목차

Kaspersky Security Center 14 Linux 도움말

새로운 기능

최신 출시 애플리케이션의 새로운 기능에 대해 알아봅니다.

Kaspersky 애플리케이션. 라이센스 및 활성화

몇 가지 단계를 수행하여 Kaspersky 애플리케이션을 활성화합니다.

하드웨어 및 소프트웨어 요구 사항

지원되는 운영 체제와 애플리케이션 버전을 확인합니다.

네트워크 보호 구성

조직의 보안을 관리합니다.

설치
중앙 관리 서버 및 Kaspersky Security Center 14 웹 콘솔을 설치합니다.

네트워크에 연결된 기기 발견
조직 네트워크의 기존 기기와 새 기기를 발견합니다.

Kaspersky 애플리케이션. 중앙 집중식 배포
Kaspersky 애플리케이션 배포.

Kaspersky 애플리케이션. 데이터베이스 및 소프트웨어 모듈 업데이트
보호 시스템의 신뢰성을 유지합니다.

모니터링 및 보고
인프라, 보호 상태 및 통계를 확인합니다.

배포 지점 및/또는 연결 게이트웨이 조정
배포 지점을 구성합니다.

새로운 기능

Kaspersky Security Center 14 Linux

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

- 이제 *중앙 관리 서버 저장소 업데이트 다운로드* 작업 외에 *배포 지점의 저장소로 업데이트 다운로드* 작업으로도 Kaspersky 보안 애플리케이션용 안티 바이러스 데이터베이스를 다운로드할 수 있습니다.
- 관리 중인 장치의 안티 바이러스 데이터베이스 및 애플리케이션 모듈은 중앙 관리 서버 또는 배포 지점을 통해 전파 및 업데이트될 수 있습니다. 조직에 가장 적합한 업데이트 구성표를 선택하여 중앙 관리 서버의 부하를 줄이고 기업 네트워크의 데이터 트래픽을 최적화할 수 있습니다.
- Kaspersky Security Center는 Kaspersky 업데이트 서버에서 Kaspersky 보안 애플리케이션이 요청한 업데이트만 다운로드합니다. 이렇게 하면 다운로드할 데이터의 크기가 줄어듭니다.
- 이제 diff 파일 기능을 사용하여 안티 바이러스 데이터베이스 및 소프트웨어 모듈을 다운로드할 수 있습니다. 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.
- *업데이트 검증* 작업이 추가되었습니다. 이 작업을 사용하면 관리 중인 장치에 업데이트를 설치하기 전에 다운로드한 업데이트의 작동 가능성과 오류를 자동 확인할 수 있습니다.
- 이제 Kaspersky Security Center에서 Kaspersky Industrial Cybersecurity for Linux Nodes 1.3을 지원합니다.

Kaspersky Security Center Linux 정보

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

Kaspersky Security Center Linux(Kaspersky Security Center라고도 함)는 완전한 Linux 환경에 대한 요구 사항을 충족하기 위해 Linux 기반 중앙 관리 서버를 사용하여 Linux® 장치 보호를 배포 및 관리하도록 설계되었습니다.

Kaspersky Security Center Linux로 기업 네트워크의 장치에 Kaspersky 보안 애플리케이션을 설치하고, 검사 및 업데이트 작업을 원격 실행하며, 관리 중인 애플리케이션의 보안 정책을 관리할 수 있습니다. 관리자는 기업 장치 상태의 스냅샷, 상세 보고서 및 보호 정책의 세밀한 설정을 제공하는 상세한 대시 보드를 사용할 수 있습니다.

Windows® 기반 중앙 관리 서버가 있는 Kaspersky Security Center와 비교하여, Kaspersky Security Center Linux에는 다른 기능 세트가 있습니다.

Kaspersky Security Center Linux는 다양한 조직에서 장치 보호 업무를 맡은 회사 네트워크 관리자와 직원을 대상으로 하는 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.
- Kaspersky 및 다른 소프트웨어 공급업체에서 애플리케이션 설치를 원격으로 수행.
- 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.
- 조직의 네트워크에 연결된 하드웨어의 인벤토리 수행.

보안 애플리케이션이 검역소 또는 백업으로 이동한 파일을 중앙에서 관리하고, 보안 애플리케이션이 처리를 연기한 파일도 관리합니다.
Kaspersky(https://www.kaspersky.com 등)나 파트너 회사를 통해 Kaspersky Security Center Linux를 구매할 수 있습니다.

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

하드웨어 및 소프트웨어 요구 사항

중앙 관리 서버

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.

지원되는 운영 체제는 다음과 같습니다:

- Debian GNU/Linux 11.x (Bullseye) 32비트/64비트
- Debian GNU/Linux 10.x (Buster) 32비트/64비트
- Debian GNU/Linux 9.x (Stretch) 32비트/64비트
- Ubuntu Server 20.04 LTS (Focal Fossa) 64비트
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64비트
- CentOS 7.x 64비트
- Red Hat Enterprise Linux Server 8.x 64비트
- Red Hat Enterprise Linux Server 7.x 64비트
- SUSE Linux Enterprise Server 12(모든 서비스 팩) 64비트
- SUSE Linux Enterprise Server 15 (모든 서비스 팩) 64비트
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7(폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
- Astra Linux Special Edition, 1.6 버전 (폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
- Astra Linux Common Edition 2.12 64비트
- ALT Server 10 64비트
- ALT Server 9.2 64비트
- ALT 8 SP Server (LKNV.11100-01) 64비트
- ALT 8 SP Server (LKNV.11100-02) 64비트
- ALT 8 SP Server (LKNV.11100-03) 64비트
- Oracle Linux 7 64비트
- Oracle Linux 8 64비트
- RED OS 7.3 Server 64비트
- RED OS 7.3 Certified Edition 64비트

지원되는 가상 플랫폼은 다음과 같습니다.

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64비트
- Microsoft Hyper-V Server 2012 R2 64비트

- Microsoft Hyper-V Server 2016 64비트
- Microsoft Hyper-V Server 2019 64비트
- Microsoft Hyper-V Server 2022 64비트
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- 커널 기반 가상 머신. 다음 운영 체제를 지원합니다.
  - ALT 8 SP Server (LKNV.11100-01) 64비트
  - ALT Server 10 64비트
  - Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7(폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
  - Debian GNU/Linux 11.x (Bullseye) 32비트/64비트
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64비트
  - RED OS 7.3 Server 64비트
  - RED OS 7.3 Server 64비트

다음 데이터베이스 서버가 지원됩니다(다른 기기에 설치할 수 있음).

- MySQL 5.7 Community 32비트/64비트
- MySQL 8.0 32비트/64비트
- MariaDB 10.5.x 32비트/64비트
- MariaDB 10.4.x 32비트/64비트
- MariaDB 10.3(빌드 10.3.22 이상) 32비트/64비트
- MariaDB Server 10.3 32비트/64비트 InnoDB 스토리지 엔진
- MariaDB Galera Cluster 10.3 32비트/64비트 InnoDB 스토리지 엔진
- MariaDB 10.1(빌드 10.1.30 이상) 32비트/64비트

Kaspersky Security Center 14 웹 콘솔

Kaspersky Security Center 14 웹 콘솔 서버

최소 하드웨어 요구 사항:

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

다음 운영 체제 중 하나(64비트 버전만 해당):

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x

- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (모든 서비스 팩)
- SUSE Linux Enterprise Server 15 (모든 서비스 팩)
- SUSE Linux Enterprise Desktop 15(서비스 팩 3) ARM 64비트
- EulerOS 2.0 SP8 ARM
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7(폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함)
- Astra Linux Special Edition, 1.6 버전 (폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함)
- Astra Linux Common Edition, 버전 2.12
- ALT Server 10
- ALT Server 9.2
- ALT 8 SP Server (LKNV.11100-01)
- ALT 8 SP Server (LKNV.11100-02)
- ALT 8 SP Server (LKNV.11100-03)
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

가상화 플랫폼 중 커널 기반 가상 머신은 다음 운영 체제에서 지원됩니다.

- ALT 8 SP Server (LKNV.11100-01) 64비트
- ALT Server 10 64비트
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7(폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
- Debian GNU/Linux 11.x (Bullseye) 32비트/64비트
- Ubuntu Server 20.04 LTS (Focal Fossa) 64비트
- RED OS 7.3 Server 64비트
- RED OS 7.3 Certified Edition 64비트

클라이언트 기기

클라이언트 기기에서 브라우저만 있으면 Kaspersky Security Center 14 웹 콘솔을 사용할 수 있습니다.

기기의 하드웨어 및 소프트웨어 요구 사항은 Kaspersky Security Center 14 웹 콘솔에 사용되는 브라우저의 요구 사항과 동일합니다.

브라우저:

- Mozilla Firefox Extended Support Release 91.8.0 이상(2022년 4월 5일에 배포된 91.8.0)
- Mozilla Firefox 릴리즈 버전 99.0 이상 (2022년 4월 5일에 출시된 99.0)
- Google Chrome 100.0.4896.88 이상(공식 빌드)
- Microsoft Edge 100 이상
- macOS의 Safari 15

네트워크 에이전트

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 장치에 대한 소프트웨어 요구 사항: Perl 언어 인터프리터 버전 5.10 이상이 설치되어 있어야 합니다.

지원되는 운영 체제는 다음과 같습니다:

- Debian GNU/Linux 11.x (Bullseye) 32비트/64비트
- Debian GNU/Linux 10.x (Buster) 32비트/64비트
- Debian GNU/Linux 9.x (Stretch) 32비트/64비트
- Ubuntu Server 20.04 LTS (Focal Fossa) 32비트/64비트
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64비트
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32비트/64비트
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32비트/64비트
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32비트/64비트
- CentOS 8.x 64비트
- CentOS 7.x 64비트
- CentOS 7.x ARM 64비트
- Red Hat Enterprise Linux Server 8.x 64비트
- Red Hat Enterprise Linux Server 7.x 64비트
- Red Hat Enterprise Linux Server 6.x 32비트/64비트
- SUSE Linux Enterprise Server 12 (모든 서비스 팩) 64비트
- SUSE Linux Enterprise Server 15 (모든 서비스 팩) 64비트
- SUSE Linux Enterprise Desktop 15 (모든 서비스 팩) 64비트
- SUSE Linux Enterprise Desktop 15 (서비스 팩 3) ARM 64비트
- openSUSE 15 64비트
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64비트
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7(폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
- Astra Linux Special Edition, 1.6 버전 (폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
- Astra Linux Common Edition 2.12 64비트
- Astra Linux Special Edition 4.7 ARM
- ALT Server 10 64비트
- ALT Server 9.2 64비트
- ALT Workstation 10 32비트/64비트
- ALT Workstation 9.2 32비트/64비트
- ALT 8 SP Server (LKNV.11100-01) 64비트
- ALT 8 SP Server (LKNV.11100-02) 64비트

- ALT 8 SP Server (LKNV.11100-03) 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
- Linux Mint 19.x 32비트
- Linux Mint 20.x 64비트
- AlterOS 7.5 이상 64비트
- GosLinux IC6 64비트
- RED OS 7.3 64비트
- RED OS 7.3 Server 64비트
- RED OS 7.3 Certified Edition 64비트
- ROSA Enterprise Linux Server 7.3 64비트
- ROSA Enterprise Linux Desktop 7.3 64비트
- ROSA COBALT Workstation 7.3 64비트
- ROSA COBALT Server 7.3 64비트
- Lotos (Linux 코어 버전 4.19.50, DE: MATE) 64비트

지원되는 가상 플랫폼은 다음과 같습니다.

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64비트
- Microsoft Hyper-V Server 2012 R2 64비트
- Microsoft Hyper-V Server 2016 64비트
- Microsoft Hyper-V Server 2019 64비트
- Microsoft Hyper-V Server 2022 64비트
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- 커널 기반 가상 머신. 다음 운영 체제를 지원합니다.
  - ALT 8 SP Server (LKNV.11100-01) 64비트
  - ALT Server 10 64비트
  - Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7(폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
  - Debian GNU/Linux 11.x (Bullseye) 32비트/64비트
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64비트
  - RED OS 7.3 64비트

- RED OS 7.3 Server 64비트
- RED OS 7.3 Server 64비트

Kaspersky Security Center Linux와 같은 버전의 Linux용 네트워크 에이전트를 설치하는 것이 좋습니다.

지원하지 않는 운영 체제 및 플랫폼

중앙 관리 서버

중앙 관리 서버는 다음 운영 체제와 호환되지 않습니다:

- Debian GNU/Linux 7.x (7.8까지) 32비트/64비트
- Debian GNU/Linux 8.x(Jessie) 32비트/64비트
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32비트/64비트
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32비트/64비트
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32비트
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64비트
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32비트/64비트
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32비트/64비트
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32비트/64비트
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32비트/64비트
- CentOS 6.x (최대 6.6) 64비트
- CentOS 7.x ARM 64비트
- CentOS 8.x 64비트
- Red Hat Enterprise Linux Server 6.x 32비트/64비트
- SUSE Linux Enterprise Desktop 12 (모든 서비스 팩) 64비트
- SUSE Linux Enterprise Desktop 15 (모든 서비스 팩) 64비트
- SUSE Linux Enterprise Desktop 15 (서비스 팩 3) ARM 64비트
- openSUSE 15 64비트
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64비트
- Astra Linux Special Edition 1.5 64비트
- Astra Linux Special Edition 4.7 ARM
- ALT Workstation 9.2 32비트/64비트
- ALT Workstation 10 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 9 64비트

- Linux Mint 19.x 32비트
- Linux Mint 20.x 64비트
- AlterOS 7.5 이상 64비트
- RED OS 7.3 64비트
- GosLinux IC6 64비트
- ROSA Enterprise Linux Server 7.3 64비트
- ROSA Enterprise Linux Desktop 7.3 64비트
- ROSA COBALT Workstation 7.3 64비트
- ROSA COBALT Server 7.3 64비트
- Lotos (Linux 코어 버전 4.19.50, DE: MATE) 64비트

데이터베이스 서버:

- PostgreSQL 13 64비트
- PostgreSQL 14 64비트
- Postgres Pro 13 64비트
- Postgres Pro 14 64비트
- PostgreSQL 15 64비트
- PostgreSQL Pangolin 64비트
- Microsoft SQL Server 2005 Express 32비트
- Microsoft SQL Server 2005(모든 에디션) 32비트/64비트
- Microsoft SQL Server 2008 Express 32비트
- Microsoft SQL Server 2008(모든 에디션) 32비트/64비트
- Microsoft SQL Server 2008 R2 (모든 에디션) 64비트
- Microsoft SQL Server 2008 R2 Service Pack 2 (모든 에디션) 64비트
- Microsoft SQL Server 2012 (모든 에디션) 64비트
- MySQL 5.0 32비트/64비트
- MySQL Enterprise 5.0 32비트/64비트
- MySQL Standard Edition 5.5 32비트/64비트
- MySQL Enterprise Edition 5.5 32비트/64비트
- MySQL Standard Edition 5.6 32비트/64비트
- MySQL Enterprise Edition 5.6 32비트/64비트
- MySQL Standard Edition 5.7 32비트/64비트
- MySQL Enterprise Edition 5.7 32비트/64비트
- MySQL 5.6 Community 32비트/64비트
- MariaDB Server 10.3 32비트/64비트 InnoDB 스토리지 엔진
- MariaDB Galera Cluster 10.4 32비트/64비트

다음 가상 플랫폼은 지원하지 않습니다:

- VMware vSphere 4.1

- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64비트
- Microsoft Hyper-V Server 2008 R2 64비트
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 이상 64비트
- Microsoft Virtual PC 2007(6.0.156.0) 32비트/64비트
- Citrix XenServer 5.6
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7
- Parallels Desktop 7
- Parallels Desktop 11
- Parallels Desktop 14
- Parallels Desktop 16
- Oracle VM VirtualBox 4.0.4-70112(Windows 게스트 로그인 전용)
- Oracle VM VirtualBox 5.x(Windows 게스트 로그인 전용)

Kaspersky Security Center 14 웹 콘솔

Kaspersky Security Center 14 웹 콘솔 서버

Kaspersky Security Center 14 웹 콘솔 서버는 다음 운영 체제와 호환되지 않습니다:

- Debian GNU/Linux 7.x (7.8까지) 32비트/64비트
- Debian GNU/Linux 8.x(Jessie) 32비트/64비트
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32비트/64비트
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32비트/64비트
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64비트
- Ubuntu Server 22.04 LTS(Jammy Jellyfish) 64비트

- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32비트/64비트
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32비트/64비트
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32비트/64비트
- CentOS 6.x (최대 6.6) 64비트
- CentOS 7.x ARM 64비트
- CentOS 8.x 64비트
- Red Hat Enterprise Linux Server 6.x 32비트/64비트
- Red Hat Enterprise Linux Server 9.x 64비트
- SUSE Linux Enterprise Desktop 12 (모든 서비스 팩) 64비트
- SUSE Linux Enterprise Desktop 15 (모든 서비스 팩) 64비트
- SUSE Linux Enterprise Desktop 15 (서비스 팩 3) ARM 64비트
- openSUSE 15 64비트
- Pardus OS 19.1 64비트
- Astra Linux Special Edition 4.7 ARM
- Astra Linux Special Edition 1.7.2(폐쇄 소프트웨어 환경 모드 및 필수 모드 포함) 64비트
- ALT Workstation 9.2 32비트/64비트
- ALT Workstation 10 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 9 64비트
- Linux Mint 19.x 32비트
- Linux Mint 20.x 64비트
- AlterOS 7.5 이상 64비트
- RED OS 7.3 64비트
- GosLinux IC6 64비트
- ROSA Enterprise Linux Server 7.3 64비트
- ROSA Enterprise Linux Desktop 7.3 64비트
- ROSA COBALT Workstation 7.3 64비트
- ROSA COBALT Server 7.3 64비트
- ROSA COBALT 7.9 64비트
- ROSA CHROME 12 64비트
- Lotos (Linux 코어 버전 4.19.50, DE: MATE) 64비트

네트워크 에이전트

다음 운영 체제는 지원하지 않습니다:

- Debian GNU/Linux 7.x (7.8까지) 32비트/64비트
- Debian GNU/Linux 8.x(Jessie) 32비트/64비트
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32비트/64비트
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32비트/64비트
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32비트/64비트
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32비트/64비트
- CentOS 6.x (최대 6.6) 64비트
- Red Hat Enterprise Linux Server 9.x 64비트
- SUSE Linux Enterprise Desktop 12 (모든 서비스 팩) 64비트
- Astra Linux Special Edition 1.7.2 버전(폐쇄형 소프트웨어 환경 모드 및 필수 모드 포함)
- Oracle Linux 8 64비트
- ROSA COBALT 7.9 64비트
- ROSA CHROME 12 64비트

다음 가상 플랫폼은 지원하지 않습니다:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64비트
- Microsoft Hyper-V Server 2008 R2 64비트
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 이상 64비트
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

Kaspersky Security Center 14 웹 콘솔 정보

Kaspersky Security Center 14 웹 콘솔은 Kaspersky 애플리케이션을 통해 보호되는 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.

Kaspersky Security Center 14 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 14 웹 콘솔에 연결하면 브라우저에서 Kaspersky Security Center 14 웹 콘솔 서버와 연결을 확립합니다.

Kaspersky Security Center 14 웹 콘솔은 다음과 같이 작동합니다.

1. 브라우저를 사용하여 Kaspersky Security Center 14 웹 콘솔에 연결합니다. 그러면 웹 포털 인터페이스의 페이지가 표시됩니다.
2. 웹 포털 컨트롤을 사용하여 실행할 명령을 선택합니다. Kaspersky Security Center 14 웹 콘솔은 다음 작업을 수행합니다.
   - 기기 목록 보기와 같은 정보 수신에 사용되는 명령을 선택한 경우 Kaspersky Security Center 14 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 14 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 14 웹 콘솔은 다중 언어 애플리케이션입니다. 애플리케이션을 다시 열지 않고도 언제든지 인터페이스 언어를 변경할 수 있습니다. Kaspersky Security Center 14 웹 콘솔을 Kaspersky Security Center와 함께 설치하면 Kaspersky Security Center 14 웹 콘솔에 설치 파일과 동일한 인터페이스 언어가 설정됩니다. Kaspersky Security Center 14 웹 콘솔만 설치하는 경우 애플리케이션에 운영 체제와 동일한 인터페이스 언어가 설정됩니다. Kaspersky Security Center 14 웹 콘솔에서 설치 파일 또는 운영 체제의 언어를 지원하지 않는 경우 기본적으로 영어가 설정됩니다.

지원되는 Kaspersky 애플리케이션 목록

Kaspersky Security Center Linux는 다음 Kaspersky 애플리케이션의 중앙 집중식의 배포와 관리를 지원합니다.

- Kaspersky Endpoint Security for Linux
- Kaspersky Industrial CyberSecurity for Linux Nodes

이 애플리케이션으로 워크스테이션과 파일 서버를 모두 보호할 수 있습니다. 제품 지원 수명 주기 웹페이지 에서 애플리케이션의 버전을 확인하십시오.

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 Linux에 대한 정보가 포함되어 있습니다. Windows 기반 솔루션에 대한 자세한 내용은 Kaspersky Security Center Windows 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 14	
	Windows 기반 솔루션	**Linux 기반 솔루션**
중앙 관리 서버 위치	온프레미스	온프레미스
데이터베이스 관리 시스템(DBMS) 위치	온프레미스	온프레미스
중앙 관리 서버를 설치할 운영 체제	Windows	Linux
관리 콘솔 유형	온프레미스 및 웹 기반	웹 기반
웹 기반 관리 콘솔을 설치할 운영 체제	Windows 또는 Linux	Windows 또는 Linux
중앙 관리 서버 계층 구조	✓	✓

관리 그룹 계층 구조	✓	✓
네트워크 검색	✓	✓ (IP 범위에만 해당)
관리 중인 기기의 최대 개수	100,000	20,000
Windows, macOS 및 Linux로 관리 중인 기기 보호	✓	— (Linux 기기만 보호)
모바일 기기 보호	✓	—
가상 컴퓨터 보호	✓	—
퍼블릭 클라우드 인프라 보호	✓	—
기기 중심 보안 관리	✓	✓
사용자 중심 보안 관리	✓	✓
애플리케이션 정책	✓	✓
Kaspersky 애플리케이션용 작업	✓	✓
Kaspersky Security Network	✓	—
KSN 프록시	✓	—
Kaspersky Private Security Network	✓	—
Kaspersky 애플리케이션용 라이센스 키의 중앙 집중식 배포	✓	✓
가상 중앙 관리 서버 지원	✓	✓
타사 소프트웨어 업데이트 설치 및 타사 소프트웨어 취약점 수정	✓	— (원격 설치 작업에만 사용)
관리 중인 기기에서 발생한 이벤트에 대한 알림	✓	✓
사용자 계정 생성 및 관리	✓	✓
정책 및 작업 상태 모니터링	✓	✓
Kaspersky 장애 조치 클러스터 배포	✓	✓

기본 개념

이 섹션에서는 Kaspersky Security Center Linux와 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

Kaspersky Security Center 14 웹 콘솔의 인터페이스에서 중앙 관리 서버 이름은 다음과 같을 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 14 웹 콘솔을 사용하는 경우 애플리케이션은 사용자가 신뢰한다고 지정한 중앙 관리 서버의 이름을 응답 파일에 표시합니다.

Kaspersky Security Center 14 웹 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.

계층 구조에서, Kaspersky Security Center Linux 중앙 관리 서버는 Windows 기반 Kaspersky Security Center나 Kaspersky Security Center 클라우드 콘솔의 기본 중앙 관리 서버에서 관리하는 보조 서버로만 작동할 수 있습니다.

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 공급업체가 Kaspersky Security Center를 사용하는 방식. 서비스 공급업체는 Kaspersky Security Center와 Kaspersky Security Center 14 웹 콘솔만 설치해야 합니다. 여러 조직에 있는 많은 수의 클라이언트 기기를 관리하기 위해 서비스 공급업체는 중앙 관리 서버 계층 구조에 가상 중앙 관리 서버를 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(*가상 서버*라고도 함)는 클라이언트 조직 네트워크의 안티 바이러스 보호 관리를 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 Center Linux에서 기본 중앙 관리 서버 및 모든 가상 중앙 관리 서버를 다시 시작해야 합니다.

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

웹 서버

Kaspersky Security Center *Web Server*(이후 *웹 서버*라고도 함)는 중앙 관리 서버와 함께 설치되는 Kaspersky Security Center의 한 구성 요소입니다. 웹 서버는 독립 실행형 설치 패키지 및 공유 폴더의 파일을 네트워크를 통해 전송하도록 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.

공유 폴더는 중앙 관리 서버로 장치를 관리하는 모든 사용자가 이용할 수 있는 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:

- <웹 서버 이름>은 Kaspersky Security Center Web Server의 이름입니다.
- <HTTPS 포트>는 관리자가 정의한 웹 서버의 HTTPS 포트입니다. 중앙 관리 서버의 속성 창, **웹 서버** 섹션에서 HTTPS 포트를 설정할 수 있습니다. 기본 포트 번호는 8061입니다.
- <개체>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 14 Linux 네트워크 에이전트" 이름
- 운영 체제가 시작될 때 자동으로 시작하도록 설정
- LocalSystem 계정 사용

네트워크 에이전트가 설치된 기기는 *관리 중인 기기* 또는 *기기*라고 합니다. 다음 경로 중 하나에서 네트워크 에이전트를 설치할 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 다음과 같습니다:

- klnagent64.service(64비트 운영 체제)
- klnagent.service(32비트 운영 체제)

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 컴퓨터를 경리 관리 그룹에서 개발자 관리 그룹으로 이동할 수 있습니다. 그리고 나면 해당 컴퓨터에는 개발자에게 필요한 애플리케이션 설정이 자동으로 수신됩니다.

관리 중인 기기

*관리 중인 장치*는 네트워크 에이전트가 설치된 Linux를 실행하는 컴퓨터입니다. 이러한 기기에 설치된 애플리케이션용 작업과 정책을 만들어 해당 기기를 관리할 수 있습니다. 관리 중인 기기에서 리포트를 수집할 수도 있습니다.

관리 중인 기기는 배포 지점과 연결 게이트웨이 기능을 하도록 지정할 수 있습니다.

각 기기는 중앙 관리 서버 하나를 통해서만 관리할 수 있습니다. 중앙 관리 서버 하나는 최대 2만 대의 장치를 관리할 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

Kaspersky Security Center 14 웹 콘솔 서버가 설치된 장치를 *관리자 워크스테이션*이라고 합니다. 관리자는 클라이언트 기기에 설치된 Kaspersky 애플리케이션을 중앙 집중식으로 원격 관리하는 목적으로 이 기기를 사용할 수 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 웹 플러그인

특수 구성 요소인 *관리 웹 플러그인*은 Kaspersky Security Center 14 웹 콘솔을 통해 Kaspersky 소프트웨어를 원격으로 관리하는 데 사용됩니다. 여기서는 관리 웹 플러그인을 *관리 플러그인*이라고도 합니다. 관리 플러그인은 Kaspersky Security Center 14 웹 콘솔과 특정 Kaspersky 애플리케이션 간의 인터페이스입니다. 관리 플러그인을 사용하여 애플리케이션용 작업과 정책을 구성할 수 있습니다.

Kaspersky 기술 지원 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 14 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:

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.
- 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 조건 발생 시 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
- 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 Kaspersky Security Center 14 웹 콘솔을 사용하여 수정할 수도 있고, 원격 장치 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 집중식으로 중앙 관리 서버의 Syslog 이벤트 로그 및 Kaspersky Security Center 이벤트 로그에 저장되며, 각 장치에도 로컬로 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)나 DNS 이름을 장치의 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 조회 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 조회 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 조회를 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 장치에서 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(이전에는 업데이트 에이전트였음)은 네트워크 에이전트가 설치된 기기이며 업데이트 배포, 애플리케이션 원격 설치 및 연결된 기기에 대한 정보 수집에 활용됩니다. 배포 지점은 다음 기능을 수행할 수 있습니다:

- 중앙 관리 서버에서 받은 업데이트 및 설치 패키지를 UDP를 사용한 멀티캐스팅 등의 방식으로 그룹 내 클라이언트 장치에 배포합니다. 업데이트는 중앙 관리 서버 또는 Kaspersky 업데이트 서버에서 받을 수 있습니다. 후자의 경우에는 배포 지점에 대해 업데이트 작업이 생성되어야 합니다.

  배포 지점은 업데이트 배포 속도를 높이고 중앙 관리 서버의 리소스를 절약합니다.

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

  그룹 내 관리 중인 장치와 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.
- 네트워크 에이전트 없이 클라이언트 장치에 설치하는 방식을 포함하여, Kaspersky 및 기타 소프트웨어 공급업체의 애플리케이션을 원격 설치합니다.

  이 기능을 사용하면 네트워크 에이전트 설치 패키지를 중앙 관리 서버가 직접 접근할 수 없는 네트워크에 있는 클라이언트 기기로 원격 전송할 수 있습니다.

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.

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 프로필이 있는 네트워크 에이전트는 브로드캐스트 도메인 탐지에 참여하지 않습니다.

Kaspersky Security Center Linux는 각 네트워크 에이전트에 다른 주소와 다른 고유 IP 멀티캐스트 주소를 할당합니다. 그러면 IP 중복으로 인해 발생할 수 있는 네트워크 과부하 문제를 방지할 수 있습니다. 이전 버전의 애플리케이션에서 할당된 IP 멀티캐스트 주소는 변경되지 않습니다.

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 Center Linux는 심각도가 *경고*인 인시던트를 생성합니다. 인시던트는 기기 속성의 **인시던트** 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.

라이센스

이 섹션에는 Kaspersky Security Center 14 Linux 라이센싱에 관한 일반 개념 정보가 나와 있습니다.

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 최종 사용자 라이센스 계약서를 자세히 확인하십시오.

Kaspersky Security Center Linux 및 구성 요소(네트워크 에이전트 등)마다 각자의 EULA가 있습니다.

다음 방법으로 Kaspersky Security Center Linux의 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 웹사이트 에서 license.txt 파일 다운로드.

다음 방법으로 Linux용 네트워크 에이전트의 최종 사용자 라이센스 계약서를 볼 수 있습니다.

- Kaspersky 웹 서버에서 네트워크 에이전트 배포 패키지 다운로드 중.
- Linux용 네트워크 에이전트 설치 중.

  Linux용 네트워크 에이전트 설치 시, 네트워크 에이전트에 대한 최종 사용자 라이센스 계약서는 영어로 표시됩니다. 설치 중 최종 사용자 라이센스 계약서 약관을 수락하기 전에 /opt/kaspersky/klnagent64/share/license 폴더에서 다른 언어로 된 네트워크 에이전트에 대한 최종 사용자 라이센스 계약서를 확인할 수 있습니다.

- Linux용 네트워크 에이전트 배포 패키지에 포함된 license.txt 문서 확인.

- Linux용 네트워크 에이전트 설치 폴더의 license.txt 문서 확인.
- Kaspersky 웹사이트 에서 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 정보

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

라이센스가 있으면 다음 종류의 서비스를 이용할 수 있습니다:

- 최종 사용자 라이센스 계약서의 조건에 따른 애플리케이션의 사용
- 기술 지원 받기

서비스 범위 및 유효 기간은 애플리케이션 활성화에 사용된 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 Linux 기능이 중지됩니다. 애플리케이션을 계속 사용하려면 상업용 라이센스를 구매해야 합니다.

  한 번만 체험판 라이센스로 애플리케이션을 활성화할 수 있습니다.
- *상업용*. 애플리케이션을 구매 시 부여되는 유료 라이센스입니다.

  상업용 라이센스가 만료되면 애플리케이션의 주요 기능이 비활성화됩니다. Kaspersky Security Center를 계속 사용하려면 상업용 라이센스를 갱신해야 합니다. 라이센스를 갱신하지 않으려면, 컴퓨터에서 애플리케이션을 제거해야 합니다.

모든 보안 위협에 대한 보호를 극대화하기 위해, 라이센스가 만료되기 전에 갱신하는 것이 좋습니다.

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 키 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 장치 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.

개인정보취급방침 보기

개인정보취급방침은 https://www.kaspersky.com/products-and-services-privacy-policy 에서 온라인으로 확인할 수 있습니다.

개인정보취급방침은 오프라인에서도 볼 수 있습니다.

- Kaspersky Security Center 설치 전에 개인정보취급방침을 읽을 수 있습니다.
- 개인정보취급방침 텍스트는 Kaspersky Security Center 설치 폴더의 license.txt 파일에 포함되어 있습니다.
- privacy_policy.txt 파일은 관리 중인 장치의 네트워크 에이전트 설치 폴더에서 사용할 수 있습니다.
- 네트워크 에이전트 배포 패키지에서 privacy_policy.txt 파일의 압축을 풀 수 있습니다.

Kaspersky Security Center 라이센스 옵션

Kaspersky Security Center는 기업 네트워크 보호를 위한 Kaspersky 애플리케이션의 일부로서 제공됩니다. Kaspersky 웹사이트에서 다운로드할 수도 있습니다.

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.
- 조직의 안티 바이러스 보안 상태 제어.
- 애플리케이션 원격 설치.
- 원격 설치에 사용할 운영 체제 이미지의 목록 보기.
- 클라이언트 기기에 설치된 애플리케이션의 중앙 집중식 구성.
- 기존 유료 애플리케이션 그룹 보기 및 편집.
- 애플리케이션 동작의 통계와 리포트, 심각 이벤트에 대한 알림.
- 네트워크 검색에 의해 감지된 하드웨어 구성 요소 목록의 확인 및 편집.
- 격리 저장소나 백업 저장소로 이동한 파일 및 처리가 연기된 파일에 대한 중앙 집중식 작업.
- 사용자 역할 관리.

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 웹사이트 에서 키 파일을 받습니다.

데이터 제공 정보

권리자에게 전송되는 데이터

Kaspersky Security Center 14 Linux 최종 사용자 라이센스 계약서에 나와 있습니다.

로컬에서 처리되는 데이터

Kaspersky Security Center Linux는 조직 네트워크의 기본 관리 및 유지 관리 작업을 한 곳에서 실행할 수 있도록 설계되었습니다. Kaspersky Security Center Linux에서 관리자는 조직 네트워크 보안 수준에 대한 자세한 정보에 접근할 수 있습니다. Kaspersky Security Center Linux를 사용하면 Kaspersky 애플리케이션에 기초한 모든 보호 구성 요소를 구성할 수 있습니다. Kaspersky Security Center Linux는 다음 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
- 기기에서 Kaspersky 애플리케이션 활성화
- 사용자 계정 관리
- 기기에서 Kaspersky 애플리케이션의 작업 관련 정보 확인
- 리포트 보기

Kaspersky Security Center Linux는 주요 기능 수행을 위해 다음 정보를 수신, 저장, 처리할 수 있습니다.

- IP 인터벌 검사를 통해 네트워크에서 기기 발견 결과로 수신하는 조직 네트워크 내 기기에 관한 정보. 중앙 관리 서버는 데이터를 스스로 수집하거나 네트워크 에이전트로부터 데이터를 수신합니다.
- 관리 중인 기기의 세부 정보. 네트워크 에이전트는 아래 나열된 데이터를 기기에서 중앙 관리 서버로 전송합니다. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에 기기의 표시 이름 및 설명을 입력합니다.
  - 장치 식별에 필요한 관리 중인 장치 및 구성 요소의 기술 사양: 장치 표시 이름 및 설명, DNS 도메인 및 DNS 이름, IPv4 주소, IPv6 주소, 네트워크 위치, MAC 주소, 운영 체제 유형, 장치가 하이퍼바이저 유형의 가상 컴퓨터인지 여부, 장치가 VDI에 속한 동적 가상 컴퓨터인지 여부.
  - 관리 중인 기기의 감사에 필요한 관리 중인 기기 및 구성 요소의 기타 사양: 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.
  - 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.
- 기기가 배포 지점인 경우 배포 지점 작업 통계. 네트워크 에이전트는 기기에서 중앙 관리 서버로 데이터를 전송합니다.
- 사용자가 Kaspersky Security Center 14 웹 콘솔에서 입력한 배포 지점 설정.
- 기기에 설치된 Kaspersky 애플리케이션의 세부 정보. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다.
  - 관리 중인 장치에 설치된 Kaspersky 애플리케이션 설정: Kaspersky 애플리케이션 이름 및 버전, 상태, 실시간 보호 상태, 마지막 장치 검사 날짜와 시간, 탐지된 위협 수, 치료하지 못한 개체 수, 애플리케이션 구성 요소의 가용성 및 상태, 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 Security Center Linux 구성 요소와 관리 중인 Kaspersky 애플리케이션의 이벤트에 포함된 데이터. 네트워크 에이전트는 기기에서 중앙 관리 서버로 데이터를 전송합니다.
- 정책 및 정책 프로필에 표시되어 있는 Kaspersky Security Center 구성 요소 및 관리 중인 Kaspersky 애플리케이션의 설정. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- Kaspersky Security Center Linux 구성 요소 및 관리 중인 Kaspersky 애플리케이션의 작업 설정. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 취약점 및 패치 매니지먼트 기능을 통해 처리되는 데이터. 네트워크 에이전트는 관리 중인 기기(하드웨어 레지스트리)에서 탐지된 하드웨어에 대한 정보를 기기에서 중앙 관리 서버로 전송합니다.
- 애플리케이션의 사용자 카테고리. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.

- 관리 중인 기기에서 애플리케이션 제어 기능으로 탐지된 실행 파일 목록. 관리 중인 애플리케이션은 네트워크 에이전트를 통해 기기에서 중앙 관리 서버로 데이터를 전송합니다. 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.
- 관리 중인 기기에 설치되어 있거나 이에 연결되어 매체 제어 기능에 의해 탐지된 외부 기기(메모리 장치, 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.
- 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.
- 입력된 활성화코드 세부 정보. 사용자는 관리 콘솔 또는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 사용자 계정: 이름, 설명, 전체 이름, 이메일 주소, 메인 전화 번호, 암호. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 관리 개체의 리비전 내역. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 삭제된 관리 개체의 레지스트리. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 파일에서 생성된 설치 패키지 및 설치 설정. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- Kaspersky Security Center 14 웹 콘솔에서 Kaspersky의 공지 사항을 표시하는 데 필요한 데이터. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- Kaspersky Security Center 14 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 14 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. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- Kaspersky Security Center Linux 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 장치와 Kaspersky Security Center Linux 구성 요소의 보안 연결을 위한 인증서. 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 사용자가 Kaspersky Security Center 14 웹 콘솔에서 입력하는 중앙 관리 서버 데이터.
- 사용자가 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 입력하는 모든 데이터.

상기 데이터는 다음 방법의 하나를 적용 시 Kaspersky Security Center Linux에 표시될 수 있습니다.

- 사용자는 Kaspersky Security Center 14 웹 콘솔 인터페이스에서 데이터를 입력합니다.
- 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 서버와 네트워크 에이전트는 배포 지점을 할당하여 네트워크 기기에 관한 정보를 수집합니다.

목록에 나열된 데이터는 중앙 관리 서버 데이터베이스에 저장됩니다. 사용자 이름과 암호는 암호화된 형식으로 저장됩니다.

로컬로 처리되는 모든 데이터는 Kaspersky Security Center Linux 구성 요소의 덤프 파일, 추적 파일 또는 로그 파일(설치 프로그램 및 유틸리티가 생성한 로그 파일 등)을 통해서만 Kaspersky로 전송될 수 있습니다.

Kaspersky는 이렇게 받은 정보를 법률 및 해당 Kaspersky 규칙에 따라 보호합니다. 데이터가 보안 채널을 통해 전송됩니다.

사용자는 관리 콘솔 또는 Kaspersky Security Center 14 웹 콘솔의 링크로 이동하여 다음 데이터 자동 전송에 동의합니다.

- Kaspersky Security Center Linux 코드
- Kaspersky Security Center Linux 버전

- Kaspersky Security Center Linux 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.

서브스크립션 정보

*Kaspersky Security Center Linux 서브스크립션*은 선택한 설정(서브스크립션 만료 날짜, 보호 장치 수)으로 애플리케이션을 사용하기 위한 주문입니다. 서비스 공급 업체(인터넷 공급 업체 등)를 통해 Kaspersky Security Center Linux에 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 Center Linux를 사용하려면 서비스 공급업체로부터 받은 활성화 코드를 적용해야 합니다.

서브스크립션 만료 또는 취소 시에만 Kaspersky Security Center Linux에 다른 활성화 코드를 적용할 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 애플리케이션 사용 시, Kaspersky Security Center Linux는 서브스크립션이 만료될 때까지 지정한 시간 간격 동안 자동으로 활성화 서버에 접속을 시도합니다. 서브스크립션은 서비스 공급 업체의 홈페이지에서 갱신할 수 있습니다.

라이센스 제한 초과 이벤트

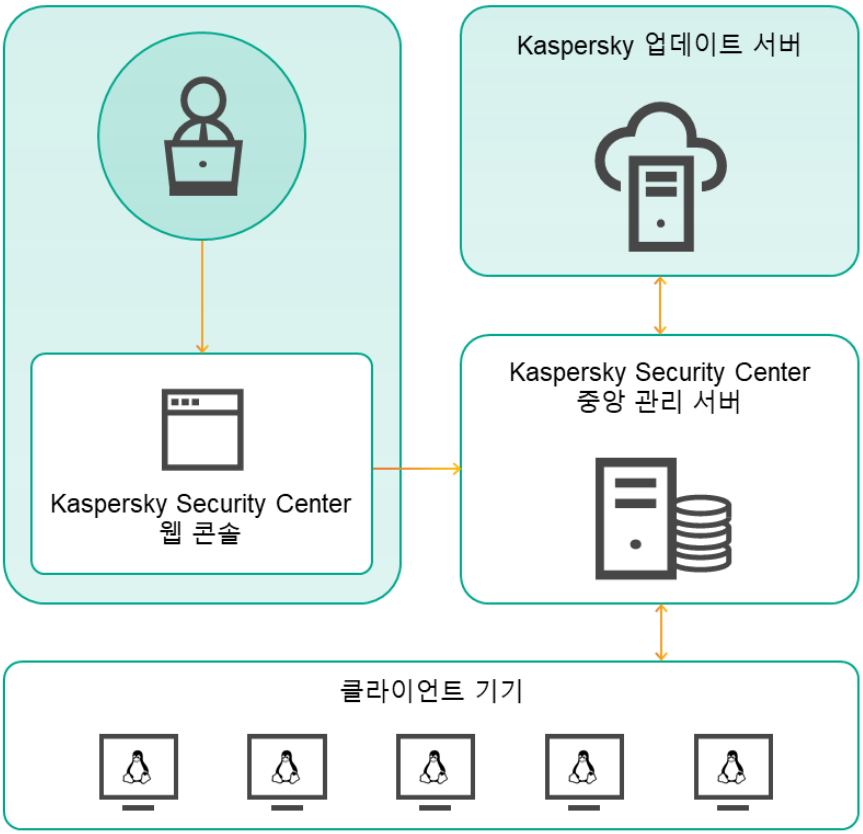
클라이언트 장치에 설치된 Kaspersky 애플리케이션에서 라이센스 제한 초과 시 Kaspersky Security Center Linux에서 이벤트 정보를 볼 수 있습니다.

라이센스 제한이 초과된 경우 이러한 이벤트의 심각도는 다음 규칙에 따라 정의됩니다:

- 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.

아키텍처

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



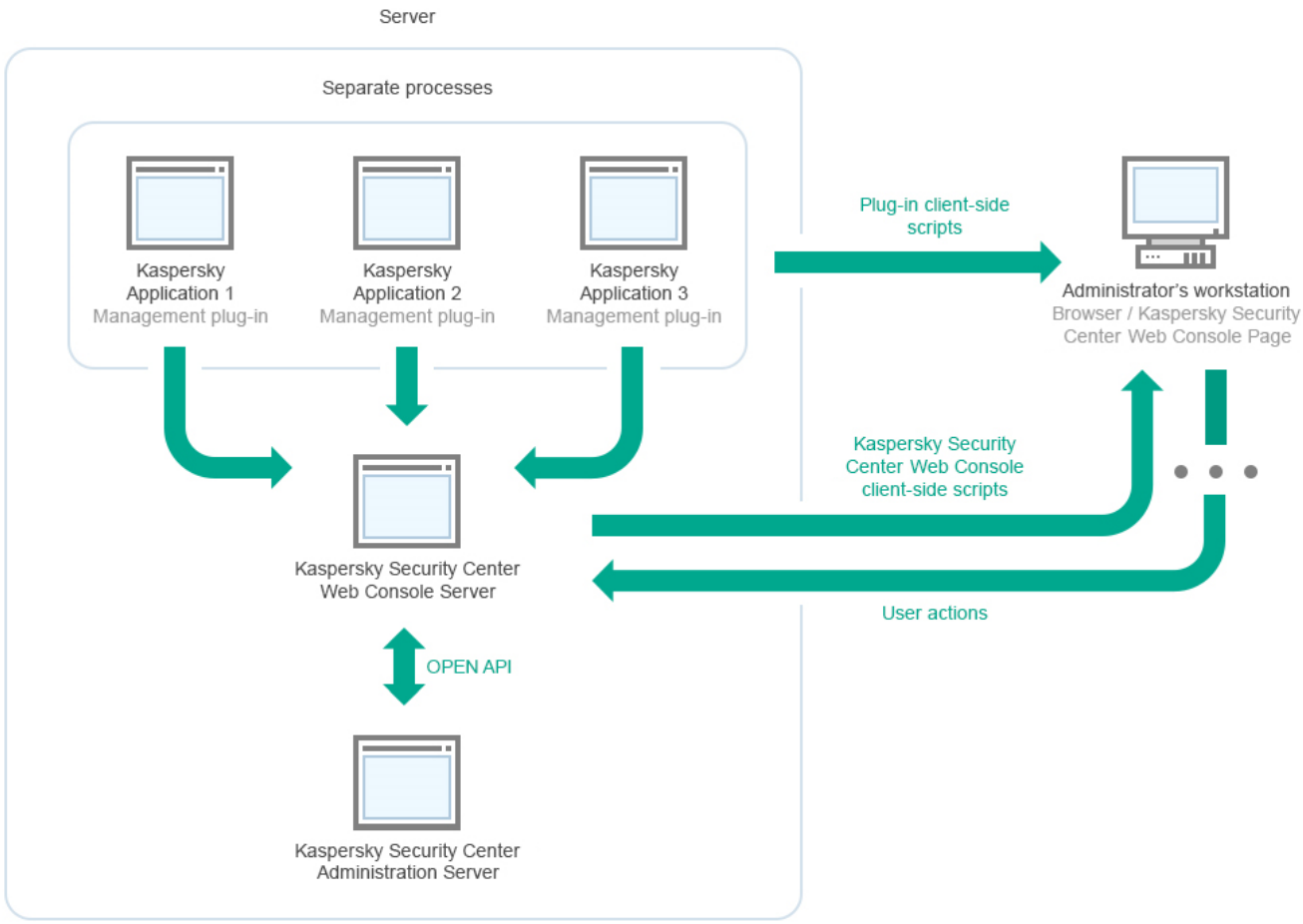
Kaspersky Security Center 14 Linux 아키텍처

Kaspersky Security Center 14 Linux는 다음 기본 구성 요소로 구성됩니다:

- **Kaspersky Security Center 14 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.
- **클라이언트 기기.** Kaspersky Security Center 14 Linux에서 보호하는 고객의 장치입니다. 보호해야 하는 각 기기에는 Kaspersky 보안 제품 중 하나가 설치되어 있어야 합니다.

Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 14 웹 콘솔의 배포 다이어그램

아래 그림은 Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 14 웹 콘솔의 배포 다이어그램을 보여줍니다.



Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 14 웹 콘솔의 배포 다이어그램

보호되는 기기에 설치된 Kaspersky 애플리케이션용 관리 플러그인(각 애플리케이션당 플러그인 하나)은 Kaspersky Security Center 14 웹 콘솔 서버와 함께 배포됩니다.

관리자는 워크스테이션에서 브라우저를 사용하여 Kaspersky Security Center 14 웹 콘솔에 접근합니다.

Kaspersky Security Center 14 웹 콘솔에서 특정 작업을 수행할 때 Kaspersky Security Center 14 웹 콘솔 서버는 OpenAPI를 통해 Kaspersky Security Center 중앙 관리 서버와 통신합니다. Kaspersky Security Center 14 웹 콘솔 서버는 Kaspersky Security Center 중앙 관리 서버에서 필요한 정보를 요청하고 작업 결과를 Kaspersky Security Center 14 웹 콘솔에 표시합니다.

Kaspersky Security Center Linux의 사용 포트

아래 표에는 중앙 관리 서버 및 클라이언트 장치에서 열려야 하는 기본 포트가 나와 있습니다. 원하는 경우 이러한 각 기본 포트 번호를 변경할 수 있습니다.

Kaspersky Security Center Linux 중앙 관리 서버의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
8060	klcsweb	TCP	게시된 설치 패키지를 클라이언트 기기로 전송	설치 패키지 게시 중앙 관리 서버 속성 창의 **웹 서버** 섹션에서 기본 포트 번호를 변경할 수 있습니다.
8061	klcsweb	TCP (TLS)	게시된 설치 패키지를 클라이언트 기기로 전송	설치 패키지 게시 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 Kaspersky Security Center Linux 설치 중 연결 포트 구성 시 네트워크 에이전트에서 연결을 수신할 기본 포트 번호를 변경할 수 있습니다. 중앙 관리 서버 계층 생성 시 보조 중앙 관리 서버에서 연결을 수신할 기본 포트 번호를 변경할 수 있습니다.
13000	klserver	UDP	네트워크 에이전트에서 꺼진 기기에 대한 정보	클라이언트 기기 관리

			수신	네트워크 에이전트 정책 설정에서 기본 포트 번호를 변경할 수 있습니다.
13299	klserver	TCP (TLS)	Kaspersky Security Center 14 웹 콘솔에서 중앙 관리 서버로의 연결 수신; OpenAPI를 통한 중앙 관리 서버로의 연결 수신	Kaspersky Security Center 14 웹 콘솔, OpenAPI 기본 포트 번호는 중앙 관리 서버 속성 창의 **일반** 섹션에 있는 **연결 포트** 하위 섹션에서 변경하거나, 중앙 관리 서버 계층 생성 시 변경할 수 있습니다.
114000	klserver	TCP	네트워크 에이전트에서 연결 수신	클라이언트 기기 관리 기본 포트 번호는 Kaspersky Security Center Linux 설치 중 연결 포트를 구성할 때나 클라이언트 장치를 중앙 관리 서버에 수동으로 연결할 때 변경할 수 있습니다.
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	관리 중인 장치를 위한 활성화 프록시 서버. 중앙 관리 서버 속성 창의 **일반** 섹션에 있는 **추가 포트** 하위 섹션에서 기본 포트 번호를 변경할 수 있습니다.
19170	klserver	HTTPS (TLS)	klsctunnel 유틸리티를 사용하여 관리 중인 기기에 터널링 연결	Kaspersky Security Center 14 웹 콘솔을 사용하여 관리 중인 기기에 원격 연결 klscflag 유틸리티를 사용하여 기본 포트 번호를 변경할 수 있습니다.

중앙 관리 서버와 데이터베이스를 서로 다른 기기에 설치하는 경우 데이터베이스가 설치된 기기에서 관련 포트를 사용할 수 있도록 열어야 합니다(예: MariaDB Server의 경우 3306 포트). 관련 정보는 DBMS 설명서를 참조하십시오.

아래 표에는 Kaspersky Security Center 14 웹 콘솔 서버에서 열어야 하는 포트가 표시되어 있습니다. 중앙 관리 서버가 설치되어 있는 동일한 기기이거나 다른 기기일 수 있습니다.

Kaspersky Security Center 14 웹 콘솔 서버의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
8 080	Node.js: 서버 측 JavaScript	TCP (TLS)	브라우저에서 Kaspersky Security Center 14 웹 콘솔로의 연결 수신	Kaspersky Security Center 14 웹 콘솔. Kaspersky Security Center 14 웹 콘솔 설치 시 기본 포트 번호를 변경할 수 있습니다. Linux ALT 운영 체제에 Kaspersky Security Center 14 웹 콘솔을 설치하는 경우 운영 체제에서 포트 8080을 사용하므로 8080 이외의 포트 번호를 지정해야 합니다.

아래 표에는 네트워크 에이전트가 설치된 관리 중인 기기에서 열어야 하는 포트가 표시되어 있습니다.

네트워크 에이전트의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
15000	klnagent	UDP	중앙 관리 서버에서 네트워크 에이전트로의 관리 신호	클라이언트 기기 관리 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. 배포 지점 속성 창에서 기본 포트 번호를 변경할 수 있습니다.

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.

다음 표에는 배포 지점 역할을 하는 네트워크 에이전트가 설치된 관리 중인 기기에서 열어야 하는 포트가 표시되어 있습니다. 네트워크 에이전트에서 사용하는 포트 외에 목록의 포트도 배포 지점 장치에서 열려 있어야 합니다(위 표 참조).

배포 지점으로 작동하는 네트워크 에이전트의 사용 포트

포트 번호	포트를 여는 프로세스의 이름	프로토콜	포트 용도	범위
13000	klnagent	TCP (TLS)	네트워크 에이전트에서 연결 수신	클라이언트 기기 관리, 업데이트 및 설치 패키지 전달. 배포 지점 속성에서 기본 포트 번호를 변경할 수 있습니다.
13111(KSN 프록시 서비스가 기기에서 실행되는 경우에만)	ksnproxy	TCP	관리 중인 기기에서 KSN 프록시 서버로의 요청 수신	KSN 프록시 서버 배포 지점 속성에서 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 배포 지점 속성에서 기본 포트 번호를 변경할 수 있습니다.

Kaspersky Security Center 14 웹 콘솔에서 사용되는 포트

아래 표에는 Kaspersky Security Center 14 웹 콘솔 서버(Kaspersky Security Center 14 웹 콘솔이라고도 함)가 설치된 기기에서 열어야 하는 포트가 나열되어 있습니다.

Kaspersky Security Center 14 웹 콘솔에서 사용되는 포트

포트 번호	서비스 이름	프로토콜	포트 용도	범위
2001	KSCWebConsolePlugin	HTTPS	KSCWebConsoleManagementService의 요청을 수신하기 위해 관리 플러그인 프로세스에서 사용하는 API 포트	관리 플러그인의 노드 프로세스 실행
1329, 2003	KSCWebConsoleManagementService	HTTPS	같은 장치에서 실행 중인 KSCWebConsole 서비스에서 요청 수신에 사용하는 API 포트	Kaspersky Security Center 14 웹 콘솔 구성 요소 업데이트
2005	KSCWebConsole	HTTPS	동일한 기기에서 실행 중인 KSCWebConsoleManagementService 서비스의 요청을 수신하는 데 사용하는 API 포트	Kaspersky Security Center 14 웹 콘솔의 노드 프로세스 실행
8200	—	HTTP	HashiCorp Vault를 통해 인증서를 생성하는 데 사용되는 API 포트(자세한 내용은 HashiCorp Vault 웹사이트 참조)	Kaspersky Security Center 14 웹 콘솔 설치 및 Kaspersky Security Center 14 웹 콘솔 구성 요소 업데이트
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Kaspersky Security Center 14 웹 콘솔과 관리 플러그인 프로세스 간 통신에 사용되는 메시지 브로커의 API 포트	Kaspersky Security Center 14 웹 콘솔과 관리 플러그인 간의 상호 작용

설치

이 섹션에서는 Kaspersky Security Center 및 Kaspersky Security Center 14 웹 콘솔 설치에 대해 설명합니다.

주요 설치 시나리오

이 시나리오를 따라 Kaspersky Security Center 14 Linux 중앙 관리 서버 및 Kaspersky Security Center 14 웹 콘솔을 설치하고, 빠른 시작 마법사를 사용하여 중앙 관리 서버 초기 설정을 수행하고, 보호 배포 마법사를 사용하여 관리 중인 장치에 Kaspersky 애플리케이션을 설치할 수 있습니다.

필수 구성 요소

Kaspersky Endpoint Security for Business용 라이센스 키(활성화 코드) 또는 Kaspersky 보안 애플리케이션용 라이센스 키(활성화코드)가 있어야 합니다.

우선 Kaspersky Security Center 14 Linux를 사용해 보려면, Kaspersky 웹사이트에서 30일 무료 평가판을 받을 수 있습니다.

단계

기본 설치 시나리오는 다음 단계로 진행됩니다.

1 조직 보호를 위한 조직도 선택

Kaspersky Security Center Linux 구성 요소에 대해 더 알아보기. (네트워크가 분산되어 있다면,) 통신 채널 처리 성능과 네트워크 구성에 따라 사용할 중앙 관리 서버의 수와 여러 사무실에 중앙 관리 서버를 배포할 방법을 정의합니다.

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.

2 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.

3 DBMS(데이터베이스 관리 시스템) 설치

Kaspersky Security Center에서 사용할 DBMS를 설치하거나 기존 DBMS를 사용합니다.

4 포트 구성

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

중앙 관리 서버에 대한 인터넷 액세스를 제공하려면, 네트워크 구성에 따라 포트를 구성하고 연결 설정을 지정합니다.

5 Kaspersky Security Center 설치

중앙 관리 서버로 사용하려는 Linux 기기를 선택하고, 해당 기기가 소프트웨어 및 하드웨어 요구 사항을 충족하는지 확인한 다음 기기에 Kaspersky Security Center를 설치합니다. 네트워크 에이전트의 서버 버전에는 자동으로 중앙 관리 서버가 설치됩니다.

6 Kaspersky Security Center 14 웹 콘솔 및 관리 웹 플러그인 설치

관리자 워크스테이션으로 사용하려는 Linux 기기를 선택하고, 해당 기기가 소프트웨어 및 하드웨어 요구 사항을 충족하는지 확인한 다음 기기에 Kaspersky Security Center 14 웹 콘솔을 설치합니다. Kaspersky Security Center 14 웹 콘솔을 중앙 관리 서버가 설치된 동일한 기기나 다른 기기에 설치할 수 있습니다.

Kaspersky Endpoint Security for Linux 관리 웹 플러그인 다운로드 후 Kaspersky Security Center 14 웹 콘솔을 설치한 장치에 설치합니다.

7 중앙 관리 서버 장치에 Kaspersky Endpoint Security for Linux 및 네트워크 에이전트 설치

기본적으로 애플리케이션은 중앙 관리 서버 장치를 관리 중인 장치로 간주하지 않습니다. 바이러스 및 기타 위협으로부터 중앙 관리 서버를 보호하고 해당 장치를 다른 관리 중인 장치와 같이 관리하려면 중앙 관리 서버 장치에 Kaspersky Endpoint Security for Linux 설치 및 Linux용 네트워크 에이전트 설치를 권장합니다. 이때 설치한 Linux용 네트워크 에이전트는 중앙 관리 서버와 함께 설치한 네트워크 에이전트의 서버 버전과 독립적으로 작동합니다.

8 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.

9 네트워크에 연결된 기기 발견

기기를 수동으로 검색합니다. Kaspersky Security Center Linux는 네트워크에서 탐지한 모든 장치의 주소와 이름을 수신합니다. 그러면 탐지한 장치에 Kaspersky Security Center Linux를 사용하여 Kaspersky 애플리케이션 및 다른 공급업체의 소프트웨어를 설치할 수 있습니다. Kaspersky Security Center Linux는 정기적으로 장치 발견을 시작합니다. 이는 네트워크에 새 인스턴스가 있을 시 자동 탐지한다는 뜻입니다.

10 관리 그룹으로 기기 정렬

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.

11 배포 지점 할당

배포 지점은 관리 그룹에 자동으로 할당되지만 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.

12 네트워크에 연결된 기기에 네트워크 에이전트 및 보안 제품 설치

기업 네트워크에 보호 기능을 배포하는 것은 기기를 발견하는 동안 중앙 관리 서버가 탐지한 기기에 네트워크 에이전트 및 보안 애플리케이션을 설치한다는 것을 의미합니다.

애플리케이션을 원격으로 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.

13 클라이언트 기기에 라이센스 키 배포

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

14 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.

15 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.

데이터베이스 관리 시스템 설치

Kaspersky Security Center에서 사용할 DBMS(데이터베이스 관리 시스템)를 설치합니다. 지원하는 DBMS 중 하나를 선택할 수 있습니다.

선택한 DBMS를 설치하는 방법에 대한 정보는 해당 설명서를 참조하십시오.

MariaDB 사용 시, DBMS가 Kaspersky Security Center와 최적으로 작동하도록 권장 설정을 구성해야 합니다.

Kaspersky Security Center 14 Linux 사용을 위한 MariaDB x64 서버 구성

Kaspersky Security Center를 위해 MariaDB 서버를 사용하는 경우 InnoDB 및 MEMORY 스토리지와 UTF-8 및 UCS-2 인코딩 지원을 활성화하십시오.

my.cnf 파일에 대한 권장 설정

my.cnf 파일을 구성하려면 다음과 같이 하십시오:

1. 텍스트 편집기에서 my.cnf 파일을 엽니다.
2. my.cnf 파일에 다음과 같은 행을 입력합니다.

```
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=< value >
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
```

`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.

파라미터 값으로 `innodb_flush_log_at_trx_commit=0` 을 사용하기를 권장합니다. "1" 또는 "2" 값은 MariaDB의 작동 속도에 부정적인 영향을 미치기 때문입니다.

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 다음 행이 포함되었는지 확인합니다.

```
join_cache_incremental=on
```

```
join_cache_hashed=on
join_cache_bka=on
```

이 행이 있고 값이 on 이라면, 옵티마이저 애드온이 활성화됩니다.

이러한 행이 없거나 off 값을 갖는 경우 다음과 같이 해야 합니다.

a. 텍스트 편집기에서 my.cnf 파일을 엽니다.

b. my.cnf 파일에 다음과 같은 행을 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 설치

이 절차에서는 Kaspersky Security Center를 설치하는 방법을 설명합니다.

설치 전:

- 데이터베이스 관리 시스템 설치
- Kaspersky Security Center를 설치할 기기에서 지원되는 Linux 배포판 중 하나를 실행하는지 확인합니다.

기기에 설치된 Linux 배포판에 따라 file—ksc64_[version_number]_amd64.deb 또는 ksc64-[version_number].x86_64.rpm 설치 파일을 사용합니다. Kaspersky 웹사이트에서 설치 파일을 다운로드하여 받습니다.

Kaspersky Security Center를 설치하려면 다음 단계를 따릅니다.

1. 명령줄에서 루트 권한이 있는 계정으로 이 지침에 제공된 명령을 실행합니다.
2. 'kladmins' 그룹과 권한 없는 계정 'ksc'를 만듭니다. 계정은 'kladmins' 그룹에 속해야 합니다. 그러려면 다음 명령을 순차적으로 실행하십시오.
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```
3. Kaspersky Security Center 설치를 실행합니다. Linux 배포판에 따라 다음 명령 중 하나를 실행합니다.
   - `# apt install /<경로>/ksc64_[ 버전_번호 ]_amd64.deb`
   - `# yum install /<경로>/ksc64-[ 버전_번호 ].x86_64.rpm -y`
4. Kaspersky Security Center 구성을 실행합니다.
   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```
5. 최종 사용자 라이센스 계약서(EULA)와 개인정보취급방침을 읽어 보십시오. 텍스트가 명령줄 창에 표시됩니다. 다음 텍스트 세그먼트를 보려면 스페이스 바를 누르십시오. 그런 다음 메시지가 표시되면 다음 값을 입력합니다.
   a. EULA의 약관을 읽고 이에 동의하는 경우 y를 입력합니다. EULA의 약관에 동의하지 않는 경우 n을 입력하십시오. Kaspersky Security Center를 사용하려면 EULA 약관에 동의해야 합니다.
   b. 개인정보취급방침의 약관을 이해하고 이에 동의하는 경우 y를 입력합니다. 그러면 귀하의 데이터가 개인정보취급방침에 설명된 대로 처리 및 전송되는 데(제 3국 포함) 동의하는 것입니다. 개인정보취급방침의 약관에 동의하지 않는 경우 n을 입력하십시오. Kaspersky Security Center를 사용하려면 개인정보취급방침 약관에 동의해야 합니다.
6. 메시지가 표시되면 다음 설정을 입력합니다.
   a. 중앙 관리 서버 DNS 이름 또는 고정 IP 주소를 입력합니다.
   b. 중앙 관리 서버 포트 번호를 입력합니다. 기본적으로 포트 14000이 사용됩니다.
   c. 중앙 관리 서버 SSL 포트 번호를 입력합니다. 기본적으로 포트 13000이 사용됩니다.
   d. 다음과 같이 관리하려는 기기 수를 대략적으로 평가하십시오.
      - 1 ~ 100개의 네트워크 기기가 있는 경우 1을 입력합니다.
      - 101 ~ 1000개의 네트워크 기기가 있는 경우 2을 입력합니다.
      - 네트워크 장치가 1,000개 이상이라면 3을 입력합니다.

e. 서비스의 보안 그룹 이름을 입력하십시오. 기본적으로 'kladmins' 그룹이 사용됩니다.

f. 계정 이름을 입력하여 중앙 관리 서버 서비스를 시작합니다. 계정은 입력된 보안 그룹에 속해야 합니다. 기본적으로 'ksc' 계정이 사용됩니다.

g. 다른 서비스를 시작하려면 해당 계정 이름을 입력하십시오. 계정은 입력된 보안 그룹에 속해야 합니다. 기본적으로 'ksc' 계정이 사용됩니다.

h. 데이터베이스가 설치된 기기의 IP 주소를 입력하십시오.

i. 데이터베이스 포트 번호를 입력하십시오. 이 포트는 중앙 관리 서버와 통신하는 데 사용됩니다. 기본적으로 포트 3306이 사용됩니다.

j. 데이터베이스 이름을 입력합니다.

k. 데이터베이스 액세스에 사용하는 데이터베이스 루트 계정의 로그인을 입력하십시오.

l. 데이터베이스 액세스에 사용하는 데이터베이스 루트 계정의 암호를 입력하십시오.
서비스가 추가되고 자동으로 시작될 때까지 기다립니다.

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. 중앙 관리 서버의 관리자 역할을 담당할 계정을 만듭니다. 사용자 이름과 암호를 입력합니다.
암호는 다음 규칙을 따라야 합니다:

- 사용자 암호는 8자 미만이거나 16자를 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(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

사용자가 추가되고 Kaspersky Security Center가 설치됩니다.

서비스 검증

다음 명령을 사용하여 서비스가 실행 중인지 확인합니다.

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

숨김 모드에서 Kaspersky Security Center 설치

응답 파일을 사용하여 숨김(비대화형) 모드, 즉 사용자 참여 없이 설치를 실행하여 Linux 장치에 Kaspersky Security Center 설치할 수 있습니다. 응답 파일에는 사용자 지정 설치 파라미터 집합(변수 및 해당 값)이 포함되어 있습니다.

설치 전:

- DBMS(데이터베이스 관리 시스템) 설치.
- Kaspersky Security Center를 설치할 기기에서 지원되는 Linux 배포판 중 하나를 실행하는지 확인합니다.

Kaspersky Security Center를 숨김 모드로 설치하려면:

1. 최종 사용자 라이센스 계약서를 읽어 보십시오. 최종 사용자 라이센스 계약서의 조건을 이해하고, 이에 동의하는 경우에만 아래 단계를 따르십시오.

2. 'kladmins' 그룹의 구성원이어야 하는 권한 없는 계정 'ksc'와 'kladmins' 그룹을 만듭니다. 이렇게 하려면 루트 권한이 있는 계정에서 다음 명령을 순서대로 실행합니다.

```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```

3. 응답 파일(TXT 형식)을 만들고 `VARIABLE_NAME=variable_value` 형식의 변수 목록을 응답 파일에 별도의 줄로 추가합니다. 응답 파일에는 아래 표에 나열된 변수가 포함되어야 합니다.

4. 예를 들어 다음 명령을 사용하여, 경로를 포함하여 응답 파일의 전체 이름을 포함하는 루트 환경에서 `KLAUTOANSWERS` 환경 변수의 값을 설정합니다.

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

5. Linux 배포판에 따라 다음 명령 중 하나를 실행하여 자동 모드에서 Kaspersky Security Center 설치를 실행합니다.

- `# apt install /<경로>/ksc64_[ 버전_번호 ]_amd64.deb`
- `# yum install /<경로>/ksc64-[ 버전_번호 ].x86_64.rpm -y`

6. Kaspersky Security Center 14 웹 콘솔로 작업할 사용자를 생성합니다. 이렇게 하려면 루트 권한이 있는 계정에서 다음 명령을 실행합니다.

`/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p < password >`, 여기서 암호는 8자 이상이어야 합니다.

-

숨김 모드에서 Kaspersky Security Center 설치 시 파라미터로 사용되는 응답 파일의 변수

변수 이름	필요한 용량	설명	가능한 값
`EULA_ACCEPTED`	예	최종 사용자 라이센스 계약서의 약관을 읽고 이해했으며 이를 수락함을 확인합니다.	`1`
`PP_ACCEPTED`	예	개인 정보 취급 방침의 조건을 이해하고 수락함을 확인합니다.	1
`KLSRV_UNATT_SERVERADDRESS`	예	중앙 관리 서버 DNS 이름 또는 고정 IP 주소.	DNS 이름 또는 IP 주소
`KLSRV_UNATT_PORT_SRV`	아니요	중앙 관리 서버 포트 번호. 선택 사항이며, 기본값은 14000입니다.	포트 번호
`KLSRV_UNATT_PORT_SRV_SSL`	아니요	중앙 관리 서버 SSL 포트 번호. 선택 사항이며, 기본값은 13000입니다.	포트 번호
`KLSRV_UNATT_PORT_KLOAPI`	아니요	중앙 관리 서버 KLOAPI 포트 번호. 선택 사항이며, 기본값은 13299입니다.	포트 번호
`KLSRV_UNATT_PORT_GUI`	아니요	중앙 관리 서버 GUI 포트 번호. 선택 사항이며, 기본값은 13291입니다.	포트 번호
`KLSRV_UNATT_NETRANGETYPE`	아니요	관리하려는 장치의 대략적인 수. 선택 사항이며, 기본값은 1입니다.	네트워크 장치가 1~100개일 때는 `1`. 네트워크 장치가 101~1,000개일 때는 `2`. 네트워크 장치가 1,000개 이상일 때는 `3`.
`KLSRV_UNATT_DBMS_INSTANCE`	예	데이터베이스 서버 IP 주소.	IP 주소
`KLSRV_UNATT_DBMS_PORT`	예	데이터베이스 서버 포트.	`3306`
`KLSRV_UNATT_DB_NAME`	예	데이터베이스 이름.	`kav`
`KLSRV_UNATT_DBMS_LOGIN`	예	데이터베이스에 대한 액세스 권한이 있는 사용자의 사용자 이름.	
`KLSRV_UNATT_DBMS_PASSWORD`	예	데이터베이스에 대한 액세스 권한이 있는 사용자의 암호.	
`KLSRV_UNATT_KLADMINSGROUP`	예	서비스의 보안 그룹 이름.	`kladmins`
`KLSRV_UNATT_KLSRVUSER`	예	중앙 관리 서버 서비스를 시작할 계정 이름. 계정은 `KLSRV_UNATT_KLADMINSGROUP` 변수에 지정된 보안 그룹의 구성원이어야 합니다.	`ksc`
`KLSRV_UNATT_KLSVCUSER`	예	다른 서비스를 시작할 계정 이름. 계정은 `KLSRV_UNATT_KLADMINSGROUP` 변수에 지정된 보안 그룹의 구성원이어야 합니다.	`ksc`

중앙 관리 서버가 Kaspersky 장애 조치 클러스터로 배포된다면 응답 파일이 다음과 같은 추가 변수를 포함해야 합니다.

KLFOC_UNATT_NODE	예	노드 번호(1 또는 2).	1 또는 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	예	상태 공유 마운트 지점.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	예	데이터 공유 마운트 지점.	
KLFOC_UNATT_CONN_MODE	예	장애 조치 클러스터 연결 모드.	VirtualAdapter 또는 ExternalLoadBalancer

KLFOC_UNATT_CONN_MODE 변수에 VirtualAdapter 값이 있다면 응답 파일이 다음 추가 변수를 포함해야 합니다.

KLFOC_UNATT_CONN_MODE_VA_NAME	다음 변수 중 하나가 필요합니다	가상 네트워크 어댑터 이름.	
KLFOC_UNATT_CONN_MODE_VA_IPV4		가상 네트워크 어댑터 IP 주소.	IP 주소
KLFOC_UNATT_CONN_MODE_VA_IPV6		가상 네트워크 어댑터 IPv6 주소.	IPv6 주소

폐쇄형 소프트웨어 환경 모드에서 Astra Linux에 Kaspersky Security Center 설치

이 섹션에서는 Astra Linux Special Edition 운영 체제에 Kaspersky Security Center 설치하는 방법을 설명합니다.

설치 전:

- 데이터베이스 관리 시스템 설치
- Kaspersky Security Center를 설치할 기기에서 지원되는 Linux 배포판 중 하나를 실행하는지 확인합니다.
- kaspersky_astra_pub_key.gpg 애플리케이션 키를 얻으려면 기술 지원에 문의하십시오 .

ksc64_[버전_번호]_amd64.deb 설치 파일을 사용합니다. Kaspersky 웹사이트에서 설치 파일을 다운로드하여 받습니다.

명령줄에서 루트 권한이 있는 계정으로 이 지침에 제공된 명령을 실행합니다.

Astra Linux Special Edition(운영 업데이트 1.7) 및 Astra Linux Special Edition(운영 업데이트 1.6) 운영 체제에 Kaspersky Security Center 설치하려면 다음을 수행하십시오.

1. /etc/digsig/digsig_initramfs.conf 파일에서 다음 설정을 지정합니다.
   `DIGSIG_ELF_MODE=1`
2. 호환성 패키지를 설치합니다.
   적절한 설치 `astra-digsig-oldkeys`
3. 애플리케이션 키용 디렉터리를 만듭니다.
   `mkdir -p /etc/digsig/keys/legacy/카스퍼스키/`
4. 이전 단계에서 만든 디렉터리에서 애플리케이션 키를 찾습니다.
   `cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/`
5. RAM 디스크 업데이트:
   업데이트`-initramfs -u -k` 모두
6. 'kladmins' 그룹과 권한 없는 계정 'ksc'를 만듭니다. 계정은 'kladmins' 그룹에 속해야 합니다. 그러려면 다음 명령을 순차적으로 실행하십시오.
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```
7. Kaspersky Security Center 설치를 실행합니다.
   - `# apt install /<경로>/ksc64_[` 버전_번호 `]_amd64.deb`

8. Kaspersky Security Center 구성을 실행합니다.

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

9. 최종 사용자 라이센스 계약서(EULA)와 개인정보취급방침을 읽어 보십시오. 텍스트가 명령줄 창에 표시됩니다. 다음 텍스트 세그먼트를 보려면 스페이스 바를 누르십시오. 그런 다음 메시지가 표시되면 다음 값을 입력합니다.

   a. EULA의 약관을 읽고 이에 동의하는 경우 y를 입력합니다. EULA의 약관에 동의하지 않는 경우 n을 입력하십시오. Kaspersky Security Center를 사용하려면 EULA 약관에 동의해야 합니다.

   b. 개인정보취급방침의 약관을 이해하고 이에 동의하는 경우 y를 입력합니다. 그러면 귀하의 데이터가 개인정보취급방침에 설명된 대로 처리 및 전송되는 데(제 3국 포함) 동의하는 것입니다. 개인정보취급방침의 약관에 동의하지 않는 경우 n을 입력하십시오. Kaspersky Security Center를 사용하려면 개인정보취급방침 약관에 동의해야 합니다.

10. 메시지가 표시되면 다음 설정을 입력합니다.

    a. 중앙 관리 서버 DNS 이름 또는 고정 IP 주소를 입력합니다.

    b. 중앙 관리 서버 포트 번호를 입력합니다. 기본적으로 포트 14000이 사용됩니다.

    c. 중앙 관리 서버 SSL 포트 번호를 입력합니다. 기본적으로 포트 13000이 사용됩니다.

    d. 다음과 같이 관리하려는 기기 수를 대략적으로 평가하십시오.

    - 1 ~ 100개의 네트워크 기기가 있는 경우 1을 입력합니다.
    - 101 ~ 1000개의 네트워크 기기가 있는 경우 2을 입력합니다.
    - 네트워크 장치가 1,000개 이상이라면 3을 입력합니다.

    e. 서비스의 보안 그룹 이름을 입력하십시오. 기본적으로 'kladmins' 그룹이 사용됩니다.

    f. 계정 이름을 입력하여 중앙 관리 서버 서비스를 시작합니다. 계정은 입력된 보안 그룹에 속해야 합니다. 기본적으로 'ksc' 계정이 사용됩니다.

    g. 다른 서비스를 시작하려면 해당 계정 이름을 입력하십시오. 계정은 입력된 보안 그룹에 속해야 합니다. 기본적으로 'ksc' 계정이 사용됩니다.

    h. 데이터베이스가 설치된 기기의 IP 주소를 입력하십시오.

    i. 데이터베이스 포트 번호를 입력하십시오. 이 포트는 중앙 관리 서버와 통신하는 데 사용됩니다. 기본적으로 포트 3306이 사용됩니다.

    j. 데이터베이스 이름을 입력합니다.

    k. 데이터베이스 액세스에 사용하는 데이터베이스 루트 계정의 로그인을 입력하십시오.

    l. 데이터베이스 액세스에 사용하는 데이터베이스 루트 계정의 암호를 입력하십시오.
    서비스가 추가되고 자동으로 시작될 때까지 기다립니다.

    - `klnagent_srv`
    - `kladminserver_srv`
    - `klactprx_srv`
    - `klwebsrv_srv`

    m. 중앙 관리 서버의 관리자 역할을 담당할 계정을 만듭니다. 사용자 이름과 암호를 입력합니다.
    암호는 다음 규칙을 따라야 합니다:

    - 사용자 암호는 8자 미만이거나 16자를 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(@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

사용자가 추가되고 Kaspersky Security Center가 설치됩니다.

서비스 검증

다음 명령을 사용하여 서비스가 실행 중인지 확인합니다.

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Kaspersky Security Center 14 웹 콘솔 설치

이 섹션에서는 Linux 운영 체제를 실행하는 기기에 Kaspersky Security Center 14 웹 콘솔 서버(Kaspersky Security Center 14 웹 콘솔이라고도 함)를 설치하는 방법에 대해 설명합니다. 설치 전에 데이터베이스 관리 시스템 및 Kaspersky Security Center 중앙 관리 서버를 설치해야 합니다.

장치에 설치된 Linux 배포판에 해당하는 다음 설치 파일 중 하나를 사용하십시오.

- 데비안 — ksc-web-console-[build_number].x86_64.deb
- RPM 기반 운영 체제 — ksc-web-console-[build_number].x86_64.rpm
- ALT 8 SP — ksc-web-console-[build_number]-alt8p.x86_64.rpm

Kaspersky 웹사이트에서 설치 파일을 다운로드하여 받습니다.

Kaspersky Security Center 14 웹 콘솔을 설치하려면 다음 단계를 따릅니다.

1. Kaspersky Security Center 14 웹 콘솔을 설치할 기기에서 지원되는 Linux 배포판 중 하나를 실행하는지 확인합니다.
2. 최종 사용자 라이센스 계약서(EULA)를 읽어 보십시오. Kaspersky Security Center Linux 배포 키트에 EULA 텍스트가 있는 TXT 파일이 없다면 Kaspersky 웹사이트 에서 다운로드할 수 있습니다. 라이센스 계약서의 약관에 동의하지 않을 경우 애플리케이션을 설치하지 마십시오.
3. Kaspersky Security Center 14 웹 콘솔을 중앙 관리 서버에 연결하기 위한 파라미터가 포함된 응답 파일을 만듭니다. 이 파일 이름을 ksc-web-console-setup.json으로 지정하고 /etc/ksc-web-console-setup.json 디렉터리에 배치합니다

   최소 파라미터 세트와 기본 주소 및 포트를 포함하는 응답 파일의 예:

   ```
   {
    "address": "127.0.0.1",
    "port": 8080,
    "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
    "acceptEula": true
   }
   ```

   Linux ALT 운영 체제에 Kaspersky Security Center 14 웹 콘솔을 설치할 때 운영 체제에서 포트 8080을 사용하므로, 8080 이외의 포트 번호를 지정해야 합니다.

   Kaspersky Security Center 14 웹 콘솔은 동일한 .rpm 설치 파일로는 업데이트할 수 없습니다. 응답 파일의 설정을 변경하고 애플리케이션을 다시 설치하는 데 이 파일을 사용하려면 먼저 애플리케이션을 제거한 다음 새 응답 파일로 다시 설치해야 합니다.

4. 사용 중인 Linux 배포판에 따라 루트 권한이 있는 계정에서 명령줄을 사용하여 확장명이 .deb 또는 .rpm인 설치 파일을 실행합니다.

   - .deb 파일로 Kaspersky Security Center 14 웹 콘솔을 설치하거나 업그레이드하려면 다음 명령을 실행하십시오.
     `$ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb`
   - .rpm 파일로 Kaspersky Security Center 14 웹 콘솔을 설치하려면 다음 명령 중 하나를 실행하십시오.
     `$ sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpm`

     또는

     `$ sudo alien -i ksc-web-console-[build_number].x86_64.rpm`
   - Kaspersky Security Center 14 웹 콘솔의 이전 버전에서 업그레이드하려면 다음 명령 중 하나를 실행하십시오.
     - RPM 기반 운영 체제를 실행하는 기기의 경우:
       `$ sudo rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm`
     - Debian 기반 운영 체제를 실행하는 기기의 경우:
       `$ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb`

그러면 설치 파일의 압축이 풀립니다. 설치가 완료될 때까지 기다립니다. Kaspersky Security Center 14 웹 콘솔은 /var/opt/kaspersky/ksc-web-console 디렉터리에 설치됩니다.

5. 다음 명령을 실행하여 모든 Kaspersky Security Center 14 웹 콘솔 서비스를 다시 시작하십시오:
   ```
   $ sudo systemctl restart KSC*
   ```

설치가 완료되면 브라우저를 사용하여 Kaspersky Security Center 14 웹 콘솔을 열고 로그인할 수 있습니다.

Kaspersky Security Center 14 웹 콘솔 설치 파라미터

Linux를 실행하는 장치에 Kaspersky Security Center 14 웹 콘솔 서버를 설치하려면 Kaspersky Security Center 14 웹 콘솔을 중앙 관리 서버에 연결하기 위한 파라미터가 포함된 응답 파일인 .json 파일을 생성해야 합니다.

다음은 최소 파라미터 세트와 기본 주소 및 포트를 포함하는 응답 파일의 예입니다.

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "defaultLangId": 1049,
 "enableLog": false,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
 "acceptEula": true,
 "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
 "webConsoleAccount": "Group1:User1",
 "managementServiceAccount": "Group1:User2",
 "serviceWebConsoleAccount": "Group1:User3",
 "pluginAccount": "Group1:User4",
 "messageQueueAccount": "Group1:User5"
}
```

Linux ALT 운영 체제에 Kaspersky Security Center 14 웹 콘솔을 설치할 때 운영 체제에서 포트 8080을 사용하므로 8080 이외의 포트 번호를 지정해야 합니다.

아래 표는 응답 파일에 지정할 수 있는 파라미터를 설명합니다.

Linux 실행 기기에 Kaspersky Security Center 14 웹 콘솔을 설치하기 위한 파라미터

파라미터	설명	사용 가능한 값
`address`	Kaspersky Security Center 14 웹 콘솔 서버의 주소입니다(필수).	문자열 값.
포트	Kaspersky Security Center 14 웹 콘솔 서버에서 중앙 관리 서버에 연결하는 데 사용하는 포트의 수입니다(필수).	숫자 값.
`defaultLangId`	사용자 인터페이스 언어입니다(기본적으로 `1033`).	언어의 숫자 코드: • German: `1031` • 영어: `1033` • 스페인어: `3082` • 스페인어(멕시코): `2058` • 프랑스어: `1036` • 일본어: `1041` • 카자흐어: `1087` • 폴란드어: `1045` • 포르투갈어(브라질): `1046`

		• 러시아어: `1049` • 터키어: `1055` • 중국어 간체: `4` • 중국어 번체: `31748` 값을 지정하지 않으면 영어(en-US)가 사용됩니다.
`enableLog`	Kaspersky Security Center 14 웹 콘솔 활동 로깅을 활성화할지 여부입니다.	부울 값: • `true` - 로깅이 활성화됩니다(기본적으로 선택되어 있음). • `false` - 로깅이 비활성화됩니다.
`trusted`	Kaspersky Security Center 14 웹 콘솔에 연결할 수 있도록 허용된 신뢰할 수 있는 중앙 관리 서버의 목록 각 중앙 관리 서버는 다음 파라미터로 정의해야 합니다. • 중앙 관리 서버 주소 • Kaspersky Security Center 14 웹 콘솔이 중앙 관리 서버에 연결하는 데 사용할 OpenAPI 포트 (기본값: 13299) • 중앙 관리 서버 인증서 경로 • 로그인 창에 표시될 중앙 관리 서버의 이름 파라미터는 세로 막대로 구분됩니다. 여러 중앙 관리 서버가 지정된 경우 두 개의 수직 막대(파이프)로 구분하십시오.	다음 형식의 문자열 값: `" server address | port | certificate path | server name "`. 예: `"X.X.X.X|13299|/cert/server-1.cer| Server 1 ||Y.Y.Y.Y|13299|/cert/server-2.cer| Server 2 "`.
`acceptEula`	EULA(최종 사용자 라이센스 계약서)의 조항에 동의하는지 여부입니다. EULA 조항이 포함된 파일이 설치 파일과 함께 다운로드됩니다.	부울 값: • `true` —최종 사용자 라이센스 계약서의 조항을 완전히 읽고 이해했으며 이에 동의합니다. • `false` - 라이센스 계약서에 동의하지 않습니다(기본적으로 선택됨). 값을 지정하지 않으면 Kaspersky Security Center 14 웹 콘솔 설치 프로그램이 EULA를 표시하고 EULA 조건에 수락하는지 묻습니다.
`certDomain`	새 인증서를 생성하려면 이 파라미터를 사용하여 새 인증서를 생성할 도메인 이름을 지정하십시오.	문자열 값.
`certPath`	기존 인증서를 사용하려면 이 파라미터를 사용하여 인증서 파일의 경로를 지정하십시오.	문자열 값. 기존 인증서를 사용할 경로 `"/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"`를 지정합니다. 사용자 지정 인증서의 경우 이 사용자 지정 인증서가 저장되는 경로를 지정합니다.
`keyPath`	기존 인증서를 사용하려면 이 파라미터를 사용하여 키 파일의 경로를 지정하십시오.	문자열 값.
`webConsoleAccount`	KSCWebConsole 서비스가 실행되는 계정의 이름입니다.	다음 형식의 문자열 값: `" group name : user name "`. 예: `" Group1 : User1 "`. 값을 지정하지 않으면 Kaspersky Security Center 14 웹 콘솔 설치 프로그램이 기본 이름인 `user_management_%uid%`(으)로 새 계정을 생성합니다.
`managementServiceAccount`	KSCWebConsoleManagement 서비스가 실행되는 권한 보유 계정 이름입니다.	다음 형식의 문자열 값: `" group name : user name "`. 예: `" Group1 : User1 "`. 값을 지정하지 않으면 Kaspersky Security Center 14 웹 콘솔 설치 프로그램이 기본 이름인 `user_nodejs_%uid%`(으)로 새 계정을 생성합니다.

`serviceWebConsoleAccount`	KSCSvcWebConsole 서비스를 실행하는 계정 이름입니다.	다음 형식의 문자열 값: "`group name : user name`". 예: "`Group1 : User1`". 값을 지정하지 않으면 Kaspersky Security Center 14 웹 콘솔 설치 프로그램이 기본 이름인 `user_svc_nodejs_%uid%`(으)로 새 계정을 생성합니다.
`pluginAccount`	KSCWebConsolePlugin 서비스를 실행하는 계정 이름입니다.	다음 형식의 문자열 값: "`group name : user name`". 예: "`Group1 : User1`". 값을 지정하지 않으면 Kaspersky Security Center 14 웹 콘솔 설치 프로그램이 기본 이름인 `user_web_plugin_%uid%`(으)로 새 계정을 생성합니다.
`messageQueueAccount`	KSCWebConsoleMessageQueue 서비스를 실행하는 계정 이름입니다.	다음 형식의 문자열 값: "`group name : user name`". 예: "`Group1 : User1`". 값을 지정하지 않으면 Kaspersky Security Center 14 웹 콘솔 설치 프로그램이 기본 이름인 `user_message_queue_%uid%`(으)로 새 계정을 생성합니다.

`webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `messageQueueAccount` 매개변수를 지정할 시, 사용자 정의 사용자 계정이 같은 보안 그룹에 속하는지 확인하십시오. 이러한 매개변수를 지정하지 않으면 Kaspersky Security Center 14 웹 콘솔 설치 프로그램이 기본 보안 그룹을 생성한 후 이 그룹에 기본 이름의 사용자 계정을 생성합니다.

Kaspersky 장애 조치 클러스터 노드에 설치된 중앙 관리 서버에 연결된 Kaspersky Security Center 14 웹 콘솔 설치

이 섹션에서는 Kaspersky 장애 조치 클러스터 노드에 설치된 중앙 관리 서버에 연결되는 Kaspersky Security Center 14 웹 콘솔 서버(이하 Kaspersky Security Center 14 웹 콘솔이라고도 함)를 설치하는 방법을 설명합니다. Kaspersky Security Center 14 웹 콘솔을 설치하기 전에 Kaspersky 장애 조치 클러스터 노드에 데이터베이스 관리 시스템과 Kaspersky Security Center 관리 서버를 설치합니다.

Kaspersky 장애 조치 클러스터 노드에 설치된 중앙 관리 서버에 연결되는 Kaspersky Security Center 14 웹 콘솔을 설치하려면:

1. Kaspersky Security Center 14 웹 콘솔 설치의 1단계와 2단계를 수행합니다.
2. 3단계에서, 응답 파일에서 Kaspersky 장애 조치 클러스터가 Kaspersky Security Center 14 웹 콘솔에 연결할 수 있도록 신뢰할 수 있는 설치 매개변수를 지정합니다. 이 매개변수의 문자열 값은 다음 형식을 가집니다.
   ```
   "trusted": "server address|port|certificate path|server name"
   ```
   신뢰하는 설치 매개변수의 구성 요소를 지정합니다.
   - **중앙 관리 서버 주소**. 클러스터 노드를 준비할 때 가상 네트워크 어댑터를 만들었다면, 어댑터의 IP 주소를 Kaspersky 장애 조치 클러스터 주소로 사용합니다. 생성하지 않았다면 사용 중인 타사 로드 밸런서의 IP 주소를 지정합니다.
   - **중앙 관리 서버 포트**. Kaspersky Security Center 14 웹 콘솔이 중앙 관리 서버에 연결하는 데 사용하는 OpenAPI 포트입니다(기본값은 13299).
   - **중앙 관리 서버 인증서**. 중앙 관리 서버 인증서는 Kaspersky 장애 조치 클러스터의 공유 데이터 저장소에 있습니다. 인증서 파일의 기본 경로: <공유 데이터 폴더>\1093\cert\klserver.cer. 공유 데이터 저장소에서 Kaspersky Security Center 14 웹 콘솔을 설치하는 장치로 인증서 파일을 복사합니다. 중앙 관리 서버 인증서의 로컬 경로를 지정합니다.
   - **중앙 관리 서버 이름**. Kaspersky Security Center 14 웹 콘솔의 로그인 창에 표시될 Kaspersky 장애 조치 클러스터 이름입니다.
3. Kaspersky Security Center 14 웹 콘솔 기본 설치를 실행합니다.

설치가 완료되면 바탕화면에 바로가기가 나타나고, Kaspersky Security Center 14 웹 콘솔에 로그인할 수 있습니다.

발견 및 배포 → 미할당 기기로 이동하여 클러스터 노드 및 파일 서버에 대한 정보를 볼 수 있습니다.

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(비대화식) 모드에서 설치를 실행할 수 있으므로 사용자가 개입할 필요가 없습니다.

숨김 모드에서 Linux에 네트워크 에이전트를 설치하려면

1. SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면 insserv-compat 패키지를 먼저 설치 해서 네트워크 에이전트를 구성합니다.
2. 최종 사용자 라이센스 계약서를 읽어 보십시오. 최종 사용자 라이센스 계약서의 조건을 이해하고, 이에 동의하는 경우에만 아래 단계를 따르십시오.

3. 다음과 같이 응답 파일의 전체 이름(경로 포함)을 입력하여 KLAUTOANSWERS 환경 변수의 값을 설정합니다.

```
export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
```

4. 환경 변수에 지정한 디렉토리에서 응답 파일(TXT 형식)을 만듭니다. 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(비대화식) 설치 모드를 활성화할지 여부를 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 정의합	기존 포트 번호면 됩니다.

		니다. 기본값은 15000입니다.	
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. 4 - 네트워크 에이전트 인스턴스를 DMZ(완충 지역)에서 연결 게이트웨이로 사용합니다.
KLNAGENT_GW_ADDRESS	아니요	연결 게이트웨이의 주소를 정의합니다. 이 값은 KLNAGENT_GW_MODE=3인 경우에만 적용할 수 있습니다.	DNS 이름 또는 IP 주소입니다.

5. 네트워크 에이전트 설치:

- 32비트 운영 체제에서 RPM 패키지로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
  `# rpm -i klnagent-<빌드 번호>.i386.rpm`
- 64비트 운영 체제에서 RPM 패키지로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
  `# rpm -i klnagent64-<빌드 번호>.x86_64.rpm`
- Arm 아키텍처용 64비트 운영 체제에서 RPM 패키지로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오:
  `# rpm -i klnagent64-<빌드 번호>.aarch64.rpm`
- 32비트 운영 체제에서 DEB 패키지로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
  `# apt-get install ./klnagent_<빌드 번호>_i386.deb`
- 64비트 운영 체제에서 DEB 패키지로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오.
  `# apt-get install ./klnagent64_<빌드 번호>_amd64.deb`
- Arm 아키텍처용 64비트 운영 체제에 DEB 패키지로 네트워크 에이전트를 설치하려면 다음 명령을 실행하십시오:
  `# apt-get install ./klnagent64_<빌드 번호>_arm64.deb`

Linux용 네트워크 에이전트 설치가 숨김 모드에서 시작됩니다. 설치 중 작업에 관한 메시지가 사용자에게 표시되지 않습니다.

DBMS 작업용 계정

중앙 관리 서버를 설치하고 작업하려면 내부 DBMS 계정이 필요합니다. 이 계정을 사용하면 DBMS에 접근할 수 있으며, 특정 권한이 필요합니다. DBMS 계정에 권한을 부여할 때는 최소 권한 원칙을 따릅니다. 즉, 필요한 작업을 수행할 수 있을 정도의 권한만 부여해야 합니다. 중앙 관리 서버를 설치하고 시작하기 전에 DBMS 계정에 권한을 부여해야 합니다.

Kaspersky Security Center 14 Linux는 MySQL 및 MariaDB DBMS를 지원합니다. 이러한 DBMS 중 하나에 대한 내부 계정을 생성한 후 이 계정에 필요한 권한을 부여합니다. 내부 MySQL 계정과 내부 MariaDB 계정의 권한 집합은 동일합니다. 필요한 권한은 다음과 같습니다.

- 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.

계정 권한을 구성하는 방법에 대한 자세한 내용은 MySQL 및 MariaDB 작업을 위한 DBMS 계정 구성을 참조하십시오.

내부 DBMS 계정에 부여한 권한은 백업에서 중앙 관리 서버 데이터를 복원하기에 충분합니다.

MySQL 및 MariaDB 작업을 위한 DBMS 계정 구성

필수 구성 요소

DBMS 계정에 권한을 할당하기 전에 다음 작업을 수행하십시오:

1. 로컬 관리자 계정으로 시스템에 로그인했는지 확인하십시오.
2. MySQL 또는 MariaDB 작업을 위한 환경을 설치합니다.

중앙 관리 서버 설치에 대한 DBMS 계정 구성

중앙 관리 서버 설치를 위한 DBMS 계정을 구성하려면:

1. DBMS 설치 시 생성한 루트 계정으로 MySQL 또는 MariaDB 작업을 위한 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.

   비밀번호로 DBMS 계정을 생성하려면 다음 명령을 실행합니다.

   ```
   /* Create a user named KSCAdmin and specify the password for KSCAdmin */
   CREATE USER 'KSCAdmin' IDENTIFIED BY '< password >';
   ```

   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 '< password >';
     ```

   - 기존 DBMS 계정에 대한 인증을 변경하려면 다음 명령을 실행합니다.

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '< password >';
     ```

3. 생성한 DBMS 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

   생성된 DBMS 계정에 필요한 권한을 부여하려면 다음 스크립트를 실행합니다.

   ```
   /* 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.

4. DBMS 계정에 부여된 권한 목록을 보려면 다음 명령을 실행합니다:

   ```
   SHOW grants for 'KSCAdmin'
   ```

5. 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'
   COLLATE 'ascii_general_ci';
   ```

DBMS 계정을 생성하는 스크립트에서 지정한 것과 같은 데이터베이스 이름을 사용합니다.

6. 중앙 관리 서버 설치.

설치가 완료되면 중앙 관리 서버 데이터베이스가 생성되고 중앙 관리 서버를 사용할 수 있습니다.

Kaspersky 장애 조치 클러스터 배포

이 섹션에는 Kaspersky 장애 조치 클러스터에 대한 일반 정보와 네트워크에서 Kaspersky 장애 조치 클러스터를 준비하고 배포하는 작업에 대한 지침이 모두 포함되어 있습니다.

시나리오: Kaspersky 장애 조치 클러스터 배포

Kaspersky 장애 조치 클러스터는 Kaspersky Security Center의 고가용성을 제공하고 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.

Kaspersky 애플리케이션 배포는 다음 단계로 진행됩니다.

1. **Kaspersky Security Center 서비스용 계정 생성**

   활성 노드, 수동 노드, 파일 서버에서 다음 단계를 수행합니다.

   1. 이름이 'kladmins'인 도메인 그룹을 생성하고 세 그룹에 모두 같은 GID를 할당합니다. 그룹에 로컬 관리자 권한을 부여합니다.
   2. 이름이 'ksc'인 사용자 계정을 생성하고 세 사용자 계정에 모두 같은 UID를 할당합니다. 'kladmins' 도메인 그룹에 계정을 추가합니다.
   3. 이름이 'rightless'인 사용자 계정을 만들고 세 사용자 계정에 모두 같은 UID를 할당합니다. 'kladmins' 도메인 그룹에 계정을 추가합니다.

2. **파일 서버 준비**

   Kaspersky 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 장애 조치 클러스터용 파일 서버 준비

3. **액티브 및 패시브 노드 준비**

   같은 하드웨어 및 소프트웨어를 사용하며 액티브 및 패시브 노드로 작동할 두 대의 컴퓨터를 준비합니다.

   방법 설명: Kaspersky 장애 조치 클러스터용 노드 준비

4. **데이터베이스 관리 시스템(DBMS) 설치**

   두 가지 옵션이 있습니다.

   - MariaBD Galera Cluster 사용 시, DBMS 전용 컴퓨터가 필요하지 않습니다. 각 노드에 MariaDB Galera Cluster를 설치합니다.
   - 다른 지원 DBMS를 사용하려면 선택한 DBMS를 전용 컴퓨터에 설치합니다.

5. **Kaspersky Security Center 설치**

   두 노드에 장애 조치 클러스터 모드로 Kaspersky Security Center를 설치합니다. 먼저 액티브 노드에 Kaspersky Security Center를 설치한 다음 패시브 노드에 설치해야 합니다.

   또한 클러스터 노드가 아닌 별도의 장치에 Kaspersky Security Center 14 웹 콘솔을 설치할 수 있습니다.

6. **장애 조치 클러스터 테스트**

   장애 조치 클러스터를 올바르게 구성했으며 제대로 작동하는지 확인합니다. 예를 들어, 액티브 노드에서 Kaspersky Security Center 서비스(kladminserver, klnagent, ksnproxy, klactprx 또는 klwebsrv) 중 하나를 중지해 보면 됩니다. 서비스가 중지되면 보호 관리가 패시브 노드로 자동 전환되어야 합니다.

결과

Kaspersky 장애 조치 클러스터가 배포됩니다. 액티브 노드와 패시브 노드를 전환하는 이벤트를 숙지해두는 것이 좋습니다.

Kaspersky 장애 조치 클러스터 정보

Kaspersky 장애 조치 클러스터는 Kaspersky Security Center의 고가용성을 제공하고 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.

Kaspersky 장애 조치 클러스터에서는 모든 Kaspersky Security Center 서비스가 자동 관리됩니다. 서비스를 수동으로 다시 시작하지 마십시오.

하드웨어 및 소프트웨어 요구 사항

Kaspersky 장애 조치 클러스터를 배포하려면 다음 하드웨어가 있어야 합니다.

- 하드웨어와 소프트웨어가 동일한 두 대의 컴퓨터. 이러한 컴퓨터는 액티브 노드와 패시브 노드 역할을 합니다.
- EXT4 파일 시스템이 있고 Linux를 실행하는 파일 서버. 파일 서버 역할을 할 전용 컴퓨터도 제공해야 합니다.

  파일 서버와 액티브 및 패시브 노드 사이에 네트워크 고대역폭을 제공했는지 확인하십시오.

- 데이터베이스 관리 시스템(DBMS)이 있는 컴퓨터. MariaBD Galera Cluster를 DBMS로 사용 시, 이를 위한 전용 컴퓨터가 필요하지 않습니다.

전환 조건

액티브 노드에 다음 이벤트 중 하나가 발생하면, 장애 조치 클러스터가 클라이언트 장치의 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 장애 조치 클러스터용 파일 서버 준비

파일 서버는 Kaspersky 장애 조치 클러스터의 필수 구성 요소입니다.

파일 서버를 준비하려면:

1. 파일 서버가 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인하십시오.
2. NFS 서버 설치 및 구성:
   - NFS 서버 설정에서 두 노드에 대해 파일 서버에 대한 액세스를 활성화해야 합니다.
   - NFS 프로토콜은 버전은 4.0 또는 4.1이어야 합니다.
   - Linux 커널의 최소 요구 사항:
     - NFS 4.0 사용 시 3.19.0-25
     - NFS 4.1 사용 시 4.4.0-176
3. 파일 서버에서 두 개의 폴더를 만들고 NFS를 사용하여 공유합니다. 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.

   다음 명령을 실행합니다.

   ```
   sudo yum install nfs-utils
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo cat /etc/exports
   sudo exportfs -a
   sudo systemctl start rpcbind
   ```

```
sudo service nfs start
```

다음 명령을 실행하여 자동 시작을 활성화합니다.

```
sudo systemctl enable rpcbind
```

4. 파일 서버를 다시 시작합니다.

파일 서버가 준비되었습니다. Kaspersky 장애 조치 클러스터를 배포하려면 이 시나리오의 추가 지침을 따르십시오.

Kaspersky 장애 조치 클러스터용 노드 준비

Kaspersky 장애 조치 클러스터의 액티브 노드와 패시브 노드 역할을 할 두 대의 컴퓨터를 준비합니다.

Kaspersky 장애 조치 클러스터용 노드를 준비하려면:

1. 하드웨어 및 소프트웨어 요구 사항을 충족하는 두 대의 컴퓨터가 있는지 확인합니다. 두 대의 컴퓨터는 장애 조치 클러스터의 액티브 노드와 패시브 노드 역할을 합니다.

2. 노드가 NFS 클라이언트로 작동하도록 하려면 각 노드에 nfs-utils 패키지를 설치합니다.

   다음 명령을 실행합니다:

   ```
   sudo yum install nfs-utils
   ```

3. 다음 명령을 실행하여 탑재 지점을 만듭니다.

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. 공유 폴더를 성공적으로 탑재할 수 있는지 확인합니다. [선택 단계]

   다음 명령을 실행합니다.

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{path to the KlFocStateShare folder}
   /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{path to the KlFocDataShare_klfoc
   folder} /mnt/KlFocDataShare_klfoc
   ```

   여기서 `{server}:{path to the KlFocStateShare folder}` 및 `{server}:{path to the KlFocDataShare_klfoc folder}`는 파일 서버의 공유 폴더에 대한 네트워크 경로입니다.

   공유 폴더를 성공적으로 탑재한 후 다음 명령을 실행하여 탑재를 해제합니다.

   ```
   sudo umount /mnt/KlFocStateShare
   sudo umount /mnt/KlFocDataShare_klfoc
   ```

5. 탑재 지점과 공유 폴더가 일치하도록 합니다.

   ```
   sudo vi /etc/fstab
   {server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare nfs
   vers=4,nolock,local_lock=none,auto,user,rw 0 0
   {server}:{path to the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc nfs
   vers=4,nolock,local_lock=none,noauto,user,rw 0 0
   ```

   여기서 `{server}:{path to the KlFocStateShare folder}` 및 `{server}:{path to the KlFocDataShare_klfoc folder}`는 파일 서버의 공유 폴더에 대한 네트워크 경로입니다.

6. 두 노드를 모두 다시 시작합니다.

7. 다음 명령을 실행하여 공유 폴더를 탑재합니다.

   ```
   mount /mnt/KlFocStateShare
   mount /mnt/KlFocDataShare_klfoc
   ```

8. 공유 폴더에 액세스할 수 있는 권한이 ksc:kladmins에 속해야 합니다.

   다음 명령을 실행합니다:

   ```
   sudo ls -la /mnt/
   ```

9. 각 노드에서 네트워크 어댑터를 만듭니다. 다음 중 하나를 수행합니다:

   - 가상 네트워크 어댑터를 사용합니다.

     a. 다음 명령으로 물리 어댑터 관리에 NetworkManager를 사용하는 지 확인합니다.

     ```
     nmcli device status
     ```

     물리 어댑터가 관리 중이 아니라는 결과가 출력되면, 물리 어댑터를 관리하도록 NetworkManager를 구성합니다. 정확한 구성 단계는 배포판에 따라 다릅니다.

     b. 다음 명령을 사용하여 인터페이스를 식별합니다.

     ```
     ip a
     ```

c. 새 구성 프로필을 만듭니다.

```
nmcli connection add type macvlan dev <물리 인터페이스> mode bridge ifname <가상 인터페이스>
ipv4.addresses <주소 마스크> ipv4.method manual autoconnect no
```

- 물리 네트워크 어댑터 또는 하이퍼바이저를 사용합니다. 이 시나리오에서는 소프트웨어 NetworkManager를 비활성화합니다.

  a. 대상 인터페이스에 대한 NetworkManager 연결을 삭제합니다.

  ```
  nmcli con del <연결 이름>
  ```

  다음 명령으로 대상 인터페이스에 연결이 있는지 확인합니다.

  ```
  nmcli con show
  ```

  b. NetworkManager.conf 파일을 편집합니다. keyfile 섹션을 찾아 대상 인터페이스를 unmanaged-devices 매개변수에 지정합니다.

  ```
  [키파일]
  unmanaged-devices=interface-name:<인터페이스 이름>
  ```

  c. NetworkManager를 다시 시작합니다.

  ```
  systemctl reload NetworkManager
  ```

  다음 명령으로 대상 인터페이스의 관리 여부를 확인합니다.

  ```
  nmcli dev status
  ```

- 타사 로드 밸런서를 사용합니다. 예를 들어 nginx 서버를 사용할 수 있습니다. 이 경우 다음을 수행하십시오.

  a. nginx가 설치된 전용 Linux 기반 컴퓨터를 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 13291, TCP 13299, TCP 17000)를 엽니다.

노드가 준비되었습니다. Kaspersky 장애 조치 클러스터를 배포하려면 시나리오의 추가 지침을 따릅니다.

Kaspersky 장애 조치 클러스터 노드에 Kaspersky Security Center 설치

이 절차에서는 Kaspersky 장애 조치 클러스터의 노드에 Kaspersky Security Center를 설치하는 방법을 설명합니다. Kaspersky Security Center는 Kaspersky 장애 조치 클러스터의 두 노드에 별도로 설치됩니다. 먼저 액티브 노드에 애플리케이션을 설치한 다음 패시브 노드에 설치합니다. 설치할 때 액티브 노드와 패시브 노드를 선택합니다.

기기에 설치된 Linux 배포판에 따라 file—ksc64_[version_number]_amd64.deb 또는 ksc64-[version_number].x86_64.rpm 설치 파일을 사용합니다. Kaspersky 웹사이트에서 설치 파일을 다운로드하여 받습니다.

KLAdmins 도메인 그룹의 사용자만 모든 노드에 Kaspersky Security Center를 설치할 수 있습니다.

기본(액티브) 노드에 설치

기본 노드에 Kaspersky Security Center를 설치하려면:

1. Kaspersky Security Center를 설치할 기기에서 지원되는 Linux 배포판 중 하나를 실행하는지 확인합니다.
2. 명령줄에서 루트 권한이 있는 계정으로 이 지침에 제공된 명령을 실행합니다.
3. Kaspersky Security Center 설치를 실행합니다. Linux 배포판에 따라 다음 명령 중 하나를 실행합니다.
   - `sudo apt install /<경로>/ksc64_[ 버전_번호 ]_amd64.deb`
   - `sudo yum install /<경로>/ksc64-[ 버전_번호 ].x86_64.rpm -y`
4. Kaspersky Security Center 구성을 실행합니다.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. 최종 사용자 라이센스 계약서(EULA)와 개인정보취급방침을 읽어 보십시오. 텍스트가 명령줄 창에 표시됩니다. 다음 텍스트 세그먼트를 보려면 스페이스 바를 누르십시오. 그런 다음 메시지가 표시되면 다음 값을 입력합니다.

   a. EULA의 약관을 읽고 이에 동의하는 경우 y를 입력합니다. EULA의 약관에 동의하지 않는 경우 n을 입력하십시오. Kaspersky Security Center를 사용하려면 EULA 약관에 동의해야 합니다.

   b. 개인정보취급방침의 약관을 이해하고 이에 동의하는 경우 y를 입력합니다. 그러면 귀하의 데이터가 개인정보취급방침에 설명된 대로 처리 및 전송되는 데(제 3국 포함) 동의하는 것입니다. 개인정보취급방침의 약관에 동의하지 않는 경우 n을 입력하십시오. Kaspersky Security Center를 사용하려면 개인정보취급방침 약관에 동의해야 합니다.

6. 중앙 관리 서버 설치 모드로 **기본 클러스터 노드**를 선택합니다.

7. 메시지가 표시되면 다음 설정을 입력합니다.

   a. 상태 공유의 탑재 지점에 대한 로컬 경로를 입력합니다.

   b. 데이터 공유의 탑재 지점에 대한 로컬 경로를 입력합니다.

   c. 장애 조치 클러스터 연결 모드를 가상 네트워크 어댑터 또는 외부 부하 분산 장치로 선택합니다.

   d. 가상 네트워크 어댑터를 사용한다면, 해당 이름을 입력합니다.

   e. 중앙 관리 서버 DNS 이름 또는 고정 IP 주소를 입력하라는 메시지가 표시되면, 가상 네트워크 어댑터의 IP 주소 또는 외부 로드 밸런서의 IP 주소를 입력합니다.

   f. 중앙 관리 서버 포트 번호를 입력합니다. 기본적으로 포트 14000이 사용됩니다.

   g. 중앙 관리 서버 SSL 포트 번호를 입력합니다. 기본적으로 포트 13000이 사용됩니다.

   h. 다음과 같이 관리하려는 기기 수를 대략적으로 평가하십시오.

      - 1 ~ 100개의 네트워크 기기가 있는 경우 1을 입력합니다.
      - 101 ~ 1000개의 네트워크 기기가 있는 경우 2을 입력합니다.
      - 네트워크 장치가 1,000개 이상이라면 3을 입력합니다.

   i. 서비스의 보안 그룹 이름을 입력하십시오. 기본적으로 'kladmins' 그룹이 사용됩니다.

   j. 계정 이름을 입력하여 중앙 관리 서버 서비스를 시작합니다. 계정은 입력된 보안 그룹에 속해야 합니다. 기본적으로 'ksc' 계정이 사용됩니다.

   k. 다른 서비스를 시작하려면 해당 계정 이름을 입력하십시오. 계정은 입력된 보안 그룹에 속해야 합니다. 기본적으로 'ksc' 계정이 사용됩니다.

   l. 데이터베이스가 설치된 기기의 IP 주소를 입력하십시오.

   m. 데이터베이스 포트 번호를 입력하십시오. 이 포트는 중앙 관리 서버와 통신하는 데 사용됩니다. 기본적으로 포트 3306이 사용됩니다.

   n. 데이터베이스 이름을 입력합니다.

   o. 데이터베이스 액세스에 사용하는 데이터베이스 루트 계정의 로그인을 입력하십시오.

   p. 데이터베이스 액세스에 사용하는 데이터베이스 루트 계정의 암호를 입력하십시오.
   서비스가 추가되고 자동으로 시작될 때까지 기다립니다.

      - klnagent_srv
      - kladminserver_srv
      - klactprx_srv
      - klwebsrv_srv

   q. 중앙 관리 서버의 관리자 역할을 담당할 계정을 만듭니다. 사용자 이름과 암호를 입력합니다. 사용자 암호는 8자 미만이거나 16자를 초과할 수 없습니다.

사용자가 추가되고 Kaspersky Security Center가 기본 노드에 설치됩니다.

보조(패시브) 노드에 설치

패비스 노드에 Kaspersky Security Center를 설치하려면:

1. Kaspersky Security Center를 설치할 기기에서 지원되는 Linux 배포판 중 하나를 실행하는지 확인합니다.

2. 명령줄에서 루트 권한이 있는 계정으로 이 지침에 제공된 명령을 실행합니다.

3. Kaspersky Security Center 설치를 실행합니다. Linux 배포판에 따라 다음 명령 중 하나를 실행합니다.

   - `sudo apt install /<경로>/ksc64_[ 버전_번호 ]_amd64.deb`
   - `sudo yum install /<경로>/ksc64-[ 버전_번호 ].x86_64.rpm -y`

4. Kaspersky Security Center 구성을 실행합니다.

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

5. 최종 사용자 라이센스 계약서(EULA)와 개인정보취급방침을 읽어 보십시오. 텍스트가 명령줄 창에 표시됩니다. 다음 텍스트 세그먼트를 보려면 스페이스 바를 누르십시오. 그런 다음 메시지가 표시되면 다음 값을 입력합니다.

   a. EULA의 약관을 읽고 이에 동의하는 경우 `y`를 입력합니다. EULA의 약관에 동의하지 않는 경우 `n`을 입력하십시오. Kaspersky Security Center를 사용하려면 EULA 약관에 동의해야 합니다.

   b. 개인정보취급방침의 약관을 이해하고 이에 동의하는 경우 `y`를 입력합니다. 그러면 귀하의 데이터가 개인정보취급방침에 설명된 대로 처리 및 전송되는 데(제 3국 포함) 동의하는 것입니다. 개인정보취급방침의 약관에 동의하지 않는 경우 `n`을 입력하십시오. Kaspersky Security Center를 사용하려면 개인정보취급방침 약관에 동의해야 합니다.

6. 중앙 관리 서버 설치 모드로 **보조 클러스터 노드**를 선택합니다.

7. 메시지가 표시되면 상태 공유의 탑재 지점에 대한 로컬 경로를 입력합니다.

Kaspersky Security Center가 보조 노드에 설치됩니다.

서비스 검증

다음 명령을 사용하여 서비스가 실행 중인지 확인합니다.

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

이제 Kaspersky 장애 조치 클러스터를 테스트하여 올바르게 구성했는지, 클러스터가 제대로 작동하는지 확인할 수 있습니다.

수동으로 클러스터 노드 시작 및 중지

유지 관리를 위해 전체 Kaspersky 장애 조치 클러스터를 중지하거나 클러스터 노드 중 하나를 일시적으로 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 /opt/kaspersky/ksc64/sbin으로 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. 유지하려는 노드에서 /opt/kaspersky/ksc64/sbin으로 이동합니다.
3. 명령줄을 열고 `detach_node.sh` 명령을 실행하여 클러스터에서 해당 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. 유지한 노드에서 /opt/kaspersky/ksc64/sbin으로 이동합니다.

8. 명령줄을 열고 `attach_node.sh` 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.

Kaspersky Security Center 작업용 인증서

이 섹션에서는 Kaspersky Security Center 인증서에 관한 정보가 나와 있으며, Kaspersky Security Center 14 웹 콘솔에 대한 인증서를 발급 및 교체하는 방법과 서버가 Kaspersky Security Center 14 웹 콘솔과 상호 작용할 시 중앙 관리 서버의 인증서를 갱신하는 방법에 대해 설명합니다.

Kaspersky Security Center 인증서 정보

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

- 중앙 관리 서버 인증서
- 웹 서버 인증서
- Kaspersky Security Center 14 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 klsetsrvcert 유틸리티 또는 Kaspersky Security Center 14 웹 콘솔의 중앙 관리 서버 속성 섹션을 통해 인증서를 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.

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

중앙 관리 서버 인증서

다음을 위해 중앙 관리 서버 인증서가 필요합니다.

- Kaspersky Security Center 14 웹 콘솔 연결 시 중앙 관리 서버 인증
- 관리 중인 장치에서 중앙 관리 서버와 네트워크 에이전트 간의 안전한 상호 작용
- 기본 중앙 관리 서버가 보조 중앙 관리 서버에 연결될 시 인증

중앙 관리 서버 인증서는 중앙 관리 서버 구성 요소 설치 시 자동 생성되며 /var/opt/kaspersky/klnagent_srv/1093/cert/ 폴더에 저장됩니다. 응답 파일 생성 시 중앙 관리 서버 인증서를 지정하여 Kaspersky Security Center 14 웹 콘솔을 설치할 수 있습니다. 이 인증서를 공통("C")이라고 합니다.

중앙 관리 서버 인증서는 397일간 유효합니다. Kaspersky Security Center는 공통 인증서가 만료되기 90일 전에 공통 예약("CR") 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 서버 인증서의 최대 유효 기간은 397일 이하여야 합니다.

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. 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.

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.

웹 서버 인증서

이 특별한 유형의 인증서는 Kaspersky Security Center 중앙 관리 서버의 구성 요소인 웹 서버에 의해 사용됩니다. 관리 중인 장치에 다운로드할 네트워크 에이전트 설치 패키지를 게시하는 데 이 인증서가 필요합니다. 이를 위해 웹 서버는 다양한 인증서를 사용할 수 있습니다.

웹 서버는 우선 순위에 따라 다음과 같은 인증서 중 하나를 사용합니다.

1. Kaspersky Security Center 14 웹 콘솔을 통해 수동으로 지정한 사용자 지정 웹 서버 인증서
2. 공통 중앙 관리 서버 인증서("C")

Kaspersky Security Center 14 웹 콘솔 인증서

Kaspersky Security Center 14 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.

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: • 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. 경로 길이 제한 값은 "없음" 및 그 외의 정수일 수 있지만, 단 "1" 이상이어야 합니다.
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 웹 브라우저의 유효한 요구 사항 및 CA/Browser Forum 의 현재 기본 요구 사항을 충족합니다.	해당 없음.
Kaspersky Security Center 14 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 14 웹 콘솔에서 지원되지 않습니다.

Kaspersky Security Center 14 웹 콘솔용 인증서 재발급

대부분의 브라우저는 인증서의 유효 기간을 제한합니다. 이 제한에 따라, Kaspersky Security Center 14 웹 콘솔 인증서의 유효 기간은 397일로 제한됩니다. 새로 자체 서명된 인증서를 수동으로 발행하여 인증 기관(CA)에서 받은 기존 인증서를 대체 할 수 있습니다. 또는 만료된 Kaspersky Security Center 14 웹 콘솔 인증서를 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.

만료된 Kaspersky Security Center 14 웹 콘솔 인증서를 재발급하려면 다음 단계를 따릅니다.

다음 중 하나를 수행하여 Kaspersky Security Center 14 웹 콘솔을 다시 설치합니다.

- Kaspersky Security Center 14 웹 콘솔의 같은 설치 파일을 사용하려면 Kaspersky Security Center 14 웹 콘솔을 제거한 후 같은 Kaspersky Security Center 14 웹 콘솔 버전을 설치합니다.
- 업그레이드된 버전의 설치 파일을 사용하려면 업그레이드 명령을 실행합니다.

Kaspersky Security Center 14 웹 콘솔 인증서가 397일의 유효 기간으로 재발급됩니다.

Kaspersky Security Center 14 웹 콘솔 인증서 교체

기본적으로 Kaspersky Security Center 14 웹 콘솔 서버(Kaspersky Security Center 14 웹 콘솔이라고도 함)를 설치하면 애플리케이션에 대한 브라우저 인증서가 자동으로 생성됩니다. 자동으로 생성된 인증서를 사용자 지정 인증서로 교체할 수 있습니다.

Kaspersky Security Center 14 웹 콘솔의 인증서를 사용자 지정 인증서로 교체하려면 다음 단계를 따릅니다.

1. Kaspersky Security Center 14 웹 콘솔을 설치하는 데 필요한 응답 파일을 만듭니다.
2. 이 파일에서 `certPath` 파라미터 및 `keyPath` 파라미터를 사용하여 사용자 지정 인증서 파일 및 키 파일에 대한 경로를 지정합니다.
3. 새 응답 파일을 지정하여 Kaspersky Security Center 14 웹 콘솔을 다시 설치합니다. 다음 중 하나를 수행합니다:
   - Kaspersky Security Center 14 웹 콘솔의 같은 설치 파일을 사용하려면 Kaspersky Security Center 14 웹 콘솔을 제거한 후 같은 Kaspersky Security Center 14 웹 콘솔 버전을 설치합니다.
   - 업그레이드된 버전의 설치 파일을 사용하려면 업그레이드 명령을 실행합니다.

Kaspersky Security Center 14 웹 콘솔이 지정된 인증서로 작동합니다.

PFX 인증서를 PEM 형식으로 변환

Kaspersky Security Center 14 웹 콘솔에서 PFX 인증서를 사용하려면 먼저 아무 OpenSSL 기반 교차 플랫폼 유틸리티나 사용하여 PEM 형식으로 변환해야 합니다.

Linux 운영 체제에서 PFX 인증서를 PEM 형식으로 변환하려면:

1. OpenSSL 기반 교차 플랫폼 유틸리티에서 다음 명령을 실행합니다.

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.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 14 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 14 웹 콘솔 설치 프로그램에서 지정할 수 있습니다.

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

새 인증서는 PKCS#12 형식(예: 조직의 PKI 사용)으로 만들어야 하며 신뢰할 수 있는 CA(인증 기관)에서 발급한 것이어야 합니다. 또한 새 인증서에는 전체 신뢰 체인과 개인 키가 포함되어야 하며, 이는 확장자가 pfx 또는 p12인 파일에 저장되어야 합니다. 새 인증서는 아래의 요구 사항을 충족해야 합니다.

인증서 유형: 공통 인증서, 공통 예약 인증서("C", "CR")

요구 사항:

- 최소 키 길이: 2048
- 기본 제한:
  - CA: 참
  - 경로 길이 제한: 없음
    경로 길이 제한 값은 "없음"이 아닌 정수일 수 있지만, "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.

> 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.

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 <type> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}][-f <time>][-r <calistfile>][-l <logfile>]
```

> 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 <type>`	교체할 인증서의 유형입니다. `<type>` 파라미터의 가능한 값은 다음과 같습니다: • `C` – 포트 13000 및 13291에서 공통 인증서를 교체합니다. • `CR` – 포트 13000 및 13291에서 공통 예약 인증서를 교체합니다.
`-f <time>`	"DD-MM-YYYY hh:mm" 형식(포트 13000 및 13291의 경우)을 사용하는 인증서 변경 일정입니다. 만료되기 전에 공통 또는 공통 예약 인증서를 교체하려면 이 파라미터를 사용하십시오. 관리 중인 기기가 새 인증서에서 중앙 관리 서버와 동기화되어야 하는 시간을 지정합니다.
`-i <inputfile>`	PKCS#12 형식의 인증서 및 비공개 키가 포함된 컨테이너(확장자가 .p12 또는 .pfx인 파일)입니다.
`-p <password>`	p12 컨테이너를 보호하는 데 사용되는 암호입니다. 인증서와 개인 키가 컨테이너에 저장되므로 컨테이너로 파일을 해독하려면 암호가 필요합니다.
`-o <chkopt>`	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.
`-g <dnsname>`	지정한 DNS 이름에 대해 새 인증서가 생성됩니다.
`-r <calistfile>`	PEM 형식의 신뢰할 수 있는 루트 인증서 기관 목록입니다.
`-l <logfile>`	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 <inputfile> -p <password> -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:

```
klsetsrvcert -f "DD-MM-YYYY hh:mm" -t CR -i <inputfile> -p <password> -o NoCA
```

여기서 `"DD-MM-YYYY hh:mm"` 은 현재 날짜보다 3~4주 앞선 날짜입니다. 인증서를 백업 인증서로 변경하는 시간 이동을 통해 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>]
```

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

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 주소나 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.
`-cert <인증서 파일 경로>`	중앙 관리 서버에 대한 접근의 인증을 위해 지정된 인증서 파일을 사용합니다.

공유 폴더 정의

중앙 관리 서버 설치 후 중앙 관리 서버 속성에서 공유 폴더의 위치를 지정할 수 있습니다. 기본적으로 공유 폴더는 중앙 관리 서버가 있는 장치에 생성됩니다. 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.

Kaspersky Security Center Linux 업그레이드

이전 버전의 중앙 관리 서버(버전 13 이상)가 설치된 장치에 중앙 관리 서버 14 버전을 설치할 수 있습니다. 14 버전으로 업그레이드할 때, 중앙 관리 서버의 모든 이전 버전 데이터 및 설정은 저장됩니다.

> 업그레이이드 중에는 중앙 관리 서버와 다른 애플리케이션이 DBMS를 동시에 사용하도록 해서는 안 됩니다.

다음 방법의 하나를 통해 중앙 관리 서버 버전을 업그레이드할 수 있습니다.

- Kaspersky Security Center 설치 파일 사용
- 중앙 관리 서버 데이터 백업을 생성하고, 새 중앙 관리 서버 버전을 설치한 후 백업에서 중앙 관리 서버 데이터 복원

네트워크에 여러 중앙 관리 서버가 있다면 모든 서버를 수동으로 업그레이드해야 합니다. Kaspersky Security Center Linux는 중앙 집중식 업그레이드를 지원하지 않습니다.

Kaspersky Security Center Linux를 이전 버전에서 업그레이드하면, 지원하는 Kaspersky 애플리케이션에 설치한 모든 플러그인이 유지됩니다. 중앙 관리 서버 플러그인 및 네트워크 에이전트 플러그인은 자동으로 업그레이드됩니다.

설치 파일을 사용하여 Kaspersky Security Center Linux 업그레이드

중앙 관리 서버를 이전 버전(버전 13부터)에서 버전 14로 업그레이드하려면 Kaspersky Security Center 설치 파일을 사용하여 이전 버전 위에 새 버전을 설치할 수 있습니다.

설치 파일을 사용하여 이전 버전의 중앙 관리 서버를 버전 14로 업그레이드하려면:

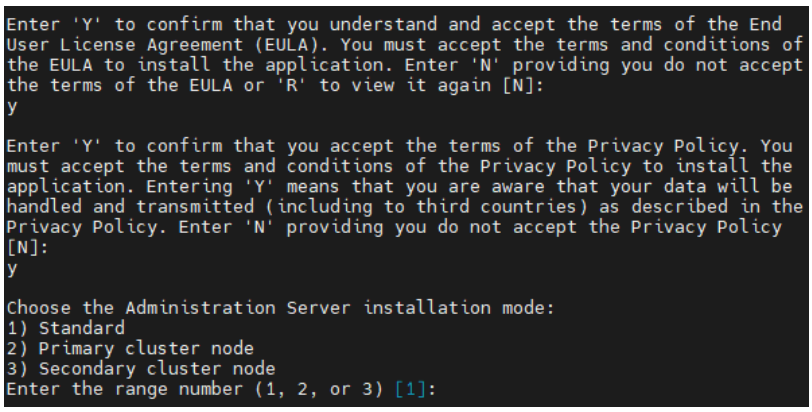
1. Kaspersky 웹사이트에서 버전 14용 전체 패키지가 포함된 Kaspersky Security Center 설치 파일을 다운로드합니다.
   - RPM 기반 운영 체제를 실행하는 장치 – ksc64-<버전 번호>-11247.x86_64.rpm
   - Debian 기반 운영 체제를 실행하는 장치 – ksc64_<버전 번호>-11247_amd64.deb
2. 중앙 관리 서버에서 사용하는 패키지 관리자를 사용하여 설치 패키지를 업그레이드합니다. 예를 들어, 루트 권한이 있는 계정으로 명령줄 터미널에서 다음 명령을 사용할 수 있습니다.
   - RPM 기반 운영 체제를 실행하는 장치:
     `$ sudo rpm -Uvh --nodeps --force ksc64-<버전 번호>-11247.x86_64.rpm`
   - Debian 기반 운영 체제를 실행하는 장치:
     `$ sudo dpkg -i ksc64_<버전 번호>-11247_amd64.deb`

   명령이 성공적으로 실행되면 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 스크립트가 생성됩니다. 이에 관한 메시지가 터미널에 표시됩니다.
3. 업그레이드된 관리 서버는 /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl 스크립트를 실행하여 구성할 수 있습니다.
4. 명령줄 터미널에 표시되는 라이센스 계약서 및 개인정보취급방침을 읽어 주십시오. 라이센스 계약서 및 개인정보취급방침의 모든 약관에 동의할 시:
   a. 'Y'를 입력하여 EULA의 이용 약관을 완전히 읽고 이했으며, 수락함을 확인합니다.
   b. 'Y'를 다시 입력하여 데이터 처리를 설명하는 개인정보취급방침을 완전히 읽고 이해했으며 수락했음을 확인합니다.

   'Y'를 두 번 입력한 후에 장치에 애플리케이션을 계속 설치할 수 있습니다.

5. '1'을 입력하여 표준 중앙 관리 서버 설치 모드를 선택합니다.

   마지막 두 단계는 아래 그림과 같습니다.



EULA 및 개인정보취급방침의 약관 수락 및 명령줄 터미널에서 표준 중앙 관리 서버 설치 모드 선택

   그러면 스크립트가 중앙 관리 서버 업그레이드를 구성하고 완료합니다. 업그레이드 중에는 업그레이드 전에 조정된 중앙 관리 서버 설정을 변경할 수 없습니다.

6. 장치에 이전 버전의 네트워크 에이전트가 설치되어 있으면 최신 버전의 네트워크 에이전트에 대한 원격 설치 작업을 만들어 실행합니다.

   > Linux용 네트워크 에이전트를 Kaspersky Security Center Linux와 같은 버전으로 업그레이드하는 것이 좋습니다.

   원격 설치 작업을 완료하면 네트워크 에이전트 버전이 업그레이드됩니다.

백업을 통해 Kaspersky Security Center Linux 업그레이드

중앙 관리 서버를 이전 버전(버전 13부터)에서 버전 14로 업그레이드하려면 중앙 관리 서버 데이터의 백업을 생성하고 새 버전의 Kaspersky Security Center를 설치한 후 이 데이터를 복원할 수 있습니다. 설치 중 문제가 발생하면 업그레이드 전에 생성한 중앙 관리 서버 데이터 백업을 사용하여 중앙 관리 서버의 이전 버전을 복원할 수 있습니다.

백업을 통해 이전 버전의 중앙 관리 서버를 14 버전으로 업그레이드하려면:

1. 업그레이드하기 전에 이전 버전의 애플리케이션으로 중앙 관리 서버 데이터를 백업하십시오.
2. Kaspersky Security Center의 이전 버전을 제거합니다.
3. 이전 중앙 관리 서버에 Kaspersky Security Center 버전 14를 설치합니다.
4. 업그레이드 전에 생성한 백업에서 중앙 관리 서버 데이터를 복원합니다.
5. 장치에 이전 버전의 네트워크 에이전트가 설치되어 있다면 최신 버전의 네트워크 에이전트에 대한 원격 설치 작업을 만들어 실행합니다.

   > Linux용 네트워크 에이전트를 Kaspersky Security Center Linux와 같은 버전으로 업그레이드하는 것이 좋습니다.

   원격 설치 작업을 완료하면 네트워크 에이전트 버전이 업그레이드됩니다.

Kaspersky Security Center 14 웹 콘솔 로그인 및 로그아웃

중앙 관리 서버와 웹 콘솔 서버를 설치한 후 Kaspersky Security Center 14 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.

Kaspersky Security Center 14 웹 콘솔에 로그인하려면:

1. 브라우저에서 <중앙 관리 서버 웹 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.

   중앙 관리 서버를 하나만 추가했다면 **사용자 이름** 및 **암호** 필드만 표시됩니다.

3. 다음 중 하나를 수행합니다:

   - 물리적 중앙 관리 서버에 로그인하려면 로컬 관리자의 사용자 이름과 암호를 입력합니다.

- 하나 이상의 가상 중앙 관리 서버가 생성된 서버에서 가상 서버에 로그인하려면:

  a. **고급 설정**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.

로그인하고 나면 마지막으로 사용한 언어와 테마가 적용된 대시보드가 표시됩니다. Kaspersky Security Center 14 웹 콘솔을 탐색하고 웹 콘솔을 통해 Kaspersky Security Center Linux를 사용할 수 있습니다.

Kaspersky Security Center 14 웹 콘솔에서 로그아웃하려면:

메인 메뉴에서 계정 설정으로 이동하여 **로그아웃**를 선택합니다.

Kaspersky Security Center 14 웹 콘솔이 닫히고 로그인 페이지가 표시됩니다.

빠른 시작 마법사

Kaspersky Security Center Linux를 사용하면 보안 위협으로부터 네트워크를 보호하기 위한 중앙 집중화 관리 시스템 구축에 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.
- 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 바이러스 검사 작업, 업데이트 다운로드 작업 및 데이터 백업 작업을 만듭니다.

  빠른 시작 마법사는 **관리 중인 기기** 폴더에 정책도 들어 있지 않은 애플리케이션에 대해서만 정책을 만듭니다. 관리 중인 기기 계층 구조의 가장 높은 레벨에 대해 동일한 이름의 작업이 이미 만들어진 경우 빠른 시작 마법사는 작업을 생성하지 않습니다.

애플리케이션은 중앙 관리 서버 설치 후 처음으로 연결될 때 빠른 시작 마법사의 실행 여부를 자동으로 물어봅니다. 언제든지 수동으로 빠른 시작 마법사를 시작할 수도 있습니다.

빠른 시작 마법사를 수동으로 시작하려면 다음과 같이 하십시오:

1. 메인 메뉴에서 중앙 관리 서버 이름 옆의 설정 아이콘()을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **일반** 섹션을 선택합니다.
3. **빠른 시작 마법사 시작**을 누릅니다.

마법사에서 중앙 관리 서버의 초기 구성을 수행하라는 메시지가 표시됩니다. 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 Linux 및 관리 중인 Kaspersky 애플리케이션용 안티 바이러스 데이터베이스의 업데이트를 다운로드하려면 인터넷 접속을 구성해야 합니다.

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 Center Linux에서 인터넷 연결에 사용한 프록시 서버의 주소입니다.

- **포트 번호**

  Kaspersky Security Center Linux 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 인증을 나중에 구성할 수도 있습니다.

2단계. 애플리케이션 활성화 방법 선택

다음 Kaspersky Security Center Linux 활성화 옵션 중 하나를 선택합니다:

- **활성화코드 입력**

  *활성화코드*는 20자의 숫자와 문자로 이루진 고유한 값입니다. 활성화 코드를 입력하여 Kaspersky Security Center Linux 활성화 키를 추가할 수 있습니다. Kaspersky Security Center 구매 후 지정한 이메일 주소를 통해 활성화코드를 받습니다.
  활성화코드로 애플리케이션을 활성화하려면 Kaspersky 활성화 서버에 접속하기 위한 인터넷 연결이 되어 있어야 합니다.
  이 활성화 옵션을 선택한 경우 **라이센스 키를 관리 중인 기기에 자동으로 배포** 옵션을 활성화할 수 있습니다.

  이 옵션을 활성화하면 라이센스 키가 관리 중인 기기에 자동으로 배포됩니다.

  이 옵션을 비활성화하면 나중에 메인 메뉴의 **동작 → 라이센스 → Kaspersky 라이센스** 섹션에서 관리 중인 장치로 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.
  Kaspersky Security Center 구매 후 지정한 이메일 주소를 통해 키 파일을 받습니다.
  라이센스 키 파일을 사용하여 애플리케이션을 활성화할 때 Kaspersky 활성화 서버에 연결하지 않아도 됩니다.
  이 활성화 옵션을 선택한 경우 **라이센스 키를 관리 중인 기기에 자동으로 배포** 옵션을 활성화할 수 있습니다.

  이 옵션을 활성화하면 라이센스 키가 관리 중인 기기에 자동으로 배포됩니다.

  이 옵션을 비활성화하면 나중에 메인 메뉴의 **동작 → 라이센스 → Kaspersky 라이센스** 섹션에서 관리 중인 장치로 라이센스 키를 배포할 수 있습니다.

- 애플리케이션 활성화 연기

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.

3단계. 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.

4단계. 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.

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
  - 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.

5단계. 빠른 시작 마법사 닫기

마법사를 닫으려면 **마침** 버튼을 누릅니다.

빠른 시작 마법사를 완료한 후, 보호 배포 마법사를 실행하여 네트워크의 장치에 보안 프로그램이나 네트워크 에이전트를 자동 설치할 수 있습니다.

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.

보호 배포 마법사 시작

언제든지 보호 배포 마법사를 수동으로 시작할 수 있습니다.

보호 배포 마법사를 수동으로 시작하려면 다음 단계를 따릅니다.

메인 메뉴에서 **발견 및 배포 → 배포 및 할당 → 보호 배포 마법사**를 누릅니다.

보호 배포 마법사 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.

1단계. 설치 패키지 선택

설치하려는 애플리케이션의 설치 패키지를 선택합니다.

필요한 애플리케이션의 설치 패키지가 목록에 없으면 **추가** 버튼을 누른 다음 목록에서 애플리케이션을 선택합니다.

2단계. 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 활성화되어 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 활성화코드가 이미 포함되어 있으면 이 창이 표시되기는 하지만 창에는 라이센스 키 세부 정보만 표시됩니다.

3단계. 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.

4단계. 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.

5단계. 원격 설치 작업 설정 지정

원격 설치 작업 설정 페이지에서 애플리케이션의 원격 설치에 대한 설정을 지정합니다.

설치 패키지 강제 다운로드 방법 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 장치의 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.

  네트워크 에이전트가 설치되지 않은 장치에 Windows용 애플리케이션(Windows용 네트워크 에이전트 포함)을 설치하려면 Windows 기반 배포 지점을 사용해야만 합니다. 따라서 Windows 애플리케이션 설치 시:

  - 이 옵션을 선택합니다.
  - 대상 클라이언트 장치에 배포 지점이 할당되었는지 확인합니다.
  - 배포 지점이 Windows 기반인지 확인합니다.

추가 설정 정의:

이미 설치되어 있는 애플리케이션은 설치하지 않음

이 옵션을 활성화하면 선택한 애플리케이션이 이 클라이언트 기기에 이미 설치된 경우 다시 설치되지 않습니다.

이 옵션을 비활성화해도 애플리케이션이 설치됩니다.

이 옵션은 기본적으로 활성화되어 있습니다.

6단계. 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 Center Linux에서 자동 제거하도록 하려면 이 옵션을 선택합니다.

호환되지 않는 애플리케이션 목록도 표시됩니다.

이 옵션을 선택하지 않으면 호환되지 않는 애플리케이션이 없는 기기에만 애플리케이션이 설치됩니다.

7단계. 관리 중인 기기로 기기 이동

모두 펼치기 | 모두 접기

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.

8단계. 기기에 접근할 수 있는 계정 선택

모두 펼치기 | 모두 접기

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.

  네트워크 에이전트가 클라이언트 기기에 설치되어 있지 않다면, 이 옵션은 이용할 수 없습니다.

- **계정 필요(네트워크 에이전트는 사용되지 않음)**

원격 설치 작업을 할당한 장치에 네트워크 에이전트가 설치되어 있지 않다면 이 옵션을 선택하십시오. 이때, 사용자 계정 지정하여 애플리케이션을 설치할 수 있습니다.

애플리케이션 설치 프로그램을 실행할 사용자 계정을 지정하려면 **추가** 버튼을 클릭하고 **로컬 계정**을 선택한 다음 사용자 계정 자격 증명을 지정합니다.

예를 들어 이 작업이 할당된 모든 장치에 필요한 모든 권한이 어떤 계정에도 없다면, 사용자 계정을 여러 개 지정할 수 있습니다. 이때, 작업 실행 시 추가한 모든 계정을 위에서부터 순서대로 사용합니다.

9단계. 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 눌러 보호 배포 마법사의 마지막 단계를 완료합니다.

중앙 관리 서버 구성

이 섹션에서는 Kaspersky Security Center Linux 중앙 관리 서버의 구성 프로세스 및 속성에 대해 설명합니다.

Kaspersky Security Center 14 웹 콘솔과 중앙 관리 서버 연결 구성

중앙 관리 서버의 연결 포트를 설정하려면 다음 단계를 따릅니다.

1. 화면 위쪽에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘()을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **연결 포트** 섹션을 선택합니다.

애플리케이션에 선택한 서버의 주요 연결 설정이 표시됩니다.

Kaspersky Security Center 로그인을 위한 IP 주소 허용 목록 구성

기본적으로 사용자는 Kaspersky Security Center 14 웹 콘솔(이하 웹 콘솔)을 열 수 있는 모든 장치에서 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 애플리케이션 을 실행하는 경우 IP 주소를 확인합니다. 이때 사용자의 장치가 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
  웹 콘솔을 통해 Kaspersky Security Center에 로그인하면 표준 운영 체제를 사용하여 웹 콘솔 서버가 설치된 기기에 방화벽을 구성할 수 있습니다. 그런 다음 누군가가 한 기기에서 Kaspersky Security Center에 로그인을 시도하고 웹 콘솔 서버가 다른 기기에 설치되어 있는 경우 방화벽이 침입자의 간섭을 방지하는 데 도움이 됩니다.
- 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(대개 /opt/kaspersky/ksc64/sbin)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 Syslog 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
```

Administration Server 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.

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 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.

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.

만약 데이터베이스에서 이벤트의 개수가 관리자가 지정한 값에 도달할 경우에는 애플리케이션은 가장 오래된 이벤트를 삭제하고 새로운 이벤트로 쓰게 됩니다. 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. 화면 위쪽에서 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.

중앙 관리 서버 데이터의 백업 복사 및 복원

데이터 백업을 사용하면 한 기기에서 다른 기기로 데이터 손실 없이 중앙 관리 서버를 이동할 수 있습니다. 또한 백업을 통해 중앙 관리 서버 데이터베이스를 다른 기기로 이동하거나 새로운 버전의 Kaspersky Security Center로 업그레이드할 때 데이터를 복원할 수 있습니다.

설치된 관리 플러그인은 백업되지 않습니다. 백업 복사본에서 중앙 관리 서버 데이터를 복원한 후, 관리 중인 애플리케이션용 플러그인을 다운로드하여 다시 설치해야 합니다.

다음 방법 중 하나를 사용하여 중앙 관리 서버 데이터의 백업 복사본을 만들 수 있습니다:

- Kaspersky Security Center 14 웹 콘솔을 통해 데이터 백업 작업을 생성하고 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(대개 /opt/kaspersky/ksc64/sbin/klbackup).

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.

klbackup 유틸리티를 사용해야만 중앙 관리 서버 데이터를 복구할 수 있습니다.

중앙 관리 서버 데이터 백업 작업 생성

백업 작업은 중앙 관리 서버 작업이며 빠른 시작 마법사를 통해 생성됩니다. 빠른 시작 마법사에서 만든 백업 작업이 삭제된 경우 이를 수동으로 만들 수 있습니다.

*중앙 관리 서버 데이터 백업*작업은 하나의 복사본으로만 만들 수 있습니다. 중앙 관리 서버에 대한 중앙 관리 서버 데이터 백업 작업을 이미 만들었다면, 작업 유형 선택 창에 이 작업이 표시되지 않습니다.

중앙 관리 서버 데이터 백업 작업을 만들려면 다음과 같이 하십시오:

1. **기기 → 작업**으로 이동합니다.
2. **추가**를 누릅니다.
   작업 추가 마법사가 시작됩니다.
3. 마법사 첫 번째 페이지의 **애플리케이션** 목록에서 **Kaspersky Security Center 14**를 선택하고 **작업 유형** 목록에서 **중앙 관리 서버 데이터 백업**을 선택합니다.
4. 마법사의 해당 페이지에서 다음 정보를 지정합니다.
   - 백업 복사본 저장용 폴더
   - 백업용 암호(선택사항)
   - 저장할 최대 백업 복사본 수
5. **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화하면 기본 작업 설정을 수정할 수 있습니다. 이 옵션을 활성화하지 않으면 기본 설정으로 작업이 생성됩니다. 나중에 언제든지 기본 설정을 수정할 수 있습니다.
6. **마침** 버튼을 누릅니다.

그러면 작업이 생성되고 작업 목록에 표시됩니다.

klbackup 유틸리티를 사용하여 데이터 백업 및 복구

Kaspersky Security Center 배포 키트의 일부인 klbackup 유틸리티를 사용하여 백업과 향후 복구를 위해 중앙 관리 서버 데이터를 복사할 수 있습니다.

비대화식 모드에서 중앙 관리 서버 데이터의 백업 복사본을 만들거나 복구하려면 다음과 같이 하십시오.

중앙 관리 서버가 설치된 기기의 명령줄에서 필요한 키 세트를 사용하여 klbackup을 실행합니다.

유틸리티 명령줄 구문:

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD] [-online]
```

> klbackup 유틸리티 명령줄에서 암호를 지정하지 않으면 유틸리티가 대화식으로 암호 입력을 요청합니다.

키에 대한 설명:

- `-path BACKUP_PATH` - BACKUP_PATH 폴더에 정보를 저장하고 BACKUP_PATH 폴더의 데이터를 복구에 사용합니다(필수 파라미터).
- `-logfile LOGFILE` - 중앙 관리 서버 데이터의 백업 및 복구에 대한 리포트를 저장합니다.
  데이터베이스 서버 계정과 klbackup 유틸리티에 BACKUP_PATH 폴더의 데이터를 변경할 수 있는 권한이 주어져야 합니다.
- `-use_ts` – 데이터 저장 시 BACKUP_PATH 폴더의 하위 폴더로 정보를 복사하며, 해당 폴더에는 `klbackup YYYY-MM-DD # HH-MM-SS` 형식으로 현재 시스템 날짜와 작업 시간이 포함된 이름이 지정됩니다. 키가 지정되지 않으면 정보가 BACKUP_PATH 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 BACKUP_PATH 폴더에 포함된 정보를 기반으로 수행됩니다. 키가 없으면 데이터가 BACKUP_PATH 폴더에 백업됩니다.
- `-password PASSWORD` – 중앙 관리 서버 인증서를 저장하거나 복구합니다.인증서를 암호화하거나 암호를 해독하려면 PASSWORD 파라미터로 지정된 암호를 사용합니다.

  > 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.
- `-online` - 볼륨 스냅샷을 생성하여 중앙 관리 서버의 오프라인 시간을 최소화하며 중앙 관리 서버 데이터를 백업합니다. 유틸리티를 사용하여 데이터를 복구하는 경우 이 옵션은 무시됩니다.

다른 기기로 중앙 관리 서버 이동

새 장치에서 중앙 관리 서버 사용 시, 다음 방법 중 하나로 이동할 수 있습니다.

- 중앙 관리 서버와 데이터베이스 서버를 새 장치로 이동합니다.
- 데이터베이스 서버를 이전 장치에 유지하고 중앙 관리 서버만 새 장치로 이동합니다.

중앙 관리 서버와 데이터베이스 서버를 새 장치로 이동하려면:

1. 이전 장치에서 중앙 관리 서버 데이터의 백업을 만듭니다.
   이렇게 하려면 Kaspersky Security Center 14 웹 콘솔을 통해 데이터 백업 작업을 실행하거나 klbackup 유틸리티를 실행하십시오.
2. 중앙 관리 서버를 설치할 새 장치를 선택하십시오. 선택한 장치의 하드웨어 및 소프트웨어가 중앙 관리 서버, Kaspersky Security Center 14 웹 콘솔, 네트워크 에이전트의 요구 사항을 충족하는지 확인하십시오. 또한 중앙 관리 서버에서 사용되는 포트를 사용할 수 있는지 확인하십시오.
3. 새 장치에 중앙 관리 서버가 사용할 데이터베이스 관리 시스템(DBMS)을 설치합니다.
   DBMS 선택 시, 중앙 관리 서버에서 다루는 장치의 수를 고려하십시오.
4. 새 장치에 중앙 관리 서버를 설치합니다.

데이터베이스 서버를 새 장치로 이동하려면 로컬 주소를 데이터베이스가 설치된 장치의 IP 주소로 지정하십시오(Kaspersky Security Center 설치 지침의 "h" 항목). 데이터베이스 서버를 이전 장치에 유지하려면 Kaspersky Security Center 설치 지침의 "h" 항목에 이전 장치의 IP 주소를 입력하십시오.

5. 설치가 완료되면 klbackup 유틸리티를 사용하여 새 장치에서 중앙 관리 서버 데이터를 복구합니다.

   이전 장치와 새 장치에서 SQL Server를 DBMS로 사용 시, 새 장치에 설치된 SQL Server 버전이 이전 장치에 설치된 SQL Server 버전과 같거나 더 최신 버전이어야 합니다. 그렇지 않으면 새 장치에서 중앙 관리 서버 데이터를 복구할 수 없습니다.

6. Kaspersky Security Center 14 웹 콘솔을 열고 중앙 관리 서버에 연결합니다.

7. 모든 클라이언트 장치가 중앙 관리 서버에 연결되어 있는지 확인합니다.

8. 이전 장치에서 중앙 관리 서버와 데이터베이스 서버를 제거합니다.

가상 중앙 관리 서버 만들기

가상 중앙 관리 서버를 생성하여 관리 그룹에 추가할 수 있습니다.

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 14 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 14 웹 콘솔 설치를 수정하여 보조 서버를 신뢰할 수 있는 중앙 관리 서버 목록에 추가합니다** 그러면 Kaspersky Security Center 14 웹 콘솔에서 가상 중앙 관리 서버에 연결할 수 있습니다.

  1. Kaspersky Security Center 14 웹 콘솔이 설치된 장치에서 관리자 권한이 있는 계정으로 장치에 설치된 Linux 배포판에 해당하는 웹 콘솔 설치 파일을 실행합니다.
  2. 설치 마법사가 시작됩니다.
  3. 마법사 첫 페이지에서 **업그레이드** 옵션을 선택합니다.
  4. **수정 유형** 페이지에서 **연결 설정 편집** 옵션을 선택합니다.
  5. **신뢰할 수 있는 중앙 관리 서버** 페이지에서 필요한 보조 관리 서버를 추가합니다.
  6. 마법사의 마지막 페이지에서 **수정**을 눌러 새 설정을 적용합니다.
  7. 애플리케이션 재구성이 성공적으로 완료되면 **마침** 버튼을 누릅니다.

- Kaspersky Security Center 14 웹 콘솔을 사용하여 가상 서버가 생성된 보조 중앙 관리 서버에 직접 연결합니다. 그런 다음 Kaspersky Security Center 14 웹 콘솔에서 가상 중앙 관리 서버로 전환할 수 있습니다.

중앙 관리 서버의 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.

계층 구조에서, Kaspersky Security Center Linux 중앙 관리 서버는 Windows 기반 Kaspersky Security Center나 Kaspersky Security Center 클라우드 콘솔의 기본 중앙 관리 서버에서 관리하는 보조 서버로만 작동할 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.

중앙 관리 서버 계층 만들기 및 보조 중앙 관리 서버 추가

계층 구조에서, Kaspersky Security Center Linux 중앙 관리 서버는 Windows 기반 Kaspersky Security Center나 Kaspersky Security Center 클라우드 콘솔의 기본 중앙 관리 서버에서 관리하는 보조 서버로만 작동할 수 있습니다.

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 14 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**를 누릅니다.
   보조 중앙 관리 서버 연결 마법사를 시작합니다.
6. 마법사의 첫 번째 페이지에서 다음 필드에 내용을 입력합니다.

   - **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.

   - **중앙 관리 서버 SSL 포트**

     기본 중앙 관리 서버의 SSL 포트 번호를 지정합니다. 기본 포트 번호는 13000입니다.

   - **중앙 관리 서버 AP 포트**

     OpenAPI를 통해 연결을 수신하는 데 사용할 기본 중앙 관리 서버의 포트 번호를 지정합니다. 기본 포트 번호는 13299입니다.

   - **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 기본 중앙 관리 서버가 보조 중앙 관리 서버에 대한 연결을 시작합니다. 그렇지 않으면 보조 중앙 관리 서버가 주 중앙 관리 서버에 대한 연결을 시작합니다.

- **프록시 서버 사용**

  프록시 서버를 사용하여 보조 중앙 관리 서버에 연결하는 경우 이 옵션을 선택합니다.
  이러한 경우 다음과 같은 프록시 서버의 설정도 지정해야 합니다.
  - **주소**
  - **사용자 이름**
  - **암호**

7. 마법사의 추가 설명을 따르십시오.

마법사가 종료되면 '기본/보조' 계층이 구축됩니다. 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 14 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 장치에 파일을 쓰거나 이메일 등으로 보낼 수 있습니다).
   인증서 파일은 향후 기본 중앙 관리 서버의 /var/opt/kaspersky/klnagent_srv/1093/cert/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. 필요한 경우 **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 14 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 14 웹 콘솔 설치를 수정하여 보조 서버를 신뢰할 수 있는 중앙 관리 서버 목록에 추가합니다** 그러면 Kaspersky Security Center 14 웹 콘솔에서 가상 중앙 관리 서버에 연결할 수 있습니다.

1. Kaspersky Security Center 14 웹 콘솔이 설치된 장치에서 관리자 권한이 있는 계정으로 장치에 설치된 Linux 배포판에 해당하는 웹 콘솔 설치 파일을 실행합니다.
2. 설치 마법사가 시작됩니다.
3. 마법사 첫 페이지에서 **업그레이드** 옵션을 선택합니다.
4. **수정 유형** 페이지에서 **연결 설정 편집** 옵션을 선택합니다.
5. **신뢰할 수 있는 중앙 관리 서버** 페이지에서 필요한 보조 관리 서버를 추가합니다.
6. 마법사의 마지막 페이지에서 **수정**을 눌러 새 설정을 적용합니다.
7. 애플리케이션 재구성이 성공적으로 완료되면 **마침** 버튼을 누릅니다.

- Kaspersky Security Center 14 웹 콘솔을 사용하여 가상 서버가 생성된 보조 중앙 관리 서버에 직접 연결합니다. 그런 다음 Kaspersky Security Center 14 웹 콘솔에서 가상 중앙 관리 서버로 전환할 수 있습니다.

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 **인증 보안** 탭을 선택합니다.
4. 계정 설정이 변경 또는 수정될 때마다 자격 증명을 요청하려면 **인증 보안** 탭에서 **사용자 계정 수정 권한 확인 인증 요청** 옵션을 선택합니다. 다른 방법으로는 **사용자가 추가 인증 없이 이 계정을 수정할 수 있도록 허용** 옵션을 선택합니다.
5. **저장** 버튼을 누릅니다.

2단계 인증

2단계 인증을 활성화하여 Kaspersky Security Center 14 웹 콘솔에 대한 무단 액세스 위험을 줄일 수 있습니다.

시나리오: 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 사용자 계정에 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한이 있어야 합니다.
- 중앙 관리 서버의 다른 사용자가 자신의 기기에 인증 애플리케이션을 설치했는지 확인합니다.

단계

모든 사용자에 대해 2단계 인증을 활성화하는 과정은 다음 단계로 진행됩니다.

1. **기기에 인증 애플리케이션 설치**

   Google Authenticator, Microsoft Authenticator 또는 시간 기반 일회용 비밀번호 알고리즘을 지원하는 기타 인증 애플리케이션을 설치할 수 있습니다.

2. **인증 애플리케이션 시간을 중앙 관리 서버가 설치된 기기의 시간과 동기화**

인증 애플리케이션에 설정된 시간은 중앙 관리 서버의 시간에 동기화되어야 합니다.

3. **계정에 대한 2단계 인증 활성화 및 계정의 비밀 키 받기**

   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.

5. **보안 코드 발행자 이름 편집**

   이름이 유사한 중앙 관리 서버가 여럿이라면, 중앙 관리 서버를 보다 정확하게 구별할 수 있도록 보안 코드 발행자 이름을 변경해야 할 수 있습니다.

6. **2단계 인증을 활성화할 필요가 없는 사용자 계정 제외**

   필요 시, 2단계 인증에서 사용자를 제외합니다. 계정이 제외된 사용자는 중앙 관리 서버에 로그인하기 위해 2단계 인증을 사용할 필요가 없습니다.

결과

이 시나리오를 완료하면:

- 계정에 대한 2단계 인증이 활성화됩니다.
- 제외된 사용자 계정을 제외하고 모든 중앙 관리 서버 사용자 계정에 2단계 인증이 활성화됩니다.

계정에 대한 2단계 인증 정보

Kaspersky Security Center Linux는 Kaspersky Security Center 14 웹 콘솔 사용자에게 2단계 인증을 제공합니다. 계정에 2단계 인증이 활성화되면, Kaspersky Security Center 14 웹 콘솔에 로그인할 때마다 사용자 이름, 암호, 추가 일회용 보안 코드를 입력합니다. 일회용 보안 코드를 받으려면 컴퓨터 또는 모바일 기기에 인증 애플리케이션이 있어야 합니다.

보안 코드에는 *발행자 이름*이라는 식별자가 있습니다. 보안 코드 발행자 이름은 인증 애플리케이션에서 중앙 관리 서버의 식별자로 사용됩니다. 보안 코드 발행자 이름을 변경할 수 있습니다. 보안 코드 발행자 이름에는 중앙 관리 서버의 이름과 동일한 기본값이 있습니다. 발행자 이름은 인증 애플리케이션에서 중앙 관리 서버의 식별자로 사용됩니다. 보안 코드 발행자 이름을 변경할 경우 새 비밀 키를 발행하여 인증 애플리케이션에 전달해야 합니다. 보안 코드는 일회용이며 최대 90초 동안 유효합니다(정확한 시간은 다를 수 있음).

2단계 인증이 활성화된 모든 사용자는 본인의 비밀 키를 재발급할 수 있습니다. 사용자가 재발급된 비밀 키로 인증하고 이를 로그인에 사용하면 중앙 관리 서버에서는 사용자 계정에 대한 새 비밀 키를 저장합니다. 사용자가 새 비밀 키를 잘못 입력하면 중앙 관리 서버에서는 새 비밀 키를 저장하지 않고 현재 비밀 키를 추가 인증에 유효한 상태로 둡니다.

> 시간 기반 일회성 비밀번호 알고리즘(TOTP)을 지원하는 모든 인증 소프트웨어(예: Google Authenticator)를 인증 애플리케이션으로 사용할 수 있습니다. 보안 코드를 생성하려면 인증 애플리케이션에 설정된 시간과 중앙 관리 서버에 설정된 시간을 동기화해야 합니다.

인증 애플리케이션은 다음과 같이 보안 코드를 생성합니다.

1. 중앙 관리 서버는 특수한 비밀 키와 QR 코드를 생성합니다.
2. 생성된 비밀 키 또는 QR 코드를 인증 애플리케이션에 전달합니다.
3. 인증 애플리케이션에서는 중앙 관리 서버의 인증 창에 전달할 일회용 보안 코드를 생성합니다.

> 여러 기기에 인증 애플리케이션을 설치하는 것이 좋습니다. 비밀 키 또는 QR 코드를 저장하고 안전한 곳에 보관하십시오. 이는 모바일 장치 분실 시 Kaspersky Security Center 14 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.

2단계 인증은 다음과 같은 규칙에 따라 작동합니다.

- **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한이 있는 사용자 계정만 모든 사용자에 대해 2단계 인증을 활성화할 수 있습니다.
- 본인 계정에 2단계 인증을 활성화한 사용자만 모든 사용자에게 2단계 인증 옵션을 활성화할 수 있습니다.
- 본인 계정에 2단계 인증을 활성화한 사용자만 모든 사용자에게 활성화된 2단계 인증 목록에서 다른 사용자 계정을 제외할 수 있습니다.
- 사용자는 본인 계정에 2단계 인증을 활성화할 수 있습니다.

- **일반 기능: 사용자 권한** 기능 영역에서 개체 ACL 수정 권한을 가진 사용자 계정이 2단계 인증을 사용하여 Kaspersky Security Center 14 웹 콘솔에 로그인하면, 모든 사용자에 대한 2단계 인증이 비활성화되었을 때는 다른 사용자를 대상으로만, 모든 사용자에 대한 2단계 인증이 활성화되었을 때는 인증 목록에서 제외된 사용자를 대상으로 2단계 인증을 비활성화할 수 있습니다.
- 2단계 인증을 사용하여 Kaspersky Security Center 14 웹 콘솔에 로그인한 사용자는 본인의 비밀 키를 재발급할 수 있습니다.
- 현재 사용 중인 중앙 관리 서버에 대해 모든 사용자의 2단계 인증 옵션을 활성화할 수 있습니다. 중앙 관리 서버에서 이 옵션을 활성화하면 가상 중앙 관리 서버의 사용자 계정에 대해서도 이 옵션을 활성화하며 보조 중앙 관리 서버의 사용자 계정에는 2단계 인증을 활성화하지 않습니다.

본인 계정에 대한 2단계 인증 활성화

자신의 계정에 대해서만 2단계 인증을 활성화할 수 있습니다.

본인 계정에 대해 2단계 인증을 활성화하기 전에 인증 애플리케이션이 모바일 기기에 설치되어 있는지 확인하십시오. 인증 애플리케이션에 설정된 시간이 중앙 관리 서버가 설치된 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 **계정 보호** 탭을 선택합니다.
4. **계정 보호** 탭:
   - 사용자 계정에 대해 2단계 인증을 활성화하려는 경우 **사용자 이름, 암호 및 보안 코드 요청(2단계 인증)** 옵션을 선택합니다:
     - 열리는 2단계 인증 창에서 인증 애플리케이션의 비밀 키를 입력하거나 QR 코드를 스캔하고 일회성 보안 코드를 받습니다.
       인증 애플리케이션에 수동으로 비밀 키를 지정하거나 모바일 기기로 QR 코드를 스캔할 수 있습니다.
     - 2단계 인증 창이 열리면 인증 애플리케이션에서 생성한 보안 코드를 지정한 다음 **확인 및 적용** 버튼을 클릭합니다.
5. **저장** 버튼을 누릅니다.

계정에 대한 2단계 인증이 활성화됩니다.

모든 사용자에 대한 2단계 인증 활성화

계정의 **일반 기능: 사용자 권한** 기능 영역에 개체 ACL 수정 권한이 있고 2단계 인증을 사용하여 인증했다면, 중앙 관리 서버의 모든 사용자에 대해 2단계 인증을 활성화할 수 있습니다. 모든 사용자에 대해 활성화하기 전에 본인 계정에 2단계 인증을 활성화하지 않은 경우 애플리케이션에서 본인 계정에 2단계 인증을 활성화하는 창이 열립니다.

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.

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.

사용자 계정에 대한 2단계 인증 비활성화

본인 및 다른 사용자의 계정에 2단계 인증을 비활성화할 수 있습니다.

일반 기능: 사용자 권한 기능 영역에 개체 ACL 수정 권한이 있는 계정은 다른 사용자 계정에 대한 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.

모든 사용자에 대한 2단계 인증 비활성화

계정에 대해 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.
3. 인증 창에 계정의 자격 증명을 입력합니다.

모든 사용자에 대해 2단계 인증이 비활성화됩니다.

2단계 인증에서 계정 제외

사용자에게 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한이 있다면 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. 메인 메뉴에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘()을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. 속성 창의 **인증 보안** 탭에 있는 2단계 인증 제외 표에서 **추가** 버튼을 누릅니다.
3. 창이 열리면 다음과 같이 합니다.
   a. 제외할 사용자 계정을 선택합니다.
   b. **확인** 버튼을 누릅니다.

선택한 사용자 계정은 2단계 인증에서 제외됩니다.

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 애플리케이션에서 생성한 새 보안 키를 지정합니다.
6. **확인 및 적용** 버튼을 클릭합니다.

사용자의 새 비밀 키가 생성됩니다.

모바일 장치 분실 시 다른 모바일 장치에 인증 애플리케이션을 설치하고 새 비밀 키를 생성하여 Kaspersky Security Center 14 웹 콘솔에 대한 접근 권한을 복원할 수 있습니다.

보안 코드 발행자 이름 편집

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 애플리케이션에 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.

허용되는 암호 입력 시도 횟수 변경

Kaspersky Security Center Linux에서는 암호 입력 시도 횟수가 제한되어 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 서버 장치에서 Linux 명령줄을 실행합니다.
2. klscflag 유틸리티에서 다음 명령을 실행합니다.
   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```
   여기서 N은 암호 입력 시도 횟수입니다.
3. 변경 사항을 적용하려면 중앙 관리 서버 서비스를 다시 시작합니다.

허용되는 암호 입력 시도의 최대 횟수가 변경됩니다.

DBMS 자격증명 변경

예를 들어 보안을 위해 자격증명 순환을 수행하기 위해 DBMS 자격증명을 변경해야 하는 경우가 있습니다.

klsrvconfig 유틸리티를 사용하여 Linux 환경에서 DBMS 자격증명을 변경하려면 다음과 같이 하십시오:

1. Linux 명령줄을 시작합니다.
2. 열린 명령줄 창에서 klsrvconfig 유틸리티를 지정합니다.
   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```
3. 새 계정 이름을 지정합니다. DBMS에 있는 계정의 자격증명을 지정해야 합니다.
4. 새 암호를 입력합니다.
5. 확인을 위해 새 암호를 지정합니다.

DBMS 자격증명이 변경됩니다.

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. 화면 위쪽에서 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.

인터페이스 구성

사용 중인 기능에 따라 섹션과 인터페이스 구성 요소를 표시하고 숨기도록 Kaspersky Security Center 14 웹 콘솔 인터페이스를 구성할 수 있습니다.

현재 사용 중인 기능 세트에 따라 Kaspersky Security Center 14 웹 콘솔 인터페이스를 구성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 계정 메뉴를 클릭합니다.
2. 드롭다운 메뉴에서 **인터페이스 옵션**을 선택합니다.
3. **인터페이스 옵션** 창이 열리면 필요한 옵션을 활성화 또는 비활성화합니다.
4. **저장**을 누릅니다.

그 후, 콘솔이 활성화된 옵션에 따라 기본 메뉴에 섹션을 표시합니다. 예를 들어, **EDR 알림 표시**를 활성화하면 메인 메뉴에 **모니터링 및 보고 → 알림** 섹션이 나타납니다.

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. 네트워크에 연결된 모든 기기가 발견되면 해당 기기에 대한 정보를 가져오고 정책을 통해 기기를 관리할 수 있습니다. 새 기기가 있는지와 이전에 발견된 기기가 네트워크에 아직 있는지를 확인하려면 정기 네트워크 검색을 수행해야 합니다.

네트워크에 연결된 기기를 발견하는 것은 다음 단계로 진행됩니다:

1. **초기 기기 발견**

   빠른 시작 마법사가 완료되면 수동으로 기기 발견을 수행합니다.

2. **이후 검색 구성**

   IP 범위 검색이 활성화되어 있으며 검색 스케줄이 조직의 요구 사항에 맞는지 확인합니다. 검색 스케줄을 구성할 때는 권장 네트워크 검색 빈도를 사용합니다.

   네트워크가 IPv6 장치를 포함하면 제로 구성 검색을 활성화할 수도 있습니다.

3. **발견된 기기를 관리 그룹에 추가하는 규칙 설정(선택 사항)**

   네트워크에 표시되는 새 기기는 정기 검색 중에 발견되어 **미할당 기기** 그룹에 자동으로 포함됩니다. 원하는 경우 **관리 중인 기기** 그룹으로 자동으로 이러한 기기를 이동하는 규칙을 설정할 수 있습니다. 보존 규칙을 설정할 수도 있습니다.

   이 규칙 설정 단계를 건너뛰면 새로 발견된 모든 기기는 **미할당 기기** 그룹으로 이동되어 해당 그룹에 유지됩니다. 원하는 경우 이러한 기기를 수동으로 **관리 중인 기기** 그룹으로 이동할 수 있습니다. 기기를 수동으로 **관리 중인 기기** 그룹으로 이동하는 경우, 각 기기 관련 정보를 분석하여 해당 기기를 관리 그룹으로 이동할지 여부와 기기를 이동하려는 그룹을 결정할 수 있습니다.

결과

시나리오를 완료하면 다음과 같은 결과를 얻을 수 있습니다:

- Kaspersky Security Center Linux 중앙 관리 서버가 네트워크에 있는 장치를 발견하여 해당 장치와 관련된 정보를 제공합니다.
- 이후 검색이 설정되어 지정된 스케줄에 따라 수행됩니다.

새로 검색한 장치는 구성한 규칙에 따라 정렬됩니다(규칙을 구성하지 않았다면, 장치가 **미할당 기기** 그룹에 남습니다).

IP 범위 검색

Kaspersky Security Center에서는 표준 DNS 요청을 사용하여 모든 IPv4 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. 이 영역이 구성되어 있지 않으면 IP 서브넷 검색에서 결과가 반환되지 않습니다.

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.

IP 범위 검색만 활성화되었다면, Kaspersky Security Center는 IPv4 주소만 있는 장치를 검색합니다. 네트워크가 IPv6 장치를 포함하면, 장치의 제로 구성 검색을 켭니다.

IP 범위 검색에 대한 설정 보기 및 수정

IP 범위 검색 속성을 보고 수정하려면 다음 단계를 따릅니다.

1. **발견 및 배포 → 발견 → IP 범위**으로 갑니다.
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:
   - **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.
   - **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

모두 펼치기 | 모두 접기

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. **발견 및 배포 → 발견 → IP 범위**로 갑니다.
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. **발견 및 배포 → 발견 → IP 범위**으로 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.

제로 구성 검색

이 검색 유형은 Linux 기반 배포 지점에 대해서만 지원됩니다.

Kaspersky Security Center는 IPv6 주소를 사용하는 장치가 있는 네트워크를 검색할 수 있습니다. 이때, IP 범위는 지정되지 않으며, Kaspersky Security Center에서 제로 구성 네트워킹(이하 *제로 구성*)을 사용하여 전체 네트워크를 검색합니다. 제로 구성 사용을 시작하려면 네트워크(중앙 관리 서버 또는 배포 지점)를 검색하는 Linux 장치에 avahi-browse 유틸리티를 설치해야 합니다.

제로 구성 검색을 활성화하려면 다음을 수행하십시오.

1. **발견 및 배포 → 발견 → IP 범위**로 갑니다.
2. **속성** 버튼을 누릅니다.
3. 창이 열리면 **제로 구성을 사용하여 IPv6 네트워크 폴링**토글 버튼을 켭니다.

그러면 Kaspersky Security Center에서 네트워크를 검색하기 시작합니다. 이 경우 지정된 IP 범위가 무시됩니다.

기기 태그

이 섹션에서는 기기 태그에 대해 설명하며 이러한 태그를 생성/수정하고 기기에 태그를 수동이나 자동으로 지정하는 지침을 제공합니다.

기기 태그 정보

Kaspersky Security Center에서는 기기를 *태그*할 수 있습니다. 태그는 기기 그룹화, 설명 또는 검색에 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 대해 태그를 지정해야 하는 경우 수동 태그를 사용할 수 있습니다. 자동 태그는 지정된 태그 규칙에 따라 Kaspersky Security Center에서 수행합니다.

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 CentOS를 실행하는 모든 기기에 `[CentOS]` 태그를 할당하는 규칙을 설정할 수 있습니다. 그런 다음 기기 조회를 만들 때 이 태그를 사용할 수 있습니다. 그러면 모든 CentOS 기기를 손쉽게 분류하여 작업을 할당할 수 있습니다.

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 **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 **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 **기기 → 태그 → 기기 태그**로 이동합니다.
2. 목록에서 삭제할 장치 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 장치에 할당한 태그라면, 장치에서 자동 제거되지 않습니다. 장치에서 태그를 제거하려면 klscflag 유틸리티를 사용하십시오.

태그가 할당된 기기 보기

태그가 할당된 기기를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **기기 → 태그 → 기기 태그**로 이동합니다.
2. 할당된 기기를 확인하려는 태그 옆의 **기기 보기** 링크를 누릅니다.
   태그 옆에 **기기 보기** 링크가 표시되지 않으면 해당 태그가 어떤 기기에도 할당되지 않은 것입니다.

나타나는 기기 목록에는 태그가 할당된 기기만 표시됩니다.

기기 태그 목록으로 돌아가려면 브라우저의 **뒤로** 버튼을 누릅니다.

기기에 할당된 태그 보기

기기에 할당된 태그를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **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.

기기에 다른 태그를 할당하거나 이미 할당된 태그를 제거할 수 있습니다. 중앙 관리 서버에 있는 모든 기기 태그를 확인할 수도 있습니다.

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 **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 할당 해제** 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 장치에 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 **기기 → 태그 → 자동 태그 입력 규칙**로 이동합니다.
- 메인 메뉴에서 **기기 → 태그**, and then click the **자동 태그 입력 규칙 설정** 링크를 누릅니다.
- 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 256자 이내여야 합니다.

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 256자 이내여야 합니다.

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 256자 이내여야 합니다.

4. 조건 섹션에서 **추가** 버튼을 눌러 새 조건을 추가합니다.
새 조건 설정 창이 열립니다.

5. 조건 이름을 입력합니다.
이름은 256자 이내여야 합니다. 이름은 규칙 내에서 고유해야 합니다.

6. 다음 조건에 따라 규칙 활성화를 설정합니다. 조건은 여러 개 선택할 수 있습니다.

- **네트워크** - 기기의 DNS 이름, 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.
- **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 관리되는 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.

애플리케이션 태그

이 섹션에서는 애플리케이션 태그에 대해 설명하며 이러한 태그를 생성 및 수정하고 타사 애플리케이션에 태그를 지정하는 지침을 제공합니다.

애플리케이션 태그 정보

Kaspersky Security Center Linux에서는 타사 애플리케이션(Kaspersky가 아닌 소프트웨어 공급 업체에서 만든 애플리케이션)에 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.

Kaspersky 애플리케이션 배포

이 섹션에서는 Kaspersky Security Center 14 웹 콘솔을 통해 조직의 클라이언트 기기에 Kaspersky 애플리케이션을 배포하는 방법에 대해 설명합니다.

시나리오: Kaspersky 애플리케이션 배포

이 시나리오는 Kaspersky Security Center 14 웹 콘솔을 통해 Kaspersky 애플리케이션을 배포하는 방법을 설명합니다. 빠른 시작 마법사 및 보호 배포 마법사를 사용하거나 필요한 모든 단계를 수동으로 완료할 수도 있습니다.

Kaspersky 애플리케이션 배포는 다음 단계로 진행됩니다.

1. **애플리케이션용 관리 웹 플러그인 다운로드**

   Kaspersky 웹사이트에서 Kaspersky Endpoint Security for Linux용 관리 웹 플러그인을 다운로드 한 다음 Kaspersky Security Center 14 웹 콘솔에 플러그인을 추가합니다.

2. **네트워크 에이전트용 설치 패키지 다운로드 및 생성**

   Kaspersky 웹사이트에서 네트워크 에이전트 배포 패키지를 다운로드 한 다음 네트워크 에이전트 설치 패키지를 생성합니다.

   다운로드한 배포 패키지로 네트워크 에이전트를 로컬 설치할 수 있습니다. 이렇게 하려면 Kaspersky Endpoint Security for Linux 설명서 의 지침을 따르십시오.

3. **Kaspersky Endpoint Security for Linux용 설치 패키지 다운로드 및 생성**

   Kaspersky 웹사이트에서 Kaspersky Endpoint Security for Linux 배포 패키지를 다운로드 한 다음 Kaspersky Endpoint Security for Linux 설치 패키지를 생성합니다.

4. **독립 실행형 설치 패키지 생성(선택 사항)**

   Kaspersky Security Center Linux에서 원격 직원의 장치 등 일부 장치에 Kaspersky 애플리케이션을 설치할 수 없을 시, 애플리케이션에 대한 독립 실행형 설치 패키지를 생성할 수 있습니다. 독립 실행형 패키지를 사용하여 Kaspersky 애플리케이션을 설치하는 경우 아래 5단계 및 6단계는 무시해도 됩니다.

5. **원격 설치 작업 생성, 구성 및 실행**

   이 단계는 보호 배포 마법사의 일부입니다. 보호 배포 마법사를 실행하지 않으려는 경우 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.

   > SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면 insserv-compat 패키지를 먼저 설치 해서 네트워크 에이전트를 구성합니다.

6. **작업 생성 및 구성**

   Kaspersky Endpoint Security for Linux의 *업데이트* 작업을 구성해야 합니다.

   이 단계는 빠른 시작 마법사의 일부분이며, 작업은 기본 설정을 사용하여 자동으로 생성 및 구성됩니다. 마법사를 실행하지 않은 경우 이러한 작업을 수동으로 생성한 다음 구성해야 합니다. 빠른 시작 마법사 사용 시, 작업 일정이 요구 사항에 맞는지 확인하십시오(기본적으로 작업 시작 예약은 **수동** 설정해야 하지만, 다른 옵션을 선택할 수도 있습니다).

7. **정책 만들기**

   Kaspersky Endpoint Security for Linux에 대한 정책을 수동으로 또는 빠른 시작 마법사를 통해 생성합니다. 정책의 기본 설정을 사용할 수 있으며, 언제든지 필요에 따라 정책의 기본 설정을 수정할 수도 있습니다.

8. **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 관리 플러그인 추가

Kaspersky Endpoint Security for Linux와 같은 Kaspersky 애플리케이션을 배포하려면 애플리케이션용 관리 웹 플러그인을 추가하고 설치해야 합니다.

Kaspersky 애플리케이션용 관리 웹 플러그인을 추가 및 설치하려면 다음 단계를 따릅니다.

1. Kaspersky 웹사이트에서 Kaspersky Endpoint Security for Linux용 관리 웹 플러그인을 다운로드 합니다.
2. Kaspersky Security Center 14 웹 콘솔을 엽니다.
3. **콘솔 설정** 드롭다운 목록에서 **웹 플러그인**를 선택합니다.
   사용 가능한 관리 플러그인 목록이 표시됩니다.
4. **파일에서 추가** 버튼을 클릭합니다.
   파일에서 추가 창이 표시됩니다.
5. **ZIP 파일 업로드** 버튼을 클릭합니다.
6. 웹 플러그인의 다운로드된 ZIP 파일을 지정합니다.
7. **서명 업로드** 버튼을 클릭합니다.
8. 웹 플러그인 서명의 다운로드된 TXT 파일을 지정합니다.
9. **추가** 버튼을 누릅니다.
   Kaspersky Security Center는 업로드된 파일을 확인한 다음 웹 플러그인을 추가하고 설치합니다.
10. 설치가 완료되면 **확인**를 누릅니다.

관리 웹 플러그인이 기본 구성으로 설치되어 관리 웹 플러그인 목록에 표시됩니다.

파일에서 설치 패키지 생성

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.

사용자 지정 설치 패키지를 만들려면 다음과 같이 하십시오:

1. 다음 중 하나를 수행합니다:
   - **발견 및 배포 → 배포 및 할당 → 설치 패키지**로 이동합니다.
   - **동작 → 저장소 → 설치 패키지**로 갑니다.

   중앙 관리 서버에서 사용 가능한 설치 패키지의 목록이 표시됩니다.
2. **추가**를 누릅니다.
   새 패키지 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
3. 마법사의 첫 페이지에서 **파일에서 설치 패키지 생성**을 선택합니다.
4. 마법사의 다음 페이지에서 패키지 이름을 지정하고 **찾기** 버튼을 누릅니다.
5. 열리는 창에서 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.
   중앙 관리 서버로의 파일 업로드가 시작됩니다.

6. Kaspersky 애플리케이션의 파일을 지정할 시, 애플리케이션에 대한 최종 사용자 라이센스 계약서(EULA)를 읽고 수락하라는 메시지가 표시될 수 있습니다. 계속하려면 EULA를 수락해야 합니다. EULA의 조건을 완전히 읽고 이해했으며 수락할 때만 **이 최종 사용자 라이센스 계약서의 이용 약관 수락** 옵션을 선택하십시오.

   또한 개인정보취급방침을 읽고 수락하라는 메시지가 표시될 수 있습니다. 계속하려면 개인정보취급방침을 수락해야 합니다. 사용자의 데이터가 개인정보취급방침의 설명대로 취급 및 전송(제삼국으로의 전송 포함)될 수 있다는 점을 이해하고 이에 동의할 때만 **개인정보취급방침에 동의함** 옵션을 선택하십시오.

7. 마법사의 다음 페이지에서 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.

8. **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.
  - **수정된 날짜**. 설치 패키지 수정 날짜.
  - **유형**. 설치 패키지의 유형.
- 명령줄 파라미터를 변경합니다.

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 장치에서 수신한 파일을 로컬로 실행하여 Kaspersky Security Center Linux 없이 애플리케이션을 설치할 수 있습니다. Kaspersky 애플리케이션 및 타사 애플리케이션의 독립 실행형 설치 패키지를 생성할 수 있습니다. 타사 애플리케이션에 대한 독립 실행형 설치 패키지를 생성하려면 사용자 지정 설치 패키지를 생성해야 합니다.

> 타인은 독립 실행형 설치 패키지를 사용할 수 없습니다.

독립 실행형 설치 패키지를 만들려면 다음과 같이 하십시오:

1. 다음 중 하나를 수행합니다:
   - **발견 및 배포→ 배포 및 할당 → 설치 패키지**로 갑니다.
   - **동작 → 저장소 → 설치 패키지**로 갑니다.

   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 마법사의 첫 페이지에서 **이 애플리케이션과 함께 네트워크 에이전트 설치** 옵션이 활성화되어 있는지 확인합니다.

   기본적으로 이 옵션은 켜져 있습니다. 기기에 네트워크 에이전트 설치 여부가 확실하지 않은 경우 이 옵션을 활성화하는 것이 좋습니다. 장치에 네트워크 에이전트가 이미 설치되어 있다면, 네트워크 에이전트가 포함된 독립 실행형 설치 패키지 설치 시 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 존재하면 마법사가 이 사실을 알려줍니다. 이 경우 다음 작업 중 하나를 선택해야 합니다:

   - **독립 실행형 설치 패키지 만들기**. 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 만들기**. 동일한 애플리케이션에 대한 독립 실행형 설치 패키지를 다시 만들려면 이 옵션을 선택합니다. 독립 실행형 설치 패키지는 동일한 폴더에 있습니다.

5. 마법사의 **관리 중인 기기 목록으로 이동** 페이지에는 **기기를 이동하지 않음** 옵션이 기본적으로 선택되어 있습니다. 네트워크 에이전트 설치 후 클라이언트 기기를 관리 그룹으로 이동하지 않으려면 옵션 선택을 변경하지 마십시오.

   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. 마법사의 다음 페이지에서 독립 실행형 설치 패키지 생성이 완료된 경우 **완료** 버튼을 누릅니다.

   독립 실행형 설치 패키지 만들기 마법사가 닫힙니다.

독립 실행형 설치 패키지가 만들어지고 중앙 관리 서버 공유 폴더의 Pkglnst 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.
- **수정된 날짜**. 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.

네트워크 에이전트 원격 설치를 위한 Linux 기기 준비

네트워크 에이전트 원격 설치를 위한 Linux 기기를 준비하려면 다음과 같이 하십시오:

1. 대상 Linux 장치에 다음 소프트웨어가 설치되어 있는지 확인합니다:
   - Sudo
   - Perl 언어 인터프리터 버전 5.10 이상
2. 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`

문제 없이 장치에 연결할 수 있는 경우 /etc/ssh/sshd_config 파일을 수정하지 마십시오. 그렇지 않으면 원격 설치 작업을 실행할 때 SSH 인증 실패가 발생할 수 있습니다.

필요한 경우 파일을 저장하고 `sudo service ssh restart` 명령을 사용하여 SSH 서비스를 다시 시작합니다.

a. 기기를 연결하는 데 사용할 사용자 계정의 sudo 암호를 사용하지 않도록 설정합니다.

b. sudo에서 `visudo` 명령을 사용하여 sudoers 구성 파일을 엽니다.
파일이 열리면 `%sudo`(Cent OS 운영 체제 사용 시 `%wheel`)로 시작하는 열을 찾습니다. 이 열 아래에 다음을 입력합니다: `<username > ALL = (ALL) NOPASSWD: ALL`. 이때, `username` 은 사용자 계정이며, SSH를 통해 해당 장치에 연결할 때 사용합니다. Astra Linux 운영 체제를 사용한다면 /etc/sudoers 파일에서 마지막 줄에 `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL` 을 추가합니다.

c. sudoers를 저장하고 닫습니다.

d. SSH를 통해 기기에 다시 연결하여 Sudo 서비스에서 암호를 입력하라는 메시지가 표시되지 않음을 확인합니다: `sudo whoami` 명령을 사용하면 이 작업을 수행할 수 있습니다.

1. /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

   변경된 설정을 적용하려면 Linux 기기를 다시 시작하거나 다음 명령을 실행합니다.
   `$ sudo systemctl restart systemd-logind.service`
2. SUSE Linux Enterprise Server 15 운영 체제가 설치된 기기에 네트워크 에이전트를 설치하려면 insserv-compat 패키지를 먼저 설치 해서 네트워크 에이전트를 구성합니다.
3. 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. 네트워크 에이전트 설치 패키지 다운로드.
   c. 원격 설치 패키지를 만들려면 다음 파일을 사용하십시오:
      - klnagent.kpd

- akinstall.sh
- 네트워크 에이전트의 .deb 또는 .rpm 패키지

4. 다음 설정을 사용하여 원격 설치 작업을 만듭니다:
   - 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 장치 연결에 사용할 사용자 계정의 설정을 지정합니다.
5. 원격 설치 작업을 실행합니다. `su` 명령에 대한 옵션을 사용하여 환경을 보존합니다: `-m, -p, --preserve-environment`.

20 버전 이전의 Fedora 버전을 실행하는 기기에 SSH로 네트워크 에이전트를 설치하는 경우 설치 시 오류가 발생할 수 있습니다. 이 경우 네트워크 에이전트를 성공적으로 설치하려면 /etc/sudoers 파일에 있는 Defaults requiretty 옵션을 주석 처리(해당 코드를 없애기 위해 주석 문법으로 처리함)하십시오. SSH 연결 중에 문제를 일으킬 수 있는 Defaults requiretty 옵션의 조건에 대한 자세한 설명은 Bugzilla bugtracker 웹사이트 를 참조하십시오.

원격 설치 작업을 사용하여 애플리케이션 설치

Kaspersky Security Center Linux에서 원격 설치 작업을 사용해 장치에 애플리케이션을 원격 설치할 수 있습니다. 이런 작업은 전용 마법사를 통해 만들어지고 기기에 할당됩니다. 기기에 빠르고 쉽게 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 장치의 DNS 이름, IP 주소, IP 서브넷을 지정할 수 있습니다.
- **기기 조회 결과에 작업 할당**. 이 경우 이전에 만든 조회에 포함되는 기기에 작업이 할당됩니다. 기본 조회 또는 직접 만든 사용자 지정 조회를 지정할 수 있습니다.
- **관리 그룹에 작업 할당**. 이 경우 이전에 만든 관리 그룹에 포함된 기기 작업이 할당됩니다.

네트워크 에이전트가 설치되지 않은 기기에 원격 설치를 제대로 하려면 a) TCP 139 및 445, b) UDP 137 및 138 포트를 열어 두어야 합니다. 기본적으로 이러한 포트는 해당 도메인에 포함된 모든 기기에 열려 있습니다. 원격 설치 준비 유틸리티와 함께 자동으로 열립니다.

특정 장치에 애플리케이션 설치

모두 펼치기 | 모두 접기

이 섹션에는 관리 그룹, 특정 IP 주소가 있는 장치, 선택한 관리 중인 장치에 애플리케이션을 원격 설치하는 방법에 대한 정보가 포함되어 있습니다.

특정 장치에 애플리케이션을 설치하려면:

1. 메인 메뉴에서 **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.
   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

     작업을 할당할 장치의 DNS 이름, IP 주소, 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 조회 결과에 작업 할당**

     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.

5. 마법사의 지침을 따릅니다.

   작업 추가 마법사는 마법사에서 선택한 애플리케이션을 지정된 장치에 원격 설치할 작업을 생성합니다. **관리 그룹에 작업 할당** 옵션 선택 시, 작업은 그룹 1입니다.

6. 이 작업을 직접 실행하거나, 작업 설정에 지정한 스케줄에 따라 실행될 때까지 기다립니다.

원격 설치 작업이 완료되면 선택한 애플리케이션이 지정된 장치에 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 Center가 선택한 Kaspersky 애플리케이션을 애플리케이션의 공유 네트워크 폴더인 Share에서 바로 클라이언트 기기에 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 선택한 경우에는 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.

   작업 추가 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 **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 없는 경우, 이 옵션을 선택한 다음, 루트 계정의 암호를 지정합니다. Kaspersky Security Center 14 Linux는 암호화된 형식으로 암호를 대상 장치에 전송하고 암호를 복호화한 후, 지정한 암호로 루트 계정을 대신하여 설치 절차를 시작합니다.

     Kaspersky Security Center 14 Linux는 SSH 연결을 생성할 때 계정이나 지정된 암호를 사용하지 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 Center 14 Linux는 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.

타사 보안 제품 교체

Kaspersky Security Center Linux를 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.

애플리케이션의 원격 설치를 구성할 때 비-호환 애플리케이션 제거

보호 배포 마법사에서 보안 제품의 원격 설치를 구성할 때 **비-호환 애플리케이션 자동 제거** 옵션을 활성화할 수 있습니다. 이 옵션을 사용하도록 설정하면 Kaspersky Security Center는 비-호환 애플리케이션을 제거한 후 보안 제품을 관리 중인 기기에 설치합니다.

방법 지침: 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.

방법 지침: 작업 만들기

애플리케이션 또는 소프트웨어 업데이트 원격 제거

모두 펼치기 | 모두 접기

Linux를 실행하는 관리 장치에서는 네트워크 에이전트를 사용해서만 애플리케이션 또는 소프트웨어 업데이트를 원격 제거할 수 있습니다.

선택한 기기에서 애플리케이션 또는 소프트웨어 업데이트를 원격으로 제거하려면 다음 단계를 따르십시오.

1. 메인 메뉴에서 **기기 → 작업**으로 이동합니다.
2. **추가**를 누릅니다.
   작업 추가 마법사가 시작됩니다. **다음** 버튼을 사용하여 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 할당될 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.

   - **비-호환 애플리케이션 제거**

     Kaspersky 보안 제품 또는 Kaspersky Security Center와 호환되지 않는 애플리케이션 목록이 표시됩니다. 제거할 애플리케이션 옆에 있는 확인란을 선택합니다.

   - **자산 관리(소프트웨어)에 등록된 애플리케이션 제거 (강제 또는 원격 제거를 해당 애플리케이션에서 지원해야 함)**

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.

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.

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 Linux 운영 체제 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**

  옵션은 이제 사용하지 않습니다. **네트워크 에이전트 이용** 옵션이나 **배포 지점에서 대상 운영 체제의 관리 공유 폴더로 다운로드** 옵션을 사용하십시오.

  파일은 중앙 관리 서버 운영 체제 도구를 사용하여 클라이언트 장치로 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.

- **제거 시도 최대 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.

  제거 시도 최대 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 **제거 시도 최대 횟수** 파라미터 값을 높이고 애플리케이션 제거 작업을 시작할 수 있습니다. 또는 새 *애플리케이션을 원격으로 제거*작업을 생성할 수 있습니다.

- **다운로드하기 전에 운영 체제 유형 확인**

  클라이언트 장치에 파일을 전송하기 전에 Kaspersky Security Center는 설치 유틸리티 설정을 클라이언트 장치의 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 장치가 포함된 관리 그룹의 장치에 일부 애플리케이션을 설치하려면, 관리 그룹에 설치 작업을 할당하고 이 옵션을 활성화하여 필요한 운영 체제 이외의 운영 체제를 실행하는 장치를 건너뜁니다.

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.

- **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.

  네트워크 에이전트가 클라이언트 기기에 설치되어 있지 않다면, 이 옵션은 이용할 수 없습니다.

- **계정 필요(네트워크 에이전트는 사용되지 않음)**

애플리케이션 원격 제거 작업을 할당한 장치에 네트워크 에이전트가 설치되어 있지 않다면 이 옵션을 선택합니다.

애플리케이션 설치 프로그램을 실행할 사용자 계정을 지정합니다. **추가** 버튼을 클릭하고 **계정**을 선택한 다음 사용자 계정 자격 증명을 지정합니다.

예를 들어 이 작업이 할당된 모든 장치에 필요한 모든 권한이 어떤 계정에도 없다면, 사용자 계정을 여러 개 지정할 수 있습니다. 이때, 작업 실행 시 추가한 모든 계정을 위에서부터 순서대로 사용합니다.

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.

네트워크 에이전트 설치를 위해 SUSE Linux Enterprise Server 15를 실행하는 기기 준비

SUSE Linux Enterprise Server 15 운영 체제가 설치된 장치에 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 편한 방법을 사용하면 됩니다.

SUSE Linux Enterprise Server 15 장치를 준비한 후 네트워크 에이전트를 배포 및 설치합니다 .

Kaspersky 애플리케이션: 라이센싱 및 활성화

이 섹션에서는 관리 중인 Kaspersky 애플리케이션의 라이센스 키 처리와 관련된 Kaspersky Security Center의 기능에 대해 설명합니다.

Kaspersky Security Center Linux로 클라이언트 장치에 Kaspersky 애플리케이션 라이센스 키를 중앙 집중식으로 배포하고 장치의 라이센스 키 사용을 모니터링하며 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. 세 개의 라이센스 키 모두에 대해 **자동으로 라이센스 키 배포** 옵션을 활성화했습니다. Kaspersky 보안 제품(Kaspersky Endpoint Security for Linux 등)이 기업의 장치에 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:

- 중앙 관리 서버 저장소에 라이센스 키 추가
- 라이센스 키 자동 배포

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: 라이센스 키를 설치 패키지에 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:

- 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.

- **활성화코드 입력**
  텍스트 필드에서 활성화코드를 지정하고 **보내기** 버튼을 누릅니다.

4. **닫기** 버튼을 누릅니다.

라이센스 키 하나 또는 여러 개가 중앙 관리 서버 저장소에 추가됩니다.

클라이언트 기기에 라이센스 키 배포

Kaspersky Security Center 14 웹 콘솔에서는 *라이센스 키 배포* 작업을 통해 클라이언트 기기에 라이센스 키를 배포할 수 있습니다.

배포하기 전에 중앙 관리 서버 저장소에 라이센스 키를 추가합니다.

클라이언트 기기에 라이센스 키를 배포하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창에서 **기기 → 작업**로 이동합니다.
2. **추가**를 누릅니다.
   작업 추가 마법사가 시작됩니다.
3. 라이센스 키를 추가할 애플리케이션을 선택합니다.
4. **작업 유형** 목록에서 **라이센스 키 추가**를 선택합니다.
5. 마법사의 지침을 따르십시오.
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. **만들기** 버튼을 누릅니다.
   그러면 작업이 생성되고 작업 목록에 표시됩니다.
8. 작업을 실행하려면 작업 목록에서 작업을 선택하고 **시작** 버튼을 누릅니다.

작업이 수행되면 라이센스 키가 선택한 기기에 배포됩니다.

라이센스 키 자동 배포

라이센스 키가 중앙 관리 서버의 라이센스 키 저장소에 있을 시 Kaspersky Security Center Linux에서 관리 중인 장치에 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 설치** 확인란을 선택합니다.
4. **저장** 버튼을 누릅니다.

라이센스 키는 모든 호환 장치에 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.

라이선스 키 속성 창에서 **관리 중인 기기에 자동으로 라이센스 키 설치** 확인란을 선택하면 라이선스 키가 네트워크에 즉시 배포됩니다. 이 옵션을 선택하지 않으면 나중에 수동으로 라이센스 키를 배포할 수 있습니다.

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 **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.

저장소에서 라이센스 키 삭제

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. **동작 → 라이센스 → Kaspersky 라이센스**로 이동합니다.
2. 저장소에서 삭제할 키 파일 또는 활성화코드를 선택합니다.
3. **삭제** 버튼을 누릅니다.
4. **확인** 버튼을 눌러 작업을 확인합니다.

선택한 키 파일 또는 활성화코드가 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.

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.

Kaspersky Security Center 14 웹 콘솔에서 다음 스케줄에 따라 라이센스가 만료되려고 할 때 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 Center 14 Linux에서 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 자산) 수:
  - 50~250
  - 250–1000

- 300대 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
- 설치된 Kaspersky Security Center 14 웹 콘솔
- Kaspersky Security Center 주요 설치 시나리오 완료됨
- 빠른 시작 마법사 완료 또는 **관리 중인 기기** 관리 그룹에서 다음과 같은 정책과 작업을 수동으로 생성:

  - Kaspersky Endpoint Security 정책
  - Kaspersky Endpoint Security 업데이트를 위한 그룹 작업
  - 네트워크 에이전트의 정책

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.

2. **Kaspersky 애플리케이션 원격 관리용 작업 구성**

   빠른 시작 마법사에서 생성된 작업을 확인하고 필요한 경우 미세 조정합니다.

   방법 지침: Kaspersky Endpoint Security 업데이트를 위한 그룹 작업 설정.

   필요한 경우 클라이언트 기기에 설치된 Kaspersky 애플리케이션을 관리하기 위한 추가 작업을 생성합니다.

3. **데이터베이스의 이벤트 부하 평가 및 제한**

   관리 대상 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: 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.

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 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.

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 인시던트를 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 14 웹 콘솔을 정상적으로 설치했는지 확인하십시오. 또한 기기 중심 접근 방식의 대안이나 추가 옵션으로사용자 중심 보안 관리를 고려할 수도 있습니다. 두 가지 관리 접근 방식에 대해 자세히 알아보십시오.

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 Kaspersky Endpoint Security for Linux 용 기본 정책을 생성합니다. 이 마법사를 사용하여 구성 프로세스를 완료한 경우에는 이 애플리케이션용으로 새 정책을 생성할 필요가 없습니다.

   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. **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 예를 들어, 특정 하드웨어 구성을 포함하거나, 특정 태그로 표시된 기기 등에 다른 정책 프로필을 적용할 수 있습니다. 태그를 사용하여 특정 기준을 충족하는 기기를 필터링합니다. 예를 들어 *CentOS* 태그를 생성하여 CentOS 운영 체제를 실행 중인 모든 기기를 이 태그로 표시한 다음 정책 프로필의 활성화 조건으로 이 태그를 지정할 수 있습니다. 그러면 CentOS를 실행 중인 모든 기기에 설치된 Kaspersky 애플리케이션이 자체 정책 프로필을 통해 관리됩니다.

   방법 지침:

   - 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. 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

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.

필수 구성 요소

시작하기 전에 Kaspersky Security Center 중앙 관리 서버 및 Kaspersky Security Center 14 웹 콘솔을 정상적으로 설치했으며 기본 배포 시나리오를 완료했는지 확인하십시오. 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 보호를 구성할 때 Kaspersky Security Center는 Kaspersky Endpoint Security용 기본 정책을 생성합니다. 이 마법사를 사용하여 구성 프로세스를 완료한 경우에는 이 애플리케이션용으로 새 정책을 생성할 필요가 없습니다.

   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 Kaspersky Security Center는 15분마다 중앙 관리 서버와 관리 중인 기기를 자동으로 동기화합니다. 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.

Kaspersky Endpoint Security용 그룹 업데이트 작업 수동 설정

Kaspersky Endpoint Security에서 권장되는 최적의 스케줄 옵션은 **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후** 및 **랜덤하게 작업 시작 시간을 자동으로 조절하는 기능 사용** 확인란 선택하는 경우입니다.

네트워크 에이전트 정책 설정

모두 펼치기 | 모두 접기

네트워크 에이전트 정책을 구성하려면 다음을 수행하십시오:

1. 메인 메뉴에서 **기기 → 정책 및 프로필**이동합니다.
2. 네트워크 에이전트 정책의 이름을 클릭합니다.

   네트워크 에이전트 정책의 속성 창이 열립니다.

일반

이 탭에서 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.

  - **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.
    이 옵션은 기본적으로 활성화되어 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 목록에는 이벤트 유형 및 중앙 관리 서버에 기본 이벤트가 저장되는 기간(일)이 표시됩니다. 이벤트 유형을 누른 후 목록에서 선택된 이벤트에 대한 이벤트 로그 및 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 **인시던트 발생** 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). **인시던트 발생** 이벤트를 구성하려면 이를 누른 다음, 발생한 이벤트를 저장할 위치와 알림 방법을 지정하면 됩니다.

네트워크 에이전트가 인시던트를 감지한 경우 관리 중인 기기의 설정을 사용하여 이 인시던트를 관리할 수 있습니다.

애플리케이션 설정

설정

설정 섹션에서는 네트워크 에이전트 정책을 구성할 수 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 장치에 설치된 네트워크 에이전트는 적용된 보안 제품 정책에 대한 정보를 보안 제품(Kaspersky Endpoint Security for Linux 등)으로 전송합니다. 보안 제품 인터페이스에서 전송된 정보를 볼 수 있습니다.

  네트워크 에이전트는 다음 정보를 전송합니다:

  - 관리 중인 기기로 정책을 전달하는 시간
  - 관리 중인 기기로 정책을 전달할 때 활성 또는 이동 사용자 정책의 이름
  - 관리 중인 기기로 정책을 전달할 때 관리 중인 기기가 포함된 관리 그룹의 이름 및 전체 경로
  - 활성 정책 프로필 목록

    이 정보를 기기에 올바른 정책을 적용하는 데 사용하고 문제 해결 목적으로 사용할 수도 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.

  이 옵션은 기본적으로 활성화되어 있습니다.

- **자산 관리(하드웨어) 정보**

  기기에 설치된 네트워크 에이전트는 기기 하드웨어에 관한 정보를 중앙 관리 서버로 전송합니다. 기기 속성에서 하드웨어 세부 정보를 볼 수 있습니다.

네트워크

네트워크 섹션에는 세 가지의 하위 섹션이 있습니다:

- **연결성**
- **연결 프로필**
- **연결 스케줄**

연결성 하위 섹션에서 중앙 관리 서버에 대한 연결을 구성하고 UDP 포트의 사용을 설정하며 그 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(하트비트)은 관리 중인 장치 10,000대당 15분으로 설정할 것을 권장합니다.

    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.

- **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 가능할 경우)의 연결 게이트웨이 사용**

  이 옵션을 사용하면 관리 그룹 속성에 지정된 설정에 따라 배포 지점의 연결 게이트웨이가 사용됩니다.
  이 옵션은 기본적으로 활성화되어 있습니다.

- **UDP 포트 사용**

  UDP 포트를 통해 관리 중인 장치를 KSN 프록시 서버에 연결하려면, **UDP 포트 사용** 옵션을 선택하고 **UDP 포트 번호**를 지정합니다. 이 옵션은 기본적으로 활성화되어 있습니다. KSN 프록시 서버에 연결하는 기본 UDP 포트는 15111입니다.

- **UDP 포트 번호**

  이 필드에는 UDP 포트 번호를 입력할 수 있습니다. 기본 포트 번호는 15000입니다.
  십진법을 사용하여 기록합니다.

네트워크 섹션의 **연결 프로필** 하위 섹션에서 네트워크 위치 설정을 지정하고 중앙 관리 서버를 사용할 수 없을 때 이동 사용자 모드를 활성화할 수 있습니다. **연결 프로필** 섹션의 설정은 Windows를 실행 중인 장치에서만 사용 가능합니다:

- **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**

  연결 프로필은 Windows를 실행 중인 기기에서만 지원됩니다. 이 옵션의 사용은 권장하지 않습니다.

  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 프로필 설정 그룹에서는 **중앙 관리 서버 연결 프로필** 목록에 새 항목을 추가할 수 없으므로 **추가** 버튼이 비활성화되어 있습니다. 사전 설정 연결 프로필도 수정할 수 없습니다.

- **중앙 관리 서버에 연결할 수 없으면 이동 사용자 모드 사용**

  이 옵션을 활성화하면 이 프로필을 통해 연결 시 클라이언트 장치에 설치된 애플리케이션은 이동 사용자 정책 및 이동 사용자 모드의 장치에 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.

- **제로 구성**

  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 중앙 관리 서버가 **검색 스케줄 설정** 링크를 눌러 구성한 스케줄에 따라 자동으로 IP 범위를 검색합니다.

  이 옵션이 비활성화되어 있으면 중앙 관리 서버가 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.

배포 지점에 대한 네트워크 설정

배포 지점에 대한 네트워크 설정 섹션에서 다음과 같이 인터넷 접근 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 선택 해제되어 있습니다.

- **사용자 이름**
- **암호**

업데이트(배포 지점)

업데이트(배포 지점) 섹션에서 diff 파일 다운로드 기능을 활성화하면 배포 지점이 Kaspersky 업데이트 서버에서 diff 파일 형식으로 업데이트됩니다.

리비전 내역

이 탭에서는 정책 리비전 목록을 확인하고 필요한 경우 정책 변경 사항을 롤백할 수 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 14 웹 콘솔 서버에 특정 애플리케이션용 관리 플러그인이 설치되어 있어야 Kaspersky Security Center 14 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 Kaspersky Security Center 14 웹 콘솔을 사용하여 수정할 수도 있고, 원격 장치 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)나 DNS 이름을 장치의 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 조회 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 조회 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 조회를 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 **기기 → 작업**로 이동합니다.
2. **추가**를 누릅니다.

   작업 추가 마법사가 시작됩니다. 해당 지침을 따릅니다.
3. 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.
4. **마침** 버튼을 누릅니다.

그러면 작업이 생성되고 작업 목록에 표시됩니다.

수동으로 작업 시작

애플리케이션은 각 작업 속성에 지정된 스케줄 설정에 따라 작업을 시작합니다. 언제든 수동으로 작업을 시작할 수 있습니다.

작업을 수동으로 시작하려면 다음 단계를 따릅니다.

1. 메인 애플리케이션 창에서 **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 Center Linux에서 생성된 작업 목록을 볼 수 있습니다.

작업 목록을 보려면 다음을 수행합니다.

기기 → 작업으로 이동합니다.

작업 목록이 표시됩니다. 작업은 관련된 애플리케이션 이름별로 그룹화됩니다. 예를 들어 *원격으로 애플리케이션 설치* 작업은 중앙 관리 서버와 관련이 있고 *업데이트* 작업은 Kaspersky Endpoint Security for Linux를 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.

  - **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:
  - **시작 스케줄 설정:**
    - **매 N시간마다**

      작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.

      기본적으로 작업은 현재 시스템 날짜와 시간부터 6시간마다 실행됩니다.

    - **매 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.

    - **매 N주마다**

      작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.

      기본적으로 작업은 월요일마다 현재 시스템 시간에 실행됩니다.

    - **매 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. Kaspersky Security Center Linux 이전 버전과의 호환성에 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.
  이 옵션은 기본적으로 활성화되어 있습니다.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

- **중앙 관리 서버 저장소 업데이트 다운로드를 완료한 후**

  저장소에 업데이트가 다운로드되고 나면 작업이 실행됩니다. 예를 들어 *업데이트* 작업에 이 스케줄을 사용할 수 있습니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 현재 작업 시작을 트리거하려면 이전 작업이 완료되어야 하는 방식(성공적으로 완료 또는 오류 발생)을 선택할 수 있습니다.

- **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 비활성화하면 클라이언트 기기에서 스케줄이 지정된 작업만 실행되며 **수동 시작**, **한번만** 또는 **즉시**의 경우, 네트워크에서 인식된 클라이언트 기기에서만 작업이 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.
  이 옵션은 기본적으로 활성화되어 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 임의 시작(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 수동으로 지정하거나 목록에서 가져오기**

  작업을 할당할 장치의 DNS 이름, IP 주소, 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 조회 결과에 작업 할당**

  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.

- **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.

- 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 계층 에서 모든 수준에 있는 선택된 관리 그룹에 종속됩니다.

    이 옵션이 비활성화되면 작업 범위에는 작업을 생성하는 동안 선택한 관리 그룹만 포함됩니다.
    이 옵션은 기본적으로 활성화되어 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:

  - **Wake-on-LAN 기능으로 이 작업이 실행되기 전에 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 장치 종료** 옵션을 활성화합니다. 이 옵션은 같은 창에서 찾을 수 있습니다.

    기본적으로 이 옵션은 비활성화되어 있습니다.

  - **작업 완료 후 기기 끄기**

    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 (분) 이상 실행된 경우 작업 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 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.

      이 옵션은 기본적으로 활성화되어 있습니다.

    - **기기의 OS 이벤트 로그에 저장**

      작업 실행과 관련된 애플리케이션 이벤트가 각 클라이언트 장치의 Syslog 이벤트 로그에 로컬로 저장됩니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    - **중앙 관리 서버의 OS 이벤트 로그에 저장**

      작업 범위의 모든 클라이언트 장치에서 수행하는 작업 실행과 관련된 애플리케이션 이벤트가 중앙 관리 서버 OS(운영 체제)의 Syslog 이벤트 로그에 중앙 집중식으로 저장됩니다.

      기본적으로 이 옵션은 비활성화되어 있습니다.

    - **모든 이벤트 저장**

      이 옵션을 선택하면 작업과 관련된 모든 이벤트가 이벤트 로그에 저장됩니다.

    - **작업 실행 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.

  이 옵션은 기본적으로 활성화되어 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 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 다음 단계를 따르십시오.

1. **기기** 탭에서 **작업**을 선택합니다.
2. **작업 시작을 위한 계정 자격 증명 관리**를 누릅니다.

마법사의 지침을 따릅니다.

1단계. 자격증명 지정

모두 펼치기 | 모두 접기

시스템에서 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 14 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 누릅니다.

선택한 행동은 마법사의 다음 단계로 이동한 후에 적용됩니다.

3단계. 결과 확인

마법사의 마지막 단계에서 발견된 각 작업의 결과를 확인합니다. 마법사를 완료하려면 **마침** 버튼을 누릅니다.

중앙 관리 서버에 저장된 작업 실행 결과 보기

Kaspersky Security Center Linux에서는 그룹 작업, 특정 장치 작업 및 중앙 관리 서버 작업의 결과를 볼 수 있습니다. 로컬 작업에 대한 실행 결과는 볼 수 없습니다.

작업 결과를 보려면 다음과 같이 하십시오:

1. 작업 속성 창에서 **일반** 섹션을 선택합니다.
2. **결과** 링크를 눌러 **작업 결과** 창을 엽니다.

클라이언트 기기 관리

이 섹션에서는 관리 그룹에서 기기를 관리하는 방법에 대해 설명합니다.

관리 중인 기기 설정

모두 펼치기 | 모두 접기

관리 중인 기기 설정을 보려면:

1. **기기 → 관리 중인 기기**를 선택합니다.
   관리 중인 기기 목록이 표시됩니다.
2. 관리 중인 기기 목록에서 필수 기기의 이름이 포함된 링크를 누릅니다.

선택한 기기의 속성 창이 표시됩니다.

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.

- **그룹**

  클라이언트 기기가 포함된 관리 그룹입니다.

- **마지막 업데이트**

  장치에서 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 옵션을 활성화하면 관리 중인 장치와 중앙 관리 서버의 연결이 유지됩니다. 이 연결을 제공하는 푸시 서버를 사용하지 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

네트워크 섹션에 클라이언트 기기의 네트워크 속성에 대한 다음 정보가 표시됩니다.

- **IP 주소**

  기기 IP 주소.

- **Windows 도메인**

  장치가 포함된 작업 그룹입니다.

- **DNS 이름**

  클라이언트 기기의 DNS 도메인 이름입니다.

- **NetBIOS 이름**

  클라이언트 장치의 이름입니다.

시스템

시스템 섹션은 클라이언트 기기에 설치된 운영 체제에 대한 정보를 제공합니다.

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 장치에서 마지막으로 악성 코드 검사를 수행한 날짜와 시간.

- **탐지된 위협 전체 개수**

  안티 바이러스 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.

애플리케이션에서 정의된 기기 상태

애플리케이션에서 정의된 장치 상태 섹션은 장치에 설치된 관리 중인 애플리케이션에서 정의한 장치 상태 정보를 제공합니다. 이 장치 상태는 Kaspersky Security Center Linux의 정의와 다를 수 있습니다.

애플리케이션

애플리케이션 섹션에는 클라이언트 기기에 설치된 모든 Kaspersky 애플리케이션이 나열됩니다. 애플리케이션 이름을 눌러 애플리케이션에 대한 일반적인 정보, 기기에서 발생한 이벤트의 목록, 애플리케이션 설정을 확인할 수 있습니다.

활성 정책 및 정책 프로필

활성 정책 및 정책 프로필 섹션에는 관리 중인 기기에서 현재 활성 상태인 정책과 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 장치 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. 연결할 수 없는 경우에는 상태가 표시되지 않습니다.

이벤트

이벤트 섹션에는 선택된 클라이언트 장치의 중앙 관리 서버에 기록된 이벤트가 표시됩니다.

태그

태그 섹션에서는 클라이언트 장치 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.

실행 파일

실행 파일 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**

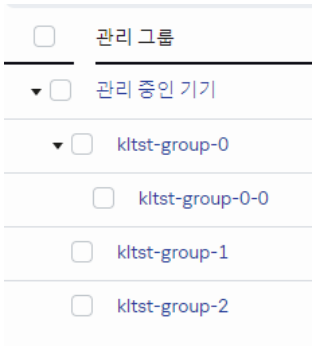
  기기가 상호 작용하는 배포 지점을 보고 구성하려면 **속성** 버튼을 누릅니다.

자산 관리(하드웨어)

자산 관리(하드웨어) 섹션에서는 클라이언트 기기에 설치된 하드웨어에 대한 정보를 확인할 수 있습니다.

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 장치와 가상 컴퓨터를 추가하고 중첩 그룹도 추가할 수 있습니다(아래 그림 참조).



관리 그룹 계층 구조 보기

관리 그룹을 만들려면 다음과 같이 하십시오:

1. **기기 → 그룹 계층 구조**으로 이동합니다.
2. 관리 그룹 구조에서 새 관리 그룹을 포함할 관리 그룹을 선택합니다.
3. **추가** 버튼을 누릅니다.
4. **새 관리 그룹의 이름** 창이 열리면 그룹 이름을 입력하고 **추가** 버튼을 클릭합니다.

지정한 이름의 새 관리 그룹 폴더가 관리 그룹의 계층 구조에 나타납니다.

관리 그룹의 구조를 만들려면 아래와 같이 진행합니다:

1. **기기 → 그룹 계층 구조**으로 이동합니다.
2. **가져오기** 버튼을 누릅니다.

새 관리 그룹 구조 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

기기 이동 규칙

*기기 이동 규칙*을 통해 관리 그룹에 기기를 자동으로 할당하도록 설정하는 것이 좋습니다. 장치 이동 규칙은 크게 이름, 실행 조건(장치 특성이 포함된 논리식), 대상 관리 그룹으로 구성됩니다. 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. Kaspersky Security Center Linux 관리자가 **기기 → 이동 규칙** 섹션에서 장치 이동 규칙을 명시적으로 생성할 수도 있습니다.

기본적으로 기기 이동 규칙은 기기를 관리 그룹으로 한 번 초기 할당할 때 사용됩니다. 이 규칙은 미할당 장치 그룹의 장치를 한 번만 이동합니다. 이 규칙으로 장치를 한 번 이동했다면, 해당 장치를 미할당 장치 그룹에 수동으로 되돌려 놓더라도 장치가 이 규칙에 따라 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 추가 안 된 기기만 이동** 확인란의 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. 이 시나리오는 특히 접근 권한, 이벤트 및 리포트 영역에서 Kaspersky Security Center Linux의 작동 원칙과도 상충합니다. 정책 프로필 사용, 장치 조회 작업, 표준 시나리오에 따라 네트워크 에이전트 할당 등 다른 방법을 사용해야 합니다.

기기 이동 규칙 생성

관리 그룹에 장치를 자동 할당하는 기기 이동 규칙을 설정할 수 있습니다.

이동 규칙을 생성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **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.

- **규칙 적용**

  다음 옵션 중 하나를 선택할 수 있습니다:
  - 각 기기에 대해 한 번 실행.

기준과 일치하는 각 기기에 대해 규칙이 한 번 적용됩니다.

- 각 기기에 대해 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).

- **관리 그룹에 추가 안 된 장치만 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 사용**

  이 옵션을 활성화하면 규칙이 저장한 후에 활성화되어 작동하기 시작합니다.
  이 옵션을 비활성화하면 규칙이 생성은 되지만 활성화되지는 않습니다. 이 옵션을 활성화할 때까지는 규칙이 작동하지 않습니다.

4. **규칙 조건** 탭에서 장치를 관리 그룹으로 이동하는 기준을 하나 이상 지정합니다.
5. **저장**를 누릅니다.

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.

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. 메인 메뉴에서 **기기 → 이동 규칙** 탭으로 이동합니다.
   발견 및 배포 → 배포 및 할당을 선택한 다음 메뉴에서 **이동 규칙**을 선택할 수도 있습니다.
   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.

- **규칙 적용**

  다음 옵션 중 하나를 선택할 수 있습니다:
  - 각 기기에 대해 한 번 실행.
    기준과 일치하는 각 기기에 대해 규칙이 한 번 적용됩니다.

- 각 기기에 대해 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).

- **관리 그룹에 추가 안 된 장치만 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 사용**

  이 옵션을 활성화하면 규칙이 저장한 후에 활성화되어 작동하기 시작합니다.
  이 옵션을 비활성화하면 규칙이 생성은 되지만 활성화되지는 않습니다. 이 옵션을 활성화할 때까지는 규칙이 작동하지 않습니다.

5. **규칙 조건** 탭에서 자동 이동할 장치에 관한 기준을 하나 이상 지정합니다.
6. **저장**를 누릅니다.

새 이동 규칙이 생성됩니다. 생성된 규칙은 이동 규칙 목록에 표시됩니다.

장치 이동 규칙 조건

모두 펼치기 | 모두 접기

클라이언트 장치를 관리 그룹으로 이동하는 규칙을 생성하거나 복사할 때 **규칙 조건** 탭에서 장치 이동 조건을 설정합니다. 이동할 장치 결정 시 다음 기준을 사용할 수 있습니다.

- 클라이언트 장치에 할당된 태그.
- 네트워크 매개변수. 예를 들어, 지정된 범위에 IP 주소가 해당하는 장치를 이동할 수 있습니다.
- 네트워크 에이전트 또는 중앙 관리 서버와 같은 클라이언트 장치에 설치된 관리 애플리케이션.
- 클라이언트 장치인 가상 컴퓨터.

아래에서 장치 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 장치 설명에 추가한 장치 태그를 기준으로 장치 이동 규칙을 구성할 수 있습니다. 이렇게 하려면 필요한 태그를 선택합니다. 또한 다음 옵션을 활성화할 수 있습니다.

- **지정된 태그가 없는 기기에 적용**

  이 옵션을 활성화하면 지정된 태그가 있는 모든 장치가 장치 이동 규칙에서 제외됩니다. 이 옵션을 비활성화하면 선택한 모든 태그가 있는 장치에 장치 이동 규칙이 적용됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **하나 이상의 지정 태그가 일치하면 적용**

  이 옵션을 활성화하면 선택된 태그 중 하나 이상이 있는 클라이언트 장치에 장치 이동 규칙이 적용됩니다. 이 옵션을 비활성화하면 선택한 모든 태그가 있는 장치에 장치 이동 규칙이 적용됩니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

네트워크 탭

이 탭에서 장치 이동 규칙이 고려하는 장치의 네트워크 데이터를 지정할 수 있습니다.

- **기기의 DNS 이름**

  이동하려는 클라이언트 장치의 DNS 도메인 이름입니다. 네트워크가 DNS 서버를 포함한다면 이 필드를 입력합니다.

  Kaspersky Security Center에 사용하는 데이터베이스에 대해 대소문자 구분 데이터 정렬이 설정되었다면, 장치 DNS 이름을 지정할 때 대소문자를 구분합니다. 그렇지 않으면 장치 이동 규칙이 작동하지 않습니다.

- **DNS 도메인**

  장치 이동 규칙은 지정된 기본 DNS 접미사에 포함된 모든 장치에 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 장치가 중앙 관리 서버에 연결되는 IP 주소를 설정할 수 있습니다. 이렇게 하려면 필요한 IP 주소를 모두 포함하도록 IP 범위를 지정합니다.
  기본적으로 이 옵션은 비활성화되어 있습니다.

- **연결 프로필이 변경됨**

  다음 값 중 하나를 선택합니다:
  - **예**. 연결 프로필이 변경된 클라이언트 장치에만 장치 이동 규칙이 적용됩니다.
  - **아니요**. 장치 이동 규칙은 연결 프로필이 변경되지 않은 클라이언트 장치에만 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 장치에만 장치 이동 규칙이 적용됩니다. 이 서버는 장치 이동 규칙을 구성하는 서버와 다릅니다.
  - **아니요**. 현재 중앙 관리 서버에서 관리하는 클라이언트 장치에만 장치 이동 규칙이 적용됩니다.
  - **어떤 값도 선택되지 않았습니다**. 조건이 적용되지 않습니다.

애플리케이션 탭

이 탭에서는 클라이언트 장치에 설치된 관리 중인 애플리케이션 및 운영 체제를 기반으로 장치 이동 규칙을 구성할 수 있습니다.

- **네트워크 에이전트가 설치됨**

  다음 값 중 하나를 선택합니다:
  - **예**. 네트워크 에이전트가 설치된 클라이언트 장치에만 장치 이동 규칙이 적용됩니다.
  - **아니요**. 네트워크 에이전트가 설치되지 않은 클라이언트 장치에만 장치 이동 규칙이 적용됩니다.
  - **어떤 값도 선택되지 않았습니다**. 조건이 적용되지 않습니다.

- **애플리케이션**

  클라이언트 장치에 장치 이동 규칙을 적용하기 위해 장치에 어떤 관리 중인 애플리케이션을 설치할지 지정합니다. 예를 들어, **Kaspersky Security Center 14 네트워크 에이전트** 또는 **Kaspersky Security Center 14 중앙 관리 서버**를 선택할 수 있습니다.

관리 중인 애플리케이션을 선택하지 않으면 조건이 적용되지 않습니다.

- **운영 체제 버전**

  운영 체제 버전에 따라 클라이언트 장치를 선택할 수 있습니다. 이를 위해 클라이언트 장치에 설치해야 하는 운영 체제를 지정합니다. 이에 따라, 선택한 운영 체제를 사용하는 클라이언트 장치에 장치 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 장치를 선택할 수 있습니다. **운영 체제 비트 크기** 필드에서 다음 값 중 하나를 선택할 수 있습니다.

  - **알 수 없음**
  - **x86**
  - **AMD64**
  - **IA64**

  클라이언트 장치의 운영 체제 비트 크기를 확인하려면:

  1. 메인 메뉴에서 **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 장치에 대해 운영 체제 비트 크기가 표시됩니다.

- **운영 체제 서비스 팩 버전**

  이 필드에서는 사용자 운영 체제의 패키지 버전을 *XY* 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 장치에만 장치 이동 규칙이 적용됩니다.
  - **설치 안 됨** 모바일 인증서가 없는 모바일 장치에만 장치 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 장치 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 장치 이동 규칙을 구성할 수도 있습니다.

가상 컴퓨터 탭

이 탭에서는 클라이언트 장치가 가상 컴퓨터인지 VDI(가상 데스크톱 인프라)에 속하는지에 따라 장치 이동 규칙을 구성할 수 있습니다.

- **이것은 가상 컴퓨터입니다**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **N/A**. 조건이 적용되지 않습니다.
  - **아니요**. 가상 컴퓨터가 아닌 장치를 이동합니다.
  - **예**. 가상 컴퓨터인 장치를 이동합니다.

- **가상 컴퓨터 유형**

- **가상 데스크톱 인프라 소속**

  드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.
  - **N/A**. 조건이 적용되지 않습니다.
  - **아니요**. VDI에 속하지 않는 장치를 이동합니다.
  - **예**. VDI에 속하는 장치를 이동합니다.

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. **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 누릅니다.
   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.
     - 장치 DNS 이름을 지정합니다.

       장치 이름 필드에는 공백, 백스페이스 문자, 그리고 , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > % 등의 금지 문자가 들어갈 수 없습니다.

   - **파일에서 기기 가져오기** 버튼을 눌러 .txt 파일에서 기기 목록을 가져옵니다. 각 기기 주소 또는 이름은 별도의 줄에 지정해야 합니다.

     파일에는 공백, 백스페이스 문자, 그리고 , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > % 등의 금지 문자가 들어갈 수 없습니다.

6. 관리 그룹에 추가할 기기 목록을 봅니다. 기기를 추가하거나 제거하여 목록을 편집할 수 있습니다.
7. 목록이 올바른지 확인한 후 **다음** 버튼을 누릅니다.

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 이동

한 관리 그룹에서 다른 관리 그룹으로 또는 미할당 기기 그룹에서 관리 그룹으로 기기를 이동할 수 있습니다.

선택한 관리 그룹으로 두 대 이상의 기기를 이동하려면 다음 단계를 따릅니다.

1. 기기를 이동할 관리 그룹을 엽니다. 이렇게 하려면 다음 중 하나를 수행하십시오.
   - 관리 그룹을 열려면 **기기 → 관리 중인 기기**로 이동하여 **현재 경로** 필드에서 경로 링크를 클릭한 다음, 열리는 왼쪽 창에서 관리 그룹을 선택합니다.
   - **미할당 기기** 그룹을 열려면 **발견 및 배포 → 미할당 기기**로 이동합니다.
2. 다른 그룹으로 이동하려는 기기 옆에 있는 확인란을 선택합니다.
3. **소속 그룹 변경** 버튼을 클릭합니다.
4. 관리 그룹의 계층 구조에서 선택한 기기를 이동할 관리 그룹 옆의 확인란을 선택합니다.
5. **이동** 버튼을 누릅니다.

선택한 기기가 선택한 관리 그룹으로 이동됩니다.

클라이언트 기기의 중앙 관리 서버 변경

특정 클라이언트 장치에 대해 중앙 관리 서버를 다른 서버로 변경할 수 있습니다. 이를 위해 *중앙 관리 서버 변경*작업을 사용합니다.

클라이언트 기기를 관리하는 중앙 관리 서버를 다른 서버로 변경하려면 다음과 같이 하십시오:

1. 기기를 관리하는 중앙 관리 서버에 연결합니다.
2. 중앙 관리 서버 변경 작업을 생성합니다.

   작업 추가 마법사가 시작됩니다. 마법사의 지침을 따릅니다. 작업 추가 마법사의 **새 작업** 창에서 **Kaspersky Security Center 14** 애플리케이션을 선택하고 **중앙 관리 서버 변경** 작업 유형을 선택합니다. 그 다음 중앙 관리 서버를 변경하려는 장치를 지정합니다.

   - **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.

   - **기기 주소를 직접 지정하거나 주소 목록에서 가져오기**

     작업을 할당할 장치의 DNS 이름, IP 주소, 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 조회 결과에 작업 할당**

     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.

3. 만들어진 작업을 실행합니다.

작업이 완료되면 작업이 만들어진 클라이언트 기기가 작업 설정에 지정된 중앙 관리 서버의 관리를 받게 됩니다.

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 **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 7일입니다.
     기본적으로 이 옵션은 켜져 있습니다.

6. **저장**을 누릅니다.

   변경 내용이 저장 및 적용됩니다.

기기 상태 정보

Kaspersky Security Center Linux는 관리 중인 장치마다 상태를 할당합니다. 특정 상태는 사용자가 정의한 조건이 충족되는지 여부에 따라 달라집니다. 장치에 상태를 할당할 때 Kaspersky Security Center Linux가 네트워크에 있는 장치의 가시성 플래그를 고려할 때도 있습니다(아래 표 참조). Kaspersky Security Center Linux에서 2시간 내에 네트워크의 장치를 찾지 못하면 장치의 가시성 플래그가 *확인되지 않음*으로 설정됩니다.

상태는 다음과 같습니다.

- *심각*또는 *심각/존재 확인*
- *경고*또는 *경고/존재 확인*
- *정상*또는 *정상/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.
너무 많은 바이러스가 탐지됨	바이러스 검사 작업 등의 바이러스 탐지를 위한 작업을 통해 기기에서 일부 바이러스가 발견되었는데 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 바이러스 검사를 수행 안 함	장치가 네트워크에 표시되며 보안 제품이 장치에 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
재부팅 필요	기기가 네트워크에 표시되지만 선택한 이유 중 하나로 인해 애플리케이션이 지정된 시간 간격보다 오랫동안 기기 다시 시작을 요구합니다.	0분 이상
비-호환 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.
만료된 라이센스	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.	0일 이상
처리 안 된 인시던트가 있음	기기에서 처리되지 않은 일부 인시던트가 발견되었습니다. 인시던트는 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션을 통해 자동으로 또는 수동으로 관리자에 의해 생성될 수 있습니다.	• 토글 버튼이 꺼져 있

		습니다. • 토글 버튼이 켜져 있습니다.
애플리케이션에서 정의된 기기 상태	관리 애플리케이션이 기기 상태를 정의합니다.	• 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 연결 끊김	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.	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 Center Linux에서는 지정한 조건 충족 시 관리 그룹의 장치 상태를 자동 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 **7일 이상**이면 클라이언트 기기에 *경고* 상태가 할당되고 값이 **7일 이상이면** *심각* 상태가 할당됩니다.

Kaspersky Security Center Linux를 이전 버전에서 업그레이드하면, *심각* 또는 *경고* 상태 할당을 위한 **데이터베이스가 오래됨** 조건 값이 변경되지 않습니다.

Kaspersky Security Center Linux에서 장치에 상태를 할당할 때, 몇 가지 조건(조건 설명 열 참조)에서 가시성 플래그를 고려합니다. 예를 들어, 데이터베이스가 오래됨 조건이 충족되어서 관리 중인 기기에 *심각* 상태가 할당되었고 나중에 기기의 가시성 플래그가 설정되었다면 기기에는 *확인* 상태가 할당됩니다.

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 **심각으로 지정** 섹션에서 목록의 조건 옆에 있는 확인란을 선택합니다.

   부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

4. 선택한 조건에 필요한 값을 설정합니다.
   모든 조건이 아닌 일부 조건에 대하여 값을 설정할 수 있습니다.
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 **경고로 지정** 섹션에서 목록의 조건 옆에 있는 확인란을 선택합니다.

   부모 정책에서 잠금 상태가 아닌 설정만 변경할 수 있습니다.

4. 선택한 조건에 필요한 값을 설정합니다.
   모든 조건이 아닌 일부 조건에 대하여 값을 설정할 수 있습니다.
5. **확인**를 누릅니다.

지정한 조건이 충족되면 관리 중인 기기에 *경고* 상태가 할당됩니다.

정책 및 정책 프로필

Kaspersky Security Center 14 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:

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.
- 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 조건 발생 시 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
🔓 정의안됨	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.

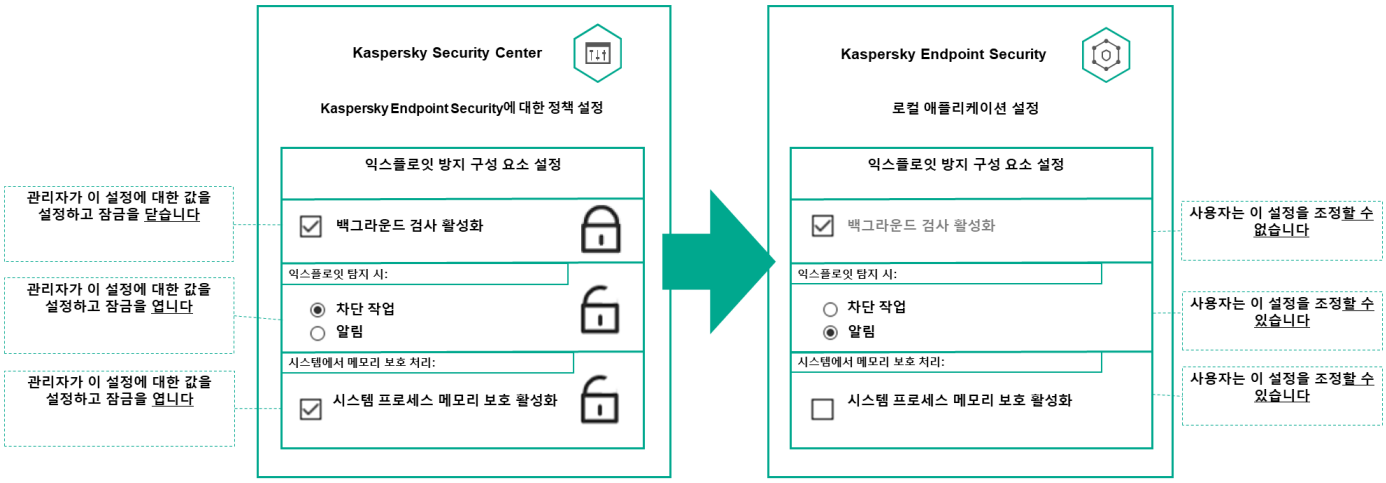
- 관리 하위 그룹 정책에 대한 잠금 설정
- 관리 중인 기기에서 Kaspersky 애플리케이션 잠금 설정

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

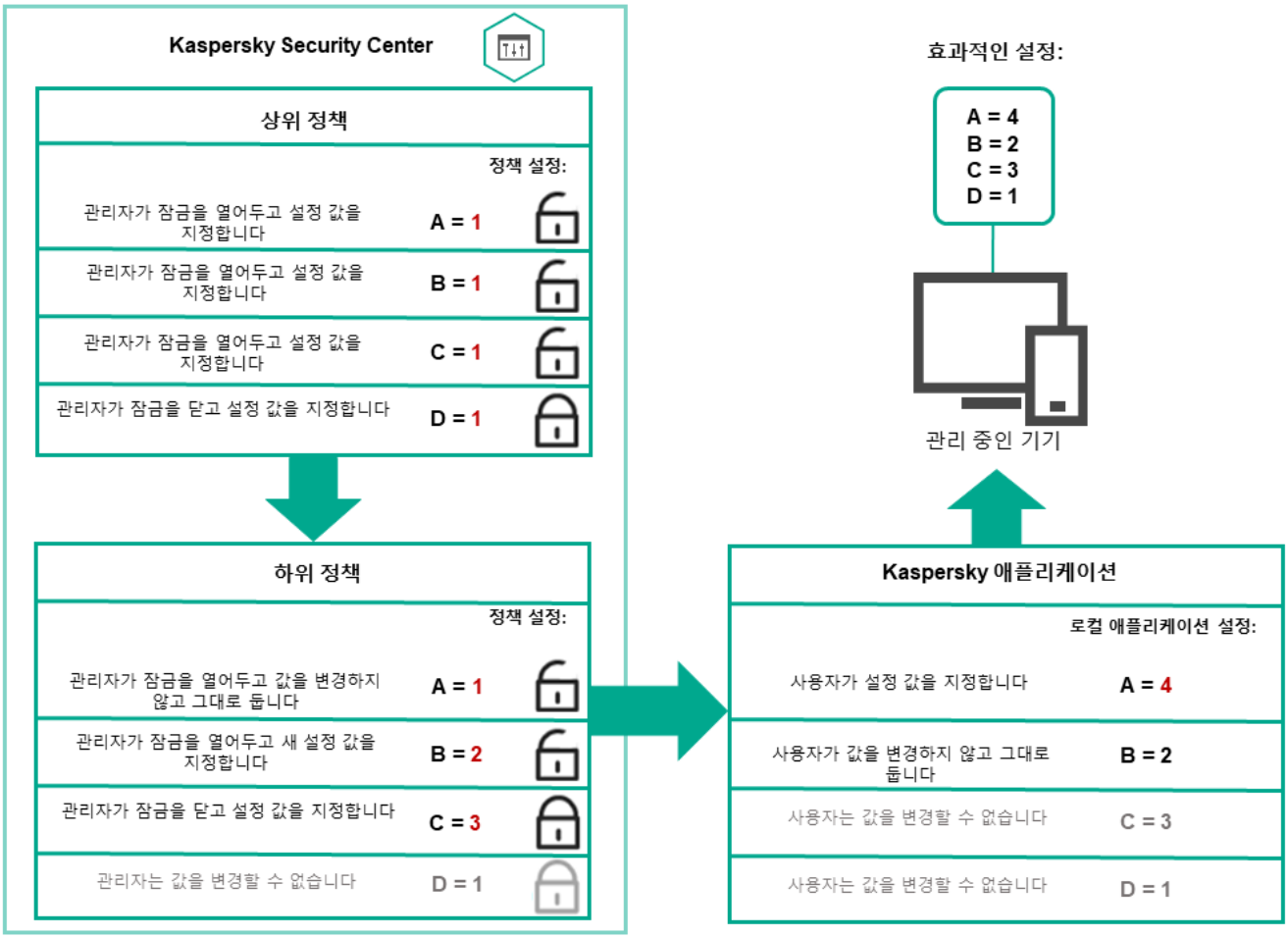
기기마다 다른 설정이 필요한 경우 기기를 관리 그룹으로 구성할 수 있습니다.

단일 관리 그룹에 대한 정책을 지정할 수 있습니다. 정책 설정은 *상속될 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).

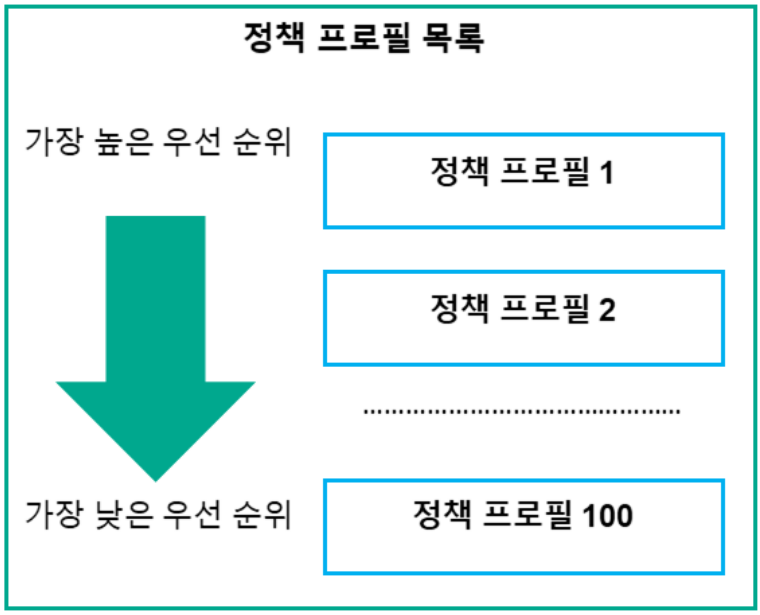


정책 계층 구조

정책 계층 구조의 정책 프로필

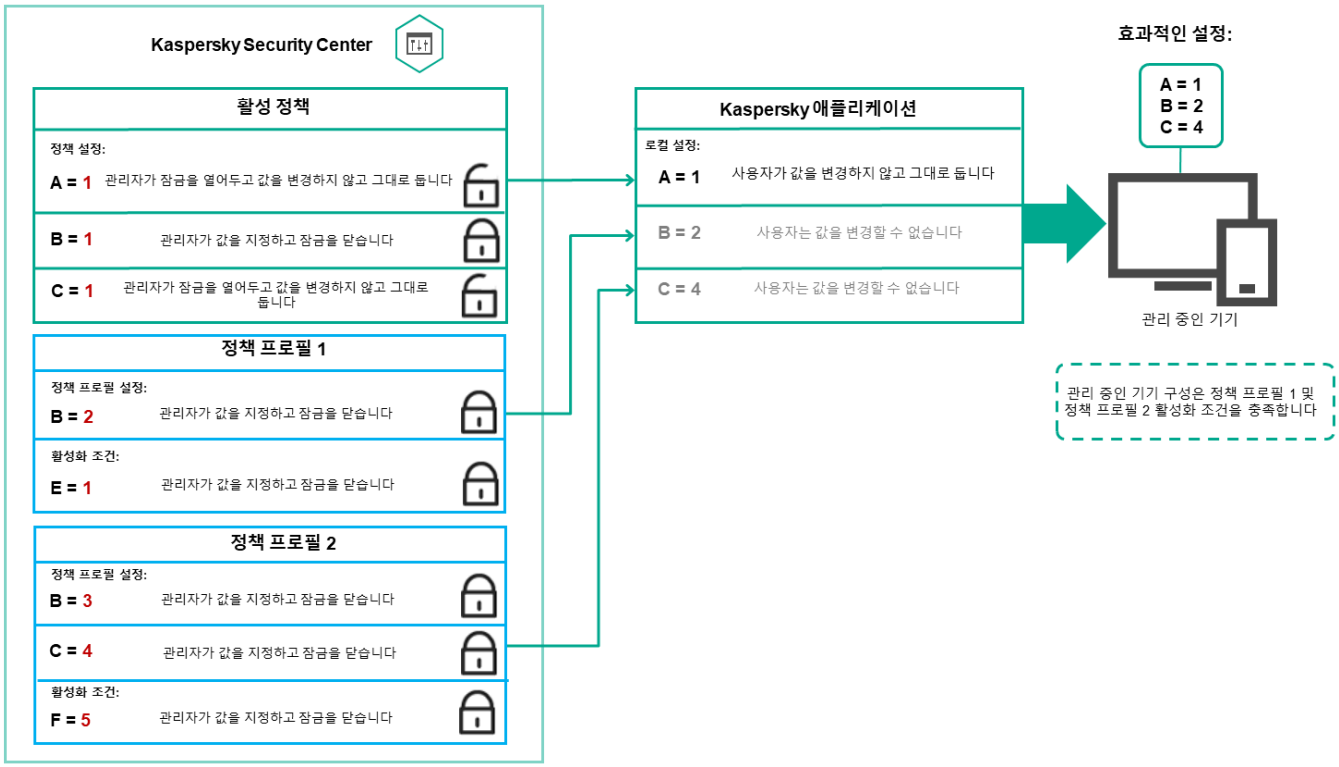
정책 프로필에는 다음과 같은 우선 순위 할당 조건이 있습니다.

- 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).

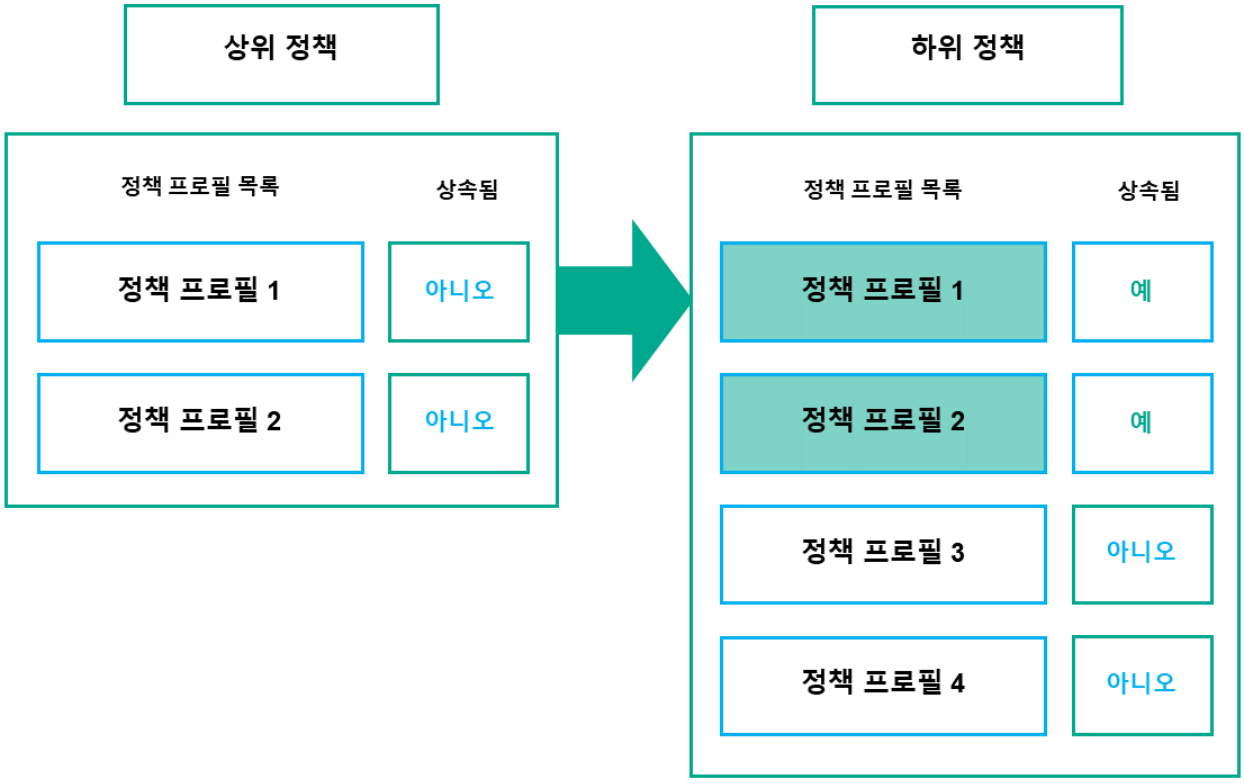


관리 중인 기기 구성은 여러 정책 프로필의 활성화 조건을 충족합니다.

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).

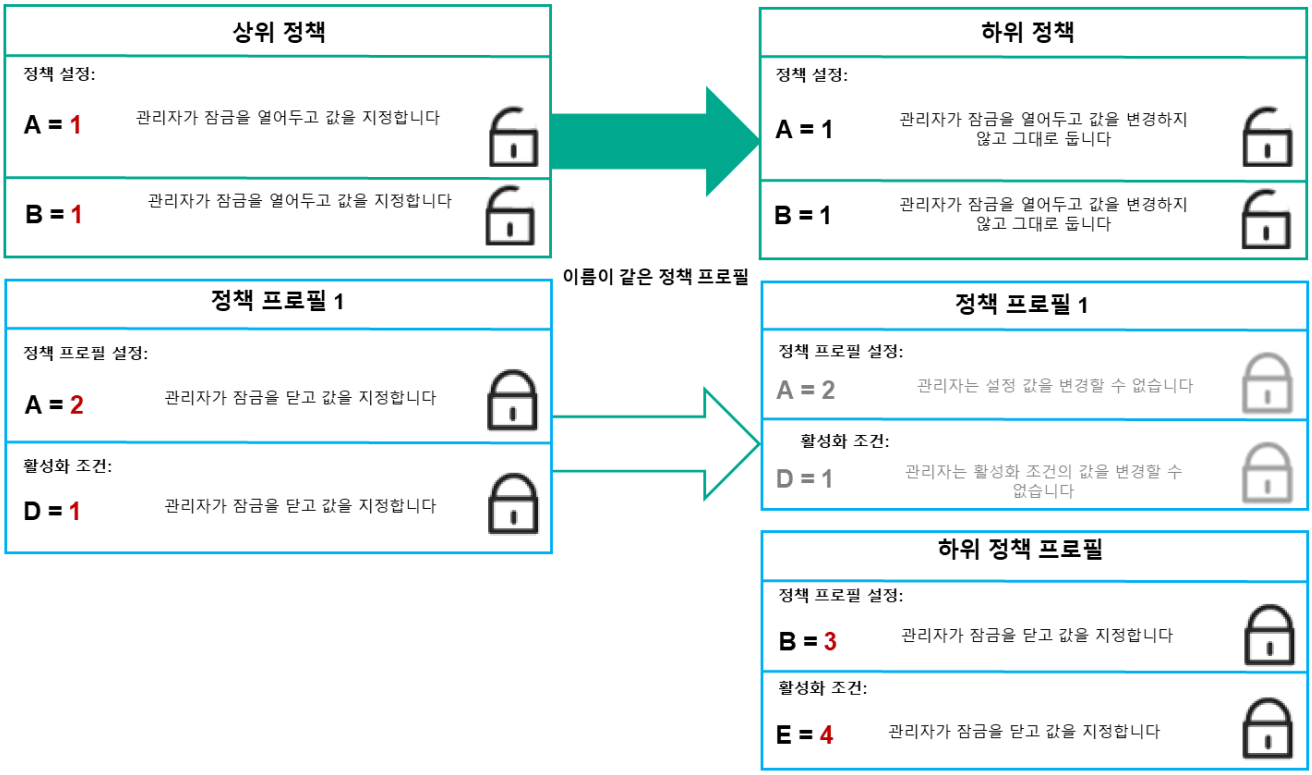


정책 프로필 상속

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 **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. **기기 → 정책 및 프로필**로 이동합니다.
2. **추가**를 누릅니다.
   애플리케이션 선택 창이 열립니다.
3. 정책을 생성할 애플리케이션을 선택합니다.
4. **다음**을 누릅니다.
   일반 탭이 선택된 상태로 새 정책 설정 창이 열립니다.
5. 원하는 경우 정책의 기본 이름, 기본 상태 및 기본 상속 설정을 변경합니다.
6. **애플리케이션 설정** 탭을 누릅니다.
   또는 **저장**을 누르고 종료할 수도 있습니다. 정책이 정책 목록에 표시되며, 나중에 정책 설정을 편집할 수 있습니다.
7. **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 Linux 도움말

   다른 보안 제품 설정에 대한 자세한 내용은 해당 애플리케이션에 대한 문서를 참조하십시오.
   설정을 편집할 때는 **취소**를 눌러 마지막 작업을 취소할 수 있습니다.
8. **저장**을 눌러 정책을 저장합니다.

정책 목록에 정책이 표시됩니다.

일반 정책 설정

모두 펼치기 | 모두 접기

일반

일반 탭에서 정책 상태를 수정하고 정책 설정에 대한 상속을 지정할 수 있습니다.

- **정책 상태** 차단에서 정책 모드 중 하나를 선택할 수 있습니다:
  - **활성**

    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.
    이 옵션은 기본적으로 활성화되어 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 수정

정책을 수정하려면 다음 단계를 따릅니다.

1. **기기 → 정책 및 프로필**로 갑니다.
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 Linux 도움말

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.

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 **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 **활성**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.

다른 관리 그룹으로 정책을 이동하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **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 **활성**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 **활성**으로 변경할 수 있습니다.

새로 이동한 정책과 이름이 동일한 정책이 이미 대상 그룹에 있는 경우 가져온 정책의 이름에 (<순차적 번호>) 색인이 추가됩니다. 예: (1).

강제 동기화

Kaspersky Security Center Linux가 관리 중인 장치의 상태, 설정, 작업, 정책을 자동으로 동기화하지만, 때로는 특정 장치에 대해 동기화가 이미 진행되었는지 관리자가 확인해야 합니다.

단일 기기 동기화

중앙 관리 서버와 관리 중인 기기 간의 강제 동기화를 수행하려면 다음 단계를 따릅니다.

1. **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 **기기 → 관리 중인 기기**로 이동하고 관리 장치 목록 위의 **현재 경로** 필드에서 경로 링크를 클릭한 다음 동기화할 장치가 포함된 관리 그룹을 선택합니다.

   - 기기 목록을 보려면 기기 조회를 실행합니다.

2. 중앙 관리 서버와 동기화하려는 기기 옆의 확인란을 선택합니다.

3. 관리 장치 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. **기기 → 관리 중인 기기**로 이동합니다.

2. 중앙 관리 서버와 동기화할 기기의 이름을 누릅니다.
일반 섹션이 선택된 상태로 속성 창이 열립니다.

3. **애플리케이션** 탭을 클릭합니다.

4. 정책 동기화 날짜를 확인할 애플리케이션을 선택합니다.

일반 섹션이 선택되어 있고 정책 전달 날짜와 시간이 표시된 애플리케이션 정책 창이 열립니다.

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. **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. 도구 모음의 **인터페이스 옵션** 섹션으로 이동합니다.
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 **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 우선순위 변경, 정책 프로필 생성, 정책 프로필 복사, 정책 프로필 활성화 규칙 생성, 정책 프로필 삭제에 대해 설명합니다.

정책 프로필 보기

정책의 프로필을 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **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 프로필의 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 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 Linux 내부 보안 그룹의 소유자에 따라 장치에 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 Center Linux의 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. 장치의 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. 장치의 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 활성화하려면 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 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.

  - **지정된 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.

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 **만들기**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.

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 그룹 계층 구조의 모든 레벨에서 사용자 세트 또는 보안 그룹 세트에 역할을 할당할 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.

애플리케이션 기능에 대한 접근 권한 구성. 역할 기반 접근 제어

Kaspersky Security Center Linux는 Kaspersky Security Center Linux 및 관리 중인 Kaspersky 애플리케이션 기능에 대한 역할 기반 접근을 위한 기능을 제공합니다.

다음 방법의 하나로 Kaspersky Security Center Linux 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 Linux 기능을 보여줍니다.

표에 나열된 사용자 작업을 수행하려면 사용자는 작업 옆에 지정된 권한이 있어야 합니다.

읽기, **수정** 및 **실행** 권한은 모든 작업, 리포트 또는 설정에 적용됩니다. 이러한 권한 외에도 사용자는 작업, 리포트 또는 기기 조회에 대한 설정을 관리하려면 **기기 조회에 대한 작업 수행** 권한이 있어야 합니다.

테이블에 누락 된 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 매니지먼트	**수정**	• 관리 그룹에 기기 추가: **수정** • 관리 그룹에서 기기 삭제: **수정** • 다른 관리 그룹에 관리 그룹 추가: **수정** • 다른 관리 그룹에서 관리 그룹 삭제: **수정**	없음	없음	없음
일반 기능: ACL에 상관없이 개체 접근	**읽기**	모든 개체에 대한 읽기 권한 얻기: **읽기**	없음	없음	없음
일반 기능: 기본 기능	• **읽기** • **수정** • **실행** • **기기 조회에 대한 동작 수행**	• 가상 서버에 대한 기기 이동 규칙(생성, 수정 또는 삭제): **수정**, **기기 조회에 대한 작업 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: **수정** • 그룹 접근 제어 목록 보기: **읽기** • Kaspersky 이벤트 로그 보기: **읽기**	• "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 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" • "금지한 애플리케이션에 대한 리포트" • "웹 제어 리포트"	없음

				• "유효한 사용자 권한에 대한 리포트" • "권한 리포트"	
일반 기능: **삭제된 개체**	• **읽기** • **수정**	• 휴지통에서 삭제된 개체 보기: **읽기** • 휴지통에서 개체 삭제: **수정**	없음	없음	없음
일반 기능: **이벤트 처리**	• **이벤트 삭제** • **이벤트 알림 설정 편집** • **이벤트 로그 기록 설정 편집** • **수정**	• 이벤트 등록 설정 변경: **이벤트 로깅 설정 편집** • 이벤트 알림 설정 변경: **이벤트 알림 설정 편집** • 이벤트 삭제: **이벤트 삭제**	없음	없음	설정: • 데이터베이스에 저장되는 최대 이벤트 수 • 삭제된 기기에서 이벤트를 저장하는 기간
일반 기능: **중앙 관리 서버의 작업**	• **읽기** • **수정** • **실행** • **개체 ACL 수정** • **기기 조회에 대한 동작 수행**	• 네트워크 에이전트 연결을 위한 중앙 관리 서버의 포트 지정: **수정** • 중앙 관리 서버에 실행된 활성화 프록시의 포트 지정: **수정** • 중앙 관리 서버에 실행된 모바일용 활성화 프록시의 포트 지정: **수정** • 독립형 패키지 배포를 위한 웹 서버의 포트 지정: **수정** • MDM 프로필 배포를 위한 웹 서버의 포트 지정: **수정** • 콘솔을 통한 연결을 위한 중앙 관리 서버의 SSL 포트 지정: **수정** • 모바일 연결을 위한 중앙 관리 서버의 포트 지정: **수정** • 중앙 관리 서버 데이터베이스에 저장되는 최대 이벤트 수 변경: **수정** • 중앙 관리 서버에서 보낼 수 있는 최대 이벤트 수 지정: **수정** • 중앙 관리 서버에서 이벤트를 보낼 수 있는 기간 지정: **수정**	• "중앙 관리 서버 데이터 백업" • "데이터베이스 점검"	없음	없음
일반 기능: **보호 배포**	• **Kaspersky 패치 관리** • **읽기** • **수정** • **실행** • **기기 조회에 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: 키 매니지먼트	• **키 파일 내보내기** • **수정**	• 키 파일 내보내기: **키 파일 내보내기** • 중앙 관리 서버 라이센스 키 설정 수정: **수정**	없음	없음	없음
일반 기능: 강제 리포트 매니지먼트	• **읽기** • **수정**	• ACL에 상관없이 리포트 생성: **쓰기** • ACL에 상관없이 리포트 실행: **읽기**	없음	없음	없음
일반 기능: 중앙 관리 서버의 계층 구조	**중앙 관리 서버 계층 구조 구성**	• 보조 중앙 관리 서버 등록, 업데이트 또는 삭제: **중앙 관리 서버의 계층 구조 구성**	없음	없음	없음
일반 기능: 사용자 권한	**개체 ACL 수정**	• 모든 객체의 보안 속성 변경: **객체 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** • **수정** • **실행** • **기기 조회에 대한 동작 수행**	• 가상 중앙 관리 서버 목록 가져오기: **읽기** • 가상 중앙 관리 서버에 대한 정보 얻기: **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	없음	없음

사전 정의된 사용자 역할

Kaspersky Security Center Linux 사용자에게 할당된 사용자 역할은 사용자에게 애플리케이션 기능에 대한 접근 권한 세트를 제공합니다.

이미 구성된 권한 세트로 사전 정의된 사용자 역할을 사용하거나 새로운 역할을 만들고 필요한 권한을 직접 구성할 수 있습니다. Kaspersky Security Center Linux에서 사용할 수 있는 사전 정의된 일부 사용자 역할은 **감사관**, **보안 책임자**, **감독관** 등 특정 직책과 연관될 수 있습니다. 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	모든 리포트 유형을 사용한 모든 작업과 삭제된 개체 보기를 포함한 모든 보기 작업이 허용됩니다(**삭제된 개체** 영역에서 **읽기** 및 **쓰기** 권한이 부여됨). 다른 작업은 허용되지 않습니다. 조직 감사를 수행하는 사용자에게 이 역할을 할당할 수 있습니다.
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.

Kaspersky Security Center Linux에서는 기능 영역의 **모바일 장치 관리: 일반** 및 **시스템 관리** 기능을 사용할 수 없습니다. **취약점 및 패치 매니지먼트/운영자** 및 **모바일 장치 매니지먼트 관리자/운영자** 역할을 가진 사용자는 **일반 기능**: **기본** 기능 영역의 권한에만 액세스할 수 있습니다.

미리 정의된 사용자 역할의 접근 권한

역할	설명
중앙 관리 서버 관리자	**일반 기능**의 다음 기능 영역에서 모든 작업을 허용합니다. • **기본 기능** • **이벤트 처리** • **중앙 관리 서버 계층 구조** • **가상 중앙 관리 서버**
중앙 관리 서버 운영자	**일반 기능**의 다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다. • **기본 기능** • **가상 중앙 관리 서버**
감사관	**일반 기능**의 다음 기능 영역에서 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **삭제된 개체** • **강제 리포트 관리** 조직 감사를 수행하는 사용자에게 이 역할을 할당할 수 있습니다.
설치 관리자	**일반 기능**의 다음 기능 영역에서 모든 작업을 허용합니다. • **기본 기능** • **Kaspersky 소프트웨어 배포** • **라이센스 키 관리** **일반 기능: 가상 중앙 관리 서버** 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다.
설치 운영자	**일반 기능**의 다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다. • **기본 기능** • **보호 배포**(이 영역에 **Kaspersky Lab 패치 관리** 권한도 부여) • **가상 중앙 관리 서버**
Kaspersky Endpoint Security 관리자	다음 기능 영역의 모든 작업을 허용합니다. • **일반 기능: 기본 기능** • Kaspersky Endpoint Security 영역(모든 기능 포함)
Kaspersky Endpoint Security 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다. • **일반 기능: 기본 기능** • Kaspersky Endpoint Security 영역(모든 기능 포함)
메인 관리자	**일반 기능**에서 다음 영역을 *제외한* 기능 영역의 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **강제 리포트 관리**
메인 운영자	다음 모든 기능 영역에 **읽기** 및 **실행** 권한을 부여합니다(해당하는 경우). • **일반 기능**: • **기본 기능**

- **삭제된 개체**
- **중앙 관리 서버에서의 동작**
- **Kaspersky Lab 소프트웨어 배포**
- **가상 중앙 관리 서버**
- Kaspersky Endpoint Security 영역(모든 기능 포함)

모바일 기기 매니지먼트 관리자	**일반 기능: 기본 기능** 기능 영역에서 모든 작업을 허용합니다.
보안 운영자	**일반 기능**의 다음 기능 영역에서 모든 작업을 허용합니다. • **ACL에 상관없이 개체 접근** • **강제 리포트 관리** **시스템 매니지먼트: 연결성** 기능 영역에 **읽기**, **수정**, **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 매니지먼트: 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 매니지먼트** 기능 영역에 **읽기** 권한을 부여합니다. 조직의 IT 보안을 담당하는 보안 책임자 및 기타 관리자에게 이 역할을 할당할 수 있습니다.

내부 사용자의 계정 추가

Kaspersky Security Center Linux에 새 내부 사용자 계정을 추가하려면:

1. 메인 메뉴에서 **사용자 및 역할 → 사용자**로 이동합니다.
2. **추가**를 누릅니다.
3. **새 항목** 창이 열리면 새 사용자 계정의 설정을 지정합니다.
   - 기본 옵션인 **사용자**를 그대로 유지합니다.
   - **이름**.
   - Kaspersky Security Center Linux에 사용자를 연결하기 위한 **암호**.
     암호는 다음 규칙을 따라야 합니다:
     - 암호는 8자에서 16자 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 문자를 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. 암호 변경으로만 해당 사용자 계정을 잠금 해제할 수 있습니다.

- **전체 이름**
- **설명**
- **이메일 주소**
- **전화**

4. **확인**을 눌러 변경을 저장합니다.

새 사용자 계정이 사용자 및 사용자 그룹 목록에 표시됩니다.

사용자 그룹 생성

사용자 그룹을 생성하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. **추가**를 누릅니다.
3. **새 항목** 창이 열리면 **그룹**을 선택합니다.
4. 새 사용자 그룹에 대해 다음 설정을 지정합니다.
   - **그룹 이름**
   - **설명**
5. **확인**을 눌러 변경을 저장합니다.

새 사용자 그룹이 사용자 및 사용자 그룹 목록에 표시됩니다.

내부 사용자의 계정 편집

Kaspersky Security Center Linux에서 내부 사용자 계정을 편집하려면:

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. 편집할 사용자 계정의 이름을 누릅니다.
3. 사용자 설정 창이 열리면 **일반** 탭에서 사용자 계정의 설정을 변경합니다.
   - **설명**
   - **전체 이름**
   - **이메일 주소**
   - **메인 전화**
   - Kaspersky Security Center Linux에 사용자를 연결하기 위한 **암호**.
     암호는 다음 규칙을 따라야 합니다:
     - 암호는 8자에서 16자 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. 허용된 시도 횟수는 변경할 수 있지만, 횟수를 줄이는 것은 보안상의 이유로 권장하지 않습니다. 지정한 암호 입력 시도 횟수를 초과하면, 해당 사용자 계정은 1시간 동안 차단됩니다. 암호 변경으로만 해당 사용자 계정을 잠금 해제할 수 있습니다.

- 필요한 경우 토글 버튼을 **비활성됨**으로 전환하여 사용자의 애플리케이션 연결을 차단합니다. 예를 들어 직원이 퇴사한 후에 계정을 비활성화할 수 있습니다.

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. **저장**을 눌러 변경 사항을 저장합니다.

업데이트된 사용자 계정이 사용자 및 보안 그룹 목록에 표시됩니다.

사용자 그룹 편집

내부 그룹만 편집할 수 있습니다.

사용자 그룹을 편집하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. 편집할 사용자 그룹의 이름을 누릅니다.
3. 그룹 설정 창이 열리면 사용자 그룹의 설정을 변경합니다.
   - **이름**
   - **설명**
4. **저장**을 눌러 변경 사항을 저장합니다.

업데이트된 사용자 그룹이 사용자 및 사용자 그룹 목록에 표시됩니다.

내부 그룹에 사용자 계정 추가

내부 그룹에는 내부 사용자의 계정만 추가할 수 있습니다.

내부 그룹에 사용자 계정을 추가하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. 그룹에 추가할 사용자 계정 옆의 확인란을 선택합니다.
3. **그룹 할당** 버튼을 누릅니다.
4. **그룹 할당** 창이 열리면 사용자 계정을 추가할 그룹을 선택합니다.
5. **할당** 버튼을 누릅니다.

사용자 계정이 해당 그룹에 추가됩니다.

기기 소유자로 특정 사용자 지정

사용자를 모바일 장치 소유자로 지정하는 방법은 Kaspersky Security for Mobile 도움말 을 참조하십시오.

기기 소유자로 특정 사용자를 지정하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할 → 사용자**로 이동합니다.
2. 기기 소유자로 지정할 사용자 계정의 이름을 누릅니다.
3. 사용자 설정 창이 열리면 **기기** 탭을 누릅니다.
4. **추가**를 누릅니다.
5. 기기 목록에서 사용자에게 할당할 기기를 선택합니다.
6. **확인**를 누릅니다.

선택한 기기가 사용자에게 할당된 기기 목록에 추가됩니다.

기기 → 관리 중인 기기에서 할당할 기기 이름을 누른 다음 기기 소유자 관리 **기기 소유자 관리** 링크를 눌러 같은 작업을 수행할 수 있습니다.

사용자 또는 보안 그룹 삭제

내부 사용자 또는 내부 보안 그룹만 삭제할 수 있습니다.

사용자 또는 보안 그룹을 삭제하려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **사용자 및 역할 → 사용자**로 이동합니다.
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 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.
   - **액세스 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.
- **액세스 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. 메인 메뉴에서 **사용자 및 역할** → **사용자**로 이동합니다.
2. 사용자 역할 범위에 추가할 사용자 및 보안 그룹 옆의 확인란을 선택합니다.
3. **역할 할당** 버튼을 누릅니다.
   역할 할당 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
4. 마법사의 **역할 선택** 페이지에서 할당할 사용자 역할을 선택합니다.
5. 마법사의 **범위 정의** 페이지에서 사용자 역할 범위에 추가할 관리 그룹을 선택합니다.
6. **역할 할당** 버튼을 눌러 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. 마법사의 **범위 정의** 페이지에서 사용자 역할 범위에 추가할 관리 그룹을 선택합니다.
6. 마법사의 **사용자 선택** 페이지에서 사용자 역할 범위에 추가할 사용자 및 보안 그룹을 선택합니다.
7. **역할 할당** 버튼을 눌러 마법사를 닫습니다.
8. 역할 속성 창을 닫습니다.

선택한 사용자 또는 보안 그룹과 선택한 관리 그룹이 사용자 역할의 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.

개체 리비전 관리

이 섹션에는 개체 리비전 관리에 대한 정보가 포함되어 있습니다. Kaspersky Security Center Linux에서는 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
- 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 설정에 대한 변경 내용과 관련된 리비전 설명
  기본적으로 개체 리비전 설명은 비어 있습니다. 리비전에 설명을 추가하려면 관련 리비전을 선택하고 **설명** 버튼을 누릅니다. **개체 리비전 설명** 창에서 리비전에 대한 설명을 추가할 수 있습니다.

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 설정에 대한 변경 내용과 관련된 리비전 설명

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.

개체 삭제

이 섹션에서는 개체를 삭제하는 방법과 삭제된 개체에 대한 정보를 확인하는 방법을 설명합니다.

다음과 같은 개체를 삭제할 수 있습니다:

- 정책
- 작업
- 설치 패키지
- 가상 중앙 관리 서버
- 사용자
- 보안 그룹
- 관리 그룹

개체를 삭제해도 개체에 대한 정보는 데이터베이스에 유지됩니다. 삭제된 개체 관련 정보의 저장 기간은 개체 리비전의 저장 기간과 같습니다(권장 저장 기간은 90일입니다). **삭제된 개체** 권한 영역에서 **수정** 권한이 있어야 저장 기간을 변경할 수 있습니다.

Klscflag 유틸리티를 사용하여 포트 13291 열기

중앙 관리 서버의 포트 13291은 중앙 관리 콘솔(MMC 기반 관리 콘솔 포함)에서 연결을 수신하는 데 사용됩니다. Windows가 아닌 컴퓨터에서는 이 포트가 기본적으로 닫혀있습니다.

MMC 기반 중앙 관리 콘솔에 대한 연결을 허용하거나 klakaut 유틸리티를 사용하려면, klscflag 유틸리티를 사용하여 이 포트를 열 수 있습니다. MMC 기반 중앙 관리 콘솔이 Kaspersky Security Center에 연결되면 기능이 저하될 수 있습니다.

klscflag 유틸리티는 KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN 매개변수의 값을 변경합니다.

> 웹 콘솔을 사용하여 Kaspersky Security Center에 연결하는 것을 권장합니다.

포트 13291을 열려면:

1. 명령줄에서 다음 명령을 실행합니다.
   ```
   $ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```
2. 다음 명령을 실행하여 Kaspersky Security Center 중앙 관리 서버 서비스를 다시 시작하십시오.
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

   포트 13291이 열립니다.

포트 13291이 성공적으로 열렸는지 확인하려면:

명령줄에서 다음 명령을 실행합니다.

```
$ /opt/kaspersky/ksc64/sbin/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)true
```

`true` 값은 포트가 열렸다는 의미입니다. 그렇지 않으면 `false` 값이 표시됩니다.

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

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.

- Kaspersky Security Center Linux 구성 요소 및 보안 애플리케이션 등 최신 Kaspersky 소프트웨어로 네트워크를 보호합니다.
- 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 않았다면, Kaspersky 데이터베이스 및 소프트웨어 모듈을 수동으로 업데이트하거나 Kaspersky 업데이트 서버에서 직접 업데이트 하는 것을 고려하십시오.

중앙 관리 서버는 인터넷에 연결되어 있어야 합니다.

시작하기 전에 다음을 수행했는지 확인하십시오:

1. Kaspersky 보안 제품을 Kaspersky Security Center 14 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 않은 경우 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: 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: 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.

5 diff 파일을 사용하여 업데이트 프로세스 최적화(선택 사항)

diff 파일을 사용하여 중앙 관리 서버와 관리 중인 장치 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 저장소 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 diff 파일 사용

6 보안 제품에 대한 업데이트 자동 설치 구성

관리 중인 애플리케이션에 대한 *업데이트* 작업을 생성하여 안티 바이러스 데이터베이스를 포함한 소프트웨어 모듈 및 Kaspersky 데이터베이스에 대한 업데이트를 적시에 제공할 수 있습니다. 업데이트를 적시에 제공하려면 작업 스케줄 구성 시 **새로운 저장소 업데이트 다운로드를 완료한 후** 옵션을 선택합니다.

네트워크에 IPv6 전용 장치가 있고 이 장치에 설치된 보안 제품을 정기적으로 업데이트하려면, 관리 중인 장치에 중앙 관리 서버 버전 13.2와 네트워크 에이전트 버전 13.2를 설치해야 합니다.

업데이트를 위해 최종 사용자 라이센스 계약서 약관을 검토하고 동의해야 하는 경우 먼저 약관에 동의해야 합니다. 그런 다음 업데이트를 관리 중인 기기로 배포할 수 있습니다.

결과

시나리오가 완료되면 업데이트를 중앙 관리 서버의 저장소에 다운로드한 후 Kaspersky Security Center Linux가 Kaspersky 데이터베이스를 업데이트하도록 구성됩니다. 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 액세스할 수 없는 경우 애플리케이션이 공용 DNS를 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 Center 는 Kaspersky 애플리케이션을 자동으로 업데이트할 수 없습니다. 애플리케이션을 업데이트하려면 Kaspersky 웹사이트에서 최신 버전의 애플리케이션 버전을 다운로드한 다음 수동으로 설치하십시오.

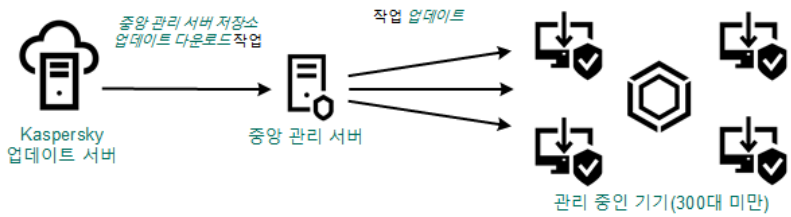
  - Kaspersky Security Center 중앙 관리 서버, Kaspersky Security Center 14 웹 콘솔
  - 네트워크 에이전트, Kaspersky Endpoint Security for Linux, 관리 웹 플러그인

네트워크의 구성에 따라 다음과 같은 체계를 사용하여 필요한 업데이트를 관리 중인 기기로 다운로드하고 배포할 수 있습니다:

- 단일 작업 사용: *중앙 관리 서버 저장소 업데이트 다운로드*
- 2개의 작업 사용:
  - *중앙 관리 서버 저장소 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 Security for Linux로 직접 업데이트
- 중앙 관리 서버에 인터넷 연결이 없을 시, 로컬 또는 네트워크 폴더를 통해

중앙 관리 서버 저장소 업데이트 다운로드 작업 사용

이 구성에서 Kaspersky Security Center는 *중앙 관리 서버 저장소 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).



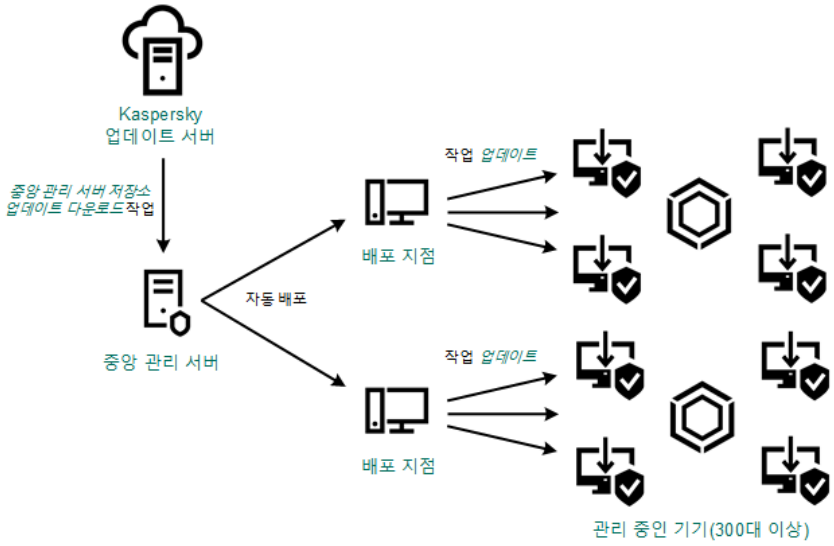
배포 지점이 없는 중앙 관리 서버 저장소 업데이트 다운로드 작업을 사용하여 업데이트

Kaspersky 업데이트 서버와 로컬 또는 네트워크 폴더는 업데이트 경로로 사용할 수 없습니다.

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 관리 중인 장치가 300대 이상이거나, 각 네트워크 세그먼트에 관리 중인 장치가 9대 이상인 다중 네트워크 구성에서는, 배포 지점을 사용하여 관리 중인 장치로 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 저장소 업데이트 다운로드 작업을 사용하여 업데이트

중앙 관리 서버 저장소 업데이트 다운로드 작업이 완료되면 Kaspersky Endpoint Security for Linux용 Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트가 중앙 관리 서버 저장소로 다운로드됩니다. 이러한 업데이트는 Kaspersky Endpoint Security for Linux 업데이트 작업을 통해 설치됩니다.

가상 중앙 관리 서버에서는 중앙 관리 서버 저장소 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.

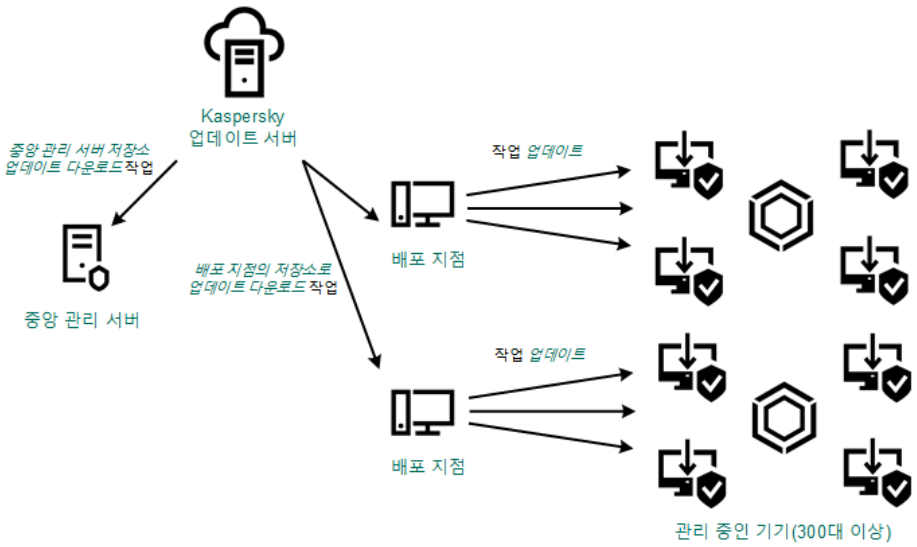
각 Kaspersky 애플리케이션은 중앙 관리 서버에서 필요한 업데이트를 요청합니다. 중앙 관리 서버는 이러한 요청을 집계하여 애플리케이션에 필요한 업데이트만 다운로드합니다. 그러므로 같은 업데이트가 여러 번 다운로드되지 않으며 불필요한 업데이트는 전혀 다운로드되지 않습니다. *중앙 관리 서버 저장소 업데이트 다운로드* 작업을 실행할 때 Kaspersky 데이터베이스 및 소프트웨어 모듈의 관련 버전을 제대로 다운로드하기 위해 Kaspersky 업데이트 서버로 다음 정보를 중앙 관리 서버가 자동 전송합니다:

- 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 저장소 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 저장소 업데이트 다운로드 작업 및 배포 지점의 저장소로 업데이트 다운로드 작업을 사용하여 업데이트

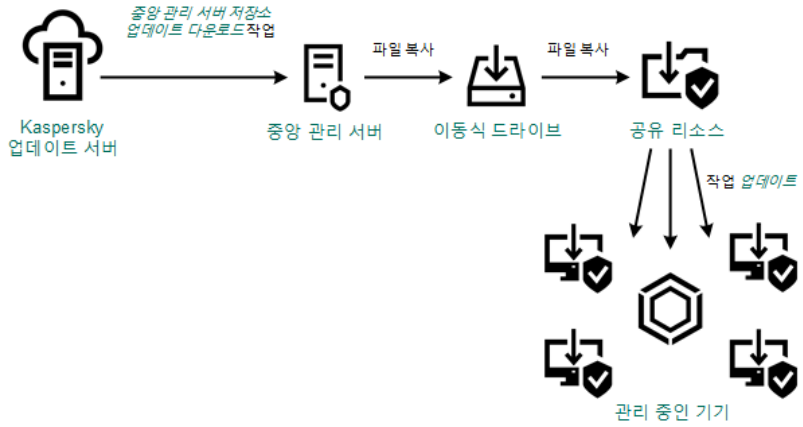
기본적으로 중앙 관리 서버 및 배포 지점은 Kaspersky 업데이트 서버와 통신하고 HTTPS 프로토콜을 사용하여 업데이트를 다운로드합니다. HTTPS 대신 HTTP 프로토콜을 사용하도록 중앙 관리 서버 및 배포 지점을 구성할 수 있습니다.

이 구성을 구현하려면 *중앙 관리 서버 저장소 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.

중앙 관리 서버 저장소 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

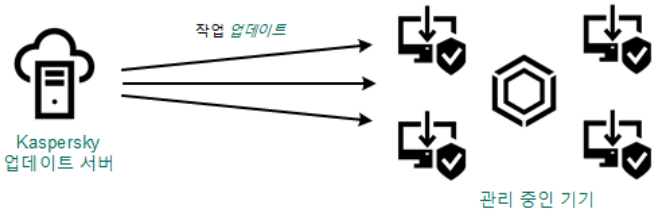
클라이언트 기기가 중앙 관리 서버에 연결되어 있지 않은 경우 로컬 폴더 또는 공유 리소스를 Kaspersky 데이터베이스, 소프트웨어 모듈 및 애플리케이션을 업데이트하는 경로로 사용할 수 있습니다. 이 체계에서는 필요한 업데이트를 중앙 관리 서버 저장소에서 이동식 드라이브로 복사한 다음 Kaspersky Endpoint Security for Linux 설정 에서 업데이트 경로로 지정된 로컬 폴더 또는 공유 리소스에 복사해야 합니다(아래 그림 참조).



로컬 폴더, 공유 폴더 또는 FTP 서버를 통해 업데이트

Kaspersky 업데이트 서버에서 관리 중인 기기의 Kaspersky Endpoint Security for Linux로 직접 업데이트

관리 중인 기기에서 Kaspersky Endpoint Security for Linux가 Kaspersky 업데이트 서버에서 직접 업데이트를 받도록 구성할 수 있습니다(아래 그림 참조).



이 체계에서 보안 제품은 Kaspersky Security Center에서 제공하는 저장소를 사용하지 않습니다. Kaspersky 업데이트 서버에서 직접 업데이트를 받으려면 보안 제품에서 Kaspersky 업데이트 서버를 업데이트 경로로 지정합니다. 이 설정에 관한 전체 설명은 Kaspersky Endpoint Security for Linux 문서를 참조하십시오.

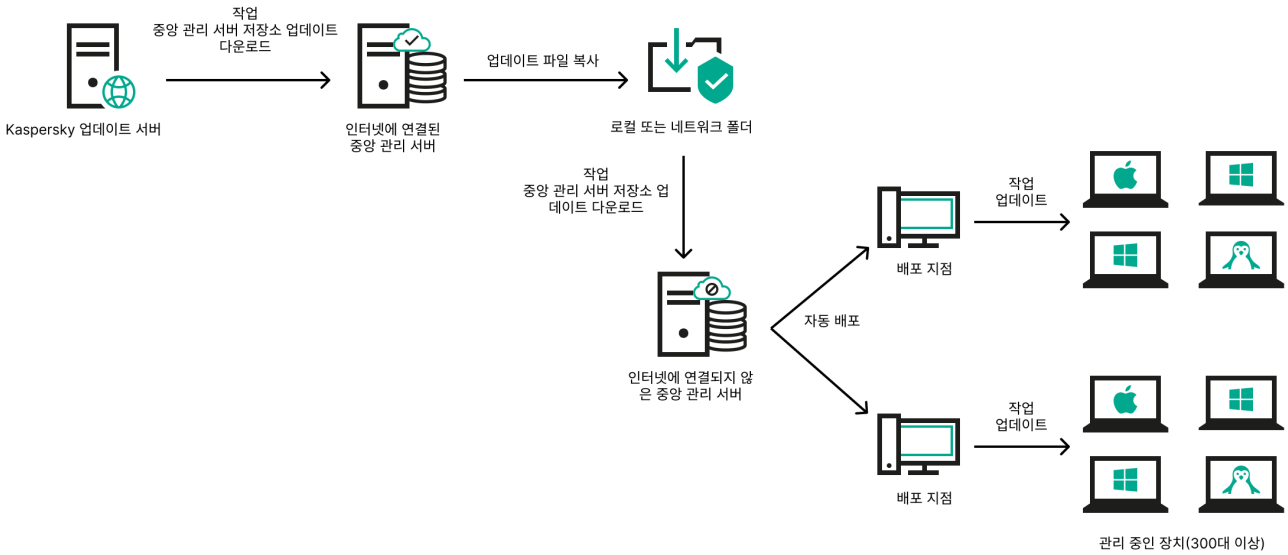
중앙 관리 서버에 인터넷 연결이 없을 시, 로컬 또는 네트워크 폴더를 통해

중앙 관리 서버가 인터넷에 연결되어 있지 않을 시, *중앙 관리 서버 저장소 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 저장소 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 저장소 업데이트 다운로드* 작업의 속성을 열고 *이전 구성표를 사용해 업데이트 다운로드* 옵션을 활성화합니다.

중앙 관리 서버 저장소에 업데이트 다운로드 작업 생성

모두 펼치기 | 모두 접기

중앙 관리 서버 저장소 업데이트 다운로드 작업을 통해 Kaspersky 업데이트 서버에서 중앙 관리 서버 저장소로 Kaspersky 보안 애플리케이션용 데이터베이스 및 소프트웨어 모듈 업데이트를 다운로드할 수 있습니다.

Kaspersky Security Center 빠른 시작 마법사는 중앙 관리 서버의 *중앙 관리 서버 저장소 업데이트 다운로드* 작업을 자동 생성합니다. 작업 목록에는 *중앙 관리 서버 저장소 업데이트 다운로드* 작업이 하나만 있을 수 있습니다. 이 작업이 중앙 관리 서버의 작업 목록에서 제거되었다면 다시 생성할 수 있습니다.

중앙 관리 서버 저장소 업데이트 다운로드 작업이 완료되고 업데이트가 다운로드되면 관리 중인 장치로 배포할 수 있습니다.

> 관리 중인 장치에 업데이트를 배포하기 전에 *업데이트 검증* 작업을 실행할 수 있습니다. 이렇게 하면 중앙 관리 서버가 다운로드한 업데이트를 제대로 설치하고, 업데이트로 보안 수준이 저하되지 않도록 할 수 있습니다. 배포하기 전에 확인하려면 *중앙 관리 서버 저장소 업데이트 다운로드* 작업 설정에서 **업데이트 검증 실행** 옵션을 구성합니다.

중앙 관리 서버 저장소 업데이트 다운로드 작업을 만들려면 다음 단계를 따릅니다.

1. **기기 → 작업**으로 이동합니다.
2. **추가**를 누릅니다.

   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. Kaspersky Security Center 애플리케이션에서는 **중앙 관리 서버 저장소 업데이트 다운로드** 작업 유형을 선택합니다.

4. 만들고 있는 작업의 이름을 지정합니다. 작업 이름은 100자를 넘지 않으며 특수 문자("*<>?\:|)를 사용할 수 없습니다.

5. **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.

6. **마침** 버튼을 누릅니다.
   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**

  Kaspersky 업데이트 서버, 로컬 또는 네트워크 폴더, 기본 중앙 관리 서버를 업데이트 경로로 사용할 수 있습니다.

  > *중앙 관리 서버 저장소에 업데이트 다운로드* 작업과 *배포 지점 저장소에 업데이트 다운로드* 작업에서, 암호로 보호된 로컬 또는 네트워크 폴더를 업데이트 경로로 지정하면 사용자 인증이 작동하지 않습니다. 이 문제를 해결하려면 먼저 암호로 보호된 폴더를 탑재한 다음 운영 체제 등을 통해 필요한 자격 증명을 지정합니다. 그런 다음 업데이트 다운로드 작업 시 이 폴더를 업데이트 경로로 선택할 수 있습니다. Kaspersky Security Center에서는 자격 증명을 입력할 필요가 없습니다.

- **업데이트 저장 폴더**

  저장된 업데이트를 보관하도록 지정한 폴더의 경로입니다. 지정된 폴더 경로를 클립보드에 복사할 수 있습니다. 그룹 작업에 대해 지정된 폴더의 경로를 변경할 수 없습니다.

- **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.

  기본적으로 이 옵션은 비활성화되어 있습니다.

- **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 Linux
    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 13이라면, 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 검증 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:

- **시작 스케줄**:

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **수동 시작**(기본적으로 선택)

    작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.
    이 옵션은 기본적으로 활성화되어 있습니다.

  - **매 N분마다**

    작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.
    기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

  - **매 N시간마다**

    작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.
    기본적으로 작업은 현재 시스템 날짜와 시간부터 6시간마다 실행됩니다.

  - **매 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.

  - **매 N주마다**

    작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.
    기본적으로 작업은 월요일마다 현재 시스템 시간에 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. Kaspersky Security Center Linux 이전 버전과의 호환성에 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.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 현재 작업 시작을 트리거하려면 이전 작업이 완료되어야 하는 방식(성공적으로 완료 또는 오류 발생)을 선택할 수 있습니다.

- 추가 작업 설정:

  - **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 비활성화하면 클라이언트 기기에서 스케줄이 지정된 작업만 실행되며 **수동 시작**, **한번만** 또는 **즉시**의 경우, 네트워크에서 인식된 클라이언트 기기에서만 작업이 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.
    이 옵션은 기본적으로 활성화되어 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 임의 시작(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.

  - **작업이 (분) 이상 실행된 경우 작업 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 저장소 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.

다운로드된 업데이트 보기

중앙 관리 서버가 *중앙 관리 서버 저장소 업데이트 다운로드* 작업을 수행하면, 데이터베이스 및 소프트웨어 모듈이 해당하는 업데이트 경로에서 다운로드되어 중앙 관리 서버의 공유 폴더에 저장됩니다. **Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트** 섹션에서 다운로드한 업데이트를 볼 수 있습니다.

다운로드된 업데이트 목록을 보려면 다음과 같이 하십시오,

메인 메뉴에서 **동작 → Kaspersky 애플리케이션 → Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트**로 이동합니다.

사용 가능한 업데이트 목록이 나타납니다.

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 저장소 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 저장소 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 Linux 등)에 대한 업데이트 및 바이러스 검사 작업을 생성합니다. 업데이트 및 바이러스 검사 작업을 생성할 때 테스트 기기로 관리 그룹을 지정합니다.

   *업데이트 검증*작업은 테스트 기기에서 업데이트 및 바이러스 검사 작업을 순차적으로 실행하여 모든 업데이트가 유효한지 확인합니다. 또한 *업데이트 검증*작업을 생성할 때 업데이트 및 바이러스 검사 작업을 지정해야 합니다.

3. *중앙 관리 서버 저장소 업데이트 다운로드* 작업을 생성합니다.

다운로드한 업데이트를 클라이언트 장치로 배포하기 전에 Kaspersky Security Center Linux에서 검증하도록 하려면:

1. 메인 애플리케이션 창에서 **기기 → 작업**로 이동합니다.
2. **중앙 관리 서버 저장소 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. 열리는 새 작업 마법사에서 사전 설정 이름을 변경하려면 작업 이름을 지정합니다.

   c. 이전에 생성한 테스트 기기가 있는 관리 그룹을 선택합니다.

   d. 먼저 Kaspersky Security Center에서 지원하는 필수 애플리케이션의 업데이트 작업을 선택한 다음 바이러스 검사 작업을 선택합니다.

이후에 다음 옵션이 표시됩니다. 활성화된 상태로 두는 것이 좋습니다.

- **데이터베이스 업데이트 이후에 기기 다시 시작**

  기기에서 안티바이러스 데이터베이스를 업데이트한 후 장치를 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 저장소 업데이트 다운로드* 작업의 속성 창을 닫습니다.

자동 업데이트 검증이 활성화됩니다. 이제 *중앙 관리 서버 저장소 업데이트 다운로드* 작업을 실행할 수 있으며 업데이트 확인부터 시작됩니다.

배포 지점의 저장소로 업데이트 다운로드 작업 만들기

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.

*선택한 관리 그룹에 대해 **배포 지점의 저장소로 업데이트 다운로드** 작업을 만들려면 다음 단계를 따릅니다.*

1. 메인 애플리케이션 창에서 **기기** → **작업**로 이동합니다.
2. **추가** 버튼을 누릅니다.
   작업 추가 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. **만들기** 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.

- 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.

  중앙 관리 서버 저장소에 업데이트 다운로드 작업과 *배포 지점 저장소에 업데이트 다운로드* 작업에서, 암호로 보호된 로컬 또는 네트워크 폴더를 업데이트 경로로 지정하면 사용자 인증이 작동하지 않습니다. 이 문제를 해결하려면 먼저 암호로 보호된 폴더를 탑재한 다음 운영 체제 등을 통해 필요한 자격 증명을 지정합니다. 그런 다음 업데이트 다운로드 작업 시 이 폴더를 업데이트 경로로 선택할 수 있습니다. Kaspersky Security Center에서는 자격 증명을 입력할 필요가 없습니다.

- **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 Linux

    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 이라면, *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:

- **시작 스케줄**

  작업이 실행되는 기준이 되는 스케줄을 선택한 다음, 선택한 스케줄을 구성합니다.

  - **수동 시작**(기본적으로 선택)

    작업은 자동으로 실행되지 않습니다. 수동으로만 작업을 시작할 수 있습니다.

    이 옵션은 기본적으로 활성화되어 있습니다.

  - **매 N분마다**

작업이 지정된 분 단위 간격에 따라 생성된 날짜의 지정된 시간부터 주기적으로 실행됩니다.
기본적으로 작업은 현재 시스템 시간부터 30분마다 실행됩니다.

- **매 N시간마다**

  작업이 지정한 날짜와 시간부터 지정된 시간 단위 간격에 따라 주기적으로 실행됩니다.
  기본적으로 작업은 현재 시스템 날짜와 시간부터 6시간마다 실행됩니다.

- **매 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.

- **매 N주마다**

  작업이 지정된 주 단위 간격에 따라 지정한 요일과 시간에 주기적으로 실행됩니다.
  기본적으로 작업은 월요일마다 현재 시스템 시간에 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. Kaspersky Security Center Linux 이전 버전과의 호환성에 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.

- **매달 선택한 주간의 지정한 날짜**

  이 작업은 매월 지정한 날짜의 지정된 시간에 주기적으로 실행됩니다.
  기본적으로 날짜는 선택되어 있지 않으며, 기본 시작 시각은 오후 6:00:00입니다.

- **바이러스 급증 시**

  바이러스 급증 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 급증을 보고하는 안티 바이러스 애플리케이션 유형에 따라 각기 다른 작업을 실행하려는 경우가 있습니다. 이러한 경우에는 필요 없는 애플리케이션 유형 모음을 제거합니다.

- **다른 작업 완료 시**

  다른 작업이 완료되면 현재 작업이 시작됩니다. 현재 작업 시작을 트리거하려면 이전 작업이 완료되어야 하는 방식(성공적으로 완료 또는 오류 발생)을 선택할 수 있습니다.

- **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 비활성화하면 클라이언트 기기에서 스케줄이 지정된 작업만 실행되며 **수동 시작**, **한번만** 또는 **즉시**의 경우, 네트워크에서 인식된 클라이언트 기기에서만 작업이 실행됩니다. 예를 들어 리소스를 많이 사용하여 업무 시간이 아닐 때만 실행하려는 작업의 경우 이 옵션을 비활성화할 수 있습니다.

  이 옵션은 기본적으로 활성화되어 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 임의 시작(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. **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.

중앙 관리 서버 저장소에 업데이트 다운로드 작업에 대한 업데이트 경로 추가

중앙 관리 서버 저장소에 업데이트를 다운로드하는 작업을 만들거나 사용할 때 다음 업데이트 경로를 선택할 수 있습니다.

- Kaspersky 업데이트 서버
- 기본 중앙 관리 서버

  이 리소스는 보조 또는 가상 중앙 관리 서버용으로 생성한 작업에 적용됩니다.
- 로컬 또는 네트워크 폴더

  중앙 관리 서버 저장소에 업데이트 다운로드 작업과 *배포 지점 저장소에 업데이트 다운로드* 작업에서, 암호로 보호된 로컬 또는 네트워크 폴더를 업데이트 경로로 지정하면 사용자 인증이 작동하지 않습니다. 이 문제를 해결하려면 먼저 암호로 보호된 폴더를 탑재한 다음 운영 체제 등을 통해 필요한 자격 증명을 지정합니다. 그런 다음 업데이트 다운로드 작업 시 이 폴더를 업데이트 경로로 선택할 수 있습니다. Kaspersky Security Center에서는 자격 증명을 입력할 필요가 없습니다.

Kaspersky 업데이트 서버가 기본적으로 사용되지만 로컬 또는 네트워크 폴더에서 업데이트를 다운로드할 수도 있습니다. 네트워크에서 인터넷에 액세스할 수 없다면 폴더를 사용할 수 있습니다. 이때, Kaspersky 업데이트 서버에서 수동으로 업데이트를 다운로드하고 다운로드한 파일을 필요한 폴더에 넣을 수 있습니다.

로컬 또는 네트워크 폴더에 대한 경로는 하나만 지정할 수 있습니다. 로컬 폴더는 중앙 관리 서버에 있는 폴더만 사용할 수 있습니다. 네트워크 폴더는 FTP 또는 HTTP 서버만 사용할 수 있습니다.

Kaspersky 업데이트 서버와 로컬 또는 네트워크 폴더를 모두 추가하면, 폴더에서 업데이트가 먼저 다운로드됩니다. 다운로드 시 오류가 발생하면 Kaspersky 업데이트 서버가 사용됩니다.

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 경로를 추가하려면:

1. **기기 → 작업**으로 이동합니다.
2. **중앙 관리 서버 저장소 업데이트 다운로드**를 클릭합니다.
3. **애플리케이션 설정** 탭으로 이동합니다.
4. **업데이트 경로** 라인에서 **구성** 버튼을 클릭합니다.
5. 창이 열리면 **추가**를 누릅니다.
6. 업데이트 경로 목록에서 필요한 경로를 추가합니다. **로컬 또는 네트워크 폴더** 확인란을 선택했다면, 폴더 경로를 지정합니다.
7. **확인**을 클릭한 다음 업데이트 경로 속성 창을 닫습니다.
8. 업데이트 경로 창에서 **확인**을 누릅니다.
9. 작업 창에서 **저장** 버튼을 클릭합니다.

이제 지정된 경로에서 중앙 관리 서버 저장소로 업데이트가 다운로드됩니다.

Kaspersky 데이터베이스 및 소프트웨어 모듈 업데이트 시 diff 파일 사용에 대한 정보

Kaspersky Security Center Linux는 Kaspersky 업데이트 서버에서 업데이트를 다운로드할 때 diff 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.

> 배포 지점은 달라진 파일 자동 배포를 위해 IP 멀티캐스팅을 사용하지 않습니다.

diff 파일 다운로드 기능 사용: 시나리오

단계

1. **중앙 관리 서버에서 기능 활성화**

   중앙 관리 서버 저장소에 업데이트 다운로드 작업 설정에서 이 기능을 활성화합니다.

2. **배포 지점에 대한 기능을 활성화하기**

   배포 지점의 저장소로 업데이트 다운로드 작업을 통해 업데이트를 받는 배포 지점에 대한 기능을 활성화합니다.

   그런 다음 중앙 관리 서버에서 업데이트를 받는 배포 지점에 대한 네트워크 에이전트 정책 설정의 기능을 활성화합니다.

   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.

배포 지점을 통해 업데이트 다운로드

Kaspersky Security Center Linux는 중앙 관리 서버, Kaspersky 서버, 로컬 또는 네트워크 폴더에서 배포 지점으로 업데이트를 받을 수 있도록 허용합니다.

배포 지점을 위해 업데이트 다운로드를 구성하려면 다음과 같이 하십시오:

1. 메인 애플리케이션 창에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘()을 누릅니다.
   중앙 관리 서버 속성 창이 열립니다.
2. **일반** 탭에서 **배포 지점** 섹션을 선택합니다.
3. 업데이트를 그룹의 클라이언트 장치로 전달할 배포 지점의 이름을 클릭합니다.
4. 배포 지점 속성 창에서 **업데이트 경로** 섹션을 선택합니다.
5. 배포 지점을 위한 업데이트 경로를 선택하십시오:

   - **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 없는 경우 **작업 만들기**링크를 눌러 작업을 만듭니다. 작업 추가 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

   - **diff 파일 다운로드**

     이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

     이 옵션은 기본적으로 활성화되어 있습니다.

배포 지점이 지정한 경로에서 업데이트를 가져오게 됩니다.

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 저장소를 사용하여 정기 업데이트를 구성합니다.

중앙 관리 서버(기본 또는 보조), 배포 지점 또는 인터넷에 연결되지 않은 장치(또는 장치 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 저장소 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 저장소 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 장치에 항상 최신 버전의 업데이트가 포함됩니다.
3. 오프라인 장치에서 로컬 폴더 또는 FTP 서버나 공유 폴더와 같은 공유 경로에서 업데이트를 받도록 Kaspersky Endpoint Security for Linux를 구성 합니다.
4. 이동식 드라이브에서 업데이트 파일을 업데이트 경로로 사용할 로컬 폴더 또는 공유 경로로 복사합니다.
5. 업데이트 설치가 필요한 오프라인 기기에서 Kaspersky Endpoint Security for Linux의 업데이트 작업을 시작합니다.

업데이트 작업이 완료되면 Kaspersky 데이터베이스 및 소프트웨어 모듈이 기기에서 최신 상태가 됩니다.

배포 지점 및 연결 게이트웨이 조정

Kaspersky Security Center Linux의 관리 그룹 구조는 다음 기능을 수행합니다.

- 정책의 범위 설정

  *정책 프로필*을 사용하여 장치에서 관련 설정 모음을 적용할 수도 있습니다.
- 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.

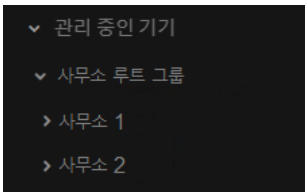
관리 그룹 구조를 구성하는 데 사용할 수 있는 방법은 다음과 같습니다:

- 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 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
10,000대 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
10,000대 이하	0(배포 지점 할당 안 함)
10~100대	1
300대 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
10,000대 이하	0(배포 지점 할당 안 함)
300대 이상	(N/300 + 1), 여기서 N은 네트워크에 연결된 기기 수를 뜻하지만 최소 3대의 배포 지점이 있어야 합니다

네트워크에 연결된 기기 수에 따라 다중 네트워크 세그먼트를 포함하는 네트워크에 배포 지점 기능을 수행하는 워크스테이션의 수

네트워크 세그먼트당 클라이언트 기기의 수	배포 지점 개수
10,000대 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.

배포 지점 자동 할당

배포 지점을 자동으로 할당하는 것이 좋습니다. 이때, Kaspersky Security Center Linux는 배포 지점을 할당해야 하는 장치를 자체 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 Center Linux를 사용하면 배포 지점 역할을 수행할 장치를 수동으로 할당할 수 있습니다.

배포 지점을 자동으로 할당하는 것이 좋습니다. 이때, Kaspersky Security Center Linux는 배포 지점을 할당해야 하는 장치를 자체 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 Center Linux는 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 장치의 게이트웨이 주소**

  원격 장치가 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. 이 옵션은 기본적으로 활성화되어 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** 섹션에서 배포 지점에서 업데이트를 배포할 관리 그룹을 지정합니다.
- **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 없는 경우 **작업 만들기**링크를 눌러 작업을 만듭니다. 작업 추가 마법사가 시작됩니다. 마법사의 지침을 따릅니다.

- **diff 파일 다운로드**

  이 옵션을 사용하면 달라진 파일 다운로드 기능이 활성화됩니다.

  이 옵션은 기본적으로 활성화되어 있습니다.

- **인터넷 연결 설정** 하위 섹션에서 인터넷 연결 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 선택 해제되어 있습니다.

  - **사용자 이름**

    프록시 서버에 대한 연결을 구성할 사용자 계정입니다.

  - **암호**

    작업을 실행할 계정의 암호입니다.

- **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 게이트웨이로의 연결 설정(게이트웨이가 DMZ에 있는 경우)**

  중앙 관리 서버가 비무장 지대(DMZ) 외부에 있을 시 로컬 영역 네트워크에서 원격 장치에 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 14 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 게이트웨이로의 연결 설정(게이트웨이가 DMZ에 있는 경우)** 옵션을 활성화한 경우에 사용할 수 있습니다.

- **모바일 기기용 포트 열기(중앙 관리 서버의 SSL 인증용)**

  모바일 장치용 포트를 열기 위해 연결 게이트웨이가 필요하다면, 이 옵션을 활성화하고 모바일 장치가 배포 지점에 연결하는 데 사용할 포트 번호를 지정합니다. 기본 포트 번호는 13292입니다. 연결을 설정할 때 중앙 관리 서버만 인증됩니다.

- **모바일 기기용 포트 열기(상호간의 SSL 인증)**

  중앙 관리 서버와 모바일 장치의 양방향 인증에 사용할 포트를 열기 위해 연결 게이트웨이가 필요하다면 이 옵션을 활성화합니다. 다음 파라미터를 지정합니다:

  - 모바일 장치가 배포 지점에 연결하는 데 사용할 포트 번호. 기본 포트 번호는 13293입니다.
  - 모바일 장치에서 사용할 연결 게이트웨이의 DNS 도메인 이름. 도메인 이름은 쉼표로 구분합니다. 지정된 도메인 이름은 배포 지점 인증서에 포함됩니다. 모바일 장치에서 사용하는 도메인 이름이 배포 지점 인증서의 일반 이름과 일치하지 않으면 모바일 장치가 배포 지점에 연결되지 않습니다.

    기본 DNS 도메인 이름은 연결 게이트웨이의 FQDN 이름입니다.

- 배포 지점별로 IP 범위의 검색을 구성합니다.

  - **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 **제로 구성을 사용하여 IPv6 네트워크 폴링** 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, **제로 구성을 사용하여 IPv6 네트워크 폴링** 옵션을 사용할 수 있습니다. Zerocong 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 지점로 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 **기기 → 관리 중인 기기** 로 이동합니다.
2. 관리 중인 장치 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 **기기 → 배포 지점** 탭으로 이동합니다.
5. 관리 그룹에 대한 새 배포 지점을 추가하려면 **할당** 버튼을 클릭합니다.
6. 할당된 배포 지점을 제거하려면 목록에서 장치를 선택하고 **할당 해제** 버튼을 클릭합니다.

수정 사항에 따라 새 배포 지점이 목록에 추가되거나 기존 배포 지점이 목록에서 제거됩니다.

푸시 서버 활성화

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.

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 사용할 시, 관리 중인 장치에서 **중앙 관리 서버와 계속 연결 유지** 옵션을 사용하거나 네트워크 에이전트의 UDP 포트로 패킷을 보낼 필요가 없습니다.

> 푸시 서버는 최대 50,000개의 동시 연결 로드를 지원합니다.

배포 지점에서 푸시 서버를 활성화하려면 다음과 같이 하십시오.

1. 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 장치에서 실행되는 제삼자 애플리케이션 관리와 관련된 Kaspersky Security Center Linux의 기능을 설명합니다.

시나리오: 애플리케이션 관리

사용자 기기에서 애플리케이션 시작을 관리할 수 있습니다. 관리 중인 기기에서 실행할 애플리케이션을 허용하거나 차단할 수 있습니다. 이 기능은 애플리케이션 제어 구성 요소에 의해 실현됩니다.

> 애플리케이션 제어 구성 요소는 Linux용 Kaspersky Endpoint Security 11.2 이상 버전에서 사용할 수 있습니다.

필수 구성 요소

- 조직에 Kaspersky Security Center Linux가 배포되어 있습니다.
- Kaspersky Endpoint Security for Linux 정책이 생성 및 활성화됩니다.

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. 관리 중인 기기에 설치할 실행 파일을 정확하게 안다면 이 단계를 건너뛰어도 됩니다.

   방법 지침: 클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기

2. **조직에서 사용된 애플리케이션에 대한 애플리케이션 카테고리 생성**

   관리 중인 장치에 저장된 실행 파일 목록을 분석합니다. 분석을 바탕으로 애플리케이션 카테고리를 만듭니다. 조직에서 사용하는 표준 애플리케이션 집합을 포괄하는 '업무용 애플리케이션' 카테고리를 만드는 것이 좋습니다. 다양한 사용자 그룹이 업무에 다양한 애플리케이션 집합을 사용할 경우 사용자 그룹마다 별도의 애플리케이션 카테고리를 만들 수 있습니다.

   방법 지침: 컨텐츠가 수동으로 추가된 애플리케이션 카테고리 만들기

3. **Kaspersky Endpoint Security for Linux 정책에서 애플리케이션 제어 구성**

   이전 단계에서 만든 애플리케이션 카테고리를 사용하여 Kaspersky Endpoint Security for Linux 정책의 애플리케이션 제어 구성 요소를 구성합니다.

4. **애플리케이션 제어 구성 확인**

   다음을 수행했는지 확인합니다.

   - 애플리케이션 카테고리 생성
   - 애플리케이션 카테고리로 애플리케이션 제어 구성

결과

시나리오가 완료되면 관리 중인 기기에서 애플리케이션 시작이 제어됩니다. 사용자는 조직에서 허용한 애플리케이션만 시작할 수 있으며 조직에서 금지한 애플리케이션은 시작할 수 없습니다.

애플리케이션 제어에 대한 자세한 내용은 Kaspersky Endpoint Security for Linux 도움말 을 참조하십시오.

애플리케이션 제어 정보

애플리케이션 제어 구성 요소는 애플리케이션을 시작하려는 사용자의 시도를 모니터링하고 애플리케이션 제어 규칙으로 애플리케이션 시작을 규제합니다.

애플리케이션 제어 구성 요소는 Linux용 Kaspersky Endpoint Security 11.2 이상 버전에서 사용할 수 있습니다.

설정이 애플리케이션 제어 규칙 중 하나와 일치하지 않는 애플리케이션의 시작은 선택한 구성 요소 운영 모드에 의해 규제됩니다.

- *거부 목록*. 이 모드는 차단 규칙에 지정된 애플리케이션을 제외한 모든 애플리케이션의 시작을 허용하려는 경우에 사용됩니다. 기본적으로 이 모드가 선택됩니다.
- *허용 목록*. 이 모드는 허용 규칙에 지정된 애플리케이션을 제외한 모든 애플리케이션의 시작을 차단하려는 경우에 사용됩니다.

애플리케이션 제어 규칙은 애플리케이션 카테고리를 통해 구현됩니다. 특정 기준을 정의하는 애플리케이션 카테고리를 생성합니다. Kaspersky Security Center Linux에서는 수동으로 추가된 컨텐츠가 있는 카테고리만 만들 수 있습니다. 카테고리에 실행 파일을 포함하도록 예를 들어 파일 메타데이터, 파일 해시 코드, 파일 인증서, KL 카테고리, 파일 경로와 같은 조건을 정의합니다.

애플리케이션 제어에 대한 자세한 내용은 Kaspersky Endpoint Security for Linux 도움말 을 참조하십시오.

클라이언트 기기에 저장된 실행 파일 목록 확보 및 보기

관리 중인 기기에 저장된 실행 파일 목록을 확보할 수 있습니다. 실행 파일의 인벤토리에 인벤토리 작업을 생성해야 합니다.

실행 파일의 인벤토리 기능은 Linux용 Kaspersky Endpoint Security 11.2 이상 버전에서 사용할 수 있습니다.

클라이언트 기기에 있는 실행 파일에 대한 인벤토리 작업을 만들려면:

1. **기기 → 작업**으로 이동합니다.
   작업 목록이 표시됩니다.
2. **추가** 버튼을 누릅니다.
   새 작업 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. **새 작업** 페이지의 **애플리케이션** 드롭다운 목록에서 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 Kaspersky Endpoint Security for Linux 온라인 도움말을 참조하십시오.

인벤토리 작업을 수행한 후 관리 중인 기기에 저장된 실행 파일 목록이 형성되고 이 목록을 확인할 수 있습니다.

인벤토리 작업 동안 MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, HTML 형식인 실행 파일이 감지됩니다.

클라이언트 기기에 저장된 실행 파일 목록을 보려면 다음 단계를 따릅니다.

동작 → 타사 애플리케이션 드롭다운 목록에서 **실행 파일**를 선택합니다.

이 페이지에는 클라이언트 기기에 저장된 실행 파일 목록이 표시됩니다.

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. **동작 → 타사 애플리케이션** 드롭 다운 목록에서 **애플리케이션 카테고리**를 선택합니다.
   애플리케이션 카테고리 목록이 있는 페이지가 표시됩니다.
2. **추가** 버튼을 누릅니다.
   새 카테고리 마법사가 시작됩니다. 마법사의 각 단계를 따릅니다.
3. 마법사의 **카테고리 생성 방법 선택** 페이지에서 **수동으로 추가된 컨텐츠가 있는 카테고리. 실행 파일의 데이터를 수동으로 카테고리에 추가합니다** 옵션을 선택합니다.
4. 마법사의 **조건** 페이지에서 **추가** 버튼을 클릭하여 카테고리 생성 시 포함할 조건 기준을 추가합니다.
5. **조건 기준** 페이지의 목록에서 카테고리 생성에 대한 규칙 유형을 선택합니다.

- **저장소에서 인증서 선택**

  이 옵션을 선택하면 저장소에서의 인증서를 지정할 수 있습니다. 지정된 인증서에 따라 서명된 실행 파일은 사용자 카테고리에 추가됩니다.

- **애플리케이션 경로 지정(마스크 지원)**

  이 옵션을 선택하면 사용자 애플리케이션 카테고리에 추가할 실행 파일이 포함된 폴더 경로를 클라이언트 기기에서 지정할 수 있습니다.

- **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 선택하고 다음 파일 메타데이터를 지정할 수 있습니다.

    - 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.

  - **수동 지정**

    이 옵션을 선택하면 사용자 카테고리에 애플리케이션을 추가하는 조건으로 파일 해시, 메타데이터 또는 인증서를 지정해야 합니다.

    파일 해시

    네트워크의 장치에 설치된 보안 제품 버전에 따라 이 카테고리의 파일에 대해 Kaspersky Security Center Linux에서 수행하는 해시 값 계산용 알고리즘을 선택해야 합니다. 계산된 해시 값에 대한 정보는 중앙 관리 서버 데이터베이스에 저장됩니다. 해시 값이 저장되어도 데이터베이스 크기가 상당히 커지지는 않습니다.

    SHA-256은 암호화 해시 함수입니다. 해당 알고리즘에서 발견된 취약점이 없으므로 최근까지 가장 믿을 수 있는 암호화 함수로 간주되고 있습니다. Kaspersky Endpoint Security for Linux는 SHA-256 컴퓨팅을 지원합니다.

    카테고리의 파일에 대해 Kaspersky Security Center Linux에서 수행하는 해시 값 계산의 옵션 선택합니다:

    - 네트워크에 설치된 보안 애플리케이션의 모든 인스턴스가 Kaspersky Endpoint Security for Linux일 시, **SHA-256** 확인란을 선택합니다.
    - Kaspersky Endpoint Security for Windows를 사용할 때만 **MD5 해시** 확인란을 선택합니다. Kaspersky Endpoint Security for Linux는 MD5 해시 기능을 지원하지 않습니다.

    메타데이터

    이 옵션을 선택하면 파일 메타 데이터를 파일 이름, 파일 버전, 공급업체로 지정할 수 있습니다. 메타데이터가 중앙 관리 서버로 전송됩니다. 동일한 메타데이터가 포함된 실행 파일이 애플리케이션 카테고리에 추가됩니다.

    인증서

    이 옵션을 선택하면 저장소에서의 인증서를 지정할 수 있습니다. 지정된 인증서에 따라 서명된 실행 파일은 사용자 카테고리에 추가됩니다.

  - **압축된 폴더에서**

    이 옵션을 선택하면 압축된 폴더의 파일을 지정한 다음 사용자 카테고리에 애플리케이션을 추가하는 데 사용할 조건을 선택할 수 있습니다. 압축된 폴더의 압축이 풀리고 선택한 조건이 해당 폴더의 파일에 적용됩니다. 조건으로 다음 기준 중 하나를 선택할 수 있습니다.

    - **파일 해시**

      해시 값을 계산하는 데 사용할 해시 함수(MD5 또는 SHA-256)를 선택합니다. 압축된 폴더의 파일과 동일한 해시 값을 가진 애플리케이션이 사용자 애플리케이션 카테고리에 추가됩니다.

      Kaspersky Endpoint Security for Windows를 사용할 때만 MD5 해시 함수를 선택하십시오. Kaspersky Endpoint Security for Linux는 MD5 해시 기능을 지원하지 않습니다.

    - **메타데이터**

      기준으로 사용할 메타 데이터를 선택합니다. 동일한 메타데이터가 포함된 실행 파일이 사용자 애플리케이션 카테고리에 추가됩니다.

    - **인증서**

      기준으로 사용할 인증서 속성(인증서 주체, 지문 또는 발급자)을 선택합니다. 동일한 속성을 가진 인증서에 따라 서명된 실행 파일이 사용자 카테고리에 추가됩니다.

선택한 기준이 조건 목록에 추가됩니다.

애플리케이션 카테고리 생성에 필요한 만큼의 기준을 추가할 수 있습니다.

6. 마법사의 **예외 규칙** 페이지에서 **추가** 버튼을 눌러 생성 중인 카테고리에서 제외할 배타적 조건 기준을 추가합니다.

7. 카테고리 생성 시 규칙 유형을 선택한 것과 같은 방식으로 **조건 기준** 페이지의 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 Kaspersky Endpoint Security for Linux 도움말을 참조하십시오.

애플리케이션 카테고리 목록 보기

구성된 애플리케이션 카테고리 목록과 각 애플리케이션 카테고리의 설정을 확인할 수 있습니다.

애플리케이션 카테고리의 목록을 확인하려면 다음 단계를 따릅니다.

동작 탭의 **타사 애플리케이션** 드롭다운 목록에서, **애플리케이션 카테고리**를 선택합니다.

애플리케이션 카테고리 목록이 있는 페이지가 표시됩니다.

애플리케이션 카테고리의 속성을 보려면

애플리케이션 카테고리의 이름을 누릅니다.

애플리케이션 카테고리의 속성 창이 표시됩니다. 속성은 여러 탭에 그룹화되어 있습니다.

애플리케이션 카테고리에 이벤트 관련 실행 파일 추가

Kaspersky Endpoint Security for Linux 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.
- **관리자에게 보내는 애플리케이션 시작 차단 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. **모니터링 및 보고** → **이벤트 조회**로 갑니다.
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.
  - **포함에 추가하기 위한 규칙**
  - **제외에 추가하기 위한 규칙**
- **조건으로 사용되는 파라미터** 섹션에서 다음 옵션의 하나를 선택합니다.
  - **인증서 세부 정보(또는 인증서가 없는 파일에 대한 SHA-256 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 SHA-256 해시 함수가 있습니다. SHA-256 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 SHA-256 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 건너뜁니다. 이 파일에 대한 정보는 카테고리에 추가되지 않습니다.

  - **SHA-256만(SHA-256이 없는 파일은 건너뜀)**

    각 파일에는 고유한 SHA-256 해시 함수가 있습니다. SHA-256 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

    실행 파일의 SHA-256 해시 함수의 세부 사항만 추가하려면 이 옵션을 선택합니다.

  - **MD5만(Kaspersky Endpoint Security 10 Service Pack 1 for Windows 이전의 버전에서 지원)**

    Kaspersky Endpoint Security for Windows를 사용할 때만 이 옵션을 선택합니다. Kaspersky Endpoint Security for Linux는 MD5 해시 기능을 지원하지 않습니다.

    각 파일에는 고유한 MD5 해시 함수가 있습니다. MD5 해시 함수를 선택하면 정의된 애플리케이션 버전과 같이 해당 파일 하나만 관련 카테고리에 포함됩니다.

5. **확인**을 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 Kaspersky Endpoint Security for Linux 도움말을 참조하십시오.

모니터링 및 보고

이 섹션은 Kaspersky Security Center Linux의 모니터링 및 리포팅 기능에 대해 설명합니다. 이러한 기능을 통해 인프라, 보호 상태 및 통계의 개요를 확인할 수 있습니다.

Kaspersky Security Center Linux 배포 후나 작동 중에, 자신의 필요에 맞게 모니터링 및 리포팅 기능을 구성할 수 있습니다.

시나리오: 모니터링 및 보고

이 섹션에서는 Kaspersky Security Center Linux에서 모니터링 및 리포팅 기능을 구성하는 시나리오를 제공합니다.

필수 구성 요소

조직의 네트워크에 Kaspersky Security Center Linux를 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. **심각 및 경고 알림에 대한 권장 작업 수행**

   방법 지침:

   조직 네트워크에 대한 권장 작업 수행

4. **조직 네트워크의 보안 상태 검토**

   방법 지침:

   - 보호 상태 위젯 검토
   - 보호 상태 리포트 생성 및 검토
   - 오류 리포트 생성 및 검토

5. **보호되지 않는 클라이언트 기기 위치 추적**

   방법 지침:

   - 새로운 기기 위젯 검토
   - 보호 배포 리포트 생성 및 검토

6. **클라이언트 기기의 보호 확인**

   방법 지침:

   - 보호 상태 및 위협 통계 카테고리에서 검토 리포트 생성
   - 심각 이벤트 조회 및 검토

7. **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:

   - 최대 이벤트 수 제한

8. **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 14 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 14 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 14 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 14 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.
- **심각으로 지정** 및 **경고로 지정** (표시등의 색상을 결정하는 규칙).

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.

> 중앙 관리 서버 계층이 네트워크에 정렬되어 있는 경우 대시보드 전용 모드를 구성하려면 **사용자 및 역할 → 사용자** 섹션에서 사용자 계정을 사용할 수 있는 서버로 이동합니다. 기본 서버 또는 물리적 보조 서버일 수 있습니다. 가상 서버에서는 모드를 조정할 수 없습니다.

대시보드 전용 모드 구성 방법:

1. 메인 메뉴에서 **사용자 및 역할 → 사용자**로 이동합니다.
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.

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 14 웹 콘솔의 **모니터링 및 보고** 섹션에서 사용할 수 있습니다.

기본적으로 리포트에는 지난 30일 동안의 정보가 포함됩니다.

Kaspersky Security Center Linux에는 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. 마법사의 첫 번째 페이지에서 리포트 이름을 입력하고 리포트 유형을 선택합니다.

4. 마법사의 **범위** 페이지에서 이 리포트 템플릿을 기반으로 하는 리포트에 데이터를 표시할 클라이언트 기기 세트(관리 그룹, 기기 조회, 선택한 기기 또는 네트워크에 연결된 모든 기기)를 선택합니다.

5. 마법사의 **보고 기간** 페이지에서 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

모두 펼치기 | 모두 접기

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.

       이 옵션은 기본적으로 활성화되어 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.

  이 옵션은 기본적으로 활성화되어 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.

   리포트를 PDF로 변환하려면 wkhtmltopdf 툴이 필요합니다. PDF 옵션을 선택하면 중앙 관리 서버는 wkhtmltopdf 툴이 장치에 설치되어 있는지 확인합니다. 툴이 설치되어 있지 않으면 중앙 관리 서버 장치에 툴을 설치해야 한다는 메시지가 표시됩니다. 툴을 수동으로 설치하고 다음 단계로 진행합니다.
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.

생성된 리포트에서 다이어그램의 일부 글꼴이 제대로 표시되지 않을 수 있습니다. 이 문제를 해결하려면 fontconfig 라이브러리를 설치합니다. 또한 운영 체제 로케일에 해당하는 글꼴이 운영 체제에 설치되어 있는지 확인합니다.

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. **모니터링 및 보고 → 리포트**로 갑니다.
2. [선택 사항] 리포트 전달 작업을 생성할 리포트 템플릿 옆의 확인란을 선택합니다.
3. **새 리포트 전달 작업** 버튼을 누릅니다.
4. 새 작업 마법사가 시작됩니다. **다음** 버튼을 사용하여 마법사를 진행합니다.
5. 마법사의 첫 번째 페이지에서 작업 이름을 입력합니다. 기본 이름은 **리포트 전달(<N>)**이며 여기서 <N>은 작업의 순차적 번호입니다.
6. 마법사의 작업 설정 페이지에서 다음 설정을 지정합니다.
   a. 작업을 통해 전달할 리포트 템플릿. 2단계에서 템플릿을 선택한 경우 이 단계를 건너뜁니다.
   b. 리포트 형식: HTML, XLS 또는 PDF.
   리포트를 PDF로 변환하려면 wkhtmltopdf 툴이 필요합니다. PDF 옵션을 선택하면 중앙 관리 서버는 wkhtmltopdf 툴이 장치에 설치되어 있는지 확인합니다. 툴이 설치되어 있지 않으면 중앙 관리 서버 장치에 툴을 설치해야 한다는 메시지가 표시됩니다. 툴을 수동으로 설치하고 다음 단계로 진행합니다.
   c. 리포트를 이메일로 전송할지 여부(이메일 알림 설정 포함).
   d. 리포트를 폴더에 저장할지 여부, 이전에 해당 폴더에 저장한 리포트를 덮어쓸지 여부 및 특정 계정을 사용하여 폴더에 접근할지 여부(공유 폴더의 경우).
7. 작업을 생성한 후에 다른 작업 설정을 수정하려는 경우 마법사의 **작업 생성 마침** 페이지에서 **생성이 완료되면 작업 세부 정보 열기** 옵션을 활성화합니다.
8. **만들기** 버튼을 눌러 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 Linux 구성 요소에서 발생하는 이벤트 유형, 자주 발생하는 이벤트 차단 관리에 대한 정보를 제공합니다.

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 14 웹 콘솔 인터페이스에서 사용할 수 있는 설정에 따라 사용자 지정 이벤트 조회를 생성하고 볼 수 있습니다.

이벤트 조회는 **이벤트 조회**를 눌러 Kaspersky Security Center 14 웹 콘솔의 **모니터링 및 보고** 섹션에서 사용할 수 있습니다.

기본적으로 이벤트 조회에는 지난 7일 동안의 정보가 포함됩니다.

Kaspersky Security Center Linux에서는 기본 이벤트 세트(미리 정의된)를 선택할 수 있습니다.

- 심각도 레벨이 서로 다른 이벤트:

- **심각 이벤트**
- **기능 실패**
- **경고**
- **정보 메시지**

- **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. 두 옵션은 모두 Kaspersky Security Center Linux가 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 조회** 로 이동합니다.
2. **추가**를 누릅니다.
3. **새 이벤트 조회** 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 **조회 결과로 이동** 확인란을 선택한 상태로 유지합니다.
6. **저장**을 눌러 이벤트 조회 생성을 확인합니다.

조회 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 조회**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 **액세스 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 조회**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 조회를 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 세부 정보 보기

이벤트 세부 정보를 보려면 다음 단계를 따릅니다.

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

이벤트를 파일로 내보내려면 다음 단계를 따릅니다.

1. 이벤트 조회 시작.
2. 필요한 이벤트 옆에 있는 확인란을 선택합니다.
3. **파일로 내보내기** 버튼을 누릅니다.

선택한 이벤트가 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 조회**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 Center Linux에서는 관리 중인 장치에 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 리포팅 작업을 수행할 수 있습니다.

중앙 관리 서버의 데이터베이스에서 이벤트에 대한 저장 기간을 설정하려면 다음 단계를 따릅니다.

1. **기기 → 정책 및 프로필**을 선택합니다.
2. 다음 중 하나를 수행합니다:
   - 네트워크 에이전트 또는 관리 중인 Kaspersky 애플리케이션의 이벤트 저장 기간을 구성하려면 해당 정책의 이름을 누릅니다.
     정책 속성 페이지가 열립니다.
   - 중앙 관리 서버 이벤트를 구성하려면 화면 위쪽에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘()을 누릅니다.
     중앙 관리 서버에 대한 정책이 있는 경우 대신 이 정책의 이름을 누르면 됩니다.
     중앙 관리 서버 속성 페이지(또는 중앙 관리 서버 정책 속성 페이지)가 열립니다.
3. **이벤트 구성** 탭을 선택합니다.
   심각 관련 이벤트 유형 목록 섹션이 표시됩니다.
4. **기능 실패**, **경고** 또는 **정보** 섹션을 선택합니다.
5. 오른쪽 창의 이벤트 유형 목록에서 저장 기간을 변경하려는 이벤트에 대한 링크를 누릅니다.
   창이 열리면 **이벤트 등록** 섹션에서 **다음 기간 동안 중앙 관리 서버에 저장(일)** 옵션이 활성화됩니다.
6. 이 토글 버튼 아래의 편집 상자에 이벤트를 저장할 일 수를 입력합니다.

7. 중앙 관리 서버 데이터베이스에 이벤트를 저장하지 않으려면 **다음 기간 동안 중앙 관리 서버에 저장(일)** 옵션을 비활성화합니다.

> 중앙 관리 서버 속성 창에서 중앙 관리 서버 이벤트를 구성했고 Kaspersky Security Center Linux 중앙 관리 서버 정책에서 이벤트 설정이 잠겨 있다면, 이벤트에 대한 저장 기간 값을 재정의할 수 없습니다.

8. **확인**를 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.

이벤트 유형

Kaspersky Security Center Linux 구성 요소마다 자체 이벤트 유형 집합이 있습니다. 이 섹션에는 Kaspersky Security Center Linux 중앙 관리 서버 및 네트워크 에이전트에서 발생하는 이벤트 유형이 나열되어 있습니다. Kaspersky 애플리케이션에서 발생하는 이벤트의 유형은 이 섹션에 나열되지 않습니다.

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 Center Linux에 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 Linux 데이터베이스에서 제공하는 공용 보기를 사용하여 이벤트를 찾아 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.

  이벤트 저장 기간을 변경할 수 있습니다. 이벤트 저장 기간 설정

중앙 관리 서버 이벤트

이 섹션에는 중앙 관리 서버와 관련된 이벤트에 대한 정보가 있습니다.

중앙 관리 서버 심각 이벤트

표에는 심각도가 **심각**인 Kaspersky Security Center Linux 중앙 관리 서버 이벤트가 나와 있습니다.

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 Center Linux는 하루에 한 번 라이센스 제한이 초과되었는지 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 Center Linux는 라이센스 구매 수량 초과 시 이벤트를 생성하는 규칙을 결정합니다.	3일
기기와의 연결 끊김	4111	KLSRV_HOST_OUT_CONTROL	이 유형의 이벤트는 관리 중인 기기가 네트워크에는 나타나지만 특정 기간 동안 중앙 관리 서버에 연결되지 않은 경우에 발생합니다.	3일

			해당 기기에서 네트워크 에이전트의 정상 작동을 방해하는 것이 무엇인지 확인하십시오. 가능한 원인으로는 네트워크 문제 및 기기에서 네트워크 에이전트가 제거되었을 수 있습니다.	
기기 상태 '심각'	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.	3일
키 파일이 거부 목록에 추가되었습니다	4124	KLSRV_LICENSE_BLACKLISTED	이 유형의 이벤트는 Kaspersky에서 사용자가 사용하는 활성화 코드 또는 키 파일을 거부 목록에 추가한 경우 발생합니다. 자세한 내용은 기술 지원에 문의하십시오.	3일
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. 이 날짜는 변경할 수 없습니다. 라이센스 만료 날짜 이전의 지정된 날짜에 중앙 관리 서버를 끄면 이벤트는 다음날까지 게시되지 않습니다. 상업용 라이센스가 만료되면 Kaspersky Security Center Linux의 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.	3일
인증서가 만료되었습니다	4132	KLSRV_CERTIFICATE_EXPIRED	이 유형의 이벤트는 모바일 기기 매니지먼트에 대한 중앙 관리 서버 인증서가 만료되는 경우 발생합니다. 만료된 인증서를 업데이트해야 합니다. 인증서 발급 설정에서 **가능하면 자동으로 인증서 재발급** 확인란의 선택하여 인증서 자동 업데이트를 구성할 수 있습니다.	3일

중앙 관리 서버 기능 실패 이벤트

아래 표에는 심각도가 **기능 실패**인 Kaspersky Security Center Linux 중앙 관리 서버 이벤트가 나와 있습니다.

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.	3일
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 Center Linux에서 타사 애플리케이션의 라이센스 키를 관리하며, 설치 수가 타사 애플리케이션 라이센스 키에서 설정한 제한을 초과할 때 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.	3일

			유료 애플리케이션 그룹 기능을 사용하여 타사 애플리케이션의 라이센스 키를 관리할 수 있습니다. 유료 애플리케이션 그룹에는 관리자가 지정한 기준에 부합하는 타사 애플리케이션이 들어 있습니다.	
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 폴더에 사용자 이름 또는 암호가 변경되었는지 확인합니다. • 이 이벤트의 원인일 수 있는 인터넷 연결을 확인합니다. 지침에 따라 데이터베이스 및 소프트웨어 모듈을 업데이트합니다.	3일
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.	3일
공유 폴더 접근 불가	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.	3일
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.	3일

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.
				3일

- 중앙 관리 서버 데이터베이스에 애플리케이션 제어 구성 요소가 보낸 이벤트가 매우 많을 수 있습니다. 이때 중앙 관리 서버 데이터베이스에서 애플리케이션 제어 이벤트 저장과 관련된 Kaspersky Endpoint Security for Linux 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.

중앙 관리 서버 경고 이벤트

표에는 심각도가 **경고**인 Kaspersky Security Center Linux 중앙 관리 서버 이벤트가 나와 있습니다.

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 장치에서 자주 등록된 이벤트를 감지할 때 발생합니다. 자세한 내용은 다음 섹션을 참조하십시오: 자주 등록된 이벤트 차단.	3일
라이센스 제한을 초과했습니다	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center Linux는 하루에 한 번 라이센스 제한이 초과되었는지 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 Center Linux는 라이센스 구매 수량 초과 시 이벤트를 생성하는 규칙을 결정합니다.	3일
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. Kaspersky Security Center 14 웹 콘솔을 사용하여 **오랫동안 기기가 네트워크에 접속하지 않았습니다** 이벤트를 생성할 시간 간격을 지정하십시오. • Kaspersky Security Center 14 웹 콘솔을 사용하여 그룹에서 장치를 자동 제거할 시간 간격을 지정하십시오.	3일
기기 이름 중복	4102	KLSRV_EVENT_HOSTS_CONFLICT	이 유형의 이벤트는 중앙 관리 서버가 둘 이상의 관	3일

			리 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.	
기기 상태 '경고'	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.	3일
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 지정한 최대 허용 값의 90%에 도달하면 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.	3일
인증서를 요청했습니다	4133	KLSRV_CERTIFICATE_REQUESTED	이 유형의 이벤트는 모바일 기기 매니지먼트에 대한 인증서가 자동으로 재발급되지 않은 경우 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.	3일
인증서가 제거되었습니다	4134	KLSRV_CERTIFICATE_REMOVED	이 유형의 이벤트는 관리자가 모바일 기기 매니지먼트에 대한 모든 유형의 인증서(일반, 메일, VPN)를 제거하는 경우 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.	3일
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 매니지먼트가 Android 운영 체제를 사용하는 관리 중인 모바일 기기에 대해 Google FCM(Firebase Cloud Messaging)을 사용하도록 구성되고 FCM 서버가 중앙 관리 서버에서 받은 일부 요청을 처리하지 못	3일

			하는 경우 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 Google Firebase 서비스 문서('다운스트림 메시지 오류 대응 코드')를 참조하십시오.	
FCM 서버에 FCM 메시지를 전송할 때 HTTP 오류 발생	4139	KLSRV_GCM_HTTP_ERROR	이 유형의 이벤트는 모바일 기기 매니지먼트가 Google FCM(Firebase Cloud Messaging)을 사용하여 Android 운영 체제를 사용하는 관리 중인 모바일 기기를 연결하도록 모바일 기기 매니지먼트를 구성하고 FCM 서버가 200(OK) 이외의 HTTP 코드를 사용하여 중앙 관리 서버 요청으로 돌아가는 경우 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 Google Firebase 서비스 문서('다운스트림 메시지 오류 대응 코드')를 참조하십시오. • 프록시 서버 측의 문제입니다(프록시 서버를 사용하는 경우). 이벤트 세부 정보에서 HTTP 코드를 읽고 그에 따라 대응하십시오.	3일
FCM 서버로 FCM 메시지 전송 실패	4140	KLSRV_GCM_GENERAL_ERROR	이 유형의 이벤트는 Google 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.	3일
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.	3일
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 확인합니다. 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. 이때 중앙 관리 서버 데이터베이스에서 애플리케이션 제어 이벤트 저장과 관련된 Kaspersky Endpoint Security for Linux 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.	3일

			DBMS 선택에 대한 정보를 검토합니다.	
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.	3일
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.	3일
새로운 Kaspersky 소프트웨어 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. Kaspersky Security Center 웹 콘솔을 사용하여 업데이트를 승인 또는 거부하십시오.	3일
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 개수 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

중앙 관리 서버 정보 이벤트

표에는 심각도가 **정보**인 Kaspersky Security Center Linux 중앙 관리 서버 이벤트가 나와 있습니다.

중앙 관리 서버 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간	비고
이 라이센스 키의 90% 이상을 사용하고 있습니다	4097	KLSRV_EV_LICENSE_CHECK_90	3일	
새 기기가 탐지되었습니다	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	3일	
기기가 자동으로 그룹에 추가되었습니다	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	3일	
기기가 네트워크에 오랫동안 접속하지 않아 그룹에서 삭제되었습니다	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	3일	
유료 애플리케이션 그룹 중 하나에서 라이센스를 설치할 수 있는 최대 수량을 곧 초과합니다(95% 이상 사용 중)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	3일	
분석을 위해 Kaspersky로 전송해야 할 파일이 있습니다	4131	KLSRV_APS_FILE_APPEARED	3일	
FCM 인스턴스 ID가 이 모바일 기기에서 변경되었습니다	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	3일	
업데이트 파일이 지정한 폴더에 성공적으로 복사되었습니다	4122	KLSRV_UPD_REPL_OK	3일	
보조 중앙 관리 서버에 연결되었습니다	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	3일	
기본 중앙 관리 서버에 연결되었습니다	4117	KLSRV_EV_MASTER_SRV_CONNECTED	3일	
데이터베이스가 업데이트되었습니다	4144	KLSRV_UPD_BASES_UPDATED	3일	

감사: 중앙 관리 서버로의 연결이 확립되었습니다	4147	KLAUD_EV_SERVERCONNECT	3일	
감사: 개체가 수정되었습니다	4148	KLAUD_EV_OBJECTMODIFY	3일	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	3일	예를 들어 이 이벤트는 오류로 작업이 실패했을 때 발생합니다.
감사: 그룹 설정이 수정되었습니다	4149	KLAUD_EV_ADMGROUP_CHANGED	3일	
감사: 중앙 관리 서버와의 연결이 종료되었습니다	4151	KLAUD_EV_SERVERDISCONNECT	3일	
감사: 개체 속성이 수정되었습니다	4152	KLAUD_EV_OBJECTPROPMODIFIED	3일	이 이벤트는 다음 속성의 변경 사항을 추적합니다. • 사용자 • 라이센스 • 서버 • 가상 서버
감사: 사용자 권한이 수정되었습니다	4153	KLAUD_EV_OBJECTACLMODIFIED	3일	

네트워크 에이전트 이벤트

이 섹션에는 네트워크 에이전트와 관련된 이벤트에 대한 정보가 있습니다.

네트워크 에이전트 경고 이벤트

아래의 표에 심각도가 **경고**인 Kaspersky Security Center 네트워크 에이전트 이벤트가 나와 있습니다.

네트워크 에이전트 경고 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간
인시던트 발생	549	GNRL_EV_APP_INCIDENT_OCCURED	3일

네트워크 에이전트 정보 이벤트

아래 표에는 심각도가 **정보**인 Kaspersky Security Center 네트워크 에이전트 이벤트가 나와 있습니다.

네트워크 에이전트 정보 이벤트

이벤트 유형 표시 이름	이벤트 유형 ID	이벤트 유형	기본 저장 기간
애플리케이션을 설치했습니다	7703	KLNAG_EV_INV_APP_INSTALLED	3일
애플리케이션을 제거했습니다	7704	KLNAG_EV_INV_APP_UNINSTALLED	3일
감시 중인 애플리케이션이 설치되었습니다	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	3일
감시 중인 애플리케이션이 제거되었습니다	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	3일
새 기기가 추가되었습니다	7708	KLNAG_EV_DEVICE_ARRIVAL	3일
기기가 제거되었습니다	7709	KLNAG_EV_DEVICE_REMOVE	3일
새 기기가 탐지되었습니다	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	3일
기기가 인증되었습니다	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	3일

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(Kaspersky Endpoint Security for Linux 등)이 하나 또는 여러 개의 관리 중인 장치에 설치되어 있으면, 같은 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** 섹션을 선택합니다.
3. **자주 등록된 이벤트 차단** 섹션:
   - 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** 섹션을 선택합니다.
3. **자주 등록된 이벤트 차단** 섹션에서 차단을 제거하려는 자주 등록된 이벤트 유형을 선택합니다.
4. **차단 제거** 버튼을 누릅니다.

자주 등록된 이벤트가 자주 등록된 이벤트 목록에서 제거됩니다. 중앙 관리 서버에서 이 유형의 이벤트를 수신합니다.

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.

만약 데이터베이스에서 이벤트의 개수가 관리자가 지정한 값에 도달할 경우에는 애플리케이션은 가장 오래된 이벤트를 삭제하고 새로운 이벤트로 쓰게 됩니다. 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.

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 Center Linux는 중요하다고 판단하는 모든 이벤트에 대한 알림을 전송하여 조직 네트워크 모니터링 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 백과 사전과 같은 Kaspersky 리소스에 대한 링크가 포함됩니다)
   - **Kaspersky 뉴스** (여기에는 Kaspersky 애플리케이션 릴리스에 대한 정보가 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 14 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 Center Linux는 관리 중인 장치마다 상태를 할당합니다. 특정 상태는 사용자가 정의한 조건이 충족되는지 여부에 따라 달라집니다. 장치에 상태를 할당할 때 Kaspersky Security Center Linux가 네트워크에 있는 장치의 가시성 플래그를 고려할 때도 있습니다(아래 표 참조). Kaspersky Security Center Linux에서 2시간 내에 네트워크의 장치를 찾지 못하면 장치의 가시성 플래그가 *확인되지 않음*으로 설정됩니다.

상태는 다음과 같습니다.

- *심각*또는 *심각/존재 확인*
- *경고*또는 *경고/존재 확인*
- *정상*또는 *정상/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 버튼

		이 꺼져 있습니다.
너무 많은 바이러스가 탐지됨	바이러스 검사 작업 등의 바이러스 탐지를 위한 작업을 통해 기기에서 일부 바이러스가 발견되었는데 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 바이러스 검사를 수행 안 함	장치가 네트워크에 표시되며 보안 제품이 장치에 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
재부팅 필요	기기가 네트워크에 표시되지만 선택한 이유 중 하나로 인해 애플리케이션이 지정된 시간 간격보다 오랫동안 기기 다시 시작을 요구합니다.	0분 이상
비-호환 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.
만료된 라이센스	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.	0일 이상
처리 안 된 인시던트가 있음	기기에서 처리되지 않은 일부 인시던트가 발견되었습니다. 인시던트는 클라이언트 기기에 설치된 관리 중인 Kaspersky 애플리케이션을 통해 자동으로 또는 수동으로 관리자에 의해 생성될 수 있습니다.	• 토글 버튼이 꺼져 있습니다.

		• 토글 버튼이 켜져 있습니다.
애플리케이션에서 정의된 기기 상태	관리 애플리케이션이 기기 상태를 정의합니다.	• 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 연결 끊김	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.	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 Center Linux에서는 지정한 조건 충족 시 관리 그룹의 장치 상태를 자동 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 **7일 이상**이면 클라이언트 기기에 *경고* 상태가 할당되고 값이 **7일 이상이면** *심각*상태가 할당됩니다.

Kaspersky Security Center Linux를 이전 버전에서 업그레이드하면, *심각*또는 *경고* 상태 할당을 위한 **데이터베이스가 오래됨** 조건 값이 변경되지 않습니다.

Kaspersky Security Center Linux에서 장치에 상태를 할당할 때, 몇 가지 조건(조건 설명 열 참조)에서 가시성 플래그를 고려합니다. 예를 들어, 데이터베이스가 오래됨 조건이 충족되어서 관리 중인 기기에 *심각*상태가 할당되었고 나중에 기기의 가시성 플래그가 설정되었다면 기기에는 *확인*상태가 할당됩니다.

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 **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 **지정된 경우 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 **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 **지정된 경우 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 Center Linux에서 발생하는 이벤트에 대한 알림을 구성할 수 있습니다. 선택한 알림 방법에 따라 다음 유형의 알림을 사용할 수 있습니다.

- 이메일 – 이벤트가 발생하면 Kaspersky Security Center Linux에서 지정된 이메일 주소로 알림을 보냅니다.
- SMS – 이벤트가 발생하면 Kaspersky Security Center Linux에서 지정된 전화번호로 알림을 보냅니다.
- 실행 파일 - 이벤트가 발생하면 실행 파일이 중앙 관리 서버에서 실행됩니다.

Kaspersky Security Center Linux에서 발생하는 이벤트의 알림 전달을 구성하려면:

1. 화면 위쪽에서 필요한 중앙 관리 서버 이름 옆의 설정 아이콘()을 누릅니다.
   일반 탭이 선택되어 있는 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.

  SMTP 서버 필드에서 세미콜론으로 구분해 이메일 서버 주소를 지정합니다. 다음 값을 사용할 수 있습니다:

  - IPv4 또는 IPv6 주소
  - SMTP 서버의 DNS 이름

  SMTP 서버 포트 필드에서 SMTP 서버 통신 포트의 번호를 지정합니다. 기본 포트 번호는 25입니다.

  DNS MX 조회 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 조회 사용 옵션을 활성화하고 TLS 설정을 활성화하지 않는 경우에는 이메일 알림 전송을 위한 ㅜ가 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 Center Linux는 SMTP 서버의 인증서가 신뢰하는 인증 기관의 서명을 받았는지도 확인합니다. 신뢰하는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하면, Kaspersky Security Center Linux가 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 누르면 알림을 제대로 구성했는지 확인할 수 있습니다. 애플리케이션은 지정한 이메일 주소로 테스트 알림을 보냅니다.

  받는 사람(이메일 주소) 필드에서 애플리케이션이 알림을 보낼 이메일 주소를 지정합니다. 이 필드에서 세미콜론으로 구분해 여러 주소를 지정할 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: 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.

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.

- 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
- 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.

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 Center Linux는 SMTP 서버의 인증서가 신뢰하는 인증 기관의 서명을 받았는지도 확인합니다. 신뢰하는 인증 기관에서 SMTP 서버의 인증서를 수신하지 못하면, Kaspersky Security Center Linux가 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".

테스트 메시지 전송를 누르면 알림을 제대로 구성했는지 확인할 수 있습니다. 애플리케이션은 지정한 수신자에게 테스트 알림을 보냅니다.

알림 수 제한 구성 링크를 누르면 애플리케이션이 지정된 시간 간격 동안 보낼 수 있는 최대 알림 수를 지정할 수 있습니다.

- **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 Center Linux에서 발생하는 모든 이벤트에 적용됩니다.

중앙 관리 서버 설정, 정책 설정 또는 애플리케이션 설정의 **이벤트 구성** 섹션에서 특정 이벤트에 대한 알림 설정을 재정의할 수 있습니다.

테스트 알림

애플리케이션은 이벤트 알림의 배포 여부 확인을 위해 클라이언트 장치의 EICAR 테스트 바이러스 탐지 알림을 사용합니다.

이벤트 알림 배포를 확인하려면 다음과 같이 하십시오:

1. 클라이언트 장치에 대한 실시간 파일 시스템 보호 작업을 중지하고 EICAR 테스트 바이러스를 클라이언트 장치로 복사합니다. 그 후 파일 시스템의 실시간 보호를 다시 활성화합니다.
2. 관리 그룹의 클라이언트 장치 또는 EICAR 테스트 바이러스가 있는 장치를 포함하는 특정 장치에 대해 검사 작업을 실행합니다.

   검사 작업이 올바르게 구성되면 테스트 바이러스가 탐지됩니다. 알림이 올바르게 구성된 경우 바이러스가 탐지되었다는 알림이 표시됩니다.

테스트 바이러스 탐지 기록을 열려면:

1. 메인 메뉴에서 **모니터링 및 보고 → 이벤트 조회**로 이동합니다.
2. **최근 이벤트** 조회 이름을 클릭합니다.

   창이 열리면 테스트 바이러스에 대한 알림이 표시됩니다.

EICAR 테스트 바이러스는 장치에 피해를 줄 수 있는 코드를 포함하지 않습니다. 그러나 제조업체 대부분의 보안 제품은 이 파일을 바이러스로 식별합니다. 공식 EICAR 웹사이트에서 테스트 바이러스를 다운로드할 수 있습니다.

실행 파일을 실행하면 표시되는 이벤트 알림

Kaspersky Security Center Linux는 실행 파일을 실행하여 클라이언트 장치의 이벤트에 대한 알림을 관리자에게 제공할 수 있습니다. 실행 파일은 관리자에게 전달할 이벤트 자리 표시자와 함께 다른 실행 파일을 반드시 포함해야 합니다.

이벤트를 설명하기 위한 자리 표시자

자리 표시자	자리 표시자 설명
%SEVERITY%	이벤트 심각도
%COMPUTER%	이벤트가 발생한 기기 이름
%DOMAIN%	도메인
%EVENT%	이벤트
%DESCR%	이벤트 설명
%RISE_TIME%	만든 시간
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	작업 이름
%KL_PRODUCT%	Kaspersky Security Center Linux 네트워크 에이전트
%KL_VERSION%	네트워크 에이전트 버전 번호
%HOST_IP%	IP 주소

%HOST_CONN_IP%	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 활성화됩니다. 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 14 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. 공지를 받고 싶지 않으면 이 기능을 비활성화할 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 공지을 비활성화하려면 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 **Kaspersky 공지** 섹션을 선택합니다.
3. 토글 버튼을 **보안 관련 공지가 비활성화됨** 위치로 전환합니다.
4. **저장** 버튼을 누릅니다.

   Kaspersky 공지가 비활성화됩니다.

SIEM 시스템으로 이벤트 내보내기

이 섹션에서는 SIEM 시스템으로 이벤트 내보내기를 구성하는 방법을 설명합니다.

시나리오: SIEM 시스템으로 이벤트 내보내기 구성

Kaspersky Security Center Linux에서는 Syslog 형식을 사용하는 모든 SIEM 시스템으로 내보내기 방식과 Kaspersky Security Center 데이터베이스에서 직접 SIEM 시스템으로 이벤트 내보내기 방식 중 하나로 SIEM 시스템으로 이벤트 내보내기를 구성할 수 있습니다. 이 시나리오를 완성하면 중앙 관리 서버가 이벤트를 SIEM 시스템에 자동으로 전송합니다.

필수 구성 요소

Kaspersky Security Center Linux에서 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 Center Linux에서 이벤트를 수신하도록 SIEM 시스템 구성**

  방법 지침: SIEM 시스템에서 이벤트 내보내기 구성

- **SIEM 시스템으로 내보낼 이벤트 선택**

  SIEM 시스템으로 내보낼 이벤트를 선택합니다. 먼저, 관리 중인 Kaspersky 애플리케이션 전체에서 발생하는 일반 이벤트를 표시합니다. 그런 다음 관리 중인 특정 Kaspersky 애플리케이션에 대한 이벤트를 표시할 수 있습니다.

- **SIEM 시스템으로 이벤트 내보내기 구성**

  다음 중 한 가지 방법으로 이벤트를 내보낼 수 있습니다:

  - TCP 프로토콜에서 TCP/IP, UDP, TLS 중 하나 사용
  - Kaspersky Security Center 데이터베이스에서 직접 이벤트 내보내기 사용(공용 보기 세트는 Kaspersky Security Center 데이터베이스에 제공됩니다. 이러한 공용 보기에 대한 설명은 klakdb.chm 문서에서 확인할 수 있습니다.)

결과

내보낼 이벤트 선택 시, SIEM 시스템으로 이벤트 내보내기를 구성한 후 내보내기 결과를 볼 수 있습니다.

시작하기 전에

Kaspersky Security Center Linux에서 이벤트 자동 내보내기를 설정할 때는 몇 가지 SIEM 시스템 설정을 지정해야 합니다. Kaspersky Security Center Linux 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 Center Linux와 SIEM 시스템 서버 간의 연결을 설정하는 데 사용되는 포트 번호입니다. Kaspersky Security Center Linux 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

- **프로토콜**

  Kaspersky Security Center Linux에서 SIEM 시스템으로 메시지를 전송하는 데 사용되는 프로토콜입니다. Kaspersky Security Center Linux 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

Kaspersky Security Center Linux의 이벤트 정보

Kaspersky Security Center Linux에서는 관리 중인 장치에 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 기기 그룹에서 발생하는 보안 시스템 이벤트에 신속하게 대응할 수 있습니다.

유형별 이벤트

Kaspersky Security Center Linux에는 다음 유형의 이벤트가 있습니다.

- 일반 이벤트. 이러한 이벤트는 모든 관리 중인 Kaspersky 애플리케이션에서 발생합니다. 일반 이벤트의 예로 바이러스 급증가 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.

출처별 이벤트

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.

이벤트는 다음 애플리케이션에서 생성할 수 있습니다.

- Kaspersky Security Center Linux 구성 요소:
  - 중앙 관리 서버
  - 네트워크 에이전트
- 관리 중인 Kaspersky 애플리케이션
  관리 중인 Kaspersky 애플리케이션에서 생성된 이벤트에 대한 자세한 내용은 해당 애플리케이션의 설명서를 참조하십시오.

심각도별 이벤트

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 기간에 Kaspersky Security Center Linux에서 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 Center Linux에서 외부 SIEM 시스템으로 이벤트를 내보내는 프로세스의 당사자는 이벤트 발신자(Kaspersky Security Center Linux)와 이벤트 수신자(SIEM 시스템)입니다. 이벤트를 성공적으로 내보내려면 SIEM 시스템 및 Kaspersky Security Center Linux 관리 콘솔에서 이를 구성해야 합니다. 구성 순서는 중요하지 않습니다. 즉, Kaspersky Security Center Linux에서 이벤트 전송을 구성한 후에 SIEM 시스템의 이벤트 수신을 구성할 수도 있고 그 반대 순서로 구성할 수도 있습니다.

이벤트 내보내기의 Syslog 형식

모든 SIEM 시스템에 Syslog 형식의 이벤트를 보낼 수 있습니다. Syslog 형식을 사용하여 중앙 관리 서버 및 관리 중인 장치에 설치된 Kaspersky 애플리케이션에서 발생하는 모든 이벤트를 전달할 수 있습니다. Syslog 형식으로 이벤트를 내보낼 때는 SIEM 시스템으로 전달할 이벤트 유형을 정확하게 선택할 수 있습니다.

SIEM 시스템의 이벤트 수신

SIEM 시스템은 Kaspersky Security Center Linux에서 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 Center Linex에서 외부 SIEM 시스템으로 이벤트를 내보내는 프로세스의 당사자는 이벤트 발신자(Kaspersky Security Center Linux)와 이벤트 수신자(SIEM 시스템)입니다. SIEM 시스템 및 Kaspersky Security Center Linux 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 Center Linux에서 보낸 이벤트를 받으려면 SIEM 시스템에서 수신자를 설정해야 합니다. 일반적으로는 SIEM 시스템에서 다음 설정을 지정해야 합니다:

- **내보내기 프로토콜**

  UDP, TCP, TLS 등 TCP를 통한 메시지 전송 프로토콜. 이 프로토콜은 Kaspersky Security Center Linux에서 지정한 프로토콜과 같아야 합니다.

- **포트**

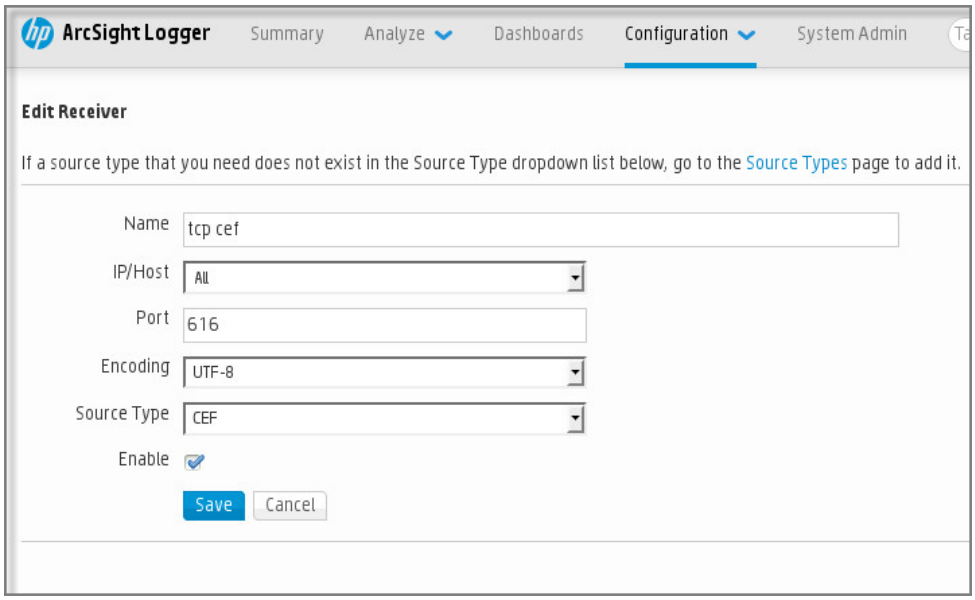
  Kaspersky Security Center Linux 연결을 위한 포트 번호를 지정합니다. 이 포트는 SIEM 시스템과의 구성 시 Kaspersky Security Center Linux에서 지정한 포트와 같아야 합니다.

- **데이터 형식**

  Syslog 형식을 지정합니다.

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. SIEM 시스템의 일부분인 메시지 파서는 메시지 컨텐츠를 이벤트 ID 심각도, 설명, 파라미터 등의 관련 필드로 분할하는 데 사용됩니다. 그러면 SIEM 시스템은 Kaspersky Security Center Linux에서 받은 이벤트를 처리하여 SIEM 시스템 데이터베이스에 저장할 수 있습니다.

각 SIEM 시스템에는 표준 메시지 파서 집합이 있습니다. Kaspersky에서도 QRadar, ArcSight 등의 일부 SIEM 시스템용 메시지 파서를 제공합니다. 해당 SIEM 시스템 웹사이트에서 이러한 메시지 파서를 다운로드할 수 있습니다. 수신자를 구성할 때 표준 메시지 파서 중 하나를 사용하거나 Kaspersky의 메시지 파서를 사용하도록 선택할 수 있습니다.

Syslog 형식으로 SIEM 시스템으로 내보내기 위한 이벤트 표시

이 섹션에서는 Syslog 형식으로 SIEM 시스템에 추가로 내보낼 이벤트를 표시하는 방법에 대해 설명합니다.

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 **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 **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:
   - 필요한 중앙 관리 서버 이름 옆의 설정 아이콘(🔧)을 누릅니다.
   - 메인 메뉴에서 **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.

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 Center Linux에서 외부 시스템으로 이벤트를 내보낼 때는 RFC 5424 표준이 사용됩니다.

Kaspersky Security Center Linux에서는 Syslog 형식을 사용해 외부 시스템으로 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 Center Linux를 구성합니다. 자동 내보내기 활성화 시, Kaspersky Security Center Linux가 즉시 이벤트 보내기를 시작합니다.
2. 외부 시스템으로 내보낼 이벤트 선택. 이 단계에서는 SIEM 시스템으로 내보낼 이벤트를 선택합니다.

SIEM 시스템으로 이벤트를 내보내기 위한 Kaspersky Security Center Linux 구성

이벤트를 SIEM 시스템으로 내보내려면, Kaspersky Security Center Linux에서 내보내기 프로세스를 구성해야 합니다.

Kaspersky Security Center 14 웹 콘솔에서 SIEM 시스템으로 내보내기를 구성하려면 다음과 같이 하십시오.

1. **콘솔 설정** 드롭다운 목록에서 **통합**을 선택합니다.
   콘솔 설정 창이 열립니다.
2. **통합** 탭을 선택합니다.
3. **통합** 탭에서 **SIEM** 섹션을 선택합니다.
4. **설정** 링크를 누릅니다.
   설정 내보내기 섹션이 열립니다.
5. **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 Center Linux와 SIEM 시스템 서버 간의 연결을 설정하는 데 사용되는 포트 번호입니다. Kaspersky Security Center Linux 설정과 SIEM 시스템의 수신기 설정에서 이 값을 지정할 수 있습니다.

- **프로토콜**

  SIEM 시스템으로 메시지를 전송하는 데 사용할 프로토콜을 선택합니다. TCP 프로토콜을 통해 TCP/IP, UDP 또는 TLS를 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 인증서 목록이 포함된 파일을 수신하여 Kaspersky Security Center Linux에 업로드할 수 있습니다. Kaspersky Security Center Linux가 SIEM 시스템 서버의 인증서에 신뢰하는 인증 기관의 서명이 있는지 확인합니다.
      신뢰할 수 있는 인증서를 추가하려면 **CA 인증서 파일 찾기** 버튼을 클릭한 다음 인증서를 업로드합니다.
    - **SHA 지문**. Kaspersky Security Center에 대한 SIEM 시스템 인증서의 SHA-1 지문을 지정할 수 있습니다. SHA-1 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 Center Linux는 SIEM 시스템 서버의 도메인 이름이 SIEM 시스템 서버 인증서의 대상 이름과 일치하지 않을 시 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 중 이름이 SIEM 시스템 인증서의 대상 이름과 일치하는 것이 있으면, Kaspersky Security Center Linux가 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. 결과적으로 Kaspersky Security Center Linux는 생성된 자체 서명 인증서를 저장하며, 사용자는 인증서의 공개 부분 또는 SHA1 지문을 SIEM 시스템에 전달할 수 있습니다.

6. 필요 시, 중앙 관리 서버 데이터베이스에서 보관된 이벤트를 내보내고 보관된 이벤트 내보내기를 시작할 시작 날짜를 설정할 수 있습니다.

   a. 링크에서 **내보내기 시작 날짜 설정**를 클릭합니다.

   b. 섹션이 열리면 **내보내기 시작 날짜** 필드에 시작 날짜를 지정합니다.

   c. **확인** 버튼을 누릅니다.

7. 옵션을 **SIEM 시스템 데이터베이스로 이벤트를 자동으로 내보내기 활성화됨** 위치로 전환합니다.

8. **저장** 버튼을 누릅니다.

SIEM 시스템으로 내보내기가 구성되었습니다. 이제 SIEM 시스템에서 이벤트 수신을 구성할 시, 중앙 관리 서버는 표시된 이벤트를 SIEM 시스템으로 내보냅니다. 내보내기 시작 날짜를 설정하면 중앙 관리 서버는 지정 날짜부터 중앙 관리 서버 데이터베이스에 저장된 표시된 이벤트도 내보냅니다.

데이터베이스에서 직접 이벤트 내보내기

Kaspersky Security Center Linux 인터페이스를 사용할 필요 없이 Kaspersky Security Center Linux 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

사용자의 편의를 위해 Kaspersky Security Center Linux 데이터베이스는 공용 보기 집합을 제공합니다. 이러한 공용 보기의 설명은 klakdb.chm 문서에서 확인할 수 있습니다.

v_akpub_ev_event 공용 보기에는 데이터베이스의 이벤트 파라미터를 나타내는 필드 집합이 포함되어 있습니다. 장치, 애플리케이션, 사용자 등, 기타 Kaspersky Security Center Linux 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 만드는 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 Linux 데이터베이스에 연결하는 데 필요한 파라미터 확인 방법에 대한 정보는 해당 섹션에 나와 있습니다.

klsql2 유틸리티를 사용하여 SQL 쿼리 생성

이 섹션에서는 klsql2 유틸리티를 사용하는 방법과 이를 사용하여 SQL 쿼리를 만드는 방법을 설명합니다. klsql2 유틸리티를 통해 SQL 쿼리를 만들 때는, 쿼리에서 Kaspersky Security Center Linux 공용 보기 주소를 직접 지정하므로 데이터베이스 이름과 접근 파라미터를 제공하지 않아도 됩니다.

klsql2 유틸리티를 사용하려면:

1. Kaspersky Security Center Linux 중앙 관리 서버가 설치된 장치에서 /opt/kaspersky/ksc64/sbin/klsql2 디렉터리로 이동합니다.

2. 이 디렉터리에서 src.sql 빈 파일을 만듭니다.

3. 원하는 텍스트 편집기에서 src.sql 파일을 엽니다.

4. src.sql 파일에 원하는 SQL 쿼리를 입력한 다음 파일을 저장합니다.

5. Kaspersky Security Center Linux 중앙 관리 서버를 설치한 장치의 명령줄에서 다음 명령을 입력하여 src.sql 파일에서 SQL 쿼리를 실행한 다음 result.xml 파일에 결과를 저장합니다.
   ```
   sudo ./klsql2 -i src.sql -o result.xml
   ```

6. 새로 작성된 result.xml 파일을 열어 쿼리 결과를 확인합니다.

src.sql 파일을 편집하여 공용 보기에 대해 원하는 쿼리를 만들 수 있습니다. 그런 후에 명령줄에서 쿼리를 실행하고 결과를 파일에 저장하면 됩니다.

klsql2 유틸리티의 SQL 쿼리 예제

이 섹션에서는 klsql2 유틸리티를 통해 만들 수 있는 SQL 쿼리의 예제를 제공합니다.

아래 그림에는 지난 7일 동안 기기에서 발생한 이벤트를 가져와서 발생 시간 순서대로 표시(최신 데이터가 먼저 표시됨)하는 과정이 나와 있습니다.

예:

```
SELECT
e.nId, /* 이벤트 식별자 */
e.tmRiseTime, /* time, 이벤트 발생 시간 */
e.strEventType, /* 이벤트 유형의 내부 이름 */
e.wstrEventTypeDisplayName, /* 이벤트의 표시되는 이름 */
e.wstrDescription, /* 이벤트의 표시되는 설명 */
e.wstrGroupName, /* 기기가 있는 그룹의 이름 */
h.wstrDisplayName, /* 이벤트가 발생한 기기의 표시되는 이름 */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* 이벤트가 발생한 기기의 IP 주소 */
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
```

Kaspersky Security Center Linux 데이터베이스 이름 확인

SQL Server, MySQL, MariaDB 데이터베이스 관리 도구를 통해 Kaspersky Security Center Linux 데이터베이스에 접근하려면, SQL 스크립트 편집기에서 데이터베이스에 연결할 수 있도록 데이터베이스 이름을 알아야 합니다.

Kaspersky Security Center Linux 데이터베이스의 이름을 확인하려면:

1. 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.

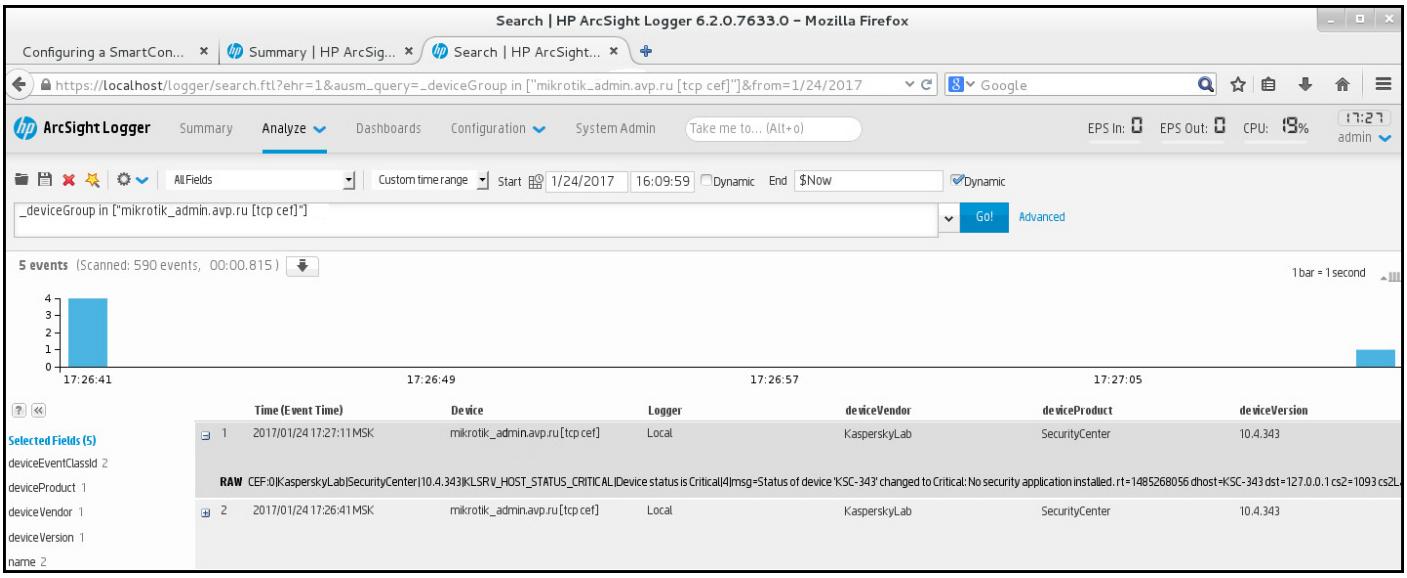
내보내기 결과 보기

이벤트 내보내기 절차가 정상적으로 완료되도록 제어할 수 있습니다. 이렇게 하려면 내보내기 이벤트가 포함된 메시지가 SIEM 시스템에서 수신되는지 확인합니다.

SIEM 시스템에서 Kaspersky Security Center Linux가 보낸 이벤트를 수신하여 적절하게 구문 분석하면, 양쪽의 구성이 모두 올바르게 된 것입니다. 그렇지 않을 시, Kaspersky Security Center Linux에서 지정한 설정을 SIEM 시스템의 구성과 대조하여 확인합니다.

아래 그림에는 ArcSight로 내보낸 이벤트가 나와 있습니다. 예를 들어 첫 번째 이벤트는 심각한 중앙 관리 서버 이벤트입니다: "*장치 상태가 위험입니다*".

SIEM 시스템에서의 내보내기 이벤트 표시 방식은 사용하는 SIEM 이벤트에 따라 다릅니다.



이벤트 예제

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 조회에서는 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 조회를 보려면 다음 단계를 따릅니다.

1. 메인 메뉴에서 **기기 → 기기 조회** 또는 **발견 및 배포 → 기기 조회** 섹션으로 이동합니다.
2. 조회 목록에서 관련 조회 이름을 누릅니다.

기기 조회 결과가 표시됩니다.

기기 조회 만들기

기기 조회를 만들려면 다음과 같이 하십시오:

1. 메인 메뉴에서 **기기 → 기기 조회**로 이동합니다.
   기기 조회 목록이 포함된 페이지가 표시됩니다.
2. **추가** 버튼을 누릅니다.
   기기 조회 설정 창이 열립니다.
3. 새 조회 이름을 입력합니다.
4. 기기 조회에 포함할 기기 유형을 지정합니다.
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

모두 펼치기 | 모두 접기

기기 조회를 구성하려면 다음과 같이 하십시오:

1. **기기 → 기기 조회**로 이동합니다.
   기기 조회 목록이 포함된 페이지가 표시됩니다.
2. 관련 사용자 정의 기기 조회를 누릅니다.
   기기 조회 설정 창이 열립니다.
3. **일반** 탭에서 이 조회에 기기를 포함하기 위해 충족해야 하는 조건을 지정합니다.
4. **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

이 옵션을 사용하면 특정 선택 조건이 반대로 적용됩니다. 즉, 조건을 충족하지 않는 모든 기기가 조회에 포함됩니다.
기본적으로 이 옵션은 비활성화되어 있습니다.

네트워크

네트워크 섹션에서는 네트워크 데이터에 따라 조회에 기기를 포함하는 데 사용할 기준을 지정할 수 있습니다.

- **기기 이름 또는 IP 주소**
- **Windows 도메인**

  지정된 작업 그룹에 포함된 모든 장치를 표시합니다.
- **관리 그룹**

  지정된 관리 그룹에 포함된 기기를 표시합니다.
- **설명**

  장치 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:

    SUSE Linux Enterprise Server 12 또는 **SUSE Linux Enterprise Server 15**와 같은 문구를 설명하려면 **SUSE Linux Enterprise Server 1?** 을 입력합니다.

    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.

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 기기는 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:
  - **활성됨**. 조회에 **중앙 관리 서버와 계속 연결 유지** 확인란을 선택한 기기가 포함됩니다.
  - **비활성됨**. 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 네트워크에서 표시되지 않는 기기를 조회에 포함시킵니다.
  - **어떤 값도 선택되지 않았습니다**. 기준이 적용되지 않습니다.

애플리케이션

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 Center 14로 관리 중인 기기**

  드롭다운 목록에서는 Kaspersky Security Center Linux로 관리 중인 장치를 조회에 포함할 수 있습니다.
  - **예**. 애플리케이션이 Kaspersky Security Center Linux로 관리 중인 장치를 조회에 포함합니다.
  - **아니요**. 애플리케이션이 Kaspersky Security Center Linux로 관리하지 않는 장치를 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 *XY*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 바이러스 검사 시간을 기준으로 클라이언트 기기를 검색할 수 있습니다. 입력 필드에서 마지막 바이러스 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) 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.

- **비-호환 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**

  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 일련 번호를 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)**

  장치 RAM 크기에 대한 값 범위입니다. 이 입력 필드의 범위와 일치하는 RAM이 있는 장치(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**. 가상 데스크톱 인프라(VDI)의 일부가 아닌 기기를 찾습니다.
  - **예**. VDI(가상 데스크톱 인프라)의 일부인 기기를 찾습니다.

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(*기기에서 보낸 데이터 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **협업 서버 보호 상태**

  서버 협업 보호 상태(*기기에서 보낸 데이터 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **메일 서버의 안티 바이러스 보호 상태**

  메일 서버 보호 상태(*기기에서 보낸 데이터 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)에 따라 기기를 검색합니다.

- **엔드포인트 센서 상태**

  엔드포인트 센서 구성 요소 상태(*기기에서 보낸 데이터 없음, 중지됨, 시작 중, 일시 중지됨, 실행 중, 실패*)를 기준으로 기기를 검색합니다.

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.

API 참조 가이드

이 Kaspersky Security Center OpenAPI 참조 가이드는 다음 작업을 지원하도록 설계되었습니다.

- 자동화 및 사용자 지정. 직접 처리하고 싶지 않은 작업을 자동화할 수 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. OpenAPI를 사용하여 클라이언트 애플리케이션을 개발할 수 있습니다.

화면 오른쪽에 있는 검색 필드를 사용하여 OpenAPI 참조 가이드에서 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).
2. 중앙 관리 서버가 설치된 장치의 KlAkOAPI.tar.gz 아카이브에서 KlAkOAPI 패키지를 설치합니다.

   OpenAPI 메소드를 호출하고, 중앙 관리 서버 및 KlAkOAPI 패키지가 설치된 장치에서만 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, 보조 중앙 관리 서버 추가 및 중앙 관리 서버 계층 삭제
지정된 호스트에 대한 연결 게이트웨이를 통해 네트워크 목록 파일 다운로드	연결 게이트웨이를 사용하여 필요한 장치의 네트워크 에이전트에 연결한 다음 네트워크 목록이 있는 파일을 기기에 다운로드합니다.	배포 지점 및 연결 게이트웨이 조정
기본 중앙 관리 서버 저장소에 저장된 라이센스 키를 보	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

조 중앙 관리 서버에 설치		
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
장치 작업 시작	연결 게이트웨이를 사용하여 필요한 장치의 네트워크 에이전트에 연결한 다음 필요한 작업을 실행할 수 있습니다.	수동으로 작업 시작
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.

Kaspersky Security Center 14 웹 콘솔과 다른 Kaspersky 솔루션 간의 통합

이 섹션에서는 Kaspersky Security Center 14 웹 콘솔에서 Kaspersky Endpoint Detection and Response, Kaspersky Managed Detection and Response와 같은 다른 Kaspersky 애플리케이션에 대한 액세스를 구성하는 방법에 대해 설명합니다.

KATA / KEDR 웹 콘솔에 대한 접근 구성

KATA(Kaspersky Anti Targeted Attack) 및 KEDR(Kaspersky Endpoint Detection and Response)은 Kaspersky Anti Targeted Attack Platform 의 두 가지 기능 블록입니다. Kaspersky Anti Targeted Attack Platform용 웹 콘솔(KATA / KEDR 웹 콘솔)을 통해 이러한 기능 블록을 관리할 수 있습니다. Kaspersky Security Center 14 웹 콘솔과 KATA/KEDR 웹 콘솔을 모두 사용 시, Kaspersky Security Center 14 웹 콘솔의 인터페이스에서 KATA/KEDR 웹 콘솔에 대한 접근을 직접 구성할 수 있습니다.

KATA / KEDR 웹 콘솔에 대한 접근을 구성하려면 다음 단계를 따릅니다.

1. 메인 애플리케이션 창의 화면 상단에서 **콘솔 설정**을 누릅니다.
2. 드롭다운 메뉴에서 **통합**을 선택합니다.
   콘솔 설정 창이 열립니다.
3. **통합** 탭에 있는 **KATA/KEDR 웹 콘솔 URL** 필드에서 KATA/KEDR 웹 콘솔의 URL을 입력합니다.
4. **저장** 버튼을 누릅니다.

고급 관리 드롭다운 목록이 메인 애플리케이션 창에 추가됩니다. 이 메뉴를 사용하여 KATA / KEDR 웹 콘솔을 열 수 있습니다. **고급 사이버 보안**을(를) 누르면 지정한 URL이 포함된 새 탭이 브라우저에 열립니다.

백그라운드 연결 설정

Kaspersky Managed Detection and Response (MDR) 등의 다른 Kaspersky 애플리케이션과 Kaspersky Security Center 간의 상호작용을 구성하려면, Kaspersky Security Center 14 웹 콘솔과 중앙 관리 서버 간의 백그라운드 연결을 구성해야 합니다. 계정에 **일반 기능: 사용자 권한** 기능 영역의 개체 ACL 수정 권한이 있을 때만 이 연결을 설정할 수 있습니다.

Kaspersky Managed Detection and Response와 Windows 기반 Kaspersky Security Center 버전 간의 상호작용만 구성할 수 있습니다.

백그라운드 연결 설정 방법:

1. **콘솔 설정** 드롭다운 목록에서 **통합**을 선택합니다.
   콘솔 설정 창이 열립니다.
2. **통합** 탭을 선택합니다.
3. **통합** 탭에서 **통합** 섹션을 선택합니다.
4. 백그라운드 연결 설정 토글 버튼을 **통합을 위한 백그라운드 연결 설정 활성화됨** 위치로 전환합니다.
5. 열려 있는 **Kaspersky Security Center 웹 콘솔 서버에서 백그라운드 연결을 설정하는 서비스가 시작됩니다** 섹션에서 **확인** 버튼을 누릅니다.

Kaspersky Security Center 14 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 Kaspersky Security Center 14 웹 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.

기술 지원 연락처

이 섹션에서는 기술 지원을 받는 방법과 기술 지원이 제공되는 약관에 대해 설명합니다.

기술 지원을 받는 방법

Kaspersky Security Center Linux 문서 또는 Kaspersky Security Center Linux에 대한 정보를 제공하는 출처에서 문제 해결 방법을 찾을 수 없다면, Kaspersky 기술 지원에 문의하십시오. 기술 지원 전문가가 Kaspersky Security Center Linux 설치 및 사용과 관련된 모든 질문에 답해 드립니다.

Kaspersky는 수명 주기 동안 Kaspersky Security Center Linux에 대한 지원을 제공합니다(제품 지원 수명 주기 페이지 참조). 기술 지원에 문의하기 전에 지원 규칙 을 읽어보시기 바랍니다.

다음 방법 중 하나로 기술 지원에 문의할 수 있습니다:

- 기술 지원 웹사이트 방문
- Kaspersky CompanyAccount 포털 에서 기술 지원 요청

Kaspersky CompanyAccount를 통해 기술 지원 받기

Kaspersky CompanyAccount 는 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 웹사이트 를 참조하십시오.

애플리케이션에 대한 정보 출처

Kaspersky 웹사이트의 Kaspersky Security Center 페이지

Kaspersky 웹사이트의 Kaspersky Security Center 페이지 에서 애플리케이션과 기능, 특징과 같은 일반적인 정보를 확인할 수 있습니다.

기술 자료의 Kaspersky Security Center 페이지

*기술 자료*는 Kaspersky 기술 지원 웹사이트에 있는 섹션입니다.

기술 자료의 Kaspersky Security Center 페이지에서 애플리케이션의 구매, 설치 및 사용에 관한 유용한 정보, 권장 사항 및 자주 하는 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 포럼 에서 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.

알려진 문제

Kaspersky Security Center Linux에는 애플리케이션 작동에 심각한 영향을 주지 않는 몇 가지 제한이 있습니다.

- 목록에 20개 이상의 항목이 포함되어 있는 상태에서(이때 항목이 여러 페이지에 표시됨) **모두 선택** 확인란을 선택하면 웹 콘솔은 현재 페이지에 표시된 항목만 선택합니다.
- *중앙 관리 서버 저장소에 업데이트 다운로드* 작업과 *배포 지점 저장소에 업데이트 다운로드* 작업에서, 암호로 보호된 로컬 또는 네트워크 폴더를 업데이트 경로로 지정하면 사용자 인증이 작동하지 않습니다. 이 문제를 해결하려면 먼저 암호로 보호된 폴더를 탑재한 다음 운영 체제 등을 통해

필요한 자격 증명을 지정합니다. 그런 다음 업데이트 다운로드 작업 시 이 폴더를 업데이트 경로로 선택할 수 있습니다. Kaspersky Security Center에서는 자격 증명을 입력할 필요가 없습니다.

- 작업 스케줄에서 옵션을 **즉시**로 설정하고 변경 사항을 저장하면 *중앙 관리 서버 변경* 작업이 자동 시작되지 않습니다.
- 다른 브라우저에서 Kaspersky Security Center 14 웹 콘솔을 열고 중앙 관리 서버 속성 창에서 중앙 관리 서버 인증서 파일을 다운로드하면 다운로드한 파일의 이름이 달라집니다.
- **백업** 저장소(**동작 → 저장소 → 백업**)에서 개체를 복원하거나 개체를 Kaspersky로 전송하려고 하면 오류가 발생합니다.
- Kaspersky Endpoint Security for Linux의 부모 정책에서 잠긴 설정은 자식 정책으로 상속되지만 잠기지는 않습니다.
- 관리 중인 장치에서 중앙 관리 서버로 전송된 하드웨어 정보는 완전하지 않을 수 있으며, 일부 하드웨어 항목은 지정되지 않을 수 있습니다.
- Kaspersky Endpoint Security for Linux 정책의 애플리케이션 제어 기능에 추가한 애플리케이션 카테고리는 삭제할 수 있습니다.
- 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.
- Kaspersky Security Center 14 웹 콘솔 설치에 대한 응답 파일의 webConsoleAccount 및 managementServiceAccount 파라미터에서 사용자 지정 사용자 계정을 지정하고 이 계정이 다른 보안 그룹에 속할 시, Kaspersky Security Center 14 웹 콘솔을 설치해도 작동하지 않습니다.
- Astra Linux 64비트 에디션에서는 klnagent-astra 패키지를 klnagent64_14 패키지로 업그레이드할 수 없습니다. 업그레이드 대신 이전 패키지 klnagent64-astra가 제거되고 새 패키지 klnagent64가 설치되므로, klnagent64_14 패키지가 있는 장치의 새 아이콘 추가됩니다. 이 장치의 이전 아이콘을 제거할 수 있습니다.

용어집

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.

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:

- 장치가 인터넷에 연결되어 있지 않습니다.
- 국가 또는 기업 LAN 외부로의 데이터 전송이 법률이나 기업 보안 정책에 의해 금지됩니다.

Kaspersky Security Center 관리자

Kaspersky Security Center 원격 중앙 집중식 관리 시스템을 통해 애플리케이션 작동을 관리하는 사용자입니다.

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 Web Server

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 Center 운영자

Kaspersky Security Center를 통해 관리되는 보호 시스템의 상태 및 작동을 감시하는 사용자입니다.

Kaspersky 업데이트 서버

Kaspersky 애플리케이션이 데이터베이스와 애플리케이션 모듈의 업데이트를 다운로드하는 Kaspersky HTTP(S) 서버입니다.

SSL

인터넷 및 로컬 네트워크에서 사용되는 데이터 암호화 프로토콜입니다. SSL(Secure Sockets Layer)은 웹 애플리케이션에서 클라이언트와 서버 간의 보안 연결을 만드는 데 사용됩니다.

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.

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 콘솔은 Kaspersky Security Center 14 웹 콘솔과 유사합니다.

관리자 권한

한 Exchange 조직 내에서 Exchange 개체를 관리하는 데 필요한 사용자의 권한 수준입니다.

관리자 워크스테이션

Kaspersky Security Center 14 웹 콘솔을 여는 장치. 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.

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.

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 Center Linux를 통한 관리를 지원하지 않는 Kaspersky 애플리케이션 또는 제삼자 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.

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.

역할 그룹

동일한 관리 권한이 부여된 Exchange ActiveSync 모바일 기기의 사용자 그룹입니다.

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 Center Linux에서 제공하는 도구로 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 Center Linux에서 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 컴퓨터 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:

- Kaspersky Security Center 14 웹 콘솔 연결 시 중앙 관리 서버 인증
- 관리 중인 장치에서 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 서브스크립션 키

현재 사용하지 않고 있는 애플리케이션의 사용 권한을 인증하는 키입니다.

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.

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.

프로필

Microsoft Exchange 서버에 연결할 때의 동작을 정의하는 Exchange 모바일 기기 의 설정 모음입니다.

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 디렉터리에 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.

Apache 및 Apache 깃털 로고는 Apache Software Foundation의 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, Cisco Systems, IOS는 미국 및 기타 특정 국가에서 Cisco Systems, Inc. 및/또는 그 자회사의 등록 상표 또는 상표입니다.

Citrix, XenServer는 Citrix Systems, Inc. 및/또는 해당 자회사 하나 이상의 상표이며 미국 특허청 및 기타 국가에 등록되어 있을 수 있습니다.

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.

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, Google Public DNS, Hangouts, YouTube는 Google LLC의 상표입니다.

EulerOS, FusionCompute, FusionSphere는 Huawei Technologies Co., Ltd.의 상표입니다.

Intel, Core, Xeon은 미국 및 기타 국가에서 Intel Corporation의 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.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, Windows Azure는 미국 및 기타 국가에서 Microsoft 그룹의 상표입니다.

Mozilla, Firefox, Thunderbird는 미국 및 기타 국가에서 Mozilla Foundation의 상표입니다.

Novell은 미국 및 기타 국가에서 Novell Enterprises Inc.의 등록 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.

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.

VMware, VMware vSphere 및 VMware Workstation은 미국 및/또는 기타 관할 지역에서 VMware, Inc.의 등록 상표 또는 상표입니다.

UNIX는 미국 및 기타 국가에서 X/Open Company Limited를 통해 독점 사용이 허가된 등록 상표입니다.

Zabbix는 Zabbix SIA의 등록 상표입니다.