지점 구성**

네트워크에 배포 지점이 할당되어 있는 경우 모든 필수 배포 지점의 속성에서 **업데이트 배포** 옵션이 활성화되어 있는지 확인합니다. 배포 지점에 대해 이 옵션이 비활성화되어 있으면 배포 지점 범위에 포함된 기기가 중앙 관리 서버의 저장소에서 업데이트를 다운로드합니다.

관리 중인 기기가 배포 지점에서만 업데이트를 받도록 하려는 경우 네트워크 에이전트 정책에서 **배포 지점을 통해서만 파일 배포** 옵션을 활성화합니다.

5. **업데이트 다운로드 또는 diff 파일의 오프라인 모델을 사용하여 업데이트 프로세스 최적화(선택 사항)**

업데이트 다운로드의 오프라인 모델(기본적으로 활성화됨) 또는 diff 파일을 사용하여 업데이트 프로세스를 최적화할 수 있습니다. 이러한 두 기능은 동시에 작동할 수 없기 때문에 각 네트워크 세그먼트에 대해 활성화할 기능을 선택해야 합니다.

업데이트 다운로드의 오프라인 모델이 활성화된 경우 네트워크 에이전트는 보안 제품이 업데이트를 요청하기 전에 업데이트가 중앙 관리 서버 저장소로 다운로드되면 관리 중인 기기에 필요한 업데이트를 다운로드합니다. 이를 통해 업데이트 프로세스의 안정성이 향상됩니다. 이 기능을 사용하려면 네트워크 에이전트 정책에서 **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드(권장)** 옵션을 활성화합니다.

업데이트 다운로드의 오프라인 모델을 사용하지 않는 경우 diff 파일을 사용하여 중앙 관리 서버와 관리 중인 기기 간의 트래픽을 최적화할 수 있습니다. 이 기능이 활성화되면 중앙 관리 서버 또는 배포 지점에서 Kaspersky 데이터베이스 또는 소프트웨어 모듈의 전체 파일 대신 diff 파일을 다운로드합니다. 달라진 파일은 데이터베이스 또는 소프트웨어 모듈의 두 파일 버전 간 차이점을 설명합니다. 따라서 diff 파일은 전체 파일보다 적은 공간을 차지합니다. 이로 인해 중앙 관리 서버 또는 배포 지점과 관리 중인 기기 간의 트래픽이 감소합니다. 이 기능을 사용하려면 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업 및/또는 *배포 지점의 저장소로 업데이트 다운로드* 작업의 속성에서 **diff 파일 다운로드** 옵션을 활성화합니다.

방법 지침:

- Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트에 달라진 파일 사용
- 관리 콘솔: 업데이트 다운로드 오프라인 모델 활성 및 비활성
- Kaspersky Security Center 웹 콘솔: 업데이트 다운로드 오프라인 모델 활성 및 비활성

6 다운로드한 업데이트 검증(선택 사항)

다운로드한 업데이트를 설치하기 전에 *업데이트 검증* 작업을 통해 업데이트를 확인할 수 있습니다. 이 작업은 지정된 테스트 기기 모음에 대한 설정을 통해 구성된 기기 업데이트 작업 및 악성 코드 검사 작업을 순차적으로 실행합니다. 작업 결과가 나오면 중앙 관리 서버에서 나머지 기기에 대한 업데이트 배포를 시작하거나 차단합니다.

업데이트 검증 작업은 *중앙 관리 서버 저장소 업데이트 다운로드* 작업에 포함되어 수행됩니다. *중앙 관리 서버 저장소 업데이트 다운로드* 작업의 속성에서 관리 콘솔의 **배포하기 전에 업데이트 검증 절차 수행** 옵션 또는 Kaspersky Security Center 웹 콘솔의 **업데이트 검증 실행** 옵션을 활성화합니다.

방법 지침:

- 관리 콘솔: 다운로드한 업데이트 검증
- Kaspersky Security Center 웹 콘솔: 다운로드한 업데이트 검증

7 소프트웨어 업데이트 승인 및 거부

기본적으로 다운로드한 소프트웨어 업데이트는 *정의 안 됨* 상태입니다. 상태를 *승인됨* 또는 *거부됨*으로 변경할 수 있습니다. 승인된 업데이트는 항상 설치됩니다. 업데이트를 위해 최종 사용자 라이센스 계약서 약관을 검토하고 동의해야 하는 경우 먼저 약관에 동의해야 합니다. 그런 다음 업데이트를 관리 중인 기기로 배포할 수 있습니다. 정의되지 않은 업데이트는 네트워크 에이전트 정책 설정에 따라 네트워크 에이전트 및 다른 Kaspersky Security Center 구성 요소에만 설치할 수 있습니다. *거부됨* 상태로 설정한 업데이트는 기기에 설치되지 않습니다. 보안 제품에 대해 거부된 업데이트가 이전에 설치된 경우 Kaspersky Security Center는 모든 기기에서 업데이트 제거를 시도합니다.

업데이트 승인 및 거부는 네트워크 에이전트 및 Windows 기반 및 Linux 기반 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션에서만 사용할 수 있습니다. 중앙 관리 서버, Kaspersky Security Center 웹 콘솔 및 관리 웹 플러그인의 원활한 업데이트를 지원하지 않습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 업데이트 승인 및 거부
- Kaspersky Security Center 웹 콘솔: 소프트웨어 업데이트 승인 및 거부

8 Kaspersky Security Center 구성 요소 업데이트 및 패치 자동 설치 구성

네트워크 에이전트 및 다른 Kaspersky Security Center 구성 요소에 대해 다운로드한 업데이트 및 패치가 자동 설치됩니다. 네트워크 에이전트 속성에서 **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 옵션을 활성화된 상태로 두면 모든 업데이트가 저장소 하나 또는 여러 개로 다운로드된 후 자동으로 설치됩니다. 이 옵션을 비활성화하면, 다운로드되어 *정의 안 됨* 상태가 태그된 Kaspersky 패치는 그 상태를 *승인됨*으로 변경한 후에만 설치할 수 있습니다.

방법 지침:

- 관리 콘솔: Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성/비활성
- Kaspersky Security Center 웹 콘솔: Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성화/비활성화

9 중앙 관리 서버의 업데이트 설치

중앙 관리 서버의 소프트웨어 업데이트는 업데이트 상태에 따라 달라지지 않습니다. 이는 자동으로 설치되지 않으며 관리 콘솔의 **모니터링** 탭(**중앙 관리 서버** <서버 이름> → **모니터링**)이나 Kaspersky Security Center 웹 콘솔의 **알림** 섹션(**모니터링 및 보고 → 알림**)에서 관리자의 사전 승인을 받아야 합니다. 그 후 관리자는 명시적으로 업데이트 설치를 실행해야 합니다.

10 보안 제품에 대한 업데이트 자동 설치 구성

관리 중인 애플리케이션에 대한 *업데이트* 작업을 생성하여 안티 바이러스 데이터베이스를 포함한 애플리케이션, 소프트웨어 및 Kaspersky 데이터베이스에 대한 업데이트를 적시에 제공할 수 있습니다. 업데이트를 적시에 제공하려면 작업 스케줄 구성 시 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후** 옵션을 선택합니다.

네트워크에 IPv6 전용 기기가 포함되어 있고 이러한 기기에 설치된 보안 애플리케이션을 정기적으로 업데이트하려면, 관리 중인 기기에 중앙 관리 서버(13.2 버전 이상)와 네트워크 에이전트(13.2 버전 이상)가 설치되어 있어야 합니다.

기본적으로 Kaspersky Endpoint Security for Windows 및 Kaspersky Endpoint Security for Linux에 대한 업데이트는 업데이트 상태를 *승인됨*으로 변경한 후에만 설치됩니다. *업데이트* 작업에서 업데이트 설정을 변경할 수 있습니다.

업데이트를 위해 최종 사용자 라이센스 계약서 약관을 검토하고 동의해야 하는 경우 먼저 약관에 동의해야 합니다. 그런 다음 업데이트를 관리 중인 기기로 배포할 수 있습니다.

방법 지침:

- 관리 콘솔: 기기에서 Kaspersky Endpoint Security 업데이트 자동 설치
- Kaspersky Security Center 웹 콘솔: 기기에 Kaspersky Endpoint Security 업데이트 자동 설치

결과

시나리오가 완료되면 Kaspersky Security Center는 Kaspersky 데이터베이스를 업데이트하도록 구성되고 업데이트가 중앙 관리 서버의 저장소 또는 배포 지점의 저장소에 다운로드된 후 Kaspersky 애플리케이션을 설치합니다. 그런 다음 네트워크 상태 모니터링을 진행할 수 있습니다.

Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션 업데이트 정보

중앙 관리 서버 및 관리 중인 기기의 보호가 최신 상태로 유지하려면 다음을 적시에 업데이트해야 합니다:

- Kaspersky 데이터베이스 및 소프트웨어 모듈

  Kaspersky 데이터베이스 및 소프트웨어 모듈을 다운로드하기 전에 Kaspersky Security Center가 Kaspersky 서버에 액세스할 수 있는지 확인합니다. 시스템 DNS를 사용하여 서버에 접근할 수 없다면 애플리케이션이 공용 DNS 서버를 사용합니다. 안티 바이러스 데이터베이스가 업데이트되고 관리 중인 기기에 대한 보안 수준을 유지하는 데 필요합니다.

- Kaspersky Security Center 구성 요소 및 보안 제품을 포함하여 설치된 Kaspersky 애플리케이션

  Kaspersky Security Center를 사용하면 Windows 기반 및 Linux 기반 클라이언트 기기에 설치된 네트워크 에이전트 및 Kaspersky 애플리케이션을 자동으로 업데이트할 수 있습니다. 중앙 관리 서버, Kaspersky Security Center 웹 콘솔 및 관리 웹 플러그인의 원활한 업데이트를 지원하지 않습니다. 이 구성 요소를 업데이트하려면 Kaspersky 웹사이트에서 최신 버전을 다운로드한 다음 수동 설치합니다.

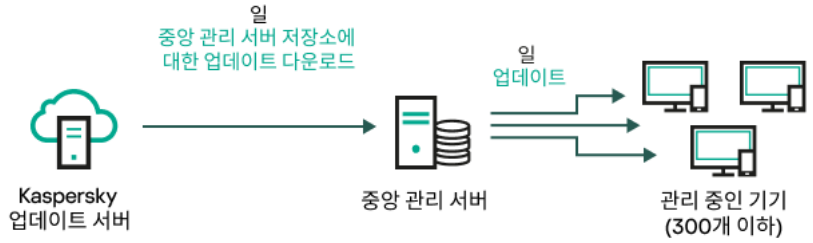
네트워크의 구성에 따라 다음과 같은 체계를 사용하여 필요한 업데이트를 관리 중인 기기로 다운로드하고 배포할 수 있습니다:

- 단일 작업 사용: *중앙 관리 서버 저장소에 업데이트 다운로드*
- 2개의 작업 사용:
  - *중앙 관리 서버 저장소에 업데이트 다운로드* 작업
  - *배포 지점의 저장소로 업데이트 다운로드* 작업

- 로컬 폴더, 공유 폴더 또는 FTP 서버를 통해 수동 업데이트
- Kaspersky 업데이트 서버에서 관리 중인 기기의 Kaspersky Endpoint Security로 직접 업데이트
- 중앙 관리 서버에 인터넷 연결이 없을 시, 로컬 또는 네트워크 폴더를 통해

중앙 관리 서버 저장소에 업데이트 다운로드 작업 사용

이 구성에서 Kaspersky Security Center는 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 통해 업데이트를 다운로드합니다. 단일 네트워크 세그먼트에 300대 미만의 관리 중인 기기가 있거나 각 네트워크 세그먼트에 10대 미만의 관리 중인 기기가 있는 소규모 네트워크에서는 업데이트가 중앙 관리 서버 저장소에서 직접 관리 중인 기기로 배포됩니다(아래 그림 참조).

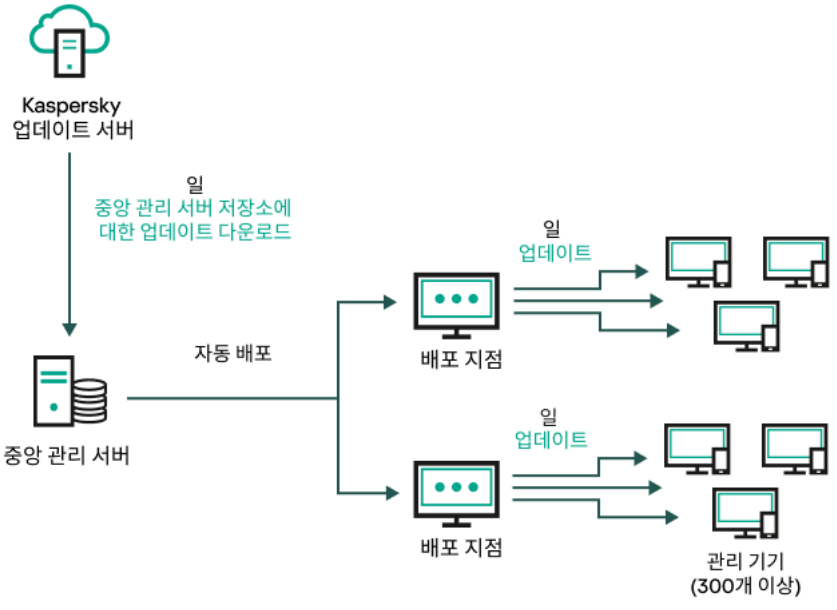


배포 지점이 없는 중앙 관리 서버 저장소에 업데이트 다운로드 작업을 사용하여 업데이트

기본적으로 중앙 관리 서버는 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버를 구성할 수 있습니다.

단일 네트워크 세그먼트에 300대 이상의 관리 중인 기기가 있거나 각 네트워크 세그먼트에 9대 이상의 관리 중인 기기가 있는 다중 네트워크 구성에서는 배포 지점을 사용하여 관리 중인 기기로 업데이트를 배포하는 것이 좋습니다(아래 그림 참조). 배포 지점은 중앙 관리 서버의 부하를 줄이고 중앙 관리 서버와 관리 중인 기기 간의 트래픽을 최적화합니다. 네트워크에 필요한 배포 지점의 수와 구성을 계산할 수 있습니다.

이 체계에서는 업데이트가 중앙 관리 서버 저장소에서 배포 지점의 저장소로 자동으로 다운로드됩니다. 배포 지점 범위에 포함된 관리 중인 기기가 중앙 관리 서버 저장소 대신 배포 지점의 저장소에서 업데이트를 다운로드합니다.



배포 지점이 있는 중앙 관리 서버 저장소에 업데이트 다운로드 작업을 사용하여 업데이트

중앙 관리 서버 저장소에 업데이트 다운로드 작업이 완료되면 다음과 같은 업데이트가 중앙 관리 서버 저장소로 다운로드됩니다.

- Kaspersky 데이터베이스 및 Kaspersky Security Center용 소프트웨어 모듈
  이러한 업데이트는 자동으로 설치됩니다.
- 관리 중인 기기에 설치된 보안 제품용 Kaspersky 데이터베이스 및 소프트웨어 모듈
  이러한 업데이트는 Kaspersky Endpoint Security for Windows 업데이트 작업을 통해 설치됩니다.
- 중앙 관리 서버용 업데이트:
  이 업데이트는 자동으로 설치되지 않습니다. 관리자는 업데이트 설치를 명시적으로 승인하고 실행해야 합니다.

  > 중앙 관리 서버에 패치를 설치하려면 로컬 관리자 권한이 필요합니다.

- Kaspersky Security Center의 구성 요소 업데이트
  기본적으로 이러한 업데이트는 자동으로 설치됩니다. 네트워크 에이전트 정책에서 설정을 변경할 수 있습니다.
- 보안 제품에 대한 업데이트
  기본적으로 Kaspersky Endpoint Security for Windows는 승인된 업데이트만 설치합니다(관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 통해 업데이트를 승인할 수 있습니다). 업데이트는 *업데이트* 작업을 통해 설치되며 이 작업의 속성에서 구성할 수 있습니다.

> 가상 중앙 관리 서버에서는 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 사용할 수 없습니다. 가상 중앙 관리 서버의 저장소에는 기본 중앙 관리 서버로 다운로드된 업데이트가 표시됩니다.

일련의 테스트 기기에서 작동 가능성과 오류를 확인하기 위한 업데이트를 구성할 수 있습니다. 검증에 성공하면 업데이트가 다른 관리 중인 기기에 배포됩니다.

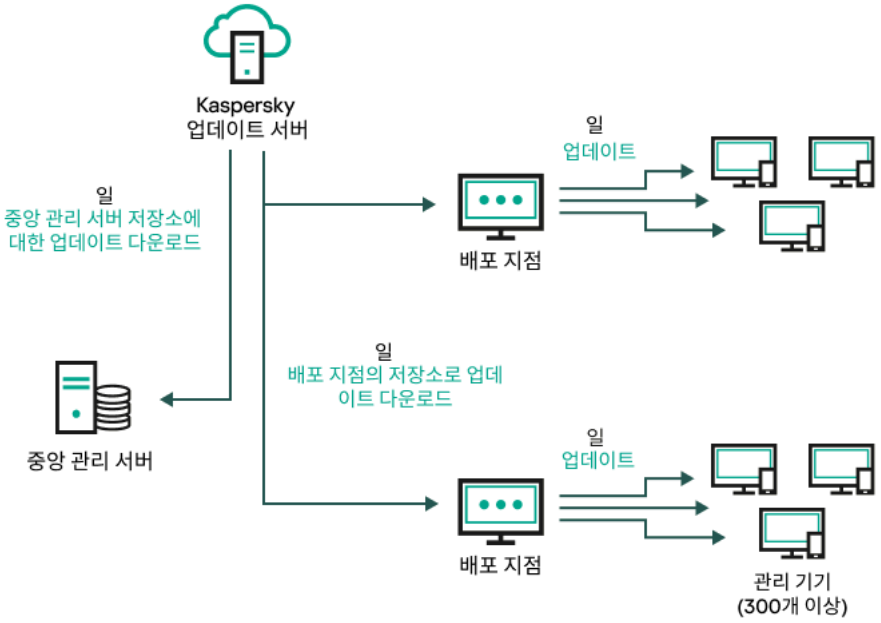
각 Kaspersky 애플리케이션은 중앙 관리 서버에서 필요한 업데이트를 요청합니다. 중앙 관리 서버는 이러한 요청을 집계하여 애플리케이션에 필요한 업데이트만 다운로드합니다. 그러므로 같은 업데이트가 여러 번 다운로드되지 않으며 불필요한 업데이트는 전혀 다운로드되지 않습니다. *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행할 때 Kaspersky 데이터베이스 및 소프트웨어 모듈의 관련 버전을 제대로 다운로드하기 위해 Kaspersky 업데이트 서버로 다음 정보를 중앙 관리 서버가 자동 전송합니다:

- 애플리케이션 ID 및 버전
- 애플리케이션 설치 ID
- 활성 키 ID
- *중앙 관리 서버 저장소 업데이트 다운로드* 작업 실행 ID

전송되는 정보에는 개인 정보 또는 기타 기밀 정보가 포함되지 않습니다. AO Kaspersky Lab은 법률로 규정된 요구 사항에 따라 정보를 보호합니다.

2개의 작업(중앙 관리 서버 저장소에 업데이트 다운로드 작업 및 배포 지점의 저장소로 업데이트 다운로드 작업) 사용

중앙 관리 서버 저장소 대신 Kaspersky 업데이트 서버에서 배포 지점의 저장소로 업데이트를 직접 다운로드할 수 있으며 이후 관리 중인 기기로 배포할 수 있습니다(아래 그림 참조). 배포 지점과 Kaspersky 업데이트 서버 간의 트래픽에 비해 중앙 관리 서버와 배포 지점 간의 트래픽에서 더 많은 비용이 발생하거나 중앙 관리 서버에서 인터넷에 연결할 수 없는 경우 배포 지점의 저장소로 업데이트 다운로드 작업을 사용하는 것이 좋습니다.



중앙 관리 서버 저장소에 업데이트 다운로드 작업 및 배포 지점의 저장소로 업데이트 다운로드 작업을 사용하여 업데이트

기본적으로 중앙 관리 서버 및 배포 지점은 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버 및 배포 지점을 구성할 수 있습니다.

이 구성을 구현하려면 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업과 함께 *배포 지점의 저장소로 업데이트 다운로드* 작업을 만듭니다. 그런 다음 배포 지점이 중앙 관리 서버 저장소가 아닌 Kaspersky 업데이트 서버에서 업데이트를 다운로드합니다.

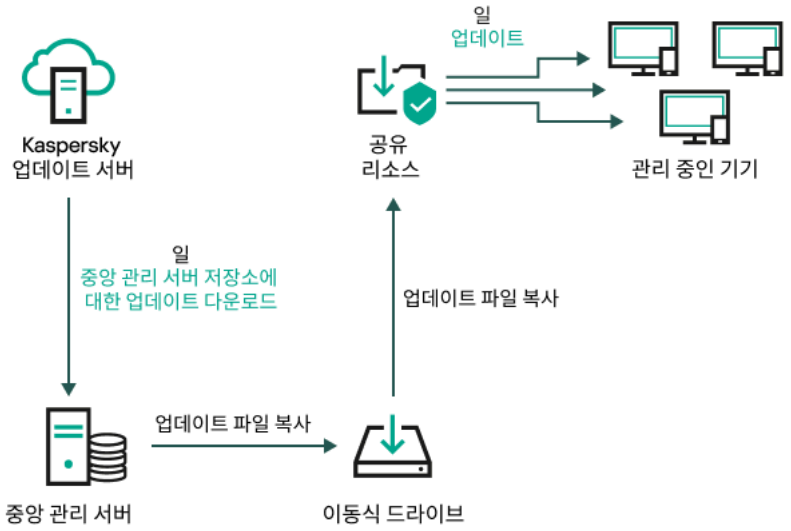
macOS를 실행하는 배포 지점 기기는 Kaspersky 업데이트 서버에서 업데이트를 다운로드할 수 없습니다.

macOS를 실행하는 하나 이상의 기기가 *배포 지점의 저장소로 업데이트 다운로드 작업 범위*에 있는 경우 모든 Windows 기기에서 작업이 성공적으로 완료되어도 작업은 *실패* 상태로 완료됩니다.

중앙 관리 서버 저장소에 업데이트 다운로드 작업 역시 이 체계에 필요합니다. 왜냐하면 이 작업은 Kaspersky Security Center용 Kaspersky 데이터베이스 및 소프트웨어 모듈을 다운로드하는 데 사용되기 때문입니다.

로컬 폴더, 공유 폴더 또는 FTP 서버를 통해 수동 업데이트

클라이언트 기기가 중앙 관리 서버에 연결되어 있지 않은 경우 로컬 폴더 또는 공유 리소스를 Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션을 업데이트하는 경로로 사용할 수 있습니다. 이 체계에서는 필요한 업데이트를 중앙 관리 서버 저장소에서 이동식 드라이브로 복사한 다음 Kaspersky Endpoint Security 설정에서 업데이트 경로로 지정된 로컬 폴더 또는 공유 리소스에 복사해야 합니다(아래 그림 참조).



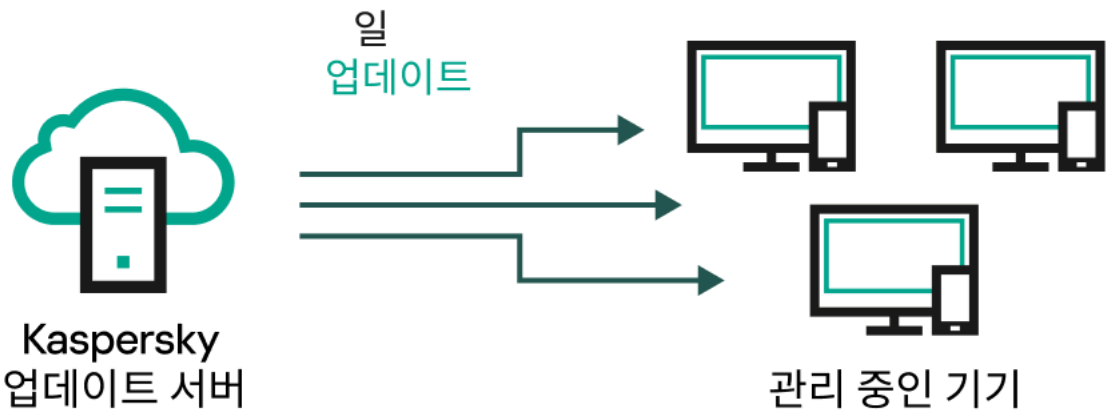
로컬 폴더, 공유 폴더 또는 FTP 서버를 통해 업데이트

Kaspersky Endpoint Security의 업데이트 소스에 대한 자세한 내용은 다음 도움말을 참조하십시오:

- Kaspersky Endpoint Security for Windows 도움말
- Kaspersky Endpoint Security for Linux 도움말

Kaspersky 업데이트 서버에서 관리 중인 기기의 Kaspersky Endpoint Security로 직접 업데이트

관리 중인 기기에서 Kaspersky Endpoint Security가 Kaspersky 업데이트 서버에서 직접 업데이트를 받도록 구성할 수 있습니다(아래 그림 참조).



Kaspersky 업데이트 서버에서 직접 보안 제품 업데이트

이 체계에서 보안 제품은 Kaspersky Security Center에서 제공하는 저장소를 사용하지 않습니다. Kaspersky 업데이트 서버에서 직접 업데이트를 받으려면 보안 제품 인터페이스에서 Kaspersky 업데이트 서버를 업데이트 경로로 지정합니다. 이러한 설정에 대한 자세한 내용은 다음 도움말을 참조하십시오:

- Kaspersky Endpoint Security for Windows 도움말
- Kaspersky Endpoint Security for Linux 도움말

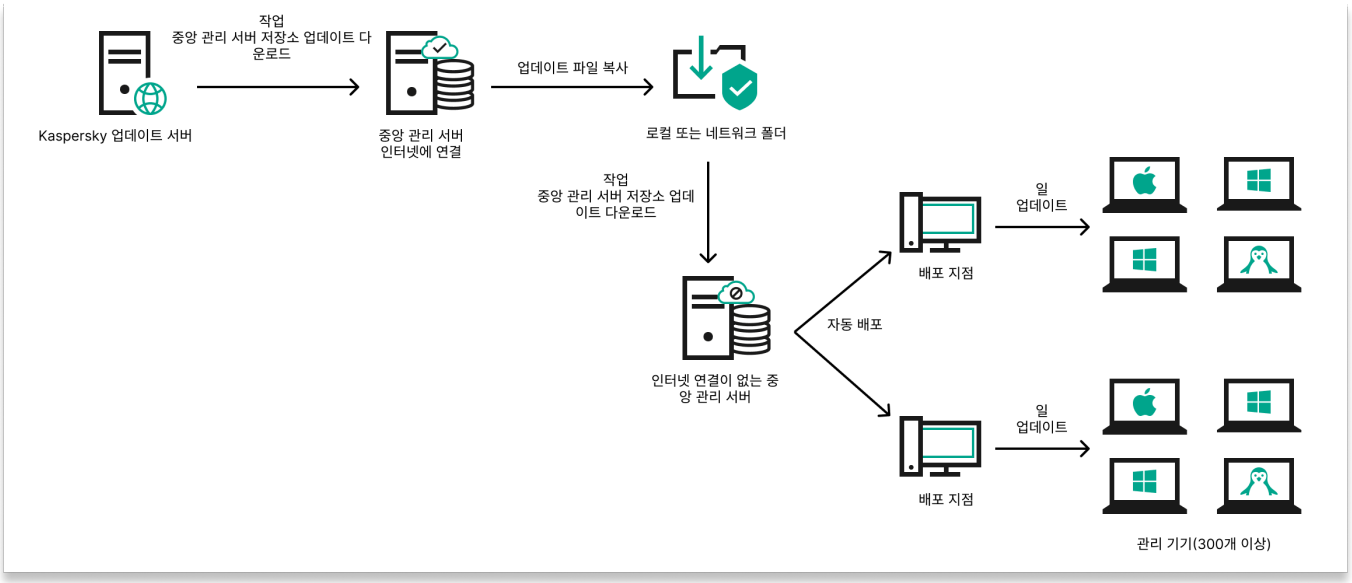
중앙 관리 서버에 인터넷 연결이 없을 시, 로컬 또는 네트워크 폴더를 통해

중앙 관리 서버가 인터넷에 연결되어 있지 않을 시, *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 구성하여 로컬 또는 네트워크 폴더에서 업데이트를 다운로드할 수 있습니다. 이때, 필요한 업데이트 파일을 지정된 폴더에 주기적으로 복사해야 합니다. 예를 들어 다음 경로 중 하나에서 필요한 업데이트 파일을 복사할 수 있습니다.

- 인터넷에 연결된 중앙 관리 서버(아래 그림 참조)

  중앙 관리 서버는 보안 애플리케이션에서 요청한 업데이트만 다운로드하므로 중앙 관리 서버에서 관리하는 보안 애플리케이션 집합(인터넷에 연결된 것과 연결되지 않은 것)이 일치해야 합니다.

  업데이트를 다운로드하는 데 사용하는 중앙 관리 서버의 버전이 13.2 이하일 시, *중앙 관리 서버 저장소에 업데이트 다운로드* 작업의 속성을 열고 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.



중앙 관리 서버에 인터넷 연결이 없을 시 로컬 또는 네트워크 폴더를 통해 업데이트

- Kaspersky 업데이트 유틸리티

  이 유틸리티는 이전 구성표를 사용하여 업데이트를 다운로드하므로, *중앙 관리 서버 저장소에 업데이트 다운로드* 작업의 속성을 열고 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.

중앙 관리 서버 저장소에 업데이트 다운로드 작업 생성

중앙 관리 서버의 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동 생성합니다. 하나의 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업만 만들 수 있습니다. 따라서 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업이 중앙 관리 서버 작업 목록에서 제거된 경우에만 이 작업을 만들 수 있습니다.

이 작업은 Kaspersky 업데이트 서버에서 중앙 관리 서버의 저장소로 업데이트를 다운로드하는 데 필요합니다. 업데이트 목록에는 다음이 포함됩니다.

- 중앙 관리 서버용 데이터베이스 및 소프트웨어 모듈 업데이트
- Kaspersky 보안 제품용 데이터베이스 및 소프트웨어 모듈 업데이트
- Kaspersky Security Center 구성 요소 업데이트
- Kaspersky 보안 제품 업데이트

업데이트를 다운로드한 후 관리 중인 기기로 배포할 수 있습니다.

관리 중인 기기에 업데이트를 배포하기 전에 *업데이트 검증* 작업을 실행할 수 있습니다. 이렇게 하면 중앙 관리 서버가 다운로드한 업데이트를 제대로 설치하고 업데이트로 인해 보안 수준이 저하되지 않도록 할 수 있습니다. 배포하기 전에 확인하려면 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업 설정에서 **업데이트 검증 실행** 옵션을 구성합니다.

***중앙 관리 서버 저장소에 업데이트 다운로드** 작업을 만들려면 다음을 수행합니다.*

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. Kaspersky Security Center 애플리케이션에서는 **중앙 관리 서버 저장소에 업데이트 다운로드** 작업 유형을 선택합니다.
4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
5. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.
6. **생성** 버튼을 누릅니다.
   그러면 작업이 생성되고 작업 목록에 표시됩니다.
7. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.
8. 작업 속성 창이 열리면 **애플리케이션 설정** 탭에서 다음 설정을 지정하십시오.

   - **업데이트 경로**

     중앙 관리 서버의 업데이트 경로로 다음과 같은 리소스를 사용할 수 있습니다:

     - Kaspersky 업데이트 서버

       Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다. 기본적으로 중앙 관리 서버는 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버를 구성할 수 있습니다.

       기본적으로 선택됩니다.

     - 기본 중앙 관리 서버

       이 리소스는 보조 또는 가상 중앙 관리 서버용으로 생성한 작업에 적용됩니다.

     - 로컬 또는 네트워크 폴더

       최신 업데이트가 포함된 로컬 또는 네트워크 폴더입니다. 네트워크 폴더는 FTP/HTTP 서버이거나 SMB 공유일 수 있습니다. 네트워크 폴더 인증이 필요할 시, SMB 프로토콜만 지원합니다. 로컬 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다.

업데이트 경로에 사용되는 FTP 또는 HTTP 서버나 네트워크 폴더는 Kaspersky 업데이트 서버 사용 시에 생성되는 구조와 일치하는 폴더 구조(업데이트 포함)를 포함해야 합니다.

업데이트가 포함된 공유 폴더가 암호로 보호 중이라면 **업데이트 경로로 사용되는 공유 폴더에 접근하기 위한 계정 지정(해당되면)** 옵션을 활성화하고 액세스에 필요한 계정 자격 증명을 입력합니다.

- **업데이트 저장 폴더**

  저장된 업데이트를 저장하기 위한 지정된 폴더의 경로입니다. 지정된 폴더 경로를 클립보드에 복사할 수 있습니다. 그룹 작업에 대해 지정된 폴더의 경로를 변경할 수 없습니다.

- 기타 설정:

  - **보조 중앙 관리 서버 강제 업데이트**

    이 옵션을 활성화하면 새 업데이트가 다운로드되는 즉시 중앙 관리 서버가 보조 중앙 관리 서버에서 업데이트 작업을 시작합니다. 업데이트 작업은 보조 중앙 관리 서버의 작업 속성에 구성된 업데이트 경로를 사용하여 시작됩니다.

    해당 옵션을 비활성화하면 보조 중앙 관리 서버의 업데이트 작업이 스케줄에 따라 시작됩니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **추가 폴더에 다운로드한 업데이트 복사**

    중앙 관리 서버에서 업데이트를 수신한 후 이를 지정된 폴더에 복사합니다. 네트워크에서 업데이트 배포를 수동으로 관리하려는 경우 이 옵션을 사용합니다.

    이 옵션을 사용할 수 있는 상황의 예로는, 조직 네트워크가 여러 독립 서브넷으로 구성되어 있으며 각 서브넷의 기기가 다른 서브넷에는 액세스할 수 없는 경우를 들 수 있습니다. 하지만 모든 서브넷의 기기는 공통 네트워크 공유에 액세스할 수 있습니다. 이 경우 서브넷 중 하나의 중앙 관리 서버가 Kaspersky 업데이트 서버에서 업데이트를 다운로드하도록 설정하고 이 옵션을 활성화한 다음 해당 네트워크 공유를 지정할 수 있습니다. 다른 중앙 관리 서버에 대한 저장소에 업데이트 다운로드 작업에서 업데이트 경로와 같은 네트워크 공유를 지정합니다.

    다운로드한 업데이트를 로컬 폴더에 복사하도록 선택한 경우, 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다. 폴더 경로는 기기의 운영 체제에 따라 달라집니다. 로컬 폴더는 Linux 기반 중앙 관리 서버에 있으므로 POSIX 형식의 경로(예: /path/to/dir)를 지정해야 합니다.

    Linux 기반 중앙 관리 서버에 있는 네트워크 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기에서 해당 네트워크 폴더를 미리 탑재해 접근할 수 있어야 합니다. 폴더 접근은 SMB 프로토콜을 통해 이루어집니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **복사가 완료되기 전에 기기 및 보조 중앙 관리 서버로 강제 업데이트 안 함**

    메인 업데이트 폴더에서 추가 업데이트 폴더로 업데이트가 복사되어야만 클라이언트 기기와 보조 중앙 관리 서버의 업데이트 다운로드 작업이 시작됩니다.

    클라이언트 기기와 보조 중앙 관리 서버가 추가 네트워크 폴더에서 업데이트를 다운로드하는 경우 이 옵션을 활성화해야 합니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 내용**:
  - **diff 파일 다운로드**

    이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

- **이전 구성표를 사용해 업데이트 다운로드**

  버전 14부터 Kaspersky Security Center 보안 센터는 새 체계를 사용하여 데이터베이스 및 소프트웨어 모듈 업데이트를 다운로드합니다. 애플리케이션이 새 구성을 사용하여 업데이트를 다운로드하려면 업데이트 소스에 새 구성과 호환되는 메타데이터가 있는 업데이트 파일이 포함되어 있어야 합니다. 업데이트 소스에 이전 구성과 호환되는 메타데이터가 있는 업데이트 파일이 포함된 경우 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다. 그렇지 않으면 업데이트 다운로드 작업이 실패합니다.

  예를 들어 로컬 또는 네트워크 폴더가 업데이트 소스로 지정되고 이 폴더의 업데이트 파일이 다음 애플리케이션 중 하나에서 다운로드된 경우 이 옵션을 활성화해야 합니다.

  - Kaspersky 업데이트 유틸리티

    이 유틸리티는 이전 구성을 사용하여 업데이트를 다운로드합니다.

  - Kaspersky Security Center 13.2 또는 이전 버전

    예를 들어, 중앙 관리 서버 1은 인터넷에 연결되어 있지 않습니다. 이 경우 인터넷에 연결된 중앙 관리 서버 2를 사용하여 업데이트를 다운로드한 다음 로컬 또는 네트워크 폴더에 업데이트를 저장하여 중앙 관리 서버 1의 업데이트 소스로 사용할 수 있습니다. 중앙 관리 서버 2의 버전이 13.2 이하인 경우 중앙 관리 서버 1의 작업에서 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 검증 실행**

  중앙 관리 서버가 업데이트 경로에서 업데이트를 다운로드하고 임시 저장소에 해당 업데이트를 저장한 다음, **업데이트 확인 작업** 필드에 정의된 작업을 실행합니다. 작업이 성공적으로 완료되면 임시 저장소에서 중앙 관리 서버의 공유 폴더로 업데이트가 복사되고, 중앙 관리 서버를 업데이트 경로로 설정한 모든 기기로 업데이트가 배포됩니다. 즉, 스케줄 유형이 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**인 작업이 시작됩니다. 업데이트를 저장소로 다운로드하는 작업은 *업데이트 검증* 작업이 완료된 후에만 완료됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

9. 작업 속성 창의 **스케줄** 탭에서 작업 시작 스케줄을 만듭니다. 필요한 경우 다음 설정을 지정합니다:

- **작업 시작:**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **수동 시작**

    작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

    기본적으로 이 옵션은 선택되어 있습니다.

- **N분마다**

  작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.
  기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

- **N시간마다**

  작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.
  작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

- **N일마다**

  작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.
  기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **요일별**

  이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **악성 코드 급증 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

  이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **랜덤하게 작업 시작 시간을 자동으로 조절하는 기능 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 자동 임의 지연**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

- **작업이 다음 시간보다 오래 실행되면 중지**

  작업 완료 여부에 관계없이 지정된 시간이 경과한 후 작업이 자동으로 중지됩니다.

  실행 시간이 너무 오래 걸리는 작업을 중단(중지)하려는 경우 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 작업 실행 시간은 120분입니다.

10. **저장** 버튼을 누릅니다.

    작업이 생성 및 구성됩니다.

중앙 관리 서버가 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 수행하면, 데이터베이스 및 소프트웨어 모듈이 해당하는 업데이트 경로에서 다운로드되어 중앙 관리 서버의 공유 폴더에 저장됩니다. 관리 그룹에 대해 이 작업을 만들면 지정한 관리 그룹에 포함되어 있는 네트워크 에이전트에만 작업이 적용됩니다.

업데이트가 중앙 관리 서버의 공유 폴더에서 클라이언트 기기와 보조 중앙 관리 서버로 배포됩니다.

다운로드한 업데이트 검증

관리 중인 기기에 업데이트를 설치하기 전에 먼저 *업데이트 검증* 작업을 통해 업데이트의 운용 가능성 및 오류를 확인할 수 있습니다. *업데이트 검증* 작업은 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업에 포함되어 자동으로 수행됩니다. 중앙 관리 서버는 경로에서 업데이트를 다운로드하고 임시 저장소에 이를 저장한 다음 *업데이트 검증* 작업을 실행합니다. 작업이 성공적으로 완료되면 업데이트가 임시 저장소에서 중앙 관리 서버의 공유 폴더로 복사됩니다. 이 중앙 관리 서버가 업데이트 경로인 모든 클라이언트 기기에 배포됩니다.

업데이트 검증 작업 결과에 임시 저장소에 있는 업데이트가 잘못된 것으로 나타나거나 *업데이트 검증* 작업이 완료되었으나 오류가 발생한 경우, 해당 업데이트는 공유 폴더로 복사되지 않습니다. 중앙 관리 서버에는 이전 업데이트 집합이 유지됩니다. 그러면 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후** 스케줄 유형이 포함된 작업이 시작되지 않습니다. 이러한 작업은 다음에 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업이 시작될 때 새 업데이트 검사가 성공적으로 완료되는 경우 수행됩니다.

한 대 이상의 테스트 기기에서 다음 조건 중 하나라도 충족되면 업데이트 집합이 잘못된 것으로 간주됩니다:

- 업데이트 작업 오류가 발생했습니다.
- 업데이트가 적용된 후 보안 제품의 실시간 보호 상태가 변경되었습니다.
- 수동 검사 작업 실행 중 감염된 개체가 탐지되었습니다.
- Kaspersky 애플리케이션에서 런타임 오류가 발생했습니다.

나열된 어떤 조건에도 해당하는 기기가 없을 경우 업데이트 세트는 올바른 것으로 간주되고 *업데이트 검증* 작업은 성공적으로 완료된 것으로 간주됩니다.

업데이트 확인 작업 생성을 시작하기 전에 전제 조건을 수행하십시오.

1. 여러 테스트 기기가 있는 관리 그룹을 만듭니다. 업데이트를 확인하려면 이 그룹이 필요합니다.

   네트워크 전체에서 보호 수준을 가장 신뢰할 수 있고 가장 일반적인 애플리케이션 구성을 가진 기기를 사용하는 것이 좋습니다. 이 접근 방식은 검사 중 바이러스 탐지의 품질과 확률을 높이고 오탐지 위험을 최소화합니다. 테스트 기기에서 바이러스가 탐지되면 *업데이트 검증* 작업은 실패한 것으로 간주됩니다.

2. Kaspersky Security Center에서 지원하는 애플리케이션(Kaspersky Endpoint Security for Windows 또는 Kaspersky Security for Windows Server 등)에 대한 업데이트 및 악성 코드 검사 작업을 생성합니다. 업데이트 및 악성 코드 검사 작업 생성 시, 테스트 기기로 관리 그룹을 지정합니다.

   업데이트 검증 작업은 테스트 기기에서 업데이트 및 악성 코드 검사 작업을 순차적으로 실행하여 모든 업데이트가 유효한지 확인합니다. 또한, *업데이트 검증* 작업 생성 시, 업데이트 및 악성 코드 검사 작업을 지정해야 합니다.

3. *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 생성합니다.

다운로드한 업데이트를 클라이언트 기기로 배포하기 전에 Kaspersky Security Center에서 이를 검증하도록 하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**로 이동합니다.
2. **중앙 관리 서버 저장소에 업데이트 다운로드** 작업을 누릅니다.
3. 열리는 작업 속성 창에서 **애플리케이션 설정** 탭으로 이동한 다음 **업데이트 검증 실행** 옵션을 활성화합니다.
4. *업데이트 검증* 작업이 있는 경우 **작업 선택** 버튼을 누릅니다. 열리는 창에서 테스트 기기가 있는 관리 그룹의 *업데이트 검증* 작업을 선택합니다.
5. 이전에 *업데이트 검증* 작업을 생성하지 않은 경우 다음을 수행합니다.
   a. **새 작업** 버튼을 누릅니다.
   b. 새 작업 마법사가 열리면, 사전 설정 이름을 변경하려는 작업의 이름을 지정합니다.
   c. 이전에 생성한 테스트 기기가 있는 관리 그룹을 선택합니다.
   d. 먼저 Kaspersky Security Center에서 지원하는 필수 애플리케이션의 업데이트 작업을 선택한 다음 악성 코드 검사 작업을 선택합니다.

      이후에 다음 옵션이 표시됩니다. 활성화된 상태로 두는 것이 좋습니다.

      - **데이터베이스 업데이트 이후에 기기 다시 시작**

        기기에서 안티바이러스 데이터베이스를 업데이트한 후 기기를 재부팅하는 것이 좋습니다.

        이 옵션은 기본으로 활성화되어 있습니다.

      - **데이터베이스 업데이트 및 기기 다시 시작 후 검증 클라이언트의 실시간 보호 상태 확인**

        이 옵션이 활성화된 경우 *업데이트 검증* 작업은 중앙 관리 서버 저장소에 다운로드한 업데이트가 유효한지, 안티바이러스 데이터베이스 업데이트 및 기기 재시작 후 보호 수준이 저하되었는지 확인합니다.

기본적으로 이 옵션은 켜져 있습니다.

e. *업데이트 검증* 작업을 실행할 계정을 지정합니다. 계정을 사용하고 **기본 계정** 옵션을 활성화된 상태로 둘 수 있습니다. 또는 필요한 액세스 권한이 있는 다른 계정으로 작업을 실행하도록 지정할 수 있습니다. 이를 위해 **계정 지정** 옵션을 선택한 다음 해당 계정의 자격 증명을 입력합니다.

6. **저장**을 눌러 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업의 속성 창을 닫습니다.

자동 업데이트 검증이 활성화됩니다. 이제 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행할 수 있으며 업데이트 확인부터 시작됩니다.

배포 지점의 저장소로 업데이트 다운로드 작업 생성

배포 지점의 저장소로 업데이트 다운로드 작업은 Windows를 실행하는 배포 지점 기기에서만 작동합니다. Linux 또는 macOS를 실행하는 배포 지점 기기는 Kaspersky 업데이트 서버에서 업데이트를 다운로드할 수 없습니다. 작업 범위에 Linux 또는 macOS를 실행하는 기기가 하나라도 포함된 경우 작업은 *실패* 상태로 표시됩니다. 모든 Windows 기기에서 작업이 성공적으로 완료되더라도 나머지 기기에서는 오류가 반환됩니다.

관리 그룹에 대해 *배포 지점의 저장소로 업데이트 다운로드* 작업을 만들 수 있습니다. 이 작업은 지정한 관리 그룹에 포함된 배포 지점에 대해 실행됩니다.

예를 들어 배포 지점과 Kaspersky 업데이트 서버 간의 트래픽보다 중앙 관리 서버와 배포 지점 간의 트래픽의 비용이 더 크거나 중앙 관리 서버에서 인터넷에 연결할 수 없을 때 이 작업을 사용할 수 있습니다.

이 작업은 Kaspersky 업데이트 서버에서 배포 지점의 저장소로 업데이트를 다운로드하는 데 필요합니다. 업데이트 목록에는 다음이 포함됩니다.

- Kaspersky 보안 제품용 데이터베이스 및 소프트웨어 모듈 업데이트
- Kaspersky Security Center 구성 요소 업데이트
- Kaspersky 보안 제품 업데이트

업데이트를 다운로드한 후 관리 중인 기기로 배포할 수 있습니다.

배포 지점에서 프록시 서버를 사용하여 인터넷에 연결하는 경우 네트워크 에이전트 정책에서 해당 설정을 지정해야 합니다.

선택한 관리 그룹에 대해 ***배포 지점의 저장소로 업데이트 다운로드*** *작업을 만들려면 다음 단계를 따릅니다.*

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**로 이동합니다.
2. **추가** 버튼을 클릭합니다.
   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. Kaspersky Security Center 애플리케이션의 경우 **작업 유형** 필드에서 **배포 지점의 저장소로 업데이트 다운로드**를 선택합니다.
4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
5. 옵션 버튼을 선택하여 관리 그룹, 기기 조회 또는 작업이 적용되는 기기를 지정합니다.

6. **작업 생성 마침** 단계에서 기본 작업 설정을 수정하려면 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

7. **생성** 버튼을 누릅니다.

   그러면 작업이 생성되고 작업 목록에 표시됩니다.

8. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

9. 작업 속성 창의 **애플리케이션 설정** 탭에서 다음 설정을 지정합니다.

- **업데이트 경로**

  배포 지점의 업데이트 경로로 다음과 같은 리소스를 사용할 수 있습니다.

  - Kaspersky 업데이트 서버

    Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다.

    이 옵션은 기본적으로 선택되어 있습니다.

  - 로컬 또는 네트워크 폴더

    최신 업데이트가 포함된 로컬 또는 네트워크 폴더입니다. 네트워크 폴더는 FTP/HTTP 서버이거나 SMB 공유일 수 있습니다. 네트워크 폴더 인증이 필요할 시, SMB 프로토콜만 지원합니다. 로컬 폴더를 선택할 경우 중앙 관리 서버가 설치된 기기의 폴더를 지정해야 합니다.

    업데이트 경로에 사용되는 FTP 또는 HTTP 서버나 네트워크 폴더는 Kaspersky 업데이트 서버 사용 시에 생성되는 구조와 일치하는 폴더 구조(업데이트 포함)를 포함해야 합니다.

- **업데이트 저장 폴더**

  저장된 업데이트를 저장하기 위한 지정된 폴더의 경로입니다. 지정된 폴더 경로를 클립보드에 복사할 수 있습니다. 그룹 작업에 대해 지정된 폴더의 경로를 변경할 수 없습니다.

- **diff 파일 다운로드**

  이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **이전 구성표를 사용해 업데이트 다운로드**

  버전 14부터 Kaspersky Security Center 보안 센터는 새 체계를 사용하여 데이터베이스 및 소프트웨어 모듈 업데이트를 다운로드합니다. 애플리케이션이 새 구성을 사용하여 업데이트를 다운로드하려면 업데이트 소스에 새 구성과 호환되는 메타데이터가 있는 업데이트 파일이 포함되어 있어야 합니다. 업데이트 소스에 이전 구성과 호환되는 메타데이터가 있는 업데이트 파일이 포함된 경우 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다. 그렇지 않으면 업데이트 다운로드 작업이 실패합니다.

  예를 들어 로컬 또는 네트워크 폴더가 업데이트 소스로 지정되고 이 폴더의 업데이트 파일이 다음 애플리케이션 중 하나에서 다운로드된 경우 이 옵션을 활성화해야 합니다.

  - Kaspersky 업데이트 유틸리티

    이 유틸리티는 이전 구성을 사용하여 업데이트를 다운로드합니다.

- Kaspersky Security Center 13.2 또는 이전 버전

  예를 들어 배포 지점은 로컬 또는 네트워크 폴더에서 업데이트를 가져오도록 구성됩니다. 이 경우 인터넷에 연결된 중앙 관리 서버를 사용하여 업데이트를 다운로드한 다음 배포 지점의 로컬 폴더에 업데이트를 저장할 수 있습니다. 중앙 관리 서버의 버전이 13.2 이하인 경우 *배포 지점 저장소에 업데이트 다운로드* 작업에서 **이전 구성표를 사용해 업데이트 다운로드** 옵션을 활성화합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

10. 작업 시작 스케줄을 만듭니다. 필요한 경우 다음 설정을 지정합니다:

- **작업 시작**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **수동 시작**

    작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

    기본적으로 이 옵션은 선택되어 있습니다.

  - **N분마다**

    작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.
    기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

  - **N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.
    작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

  - **N일마다**

    작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.
    기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

  - **요일별**

    이 작업은 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
    기본적으로 이 작업은 매주 금요일 오후 6:00:00에 실행됩니다.

  - **월별**

    이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
    지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
    기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

  기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

  > 해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

  요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

- **누락된 작업 실행**

  이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

  이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 자동 임의 지연**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

11. **저장** 버튼을 누릅니다.

    작업이 생성 및 구성됩니다.

    작업 생성 중에 지정하는 설정뿐 아니라 생성된 작업의 기타 속성도 변경할 수 있습니다.

배포 지점의 저장소로 업데이트 다운로드 작업을 수행하면 데이터베이스 및 소프트웨어 모듈용 업데이트가 업데이트 경로에서 다운로드되어 공유 폴더에 저장됩니다. 다운로드한 업데이트는 지정한 관리 그룹에 포함되어 있으며 업데이트 다운로드 작업이 명시적으로 설정되지 않은 배포 지점에만 사용됩니다.

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치 활성/비활성

중앙 관리 서버용 업데이트 및 패치는 관리자의 명시적인 승인을 받은 후 수동으로만 설치할 수 있습니다.

Kaspersky Security Center 구성 요소용 업데이트 및 패치 자동 설치는 기기에 네트워크 에이전트를 설치할 때 기본적으로 활성됩니다. 네트워크 에이전트 설치 중에 업데이트 및 패치 자동 설치를 비활성할 수도 있고, 나중에 정책을 사용하여 자동 설치를 비활성할 수도 있습니다.

기기에서 네트워크 에이전트 로컬 설치를 수행하는 동안 Kaspersky Security Center 구성 요소의 자동 업데이트와 패치를 비활성하려면 다음과 같이 하십시오:

1. 기기에서 네트워크 에이전트 로컬 설치를 시작합니다.
2. **고급 설정** 단계에서 **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 확인란 선택을 취소합니다.
3. 마법사의 지침을 따릅니다.

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치가 비활성된 네트워크 에이전트가 기기에 설치됩니다. 정책을 사용하여 나중에 자동 업데이트 및 패치를 활성할 수 있습니다.

설치 패키지를 통해 기기에서 네트워크 에이전트 설치를 수행하는 동안 Kaspersky Security Center 구성 요소의 자동 업데이트와 패치를 비활성하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 저장소 → 설치 패키지**로 이동합니다.
2. **Kaspersky Security Center 네트워크 에이전트 <버전 번호>** 패키지를 누릅니다.
3. 속성 창에서 **설정** 탭을 엽니다.
4. **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 토글 버튼을 끕니다.

Kaspersky Security Center 구성 요소 자동 업데이트 및 패치가 비활성된 네트워크 에이전트가 이 패키지에서 설치됩니다. 정책을 사용하여 나중에 자동 업데이트 및 패치를 활성할 수 있습니다.

기기에 네트워크 에이전트를 설치하는 중에 이 확인란을 선택하거나 선택을 취소한 경우 나중에 네트워크 에이전트 정책을 사용하여 자동 업데이트를 활성하거나 비활성할 수 있습니다.

네트워크 에이전트 정책을 사용하여 Kaspersky Security Center 구성 요소의 자동 업데이트와 패치를 활성하거나 비활성하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**이동합니다.
2. 네트워크 에이전트 정책을 누릅니다.
3. 정책 속성 창에서 **애플리케이션 설정** 탭을 엽니다.
4. **패치 및 업데이트 관리** 섹션에서 **승인 상태가 정의 안 된 구성 요소용 업데이트와 패치가 있을 경우 이를 자동으로 설치** 토글 버튼을 켜거나 꺼 자동 업데이트 및 패치를 각각 활성화 또는 비활성화합니다.
5. 이 토글 버튼에 대해 잠금(🔒)을 설정합니다.

정책이 선택한 기기에 적용되고 해당 기기에서 Kaspersky Security Center 구성 요소 자동 업데이트 및 패치가 활성되거나 비활성됩니다.

Kaspersky Endpoint Security for Windows 업데이트 자동 설치

클라이언트 기기에 있는 Kaspersky Endpoint Security for Windows의 데이터베이스 및 소프트웨어 모듈에 대한 자동 업데이트를 구성할 수 있습니다.

기기에서 Kaspersky Endpoint Security for Windows에 대해 다운로드와 자동 업데이트 설치를 구성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **작업**로 이동합니다.

2. **추가** 버튼을 클릭합니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

3. Kaspersky Endpoint Security for Windows 애플리케이션의 경우 작업 하위 유형으로 **업데이트**를 선택합니다.

4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

5. 작업 범위를 선택합니다.

6. 관리 그룹, 기기 조회 또는 작업이 적용되는 기기를 지정합니다.

7. **작업 생성 마침** 단계에서 기본 작업 설정을 수정하려면 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

8. **생성** 버튼을 누릅니다.

   그러면 작업이 생성되고 작업 목록에 표시됩니다.

9. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

10. 작업 속성 창의 **애플리케이션 설정** 탭에서 로컬 또는 모바일 모드에서 업데이트 작업 설정을 정의합니다.

    - **로컬 모드**: 기기와 중앙 관리 서버 사이에 연결이 구성됩니다.

    - **모바일 모드**: Kaspersky Security Center와 기기 간에 설정된 연결이 없습니다(기기가 인터넷에 연결되지 않았을 때 등).

11. Kaspersky Endpoint Security for Windows용 데이터베이스 및 애플리케이션 모듈을 업데이트하는 데 사용할 업데이트 경로를 활성화합니다. 필요한 경우 **위로 이동** 및 **아래로 이동** 버튼을 사용하여 목록에서 경로 위치를 변경합니다. 여러 업데이트 경로가 활성화된 경우 Kaspersky Endpoint Security for Windows는 목록 상단부터 차례로 연결을 시도하고 사용 가능한 첫 번째 경로에서 업데이트 패키지를 검색하여 업데이트 작업을 수행합니다.

12. **승인된 애플리케이션 모듈 업데이트 설치** 옵션을 활성화하여 애플리케이션 데이터베이스와 함께 소프트웨어 모듈 업데이트를 다운로드하고 설치합니다.

    옵션이 선택되어 있다면, Kaspersky Endpoint Security for Windows는 소프트웨어 모듈 업데이트가 있을 경우 이를 사용자에게 알리고 업데이트 작업을 실행할 때 업데이트 패키지에 소프트웨어 모듈 업데이트를 포함합니다. Kaspersky Endpoint Security for Windows는 *승인됨* 상태를 설정한 업데이트만 설치하며, 이러한 업데이트는 애플리케이션 인터페이스 또는 Kaspersky Security Center를 통해 로컬로 설치됩니다.

    중요 애플리케이션 모듈 업데이트 자동 설치 옵션을 활성화할 수도 있습니다. 소프트웨어 모듈에 대한 업데이트가 있는 경우, Kaspersky Endpoint Security for Windows는 자동으로 *심각* 상태의 업데이트만 설치합니다. 나머지 업데이트는 관리자의 승인 이후에 설치됩니다.

    소프트웨어 모듈 업데이트가 라이센스 계약서 및 개인정보취급방침의 조장에 대해 검토하고 수락을 요구한다면, 애플리케이션은 최종 사용자 라이센스 계약서 및 개인정보취급방침이 관리자에 의해 수락된 후 업데이트를 설치합니다.

13. 지정된 폴더에 애플리케이션의 다운로드된 업데이트를 저장하려면 **폴더로 업데이트 복사** 확인란을 선택한 다음 폴더 경로를 지정합니다.

14. 작업 스케줄을 지정합니다. 업데이트를 적시에 제공하려면 **새로운 저장소 업데이트 다운로드를 완료한 후** 옵션을 선택하는 것이 좋습니다.

15. **저장**을 누릅니다.

업데이트 작업을 실행할 때 애플리케이션은 Kaspersky 업데이트 서버로 요청을 보냅니다.

일부 업데이트는 최신 버전의 관리 플러그인 설치를 요구하기도 합니다.

소프트웨어 업데이트 승인 및 거부

업데이트 설치 작업의 설정에서 설치할 업데이트에 대한 승인이 필요할 수 있습니다. 설치해야 하는 업데이트는 승인하고 설치하면 안 되는 업데이트는 거부할 수 있습니다.

예를 들어 업데이트가 기기 작동을 방해하지 않는지 테스트 환경에서 업데이트 설치를 먼저 확인한 후에만 클라이언트 기기에서 해당 업데이트 설치를 허용할 수 있습니다.

업데이트 승인 및 거부는 Windows 기반 클라이언트 기기에 설치한 네트워크 에이전트 및 관리 중인 애플리케이션에서만 사용할 수 있습니다. 중앙 관리 서버, Kaspersky Security Center 웹 콘솔 및 관리 웹 플러그인의 원활한 업데이트를 지원하지 않습니다. 이 구성 요소를 업데이트하려면 Kaspersky 웹사이트에서 최신 버전을 다운로드한 다음 수동 설치합니다.

업데이트 하나 또는 여러 개를 승인하거나 거부하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → Kaspersky 애플리케이션 → 원활한 업데이트**로 이동합니다.
   사용 가능한 업데이트 목록이 나타납니다.

   관리 중인 애플리케이션을 업데이트하려면 Kaspersky Security Center의 특정 최소 버전을 설치해야 할 수 있습니다. 이 버전이 현재 버전보다 최신 버전이면 이러한 업데이트가 표시되지만 승인할 수는 없습니다. 또한 Kaspersky Security Center를 업그레이드할 때까지 이러한 업데이트에서 설치 패키지를 생성 할 수 없습니다. Kaspersky Security Center 인스턴스를 필요한 최소 버전으로 업그레이드하라는 메시지가 표시됩니다.

2. 승인하거나 거부할 업데이트를 선택합니다.

3. **승인**을 눌러 선택한 업데이트를 승인하거나 **거부**를 눌러 선택한 업데이트를 거부합니다.
   기본값은 *정의 안 됨*입니다.

승인됨 상태를 할당하는 업데이트는 설치 대기열에 배치됩니다.

거부됨 상태를 할당하는 업데이트는 이전에 설치되었던 모든 기기에서 제거 가능한 경우 제거됩니다. 또한 앞으로 다른 기기에도 설치되지 않습니다.

Kaspersky 애플리케이션용 일부 업데이트는 제거할 수 없습니다. 이러한 업데이트에 대해 *거부됨* 상태를 설정하더라도 Kaspersky Security Center가 해당 업데이트가 이전에 설치되었던 기기에서 업데이트를 제거하지는 않습니다. 하지만 이러한 업데이트는 앞으로 다른 기기에 설치되지 않습니다.

타사 소프트웨어 업데이트에 대해 *거부됨* 상태를 설정하는 경우 이러한 업데이트를 설치하도록 계획했으나 아직 설치하지는 않은 기기에 업데이트가 설치되지 않습니다. 업데이트를 이미 설치한 기기에서는 업데이트가 그대로 유지됩니다. 이러한 업데이트를 삭제해야 하는 경우 로컬에서 수동으로 삭제할 수 있습니다.

중앙 관리 서버 업데이트

중앙 관리 서버 마법사 업데이트을(를) 사용하여 중앙 관리 서버 업데이트를 설치할 수 있습니다.

중앙 관리 서버 업데이트 설치하기:

1. 메인 메뉴에서 **동작 → Kaspersky 애플리케이션 → 원활한 업데이트** 로 이동합니다.
2. 다음 방법 중 하나로 중앙 관리 서버 마법사 업데이트을(를) 실행합니다.
   - 업데이트 목록에서 중앙 관리 서버 업데이트의 이름을 누르고, 창이 열리면 **중앙 관리 서버 업데이트 마법사 실행** 링크를 누릅니다.
   - 창 위쪽의 알림 필드에서 **중앙 관리 서버 업데이트 마법사 실행** 링크를 누릅니다.
3. 중앙 관리 서버 마법사 업데이트 창에서 다음 중 하나를 선택하여 업데이트를 설치할 시점을 지정합니다.
   - **지금 설치**. 지금 업데이트를 설치하려면 이 옵션을 선택합니다.
   - **설치 연기**. 나중에 업데이트를 설치하려면 이 옵션을 선택합니다. 이 경우 업데이트 알림이 표시됩니다.
   - **업데이트 무시**. 업데이트를 설치하지 않고 업데이트 알림을 받지 않으려면 이 옵션을 선택합니다.
4. 업데이트를 설치하기 전에 중앙 관리 서버의 백업을 생성하려면 **업데이트를 설치하기 전에 중앙 관리 서버의 백업 복사본 생성** 옵션을 선택합니다.
5. **확인** 버튼을 눌러 마법사를 완료합니다.

백업 프로세스가 중단되면 업데이트 설치 프로세스도 중단됩니다.

업데이트 다운로드 오프라인 모델 활성 및 비활성

업데이트 다운로드 오프라인 모델은 비활성하지 않는 것이 좋습니다. 이 모델을 비활성하면 기기로 업데이트를 전달하는 작업이 실패할 수 있습니다. 경우에 따라 Kaspersky 기술 지원 서비스 전문가가 **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드** 옵션을 비활성화하는 것이 좋다는 지침을 제공할 수 있습니다. 이 경우 Kaspersky 애플리케이션용 업데이트 수신을 위한 작업을 설정했는지 확인해야 합니다.

관리 그룹의 업데이트 다운로드 오프라인 모델을 활성화하거나 비활성화하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. **그룹**를 누릅니다.
3. 관리 그룹 구조에서 업데이트 다운로드 오프라인 모델을 활성해야 하는 관리 그룹을 선택합니다.
4. 네트워크 에이전트 정책을 누릅니다.
   네트워크 에이전트 정책의 속성 창이 열립니다.

   기본적으로 하위 정책 설정은 상위 정책에서 상속되며 수정할 수 없습니다. 수정하려는 정책이 상속된 경우 먼저 필요한 관리 그룹에서 네트워크 에이전트에 대한 새 정책을 만들어야 합니다. 새로 생성된 정책에서 상위 정책에서 고정되지 않은 설정을 수정할 수 있습니다.

5. **애플리케이션 설정** 탭에서 **패치 및 업데이트 관리** 섹션을 선택합니다.
6. **미리 중앙 관리 서버에서 업데이트 및 안티 바이러스 데이터베이스 다운로드(권장)** 옵션을 활성화 또는 비활성화하여 업데이트 다운로드 오프라인 모델을 활성하거나 비활성합니다.
   기본적으로 업데이트 다운로드의 오프라인 모델은 활성되어 있습니다.

업데이트 다운로드 오프라인 모델이 활성 또는 비활성됩니다.

오프라인 기기에서 Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트

관리 중인 기기에서 Kaspersky 데이터베이스 및 소프트웨어 모듈을 업데이트하는 것은 바이러스 및 기타 위협으로부터 기기 보호를 유지하는 데 중요한 작업입니다. 관리자는 일반적으로 중앙 관리 서버 저장소 또는 배포 지점 저장소를 사용하여 정기 업데이트를 구성합니다.

중앙 관리 서버(기본 또는 보조), 배포 지점 또는 인터넷에 연결되지 않은 기기(또는 기기 그룹)에서 데이터베이스 및 소프트웨어 모듈을 업데이트한다면, FTP 서버 또는 로컬 폴더와 같은 대체 업데이트 경로를 사용해야 합니다. 이 경우 플래시 드라이브 또는 외장 하드 드라이브와 같은 대용량 스토리지 기기를 사용하여 필요한 업데이트 파일을 전달해야 합니다.

다음에서 필요한 업데이트를 복사할 수 있습니다.

- 중앙 관리 서버.

  중앙 관리 서버 저장소에 오프라인 기기에 설치된 보안 제품에 필요한 업데이트가 포함되도록 하려면 관리 중인 온라인 기기 중 하나 이상에 동일한 보안 제품이 설치되어 있어야 합니다. 이 애플리케이션은 중앙 관리 서버 저장소에 업데이트 다운로드 작업을 통해 중앙 관리 서버 저장소에서 업데이트를 받도록 구성해야 합니다.

- 동일한 보안 제품이 설치되어 있고 중앙 관리 서버 저장소, 배포 지점 저장소 또는 Kaspersky 업데이트 서버에서 직접 업데이트를 받도록 구성된 모든 기기.

다음은 중앙 관리 서버 저장소에서 복사하여 데이터베이스 및 소프트웨어 모듈의 업데이트를 구성하는 예입니다.

오프라인 기기에서 Kaspersky 데이터베이스 및 소프트웨어 모듈을 업데이트하려면 다음 단계를 따릅니다.

1. 이동식 드라이브를 중앙 관리 서버가 설치된 기기에 연결합니다.

2. 업데이트 파일을 이동식 드라이브에 복사합니다.

   기본적으로 업데이트는 다음에 위치합니다. \\<server name> \ KLSHARE \ Updates

   또는 선택한 폴더에 업데이트를 정기적으로 복사하도록 Kaspersky Security Center를 구성할 수 있습니다. 이렇게 하려면 중앙 관리 서버 저장소에 업데이트 다운로드 작업의 속성에서 **추가 폴더에 다운로드한 업데이트 복사** 옵션을 사용합니다. 이 옵션의 대상 폴더로 플래시 드라이브 또는 외장 하드 드라이브에 있는 폴더를 지정하면, 이 대용량 스토리지 기기에 항상 최신 버전의 업데이트가 포함됩니다.

3. 오프라인 기기에서 로컬 폴더 또는 TP 서버나 공유 폴더와 같은 공유 경로에서 업데이트를 받도록 보안 애플리케이션(예: Kaspersky Endpoint Security for Windows)을 구성합니다.

4. 이동식 드라이브에서 업데이트 파일을 업데이트 경로로 사용할 로컬 폴더 또는 공유 경로로 복사합니다.

5. 업데이트 설치가 필요한 오프라인 기기에서 Kaspersky Endpoint Security for Windows의 업데이트 작업을 시작합니다.

업데이트 작업이 완료되면 Kaspersky 데이터베이스 및 소프트웨어 모듈이 기기에서 최신 상태가 됩니다.

웹 플러그인 백업 및 복원

Kaspersky Security Center 웹 콘솔을 사용하면 웹 플러그인의 현재 상태를 백업하여 나중에 저장된 상태를 복원할 수 있습니다. 예를 들어 웹 플러그인을 최신 버전으로 업데이트하기 전에 백업해둘 수 있습니다. 업데이트 후 최신 버전이 요구 사항이나 기대치를 충족하지 못하는 경우 백업에서 웹 플러그인의 이전 버전을 복원할 수 있습니다.

웹 플러그인을 백업하려면:

1. 메인 메뉴에서 **설정 → 웹 플러그인**으로 이동합니다.

2. **웹 플러그인** 섹션에서 백업할 웹 플러그인을 선택하고 **백업 복사본 생성** 버튼을 클릭합니다.

선택한 웹 플러그인이 백업됩니다. 생성한 백업은 **백업** 섹션에서 볼 수 있습니다.

백업에서 웹 플러그인을 복원하려면:

1. 메인 메뉴에서 **설정** → **백업**으로 이동합니다.
2. **백업** 섹션에서 복원할 웹 플러그인을 선택하고, **백업에서 복원** 버튼을 클릭합니다.

선택한 백업에서 웹 플러그인이 복원됩니다.

배포 지점 및 연결 게이트웨이 조정

Kaspersky Security Center의 관리 그룹 구조는 다음과 같은 기능을 수행합니다:

- 정책의 범위 설정

  *정책 프로필*을 사용하여 기기에서 관련 설정 모음을 적용할 수도 있습니다. 이때는 태그, Active Directory 조직 구성 단위의 기기 위치, Active Directory 보안 그룹의 구성원 자격 등을 사용하여 정책의 범위를 설정합니다.

- 그룹 작업의 범위 설정

  관리 그룹의 계층 구조를 기준으로 하지 않는 그룹 작업은 특정 방식으로 범위를 정의합니다: 즉, 이러한 작업의 경우에는 기기 조회용 작업과 특정 기기용 작업을 사용합니다.

- 기기, 가상 중앙 관리 서버 및 보조 중앙 관리 서버에 대한 접근 권한 설정

- 배포 지점 할당

관리 그룹의 구조를 작성할 때는 배포 지점을 가장 적절하게 할당할 수 있도록 조직 네트워크의 토폴로지를 고려해야 합니다. 배포 지점을 최적의 방식으로 배포하면 조직 네트워크의 트래픽을 절약할 수 있습니다.

조직 스키마와 네트워크 토폴로지에 따라 관리 그룹 구조에 다음 표준 구성을 적용할 수 있습니다:

- 단일 사무소
- 다수의 소규모 원격 사무소

배포 지점 기능을 하는 기기는 무단으로 접근할 수 없도록 보호(물리적 보호 포함)해야 합니다.

배포 지점의 표준 구성: 단일 사무소

표준 "단일 사무소" 구성에서는 모든 기기가 조직 네트워크에 있으므로 기기 간에 서로 "인식"할 수 있습니다. 조직 네트워크는 협채널을 통해 연결된 몇 개의 개별 요소(네트워크 또는 네트워크 세그먼트)로 구성될 수 있습니다.

관리 그룹 구조를 구성하는 데 사용할 수 있는 방법은 다음과 같습니다:

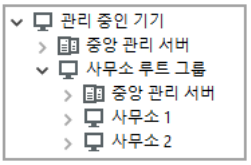
- 네트워크 토폴로지를 고려하여 관리 그룹 구조 구성. 관리 그룹의 구조가 정밀하게 네트워크 토폴로지를 반영하지 않을 수 있습니다. 네트워크의 각 부분과 특정 관리 그룹을 연결하는 걸로도 충분합니다. 배포 지점의 자동 할당을 사용할 수도 있고 수동으로 할당할 수도 있습니다.

- 네트워크 토폴로지를 고려하지 않고 관리 그룹 구조 구성. 이 경우 배포 지점의 자동 할당을 비활성하고 네트워크의 각 부분(예: **관리 중인 기기** 그룹)에서 하나 이상의 기기가 루트 관리 그룹의 배포 지점 역할을 하도록 직접 지정해야 합니다. 모든 배포 지점은 동일한 수준에 있으며 조직 네트워크의 모든 기기에 동일한 영역을 적용합니다. 이때, 각 네트워크 에이전트는 경로가 가장 짧은 배포 지점과 연결됩니다. 배포 지점 연결 경로는 tracert 유틸리티로 추적할 수 있습니다.

배포 지점의 표준 구성: 다수의 소규모 원격 사무소

이 표준 구성은 인터넷을 통해 본사 사무소와 통신할 수 있는 여러 소규모 원격 사무소를 제공합니다. 각 원격 사무소에는 NAT가 적용됩니다. 즉, 원격 사무소는 서로 격리되므로 사무소 간의 연결은 불가능합니다.

이 구성을 관리 그룹 구조에 반영해야 합니다: 각 원격 사무소에 대해 별도의 관리 그룹(아래 그림의 **사무소 1** 및 **사무소 2** 그룹)을 만들어야 합니다.



관리 그룹 구조에 포함된 원격 사무소

사무소에 해당하는 각 관리 그룹에는 배포 지점을 하나 이상 할당해야 합니다. 배포 지점은 원격 사무소의 기기여야 하며, 디스크에 여유 공간이 충분해야 합니다. 예를 들어 **사무소 1** 그룹에 배포된 기기는 **사무소 1** 관리 그룹에 할당된 배포 지점에 접근합니다.

일부 사용자가 노트북을 소지하고 사무소 간을 실제로 이동하는 경우에는 기존 배포 지점 외에 각 원격 사무소에서 둘 이상의 기기를 선택하여 상위 레벨 관리 그룹(위 그림에서는 **사무소 루트 그룹**)의 배포 지점 역할을 하도록 할당해야 합니다.

예: **사무소 1** 관리 그룹에 배포된 노트북이 **사무소 2** 관리 그룹에 해당하는 사무소로 실제로 이동되었습니다. 노트북이 이동된 후 네트워크 에이전트가 **사무소 1** 그룹에 할당된 배포 지점 접근을 시도하지만 해당 배포 지점은 사용할 수 없는 상태입니다. 그러면 네트워크 에이전트는 **사무소 루트 그룹**에 할당된 배포 지점에 대한 접근 시도를 시작합니다. 원격 사무소는 서로 격리되어 있으므로 **사무소 루트 그룹** 관리 그룹에 할당된 배포 지점 접근 시도는 네트워크 에이전트가 **사무소 2** 그룹의 배포 지점 접근을 시도할 때만 성공합니다. 즉, 노트북은 초기 사무소에 해당하는 관리 그룹에 그대로 유지되지만 해당 시점에 물리적으로 위치해 있는 사무소의 배포 지점을 사용합니다.

배포 지점 할당 정보

관리 중인 기기를 수동으로 또는 자동으로배포 지점으로 할당할 수 있습니다.

관리 중인 기기를 수동으로 배포 지점으로 할당하는 경우 네트워크에서 어떤 기기든 선택할 수 있습니다.

배포 지점을 자동으로 할당하는 경우 Kaspersky Security Center는 다음 조건을 충족하는 관리 중인 기기만 선택할 수 있습니다.

- 기기에 최소 50GB의 디스크 여유 공간이 있습니다.
- 관리 중인 기기가 Kaspersky Security Center와 직접 연결되어 있습니다(게이트웨이 없이).
- 관리 중인 기기가 랩탑이 아닙니다.

> 네트워크가 지정된 조건을 충족하지 않는 경우 Kaspersky Security Center는 어떤 기기도 배포 지점으로 자동 할당하지 않습니다.

배포 지점 자동 할당

배포 지점을 자동으로 할당하는 것이 좋습니다. 이 경우 Kaspersky Security Center는 배포 지점을 할당해야 하는 기기를 자체적으로 선택합니다.

배포 지점을 자동으로 할당하려면 다음 절차를 따르십시오.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **배포 지점** 섹션을 선택합니다.
3. **배포 지점 자동 할당** 옵션을 선택합니다.

   > 배포 지점 역할을 수행하는 기기를 자동으로 할당하면, 배포 지점을 수동으로 구성할 수 없으며 배포 지점 목록도 편집할 수 없습니다.

4. **저장** 버튼을 누릅니다.

중앙 관리 서버는 자동으로 배포 지점을 할당하고 구성합니다.

배포 지점 수동 할당

Kaspersky Security Center를 사용하면 배포 지점 역할을 수행하는 기기를 수동으로 할당할 수 있습니다.

배포 지점을 자동으로 할당하는 것이 좋습니다. 이 경우 Kaspersky Security Center는 배포 지점을 할당해야 하는 기기를 자체적으로 선택합니다. 그러나 어떠한 이유로 배포 지점을 자동으로 할당하지 않도록 해야 하는 경우(예, 배포 지점 전용 서버를 사용하고자 할 경우)에는 배포 지점 개수와 구성을 계산한 후에 배포 지점을 수동으로 할당할 수 있습니다.

배포 지점 기능을 하는 기기는 무단으로 접근할 수 없도록 보호(물리적 보호 포함)해야 합니다.

수동으로 배포 지점 역할을 수행하는 기기를 할당하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **배포 지점** 섹션을 선택합니다.
3. **배포 지점 수동 할당** 옵션을 선택합니다.
4. **할당** 버튼을 누릅니다.
5. 배포 지점을 만들 기기를 선택합니다.
   기기를 선택할 때 배포 지점의 운영 특성과 배포 지점 역할을 수행하는 기기에 대한 요구 사항을 유의하십시오.
6. 선택한 배포 지점의 범위에 포함할 관리 그룹을 선택합니다.
7. **확인** 버튼을 누릅니다.
   추가한 배포 지점은 **배포 지점** 섹션의 배포 지점 목록에 표시됩니다.
8. 목록에서 새로 추가된 배포 지점을 클릭하여 속성 창을 엽니다.
9. 속성 창에서 배포 지점 구성:
   - **일반** 섹션에는 클라이언트 기기와 배포 지점 간의 상호 작용 설정이 포함되어 있습니다:
     - **SSL 포트**

       SSL을 사용하는 클라이언트 기기와 배포 지점 간의 암호화된 연결용 SSL 포트의 번호입니다.
       기본적으로 포트 13000이 사용됩니다.

     - **멀티캐스트 사용**

       이 옵션을 사용하면 IP 멀티캐스트를 사용하여 설치 패키지가 그룹의 클라이언트 기기에 자동으로 배포됩니다.
       IP 멀티캐스팅을 사용하면 설치 패키지에서 클라이언트 기기 그룹으로 애플리케이션을 설치하는 데 걸리는 시간은 줄어들지만 단일 클라이언트 기기로 애플리케이션을 설치하는 경우에는 설치 시간이 증가합니다.

     - **IP 멀티캐스트 주소**

       멀티캐스팅에 사용할 IP 주소입니다. 224.0.0.0 – 239.255.255.255 범위의 IP 주소를 정의할 수 있습니다
       기본적으로 Kaspersky Security Center는 주어진 범위 내에서 고유한 IP 멀티캐스트 주소를 자동으로 할당합니다.

     - **IP 멀티캐스트 포트 번호**

       IP 멀티캐스팅용 포트의 번호입니다.

기본 포트 번호는 15001입니다. 중앙 관리 서버가 설치된 기기가 배포 지점으로 지정된 경우 기본적으로 포트 13001이 SSL 연결에 사용됩니다.

- **원격 기기의 배포 지점 주소**

  원격 기기가 배포 지점에 연결하는 데 사용하는 IPv4 주소입니다.

- **업데이트 배포**

  업데이트는 다음 소스에서 관리 중인 기기로 배포됩니다.

  - 이 옵션이 활성화된 경우 이 배포 지점입니다.
  - 이 옵션이 비활성화된 경우 다른 배포 지점, 중앙 관리 서버 또는 Kaspersky 업데이트 서버입니다.

  배포 지점을 사용하여 업데이트를 배포하면 다운로드 수가 줄어들기 때문에 트래픽을 절약할 수 있습니다. 또한 중앙 관리 서버의 로드를 줄이고 배포 지점 간에 부하를 재배치할 수 있습니다. 네트워크에 필요한 배포 지점의 수를 계산 하여 트래픽과 부하를 최적화할 수 있습니다.

  이 옵션을 비활성화하면 업데이트 다운로드 수와 중앙 관리 서버의 부하가 증가할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다.

- **설치 패키지 배포**

  설치 패키지는 다음 소스에서 관리 중인 기기로 배포됩니다.

  - 이 옵션이 활성화된 경우 이 배포 지점입니다.
  - 이 옵션이 비활성화된 경우 다른 배포 지점, 중앙 관리 서버 또는 Kaspersky 업데이트 서버입니다.

  배포 지점을 사용하여 설치 패키지를 배포하면 다운로드 수가 줄어들기 때문에 트래픽을 절약할 수 있습니다. 또한 중앙 관리 서버의 로드를 줄이고 배포 지점 간에 부하를 재배치할 수 있습니다. 네트워크에 필요한 배포 지점의 수를 계산 하여 트래픽과 부하를 최적화할 수 있습니다.

  이 옵션을 비활성화하면 설치 패키지 다운로드 수와 중앙 관리 서버의 부하가 증가할 수 있습니다. 기본적으로 이 옵션은 켜져 있습니다.

- **푸시 서버 실행**

  Kaspersky Security Center에서 배포 지점은 모바일 프로토콜을 통해 관리되는 기기 및 네트워크 에이전트를 통해 관리되는 기기에 대한 푸시 서버로 작동될 수 있습니다. 예를 들어, KasperskyOS 기기를 중앙 관리 서버에 강제로 동기화하려면 푸시 서버를 활성화해야 합니다. 푸시 서버에는 푸시 서버가 활성화된 배포 지점과 동일한 수준의 관리 중인 기기가 있습니다. 동일한 관리 그룹에 여러 배포 지점이 할당된 경우 각 배포 지점에서 푸시 서버를 활성화할 수 있습니다. 이 경우 중앙 관리 서버는 배포 지점 간의 로드 균형을 조정합니다.

- **푸시 서버 포트**

  푸시 서버용 포트 번호. 비어 있는 포트의 번호를 지정할 수 있습니다.

- **범위** 섹션에서는 배포 지점이 어느 범위까지 업데이트를 배포할 것인지 지정합니다(관리 그룹 및/또는 네트워크 위치).

  Windows 운영 체제를 실행하는 기기만 해당 네트워크 위치를 확인할 수 있습니다. 다른 운영 체제를 실행하는 기기의 경우에는 네트워크 위치를 확인할 수 없습니다.

- 배포 지점이 중앙 관리 서버 이외의 시스템에서 작동한다면 **업데이트 경로** 섹션에서 배포 지점에 대한 업데이트 경로를 선택할 수 있습니다.

  - **업데이트 경로**

    배포 지점에 대한 업데이트 경로를 지정해 주십시오:
    - 배포 지점이 중앙 관리 서버에서 업데이트를 받게 하려면, **중앙 관리 서버에서 가져오기**를 선택합니다.
    - 배포 지점이 작업을 사용하여 업데이트를 수신하려면 **업데이트 다운로드 작업 사용**을 선택한 다음 *배포 지점 저장소에 업데이트 다운로드* 작업을 지정합니다.
      - 이러한 작업이 기기에 이미 있는 경우 목록에서 작업을 선택합니다.
      - 기기에 해당 작업이 없다면 **작업 생성**링크를 눌러 작업을 만듭니다. 새 작업 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

  - **diff 파일 다운로드**

    이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

    기본적으로 이 옵션은 켜져 있습니다.

- 배포 지점에서 인터넷에 연결할 때 프록시 서버를 사용하는 경우 **인터넷 연결 설정** 하위 섹션에서 다음 설정을 지정할 수 있습니다:

  - **프록시 서버 사용**

    이 확인란을 선택하면 입력 필드에서 프록시 서버 연결을 구성할 수 있습니다.
    기본적으로 이 확인란은 선택되어 있지 않습니다.

  - **프록시 서버 주소**

    프록시 서버 주소입니다.

  - **포트 번호**

    연결에 사용되는 포트 번호.

  - **로컬 주소에서 프록시 서버 사용 안 함**

    이 옵션을 사용하면 로컬 네트워크에서 기기로 연결하는 데 프록시 서버가 사용되지 않습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **프록시 서버 인증**

  이 확인란을 선택하면 입력 필드에서 프록시 서버 인증에 사용할 자격증명을 지정할 수 있습니다.
  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **사용자 이름**

  프록시 서버에 대한 연결을 구성할 사용자 계정입니다.

- **암호**

  작업을 실행할 계정의 암호입니다.

- **KSN 프록시** 섹션에서는 애플리케이션이 배포 지점을 사용하여 관리 중인 기기에서 KSN 요청을 전달하도록 구성할 수 있습니다:

  - **배포 지점 측에서 KSN 프록시 기능 활성화**

    배포 지점으로 사용되는 기기에서 KSN 프록시 서비스가 실행됩니다. 네트워크에서 트래픽을 재분배하고 최적화하려면 이 기능을 사용합니다.

    배포 지점은 Kaspersky Security Network 진술문에 나열된 KSN 통계를 Kaspersky에 보냅니다.

    기본적으로 이 옵션은 비활성화되어 있습니다. 중앙 관리 서버 속성 창에서 **KSN 프록시 서버로 중앙 관리 서버 사용**과 **Kaspersky Security Network 사용에 동의합니다** 옵션이 활성화되어야만 이 옵션이 활성화됩니다.

    액티브-패시브 클러스터의 노드에 배포 지점을 할당하고 이 노드에 KSN 프록시 서버를 활성화할 수 있습니다.

  - **중앙 관리 서버에 KSN 요청 전달**

    배포 지점이 관리 중인 기기에서 중앙 관리 서버로 KSN 요청을 전달합니다.
    기본적으로 이 옵션은 켜져 있습니다.

  - **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근**

    배포 지점이 관리 중인 기기에서 KSN 클라우드 또는 KPSN으로 KSN 요청을 전달합니다. 배포 지점 자체에서 생성된 KSN 요청은 KSN 클라우드 또는 KPSN으로 직접 전송됩니다.

    네트워크 에이전트 버전 11 이하가 설치된 배포 지점은 KPSN에 직접 접근할 수 없습니다. KSN 요청을 KPSN으로 전송하도록 배포 지점을 재구성하면, 각 배포 지점에 대하여 **중앙 관리 서버에 KSN 요청 전달** 옵션을 활성화합니다.

    네트워크 에이전트 버전 12 이상이 설치된 배포 지점은 KPSN에 직접 접근할 수 있습니다.

- **KPSN에 연결할 때 프록시 서버 설정 무시**

  배포 지점 속성 또는 네트워크 에이전트 정책에 프록시 서버 설정이 구성되어 있지만 네트워크 아키텍처에서 KPSN을 직접 사용해야 한다면 이 옵션을 활성화합니다. 이렇게 하지 않으면 관리 중인 애플리케이션의 요청을 KPSN으로 전송할 수 없습니다.

  이 옵션을 사용하려면 **인터넷을 통해 KSN 클라우드/KPSN에 직접 접근** 옵션을 활성화해야 합니다.

- **Port**

  관리 중인 기기가 KSN 프록시 서버에 연결하는 데 사용할 TCP 포트의 번호입니다. 기본 포트 번호는 13111입니다.

- **UDP 포트 사용**

  UDP 포트를 통해 관리 중인 기기를 KSN 프록시 서버에 연결하려면, **UDP 포트 사용** 옵션을 선택하고 UDP 포트 번호를 지정합니다. 기본적으로 이 옵션은 켜져 있습니다.

- **UDP 포트**

  관리 중인 기기가 KSN 프록시 서버에 연결하는 데 사용할 UDP 포트의 번호입니다. KSN 프록시 서버에 연결하는 기본 UDP 포트는 15111입니다.

- 배포 지점이 중앙 관리 서버 이외의 시스템에서 작동한다면 **연결 게이트웨이** 섹션에서 네트워크 에이전트 인스턴스와 중앙 관리 서버 간의 연결을 위한 게이트웨이 역할을 하도록 배포 지점을 구성할 수 있습니다.

  - **연결 게이트웨이**

    네트워크 구성으로 중앙 관리 서버와 네트워크 에이전트 간의 직접 연결을 설정할 수 없다면, 배포 지점을 사용하여 중앙 관리 서버와 네트워크 에이전트 간의 연결 게이트웨이 역할을 하도록 할 수 있습니다.

    네트워크 에이전트와 중앙 관리 서버 간의 연결 게이트웨이 역할을 할 배포 지점이 필요하다면 이 옵션을 활성화합니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

  - **중앙 관리 서버에서 게이트웨이로 연결 설정(DMZ에 게이트웨이가 있을 시)**

    중앙 관리 서버가 비무장 지대(DMZ) 외부에 있을 시 로컬 영역 네트워크에서 원격 기기에 설치된 네트워크 에이전트는 중앙 관리 서버에 연결할 수 없습니다. 역방향 연결이 있는 연결 게이트웨이로 배포 지점을 사용할 수 있습니다(관리 서버는 배포 지점에 대한 연결을 설정).

    중앙 관리 서버를 DMZ의 연결 게이트웨이에 연결해야 한다면 이 옵션을 활성화합니다.

  - **Kaspersky Security Center 웹 콘솔용 로컬 포트 열기**

    DMZ 또는 인터넷에 있는 웹 콘솔용 포트를 열기 위해 DMZ의 연결 게이트웨이가 필요하다면 이 옵션을 활성화합니다. 웹 콘솔에서 배포 지점으로의 연결에 사용할 포트 번호를 지정합니다. 기본 포트 번호는 13299입니다.

    이 옵션은 **중앙 관리 서버에서 게이트웨이로 연결 설정(DMZ에 게이트웨이가 있을 시)** 옵션을 활성화한 경우에 사용할 수 있습니다.

연결 게이트웨이 역할을 하는 배포 지점을 통해 모바일 기기를 중앙 관리 서버에 연결할 때 다음 옵션을 활성화할 수 있습니다.

- **모바일 기기용 포트 열기(중앙 관리 서버의 SSL 인증용)**

  모바일 기기용 포트를 열기 위해 연결 게이트웨이가 필요하다면, 이 옵션을 활성화하고 모바일 기기가 배포 지점에 연결하는 데 사용할 포트 번호를 지정합니다. 기본 포트 번호는 13292입니다. 모바일 기기가 중앙 관리 서버 인증서를 확인합니다. 연결을 설정할 때 중앙 관리 서버만 인증됩니다.

- **모바일 기기용 포트 열기(상호간의 SSL 인증)**

  중앙 관리 서버와 모바일 기기의 양방향 인증에 사용할 포트를 열기 위해 연결 게이트웨이가 필요하다면 이 옵션을 활성화합니다. 모바일 기기는 중앙 관리 서버 인증서를 확인하고 중앙 관리 서버는 모바일 기기 인증서를 확인합니다. 다음 파라미터를 지정합니다:

  - 모바일 기기가 배포 지점에 연결하는 데 사용할 포트 번호. 기본 포트 번호는 13293입니다.
  - 모바일 기기에서 사용할 연결 게이트웨이의 DNS 도메인 이름. 도메인 이름은 쉼표로 구분합니다. 지정된 도메인 이름은 배포 지점 인증서에 포함됩니다. 모바일 기기에서 사용하는 도메인 이름이 배포 지점 인증서의 일반 이름과 일치하지 않으면 모바일 기기가 배포 지점에 연결되지 않습니다.

    기본 DNS 도메인 이름은 연결 게이트웨이의 FQDN 이름입니다.

두 경우 모두 배포 지점에서 TLS 세션을 설정하는 동안에만 인증서를 확인합니다. 인증서는 중앙 관리 서버의 확인을 위해 전달되지 않습니다. 모바일 기기와 TLS 세션이 설정되면 배포 지점에서 중앙 관리 서버 인증서를 사용하여 모바일 기기와 중앙 관리 서버 간의 동기화를 위한 터널을 생성합니다. 양방향 SSL 인증을 위해 포트를 열 경우, 모바일 기기 인증서를 배포하려면 설치 패키지를 사용해야만 합니다.

- 배포 지점에 의한 Windows 도메인, Active Directory 및 IP 범위의 검색을 구성합니다:

  - **Windows 도메인**

    Windows 도메인에 대해 기기 발견을 활성화하고 발견 스케줄을 설정할 수 있습니다.

  - **도메인 컨트롤러**

    Active Directory에 대해 네트워크 검색을 활성화하고 검색 스케줄을 설정할 수 있습니다.

    Windows 배포 지점을 사용한다면 다음 옵션 중 하나를 선택할 수 있습니다.

    - **현재 Active Directory 도메인 검색**.
    - **Active Directory 도메인 포레스트 검색**.
    - **선택한 Active Directory 도메인만 검색**. 이 옵션을 선택하는 경우 Active Directory 도메인 하나 이상을 목록에 추가합니다.

    네트워크 에이전트 버전 15가 설치된 Linux 배포 지점을 사용하는 경우 주소 및 사용자 자격 증명을 지정한 Active Directory 도메인만 검색할 수 있습니다. 현재 Active Directory 도메인 및 Active Directory 도메인 포레스트에 대한 검색을 사용할 수 없습니다.

    도메인 컨트롤러에 대해 기기 발견을 활성화할 수 있습니다.

도메인 컨트롤러 검색 활성화 옵션을 선택하면 검색할 도메인 컨트롤러를 선택하고 이에 대한 검색 스케줄도 지정할 수 있습니다.

Linux 배포 지점을 사용하면 **지정한 도메인 검색** 섹션에서 **추가**를 클릭한 다음 도메인 컨트롤러의 주소와 사용자 자격 증명을 지정합니다.

Windows 배포 지점을 사용한다면 다음 옵션 중 하나를 선택할 수 있습니다.

- **현재 도메인 검색**
- **전체 도메인 포레스트 검색**
- **지정한 도메인 검색**

- **IP 범위**

IPv4 범위 및 IPv6 네트워크에 대해 기기 발견을 활성화할 수 있습니다.

범위 검색 사용 옵션을 사용하는 경우 검사 범위를 추가하고 해당 범위에 대해 스케줄을 설정할 수 있습니다. 검사한 범위 목록에 IP 범위를 추가할 수 있습니다.

이 **Zeroconf을 사용하여 IPv6 네트워크 검색** 옵션을 활성화하면 배포 지점에서 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 IPv6 네트워크를 자동으로 검색합니다. 이 경우 배포 지점에서 전체 네트워크를 검색하기 때문에 지정된 IP 범위가 무시됩니다. 배포 지점에서 Linux를 실행 시, **Zeroconf을 사용하여 IPv6 네트워크 검색** 옵션을 사용할 수 있습니다. Zeroconf IPv6 검색을 사용하려면, 배포 지점에 avahi-browse 유틸리티를 설치해야 합니다.

- **고급** 섹션에서 배포된 데이터를 저장하기 위해 배포 지점이 사용할 폴더를 지정합니다:

- **기본 폴더 사용**

이 옵션을 선택하면 애플리케이션이 배포 지점의 네트워크 에이전트 설치 폴더를 사용합니다.

- **지정한 폴더 사용**

이 옵션을 선택하면 아래의 필드에서 폴더의 경로를 지정할 수 있습니다. 이 폴더는 배포 지점의 로컬 폴더일 수도 있고, 회사 네트워크에 있는 기기의 폴더일 수도 있습니다.

배포 지점에서 네트워크 에이전트를 실행하는 데 사용되는 사용자 계정에는 지정한 폴더에 대한 읽기/쓰기 권한이 있어야 합니다.

10. **확인** 버튼을 누릅니다.

선택한 기기는 배포 지점으로 역할을 수행하게 됩니다.

관리 그룹의 배포 지점 목록 수정

특정 관리 그룹에 할당된 배포 지점 목록을 보고 배포 지점을 추가하거나 제거하여 목록을 수정할 수 있습니다.

관리 그룹에 할당된 배포 지점 목록을 보고 수정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
2. 관리 중인 기기 목록 위의 **현재 경로** 필드에서 경로 링크를 클릭합니다.
3. 열리는 왼쪽 창에서 할당된 배포 지점을 보려는 관리 그룹을 선택합니다.
   이렇게 하면 **배포 지점** 메뉴 항목이 활성화됩니다.
4. 메인 메뉴에서 **에셋(기기) → 배포 지점** 탭으로 이동합니다.
5. 관리 그룹에 대한 새 배포 지점을 추가하려면 관리 중인 기기 목록 위에 있는 **할당** 버튼을 클릭하고 열리는 창에서 기기를 선택합니다.
6. 할당된 배포 지점을 제거하려면 목록에서 기기를 선택하고 **할당 해제** 버튼을 클릭합니다.

수정 사항에 따라 새 배포 지점이 목록에 추가되거나 기존 배포 지점이 목록에서 제거됩니다.

강제 동기화

Kaspersky Security Center는 관리 중인 기기치의 상태, 설정, 작업 및 정책을 자동으로 동기화하지만 경우에 따라 지정된 기기에 대해 동기화를 강제로 실행해야 할 수도 있습니다. 다음 기기에 대해 강제 동기화를 실행할 수 있습니다.

- 네트워크 에이전트가 설치된 미할당 기기
- KasperskyOS를 실행하는 기기
  KasperskyOS 기기에 대해 강제 동기화를 실행하기 전에 기기가 배포 지점 범위에 포함되어 있고 배포 지점에 푸시 서버가 활성화되어 있는지 확인하십시오.
- iOS 기기
- Android 기기
  Android 기기에 대해 강제 동기화를 실행하기 전에 Firebase Cloud Messaging을 구성해야 합니다.

단일 기기 동기화

중앙 관리 서버와 관리 중인 기기 간의 강제 동기화를 수행하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기** 로 이동합니다.
2. 중앙 관리 서버와 동기화할 기기의 이름을 누릅니다.
   일반 섹션이 선택된 상태로 속성 창이 열립니다.
3. **강제 동기화** 버튼을 클릭합니다.

애플리케이션이 선택한 기기를 중앙 관리 서버와 동기화합니다.

여러 기기 동기화

중앙 관리 서버와 여러 관리 중인 기기 간의 강제 동기화를 수행하려면 다음 단계를 따릅니다.

1. 관리 그룹의 기기 목록 또는 기기 조회를 엽니다.

   - 기본 메뉴에서 **에셋(기기)** → **관리 중인 기기**로 이동하여 관리 중인 기기 목록 위의 **현재 경로** 필드에서 경로 링크를 클릭한 다음, 동기화할 기기가 포함된 관리 그룹을 선택합니다.
   - 기기 목록을 보려면 기기 조회를 실행합니다.

2. 중앙 관리 서버와 동기화하려는 기기 옆의 확인란을 선택합니다.

3. 관리 중인 기기 목록 위의 줄임표 버튼(**...**)을 클릭하고 **강제 동기화** 버튼을 클릭합니다.
   애플리케이션이 선택한 기기를 중앙 관리 서버와 동기화합니다.

4. 기기 목록에서 선택한 기기에 대해 중앙 관리 서버에 마지막으로 연결한 시간이 현재 시간으로 변경되었는지 확인합니다. 시간이 변경되지 않은 경우 **새로 고침** 버튼을 눌러 페이지 컨텐츠를 업데이트합니다.

선택한 기기가 중앙 관리 서버와 동기화됩니다.

정책 전달 시간 보기

중앙 관리 서버에서 Kaspersky 애플리케이션의 정책을 변경한 후 관리자는 변경된 정책이 특정 관리 중인 기기로 전달되었는지를 확인할 수 있습니다. 정책은 일반 동기화 또는 강제 동기화 중에 전달될 수 있습니다.

애플리케이션 정책이 관리 중인 기기로 전달된 날짜와 시간을 확인하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **관리 중인 기기** 로 이동합니다.

2. 중앙 관리 서버와 동기화할 기기의 이름을 누릅니다.
   일반 섹션이 선택된 상태로 속성 창이 열립니다.

3. **애플리케이션** 탭을 선택합니다.

4. 정책 동기화 날짜를 확인할 애플리케이션을 선택합니다.
   일반 섹션이 선택되어 있고 정책 전달 날짜와 시간이 표시된 애플리케이션 정책 창이 열립니다.

푸시 서버 활성화

Kaspersky Security Center에서 배포 지점은 모바일 프로토콜을 통해 관리 중인 기기 및 네트워크 에이전트를 통해 관리 중인 기기에 대한 푸시 서버로 작동될 수 있습니다. 예를 들어, KasperskyOS 기기를 중앙 관리 서버에 강제로 동기화하려면 푸시 서버를 활성화해야 합니다. 푸시 서버에는 푸시 서버가 활성화된 배포 지점과 동일한 수준의 관리 중인 기기가 있습니다. 동일한 관리 그룹에 여러 배포 지점이 할당된 경우 각 배포 지점에서 푸시 서버를 활성화할 수 있습니다. 이 경우 중앙 관리 서버는 배포 지점 간의 로드 균형을 조정합니다.

배포 지점을 푸시 서버로 사용하여 관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결을 유지할 수 있습니다. 로컬 작업 실행 및 중지, 관리 중인 애플리케이션에 대한 통계 수신 또는 터널 생성과 같은 일부 작업에는 지속적인 연결이 필요합니다. 배포 지점을 푸시 서버로 사용하는 경우 관리 중인 기기에서 **중앙 관리 서버와 계속 연결 유지** 옵션을 사용하거나 네트워크 에이전트의 UDP 포트로 패킷을 보냅니다.

푸시 서버는 최대 50,000개의 동시 연결 로드를 지원합니다.

배포 지점에서 푸시 서버를 활성화하려면 다음과 같이 하십시오.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **배포 지점** 섹션을 선택합니다.
3. 푸시 서버를 활성화할 배포 지점의 이름을 클릭합니다.
   그러면 배포 지점 속성 창이 열립니다.
4. **일반** 섹션에서 **푸시 서버 실행** 옵션을 활성화합니다.
5. **푸시 서버 포트** 필드에서 포트 번호를 입력합니다. 비어 있는 포트의 번호를 지정할 수 있습니다.
6. **원격 호스트용 주소** 필드에서 배포 지점 기기의 IP 주소 또는 이름을 지정합니다.
7. **확인** 버튼을 누릅니다.

선택한 배포 지점에서 푸시 서버가 활성화됩니다.

클라이언트 기기에서 타사 애플리케이션 관리

이 섹션에서는 클라이언트 기기에 설치된 타사 애플리케이션 관리와 관련된 Kaspersky Security Center에 관해 설명합니다.

타사 소프트웨어 업데이트 설치

Kaspersky Security Center를 사용하면 관리 중인 기기에 설치된 타사 소프트웨어의 업데이트를 관리하고 필요한 업데이트를 설치해 Microsoft 애플리케이션과 다른 공급업체 제품의 취약점을 수정할 수 있습니다.

Kaspersky Security Center는 *취약점 및 필요한 업데이트 검색* 작업을 통해 업데이트를 검색합니다. 이 작업이 완료되면 중앙 관리 서버는 작업 속성에서 지정한 기기에 설치된 타사 소프트웨어에 대하여 탐지된 취약점 및 필요한 업데이트의 목록을 받습니다. 사용 가능한 업데이트에 관한 정보를 확인한 후 기기에 설치합니다.

Kaspersky Security Center는 애플리케이션의 이전 버전을 제거하고 새 버전으로 설치해 일부 애플리케이션을 업데이트합니다.

관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

취약점 및 패치 관리 기능을 사용하여 타사 소프트웨어 업데이트 설치 시, 보안상의 이유로 Kaspersky 기술을 사용해 악성 코드를 자동 검사합니다. 이러한 기술은 자동 파일 검사에 사용되며, 샌드박스 환경에서의 바이러스 검사, 정적 분석, 동적 분석, 행동 분석, 머신 러닝 등을 포함합니다.

Kaspersky 전문가는 취약점 및 패치 관리 기능으로 설치할 수 있는 타사 소프트웨어 업데이트에 대한 수동 분석을 수행하지 않습니다. 또한 Kaspersky 전문가는 이러한 업데이트에서 알려지거나 알려지지 않은 취약점이나 문서화되지 않은 기능을 검색하지 않으며, 위 단락에 지정된 유형 외에 다른 유형의 업데이트 분석도 수행하지 않습니다.

타사 소프트웨어 업데이트 설치 관련 작업

타사 소프트웨어 업데이트의 메타데이터가 저장소에 다운로드되면 다음 작업을 통해 클라이언트 기기에 업데이트를 설치할 수 있습니다.

- *필수 업데이트 설치 및 취약점 수정* 작업

  필수 업데이트 설치 및 취약점 수정 작업은 Windows Update 서비스에서 제공하는 업데이트, 기타 공급업체 소프트웨어의 업데이트 등 Microsoft 애플리케이션 업데이트 설치에 사용됩니다. 이 작업은 취약점 및 패치 관리 기능에 대한 라이센스가 있을 때만 만들 수 있습니다.

  이 작업이 완료되면 업데이트가 관리 중인 기기에 자동으로 설치됩니다. 새 업데이트의 메타데이터가 중앙 관리 서버 저장소에 다운로드되면 Kaspersky Security Center에서는 이 업데이트가 업데이트 규칙에 지정된 기준을 충족하는지 검사합니다. 기준을 충족하는 모든 새 업데이트는 다음 작업 실행 시 자동으로 다운로드 및 설치됩니다.

- *Windows Update 업데이트 설치* 작업

  Windows Update 업데이트 설치 작업에는 라이센스가 필요하지 않지만 Windows Update 업데이트를 설치하는 데만 사용할 수 있습니다.

  이 작업이 완료되면 작업 속성에 지정된 업데이트만 설치됩니다. 나중에 중앙 관리 서버 저장소에 다운로드된 새 업데이트를 설치하려면 기존 작업의 업데이트 목록에 필수 업데이트를 추가하거나 Windows Update 업데이트 작업을 새로 만들어야 합니다.

WSUS 서버로 이 중앙 관리 서버 사용

이용 가능한 Microsoft Windows 업데이트에 대한 정보는 Windows Update 서비스에 의해 제공됩니다. 중앙 관리 서버를 WSUS(Windows Server Update Services) 서버로 사용할 수 있습니다. 중앙 관리 서버를 WSUS 서버로 사용하려면 Windows 업데이트 동기화 수행 작업을 만들고 네트워크 에이전트 정책에서 **중앙 관리 서버를 WSUS 서버로 사용** 옵션을 선택합니다. Windows 업데이트로 데이터 동기화를 구성하면 중앙 관리 서버가 설정된 빈도에 따라 기기의 Windows 업데이트 서비스에 중앙 집중식 모드로 업데이트를 제공합니다.

시나리오: 타사 소프트웨어 업데이트

이 섹션에서는 클라이언트 기기에 설치된 타사 소프트웨어의 업데이트 관련 시나리오를 제공합니다. 타사 소프트웨어에는 Microsoft 및 기타 소프트웨어 공급업체의 애플리케이션이 포함됩니다. Microsoft 애플리케이션 업데이트는 Windows Update 서비스에서 제공합니다.

필수 구성 요소

Microsoft 소프트웨어 이외의 타사 소프트웨어 업데이트를 설치하려면 중앙 관리 서버가 인터넷에 연결되어 있어야 합니다.

기본적으로 중앙 관리 서버에서 Microsoft 소프트웨어 업데이트를 관리 중인 기기에 설치하는 경우 인터넷 연결이 필요하지 않습니다. 예를 들어 관리 중인 기기는 Microsoft Update 서버 또는 회사의 네트워크에 배포된 Microsoft WSUS(Windows Server Update Services)가 있는 Windows Server에서 직접 Microsoft 소프트웨어 업데이트를 다운로드할 수 있습니다. 중앙 관리 서버를 WSUS 서버로 사용하려면 중앙 관리 서버가 인터넷에 연결되어 있어야 합니다.

단계

타사 소프트웨어 업데이트는 다음과 같이 단계적으로 진행됩니다.

1 필요한 업데이트 검색

관리 중인 기기에 필요한 타사 소프트웨어 업데이트를 찾으려면 *취약점 및 필요한 업데이트 검색* 작업을 실행합니다. 이 작업이 완료되면 Kaspersky Security Center는 작업 속성에서 지정한 기기에 설치된 타사 소프트웨어에 대하여 탐지된 취약점 및 필요한 업데이트의 목록을 받습니다.

취약점 및 필요한 업데이트 검색 작업은 중앙 관리 서버 빠른 시작 마법사가 자동 생성합니다. 마법사를 실행하지 않았다면 지금 작업을 생성하거나 빠른 시작 마법사를 실행합니다.

방법 지침:

- 관리 콘솔: 애플리케이션 취약점 검사, 취약점 및 필요한 업데이트 검색 작업 스케줄 지정
- Kaspersky Security Center 웹 콘솔: 취약점 및 필요한 업데이트 검색 작업 만들기, 취약점 및 필요한 업데이트 검색 작업 설정

2 발견된 업데이트 목록 분석

소프트웨어 업데이트 목록을 확인하고 설치할 업데이트를 결정합니다. 각 업데이트에 대한 상세 정보를 확인하려면 목록에서 업데이트 이름을 누릅니다. 목록에 있는 각 업데이트에 대해 클라이언트 기기에서 업데이트 설치 관련 통계를 확인할 수도 있습니다.

방법 지침:

- 관리 콘솔: 사용 가능한 업데이트 관련 정보 보기
- Kaspersky Security Center 웹 콘솔: 사용 가능한 타사 소프트웨어 업데이트 관련 정보 보기

3 업데이트 설치 구성

Kaspersky Security Center에서 타사 소프트웨어 업데이트 목록을 받으면 *필수 업데이트 설치 및 취약점 수정* 작업 또는 *Windows Update 업데이트 설치* 작업을 사용하여 클라이언트 기기에 업데이트를 설치할 수 있습니다. 이러한 작업 중 하나를 만듭니다. **작업** 탭 또는 **소프트웨어 업데이트** 목록을 사용하여 이러한 작업을 만들 수 있습니다.

필수 업데이트 설치 및 취약점 수정 작업은 Windows Update 서비스에서 제공하는 업데이트, 기타 공급업체 소프트웨어의 업데이트 등 Microsoft 애플리케이션 업데이트 설치에 사용됩니다. 이 작업은 취약점 및 패치 관리 기능에 대한 라이센스가 있을 때만 만들 수 있습니다.

Windows Update 업데이트 설치 작업에는 라이센스가 필요하지 않지만 Windows Update 업데이트를 설치하는 데만 사용할 수 있습니다.

소프트웨어 설치에 관한 EULA(최종 사용자 라이센스 계약서)에 동의해야 설치할 수 있는 소프트웨어 업데이트도 있습니다. EULA에 동의하지 않으면 소프트웨어 업데이트가 설치되지 않습니다.

스케줄에 따라 업데이트 설치 작업을 시작할 수 있습니다. 작업 스케줄을 지정할 때 업데이트 설치 작업은 *취약점 및 필요한 업데이트 검색* 작업이 완료된 후에 시작해야 합니다.

방법 지침:

- 관리 콘솔: 애플리케이션의 취약점 수정, 사용 가능한 업데이트 관련 정보 보기
- Kaspersky Security Center 웹 콘솔: 필수 업데이트 설치 및 취약점 수정 작업 생성, Windows Update 업데이트 설치 작업 생성, 사용 가능한 타사 소프트웨어 업데이트 관련 정보 보기

4 작업 스케줄 지정

업데이트 목록을 항상 최신 상태로 유지하기 위해 *취약점 및 필요한 업데이트 검색* 작업 스케줄을 지정하여 가끔 자동으로 실행합니다. 기본적으로 *취약점 및 필요한 업데이트 검색* 작업은 수동 시작으로 설정되어 있습니다.

사용자가 *필수 업데이트 설치 및 취약점 수정* 작업을 만든 경우 *취약점 및 필요한 업데이트 검색* 작업과 빈도가 같거나 적게 실행하도록 스케줄을 지정할 수 있습니다. *Windows Update 업데이트 설치* 작업의 스케줄을 지정할 때 이러한 작업의 경우 작업을 시작하기 전에 매번 업데이트 목록을 정해야 합니다.

작업 스케줄을 지정할 때는 *취약점 및 필요한 업데이트 검색* 작업이 완료된 후에 업데이트 설치 작업을 시작해야 합니다.

5 소프트웨어 업데이트 승인 및 거부(선택 사항)

필수 업데이트 설치 및 취약점 수정 작업을 만들었다면 작업 속성에서 업데이트 설치 관련 규칙을 지정할 수 있습니다. Windows Update 업데이트 설치 작업을 만들었다면 이 단계는 건너뛰십시오.

업데이트 상태가 *정의 안 됨*, *승인됨* 또는 *거부됨*인지에 따라 각 규칙에 대해 설치할 업데이트를 정의할 수 있습니다. 예를 들어, Windows Update 업데이트 설치만을 *승인됨* 상태인 사용자에게만 허용하려면 서버에 대한 특정 작업을 만들고 이 작업의 규칙을 설정하는 것이 좋습니다. 그런 다음 설치하고자 하는 업데이트에 대해 *승인됨* 상태를 수동으로 설정합니다. 이 경우 *정의 안 됨* 또는 *거부됨* 상태인 Windows Update 업데이트는 작업에서 지정한 서버에 설치되지 않습니다.

승인됨 상태를 사용하여 업데이트 설치를 관리하면 소량 업데이트에 효율적입니다. 여러 업데이트를 설치하려면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 구성할 수 있는 규칙을 사용하십시오. 규칙에 명시된 기준을 충족하지 않는 업데이트에 대해서만 *승인됨* 상태를 설정하는 것이 좋습니다. 대량의 업데이트를 수동으로 승인하면 중앙 관리 서버의 성능이 저하되어 결국 서버 과부하로 이어질 수 있습니다.

기본적으로 다운로드한 소프트웨어 업데이트는 *정의 안 됨* 상태입니다. **소프트웨어 업데이트** 목록(**동작 → 패치 관리 → 소프트웨어 업데이트**)에서 상태를 *승인됨* 또는 *거부됨*으로 변경할 수 있습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 업데이트 승인 및 거부
- Kaspersky Security Center 웹 콘솔: 타사 소프트웨어 업데이트 승인 및 거부

6 WSUS(Windows Server Update Services) 서버로 작동하도록 중앙 관리 서버 구성(선택 사항)

기본적으로 Windows Update 업데이트는 Microsoft 서버에서 관리 중인 기기로 다운로드됩니다. 중앙 관리 서버를 WSUS 서버로 사용하도록 이 설정을 변경할 수 있습니다. 이 경우, 중앙 관리 서버는 지정된 빈도로 Windows 업데이트와 업데이트 데이터를 동기화하고 중앙 집중식 모드로 클라이언트 기기에 Windows Update에 대한 업데이트를 제공합니다.

중앙 관리 서버를 WSUS 서버로 사용하려면 Windows 업데이트 동기화 수행 작업을 만들고 네트워크 에이전트 정책에서 **중앙 관리 서버를 WSUS 서버로 사용** 확인란을 선택합니다.

방법 지침:

- 관리 콘솔: 중앙 관리 서버와 Windows Update의 업데이트 동기화, 네트워크 에이전트 정책에서 Windows 업데이트 구성
- Kaspersky Security Center 웹 콘솔: Windows Update 동기화 수행 작업 생성

7. **업데이트 설치 작업 실행**

   필수 업데이트 설치 및 취약점 수정 작업 또는 *Windows Update 업데이트 설치* 작업을 시작합니다. 이러한 작업을 시작하면 관리 중인 기기에 업데이트가 다운로드되고 설치됩니다. 작업이 완료되면 작업 목록에서 상태가 *성공적으로 완료*인지 확인하십시오.

8. **타사 소프트웨어의 업데이트 설치 결과 관련 보고서 생성(선택 사항)**

   업데이트 설치에 관한 자세한 통계를 보려면 **타사 소프트웨어 업데이트 설치 결과 리포트**를 만듭니다.

   방법 지침:

   - 관리 콘솔: 리포트 만들기 및 보기
   - Kaspersky Security Center 웹 콘솔: 리포트 생성 및 보기

결과

필수 업데이트 설치 및 취약점 수정 작업을 만들고 구성했다면 업데이트가 관리 중인 기기에 자동으로 설치됩니다. 새 업데이트가 중앙 관리 서버 저장소에 다운로드되면 Kaspersky Security Center에서는 업데이트 규칙에 지정된 기준을 충족하는지 검사합니다. 기준을 충족하는 모든 새 업데이트는 다음 작업 실행 시 자동으로 설치됩니다.

Windows Update 업데이트 작업을 만들었다면 *Windows Update 업데이트* 작업 속성에 지정된 업데이트만 설치됩니다. 나중에 중앙 관리 서버 저장소에 다운로드된 새 업데이트를 설치하려면 기존 작업의 업데이트 목록에 필수 업데이트를 추가하거나 *Windows Update 업데이트* 작업을 새로 만들어야 합니다.

타사 소프트웨어 업데이트 설치

다음 작업 중 하나를 만들고 실행하여 관리 중인 기기에 타사 소프트웨어 업데이트를 설치할 수 있습니다.

- *취약점 관련 업데이트를 설치하고 취약점 수정*

  *취약점 관련 업데이트를 설치하고 취약점 수정*은 취약점 및 패치 관리 기능에 대한 라이센스가 있을 때만 만들 수 있습니다. 이 작업으로 Microsoft에서 제공하는 Windows Update 업데이트와 다른 공급업체 제품의 업데이트를 모두 설치할 수 있습니다.

- *Windows 업데이트 패치 설치*

  Windows 업데이트 패치 설치 작업을 사용하면 Windows Update 업데이트만 설치할 수 있습니다.

> 관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

옵션으로 다음과 같은 방법을 통해 필수 업데이트를 설치하는 작업을 생성할 수 있습니다.

- 업데이트 목록을 열고 설치할 업데이트를 지정합니다.

  그러면 선택한 업데이트를 설치하는 새 작업이 생성됩니다. 옵션으로 선택한 업데이트를 기존 작업에 추가할 수 있습니다.

- 업데이트 설치 마법사를 실행합니다.

> 업데이트 설치 마법사는 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

마법사는 업데이트 설치 작업의 생성 및 구성을 단순화하여, 같은 업데이트 설치를 위한 중복 작업을 생성하지 않도록 합니다.

업데이트 목록을 사용하여 타사 소프트웨어 업데이트 설치

업데이트 목록을 사용하여 타사 소프트웨어 업데이트를 설치하려면 다음 단계를 따릅니다.

1. 업데이트 목록 중 하나를 엽니다.

   - 일반 업데이트 목록을 열려면 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 업데이트**로 이동합니다.
   - 관리 중인 기기의 업데이트 목록을 열려면 메인 메뉴에서 **에셋(기기) → 관리 중인 기기 →** <기기 이름> **→ 고급 → 사용 가능한 업데이트**로 이동합니다.
   - 특정 애플리케이션에 대한 업데이트 목록을 열려면 메인 메뉴에서 **동작 → 타사 애플리케이션 → 자산 관리(소프트웨어) →** <애플리케이션 이름> **→ 사용 가능한 업데이트**로 이동합니다.

   사용 가능한 업데이트 목록이 나타납니다.

2. 설치하려는 업데이트 옆에 있는 확인란을 선택합니다.

3. **업데이트 설치** 버튼을 누릅니다.

   EULA(최종 사용자 라이센스 계약서)에 동의해야 설치할 수 있는 소프트웨어 업데이트도 있습니다. EULA에 동의하지 않으면 소프트웨어 업데이트가 설치되지 않습니다.

4. 다음 옵션 중 하나를 선택합니다:

   - **새 작업**

     새 작업 마법사가 시작됩니다. 취약점 및 패치 관리 라이센스가 있다면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 미리 선택되어 있습니다. 라이센스가 없는 경우 *Windows 업데이트 패치 설치* 작업을 선택합니다. 마법사의 단계에 따라 작업 생성을 완료합니다.

   - **업데이트 설치(특정 작업에 규칙 추가)**

     선택한 업데이트를 추가할 작업을 선택합니다. 취약점 및 패치 관리 라이센스가 있다면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 선택합니다. 선택한 업데이트를 설치하는 새로운 규칙이 선택한 작업에 자동으로 추가됩니다. 라이센스가 없다면 *Windows 업데이트 패치 설치* 작업을 선택합니다. 선택한 업데이트가 작업 속성에 추가됩니다.

     작업 속성 창이 열립니다. **저장** 버튼을 눌러 변경 사항을 적용합니다.

   새 작업을 만들기로 선택한 경우 작업은 **에셋(기기) → 작업**에 있는 작업 목록에서 생성되고 표시됩니다. 기존 작업에 업데이트를 추가하기로 선택한 경우 업데이트는 작업 속성에 저장됩니다.

타사 소프트웨어 업데이트를 설치하려면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업 또는 *Windows 업데이트 패치 설치* 작업을 시작합니다. 이러한 작업은 수동으로 또는 시작하는 작업의 속성에서 스케줄 설정을 지정하여 시작할 수 있습니다. 작업 스케줄을 지정할 때 업데이트 설치 작업은 *취약점 및 필요한 업데이트 검색* 작업이 완료된 후에 시작해야 합니다.

업데이트 설치 마법사를 사용하여 타사 소프트웨어 업데이트 설치

업데이트 설치 마법사는 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

업데이트 설치 마법사를 사용하여 타사 소프트웨어 업데이트 설치 작업을 생성하려면:

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 업데이트**로 이동합니다.
   사용 가능한 업데이트 목록이 나타납니다.

2. 설치하려는 업데이트 옆에 있는 확인란을 선택합니다.

3. **업데이트 설치 마법사 실행** 버튼을 누릅니다.
   업데이트 설치 마법사가 시작됩니다. **업데이트 설치 작업 선택** 페이지에 다음 유형의 모든 기존 작업 목록이 표시됩니다.

   - *취약점 관련 업데이트를 설치하고 취약점 수정*
   - *Windows 업데이트 패치 설치*
   - *취약점 해결*

   새 업데이트를 설치하려면 마지막 두 가지 유형의 작업을 수정해서는 안 됩니다. 새 업데이트를 설치하기 위해 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업만 사용할 수 있습니다.

4. 마법사에서 선택한 업데이트 설치 작업만 표시하도록 하려면 **이 업데이트를 설치하는 작업만 표시** 옵션을 활성화합니다.

5. 다음 중 원하는 작업을 선택합니다.

   - 작업을 시작하려면 작업 이름 옆에 있는 확인란을 선택한 다음 **시작** 버튼을 누릅니다.
   - 기존 작업에 새 규칙을 추가하려면 다음 단계를 따릅니다.

     a. 작업 이름 옆에 있는 확인란을 선택한 다음 **규칙 추가** 버튼을 누릅니다.

     b. 페이지가 열리면 새 규칙을 구성합니다.

     - **중요도에 따른 업데이트 설치 규칙**

       소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

       이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 선택한 업데이트의 심각도(**중간**, **높음**, **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

       이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

       기본적으로 이 옵션은 비활성화되어 있습니다.

     - **MSRC에 따른 이 중요도의 업데이트 설치 규칙**

       소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

       이 옵션을 활성화하면(Windows Update 업데이트만 해당) 업데이트는 MSRC(Microsoft Security Response Center)에서 설정한 심각도가 목록에서 선택한 값(**낮음**, **중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **이 공급 업체에 따른 업데이트 설치 규칙**

  이 옵션은 타사 애플리케이션 업데이트에만 사용할 수 있습니다. Kaspersky Security Center는 동일한 공급업체에서 만든 애플리케이션과 관련된 업데이트만 선택된 업데이트로 설치합니다. 다른 공급업체에서 만든 애플리케이션에 대한 업데이트 및 거부된 업데이트는 설치되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **유형에 해당하는 업데이트 설치 규칙**
- **선택한 업데이트에 해당하는 설치 규칙**
- **선택한 업데이트 승인**

  선택한 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **선택된 업데이트를 설치하는 데 필요한 이전의 모든 애플리케이션 업데이트 자동 설치**

  선택한 업데이트를 설치하는 데 필요한 경우 중간 애플리케이션 버전 설치에 동의한다면 이 옵션을 활성화한 상태로 유지하십시오.

  이 옵션을 비활성화하면 애플리케이션의 선택한 버전만 설치됩니다. 후속 버전의 증분 방식 설치를 시도하지 않고 단순하게 애플리케이션을 업데이트하려면 이 옵션을 비활성화합니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

  기기에 설치되어 있는 애플리케이션 버전 3을 버전 5로 업데이트하려고 하는데 이 애플리케이션의 버전 5는 버전 4가 설치되어 있어야 설치 가능한 경우를 예로 들어 보겠습니다. 이 옵션을 활성화하면 소프트웨어는 먼저 버전 4를 선택한 후에 버전 5를 선택합니다. 이 옵션을 비활성화하면 소프트웨어가 애플리케이션을 업데이트하지 못합니다.

  기본적으로 이 옵션은 켜져 있습니다.

c. **추가** 버튼을 누릅니다.

- 작업을 만들려면 다음 단계를 따릅니다.

  a. **새 작업** 버튼을 누릅니다.

  b. 페이지가 열리면 새 규칙을 구성합니다.

  - **중요도에 따른 업데이트 설치 규칙**

    소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 선택한 업데이트의 심각도(**중간**, **높음**, **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **MSRC에 따른 이 중요도의 업데이트 설치 규칙**

  소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

  이 옵션을 활성화하면(Windows Update 업데이트만 해당) 업데이트는 MSRC(Microsoft Security Response Center)에서 설정한 심각도가 목록에서 선택한 값(**낮음**, **중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

  이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **이 공급 업체에 따른 업데이트 설치 규칙**

  이 옵션은 타사 애플리케이션 업데이트에만 사용할 수 있습니다. Kaspersky Security Center는 동일한 공급업체에서 만든 애플리케이션과 관련된 업데이트만 선택된 업데이트로 설치합니다. 다른 공급업체에서 만든 애플리케이션에 대한 업데이트 및 거부된 업데이트는 설치되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **유형에 해당하는 업데이트 설치 규칙**
- **선택한 업데이트에 해당하는 설치 규칙**
- **선택한 업데이트 승인**

  선택한 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **선택된 업데이트를 설치하는 데 필요한 이전의 모든 애플리케이션 업데이트 자동 설치**

  선택한 업데이트를 설치하는 데 필요한 경우 중간 애플리케이션 버전 설치에 동의한다면 이 옵션을 활성화한 상태로 유지하십시오.

  이 옵션을 비활성화하면 애플리케이션의 선택한 버전만 설치됩니다. 후속 버전의 증분 방식 설치를 시도하지 않고 단순하게 애플리케이션을 업데이트하려면 이 옵션을 비활성화합니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

  기기에 설치되어 있는 애플리케이션 버전 3을 버전 5로 업데이트하려고 하는데 이 애플리케이션의 버전 5는 버전 4가 설치되어 있어야 설치 가능한 경우를 예로 들어 보겠습니다. 이 옵션을 활성화하면 소프트웨어는 먼저 버전 4를 선택한 후에 버전 5를 선택합니다. 이 옵션을 비활성화하면 소프트웨어가 애플리케이션을 업데이트하지 못합니다.

  기본적으로 이 옵션은 켜져 있습니다.

c. **추가** 버튼을 누릅니다.

작업 시작을 선택했다면 마법사를 닫아도 됩니다. 작업은 백그라운드 모드에서 완료됩니다. 추가 조치는 필요하지 않습니다.

기존 작업에 규칙을 추가하기로 선택했다면 작업 속성 창이 열립니다. 새 규칙이 이미 작업 속성에 추가되었습니다. 규칙 또는 기타 작업 설정을 확인하거나 수정할 수 있습니다. **저장** 버튼을 눌러 변경 사항을 적용합니다.

작업 생성을 선택했다면 새 작업 마법사에서 작업 생성을 계속 진행합니다. 업데이트 설치 마법사에 추가한 새로운 규칙이 새 작업 마법사에 표시됩니다. 마법사를 완료하면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 작업 목록에 추가됩니다.

취약점 및 필요한 업데이트 검색 작업 만들기

취약점 및 필요한 업데이트 검색 작업을 통해 Kaspersky Security Center는 관리 중인 기기에 설치된 타사 소프트웨어에 대해 감지된 취약점 및 필수 업데이트 목록을 받습니다.

빠른 시작 마법사가 실행 중이면 취약점 및 필요한 업데이트 검색 작업이 자동 생성됩니다. 마법사를 실행하지 않았다면 수동으로 작업을 만들 수 있습니다.

취약점 및 필요한 업데이트 검색 작업 만들기:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. Kaspersky Security Center 애플리케이션의 경우 **취약점 및 필요한 업데이트 검색** 작업 유형을 선택합니다.
4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
5. 이 작업이 할당되는 기기를 선택합니다.
6. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.
7. **생성** 버튼을 누릅니다.
   그러면 작업이 생성되고 작업 목록에 표시됩니다.
8. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.
9. 작업 속성 창에서 일반 작업 설정을 지정합니다.
10. **애플리케이션 설정** 탭에서 다음 설정을 지정합니다.

- **Microsoft에서 작성한 취약점 및 업데이트 검색**

  취약점 및 업데이트를 검색할 때 Kaspersky Security Center는 현재 사용 가능한 Microsoft 업데이트 소스의 해당 Microsoft 업데이트에 대한 정보를 사용합니다.

예를 들어 Microsoft 업데이트 및 타사 애플리케이션 업데이트에 대해 다양한 설정을 사용하는 다양한 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

기본적으로 이 옵션은 켜져 있습니다.

선택 사항인 Microsoft Windows 업데이트에 대한 정보는 중앙 관리 서버로 전송되지 않습니다.

- **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트**

  관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결됩니다. 다음 서버는 Microsoft 업데이트의 소스로 작동할 수 있습니다.

  - Kaspersky Security Center 중앙 관리 서버(네트워크 에이전트 정책 설정 참조)
  - 조직의 네트워크에 Microsoft WSUS(Windows 서버 업데이트 서비스)가 배포된 Windows Server
  - Microsoft 업데이트 서버

  이 옵션을 활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결하여 해당하는 Microsoft Windows 업데이트 관련 정보를 새로 고칩니다.

  이 옵션을 비활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 이전에 Microsoft 업데이트 소스에서 받은 해당 Microsoft Windows 업데이트에 관한 정보를 사용합니다.

  Microsoft 업데이트 소스에 연결할 때는 리소스가 많이 사용될 수 있습니다. **소프트웨어 업데이트 및 취약점** 섹션에 있는 네트워크 에이전트 정책의 속성이나 다른 작업에서 이 업데이트 소스에 대한 정기 연결을 설정하는 경우 이 옵션을 비활성화할 수 있습니다. 이 옵션을 비활성화하고 싶지 않으면, 서버 과부하를 줄이기 위해 360분 내에 작업 시작 시간을 랜덤하게 지정하도록 작업 스케줄을 구성할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  다음 옵션 조합의 조합으로 네트워크 에이전트 정책 설정 업데이트를 받는 옵션을 정의합니다.

  - 관리 중인 기기의 Windows 업데이트 에이전트는 *취약점 및 필요한 업데이트 검색* 작업의 속성에서 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화하고 네트워크 에이전트 정책 설정에서 **Windows 업데이트 검색 모드** 옵션을 **액티브**으로 설정했을 때만 업데이트 서버에 연결하여 업데이트를 가져옵니다.
  - *취약점 검사* 작업을 수행할 때 네트워크 에이전트가 Microsoft Windows 업데이트 경로에 대한 연결 시작과 업데이트 다운로드가 필요하지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하는 동시에 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화된 상태로 유지해야 합니다. 이를 통해 리소스를 절약하고 이전에 받은 Windows 업데이트를 사용하여 취약점을 검사할 수 있습니다. 다른 방법으로 Microsoft Windows 업데이트 수신을 구성하는 경우 수동 모드를 사용할 수 있습니다. Microsoft Windows 업데이트 수신이 다른 방법으로 구성되지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하지 마십시오. 이 경우 업데이트 정보가 수신되지 않습니다.
  - **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션의 상태(활성화 또는 비활성화)에 무관하게 **Windows 업데이트 검색 모드** 옵션이 **비활성화됨**로 설정되면 Kaspersky Security Center는 업데이트 정보를 요청하지 않습니다.

- **Kaspersky에서 작성한 타사 취약점 및 업데이트 검색**

  이 옵션을 활성화하면 Kaspersky Security Center는 **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정** 아래에 지정된 폴더와 Windows 레지스트리에서 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)에 필요한 업데이트와 취약점을 검색합니다. 지원되는 타사 애플리케이션의 전체 목록은 Kaspersky에서 관리합니다.

  이 옵션을 비활성화하면 Kaspersky Security Center는 타사 애플리케이션에 필요한 업데이트와 취약점을 검색하지 않습니다. 예를 들어 Microsoft Windows 업데이트 및 타사 애플리케이션 업데이트에 대해 다른 설정을 사용하는 다른 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정**

  Kaspersky Security Center가 취약점을 수정하고 업데이트를 설치해야 하는 타사 애플리케이션을 검색하는 폴더입니다. 시스템 변수를 사용할 수 있습니다.

  애플리케이션이 설치된 폴더를 지정합니다. 목록에는 기본적으로 대다수 애플리케이션이 설치된 시스템 폴더가 포함됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

  작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **고급 진단 파일의 최대 크기(MB)**

  기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

11. **저장** 버튼을 누릅니다.

    작업이 생성 및 구성됩니다.

작업 결과에 0x80240033 경고 'Windows 업데이트 에이전트 오류 80240033("라이센스 약관을 다운로드할 수 없습니다.")' 오류가 포함되어 있는 경우 Windows 레지스트리를 통해 이 문제를 해결할 수 있습니다.

취약점 및 필요한 업데이트 검색 작업 설정

빠른 시작 마법사가 실행 중이면 *취약점 및 필요한 업데이트 검색* 작업이 자동 생성됩니다. 마법사를 실행하지 않았다면 수동으로 작업을 만들 수 있습니다.

일반 작업 설정 외에도 *취약점 및 필요한 업데이트 검색* 작업 생성 시 이후 또는 만든 작업의 속성을 구성할 때 다음 설정을 지정할 수 있습니다.

- **Microsoft에서 작성한 취약점 및 업데이트 검색**

  취약점 및 업데이트를 검색할 때 Kaspersky Security Center는 현재 사용 가능한 Microsoft 업데이트 소스의 해당 Microsoft 업데이트에 대한 정보를 사용합니다.

  예를 들어 Microsoft 업데이트 및 타사 애플리케이션 업데이트에 대해 다양한 설정을 사용하는 다양한 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  선택 사항인 Microsoft Windows 업데이트에 대한 정보는 중앙 관리 서버로 전송되지 않습니다.

- **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트**

  관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결됩니다. 다음 서버는 Microsoft 업데이트의 소스로 작동할 수 있습니다.

  - Kaspersky Security Center 중앙 관리 서버(네트워크 에이전트 정책 설정 참조)
  - 조직의 네트워크에 Microsoft WSUS(Windows 서버 업데이트 서비스)가 배포된 Windows Server
  - Microsoft 업데이트 서버

  이 옵션을 활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 Microsoft 업데이트 소스에 연결하여 해당하는 Microsoft Windows 업데이트 관련 정보를 새로 고칩니다.

  이 옵션을 비활성화하면 관리 중인 기기의 Windows 업데이트 에이전트는 이전에 Microsoft 업데이트 소스에서 받은 해당 Microsoft Windows 업데이트에 관한 정보를 사용합니다.

  Microsoft 업데이트 소스에 연결할 때는 리소스가 많이 사용될 수 있습니다. **소프트웨어 업데이트 및 취약점** 섹션에 있는 네트워크 에이전트 정책의 속성이나 다른 작업에서 이 업데이트 소스에 대한 정기 연결을 설정하는 경우 이 옵션을 비활성화할 수 있습니다. 이 옵션을 비활성화하고 싶지 않으면, 서버 과부하를 줄이기 위해 360분 내에 작업 시작 시간을 랜덤하게 지정하도록 작업 스케줄을 구성할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

다음 옵션 조합의 조합으로 네트워크 에이전트 정책 설정 업데이트를 받는 옵션을 정의합니다.

- 관리 중인 기기의 Windows 업데이트 에이전트는 *취약점 및 필요한 업데이트 검색* 작업의 속성에서 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화하고 네트워크 에이전트 정책 설정에서 **Windows 업데이트 검색 모드** 옵션을 **액티브**으로 설정했을 때만 업데이트 서버에 연결하여 업데이트를 가져옵니다.

- *취약점 검사* 작업을 수행할 때 네트워크 에이전트가 Microsoft Windows 업데이트 경로에 대한 연결 시작과 업데이트 다운로드가 필요하지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하는 동시에 **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션을 활성화된 상태로 유지해야 합니다. 이를 통해 리소스를 절약하고 이전에 받은 Windows 업데이트를 사용하여 취약점을 검사할 수 있습니다. 다른 방법으로 Microsoft Windows 업데이트 수신을 구성하는 경우 수동 모드를 사용할 수 있습니다. Microsoft Windows 업데이트 수신이 다른 방법으로 구성되지 않은 경우 **Windows 업데이트 검색 모드** 옵션을 **패시브**으로 설정하지 마십시오. 이 경우 업데이트 정보가 수신되지 않습니다.

- **작업 전 WSUS 업데이트 서버에 연결해 로컬 데이터를 최신으로 업데이트** 옵션의 상태(활성화 또는 비활성화)에 무관하게 **Windows 업데이트 검색 모드** 옵션이 **비활성화됨**로 설정되면 Kaspersky Security Center는 업데이트 정보를 요청하지 않습니다.

- **Kaspersky에서 작성한 타사 취약점 및 업데이트 검색**

  이 옵션을 활성화하면 Kaspersky Security Center는 **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정** 아래에 지정된 폴더와 Windows 레지스트리에서 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)에 필요한 업데이트와 취약점을 검색합니다. 지원되는 타사 애플리케이션의 전체 목록은 Kaspersky에서 관리합니다.

  이 옵션을 비활성화하면 Kaspersky Security Center는 타사 애플리케이션에 필요한 업데이트와 취약점을 검색하지 않습니다. 예를 들어 Microsoft Windows 업데이트 및 타사 애플리케이션 업데이트에 대해 다른 설정을 사용하는 다른 작업이 있는 경우 이 옵션을 비활성화할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **파일 시스템에 있는 애플리케이션의 고급 검색 경로 지정**

  Kaspersky Security Center가 취약점을 수정하고 업데이트를 설치해야 하는 타사 애플리케이션을 검색하는 폴더입니다. 시스템 변수를 사용할 수 있습니다.

  애플리케이션이 설치된 폴더를 지정합니다. 목록에는 기본적으로 대다수 애플리케이션이 설치된 시스템 폴더가 포함됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

  작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **고급 진단 파일의 최대 크기(MB)**

  기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

작업 스케줄에 대한 권장 사항

취약점 및 필요한 업데이트 검색 작업 일정 예약 시 **누락된 작업 실행** 및 **자동으로 작업 시작 임의 지연 사용**의 두 가지 옵션이 활성화되어 있는지 확인합니다.

기본적으로 *취약점 및 필요한 업데이트 검색* 작업은 수동 시작으로 설정되어 있습니다. 이 시간에 모든 기기를 종료하는 조직의 회사 규칙이 제공되는 경우에는 다음 날 아침에 기기가 다시 켜진 이후 *취약점 및 필요한 업데이트 검색* 작업이 실행됩니다. 취약점 검사가 수행되면 CPU와 디스크 하위 시스템의 부하가 증가할 수 있으므로, 이러한 방식의 활동은 바람직하지 않을 수도 있습니다. 조직에서 채택한 회사 규칙에 따라 이 작업에 가장 편리한 스케줄을 설정해야 합니다.

필수 업데이트 설치 및 취약점 수정 작업 만들기

취약점 관련 업데이트를 설치하고 취약점 수정 작업은 취약점 및 패치 관리 라이선스가 있어야만 사용 가능합니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 사용하여 관리 중인 기기에 설치된 Microsoft 소프트웨어를 포함한 타사 소프트웨어의 취약점에 대한 업데이트 및 수정을 수행합니다. 이 작업을 통해 여러 업데이트를 설치하고 특정 규칙에 따라 여러 취약점을 수정할 수 있습니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 사용하여 업데이트를 설치하거나 취약점을 수정하려면 다음 작업을 수행하면 됩니다.

- 설치 업데이트 마법사 또는 취약점 수정 마법사를 실행합니다.
- *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 만듭니다.
- 기존 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업에 업데이트 설치에 대한 규칙을 추가합니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업 만들기:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. Kaspersky Security Center 애플리케이션의 경우 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업 유형을 선택합니다.

   작업이 표시되지 않으면 계정에 **시스템 관리**: **취약성 및 패치 관리** 기능 영역에 대한 **읽기**, **수정**, **실행** 권한이 있는지 확인하십시오. 이러한 액세스 권한이 없으면 *필요한 업데이트 설치 및 취약성 수정* 작업을 생성하고 구성할 수 없습니다.

4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

5. 이 작업이 할당되는 기기를 선택합니다.

6. 업데이트 설치 규칙을 지정하고 다음 설정을 지정합니다.

- **기기 다시 시작 또는 종료 시 설치 시작**

  이 옵션을 활성화하면 기기가 다시 시작되거나 종료되기 전에 업데이트가 설치됩니다. 그렇지 않으면 업데이트는 스케줄에 따라 설치됩니다.

  업데이트 설치가 기기 성능에 영향을 줄 수 있는 경우 이 옵션을 사용합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **필요한 일반 시스템 구성 요소 설치**

  이 옵션을 활성화하면 업데이트를 설치하기 전에 애플리케이션은 업데이트 설치를 설치하기 위해 필요한 모든 일반 시스템 구성 요소(선결 조건)를 자동으로 설치합니다. 이러한 필수 구성 요소의 예로는 운영 체제 업데이트 등이 있습니다.

  이 옵션을 비활성화하는 경우에는 필수 구성 요소를 수동으로 설치해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 시 새 애플리케이션 버전의 설치 허용**

  이 옵션을 활성화하면 업데이트 시 소프트웨어 애플리케이션의 새 버전이 설치되는 경우 업데이트가 허용됩니다.

  이 옵션을 비활성화하면 소프트웨어가 업그레이드되지 않습니다. 그러면 소프트웨어의 새 버전을 수동으로 또는 다른 작업을 통해 설치할 수 있습니다. 예를 들어 새 소프트웨어 버전이 회사 인프라를 지원하지 않거나 테스트 인프라에서 업그레이드를 확인하려는 경우 이 옵션을 사용할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  애플리케이션을 업그레이드하면 클라이언트 기기에 설치된 종속 애플리케이션의 오작동이 발생할 수 있습니다.

- **업데이트를 기기에 다운로드만 하고 설치는 하지 않음**

  이 옵션을 활성화하면 애플리케이션은 기기에 업데이트를 다운로드하지만 자동으로 해당 업데이트를 설치하지는 않습니다. 그러면 다운로드한 업데이트를 수동으로 설치할 수 있습니다.

  Microsoft 업데이트는 시스템 Windows 저장소에 다운로드됩니다. 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트는 **업데이트 다운로드 경로** 필드에 지정된 폴더에 다운로드됩니다.

  이 옵션을 비활성화하면 업데이트가 기기에 자동으로 설치됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 다운로드 경로**

  이 폴더는 타사 애플리케이션(Kaspersky이 아닌 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트를 다운로드하는 데 사용됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

  작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **고급 진단 파일의 최대 크기(MB)**

  기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

7. 운영 체제 다시 시작 설정을 지정합니다.

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **반복해서 물어보기(분)**

  이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

  이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

- **다음 시간 이후에 재시작(분)**

  사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 다음 시간 후 애플리케이션 강제 종료(분)**

  사용자 기기가 잠겨 있으면 애플리케이션은 지정된 비활성 기간이 지난 후 자동으로 또는 수동으로 강제 종료됩니다.

  이 옵션을 사용하면 입력 필드에 지정된 시간 간격 만료 시 애플리케이션이 잠긴 기기에서 강제 종료됩니다.

  이 옵션이 비활성화되어 있으면 애플리케이션이 잠긴 기기에서 종료되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

8. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

9. **마침** 버튼을 누릅니다.

   그러면 작업이 생성되고 작업 목록에 표시됩니다.

10. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

11. 작업 속성 창에서 필요에 따라 일반 작업 설정을 지정합니다.

12. **저장** 버튼을 누릅니다.

    작업이 생성 및 구성됩니다.

작업 결과에 0x80240033 경고 'Windows 업데이트 에이전트 오류 80240033("라이센스 약관을 다운로드할 수 없습니다.")' 오류가 포함되어 있는 경우 Windows 레지스트리를 통해 이 문제를 해결할 수 있습니다.

업데이트 설치에 대한 규칙 추가

이 기능은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업으로 소프트웨어 업데이트를 설치하거나 소프트웨어 취약점을 수정할 때는 업데이트 설치 규칙을 반드시 지정해야 합니다. 이러한 규칙에 따라 설치할 업데이트와 수정할 취약점이 결정됩니다.

정확한 설정은 모든 업데이트, Windows Update 업데이트 또는 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급업체에서 만든 애플리케이션) 업데이트 중 어디에 대한 규칙을 추가하는지에 따라 달라집니다. Windows Update 업데이트 또는 타사 애플리케이션 업데이트에 대한 규칙을 추가하는 경우 업데이트를 설치할 특정 애플리케이션 및 애플리케이션 버전을 선택할 수 있습니다. 모든 업데이트용 규칙을 추가할 때는 설치할 특정 업데이트 및 업데이트 설치를 통해 수정할 취약점을 선택할 수 있습니다.

다음과 같은 방법으로 업데이트 설치 규칙을 추가할 수 있습니다.

- 새 취약점 관련 업데이트를 설치하고 취약점 수정 작업을 만드는 동안 규칙을 추가합니다.
- 기존 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업의 속성 창에 있는 **애플리케이션 설정** 탭에서 규칙을 추가합니다.
- 업데이트 설치 마법사 또는 취약점 수정 마법사를 사용합니다.

모든 업데이트에 대한 새 규칙을 추가하려면 다음 단계를 따릅니다.

1. **추가** 버튼을 누릅니다.
   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
2. **규칙 유형** 페이지에서 **모든 업데이트에 대한 규칙**을 선택합니다.
3. **일반 기준** 페이지에서 드롭다운 목록을 사용하여 다음 설정을 지정합니다:
   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.
     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.
   - **다음 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

     이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.
4. **업데이트** 페이지에서 설치할 업데이트를 선택합니다:
   - **적합한 모든 업데이트 설치**

     마법사의 **일반 기준** 페이지에 지정된 기준을 충족하는 모든 소프트웨어 업데이트를 설치합니다. 기본적으로 선택됩니다.

- **다음 목록의 업데이트만 설치**

  목록에서 수동으로 선택하는 소프트웨어 업데이트만 설치합니다. 이 목록에는 사용 가능한 모든 소프트웨어 업데이트가 포함되어 있습니다.

  예를 들어 테스트 환경에서 설치를 확인하거나 중요한 애플리케이션 또는 특정 애플리케이션만 업데이트하려는 등의 경우 특정 업데이트를 선택할 수 있습니다.

  - **선택된 업데이트를 설치하는 데 필요한 이전의 모든 애플리케이션 업데이트 자동 설치**

    선택한 업데이트를 설치하는 데 필요한 경우 중간 애플리케이션 버전 설치에 동의한다면 이 옵션을 활성화한 상태로 유지하십시오.

    이 옵션을 비활성화하면 애플리케이션의 선택한 버전만 설치됩니다. 후속 버전의 증분 방식 설치를 시도하지 않고 단순하게 애플리케이션을 업데이트하려면 이 옵션을 비활성화합니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

    기기에 설치되어 있는 애플리케이션 버전 3을 버전 5로 업데이트하려고 하는데 이 애플리케이션의 버전 5는 버전 4가 설치되어 있어야 설치 가능한 경우를 예로 들어 보겠습니다. 이 옵션을 활성화하면 소프트웨어는 먼저 버전 4를 선택한 후에 버전 5를 선택합니다. 이 옵션을 비활성화하면 소프트웨어가 애플리케이션을 업데이트하지 못합니다.

    기본적으로 이 옵션은 켜져 있습니다.

5. **취약점** 페이지에서 선택한 업데이트를 설치하면 수정되는 취약점을 선택합니다:

   - **기타 기준과 일치하는 모든 취약점 수정**

     마법사의 **일반 기준** 페이지에 지정된 기준을 충족하는 모든 취약점을 수정합니다. 기본적으로 선택됩니다.

   - **다음 목록의 취약점만 수정**

     목록에서 수동으로 선택하는 취약점만 수정합니다. 이 목록에는 탐지된 모든 취약점이 포함되어 있습니다.

     예를 들어 테스트 환경에서 수정을 확인하거나 중요한 애플리케이션 또는 특정 애플리케이션의 취약점만 수정하려는 등의 경우 특정 취약점을 선택할 수 있습니다.

6. **이름** 페이지에서 추가할 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 **설정** 섹션에서 나중에 이 이름을 변경할 수 있습니다.

규칙 생성 마법사의 작업이 완료되면 새 작업 마법사의 규칙 목록 또는 작업 속성에 새 규칙이 추가되고 표시됩니다.

Windows Update 업데이트에 대한 새 규칙을 추가하려면 다음 단계를 따릅니다.

1. **추가** 버튼을 누릅니다.

   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

2. **규칙 유형** 페이지에서 **Windows 업데이트 규칙**을 선택합니다.

3. **일반 기준** 페이지에서 다음 설정을 지정합니다:

   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.

     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

   - **다음 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

     이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

   - **다음 MSRC 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 MSRC(Microsoft Security Response Center)에서 설정한 심각도가 목록에서 선택한 값(**낮음**, **중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

     이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

4. **애플리케이션** 페이지에서 업데이트를 설치할 애플리케이션 및 애플리케이션 버전을 선택합니다. 기본적으로 모든 애플리케이션이 선택되어 있습니다.

5. **업데이트 카테고리** 페이지에서 설치할 업데이트의 카테고리를 선택합니다. 이러한 카테고리는 Microsoft 업데이트 카탈로그의 카테고리와 동일합니다. 기본적으로 모든 카테고리가 선택되어 있습니다.

6. **이름** 페이지에서 추가할 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 **설정** 섹션에서 나중에 이 이름을 변경할 수 있습니다.

   규칙 생성 마법사의 작업이 완료되면 새 작업 마법사의 규칙 목록 또는 작업 속성에 새 규칙이 추가되고 표시됩니다.

타사 애플리케이션의 업데이트를 위한 새 규칙을 추가하려면 다음 단계를 따릅니다.

1. **추가** 버튼을 누릅니다.

   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

2. **규칙 유형** 페이지에서 **타사 업데이트 규칙**을 선택합니다.

3. **일반 기준** 페이지에서 다음 설정을 지정합니다:

   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.

     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

   - **다음 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

     이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

4. **애플리케이션** 페이지에서 업데이트를 설치할 애플리케이션 및 애플리케이션 버전을 선택합니다. 기본적으로 모든 애플리케이션이 선택되어 있습니다.

5. **이름** 페이지에서 추가할 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 설정 섹션에서 나중에 이 이름을 변경할 수 있습니다.

규칙 생성 마법사의 작업이 완료되면 새 작업 마법사의 규칙 목록 또는 작업 속성에 새 규칙이 추가되고 표시됩니다.

Windows Update 업데이트 설치 작업 만들기

Windows 업데이트 패치 설치 작업을 통해 Windows Update 서비스에서 제공하는 소프트웨어 업데이트를 관리 중인 기기에 설치할 수 있습니다.

취약점 및 패치 관리 라이센스가 없다면 *Windows 업데이트 패치 설치* 유형의 새 작업을 만들 수 없습니다. 기존의 *Windows 업데이트 패치 설치* 작업에 추가하면 새 업데이트를 설치할 수 있습니다. *Windows 업데이트 패치 설치* 작업 대신 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 사용하는 것이 좋습니다. *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 사용하면 정의한 규칙에 따라 여러 업데이트를 수정하고 여러 취약점을 수정할 수 있습니다. 또한 이 작업을 통해 Microsoft 이외의 소프트웨어 공급업체에서 제공하는 업데이트도 설치할 수 있습니다.

관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

Windows Update 업데이트 설치 작업을 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. Kaspersky Security Center 애플리케이션의 경우 **Windows 업데이트 패치 설치** 작업 유형을 선택합니다.
4. 만들고 있는 작업의 이름을 지정합니다.
   작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
5. 이 작업이 할당되는 기기를 선택합니다.
6. **추가** 버튼을 누릅니다.
   업데이트 목록이 열립니다.
7. 설치할 Windows Update 업데이트를 선택한 다음 **확인**을 누릅니다.
8. 운영 체제 다시 시작 설정을 지정합니다.

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **반복해서 물어보기(분)**

  이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

  이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

- **다음 시간 이후에 재시작(분)**

  사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

9. 다음 계정 설정을 지정합니다.

   - **기본 계정**

     해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.

     기본적으로 이 옵션은 선택되어 있습니다.

   - **계정 지정**

     계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

   - **계정**

     작업 실행에 사용되는 계정입니다.

   - **암호**

     작업을 실행할 계정의 암호입니다.

10. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

11. **마침** 버튼을 누릅니다.

    그러면 작업이 생성되고 작업 목록에 표시됩니다.

12. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

13. 작업 속성 창에서 필요에 따라 일반 작업 설정을 지정합니다.

14. **저장** 버튼을 누릅니다.

작업이 생성 및 구성됩니다.

사용 가능한 타사 소프트웨어 업데이트에 대한 정보 보기

클라이언트 기기에 설치된 Microsoft 소프트웨어를 비롯한 타사 소프트웨어에 사용 가능한 업데이트 목록을 볼 수 있습니다.

클라이언트 기기에 설치된 타사 애플리케이션에 이용 가능한 업데이트 목록을 보려면 다음 단계를 따릅니다.

메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 업데이트**로 이동합니다.

사용 가능한 업데이트 목록이 나타납니다.

필터를 지정하여 소프트웨어 업데이트 목록을 볼 수 있습니다. 필터를 관리하려면 소프트웨어 업데이트 목록의 우측 상단에서 **필터** 아이콘()을 누릅니다. 소프트웨어 취약점 목록 위의 **필터 사전 설정** 드롭다운 목록에서 사전 설정된 필터 중 하나를 선택해도 됩니다.

업데이트의 속성을 보려면 다음과 같이 하십시오:

1. 필요한 소프트웨어 업데이트의 이름을 누릅니다.

2. 해당 업데이트의 속성 창이 열리고 다음 탭에 그룹화된 정보가 표시됩니다.

- **일반**

  이 탭에는 선택한 업데이트의 일반 세부 정보가 표시됩니다.

  - 승인 상태 업데이트(드롭다운 목록에서 새 상태를 선택하여 수동으로 변경할 수 있음)
  - 업데이트가 속한 WSUS(Windows Server Update Services) 카테고리
  - 업데이트가 등록된 날짜와 시간
  - 업데이트가 생성된 날짜와 시간
  - 업데이트의 중요도
  - 업데이트에 따른 설치 요구 사항
  - 업데이트가 속한 애플리케이션 제품군
  - 업데이트가 적용되는 애플리케이션
  - 업데이트 리비전 번호

- **특성**

  이 탭에는 선택한 업데이트에 대한 자세한 정보를 얻는 데 사용할 수 있는 속성 세트가 표시됩니다. 이 세트는 업데이트를 Microsoft에서 게시했는지 아니면 타사 공급업체에서 게시했는지에 따라 다릅니다.

이 탭에는 Microsoft 업데이트에 대한 다음 정보가 표시됩니다.

- MSRC(Microsoft Security Response Center)에 따른 업데이트의 심각도
- 업데이트를 설명하는 Microsoft 기술 자료 문서의 링크
- 업데이트를 설명하는 Microsoft 보안 게시판 문서의 링크
- 업데이트 식별자(ID)

이 탭에는 타사 업데이트에 대한 다음 정보가 표시됩니다.

- 업데이트가 패치인지 전체 배포 패키지인지 여부
- 업데이트의 현지화 언어
- 업데이트가 자동 또는 수동으로 설치되는지 여부
- 업데이트 적용 후 취소 여부
- 업데이트 다운로드 링크

- **기기**

  이 탭에는 선택한 업데이트가 설치된 기기 목록이 표시됩니다.

- **수정된 취약점**

  이 탭에는 선택한 업데이트로 수정할 수 있는 취약점 목록이 표시됩니다.

- **업데이트 크로스오버**

  이 탭은 동일한 애플리케이션에 대해 게시된 다양한 업데이트 간의 가능한 교차를 표시합니다. 즉, 선택한 업데이트가 다른 업데이트를 대체할 수 있는지 또는 그 반대의 경우 다른 업데이트로 대체될 수 있는지 여부를 표시합니다(Microsoft 업데이트만 해당).

- **이 업데이트를 설치하기 위한 작업**

  이 탭에는 선택한 업데이트의 설치가 범위에 포함된 작업 목록이 표시됩니다. 이 탭을 사용하면 업데이트를 위한 새 원격 설치 작업을 만들 수도 있습니다.

필요한 소프트웨어 업데이트를 보려면 다음 단계를 따릅니다.

1. 필수 소프트웨어 업데이트 옆에 있는 확인란을 선택합니다.
2. **업데이트 설치 상태 통계** 버튼을 누릅니다.

   업데이트 설치 상태 다이어그램이 표시됩니다. 상태를 누르면 선택한 상태의 업데이트가 있는 기기의 목록이 열립니다.

선택한 Windows 실행 기기 중 관리 중인 기기에 설치된 Microsoft 소프트웨어와 같이 타사 소프트웨어에 사용할 수 있는 소프트웨어 업데이트에 관한 정보를 볼 수 있습니다.

선택한 관리 중인 기기에 설치된 타사 소프트웨어에 사용 가능한 업데이트 목록을 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
   관리 중인 기기 목록이 표시됩니다.
2. 관리 중인 기기 목록에서 타사 소프트웨어 업데이트를 보려는 기기 이름이 포함된 링크를 누릅니다.
   선택한 기기의 속성 창이 표시됩니다.
3. 선택한 기기의 속성 창에서 **고급** 탭을 선택합니다.
4. 좌측 창에서 **사용 가능한 업데이트** 섹션을 선택합니다. 설치된 업데이트만 보려면 **설치된 업데이트 표시** 옵션을 활성화합니다.

선택한 기기에 사용 가능한 타사 소프트웨어 업데이트 목록이 표시됩니다.

사용 가능한 소프트웨어 업데이트 목록을 파일로 내보내기

현재 표시되는 Microsoft 소프트웨어 등의 타사 소프트웨어 업데이트를 CSV 또는 TXT 파일로 내보낼 수 있습니다. 예를 들어 정보 보안 관리자에게 보내거나 통계 목적으로 저장하는 데 이러한 파일을 사용할 수 있습니다.

관리 중인 모든 기기에 설치된 타사 소프트웨어에 사용 가능한 업데이트 목록을 텍스트 파일로 내보내려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 업데이트**로 이동합니다.
   이 페이지에는 관리 중인 모든 기기에 설치된 타사 소프트웨어에 대해 사용할 수 있는 업데이트 목록이 표시됩니다.
2. 선호하는 내보내기 형식에 따라 **TXT로 내보내기** 또는 **CSV로 내보내기** 버튼을 누릅니다.

Microsoft 소프트웨어 등의 타사 소프트웨어에 대해 사용 가능한 업데이트 목록이 포함된 파일이 현재 사용 중인 기기에 다운로드됩니다.

선택한 관리 중인 기기에 설치된 타사 소프트웨어에 사용 가능한 업데이트 목록을 텍스트 파일로 내보내려면 다음 단계를 따릅니다.

1. 선택한 관리 중인 기기에서 사용 가능한 타사 소프트웨어 업데이트 목록을 엽니다.
2. 내보낼 소프트웨어 업데이트를 선택합니다.
   전체 소프트웨어 업데이트 목록을 내보내려면 이 단계를 건너 뜁니다.
   전체 소프트웨어 업데이트 목록을 내보내려면 현재 페이지에 표시된 업데이트만 내보냅니다.
   설치된 업데이트만 내보내려면 **설치된 업데이트 표시** 확인란을 선택합니다.
3. 선택하는 내보내기 형식에 따라 **TXT로 내보내기** 또는 **CSV로 내보내기** 버튼을 누릅니다.

선택한 관리 중인 기기에 설치된 Microsoft 소프트웨어 등의 타사 소프트웨어에 대한 업데이트가 포함된 파일이 현재 사용 중인 기기에 다운로드됩니다.

타사 소프트웨어 업데이트 승인 및 거부

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 구성할 때 설치할 업데이트에 특정 상태가 필요한 규칙을 만들 수 있습니다. 예를 들어 업데이트 규칙은 다음 설치를 허용할 수 있습니다.

- 승인된 업데이트만
- 승인 및 정의되지 않은 업데이트만
- 업데이트 상태에 관계없이 모든 업데이트

설치해야 하는 업데이트는 승인하고 설치하면 안 되는 업데이트는 거부할 수 있습니다.

승인됨 상태를 사용하여 업데이트 설치를 관리하면 소량 업데이트에 효율적입니다. 다양한 업데이트를 설치하려면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업에서 구성할 수 있는 규칙을 사용하십시오. 규칙에 명시된 기준을 충족하지 않는 업데이트에 대해서만 *승인됨* 상태를 설정하는 것이 좋습니다. 대량의 업데이트를 수동으로 승인하면 중앙 관리 서버의 성능이 저하되어 결국 서버 과부하로 이어질 수 있습니다.

업데이트 하나 또는 여러 개를 승인하거나 거부하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 업데이트**로 이동합니다.
   사용 가능한 업데이트 목록이 나타납니다.
2. 승인하거나 거부할 업데이트를 선택합니다.
3. **승인**을 눌러 선택한 업데이트를 승인하거나 **거부**를 눌러 선택한 업데이트를 거부합니다.
   기본값은 *정의 안 됨*입니다.

선택한 업데이트에는 정의된 상태가 있습니다.

옵션으로 특정 업데이트의 속성에서 승인 상태를 변경할 수 있습니다.

속성에서 업데이트를 승인하거나 거부하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 업데이트**로 이동합니다.
   사용 가능한 업데이트 목록이 나타납니다.
2. 승인하거나 거부할 업데이트의 이름을 누릅니다.
   업데이트 속성 창이 열립니다.

3. **일반** 섹션에서 **승인 상태 업데이트** 옵션을 변경하여 업데이트 상태를 선택합니다. *승인됨*, *거부됨* 또는 *정의 안 됨* 상태를 선택할 수 있습니다.

4. **저장** 버튼을 눌러 변경 사항을 적용합니다.

선택한 업데이트에는 정의된 상태가 있습니다.

타사 소프트웨어 업데이트에 대해 **거부됨** 상태를 설정하는 경우 이러한 업데이트를 설치하도록 계획했으나 아직 설치하지는 않은 기기에 업데이트가 설치되지 않습니다. 업데이트를 이미 설치한 기기에서는 업데이트가 그대로 유지됩니다. 이러한 업데이트를 삭제해야 하는 경우 로컬에서 수동으로 삭제할 수 있습니다.

Windows 업데이트 동기화 수행 작업 만들기

Windows 업데이트 동기화 수행 작업은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

중앙 관리 서버를 WSUS 서버로 사용하려면 *Windows 업데이트 동기화 수행* 작업이 필요합니다. 이 경우, 중앙 관리 서버에서는 Windows 업데이트를 데이터베이스에 다운로드하고, 네트워크 에이전트를 통해 중앙 집중식 모드로 클라이언트 기기에 Windows Update에 대한 업데이트를 제공합니다. 네트워크에 WSUS 서버가 없으면 각 클라이언트 기기는 외부 서버에서 Microsoft 업데이트를 독립적으로 다운로드합니다.

Windows 업데이트 동기화 수행 작업은 Microsoft 서버에서 메타데이터만 다운로드합니다. Kaspersky Security Center는 업데이트 설치 작업을 실행할 때 업데이트를 다운로드하며 설치를 위해 선택한 업데이트만 다운로드합니다.

Windows 업데이트 동기화 수행 작업을 실행하면 애플리케이션은 Microsoft 업데이트 서버에서 현재 업데이트 목록을 수신합니다. 그런 다음 Kaspersky Security Center는 오래된 업데이트 목록을 취합합니다. 다음 번 **취약점 및 필요한 업데이트 검색** 작업 시작 시 Kaspersky Security Center는 오래된 모든 업데이트에 플래그를 지정하고 해당 업데이트의 삭제 시간을 설정합니다. 다음 번 **Windows 업데이트 동기화 수행** 작업 시작 시 30일 전에 삭제 플래그가 지정된 모든 업데이트가 삭제됩니다. 또한 Kaspersky Security Center는 180일 전에 삭제 플래그가 지정된 오래된 업데이트를 확인한 다음 해당 이전 업데이트를 삭제합니다.

Windows 업데이트 동기화 수행 작업이 완료되고 오래된 업데이트가 삭제될 때 데이터베이스에 삭제된 업데이트 파일과 관련된 해시 코드와 함께 %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 파일(이전에 다운로드된 경우)과 연관된 파일이 남아 있을 수 있습니다. **중앙 관리 서버 점검** 작업을 실행하여 데이터베이스 및 해당 파일에서 오래된 레코드를 삭제할 수 있습니다.

Windows 업데이트 동기화 수행 작업을 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.

2. **추가**를 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

3. Kaspersky Security Center 애플리케이션의 경우 **Windows 업데이트 동기화 수행** 작업 유형을 선택합니다.

4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

5. 작업 실행 시 업데이트 파일을 다운로드하도록 표현하려면 **빠른 설치 파일 다운로드** 옵션을 활성화합니다.

Kaspersky Security Center가 Microsoft Windows 업데이트 서버와 업데이트를 동기화할 때는 모든 파일에 대한 정보가 중앙 관리 서버 데이터베이스에 저장됩니다. 또한 Windows 업데이트 에이전트와 상호 작용하는 동안 업데이트에 필요한 모든 파일이 드라이브에도 다운로드됩니다. 특히 Kaspersky Security Center는 빠른 업데이트 파일에 대한 정보를 데이터베이스에 다운로드하여 필요할 때 다운로드합니다. 빠른 업데이트 파일을 다운로드하는 경우 드라이브의 사용 가능한 공간이 줄어듭니다.

디스크 공간 볼륨 감소를 방지하고 트래픽을 줄이려면 **빠른 설치 파일 다운로드** 옵션을 비활성화합니다.

6. 업데이트를 다운로드할 애플리케이션을 선택합니다.

   모든 애플리케이션 확인란을 선택하면 모든 기존 애플리케이션 및 향후 출시될 수 있는 모든 애플리케이션에 대해 업데이트를 다운로드합니다.

7. 중앙 관리 서버로 다운로드할 업데이트 카테고리를 선택합니다.

   모든 카테고리 확인란을 선택하면 모든 기존 업데이트 카테고리 및 향후 표시될 수 있는 모든 카테고리에 대해 업데이트를 다운로드합니다.

8. 중앙 관리 서버로 다운로드할 업데이트의 현지화 언어를 선택합니다. 다음 옵션 중 하나를 선택합니다:

   - **새로운 언어를 포함해 모든 언어 다운로드**

     이 옵션을 선택하면 업데이트의 사용 가능한 모든 현지화 언어가 중앙 관리 서버에 다운로드됩니다. 기본적으로 이 옵션은 선택되어 있습니다.

   - **선택한 언어만 다운로드**

     이 옵션을 선택하면 중앙 관리 서버에 다운로드할 언어를 업데이트의 현지화 언어 목록에서 선택할 수 있습니다.

9. 작업을 실행할 때 사용할 계정을 지정합니다. 다음 옵션 중 하나를 선택합니다:

   - **기본 계정**

     해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.

     기본적으로 이 옵션은 선택되어 있습니다.

   - **계정 지정**

     계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

10. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

11. **마침** 버튼을 누릅니다.

    그러면 작업이 생성되고 작업 목록에 표시됩니다.

12. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

13. 작업 속성 창에서 필요에 따라 일반 작업 설정을 지정합니다.

14. **저장** 버튼을 누릅니다.

작업이 생성 및 구성됩니다.

타사 애플리케이션 자동 업데이트

일부 타사 애플리케이션은 자동으로 업데이트될 수 있습니다. 애플리케이션 공급업체는 애플리케이션이 자동 업데이트 기능을 지원하는지 여부를 정의합니다. 관리 중인 기기에 설치된 타사 애플리케이션이 자동 업데이트를 지원하는 경우 애플리케이션 속성에서 자동 업데이트 설정을 지정할 수 있습니다. 자동 업데이트 설정을 변경하면 네트워크 에이전트에서 애플리케이션이 설치된 각 관리 중인 기기에 새 설정을 적용합니다.

자동 업데이트 설정은 취약점 및 패치 관리 기능의 다른 개체 및 설정과 독립적입니다. 예를 들면, 이 설정은 *취약점 관련 업데이트를 설치하고 취약점 수정*, *Windows 업데이트 패치 설치*, *취약점 해결* 같은 업데이트 승인 상태 또는 업데이트 설치 작업에 의존하지 않습니다.

타사 애플리케이션에 대한 자동 업데이트 설정을 구성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 자산 관리(소프트웨어)**로 이동합니다.

2. 자동 업데이트 설정을 변경할 애플리케이션의 이름을 누릅니다.
   검색을 단순화하기 위해 **자동 업데이트 상태** 열로 목록에 필터를 적용할 수 있습니다.
   애플리케이션 속성 창이 열립니다.

3. **일반** 섹션에서 다음 설정 값을 선택합니다.
   자동 업데이트 상태

   다음 옵션 중 하나를 선택합니다:

   - **정의 안 됨**
     자동 업데이트 기능이 비활성화되었습니다. Kaspersky Security Center에서는 *취약점 관련 업데이트를 설치하고 취약점 수정*, *Windows 업데이트 패치 설치*, *취약점 해결* 작업을 사용하여 타사 애플리케이션 업데이트를 설치합니다.

   - **허락됨**
     공급업체가 애플리케이션에 대한 업데이트를 릴리스하면 이 업데이트가 관리 중인 기기에 자동으로 설치됩니다. 추가 조치는 필요하지 않습니다.

   - **차단됨**
     애플리케이션 업데이트는 자동으로 설치되지 않습니다. Kaspersky Security Center에서는 *취약점 관련 업데이트를 설치하고 취약점 수정*, *Windows 업데이트 패치 설치*, *취약점 해결* 작업을 사용하여 타사 애플리케이션 업데이트를 설치합니다.

4. **저장** 버튼을 눌러 변경 사항을 적용합니다.

자동 업데이트 설정이 선택한 애플리케이션에 적용됩니다.

타사 소프트웨어 취약점 수정

이 섹션에서는 관리 중인 기기에 설치된 소프트웨어의 취약점 수정과 관련된 Kaspersky Security Center의 기능을 설명합니다.

시나리오: 타사 소프트웨어 취약점 찾기 및 수정

이 섹션에서는 Windows를 실행하는 관리 중인 기기에서 취약점을 찾아 수정하는 시나리오를 제공합니다. 운영 체제 및 Microsoft 소프트웨어를 포함한 타사 소프트웨어에서 소프트웨어 취약점을 찾아 수정할 수 있습니다.

필수 구성 요소

- 조직에 Kaspersky Security Center가 배포되어 있습니다.
- 조직에 Windows를 실행하는 관리 중인 기기가 있습니다.
- 중앙 관리 서버가 다음 작업을 수행하려면 인터넷 연결이 필요합니다.
  - Microsoft 소프트웨어의 취약성에 대한 권장 수정 목록을 작성합니다. 이 목록은 Kaspersky 전문가가 생성하고 정기적으로 업데이트합니다.
  - Microsoft 소프트웨어가 아닌 타사 소프트웨어의 취약성을 수정합니다.

단계

소프트웨어 취약점 찾기 및 수정은 다음 단계로 진행됩니다:

1. **관리 중인 기기에 설치된 소프트웨어의 취약점 검사**

   관리 중인 기기에 설치된 소프트웨어에서 취약점을 찾으려면 *취약점 및 필요한 업데이트 검색* 작업을 실행합니다. 이 작업이 완료되면 Kaspersky Security Center는 작업 속성에서 지정한 기기에 설치된 타사 소프트웨어에 대하여 탐지된 취약점 및 필요한 업데이트의 목록을 받습니다.

   취약점 및 필요한 업데이트 검색 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동으로 생성합니다. 마법사를 실행하지 않았다면 지금 시작하거나 수동으로 작업을 만듭니다.

   방법 지침:

   - 관리 콘솔: 애플리케이션 취약점 검사, 취약점 및 필요한 업데이트 검색 작업 스케줄 지정
   - Kaspersky Security Center 웹 콘솔: 취약점 및 필요한 업데이트 검색 작업 만들기, 취약점 및 필요한 업데이트 검색 작업 설정

2. **탐지된 소프트웨어 취약점 목록 분석**

   소프트웨어 취약점 목록을 보고 수정할 취약점을 결정합니다. 각 취약점에 대한 자세한 정보를 보려면 목록에서 취약점 이름을 누릅니다. 목록의 각 취약점에 대해 관리 중인 기기의 취약점에 대한 통계를 볼 수도 있습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 취약점에 대한 정보 보기, 관리 중인 기기의 취약점 통계 보기
- Kaspersky Security Center 웹 콘솔: 소프트웨어 취약점 정보 보기, 관리 중인 기기의 취약점 통계 보기

3 취약점 수정 구성

소프트웨어 취약점이 탐지되면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업 또는 *취약점 해결* 작업을 사용하여 관리 중인 기기에서 소프트웨어 취약점을 수정할 수 있습니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 사용하여 관리 중인 기기에 설치된 Microsoft 소프트웨어를 포함한 타사 소프트웨어의 취약점에 대한 업데이트 및 수정을 수행합니다. 이 작업을 통해 여러 업데이트를 설치하고 특정 규칙에 따라 여러 취약점을 수정할 수 있습니다. 이 작업은 취약점 및 패치 관리 기능에 대한 라이센스가 있을 때만 만들 수 있습니다. 소프트웨어 취약점을 수정하기 위해 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업에서는 권장 소프트웨어 업데이트를 사용합니다.

취약점 해결 작업에는 취약점 및 패치 관리 기능에 대한 라이센스 옵션이 필요하지 않습니다. 이 작업을 사용하려면 작업 설정에 나열된 타사 소프트웨어의 취약점에 대한 사용자 수정을 수동으로 지정해야 합니다. *취약점 해결* 작업에서는 Microsoft 소프트웨어에 권장 수정을 사용하고 타사 소프트웨어에는 사용자 수정을 사용합니다.

취약점 수정 마법사를 시작하여 이러한 작업 중 하나를 자동으로 만들거나 수동으로 이러한 작업을 만들 수도 있습니다.

방법 지침:

- 관리 콘솔: 타사 소프트웨어의 취약점에 대한 사용자 수정 선택, 애플리케이션의 취약점 수정
- Kaspersky Security Center 웹 콘솔: 타사 소프트웨어의 취약점에 대한 사용자 수정 선택, 타사 소프트웨어의 취약점 수정, 필요한 업데이트 설치 및 취약점 수정 작업 만들기

4 작업 스케줄 지정

취약점 목록을 항상 최신 상태로 유지하기 위해 *취약점 및 필요한 업데이트 검색* 작업의 스케줄을 지정하여 가끔 자동으로 실행합니다. 권장하는 평균 빈도는 일주일에 한 번입니다.

사용자가 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 만든 경우 *취약점 및 필요한 업데이트 검색* 작업과 빈도가 같거나 적게 실행하도록 스케줄을 지정할 수 있습니다. *취약점 해결* 작업 예약 시 Microsoft 소프트웨어 수정을 선택하거나 작업을 시작하기 전에 매번 타사 소프트웨어의 사용자 수정을 지정해야 합니다.

작업의 스케줄을 지정할 때 *취약점 및 필요한 업데이트 검색* 작업이 완료된 후에 취약점 수정 작업을 시작해야 합니다.

5 소프트웨어 취약점 무시(선택 사항)

원하는 경우 모든 관리 중인 기기 또는 선택한 관리 중인 기기에서만 소프트웨어 취약점 수정을 무시할 수 있습니다.

방법 지침:

- 관리 콘솔: 소프트웨어 취약점 무시
- Kaspersky Security Center 웹 콘솔: 소프트웨어 취약점 무시

6 취약점 수정 작업 실행

취약점 관련 업데이트를 설치하고 취약점 수정 작업 또는 *취약점 수정* 작업을 시작합니다. 작업이 완료되면 작업 목록에서 상태가 *성공적으로 완료*인지 확인하십시오.

7 소프트웨어 취약점 수정 결과에 대한 리포트 작성(선택 사항)

취약점 수정에 대한 자세한 통계를 보려면 취약점 리포트를 생성합니다. 이 리포트에는 수정되지 않은 소프트웨어 취약점에 대한 정보가 표시됩니다. 따라서 조직의 Microsoft 소프트웨어를 포함한 타사 소프트웨어의 취약점을 찾고 수정하는 방법에 대한 아이디어를 얻을 수 있습니다.

방법 지침:

- 관리 콘솔: 리포트 만들기 및 보기
- Kaspersky Security Center 웹 콘솔: 리포트 생성 및 보기

8. **타사 소프트웨어의 취약점 발견 및 수정 구성 확인**

   다음을 수행했는지 확인합니다.

   - 관리 중인 기기의 소프트웨어 취약점 목록을 구하고 검토했습니다.
   - 원하는 경우 소프트웨어 취약점을 무시했습니다.
   - 취약점을 수정하기 위한 작업을 구성했습니다.
   - 소프트웨어 취약점을 찾아 수정하기 위한 작업이 순차적으로 시작되도록 작업 스케줄을 지정했습니다.
   - 소프트웨어 취약점 수정 작업이 실행되었는지 확인했습니다.

결과

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 생성하고 구성한 경우 관리 중인 기기에서 취약점이 자동으로 수정됩니다. 작업이 실행될 때 사용 가능한 소프트웨어 업데이트의 목록을 작업 설정에 지정된 규칙과 연관시킵니다. 규칙의 기준을 충족하는 모든 소프트웨어 업데이트가 중앙 관리 서버 저장소에 다운로드되고 소프트웨어 취약점을 수정하기 위해 설치됩니다.

사용자가 *취약점 해결* 작업을 만든 경우 Microsoft 소프트웨어의 소프트웨어 취약점만 수정됩니다.

소프트웨어 취약점 찾기 및 수정 정보

Kaspersky Security Center는 Microsoft Windows 제품군 운영 체제를 실행하는 관리 중인 기기에서 소프트웨어 취약점을 탐지하고 수정합니다. 취약점은 운영 체제 및 Microsoft 소프트웨어를 포함한 타사 소프트웨어에서 탐지됩니다.

미국 내 소프트웨어에서 업데이트 기능(바이러스 백신 시그니처 업데이트 및 코드베이스 업데이트 포함)과 KSN 기능이 제공되지 않을 수도 있습니다.

소프트웨어 취약점 찾기

소프트웨어 취약점을 찾기 위해 Kaspersky Security Center는 알려진 취약점 데이터베이스의 특성을 사용합니다. 이 데이터베이스는 Kaspersky 전문가가 만듭니다. 여기에는 취약점 설명, 취약점 탐지 날짜, 취약점 심각도와 같은 취약점에 대한 정보가 포함됩니다. 소프트웨어 취약점의 세부 정보는 Kaspersky 웹사이트에서 확인할 수 있습니다.

Kaspersky Security Center는 *취약점 및 필요한 업데이트 검색* 작업을 사용하여 소프트웨어 취약점을 찾습니다.

경우에 따라 다음 방법 중 하나로 Microsoft Windows 운영 체제에서 탐지한 취약점을 수정할 수 있습니다:

- OS용 업데이트 설치.
- OS를 최신 버전으로 업그레이드(예: Windows 10에서 Windows 11로).

이 시나리오에서 Kaspersky Security Center는 같은 취약점에 대해 두 개의 항목을 표시합니다.

소프트웨어 취약점 수정

소프트웨어 취약점을 해결하기 위해 Kaspersky Security Center는 소프트웨어 공급업체가 제공하는 소프트웨어 업데이트를 사용합니다. 소프트웨어 업데이트 메타데이터는 다음 작업을 실행한 결과로 중앙 관리 서버 저장소로 다운로드됩니다:

- *중앙 관리 서버 저장소에 업데이트 다운로드*. 이 작업은 Kaspersky 및 타사 소프트웨어의 업데이트 메타데이터를 다운로드하기 위한 것입니다. 이 작업은 Kaspersky Security Center 빠른 시작 마법사가 자동으로 생성합니다. 중앙 관리 서버 저장소 작업에 대한 다운로드 업데이트를 수동으로 만들 수 있습니다.
- *Windows 업데이트 동기화 수행*. 이 작업은 Microsoft 소프트웨어용 업데이트 메타데이터를 다운로드하기 위한 것입니다.

취약점을 수정하기 위한 소프트웨어 업데이트는 전체 배포 패키지 또는 패치로 표시될 수 있습니다. 소프트웨어 취약점을 수정하는 소프트웨어 업데이트 이름은 *수정*입니다. *권장 수정*은 Kaspersky 전문가 설치가 권장되는 수정입니다. *사용자 수정*은 사용자 설치가 수동으로 지정되는 수정입니다. 사용자 수정을 설치하려면 이 수정이 포함된 설치 패키지를 만들어야 합니다.

취약점 및 패치 관리 기능이 있는 Kaspersky Security Center 라이센스가 있다면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 사용하여 소프트웨어 취약점을 수정할 수 있습니다. 이 작업은 권장 수정을 설치하여 여러 취약점을 자동으로 수정합니다. 이 작업에서는 여러 취약점을 수정하기 위해 특정 규칙을 수동으로 구성할 수 있습니다.

취약점 및 패치 관리 기능이 있는 Kaspersky Security Center 라이센스가 없다면 *취약점 해결* 작업을 사용하여 소프트웨어 취약점을 수정할 수 있습니다. 이 작업을 통해 Microsoft 소프트웨어에 대한 권장 수정과 타사 소프트웨어에 대한 사용자 수정을 설치하여 취약점을 수정할 수 있습니다.

취약점 및 패치 관리 기능을 사용하여 타사 소프트웨어 업데이트 설치 시, 보안상의 이유로 Kaspersky 기술을 사용해 악성 코드를 자동 검사합니다. 이러한 기술은 자동 파일 검사에 사용되며, 샌드박스 환경에서의 바이러스 검사, 정적 분석, 동적 분석, 행동 분석, 머신 러닝 등을 포함합니다.

Kaspersky 전문가는 취약점 및 패치 관리 기능으로 설치할 수 있는 타사 소프트웨어 업데이트에 대한 수동 분석을 수행하지 않습니다. 또한 Kaspersky 전문가는 이러한 업데이트에서 알려지거나 알려지지 않은 취약점이나 문서화되지 않은 기능을 검색하지 않으며, 위 단락에 지정된 유형 외에 다른 유형의 업데이트 분석도 수행하지 않습니다.

관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

일부 소프트웨어 취약점 수정에서 EULA(최종 사용자 라이센스 계약서) 동의가 요청되는 경우 설치 중인 소프트웨어의 EULA에 동의해야 합니다. EULA에 동의하지 않으면 소프트웨어 취약점이 수정되지 않습니다.

타사 소프트웨어 취약점 수정

소프트웨어 취약점 목록을 확보한 후 Windows를 실행하는 관리 중인 기기에서 소프트웨어 취약점을 수정할 수 있습니다. *취약점 해결* 작업 또는 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 만들어서 실행하는 방식으로 Microsoft 소프트웨어를 비롯해 운영 체제 및 타사 소프트웨어의 소프트웨어 취약점을 수정할 수 있습니다.

관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

옵션으로 다음과 같은 방법을 통해 소프트웨어 취약점을 수정하는 작업을 생성할 수 있습니다.

- 취약점 목록을 열고 수정할 취약점을 지정합니다.

  그러면 소프트웨어 취약점을 수정하는 새로운 작업이 생성됩니다. 옵션으로 선택한 취약점을 기존 작업에 추가할 수 있습니다.

- 취약점 수정 마법사를 실행합니다.

  취약점 수정 마법사는 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

  마법사는 취약점 수정 작업의 생성 및 구성을 단순화하여 같은 업데이트를 설치하는 중복 작업이 생성되지 않도록 합니다.

취약점 목록을 사용하여 소프트웨어 취약점 수정

소프트웨어 취약점을 수정하려면 다음 단계를 따릅니다.

1. 취약점 목록 중 하나를 엽니다.

   - 일반 취약점 목록을 열려면 **동작** → **패치 관리** → **소프트웨어 취약점**으로 이동합니다.
   - 관리 중인 기기의 취약점 목록을 열려면 메인 메뉴에서 **에셋(기기)** → **관리 중인 기기** → <기기 이름> → **고급** → **소프트웨어 취약점**으로 이동합니다.
   - 특정 애플리케이션에 대한 취약점 목록을 열려면 메인 메뉴에서 **동작** → **타사 애플리케이션** → **자산 관리(소프트웨어)** → <애플리케이션 이름> → **취약점**으로 이동합니다.

   타사 소프트웨어의 취약점 목록이 포함된 페이지가 표시됩니다.

2. 목록에서 하나 이상의 취약점을 선택한 다음 **취약점 수정** 버튼을 누릅니다.

   선택한 취약점 중 하나를 수정하는 권장 소프트웨어 업데이트가 없는 경우 정보 메시지가 표시됩니다.

   일부 소프트웨어 취약점 수정에서 EULA(최종 사용자 라이센스 계약서) 동의가 요청되는 경우 설치 중인 소프트웨어의 EULA에 동의해야 합니다. EULA에 동의하지 않으면 소프트웨어 취약점이 수정되지 않습니다.

3. 다음 옵션 중 하나를 선택합니다:

   - **새 작업**

     새 작업 마법사가 시작됩니다. 취약점 및 패치 관리 라이센스가 있다면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 미리 선택되어 있습니다. 라이센스가 없는 경우 *취약점 해결* 작업이 미리 선택되어 있습니다. 마법사의 단계에 따라 작업 생성을 완료합니다.

   - **취약점 수정(특정 작업에 규칙 추가)**

     선택한 취약점을 추가할 작업을 선택합니다. 취약점 및 패치 관리 라이센스가 있다면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 선택합니다. 선택한 취약점을 수정하는 새로운 규칙이 선택한 작업에 자동으로 추가됩니다. 라이센스가 없다면 *취약점 해결* 작업을 선택합니다. 선택한 취약점이 작업 속성에 추가됩니다.

     작업 속성 창이 열립니다. **저장** 버튼을 눌러 변경 사항을 적용합니다.

   새 작업을 만들기로 선택한 경우 작업은 **에셋(기기) → 작업**에 있는 작업 목록에서 생성되고 표시됩니다. 기존 작업에 취약점을 추가하기로 선택한 경우 취약점은 작업 속성에 저장됩니다.

타사 소프트웨어 취약점을 수정하려면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업 또는 *취약점 해결* 작업을 시작합니다. *취약점 해결* 작업을 만들었다면 작업 설정에 나열된 소프트웨어 취약점을 수정하기 위해 소프트웨어 업데이트를 수동으로 지정해야 합니다.

취약점 수정 마법사를 사용하여 소프트웨어 취약점 수정

취약점 수정 마법사는 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

취약점 수정 마법사를 사용하여 소프트웨어 취약점을 수정하려면:

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 취약점**으로 이동합니다.

   관리 중인 기기에 설치된 타사 소프트웨어의 취약점 목록이 포함된 페이지가 표시됩니다.

2. 다운로드하려는 취약점 옆에 있는 확인란을 선택합니다.

3. **취약점 수정 마법사 실행** 버튼을 누릅니다.

   취약점 수정 마법사가 시작됩니다. **취약점 수정 작업 선택** 페이지에 다음 유형의 모든 기존 작업 목록이 표시됩니다.

   - *취약점 관련 업데이트를 설치하고 취약점 수정*
   - *Windows 업데이트 패치 설치*
   - *취약점 해결*

   새 업데이트를 설치하려면 마지막 두 가지 유형의 작업을 수정해서는 안 됩니다. 새 업데이트를 설치하기 위해 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업만 사용할 수 있습니다.

4. 마법사에서 선택한 취약점 수정 작업만 표시하도록 하려면, **이 취약점을 수정하는 작업만 표시** 옵션을 활성화합니다.

5. 다음 중 원하는 작업을 선택합니다.

- 작업을 시작하려면 작업 이름 옆에 있는 확인란을 선택한 다음 **시작** 버튼을 누릅니다.
- 기존 작업에 새 규칙을 추가하려면 다음 단계를 따릅니다.

  a. 작업 이름 옆에 있는 확인란을 선택한 다음 **규칙 추가** 버튼을 누릅니다.

  b. 페이지가 열리면 새 규칙을 구성합니다.

  - **심각도에 따라 취약점을 수정하기 위한 규칙**

    소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

    이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 선택한 업데이트의 심각도(**중간**, **높음**, **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

    이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **선택한 취약점에 권장되는 것으로 정의된 업데이트와 동일한 유형의 업데이트에 의한 취약점 수정 규칙**(Microsoft 소프트웨어 취약점에만 사용 가능)
  - **선택한 공급업체의 애플리케이션 취약점을 수정하기 위한 규칙**(타사 소프트웨어 취약점에만 사용 가능)
  - **선택한 애플리케이션의 모든 버전에 있는 취약점을 수정하기 위한 규칙**(타사 소프트웨어 취약점에만 사용 가능)
  - **선택한 취약점을 수정하기 위한 규칙**
  - **이 취약점을 수정하는 업데이트 승인**

    선택한 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  c. **추가** 버튼을 누릅니다.

- 작업을 만들려면 다음 단계를 따릅니다.

  a. **새 작업** 버튼을 누릅니다.

  b. 페이지가 열리면 새 규칙을 구성합니다.

  - **심각도에 따라 취약점을 수정하기 위한 규칙**

    소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 선택한 업데이트의 심각도(**중간**, **높음**, **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **선택한 취약점에 권장되는 것으로 정의된 업데이트와 동일한 유형의 업데이트에 의한 취약점 수정 규칙**(Microsoft 소프트웨어 취약점에만 사용 가능)
- **선택한 공급업체의 애플리케이션 취약점을 수정하기 위한 규칙**(타사 소프트웨어 취약점에만 사용 가능)
- **선택한 애플리케이션의 모든 버전에 있는 취약점을 수정하기 위한 규칙**(타사 소프트웨어 취약점에만 사용 가능)
- **선택한 취약점을 수정하기 위한 규칙**
- **이 취약점을 수정하는 업데이트 승인**

  선택한 업데이트의 설치가 승인됩니다. 적용된 일부 업데이트 설치 규칙이 승인된 업데이트 설치만 허용하는 경우 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

c. **추가** 버튼을 누릅니다.

작업 시작을 선택했다면 마법사를 닫아도 됩니다. 작업은 백그라운드 모드에서 완료됩니다. 추가 조치는 필요하지 않습니다.

기존 작업에 규칙을 추가하기로 선택했다면 작업 속성 창이 열립니다. 새 규칙이 이미 작업 속성에 추가되었습니다. 규칙 또는 기타 작업 설정을 확인하거나 수정할 수 있습니다. **저장** 버튼을 눌러 변경 사항을 적용합니다.

작업 생성을 선택했다면 새 작업 마법사에서 작업 생성을 계속 진행합니다. 취약점 수정 마법사에 추가한 새로운 규칙이 새 작업 마법사에 표시됩니다. 새 작업 마법사를 완료하면 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업이 작업 목록에 추가됩니다.

취약점 수정 작업 생성

취약점 해결 작업을 통해 Windows를 실행하는 관리 중인 기기에서 소프트웨어 취약점을 수정할 수 있습니다. Microsoft 소프트웨어를 포함한 타사 소프트웨어의 소프트웨어 취약점을 수정할 수 있습니다.

취약점 및 패치 관리 라이센스가 없다면 *취약점 해결* 유형의 새 작업을 만들 수 없습니다. 새 취약점을 수정하려면 기존 *취약점 해결* 작업에 추가하면 됩니다. *취약점 해결* 작업 대신 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 사용하는 것이 좋습니다. *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 사용하면 정의한 규칙에 따라 여러 업데이트를 수정하고 여러 취약점을 수정할 수 있습니다.

관리 중인 기기에서 타사 애플리케이션을 업데이트하거나 타사 애플리케이션의 취약점을 수정하려면 사용자의 행동이 필요할 수 있습니다. 예를 들어, 현재 열려 있는 타사 애플리케이션을 닫으라는 메시지가 표시될 수 있습니다.

취약점 해결 작업 만들기:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼으로 마법사를 진행합니다.
3. Kaspersky Security Center 애플리케이션의 경우 **취약점 해결** 작업 유형을 선택합니다.
4. 만들고 있는 작업의 이름을 지정합니다.
   작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.
5. 이 작업이 할당되는 기기를 선택합니다.
6. **추가** 버튼을 누릅니다.
   취약점 목록이 열립니다.
7. 수정할 취약점을 선택한 다음 **확인**을 누릅니다.
   일반적으로 Microsoft 소프트웨어 취약점에는 권장 수정 사항이 있습니다. 추가 작업이 필요하지 않습니다. 다른 공급업체의 소프트웨어 취약점의 경우 먼저 수정할 각 취약점에 대해 사용자 수정을 지정해야 합니다. 그런 다음 이러한 취약점을 *취약점 해결* 작업에 추가할 수 있습니다.
8. 운영 체제 다시 시작 설정을 지정합니다.

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **반복해서 물어보기(분)**

  이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

- **다음 시간 이후에 재시작(분)**

  사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 애플리케이션 강제 종료**

  애플리케이션을 실행하면 클라이언트 기기가 다시 시작되지 않을 수 있습니다. 예를 들어 워드 프로세싱 애플리케이션에서 문서를 편집한 후에 저장하지 않으면 애플리케이션에서 기기 다시 시작을 허용하지 않습니다.

  이 옵션을 활성화하면 잠긴 기기를 다시 시작하기 전에 해당 기기의 애플리케이션을 강제로 닫습니다. 그러면 사용자가 저장하지 않은 변경 내용은 손실될 수 있습니다.

  이 옵션을 비활성화하면 잠긴 기기가 다시 시작되지 않습니다. 이 기기의 작업 상태에는 기기를 다시 시작해야 함이 표시됩니다. 사용자는 잠긴 기기에서 실행 중인 모든 애플리케이션을 수동으로 닫고 이러한 기기를 다시 시작해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

9. 다음 계정 설정을 지정합니다.

   - **기본 계정**

     해당 작업을 수행하는 애플리케이션과 동일한 계정을 사용하여 작업이 실행됩니다.

     기본적으로 이 옵션은 선택되어 있습니다.

   - **계정 지정**

     계정 및 **암호** 필드를 작성하여 작업 실행에 사용되는 계정의 세부 정보를 지정합니다. 계정에는 이 작업에 대한 충분한 권한이 있어야 합니다.

   - **계정**

     작업 실행에 사용되는 계정입니다.

   - **암호**

     작업을 실행할 계정의 암호입니다.

10. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

11. **마침** 버튼을 누릅니다.

    그러면 작업이 생성되고 작업 목록에 표시됩니다.

12. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

13. 작업 속성 창에서 필요에 따라 일반 작업 설정을 지정합니다.

14. **저장** 버튼을 누릅니다.

    작업이 생성 및 구성됩니다.

필수 업데이트 설치 및 취약점 수정 작업 만들기

> *취약점 관련 업데이트를 설치하고 취약점 수정* 작업은 취약점 및 패치 관리 라이선스가 있어야만 사용 가능합니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 사용하여 관리 중인 기기에 설치된 Microsoft 소프트웨어를 포함한 타사 소프트웨어의 취약점에 대한 업데이트 및 수정을 수행합니다. 이 작업을 통해 여러 업데이트를 설치하고 특정 규칙에 따라 여러 취약점을 수정할 수 있습니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업을 사용하여 업데이트를 설치하거나 취약점을 수정하려면 다음 작업을 수행하면 됩니다.

- 설치 업데이트 마법사 또는 취약점 수정 마법사를 실행합니다.
- *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 만듭니다.
- 기존 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업에 업데이트 설치에 대한 규칙을 추가합니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업 만들기:

1. 메인 메뉴에서 **에셋(기기)** → **작업**으로 이동합니다.

2. **추가**를 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

3. Kaspersky Security Center 애플리케이션의 경우 **취약점 관련 업데이트를 설치하고 취약점 수정** 작업 유형을 선택합니다.

   작업이 표시되지 않으면 계정에 **시스템 관리**: **취약성 및 패치 관리** 기능 영역에 대한 **읽기**, **수정**, **실행** 권한이 있는지 확인하십시오. 이러한 액세스 권한이 없으면 *필요한 업데이트 설치 및 취약성 수정* 작업을 생성하고 구성할 수 없습니다.

4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

5. 이 작업이 할당되는 기기를 선택합니다.

6. 업데이트 설치 규칙을 지정하고 다음 설정을 지정합니다.

   - **기기 다시 시작 또는 종료 시 설치 시작**

     > 이 옵션을 활성화하면 기기가 다시 시작되거나 종료되기 전에 업데이트가 설치됩니다. 그렇지 않으면 업데이트는 스케줄에 따라 설치됩니다.
     >
     > 업데이트 설치가 기기 성능에 영향을 줄 수 있는 경우 이 옵션을 사용합니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **필요한 일반 시스템 구성 요소 설치**

  이 옵션을 활성화하면 업데이트를 설치하기 전에 애플리케이션은 업데이트 설치를 설치하기 위해 필요한 모든 일반 시스템 구성 요소(선결 조건)를 자동으로 설치합니다. 이러한 필수 구성 요소의 예로는 운영 체제 업데이트 등이 있습니다.

  이 옵션을 비활성화하는 경우에는 필수 구성 요소를 수동으로 설치해야 합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 시 새 애플리케이션 버전의 설치 허용**

  이 옵션을 활성화하면 업데이트 시 소프트웨어 애플리케이션의 새 버전이 설치되는 경우 업데이트가 허용됩니다.

  이 옵션을 비활성화하면 소프트웨어가 업그레이드되지 않습니다. 그러면 소프트웨어의 새 버전을 수동으로 또는 다른 작업을 통해 설치할 수 있습니다. 예를 들어 새 소프트웨어 버전이 회사 인프라를 지원하지 않거나 테스트 인프라에서 업그레이드를 확인하려는 경우 이 옵션을 사용할 수 있습니다.

  기본적으로 이 옵션은 켜져 있습니다.

  애플리케이션을 업그레이드하면 클라이언트 기기에 설치된 종속 애플리케이션의 오작동이 발생할 수 있습니다.

- **업데이트를 기기에 다운로드만 하고 설치는 하지 않음**

  이 옵션을 활성화하면 애플리케이션은 기기에 업데이트를 다운로드하지만 자동으로 해당 업데이트를 설치하지는 않습니다. 그러면 다운로드한 업데이트를 수동으로 설치할 수 있습니다.

  Microsoft 업데이트는 시스템 Windows 저장소에 다운로드됩니다. 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트는 **업데이트 다운로드 경로** 필드에 지정된 폴더에 다운로드됩니다.

  이 옵션을 비활성화하면 업데이트가 기기에 자동으로 설치됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **업데이트 다운로드 경로**

  이 폴더는 타사 애플리케이션(Kaspersky이 아닌 소프트웨어 공급 업체에서 만든 애플리케이션)의 업데이트를 다운로드하는 데 사용됩니다.

- **고급 진단 사용**

  이 기능을 활성화하면 Kaspersky Security Center 원격 진단 유틸리티에서 네트워크 에이전트에 대해 추적 파일 쓰기가 비활성화되어 있어도 네트워크 에이전트가 추적 로그를 씁니다. 추적 로그는 2개 파일에 차례대로 기록됩니다. 이 두 파일의 총 크기는 **고급 진단 파일의 최대 크기(MB)** 값에 의해 결정됩니다. 두 파일이 모두 꽉 차면 네트워크 에이전트가 해당 파일에 쓰기를 다시 시작합니다. 추적 로그가 포함된 파일은 %WINDIR%\Temp 폴더에 저장됩니다. 이러한 파일은 원격 진단 유틸리티에서 액세스, 다운로드 또는 삭제할 수 있습니다.

  이 기능을 비활성화하면 네트워크 에이전트가 Kaspersky Security Center 원격 진단 유틸리티의 설정에 따라 추적 로그를 씁니다. 추가 추적 로그는 기록되지 않습니다.

작업을 생성할 때는 고급 진단을 활성화하지 않아도 됩니다. 나중에 일부 기기에서 작업 실행이 실패하여 다른 작업 실행 중에 추가 정보를 수집하려 하거나 할 때 이 기능을 사용할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **고급 진단 파일의 최대 크기(MB)**

  기본값은 100MB이고 사용 가능한 값은 1MB~2048MB입니다. Kaspersky 기술 지원 전문가에게 전송한 고급 진단 파일의 정보로는 문제를 해결하기에 부족한 경우 전문가가 기본값 변경을 요청할 수 있습니다.

7. 운영 체제 다시 시작 설정을 지정합니다.

- **기기 다시 시작 안 함**

  작업 후에 클라이언트 기기가 자동으로 다시 시작되지 않습니다. 이 작업을 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 작업에 적합합니다.

- **기기 다시 시작**

  이 옵션을 선택하면 작업을 완료하기 위해 클라이언트 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 작업에 유용합니다.

- **사용자 확인 후 처리**

  클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. 이 옵션은 사용자가 기기를 다시 시작하기에 가장 편리할 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합합니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **반복해서 물어보기(분)**

  이 옵션을 활성화하면 애플리케이션에서 운영 체제를 다시 시작한다는 메시지가 지정된 빈도로 사용자에게 표시됩니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 간격은 5분입니다. 사용 가능한 값은 1~1440분입니다.

  이 옵션을 비활성화하면 메시지가 한 번만 표시됩니다.

- **다음 시간 이후에 재시작(분)**

  사용자에게 메시지를 표시한 후 지정된 시간 간격이 만료되면 애플리케이션이 운영 체제를 강제로 다시 시작합니다.

  기본적으로 이 옵션은 켜져 있습니다. 기본 지연 시간은 30분입니다. 사용 가능한 값은 1~1440분입니다.

- **잠긴 세션에서 다음 시간 후 애플리케이션 강제 종료(분)**

  사용자 기기가 잠겨 있으면 애플리케이션은 지정된 비활성 기간이 지난 후 자동으로 또는 수동으로 강제 종료됩니다.

  이 옵션을 사용하면 입력 필드에 지정된 시간 간격 만료 시 애플리케이션이 잠긴 기기에서 강제 종료됩니다.

  이 옵션이 비활성화되어 있으면 애플리케이션이 잠긴 기기에서 종료되지 않습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

8. 기본 작업 설정을 수정하려면 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

9. **마침** 버튼을 누릅니다.

   그러면 작업이 생성되고 작업 목록에 표시됩니다.

10. 작업 속성 창을 열려면 생성된 작업의 이름을 누릅니다.

11. 작업 속성 창에서 필요에 따라 일반 작업 설정을 지정합니다.

12. **저장** 버튼을 누릅니다.

    작업이 생성 및 구성됩니다.

작업 결과에 0x80240033 경고 'Windows 업데이트 에이전트 오류 80240033("라이센스 약관을 다운로드할 수 없습니다.")' 오류가 포함되어 있는 경우 Windows 레지스트리를 통해 이 문제를 해결할 수 있습니다.

업데이트 설치에 대한 규칙 추가

이 기능은 취약점 및 패치 관리 라이센스가 있어야만 사용 가능합니다.

취약점 관련 업데이트를 설치하고 취약점 수정 작업으로 소프트웨어 업데이트를 설치하거나 소프트웨어 취약점을 수정할 때는 업데이트 설치 규칙을 반드시 지정해야 합니다. 이러한 규칙에 따라 설치할 업데이트와 수정할 취약점이 결정됩니다.

정확한 설정은 모든 업데이트, Windows Update 업데이트 또는 타사 애플리케이션(Kaspersky 및 Microsoft 이외의 소프트웨어 공급업체에서 만든 애플리케이션) 업데이트 중 어디에 대한 규칙을 추가하는지에 따라 달라집니다. Windows Update 업데이트 또는 타사 애플리케이션 업데이트에 대한 규칙을 추가하는 경우 업데이트를 설치할 특정 애플리케이션 및 애플리케이션 버전을 선택할 수 있습니다. 모든 업데이트용 규칙을 추가할 때는 설치할 특정 업데이트 및 업데이트 설치를 통해 수정할 취약점을 선택할 수 있습니다.

다음과 같은 방법으로 업데이트 설치 규칙을 추가할 수 있습니다.

- 새 취약점 관련 업데이트를 설치하고 취약점 수정 작업을 만드는 동안 규칙을 추가합니다.
- 기존 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업의 속성 창에 있는 **애플리케이션 설정** 탭에서 규칙을 추가합니다.
- 업데이트 설치 마법사 또는 취약점 수정 마법사를 사용합니다.

모든 업데이트에 대한 새 규칙을 추가하려면 다음 단계를 따릅니다.

1. **추가** 버튼을 누릅니다.
   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

2. **규칙 유형** 페이지에서 **모든 업데이트에 대한 규칙**을 선택합니다.

3. **일반 기준** 페이지에서 드롭다운 목록을 사용하여 다음 설정을 지정합니다:

   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.
     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

   - **다음 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

     이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

4. **업데이트** 페이지에서 설치할 업데이트를 선택합니다:

   - **적합한 모든 업데이트 설치**

     마법사의 **일반 기준** 페이지에 지정된 기준을 충족하는 모든 소프트웨어 업데이트를 설치합니다. 기본적으로 선택됩니다.

   - **다음 목록의 업데이트만 설치**

     목록에서 수동으로 선택하는 소프트웨어 업데이트만 설치합니다. 이 목록에는 사용 가능한 모든 소프트웨어 업데이트가 포함되어 있습니다.

     예를 들어 테스트 환경에서 설치를 확인하거나 중요한 애플리케이션 또는 특정 애플리케이션만 업데이트하려는 등의 경우 특정 업데이트를 선택할 수 있습니다.

     - **선택된 업데이트를 설치하는 데 필요한 이전의 모든 애플리케이션 업데이트 자동 설치**

       선택한 업데이트를 설치하는 데 필요한 경우 중간 애플리케이션 버전 설치에 동의한다면 이 옵션을 활성화한 상태로 유지하십시오.

이 옵션을 비활성화하면 애플리케이션의 선택한 버전만 설치됩니다. 후속 버전의 증분 방식 설치를 시도하지 않고 단순하게 애플리케이션을 업데이트하려면 이 옵션을 비활성화합니다. 이전 애플리케이션 버전을 설치하지 않으면 선택한 업데이트를 설치할 수 없는 경우에는 애플리케이션 업데이트가 실패합니다.

기기에 설치되어 있는 애플리케이션 버전 3을 버전 5로 업데이트하려고 하는데 이 애플리케이션의 버전 5는 버전 4가 설치되어 있어야 설치 가능한 경우를 예로 들어 보겠습니다. 이 옵션을 활성화하면 소프트웨어는 먼저 버전 4를 선택한 후에 버전 5를 선택합니다. 이 옵션을 비활성화하면 소프트웨어가 애플리케이션을 업데이트하지 못합니다.

기본적으로 이 옵션은 켜져 있습니다.

5. **취약점** 페이지에서 선택한 업데이트를 설치하면 수정되는 취약점을 선택합니다:

   - **기타 기준과 일치하는 모든 취약점 수정**

     마법사의 **일반 기준** 페이지에 지정된 기준을 충족하는 모든 취약점을 수정합니다. 기본적으로 선택됩니다.

   - **다음 목록의 취약점만 수정**

     목록에서 수동으로 선택하는 취약점만 수정합니다. 이 목록에는 탐지된 모든 취약점이 포함되어 있습니다.

     예를 들어 테스트 환경에서 수정을 확인하거나 중요한 애플리케이션 또는 특정 애플리케이션의 취약점만 수정하려는 등의 경우 특정 취약점을 선택할 수 있습니다.

6. **이름** 페이지에서 추가할 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 **설정** 섹션에서 나중에 이 이름을 변경할 수 있습니다.

규칙 생성 마법사의 작업이 완료되면 새 작업 마법사의 규칙 목록 또는 작업 속성에 새 규칙이 추가되고 표시됩니다.

Windows Update 업데이트에 대한 새 규칙을 추가하려면 다음 단계를 따릅니다.

1. **추가** 버튼을 누릅니다.

   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

2. **규칙 유형** 페이지에서 **Windows 업데이트 규칙**을 선택합니다.

3. **일반 기준** 페이지에서 다음 설정을 지정합니다:

   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.

     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

- **다음 심각도와 같거나 높은 취약점만 수정**

  소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

  이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

  이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **다음 MSRC 심각도와 같거나 높은 취약점만 수정**

  소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

  이 옵션을 활성화하면 업데이트는 MSRC(Microsoft Security Response Center)에서 설정한 심각도가 목록에서 선택한 값(**낮음**, **중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

  이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

4. **애플리케이션** 페이지에서 업데이트를 설치할 애플리케이션 및 애플리케이션 버전을 선택합니다. 기본적으로 모든 애플리케이션이 선택되어 있습니다.

5. **업데이트 카테고리** 페이지에서 설치할 업데이트의 카테고리를 선택합니다. 이러한 카테고리는 Microsoft 업데이트 카탈로그의 카테고리와 동일합니다. 기본적으로 모든 카테고리가 선택되어 있습니다.

6. **이름** 페이지에서 추가할 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 **설정** 섹션에서 나중에 이 이름을 변경할 수 있습니다.

규칙 생성 마법사의 작업이 완료되면 새 작업 마법사의 규칙 목록 또는 작업 속성에 새 규칙이 추가되고 표시됩니다.

타사 애플리케이션의 업데이트를 위한 새 규칙을 추가하려면 다음 단계를 따릅니다.

1. **추가** 버튼을 누릅니다.

   규칙 생성 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

2. **규칙 유형** 페이지에서 **타사 업데이트 규칙**을 선택합니다.

3. **일반 기준** 페이지에서 다음 설정을 지정합니다:

   - **설치할 업데이트 세트**

     클라이언트 기기에 설치해야 하는 업데이트를 선택하십시오.

     - **승인된 업데이트만 설치**. 이 옵션을 선택하면 승인된 업데이트만 설치됩니다.
     - **모든 업데이트 설치(거부된 것 제외)**. 이 옵션을 선택하면 승인 상태가 *승인됨* 또는 *정의 안 됨*인 업데이트가 설치됩니다.
     - **모든 업데이트 설치(거부된 것 포함)**. 이 옵션을 선택하면 승인 상태에 관계없이 모든 업데이트가 설치됩니다. 이 옵션을 선택할 때는 주의하십시오. 예를 들어 테스트 인프라에서 거부된 일부 업데이트의 설치를 확인하려는 경우 이 옵션을 사용하십시오.

   - **다음 심각도와 같거나 높은 취약점만 수정**

     소프트웨어 업데이트를 설치하면 소프트웨어 사용 환경의 성능이 저하될 수 있습니다. 이러한 경우에는 소프트웨어 작동에 반드시 필요한 업데이트만 설치하고 다른 업데이트는 건너뛸 수 있습니다.

     이 옵션을 활성화하면 업데이트는 Kaspersky에서 설정한 심각도가 목록에서 선택한 값(**중간**, **높음** 또는 **심각**) 이상인 취약점만 수정합니다. 심각도가 선택한 값보다 낮은 취약점은 수정되지 않습니다.

     이 옵션을 비활성화하면 업데이트가 심각도에 관계없이 모든 취약점을 수정합니다.

     기본적으로 이 옵션은 비활성화되어 있습니다.

4. **애플리케이션** 페이지에서 업데이트를 설치할 애플리케이션 및 애플리케이션 버전을 선택합니다. 기본적으로 모든 애플리케이션이 선택되어 있습니다.

5. **이름** 페이지에서 추가할 규칙의 이름을 지정합니다. 생성된 작업 속성 창의 설정 섹션에서 나중에 이 이름을 변경할 수 있습니다.

   규칙 생성 마법사의 작업이 완료되면 새 작업 마법사의 규칙 목록 또는 작업 속성에 새 규칙이 추가되고 표시됩니다.

타사 소프트웨어의 취약점에 사용자 수정 선택

취약점 해결 작업을 사용하려면 작업 설정에 나열된 타사 소프트웨어의 취약점을 수정하기 위한 소프트웨어 업데이트를 수동으로 지정해야 합니다. *취약점 해결* 작업에서는 Microsoft 소프트웨어에 권장 수정을 사용하고 타사 소프트웨어에 사용자 수정을 사용합니다. *사용자 수정*은 관리자가 설치를 위해 수동으로 지정하는 취약점을 수정하기 위한 소프트웨어 업데이트입니다.

타사 소프트웨어의 취약점에 대한 사용자 수정을 선택하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 취약점**으로 이동합니다.

   이 페이지에는 클라이언트 기기에서 감지된 소프트웨어 취약점 목록이 표시됩니다.

2. 소프트웨어 취약점 목록에서 사용자 수정을 지정할 소프트웨어 취약점 이름이 포함된 링크를 누릅니다.

   취약점 속성 창이 열립니다.

3. 왼쪽 창에서 **사용자 수정 또는 기타 수정** 섹션을 선택합니다.

   선택한 소프트웨어 취약점에 대한 사용자 수정 목록이 표시됩니다.

4. **추가**를 클릭합니다.

   사용 가능한 설치 패키지 목록이 표시됩니다. 표시되는 설치 패키지 목록은 **동작 → 저장소 → 설치 패키지** 목록에 해당합니다. 선택한 취약점에 대한 사용자 수정이 포함된 설치 패키지를 만들지 않았다면 새 패키지 마법사를 시작하여 패키지를 만들 수 있습니다.

5. 타사 소프트웨어의 취약점에 대한 사용자 수정이 포함된 설치 패키지를 선택합니다.

6. **저장**을 누릅니다.

   소프트웨어 취약점에 대한 사용자 수정이 포함된 설치 패키지가 지정됩니다. *취약점 해결* 작업이 시작되면 설치 패키지가 설치되고 소프트웨어 취약점이 수정됩니다.

관리 중인 모든 기기에서 감지된 소프트웨어 취약점에 대한 정보 보기

관리 중인 기기에서 취약점에 대해 소프트웨어를 검사한 후에는 관리 중인 모든 기기에서 감지된 소프트웨어 취약점 목록을 확인할 수 있습니다. 중앙 관리 서버 계층에 대한 작업을 실행하면 선택한 중앙 관리 서버에서만 탐지된 취약점이 있는 관리 중인 기기의 목록을 확인할 수 있습니다.

관리 중인 모든 기기에서 감지된 소프트웨어 취약점 목록을 보려면 다음 단계를 따릅니다.

메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 취약점**으로 이동합니다.

이 페이지에는 클라이언트 기기에서 감지된 소프트웨어 취약점 목록이 표시됩니다.

취약점 리포트도 생성하고 확인할 수 있습니다.

필터를 지정하여 소프트웨어 취약점 목록을 확인할 수 있습니다. 소프트웨어 취약점 목록 오른쪽 상단에서 **필터** 아이콘()을 눌러 필터를 관리합니다. 소프트웨어 취약점 목록 위의 **필터 사전 설정** 드롭다운 목록에서 사전 설정된 필터 중 하나를 선택해도 됩니다.

목록에서 취약점에 대한 자세한 정보를 얻을 수 있습니다.

소프트웨어 취약점에 대한 정보를 얻으려면 다음 단계를 따릅니다.

소프트웨어 취약점 목록에서 취약점 이름이 포함된 링크를 누릅니다.

소프트웨어 취약점의 속성 창이 열립니다.

선택된 관리 중인 기기에서 감지된 소프트웨어 취약점에 대한 정보 보기

Windows를 실행하는 선택된 관리 중인 기기에서 감지된 소프트웨어 취약점에 대한 정보를 볼 수 있습니다.

선택한 관리 중인 기기에서 탐지된 소프트웨어 취약점 목록을 보려면:

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
   관리 중인 기기 목록이 표시됩니다.

2. 관리 중인 기기 목록에서 보호되는 소프트웨어 취약점을 보려는 기기 이름이 포함된 링크를 누릅니다.
   선택한 기기의 속성 창이 표시됩니다.

3. 선택한 기기의 속성 창에서 **고급** 탭을 선택합니다.

4. 좌측 창에서 **소프트웨어 취약점** 섹션을 선택합니다.

   선택한 관리 중인 기기에서 감지된 소프트웨어 취약점 목록이 표시됩니다.

선택한 소프트웨어 취약점 속성을 보려면 다음 단계를 따릅니다.

소프트웨어 취약점 목록에서 소프트웨어 취약점 이름이 포함된 링크를 누릅니다.

선택한 소프트웨어 취약점 속성 창이 표시됩니다.

관리 중인 기기의 취약점 통계 보기

관리 중인 기기의 각 소프트웨어 취약점에 대한 통계를 볼 수 있습니다. 통계는 다이어그램으로 표시됩니다. 다이어그램에는 다음과 같은 상태와 함께 기기의 수가 표시됩니다:

- *무시: <기기의 수>.* 이 상태는 취약점 속성에서 취약점을 무시하는 옵션을 직접 설정했을 때 할당됩니다.
- *수정: <기기의 수>.* 이 상태는 취약점 수정 작업이 성공적으로 완료되었을 때만 할당됩니다.
- *수정 스케줄 지정: <기기의 수>.* 이 상태는 취약점을 수정하기 위한 작업을 만들었지만 아직 작업이 수행되지 않았을 때 할당됩니다.
- *패치 적용: <기기의 수>.* 이 상태는 취약점 수정을 위한 소프트웨어 업데이트를 수동으로 선택했지만 이 소프트웨어 업데이트로 취약점을 수정하지 못했을 때 할당됩니다.
- *수정 필요: <기기의 수>.* 이 상태는 취약점이 관리 중인 기기 중 일부에서만 수정되었으며, 관리 중인 다른 기기에서도 취약점을 수정해야 할 때 할당됩니다.

관리 중인 기기의 취약점 통계를 보려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 취약점**으로 이동합니다.
   이 페이지에는 관리 중인 기기에서 탐지된 애플리케이션의 취약점의 목록이 표시됩니다.

2. 필수 취약점 옆에 있는 확인란을 선택합니다.

3. **기기의 취약점 통계** 버튼을 누릅니다.

   취약점 상태 다이어그램이 표시됩니다. 상태를 클릭하면 선택한 상태의 취약점이 있는 기기의 목록이 열립니다.

소프트웨어 취약점 목록을 텍스트 파일로 내보내기

표시된 취약점 목록을 CSV 또는 TXT 파일로 내보낼 수 있습니다. 예를 들어 정보 보안 관리자에게 보내거나 통계 목적으로 저장하는 데 이러한 파일을 사용할 수 있습니다.

모든 관리 중인 기기에서 감지된 소프트웨어 취약점 목록을 텍스트 파일로 내보내려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 취약점**으로 이동합니다.
   이 페이지에는 관리 중인 기기에서 탐지된 애플리케이션의 취약점의 목록이 표시됩니다.
2. 선호하는 내보내기 형식에 따라 **TXT로 내보내기** 또는 **CSV로 내보내기** 버튼을 누릅니다.

소프트웨어 취약점 목록이 포함된 파일이 현재 사용 중인 기기에 다운로드됩니다.

선택한 관리 중인 기기에서 감지된 소프트웨어 취약점 목록을 텍스트 파일로 내보내려면 다음 단계를 따릅니다.

1. 선택한 관리 중인 기기에서 감지된 소프트웨어 취약점 목록을 엽니다.
2. 내보낼 소프트웨어 취약점을 선택합니다.
   관리 중인 기기에서 감지된 소프트웨어 취약점의 전체 목록을 내보내려면 이 단계를 건너뜁니다.
   관리 중인 기기에서 감지된 소프트웨어 취약점의 전체 목록을 내보내려 하면 현재 페이지에 표시된 취약점만 내보내집니다.
3. 선호하는 내보내기 형식에 따라 **TXT로 내보내기** 또는 **CSV로 내보내기** 버튼을 누릅니다.

선택한 관리 중인 기기에서 감지된 소프트웨어 취약점 목록이 포함된 파일이 현재 사용 중인 기기에 다운로드됩니다.

소프트웨어 취약점 무시

수정할 소프트웨어 취약점을 무시할 수 있습니다. 소프트웨어 취약점을 무시하는 이유는 다음과 같은 것이 있을 수 있습니다:

- 해당 소프트웨어 취약점이 조직에 치명적이라고 생각하지 않습니다.
- 소프트웨어 취약점 수정이 취약점 수정이 필요한 소프트웨어와 관련된 데이터를 손상시킬 수 있다는 것을 이해합니다.
- 다른 방법을 사용하여 관리 중인 기기를 보호하기 때문에 소프트웨어 취약점이 조직의 네트워크에 위험하지 않다고 확신합니다.

모든 관리 중인 기기나 선택한 관리 중인 기기에서 소프트웨어 취약점을 무시할 수 있습니다.

모든 관리 중인 기기에서 소프트웨어 취약점을 무시하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 패치 관리 → 소프트웨어 취약점**으로 이동합니다.
   이 페이지에는 관리 중인 기기에서 감지된 소프트웨어 취약점 목록이 표시됩니다.
2. 소프트웨어 취약점 목록에서 무시할 소프트웨어 취약점 이름이 포함된 링크를 누릅니다.
   소프트웨어 취약점 속성 창이 열립니다.
3. **일반** 탭에서 **취약점 무시** 옵션을 활성화합니다.
4. **저장** 버튼을 누릅니다.
   소프트웨어 취약점 속성 창이 닫힙니다.

모든 관리 중인 기기에서 소프트웨어 취약점이 무시됩니다.

선택한 관리 중인 기기에서 소프트웨어 취약점을 무시하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
   관리 중인 기기 목록이 표시됩니다.
2. 관리 중인 기기 목록에서 소프트웨어 취약점을 무시할 기기 이름이 포함된 링크를 누릅니다.
   기기 속성 창이 열립니다.
3. 기기 속성 창에서 **고급** 탭을 선택합니다.
4. 좌측 창에서 **소프트웨어 취약점** 섹션을 선택합니다.
   기기에서 감지된 소프트웨어 취약점 목록이 표시됩니다.
5. 소프트웨어 취약점 목록에 선택한 기기에서 무시할 취약점을 선택합니다.
   소프트웨어 취약점 속성 창이 열립니다.
6. 소프트웨어 취약점 속성 창의 **일반** 탭에서 **취약점 무시** 옵션을 활성화합니다.
7. **저장** 버튼을 누릅니다.
   소프트웨어 취약점 속성 창이 닫힙니다.
8. 기기 속성 창을 닫습니다.

선택한 기기에서 소프트웨어 취약점이 무시됩니다.

무시한 소프트웨어 취약점은 *취약점 해결* 작업 또는 *취약점 관련 업데이트를 설치하고 취약점 수정* 작업을 완료한 후에 수정되지 않습니다. 취약점 목록에서 필터를 사용하여 무시한 소프트웨어 취약점을 제외할 수 있습니다.

클라이언트 기기에서 실행되는 애플리케이션 관리

이 섹션에서는 클라이언트 기기에서 실행되는 애플리케이션 관리와 관련된 Kaspersky Security Center의 기능을 설명합니다.

애플리케이션 제어로 실행 파일 관리

애플리케이션 제어 구성 요소를 사용하여 사용자 기기에서 실행 파일의 시작을 허용하거나 차단할 수 있습니다. 애플리케이션 제어 구성 요소는 Windows 기반 및 Linux 기반 운영 체제를 지원합니다.

Linux 기반 운영 체제는 Kaspersky Endpoint Security 11.2 for Linux부터 애플리케이션 제어 구성 요소를 사용할 수 있습니다. 또한 이 구성 요소는 Kaspersky Embedded Systems Security for Windows 3.0 이상에서도 사용할 수 있습니다.

필수 구성 요소

- 조직에 Kaspersky Security Center가 배포되어 있습니다.
- Kaspersky Endpoint Security for Windows 또는 Kaspersky Endpoint Security for Linux의 정책이 생성되고 활성화됩니다.
- Kaspersky Embedded Systems Security for Windows 또는 Kaspersky Embedded Systems Security for Linux 정책이 생성되어 활성 상태입니다.

단계

애플리케이션 제어 사용 시나리오는 다음과 같은 단계로 진행됩니다.

1. **클라이언트 기기에서 실행 파일 목록 구성 및 보기**

   이 단계는 관리 중인 기기에서 찾을 수 있는 실행 파일을 파악하는 데 도움이 됩니다. 실행 파일 목록을 보고 허용 및 금지되는 실행 파일 목록과 비교합니다. 실행 파일 사용에 관한 제한은 조직의 정보 보안 정책과 관련될 수 있습니다.

   방법 지침:

   - 관리 콘솔: 실행 파일 인벤토리
   - Kaspersky Security Center 웹 콘솔: 클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기

2. **조직에서 사용되는 실행 파일 카테고리 생성**

   관리 중인 기기에 저장된 실행 파일 목록을 분석합니다. 분석 결과를 바탕으로 실행 파일에 대한 카테고리를 생성합니다. 조직에서 사용하는 표준 실행 파일 집합을 포괄하는 "업무용 애플리케이션" 카테고리를 만드는 것이 좋습니다. 다양한 보안 그룹이 업무에 자체 실행 파일 집합을 사용한다면 보안 그룹마다 별도의 카테고리를 만들 수 있습니다.

   방법 지침:

   - 관리 콘솔: 콘텐츠가 수동으로 추가된 애플리케이션 카테고리 생성, 선택한 기기의 실행 파일을 포함한 애플리케이션 카테고리 생성, 특정 폴더의 실행 파일을 포함한 애플리케이션 카테고리 생성.
   - Kaspersky Security Center 웹 콘솔: 콘텐츠가 수동으로 추가된 애플리케이션 카테고리 생성, 선택한 기기의 실행 파일을 포함한 애플리케이션 카테고리 생성, 특정 폴더의 실행 파일을 포함한 애플리케이션 카테고리 생성.

3. **Kaspersky Endpoint Security 정책에서 애플리케이션 제어 구성**

   이전 단계에서 만든 카테고리를 사용하여 Kaspersky Endpoint Security 정책의 애플리케이션 제어 구성 요소를 구성합니다.

   방법 지침:

   - 관리 콘솔: 클라이언트 기기의 애플리케이션 시작 관리 구성
   - Kaspersky Security Center 웹 콘솔: Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성

4. **Kaspersky Embedded Systems Security 애플리케이션 정책에서 애플리케이션 제어 구성**

   생성한 카테고리를 사용하여 Kaspersky Embedded Systems Security for Windows 정책에서 애플리케이션 제어 구성 요소를 구성합니다. 애플리케이션 제어 구성 요소에 관한 자세한 내용은 Kaspersky Embedded Systems Security for Windows 도움말 이나 Kaspersky Embedded Systems Security for Linux 도움말 을 참조하십시오.

사용하는 규칙의 수가 많으면 정책을 불러올 때 오류가 발생할 수 있습니다. 다음 명령을 사용하여 최대 요청 크기를 바이트 단위로 늘릴 수 있습니다.

- JSON 요청:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
  ```

- HTTP 요청:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  여기서 `<max_request_size>`는 요청의 최대 바이트 크기입니다(예: `200000000`).

5. **테스트 모드에서 애플리케이션 제어 구성 요소 사용 설정**

   애플리케이션 제어 규칙으로 사용자의 업무에 필요한 실행 파일이 차단되지 않도록 하려면 애플리케이션 제어 규칙에 대한 테스트를 활성화하고 새 규칙 생성 이후 작업을 분석해 보는 것이 좋습니다. 테스트가 활성화되면 Kaspersky Endpoint Security for Windows나 Kaspersky Embedded Systems Security는 애플리케이션 제어 규칙으로 시작이 금지된 실행 파일을 차단하는 대신 중앙 관리 서버에 시작에 관한 알림을 전송합니다.

   애플리케이션 제어 규칙을 테스트할 때 다음 작업을 수행하는 것이 좋습니다.

   - 테스트 기간을 결정합니다. 테스트 기간은 며칠부터 두 달까지 다양합니다.
   - 애플리케이션 제어 동작의 테스트 결과 이벤트를 살펴봅니다.

   Kaspersky Security Center 웹 콘솔 사용 지침: Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성 요소 구성. 이 지침에 따라 구성 프로세스에서 **테스트 모드** 옵션을 활성화합니다.

6. **애플리케이션 제어 구성 요소의 카테고리 설정 변경**

   필요한 경우 애플리케이션 제어 설정을 변경합니다. 테스트 결과를 바탕으로 애플리케이션 제어 구성 요소 이벤트와 관련된 실행 파일을 컨텐츠가 수동으로 추가된 카테고리에 추가할 수 있습니다.

   방법 지침:

   - 관리 콘솔: 애플리케이션 카테고리에 이벤트 관련 실행 파일 추가
   - Kaspersky Security Center 웹 콘솔: 애플리케이션 카테고리에 이벤트 관련 실행 파일 추가

7. **동작 모드인 애플리케이션 제어 규칙 적용**

   애플리케이션 규칙을 테스트하고 카테고리의 구성이 완료된 후에는 동작 모드인 애플리케이션 제어 규칙을 적용할 수 있습니다.

   Kaspersky Security Center 웹 콘솔 사용 지침: Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성 요소 구성. 이 지침에 따라 구성 프로세스에서 **테스트 모드** 옵션을 비활성화합니다.

8. **애플리케이션 제어 구성 확인**

   다음을 수행했는지 확인합니다.

   - 실행 파일에 대한 카테고리 생성.
   - 카테고리로 애플리케이션 제어 구성.
   - 동작 모드인 애플리케이션 제어 규칙 적용.

결과

시나리오가 완료되면 관리 중인 기기에서 실행 파일 시작이 제어됩니다. 사용자는 조직에서 허용한 사용 파일만 실행할 수 있으며 조직에서 금지한 실행 파일은 실행할 수 없습니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

애플리케이션 제어 모드 및 카테고리

애플리케이션 제어 구성 요소는 사용자의 실행 파일 시작 시도를 모니터링합니다. 애플리케이션 제어 규칙을 사용하여 실행 파일의 시작을 제어할 수 있습니다.

애플리케이션 제어 구성 요소는 Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security 11.2 for Linux 이상 버전 및 Kaspersky Security for Virtualization Light Agent에서 사용할 수 있습니다. 이 섹션의 모든 지침은 Kaspersky Endpoint Security for Windows의 애플리케이션 제어 구성에 대해 설명합니다.

설정이 애플리케이션 제어 규칙 중 하나와 일치하지 않는 실행 파일의 시작은 선택한 구성 요소 운영 모드로 규제됩니다.

- *거부 목록*. 이 모드는 차단 규칙에 지정된 실행 파일을 제외한 모든 실행파일의 시작을 허용할 때 사용합니다. 기본적으로 이 모드가 선택됩니다.
- *허용 목록*. 이 모드는 허용 규칙에 지정된 실행 파일을 제외한 모든 실행파일의 시작을 차단할 때 사용합니다.

애플리케이션 제어 규칙은 실행 파일에 대한 카테고리를 통해 구현됩니다. Kaspersky Security Center에는 다음과 같은 세 가지 유형의 카테고리가 있습니다.

- 수동으로 추가된 컨텐츠가 있는 카테고리. 카테고리에 실행 파일을 포함하도록 예를 들어 파일 메타데이터, 파일 해시 코드, 파일 인증서, KL 카테고리, 파일 경로와 같은 조건을 정의합니다.
- 선택한 기기의 실행 파일이 포함된 카테고리. 실행 파일이 카테고리에 자동으로 포함되는 기기를 지정합니다.
- 선택한 폴더의 실행 파일이 포함된 카테고리. 관리자는 선택한 카테고리에 포함할 실행 파일이 있는 폴더를 지정합니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent

- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기

다음 방법의 하나를 사용하여 클라이언트 기기에 저장된 실행 파일 목록을 얻을 수 있습니다.

- Kaspersky Endpoint Security 정책에서 애플리케이션 시작에 관한 알림 활성화.
- 인벤토리 작업 생성.

Kaspersky Endpoint Security 정책에서 애플리케이션 시작에 관한 알림 활성화

애플리케이션 시작에 대한 알림을 활성화하려면 다음을 수행합니다.

1. Kaspersky Endpoint Security 정책 설정을 열고 **일반 설정** → **리포트 및 저장소**로 갑니다.
2. **중앙 관리 서버로의 데이터 전송** 설정 그룹에서 **시작된 애플리케이션 정보** 확인란을 선택하고 변경 사항을 저장합니다.

   사용자가 실행 파일을 시작하려고 하면 해당 파일에 대한 정보가 클라이언트 기기의 실행 파일 목록에 추가됩니다. Kaspersky Endpoint Security는 이 정보를 네트워크 에이전트로 전송하고, 네트워크 에이전트는 이를 중앙 관리 서버로 전송합니다.

인벤토리 작업 생성

실행 파일 인벤토리 기능은 다음 애플리케이션에서 사용할 수 있습니다:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux 버전 11.2 이상
- Kaspersky Security for Virtualization 4.0 Light Agent 및 이후 버전

설치된 애플리케이션에 대한 정보를 얻으면서 데이터베이스의 부하를 줄일 수 있습니다. 데이터베이스 공간을 절약하려면 표준 소프트웨어 집합이 설치된 참조 기기에서 인벤토리 작업을 실행하는 것이 좋습니다. 권장 수는 1~3개입니다.

> 다음 데이터베이스를 사용한다면 인벤토리 작업을 실행하지 않는 것이 좋습니다: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB(모든 버전).

클라이언트 기기에 있는 실행 파일에 대한 인벤토리 작업을 만들려면:

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**로 이동합니다.
   작업 목록이 표시됩니다.
2. **추가** 버튼을 누릅니다.
   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.

3. **새 작업 설정** 페이지의 **애플리케이션** 드롭다운 목록에서 클라이언트 기기의 운영 체제 유형에 따라 Kaspersky Endpoint Security for Windows 또는 Kaspersky Endpoint Security for Linux를 선택합니다.

4. **작업 유형** 드롭다운 목록에서 **인벤토리**를 선택합니다.

5. **작업 생성 마침** 페이지에서 **마침** 버튼을 클릭합니다.

새 작업 마법사를 종료한 후 **인벤토리** 작업이 생성 및 구성됩니다. 원한다면 생성된 작업에 대한 설정을 변경할 수 있습니다. 그러면 작업 목록에 새로 생성된 작업이 나타납니다.

인벤토리 작업에 대한 자세한 설명은 다음 도움말을 참조하십시오:

- Kaspersky Endpoint Security for Windows 도움말
- Kaspersky Endpoint Security for Linux 도움말
- Kaspersky Security for Virtualization Light Agent

인벤토리 작업을 수행한 후 관리 중인 기기에 저장된 실행 파일 목록이 형성되고 이 목록을 확인할 수 있습니다.

인벤토리 중에 다음 형식의 실행 파일을 탐지할 수 있습니다(인벤토리 작업 속성에서 선택한 옵션에 따라 다름): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, HTML.

관리 중인 기기에 저장된 실행 파일 목록 보기

클라이언트 기기에 저장된 실행 파일 목록을 보려면 다음 단계를 따릅니다.

메인 메뉴에서 **동작 → 타사 애플리케이션 → 실행 파일**로 이동합니다.

이 페이지에는 클라이언트 기기에 저장된 실행 파일 목록이 표시됩니다.

필요하다면 관리 중인 기기의 실행 파일을 Kaspersky Security Center 웹 콘솔이 열려 있는 기기로 보낼 수 있습니다.

실행 파일을 보내려면:

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 실행 파일**로 이동합니다.

2. 보내려는 실행 파일의 링크를 클릭합니다.

3. 창이 열리면 **기기** 섹션으로 가서 실행 파일을 보내고자 하는 관리 중인 기기의 확인란을 선택합니다.

   실행 파일을 보내기 전에 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택하여 관리 중인 기기가 중앙 관리 서버에 직접 연결되어 있는지 확인합니다.

4. **보내기** 버튼을 클릭합니다.

Kaspersky Security Center 웹 콘솔이 열려 있는 기기로 전송할 수 있도록, 선택한 실행 파일이 다운로드됩니다.

컨텐츠가 수동으로 추가된 애플리케이션 카테고리 만들기

조직에서 시작을 허용 또는 차단할 실행 파일의 템플릿으로 기준 집합을 지정할 수 있습니다. 기준에 해당하는 실행 파일을 바탕으로 애플리케이션 카테고리를 만들고 애플리케이션 제어 구성 요소 구성에 사용할 수 있습니다.

수동으로 추가된 컨텐츠가 있는 애플리케이션 카테고리를 만들려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 애플리케이션 카테고리**로 이동합니다.
   애플리케이션 카테고리 목록이 있는 페이지가 표시됩니다.

2. **추가** 버튼을 누릅니다.
   새 카테고리 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

3. 마법사의 **카테고리 생성 방법 선택** 단계에서 **수동으로 추가된 콘텐츠가 있는 카테고리. 실행 파일의 데이터를 수동으로 카테고리에 추가합니다** 옵션을 선택합니다.

4. **조건** 단계에서 **추가** 버튼을 눌러 카테고리 생성 시 포함할 조건 기준을 추가합니다.

5. **조건 기준** 단계의 목록에서 카테고리 생성에 대한 규칙 유형을 선택합니다.

   - **KL 카테고리에서**

     이 옵션을 선택하면 사용자 카테고리에 애플리케이션을 추가하는 조건으로 Kaspersky 애플리케이션 카테고리를 지정할 수 있습니다. 그러면 지정된 Kaspersky 카테고리의 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

   - **저장소에서 인증서 선택**

     이 옵션을 선택하면 저장소에서 인증서를 지정할 수 있습니다. 카테고리 조건은 지정된 인증서로 서명된 실행 파일에만 적용됩니다.

     인벤토리 작업을 생성 및 시작하거나 Kaspersky Endpoint Security 정책의 **시작된 애플리케이션 정보** 체크박스를 선택하면 저장소에 인증서가 추가됩니다. 두 작업을 모두 수행할 수 있습니다.

   - **애플리케이션 경로 지정(마스크 지원)**

     이 옵션을 선택하면 사용자 애플리케이션 카테고리에 추가할 실행 파일이 포함된 파일 경로 또는 폴더 경로를 클라이언트 기기에서 지정할 수 있습니다. *C:\path_to_exe**와 같은 정규식을 사용할 수 있습니다(예: *C:\Program Files\Internet Explorer**).

   - **이동식 드라이브**

     이 옵션을 선택하면 애플리케이션이 실행되는 미디어(모든 드라이브 또는 이동식 드라이브) 유형을 지정할 수 있습니다. 선택한 드라이브 유형에서 실행된 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

- **해시, 메타데이터 또는 인증서**:
  - **실행 파일 목록에서 선택**

    이 옵션을 선택하면 클라이언트 기기의 실행 파일 목록을 사용하여 실행 파일을 선택하고 애플리케이션을 카테고리에 추가할 수 있습니다.

  - **자산 관리(소프트웨어)에서 선택**

    이 옵션을 선택하면 자산 관리(소프트웨어)가 표시됩니다. 레지스트리에서 애플리케이션을 선택하면 선택한 애플리케이션의 다음과 같은 메타데이터가 입력된 파라미터 창이 열립니다.

    - 파일 이름.
    - 파일 버전. 버전의 정확한 값을 지정하거나 '5.0 이상'과 같이 조건을 설명할 수 있습니다.
    - 애플리케이션 이름.
    - 애플리케이션 버전. 버전의 정확한 값을 지정하거나 '5.0 이상'과 같이 조건을 설명할 수 있습니다.
    - 공급업체.

    지정된 파라미터 조건을 충족하는 실행 파일의 실행만 차단되며, 선택한 애플리케이션의 실행은 차단되지 않습니다. 선택한 애플리케이션의 메타데이터가 애플리케이션을 실행할 때 시작되는 실행 파일의 메타데이터와 일치하면 다음 단계로 진행할 수 있습니다. 그렇지 않으면 실행 파일의 메타데이터와 일치하도록 값을 직접 변경해야 합니다.

  - **수동 지정**

    이 옵션을 선택하면 사용자 카테고리에 애플리케이션을 추가하는 조건으로 파일 해시, 메타데이터 또는 인증서를 지정해야 합니다.

    파일 해시

    네트워크의 기기에 설치된 보안 제품 버전에 따라 이 카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산용 알고리즘을 선택해야 합니다. 해시 함수로 계산된 해시 값에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다.

    SHA256은 암호화 해시 함수입니다. 해당 알고리즘에서 발견된 취약점이 없으므로 최근까지 가장 믿을 수 있는 암호화 함수로 간주되고 있습니다. SHA256 계산은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원됩니다. MD5 해시 계산 기능은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전의 모든 버전에서 지원됩니다.

카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산의 옵션 선택합니다:

- 네트워크에 설치된 보안 애플리케이션의 모든 인스턴스가 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이상일 시, **SHA256** 확인란을 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전인 경우 실행 파일의 SHA256 해시 기준에 따라 만든 카테고리를 추가하지 않는 것이 좋습니다. 이러한 카테고리를 추가하면 보안 제품 작동 시에 오류가 발생할 수 있습니다. 이 경우 카테고리의 파일에 대해 MD5 암호화 해시 함수를 사용할 수 있습니다.

- Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전이 네트워크에 설치되었다면 **MD5 해시**를 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서는 실행 파일의 MD5 체크섬 기준을 기반으로 만든 카테고리를 추가할 수 없습니다. 이 경우 카테고리의 파일에 대해 SHA256암호화 해시 함수를 사용할 수 있습니다.

- 네트워크의 다른 기기가 Kaspersky Endpoint Security 10의 이전 버전과 이후 버전을 모두 사용한다면 **SHA256** 확인란과 **MD5 해시** 확인란을 모두 선택합니다.

메타데이터

이 옵션을 선택하면 파일 메타 데이터를 파일 이름, 파일 버전, 공급업체로 지정할 수 있습니다. 카테고리 조건은 메타데이터가 같은 실행 파일에만 적용됩니다.

인증서

이 옵션을 선택하면 저장소에서 인증서를 지정할 수 있습니다. 카테고리 조건은 지정된 인증서로 서명된 실행 파일에만 적용됩니다.

인벤토리 작업을 생성 및 시작하거나 Kaspersky Endpoint Security 정책의 **시작된 애플리케이션 정보** 체크박스를 선택하면 저장소에 인증서가 추가됩니다. 두 작업을 모두 수행할 수 있습니다.

- **파일 또는 MSI 패키지/압축된 폴더에서**

  이 옵션을 선택하면 사용자 카테고리에 애플리케이션을 추가하는 조건으로 MSI 설치 파일을 지정할 수 있습니다. 그러면 애플리케이션 설치 파일 메타데이터가 중앙 관리 서버로 전송됩니다. 지정된 MSI 설치 파일과 동일한 설치 파일 메타데이터를 가진 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

선택한 기준이 조건 목록에 추가됩니다.

애플리케이션 카테고리 생성에 필요한 만큼의 기준을 추가할 수 있습니다.

6. **예외** 단계에서 **추가** 버튼을 눌러 생성 중인 카테고리에서 제외할 배타적 조건 기준을 추가합니다.

7. 카테고리 생성 시 규칙 유형을 선택한 것과 같은 방식으로 **조건 기준** 단계의 목록에서 규칙 유형을 선택합니다.

마법사가 완료되면 애플리케이션 카테고리가 생성됩니다. 애플리케이션 카테고리 목록에 표시됩니다. 애플리케이션 제어를 구성할 때 생성된 애플리케이션 카테고리를 사용할 수 있습니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

선택한 장치의 실행 파일을 포함하는 애플리케이션 카테고리 만들기

선택한 기기의 실행 파일을 허용하거나 차단할 실행 파일의 템플릿으로 사용할 수 있습니다. 선택한 기기의 실행 파일을 기반으로 카테고리를 만들고 애플리케이션 제어 구성 요소 구성에서 사용할 수 있습니다.

기기에서 실행 파일 목록을 가져오려면 다음을 따릅니다.

1. Kaspersky Endpoint Security for Windows 또는 Kaspersky Endpoint Security for Linux의 정책이 생성되고 활성화되도록 해야 합니다. 정책에서 애플리케이션 제어 구성 요소를 활성화합니다.
2. 클라이언트 기기에 저장된 실행 파일 목록을 확보합니다.

선택한 기기의 실행 파일을 포함하는 카테고리를 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 애플리케이션 카테고리**로 이동합니다.
   애플리케이션 카테고리 목록이 있는 페이지가 표시됩니다.
2. **추가** 버튼을 누릅니다.
   새 카테고리 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. **카테고리 생성 방법 선택** 단계에서 카테고리 이름을 지정하고 **선택한 기기의 실행 파일을 포함한 카테고리. 이러한 실행 파일은 자동으로 처리되며 해당 카테고리에 그 메트릭이 추가됩니다** 옵션을 선택합니다.
4. **추가**를 누릅니다.
5. 창이 열리면 기기 또는 카테고리를 만드는 데 사용할 실행 파일의 기기를 선택합니다.
6. 다음 설정을 지정합니다:
   - **해시 값 계산 알고리즘**

     네트워크의 기기에 설치된 보안 제품 버전에 따라 이 카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산용 알고리즘을 선택해야 합니다. 해시 함수로 계산된 해시 값에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다.

     SHA256은 암호화 해시 함수입니다. 해당 알고리즘에서 발견된 취약점이 없으므로 최근까지 가장 믿을 수 있는 암호화 함수로 간주되고 있습니다. SHA256 계산은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원됩니다. MD5 해시 계산 기능은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전의 모든 버전에서 지원됩니다.

     카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산의 옵션 선택합니다:

     - 네트워크에 설치된 보안 애플리케이션의 모든 인스턴스가 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이상일 시, **SHA256** 확인란을 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전인 경우 실행 파일의 SHA256 해시 기준에 따라 만든 카테고리를 추가하지 않는 것이 좋습니다. 이러한 카테고리를 추가하면 보안 제품 작동 시에 오류가 발생할 수 있습니다. 이 경우 카테고리의 파일에 대해 MD5 암호화 해시 함수를 사용할 수 있습니다.
     - Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전이 네트워크에 설치되었다면 **MD5 해시**를 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서는 실행 파일의 MD5 체크섬 기준을 기반으로 만든 카테고리를 추가할 수 없습니다. 이 경우 카테고리의 파일에 대해 SHA256암호화 해시 함수를 사용할 수 있습니다.

     네트워크의 다른 기기가 Kaspersky Endpoint Security 10의 이전 버전과 이후 버전을 모두 사용한다면 **SHA256** 확인란과 **MD5 해시** 확인란을 모두 선택합니다.

이 카테고리에 있는 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원) 확인란은 기본적으로 선택되어 있습니다.

이 카테고리에 있는 파일에 대해 MD5 계산 (Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전에서 지원) 확인란은 기본적으로 선택되어 있지 않습니다.

- **중앙 관리 서버 저장소와 데이터 동기화**

  중앙 관리 서버에서 지정된 폴더의 변경 사항을 주기적으로 확인하도록 하려면 이 옵션을 선택합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

  이 옵션을 활성화할 경우 지정된 폴더의 변경 사항을 확인할 기간(시간 단위)을 지정합니다. 기본적으로 검사 간격은 24시간입니다.

- **파일 유형**

  이 섹션에서는 애플리케이션 카테고리를 만드는 데 사용되는 파일 형식을 지정할 수 있습니다.

  모든 파일. 카테고리를 만들 때 모든 파일을 고려합니다. 기본적으로 이 옵션은 선택되어 있습니다.

  애플리케이션 카테고리 이외의 파일만. 카테고리를 만들 때 애플리케이션 카테고리 외부의 파일만 고려합니다.

- **폴더**

  이 섹션에서는 선택된 기기의 폴더 중 애플리케이션 카테고리를 만드는 데 사용할 파일이 포함되어 있는 폴더를 지정할 수 있습니다.

  모든 폴더. 카테고리 생성 시 모든 폴더를 고려합니다. 기본적으로 이 옵션은 선택되어 있습니다.

  지정한 폴더. 카테고리 생성 시 지정된 폴더만 고려합니다. 이 옵션을 선택하면 폴더 경로를 지정해야 합니다.

마법사가 완료되면 실행 파일 카테고리가 생성됩니다. 카테고리 목록에 표시됩니다. 애플리케이션 제어를 구성할 때 생성된 카테고리를 사용할 수 있습니다.

선택한 폴더의 실행 파일을 포함하는 애플리케이션 카테고리 만들기

선택한 폴더의 실행 파일을 조직에서 허용 또는 차단할 실행 파일의 표준으로 사용할 수 있습니다. 선택한 폴더의 실행 파일을 기준으로 애플리케이션 제어 구성 요소 구성에서 애플리케이션 카테고리를 만들고 사용할 수 있습니다.

선택한 폴더에서 실행 파일을 포함하는 카테고리를 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 애플리케이션 카테고리**로 이동합니다.

   애플리케이션 카테고리 목록이 있는 페이지가 표시됩니다.

2. **추가** 버튼을 누릅니다.

   새 카테고리 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

3. **카테고리 생성 방법 선택** 단계에서 카테고리 이름을 지정하고 **지정한 폴더의 실행 파일을 포함하는 카테고리. 지정한 폴더에 복사된 애플리케이션 실행 파일을 자동으로 처리하며, 해당 정보는 카테고리에 추가됩니다** 옵션을 선택합니다.

4. 실행 파일이 카테고리 생성에 사용되는 폴더를 지정합니다.

5. 다음 설정을 정의합니다:

- **이 카테고리에 동적 링크 라이브러리(DLL) 포함**

  애플리케이션 카테고리에 동적-링크 라이브러리(DLL 형식의 파일)이 포함되고 시스템에서 실행 중인 이러한 라이브러리의 동작을 애플리케이션 제어 구성 요소가 기록합니다. 카테고리에 DLL 파일이 포함되면 Kaspersky Security Center의 성능이 저하될 수 있습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **이 카테고리에 스크립트 데이터 포함**

  애플리케이션 카테고리에 스크립트 데이터가 포함되며 웹 위협 보호 구성 요소에서 스크립트를 차단하지 않습니다. 카테고리에 스크립트 데이터가 포함되면 Kaspersky Security Center의 성능이 저하될 수 있습니다.

  기본적으로 이 확인란은 선택되어 있지 않습니다.

- **해시 값 계산 알고리즘**: **이 카테고리의 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원) / 이 카테고리의 파일에 대해 MD5 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 서비스 팩 2 이전 버전에서 지원)**

  네트워크의 기기에 설치된 보안 제품 버전에 따라 이 카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산용 알고리즘을 선택해야 합니다. 해시 함수로 계산된 해시 값에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다.

  SHA256은 암호화 해시 함수입니다. 해당 알고리즘에서 발견된 취약점이 없으므로 최근까지 가장 믿을 수 있는 암호화 함수로 간주되고 있습니다. SHA256 계산은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원됩니다. MD5 해시 계산 기능은 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전의 모든 버전에서 지원됩니다.

  카테고리의 파일에 대해 Kaspersky Security Center에서 수행하는 해시 값 계산의 옵션 선택합니다:

  - 네트워크에 설치된 보안 애플리케이션의 모든 인스턴스가 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이상일 시, **SHA256** 확인란을 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전인 경우 실행 파일의 SHA256 해시 기준에 따라 만든 카테고리를 추가하지 않는 것이 좋습니다. 이러한 카테고리를 추가하면 보안 제품 작동 시에 오류가 발생할 수 있습니다. 이 경우 카테고리의 파일에 대해 MD5 암호화 해시 함수를 사용할 수 있습니다.

  - Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전이 네트워크에 설치되었다면 **MD5 해시**를 선택합니다. Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서는 실행 파일의 MD5 체크섬 기준을 기반으로 만든 카테고리를 추가할 수 없습니다. 이 경우 카테고리의 파일에 대해 SHA256암호화 해시 함수를 사용할 수 있습니다.

  네트워크의 다른 기기가 Kaspersky Endpoint Security 10의 이전 버전과 이후 버전을 모두 사용한다면 **SHA256** 확인란과 **MD5 해시** 확인란을 모두 선택합니다.

  이 카테고리에 있는 파일에 대해 SHA256 계산(Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이후 버전에서 지원) 확인란은 기본적으로 선택되어 있습니다.

  이 카테고리에 있는 파일에 대해 MD5 계산 (Kaspersky Endpoint Security 10 Service Pack 2 for Windows 이전 버전에서 지원) 확인란은 기본적으로 선택되어 있지 않습니다.

- **폴더 내 변경 사항을 강제로 검사**

  이 옵션을 사용하면 애플리케이션이 정기적으로 폴더에 카테고리 컨텐츠 추가에 대한 변경 사항이 있는지 확인합니다. 확인란 옆에 있는 항목에서 확인 주기(시간)를 지정할 수 있습니다. 기본적으로 강제로 확인하는 시간 간격은 24시간입니다.

  이 옵션이 비활성화되어 있으면 애플리케이션이 해당 폴더에 대해 모든 확인을 강제로 시작하지 않습니다. 파일이 수정되거나 추가되거나 삭제되었다면 서버는 파일로의 접근을 시도합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

마법사가 완료되면 실행 파일 카테고리가 생성됩니다. 카테고리 목록에 표시됩니다. 애플리케이션 제어 구성에서 카테고리를 사용할 수 있습니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

애플리케이션 카테고리 목록 보기

구성된 실행 파일 카테고리 목록과 각 카테고리의 설정을 확인할 수 있습니다.

애플리케이션 카테고리의 목록을 확인하려면,

메인 메뉴에서 **동작 → 타사 애플리케이션 → 애플리케이션 카테고리**로 이동합니다.

애플리케이션 카테고리 목록이 있는 페이지가 표시됩니다.

애플리케이션 카테고리의 속성을 보려면

카테고리의 이름을 누릅니다.

카테고리의 속성 창이 표시됩니다. 속성은 여러 탭에 그룹화되어 있습니다.

애플리케이션 카테고리에 이벤트 관련 실행 파일 추가

Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어를 구성하면 이벤트 목록에 다음 이벤트가 표시됩니다.

- **애플리케이션 시작 금지됨**(*심각* 이벤트) 이 이벤트는 애플리케이션 제어가 규칙을 적용하도록 구성된 경우 표시됩니다.
- **테스트 모드에서 애플리케이션 시작 금지됨**(*정보* 이벤트) 이 이벤트는 애플리케이션 제어가 규칙을 테스트하도록 구성된 경우 표시됩니다.
- **애플리케이션 시작 금지에 관해 관리자에게 보내는 메시지**(*경고* 이벤트). 이 이벤트는 애플리케이션 제어가 규칙을 적용하도록 구성되어 있고 사용자가 시작 시 차단된 애플리케이션에 대한 접근 권한을 요청한 경우 표시됩니다.

애플리케이션 제어 작업 관련 이벤트를 확인하려면 이벤트 조회를 생성하는 것이 좋습니다.

애플리케이션 제어 관련 실행 파일을 기존 애플리케이션 카테고리 또는 새 애플리케이션 카테고리에 추가할 수 있습니다. 컨텐츠가 수동으로 추가된 애플리케이션 카테고리에만 실행 파일을 추가할 수 있습니다.

애플리케이션 카테고리에 애플리케이션 제어 이벤트 관련 실행 파일을 추가하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고 → 이벤트 선택**로 이동합니다.
   이벤트 조회 목록이 표시됩니다.
2. 애플리케이션 제어 관련 이벤트를 확인할 이벤트 조회를 선택하고 이 이벤트 조회를 시작합니다.
   애플리케이션 제어 관련 이벤트 조회를 만들지 않은 경우 **최근 이벤트**와 같이 사전 정의된 조회를 선택해서 시작할 수 있습니다.
   이벤트 목록이 표시됩니다.
3. 연결된 실행 파일을 애플리케이션 카테고리에 추가하고자 하는 이벤트를 선택한 다음 **카테고리에 할당** 버튼을 누릅니다.
   새 카테고리 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
4. 마법사 페이지에서 관련 설정을 지정합니다:
   - **이벤트와 관련된 실행 파일에 대한 조치** 섹션에서 다음 옵션 중 하나를 선택합니다.
     - **새 애플리케이션 카테고리에 추가**

       이벤트 관련 실행 파일을 기준으로 새 애플리케이션 카테고리를 만들려면 이 옵션을 선택합니다.
       기본적으로 이 옵션은 선택되어 있습니다.
       이 옵션을 선택했다면 새 카테고리 이름을 지정합니다.

     - **기존 애플리케이션 카테고리에 추가**

       기존 애플리케이션 카테고리에 이벤트 관련 실행 파일을 추가하려면 이 옵션을 선택합니다.
       기본적으로 이 옵션은 선택되어 있지 않습니다.

이 옵션을 선택했다면 컨텐츠를 수동으로 추가한 애플리케이션 카테고리 중 실행 파일을 추가할 카테고리를 선택합니다.

- **규칙 유형** 섹션에서 다음 설정 중 하나를 선택합니다.
  - **포함 추가 규칙**
  - **제외 추가 규칙**
- **조건으로 사용할 파라미터** 섹션에서 다음 옵션의 하나를 선택합니다.
  - **인증서 세부 정보(또는 인증서가 없는 파일에 대한 SHA256 해시 값)**

    파일은 인증서로 서명될 수 있습니다. 여러 파일이 동일한 인증서로 서명될 수 있습니다. 예를 들어 동일한 애플리케이션의 서로 다른 버전이 동일한 인증서로 서명되거나 동일한 제조사의 여러 애플리케이션이 동일한 인증서로 서명될 수 있습니다. 인증서를 선택할 때 여러 버전의 애플리케이션이나 동일한 제조사의 여러 애플리케이션이 카테고리에 포함될 수 있습니다.

    각 파일에는 고유한 SHA256 해시 함수가 있습니다. SHA256 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

    카테고리 규칙에 실행 파일의 인증서 세부 정보(또는 인증서가 없는 파일의 경우 SHA256 해시 함수)를 추가하려면 이 옵션을 선택합니다.

    기본적으로 이 옵션은 선택되어 있습니다.
  - **인증서 세부 정보(인증서가 없는 파일은 건너뜀)**

    파일은 인증서로 서명될 수 있습니다. 여러 파일이 동일한 인증서로 서명될 수 있습니다. 예를 들어 동일한 애플리케이션의 서로 다른 버전이 동일한 인증서로 서명되거나 동일한 제조사의 여러 애플리케이션이 동일한 인증서로 서명될 수 있습니다. 인증서를 선택할 때 여러 버전의 애플리케이션이나 동일한 제조사의 여러 애플리케이션이 카테고리에 포함될 수 있습니다.

    실행 파일의 인증서 세부 사항을 카테고리 규칙에 추가하려면 이 옵션을 선택합니다. 실행 파일에 인증서가 없으면 이 파일은 건너 뜁니다. 이 파일에 대한 정보는 카테고리에 추가되지 않습니다.
  - **SHA256만(해시가 없는 파일은 건너뜀)**

    각 파일에는 고유한 SHA256 해시 함수가 있습니다. SHA256 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

    실행 파일의 SHA256 해시 함수의 세부 사항만 추가하려면 이 옵션을 선택합니다.
  - **MD5만(Kaspersky Endpoint Security 10 Service Pack 1 for Windows 이전의 버전에서 지원)**

    각 파일에는 고유한 MD5 해시 함수가 있습니다. MD5 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

    실행 파일의 MD5 해시 함수의 세부 사항만 추가하려면 이 옵션을 선택합니다. MD5 해시 계산 기능은 Kaspersky Endpoint Security 10 Service Pack 1 for Windows 및 그 이전 버전에서 지원됩니다.

5. **확인**를 누릅니다.

마법사가 완료되면 애플리케이션 제어 이벤트와 관련된 실행 파일이 기존 애플리케이션 카테고리 또는 새 애플리케이션 카테고리에 추가됩니다. 수정 또는 생성한 애플리케이션 카테고리의 설정을 볼 수 있습니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어 구성

애플리케이션 제어 카테고리 생성 후 Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어를 구성하는 데 사용할 수 있습니다.

Kaspersky Endpoint Security for Windows 정책에서 애플리케이션 제어를 구성하려면:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
   정책 목록이 포함된 페이지가 표시됩니다.
2. **Kaspersky Endpoint Security for Windows** 정책을 누릅니다.
   정책 설정 창이 열립니다.
3. **애플리케이션 설정 → 보안 제어 → 애플리케이션 제어**로 이동합니다.
   애플리케이션 제어 설정이 포함된 **애플리케이션 제어** 창이 표시됩니다.
4. **애플리케이션 제어** 옵션은 기본적으로 활성화되어 있습니다. **애플리케이션 제어 비활성화** 토글 버튼이 비활성화 위치로 전환되었는지 확인합니다.
5. **애플리케이션 제어 설정** 블록 설정에서 작동 모드를 활성화하여 애플리케이션 제어 규칙을 적용하고 Kaspersky Endpoint Security for Windows가 애플리케이션 시작을 차단하도록 허용합니다.
   애플리케이션 제어 규칙을 테스트하려면 **애플리케이션 제어 설정** 섹션에서 테스트 모드를 활성화합니다. 테스트 모드에서 Kaspersky Endpoint Security for Windows는 애플리케이션 시작을 차단하지 않지만 트리거된 규칙에 대한 정보를 리포트에 기록합니다. 이 정보를 보려면 **리포트 보기** 링크를 클릭하십시오.
6. Kaspersky Endpoint Security for Windows로 사용자가 애플리케이션을 시작할 때 DLL 모듈의 로딩을 모니터링하려면 **DDL 모듈 로드 제어** 옵션을 활성화합니다.
   모듈과 모듈을 로드한 애플리케이션에 관한 정보가 보고서에 저장됩니다.
   Kaspersky Endpoint Security for Windows는 **DLL 모듈 로드 제어** 옵션이 선택된 후에 로드된 드라이버와 DLL 모듈만 모니터링합니다. Kaspersky Endpoint Security for Windows로 Kaspersky Endpoint Security for Windows 시작 전에 로드된 모든 DLL 모듈과 드라이버를 모니터링하려면 **DLL 모듈 로드 제어** 옵션을 선택한 후 컴퓨터를 재시작합니다.
7. (선택 사항) **메시지 템플릿** 블록에서 처음부터 애플리케이션이 차단될 경우 표시되는 메시지 템플릿과 전송되는 이메일 메시지 템플릿을 변경합니다.
8. **애플리케이션 제어 모드** 블록 설정에서 **거부 목록** 또는 **허용 목록** 모드를 선택합니다.
   거부 목록 모드가 기본값으로 선택됩니다.

9. **규칙 목록 설정** 링크를 누릅니다.

   거부 목록 및 허용 목록 창을 열고 애플리케이션 카테고리를 추가합니다. 기본적으로 **거부 목록** 모드가 선택되어 있으면 **거부 목록** 탭이 선택되고, **허용 목록** 모드가 선택되어 있으면 **허용 목록** 탭이 선택됩니다.

10. **거부 목록 및 허용 목록** 창에서 **추가** 버튼을 누릅니다.

    애플리케이션 제어 규칙 창이 열립니다.

11. **Please choose a category** 링크를 클릭합니다.

    애플리케이션 카테고리 창이 열립니다.

12. 이전에 만든 애플리케이션 카테고리를 추가합니다.

    편집 버튼을 누르면 만든 카테고리의 설정을 편집할 수 있습니다.

    추가 버튼을 누르면 새 카테고리를 만들 수 있습니다.

    삭제 버튼을 누르면 목록에서 카테고리를 삭제할 수 있습니다.

13. 애플리케이션 카테고리의 목록이 완료되면 **확인** 버튼을 누릅니다.

    애플리케이션 카테고리 창이 닫힙니다.

14. **애플리케이션 제어** 규칙 창의 **대상 및 권한** 섹션에서 애플리케이션 제어 규칙을 적용할 사용자 및 사용자 그룹 목록을 만듭니다.

15. **확인** 버튼을 눌러 설정을 저장하고 **애플리케이션 제어 규칙** 창을 닫습니다.

16. **확인** 버튼을 눌러 설정을 저장하고 **거부 목록 및 허용 목록** 창을 닫습니다.

17. **확인** 버튼을 눌러 설정을 저장하고 **애플리케이션 제어** 창을 닫습니다.

18. Kaspersky Endpoint Security for Windows 정책 설정이 포함된 창을 닫습니다.

애플리케이션 제어가 구성됩니다. 정책이 클라이언트 기기에 전파되고 나면 실행 파일 시작이 관리됩니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

클라이언트 기기에 설치된 애플리케이션 목록 가져오기 및 보기

Kaspersky Security Center는 Linux 및 Windows을 사용하는 관리 중인 클라이언트 기기에 설치된 모든 소프트웨어의 인벤토리를 수행합니다.

네트워크 에이전트는 기기에 설치된 애플리케이션 목록을 수집하고 이를 중앙 관리 서버로 전송합니다. 네트워크 에이전트가 애플리케이션 목록을 업데이트하는 데 약 10~15분이 소요됩니다.

Windows 기반 클라이언트 기기에서는 네트워크 에이전트가 설치된 애플리케이션에 대한 정보 대부분을 Windows 레지스트리에서 받습니다. Linux 기반 클라이언트 기기에서는 패키지 관리자가 설치된 애플리케이션에 대한 정보를 네트워크 에이전트에 제공합니다.

Linux 기기에서 **자산 관리(소프트웨어)** 섹션의 애플리케이션이 탐지되었다면 애플리케이션 속성에는 관련 실행 파일에 대한 정보가 포함되지 않습니다.

관리 중인 기기에 설치된 애플리케이션 목록을 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 자산 관리(소프트웨어)**로 이동합니다.

   이 페이지에는 관리 중인 기기에 설치된 애플리케이션이 있는 테이블이 표시됩니다. 공급업체 이름, 버전 번호, 실행 파일 목록, 애플리케이션이 설치된 기기 목록, 사용 가능한 소프트웨어 업데이트 목록, 탐지된 소프트웨어 취약점 목록 등의 속성을 확인할 애플리케이션을 선택합니다.

2. 다음과 같이 애플리케이션이 설치된 테이블의 데이터를 그룹화하고 필터링할 수 있습니다:

   - 표의 오른쪽 상단 모서리에 있는 설정 아이콘( )을 클릭합니다.

     호출된 **열 설정** 메뉴에서 테이블에 표시할 열을 선택합니다. 애플리케이션이 설치된 클라이언트 기기의 운영 체제 유형을 보려면 **운영 체제 유형** 열을 선택합니다.

   - 표 오른쪽 상단 모서리에 있는 필터 아이콘( )을 클릭한 다음 호출되는 메뉴에서 필터 기준을 지정하고 적용합니다.

     설치된 애플리케이션의 필터링된 테이블이 표시됩니다.

관리 중인 특정 기기에 설치된 애플리케이션 목록을 보려면,

기본 메뉴에서 **기기 → 관리 중인 기기 → <기기 이름> → 고급 → 자산 관리(소프트웨어)**로 이동합니다. 메뉴에서 애플리케이션 목록을 CSV 파일 또는 TXT 파일로 내보낼 수 있습니다.

애플리케이션 제어에 대한 자세한 내용은 다음 도움말 항목을 참조하십시오:

- Kaspersky Endpoint Security for Windows 온라인 도움말
- Kaspersky Endpoint Security for Linux 온라인 도움말
- Kaspersky Security for Virtualization Light Agent
- Kaspersky Embedded Systems Security for Windows 도움말
- Kaspersky Embedded Systems Security for Linux 도움말

Kaspersky 데이터베이스의 타사 애플리케이션 설치 패키지 만들기

Kaspersky Security Center 웹 콘솔을 사용하면 설치 패키지를 사용하여 타사 애플리케이션을 원격으로 설치할 수 있습니다. 이러한 타사 애플리케이션은 전용 Kaspersky 데이터베이스에 포함되어 있습니다. 처음으로 *중앙 관리 서버 저장소에 업데이트 다운로드* 작업을 실행하면 이 데이터베이스가 자동 생성됩니다.

Kaspersky 데이터베이스의 타사 애플리케이션 설치 패키지를 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동합니다.
2. **추가** 버튼을 클릭합니다.
3. 새 패키지 마법사 페이지가 열리면 **Kaspersky 데이터베이스에서 설치 패키지를 만들 애플리케이션 선택** 옵션을 선택하고 **다음**을 클릭합니다.
4. 애플리케이션 목록이 열리면 관련 애플리케이션을 선택하고 **다음**을 누릅니다.
5. 드롭다운 목록에서 관련 현지화 언어를 선택하고 **다음**을 누릅니다.

   이 단계는 애플리케이션에서 여러 언어 옵션이 제공되는 경우에만 표시됩니다.

6. 설치를 위해 라이센스 계약서에 동의하라는 메시지가 표시될 경우 **최종 사용자 라이센스 계약서** 페이지가 열리면 링크를 눌러 공급업체 웹사이트의 라이센스 계약서를 읽고 **이 최종 사용자 라이센스 계약서의 이용 약관을 모두 읽고 이해했으며 수락함을 확인합니다** 확인란을 선택합니다.
7. **새로운 설치 패키지 이름** 페이지가 열리면 **패키지 이름** 필드에서 설치 패키지 이름을 입력하고 **다음**을 누릅니다.

새로 생성된 설치 패키지가 중앙 관리 서버에 업로드될 때까지 기다립니다. 새 패키지 마법사에서 패키지 생성 프로세스가 성공적으로 완료되었음을 알려주는 메시지를 표시하면 **마침**를 누릅니다.

새로 만든 설치 패키지가 설치 패키지 목록에 나타납니다. *원격으로 애플리케이션 설치* 작업을 만들거나 재구성할 때 이 패키지를 선택할 수 있습니다.

Kaspersky 데이터베이스에서 타사 애플리케이션의 설치 패키지 설정 보기 및 수정

이전에 Kaspersky 데이터베이스에 나열된 타사 애플리케이션의 설치 패키지를 생성한 경우 나중에 이 패키지의 설정을 보고 수정할 수 있습니다.

Kaspersky 데이터베이스에서 타사 애플리케이션의 설치 패키지 설정을 수정하려면 취약점 및 패치 관리 라이센스가 있어야 합니다.

Kaspersky 데이터베이스에서 타사 애플리케이션의 설치 패키지 설정을 보고 수정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동합니다.
2. 설치 패키지 목록이 열리면 관련 패키지의 이름을 누릅니다.
3. 속성 페이지가 열리면 필요한 경우 설정을 수정합니다.
4. **저장** 버튼을 누릅니다.

수정한 설정이 저장됩니다.

Kaspersky 데이터베이스의 타사 애플리케이션 설치 패키지 설정

타사 애플리케이션의 설치 패키지 설정은 다음 탭으로 그룹화됩니다.

아래 나열된 설정 중 일부만 기본적으로 표시되므로 **필터** 버튼을 누르고 목록에서 관련 열 이름을 선택하면 해당하는 열을 추가할 수 있습니다.

- **일반** 탭:
  - 수동으로 편집할 수 있는 설치 패키지 이름이 포함된 입력 필드
  - **애플리케이션**

    설치 패키지가 생성되는 타사 애플리케이션의 이름입니다.
  - **버전**

    설치 패키지가 생성되는 타사 애플리케이션의 버전 번호입니다.
  - **크기**

    타사 설치 패키지의 크기(KB)입니다.
  - **만든 날짜**

    타사 설치 패키지를 만든 날짜와 시간입니다.
  - **경로**

    타사 설치 패키지가 저장된 네트워크 폴더의 경로입니다.
- **설치 절차** 탭:
  - **필요한 일반 시스템 구성 요소 설치**

    이 옵션을 활성화하면 업데이트를 설치하기 전에 애플리케이션은 업데이트 설치를 설치하기 위해 필요한 모든 일반 시스템 구성 요소(선결 조건)를 자동으로 설치합니다. 이러한 필수 구성 요소의 예로는 운영 체제 업데이트 등이 있습니다.

    이 옵션을 비활성화하는 경우에는 필수 구성 요소를 수동으로 설치해야 합니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.
  - 업데이트 속성을 표시하고, 다음 열을 포함하는 표:
    - **이름**

      업데이트 이름입니다.

- **설명**

  업데이트에 대한 설명입니다.

- **출처**

  Microsoft 또는 다른 타사 개발자가 릴리스했는지 여부를 가리키는 업데이트 소스입니다.

- **유형**

  드라이버용인지 또는 애플리케이션용인지를 가리키는 업데이트 유형입니다.

- **카테고리**

  Microsoft 업데이트에 대해 표시되는 WSUS(Windows Server 업데이트 서비스) 카테고리(중요 업데이트, 정의 업데이트, 드라이버, 기능 팩, 보안 업데이트, 서비스 팩, 도구, 업데이트 롤업, 업데이트 또는 업그레이드)입니다.

- **MSRC에서 정의한 중요도**

  MSRC(Microsoft Security Response Center)에서 정의한 업데이트의 심각도입니다.

- **중요도**

  Kaspersky에서 정의한 업데이트의 심각도입니다.

- **패치 중요도**

  Kaspersky 애플리케이션용인 경우 패치의 심각도입니다.

- **문서**

  업데이트를 설명하는 기술 자료 문서의 식별자(ID)입니다.

- **보안 공지 문서**

  업데이트를 설명하는 보안 게시판의 ID입니다.

- **설치하도록 할당 안 됨(새 버전)**

  업데이트가 설치하도록 할당 안 됨 상태인지 여부를 표시합니다.

- **설치 대상**

  업데이트가 설치 대상 상태인지 여부를 표시합니다.

- **설치 중**

  업데이트가 설치 중 상태인지 여부를 표시합니다.

- **설치됨**

  업데이트가 설치됨 상태인지 여부를 표시합니다.

- **실패**

  업데이트가 실패 상태인지 여부를 표시합니다.

- **재시작 필요**

  업데이트가 재시작 필요함 상태인지 여부를 표시합니다.

- **등록된 날짜**

  업데이트가 등록된 날짜와 시간을 표시합니다.

- **대화식 모드로 설치됨**

  업데이트를 설치하는 동안 사용자와의 상호 작용이 필요한지 여부를 표시합니다.

- **철회됨**

  업데이트가 철회된 날짜와 시간을 표시합니다.

- **승인 상태 업데이트**

  업데이트 설치 승인 여부를 표시합니다.

- **리비전**

  업데이트의 현재 리비전 번호를 표시합니다.

- **업데이트 ID**

  업데이트 ID를 표시합니다.

- **애플리케이션 버전**

  애플리케이션을 업데이트할 버전 번호를 표시합니다.

- **대체됨**

  업데이트를 대체할 수 있는 다른 업데이트를 표시합니다.

- **대체 중**

  업데이트로 대체할 수 있는 다른 업데이트를 표시합니다.

- **라이센스 계약서 약관 수락 필요**

  업데이트 시 EULA(최종 사용자 라이센스 계약서) 약관에 동의해야 하는지 여부를 표시합니다.

- **상세 설명**

  업데이트 공급업체의 이름을 표시합니다.

- **애플리케이션 제품군**

  업데이트가 속한 애플리케이션 제품군의 이름을 표시합니다.

- **애플리케이션**

  업데이트가 속한 애플리케이션의 이름을 표시합니다.

- **현지화 언어**

  업데이트 현지화 언어를 표시합니다.

- **설치하도록 할당 안 됨(새 버전)**

  업데이트가 설치하도록 할당 안 됨(새 버전) 상태인지 여부를 표시합니다.

- **필수 구성 요소 설치 필요**

  업데이트가 필수 구성 요소 설치 필요 상태인지 여부를 표시합니다.

- **다운로드 모드**

  업데이트 다운로드 모드를 표시합니다.

- **패치**

  업데이트가 패치인지 여부를 표시합니다.

- **설치 안 됨**

  업데이트가 설치 안 됨 상태인지 여부를 표시합니다.

- 설치 중 명령줄 파라미터로 사용되는 이름, 설명, 값과 함께 설치 패키지 설정을 표시하는 **설정** 탭. 패키지가 이러한 설정을 제공하지 않으면 해당 메시지가 표시됩니다. 이러한 설정의 값을 수정할 수 있습니다.

- 설치 패키지 리비전을 표시하고 다음 열을 포함하는 **리비전 내역** 탭:
  - **리비전** – 설치 패키지 리비전 번호를 표시합니다.
  - **시간** – 설치 패키지 설정이 수정된 날짜 및 시간입니다.
  - **사용자** – 설치 패키지 설정을 수정한 사용자 이름입니다.
  - **처리** – 리비전 내 설치 패키지에서 수행된 작업을 나열합니다.
  - **설명** - 설치 패키지 설정 변경 내용 관련 리비전 설명.
    기본적으로 리비전 설명은 비어 있습니다. 리비전에 설명을 추가하려면, 관련 리비전을 선택하고 **설명 편집** 버튼을 클릭합니다. 창이 열리면 리비전 관한 설명 텍스트를 입력합니다.

애플리케이션 태그

Kaspersky Security Center를 사용하면 자산 관리(소프트웨어)에서 애플리케이션에 태그를 지정할 수 있습니다. 애플리케이션 그룹화 또는 검색에 사용할 수 있는 애플리케이션의 레이블입니다. 애플리케이션에 할당된 태그는 기기 조회에서 조건으로 사용할 수 있습니다.

예를 들어 [브라우저] 태그를 만든 다음 모든 브라우저(Microsoft Internet Explorer, Google Chrome, Mozilla Firefox 등)에 할당할 수 있습니다.

애플리케이션 태그 생성

애플리케이션 태그를 생성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 애플리케이션 태그**로 이동합니다.
2. **추가**를 누릅니다.
   새 태그 창이 열립니다.
3. 태그 이름을 입력합니다.
4. **확인**을 눌러 변경을 저장합니다.

애플리케이션 태그 목록에 새 태그가 표시됩니다.

애플리케이션 태그 이름 변경

애플리케이션 태그의 이름을 바꾸려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 애플리케이션 태그**로 이동합니다.
2. 이름을 바꿀 태그 옆의 확인란을 선택하고 **편집**을 누릅니다.
   태그 속성 창이 열립니다.

3. 태그 이름을 변경합니다.

4. **확인**을 눌러 변경을 저장합니다.

업데이트된 태그가 애플리케이션 태그 목록에 표시됩니다.

애플리케이션에 태그 할당

애플리케이션에 태그를 하나 또는 여러 개 할당하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 자산 관리(소프트웨어)**로 이동합니다.

2. 태그를 할당할 애플리케이션의 이름을 누릅니다.

3. **태그** 탭을 선택합니다.

중앙 관리 서버에 있는 모든 애플리케이션 태그가 탭에 표시됩니다. 선택한 애플리케이션에 할당된 태그의 경우 **태그 할당 방식** 열의 확인란이 선택되어 있습니다.

4. 할당하려는 태그에 대해 **태그 할당 방식** 열의 확인란을 선택합니다.

5. **저장**을 눌러 변경 사항을 저장합니다.

태그가 애플리케이션에 할당됩니다.

애플리케이션에서 할당된 태그 제거

애플리케이션에서 태그를 하나 또는 여러 개 제거하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 자산 관리(소프트웨어)**로 이동합니다.

2. 태그를 제거할 애플리케이션의 이름을 누릅니다.

3. **태그** 탭을 선택합니다.

중앙 관리 서버에 있는 모든 애플리케이션 태그가 탭에 표시됩니다. 선택한 애플리케이션에 할당된 태그의 경우 **태그 할당 방식** 열의 확인란이 선택되어 있습니다.

4. 제거하려는 태그에 대해 **태그 할당 방식** 열의 확인란을 선택 취소합니다.

5. **저장**을 눌러 변경 사항을 저장합니다.

태그가 애플리케이션에서 제거됩니다.

제거된 애플리케이션 태그가 삭제되지는 않습니다. 원하는 경우 태그를 수동으로 삭제할 수 있습니다.

애플리케이션 태그 삭제

애플리케이션 태그를 삭제하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **동작 → 타사 애플리케이션 → 애플리케이션 태그**로 이동합니다.
2. 목록에서 삭제할 애플리케이션 태그를 선택합니다.
3. **삭제** 버튼을 누릅니다.
4. 확인 창이 열리면 **확인**를 누릅니다.

애플리케이션 태그가 삭제됩니다. 삭제된 태그는 할당되었던 모든 애플리케이션에서 자동으로 제거됩니다.

모니터링 및 보고

이 섹션에서는 Kaspersky Security Center의 모니터링 및 보고 기능에 대해 설명합니다. 이러한 기능을 통해 인프라, 보호 상태 및 통계의 개요를 확인할 수 있습니다.

Kaspersky Security Center 배포 후나 작동 중에 요구에 가장 적합하도록 모니터링 및 리포팅 기능을 구성할 수 있습니다.

시나리오: 모니터링 및 보고

이 섹션에서는 Kaspersky Security Center에서 모니터링 및 리포팅 기능을 구성하는 시나리오를 제공합니다.

필수 구성 요소

조직의 네트워크에 Kaspersky Security Center를 배포한 후 모니터링을 시작하고 기능에 대한 리포트를 생성할 수 있습니다.

조직의 네트워크에서 모니터링 및 리포팅은 단계적으로 진행됩니다.

1. **기기 상태 전환 구성**

   특정 조건에 따라 기기 상태에 대한 설정을 익힙니다. 이러한 설정을 변경하여 *심각* 또는 *경고* 심각도의 이벤트 수를 변경할 수 있습니다. 기기 상태 전환을 구성할 때 다음 사항을 확인하십시오.

   - 새 설정은 조직의 정보 보안 정책과 상충하지 않습니다.
   - 조직 네트워크의 중요한 보안 이벤트에 적시에 대응할 수 있습니다.

2. **클라이언트 기기에서 이벤트 알림 구성**

   방법 지침:

   클라이언트 기기에서 이벤트 알림(이메일, SMS 또는 실행 파일 실행을 통해) 구성

3. **바이러스 발생 이벤트에 대한 보안 네트워크 응답 변경**

   중앙 관리 서버 속성에서 특정 임계값을 변경할 수 있습니다. 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.

4. **심각 및 경고 알림에 대한 권장 작업 수행**

   방법 지침:

   조직 네트워크에 대한 권장 작업 수행

5. **조직 네트워크의 보안 상태 검토**

   방법 지침:

   - 보호 상태 위젯 검토
   - 보호 상태 리포트 생성 및 검토
   - 오류 리포트 생성 및 검토

6. **보호되지 않는 클라이언트 기기 위치 추적**

   방법 지침:

   - 새로운 기기 위젯 검토
   - 보호 배포 리포트 생성 및 검토

7. **클라이언트 기기의 보호 확인**

   방법 지침:

   - 보호 상태 및 위협 통계 카테고리에서 검토 리포트 생성
   - 심각 이벤트 조회 및 검토

8. **데이터베이스의 이벤트 부하 평가 및 제한**

   관리 중인 애플리케이션 작업 중 발생하는 이벤트에 대한 정보는 클라이언트 기기에서 전송되어 중앙 관리 서버 데이터베이스에 등록됩니다. 중앙 관리 서버의 부하를 줄이려면 데이터베이스에 저장할 수 있는 최대 이벤트 수를 평가 및 제한합니다.

   방법 지침:

   - 데이터베이스 공간 계산
   - 최대 이벤트 수 제한

9. **라이센스 정보 검토**

   방법 지침:

   - 라이센스 키 사용 현황 위젯을 대시 보드에 추가한 후 검토
   - 라이센스 키 사용 리포트 생성 및 검토

결과

시나리오가 완료되면 조직의 네트워크 보호에 대한 정보를 받게 되므로 추가 보호 작업을 계획할 수 있습니다.

모니터링 및 리포팅 유형 정보

조직 네트워크의 보안 이벤트에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다. 이벤트를 기반으로 Kaspersky Security Center 웹 콘솔은 조직의 네트워크에서 다음 유형의 모니터링 및 리포팅을 제공합니다.

- 대시보드
- 리포트
- 이벤트 조회
- 알림

대시보드

대시보드를 사용하면 정보를 그래픽으로 표시하여 조직 네트워크의 보안 트렌드를 모니터링할 수 있습니다.

리포트

리포트 기능을 사용하면 조직의 네트워크 보안에 대한 자세한 숫자 정보를 얻고, 이 정보를 파일에 저장하며, 이메일로 보내고, 인쇄할 수 있습니다.

이벤트 조회

이벤트 조회는 중앙 관리 서버 데이터베이스에서 선택한 이벤트를 미리 정의된 조회 항목을 사용해 화면에 그 결과를 보여 줍니다. 이러한 이벤트 세트는 다음 카테고리에 따라 그룹화됩니다:

- 심각도 기준 — **심각 이벤트**, **기능 실패**, **경고** 및 **정보 이벤트**
- 시간 기준 — **최근 이벤트**
- 유형 기준 - **사용자 개선 요청 사항** 및 **감사 이벤트**

구성을 위해 Kaspersky Security Center 웹 콘솔 인터페이스에서 사용할 수 있는 설정에 따라 사용자 지정 이벤트 조회를 생성하고 볼 수 있습니다.

알림

알림을 통해 이벤트에 대해 경고하고 적절하다고 생각하는 권장 작업을 하나 또는 여러 개 수행하여 이러한 이벤트에 대한 응답 속도를 높일 수 있습니다.

대시보드 및 위젯

이 섹션에는 대시보드 및 대시보드가 제공하는 위젯에 대한 정보가 포함되어 있습니다. 이 섹션에는 위젯을 관리하고 위젯 설정을 구성하는 방법에 대한 지침이 포함되어 있습니다.

대시보드 사용

대시보드를 사용하면 정보를 그래픽으로 표시하여 조직 네트워크의 보안 트렌드를 모니터링할 수 있습니다.

대시보드는 **대시보드**를 눌러 Kaspersky Security Center 웹 콘솔의 **모니터링 및 보고** 섹션에서 사용할 수 있습니다.

대시보드에서는 사용자 지정할 수 있는 위젯을 제공합니다. 파이형 차트 또는 도넛형 차트, 표, 그래프, 막대형 차트 및 목록으로 표시되는 다양한 위젯 중에서 선택할 수 있습니다. 위젯에 표시되는 정보는 자동으로 업데이트되며 업데이트 기간은 1~2분입니다. 업데이트 간의 간격은 위젯별로 다릅니다. 설정 메뉴를 사용하여 언제든지 위젯에서 데이터를 수동으로 새로 고칠 수 있습니다.

기본적으로 위젯에는 중앙 관리 서버의 데이터베이스에 저장된 모든 이벤트 관련 정보가 포함됩니다.

Kaspersky Security Center 웹 콘솔에는 다음 범주에 대한 기본 위젯 세트가 있습니다.

- **보호 상태**
- **배포**
- **업데이트**
- **위협 통계**
- **기타**

일부 위젯에는 링크가 포함된 텍스트 정보가 있습니다. 링크를 누르면 자세한 정보를 볼 수 있습니다.

대시보드를 구성할 때는 필요한 위젯을 추가하거나 필요하지 않은 위젯을 숨기고, 위젯의 크기나 모양을 변경하고, 위젯을 옮기고, 위젯 설정을 변경할 수 있습니다.

대시보드에 위젯 추가

대시보드에 위젯을 추가하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **대시보드**로 이동합니다.
2. **웹 위젯 추가 또는 복원** 버튼을 누릅니다.
3. 사용 가능한 위젯 목록에서 대시보드에 추가할 위젯을 선택합니다.

   위젯은 카테고리별로 그룹화되어 있습니다. 특정 카테고리에 포함된 위젯 목록을 보려면 카테고리 이름 옆에 있는 펼침 단추 아이콘(>)을 누릅니다.
4. **추가** 버튼을 누릅니다.

선택한 위젯이 대시보드 끝에 추가됩니다.

이제 추가한 위젯의 표시와 파라미터를 편집할 수 있습니다.

대시보드에서 위젯 숨기기

대시보드에서 표시된 위젯을 숨기려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **대시보드**로 이동합니다.
2. 숨길 위젯 옆의 설정 아이콘(⚙)을 누릅니다.
3. **웹 위젯 숨기기**를 선택합니다.
4. **경고** 창이 열리면 **확인**를 누릅니다.

선택한 위젯이 숨겨집니다. 나중에 다시 이 위젯을 대시보드에 추가할 수 있습니다.

대시보드에서 위젯 이동

대시보드에서 위젯을 이동하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **대시보드**로 이동합니다.
2. 이동할 위젯 옆의 설정 아이콘(⚙)을 누릅니다.
3. **이동**을 선택합니다.
4. 위젯을 이동할 위치를 누릅니다. 다른 위젯만 선택할 수 있습니다.

선택한 위젯의 위치가 바뀝니다.

위젯 크기 또는 모양 변경

그래프가 표시되는 위젯의 경우 해당 표시를 막대형 차트나 꺾은 선형 차트로 변경할 수 있습니다. 크기를 소형, 중형, 최대로 변경할 수 있는 위젯도 있습니다.

위젯 표시를 변경하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **대시보드**로 이동합니다.
2. 편집할 위젯 옆의 설정 아이콘(⚙)을 누릅니다.
3. 다음 중 하나를 수행합니다:
   - 위젯을 막대형 차트로 표시하려면 **차트 유형: 막대**를 선택합니다.
   - 위젯을 꺾은 선형 차트로 표시하려면 **차트 유형: 선**을 선택합니다.

- 위젯이 차지하는 공간을 변경하려면 다음 값 중 하나를 선택합니다.
  - **컴팩트**
  - **컴팩트(막대 전용)**
  - **중간(도넛 차트)**
  - **중간(막대 차트)**
  - **최대**

선택한 위젯의 표시가 변경됩니다.

위젯 설정 변경

위젯의 설정을 변경하면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **대시보드**로 이동합니다.
2. 변경할 위젯 옆의 설정 아이콘(⚙)을 누릅니다.
3. **설정 표시**를 선택합니다.
4. 위젯 설정 창이 열리면 위젯 설정을 필요한 대로 변경합니다.
5. **저장**을 눌러 변경 사항을 저장합니다.

선택한 위젯의 설정이 변경됩니다.

설정 세트는 특정 위젯별로 다릅니다. 다음은 몇 가지 일반 설정입니다.

- **웹 위젯 범위**(위젯에 정보가 표시되는 개체 세트) - 관리 그룹이나 기기 선택을 예로 들 수 있습니다.
- **작업 선택** (위젯에 정보가 표시되는 작업).
- **시간 간격**(정보가 위젯에 표시되는 시간 간격) - 지정된 두 날짜 사이의 범위입니다. 지정한 날짜에서 현재 날짜까지이거나, 현재 날짜에서 지정된 기간(일)을 뺀 기간입니다.
- **다음이 지정되면 심각으로 설정** 및 **다음이 지정되면 경고로 설정** (표시등의 색상을 결정하는 규칙).

위젯 설정을 변경한 후 위젯의 데이터를 직접 새로고침할 수 있습니다.

위젯의 데이터를 새로고침하려면:

1. 메인 메뉴에서 **모니터링 및 보고** → **대시보드**로 이동합니다.
2. 이동할 위젯 옆의 설정 아이콘(⚙)을 누릅니다.
3. **새로 고침**을 선택합니다.

위젯의 데이터가 새로고침됩니다.

대시보드 전용 모드 정보

네트워크를 관리하지 않지만 Kaspersky Security Center에서 네트워크 보호 통계를 보고자 하는 직원(예: 최고 관리자)을 위한 대시보드 전용 모드를 구성할 수 있습니다. 사용자가 이 모드를 활성화하면 미리 정의된 위젯 세트가 있는 대시보드만 사용자에게 표시됩니다. 따라서 위젯에 지정된 통계(예: 관리되는 모든 기기의 보호 상태, 최근에 탐지된 위협 수 또는 네트워크에서 가장 빈번한 위협 목록)를 모니터링할 수 있습니다.

사용자가 대시보드 전용 모드에서 작업하는 경우 다음 제한 사항이 적용됩니다.

- 메인 메뉴는 사용자에게 표시되지 않으므로 네트워크 보호 설정을 변경할 수 없습니다.
- 사용자는 위젯 추가 또는 숨기기와 같은 위젯으로 작업을 수행할 수 없습니다. 따라서 사용자에게 필요한 모든 위젯을 대시보드에 올려 놓고 개체를 계산하는 규칙을 설정하거나 시간 간격을 지정하는 등의 구성을 해야 합니다.

대시보드 전용 모드는 자신에게 할당할 수 없습니다. 이 모드에서 작업하려면 시스템 관리자, MSP(관리 서비스 제공자) 또는 **일반 기능: 사용자 권한** 기능 영역에서 **개체 ACL 수정** 권한이 있는 사용자에게 문의하십시오.

대시보드 전용 모드 구성

대시보드 전용 모드 구성을 시작하기 전에 다음 전제 조건이 충족되는지 확인해야 합니다.

- **일반 기능: 사용자 권한** 기능 영역에 **개체 ACL 수정** 권한이 있습니다. 이 권한이 없으면 모드 구성을 위한 탭이 없습니다.
- 사용자가 **일반 기능: 기본 기능** 기능 영역에 **읽기** 권한이 있습니다.

> 네트워크에 중앙 관리 서버 계층이 정렬되어 있다면, **사용자 및 역할 → 사용자 및 그룹** 섹션의 **사용자** 탭에서 사용자 계정을 사용할 수 있는 서버로 이동하여 대시보드 전용 모드를 구성할 수 있습니다. 기본 서버 또는 물리적 보조 서버일 수 있습니다. 가상 서버에서는 모드를 조정할 수 없습니다.

대시보드 전용 모드 구성 방법:

1. 기본 메뉴에서 **사용자 및 역할 → 사용자 및 그룹**으로 이동한 다음 **사용자** 탭을 선택합니다.
2. 위젯으로 대시보드를 조정하려는 사용자 계정 이름을 누릅니다.
3. 사용자 설정 창이 열리면 **Dashboard** 탭을 선택합니다.
   열리는 탭에는 사용자와 동일한 대시보드가 표시됩니다.
4. **대시보드 전용 모드로 콘솔 표시** 옵션이 활성화된 경우 토글 버튼을 전환하여 비활성화합니다.
   이 옵션이 활성화되면 대시보드도 변경할 수 없습니다. 옵션을 비활성화한 후 위젯을 관리할 수 있습니다.

5. 대시보드 모양을 구성합니다. **대시보드** 탭에 준비된 위젯 세트는 사용자 정의 가능한 계정이 있는 사용자가 사용할 수 있습니다. 위젯의 설정이나 크기를 변경하거나 대시보드에서 위젯을 추가 또는 제거할 수 없습니다. 따라서 사용자가 네트워크 보호 통계를 볼 수 있도록 조정합니다. 이를 위해 **대시보드** 탭에서 **모니터링 및 보고** → **대시보드** 섹션에서와 같은 위젯으로 동일한 작업을 수행할 수 있습니다.

   - 대시보드에 위젯을 추가합니다.
   - 사용자에게 필요하지 않은 위젯을 숨깁니다.
   - 위젯을 특정 순서로 이동합니다.
   - 위젯의 크기나 모양을 변경합니다.
   - 위젯 설정을 변경합니다.

6. 토글 버튼을 전환하여 **대시보드 전용 모드로 콘솔 표시** 옵션을 활성화합니다.

   그 후에는 사용자가 대시보드만 사용할 수 있습니다. 통계를 모니터링할 수 있지만 네트워크 보호 설정 및 대시보드 모양을 변경할 수는 없습니다. 사용자와 동일한 대시보드가 표시되므로 대시보드를 변경할 수도 없습니다.

   이 옵션을 비활성화하면 기본 메뉴가 사용자에게 표시되므로 사용자는 보안 설정 및 위젯 변경을 포함하여 Kaspersky Security Center에서 다양한 작업을 수행할 수 있습니다.

7. 대시보드 전용 모드 구성을 마치면 **저장** 버튼을 클릭합니다. 그렇게 해야만 준비된 대시보드가 사용자에게 표시됩니다.

8. 사용자가 지원되는 Kaspersky 애플리케이션의 통계를 보기 위해이 접근 권한이 필요한 경우 사용자에 대한 권한을 구성합니다. 이후 Kaspersky 애플리케이션 데이터는 사용자를 위해 해당 애플리케이션의 위젯에 표시됩니다.

사용자는 사용자 지정 계정으로 Kaspersky Security Center에 로그인하고 대시보드 전용 모드에서 네트워크 보호 통계를 모니터링할 수 있습니다.

관리 및 보호 리포트

이 섹션에서는 보고서 사용, 사용자 정의 보고서 템플릿 관리, 보고서 템플릿을 사용한 새 보고서 생성, 보고서 전달 작업 생성 방법에 대해 설명합니다.

리포트 사용

리포트 기능을 사용하면 조직의 네트워크 보안에 대한 자세한 숫자 정보를 얻고, 이 정보를 파일에 저장하며, 이메일로 보내고, 인쇄할 수 있습니다.

리포트는 **리포트**를 눌러 Kaspersky Security Center 웹 콘솔의 **모니터링 및 보고** 섹션에서 사용할 수 있습니다.

기본적으로 리포트에는 지난 30일 동안의 정보가 포함됩니다.

Kaspersky Security Center에는 다음 범주에 대한 기본 리포트 세트가 있습니다.

- **보호 상태**
- **배포**

- **업데이트**
- **위협 통계**
- **기타**

사용자 지정 리포트 템플릿을 생성하고, 리포트 템플릿을 편집 및 삭제할 수 있습니다.

기존 템플릿을 기반으로 하는 리포트를 생성하고, 리포트를 파일로 내보내고, 리포트 전달용 작업을 생성할 수 있습니다.

리포트 템플릿 만들기

리포트 템플릿을 만들려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **모니터링 및 보고** → **리포트**로 이동합니다.
2. **추가**를 누릅니다.
   새 리포트 템플릿 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. 리포트 이름을 입력하고 리포트 유형을 선택합니다.
4. 마법사의 **범위** 단계에서 이 리포트 템플릿을 기반으로 하는 리포트에 데이터를 표시할 클라이언트 기기 세트(관리 그룹, 기기 조회, 선택한 기기, 네트워크에 연결된 모든 기기 등)를 선택합니다.
5. 마법사의 **보고 기간** 단계에서 리포트 기간을 지정합니다. 사용 가능한 값은 다음과 같습니다:
   - 지정한 두 날짜 사이
   - 지정한 날짜에서 리포트 생성 날짜까지
   - 리포트 생성 날짜에서 리포트 생성 날짜까지의 지정된 기간(일)을 뺀 기간

   이 페이지가 표시되지 않는 리포트도 있습니다.
6. **확인**을 눌러 마법사를 닫습니다.
7. 다음 중 하나를 수행합니다:
   - **저장 및 실행** 버튼을 눌러 새 리포트 템플릿을 저장하고 해당 템플릿을 기반으로 하는 리포트를 실행합니다.
     리포트 템플릿이 저장됩니다. 리포트가 생성됩니다.
   - **저장** 버튼을 눌러 새 리포트 템플릿을 저장합니다.
     리포트 템플릿이 저장됩니다.

새 템플릿을 사용하여 리포트를 만들고 볼 수 있습니다.

리포트 템플릿 속성 보기 및 편집

리포트 템플릿 이름 또는 리포트에 표시되는 필드와 같은 리포트 템플릿의 기본 속성을 확인하고 편집할 수 있습니다.

리포트 템플릿의 속성을 확인하고 편집하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **모니터링 및 보고** → **리포트**로 이동합니다.
2. 속성을 보고 편집하려는 리포트 템플릿 옆의 확인란을 선택합니다.
   먼저 리포트를 생성한 다음 **편집** 버튼을 눌러도 됩니다.
3. **리포트 템플릿 속성 열기** 버튼을 클릭합니다.
   일반 탭이 선택된 상태로 **<리포트 이름> 리포트 편집** 창이 열립니다.
4. 리포트 템플릿 속성을 편집합니다.
   - **일반** 탭:
     - 리포트 템플릿 이름
     - **표시되는 최대 항목 수**

       이 옵션을 활성화하면 상세 리포트 데이터가 포함된 표에 표시되는 항목 수가 지정된 값을 초과하지 않습니다.

       리포트 항목은 먼저 리포트 템플릿 속성의 **필드** → **상세 정보 필드**드 섹션에 지정된 규칙에 따라 정렬되며, 결과 항목 중 첫 번째 항목만 유지됩니다. 상세 리포트 데이터가 포함된 표의 제목에는 표시되는 항목 수, 그리고 다른 리포트 템플릿 설정과 일치하는 총 사용 가능 항목 수가 나타납니다.

       이 옵션을 비활성화하면 상세 리포트 데이터가 포함된 표에 사용 가능한 모든 항목이 표시됩니다. 이 옵션은 사용하도록 설정하는 것이 좋습니다. 표시되는 리포트 항목의 수를 제한하면 DBMS(데이터베이스 관리 시스템)의 부하가 감소하며 리포트를 생성하고 내보내는 데 걸리는 시간도 단축됩니다. 항목이 너무 많이 포함된 리포트도 있습니다. 이러한 리포트에서는 모든 항목을 읽고 분석하기가 어려울 수도 있습니다. 또한 이러한 리포트를 생성하는 과정에서 기기의 메모리가 소진될 수도 있으며, 그러면 리포트를 확인할 수 없습니다.

       기본적으로 이 옵션은 켜져 있습니다. 기본값은 1000입니다.

     - **그룹**

       설정 버튼을 눌러 리포트 생성 대상 클라이언트 기기 세트를 변경합니다. 일부 리포트 유형의 경우 이 버튼을 사용하지 못할 수 있습니다. 실제 설정은 리포트 템플릿 생성 중에 지정한 설정에 따라 달라집니다.

     - **시간 간격**

       설정 버튼을 눌러 리포트 기간을 수정합니다. 일부 리포트 유형의 경우 이 버튼을 사용하지 못할 수 있습니다. 사용 가능한 값은 다음과 같습니다:

       - 지정한 두 날짜 사이
       - 지정한 날짜에서 리포트 생성 날짜까지
       - 리포트 생성 날짜에서 리포트 생성 날짜까지의 지정된 기간(일)을 뺀 기간

     - **보조 및 가상 중앙 관리 서버의 데이터 포함**

       이 옵션을 활성화하면 리포트 템플릿 생성 대상인 중앙 관리 서버에 속한 보조 및 가상 중앙 관리 서버의 정보가 리포트에 포함됩니다.

       현재 중앙 관리 서버의 데이터만 보려면 이 옵션을 비활성화합니다.

       기본적으로 이 옵션은 켜져 있습니다.

- **최대 중첩 레벨**

  현재 중앙 관리 서버에서 지정한 값 이하의 중첩 레벨 아래에 있는 보조 및 가상 중앙 관리 서버의 데이터가 리포트에 포함됩니다.

  기본값은 1입니다. 트리의 하위 레벨에 있는 보조 중앙 관리 서버에서 정보를 가져와야 하는 경우 이 값을 변경할 수 있습니다.

- **데이터 대기 시간 간격(분)**

  리포트 템플릿 생성 대상인 중앙 관리 서버가 리포트를 생성하기 전에 지정된 시간(분) 동안 보조 중앙 관리 서버의 데이터를 기다립니다. 이 기간이 끝날 때까지 보조 중앙 관리 서버에서 데이터가 수신되지 않아도 리포트는 실행됩니다. 리포트에는 실제 데이터가 아니라 캐시에서 가져온 데이터(**보조 중앙 관리 서버에서 데이터 캐시**옵션을 활성화한 경우) 또는 **N/A**(사용 불가)가 표시됩니다.

  기본값은 5분입니다.

- **보조 중앙 관리 서버에서 데이터 캐시**

  보조 중앙 관리 서버가 리포트 템플릿 생성 대상인 중앙 관리 서버에 데이터를 주기적으로 전송합니다. 전송된 데이터는 이 중앙 관리 서버에서 캐시에 저장됩니다.

  현재 중앙 관리 서버가 리포트를 생성하는 중에 보조 중앙 관리 서버에서 데이터를 수신할 수 없으면 리포트에는 캐시에서 가져온 데이터가 표시됩니다. 데이터가 캐시로 전송된 날짜도 표시됩니다.

  이 옵션을 활성화하면 최신 데이터를 가져올 수 없어도 보조 중앙 관리 서버에서 정보를 확인할 수 있습니다. 하지만 표시되는 데이터는 오래된 데이터일 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **캐시 업데이트 간격(시)**

  보조 중앙 관리 서버가 리포트 템플릿 생성 대상인 중앙 관리 서버에 데이터를 주기적으로 전송합니다. 이 기간을 시간 단위로 지정할 수 있습니다. 0시간을 지정하면 리포트 생성 시에만 데이터가 전송됩니다.

  기본값은 0입니다.

- **보조 중앙 관리 서버에서 자세한 정보 전송**

  생성된 리포트에서 상세 리포트 데이터가 포함된 표에 리포트 템플릿 생성 대상인 중앙 관리 서버의 보조 중앙 관리 서버 데이터가 포함됩니다.

  이 옵션을 활성화하면 리포트 생성 속도가 느려지며 중앙 관리 서버 간의 트래픽이 증가합니다. 그러나 리포트 하나에서 모든 데이터를 확인할 수 있습니다.

  이 옵션을 활성화하는 대신 상세 리포트 데이터를 분석하여 결함이 있는 보조 중앙 관리 서버를 탐지한 다음 결함이 있는 중앙 관리 서버에 대해서만 같은 리포트를 생성할 수 있습니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **필드** 탭

  리포트에 표시할 필드를 선택한 다음 **위로 이동** 버튼과 **아래로 이동** 버튼을 사용하여 이러한 필드의 순서를 변경합니다. **추가** 버튼이나 **편집** 버튼을 사용하여 각 필드를 기준으로 리포트의 정보를 정렬 및 필터링해야 하는지 여부를 지정합니다.

섹션 **세부 사항 필터 필드**에서 **필터 변환** 버튼을 눌러 확장 필터링 형식을 사용할 수도 있습니다. 이 형식을 통해 논리 OR 연산을 사용하여 다양한 필드에 지정된 필터링 조건을 결합할 수 있습니다. 버튼을 누르면 **필터 변환** 패널이 오른쪽에 열립니다. **필터 변환** 버튼을 눌러 변환을 확인합니다. 이제 논리 OR 연산을 사용하여 적용된 섹션 **상세 정보 필드**의 조건으로 변환된 필터를 정의할 수 있습니다.

리포트를 복잡한 필터링 조건을 지원하는 형식으로 변환하면 리포트는 이전 버전의 Kaspersky Security Center(11 이하)와 호환되지 않습니다. 또한, 변환된 리포트는 이렇게 호환되지 않는 버전을 실행하는 보조 중앙 관리 서버의 데이터를 포함하지 않습니다.

5. **저장**을 눌러 변경 사항을 저장합니다.
6. **<리포트 이름> 리포트 편집** 창을 닫습니다.

업데이트된 리포트 템플릿이 리포트 템플릿 목록에 표시됩니다.

리포트를 파일로 내보내기

XML, HTML 또는 PDF 파일로 리포트를 내보낼 수 있습니다.

리포트를 파일로 내보내려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **리포트**로 이동합니다.
2. 파일로 내보내려는 리포트 옆의 확인란을 선택합니다.
3. **리포트 내보내기** 버튼을 누릅니다.
4. 창이 열리면 **이름** 필드에 있는 리포트 파일 이름을 변경합니다. 기본적으로 파일 이름은 선택한 리포트 템플릿 이름과 일치합니다.
5. 리포트 파일 유형(XML, HTML 또는 PDF)을 선택합니다.
6. **리포트 내보내기** 버튼을 누릅니다.

   선택한 형식의 리포트가 기기(기기의 기본 폴더)로 다운로드됩니다. 또는 원하는 위치에 파일을 저장할 수 있도록 브라우저에 표준 **다른 이름으로 저장** 창이 열립니다.

리포트가 파일에 저장됩니다.

리포트 만들기 및 보기

리포트를 만들고 보려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **모니터링 및 보고** → **리포트**로 이동합니다.
2. 리포트를 만드는 데 사용할 리포트 템플릿의 이름을 누릅니다.

   선택한 템플릿을 사용하는 리포트가 생성되고 표시됩니다.

보고서 데이터는 중앙 관리 서버의 현지화 설정에 따라 표시됩니다.

리포트에는 다음 데이터가 표시됩니다:

- **요약** 탭:
  - 리포트 이름과 유형, 리포트에 대한 간략한 설명과 보고 기간, 리포트가 생성된 대상 기기 그룹에 대한 정보.
  - 가장 대표적인 리포트 데이터를 보여 주는 그래픽 차트.
  - 계산된 리포트 지표로 구성된 통합 테이블.
- **자세히** 탭에 표시되는 세부 리포트 데이터로 구성된 테이블.

리포트 전달 작업 만들기

선택한 리포트를 전달하는 작업을 생성할 수 있습니다.

리포트 전달 작업을 만들려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **리포트**로 이동합니다.
2. 리포트 전달 작업을 생성할 리포트 템플릿 옆의 확인란을 선택합니다.
3. **전송 작업 생성** 버튼을 누릅니다.
   새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
4. 마법사의 **새 작업 설정** 단계에서 작업 이름을 입력합니다.
   기본 이름은 **리포트 전달**입니다. 이미 같은 이름의 작업이 있다면 작업 이름에 순서 번호(<N>)가 추가됩니다.
5. 마법사의 **리포트 구성** 단계에서 다음 설정을 지정합니다.
   a. 작업을 통해 전달할 리포트 템플릿.
   b. 리포트 형식: HTML, XLS 또는 PDF.
      리포트를 PDF로 변환하려면 wkhtmltopdf 툴이 필요합니다. PDF 옵션을 선택하면 중앙 관리 서버는 wkhtmltopdf 툴이 기기에 설치되어 있는지 확인합니다. 툴이 설치되어 있지 않으면 중앙 관리 서버 기기에 툴을 설치해야 한다는 메시지가 표시됩니다. 툴을 수동으로 설치하고 다음 단계로 진행합니다.

c. 리포트를 이메일로 전송할지 여부(이메일 알림 설정 포함).

이메일 주소는 최대 20개까지 지정할 수 있습니다. 이메일 주소를 구분하려면 **Enter**를 누릅니다. 또는 쉼표로 구분된 이메일 주소 목록을 붙여 넣고 **Enter**를 누릅니다.

d. 리포트를 폴더에 저장할지 여부, 이전에 해당 폴더에 저장한 리포트를 덮어쓸지 여부 및 특정 계정을 사용하여 폴더에 접근할지 여부(공유 폴더의 경우).

6. 마법사의 **작업 스케줄 구성** 단계에서 작업 시작 스케줄을 선택합니다.

다음 작업 스케줄 옵션을 사용할 수 있습니다:

- **수동 시작**

  작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **N분마다**

  작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.
  기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

- **N시간마다**

  작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.
  작업은 기본적으로 현재 시스템 날짜 및 시간부터 6시간마다 실행됩니다.

- **N일마다**

  작업이 지정된 일 단위 간격에 따라 주기적으로 실행됩니다. 또한 첫 번째 작업 실행 날짜와 시간을 지정할 수 있습니다. 이러한 추가 옵션은 작업을 생성하는 대상이 되는 애플리케이션에서 지원하는 경우 사용할 수 있습니다.
  기본적으로 작업은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- **N주마다**

  작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.
  기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

- **월별**

  이 작업은 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  지정한 날짜가 없는 달에는 해당월의 말일에 작업이 실행됩니다.
  기본적으로 이 작업은 매월 1일 현재 시스템 시간에 실행됩니다.

- **지정한 날짜에**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.

기본적으로 시작 시간은 18:00이며 날짜는 선택되지 않습니다.

해당 월의 특정 날짜 또는 주차(첫 번째 주, 두 번째 주)가 아닌 해당 월의 요일 순번을 선택한다는 점에 유의하십시오. 예를 들어, 커서를 **첫 번째** 행의 **화** 셀에 놓으면 작업이 매달 첫 번째 화요일마다 실행된다는 것을 의미합니다.

요일을 여러 개 선택할 수 있습니다.

- **바이러스 발생 시**

  바이러스 발생 이벤트가 발생하고 나면 작업이 실행됩니다. 바이러스 급증을 모니터링할 애플리케이션 유형을 선택합니다. 다음과 같은 애플리케이션 유형을 사용할 수 있습니다:

  - 워크스테이션 및 파일 서버용 안티 바이러스
  - 경계 방어용 안티 바이러스
  - 메일 시스템용 안티 바이러스

  기본적으로 모든 애플리케이션 유형이 선택되어 있습니다.

  바이러스 발생을 보고하는 보안 애플리케이션 유형에 따라 다른 작업을 실행하고 싶을 수 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 이 옵션은 두 작업을 모두 같은 기기에 할당했을 때만 작동합니다. 예를 들어 **기기 켜기** 옵션을 사용하여 *기기 관리* 작업을 실행하고 해당 작업이 완료되면 트리거 작업으로 *바이러스 검사* 작업을 실행할 수 있습니다.

  표에서 트리거 작업과 해당 작업을 완료해야 하는 상태(**완료** 또는 **실패**)를 선택해야 합니다.

  필요하면, 다음과 같이 표에서 작업을 검색, 정렬 및 필터링할 수 있습니다.

  - 이름으로 작업을 검색하려면 검색 필드에 작업 이름을 입력합니다.
  - 정렬 아이콘을 눌러 작업을 이름순으로 정렬합니다.
    기본적으로 작업은 알파벳 오름차순으로 정렬됩니다.
  - 필터 아이콘을 클릭하고 열린 창에서 그룹으로 작업을 필터링한 다음 **적용** 버튼을 클릭합니다.

7. 마법사의 이 단계에서 다른 작업 스케줄 설정을 구성합니다:

- **작업 일정** 섹션에서 이전에 선택한 스케줄을 확인하거나 재구성하고 시간 간격 및 월/주중 특정 날짜를 설정하거나, 바이러스 급증 조건이나 다른 작업 완료를 작업 시작 트리거로 설정합니다. 해당 스케줄을 선택했다면 이 섹션에서 시작 시각을 지정할 수도 있습니다.
- **추가 설정** 섹션에서 다음 설정을 지정합니다:
  - **누락된 작업 실행**

    이 옵션은 작업을 시작하려 할 때 네트워크에 클라이언트 기기가 표시되지 않는 경우의 작업 동작을 결정합니다.

이 옵션을 활성화하면 다음에 클라이언트 기기에서 Kaspersky 애플리케이션을 실행할 때 시스템이 작업 시작을 시도합니다. 작업 스케줄이 **수동 시작**, **한번만** 또는 **즉시**인 경우 기기가 네트워크에 표시되거나 작업 범위에 포함되는 즉시 작업이 시작됩니다.

이 옵션을 중지하면 클라이언트 기기에서 스케줄된 작업만 실행됩니다. **수동 시작**, **한번만**, **즉시** 스케줄에서는 작업이 네트워크에 표시되는 클라이언트 기기에서만 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

기본적으로 이 옵션은 비활성화되어 있습니다.

- **자동으로 작업 시작 임의 지연 사용**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 내에서 무작위로 작업이 시작됩니다. 이러한 방식을 *작업 시작 분산*이라고도 합니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  분산 시작 시간은 작업이 할당되는 클라이언트 기기의 수에 따라 작업을 만들 때 자동으로 계산됩니다. 그 이후에는 작업이 항상 계산된 시작 시간에 시작됩니다. 하지만 작업 설정을 편집하거나 작업을 수동으로 시작하면 작업 시작 시각의 계산된 값이 변경됩니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

- **다음 간격으로 작업 시작 자동 임의 지연**

  이 옵션을 활성화하면 클라이언트 기기에서 지정된 시간 간격 사이에 무작위로 작업이 시작됩니다. 작업 시작을 분산시키면 스케줄된 작업을 실행할 때 많은 클라이언트 기기 요청이 동시에 중앙 관리 서버로 집중되는 것을 방지할 수 있습니다.

  이 옵션을 비활성화하면 작업이 스케줄에 따라서만 클라이언트 기기에서 시작됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 새로 고침 간격은 1분입니다.

- **작업이 다음 시간보다 오래 실행되면 중지**

  작업 완료 여부에 관계없이 지정된 시간이 경과한 후 작업이 자동으로 중지됩니다.

  실행 시간이 너무 오래 걸리는 작업을 중단(중지)하려는 경우 이 옵션을 활성화합니다.

  기본적으로 이 옵션은 비활성화되어 있습니다. 기본 작업 실행 시간은 120분입니다.

8. 마법사의 **작업을 실행할 계정 선택** 단계에서 작업 실행에 사용할 사용자 계정의 자격 증명을 지정합니다.

9. 작업 생성 후에 다른 작업 설정을 수정하려면, 마법사의 **작업 생성 마침** 단계에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다(이 옵션은 기본적으로 활성화됩니다).

10. **마침** 버튼을 클릭하여 작업을 생성하고 마법사를 닫습니다.

    리포트 전달 작업이 생성됩니다. **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화하면 작업 설정 창이 열립니다.

리포트 템플릿 삭제

리포트 템플릿을 하나 또는 여러 개 삭제하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고 → 리포트**로 이동합니다.

2. 삭제할 리포트 템플릿 옆의 확인란을 선택합니다.

3. **삭제** 버튼을 누릅니다.

4. 창이 열리면 **확인** 버튼을 눌러 사용자의 선택을 확인합니다.

선택한 리포트 템플릿이 삭제됩니다. 이러한 리포트 템플릿이 리포트 전달 작업에 포함되었던 경우 해당 작업에서도 제거됩니다.

이벤트 및 이벤트 선택

이 섹션에서는 이벤트 및 이벤트 선택, Kaspersky Security Center 구성 요소에서 발생하는 이벤트 유형, 자주 발생하는 이벤트 차단 관리에 대한 정보를 제공합니다.

Kaspersky Security Center 이벤트 정보

Kaspersky Security Center에서는 관리 중인 기기에 설치된 중앙 관리 서버 및 Kaspersky 애플리케이션의 작동 중 발생한 이벤트 정보를 볼 수 있습니다. 이벤트에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다.

이벤트 유형

Kaspersky Security Center에는 다음과 같은 유형의 이벤트가 있습니다:

- 일반 이벤트. 이러한 이벤트는 모든 관리 중인 Kaspersky 애플리케이션에서 발생합니다. 일반 이벤트의 예로 바이러스 발생가 있습니다. 일반 이벤트에서는 구문과 의미를 엄격하게 정의합니다. 일반 이벤트는 리포트와 대시보드 등에 사용합니다.

- 관리 중인 Kaspersky 애플리케이션별 이벤트. 각 관리 중인 Kaspersky 애플리케이션에는 자체 이벤트 집합이 있습니다.

이벤트 소스

이벤트는 다음 애플리케이션에서 생성할 수 있습니다.

- Kaspersky Security Center 구성 요소:
  - 중앙 관리 서버
  - 네트워크 에이전트
  - iOS MDM 서버
  - Exchange 모바일 기기 서버
- 관리 중인 Kaspersky 애플리케이션

  관리 중인 Kaspersky 애플리케이션에서 생성된 이벤트에 대한 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.

애플리케이션 정책의 **이벤트 구성** 탭에서 애플리케이션에서 생성할 수 있는 이벤트의 전체 목록을 볼 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 볼 수 있습니다.

이벤트의 중요성 수준

각 이벤트에는 고유한 심각도가 있습니다. 발생 조건에 따라 이벤트에는 여러 심각도가 할당될 수 있습니다. 네 가지 심각도가 있습니다.

- *심각 이벤트*는 데이터 손실, 운영상의 오작동, 심각한 오류 등을 초래할 수 있는 심각한 문제 발생을 나타내는 이벤트입니다.
- *기능 실패*는 애플리케이션 작동 중이나 절차 수행 중에 심각한 문제, 오류 또는 오작동이 발생했음을 나타내는 이벤트입니다.
- *경고*는 반드시 심각한 것은 아니지만 향후 문제 발생 가능성을 나타내는 이벤트입니다. 이벤트 발생 후 데이터나 기능 손실 없이 애플리케이션을 복원할 수 있는 경우 대부분의 이벤트는 경고로 지정됩니다.
- *정보* 이벤트는 정상적인 작업 완료, 적절한 애플리케이션 작동 또는 절차 완료에 대해 알리기 위해 발생하는 이벤트입니다.

각 이벤트에는 정의된 저장 기간이 있으며, 이 시간 동안 Kaspersky Security Center에서 이벤트를 보거나 수정할 수 있습니다. 정의된 저장 기간이 0이어서 기본적으로 중앙 관리 서버 데이터베이스에 저장되지 않는 이벤트도 있습니다. 1일 이상 중앙 관리 서버 데이터베이스에 저장되는 이벤트만 외부 시스템으로 내보낼 수 있습니다.

이벤트 조회 사용

이벤트 조회는 중앙 관리 서버 데이터베이스에서 선택한 이벤트를 미리 정의된 조회 항목을 사용해 화면에 그 결과를 보여 줍니다. 이러한 이벤트 세트는 다음 카테고리에 따라 그룹화됩니다:

- 심각도 기준 — **심각 이벤트**, **기능 실패**, **경고** 및 **정보 이벤트**
- 시간 기준 — **최근 이벤트**
- 유형 기준 - **사용자 개선 요청 사항** 및 **감사 이벤트**

구성을 위해 Kaspersky Security Center 웹 콘솔 인터페이스에서 사용할 수 있는 설정에 따라 사용자 지정 이벤트 조회를 생성하고 볼 수 있습니다.

이벤트 조회는 **이벤트 선택**를 눌러 Kaspersky Security Center 웹 콘솔의 **모니터링 및 보고** 섹션에서 사용할 수 있습니다.

기본적으로 이벤트 조회에는 지난 7일 동안의 정보가 포함됩니다.

Kaspersky Security Center에는 기본 이벤트(미리 정의된) 조회가 있습니다.

- 심각도 레벨이 서로 다른 이벤트:
  - **심각 이벤트**
  - **기능 실패**
  - **경고**
  - **정보 이벤트**
- **사용자 요청**(관리 중인 애플리케이션의 이벤트)

- **최근 이벤트**(지난주)
- **감사 이벤트**.

추가 사용자 정의 조회를 만들고 구성할 수도 있습니다. 사용자 정의 조회에서는 이벤트가 생성된 기기의 속성(기기 이름, IP 범위 및 관리 그룹), 이벤트 유형과 심각도, 애플리케이션 및 구성 요소 이름, 그리고 시간 간격을 기준으로 이벤트를 필터링할 수 있습니다. 검색 범위에 작업 결과를 포함할 수도 있습니다. 단어를 하나 또는 여러 개 입력할 수 있는 간단한 검색 필드를 사용할 수도 있습니다. 이벤트 이름, 설명, 구성 요소 이름 등의 속성에 입력한 단어가 하나라도 포함된 모든 이벤트가 표시됩니다.

미리 정의된 조회와 사용자 정의 조회 둘 다에 대해 표시되는 이벤트 수나 검색할 레코드 수를 제한할 수 있습니다. 이 두 옵션은 모두 Kaspersky Security Center가 이벤트를 표시하는 데 걸리는 시간에 영향을 줍니다. 데이터베이스가 클수록 프로세스 시간도 더 많이 걸릴 수 있습니다.

다음 중 원하는 작업을 수행할 수 있습니다.

- 이벤트 선택 속성 편집
- 이벤트 선택 생성
- 이벤트 선택 세부정보 보기
- 이벤트 선택 삭제
- 중앙 관리 서버 데이터베이스에서 이벤트 삭제

이벤트 조회 만들기

이벤트 조회를 만들려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **모니터링 및 보고** → **이벤트 선택** 로 이동합니다.
2. **추가**를 누릅니다.
3. **새 이벤트 선택** 창이 열리면 새 이벤트 조회의 설정을 지정합니다. 창의 섹션 하나 이상에서 이 작업을 수행합니다.
4. **저장**을 눌러 변경 사항을 저장합니다.
   확인 창이 열립니다.
5. 이벤트 조회 결과를 보려면 **선택 결과로 이동** 확인란을 선택한 상태로 유지합니다.
6. **저장**을 눌러 이벤트 조회 생성을 확인합니다.

선택 결과로 이동 확인란을 선택해 둔 경우 이벤트 조회 결과가 표시됩니다. 그렇지 않으면 이벤트 조회 목록에 새 이벤트 조회가 표시됩니다.

이벤트 조회 편집

이벤트 조회를 편집하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **이벤트 선택**로 이동합니다.
2. 편집할 이벤트 조회 옆에 있는 확인란을 선택합니다.
3. **속성** 버튼을 누릅니다.
   이벤트 조회 설정 창이 열립니다.
4. 이벤트 조회의 속성을 편집합니다.

   > 미리 정의된 이벤트 조회의 경우에는 다음 탭의 속성만 편집할 수 있습니다. **일반**(조회 이름은 제외), **시간** 및 **접근 권한**.

   사용자 정의 조회의 경우에는 모든 속성을 편집할 수 있습니다.
5. **저장**을 눌러 변경 사항을 저장합니다.

편집한 이벤트 조회가 목록에 표시됩니다.

이벤트 조회 목록 보기

이벤트 조회를 보려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **모니터링 및 보고** → **이벤트 선택**로 이동합니다.
2. 시작할 이벤트 조회 옆의 확인란을 선택합니다.
3. 다음 중 하나를 수행합니다:
   - 이벤트 조회 결과에서 정렬을 구성하려면 다음을 수행합니다.
     a. **정렬 재구성 및 시작** 버튼을 클릭합니다.
     b. **이벤트 선택을 위한 정렬 재구성** 창이 표시되면 정렬 설정을 지정합니다.
     c. 조회 이름을 누릅니다.
   - 중앙 관리 서버에서 정렬된 대로 이벤트 목록을 보려는 경우에는 조회 이름을 누릅니다.

이벤트 조회 결과가 표시됩니다.

이벤트 조회 내보내기

Kaspersky Security Center를 사용하면 이벤트 조회 및 해당 설정을 KLO 파일에 저장할 수 있습니다. 이 KLO 파일을 사용하여 Kaspersky Security Center Windows 및 Kaspersky Security Center Linux로 저장된 이벤트 조회를 가져올 수 있습니다.

사용자 정의 이벤트 선택 항목만 내보낼 수 있습니다. Kaspersky Security Center 기본 세트(사전 정의된 조회)의 이벤트 조회는 파일에 저장할 수 없습니다.

이벤트 선택을 내보내려면:

1. 메인 메뉴에서 **모니터링 및 보고 → 이벤트 선택**로 이동합니다.
2. 내보낼 이벤트 선택 옆에 있는 확인란을 선택합니다.

   동시에 여러 이벤트 선택을 내보낼 수는 없습니다. 둘 이상의 조회를 선택하면 **내보내기** 버튼이 비활성화됩니다.
3. **내보내기** 버튼을 클릭합니다.
4. **다른 이름으로 저장** 창이 열리면 이벤트 선택 파일 이름과 경로를 지정한 후 **저장** 버튼을 클릭합니다.

   다른 이름으로 저장 창은 Google Chrome, Microsoft Edge, Opera를 사용 시에만 표시됩니다. 다른 브라우저 사용 시, 이벤트 선택 파일이 **다운로드** 폴더에 자동으로 저장됩니다.

이벤트 조회 가져오기

Kaspersky Security Center를 사용하면 KLO 파일에서 이벤트 조회를 가져올 수 있습니다. KLO 파일에는 내보낸 이벤트 선택과 해당 설정이 포함되어 있습니다.

이벤트 선택을 가져오려면:

1. 메인 메뉴에서 **모니터링 및 보고 → 이벤트 선택**로 이동합니다.
2. **가져오기** 버튼을 클릭한 다음 가져올 이벤트 선택 파일을 선택합니다.
3. 열린 창에서 KLO 파일의 경로를 지정한 후 **열기** 버튼을 클릭합니다. 이벤트 선택 파일은 하나만 선택할 수 있습니다.

   이벤트 선택 처리가 시작됩니다.

가져오기 결과가 포함된 알림이 표시됩니다. 이벤트 선택을 성공적으로 가져오면 **가져오기 세부 정보 보기** 링크를 클릭하여 이벤트 선택 속성을 볼 수 있습니다.

가져오기에 성공하면 이벤트 선택이 조회 목록에 표시됩니다. 이벤트 선택 설정도 가져옵니다.

새로 가져온 이벤트 선택의 이름이 기존과 같다면, 가져온 이벤트 선택의 이름은 **(<다음 시퀀스 번호>)** 인덱스로 확장됩니다(예: **(1)**, **(2)**).

이벤트 세부 정보 보기

이벤트 세부 정보를 보려면:

1. 이벤트 조회 시작.
2. 필요한 이벤트의 시간을 누릅니다.
   이벤트 속성 창이 열립니다.
3. 표시되는 창에서 다음 작업을 수행할 수 있습니다.
   - 선택한 이벤트 관련 정보를 확인합니다
   - 이벤트 선택 결과에서 다음 이벤트와 이전 이벤트로 이동합니다
   - 이벤트가 발생한 기기로 이동합니다
   - 이벤트가 발생한 기기가 포함된 관리 그룹으로 이동합니다
   - 작업과 관련된 이벤트의 경우 작업 속성으로 이동합니다

이벤트를 파일로 내보내기

Kaspersky Security Center를 사용하면 이벤트 선택 항목에서 이벤트를 TXT 파일로 저장할 수 있습니다.

이벤트를 파일로 내보내려면 다음 단계를 따릅니다.

1. 이벤트 조회 시작.
2. 필요한 이벤트 옆에 있는 확인란을 선택합니다.
   여러 개, 혹은 전체 이벤트를 선택할 수 있습니다.
3. **파일로 내보내기** 버튼을 누릅니다.

   선택한 이벤트가 TXT 파일로 내보내집니다.

이벤트에서 개체 내역 보기

리비전 관리를 지원하는 개체의 생성 또는 수정 이벤트에서 개체의 리비전 내역으로 전환할 수 있습니다.

이벤트에서 개체 내역을 보려면 다음 단계를 따릅니다.

1. 이벤트 조회 시작.
2. 필요한 이벤트 옆에 있는 확인란을 선택합니다.
3. **리비전 내역** 버튼을 클릭합니다.

   개체의 리비전 내역이 열립니다.

이벤트 삭제

이벤트를 하나 또는 여러 개 삭제하려면 다음 단계를 따릅니다.

1. 이벤트 조회 시작.
2. 필요한 이벤트 옆에 있는 확인란을 선택합니다.
3. **삭제** 버튼을 누릅니다.

   선택한 이벤트가 삭제됩니다. 삭제된 이벤트는 복원할 수 없습니다.

이벤트 조회 삭제

사용자 정의 이벤트 조회만 삭제할 수 있습니다. 미리 정의된 이벤트 조회는 삭제할 수 없습니다.

이벤트 조회를 하나 또는 여러 개 삭제하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고** → **이벤트 선택**로 이동합니다.
2. 삭제할 이벤트 조회 옆의 확인란을 선택합니다.
3. **삭제**를 클릭합니다.
4. 확인 창이 열리면 **확인**를 누릅니다.

   이벤트 조회가 삭제됩니다.

이벤트의 저장 기간 설정

Kaspersky Security Center에서는 관리 중인 기기에 설치된 중앙 관리 서버 및 Kaspersky 애플리케이션의 작동 중 발생한 이벤트 정보를 볼 수 있습니다. 이벤트에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다. 기본값으로 지정한 것보다 더 길거나 짧은 기간 동안 일부 이벤트를 저장해야 할 수 있습니다. 이벤트 저장 기간의 기본 설정을 변경할 수 있습니다.

중앙 관리 서버의 데이터베이스에 일부 이벤트를 저장하지 않으려면 중앙 관리 서버 정책 및 Kaspersky 애플리케이션 정책 또는 중앙 관리 서버 속성(중앙 관리 서버 이벤트에만 해당)에서 적절한 설정을 비활성화하면 됩니다. 이렇게 하면 데이터베이스의 이벤트 유형 수가 줄어듭니다.

이벤트의 저장 기간이 길수록 데이터베이스가 최대 용량에 더 빨리 도달합니다. 그러나 이벤트 저장 기간이 길면 더 오랜 기간 동안 모니터링 및 보고 작업을 수행할 수 있습니다.

중앙 관리 서버의 데이터베이스에서 이벤트에 대한 저장 기간을 설정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **에셋(기기)** → **정책 및 프로필**이동합니다.
2. 필요한 정책의 이름을 누릅니다.

   관리 중인 Kaspersky 애플리케이션, 네트워크 에이전트 또는 중앙 관리 서버의 정책을 선택할 수 있습니다. 중앙 관리 서버의 경우, 원하는 중앙 관리 서버 이름 옆의 설정 아이콘( )을 클릭하여 이벤트 저장 기간을 구성할 수 있습니다.
3. **이벤트 구성** 탭을 선택합니다.

   심각 관련 이벤트 유형 목록 섹션이 표시됩니다. 필요에 따라 **기능 실패**, **경고** 또는 **정보** 섹션으로 이동할 수 있습니다.
4. 오른쪽 창의 이벤트 유형 목록에서 저장 기간을 변경하려는 이벤트에 대한 링크를 누릅니다.

   창이 열리면 **이벤트 등록** 섹션에서 **다음 기간만큼 중앙 관리 서버에 저장(일)** 토글 버튼이 활성화됩니다.
5. 이 토글 버튼 아래의 편집 상자에 이벤트를 저장할 일 수를 입력합니다.
6. 중앙 관리 서버 데이터베이스에 이벤트를 저장하지 않으려면 **다음 기간만큼 중앙 관리 서버에 저장(일)** 옵션을 비활성화합니다.

   > 중앙 관리 서버 속성 창에서 중앙 관리 서버 이벤트를 구성하고 이벤트 설정이 Kaspersky Security Center 중앙 관리 서버 정책에 잠겨있는 경우, 이벤트에 대한 저장 기간 값을 재정의할 수 없습니다.
7. **확인**을 클릭한 후 오른쪽 창이 닫히면 **저장** 버튼을 누릅니다.

   정책의 속성 창이 닫힙니다.

이제부터 중앙 관리 서버가 선택한 유형의 이벤트를 수신하고 저장할 때 변경된 저장 기간이 적용됩니다. 중앙 관리 서버는 이전에 수신된 이벤트의 저장 기간을 변경하지 않습니다.

Kaspersky Security Center 구성 요소의 이벤트

각 Kaspersky Security Center 구성 요소에는 자체 이벤트 유형 집합이 있습니다. 이 섹션에는 Kaspersky Security Center 중앙 관리 서버, 네트워크 에이전트, iOS MDM 서버에서 발생하는 이벤트 유형이 나열되어 있습니다. Kaspersky 애플리케이션에서 발생하는 이벤트의 유형은 이 섹션에 나열되지 않습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

이벤트 유형 데이터 구조 설명

각 이벤트 유형에 대해 표시 이름, 식별자(ID), 알파벳 코드, 설명 및 기본 저장 기간이 제공됩니다.

- **이벤트 유형 표시 이름**. 구성한 이벤트가 발생하면 Kaspersky Security Center에 이 텍스트가 표시됩니다.
- **이벤트 유형 ID**. 이벤트 분석용 타사 도구를 사용하여 이벤트를 처리할 때 이 숫자 코드를 사용합니다.
- **이벤트 유형**(알파벳 코드). Kaspersky Security Center 데이터베이스에서 제공되는 공용 보기를 사용하여 이벤트를 찾아서 처리할 때와 SIEM 시스템으로 이벤트를 내보낼 때 이 코드를 사용합니다.
- **설명**. 이 텍스트에는 이벤트가 발생한 상황과 그러한 경우에 수행할 수 있는 작업이 포함되어 있습니다.
- **기본 저장 기간**. 이벤트가 중앙 관리 서버 데이터베이스에 저장되며 중앙 관리 서버의 이벤트 목록에 표시되는 기간(일)입니다. 이 기간이 지나면 이벤트는 삭제됩니다. 이벤트 저장 기간 값이 0이면 해당 이벤트가 탐지되기는 하지만 중앙 관리 서버의 이벤트 목록에는 표시되지 않습니다. 운영 체제 이벤트 로그에 그러한 이벤트를 저장하도록 구성한 경우에는 해당 로그에서 이벤트를 확인할 수 있습니다.

  다음과 같이 이벤트의 저장 기간을 변경할 수 있습니다:

  - 관리 콘솔: 이벤트의 저장 기간 설정
  - Kaspersky Security Center 웹 콘솔: 이벤트의 저장 기간 설정

기타 데이터에는 다음 필드가 포함될 수 있습니다.

- **event_id**: 자동으로 생성되어 할당되는 데이터베이스 내 이벤트의 고유 번호를 **이벤트 유형 ID**와 혼동하지 마십시오.
- **task_id**: 이벤트를 발생시킨 작업의 ID(있는 경우)
- **심각도**: 다음 심각도 중 하나(심각도 오름차순):

  0) 잘못된 심각도

  1) 정보

  2) 경고

  3) 오류

  4) 심각

중앙 관리 서버 이벤트

이 섹션에는 중앙 관리 서버와 관련된 이벤트에 대한 정보가 있습니다.

중앙 관리 서버 심각 이벤트

표에는 **심각** 심각도를 가진 Kaspersky Security Center 중앙 관리 서버의 이벤트가 표시됩니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

관리 콘솔의 중앙 관리 서버 속성 창에서 포트를 지정했다면 **Kaspersky Security Center**가 모니터링 및 알림 시스템인 Prometheus에서 얻을 수 있는 메트릭과 심각 이벤트를 게시합니다. Prometheus는 메트릭과 심각 이벤트를 획득한 다음 각 이벤트에 대한 경고를 생성합니다.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

중앙 관리 서버 심각 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
라이센스 제한을 초과했습니다	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Security Center는 하루에 한 번 라이센스 제한 초과 여부를 확인합니다. 이 유형의 이벤트는 중앙 관리 서버가 클라이언트 기기에 설치된 Kaspersky 애플리케이션에 의해 일부 라이센스가 그 제한이 초과되었음을 탐지하고 하나의 라이센스로 사용한 라이센스 수가 해당 라이센스에 적용된 총 구매 수의 110%를 초과하는 경우에 발생합니다. 이 이벤트가 발생하더라도 클라이언트 기기는 보호됩니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록을 살펴봅니다. 사용하지 않는 기기를 삭제합니다. • 추가 라이센스를 배포합니다(중앙 관리 서버에 유효한 활성화코드 또는 키 파일 추가). Kaspersky Security Center는 라이센스 구매 수량을 초과할 때 이벤트를 생성하는 규칙을 결정합니다.	180일
바이러스 발생	26(파일 위협 보호의 경우)	GNRL_EV_VIRUS_OUTBREAK	이 유형의 이벤트는 몇몇 관리 중인 기기에서 탐지된 악성 코드 개체 수가 짧은 기간 내에 임계값을 초과할 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 속성에서 임계값을 구성할 수 있습니다. • 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.	180일
바이러스 발생	27(메일 위협 보호의 경우)	GNRL_EV_VIRUS_OUTBREAK	이 유형의 이벤트는 몇몇 관리 중인 기기에서 탐지된 악성 코드 개체 수가 짧은 기간 내에 임계값을 초과할 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 속성에서 임계값을 구성할 수 있습니다. • 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.	180일
바이러스 발생	28(방화벽의 경우)	GNRL_EV_VIRUS_OUTBREAK	이 유형의 이벤트는 몇몇 관리 중인 기기에서 탐지된 악성 코드 개체 수가 짧은 기간 내에 임계값을 초과할 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 속성에서 임계값을 구성할 수 있습니다. • 활성화할 더 엄격한 정책을 생성하거나 이 이벤트가 발생하면 실행할 작업을 생성할 수도 있습니다.	180일
기기와의 연결이 끊어짐	4111	KLSRV_HOST_OUT_CONTROL	이 유형의 이벤트는 관리 중인 기기가 네트워크에는 나타나지만 특정 기간 동안 중앙 관리 서버에 연결되지 않은 경우에 발생합니다. 해당 기기에서 네트워크 에이전트의 정상 작동을 방해하는 것이 무엇인지 확인하십시오. 가능한 원인으로는 네트워크 문제 및 기기에서 네트워크 에이전트가 제거되었을 수 있습니다.	180일
기기 상태가 '심각'입니다	4113	KLSRV_HOST_STATUS_CRITICAL	이 유형의 이벤트는 관리 중인 기기가 *심각* 상태로 변한 경우 발생합니다. 기기 상태가 *심각*으로 변경되는 조건을 구성할 수 있습니다.	180일
키 파일이 거부 목록에 추가되었습니다	4124	KLSRV_LICENSE_BLACKLISTED	이 유형의 이벤트는 Kaspersky에서 사용자가 사용하는 활성화코드 또는 키 파일을 거부 목록에 추가한 경우 발생합니다. 자세한 내용은 기술 지원에 문의하십시오.	180일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
기능 제한 모드	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	이 유형의 이벤트는 Kaspersky Security Center가 취약점 및 패치 관리 기능과 모바일 기기 관리 기능 없이 기본 기능으로 동작하려고 할 때 발생합니다. 다음은 이벤트의 원인 및 그에 대한 대응 방안입니다: • 라이센스 기간 만료됨. 이 경우 Kaspersky Security Center의 전체 기능 모드를 사용할 수 있는 라이센스를 추가합니다(유효한 활성화코드 또는 키 파일을 중앙 관리 서버에 추가). • 중앙 관리 서버가 라이센스 제한에 지정된 것보다 더 많은 기기를 관리함. 이 경우 중앙 관리 서버의 일부 기기를 다른 중앙 관리 서버의 관리 그룹으로 이동합니다(다른 중앙 관리 서버의 라이센스 제한에 여유가 있을 경우).	180일
라이센스가 곧 만료됩니다	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	이 유형의 이벤트는 상업용 라이센스 만료 날짜가 다가오면 발생합니다. Kaspersky Security Center는 하루에 한 번 라이센스 만료일이 얼마나 남았는지 확인합니다. 이러한 유형의 이벤트는 라이센스 만료 날짜로부터 30일, 15일, 5일, 1일 전에 게시됩니다. 일 수는 변경할 수 없습니다. 라이센스 만료 날짜 이전의 지정된 날짜에 중앙 관리 서버를 끄면 이벤트는 다음날까지 게시되지 않습니다. 상업용 라이센스가 만료되면 Kaspersky Security Center에서는 기본 기능만 제공됩니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 예약 라이센스 키가 중앙 관리 서버에 추가되었는지 확인합니다. • 서브스크립션을 사용하는 경우 갱신해야 합니다. 만기일까지 서비스 공급 업체에게 선불이 완료되면 무기한 서브스크립션이 자동으로 갱신됩니다.	180일
인증서가 만료되었습니다	4132	KLSRV_CERTIFICATE_EXPIRED	모바일 기기의 클라이언트 인증서가 만료되면 이 유형의 이벤트가 발생합니다.	180일
중앙 관리 서버 인증서가 만료되었습니다.	6129	ServerCertificateExpired	모바일 기기 및 UEFI 기기의 중앙 관리 서버 인증서가 만료되면 이 유형의 이벤트가 발생합니다. 만료된 인증서를 업데이트해야 합니다.	180일
Kaspersky 애플리케이션 모듈 업데이트를 취소했습니다	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	이러한 유형의 이벤트는 Kaspersky 기술 지원 전문가가 seamless 업데이트를 철회한 경우(이 업데이트에 대해 *철회됨* 상태가 표시됨) 발생합니다. 새로운 버전으로 업데이트해야 할 경우를 예로 들 수 있습니다. 이 이벤트는 Kaspersky Security Center 패치와 관련이 있으며 관리 중인 Kaspersky 애플리케이션의 모듈과는 관련이 없습니다. 이 이벤트는 seamless 업데이트가 설치되지 않은 이유를 제공합니다.	180일
감사: SIEM으로 내보내기에 실패했습니다	5130	KLAUD_EV_SIEM_EXPORT_ERROR	이 유형의 이벤트는 SIEM 시스템 연결 오류로 인해 SIEM 시스템으로 이벤트를 내보내기에 실패할 때 발생합니다.	180일

중앙 관리 서버 기능 실패 이벤트

아래 표에는 심각도가 **기능 실패**인 Kaspersky Security Center 중앙 관리 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
런타임 오류	4125	KLSRV_RUNTIME_ERROR	이 유형의 이벤트는 알 수 없는 문제로 인해 발생합니다. 이러한 문제의 대부분은 DBMS 문제, 네트워크 문제 및 기타 소프트웨어 및 하드웨어 문제입니다. 이벤트에 대한 자세한 내용은 이벤트 설명에서 확인할 수 있습니다.	180일
유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 초과했습니다	4126	KLSRV_INVLICPROD_EXCEDED	중앙 관리 서버는 정기적으로(매시간) 이 유형의 이벤트를 생성합니다. 이 유형의 이벤트는 Kaspersky Security Center에서 타사 애플리케이션의 라이센스 키를 관리하고 설치된 개수가 타사 애플리케이션의 라이센스 키에서 설정한 제한을 초과하는 경우에 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록을 살펴봅니다. 애플리케이션이 사용되지 않는 기기에서 해당 타사 애플리케이션을 삭제합니다. • 타사 라이센스의 구매 수량을 늘립니다. 유료 애플리케이션 그룹 기능을 사용하여 타사 애플리케이션의 라이센스 키를 관리할 수 있습니다. 유료 애플리케이션 그룹에는 관리자가 지정한 기준에 부합하는 타사 애플리케이션이 들어 있습니다.	180일
클라우드 세그먼트를 검색하지 못했습니다	4143	KLSRV_KLCLOUD_SCAN_ERROR	이 유형의 이벤트는 중앙 관리 서버가 클라우드 환경에서 네트워크 세그먼트를 검색하지 못할 때 발생합니다. 이벤트 설명에서 세부 정보를 읽고 그에 따라 대응하십시오.	저장되지 않음
지정한 폴더로 업데이트 파일을 복사하지 못했습니다	4123	KLSRV_UPD_REPL_FAIL	이 유형의 이벤트는 소프트웨어 업데이트가 추가 공유 폴더에 복사될 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 해당 폴더에 접근하기 위해 사용하는 사용자 계정에 쓰기 권한이 있는지 확인합니다. • 해당 폴더의 사용자 이름 및/또는 암호가 변경되었는지 확인합니다. • 이 이벤트의 원인일 수 있는 인터넷 연결을 확인합니다. 지침에 따라 데이터베이스 및 소프트웨어 모듈을 업데이트합니다.	180일
하드 드라이브에 여유 공간이 없습니다	4107	KLSRV_DISK_FULL	이 유형의 이벤트는 중앙 관리 서버가 설치된 기기의 하드 드라이브에 여유 공간이 부족한 경우 발생합니다. 기기의 디스크 공간을 확보하십시오.	180일
공유 폴더를 사용할 수 없습니다	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	이 유형의 이벤트는 중앙 관리 서버의 공유 폴더를 사용할 수 없는 경우 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버(공유 폴더가 있는)가 켜져 있고 사용 가능한지 확인합니다. • 해당 폴더의 사용자 이름 또는 암호가 변경되었는지 확인합니다. • 네트워크 연결을 확인합니다.	180일
중앙 관리 서버 정보 데이터베이스를 이용할 수 없습니다	4109	KLSRV_DATABASE_UNAVAILABLE	이 유형의 이벤트는 중앙 관리 서버 데이터베이스를 사용할 수 없게 되면 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • SQL Server가 설치된 원격 서버를 사용할 수 있는지 확인합니다. • DBMS 로그를 보고 중앙 관리 서버 데이터베이스를 사용할 수 없는 이유를 확인합니다. 예를 들어 예방 차원의 유지 보수 때문에 SQL Server가 설치된 원격 서버를 사용할 수 없을 수 있습니다.	180일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
중앙 관리 서버 데이터베이스 공간 부족	4110	KLSRV_DATABASE_FULL	이 유형의 이벤트는 중앙 관리 서버 데이터베이스에 사용 가능한 공간이 없을 때 발생합니다. 데이터베이스 용량이 꽉 차고 데이터베이스에 추가 기록이 불가능할 경우 중앙 관리 서버가 동작하지 않습니다. 다음은 사용하는 DBMS에 따라 이 이벤트의 원인 및 해당 이벤트에 대한 적절한 대응 방안입니다: • SQL Server Express Edition DBMS를 사용하는 경우: SQL Server Express 설명서에서 현재 사용하는 버전에 대한 데이터베이스 크기 제한을 검토합니다. 아마도 중앙 관리 서버 데이터베이스가 그 데이터베이스 크기 제한을 초과했을 수 있습니다. 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한합니다. 중앙 관리 서버 데이터베이스에 애플리케이션 제어 구성 요소가 보낸 이벤트가 매우 많을 수 있습니다. 이 경우 중앙 관리 서버 데이터베이스에서 애플리케이션 제어 이벤트 저장과 관련된 Kaspersky Endpoint Security for Windows 정책 설정을 변경할 수 있습니다. • SQL Server Express Edition 이외의 DBMS를 사용하는 경우: 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한하지 않습니다. 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다. DBMS 선택에 대한 정보를 검토합니다.	180일

중앙 관리 서버 경고 이벤트

표에는 심각도가 **경고**인 Kaspersky Security Center 중앙 관리 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

중앙 관리 서버 경고 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
자주 등록된 이벤트가 탐지되었습니다		KLSRV_EVENT_SPAM_EVENTS_DETECTED	이 유형의 이벤트는 중앙 관리 서버가 관리 중인 기기에서 자주 등록된 이벤트를 감지할 때 발생합니다. 자세한 내용은 다음 섹션을 참조하십시오: 자주 등록된 이벤트 차단.	90일
라이센스 제한을 초과했습니다	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center는 하루에 한 번 라이센스 제한 초과 여부를 확인합니다. 이 유형의 이벤트는 중앙 관리 서버가 클라이언트 기기에 설치된 Kaspersky 애플리케이션에 의해 일부 라이센스가 그 제한이 초과되었음을 탐지하고 하나의 라이센스로 사용한 라이센스 수가 해당 라이센스에 적용된 총 구매 수의 100%에서 110% 이내인 경우에 발생합니다. 이 이벤트가 발생하더라도 클라이언트 기기는 보호됩니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록을 살펴봅니다. 사용하지 않는 기기를 삭제합니다. • 추가 라이센스를 배포합니다(중앙 관리 서버에 유효한 활성화코드 또는 키 파일 추가). Kaspersky Security Center는 라이센스 구매 수량을 초과할 때 이벤트를 생성하는 규칙을 결정합니다.	90일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
오랫동안 기기가 네트워크에 접속하지 않았습니다	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	이 유형의 이벤트는 관리 중인 기기가 일정 시간 동안 비활성 상태로 표시될 때 발생합니다. 대부분의 경우 관리 중인 기기가 해제될 때 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 관리 중인 기기 목록에서 기기를 수동으로 제거하십시오. • 관리 콘솔을 사용하거나 Kaspersky Security Center 웹 콘솔을 사용하여 **오랫동안 기기가 네트워크에 접속하지 않았습니다** 이벤트가 생성된 후 시간 간격을 지정하십시오. • 관리 콘솔을 사용하거나 Kaspersky Security Center 웹 콘솔을 사용하여 그룹에서 기기가 자동으로 제거된 후 시간 간격을 지정하십시오.	90일
기기 이름 중복	4102	KLSRV_EVENT_HOSTS_CONFLICT	이 유형의 이벤트는 중앙 관리 서버가 둘 이상의 관리 중인 기기를 단일 기기로 간주할 때 발생합니다. 대부분의 경우 복제된 하드 드라이브가 관리 중인 기기의 소프트웨어 배포에 사용되었으며 참조 기기에서 네트워크 에이전트를 전용 디스크 복제 모드로 전환하지 않은 경우 발생합니다. 이 문제를 방지하려면 이 기기의 하드 드라이브를 복제하기 전에 참조 기기에서 네트워크 에이전트를 디스크 복제 모드로 전환하십시오.	90일
기기 상태가 '경고'입니다	4114	KLSRV_HOST_STATUS_WARNING	이 유형의 이벤트는 관리 중인 기기가 *경고* 상태로 변한 경우 발생합니다. 기기 상태가 *경고*로 변경되는 조건을 구성할 수 있습니다.	90일
유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 곧 초과합니다	4127	KLSRV_INVLICPROD_FILLED	이 유형의 이벤트는 유료 애플리케이션 그룹에 포함된 타사 애플리케이션의 설치 수가 라이센스 키 속성에서 지정된 최대 허용 값인 90%에 도달하는 경우 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 일부 관리 중인 기기에서 타사 애플리케이션을 사용하지 않는 경우 이러한 기기에서 애플리케이션을 삭제하십시오. • 조만간 타사 애플리케이션의 설치 수가 허용된 최대 값을 초과할 것으로 예상되는 경우 더 많은 기기에 대한 타사 라이센스를 미리 확보하는 것이 좋습니다. 유료 애플리케이션 그룹 기능을 사용하여 타사 애플리케이션의 라이센스 키를 관리할 수 있습니다.	90일
인증서를 요청했습니다	4133	KLSRV_CERTIFICATE_REQUESTED	이 유형의 이벤트는 모바일 기기 관리에 대한 인증서가 자동으로 재발급되지 않을 때 발생합니다. 이벤트에 대한 원인과 적절한 대응은 다음과 같을 수 있습니다. • **가능하면 자동으로 인증서 재발급** 옵션이 비활성화된 인증서에 대한 자동 재발급이 시작되었습니다. 이는 인증서 생성 중에 발생한 오류 때문일 수 있습니다. 인증서를 수동으로 재발급해야 할 수 있습니다. • 공개 키 인프라와 통합을 사용하는 경우 PKI와의 통합 및 인증서 발급에 사용되는 계정의 SAM-Account-Name 특성이 누락된 것이 원인일 수 있습니다. 계정 속성을 검토하십시오.	90일
인증서가 제거되었습니다	4134	KLSRV_CERTIFICATE_REMOVED	이 유형의 이벤트는 관리자가 모바일 기기 관리에 대한 모든 유형의 인증서(일반, 메일, VPN)를 제거할 때 발생합니다. 인증서를 제거한 후에는 이 인증서를 통해 연결된 모바일 기기를 중앙 관리 서버에 연결할 수 없습니다. 이 이벤트는 모바일 기기 관리와 관련된 오작동을 조사할 때 유용할 수 있습니다.	90일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
인증서가 만료됩니다	6128	ServerCertificateExpiresSoon	모바일 기기 및 UEFI 기기의 중앙 관리 서버 인증서가 만료되면 이 유형의 이벤트가 발생합니다. 만료된 인증서를 업데이트해야 합니다.	90일
APNs 인증서가 만료되었습니다	4135	KLSRV_APN_CERTIFICATE_EXPIRED	이 유형의 이벤트는 APNs 인증서가 만료되는 경우 발생합니다. 수동으로 APNs 인증서를 갱신하고 iOS MDM 서버에 설치해야 합니다.	저장되지 않음
APNs 인증서가 곧 만료됩니다	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	이 유형의 이벤트는 APNs 인증서가 만료되기까지 남은 기간이 14일 미만인 경우 발생합니다. APNs 인증서가 만료되면 수동으로 APNs 인증서를 갱신하고 iOS MDM 서버에 설치해야 합니다. 만료 날짜 이전에 APNs 인증서 갱신을 예약하는 것이 좋습니다.	저장되지 않음
모바일 기기로의 FCM 메시지 전송 실패	4138	KLSRV_GCM_DEVICE_ERROR	이 유형의 이벤트는 모바일 기기 관리가 Android 운영 체제를 사용하는 관리 중인 모바일 기기에 대해 FCM (Firebase Cloud Messaging)를 사용하도록 구성되고 FCM 서버가 중앙 관리 서버에서 받은 일부 요청을 처리하지 못할 때 발생합니다. 이는 관리 중인 모바일 기기 중 일부에 푸시 알림이 수신되지 않음을 의미합니다. 이벤트 설명의 세부 정보에서 HTTP 코드를 읽고 그에 따라 대응하십시오. FCM 서버에서 수신한 HTTP 코드 및 관련 오류에 대한 자세한 내용은 Firebase 서비스 문서('다운스트림 메시지 오류 대응 코드')를 참조하십시오.	90일
FCM 서버에 FCM 메시지를 전송할 때 HTTP 오류 발생	4139	KLSRV_GCM_HTTP_ERROR	이 유형의 이벤트는 모바일 기기 관리가 FCM (Firebase Cloud Messaging)를 사용하여 Android 운영 체제를 사용하는 관리 중인 모바일 기기를 연결하도록 모바일 기기 관리를 구성하고 FCM 서버가 200(OK) 이외의 HTTP 코드를 사용하여 중앙 관리 서버 요청으로 돌아갈 때 발생합니다. 이벤트에 대한 원인과 적절한 대응은 다음과 같을 수 있습니다. • FCM 서버 측의 문제입니다. 이벤트 설명의 세부 정보에서 HTTP 코드를 읽고 그에 따라 대응하십시오. FCM 서버에서 수신한 HTTP 코드 및 관련 오류에 대한 자세한 내용은 Firebase 서비스 문서('다운스트림 메시지 오류 대응 코드')를 참조하십시오. • 프록시 서버 측의 문제입니다(프록시 서버를 사용하는 경우). 이벤트 설명의 세부 정보에서 HTTP 코드를 읽고 그에 따라 대응하십시오.	90일
FCM 서버로 FCM 메시지 전송 실패	4140	KLSRV_GCM_GENERAL_ERROR	이 유형의 이벤트는 Firebase Cloud Messaging HTTP 프로토콜로 작업할 때 중앙 관리 서버 측의 예상치 못한 오류로 인해 발생합니다. 이벤트 설명에서 세부 정보를 읽고 그에 따라 대응하십시오. 문제에 대한 해결 방법을 스스로 찾을 수 없는 경우 Kaspersky 기술 지원에 문의하는 것이 좋습니다.	90일
하드 드라이브에 여유 공간이 부족합니다	4105	KLSRV_NO_SPACE_ON_VOLUMES	이 유형의 이벤트는 중앙 관리 서버가 설치된 기기의 디스크 공간이 부족한 경우 발생합니다. 기기의 디스크 공간을 확보하십시오.	90일

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
중앙 관리 서버 데이터베이스에 여유 공간이 거의 없습니다	4106	KLSRV_NO_SPACE_IN_DATABASE	이 유형의 이벤트는 중앙 관리 서버 데이터베이스의 공간이 너무 부족할 경우 발생합니다. 이 문제를 해결하지 않으면 중앙 관리 서버 데이터베이스가 곧 제한 용량에 도달하고 중앙 관리 서버가 정상 작동하지 않게 됩니다. 다음은 사용하는 DBMS에 따라 이 이벤트의 원인 및 해당 이벤트에 대한 적절한 대응 방안입니다. SQL Server Express Edition DBMS를 사용하는 경우: • SQL Server Express 설명서에서 현재 사용하는 버전에 대한 데이터베이스 크기 제한을 검토합니다. 아마도 중앙 관리 서버 데이터베이스가 곧 데이터베이스 크기 제한에 도달하려고 합니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한합니다. • 중앙 관리 서버 데이터베이스에 애플리케이션 제어 구성 요소가 보낸 이벤트가 매우 많을 수 있습니다. 이 경우 중앙 관리 서버 데이터베이스에서 애플리케이션 제어 이벤트 저장과 관련된 Kaspersky Endpoint Security for Windows 정책 설정을 변경할 수 있습니다. SQL Server Express Edition 이외의 DBMS를 사용하는 경우: • 중앙 관리 서버 데이터베이스에 저장할 이벤트 수를 제한하지 않습니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다. DBMS 선택에 대한 정보를 검토합니다.	90일
보조 중앙 관리 서버와의 연결이 중단되었습니다	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	이 유형의 이벤트는 보조 중앙 관리 서버에 대한 연결이 끊어지는 경우 발생합니다. 보조 중앙 관리 서버가 설치된 기기에서 Kaspersky 이벤트 로그를 읽고 그에 따라 대응하십시오.	90일
기본 중앙 관리 서버와의 연결이 중단되었습니다	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	이 유형의 이벤트는 기본 중앙 관리 서버에 대한 연결이 끊어지는 경우 발생합니다. 기본 중앙 관리 서버가 설치된 기기에서 Kaspersky 이벤트 로그를 읽고 그에 따라 대응하십시오.	90일
새로운 Kaspersky 애플리케이션 모듈 업데이트가 등록되었습니다	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	이 유형의 이벤트는 중앙 관리 서버가 설치 승인이 필요한 관리 중인 기기에 설치된 Kaspersky 소프트웨어에 대한 새 업데이트를 등록하는 경우 발생합니다. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 사용하여 업데이트를 승인 또는 거부하십시오.	90일
데이터베이스의 이벤트 수 제한을 초과하여 이벤트 삭제가 시작되었습니다	4145	KLSRV_EVP_DB_TRUNCATING	이 유형의 이벤트는 중앙 관리 서버 데이터베이스가 제한 용량에 도달한 후 중앙 관리 서버 데이터베이스의 이전 이벤트를 삭제하기 시작한 경우에 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 데이터베이스에 저장되는 최대 이벤트 수를 변경합니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다.	저장되지 않음
데이터베이스의 이벤트 수 제한을 초과하여 이벤트가 삭제되었습니다	4146	KLSRV_EVP_DB_TRUNCATED	이 유형의 이벤트는 중앙 관리 서버 데이터베이스가 제한 용량에 도달한 후 중앙 관리 서버 데이터베이스의 이전 이벤트가 삭제된 경우에 발생합니다. 다음과 같은 방법으로 이벤트에 대응할 수 있습니다: • 중앙 관리 서버 데이터베이스에 저장되는 최대 허용 이벤트 수를 변경합니다. • 중앙 관리 서버 데이터베이스에 저장할 이벤트 목록을 줄입니다.	저장되지 않음

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
감사(SIEM 서버 테스트 연결 실패)	5120	KLAUD_EV_SIEM_TEST_FAILED	이 유형의 이벤트는 SIEM 서버에 대한 연결 테스트가 실패했을 때 발생합니다.	30일
인증서를 자동 발급하지 못했습니다		KLSRV_인증서_자동_발급_오류	이 이벤트는 모바일 기기(모바일 프로토콜에 따라 작동하는 기기)를 위한 클라이언트 인증서를 생성하는 동안 오류가 발생했을 때 일어납니다.	90일

중앙 관리 서버 정보 이벤트

표에는 심각도가 **정보**인 Kaspersky Security Center 중앙 관리 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 보고 구성할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

중앙 관리 서버 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간	비고
현재 라이센스 키를 90% 이상 사용했습니다	4097	KLSRV_EV_LICENSE_CHECK_90	30일	
새 기기가 탐지되었습니다	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30일	
기기가 자동으로 그룹에 추가되었습니다	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30일	
기기가 규칙에 따라 그룹으로 자동 이동되었습니다	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30일	
기기가 네트워크에 오랫동안 접속하지 않아 그룹에서 삭제되었습니다	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30일	
유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 곧 초과합니다(95% 이상 사용 중)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30일	
분석을 위해 Kaspersky로 전송해야 할 파일이 있습니다	4131	KLSRV_APS_FILE_APPEARED	30일	
FCM 인스턴스 ID가 이 모바일 기기에서 변경되었습니다	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30일	
업데이트 파일이 지정한 폴더에 복사되었습니다	4122	KLSRV_UPD_REPL_OK	30일	
보조 중앙 관리 서버에 연결되었습니다	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30일	
기본 중앙 관리 서버에 연결되었습니다	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30일	
데이터베이스가 업데이트되었습니다	4144	KLSRV_UPD_BASES_UPDATED	30일	
감사: 중앙 관리 서버로의 연결이 확립되었습니다	4147	KLAUD_EV_SERVERCONNECT	30일	이러한 유형의 이벤트는 사용자가 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔을 사용하여 중앙 관리 서버에 연결할 때 발생합니다. 이러한 이벤트에는 MMC 기반 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 서버가 설치된 기기의 IP 주소에 대한 정보가 포함됩니다.

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간	비고
감사: 개체가 수정되었습니다	4148	KLAUD_EV_OBJECTMODIFY	30일	이 이벤트는 다음 개체의 변경 사항을 추적합니다. • 관리 그룹 • 보안 그룹 • 사용자 • 패키지 • 작업 • 정책 • 서버 • 가상 서버
감사: 개체 상태가 변경되었습니다	4150	KLAUD_EV_TASK_STATE_CHANGED	30일	예를 들어 이 이벤트는 오류로 작업이 실패했을 때 발생합니다.
감사: 그룹 설정이 수정되었습니다	4149	KLAUD_EV_ADMGROUP_CHANGED	30일	
감사: 중앙 관리 서버와의 연결이 종료되었습니다	4151	KLAUD_EV_SERVERDISCONNECT	30일	
감사: 개체 속성이 수정되었습니다	4152	KLAUD_EV_OBJECTPROPMODIFIED	30일	이 이벤트는 다음 속성의 변경 사항을 추적합니다. • 사용자 • 라이센스 • 서버 • 가상 서버
감사: 사용자 권한이 수정되었습니다	4153	KLAUD_EV_OBJECTACLMODIFIED	30일	
감사: 중앙 관리 서버에서 암호화 키를 가져오거나 내보냈습니다	5100	KLAUD_EV_DPEKEYSEXPORT	30일	
감사: SIEM 서버 테스트 연결 성공	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30일	이 이벤트는 SIEM 서버에 대한 연결 테스트가 성공했을 때 발생합니다.
예약 인증서가 생성되었습니다		서버 예약 인증서 생성됨	30일	이 이벤트는 중앙 관리 서버 인증서를 생성하면 발생합니다.
인증서 갱신		서버 인증서 갱신됨	30일	이 이벤트는 중앙 관리 서버 인증서를 갱신하면 발생합니다.

예약 인증서가 생성되었습니다 및 **인증서 갱신** 이벤트는 모바일 기기 및 UEFI 기기용 중앙 관리 서버 인증서에 대해 이러한 이벤트에 해당하는 작업이 수행될 때만 중앙 관리 서버에서 자동으로 게시되며 관리 콘솔에 표시됩니다.

네트워크 에이전트 이벤트

이 섹션에는 네트워크 에이전트와 관련된 이벤트에 대한 정보가 있습니다.

네트워크 에이전트 기능 실패 이벤트

표에는 **기능 실패** 심각도가 포함된 Kaspersky Security Center 네트워크 에이전트 이벤트가 표시됩니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

네트워크 에이전트 기능 실패 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	설명	기본 저장 기간
업데이트 설치 오류	7702	KLNAG_EV_PATCH_INSTALL_ERROR	이 유형의 이벤트는 Kaspersky Security Center 구성 요소에 대한 자동 업데이트 및 패치에 실패한 경우에 발생합니다. 이 이벤트는 관리 중인 Kaspersky 애플리케이션의 업데이트와 관련이 없습니다. 이벤트 설명을 읽습니다. 중앙 관리 서버의 Windows 문제가 이 이벤트의 원인일 수 있습니다. 이벤트 설명에 Windows 구성 문제가 언급되어 있으면 이 문제를 해결하십시오.	30일
타사 소프트웨어 업데이트를 설치하지 못했습니다	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	이 유형의 이벤트는 취약점 및 패치 관리와 모바일 기기 관리 기능이 사용 중이고 타사 소프트웨어를 업데이트하지 못했을 때 발생합니다. 타사 소프트웨어에 대한 링크가 올바른지 확인합니다. 이벤트 설명을 읽습니다.	30일
Windows 업데이트 패치를 설치하지 못했습니다	7717	KLNAG_EV_WUA_INSTALL_ERROR	이 유형의 이벤트는 Windows 업데이트에 실패했을 때 발생합니다. 네트워크 에이전트 정책에서 Windows 업데이트 구성. 이벤트 설명을 읽습니다. Microsoft 기술 자료에서 오류를 찾습니다. 문제를 직접 해결할 수 없는 경우 Microsoft 기술 지원에 문의합니다.	30일
사용자 관리: 오류	7723	KLNAG_EV_USR_MNG_ERR	일반 경고 이벤트.	30일
Sudoers 파일을 참조값으로 복구하지 못했습니다	7726	KLNAG_EV_SUDOER_RESTORED_ERR	이벤트는 sudoers 파일 대체 오류 설명을 포함합니다.	30일
루트 인증서를 설치하지 못했습니다	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	이벤트는 인증서 설치 오류 설명을 포함합니다.	30일
루트 인증서를 제거하지 못했습니다	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	이벤트는 인증서 제거 오류 설명을 포함합니다.	30일

네트워크 에이전트 경고 이벤트

아래의 표에 **경고** 심각도를 가진 Kaspersky Security Center 네트워크 에이전트의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

네트워크 에이전트 경고 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간
소프트웨어 모듈 업데이트 설치 시 경고가 발생했습니다	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30일
타사 소프트웨어 업데이트 설치가 완료했지만 경고 메시지가 있습니다	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30일
타사 소프트웨어 업데이트 설치가 연기되었습니다	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30일
보안 문제가 발생했습니다	549	GNRL_EV_APP_INCIDENT_OCCURED	30일
KSN 프록시가 시작되었지만 KSN 이용 가능 여부를 확인하지 못했습니다	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30일
사용자 관리: 경고	7722	KLNAG_EV_USR_MNG_WRN	30일
찾은 Sudoers 파일이 참조값과 일치하지 않습니다	7724	KLNAG_EV_SUDOER_DIFFERENT	30일

네트워크 에이전트 정보 이벤트

아래 표에는 **정보** 심각도를 가진 Kaspersky Security Center 네트워크 에이전트의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

네트워크 에이전트 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간
소프트웨어 모듈 업데이트를 설치했습니다	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30일
소프트웨어 모듈 업데이트 설치를 시작했습니다	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30일
애플리케이션을 설치했습니다	7703	KLNAG_EV_INV_APP_INSTALLED	30일
애플리케이션을 제거했습니다	7704	KLNAG_EV_INV_APP_UNINSTALLED	30일
감시 중인 애플리케이션이 설치되었습니다	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30일
감시 중인 애플리케이션이 제거되었습니다	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30일
타사 애플리케이션이 설치되었습니다	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30일
새 기기가 추가되었습니다	7708	KLNAG_EV_DEVICE_ARRIVAL	30일
기기가 제거되었습니다	7709	KLNAG_EV_DEVICE_REMOVE	30일
새 기기가 탐지되었습니다	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30일
기기가 인증되었습니다	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30일
Windows Desktop Sharing: 파일을 읽음	7712	KLUSRLOG_EV_FILE_READ	30일
Windows Desktop Sharing: 파일을 수정함	7713	KLUSRLOG_EV_FILE_MODIFIED	30일
Windows Desktop Sharing: 애플리케이션을 시작함	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30일
Windows Desktop Sharing: 시작됨	7715	KLUSRLOG_EV_WDS_BEGIN	30일
Windows Desktop Sharing: 중지됨	7716	KLUSRLOG_EV_WDS_END	30일
타사 소프트웨어 업데이트가 설치되었습니다	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30일
타사 소프트웨어 업데이트 설치가 시작되었습니다	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30일
KSN 프록시가 시작되었습니다. KSN 이용 가능 여부 확인 성공	7719	KSNPROXY_STARTED_CON_CHK_OK	30일
KSN 프록시가 중지되었습니다	7720	KSNPROXY_STOPPED	30일

iOS MDM 서버 이벤트

이 섹션에는 iOS MDM 서버와 관련된 이벤트에 대한 정보가 있습니다.

iOS MDM 서버 기능 실패 이벤트

표에는 **기능 실패** 심각도를 가진 Kaspersky Security Center iOS MDM 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

iOS MDM 서버 기능 실패 이벤트

이벤트 유형 표시 이름	이벤트 유형	기본 저장 기간
프로필 목록 요청 실패	PROFILELIST_COMMAND_FAILED	30일
프로필 설치 실패	INSTALLPROFILE_COMMAND_FAILED	30일
프로필 삭제 실패	REMOVEPROFILE_COMMAND_FAILED	30일
프로비저닝 프로필 목록 요청 실패	PROVISIONINGPROFILELIST_COMMAND_FAILED	30일
프로비저닝 프로필 설치 실패	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30일
프로비저닝 프로필 삭제 실패	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30일
디지털 인증서 목록 요청 실패	CERTIFICATELIST_COMMAND_FAILED	30일
설치된 애플리케이션 목록 요청 실패	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30일
모바일 기기에 대한 일반 정보 요청 실패	DEVICEINFORMATION_COMMAND_FAILED	30일
보안 정보 요청 실패	SECURITYINFO_COMMAND_FAILED	30일
모바일 기기 잠금 실패	DEVICELOCK_COMMAND_FAILED	30일
암호 초기화 실패	CLEARPASSCODE_COMMAND_FAILED	30일
모바일 기기에서 데이터 삭제 실패	ERASEDEVICE_COMMAND_FAILED	30일
앱 설치 실패	INSTALLAPPLICATION_COMMAND_FAILED	30일
앱에 대한 교환 코드 설정 실패	APPLYREDEMPTIONCODE_COMMAND_FAILED	30일
관리 중인 앱 목록 요청 실패	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30일
관리 중인 앱 제거 실패	REMOVEAPPLICATION_COMMAND_FAILED	30일
로밍 설정 거부	SETROAMINGSETTINGS_COMMAND_FAILED	30일
앱 동작 중 오류 발생	PRODUCT_FAILURE	30일
명령 결과에 잘못된 데이터가 있습니다	MALFORMED_COMMAND	30일
푸시 알림 전송 실패	SEND_PUSH_NOTIFICATION_FAILED	30일
명령 전송 실패	SEND_COMMAND_FAILED	30일
기기를 찾을 수 없습니다	DEVICE_NOT_FOUND	30일

iOS MDM 서버 경고 이벤트

아래 표에는 **경고** 심각도를 가진 Kaspersky Security Center iOS MDM 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

iOS MDM 서버 경고 이벤트

이벤트 유형 표시 이름	이벤트 유형	기본 저장 기간
잠긴 모바일 기기로의 연결 시도가 탐지되었습니다	INACTICE_DEVICE_TRY_CONNECTED	30일
프로필이 삭제되었습니다	MDM_PROFILE_WAS_REMOVED	30일
클라이언트 인증서를 재사용하려는 시도가 탐지되었습니다	CLIENT_CERT_ALREADY_IN_USE	30일
비활성 기기가 탐지되었습니다	FOUND_INACTIVE_DEVICE	30일
교환 코드가 필요합니다	NEED_REDEMPTION_CODE	30일
정책에 포함된 프로필이 기기에서 제거되었습니다	UMDM_PROFILE_WAS_REMOVED	30일

iOS MDM 서버 정보 이벤트

표에는 **정보** 심각도를 가진 Kaspersky Security Center iOS MDM 서버의 이벤트가 나와 있습니다.

애플리케이션에서 생성할 수 있는 각 이벤트에 대해 애플리케이션 정책의 **이벤트 구성** 탭에서 알림 설정 및 스토리지 설정을 지정할 수 있습니다. 모든 이벤트에 대한 알림 설정을 한 번에 구성하려면 중앙 관리 서버 속성에서 일반 알림 설정을 구성합니다.

iOS MDM 서버 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형	기본 저장 기간
새 모바일 기기가 연결되었습니다	NEW_DEVICE_CONNECTED	30일
프로필 목록을 성공적으로 요청했습니다	PROFILELIST_COMMAND_SUCCESSFULL	30일
프로필을 성공적으로 설치했습니다	INSTALLPROFILE_COMMAND_SUCCESSFULL	30일
프로필을 성공적으로 삭제했습니다	REMOVEPROFILE_COMMAND_SUCCESSFULL	30일
프로비저닝 프로필 목록을 성공적으로 요청했습니다	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30일
프로비저닝 프로필을 성공적으로 설치했습니다	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30일
프로비저닝 프로필을 성공적으로 제거했습니다	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30일
디지털 인증서 목록을 성공적으로 요청했습니다	CERTIFICATELIST_COMMAND_SUCCESSFULL	30일
설치된 애플리케이션 목록을 성공적으로 요청했습니다	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30일
모바일 기기에 대한 일반 정보를 성공적으로 요청했습니다	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30일
보안 정보를 성공적으로 요청했습니다	SECURITYINFO_COMMAND_SUCCESSFULL	30일
모바일 기기가 성공적으로 잠겼습니다	DEVICELOCK_COMMAND_SUCCESSFULL	30일
암호를 성공적으로 초기화했습니다	CLEARPASSCODE_COMMAND_SUCCESSFULL	30일
모바일 기기에서 데이터를 성공적으로 삭제했습니다	ERASEDEVICE_COMMAND_SUCCESSFULL	30일
앱을 성공적으로 설치했습니다	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30일
이 앱에 대해 교환 코드를 성공적으로 설정했습니다	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30일
관리 중인 앱 목록을 성공적으로 요청했습니다	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30일
관리 중인 앱을 성공적으로 제거했습니다	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30일
로밍 설정을 성공적으로 적용했습니다	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30일

자주 등록된 이벤트 차단 중

이 섹션에서는 관리 중인 자주 등록된 이벤트 차단 및 자주 등록된 이벤트 차단 제거에 대한 정보를 제공합니다.

자주 등록된 이벤트 차단 정보

관리 중인 애플리케이션(예: Kaspersky Endpoint Security for Windows)이 하나 또는 여러 개의 관리 중인 기기에 설치된 경우 동일한 유형의 여러 이벤트를 중앙 관리 서버로 보낼 수 있습니다. 자주 등록된 이벤트를 수신하면 중앙 관리 서버의 데이터베이스에 과부하가 발생하고 다른 이벤트를 덮어 쓸 수 있습니다. 중앙 관리 서버는 수신된 모든 이벤트의 수가 데이터베이스에 지정된 제한을 초과하면 가장 자주 등록된 이벤트 차단을 시작합니다.

중앙 관리 서버에서는 자주 등록된 이벤트가 자동으로 수신되지 않도록 차단합니다. 자주 등록된 이벤트를 직접 차단하거나 차단할 이벤트를 선택할 수는 없습니다.

이벤트가 차단되었는지 확인하려면 알림 목록을 보거나 이 이벤트가 중앙 관리 서버 속성의 **자주 등록된 이벤트 차단 중** 섹션에 존재하는지 확인하면 됩니다. 이벤트가 차단된 경우 다음을 수행할 수 있습니다:

- 데이터베이스 덮어 쓰기를 방지하려면 이러한 유형의 이벤트 수신을 계속 차단하면 됩니다.
- 예를 들어 자주 등록된 이벤트를 중앙 관리 서버로 전송하는 이유를 알아보려면 자주 등록된 이벤트의 차단을 해제 하고 이 유형의 이벤트를 계속 수신합니다.
- 자주 등록된 이벤트가 다시 차단될 때까지 계속 수신하려면 자주 등록된 이벤트 차단에서 제거하면 됩니다.

자주 등록된 이벤트 차단 관리

중앙 관리 서버는 자주 등록된 이벤트의 수신을 자동으로 차단하지만 차단을 해제하고 자주 등록된 이벤트를 계속 수신할 수 있습니다. 이전에 차단 해제한 자주 등록된 이벤트 수신을 차단할 수도 있습니다.

자주 등록된 이벤트 차단을 관리하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **자주 등록된 이벤트 차단 중** 섹션을 선택합니다.
3. **자주 등록된 이벤트 차단 중** 섹션에서:
   - 자주 등록된 이벤트 수신을 차단 해제하려면 다음을 따르십시오.
     a. 차단 해제할 자주 등록된 이벤트를 선택한 다음, **제외** 버튼을 누릅니다.
     b. **저장** 버튼을 누릅니다.
   - 자주 등록된 이벤트 수신을 차단하려면 다음을 따르십시오.
     a. 차단할 자주 등록된 이벤트를 선택한 다음, **차단** 버튼을 누릅니다.
     b. **저장** 버튼을 누릅니다.

중앙 관리 서버는 차단 해제된 자주 등록된 이벤트를 수신하고 차단된 자주 등록된 이벤트는 수신하지 않습니다.

자주 등록된 이벤트 차단 제거

자주 등록된 이벤트에 대한 차단을 제거하고 중앙 관리 서버에서 이러한 자주 등록된 이벤트를 다시 차단할 때까지 수신하기 시작할 수 있습니다.

자주 등록된 이벤트 차단 제거하기:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **자주 등록된 이벤트 차단 중** 섹션을 선택합니다.

3. **자주 등록된 이벤트 차단 중** 섹션에서 차단을 제거하려는 자주 등록된 이벤트 유형을 선택합니다.

4. **차단에서 제거** 버튼을 누릅니다.

자주 등록된 이벤트가 자주 등록된 이벤트 목록에서 제거됩니다. 중앙 관리 서버에서 이 유형의 이벤트를 수신합니다.

Kaspersky Security for Microsoft Exchange Servers에서 이벤트 수신

Kaspersky Endpoint Security for Windows와 같은 관리 중인 애플리케이션 작동 중 이벤트에 대한 정보는 관리 중인 기기에서 전송되어 중앙 관리 서버 데이터베이스에 등록됩니다. 기본적으로 Kaspersky Security for Microsoft Exchange Server 버전 9.0 MR6 이하의 이벤트는 중앙 관리 서버 데이터베이스에 등록되지 않습니다. Kaspersky Security for Microsoft Exchange Server 9.0 MR6 또는 이전 버전이 조직의 관리 중인 기기에 설치되어 있고 이 애플리케이션에서 이벤트를 수신하려면 klscflag 유틸리티를 사용하여 이 애플리케이션에 대한 이벤트 등록을 활성화하십시오.

Kaspersky Security for Microsoft Exchange Server에 대한 이벤트 등록을 활성화하려면:

1. 중앙 관리 서버 기기에서 관리자 권한이 있는 계정으로 Windows 명령 프롬프트를 실행합니다.

2. 현재 디렉터리를 Kaspersky Security Center 설치 폴더(일반적으로 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center)로 변경합니다.

3. 다음 명령 중 하나를 실행합니다:

   - Windows Server 장애 조치 클러스터에 설치된 중앙 관리 서버:

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Kaspersky Security Center 장애 조치 클러스터 노드에 설치된 중앙 관리 서버:

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - 클러스터에서 작동하지 않는 중앙 관리 서버:

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

Kaspersky Security for Microsoft Exchange Server에 대한 이벤트 등록이 활성화되었습니다.

Kaspersky Security for Microsoft Exchange Server의 경우 이벤트의 저장 기간을 설정하거나 중앙 관리 서버 저장소에 저장해야 하는 이벤트를 선택할 수 없습니다. 저장소에 저장할 수 있는 최대 이벤트 수를 설정할 수 있습니다. 이 설정은 모든 Kaspersky 애플리케이션에서 수신된 이벤트에 적용됩니다.

알림 및 기기 상태

이 섹션에는 알림을 확인하고, 알림 전달을 구성하고, 기기 상태를 사용하고, 기기 상태 변경을 활성화하는 방법에 대한 정보가 포함되어 있습니다.

알림 사용

알림을 통해 이벤트에 대해 경고하고 적절하다고 생각하는 권장 작업을 하나 또는 여러 개 수행하여 이러한 이벤트에 대한 응답 속도를 높일 수 있습니다.

선택한 알림 방법에 따라 다음 유형의 알림을 사용할 수 있습니다.

- 화면 알림
- SMS로 알림
- 이메일로 알림
- 실행 파일 또는 스크립트로 알림

화면 알림

화면 알림은 심각도(*심각*, *경고* 및 *정보*)별로 그룹화된 이벤트에 대해 경고합니다.

화면 알림은 다음 두 가지 상태 중 하나일 수 있습니다.

- *검토됨*. 알림에 대해 권장되는 작업을 수행했거나 알림에 대해 이 상태를 수동으로 할당했음을 의미합니다.
- *검토되지 않음*. 알림에 대해 권장되는 작업을 수행하지 않았거나 알림에 대해 이 상태를 수동으로 할당하지 않았음을 의미합니다.

기본적으로 알림 목록에는 *검토되지 않음* 상태의 알림이 포함됩니다.

화면 알림을 확인하고 실시간으로 응답하여 조직의 네트워크를 모니터링할 수 있습니다.

이메일, SMS, 실행 파일 또는 스크립트로 알림

Kaspersky Security Center는 중요하다고 생각하는 모든 이벤트에 대한 알림을 전송하여 조직의 네트워크를 모니터링하는 기능을 제공합니다. 모든 이벤트에 대해 이메일, SMS를 통해 또는 실행 파일이나 스크립트를 실행하여 알림을 구성할 수 있습니다.

이메일 또는 SMS로 알림을 받으면 이벤트에 대한 응답을 결정할 수 있습니다. 이 응답은 조직의 네트워크에 가장 적합한 응답이어야 합니다. 실행 파일 또는 스크립트를 실행하여 이벤트에 대한 응답을 미리 정의합니다. 이벤트에 대한 기본 응답으로 실행 파일 또는 스크립트 실행을 고려할 수도 있습니다. 실행 파일을 실행한 후 다른 단계를 수행하여 이벤트에 응답할 수 있습니다.

화면 알림 보기

다음 세 가지 방법으로 화면에서 알림을 볼 수 있습니다.

- **모니터링 및 보고 → 알림** 섹션에서. 여기에서 미리 정의된 카테고리와 관련된 알림을 볼 수 있습니다.
- 현재 사용 중인 섹션에 관계없이 열 수 있는 별도의 창에서. 이 경우 알림을 '검토됨'으로 표시할 수 있습니다.
- **모니터링 및 보고 → 대시보드** 섹션의 **선택한 심각도별 알림** 위젯에서. 이 위젯에서는 심각도가 *심각* 및 *경고*인 이벤트 알림만 볼 수 있습니다.

예를 들어, 이벤트에 응답하는 등의 작업을 수행할 수 있습니다.

미리 정의된 카테고리의 알림을 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **모니터링 및 보고 → 알림**이동합니다.
   왼쪽 창에서 **모든 정보** 카테고리를 선택하면 오른쪽 창에 모든 알림이 표시됩니다.
2. 왼쪽 창에서 카테고리 중 하나를 선택합니다.
   - **배포**
   - **기기**
   - **보호**
   - **업데이트** (여기에는 다운로드 가능한 Kaspersky 애플리케이션에 대한 알림과 다운로드된 안티 바이러스 데이터베이스 업데이트에 대한 알림이 포함됩니다)
   - **익스플로잇 방지**
   - **중앙 관리 서버** (여기에는 중앙 관리 서버와 관련된 이벤트만 포함됩니다)
   - **유용한 링크** (여기에는 Kaspersky 기술 지원, Kaspersky 포럼, 라이센스 갱신 페이지 또는 Kaspersky IT 백과사전과 같은 Kaspersky 리소스에 대한 링크가 포함됩니다)

   선택한 카테고리의 알림 목록이 표시됩니다. 목록에는 다음이 포함됩니다.

- 알림 항목과 관련된 아이콘: 배포 (), 보호 (), 업데이트 (), 기기 관리 (), 익스플로잇 방지 (), 중앙 관리 서버 ().
- 알림 심각도. 다음 중요도에 대한 알림이 표시됩니다: **중요 알림**(), **경고 알림**(), **정보 알림**. 목록의 알림은 심각도별로 그룹화됩니다.
- **알림**. 여기에는 알림에 대한 설명이 포함됩니다.
- **처리**. 여기에는 수행이 권장되는 빠른 작업에 대한 링크가 포함되어 있습니다. 예를 들어 이 링크를 누르면 저장소로 이동하여 기기에 보안 제품을 설치하거나 기기 목록 또는 이벤트 목록을 볼 수 있습니다. 알림에 대해 권장되는 작업을 수행하면 이 알림에 *검토 됨* 상태가 할당됩니다.
- **상태 등록됨**. 여기에는 알림이 중앙 관리 서버에 등록된 순간부터 경과한 일 수 또는 시간이 포함됩니다.

심각도별로 별도의 창에서 화면 알림을 보려면:

1. Kaspersky Security Center 웹 콘솔의 오른쪽 상단에서 플래그 아이콘()을 누릅니다.

   플래그 아이콘에 빨간색 점이 있으면 검토되지 않은 알림이 있는 것입니다.

   알림이 나열된 창이 열립니다. 기본적으로 **모든 정보** 탭이 선택되어 있으며 심각도에 따라 알림이 *심각*, *경고*, *정보*로 그룹화됩니다.

2. **시스템** 탭을 선택합니다.

   심각도가 *심각*() 및 *경고*()인 알림 목록이 표시됩니다. 알림 목록에는 다음이 포함됩니다.

   - 색상 마커. 심각 알림은 빨간색으로 표시됩니다. 경고 알림은 노란색으로 표시됩니다.
   - 알림 항목을 나타내는 아이콘: 배포 (), 보호 (), 업데이트 (), 기기 관리 (), 익스플로잇 방지 (), 중앙 관리 서버 ().
   - 알림에 대한 설명.
   - 플래그 아이콘. 알림에 *검토되지 않음* 상태가 할당되어 있으면 플래그 아이콘이 회색으로 표시됩니다. 회색 플래그 아이콘을 선택하고 알림에 *검토됨* 상태를 할당하면 아이콘 색상이 흰색으로 변경됩니다.
   - 권장 작업 대한 링크. 링크를 누른 후 권장 작업을 수행하면 알림이 *검토됨* 상태가 됩니다.
   - 알림이 중앙 관리 서버에 등록된 날짜 이후로 경과한 일 수.

3. **더 보기** 탭을 선택합니다.

   심각도가 *정보*인 알림 목록이 표시됩니다.

   목록의 구성은 **시스템** 탭의 목록과 동일합니다(위 설명 참조). 유일한 차이점은 색상 마커가 없다는 것입니다.

중앙 관리 서버에 등록된 날짜 간격으로 알림을 필터링할 수 있습니다. **필터 표시** 확인란을 사용하여 필터를 관리합니다.

위젯에서 화면 알림을 보려면 다음 단계를 따릅니다.

1. **대시보드** 섹션에서 **웹 위젯 추가 또는 복원**을 선택합니다.
2. 창이 열리면 **기타** 카테고리를 누르고 **선택한 심각도별 알림** 위젯을 선택한 다음 추가를 누릅니다.

   이제 위젯이 **대시보드** 탭에 표시됩니다. 기본적으로 심각도가 *심각*인 알림이 위젯에 표시됩니다.

   위젯에서 **설정** 버튼을 클릭하고 위젯 설정을 변경하여 심각도가 *경고*인 알림을 확인합니다. 또는 *경고* 심각도가 포함된 **선택한 심각도별 알림** 위젯을 추가할 수도 있습니다.

   위젯의 알림 목록은 크기에 따라 제한되며 두 개의 알림이 포함됩니다. 이 두 알림은 최신 이벤트와 관련이 있습니다.

위젯의 알림 목록에는 다음이 포함됩니다.

- 알림 항목과 관련된 아이콘: 배포 (), 보호 (), 업데이트 (), 기기 관리 (), 익스플로잇 방지 (), 중앙 관리 서버 ().
- 권장 작업에 대한 링크가 포함된 알림 설명. 링크를 누른 후 권장 작업을 수행하면 알림이 *검토됨* 상태가 됩니다.

- 알림이 중앙 관리 서버에 등록된 날짜 이후 경과한 일 수 또는 시간.
- 다른 알림에 대한 링크. 이 링크를 누르면 **모니터링 및 보고** 섹션의 **알림** 섹션에서 알림 보기로 이동합니다.

기기 상태 정보

Kaspersky Security Center는 관리 중인 기기마다 상태를 할당합니다. 특정 상태는 사용자가 정의한 조건이 충족되는지 여부에 따라 달라집니다. 기기에 상태를 할당할 때 Kaspersky Security Center에서 네트워크에 있는 기기의 가시성 플래그를 고려하는 경우가 있습니다(아래 표 참조). 예를 들어, *데이터베이스가 오래됨* 조건이 충족되어서 관리 중인 기기에 *심각* 상태가 할당되었고 나중에 기기의 가시성 플래그가 설정되었다면 기기에는 *확인* 상태가 할당됩니다. Kaspersky Security Center에서 2시간 내에 네트워크의 기기를 찾지 못하면 기기의 가시성 플래그가 *확인되지 않음*으로 설정됩니다.

상태는 다음과 같습니다.

- *심각* 또는 *심각/존재 확인*
- *경고* 또는 *경고/존재 확인*
- *확인* 또는 *확인/존재 확인*

아래 표에는 기기에 *심각* 또는 *경고* 상태를 할당하기 위해 충족해야 하는 기본 조건과 가능한 모든 값이 나와 있습니다.

기기에 상태를 할당하기 위한 조건

조건	조건 설명	사용 가능한 값
보안 제품이 설치 안 됨	기기에 네트워크 에이전트는 설치되어 있는데 보안 제품은 설치되어 있지 않습니다.	• 토글 버튼이 켜져 있습니다. • 토글 버튼이 꺼져 있습니다.
바이러스가 너무 많이 탐지됨	*악성 코드 검사* 작업 등의 바이러스 탐지 작업을 통해 기기에서 일부 바이러스가 발견되었으며, 발견된 바이러스 수가 지정된 값을 초과합니다.	0개 이상
실시간 보호 레벨이 관리자가 설정한 레벨과 다름	기기가 네트워크에 연결되었지만 실시간 보호 레벨이 조건에서 기기 상태에 대해 관리자가 설정한 레벨과 다릅니다.	• 중지됨 • 일시 중지됨 • 실행 중
오랫동안 악성 코드를 검사하지 않음	기기가 네트워크에 표시되며 보안 제품이 기기에 설치되어 있지만, *악성 코드 검사* 작업과 로컬 검사 작업이 지정된 시간 간격보다 오랫동안 실행되지 않았습니다. 이 조건은 중앙 관리 서버 데이터베이스에 추가된 지 7일 이상이 지난 기기에만 해당됩니다.	1일 이상
데이터베이스가 오래됨	기기가 네트워크에 표시되며 보안 제품이 기기에 설치되어 있지만 지정된 시간 간격보다 오랫동안 이 기기에서 안티 바이러스 데이터베이스가 업데이트되지 않았습니다. 이 조건은 중앙 관리 서버 데이터베이스에 추가된 지 1일 이상이 지난 기기에만 해당됩니다.	1일 이상
오랫동안 중앙 관리 서버에 연결 안 됨	네트워크 에이전트가 기기에 설치되었지만 기기가 꺼져 있어 지정된 시간 간격보다 오랫동안 중앙 관리 서버에 연결되지 않았습니다.	1일 이상
처리 안 된 위협이 탐지됨	**처리 안 된 위협** 폴더의 처리되지 않은 개체 수가 지정된 값을 초과합니다.	항목 0개 이상

조건	조건 설명	사용 가능한 값
재시작 필요	기기가 네트워크에 표시되지만 선택한 이유 중 하나로 인해 애플리케이션이 지정된 시간 간격보다 오랫동안 기기 다시 시작을 요구합니다.	0분 이상
비호환 애플리케이션이 설치되어 있음	기기가 네트워크에 표시되지만 네트워크 에이전트를 통해 수행된 소프트웨어 인벤토리에서 기기에 호환되지 않는 애플리케이션이 설치되어 있음을 탐지했습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
소프트웨어 취약점이 탐지됨	기기가 네트워크에 표시되며 네트워크 에이전트가 기기에 설치되어 있지만 *취약점 및 필요한 업데이트 검색* 작업을 통해 기기에 설치된 애플리케이션에서 지정된 심각도의 취약점이 탐지되었습니다.	• 심각 • 높음 • 중간 • 취약점을 수정할 수 없으면 무시 • 설치용 업데이트가 할당되어 있으면 무시
라이센스 만료됨	기기가 네트워크에 표시되지만 라이센스가 만료되었습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
라이센스가 곧 만료됨	기기가 네트워크에 표시되지만 기기에서 지정한 기간(일) 이내에 라이센스가 만료됩니다.	0대 이하
오랫동안 Windows 업데이트 패치를 검색하지 않음	기기가 네트워크에 표시되지만 *Windows 업데이트 동기화 수행* 작업이 지정된 시간 간격보다 오랫동안 실행되지 않았습니다.	1일 이상
유효하지 않은 암호화 상태	기기에 네트워크 에이전트가 설치되어 있는데 기기 암호화 결과가 지정된 값과 같습니다.	• 사용자의 거부로 인해 정책을 준수하지 않습니다(외부 기기에만 해당됨). • 오류로 인해 정책을 준수하지 않습니다. • 정책 적용 시 기기를 다시 시작해야 합니다. • 암호화 정책을 지정하지 않았습니다. • 지원되지 않습니다. • 정책 적용 시.
모바일 기기 설정이 정책과 일치하지 않음	모바일 기기 설정이 규정 준수 규칙 확인 중에 Kaspersky Endpoint Security for Android 정책에서 지정한 설정과 다릅니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
처리되지 않은 보안 문제가 있음	기기에서 처리되지 않은 일부 보안 문제가 발견되었습니다. 보안 문제는 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션을 통해 자동 또는 수동으로 관리자에 의해 생성될 수 있습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
애플리케이션에서 정의된 기기 상태	관리 애플리케이션이 기기 상태를 정의합니다. 관리 중인 기기는 Kaspersky Security Center 설정과 상관없이 관리 중인 애플리케이션에서 정의한 상태를 가질 수 있습니다. 이후 해당 상태가 Kaspersky Security Center에서 정의한 상태 중 하나를 반환하면, 중앙 관리 서버는 관리 중인 애플리케이션에서 반환한 상태와 중앙 관리 서버에서 할당한 상태 중 가장 심각한 상태를 관리 중인 기기에 할당합니다. 관리 중인 애플리케이션에서 정의한 상태에는 관리 중인 애플리케이션에서 전송한 설명이 있습니다. 관리 중인 기기 목록 , **상태 설명** 열에서 설명을 확인할 수 있습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.

조건	조건 설명	사용 가능한 값
기기 디스크 공간 부족	기기의 사용 가능한 디스크 공간이 지정된 값보다 작거나 기기를 중앙 관리 서버와 동기화할 수 없습니다. 기기가 중앙 관리 서버와 성공적으로 동기화되고 기기의 사용 가능한 여유 공간이 지정된 값보다 크거나 같으면 *심각* 또는 *경고* 상태가 *정상* 상태로 변경됩니다.	0MB 이상.
기기와의 연결이 끊어짐	기기를 발견하는 동안 기기가 네트워크에 연결된 것으로 인식되었지만 중앙 관리 서버와의 동기화 시도가 3회 이상 실패했습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.
보호가 비활성화됨	기기가 네트워크에 연결되었지만 기기의 보안 제품이 지정된 시간 간격보다 오랫동안 작동 중지된 상태로 유지되었습니다. 이때 보안 애플리케이션의 상태는 *정지* 또는 *실패*로 표시되며, 이는 *시작 중*, *실행 중*, *일시 중지*와는 다릅니다.	0분 이상
보안 제품이 실행 중이지 않음	기기가 네트워크에 표시되며 기기에 보안 제품이 설치는 되어 있지만 실행되고 있지는 않습니다.	• 토글 버튼이 꺼져 있습니다. • 토글 버튼이 켜져 있습니다.

Kaspersky Security Center에서는 지정한 조건이 충족되면 관리 그룹의 기기 상태를 자동으로 전환하도록 설정할 수 있습니다. 지정한 조건이 충족되면 클라이언트 기기에는 *심각* 또는 *경고* 상태 중 하나가 할당됩니다. 지정한 조건이 충족되지 않으면 클라이언트 기기에 *확인* 상태가 할당됩니다.

서로 다른 상태는 한 조건의 서로 다른 값을 나타낼 수 있습니다. 예를 들어 기본적으로 **데이터베이스가 오래됨** 조건 값이 **3일 이상**이면 클라이언트 기기에 *경고* 상태가 할당되고 값이 **7일 이상이면** *심각* 상태가 할당됩니다.

Kaspersky Security Center를 이전 버전에서 업그레이드하면 *심각* 또는 *경고*로 상태를 할당하기 위한 **데이터베이스가 오래됨** 조건의 값이 변경되지 않습니다.

기기 상태 전환 구성

조건을 변경하여 *심각* 또는 *경고* 상태를 기기에 할당할 수 있습니다.

기기 상태가 심각으로 변경되도록 설정하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 그룹 계층 구조**로 이동합니다.
2. 그룹 목록이 열리면 기기 상태 전환을 변경할 그룹 이름이 있는 링크를 누릅니다.
3. 속성 창이 열리면 **기기 상태** 탭을 선택합니다.
4. 왼쪽 창에서 **심각**을 선택합니다.
5. 오른쪽 창의 **지정되었다면 심각으로 설정** 섹션에서 기기 전환 조건을 *심각* 상태로 활성화합니다.

   부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

6. 목록에서 조건 옆에 있는 라디오 버튼을 선택합니다.
7. 목록의 왼쪽 상단에서 **편집** 버튼을 누릅니다.

8. 선택한 조건에 필요한 값을 설정합니다.
   모든 조건에 대해 값을 설정할 수 있는 것은 아닙니다.

9. **확인**를 누릅니다.

지정한 조건이 충족되면 관리 중인 기기에 *심각* 상태가 할당됩니다.

기기 상태가 경고로 변경되도록 설정하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **에셋(기기) → 그룹 계층 구조**로 이동합니다.
2. 그룹 목록이 열리면 기기 상태 전환을 변경할 그룹 이름이 있는 링크를 누릅니다.
3. 속성 창이 열리면 **기기 상태** 탭을 선택합니다.
4. 왼쪽 창에서 **경고**를 선택합니다.
5. 오른쪽 창의 **지정되었다면 경고로 설정** 섹션에서 기기 전환 조건을 *경고* 상태로 활성화합니다.

   > 부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

6. 목록에서 조건 옆에 있는 라디오 버튼을 선택합니다.
7. 목록의 왼쪽 상단에서 **편집** 버튼을 누릅니다.
8. 선택한 조건에 필요한 값을 설정합니다.
   모든 조건에 대해 값을 설정할 수 있는 것은 아닙니다.

9. **확인**를 누릅니다.

지정한 조건이 충족되면 관리 중인 기기에 *경고* 상태가 할당됩니다.

알림 전달 구성

Kaspersky Security Center에서 발생하는 이벤트에 대한 알림을 구성할 수 있습니다. 선택한 알림 방법에 따라 다음 유형의 알림을 사용할 수 있습니다.

- 이메일 - 이벤트가 발생하면 Kaspersky Security Center에서 지정된 이메일 주소로 알림을 보냅니다.
- SMS - 이벤트가 발생하면 Kaspersky Security Center에서 지정된 전화 번호로 알림을 보냅니다.
- 실행 파일 - 이벤트가 발생하면 실행 파일이 중앙 관리 서버에서 실행됩니다.

Kaspersky Security Center에서 발생하는 이벤트의 알림 전달을 구성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   일반 탭이 선택된 상태로 중앙 관리 서버 속성 창이 열립니다.

2. **알림** 섹션을 누르고 오른쪽 창에서 원하는 알림 방법에 대한 탭을 선택합니다.

- **이메일**

이메일 탭에서 이메일로 이벤트 알림을 구성할 수 있습니다.

받는 사람(이메일 주소) 필드에서 애플리케이션이 알림을 보낼 이메일 주소를 지정합니다. 이 필드에서 세미콜론으로 구분해 여러 주소를 지정할 수 있습니다.

SMTP 서버 필드에서 세미콜론으로 구분해 이메일 서버 주소를 지정합니다. 다음 값을 사용할 수 있습니다:

- IPv4 또는 IPv6 주소
- 기기의 Windows 네트워크 이름(NetBIOS 이름)
- SMTP 서버의 DNS 이름

SMTP 서버 포트 필드에서 SMTP 서버 통신 포트의 번호를 지정합니다. 기본 포트 번호는 25입니다.

DNS MX 룩업 사용 옵션을 활성화하면 SMTP 서버의 동일한 DNS 이름에 대해 IP 주소의 여러 MX 레코드를 사용할 수 있습니다. 동일한 DNS 이름에는 이메일 메시지 수신 우선 순위 값이 다른 여러 MX 레코드가 있을 수 있습니다. 중앙 관리 서버는 MX 레코드 우선 순위의 오름차순으로 SMTP 서버에 이메일 알림을 보내려고 시도합니다.

> **DNS MX 룩업 사용** 옵션을 활성화하고 TLS 설정을 활성화하지 않는 경우에는 이메일 알림 전송을 위한 추가 보호 수단으로 서버 기기에 DNSSEC 설정을 사용하는 것이 좋습니다.

ESMTP 인증 사용 옵션을 활성화하면 **사용자 이름** 및 **암호** 필드에서 ESMTP 인증 설정을 지정할 수 있습니다. 기본적으로 이 옵션은 선택되어 있지 않으며 ESMTP 인증 설정을 사용할 수 없습니다.

다음과 같이 SMTP 서버와의 연결에 대한 TLS 설정을 지정할 수 있습니다.

- **TLS 사용 안 함**

이메일 메시지 암호화를 비활성화하려는 경우 이 옵션을 선택할 수 있습니다.

- **SMTP 서버에서 지원하는 경우 TLS 사용**

SMTP 서버에 대한 TLS 연결을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 TLS를 사용하지 않고 SMTP 서버에 연결합니다.

- **항상 TLS를 사용하고 서버 인증서의 유효성을 확인합니다**

TLS 인증 설정을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 SMTP 서버에 연결할 수 없습니다.

> SMTP 서버와의 연결을 보다 잘 보호하려면 이 옵션을 사용하는 것이 좋습니다. 이 옵션을 선택하면 TLS 연결에 대한 인증 설정을 설정할 수 있습니다.

항상 TLS를 사용하고 서버 인증서의 유효성을 확인합니다 값을 선택한 경우에는 SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

다음과 같이 **인증서 지정** 링크를 클릭하여 TLS 연결용 인증서를 지정할 수 있습니다.

- 다음 SMTP 서버 인증서 파일을 찾습니다.

신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 중앙 관리 서버에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

- 다음과 같이 클라이언트 인증서 파일을 찾습니다.

신뢰할 수 있는 인증 기관과 같은 다양한 출처에서 수신된 인증서를 사용할 수 있습니다. 다음 인증서 유형 중 하나를 사용하여 인증서와 개인 키를 지정해야 합니다:

- X-509 인증서:

인증서가 있는 파일과 개인 키가 있는 파일을 지정해야 합니다. 두 파일은 서로 의존하지 않으며 파일의 로딩 순서는 중요하지 않습니다. 두 파일이 모두 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

- pkcs12 컨테이너:

인증서와 개인 키가 포함 된 단일 파일을 업로드해야 합니다. 파일이 로딩되면 개인 키를 디코딩하기 위한 암호를 지정해야 합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

제목 필드에서 이메일 제목을 지정합니다. 이 필드는 비워 둘 수 있습니다.

제목 템플릿 드롭다운 목록에서 제목에 대한 템플릿을 선택합니다. 선택한 템플릿에 의해 결정된 변수가 자동으로 **제목** 필드에 배치됩니다. 여러 제목 템플릿을 선택하여 이메일 제목을 구성할 수 있습니다.

보낸 사람 이메일 주소 필드에서 보낸 사람 이메일 주소를 지정합니다. 이 필드를 비워두면 기본적으로 받는 사람 주소가 사용됩니다. 실제 이메일 주소를 사용하는 것이 좋습니다.

알림 메시지 필드는 이벤트가 발생할 때 애플리케이션이 보내는 이벤트에 대한 정보의 표준 문구를 포함하고 있습니다. 이 문구에는 이벤트 이름, 기기 이름 및 도메인 이름과 같은 대체 파라미터가 포함됩니다. 해당 이벤트에 더 많은 관련 세부 사항을 포함하고 있는 다른 대체 파라미터를 추가해 메시지 문구를 편집할 수 있습니다.

> 만일 알림 텍스트가 % 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 입력해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

테스트 메시지 전송 버튼을 누르면 알림을 제대로 구성했는지 확인할 수 있습니다. 애플리케이션은 지정한 이메일 주소로 테스트 알림을 보냅니다.

- SMS

SMS 탭에서는 휴대폰으로 여러 이벤트에 대한 SMS 알림 전송을 구성할 수 있습니다. SMS 메시지는 메일 게이트웨이를 통해 전송됩니다.

SMTP 서버 필드에서 세미콜론으로 구분해 이메일 서버 주소를 지정합니다. 다음 값을 사용할 수 있습니다:

- IPv4 또는 IPv6 주소
- 기기의 Windows 네트워크 이름(NetBIOS 이름)
- SMTP 서버의 DNS 이름

SMTP 서버 포트 필드에서 SMTP 서버 통신 포트의 번호를 지정합니다. 기본 포트 번호는 25입니다.

ESMTP 인증 사용 옵션을 활성화하면 **사용자 이름** 및 **암호** 필드에서 ESMTP 인증 설정을 지정할 수 있습니다. 기본적으로 이 옵션은 선택되어 있지 않으며 ESMTP 인증 설정을 사용할 수 없습니다.

다음과 같이 SMTP 서버와의 연결에 대한 TLS 설정을 지정할 수 있습니다.

- **TLS 사용 안 함**

이메일 메시지 암호화를 비활성화하려는 경우 이 옵션을 선택할 수 있습니다.

- **SMTP 서버에서 지원하는 경우 TLS 사용**

SMTP 서버에 대한 TLS 연결을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 TLS를 사용하지 않고 SMTP 서버에 연결합니다.

- **항상 TLS를 사용하고 서버 인증서의 유효성을 확인합니다**

TLS 인증 설정을 사용하려는 경우 이 옵션을 선택할 수 있습니다. SMTP 서버가 TLS를 지원하지 않는 경우 중앙 관리 서버는 SMTP 서버에 연결할 수 없습니다.

SMTP 서버와의 연결을 보다 잘 보호하려면 이 옵션을 사용하는 것이 좋습니다. 이 옵션을 선택하면 TLS 연결에 대한 인증 설정을 설정할 수 있습니다.

항상 TLS를 사용하고 서버 인증서의 유효성을 확인합니다 값을 선택한 경우에는 SMTP 서버 인증을 위한 인증서를 지정하고 모든 TLS 버전을 통해 통신을 활성화할지 또는 TLS 1.2 이상 버전을 통해서만 활성화할지를 선택할 수 있습니다. 또한, SMTP 서버에서 클라이언트 인증용 인증서를 지정할 수 있습니다.

다음과 같이 **인증서 지정** 링크를 클릭하여 SMTP 서버 인증서 파일을 지정할 수 있습니다.

신뢰할 수있는 인증 기관에서 인증서 목록이 포함된 파일을 수신하여 중앙 관리 서버에 업로드할 수 있습니다. Kaspersky Security Center가 SMTP 서버의 인증서가 신뢰할 수 있는 인증 기관에 의해 서명되었는지 확인합니다. 신뢰할 수 있는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하는 경우, Kaspersky Security Center는 SMTP 서버에 연결할 수 없습니다.

받는 사람(이메일 주소) 필드에서 애플리케이션이 알림을 보낼 이메일 주소를 지정합니다. 이 필드에서 세미콜론으로 구분해 여러 주소를 지정할 수 있습니다. 지정한 이메일 주소와 연결된 전화 번호로 알림이 전달됩니다.

제목 필드에서 이메일 제목을 지정합니다.

제목 템플릿 드롭다운 목록에서 제목에 대한 템플릿을 선택합니다. 선택한 템플릿에 따른 변수가 **제목** 필드에 추가됩니다. 여러 제목 템플릿을 선택하여 이메일 제목을 구성할 수 있습니다.

보낸 사람 이메일 주소: 이 설정이 지정되지 않은 경우 받는 사람 주소가 대신 사용됩니다. 경고: 실제 이메일 주소를 사용하는 것이 좋습니다 필드에서 보낸 사람 이메일 주소를 지정합니다. 이 필드를 비워두면 기본적으로 받는 사람 주소가 사용됩니다. 실제 이메일 주소를 사용하는 것이 좋습니다.

SMS 메시지 수신자의 전화 번호 필드에서 SMS 알림 수신자의 휴대전화 번호를 지정합니다.

알림 메시지 이 필드에서 이벤트가 발생할 때 애플리케이션이 보내는 이벤트에 대한 정보의 문구를 지정합니다. 이 문구에는 이벤트 이름, 기기 이름 및 도메인 이름과 같은 대체 파라미터가 포함됩니다.

만일 알림 텍스트가 % 문자를 포함하고 있다면, 메시지 전송을 허용하기 위해 열에서 해당 문자를 두 번 연속으로 입력해야 합니다. 예를 들어 "CPU 부하는 100%%입니다".

알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

테스트 메시지 전송를 누르면 알림을 제대로 구성했는지 확인할 수 있습니다. 애플리케이션은 지정한 수신자에게 테스트 알림을 보냅니다.

- **실행되는 실행 파일**

이 알림 방법을 선택하면 입력 필드에 이벤트가 발생할 때 시작되는 애플리케이션을 지정할 수 있습니다.

이벤트가 발생할 때 중앙 관리 서버에서 실행되는 실행 파일 필드에서 실행할 파일의 폴더와 이름을 지정합니다. 파일을 지정하기 전에, 알림 메시지에 전송할 이벤트 상세 정보를 정의하는 파일을 준비하고 자리 표시자를 지정합니다. 지정하는 폴더와 파일은 중앙 관리 서버에 위치해야 합니다.

알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

3. 탭에서 알림 설정을 정의합니다.

4. **확인** 버튼을 눌러 중앙 관리 서버 속성 창을 닫습니다.

저장된 알림 전달 설정은 Kaspersky Security Center에서 발생하는 모든 이벤트에 적용됩니다.

중앙 관리 서버 설정, 정책 설정 또는 애플리케이션 설정의 **이벤트 구성** 섹션에서 특정 이벤트에 대한 알림 설정을 재정의할 수 있습니다.

실행 파일을 실행하면 표시되는 이벤트 알림

Kaspersky Security Center는 실행 파일을 실행하여 클라이언트 기기의 이벤트에 대한 알림을 관리자에게 제공할 수 있습니다. 실행 파일은 관리자에게 전달할 이벤트 자리 표시자가 있는 다른 실행 파일을 반드시 포함해야 합니다(아래 표 참조).

이벤트를 설명하기 위한 자리 표시자

자리 표시자	자리 표시자 설명
%SEVERITY%	이벤트 심각도. 가능한 값: • **정보** • **경고** • **오류** • **심각**
%COMPUTER%	이벤트가 발생한 기기 이름. 기기 이름은 최대 256자입니다.
%DOMAIN%	이벤트가 발생한 기기 도메인 이름.
%EVENT%	이벤트 유형 이름. 이벤트 유형 이름은 최대 50자입니다.
%DESCR%	이벤트 설명. 설명은 최대 1,000자입니다.
%RISE_TIME%	이벤트 생성 시각.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	작업 이름. 작업 이름은 최대 100자입니다.
%KL_PRODUCT%	애플리케이션 이름.
%KL_VERSION%	애플리케이션 버전 번호.
%KLCSAK_EVENT_SEVERITY_NUM%	이벤트 심각도 번호. 가능한 값: • 1 – **정보** • 2 – **경고** • 3 – **오류** • 4 – **심각**
%HOST_IP%	이벤트가 발생한 기기 IP 주소.
%HOST_CONN_IP%	이벤트가 발생한 기기 연결 IP 주소.

예:
이벤트 알림은 script1.bat와 같은 실행 파일을 통해 전송됩니다. 이 파일 내에는 %COMPUTER% 자리 표시자가 시작된 script2.bat 등의 다른 실행 파일이 들어 있습니다. 이벤트가 발생하면 관리자 기기에서 script1.bat 파일이 실행됩니다. 그러면 %COMPUTER% 자리 표시자가 포함된 script2.bat 파일이 실행됩니다. 따라서 관리자는 이벤트가 발생한 기기의 이름을 수신합니다.

Kaspersky 공지

이 섹션에서는 Kaspersky 관련 공지를 사용, 구성, 비활성화하는 방법을 설명합니다.

Kaspersky 관련 공지

Kaspersky 공지 섹션(**모니터링 및 보고 → Kaspersky 공지**)에서는 사용 중인 Kaspersky Security Center 버전과 관리 중인 기기에 설치된 관리 애플리케이션에 대한 정보를 계속 제공합니다. Kaspersky Security Center는 오래된 공지를 제거하고 새로운 정보를 추가하여 섹션의 정보를 정기적으로 업데이트합니다.

Kaspersky Security Center는 현재 연결된 중앙 관리 서버 및 이 중앙 관리 서버의 관리 중인 기기에 설치된 Kaspersky 애플리케이션과 관련된 Kaspersky 공지만 표시합니다. 공지 사항은 기본, 보조 또는 가상 등 모든 유형의 중앙 관리 서버에 대해 개별적으로 표시됩니다.

Kaspersky 공지를 받으려면 중앙 관리 서버가 인터넷에 연결되어 있어야 합니다.

공지에는 다음 유형의 정보가 포함됩니다.

- 보안 관련 공지

  보안 관련 공지는 네트워크에 설치된 Kaspersky 애플리케이션을 최신 상태로 유지하고 완벽하게 작동시키기 위한 것입니다. 공지에는 Kaspersky 애플리케이션의 중요 업데이트, 발견된 취약점에 대한 수정 사항, Kaspersky 애플리케이션의 기타 문제를 수정하는 방법에 대한 정보가 포함될 수 있습니다. 보안 관련 공지는 기본적으로 활성화되어 있습니다. 공지를 받고 싶지 않으면 이 기능을 비활성화할 수 있습니다.

  네트워크 보호 구성에 해당하는 정보를 표시하기 위해 Kaspersky Security Center는 데이터를 Kaspersky 클라우드 서버로 보내고 네트워크에 설치된 Kaspersky 애플리케이션과 관련된 알림만 받습니다. 서버로 전송할 수 있는 데이터 세트는 Kaspersky Security Center 중앙 관리 서버를 설치할 때 수락하는 최종 사용자 라이센스 계약서에 나와 있습니다.

- 마케팅 공지

  마케팅 공지에는 Kaspersky 애플리케이션의 특가 판매, 광고, Kaspersky 뉴스에 대한 정보가 포함됩니다. 마케팅 공지는 기본적으로 비활성화되어 있습니다. 이러한 유형의 공지는 Kaspersky Security Network(KSN)를 활성화한 경우에만 받을 수 있습니다. KSN을 비활성화하여 마케팅 공지를 비활성화할 수 있습니다.

  네트워크 기기 보호와 일상적인 작업에 도움이 될 수 있는 관련 정보만 표시하기 위해 Kaspersky Security Center는 데이터를 Kaspersky 클라우드 서버로 보내고 적절한 공지를 받습니다. 서버로 전송할 수 있는 데이터 세트는 KSN 성명서의 처리된 데이터 섹션에 나와 있습니다.

새로운 정보는 중요도에 따라 다음과 같은 카테고리로 나뉩니다.

1. 중요한 정보
2. 중요한 뉴스
3. 경고
4. 정보

Kaspersky 공지 섹션에 새로운 정보가 표시되면 Kaspersky Security Center 웹 콘솔에 공지의 심각도에 따라 해당하는 알림 라벨이 표시됩니다. 이 라벨을 눌러 Kaspersky 공지 섹션에서 해당 공지를 확인할 수 있습니다.

보고자 하는 공지 카테고리와 알림 라벨을 표시할 위치를 포함하여 Kaspersky 공지 설정을 지정할 수 있습니다.

Kaspersky 공지 설정 지정

Kaspersky 공지 섹션에서 보고자 하는 공지 카테고리와 알림 라벨을 표시할 위치를 포함하여 Kaspersky 공지 설정을 지정할 수 있습니다.

Kaspersky 공지 구성하기:

1. 메인 메뉴에서 **모니터링 및 보고** → **Kaspersky 공지 사항**으로 이동합니다.
2. **설정** 링크를 누릅니다.
   Kaspersky 공지 설정 창이 열립니다.
3. 다음 설정을 지정합니다:
   - 보고자 하는 공지의 심각도를 선택합니다. 다른 카테고리의 공지는 표시되지 않습니다.
   - 알림 라벨을 보려는 위치를 선택합니다. 라벨은 모든 콘솔 섹션 또는 **모니터링 및 보고** 섹션 및 하위 섹션에 표시됩니다.
4. **확인** 버튼을 누릅니다.
   Kaspersky 공지 설정이 지정됩니다.

Kaspersky 공지 비활성화

Kaspersky 공지 섹션(**모니터링 및 보고** → **Kaspersky 공지**)에서는 사용 중인 Kaspersky Security Center 버전과 관리 중인 기기에 설치된 관리 애플리케이션에 대한 정보를 계속 제공합니다. Kaspersky 공지를 받고 싶지 않으면 이 기능을 비활성화할 수 있습니다.

Kaspersky 공지에는 보안 관련 공지와 마케팅 공지 등 두 가지 유형의 정보가 포함됩니다. 각 유형의 공지를 개별적으로 비활성화할 수 있습니다.

보안 관련 공지 비활성화하기:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **Kaspersky 공지 사항** 섹션을 선택합니다.
3. 토글 버튼을 **보안 관련 공지 사항 비활성화됨** 위치로 전환합니다.
4. **저장** 버튼을 클릭합니다.
   Kaspersky 공지가 비활성화됩니다.

마케팅 공지는 기본적으로 비활성화되어 있습니다. Kaspersky Security Network(KSN)를 활성화한 경우에만 마케팅 공지를 받을 수 있습니다. KSN을 비활성화하여 이러한 유형의 공지를 비활성화할 수 있습니다.

마케팅 공지 비활성화하기:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **KSN 프록시 설정** 섹션을 선택합니다.
3. **Kaspersky Security Network 사용 활성화됨** 옵션을 비활성화합니다.
4. **저장** 버튼을 누릅니다.
   마케팅 공지가 비활성화됩니다.

위협 탐지에 대한 정보 보기

알림에 대한 정보 표시를 활성화하거나 비활성화할 수 있습니다.

*메인 메뉴에서 **경고** 섹션 표시를 활성화 또는 비활성화하려면:*

1. 메인 메뉴에서 계정 설정으로 이동하여 **인터페이스 옵션**을 선택합니다.
2. **Interface options** 창이 열리면 **EDR 경고 표시** 옵션을 활성화 또는 비활성화합니다.
3. **저장**을 누릅니다.

콘솔이 메인 메뉴의 **모니터링 및 보고** 섹션에서 **경고** 하위 섹션을 표시합니다. **경고** 하위 섹션에서 엔드포인트 기기의 위협 탐지에 대한 정보를 볼 수 있습니다. EDR Optimum에 대한 라이센스 키를 추가하면 Kaspersky Security Center 웹 콘솔이 자동으로 메인 메뉴의 **모니터링 및 보고** 섹션에 **경고** 하위섹션을 표시합니다. 또한, 알림에 대한 정보를 표시하는 위젯을 추가할 수 있습니다.

경고 하위 섹션은 **EDR 경고 표시** 옵션을 활성화하기 전에 EDR Optimum의 라이센스 키를 추가했을 때만 자동 표시됩니다. **EDR 경고 표시** 옵션을 활성화한 후 라이센스 키를 추가했다면 이 옵션을 다시 활성화한 후에만 **경고** 하위 섹션이 표시됩니다.

탐지된 위협에 대한 상세 정보를 경고 카드에 올바르게 표시하려면 Kaspersky Endpoint Agent 플러그인과 Kaspersky Endpoint Security 플러그인 (Kaspersky Endpoint Security for Linux 12.1 이상, Kaspersky Endpoint Security for Mac 12.1 이상 또는 Kaspersky Endpoint Security for Windows 12.6 이상)의 호환되는 버전을 설치해야 합니다.

필터 메뉴를 사용하여 날짜 및 필드 값으로 경고를 필터링합니다.

개체 유형 필드에는 다음 값이 포함됩니다.

- 알 수 없음
- 피싱 링크
- 바이러스
- 트로이목마
- 악성 도구

- 백도어
- 웜
- 기타 애플리케이션
- 애드웨어
- 포르노웨어
- 위험한 실행 압축 프로그램
- 위험한 행동

자동 응답 필드에는 다음 값이 포함됩니다.

- 악성 개체 탐지
- 개체 삭제
- 개체 치료
- 개체 치료 실패
- 개체가 격리 저장소로 이동됨
- 암호로 보호된 압축 파일 탐지
- 바이러스 탐지

Cloud Discovery

Kaspersky Security Center로 Windows를 실행하는 관리 중인 기기의 클라우드 서비스 사용을 모니터링하고 원하지 않는 클라우드 서비스에 대한 접근을 차단할 수 있습니다. Cloud Discovery는 브라우저와 데스크톱 애플리케이션으로 이러한 서비스에 대한 접근 권한을 획득하려는 시도를 추적합니다. 또한 암호화되지 않은 연결(HTTP 프로토콜 사용 등)을 통해 클라우드 서비스 접근 권한을 획득하려는 시도를 추적합니다. 이 기능은 섀도우 IT의 클라우드 서비스 사용 탐지 및 중지하는 데 유용합니다.

> 차단 기능은 Kaspersky Next EDR Optimum 또는 Kaspersky Next XDR Expert 라이센스로 Kaspersky Security Center를 활성화했을 때만 사용할 수 있습니다.

> 차단 기능은 Kaspersky Endpoint Security 11.2 for Windows 이상에서만 사용할 수 있습니다. 이전 버전의 보안 애플리케이션에서는 클라우드 서비스 사용 모니터링만 할 수 있습니다.

Cloud Discovery 기능을 활성화하고 기능을 활성화할 보안 정책이나 프로필을 선택할 수 있습니다. 각 보안 정책이나 프로필에서 별도로 기능을 활성화하거나 비활성화할 수도 있습니다. 접근을 허용하지 않으려는 클라우드 서비스에 대한 접근을 차단할 수 있습니다.

원치 않는 클라우드 서비스에 대한 접근을 차단하려면 다음 사전 조건을 충족했는지 확인합니다.

- Kaspersky Endpoint Security 11.2 for Windows 이상을 사용합니다. 이전 버전의 보안 애플리케이션에서는 클라우드 서비스 사용 모니터링만 할 수 있습니다.
- 클라우드 서비스에 대한 원치 않는 접근 차단 기능이 포함된 Kaspersky Next 라이센스 단계를 구매했습니다. 자세한 내용은 Kaspersky Next 도움말을 참조하십시오.

Cloud Discovery 위젯과 Cloud Discovery 리포트는 클라우드 서비스 액세스 권한 획득 시도에 관한 성공 및 차단 정보를 표시합니다. 이 위젯은 각 클라우드 서비스의 위험 수준도 표시합니다. Kaspersky Security Center는 기능이 활성화된 보안 정책이나 프로필로만 보호되는 관리 중인 기기 전체에서 클라우드 서비스 사용 관련 정보를 가져옵니다.

위젯으로 Cloud Discovery 활성화

Cloud Discovery 기능을 사용하면 해당 기능이 있는 보안 정책으로 보호하는 관리 중인 기기 전체에서 클라우드 서비스 사용 관련 정보를 가져올 수 있습니다. Kaspersky Endpoint Security for Windows 정책에 대해서만 클라우드 검색을 활성화하거나 비활성화할 수 있습니다.

클라우드 검색 기능 활성화 방법은 두 가지입니다.

- 클라우드 검색 위젯 사용.
- Kaspersky Endpoint Security for Windows 정책의 속성에서.

  Kaspersky Endpoint Security for Windows 정책 속성에서 클라우드 검색 기능 활성화 방법에 관한 자세한 내용은 Kaspersky Endpoint Security for Windows 도움말의 Cloud Discovery 섹션을 참조하십시오.

Kaspersky Endpoint Security for Windows 정책 파라미터의 클라우드 검색 기능만 비활성화할 수 있습니다.

클라우드 검색을 활성화하려면 **일반 기능: 기본 기능** 기능 영역에서 **쓰기** 권한이 있어야 합니다.

Cloud Discovery 위젯으로 Cloud Discovery 기능을 활성화하려면:

1. Kaspersky Security Center로 갑니다.
2. 메인 메뉴에서 **모니터링 및 보고 → 대시보드**로 이동합니다.
3. **Cloud Discovery** 위젯에서 **활성화** 버튼을 클릭합니다.

   Kaspersky Endpoint Security for Windows 버전 12.4를 설치했다면 Kaspersky Endpoint Security for Windows 정책 속성에서 클라우드 검색 기능을 활성화합니다. 자세한 내용은 Kaspersky Endpoint Security for Windows 도움말의 Cloud Discovery 섹션을 참조하십시오.

   Kaspersky Endpoint Security for Windows가 12.4 이전 버전이라면 Kaspersky Endpoint Security for Windows 플러그인을 버전 12.5로 업데이트합니다.

4. **Cloud Discovery 활성화** 창이 열리면 기능을 사용할 보안 정책을 선택한 다음 **활성화** 버튼을 클릭합니다.

   웹 트래픽에 스크립트를 삽입하여 웹 페이지와 상호 작용, **웹 세션 모니터**, **암호화된 연결 검사** 정책 설정이 자동 활성화됩니다.

Cloud Discovery 기능이 활성화되고 위젯이 대시보드에 추가됩니다.

대시보드에 Cloud Discovery 위젯 추가

Cloud Discovery를 대시보드에 추가하여 관리 중인 기기에서 클라우드 서비스 사용을 모니터링할 수 있습니다.

Cloud Discovery 위젯을 대시보드에 추가하려면 **일반 기능: 기본 기능쓰기**쓰기 권한이 있어야 합니다.

대시보드에 Cloud Discovery 위젯을 추가하려면:

1. Kaspersky Security Center로 갑니다.
2. 메인 메뉴에서 **모니터링 및 보고 → 대시보드**로 이동합니다.
3. **웹 위젯 추가 또는 복원** 버튼을 클릭합니다.
4. 사용 가능한 위젯 목록에서 **기타** 카테고리 옆의 펼침 단추 아이콘(>)을 클릭합니다.
5. **Cloud Discovery** 위젯을 선택한 다음 **추가** 버튼을 클릭합니다.

   Cloud Discovery 기능이 비활성화되면 위젯으로 Cloud Discovery 활성화 섹션의 지침을 따릅니다.

선택한 위젯이 대시보드 끝에 추가됩니다.

클라우드 서비스 사용에 대한 정보 보기

클라우드 서비스의 접근 권한 획득 시도에 대한 정보를 표시하는 **클라우드 검색** 위젯을 볼 수 있습니다. 이 위젯은 각 클라우드 서비스의 위험 수준도 표시합니다. Kaspersky Security Center는 기능이 활성화된 보안 프로필로만 보호되는 관리 중인 기기 전체에서 클라우드 서비스 사용 관련 정보를 가져옵니다.

보기 전에 다음을 확인합니다.

- Cloud Discovery 위젯이 대시보드에 추가됩니다.
- Cloud Discovery 기능이 활성화됩니다.
- **일반 기능: 기본 기능** 기능 영역의 **읽기** 권한이 있습니다.

Cloud Discovery 위젯을 보려면 다음을 따릅니다.

1. Kaspersky Security Center로 갑니다.
2. 메인 메뉴에서 **모니터링 및 보고 → 대시보드**로 이동합니다.

   Cloud Discovery 위젯이 대시보드에 표시됩니다.

3. **Cloud Discovery** 위젯 왼쪽에서 클라우드 서비스 카테고리를 선택합니다.

   위젯 오른쪽 표에 선택한 카테고리에서 접근을 가장 자주 시도하는 서비스가 최대 5개까지 표시됩니다. 성공한 시도와 차단된 시도가 모두 계산됩니다.

4. 위젯 오른쪽에서 특정 서비스를 선택합니다.

   아래 표에는 서비스 접근을 가장 자주 시도하는 기기가 최대 10대까지 표시됩니다. 이 표에서 성공적인 접근 시도에 관한 리포트와 차단된 접근 시도에 관한 리포트, 두 가지를 생성할 수 있습니다.

   또한 이 표에서 특정 기기의 클라우드 서비스에 대한 접근을 차단할 수 있습니다.

위젯이 요청한 정보를 표시합니다.

위젯이 표시되면 다음을 할 수 있습니다.

- **모니터링 및 보고 → 리포트** 섹션으로 이동하여 Cloud Discovery 리포트를 봅니다.
- 선택한 클라우드 서비스에 대한 접근을 차단하거나 허용합니다.

> 차단 기능은 Kaspersky Next EDR Optimum 또는 Kaspersky Next XDR Expert 라이센스로 Kaspersky Security Center를 활성화했을 때만 사용할 수 있습니다.

> 차단 기능은 Kaspersky Endpoint Security 11.2 for Windows 이상에서만 사용할 수 있습니다. 이전 버전의 보안 애플리케이션에서는 클라우드 서비스 사용 모니터링만 할 수 있습니다.

클라우드 서비스의 위험도

Cloud Discovery는 각 클라우드 서비스에 대한 위험도를 제공합니다. 위험도로 조직의 보안 요구사항에 적합하지 않은 서비스를 결정할 수 있습니다. 예를 들어 위험도를 고려하여 특정 서비스에 대한 접근 차단 여부를 결정할 수 있습니다.

> 위험도는 추정된 지표이며 클라우드 서비스 또는 서비스 제조업체의 품질에 아무 영향도 주지 않습니다. 위험도는 Kaspersky 전문가의 권장 사항입니다.

클라우드 서비스의 위험도는 Cloud Discovery 위젯과 모니터링하는 모든 클라우드 서비스 목록에 표시됩니다.

원치 않는 클라우드 서비스에 대한 접근 차단

접근을 허용하지 않으려는 클라우드 서비스에 대한 접근을 차단할 수 있습니다. 이전에 차단한 클라우드 서비스에 대한 접근을 허용할 수도 있습니다.

특히 특정 서비스에 대한 접근 차단 여부를 결정할 때 위험 수준을 고려할 수 있습니다.

보안 정책이나 프로필에 대한 클라우드 서비스 접근을 차단하거나 허용할 수 있습니다.

원치 않는 클라우드 서비스의 접근 차단 방법은 두 가지입니다.

- 클라우드 검색 위젯 사용.

  이때, 서비스 접근을 하나씩 차단할 수 있습니다.

- Kaspersky Endpoint Security for Windows 정책의 속성에서.

  이 경우 해당 서비스에 대한 접근을 하나씩 차단하거나, 전체 카테고리를 한 번에 차단할 수 있습니다.

  Kaspersky Endpoint Security for Windows 정책 속성에서 클라우드 검색 기능 활성화 방법에 관한 자세한 내용은 Kaspersky Endpoint Security for Windows 도움말의 Cloud Discovery 섹션을 참조하십시오.

위젯으로 클라우드 서비스에 대한 접근을 차단하거나 허용하려면:

1. 클라우드 검색 위젯을 열고 필요한 클라우드 서비스를 선택합니다.
2. **이 서비스를 사용하는 상위 10개 기기** 창에서 서비스를 차단하거나 허용할 보안 정책이나 프로필을 찾습니다.
3. 필요한 줄의 **정책 또는 프로필의 접근 상태** 열에서 다음 중 하나를 수행합니다.
   - 서비스를 차단하려면 드롭다운 목록에서 **차단됨**을 선택합니다.
   - 서비스를 허용하려면 드롭다운 목록에서 **허락됨**을 선택합니다.
4. **저장** 버튼을 클릭합니다.

보안 정책이나 프로필에 선택한 서비스에 대한 접근이 차단되거나 허용됩니다.

Kaspersky Security Center 웹 콘솔 활동 로깅

Kaspersky Security Center 웹 콘솔 활동 로깅은 소프트웨어 오작동의 원인을 조사하는 데 도움이 될 수 있습니다. Kaspersky Security Center 웹 콘솔 오작동에 대해 Kaspersky 기술 지원에 문의하면 Kaspersky 기술 지원 전문가가 Kaspersky Security Center 웹 콘솔 로그 파일을 요청할 수 있습니다. Kaspersky Security Center 웹 콘솔 로그 파일은 애플리케이션을 사용하는 동안 <Kaspersky Security Center 웹 콘솔 설치 폴더>/로그 폴더에 저장됩니다. 로그 파일은 Kaspersky 기술 지원 전문가에게 자동으로 전송되지 않습니다.

Kaspersky Security Center 웹 콘솔 활동 로깅을 활성화하려면 다음 단계를 따릅니다.

Kaspersky Security Center 웹 콘솔 설치 마법사의 **Kaspersky Security Center 웹 콘솔 연결 설정** 창에서 **Kaspersky Security Center 웹 콘솔 활동 로깅 활성화** 확인란을 선택합니다.

로그 파일은 텍스트 형식입니다.

로그 파일 이름은 로그-<구성 요소 이름>.<기기 이름> -<파일 버전 번호>.YYYY-MM-DD 형식이며, 여기에서:

- <구성 요소 이름>은 Kaspersky Security Center 구성 요소의 이름 또는 Kaspersky Security Center 웹 콘솔 관리 플러그인 이름입니다.
- <기기 이름>은 <구성 요소 이름>일 실행 중인 기기의 이름입니다.
- <파일 버전 번호>는 <기기 이름>에서 작업 중인 <구성 요소 이름>에 대해 생성된 로그 파일의 번호입니다. 하루 내에 동일한 <구성 요소 이름> 및 <기기 이름>에 대한 여러 로그 파일을 만들 수 있습니다. 로그 파일의 최대 크기는 50MB입니다. 최대 파일 크기에 도달하면 새 로그 파일이 생성됩니다. 새 로그 파일 <파일 버전 번호>가 1씩 증가합니다.
- YYYY, MM 및 DD는 로그가 처음 생성된 연도, 월, 일입니다. 새로운 날이 시작되면 새로운 로그 파일이 생성됩니다.

Kaspersky Security Center와 기타 솔루션 간의 통합

이 섹션에서는 Kaspersky Security Center Linux 웹 콘솔에서 Kaspersky Managed Detection and Response와 같은 다른 Kaspersky 애플리케이션에 대한 액세스를 구성하는 방법에 대해 설명합니다. 또한 이 섹션에서는 SIEM 시스템으로 내보내기를 구성하는 방법에 대해 설명합니다.

백그라운드 연결 설정

Kaspersky Security Center 웹 콘솔이 백그라운드 작업을 수행하도록 하려면, Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 간에 백그라운드 연결을 설정해야 합니다. 계정에 **일반 기능: 사용자 권한** 기능 영역의 **개체 ACL 수정** 권한이 있을 때만 이 연결을 설정할 수 있습니다.

Kaspersky Endpoint Security for Windows 12.6 플러그인을 설치하거나, Kaspersky Endpoint Security for Windows 플러그인을 11.7 이전 버전에서 업데이트하고 백그라운드 연결을 아직 설정하지 않았다면, 백그라운드 연결을 설정해야 한다는 알림이 표시됩니다. 또한, 서비스 계정에 **일반 기능: 중앙 관리 서버의 작업** 기능 영역의 권한을 부여해야 합니다.

백그라운드 연결 설정 방법:

1. 메인 메뉴에서 **설정** → **통합** 섹션으로 이동합니다.
2. **통합** 섹션에서 백그라운드 연결을 설정하기 위한 토글 버튼을 **통합을 위한 백그라운드 연결 활성화됨** 위치로 전환합니다.
3. 열려 있는 **백그라운드 연결 활성화** 섹션에서 **확인** 버튼을 누릅니다.

Kaspersky Security Center 웹 콘솔과 중앙 관리 서버 간의 백그라운드 연결이 설정됩니다. 중앙 관리 서버는 백그라운드 연결용 계정을 생성하고 이 계정은 Kaspersky Security Center와 다른 Kaspersky 애플리케이션 또는 솔루션 간의 상호 작용을 유지하기 위한 서비스 계정으로 사용됩니다. 이 서비스 계정의 이름에는 NWCSvcUser 접두사가 포함됩니다.

중앙 관리 서버는 보안상의 이유로 30일에 한 번씩 서비스 계정의 암호를 자동으로 변경합니다. 서비스 계정은 수동으로 삭제할 수 없습니다. 교차 서비스 연결을 비활성화하면 중앙 관리 서버가 이 계정을 자동으로 삭제합니다. 중앙 관리 서버는 각 관리 콘솔용 단일 서비스 계정을 만들고 ServiceNwcGroup이라는 이름의 보안 그룹에 모든 서비스 계정을 할당합니다. 중앙 관리 서버는 Kaspersky Security Center 설치 프로세스 중에 이 보안 그룹을 자동으로 생성합니다. 보안 그룹은 수동으로 삭제할 수 없습니다.

SIEM 시스템으로 이벤트 내보내기

이 섹션에서는 SIEM 시스템으로 이벤트 내보내기를 구성하는 방법을 설명합니다.

SIEM 시스템으로 이벤트 내보내기 구성

Kaspersky Security Center에서는 Syslog 형식을 사용하는 모든 SIEM 시스템으로 내보내기, LEEF 및 CEF 형식을 사용하는 QRadar, Splunk, ArcSight SIEM 시스템으로 내보내기 또는 Kaspersky Security Center 데이터베이스에서 직접 SIEM 시스템으로 이벤트 내보내기 중 하나의 방법으로 구성할 수 있습니다. 이 시나리오를 완료하면 중앙 관리 서버가 이벤트를 SIEM 시스템에 자동으로 전송합니다.

필수 구성 요소

Kaspersky Security Center에서 이벤트 구성 내보내기를 시작하기 전:

- 이벤트 내보내기 방법에 대해 자세히 알아보기.
- 시스템 설정 값이 있는지 확인합니다.

> 이 시나리오의 단계는 순서에 관계없이 수행할 수 있습니다.

SIEM 시스템에 대한 이벤트 내보내기 과정은 다음 단계로 구성됩니다:

- **Kaspersky Security Center에서 이벤트를 수신하도록 SIEM 시스템을 구성합니다.**

  방법 지침: SIEM 시스템에서 이벤트 내보내기 구성

- **SIEM 시스템으로 내보낼 이벤트를 선택하기:**

  방법 지침:

  - 관리 콘솔: Syslog 형식으로 내보낼 Kaspersky 애플리케이션의 이벤트 표시, Syslog 형식으로 내보낼 일반 이벤트 표시
  - Kaspersky Security Center 웹 콘솔: Syslog 형식으로 내보낼 Kaspersky 애플리케이션의 이벤트 표시, Syslog 형식으로 내보낼 일반 이벤트 표시

- **다음 중 하나의 방법을 사용하여 SIEM 시스템으로 이벤트 내보내기를 구성하기:**

  - TCP 프로토콜에서 TCP, UDP, TLS 중 하나 사용.

    방법 지침:

    - 관리 콘솔: SIEM 시스템으로 이벤트 내보내기 구성
    - Kaspersky Security Center 웹 콘솔: SIEM 시스템으로 이벤트 내보내기 구성

  - Kaspersky Security Center 데이터베이스에서 직접 이벤트 내보내기 사용(공용 보기 세트는 Kaspersky Security Center 데이터베이스에서 제공됩니다. 이러한 공용 보기에 대한 설명은 klakdb.chm 문서에서 확인할 수 있습니다).

결과

내보내기 원하는 이벤트를 선택한 경우에는 SIEM 시스템으로 이벤트 내보내기를 구성한 후 내보내기 결과를 볼 수 있습니다.

시작하기 전에

Kaspersky Security Center에서 이벤트 자동 내보내기를 설정할 때는 몇 가지 SIEM 시스템 설정을 지정해야 합니다. Kaspersky Security Center 설정을 준비하려면 이러한 설정을 미리 확인하는 것이 좋습니다.

SIEM 시스템으로의 이벤트 자동 전송을 올바르게 구성하려면 다음 설정을 확인해야 합니다:

- **SIEM 시스템 서버 주소**

  현재 사용 중인 SIEM 시스템이 설치된 서버의 IP 주소입니다. SIEM 시스템 설정에서 이 값을 확인하십시오.

- **SIEM 시스템 서버 포트**

  Kaspersky Security Center와 SIEM 시스템 서버 간의 연결을 설정하는 데 사용되는 포트 번호입니다. Kaspersky Security Center 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

- **프로토콜**

  Kaspersky Security Center에서 SIEM 시스템으로 메시지를 전송하는 데 사용되는 프로토콜입니다. Kaspersky Security Center 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

Kaspersky Security Center의 이벤트 정보

Kaspersky Security Center에서는 관리 중인 기기에 설치된 중앙 관리 서버 및 Kaspersky 애플리케이션의 작동 중 발생한 이벤트 정보를 볼 수 있습니다. 이벤트에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다. 이 정보를 외부 SIEM 시스템으로 내보낼 수 있습니다. 외부 SIEM 시스템으로 이벤트 정보를 내보내면 SIEM 시스템 관리자가 관리 중인 기기 또는 관리 그룹에서 발생하는 보안 시스템 이벤트에 신속하게 대응할 수 있습니다.

이벤트 유형

Kaspersky Security Center에는 다음과 같은 유형의 이벤트가 있습니다:

- 일반 이벤트. 이러한 이벤트는 모든 관리 중인 Kaspersky 애플리케이션에서 발생합니다. 일반 이벤트의 예로 바이러스 발생가 있습니다. 일반 이벤트에서는 구문과 의미를 엄격하게 정의합니다. 일반 이벤트는 리포트와 대시보드 등에 사용합니다.

- 관리 중인 Kaspersky 애플리케이션별 이벤트. 각 관리 중인 Kaspersky 애플리케이션에는 자체 이벤트 집합이 있습니다.

이벤트 소스

이벤트는 다음 애플리케이션에서 생성할 수 있습니다.

- Kaspersky Security Center 구성 요소:
  - 중앙 관리 서버
  - 네트워크 에이전트
  - iOS MDM 서버
- 관리 중인 Kaspersky 애플리케이션

  관리 중인 Kaspersky 애플리케이션에서 생성된 이벤트에 대한 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.

애플리케이션 정책의 **이벤트 구성** 탭에서 애플리케이션에서 생성할 수 있는 이벤트의 전체 목록을 볼 수 있습니다. 중앙 관리 서버는 중앙 관리 서버 속성에서 이벤트 목록을 추가로 볼 수 있습니다.

이벤트의 중요성 수준

각 이벤트에는 고유한 심각도가 있습니다. 발생 조건에 따라 이벤트에는 여러 심각도가 할당될 수 있습니다. 네 가지 심각도가 있습니다.

- *심각 이벤트*는 데이터 손실, 운영상의 오작동, 심각한 오류 등을 초래할 수 있는 심각한 문제 발생을 나타내는 이벤트입니다.
- *기능 실패*는 애플리케이션 작동 중이나 절차 수행 중에 심각한 문제, 오류 또는 오작동이 발생했음을 나타내는 이벤트입니다.
- *경고*는 반드시 심각한 것은 아니지만 향후 문제 발생 가능성을 나타내는 이벤트입니다. 이벤트 발생 후 데이터나 기능 손실 없이 애플리케이션을 복원할 수 있는 경우 대부분의 이벤트는 경고로 지정됩니다.
- *정보* 이벤트는 정상적인 작업 완료, 적절한 애플리케이션 작동 또는 절차 완료에 대해 알리기 위해 발생하는 이벤트입니다.

각 이벤트에는 정의된 저장 기간이 있으며, 이 시간 동안 Kaspersky Security Center에서 이벤트를 보거나 수정할 수 있습니다. 정의된 저장 기간이 0이어서 기본적으로 중앙 관리 서버 데이터베이스에 저장되지 않는 이벤트도 있습니다. 1일 이상 중앙 관리 서버 데이터베이스에 저장되는 이벤트만 외부 시스템으로 내보낼 수 있습니다.

이벤트 내보내기 정보

조직 및 기술 레벨에서 보안 문제를 처리하고, 보안 모니터링 서비스를 제공하고, 여러 솔루션의 정보를 통합하는 중앙 집중식 시스템 내에서 이벤트 내보내기를 사용할 수 있습니다. 네트워크 하드웨어 및 애플리케이션이나 SOC(보안 운영 센터)에서 생성하는 보안 경고와 이벤트의 실시간 분석 기능을 제공하는 이러한 시스템을 SIEM 시스템이라고 합니다.

이러한 시스템은 네트워크, 보안, 서버, 데이터베이스, 애플리케이션 등의 여러 경로에서 데이터를 수집할 수 있습니다. 또한 SIEM 시스템은 심각 이벤트 누락을 방지할 수 있도록 모니터링된 데이터를 통합하는 기능도 제공합니다. 그리고 곧 발생할 것으로 예상되는 보안 문제를 관리자에게 알리기 위해 상관 관계가 지정된 이벤트와 경고의 자동 분석도 수행합니다. 경고는 대시보드를 통해 구현할 수도 있고 이메일 등의 타사 채널을 통해 전송할 수도 있습니다.

Kaspersky Security Center에서 외부 SIEM 시스템으로 이벤트를 내보내는 프로세스의 당사자는 이벤트 발신자(Kaspersky Security Center)와 이벤트 수신자(SIEM 시스템)입니다. 이벤트를 성공적으로 내보내려면 SIEM 시스템 및 Kaspersky Security Center 관리 콘솔에서 이를 구성해야 합니다. 구성 순서는 중요하지 않습니다. 즉, Kaspersky Security Center에서 이벤트 전송을 구성한 후에 SIEM 시스템의 이벤트 수신을 구성할 수도 있고 그 반대 순서로 구성할 수도 있습니다.

Kaspersky Security Center에서 이벤트를 보내는 방법

다음의 세 가지 방법으로 Kaspersky Security Center에서 외부 시스템으로 이벤트를 보낼 수 있습니다:

- Syslog 프로토콜을 통해 SIEM 시스템으로 이벤트 보내기

  Syslog 프로토콜을 사용하는 경우 Kaspersky Security Center 중앙 관리 서버 및 관리 중인 기기에 설치된 Kaspersky 애플리케이션에서 발생하는 모든 이벤트를 전달할 수 있습니다. Syslog 프로토콜은 표준 메시지 로깅 프로토콜입니다. SIEM 시스템으로 이벤트를 내보내는 데 사용할 수 있습니다.

  이를 위해 SIEM 시스템에 릴레이할 이벤트를 표시해야 합니다. 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔에서 이벤트를 표시할 수 있습니다. 표시된 이벤트만 SIEM 시스템으로 릴레이됩니다. 아무것도 표시하지 않으면 이벤트가 릴레이되지 않습니다.

- CEF 및 LEEF 프로토콜을 통해 QRadar, Splunk 및 ArcSight 시스템으로 이벤트 보내기

  CEF 및 LEEF 프로토콜을 사용하여 일반 이벤트를 내보낼 수 있습니다. CEF 및 LEEF 프로토콜을 통해 이벤트를 내보낼 때는 내보낼 특정 이벤트를 선택할 수 없습니다. 대신 모든 일반 이벤트가 내보내집니다. Kaspersky Security Center 이벤트를 CEF 및 LEEF 형식의 이벤트로 변환하려는 경우 siem_conversion_rules.xml file 파일을 사용해야 합니다. 이 파일에는 Kaspersky Security Center 이벤트 속성 목록과 CEF 및 LEEF 형식의 이벤트에 해당하는 속성이 포함되어 있습니다. 또한 siem_conversion_rules.xml 파일에는 이벤트에 해당하는 메시지를 생성하기 위한 규칙이 포함되어 있습니다. 이 파일은 Kaspersky Security Center 배포 키트에 포함되어 있습니다.

  Syslog 프로토콜과는 달리 CEF 및 LEEF 프로토콜은 범용 프로토콜이 아닙니다. CEF 및 LEEF는 QRadar, Splunk, ArcSight 등의 적합한 SIEM 시스템용 프로토콜입니다. 그러므로 이러한 프로토콜 중 하나를 통해 이벤트를 내보내도록 선택하는 경우에는 SIEM 시스템에서 필요한 파서를 사용합니다.

- Kaspersky Security Center 데이터베이스에서 SIEM 시스템으로 직접 보내기

  SQL 쿼리를 사용하여 데이터베이스 공용 보기에서 이벤트를 직접 받으려는 경우 이러한 이벤트 내보내기 방법을 사용할 수 있습니다. 쿼리 결과는 외부 시스템의 입력 데이터로 사용 가능한 XML 파일에 저장됩니다. 공용 보기에서 제공되는 이벤트만 데이터베이스에서 직접 내보낼 수 있습니다.

SIEM 시스템의 이벤트 수신

SIEM 시스템은 Kaspersky Security Center에서 이벤트를 받아서 올바르게 구문 분석해야 합니다. 따라서 SIEM 시스템을 적절하게 구성해야 합니다. 구성은 사용하는 특정 SIEM 시스템에 따라 달라집니다. 그러나 수신기와 파서 구성 등 모든 SIEM 시스템 구성에서 일반적으로 수행하는 여러 단계가 있습니다.

SIEM 시스템에서 이벤트 내보내기 구성 정보

Kaspersky Security Center에서 외부 SIEM 시스템으로 이벤트를 내보내는 프로세스의 당사자는 이벤트 발신자(Kaspersky Security Center)와 이벤트 수신자(SIEM 시스템)입니다. SIEM 시스템 및 Kaspersky Security Center 관리 콘솔에서 이벤트 내보내기를 구성해야 합니다.

SIEM 시스템에서 지정하는 설정은 사용하는 개별 시스템에 따라 달라집니다. 일반적으로는 모든 SIEM 시스템에서 수신자를 설정해야 하며 필요에 따라 수신된 이벤트를 구문 분석할 메시지 파서를 설정해야 합니다.

수신자 설정

Kaspersky Security Center에서 보낸 이벤트를 받으려면 SIEM 시스템에서 수신자를 설정해야 합니다. 일반적으로는 SIEM 시스템에서 다음 설정을 지정해야 합니다:

- **내보내기 프로토콜 또는 입력 유형**

  이는 메시지 전송 프로토콜입니다(예: UDP). 해당 프로토콜은 Kaspersky Security Center에서 지정한 프로토콜과 같아야 합니다.

- **Port**

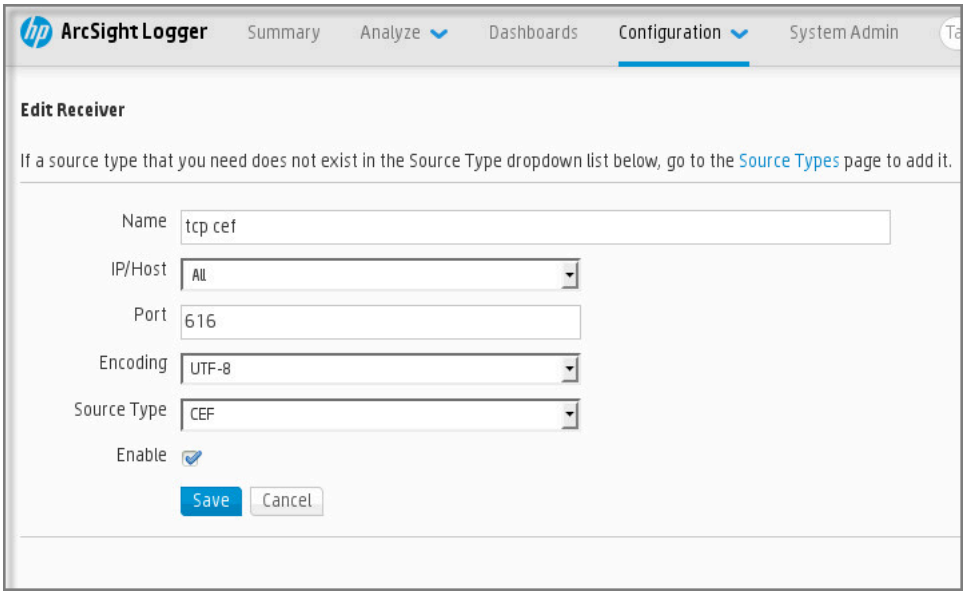
  Kaspersky Security Center 연결을 위한 포트 번호입니다. 이 포트는 Kaspersky Security Center에서 지정한 포트와 같아야 합니다.

- **메시지 프로토콜 또는 경로 유형**

  SIEM 시스템으로 이벤트를 내보내는 데 사용되는 프로토콜입니다. 다음의 표준 프로토콜 중 하나일 수 있습니다: Syslog, CEF 또는 LEEF. SIEM 시스템은 지정한 프로토콜에 따라 메시지 파서를 선택합니다.

사용하는 SIEM 시스템에 따라 몇 가지 추가 수신자 설정을 지정해야 할 수 있습니다.

아래 그림에는 ArcSight의 수신자 설정 화면이 나와 있습니다.



ArcSight의 수신자 설정

메시지 파서

내보낸 이벤트는 SIEM 시스템에 메시지로 전달됩니다. 이러한 메시지를 적절하게 구문 분석해야 SIEM 시스템에서 이벤트에 대한 정보를 사용할 수 있습니다. 메시지 파서는 SIEM 시스템의 일부로, 메시지 내용을 이벤트 ID, 심각도, 설명, 파라미터 등의 관련 필드로 분할하는 데 사용됩니다. 그러면 SIEM 시스템은 Kaspersky Security Center에서 받은 이벤트를 처리하여 SIEM 시스템 데이터베이스에 저장할 수 있습니다.

Syslog 형식으로 SIEM 시스템으로 내보내기 위한 이벤트 표시

이벤트 자동 내보내기를 사용하도록 설정한 후에는 외부 SIEM 시스템으로 내보낼 이벤트를 선택해야 합니다.

다음 조건 중 하나를 기준으로 하여 외부 시스템으로의 Syslog 형식 이벤트 내보내기를 구성할 수 있습니다.

- 일반 이벤트 표시. 이벤트 설정 또는 중앙 관리 서버 설정을 통해 정책에서 내보낼 이벤트를 표시하면 SIEM 시스템은 특정 정책을 통해 관리되는 모든 애플리케이션에서 발생한 표시된 이벤트를 수신하게 됩니다. 내보낸 이벤트를 정책에서 선택한 경우에는 이 정책을 통해 관리되는 개별 애플리케이션에 대해 이벤트를 재정의할 수 없습니다.
- 관리 애플리케이션에 대한 이벤트 표시. 관리 중인 기기에 설치된 개별 관리 애플리케이션에 대해 내보낼 이벤트를 선택하는 경우 SIEM 시스템은 해당 애플리케이션에서 발생한 이벤트만 수신하게 됩니다.

Syslog 형식으로 SIEM 시스템으로 내보내기 위한 이벤트 표시 정보

이벤트 자동 내보내기를 사용하도록 설정한 후에는 외부 SIEM 시스템으로 내보낼 이벤트를 선택해야 합니다.

다음 조건 중 하나를 기준으로 하여 외부 시스템으로의 Syslog 형식 이벤트 내보내기를 구성할 수 있습니다.

- 일반 이벤트 표시. 이벤트 설정 또는 중앙 관리 서버 설정을 통해 정책에서 내보낼 이벤트를 표시하면 SIEM 시스템은 특정 정책을 통해 관리되는 모든 애플리케이션에서 발생한 표시된 이벤트를 수신하게 됩니다. 내보낸 이벤트를 정책에서 선택한 경우에는 이 정책을 통해 관리되는 개별 애플리케이션에 대해 이벤트를 재정의할 수 없습니다.
- 관리 애플리케이션에 대한 이벤트 표시. 관리 중인 기기에 설치된 개별 관리 애플리케이션에 대해 내보낼 이벤트를 선택하는 경우 SIEM 시스템은 해당 애플리케이션에서 발생한 이벤트만 수신하게 됩니다.

Syslog 형식으로 내보내기 위한 Kaspersky 애플리케이션의 이벤트 표시

관리 중인 기기에 설치된 특정 개별 관리 애플리케이션에서 발생한 이벤트를 내보내려는 경우 해당 애플리케이션 정책에서 내보낼 이벤트를 선택합니다. 이 경우 표시된 이벤트를 정책 범위에 포함된 모든 기기에서 내보냅니다.

특정 관리 기기에 대해 내보낼 이벤트 표시 방법:

1. 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동합니다.
2. 이벤트를 표시할 애플리케이션의 정책을 누릅니다.
   정책 설정 창이 열립니다.
3. **이벤트 구성** 섹션으로 이동합니다.
4. SIEM 시스템으로 내보내려는 리포트 옆의 확인란을 선택합니다.
5. **Syslog를 사용하여 SIEM 시스템으로 내보내기로 표시**를 누릅니다.

> 또한, 이벤트 링크를 클릭하면 열리는 **이벤트 등록** 섹션에서 SIEM 시스템으로 내보내기 위한 이벤트를 표시할 수 있습니다.

6. 해당 이벤트 또는 SIEM 시스템으로 내보내기 위해 표시한 이벤트의 **Syslog** 열에 확인 표시(✓)가 나타납니다.

7. **저장** 버튼을 누릅니다.

관리 중인 애플리케이션에서 표시된 이벤트를 SIEM 시스템으로 내보낼 수 있습니다.

특정 관리 기기의 SIEM 시스템으로 내보낼 이벤트를 표시할 수 있습니다. 애플리케이션 정책에서 이전에 내보낸 이벤트가 선택된 경우에는 이 정책을 통해 관리 중인 기기에 대해 표시된 이벤트를 재정의할 수 없습니다.

개별 관리 기기에 대해 내보낼 이벤트 표시 방법:

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
   관리 중인 기기 목록이 표시됩니다.

2. 관리 중인 기기 목록에서 필요한 기기 이름이 포함된 링크를 누릅니다.
   선택한 기기의 속성 창이 표시됩니다.

3. **애플리케이션** 섹션으로 이동합니다.

4. 애플리케이션 목록에서 필요한 애플리케이션 이름이 포함된 링크를 누릅니다.

5. **이벤트 구성** 섹션으로 이동합니다.

6. SIEM 시스템으로 내보내려는 리포트 옆의 확인란을 선택합니다.

7. **Syslog를 사용하여 SIEM 시스템으로 내보내기로 표시**를 누릅니다.

   또한, 이벤트 링크를 클릭하면 열리는 **이벤트 등록** 섹션에서 SIEM 시스템으로 내보내기 위한 이벤트를 표시할 수 있습니다.

8. 해당 이벤트 또는 SIEM 시스템으로 내보내기 위해 표시한 이벤트의 **Syslog** 열에 확인 표시(✓)가 나타납니다.

이제 SIEM 시스템으로 내보내기가 구성된 경우 중앙 관리 서버는 SIEM 시스템에 표시된 이벤트를 전송합니다.

Syslog 형식으로 내보낼 일반 이벤트 표시

Syslog 형식을 사용하여 중앙 관리 서버가 SIEM 시스템으로 내보낼 일반 이벤트를 표시할 수 있습니다.

SIEM 시스템으로 내보내기 위한 일반 이벤트 표시 방법:

1. 다음 중 하나를 수행합니다:

   - 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘(⚙)을 누릅니다.
   - 메인 메뉴에서 **에셋(기기) → 정책 및 프로필**로 이동한 다음 정책 링크를 클릭합니다.

2. 창이 열리면 **이벤트 구성** 탭으로 이동합니다.

3. **Syslog를 사용하여 SIEM 시스템으로 내보내기로 표시**를 클릭합니다.

> 또한, 이벤트 링크를 클릭하면 열리는 **이벤트 등록** 섹션에서 SIEM 시스템으로 내보내기 위한 이벤트를 표시할 수 있습니다.

4. 해당 이벤트 또는 SIEM 시스템으로 내보내기 위해 표시한 이벤트의 **Syslog** 열에 확인 표시(✓)가 나타납니다.

이제 SIEM 시스템으로 내보내기가 구성된 경우 중앙 관리 서버는 SIEM 시스템에 표시된 이벤트를 전송합니다.

CEF 및 LEEF 형식을 사용하여 이벤트 내보내기 정보

CEF 및 LEEF 프로토콜을 사용하여 SIEM 시스템 일반 이벤트와 함께 Kaspersky 애플리케이션에서 중앙 관리 서버로 전송한 이벤트로 내보낼 수 있습니다. 내보내기 이벤트 집합은 미리 정의되어 있으므로 내보낼 이벤트를 선택할 수는 없습니다. SIEM 시스템(QRadar, ArcSight 또는 Splunk)으로 이벤트를 보내기 전에, siem_conversion_rules.xml 파일에 지정된 규칙을 사용하여 Kaspersky Security Center 이벤트를 CEF 및 LEEF 형식의 이벤트로 해석해야 합니다.

사용하는 SIEM 시스템에 따라 내보내기 형식을 선택합니다. 아래 표에는 SIEM 시스템 및 해당 내보내기 형식이 나와 있습니다.

SIEM 시스템으로 이벤트 내보내기 형식

SIEM 시스템	내보내기 형식
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF(Log Event Extended Format)는 IBM Security QRadar SIEM용으로 사용자 지정된 이벤트 형식입니다. QRadar는 LEEF 이벤트를 통합, 식별 및 처리할 수 있습니다. LEEF 이벤트는 UTF-8 문자 인코딩을 사용해야 합니다. LEEF 프로토콜에 대한 세부 정보는 IBM Knowledge Center에서 확인할 수 있습니다.

- CEF(Common Event Format) - 서로 다른 여러 보안 및 네트워크 기기와 애플리케이션의 보안 관련 정보 상호 운용성을 개선하는 개방형 로그 관리 표준입니다. CEF에서는 공통 이벤트 로그 형식을 사용할 수 있으므로, 기업 관리 시스템에서 분석을 위해 데이터를 쉽게 통합하고 집계할 수 있습니다. CEF 이벤트는 UTF-8 문자 인코딩을 사용해야 합니다.

자동 내보내기 시에는 Kaspersky Security Center가 SIEM 시스템으로 일반 이벤트를 보냅니다. 이벤트 자동 내보내기를 사용하도록 설정한 직후에 내보내기가 시작됩니다. 이 섹션에서는 자동 이벤트 내보내기를 사용하도록 설정하는 방법을 자세히 설명합니다.

이벤트를 CEF 또는 LEEF 형식으로 변환

SIEM 시스템(QRadar, ArcSight 또는 Splunk)으로 이벤트를 보내기 전에, siem_conversion_rules.xml 파일에 지정된 규칙을 사용하여 Kaspersky Security Center 이벤트를 CEF 및 LEEF 형식의 이벤트로 해석해야 합니다. 이 파일은 Kaspersky Security Center 배포 키트에 포함되어 있습니다.

siem_conversion_rules.xml 파일에는 이벤트를 CEF 및 LEEF 형식으로 변환하기 위한 사전 정의된 해석 규칙이 포함되어 있습니다. 추가 이벤트 해석 규칙을 사용하려면 해당 규칙을 파일에 수동으로 추가하면 됩니다.

siem_conversion_rules.xml 파일에는 <product name="SP_QRADAR" vendor="IBM"> 및 <product name="SP_QRADAR" vendor="IBM"> 섹션이 포함됩니다. <product name="SP_QRADAR" vendor="IBM"> 섹션에는 QRadar SIEM 시스템으로 내보낼 수 있는 LEEF 형식의 이벤트를 생성하기 위한 규칙이 포함되어 있습니다. <product name="SP_ARCSIGHT" vendor="HP"> 섹션에는 ArcSight 또는 Splunk SIEM 시스템으로 내보낼 수 있는 CEF 형식의 이벤트를 생성하기 위한 규칙이 포함되어 있습니다.

각 섹션에는 <common> 하위 섹션이 있습니다. 여기에는 Kaspersky Security Center 이벤트 속성 및 LEEF 형식으로 된 이벤트의 해당 속성이 있습니다. 이러한 공통 속성은 내보낼 수 있는 모든 유형의 이벤트에 사용됩니다.

또한 각 섹션에는 <event> 하위 섹션이 있습니다. 각 <event> 하위 섹션에는 <common> 섹션에 나열된 속성에 추가되는 속성이 포함되어 있습니다.

siem_conversion_rules.xml 파일에 새로운 이벤트 생성 규칙을 수동으로 추가할 수 있습니다.

새로운 이벤트 생성 규칙을 추가하려면 다음 절차를 따르십시오.

1. 새로운 <event> 하위 섹션을 <product name="SP_QRADAR" vendor="IBM"> 또는 <product name="SP_QRADAR" vendor="IBM"> 섹션에 추가한 다음, 필요한 경우 추가 이벤트 속성을 지정합니다.

2. 이벤트가 공통 속성으로만 구성된 경우, <event> 하위 섹션은 비어 있습니다.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Syslog 형식을 사용한 이벤트 내보내기 정보

Syslog 형식을 사용하여 중앙 관리 서버 및 관리 중인 기기에 설치된 기타 Kaspersky 애플리케이션에서 발생하는 이벤트를 SIEM 시스템으로 내보낼 수 있습니다.

Syslog 프로토콜은 메시지 로깅용 표준 프로토콜입니다. 이 프로토콜을 사용하는 경우 메시지, 메시지를 저장하는 시스템, 그리고 메시지를 보고/분석하는 소프트웨어를 구분할 수 있습니다. 각 메시지에는 메시지를 생성하는 소프트웨어 유형을 나타내는 기능 코드 레이블이 지정되며 심각도가 할당됩니다.

Syslog 형식은 Internet Engineering Task Force(인터넷 표준)에서 게시한 RFC(Request for Comments) 문서를 통해 정의됩니다. Kaspersky Security Center에서 외부 시스템으로 이벤트를 내보낼 때는 RFC 5424 표준이 사용됩니다.

Kaspersky Security Center에서는 Syslog 형식을 사용한 외부 시스템으로의 이벤트 내보내기를 구성할 수 있습니다.

내보내기 프로세스에서는 다음의 두 단계를 수행합니다:

1. 자동 이벤트 내보내기를 사용하도록 설정. 이 단계에서는 SIEM 시스템으로 이벤트를 보내도록 Kaspersky Security Center를 구성합니다. 자동 내보내기를 사용하도록 설정한 직후에 Kaspersky Security Center가 이벤트 보내기를 시작합니다.

2. 외부 시스템으로 내보낼 이벤트 선택. 이 단계에서는 SIEM 시스템으로 내보낼 이벤트를 선택합니다.

SIEM 시스템으로 이벤트를 내보내기 위한 Kaspersky Security Center 구성

이벤트를 SIEM 시스템으로 내보내려면, Kaspersky Security Center 웹 콘솔에서 내보내기 프로세스를 구성해야 합니다.

SIEM 시스템(QRadar, ArcSight 또는 Splunk)으로 이벤트를 보내기 전에, siem_conversion_rules.xml 파일에 지정된 규칙을 사용하여 Kaspersky Security Center 이벤트를 CEF 및 LEEF 형식의 이벤트로 해석해야 합니다.

Kaspersky Security Center 웹 콘솔에서 SIEM 시스템으로 내보내기를 구성하려면:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.

2. **일반** 탭에서 **SIEM로 내보내기** 섹션을 선택합니다.

3. **설정** 링크를 누릅니다.
   설정 내보내기 섹션이 열립니다.

4. **설정 내보내기** 섹션에서 다음 설정을 지정합니다.

   - **SIEM 시스템 서버 주소**

     현재 사용 중인 SIEM 시스템이 설치된 서버의 IP 주소입니다. SIEM 시스템 설정에서 이 값을 확인하십시오.

   - **SIEM 시스템 포트**

     Kaspersky Security Center와 SIEM 시스템 서버 간의 연결을 설정하는 데 사용되는 포트 번호입니다. Kaspersky Security Center 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

- **프로토콜**

  SIEM 시스템으로 메시지를 전송하는 데 사용할 프로토콜을 선택합니다. TCP, UDP 또는 TLS over TCP 프로토콜을 선택할 수 있습니다.

  TCP 프로토콜을 통해 TLS를 선택하면 다음과 같은 TLS 설정을 지정할 수 있습니다.

  - **서버 인증**

    서버 인증 필드에서 다음과 같이 **신뢰할 수 있는 인증서** 또는 **SHA 지문** 값을 선택할 수 있습니다.

    - **신뢰할 수 있는 인증서**. 신뢰하는 인증 기관(CA)에서 루트 인증서가 포함된 전체 인증서 체인을 수신하여 Kaspersky Security Center에 업로드할 수 있습니다. Kaspersky Security Center가 SIEM 시스템 서버의 인증서 체인에 신뢰하는 인증 기관의 서명이 있는지 확인합니다.

      신뢰할 수 있는 인증서를 추가하려면 **CA 인증서 파일 찾기** 버튼을 클릭한 다음 인증서를 업로드합니다.

    - **SHA 지문**. Kaspersky Security Center에서 SIEM 시스템의 전체 인증서 체인(루트 인증서 포함)의 SHA1 지문을 지정할 수 있습니다. SHA1 지문을 추가하려면 **지문** 필드에 입력한 다음 **추가** 버튼을 누릅니다.

      클라이언트 인증 추가 설정을 사용하여 Kaspersky Security Center를 인증하기 위한 인증서를 생성할 수 있습니다. 따라서 Kaspersky Security Center에서 발급한 자체 서명 인증서를 사용하게 됩니다. 이 경우 신뢰할 수 있는 인증서와 SHA 지문을 모두 사용하여 SIEM 시스템 서버를 인증할 수 있습니다.

  - **주체 이름/주체 대체 이름 추가**

    대상 이름은 인증서가 수신되는 도메인 이름입니다. Kaspersky Security Center는 SIEM 시스템 서버의 도메인 이름이 SIEM 시스템 서버 인증서의 대상 이름과 일치하지 않는 경우 SIEM 시스템 서버에 연결할 수 없습니다. 그러나 SIEM 시스템 서버는 인증서에서 이름이 변경된 경우 도메인 이름을 변경할 수 있습니다. 이 경우 **주체 이름/주체 대체 이름 추가** 필드에 주체 이름을 지정할 수 있습니다. 지정된 대상 이름이 SIEM 시스템 인증서의 대상 이름과 일치하면 Kaspersky Security Center가 SIEM 시스템 서버 인증서의 유효성을 검증합니다.

  - **클라이언트 인증 추가**

    클라이언트 인증의 경우 인증서를 삽입하거나 Kaspersky Security Center에서 생성할 수 있습니다.

    - **인증서 삽입** . 신뢰할 수 있는 인증 기관(CA)과 같은 다양한 경로에서 수신된 인증서를 사용할 수 있습니다. 다음 인증서 유형 중 하나를 사용하여 인증서와 개인 키를 지정해야 합니다:

      - **X.509 인증서 PEM**. **인증서가 있는 파일** 필드에 인증서가 있는 파일을 업로드하고 **키가 있는 파일** 필드에 개인 키가 있는 파일을 업로드합니다. 두 파일은 서로 의존하지 않으며 파일의 로딩 순서는 중요하지 않습니다. 두 파일이 모두 업로드되면 **암호 또는 인증서 확인** 필드에 개인 키 디코딩을 위한 암호를 지정합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

      - **X.509 인증서 PKCS12**. **인증서가 있는 파일** 필드에 인증서와 개인 키가 포함된 단일 파일을 업로드합니다. 파일이 업로드되면 **암호 또는 인증서 확인** 필드에 개인 키 디코딩을 위한 암호를 지정합니다. 개인 키가 인코딩되지 않은 경우 암호는 빈 값을 가질 수 있습니다.

    - **키 생성**. Kaspersky Security Center에서 자체 서명 인증서를 생성할 수 있습니다. Kaspersky Security Center는 생성된 인증서를 저장하고 인증서의 공개 부분 또는 SHA1 지문을 SIEM 시스템에 전달할 수 있습니다.

- **데이터 형식**

  SIEM 시스템의 요구 사항에 따라 시스템 로그, CEF, LEEF 형식을 선택할 수 있습니다.

시스템 로그 데이터 형식을 선택한다면, 다음을 지정해야 합니다.

- **최대 메시지 크기, 바이트**

  SIEM 시스템으로 전달되는 메시지 하나의 최대 크기(바이트)를 지정합니다. 각 이벤트는 메시지 하나로 전달됩니다. 실제 메시지 길이가 지정된 값을 초과하면 메시지가 잘리며 데이터가 손실될 수 있습니다. 기본 크기는 2048바이트입니다. 이 필드는 **프로토콜** 필드에서 시스템 로그 형식을 선택했을 때만 사용할 수 있습니다.

5. 필요 시, 중앙 관리 서버 데이터베이스에서 보관된 이벤트를 내보내고 보관된 이벤트 내보내기를 시작할 시작 날짜를 설정할 수 있습니다.

   a. **내보내기 시작 날짜 설정** 링크를 클릭합니다.

   b. 섹션이 열리면 **시스템 이벤트 내보내기 시작 날짜** 필드에 시작 날짜를 지정합니다.

   c. **확인** 버튼을 누릅니다.

6. 옵션을 **SIEM 시스템 데이터베이스로 이벤트 자동 내보내기 활성화됨** 위치로 전환합니다.

7. SIEM 시스템 연결이 구성되었는지 확인하려면 **연결 확인** 버튼을 클릭합니다.
   SIEM 시스템 서버와의 연결이 설정되고 테스트 이벤트가 전송됩니다. 연결 상태가 표시됩니다.

   확인은 TCP 및 TLS over TCP 프로토콜에 대해서만 수행됩니다.

8. **저장** 버튼을 누릅니다.

SIEM 시스템으로 내보내기가 구성되었습니다.

데이터베이스에서 직접 이벤트 내보내기

Kaspersky Security Center 인터페이스를 사용할 필요 없이 Kaspersky Security Center 데이터베이스에서 직접 이벤트를 가져올 수 있습니다. 공용 보기를 직접 쿼리하여 이벤트 데이터를 가져올 수도 있고, `기존 공용 보기를 기준으로 보기를 직접 만든 다음 주소를 지정해 필요한 데이터를 얻을 수도 있습니다.

공용 보기

Kaspersky Security Center 데이터베이스에서는 편의상 공용 보기 집합이 제공됩니다. 이러한 공용 보기의 설명은 klakdb.chm 문서에서 확인할 수 있습니다.

v_akpub_ev_event 공용 보기에는 데이터베이스의 이벤트 파라미터를 나타내는 필드 집합이 포함되어 있습니다. 기기, 애플리케이션, 사용자 등의 기타 Kaspersky Security Center 항목에 해당하는 공용 보기에 대한 정보도 klakdb.chm 문서에서 확인할 수 있습니다. 쿼리에서 이 정보를 사용할 수 있습니다.

이 섹션에는 klsql2 유틸리티를 통해 SQL 쿼리를 실행하는 지침과 쿼리 예제가 포함되어 있습니다.

SQL 쿼리 또는 데이터베이스 보기를 만들려는 경우 데이터베이스 작업을 위한 기타 프로그램도 사용할 수 있습니다. 인스턴스 이름, 데이터베이스 이름 등 Kaspersky Security Center 데이터베이스에 연결하는 데 필요한 파라미터를 확인하는 방법에 대한 정보는 해당 섹션에 나와 있습니다.

klsql2 유틸리티를 사용하여 SQL 쿼리 생성

이 문서에서는 klsql2 유틸리티를 다운로드하고 사용하는 방법과 이 유틸리티로 SQL 쿼리를 실행하는 방법을 설명합니다.

klsql2 유틸리티를 사용하려면:

1. Kaspersky Security Center의 설치 폴더에서 klsql2 유틸리티를 넣습니다. 기본 설치 경로는 <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center입니다. 이전 Kaspersky Security Center 버전용 klsql2 유틸리티 버전을 사용하지 마십시오.

2. 텍스트 편집기에서 .sql 확장자를 가진 파일을 생성하고 유틸리티와 같은 폴더에 파일을 넣습니다.

3. 생성된 .sql 파일에 원하는 SQL 쿼리를 입력한 다음 파일을 저장합니다.

4. Kaspersky Security Center 중앙 관리 서버를 설치한 기기의 명령줄에서 다음 명령을 입력하여 .sql 파일에서 SQL 쿼리를 실행한 다음 result.xml 파일에 결과를 저장합니다.

   ```
   klsql2 -i src.sql -u <사용자 이름> -p <암호> -o result.xml
   ```

   여기서 <사용자 이름> 및 <암호>는 데이터베이스에 대한 액세스 권한이 있는 사용자 계정의 자격 증명입니다.

5. 필요하다면 데이터베이스에 액세스할 수 있는 사용자 계정의 로그인 및 암호를 입력합니다.

6. 새로 작성된 result.xml 파일을 열어 SQL 쿼리 결과를 확인합니다.

.sql 파일을 편집하여 공용 보기에 대해 원하는 SQL 쿼리를 만들 수 있습니다. 그런 후에 명령줄에서 SQL 쿼리를 실행하고 결과를 파일에 저장하면 됩니다.

klsql2 유틸리티의 SQL 쿼리 예제

이 섹션에서는 klsql2 유틸리티를 통해 실행하는 SQL 쿼리의 예제를 제공합니다.

아래 그림에는 지난 7일 동안 기기에서 발생한 이벤트를 가져와서 발생 시간 순서대로 표시하는 과정이 나와 있습니다. 최신 데이터가 먼저 표시됩니다.

Microsoft SQL Server의 예:

```
SELECT
  /* 이벤트 식별자 */
  e.nId,

  /* 이벤트 발생 시간 */
  e.tmRiseTime,

  /* 이벤트 유형의 내부 이름 */
  e.strEventType,

  /* 이벤트의 표시 이름 */
  e.wstrEventTypeDisplayName,

  /* 이벤트의 표시 설명 */
  e.wstrDescription,

  /* 기기가 있는 그룹의 이름 */
  e.wstrGroupName,

  /* 이벤트가 발생한 기기의 표시되는 이름 */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* 이벤트가 발생한 기기의 IP 주소 */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

PostgreSQL의 예:

```
SELECT
  /* 이벤트 식별자 */
  "e"."nId",

  /* 이벤트 발생 시간 */
  "e"."tmRiseTime",

  /* 이벤트 유형의 내부 이름 */
  "e"."strEventType",

  /* 이벤트의 표시 이름*/
  "e"."wstrEventTypeDisplayName",

  /* 이벤트의 표시 설명 */
  "e"."wstrDescription",

  /* 이벤트의 표시 설명 */
  "e"."wstrGroupName",

  /* 이벤트가 발생한 기기의 표시되는 이름 */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* 이벤트가 발생한 기기의 IP 주소 */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

MySQL 또는 MariaDB의 예:

```
SELECT

  /* 이벤트 식별자 */
  `e`.`nId`,

  /* 이벤트 발생 시간 */
  `e`.`tmRiseTime`,

  /* 이벤트 유형의 내부 이름 */
  `e`.`strEventType`,

  /* 이벤트의 표시 이름 */
  `e`.`wstrEventTypeDisplayName`,

  /* 이벤트의 표시 설명 */
  `e`.`wstrDescription`,

  /* 기기 그룹 이름 */
  `e`.`wstrGroupName`,

  /* 이벤트가 발생한 기기의 표시되는 이름 */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* 이벤트가 발생한 기기의 IP 주소 */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Kaspersky Security Center 데이터베이스 이름 확인

SQL Server, MySQL 또는 MariaDB 데이터베이스 관리 도구를 통해 Kaspersky Security Center 데이터베이스에 접근하려는 경우에는 SQL 스크립트 편집기에서 데이터베이스에 연결할 수 있도록 데이터베이스 이름을 알아야 합니다.

Kaspersky Security Center 데이터베이스의 이름을 확인하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘( )을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **현재 데이터베이스 세부 정보** 섹션을 선택합니다.

   데이터베이스 이름 필드에 데이터베이스 이름이 지정됩니다. 데이터베이스 이름을 사용하여 SQL 쿼리의 데이터베이스 주소를 지정합니다.

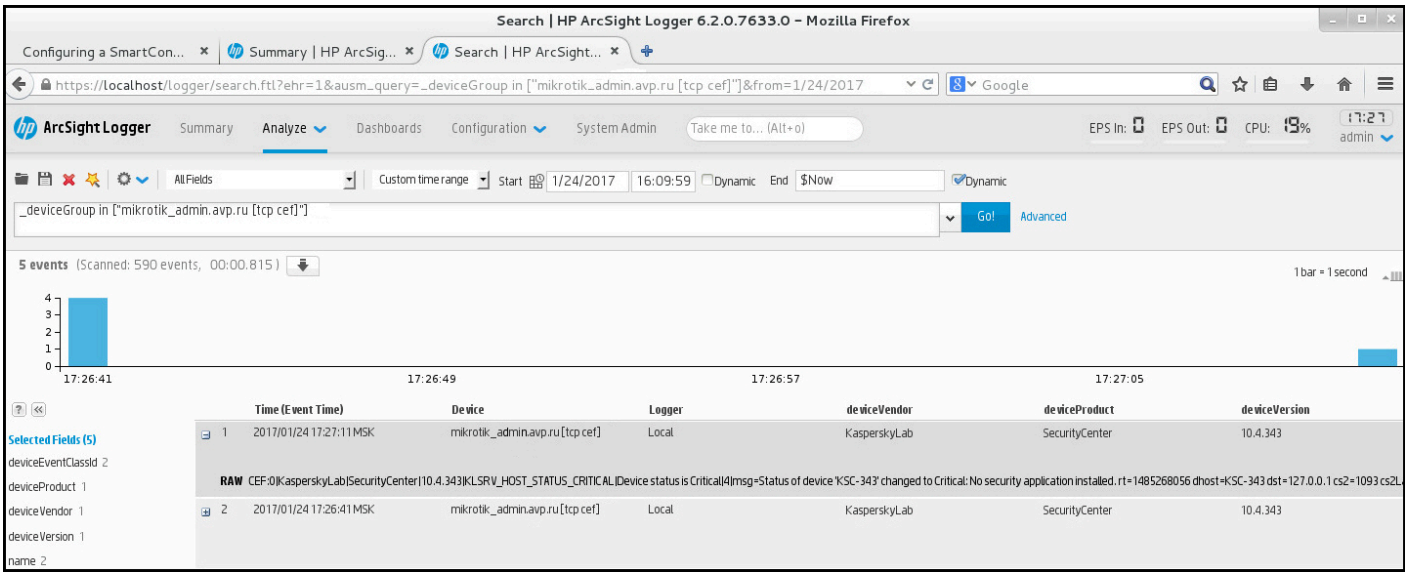
내보내기 결과 보기

이벤트 내보내기 절차가 정상적으로 완료되도록 제어할 수 있습니다. 이렇게 하려면 내보내기 이벤트가 포함된 메시지가 SIEM 시스템에서 수신되는지 확인합니다.

Kaspersky Security Center에서 보낸 이벤트가 SIEM 시스템에서 수신되어 적절하게 구문 분석되면 양쪽에서 모두 구성을 올바르게 수행한 것입니다. 그렇지 않은 경우에는 Kaspersky Security Center에서 지정한 설정을 SIEM 시스템의 구성과 대조하여 확인합니다.

아래 그림에는 ArcSight로 내보낸 이벤트가 나와 있습니다. 예를 들어 첫 번째 이벤트는 심각한 중앙 관리 서버 이벤트입니다: "*기기 상태가 위험입니다*".

SIEM 시스템에서의 내보내기 이벤트 표시 방식은 사용하는 SIEM 이벤트에 따라 다릅니다.



이벤트 예제

클라우드 환경에서 Kaspersky Security Center 웹 콘솔 작동하기

이 섹션에서는 Amazon Web Services, Microsoft Azure, Google Cloud와 같은 클라우드 환경에서의 Kaspersky Security Center 배포 및 유지 관리와 관련된 Kaspersky Security Center 웹 콘솔 기능에 대한 정보를 제공합니다.

클라우드 환경에서 작동하려면 특수한 라이센스가 필요합니다. 이러한 라이센스가 없는 경우 클라우드 기기와 관련된 인터페이스 구성 요소가 표시되지 않습니다.

Kaspersky Security Center 웹 콘솔의 클라우드 환경 구성

클라우드 환경 구성 마법사를 사용하여 Kaspersky Security Center를 구성하려면 다음이 있어야 합니다:

- 클라우드 환경에 대한 특정 자격 증명:
  - 클라우드 세그먼트 검색 권한이 부여된 IAM 역할 또는 클라우드 세그먼트 검색 권한이 부여된 IAM 사용자 계정(Amazon Web Services 작업용)
  - Azure 애플리케이션 ID, 암호, 서브스크립션(Microsoft Azure 작업용)
  - Google 클라이언트 이메일, 프로젝트 ID, 비공개 키(Google Cloud 작업용)

- 설치 패키지:
  - Windows용 네트워크 에이전트
  - Linux용 네트워크 에이전트
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux용 웹 플러그인
- 다음 중 하나를 수행합니다:
  - Kaspersky Endpoint Security for Windows용 설치 패키지 및 웹 플러그인(권장)
  - Kaspersky Security for Windows Server용 설치 패키지 및 웹 플러그인

바로 사용할 수 있는 이미지에서 Kaspersky Security Center 배포 시, 관리 콘솔을 통해 중앙 관리 서버에 처음 연결할 때 클라우드 환경 구성 마법사가 자동 시작됩니다. 언제든지 마법사를 수동으로 시작할 수도 있습니다.

클라우드 환경 구성 마법사를 수동으로 시작하려면:

메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 클라우드 환경 구성**로 이동합니다.

마법사가 시작됩니다.

클라우드 환경 구성의 평균 작업 세션 시간은 약 15분입니다.

1단계. 필요한 플러그인 및 설치 패키지 확인

아래 나열된 필수 웹 플러그인 및 설치 패키지가 모두 있다면 이 단계는 표시되지 않습니다.

클라우드 환경을 구성하려면 다음 구성 요소가 있어야 합니다:

- 설치 패키지:
  - Windows용 네트워크 에이전트
  - Linux용 네트워크 에이전트
  - Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Linux용 웹 플러그인
- 다음 중 하나를 수행합니다:
  - Kaspersky Endpoint Security for Windows용 설치 패키지 및 웹 플러그인(권장)
  - Kaspersky Security for Windows Server용 설치 패키지 및 웹 플러그인

    Kaspersky Security for Windows Server 대신 Kaspersky Endpoint Security for Windows를 사용할 것을 권장합니다.

Kaspersky Security Center는 이미 가지고 있는 구성 요소를 자동 탐지하고 누락된 구성 요소만 나열합니다. **다운로드할 애플리케이션 선택** 버튼을 클릭한 다음 필요한 플러그인 및 설치 패키지를 선택하여 나열된 구성 요소를 다운로드합니다. 구성 요소를 다운로드한 후 **새로 고침** 버튼을 사용하여 누락된 구성 요소 목록을 업데이트할 수 있습니다.

2단계. 애플리케이션 라이센싱

이 단계는 BYOL AMI를 사용 중이고 Kaspersky Security for Virtualization 라이센스 또는 Kaspersky Hybrid Cloud Security 라이센스로 애플리케이션을 활성화한 적이 없는 경우에만 표시됩니다.

라이센스 키를 지정하고 **다음**을 눌러 계속 진행합니다.

라이센스 키가 중앙 관리 서버 스토리지에 추가됩니다.

마법사를 다시 실행하면 이 단계가 표시되지 않습니다.

3단계. 클라우드 환경 및 권한 선택

이 섹션에서는 Kaspersky Security Center 12.1 이상 버전에만 적용되는 기능에 대해 설명합니다.

다음 설정을 지정합니다:

- **클라우드 환경**

  Kaspersky Security Center를 배포할 클라우드 환경을 AWS, Azure 또는 Google 클라우드 중에서 선택합니다.

  둘 이상의 클라우드 환경에서 작업하려면, 하나의 환경을 선택한 다음 마법사를 다시 실행합니다.

- **연결 이름**

  연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.

  이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.

  둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

지정한 클라우드 환경에서 인증을 받으려면 자격 증명을 입력합니다.

AWS

클라우드 세그먼트 유형으로 AWS를 선택한 경우 클라우드 세그먼트의 추가 검색을 위해서는 IAM 역할 또는 AWS IAM 액세스 키가 필요합니다.

- **EC2 인스턴스에 할당된 AWS IAM 역할**

  중앙 관리 서버에 필요한 권한이 포함된 IAM 역할이 있는 경우 이 옵션을 선택합니다.

- **AWS IAM 사용자**

  AWS IAM 액세스 키가 있는 경우 이 옵션을 선택합니다. 다음과 같이 키 데이터를 입력합니다.

  - **접근 키 ID**

    IAM 액세스 키 ID는 영숫자 문자 시퀀스입니다. IAM 사용자 계정을 만들 때 키 ID가 제공됩니다.

    IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

  - **비밀 키**

    IAM 사용자 계정을 만들 때 액세스 키 ID와 함께 제공된 비밀 키입니다.

    비밀 키의 문자는 별표로 표시됩니다. 비밀 키 입력을 시작하면 **표시** 버튼이 나타납니다. 이 버튼을 필요한 시간 동안 누르고 있으면 입력한 문자가 표시됩니다.

    IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

    입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

Azure

클라우드 세그먼트 유형으로 Azure를 선택한 경우 추가적인 클라우드 세그먼트 검색에 사용할 연결에 대해 다음과 같은 설정을 지정합니다.

- **Azure 애플리케이션 ID**

  Azure Portal에서 생성한 애플리케이션 ID입니다.

  검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

- **Azure 서브스크립션 ID**

  Azure Portal에서 생성한 서브스크립션입니다.

- **Azure 애플리케이션 암호**

  애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

  암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

  입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

- **Azure 스토리지 계정 이름**

  Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

- **Azure 스토리지 액세스 키**

  Kaspersky Security Center에서 사용하기 위해 Azure 스토리지 계정을 생성할 때 제공된 암호(키)입니다.

  키는 "Azure 스토리지 계정 개요" 섹션의 "키" 하위 섹션에서 제공됩니다.

  입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

Google Cloud

클라우드 세그먼트 유형으로 Google Cloud를 선택한 경우 추가적인 클라우드 세그먼트 검색에 사용할 연결에 대해 다음과 같은 설정을 지정하십시오.

- **클라이언트 이메일 주소**

  클라이언트 이메일은 Google Cloud에 프로젝트를 등록하는 데 사용한 이메일 주소입니다.

- **프로젝트 ID**

  프로젝트 ID는 Google Cloud에 프로젝트를 등록할 때 받은 ID입니다.

- **개인 키**

  개인 키는 Google Cloud에 프로젝트를 등록할 때 개인 키로 받은 문자열입니다. 실수가 생기지 않도록 이 문자열을 복사 후 붙여 넣으십시오.

  입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

지정한 연결은 애플리케이션 설정에 저장됩니다.

클라우드 환경 구성 마법사를 사용하면 하나의 세그먼트만 지정할 수 있습니다. 나중에 더 많은 연결을 지정하여 다른 클라우드 세그먼트를 관리할 수 있습니다.

다음을 눌러 계속 진행합니다.

4단계. 세그먼트 폴링, 클라우드와의 동기화 구성 및 추가 작업 선택

이 단계에서는 클라우드 세그먼트 검색이 시작되며 클라우드 기기용 특수 관리 그룹이 만들어집니다. 검색 중 검색된 기기는 이 그룹에 배치됩니다. 클라우드 세그먼트 검색 일정이 구성됩니다(기본적으로 5분마다, 이 설정은 나중에 변경 가능).

클라우드와 동기화 자동 이동 규칙도 만들어집니다. 이 단계 후에는 클라우드 네트워크를 검사할 때마다 발견된 가상 기기가 **관리 중인 기기\클라우드** 그룹 내의 해당 하위 그룹으로 이동됩니다.

다음 설정을 정의합니다:

- **클라우드 구조와 관리 그룹 동기화**

  이 옵션을 활성화하면 **클라우드** 그룹이 **관리 중인 기기** 그룹 내에 자동으로 만들어지고 클라우드 기기 발견이 시작됩니다. 각 클라우드 네트워크 검사 중에 탐지된 인스턴스 및 가상 컴퓨터는 클라우드 그룹에 배치됩니다. 이 그룹 내의 관리 하위 그룹 구조는 클라우드 세그먼트의 구조와 일치합니다. AWS에서는 구조에 가용 영역 및 배치 그룹이 표시되지 않으며 Azure에서는 구조에 서브넷이 표시되지 않습니다. 클라우드 환경의 인스턴스로 식별되지 않은 기기는 **미할당 기기** 그룹에 포함됩니다. 이 그룹 구조를 통해 그룹 설치 작업을 사용하여 인스턴스에 안티 바이러스 애플리케이션을 설치할 수 있으며 그룹별로 다른 정책을 설정할 수 있습니다.

  이 옵션을 비활성화하면 **클라우드** 그룹도 생성되며 클라우드 기기 발견도 시작됩니다. 하지만 클라우드 세그먼트 구조와 일치하는 하위 그룹이 그룹 내에 생성되지는 않습니다. 탐지된 모든 인스턴스는 **클라우드** 관리 그룹에 있으므로 목록 하나에 표시됩니다. Kaspersky Security Center 작업이 동기화를 요구한다면 **클라우드와 동기화** 규칙의 속성을 수정하고 그 규칙을 강제로 적용할 수 있습니다. 이 규칙을 적용하면 클라우드 그룹의 하위 그룹 구조가 클라우드 세그먼트의 구조와 일치하도록 변경됩니다.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **보호 배포**

  이 옵션을 선택하면 마법사가 인스턴스에 보안 제품을 설치하는 작업을 생성합니다. 마법사가 완료되면 클라우드 세그먼트의 기기에서 보호 배포 마법사가 자동 시작되며 ,해당 기기에 네트워크 에이전트 및 보안 제품을 설치할 수 있습니다.

  Kaspersky Security Center는 기본 도구를 사용하여 배포를 수행할 수 있습니다. EC2 인스턴스나 Azure 가상 컴퓨터에 애플리케이션을 설치할 권한이 없다면 **원격 설치** 작업을 수동으로 구성하고 필요한 권한이 있는 계정을 지정할 수 있습니다. 이 경우 AWS API 또는 Azure를 사용하여 검색된 기기에 대해서는 원격 설치 작업이 작동하지 않습니다. 이 작업은 Active Directory 검색, Windows 도메인 검색 또는 IP 범위 검색을 사용하여 검색된 기기에 대해서만 작동합니다.

  이 옵션을 선택하지 않으면 보호 배포 마법사가 시작되지 않으며 인스턴스에 보안 제품을 설치하는 작업이 생성되지 않습니다. 이 두 작업은 나중에 수동으로 수행할 수 있습니다.

보호 배포 옵션을 선택하면 **기기 다시 시작** 섹션을 사용할 수 있게 됩니다. 이 섹션에서 대상 기기의 운영 체제를 다시 시작해야 하는 경우 수행할 작업을 선택해야 합니다. 애플리케이션 설치 중에 기기 운영 체제를 다시 시작해야 하는 경우 인스턴스를 다시 시작할지 여부를 선택합니다:

- **다시 시작 안 함**

  이 옵션을 선택하면 보안 제품 설치 후에 기기가 다시 시작되지 않습니다.

- **다시 시작**

  이 옵션을 선택하면 보안 제품 설치 후에 기기가 다시 시작됩니다.

다음을 눌러 계속 진행합니다.

Google 클라우드는 Kaspersky Security Center 기본 도구로만 배포를 수행할 수 있습니다. Google 클라우드를 선택한 경우 **보호 배포** 옵션을 사용할 수 없습니다.

5단계. 정책 및 작업을 생성할 애플리케이션 선택

이 단계는 Kaspersky Endpoint Security for Windows 및 Kaspersky Security for Windows Server 모두에 대한 설치 패키지와 플러그인이 있을 때만 표시됩니다. 해당 애플리케이션 중 하나에 대한 플러그인 및 설치 패키지만 있다면 이 단계를 건너뛰고 Kaspersky Security Center가 기존 애플리케이션에 대한 정책 및 작업을 생성합니다.

정책 및 작업을 생성할 애플리케이션을 선택합니다:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

6단계. Kaspersky Security Center용 Kaspersky Security Network 구성

Kaspersky Security Center(KSN) 작동 관련 정보를 Kaspersky Security Network 기술 자료로 전달하기 위한 설정을 지정합니다. 다음 옵션 중 하나를 선택합니다:

- **Kaspersky Security Network 사용에 동의합니다**

  클라이언트 기기에 설치된 Kaspersky Security Center 및 관리 중인 애플리케이션은 작업 세부 정보를 Kaspersky Security Network로 자동 전송합니다. Kaspersky Security Network에 참여하면 바이러스 및 기타 위협 관련 정보가 포함된 데이터베이스를 보다 빠르게 업데이트할 수 있으므로 새로운 보안 위협에 더욱 신속하게 대응할 수 있습니다.

- **Kaspersky Security Network 사용에 동의하지 않습니다**

  Kaspersky Security Center 및 관리 중인 애플리케이션은 Kaspersky Security Network로 정보를 제공하지 않습니다.

  이 옵션을 선택하면 Kaspersky Security Network 사용이 비활성화됩니다.

Kaspersky Security Network에 참여하는 것이 좋습니다.

관리 중인 애플리케이션에 대한 KSN 계약도 표시될 수 있습니다. Kaspersky Security Network 사용에 동의하면 관리 중인 애플리케이션에서 Kaspersky로 데이터를 전송합니다. Kaspersky Security Network 참여에 동의하지 않으면 관리되는 애플리케이션이 Kaspersky에 데이터를 보내지 않습니다. (나중에 애플리케이션 정책에서 이 설정을 변경할 수 있습니다.)

다음을 눌러 계속 진행합니다.

7단계. 초기 보호 구성 생성

만들어진 정책 및 작업 목록을 확인할 수 있습니다.

정책 및 작업 만들기가 완료되기를 기다렸다가 **다음**을 눌러 계속 진행합니다. 마법사 마지막 페이지에서 **마침** 버튼을 눌러 종료합니다.

Kaspersky Security Center 웹 콘솔을 통한 네트워크 세그먼트 검색

중앙 관리 서버는 AWS API, Azure API 또는 Google API 도구를 사용해 클라우드 세그먼트를 정기적으로 검색하여 네트워크의 구조(및 내부 기기) 및 해당 네트워크의 기기에 대한 정보를 받습니다. Kaspersky Security Center는 수집된 정보와 회사 네트워크 구조의 세부 정보를 사용하여 미할당 기기 및 관리 중인 기기 폴더의 컨텐츠를 업데이트할 때 이 정보를 사용합니다. 기기가 관리 그룹으로 자동으로 이동하도록 구성된 경우에는 발견된 기기가 관리 그룹에 포함됩니다.

중앙 관리 서버에서 클라우드 세그먼트를 검색할 수 있게 하려면, AWS의 경우 IAM 역할 또는 IAM 사용자 계정, Azure의 경우 애플리케이션 ID 및 암호, 또는 Google 클라이언트 이메일, Google 프로젝트 ID 및 개인 키(Google Cloud)와 함께 제공되는 해당 권한이 있어야 합니다.

연결을 추가하고 삭제할 수 있으며 각 클라우드 세그먼트에 대한 검색 일정을 설정할 수 있습니다.

클라우드 세그먼트 검색에 대한 연결 추가

이용 가능한 연결 목록에 클라우드 세그먼트 검색에 대한 연결을 추가하려면 아래와 같이 진행합니다:

1. 메인 메뉴에서 **발견 및 배포** → **발견** → **클라우드**로 이동합니다.
2. 창이 열리면 **속성**을 누릅니다.
3. **설정** 창이 열리면 **추가**를 누릅니다.
   클라우드 세그먼트 설정 창이 열립니다.
4. 추가적인 클라우드 세그먼트 검색에 사용할 연결에 대해 클라우드 환경의 이름을 지정합니다.

   - **클라우드 환경**

     Kaspersky Security Center를 배포할 클라우드 환경을 AWS, Azure 또는 Google 클라우드 중에서 선택합니다.

     둘 이상의 클라우드 환경에서 작업하려면, 하나의 환경을 선택한 다음 마법사를 다시 실행합니다.

   - **연결 이름**

     연결의 이름을 입력합니다. 이름은 256자를 초과할 수 없습니다. 유니코드 문자만 사용할 수 있습니다.

     이 이름은 클라우드 기기의 관리 그룹 이름으로도 사용됩니다.

     둘 이상의 클라우드 환경에서 작업하려는 경우 "Azure 세그먼트," "AWS 세그먼트," 또는 "Google 세그먼트"와 같이 연결 이름에 환경 이름을 포함시키십시오.

5. 지정한 클라우드 환경에서 인증을 받으려면 자격 증명을 입력합니다.

- AWS를 선택한 경우 다음 설정을 지정하십시오.
  - **AWS IAM 역할 사용**

    이미 AWS 서비스를 사용하기 위해 중앙 관리 서버에 대한 IAM 역할을 만들었다면 이 옵션을 선택합니다.

  - **AWS IAM 사용자 계정 자격 증명**

    필요한 권한을 가진 IAM 사용자 계정이 있고 키 ID와 비밀 키를 입력할 수 있다면 이 옵션을 선택합니다.

    AWS IAM 사용자 계정 자격 증명을 지정한 경우 다음을 지정합니다.

    - **접근 키 ID**

      IAM 액세스 키 ID는 영숫자 문자 시퀀스입니다. IAM 사용자 계정을 만들 때 키 ID가 제공됩니다.

      IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

    - **비밀 키**

      IAM 사용자 계정을 만들 때 액세스 키 ID와 함께 제공된 비밀 키입니다.

      비밀 키의 문자는 별표로 표시됩니다. 비밀 키 입력을 시작하면 **표시** 버튼이 나타납니다. 이 버튼을 필요한 시간 동안 누르고 있으면 입력한 문자가 표시됩니다.

      IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

    입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

- Azure를 선택한 경우 다음 설정을 지정하십시오.
  - **Azure 애플리케이션 ID**

    Azure Portal에서 생성한 애플리케이션 ID입니다.

    검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

  - **Azure 서브스크립션 ID**

    Azure Portal에서 생성한 서브스크립션입니다.

  - **Azure 애플리케이션 암호**

    애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

- **Azure 스토리지 계정 이름**

  Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

- **Azure 스토리지 접근 키**

  Kaspersky Security Center에서 사용하기 위해 Azure 스토리지 계정을 생성할 때 제공된 암호(키)입니다.

  키는 "Azure 스토리지 계정 개요" 섹션의 "키" 하위 섹션에서 제공됩니다.

  입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

Google 클라우드를 선택한 경우 다음 설정을 지정하십시오.

- **클라이언트 이메일 주소**

  클라이언트 이메일은 Google Cloud에 프로젝트를 등록하는 데 사용한 이메일 주소입니다.

- **프로젝트 ID**

  프로젝트 ID는 Google Cloud에 프로젝트를 등록할 때 받은 ID입니다.

- **개인 키**

  개인 키는 Google Cloud에 프로젝트를 등록할 때 개인 키로 받은 문자열입니다. 실수가 생기지 않도록 이 문자열을 복사 후 붙여 넣으십시오.

  입력한 문자를 보려면 **보기** 버튼을 길게 누릅니다.

6. 원하는 경우 **검색 스케줄 설정**을 누르고 기본 설정을 변경합니다.

이 연결은 애플리케이션 설정에 저장됩니다.

새 클라우드 세그먼트를 처음으로 검색하고 나면 이 세그먼트에 해당하는 하위 그룹이 **관리 중인 기기\클라우드** 관리 그룹에 표시됩니다.

잘못된 자격증명을 지정하면 클라우드 세그먼트 검색 중에 인스턴스가 검색되지 않으며 **관리 중인 기기\클라우드** 관리 그룹에 새 하위 그룹이 표시되지 않습니다.

클라우드 세그먼트 검색에 대한 연결 삭제

특정 클라우드 세그먼트를 더 이상 검색할 필요가 없는 경우 해당하는 연결을 사용 가능한 연결 목록에서 삭제할 수 있습니다. 클라우드 세그먼트 검색 권한이 다른 자격 증명을 가진 다른 사용자에게로 이전된 경우 등에도 연결을 삭제할 수 있습니다.

연결을 삭제하려면 다음과 같이 진행합니다:

1. 메인 메뉴에서 **발견 및 배포** → **발견** → **클라우드**로 이동합니다.
2. 창이 열리면 **속성**을 누릅니다.
3. **설정** 창이 열리면 삭제할 세그먼트 이름을 누릅니다.
4. **삭제**를 누릅니다.
5. 창이 열리면 **확인** 버튼을 눌러 사용자의 선택을 다시 확인합니다.

   연결이 삭제됩니다. 이 연결에 해당하는 클라우드 세그먼트의 기기는 관리 그룹에서 자동으로 삭제됩니다.

Kaspersky Security Center 웹 콘솔을 통한 검색 스케줄 구성

클라우드 세그먼트 검색은 스케줄에 따라 수행됩니다. 검색 빈도를 설정할 수 있습니다.

클라우드 환경 구성 설정에서 검색 빈도를 5분으로 자동 설정합니다. 언제든지 이 값을 변경하여 다른 스케줄을 설정할 수 있습니다. 그러나 검색 실행 빈도는 5분보다 더 짧게 구성하지 않는 것이 좋습니다. 빈도를 너무 짧게 구성하면 API 작업에서 오류가 발생할 수 있기 때문입니다.

클라우드 세그먼트 검색 스케줄을 구성하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **발견 및 배포** → **발견** → **클라우드**로 이동합니다.
2. 창이 열리면 **속성**을 누릅니다.
3. **설정** 창이 열리면 검색 스케줄을 구성할 세그먼트의 이름을 누릅니다.
   이렇게 하면 **클라우드 세그먼트 설정** 창이 열립니다.
4. **클라우드 세그먼트 설정** 창에서 **검색 스케줄 설정** 버튼을 누릅니다.
   이렇게 하면 **스케줄** 창이 열립니다.
5. **스케줄** 창에서 다음 설정을 정의합니다.

   - **시작 스케줄**
     검색 스케줄 옵션:

     - **N일마다**

       검색이 지정한 날짜와 시간부터 지정된 일 단위 간격에 따라 주기적으로 실행됩니다.
       기본적으로 검색은 현재 시스템 날짜와 시간부터 매일 실행됩니다.

- N분마다

  검색이 지정한 시간부터 지정된 분 단위 간격에 따라 주기적으로 실행됩니다.
  기본적으로 검색은 현재 시스템 시간부터 5분마다 실행됩니다.

- 요일별

  검색이 지정한 요일의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 검색은 매주 금요일 오후 6:00:00에 실행됩니다.

- 매달 선택한 주간의 지정한 날짜

  검색이 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

- **시작 간격**

  N이 같은 대상(분 또는 일)을 지정합니다.

- **시작**

  첫 검색을 시작할 시점을 지정합니다.

- **누락된 작업 실행**

  중앙 관리 서버는 검색이 예정된 시간 동안 꺼지거나 사용할 수 없는 상태가 되면 켜진 직후 검색을 시작하거나 검색이 예정된 다음 시간까지 기다릴 수 있습니다.
  이 옵션을 활성화하면 중앙 관리 서버는 켜진 직후에 검색을 시작합니다.
  이 옵션을 비활성화하면 중앙 관리 서버는 검색이 예정된 다음 시간까지 기다립니다.
  기본적으로 이 옵션은 켜져 있습니다.

6. 변경 사항을 저장합니다.

   세그먼트의 검색 스케줄이 구성 및 저장됩니다.

Kaspersky Security Center 웹 콘솔을 통한 클라우드 세그먼트 검색 결과 보기

클라우드 세그먼트 검색 결과, 즉 중앙 관리 서버에서 관리되는 클라우드 기기의 목록을 확인할 수 있습니다.

클라우드 세그먼트 검색 결과를 보려면

메인 메뉴에서 **발견 및 배포** → **발견** → **클라우드**로 이동합니다.

이렇게 하면 검색에 사용할 수 있는 클라우드 세그먼트가 표시됩니다.

Kaspersky Security Center 웹 콘솔을 통한 클라우드 기기 속성 보기

클라우드 기기의 속성을 볼 수 있습니다.

클라우드 기기의 속성을 보려면 다음과 같이 하십시오.

1. 메인 메뉴에서 **에셋(기기) → 관리 중인 기기** 로 이동합니다.
2. 속성을 볼 기기의 이름을 누릅니다.
   일반 섹션이 선택된 상태로 속성 창이 열립니다.
3. 클라우드 기기에 대한 속성을 보려면 속성 창에서 **시스템** 섹션을 선택합니다.
   기기의 클라우드 플랫폼에 따라 속성이 표시됩니다.
   AWS의 기기에 대해 다음 속성이 표시됩니다.

   - **API를 사용해 발견된 기기**(값: **AWS**)
   - **클라우드 리전**
   - **클라우드 VPC**
   - **클라우드 가용 영역**
   - **클라우드 서브넷**
   - **클라우드 배치 그룹**(이 단위는 인스턴스가 배치 그룹에 속하는 경우에만 표시되고 그렇지 않으면 표시되지 않음)

   Azure의 기기에 대해 다음 속성이 표시됩니다.

   - **API를 사용해 발견된 기기**(값: **Microsoft Azure**)
   - **클라우드 리전**
   - **클라우드 서브넷**

   Google Cloud의 기기에 대해 다음 속성이 표시됩니다.

   - **API를 사용해 발견된 기기**(값: **Google Cloud**)
   - **클라우드 리전**
   - **클라우드 VPC**
   - **클라우드 가용 영역**
   - **클라우드 서브넷**

클라우드와 동기화: 이동 규칙 구성

클라우드 환경 구성 동작을 수행하는 동안 클라우드와 동기화 규칙이 자동으로 만들어집니다. 이 규칙을 사용하면 중앙 집중식 관리에 사용할 수 있도록 각 검색에서 감지된 기기를 미할당 기기 그룹에서 관리 중인 기기\클라우드 그룹에 자동으로 이동 수 있습니다. 이 규칙은 기본적으로 만들어진 후에 활성화됩니다. 언제든지 규칙을 비활성하거나 수정하거나 강제로 적용할 수 있습니다.

클라우드와 동기화 규칙 속성을 편집하거나 규칙을 강제로 적용하려면 아래와 같이 진행합니다.

1. 메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 이동 규칙**으로 이동합니다.
   이동 규칙 목록이 열립니다.
2. 이동 규칙 목록에서 **클라우드와 동기화**를 선택합니다.
   그러면 규칙 속성 창이 열립니다.
3. 필요한 경우 **클라우드 세그먼트** 탭의 **규칙 조건** 탭에서 다음 설정을 지정합니다.

- **기기가 클라우드 세그먼트에 있습니다**

  선택한 클라우드 세그먼트에 있는 기기에만 이 규칙이 적용됩니다. 그렇지 않은 경우에는 검색된 모든 기기에 규칙이 적용됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **자식 개체 포함**

  선택한 세그먼트 및 모든 중첩 클라우드 하위 섹션에 있는 모든 기기에 규칙이 적용됩니다. 그렇지 않은 경우에는 루트 세그먼트에 있는 기기에만 규칙이 적용됩니다.

  기본적으로 이 옵션은 선택되어 있습니다.

- **중첩된 개체에서 해당하는 하위 그룹으로 기기 이동**

  이 옵션을 활성화하면 중첩된 개체의 기기가 개체 구조에 해당하는 하위 그룹으로 이동됩니다.

  이 옵션을 비활성화하면 중첩된 개체의 기기가 클라우드 하위 그룹 루트로 자동으로 이동되며 추가 분기는 설정되지 않습니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성**

  이 옵션을 활성화하는 경우 **관리 중인 기기\클라우드** 그룹 구조에 기기가 포함된 섹션과 일치하는 하위 그룹이 없으면 Kaspersky Security Center에서 해당 하위 그룹을 생성합니다. 예를 들어 기기 발견 중에 새 서브넷이 발견되면 **관리 중인 기기\클라우드** 그룹 아래에 같은 이름의 새 그룹이 생성됩니다.

  이 옵션을 비활성화하면 Kaspersky Security Center에서 새 하위 그룹을 생성하지 않습니다. 예를 들어 네트워크 검색 중에 새 서브넷이 발견되어도 **관리 중인 기기\클라우드** 그룹 아래에 같은 이름의 새 그룹이 생성되지 않으며 서브넷의 기기는 **관리 중인 기기\클라우드** 그룹으로 이동됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

- **클라우드 세그먼트에 일치하는 항목이 없는 하위 그룹 삭제**

  이 옵션을 활성화하면 애플리케이션이 기존 클라우드 개체와 일치하지 않는 모든 하위 그룹을 클라우드 그룹에서 삭제합니다.

  이 옵션을 비활성화하면 기존 클라우드 개체와 일치하지 않는 하위 그룹이 유지됩니다.

  기본적으로 이 옵션은 켜져 있습니다.

  클라우드 환경 구성 사용 시 **클라우드 구조와 관리 그룹 동기화** 옵션을 활성화했다면 **클라우드와 동기화** 및 **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성** 옵션이 활성화된 상태로 **클라우드 세그먼트에 일치하는 항목이 없는 하위 그룹 삭제** 규칙이 생성됩니다.

  클라우드 구조와 관리 그룹 동기화 옵션을 활성화하지 않았다면 이러한 옵션이 비활성화된 상태(지워진 상태)로 **클라우드와 동기화** 규칙이 생성됩니다. Kaspersky Security Center를 사용하는 작업에서 **관리 중인 기기\클라우드** 하위 그룹의 하위 그룹 구조가 클라우드 세그먼트의 구조와 일치해야 한다면 규칙 속성에서 **새로 탐지된 기기의 컨테이너에 해당하는 하위 그룹 생성** 및 **클라우드 세그먼트에 일치하는 항목이 없는 하위 그룹 삭제** 옵션을 활성화하고 규칙을 강제로 적용합니다.

4. **API를 사용해 발견된 기기** 드롭다운 목록에서 다음 값 중 하나를 선택하십시오:

   - **아니요**. 기기를 AWS, Azure 또는 Google API를 사용해 찾을 수 없습니다. 즉 클라우드 환경 밖에 있거나 클라우드 환경 내에 있지만 어떠한 이유로 인해 API를 사용해 찾을 수 없다는 것입니다.
   - **AWS**. AWS API를 사용하여 기기를 발견합니다. 즉, 해당 기기는 명확히 AWS 클라우드 환경에 있습니다.
   - **Azure**. Azure API를 사용하여 기기를 발견합니다. 즉, 해당 기기는 명확히 Azure 클라우드 환경에 있습니다.
   - **Google Cloud**. Google API를 사용하여 기기를 발견했습니다. 즉, 해당 기기는 명확히 Google 클라우드 환경에 있습니다.
   - 값 없음. 이 기준은 적용할 수 없습니다.

5. 필요한 경우 다른 섹션에서 기타 규칙 속성을 설정합니다.

이동 규칙이 구성됩니다.

Azure 가상 컴퓨터에 애플리케이션 원격 설치

Microsoft Azure 가상 컴퓨터에 애플리케이션을 설치하려면 유효한 라이센스가 있어야 합니다.

Kaspersky Security Center는 다음 시나리오를 지원합니다:

- Azure API를 통해 클라이언트 기기를 검색하고 설치를 수행합니다. Azure API를 사용하면 다음 애플리케이션만 설치할 수 있습니다:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- 클라이언트 기기는 Azure API를 통해 검색됩니다. 설치는 배포 지점을 통해 수행되거나 배포 지점이 없을 시 독립 실행형 설치 패키지를 사용하여 수동으로 수행됩니다. 이 방법으로 Kaspersky Security Center에서 지원하는 모든 애플리케이션을 설치할 수 있습니다.

Azure 가상 컴퓨터에 애플리케이션 원격 설치 작업을 만들려면:

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다.
3. 마법사의 지침을 따릅니다:
   a. 작업 유형으로 **원격으로 애플리케이션 설치**를 선택합니다.
   b. **설치 패키지** 페이지에서 **Microsoft Azure API를 통해 원격 설치**를 선택합니다.
   c. 기기에 액세스할 계정을 선택할 때 기존 Azure 계정을 사용하거나 **추가**를 클릭하고 Azure 계정의 자격 증명을 입력합니다:
      - **Azure 계정 이름**

        지정하려는 자격 증명의 이름을 입력합니다. 이 이름은 작업을 실행할 계정 목록에 표시됩니다.

      - **Azure 애플리케이션 ID**

        Azure Portal에서 생성한 애플리케이션 ID입니다.
        검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

      - **Azure 애플리케이션 암호**

        애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.
        암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

   d. **관리 중인 기기\클라우드** 그룹에서 관련 기기를 선택합니다.

마법사를 마친 이후에 작업 목록에 애플리케이션 원격 설치를 위한 작업이 표시됩니다.

클라우드 DBMS를 사용하여 중앙 관리 서버 데이터 작업의 백업 생성

백업 작업은 중앙 관리 서버 작업입니다. 클라우드 환경 (AWS 또는 Azure)에 있는 DBMS를 사용하려면 백업 작업을 생성합니다.

중앙 관리 서버 데이터 백업 작업을 만들려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창에서 **에셋(기기)** → **작업**으로 이동합니다.
2. **추가**를 누릅니다.
   새 작업 마법사가 시작됩니다.

3. 마법사 첫 번째 페이지의 **애플리케이션** 목록에서 **Kaspersky Security Center 15.1**를 선택하고 **작업 유형** 목록에서 **중앙 관리 서버 데이터 백업**을 선택합니다.

4. 마법사의 해당 페이지에서 다음 정보를 지정합니다:

- AWS에서 데이터베이스로 작업하는 경우:
  - **S3 버킷 이름**

    백업용으로 생성한 S3 버킷의 이름입니다.

  - **액세스 키 ID**

    S3 버킷 스토리지 인스턴스 사용을 위해 IAM 사용자 계정을 만들 때 키 ID(영숫자 문자 시퀀스)가 제공됩니다.

    S3 버킷에서 RDS DB를 선택한 경우 이 필드를 사용할 수 있습니다.

  - **비밀 키**

    IAM 사용자 계정을 만들 때 액세스 키 ID와 함께 제공된 비밀 키입니다.

    비밀 키의 문자는 별표로 표시됩니다. 비밀 키 입력을 시작하면 **표시** 버튼이 나타납니다. 이 버튼을 필요한 시간 동안 누르고 있으면 입력한 문자가 표시됩니다.

    IAM 역할 대신에 승인을 받기 위해 AWS IAM 액세스 키를 선택한 경우 이 필드를 사용할 수 있습니다.

- Microsoft Azure에서 데이터베이스로 작업하는 경우:
  - **Azure 스토리지 계정 이름**

    Kaspersky Security Center에서 사용하기 위해 생성한 Azure 스토리지 계정의 이름입니다.

  - **Azure 서브스크립션 ID**

    Azure Portal에서 생성한 서브스크립션입니다.

  - **Azure 암호**

    애플리케이션 ID를 만들 때 제공된 애플리케이션 ID의 암호입니다.

    암호 문자는 별표로 표시됩니다. 암호 입력을 시작하면 **보기** 버튼을 사용할 수 있게 됩니다. 이 버튼을 길게 누르면 입력한 문자가 표시됩니다.

  - **Azure 애플리케이션 ID**

    Azure Portal에서 생성한 애플리케이션 ID입니다.

    검색 및 기타 용도로 사용할 Azure 애플리케이션 ID를 하나만 입력할 수 있습니다. 다른 Azure 세그먼트를 검색하려는 경우에는 기존 Azure 연결을 먼저 삭제해야 합니다.

- **Azure SQL 서버 이름**

  Azure SQL Server 속성에서 제공되는 이름 및 리소스 그룹입니다.

- **Azure SQL 서버 리소스 그룹**

  Azure SQL Server 속성에서 제공되는 이름 및 리소스 그룹입니다.

- **Azure 스토리지 액세스 키**

  스토리지 계정 속성의 접근 허용 키 섹션에서 제공됩니다. 원하는 어떤 키든 사용할 수 있습니다(key1 또는 key2).

그러면 작업이 생성되고 작업 목록에 표시됩니다. **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화하면 작업이 생성된 직후에 기본 작업 설정을 수정할 수 있습니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.

클라이언트 기기 원격 진단

Windows 기반 및 Linux 기반 클라이언트 기기에서 다음 작업의 원격 실행에 대한 원격 진단을 사용할 수 있습니다.

- 추적 활성화 및 비활성화, 추적 로그 레벨 변경, 추적 로그 파일 다운로드
- 시스템 정보 및 애플리케이션 설정 다운로드
- 이벤트 로그 다운로드
- 애플리케이션에 대한 덤프 파일 생성
- 진단 시작 및 진단 리포트 다운로드
- 애플리케이션 시작, 중지 및 다시 시작

클라이언트 기기에서 다운로드한 이벤트 로그 및 진단 리포트를 사용하여 문제를 직접 해결할 수 있습니다. 또한, Kaspersky 기술 지원에 문의하면 기술 지원 전문가가 Kaspersky에서 추가로 분석할 수 있도록 클라이언트 기기에서 추적 로그 파일, 덤프 파일, 이벤트 로그, 진단 리포트를 다운로드하라고 요청할 수 있습니다.

원격 진단 창 열기

Windows 기반 및 Linux 기반 클라이언트 기기에서 원격 진단을 수행하려면 먼저 원격 진단 창을 열어야 합니다.

원격 진단 창을 열려면 다음 단계를 따릅니다.

1. 원격 진단 창을 열 기기를 선택하려면 다음 중 하나를 수행합니다.
   - 기기가 관리 그룹에 속한다면 메인 메뉴에서 **에셋(기기) → 관리 중인 기기**로 이동합니다.
   - 기기가 미할당 기기 그룹에 속한다면 메인 메뉴에서 **발견 및 배포 → 미할당 기기**로 이동합니다.
2. 필요한 기기의 이름을 누릅니다.
3. 기기 속성 창이 열리면 **고급** 탭을 선택합니다.
4. 창이 열리면 **원격 진단**을 클릭합니다.
   이렇게 하면 클라이언트 기기의 **원격 진단** 창이 열립니다. 중앙 관리 서버와 클라이언트 기기 간의 연결이 설정되지 않으면 오류 메시지가 표시됩니다.

또는 Linux 기반 클라이언트 기기에 대한 모든 진단 정보를 한 번에 가져와야 한다면 이 기기에서 Collect.sh 스크립트를 실행할 수 있습니다.

애플리케이션에 대한 추적 로그 활성화 및 비활성화

Xperf 추적 로그를 포함한 애플리케이션 추적을 활성화하고 비활성화할 수 있습니다.

추적 로그 활성화 및 비활성화

원격 기기에서 추적 로그를 활성화하거나 비활성화하려면 다음 단계를 따릅니다.

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창에서 **Kaspersky 애플리케이션** 탭을 선택합니다.
   애플리케이션 관리 섹션에서 기기에 설치된 Kaspersky 애플리케이션 목록이 표시됩니다.
3. 애플리케이션 목록에서 추적을 활성화 또는 비활성화할 애플리케이션을 선택합니다.
   원격 진단 옵션 목록이 열립니다.
4. 추적을 활성화하려면:
   a. 목록의 **추적 로그** 섹션에서 **추적 활성화**를 클릭합니다.
   b. 열리는 **추적 로그 레벨 수정** 창에서는 설정의 기본값을 유지하는 것이 좋습니다. 필요한 경우 기술 지원 전문가가 구성 프로세스를 안내합니다. 다음과 같은 설정을 사용할 수 있습니다:
      - **추적 로그 레벨**

        추적 로그 레벨은 추적 로그 파일에 포함되는 세부 정보의 양을 정의합니다.

- **순환식 저장 모드 추적 로그**

  추적 로그 파일 크기의 과도한 증가를 방지하기 위해 애플리케이션이 추적 로그 정보를 덮어씁니다. 추적 로그 정보를 저장하는 데 사용할 최대 파일 수와 각 파일의 최대 크기를 지정합니다. 최대 크기의 추적 로그 파일이 최대 수만큼 기록되면 새 추적 로그 파일을 기록할 수 있도록 가장 오래된 추적 로그 파일이 삭제됩니다.

  이 설정은 Kaspersky Endpoint Security에서만 사용할 수 있습니다.

c. **저장**을 클릭합니다.

선택한 애플리케이션에 대해 추적 로그가 활성화됩니다. 일부 경우에 추적 로그를 작동하려면 보안 제품 및 작업을 다시 시작해야 합니다.

Linux 기반 클라이언트 기기에서 네트워크 에이전트 구성 요소의 갱신자에 대한 추적은 네트워크 에이전트 설정으로 규제됩니다. 따라서, Linux를 실행하는 클라이언트 기기에서 이 구성 요소에 대해 **추적 활성화** 및 **추적 로그 레벨 수정** 옵션이 비활성화됩니다.

5. 선택한 애플리케이션에 대한 추적을 비활성화하려면 **추적 로그 중지** 버튼을 클릭합니다.

   선택한 애플리케이션에 대한 추적 로그가 비활성화됩니다.

Xperf 추적 로그 활성화

Kaspersky Endpoint Security의 경우에는 기술 지원 전문가가 시스템 성능 관련 정보를 확인하기 위해 Xperf 추적 로그를 활성화하도록 요청할 수 있습니다.

Xperf 추적을 활성화 및 구성하거나 비활성화하려면:

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창에서 **Kaspersky 애플리케이션** 탭을 선택합니다.

   애플리케이션 관리 섹션에서 기기에 설치된 Kaspersky 애플리케이션 목록이 표시됩니다.
3. 애플리케이션 목록에서 Kaspersky Endpoint Security for Windows를 선택합니다.

   Kaspersky Endpoint Security for Windows에 대한 원격 진단 옵션 목록이 표시됩니다.
4. 목록의 **Xperf 추적 로그** 섹션에서 **Xperf 추적 활성화**를 클릭합니다.

   Xperf 추적 로그가 이미 활성화된 경우 **Xperf 추적 로그 끄기** 버튼이 대신 표시됩니다. Kaspersky Endpoint Security for Windows에 대한 Xperf 추적을 비활성화하려면 이 버튼을 클릭하십시오.
5. **Xperf 추적 로그 레벨 변경** 창이 열리면 기술 지원 전문가의 요청에 따라 다음 중 하나를 선택합니다.

   a. 다음 추적 로그 레벨 중 하나를 선택합니다.

   - **Light 레벨**

     이 유형의 추적 로그 파일은 시스템과 관련된 최소한의 정보를 포함합니다.

     기본적으로 이 옵션은 선택되어 있습니다.

- **Deep 레벨**

  이 유형의 추적 로그 파일은 *Light* 유형의 추적 로그 파일에 비해 더 자세한 정보를 포함합니다. *Light* 유형의 추적 로그 파일만으로는 성능을 평가하기에 충분하지 않은 경우 기술 지원 전문가가 이 파일을 요청할 수 있습니다. *Deep* 추적 로그 파일에는 하드웨어, 운영 체제, 시작/완료한 프로세스와 애플리케이션 목록, 성능 평가에 사용되는 이벤트, Windows 시스템 평가 도구의 이벤트 관련 정보를 비롯하여 시스템에 대한 기술 정보가 포함됩니다.

b. 다음 Xperf 추적 로그 유형 중 하나를 선택합니다.

- **기본 유형**

  Kaspersky Endpoint 보안 제품 작동 중에 추적 로그 정보가 수신됩니다.
  기본적으로 이 옵션은 선택되어 있습니다.

- **재시작 시 유형**

  관리 중인 기기에서 운영 체제가 시작될 때 추적 로그 정보가 수신됩니다. 기기를 켜고 나서 Kaspersky Endpoint Security를 시작하기 전에 시스템 성능에 영향을 주는 문제가 발생하는 경우 이 추적 로그 유형이 효과적입니다.

추적 로그 파일 크기의 과도한 증가를 방지하기 위해 **회전 파일 크기(MB)** 옵션을 활성화하라는 요청을 받을 수도 있습니다. 그런 후에는 추적 로그 파일의 최대 크기를 지정합니다. 파일이 최대 크기가 되면 새로운 정보가 가장 오래된 추적 로그 정보를 덮어씁니다.

c. 회전 파일 크기를 정의합니다.

d. **저장**을 누릅니다.

Xperf 추적 로그가 활성화되고 구성됩니다.

6. Kaspersky Endpoint Security for Windows에 대한 Xperf 추적을 비활성화하려면 **Xperf 추적 로그** 섹션에서 **Xperf 추적 로그 끄기**를 클릭합니다.
   Xperf 추적 로그가 비활성화되었습니다.

애플리케이션 추적 로그 파일 다운로드

애플리케이션의 추적 로그 파일을 다운로드하려면 다음과 같이 하십시오:

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창에서 **Kaspersky 애플리케이션** 탭을 선택합니다.
   애플리케이션 관리 섹션에서 기기에 설치된 Kaspersky 애플리케이션 목록이 표시됩니다.
3. 애플리케이션 목록에서 추적 파일을 다운로드할 애플리케이션을 선택합니다.
4. **추적 로그** 섹션에서 **추적 파일** 버튼을 누릅니다.
   그러면 **기기 추적 로그** 창이 열리며, 여기에는 추적 로그 파일 목록이 표시됩니다.
5. 추적 파일 목록에서 다운로드할 파일을 선택합니다.

6. 다음 중 하나를 수행합니다:

   - **다운로드**를 클릭하여 선택한 파일을 다운로드합니다. 다운로드할 파일을 하나 또는 여러 개 선택할 수 있습니다.
   - 다음과 같이 선택한 파일의 일부를 다운로드합니다.

     a. **일부 다운로드**를 클릭합니다.

     동시에 여러 파일을 부분 다운로드할 수는 없습니다. 둘 이상의 추적 파일을 선택하면 **일부 다운로드** 버튼이 비활성화됩니다.

     b. 창이 열리면 필요에 따라 이름과 파일 부분을 지정하여 다운로드합니다.

     Linux 기반 기기에서는 파일 부분 이름을 편집할 수 없습니다.

     c. **다운로드**를 클릭합니다.

선택한 파일 또는 해당 부분이 지정한 위치로 다운로드됩니다.

추적 로그 파일 삭제

더 이상 필요하지 않은 추적 로그 파일은 삭제해도 됩니다.

추적 로그 파일을 삭제하려면 다음 단계를 따릅니다.

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창이 열리면 **이벤트 로그** 탭을 선택합니다.
3. **추적 파일** 섹션에서 삭제할 추적 파일에 따라 **Windows 업데이트 로그** 또는 **원격 설치 로그**를 클릭합니다.

   Windows 업데이트 로그 링크는 Windows 기반 클라이언트 기기에서만 사용할 수 있습니다.

   그러면 **기기 추적 로그** 창이 열리며, 여기에는 추적 로그 파일 목록이 표시됩니다.
4. 추적 파일 목록에서 삭제할 파일을 하나 또는 여러 개 선택합니다.
5. **제거** 버튼을 누릅니다.

선택한 추적 파일이 삭제됩니다.

애플리케이션 설정 다운로드

클라이언트 기기에서 애플리케이션 설정을 다운로드하려면 다음 단계를 따릅니다.

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창에서 **Kaspersky 애플리케이션** 탭을 선택합니다.
3. **애플리케이션 설정** 섹션에서 **다운로드** 버튼을 클릭하여 클라이언트 기기에 설치된 애플리케이션 설정 정보를 다운로드합니다.

정보가 포함된 ZIP 아카이브가 지정된 위치에 다운로드됩니다.

이벤트 로그 다운로드

원격 기기에서 이벤트 로그를 다운로드하려면:

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창의 **이벤트 로그** 탭에서 **모든 기기 로그**를 클릭합니다.
3. **모든 기기 로그** 창에서 관련 로그를 하나 또는 여러 개 선택합니다.
4. 다음 중 하나를 수행합니다:
   - **전체 파일 다운로드**를 눌러 선택한 로그를 다운로드합니다.
   - 다음과 같이 선택한 로그의 일부를 다운로드합니다.
     a. **일부 다운로드**을 누릅니다.
     동시에 여러 로그를 부분 다운로드할 수 없습니다. 둘 이상의 이벤트 로그를 선택하면 **일부 다운로드** 버튼이 비활성화됩니다.
     b. 창이 열리면 필요에 따라 이름과 로그 부분을 지정하여 다운로드합니다.
     Linux 기반 기기에서는 로그 부분 이름을 편집할 수 없습니다.
     c. **다운로드**를 클릭합니다.

선택한 이벤트 로그 또는 일부가 지정된 위치에 다운로드됩니다.

애플리케이션 시작, 중지, 다시 시작

클라이언트 기기에서 애플리케이션을 시작, 중지 및 다시 시작할 수 있습니다.

애플리케이션을 시작 또는 중지하거나 다시 시작하려면 다음과 같이 하십시오:

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창에서 **Kaspersky 애플리케이션** 탭을 선택합니다.
   애플리케이션 관리 섹션에서 기기에 설치된 Kaspersky 애플리케이션 목록이 표시됩니다.
3. 애플리케이션 목록에서 시작, 중지 또는 다시 시작할 애플리케이션을 선택합니다.
4. 다음 버튼 중 하나를 눌러 작업을 선택합니다.
   - **애플리케이션 중지**
     이 버튼은 애플리케이션이 현재 실행 중인 경우에만 사용할 수 있습니다.
   - **애플리케이션 다시 시작**
     이 버튼은 애플리케이션이 현재 실행 중인 경우에만 사용할 수 있습니다.

- **애플리케이션 시작**

  이 버튼은 애플리케이션이 현재 실행되고 있지 않은 경우에만 사용할 수 있습니다.

선택한 작업에 따라 클라이언트 기기에서 필요한 애플리케이션이 시작, 중지 또는 다시 시작됩니다.

네트워크 에이전트를 다시 시작하면 기기와 중앙 관리 서버의 현재 연결이 끊어진다는 메시지가 표시됩니다.

Kaspersky Security Center 네트워크 에이전트의 원격 진단 실행 및 결과 다운로드

원격 기기에서 Kaspersky Security Center 네트워크 에이전트 진단을 시작하고 결과를 다운로드하려면:

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창에서 **Kaspersky 애플리케이션** 탭을 선택합니다.

   애플리케이션 관리 섹션에서 기기에 설치된 Kaspersky 애플리케이션 목록이 표시됩니다.
3. 애플리케이션 목록에서 **Kaspersky Security Center 네트워크 에이전트**를 선택합니다.

   원격 진단 옵션 목록이 열립니다.
4. **진단 리포트** 섹션에서 **진단 실행** 버튼을 클릭합니다.

   이렇게 하면 원격 진단 프로세스가 시작되고 진단 보고서가 생성됩니다. 진단 프로세스가 완료되면 **진단 리포트 다운로드** 버튼을 사용할 수 있습니다.
5. 리포트를 다운로드하려면 **진단 리포트 다운로드** 버튼을 클릭합니다.

리포트가 지정된 위치에 다운로드됩니다.

클라이언트 기기에서 애플리케이션 실행

Kaspersky 기술 지원 전문가가 요청할 경우 클라이언트 기기에서 애플리케이션을 실행해야 할 수 있습니다. 해당 기기에 애플리케이션을 직접 설치하지 않아도 됩니다.

클라이언트 기기에서 애플리케이션을 실행하려면 다음 단계를 따릅니다.

1. 클라이언트 기기에 원격 진단 창을 엽니다.
2. 원격 진단 창에서 **원격 애플리케이션 실행** 탭을 선택합니다.
3. **애플리케이션 파일** 섹션에서 **찾기** 버튼을 클릭하여 클라이언트 기기에서 실행하려는 애플리케이션이 포함된 ZIP 아카이브를 선택합니다.

   > ZIP 아카이브에는 유틸리티 폴더가 포함되어야 합니다. 이 폴더에는 원격 기기에서 실행할 실행 파일이 포함되어 있습니다.

   필요하다면 실행 파일 이름과 명령줄 인수를 지정할 수 있습니다. 이렇게 하려면 **원격 기기에서 실행할 압축파일 내의 실행 파일**과 **명령줄 인수** 필드를 채우십시오.

4. **업로드 및 실행** 버튼을 클릭하여 클라이언트 기기에서 지정된 애플리케이션을 실행합니다.

5. Kaspersky 지원 전문가의 지침을 따릅니다.

애플리케이션에 대한 덤프 파일 생성

애플리케이션 덤프 파일을 사용하면 특정 시점에 클라이언트 기기에서 실행 중인 애플리케이션의 매개변수를 볼 수 있습니다. 이 파일에는 애플리케이션에 대해 로드된 모듈 정보도 포함되어 있습니다.

Linux 기반 기기의 덤프 파일 수집은 지원하지 않습니다.

원격 진단으로 덤프 파일을 수집하려면 kldumper 유틸리티가 사용됩니다. 이 유틸리티는 기술 지원 전문가의 요청에 따라 Kaspersky 애플리케이션의 프로세스 덤프 파일을 수집하도록 설계되었습니다. kldumper 유틸리티 사용을 위한 요구 사항에 대한 상세 정보는 Kaspersky Security Center 기술 자료를 참조하십시오.

애플리케이션에 대한 덤프 파일을 생성하려면:

1. 클라이언트 기기에 원격 진단 창을 엽니다.

2. 원격 진단 창에서 **원격 애플리케이션 실행** 탭을 선택합니다.

3. **프로세스 덤프 파일 생성** 섹션에서 덤프 파일을 생성할 애플리케이션의 실행 파일을 지정합니다.

4. **덤프 파일 다운로드** 버튼을 클릭합니다.

   지정한 애플리케이션의 덤프 파일이 포함된 압축 파일이 다운로드됩니다.

   지정한 애플리케이션을 클라이언트 기기에서 실행하고 있지 않다면 다운로드한 압축 파일에 포함된 "결과" 폴더는 비어 있게 됩니다.

   지정한 애플리케이션은 실행 중이지만 다운로드에 오류가 발생하여 실패하거나 다운로드한 압축 파일에 포함된 "결과" 폴더가 비어 있는 경우 Kaspersky Security Center 기술 자료를 참조하십시오.

Linux 기반 클라이언트 기기에서 원격 진단 실행

Kaspersky Security Center를 사용하면 클라이언트 기기에서 기본 진단 정보를 다운로드할 수 있습니다. 또는 Kaspersky의collect.sh 스크립트를 사용하여 Linux 기반 기기에 대한 진단 정보를 얻을 수 있습니다. 이 스크립트는 진단이 필요한 Linux 기반 클라이언트 기기에서 실행된 후, 진단 정보, 이 기기에 관한 시스템 정보, 애플리케이션 추적 파일, 기기 로그, 긴급 강제 종료된 애플리케이션의 덤프 파일이 포함된 파일을 생성합니다.

Linux 기반 클라이언트 기기에 대한 모든 진단 정보를 한 번에 얻으려면 Collect.sh 스크립트를 사용할 것을 권장합니다. Kaspersky Security Center를 통해 진단 정보를 원격 다운로드한다면 원격 진단 인터페이스의 모든 섹션을 거쳐야 합니다. 또한 Linux 기반 기기에 대한 진단 정보를 완전히 얻지 못할 수도 있습니다.

진단 정보와 함께 생성된 파일을 Kaspersky 기술 지원팀에 보내야 한다면 파일을 보내기 전에 모든 기밀 정보를 삭제합니다.

Collect.sh 스크립트를 사용하여 Linux 기반 클라이언트 기기에서 진단 정보를 다운로드하려면:

1. Collect.sh 스크립트를 다운로드합니다(collect.tar.gz 압축 파일).
2. 진단할 Linux 기반 클라이언트 기기에 다운로드한 압축 파일을 복사합니다.
3. 다음 명령을 실행하여 Collect.tar.gz 압축 파일의 압축을 풉니다.

   ```
   # tar -xzf collect.tar.gz
   ```

4. 다음 명령을 실행하여 스크립트 실행 권한을 지정합니다.

   ```
   # chmod +x collect.sh
   ```

5. 관리자 권한이 있는 계정을 사용하여 Collect.sh 스크립트를 실행합니다.

   ```
   # ./collect.sh
   ```

진단 정보가 포함된 파일이 생성되어 /tmp/$HOST_NAME-collect.tar.gz 폴더에 저장됩니다.

격리 및 백업 저장소에서 파일 다운로드 및 삭제

이 섹션에서는 Kaspersky Security Center 웹 콘솔의 격리 및 백업에서 파일을 다운로드하고 삭제하는 방법에 대한 정보를 제공합니다.

격리 및 백업 저장소에서 파일 다운로드

기기 설정에서 **중앙 관리 서버와 계속 연결 유지** 옵션이 활성화되어 있거나 연결 게이트웨이가 사용 중일 때만 격리 저장소 및 백업 저장소에서 파일을 다운로드할 수 있습니다. 그렇지 않으면 다운로드할 수 없습니다.

격리 또는 백업 저장소에서 하드 드라이브로 파일의 복사본을 저장하는 방법:

1. 다음 중 하나를 수행합니다:
   - 격리에서 파일 복사본을 저장하려면 메인 메뉴에서 **동작** → **저장소** → **격리**로 이동합니다.
   - 백업에서 파일 사본을 저장하려면 메인 메뉴에서 **동작** → **저장소**→ **백업**로 이동합니다.
2. 창이 열리면 다운로드하려는 파일을 선택하고 **다운로드**를 누릅니다.

   다운로드가 시작됩니다. 클라이언트 기기의 격리에 보관된 파일의 사본은 지정된 폴더에 저장됩니다.

Kaspersky Security Center 웹 콘솔 인터페이스의 언어 변경

Kaspersky Security Center 웹 콘솔 인터페이스의 언어를 선택할 수 있습니다.

인터페이스 언어를 변경하려면:

1. 메인 메뉴에서 **설정** → **언어** 섹션으로 이동합니다.
2. 지원되는 현지화 언어 중 하나를 선택합니다.

API 참조 가이드

이 Kaspersky Security Center OpenAPI 참조 가이드는 다음 작업을 지원하도록 설계되었습니다.

- 자동화 및 사용자 지정. 관리 콘솔을 사용하여 수동 처리를 원치 않는 작업들을 자동화할 수 있습니다. 관리 콘솔에서 아직 지원되지 않는 사용자 지정 시나리오를 구현할 수도 있습니다. 예를 들어 관리자는 Kaspersky Security Center OpenAPI를 사용하여 관리 그룹의 구조를 개발하고 해당 구조를 최신 상태로 유지하는 스크립트를 생성 및 실행할 수 있습니다.

- 사용자 지정 개발. 예를 들어 제한된 작업들을 허용하는 클라이언트용 대체 MMC 기반 관리 콘솔을 개발할 수 있습니다.

OpenAPI 참조 가이드에서 화면 오른쪽의 검색 필드를 사용하여 필요한 정보를 찾을 수 있습니다.

OPENAPI 참조 가이드

스크립트 샘플

OpenAPI 참조 가이드에는 아래 표에 나열된 Python 스크립트 샘플이 포함되어 있습니다. 이 샘플은 OpenAPI 메서드를 호출하고 네트워크 보호를 위한 다양한 작업("기본/보조" 계층 생성, Kaspersky Security Center에서 작업 실행, 배포 지점 할당 등)을 자동 수행하는 방법을 보여줍니다. 이 샘플을 있는 그대로 실행하거나 샘플을 기반으로 고유한 스크립트를 작성할 수 있습니다.

OpenAPI 메서드를 호출하고 스크립트를 실행하려면:

1. KlAkOAPI.tar.gz 아카이브를 다운로드합니다. 이 아카이브에는 KlAkOAPI 패키지 및 샘플이 포함되어 있습니다(아카이브 또는 OpenAPI 참조 가이드에서 복사할 수 있습니다). KlAkOAPI.tar.gz 압축파일은 Kaspersky Security Center 설치 폴더에도 있습니다.

2. 중앙 관리 서버가 설치된 기기의 KlAkOAPI.tar.gz 아카이브에서 KlAkOAPI 패키지를 설치합니다.

   OpenAPI 메소드를 호출하고, 중앙 관리 서버 및 KlAkOAPI 패키지가 설치된 기기에서만 샘플 및 자체 스크립트를 실행할 수 있습니다.

사용자 시나리오와 Kaspersky Security Center OpenAPI 메소드 샘플의 일치

샘플	샘플의 목적	시나리오
KlAkParams 로그	`KlAkParams` 데이터 구조를 사용하여 데이터를 추출하고 처리할 수 있습니다. 샘플은 이 데이터 구조로 작업하는 방법을 보여줍니다. 샘플 출력은 다양한 방식으로 나타날 수 있습니다. HTTP 메서드를 보내거나 코드에서 사용하기 위해 데이터를 가져올 수 있습니다.	모니터링 및 보고
"기본/보조" 계층 생성 및 삭제	보조 중앙 관리 서버를 추가하고 "기본/보조" 계층을 구축할 수 있습니다. 또는 계층에서 보조 중앙 관리 서버의 연결을 끊을 수 있습니다.	• 중앙 관리 서버 계층 만들기 및 보조 중앙 관리 서버 추가 • 중앙 관리 서버의 계층 구조 삭제
Active Directory 단위를 기반으로 하는 구조로 그룹 계층 생성	Active Directory 단위를 검색하고 검색된 기기 그룹의 계층 구조를 형성할 수 있습니다.	관리 그룹 생성
캐시된 Active Directory 단위를 기반으로 하는 구조로 그룹 계층 생성	이전에 검색한 Active Directory 단위를 기반으로 관리 중인 기기 그룹의 계층 구조를 형성할 수 있습니다. 마지막 폴링 후 Active Directory에 새 기기가 나타나면 저장된 폴링 결과에 없기 때문에 그룹에 추가되지 않습니다.	관리 그룹 생성
지정된 기기에 대한 연결 게이트웨이를 통해 네트워크 목록 파일 다운로드	연결 게이트웨이를 사용하여 필요한 기기의 네트워크 에이전트에 연결한 다음 네트워크 목록이 있는 파일을 기기에 다운로드합니다.	배포 지점 및 연결 게이트웨이 조정

샘플	샘플의 목적	시나리오
기본 중앙 관리 서버 저장소에 저장된 라이센스 키를 보조 중앙 관리 서버에 설치	기본 중앙 관리 서버에 연결하고 필요한 라이센스 키를 다운로드한 후, 이 키를 계층에 포함된 보조 중앙 관리 서버 전체에 전송할 수 있습니다.	관리 애플리케이션 라이센싱
유효 사용자 권한 보고서 작성	다른 리포트를 만들 수 있습니다. 예를 들어, 이 샘플을 사용하여 유효 사용자 권한 보고서를 생성할 수 있습니다. 이 보고서는 사용자의 그룹 및 역할에 따라 사용자가 갖는 권한을 설명합니다. 보고서를 HTML, PDF 또는 Excel 형식으로 다운로드할 수 있습니다.	리포트 만들기 및 보기
기기에 대한 작업 시작	연결 게이트웨이를 사용하여 필요한 기기의 네트워크 에이전트에 연결한 다음 필요한 작업을 실행할 수 있습니다.	수동으로 작업 시작
Active Directory 사이트 및 서비스를 기반으로 IP 서브넷 생성	사용하는 Active Directory 단위를 기반으로 IP 서브넷을 생성할 수 있습니다. 샘플은 지정된 IP 범위의 폴링을 시작하고 검색된 서브넷을 삭제하여 새 서브넷과의 충돌을 방지합니다. 따라서 서브넷을 유지하는 것이 중요한 네트워크에서는 이 샘플을 실행하지 마십시오. 폴링 후 샘플은 Active Directory를 참조하고 그 안의 모든 기기를 검사하고 IP 서브넷을 만듭니다. 이를 위해 샘플은 모든 기기의 마스크와 IP 주소를 사용합니다.	네트워크 보호 구성
그룹의 기기에 대한 배포 지점 등록	관리 중인 기기를 배포 지점(이전에는 업데이트 에이전트라고 함)으로 할당할 수 있습니다.	Kaspersky 데이터베이스 및 애플리케이션 업데이트
모든 그룹 열거	관리 그룹으로 다양한 작업을 수행할 수 있습니다. 샘플은 다음을 수행하는 방법을 보여줍니다. • "관리 중인 기기" 루트 그룹의 식별자 가져오기 • 그룹 계층 구조를 통해 이동 • 이름 및 중첩과 함께 그룹의 전체 확장 계층 검색	중앙 관리 서버 구성
작업 열거, 쿼리 작업 통계, 작업 실행	다음 정보를 확인할 수 있습니다. • 작업 진행 내역 • 현재 작업 상태 • 다른 상태의 작업 수 작업을 실행할 수도 있습니다. 기본적으로 샘플은 통계를 출력한 후 작업을 실행합니다.	작업 실행 감시
작업 생성 및 실행	작업을 생성할 수 있습니다. 샘플에서 다음 작업 파라미터를 지정합니다. • 유형 • 실행 방법 • 이름 • 작업이 사용될 기기 그룹 기본적으로 샘플은 "메시지 표시" 유형으로 작업을 만듭니다. 중앙 관리 서버의 관리 중인 모든 기기에 대해 이 작업을 실행할 수 있습니다. 필요 시, 작업 파라미터를 직접 지정할 수 있습니다.	작업 만들기
라이센스 키 열거	중앙 관리 서버의 관리 중인 기기에 설치된 Kaspersky 애플리케이션의 모든 활성 라이센스 키 목록을 얻을 수 있습니다. 목록에는 이름, 유형, 만료 날짜 등 모든 라이센스 키에 대한 상세 데이터가 포함됩니다.	사용 중인 라이센스 키 정보 보기
내부 사용자 생성 및 찾기	추가 작업을 위해 계정을 만들 수 있습니다.	중앙 관리 서버를 시작할 계정 선택
사용자 지정 카테고리 생성	필요한 파라미터로 애플리케이션 카테고리를 만들 수 있습니다.	수동으로 추가된 컨텐츠가 있는 애플리케이션 카테고리 만들기
SrvView를 사용하여 사용자 열거	SrvView 클래스를 사용해 Kaspersky Security Center 중앙 관리 서버에서 상세 정보를 요청할 수 있습니다. 예를 들어 이 샘플을 사용하여 사용자 목록을 가져올 수 있습니다.	사용자 계정 관리

OpenAPI를 통해 Kaspersky Security Center와 상호 작용하는 애플리케이션

일부 애플리케이션은 OpenAPI를 통해 Kaspersky Security Center와 상호 작용합니다. 이 애플리케이션에는 Kaspersky Anti Targeted Attack Platform 또는 Kaspersky Security for Virtualization 등이 포함됩니다. OpenAPI를 기반으로 개발된 사용자 지정 클라이언트 애플리케이션일 수도 있습니다.

OpenAPI를 통해 Kaspersky Security Center와 상호 작용하는 애플리케이션은 중앙 관리 서버에 연결됩니다. 중앙 관리 서버에 연결하기 위한 IP 주소 허용 목록을 구성한 경우 Kaspersky Security Center OpenAPI를 사용하는 애플리케이션이 설치된 기기의 IP 주소를 추가합니다. 사용하는 애플리케이션이 OpenAPI에서 작동하는지 확인하려면 이 애플리케이션의 도움말을 참조하십시오.

서비스 공급업체를 위한 모범 사례

이 섹션에서는 Kaspersky Security Center를 구성하고 사용하는 방법에 대한 정보를 제공합니다.

이 섹션에서는 애플리케이션을 배포, 구성 및 사용하는 방법에 대한 권장 사항을 제공하며 애플리케이션 작동 시에 일반적으로 발생하는 문제를 해결하는 방법을 설명합니다.

Kaspersky Security Center 배포 계획

조직 네트워크에서 Kaspersky Security Center 구성 요소의 배포를 계획할 때는 프로젝트의 규모와 범위를 고려해야 합니다. 구체적으로 고려해야 하는 요인은 다음과 같습니다:

- 총 기기 개수
- MSP 클라이언트의 수

중앙 관리 서버 한 대는 기기를 최대 10만 대를 지원할 수 있습니다. 조직 네트워크의 총 기기 개수가 10만 대보다 많으면 서비스 공급업체 측에 다수의 중앙 관리 서버를 배포한 다음 중앙에서 편리하게 관리할 수 있도록 계층 구조로 결합해야 합니다.

하나의 중앙 관리 서버에 최대 500개의 가상 서버를 생성할 수 있으므로 500개의 MSP 클라이언트마다 개별적인 중앙 관리 서버가 필요합니다.

배포 계획 단계에서는 중앙 관리 서버에 특수 인증서 X.509를 할당할지를 고려해야 합니다. 다음과 같은 경우 중앙 관리 서버에 X.509 인증서를 할당하면 유용할 수 있습니다. 아래 목록에 해당하는 경우 중 일부가 제시되어 있습니다:

- SSL 종료 프록시를 통해 SSL(Secure Socket Layer) 트래픽 검사
- 인증서 필드의 필수 값 지정
- 인증서에 필요한 암호화 강도 제공

중앙 관리 서버에 대한 인터넷 접속 제공

클라이언트 네트워크의 기기가 인터넷을 통해 중앙 관리 서버에 접근할 수 있도록 하려면 다음 중앙 관리 서버 포트를 사용할 수 있게 설정해야 합니다:

- 13000 TCP - 클라이언트 네트워크에 배포된 네트워크 에이전트 연결용 중앙 관리 서버 TLS 포트
- 8061 TCP - 관리 콘솔 도구를 사용하여 독립 실행형 패키지를 게시하기 위한 HTTPS 포트
- 8060 TCP - 관리 콘솔 도구를 사용하여 독립 실행형 패키지를 게시하기 위한 HTTP 포트
- 13292 TCP - 관리해야 하는 모바일 기기가 있는 경우에만 필요한 TLS 포트

Kaspersky Security Center 웹 콘솔을 통해 클라이언트에 기본적인 네트워크 관리 옵션을 제공해야 한다면, 다음 Kaspersky Security Center 웹 콘솔 TCP 8080 포트(HTTPS 포트)도 열어야 합니다:

Kaspersky Security Center 표준 구성

하나 이상의 중앙 관리 서버가 MSP의 서버에 배포됩니다. 중앙 관리 서버 수는 사용 가능한 하드웨어, MSP 클라이언트 전체 수 또는 관리 중인 기기의 전체 수를 기준으로 선택할 수 있습니다.

중앙 관리 서버 한 대는 기기를 최대 100,000대까지 지원합니다. 조만간 관리 중인 기기의 수가 늘어날 가능성을 고려해야 합니다: 단일 중앙 관리 서버에 약간 더 적은 수의 기기를 연결하면 유용할 수 있습니다.

하나의 중앙 관리 서버에 최대 500개의 가상 서버를 생성할 수 있으므로 500개의 MSP 클라이언트마다 개별적인 중앙 관리 서버가 필요합니다.

여러 서버를 사용하는 경우에는 서버를 계층 구조로 결합하는 것이 좋습니다. 중앙 관리 서버 계층 구조를 사용하면 정책 및 작업 중복을 방지할 수 있으며 전체 관리 중인 기기 집합을 단일 중앙 관리 서버에서 관리되는 것처럼 처리하여 기기 검색, 기기 조회 작성, 리포트 작성 등을 수행할 수 있습니다.

각 MSP 클라이언트에 해당하는 가상 서버마다 배포 지점을 하나 이상 할당해야 합니다. MSP 클라이언트와 중앙 관리 서버가 인터넷을 통해 연결 시, 배포 지점에 대해 *배포 지점의 저장소로 업데이트 다운로드* 작업을 만들면 유용할 수 있습니다. 그러면 배포 지점은 중앙 관리 서버가 아닌 Kaspersky 서버에서 업데이트를 직접 다운로드합니다.

MSP 클라이언트 네트워크의 일부 기기가 인터넷에 직접 연결할 수 없을 시, 배포 지점을 연결 게이트웨이 모드로 전환해야 합니다. 이 경우 MSP 클라이언트 네트워크에 있는 기기의 네트워크 에이전트는 추가 동기화를 위해 중앙 관리 서버에 연결되지만 직접 연결되지는 않으며 게이트웨이를 통해 연결됩니다.

중앙 관리 서버는 MSP 클라이언트 네트워크를 검색하지 못할 가능성이 높으므로, 배포 지점이 이 기능을 수행하도록 하는 것이 좋습니다.

중앙 관리 서버는 NAT가 적용된 MSP 클라이언트 네트워크에 배치된 관리 중인 기기의 15000 UDP 포트로 알림을 전송할 수 없습니다. 이 문제를 해결하려는 경우 배포 지점 역할을 하고 연결 게이트웨이 모드에서 실행 중인 기기의 속성에서 중앙 관리 서버에 대한 지속적인 연결 모드(**중앙 관리 서버와 계속 연결 유지** 확인란)를 작동하면 유용할 수 있습니다. 전체 배포 지점 개수가 300개 미만일 경우 이 지속 연결 모드를 사용할 수 있습니다.

배포 지점 정보

네트워크 에이전트가 설치된 기기를 배포 지점로 사용할 수 있습니다. 이 모드에서 네트워크 에이전트는 다음 기능을 수행할 수 있습니다:

- 클라이언트 기기로 다음을 포함하는 파일을 전송합니다.
  - Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트

    중앙 관리 서버나 Kaspersky 서버에서 업데이트를 가져올 수 있습니다. 후자의 경우 *배포 지점의 저장소로 업데이트 다운로드* 작업이 배포 지점 역할을 수행하는 기기에 만들어져야 합니다.
  - 타사 소프트웨어 업데이트
  - 설치 패키지
  - 중앙 관리 서버를 WSUS 서버로 사용 시 Windows 업데이트

- 다른 기기에 소프트웨어를 설치하고 네트워크 에이전트 초기 배포를 수행합니다.
- 네트워크를 검색해서 새로운 기기를 탐지하고 기존 기기에 대한 정보를 업데이트합니다. 배포 지점은 중앙 관리 서버의 기기 발견 방법을 똑같이 적용할 수 있습니다.

조직 네트워크에서 배포 지점을 배포하는 목적은 다음과 같습니다:

- 업데이트 경로로 작동하는 중앙 관리 서버의 부하 감소.
- 인터넷 트래픽 최적화. 이때는 MSP 클라이언트 네트워크의 각 기기가 업데이트를 받기 위해 Kaspersky 서버 또는 중앙 관리 서버에 접근하지 않아도 됩니다.
- 중앙 관리 서버에 MSP 클라이언트 네트워크의 NAT(중앙 관리 서버 기준) 외부 기기에 대한 접근 권한을 제공. 이를 통해 중앙 관리 서버는 다음 작업을 수행할 수 있습니다:
  - IPv4 또는 IPv6 네트워크의 UDP를 통해 기기로 알림 전송
  - IPv4 또는 IPv6 네트워크 검색
  - 초기 배포 수행
  - 푸시 서버로 작동

배포 지점은 관리 그룹용으로 할당됩니다. 이 경우 배포 지점의 범위에는 관리 그룹 및 모든 하위 그룹 내의 모든 기기가 포함됩니다. 그러나 배포 지점 역할을 하는 기기가 할당된 관리 그룹에 포함되어 있지 않을 수도 있습니다.

배포 지점을 연결 게이트웨이로 만들 수 있습니다. 이 경우에는 배포 지점 범위의 기기가 직접 중앙 관리 서버에 연결되는 것이 아니라 이 게이트웨이를 통해 연결됩니다. 네트워크 에이전트가 포함된 기기와 중앙 관리 서버 간의 직접 연결을 설정할 수 없는 경우 이 모드를 사용하는 것이 좋습니다.

배포 지점 기능을 하는 기기는 무단으로 접근할 수 없도록 보호(물리적 보호 포함)해야 합니다.

중앙 관리 서버 계층 구조

한 MSP에서 다수의 중앙 관리 서버를 실행할 수 있습니다. 개별 중앙 관리 서버를 여러 개 관리하려면 불편할 수도 있으므로 계층 구조를 적용할 수 있습니다. 두 중앙 관리 서버에 대한 "기본/보조" 구성에서는 다음 옵션을 제공합니다.

- 보조 중앙 관리 서버는 기본 중앙 관리 서버에서 정책과 작업을 상속하므로 설정이 중복되지 않습니다.
- 기본 중앙 관리 서버의 기기 조회 시 보조 중앙 관리 서버의 기기가 포함될 수 있습니다.
- 기본 중앙 관리 서버의 리포트에는 상세 정보를 비롯한 보조 중앙 관리 서버의 데이터가 포함될 수 있습니다.

기본 중앙 관리 서버는 위에 나열된 옵션 범위 내에서 가상이 아닌 보조 중앙 관리 서버에서만 데이터를 수신합니다. 이 제한은 기본 중앙 관리 서버와 데이터베이스를 공유하는 가상 중앙 관리 서버에는 적용되지 않습니다.

가상 중앙 관리 서버

실제 중앙 관리 서버를 기준으로 하여 보조 중앙 관리 서버와 비슷한 가상 중앙 관리 서버를 여러 개 만들 수 있습니다. 가상 중앙 관리 서버 모델은 ACL(접근 제어 목록)을 기반으로 하는 임의 접근 모델에 비해 기능성이 뛰어나며 보다 광범위한 격리 수준을 제공합니다. 각 가상 중앙 관리 서버는 정책 및 작업을 포함하는 할당된 기기에 대한 관리 그룹의 전용 구조 외에 자체 미할당 기기 그룹, 자체 리포트 세트, 선택한 기기와 이벤트, 설치 패키지, 이동 규칙 등도 제공합니다. MSP 클라이언트를 서로 최대한 격리하려면 사용할 기능으로 가상 중앙 관리 서버를 선택하는 것이 좋습니다. 또한 각 MSP 클라이언트용으로 가상 중앙 관리 서버를 만들면 Kaspersky Security Center 웹 콘솔을 통해 기본적인 네트워크 관리 옵션을 클라이언트에 제공할 수 있습니다.

가상 중앙 관리 서버는 보조 중앙 관리 서버와 매우 비슷하지만 다음과 같은 점이 다릅니다:

- 가상 중앙 관리 서버에는 대부분의 글로벌 설정과 자체 TCP 포트가 없습니다.
- 가상 중앙 관리 서버에는 보조 중앙 관리 서버가 없습니다.
- 가상 중앙 관리 서버에는 다른 가상 중앙 관리 서버가 없습니다.
- 실제 중앙 관리 서버는 모든 가상 중앙 관리 서버의 기기, 그룹, 이벤트 및 관리 중인 기기에 있는 개체(격리의 항목, 자산 관리(소프트웨어) 등)를 확인합니다.
- 가상 중앙 관리 서버는 배포 지점이 연결된 네트워크만 검사할 수 있습니다.

Kaspersky Endpoint Security for Android를 사용하여 모바일 기기 관리

Kaspersky Endpoint Security for Android™가 설치된 모바일 기기(이하 KES 기기로 지칭함)는 중앙 관리 서버를 통해 관리됩니다. Kaspersky Security Center는 KES 기기 관리를 위해 다음 기능을 지원합니다:

- 모바일 기기를 클라이언트 기기로 취급:
  - 관리 그룹 멤버십
  - 상태, 이벤트 및 리포트 보기와 같은 모니터링
  - 로컬 설정 수정 및 Kaspersky Endpoint Security for Android용 정책 할당
- 중앙 집중식 모드로 명령 전송
- 원격으로 모바일 앱 패키지 설치

중앙 관리 서버는 TLS, TCP 포트 13292를 통해 KES 기기를 관리합니다.

배포 및 초기 설정

Kaspersky Security Center는 배포 방식 애플리케이션입니다. Kaspersky Security Center는 다음과 같은 애플리케이션을 포함합니다:

- 중앙 관리 서버 – 조직의 기기를 관리하고 DBMS에 데이터를 저장하는 데 사용되는 핵심 구성 요소입니다.
- 관리 콘솔 – 관리자를 위한 기본적인 도구입니다. 관리 콘솔은 중앙 관리 서버와 함께 제공되지만 관리자가 실행하는 기기 한 대나 여러 대에 개별적으로 설치할 수도 있습니다.
- Kaspersky Security Center 웹 콘솔 - 기본적인 작업을 수행할 수 있는 중앙 관리 서버용 웹 인터페이스입니다. 하드웨어 및 소프트웨어 요구 사항을 충족하는 모든 기기에 이 구성 요소를 설치할 수 있습니다.
- 네트워크 에이전트 — 기기에 설치된 보안 제품을 관리하고 해당 기기에 대한 정보를 받습니다. 네트워크 에이전트는 조직의 기기에 설치됩니다.

다음과 같은 방식으로 조직 네트워크에서 Kaspersky Security Center 배포를 수행합니다:

- 중앙 관리 서버 설치
- Kaspersky Security Center 웹 콘솔 설치
- 관리자의 기기에 관리 콘솔 설치
- 기업 기기에 네트워크 에이전트 및 보안 제품 설치

중앙 관리 서버 설치 권장 사항

이 섹션에서는 중앙 관리 서버를 설치하는 권장 방법을 설명합니다. 또한 클라이언트 기기에서 네트워크 에이전트를 배포하기 위해 중앙 관리 서버 기기에서 공유 폴더를 사용하는 경우에 대해서도 설명합니다.

Failover 클러스터에 중앙 관리 서버 서비스용 계정 생성

기본적으로 설치 관리자는 중앙 관리 서버 서비스용으로 권한이 없는 계정을 자동으로 만듭니다. 이 동작은 일반 기기에 중앙 관리 서버를 설치할 때 활용하면 가장 편리합니다.

그러나 Failover 클러스터에 중앙 관리 서버를 설치하려면 다른 방법을 사용해야 합니다:

1. 중앙 관리 서버 서비스용으로 권한이 없는 도메인 계정을 만든 다음 KLAdmins 도메인 보안 그룹의 구성원으로 지정.
2. 중앙 관리 서버 설치 프로그램에 이 서비스를 위해 생성한 도메인 계정을 지정합니다.

DBMS 선택

중앙 관리 서버에서 사용할 데이터베이스 관리 시스템(DBMS)을 선택할 때는 중앙 관리 서버에서 관리하는 기기 개수를 고려해야 합니다.

아래 표에는 유효한 DBMS 옵션과 해당 옵션 사용 시의 권장 사항 및 제한 사항이 나와 있습니다.

DBMS에 대한 권장 사항 및 제한 사항

DBMS	권장 사항 및 제한 사항
SQL Server Express Edition 2016 이상	10,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 데이터베이스 오버플로 방지를 위해 이벤트 저장소의 최대 이벤트 수를 제한할 수 있습니다. 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오. 중앙 관리 서버와 다른 애플리케이션이 SQL Server Express Edition DBMS를 동시에 사용하도록 해서는 안 됩니다. **Windows 업데이트 동기화 수행** 작업에는 Microsoft SQL Express 데이터베이스를 지원하지 않습니다.
Express 2016 이상 이외의 로컬 SQL Server Edition	제한 없음
Express 2016 이상 이외의 원격 SQL Server Edition	두 기기가 같은 Windows® 도메인에 있는 경우에만 유효합니다. 기기의 도메인이 다른 경우에는 도메인 간에 양방향 신뢰 관계를 설정해야 합니다
로컬 또는 원격 MySQL 5.5, 5.6, 5.7 (MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5 버전은 더 이상 지원하지 않습니다.)	10,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.
로컬 또는 원격 MySQL 8.0.20 이상	50,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.
로컬 또는 원격 MariaDB(지원되는 버전 참조)	20,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.
PostgreSQL, Postgres Pro(지원하는 버전 참조)	50,000대 미만의 기기에 대해 단일 중앙 관리 서버를 실행하려면 이 DBMS 중 하나를 사용하십시오. 소프트웨어 인벤토리 작업을 비활성화하고 시작된 애플리케이션의 중앙 관리 서버 알림을 비활성화하는 것이 좋습니다(Kaspersky Endpoint Security 정책 설정에서). 자세한 내용은 데이터베이스 공간 계산 항목을 참조하십시오.

PostgreSQL, MariaDB, MySQL DBMS를 사용한다면 **이벤트** 탭의 선택한 클라이언트 기기에 대한 이벤트 목록이 완전하지 않을 수 있습니다. 이 문제는 DBMS에 저장된 이벤트가 매우 많을 때 발생합니다. 다음 작업 중 하나로 표시할 이벤트 수를 늘릴 수 있습니다:

- 불필요한 이벤트 제거.
- 불필요한 이벤트의 저장 기간 단축.

기기의 중앙 관리 서버에 기록된 이벤트의 전체 목록을 보려면 리포트를 사용하십시오.

SQL Server 2019를 DBMS로 사용하고 CU12 이상의 누적 패치가 없는 경우 Kaspersky Security Center를 설치한 후에 다음을 수행해야 합니다.

1. SQL Management Studio를 사용하여 SQL Server에 연결합니다.
2. 다음 명령을 실행하십시오(데이터베이스에 다른 이름을 선택한 경우 KAV 대신 해당 이름을 사용하십시오).

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. SQL Server 2019 서비스를 다시 시작합니다.

그렇지 않으면 SQL Server 2019 사용 시 "이 쿼리를 실행하기 위한 리소스 풀 'internal'에 시스템 메모리가 부족합니다."와 같은 오류가 발생할 수 있습니다.

중앙 관리 서버 주소 지정

중앙 관리 서버를 설치할 때는 중앙 관리 서버의 외부 주소를 지정할 수 있습니다. 이 주소는 네트워크 에이전트 설치 패키지를 만들 때 기본 주소로 사용됩니다. 그리고 나면 관리 콘솔 도구를 사용하여 중앙 관리 서버 호스트의 주소를 변경할 수 있습니다. 이미 만들어진 네트워크 에이전트 설치 패키지에서는 주소가 자동으로 변경되지 않습니다.

클라이언트 조직의 네트워크에 보호 구성

중앙 관리 서버 설치가 완료되고 나면 관리 콘솔이 시작되어 관련 마법사를 통해 초기 설정을 수행하라는 메시지가 표시됩니다. 빠른 시작 마법사가 실행 중이면 루트 관리 그룹에 다음 정책과 작업이 만들어집니다:

- Kaspersky Endpoint Security 정책
- Kaspersky Endpoint Security 업데이트를 위한 그룹 작업
- Kaspersky Endpoint Security가 설치된 기기 검사를 위한 그룹 작업
- 네트워크 에이전트의 정책
- 취약점 검사 작업(네트워크 에이전트의 작업)
- 업데이트 설치 및 취약점 수정 작업(네트워크 에이전트의 작업)

정책과 작업은 기본 설정을 사용하여 만들어지는데, 이러한 기본 설정은 조직에 가장 적합하지 않을 수도 있고 조직에서 허용되지 않을 수도 있습니다. 따라서 만들어진 개체의 속성을 확인하여 필요한 경우 수동으로 수정해야 합니다.

이 섹션에서는 중앙 관리 서버의 정책, 작업 및 기타 설정을 수동으로 구성하는 방법 및 배포 지점, 관리 그룹 구조 및 작업 계층 구조 구성 및 기타 설정에 대한 정보가 포함되어 있습니다.

Kaspersky Endpoint Security 정책 수동 설정

이 섹션에서는 빠른 시작 마법사를 통해 생성한 Kaspersky Endpoint Security 정책의 권장 구성 방법을 설명합니다. 정책 속성 창에서 설정을 수행할 수 있습니다.

설정을 편집할 때는 워크스테이션에서 관련 설정의 값을 사용할 수 있도록 해당 설정 위에 있는 잠금 아이콘을 클릭해야 합니다.

지능형 위협 보호 섹션의 정책 구성

이 섹션에 나와 있는 설정의 전체 설명은 Kaspersky Endpoint Security for Windows 설명서를 참조하십시오.

지능형 위협 보호 섹션에서 Kaspersky Endpoint Security for Windows용 Kaspersky Security Network의 사용을 구성할 수 있습니다. 행동 탐지, 익스플로잇 방지, 호스트 침입 방지 및 치료 엔진과 같은 Kaspersky Endpoint Security for Windows 모듈을 구성할 수도 있습니다.

Kaspersky Security Network 하위 섹션에서 **Kaspersky Security Network** 옵션을 활성화하는 것이 좋습니다. 네트워크에서 트래픽을 재분배하고 최적화하려면 이 기능을 사용합니다. **Kaspersky Security Network** 옵션이 비활성화되었다면, 직접 KSN 서버 사용을 활성화할 수 있습니다.

필수 위협 보호 섹션의 정책 구성

이 섹션에 나와 있는 설정의 전체 설명은 Kaspersky Endpoint Security for Windows 설명서를 참조하십시오.

정책 속성 창의 **필수 위협 보호** 섹션에서 **방화벽** 및 **파일 위협 보호** 하위 섹션에 추가 설정을 지정하는 것이 좋습니다.

방화벽 하위 섹션에는 클라이언트 기기에서 애플리케이션의 네트워크 활동을 제어할 수 있는 설정이 포함되어 있습니다. 클라이언트 기기는 공용, 로컬, 신뢰 상태 중 하나가 할당된 네트워크를 사용합니다. 네트워크 상태에 따라 Kaspersky Endpoint Security는 기기에서 네트워크 활동을 허용하거나 거부할 수 있습니다. 조직에 새 네트워크를 추가할 때 적절한 네트워크 상태를 할당해야 합니다. 예를 들어 클라이언트 기기가 랩톱이라면 랩톱이 항상 로컬 네트워크에 연결되어 있는 것은 아니므로 이 기기는 공용 또는 신뢰하는 네트워크를 사용할 것을 권장합니다. **방화벽** 하위 섹션에서 조직에서 사용하는 네트워크에 상태를 올바르게 할당했는지 확인할 수 있습니다.

네트워크 목록을 확인하려면 다음을 수행합니다:

1. 정책 속성에서 애플리케이션 **필수 위협 보호** → **방화벽**으로 이동합니다.
2. **사용 가능한 네트워크** 섹션에서 **설정** 버튼을 클릭합니다.
3. **방화벽** 창이 열리면 **네트워크** 탭으로 이동하여 네트워크 목록을 확인합니다.

파일 위협 보호 하위 섹션에서 네트워크 드라이브 검사를 비활성화할 수 있습니다. 네트워크 드라이브 검사 시 네트워크 드라이브의 부하가 높아질 수 있습니다. 그러므로 파일 서버에서 간접 검사를 수행하는 것이 더 편리합니다.

네트워크 드라이브 검사를 중지하려면 다음을 수행합니다:

1. 정책 속성에서 **필수 위협 보호** → **파일 위협 보호**로 갑니다.
2. **보안 레벨** 섹션에서 **설정** 버튼을 클릭합니다.
3. **파일 위협 보호** 창이 열리면 **일반** 탭에서 **모든 네트워크 드라이브** 확인란 선택을 취소합니다.

일반 설정 섹션의 정책 구성

이 섹션에 나와 있는 설정의 전체 설명은 Kaspersky Endpoint Security 설명서를 참조하십시오.

아래에서는 고급 설정 작업에 대해 설명합니다. 이 작업은 Kaspersky Endpoint Security 정책 속성 창의 **일반 설정** 섹션에서 수행하는 것이 좋습니다.

일반 설정 섹션, 리포트 및 저장소 하위 섹션

중앙 관리 서버로 데이터 전송 섹션에서 **시작된 애플리케이션 정보** 확인란을 확인해 주십시오. 이 확인란을 선택하면 네트워크에 연결된 기기에 설치된 모든 소프트웨어 모듈의 모든 버전에 관한 정보가 중앙 관리 서버 데이터베이스에 저장됩니다. 이 정보를 저장하려면 Kaspersky Security Center 데이터베이스에서 수십 GB에 달하는 매우 많은 양의 디스크 공간이 필요할 수 있습니다. 그러므로 상위 레벨 정책에서 **시작된 애플리케이션 정보** 확인란이 아직 선택되어 있으면 선택을 취소해야 합니다.

일반 설정 섹션, 인터페이스 하위 섹션

관리 콘솔을 통해 중앙 집중식 모드로 조직 네트워크의 위협 보호를 관리해야 한다면, **사용자와의 통신** 섹션에서 **애플리케이션 인터페이스 표시** 확인란 선택을 취소하여 워크스테이션에서 Kaspersky Endpoint Security 사용자 인터페이스 표시를 중지하고, **암호 보호** 섹션에서 **암호 보호 활성화** 확인란을 선택하여 암호 보호를 작동시켜야 합니다.

이벤트 구성 섹션의 정책 구성

이벤트 구성 섹션에서는 다음을 제외한 중앙 관리 서버의 모든 이벤트 저장을 중지해야 합니다:

- **심각** 이벤트 탭:
  - *애플리케이션 자동 시작이 비활성화되었습니다*
  - *접근 거부됨*
  - *애플리케이션 시작이 금지됨*
  - *치료 불가*
  - *최종 사용자 라이센스 계약서 위반*
  - *암호화 모듈을 로드할 수 없음*
  - *두 작업을 동시에 시작할 수 없음*

- *활성 위협 탐지됨. 고급 치료 시작 필요*
- *네트워크 공격이 탐지됨*
- *일부 구성 요소가 업데이트되지 않았습니다*
- *활성화 오류*
- *휴대용 모드 활성화 오류*
- *Kaspersky Security Center와 통신 오류*
- *휴대용 모드 비활성화 오류*
- *애플리케이션 구성 요소 변경 오류*
- *파일 암호화/복호화 규칙 적용 오류*
- *정책을 적용할 수 없음*
- *프로세스 종료*
- *네트워크 활동이 차단됨*

- **기능 실패** 탭: *잘못된 작업 설정. 설정이 적용되지 않음*
- **경고** 탭:
  - *자기 보호가 비활성화되었습니다*
  - *잘못된 예비 키*
  - *사용자가 암호화 정책을 거부함*
- **정보** 탭: *테스트 모드에서의 애플리케이션 시작이 차단됨*

Kaspersky Endpoint Security용 그룹 업데이트 작업 수동 설정

중앙 관리 서버가 업데이트 경로 역할을 하는 경우 Kaspersky Endpoint Security에서 권장되는 최적의 스케줄 옵션은 **작업 시작 자동 임의 지연 사용** 확인란을 선택한 상태로 **저장소에 신규 업데이트를 다운로드했을 때**입니다.

Kaspersky 서버에서 저장소로 업데이트를 다운로드하는 로컬 작업을 각 배포 지점에서 만드는 경우 Kaspersky Endpoint Security 그룹 업데이트 작업에 권장되는 최적의 옵션은 정기 스케줄입니다. 이 경우에는 임의 실행 간격 값을 1시간으로 설정해야 합니다.

Kaspersky Endpoint Security가 설치된 기기 검사를 위한 그룹 작업 수동 설정

빠른 시작 마법사에서 기기 검사를 위한 그룹 작업을 생성합니다. 기본적으로 작업에는 **금요일 오후 7시에 실행** 스케줄이 할당되고, 작업은 자동으로 임의 실행되며, **누락된 작업 실행** 확인란 선택은 취소되어 있습니다.

즉, 예를 들어 조직의 기기가 금요일 오후 6시 30분에 종료되면 기기 검사 작업은 실행되지 않습니다. 조직에서 채택한 회사 규칙에 따라 이 작업에 가장 편리한 스케줄을 설정해야 합니다.

취약점 및 필요한 업데이트 검색 작업 스케줄 지정

빠른 시작 마법사에서 네트워크 에이전트용 *취약점 및 필요한 업데이트 검색* 작업을 만듭니다. 기본적으로 작업에는 **화요일 오후 7시에 실행** 스케줄이 할당되고, 작업은 자동으로 임의 실행되며, **누락된 작업 실행** 확인란은 선택되어 있습니다.

이 시간에 모든 기기를 종료하는 조직의 회사 규칙이 제공되는 경우에는 기기가 다시 켜진 후(수요일 아침)에 *취약점 및 필요한 업데이트 검색* 작업이 실행됩니다. 취약점 검사가 수행되면 CPU와 디스크 하위 시스템의 부하가 증가할 수 있으므로, 이러한 방식의 활동은 바람직하지 않을 수도 있습니다. 조직에서 채택한 회사 규칙에 따라 이 작업에 가장 편리한 스케줄을 설정해야 합니다.

업데이트 설치 및 취약점 수정을 위한 그룹 작업 수동 설정

빠른 시작 마법사에서 네트워크 에이전트용으로 업데이트 설치 및 취약점 수정을 위한 그룹 작업을 생성합니다. 기본적으로 작업은 매일 오전 1시에 실행되도록 설정되고, 작업은 자동으로 임의 실행되며, **누락된 작업 실행** 옵션이 활성화되어 있지 않습니다.

야간에는 기기를 종료하는 조직의 회사 규칙이 제공되는 경우 업데이트 설치는 실행되지 않습니다. 조직에서 채택한 회사 규칙에 따라 취약점 검사 작업에 가장 편리한 스케줄을 설정해야 합니다. 또한 업데이트 설치 시에는 기기를 다시 시작해야 할 수 있습니다.

관리 그룹 구조 작성 및 배포 지점 할당

Kaspersky Security Center의 관리 그룹 구조는 다음과 같은 기능을 수행합니다:

- 정책의 범위 설정

  정책 프로필을 사용하여 기기에서 관련 설정 모음을 적용할 수도 있습니다. 이 경우에는 태그, Active Directory 조직 구성 단위의 기기 위치, Active Directory 보안 그룹의 구성원 자격 등을 사용하여 정책의 범위를 설정합니다.

- 그룹 작업의 범위 설정

  관리 그룹의 계층 구조를 기준으로 하지 않는 그룹 작업은 특정 방식으로 범위를 정의합니다: 즉, 이러한 작업의 경우에는 기기 조회용 작업과 특정 기기용 작업을 사용합니다.

- 기기, 가상 중앙 관리 서버 및 보조 중앙 관리 서버에 대한 접근 권한 설정.

- 배포 지점 할당

관리 그룹의 구조를 작성할 때는 배포 지점을 가장 적절하게 할당할 수 있도록 조직 네트워크의 토폴로지를 고려해야 합니다. 배포 지점을 최적의 방식으로 배포하면 조직 네트워크의 트래픽을 절약할 수 있습니다.

기업의 조직 스키마와 MSP 클라이언트에 의해 채택된 네트워크 토폴로지에 따라 관리 그룹 구조에 다음 표준 구성을 적용할 수 있습니다:

- 단일 사무소
- 다수의 분리된 소규모 사무소

표준 MSP 클라이언트 구성: 단일 사무소

표준 "단일 사무소" 구성에서는 모든 기기가 조직 네트워크에 있으므로 기기 간에 서로 "인식"할 수 있습니다. 조직 네트워크는 협채널을 통해 연결된 몇 개의 개별 요소(네트워크 또는 네트워크 세그먼트)로 구성될 수 있습니다.

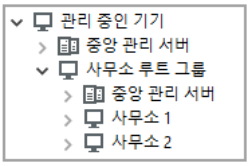
관리 그룹 구조를 구성하는 데 사용할 수 있는 방법은 다음과 같습니다:

- 네트워크 토폴로지를 고려하여 관리 그룹 구조 구성. 관리 그룹의 구조가 정밀하게 네트워크 토폴로지를 반영하지 않을 수 있습니다. 네트워크의 각 부분과 특정 관리 그룹을 연결하는 걸로도 충분합니다. 배포 지점의 자동 할당을 사용할 수도 있고 수동으로 할당할 수도 있습니다.
- 네트워크 토폴로지를 고려하지 않고 관리 그룹 구조 구성. 이 경우 배포 지점의 자동 할당을 비활성하고 네트워크의 각 부분(예: **관리 중인 기기** 그룹)에서 하나 이상의 기기가 루트 관리 그룹의 배포 지점 역할을 하도록 직접 지정해야 합니다. 모든 배포 지점은 동일한 수준에 있으며 조직 네트워크의 모든 기기에 동일한 영역을 적용합니다. 이때, 각 네트워크 에이전트는 경로가 가장 짧은 배포 지점과 연결됩니다. 배포 지점 연결 경로는 tracert 유틸리티로 추적할 수 있습니다.

표준 MSP 클라이언트 구성: 다수의 소규모 원격 사무소

이 표준 구성은 인터넷을 통해 본사 사무소와 통신할 수 있는 여러 소규모 원격 사무소를 제공합니다. 각 원격 사무소에는 NAT가 적용됩니다. 즉, 원격 사무소는 서로 격리되므로 사무소 간의 연결은 불가능합니다.

이 구성을 관리 그룹 구조에 반영해야 합니다: 각 원격 사무소에 대해 별도의 관리 그룹(아래 그림의 **사무소 1** 및 **사무소 2** 그룹)을 만들어야 합니다.



관리 그룹 구조에 포함된 원격 사무소

사무소에 해당하는 각 관리 그룹에는 배포 지점을 하나 이상 할당해야 합니다. 배포 지점은 원격 사무소의 기기여야 하며, 디스크에 여유 공간이 충분해야 합니다. 예를 들어 **사무소 1** 그룹에 배포된 기기는 **사무소 1** 관리 그룹에 할당된 배포 지점에 접근합니다.

일부 사용자가 노트북을 소지하고 사무소 간을 실제로 이동하는 경우에는 기존 배포 지점 외에 각 원격 사무소에서 둘 이상의 기기를 선택하여 상위 레벨 관리 그룹(위 그림에서는 **사무소 루트 그룹**)의 배포 지점 역할을 하도록 할당해야 합니다.

예: **사무소 1** 관리 그룹에 배포된 노트북이 **사무소 2** 관리 그룹에 해당하는 사무소로 실제로 이동되었습니다. 노트북이 이동된 후 네트워크 에이전트가 **사무소 1** 그룹에 할당된 배포 지점 접근을 시도하지만 해당 배포 지점은 사용할 수 없는 상태입니다. 그러면 네트워크 에이전트는 **사무소 루트 그룹**에 할당된 배포 지점에 대한 접근 시도를 시작합니다. 원격 사무소는 서로 격리되어 있으므로 **사무소 루트 그룹** 관리 그룹에 할당된 배포 지점 접근 시도는 네트워크 에이전트가 **사무소 2** 그룹의 배포 지점 접근을 시도할 때만 성공합니다. 즉, 노트북은 초기 사무소에 해당하는 관리 그룹에 그대로 유지되지만 해당 시점에 물리적으로 위치해 있는 사무소의 배포 지점을 사용합니다.

정책 프로필을 사용하는 정책 계층 구조

이 섹션에서는 관리 그룹에 있는 기기에 정책을 적용하게 하는 방법에 대한 정보를 제공합니다. 이 섹션에서는 정책 프로필에 대한 정보도 제공합니다.

정책 계층 구조

Kaspersky Security Center에서는 정책을 사용해 여러 기기에 대해 단일 설정 모음을 정의합니다. 예를 들어 관리 그룹 G에 대해 정의된 애플리케이션 P의 정책 범위에는 그룹 G와 그 하위 그룹에 배포되었으며 애플리케이션 P가 설치된 관리 중인 기기가 포함됩니다. 단, 속성에서 **부모 그룹에서 상속** 확인란 선택을 취소한 하위 그룹은 제외됩니다.

정책은 로컬 설정과 달리 해당 설정 옆에 자물쇠 아이콘()이 있습니다. 설정이나 설정 그룹이 정책 속성에서 잠금 상태인 경우에는 먼저 유효 설정을 만들 때 이 설정이나 설정 그룹을 사용해야 하며, 둘째로는 해당 설정이나 설정 그룹을 다운스트림 정책에 기록해야 합니다.

기기에서 유효 설정을 만드는 과정은 다음과 같이 설명할 수 있습니다: 잠금 상태가 아닌 모든 설정의 값을 정책에서 가져온 다음 로컬 설정의 값으로 덮어씁니다. 그런 후에 생성된 모음을 정책에서 가져온 "잠금" 상태의 설정 값으로 덮어씁니다.

동일 애플리케이션의 정책은 관리 그룹 계층 구조를 통해 서로 영향을 줍니다: 업스트림 정책에 있는 잠금 상태의 설정은 다운스트림 정책의 동일 설정을 덮어씁니다.

이동 사용자를 위한 특수 정책이 있습니다. 이 정책은 이동 사용자 모드로 전환되는 기기에 적용됩니다. 이동 사용자 정책은 관리 그룹 계층 구조를 통해 다른 정책에 영향을 주지 않습니다.

정책 프로필

대부분의 상황에서는 관리 그룹 계층 구조만을 통해 기기에 정책을 적용하는 방식이 불편할 수 있습니다. 즉, 각 관리 그룹용으로 설정이 한두 개만 다른 단일 정책의 여러 인스턴스를 만들고 나중에 해당 정책의 컨텐츠를 동기화해야 할 수 있습니다.

이러한 문제를 방지하기 위해 Kaspersky Security Center는 *정책 프로필*을 지원합니다. 정책 프로필은 정책 설정의 명명된 하위 집합입니다. 이 하위 집합은 정책과 함께 대상 기기에 배포되며 *프로필 활성화 조건*이라는 특수 조건에서 정책을 보완합니다. 클라이언트 기기(컴퓨터 또는 모바일 기기)에서 활성 상태인 "기본" 정책과 다른 설정만 프로필에 포함됩니다. 프로필을 활성화하면 프로필 활성화 전에 기기에서 활성 상태였던 정책 설정이 수정됩니다. 해당 설정은 프로필에 지정된 값을 사용합니다.

현재 정책 프로필에 적용되는 제한은 다음과 같습니다:

- 프로필은 정책당 100개까지 포함할 수 있습니다.
- 정책 프로필은 다른 프로필을 포함할 수 없습니다.
- 정책 프로필은 알림 설정을 포함할 수 없습니다.

프로필의 컨텐츠

정책 프로필에는 다음과 같은 구성 요소가 포함됩니다:

- 이름. 이름이 같은 프로필은 공통 규칙에 따라 관리 그룹의 계층을 통해 서로 영향을 줍니다.
- 정책 설정의 하위 집합. 모든 설정을 포함하는 정책과 달리 프로필은 실제로 필요한 설정(잠금 상태의 설정)만 포함합니다.
- 활성화 조건은 기기 속성이 포함된 논리식입니다. 프로필은 프로필 활성화 조건이 참일 때만 활성화되어 정책을 보완합니다. 기타 모든 경우에는 프로필이 비활성 상태이며 무시됩니다. 이 논리식에 포함할 수 있는 기기 속성은 다음과 같습니다:
  - 이동 사용자 모드의 상태.
  - 네트워크 환경의 속성 – 네트워크 에이전트 연결에 대한 활성화 규칙의 이름.
  - 기기에서 지정된 태그의 유무.
  - Active Directory 단위에서의 기기 할당: 명시적(기기가 지정된 OU에 직접 포함되어 있음) 또는 암묵적(기기가 특정 중첩 레벨에서 지정된 OU 내에 있는 OU에 포함되어 있음).
  - Active Directory 보안 그룹에 있는 기기 구성원 (명시적 또는 암묵적).
  - Active Directory 보안 그룹에 있는 기기 소유자 구성원 (명시적 또는 암묵적).
- 프로필 중지 확인란. 중지된 프로필은 항상 무시되며, 해당 프로필의 개별 활성화 조건을 확인하지 않습니다.
- 프로필 우선 순위. 개별 프로필의 활성화 조건은 서로 독립적이므로 여러 프로필을 동시에 활성화할 수 있습니다. 활성 프로필에 겹치지 않는 설정 모음이 포함되어 있으면 문제가 발생하지 않습니다. 그러나 두 활성 프로필에 동일 설정의 서로 다른 값이 포함되어 있으면 프로필이 모호해집니다. 프로필 우선 순위를 활용하여 이와 같은 모호한 프로필을 방지할 수 있습니다: 모호한 변수의 값을 우선 순위가 더 높은 프로필(프로필 목록에서 순위가 더 높은 프로필)에서 가져옵니다.

정책이 계층 구조를 통해 서로 영향을 줄 때의 프로필 동작

이름이 같은 프로필은 정책 병합 규칙에 따라 병합됩니다. 업스트림 정책의 프로필이 다운스트림 정책의 프로필보다 우선 순위가 높습니다. 업스트림 정책에서 설정 편집이 금지된 경우, 즉 설정이 잠금 상태인 경우 다운스트림 정책은 업스트림 정책의 프로필 활성화 조건을 사용합니다. 업스트림 정책에서 설정 편집이 허용되는 경우에는 다운스트림 정책의 프로필 활성화 조건이 사용됩니다.

정책 프로필의 활성화 조건에는 **오프라인 상태인 기기** 속성이 포함될 수 있으므로 이동 사용자를 위한 정책의 기능은 프로필로 완전히 교체되며 더 이상 지원되지 않습니다.

이동 사용자를 위한 정책은 프로필을 포함할 수 있지만 해당 프로필은 기기가 이동 사용자 모드로 전환된 후에만 활성화할 수 있습니다.

작업

Kaspersky Security Center에서는 *작업*을 만들고 실행하여 기기에 설치된 Kaspersky 보안 제품을 관리할 수 있습니다. 작업은 애플리케이션을 설치, 실행 및 중단하고, 파일을 검사하며, 데이터베이스와 소프트웨어 모듈을 업데이트하고, 애플리케이션에 대해 기타 작업을 수행하는 데 필요합니다.

특정 애플리케이션용 관리 플러그인이 설치되어 있어야 해당 애플리케이션용 작업을 생성할 수 있습니다.

중앙 관리 서버와 기기에서 작업을 수행할 수 있습니다.

다음 작업이 중앙 관리 서버에서 수행됩니다:

- 리포트 자동 배포
- 중앙 관리 서버 저장소 업데이트 다운로드
- 중앙 관리 서버 데이터 백업
- 데이터베이스 유지 보수
- Windows 업데이트 동기화
- 참조 기기의 운영 체제(OS) 이미지에 따라 설치 패키지 만들기

기기에서 수행되는 작업 유형은 다음과 같습니다:

- *로컬 작업* - 특정 기기에서 수행되는 작업

  로컬 작업은 관리자가 관리 콘솔 도구를 사용하여 수정할 수도 있고, 원격 기기의 사용자가 보안 제품 인터페이스 등을 통해 수정할 수도 있습니다. 관리자와 관리 중인 기기 사용자가 로컬 작업을 동시에 수정한 경우에는 우선 순위가 더 높은 관리자가 수행한 변경 사항이 적용됩니다.

- *그룹 작업* - 특정 그룹의 모든 기기에서 수행되는 작업

  작업 속성에 별도로 지정된 경우가 아니면 그룹 작업은 선택한 그룹의 모든 하위 그룹에도 영향을 줍니다. 그룹 작업은 이 그룹이나 해당 하위 그룹에 배포한 보조 및 가상 중앙 관리 서버에 연결된 기기에도 선택적으로 적용됩니다.

- *글로벌 작업* - 그룹에 포함되어 있는지 여부에 관계없이 선택한 기기에서 수행되는 작업

각 애플리케이션에 대해 그룹 작업, 글로벌 작업 또는 로컬 작업을 원하는 수만큼 만들 수 있습니다.

작업 설정을 변경하고 작업 진행 상황을 확인하며, 해당 설정의 복사, 내보내기, 가져오기 및 삭제를 수행할 수 있습니다.

작업을 만든 애플리케이션이 실행 중인 경우에만 기기에서 작업이 시작됩니다.

작업의 결과는 중앙 관리 서버에 중앙 집중식으로 Microsoft Windows 이벤트 로그 및 Kaspersky Security Center 이벤트 로그에 저장되며, 각 기기에 로컬로도 동일하게 저장됩니다.

작업 설정에 기밀 데이터를 포함하지 마십시오. 예를 들어, 도메인 관리자 암호를 지정하지 마십시오.

기기 이동 규칙

*기기 이동 규칙*을 사용하여 MSP 클라이언트에 해당하는 가상 서버의 관리 그룹으로 기기를 할당하는 작업을 자동화하는 것이 좋습니다. 기기 이동 규칙은 세 가지 주요 부분으로 구성됩니다: 이 세 가지 부분은 이름, 실행 조건(기기 특성이 포함된 논리식), 그리고 대상 관리 그룹입니다. 기기 특성이 규칙 실행 조건을 충족하면 규칙이 기기를 대상 관리 그룹으로 이동합니다.

모든 기기 이동 규칙에는 우선 순위가 있습니다. 중앙 관리 서버는 기기 특성이 각 규칙의 실행 조건을 충족하는지를 우선 순위의 오름차순으로 확인합니다. 기기 특성이 규칙의 실행 조건을 충족하는 경우 기기가 대상 그룹으로 이동되며 해당 기기에 대한 규칙 처리가 완료됩니다. 기기 특성이 여러 규칙의 조건을 충족하는 경우에는 우선 순위가 가장 높은 규칙(규칙 목록에서 순위가 가장 높은 규칙)의 대상 그룹으로 기기가 이동됩니다.

기기 이동 규칙은 묵시적으로 만들 수 있습니다. 예를 들어 원격 설치 작업 또는 설치 패키지의 속성에서 네트워크 에이전트를 기기에 설치한 후 기기를 이동해야 하는 관리 그룹을 지정할 수 있습니다. 또한 Kaspersky Security Center 관리자가 이동 규칙 목록에서 기기 이동 규칙을 명시적으로 만들 수도 있습니다. 이 목록은 관리 콘솔의 **미할당 기기** 그룹 속성에 있습니다.

기본적으로 기기 이동 규칙은 기기를 관리 그룹으로 한 번 초기 할당할 때 사용됩니다. 이 규칙은 **미할당 기기** 그룹의 기기를 한 번만 이동합니다. 기기가 이 규칙에 의해 한 번 이동된 경우 해당 기기를 **미할당 기기** 그룹에 수동으로 되돌려 놓더라도 규칙은 해당 기기를 다시 이동하지 않습니다. 이동 규칙은 이러한 방식으로 적용하는 것이 좋습니다.

일부 관리 그룹에 이미 할당된 기기를 이동할 수 있습니다. 이렇게 하려면 규칙 속성에서 **관리 그룹에 추가 안 된 기기만 이동** 확인란 선택을 취소합니다.

일부 관리 그룹에 이미 할당된 기기에 이동 규칙을 적용하면 중앙 관리 서버의 부하가 크게 증가합니다.

단일 기기에 반복적으로 적용되는 이동 규칙을 만들 수 있습니다.

하지만 기기에 특수 정책을 적용하거나, 특수 그룹 작업을 실행하거나, 특정 배포 지점을 통해 기기를 업데이트하는 등의 작업을 위해 단일 기기를 그룹 간에 반복적으로 이동하지 않는 것이 좋습니다.

이러한 방식의 이동은 지원되지 않습니다. 이와 같이 기기를 이동하는 경우 중앙 관리 서버의 부하와 네트워크 트래픽이 지나치게 증가하기 때문입니다. 그리고 이러한 이동은 특히 접근 권한, 이벤트 및 리포트 측면에서 Kaspersky Security Center의 작동 원칙과도 충돌합니다. 다른 해결 방법을 찾아야 합니다. 예를 들어 정책 프로필을 사용하거나 기기 조회용 작업을 사용하거나 표준 시나리오에 따라 네트워크 에이전트를 할당하는 등의 방법을 사용할 수 있습니다.

소프트웨어 분류

애플리케이션 실행을 모니터링하는 데 기본적으로 사용되는 도구는 *Kaspersky 카테고리*(이하 *KL 카테고리*로 지칭함)입니다. Kaspersky Security Center 관리자는 KL 카테고리를 사용하여 소프트웨어 분류를 간편하게 지원하고 관리 중인 기기로 전송되는 트래픽을 최소화할 수 있습니다.

기존 KL 카테고리로 분류할 수 없는 애플리케이션(예: 사용자 지정 방식으로 작성된 소프트웨어)에 대해서만 사용자 카테고리를 만들어야 합니다. 애플리케이션 설치 패키지(MSI) 또는 설치 패키지가 포함된 폴더를 기준으로 하여 사용자 카테고리를 만듭니다.

KL 카테고리를 통해 분류되지 않은 대량의 소프트웨어 모음을 사용할 수 있는 경우에는 자동으로 업데이트되는 카테고리를 만들면 유용할 수 있습니다. 그러면 배포 패키지가 포함된 폴더를 수정할 때마다 실행 파일의 체크섬이 해당 카테고리에 자동으로 추가됩니다.

문서, %windir%, %ProgramFiles% 및 %ProgramFiles(x86)% 폴더에 자동 업데이트되는 소프트웨어 범주를 생성하지 마십시오. 이러한 폴더의 파일 풀은 자주 변경되므로 중앙 관리 서버의 부하와 네트워크 트래픽이 증가합니다. 소프트웨어 모음이 저장되는 전용 폴더를 만들어 주기적으로 새 항목을 해당 폴더에 추가해야 합니다.

멀티테넌트 애플리케이션 정보

Kaspersky Security Center를 사용하면 서비스 공급자 및 테넌트 관리자가 멀티테넌트를 지원하는 Kaspersky 애플리케이션을 사용할 수 있습니다. 멀티테넌트 Kaspersky 애플리케이션이 서비스 공급자의 인프라에 설치되면 테넌트가 해당 애플리케이션의 사용을 시작할 수 있습니다.

서로 다른 테넌트와 관련된 작업 및 정책을 분리하려면 각 테넌트에 대한 전용 가상 중앙 관리 서버를 Kaspersky Security Center에 생성해야 합니다. 테넌트에 대해 실행 중인 멀티테넌트 애플리케이션에 대한 모든 작업 및 정책은 해당 테넌트에 해당하는 가상 중앙 관리 서버의 관리 중인 기기 관리 그룹에 생성되어야 합니다. 기본 중앙 관리 서버와 관련된 관리 그룹에 대해 생성된 작업은 테넌트로 관리하는 기기에 영향을 주지 않습니다.

서비스 공급자 관리자와 달리 테넌트 관리자는 해당 테넌트의 기기에 대해서만 작업 및 애플리케이션 정책을 생성하고 볼 수 있습니다. 서비스 공급자 관리자와 테넌트 관리자가 사용할 수 있는 작업 및 정책 설정 세트가 다릅니다. 일부 작업 및 정책 설정은 테넌트 관리자가 사용할 수 없습니다.

테넌트의 계층 구조 내에서 멀티테넌트 애플리케이션용으로 생성된 정책은 상위 레벨 관리 그룹 및 하위 레벨 관리 그룹으로 상속됩니다. 정책은 해당 테넌트에 속한 모든 클라이언트 기기로 전파됩니다.

중앙 관리 서버 설정 백업 및 복원

중앙 관리 서버와 해당 데이터베이스의 설정 백업은 백업 작업 및 klbackup 유틸리티를 통해 수행됩니다. 백업 복사본에는 인증서, 관리 중인 기기의 드라이브 암호화용 마스터 키, 다양한 라이센스용 키, 모든 컨텐츠/작업/정책 등이 들어 있는 관리 그룹의 구조와 같은 중앙 관리 서버와 관련된 모든 기본 설정 및 개체가 포함됩니다. 백업 복사본이 이 있으면 중앙 관리 서버의 동작을 최대한 빨리 복구할 수 있습니다(복구에는 약 10분~2시간이 소요됨). 백업 복사본이 이 있으면 중앙 관리 서버의 동작을 최대한 빨리 복구할 수 있습니다(복구에는 십여 분에서 몇 시간 소요).

백업 복사본을 사용할 수 없으면 오류 발생 시 인증서와 모든 중앙 관리 서버 설정이 손실되어 복구할 수 없게 될 수 있습니다. 그러면 Kaspersky Security Center를 처음부터 다시 구성해야 하며, 조직 네트워크에서 네트워크 에이전트 초기 배포를 다시 수행해야 합니다. 관리 중인 기기의 드라이브 암호화를 위한 모든 기본 키도 손실되므로 Kaspersky Endpoint Security가 설치된 기기에서 암호화된 데이터가 손실되어 복구할 수 없게 될 위험이 있습니다. 따라서, 표준 백업 작업을 사용하여 중앙 관리 서버를 정기적으로 백업해야 합니다.

빠른 시작 마법사에서는 중앙 관리 서버 설정에 대한 백업 작업을 만들어 매일 오전 4시에 실행되도록 설정합니다. 백업 복사본은 기본적으로 %ALLUSERSPROFILE%\Application Data\KasperskySC 폴더에 저장됩니다.

다른 기기에 설치된 Microsoft SQL Server 인스턴스를 DBMS로 사용하는 경우에는 UNC 경로를 지정하여 백업 작업을 수정해야 합니다. UNC 경로는 중앙 관리 서버 서비스와 SQL Server 서비스 둘 다에서 백업 복사본을 저장할 폴더로 작성 가능합니다. 이 요구 사항은 Microsoft SQL Server DBMS에 포함된 백업의 특수 기능과 연관된 것입니다.

Microsoft SQL Server의 로컬 인스턴스를 DBMS로 사용하는 경우에는 중앙 관리 서버와 함께 백업 복사본이 손상되지 않도록 보호하기 위해 전용 매체에 백업 복사본을 저장하는 방식도 권장합니다.

백업 복사본에는 중요한 데이터가 포함되므로 백업 작업 및 klbackup 유틸리티는 백업 복사본의 암호 보호 기능을 제공합니다. 백업 작업은 기본적으로 암호가 비어 있는 상태로 작성됩니다. 백업 작업의 속성에서 암호를 설정해야 합니다. 이 요구 사항을 무시하면 중앙 관리 서버 인증서의 모든 키, 라이센스용 키, 그리고 관리 중인 기기의 드라이브 암호화용 기본 키가 암호화되지 않은 상태로 유지되는 상황이 발생합니다.

정기적인 백업 외에도 중요한 변경(중앙 관리 서버 업그레이드 및 패치 설치 포함)을 수행하기 전에는 항상 백업 복사본을 만들어야 합니다.

Microsoft SQL Server를 DBMS로 사용하면 백업 복사본의 크기를 최소화할 수 있습니다. 이렇게 하려면 SQL Server 설정에서 **백업 압축** 옵션을 활성화합니다.

가장 최근에 설치되었으며 버전이 백업 복사본을 만든 인스턴스 이상인 작동 가능한 중앙 관리 서버 인스턴스에서 klbackup 유틸리티를 사용하여 백업 복사본 복원을 수행합니다.

복원을 수행할 중앙 관리 서버 인스턴스는 버전이 같거나 이후이고 유형이 같은 DBMS(같은 SQL Server 또는 MySQL 등)를 사용해야 합니다. 중앙 관리 서버의 버전은 원래 버전과 같을 수도 있고(패치가 원래 중앙 관리 서버와 동일하거나 그 이상임) 더 최신 버전일 수도 있습니다.

이 섹션에서는 중앙 관리 서버의 설정과 개체를 복원하기 위한 표준 시나리오에 대해 설명합니다.

중앙 관리 서버가 설치된 기기가 작동하지 않음

중앙 관리 서버가 설치된 기기가 오류로 인해 작동하지 않으면 다음 작업을 수행하는 것이 좋습니다:

- 새 중앙 관리 서버에 같은 주소를 할당해야 합니다. 네트워크 에이전트를 배포할 때 설정된 항목에 따라 NetBIOS 이름, FQDN 또는 고정 IP를 할당해야 합니다.
- 유형이 원래 DBMS와 같고 버전이 원래 DBMS 이상인 DBMS를 사용하여 중앙 관리 서버를 설치합니다. 패치가 원래 서버와 같거나 그 이상인 동일 버전의 서버 또는 최신 버전의 서버를 설치할 수 있습니다. 설치 후에는 마법사를 통해 초기 설정을 수행하지 않습니다.
- **시작** 메뉴에서 klbackup 유틸리티를 실행하여 복원을 수행합니다.

데이터베이스 또는 중앙 관리 서버의 설정이 손상됨

전원 서지 등이 발생한 이후 설정이나 데이터베이스가 손상되어 중앙 관리 서버가 작동하지 않는 경우에는 다음 복원 시나리오를 사용하는 것이 좋습니다:

1. 손상된 기기에서 파일 시스템을 검사합니다.
2. 작동하지 않는 중앙 관리 서버 버전을 제거합니다.
3. 유형이 원래 DBMS와 같고 버전이 원래 DBMS 이상인 DBMS를 사용하여 중앙 관리 서버를 다시 설치합니다. 패치가 원래 서버와 같거나 그 이상인 동일 버전의 서버 또는 최신 버전의 서버를 설치할 수 있습니다. 설치 후에는 마법사를 통해 초기 설정을 수행하지 않습니다.
4. **시작** 메뉴에서 klbackup 유틸리티를 실행하여 복원을 수행합니다.

klbackup 유틸리티를 사용하는 방식 이외의 방식으로 중앙 관리 서버를 복원하는 행위는 금지됩니다.

타사 소프트웨어를 통해 중앙 관리 서버 복원을 시도하면 배포된 애플리케이션 Kaspersky Security Center의 노드에서 데이터 동기화가 해제되며, 그러면 애플리케이션이 잘못된 방식으로 작동하게 됩니다.

네트워크 에이전트 및 보안 제품 배포

조직의 기기를 관리하려면 각 기기에 네트워크 에이전트를 설치해야 합니다. 조직 기기에 분포된 Kaspersky Security Center를 배포할 때는 대개 해당 기기에 네트워크 에이전트를 먼저 설치합니다.

Microsoft Windows XP에서 네트워크 에이전트는 다음 동작을 올바르게 수행하지 못할 수 있습니다: Kaspersky 서버(배포 지점)에서 업데이트 직접 다운로드, KSN 프록시 서버 기능(배포 지점), 타사 취약점 탐지(취약점 및 패치 관리 사용 시).

초기 배포

네트워크 에이전트가 기기에 이미 설치된 경우에는 이 네트워크 에이전트를 통해 해당 기기에서 애플리케이션 원격 설치를 수행합니다. 설치할 애플리케이션의 배포 패키지는 네트워크 에이전트와 중앙 관리 서버 간의 통신 채널을 통해 관리자가 정의한 설치 설정과 함께 전송됩니다. 릴레이 배포 노드, 즉 배포 지점, 멀티캐스트 전달 등을 사용하여 배포 패키지를 전송할 수 있습니다. 이미 네트워크 에이전트를 설치한 관리 중인 기기에 애플리케이션을 설치하는 방법에 대한 자세한 내용은 이 섹션 아래를 참조하십시오.

다음 방법 중 하나를 사용하여 Windows를 실행 중인 기기에서 네트워크 에이전트 초기 설치를 수행할 수 있습니다:

- 애플리케이션 원격 설치용 타사 도구를 사용합니다.
- Windows 그룹 정책: 그룹 정책에 표준 Windows 관리 도구 사용.
- Kaspersky Security Center의 원격 설치 작업에 포함된 특수 옵션을 사용하여 강제 모드로 수행합니다.
- 기기 사용자에게 Kaspersky Security Center에서 생성된 독립 실행형 패키지의 링크를 전송합니다. 독립 실행형 패키지는 선택한 애플리케이션의 배포 패키지를 포함하는 설정이 정의된 실행 모듈입니다.
- 기기에서 애플리케이션 설치 관리자를 실행하여 수동으로 수행합니다.

Microsoft Windows 이외의 플랫폼에서는 기존 타사 도구를 사용하거나 수동으로(미리 구성된 배포 패키지가 들어 있는 압축 파일을 사용자에게 전송함) 관리 중인 기기에서 네트워크 에이전트 초기 설치를 수행해야 합니다. Windows 이외의 플랫폼에서는 네트워크 에이전트를 새 버전으로 업그레이드하거나 다른 Kaspersky 애플리케이션을 설치할 수 있으며, 기기에 이미 설치된 네트워크 에이전트를 사용하여 원격 설치 작업을 수행할 수 있습니다. 이 경우 설치 과정은 Microsoft Windows가 설치된 기기에서의 과정과 동일합니다.

관리 네트워크에서 애플리케이션 배포를 위한 방법과 전략을 선택할 때는 다음과 같은 여러 가지 요인을 고려해야 합니다. 아래 목록에는 고려해야 하는 요인 중 일부가 나와 있습니다:

- 기업 네트워크 구성
- 총 기기 개수
- 관리 네트워크의 Windows 도메인 유무, 해당 도메인에서의 Active Directory 그룹 정책 수정 가능성
- Kaspersky 애플리케이션 초기 배포가 계획된 기기에서 로컬 관리자 권한이 있는 사용자 계정 확인(예: 로컬 관리자 권한이 있는 도메인 사용자 계정 사용 가능성 또는 해당 기기에서 관리자 권한이 있는 통합 로컬 사용자 계정의 유무)
- 중앙 관리 서버와 MSP 클라이언트 네트워크 간의 네트워크 채널 연결 유형 및 대역폭과 해당 네트워크 내의 채널 대역폭
- 배포 시작 시 원격 기기에 적용되는 보안 설정(예: UAC 및 단순 파일 공유 모드 사용)

설치 관리자 구성

네트워크에서 Kaspersky 애플리케이션 배포를 시작하기 전에 애플리케이션 설치 중에 정의되는 설치 설정을 지정해야 합니다. 네트워크 에이전트를 설치할 때는 최소한 중앙 관리 서버와 프록시 설정 연결을 위한 주소를 지정해야 하며, 몇 가지 고급 설정도 필요할 수 있습니다. 선택한 설치 방법에 따라 각기 다른 방식으로 설정을 정의할 수 있습니다. 가장 단순한 경우(선택한 기기에서 수동 대화식 설치 수행)에는 설치 관리자의 사용자 인터페이스를 통해 모든 관련 설정을 정의할 수 있습니다. 그러므로 경우에 따라서는 사용자가 설치 관리자 인터페이스에서 입력해야 하는 중앙 관리 서버 주소 등의 설정과 함께 네트워크 에이전트 배포 패키지 링크를 사용자에게 전송하는 방식으로 초기 배포를 수행할 수도 있습니다.

이 방법은 사용자에게 불편하며 수동으로 설정을 정의하면 오류가 발생할 위험이 높으므로 사용하지 않는 것이 좋습니다. 또한, 기기 그룹에서 애플리케이션을 숨김 설치하는 경우에도 이 방법을 사용할 수 없습니다. 일반적으로는 관리자가 중앙 집중식 모드에서 설정 값을 지정해야 하며, 나중에 독립 실행형 패키지를 만들 때 이러한 값을 사용할 수 있습니다. 독립 실행형 패키지는 관리자가 정의한 설정이 적용된 배포 패키지가 들어 있는 자동으로 압축 해제되는 압축 파일입니다. 최종 사용자의 다운로드와 선택한 네트워크 기기에서의 숨김 설치를 모두 허용하는 리소스(Kaspersky Security Center 웹 서버 등)에서 독립 실행형 패키지를 찾을 수 있습니다.

설치 패키지

애플리케이션 설치 설정을 정의하는 첫 번째 방법이자 기본 방법은 Kaspersky Security Center 도구와 대다수 타사 도구를 사용하는 모든 설치 방법에 적합한 범용 방법입니다. 이 방법을 사용할 때는 Kaspersky Security Center에서 애플리케이션 설치 패키지를 만듭니다.

다음과 같은 방법을 사용하여 설치 패키지를 생성합니다:

- 포함된 *설명자*(설치를 위한 규칙과 결과 분석 및 기타 정보를 포함하는 확장자가 .kud인 파일)를 기준으로 하여 지정한 배포 패키지에서 자동으로 생성
- 설치 관리자의 실행 파일이나 Microsoft Windows Installer(MSI) 형식 설치 관리자에서 생성(표준 또는 지원되는 애플리케이션의 경우)

생성된 설치 패키지는 하위 폴더와 파일이 있는 폴더의 계층 구조로 구성됩니다. 설치 패키지에는 원본 배포 패키지 외에 편집 가능한 설정(설치를 완료하려면 운영 체제를 다시 시작해야 하는지 여부 등을 처리하기 위한 규칙과 설치 관리자의 설정 포함)과 부수적인 보조 모듈도 포함됩니다.

특정 애플리케이션을 지원하는 데 필요한 설치 설정의 값은 설치 패키지를 만들 때 관리 콘솔 사용자 인터페이스에서 지정할 수 있습니다. 이미 만든 설치 패키지의 속성에서는 추가 설정이 제공됩니다. Kaspersky Security Center 도구를 통해 애플리케이션 원격 설치를 수행할 때는 설치 패키지가 대상 기기로 전송되므로, 애플리케이션의 설치 관리자를 실행하면 관리자가 정의한 모든 설정이 해당 애플리케이션에 제공됩니다. Kaspersky 애플리케이션 설치를 위해 타사 도구를 사용하는 경우에는 대상 기기에서 전체 설치 패키지를 사용할 수 있는지, 즉 배포 패키지와 해당 설정을 사용할 수 있는지만 확인하면 됩니다. Kaspersky Security Center에서는 공유 데이터 폴더 내의 전용 하위 폴더에 설치 패키지를 만들어서 저장합니다.

> 설치 패키지 파라미터에서 권한 있는 사용자 계정의 세부정보를 입력하지 마십시오.

타사 도구를 통한 배포 전에 Kaspersky 애플리케이션에 이 구성 방법을 사용하는 방법에 대한 자세한 내용은 "Microsoft Windows의 그룹 정책을 사용하는 배포" 섹션을 참조하십시오.

Kaspersky Security Center를 설치한 직후에는 설치 패키지 몇 개가 자동으로 생성됩니다; 이러한 패키지는 Microsoft Windows용 보안 제품 패키지와 네트워크 에이전트 패키지를 포함하며 즉시 설치 가능합니다.

경우에 따라서는 MSP 클라이언트 네트워크에서 설치 패키지를 사용하여 애플리케이션을 배포하는 경우 가상 서버에서 MSP 클라이언트에 해당하는 설치 패키지를 만들어야 할 수 있습니다. 가상 서버에서 설치 패키지를 만들면 MSP 클라이언트별로 다른 설치 설정을 사용할 수 있습니다. 첫째로, 이처럼 설치 패키지를 만들면 네트워크 에이전트 설치 패키지를 처리할 때 유용합니다. 각 MSP 클라이언트의 네트워크에 배포되는 네트워크 에이전트는 서로 다른 주소를 사용해 중앙 관리 서버에 연결하기 때문입니다. 실제로 연결 주소에 따라 네트워크 에이전트가 연결하는 서버가 결정됩니다.

가상 중앙 관리 서버에서 새 설치 패키지를 즉시 만들 수 있을 뿐 아니라, 가상 중앙 관리 서버에서 설치 패키지의 기본 작동 모드를 통해 기본 중앙 관리 서버에서 가상 중앙 관리 서버로 설치 패키지를 "배포"할 수도 있습니다. 해당하는 중앙 관리 서버 작업을 사용하여 선택한 가상 중앙 관리 서버(선택한 관리 그룹 내의 모든 서버 포함)로 선택한 설치 패키지 또는 모든 설치 패키지를 배포할 수 있습니다. 또한, 새 가상 중앙 관리 서버를 만들 때 기본 중앙 관리 서버의 설치 패키지 목록을 선택할 수도 있습니다. 선택한 패키지는 새로 만든 가상 중앙 관리 서버로 즉시 배포됩니다.

설치 패키지를 배포할 때 해당 컨텐츠가 모두 복사되지는 않습니다. 배포하는 설치 패키지에 해당하는 가상 중앙 관리 서버의 파일 저장소에는 해당 가상 서버와 관련된 설정의 파일만 저장됩니다. 설치하는 애플리케이션의 배포 패키지를 포함한 설치 패키지의 주요 부분은 변경되지 않고 그대로 유지되며 기본 중앙 관리 서버 저장소에만 저장됩니다. 따라서 시스템 성능은 크게 개선하고 필요한 디스크 볼륨은 줄일 수 있습니다. 원격 설치 작업을 실행하거나 독립 실행형 설치 패키지를 만들 때와 같이 가상 중앙 관리 서버로 배포된 설치 패키지를 처리할 때는 기본 중앙 관리 서버의 원본 설치 패키지 데이터가 가상 중앙 관리 서버의 배포된 패키지에 해당하는 설정 파일과 "병합"됩니다.

> 애플리케이션의 라이센스 키를 설치 패키지 속성에서 설정할 수는 있지만, 이 라이센스 배포 방법은 사용하지 않는 것이 좋습니다. 폴더의 파일에 대한 읽기 권한이 실수로 제공될 수 있기 때문입니다. 자동으로 배포되는 라이센스 키를 사용하거나 라이센스 키 설치 작업을 사용해야 합니다.

MSI 속성 및 변환 파일

Windows 플랫폼에서 설치를 구성하는 또 다른 방법은 MSI 속성 및 변환 파일을 정의하는 것입니다. Microsoft Installer 형식 설치 관리자용 타사 도구를 통해 설치를 수행할 때와, Windows 그룹 정책 처리용 표준 Microsoft 도구 또는 기타 타사 도구를 사용하여 Windows 그룹 정책을 통해 설치를 수행할 때 이 방법을 사용할 수 있습니다.

애플리케이션 원격 설치용 타사 도구를 사용한 배포

Microsoft System Center 등의 애플리케이션 원격 설치용 도구가 조직에서 제공되는 경우에는 해당 도구를 사용하여 초기 배포를 수행하면 편리합니다.

이 경우 다음 작업을 수행해야 합니다:

- 사용할 배포 도구에 가장 적합한 설치 구성 방법을 선택합니다.
- 관리 콘솔 인터페이스를 통한 설치 패키지 설정 수정 작업과, 설치 패키지 데이터에서 애플리케이션 배포에 사용하도록 선택한 타사 도구의 작동을 동기화할 메커니즘을 정의합니다.

Kaspersky Security Center의 원격 설치 작업에 대한 일반 정보

Kaspersky Security Center에서는 원격 설치 작업으로 구현되는 광범위한 애플리케이션 원격 설치 방법을 제공합니다. 지정한 관리 그룹과 특정 기기 또는 기기 조회에 모두 사용 가능한 원격 설치 작업을 만들 수 있습니다. 이러한 작업은 관리 콘솔의 **작업** 폴더에 표시됩니다. 작업을 만들 때는 해당 작업 내에서 설치할 설치 패키지(네트워크 에이전트 및/또는 기타 애플리케이션의 설치 패키지)를 선택할 수 있으며, 원격 설치 방법을 정의하는 특정 설정도 지정할 수 있습니다.

관리 그룹에 대한 작업은 지정한 그룹에 포함되어 있는 기기와 해당 관리 그룹 내 모든 하위 그룹의 모든 기기에 영향을 줍니다. 작업에서 해당하는 설정을 작동하는 경우 그룹 또는 그룹의 하위 그룹에 포함된 보조 중앙 관리 서버의 기기에 대해 작업이 수행됩니다.

특정 기기에 대한 작업을 수행하면 작업이 시작될 때의 조회 컨텐츠에 따라 각 실행 시 클라이언트 기기 목록이 새로 고쳐집니다. 보조 중앙 관리 서버에 연결된 기기가 조회에 포함되는 경우에는 해당 기기에서도 작업이 실행됩니다.

보조 중앙 관리 서버에 연결된 기기에서 원격 설치 작업이 정상적으로 작동하도록 하려면 배포 작업을 사용하여 작업에서 사용되는 설치 패키지를 해당 보조 중앙 관리 서버로 미리 배포해야 합니다.

Microsoft Windows의 그룹 정책을 사용하는 배포

다음 조건이 충족되는 경우 Microsoft Windows 그룹 정책을 통해 네트워크 에이전트 초기 배포를 수행하는 것이 좋습니다:

- 이 기기는 Active Directory 도메인의 구성원입니다.
- 관리자 권한에는 도메인 컨트롤러 접근 권한이 부여되므로 Active Directory 그룹 정책을 만들고 수정할 수 있습니다.
- 구성한 설치 패키지는 대상 관리 중인 기기를 호스팅하는 네트워크(모든 대상 기기가 읽을 수 있는 공유 폴더)로 이동할 수 있습니다.
- 배포 구성에서 대상 기기에 대해 네트워크 에이전트 배포를 시작하기 전에 해당 기기의 다음 정기 다시 시작 시까지 기다리도록 허용하는 경우 또는 해당 기기에 Windows 그룹 정책을 강제로 적용할 수 있는 경우.

이 배포 구성은 다음과 같은 과정으로 진행됩니다:

- 공유 폴더(대상 기기의 LocalSystem 계정에 읽기 권한이 있는 폴더)에 Microsoft Installer 형식의 애플리케이션 배포 패키지(MSI 패키지)를 배치합니다.
- Active Directory 그룹 정책에서 배포 패키지용으로 설치 개체를 만듭니다.
- 대상 기기가 포함되는 조직 구성 단위(OU) 및 / 또는 보안 그룹을 지정하여 설치 범위를 설정합니다.
- 다음 번에 기기 사용자가 시스템에 로그인하기 전에 대상 기기가 도메인에 로그인하면 설치된 모든 애플리케이션에서 필요한 애플리케이션의 유무를 확인합니다. 애플리케이션을 찾을 수 없으면 정책에 지정된 리소스에서 배포 패키지를 다운로드하여 설치합니다.

이 배포 구성의 장점은 운영 체제가 로드되는 중에, 즉 사용자가 시스템에 로그인하기도 전에 할당된 애플리케이션이 대상 기기에 설치된다는 것입니다. 충분한 권한이 있는 사용자가 애플리케이션을 제거하더라도 다음 번에 운영 체제를 시작하면 애플리케이션이 다시 설치됩니다. 이 배포 구성의 단점은 추가 도구를 사용하지 않더라도 기기를 다시 시작할 때까지는 관리자가 그룹 정책에 대해 적용한 변경 사항이 적용되지 않는다는 것입니다.

네트워크 에이전트와 기타 애플리케이션의 개별 설치 관리자가 Windows Installer 형식이라면 그룹 정책을 사용하여 네트워크 에이전트와 기타 애플리케이션을 모두 설치할 수 있습니다.

MSI 패키지에서 네트워크 에이전트 설치는 숨김 모드에서만 가능하며 MSI 패키지를 통한 대화식 설치는 지원하지 않습니다.

게다가 이 배포 방법을 선택하면 Windows 그룹 정책을 적용한 후 기기에 복사할 파일을 가져올 파일 리소스에 대한 부하도 평가해야 합니다. 구성한 설치 패키지를 해당 리소스로 전달할 방법과 설정에서 관련 변경 사항을 동기화할 방법도 선택해야 합니다.

Kaspersky Security Center의 원격 설치 작업을 통해 Microsoft Windows 정책 처리

중앙 관리 서버 기기에서 대상 기기가 포함된 도메인의 컨트롤러에 접근할 수 있으며, 대상 기기에서 설치 패키지가 저장된 중앙 관리 서버의 공유 폴더에 접근하여 폴더의 내용을 읽을 수 있는 경우에만 이 배포 방법을 사용할 수 있습니다. 따라서 MSP에는 이 배포 방법이 적용된다고 간주할 수 없습니다.

Microsoft Windows 정책을 통한 애플리케이션 무지원 설치

관리자는 자신을 대신하여 Windows 그룹 정책에서 설치를 수행하는 데 필요한 개체를 만들 수 있습니다. 이 경우에는 패키지를 독립 실행형 파일 서버에 업로드하고 패키지의 링크를 제공해야 합니다.

가능한 설치 시나리오는 다음과 같습니다:

- 관리자가 설치 패키지를 만들고 관리 콘솔에서 패키지의 속성을 설정합니다. 그런 다음 이 패키지의 전체 EXEC 하위 폴더를 Kaspersky Security Center의 공유 폴더에서 조직의 전용 파일 리소스에 있는 폴더로 복사합니다. 그룹 정책 개체가 조직의 전용 파일 리소스에 있는 하위 폴더에 저장된 이 패키지의 MSI 파일 링크를 제공합니다.

- 관리자가 네트워크 에이전트의 패키지를 포함한 애플리케이션 배포 패키지를 인터넷에서 다운로드하여 조직의 전용 파일 리소스에 업로드합니다. 그룹 정책 개체가 조직의 전용 파일 리소스에 있는 하위 폴더에 저장된 이 패키지의 MSI 파일 링크를 제공합니다. MSI 속성을 구성하거나 MST 변환 파일을 구성하여 설치 설정을 정의합니다.

Kaspersky Security Center의 원격 설치 작업을 통한 강제 배포

네트워크 에이전트나 다른 애플리케이션의 초기 배포 수행을 위해, Kaspersky Security Center의 원격 설치 작업으로 선택한 설치 패키지를 강제 설치할 수 있습니다. 단, 기기마다 로컬 관리자 권한이 있는 사용자 계정이 있어야 합니다.

중앙 관리 서버가 기기에 직접 접근할 수 없을 때도 강제 설치를 적용할 수 있습니다: 기기가 격리된 네트워크에 있거나, 기기는 로컬 네트워크에 있고 중앙 관리 서버 항목은 DMZ에 있을 때를 예로 들 수 있습니다.

초기 배포 시 네트워크 에이전트가 설치되지 않습니다. 따라서 원격 설치 작업의 설정에서 네트워크 에이전트를 사용하여 애플리케이션 설치에 필요한 파일 배포를 선택할 수 없습니다. 중앙 관리 서버나 배포 지점을 통해서만 운영 체제 리소스를 사용하여 파일을 배포할 수 있습니다.

대상 기기에 대한 관리 권한이 있는 계정으로 중앙 관리 서버 서비스를 실행해야 합니다. 또는 원격 설치 작업의 설정에서 admin$ 공유에 접근 권한이 있는 계정을 지정할 수 있습니다.

기본적으로 원격 설치 작업은 중앙 관리 서버를 실행 중인 계정의 자격 증명을 사용하여 기기에 연결합니다. 이는 admin$ 공유 폴더에 접근할 수 있는 계정입니다. 대상 기기에 네트워크 에이전트가 설치되어 있지 않은 경우에만 원격 설치 작업 설정에서 이 계정을 지정해야 합니다.
Linux 기반 장치를 실행할 원격 설치 작업을 생성할 때는 항상 SSH 연결을 생성하기 위한 계정을 반드시 지정해야 합니다.

대상 기기가 속하는 Kaspersky Security Center 관리 그룹을 선택하거나, 특정 기준에 따라 기기 조회를 만들어 목록으로 대상 기기를 명시적으로 지정할 수 있습니다. 설치 시작 시간은 작업 스케줄에 따라 정의됩니다. 작업 속성에서 **누락된 작업 실행** 설정을 활성화하면 대상 기기가 켜진 직후나 대상 관리 그룹으로 이동될 때 작업을 실행할 수 있습니다.

강제 설치 시에는 설치 패키지를 대상 기기로 전달하고, 파일을 각 대상 기기의 admin$ 리소스에 복사하고, 해당 기기에서 지원 서비스를 원격 등록합니다. 네트워크 상호 작용을 수행할 수 있도록 하는 Kaspersky Security Center 기능을 통해 대상 기기로 설치 패키지를 전달합니다. 이 경우 다음 조건이 충족되어야 합니다:

- 대상 기기는 중앙 관리 서버나 배포 지점 측에서 액세스할 수 있습니다.
- 네트워크에서 대상 기기에 대한 이름 해석이 정상 작동합니다.
- 대상 기기에서 관리 공유(admin$)가 작동하는 상태로 유지되어야 합니다.
- 대상 기기에서 다음 시스템 서비스가 실행 중입니다:
  - Server(LanmanServer)
    이 서비스는 기본적으로 실행 중입니다.
  - DCOM Server Process Launcher(DcomLaunch)
  - RPC Endpoint Mapper(RpcEptMapper)
  - Remote Procedure Call(RpcSs)
- Windows 도구를 통한 원격 접근 활성화를 위해 TCP 445 포트가 대상 기기에서 열려 있습니다.

  TCP 139, UDP 137, UDP 138은 이전 프로토콜에서 사용되며, 현재 애플리케이션에서는 이제 필요하지 않습니다.

  중앙 관리 서버와 배포 지점에서 대상 기기로 연결하려면, 방화벽에서 동적 아웃바운드 액세스 포트를 허용해야 합니다.
- 네트워크 에이전트 배포 중 Active Directory 도메인 정책 보안 설정이 NTLM 프로토콜의 동작을 제공할 수 있습니다.
- Microsoft Windows XP를 실행하는 대상 기기에서는 단순 파일 공유 모드를 중지합니다.

- 대상 기기에서, 접근 공유 및 보안 모델은 *클래식(로컬 사용자가 본인으로 인증)*으로 설정됩니다. 이는 *게스트 전용(로컬 유저가 게스트로 인증)*일 수 없습니다.

- 대상 기기가 도메인의 구성원이거나 대상 기기에서 관리자 권한이 있는 통일 계정을 미리 만들어야 합니다.

Windows Server 2003 이상 Active Directory 도메인에 가입되지 않은 기기에 네트워크 에이전트나 기타 애플리케이션을 배포하려면, 해당 기기에서 UAC를 비활성화해야 합니다. 원격 UAC는 로컬 관리 계정이 네트워크 에이전트나 다른 애플리케이션의 강제 배포에 필요한 admin$에 접근하지 못하는 이유 중 하나입니다. 원격 UAC를 중지해도 로컬 UAC에 영향을 주지 않습니다.

아직 Kaspersky Security Center 관리 그룹에 할당되지 않은 새 기기에 설치를 수행하는 중에 원격 설치 작업 속성을 열고 네트워크 에이전트를 설치한 후 기기를 이동할 관리 그룹을 지정할 수 있습니다.

그룹 작업을 만들 때는 각 그룹 작업이 선택한 그룹 내에 중첩된 모든 그룹의 모든 기기에 적용된다는 점을 기억하십시오. 그러므로 하위 그룹에 중복된 설치 작업을 포함하면 안 됩니다.

자동 설치를 활용하면 애플리케이션 강제 설치 작업을 간단히 생성할 수 있습니다. 이렇게 하려면 관리 그룹 속성을 열고 설치 패키지 목록을 연 다음 이 그룹의 기기에 설치해야 하는 패키지를 선택해야 합니다. 그러면 이 그룹과 모든 해당 하위 그룹의 모든 기기에 선택한 설치 패키지가 자동으로 설치됩니다. 패키지가 설치되는 시간 간격은 네트워크 처리 성능과 총 네트워크 연결 기기 개수에 따라 달라집니다.

대상 기기로 설치 패키지를 전달하는 동안 중앙 관리 서버의 부하를 줄이기 위해 설치 작업에서 배포 지점을 통한 설치를 선택할 수 있습니다. 이 설치 방법을 사용하면 배포 지점 역할을 하는 기기의 부하가 크게 증가합니다. 따라서 배포 지점의 요구 사항을 충족하는 기기를 선택하는 것이 좋습니다. 배포 지점을 사용한다면 배포 지점이 대상 기기를 호스팅하는 격리된 각 서브넷에 있는지 확인해야 합니다.

저용량 채널을 통해 중앙 관리 서버와 통신하는 서브넷의 기기에서 설치를 수행할 때 동일 서브넷의 기기 간에 더 광범위한 채널을 사용할 수 있는 경우에도 배포 지점을 로컬 설치 센터로 사용하는 방식이 유용할 수 있습니다.

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 폴더가 있는 파티션의 디스크 여유 공간은 설치되는 애플리케이션의 배포 패키지 총 크기보다 커야 합니다.

Kaspersky Security Center에서 만든 독립 실행형 패키지 실행

앞에서 설명한 네트워크 에이전트 및 기타 애플리케이션의 초기 배포 방법을 항상 구현할 수 있는 것은 아닙니다. 해당하는 모든 조건을 충족할 수는 없기 때문입니다. 이러한 경우에는 설치 패키지와 관리자가 준비한 관련 설치 설정을 함께 사용하여 Kaspersky Security Center를 통해 *독립 실행형 설치 패키지*라는 일반 실행 파일을 만들 수 있습니다. 독립 실행형 설치 패키지는 적절한 경우(대상 기기 사용자를 위해 해당 웹 서버에 대한 외부 접근이 구성됨) Kaspersky Security Center에 포함된 내부 웹 서버에 게시할 수도 있고, Kaspersky Security Center 웹 콘솔에 포함되어 있는 독점 배포된 웹 서버에 게시할 수도 있습니다. 다른 웹 서버에 독립 실행형 패키지를 복사할 수도 있습니다.

Kaspersky Security Center를 통해 현재 웹 서버로 사용되는 독립 실행형 패키지 파일에 대한 링크가 포함된 이메일 메시지를 선택한 사용자에게 전송하여 대화식 모드나 숨김 설치용 "-s" 키를 사용해 파일을 실행하라는 메시지를 표시할 수 있습니다. 독립 실행형 설치 패키지를 이메일 메시지에 첨부한 다음 이 웹 서버에 접근할 수 없는 기기 사용자에게 전송할 수 있습니다. 관리자는 외부 기기에 독립 실행형 패키지를 복사하여 관련 기기로 전송한 다음 나중에 실행할 수도 있습니다.

네트워크 에이전트 패키지나 보안 제품과 같은 기타 애플리케이션의 패키지 중 하나 또는 두 패키지에서 모두 독립 실행형 패키지를 만들 수 있습니다. 네트워크 에이전트와 기타 애플리케이션에서 모두 독립 실행형 패키지를 만든 경우에는 네트워크 에이전트를 사용하여 설치가 시작됩니다.

네트워크 에이전트를 사용하여 독립 실행형 패키지를 만들 때는 새 기기(관리 그룹에 미할당 기기)에서 네트워크 에이전트 설치가 완료되면 해당 기기를 자동으로 이동할 관리 그룹을 지정할 수 있습니다.

독립 실행형 패키지는 대화식 모드(기본값)로 실행하여 패키지에 포함된 애플리케이션의 설치 결과를 표시할 수도 있고, "-s" 키를 사용하여 실행하는 경우 숨김 모드로 실행할 수도 있습니다. 스크립트(예: 운영 체제 이미지를 배포한 후에 실행되도록 구성된 스크립트)에서 설치하려는 경우 숨김 모드를 사용할 수 있습니다. 숨김 모드에서 수행된 설치 결과는 프로세스의 반환 코드를 통해 확인할 수 있습니다.

애플리케이션 수동 설치용 옵션

관리자나 숙련된 사용자는 대화식 모드에서 수동으로 애플리케이션을 설치할 수 있습니다. 이때 원본 배포 패키지를 사용할 수도 있고, 원본 배포 패키지에서 생성되어 Kaspersky Security Center의 공유 폴더에 저장된 설치 패키지를 사용할 수도 있습니다. 기본적으로 설치 관리자는 대화식 모드로 실행되며 사용자에게 필요한 모든 값을 입력하라는 메시지를 표시합니다. 그러나 "-s" 키를 사용하여 설치 패키지 루트에서 setup.exe 프로세스를 실행할 때는 설치 관리자가 설치 패키지를 구성할 때 정의한 설정을 사용하여 숨김 모드로 실행됩니다.

설치 패키지의 루트에서 setup.exe를 실행할 때는 패키지가 먼저 임시 로컬 폴더에 복사된 후에 해당 로컬 폴더에서 애플리케이션 설치 관리자가 실행됩니다.

네트워크 에이전트가 설치된 기기에 애플리케이션 원격 설치

기본 중앙 관리 서버나 해당 보조 서버에 연결된 작동 가능한 네트워크 에이전트가 기기에 설치되어 있으면 해당 기기에서 네트워크 에이전트를 업그레이드할 수 있을 뿐 아니라 네트워크 에이전트를 통해 지원되는 애플리케이션을 설치, 업그레이드 또는 제거할 수도 있습니다.

원격 설치 작업의 속성에서 **네트워크 에이전트 이용** 확인란을 선택하여 이 옵션을 작동시킬 수 있습니다.

이 확인란을 선택하면 관리자가 정의한 설치 설정이 포함된 설치 패키지가 네트워크 에이전트와 중앙 관리 서버 간의 통신 채널을 통해 대상 기기로 전송됩니다.

중앙 관리 서버의 부하를 최적화하고 중앙 관리 서버와 기기 간의 트래픽을 최소화하려는 경우 모든 원격 네트워크 또는 모든 브로드캐스팅 도메인에 배포 지점을 할당하면 유용합니다(배포 지점 정보 및 관리 그룹 구조 작성 및 배포 지점 할당 섹션 참조). 이 경우 설치 패키지와 설치 관리자 설정은 배포 지점을 통해 중앙 관리 서버에서 대상 기기로 배포됩니다.

또한 설치 패키지 브로드캐스팅(멀티캐스트) 전송에 배포 지점을 사용할 수도 있습니다. 이렇게 하면 애플리케이션을 배포할 때 네트워크 트래픽을 크게 줄일 수 있습니다.

네트워크 에이전트와 중앙 관리 서버 간의 통신 채널을 통해 대상 기기로 설치 패키지를 전송할 때는 전송용으로 준비한 모든 설치 패키지가 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer 폴더에도 캐시됩니다. 다양한 유형의 대형 설치 패키지 여러 개를 사용하며 많은 수의 배포 지점을 작업에 포함하는 경우에는 이 폴더의 크기가 매우 커질 수 있습니다.

FTServer 폴더에서 파일을 수동으로 삭제할 수는 없습니다. 원본 설치 패키지를 삭제하면 해당하는 데이터가 FTServer 폴더에서 자동으로 삭제됩니다.

배포 지점 쪽에서 수신된 모든 데이터는 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp 폴더에 저장됩니다.

$FTCITmp 폴더에서 파일을 수동으로 삭제할 수는 없습니다. 이 폴더에서 데이터를 사용하는 작업이 완료되면 이 폴더의 컨텐츠가 자동으로 삭제됩니다.

설치 패키지는 중앙 관리 서버와 네트워크 에이전트 간의 통신 채널을 통해 네트워크 전송에 최적화된 형식으로 중간 저장소에서 배포되므로, 각 설치 패키지의 원래 폴더에 저장된 설치 패키지를 변경할 수는 없습니다. 해당 변경 사항은 중앙 관리 서버를 통해 자동으로 등록되지 않습니다. 설치 패키지의 파일은 수동으로 수정하지 않는 것이 좋지만, 수동으로 수정해야 한다면 관리 콘솔에서 설치 패키지의 설정을 편집해야 합니다. 관리 콘솔에서 설치 패키지의 설정을 편집하면 중앙 관리 서버가 대상 기기로 전송하기 위해 준비했던 캐시의 패키지 이미지를 업데이트합니다.

원격 설치 작업에서 기기 다시 시작 관리

특히 Windows에서는 애플리케이션 원격 설치를 완료하려면 기기를 다시 시작해야 하는 경우가 많습니다.

Kaspersky Security Center의 원격 설치 작업 사용 시, 새 작업 마법사 또는 생성된 작업의 속성 창(**운영 체제 다시 시작** 섹션)에서 Windows 기기를 다시 시작해야 할 때 수행할 작업을 선택할 수 있습니다:

- **기기 다시 시작 안 함**. 이 옵션을 선택하면 자동 다시 시작이 수행되지 않습니다. 설치를 완료하려면 수동으로 다시 시작하거나 기기 관리 작업을 통해야 합니다. 필요한 다시 시작에 대한 정보는 작업 결과와 기기 상태에 저장됩니다. 이 옵션은 무중단 작동이 필요한 서버 및 기타 기기에서 수행하는 설치 작업에 적합합니다.

- **기기 다시 시작**. 이 옵션을 선택하면 설치를 완료하기 위해 기기를 다시 시작해야 하는 경우 기기가 항상 자동으로 다시 시작됩니다. 이 옵션은 동작 시 정기적으로 일시 중지(종료 또는 다시 시작)되는 기기의 설치 작업에 유용합니다.

- **사용자 확인 후 실행**. 이 경우 클라이언트 기기의 화면에 수동으로 기기를 다시 시작할 것인지 묻는 다시 시작 알림이 사용자에게 표시됩니다. 이 옵션의 경우 몇 가지 고급 설정을 정의할 수 있습니다: 이러한 설정은 사용자용 메시지의 문구, 메시지 표시 빈도, 그리고 사용자 확인 없이 기기를 강제로 다시 시작할 때까지의 시간 간격입니다. **사용자 확인 후 처리**는 사용자가 기기를 다시 시작할 가장 편리한 시간을 선택할 수 있어야 하는 워크스테이션에 가장 적합한 옵션입니다.

안티 바이러스 애플리케이션의 설치 패키지에서 데이터베이스를 업데이트하는 작업의 적합성

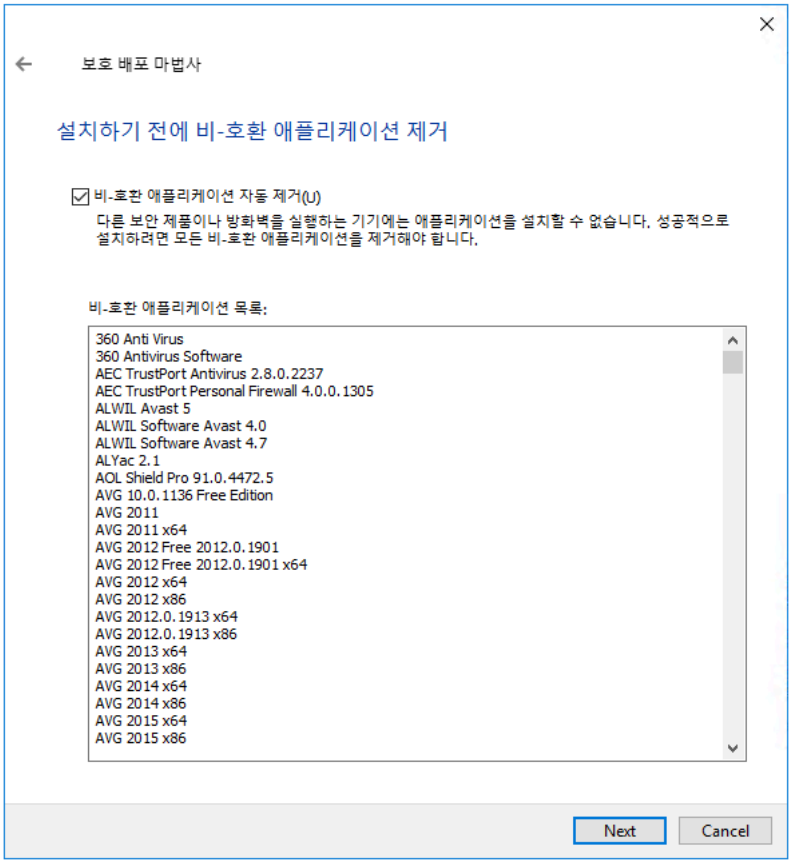
보호 배포를 시작하기 전에 보안 제품 배포 패키지와 함께 제공된 안티 바이러스 데이터베이스(자동 패치 모듈 포함) 업데이트 가능성을 고려해야 합니다. 배포를 시작하기 전에 선택한 설치 패키지의 마우스 오른쪽 메뉴에서 해당하는 명령을 사용하는 등의 방법으로 애플리케이션의 설치 패키지에서 데이터베이스를 업데이트하면 유용합니다. 이렇게 하면 대상 기기에서 보호 배포를 완료하는 데 필요한 다시 시작 횟수를 줄일 수 있습니다. 기본 중앙 관리 서버에서 가상 서버로 전달된 설치 패키지가 원격 설치에 사용되는 경우에는 기본 서버에서 원본 패키지의 데이터베이스만 업데이트하면 됩니다. 이 경우 가상 서버에서 전달된 패키지의 데이터베이스는 업데이트하지 않아도 됩니다.

호환되지 않는 제삼자 보안 애플리케이션 제거

Kaspersky Security Center를 통해 Kaspersky 보안 제품을 설치할 때는 설치하는 애플리케이션과 호환되지 않는 타사 소프트웨어를 제거해야 할 수 있습니다. 기본적으로 두 가지 방식을 통해 타사 애플리케이션을 제거할 수 있습니다.

설치 프로그램을 사용하여 호환되지 않는 애플리케이션 자동 제거

설치 프로그램을 실행하면 Kaspersky 애플리케이션과 호환되지 않는 애플리케이션 목록이 표시됩니다.



원격 설치 마법사에 표시되는 호환되지 않는 애플리케이션 목록

Kaspersky Security Center는 호환되지 않는 소프트웨어를 탐지합니다. 따라서, **비호환 애플리케이션 자동 제거** 확인란을 선택하고 설치를 계속할 수 있습니다. 이 확인란을 선택 해제하고 호환되지 않는 소프트웨어를 제거하지 않으면, 오류가 발생하여 Kaspersky 애플리케이션이 설치되지 않습니다.

다양한 설치 유형을 사용하여 호환되지 않는 애플리케이션을 자동 제거할 수 있습니다.

전용 작업을 통해 비-호환 애플리케이션 제거

호환되지 않는 애플리케이션을 제거하려면 *애플리케이션을 원격으로 제거* 작업을 사용합니다. 이 작업은 보안 제품 설치 작업 전에 기기에서 실행해야 합니다. 예를 들어, 설치 작업에서 **다른 작업 완료 시** 스케줄 유형을 선택할 수 있습니다. 이때, 다른 작업은 *애플리케이션을 원격으로 제거*입니다.

이 제거 방법은 보안 제품 설치 관리자가 비-호환 애플리케이션을 올바르게 제거할 수 없는 경우에 적합합니다.

명령 프롬프트를 사용하여 암호로 보호된 네트워크 에이전트 제거

제거 암호를 설정한 네트워크 에이전트를 원격으로 제거하려면 명령 프롬프트를 사용할 수 있습니다.

Kaspersky Security Center가 더 이상 관리하지 않는 기기에 설치된 암호로 보호되는 네트워크 에이전트의 암호를 분실하거나 잊어버린 경우 klmover 유틸리티, 클리너 도구(cleaner.exe), 명령 프롬프트를 사용하여 네트워크 에이전트를 제거할 수 없습니다. 이 때는 암호로 보호된 네트워크 에이전트가 설치된 기기에 운영 체제를 다시 설치해야 합니다.

명령 프롬프트를 통해 네트워크 에이전트를 제거하려면:

1. 제거 암호를 16진법 코드로 변환합니다.

   인터넷 리소스, 프로그래밍 환경, 텍스트 편집기 또는 기타 적절한 도구를 사용하여 암호를 16진법 코드로 변환합니다.

   생성된 16진법 코드를 여러 부분으로 구분하는 데 사용되는 출력 구분 기호가 `00`으로 설정되었는지 확인합니다. 예를 들어, 16진법 코드 `51 77 65 72 74 79`는 잘못되었으며, 16진법 코드 `510077006500720074007900`가 올바릅니다.

2. 명령 프롬프트에 다음 명령을 입력하고 **ENTER**를 누릅니다:

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   아래 표에서 사용 중인 네트워크 에이전트의 제품 코드를 찾을 수 있습니다.

네트워크 에이전트 제품 코드

현지화	제품 코드
아랍어	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
불가리아어	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
체코어	{478A6A0B-D177-4402-B703-808C05C56B13}
영어	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
프랑스어	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
독일어	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
헝가리어	{8899A4D4-D678-49F8-AD96-0B784F58D355}
이탈리아어	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
일본어	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
한국어	{70812A40-973B-4DA1-96B9-C2011280CD99}
폴란드어	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
포르투갈어	{0F05E4E5-5A89-482C-9A62-47CC58643788}
루마니아어	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
러시아어	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
중국어 간체	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
스페인어	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
스페인어(멕시코)	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}

중국어 번체	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
터키어	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Kaspersky Security Center의 애플리케이션 원격 설치 도구를 사용하여 관리 중인 기기에서 관련 실행 파일 실행

새 패키지 마법사를 사용하면 실행 파일을 선택하고 해당 파일에 대해 명령줄 설정을 정의할 수 있습니다. 이를 위해 선택한 파일 자체나 해당 파일이 저장된 전체 폴더를 설치 패키지에 추가할 수 있습니다. 그런 후에는 원격 설치 작업을 만들고 작성된 설치 패키지를 선택해야 합니다.

작업이 실행되는 동안 명령 프롬프트의 정의된 설정을 포함하는 지정된 실행 파일이 대상 기기에서 실행됩니다.

Microsoft Windows Installer(MSI) 형식의 설치 관리자를 사용하는 경우 Kaspersky Security Center에서 표준 도구를 통해 설치 결과를 분석합니다.

취약점 및 패치 관리 라이센스를 사용할 수 있는 경우에는 기업 환경에서 지원되는 애플리케이션용 설치 패키지를 만들 때 Kaspersky Security Center가 업데이트 가능 데이터베이스에 포함되어 있는 설치 결과 분석 내용과 설치를 위한 규칙도 사용합니다.

그렇지 않은 경우 실행 파일에 대한 기본 작업은 실행 중인 프로세스 및 모든 자식 프로세스가 완료될 때까지 대기합니다. 실행 중인 프로세스가 모두 완료되고 나면 초기 프로세스의 반환 코드에 관계없이 작업이 정상적으로 완료됩니다. 이 작업의 해당 동작을 변경하려면 작업을 만들기 전에 Kaspersky Security Center가 새로 작성된 설치 패키지의 폴더 및 하위 폴더에 생성한 .kud 파일을 수동으로 수정해야 합니다.

.kpd 파일은 ASCII 인코딩을 사용합니다. .kud 파일은 유니코드 인코딩을 사용합니다.

작업이 실행 중인 프로세스가 완료될 때까지 대기하지 않도록 하려면 [SetupProcessResult] 섹션에서 Wait 설정의 값을 0으로 설정합니다:

```
[SetupProcessResult]
Wait=0
```

작업이 Windows에서 실행 중인 프로세스만 완료될 때까지 대기하고 모든 자식 프로세스가 완료되기를 대기하지는 않도록 하려면 다음과 같이 [SetupProcessResult] 섹션에서 WaitJob 설정의 값을 0으로 설정합니다:

```
[SetupProcessResult]
WaitJob=0
```

작업이 완료되거나 실행 중인 프로세스의 반환 코드에 따라 오류를 반환하도록 하려면, 다음과 같이 오류 코드를 파일에 저장하는 실행 가능한 .bat 파일을 만듭니다.

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

그런 다음 새로 만든 설치 패키지의 폴더에 있는 Kaspersky Security Center가 생성한 .kud 파일을 수정합니다.

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
```

```
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

이 경우에는 목록에 포함된 코드 이외의 코드가 반환되면 오류가 반환됩니다.

작업 정상 완료 또는 오류에 대한 주석이 포함된 문자열을 작업 결과에 표시하려면 다음과 같이 [SetupProcessResult_SuccessCodes] 및 [SetupProcessResult_ErrorCodes] 섹션에 프로세스 반환 코드에 해당하는 오류의 간단한 설명을 입력합니다:

```
[SetupProcessResult_SuccessCodes]
0= Installation completed successfully
3010=A restart is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation canceled by the user
1603=Fatal error during installation
```

작업 완료를 위해 기기를 다시 시작해야 하는 경우 Kaspersky Security Center 도구를 사용하여 기기 다시 시작을 관리하려면 다시 시작을 수행해야 함을 나타내는 프로세스의 반환 코드를 [SetupProcessResult_NeedReboot] 섹션에 포함합니다:

```
[SetupProcessResult_NeedReboot]
3010=
```

배포 모니터링

Kaspersky Security Center 배포를 모니터링하고 보안 제품과 네트워크 에이전트가 관리 중인 기기에 설치되었는지 확인하려면 **배포** 섹션의 표시등을 확인해야 합니다. 이 표시등은 관리 콘솔 기본 창의 중앙 관리 서버 노드 작업 영역에 있습니다. 표시등은 현재 배포 상태를 반영합니다. 네트워크 에이전트와 보안 제품이 설치된 기기의 수가 표시등 옆에 표시됩니다. 실행 중인 설치 작업이 있으면 여기서 해당 진행률을 모니터링할 수 있습니다. 설치 오류 발생 시에는 오류 수가 여기에 표시됩니다. 링크를 클릭하여 오류의 세부 정보를 확인할 수 있습니다.

그룹 탭에서 **관리 중인 기기** 폴더 작업 영역에 있는 배포 스키마를 사용할 수도 있습니다. 이 차트에는 배포 프로세스가 반영되어 네트워크 에이전트가 설치된/설치되지 않은 기기 또는 네트워크 에이전트와 보안 제품이 모두 설치된 기기의 수가 표시됩니다.

배포 진행률이나 특정 설치 작업의 동작에 대한 추가 세부 사항을 확인하려면 관련 원격 설치 작업의 결과 창을 엽니다: 작업을 오른쪽 클릭하고 마우스 오른쪽 메뉴에서 **결과**를 선택합니다. 그러면 창에 두 개의 목록이 표시됩니다: 위쪽 목록에는 기기의 작업 상태가 포함되어 있고, 아래쪽 목록에는 현재 위쪽 목록에서 선택한 기기의 작업 이벤트가 포함되어 있습니다.

배포 오류에 대한 정보는 중앙 관리 서버의 Kaspersky 이벤트 로그에 추가됩니다. **리포트 및 알림** 폴더의 **이벤트** 하위 폴더에서 해당 이벤트를 선택해도 오류 정보가 제공됩니다.

설치 관리자 구성

이 섹션에서는 Kaspersky Security Center 설치 관리자의 파일과 설치 설정에 대한 정보, 그리고 중앙 관리 서버 및 네트워크 에이전트를 숨김 모드로 설치하기 위한 권장 방법을 제공합니다.

일반 정보

Kaspersky Security Center 15.1의 구성 요소(중앙 관리 서버, 네트워크 에이전트, 관리 콘솔) 설치 관리자는 Windows Installer 기술을 기반으로 작성되었습니다. 설치 관리자의 핵심 요소는 MSI 패키지입니다. 이 패키징 형식에서는 Windows Installer에서 제공하는 모든 이점: 확장성, 패칭 시스템 사용 가능성, 변환 시스템, 타사 솔루션을 통한 중앙 집중식 설치, 운영 체제에 대한 자동 등록 등을 사용할 수 있습니다.

숨김 모드로 설치 (응답 파일 사용)

중앙 관리 서버 및 네트워크 에이전트의 설치 관리자에는 응답 파일(ss_install.xml) 사용 기능이 포함되어 있습니다. 이 파일에는 사용자의 작업 없이 숨김 모드로 설치를 수행하기 위한 파라미터가 통합되어 있습니다. ss_install.xml 파일은 MSI 패키지와 같은 폴더에 있습니다; 숨김 모드로 설치하는 동안 이 파일이 자동으로 사용됩니다. 명령줄 키 "/s"로 숨김 설치 모드를 활성화할 수 있습니다.

실행 방법의 대략적인 예는 다음과 같습니다:

```
setup.exe /s
```

> 숨김 모드에서 설치 프로그램을 시작하기 전에 EULA(최종 사용자 라이센스 계약서)를 읽어 보십시오. Kaspersky Security Center 배포 키트에 EULA 텍스트가 있는 TXT 파일이 없다면 Kaspersky 웹사이트 에서 다운로드할 수 있습니다.

ss_install.xml 파일은 Kaspersky Security Center 설치 관리자 파라미터의 내부 형식 인스턴스입니다. 배포 패키지에는 기본 파라미터가 들어 있는 ss_install.xml 파일이 포함됩니다.

> ss_install.xml 파일을 수동으로 수정하지 마십시오. 관리 콘솔에서 설치 패키지의 파라미터를 편집할 때 Kaspersky Security Center의 도구를 통해 이 파일을 수정할 수 있습니다.

중앙 관리 서버 설치를 위한 응답 파일을 수정하려면:

1. Kaspersky Security Center 배포 패키지를 엽니다. 전체 패키지 EXE 파일 사용 시, 압축을 풉니다.
2. Server 폴더에서 명령줄을 열고 다음 명령을 실행합니다:

   ```
   setup.exe /r ss_install.xml
   ```

   Kaspersky Security Center 설치 프로그램이 시작됩니다.
3. 마법사의 단계를 따라 Kaspersky Security Center 설치를 구성하십시오.

   마법사를 완료하면 지정한 새 설정에 따라 응답 파일이 자동으로 수정됩니다.

숨김 모드로 네트워크 에이전트 설치(응답 파일 사용 안 함)

표준 방식으로 MSI 속성 값을 지정하여 단일 msi 패키지를 사용해 네트워크 에이전트를 설치할 수 있습니다. 이 경우 그룹 정책을 사용하여 네트워크 에이전트를 설치할 수 있습니다.

설치 패키지 Kaspersky Network Agent.msi의 이름을 바꾸지 마십시오. 이 패키지 이름을 바꾸면 네트워크 에이전트의 향후 업데이트 시 설치 오류가 발생할 수 있습니다.

응답 파일에 정의된 파라미터와 MSI 속성을 통해 정의하는 파라미터 간의 충돌을 방지하려는 경우 `DONT_USE_ANSWER_FILE=1` 속성을 설정하여 응답 파일을 중지할 수 있습니다. MSI 파일은 Kaspersky Security Center 배포 패키지의 Packages\NetAgent\exec 폴더에 있습니다. msi 패키지를 사용하여 네트워크 에이전트 설치 관리자를 실행하는 방식의 예는 다음과 같습니다.

숨김 모드에서 네트워크 에이전트를 설치하려면 최종 사용자 라이센스 계약서의 조항에 동의해야 합니다. 최종 사용자 라이센스 계약서의 조항을 모두 읽고 이해했으며, 이에 동의하는 경우에만 `EULA=1` 파라미터를 사용하십시오.

```
예:
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

응답 파일(확장자가 mst인 파일)을 미리 준비하여 msi 패키지의 파라미터 설정을 정의할 수도 있습니다. 이 명령은 다음과 같이 표시됩니다:

```
예:
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

단일 명령에서 여러 응답 파일을 지정할 수 있습니다.

Windows 설치 프로그램을 사용하여 네트워크 에이전트를 업그레이드하려면 다음 명령을 실행하십시오.

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

setup.exe를 통한 부분 설치 구성

setup.exe를 통해 애플리케이션 설치를 실행할 때는 MSI의 모든 속성 값을 MSI 패키지에 추가할 수 있습니다.

이 명령은 다음과 같이 표시됩니다:

```
예:
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

중앙 관리 서버 설치 파라미터

아래 표에는 중앙 관리 서버를 설치할 때 구성할 수 있는 MSI 속성에 대한 설명이 나와 있습니다. EULA 및 PRIVACYPOLICY를 제외한 모든 파라미터는 선택 사항입니다.

MSI 속성	설명	사용 가능한 값
EULA	라이센스 계약서 조건에 동의(필수)	• 1 – 최종 사용자 라이센스 계약서의 조건을 모두 읽고 이해했으며, 이에 동의합니다. • 다른 값 및 값 없음 – 라이센스 계약서 조건에 동의하지 않음(설치가 수행되지 않음).
PRIVACYPOLICY	개인정보취급방침 조건에 동의(필수)	• 1 – 개인정보취급방침에 설명된 대로 제 데이터가 처리되고 전송(제3국으로의 전송 포함)되는 것을 알고 있으며 이에 동의합니다. 개인정보취급방침을 모두 읽고 이해했음을 확인합니다. • 다른 값 및 값 없음 - 개인정보취급방침 조건에 동의하지 않음(설치가 수행되지 않음).
INSTALLATIONMODETYPE	중앙 관리 서버 설치 유형	• 표준 • 사용자 지정
INSTALLDIR	애플리케이션 설치 폴더	문자열 값.
ADDLOCAL	쉼표로 구분된 설치할 구성 요소 목록	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. 중앙 관리 서버를 적절히 설치하기 위한 최소한의 구성 요소 목록: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	네트워크 크기	• NRT_1_100—1대 ~ 100대. • NRT_100_1000—101~1000대. • NRT_GREATER_1000 - 기기 1000대 초과.
SRV_ACCOUNT_TYPE	중앙 관리 서버 서비스 동작을 위한 사용자를 지정하는 방식	• SrvAccountDefault – 사용자 계정이 자동으로 만들어짐. • SrvAccountUser - 사용자 계정을 수동으로 정의함.
SERVERACCOUNTNAME	서비스의 사용자 이름	문자열 값.
SERVERACCOUNTPWD	서비스의 사용자 암호	문자열 값.
DBTYPE	데이터베이스 유형	• MySQL – MySQL 또는 MariaDB 데이터베이스가 사용됩니다. • MSSQL – Microsoft SQL Server(SQL Express) 데이터베이스가 사용됩니다.
MYSQLSERVERNAME	MySQL 또는 MariaDB 서버의 전체 이름	문자열 값.
MYSQLSERVERPORT	MySQL 또는 MariaDB 서버에 연결할 포트 번호	숫자 값.
MYSQLDBNAME	MySQL 또는 MariaDB 서버 데이터베이스의 이름	문자열 값.
MYSQLACCOUNTNAME	MySQL 또는 MariaDB 서버 데이터베이스 연결을 위한 사용자 이름	문자열 값.
MYSQLACCOUNTPWD	MySQL 또는 MariaDB 서버 데이터베이스 연결을 위한 사용자 암호	문자열 값.
MSSQLCONNECTIONTYPE	MSSQL 데이터베이스의 사용 유형	• InstallMSSEE – 패키지에서 설치 • ChooseExisting – 설치된 서버 사용
MSSQLSERVERNAME	SQL Server 인스턴스의 전체 이름	문자열 값.
MSSQLDBNAME	SQL Server 데이터베이스의 이름	문자열 값.
MSSQLAUTHTYPE	SQL Server 연결을 위한 인증 방법	• Windows • SQLServer
MSSQLACCOUNTNAME	SQLServer 모드에서 SQL Server에 연결하기 위한 사용자 이름	문자열 값.
MSSQLACCOUNTPWD	SQLServer 모드에서 SQL Server에 연결하기 위한 사용자 암호	문자열 값.

CREATE_SHARE_TYPE	공유 폴더를 지정하는 방법	• Create - 새 공유 폴더 만들기. 이 경우 다음 속성을 정의해야 합니다:
		  • SHARELOCALPATH – 로컬 폴더의 경로
		  • SHAREFOLDERNAME – 폴더의 네트워크 이름
		• Null – EXISTSHAREFOLDERNAME 속성이 지정되어야 함

MSI 속성	설명	사용 가능한 값
EXISTSHAREFOLDERNAME	기존 공유 폴더의 전체 경로	문자열 값.
SERVERPORT	중앙 관리 서버에 연결할 포트 번호입니다	숫자 값.
SERVERSSLPORT	SSL을 이용해 중앙 관리 서버에 연결할 경우의 포트 번호	숫자 값.
SERVERADDRESS	중앙 관리 서버 주소	문자열 값.
SERVERCERT2048BITS	중앙 관리 서버 인증서용 키 길이(비트)	• 1 – 중앙 관리 서버 인증서용 키 길이는 2048비트입니다. • 0 – 중앙 관리 서버 인증서용 키 길이는 1024비트입니다. • 값이 지정되지 않았다면 중앙 관리 서버 인증서용 키 크기는 2048비트입니다.
MOBILESERVERADDRESS	모바일 기기 연결을 위한 중앙 관리 서버의 주소; MobileSupport 구성 요소를 선택하지 않은 경우 무시됨	문자열 값.

네트워크 에이전트 설치 설정

아래 표에는 네트워크 에이전트를 설치할 때 구성할 수 있는 MSI 속성에 대한 설명이 나와 있습니다. SERVERADDRESS를 제외한 모든 파라미터는 선택 사항입니다.

MSI 속성

MSI 속성	설명	사용 가능한 값
DONT_USE_ANSWER_FILE	응답 파일에서 설치 파라미터 읽기	• 1 • 값 없음
INSTALLDIR	설치 폴더	
SERVERADDRESS	중앙 관리 서버 주소 (필수)	
SERVERPORT	중앙 관리 서버에 연결할 포트 수	
SERVERSSLPORT	SSL 연결 포트 번호	
USESSL	SSL 연결을 사용할지 여부	• 1 • 값 없음
OPENUDPPORT	UDP 포트를 열지 여부	• 1 • 값 없음
UDPPORT	UDP 포트 번호	
USEPROXY	프록시 서버를 사용할지 여부	• 1 • 값 없음
PROXYADDRESS	프록시 주소	
PROXYPORT	중앙 관리 서버에 연결할 포트 수	
PROXYLOGIN	프록시 서버에 연결할 계정	
PROXYPASSWORD	프록시 서버에 연결할 계정 암호. 설치 패키지 파라미터에서 권한 있는 사용자 계정의 세부정보를 입력하지 마십시오.	
GATEWAYMODE	연결 게이트웨이 사용 모드	• 0 - 연결 게이트웨이 사용 안 함 • 1 - 이 네트워크 에이전트를 연결 게이트웨이로 사용 • 2 - 연결 게이트웨이를 통해 중앙 관리 서버에 연결
GATEWAYADDRESS	연결 게이트웨이 주소	
CERTSELECTION	인증서를 받는 방법	• GetOnFirstConnection - 중앙 관리 서버에서 인증서 수신. • GetExistent - 기존 인증서를 선택합니다. 이 옵션을 선택하면 CERTFILE 속성을 정의해야 합니다.

MSI 속성	설명	사용 가능한 값
CERTFILE	인증서 파일 경로	
VMVDI	VDI에 대해 동적 모드 사용	• 1 • 값 없음
LAUNCHPROGRAM	설치 완료 후 네트워크 에이전트 서비스 실행 여부	• 1 • 값 없음

가상 인프라

Kaspersky Security Center는 가상 컴퓨터 사용을 지원합니다. 각 가상 머신에 네트워크 에이전트 및 보안 제품을 설치할 수 있으며 하이퍼바이저 수준에서 가상 머신을 보호할 수도 있습니다. 첫 번째 경우 표준 보안 애플리케이션이나 Kaspersky Security for Virtualization Light Agent를 사용하여 가상 머신을 보호할 수 있습니다. 두 번째 경우에는 Kaspersky Security for Virtualization Agentless를 사용할 수 있습니다.

Kaspersky Security Center는 가상 머신을 이전 상태로 롤백할 수 있습니다.

가상 컴퓨터 부하를 줄이기 위한 팁

가상 컴퓨터에 네트워크 에이전트를 설치할 때는 가상 컴퓨터에 거의 사용되지 않을 것으로 보이는 일부 Kaspersky Security Center 기능을 중지하는 것이 좋습니다.

가상 컴퓨터 또는 가상 컴퓨터 생성용 템플릿에 네트워크 에이전트를 설치할 때는 다음 작업이 권장됩니다.

- 원격 설치를 실행하는 경우 네트워크 에이전트 설치 패키지의 속성 창에 있는 **고급** 섹션에서 **VDI 설정 최적화** 옵션을 선택합니다.
- 마법사를 통해 대화형 설치를 실행할 시, 마법사 창에서 **가상 인프라를 위해 네트워크 에이전트 설정 최적화** 옵션을 선택합니다.

이러한 옵션을 선택하면 네트워크 에이전트의 설정이 변경되어 정책을 적용하기 전까지는 다음 기능이 기본적으로 비활성화된 상태로 유지됩니다.

- 설치된 소프트웨어에 대한 정보 가져오기
- 하드웨어에 대한 정보 가져오기
- 탐지된 취약점에 대한 정보 가져오기
- 요구되는 업데이트에 대한 정보 가져오기

이러한 기능은 통합 소프트웨어 및 가상 하드웨어를 사용하므로 대개 가상 컴퓨터에서 필요하지 않습니다.

기능 중지는 취소가 가능합니다. 중지한 기능이 필요한 경우 네트워크 에이전트의 정책이나 네트워크 에이전트 로컬 설정을 통해 기능을 작동시킬 수 있습니다. 네트워크 에이전트의 로컬 설정은 관리 콘솔에서 관련 기기의 마우스 오른쪽 메뉴를 통해 제공됩니다.

동적 가상 컴퓨터 지원

Kaspersky Security Center는 동적 가상 컴퓨터를 지원합니다. 조직 네트워크에 가상 인프라가 배포되었다면 특정한 경우에 동적(임시) 가상 컴퓨터를 사용할 수 있습니다. 동적 VM은 관리자가 준비한 템플릿에 따라 고유한 이름으로 작성됩니다. 사용자가 필요한 시간 동안 VM에서 작업을 한 후 VM을 끄면 가상 인프라에서 해당 가상 컴퓨터가 제거됩니다. 조직 네트워크에 Kaspersky Security Center를 배포한 경우에는 네트워크 에이전트가 설치된 가상 컴퓨터가 중앙 관리 서버 데이터베이스에 추가됩니다. 가상 컴퓨터를 끈 후에는 중앙 관리 서버의 데이터베이스에서도 해당 항목을 제거해야 합니다.

가상 컴퓨터에서 항목 자동 제거 기능이 작동하도록 하려면 동적 가상 컴퓨터용 템플릿에 네트워크 에이전트를 설치할 때 **VDI에 대해 동적 모드 사용** 옵션을 선택합니다:

- 원격 설치 시: 네트워크 에이전트 설치 패키지의 속성 창(**고급** 섹션)
- 대화형 설치 시 - 네트워크 에이전트 설치 마법사

실제 기기에 네트워크 에이전트를 설치할 때는 **VDI에 대해 동적 모드 사용** 옵션을 선택하지 마십시오.

동적 가상 컴퓨터를 제거한 후 일정 시간 동안 중앙 관리 서버에 해당 가상 컴퓨터의 이벤트를 저장하려는 경우 중앙 관리 서버 속성 창의 **이벤트 저장소** 섹션에서 **기기가 삭제된 후 이벤트 저장** 옵션을 선택하고 이벤트의 최대 저장 기간을 일 단위로 지정합니다.

동적 가상 컴퓨터에서는 드라이브 암호화를 활성화하지 않는 것이 좋습니다.

가상 컴퓨터 복사 지원

네트워크 에이전트가 설치된 가상 컴퓨터를 복사하거나 네트워크 에이전트가 설치된 템플릿에서 가상 컴퓨터를 만드는 작업은 하드 드라이브 이미지를 캡처 및 복사하여 네트워크 에이전트를 배포하는 작업과 동일합니다. 대부분의 경우 가상 컴퓨터를 복사할 때 디스크 이미지 복사를 통해 네트워크 에이전트를 배포하는 경우와 동일한 단계를 수행해야 합니다.

그러나 아래의 두 가지 경우에서는 복사를 자동으로 탐지하는 네트워크 에이전트에 대해 설명합니다. 위에서 설명한 이유로 인해 "기기의 하드 드라이브 캡처 및 복사를 통한 배포"에서 설명하는 복잡한 작업은 수행하지 않아도 됩니다:

- 네트워크 에이전트를 설치할 때 **VDI에 대해 동적 모드 사용** 옵션을 선택함: 운영 체제를 다시 시작할 때마다 이 가상 컴퓨터가 복사되었는지 여부에 관계없이 새 기기로 인식됩니다.
- 다음 하이퍼바이저 중 하나를 사용 중임: VMware™, HyperV® 또는 Xen®: 네트워크 에이전트가 가상 하드웨어의 변경된 ID를 기준으로 가상 컴퓨터 복사를 탐지합니다.

가상 하드웨어의 변경 사항 분석 정보 신뢰도가 아주 높은 것은 아닙니다. 이 방법을 광범위하게 적용하기 전에 소규모 가상 컴퓨터 풀에서 현재 조직에서 사용되는 하이퍼바이저 버전에 대해 이 방법을 테스트해야 합니다.

네트워크 에이전트가 설치된 기기의 파일 시스템 롤백 지원

Kaspersky Security Center는 배포 방식 애플리케이션입니다. 네트워크 에이전트가 설치된 기기에서 파일 시스템을 이전 상태로 롤백하면 데이터 동기화가 해제되며 Kaspersky Security Center가 잘못된 방식으로 작동하게 됩니다.

다음과 같은 경우 파일 시스템 또는 파일 시스템의 일부분을 롤백할 수 있습니다:

- 하드 드라이브의 이미지를 복사할 때.
- 가상 인프라를 통해 가상 컴퓨터 상태를 복원할 때.
- 백업 복사본 또는 복구 지점에서 데이터를 복원할 때.

네트워크 에이전트가 설치된 기기의 타사 소프트웨어가 the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 폴더에 영향을 주는 시나리오는 Kaspersky Security Center의 심각한 시나리오뿐입니다. 그러므로 가능하면 항상 복구 절차에서 이 폴더를 제외해야 합니다.

일부 조직의 업무 규칙에서는 기기의 파일 시스템을 롤백하는 기능을 제공하기 때문에 Kaspersky Security Center 10 Maintenance Release 1부터는 네트워크 에이전트가 설치된 기기의 파일 시스템 롤백 지원이 추가되었습니다. 이 경우 중앙 관리 서버와 네트워크 에이전트가 버전 10 Maintenance Release 1 이상이어야 합니다. 이러한 기기는 탐지되는 경우 중앙 관리 서버에 자동으로 다시 연결되며 전체 데이터 정리 및 전체 동기화가 수행됩니다.

기본적으로 Kaspersky Security Center 15.1에서는 파일 시스템 롤백 탐지 지원이 활성화되어 있습니다.

네트워크 에이전트가 설치된 기기의 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ 폴더는 가급적 롤백하지 않아야 합니다. 데이터의 전체 다시 동기화를 수행하려면 리소스가 많이 필요하기 때문입니다.

중앙 관리 서버가 설치된 기기에서는 시스템 상태를 절대 롤백해서는 안 됩니다. 중앙 관리 서버에서 사용하는 데이터베이스도 롤백하면 안 됩니다.

표준 klbackup 유틸리티를 통해서만 백업 복사본에서 중앙 관리 서버 상태를 복원할 수 있습니다.

이동 사용자를 위한 연결 프로필 정보

노트북(이하 "기기"로 지칭함)의 이동 사용자는 기업 네트워크의 기기 현재 위치에 따라 중앙 관리 서버 간을 전환하거나 중앙 관리 서버에 연결하는 방법을 변경해야 할 수 있습니다.

연결 프로필은 Windows 및 macOS를 실행 중인 기기에서만 지원됩니다.

단일 중앙 관리 서버의 여러 주소 사용

네트워크 에이전트가 설치된 기기는 조직의 인트라넷이나 인터넷에서 중앙 관리 서버에 연결할 수 있습니다. 이러한 상황에서는 네트워크 에이전트가 중앙 관리 서버에 연결하는 데 다른 주소를 사용해야 할 수 있습니다. 인터넷 연결에는 외부 중앙 관리 서버 주소를 사용하고, 내부 네트워크 연결에는 내부 중앙 관리 서버 주소를 사용할 수 있습니다.

이처럼 여러 중앙 관리 서버 주소를 사용하려면 인터넷에서 중앙 관리 서버에 연결하는 데 사용할 프로필을 네트워크 에이전트 정책에 추가해야 합니다. 정책 속성(**연결** 섹션, **연결 프로필** 하위 섹션)에서 프로필을 추가합니다. 프로필 만들기 창에서 **지정한 서버에서 업데이트만 다운로드** 옵션을 비활성화하고 **이 프로필에 지정된 중앙 관리 서버 설정과 연결 설정을 동기화** 옵션을 선택해야 합니다. 중앙 관리 서버에 접속할 때 연결 게이트웨이를 사용한다면(예, 인터넷 접속: 연결 게이트웨이로 DMZ에 있는 네트워크 에이전트에서 설명되어 있는 Kaspersky Security Center 구성), 해당 연결 프로필의 관련 필드에서 연결 게이트웨이 주소를 지정해야 합니다.

현재 네트워크에 따라 중앙 관리 서버 간 전환

조직이 각기 다른 중앙 관리 서버를 사용하는 여러 사무소를 운영하며 네트워크 에이전트가 설치된 기기 중 일부를 해당 사무소 간에 이동하는 경우에는 현재 기기가 있는 사무소 내 로컬 네트워크의 중앙 관리 서버에 네트워크 에이전트를 연결해야 합니다.

이 경우 원래 홈 중앙 관리 서버가 있는 본사 사무소를 제외한 각 사무소에 대해 네트워크 에이전트 정책의 속성에서 중앙 관리 서버 연결용 프로필을 만들어야 합니다. 연결 프로필에서 중앙 관리 서버 주소를 지정해야 하며 **지정한 서버에서 업데이트만 다운로드** 옵션을 활성화 또는 비활성화해야 합니다.

- 로컬 서버는 업데이트 다운로드용으로만 사용하고 홈 중앙 관리 서버와 네트워크 에이전트를 동기화해야 하는 경우 옵션을 선택합니다.
- 로컬 중앙 관리 서버를 통해서만 네트워크 에이전트를 관리해야 하는 경우 이 옵션을 비활성화합니다.

그 후에는 새로 만든 프로필로 전환할 조건을 설정해야 합니다: 본사 사무소를 제외한 각 사무소에 대해 조건을 하나 이상 설정합니다. 모든 조건은 사무소의 네트워크 환경과 관련된 항목을 탐지하는 데 사용됩니다. 조건이 참이면 해당 프로필이 활성화됩니다. 참인 조건이 없으면 네트워크 에이전트가 홈 중앙 관리 서버로 전환됩니다.

모바일 기기 관리 기능 배포

이 섹션에서는 모바일 기기 관리 기능의 초기 배포에 관한 정보를 제공합니다.

KES 기기를 중앙 관리 서버에 연결

중앙 관리 서버에 기기를 연결하는 데 사용하는 방법에 따라 KES 기기용 Kaspersky Device Management for iOS에 대해 두 가지 배포 구성을 사용할 수 있습니다:

- 기기를 중앙 관리 서버에 직접 연결하는 배포 구성
- Kerberos 제한 위임을 지원하는 역방향 프록시와 관련된 배포 방식

중앙 관리 서버에 기기 직접 연결

KES 기기는 중앙 관리 서버의 포트 13292에 직접 연결할 수 있습니다.

인증에 사용하는 방법에 따라 두 가지 옵션을 통해 중앙 관리 서버에 KES 기기를 연결할 수 있습니다:

- 사용자 인증서를 사용하여 기기 연결
- 사용자 인증서 없이 기기 연결

사용자 인증서를 사용하여 기기 연결

사용자 인증서를 사용하여 연결하는 기기는 중앙 관리 서버 도구를 통하여 해당 인증서가 할당된 사용자 계정과 연결됩니다.

이 경우 양방향 SSL 인증(상호 인증)이 사용됩니다. 중앙 관리 서버와 기기가 모두 인증서를 통해 인증됩니다.

사용자 인증서 없이 기기 연결

사용자 인증서 없이 연결하는 기기는 중앙 관리 서버의 사용자 계정과 연결되지 않습니다. 그러나 기기는 인증서를 수신하면 중앙 관리 서버 도구를 통하여 해당 인증서가 할당된 사용자와 연결됩니다.

해당 기기를 중앙 관리 서버에 연결할 때는 단방향 SSL 인증이 적용되므로, 중앙 관리 서버만 인증서를 통해 인증됩니다. 기기가 사용자 인증서를 가져오면 인증 유형이 양방향 SSL 인증 (상호 인증)으로 변경됩니다.

Kerberos 제한 위임(KCD)을 사용하는 서버에 KES 기기를 연결하기 위한 구성

Kerberos 제한 위임(KCD)을 사용하는 중앙 관리 서버에 KES 기기를 연결하기 위한 구성에서는 다음 기능이 제공됩니다:

- KCD를 지원하는 역방향 프록시와 통합.
- 모바일 기기 인증에 Kerberos 제한 위임(이하 KCD로 지칭함)을 사용하는 기능.
- 사용자 인증서를 적용하기 위해 공개키 인프라(이하 PKI로 지칭함)와 통합하는 기능.

이 연결 구성을 사용할 때는 다음 사항을 참고하십시오:

- 역방향 프록시에 대한 KES 기기 연결 유형은 "양방향 SSL 인증"이어야 합니다. 즉, 기기가 관련 사용자 인증서를 통해 역방향 프록시에 연결해야 합니다. 기기가 이와 같이 연결되도록 하려면 기기에 설치된 Kaspersky Endpoint Security for Android의 설치 패키지에 사용자 인증서를 통합해야 합니다. 이 KES 패키지는 이 기기(사용자) 전용으로 중앙 관리 서버에서 만든 것이어야 합니다.
- 모바일 프로토콜용 기본 서버 인증서 대신 특수(사용자 지정) 인증서를 지정해야 합니다:
  1. 중앙 관리 서버 속성 창의 **설정** 섹션에서 **모바일 기기용 포트 열기** 확인란을 선택하고 드롭다운 목록에서 **인증서 추가**를 선택합니다.
  2. 열리는 창에서 모바일 프로토콜에 대한 액세스 포인트를 중앙 관리 서버에 게시할 때 역방향 프록시에서 설정한 것과 같은 인증서를 지정합니다.
- 도메인의 인증 기관(CA)에서 KES 기기용 사용자 인증서를 발급해야 합니다. 도메인에 루트 CA가 여러 개 포함되어 있으면 역방향 프록시에서 게시할 때 설정했던 CA에서 사용자 인증서를 발급해야 합니다.

  다음 방법 중 하나를 사용하여 사용자 인증서가 위에서 설명한 요구 사항을 준수함을 확인할 수 있습니다:

  - 새 패키지 마법사와 인증서 설치 마법사에서 특수 사용자 인증서를 지정합니다.
  - 중앙 관리 서버를 도메인 PKI와 통합하고 인증서 발급을 위한 규칙에서 해당하는 설정을 정의합니다:
    1. 콘솔 트리에서 **모바일 기기 관리** 폴더를 확장하고 **인증서** 하위 폴더를 선택합니다.
    2. **인증서** 폴더의 작업 영역에서 **인증서 발급 규칙 구성** 버튼을 눌러 **인증서 발급 규칙** 창을 엽니다.

3. **PKI와 통합** 섹션에서 공개키 인프라와의 통합을 구성합니다.

4. **모바일 인증서 발급** 섹션에서 인증서의 소스를 지정합니다.

아래에는 다음 사항을 가정하고 Kerberos 제한 위임(KCD)을 설정하는 과정의 예가 나와 있습니다:

- 중앙 관리 서버의 모바일 프로토콜에 대한 액세스 포인트가 13292 포트로 설정되어 있음.
- 역방향 프록시가 있는 기기의 이름은 firewall.mydom.local입니다.
- 중앙 관리 서버가 설치된 기기의 이름은 ksc.mydom.local임.
- 모바일 프로토콜에 대한 액세스 포인트의 외부 게시 이름은 kes4mob.mydom.global임.

중앙 관리 서버용 도메인 계정

중앙 관리 서버를 실행할 도메인 계정(예: KSCMobileSrvcUsr)을 만들어야 합니다. 중앙 관리 서버 서비스용 계정은 중앙 관리 서버를 실행할 때 지정하거나 klsrvswch 유틸리티를 통해 지정할 수 있습니다. klsrvswch 유틸리티는 중앙 관리 서버의 설치 폴더에 있습니다. 기본 설치 경로: <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

도메인 계정을 지정해야 하는 이유는 다음과 같습니다:

- KES 기기 관리용 기능은 중앙 관리 서버의 필수 요소입니다.
- Kerberos 제한 위임(KCD)이 올바르게 작동하도록 하려면 수신 쪽(중앙 관리 서버)을 도메인 계정으로 실행해야 합니다.

http/kes4mob.mydom.local의 서비스 사용자 이름

도메인의 KSCMobileSrvcUsr 계정에 중앙 관리 서버가 설치된 기기의 포트 13292에서 모바일 프로토콜 서비스를 게시하기 위한 SPN을 추가합니다. 중앙 관리 서버가 설치된 kes4mob.mydom.local 기기의 경우 이는 다음과 같이 표시됩니다:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

역방향 프록시(firewall.mydom.local)를 사용하여 기기의 도메인 속성 구성

트래픽을 위임하려면 SPN으로 정의된 서비스(http/kes4mob.mydom.local:13292)가 역방향 프록시가 설치된 기기(firewall.mydom.local)를 신뢰하도록 설정합니다.

SPN으로 정의된 서비스(http/kes4mob.mydom.local:13292)가 역방향 프록시가 설치된 기기를 신뢰하도록 설정하려면 관리자가 다음 작업을 수행해야 합니다:

1. Microsoft Management Console 스냅인 "Active Directory 사용자 및 컴퓨터"에서 역방향 프록시가 설치된 기기(firewall.mydom.local)를 선택합니다.
2. 기기 속성의 **위임** 탭에서 **지정한 서비스로만 위임하도록 이 컴퓨터 신뢰** 토글을 **모든 인증 프로토콜 사용**으로 설정합니다.
3. **이 계정이 위임된 자격증명을 제공할 수 있는 서비스** 목록에서 SPN http/kes4mob.mydom.local:13292를 추가합니다.

게시(kes4mob.mydom.global)용 특수(사용자 지정) 인증서

중앙 관리 서버의 모바일 프로토콜을 게시하려면 FQDN kes4mob.mydom.global용으로 특수(사용자 지정) 인증서를 발급하여 관리 콘솔 내 중앙 관리 서버의 모바일 프로토콜 설정에서 기본 서버 인증서 대신 해당 인증서를 지정해야 합니다. 이렇게 하려면 중앙 관리 서버의 속성 창 **설정** 섹션에서 **모바일 기기용 포트 열기** 확인란을 선택하고 드롭다운 목록에서 **인증서 추가**를 선택합니다.

서버 인증서 컨테이너(확장자가 p12 또는 pfx인 파일)에는 루트 키 체인(공개키)도 포함되어야 합니다.

역방향 프록시에서 게시 구성

역방향 프록시에서 모바일 기기 쪽으로부터 kes4mob.mydom.global의 포트 13292로 전송되는 트래픽에 대해 FQDN(kes4mob.mydom.global)용으로 발급된 서버 인증서를 사용하여 SPN(http/kes4mob.mydom.local:13292)에서 KCD를 구성해야 합니다. 게시 작업과 게시된 액세스 포인트(중앙 관리 서버의 포트 13292)는 같은 서버 인증서를 공유해야 합니다.

Firebase Cloud Messaging 사용

Android 운영 체제에 의해 관리되는 KES 기기에 적절히 명령을 전달하기 위해 Kaspersky Security Center는 푸시 알림 메커니즘을 사용합니다. Firebase 클라우드 메시지(이하 FCM)를 통해 KES 기기와 중앙 관리 서버 간에 푸시 알림을 교환합니다. Kaspersky Security Center 관리 콘솔에서 해당 서비스에 KES 기기를 연결하기 위해 Firebase Cloud Messaging 설정을 지정할 수 있습니다.

Firebase Cloud Messaging 설정을 가져오려면 Google 계정이 있어야 합니다.

FCM을 사용하도록 설정하려면 다음을 수행합니다:

1. 관리 콘솔에서 **모바일 기기 관리** 노드와 **모바일 기기** 폴더를 선택합니다.
2. **모바일 기기** 폴더의 마우스 오른쪽 메뉴에서 **속성**을 선택합니다.
3. 폴더 속성에서 **Firebase Cloud Messaging 설정** 섹션을 선택합니다.
4. **Firebase 프로젝트 번호** 필드에서 FCM 발신자 ID를 지정합니다.
5. **개인 키 파일(JSON 형식)** 필드에서 개인 키 파일을 선택합니다.

   중앙 관리 서버와의 다음 동기화에서 Android 운영 체제에 의해 관리되는 KES 기기는 Firebase Cloud Messaging에 연결됩니다.

기기 초기 설정으로 재설정 버튼을 클릭하여 Firebase Cloud Messaging의 설정을 편집할 수 있습니다.

다른 Firebase 프로젝트로 전환하면 FCM이 재개될 때까지 10분을 기다려야 합니다.

FCM 서비스는 다음 주소 범위에서 실행됩니다:

- KES 기기 쪽에서는 다음 주소의 포트 443(HTTPS), 5228(HTTPS), 5229(HTTPS) 및 5230(HTTPS) 접근 권한이 필요합니다:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Google의 ASN 15169에 나열된 모든 IP 주소
- 중앙 관리 서버 쪽에서는 다음 주소의 포트 443(HTTPS) 접근 권한이 필요합니다:
  - fcm.googleapis.com
  - Google의 ASN 15169에 나열된 모든 IP 주소

관리 콘솔의 중앙 관리 서버 속성에서 프록시 서버 설정(**고급/인터넷 연결 구성**)을 정의한 경우에는 FCM과의 통신에 해당 설정이 사용됩니다.

FCM 구성: 발신자 ID 및 개인 키 파일 가져오기

FCM을 구성하려면:

1. Google 포털에 등록합니다.
2. Firebase 콘솔로 이동합니다.
3. 다음 중 하나를 수행합니다:
   - 새 프로젝트를 생성하려면 **프로젝트 생성**을 클릭하고 화면의 지침을 따릅니다.
   - 기존 프로젝트를 엽니다.
4. 기어 아이콘을 클릭하고 **프로젝트 설정**을 선택합니다.
   프로젝트 설정 창이 열립니다.
5. **클라우드 메시지** 탭을 선택합니다.
6. **Firebase 클라우드 메시지 API(V1)** 섹션의 **발신자 ID** 필드에서 관련 발신자 ID를 검색합니다.
7. **서비스 계정** 탭을 선택하고 **새 개인 키 생성**을 클릭합니다.
8. 창이 열리면 **키 생성**을 클릭하여 개인 키 파일을 생성하고 다운로드합니다.

이제 Firebase 클라우드 메시지가 구성되었습니다.

공개 키 인프라와의 통합

기본적으로는 중앙 관리 서버의 도메인 사용자 인증서 발급 과정을 간소화하기 위해 공개키 인프라(이하 PKI로 지칭함)와의 통합을 수행합니다.

관리자는 관리 콘솔에서 사용자에게 도메인 인증서를 할당할 수 있습니다. 다음 방법 중 하나를 사용해 이 할당을 수행할 수 있습니다:

- 인증서 설치 마법사에서 사용자에게 파일의 특수(사용자 지정) 인증서를 할당합니다.
- PKI와의 통합을 수행하고 특정 인증서 유형 또는 모든 인증서 유형의 인증서 소스 역할을 할 PKI 할당.

PKI와의 통합 설정은 **공개 키 인프라와 통합** 링크를 눌러 **모바일 기기 관리/인증서** 폴더의 작업 영역에서 사용할 수 있습니다.

도메인 사용자 인증서 발급을 위한 PKI와의 통합 관련 일반 원칙

관리 콘솔에서 **모바일 기기 관리/인증서** 폴더의 작업 영역에 있는 **공개 키 인프라와 통합** 링크를 클릭하여 중앙 관리 서버가 도메인 CA를 통해 도메인 사용자 인증서를 발급하는 데 사용하도록 할 도메인 계정(이하 PKI와의 통합을 수행하는 계정으로 지칭함)을 지정합니다.

이때 다음 사항을 참고하십시오:

- PKI와의 통합 설정을 사용하면 모든 인증서 유형의 기본 템플릿을 지정할 수 있습니다. **인증서 발급 규칙 구성** 버튼을 눌러 **모바일 기기 관리/인증서** 폴더의 작업 영역에서 제공되는 인증서 발급을 위한 규칙을 통해 모든 인증서 유형에 대해 개별 템플릿을 지정할 수 있습니다.
- 중앙 관리 서버가 설치된 기기에서 PKI와의 통합을 수행하는 계정의 인증서 저장소에 특수 등록 에이전트(EA) 인증서를 설치해야 합니다. 등록 에이전트(EA) 인증서는 도메인 CA(인증 기관)의 관리자가 발급합니다.

PKI와의 통합을 수행하는 계정은 다음 기준을 충족해야 합니다:

- 도메인 사용자여야 합니다.
- PKI와의 통합을 시작하는 중앙 관리 서버가 설치된 기기의 로컬 관리자여야 합니다.
- *서비스로 로그온*할 수 있는 권한이 있어야 합니다.
- 영구 사용자 프로필을 만들려면 중앙 관리 서버가 설치된 기기를 한 번 이상 이 계정으로 실행해야 합니다.

Kaspersky Security Center 웹 서버

Kaspersky Security Center 웹 서버(이후 웹 서버라고도 함)는 Kaspersky Security Center의 한 구성 요소입니다. 웹 서버는 독립 실행형 설치 패키지 게시, 모바일 기기용 독립 실행형 설치 패키지 및 공유 폴더의 파일을 게시하도록 설계되었습니다.

설치 패키지는 웹 서버에 자동으로 게시되며 처음으로 다운로드하고 나면 제거됩니다. 관리자는 이메일 등의 편리한 방법을 사용하여 새 링크를 전송할 수 있습니다.

사용자는 이 링크를 눌러 요청된 정보를 모바일 기기로 다운로드할 수 있습니다.

웹 서버 설정

웹 서버를 미세 조정해야 하는 경우 그 속성을 통해 HTTP용 포트(8060)와 HTTPS용 포트(8061)를 변경할 수 있습니다. 포트 변경 외에 HTTPS용 서버 인증서를 교체할 수 있으며 HTTP용 웹 서버의 FQDN도 변경할 수 있습니다.

기타 정기 작업

이 섹션에서는 Kaspersky Security Center의 일상적인 작업에 대한 권장 사항을 제공합니다.

관리 콘솔에서 표시등 및 기록된 이벤트 모니터링

관리 콘솔에서는 표시등을 확인하여 Kaspersky Security Center 및 관리 중인 기기의 현재 상태를 평가할 수 있습니다. 표시등은 **중앙 관리 서버** 노드 작업 영역의 **모니터링** 탭에 표시됩니다. 이 탭에서는 표시등과 기록된 이벤트가 포함된 6개 정보 패널이 제공됩니다. 표시등은 패널 왼쪽에 있는 색상이 지정된 세로 막대입니다. 표시등이 포함된 각 창은 Kaspersky Security Center의 특정 기능 범위에 해당합니다(아래 표 참조).

관리 콘솔의 표시등에 해당하는 범위

패널 이름	표시등 범위
배포	조직 네트워크에 있는 기기에 네트워크 에이전트 및 보안 제품 설치
관리 계획	관리 그룹의 구조. 네트워크 검사. 기기 이동 규칙
보호 설정	보안 애플리케이션 기능: 보호 상태, 악성 코드 검사
업데이트	업데이트 및 패치
모니터링	보호 상태
중앙 관리 서버	중앙 관리 서버 기능 및 속성

각 표시등은 5가지 색상 중 하나로 켜질 수 있습니다(아래 표 참조). 표시등의 색상은 Kaspersky Security Center의 현재 상태와 기록된 이벤트에 따라 달라집니다.

표시등의 색상 코드

상태	표시등 색상	표시등 색상의 의미
정보	녹색	관리자의 개입 필요 없음.
경고	노란색	관리자의 개입 필요.
심각	빨간색	심각한 문제 발생. 문제를 해결하려면 관리자의 개입이 필요합니다.
정보	하늘색	관리 중인 기기 보안에 대한 실제 위협 또는 위협 가능성과 관련이 없는 이벤트가 기록됨.
정보	회색	이벤트 세부 정보를 사용할 수 없거나 아직 가져오지 않음.

관리자는 **모니터링** 탭의 모든 정보 패널에서 표시등 색을 녹색으로 유지해야 합니다.

정보 패널에는 표시등에 영향을 미치는 기록된 이벤트와 Kaspersky Security Center 상태도 표시됩니다(아래 표 참조).

표시등 색상	이벤트 유형 표시 이름	이벤트 유형	설명
빨간색	**라이센스가 만료된 기기: %1대**	IDS_AK_STATUS_LIC_EXPAIRED	이 유형의 이벤트는 상업용 라이센스가 만료되면 발생합니다. Kaspersky Security Center는 하루에 한 번 기기에서 라이센스 만료 상태를 확인합니다. 상업용 라이센스가 만료되면 Kaspersky Security Center에서는 기본 기능만 제공됩니다. Kaspersky Security Center를 계속 사용하려면 상업용 라이센스를 갱신하십시오.
빨간색	**보안 제품이 실행 중이지 않음: %1대**	IDS_AK_STATUS_AV_NOT_RUNNING	이 유형의 이벤트는 기기에 설치된 보안 애플리케이션이 실행되고 있지 않을 때 발생합니다. 기기에서 Kaspersky Endpoint Security가 실행 중인지 확인합니다.
빨간색	**보호가 비활성화됨: %1대**	IDS_AK_STATUS_RTP_NOT_RUNNING	이 유형의 이벤트는 기기의 보안 애플리케이션이 지정된 간격보다 오랫동안 비활성화되었을 때 발생합니다. 기기에서 실시간 보호의 현재 상태를 확인하고 필요한 모든 보호 구성 요소가 활성화되어 있는지 확인하십시오.
빨간색	**소프트웨어 취약점이 기기에서 탐지됨**	IDS_AK_STATUS_VULNERABILITIES_FOUND	이 유형의 이벤트는 *취약성 및 필수 업데이트 찾기* 작업으로 기기에 설치된 애플리케이션에서 지정된 심각도 수준의 취약성이 탐지되면 발생합니다. **애플리케이션 관리** 폴더의 **소프트웨어 업데이트** 하위 폴더에서 사용 가능한 업데이트 목록을 확인할 수 있습니다. 이 폴더에는 기기에 배포할 수 있는 Microsoft 애플리케이션과 중앙 관리 서버가 검색한 기타 소프트웨어 공급업체 제품의 업데이트 목록이 들어 있습니다. 사용 가능한 업데이트 정보를 확인한 후 기기에 설치합니다.
빨간색	**중앙 관리 서버에 심각 이벤트가 등록됨**	IDS_AK_STATUS_EVENTS_OCCURED	이 유형의 이벤트는 중앙 관리 서버의 심각 이벤트가 감지될 때 발생합니다. 중앙 관리 서버에 저장된 이벤트 목록을 확인한 다음 심각 이벤트를 하나씩 수정하십시오.
빨간색	**중앙 관리 서버에 오류 이벤트가 기록됨**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	이 유형의 이벤트는 예기치 않은 오류가 중앙 관리 서버 측에 기록될 때 발생합니다. 중앙 관리 서버에 저장된 이벤트 목록을 확인하고 오류를 하나씩 수정하십시오.
빨간색	**연결이 끊긴 기기: %1대**	IDS_AK_STATUS_ADM_LOST_CONTROL1	이 유형의 이벤트는 중앙 관리 서버와 기기 간의 연결이 끊어지면 발생합니다. 연결 해제된 기기 목록을 보고 다시 연결해 보십시오.
빨간색	**오랫동안 중앙 관리 서버에 연결 안 된 기기: %1대**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	이 유형의 이벤트는 기기가 꺼져서 지정된 시간 내에 중앙 관리 서버에 연결되지 않았을 때 발생합니다. 기기가 켜져 있고 네트워크 에이전트가 실행 중인지 확인하십시오.
빨간색	**'정상' 상태가 아닌 기기: %1대**	IDS_AK_STATUS_HOST_NOT_OK	이 유형의 이벤트는 중앙 관리 서버에 연결된 기기의 *정상* 상태가 *위험* 또는 *경고*로 변경되면 발생합니다. Kaspersky Security Center 원격 진단 유틸리티를 사용하여 문제를 해결할 수 있습니다.
빨간색	**데이터베이스가 오래된 기기: %1대**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	이 유형의 이벤트는 바이러스 백신 데이터베이스가 지정된 시간 내에 기기에서 업데이트되지 않았을 때 발생합니다. 지침에 따라 Kaspersky 데이터베이스를 업데이트합니다.
빨간색	**오랫동안 Windows 업데이트 패치를 검색하지 않은 기기: %1대**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	이 유형의 이벤트는 *Windows Update 동기화 수행* 작업이 지정된 시간 내에 실행되지 않았을 때 발생합니다. 지침에 따라 Windows 업데이트를 중앙 관리 서버와 동기화하십시오.
빨간색	**Kaspersky Security Center용 %1 플러그인을 설치해야 합니다**	IDS_AK_STATUS_PLUGINS_REQUIRED2	이 유형의 이벤트는 Kaspersky 애플리케이션용 추가 플러그인을 설치해야 할 때 발생합니다. Kaspersky 기술 지원 웹페이지에서 Kaspersky 애플리케이션에 필요한 관리 플러그인을 다운로드하고 설치합니다.

관리 중인 기기에 원격 접근

이 섹션에서는 관리 중인 기기에 대한 원격 접근에 대한 정보를 제공합니다.

"중앙 관리 서버와 계속 연결 유지" 옵션을 사용하여 관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결 제공

푸시 서버를 사용하지 않는 경우 Kaspersky Security Center에서는 기본적으로 관리 중인 기기와 중앙 관리 서버 간의 지속적인 연결 기능이 제공되지 않습니다. 관리 중인 기기의 네트워크 에이전트는 주기적으로 연결을 설정하여 중앙 관리 서버와의 동기화를 수행합니다. 이러한 동기화 세션 간의 간격은 네트워크 에이전트 정책에서 정의됩니다. 조기 동기화가 필요한 경우 중앙 관리 서버(사용 중인 경우 배포 지점)는 IPv4 또는 IPv6 네트워크를 통해 서명된 네트워크 패킷을 네트워크 에이전트의 UDP 포트로 보냅니다. 기본 포트 번호는 15000입니다. 중앙 관리 서버와 관리 중인 기기 간에 UDP를 통한 연결이 불가능한 경우에는 네트워크 에이전트와 중앙 관리 서버 간의 다음 정기 연결 시 동기화 간격 내에 동기화가 실행됩니다.

로컬 작업 실행/중지, 관리 중인 애플리케이션의 통계 수신, 터널 만들기 등의 일부 작업은 네트워크 에이전트와 중앙 관리 서버를 미리 연결하지 않으면 수행할 수 없습니다. 이 문제를 해결하려면 푸시 서버를 사용하지 않는 경우 **중앙 관리 서버와 계속 연결 유지** 옵션을 사용하여 관리 중인 기기와 중앙 관리 서버 사이에 지속적인 연결이 있는지 확인합니다.

관리 중인 기기와 중앙 관리 서버 간에 지속적인 연결을 제공하려면:

1. 콘솔 트리에서 **관리 중인 기기** 폴더를 선택합니다.
2. 폴더의 작업 공간에서 지속적인 연결을 제공하려는 관리 중인 기기를 선택합니다.
3. 기기의 마우스 오른쪽 메뉴에서 **속성**를 선택합니다.
   선택한 정책의 속성 창이 열립니다.
4. 표시된 창의 **일반** 섹션에서 **중앙 관리 서버와 계속 연결 유지** 옵션을 선택합니다.

관리 중인 기기와 중앙 관리 서버 사이에 지속적인 연결이 구성됩니다.

중앙 관리 서버와 계속 연결 유지 확인란을 선택한 상태에서 사용 가능한 기기의 최대 총 개수는 300입니다.

기기와 중앙 관리 서버 간 연결 시간 확인 정보

기기를 종료하면 네트워크 에이전트가 중앙 관리 서버에 해당 이벤트를 알립니다. 관리 콘솔에서는 해당 기기가 종료된 것으로 표시됩니다. 그러나 네트워크 에이전트가 이러한 모든 이벤트를 중앙 관리 서버에 알릴 수는 없습니다. 따라서 중앙 관리 서버는 각 기기의 **중앙 관리 서버에 연결** 특성(이 특성의 값은 관리 콘솔의 기기 속성 **일반** 섹션에 표시됨)을 주기적으로 분석하여 네트워크 에이전트 현재 설정의 동기화 간격과 비교합니다. 연속하는 4회 이상의 동기화 간격 동안 응답하지 않은 기기는 종료된 것으로 표시됩니다.

강제 동기화 정보

Kaspersky Security Center가 관리 중인 기기의 상태, 설정, 작업 및 정책을 자동으로 동기화하지만, 경우에 따라 관리자가 현재 시점에서 지정된 기기에 대해 동기화가 이미 수행되었는지를 정확히 파악해야 할 수도 있습니다.

관리 콘솔 내 관리 중인 기기의 마우스 오른쪽 메뉴에서 **모든 작업** 메뉴 항목에는 **강제 동기화** 명령이 포함되어 있습니다. Kaspersky Security Center 15.1에서 이 명령을 실행하면 중앙 관리 서버가 해당 기기에 연결을 시도합니다. 이 시도가 성공하면 강제 동기화가 수행됩니다. 그렇지 않은 경우에는 네트워크 에이전트와 중앙 관리 서버 간에 스케줄된 다음 연결 이후에만 강제 동기화가 수행됩니다.

터널링 정보

Kaspersky Security Center에서는 중앙 관리 서버를 통해 관리 콘솔에서, 그리고 네트워크 에이전트를 통해 관리 중인 기기의 지정된 포트로 TCP 연결을 터널링할 수 있습니다. 터널링은 관리 콘솔과 대상 기기를 직접 연결할 수 없는 경우 기기의 클라이언트 애플리케이션을 관리 중인 기기의 TCP 포트에 설치된 관리 콘솔과 연결하는 데 사용됩니다.

예를 들어 기존 세션에 연결하고 새 원격 세션을 만들기 위한 용도로 원격 데스크톱에 연결하는 데 터널링을 사용할 수 있습니다.

외부 도구를 사용하여 터널링을 작동시킬 수도 있습니다. 예를 들어 관리자는 putty 유틸리티, VNC 클라이언트 및 기타 도구를 이러한 방식으로 실행할 수 있습니다.

사이징 가이드

이 섹션은 Kaspersky Security Center 사이징에 대한 정보를 제공합니다.

이 설명서 정보

Kaspersky Security Center 15.1(또는 "Kaspersky Security Center") 사이징 가이드는 Kaspersky Security Center를 설치하고 관리할 뿐만 아니라 Kaspersky Security Center를 사용하는 조직에 기술 지원을 제공하는 전문가 용으로 작성되었습니다.

모든 권장 사항 및 계산은 Kaspersky Security Center가 모바일 기기를 포함하여 Kaspersky 소프트웨어가 설치된 기기의 보호를 관리하는 네트워크에 대해 제공됩니다. 모바일 기기 또는 기타 모든 관리 중인 기기를 별도로 고려해야 하는 경우, 이 내용은 구체적으로 명시되어 있습니다.

다양한 운영 조건에서 최적의 성능을 유지하려면 네트워크에 있는 기기 수, 네트워크 토폴로지 및 필요한 Kaspersky Security Center 기능을 고려하십시오.

이 설명서에는 다음 정보를 제공합니다:

- Kaspersky Security Center 제한 사항
- Kaspersky Security Center의 핵심 노드에 대한 계산 - 중앙 관리 서버 및 배포 지점:
  - 중앙 관리 서버 및 배포 지점에 대한 하드웨어 요구 사항
  - 중앙 관리 서버의 수와 계층 구조 계산
  - 배포 지점의 수와 구성 계산
- 네트워크에 연결된 기기의 수에 따라 데이터베이스에 기록되는 이벤트 구성
- 성능 최적화를 위한 일반적인 모범 사례
- Kaspersky Security Center의 최적 성능을 목표로 하는 특정 작업 구성
- Kaspersky Security Center 중앙 관리 서버와 모든 보호 기기 간의 트래픽 양(네트워크 부하)

다음과 같은 경우 이 설명서를 참조하는 것이 좋습니다:

- Kaspersky Security Center 설치 전에 리소스 이용을 계획할 때
- Kaspersky Security Center가 배포되는 네트워크의 규모에 중대한 변경 사항을 계획할 때
- 제한된 네트워크 세그먼트(테스트 환경)에서 Kaspersky Security Center를 사용하다가 회사 네트워크에 Kaspersky Security Center를 전체 규모로 배포할 때
- 사용된 Kaspersky Security Center 기능 세트를 변경할 때

Kaspersky Security Center의 제한 사항에 대한 정보

아래 표에는 Kaspersky Security Center 최신 버전의 제한 사항이 표시되어 있습니다.

Kaspersky Security Center 제한 사항

제한 유형	값
중앙 관리 서버당 관리 중인 기기의 최대 수	100,000
중앙 관리 서버와 계속 연결 유지 옵션이 선택된 기기의 최대 개수	300
관리 그룹의 최대 개수	10,000
저장할 이벤트의 최대 개수	45,000,000
최대 정책 개수	2 000
최대 작업 개수	2 000
총 Active Directory 개체(조직 단위, OU) 및 사용자의 계정, 기기, 보안 그룹) 개수의 최댓값	1,000,000
정책 내 프로필 개수의 최댓값	100
단일 기본 중앙 관리 서버의 보조 중앙 관리 서버 개수 최댓값	500
가상 중앙 관리 서버 개수의 최댓값	500
단일 배포 지점이 관리할 수 있는 최대 기기 수(배포 지점은 모바일이 아닌 기기만 관리할 수 있음)	10,000
단일 연결 게이트웨이를 사용할 수 있는 최대 기기 수	10,000, 모바일 기기 포함
중앙 관리 서버당 최대 모바일 기기 수	100,000 - 고정된 관리 중인 기기 수

중앙 관리 서버에 대한 계산

이 섹션에서는 중앙 관리 서버로 사용되는 기기에 대한 소프트웨어 및 하드웨어 요구 사항을 제공합니다. 또한 조직 네트워크의 구성에 따라 중앙 관리 서버의 수와 계층을 계산하기 위한 권장 사항이 제공됩니다.

중앙 관리 서버에 대한 하드웨어 리소스 계산

이 섹션에는 중앙 관리 서버에 대한 하드웨어 리소스 준비를 계획하기 위한 지침을 제공하는 계산 방법이 들어 있습니다. 취약점 및 패치 관리 기능을 사용할 때 디스크 공간을 계산하기 위한 권장 사항은 별도로 제공됩니다.

DBMS 및 중앙 관리 서버의 하드웨어 요구 사항

아래 표에는 테스트 중에 얻은 중앙 관리 서버 및 DBMS의 권장 최소 하드웨어 요구 사항이 나와 있습니다. 지원하는 운영 체제 및 DBMS 전체 목록을 보려면 하드웨어 및 소프트웨어 요구 사항 목록을 참조하십시오.

중앙 관리 서버와 DBMS가 서로 다른 기기에 있고 네트워크에 5만 대의 기기가 있음

중앙 관리 서버가 설치된 기기의 구성

하드웨어	값
CPU	4코어, 2500MHz
RAM	8 GB
하드 드라이브	300GB, RAID 권장
네트워크 어댑터	1기가비트

DBMS가 설치되는 기기의 구성

하드웨어	값
CPU	4코어, 2500MHz
RAM	16 GB
하드 드라이브	200 GB, SATA RAID
네트워크 어댑터	1기가비트

중앙 관리 서버와 DBMS가 동일한 기기에 있고 네트워크에 5만 대의 기기가 있음

중앙 관리 서버 및 DBMS가 설치되는 기기의 구성

하드웨어	값
CPU	8코어, 2500MHz
RAM	16 GB
하드 드라이브	500 GB, SATA RAID
네트워크 어댑터	1기가비트

중앙 관리 서버와 DBMS가 서로 다른 기기에 있고 네트워크에 10만 대의 기기가 있음

중앙 관리 서버가 설치된 기기의 구성

하드웨어	값
CPU	8코어, 2.13 GHz
RAM	8 GB
하드 드라이브	RAID가 구성된 1TB
네트워크 어댑터	1기가비트

DBMS가 설치된 기기의 구성

하드웨어	값
CPU	8코어, 2.53 GHz
RAM	26 GB
하드 드라이브	500 GB, SATA RAID
네트워크 어댑터	1기가비트

이 테스트는 다음 설정에서 실행되었습니다:

- 배포 지점 자동 할당은 중앙 관리 서버에서 활성화되거나 권장 계산표에 따라 수동으로 배포 지점이 할당됩니다.
- 백업 작업에서는 전용 서버에 있는 파일 리소스에 백업 복사본을 저장합니다.

- 네트워크 에이전트의 동기화 간격은 아래 표에 지정된 대로 설정됩니다.

  네트워크 에이전트의 동기화 간격

동기화 주기(분)	관리 중인 기기 수
15	10,000
30	20,000
45	30,000
60	40,000
75	50,000
150	100,000

데이터베이스 공간 계산

데이터베이스에서 이용되어야 하는 대략적인 용량은 다음 공식을 이용해 계산할 수 있습니다:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

여기서:

- C는 기기의 수입니다.
- E는 저장되는 이벤트 수입니다.
- A는 Active directory 개체의 총 개수입니다:
  - 기기 계정
  - 사용자 계정
  - 보안 그룹의 계정
  - Active Directory 조직 단위

  Active Directory 검색이 비활성되어 있다면 A는 0과 같은 것으로 간주됩니다.
- N은 엔드포인트 기기에서 인벤토리에 포함된 실행 파일의 평균 수입니다.
- F는 실행 파일이 인벤토리에 포함된 엔드포인트 기기의 수입니다.

Kaspersky Endpoint Security 정책 설정에서 실행하는 애플리케이션 정보를 중앙 관리 서버에 알리려고 한다면 데이터베이스에 해당 애플리케이션에 대한 정보를 저장하기 위해 추가로 (0.03 * C) 기가 바이트가 필요합니다.

중앙 관리 서버가 Windows 업데이트를 배포하면(Windows Server Update Services 서버 역할 수행), 해당 데이터베이스는 추가적으로 2.5GB의 용량을 더 필요로 합니다.

운영 중에는 데이터베이스에는 언제나 약간의 *할당 안 된 공간*이 나타납니다. 그렇기 때문에 데이터베이스 파일(기본적으로 SQL 서버를 DBMS로 사용하면, KAV.MDF 파일임)의 실제 크기는 데이터베이스에서 차지하고 있는 용량보다 약 2배 이상으로 큽니다.

트랜잭션 로그의 크기를 명시적으로 제한하는 것은 권장하지 않습니다(기본적으로 KAV_log.LDF 파일임. 만일 SQL Server를 DBMS로 사용하는 경우). MAXSIZE 파라미터의 기본 값을 유지하는 것이 좋습니다. 그러나 이 파일의 크기를 제한해야 하는 경우에는 KAV_log.LDF의 MAXSIZE 파라미터의 일반적인 필수 최소값이 20480MB라는 점을 고려하십시오.

디스크 공간 계산(취약점 및 패치 관리 기능 사용 유무)

취약점 및 패치 관리 기능을 사용하지 않고 디스크 공간 계산

%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 폴더에 필요한 중앙 관리 서버 디스크 공간은 대략 다음 수식을 사용하여 계산할 수 있습니다:

(724 * C + 0.15 * E + 0.17 * A), KB

여기서:

- C는 기기의 수입니다.
- E는 저장되는 이벤트 수입니다.
- A는 Active directory 개체의 총 개수입니다:
  - 기기 계정
  - 사용자 계정
  - 보안 그룹의 계정
  - Active Directory 조직 단위

Active Directory 검색이 비활성되어 있다면 A는 0과 같은 것으로 간주됩니다.

취약점 및 패치 관리 기능을 사용할 때 추가적인 디스크 공간 계산

- 업데이트. 업데이트를 저장하려면 공유 폴더에 4 GB 이상의 공간이 추가적으로 필요합니다.
- 설치 패키지. 일부 업데이트 패키지가 중앙 관리 서버에 저장되는 경우에는 공유 폴더에 모든 설치하기 위해 이용 가능한 설치 패키지의 총 크기에 해당하는 디스크 여유 공간이 추가로 필요합니다.
- 원격 설치 작업. 중앙 관리 서버에 원격 설치 작업이 있다면 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 폴더에는 설치할 모든 설치 패키지의 총 크기에 해당하는 디스크 여유 공간이 추가로 필요합니다.
- 패치. 패치 설치 시 중앙 관리 서버를 사용하는 경우에는 다음과 같은 디스크 여유 공간이 추가로 필요합니다:
  - 패치 폴더는 다운로드한 모든 패치의 총 크기에 해당하는 디스크 공간을 가지고 있습니다. 패치는 기본적으로 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles 폴더에 저장됩니다.

    klsrvswch 유틸리티를 사용하여 패치를 다른 폴더에 저장할 수 있습니다. klsrvswch 유틸리티는 중앙 관리 서버가 설치된 폴더에 있습니다. 기본 설치 경로: <디스크>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

중앙 관리 서버를 WSUS 서버로 사용하는 경우에는 이 폴더에 100GB 이상의 공간을 할당하는 것이 좋습니다.

- %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit 폴더에는 업데이트(패치) 설치 및 취약점 수정 작업의 인스턴스에서 불러오는 패치의 전체 크기와 동일한 디스크 공간이 있어야 합니다.

중앙 관리 서버의 수 및 구성 계산

기본 중앙 관리 서버의 부하를 줄이기 위해 각 관리 그룹에 별도의 중앙 관리 서버를 할당할 수 있습니다. 하나의 기본 중앙 관리 서버에 대한 보조 중앙 관리 서버의 수는 500개를 초과할 수 없습니다.

조직 네트워크의 구성에 따라 중앙 관리 서버 구성을 생성하는 것이 좋습니다.

동적 가상 컴퓨터를 Kaspersky Security Center에 연결하기 위한 권장 사항

동적 가상 컴퓨터(또는 동적 VM)은 정적 가상 컴퓨터보다 리소스를 더 많이 사용합니다.

동적 가상 컴퓨터에 대한 자세한 내용은 동적 가상 컴퓨터 지원을 참조하십시오.

새 동적 VM이 연결되면 Kaspersky Security Center는 관리 콘솔에서 이 동적 VM에 대한 아이콘을 생성하고 동적 VM을 관리 그룹으로 이동합니다. 그런 다음 동적 VM이 중앙 관리 서버 데이터베이스에 추가됩니다. 중앙 관리 서버는 이 동적 VM에 설치된 네트워크 에이전트와 완전히 동기화됩니다.

조직의 네트워크에서 네트워크 에이전트는 각 동적 VM에 대해 다음과 같은 네트워크 목록을 생성합니다:

- 하드웨어
- 설치된 소프트웨어
- 감지된 취약점
- 애플리케이션 제어 구성 요소의 이벤트 및 실행 파일 목록

네트워크 에이전트는 이러한 네트워크 목록을 중앙 관리 서버로 전송합니다. 네트워크 목록의 크기는 동적 VM에 설치된 구성 요소에 따라 다르며 Kaspersky Security Center 및 데이터베이스 관리 시스템(DBMS)의 성능에 영향을 줄 수 있습니다. 부하는 비선형적으로 증가할 수 있습니다.

사용자가 동적 VM 작업을 마치고 전원을 끄면 이 시스템은 가상 인프라에서 제거되고 이 시스템에 대한 항목은 중앙 관리 서버 데이터베이스에서 제거됩니다.

이러한 모든 작업은 Kaspersky Security Center 및 중앙 관리 서버 데이터베이스 리소스를 많이 사용하며 Kaspersky Security Center 및 DBMS의 성능을 저하시킬 수 있습니다. Kaspersky Security Center에 동적 VM을 최대 20,000개까지만 연결할 것을 권장합니다.

연결된 동적 VM이 표준 작업(데이터베이스 업데이트 등)을 수행하고 메모리를 80% 이하로, 사용 가능한 코어를 75~80% 이하로 사용한다면, Kaspersky Security Center에 동적 VM을 20,000개 이상 연결할 수 있습니다.

동적 VM에서 정책 설정, 소프트웨어, 운영 체제를 변경하면 리소스 소모가 줄거나 늘어납니다. 리소스의 80~95%를 소모하는 것을 최적으로 간주합니다.

배포 지점 및 연결 게이트웨이에 대한 계산

이 섹션에서는 배포 지점로 사용되는 기기에 대한 하드웨어 요구 사항과 함께 기업 네트워크의 구성에 따라 배포 지점 및 연결 게이트웨이의 수를 계산하기 위한 권장 사항을 제공합니다.

배포 지점의 요구 사항

클라이언트 기기 10,000대를 처리하려면 배포 지점이 최소한 다음 요구 사항을 충족해야 합니다(테스트 스탠드의 구성이 제공됨):

- CPU: 인텔® Core™ i7-7700 CPU, 3.60GHz 4코어.
- RAM: 8 GB.
- 무료 저장 공간: 120GB.

중앙 관리 서버를 배포 지점으로 할당하면 중앙 관리 서버의 부하가 증가하므로 권장하지 않습니다.

만일 중앙 관리 서버에서 어떤 원격 설치 작업이 보류 중이라면, 배포 지점이 설치된 기기 또한 설치 패키지의 용량과 같은 여유 공간을 필요로 합니다.

만일 중앙 관리 서버에서 하나 이상의 업데이트(패치) 설치 작업과 취약점 수정 작업이 보류 중이라면, 배포 지점이 설치된 기기 또한 설치할 모든 패치 전체 용량의 2배의 여유 공간을 필요로 합니다.

배포 지점이 Kaspersky 업데이트 서버에서 직접 데이터베이스 업데이트 및 애플리케이션 소프트웨어 모듈을 받는 체계를 사용한다면 배포 지점이 인터넷에 연결되어 있어야 합니다.

배포 지점의 개수 및 구성 계산

네트워크에 포함된 클라이언트 기기가 많을수록 배포 지점도 더 많이 필요합니다. 배포 지점 자동 할당 기능을 중지하는 않는 것을 권장합니다. 배포 지점 자동 할당 기능이 활성되면 클라이언트 기기의 수가 매우 많으면 중앙 관리 서버는 배포 지점을 할당하고 그 구성을 정의합니다.

독점 할당된 배포 지점 사용

특정 기기를 배포 지점(예, 독점적으로 할당된 서버)로 사용하려는 경우 배포 지점의 자동 할당을 사용하지 않도록 선택할 수 있습니다. 이 경우 배포 지점을 할당할 기기에 사용 가능한 디스크 공간이 충분하고 정기적으로 종료되지 않으며 절전 모드가 해제되어 있는지 확인하십시오.

네트워크에 연결된 기기 수에 따라 단일 네트워크 세그먼트를 포함하는 네트워크에 할당된 배포 지점의 수

네트워크 세그먼트에 있는 클라이언트 기기의 수	배포 지점 개수
300대 이하	0(배포 지점 할당 안 함)
300대 이상	적합: (N/10,000 + 1), 권장: (N/5,000 + 2), 여기서 N은 네트워크에 연결된 기기 개수

네트워크에 연결된 기기 수에 따라 다중 네트워크 세그먼트를 포함하는 네트워크에 할당된 배포 지점의 수

네트워크 세그먼트당 클라이언트 기기의 수	배포 지점 개수
10대 이하	0(배포 지점 할당 안 함)
10~100대	1
100대 이상	적합: (N/10,000 + 1), 권장: (N/5,000 + 2), 여기서 N은 네트워크에 연결된 기기 개수

표준 클라이언트 기기(워크스테이션)를 배포 지점으로 사용

표준 클라이언트 기기(워크스테이션)를 배포 지점으로 사용하려는 경우에는 통신 채널과 중앙 관리 서버에 과도한 부하가 걸리지 않도록 아래 표에 나와 있는 것처럼 배포 지점을 할당하는 것이 좋습니다:

네트워크에 연결된 기기 수에 따라 단일 네트워크 세그먼트를 포함하는 네트워크에 배포 지점 기능을 수행하는 워크스테이션의 수

네트워크 세그먼트에 있는 클라이언트 기기의 수	배포 지점 개수
300대 이하	0(배포 지점 할당 안 함)
300대 이상	(N/300 + 1), 여기서 N은 네트워크에 연결된 기기 수를 뜻하지만 최소 3대의 배포 지점이 있어야합니다

네트워크에 연결된 기기 수에 따라 다중 네트워크 세그먼트를 포함하는 네트워크에 배포 지점 기능을 수행하는 워크스테이션의 수

네트워크 세그먼트당 클라이언트 기기의 수	배포 지점 개수
10대 이하	0(배포 지점 할당 안 함)
10~30대	1
31~300대	2
300대 이상	(N/300 + 1), 여기서 N은 네트워크에 연결된 기기 수를 뜻하지만 최소 3대의 배포 지점이 있어야합니다

배포 지점이 종료되거나 다른 원인으로는 사용할 수 없는 경우 이 배포 지점에 연결된 관리 중인 기기는 업데이트를 위해 중앙 관리 서버에 접근할 수 있습니다.

연결 게이트웨이 수 계산

연결 게이트웨이를 사용하려는 경우에는 이 기능용으로 특수 기기를 지정하는 것이 좋습니다.

연결 게이트웨이는 모바일 기기를 포함하여 최대 10,000개의 관리 중인 기기를 관리할 수 있습니다.

작업 및 정책에 대한 이벤트 정보 로깅

이 섹션에서는 중앙 관리 서버 데이터베이스에 이벤트를 저장하는 것과 관련된 계산을 제공하고 이벤트 수를 최소화하여 중앙 관리 서버의 부하를 줄이는 방법에 대한 권장 사항을 제공합니다.

기본적으로 각 작업 및 정책의 속성은 작업 실행 및 정책 적용과 관련된 모든 이벤트를 저장합니다.

그러나 작업이 매우 자주(예, 주당 한 번 이상) 실행되고 상당히 많은 수의 기기(예, 10,000대 이상)에서 실행되는 경우 이벤트 수가 너무 많아서 데이터베이스 한계를 초과할 수 있습니다. 이 경우 작업 설정에서 다음 두 옵션 중 하나를 선택하는 것이 좋습니다:

- **작업 진행 상태와 관련된 이벤트 저장**. 이때, 데이터베이스는 작업이 실행되는 각 기기에서 작업 실행, 진행, 완료(성공, 경고 또는 오류)에 대한 정보만 수신합니다.

- **작업 실행 결과만 저장**. 이 경우 데이터베이스는 작업이 실행되는 각 기기에서 작업 완료에 대한 정보(성공, 경고 또는 오류)만 수신합니다.

상당히 많은 수의 기기(예, 10,000대 이상)에 대해 정책이 정의된 경우 이벤트 수가 많아지고 이벤트가 데이터베이스에 대량으로 유입될 수 있습니다. 이 경우 정책 설정에서 우선되는 심각 이벤트만 선택하고 로그 기록을 활성화하는 것이 좋습니다. 다른 모든 이벤트의 로그 기록은 비활성화하는 것이 좋습니다.

이렇게 하면 데이터베이스의 이벤트 수를 줄이고, 데이터베이스의 이벤트 테이블에 대한 분석과 관련된 시나리오의 실행 속도를 높이며 다량의 이벤트가 심각 이벤트를 덮어쓰는 위험을 줄일 수 있습니다.

또한 작업 또는 정책과 관련된 이벤트의 저장 기간을 줄일 수 있습니다. 기본 기간은 작업 관련 이벤트는 7일, 정책 관련 이벤트는 30일입니다. 이벤트 저장 기간 변경 시, 조직의 작업 절차와 시스템 관리자가 각 이벤트 분석에 할당할 수 있는 시간을 고려하십시오.

다음과 같은 경우 이벤트 저장 설정을 수정하는 것이 좋습니다:

- Kaspersky Security Center 데이터베이스의 전체 이벤트 중 많은 부분을 차지하는 것은 그룹 작업의 중간 상태 변경과 관련된 이벤트와 정책 적용 관련 이벤트입니다.

- 데이터베이스에 저장되는 전체 이벤트의 수에 대해 설정한 한도를 초과하면, Kaspersky 이벤트 로그에서 이벤트 자동 제거에 대한 항목을 표시하기 시작합니다.

하루에 하나의 기기에서 발생하는 최적의 이벤트 수가 20개를 초과하지 않아야 한다는 가정을 기반으로 이벤트 기록 옵션을 선택하십시오. 필요한 경우 이 제한을 약간 늘릴 수 있지만 네트워크에 연결된 기기 수가 상대적으로 적을 때만(10,000 미만) 이 제한을 늘릴 수 있습니다.

어떤 작업의 특정한 고려 사항 및 최적 설정

어떤 작업에는 네트워크에 연결된 기기의 수와 관련된 특정한 고려 사항이 있습니다. 이 섹션에서는 그러한 작업의 최적 구성에 대한 권장 사항을 제공합니다.

기기 발견, 데이터 백업 작업, 중앙 관리 서버 점검 작업 및 Kaspersky Endpoint Security 업데이트용 그룹 작업은 Kaspersky Security Center의 기본 기능 중 일부입니다.

기기 발견 빈도

도메인 컨트롤러에 과도한 부하가 발생할 수 있으므로 기기 발견의 기본 빈도를 늘리는 것은 바람직하지 않습니다. 대신 조직의 필요에 따라 허용되는 최소 빈도로 검색을 예약하는 것이 좋습니다. 최적의 일정을 계산하기 위한 권장 사항은 아래 표에 나와 있습니다.

네트워크에 연결된 기기 개수	권장하는 기기 발견 빈도
10,000대 이하	기본 빈도 또는 그 이하
10,000 또는 그 이상	하루에 한번 또는 그 이하

중앙 관리 서버 데이터 백업 작업 및 중앙 관리 서버 점검 작업

중앙 관리 서버는 다음 작업이 실행 중일 때 작업을 중지합니다:

- 중앙 관리 서버 데이터 백업
- 중앙 관리 서버 점검

이러한 작업이 실행 중일 때 데이터베이스는 어떠한 데이터도 수신할 수 없습니다.

다른 중앙 관리 서버 작업과 동시에 실행되지 않도록 이 작업들을 다시 예약해야 할 수 있습니다.

Kaspersky Endpoint Security 업데이트를 위한 그룹 작업

중앙 관리 서버가 업데이트 경로 역할을 하는 경우 Kaspersky Endpoint Security 버전 10 이상 버전에서 권장되는 그룹 업데이트 작업에 대한 스케줄 옵션은 **랜덤하게 작업 시작 시간을 자동으로 조절하는 기능 사용** 확인란을 선택하고 **저장소 업데이트 다운로드를 완료한** 후입니다.

Kaspersky 서버에서 저장소로 업데이트를 다운로드하는 로컬 작업을 각 배포 지점에서 만드는 경우 Kaspersky Endpoint Security 그룹 업데이트 작업에 권장되는 옵션은 정기 스케줄입니다. 이 경우 임의 기간의 값은 1시간이어야 합니다.

인벤토리 작업

실행 파일에 관한 정보를 얻으면서 데이터베이스의 부하를 줄일 수 있습니다. 이렇게 하려면 표준 소프트웨어 집합이 설치된 참조 기기에서 Kaspersky Endpoint Security용 인벤토리 작업을 실행하는 것이 좋습니다.

단일 기기에서 중앙 관리 서버가 수신하는 실행 파일의 수는 150,000개를 초과할 수 없습니다. Kaspersky Security Center가 이 제한에 도달하면 새 파일을 받을 수 없습니다.

일반적으로 클라이언트 기기에 있는 파일 개수는 60,000개를 초과하지 않습니다. 파일 서버의 실행 파일 수는 150,000 임계 값보다 클 수 있으며 심지어 임계 값을 초과할 수 있습니다.

Kaspersky Endpoint Security 11이 설치되어 있고 타사 애플리케이션이 설치되어 있지 않은 Windows 7 운영 체제를 실행하는 기기에서 인벤토리 작업의 결과가 다음과 같이 측정되었습니다:

- **DLL 모듈 인벤토리** 및 **스크립트 파일 인벤토리** 확인란을 해제한 경우: 약 3,000개 파일.
- **DLL 모듈 인벤토리** 및 **스크립트 파일 인벤토리** 확인란을 선택한 경우: 설치된 운영 체제 서비스 팩의 수에 따라 10,000~20,000개 파일.
- **스크립트 파일 인벤토리** 확인란만 선택한 경우: 약 10,000개의 파일.

중앙 관리 서버 및 보호 제품이 설치된 기기 간의 네트워크 부하 분산에 대한 세부 정보

이 섹션에서는 측정이 수행된 조건에 대한 설명과 함께 네트워크 트래픽의 테스트 측정 결과를 제공합니다. 조직 내(또는 중앙 관리 서버와 보호할 기기가 있는 다른 조직 간)의 네트워크 채널의 처리 용량과 네트워크 인프라를 계획할 때 이 정보를 참조할 수 있습니다. 네트워크의 처리 용량을 알면 서로 다른 데이터 전송 작업에 걸리는 시간을 대략적으로 예측할 수도 있습니다.

다양한 시나리오에서의 트래픽 사용량

아래 표는 서로 다른 시나리오에서 중앙 관리 서버와 관리 중인 기기 간의 트래픽에 대해 수행된 테스트 측정 결과를 보여줍니다.

기본적으로 기기는 15분마다 또는 더 긴 간격으로 중앙 관리 서버와 동기화됩니다. 그러나 중앙 관리 서버에서 정책 또는 작업 설정을 수정하면 해당 정책(또는 작업)이 적용되는 기기에서 우선 동기화가 진행되며 새 설정이 해당 기기로 전송됩니다.

중앙 관리 서버와 관리 중인 기기 간의 트래픽 용량

시나리오	중앙 관리 서버에서 각 관리 중인 기기로 발생하는 트래픽	각 관리 중인 기기에서 중앙 관리 서버로 발생하는 트래픽
업데이트된 데이터베이스로 Kaspersky Endpoint Security 11.7 for Windows 설치	390 MB	3.3 MB
네트워크 에이전트 설치	75 MB	397 KB
네트워크 에이전트와 Kaspersky Endpoint Security 11.7 for Windows의 동시 설치	459 MB	3.6 MB
패키지에 있는 데이터베이스를 업데이트하지 않은 안티 바이러스 데이터베이스의 초기 업데이트(Kaspersky Security Network 참여가 비활성화된 경우)	113 MB	1,8 MB
안티 바이러스 데이터베이스의 일일 업데이트, 안티 바이러스 데이터베이스의 초기 업데이트(Kaspersky Security Network 참여가 활성화된 경우)	22 MB	373 MB
기기에서 데이터베이스를 업데이트하기 전의 초기 동기화(정책 및 작업 전송)	382 KB	446 KB
기기에서 데이터베이스를 업데이트한 후의 초기 동기화	20 KB	157 KB
중앙 관리 서버에서의 변경 없는 상태에서의 동기화(일정에 따라)	18 KB	23 KB
그룹 정책에서 하나의 설정이 변경되었을 때 동기화(설정이 변경되는 즉시)	19 KB	20 KB
그룹 작업에서 하나의 설정이 변경되었을 대 동기화(설정이 변경되는 즉시)	14 KB	11 KB
강제 동기화	110 KB	109 KB
바이러스 탐지 이벤트(1개 바이러스)	44 KB	50 KB
바이러스 탐지 이벤트(10개 바이러스)	58 KB	77 KB
자산 관리(소프트웨어) 목록이 활성화된 후 일회성 트래픽	최대 10KB	최대 12KB
자산 관리(소프트웨어) 목록이 활성화된 경우 매일 트래픽	최대 840KB	최대 1MB

24시간 기준 평균 트래픽 사용

중앙 관리 서버와 관리 중인 기기 간의 평균 24시간 트래픽 사용량은 다음과 같습니다.

- 중앙 관리 서버에서 관리 중인 기기로 발생하는 트래픽은 840KB입니다.
- 관리 중인 기기에서 중앙 관리 서버로 발생하는 트래픽은 1MB입니다.

트래픽은 다음 조건에서 측정되었습니다.

- 관리 중인 기기에는 네트워크 에이전트 및 Kaspersky Endpoint Security 11.6 for Windows가 설치되어 있습니다.
- 이 기기에 배포 지점은 할당되지 않았습니다.
- 취약점 및 패치 관리가 활성화되지 않았습니다.
- 중앙 관리 서버와의 동기화 주기는 15분이었습니다.

기술 지원 연락처

이 섹션에서는 기술 지원을 받는 방법과 기술 지원이 제공되는 약관에 대해 설명합니다.

기술 지원을 받는 방법

Kaspersky Security Center 문서 또는 Kaspersky Security Center에 대한 정보를 제공하는 출처에서 이슈에 대한 해결 방법을 찾을 수 없다면 Kaspersky 기술 지원에 문의하십시오. 기술 지원 전문가가 Kaspersky Security Center 설치 및 사용과 관련된 질문에 대답해 드립니다.

Kaspersky는 수명주기 동안 Kaspersky Security Center에 대한 지원을 제공합니다(애플리케이션 지원 수명주기 페이지 참조). 기술 지원에 문의하기 전에 지원 규칙을 읽어보시기 바랍니다.

다음 방법 중 하나로 기술 지원에 문의할 수 있습니다:

- 기술 지원 웹사이트 방문
- Kaspersky CompanyAccount 포털에서 기술 지원 요청

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 CompanyAccount를 사용해 온라인 요청의 상태를 추적하고 요청 내역을 저장할 수도 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 참조하십시오.

중앙 관리 서버의 덤프 파일 받기

중앙 관리 서버의 덤프 파일에는 특정 시점의 중앙 관리 서버 프로세스에 대한 모든 정보가 포함되어 있습니다. 중앙 관리 서버의 덤프 파일은 %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps 폴더에 저장됩니다. Kaspersky Security Center를 사용하는 동안에 덤프 파일은 저장되며 제거 시 영구적으로 삭제됩니다. 덤프 파일은 Kaspersky로 자동 전송되지 않습니다.

중앙 관리 서버가 충돌한다면 Kaspersky 기술 지원에 문의하십시오. 기술 지원 전문가는 추가 분석을 위해 중앙 관리 서버 덤프 파일을 Kaspersky에서 전송하도록 요청할 수 있습니다.

덤프 파일에는 개인 데이터가 포함될 수 있습니다. Kaspersky로 정보를 전송하기 전에 무단 엑세스로부터 정보를 보호하는 것을 권장합니다.

애플리케이션에 대한 정보 출처

Kaspersky 웹사이트의 Kaspersky Security Center 페이지

Kaspersky 웹사이트의 Kaspersky Security Center 페이지에서 애플리케이션과 기능, 특징과 같은 일반적인 정보를 확인할 수 있습니다.

기술 자료의 Kaspersky Security Center 페이지

*기술 자료*는 Kaspersky 기술 지원 웹사이트에 있는 섹션입니다.

지식 기반의 Kaspersky Security Center 페이지에서는 애플리케이션의 구매, 설치 및 사용에 관한 유용한 정보, 권장 사항 및 자주 묻는 질문에 대한 답변을 참조할 수 있습니다.

기술 자료의 문서에서는 Kaspersky Security Center 및 기타 Kaspersky 애플리케이션과 관련된 질문에 대한 답변을 제공할 수 있습니다. 기술 자료의 문서에는 기술 지원 뉴스도 포함될 수 있습니다.

커뮤니티 웹사이트에서 Kaspersky 애플리케이션에 대해 의견 교환

질문에 대한 대답을 빨리 받지 않아도 된다면 당사 포럼에서 Kaspersky 전문가나 다른 사용자와 해당 사항에 대해 토론할 수 있습니다.

포럼에서 논의 주제를 보고, 의견을 남기고, 새 논의를 시작할 수 있습니다.

> 웹사이트 리소스를 보려면 인터넷에 연결되어 있어야 합니다.

문제에 대한 해결책을 직접 찾을 수 없다면, 기술 지원에 문의하시기 바랍니다.

용어집

Amazon EC2 인스턴스

Amazon Web Services를 사용하여 AMI 이미지를 기반으로 만들어진 가상 컴퓨터입니다.

AMI(Amazon 머신 이미지)

가상 컴퓨터를 실행하는 데 필요한 소프트웨어 구성을 포함하는 템플릿입니다. 하나의 AMI를 기반으로 여러 인스턴스를 만들 수 있습니다.

AWS IAM 액세스 키

키 ID(예: "AKIAIOSFODNN7EXAMPLE") 및 비밀 키(예: "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY")로 구성된 조합. IAM 사용자에게 속해 있으며 AWS 서비스 접근 권한을 획득하는 데 사용됩니다.

AWS Management Console

AWS 리소스를 보고 관리하기 위한 웹 인터페이스입니다. AWS Management Console은 https://aws.amazon.com/console/ 웹에서 사용할 수 있습니다.

AWS 애플리케이션 프로그램 인터페이스(AWS API)

Kaspersky Security Center에서 사용하는 AWS 플랫폼의 API입니다. 특히 AWS API 도구는 인스턴스에서 클라우드 세그먼트를 검색하고 네트워크 에이전트를 설치하는 데 사용됩니다.

Cloud Discovery

Cloud Discovery는 조직의 클라우드 인프라를 보호하는 CASB(클라우드 액세스 보안 브로커) 솔루션의 구성 요소입니다. Cloud Discovery는 클라우드 서비스에 대한 사용자 접근을 관리합니다. 예를 들어 클라우드 서비스에는 Microsoft Teams, Salesforce, Microsoft Office 365가 포함됩니다. 클라우드 서비스는 *데이터 교환*, *메신저*, *이메일* 등의 카테고리로 그룹화됩니다.

DMZ(완충 지역)

완충 지역은 전 세계 웹으로부터의 요청에 응답하는 서버가 포함된 로컬 네트워크의 세그먼트입니다. 조직 로컬 네트워크의 보안을 유지하기 위해 완충 지역으로부터의 LAN 액세스는 방화벽을 통해 보호됩니다.

HTTPS

브라우저와 웹 서버 간의 암호화를 사용하는 데이터 전송용 보안 프로토콜입니다. HTTPS는 회사 또는 재무 데이터와 같은 제한된 정보 접근 권한을 얻는 데 사용됩니다.

IAM 사용자

AWS 서비스 사용자. IAM 사용자에게는 클라우드 세그먼트 검색을 수행할 권한이 있습니다.

IAM 역할

AWS 기반 서비스에 대한 요청 권한 설정. IAM 역할은 특정 사용자 또는 그룹에 연결되지 않습니다. IAM 역할은 AWS IAM 액세스 키 없이 액세스 권한을 제공합니다. IAM 사용자, EC2 인스턴스 및 AWS 기반 애플리케이션 또는 서비스에 IAM 역할을 할당할 수 있습니다.

IAM(ID 및 접근 관리)

다른 AWS 서비스 및 리소스에 대한 사용자 접근을 관리하는 AWS 서비스.

iOS MDM 기기

iOS MDM 프로토콜을 사용해 iOS MDM 서버에 연결하는 모바일 기기. iOS 운영 체제에서 실행되는 기기는 iOS MDM 프로토콜을 통해 연결 및 관리할 수 있습니다.

iOS MDM 서버

클라이언트 기기에 설치되어 iOS 모바일 기기를 중앙 관리 서버에 연결하고 Apple Push Notifications(APNs)를 통해 iOS 모바일 기기를 관리하는 Kaspersky Security Center 구성 요소입니다.

iOS MDM 프로필

iOS 모바일 기기의 중앙 관리 서버 연결을 위한 설정 모음입니다. 모바일 기기가 중앙 관리 서버에 연결된 후 사용자가 모바일 기기에 iOS MDM 프로필을 설치합니다.

JavaScript

웹 페이지 성능을 확장하는 프로그래밍 언어입니다. JavaScript를 사용하여 만든 웹 페이지는 웹 서버의 새 데이터로 웹 페이지를 새로 고치지 않고도 인터페이스 요소 보기를 변경하거나 추가 창을 여는 등의 기능을 수행할 수 있습니다. JavaScript를 사용하여 만든 페이지를 보려면 브라우저 구성에서 JavaScript 지원을 사용하도록 설정합니다.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network는 Kaspersky 애플리케이션이 설치된 기기 사용자가 기기에서 Kaspersky Security Network로 데이터를 보내지 않고도 Kaspersky Security Network의 평판 데이터베이스와 기타 통계 데이터에 접근할 수 있도록 하는 솔루션입니다. Kaspersky Private Security Network는 다음과 같은 이유로 Kaspersky Security Network에 참여할 수 없는 기업 고객용으로 제공됩니다:

- 기기가 인터넷에 연결되어 있지 않습니다.
- 국가 또는 기업 LAN 외부로의 데이터 전송이 법률이나 기업 보안 정책에 의해 금지됩니다.

Kaspersky Security Center SHV(System Health Validator)

Kaspersky Security Center와 Microsoft NAP의 동시 작동 시 운영 체제의 운용 가능성을 확인하는 데 사용되는 Kaspersky Security Center 구성 요소입니다.

Kaspersky Security Center 관리자

Kaspersky Security Center 원격 중앙 집중식 관리 시스템을 통해 애플리케이션 작동을 관리하는 사용자입니다.

Kaspersky Security Center 업그레이드

이전 버전의 Kaspersky Security Center 애플리케이션이 설치된 기기에 최신 버전을 설치하는 절차입니다.

Kaspersky Security Center 운영자

Kaspersky Security Center를 통해 관리되는 보호 시스템의 상태 및 작동을 감시하는 사용자입니다.

Kaspersky Security Center 웹 서버

중앙 관리 서버와 함께 설치되는 Kaspersky Security Center의 구성 요소입니다. 웹 서버는 독립 실행형 설치 패키지, iOS MDM 프로필 및 공유 폴더의 파일을 네트워크를 통해 게시하도록 설계되었습니다.

Kaspersky Security Network(KSN)

파일, 웹 리소스 및 소프트웨어의 평판 정보를 지속적으로 업데이트하여 Kaspersky 데이터베이스에 접속할 수 있는 클라우드 서비스 인프라입니다. Kaspersky Security Network의 데이터를 사용하면 위협이 발생할 때 Kaspersky 애플리케이션의 처리 속도가 더욱 빨라지며 일부 보호 구성 요소의 성능이 개선되며, 정상적인 개체를 바이러스로 잘못 탐지할 가능성이 줄어듭니다.

Kaspersky 업데이트 서버

Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다.

KES 기기

Kaspersky Security Center 중앙 관리 서버에 연결되고 Kaspersky Endpoint Security for Android 앱으로 관리되는 모바일 기기.

Lightweight Nagent(LWNGT)

모바일 기기에서 Kaspersky Endpoint Security와의 상호 작용을 위한 프로토콜입니다. 모바일 프로토콜이라고도 하는 LWNGT는 모바일 기기에 네트워크 에이전트를 실제로 설치하지 않고 네트워크 에이전트의 기능을 수행합니다.

MITM 공격

중간자. 해커가 두 액세스 포인트 사이의 통신 링크를 하이재킹 및 중계하고 필요하다면 이러한 액세스 포인트 사이의 연결을 수정하는, 조직의 IT 인프라에 대한 공격입니다.

SSL

인터넷 및 로컬 네트워크에서 사용되는 데이터 암호화 프로토콜입니다. SSL(Secure Sockets Layer)은 웹 애플리케이션에서 클라이언트와 서버 간의 보안 연결을 만드는 데 사용됩니다.

UEFI 보호 기기

BIOS 수준에서 통합된 UEFI용 Kaspersky 솔루션 또는 애플리케이션이 설치된 기기. 통합 보호 기능은 시스템이 시작되는 순간부터 기기 보안을 시작하며 통합 소프트웨어가 없는 기기에 대한 보호는 보안 제품이 시작된 이후에만 기능을 시작합니다.

Windows 서버 업데이트 서비스(WSUS)

조직 네트워크의 사용자 컴퓨터에 Microsoft 애플리케이션 업데이트를 배포할 때 사용되는 애플리케이션입니다.

가상 중앙 관리 서버

클라이언트 조직의 네트워크를 관리하도록 설계된 Kaspersky Security Center의 구성 요소입니다.

가상 중앙 관리 서버는 보조 중앙 관리 서버의 특수한 형태이며 실제 중앙 관리 서버와 비교하여 다음과 같은 제약이 따릅니다.

- 가상 중앙 관리 서버는 기본 중앙 관리 서버에서만 만들 수 있습니다.
- 가상 중앙 관리 서버는 작동 시 기본 중앙 관리 서버 데이터베이스를 사용합니다. 데이터 백업 및 복원 작업과 업데이트 검사 및 다운로드 작업은 가상 중앙 관리 서버에서 지원되지 않습니다.
- 가상 서버에서는 보조 중앙 관리 서버(가상 서버 포함) 만들기가 지원되지 않습니다.

강제 설치

특정 클라이언트 기기에 소프트웨어를 설치할 수 있는 Kaspersky 애플리케이션을 원격 설치하는 방법입니다. 강제 설치를 성공적으로 완료하려면 이 작업에 사용된 계정에 클라이언트 기기에서 애플리케이션을 원격으로 실행할 수 있는 충분한 권한이 있어야 합니다. 이 방법은 Microsoft Windows 운영 체제를 실행하고 이 기능을 지원하는 기기에서 애플리케이션을 설치할 경우 권장됩니다.

강화 가이드

침입 위험을 줄이기 위한 Kaspersky Security Center 및 해당 구성 요소의 권장 사항 및 기능 세트.

공유 인증서

인증서는 사용자 모바일 기기를 식별하는 데 사용됩니다.

관리 그룹

기능별로 또는 설치된 Kaspersky 애플리케이션별로 그룹화된 기기 집합입니다. 기기는 관리의 편의를 위해 단일 항목으로 그룹화됩니다. 그룹에는 다른 그룹이 포함될 수 있습니다. 그룹에서 설치된 각 애플리케이션에 대해 그룹 정책과 그룹 작업을 만들 수 있습니다.

관리 중인 기기

관리 그룹에 포함된 회사 네트워크 내 기기입니다.

관리 콘솔

Windows 기반 Kaspersky Security Center(MMC 기반 관리 콘솔이라고도 함)의 구성 요소입니다. 이 구성 요소는 중앙 관리 서버 및 네트워크 에이전트의 관리 서비스에 대한 사용자 인터페이스를 제공합니다.

관리 플러그인

관리 콘솔을 통해 애플리케이션 관리를 위한 인터페이스를 제공하는 전문 구성 요소입니다. 각 애플리케이션마다 자체 플러그인이 있습니다. 플러그인은 Kaspersky Security Center를 사용하여 관리할 수 있는 모든 Kaspersky 애플리케이션에 포함됩니다.

관리자 권한

한 Exchange 조직 내에서 Exchange 개체를 관리하는 데 필요한 사용자의 권한 수준입니다.

관리자 워크스테이션

관리 콘솔을 설치했거나 Kaspersky Security Center 웹 콘솔을 여는 데 사용한 기기. 이 구성 요소는 Kaspersky Security Center 관리 인터페이스를 제공합니다.

관리자 워크스테이션은 Kaspersky Security Center의 서버 부분을 구성하고 관리하는 데 사용됩니다. 관리자의 워크스테이션을 사용해 관리자는 Kaspersky 애플리케이션을 기반으로 회사 LAN의 중앙 집중식 안티 바이러스 보호 시스템을 구축하고 관리합니다.

구성 프로필

iOS MDM 모바일 기기를 대상으로 하는 설정 및 제한 모음이 포함된 정책입니다.

그룹 작업

관리 그룹에 대해 정의된 작업과 해당 관리 그룹에 포함된 모든 클라이언트 기기에서 수행되는 작업.

기기 소유자

기기 소유자는 기기와 어떤 작업 수행을 할 때 관리자가 연락할 수 있는 사용자입니다.

내부 사용자 계정

내부 사용자 계정은 가상 중앙 관리 서버 작업에 사용됩니다. Kaspersky Security Center는 애플리케이션의 내부 사용자에게 실제 사용자의 권한을 부여합니다.

내부 사용자의 계정이 생성되어 Kaspersky Security Center 내에서만 사용됩니다. 내부 사용자에 대한 어떤 데이터도 운영 체제로 전송되지 않습니다. Kaspersky Security Center에서 내부 사용자를 인증합니다.

네트워크 보호 상태

회사 네트워크의 기기 보안을 정의하는 현재 보호 상태입니다. 네트워크 보호 상태에는 설치된 보안 제품, 라이센스 키 사용, 탐지된 위협의 수와 유형 등이 포함됩니다.

네트워크 안티 바이러스 보호

바이러스와 스팸이 조직 네트워크에 침입할 위험을 줄이며 네트워크 공격, 피싱 및 기타 위협을 방지하는 기술적 및 조직적 방법의 집합입니다. 보안 제품과 서비스를 사용하고, 회사 데이터 보안 정책을 적용 및 준수하면 네트워크 보안 수준이 높아집니다.

네트워크 에이전트

중앙 관리 서버와 Kaspersky 애플리케이션 간의 상호 작용을 위해 특정 네트워크 노드(워크스테이션 또는 서버)에 설치되는 Kaspersky Security Center의 구성 요소입니다. 이 구성요소는 Kaspersky의 모든 Microsoft® Windows® 용 애플리케이션에 공통으로 적용됩니다. Unix 같은 OS 및 Mac 시스템용으로 개발된 Kaspersky 애플리케이션에는 별도의 네트워크 에이전트 버전이 있습니다.

네트워크 위치 인식(NLA)

운영 체제가 현재 네트워크를 식별할 수 있도록 지원하는 Windows 서비스입니다. NLA는 네트워크 변경 사항을 감지하고 기기의 보안 구성을 조정합니다.

라이센스 기간

애플리케이션 기능에 대한 접근 및 추가 서비스를 사용할 수 있는 권한이 제공되는 기간입니다. 사용할 수 있는 서비스는 라이센스 유형에 따라 달라집니다.

로컬 설치

회사 네트워크의 기기에 보안 제품을 설치하는 작업입니다. 보안 제품 배포 패키지에서 수동 설치를 시작하거나 게시된 설치 패키지를 기기에 미리 다운로드한 다음 수동으로 시작한다고 가정합니다.

로컬 작업

단일 기기에서 정의되어 실행되는 작업입니다.

모바일 기기 서버

관리 콘솔을 통해 모바일 기기에 대한 접근 및 관리 기능을 제공하는 Kaspersky Security Center의 한 구성 요소입니다.

바이러스 급증 기준 임계값

제한된 시간 내에 특정 유형에 허용되는 최대 이벤트 수입니다. 이 숫자를 초과하면 바이러스 활동이 증가하고 바이러스 급증 위협이 있는 것으로 해석됩니다. 이 기능은 관리자가 바이러스 공격 보안위협을 적시에 처리할 수 있도록 하므로 바이러스가 급증하는 경우 매우 중요한 역할을 합니다.

배포 지점

네트워크 에이전트가 설치되어 있으며 업데이트 배포, 애플리케이션 원격 설치, 관리 그룹 및/또는 브로드캐스팅 도메인 내에 있는 컴퓨터에 대한 정보 획득 등에 사용되는 컴퓨터입니다. 배포 지점은 업데이트 배포 시 중앙 관리 서버에서의 부하를 줄이고 네트워크 트래픽을 최적화하기 위해 고안되었습니다. 배포 지점은 중앙 관리 서버에 의해 자동으로 또는 관리자에 의해 수동으로 할당될 수 있습니다. 배포 지점의 이전 명칭은 업데이트 에이전트였습니다.

백업 폴더

백업 유틸리티를 사용하여 만든 중앙 관리 서버 데이터 복사본을 저장할 수 있는 특수 폴더입니다.

보호 상태

컴퓨터 보안 레벨을 반영하는 현재 보호 상태입니다.

복원

격리 저장소 또는 백업 저장소에서 개체가 격리, 치료 또는 삭제되기 전 저장되었던 원래 폴더 또는 사용자 정의 폴더로 원래 개체를 재배치하는 것입니다.

브로드캐스트 도메인

모든 노드가 OSI (Open Systems Interconnection Basic Reference Model) 수준에서 브로드캐스팅 채널을 사용해 데이터를 교환할 수 있는 네트워크의 논리적인 영역.

비-호환 애플리케이션

Kaspersky Security Center를 통한 관리를 지원하지 않는 Kaspersky 애플리케이션 또는 타사 개발사의 안티 바이러스 애플리케이션입니다.

사용 가능한 업데이트

일정 기간 동안 누적된 긴급 업데이트, 애플리케이션 아키텍처 변경 사항 등을 포함하는 Kaspersky 애플리케이션 모듈용 업데이트 세트입니다.

서비스 공급업체 관리자

안티 바이러스 보호 서비스 공급업체의 직원입니다. 이 관리자는 Kaspersky 안티 바이러스 제품을 기반으로 안티 바이러스 보호 시스템에 대한 설치 및 유지보수 작업을 수행하는 동시에 고객에게 기술 지원을 제공합니다.

설치 패키지

Kaspersky Security Center 원격 관리 시스템을 사용하여 Kaspersky 애플리케이션을 원격으로 설치하기 위해 만들어진 파일입니다. 설치 패키지에는 애플리케이션을 설치하고 설치 후 즉시 이를 실행하는데 필요한 설정 범위가 있습니다. 설정은 애플리케이션 기본 값에 해당합니다. 설치 패키지는 애플리케이션 배포 키트에 포함된 .kpd 및 .kud 확장자 파일을 사용해 만들어 집니다.

수동 설치

배포 패키지에서 회사 네트워크의 기기에 보안 제품을 설치하는 작업입니다. 수동 설치 시에는 관리자 또는 다른 IT 전문가의 도움이 필요합니다. 일반적으로는 원격 설치 완료 시 오류가 발생한 경우 수동 설치를 수행합니다.

악성 코드 급증

기기를 바이러스에 감염시키려고 하는 일련의 적극적인 시도입니다.

안티 바이러스 데이터베이스

Kaspersky에서 안티 바이러스 데이터베이스를 배포할 당시에 컴퓨터 보안 위협으로 인식한 정보가 담긴 데이터베이스입니다. 안티 바이러스 데이터베이스의 항목을 통해 검사한 개체에서 악성 코드를 탐지할 수 있습니다. 안티 바이러스 데이터베이스는 Kaspersky 전문가에 의해 만들어져 매 시간 업데이트됩니다.

안티 바이러스 보호 서비스 공급업체

Kaspersky 솔루션을 기반으로 클라이언트 조직에 안티 바이러스 보호 서비스를 제공하는 조직입니다.

애플리케이션 직접 관리

로컬 인터페이스를 통한 애플리케이션 관리를 의미합니다.

앱 마켓

Kaspersky Security Center 구성 요소. 앱 마켓은 사용자가 소유한 Android 기기에 애플리케이션을 설치하기 위해 사용됩니다. 앱 마켓은 Google Play에 있는 애플리케이션으로의 링크와 애플리케이션의 APK 파일을 게시합니다.

업데이트

Kaspersky 업데이트 서버에서 검색된 새로운 파일(데이터베이스 또는 애플리케이션 모듈)을 대체 또는 추가하는 절차입니다.

연결 게이트웨이

*연결 게이트웨이*는 특수 모드에서 작동하는 네트워크 에이전트입니다. 연결 게이트웨이는 다른 네트워크 에이전트의 연결을 수락하고 서버와의 자체 연결을 통해 이를 중앙 관리 서버로 터널링합니다. 일반 네트워크 에이전트와 달리 연결 게이트웨이는 중앙 관리 서버에 대한 연결을 설정하지 않고 중앙 관리 서버의 연결을 기다립니다.

원격 설치

Kaspersky Security Center에서 제공하는 도구를 통해 Kaspersky 애플리케이션을 설치합니다.

유료 애플리케이션 그룹

관리자(예: 공급사)가 지정한 기준에 따라 생성된 애플리케이션 그룹으로 이 분류에 따라 클라이언트 기기 설치 현황에 대한 통계를 유지합니다.

이벤트 심각도

이벤트 속성은 Kaspersky 애플리케이션을 작동할 때 결정됩니다. 다음과 같은 심각도가 있습니다.

- 심각 이벤트
- 기능 실패
- 경고
- 정보

같은 유형의 이벤트라도 이벤트가 발생한 상황에 따라 다른 심각도를 가집니다.

이벤트 저장소

Kaspersky Security Center에서 발생하는 이벤트에 대한 정보 저장을 전담하는 중앙 관리 서버 데이터베이스의 일부입니다.

인증 에이전트

암호화된 하드 드라이브에 접근하고 부팅 가능한 하드 드라이브 암호화 후 운영 체제를 로드하기 위한 인증을 완료하기 위한 인터페이스입니다.

작업

Kaspersky 애플리케이션이 수행하는 기능은 다음과 같은 작업으로 구현됩니다: 실시간 파일 보호, 컴퓨터 전체 검사 및 데이터베이스 업데이트.

작업 설정

각 작업 유형과 관련된 애플리케이션 설정입니다.

정책

정책은 애플리케이션의 설정을 결정하고 관리 그룹 내의 컴퓨터에 설치된 애플리케이션을 구성하는 기능을 관리합니다. 각각의 애플리케이션에 대해 개별 정책을 만들어야 합니다. 각 관리 그룹 내에 설치된 각 애플리케이션을 위한 여러 정책을 만들 수 있지만 한 번에 하나의 정책만 관리 그룹 내의 각 애플리케이션에 적용할 수 있습니다.

중앙 관리 서버

회사 네트워크에 설치된 모든 Kaspersky 애플리케이션에 대한 정보가 중앙 집중식으로 저장되는 Kaspersky Security Center 구성 요소입니다. 이러한 애플리케이션을 관리하는 데에도 사용됩니다.

중앙 관리 서버 데이터 백업

백업 유틸리티를 사용한 백업 및 이후 복원을 위해 중앙 관리 서버 데이터를 복사하는 것입니다. 이 유틸리티는 다음 내용을 저장할 수 있습니다:

- 중앙 관리 서버의 데이터베이스(중앙 관리 서버에 저장된 정책, 작업, 애플리케이션 설정, 이벤트)
- 관리 그룹 및 클라이언트 기기 구조에 관한 구성 정보

- 애플리케이션의 원격 설치를 위한 설치 파일 저장소(폴더의 컨텐츠: 패키지, 업데이트 제거)
- 중앙 관리 서버 인증서

중앙 관리 서버 데이터 복원

백업 유틸리티를 사용하여 백업에 저장된 정보로부터 중앙 관리 서버 데이터를 복원하는 것입니다. 이 유틸리티는 다음 내용을 복원할 수 있습니다:

- 중앙 관리 서버의 데이터베이스(중앙 관리 서버에 저장된 정책, 작업, 애플리케이션 설정, 이벤트)
- 관리 그룹 및 클라이언트 기기 구조에 관한 구성 정보
- 애플리케이션의 원격 설치를 위한 설치 파일 저장소(폴더의 컨텐츠: 패키지, 업데이트 제거)
- 중앙 관리 서버 인증서

중앙 관리 서버 인증서

중앙 관리 서버가 다음 목적으로 사용하는 인증서:

- MMC 기반 관리 콘솔 또는 Kaspersky Security Center 웹 콘솔 연결 시 중앙 관리 서버 인증
- 관리 중인 기기에서 중앙 관리 서버와 네트워크 에이전트 간의 안전한 상호 작용
- 기본 중앙 관리 서버를 보조 중앙 관리 서버에 연결 시 중앙 관리 서버 인증

이 인증서는 중앙 관리 서버를 설치할 때 자동으로 생성되어 중앙 관리 서버에 저장됩니다.

중앙 관리 서버 클라이언트(클라이언트 기기)

네트워크 에이전트가 설치되고 관리되는 Kaspersky 애플리케이션이 실행 중인 기기, 서버 또는 워크스테이션입니다.

중앙 집중식 애플리케이션 관리

Kaspersky Security Center에서 제공하는 관리 서비스를 사용하여 애플리케이션을 원격으로 관리하는 것입니다.

추가(또는 예비) 라이센스 키

현재 사용하지 않고 있는 애플리케이션의 사용 권한을 인증하는 키입니다.

취약점

시스템이나 애플리케이션에 침투하여 무결성을 손상시키기 위해 악성 코드 제작자에 의해 악용될 수 있는 운영 체제 또는 애플리케이션의 결함입니다. 시스템의 취약점이 많으면 바이러스가 시스템에 침투하여 시스템 및 설치된 애플리케이션의 정상적인 작동을 방해할 수 있으므로 시스템이 안정적이지 못하게 됩니다.

클라우드 환경

클라우드 플랫폼을 기반으로 하며 네트워크에 통합되어 있는 가상 컴퓨터 및 기타 가상 리소스입니다.

클라이언트 관리자

안티 바이러스 보호 상태 모니터링을 담당하는 클라이언트 조직의 직원입니다.

키 파일

체험판 또는 사용 라이센스로 Kaspersky 애플리케이션을 사용할 수 있게 하는 xxxxxxxx.key 형식의 파일입니다.

특정 기기 작업

임의 관리 그룹에 속해 있는 한 클라이언트 기기 집합에 할당되는 작업으로, 해당 기기에서 수행됩니다.

패치 심각도

패치의 특성. Microsoft 패치와 타사 패치의 심각도는 다음과 같은 5가지입니다:

- 심각
- 높음
- 중간
- 낮음
- 알 수 없음

타사 패치 또는 Microsoft 패치의 심각도는 해당 패치가 수정하는 취약점 가운데 심각도가 가장 높은 취약점에 따라 결정됩니다.

프로그램 설정

애플리케이션 설정은 모든 종류의 작업에 공통적으로 적용되며, 애플리케이션 성능 설정, 보고 설정 및 백업 설정과 같은 애플리케이션의 전반적인 작업을 제어하는 역할을 합니다.

프로비저닝 프로필

iOS 모바일 기기에서 애플리케이션을 운영하기 위한 설정 집합입니다. 프로비저닝 프로필에는 라이센스에 대한 정보가 포함되어 있으며 특정 애플리케이션에 연결됩니다.

홈 중앙 관리 서버

홈 중앙 관리 서버는 네트워크 에이전트를 설치할 때 지정했던 중앙 관리 서버입니다. 홈 중앙 관리 서버는 네트워크 에이전트 연결 프로필 설정에서 사용할 수 있습니다.

활성 라이센스 키

현재 애플리케이션에서 사용 중인 키입니다.

타사 코드 정보

타사 코드에 대한 정보는 애플리케이션 설치 폴더에 있는 legal_notices.txt라는 파일에서 확인할 수 있습니다.

상표 고지

등록된 상표 및 서비스 마크는 해당 소유주의 재산입니다.

Adobe, Acrobat, Flash, Shockwave, PostScript는 미국 및/또는 기타 국가에서 Adobe의 상표 또는 등록 상표입니다.

AMD와 AMD64는 Advanced Micro Devices, Inc의 상표 또는 등록 상표입니다.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace는 Amazon.com, Inc. 또는 그 계열사의 상표입니다.

Apache은 미국 및/또는 기타 국가에서 Apache Software Foundation의 등록 상표 또는 상표입니다.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, Touch ID는 Apple Inc.의 상표입니다.

Arm은 미국 및/또는 기타 지역에서 Arm Limited(또는 그 자회사)의 등록 상표입니다.

Bluetooth 단어, 표시 및 로고는 Bluetooth SIG, Inc.의 소유입니다.

Ubuntu, LTS는 Canonical Ltd.의 등록 상표입니다.

Cisco Systems, Cisco, Cisco Jabber, IOS는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 자회사의 등록 상표 또는 상표입니다.

Citrix, XenServer는 미국 및/또는 기타 국가에서 Cloud Software Group, Inc. 및/또는 그 자회사의 등록 상표 또는 상표입니다.

Corel은 캐나다, 미국 및/또는 기타 국가에서 Corel Corporation 및/또는 해당 자회사의 상표 또는 등록 상표입니다.

Cloudflare, Cloudflare 로고, Cloudflare Workers는 미국 및 기타 관할 지역에서 Cloudflare, Inc.의 상표 및/또는 등록 상표입니다.

Dropbox는 Dropbox, Inc.의 상표입니다.

Radmin은 Famatech의 등록 상표입니다.

Firebird는 Firebird 재단의 등록 상표입니다.

Foxit은 Foxit Corporation의 등록 상표입니다.

FreeBSD는 FreeBSD 재단의 등록 상표입니다.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS, YouTube는 Google LLC의 상표입니다.

EulerOS, FusionCompute, FusionSphere는 Huawei Technologies Co., Ltd.의 상표입니다.

Intel, Core, Xeon은 Intel Corporation 또는 그 자회사의 상표입니다.

IBM, QRadar는 전 세계 많은 사법기관에 등록된 International Business Machines Corporation의 상표입니다.

Node.js는 Joyent, Inc.의 상표입니다.

Linux는 미국 및 기타 국가에서 Linus Torvalds의 등록 상표입니다.

Logitech은 미국 및/또는 기타 국가에서 Logitech의 등록 상표 또는 상표입니다.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista, Windows Azure는 Microsoft 그룹의 상표입니다.

CVE는 The MITRE Corporation의 등록 상표입니다.

Mozilla, Firefox, Thunderbird는 미국 및 기타 국가에서 Mozilla Foundation의 상표입니다.

Novell은 미국 및 기타 국가에서 Novell Enterprises Inc.의 등록 상표입니다.

NetWare는 미국 및 기타 국가에서 Novell Inc.의 등록 상표입니다.

OpenVPN은 OpenVPN, Inc.의 등록 상표입니다.

OpenSSL은 OpenSSL 소프트웨어 재단이 소유한 상표입니다.

Oracle, Java, JavaScript 및 TouchDown는 Oracle 및/또는 그 계열사의 등록 상표입니다.

Parallels, Parallels 로고, Coherence는 Parallels International GmbH의 상표 또는 등록 상표입니다.

Chef는 미국 및/또는 기타 국가에서 Progress Software Corporation 및/또는 해당 자회사의 상표 또는 등록 상표입니다.

Puppet은 Puppet, Inc.의 상표 또는 등록 상표입니다.

Python은 Python Software Foundation의 상표 또는 등록 상표입니다.

Red Hat, CentOS, Fedora, Red Hat Enterprise Linux는 미국 및 기타 국가에서 Red Hat, Inc. 또는 해당 자회사의 등록 상표입니다.

Ansible은 미국 및 기타 국가에서 Red Hat, Inc.의 등록 상표입니다.

CentOS는 미국 및 기타 국가에서 Red Hat, Inc. 또는 해당 자회사의 상표 또는 등록 상표입니다.

BlackBerry는 Research In Motion Limited의 소유이고 미국에 등록되어 있으며 기타 국가에서 등록 출원 중이거나 등록되어 있을 수 있습니다.

Rocky Linux는 The Rocky Enterprise Software Foundation의 상표입니다.

SAMSUNG은 미국 또는 기타 국가에서 SAMSUNG의 상표입니다.

Debian은 Software in the Public Interest, Inc.의 등록 상표입니다.

Splunk, SPL은 미국 및 기타 국가에서 Splunk Inc.의 상표 및 등록 상표입니다.

SUSE는 미국 및 기타 국가에서 SUSE LLC의 등록 상표입니다.

Symbian 상표는 Symbian Foundation Ltd. 소유입니다.

OpenAPI는 Linux Foundation의 상표입니다.

UNIX는 미국 및 기타 국가에서 X/Open Company Limited를 통해 독점 사용이 허가된 등록 상표입니다.

Zabbix는 Zabbix SIA의 등록 상표입니다.

알려진 문제

Kaspersky Security Center 웹 콘솔에는 애플리케이션 작동에 있어 중요한 영향을 주지는 않는 여러 제한이 있습니다:

- Microsoft Windows XP에 네트워크 에이전트가 설치되어 있는 경우 관리 중인 애플리케이션 구성 요소에 대한 정보를 사용할 수 없습니다.
- 활성화 코드를 입력하여 EDR Optimum에 대한 라이센스 키를 중앙 관리 서버 저장소에 추가한 경우에만 콘솔에서 메인 메뉴의 **경고** 섹션에 있는 **모니터링 및 보고** 하위 섹션을 표시합니다.
- 암호화의 강도를 높이려면 SHA-2를 사용하여 중앙 관리 서버 인증서를 서명해야 하고 키 길이가 2048 이상이어야 합니다. 인증서를 재발급해야 한다면 Kaspersky Security Center 기술 자료를 참조하십시오.
- Kaspersky Security Center 15.1 웹 콘솔에서 **N일마다** 및 **요일별** 스케줄 설정을 사용하여 작업을 생성한 다음 Kaspersky Security Center 웹 콘솔 또는 Kaspersky Security Center 관리 콘솔에서 이 작업을 열면(예를 들어, 작업이 Linux 기반과 Windows 기반일 수 있는 보조 중앙 관리 서버에도 적용되어 있으면), 스케줄 설정이 잘못 표시되거나 오류가 발생할 수 있습니다.
- Kaspersky Security Center 웹 콘솔에서 SIEM 시스템으로 내보내기를 구성하고 UDP 프로토콜을 선택했을 때, **연결 확인** 버튼을 클릭하면 오류가 발생합니다. 이는 UDP가 연결을 설정하지 않아 데이터 전달을 보장할 수 없기 때문입니다.
- Astra Linux Special Edition RUSB.10015-01(작업 업데이트 1.7)을 실행하는 Arm 아키텍처 기반 기기에서 네트워크 에이전트 제거 작업을 실행하면, 네트워크 에이전트를 제거해도 작업 목록의 현재 진행에서 작업 상태가 멈춰있습니다.
- Exchange ActiveSync는 더는 지원하지 않지만 Kaspersky Device Management for iOS 정책의 속성 창에 여전히 **EAS 기기 설정** 섹션이 포함되어 있습니다.
- 기기 이름에 키릴 문자가 포함된 기기에 Kaspersky Security Center를 설치하고 중앙 관리 서버에서 KSN 프록시를 활성화하면, HTTPS를 통한 KSN 연결에 실패합니다.
- **사용자 계정 수정 권한 확인을 위한 인증 요청** 옵션이 설정된 사용자 계정의 속성을 변경하려고 한 다음 **취소** 창에서 **계정 보호**를 클릭하면, 예기치 않은 오류가 발생합니다.
- 기기의 시간이나 시간대를 변경한다면 Kaspersky Security Center 웹 콘솔 서비스를 다시 시작해야 합니다.
- 기기에서 프록시를 사용하고 프록시 환경 변수를 설정하면, Kaspersky Security Center 웹 콘솔 설치 프로그램이 중지될 수 있습니다.
- *배포 지점 저장소로 업데이트 다운로드* 또는 *업데이트 확인* 작업을 가져오면 **작업을 할당할 기기 선택** 옵션이 활성화됩니다. 이러한 작업은 기기 조회나 특정 기기에 할당할 수 없습니다. *배포 지점 저장소로 업데이트 다운로드* 또는 특정 기기에 *업데이트 확인* 작업을 할당하면 작업을 가져올 때 오류가 발생합니다.
- 네트워크 에이전트 버전 15가 설치된 Linux 배포 지점을 사용하여 Active Directory 검색을 수행하는 경우 주소 및 사용자 자격 증명을 지정한 Active Directory 도메인만 검색할 수 있습니다. 현재 Active Directory 도메인 및 Active Directory 도메인 포레스트에 대한 검색을 사용할 수 없습니다.
- Windows 네트워크 검색을 실행한 후 클라이언트 기기를 찾지 못할 수 있습니다.
- **보조 중앙 관리 서버 추가 마법사**에서 향후 보조 서버 인증을 위해 2단계 인증이 활성화된 계정을 지정하면 마법사에서 오류가 발생합니다. 이 문제를 해결하려면 2단계 인증이 비활성화된 계정을 지정하거나 향후 보조 서버에서 계층을 생성하십시오.

- Kaspersky Security Center 웹 콘솔에 로그인한 상태로 도메인 인증을 사용하여 가상 중앙 관리 서버로 연결을 지정한 후 로그아웃했다가 다시 기본 중앙 관리 서버로 로그인을 시도하면, Kaspersky Security Center 웹 콘솔이 가상 중앙 관리 서버로 연결합니다. 기본 중앙 관리 서버에 연결하려면 브라우저를 다시 엽니다.

- 빠른/전체 Windows 네트워크 검색 시 빈 결과를 반환합니다.

- ID 및 액세스 관리와 함께 Kaspersky Security Center 웹 콘솔을 설치한 다음 Kaspersky Security Center 웹 콘솔용 중앙 관리 서버를 변경해도 ID 및 액세스 관리가 새 중앙 관리 서버에 대한 정보를 가져오지 않습니다.

- 관리 중인 장치에 네트워크 어댑터가 둘 이상 있을 시, 장치가 중앙 관리 서버에 연결하는 데 사용하지 않는 네트워크 어댑터의 MAC 주소 정보를 중앙 관리 서버에 보냅니다.

- CEF 데이터 형식이 선택되면 SIEM에 대한 테스트 연결이 실패합니다.

- NTLM 인증은 보호되는 사용자 그룹 내의 사용자 계정에는 작동하지 않습니다.