kaspersky

Kaspersky Endpoint Security for Linux

目录

Kaspersky Endpoint Security 12.1 for Linux

Kaspersky Endpoint Security 12.1 for Linux（“Kaspersky Endpoint Security”，“应用程序”）专门用于保护运行 Linux® 操作系统的设备免受各种类型的威胁，包括网络和诈骗攻击。

该应用程序能够保护物理设备和虚拟机。可将 Kaspersky Endpoint Security 用作 Kaspersky Security for Virtualization Light Agent 的一部分，以保护运行 Linux 客户机操作系统的虚拟机。

该应用程序的以下功能组件和任务提供用于保护和控制设备的主要功能：

- **文件威胁防护**可防止用户设备的文件系统受到感染。*文件威胁防护*组件在 Kaspersky Endpoint Security 启动时自动启动，并实时扫描所有打开、保存和启动的文件。

  您还可以使用以下扫描任务按需扫描受保护的设备：

  - 恶意软件扫描。应用程序扫描设备本地磁盘上的文件系统对象中以及通过 SMB 和 NFS 协议访问的已挂载和已共享的资源中是否存在恶意软件。您可以使用此任务对设备执行全盘扫描或自定义扫描。
  - 关键区域扫描。应用程序会扫描引导扇区、启动对象、进程内存和内核内存。

- **可移动驱动器扫描**。*可移动驱动器扫描*组件允许您实时监控可移动驱动器与设备的连接，并扫描可移动驱动器及其引导扇区中是否存在恶意软件。Kaspersky Endpoint Security 会扫描以下可移动驱动器：CD、DVD、蓝光光盘、闪存驱动器（包括 USB 调制解调器）、外部硬盘驱动器和软盘。

- **容器扫描**。*容器扫描*组件允许您实时扫描命名空间和正在运行的容器中是否存在恶意软件。支持与 Docker 容器管理系统、CRI-O 框架以及 Podman 和 runc 实用程序集成。您可以使用“*容器扫描*”任务按需扫描容器和镜像。

- **Web 威胁防护**。*Web 威胁防护*组件允许您扫描入站流量，防止从互联网下载恶意文件，还可以阻止网络钓鱼、广告软件和其他恶意网站。Kaspersky Endpoint Security 可以扫描加密连接。

- **网络威胁防护**。使用*网络威胁防护*组件，您可以扫描入站网络流量，查找典型的网络攻击活动。

- **防火墙管理**。*防火墙管理*组件允许您监控操作系统的防火墙设置，并根据您配置的网络数据包规则过滤所有网络活动。

- **反加密勒索**。*反加密勒索*组件允许您扫描远程设备使用 SMB/NFS 协议通过网络访问对本地目录中文件的调用，防止文件受到远程恶意加密。

- **设备控制**。*设备控制*组件允许您管理用户对已安装到或已连接到客户端设备的设备（例如，硬盘驱动器、摄像头或 Wi-Fi 模块）的访问。这样，您可以在连接外部设备时保护客户端设备免受感染，并防止数据丢失或泄漏。用户对设备的访问受您配置的访问制度和访问规则的约束。

- **应用程序控制**。*应用程序控制*组件允许您管理用户设备上应用程序的启动。通过限制对应用程序的访问，能够降低设备感染的风险。应用程序启动受您配置的应用程序控制规则的约束。

- **清查**。“*清查*”任务提供有关客户端设备上存储的所有应用程序可执行文件的信息。该信息可用于创建应用程序控制规则。

- **Web 控制**。*Web 控制*组件可控制用户对 Web 资源的访问。这样可以减少流量消耗和对工作时间的不当使用。如果用户尝试打开受 Web 控制限制访问的网站， Kaspersky Endpoint Security 会阻止访问或显示警告。

- **行为检测**。*行为检测*组件允许您监控操作系统中应用程序的任何恶意活动。当检测到恶意活动时，Kaspersky Endpoint Security 可以终止执行恶意活动的应用程序进程。

- **系统完整性监控**允许您跟踪操作系统的文件和目录更改。*系统完整性监控*组件实时监控组件设置中指定的监控范围内的对象所执行的操作。您可以使用“*系统完整性检查*”任务来按需检查系统的完整性。执行检查时，将

监控范围内对象的当前状态与其初始状态进行比较，该初始状态先前已被确定为基线。

Kaspersky Endpoint Security 允许您检测感染对象并消除其中检测到的威胁。为此，该应用程序可以使用：

- 应用程序数据库来检测和清除受感染的文件。在扫描过程中，应用程序会分析每个文件是否存在威胁：它将文件代码与特定威胁的代码进行比较，并查找可能的匹配项。
- 卡巴斯基安全网络。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对各种威胁作出响应，提高一些保护组件的性能，并减少误报风险。

清除或删除文件之前，Kaspersky Endpoint Security 会在设备的备份中保存文件的备份副本。如果您在清除后部分或完全无法访问已清除文件中的重要信息，可以从备份副本恢复文件。

执行扫描任务时，Kaspersky Endpoint Security 可以清除并删除受修改保护的文件：具有不可变和仅追加属性的文件以及具有“不可变”和“仅追加”属性的目录中的文件。备份中会存储在清除或删除文件之前创建的文件副本。如有必要，您可以从备份副本恢复文件。当扫描任务完成后，已清除文件的“不可变”和“仅追加”属性将被重置。

Kaspersky Endpoint Security 可以在仅通知模式下运行。*“仅通知”模式*是应用程序的一种操作模式，如果检测到威胁，应用程序组件和任务不会尝试清除或删除恶意对象、拒绝访问或阻止应用程序的活动。应用程序仅会告知用户检测到威胁。

Kaspersky Endpoint Security 支持与其他卡巴斯基解决方案集成，以扩展应用程序的功能：

- 与 Kaspersky Managed Detection and Response 的集成可实现持续搜索、检测和消除针对您组织的威胁。
- 与 Kaspersky Anti Targeted Attack Platform 解决方案的组件 Kaspersky Endpoint Detection and Response (KATA) 进行集成可确保保护您组织的 IT 基础设施并及时检测威胁，包括零日攻击、针对性攻击和高级持续性威胁。
- 与 Kaspersky Endpoint Detection and Response Optimum 的集成可以保护组织的 IT 基础设施免受漏洞利用、勒索软件、无文件攻击以及攻击者使用合法系统工具损害设备或数据等威胁。

您可以将 Kaspersky Endpoint Security 用作容器应用程序（以下也称为“KESL 容器”），以嵌入到外部系统中来扫描存储库中的容器镜像。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则不支持 KESL 容器功能。

此外，还提供了其他应用程序功能来确保应用程序保持最新：

- 使用密钥文件或激活码来激活应用程序。

  如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，将在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）上执行激活。

- 按计划并按需求通过管理服务器，从卡巴斯基更新服务器或者从用户指定的源更新数据库和应用程序模块。

  如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，应用程序将从 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）接收数据库和应用程序模块的更新。

- 根据用户角色控制用户对应用程序功能的访问。
- 将应用程序运行时发生的事件通知管理员。
- 使用完整性检查工具检查应用程序组件的完整性。

您可以使用以下方法来管理 Kaspersky Endpoint Security：

- 通过 Kaspersky Security Center Web Console、Kaspersky Security Center 云控制台或管理控制台使用 Kaspersky Security Center。
- 从命令行使用控制命令。
- 使用图形用户界面。

> 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则无法使用 Kaspersky Security Center 云控制台和图形用户界面来管理应用程序。

在美国境内，为遵守贸易限制，从 2024 年 9 月 10 日美国东部夏令时间 (EDT) 凌晨 12:00 开始，该应用程序将不再提供更新功能（包括反病毒签名更新和代码库更新）以及 KSN 功能。

关于 Kaspersky Endpoint Security 使用模式

可在以下模式之一下使用 Kaspersky Endpoint Security：

- 保护工作站和服务器的标准模式（“标准模式”）。Kaspersky Endpoint Security 用作独立应用程序来保护运行 Linux 操作系统的设备。
- 在 Light Agent 模式下，将虚拟环境作为Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分（"Light Agent 模式"）进行保护。Kaspersky Endpoint Security 用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 解决方案的 Light Agent 组件来保护运行 Linux 客户机操作系统的虚拟机。

默认在标准模式下使用应用程序。

如果要在 Light Agent 模式下使用应用程序，则需要执行以下操作：

1. 使用 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 在每个需要保护的虚拟机上安装 Kaspersky Endpoint Security。还可以在虚拟机模板上安装应用程序。

   在安装过程中，您必须通过以下其中一种方式指定应用程序将在 Light Agent 模式下使用：

   - 在应用程序的安装后配置期间使用交互模式或自动模式（如果使用命令行安装）。
   - 在应用程序安装包的属性中或安装包中包含的 autoinstall.ini 配置文件中（如果使用 Kaspersky Security Center 安装）。

   > 安装 Kaspersky Endpoint Security 后，将无法更改应用程序使用模式。

   选择 Light Agent 模式时，还可以在 Light Agent 模式下配置 Kaspersky Endpoint Security 的以下设置：

- 想要保护的虚拟机在虚拟基础架构中的角色：服务器或工作站。虚拟机的角色决定了在此虚拟机上使用应用程序时所用的授权许可以及可用的功能。

- VDI 保护模式。如果要在用于创建临时虚拟机的虚拟机模板上安装应用程序，建议启用此模式。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的操作。

2. 配置用于将 Light Agent 连接到 SVM 的设置和用于将 Light Agent 连接到 Integration Server 的设置。

   处于 Light Agent 模式的 Kaspersky Endpoint Security 会与 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 解决方案的其他组件交互：SVM 上安装的 Integration Server 和 Protection Server（有关更多信息，请参阅"Kaspersky Endpoint Security for Virtualization Light Agent 帮助"）。为了与 Protection Server 进行交互，Kaspersky Endpoint Security 会与安装了该 Protection Server 的 SVM 建立并保持连接。

   如果您希望 Light Agent 通过 Integration Server 接收有关 SVM 的信息，或者要保护 Protection Server 与 Light Agent 之间的连接，则需要连接到 Integration Server。

   可以使用 Kaspersky Security Center 管理控制台或 Kaspersky Security Center Web Console 在 Kaspersky Endpoint Security 策略的属性中配置连接设置。

在 Light Agent 模式下，可以使用以下应用程序命令获取有关应用程序操作设置的信息以及与 Integration Server 和 SVM 的连接有关的信息：`kesl-control --ksvla-info`、`kesl-control --viis-info` 和 `kesl-control --svm-info`。

有关应用程序使用模式的信息显示在受管理设备上 Kaspersky Security Center 的 Kaspersky Endpoint Security 的属性中的"**组件**"部分。信息显示在"**用于保护虚拟环境的 Light Agent 模式**"行中，如下所示：

- 状态"*运行中*"表示正在 Light Agent 模式下使用应用程序。

- 状态"*未安装*"表示正在标准模式下使用应用程序。

关于在 Light Agent 模式下激活应用程序

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，则无需单独激活应用程序。您仅激活 Kaspersky Security for Virtualization Light Agent。激活是在 Protection Server 端（Kaspersky Security for Virtualization Light Agent 的一个组件）通过在 SVM 上添加授权许可密钥来执行的。有关更多详细信息，请参阅"Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助"部分。

若要激活Kaspersky Endpoint Detection and Response Optimum功能，您还需要向 SVM 添加 EDR Optimum 授权许可密钥。用于激活Kaspersky Hybrid Cloud Security for Virtualization Light Agent 解决方案组件的授权许可不包含此功能。

激活解决方案并将 Light Agent 连接到 SVM 后，Protection Server 组件会将授权许可信息发送到 Light Agent。选择要连接的 SVM 时，Light Agent 会考虑已添加到 SVM 的授权许可密钥类型等设置。如果已添加到 SVM 的密钥类型与虚拟基础架构（服务器或工作站）中受保护虚拟机的角色不匹配，Light Agent 不会连接到 SVM。有关更多详细信息，请参阅"Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助"。

您使用 `kesl-control -L --query` 命令查看包含 Light Agent 的受保护虚拟机上用于激活 Light Agent for Linux 的授权许可信息。

无法使用"*添加密钥*"任务或通过用于添加和删除授权许可密钥的 Kaspersky Endpoint Security 命令来管理授权许可密钥。

关于在 Light Agent 模式下更新应用程序数据库和模块

Light Agent 模式下的 Kaspersky Endpoint Security 使用反恶意软件数据库，应用程序需要此数据库才能作为 Kaspersky Security for Virtualization Light Agent 的一部分来运行。Kaspersky Endpoint Security 从 Protection Server 接收应用程序数据库和模块更新。有关更多详细信息，请参阅 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助。

受保护虚拟机上的数据库和模块使用 Kaspersky Endpoint Security 的特殊本地任务“*更新*”进行更新，其中，SVM 上的文件夹被指定为更新源。该更新任务自动启动。您不能删除此任务，也不能更改其设置。

不支持除 SVM 上的文件夹以外的更新源。不支持使用组更新任务。

上一次的反恶意软件数据库更新也在 Protection Server 端回滚。在 SVM 上回滚应用程序数据库和模块更新后，将在受保护虚拟机上自动启动一个特殊的“*更新*”本地任务。完成该任务后，Light Agent 会恢复为使用先前的一组反恶意软件数据库。

不支持使用 Kaspersky Endpoint Security 的“*回滚*”本地和组任务。

在 Light Agent 模式下使用应用程序的其他功能

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security：

- 不支持 KESL 容器功能。
- 不支持使用 Kaspersky Security Center 云控制台和图形用户界面管理应用程序。
- 不支持使用云数据库。
- Kaspersky Endpoint Security 使用 KSN 代理服务器与 KSN 服务器交互。不支持与 KSN 直接通信。
- 连接到 Integration Server、SVM 或 KSN 服务器时，不支持使用应用程序的代理服务器。
- 与Kaspersky Symphony XDR集成不受支持。

分发包

您可以在卡巴斯基网站上下载 Kaspersky Endpoint Security 分发包中包含的文件以及使用 Kaspersky Security Center 远程安装应用程序所需的文件。

该分发包包括 Kaspersky Endpoint Security 安装包，其中包含以下文件：

- kesl-12.1.0-<版本号>.i386.rpm、kesl_12.1.0-<版本号>_i386.deb
  包含主要的应用程序文件。可以根据程序包管理器的类型将程序包安装到 32 位操作系统。
- kesl-12.1.0-<版本号>.x86_64.rpm、kesl_12.1.0-<版本号>_amd64.deb
  包含主要的应用程序文件。可以根据程序包管理器的类型将程序包安装到 64 位操作系统。
- kesl-12.1.0-<版本号>.aarch64.rpm、kesl_12.1.0-<版本号>_arm64.deb
  包含主要的应用程序文件。相关软件包管理器的软件包可以安装在 Arm® 架构的 64 位操作系统上。

- kesl-gui-12.1.0-<版本号>.i386.rpm、kesl-gui_12.1.0-<版本号>_i386.deb
  包含应用程序图形用户界面的文件。可以根据程序包管理器的类型将程序包安装到 32 位操作系统。
- kesl-gui-12.1.0-<版本号>.x86_64.rpm、kesl-gui_12.1.0-<版本号>_amd64.deb
  包含应用程序图形用户界面的文件。可以根据程序包管理器的类型将程序包安装到 64 位操作系统。
- kesl-gui-12.1.0-<版本号>.aarch64.rpm、kesl-gui_12.1.0-<版本号>_arm64.deb
  包含应用程序图形用户界面的文件。相关软件包管理器的软件包可以安装在 Arm 架构的 64 位操作系统上。
- kesl-12.1.0.<版本号>.zip
  包含用于使用 Kaspersky Security Center 远程安装应用程序的文件，包括 license.<语言 ID> 和 ksn_license.<语言 ID> 文件。

  > Kaspersky Security Center 网络代理不包含在分发包中。您可以在应用程序下载页面的“**Kaspersky Security Center**”部分中下载它。

- docker-service-kesl64-12.1.0-<版本号>.tgz
  包含用于创建 KESL 容器应用程序镜像的文件。
- ksn_license.<语言 ID>
  包含卡巴斯基安全网络声明文本。
- license.<language ID
  包含授权许可协议文本。授权许可协议规定了使用该应用程序的条款。

使用应用程序文档中未描述或技术支持专家未推荐的方式独立更改应用程序文件可能会导致应用程序和操作系统性能不佳和出现故障、减少对设备的保护、数据无法访问和损坏，以及将额外的统计数据发送到 KSN。

硬件和软件要求

本节包含 Kaspersky Endpoint Security 的硬件和软件要求。

硬件要求

Kaspersky Endpoint Security 具有以下硬件要求：

最低硬件要求：

- Core ™ 2 Duo 1.86 GHz 或更快的处理器
- 至少 1 GB 的交换分区
- 32 位操作系统 1 GB RAM，64 位操作系统 2 GB RAM

- 4 GB 的可用硬盘空间，用于安装应用程序和存储临时文件和日志文件
- 使用图形用户界面时，显示器必须能够显示 1000 像素宽、600 像素高的窗口（如果应用屏幕缩放，这些尺寸也会缩放）
- 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则带宽为 100 Mbit/s 的虚拟网络接口

Arm 架构的最低硬件要求：

- Armv8.2-A Kunpeng 920 或 Armv8-A Baikal-M (BE-M1000) 处理器或 m-TrusT Terminal
- 至少 1 GB 的交换分区
- 2 GB 的 RAM
- 3 GB 的可用硬盘空间，用于安装应用程序和存储临时文件和日志文件
- 使用图形用户界面时，显示器必须能够显示 1000 像素宽、600 像素高的窗口（如果应用屏幕缩放，这些尺寸也会缩放）

基于 Arm 架构的操作系统不支持在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境。

软件要求

要安装 Kaspersky Endpoint Security，设备上必须安装以下操作系统之一：

- 32 位操作系统：
  - Debian GNU/Linux 11.0 及更高版本
  - Debian GNU/Linux 12.0 及更高版本
  - Mageia™ 4

    运行 Mageia 4 操作系统的设备不支持 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response (KATA) 的集成。
  - ALT 8 SP Workstation (8.4)
  - ALT 8 SP Server (8.4)
  - ALT SP Workstation 版本 10
  - ALT SP Server 版本 10
- 64 位操作系统：
  - AlmaLinux OS 8 及更高版本

- AlmaLinux OS 9 及更高版本
- AlterOS® 7.5 及更高版本
- Amazon™ Linux 2
- Astra Linux Common Edition 2.12
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)
- Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)

  在强制访问控制和封闭软件环境模式下运行 Astra Linux 操作系统的设备不支持在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境。

“移动”模式下的 Astra Linux 操作系统仅在桌面模式下的平板电脑（平板电脑）上受支持。

- CentOS 7.2 及更高版本
- CentOS Stream 8
- CentOS Stream 9
- Debian GNU/Linux 11.0 及更高版本
- Debian GNU/Linux 12.0 及更高版本
- EMIAS 1.0 及更高版本
- EulerOS 2.0 SP10
- Kylin 10
- Linux Mint 20.3 及更高版本
- Linux Mint 21.1 及更高版本
- openSUSE Leap 15.0 及更高版本
- Oracle Linux 7.3 及更高版本
- Oracle Linux 8.0 及更高版本
- Oracle Linux 9.0 及更高版本
- Red Hat Enterprise Linux 7.2 及更高版本
- Red Hat Enterprise Linux 8.0 及更高版本

- Red Hat Enterprise Linux 9.0 及更高版本
- Rocky Linux 8.5 及更高版本
- Rocky Linux 9.1
- SberLinux 8.8 (Dykhtau)
- SberOS 3.2.0
- SUSE Linux Enterprise Server 12.5 及更高版本
- SUSE Linux Enterprise Server 15 及更高版本
- Ubuntu® 20.04 LTS
- Ubuntu 22.04 LTS
- Ubuntu 24.04 LTS
- ALT 8 SP Workstation (8.4)
- ALT 8 SP Server (8.4)
- ALT Education 10.1
- ALT Workstation 10.1
- ALT Server 10.1
- ALT SP Workstation 版本 10
- ALT SP Server 版本 10。
- Atlant，Alcyone build，版本 2022.02
- GosLinux 7.17
- GosLinux 7.2
- MSVSPHERE 9.2 ARM
- MSVSPHERE 9.2 SERVER
- RED OS® 7.3
- RED OS 8.0
- ROSA Cobalt 7.9
- ROSA Chrome 12
- SynthesisM Client 8.6
- SynthesisM Server 8.6

- Arm 架构的 64 位操作系统：
  - Astra Linux Special Edition RUSB.10152-02 (operational update 4.7)
  - CentOS Stream 9
  - EulerOS 2.0 SP10
  - SUSE Linux Enterprise Server 15
  - Ubuntu 22.04 LTS
  - ALT 8 SP Workstation (8.4)
  - ALT 8 SP Server (8.4)
  - ALT SP Workstation 版本 10
  - ALT SP Server 版本 10
  - RED OS 7.3

Arm 架构的操作系统不支持在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境。

由于 fanotify 的技术限制，该应用程序不支持以下文件系统：autofs、binfmt_misc、cgroup、configfs、debugfs、devpts、devtmpfs、fuse、fuse.gvfsd-fuse、gfs2、gvfs、hugetlbfs、mqueue、nfsd、proc、parsecfs、pipefs、pstore、usbfs、 rpc_pipefs、securityfs、selinuxfs、sysfs、tracefs。

支持的 Kaspersky Security Center 版本

Kaspersky Endpoint Security 与以下 Kaspersky Security Center 版本兼容：

- Kaspersky Security Center 13.2。MMC 管理插件可用于通过管理控制台管理 Kaspersky Endpoint Security。
- Kaspersky Security Center 14。可以使用 MMC 管理插件通过管理控制台管理 Kaspersky Endpoint Security，也可以使用 Web 管理插件通过 Kaspersky Security Center Web Console 进行管理。
- Kaspersky Security Center 14.2 Windows。可以使用 MMC 管理插件通过管理控制台管理 Kaspersky Endpoint Security，也可以使用 Web 管理插件通过 Kaspersky Security Center Web Console 进行管理。
- Kaspersky Security Center 14.2 Linux。Web 管理插件可用于通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security。
- Kaspersky Security Center 15 Linux。Web 管理插件可用于通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security。
- Kaspersky Security Center 15.1 Linux。Web 管理插件可用于通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境（作为 Kaspersky Security for Virtualization Light Agent 的一部分），我们建议使用以下一个版本的 Kaspersky Security Center 管理该应用程序。

- Kaspersky Security Center 14.2 Windows。
- Kaspersky Security Center 15 Linux。
- Kaspersky Security Center 15.1 Linux。

Kaspersky Security Center 网络代理是通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security 所必需的。

Kaspersky Security Center 网络代理不包含在 Kaspersky Endpoint Security 分发包中。您可以在应用程序下载页面的“**Kaspersky Security Center**”部分中下载它。

如果您正在使用与 Kaspersky Endpoint Detection and Response (KATA) 组件的应用程序集成，我们建议使用以下版本的 Kaspersky Security Center 来管理应用程序：

- Kaspersky Security Center 14.2 Windows。
- Kaspersky Security Center 15 Linux。
- Kaspersky Security Center 15.1 Linux。

Kaspersky Anti Targeted Attack Platform 支持的版本

Kaspersky Endpoint Security 与以下版本的 Kaspersky Anti Targeted Attack Platform 兼容：

- Kaspersky Anti Targeted Attack Platform 5.1。受支持，但有限制。
- Kaspersky Anti Targeted Attack Platform 6.0。
- Kaspersky Anti Targeted Attack Platform 6.1。

有关 Kaspersky Anti Targeted Attack Platform 解决方案的更多详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

新增功能

Kaspersky Endpoint Security 现在拥有以下功能和改进：

- 现在，您可以设置与 Kaspersky Endpoint Detection and Response Optimum 的集成，它可以保护组织的 IT 基础设施免受漏洞利用、勒索软件、无文件攻击以及攻击者使用合法系统工具损害设备或数据等威胁。
- 现在您可以向应用程序添加两个活动授权许可密钥：用于激活应用程序的主密钥和用于激活 Kaspersky Endpoint Detection and Response Optimum 功能的附加密钥。如果您的主授权许可不包含 Kaspersky Endpoint Detection and Response Optimum 功能，则需要附加密钥。
- 添加了新的*Web 控制*组件，用于控制用户对 Web 资源的访问。这样可以减少流量消耗和对工作时间的不当使用。如果用户尝试打开受 Web 控制限制访问的网站， Kaspersky Endpoint Security 会阻止访问或显示警告。
- 新增加的 Kaspersky Endpoint Security 稳定性监控功能可让您跟踪应用程序异常终止的次数，并将应用程序不稳定运行的情况通知管理员。
- 使用 Kaspersky Security Center Web Console 安装 Kaspersky Endpoint Security 的程序得到了改进：在应用程序安装包的属性中，您现在可以指定以前仅在 autoinstall.ini 配置文件中可用的初始配置参数。
- 更多应用程序设置可以使用 Kaspersky Security Center Web Console 和 Kaspersky Security Center 管理控制台指定：您可以编辑以前只能通过编辑 kesl.ini 配置文件进行设置的设置。
- 现在您可以在运行扫描任务时启用或禁用全局排除和文件威胁防护排除。
- 现在您可以设置与 Kaspersky Symphony XDR 的集成：如果 Kaspersky Endpoint Security 应用程序在标准模式下使用，则应用程序可以执行“启动恶意软件扫描”和“数据库更新”响应操作。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，则与 Kaspersky Symphony XDR 集成不受支持。
- 现在，当使用 Kaspersky Security Center 管理应用程序时，您可以将有关安装在客户端设备中或连接到这些设备的所有设备（包括以前安装和连接但当前已断开连接的设备）的信息发送到管理服务器。
- 流量拦截规则得到了完善，支持同一网络中容器的交互。
- 支持的操作系统列表已更新。

准备安装 Kaspersky Endpoint Security

常规操作

在开始安装 Kaspersky Endpoint Security 之前，您需要执行以下操作：

- 检查您的设备是否满足应用程序的硬件和软件要求。
- 确保您的设备上未安装第三方反病毒软件。
- 确保您的设备上未安装 Kaspersky Endpoint Agent for Linux。如果已安装 Kaspersky Endpoint Agent for Linux，您将在安装过程中看到一条关于需要手动将其删除的消息。
- 确保您的设备上安装了 Perl 5.10 或更高版本的解释器。
- 确保 semanage 实用程序已安装在系统中。如果未安装该实用程序，请安装 policycoreutils-python 或 policycoreutils-python-utils 包，具体取决于包管理器。
- 在操作系统不支持 fanotify 技术的设备上，请确保安装以下软件：
  - 用于编译应用程序和运行任务的软件包（gcc、binutils、glibc、glibc-devel、make）
  - 包含操作系统内核标头文件的软件包，用于编译 Kaspersky Endpoint Security 模块。
- 根据操作系统，在您的设备上安装以下软件包之一：
  - 在运行 SUSE Linux Enterprise Server 15 操作系统的设备上，必须安装 insserv-compat 软件包。
  - 在运行 Red Hat Enterprise Linux 8 或 RED OS 操作系统的设备上，安装 perl-Getopt-Long 软件包。
  - 在运行 Red Hat Enterprise Linux 或 RED OS 操作系统的设备上，安装 perl-File-Copy 软件包。该软件包是运行初始应用程序配置脚本所必需的，但默认情况下可能不存在。
- 默认情况下，Astra Linux 操作系统会阻止 ptrace（禁用 ptrace 功能），这可能会影响 Kaspersky Endpoint Security 的操作。为使 Kaspersky Endpoint Security 正常工作，请在安装 Astra Linux 时解除阻止 ptrace。如果已经安装 Astra Linux，请参阅“Astra Linux 帮助中心”网站，获取有关如何启用/禁用此模式的说明（“**阻止 ptrace**”部分中的“**配置保护和阻止机制**”）。
- 如果您的设备使用的 Linux 内核版本低于 3.16，那么为了使 Kaspersky Endpoint Detection and Response (KATA) 集成任务正常运行，您需要确保 auditd 服务未启动且未安装。
- 为使防火墙管理、Web 威胁防护和网络威胁防护组件正常运行，您的设备上需要安装 iptables 实用程序。
- 为使 Kaspersky Endpoint Security 管理插件正常工作，必须在管理服务器上安装 Microsoft® Visual C++® 2015 Redistributable Update 3 RC（请参阅 https://www.microsoft.com/en-us/download/details.aspx?id=52685）。
- 要正确运行应用程序，请确保 root 账户是以下目录的所有者，并且只有所有者拥有对这些目录的写入权限：/var、/var/opt、/var/opt/kaspersky、/var/log/kaspersky、/opt、/opt/kaspersky、/usr/bin、/usr/lib、/

在 Light Agent 模式下安装 Kaspersky Endpoint Security 之前的附加操作

如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境（用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分），在开始安装 Kaspersky Endpoint Security 之前必须执行以下附加操作：

- 确保在想要保护的虚拟机上安装以下软件包，具体取决于部署了 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的虚拟基础架构：
  - 在 Microsoft Hyper-V 基础结构中，必须在虚拟机上安装 Integration Services 软件包。
  - 在 VMware vSphere 基础架构中，必须在虚拟机上安装 VMware Tools 软件包。
  - 在 XenServer 基础架构中，必须在虚拟机上安装 XenTools。
  - 在 HUAWEI FusionSphere 基础架构中，必须在虚拟机上安装 HUAWEI Tools 软件包。
  - 在基于 KVM、OpenStack、VK Cloud、TIONIX Cloud Platform、Astra Linux 或 Viola Virtualization Server 的基础架构中，必须在虚拟机上安装 QEMU Guest Agent。
- 确保用于监控虚拟机之间流量的网络设备或软件的设置允许网络流量通过 Light Agent 模式下的 Kaspersky Endpoint Security 与 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的其他组件交互时使用的端口。有关解决方案组件的更多详细信息，请参阅"Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助"。

用于执行 Light Agent 操作的端口

端口和协议	Direction	目的和说明
7271 TCP	从 Light Agent 到 Integration Server。	在 Light Agent 与 Integration Server 交互时适用。
8000 UDP	从 SVM 到 Light Agent。	通过 SVM 地址列表向 Light Agent 传输有关可用 SVM 的信息时适用。
8000 UDP	从 Light Agent 到 SVM。	可供 Light Agent 检索有关 SVM 状态的信息。
11111 TCP	从 Light Agent 到 SVM。	在连接不受保护时将服务请求（例如获取授权许可信息）从 Light Agent 传输到 Protection Server 的情况下适用。
11112 TCP	从 Light Agent 到 SVM。	在连接受保护时将服务请求（例如获取授权许可信息）从 Light Agent 传输到 Protection Server 的情况下适用。
9876 TCP	从轻代理到 SVM。	在连接不受保护时将文件扫描请求从 Light Agent 传输到 Protection Server 的情况下适用。
9877 TCP	从 Light Agent 到 SVM。	在连接受保护时将文件扫描请求从 Light Agent 传输到 Protection Server 的情况下适用。
80 TCP	从 Light Agent 到 SVM。	用于更新 Light Agent 上解决方案的数据库和应用程序模块。
15000 UDP	从 Kaspersky Security Center 到 SVM。	通过 Kaspersky Security Center 管理 Protection Server 时适用。
15000 UDP	从 Kaspersky Security Center 到 Light Agent。	通过 Kaspersky Security Center 管理 Light Agent 时适用。
13000 TCP	从 Light Agent 到 Kaspersky Security Center。	在连接受保护时通过 Kaspersky Security Center 管理 Light Agent 的情况下适用。
14000	从 Light Agent 到	在连接不受保护时通过 Kaspersky Security Center 管理 Light

TCP	Kaspersky Security Center。	Agent 的情况下适用。

Kaspersky Endpoint Security 的安装和初始配置

在安装 Kaspersky Endpoint Security 之前，您需要准备安装。

下面的方案描述如何安装和执行 Kaspersky Endpoint Security 的初始配置、如何安装和配置 Kaspersky Security Center 网络代理以及如何安装 Kaspersky Endpoint Security 管理插件。此安装方案依赖于您在使用 Kaspersky Endpoint 时所用的模式。

标准模式

如果您计划在标准模式下使用 Kaspersky Endpoint Security，安装过程包括以下步骤：

1. **网络代理的安装和初始配置**

   如果您计划使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security，请在受保护的设备上安装和配置 Kaspersky Security Center 网络代理。

2. **安装 Kaspersky Endpoint Security 管理插件**

   如果您计划使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security，请安装 Kaspersky Endpoint Security 管理插件。根据用于管理 Kaspersky Security Center 的控制台，使用以下管理插件：

   - Kaspersky Endpoint Security 管理 Web 插件允许您使用 Kaspersky Security Center 云控制台和 Kaspersky Security Center Web Console 管理应用程序。Web 插件安装在已安装 Kaspersky Security Center Web Console 的设备上。
   - Kaspersky Endpoint Security MMC 管理插件允许您使用 Kaspersky Security Center 管理控制台管理应用程序。MMC 插件安装在已安装 Kaspersky Security Center 管理控制台的设备上。

3. **安装应用程序包和图形用户界面**

   Kaspersky Endpoint Security 以 DEB 和 RPM 软件包进行分发。应用程序和图形用户界面有单独的软件包。从适当格式的软件包中安装 Kaspersky Endpoint Security 和图形用户界面（如有必要）。

   可以通过以下方法之一进行安装：

   - 使用 Kaspersky Security Center。
   - 使用命令行。

4. **Kaspersky Endpoint Security 的初始配置**

   必须执行初始配置才能启用对客户端设备的保护。

   如果您使用 Kaspersky Security Center 安装了 Kaspersky Endpoint Security，在安装完成后，请完成开始过程。

   如果您使用命令行安装了 Kaspersky Endpoint Security，在安装完成后，请运行初始配置脚本或在自动模式下执行初始配置。

Light Agent 模式

> 基于 Arm 架构的操作系统不支持在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境。

如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，安装过程包括以下步骤：

1. **网络代理的安装和初始配置**

在虚拟机和虚拟机模板上安装和配置 Kaspersky Security Center 代理。

如果要在将用于创建临时虚拟机的模板上安装网络代理，建议配置的设置可让您优化临时虚拟机上的性能。有关在虚拟机模板上安装的更多详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

2. **安装 Kaspersky Endpoint Security 管理插件**

   安装 Kaspersky Endpoint Security 管理插件。根据用于管理 Kaspersky Security Center 的控制台，使用以下管理插件：

   - Kaspersky Endpoint Security 管理 Web 插件允许您使用 Kaspersky Security Center 云控制台和 Kaspersky Security Center Web Console 管理应用程序。Web 插件安装在已安装 Kaspersky Security Center Web Console 的设备上。
   - Kaspersky Endpoint Security MMC 管理插件允许您使用 Kaspersky Security Center 管理控制台管理应用程序。MMC 插件安装在已安装 Kaspersky Security Center 管理控制台的设备上。

3. **Kaspersky Endpoint Security 的应用程序包安装和初始配置**

   Kaspersky Endpoint Security 以 DEB 和 RPM 软件包进行分发。从所需格式的软件包安装 Kaspersky Endpoint Security。应用程序和图形用户界面有单独的软件包。

   > 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则不支持图形用户界面。

   可以通过以下方法之一安装应用程序：

   - 使用 Kaspersky Security Center。

     在开始安装之前，您必须通过以下方式之一执行应用程序的初始配置：

     - 在安装包属性的“**设置**”选项卡中（此方法仅在 Kaspersky Security Center Web Console 中可用）。
     - 使用安装包中包含的配置文件。

     您必须选择 Light Agent 模式（在配置文件中，设置 `KSVLA_MODE=yes`）。如果您在将用于创建临时虚拟机的模板上安装 Kaspersky Endpoint Security，我们建议同时启用 VDI 保护模式，以优化临时虚拟机上的应用程序性能（在配置文件中，设置 `VDI_MODE=yes`）。

   - 使用命令行。如果使用命令行执行安装，则在初始配置期间选择应用程序使用模式。

4. **Kaspersky Endpoint Security 的初始配置**

   必须执行初始配置才能启用对客户端设备的保护。

   如果您使用 Kaspersky Security Center 安装了 Kaspersky Endpoint Security，在安装完成后，请完成开始过程。

   如果您使用命令行安装了 Kaspersky Endpoint Security，在安装完成后，请运行初始配置脚本或在自动模式下执行初始配置。在初始配置期间通过以下方式之一选择 Light Agent 模式：

   - 在初始配置脚本的 `Specifying the application usage` 步骤中输入 `yes`。
   - 在初始安装配置文件中指定 `KSVLA_MODE=yes` 设置。

   如果您在将用于创建临时虚拟机的模板上安装 Kaspersky Endpoint Security，建议也配置设置，这可让您优化临时虚拟机上的操作。有关在虚拟机模板上安装的更多详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

Kaspersky Security Center 网络代理的安装和初始配置

为了通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security，必须安装网络代理。

网络代理可促进客户端设备与 Kaspersky Security Center 管理服务器的连接。它必须安装在将连接到集中式远程管理系统 Kaspersky Security Center 的每台客户端设备上。

您可以执行网络代理的安装和初始配置：

- 使用 Kaspersky Security Center Web Console 或管理控制台从管理员工作站远程操作；
- 使用命令行。

使用 Kaspersky Security Center 安装网络代理

在使用 Kaspersky Security Center 开始远程安装网络代理之前，您必须准备好用于远程安装的设备（请参阅“Kaspersky Security Center 帮助”系统，“准备运行 Linux 的设备并在运行 Linux 的设备上远程安装网络代理”部分）。

网络代理安装包用于远程安装。您可以从卡巴斯基网站的“**Kaspersky Security Center**”部分下载创建网络代理安装包所需的文件。

要远程安装网络代理：

1. 选择网络代理安装包。

   在创建安装包期间，您必须接受网络代理最终用户授权许可协议的条款。您可以在网络代理分发包内的 license.txt 文档中阅读最终用户授权许可协议的文本。

   在安装包设置中，指定网络代理要连接的管理服务器的地址，以及连接端口。

2. 使用远程安装任务安装网络代理。

有关如何安装网络代理的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

使用命令行安装网络代理

您可以通过以下方式之一使用命令行安装网络代理：

- 使用应答文件在静默模式下运行安装和初始配置。应答文件是一个文本文件，其中包含一组自定义设置，用于网络代理的安装和初始配置。
- 根据软件包管理器的类型通过 RPM 或 DEB 软件包安装网络代理，然后在交互模式下使用脚本来执行网络代理的初始配置。该脚本使用以下命令运行：
  - 对于 32 位操作系统：

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

  - 对于 64 位操作系统：

    ```
    # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
    ```

网络代理安装必须以 root 特权启动。

在静默模式下安装网络代理：

1. 创建应答文件。在应答文件中，按< 设置 >=< 值 >的格式输入网络代理安装和初始配置设置列表，每个设置单独占一行。

   如要正确使用应答文件，必须包含以下必要设置：

   - KLNAGENT_SERVER：管理服务器的完全限定域名 (FQDN) 或 IP 地址。
   - KLNAGENT_AUTOINSTALL：此设置决定是否启用在静默模式下安装。指定为 1。
   - EULA_ACCEPTED：同意网络代理的最终用户授权许可协议的条件。您必须接受最终用户授权许可协议的条款才能继续进行安装。您可以在网络代理分发包内的 license.txt 文档中阅读最终用户授权许可协议的文本。如果您理解并接受最终用户授权许可协议的条件，请指定为 1。

   您还可以为网络代理的安装和初始配置添加其他设置。有关可能设置的完整列表，请参阅 Kaspersky Security Center 帮助系统（"在静默模式下安装 Linux 网络代理（带应答文件）"部分）。

2. 如下例所示，输入应答文件的完整名称（包括路径），设置 KLAUTOANSWERS 环境变量的值：

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

3. 安装网络代理：

   - 要将网络代理从 RPM 软件包安装到 32 位操作系统，请执行以下命令：

     ```
     # rpm -i klnagent-< 版本号 >.i386.rpm
     ```

   - 要将网络代理从 RPM 软件包安装到 64 位操作系统，请执行以下命令：

     ```
     # rpm -i klnagent64-< 版本号 >.x86_64.rpm
     ```

   - 要从 RPM 软件包将网络代理安装到 Arm 架构的 64 位操作系统，请执行以下命令：

     ```
     # rpm -i klnagent64-< 版本号 >.aarch64.rpm
     ```

   - 要将网络代理从 DEB 软件包安装到 32 位操作系统，请执行以下命令：

     ```
     # apt-get install ./klnagent_< 版本号 >_i386.deb
     ```

   - 要将网络代理从 DEB 软件包安装到 64 位操作系统，请执行以下命令：

     ```
     # apt-get install ./klnagent64_< 版本号 >_amd64.deb
     ```

   - 要从 DEB 软件包将网络代理安装到 Arm 架构的 64 位操作系统，请执行以下命令：

     ```
     # apt-get install ./klnagent64_< 版本号 >_arm64.deb
     ```

安装 Kaspersky Endpoint Security 管理插件

以下 Kaspersky Endpoint Security 管理插件用于使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security：

- Kaspersky Endpoint Security 管理 Web 插件允许您使用 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台管理应用程序。

- Kaspersky Endpoint Security MMC 管理插件允许您使用 Kaspersky Security Center 管理控制台管理应用程序。

您可以同时为多个不同版本的 Kaspersky Endpoint Security 安装管理插件。这样您可以使用不同管理插件版本创建的策略来管理应用程序。

您还可以将使用先前版本的管理插件创建的策略和任务转换为最新版本。

安装 Kaspersky Endpoint Security Web 插件

Kaspersky Endpoint Security 管理 Web 插件必须安装在已安装 Kaspersky Security Center Web Console 的客户端设备上。所有有权在浏览器中访问 Kaspersky Security Center Web Console 的管理员都可以使用 Web 插件的功能。

您可以按照以下方式安装 Web 插件：

- 使用 Kaspersky Security Center Web Console 的初始配置向导。

  首次将 Kaspersky Security Center Web Console 连接到管理服务器时，Kaspersky Security Center Web Console 会自动提示您运行初始设置向导。您也可以在 Kaspersky Security Center Web Console 界面中运行初始设置向导（**设备发现和部署 → 部署和分配 → 初始设置向导**）。初始配置向导还可以检查安装的 Web 插件是否为最新并下载必要更新。有关 Kaspersky Security Center Web Console 的初始设置向导的更多信息，请参阅“Kaspersky Security Center 帮助”部分。

- 使用卡巴斯基 Web 插件列表或外部源的分发包手动安装。

如要手动安装 Kaspersky Endpoint Security Web 插件：

1. 在 Kaspersky Security Center Web Console 主窗口中，选择“**设置**”→“**Web 插件**”。

   已安装的 Web 插件列表将打开。

2. 通过以下方式之一开始安装 Kaspersky Endpoint Security Web 插件：

   - 从卡巴斯基 Web 插件列表安装：

     a. 单击“**添加**”。

     所有可用的卡巴斯基 Web 插件列表将打开。当新版本的 Web 插件发布后，该列表会自动更新。

     b. 在列表中找到 **Kaspersky Endpoint Security <版本号> for Linux** Web 插件并单击其名称。

     c. 在打开的窗口（带有 Web 插件说明）中，单击“**安装插件**”按钮。

     d. 等待安装完成，然后在信息窗口中单击“**确定**”。

   - 从外部源安装 Web 插件（安装 Web 插件所需的压缩文件包含在分发包中）：

     a. 单击“**从文件添加**”按钮。

     b. 在打开的窗口中，指定包含 Web 插件分发包的 ZIP 压缩文件的路径以及 TXT 格式的签名文件的路径。该文件位于包含 Web 插件的压缩文件中。

     c. 单击“**添加**”。

     d. 等待安装完成，然后在信息窗口中单击“**确定**”。

新插件显示在已安装的 Web 插件列表中（**设置 → Web 插件**）。

如果您在 Kaspersky Security Center 管理服务器的属性中选择 Kaspersky Endpoint Security 分发包中未包含的语言，则授权许可协议和整个 Kaspersky Security Center Web Console 界面将以英语显示。

安装 Kaspersky Endpoint Security MMC 插件

Kaspersky Endpoint Security MMC 管理插件必须安装在已安装 Kaspersky Security Center 管理控制台的同一客户端设备上。

在安装 Kaspersky Endpoint Security MMC 管理插件之前，请确保已安装 Kaspersky Security Center 和 Redist C ++ 2015（Microsoft Visual C ++ 2015 Redistributable）。

如要安装 MMC 插件，

在安装 Kaspersky Security Center 管理控制台的设备上，运行可执行文件 klcfginst.msi。

该文件包含在 Kaspersky Endpoint Security 分发包中。

安装完成后，MMC 管理插件将显示在 Kaspersky Security Center 管理服务器属性中的已安装 MMC 管理插件列表中。

如要查看已安装的 MMC 管理插件列表：

1. 在 Kaspersky Security Center 管理控制台树中，选择**管理服务器 <服务器名称>**节点，然后通过以下方式之一打开管理服务器属性窗口：
   - 使用**管理服务器 <服务器名称>**节点上下文菜单中的“**属性**”项；
   - 在“**管理服务器**”部分中，单击位于**管理服务器 <服务器名称>**节点工作区中的“**管理服务器属性**”链接。
2. 在左侧列表的“**高级**”部分中，选择“**有关已安装的应用程序管理插件的信息**”部分。
   在窗口右侧，已安装的管理插件列表显示 Kaspersky Endpoint Security 的 MMC 管理插件：**Kaspersky Endpoint Security <版本号> for Linux**。

使用 Kaspersky Security Center 安装和初始配置应用程序

您可以使用 Kaspersky Security Center Web Console 或管理控制台从管理员工作站将 Kaspersky Endpoint Security 远程安装到客户端设备。

对于远程安装，使用 Kaspersky Endpoint Security 安装包。Kaspersky Endpoint Security 安装包通用于所有受支持的操作系统和处理器架构类型。您可以使用 Kaspersky Security Center Web Console 或管理控制台创建安装包。

如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境（作为 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分），则需要通过安装包属性（该方法仅适用于 Web Console）或安装包中包含的 autoinstall.ini 配置文件对应用程序进行初始配置。

您可以通过多种方式在公司网络中的设备上部署 Kaspersky Endpoint Security。

Kaspersky Security Center Web Console 支持以下主要部署方法：

- 使用"保护部署向导"安装应用程序。
- 使用远程安装任务安装应用程序。

Kaspersky Security Center 管理控制台支持以下主要部署方法：

- 使用远程安装向导安装应用程序。
- 使用远程安装任务安装应用程序。

有关部署过程的说明，请参阅 Kaspersky Security Center 帮助。

如有必要，您可以使用 Kaspersky Security Center 客户端设备的远程诊断查看应用程序远程安装日志。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则不支持在安装过程中激活应用程序和自动授权许可密钥分发。如果 Kaspersky Endpoint Security 在连接到 SVM 后从 Protection Server 收到有关授权许可的信息；无需单独激活 Kaspersky Endpoint Security。

使用 Kaspersky Security Center 安装应用程序完成后，您必须准备运行该应用程序。

要使用 Kaspersky Security Center 来管理安装在客户端设备上的 Kaspersky Endpoint Security，您需要将这些设备放在管理组中。在开始安装 Kaspersky Endpoint Security 之前，您可以创建 Kaspersky Security Center 管理组，将安装了 Kaspersky Endpoint Security 的设备移动到这些组中，并配置规则以自动将设备移动到这些管理组。如果未配置将设备移动到管理组的规则，Kaspersky Security Center 会将所有安装了管理代理并连接到管理服务器的设备移动到"**未分配的设备**"列表中。在这种情况下，您需要手动将计算机移动到管理组中（有关详细信息，请参阅 Kaspersky Security Center 帮助）。

在 Web Console 中创建安装包

在 Kaspersky Security Center Web Console 中，可以通过以下两种方式创建安装包：

- 使用先前准备的压缩文件。
- 使用卡巴斯基服务器上托管的分发包。

如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则必须在所创建的安装包的属性中的**"设置"**选项卡中执行应用程序的初始配置。您还可以使用安装包中包含的配置文件执行应用程序的初始配置。

要准备用于创建安装包的压缩文件：

1. 从应用程序下载页面下载 kesl.zip 压缩文件。它位于 **Kaspersky Endpoint Security for Linux（其他分发 -> 用于远程安装产品的文件）**中。

2. 将 kesl.zip 压缩文件解压到可供 Kaspersky Security Center Administration Server 访问的一个文件夹中。将对应于要安装应用程序的操作系统类型及其软件包管理器类型的分发文件放在同一文件夹中：

   - 要安装 Kaspersky Endpoint Security：
     - kesl-12.1.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl_12.1.0-<版本号>_i386.deb（适用于使用 dpkg 的 32 位操作系统）
     - kesl-12.1.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）
     - kesl_12.1.0-<版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
     - kesl-12.1.0-<版本号>.aarch64.rpm（适用于 Arm 架构的使用 rpm 的 64 位操作系统）
     - kesl-12.1.0-<版本号>_arm64.deb（适用于 Arm 架构的使用 dpkg 的 64 位操作系统）
   - 要安装 GUI：
     - kesl-gui-12.1.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl-gui-12.1.0-<版本号>_i386.deb（适用于使用 dpkg 的 32 位操作系统）
     - kesl-gui-12.1.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）
     - kesl-gui-12.1.0-<版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
     - kesl-gui-12.1.0-<版本号>.aarch64.rpm（适用于 Arm 架构的使用 rpm 的 64 位操作系统）
     - kesl-gui-12.1.0-<版本号>_arm64.deb（适用于 Arm 架构的使用 dpkg 的 64 位操作系统）

   如果您不想安装图形用户界面，请不要将这些文件放入文件夹中；这会进一步缩小安装包的体积。

   如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则不支持图形用户界面。

   注意，如果您不打算使用图形用户界面，则需要在所创建的安装包的属性中或 autoinstall.ini 配置文件中设置 `USE_GUI=No`。否则，安装将失败。

   如果您要使用已创建的安装包在多种类型的操作系统或软件包管理器上安装应用程序，请将所有所需类型的操作系统和软件包管理器的文件放入该文件夹中。

3. 如果想要使用配置文件执行应用程序的初始配置，请打开 autoinstall.ini 配置文件并根据需要进行编辑。autoinstall.ini 文件位于 kesl.zip 压缩文件所解压到的文件夹中。

   如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则需要在 autoinstall.ini 配置文件中设置 `KSVLA_MODE=yes`。

您还可以在所创建的安装包的属性中的“**设置**”选项卡中执行应用程序的初始配置。

4. 如果您计划在标准模式下使用 Kaspersky Endpoint Security 并希望使用之前下载的数据库，请将准备好的包含适用于所有所需操作系统类型的数据库的压缩文件放入该文件夹中。打开 autoinstall.ini 配置文件并指定 `UPDATE_EXECUTE=no`。autoinstall.ini 文件位于将 kesl.zip 压缩文件解压到的文件夹。

5. 将所有准备好的文件放入 ZIP、CAB、TAR 或 TAR. gz 格式的压缩文件中，文件名任意。

要在 Kaspersky Security Center Web Console 中创建 Kaspersky Endpoint Security 的安装包：

1. 在 Web Console 主窗口中，选择以下任一部分：

   - **设备发现和部署 → 部署和分配 → 安装包**。
   - **操作 → 存储库 → 安装包**。

   将打开管理服务器上可用的安装包列表。

2. 单击“**添加**”。

   创建安装包的向导将启动。按照向导的说明进行操作。

3. 在安装向导的第一页，选择创建安装包的方法：

   - **从文件创建安装包**。将从您提前准备的压缩文件中创建安装包。如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，必须选择此选项。
   - **创建卡巴斯基应用程序安装包**。将从卡巴斯基服务器上的分发包创建安装包。

   > Kaspersky Security Center 云控制台不允许从文件创建安装包。

4. 根据所选的软件包创建方法：

   - 指定软件包名称，单击**浏览**按钮，并指定为创建安装包而准备的压缩文件的路径。
   - 选择 Kaspersky Endpoint Security 分发包。在右侧窗口中，阅读有关分发包的信息，单击**下载并创建安装包**按钮。安装包创建过程开始。

5. 在创建安装包期间，请接受最终用户授权许可协议和隐私策略的条款。当向导提示时，请阅读您与卡巴斯基之间的授权许可协议，以及描述数据处理和传输的隐私策略。要继续创建安装包，请确认您已完全阅读并接受授权许可协议和隐私策略的条款。

安装包将被创建并添加到安装包列表中。使用安装包，您可以在公司网络中的设备上安装应用程序或更新应用程序版本。

您可以在安装包的属性中的“**设置**”选项卡中执行应用程序的初始配置（参见下表）。

> 无法在低于 14.2 版本的 Kaspersky Security Center Web Console 中配置 Kaspersky Endpoint Security 的安装包。使用 autoinstall.ini 配置文件来配置设置。

安装包设置

部分	Description
指定区域设置。	选中此复选框以指定应用程序运行期间使用的区域设置。区域设置采用 RFC

	3066 指定的格式。如果不指定此设置，则使用默认区域设置。
激活应用程序	选中该复选框以激活应用程序。 您还可以在安装后激活应用程序。 只有在标准模式下使用应用程序时，该设置才适用。
选择更新源。	指定更新源： • 卡巴斯基更新服务器。 • Kaspersky Security Center。 • 本地或全球网络上的其他源。 只有在标准模式下使用应用程序时，该设置才适用。
安装后运行数据库更新任务。	选中此复选框可在安装应用程序后运行“更新”任务。 只有在标准模式下使用应用程序时，该设置才适用。
指定代理服务器设置。	选中此复选框可指定用于连接到互联网的代理服务器的地址。 只有在标准模式下使用应用程序时，该设置才适用。
安装内核源	选中此复选框可自动启动内核模块编译。
使用图形用户界面。	选中此复选框可启用图形用户界面。 只有在标准模式下使用应用程序时，该设置才适用。
指定具有管理员角色的用户。	选中此复选框，以指定要向其分配管理员 (admin) 角色的用户。
自动配置 SELinux。	选中此复选框，自动将 SELinux 配置为与 Kaspersky Endpoint Security 一起使用。
从特权组中删除用户	选中此复选框可以在安装应用程序之前从“kesladmin”和“keslaudit”特权组中删除用户。 如果选中该复选框并且“nogroup”组不存在，则安装将失败，并提示您手动从特权组中删除用户。
安装后首次启动应用程序时禁用保护组件和扫描任务。	选中此复选框可以在安装后启动应用程序时禁用保护组件和扫描任务。 禁用保护组件后的安装很方便，例如，为了重现应用程序操作中的问题并创建跟踪文件。 如果启用了必要的组件和任务，则应用程序重启后，启用的组件和任务将继续工作。

在 Light Agent 模式下使用应用程序	如果您希望在 Light Agent 模式下使用应用程序来保护虚拟环境（作为 Kaspersky Security for Virtualization Light Agent 的一部分），请选中此复选框。 如果清除此复选框，则将在标准模式下使用应用程序。
启用 VDI 保护模式。	选中此复选框以启用 VDI 保护模式。如果要在将用于创建临时虚拟机的虚拟机模板上安装应用程序，建议启用此模式。 仅当在 Light Agent 模式下使用应用程序时，才应用此设置。
受保护虚拟机用作服务器。	如果安装应用程序的虚拟机在虚拟基础架构中用作服务器，请选中此复选框。 仅当在 Light Agent 模式下使用应用程序时，才应用此设置。

在管理控制台中创建安装包

在创建 Kaspersky Endpoint Security 安装包之前，需要准备安装包中包含的文件。

要准备用于创建安装包的文件：

1. 从应用程序下载页面下载 kesl.zip 压缩文件。它位于 **Kaspersky Endpoint Security for Linux**（**其他分发 -> 用于远程安装产品的文件**）中。
2. 将 kesl.zip 压缩文件解压到可供 Kaspersky Security Center Administration Server 访问的一个文件夹中。将对应于要安装应用程序的操作系统类型及其软件包管理器类型的分发文件放在同一文件夹中：
   - 要安装 Kaspersky Endpoint Security：
     - kesl-12.1.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl_12.1.0-<版本号>_i386.deb（适用于使用 dpkg 的 32 位操作系统）
     - kesl-12.1.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）
     - kesl_12.1.0-<版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
     - kesl-12.1.0-<版本号>.aarch64.rpm（适用于 Arm 架构的使用 rpm 的 64 位操作系统）
     - kesl-12.1.0-<版本号>_arm64.deb（适用于 Arm 架构的使用 dpkg 的 64 位操作系统）
   - 要安装 GUI：
     - kesl-gui-12.1.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl-gui-12.1.0-<版本号>_i386.deb（适用于使用 dpkg 的 32 位操作系统）
     - kesl-gui-12.1.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）

- kesl-gui-12.1.0-<版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
- kesl-gui-12.1.0-<版本号>.aarch64.rpm（适用于 Arm 架构的使用 rpm 的 64 位操作系统）
- kesl-gui-12.1.0-<版本号>_arm64.deb（适用于 Arm 架构的使用 dpkg 的 64 位操作系统）

如果您不想安装图形用户界面，请不要将这些文件放入文件夹中；这会进一步缩小安装包的体积。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则不支持图形用户界面。

注意，如果您不打算使用图形用户界面，则需要在所创建的安装包的属性中或 autoinstall.ini 配置文件中设置 `USE_GUI=No`。否则，安装将失败。

如果您要使用已创建的安装包在多种类型的操作系统或软件包管理器上安装应用程序，请将所有所需类型的操作系统和软件包管理器的文件放入该文件夹中。

3. 如果想要使用配置文件执行应用程序的初始配置，请打开 autoinstall.ini 配置文件并根据需要进行编辑。autoinstall.ini 文件位于 kesl.zip 压缩文件所解压到的文件夹中。

   如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则需要在 autoinstall.ini 配置文件中设置 `KSVLA_MODE=yes`。

4. 如果您计划在标准模式下使用 Kaspersky Endpoint Security 并希望使用之前下载的数据库，请将准备好的包含适用于所有所需操作系统类型的数据库的压缩文件放入该文件夹中。打开 autoinstall.ini 配置文件并指定 `UPDATE_EXECUTE=no`。autoinstall.ini 文件位于将 kesl.zip 压缩文件解压到的文件夹。

要在 Kaspersky Security Center 管理控制台中创建 Kaspersky Endpoint Security 安装包：

1. 在控制台树中，选择**附加 → 远程安装 → 安装包**。
2. 单击**“创建安装包”**按钮。

   创建安装包的向导将启动。
3. 在打开的向导窗口中，单击**“为卡巴斯基应用程序创建安装包”**按钮。
4. 指定新安装包的名称并继续下一步。
5. 选择 Kaspersky Endpoint Security 分发包。为此，请使用**“浏览”**按钮打开标准浏览窗口，然后指定 kesl.kud 文件的路径。该文件位于 kesl.zip 压缩文件所解压到的文件夹中。

   应用程序名称显示在窗口中。

   继续下一步。
6. 请阅读您与 Kaspersky 之间的最终用户授权许可协议，以及描述数据处理和传输的隐私策略。

   要继续创建安装包，请确认您已完全阅读并接受授权许可协议和隐私策略的条款。要进行确认，请在打开的窗口中选中两个复选框。

   继续下一步。
7. 该向导下载将应用程序安装到 Kaspersky Security Center Administration Server 所需的文件。等待下载完成。

8. 完成向导。

创建的安装包位于 Kaspersky Security Center 管理控制台树的**附加** → **远程安装** → **安装包**文件夹。您可以多次使用相同的安装包。

准备包含应用程序数据库的压缩文件，以创建包含集成数据库的安装包

在某些情况下，您可能需要创建包含预先下载的应用程序数据库的远程安装包。例如，如果您在运行 Astra Linux Special Edition 操作系统的设备上安装应用程序，或者希望立即安装应用程序，并使用准备好的当前数据库（以避免稍后单独更新数据库）。

要创建带有集成数据库的安装包来安装应用程序：

1. 使用命令行或使用 Kaspersky Security Center 在设备上安装 Kaspersky Endpoint Security 并执行初始配置。
2. 更新应用程序数据库。您可以在应用程序初始配置期间或安装后更新数据库，方法是在命令行中运行 Update 类型的任务，或在 Kaspersky Security Center 管理控制台或 Kaspersky Security Center Web Console 中运行 *Update* 任务。
3. 将 /var/opt/kaspersky/kesl/private/updates/ 目录的内容复制到以下子目录之一，具体取决于您要为其创建带有集成数据库的安装包的操作系统的架构：/i386/、/x86_64/ 或 /arm64/。
4. 将包含数据库的目录放入 kesl-bases.tgz 压缩文件中，保留嵌套目录的结构。您只能在压缩文件中放置一个子目录，其中包含适用于所需操作系统架构的数据库，或者如果您计划创建适用于多个具有不同架构的操作系统的安装包，可以将所有适用于不同架构的包含数据库的子目录（/i386/、/x86_64/ 或 /arm64/）放置在单个压缩文件中。
5. 在 Kaspersky Security Center 管理控制台或 Kaspersky Security Center Web Console 中创建安装包时，可以使用所创建的包含应用程序数据库的压缩文件。

Autoinstall.ini 配置文件设置

在 autoinstall.ini 配置文件中，可以指定下表所示的设置。适用的设置集取决于应用程序的使用模式。

Autoinstall.ini 配置文件设置

设置	描述	值
KSVLA_MODE	Kaspersky Endpoint Security 使用模式。	yes – 在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境（用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。 no（默认值）– 在标准模式下使用 Kaspersky Endpoint Security。
SERVER_MODE	受保护虚拟机的角色（服务器或工作站）。 仅当在 Light Agent 模式下使用应用程序时，才应用此设置。	yes（默认值） – 受保护虚拟机用作服务器。 no – 受保护虚拟机用作工作站。

VDI_MODE	启用 VDI 保护模式，以优化临时虚拟机上的应用程序性能。 仅当在 Light Agent 模式下使用应用程序时，才应用此设置。	yes – 启用 VDI 保护模式。如果要在将用于创建临时虚拟机的虚拟机模板上安装 Kaspersky Endpoint Security，建议这样操作。 no（默认值）– 不启用 VDI 保护模式。
EULA_AGREED	必要设置。 接受最终用户授权许可协议条款。	yes（默认值）– 接受最终用户授权许可协议的条款以继续应用程序安装过程。 no — 不接受最终用户授权许可协议。应用程序安装将终止。
PRIVACY_POLICY_AGREED	必要设置。 接受隐私策略条款。	yes（默认值）– 接受隐私策略的条款以继续应用程序安装过程。 no：不接受隐私策略。应用程序安装将终止。
USE_KSN	必要设置。 启用卡巴斯基安全网络：要启用 KSN，必须接受卡巴斯基安全网络声明的条款。	yes – 接受卡巴斯基安全网络声明的条款并启用 KSN。 no（默认值）– 不接受卡巴斯基安全网络声明。 如果在标准模式下使用 Kaspersky Endpoint Security 并且您已启用 KSN，则会自动启用该应用程序的云模式。在此模式下，Kaspersky Endpoint Security 使用轻量级版本的恶意软件数据库。
GROUP_CLEAN	必要设置。 从 kesladmin 和 keslaudit 特权组中删除用户。	是 – 从特权组中删除用户。如果值为“是”并且没有 nogroup 组，安装将失败，并且您将被提示手动从特权组中删除用户。 否 – 不从特权组中删除用户。
LOCALE	可选设置。 发送到 Kaspersky Security Center 的应用程序事件使用的区域设置。	区域设置采用 RFC 3066 指定的格式。 如果未指定 Locale 设置，则使用操作系统区域设置。如果应用程序无法确定操作系统本地化语言或不支持操作系统本地化，则将使用默认值 – en_US.utf8。 图形界面和应用程序命令行的区域设置取决于 LANG 环境变量的值。如果将 Kaspersky Endpoint Security 不支持的区域设置指定为 LANG 环境变量的值，则图形界面和命令行将以英语显示。
INSTALL_LICENSE	激活码或密钥文件。 只有在标准模式下使用应用程序时，该设置才适用。	

UPDATER_SOURCE	更新源。 只有在标准模式下使用应用程序时，该设置才适用。	SCServer —使用 Kaspersky Security Center 管理服务器作为更新源。 KLServers — 使用卡巴斯基服务器作为更新源。默认情况下使用此值。 更新源地址
PROXY_SERVER	用于连接到互联网的代理服务器的地址。 只有在标准模式下使用应用程序时，该设置才适用。	代理服务器地址
UPDATE_EXECUTE	在安装过程中启动应用程序数据库更新任务。 只有在标准模式下使用应用程序时，该设置才适用。	yes（默认值）– 启动更新任务。 no — 不启动更新任务。
KERNEL_SRCS_INSTALL	自动启动内核模块编译。	yes（默认值）— 编译内核模块。 no — 不编译内核模块。
USE_GUI	使用图形用户界面。 只有在标准模式下使用应用程序时，该设置才适用。	yes – 启用图形用户界面。 no（默认值）– 禁用图形用户界面。
ADMIN_USER	被分配了管理员角色 (admin) 的用户。	否
CONFIGURE_SELINUX	自动配置 SELinux 以使用 Kaspersky Endpoint Security。	yes（默认值）– 自动配置 SELinux 以使用 Kaspersky Endpoint Security。 no – 不自动配置 SELinux 以使用 Kaspersky Endpoint Security。
DISABLE_PROTECTION	安装后禁用应用程序的功能组件。 例如，在禁用组件的情况下安装应用程序，可便于重现应用程序的问题并创建跟踪文件。 如果在使用 DISABLE_PROTECTION = yes 参数安装应用程序后启用了必要的组件，则启用的组件将在应用程序重启后继续工作。	是 – 在安装后启动应用程序时，禁用保护组件和扫描任务。 否 – 在安装后启动应用程序时，不禁用保护组件和扫描任务。
DISABLE_FILEAV_ACTIONS	在安装应用程序组件后禁用应	yes：安装后启动应用程序时禁用清除和

	用程序组件的清除和文件删除功能。 如果禁用了清除和文件删除功能并检测到威胁，则应用程序将仅通知用户在文件中检测到威胁，不会尝试清除或删除检测到威胁的文件。 安装应用程序后，您可以使用 kesl.ini 配置文件中的 `DisableFileAvActions` 参数启用文件清除和删除功能。	文件删除功能。 no（默认值）：安装后启动应用程序时不禁用清除和文件删除功能。

如果要更改 autoinstall.ini 配置文件中的设置，请按以下格式指定设置的值：<设置名称>=<设置值>（应用程序不处理设置名称与其值之间的空格）。

使用 Kaspersky Security Center 开始

通过 Kaspersky Security Center 部署 Kaspersky Endpoint Security 后，必须为该应用程序的运行做好准备。要执行的操作取决于您计划使用 Kaspersky Endpoint Security 时所用的模式。

标准模式

如果您计划在标准模式下使用 Kaspersky Endpoint Security，请在部署应用程序后执行以下操作：

- 激活应用程序。您可以使用管理控制台或 Kaspersky Security Center Web Console 创建和执行激活任务，还可以将授权许可密钥从 Kaspersky Security Center 密钥存储分发到设备。
- 使用管理控制台或 Kaspersky Security Center Web Console 更新应用程序数据库和模块。您可以使用*更新*任务，该任务是在安装 MMC 管理插件或 Kaspersky Endpoint Security Web 管理插件后由 Kaspersky Security Center 的初始配置向导自动创建的。
- 使用 Kaspersky Security Center 管理控制台或 Web Console 配置集中管理应用程序的策略。您可以使用在安装 MMC 管理插件或 Kaspersky Endpoint Security Web 管理插件后由 Kaspersky Security Center 的初始配置向导自动创建的策略。

  您还可以使用管理控制台或 Web Console 配置应用程序管理任务。

Light Agent 模式

如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，请在部署应用程序后执行以下操作：

1. 配置 Light Agent 的 SVM 检测设置。为此，您需要创建并配置策略，以在客户端设备上集中管理应用程序。您可以使用管理控制台或 Web Console 处理策略。

   需要在策略属性中配置以下设置：

   - 用于将 Light Agent 连接到 Integration Server 的设置。
   - 用于将 Light Agent 连接到 SVM 的设置。

2. 确保在 Light Agent 和 SVM 与 Integration Server 之间建立了连接。

   可以通过在受保护虚拟机上使用 Kaspersky Endpoint Security 命令来获取连接信息：

   - 可以使用 `kesl-control [-V] --svm-info` 命令查看与 SVM 的连接信息。
   - 可以使用 `kesl-control [-V] --viis-info` 命令查看与 Integration Server 的连接信息。

3. 确保用作 Light Agent 的 Kaspersky Endpoint Security 接收到有关激活 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的授权许可的信息。

   在 SVM 上激活解决方案并将 Light Agent 连接到 SVM 后，Protection Server 组件会将授权许可信息发送到 Light Agent 。可以使用 `kesl-control -L --query` 命令在受保护虚拟机上查看用作解决方案一部分的 Kaspersky Endpoint Security 所用的授权许可的相关信息。

4. 确保在受保护虚拟机上安装了 Light Agent 运行所需的数据库更新。

   受保护虚拟机上的数据库通过一个特殊的*更新*任务进行更新，在该任务中， SVM 上的一个文件夹被指定为更新源。该更新任务自动启动。

   可以在 Light Agent 中使用 `kesl-control --app-info` 命令来检查受保护虚拟机上数据库的最新情况。

   您还可以使用管理控制台或 Web Console 配置应用程序管理任务。

使用 Kaspersky Security Center 激活应用程序

*激活*是激活授权许可的过程，可让您使用应用程序的完整功能版本，直到授权许可到期。

如果您计划在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，安装后无需激活应用程序。您通过向 SVM 中添加授权许可密钥在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）上激活 Kaspersky Hybrid Cloud Security for Virtualization Light Agent。有关更多详细信息，请参阅 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助。

激活 Kaspersky Endpoint Security 的过程涉及添加应用程序授权许可密钥。

您可以用以下方式通过 Kaspersky Security Center 将授权许可密钥添加到应用程序：

- 通过将密钥添加到 Kaspersky Endpoint Security 安装包。

  此方法允许在部署 Kaspersky Endpoint Security 时在安装包的属性中添加应用程序密钥。应用程序将在安装后自动激活。

- 使用"添加密钥"任务。

  使用此方法可以将授权许可密钥添加到特定设备或属于管理组的设备。您可以使用 Kaspersky Security Center Web Console 或管理控制台创建并运行添加密钥任务。

- 通过将 Kaspersky Security Center 管理服务器上存储的授权许可密钥分发到客户端设备。

  使用此方法可以自动将密钥添加到已连接到 Kaspersky Security Center 的客户端设备和新客户端设备。要使用此方法，请先将密钥添加到 Kaspersky Security Center 管理服务器的密钥存储中。

您可以使用 Kaspersky Security Center 管理控制台或 Kaspersky Security Center Web Console 创建添加密钥到应用程序的任务、将密钥添加到密钥存储以及将密钥分发到客户端设备。

如果您在未包含Kaspersky Endpoint Detection and Response Optimum功能的授权许可下使用该应用程序，则在激活该应用程序后，您需要添加 EDR Optimum 密钥。

使用 Kaspersky Security Center Web Console 激活

在创建添加密钥任务或分发密钥之前，将密钥添加到 Kaspersky Security Center 管理服务器密钥存储。

要使用 Web Console 将密钥添加到 Kaspersky Security Center 密钥存储：

1. 在 Web Console 主窗口中，选择“**操作**”→“**Kaspersky 授权许可**”。
2. 单击“**添加**”。
3. 在打开的窗口中，选择如何将密钥添加到存储库：
   - **输入激活码**以使用激活码添加密钥。
   - **添加密钥文件**以使用密钥文件添加密钥。
4. 根据您在上一步选择的密钥添加方法，执行以下操作之一：
   - 输入激活码，然后单击“**提交**”。
   - 单击“**选择密钥文件**”按钮，然后在打开的窗口中选择具有 key 扩展名的文件。
5. 单击“**关闭**”。

添加的密钥将出现在密钥列表中。

要使用“添加密钥”任务通过 Web Console 向应用程序添加密钥：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**任务**”。
   将打开任务列表。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择应用程序名称：Kaspersky Endpoint Security。
   b. 在“**任务类型**”下拉列表中，选择“**添加密钥**”。
   c. 在“**任务名称**”字段中，输入简短描述，例如“`Activation of Kaspersky Endpoint Security`”。
   d. 在“**任务将分配到的设备**”区域中，选择任务范围。单击“**下一步**”。
4. 按照所选任务范围选项选择设备。单击“**下一步**”。
   将打开“**Kaspersky Security Center 密钥存储**”窗口。
5. 如果您之前已将密钥添加到 Kaspersky Security Center 密钥存储，请从列表中选择该密钥，然后单击“**下一步**”。

6. 如果在密钥存储中找不到所需密钥，请单击“**添加密钥**”按钮。

   a. 在打开的窗口中，选择如何将密钥添加到存储库：

      - **输入激活码**以使用激活码添加密钥。
      - **添加密钥文件**以使用密钥文件添加密钥。

   b. 根据您在上一步选择的密钥添加方法，执行以下操作之一：

      - 输入激活码，然后单击“**提交**”。
      - 单击“**选择密钥文件**”按钮，然后在打开的窗口中选择具有 key 扩展名的文件。

   c. 阅读有关密钥的信息，然后单击“**关闭**”。

   d. 添加的密钥将出现在密钥列表中。从列表中选择该密钥，然后单击“**下一步**”。

7. 阅读有关授权许可的信息，然后单击“**下一步**”。

8. 完成向导。
   在任务列表中将显示一个新任务。

9. 选中任务旁边的复选框。单击**启动**按钮。

在“*添加密钥*”任务的属性中，可以将*备用密钥*添加到设备。当与活动密钥关联的授权许可到期或活动密钥被删除时，备用密钥成为活动密钥。备用密钥可避免当授权许可到期时应用程序功能受限。

> 如果您正在添加备用密钥，但尚未将活动密钥添加到应用程序，则任务将以错误结束。

要使用 Web Console 通过将管理服务器上存储的密钥分发到设备来将密钥添加到应用程序：

1. 在 Web Console 主窗口中，选择**“操作”→“Kaspersky 授权许可”**。

2. 使用带有密钥所适用的应用程序名称的链接打开密钥属性。

3. 在“**常规**”选项卡上，选中“**自动将授权许可密钥分发到受管理设备**”复选框。

4. 单击“**保存**”。

   授权许可密钥将自动分发到相应的客户端设备。在将密钥作为活动密钥或备用密钥进行自动分发的过程中，会考虑对设备数量的授权许可限制（在密钥属性中设置）。如果达到授权许可限制，将自动停止向设备分发此密钥。您可以在“**设备**”选项卡上的密钥属性中查看已添加密钥的设备数量以及其他信息。

您可以通过以下方式使用 Kaspersky Security Center Web Console 控制授权许可使用：

- 查看授权许可密钥使用报告（**监控和报告→报告**）。
- 查看受管理设备的状态（“**资产（设备）**”→“**受管理设备**”）。如果未激活应用程序，则设备的状态为，并且状态说明为“**保护已禁用**”。
- 查看密钥属性（“**操作**”→“**卡巴斯基授权许可**”）。

Kaspersky Security Center 云控制台中激活过程的特殊注意事项

Kaspersky Security Center 云控制台提供了一个试用版。该*试用版*是 Kaspersky Security Center 云控制台的特殊版本，旨在让用户熟悉云控制台的功能。在此版本中，您可以在 30 天内在工作区中执行操作。所有托管应用程序（包括 Kaspersky Endpoint Security）都在 Kaspersky Security Center 云控制台试用授权许可下自动激活。但是，当云控制台的试用授权许可到期后，Kaspersky Endpoint Security 无法使用自己的试用授权许可激活。有关云控制台的更多详细信息，请参阅 Kaspersky Security Center 云控制台文档。

Kaspersky Security Center 云控制台的试用版不允许以后切换到商业版。在 30 天期限到期后，任何试用工作区及其所有内容都将被自动删除。

使用命令行安装和初始配置应用程序

使用命令行安装应用程序时，可以执行以下操作：

- 安装应用程序和图形用户界面。

  如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境（作为 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分），将不支持图形用户界面。只需要安装应用程序包，无需安装图形用户界面。

- 安装应用程序，不安装图形用户界面。
- 在安装应用程序的设备上安装图形用户界面。

  无法在未安装应用程序的设备上安装图形用户界面。

如果 apt 软件包管理器的版本低于 1.1.X，请使用 dpkg/rpm 软件包管理器（取决于操作系统）进行安装。

应用程序安装完成后，以交互或自动方式执行应用程序的初始配置。

使用命令行安装应用程序

安装应用程序，不安装图形用户界面

要从 RPM 软件包将 Kaspersky Endpoint Security 安装到 32 位操作系统，请执行以下命令：

```
# rpm -i kesl-12.1.0-<版本号>.i386.rpm
```

要从 RPM 软件包将 Kaspersky Endpoint Security 安装到 64 位操作系统，请执行以下命令：

```
# rpm -i kesl-12.1.0-<版本号>.x86_64.rpm
```

要从 RPM 软件包将 Kaspersky Endpoint Security 安装到 Arm 架构的 64 位操作系统，请执行以下命令：

```
# rpm -i kesl-12.1.0-<版本号>.aarch64.rpm
```

要从 DEB 软件包将 Kaspersky Endpoint Security 安装到 32 位操作系统，请执行以下命令：

```
# apt-get install ./kesl_12.1.0-<版本号>_i386.deb
```

要从 DEB 软件包将 Kaspersky Endpoint Security 安装到 64 位操作系统，请执行以下命令：

```
# apt-get install ./kesl_12.1.0-<版本号>_amd64.deb
```

要从 DEB 软件包将 Kaspersky Endpoint Security 安装到 Arm 架构的 64 位操作系统，请执行以下命令：

```
# apt-get install ./kesl_12.1.0-<版本号>_arm64.deb
```

图形用户界面安装

若要通过 RPM 软件包将图形用户界面安装到 32 位操作系统，请执行以下命令：

```
# rpm -i kesl-gui-12.1.0-<版本号>.i386.rpm
```

若要通过 RPM 软件包将图形用户界面安装到 64 位操作系统，请执行以下命令：

```
# rpm -i kesl-gui-12.1.0-<版本号>.x86_64.rpm
```

要从 RPM 软件包将图形用户界面安装到 Arm 架构的 64 位操作系统，请执行以下命令：

```
# rpm -i kesl-gui-12.1.0-<版本号>.aarch64.rpm
```

若要通过 DEB 软件包将图形用户界面安装到 32 位操作系统，请执行以下命令：

```
# apt-get install ./kesl-gui_12.1.0-<版本号>_i386.deb
```

若要通过 DEB 软件包将图形用户界面安装到 64 位操作系统，请执行以下命令：

```
# apt-get install ./kesl-gui_12.1.0-<版本号>_amd64.deb
```

要从 DEB 软件包将图形用户界面安装到 Arm 架构的 64 位操作系统，请执行以下命令：

```
# apt-get install ./kesl-gui_12.1.0-<版本号>_arm64.deb
```

以交互模式对应用程序进行初始配置

使用命令行安装 Kaspersky Endpoint Security 后，通过运行初始配置脚本来执行初始应用程序设置。初始配置脚本包含在 Kaspersky Endpoint Security 分发包中。

使用命令行安装应用程序后，需要执行初始设置才能启用对客户端设备的保护。

要运行 Kaspersky Endpoint Security 初始配置脚本，请执行以下命令：

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

Kaspersky Endpoint Security 软件包安装完成后，必须以 root 特权运行初始配置脚本。该脚本会逐步请求提供 Kaspersky Endpoint Security 设置的值。脚本执行完成和控制台释放表明初始应用程序设置已完成。

要检查返回码，执行以下命令：

```
echo $?
```

如果命令返回代码 0，则初始应用程序设置成功完成。

选择应用程序使用模式

在此步骤中，选择 Kaspersky Endpoint Security 使用模式：

- 如果要在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，请输入“yes”。
- 如果要在标准模式下使用 Kaspersky Endpoint Security，请输入“no”。

初始配置完成后，即无法更改应用程序使用模式。

定义虚拟机的角色

只有在第一步中选择在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境时，才会显示此步骤。

在此步骤中，指定要安装 Kaspersky Endpoint Security 的虚拟机的角色（服务器或工作站）：

- 如果要将虚拟机作为服务器，请输入 是。
- 如果要将虚拟机作为工作站，请输入 否。

启用 VDI 保护模式

只有在第一步中选择在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境时，才会显示此步骤。

在此步骤中，可以启用 VDI 保护模式。此模式可以优化 Kaspersky Endpoint Security 在临时虚拟机上的操作。如果启用 VDI 保护模式，则不会安装需要重启虚拟机的更新。当接收到需要重启的更新时，安装在虚拟机上的 Light Agent 会向 Kaspersky Security Center 发送消息，告知需要更新受保护虚拟机模板。

如果要启用 VDI 保护模式，请指定“yes”。如果要在将用于创建临时虚拟机的虚拟机模板上安装 Kaspersky Endpoint Security，建议这样操作。

如果不希望启用 VDI 保护模式，请指定“no”。如果要在持久虚拟机或将用于创建持久虚拟机的虚拟机模板上安装 Kaspersky Endpoint Security，建议这样指定。

选择区域设置

在此步骤中，应用程序以 RFC 3066 格式显示支持的区域设置标识符列表。

以该列表中确定的格式指定区域设置。该区域设置将用于发送到 Kaspersky Security Center 的应用程序事件，以及授权许可协议、隐私策略和卡巴斯基安全网络声明的文本。

图形界面和应用程序命令行的区域设置取决于 LANG 环境变量的值。如果将 Kaspersky Endpoint Security 不支持的区域设置指定为 LANG 环境变量的值，则图形界面和命令行将以英语显示。

查看最终用户授权许可协议和隐私策略

在此步骤中，请阅读您与卡巴斯基之间的最终用户授权许可协议，以及描述数据处理和传输的隐私策略。

接受最终用户授权许可协议

在此步骤中，您必须接受或拒绝最终用户授权许可协议的条款。

退出查看模式后，请输入以下值之一：

- 如果您接受最终用户授权许可协议的条款，请输入 yes（或 y）。
- 如果您不接受最终用户授权许可协议的条款，则输入 no（或 n）。

如果您不接受最终用户授权许可协议的条款，则应用程序将终止 Kaspersky Endpoint Security 安装过程。

接受隐私策略

在此步骤中，您必须接受或拒绝隐私策略的条款。

退出查看模式后，请输入以下值之一：

- 如果您接受隐私策略的条款，请输入 yes（或 y）。

- 如果您不接受隐私策略的条款，则输入 no（或 n）。

如果您不接受隐私政策的条款，则应用程序将终止 Kaspersky Endpoint Security 安装过程。

使用卡巴斯基安全网络

在此步骤中，您必须接受或拒绝卡巴斯基安全网络声明中的使用条款。包含卡巴斯基安全网络声明文本的文件 ksn_license.<语言 ID> 位于目录 /opt/kaspersky/kesl/doc/ 中。

输入以下值之一：

- 如果您同意卡巴斯基安全网络声明的条款，请输入 yes（或 y）。将启用扩展 KSN 模式。
- 如果您不同意卡巴斯基安全网络声明的条款，则输入 no（或 n）。

拒绝参与卡巴斯基安全网络不会中断 Kaspersky Endpoint Security 初始应用程序设置。您可以随时启用、禁用或更改卡巴斯基安全网络模式。

如果在标准模式下使用 Kaspersky Endpoint Security 并且您已启用卡巴斯基安全网络，则会自动启用该应用程序的云模式。在此模式下，Kaspersky Endpoint Security 使用轻量级版本的反恶意软件数据库。Light Agent 模式不支持使用轻量级反恶意软件数据库来保护虚拟环境。

从特权组中删除用户

只有在 kesladmin 组和/或 keslaudit 组中检测到用户时，才会显示此步骤。

在此步骤中，指定是否从 kesladmin 和 keslaudit 特权组中删除用户。kesladmin 和 keslaudit 组中包含的用户将获得访问应用程序功能的特权。

要从 kesladmin 和/或 keslaudit 组中删除所有检测到的用户，请输入 是。主组为 kesladmin 或 keslaudit 的用户将被移至 nogroup 组。如果没有 nogroup 组，安装将失败，并且您将被提示手动从特权组中删除用户。

如果不希望应用程序从特权组中删除用户，请输入 否。

将管理员角色分配给一位用户

在此步骤中，您可以向用户授予管理员 (admin) 角色。

输入要向其授予管理员角色的用户的名称。

您也可以在后续随时向用户授予管理员角色。

确定文件操作拦截器类型

在此步骤中，确定所用操作系统的文件操作拦截器的类型。对于不支持 fanotify 技术的操作系统，将启动内核模块编译。

如果在内核模块编译过程中未检测到必需的软件包，则 Kaspersky Endpoint Security 会提示您安装它们。如果软件包下载失败，将显示一条错误消息。

如果所有必要软件包均可用，在文件威胁防护任务启动时将会自动编译内核模块。

您可以在 Kaspersky Endpoint Security 初始配置完成后编译内核模块。

启用 SELinux 的自动配置

仅当您的操作系统上安装了 SELinux 时，才会显示此步骤。

在此步骤中，您可以启用 SELinux 的自动配置，以使用 Kaspersky Endpoint Security。

输入 `yes` 可启用 SELinux 的自动配置。如果 SELinux 无法自动配置，应用程序会显示错误消息并提示用户手动配置 SELinux。

如果您不希望应用程序自动配置 SELinux，请输入 `no`。

默认情况下，应用程序建议为 `yes`。

如有必要，在 Kaspersky Endpoint Security 的初始设置完成后，您可以手动配置 SELinux，以在稍后使用应用程序。

配置更新源

只有在第一步中选择在标准模式下使用 Kaspersky Endpoint Security 时，才会显示此步骤。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收 Light Agent 的数据库和应用模块更新。

在此步骤中，为数据库和应用程序模块指定更新源。

输入以下值之一：

- `KLServers`：应用程序从一个卡巴斯基更新服务器接收更新。
- `SCServer`：应用程序将更新从组织内安装的 Kaspersky Security Center 管理服务器下载到受保护设备。如果您使用 Kaspersky Security Center 对您组织中的设备保护进行集中管理，则可以选择此更新源。
- `<URL>`：应用程序从自定义源下载更新。您可以在局域网或互联网上指定自定义更新源的地址。
- `<path>` 应用程序从指定目录接收更新。

配置代理服务器设置

只有在第一步中选择在标准模式下使用 Kaspersky Endpoint Security 时，才会显示此步骤。

在此步骤中，如果您正在使用代理服务器访问互联网，则必须指定代理服务器设置。从更新服务器下载应用程序数据库需要互联网连接。

要配置代理服务器设置，请执行以下操作之一：

- 如果使用代理服务器连接到互联网，请使用以下格式之一指定代理服务器的地址：
  - < 代理服务器的 IP 地址 >:< 端口号 >（如果代理服务器连接不需要身份验证）；
  - < 用户名 >:< 密码 >@< 代理服务器的 IP 地址 >:< 端口号 >（如果代理服务器连接需要身份验证）。

    通过 HTTP 代理连接时，我们建议使用不用于登录其他系统的单独账户。HTTP 代理使用不安全的连接，账户可能会被入侵。
- 如果不使用代理服务器连接到互联网，请输入 no 作为答案。

默认情况下，应用程序建议为 no。

您可以稍后配置代理服务器设置，而不使用初始配置脚本。

启动应用程序数据库更新

只有在第一步中选择在标准模式下使用 Kaspersky Endpoint Security 时，才会显示此步骤。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收 Light Agent 的数据库和应用模块更新。

在此步骤中，您可以在客户端设备上运行应用程序数据库更新任务。应用程序数据库包含威胁特征码的描述及其处理方式。应用程序会在搜索和消除威胁时使用这些记录。卡巴斯基病毒分析人员会定期添加有关威胁的新记录。

如果您不想开始下载应用程序数据库，请输入 no。

如果想要在设备上启动数据库更新任务，请输入 yes 。

默认情况下，应用程序建议为 yes。

如果选择 yes ，则数据库更新后应用程序将自动重新启动。

只有更新应用程序数据库后，Kaspersky Endpoint Security 才能保护设备。

您可以稍后启动 Update 任务，而不使用初始配置脚本。

启用应用程序数据库自动更新

只有在第一步中选择在标准模式下使用 Kaspersky Endpoint Security 时，才会显示此步骤。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收 Light Agent 的数据库和应用模块更新。

在此步骤中，您可以启用应用程序数据库的自动更新。

输入 yes 以启用应用程序数据库自动更新。默认情况下，应用程序每 60 分钟检查一次可用的数据库更新。如果有更新，应用程序会下载更新的数据库。

如果不希望应用程序自动更新数据库，请输入 no。

通过配置更新任务计划，可以启用稍后自动更新数据库，而不使用初始配置脚本。

应用程序激活

只有在第一步中选择在标准模式下使用 Kaspersky Endpoint Security 时，才会显示此步骤。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收有关授权许可的信息；不需要单独激活 Kaspersky Endpoint Security。

在此步骤中，您可以使用激活码或密钥文件来激活应用程序。

要使用激活码激活应用程序，请输入激活码。

要使用密钥文件激活应用程序，请指定密钥文件的完整路径。

如果未指定激活码或密钥文件，则将使用试用密钥激活该应用程序一个月。

您可以稍后激活应用程序，而不使用初始配置脚本。

以自动模式对应用程序进行初始配置

您可以在自动模式下执行初始应用程序设置。

要启动应用程序的自动初始设置，请执行以下命令：

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=< 初始配置文件 >
```

其中，< 安装后配置文件 > 是包含初始配置设置的配置文件的路径。您可以创建该文件，或从 autoinstall.ini 配置文件（用于使用 Kaspersky Security Center 远程安装应用程序）复制必要的结构。

当初始设置脚本完成并释放控制台后，应用程序的初始设置完成。

要检查返回码，执行以下命令：

```
echo $?
```

如果命令返回代码 0，则初始应用程序设置成功完成。

要在脚本完成后正确更新应用程序模块，您可能需要重新启动应用程序。使用 `kesl-control --app-info` 命令检查应用程序的更新状态。

初始设置配置文件中的设置

在安装后配置文件中，可以指定下表所示的设置。适用的设置集取决于应用程序的使用模式。

初始设置配置文件中的设置

设置	描述	值
KSVLA_MODE	Kaspersky Endpoint Security 使用模式。	yes – 在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境（用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。 否 – 在标准模式下使用 Kaspersky Endpoint Security。
SERVER_MODE	受保护虚拟机的角色（服务器或工作站）。 仅当在 Light Agent 模式下使用应用程序时，才应用此设置。	是 – 受保护虚拟机用作服务器。 no – 受保护虚拟机用作工作站。
VDI_MODE	启用 VDI 保护模式，以优化临时虚拟机上的应用程序性能。 仅当在 Light Agent 模式下使用应用程序时，才应用此设置。	yes – 启用 VDI 保护模式。如果要在将用于创建临时虚拟机的虚拟机模板上安装 Kaspersky Endpoint Security，建议这样操作。 no – 不启用 VDI 保护模式。
EULA_AGREED	必要设置。 接受最终用户授权许可协议条款。	yes：接受最终用户授权许可协议的条款以继续进行应用程序安装。 no — 不接受最终用户授权许可协议。应用程序安装将终止。
PRIVACY_POLICY_AGREED	必要设置。 接受隐私策略条款。	yes：接受隐私策略以继续安装应用程序。 no：不接受隐私策略。应用程序安装将终止。
USE_KSN	必要设置。 启用卡巴斯基安全网络：要启用 KSN，必须接受卡巴斯基安全网络声明的条款。	yes – 接受卡巴斯基安全网络声明的条款并启用 KSN。 no – 不接受卡巴斯基安全网络声明。

		如果在标准模式下使用 Kaspersky Endpoint Security 并且您已启用 KSN，则会自动启用该应用程序的云模式。在此模式下，Kaspersky Endpoint Security 使用轻量级版本的恶意软件数据库。
GROUP_CLEAN	必要设置。 从 kesladmin 和 keslaudit 特权组中删除用户。	是 – 从特权组中删除用户。如果值为“是”并且没有 nogroup 组，安装将失败，并且您将被提示手动从特权组中删除用户。 否 – 不从特权组中删除用户。
LOCALE	可选设置。 发送到 Kaspersky Security Center 的应用程序事件使用的区域设置。	区域设置采用 RFC 3066 指定的格式。 如果未指定 `Locale` 设置，则使用操作系统区域设置。如果应用程序无法确定操作系统本地化语言或不支持操作系统本地化，则将使用默认值 – `en_US.utf8`。 图形界面和应用程序命令行的区域设置取决于 `LANG` 环境变量的值。如果将 Kaspersky Endpoint Security 不支持的区域设置指定为 `LANG` 环境变量的值，则图形界面和命令行将以英语显示。
INSTALL_LICENSE	激活码或密钥文件。 只有在标准模式下使用应用程序时，该设置才适用。	
UPDATER_SOURCE	更新源。 只有在标准模式下使用应用程序时，该设置才适用。	`SCServer` —使用 Kaspersky Security Center 管理服务器作为更新源。 `KLServers` — 使用卡巴斯基服务器作为更新源。 更新源地址
PROXY_SERVER	用于连接到互联网的代理服务器的地址。 只有在标准模式下使用应用程序时，该设置才适用。	代理服务器地址
UPDATE_EXECUTE	在安装过程中启动应用程序数据库更新任务。	`yes` — 启动更新任务。 `no` — 不启动更新任务。

	只有在标准模式下使用应用程序时，该设置才适用。	
KERNEL_SRCS_INSTALL	自动启动内核模块编译。	yes — 编译内核模块。 no — 不编译内核模块。
ADMIN_USER	被分配了管理员角色 (admin) 的用户。	
CONFIGURE_SELINUX	自动配置 SELinux 以使用 Kaspersky Endpoint Security。	yes – 自动配置 SELinux 以使用 Kaspersky Endpoint Security。 no – 不自动配置 SELinux 以使用 Kaspersky Endpoint Security。
DISABLE_PROTECTION	安装应用程序后禁用保护组件和扫描任务。 禁用保护组件后的安装很方便，例如，为了重现应用程序操作中的问题并创建跟踪文件。 如果在使用 DISABLE_PROTECTION = yes 参数安装应用程序后启用了必要的组件和任务，则启用的组件和任务将在应用程序重启后继续工作。	是 – 在安装后启动应用程序时，禁用保护组件和扫描任务。 否 – 在安装后启动应用程序时，不禁用保护组件和扫描任务。
DISABLE_FILEAV_ACTIONS	在安装应用程序组件后禁用应用程序组件的清除和文件删除功能。 如果禁用了清除和文件删除功能并检测到威胁，则应用程序将仅通知用户检测到威胁，不会尝试清除或删除检测到威胁的文件。 安装应用程序后，您可以使用 kesl.ini 配置文件中的 DisableFileAvActions 参数启用文件清除和删除功能。	yes：安装后启动应用程序时禁用清除和文件删除功能。 no（默认值）：安装后启动应用程序时不禁用清除和文件删除功能。

如果要更改应用程序初始设置的配置文件中的设置，请按以下格式指定设置的值：<设置名称>=<设置值>（应用程序不处理设置名称与其值之间的空格）。

在 SELinux 系统中配置权限

手动配置 SELinux 以与应用程序配合使用

如果在应用程序的初始设置期间无法自动配置 SELinux，或者您拒绝了自动配置，您可以手动配置 SELinux 以使用 Kaspersky Endpoint Security。

要手动配置 SELinux 以使用应用程序：

1. 将 SELinux 切换为宽容模式：
   - 如果已激活 SELinux，请执行以下命令：

     ```
     # setenforce Permissive
     ```

   - 如果禁用了 SELinux，请在配置文件 /etc/SELinux/config 中设定 `SELINUX=permissive` 设置，然后重新启动操作系统。
2. 确保 semanage 实用程序已安装在系统。如果未安装该实用程序，请安装 policycoreutils-python 或 policycoreutils-python-utils 包，具体取决于包管理器。
3. 如果您使用自定义 SELinux 策略而不是默认的目标策略，请根据所使用的 SELinux 策略为 Kaspersky Endpoint Security 的每个源可执行文件分配一个标签。为此，请运行以下命令：

   ```
   # semanage fcontext -a -t bin_t <可执行文件>
   # restorecon -v <可执行文件>
   ```

   其中`<executable file>`是：
   - /var/opt/kaspersky/kesl/12.1.0.<版本号>_<安装时间戳>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.1.0.<版本号>_<安装时间戳>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.1.0.<版本号>_<安装时间戳>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.1.0.<版本号>_<安装时间戳>/opt/kaspersky/kesl/shared/kesl
4. 运行以下任务：
   - 文件威胁防护任务：

     ```
     kesl-control --start-task 1
     ```

   - 关键区域扫描任务：

     ```
     kesl-control --start-task 4 -W
     ```

   推荐使用 Kaspersky Endpoint Security 运行您计划运行的所有任务。
5. 启动图形用户界面（如果您计划使用它）。
6. 确保 audit.log 文件中没有错误：

   ```
   # grep kesl /var/log/audit/audit.log
   ```

7. 如果 audit.log 文件中存在错误，请根据阻止记录创建并下载新的规则模块以修复错误，然后重启计划在使用 Kaspersky Endpoint Security 时运行的所有任务。为此，请运行以下命令：

   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```

如果出现与 Kaspersky Endpoint Security 相关的新审计消息，则必须更新包含规则模块文件的文件。

8. 将 SELinux 切换为阻止模式：

```
# setenforce Enforcing
```

如果使用自定义 SELinux 策略，请在安装应用程序更新后为 Kaspersky Endpoint Security 源可执行文件手动分配标签（执行步骤 1、3–8）。

您可以在操作系统的文档中找到更多信息。

配置 SELinux 以运行“启动进程”任务

如果 SELinux 以 `Enforcing` 模式安装在您的操作系统中，则启动启动进程任务需要对 SELinux 进行额外配置。

配置 SELinux 以运行“启动进程”任务

1. 将 SELinux 切换为宽容模式：
   - 如果已激活 SELinux，请执行以下命令：

     ```
     # setenforce Permissive
     ```

   - 如果禁用了 SELinux，请在配置文件 /etc/SELinux/config 中设定 `SELINUX=permissive` 设置，然后重新启动操作系统。
2. 确保 semanage 实用程序已安装在系统。如果未安装该实用程序，请安装 policycoreutils-python 或 policycoreutils-python-utils 包，具体取决于包管理器。
3. 启动“启动进程”任务。
4. 确保 audit.log 文件中没有错误：

   ```
   # grep kesl /var/log/audit/audit.log
   ```

5. 如果 audit.log 文件中存在错误，则根据阻止规则创建并加载新的规则模块来修复错误，然后再次运行“启动进程”任务。

   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```

6. 将 SELinux 切换为阻止模式：

   ```
   # setenforce Enforcing
   ```

在封闭软件环境模式下针对 Astra Linux OS 运行应用程序

本节介绍如何在 Astra Linux Special Edition 操作系统中启动应用程序。

适用于 Astra Linux Special Edition (operational update 1.7) 和 Astra Linux Special Edition (operational update 1.6)

要在 Astra Linux Special Edition (operational update 1.7) 或 Astra Linux Special Edition (operational update 1.6) 操作系统上启动应用程序：

1. 在 /etc/digsig/digsig_initramfs.conf 文件中指定以下设置：

   ```
   DIGSIG_ELF_MODE=1
   ```

2. 安装兼容包：

   ```
   apt install astra-digsig-oldkeys
   ```

3. 为应用程序密钥创建一个目录：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. 将应用程序密钥 (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) 置于上一步中创建的目录中：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. 更新 initramfs 映像：

   ```
   update-initramfs -u -k all
   ```

对于 Astra Linux Special Edition（operational update 1.5）

要在 Astra Linux Special Edition (operational update 1.5) 操作系统中运行应用程序：

1. 在 /etc/digsig/digsig_initramfs.conf 文件中指定以下设置：

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. 为应用程序密钥创建一个目录：

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

3. 将应用程序密钥 (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) 置于上一步中创建的目录中：

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

4. 更新 initramfs 映像：

   ```
   sudo update-initramfs -u -k all
   ```

在强制访问控制会话期间，可以使用应用程序图形用户界面。

从先前的版本更新应用程序

只有 Kaspersky Endpoint Security 12.0 for Linux 可以更新到 Kaspersky Endpoint Security 12.1 for Linux。

不支持将更早的 Kaspersky Endpoint Security 版本升级到版本 12.1。如果您安装了更早版本的 Kaspersky Endpoint Security，则需要先将其卸载，然后安装 Kaspersky Endpoint Security 12.1 for Linux。

在安装 Kaspersky Endpoint Security 之前，您需要准备安装。

应用程序更新过程包括以下步骤：

1. **更新 Kaspersky Security Center 网络代理**

   如果您使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security，则必须更新受保护设备上的网络代理。通过安装新版本的网络代理来执行更新。

   如果未更新网络代理，则无法使用 Kaspersky Security Center 管理应用程序。

   > 在运行 Astra Linux Special Edition 操作系统的设备上，我们建议使用 Kaspersky Security Center 远程更新网络代理，因为使用 Kaspersky Security Center 管理控制台中的命令行进行更新会创建同一受管理设备的副本，并且旧设备变得不可访问。

   在网络代理更新期间，应用程序将继续正常工作。

2. **更新 Kaspersky Endpoint Security 管理插件**

   如果您使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security，则必须更新 Kaspersky Endpoint Security 管理 Web 插件或 MMC 插件，具体取决于您管理 Kaspersky Security Center 所使用的控制台。

3. **更新受保护设备上的应用程序和图形用户界面**

   您必须更新受保护设备上安装的应用程序。更新后的应用程序保留安装时选择的应用程序使用模式。如果您想在不同的模式下使用应用程序，必须卸载该应用程序，然后再执行应用程序的安装和初始配置。

   如果您在标准模式下使用 Kaspersky Endpoint Security，并且使用应用程序的图形用户界面，则还必须更新图形用户界面。

   您可以通过以下方式更新应用程序和应用程序的图形用户界面：

   - 使用 Kaspersky Security Center 远程执行。
   - 通过命令行在本地操作。

> 如果更新应用程序时发生错误，则会回滚更新，并启动应用程序的先前版本。在这种情况下，将显示一条错误消息，但软件包管理器 (rpm/dpkg) 将指示新版本。

即使 Kaspersky Endpoint Security 在更新过程开始之前启动，只要更新成功完成，就会启动新的应用程序版本。

在将应用程序更新到较新的版本时，先前版本的转储文件将被删除。

> 如果在标准模式下使用 Kaspersky Endpoint Security，我们建议在更新应用程序后启动数据库更新任务。

更新 Kaspersky Endpoint Security 管理插件

通过安装新版本的管理插件来更新 Kaspersky Endpoint Security 的管理插件。根据您使用的 Kaspersky Security Center 管理控制台，您必须安装：

- Kaspersky Endpoint Security 管理 Web 插件
- Kaspersky Endpoint Security MMC 管理插件

为 Kaspersky Endpoint Security 12.0 for Linux 配置的策略和任务与应用程序的更新版本不兼容。如果您使用 Kaspersky Security Center 管理控制台来管理应用程序，则在更新管理 MMC 插件后，您可以使用 Kaspersky Security Center 策略和任务批量转换向导来转换策略和任务（有关详细信息，请参阅Kaspersky Security Center 帮助）。

对于大多数设置，转换后的策略和任务使用为应用程序先前版本配置的值。一些设置被分配特殊值。以前版本的策略和任务中未配置的设置在转换后的策略和任务中采用默认值。

Kaspersky Security Center Web Console 中不提供转换策略和任务的程序。如果使用 Web Console 来管理应用程序，您必须在 Kaspersky Security Center 中为该应用程序创建新的策略和任务。您可以通过导出和导入设置将策略和任务的某些设置值从策略或任务的先前版本迁移到新版本。

安装新版本的 Kaspersky Endpoint Security 管理插件后，先前版本的管理插件仍可继续使用。您可以使用这些插件来管理 Kaspersky Endpoint Security 的先前版本。

如果您已在所有客户端设备上更新了应用程序，则可以卸载先前版本的 Kaspersky Endpoint Security 管理插件。

使用 Kaspersky Security Center 更新应用程序

通过在受保护设备上远程安装新版本的应用程序软件包和图形用户界面来更新应用程序和图形用户界面。

> 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则不支持图形用户界面。

对于远程安装，使用 Kaspersky Endpoint Security 安装包。您可以使用 Kaspersky Security Center Web Console 或管理控制台创建安装包。

Kaspersky Security Center Web Console 支持以下主要部署方法：

- 使用“保护部署向导”安装应用程序。
- 使用远程安装任务安装应用程序。

Kaspersky Security Center 管理控制台支持以下主要部署方法：

- 使用远程安装向导安装应用程序。
- 使用远程安装任务安装应用程序。

有关部署过程的说明，请参阅 Kaspersky Security Center 帮助。

使用命令行更新应用程序

使用命令行更新应用程序，是根据软件包管理器的类型使用 RPM 或 DEB 格式的软件包在设备上安装新版本的应用程序。

如果您使用的是图形用户界面，要进行更新，您必须先使用命令 `rpm -e --nodeps kesl-gui` 卸载先前版本的图形用户界面软件包，然后安装包含图形用户界面 12.1 版文件的软件包。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则不支持图形用户界面。

如果新版本的应用程序更改了最终用户授权许可协议和/或隐私策略的条件，您必须在更新期间接受新条件。阅读新版本的最终用户授权许可协议和/或隐私策略：

- 新版本的最终用户授权许可协议位于（~/.kesl/<应用程序版本>/license.<语言 ID>）目录中。
- 新版本的隐私策略位于（~/.kesl/<应用程序版本>/license.<语言 ID>）目录中。

如果您不接受最终用户授权许可协议和/或隐私策略的条件，应用程序将不会更新。

如果卡巴斯基安全网络声明的条款在新版本的应用程序中发生变化，您需要接受或拒绝加入卡巴斯基安全网络的新使用条款。阅读位于（~/.kesl/<应用程序版本>/ksn_license.<语言 ID>）目录中的新版本文档。拒绝参与卡巴斯基安全网络不会中断 Kaspersky Endpoint Security 更新过程。您可以稍后启用、禁用或更改卡巴斯基安全网络模式。

如果您使用了 KSN 并且接受了先前版本应用程序的卡巴斯基安全网络声明的条件，则更新应用程序时，您需要接受卡巴斯基安全网络声明的条件。否则，将会禁止使用 KSN。

如要在更新期间接受新协议的条件，请使用环境变量 `KESL_EULA_AGREED=yes`、`KESL_PRIVACY_POLICY_AGREED=yes` 和 `KESL_USE_KSN=yes/no`。

要更新应用程序：

1. 根据软件包管理器，使用以下命令安装应用程序软件包。如果您安装了以前版本应用程序的图形用户界面，那么还需要启动包含图形用户界面文件的软件包。

   - 对于 RPM 软件包。

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.1.0-<版本号>.<arch>.rpm [kesl-gui-12.1.0-<版本号>.<arch>.rpm]`

     其中 <arch> 是架构类型：

     - i386 – 用于 32 位操作系统
     - x86_64 – 用于 64 位操作系统
     - aarch64 – 用于 Arm 架构 64 位操作系统

     在基于 rpm 的操作系统上，如果应用程序包和 GUI 包都已安装，我们不建议只更新其中一个包而不更新另一个包。

   - 对于 DEB 软件包：

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.1.0-<版本号>_<arch>.deb [./kesl-gui_12.1.0-<版本号>_<arch>.deb]`

     其中 <arch> 是架构类型：

     - i386 – 用于 32 位操作系统

- amd64 – 用于 64 位操作系统
- arm64 – 用于 Arm 架构 64 位操作系统

> 在基于 dpkg 的操作系统上，如果应用程序包和 GUI 包都已安装，则其中一个包无法在没有另一个包的情况下进行更新。

2. Kaspersky Endpoint Security 将自动重启。

3. 某些操作系统可能需要重新启动。如有必要，应用程序将显示相应的消息。

如果您使用命令行来管理应用程序，那么升级后，大多数应用程序设置都会使用为该应用程序的先前版本配置的值。一些设置被分配特殊值。应用程序先前版本中缺少的设置在应用程序的新版本中采用默认值。

> 更新完成后且应用程序重新启动前对应用程序设置进行的更改不会保存。

更新应用程序时设置参数值的特殊注意事项

如果您使用 Kaspersky Security Center 管理控制台来管理应用程序，并且在更新应用程序后，您想要使用在 Kaspersky Security Center 中为应用程序的先前版本配置的策略和任务设置的值，那么您需要转换策略和任务（详情请参见Kaspersky Security Center 帮助）。

Kaspersky Security Center Web Console 中不提供转换策略和任务的程序。如果使用 Web Console 来管理应用程序，您将需要为应用程序的更新版本创建新的策略和任务。您可以通过导出和导入设置将策略和任务的某些设置从策略或任务的先前版本迁移到新版本。

在命令行上，大多数设置迁移自应用程序的先前版本。您也可以通过将设置导出到文件，然后从该文件导入它们来迁移应用程序设置。

默认值将被分配给应用程序先前版本中不存在的设置。一些设置会被分配特殊值。

排除设置

任务在 MMC 插件中转换后，扫描任务（ODS 类型）和容器扫描任务中的**使用全局排除**和**使用文件威胁防护排除**复选框将被清除。Web 插件不支持任务的转换。

在命令行上更新应用程序后，`UseOASExclusions`和`UseGlobalExclusions`设置被设置为`No`。

卡巴斯基安全网络设置

在 MMC 插件中转换策略后，**“不使用 Kaspersky Endpoint Security”**选项将在策略属性中得到选择。Web 插件不支持策略转换。

在命令行上升级应用程序后，如果在更新时设置了`KESL_USE_KSN=No`，则UseKSN设置将被设置为`No`，如果设置了`KESL_USE_KSN=Yes`，则`UseKSN=Extended`被应用。在其他情况下，`UseKSN`设置的值在更新后不会改变。

要启动或恢复使用卡巴斯基安全网络，您必须执行以下操作：

- 如果使用 MMC 或 Web 插件，请选择**基本 KSN 模式**或**扩展 KSN 模式**。
- 如果使用命令行，请将`UseKSN`设置为`Basic`或`Extended`。

云模式设置

在 MMC 插件中转换策略后，**“启用云模式”**复选框将被清除。Web 插件不支持策略转换。

在命令行上更新应用程序后， `CloudMode`将被设置为：

- 如果升级后`UseKSN=No`，则`CloudMode=No`。
- 如果升级后`UseKSN=Yes`，则`CloudMode=Yes`，`CloudMode=Yes`是在升级前设置的。

如果启用了 KSN，则云模式可用。要启用云模式：

- 如果使用 MMC 或 Web 插件，请选择**扩展 KSN 模式**选项并选中**启用云模式**复选框。
- 如果使用命令行，请将`UseKSN`和`CloudMode`设置为`Yes`。

文件操作拦截模式

如果在应用程序的先前版本中清除了**“扫描期间阻止对文件的访问”**复选框，则在 MMC 插件中转换策略后，“文件威胁防护”任务的**“第一项操作”**将被设置为**“阻止”**。Web 插件不支持策略转换。

在新版本的应用程序中，确定文件操作拦截模式的命令行选项名称已从`InterceptorProtectionMode=Block|Notify`更改为`FileBlockDuringScan=Yes|No`。如果在以前版本的应用程序中，`InterceptorProtectionMode`曾被设置为`Notify`，则在使用命令行更新应用程序后，`FileBlockDuringScan`将被设置为`No`，并且文件威胁防护任务的`FirstAction`设置将被设置为`Block`。

卸载应用程序

卸载 Kaspersky Endpoint Security 包括以下步骤：

1. **卸载应用程序及其图形用户界面**

   从受保护设备卸载应用程序软件包，如果您使用图形用户界面，还需卸载图形用户界面软件包。

   您可以同时卸载应用程序软件包和图形用户界面软件包，或者仅卸载图形用户界面软件包。如果安装了图形用户界面软件包，则无法仅卸载应用程序包。

   您可以通过以下方式卸载应用程序和应用程序的图形用户界面：

   - 使用 Kaspersky Security Center 远程执行。
   - 通过命令行在本地操作。

   > 卸载应用程序时，设备上的所有 Kaspersky Endpoint Security 任务都会停止。

2. **移除网络代理**

   如果您使用 Kaspersky Security Center 来管理 Kaspersky Endpoint Security，则必须从受保护设备卸载网络代理。

   您可以通过以下方式卸载网络代理：

   - 使用 Kaspersky Security Center 远程执行。
   - 通过命令行在本地操作。

3. **卸载 Kaspersky Endpoint Security 管理插件**

   如果您使用 Kaspersky Security Center 来管理 Kaspersky Endpoint Security，则必须卸载 Kaspersky Endpoint Security 管理 Web 插件或 MMC 插件，具体取决于您管理 Kaspersky Security Center 所使用的控制台。

> 卸载应用程序后，该应用程序保存的所有信息都将被删除，授权许可数据库除外。已安装的应用程序证书也会被删除。授权许可数据库已保存，您可以使用它来重新安装应用程序。

如果应用程序安装在 systemd 中，则 systemd 设置将在应用程序卸载后恢复到初始状态。

使用 Kaspersky Security Center 卸载应用程序和网络代理

您可以远程卸载客户端设备上的 Kaspersky Endpoint Security 和网络代理。

在 Kaspersky Security Center Web Console 或管理控制台中使用远程卸载应用程序任务来执行卸载。有关更多详细信息，请参阅 Kaspersky Security Center 帮助系统。

> 如果只想移除图形用户界面而不移除应用程序，请在 autoinstall.ini 配置文件中指定 `USE_GUI=No` 设置值，然后启动远程应用程序安装任务。

卸载在后台进行。应用程序卸载完成后，系统将提示您重新启动客户端设备。

使用命令行卸载应用程序

卸载应用程序包和图形用户界面软件包

要卸载从 RPM 软件包安装的应用程序和图形用户界面，请执行以下命令：

```
# rpm -e kesl kesl-gui
```

要卸载从 DEB 软件包安装的应用程序和图形用户界面，请执行以下命令：

```
# apt-get purge kesl kesl-gui
```

卸载应用程序包，不卸载图形用户界面软件包

要卸载从 RPM 软件包安装的应用程序而不移除图形用户界面软件，请执行以下命令：

```
# rpm -e kesl
```

要卸载从 DEB 软件包安装的应用程序而不移除图形用户界面软件，请执行以下命令：

```
# apt-get purge kesl
```

移除图形用户界面软件包

要移除从 RPM 软件包安装的图形用户界面，请执行以下命令：

```
# rpm -e kesl-gui
```

要移除从 DEB 软件包安装的图形用户界面，请执行以下命令：

```
# apt-get purge kesl-gui
```

卸载过程完成后，会显示有关卸载结果的消息。

使用命令行移除网络代理

要卸载从 RPM 软件包安装到 32 位操作系统上的网络代理，请执行以下命令：

```
# rpm -e klnagent
```

要卸载从 RPM 软件包安装到 64 位操作系统上的网络代理，请执行以下命令：

```
# rpm -e klnagent64
```

要卸载从 DEB 软件包安装到 32 位操作系统上的网络代理，请执行以下命令：

```
# apt-get purge klnagent
```

要卸载从 DEB 软件包安装到 64 位操作系统上的网络代理，请执行以下命令：

```
# apt-get purge klnagent64
```

卸载过程完成后，会显示有关卸载结果的消息。

卸载 Kaspersky Endpoint Security 管理插件

Kaspersky Endpoint Security Web 管理插件已从 Kaspersky Security Center Web Console 的已安装插件列表中卸载（**设置 → Web 插件**）。

要卸载 MMC 插件，请使用从操作系统中用于卸载应用程序的标准工具。在应用程序列表中，选择要卸载的 **Kaspersky Endpoint Security <版本号> for Linux**。

应用程序授权

本节提供 Kaspersky Endpoint Security 授权许可信息。

关于最终用户授权许可协议

*最终用户授权许可协议*是您与 AO Kaspersky Lab 之间达成的约束协议，其中规定了使用应用程序时应遵循的条款。

开始使用该应用程序之前，请仔细通篇阅读“最终用户授权许可协议”的条款。

您可以通过以下方式查看 Kaspersky Endpoint Security 解决方案的最终用户许可协议条款以及描述数据处理和传输的隐私政策：

- 通过阅读 license.<language ID> 文件中的文本。该文件包括在应用程序分发包中。
- 在 Kaspersky Endpoint Security 安装期间。

  在创建应用程序安装包（如果使用 Kaspersky Security Center 安装）时或在初始应用程序配置（如果使用命令行安装）期间，确认您同意最终用户授权许可协议和隐私政策的文本即表示您接受最终用户授权许可协议和隐私政策的条款。如果您不接受最终用户授权许可协议或隐私政策的条款，则必须取消安装应用程序且不得使用该应用程序。

- 在安装 Kaspersky Endpoint Security 后。

  应用程序安装后，包含 Kaspersky Endpoint Security 最终用户授权许可协议和隐私政策文本的文件位于受保护设备的 /opt/kaspersky/kesl/doc/license.<语言 ID>文件夹中。

关于授权许可

*授权许可*是指根据最终用户授权许可协议，在有限时间内授予您使用 Kaspersky Endpoint Security 的权限。

可用功能列表和应用程序的有效期取决于使用该应用程序时所用的授权许可。

提供以下授权许可类型：

- *试用* – 用于试用该应用程序的免费授权许可。

  试用授权许可的有效期很短。当试用版授权许可过期时，所有 Kaspersky Endpoint Security 功能都将被禁用。要继续使用该应用程序，您需要购买商业版的授权许可。

  只能在一个试用期内根据试用授权许可使用应用程序。

- *商用*为付费授权许可。

  当商业授权许可到期后，应用程序的主要功能将停止运行。要继续使用 Kaspersky Endpoint Security，您需要续订商业授权许可。授权许可过期后，您将无法再使用该应用程序，必须将其从设备上卸载。

  建议在授权许可到期前进行续订，以确保继续保护设备免受安全威胁。

关于授权许可证书

*授权许可证书*是与密钥文件或激活码一起提供的文档。

授权许可证书包含有关所提供的授权许可的以下信息：

- 授权许可密钥或订单号
- 关于授权许可用户的信息
- 有关可以使用所提供的授权许可激活的应用程序的信息
- 授权许可的单元数限制（例如，根据该授权许可可以使用应用程序的设备数量）
- 授权许可有效开始日期
- 授权许可到期日期或有效期限
- 授权许可类型

关于授权许可密钥

*授权许可*密钥是一系列位，可用于根据最终用户授权许可协议的条款激活应用程序以供继续使用。授权许可密钥由卡巴斯基生成。

您可以使用下面的方法添加一个授权许可密钥到应用程序：通过应用*密钥文件*或输入*激活码*。在应用程序中添加密钥后，将在应用程序界面中以唯一的字母数字序列形式显示授权许可密钥。

如果违反了最终用户授权许可协议的条款，授权许可密钥可能会被卡巴斯基阻止。如果授权许可密钥被阻止，则添加另一个授权许可密钥才能正常运行应用程序。

Kaspersky Endpoint Security 应用程序支持以下*类型*的授权许可密钥：

- *应用程序密钥*– 用于激活 Kaspersky Endpoint Security 应用程序功能的授权许可密钥。可用的应用程序功能集取决于与应用程序密钥关联的授权许可。
- *EDR Optimum 密钥*– Kaspersky Endpoint Detection and Response Optimum 插件的附加授权许可密钥，用于激活Kaspersky Endpoint Detection and Response Optimum的功能。如果您在不包含 Kaspersky Endpoint Detection and Response Optimum 功能的授权许可下使用该应用程序，则需要此密钥。

授权许可密钥可以是活动密钥，也可以是备用密钥。

*活动授权许可密钥*当前用于运行应用程序。可以将试用授权许可密钥、商业授权许可密钥（商业密钥）或订阅密钥添加为活动密钥。应用程序中每种类型只能添加一个活动密钥。

*保留授权许可密钥*是允许用户使用应用程序但当前未使用的授权许可密钥。与活动授权许可密钥相关联的授权许可过期时，保留授权许可密钥将自动成为活动授权许可密钥。只有在添加了同样类型的活动授权许可密钥之后，才可以添加备用授权许可密钥。

试用授权许可密钥只能作为活动授权许可密钥添加。试用授权许可密钥或订阅密钥不能作为备用授权许可密钥添加。

关于激活码

*激活码*是由 20 个拉丁字母和数字组成的唯一序列。必须输入激活码才能添加用于激活 Kaspersky Endpoint Security 的授权许可密钥。通过在购买 Kaspersky Endpoint Security 或申请 Kaspersky Endpoint Security 试用版本时提供的电子邮件地址接收激活码。

要使用激活码激活本应用程序，需要因特网访问以连接到卡巴斯基的激活服务器。

如果您激活应用程序后丢失了激活码，请联系您购买授权许可的卡巴斯基合作伙伴。

关于密钥文件

*密钥文件*是从卡巴斯基收到的带有 .key 扩展名的文件。密钥文件旨在添加用于激活应用程序的授权许可密钥。

通过在购买 Kaspersky Endpoint Security 或订购 Kaspersky Endpoint Security 试用版本时提供的电子邮件地址接收密钥文件。

使用密钥文件无需连接至卡巴斯基激活服务器以激活应用程序。

如果意外删除了密钥文件，您可以将其还原。例如，您可能需要密钥文件来注册 Kaspersky CompanyAccount。

要还原密钥文件，请执行以下任一操作：

- 联系授权许可销售商。
- 获得激活码后，请在卡巴斯基网站上获取密钥文件。

关于订阅

Kaspersky Endpoint Security 订阅是具有特定设置（订阅过期日期、受保护的设备数量）的应用程序购买订单。您可以从服务提供商（例如您的互联网服务提供商）处订购 Kaspersky Endpoint Security 订阅。您可以续订或取消订阅。您可以在服务提供商的网站上管理您的订阅。

订阅可以是有限订阅（例如一年时间）或无限订阅（无过期时间）。要在有限订阅到期后继续使用应用程序，您需要续订订阅。如果已按时对供应商的服务进行预付费，无限期订阅会自动续订。

有限订阅到期后，可能会为您提供续订订阅的宽限期。在此期间，应用程序将保留其功能。服务提供商决定是否提供宽限期，如果提供的话，他们也会确定宽限期期限。

管理订阅的选项集可能因服务提供商而异。在应用程序保留其功能的情况下，服务提供商可能不会为续订订阅提供宽限期。

要在订阅下使用 Kaspersky Endpoint Security，您需要使用从服务提供商处接收到的激活码。应用激活码后，将向应用程序添加与使用订阅下应用程序的授权许可对应的活动密钥。只有使用激活码时才能添加保留密钥，不能为密钥文件或订阅添加保留密钥。

在订阅期内购买的激活码不能用于激活之前的 Kaspersky Endpoint Security 版本。

不同授权许可下的应用程序功能比较

Kaspersky Endpoint Security 中可用的应用程序功能集取决于授权许可（见下表）。

应用程序功能比较基于英特尔架构处理器的解决方案。有关基于 Arm 架构的解决方案的授权许可和可用功能的信息，请联系您所在地区的服务提供商。

应用程序功能的比较

功能	卡巴斯基网络安全解决方案标准版	Kaspersky Endpoint Security for Business Advanced	卡巴斯基网络安全解决方案完整版	卡巴斯基混合云安全（桌面版）	卡巴斯基虚拟化安全解决方案（桌面版）	卡巴斯基混合云安全（桌面版、企业版）	卡巴斯基虚拟化安全解决方案（核心版、服务器版）	卡巴斯基混合云安全（核心版、CPU 版、服务器版）	卡巴斯基混合云安全（CPU 版、服务器版）	Kaspersky Endpoint Detection and Response Optimum	Kaspersk Optimu Securit
文件威胁防护	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web 威胁防护	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
网络威胁防护	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
防火墙管理	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
行为检测	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
设备控制	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
可移动驱动器扫描	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
反加密勒索软件（用于共享文件夹）	✓	✓	✓	–	–	✓	✓	✓	✓	✓	✓
容器扫描	–	–	–	–	–	✓	–	–	✓	✓	✓
系统完整	–	–	–	–	–	✓	–	–	✓	–	–

性监控											
应用程序控制	–	✓	✓	✓	✓	✓	–	–	✓	–	–
Web 控制	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kaspersky Endpoint Detection and Response Optimum 集成	–	–	–	–	–	–	–	–	–	✓	✓

数据提供

本节介绍 Kaspersky Endpoint Security 可能存储在设备上并在运行期间自动发送到卡巴斯基的信息。

卡巴斯基根据法律和适用的卡巴斯基法规保护接收到的任何信息。数据通过加密的信道传输。

有关处理、存储和销毁在使用应用程序期间获得和传输到卡巴斯基的各类信息的更多详情，请阅读最终用户授权许可协议、KSN 声明和卡巴斯基网站上的隐私策略。包含最终用户授权许可协议和卡巴斯基安全网络声明的 license.<语言 ID> 和 ksn_license.<语言 ID> 文件包含在应用程序分发包中。

使用激活码时提供的数据

如果 Kaspersky Endpoint Security 用于标准模式且是使用激活码激活的，为了验证使用应用程序是否在被合法使用并获取有关应用程序分发和使用的统计信息，您同意向卡巴斯基自动提供以下信息：

- 所安装应用程序的类型、版本和本地化
- 已安装应用程序更新的版本
- 设备 ID 和设备上的应用程序安装 ID
- 用于激活应用程序的激活码
- 当前授权许可 ID
- 应用程序授权许可密钥创建日期和时间
- 用户设备上的日期和时间
- 应用程序授权许可期限的到期日期和时间
- 操作系统的类型、版本和比特大小

从卡巴斯基更新服务器下载更新时提供的数据

如果 Kaspersky Endpoint Security 在标准模式下使用且您使用卡巴斯基更新服务器下载更新，为了提高更新过程的效率并获取有关应用程序分发和使用的统计信息，您同意向卡巴斯基自动提供以下信息：

- 来源于授权许可的应用程序 ID
- 应用程序的完整版本
- 应用程序授权许可 ID
- 使用的应用程序授权许可类型
- 应用程序安装 ID (PCID)
- 应用程序更新启动的 ID

- 正在处理的网址

在 Light Agent 模式下使用应用程序时传输的数据

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 作为 Kaspersky Security for Virtualization Light Agent 的一部分来保护虚拟环境，则应用程序会保存以下信息（其中可能包含个人和机密数据），并在应用程序的操作过程中将其发送到其他解决方案组件。

- 为了激活，Kaspersky Endpoint Security 会向 Protection Server 发送以下数据：授权许可密钥状态确认的有效期、受保护虚拟机的 BIOS ID，以及 Light Agent 工作所需的授权许可的信息。
- 为了更新 Light Agent 数据库，Kaspersky Endpoint Security 会将以下数据发送到 Protection Server：从授权许可获取的软件标识符；完整版软件；软件授权许可标识符；软件安装标识符（PCID）；处理后的网址；授权许可类型；更新开始的标识符。
- 为了提供保护，Kaspersky Endpoint Security 会在扫描任务运行时向 Protection Server 发送扫描对象所需的信息。传输的信息可能包括文件系统中文件的名称和路径、文件的校验和、网址以及扫描的对象或其片段。
- 在由 VMware vCenter Server 和 VMware NSX Manager 管理的基础架构中，Kaspersky Endpoint Security 可能会在检测到病毒、恶意软件或典型网络攻击活动时向 Integration Server 发送有关分配给受保护虚拟机的安全标签的信息。受保护虚拟机的 ID 也会被发送。
- 为了获取选择 SVM 进行连接时使用的信息，Kaspersky Endpoint Security 会将受保护虚拟机的标识符发送到 Integration Server 和 Protection Server。
- 在多租户模式下使用 Kaspersky Security for Virtualization Light Agent 解决方案时，生成租户保护报告所需的信息可能会从 Kaspersky Endpoint Security Protection Server 发送到 SVM。可以发送以下数据：受保护虚拟机的标识符；受保护虚拟机上安装的来宾操作系统的类型和版本；Kaspersky Endpoint Security 连接到 SVM 的时间间隔。
- 为了获取统计数据，Kaspersky Endpoint Security 会将以下信息发送到 Protection Server：有关受保护虚拟机的操作系统版本的信息；Kaspersky Endpoint Security 本地化情况；活动的 Kaspersky Endpoint Security 组件的名称；受保护虚拟机的标识符 (BIOS ID)。

指定的信息通过加密的数据通道传输（扫描对象所需的信息以及选择 SVM 时使用的信息除外）。默认情况下，Kaspersky Endpoint Security 与 Protection Server 之间的连接不加密。您可以在 Kaspersky Endpoint Security 设置中启用 Light Agent 和 Protection Server 之间的数据通道加密。

发送到 Kaspersky Security Center 的数据

在运行期间，Kaspersky Endpoint Security 将以下信息保存并提交到 Kaspersky Security Center，其中可能包含个人和机密数据：

- 有关应用程序使用的数据库的信息：
  - 应用程序所需的数据库类别列表
  - 数据库发布并加载到应用程序中的日期和时间
  - 下载的应用程序数据库更新发布的日期
  - 上次应用程序数据库更新的时间

    - 当前使用的应用程序数据库中的记录数
- 应用程序授权许可信息：
    - 授权许可序列号和类型
    - 授权许可有效期（天）
    - 授权许可涵盖的设备数量
    - 授权许可期限的开始和结束日期
    - 授权许可密钥状态
    - 上次与激活服务器成功同步的日期和时间（如果使用激活码激活了应用程序）
    - 授权许可适用的应用程序的标识符
    - 授权许可下可用的功能
    - 提供授权许可的组织的名称
    - 在订阅下使用应用程序时的额外信息（订阅标志、订阅到期日期和可续订订阅的天数、订阅提供者的网址、当前订阅状态和此状态的原因）、应用程序在设备上激活的日期和时间
    - 设备上的应用程序授权许可的到期日期和时间
- 有关应用程序更新的信息：
    - 要安装或移除的更新列表
    - 更新发布日期和*关键*状态的迹象
    - 更新的名称、版本和简短说明
    - 更新的详细说明的链接
    - 应用程序更新的最终用户授权许可协议和隐私策略的标识符和文本
    - 应用程序更新的卡巴斯基安全网络声明的标识符和文本
    - 显示是否可以删除更新的指示器
    - 应用程序策略和管理插件的版本
    - 用于下载应用程序管理插件的网址
    - 已安装的应用程序更新的名称、版本和安装日期
    - 更新安装或移除完成后出错时的错误代码和描述
    - 因应用程序更新而必须重新启动设备或应用程序的迹象和原因
- 用户同意或不同意卡巴斯基安全网络声明、最终用户授权许可协议和隐私策略的条款和条件
- 分配给设备的标签列表

- 设备状态及状态分配原因的列表。
- 应用程序的整体状态及其所有组件的状态；有关策略合规性的信息、设备实时保护状态、应用程序稳定性状态、有关应用程序停止的信息。
- 上次设备扫描的日期和时间；扫描对象的数量；检测到的恶意对象的数量；被阻止、删除和清除的对象的数量；无法清除的对象的数量；扫描错误的数量；检测到的网络攻击的数量
- 有关应用程序设置当前应用的值的数据
- 组任务和本地任务的当前状态和执行结果及其设置值
- 有关连接到客户端设备的外部设备的信息（ID、名称、类型、制造商、描述、序列号、VID/PID）。
- 备份存储中的文件备份副本的信息（对象的名称、路径、大小和类型、对象的描述、检测到的威胁的名称、用于检测威胁的应用程序数据库的版本、对象移动到备份存储的日期和时间）、对备份存储中的对象执行的操作（移除、恢复）以及管理员请求的文件。
- 有关每个应用程序组件的操作和每个任务的执行的信息，以事件形式表示：
  - 事件的日期和时间
  - 事件的名称和类型
  - 事件严重性级别
  - 发生事件时正在运行的任务或应用程序组件的名称
  - 有关触发了事件的应用程序的信息：应用程序名称、磁盘上的文件路径、进程标识符、设置值（如果触发了应用程序启动或设置修改事件）
  - 用户 ID
  - 其操作触发了事件的发起者（任务计划程序、应用程序、Kaspersky Security Center 或用户）的名称
  - 发起访问文件的用户的名称和标识符
  - 对象或操作的处理结果（描述、类型、名称、威胁程度和准确性、文件名和设备上的操作类型、与操作有关的应用程序决策）
  - 有关对象的信息（对象的名称和类型、对象在磁盘上的路径、对象的版本、大小、关于执行的操作的信息、事件触发器描述、不处理和跳过对象的原因描述）
  - 设备信息（制造商名称、设备名称、路径、设备类型、总线类型、标识符、VID/PID、系统设备标志、设备访问规则计划的名称）
  - 有关阻止和取消阻止设备的信息；有关被阻止的连接的信息（名称、描述、设备名称、协议、远程地址和端口、本地地址和端口、数据包规则、操作）
  - 有关所请求的网址的信息
  - 有关所检测到的对象的信息
  - 检测类型、方法和 ID
  - 有关已执行操作的信息

- 有关应用程序数据库的信息（下载的数据库更新的发布日期、数据库使用信息、数据库使用错误、有关取消已安装的数据库更新的信息）
- 有关加密检测的信息（勒索软件名称；检测到加密的设备的名称；有关阻止和解除阻止设备的信息）
- 应用程序设置和网络设置
- 有关触发的应用程序控制规则（名称和类型）及其应用程序结果的信息
- 有关容器和容器镜像的信息（容器或容器镜像的名称、容器或容器镜像的路径、存储库 URL）
- 有关活动和被阻止的连接的信息（名称、描述和类型）
- 有关阻止和取消阻止访问不受信任的设备的信息
- 有关使用 KSN 的信息（KSN 连接状态、KSN 基础设施、扩展模式下 KSN 声明的标识符、扩展模式下 KSN 声明的接受、KSN 声明的标识符、KSN 声明的接受）
- 有关证书的信息（域名、主题名称、颁发者名称、到期日期、证书状态、证书类型、证书添加日期、颁发日期、序列号、SHA256 指纹）
- 有关作为公司软件解决方案一部分的外部系统的信息（Integration Server 地址）
- 有关为设备启用和禁用网络隔离的信息
- 有关在 Light Agent 模式下工作的信息：虚拟机模板的名称、Integration Server 的地址
- 启用或禁用网络隔离的设备的名称
- 扫描任务统计信息：扫描的对象数量；发现的威胁数量；感染对象数量；疑似感染对象数量；被清除的对象数量；添加到备份的对象数量；已删除的对象数量；未清除的对象数量；扫描错误数量；受密码保护的对象数量；跳过的对象数量；扫描的容器和图像数量
- 有关应用程序中使用的 EDR Optimum 组件的版本的信息
- 威胁发展链信息：威胁发展链在线列表名称、威胁发展链 ID

- 有关系统完整性扫描任务操作的信息（名称、类型、路径）以及有关系统基线的信息
- 有关网络活动、数据包规则和网络攻击的信息
- 用户角色信息：
  - 发起更改用户角色的用户的名称和标识符
  - 用户角色
  - 已分配或撤销角色的用户的名称
- 有关在客户端设备上检测到的应用程序的可执行文件的信息（文件的名称、路径、类型和哈希；应用程序所属的类别列表；应用程序所属的 KL 类别；应用程序所属的信任组；文件首次启动时间；应用程序的名称和版本；应用程序供应商的名称；有关用于签署应用程序的证书的信息：序列号、指纹、颁发者、主题、发布日期、到期日期和公钥）。
- 威胁发展链在线列表信息：威胁发展链 ID；威胁发展链的创建时间戳；威胁发展链的格式（文本或压缩文件）；威胁发展链的主体大小（以字节为单位）。

在应用程序界面中点击链接时提供的数据

单击 Kaspersky Endpoint Security 界面中的链接时，您同意自动提供以下信息给卡巴斯基：

- 应用程序的完整版本
- 应用程序区域设置
- 应用程序 ID (PID)
- 链接名称

使用卡巴斯基安全网络时提供的数据

在扩展模式下使用卡巴斯基安全网络，即表示您同意自动向卡巴斯基提交卡巴斯基安全网络声明中列出的所有数据。此外，入侵者可能用来破坏设备和设备操作系统中存储的数据的文件（或文件的一部分）可能会被发送到卡巴斯基进行扫描。

包含卡巴斯基安全网络声明文本的 ksn_license.<语言 ID> 文件包括在应用程序分发包中。

使用 Kaspersky Anti Targeted Attack Platform 时提供的数据

将 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA)（Kaspersky Anti Targeted Attack Platform 解决方案的一个组件）集成时，Kaspersky Endpoint Security 存储以下内部信息，其中可能包含个人和机密数据：

- KATA 服务器地址
- 用于与 Kaspersky Endpoint Detection and Response (KATA) 集成的服务器证书的公钥
- 用于与 Kaspersky Endpoint Detection and Response (KATA) 集成的带有客户端证书的加密容器
- 用于在代理服务器上进行身份验证的凭据
- 与 KATA 服务器同步的频率设置以及向 KATA 服务器发送数据的设置
- 与 KATA 服务器的连接状态以及有关客户端证书和服务器证书错误的信息
- 从 KATA 服务器接收的任务设置：
  - 任务启动计划设置
  - 必须被用于启动任务的账户名称和密码
  - 设置的版本
  - 服务启动类型
  - 服务名称

- 用于启动进程的命令行（包括参数）
- 对象的 MD5 和 SHA256 哈希
- 对象的路径
- IOC 文件

- 隔离设置，根据该设置，设备将被阻止连接到除排除项中指定的设备以外的其他设备

将 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 集成时，Kaspersky Endpoint Security 会存储以下信息并可能将其发送到 KATA 服务器：

- 对 EDR (KATA) 组件的同步请求的信息：
  - 唯一标识符
  - 服务器地址的基本部分
  - 设备名称
  - 设备的 IP 地址
  - 设备的 MAC 地址
  - 设备上的本地时间
  - 设备上安装的操作系统的名称和版本
  - Kaspersky Endpoint Security 的版本
  - 正在使用的应用程序数据库的发布日期
  - 授权许可状态
- 任务执行报告中对 EDR (KATA) 组件的请求信息：
  - 设备的 IP 地址
  - 唯一标识符
  - 服务器地址的基本部分
  - 设备的 MAC 地址
  - 任务执行错误和返回代码
  - 任务完成状态
  - 任务完成时间
  - 使用的任务设置版本
  - 有关应服务器请求在设备上启动或停止的进程的信息：PID 和 UniquePID、错误代码、对象的 MD5 和 SHA256 校验和

- 服务器请求的文件
- 获取对象信息时的错误信息：已处理但有错误的对象的全称；错误代码
- 网络隔离状态
- 对于 IOC，扫描结果返回（是否检测到每个指标、找到的对象以及检测到指标的哪个分支的信息）。
- 对于在其中检测到 IOC 的对象，根据指标类型返回不同的值：
  - ArpEntry：ARP 表中的 IP 地址（包括 ipv6），ARP 表中的物理地址。
  - 文件：文件的 MD5 哈希值、文件的 SHA256 哈希值、完整文件名（包括路径）、文件大小。
  - 端口：扫描时用于建立连接的远程 IP 地址和端口；本地适配器的 IP 地址和端口；协议类型（TCP、UDP、IP、RAWIP）。
  - 进程：进程名称；进程参数；进程文件的路径；进程的系统 PID；父进程的系统 PID；启动进程的用户名；进程开始的日期和时间。
  - SystemInfo：操作系统名称；操作系统版本；没有域的设备的网络名称；域或工作组。
  - 用户：用户名。

- 遥测数据包中的数据：
  - 有关文件的信息：
    - 文件的唯一 ID
    - 文件路径
    - 文件名
    - 文件大小
    - 文件属性
    - 文件的创建日期和时间
    - 文件的最后修改日期和时间
    - 对象的 MD5 和 SHA256 哈希值
    - 有关拥有该文件的用户和组的信息（名称和 ID）
  - 有关正在运行的进程的信息：
    - 进程文件的唯一 ID
    - 启动该进程的命令行选项
    - 进程 ID
    - 会话 ID

- 进程启动的日期和时间
- 启动进程的用户和组的信息（名称和 ID）

- 有关被检测到并处理的威胁的信息：
  - 根据卡巴斯基分类，检测到的威胁的名称以及检测到威胁的技术。
  - 应用程序数据库版本
  - 从其下载感染对象的网址。
  - 威胁处理状态。
  - 威胁无法消除的原因。
  - 威胁文件的唯一 ID
- 文件修改数据：
  - 被修改文件的唯一 ID
  - 做出更改的进程的唯一 ID
  - 有关修改的信息
- 有关系统变化的数据：
  - 做出更改的进程的唯一 ID
  - 有关发生的变化的信息
- 用户登录信息：
  - 会话 ID
  - 用户信息（名称和 ID）
  - 从其建立会话的设备的 IP 地址
- 有关正在被终止的进程的数据：进程的唯一 ID。

此处列出的信息也可以保存在跟踪文件和转储中。

使用 Kaspersky Endpoint Detection and Response Optimum 时提供的数据

与*IOC 扫描*任务结果一起传输的数据

Kaspersky Endpoint Security 会自动将有关*IOC 扫描*任务结果的数据发送到 Kaspersky Security Center。

*IOC扫描*任务结果数据可能包含以下信息：

- 网络信息：
  - 地址解析协议 (ARP) 表中的 IP 地址
  - 地址解析协议表中的 MAC 地址
  - DNS 记录的类型和名称
  - 受保护设备的 IP 地址
  - 受保护设备的 MAC 地址
  - 远程连接的 IP 地址和端口
  - 本地网络适配器的 IP 地址
  - 本地适配器上的开放端口号
  - 根据互联网号码分配机构 (IANA) 标准的协议编号
- 有关进程的信息：
  - 进程名称
  - 进程参数
  - 进程的可执行文件路径
  - 进程 ID (PID)
  - 父进程 ID
  - 启动进程的用户的名称
  - 进程启动的日期和时间
- 有关服务的信息：
  - 服务名称
  - 服务说明
  - 服务可执行文件的路径和名称
  - 服务 ID
  - 服务类型（内核驱动程序、适配器等）
  - 服务状态
  - 服务启动模式
  - 启动服务的用户的名称

- 有关文件系统的信息：
  - 卷名
  - 卷函
  - 卷类型
- 有关操作系统的信息：
  - 操作系统的名称和版本
  - 受保护设备的网络名称
  - 设备所属的域或组
- 有关 Web 活动的信息：
  - 浏览器名称
  - 浏览器版本
  - 上次访问 Web 资源的时间
  - HTTP 请求的网址
  - 发出 HTTP 请求的用户的姓名
  - 发出 HTTP 请求的进程的名称
  - 发出 HTTP 请求的进程的可执行文件的路径
  - 发出 HTTP 请求的进程的 ID
  - HTTP referer（HTTP 请求来源的网址）
  - 请求资源的网址
  - 已处理的 Web 请求的用户代理 (HTTP User-Agent)
  - HTTP 请求执行时间
  - 发出 HTTP 请求的进程的唯一 ID

用于创建威胁发展链的数据

用于创建威胁发展链的数据可能包含以下信息：

- 警报常规信息：
  - 警报日期和时间
  - 对象名称
  - 扫描模式

- 与警报相关的最后一个操作的状态
- 警报处理失败的原因

- 已处理对象的信息：
  - 进程标识符
  - 父进程 ID
  - 进程文件 ID
  - 进程的命令行
  - 启动进程的用户的名称
  - 进程在其中启动的会话的 ID
  - 进程在其中启动的会话的类型
  - 已处理对象的完整性级别
  - 用户是否属于特权组
  - 已处理对象的 ID
  - 已处理对象的全称
  - 受保护设备的的 ID
  - 对象的完整名称（本地文件或网址）
  - 已处理对象的 MD5 和 SHA256 校验和
  - 已处理对象的类型
  - 对象创建和最后修改的日期
  - 已处理对象的大小
  - 已处理对象的属性
  - 有关签署该对象的组织的信息
  - 对象数字证书验证结果
  - 对象的安全标识符 (SID)
  - 对象的时区 ID
  - 对象从其下载的网址（仅适用于文件）
  - 下载文件的应用程序的名称
  - 下载文件的应用程序的 MD5 和 SHA256 校验和

- 上次修改文件的应用程序名称
- 上次修改文件的应用程序的 MD5 和 SHA256 校验和
- 已处理对象的启动次数
- 已处理对象首次启动的日期和时间
- 文件的唯一 ID
- 文件全名（本地文件或网址）
- 已处理的 Web 请求的网址
- 已处理的 Web 请求的链接来源（HTTP referer）
- 已处理的 Web 请求的用户代理
- 已处理的 Web 请求的类型（GET 或 POST）
- 已处理的 Web 请求的本地 IP 端口
- 已处理的 Web 请求的远程 IP 端口
- 已处理的 Web 请求的连接方向（入站或出站）
- 被注入恶意代码的进程的 ID

应用程序管理理念

要管理 Kaspersky Endpoint Security，您可以使用：

- Kaspersky Security Center；
- 命令行；
- 图形用户界面。

> 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则无法使用 Kaspersky Security Center 云控制台和图形用户界面来管理应用程序。

使用 Kaspersky Endpoint Security 图形用户界面可以执行的操作是有限的。

本节介绍通过 Kaspersky Security Center 和命令行管理应用程序的具体细节，并介绍在 Kaspersky Security Center 管理控制台和命令行中执行操作的主要方法。

使用 Kaspersky Security Center 管理应用程序

Kaspersky Security Center 允许您远程和集中管理 Kaspersky Endpoint Security 在客户端设备上的操作。您可以远程安装和卸载、启动和停止 Kaspersky Endpoint Security；配置应用程序以及应用程序的各个组件和任务的设置；以及启动和停止受管理设备上的任务。

您可以使用以下 Kaspersky Security Center 管理控制台来通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security：

- Kaspersky Security Center 管理控制台（以下也称为“管理控制台”）。这是安装在管理员工作站上的 Microsoft 管理控制台 (MMC) 管理单元，为管理服务器和网络代理管理服务提供用户界面。

  通过 Kaspersky Security Center 管理控制台管理 Kaspersky Endpoint Security 的界面由基于 MMC 的管理控制台的 MMC 管理插件（以下也称为“MMC 插件”）提供。

  > 本帮助介绍如何管理 Kaspersky Security Center 14.2 Windows 的管理控制台。

- Kaspersky Security Center Web Console（以下也称为 Web Console）。这是用于管理基于卡巴斯基应用程序的保护系统的 Web 界面。您可以在任何有权访问管理服务器的设备上使用浏览器在 Kaspersky Security Center Web Console 中工作。

  通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security 的界面由 Web 管理插件（以下也简称为 Web 插件）提供。

  > 本帮助介绍如何管理 Kaspersky Security Center 15.1 Linux 的 Web Console。

- Kaspersky Security Center 云控制台。这是 Kaspersky Security Center 应用程序云版本内的基于云的管理控制台，也称为 Kaspersky Security Center 云控制台。云控制台的界面类似于 Kaspersky Security Center Web Console 界面。通过 Kaspersky Security Center 云控制台管理 Kaspersky Endpoint Security 的界面也由 Web 插件提供。

Kaspersky Security Center 云控制台不支持管理将 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 集成的设置。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则无法使用 Kaspersky Security Center 云控制台来管理应用程序。

MMC 插件和 Web 插件允许您在 Kaspersky Security Center 中创建策略和任务来管理 Kaspersky Endpoint Security 的操作：

- *策略*是指应用于管理组内所有设备的一组设置。策略允许您将相同的应用程序设置应用于管理组内的所有客户端设备。

  Kaspersky Endpoint Security 策略定义了 Kaspersky Endpoint Security 操作的常规设置以及在应用该策略的设备上操作应用程序各个功能组件的设置。

- 在 Kaspersky Security Center 中创建的 Kaspersky Endpoint Security *任务*在受保护设备上运行，并执行 Kaspersky Endpoint Security 功能，例如按需扫描、应用程序激活以及应用程序数据库和模块的更新。

  在 Kaspersky Security Center 中，您可以创建在单个设备上执行的任务（本地任务）、在管理组内所有设备上执行的任务（组任务）或者在随机选择的设备上执行的任务（设备集任务）。

无论您使用哪种 Kaspersky Security Center 管理控制台，您都必须将安装了 Kaspersky Endpoint Security 的设备分配给管理组，以便使用 Kaspersky Security Center 管理这些设备上的 Kaspersky Endpoint Security。您可以在安装 Kaspersky Endpoint Security 之前在 Kaspersky Security Center 中创建管理组，并配置规则以自动将设备移至管理组。您还可以在安装 Kaspersky Endpoint Security 后手动将设备移至管理组（有关详细信息，请参阅 Kaspersky Security Center 文档）。

Kaspersky Endpoint Security 管理插件

以下管理插件为使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security 所需的插件：

- Kaspersky Endpoint Security 管理 Web 插件（以下也称为 *Web 插件*）可促进使用 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台在 Kaspersky Endpoint Security 和 Kaspersky Security Center 之间进行交互。

  Web 插件必须安装在已安装 Kaspersky Security Center Web Console 的设备上。所有可以在浏览器中访问 Kaspersky Security Center Web Console 的管理员都可以使用 Web 插件来管理 Kaspersky Endpoint Security。

- Kaspersky Endpoint Security MMC 管理插件（以下也称为 *MMC 插件*）便于 Kaspersky Endpoint Security 与 Kaspersky Security Center 使用管理控制台进行交互。

  MMC 插件必须安装安装在 Kaspersky Security Center 管理控制台所安装的设备上。

借助 Kaspersky Endpoint Security 管理插件，您可以使用策略和任务来管理 Kaspersky Endpoint Security。

有关管理插件的更多详细信息，请参见 Kaspersky Security Center 文档。

Kaspersky Security Center 策略

*策略*是应用于包含在管理组中的所有客户端设备的一组 Kaspersky Endpoint Security 设置。

您可以为单个应用程序配置拥有不同设置值的多个策略。但是，管理组内的应用程序一次只能有一个活动策略。在创建新策略时，管理组中的所有其他策略都将变为非活动状态。您可以稍后更改策略状态。

策略具有层次结构，类似于管理组。默认情况下，子策略从父策略继承设置。*子策略*是嵌套层次结构级别的策略，即嵌套管理组和辅助管理服务器的策略。您可以启用从父策略继承设置。

您可以在本地修改策略为管理组中的各个计算机指定的设置值，只要策略不禁止修改这些设置。

使用策略配置文件可让您灵活配置应用程序的操作设置。*策略配置文件*可能包含与"基本"策略设置不同的设置，并在满足配置的条件（激活规则）时应用于客户端设备。使用策略配置文件可让您灵活配置用于不同设备的操作设置。您可以在策略属性的**策略配置文件**部分中对配置文件进行创建和配置。

每个策略设置都有一个"锁定"属性，用于指示是否可以修改子策略设置和本地应用程序设置。策略属性内设置的"锁定"状态决定是否可以编辑客户端设备上的应用程序设置：

- 当设置被"锁定"时 (🔒)，您无法在本地或嵌套层次结构级别的策略中编辑其值。该策略指定的设置值用于管理组内和嵌套组内的所有客户端设备。
- 当设置被"解锁"时 (🔓)，您可以在本地或在嵌套层次结构级别的策略中编辑其值。如果在本地指定设置值，或在管理组内的客户端设备的嵌套层次结构策略属性中指定设置值，则不会应用策略属性中指定的设置值。

在 Web 插件和 MMC 插件中，带有"锁"的参数数量不同。Web 插件包含 MMC 插件中不存在的"锁"。

首次应用策略后，应用程序的设置将根据策略设置进行改变。

有关策略和策略配置文件的更多详细信息，请参阅"Kaspersky Security Center 帮助"系统。

在 Kaspersky Security Center 中创建的 Kaspersky Endpoint Security 任务

您可以在 Kaspersky Security Center 中为 Kaspersky Endpoint Security 创建以下类型的任务：

- 在单个设备上运行的本地任务；
- 在管理组内的设备上运行的组任务；
- 在多台设备上运行的设备集任务，无论是否包含在管理组中。

> 设备集的任务仅在任务设置中指定的设备上执行。如果将新设备添加到为其创建任务的设备选择中，则此任务不会应用于新设备。要使该任务应用于这些计算机，您必须创建一个新的任务或者编辑现有任务的设置。

您可以创建任意数量的组任务、设备集任务或本地任务。

> 仅当 Kaspersky Endpoint Security 在设备上运行时，才会执行这些任务。

Kaspersky Security Center 文档中提供了有关 Kaspersky Security Center 中创建的任务的常规信息。

以下任务用于在 Kaspersky Security Center 中管理 Kaspersky Endpoint Security：

- 恶意软件扫描。在此任务执行期间，应用程序会扫描在任务设置中指定的设备区域以查找病毒和其他威胁。
- 关键区域扫描。在此任务执行期间，应用程序会扫描引导扇区、启动对象、进程内存和内核内存。

- 容器扫描。在此任务执行期间，应用程序会扫描容器和映像中是否有病毒和其他恶意软件。
- 清查。在此任务执行期间，应用程序会接收有关设备上存储的所有可执行文件的信息。
- 系统完整性检查。在此任务执行期间，应用程序通过将受监控对象的当前状态与之前作为基线建立的原始状态进行比较，以确定每个对象的更改。
- 添加密钥。在此任务执行期间，应用程序会添加一个密钥（包括一个保留密钥）来激活应用程序。
- 更新。在此任务执行期间，应用程序会根据配置的更新设置更新数据库。
- 回滚。在此任务执行期间，应用程序会回滚上一次数据库更新。

策略设置的集合和任务设置的默认值取决于授权许可类型。如果在 Light Agent 模式下使用应用程序保护虚拟环境，则“添加密钥”、“更新”和“回滚”任务不适用。此外，KESL 容器不支持某些应用程序功能。

登录和注销 Web Console 和云控制台

Kaspersky Security Center Web Console

要登录 Web Console，您需要知道在 Web Console 安装过程中指定的管理服务器的 Web 地址和端口号（默认使用端口 8080）。浏览器还必须启用 JavaScript。

要登录 Web Console：

1. 在浏览器中，转到 < 管理服务器网址 >:< 端口号 > 地址。
   将显示登录页面。
2. 输入您的账户的用户名和密码。

   建议确保密码复杂性和反暴力破解机制，使密码无法在 6 个月内被猜出。
3. 单击“**登录**”。
   如果管理服务器不响应，或者如果您输入错误的凭证，将显示错误消息。

登录后，将以上次使用的语言和主题显示仪表板。

有关 Web Console 界面的更多详细信息，请参阅 Kaspersky Security Center 文档。

要注销 Web Console：

请在屏幕左下角选择“**<账户名>**”→“**退出**”。

将关闭 Web Console，并显示登录页面。

Kaspersky Security Center 云控制台

对于 Kaspersky Security Center Cloud Console，请在 Cloud Console 门户上使用 Web 令牌登录您的账户。

有关 Kaspersky Security Center 云控制台的详细信息，请参阅 Kaspersky Security Center 云控制台文档。

在 Web Console 中管理策略

您可以使用 Web Console 中的策略执行以下操作：

- 创建策略。
- 编辑策略设置。

  如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。KESL 容器不支持某些设置的配置。

- 导出和导入策略设置。
- 复制和移动策略。
- 删除策略。
- 更改策略状态。
- 创建策略配置文件。

有关使用策略的常规信息，请参阅“Kaspersky Security Center 帮助”。

在 Web Console 中创建策略

要在 Web Console 中创建策略：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**策略和策略配置文件**”。
   将打开策略和策略配置文件的列表。
2. 选择包含必须应用该策略的设备的管理组。为此，请单击策略和策略配置文件列表上方的“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。
3. 单击“**添加**”。
   策略向导启动。
4. 在下拉列表中，选择 **Kaspersky Endpoint Security 12.1 for Linux**。
   继续执行向导的下一步。
5. 指定 Kaspersky Endpoint Security 使用模式：
   - **用于保护工作站和服务器的标准模式** – 应用程序用于保护运行 Linux 操作系统的设备。
   - **用于保护虚拟环境的 Light Agent 模式** – 作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分，该应用程序用于保护运行 Linux 访客操作系统的虚拟机。

6. 如果您在 Light Agent 模式下使用该应用程序保护虚拟环境，请配置 SVM 检测设置：

a. 选择 Light Agent 用来发现可连接的 SVM 的方法。

- 使用 Integration Server

  如果选择此选项，Light Agent 将连接到 Integration Server 来获取可连接的 SVM 列表及其详细信息。

- 使用 SVM 地址的自定义列表

  如果选择此选项，您可以指定由此策略管理的 Light Agent 可以连接的 SVM 列表。Light Agent 只会连接到该列表上指定的 SVM。

如果选择“**使用自定义的 SVM 地址列表**”选项，Light Agent 使用高级 SVM 选择算法，并且在 SVM 上启用大型基础架构保护模式（有关详细信息，请参阅“Kaspersky Security for Virtualization Light Agent 帮助”），那么只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到该 SVM。在“**SVM 选择算法**”部分中，需要将“**SVM 路径**”设置为“**忽略 SVM 路径**”。如果设置任何其他值，Light Agent 都无法连接到 SVM。

b. 如果选择 Integration Server，向导将显示用于将 Light Agent 连接到 Integration Server 的当前设置：用于连接的地址和端口。如有必要，指定新的连接设置：

a. 单击“**配置**”按钮，然后在打开的窗口中指定新的连接设置：

- Address

  安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。

  如果指定 NetBIOS 名称、“localhost”或 127.0.0.1 为地址，则连接 Integration Server 将失败并出现错误。

- Port

  用于连接到 Integration Server 的端口。

  默认情况下使用 7271 端口。

b. 单击“**检查**”按钮。

c. Web 插件将检查从 Integration Server 收到的 SSL 证书。如果证书包含错误或不受信任，“**与 Integration Server 的连接**”窗口中会显示相应的消息。

您可以单击“**查看收到的证书**”行来查看有关从 Integration Server 收到的证书的信息。如果您遇到 SSL 证书问题，我们建议您确保所使用的数据传输通道是安全的。

要保存收到的证书并继续连接到 Integration Server，请在“**选择操作**”块中选择“**忽略**”选项。

d. 指定 Integration Server 管理员的密码（`admin` 账户的密码），然后单击“**测试**”按钮。

"新建策略"向导将连接到 Integration Server。如果连接失败，窗口中会显示一条错误消息。如果连接成功，"**连接到 Integration Server**"窗口将关闭，并且"新建策略向导"窗口的"**连接到 Integration Server**"字段将显示"**已连接**"状态。

c. 如果您选择手动定义的 SVM 地址列表，该窗口将显示由此策略管理的 Light Agent 可以连接到的 SVM 列表。要向列表中添加 SVM，请单击"**添加**"按钮，然后在打开的窗口中指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。您可以在新行输入 SVM 的多个 IP 地址或 FQDN。

只能指定映射到单个 IP 地址的完全限定域名 (FQDN)。使用与多个 IP 地址对应的完全限定域名可能会导致应用程序出错。

您可以单击"**删除**"按钮来删除在列表中选定的地址。

继续执行向导的下一步。

7. 决定是否要使用卡巴斯基安全网络。仔细阅读卡巴斯基安全网络声明，然后执行以下操作之一：

- 如果您同意声明的所有条款和条件，并希望应用程序使用卡巴斯基安全网络，请选中"**我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件**"。
- 如果您不想使用卡巴斯基安全网络，请选择"**我不接受卡巴斯基安全网络声明的条款和条件**"，然后在打开的窗口中确认您的决定。

拒绝使用卡巴斯基安全网络不会中断策略创建过程。您可以随时在策略设置中启用或禁用卡巴斯基安全网络，或更改受管理设备的 KSN 模式。

继续执行向导的下一步。

8. 将打开新建策略设置窗口的"**常规**"选项卡。指定新策略的名称。

您还可以配置以下策略设置：

- 策略状态：
  - **活动**。当前应用于设备的策略。如果选择此选项，则下次设备与管理服务器同步时，此策略将在设备上变为活动状态。默认选中该选项。
  - **非活动**。当前未应用于设备的策略。如果选择此选项，策略将变为非活动状态，但仍保留在"**策略**"文件夹中。您可以稍后激活非活动策略。
- 策略设置继承：
  - **从父策略继承设置**。如果启用此选项，则策略设置值将继承上一级组策略，因而被锁定。此切换开关默认打开。
  - **强制设置子策略继承**。如果启用此选项，将锁定子策略的设置值。此切换开关默认关闭。

有关策略设置的常规信息，请参阅"Kaspersky Security Center 帮助"部分。

9. 如果您想配置其他策略设置，请转到"**应用程序设置**"选项卡并进行必要的更改。

您也可以稍后更改策略设置。

10. 单击"**保存**"。

创建的策略将显示在策略列表中。

有关管理策略的常规信息，请参阅“Kaspersky Security Center 帮助”。

在 Web Console 中更改策略设置

要在 Web Console 中编辑策略设置：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**策略和策略配置文件**”。
   将打开策略列表。
2. 选择包含应用了策略的设备的管理组。为此，请单击窗口上部的“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。
   该列表仅显示为所选管理组配置的策略。
3. 单击列表中所需策略的名称。
   将打开策略属性窗口。
4. 在“应用程序设置”选项卡上修改**策略设置**。
5. 单击“**保存**”按钮以保存更改。

该策略将与更新的设置一起保存。

Web Console 中的策略设置

策略设置的默认设置和值取决于用于激活应用程序的授权许可。是否对应用程序应用某些策略设置取决于应用程序模式。此外，KESL 容器不支持某些应用程序功能。

您可以在“策略属性”窗口的“**应用程序设置**”选项卡上配置策略设置。

策略设置

部分	子部分
基本威胁防护	文件威胁防护 文件威胁防护排除项 防火墙管理 Web 威胁防护 网络威胁防护
高级威胁防护	卡巴斯基安全网络 反加密 行为检测
检测与响应	Managed Detection and Response Endpoint Detection and Response Optimum Endpoint Detection and Response (KATA)
安全控制	应用程序控制 设备控制 系统完整性监控

	Web 控制
本地任务	任务管理 可移动驱动器扫描
常规设置	代理服务器设置 应用程序设置 容器扫描设置 网络设置 全局排除项 存储设置
Light Agent 模式	SVM 检测设置 Integration Server 连接设置 SVM 连接标签 SVM 选择算法 保护连接

在管理控制台中管理策略

您可以在 Kaspersky Security Center 管理控制台中执行以下操作：

- 创建策略。
- 编辑策略设置。

  如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。KESL 容器不支持某些设置的配置。

- 导出和导入策略设置。
- 删除策略。
- 更改策略状态。
- 创建策略配置文件。

有关使用策略的常规信息，请参阅“Kaspersky Security Center 帮助”。

使用管理控制台创建策略。

要在管理控制台中创建策略：

1. 在管理控制台树中的“**受管理设备**”文件夹中，选择包含应当应用该策略的设备的管理组。
   您可以在采用该管理组名称的文件夹的“**设备**”选项卡上查看属于该管理组的设备列表。
2. 在工作区中选择**策略**选项卡。

3. 单击“**新建策略**”按钮以启动“新建策略”向导。

   您还可以通过单击策略列表上下文菜单中的“**创建**”→”**策略**”项来启动向导。

4. 在向导的第一步中，从列表中选择 **Kaspersky Endpoint Security 12.1 for Linux**。

   继续执行向导的下一步。

5. 指定新策略的名称。

6. 要在正在创建的策略中使用 Kaspersky Endpoint Security 早期版本中的设置，请选中“**使用早期应用程序版本的策略设置**”复选框。

   继续执行向导的下一步。

7. 决定是否要使用卡巴斯基安全网络。仔细阅读卡巴斯基安全网络声明，然后执行以下操作之一：

   - 如果您同意声明的所有条款和条件，并希望应用程序使用卡巴斯基安全网络，请选中“**我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件**”。
   - 如果您不想使用卡巴斯基安全网络，请选择“**我不接受卡巴斯基安全网络声明的条款和条件**”，然后在打开的窗口中确认您的决定。

   拒绝使用卡巴斯基安全网络不会中断策略创建过程。您可以随时在策略设置中启用或禁用卡巴斯基安全网络，或更改受管理设备的 KSN 模式。

   继续执行向导的下一步。

8. 指定 Kaspersky Endpoint Security 使用模式：

   - **用于保护工作站和服务器的标准模式** — 应用程序用于保护运行 Linux 操作系统的设备。
   - **用于保护虚拟环境的 Light Agent 模式** – 作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分，该应用程序用于保护运行 Linux 访客操作系统的虚拟机。

   继续执行向导的下一步。

9. 如果您在 Light Agent 模式下使用该应用程序保护虚拟环境，请配置 SVM 检测设置：

   a. 选择 Light Agent 用来发现可连接的 SVM 的方法。

   - **使用 Integration Server**

     如果选择此选项，Light Agent 将连接到 Integration Server 来获取可连接的 SVM 列表及其详细信息。

   - **使用 SVM 地址的自定义列表**

     如果选择此选项，您可以指定由此策略管理的 Light Agent 可以连接的 SVM 列表。Light Agent 只会连接到该列表上指定的 SVM。

   如果选择“**使用自定义的 SVM 地址列表**”选项，Light Agent 使用高级 SVM 选择算法，并且在 SVM 上启用大型基础架构保护模式（有关详细信息，请参阅“Kaspersky Security for Virtualization Light Agent 帮助”），那么只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到该 SVM。在“**SVM 选择算法**”部分中，需要将“**SVM 路径**”设置为“**忽略 SVM 路径**”。如果设置任何其他值，Light Agent 都无法连接到 SVM。

b. 如果选择 Integration Server，向导将显示用于将 Light Agent 连接到 Integration Server 的当前设置：用于连接的地址和端口。如有必要，指定新的连接设置：

a. 单击“**编辑**”按钮并在打开的窗口中指定新的连接设置：

- **Address**

  安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。

  如果安装了 Kaspersky Security Center 管理控制台的设备属于某个域，则该字段默认指示该设备的域名。

  如果安装了 Kaspersky Security Center 管理控制台的设备不属于某个域，或者 Integration Server 安装在其他设备上，则必须手动填写该字段。

  > 如果指定 NetBIOS 名称、“localhost”或 127.0.0.1 为地址，则连接 Integration Server 将失败并出现错误。

- **Port**

  用于连接到 Integration Server 的端口。

  默认情况下使用 7271 端口。

b. 单击“**确定**”。

c. 如果托管 Kaspersky Security Center 管理控制台的设备不属于某个域，或者您的账户不属于 KLAdmins 本地组或域组或本地管理员组，则使用 Integration Server 管理员账户进行 Integration Server 上的身份验证。

在打开的窗口中，输入 Integration Server 管理员的密码（ `admin` 账户的密码），然后单击“**确定**”按钮。

d. MMC 插件将检查从 Integration Server 接收的 SSL 证书。如果证书包含错误或不受信任，将打开“**验证 Integration Server 证书**”窗口。您可以单击窗口中的链接查看收到的证书的详细信息。

> 如果您遇到 SSL 证书问题，我们建议您确保所使用的数据传输通道是安全的。

要继续连接到 Integration Server，请单击“**忽略**”按钮。收到的证书将作为受信任证书安装到安装了 Kaspersky Security Center 管理控制台的设备上。

c. 如果您选择手动定义的 SVM 地址列表，该窗口将显示由此策略管理的 Light Agent 可以连接到的 SVM 列表。要向列表中添加 SVM，请单击“**添加**”按钮，然后在打开的窗口中指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。您可以在新行输入 SVM 的多个 IP 地址或 FQDN。

> 只能指定映射到单个 IP 地址的完全限定域名 (FQDN)。使用与多个 IP 地址对应的完全限定域名可能会导致应用程序出错。

您可以单击“**删除**”按钮来删除在列表中选定的地址。

继续执行向导的下一步。

10. 如有必要，配置“文件威胁防护”的常规设置。

继续执行向导的下一步。

11. 如有必要，请编辑已默认配置的文件威胁防护设置。
    继续执行向导的下一步。
12. 如有必要，请配置“从文件威胁防护中排除”。
    继续执行向导的下一步。
13. 如有必要，请修改对受感染对象的默认操作。
    继续执行向导的下一步。
14. 完成“新建策略”向导。

创建的策略显示在“**策略**”选项卡上管理组的策略列表中以及控制台树的“**策略**”文件夹中。

您可以稍后更改策略设置。有关管理策略的常规信息，请参阅“Kaspersky Security Center 帮助”系统。

在 Kaspersky Security Center 管理控制台中更改策略设置

要在管理控制台中编辑策略设置：

1. 在 Kaspersky Security Center 管理控制台树的“**受管理设备**”文件夹中，打开包含所需设备、名称为管理组的文件夹。
2. 在工作区中选择“**策略**”选项卡。
3. 在策略列表中，选择所需的策略并双击它以打开“**属性：<策略名称>**”窗口。
   您还可以通过使用策略上下文菜单中的“**属性**”项或单击位于策略设置部分中策略列表右侧的“**配置策略设置**”链接来打开策略属性窗口。
4. 编辑策略设置。
5. 在**属性：<策略名称>**窗口中，单击“**确定**”以保存更改。

管理控制台中的策略设置

策略设置的默认设置和值取决于用于激活应用程序的授权许可。是否对应用程序应用某些策略设置取决于应用程序模式。此外，KESL 容器不支持某些应用程序功能。

您可以在策略属性窗口的部分和子部分中配置策略设置。有关配置常规策略设置和事件设置的信息，请参阅“Kaspersky Security Center 帮助”部分。

策略设置

部分	子部分
基本威胁防护	文件威胁防护 文件威胁防护排除项 防火墙管理

	Web 威胁防护 网络威胁防护
高级威胁防护	卡巴斯基安全网络 反加密 行为检测
检测与响应	Managed Detection and Response Endpoint Detection and Response (KATA)
安全控制	应用程序控制 设备控制 系统完整性监控 Web 控制
本地任务	任务管理 可移动驱动器扫描
常规设置	代理服务器设置 应用程序设置 容器扫描设置 网络设置 全局排除项 排除进程内存 存储设置
Light Agent 模式	与 Integration Server 的连接 SVM 检测设置 SVM 连接标签 SVM 选择算法 保护连接

在 Web Console 中管理任务

您可以在 Web Console 中对 Kaspersky Endpoint Security 的任务执行以下操作：

- 创建新任务。
- 编辑任务设置。

  如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。KESL 容器不支持某些设置的配置。

- 启动、停止、暂停和继续任务。

  “*更新*”任务无法暂停或继续，只能启动或停止。

- 导出和导入任务。
- 删除任务。

在任务列表中，您可以监控任务执行结果，其中包括任务状态和任务在设备上的表现的统计信息。您还可以创建一系列事件来监控任务执行情况（“**监控和报告**”→“**事件选择**”）。有关事件选择的详细信息，请参阅 Kaspersky Security Center 文档。

任务执行结果也保存在设备本地和 Kaspersky Security Center 报告中。

有关任务管理的常规信息，请参阅“Kaspersky Security Center 帮助”系统。

如果设备受策略管理，则可能无法使用命令行或设备上的本地用户界面查看和管理在 Kaspersky Security Center 中创建的任务。

在 Web Console 中创建任务

要在 Web Console 中创建任务：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**任务**”。
   将打开任务列表。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 在向导的第一步，执行以下操作：
   a. 在“**应用程序**”下拉列表中，选择 **Kaspersky Endpoint Security 12.1 for Linux**。
   b. 在“**任务类型**”下拉列表中，选择要创建的任务类型。
   c. 在“**任务名称**”字段中，输入新任务的名称。
   d. 在“**任务将被分配到的设备**”部分，选择定义任务范围的方法。任务范围包括将运行该任务的设备：
      - 如果要在特定管理组中包含的所有设备上运行该任务，请选择“**将任务分配给管理组**”选项。
      - 如果要在指定设备上运行任务，请选择“**手动指定设备地址，或从列表中导入地址**”选项。
      - 如果要根据预定义的标准在设备选择中包含的设备上运行任务，请选择“**将任务分配给设备选择**”选项。有关如何创建设备选择的信息，请参阅“Kaspersky Security Center 帮助”系统。

   继续执行向导的下一步。
4. 根据选择的定义任务范围的方法，执行以下操作之一：
   - 在管理组树中，选中所需管理组旁边的复选框。
   - 在设备列表中，选中所需设备旁边的复选框。如果所需的设备未列出，您可以通过以下方式添加：

- 使用“**添加设备**”按钮。您可以按名称或 IP 地址添加设备，从指定的 IP 范围添加设备，或者从管理服务器轮询企业 LAN 时检测到的设备列表中选择设备。
- 使用“**从文件导入设备**”按钮。对于导入，使用包含设备地址列表的 TXT 文件，其中每个地址必须位于单独的行上。

- 从列表中，选择包含所需设备的所选内容名称。

继续执行向导的下一步。

5. 要在创建后立即配置任务设置，请在向导的最后一步选中“**创建后打开任务属性窗口**”复选框。使用默认设置创建任务。

6. 完成向导。

在任务列表中将显示一个新任务。

在 Web Console 中更改任务设置

要在 Web Console 中编辑任务设置：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**任务**”。

   将打开任务列表。

2. 执行下列操作之一：

   - 要编辑在特定管理组中包含的所有设备上运行的任务的设置，请单击窗口上部“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

     该列表仅显示为所选管理组配置的任务。

   - 要编辑在一个或多个设备上运行的任务（一组设备的任务）的设置，请单击窗口上部“**当前路径**”字段中的链接，然后在打开的窗口中选择具有管理服务器名称的顶部节点。

     该列表显示在管理服务器上创建的所有任务。

3. 在任务列表中，选择所需任务并通过单击任务名称中的链接打开任务属性窗口。

4. 配置任务设置：

   - 在“**常规**”选项卡上，您可以编辑任务的名称。
   - 在“**应用程序设置**”选项卡上，您可以配置具体的任务设置。可配置设置的可用性取决于任务的类型。
   - 在“**计划**”选项卡上，您可以配置任务运行计划以及启动和停止任务的其他设置。

   任务属性窗口的“**常规**”、“**结果**”、“**设置**”、“**计划**”和“**修订历史记录**”选项卡是 Kaspersky Security Center 的标准组件；有关更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

5. 单击“**保存**”按钮以保存更改。

在 Web Console 中启动、停止、暂停和恢复任务

要在 Web Console 中启动、停止、暂停或恢复任务：

1. 在 Kaspersky Security Center Web Console 的主窗口中，选择“**资产（设备）**”→“**任务**”。

   将打开任务列表。

2. 执行下列操作之一：

   - 要启动或停止在特定管理组中包含的所有设备上运行的任务，请单击窗口上部“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

     该列表仅显示为所选管理组创建的任务。

   - 要启动或停止在一个或多个设备上运行的任务（针对一组设备的任务），请单击窗口上部“**当前路径**”字段中的链接，然后在打开的窗口中选择带有管理服务器名称的顶部节点。

     该列表显示在管理服务器上创建的所有任务。

3. 在任务列表中，选中所需任务名称旁边的框，然后单击任务列表上方的操作按钮。

在管理控制台中管理任务

您可以在管理控制台中对 Kaspersky Endpoint Security 的任务执行以下操作：

- 创建新任务。
- 编辑任务设置。

  > 如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。KESL 容器不支持某些设置的配置。

- 启动、停止、暂停和继续任务。

  > “*更新*”任务无法暂停或继续，只能启动或停止。

- 导出和导入任务。
- 删除任务。

在任务列表中，您可以监控任务执行结果，其中包括任务状态和任务在设备上的表现的统计信息。

有关任务执行进度和结果的信息，可在 Kaspersky Endpoint Security 发送到 Kaspersky Security Center 管理服务器的事件列表中查看（在“**管理服务器 <服务器名称>**”节点工作区的“**事件**”选项卡上）。您还可以创建一系列事件来监控任务的执行情况。有关事件选择的详细信息，请参阅 Kaspersky Security Center 文档。

任务执行结果也保存在设备本地和 Kaspersky Security Center 报告中。

有关任务管理的常规信息，请参阅“Kaspersky Security Center 帮助”系统。

> 如果设备受策略管理，则可能无法使用命令行或设备上的本地用户界面查看和管理在 Kaspersky Security Center 中创建的任务。

在管理控制台中创建任务

要在管理控制台中创建任务：

1. 在管理控制台中，执行以下操作之一：

   - 要创建将在所选管理组中包含的设备上运行的任务，请在“**受管理设备**”文件夹中的控制台树中选择此管理组，然后选择工作区中的“**任务**”选项卡并单击“**新建任务**”按钮。

     将为所选管理组的设备启动“新建任务”向导。

   - 要创建将在一个或多个设备上执行的任务（一组设备的任务），请选择控制台树中的“**任务**”文件夹，然后单击工作区中的“**新建任务**”按钮。

     将针对该组设备启动“新建任务”向导。

2. 在向导的第一步中，选择 **Kaspersky Endpoint Security 12.1 for Linux** 和任务类型。

   继续执行向导的下一步。

3. 如果您正在为一组设备创建任务，向导将提示您定义任务范围。任务范围包括将运行该任务的设备。

   a. 指定定义任务范围的方法：从管理服务器检测到的设备列表中选择设备；手动设置设备地址；从文件导入设备列表或指定之前配置的设备选择（有关更多详细信息，请参阅“Kaspersky Security Center 帮助”系统）。

   b. 根据您指定的定义任务范围的方法，在打开的窗口中执行以下操作之一：

      - 在检测到的设备列表中，指定将运行任务的设备。为此，请选中设备名称左侧列表中的复选框。
      - 单击“**添加**”或“**添加 IP 范围**”按钮，并手动输入设备地址。
      - 单击“**导入**”按钮，然后在打开的窗口中选择包含设备地址列表的 TXT 文件。
      - 单击“**浏览**”按钮，在打开的窗口中指定包含将运行任务的设备的所选内容名称。

   继续执行向导的下一步。

4. 按照向导中的说明配置可用的任务设置。

5. 输入新任务的名称并继续执行向导的下一步。

6. 要在向导完成后立即启动任务，请在最后一步中选中“**向导完成后运行任务**”复选框。

7. 完成向导。

   在任务列表中将显示一个新任务。

在管理控制台中更改任务设置

要在管理控制台中编辑任务设置：

1. 在管理控制台中，执行以下操作之一：

- 要编辑在指定管理组中包含的设备上运行的任务的设置，请在控制台树中选择此管理组，然后在工作区中选择“**任务**”选项卡。
- 要编辑在一台或多台设备上运行的任务（一组设备的任务）的设置，请选择控制台树中的“**任务**”文件夹。

2. 在任务列表中，选择所需的任务并双击它以打开“**属性：<任务名称>**”窗口。

   您还可以使用任务上下文菜单中的“**属性**”项打开任务属性窗口。

3. 编辑任务设置。可配置设置的可用性取决于任务的类型。

   任务属性窗口的“**常规**”、“**通知**”、“**计划**”和“**修订历史记录**”选项卡是 Kaspersky Security Center 的标准配置；有关更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

4. 在“**属性：<任务名称>**”窗口中单击“**应用**”或“**确定**”以保存所做的更改。

在管理控制台中启动、停止、暂停和恢复任务

要在管理控制台中启动、停止、暂停或恢复任务：

1. 在管理控制台中，执行以下操作之一：
   - 要启动或停止在指定管理组中包含的设备上运行的任务，请在控制台树中选择此管理组，然后在工作区中选择“**任务**”选项卡。

     将打开为所选管理组创建的任务列表。
   - 要启动或停止在一台或多台设备上运行的任务（一组设备的任务），请选择控制台树中的“**任务**”文件夹。

     将打开管理服务器上创建的所有任务的列表。
2. 在任务列表中，选择所需的任务，打开该任务的上下文菜单，然后选择要执行的操作。

使用命令行管理应用程序

使用命令行，您可以在设备上安装、卸载、启动和停止 Kaspersky Endpoint Security，还可以在本地管理应用程序。

该应用程序的功能组件由在操作系统中运行的 *Kaspersky Endpoint Security 本地任务*支持。您可以通过在命令行中启动或停止 Kaspersky Endpoint Security 任务来在设备上启用或禁用应用程序的功能组件。启动 Kaspersky Endpoint Security 任务时还将执行一次性设备扫描。您可以通过配置 Kaspersky Endpoint Security *任务设置*来定义设备上的功能组件设置和设备扫描设置。

除了任务设置之外，还提供了以下设置以用于配置应用程序：

- 常规容器扫描设置。
- 加密连接扫描设置。
- 常规应用程序设置，定义应用程序整体的运行以及各个功能的操作。

在命令行中，使用 *Kaspersky Endpoint Security 管理命令*来管理 Kaspersky Endpoint Security。

启用自动添加 kesl-control 命令（bash 完成）

对于 bash shell，可以禁用自动添加 kesl-control 命令。

要在当前 bash shell 会话中启用自动添加 kesl-control 命令，请运行以下命令：

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

要为所有新的 bash shell 会话启用自动添加，请运行以下命令：

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~.bashrc
```

在命令行中管理任务

以下是使用命令行管理 Kaspersky Endpoint Security 的应用程序任务：

- *文件威胁防护*。此任务允许您启用或禁用实时文件威胁防护并定义文件威胁防护组件的设置。应用程序启动时会自动启动此任务。
- *恶意软件扫描*。此任务允许您根据需要扫描文件系统对象中的恶意软件并定义扫描的设置。您可以使用此任务对设备执行全盘扫描或自定义扫描。
- *关键区域扫描*。此任务允许您根据需要运行操作系统的关键区域扫描并定义扫描的设置。
- *自定义文件扫描*。此任务用于配置和存储使用 `kesl-control --scan-file` 命令扫描指定文件和目录时使用的设置。命令执行的结果是，应用程序创建并启动临时文件扫描任务。
- *容器扫描*。此任务允许您根据需要扫描容器和镜像并定义扫描的设置。
- *自定义容器扫描*。此任务用于配置和存储使用 `kesl-control [-T] --scan-container` 命令扫描指定容器和镜像时使用的设置。命令执行的结果是，应用程序创建并启动一个临时的“容器扫描”任务。
- *可移动驱动器扫描*。此任务允许您实时监控可移动驱动器与设备的连接，并定义可移动驱动器扫描的设置以及其引导扇区的扫描，以检查是否存在恶意软件。
- *Web 威胁防护*。此任务允许您启用或禁用 Web 威胁防护并定义 Web 威胁防护组件的设置。
- *网络威胁防护*。此任务允许您启用或禁用网络威胁防护并定义网络威胁防护组件的设置。
- *反加密勒索*。此任务允许您启用或禁用对文件进行远程恶意加密的保护，并定义反加密勒索组件的设置。
- *防火墙管理*。此任务允许您启用或禁用防火墙管理并定义设备上的网络连接控制设置。
- *应用程序控制*。此任务允许您启用或禁用应用程序控制并定义应用程序控制组件的设置。
- *清查*。此任务允许您获取有关设备上存储的所有应用程序可执行文件的信息。
- *设备控制*。此任务允许您启用或禁用设备控制并定义设备控制组件的设置。当 Kaspersky Endpoint Security 启动时，此任务会自动启动。
- *Web 控制*。此任务允许您启用或禁用Web 控制并定义Web 控制组件的设置。

- *行为检测*。此任务允许您监控应用程序在操作系统中的恶意活动。当 Kaspersky Endpoint Security 启动时，此任务会自动启动。
- *系统完整性监控*。该任务允许您对系统完整性监控组件设置中指定监控范围内的对象执行的操作进行实时监控。
- *系统完整性检查*。此任务允许您通过将监控对象的当前状态与之前记录的状态进行比较来检查已包含在监控范围内的文件和目录的变化。
- *备份管理*。使用该任务可以将文件的备份副本保存至设备上的备份。该任务在应用程序启动时自动启动，并驻留在设备操作内存中。该任务无法启动、停止或删除。
- *授权许可*。使用此任务可以激活安装在设备上的应用程序。该任务在应用程序启动时自动启动，并驻留在设备操作内存中。该任务没有设置；授权许可密钥使用特殊管理命令进行管理。该任务无法启动、停止或删除。
- *更新*。您可以使用此任务执行计划和按需的应用程序数据库和模块更新并编辑更新设置。
- *回滚*。您可以使用该任务回滚应用程序数据库和模块的上一次更新。
- *Kaspersky Endpoint Detection and Response (KATA) 集成*。该任务允许您启用或禁用与 Kaspersky Endpoint Detection and Response (KATA) 的集成并定义集成设置。

每个应用程序任务都有一个在命令行上使用的名称、一个 ID 和一个类型（见下表）。

所有任务（包括已删除的任务）的 ID 都是唯一的。应用程序不会重复使用已删除任务的标识符。新任务的标识符是最近创建的任务的标识符的下一个连续数字。

任务名称不区分大小写。

安装应用程序时会创建*预定义任务*。这些任务无法删除。每个预定义任务都有一个名称和 ID。

使用应用程序时创建的任务称为*用户任务*。创建任务时，请指定其名称。用户任务的 ID 由应用程序在创建任务时定义和分配。用户任务的 ID 从 100 开始。

应用程序在操作时会创建*临时扫描任务*。临时任务名称和 ID 由应用程序分配。临时任务完成后会自动删除。

应用程序任务

任务	命令行中的任务名称	任务 ID	任务类型
文件威胁防护	File_Threat_Protection	1	OAS
恶意软件扫描	Scan_My_Computer	2	ODS
恶意软件扫描（用户任务）	用户自定义	从 100 开始	ODS
自定义文件扫描	Scan_File	3	ODS
关键区域扫描	Critical_Areas_Scan	4	ODS
更新	更新	6	更新
更新（用户任务）	用户自定义	从 100 开始	更新
回滚	回滚	7	回滚
回滚（用户任务）	用户自定义	从 100 开始	回滚

授权	授权许可	9	授权许可
备份管理	备份	10	备份
系统完整性监控	System_Integrity_Monitoring	11	OAFIM
系统完整性监控（用户任务）	用户自定义	从 100 开始	光子晶体振荡器
防火墙管理	Firewall_Management	12	防火墙
反加密	Anti_Cryptor	13	AntiCryptor
Web 威胁防护	Web_Threat_Protection	14	WTP
设备控制	Device_Control	15	DeviceControl
可移动驱动器扫描	Removable_Drives_Scan	16	RDS
网络威胁防护	Network_Threat_Protection	17	NTP
容器扫描	Container_Scan	18	ContainerScan
容器扫描（用户任务）	用户自定义	从 100 开始	ContainerScan
自定义容器扫描	Custom_Container_Scan	19	ContainerScan
行为检测	Behavior_Detection	20	BehaviorDetection
应用程序控制	Application_Control	21	AppControl
清查	Inventory_Scan	22	InventoryScan
清查（用户任务）	用户自定义	从 100 开始	InventoryScan
Kaspersky Endpoint Detection and Response (KATA) 集成	KATAEDR	24	KATAEDR
Web 控制	Web_Control	26	WebControl

您可以对任务执行以下操作：

- 启动和停止除“*备份*”和“*授权许可*”任务之外的所有预定义任务和用户任务。
- 暂停和恢复 *ODS*、*ODFIM* 和 *InventoryScan* 任务。
- 创建和删除用户任务。根据应用程序使用模式，可以创建以下类型的任务：
  - 标准模式：*ODS*、*更新*、*回滚*、*ODFIM*，*ContainerScan* 和 *InventoryScan*；
  - 用于保护虚拟环境的 Light Agent 模式：*ODS*、*ODFIM*，*ContainerScan* 和 *InventoryScan*。
- 更改所有用户任务和所有预定义任务（“*回滚*”和“*授权许可*”任务除外）的设置。

  如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则不能编辑预定义任务“*更新*”的设置。

- 配置任务启动计划。

在命令行中查看任务列表

要查看应用程序任务列表，请执行以下命令：

```
kesl-control --get-task-list [--json]
```

其中：

`--json` – 应用程序任务列表的输出格式。如果不指定文件格式，输出将是 INI 文件。

将显示 Kaspersky Endpoint Security 任务列表。

将为每个任务显示以下信息：

- `Name`：任务名称
- `ID`：任务 ID
- `Type`：任务类型
- `State`：任务的当前状态

如果 Kaspersky Security Center 策略禁止用户在本地查看和编辑任务，则只会显示有关 *Scan_File*、*Backup*、*License*、*File_Threat_Protection*、*System_Integrity_Monitoring* 和 *Anti_Cryptor* 任务的信息。不提供有关其他任务的信息。

在命令行中查看任务的状态

要查看任务状态，请执行以下命令：

```
kesl-control --get-task-state <任务 ID/名称> [--json]
```

其中：

- `<任务 ID/名称>`是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- 指定 `--json`，则以 JSON 格式输出设置。

应用程序任务可以采取以下主要状态：

- `Started` - 任务正在运行。
- `Starting` - 任务正在启动。
- `Stopped` - 任务已停止。

- `Stopping` - 任务正在停止。

ODS、*ODFIM* 和 *InventoryScan* 任务还可以是以下状态之一：

- `Pausing` — 任务正在暂停。
- `Suspended` — 任务已暂停。
- `Resuming` — 任务正在恢复。

在命令行中创建任务

如果在标准模式下使用应用程序，则可以创建以下类型的任务：*ODS*、*更新*、*回滚*、*ODFIM*、*ContainerScan* 和 *InventoryScan*。

如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则可以创建以下类型的任务：*ODS*、*ODFIM*、*ContainerScan* 和 *InventoryScan*。

您可以使用默认设置或配置文件中指定的设置来创建任务。

要使用默认设置创建任务，请执行以下命令：

```
kesl-control -create-task <任务名称> --type <任务类型>
```

其中：

- <任务名称> 是您为新任务指定的名称。
- <任务类型> 是所创建任务的类型的标识符。

要使用配置文件中指定的设置创建任务，请运行以下命令：

```
kesl-control --create-task <任务名称> --type <任务类型> --file <配置文件路径> [--json]
```

其中：

- <任务名称> 是您为新任务指定的名称。
- <任务类型> 是所创建任务的类型的标识符。
- <文件路径> 是包含用于创建任务的设置的配置文件的完整路径。
- 指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json` 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

在命令行中启动、停止、暂停和恢复任务

您可以启动和停止预定义任务和用户任务，但“*备份*”和“*授权许可*”类型的任务除外。

您可以暂停和恢复 *ODS*、*ODFIM* 和 *InventoryScan* 类型的任务。

要启动任务，请执行以下命令：

```
kesl-control --start-task <任务 ID/名称> [-W] [--progress]
```

其中：

- `<任务 ID/名称>` 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- `[-W]` 是与任务启动命令配合使用的命令，用于启用与该任务相关的当前事件的显示。
- `[--progress]` 是想要显示任务进度时必须指定的键。

  示例：
  启动 ID 为 1 的任务，并启用与该任务相关的当前事件的显示：

  ```
  kesl-control --start-task 1 -W
  ```

要停止任务，请执行以下命令：

```
kesl-control --stop-task <任务 ID/名称> [-W]
```

其中：

- `<任务 ID/名称>` 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- `[-W]` 是与 stop task 命令配合使用的命令，用于启用与此任务相关的当前事件的显示。

要暂停任务，请执行以下命令：

```
kesl-control --suspend-task <任务 ID/名称>
```

要恢复任务，请执行以下命令：

```
kesl-control --resume-task <任务 ID/名称>
```

在命令行中删除任务

您只能删除用户任务。无法删除预定义任务。

要删除任务，请执行以下命令：

```
kesl-control --delete-task <任务 ID/名称>
```

其中 `<任务 ID/名称>` 是任务创建时指定的 ID，或者是命令行中的任务名称。

在命令行中显示任务设置

您可以显示所有用户任务和所有预定义任务设置的当前值，但“*回滚*”和“*授权许可*”任务除外（这些任务没有设置）。

您可以将任务设置的当前值输出到控制台或可用于更改任务设置的配置文件。

要将任务设置的当前值输出到控制台，请执行以下命令：

```
kesl-control --get-settings <任务 ID/名称> [--json]
```

其中：

- `<任务 ID/名称>`是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- 指定 `--json`，则以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

要将任务设置的当前值输出到配置文件，请执行以下命令：

```
kesl-control --get-settings <任务 ID/名称> --file <配置文件路径> [--json]
```

其中：

- `<任务 ID/名称>` 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- `--file <配置文件路径>` – 将写入任务设置的配置文件的完整路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定目录不存在，则不会创建配置文件。
- 指定 `--json`，则以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

在命令行中编辑任务设置

您可以编辑所有用户任务和所有预定义任务（“*回滚*”和“*授权许可*”任务除外）的设置。

> 如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则不能编辑预定义任务“*更新*”的设置。

在命令行中，您可以使用 `kesl-control --set-settings` 命令编辑任务的设置：

- 您可以使用包含任务设置的配置文件来编辑所有任务设置。您可以使用显示任务设置的命令获取配置文件。
- 您可以使用命令行键，以`<设置名称>=<设置值>`格式来编辑单个任务设置。您可以使用用于显示任务设置的命令来获取任务设置的当前值。
- 您可以将任务设置恢复为其默认值。

您可以使用包含任务设置或命令行键的配置文件，添加或删除扫描范围和排除范围。配置扫描范围和排除范围适用于 *OAS*、*ODS*、*OAFIM*、*ODFIM* 和 *AntiCryptor* 类型的任务。

为了优化扫描任务的操作，对于具有 btrfs 文件系统并启用了活动快照的系统，建议将系统以只读模式挂载的快照的路径添加到排除项中。例如，对于基于 SUSE/OpenSUSE 的系统，可以为路径添加以下排除项：`/.snapshots/*/snapshot/`。

对于某些任务，还提供了单独的管理命令，可让您编辑任务设置。

使用配置文件编辑任务设置

如要使用配置文件编辑任务设置的值：

1. 使用命令 `kesl-control --get-settings` 将任务设置输出到配置文件中。
2. 打开配置文件并编辑必要设置的值。

   对于 *OAS*、*ODS*、*OAFIM*、*ODFIM* 和 *AntiCryptor* 类型的任务，您可以添加或删除扫描范围和排除范围。

   如果要添加扫描范围，请在文件中添加具有以下设置的 `[ScanScope.item_ #]` 部分：

   - `AreaDesc` 是对扫描范围的说明，其中包含有关该范围的其他信息。
   - `UseScanArea` 启用对指定范围的扫描。
   - `Path` 是包含扫描对象的目录的路径。您可以指定本地目录的路径，或启用对客户端设备上安装的远程目录进行扫描。
   - `AreaMask.item_#` 是扫描范围的限制。您可以为要扫描文件的名称指定一个掩码。默认情况下，对扫描范围内的所有对象启用扫描。您可以指定多个 `AreaMask.item_#` 项。

   如果要添加排除范围，请在文件中添加具有以下设置的 `[ExcludedFromScanScope.item_#]` 部分：

   - `AreaDesc` – 排除范围的说明，其中包含有关扫描排除范围的其他信息。
   - `UseScanArea` 启用排除指定范围。
   - `Path` 是包含排除对象的目录的路径。您可以指定本地目录的路径，或排除客户端设备上安装的远程目录。可能的设置值取决于任务类型。
   - `AreaMask.item_#` 是排除范围的限制。您可以为要从扫描范围中排除的文件的名称指定一个掩码。默认情况下，排除范围内的所有对象。

     示例：

     ```
     [ExcludedFromScanScope.item_0000]
     AreaDesc=
     UseScanArea=Yes
     Path=/tmp/notchecked
     AreaMask.item_0000=*
     ```

   您可以指定多个 `[ScanScope.item_#]` 和 `[ExcludedFromScanScope.item_#]` 部分。应用程序将按索引升序处理范围。
3. 保存配置文件。
4. 执行命令：

```
kesl-control --set-settings <任务 ID/名称> --file <配置文件的路径> [--json]
```

其中：

- <任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- --file <配置文件路径> – 将从中导入任务设置的配置文件的完整路径。
- --json：如果您要以 JSON 格式从配置文件导入设置，请指定此键。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

文件中定义的所有任务设置值都将导入应用程序。

如果您在“应用程序控制”任务设置中更改了允许列表，或者禁止启动所有应用程序或影响 Kaspersky Endpoint Security 运行的应用程序，请运行带有 --accept 键的 --set-settings 命令。

使用命令行键编辑任务设置

使用 kesl-control --set-settings 命令键，您可以编辑任务设置的单个值，还可以添加或删除 OAS、*ODS*、*OAFIM*、*ODFIM* 和 *AntiCryptor* 类型的*任务*的扫描范围和排除范围。

配置单个任务设置

如要使用命令行键编辑任务设置的单个值，请执行以下命令：

```
kesl-control --set-settings <任务 ID/名称> <设置名称>=<设置值> [<设置名称>=<设置值>]
```

其中：

- <任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- <设置名称>=<设置值> 是其中一项任务设置的名称和值。您可以使用用于显示任务设置的命令来获取任务设置的当前值。

指定任务设置的值将发生更改。

如果您在“应用程序控制”任务设置中更改了允许列表，或者禁止启动所有应用程序或影响 Kaspersky Endpoint Security 运行的应用程序，请运行带有 --accept 键的 --set-settings 命令。

添加和删除扫描范围

如要使用命令行键添加扫描范围，请执行以下命令：

```
kesl-control --set-settings <任务 ID/名称> --add-path <路径>
```

其中：

- < 任务 ID/名称 > 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- --add-path < 路径 > 添加要扫描对象的目录路径。

  任务设置中将添加一个新的 [ScanScope.item_#] 部分。应用程序将扫描 Path 设置指定的目录中的对象。扫描范围的其余设置采用默认值。

  如果任务设置中已经包含 Path 设置具有指定值的 [ScanScope.item_ #] 部分，则不会添加重复的部分。

  如果 UseScanArea 设置设为 No，在执行此命令后其值将变为 Yes，位于此目录中的对象将被扫描。

示例：
为 ID=100 的任务添加扫描范围：

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/home
```

以下扫描范围设置将添加到任务中：

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

如要使用命令行键删除扫描范围，请执行以下命令：

```
kesl-control --set-settings < 任务 ID/名称 > --del-path < 路径 >
```

其中：

- < 任务 ID/名称 > 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- --del-path < 路径 > 删除要扫描对象的目录路径。

  包含指定路径的 [ScanScope.item_#] 部分将从任务设置中删除。应用程序将不会扫描指定目录中的对象。

添加和删除排除范围

如要使用命令行键添加排除范围，请执行以下命令：

```
kesl-control --set-settings < 任务 ID/名称 > --add-exclusion < 路径 >
```

其中：

- < 任务 ID/名称 > 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

- `--add-exclusion <路径>` 添加要从扫描中排除的对象所在的目录路径。

  任务设置中将添加一个新的 `[ExcludedFromScanScope.item_#]` 部分。应用程序将从扫描中排除 `Path` 设置指定的目录中的对象。排除范围的其余设置采用默认值。

  如果任务设置中已经包含 `Path` 设置具有指定值的 `[ExcludedFromScanScope.item_#]` 部分，则不会添加重复的部分。

  如果 `UseScanArea` 设置设为 `No`，在执行此命令后，其值将变为 `Yes`，位于此目录下的对象将被排除在扫描之外。

如要使用命令行键删除排除范围，请执行以下命令：

```
kesl-control --set-settings <任务 ID/名称> --del-exclusion <路径>
```

其中：

- `<任务 ID/名称>` 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- `--del-exclusion <路径>` 删除要排除的对象的目录路径。

  包含指定路径的 `[ExcludedFromScanScope.item_#]` 部分将从任务设置中删除。应用程序不会从扫描中排除指定目录中的对象。

在命令行中恢复默认任务设置

您可以恢复所有用户任务和所有预定义任务的默认设置，但“*回滚*”和“*授权许可*”类型的任务除外（这些任务没有设置）。

要将任务设置重置为默认值，请执行以下命令：

```
kesl-control --set-settings <任务 ID/名称> --set-to-default
```

其中 `<任务 ID/名称>` 是任务创建时指定的 ID，或者是命令行中的任务名称。

应用程序将设置值改为默认值。

在命令行中配置任务计划

如果在标准模式下使用应用程序，则可以配置以下类型任务的运行计划：*ODS*、*更新*、*回滚*、*ODFIM*，*ContainerScan* 和 *InventoryScan*。

如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则可以配置以下类型任务的启运行计划：*ODS*、*ODFIM*，*ContainerScan* 和 *InventoryScan*。

您可以将任务运行计划设置的当前值输出到控制台或配置文件。

要将任务运行计划的当前设置输出到控制台，请执行以下命令：

```
kesl-control --get-schedule <任务 ID/名称> [--json]
```

其中：

- <任务 ID/名称>是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- 指定 --json，则以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

要将任务运行计划的当前设置输出到配置文件，请执行以下命令：

```
kesl-control --get-schedule <任务 ID/名称> --file <配置文件路径> [--json]
```

其中：

- <任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- --file <配置文件路径> 是将输出任务运行计划设置的配置文件的路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定目录不存在，则不会创建配置文件。
- 指定 --json，则以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

例如：

将更新任务设置保存在名为 update_schedule.ini 的文件中，然后将创建的文件保存在当前目录中：

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

在控制台中显示更新任务计划：

```
kesl-control --get-schedule 6
```

您可以通过下列方式编辑任务运行计划的设置：

- 从包含所有计划设置的配置文件中导入设置。
- 使用命令行，以<设置名称>=<设置值>格式指定任务运行计划的单个设置。

要使用配置文件编辑任务运行计划设置的值，请执行以下操作：

1. 使用命令 kesl-control --get-schedule 将任务设置输出到配置文件。
2. 编辑文件中必要设置的值并保存更改。
3. 执行命令：

   ```
   kesl-control --set-schedule <任务 ID/名称> --file <配置文件路径> [--json]
   ```

   其中：

   <任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

   --file <配置文件路径> – 将从中导入任务计划设置的配置文件的完整路径。

   --json：如果您要以 JSON 格式从配置文件导入设置，请指定此键。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

   文件中定义的任务运行计划的所有设置值都将导入应用程序。

示例：
从名为 /home/test/on_demand_schedule.ini 的配置文件将计划设置导入到 ID=2 的任务中：

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

要使用命令行编辑任务运行计划设置的各个值，请执行以下命令：

```
kesl-control --set-schedule <任务 ID/名称> <设置名称>=<设置值> [<设置名称>=<设置值>]
```

其中：

- <任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。
- <设置名称>=<设置值> 是其中一项任务计划设置的名称和值。

任务运行计划的指定设置的值被更改。

例如：
要将任务安排为每十小时启动一次，请指定以下设置：

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

要将任务安排为每十分钟启动一次，请指定以下设置：

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

要将任务安排为在每月的第 15 天启动，请指定以下设置：

```
RuleType=Monthly

RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

要将任务安排为每星期二启动一次，请指定以下设置：

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

要将任务安排为每 11 天启动一次，请指定以下设置：

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

在命令行中管理常规应用程序设置

常规应用程序设置定义了应用程序整体的运行以及各个功能的操作。

您可以使用特殊的管理命令来管理常规应用程序设置：

- 将常规应用程序设置的当前值输出到控制台或配置文件。
- 使用包含所有常规设置的配置文件或使用格式为 < 设置名称 >=< 设置值 > 的命令行键来编辑常规应用程序设置。

使用常规设置，您可以：

- 在应用程序中配置卡巴斯基安全网络和反恶意软件数据库精简版的使用。
- 在应用程序中配置代理服务器的使用。
- 选择文件操作拦截模式（扫描期间阻止/不阻止文件）。
- 配置从挂载点扫描范围中排除（全局排除项）。
- 配置从进程内存扫描范围中排除。
- 启用或禁用实时容器扫描。
- 启用或禁用对入侵者可能用来破坏设备或数据的合法应用程序的检测。
- 启用或禁用与 Kaspersky Managed Detection and Response 的集成。
- 配置事件日志的使用。

- 配置扫描任务（ODS 类型）的 CPU 资源使用率限制。
- 限制非特权用户可以同时启动的用户扫描任务的数量。

显示常规应用程序设置

您可以将常规应用程序设置的当前值输出到控制台或可用于编辑任务设置的配置文件。

要将常规应用程序设置的当前值输出到控制台，请执行以下命令：

```
kesl-control --get-app-settings [--json]
```

其中指定 `--json` 后，以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

要将常规应用程序设置的当前值输出到配置文件，请执行以下命令：

```
kesl-control --get-app-settings --file <配置文件路径> [--json]
```

其中：

- `--file` 配置文件路径 > – 将写入应用程序常规设置的配置文件路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定目录不存在，则不会创建配置文件。
- 指定 `--json`，则以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

  示例：
  在名为 kesl_config.ini 的文件中显示常规应用程序设置。将创建的文件保存在当前目录中：
  `kesl-control --get-app-settings --file kesl_config.ini`

编辑常规应用程序设置

在命令行中，您可以使用命令 `kesl-control --set-app-settings` 编辑常规应用程序设置：

- 您可以使用包含常规应用程序设置的配置文件编辑所有常规设置。您可以使用显示常规设置的命令获取配置文件。
- 您可以使用命令行键，以 < 设置名称 >=< 设置值 > 格式编辑单个设置。您可以使用显示常规设置的命令获取常规应用程序设置的当前值。

要使用配置文件编辑常规应用程序设置的值：

1. 将常规应用程序设置输出到配置文件。
2. 编辑文件中必要参数的值并保存更改。
3. 执行命令：

   ```
   kesl-control --set-app-settings --file <配置文件路径> [--json]
   ```

其中：

- `--file` <配置文件路径>是包含常规应用程序设置的配置文件的完整路径。
- `--json`：如果您要以 JSON 格式从配置文件导入设置，请指定此键。如果不指定 `--json` 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

文件中定义的常规设置的所有值都将被导入应用程序。

要使用命令行键编辑常规应用程序设置的值，请执行以下命令：

```
kesl-control --set-app-settings <设置名称>=<设置值> [<设置名称>=<设置值>]
```

其中<设置名称>=<设置值>是其中一项常规应用程序设置的名称和值。

指定的常规设置的值将会更改。

例如：

从配置文件 /home/test/kesl_config.ini 将常规设置导入到应用程序：

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

将跟踪文件的详细级别设置为低：

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

添加想要从文件操作拦截中排除的挂载点：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

使用筛选器来限制查询结果

筛选器允许您在执行应用程序管理命令时限制查询结果。

筛选条件是通过一个或多个*逻辑表达式*来指定的，这些表达式使用逻辑运算符 `and` 进行组合。筛选条件必须用引号括起来：

"<字段> <比较运算符> '<值>'"

"<值> <比较运算符> '<值>' and <字段> <比较运算符> '<值>'"

其中：

- <字段>是数据库字段的名称。
- <比较运算符>是下列比较运算符之一：
  - > 表示“大于”
  - < 表示“小于”
  - `like` 匹配指定的值。在指定值时，可以使用 % 掩码：例如，逻辑表达式“FileName like '%etc%'”设置了“在 FileName 字段中包含文本‘etc’的限制”

- == 表示“等于”
- != 表示“不等于”
- >= 表示“大于或等于”
- <= 表示“小于或等于”

- < 值 > 表示该字段的值。该值必须用单引号 (') 括起来。

  您可以使用 UNIX 时间（自 1970 年 1 月 1 日 00:00:00 (UTC) 起经过的秒数）或 YYYY-MM-DD hh:mm:ss 格式指定日期值。用户指定用户当地时区的日期和时间，应用程序以同一时区显示它们。

您可以在以下应用程序管理命令中使用筛选器：

- 显示有关应用程序某些当前事件的信息：

  `kesl-control -W --query "< 筛选条件 >"`

- 显示事件日志中有关某些应用程序事件的信息：

  `kesl-control -E --query "< 筛选条件 >"`

- 显示备份中某些对象的相关信息：

  `kesl-control -B --query "< 筛选条件 >"`

- 从备份中删除某些对象：

  `kesl-control -B --mass-remove --query "< 筛选条件 >"`

  例如：

  获取在 FileName 字段包含文本“etc”的事件的信息：

  ```
  kesl-control -E --query "FileName like '%etc%'"
  ```

  显示有关“ThreatDetected”类型的事件的信息：

  ```
  kesl-control -E--query "EventType == 'ThreatDetected'"
  ```

  显示由 ODS 类型的任务创建的“ThreatDetected”类型的事件信息：

  ```
  kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
  ```

  获取在 UNIX™ 时间戳系统（自 1970 年 1 月 1 日 00:00:00 (UTC) 起经过的秒数）中指定日期后生成的事件的相关信息：

  ```
  kesl-control -E --query "Date > '1583425000'"
  ```

  获取以 YYYY-MM-DD hh:mm:ss 格式指定的日期后生成的事件的相关信息：

  ```
  kesl-control -E --query "Date > '2022-12-22 18:52:45'"
  ```

  获取备份存储中严重级别为“高”的文件的信息：

  ```
  kesl-control -B --query "DangerLevel == 'High'"
  ```

导出和导入应用程序设置

如果通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security，则无法导入设置。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则无法导出或导入“*更新*”类型的预定义任务的设置。

Kaspersky Endpoint Security 可让您导出和导入所有应用程序设置，以进行故障排除、验证设置或简化其他用户设备上的应用程序配置。导出设置时，所有应用程序设置（包括常规"容器扫描"设置、加密连接扫描设置、常规应用程序设置和任务设置）都保存在一个配置文件中。您可以使用此配置文件将设置导入应用程序。

在导入或导出设置时，必须启动应用程序。设置导入后，必须重新启动应用程序。

从较早的应用程序版本导入或导出设置时，新设置将设置为默认值。无法将设置导入到较旧的应用程序版本。

要导出应用程序设置，请执行以下命令：

```
kesl-control --export-settings --file <配置文件路径> [--json]
```

其中：

- `--file <配置文件路径>` – 将保存应用程序设置的配置文件的完整路径。
- 指定 `--json` 后，以 JSON 格式将设置导出到配置文件。如果不指定 `--json` 键，设置将导出到 INI 文件。

要从文件导入应用程序设置，请执行以下命令：

```
kesl-control --import-settings --file <配置文件路径> [--json]
```

其中：

- `--file <配置文件路径>` – 用于将设置导入到应用程序的配置文件的完整路径。
- 指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json` 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

从文件导入应用程序设置时，`UseKSN` 和 `CloudMode` 设置将设为 `No`。要开始或恢复使用卡巴斯基安全网络，请将 `UseKSN` 设置的值设为"`Basic`"或"`Extended`"。要启用云模式，必须将 `CloudMode` 设为 `Yes`。如果启用了 KSN，则云模式可用。

导入应用程序设置后，内部任务 ID 可能会更改。建议使用任务名称来管理任务。

使用命令行管理用户角色

根据用户角色向用户提供通过命令行访问 Kaspersky Endpoint Security 功能的权限。*角色*是用于管理应用程序的一组权限和特权。

在操作系统中创建了四组系统用户：*kesladmin*、*kesluser*、*keslaudit* 和 *nokesl*。向系统用户分配应用程序角色时，该用户将添加到相应的角色组中（请参阅下面的*角色*表）。撤消用户的角色时，该用户将从相应的角色组中移除。

如果没有为系统用户分配应用程序角色，则该用户属于*没有权限的用户*这个单独的组。

因此，这些角色对应于四组操作系统用户：

- kesladmin — 管理员角色
- kesluser - 用户角色
- keslaudit — 审计员角色
- 如果没有分配其他角色，则会将 nokesl 分配给用户。在这种情况下，用户属于*没有特权的用户*这个单独的组

用户角色

角色名	应用程序中的角色	操作系统用户	权限
管理员	admin	kesladmin	管理应用程序设置和任务设置。 管理应用程序授权许可。 为用户分配角色。 撤销用户角色（管理员无权撤销自己的管理员角色）。 查看和管理用户的存储。
用户	user	kesluser	仅管理用户文件扫描任务。 启动和停止更新任务。 查看此用户创建的任务的报告。 查看所有应用程序用户常见的特定事件。
审计员	audit	keslaudit	查看应用程序设置 查看应用程序状态。 查看所有任务、其设置和开始计划。 查看所有活动。 查看备份中的所有对象。
—	—	nokesl	未在应用程序中分配角色，没有权限。

查看用户和角色列表

要查看用户及其角色的列表，请执行以下命令：

```
kesl-control [-U] --get-user-list
```

为用户分配角色

要将角色分配给特定用户，请执行以下命令：

```
kesl-control [-U] --grant-role <角色> <用户>
```

示例：
要将审计角色分配给用户 test15：

```
kesl-control --grant-role audit test15
```

撤销用户角色

要撤销特定用户的角色，请执行以下命令：

```
kesl-control [-U] --revoke-role <角色> <用户>
```

示例：
要为用户 test15 撤销 audit 角色：

```
kesl-control --revoke-role audit test15
```

启动和停止应用程序

将 Kaspersky Endpoint Security 安装到设备后，应用程序将自动启动。默认情况下，启动操作系统时，应用程序将自动启动（处于每个操作系统的默认执行级别）。

默认情况下，启动 Kaspersky Endpoint Security 时，应用程序的以下功能组件将自动启动：

- 文件威胁防护。
- 设备控制。
- 行为检测。
- Web 威胁防护 — 仅当操作系统中安装了某个受支持的浏览器且在设备上允许本地管理 Web 威胁防护设置（未应用策略或策略未在策略属性中设置“锁定”）。
- 网络威胁防护—仅当通过策略定义设备上的网络威胁防护设置时。策略属性中默认启用网络威胁防护。如果在设备上应用本地配置的设置，则默认禁用网络威胁防护。

当应用程序启动时，设备上将自动启动服务任务，以确保附加应用程序功能的运行：应用程序激活功能和备份功能。

默认情况下，应用程序还将启动在命令行中配置的用户任务，这些任务的运行模式已被配置为“应用程序启动后”（PS 运行模式）。

如果停止应用程序，设备上运行的所有任务都将中断。应用程序重新启动后，中断的用户任务不会自动恢复。

使用 Web Console 启动和停止应用程序

要远程启动或停止应用程序：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。
   将打开受管理设备列表。
2. 在列表中，选择要在其上启动或停止应用程序的设备，然后单击带有设备名称的链接以打开设备属性窗口。
3. 选择“**应用程序**”选项卡。
4. 选中 **Kaspersky Endpoint Security 12.1 for Linux** 复选框。
5. 执行下列操作之一：
   - 要启动应用程序，请单击“**开始**”按钮。
   - 要停止应用程序，请单击“**停止**”按钮。

您可以使用“**监控和报告/仪表板**”窗口中的“**保护状态**”Web 小部件来监控应用程序运行状态。

使用管理控制台启动和停止应用程序

要在客户端设备上启动或停止应用程序：

1. 在管理控制台树中，进入“**受管理设备**”文件夹，选择包含必要设备的管理组。
2. 在工作区中选择“**设备**”选项卡。
3. 在受管理设备列表中，选择要为其启动或停止应用程序的设备。在设备上下文菜单中，选择“**属性**”。
4. 在“**属性：<设备名称>**”窗口中，选择“**应用程序**”部分。
   窗口右侧将显示设备上安装的卡巴斯基应用程序列表。
5. 选择 **Kaspersky Endpoint Security 12.1 for Linux**。
6. 执行下列操作之一：
   - 要运行应用程序，请单击卡巴斯基应用程序列表右侧的  按钮或在应用程序上下文菜单中选择“**启动**”。
   - 要停止应用程序，请单击卡巴斯基应用程序列表右侧的  按钮或在应用程序上下文菜单中选择“**停止**”。

使用命令行启动和停止应用程序

要运行应用程序，根账户必须是以下目录的所有者，并且只有所有者必须具有对这些目录的写入权限：/var、/var/opt、/var/opt/kaspersky、/var/log/kaspersky、/opt、/opt/kaspersky、/usr/bin、/usr/lib、/us

启动、重启和停止 Kaspersky Endpoint Security

要启动应用程序，请运行以下命令：

```
systemctl start kesl
```

要停止应用程序，请运行以下命令：

```
systemctl stop kesl
```

要重启应用程序，请运行以下命令：

```
systemctl restart kesl
```

监控 Kaspersky Endpoint Security 的状态

Kaspersky Endpoint Security 状态由监视服务监控。监视服务在应用程序启动时自动启动。

如果应用程序崩溃，则会生成 dump 文件，并自动重启应用程序。

要导出应用程序设置，请运行以下命令：

```
systemctl status kesl
```

查看设备的保护状态和应用程序设置

您可以查看有关设备保护状态的信息，以及设备上 Kaspersky Endpoint Security 及其组件的状态。

您可以通过以下方式获取有关设备保护状态的信息：

- 在 Web Console 或管理控制台中，使用客户端设备的状态（*正常*、*严重*、*警告*）。安装了 Kaspersky Security Center 网络代理的设备是 Kaspersky Security Center 的客户端设备。客户端设备的状态可能由于以下原因变为“*严重*”或“*警告*”：

  - 按照 Kaspersky Security Center 定义的规则。例如，如果设备上未安装安全应用程序、长时间未执行病毒扫描、应用程序数据库已过时、授权许可已过期或应用程序不稳定，则状态会发生变化。有关更改状态的原因以及配置分配状态的条件的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

  - Kaspersky Security Center 从托管应用程序（即 Kaspersky Endpoint Security）接收设备状态。

    必须在 Kaspersky Security Center 中分配“*严重*”和“*警告*”状态的条件列表中启用从托管应用程序接收设备状态。分配设备状态的条件在管理组的属性窗口中配置。

  有关客户端设备状态的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

- 在 Web Console 或管理控制台中，使用设备上 Kaspersky Endpoint Security 功能组件的状态。在设备上安装的 Kaspersky Endpoint Security 的属性中，显示了应用程序的功能组件列表。对于每个组件，都会显示其状态。

- 在命令行中，使用命令 `kesl-control --app-info`。该命令显示有关应用程序的操作以及应用程序的功能组件和任务状态的信息。

在 Web Console 中查看设备的保护状态

要在 Web Console 中查看设备的保护状态：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。

   将打开受管理设备列表。

2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

3. 在列表中，找到要查看信息的设备，然后单击设备名称。

4. 在打开的受管理设备的属性窗口中，在“**常规**”选项卡上，选择“**保护**”部分。

“**保护**”部分显示有关设备的以下信息：

- **在网络中可见**是所选设备在网络中的可见性：“*是*”或“*否*”。

- **设备状态**是根据管理员针对所选设备设置的保护状态标准以及设备在网络中的活动情况，生成的客户端设备的状态：*正常*、*严重*或*警告*。

- **状态描述**表示设备状态更改为“*严重*”或“*警告*”的原因。

- **保护状态**代表所选设备上"文件威胁防护"的当前状态，例如"*运行中*"、"*已停止*"或"*已暂停*"。
- **上次完全检查**表示所选设备上次完成完全检查任务的日期和时间。
- **检测到的病毒数**表示自安装 Kaspersky Endpoint Security 以来在所选设备上检测到的恶意对象总数（检测到的威胁计数器）。
- **清除失败的对象**表示 Kaspersky Endpoint Security 无法清除的受感染对象数量。

在管理控制台中查看设备的保护状态

要在管理控制台中查看设备的保护状态：

1. 在管理控制台树中，进入"**受管理设备**"文件夹，选择包含必要设备的管理组。
2. 在工作区中选择"**设备**"选项卡。
3. 在受设备列表中，选择所需的设备并双击它以打开"**属性：<任务名称>**"窗口。
4. 在打开的受管理设备属性窗口中，选择"**保护**"部分。

"**保护**"部分显示有关设备的以下信息：

- **设备状态**：根据管理员针对所选设备保护状态和设备在网络中的活动情况所设置的标准，生成的客户端设备状态。
- **所有问题**：所选设备上安装的受管理应用程序检测到的问题的完整列表。每个问题都有应用程序提示分配给设备的状态。
- **实时保护状态**：所选设备上"文件威胁防护"的当前状态，例如"*运行中*"或"*已停止*"。当保护状态发生变化时，只有在设备与管理服务器同步之后，新的状态才会显示在设备属性窗口中。
- **上一次按需扫描**：上一次在所选设备上执行恶意软件扫描的日期和时间。
- **检测到的威胁总数**：自安装应用程序（首次扫描）以来，或自上次重置威胁计数器以来，在所选设备上检测到的威胁总数。

  要重置计数器，请单击"**重置**"按钮。
- **活动威胁**：所选设备上未处理的文件数。

在 Web Console 中查看有关应用程序运行的信息

要在 Web Console 中查看有关应用程序操作的信息：

1. 在 Web Console 的主窗口中，选择"**资产（设备）**"→"**受管理设备**"。

   将打开受管理设备列表。
2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方"**当前路径**"字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

3. 在列表中，找到要查看信息的设备，然后单击设备名称。

4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。

5. 在设备上安装的卡巴斯基应用程序列表中，单击 **Kaspersky Endpoint Security 12.1 for Linux** 应用程序的名称。

   应用程序属性窗口将打开。

Kaspersky Endpoint Security 12.1 for Linux 窗口将显示有关 Kaspersky Endpoint Security 的以下信息：

- **信息**部分中的**常规**选项卡显示有关已安装应用程序的常规信息：
  - **名称**是应用程序的名称。
  - **版本**是应用程序的版本号。
  - **已安装**是在设备上安装应用程序时的日期和时间。
  - **上次软件更新**是 Kaspersky Endpoint Security 软件模块上次更新的日期和时间
  - **上次同步**是设备上次连接到 Kaspersky Security Center 管理服务器的日期和时间。
  - **当前状态**：设备上的文件威胁防护状态，例如“*运行中*”或“*已暂停*”。
  - 在**已安装的更新**下，您可以找到有关应用程序模块更新的信息。
  - 在**应用程序数据库**下，您可以找到有关应用程序数据库更新发布的日期和时间以及上次更新的日期和时间的信息。
- 在**“常规”**选项卡上，**“授权许可”**部分包含有关添加到应用程序的授权许可密钥以及与这些密钥对应的授权许可的信息。
- 在**常规**选项卡上，**组件**部分包含应用程序的功能组件列表。将显示每个组件的状态（例如，*“已停止”*、*“已暂停”*、“*未安装*”）和版本。

  在**保护虚拟环境的 Light Agent 模式**行中，您可以看到有关应用程序使用模式的信息：
  - 状态“*运行中*”表示正在 Light Agent 模式下使用应用程序。
  - 状态“*未安装*”表示正在标准模式下使用应用程序。
- **事件**选项卡显示设备上的应用程序事件列表。
- “**事件设置**”部分显示应用程序在事件存储中存储的事件类型以及存储时长。
- 在**应用程序设置**选项卡的**Detection and Response**部分中，您可以管理设备的网络隔离。

在管理控制台中查看有关应用程序运行的信息

要在 Kaspersky Security Center 管理控制台中查看有关应用程序操作的信息：

1. 在 Kaspersky Security Center 管理控制台树的“**受管理设备**”文件夹中，选择包含所需设备的管理组。

2. 在工作区中选择“**设备**”选项卡。

3. 在受管理设备列表中，选择所需的设备并双击以打开“**属性：<任务名称>**”窗口。

4. 在显示的受管理设备属性窗口中，选择“**应用程序**”部分。
   窗口右侧将显示设备上安装的卡巴斯基应用程序列表。

5. 选择 **Kaspersky Endpoint Security 12.1 for Linux** 并双击以打开应用程序属性窗口。或者，您也可以使用窗口下方的“**属性**”按钮。
   Kaspersky Endpoint Security 12.1 for Linux 设置窗口将打开。

Kaspersky Endpoint Security 12.1 for Linux 设置窗口将显示有关 Kaspersky Endpoint Security 的以下信息：

- **常规**部分包含有关已安装应用程序的常规信息：
  - **版本号**：应用程序的版本号。
  - **已安装**—在设备上安装应用程序的日期和时间。
  - **当前状态**：设备上的文件威胁防护状态，例如“*运行中*”或“*已暂停*”。
  - **上次软件更新**：Kaspersky Endpoint Security 软件模块上次更新的日期和时间。
  - **已安装更新**：已安装更新的软件模块的列表。
  - **应用程序数据库**：应用程序数据库更新发布的日期和时间。
- “**组件**”部分包含标准应用程序组件的列表。将显示每个组件的状态（例如，“*已停止*”、“*已暂停*”、“*未安装*”）和版本。
  在**保护虚拟环境的 Light Agent 模式**行中，您可以看到有关应用程序使用模式的信息：
  - 状态“*运行中*”表示正在 Light Agent 模式下使用应用程序。
  - 状态“*未安装*”表示正在标准模式下使用应用程序。
- “**授权许可密钥**”部分包含有关活动和备用授权许可密钥的信息：
  - **序号** – 唯一的字母数字序列。
  - **Status** – 授权许可密钥的状态，例如活动或备用。
  - **类型**：授权许可类型（商业或试用）。
  - **授权许可有效期** – 您可以使用以此密钥激活的应用程序的天数。
  - **授权许可限制** – 可以使用密钥的设备数量。
  - **激活日期**（此字段仅适用于活动密钥）：添加活动密钥的日期。
  - **授权许可到期日期**（此字段仅适用于活动密钥）：不能再以当前活动密钥使用应用程序的日期。
- “**事件设置**”部分显示应用程序在事件存储中存储的事件类型以及存储时长。
- **高级**部分包含有关应用程序管理插件的信息。

在命令行中查看有关应用程序操作的信息

要查看有关应用程序的信息，请执行以下命令：

```
kesl-control --app-info [--json]
```

其中 `--json`：以 JSON 格式输出数据。如果未指定 `--json` 键，则设置将以 INI 格式导入。

命令执行的结果会在控制台中显示如下信息：

- **Name**。应用程序名称。
- **版本**。当前应用程序版本。
- **策略**。有关 Kaspersky Security Center 策略是否应用于设备的信息。
- **应用程序授权许可信息** 应用程序授权许可信息或应用程序授权许可密钥状态。
- **应用程序授权许可到期日期**。应用程序授权许可到期的日期和时间，以 UTC 表示。
- **EDR Optimum 授权许可信息**。有关据其使用 Kaspersky Endpoint Detection and Response Optimum 功能的授权许可的信息，或 EDR Optimum 授权许可密钥的状态。
- **EDR Optimum 授权许可到期日期**。使用 Kaspersky Endpoint Detection and Response Optimum 功能的授权许可到期的日期和时间 (UTC)。
- **订阅状态**。订阅状态。如果应用程序在订阅下启动，则将显示此字段。
- **MDR BLOB 文件状态**。用于与 Kaspersky Managed Detection and Response 集成的 BLOB 配置文件的状态。
- **MDR BLOB 授权许可到期日期**。Kaspersky Managed Detection and Response 授权许可到期的日期和时间，以 UTC 表示。
- **备份区状态**。备份区状态。
- **备份区空间使用**。备份容量。
- **Scan_My_Computer 任务的上次运行日期**。上次运行“恶意软件扫描”任务的时间。
- **数据库的上次发布日期**。应用程序数据库的上次发布日期和时间。
- **应用程序数据库**。有关应用程序数据库是否已下载的信息。
- **使用卡巴斯基安全网络**。有关使用卡巴斯基安全网络的信息：`KSN 扩展模式`、`KSN 基本模式`或`已禁用`。
- **用于保护虚拟环境的 Light Agent 模式**。应用程序正在 Light Agent 模式下使用以保护虚拟环境的信息。如果应用程序在标准模式下使用，则不会显示该行。
- **卡巴斯基安全网络基础架构**。有关用于与卡巴斯基信誉数据库配合使用的基础架构解决方案的信息：卡巴斯基安全网络或卡巴斯基私人安全网络。

- “文件杀毒和删除被禁用”。有关启用应用程序操作模式的信息，在该模式下，无论在策略属性中配置的设置如何，都不会对磁盘上的文件进行消毒和删除。
- 集成 Kaspersky Managed Detection and Response。与 Kaspersky Managed Detection and Response 集成的状态：已启用、已禁用。
- Kaspersky Endpoint Detection and Response Optimum 集成。与 Kaspersky Endpoint Detection and Response Optimum 集成的状态。
- 文件威胁防护。实时文件威胁防护状态。
- 容器监控。实时容器扫描状态。
- 系统完整性监控。系统完整性监控组件状态。
- 防火墙管理。防火墙管理组件状态。
- 反加密勒索。反加密勒索组件状态。
- Web 威胁防护。Web 威胁防护组件状态。
- 设备控制。设备控制组件状态。
- 可移动驱动器扫描。可移动驱动器扫描组件状态。
- 网络威胁防护。网络威胁防护组件状态。
- 行为检测。行为检测组件状态。
- 应用程序控制。应用程序控制组件状态。
- Web 控制。Web 控制组件状态。
- Kaspersky Endpoint Detection and Response (KATA) 集成。Kaspersky Endpoint Detection and Response (KATA) 集成状态。
- 更新后的操作。应用程序更新操作和用户要执行的操作。
- 不稳定的应用程序操作。有关应用程序失败和转储文件创建的信息。如果在上次启动应用程序时发生了失败，则显示该字段。

应用程序激活和授权许可密钥管理

*激活*是激活授权许可的过程，允许您使用应用程序的完整功能版本，直到授权许可到期。

激活 Kaspersky Endpoint Security 的过程涉及添加活动的应用程序授权许可密钥到设备。

如果您在不包含Kaspersky Endpoint Detection and Response Optimum功能的授权许可下使用应用程序，则若要激活此功能，您需要添加额外的 Kaspersky Endpoint Detection and Response Optimum 附加授权许可密钥（"EDR Optimum 密钥"）到设备。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则无需单独激活应用程序。您激活 Kaspersky Hybrid Cloud Security for Virtualization Light Agent；激活在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一个组件）上执行，方法是将授权许可密钥添加到 SVM。若要激活Kaspersky Endpoint Detection and Response Optimum 的功能，您还需要将 EDR Optimum 密钥添加到 SVM。

可以通过以下方法之一激活应用程序：

- 使用 Kaspersky Security Center 远程执行：
  - 在 Kaspersky Endpoint Security 安装期间。您可以将应用程序授权许可密钥添加到安装包中。应用程序将在安装后自动激活。
  - 安装 Kaspersky Endpoint Security 后，使用应用程序激活任务。
  - 安装 Kaspersky Endpoint Security 后，通过将许可证密钥从管理服务器分发到客户端设备。
- 使用命令行：
  - 在 Kaspersky Endpoint Security 的初始配置期间。
  - 安装 Kaspersky Endpoint Security 后，使用管理命令。

要将 EDR Optimum 密钥添加到设备，您可以使用添加密钥任务或将密钥分发到客户端设备的程序。您不需要指定密钥的类型。

仅在添加应用程序授权许可密钥后，您才可以添加 EDR Optimum 密钥。

您还可以向设备添加备用应用程序密钥和备用 EDR Optimum 密钥。当与活动密钥关联的授权许可到期或活动密钥被删除时，备用密钥成为活动密钥。备用密钥可避免当授权许可到期时应用程序功能受限。

只有在添加了活动授权许可密钥之后，才可以添加备用授权许可密钥。

您可以查看有关添加到设备的授权许可密钥的信息：

- 在 Web Console 或管理控制台中远程进行。在客户端设备上，应用程序的属性包含有关"**授权许可密钥**"部分中的活动密钥和备用密钥的信息。
- 在命令行中使用管理命令。

在命令行中查看有关授权许可和密钥的信息

在命令行中，使用 `-L --query` 命令，您可以查看有关添加到应用程序的活动授权许可密钥和备用授权许可密钥的信息，以及有关应用程序已激活的授权许可的信息。如果已向应用程序添加了用于激活 Kaspersky Endpoint Detection and Response Optimum功能的单独密钥，则有关 EDR Optimum 的活动和备用授权许可密钥以及 EDR Optimum 授权许可的信息也会得到显示。

要查看有关设备上的授权许可密钥和授权许可的信息，请运行以下命令：

```
kesl-control -L --query [--json]
```

其中 `--json`：以 JSON 格式输出数据。如果未指定 `--json` 键，则设置将以 INI 格式导入。

命令执行的结果会在控制台中显示如下信息：

- 有关活动应用程序密钥的信息（如果已添加密钥）：
  - 使用应用程序的授权许可到期的日期和时间。
  - 距授权许可期限结束的剩余天数。
  - 有关保护功能限制的信息。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。
  - 与密钥关联的授权许可类型。
  - 密钥的授权许可限制（授权许可单元的数量）。
  - 该密钥要激活的应用程序的名称。
  - 活动授权许可密钥（唯一的字母数字序列）。
  - 激活日期。
- 应用程序备用密钥信息。如果应用程序在标准模式下使用且已添加备用密钥则显示。如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则不会显示有关备用密钥的信息；备用密钥将添加到 SVM。
  - 使用应用程序的授权许可到期的日期和时间。
  - 距授权许可期限结束的剩余天数。
  - 有关保护功能限制的信息。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。
  - 与密钥关联的授权许可类型。

- 密钥的授权许可限制（授权许可单元的数量）。
- 该密钥要激活的应用程序的名称。
- 激活日期。

- 有关 EDR Optimum 活动密钥的信息（如果已添加密钥）：
  - 使用 Kaspersky Endpoint Detection and Response Optimum 功能的授权许可到期的日期和时间。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。
  - 与密钥关联的授权许可类型。
  - 密钥的授权许可限制（授权许可单元的数量）。
  - 该密钥要激活的应用程序的名称。
  - 活动授权许可密钥（唯一的字母数字序列）。
  - 激活日期。
- EDR Optimum 备用密钥信息。如果应用程序在标准模式下使用且已添加 EDR Optimum 备用密钥则显示。如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则不会显示有关备用密钥的信息；备用密钥将添加到 SVM。
  - 使用 Kaspersky Endpoint Detection and Response Optimum 功能的授权许可到期的日期和时间。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。
  - 与密钥关联的授权许可类型。
  - 密钥的授权许可限制（授权许可单元的数量）。
  - 该密钥要激活的应用程序的名称。
  - 激活日期。

命令行中的授权许可密钥管理

如要管理设备上的授权许可密钥，可以使用授权许可密钥管理命令。

只有在标准模式下使用应用程序时，才能执行管理授权许可密钥的命令。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则管理授权许可密钥的命令将终止并显示错误。您可以将应用程序作为 Kaspersky Security for Virtualization Light Agent 的一部分进行激活，因此无需单独激活该应用程序。

如要将活动密钥添加到应用程序，请运行以下命令：

```
kesl-control [-L] --add-active-key <密钥文件路径/激活码>
```

其中：

- <密钥文件的路径> - 密钥文件的路径。如果密钥文件位于当前目录中，则仅指定文件名就足够了。
- <activation code> - 激活码。

如要将备用授权许可密钥添加到应用程序，请执行以下命令：

```
kesl-control [-L] --add-reserve-key <密钥文件路径/激活码>
```

如果活动密钥尚未被添加到设备上的应用程序，则命令失败。

您可以使用添加密钥命令来添加应用程序授权许可密钥以及 EDR Optimum 授权许可密钥。您不需要在命令中指定密钥的类型。

若要删除活动应用程序密钥，请运行以下命令：

```
kesl-control [-L] --remove-active-key
```

若要删除备用应用程序密钥，请运行以下命令：

```
kesl-control [-L] --remove-reserve-key
```

若要删除活动 EDR Optimum 密钥，请运行以下命令：

```
kesl-control [-L] --remove-active-key --edr-optimum
```

若要删除备用 EDR Optimum 密钥，请运行以下命令：

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

更新应用程序数据库和模块

在美国境内，为遵守贸易限制，自 2024 年 9 月 10 日美国东部夏令时间 (EDT) 凌晨 12:00 起，该应用程序将不再提供更新功能（包括反病毒签名更新和代码库更新）。

更新 Kaspersky Endpoint Security 的数据库和应用程序模块可确保为您的设备提供最新保护。新病毒、恶意软件和其他类型的威胁每天都在全世界出现。应用程序数据库包含有关威胁和威胁消除方法的信息。要快速检测到威胁，建议您定期更新应用程序数据库和模块。

定期更新数据库需要当前的应用程序授权许可。如果没有最新的授权许可，您将只能执行一次更新。

在更新过程中，数据库和应用程序模块将被下载并安装到您的设备上。

您可以从卡巴斯基更新服务器、管理服务器存储库、本地或网络目录以及其他更新源获取数据库和应用程序模块的更新。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则 SVM 上的目录将用作更新源。

更新时，您设备上的应用程序模块和数据库将与更新源处的最新版本进行对比。如果您当前数据库和程序模块与相应的最新版本不同，缺少的更新部分将安装在您的设备上。

如果数据库过时，更新包可能会很大，这可能会花费更多的互联网流量（最多达几十 MB）。磁盘空间量最多可达 3 GB。

通过标准网络协议从卡巴斯基更新服务器或者其他 FTP、HTTP 或 HTTPS 服务器下载更新。默认情况下，系统将自动确定互联网连接设置。如果您使用代理服务器，请在应用程序的常规设置中指定代理服务器设置。

无论更新源是什么，都会下载更新包并使用“*更新*”任务在设备上安装数据库和应用程序模块更新。

应用程序中创建了预定义任务“*更新*”。使用此任务，您可以对数据库和应用程序模块进行计划和按需更新并配置更新设置。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则受保护虚拟机上的数据库使用特殊的“*更新*”本地任务进行更新，其中 SVM 上的目录被指定为更新源。该更新任务自动启动。您不能删除此任务，也不能更改其设置。

不支持使用在 Kaspersky Security Center 中创建的任务来更新数据库和应用程序模块。

如果在标准模式下使用 Kaspersky Endpoint Security，则在 Kaspersky Security Center 中，您可以使用初始设置向导在安装 MMC 管理插件或 Kaspersky Endpoint Security Web 管理插件后创建的“*更新*”组任务。

您还可以在命令行和 Kaspersky Security Center 中创建更新用户任务。

您可以配置以下设置来更新数据库和应用程序模块：

- 根据所使用的更新方案，选择应用程序接收更新的来源。

- 配置尝试连接所选更新源时的响应超时。如果更新源在指定时间内未响应，应用程序将联系列表中的下一个更新源。
- 选择下载安装应用程序模块和应用程序版本更新的模式：下载并安装、仅下载、不下载。
- 配置更新任务的运行计划。默认情况下，应用程序每 60 分钟更新一次数据库。

更新数据库和模块

更新期间，以下对象将下载并安装到您的设备中：

- 应用程序数据库。应用程序数据库包括恶意软件特征数据库、网络攻击描述、恶意和钓鱼网址数据库、条幅数据库、垃圾邮件数据库以及其他数据。

  如果设备上的数据库更新中断或终止并显示错误，应用程序将继续使用先前安装的数据库版本。如果之前没有安装应用程序数据库，应用程序将继续在"无数据库"模式下运行。数据库和应用程序模块更新仍然可用。

  如果数据库下载时间不超过三天，则为最新数据库。默认情况下，如果最近安装的数据库更新在卡巴斯基服务器上发布的时间已超过三天但少于七天，则应用程序将生成"*数据库已过期*"事件 (*BasesAreOutOfDate*)。如果数据库已七天未更新，应用程序会生成"*数据库已严重过期*"(*BasesAreTotallyOutOfDate*) 事件。

- 应用程序模块。模块更新旨在消除应用程序中的漏洞并改进保护设备的方法。模块更新可能会更改应用程序组件的行为并添加新功能。

  可以安装应用程序模块，而无需考虑应用程序的状态（已启动或已停止，由 Kaspersky Security Center 策略管理）和更新计划。在应用程序模块更新过程中，Kaspersky Endpoint Security 会继续保护您的设备。在更新期间，应用程序设置和应用程序日志文件将迁移到新版本的应用程序。更新后，需要重启 Kaspersky Endpoint Security。

  如果应用程序设置的传输由于任何原因失败，应用程序将设置为默认值。

  更新完成后且应用程序重新启动前对应用程序设置进行的更改不会保存。

  使用自动补丁更新应用程序版本后，与操作系统防火墙交互的机制会发生变化：使用 iptables 和 iptables-restore 系统实用程序管理规则。

  如果应用程序在更新后不能正常工作，它会自动回滚到以前的版本。建议联系卡巴斯基技术支持。

更新来源和场景

*更新源*是包含 Kaspersky Endpoint Security 数据库和应用程序模块更新的资源。更新源可以是 FTP、HTTP 或 HTTPS 服务器（如卡巴斯基更新服务器），以及用户挂载的本地或网络目录。

如果 Kaspersky Endpoint Security 在 Light Agent 模式下保护虚拟环境，则受保护虚拟机上的数据库将从 SVM 上的目录进行更新。

主要的应用程序更新源是卡巴斯基更新服务器。您可以在"*更新*"任务设置中指定其他更新源。如果无法从一个更新源执行更新，Kaspersky Endpoint Security 会切换到下一个更新源。

Kaspersky Endpoint Security 支持以下方案来更新数据库和应用程序模块：

- 从卡巴斯基更新服务器进行更新。卡巴斯基更新服务器位于世界各地的不同国家/地区，这确保了更新的高可靠性。如果无法从其中一个服务器执行更新，应用程序会切换到下一个服务器。通过 HTTPS 协议下载更新。
- 集中更新可减少外部互联网流量，并提供方便的更新监控。

集中更新包括以下步骤：

1. 将更新包下载到组织网络内的存储库。

   您可以使用 Kaspersky Security Center 管理服务器的存储库作为存储库。

   更新包通过管理服务器的“*将更新下载到管理服务器存储库*”任务下载到管理服务器存储库。

   如果您使用 Kaspersky Security Center 云控制台来管理应用程序，则可以使用分发点（已安装网络代理的设备）的存储库作为存储库。有关分发点的更多详细信息，请参阅“Kaspersky Security Center 帮助”。

2. 将更新包分发到客户端设备

   更新包由 Kaspersky Endpoint Security 的“*更新*”任务分发到客户端设备。在任务设置中，选择 Kaspersky Security Center 管理服务器作为更新源。

- 从用户挂载的本地或网络目录 (SMB/NFS)，或从 FTP、HTTP 或 HTTPS 服务器进行更新。您可以在“*更新*”任务设置中指定自定义更新源。

在 Web Console 中更新应用程序数据库和模块

更新 Kaspersky Endpoint Security 数据库和应用程序模块的过程取决于应用程序使用模式。本节介绍在标准模式下更新应用程序的过程。如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则无法使用在 Kaspersky Security Center 中创建的任务来更新数据库和应用程序模块。使用本地预定义任务执行更新。

在 Web Console 中，您可以使用“*更新*”任务更新数据库和应用程序模块。您可以使用自动创建的“*更新*”组任务，也可以创建用户任务进行更新。

要在 Web Console 中配置更新设置：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**任务**”。

   将打开任务列表。

2. 执行下列操作之一：

   - 如果要编辑在特定管理组中包含的所有设备上运行的任务的设置，请单击窗口上部“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

     该列表仅显示为所选管理组配置的任务。

   - 如果要编辑在一个或多个设备上运行的任务（一组设备的任务）的设置，请单击窗口上部“**当前路径**”字段中的链接，然后在打开的窗口中选择带有管理服务器名称的顶部节点。

     该列表显示在管理服务器上创建的所有任务。

3. 在任务列表中，选择所需的“**更新**”任务并通过单击任务名称中的链接打开任务属性窗口。

4. 在任务属性窗口中，选择“**应用程序设置**”选项卡。在左侧列表中选择**更新源**部分。

5. 根据所使用的更新方案，选择应用程序将从中接收数据库和模块更新的更新源。

   如果您使用 Web Console 管理应用程序，则更新源列表包含卡巴斯基更新服务器和 Kaspersky Security Center 管理服务器。如果您使用 Kaspersky Security Center 云控制台管理应用程序，更新源列表包含卡巴斯基更新服务器和分发点（有关分发点的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统）。您可以将其他更新源添加到列表中。

您可以通过选择“**本地或全球网络上的其他源**”选项来创建更新源列表。您可以将 FTP、HTTP 或 HTTPS 服务器指定为更新源。如果无法从一个更新源执行更新，Kaspersky Endpoint Security 会切换到下一个更新源。应用程序按照更新源在表中出现的顺序访问更新源。

6. 转到“**设置**”部分并配置其他更新设置。

7. 选择“**计划**”选项卡并配置运行更新任务的计划。

   如果您已选择 **Kaspersky Security Center** 作为更新源，请从“**计划启动**”下拉列表中选择“**当下载更新到存储库时**”。有关计划任务的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

8. 单击“**保存**”按钮以保存更改。

任务将根据配置的计划启动。您也可以手动运行任务。

Update 任务部分的更新源

设置	描述
更新源	在此部分中，您可以选择更新源： • **卡巴斯基更新服务器**，其中发布卡巴斯基应用程序的数据库更新（默认值）。 • **Kaspersky Security Center** – Kaspersky Security Center 管理服务器（此选项仅适用于 Web Console）。 • **分发点**（此选项仅适用于 Kaspersky Security Center 云控制台）。 • **本地或全球网络上的其他源** – HTTP、HTTPS 或 FTP 服务器或本地网络服务器上的目录。
如果其它更新源不可用则使用卡巴斯基更新服务器	此复选框用于启用或禁用当选定的更新源不可用时使用卡巴斯基更新服务器作为更新源的功能。 如果在“**更新源**”块中选择了“**本地或全球网络上的其他源**”或“**Kaspersky Security Cente**”选项，则该复选框可用。 默认选中该复选框。
自定义更新源	此表包含自定义数据库更新源的列表。在更新过程中，应用程序将按照更新源在表中的显示顺序访问更新源。 该表包含以下列： • **更新源**是 HTTP、HTTPS 或 FTP 服务器或本地网络服务器上的目录。 • 该切换开关指示是否在任务中使用源（“**已启用**”或“**已禁用**”）。您可以开关表中的切换开关，以及选中或清除“**更新源**”窗口中的“**使用此源**”复选框，该窗口通过单击带有源名称的链接打开。 如果已选择**本地或全球网络上的其他源**选项，则此表可用。 该表默认为空。 您可以在表中添加、编辑、删除、上移或下移更新源。 单击“**下移**”按钮可将所选项目在表中向下移动。 如果在表中只选择一个项目，则此按钮可用。

	单击“**上移**”按钮可将所选项目在表中向上移动。 如果在表中只选择一个项目，则此按钮可用。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Update 任务设置部分

设置	Description
等候更新源响应的最长时间(秒)	应用程序等待来自所选更新源的响应的最长时长（秒）。如果在此时间内没有响应到达，则在任务日志中记录一个涉及与更新源失联的事件。 可用值：0-120。如果指定 0，则应用程序会无限期地等待来自所选源的响应。 默认值：10 秒。
应用程序更新下载模式	在下拉列表中，可以选择更新应用数据库时使用的模式： • **不下载**更新。如果选择此列表项，则无法更新应用程序。 • **仅下载**更新文件，但不将其安装在客户端设备上（默认值）。 • **下载并安装**更新到客户端设备。安装更新后，将自动重新启动应用程序。 KESL 容器不支持此功能。

在管理控制台中更新应用程序数据库和模块

更新 Kaspersky Endpoint Security 数据库和应用程序模块的过程取决于应用程序使用模式。本节介绍在标准模式下更新应用程序的过程。如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则无法使用在 Kaspersky Security Center 中创建的任务来更新数据库和应用程序模块。使用本地预定义任务执行更新。

在管理控制台中，您可以使用“*更新*”任务更新数据库和应用程序模块。您可以使用自动创建的“*更新*”组任务，也可以创建用户任务进行更新。

要在管理控制台中配置更新设置：

1. 在管理控制台中，执行以下操作之一：

- 要编辑在指定管理组中包含的设备上运行的任务的设置，请在控制台树中选择此管理组，然后在工作区中选择“**任务**”选项卡。
- 要编辑在一台或多台设备上运行的任务（一组设备的任务）的设置，请选择控制台树中的“**任务**”文件夹。

2. 在任务列表中，选择所需的“**更新**”任务，然后双击以打开任务属性窗口。
3. 在任务属性窗口中，选择左侧列表中的“**更新源**”部分。
4. 根据所使用的更新方案，选择应用程序将从中接收数据库和模块更新的更新源。

   更新源列表包含卡巴斯基更新服务器和 Kaspersky Security Center 管理服务器。您可以将其他更新源添加到列表中。

   您可以通过选择“**本地或全球网络上的其他源**”选项来创建更新源列表。您可以将 FTP、HTTP 或 HTTPS 服务器指定为更新源。如果无法从一个更新源执行更新，Kaspersky Endpoint Security 会切换到下一个更新源。应用程序按照更新源在表中出现的顺序访问更新源。
5. 选择“**设置**”部分并配置其他更新设置。
6. 选择“**计划**”部分并配置运行更新任务的计划。

   如果您已选择 **Kaspersky Security Center** 作为更新源，请从“**计划启动**”下拉列表中选择“**当下载更新到存储库时**”。有关计划任务的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。
7. 在“**属性：<任务名称>**”窗口中单击“**应用**”或“**确定**”以保存所做的更改。

任务将根据配置的计划启动。您也可以手动运行任务。

Update 任务部分的更新源

设置	描述
更新源	在此部分中，您可以选择更新源： • **卡巴斯基更新服务器**，其中发布卡巴斯基应用程序的数据库更新（默认值）。 • **Kaspersky Security Center** – Kaspersky Security Center 管理服务器。 • **本地或全球网络上的其他源** – HTTP、HTTPS 或 FTP 服务器或本地网络服务器上的目录。
如果其它更新源不可用则使用卡巴斯基更新服务器	此复选框用于启用或禁用当选定的更新源不可用时使用卡巴斯基更新服务器作为更新源的功能。 如果在“**更新源**”块中选择了“**本地或全球网络上的其他源**”或“**Kaspersky Security Cente**”选项，则该复选框可用。 默认选中该复选框。
自定义更新源	此表包含自定义数据库更新源的列表。在更新过程中，应用程序将按照更新源在表中的显示顺序访问更新源。 该表包含以下列： • **源地址** - HTTP、HTTPS 或 FTP 服务器或本地网络服务器上的目录。 • **状态**指示源是否在任务中使用（**正在使用**或**未使用**）。您可以通过在单击**编辑**按钮时打开的**更新源**窗口中选中或清除**使用此源**复选框来更改状态。 如果已选择**本地或全球网络上的其他源**选项，则此表可用。 您可以在表中添加、编辑、删除、上移或下移更新源。

	单击“**下移**”按钮可将所选项目在表中向下移动。 如果在表中只选择一个项目，则此按钮可用。 单击“**上移**”按钮可将所选项目在表中向上移动。 如果在表中只选择一个项目，则此按钮可用。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。 该表默认为空。

Update 任务设置部分

设置	Description
等候更新源响应的最长时间(秒)	应用程序等待来自所选更新源的响应的最长时长（秒）。如果在此时间内没有响应到达，则在任务日志中记录一个涉及与更新源失联的事件。 可用值：0-120。如果指定 0，则应用程序会无限期地等待来自所选源的响应。 默认值：10 秒。
应用程序更新下载模式	在下拉列表中，可以选择更新应用数据库时使用的模式： • **不下载**更新。如果选择此列表项，则无法更新应用程序。 • **仅下载**更新文件，但不将其安装在客户端设备上（默认值）。 • **下载并安装**更新到客户端设备。安装更新后，将自动重新启动应用程序。 KESL 容器不支持此功能。

在命令行中更新应用程序数据库和模块

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则受保护虚拟机上的数据库使用特殊的“*更新*”本地任务进行更新，其中 SVM 上的目录被指定为更新源。该更新任务自动启动。您不能删除此任务，也不能更改其设置。

在命令行上，您可以通过以下方式更新数据库和应用程序模块：

- 使用“*更新*”预定义任务。您可以手动启动、停止、暂停或恢复此任务并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。
- 使用用户任务进行更新（“*更新*”类型的任务）。您可以手动启动用户任务并配置任务计划。

更新任务设置

设置	描述	值
SourceType	应用程序接收更新的来源。	KLServers（默认值）：应用程序从一个卡巴斯基更新服务器接收更新。通过 HTTPS 协议下载更新。 SCServer。应用程序将更新从本地网络上安装的管理服务器下载到受保护设备上。如果您使用 Kaspersky Security Center 对您组织中的设备保护进行集中管理，则可以选择此更新源。 Custom - 应用程序从 [CustomSources.item_#] 部分中指定的自定义来源下载更新。您可以指定 FTP、HTTP 和 HTTPS 服务器上的目录或受保护客户端设备上挂载的任何设备上的目录，包括通过 Samba 或 NFS 协议挂载的远程设备上的目录。
UseKLServersWhenUnavailable	如果所有自定义更新源都不可用，应用程序对 Kaspersky 更新服务器的访问。	Yes（默认值）- 如果所有自定义更新源都不可用，应用程序将连接到 Kaspersky 更新服务器。 No - 如果所有自定义更新源都不可用，应用程序将不会连接到 Kaspersky 更新服务器。
ApplicationUpdateMode	应用程序更新下载和安装模式。	Disabled - 不下载或安装应用程序更新。 DownloadOnly（默认值）- 下载应用程序更新，但不安装它们。 DownloadAndInstall - 自动下载并安装应用程序更新。安装更新后，将自动重新启动应用程序。
ConnectionTimeout	尝试连接到更新源时，更新源的响应超时时间（以秒为单位）。如果更新源在指定的时间间隔内未响应，则应用程序将联系列表中的下一个更新源。	您只能使用 0 到 120 范围内的整数。 默认值：10。
[CustomSources.item_#] 部分包含以下设置：		
URL	局域网或互联网上的自定义更新源的地址。	默认值为未定义。 例如： URL=http://example.com/bases/ - 包含更新的目录的 HTTP 服务器地址。

		URL=/home/bases/ - 受保护的计算机上包含应用程序数据库的目录。
Enabled	使用 URL 设置中指定的更新源。 要运行该任务，需要启用至少一个更新源。	Yes – 应用程序使用更新源。 No – 应用程序不使用更新源。 默认值为未定义。

使用 Kaspersky Update Utility 进行更新

为了节省互联网流量，您可以使用 Kaspersky Update Utility 配置组织 LAN 的设备从共享目录更新应用程序数据库和模块。为此，组织 LAN 上的其中一台设备必须从 Kaspersky Security Center 管理服务器或卡巴斯基更新服务器接收更新包，然后使用该实用程序将接收到的更新包复制到共享目录。组织 LAN 上的其他设备将能够从该共享目录接收更新包。

要使用 Kaspersky Update Utility 从共享目录配置数据库更新：

1. 在组织的 LAN 上的其中一台设备上安装 Kaspersky Update Utility。

   您可以从卡巴斯基技术支持网站下载 Kaspersky Update Utility 分发包。

2. 在 Kaspersky Update Utility 设置中配置将更新包复制到共享目录。

   选择更新源（例如，管理服务器存储库）和 Kaspersky Update Utility 将更新包复制到其中的共享目录。有关使用 Kaspersky Update Utility 的详细信息，请参阅卡巴斯基知识库。

3. 配置组织 LAN 上的其余设备从指定共享目录更新应用程序数据库和模块。

   a. 使用 Web Console 或管理控制台打开将在所需设备上执行的“**更新**”任务的属性。

   b. 在任务属性中，选择“**更新源**”部分。

   c. 在“**更新源**”部分中，选择“**本地或全球网络上的其他源**”选项。

4. 在“更新源”表中，单击“**添加**”按钮并指定共享目录的路径。

   源地址必须与 Kaspersky Update Utility 设置中指示的地址匹配。

5. 选中“**使用此源**”复选框，单击“**确定**”。

6. 在表中，使用“**向上**”和“**向下**”按钮设置更新源的顺序。

7. 将更改保存到任务设置中。

回滚应用程序数据库和模块更新

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则该任务不能用于回滚数据库更新。

第一次更新应用程序数据库后，就可以将应用程序数据库回滚至先前版本了。

每次用户开始更新过程时，Kaspersky Endpoint Security 都会为当前应用程序数据库创建一个备份副本。这可让您在需要时将应用程序数据库回滚到以前的版本。

回滚上一次数据库更新可能很有用，例如，当新的应用程序数据库版本包含无效签名而导致 Kaspersky Endpoint Security 阻止安全的应用程序时。

在命令行中，要回滚更新，您可以运行“*回滚*”预定义任务或创建并运行用于回滚更新的用户任务（“*回滚*”类型的任务）。

在 Kaspersky Security Center 中，您可以使用 Web Console 或管理控制台为管理组或单个设备创建回滚任务。

“*回滚*”任务没有任何设置。

文件威胁防护。

文件威胁防护组件可防止设备的文件系统受到感染。当 Kaspersky Endpoint Security 启动时，该组件会使用默认设置自动启用。它驻留在设备操作内存中，并实时扫描已经打开、保存和启动的所有文件。

检测到恶意软件后，Kaspersky Endpoint Security 可能会移除受感染的文件并终止从该文件启动的恶意软件进程。

组件的运行会受到文件操作拦截模式的影响，您可以在应用程序的常规设置中选择该模式。默认在扫描期间阻止对文件的访问。

如果启用了文件威胁防护和容器监控，应用程序还会扫描所有受支持的操作系统上的所有命名空间和容器。

您可以启用或禁用“文件威胁防护”，还可以配置保护设置：

- 选择文件扫描模式（打开时扫描或打开并修改时扫描）。
- 启用或禁用对压缩文件、邮件数据库、文本格式的电子邮件消息的扫描。
- 暂时从重新扫描范围中排除文本格式的文件。
- 限制要扫描的对象的大小以及对象扫描的持续时间。
- 选择应用程序将对感染对象执行的操作。
- 配置扫描范围。该应用程序将扫描文件系统指定区域中的对象。
- 配置从扫描范围中排除的对象。*扫描排除项*是一组条件。当满足这些条件时，该应用程序不会扫描对象中是否存在病毒和其他恶意软件。您可以从扫描范围中排除以下对象：
  - 按名称或掩码排除的对象
  - 按对象中检测到的威胁的名称排除的对象
  - 文件系统指定区域中的文件和目录
  - 指定进程正在修改的进程和文件
- 配置扫描期间启发式分析器和 iChecker 技术的使用。
- 启用或禁用对有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息进行记录。

要优化“文件威胁防护”任务，您可以从扫描范围中排除正在从网络目录复制的任何文件。只有在复制到本地目录的过程完成后才会扫描文件。要从扫描范围中排除位于网络目录中的文件，请根据用于从网络目录复制的实用程序（例如 `cp` 实用程序）的进程配置排除。如果您使用 Kaspersky Security Center 管理应用程序，则可以在 Web Console 或管理控制台中根据进程配置排除。如果您使用命令行管理应用程序，则可以通过向 OAS 任务设置中添加 `[ExcludedForProgram.item_ #]` 部分来配置进程排除。

在 Web Console 中配置文件威胁防护

在 Web Console 中，您可以在策略属性中管理文件威胁防护（**应用程序设置 → 基本威胁防护 → 文件威胁防护**）。

设置	描述
文件威胁防护已启用/已禁用	此切换开关用于启用或禁用所有受管理设备上的文件威胁防护组件。 默认情况下，复选切换按钮处于打开状态。
文件威胁防护模式	在此下拉列表中，您可以选择文件威胁防护组件模式： • **智能检查**（默认值）– 当有人尝试打开文件时对其进行扫描，如果文件已被修改，则当有人尝试关闭它时再次进行扫描。如果某个进程在特定时间段内多次访问和修改一个文件，则仅当该进程最后一次关闭文件后，应用程序才会再次扫描该文件。 • **打开时** – 在有人尝试打开文件以进行读取、执行或修改时对其进行扫描。 • **打开和修改时** – 在有人尝试打开文件时对其进行扫描，如果文件已被修改，则在尝试关闭文件时再次扫描该文件。
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **阻止**访问对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。 • **阻止**访问对象（默认值）。
扫描范围	单击“**配置扫描范围**”链接将打开“**保护范围**”窗口。
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中该复选框，应用程序将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过启用并配置“**如果扫描时间超过以下值(秒)则跳过文件**”和“**跳过大于以下大小的文件(MB)**”设置，可以减少压缩文件扫描时间。 如果清除该复选框，应用程序不会扫描压缩文件。 默认情况下，清除此复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中该复选框，应用程序将扫描自解压存档。 如果清除了该复选框，则应用程序不会扫描自解压存档。 如果清除**扫描压缩文件**复选框，则此复选框可用。 默认情况下，清除此复选框。

扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中该复选框，应用程序将扫描邮件数据库文件。 如果清除了该复选框，则应用程序不会扫描邮件数据库文件。 默认情况下，清除此复选框。
扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则应用程序将扫描纯文本邮件。 如果清除此复选框，则应用程序不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过文本文件	从扫描中临时排除纯文本格式的文件。 如果选中该复选框，应用程序不会扫描文本文件，前提是它们在最近一次扫描后 10 分钟内被同一进程重复使用。此设置使优化应用程序日志扫描成为可能。 如果清除了该复选框，应用程序将扫描文本文件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，应用程序将停止扫描该文件。 可用值：`0-9999`。如果该值设置为 `0`，则扫描时间不受限制。 默认值为 `60`。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：`0-999999`。如果该值设置为 `0`，则应用程序将扫描任何大小的文件。 默认值为 `0`。
记录清洁对象	此复选框用于启用或禁用记录 *ObjectProcessed* 事件。 如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 事件。 如果清除该复选框，则应用程序不会记录事件。 默认情况下，清除此复选框。
记录未处理的对象	此复选框用于启用或禁用当扫描期间无法处理文件时记录 *ObjectNotProcessed* 事件。 如果选中此复选框，则应用程序将记录 *ObjectNotProcessed* 事件。 如果清除该复选框，则应用程序不会记录事件。 默认情况下，清除此复选框。
记录打包对象	此复选框用于启用或禁用针对检测到的所有打包对象记录 *PackedObjectDetected* 事件。 如果选中此复选框，则应用程序将记录 *PackedObjectDetected* 事件。 如果清除该复选框，则应用程序不会记录事件。 默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中该复选框，应用程序将仅扫描自上次扫描以来新增的文件或修改的文件。 如果清除该复选框，则无论文件创建或修改日期如何，应用程序都会扫描文件。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用对象扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“**使用启发式分析**”复选框，则可以在下拉列表中选择启发式分析级别： • **轻度**是详细程度最低的扫描，系统负载最小。

- **中度**是中度扫描，系统负载平衡。
- **深度**是最详细的扫描，系统负载最大。
- **推荐**（默认值）是卡巴斯基专家推荐的最优级别。它确保在保护质量和对受保护服务器性能的影响之间达到最优平衡。

“保护范围”窗口

该表包含扫描范围：应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个包括所有共享目录的保护范围。

保护范围设置

设置	Description
范围名称	扫描范围名称。
Path	应用程序扫描的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

“添加保护范围”窗口

在此窗口中，您可以添加和配置保护范围。

保护范围设置

设置	Description
范围名称	用于输入保护范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将在操作期间处理此保护范围。 如果清除此复选框，则应用程序在操作期间不会处理此保护范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	您可以在该下拉列表中选择文件系统的类型： • **本地**（默认值）— 本地目录。如果选择此项，则需要指定本地目录的路径。 • **挂载** – 挂载的远程或本地目录。如果选择此项，则需要指定文件系统的协议或名称。 • **共享** – 可通过 Samba 或 NFS 协议访问的受保护服务器的文件系统资源。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。 • **所有共享** – 可通过 Samba 和 NFS 协议访问的所有受保护服务器的文件系统资源。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**共享**或**挂载**类型，则此下拉列表可用。
Path	用于指定要包括在保护范围中的目录路径的输入字段。您可以使用掩码和标签指定路径。

	您可以使用特殊标签来指定容器或镜像： • [container-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >]/< 本地目录的路径 > • [image-id:< 标识符 >]/< 本地目录的路径 > • [image-name:< 名称 >]/< 本地目录的路径 > 您还可以使用唯一的 [container-id:< 标识符 >]、[container-name:< 名称 >]、[image-id:< 标识符 >] 和 [image-name:< 名称 >]/< 本地目录的路径 > 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • [container-name:< 内存 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [image-name:< 名称 >][image-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-name:< 名称 >][image-id:< 标识符 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > 您可以在名称和标识符中使用掩码（? 和 * 字符）。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下指定 / 路径 – 应用程序扫描本地文件系统的所有目录。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。 如果在文件系统下拉列表中选择**本地**类型选项，并且未指定路径，则应用程序会扫描本地文件系统的所有目录。
共享资源的名称	用于输入要添加到保护范围中的目录所在的文件系统共享资源名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。

掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

文件威胁防护排除项

*保护排除*是一组条件，在这些条件下， Kaspersky Endpoint Security 不会扫描对象以检查病毒和其他恶意软件。您还可以按掩码和威胁名称排除对象，并配置进程排除项。

在 Web Console 中，您可以在策略属性中配置文件威胁防护排除项（**应用程序设置 → 基本威胁防护 → 文件威胁防护排除项**）。

保护排除项设置

设置	描述
排除范围	单击“**配置排除项**”链接将打开“排除范围”窗口。在此窗口中，您可以定义保护排除项列表。
按掩码筛选的排除项	单击“**按掩码配置排除项**”链接将打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称筛选的排除项	单击“**按威胁名称配置排除项**”链接将打开“按威胁名称筛选的排除项”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。
按进程筛选的排除项	单击“**按进程配置排除项**”链接将打开“**按进程筛选的排除项**”窗口。在此窗口中，可以排除进程的活动。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加排除范围”窗口

在此窗口中，您可以添加和配置排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时排除范围。 如果选中该复选框，则应用程序会在其运行期间将此范围排除在扫描或保护之外。 如果清除该复选框，则应用程序在其运行期间将此范围包括在扫描或保护中。您可以在以后选中此复选框来从扫描或保护中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	在此下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型： • **“本地”**，表示本地目录。 • **挂载**，表示设备上挂载的远程目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**挂载**类型，则此下拉列表可用。
Path	要添加到排除范围的目录路径的输入字段。您可以使用掩码和标签指定路径。

	您可以使用特殊标签来指定容器或镜像： • [container-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >]/< 本地目录的路径 > • [image-id:< 标识符 >]/< 本地目录的路径 > • [image-name:< 名称 >]/< 本地目录的路径 > 您还可以使用唯一的 [container-id:< 标识符 >]、[container-name:< 名称 >]、[image-id:< 标识符 >] 和 [image-name:< 名称 >]/< 本地目录的路径 > 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • [container-name:< 内存 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [image-name:< 名称 >][image-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-name:< 名称 >][image-id:< 标识符 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > 您可以在名称和标识符中使用掩码（? 和 * 字符）。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。
共享资源的	用于输入要添加到排除范围中的目录所在的文件系统共享资源名称的字段。

名称	如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在**路径**字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： `*.txt` 掩码表示所有文本文件。 `*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

“按进程筛选的排除项”窗口

该表包含按进程筛选的排除范围。按进程筛选的排除范围允许您从扫描中排除指定进程的活动和指定进程修改的文件。默认情况下，该表包括两个包含网络代理路径的排除范围。如有必要，您可以删除这些排除项。

按进程筛选的排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	排除的进程的完整路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

“受信任进程”窗口

在此窗口中，可以添加和配置按进程筛选的排除范围。

排除范围设置

设置	描述
基于进程的排除项范围名称	用于输入基于进程的排除项范围名称的字段。此名称将显示在“**按进程筛选的排除项**”窗口的表格中。 该输入字段不能为空。
使用/不使用该排除项	该切换开关用于启用或禁用此扫描范围排除项。 默认情况下，复选切换开关处于打开状态。
应用到子进程	排除“**排除的进程的路径**”设置中指示的排除进程的子进程。 默认情况下，清除此复选框。
排除的进程的路径	要从扫描中排除的进程的完整路径。
文件系统，访问协议和路径	该组设置可让您为进程修改的文件设置扫描排除项。 在文件系统下拉列表中，您可以选择要从扫描中排除的目录的文件系统类型： • “**本地**”，表示本地目录。 • **挂载** - 已挂载的目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**已挂载**类型，则**访问协议**下拉列表可用。
路径	在该输入字段中，可以输入要添加到排除范围的目录的路径。您可以使用掩码指定路径。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。
共享资源的名称	用于输入要添加到排除范围中的目录所在的文件系统共享资源名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在"**访问协议**"下拉列表中选择了"**自定义**"项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于"**文件系统，访问协议和路径**"区块中指示的目录中的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击"**删除**"按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开"**对象掩码**"窗口。在此窗口中的"**定义对象掩码**"字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击"**添加**"按钮将打开"**对象掩码**"窗口。在此窗口中的"**定义对象掩码**"字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在管理控制台中配置文件威胁防护

在管理控制台中，您可以在策略属性中管理文件威胁防护（**基本威胁防护 → 文件威胁防护**）。

文件威胁防护组件设置

设置	Description
启用文件威胁防护	此复选框用于启用或禁用所有受管理设备上的文件威胁防护组件。 默认选中该复选框。
文件威胁防护模式	在此下拉列表中，您可以选择文件威胁防护组件模式： • **智能检查**（默认值）— 当有人尝试打开文件时对其进行扫描，如果文件已被修改，则当有人尝试关闭它时再次进行扫描。如果某个进程在特定时间段内多次访问和修改一个文件，则仅当该进程最后一次关闭文件后，应用程序才会再次扫描该文件。 • **打开时** — 在有人尝试打开文件以进行读取、执行或修改时对其进行扫描。 • **打开和修改时** — 在有人尝试打开文件时对其进行扫描，如果文件已被修改，则在尝试关闭文件时再次扫描该文件。
扫描	这组设置包含用于打开窗口的按钮，您可以在这些窗口中配置扫描范围和扫描设置。
检测威胁时的操作	这组设置包含**配置**按钮。单击此按钮将打开“检测到威胁后的操作”窗口，您可以在其中配置应用程序针对检测到的受感染对象执行的操作。

“扫描范围”窗口

该表包含扫描范围：应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。

扫描范围设置

设置	Description
范围名称	扫描范围名称。
Path	应用程序扫描的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“上移”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

<新扫描范围>窗口

在此窗口中，您可以添加和配置扫描范围。

扫描范围设置

设置	Description
扫描范围名称	用于输入扫描范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将处理此扫描范围。 如果清除此复选框，则应用程序不会处理此扫描范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	该设置块可让您设置扫描范围。 您可以在文件系统下拉列表中选择文件系统类型： • **本地**（默认值）— 本地目录。如果选择此项，则需要指定本地目录的路径。 • **挂载** – 挂载的远程或本地目录。如果选择此项，则需要指定文件系统的协议或名称。 • **共享** – 可通过 Samba 或 NFS 协议访问的受保护服务器的文件系统资源。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。 • **所有共享** – 可通过 Samba 和 NFS 协议访问的所有受保护服务器的文件系统资源。
	如果在文件系统下拉列表中选择**共享**或**挂载**，则可以在右侧下拉列表中选择远程访问协议：

- **NFS**：使用 NFS 协议挂载到设备上的远程目录。
- **Samba**：使用 Samba 协议挂载到设备上的远程目录。
- **自定义** — 在下面的字段中指定的设备文件系统的资源。

如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到扫描范围的目录的路径。您可以使用掩码和标签指定路径。

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<标识符>]/<本地目录的路径>`
- `[container-name:<名称>]/<本地目录的路径>`
- `[image-id:<标识符>]/<本地目录的路径>`
- `[image-name:<名称>]/<本地目录的路径>`

您还可以使用唯一的 `[container-id:<标识符>]`、`[container-name:<名称>]`、`[image-id:<标识符>]` 和 `[image-name:<名称>]/<本地目录的路径>` 标签组合。

一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。

例如：

- `[container-name:<内存>][image-name:<名称>]/<本地目录的路径>`
- `[container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`
- `[image-name:<名称>][image-id:<标识符>]/<本地目录的路径>`
- `[container-name:<名称>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`
- `[container-name:<名称>][image-id:<标识符>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

您可以用 `*`（星号）字符来创建文件或目录名称掩码。

您可以指定单个 `*` 字符来表示文件或目录名称中 `/` 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 `*` 字符来表示文件或目录名称中的任意一组字符（包括空集和 `/` 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。

`**` 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

可以使用单个 `?` 字符表示文件名或目录名中的任意一个字符。

	默认情况下指定 **/** 路径 – 应用程序扫描本地文件系统的所有目录。 如果在文件系统下拉列表中选择**本地**类型选项，并且未指定路径，则应用程序会扫描本地文件系统的所有目录。
文件系统名称	用于输入要添加到扫描范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“扫描设置”窗口

在此窗口中，您可以在启用文件威胁防护的同时配置文件扫描设置。

文件威胁防护设置

设置	Description
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中此复选框，则 Kaspersky Endpoint Security 将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过在“**常规扫描设置**”部分中启用和配置“**如果扫描时间超过以下值（秒）则跳过文件**”和“**跳过大于以下大小的文件(MB)**”设置，您可以减少扫描压缩文件的时间。 如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描压缩文件。 默认情况下，清除此复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中此复选框，则 Kaspersky Endpoint Security 将扫描自解压缩文件。 如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描自解压缩文件。 如果清除**扫描压缩文件**复选框，则此复选框可用。 默认情况下，清除此复选框。
扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中此复选框，则 Kaspersky Endpoint Security 将扫描邮件数据库文件。 如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描邮件数据库文件。 默认情况下，清除此复选框。

扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则 Kaspersky Endpoint Security 将扫描纯文本邮件。 如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过文本文件	从扫描中临时排除纯文本格式的文件。 如果选中该复选框，Kaspersky Endpoint Security 不会扫描文本文件，前提是它们在最近一次扫描后 10 分钟内被同一进程重复使用。此设置使优化应用程序日志扫描成为可能。 如果取消选中此复选框，Kaspersky Endpoint Security 将扫描文本文件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，Kaspersky Endpoint Security 将停止扫描该文件。 可用值：0–9999。如果该值设置为 0，则扫描时间不受限制。 默认值：60。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：0–999999。如果该值设置为 0，则 Kaspersky Endpoint Security 将扫描任何大小的文件。 默认值：0。
记录清洁对象	此复选框启用或禁用 *ObjectProcessed* 类型事件的日志记录。 如果选中此复选框，Kaspersky Endpoint Security 会记录所有扫描对象的 *ObjectProcessed* 类型事件。 如果清除此复选框，则 Kaspersky Endpoint Security 不会记录 *ObjectProcessed* 类型事件。 默认情况下，清除此复选框。
记录未处理的对象	此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。 如果选中此复选框，则 Kaspersky Endpoint Security 将记录 *ObjectNotProcessed* 类型事件。 如果清除此复选框，则 Kaspersky Endpoint Security 不会记录 *ObjectNotProcessed* 类型事件。 默认情况下，清除此复选框。
记录打包对象	此复选框为检测到的所有打包对象启用或禁用 *PackedObjectDetected* 类型事件的记录 如果选中此复选框，则 Kaspersky Endpoint Security 将记录 *PackedObjectDetected* 类型事件。 如果清除此复选框，则 Kaspersky Endpoint Security 不会记录 *PackedObjectDetected* 类型事件。 默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中此复选框，则 Kaspersky Endpoint Security 仅扫描自上次文件扫描以来的新文件或修改的文件。 如果清除此复选框，则 Kaspersky Endpoint Security 将扫描所有文件，不管创建日期或修改日期如何。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用文件扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“使用启发式分析”复选框，则可以在下拉列表中选择启发式分析级别：

	• **轻度**是详细程度最低的扫描，系统负载最小。 • **中度**是中度扫描，系统负载平衡。 • **深度**是最详细的扫描，系统负载最大。 • **推荐**（默认值）是卡巴斯基专家推荐的最优级别。它确保了保护质量和对受保护设备性能的影响的最佳组合。

“检测到威胁时的操作”窗口

在此窗口中，您可以配置 Kaspersky Endpoint Security 对于所检测到的受感染对象执行的操作：

文件威胁防护设置

设置	Description
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **阻止**访问对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。 • **阻止**访问对象（默认值）。

文件威胁防护排除项

*保护排除*是一组条件，在这些条件下， Kaspersky Endpoint Security 不会扫描对象以检查病毒和其他恶意软件。您还可以按掩码和威胁名称排除对象，并配置进程排除项。

在管理控制台中，您可以在策略属性中配置文件威胁防护排除项（**基本威胁防护 → 文件威胁防护排除项**）。

扫描排除项设置

设置组	Description
排除项	这组设置包含“**配置**”按钮。单击此按钮将打开“排除范围”窗口。在此窗口中，您可以定

	义要从扫描范围中排除的范围列表。
按掩码筛选的排除项	这组设置包含“**配置**”按钮，用于打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称筛选的排除项	这组设置包含**配置**按钮，用于打开“按威胁名称筛选的排除项”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。
按进程筛选的排除项	这组设置包含“**配置**”按钮，用于打开“**按进程筛选的排除项**”窗口。在此窗口中，可以排除进程的活动。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

<新建扫描范围>窗口

在此窗口中，您可以添加和配置扫描排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从扫描中排除相应范围。 如果选中此复选框，则应用程序在扫描期间将排除此区域。 如果清除此复选框，则应用程序在扫描范围中包含此区域。您可以在以后选中此复选框来排除此范围。 默认选中该复选框。

文件系统，访问协议和路径	该设置块可让您设置排除范围。 在文件系统下拉列表中，您可以选择要从扫描中排除的目录的文件系统类型： • “**本地**”，表示本地目录。 • **挂载** - 已挂载的目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
	如果在文件系统下拉列表中选择**挂载**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。
	如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到排除范围的目录的路径。您可以使用掩码和标签指定路径。 您可以使用特殊标签来指定容器或镜像： • `[container-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>]/<本地目录的路径>` • `[image-id:<标识符>]/<本地目录的路径>` • `[image-name:<名称>]/<本地目录的路径>` 您还可以使用唯一的 `[container-id:<标识符>]`、`[container-name:<名称>]`、`[image-id:<标识符>]` 和 `[image-name:<名称>]/<本地目录的路径>` 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • `[container-name:<内存>][image-name:<名称>]/<本地目录的路径>` • `[container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[image-name:<名称>][image-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[container-name:<名称>][image-id:<标识符>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` 您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
文件系统名称	用于输入要添加到排除范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在路径字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

“按进程筛选的排除项”窗口

该表包含按进程筛选的排除范围。按进程筛选的排除范围允许您从扫描中排除指定进程的活动和指定进程修改的文件。默认情况下，该表包括两个包含网络代理路径的排除范围。如有必要，您可以删除这些排除项。

按进程筛选的排除范围设置

设置	描述

排除范围名称	排除范围名称。
Path	排除的进程的完整路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

还可以单击**高级 -> 导入**将文件中的排除项列表导入，单击**高级 -> 导出所选**或**高级 -> 全部导出**可将所添加的排除项列表导出到文件。

“受信任进程”窗口

在此窗口中，可以添加和配置按进程筛选的排除范围。

按进程筛选的排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在“**按进程筛选的排除项**”窗口的表格中。 该输入字段不能为空。
排除的进程的路径	要从扫描中排除的进程的完整路径。
应用到子进程	排除“**排除的进程的路径**”设置中指示的排除进程的子进程。 默认情况下，清除此复选框。
使用此范围	该复选框用于启用或禁用此排除范围。 如果选中此复选框，则应用程序在扫描期间将排除此区域。 如果清除此复选框，则应用程序在扫描范围中包含此区域。您可以在以后选中此复选框来排除此范围。 默认选中该复选框。
被修改文件的路径	该组设置允许您为进程修改的文件设置扫描排除项。 在文件系统下拉列表中，您可以选择要从扫描中排除的目录的文件系统类型： • “**本地**”，表示本地目录。如果选择此项，则需要指定本地目录的路径。 • **挂载** – 挂载的远程或本地目录。如果选择此项，则需要指定文件系统的协议或名称。 • **共享** – 可通过 Samba 或 NFS 协议访问的受保护服务器的文件系统资源。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。 • **所有共享** – 可通过 Samba 和 NFS 协议访问的所有受保护服务器的文件系统资源。
	如果在文件系统下拉列表中选择**挂载**或**共享**，则可以在访问协议下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。

	• **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。
	如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到排除范围的目录的路径。您可以使用掩码指定路径。该输入字段不能为空。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。 掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。
文件系统名称	用于输入要添加到排除范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于“**被修改文件的路径**”字段中指定的目录中的对象。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： `*.txt` 掩码表示所有文本文件。 `*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在命令行中配置文件威胁防护

在命令行中，您可以使用“文件威胁防护”预定义任务 (*File_Threat_Protection*) 来管理“文件威胁防护”。

默认启动“文件威胁防护”任务。您可以手动启动和停止该任务。

要从命令行启动和停止“文件威胁防护”任务，需要管理员角色权限。

您可以通过编辑“文件威胁防护”预定义任务的设置来配置“文件威胁防护”设置。

“文件威胁防护任务”设置

该表介绍了您可以为文件威胁防护任务指定的所有设置的所有可用值和默认值。

“文件威胁防护任务”设置

设置	描述	
ScanArchived	启用存档扫描（包括 SFX 自解压存档）。 应用程序会扫描以下压缩文件：.zip；.7z *；.7-z；.rar；.iso；.cab；.jar；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支持的压缩文件格式列表取决于所使用的应用程序数据库。	Yes - 扫 FirstA 档类型， 可能删除 No（默
ScanSfxArchived	仅允许扫描自解压存档（包含可执行文件提取模块的存档）。	Yes - 扫 No（默
ScanMailBases	启用对 Microsoft Outlook®、Outlook Express、The Bat 和其他邮件客户端的电子邮件数据库的扫描。	Yes — 扫 No（默 文件。
ScanPlainMail	启用对纯文本电子邮件的扫描。	Yes — 扫 No（默
SkipPlainTextFiles	从扫描中临时排除纯文本格式的文件。 如果此设置的值为 SkipPlainTextFiles=Yes，则应用程序不会扫描文本文件，前提是它们在最近一次扫描后 10 分钟内被同一进程重复使用。此设置使优化应用程序日志扫描成为可能。	Yes — 如 钟内被同 本文件。 No（默
SizeLimit	指定要扫描的对象的最大大小（以 MB 为单位）。如果要扫描的对象大于指定值，应用程序将跳过此对象。	0 – 999 0 — 应用 默认值：
TimeLimit	最长对象扫描持续时间（以秒为单位）。 如果扫描对象所花费的时间超过此设置指定的时间，应用程序将停止扫描对象。	0 – 999 0 — 对象 默认值：
FirstAction	选择应用程序将对受感染对象执行的第一个操作。	Disinf 将其副本 如，如果

		类型）， 第一项操 Second Remove 份副本/ Recomm 序根据对 选择该对 Kaspers 马，因为 中，因此 Block - 感染对象 默认值：
SecondAction	选择应用程序将对受感染对象执行的第二个操作。如果第一项操作失败，则应用程序将执行第二项操作。	Second FirstA 如果选择 作，则无 况下，执 第二项操 第二项操 默认值：
UseExcludeMasks	对 ExcludeMasks.item_# 设置指定的对象启用扫描排除项。	Yes — 从 Exclud No（默 Exclud
ExcludeMasks.item_#	按名称或掩码在扫描中排除对象。 您可以使用此设置来按名称从指定的扫描范围中排除单个文件，或者使用 Shell 格式的掩码一次性排除多个文件。	默认值为 示例： UseE Excl Excl
UseExcludeThreats	对包含 ExcludeThreats.item_# 设置指定的威胁的对象启用扫描排除项。	Yes — 从 Exclud 的对象。 No（默 Exclud 的对象。
ExcludeThreats.item_#	按对象中检测到的威胁的名称从扫描中排除对象。在为此设置指定值之前，请确保已启用 UseExcludeThreats 设置。 要从扫描中排除对象，请指定在该对象中检测到的威胁的全名 – 包含应用程序确定已感染的对象的字符串。 例如，您可能正在使用实用程序来收集有关您的网络的信息。要防止应用程序对其进行阻止，请将其中包含的威胁的全名添加到排除在扫描范围之外的威胁列表中。 您可以在应用程序日志中或在网站 https://threats.kaspersky.com 上找到在对象中检测到的威胁的全名。	该设置仅 默认值为 示例： UseE Excl Test Excl roja
ReportCleanObjects	允许记录有关应用程序报告为未受感染的扫描对象的信息。	Yes — 记

	例如，您可以启用此设置，以确保应用程序已扫描了特定对象。	No（默 信息。
ReportPackedObjects	启用记录作为复合对象一部分的已扫描对象的有关信息。 例如，您可以启用此设置，以确保应用程序已扫描压缩文件中的某个对象。	Yes — No（默 对象的
ReportUnprocessedObjects	启用记录由于某种原因尚未处理的对象的有关信息。	Yes — No（默 息。
UseAnalyzer	启用启发式分析。 启发式分析可帮助应用程序检测威胁，甚至在病毒分析人员尚未意识到威胁之前。	Yes（ No — 禁
HeuristicLevel	指定启发式分析级别。 启发式分析级别在威胁搜索的全面性、操作系统资源的负载以及扫描持续时间之间建立平衡。启发式分析级别越高，扫描所需的资源和时间就越多。	Light Medium 负载均 Deep — 大。 Recomm
UseIChecker	启用 iChecker 技术。	Yes（ No — 禁
ScanByAccessType	文件威胁防护任务操作模式。ScanByAccessType 设置只适用于文件威胁防护任务。	SmartC 文件时 则在尝 某个进 对其进 该对象 OpenAn 其进行 关闭文 Open - 执行或
[ScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描范围的说明，其中包含有关扫描范围的其他信息。 使用此设置指定的字符串的最大长度为 4096 个字符。	默认值： 示例： Area
UseScanArea	启用指定范围的扫描。要运行任务，请启用至少一个范围的扫描。	Yes（ No — 不
AreaMask.item_#	扫描范围限制。通过此扫描范围，应用程序仅扫描使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序会扫描位于扫描范围内的所有对象。您可以为此设置指定多个值。	默认值： 示例： Area
路径	包含要扫描的对象的目录的路径。	< 本地 象。您

您可
像：

- [
  地
- [
  地
- [
  录
- [
  录

您还
< 标
称 >]
[ima
路径

一个
的任

例如：

- [
  [
  录
- [
  [
  录
- [
  ic
- [
  [
  [
  录
- [
  [
  [
  [
  录

您可
和 *

		您可 目录 您可 录名 （包 或 /d 您可 件或 空集 如： /dir ** 掩 例如， 掩码。 可以 名中 Shared 设备文 Shared 的设备 Mounte 设备上 Mounte 到设备 AllRem NFS 协 AllSha 访问的 < 文件 的所有
[ExcludedFromScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描排除范围的说明，其中包含有关扫描排除范围的其他信息。	默认值
UseScanArea	从扫描中排除指定的范围。	Yes（默 No – 不
AreaMask.item_#	扫描排除范围的限制。在排除范围中，应用程序仅从扫描中排除使用 shell 格式的掩码指定的文件。 如果不指定此设置，应用程序不会扫描排除范围内的任何对象。您可以为此设置指定多个值。	默认值：
路径	包含要排除的对象的目录的路径。	< 本地 录（包 码和标

您可
像：

- [
  地
- [
  地
- [
  录
- [
  录

您还
< 标
称 >]
[ima
路径

一个
的任

例如：

- [
  [
  录
- [
  [
  录
- [
  ic
- [
  [
  [
  录
- [
  [
  [
  [
  录

您可
和 *

		您可 目录 您可 录名 （包 或 /d 您可 件或 空集 如： /dir ** 掩 例如， 掩码。 可以 名中 Mounte 议在设 Mounte 议在设 AllRem SMB 和 目录。 <文件系 文件系
[ExcludedForProgram.item_#] 部分包含以下设置：		
ProgramPath	排除的进程的路径。	<进程 中的进
ApplyToDescendants	从扫描中排除 ProgramPath 设置指定的排除进程的子进程。	Yes – 从 进程。 No（默 不排除
AreaDesc	进程排除范围的说明。	默认值：
UseExcludedForProgram	从扫描中排除指定的范围。	Yes（默 No – 不
AreaMask.item_#	进程排除范围的限制。在进程排除范围中，应用程序仅从扫描中排除使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序将从扫描中排除进程排除范围内的所有对象。您可以为此设置指定多个值。	默认值：
路径	包含由进程修改的文件的目录的路径。	<本地 录中的

		您可 目录 您可 录名 （包 或 /d 您可 件或 空集 如： /dir ** 掩 例如， 掩码。 可以 名中 Shared 议访问 Shared 协议访 Mounte 议在设 Mounte 议在设 AllRem SMB 和 目录。 AllSha NFS 协 < 文件 文件系

优化网络目录扫描

要优化“文件威胁防护”任务，您可以从扫描中排除从网络目录复制到本地目录中的任何文件。为此，请根据用于从网络目录复制的实用程序（例如 cp 实用程序）的进程配置排除项。

要配置从扫描中排除网络目录：

1. 使用以下命令将“文件威胁防护”任务设置（*File_Threat_Protection，ID：1*）输出到配置文件：

   `kesl-control --get-settings 1 --file <配置文件的完整路径> [--json]`

2. 打开配置文件并添加 `[ExcludedForProgram.item_ #]` 部分，设置如下：

   - `ProgramPath` – 要排除的进程或包含要排除的进程的目录的路径。

- `ApplyToDescendants` 参数指示扫描是否应该排除已排除进程的子进程（可能的值：`Yes` 或 `No`）。
- `AreaDesc` – 进程排除范围的说明，其中包含有关扫描排除范围的其他信息。
- `UseExcludedForProgram` 允许在任务运行期间排除指定范围（可能的值：`Yes` 或 `No`）。
- `Path` – 文件或包含进程修改的文件的目录的路径。
- `AreaMask.item_#` – 要从扫描范围排除的文件的文件名掩码。您还可以指定文件的完整路径。

```
示例：
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/cp
ApplyToDescendants=No
AreaDesc=
UseExcludedForProgram=Yes
Path=AllRemoteMounted
AreaMask.item_0000=*
```

3. 执行命令：

   `kesl-control --set-settings 1 --file <配置文件的完整路径> [--json]`

   如果要以 JSON 格式从配置文件导入设置，请指定 `--json` 键。如果不指定此键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

应用程序不会扫描网络目录中的文件，但会扫描 `cp` 命令本身（对于上面给出的示例）和本地文件。

扫描符号链接和硬链接的特殊注意事项

Kaspersky Endpoint Security 可以扫描文件符号链接和硬链接。

扫描符号链接

仅当由符号链接引用的文件在文件威胁防护组件的扫描范围内时，应用程序才会扫描符号链接。

如果符号链接引用的文件不在文件威胁防护组件的扫描范围内，则应用程序不会扫描此文件。但是，如果文件包含恶意代码，则设备的安全性将受到威胁。

扫描硬链接

当处理具有多个硬链接的文件时，应用程序根据对对象的指定操作选择操作：

- 如果选择了**执行推荐的操作**选项，则应用程序会根据在对象中检测到的威胁的危险程度以及清除该威胁的可能性的有关数据，针对该对象自动选择并执行操作。
- 如果选择了**移除**操作，则应用程序会移除正在处理的硬链接。将不会处理此文件的其余硬链接。
- 如果选择了 **Disinfect** 操作，则应用程序将清除原始文件。如果清除失败，则应用程序将删除该硬链接并使用已删除硬链接的名称在其原位置创建原始文件的副本。

从备份存储中恢复带有硬链接的文件时，应用程序将使用已被移动到备份存储中的硬链接的名称创建源文件的副本。将不会恢复与源文件其他硬链接的连接。

恶意软件扫描

*恶意软件扫描*是根据需要对设备上的文件执行一次性全盘扫描或自定义扫描。Kaspersky Endpoint Security 可以同时执行多个"恶意软件扫描"任务。

在应用程序中创建"*恶意软件扫描 (Scan_My_Computer)*"预定义任务。您可以使用此任务对设备执行全盘扫描。在全盘扫描期间，应用程序会使用推荐的安全设置扫描位于设备本地驱动器上的所有对象，以及通过 Samba 或 NFS 协议访问的所有已挂载和共享的对象。

在 Kaspersky Security Center 中，安装 MMC 管理插件或 Kaspersky Endpoint Security Web 管理插件后，Kaspersky Security Center 初始设置向导会自动创建"恶意软件扫描"组任务。

在全盘扫描期间，处理器处于忙碌状态。建议业务闲时进行扫描。

您可以在 Kaspersky Security Center 和命令行中配置自动创建任务的设置，还可以创建"恶意软件扫描"用户任务。

检测到恶意软件后，Kaspersky Endpoint Security 可能会移除受感染的文件并终止从该文件启动的恶意软件进程。

如果在执行恶意软件扫描任务期间，应用程序被控制服务或用户手动重新启动，任务将被停止。应用程序会记录 *OnDemandTaskInterrupted* 事件。

您可以运行"恶意软件扫描"任务并配置扫描设置：

- 选择要扫描的操作系统对象：文件、压缩文件、引导扇区、进程内存和内核内存、启动对象。
- 限制要扫描的对象的大小以及对象扫描的持续时间。
- 选择应用程序将对感染对象执行的操作。
- 配置从扫描范围中排除的对象：
  - 按名称或掩码进行排除
  - 按对象中检测到的威胁名称进行排除
- 扫描时启用或禁用全局排除和文件威胁防护排除。
- 启用有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息记录。
- 配置扫描期间启发式分析器和 iChecker 技术的使用。
- 限制需要扫描其引导扇区的设备集。
- 配置扫描范围和扫描排除范围。

Web Console 中的恶意软件扫描

在 Web Console 中，您可以使用"*恶意软件扫描*"任务来扫描恶意软件。

您可以运行自动创建的组任务进行扫描，也可以创建并运行用户任务以进行扫描。您可以通过编辑"恶意软件扫描"任务的设置来配置扫描设置。

恶意软件扫描任务设置

设置	Description
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中该复选框，应用程序将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过在"**常规扫描设置**"部分中配置"**如果扫描时间超过以下值（秒）则跳过文件**"和"**跳过大于以下大小的文件(MB)**"设置，您可以减少扫描压缩文件的时间。 如果清除该复选框，应用程序不会扫描压缩文件。 默认选中该复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中该复选框，应用程序将扫描自解压存档。 如果清除了该复选框，则应用程序不会扫描自解压存档。 如果清除**扫描压缩文件**复选框，则此复选框可用。 默认选中该复选框。
扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中该复选框，应用程序将扫描邮件数据库文件。 如果清除了该复选框，则应用程序不会扫描邮件数据库文件。 默认情况下，清除此复选框。
扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则应用程序将扫描纯文本邮件。 如果清除此复选框，则应用程序不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，应用程序将停止扫描该文件。 可用值：0–9999。如果该值设置为 0，则扫描时间不受限制。 默认值：0。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：0–999999。如果该值设置为 0，则应用程序将扫描任何大小的文件。 默认值：0。
记录清洁对象	此复选框启用或禁用 *ObjectProcessed* 类型事件的日志记录。 如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 类型的事件。 如果清除此复选框，则应用程序不会记录任何已扫描对象的 *ObjectProcessed* 类型的事件。 默认情况下，清除此复选框。
记录未处理的对象	此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。 如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。 如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。 默认情况下，清除此复选框。
记录打包对	此复选框为检测到的所有打包对象启用或禁用 *PackedObjectDetected* 类型事件的记录。

象	如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。 如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。 默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中该复选框，应用程序将仅扫描自上次扫描以来新增的文件或修改的文件。 如果清除该复选框，则无论文件创建或修改日期如何，应用程序都会扫描文件。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用文件扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“**使用启发式分析**”复选框，则可以在下拉列表中选择启发式分析级别： • **轻度**是详细程度最低的扫描，系统负载最小。 • **中度**是中度扫描，系统负载平衡。 • **深度**是最详细的扫描，系统负载最大。 • **推荐**（默认值）是卡巴斯基专家推荐的最优级别。它确保了保护质量和对受保护设备性能的影响的最佳组合。
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **跳过**对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。 • **跳过**对象（默认值）。
扫描范围	包含任务扫描的范围的表。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。 您可以在表中添加、配置、删除、上移或下移扫描范围。

单击“**下移**”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

单击扫描范围名称将打开“**<扫描范围名称>**”窗口。在此窗口中，可以修改所选扫描范围的设置。

点击“**添加**”按钮将打开“**<新建扫描范围>**”窗口。在此窗口中，可以定义新的扫描范围。

“添加扫描范围”窗口

在此窗口中，您可以添加和配置扫描范围。

扫描范围设置

设置	Description
范围名称	用于输入扫描范围名称的字段。此名称将显示在“**扫描设置**”部分的**扫描范围**表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将处理此扫描范围。 如果清除此复选框，则应用程序不会处理此扫描范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	您可以在该下拉列表中选择文件系统的类型： • **本地**（默认值）— 本地目录。如果选择此项，则需要指定本地目录的路径。 • **挂载** – 挂载的远程或本地目录。如果选择此项，则需要指定文件系统的协议或名称。

	• **共享** – 可通过 Samba 或 NFS 协议访问的受保护服务器的文件系统资源。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。 • **所有共享** – 可通过 Samba 和 NFS 协议访问的所有受保护服务器的文件系统资源。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**共享**或**挂载**类型，则此下拉列表可用。
Path	这是用于指定要包括在扫描范围中的目录路径的输入字段。您可以使用掩码和标签指定路径。 您可以使用特殊标签来指定容器或镜像： • `[container-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>]/<本地目录的路径>` • `[image-id:<标识符>]/<本地目录的路径>` • `[image-name:<名称>]/<本地目录的路径>` 您还可以使用唯一的 `[container-id:<标识符>]`、`[container-name:<名称>]`、`[image-id:<标识符>]` 和 `[image-name:<名称>]/<本地目录的路径>` 标签组合。 一个区域内允许使用1到4个唯一标签的任意组合。标签的排列顺序不重要。 例如： • `[container-name:<内存>][image-name:<名称>]/<本地目录的路径>` • `[container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[image-name:<名称>][image-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[container-name:<名称>][image-id:<标识符>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` 您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下指定 / 路径 — 应用程序扫描本地文件系统的所有目录。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。 如果在文件系统下拉列表中选择**本地**类型选项，并且未指定路径，则应用程序会扫描本地文件系统的所有目录。
共享资源的名称	用于输入要添加到扫描范围中的目录所在的文件系统共享资源名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。
掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“扫描范围”部分

您可以为恶意软件扫描任务配置扫描范围设置。应用程序允许您扫描文件、引导扇区、客户端设备内存和启动对象。

恶意软件扫描范围任务设置

设置	Description
扫描文件	此复选框启用或禁用文件扫描。 如果选中该复选框，应用程序将扫描文件。 如果清除了该复选框，则应用程序不会扫描文件。 默认选中该复选框。
扫描启动扇区	此复选框启用或禁用引导扇区扫描。

	如果选中该复选框，应用程序将扫描引导扇区。 如果清除该复选框，则应用程序不扫描引导扇区。 默认情况下，清除此复选框。
扫描内核内存和正在运行的进程	此复选框启用或禁用客户端设备内存扫描。 如果选中该复选框，应用程序将扫描内核内存和正在运行的进程。 如果清除该复选框，应用程序不会扫描内核内存和正在运行的进程。 默认情况下，清除此复选框。
扫描启动对象	此复选框启用或禁用启动对象扫描。 如果选中该复选框，应用程序将扫描启动对象。 如果清除了该复选框，则应用程序不会扫描启动对象。 默认情况下，清除此复选框。
要扫描的设备	单击“**配置设备掩码**”链接将打开“**扫描范围**”窗口，您可以在其中指定必须扫描其引导扇区的设备。

“扫描范围”窗口

该表包含应用程序必须扫描其引导扇区的设备的名称掩码。默认情况下，该表包含 **/**** 设备名称掩码（所有设备）。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”部分

在恶意软件扫描任务的**排除范围**部分，您可以配置排除范围、按掩码和威胁名称排除，以及在任务运行时全局排除和文件威胁防护排除的使用。

扫描排除项设置

设置	描述
配置排除项范围	单击“**配置排除项**”链接将打开“排除范围”窗口。在此窗口中，您可以定义扫描排除项列表。
按掩码配置排除项	单击“**按掩码配置排除项**”链接将打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称配	单击“**按威胁名称配置排除项**”链接将打开“按威胁名称筛选的排除项”窗口。在此窗口

置排除项	中，您可以根据威胁名称配置在扫描中排除对象。
使用全局排除项	该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。 如果选中此复选框，则应用程序将从扫描中排除配置的挂载点。 默认选中该复选框。
使用文件威胁防护排除项	此复选框可启用或禁用应用程序运行时使用配置的文件威胁防护排除。 如果选中该复选框，应用程序将不会扫描文件威胁防护组件的排除项中指定的对象。 默认选中该复选框。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加排除范围”窗口

在此窗口中，您可以添加和配置排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时排除范围。 如果选中该复选框，则应用程序会在其运行期间将此范围排除在扫描或保护之外。 如果清除该复选框，则应用程序在其运行期间将此范围包括在扫描或保护中。您可以在以后选中此复选框来从扫描或保护中排除此范围。

	默认选中该复选框。
文件系统，访问协议和路径	在此下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型： • “**本地**”，表示本地目录。 • **挂载**，表示设备上挂载的远程目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**挂载**类型，则此下拉列表可用。
Path	要添加到排除范围的目录路径的输入字段。您可以使用掩码和标签指定路径。 您可以使用特殊标签来指定容器或镜像： • `[container-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>]/<本地目录的路径>` • `[image-id:<标识符>]/<本地目录的路径>` • `[image-name:<名称>]/<本地目录的路径>` 您还可以使用唯一的 `[container-id:<标识符>]`、`[container-name:<名称>]`、`[image-id:<标识符>]` 和 `[image-name:<名称>]/<本地目录的路径>` 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • `[container-name:<内存>][image-name:<名称>]/<本地目录的路径>` • `[container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[image-name:<名称>][image-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[container-name:<名称>][image-id:<标识符>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` 您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。
共享资源的名称	用于输入要添加到排除范围中的目录所在的文件系统共享资源名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在**路径**字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

管理控制台中的恶意软件扫描

在管理控制台中，您可以使用“*恶意软件扫描*”任务扫描恶意软件。

您可以运行自动创建的组任务进行扫描，也可以创建并运行用户任务以进行扫描。您可以通过编辑“恶意软件扫描”任务的设置来配置扫描设置。

在恶意软件扫描任务属性的**设置**部分中，您可以配置下表列出的设置。

恶意软件扫描任务设置

设置	Description
扫描	这组设置包含用于打开窗口的按钮，您可以在其中配置扫描范围、扫描范围设置和扫描设置。
检测威胁时的操作	这组设置包含**配置**按钮。单击此按钮将打开“检测到威胁后的操作”窗口，您可以在其中配置应用程序针对检测到的受感染对象执行的操作。

在恶意软件扫描任务属性的排除项 部分，您还可以按掩码和威胁名称配置排除范围或排除项。

“扫描范围”窗口

该表包含扫描范围：应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。

扫描范围设置

设置	Description
范围名称	扫描范围名称。
Path	应用程序扫描的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

<新扫描范围>窗口

在此窗口中，您可以添加和配置扫描范围。

扫描范围设置

设置	Description
扫描范围名称	用于输入扫描范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将处理此扫描范围。 如果清除此复选框，则应用程序不会处理此扫描范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	该设置块可让您设置扫描范围。 您可以在文件系统下拉列表中选择文件系统类型： • **本地**（默认值）— 本地目录。如果选择此项，则需要指定本地目录的路径。 • **挂载** – 挂载的远程或本地目录。如果选择此项，则需要指定文件系统的协议或名称。 • **共享** – 可通过 Samba 或 NFS 协议访问的受保护服务器的文件系统资源。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。 • **所有共享** – 可通过 Samba 和 NFS 协议访问的所有受保护服务器的文件系统资源。
	如果在文件系统下拉列表中选择**共享**或**挂载**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。
	如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到扫描范围的目录的路径。您可以使用掩码和标签指定路径。

	您可以使用特殊标签来指定容器或镜像： • [container-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >]/< 本地目录的路径 > • [image-id:< 标识符 >]/< 本地目录的路径 > • [image-name:< 名称 >]/< 本地目录的路径 > 您还可以使用唯一的 [container-id:< 标识符 >]、[container-name:< 名称 >]、[image-id:< 标识符 >] 和 [image-name:< 名称 >]/< 本地目录的路径 > 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • [container-name:< 内存 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [image-name:< 名称 >][image-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-name:< 名称 >][image-id:< 标识符 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > 您可以在名称和标识符中使用掩码（? 和 * 字符）。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下指定 / 路径 – 应用程序扫描本地文件系统的所有目录。 如果在文件系统下拉列表中选择**本地**类型选项，并且未指定路径，则应用程序会扫描本地文件系统的所有目录。
文件系统名称	用于输入要添加到扫描范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序扫描的对象的名称掩码。

默认情况下，该列表包含 * 掩码（所有对象）。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“扫描范围设置”窗口

在此窗口中，您可以配置恶意软件扫描任务的扫描设置。应用程序可让您扫描文件、引导扇区、设备内存和启动对象。

扫描范围设置

设置	Description
扫描文件	此复选框启用或禁用文件扫描。 如果选中该复选框，应用程序将扫描文件。 如果清除了该复选框，则应用程序不会扫描文件。 默认选中该复选框。
扫描启动扇区	此复选框启用或禁用引导扇区扫描。 如果选中该复选框，应用程序将扫描引导扇区。 如果清除该复选框，则应用程序不扫描引导扇区。 默认情况下，清除此复选框。
扫描内核内存和正在运行的进程	此复选框启用或禁用设备内存扫描。 如果选中该复选框，应用程序将扫描内核内存和正在运行的进程。 如果清除该复选框，应用程序不会扫描内核和正在运行的进程。 默认情况下，清除此复选框。
扫描启动对象	此复选框启用或禁用启动对象扫描。 如果选中该复选框，应用程序将扫描启动对象。 如果清除了该复选框，则应用程序不会扫描启动对象。 默认情况下，清除此复选框。
要扫描的设备	这组设置包含**配置**按钮。单击此按钮将打开“扫描范围”窗口，您可以在其中指定必须扫描其引导扇区的设备。
使用全局排除项	该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。 如果选中此复选框，则应用程序将从扫描中排除配置的挂载点。 默认选中该复选框。
使用文件威胁防护排除项	此复选框可启用或禁用应用程序运行时使用配置的文件威胁防护排除。

	如果选中该复选框，应用程序将不会扫描文件威胁防护组件的排除项中指定的对象。 默认选中该复选框。

“扫描范围”窗口

该表包含应用程序必须扫描其引导扇区的设备的名称掩码。默认情况下，该表包含 **/**** 设备名称掩码（所有设备）。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“扫描设置”窗口

在此窗口中，您可以配置任务的文件扫描设置。

扫描设置

设置	Description
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中该复选框，应用程序将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过在“**常规扫描设置**”部分中配置“**如果扫描时间超过以下值（秒）则跳过文件**”和“**跳过大于以下大小的文件 (MB)**”设置，您可以减少扫描压缩文件的时间。 如果清除该复选框，应用程序不会扫描压缩文件。 默认选中该复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中该复选框，应用程序将扫描自解压存档。 如果清除了该复选框，则应用程序不会扫描自解压存档。 如果清除**扫描压缩文件**复选框，则此复选框可用。 默认选中该复选框。
扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中该复选框，应用程序将扫描邮件数据库文件。 如果清除了该复选框，则应用程序不会扫描邮件数据库文件。 默认情况下，清除此复选框。

扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则应用程序将扫描纯文本邮件。 如果清除此复选框，则应用程序不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，应用程序将停止扫描该文件。 可用值：0–9999。如果该值设置为 0，则扫描时间不受限制。 默认值：0。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：0–999999。如果该值设置为 0，则应用程序将扫描任何大小的文件。 默认值：0。
记录清洁对象	此复选框启用或禁用 *ObjectProcessed* 类型事件的日志记录。 如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 类型的事件。 如果清除此复选框，则应用程序不会记录任何已扫描对象的 *ObjectProcessed* 类型的事件。 默认情况下，清除此复选框。
记录未处理的对象	此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。 如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。 如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。 默认情况下，清除此复选框。
记录打包对象	此复选框为检测到的所有打包对象启用或禁用 *PackedObjectDetected* 类型事件的记录。 如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。 如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。 默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中该复选框，应用程序将仅扫描自上次扫描以来新增的文件或修改的文件。 如果清除该复选框，则无论文件创建或修改日期如何，应用程序都会扫描文件。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用文件扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“**使用启发式分析**”复选框，则可以在下拉列表中选择启发式分析级别： • **轻度**是详细程度最低的扫描，系统负载最小。 • **中度**是中度扫描，系统负载平衡。 • **深度**是最详细的扫描，系统负载最大。 • **推荐**（默认值）是卡巴斯基专家推荐的最优级别。它确保了保护质量和对受保护设备性能的影响的最佳组合。

“检测到威胁时的操作”窗口

在此窗口中，您可以配置 Kaspersky Endpoint Security 对于所检测到的受感染对象执行的操作：

检测到威胁后的操作

设置	Description
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **跳过**对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。 • **跳过**对象（默认值）。

“排除项”部分

*扫描排除项*是一组条件。当满足这些条件时，Kaspersky Endpoint Security 不会扫描对象中是否存在病毒和其他恶意软件。您还可以按掩码和威胁名称排除扫描对象。

扫描排除项设置

设置组	Description
排除范围	这组设置包含**配置**按钮。单击此按钮将打开“**排除范围**”窗口。在此窗口中，您可以定义要从扫描范围中排除的范围列表。
按掩码筛选的排除项	这组设置包含“**配置**”按钮，用于打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称筛选的排除项	这组设置包含**配置**按钮，用于打开“按威胁名称筛选的排除项”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

<新建扫描范围>窗口

在此窗口中，您可以添加和配置扫描排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从扫描中排除相应范围。 如果选中此复选框，则应用程序在扫描期间将排除此区域。 如果清除此复选框，则应用程序在扫描范围中包含此区域。您可以在以后选中此复选框来排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	该设置块可让您设置排除范围。 在文件系统下拉列表中，您可以选择要从扫描中排除的目录的文件系统类型： • “**本地**”，表示本地目录。 • **挂载** - 已挂载的目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
	如果在文件系统下拉列表中选择**挂载**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。

如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到排除范围的目录的路径。您可以使用掩码和标签指定路径。

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<标识符>]/<本地目录的路径>`
- `[container-name:<名称>]/<本地目录的路径>`
- `[image-id:<标识符>]/<本地目录的路径>`
- `[image-name:<名称>]/<本地目录的路径>`

您还可以使用唯一的 `[container-id:<标识符>]`、`[container-name:<名称>]`、`[image-id:<标识符>]` 和 `[image-name:<名称>]/<本地目录的路径>` 标签组合。

一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。

例如：

- `[container-name:<内存>][image-name:<名称>]/<本地目录的路径>`
- `[container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`
- `[image-name:<名称>][image-id:<标识符>]/<本地目录的路径>`
- `[container-name:<名称>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`
- `[container-name:<名称>][image-id:<标识符>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

您可以用 `*`（星号）字符来创建文件或目录名称掩码。

您可以指定单个 `*` 字符来表示文件或目录名称中 `/` 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 `*` 字符来表示文件或目录名称中的任意一组字符（包括空集和 `/` 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。

`**` 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。

掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。

可以使用单个 `?` 字符表示文件名或目录名中的任意一个字符。

	默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
文件系统名称	用于输入要添加到排除范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在路径字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

在命令行中扫描恶意软件

在命令行上，您可以通过以下方式扫描恶意软件：

- 使用“恶意软件扫描”预定义任务 (*Scan_My_Computer*)。您可以手动启动、停止、暂停或恢复此任务并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。
- 使用“恶意软件扫描”用户任务（*ODS* 类型的任务）。您可以手动启动、停止、暂停或恢复用户任务，并配置任务计划。
- 使用命令 `kesl-control --scan-file` ，您可以对指定的文件和目录执行*自定义扫描*。

“恶意软件扫描”预定义任务设置

该表介绍了可为恶意软件扫描任务指定的所有设置的全部可用值以及默认值。

恶意软件扫描任务设置

设置	描述	

ScanFiles	启用文件扫描。	Yes（默 No — 不
ScanBootSectors	启用引导扇区扫描。	Yes（默 No — 不
ScanComputerMemory	启用进程内存和内核内存扫描。	Yes（默 存。 No — 不
ScanStartupObjects	启用启动对象扫描。	Yes（默 No — 不
ScanArchived	启用存档扫描（包括 SFX 自解压存档）。 应用程序会扫描以下压缩文件：.zip；.7z *；.7-z；.rar；.iso；.cab；.jar；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支持的压缩文件格式列表取决于所使用的应用程序数据库。	Yes（默 了 Firs 据存档 象，也 No - 不
ScanSfxArchived	仅允许扫描自解压存档（包含可执行文件提取模块的存档）。	Yes（默 No - 不
ScanMailBases	启用对 Microsoft Outlook、Outlook Express、The Bat 和其他邮件客户端的电子邮件数据库的扫描。	Yes — No（默 文件。
ScanPlainMail	启用对纯文本电子邮件的扫描。	Yes — No（默
SizeLimit	指定要扫描的对象的最大大小（以 MB 为单位）。如果要扫描的对象大于指定值，应用程序将跳过此对象。	0 – 999 0 — 应 默认值：
TimeLimit	最长对象扫描持续时间（以秒为单位）。如果扫描对象所花费的时间超过此设置指定的时间，应用程序将停止扫描对象。	0 – 999 0 — 对 默认值：
FirstAction	选择应用程序将对受感染对象执行的第一个操作。	Disinf 将其副 如，如 类型）， 第一项 Second Remove 份副本 Recomm 序根据 选择该 Kaspers 马，因 中，因 Skip — 染的对 默认值：
SecondAction	选择应用程序将对受感染对象执行的第二个操作。如果第一项操	Second

	作失败，则应用程序将执行第二项操作。	FirstA 如果选 作，则 况下， 第二项 二项操 默认值：
UseExcludeMasks	对 ExcludeMasks.item_# 设置指定的对象启用扫描排除项。	Yes — Exclud No（默 Exclud
ExcludeMasks.item_#	按名称或掩码在扫描中排除对象。您可以使用此设置来按名称从指定的扫描范围中排除单个文件，或者使用 Shell 格式的掩码一次性排除多个文件。 在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。	默认值 示例： UseE Excl Excl
UseExcludeThreats	对包含 ExcludeThreats.item_# 设置指定的威胁的对象启用扫描排除项。	Yes — Exclud 的对象。 No（默 Exclud 的对象。
ExcludeThreats.item_#	按对象中检测到的威胁的名称从扫描中排除对象。在为此设置指定值之前，请确保已启用 UseExcludeThreats 设置。 要从扫描中排除对象，请指定在该对象中检测到的威胁的全名 – 包含应用程序确定已感染的对象的字符串。 例如，您可能正在使用实用程序来收集有关您的网络的信息。要防止应用程序对其进行阻止，请将其中包含的威胁的全名添加到排除在扫描范围之外的威胁列表中。 您可以在应用程序日志中或在网站 https://threats.kaspersky.com 上找到在对象中检测到的威胁的全名。	该设置 默认值 示例： UseE Excl Test Excl roja
UseGlobalExclusions	针对扫描启用全局排除项。	Yes（默 No — 不
UseOASExclusions	针对扫描启用文件威胁防护排除项。	Yes（默 项。 No — 不
ReportCleanObjects	允许记录有关应用程序报告为未受感染的扫描对象的信息。 例如，您可以启用此设置，以确保应用程序已扫描了特定对象。	Yes — No（默 信息。
ReportPackedObjects	启用记录作为复合对象一部分的已扫描对象的有关信息。 例如，您可以启用此设置，以确保应用程序已扫描压缩文件中的某个对象。	Yes — No（默 对象的
ReportUnprocessedObjects	启用记录由于某种原因尚未处理的对象的有关信息。	Yes —

		No（默 息。
UseAnalyzer	启用启发式分析。 启发式分析可帮助应用程序检测威胁，甚至在病毒分析人员尚未意识到威胁之前。	Yes（ No — 禁
HeuristicLevel	指定启发式分析级别。 您可以指定启发式分析级别。启发式分析级别在威胁搜索的全面性、操作系统资源的负载以及扫描持续时间之间建立平衡。启发式分析级别越高，扫描所需的资源和时间就越多。	Light Medium 负载均 Deep — 大。 Recomm
UseIChecker	启用 iChecker 技术。	Yes（ No — 禁
DeviceNameMasks.item_#	设备名称列表。应用程序将扫描这些设备的引导扇区。 设置值不能为空。必须至少指定一个设备名掩码才能运行此任务。	AllObj < 设备名 匹配的 默认值： 符，包
[ScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描范围的说明，其中包含有关扫描范围的其他信息。使用此设置指定的字符串的最大长度为 4096 个字符。	默认值： 示例： Area
UseScanArea	启用指定范围的扫描。要运行任务，请启用至少一个范围的扫描。	Yes（ No — 不
AreaMask.item_#	扫描范围限制。在扫描范围内，应用程序仅扫描使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序会扫描位于扫描范围内的所有对象。您可以为此设置指定多个值。	默认值： 示例： Area
路径	包含要扫描的对象的目录的路径。	< 本地 象。 Shared 设备文 Shared 的设备 Mounte 设备上 Mounte 到设备 AllRem NFS 协 AllSha 访问的

		< 文件系 的所有
[ExcludedFromScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描排除范围的说明，其中包含有关扫描排除范围的其他信息。	默认值
UseScanArea	从扫描中排除指定的范围。	Yes（ No — 不
AreaMask.item_#	扫描排除范围的限制。在排除范围中，应用程序仅排除使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序将排除位于排除范围内的所有对象。您可以为此设置指定多个值。	默认值：
路径	包含要排除的对象的目录的路径。	< 本地目 录（包括 码指定路 您可以 目录名 您可以 录名称 （包括 或 /d 您可以 件或目 空集来 如：/ /dir ** 掩 例如， 掩码。 可以使 名中的 为了优化 文件系统 系统以及 除项中。 的系统， 项：/. Mounte 议在设备 Mounte 议在设备 AllRem SMB 和 目录。 < 文件系 文件系统

		仅当 应用 务启 扫描

文件和目录的自定义扫描

您可以使用命令 `kesl-control --scan-file` 对指定的文件和目录执行自定义扫描。

使用预定义任务 *Scan_File*（ID：3）中存储的设置执行自定义扫描。您可以通过编辑该任务的设置来配置文件自定义扫描的设置（见下表）。

如要启动对指定文件和目录的自定义扫描，请执行以下命令：

```
kesl-control --scan-file <路径> [--action <操作>]
```

其中：

- <路径> 是要扫描的文件或目录的路径。您可以指定多个路径，用空格分隔。
- `--action` <操作> 是应用程序将对受感染对象执行的操作。如果您未指定 `--action` 键，应用程序将执行推荐的操作。

执行该命令后，会创建一个临时的文件扫描任务，完成后自动删除。在这种情况下，扫描结果将输出到控制台。

该表介绍了可为 *Scan_File* 任务指定的所有设置的全部可用值和默认值。

执行自定义扫描时，不考虑 *Scan_File* 任务中定义的 `[ScanScope.item_ #]` 和 `[ExcludedFromScanScope.item_ #]` 部分。

Scan_File 任务设置

设置	描述	
`ScanFiles`	启用文件扫描。	Yes（默 No — 不
`ScanBootSectors`	启用引导扇区扫描。	Yes — No（默
`ScanComputerMemory`	启用进程内存和内核内存扫描。	Yes — No（默 存。
`ScanStartupObjects`	启用启动对象扫描。	Yes — No（默
`ScanArchived`	启用存档扫描（包括 SFX 自解压存档）。	Yes（默 了 Firs

	应用程序会扫描以下压缩文件：.zip；.7z *；.7-z；.rar；.iso；.cab；.jar；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支持的压缩文件格式列表取决于所使用的应用程序数据库。	据存档 象，也 No - 不
ScanSfxArchived	仅允许扫描自解压存档（包含可执行文件提取模块的存档）。	Yes（ No - 不
ScanMailBases	启用对 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件客户端的电子邮件数据库的扫描。	Yes — No（默 文件。
ScanPlainMail	启用对纯文本电子邮件的扫描。	Yes — No（默
SizeLimit	指定要扫描的对象的最大大小（以 MB 为单位）。如果要扫描的对象大于指定值，应用程序将跳过此对象。	0 – 999 0 — 应 默认值：
TimeLimit	最长对象扫描持续时间（以秒为单位）。如果扫描对象所花费的时间超过此设置指定的时间，应用程序将停止扫描对象。	0 – 999 0 — 对 默认值：
FirstAction	选择应用程序将对受感染对象执行的第一个操作。	Disinf 将其副 如，如 类型）， 第一项 Second Remove 份副本 Recomm 序根据 选择该 Kaspers 马，因 中，因 Skip — 染的对 默认值：
SecondAction	选择应用程序将对受感染对象执行的第二个操作。如果第一项操作失败，则应用程序将执行第二项操作。	Second FirstA 如果选 作，则 况下， 第二项 二项操 默认值：
UseExcludeMasks	对 ExcludeMasks.item_# 设置指定的对象启用扫描排除项。	Yes — Exclud No（默 Exclud
ExcludeMasks.item_#	按名称或掩码在扫描中排除对象。您可以使用此设置来按名称从指定的扫描范围中排除单个文件，或者使用 Shell 格式的掩码一次	默认值

	性排除多个文件。	示例: UseE Excl Excl
UseExcludeThreats	对包含 ExcludeThreats.item_# 设置指定的威胁的对象启用扫描排除项。	Yes —
Exclud
的对象。 No（默
Exclud
的对象。
ExcludeThreats.item_#	按对象中检测到的威胁的名称从扫描中排除对象。在为此设置指定值之前，请确保已启用 UseExcludeThreats 设置。 要从扫描中排除对象，请指定在该对象中检测到的威胁的全名 – 包含应用程序确定已感染的对象的字符串。 例如，您可能正在使用实用程序来收集有关您的网络的信息。要防止应用程序对其进行阻止，请将其中包含的威胁的全名添加到排除在扫描范围之外的威胁列表中。 您可以在应用程序日志中或在网站 https://threats.kaspersky.com 上找到在对象中检测到的威胁的全名。	该设置
默认值
示例: UseE Excl Test Excl roja
UseGlobalExclusions	针对扫描启用全局排除项。	Yes（
No — 不
UseOASExclusions	针对扫描启用文件威胁防护排除项。	Yes（
项。 No — 不
ReportCleanObjects	允许记录有关应用程序报告为未受感染的扫描对象的信息。 例如，您可以启用此设置，以确保应用程序已扫描了特定对象。	Yes —
No（默
信息。
ReportPackedObjects	启用记录作为复合对象一部分的已扫描对象的有关信息。 例如，您可以启用此设置，以确保应用程序已扫描压缩文件中的某个对象。	Yes —
No（默
对象的
ReportUnprocessedObjects	启用记录由于某种原因尚未处理的对象的有关信息。	Yes —
No（默
息。
UseAnalyzer	启用启发式分析。 启发式分析可帮助应用程序检测威胁，甚至在病毒分析人员尚未意识到威胁之前。	Yes（
No — 禁
HeuristicLevel	指定启发式分析级别。 您可以指定启发式分析级别。启发式分析级别在威胁搜索的全面性、操作系统资源的负载以及扫描持续时间之间建立平衡。启发式分析级别越高，扫描所需的资源和时间就越多。	Light
Medium
负载均
Deep —
大。 Recomm
UseIChecker	启用 iChecker 技术。	Yes（

		No — 禁
DeviceNameMasks.item_#	设备名称列表。应用程序将扫描这些设备的引导扇区。 设置值不能为空。必须至少指定一个设备名掩码才能运行此任务。	AllObj < 设备名匹配的 默认值：符，包
[ScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描范围的说明，其中包含有关扫描范围的其他信息。使用此设置指定的字符串的最大长度为 4096 个字符。	默认值： 示例：Area
UseScanArea	启用指定范围的扫描。要运行任务，请启用至少一个范围的扫描。	Yes（默 No — 不
AreaMask.item_#	扫描范围限制。在扫描范围内，应用程序仅扫描使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序会扫描位于扫描范围内的所有对象。您可以为此设置指定多个值。	默认值： 示例：Area
路径	包含要扫描的对象的目录的路径。	< 本地目象。 Shared 设备文 Shared 的设备 Mounte 设备上 Mounte 到设备 AllRem NFS 协 AllSha 访问的 < 文件系的所有
[ExcludedFromScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描排除范围的说明，其中包含有关扫描排除范围的其他信息。	默认值
UseScanArea	从扫描中排除指定的范围。	Yes（默 No — 不
AreaMask.item_#	扫描排除范围的限制。在排除范围中，应用程序仅排除使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序将排除位于排除范围内的所有对象。您可以为此设置指定多个值。	默认值：
路径	包含要排除的对象的目录的路径。	< 本地目录（包

码指定

您可
目录

您可
录名
（包
或 /d

您可
件或
空集
如：
/dir

** 掩
例如，
掩码。

可以
名中

为了优
文件系
系统以
除项中。
的系统，
项：/.

Mounte
议在设

Mounte
议在设

AllRem
SMB 和
目录。

< 文件
文件系

仅当
应用
务启
扫描

关键区域扫描

执行关键区域扫描时，Kaspersky Endpoint Security 可以扫描引导扇区、启动对象、进程内存和内核内存。

检测到恶意软件后，该应用程序可能会删除受感染的文件并终止从该文件启动的恶意软件进程。

您可以启动关键区域扫描并配置扫描的设置：

- 选择要扫描的操作系统对象。默认启用对引导扇区、进程内存和内核内存、启动对象和压缩文件的扫描。默认情况下，关键区域扫描期间不会扫描文件。
- 限制要扫描的对象的大小以及对象扫描的持续时间。
- 选择应用程序将对感染对象执行的操作。
- 配置从扫描范围中排除的对象：
  - 按名称或掩码进行排除
  - 按对象中检测到的威胁名称进行排除
- 扫描时启用或禁用全局排除和文件威胁防护排除。
- 启用有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息记录。
- 配置扫描期间启发式分析器和 iChecker 技术的使用。
- 限制需要扫描其引导扇区的设备集。
- 配置扫描范围和扫描排除范围。

Web Console 中的关键区域扫描

在 Web Console 中，您可以使用“*关键区域扫描*”任务对受保护设备的操作系统执行关键区域扫描。

您可以创建并运行关键区域扫描用户任务。您可以通过编辑任务的设置来配置扫描设置。

关键区域扫描任务设置

设置	Description
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中该复选框，应用程序将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过在“**常规扫描设置**”部分中配置“**如果扫描时间超过以下值（秒）则跳过文件**”和“**跳过大于以下大小的文件 (MB)**”设置，您可以减少扫描压缩文件的时间。 如果清除该复选框，应用程序不会扫描压缩文件。 默认选中该复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中该复选框，应用程序将扫描自解压存档。 如果清除了该复选框，则应用程序不会扫描自解压存档。

	如果清除**扫描压缩文件**复选框，则此复选框可用。 默认选中该复选框。
扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中该复选框，应用程序将扫描邮件数据库文件。 如果清除了该复选框，则应用程序不会扫描邮件数据库文件。 默认情况下，清除此复选框。
扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则应用程序将扫描纯文本邮件。 如果清除此复选框，则应用程序不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，应用程序将停止扫描该文件。 可用值：0–9999。如果该值设置为 0，则扫描时间不受限制。 默认值：0。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：0–999999。如果该值设置为 0，则应用程序将扫描任何大小的文件。 默认值：0。
记录清洁对象	此复选框启用或禁用 *ObjectProcessed* 类型事件的日志记录。 如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 类型的事件。 如果清除此复选框，则应用程序不会记录任何已扫描对象的 *ObjectProcessed* 类型的事件。 默认情况下，清除此复选框。
通知未处理的文件	此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。 如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。 如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。 默认情况下，清除此复选框。
记录打包对象	此复选框为检测到的所有打包对象启用或禁用 *PackedObjectDetected* 类型事件的记录。 如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。 如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。 默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中该复选框，应用程序将仅扫描自上次扫描以来新增的文件或修改的文件。 如果清除该复选框，则无论文件创建或修改日期如何，应用程序都会扫描文件。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用文件扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“**使用启发式分析**”复选框，则可以在下拉列表中选择启发式分析级别： • **轻度**是详细程度最低的扫描，系统负载最小。 • **中度**是中度扫描，系统负载平衡。

	• **深度**是最详细的扫描，系统负载最大。 • **推荐**（默认值）是卡巴斯基专家推荐的最优级别。它确保了保护质量和对受保护设备性能的影响的最佳组合。
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **跳过**对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。 • **跳过**对象（默认值）。
扫描范围	包含任务扫描的范围的表。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。 您可以在表中添加、配置、删除、上移或下移扫描范围。 单击“**下移**”按钮可将所选项目在表中向下移动。 Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。 如果在表中只选择了就一个项目，则此按钮可用。 单击“**上移**”按钮可将所选项目在表中向上移动。 Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。 如果在表中只选择了就一个项目，则此按钮可用。 单击**删除**按钮会将所选范围排除在扫描范围之外。 如果在表中选择至少一个扫描范围，则此按钮可用。

	单击扫描范围名称将打开“**<扫描范围名称>**”窗口。在此窗口中，可以修改所选扫描范围的设置。 点击“**添加**”按钮将打开“**<新建扫描范围>**”窗口。在此窗口中，可以定义新的扫描范围。

“添加扫描范围”窗口

在此窗口中，您可以添加和配置扫描范围。

扫描范围设置

设置	Description
范围名称	用于输入扫描范围名称的字段。此名称将显示在“**扫描设置**”部分的**扫描范围**表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将处理此扫描范围。 如果清除此复选框，则应用程序不会处理此扫描范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	您可以在该下拉列表中选择文件系统的类型： • **本地**（默认值）— 本地目录。如果选择此项，则需要指定本地目录的路径。 • **挂载** – 挂载的远程或本地目录。如果选择此项，则需要指定文件系统的协议或名称。 • **共享** – 可通过 Samba 或 NFS 协议访问的受保护服务器的文件系统资源。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。 • **所有共享** – 可通过 Samba 和 NFS 协议访问的所有受保护服务器的文件系统资源。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**共享**或**挂载**类型，则此下拉列表可用。
Path	这是用于指定要包括在扫描范围中的目录路径的输入字段。您可以使用掩码和标签指定路径。

	您可以使用特殊标签来指定容器或镜像： • [container-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >]/< 本地目录的路径 > • [image-id:< 标识符 >]/< 本地目录的路径 > • [image-name:< 名称 >]/< 本地目录的路径 > 您还可以使用唯一的 [container-id:< 标识符 >]、[container-name:< 名称 >]、[image-id:< 标识符 >] 和 [image-name:< 名称 >]/< 本地目录的路径 > 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • [container-name:< 内存 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [image-name:< 名称 >][image-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-name:< 名称 >][image-id:< 标识符 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > 您可以在名称和标识符中使用掩码（? 和 * 字符）。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下指定 / 路径 – 应用程序扫描本地文件系统的所有目录。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。 如果在文件系统下拉列表中选择**本地**类型选项，并且未指定路径，则应用程序会扫描本地文件系统的所有目录。
共享资源的名称	用于输入要添加到扫描范围中的目录所在的文件系统共享资源名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。

掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“删除”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击添加按钮将打开一个窗口，您可以在其中指定新项目设置。

“扫描范围”部分

关键区域扫描任务的扫描范围设置

设置	Description
扫描文件	此复选框启用或禁用文件扫描。 如果选中该复选框，应用程序将扫描文件。 如果清除了该复选框，则应用程序不会扫描文件。 默认情况下，清除此复选框。
扫描启动扇区	此复选框启用或禁用引导扇区扫描。 如果选中该复选框，应用程序将扫描引导扇区。 如果清除该复选框，则应用程序不扫描引导扇区。 默认选中该复选框。
扫描内核内存和正在运行的进程	此复选框启用或禁用客户端设备内存扫描。 如果选中该复选框，应用程序将扫描内核内存和正在运行的进程。 如果清除该复选框，应用程序不会扫描内核内存和正在运行的进程。 默认选中该复选框。
扫描启动对象	此复选框启用或禁用启动对象扫描。 如果选中该复选框，应用程序将扫描启动对象。 如果清除了该复选框，则应用程序不会扫描启动对象。 默认选中该复选框。
要扫描的设备	单击“配置设备掩码”链接将打开“扫描范围”窗口，您可以在其中指定必须扫描其引导扇区的设备。

“扫描范围”窗口

该表包含应用程序必须扫描其引导扇区的设备的名称掩码。默认情况下，该表包含 /** 设备名称掩码（所有设备）。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”部分

在关键区域扫描任务的**排除范围**部分，您可以配置排除范围、按掩码排除和按威胁名称排除，以及在任务运行时全局排除和文件威胁防护排除的使用。

扫描排除项设置

设置	描述
配置排除项范围	单击“**配置排除项**”链接将打开“**排除范围**”窗口。在此窗口中，您可以定义扫描排除项列表。
按掩码配置排除项	单击“**按掩码配置排除项**”链接将打开“**按掩码筛选的排除项**”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称配置排除项	单击“**按威胁名称配置排除项**”链接将打开“**按威胁名称筛选的排除项**”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。
使用全局排除项	该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。 如果选中此复选框，则应用程序将从扫描中排除配置的挂载点。 默认选中该复选框。
使用文件威胁防护排除项	此复选框可启用或禁用应用程序运行时使用配置的文件威胁防护排除。 如果选中该复选框，应用程序将不会扫描文件威胁防护组件的排除项中指定的对象。 默认选中该复选框。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加排除范围”窗口

在此窗口中，您可以添加和配置排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时排除范围。 如果选中该复选框，则应用程序会在其运行期间将此范围排除在扫描或保护之外。 如果清除该复选框，则应用程序在其运行期间将此范围包括在扫描或保护中。您可以在以后选中此复选框来从扫描或保护中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	在此下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型： • **“本地”**，表示本地目录。 • **挂载**，表示设备上挂载的远程目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**挂载**类型，则此下拉列表可用。
Path	要添加到排除范围的目录路径的输入字段。您可以使用掩码和标签指定路径。

	您可以使用特殊标签来指定容器或镜像： • [container-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >]/< 本地目录的路径 > • [image-id:< 标识符 >]/< 本地目录的路径 > • [image-name:< 名称 >]/< 本地目录的路径 > 您还可以使用唯一的 [container-id:< 标识符 >]、[container-name:< 名称 >]、[image-id:< 标识符 >] 和 [image-name:< 名称 >]/< 本地目录的路径 > 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • [container-name:< 内存 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [image-name:< 名称 >][image-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-name:< 名称 >][image-id:< 标识符 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > 您可以在名称和标识符中使用掩码（? 和 * 字符）。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。
共享资源的	用于输入要添加到排除范围中的目录所在的文件系统共享资源名称的字段。

名称	如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在**路径**字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： `*.txt` 掩码表示所有文本文件。 `*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

管理控制台中的关键区域扫描

在管理控制台中，您可以使用“*关键区域扫描*”任务对受保护设备的操作系统执行关键区域扫描。

您可以创建并运行关键区域扫描用户任务。您可以通过编辑任务的设置来配置扫描设置。

在关键区域扫描任务属性的**“设置”**部分中，您可以配置下表列出的设置。

关键区域扫描任务设置

设置	Description
扫描	这组设置包含用于打开窗口的按钮，您可以在其中配置扫描范围、扫描范围设置和扫描设置。
检测威胁时的操作	这组设置包含**配置**按钮。单击此按钮将打开“**检测到威胁后的操作**”窗口，您可以在其中配置应用程序针对检测到的受感染对象执行的操作。

在关键区域扫描任务属性的排除项部分中，您还可以按掩码和威胁名称配置排除范围或排除项。

“扫描范围”窗口

该表包含扫描范围：应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。

扫描范围设置

设置	Description
范围名称	扫描范围名称。
Path	应用程序扫描的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

<新扫描范围>窗口

在此窗口中，您可以添加和配置扫描范围。

扫描范围设置

设置	Description
扫描范围名称	用于输入扫描范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。

	如果选中此复选框，应用程序将处理此扫描范围。 如果清除此复选框，则应用程序不会处理此扫描范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	该设置块可让您设置扫描范围。 您可以在文件系统下拉列表中选择文件系统类型： • **本地**（默认值）— 本地目录。如果选择此项，则需要指定本地目录的路径。 • **挂载** – 挂载的远程或本地目录。如果选择此项，则需要指定文件系统的协议或名称。 • **共享** – 可通过 Samba 或 NFS 协议访问的受保护服务器的文件系统资源。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。 • **所有共享** – 可通过 Samba 和 NFS 协议访问的所有受保护服务器的文件系统资源。
	如果在文件系统下拉列表中选择**共享**或**挂载**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。
	如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到扫描范围的目录的路径。您可以使用掩码和标签指定路径。

	您可以使用特殊标签来指定容器或镜像： • [container-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >]/< 本地目录的路径 > • [image-id:< 标识符 >]/< 本地目录的路径 > • [image-name:< 名称 >]/< 本地目录的路径 > 您还可以使用唯一的 [container-id:< 标识符 >]、[container-name:< 名称 >]、[image-id:< 标识符 >] 和 [image-name:< 名称 >]/< 本地目录的路径 > 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • [container-name:< 内存 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [image-name:< 名称 >][image-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-name:< 名称 >][image-id:< 标识符 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > 您可以在名称和标识符中使用掩码（? 和 * 字符）。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下指定 / 路径 – 应用程序扫描本地文件系统的所有目录。 如果在文件系统下拉列表中选择**本地**类型选项，并且未指定路径，则应用程序会扫描本地文件系统的所有目录。
文件系统名称	用于输入要添加到扫描范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序扫描的对象的名称掩码。

默认情况下，该列表包含 * 掩码（所有对象）。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“扫描范围设置”窗口

在此窗口中，您可以配置关键区域扫描任务的扫描设置。应用程序可让您扫描文件、引导扇区、启动对象、进程内存和内核内存。

扫描范围设置

设置	Description
扫描文件	此复选框启用或禁用文件扫描。 如果选中此复选框，则 Kaspersky Endpoint Security 将扫描文件。 如果取消选中此复选框，则 Kaspersky Endpoint Security 不会扫描文件。 默认情况下，清除此复选框。
扫描启动扇区	此复选框启用或禁用引导扇区扫描。 如果选中此复选框，则 Kaspersky Endpoint Security 将扫描引导扇区。 如果取消选中此复选框，则 Kaspersky Endpoint Security 不会扫描引导扇区。 默认选中该复选框。
扫描内核内存和正在运行的进程	此复选框启用或禁用设备内存扫描。 如果选中该复选框，Kaspersky Endpoint Security 将扫描内核内存和正在运行的进程。 如果清除该复选框，Kaspersky Endpoint Security 不会扫描内核和正在运行的进程。 默认选中该复选框。
扫描启动对象	此复选框启用或禁用启动对象扫描。 如果选中此复选框，则 Kaspersky Endpoint Security 将扫描启动对象。 如果取消选中此复选框，则 Kaspersky Endpoint Security 不会扫描启动对象。 默认选中该复选框。
要扫描的设备	这组设置包含**配置**按钮。单击此按钮将打开“扫描范围”窗口，您可以在其中指定必须扫描其引导扇区的设备。
使用全局排除项	该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。 如果选中此复选框，则应用程序将从扫描中排除配置的挂载点。 默认选中该复选框。

使用文件威胁防护排除项	此复选框可启用或禁用应用程序运行时使用配置的文件威胁防护排除。 如果选中该复选框，应用程序将不会扫描文件威胁防护组件的排除项中指定的对象。 默认选中该复选框。

“扫描范围”窗口

该表包含应用程序必须扫描其引导扇区的设备的名称掩码。默认情况下，该表包含 **/**** 设备名称掩码（所有设备）。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“扫描设置”窗口

在此窗口中，您可以配置任务的文件扫描设置。

扫描设置

设置	Description
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中该复选框，应用程序将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过在“**常规扫描设置**”部分中配置“**如果扫描时间超过以下值（秒）则跳过文件**”和“**跳过大于以下大小的文件 (MB)**”设置，您可以减少扫描压缩文件的时间。 如果清除该复选框，应用程序不会扫描压缩文件。 默认选中该复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中该复选框，应用程序将扫描自解压存档。 如果清除了该复选框，则应用程序不会扫描自解压存档。 如果清除**扫描压缩文件**复选框，则此复选框可用。 默认选中该复选框。
扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中该复选框，应用程序将扫描邮件数据库文件。

	如果清除了该复选框，则应用程序不会扫描邮件数据库文件。 默认情况下，清除此复选框。
扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则应用程序将扫描纯文本邮件。 如果清除此复选框，则应用程序不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，应用程序将停止扫描该文件。 可用值：0–9999。如果该值设置为 0，则扫描时间不受限制。 默认值：0。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：0–999999。如果该值设置为 0，则应用程序将扫描任何大小的文件。 默认值：0。
记录清洁对象	此复选框启用或禁用 *ObjectProcessed* 类型事件的日志记录。 如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 类型的事件。 如果清除此复选框，则应用程序不会记录任何已扫描对象的 *ObjectProcessed* 类型的事件。 默认情况下，清除此复选框。
记录未处理的对象	此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。 如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。 如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。 默认情况下，清除此复选框。
记录打包对象	此复选框为检测到的所有打包对象启用或禁用 *PackedObjectDetected* 类型事件的记录。 如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。 如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。 默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中该复选框，应用程序将仅扫描自上次扫描以来新增的文件或修改的文件。 如果清除该复选框，则无论文件创建或修改日期如何，应用程序都会扫描文件。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用文件扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“使用启发式分析”复选框，则可以在下拉列表中选择启发式分析级别： • 轻度是详细程度最低的扫描，系统负载最小。 • 中度是中度扫描，系统负载平衡。 • 深度是最详细的扫描，系统负载最大。 • 推荐（默认值）是卡巴斯基专家推荐的最优级别。它确保了保护质量和对受保护设备性能的影响的最佳组合。

“检测到威胁时的操作”窗口

在此窗口中，您可以配置 Kaspersky Endpoint Security 对于所检测到的受感染对象执行的操作：

检测到威胁后的操作

设置	Description
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **跳过**对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。 • **跳过**对象（默认值）。

“排除项”部分

*扫描排除项*是一组条件。当满足这些条件时，Kaspersky Endpoint Security 不会扫描对象中是否存在病毒和其他恶意软件。您还可以按掩码和威胁名称排除扫描对象。

扫描排除项设置

设置组	Description
排除范围	这组设置包含**配置**按钮。单击此按钮将打开“**排除范围**”窗口。在此窗口中，您可以定义要从扫描范围中排除的范围列表。
按掩码筛选的排除项	这组设置包含“**配置**”按钮，用于打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称筛选的排除项	这组设置包含**配置**按钮，用于打开“按威胁名称筛选的排除项”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

<新建扫描范围>窗口

在此窗口中，您可以添加和配置扫描排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从扫描中排除相应范围。 如果选中此复选框，则应用程序在扫描期间将排除此区域。 如果清除此复选框，则应用程序在扫描范围中包含此区域。您可以在以后选中此复选框来排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	该设置块可让您设置排除范围。 在文件系统下拉列表中，您可以选择要从扫描中排除的目录的文件系统类型： • “**本地**”，表示本地目录。 • **挂载** - 已挂载的目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
	如果在文件系统下拉列表中选择**挂载**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。

如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到排除范围的目录的路径。您可以使用掩码和标签指定路径。

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<标识符>]/<本地目录的路径>`
- `[container-name:<名称>]/<本地目录的路径>`
- `[image-id:<标识符>]/<本地目录的路径>`
- `[image-name:<名称>]/<本地目录的路径>`

您还可以使用唯一的 `[container-id:<标识符>]`、`[container-name:<名称>]`、`[image-id:<标识符>]` 和 `[image-name:<名称>]/<本地目录的路径>` 标签组合。

一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。

例如：

- `[container-name:<内存>][image-name:<名称>]/<本地目录的路径>`
- `[container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`
- `[image-name:<名称>][image-id:<标识符>]/<本地目录的路径>`
- `[container-name:<名称>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`
- `[container-name:<名称>][image-id:<标识符>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

您可以用 `*`（星号）字符来创建文件或目录名称掩码。

您可以指定单个 `*` 字符来表示文件或目录名称中 `/` 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 `*` 字符来表示文件或目录名称中的任意一组字符（包括空集和 `/` 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。

`**` 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。

掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。

可以使用单个 `?` 字符表示文件名或目录名中的任意一个字符。

	默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
文件系统名称	用于输入要添加到排除范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在路径字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

命令行中的关键区域扫描

在命令行中，您可以使用“关键区域扫描”预定义任务 (*Critical_Areas_Scan*) 对受保护设备的操作系统执行关键区域扫描。

您可以手动启动、停止、暂停或恢复此任务并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。

关键区域扫描任务设置

设置	描述	
`ScanFiles`	启用文件扫描。	`Yes` — 扫 `No`（默
`ScanBootSectors`	启用引导扇区扫描。	`Yes`（默 `No` — 不
`ScanComputerMemory`	启用进程内存和内核内存扫描。	`Yes`（默 存。 `No` — 不

ScanStartupObjects	启用启动对象扫描。	Yes（默 No — 不
ScanArchived	启用存档扫描（包括 SFX 自解压存档）。 应用程序会扫描以下压缩文件：.zip；.7z *；.7-z；.rar；.iso；.cab；.jar；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支持的压缩文件格式列表取决于所使用的应用程序数据库。	Yes（默 了 Firs 据存档 象，也 No - 不
ScanSfxArchived	仅允许扫描自解压存档（包含可执行文件提取模块的存档）。	Yes（默 No - 不
ScanMailBases	启用对 Microsoft Outlook、Outlook Express、The Bat 和其他邮件客户端的电子邮件数据库的扫描。	Yes — No（默 文件。
ScanPlainMail	启用对纯文本电子邮件的扫描。	Yes — No（默
SizeLimit	指定要扫描的对象的最大大小（以 MB 为单位）。如果要扫描的对象大于指定值，应用程序将跳过此对象。	0 – 999 0 — 应 默认值：
TimeLimit	最长对象扫描持续时间（以秒为单位）。如果扫描对象所花费的时间超过此设置指定的时间，应用程序将停止扫描对象。	0 – 999 0 — 对 默认值：
FirstAction	选择应用程序将对受感染对象执行的第一个操作。	Disinf 将其副 如，如 类型）， 第一项 Second Remove 份副本 Recomm 序根据 选择该 Kaspers 马，因 中，因 Skip — 染的对 默认值：
SecondAction	选择应用程序将对受感染对象执行的第二个操作。如果第一项操作失败，则应用程序将执行第二项操作。	Second FirstA 如果选 作，则 况下， 第二项 二项操 默认值：
UseExcludeMasks	对 ExcludeMasks.item_# 设置指定的对象启用扫描排除项。	Yes — Exclud

		No（默 Exclud
ExcludeMasks.item_#	按名称或掩码在扫描中排除对象。您可以使用此设置来按名称从指定的扫描范围中排除单个文件，或者使用 Shell 格式的掩码一次性排除多个文件。 在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。	默认值 示例: UseE Excl Excl
UseExcludeThreats	对包含 ExcludeThreats.item_# 设置指定的威胁的对象启用扫描排除项。	Yes — 从 Exclud 的对象。 No（默 Exclud 的对象。
ExcludeThreats.item_#	按对象中检测到的威胁的名称从扫描中排除对象。在为此设置指定值之前，请确保已启用 UseExcludeThreats 设置。 要从扫描中排除对象，请指定在该对象中检测到的威胁的全名 – 包含应用程序确定已感染的对象的字符串。 例如，您可能正在使用实用程序来收集有关您的网络的信息。要防止应用程序对其进行阻止，请将其中包含的威胁的全名添加到排除在扫描范围之外的威胁列表中。 您可以在应用程序日志中或在网站 https://threats.kaspersky.com 上找到在对象中检测到的威胁的全名。	该设置 默认值 示例: UseE Excl Test Excl roja
UseGlobalExclusions	针对扫描启用全局排除项。	Yes（默 No — 不
UseOASExclusions	针对扫描启用文件威胁防护排除项。	Yes（默 项。 No — 不
ReportCleanObjects	允许记录有关应用程序报告为未受感染的扫描对象的信息。 例如，您可以启用此设置，以确保应用程序已扫描了特定对象。	Yes — 记 No（默 信息。
ReportPackedObjects	启用记录作为复合对象一部分的已扫描对象的有关信息。 例如，您可以启用此设置，以确保应用程序已扫描压缩文件中的某个对象。	Yes — 记 No（默 对象的
ReportUnprocessedObjects	启用记录由于某种原因尚未处理的对象的有关信息。	Yes — 记 No（默 息。
UseAnalyzer	启用启发式分析。 启发式分析可帮助应用程序检测威胁，甚至在病毒分析人员尚未意识到威胁之前。	Yes（默 No — 禁
HeuristicLevel	指定启发式分析级别。 您可以指定启发式分析级别。启发式分析级别在威胁搜索的全面性、操作系统资源的负载以及扫描持续时间之间建立平衡。启发式分析级别越高，扫描所需的资源和时间就越多。	Light Medium 负载均

		Deep — 大。 Recomm
UseIChecker	启用 iChecker 技术。	Yes（默 No — 禁
DeviceNameMasks.item_#	设备名称列表。应用程序将扫描这些设备的引导扇区。 设置值不能为空。必须至少指定一个设备名掩码才能运行此任务。	AllObj < 设备名 匹配的 默认值： 符，包
[ScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描范围的说明，其中包含有关扫描范围的其他信息。使用此设置指定的字符串的最大长度为 4096 个字符。	默认值： 示例： Area
UseScanArea	启用指定范围的扫描。要运行任务，请启用至少一个范围的扫描。	Yes（默 No — 不
AreaMask.item_#	扫描范围限制。在扫描范围内，应用程序仅扫描使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序会扫描位于扫描范围内的所有对象。您可以为此设置指定多个值。	默认值： 示例： Area
路径	包含要扫描的对象的目录的路径。	< 本地目 象。 Shared 设备文 Shared 的设备 Mounte 设备上 Mounte 到设备 AllRem NFS 协 AllSha 访问的 < 文件系 的所有
[ExcludedFromScanScope.item_#] 部分包含以下设置：		
AreaDesc	扫描排除范围的说明，其中包含有关扫描排除范围的其他信息。	默认值
UseScanArea	从扫描中排除指定的范围。	Yes（默 No — 不
AreaMask.item_#	扫描排除范围的限制。在排除范围中，应用程序仅排除使用 shell 格式的掩码指定的文件。	默认值：

	如果未指定此设置，则应用程序将排除位于排除范围内的所有对象。您可以为此设置指定多个值。	
路径	包含要排除的对象的目录的路径。	< 本地目 录中的对 您可以 目录名 您可以 录名和 （包括 或 /d 您可以 件或目 空集和 如：/ /dir ** 掩 例如， 掩码。 可以使 名中的 为了优化 文件系统 系统以及 除项中。 的系统， 项：/. < 本地目 录（包括 码指定路

您可
目录

您可
录名
（包
或 /d

您可
件或
空集
如：
/dir

** 掩
例如，
掩码。

可以
名中

为了优
文件系
系统以
除项中。
的系统，
项：/.

Mounte
议在设

Mounte
议在设

AllRem
SMB 和
目录。

< 文件
文件系

仅当
应用
务启
扫描

可移动驱动器扫描

Kaspersky Endpoint Security 会对以下连接到受保护设备的可移动驱动器进行扫描：CD、DVD、蓝光光盘、闪存驱动器（包括 USB 调制解调器），外部硬盘驱动器和软盘。

如果启用了可移动驱动器扫描，Kaspersky Endpoint Security 会监控可移动驱动器与受保护设备之间的连接，如果检测到已连接的可移动驱动器，它会扫描该驱动器及其引导扇区是否存在病毒和其他恶意软件。

默认情况下，应用程序不会监控可移动驱动器的连接或对其进行扫描。

KESL 容器不支持此功能。

在 Web Console 中配置可移动驱动器扫描

在 Web Console 中，您可以在策略属性中配置可移动驱动器扫描设置（**应用程序设置 →本地任务→可移动驱动器扫描**）。

可移动驱动器扫描组件设置

设置	描述
可移动驱动器扫描已启用/已禁用	此选项启用或禁用可移动驱动器连接到用户设备时对其进行的扫描。 默认情况下，切换按钮处于关闭状态。
连接可移动驱动器时的操作	在下拉列表中，您可以选择应用程序在将可移动驱动器连接到用户设备时要执行的操作： • 连接可移动驱动器时**不扫描**（默认值）。 • **“快速扫描”**—仅扫描可移动驱动器（不包括 CD/DVD 驱动器和蓝光光盘）上的特定类型的文件，不解压复合对象。快速扫描使用“*关键区域扫描*”任务的默认设置执行。 在可移动驱动器上扫描以下文件格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 • **详细扫描** — 扫描可移动驱动器（不包括 CD/DVD 驱动器和蓝光光盘）上的所有文件。详细扫描使用“*恶意软件扫描*”任务的默认设置执行。
连接 CD / DVD 驱动器时的操作	在下拉列表中，您可以选择应用程序将 CD/DVD 驱动器和蓝光驱动器连接到用户设备时要执行的操作： • 连接 CD/DVD 驱动器和蓝光光盘时**不扫描**（默认值）。 • **快速扫描**：仅扫描 CD/DVD 驱动器和蓝光光盘上的特定类型的文件。快速扫描使用“*关键区域扫描*”任务的默认设置执行。

	在可移动驱动器上扫描以下文件格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 • **详细扫描** — 扫描 CD/DVD 驱动器和蓝光光盘上的所有文件。详细扫描使用“*恶意软件扫描*”任务的默认设置执行。
扫描期间阻止对可移动驱动器的访问	此复选框用于启用或禁用在执行扫描期间阻止已连接驱动器上的文件。 默认情况下，清除此复选框。

在管理控制台中配置可移动驱动器扫描

在管理控制台中，您可以在策略属性中配置可移动驱动器扫描设置（应用程序设置 →**本地任务**→**可移动驱动器扫描**）。

可移动驱动器扫描组件设置

设置	描述
在可移动驱动器连接到设备后，启用可移动驱动器扫描	此复选框启用或禁用可移动驱动器连接到用户设备时对其进行的扫描。 默认情况下，清除此复选框。
连接可移动驱动器时的操作	在下拉列表中，您可以选择应用程序在将可移动驱动器连接到用户设备时要执行的操作： • 连接可移动驱动器时**不扫描**（默认值）。 • “**快速扫描**”—仅扫描可移动驱动器（不包括 CD/DVD 驱动器和蓝光光盘）上的特定类型的文件，不解压复合对象。快速扫描使用“*关键区域扫描*”任务的默认设置执行。 在可移动驱动器上扫描以下文件格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 • **详细扫描** — 扫描可移动驱动器（不包括 CD/DVD 驱动器和蓝光光盘）上的所有文件。详细扫描使用“*恶意软件扫描*”任务的默认设置执行。
连接 CD / DVD 驱动器时的操作	在下拉列表中，您可以选择应用程序将 CD/DVD 驱动器和蓝光驱动器连接到用户设备时要执行的操作： • 连接 CD/DVD 驱动器和蓝光光盘时**不扫描**（默认值）。

	• **快速扫描**：仅扫描 CD/DVD 驱动器和蓝光光盘上的特定类型的文件。快速扫描使用“*关键区域扫描*”任务的默认设置执行。 在可移动驱动器上扫描以下文件格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 • **详细扫描** — 扫描 CD/DVD 驱动器和蓝光光盘上的所有文件。详细扫描使用“*恶意软件扫描*”任务的默认设置执行。
扫描期间阻止对可移动驱动器的访问	此复选框用于启用或禁用在执行扫描期间阻止已连接驱动器上的文件。 默认情况下，清除此复选框。

在命令行中配置可移动驱动器扫描

在命令行中，您可以使用“可移动驱动器扫描”预定义任务 (*Removable_Drives_Scan*) 管理可移动驱动器扫描。

默认情况下，可移动驱动器扫描将停止。您可以手动启动和停止该任务。您可以通过编辑该任务的设置来配置扫描设置。

如果任务正在运行，应用程序将监视可移动驱动器与设备的连接，并且当可移动驱动器连接时，它会创建并启动临时引导扇区扫描任务（ *ODS* 类型的任务）。此任务无法停止。任务执行完成后，应用程序会自动删除该任务。

如果您在可移动驱动器扫描任务设置中启用了文件扫描，应用程序还会启动一个或多个临时自定义文件扫描任务（*ODS* 类型的任务）。如有必要，具有管理员权限的用户可以停止这些任务。

如果更改“可移动驱动器扫描”任务设置，新值将不会应用于已在运行的临时任务。停止“可移动驱动器扫描”任务不会停止已经运行的临时任务。

“可移动驱动器扫描”任务设置

设置	描述	值
`ScanRemovableDrives`	启用在可移动驱动器连接到设备时，对其进行扫描的功能。 此设置不适用于 CD/DVD 驱动器和蓝光光盘（请参阅 `ScanOpticalDrives` 设置）。	`DetailedScan` - 扫描可移动驱动器（不包括 CD/DVD 驱动器和蓝光光盘）上的所有文件。 使用 *Scan_File* 任务（ID：3）的默认设置执行详细扫描。 `QuickScan` - 仅扫描可移动驱动器（不包括 CD/DVD 驱动器和蓝光光盘）上的特定类型的文件。

		在可移动驱动器上扫描以下文件格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 使用 Critical_Areas_Scan 任务（ID：4）的*默认*设置执行快速扫描。 NoScan（默认值）- 连接时不扫描可移动驱动器。
ScanOpticalDrives	在 CD/DVD 驱动器和蓝光光盘连接到设备时启用扫描。	DetailedScan - 扫描 CD/DVD 驱动器和蓝光光盘上的所有文件。 使用 *Scan_File* 任务 (ID: 3) 的默认设置执行详细扫描。 QuickScan - 仅扫描 CD/DVD 驱动器和蓝光光盘上特定类型的文件。 在可移动驱动器上扫描以下文件格式：com、exe、sys、prg、bin、bat、cmd、dpl、dll、scr、cpl、ocx、tsp、drv、vxd、pif、lnk、reg、ini、cia、vbs、vbe、js、jse、htm、htt、hta、asp、chm、pht、wsh、wsf、the、hip、eml、nws、msg、pig、mbx、doc*、dot*、fpm、rtf、shs、dwg、msi、otm、pdf、swf、jpeg、jpeg、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。 使用 *Critical_Areas_Scan* 任务 (ID:4) 的默认设置执行快速扫描。 NoScan（默认值）- 连接时 CD/DVD 驱动器和蓝光光盘时不扫描。
BlockDuringScan	允许在扫描过程中阻止已连接的磁盘上的文件。在扫描引导扇区时，文件不会被阻止。	Yes - 在扫描过程中阻止文件。 No（默认值）- 扫描过程中不阻止文件。

容器扫描

您可以实时、按需扫描容器和镜像中是否存在恶意软件：

- *容器监控*组件可让您实时扫描已启动的容器和命名空间。
- 您可以使用“*容器扫描*”任务按需扫描容器和镜像。

应用程序支持与 Docker 容器管理系统、CRI-O 框架以及 Podman 和 runc 实用程序集成。

要使用“容器扫描”任务，需要包含此功能的授权许可。

容器监控

容器监控组件默认处于启用状态。该应用程序实时扫描正在运行的容器和命名空间。

为了使容器监控组件正常工作，必须启用文件威胁防护组件。扫描容器和命名空间时使用文件威胁防护设置。

除非操作系统中安装了用于使用容器和命名空间的组件，否则应用程序不会扫描命名空间和容器。在这种情况下，命令行中“容器监控”的组件状态显示为“`Task is available and not running`”，而在 Kaspersky Security Center 中则显示为“`Stopped`”。

您可以启用或禁用容器监控组件，还可以配置实时扫描容器和命名空间的设置：

- 选择应用程序在检测到受感染对象时对容器执行的操作。

  在支持此功能的授权许可下使用应用程序时，此设置可用。

- 配置 Kaspersky Endpoint Security 与 Docker 容器管理系统、CRI-O 框架以及 Podman 和 runc 实用程序的集成。

在 Web Console 中配置容器监控

在 Web Console 中，您可以在策略属性中管理*容器监控*组件的运行（**应用程序设置 → 常规设置 → 容器扫描设置**）。

容器监控设置

设置	描述
命名空间和容器扫描已启用/已禁用	此切换开关可启用或禁用命名空间和容器的实时扫描。 默认情况下，复选切换开关处于打开状态。
检测到威胁时对容器的操作	您可以选择应用程序在检测到受感染对象时对容器执行的操作：

	• **跳过容器**：如果检测到受感染的对象，应用程序不会对容器执行任何操作。 • **停止容器**：如果检测到受感染的对象，应用程序将停止容器。 • **如果清除失败则停止容器**（默认值）— 如果对受感染对象的清除失败，应用程序将停止容器。 在支持此功能的授权许可下使用应用程序时，此设置可用。
使用 Docker	该复选框可启用或禁用 Docker 环境。 默认选中该复选框。
Docker 套接字路径	用于指定 Docker 套接字的路径或 URI（统一资源标识符）的输入字段。 默认值：/var/run/docker.sock.
使用 CRI-O	该复选框启用或禁用 CRI-O 环境。 默认选中该复选框。
文件路径	用于指定 CRI-O 配置文件路径的输入字段。 默认值：/etc/crio/crio.conf。
使用 Podman	该复选框启用或禁用 Podman 实用程序。 默认选中该复选框。
文件路径	用于指定 Podman 实用程序可执行文件路径的输入字段。 默认值：/usr/bin/podman。
根目录	用于指定容器存储的根目录路径的输入字段。 默认值：/var/lib/containers/storage。
使用 runc	该复选框启用或禁用 runc 实用程序。 默认选中该复选框。
文件路径	用于指定 runc 实用程序可执行文件路径的输入字段。 默认值：/usr/bin/runc。
根目录	用于指定容器状态存储的根目录路径的输入字段。 默认值：/run/runc。

在管理控制台中配置容器监控

在管理控制台中，您可以在策略属性中管理容器监控组件的运行（应用程序设置 → **常规设置** → **容器扫描设置**）。

容器监控设置

设置	描述
启用命名空间和容器扫描	此复选框可启用或禁用命名空间和容器的实时扫描。 默认选中该复选框。
检测到威胁时对容器的操作	在下拉列表中，您可以选择检测到受感染对象时要对容器执行的操作：

	• **跳过容器**：如果检测到受感染的对象，应用程序不会对容器执行任何操作。 • **停止容器**：如果检测到受感染的对象，应用程序将停止容器。 • **如果清除失败则停止容器**（默认值）— 如果对受感染对象的清除失败，应用程序将停止容器。 在支持此功能的授权许可下使用应用程序时，此设置可用。
容器扫描设置	这组设置包含“**配置**”按钮。单击此按钮将打开“容器扫描设置”窗口。

“容器扫描设置”窗口

在此窗口中，您可以编辑设置，将 Kaspersky Endpoint Security 与 Docker 容器管理系统、CRI-O 环境以及 Podman 和 runc 实用程序集成。

容器扫描设置

设置	Description
使用 Docker	该复选框可启用或禁用 Docker 环境。 默认选中该复选框。
Docker 套接字路径	用于指定 Docker 套接字的路径或 URI（统一资源标识符）的输入字段。 默认值：/var/run/docker.sock.
使用 CRI-O	该复选框启用或禁用 CRI-O 环境。 默认选中该复选框。
文件路径	用于指定 CRI-O 配置文件路径的输入字段。 默认值：/etc/crio/crio.conf。
使用 Podman	该复选框启用或禁用 Podman 实用程序。 默认选中该复选框。
文件路径	用于指定 Podman 实用程序可执行文件路径的输入字段。 默认值：/usr/bin/podman。
根目录	用于指定容器存储的根目录路径的输入字段。
使用 runc	该复选框启用或禁用 runc 实用程序。 默认选中该复选框。
文件路径	用于指定 runc 实用程序可执行文件路径的输入字段。 默认值：/usr/bin/runc。
根目录	用于指定容器状态存储的根目录路径的输入字段。 默认值：/run/runc。

在命令行中配置容器监控

在命令行中，您可以使用常规应用程序设置中的 NamespaceMonitoring=Yes/No 设置来启用或禁用命名空间和容器的实时扫描。

您可以使用包含所有常规应用程序设置的配置文件或使用命令行键来编辑设置 NamespaceMonitoring 的值。

实时扫描命名空间和容器时，使用常规容器扫描设置。您可以使用 Kaspersky Endpoint Security 的特殊管理命令来查看和编辑这些设置：

- 您可以将常规“容器扫描”设置的当前值输出到控制台或配置文件。您可以使用此文件来编辑设置。
- 您可以使用包含设置的配置文件来编辑所有常规“容器扫描”设置。您可以使用显示常规“容器扫描”设置的命令来获取配置文件。
- 您可以使用命令行键，以 < 设置名称 >=< 设置值 > 格式编辑单个设置。您可以使用显示常规“容器扫描”设置的命令获取设置的当前值。

要将常规“容器扫描”设置的当前值输出到控制台，请执行以下命令：

```
kesl-control --get-container-settings [--json]
```

，其中指定 --json 后，以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

要将常规“容器扫描”设置的当前值输出到文件，请执行以下命令：

```
kesl-control --get-container-settings --file <配置文件路径> [--json]
```

其中：

- --file <配置文件路径>是保存常规“容器扫描”设置的文件的路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在具有指定名称的文件，则该文件将被覆盖。如果在磁盘上找不到指定目录，则不会创建文件。
- 指定 --json 后，以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

要使用配置文件编辑常规“容器扫描”设置的值：

1. 将常规“容器扫描”设置输出到配置文件，如上所述。
2. 编辑文件中必要参数的值并保存更改。
3. 执行命令：

   ```
   kesl-control --set-container-settings --file <配置文件路径> [--json]
   ```

   其中：

   - --file <配置文件路径>是包含常规“容器扫描”设置的配置文件的完整路径。
   - --json：如果您要以 JSON 格式从配置文件导入设置，请指定此键。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

   文件中定义的所有常规“容器扫描”设置的值都将导入应用程序。

要使用命令行键编辑常规“容器扫描”设置的值，请执行以下命令：

```
kesl-control --set-container-settings <设置名称>=<设置值> [<设置名称>=<设置值>]
```

其中<设置名称>=<设置值>是其中一项常规"容器扫描"设置的名称和值。

指定的常规"容器扫描"设置的值将被更改。

按需扫描容器和镜像

运行"*容器扫描*"任务时，Kaspersky Endpoint Security 会扫描容器和镜像中是否存在病毒和其他恶意软件。应用程序可以同时运行多个"容器扫描"任务。

支持与 Docker 容器管理系统、CRI-O 框架以及 Podman 和 runc 实用程序集成。

要使用该任务，需要包含相应功能的授权许可。

您可以启动容器扫描并配置扫描的设置：

- 按名称或名称掩码指定要扫描的容器和镜像。
- 启用扫描所有镜像层和容器。
- 选择应用程序将对容器执行的操作以及当检测到受感染对象时应用程序将对镜像执行的操作。
- 配置扫描容器或镜像内对象的设置：
  - 启用或禁用对压缩文件、邮件数据库、文本格式的电子邮件消息的扫描。
  - 限制要扫描的对象的大小以及对象扫描的持续时间。
  - 选择应用程序将对感染对象执行的操作。
  - 配置从扫描范围中排除的对象：
    - 按名称或掩码进行排除
    - 按对象中检测到的威胁名称进行排除
  - 扫描时启用或禁用全局排除。
  - 配置扫描期间启发式分析器和 iChecker 技术的使用。
  - 启用或禁用对有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息进行记录。

Web Console 中的容器扫描

在 Web Console 中，您可以使用*容器扫描*任务来扫描容器和镜像。

您可以创建并运行"容器扫描"用户任务。您可以通过编辑任务的设置来配置扫描设置。

设置	Description
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中该复选框，应用程序将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过在"**常规扫描设置**"部分中配置"**如果扫描时间超过以下值（秒）则跳过文件**"和"**跳过大于以下大小的文件(MB)**"设置，您可以减少扫描压缩文件的时间。 如果清除该复选框，应用程序不会扫描压缩文件。 默认选中该复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中该复选框，应用程序将扫描自解压存档。 如果清除了该复选框，则应用程序不会扫描自解压存档。 如果清除**扫描压缩文件**复选框，则此复选框可用。 默认选中该复选框。
扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中该复选框，应用程序将扫描邮件数据库文件。 如果清除了该复选框，则应用程序不会扫描邮件数据库文件。 默认情况下，清除此复选框。
扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则应用程序将扫描纯文本邮件。 如果清除此复选框，则应用程序不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，应用程序将停止扫描该文件。 可用值：0–9999。如果该值设置为 0，则扫描时间不受限制。 默认值：0。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：0–999999。如果该值设置为 0，则应用程序将扫描任何大小的文件。 默认值：0。
记录清洁对象	此复选框启用或禁用 *ObjectProcessed* 类型事件的日志记录。 如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 类型的事件。 如果清除此复选框，则应用程序不会记录任何已扫描对象的 *ObjectProcessed* 类型的事件。 默认情况下，清除此复选框。
记录未处理的对象	此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。 如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。 如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。 默认情况下，清除此复选框。
记录打包对象	此复选框为检测到的所有打包对象启用或禁用 *PackedObjectDetected* 类型事件的记录。 如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。 如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。

	默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中该复选框，应用程序将仅扫描自上次扫描以来新增的文件或修改的文件。 如果清除该复选框，则无论文件创建或修改日期如何，应用程序都会扫描文件。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用文件扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“**使用启发式分析**”复选框，则可以在下拉列表中选择启发式分析级别： • **轻度**是详细程度最低的扫描，系统负载最小。 • **中度**是中度扫描，系统负载平衡。 • **深度**是最详细的扫描，系统负载最大。 • **推荐**（默认值）是卡巴斯基专家推荐的最优级别。它确保了保护质量和对受保护设备性能的影响的最佳组合。
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **跳过**对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。 • **跳过**对象（默认值）。
扫描容器	此复选框启用或禁用容器扫描。如果选中该复选框，您可以为要扫描的容器指定名称或名称掩码。 默认选中该复选框。
名称掩码	用于指定要扫描的容器的名称或名称掩码的输入字段。 默认情况下，指定 * 掩码 — 将扫描所有容器。
针对威胁检测的操作	您可以选择应用程序在检测到受感染对象时对容器执行的操作： • **跳过容器** — 检测到受感染的对象时，不对容器执行任何操作。 • **停止容器** — 检测到受感染对象时停止容器。

	• **如果清除失败则停止容器**（默认值）— 如果对受感染对象进行清除或消除威胁失败，则停止容器。 由于 CRI-O 环境的工作方式，CRI-O 环境中的容器中的受感染对象不会被清除或删除。我们建议选择“**停止容器**”操作。
扫描映像	此复选框启用或禁用映像扫描。如果选中该复选框，您可以为要扫描的映像指定名称或名称掩码。 默认选中该复选框。
名称掩码	用于指定要扫描的映像的名称或名称掩码的输入字段。 默认情况下，指定 * 掩码（扫描所有映像）。
检测到威胁后的操作	您可以选择应用程序在检测到受感染对象时对容器执行的操作： • **跳过映像**（默认值）— 检测到受感染的对象时，不对映像执行任何操作。 • 检测到受感染对象时**删除映像**（不推荐）。所有依赖项也将被删除。正在运行的容器将被停止，然后删除。
扫描每个层	此复选框启用或禁用扫描所有映像层和正在运行的容器。 默认情况下，清除此复选框。

“排除范围”部分

在容器扫描任务的**排除范围**部分，您可以按掩码和按威胁名称配置排除项，以及在任务运行时使用全局排除。

扫描排除项设置

设置	描述
按掩码配置排除项	单击“**按掩码配置排除项**”链接将打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称配置排除项	单击“**按威胁名称配置排除项**”链接将打开“按威胁名称筛选的排除项”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。
使用全局排除项	该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。 如果选中此复选框，则应用程序将从扫描中排除配置的挂载点。 默认选中该复选框。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

管理控制台中的容器扫描

在管理控制台中，您可以使用“*容器扫描*”任务扫描容器和镜像。

您可以创建并运行“容器扫描”用户任务。您可以通过编辑任务的设置来配置扫描设置。

在容器扫描任务属性的**设置**部分中，您可以配置下表列出的设置。

容器扫描任务设置

设置	Description
扫描	这组设置包含用于打开窗口的按钮，您可以在这些窗口中配置容器扫描设置和常规扫描设

	置。
检测威胁时的操作	这组设置包含**配置**按钮。单击此按钮将打开"**检测到威胁后的操作**"窗口，您可以在其中配置应用程序针对检测到的受感染对象执行的操作。

在**排除项**部分的任务属性中，您还可以按掩码和按威胁名称为容器扫描任务配置排除项。

"容器扫描设置"窗口

在此窗口中，您可以配置容器和映像扫描设置。

容器和映像扫描设置

设置	Description
扫描容器	此复选框启用或禁用容器扫描。如果选中该复选框，您可以为要扫描的容器指定名称或名称掩码。 默认选中该复选框。
名称掩码	用于指定要扫描的容器的名称或名称掩码的输入字段。 默认情况下，指定 * 掩码 — 将扫描所有容器。
针对威胁检测的操作	在下拉列表中，您可以选择检测到受感染对象时要对容器执行的操作： • **跳过容器** — 检测到受感染的对象时，不对容器执行任何操作。 • **停止容器** — 检测到受感染对象时停止容器。 • **如果清除失败则停止容器**（默认值）— 如果对受感染对象进行清除或消除威胁失败，则停止容器。 由于 CRI-O 环境的工作方式，CRI-O 环境中的容器中的受感染对象不会被清除或删除。我们建议选择"**停止容器**"操作。
扫描映像	此复选框启用或禁用映像扫描。如果选中该复选框，您可以为要扫描的映像指定名称或名称掩码。 默认选中该复选框。
名称掩码	用于指定要扫描的映像的名称或名称掩码的输入字段。 默认情况下，指定 * 掩码（扫描所有映像）。
检测到威胁后的操作	在下拉列表中，您可以选择检测到受感染对象时要对映像执行的操作： • **跳过映像**（默认值）— 检测到受感染的对象时，不对映像执行任何操作。 • 检测到受感染对象时**删除映像**（不推荐）。所有依赖项也将被删除。正在运行的容器将被停止，然后删除。
扫描每个层	此复选框启用或禁用扫描所有映像层和正在运行的容器。 默认情况下，清除此复选框。

"扫描设置"窗口

在此窗口中，您可以配置任务的文件扫描设置。

扫描设置

设置	Description
扫描压缩文件	此复选框用于启用或禁用压缩文件扫描。 如果选中该复选框，应用程序将扫描压缩文件。 要扫描压缩文件，应用程序必须先将其解压缩，这可能会降低扫描速度。通过在“**常规扫描设置**”部分中配置“**如果扫描时间超过以下值（秒）则跳过文件**”和“**跳过大于以下大小的文件(MB)**”设置，您可以减少扫描压缩文件的时间。 如果清除该复选框，应用程序不会扫描压缩文件。 默认选中该复选框。
扫描 SFX 压缩文件	此复选框启用或禁用*自解压存档*扫描。自解压缩文件是包含可执行解压模块的压缩文件。 如果选中该复选框，应用程序将扫描自解压存档。 如果清除了该复选框，则应用程序不会扫描自解压存档。 如果清除**扫描压缩文件**复选框，则此复选框可用。 默认选中该复选框。
扫描邮件数据库	此复选框用于启用或禁用扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。 如果选中该复选框，应用程序将扫描邮件数据库文件。 如果清除了该复选框，则应用程序不会扫描邮件数据库文件。 默认情况下，清除此复选框。
扫描邮件格式文件	此复选框用于启用或禁用扫描纯文本电子邮件文件。 如果选中此复选框，则应用程序将扫描纯文本邮件。 如果清除此复选框，则应用程序不会扫描纯文本邮件。 默认情况下，清除此复选框。
跳过扫描时间超过以下值的文件(秒)	在此字段中，可以指定扫描文件的最长时间（以秒为单位）。在指定时间后，应用程序将停止扫描该文件。 可用值：0–9999。如果该值设置为 0，则扫描时间不受限制。 默认值：0。
跳过大于以下大小的文件(MB)	在此字段中，可以指定要扫描的文件的最大大小（以 MB 为单位）。 可用值：0–999999。如果该值设置为 0，则应用程序将扫描任何大小的文件。 默认值：0。
记录清洁对象	此复选框启用或禁用 *ObjectProcessed* 类型事件的日志记录。 如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 类型的事件。 如果清除此复选框，则应用程序不会记录任何已扫描对象的 *ObjectProcessed* 类型的事件。 默认情况下，清除此复选框。
记录未处理的对象	此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。 如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。 如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。 默认情况下，清除此复选框。
记录打包对象	此复选框为检测到的所有打包对象启用或禁用 *PackedObjectDetected* 类型事件的记录。

	如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。 如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。 默认情况下，清除此复选框。
使用 iChecker 技术	此复选框用于启用或禁用仅扫描自上次文件扫描以来的新文件和修改的文件。 如果选中该复选框，应用程序将仅扫描自上次扫描以来新增的文件或修改的文件。 如果清除该复选框，则无论文件创建或修改日期如何，应用程序都会扫描文件。 默认选中该复选框。
使用启发式分析	此复选框用于启用或禁用文件扫描期间的启发式分析。 默认选中该复选框。
启发式分析级别	如果选中“**使用启发式分析**”复选框，则可以在下拉列表中选择启发式分析级别： • **轻度**是详细程度最低的扫描，系统负载最小。 • **中度**是中度扫描，系统负载平衡。 • **深度**是最详细的扫描，系统负载最大。 • **推荐**（默认值）是卡巴斯基专家推荐的最优级别。它确保了保护质量和对受保护设备性能的影响的最佳组合。

•

“检测到威胁时的操作”窗口

在此窗口中，您可以配置 Kaspersky Endpoint Security 对于所检测到的受感染对象执行的操作：

检测到威胁后的操作

设置	Description
第一个操作	在此下拉列表中，可以选择应用程序对已检测到的受感染对象执行的第一个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据有关文件中检测到的威胁的危险级别以及对其进行清除的可能性的数据，对对象**执行推荐的操作**（默认值）。 • **跳过**对象。
第二个操作	在此下拉列表中，可以选择应用程序在对受感染对象执行的第一个操作失败后执行的第二个操作： • **清除**对象。受感染对象副本将移至备份中。 • **删除**对象。受感染对象副本将移至备份中。 • 根据在文件中检测到的威胁的危险级别以及将其清除的可能性的数据，对对象**执行推荐的操作**。

	• **跳过**对象（默认值）。

•

“排除项”部分

扫描排除项设置

设置组	Description
按掩码筛选的排除项	这组设置包含“**配置**”按钮，用于打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。
按威胁名称筛选的排除项	这组设置包含**配置**按钮，用于打开“按威胁名称筛选的排除项”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。
使用全局排除项	该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。 如果选中此复选框，则应用程序将从扫描中排除配置的挂载点。 默认选中该复选框。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从排除列表中删除所选威胁。

如果在列表中选择至少一个威胁名称，则此按钮可用。

单击表中的威胁名称将打开**威胁名称**窗口。在此窗口中，您可以编辑要从扫描中排除的威胁的名称。

单击“**添加**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

命令行中的容器扫描

在命令行上，您可以通过以下方式扫描容器和镜像：

- 使用“容器扫描”预定义任务 (*Container_Scan*)。您可以手动启动或停止该任务，并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。
- 使用“容器扫描”用户任务（*ContainerScan* 类型的任务）。您可以手动启动和停止用户任务，并配置任务运行计划。
- 通过使用命令 `kesl-control --scan-container`，您可以对指定的容器和镜像执行*自定义扫描*。

容器扫描任务设置

该表描述了所有容器和映像扫描设置的全部可用值以及默认值。

容器扫描任务设置

设置	描述	值
`ScanContainers`	扫描按掩码指定的容器。您可以使用 `ContainerNameMask` 设置指定掩码。	`Yes`（默认值）— 扫描由掩码定义的容器。 `No` — 不扫描由掩码定义的容器。

`ContainerNameMask`	指定定义要扫描的容器的名称或名称掩码。
	掩码以命令 Shell 格式指定。您可以使用 ? 和 * 字符。
	在指定此设置之前，请确保 `ScanContainers=Yes`。
		默认值：*（扫描所有容器）。
		例如：
		扫描具有 my_container 名称的容器：
		`ContainerNameMask=my_container`
		扫描名称以 my_container 开头的所有容器：
		`ContainerNameMask=my_container*`
		扫描所有符合这些条件的容器：名称以 my_ 开头，后接任意五个字符、再接 _container，最后以任意字符序列结尾：
		`ContainerNameMask=my_?????_container*`

ScanImages	扫描按掩码指定的映像。您可以使用 ImageNameMask 设置指定掩码。	Yes（默认值）— 扫描由掩码定义的映像。 No — 不扫描由掩码定义的映像。
ImageNameMask	指定定义要扫描的映像的名称或名称掩码。 在指定此设置之前，请确保 ScanImages 设置值已设为 Yes。 掩码以命令 Shell 格式指定。 如果要指定多个掩码，则必须在具有指定新索引的新行上指定每个掩码。	默认值：*（扫描所有映像）。 例如： 扫描带有“my_image”名称和“latest”标签的映像： ImageNameMask=my_image:latest 扫描名称以 my_image_ 开头且带有任何标签的所有映像： ImageNameMask=my_image*
DeepScan	检查所有映像层和正在运行的容器。	Yes - 扫描所有层。 No（默认值）- 不扫描任何层。
ContainerScanAction	检测到受感染对象时要对容器执行的操作。下面介绍了对容器内受感染对象的操作。	StopContainerIfFailed（默认值）- 如果无法清除或删除受感染对象，则应用程序会停止容器。 由于 CRI-O 环境的工作方式，CRI-O 环境中的容器中的受感染对象不会被清除或删除。我们建议选择“StopContainer”操作。 StopContainer — 检测到受感染的对象时，应用程序会停止容器。 Skip - 检测到受感染的对象时，应用程序不会对容器执行任何操作。
ImageAction	指定检测到受感染对象时要对映像执行的操作。下面介绍了对映像内受感染对象的操作。	Skip（默认值）- 检测到受感染的对象时，应用程序不会对映像执行任何操作。 Delete — 当检测到受感染的对象时，应用程序会删除映像（不推荐）。 所有依赖项也将被删除。正在运行的容器将被停止，然后删除。

下面描述的设置适用于容器和映像内的对象。

容器扫描任务设置

设置	描述	
ScanArchived	启用存档扫描（包括 SFX 自解压存档）。 应用程序会扫描以下压缩文件：.zip；.7z *；.7-z；.rar；.iso；.cab；.jar；.bz；.bz2；.tbz；.tbz2；.gz；.tgz；.arj。支持的压缩文件格式列表取决于所使用的应用程序数据库。	Yes（默 了 Firs 据存档 象，也 No - 不

ScanSfxArchived	仅允许扫描自解压存档（包含可执行文件提取模块的存档）。	Yes（默 No - 不
ScanMailBases	启用对 Microsoft Outlook、Outlook Express、The Bat 和其他邮件客户端的电子邮件数据库的扫描。	Yes — No（默 文件。
ScanPlainMail	启用对纯文本电子邮件的扫描。	Yes — No（默
TimeLimit	最长对象扫描持续时间（以秒为单位）。如果扫描对象所花费的时间超过此设置指定的时间，应用程序将停止扫描对象。	0 – 999 0 — 对 默认值：
SizeLimit	指定要扫描的对象的最大大小（以 MB 为单位）。如果要扫描的对象大于指定值，应用程序将跳过此对象。	0 – 999 0 — 应 默认值：
FirstAction	选择应用程序将对受感染对象执行的第一个操作。	Disinf 将其副 如，如 类型）， 第一项 Second Remove 份副本 Recomm 序根据 选择该 Kaspers 马，因 中，因 Skip — 染的对 默认值：
SecondAction	选择应用程序将对受感染对象执行的第二个操作。如果第一项操作失败，则应用程序将执行第二项操作。	Second FirstA 如果选 作，则 况下， 第二项 二项操 默认值：
UseExcludeMasks	对 ExcludeMasks.item_# 设置指定的对象使用扫描排除项。	Yes — Exclud No（默 Exclud
ExcludeMasks.item_#	按名称或掩码在扫描中排除对象。您可以使用此设置来按名称从指定的扫描范围中排除单个文件，或者使用 Shell 格式的掩码一次性排除多个文件。	默认值 示例： UseE Excl Excl

UseExcludeThreats	对包含 ExcludeThreats.item_# 设置指定的威胁的对象使用扫描排除项。	Yes —
Exclud
的对象。 No（默
Exclud
的对象。
ExcludeThreats.item_#	按对象中检测到的威胁的名称从扫描中排除对象。在为此设置指定值之前，请确保已启用 UseExcludeThreats 设置。 要从扫描中排除对象，请指定在该对象中检测到的威胁的全名 – 包含应用程序确定已感染的对象的字符串。 例如，您可能正在使用实用程序来收集有关您的网络的信息。要防止应用程序对其进行阻止，请将其中包含的威胁的全名添加到排除在扫描范围之外的威胁列表中。 您可以在应用程序日志中或在网站 https://threats.kaspersky.com 上找到在对象中检测到的威胁的全名。	该设置
默认值
示例:
UseE
Excl
Test
Excl
roja
UseGlobalExclusions	针对扫描启用全局排除项。	Yes（
 No — 不
ReportCleanObjects	允许记录有关应用程序报告为未受感染的扫描对象的信息。 例如，您可以启用此设置，以确保应用程序已扫描了特定对象。	Yes —
 No（默
信息。
ReportPackedObjects	启用记录作为复合对象一部分的已扫描对象的有关信息。 例如，您可以启用此设置，以确保应用程序已扫描压缩文件中的某个对象。	Yes —
 No（默
对象的
ReportUnprocessedObjects	启用记录由于某种原因尚未处理的对象的有关信息。	Yes —
 No（默
息。
UseAnalyzer	启用启发式分析。 启发式分析可帮助应用程序检测威胁，甚至在病毒分析人员尚未意识到威胁之前。	Yes（
 No — 禁
HeuristicLevel	指定启发式分析级别。 您可以指定启发式分析级别。启发式分析级别在威胁搜索的全面性、操作系统资源的负载以及扫描持续时间之间建立平衡。启发式分析级别越高，扫描所需的资源和时间就越多。	Light
 Medium
负载均
 Deep —
大。
 Recomm
UseIChecker	启用 iChecker 技术。	Yes（
 No — 禁

自定义扫描容器和镜像

您可以使用命令 kesl-control --scan-container 对指定容器和镜像执行自定义扫描。

使用预定义任务“*Custom_Container_Scan*”（ID：19）中存储的设置执行自定义扫描。您可以通过编辑此任务的设置来配置“自定义容器扫描”设置。默认情况下，“*Custom_Container_Scan*”任务的设置与“*Container_Scan*”任务（ID：18）相同。

要启动“自定义容器扫描”任务，请执行以下命令：

```
kesl-control --scan-container <容器/镜像 [:标签 ]>
```

其中 `<容器/镜像 [:标签 ]>` 是容器或镜像的名称或 ID。您可以使用掩码来扫描多个对象。

您可以用 `*`（星号）字符来创建文件或目录名称掩码。

您可以指定单个 `*` 字符来表示文件或目录名称中 `/` 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 `*` 字符来表示文件或目录名称中的任意一组字符（包括空集和 `/` 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。

`**` 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

可以使用单个 `?` 字符表示文件名或目录名中的任意一个字符。

如果有多个具有相同名称的实体，应用程序将扫描所有实体。

执行该命令后，会创建一个临时的容器和镜像扫描任务，完成后会自动删除。在这种情况下，扫描结果将输出到控制台。

例如：
扫描名为 my_container 的容器：
```
kesl-control --scan-container my_container
```
扫描名为 my_image 的镜像（所有标签）：
```
kesl-control --scan-container my_image*
```

与 Jenkins 集成

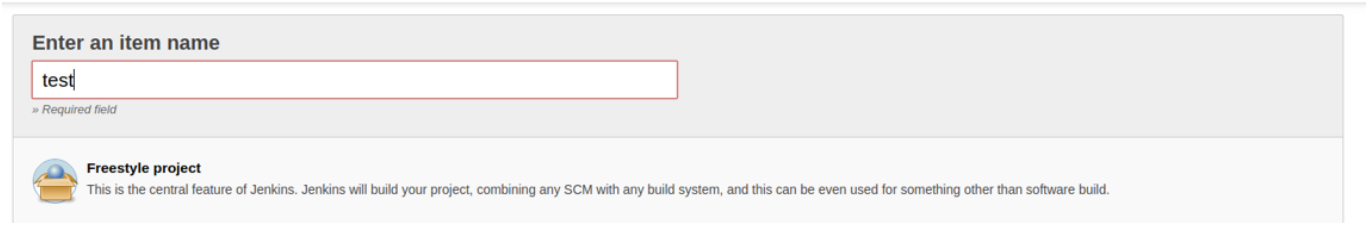
Kaspersky Endpoint Security 支持与 Jenkins 集成。Jenkins Pipeline 插件可用于在不同阶段扫描 Docker 映像。例如，您可以在开发期间或发布之前扫描存储库中的 Docker 映像。

要将 Kaspersky Endpoint Security 与 Jenkins 集成：

1. 请在 Jenkins 节点上安装 Kaspersky Endpoint Security。
2. 在 Jenkins 节点上安装 Docker Engine。
   有关详细信息，请参见 Docker Engine 文档。
3. 向 Jenkins 用户授予 Kaspersky Endpoint Security 管理员权限：
   ```
   kesl-control --grant-role admin <Jenkins 用户名>
   ```
4. 将 Jenkins 用户添加到 docker 组：
   ```
   sudo usermod -aG docker <Jenkins 用户名>
   ```

通常使用 jenkins 这一名称。

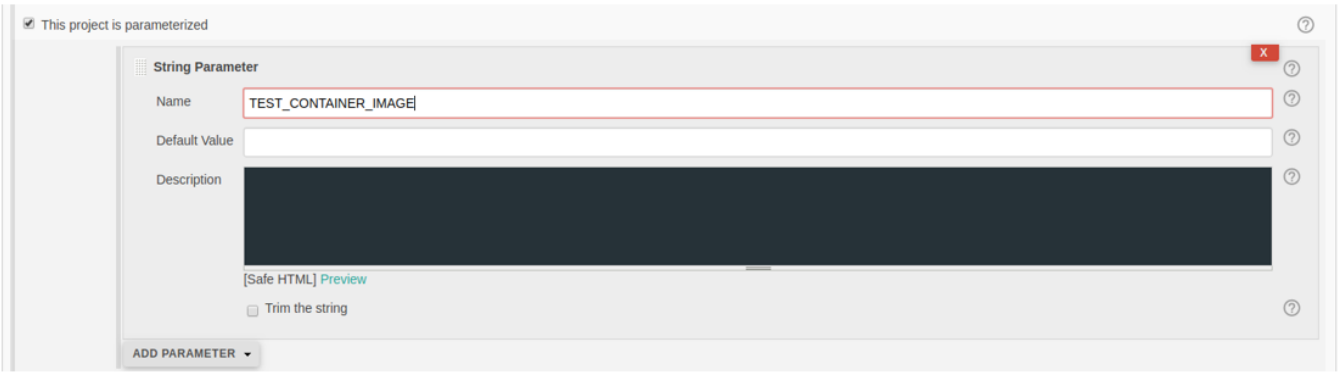
5. 在 Jenkins 中，创建一个名为 `test` 的新构建作业（**新建项目 → 输入项目名称**）。



6. 根据您的需求配置您的项目。假设结果是，您有一个映像或一个已启动的容器需要扫描。

7. 要启动 Docker 容器，请将以下脚本添加到 Jenkins 构建过程中。如果您使用 Jenkins 插件或其他方式来启动 Docker 容器，请将运行中的 Docker 容器的 ID 保存到 /tmp/kesl_cs_info 文件中，以便进一步扫描：

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE}
/storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. 构建工件后，在步骤中添加以下脚本以构建 jenkins。

对于扫描，此脚本支持一个容器。如有必要，请根据您的需求修改脚本。

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
```

```
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. 要从存储库中扫描 Docker 映像，请使用以下脚本：

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. 保存构建作业。

防火墙管理

在局域网 (LAN) 和互联网中使用的设备暴露于病毒、其他恶意软件、以及一系列针对操作系统和软件漏洞的攻击环境中。操作系统防火墙可保护用户设备上存储的数据，当设备连接到互联网或 LAN 时，防火墙可阻止大多数威胁。

操作系统的防火墙可以检测用户设备上的所有网络连接，并提供这些网络连接的 IP 地址列表。防火墙管理组件允许您通过配置网络数据包规则来设置网络连接的状态。

KESL 容器不支持此功能。

您可以使用网络数据包规则指定想要的设备保护级别，例如从完全阻止所有应用程序的互联网访问到允许无限制访问。除非指定了防火墙管理组件的相应阻止规则，否则默认情况下将允许所有出站连接。

默认禁用防火墙管理组件。

建议在启用防火墙管理组件之前禁用其他操作系统防火墙管理工具。

启用防火墙管理组件后，Kaspersky Endpoint Security 将使用操作系统提供的工具自动删除为防火墙配置的所有自定义规则。禁用组件后，这些规则不会恢复。如需要，请在启用防火墙管理组件之前保存自定义防火墙规则。

如果启用了防火墙管理，Kaspersky Endpoint Security 将扫描操作系统防火墙并阻止任何更改防火墙设置的尝试，例如当应用程序或实用程序试图添加或删除防火墙规则时。Kaspersky Endpoint Security 每 60 秒检查一次操作系统防火墙，并在必要时恢复使用应用程序创建的防火墙规则集。检查期间无法更改。

在 Red Hat Enterprise Linux 和 CentOS 8 操作系统中，在 Kaspersky Endpoint Security 中创建的防火墙规则只能通过使用管理命令（`kesl-control -F --query` 命令）进行查看。

禁用防火墙管理后，Kaspersky Endpoint Security 仍扫描操作系统防火墙。这样将允许应用程序还原动态规则。

您可以启用或禁用防火墙管理，还可以配置以下设置：

- 配置 Kaspersky Endpoint Security 在检测到建立网络连接的尝试时将应用的网络数据包规则列表。您可以添加或删除网络数据包规则，也可以更改网络数据包规则的执行优先级。
- 选择当没有任何其他网络数据包规则适用于此类连接时将对传入连接和数据包执行的默认操作。
- 将网络地址映射到预设的网络区域。您可以向网络区域添加 IP 地址或子网，也可以从网络区域中删除地址。
- 启用或禁用网络代理端口自动添加允许规则。

为避免具有 nftables 的系统可能出现问题，Kaspersky Endpoint Security 在为操作系统的防火墙添加规则时使用 iptables 和 iptables-restore 系统实用程序。该应用程序会创建一个名为 kesl_bypass 的特殊允许规则链，并将其添加到 iptables 和 ip6tables 实用程序的 mangle 表的列表顶部。kesl_bypass 链的规则允许从 Kaspersky Endpoint Security 的扫描中排除流量。该链中的规则可以通过操作系统进行更改。删除应用程序后，仅当 kesl_bypass 规则链为空时，才会从 iptables 和 ip6tables 中删除该规则链。

关于网络数据包规则

*网络数据包规则*是由 Kaspersky Endpoint Security 采取的操作，以允许或拒绝检测到的网络连接尝试。

网络数据包规则将对网络数据包进行限制，与应用程序无关。此类规则将限制通过选定数据协议的特定端口的入站和出站网络流量。

除非指定了防火墙管理的相应阻止规则，否则默认情况下允许所有出站连接（默认操作设置）。默认操作以最低优先级执行：如果未触发其他网络数据包规则，或者未指定任何网络数据包规则，则允许连接。

默认情况下，防火墙管理已指定了某些网络数据包规则。您可以创建自己的网络数据包规则，并为每个网络数据包规则指定执行优先级。

关于动态规则

Kaspersky Endpoint Security 允许向防火墙添加或删除*动态规则*，以确保应用程序正常运行。例如，网络代理可以添加动态规则，该规则允许连接到由应用程序或 Kaspersky Security Center 启动的 Kaspersky Security Center。“反加密勒索”的规则也是动态的。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，动态规则会被自动添加到防火墙，以允许连接到 SVM 和 Integration Server。

Kaspersky Endpoint Security 不会控制动态规则，也不会阻止应用程序组件对网络资源的访问。动态规则不依赖于防火墙管理组件状态（已启用/已禁用）或组件操作设置的更改。执行动态规则的优先级高于网络数据包规则的优先级。如果删除动态规则组中的任何规则，则应用程序会还原动态规则组（例如，使用 iptables 实用程序）。

您可以查看动态规则集（使用 `kesl-control -F --query` 命令）；但不能修改动态规则设置。

关于预定义的网络区域名称

*预定义的网络区域*是一组特定的 IP 地址或子网。通过使用预定义的网络区域，您可以对多个 IP 地址或子网使用相同的规则，而无需为每个 IP 地址或子网创建单独的规则。创建网络数据包规则时，网络区域可以用作“远程地址”参数的值。Kaspersky Endpoint Security 具有三个带有特定名称的预定义网络区域：

- **Public**。添加网络地址或子网到本区域，如果它已被分配给不受任何反病毒应用程序、防火墙或过滤器的保护（例如网吧网络）保护的网络。
- **Local**。添加网络地址或子网到本区域，如果它已被分配给其用户可访问此设备上文件和打印机的网络（例如，局域网或家庭网络）。
- **受信任**。此区域用于其中的设备不会暴露于攻击或未经授权数据访问尝试的安全网络。

您不能创建或删除网络区域。您可以向/从一个网络区域添加或删除 IP 地址和子网。

Web Console 中的防火墙管理

在 Web Console 中，您可以在策略属性中配置防火墙管理设置（**应用程序设置→ 基本威胁防护 → 防火墙管理**）。

防火墙管理设置

设置	描述
防火墙管理已启	此切换开关用于启用或禁用防火墙管理。

用/已禁用	默认情况下，切换按钮处于关闭状态。
网络数据包规则	单击“**配置网络数据包规则**”链接将打开“网络数据包规则”窗口。在此窗口中，可以配置防火墙管理组件在检测到网络连接尝试时应用的网络数据包规则列表。
可用网络	单击“**配置可用网络**”链接将打开“可用网络”窗口。在此窗口中，您可以配置防火墙管理组件将监视的网络列表。
传入连接	在此下拉列表中，您可以选择要对传入网络连接执行的操作： • **允许**网络连接（默认值）。 • **阻止**传入网络连接。
传入数据包	在此下拉列表中，可以选择要针对传入数据包执行的操作： • **允许**传入的数据包（默认值）。 • **阻止**传入数据包。
始终为网络代理端口添加允许规则	此复选框启用或禁用网络端口的自动添加允许规则。 默认选中该复选框。

“网络数据包规则”窗口

网络数据包规则表包含防火墙管理组件用于监视网络活动的网络数据包规则。您可以为网络数据包规则配置下表所示的设置。

网络数据包规则设置

设置	Description
Name	网络数据包规则名称
操作	“防火墙管理”在检测到网络活动时要执行的操作。
本地地址	安装了 Kaspersky Endpoint Security 且可以发送和/或接收网络数据包的设备的网络地址。
远程地址	可以发送和/或接收网络数据包的远程设备的网络地址。
Direction	被监控的网络活动的方向。
协议	为其监控网络活动的数据传输协议的类型。
本地端口	连接受监控的本地设备的端口号。
远程端口	连接受监控的远程设备的端口号。
ICMP 类型	ICMP 类型。防火墙管理组件将监控由主机或网关发送的指定类型的消息。
ICMP 代码	ICMP 代码。防火墙管理组件监控主机或网关发送的**ICMP 类型**字段中指定的类型和**ICMP 代码**字段中指定的代码的消息。
记录	此列显示应用程序是否记录网络数据包规则的操作。 如果值为 **Yes**，应用程序将记录网络数据包规则的操作。 如果值为 **No**，应用程序将不会记录网络数据包规则的操作。

默认情况下，网络数据包规则表为空。

您可以在表中添加、编辑、删除、上移或下移网络数据包规则。

单击“**下移**”按钮可将所选项目在表中向下移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“网络数据包规则”窗口

在此窗口中，您可以配置网络数据包规则。

网络数据包规则设置

设置	描述
规则名称	用于输入网络数据包规则名称的字段。
操作	在该下拉列表中，您可以选择防火墙管理组件检测到网络活动时要执行的操作： • **阻止**网络活动。 • **允许**网络活动（默认值）。
协议	在该下拉列表中，您可以选择要监控其网络活动的数据传输协议的类型： • **任何**（默认值） • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**

指定 ICMP 类型	此复选框允许指定 ICMP 类型。防火墙管理组件将监控由主机或网关发送的指定类型的消息。 如果选中此复选框，将显示用于输入 ICMP 类型的字段。 仅当在“**协议**”下拉列表中选择了“**ICMP**”或“**ICMPv6**”数据传输协议时，才会显示此复选框。 默认情况下，清除此复选框。
指定 ICMP 代码	此复选框允许指定 ICMP 代码。防火墙管理组件监控主机或网关发送的指定类型（在**指定 ICMP 类型**复选框下的字段中）和指定代码（在**指定 ICMP 代码**复选框下的字段中）的消息。 如果选中此复选框，将显示用于输入 ICMP 代码的字段。 仅当在“**协议**”下拉列表中选择了“**ICMP**”或“**ICMPv6**”数据传输协议时，才会显示此复选框。仅当选中“**指定 ICMP 类型**”复选框时才可用。 默认情况下，清除此复选框。
Direction	在此下拉列表中，您可以指定所监控的网络活动的方向： • **传入数据包**（默认值）。如果选择此选项，防火墙管理组件将监控传入数据包。 • **传入**。如果选择此选项，防火墙管理组件将监控传入网络活动。 • **传入/传出**。如果选择此选项，防火墙管理组件将监控传入和传出网络活动。 • **传入/传出数据包**。如果选择此选项，防火墙管理组件将监控传入和传出数据包。 • **传出数据包**。如果选择此选项，防火墙管理组件将监控传出数据包。 • **传出**。如果选择此选项，防火墙管理组件将监控传出网络活动。
远程地址	在此下拉列表中，您可以指定可以发送和接收网络数据包的远程设备的网络地址： • **任何地址**（默认值）。如果选择此选项，则网络规则将控制由具有任何 IP 地址的远程设备发送和接收的网络数据包。 • **所有子网地址**。如果选择此选项，则网络规则将控制由具有与选定网络类型关联的 IP 地址的远程设备发送和接收的网络数据包：**公用网络**、**本地网络**或**受信任网络**。 • **指定的地址**。如果选择此选项，则网络规则将控制由具有在“**地址**”字段中指定的 IP 地址的远程设备发送和接收的网络数据包。
指定远程端口	此复选框允许您指定必须监控其间连接的远程设备的端口号。 如果选中此复选框，将显示用于输入端口号的字段。 仅当在“**协议**”下拉列表中选择了“**TCP**”或“**UDP**”数据传输协议时，才会显示此复选框。 默认情况下，清除此复选框。
本地地址	在此下拉列表中，您可以指定已安装 Kaspersky Endpoint Security 并可以发送和接收网络数据包的设备的网络地址： • **任何地址**（默认值）。如果选择此选项，则网络规则将控制安装了 Kaspersky Endpoint Security 并具有任何 IP 地址的设备发送和/或接收网络数据包。 • **指定的地址**。如果选择此选项，则网络规则将控制由具有在“**地址**”字段中指定的网络地址并安装了 Kaspersky Endpoint Security 的设备发送和接收的网络数据包。
指定本地端口	此复选框允许您指定必须监控其间连接的本地设备的端口号。 如果选中此复选框，将显示用于输入端口号的字段。 仅当在“**协议**”下拉列表中选择了“**TCP**”或“**UDP**”数据传输协议时，才会显示此复选框。

	默认情况下，清除此复选框。
记录事件	此复选框允许您指定是否在报告中记录网络规则的操作。 如果选中该复选框，应用程序会将网络规则的操作写入报告。 如果清除该复选框，应用程序不会将网络规则的操作写入报告。 默认情况下，清除此复选框。

“可用网络”窗口

可用网络表包含由防火墙管理组件控制的网络。可用网络表默认为空。

可用网络设置

设置	Description
IP 地址	网络 IP 地址。
网络类型	网络类型（**公用网络**、**本地网络**或**受信任网络**）。

您可以添加、编辑和删除可用网络。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“网络连接”窗口

在此窗口中，您可以配置防火墙管理组件将监控的网络连接。

网络连接

设置	Description
IP 地址	用于输入网络 IP 地址的字段。
网络类型	您可以选择网络的类型： • 公用 • 本地 • 受信任

管理控制台中的防火墙管理

在管理控制台中，您可以在策略属性中配置防火墙管理设置（应用程序设置→ **基本威胁防护** → **防火墙管理**）。

防火墙管理设置

设置	Description
启用防火墙管理	此复选框用于启用或禁用防火墙管理。 默认情况下，清除此复选框。
网络数据包规则	这组设置包含**配置**按钮。单击此按钮将打开“网络数据包规则”窗口。在此窗口中，您可以配置防火墙管理组件在检测到网络连接尝试时应用的网络数据包规则。
可用网络	这组设置包含**配置**按钮。单击此按钮可打开可用网络窗口。在此窗口中，您可以配置防火墙管理组件将监视的网络列表。
传入连接	在此下拉列表中，您可以选择要对传入网络连接执行的操作： • **允许**网络连接（默认值）。 • **阻止**传入网络连接。
传入数据包	在此下拉列表中，可以选择要针对传入数据包执行的操作： • **允许**传入的数据包（默认值）。 • **阻止**传入数据包。
始终为网络代理端口添加允许规则	此复选框启用或禁用网络端口的自动添加允许规则。 默认选中该复选框。

“网络数据包规则”窗口

网络数据包规则表包含防火墙管理组件用于监视网络活动的网络数据包规则。您可以为网络数据包规则配置下表所示的设置。

网络数据包规则设置

设置	Description
Name	网络数据包规则名称
操作	“防火墙管理”在检测到网络活动时要执行的操作。
本地地址	安装了 Kaspersky Endpoint Security 且可以发送和/或接收网络数据包的设备的网络地址。
远程地址	可以发送和/或接收网络数据包的远程设备的网络地址。
记录	此列显示应用程序是否记录网络数据包规则的操作。 如果值为 **Yes**，应用程序将记录网络数据包规则的操作。 如果值为 **No**，应用程序将不会记录网络数据包规则的操作。

默认情况下，网络数据包规则表为空。

您可以在表中添加、编辑、删除、上移或下移网络数据包规则。

单击“**下移**”按钮可将所选项目在表中向下移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加网络数据包规则”窗口

在此窗口中，您可以配置添加的网络数据包规则设置。

网络数据包规则设置

设置	Description
协议	您可以选择要监控其网络活动的数据传输协议的类型： • 任何（默认值） • GRE • ICMP • ICMPv6 • IGMP • TCP • UDP
Direction	您可以指定被监控的网络活动的方向： • **传入数据包**。如果选择此选项，防火墙管理组件将监控传入数据包。 • **传入**。如果选择此选项，防火墙管理组件将监控传入网络活动。 • **传入/传出**。如果选择此选项，防火墙管理组件将监控传入和传出网络活动。

	• **传入/传出数据包**。如果选择此选项，防火墙管理组件将监控传入和传出数据包。 • **传出数据包**。如果选择此选项，防火墙管理组件将监控传出数据包。 • **传出**。如果选择此选项，防火墙管理组件将监控传出网络活动。
ICMP 类型	您可以指定 ICMP 类型。防火墙管理组件将监控由主机或网关发送的指定类型的消息。 如果选择了**指定的**选项，则将显示用于输入 ICMP 类型的字段。 仅当在**协议**下拉列表中选择了 **ICMP** 或 **ICMPv6** 数据传输协议时，才会显示此窗口。
ICMP 代码	您可以指定 ICMP 代码。防火墙管理组件监控主机或网关发送的**ICMP 类型**字段中指定的类型和**ICMP 代码**字段中指定的代码的消息。 如果选择了**指定的**选项，则将显示用于输入 ICMP 代码的字段。 仅当在**协议**下拉列表中选择了 **ICMP** 或 **ICMPv6** 数据传输协议时，才会显示此窗口。
远程端口	您可以指定要监视其间连接的远程设备的端口号。 如果选择了**指定的**选项，则将显示用于输入端口号的字段。 仅当在**协议**下拉列表中选择了 **TCP** 或 **UDP** 数据传输协议时，才会显示此窗口。
本地端口	您可以指定要监视其间连接的本地设备的端口号。 如果选择了**指定的**选项，则将显示用于输入端口号的字段。 仅当在**协议**下拉列表中选择了 **TCP** 或 **UDP** 数据传输协议时，才会显示此窗口。
远程地址	您可以指定可以发送和接收网络数据包的远程设备的网络地址： • **任何地址**（默认值）。如果选择此项，则网络规则将控制由具有任何 IP 地址的远程设备发送和/或接收的网络数据包。 • **指定的地址**。如果选择此项，则网络规则将控制具有在下面字段中指定的 IP 地址的远程设备的网络数据包发送和接收。 • **按网络类型**。如果选择此项，则网络规则将控制由具有与选定网络类型关联的 IP 地址的远程设备发送和接收的网络数据包：**公用网络**、**本地网络**或**受信任网络**。
本地地址	您可以指定安装了 Kaspersky Endpoint Security 并且可以发送和接收网络数据包的设备的网络地址： • **任何地址**（默认值）。如果选择此选项，则网络规则将控制由安装了 Kaspersky Endpoint Security 的设备发送和/或接收的网络数据包，无论其 IP 地址如何。 • **指定的地址**。如果选择此选项，则网络规则将控制安装了 Kaspersky Endpoint Security 且可以发送和接收网络数据包的设备的网络地址。这些网络地址在下面的字段中指定。
操作	您可以选择防火墙管理组件检测到网络活动时要执行的操作： • **阻止**网络活动。 • **允许**网络活动（默认值）。
记录	您可以指定是否将网络规则的操作记录在报告中。
规则名称	用于输入网络数据包规则名称的字段。

“可用网络”窗口

可用网络表包含由防火墙管理组件控制的网络。可用网络表默认为空。

可用网络设置

设置	Description
IP 地址	网络 IP 地址。
网络类型	网络类型（**公用网络**、**本地网络**或**受信任网络**）。

您可以添加、编辑和删除可用网络。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“网络连接”窗口

在此窗口中，您可以配置防火墙管理组件将监控的网络连接。

网络连接

设置	Description
IP 地址	用于输入网络 IP 地址的字段。
网络类型	您可以选择网络的类型： • 公用 • 本地 • 受信任

命令行中的防火墙管理

在命令行中，您可以使用“防火墙管理”预定义任务 (*Firewall_Management*) 来配置防火墙管理。

“防火墙管理”任务默认不运行。您可以手动启动和停止该任务。

您可以使用管理任务设置的命令编辑预定义任务的设置来配置防火墙管理设置。

您还可以使用防火墙管理命令配来置防火墙管理设置：

- 创建和删除网络数据包规则并更改其执行优先级。
- 创建网络区域中的 IP 地址或子网列表。
- 使用命令 `kesl-control -F --query` 查看在 Kaspersky Endpoint Security 中创建的防火墙规则。

防火墙管理任务设置

设置	描述	值
DefaultIncomingAction	当没有任何网络规则适用于此类连接时，对入站连接执行的默认操作。	Allow（默认值）- 允许入站连接。 Block - 阻止入站连接。
DefaultIncomingPacketAction	当没有任何网络数据包规则适用于此类连接时，对传入数据包执行的默认操作。	Allow（默认值）- 允许传入数据包。 Block - 阻止传入数据包。
OpenNagentPorts	将网络代理动态规则添加到网络数据包规则中。	Yes（默认值）- 在网络数据包规则中添加网络代理动态规则。 No - 不将网络代理动态规则添加到网络数据包规则中。
[PacketRules.item_#] 部分包含防火墙管理任务的网络数据包规则。您可以按任意顺序指定多个 [PacketRules.item_#] 部分。应用程序将按索引升序处理范围。 每个 [PacketRules.item_#] 部分均包含以下设置：		
Name	网络数据包规则名称。	默认值：Packet rule # <n>，其中 n 为索引。
FirewallAction	将针对此网络数据包规则中指定的连接执行的操作。	Allow（默认值）- 允许网络连接。 Block - 阻止网络连接。
协议	网络活动将被监控的协议类型。	Any（默认值）- 防火墙管理任务监控所有网络活动。 TCP UDP ICMP ICMPv6 IGMP GRE
RemotePorts	连接被监控的远程设备的端口号。可以为该值指定整数或间隔。 只有将 Protocol 设置设为 TCP 或 UDP 时，才能指定此设置。	Any（默认值）- 监控所有远程端口。 0 – 65535。
LocalPorts	连接被监控的本地设备的端口号。可以为该值指定整数或间隔。	Any（默认值）- 监控所有本地端口。

	只有将 Protocol 设置设为 TCP 或 UDP 时，才能指定此设置。	0 – 65535。
ICMPType	ICMP 数据包类型。 只有将 Protocol 设置设为 ICMP 或 ICMPv6 时，才能指定此设置。	Any（默认值）- 监控所有 ICMP 数据包类型。 符合数据传输协议规范的一个整数。
ICMPCode	ICMP 数据包代码。 只有将 Protocol 设置设为 ICMP 或 ICMPv6 时，才能指定此设置。	Any（默认值）- 监控所有 ICMP 数据包节点。 符合数据传输协议规范的一个整数。
Direction	被监控的网络活动的方向。	IncomingOutgoing 或 InOut（默认值）- 监控入站和出站连接。 Incoming 或 In - 监控入站连接。 Outgoing 或 Out - 监控出站连接。 IncomingPacket 或 InPacket - 监控传入数据包。 OutgoingPacket 或 OutPacket - 监控传出数据包。 IncomingOutgoingPacket 或 InOutPacket - 监控传入和传出数据包。
RemoteAddress	可以发送和/或接收网络数据包的远程设备的网络地址。	Any（默认值）— 监控由具有任意 IP 地址的远程设备发送和/或接收的网络数据包。 Trusted - 可信网络的预定义网络区域。 Local - 本地网络的预定义网络区域。 Public - 公用网络的预定义网络区域。 d.d.d.d — IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。 d.d.d.d/p — IPv4 地址的子网，其中 p 是介于 0 到 32 之间的数字。 x:x:x:x:x:x:x:x — IPv6 地址，其中 x 是介于 0 到 ffff 之间的十六进制数字。 x:x:x:x::0/p — IPv6 地址子网，其中 p 是介于 0 到 64 之间的数字。
LocalAddress	安装了 Kaspersky Endpoint Security 且可以发送和/或接收网络数据包的设备的网络地址。	Any（默认值）— 监控由具有任意 IP 地址的本地设备发送和/或接收的网络数据包。

		`d.d.d.d` — IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。 `d.d.d.d/p` — IPv4 地址的子网，其中 p 是介于 0 到 32 之间的数字。 `x:x:x:x:x:x:x:x` — IPv6 地址，其中 x 是介于 0 到 ffff 之间的十六进制数字。 `x:x:x:x::0/p` — IPv6 地址子网，其中 p 是介于 0 到 64 之间的数字。
`LogAttempts`	在报告中包含网络规则操作的记录。	`Yes`—在报告中记录操作。 `No`（默认值）—不在报告中记录操作。
[NetworkZonesPublic] 部分包含与公共网络关联的网络地址。您可以指定多个 IP 地址或 IP 地址的子网。		
`Address.item_#`	指定 IP 地址或 IP 地址的子网。	`d.d.d.d` — IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。 `d.d.d.d/p` — IPv4 地址的子网，其中 p 是介于 0 到 32 之间的数字。 `x:x:x:x:x:x:x:x` — IPv6 地址，其中 x 是介于 0 到 ffff 之间的十六进制数字。 `x:x:x:x::0/p` — IPv6 地址子网，其中 p 是介于 0 到 64 之间的数字。 默认值：""（此区域中没有网络地址）
[NetworkZonesLocal] 部分包含与本地网络关联的网络地址。您可以指定多个 IP 地址或 IP 地址的子网。		
`Address.item_#`	指定 IP 地址或 IP 地址的子网。	`d.d.d.d` — IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。 `d.d.d.d/p` — IPv4 地址的子网，其中 p 是介于 0 到 32 之间的数字。 `x:x:x:x:x:x:x:x` — IPv6 地址，其中 x 是介于 0 到 ffff 之间的十六进制数字。 `x:x:x:x::0/p` — IPv6 地址子网，其中 p 是介于 0 到 64 之间的数字。 默认值：""（此区域中没有网络地址）
[NetworkZonesTrusted] 部分包含与可信网络关联的网络地址。您可以指定多个 IP 地址或 IP 地址的子网。		
`Address.item_#`	指定 IP 地址或 IP 地址的子网。	`d.d.d.d` — IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。

		d.d.d.d/p — IPv4 地址的子网，其中 p 是介于 0 到 32 之间的数字。 x:x:x:x:x:x:x:x — IPv6 地址，其中 x 是介于 0 到 ffff 之间的十六进制数字。 x:x:x:x::0/p — IPv6 地址子网，其中 p 是介于 0 到 64 之间的数字。 默认值：""（此区域中没有网络地址）

在命令行中配置网络数据包规则列表

要添加网络数据包规则，请执行以下命令：

```
kesl-control --add-rule [--name <规则名称>] [--action <操作>] [--protocol <协议>] [--direction <方向>] [--remote <远程地址>[:<端口范围>]] [--local <本地地址>[:<端口范围>]] [--at <索引>]
```

其中：

- `--name <规则名称>` 是网络数据包规则的名称。
- `--action <操作>` 是对网络数据包规则中指定的连接执行的操作。
- `--protocol <协议>` 是要监控其网络活动的数据传输协议的类型。
- `--direction <方向>` 是被监控的网络活动的方向。
- `--remote <远程地址[:<端口范围>]>` 是远程设备的网络地址。您可以将预定义网络区域的名称指定作为远程地址。
- `--local <本地地址[:<端口范围>]>` 是已安装 Kaspersky Endpoint Security 的设备的网络地址。
- `--at <索引>` 是网络数据包规则列表中的规则索引。如果未指定 `--at` 键或其值大于列表中的规则数，则新规则会被添加到列表末尾。

命令中未指定值的参数被设置为其默认值。

例如：

要创建规则阻止到 TCP 端口 23 的所有传入和已建立的连接，请执行以下命令：

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote any
```

要为公共网络区域创建规则以阻止通过 TCP 端口 23 的传入和已建立的连接，请执行以下命令：

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote Public
```

要删除网络数据包规则，请执行以下命令之一：

- `kesl-control --del-rule --name <规则名称>`

- `kesl-control --del-rule --index <索引>`

  其中：

- `--name <规则名称>`是网络数据包规则的名称。
- `--index <索引>` 是网络数据包规则列表中的当前规则索引。

如果网络数据包规则列表包含多个名称相同的规则或者不包含具有指定名称或索引的规则，则会发生错误。

如要更改网络数据包规则的执行优先级，请执行以下命令之一：

- `kesl-control --move-rule --name <规则名称> --at <索引>`
- `kesl-control --move-rule --index <索引> --at <索引>`

  其中：

- `--name <规则名称>`是网络数据包规则的名称。
- `--index <索引>` 是网络数据包规则列表中的当前规则索引。
- `--at <索引>` 是网络数据包规则列表中的新规则索引。

在命令行中配置网络区域

要将网络地址添加到区域，请执行以下命令：

```
kesl-control --add-zone --zone <区域> --address <地址>
```

其中：

- `--zone <区域>` 是网络区域的预定义名称。可能的值：`Public`、`Local`、`Trusted`。
- `--address <地址>` 是网络地址或子网。

如要从区域中删除网络地址，请执行以下命令之一：

- `kesl-control --del-zone --zone <区域> --address <地址>`
- `kesl-control --del-zone --zone <区域> --index <区域中的地址索引>`

如果一个区域包含多个具有相同网络地址的项目，则将不执行 `--del-zone` 命令。

如果指定的网络地址或索引不存在，则会生成错误消息。

Web 威胁防护

Web 威胁防护组件允许您扫描通过 HTTP、HTTPS 和 FTP、网站和 IP 地址的入站流量，防止从互联网下载恶意文件，并阻止访问网络钓鱼、广告软件和其他恶意网站。

KESL 容器不支持此功能。

启用“网络威胁防护”后，拦截的 TCP 端口的当前连接将被重置。

默认情况下，“Web 威胁防护”任务被禁用。但是，如果允许在设备上对“Web 威胁防护”设置进行本地管理（策略未应用或未在策略属性中设置“锁定”），并且在系统中检测到以下可执行浏览器文件之一（包括 snap 格式），则会自动启用该任务：

- chrome
- chromium
- chromium-browser
- firefox
- firefox-esr
- google-chrome
- opera
- yandex-browser

您可以启用或禁用“Web 威胁防护”，还可以配置防护设置：

- 选择应用程序在检测到危险对象的 Web 资源上执行的操作。
- 配置受信任的网址列表。该应用程序不会扫描其网址包含在此列表中的网站的内容。
- 选择应用程序在扫描入站流量时将检测的对象。
- 配置加密连接扫描以扫描 HTTPS 流量。

  要扫描 FTP 流量，必须在加密连接扫描设置中配置对所有网络端口的控制。

打开网站时，应用程序会执行以下操作：

1. 使用下载的应用程序数据库检查网站的安全性。
2. 如果启用，使用启发式分析检查网站安全性。

   在启发式分析过程中，Kaspersky Endpoint Security 将分析操作系统中应用程序的活动。启发式分析可以检测 Kaspersky Endpoint Security 数据库中当前没有记录的危险对象。

3. 如果启用了卡巴斯基安全网络，则使用卡巴斯基的信誉数据库检查网站的可信任性。

建议您启用卡巴斯基安全网络的使用，以帮助“Web 威胁防护”更有效地运行。

4. 阻止或允许打开网站。

当试图打开一个危险的网站时，应用程序会执行以下操作：

- 对于 HTTP 或 FTP 流量，应用程序会阻止访问并显示警告消息。
- 对于 HTTPS 流量，浏览器会显示一个错误页面。

删除应用程序证书可能会导致 Web 威胁防护组件无法正常运行。

Kaspersky Endpoint Security 会将一个特殊的允许规则链 (kesl_bypass) 添加到 iptables 和 ip6tables 实用程序的 mangle 表中。该允许规则链允许从应用程序的扫描中排除流量。如果链中配置了流量排除规则，则会影响 Web 威胁防护组件的操作。

在 Web Console 中配置 Web 威胁防护

在 Web Console 中，您可以在策略属性中配置“Web 威胁防护”设置（**应用程序设置 → 基本威胁防护 → Web 威胁防护**）。

Web 威胁防护组件设置

设置	描述
Web 威胁防护已启用/已禁用	此切换开关用于启用或禁用 Web 威胁防护组件。 默认情况下，切换按钮处于关闭状态。
检测威胁时的操作	在此部分中，可以指定应用程序对检测到危险对象的 Web 资源执行的操作： • 在 Web 流量中检测到危险对象时**通知**用户。Web 威胁防护允许将此对象下载到设备。此时，应用程序会记录有关危险对象的信息，并将其添加到活动威胁列表中。 • **阻止**对 Web 流量中检测到的所有危险对象的访问，显示有关阻止的访问尝试的通知，并记录有关危险对象的信息（默认值）。
检测恶意对象	此复选框启用或禁用根据恶意网址数据库检查链接的功能。 默认选中该复选框。
检测钓鱼链接	此复选框启用或禁用根据网络钓鱼网址数据库检查链接的功能。 默认选中该复选框。
使用启发式分析来检测钓鱼链接	此复选框启用或禁用通过启发式分析来检测钓鱼链接的功能。 如果选中了**检测钓鱼链接**复选框，则此复选框可用，默认情况下处于选中状态。
检测广告软件	此复选框启用或禁用根据广告软件网址数据库检查链接的功能。 默认情况下，清除此复选框。
检测入侵	此复选框用于启用或禁用根据入侵者可以用来破坏设备或数据的合法应用程序数据库检查链

者可以用来损害设备或数据的合法应用程序	接的功能。 默认情况下，清除此复选框。
受信任网址	此表包含您认为其内容可信的 URL 和网页的地址。 您只能将 HTTP/HTTPS 网址添加到受信任的网址列表中。 您可以使用掩码指定网址。不支持使用掩码指定 IP 地址。 创建地址掩码时，请使用星号 (*) 作为一个或多个字符的占位符。如果输入 *abc* 地址掩码，它将应用于包含“abc”序列的所有网络资源（例如，www.virus.com/download_virus/page_0-9abcdef.html）。要将星号作为字符而不是掩码包含在地址掩码中，请输入两次 * 字符（例如，www.virus.com/**/page_0-9abcdef.html 表示 www.virus.com/*/page_0-9abcdef.html）。 默认情况下，该表为空。 您可以在表中添加、编辑和删除网址。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“网址”窗口

在此窗口中，您可以将网址或网址掩码添加到受信任网址列表中。

您只能将 HTTP/HTTPS 网址添加到受信任的网址列表中。您可以使用掩码指定网址。不支持使用掩码指定 IP 地址。

创建地址掩码时，请使用星号 (*) 作为一个或多个字符的占位符。如果输入 *abc* 地址掩码，它将应用于包含“abc”序列的所有网络资源（例如，www.virus.com/download_virus/page_0-9abcdef.html）。要将星号作为字符而不是掩码包含在地址掩码中，请输入两次 * 字符（例如，www.virus.com/**/page_0-9abcdef.html 表示 www.virus.com/*/page_0-9abcdef.html）。

在管理控制台中配置“Web 威胁防护”

在管理控制台中，您可以在策略属性中配置Web 威胁防护（**基本威胁防护→Web 威胁防护**）。

Web 威胁防护组件设置

设置	描述

启用 Web 威胁防护	此复选框用于启用或禁用 Web 威胁防护。 默认情况下，清除此复选框。
受信任网址	这组设置包含**配置**按钮，用于打开受信任网址窗口，您可以在其中指定受信任的网址列表。该应用程序不会扫描其网址包含在此列表中的网站的内容。
针对威胁检测的操作	应用程序对在其中检测到危险对象的 Web 资源执行的操作： • **阻止**对 Web 流量中检测到的所有危险对象的访问，显示有关阻止的访问尝试的通知，并记录有关危险对象的信息（默认值）。 • 在 Web 流量中检测到危险对象时**通知**用户。Web 威胁防护允许将此对象下载到设备。此时，应用程序会记录有关危险对象的信息，并将其添加到活动威胁列表中。
扫描设置	这组设置包含**配置**按钮，用于打开扫描设置窗口，您可以在其中配置用于扫描传入流量的设置。

“受信任的网址”窗口

在此窗口中，您可以添加您认为其内容受信任的网址和网页。

您只能将 HTTP/HTTPS 网址添加到受信任的网址列表中。您可以使用掩码指定网址。不支持使用掩码指定 IP 地址。默认情况下，该列表为空。

创建地址掩码时，请使用星号 (*) 作为一个或多个字符的占位符。如果输入 *abc* 地址掩码，它将应用于包含“abc”序列的所有网络资源（例如，www.virus.com/download_virus/page_0-9abcdef.html）。要将星号作为字符而不是掩码包含在地址掩码中，请输入两次 * 字符（例如，www.virus.com/**/page_0-9abcdef.html 表示 www.virus.com/*/page_0-9abcdef.html）。

您可以在列表中添加、编辑和删除网址。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“网址”窗口

在此窗口中，您可以将网址或网址掩码添加到受信任网址列表中。

您只能将 HTTP/HTTPS 网址添加到受信任的网址列表中。您可以使用掩码指定网址。不支持使用掩码指定 IP 地址。

创建地址掩码时，请使用星号 (*) 作为一个或多个字符的占位符。如果输入 *abc* 地址掩码，它将应用于包含“abc”序列的所有网络资源（例如，www.virus.com/download_virus/page_0-9abcdef.html）。要将星号作为字符而不是掩码包含在地址掩码中，请输入两次 * 字符（例如，www.virus.com/**/page_0-9abcdef.html 表示 www.virus.com/*/page_0-9abcdef.html）。

“扫描设置”窗口

在此窗口中，您可以配置在运行 Web 威胁防护组件期间扫描传入流量的设置。

Web 威胁防护设置

设置	Description
检测恶意对象	此复选框启用或禁用根据恶意网址数据库检查链接的功能。 默认选中该复选框。
检测钓鱼链接	此复选框启用或禁用根据网络钓鱼网址数据库检查链接的功能。 默认选中该复选框。
使用启发式分析来检测钓鱼链接	此复选框启用或禁用通过启发式分析来检测钓鱼链接的功能。 如果选中了**检测钓鱼链接**复选框，则此复选框可用，默认情况下处于选中状态。
检测广告软件	此复选框启用或禁用根据广告软件网址数据库检查链接的功能。 默认情况下，清除此复选框。
检测入侵者可以用来损害设备或数据的合法应用程序	此复选框用于启用或禁用根据入侵者可以用来破坏设备或数据的合法应用程序数据库检查链接的功能。 默认情况下，清除此复选框。

在命令行中配置 Web 威胁防护

在命令行中，您可以使用“Web 威胁防护”预定义任务 (*Web_Threat_Protection*) 来管理 Web 威胁防护。

如果在系统中检测到某个受支持的浏览器且在设备上允许本地管理 Web 威胁防护设置（未应用策略或策略未在策略属性中设置“锁定”），则该任务会自动启动。

您可以手动启动和停止任务。您可以通过编辑“Web 威胁防护”预定义任务的设置来配置 Web 威胁防护设置。

Web 威胁防护任务设置

设置	描述	值
`ActionOnDetect`	指定在检测到 Web 流量中的受感染对象时要执行的操作。	`Inform` - 允许下载检测到的对象，显示关于被阻止的访问尝试的通知，并记录受感染对象的信息。 `Block`（默认值）- 阻止对检测到的对象的访问，显示关于被阻止的访问尝试的通知，并记录被感染对象的信息。
`CheckMalicious`	启用或禁用根据恶意网址数据库检查链接的功能。	`Yes`（默认值）- 检查链接是否列在恶意链接数据库中。

		No - 不检查链接是否列在恶意链接数据库中。
CheckPhishing	启用或禁用根据网络钓鱼网址数据库检查链接的功能。	Yes（默认值）- 检查链接是否列在网络钓鱼链接数据库中。 No - 不检查链接是否列在网络钓鱼链接数据库中。
UseHeuristicForPhishing	启用或禁用使用启发式分析来扫描网页中是否存在钓鱼链接。	Yes（默认值）- 使用启发式分析来检测钓鱼链接。如果指定了此值，则启发式分析的级别是 Light（以最小的系统负载进行最低程度的扫描）。您无法更改 Web 威胁防护任务的启发式分析级别。 No - 不使用启发式分析来检测钓鱼链接。
CheckAdware	启用或禁用根据广告软件网址数据库检查链接的功能。	Yes - 检查链接是否列在广告软件链接数据库中。 No（默认值）- 不检查链接是否列在广告软件链接数据库中。
CheckOther	启用或禁用根据网址（包含入侵者可以用来破坏设备或数据的合法应用程序）数据库扫描链接的功能。	Yes—检查这些链接是否列入网址（包含可能被入侵者用来破坏您的设备或数据的合法应用程序）数据库。 No（默认值）—不检查这些链接是否列入网址（包含可能被入侵者用来破坏您的设备或数据的合法应用程序）数据库。
UseTrustedAddresses	启用或禁用受信任网址列表。应用程序不会扫描受信任的网址中是否存在病毒或其他恶意对象。您可以使用 TrustedAddresses.item_# 参数指定受信任的网址。	Yes（默认值）- 使用受信任网址列表。 No - 不使用受信任网址列表。
TrustedAddresses.item_#	指定受信任网址。	默认值为未定义。 您可以使用掩码指定网址。 创建地址掩码时，请使用星号 (*) 作为一个或多个字符的占位符。如果输入 *abc* 地址掩码，它将应用于包含“abc”序列的所有网络资源（例如，www.virus.com/download_virus/page_0-9abcdef.html）。要将星号作为字符而不是掩码包含在地址掩码中，请输入两次 * 字符（例如，www.virus.com/**/page_0-9abcdef.html 表示 www.virus.com/*/page_0-9abcdef.html）。 不支持使用掩码指定 IP 地址。

加密连接扫描

加密连接扫描的设置用于Web 威胁防护和Web 控制组件的运行。Web 威胁防护组件可以解密和检查通过安全连接发送的网络流量。默认启用加密连接扫描。

您可以启用或禁用加密连接扫描，还可以配置扫描设置：

- 选择应用程序在检测到不受信任的证书时要执行的操作。
- 选择网站上发生加密连接扫描错误时要执行的操作。
- 启用或禁用使用互联网进行证书验证。
- 查看和配置受信任域列表。应用程序将不会扫描访问指定域时建立的加密连接。
- 配置应用程序在执行加密连接扫描时将视为可信的证书列表。
- 配置应用程序要监控的网络端口列表。您可以指定要监视的网络端口或网络端口范围。

更改加密连接扫描设置时，应用程序会在日志文件中记录 *NetworkSettingsChanged* 事件。

在 Web Console 中配置加密连接扫描

在 Web Console 中，您可以在策略属性（**应用程序设置 → 常规设置→网络设置**）中配置加密连接扫描的设置。

加密连接扫描设置

设置	描述
加密连接扫描已启用/已禁用	此切换开关用于启用或禁用加密连接扫描。 此切换开关默认打开。
受信任的根证书	单击“**管理受信任的根证书**”将打开“受信任的根证书”窗口，您可以在其中配置受信任的证书列表。执行加密连接扫描时使用受信任的证书。
访问包含不受信任的证书的域	您可以选择访问具有不受信任证书的域时应用程序将执行的操作： • “**允许**”（默认值）— 允许连接到具有不受信任证书的域。 • “**阻止**”— 阻止连接到具有不受信任证书的域。
访问具有加密连接扫描错误的域	您可以选择访问存在加密连接扫描错误的域时应用程序将执行的操作： • “**允许并向排除项添加域**”（默认值）— 将导致错误的域添加到存在扫描错误的域列表中，并且在访问此域时不扫描加密的网络流量。 • “**阻止**”— 阻止连接到存在扫描错误的域。
证书验证策略	您可以选择应用程序验证证书的方式： • **本地检查**：应用程序不通过互联网来验证证书。 • **完全检查**（默认值）：应用程序通过互联网检查和下载验证证书所需的缺失链。

受信任域	单击“**配置受信任域**”将打开“受信任域”窗口，您可以在其中配置受信任的域名列表。
监控所有网络端口	如果选择此选项，应用程序将监控所有网络端口。
仅监控所选网络端口	如果选择此选项，应用程序将仅监控“被监控的端口”窗口中指定的网络端口。 默认选中该选项。
被监控的端口	单击“**配置网络端口设置**”链接将打开“被监控的端口”窗口，您可以在其中指定应用程序要监控的网络端口。

“受信任的证书”窗口

您可以配置 Kaspersky Endpoint Security 认为可信的证书列表。扫描加密连接时，将使用受信任的证书列表。

将显示每个证书的以下信息：

- 证书主题
- 序列号
- 证书颁发者
- 证书开始日期
- 证书到期日期
- SHA256 证书指纹

默认情况下，证书列表为空。

您可以添加和移除证书。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

“添加受信任的证书”窗口

在此窗口中，您可以添加 Kaspersky Endpoint Security 将信任的证书。

“**添加证书**”链接将打开标准文件选择窗口。指示包含证书的文件（DER 或 PEM 格式）的路径。

选择证书文件后，窗口显示证书信息和文件路径。

“受信任域”窗口

此列表包含将从加密连接扫描中排除的域名和域名掩码。

示例：`*example.com`。例如，`*example.com/*` 是不正确的，因为需要指定域地址而不是网页。

默认情况下，该列表为空。

您可以在受信任域列表中添加、编辑和移除域。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

被监控的端口

如果在“网络设置”窗口的“**被监控的端口**”中选择了“**仅监控所选网络端口**”选项，则该表将包含应用程序必须监控的网络端口。

该表包含两列：

- **端口** – 受监控的端口。
- **描述** — 受监控端口的描述。

默认情况下，该表显示通常用于传输邮件和网络通信的网络端口列表。网络端口列表包含在应用程序包中。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

在管理控制台中配置加密连接扫描

在管理控制台中，您可以在策略属性（**常规设置→网络设置**）中配置加密连接扫描的设置。

加密连接扫描设置

设置	描述
启用加密连接扫	此复选框启用或禁用加密连接扫描。

描	默认选中该复选框。
访问包含不受信任的证书的域	在下拉列表中，您可以选择访问具有不受信任证书的域时应用程序将执行的操作： • “**允许**”（默认值）— 允许连接到具有不受信任证书的域。 • “**阻止**”— 阻止连接到具有不受信任证书的域。
访问具有加密连接扫描错误的域	在下拉列表中，您可以选择访问存在加密连接扫描错误的域时应用程序将执行的操作： • “**允许并向排除项添加域**”（默认值）— 将导致错误的域添加到存在扫描错误的域列表中，并且在访问此域时不扫描加密的网络流量。 • “**阻止**”— 阻止连接到存在扫描错误的域。
证书验证策略	在此下拉列表中，您可以选择应用程序验证证书的方式： • **本地检查**：应用程序不通过互联网来验证证书。 • **完全检查**（默认值）：应用程序通过互联网检查和下载验证证书所需的缺失链。
受信任域	这组设置包含“**配置**”按钮，用于打开“受信任域”窗口，您可以在其中配置受信任的域名列表。
受信任的根证书	这组设置包含“**配置**”按钮，用于打开“受信任的根证书”窗口，您可以在其中配置受信任的根证书列表。执行加密连接扫描时使用受信任的证书。
网络端口设置	这组设置包含**配置**按钮。单击此按钮将打开“被监控的端口”窗口。

“受信任域”窗口

此列表包含将从加密连接扫描中排除的域名和域名掩码。

示例：`*example.com`。例如，`*example.com/*` 是不正确的，因为需要指定域地址而不是网页。

默认情况下，该列表为空。

您可以在受信任域列表中添加、编辑和移除域。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“受信任的证书”窗口

您可以配置 Kaspersky Endpoint Security 认为可信的证书列表。扫描加密连接时，将使用受信任的证书列表。

将显示每个证书的以下信息：

- **主题** – 证书主题
- **序号** – 证书的序列号
- **颁发者** – 证书的颁发者
- **有效自** – 证书生效日期
- **到期日期** – 证书到期日期
- **SHA256 指纹**是 SHA256 证书指纹

默认情况下，证书列表为空。

您可以添加和移除证书。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

“添加证书”窗口

在此窗口中，您可以通过以下方式之一将证书添加到受信任的证书列表中：

- 指示证书文件的路径。“**浏览**”按钮将打开标准文件选择窗口。指示包含证书的文件（DER 或 PEM 格式）的路径。
- 将证书文件的内容复制到“**输入证书详情**”字段中。

被监控的端口

网络端口设置

设置	Description
监控所有网络端口	如果选择此选项，应用程序将监控所有网络端口。
仅监控所选网络端口	如果选择此选项，应用程序将仅监控表中指定的网络端口。 默认选中该选项。
网络端口设置	如果选择了**仅监控指定端口**选项，则此表包含应用程序监控的网络端口。该表包含两列： • **端口** – 受监控的端口。 • **描述** — 受监控端口的描述。

默认情况下，该表显示通常用于传输邮件和网络通信的网络端口列表。网络端口列表包含在应用程序包中。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

在命令行中配置加密连接扫描

命令行中提供了特殊的管理命令，用于管理加密连接扫描的设置。使用管理加密连接扫描设置的命令，您可以：

- 配置加密连接扫描的设置。
- 查看加密连接扫描的排除项。
- 清除应用程序自动从扫描范围中排除的域列表。
- 管理应用程序认为受信任的证书列表。

查看和编辑加密连接扫描的设置

您可以使用特殊的管理命令查看和编辑加密连接扫描的设置：

- 您可以将加密连接扫描设置的当前值输出到控制台或配置文件。您可以使用此文件来编辑设置。
- 您可以使用包含设置的配置文件编辑加密连接扫描的所有设置。您可以使用显示加密连接扫描设置的命令获取配置文件。
- 您可以使用命令行键，以 < 设置名称 >=< 设置值 > 格式编辑单个设置。您可以使用显示加密连接扫描设置的命令获取设置的当前值。

要将加密连接扫描设置的当前值输出到控制台，请执行以下命令：

```
kesl-control --get-net-settings [--json]
```

其中指定 `--json` 后，以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

要将加密连接扫描设置的当前值输出到文件，请执行以下命令：

```
kesl-control --get-net-settings --file <配置文件路径> [--json]
```

其中：

- `--file <配置文件路径>` 是用于保存加密连接扫描设置的配置文件的路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在具有指定名称的文件，则该文件将被覆盖。如果在磁盘上找不到指定目录，则不会创建文件。
- 指定 `--json` 后，以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

要使用配置文件编辑加密连接扫描设置的值：

1. 如上所述，将常规应用程序设置输出到配置文件。
2. 编辑文件中必要参数的值并保存更改。
3. 执行命令：

   `kesl-control --set-net-settings --file <配置文件路径> [--json]`

   其中：

   - `--file <配置文件路径>` 是包含加密连接扫描设置的配置文件的完整路径。
   - 指定 `--json`，则以 JSON 格式将配置文件中的设置导入应用程序。如果不指定 `--json` 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

   文件中定义的加密连接扫描设置的所有值都将导入应用程序。

要使用命令行编辑加密连接扫描设置的值，请执行以下命令：

`kesl-control --set-net-settings <设置名称>=<设置值> [<设置名称>=<设置值>]`

其中 `<设置名称>=<设置值>` 是其中一项加密连接扫描设置的名称和值。

加密连接扫描的指定设置的值将被更改。

查看加密连接扫描的排除项

您可以查看加密连接扫描的以下排除项列表：

- 用户添加的排除项列表；
- 应用程序添加的排除项列表；
- 从应用程序数据库收到的排除项列表。

要查看由用户添加的安全连接扫描排除项列表，请执行以下命令：

```
kesl-control -N --query user
```

要查看由用户添加的安全连接扫描排除项列表，请执行以下命令：

```
kesl-control -N --query auto
```

要查看从应用程序数据库收到的安全连接扫描排除项列表，请执行以下命令：

```
kesl-control -N --query kl
```

要清除应用程序自动排除在扫描范围之外的域列表，请执行以下命令：

```
kesl-control -N --clear-web-auto-excluded
```

管理受信任证书列表

要将证书添加到受信任的证书列表，请运行以下命令：

```
kesl-control --add-certificate <证书路径>
```

其中：

<证书路径> 是要添加的证书文件（PEM 或 DER 格式）的路径。

要从受信任的证书列表中移除证书，请运行以下命令：

```
kesl-control --remove-certificate <证书主题>
```

要查看受信任的证书列表，请执行以下命令：

```
kesl-control --list-certificates
```

将显示每个证书的以下信息：

- 证书主题
- 序列号
- 证书颁发者
- 证书开始日期
- 证书到期日期
- SHA256 证书指纹

网络威胁防护

使用网络威胁防护组件，您可以扫描入站网络流量，查找典型的网络攻击活动。

KESL 容器不支持此功能。

Kaspersky Endpoint Security 从当前的应用程序数据库中接收 TCP 端口号，并扫描这些端口的传入流量。

为了扫描网络流量，“网络威胁防护”任务从应用程序数据库接收端口号，并接受通过所有这些端口的连接。在网络扫描过程中，它可能看起来像是设备上的一个开放端口，即使系统上没有任何应用程序正在侦听此端口。建议通过防火墙关闭未使用的端口。

启用“网络威胁防护”后，拦截的 TCP 端口的当前连接将被重置。

如果启用了网络威胁防护，在检测到受保护设备上的网络攻击尝试时，应用程序将阻止攻击设备的网络活动并创建“*检测到网络攻击*”事件。该事件包含有关攻击设备的信息。

默认情况下，来自攻击设备的网络流量会被阻止一小时。一旦阻止时间到期，应用程序就会解除对设备的阻止。

如果设备上的“网络威胁防护”设置是通过策略定义的，则默认启用网络威胁防护。如果在设备上应用本地配置的设置，则默认禁用网络威胁防护。

您可以启用或禁用网络威胁防护，还可以配置防护设置：

- 选择应用程序在检测到属于典型网络攻击的网络活动时执行的操作。
- 此复选框会启用或禁用在检测到网络攻击企图时阻止网络活动。
- 设置阻止攻击设备的持续时间。
- 配置应用程序不会阻止其网络活动的 IP 地址列表。

您可以在命令行中使用管理受阻止设备的命令来查看受阻止的设备列表，并手动解除对这些设备的阻止。除“*检测到网络攻击*”事件外，Kaspersky Security Center 不提供用于监控和管理被阻止设备的工具。

Kaspersky Endpoint Security 会将一个特殊的允许规则链 (kesl_bypass) 添加到 iptables 和 ip6tables 实用程序的 mangle 表中。该允许规则链允许从应用程序的扫描中排除流量。如果链中配置了流量排除规则，则会影响“网络威胁防护”任务的操作。例如，要排除传出 HTTP 流量，您需要添加以下命令：`iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT`。

在 Web Console 中配置网络威胁防护

在 Web Console 中，您可以在策略属性中配置“网络威胁防护”设置（**应用程序设置 → 基本威胁防护 → 网络威胁防护**）。

网络威胁防护组件设置

设置	描述
网络威胁防护	此切换开关用于启用或禁用网络威胁防护。

已启用/已禁用	默认情况下，复选切换按钮处于打开状态。
检测到威胁后的操作	在检测到属于典型网络攻击的网络活动时执行的操作。 • 告知用户。该应用程序允许网络活动并记录有关检测到的网络活动的信息。 • 阻止来自攻击设备的网络活动并记录有关检测到的网络活动的信息（默认值）。
阻止攻击设备已启用/已禁用	此切换开关用于启用或禁用在检测到网络攻击企图时阻止网络活动的功能。 默认情况下，复选切换开关处于打开状态。
阻止攻击设备（分钟）	在此字段中，您可以指定攻击方设备被阻止的持续时间（以分钟为单位）。在指定时间之后，Kaspersky Endpoint Security 允许来自该设备的网络活动。 可用值：介于 1 到 32768 之间的整数。 默认值：60。
排除项	该表包含 IP 地址列表。来自这些地址的网络攻击将不会被阻止。默认情况下，该列表为空。 您可以在表中添加、编辑和删除 IP 地址。 单击“删除”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击添加按钮将打开一个窗口，您可以在其中指定新项目设置。

“IP 地址”窗口

在此窗口中，您可以添加和编辑 IP 地址。来自这些 IP 地址的网络攻击将不会被 Kaspersky Endpoint Security 阻止。

IP 地址

设置	描述
输入 IP 地址	用于输入一个 IP 地址的字段。 您可以指定 IPv4 和 IPv6 版本的 IP 地址。

在管理控制台中配置网络威胁防护

在管理控制台中，您可以配置策略属性（基本威胁防护→网络威胁防护）中的“网络威胁防护”设置。

网络威胁防护组件设置

设置	Description
启用网络威	此复选框启用或禁用网络威胁防护。

胁防护	默认选中该复选框。
检测到威胁后的操作	在检测到属于典型网络攻击的网络活动时执行的操作。 • **告知**用户。该应用程序允许网络活动并记录有关检测到的网络活动的信息。 • **阻止**来自攻击设备的网络活动并记录有关检测到的网络活动的信息（默认值）。
阻止攻击设备	此复选框会启用或禁用在检测到网络攻击企图时阻止网络活动的功能。 默认选中该复选框。
阻止攻击设备（分钟）	在此字段中，您可以指定攻击方设备被阻止的持续时间（以分钟为单位）。在指定时间之后，Kaspersky Endpoint Security 允许来自该设备的网络活动。 可用值：介于 1 到 32768 之间的整数。 默认值：60。
排除项	这组设置包含“**配置**”按钮，用于打开“排除项”窗口，您可以在其中指定 IP 地址列表。来自这些 IP 地址的网络攻击将不会被阻止。

“排除项”窗口

在此窗口中，您可以添加不阻止其网络攻击的 IP 地址。

默认情况下，该列表为空。

您可以在列表中添加、编辑和删除 IP 地址。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“IP 地址”窗口

在此窗口中，您可以添加和编辑 IP 地址。来自这些 IP 地址的网络攻击将不会被 Kaspersky Endpoint Security 阻止。

IP 地址

设置	描述
输入 IP 地址	用于输入一个 IP 地址的字段。 您可以指定 IPv4 和 IPv6 版本的 IP 地址。

在命令行中配置网络威胁防护

在命令行中，您可以使用“网络威胁防护”预定义任务 (*Network_Threat_Protection*) 来管理“网络威胁防护”。

默认情况下，“网络威胁防护”任务不运行。您可以手动启动和停止任务。

您可以通过编辑“网络威胁防护”预定义任务的设置来配置“网络威胁防护”设置。

“网络威胁防护”任务设置

设置	描述	值
`ActionOnDetect`	在检测到属于典型网络攻击的网络活动时执行的操作。 将此设置的值从阻止更改为通知会清除被阻止设备列表。	`Notify` – 允许网络活动，记录有关检测到的网络活动的信息。如果指定此值，则忽略 `BlockAttackingHosts` 参数的值。 `Block`（默认值）– 阻止网络活动并记录相关信息。
`BlockAttackingHosts`	阻止攻击设备的网络活动。	`Yes`（默认值）— 阻止攻击设备的网络活动。 `No`– 不阻止攻击设备的网络活动。如果指定此值并且 `ActionOnDetect` 参数被设置为 `Block`，则应用程序会阻止来自攻击设备的网络活动，但不会将该设备添加到被阻止设备列表中。
`BlockDurationMinutes`	指定攻击方设备将被阻止的时长（以分钟为单位）。	1 – 32768 默认值：60。
`UseExcludeIPs`	在检测到网络攻击时不会阻止其网络活动的 IP 地址列表的使用。应用程序将只记录来自这些设备的危险活动信息。 您可以使用 `ExcludeIPs.item_#` 设置将 IP 地址添加到排除列表中。	`Yes` - 使用排除的 IP 地址的列表。 `No`（默认值）- 不使用排除的 IP 地址的列表。
`ExcludeIPs.item_#`	指定一个 IP 地址，其网络活动将不会被应用程序阻止。默认情况下，该列表为空。	`d.d.d.d` — IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。 `d.d.d.d/p` — IPv4 地址的子网，其中 p 是介于 0 到 32 之间的数字。 `x:x:x:x:x:x:x:x` — IPv6 地址，其中 x 是介于 0 到 ffff 之间的十六进制数字。 `x:x:x:x::0/p` — IPv6 地址子网，其中 p 是介于 0 到 64 之间的数字。 默认值为未定义。

针对远程恶意加密的防护

反加密勒索组件允许您保护通过 SMB/NFS 协议进行网络访问的本地目录中的文件，使其免受远程恶意加密侵扰。

要使用该组件，需要包含相应功能的授权许可。

KESL 容器不支持此功能。

如果启用了反加密勒索，Kaspersky Endpoint Security 将针对受保护设备的共享网络目录中的文件资源扫描远程设备的操作是否存在恶意加密。如果应用程序将远程设备访问共享网络资源的操作视为恶意加密，则应用程序将创建并启用操作系统的防火墙规则，阻止来自受感染设备的网络流量。受感染的设备将被添加到不受信任的设备列表中，并且所有不受信任的设备对共享网络目录的访问都会受到阻止。应用程序将创建一个*加密检测*事件，其中包含有关受感染设备的信息。

默认情况下，应用程序阻止非可信设备对网络文件资源访问的时间长度为 30 分钟。当阻止时间到期时，应用程序会将受感染的设备从不受信任的设备列表中删除，并自动恢复该设备对网络文件资源的访问权限。

无法使用 iptables 实用程序删除由反加密勒索组件创建的防火墙规则，因为应用程序每分钟都会恢复一组规则。

默认禁用针对远程恶意加密的防护。

您可以启用或禁用针对恶意加密的防护（反加密勒索），也可以配置防护设置：

- 选择检测到加密时应用程序将执行的操作：通知用户或阻止执行恶意加密的设备。

  如果选择了*"通知"*操作，则在启用反加密勒索时，应用程序仍会扫描远程设备在网络文件共享上的操作，以检查是否存在恶意加密。如果检测到恶意活动，则会创建*加密检测*事件，但不会阻止受感染的设备。

- 设置阻止不受信任的设备的持续时间。

- 指定应用程序要防护恶意加密的文件和目录。

- 指定从恶意加密防护中排除的文件和目录。

  如果在加密防护范围之外的目录中检测到加密活动（反加密勒索），应用程序不会将操作视为加密。

您可以在命令行中使用管理受阻止设备的命令来查看受阻止的设备列表，并手动解除对这些设备的阻止。除了*加密检测*事件之外，Kaspersky Security Center 不提供其他工具来监控和管理受阻止的设备。

为了保证反加密组件正常工作，必须在操作系统上安装至少一项服务（Samba 或 NFS）。NFS 服务要求安装 rpcbind 软件包。

反加密勒索组件可以与 SMB1、SMB2、SMB3、NFS3、TCP/UDP 和 IP/IPv6 协议一起正常运行。不支持使用 NFS2 和 NFS4 协议。建议配置服务器设置，以保证不能使用 NFS2 和 NFS4 协议挂载资源。

在将设备活动识别为恶意活动之前，Kaspersky Endpoint Security 不会阻止对网络文件资源的访问。因此，在应用程序检测到恶意活动之前，至少有一个文件将被加密。

在 Web Console 中配置反加密勒索

在 Web Console 中，您可以在策略属性中配置反加密勒索设置（**应用程序设置** → **高级威胁防护** → **反加密勒索**）。

反加密勒索组件设置

设置	描述
反加密勒索保护已启用/已禁用	此切换开关用于启用或禁用对本地目录中可通过 SMB/NFS 协议从网络访问的文件的保护，防止这些文件被远程恶意加密。 默认情况下，切换按钮处于关闭状态。
保护范围	单击“**配置保护范围**”链接将打开“保护范围”窗口。
检测到加密后的操作	Kaspersky Endpoint Security 检测到恶意加密时执行的操作： • **告知**用户。Kaspersky Endpoint Security 不会阻止执行加密的设备；它只会在事件日志中记录有关检测到恶意加密的事件。 • **阻止**设备执行加密（默认值）。
阻止不受信任的主机（分钟）	在此字段中，您可以按分钟为单位，指定不受信任的设备阻止持续时间 如果受到危害的主机被阻止，并且您更改了此设置值，则该主机的阻止时间不会变化。阻止时间不是动态值，它在阻止时进行计算。 可用值：介于 1 到 4294967295 之间的整数。 默认值：30。
排除项	单击“**配置排除项**”链接将打开“**排除范围**”窗口。
按掩码筛选的排除项	单击“**按掩码配置排除项**”链接将打开“**按掩码筛选的排除项**”窗口。

“保护范围”窗口

该表包含反加密组件的保护范围。应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。

保护范围设置

设置	Description
范围名称	保护范围名称。
Path	应用程序保护的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序保护指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

“添加保护范围”窗口

在此窗口中，您可以添加或配置反加密组件的保护范围。

保护范围设置

设置	Description
范围名称	用于输入保护范围名称的字段。此名称将显示在“保护范围”窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将在组件工作期间处理此保护范围。 如果清除此复选框，则应用程序不会在组件工作期间处理此保护范围。您可以在以后选中此复选框，来在组件操作设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	您可以在该下拉列表中选择文件系统的类型： • **本地**（默认值）— 本地目录。 • **共享**显示可通过 Samba 或 NFS 协议访问的服务器文件系统资源。 • **全部共享**显示可通过 Samba 和 NFS 协议访问的所有服务器文件系统资源。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 如果在文件系统下拉列表中选择“**共享**”选项，则此下拉列表可用。
Path	用于指定要包括在保护范围中的目录路径的输入字段。您可以使用掩码指定路径。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。 该字段不能为空。 默认情况下，指定 **/** 路径（根目录）。
掩码	该列表包含应用程序在反加密组件工作期间扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加排除范围”窗口

在此窗口中，您可以添加和配置排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时排除范围。 如果选中该复选框，则应用程序会在其运行期间将此范围排除在扫描或保护之外。 如果清除该复选框，则应用程序在其运行期间将此范围包括在扫描或保护中。您可以在以后选中此复选框来从扫描或保护中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	在此下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型： • **“本地”**，表示本地目录。 • **挂载**，表示设备上挂载的远程目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**挂载**类型，则此下拉列表可用。
Path	要添加到排除范围的目录路径的输入字段。您可以使用掩码和标签指定路径。

	您可以使用特殊标签来指定容器或镜像： • [container-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >]/< 本地目录的路径 > • [image-id:< 标识符 >]/< 本地目录的路径 > • [image-name:< 名称 >]/< 本地目录的路径 > 您还可以使用唯一的 [container-id:< 标识符 >]、[container-name:< 名称 >]、[image-id:< 标识符 >] 和 [image-name:< 名称 >]/< 本地目录的路径 > 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • [container-name:< 内存 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [image-name:< 名称 >][image-id:< 标识符 >]/< 本地目录的路径 > • [container-name:< 名称 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > • [container-name:< 名称 >][image-id:< 标识符 >][container-id:< 标识符 >][image-name:< 名称 >]/< 本地目录的路径 > 您可以在名称和标识符中使用掩码（? 和 * 字符）。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。
共享资源的	用于输入要添加到排除范围中的目录所在的文件系统共享资源名称的字段。

名称	如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在**路径**字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： `*.txt` 掩码表示所有文本文件。 `*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在管理控制台中配置反加密勒索

在管理控制台中，您可以在策略属性中配置反加密勒索设置（**高级威胁防护 → 反加密勒索**）。

反加密勒索组件设置

设置	Description
启用反加密勒索	此复选框用于启用或禁用对本地目录中可通过 SMB/NFS 协议从网络访问的文件的保护，防止这些文件被远程恶意加密。 默认情况下，清除此复选框。
保护范围	这组设置包含用于打开窗口的按钮，您可以在这些窗口中配置扫描范围和保护设置。
排除项	这组设置包含“**配置**”按钮。单击此按钮将打开“**排除范围**”窗口。在此窗口中，您可以定义要从扫描范围中排除的范围列表。
按掩码筛选的排除项	这组设置包含“**配置**”按钮，用于打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。

“扫描范围”窗口

该表包含扫描范围：应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。

扫描范围设置

设置	Description
范围名称	扫描范围名称。
Path	应用程序扫描的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

<新扫描范围>窗口

在此窗口中，您可以添加或配置反加密组件的保护范围。

保护范围设置

设置	Description
范围名称	用于输入保护范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将在组件工作期间处理此保护范围。 如果清除此复选框，则应用程序不会在组件工作期间处理此保护范围。您可以在以后选中此复选框，来在组件操作设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	该设置块可让您设置扫描范围。 您可以在文件系统下拉列表中选择文件系统类型： • “**本地**”，表示本地目录。 • **共享**显示可通过 Samba 或 NFS 协议访问的服务器文件系统资源。 • **全部共享**（默认值）显示可通过 Samba 和 NFS 协议访问的所有服务器文件系统资源。
	如果在文件系统下拉列表中选择**共享**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。

	如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到保护范围的目录的路径。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该字段不能为空。
掩码	该列表包含应用程序在反加密组件工作期间扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“保护设置”窗口

保护设置

设置	描述
检测到加密后的操作	Kaspersky Endpoint Security 检测到恶意加密时执行的操作： • 告知用户。Kaspersky Endpoint Security 不会阻止执行加密的设备；它只会在事件日志中记录有关检测到恶意加密的事件。 • 阻止设备执行加密（默认值）。
阻止不受信任	在此字段中，您可以按分钟为单位，指定不受信任的设备阻止持续时间。在指定的时间过后，Kaspersky Endpoint Security 将从阻止的设备列表中删除不受信任的设备。主机对网络文件资

的主机（分钟）	源的访问将在它从不受信任的主机列表中删除后自动恢复。 如果受到危害的主机被阻止，并且您更改了此设置值，则该主机的阻止时间不会变化。阻止时间不是动态值，它在阻止时进行计算。 可用值：介于 1 到 4294967295 之间的整数。 默认值：30。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

<新建扫描范围>窗口

在此窗口中，您可以添加和配置扫描排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从扫描中排除相应范围。 如果选中此复选框，则应用程序在扫描期间将排除此区域。 如果清除此复选框，则应用程序在扫描范围中包含此区域。您可以在以后选中此复选框来排除此范围。 默认选中该复选框。
文件系统，访问协议和	该设置块可让您设置排除范围。 在文件系统下拉列表中，您可以选择要从扫描中排除的目录的文件系统类型：

路径	• “**本地**”，表示本地目录。 • **挂载** - 已挂载的目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
	如果在文件系统下拉列表中选择**挂载**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。
	如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要添加到排除范围的目录的路径。您可以使用掩码和标签指定路径。 您可以使用特殊标签来指定容器或镜像： • `[container-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>]/<本地目录的路径>` • `[image-id:<标识符>]/<本地目录的路径>` • `[image-name:<名称>]/<本地目录的路径>` 您还可以使用唯一的 `[container-id:<标识符>]`、`[container-name:<名称>]`、`[image-id:<标识符>]` 和 `[image-name:<名称>]/<本地目录的路径>` 标签组合。 一个区域内允许使用 1 到 4 个唯一标签的任意组合。标签的排列顺序不重要。 例如： • `[container-name:<内存>][image-name:<名称>]/<本地目录的路径>` • `[container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[image-name:<名称>][image-id:<标识符>]/<本地目录的路径>` • `[container-name:<名称>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` • `[container-name:<名称>][image-id:<标识符>][container-id:<标识符>][image-name:<名称>]/<本地目录的路径>` 您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
文件系统名称	用于输入要添加到排除范围中的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在路径字段中指定的目录内的对象。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。 如果在列表中选择至少一个文件掩码，则此按钮可用。 单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从扫描中排除的对象。应用程序不会扫描名称包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可使 Kaspersky Endpoint Security 删除已排除在扫描之外的文件的选定名称掩码。

如果在列表中选择至少一个文件掩码，则此按钮可用。

单击掩码将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以修改 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在命令行中配置反加密勒索

在命令行中，您可以使用“反加密勒索”任务 (*Anti_Cryptor*) 来管理反加密勒索。

默认情况下，“反加密勒索”任务不运行。您可以手动启动和停止该任务。

您可以通过编辑“反加密勒索”预定义任务的设置来配置“反加密勒索”设置。

“反加密勒索”任务设置

设置	描述	值
ActionOnDetect	启用不受信任主机阻止。	`Block`（默认值）— 启用不受信任主机阻止。 `Notify` — 禁用不受信任主机阻止。
`BlockTime`	不受信任设备被阻止的时长（分钟）。 如果受到危害的主机被阻止，且您更改了 `BlockTime` 设置的值，则对该主机的阻止时间不会变动。阻止时间不是动态值，在阻止时进行计算。	从 1 到 4294967295 的整数。 默认值：30。
`UseExcludeMasks`	对 `ExcludeMasks.item_#` 设置指定的对象启用保护范围排除项。 仅当为 `ExcludeMasks.item_#` 设置指定一个值后，此设置才适用。	`Yes` — 从保护范围中排除由 `ExcludeMasks.item_#` 设置指定的对象。 `No`（默认值）— 不从保护范围中排除由 `ExcludeMasks.item_#` 设置指定的对象。
`ExcludeMasks.item_#`	按名称或掩码将对象排除在保护范围之	默认值为未定义。

	外。您可以使用此设置来按名称从指定的保护范围中排除单个文件，或者使用 Shell 格式的掩码一次性排除多个文件。 在为此设置指定值之前，请确保已启用 `UseExcludeMasks` 设置。 如果要指定多个掩码，请在具有新索引的新行上指定每个掩码。	
[ScanScope.item_#] 部分包含由应用程序保护的范围。对于“反加密勒索”任务，您需要至少指定一个保护范围；只能指定共享目录。 您可以按任意顺序指定多个“[ScanScope.item_#]”部分。应用程序将按索引升序处理范围。 [ScanScope.item_#] 部分包含以下设置：		
`AreaDesc`	保护范围的说明；包含有关保护范围的其他信息。	默认值：`All shared directories`。
`UseScanArea`	启用对指定范围的保护。要运行任务，请启用至少一个范围的保护。	`Yes`（默认值）- 保护指定的范围。 `No` - 不保护指定的范围。
`AreaMask.item_#`	保护范围限制。在保护范围内，应用程序仅保护使用 shell 格式的掩码指定的对象。 您可以按任意顺序指定多个 `AreaMask.item_#` 项目。应用程序将按索引升序处理范围。	默认值：`*`（保护所有对象）
路径	包含要保护的对象的目录的路径。	< 本地目录的路径 > – 保护可通过 SMB/NFS 访问的本地目录。您可以使用掩码指定路径。 您可以用 `*`（星号）字符来创建文件或目录名称掩码。 您可以指定单个 `*` 字符来表示文件或目录名称中 `/` 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 `*` 字符来表示文件或目录名称中的任意一组字符（包括空集和 `/` 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 `**` 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 可以使用单个 `?` 字符表示文件名或目录名中的任意一个字符。 `AllShared`（默认值）- 保护可通过 SMB/NFS 访问的所有资源。

		Shared:SMB – 保护可通过 SMB 访问的资源。 Shared:NFS – 保护可通过 NFS 访问的资源。
[ExcludedFromScanScope.item_#] 部分包含要从所有 [ScanScope.item_#] 部分中排除的对象。与任何 [ExcludedFromScanScope.item_#] 部分的规则匹配的对象不会被扫描。[ExcludedFromScanScope.item_#] 部分的格式类似于 [ScanScope.item_#] 部分的格式。您可以按任意顺序指定多个 [ExcludedFromScanScope.item_#] 部分。应用程序将按索引升序处理范围。 [ExcludedFromScanScope.item_#] 部分包含以下设置：		
AreaDesc	保护排除范围的说明，其中包含有关排除范围的其他信息。	默认值：All objects。
UseScanArea	从保护中排除指定的范围。	Yes（默认值）- 将指定范围排除在保护之外。 No - 不将指定范围排除在保护之外。
AreaMask.item_#	保护排除范围的限制。在排除范围中，应用程序仅排除使用 shell 格式的掩码指定的对象。 您可以按任意顺序指定多个 AreaMask.item_# 项目。应用程序将按索引升序处理范围。	默认值：*（排除所有对象）。
路径	包含从保护中排除的对象的目录的路径。	< 本地目录的路径 > – 从保护中排除指定目录中的对象。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 Mounted:NFS – 从保护中排除使用 NFS 协议在客户端设备上挂载的远程目录。

		`Mounted:SMB` – 从保护中排除使用 Samba 协议在客户端设备上挂载的远程目录。 `AllRemoteMounted` – 从保护中排除使用 Samba 和 NFS 协议挂载在客户端设备上的所有远程目录。

管理被阻止的设备

在保护设备免受网络威胁和远程恶意加密的同时，Kaspersky Endpoint Security 可以阻止其操作被视为恶意的远程设备：

- 如果检测到恶意加密，应用程序将阻止远程设备访问受保护设备的共享网络目录。
- 一旦检测到受保护设备上出现网络攻击尝试，应用程序就会阻止来自攻击设备的网络流量。

您可以在“网络威胁防护”和“针对远程恶意加密的防护”设置中更改阻止持续时间。指定时间一过，应用程序就会解除对设备的阻止。

如果您使用命令行来管理应用程序，则可以使用管理被阻止设备的命令查看由于该应用程序在设备上运行而被阻止的设备的列表，并在阻止时间到期之前手动解除对这些设备的阻止。除 *检测到网络攻击*和 *检测到加密*事件外，Kaspersky Security Center 不提供用于监控和管理被阻止设备的工具。

-H 前缀表示该命令属于用于管理被“反加密勒索”和“网络威胁保护”阻止的设备的命令组。

The kesl-control --get-blocked-hosts 命令

该命令可让您将被阻止设备的列表输出到控制台。

命令语法

```
kesl-control [-H] --get-blocked-hosts
```

The kesl-control --allow-hosts 命令

该命令可让您解除对被阻止设备的阻止。

命令语法

```
kesl-control [-H] --allow-hosts <地址>
```

参数和键

<地址> 是设备或子网的 IP 地址（IPv4/IPv6，包括缩写形式的地址）。您可以指定设备或子网的多个 IP 地址，用空格分隔。

要查看受阻止设备的列表，请执行以下命令：

```
kesl-control --get-blocked-hosts
```

命令执行的结果是，应用程序将被阻止设备的列表输出到控制台。

要解除阻止设备，请执行以下命令：

```
kesl-control --allow-hosts <地址>
```

其中 < 地址 > 是设备或子网的一个或多个 IP 地址（IPv4/IPv6，包括缩写形式的地址）。您可以指定设备或子网的多个 IP 地址，用空格分隔。

命令执行的结果是，应用程序解除对指定设备的阻止。

```
例如：
IPv4 地址：
dec - 192.168.0.1
dec - 192.168.0.0/24
IPv6 地址：
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::
```

应用程序控制

应用程序控制组件允许您管理受保护设备上应用程序的启动。“应用程序控制”通过限制用户对应用程序的访问来降低设备感染的风险。

要使用该组件，需要包含相应功能的授权许可。

KESL 容器不支持此功能。

应用程序启动受*应用程序控制规则*的约束。

应用程序控制组件有两种运行模式可选：

- *拒绝列表*。在此模式下，Kaspersky Endpoint Security 允许所有用户启动应用程序控制规则中未指定的任何应用程序。默认情况下，应用程序控制组件在此模式下运行。
- *允许列表*。在此模式下，Kaspersky Endpoint Security 禁止所有用户启动应用程序控制规则中未指定的任何应用程序。

因此，如果创建了最大限度的“应用程序控制”规则，Kaspersky Endpoint Security 将禁止启动所有未经组织的本地网络管理员验证的新应用程序，但可以确保操作系统和用户履行工作职责所需的经过验证的应用程序的性能。

Kaspersky Security Center 管理员或在应用程序中分配了管理员角色的本地用户可以在 root 账户下使用“应用程序控制”允许或拒绝进程启动。

默认情况下，“应用程序控制”被禁用。您可以启用或禁用“应用程序控制”，还可以配置该组件的操作设置：

- 选择应用程序控制模式：*允许列表*或*拒绝列表*。
- 为各个模式创建应用程序控制规则。
- 选择 Kaspersky Endpoint Security 在检测到尝试启动符合规则的应用程序时将执行的操作：*应用规则*或*测试规则*并通知尝试启动符合规则的应用程序的行为。

您可以使用“清查”任务接收有关受保护设备上安装的应用程序的信息。

应用程序控制任务不能控制 Kaspersky Endpoint Security 不支持的解释器启动脚本，也不能控制启动未通过命令行传递给解释器的脚本。Kaspersky Endpoint Security 支持以下解释器：python、perl、bash、ssh。

如果应用程序控制规则允许解释器启动，Kaspersky Endpoint Security 不会阻止从该解释器启动的脚本。如果应用程序控制规则禁止启动解释器命令行中指定的至少一个脚本，Kaspersky Endpoint Security 会阻止解释器命令行中指定的所有脚本。排除：cat script.py | python。

关于应用程序控制规则

*应用程序控制规则*是一组设置，其中包含规则触发条件以及触发规则时应用程序控制组件的操作（启动应用程序时允许或阻止用户）：

- 属于应用程序类别的应用程序。*应用程序类别*是一组具有共同特征的应用程序。例如，包含已安装应用程序的可执行文件的类别或操作所需的应用程序类别，其中包括组织使用的一组标准应用程序。每个类别只能在一条规则中使用。

  Kaspersky Endpoint Security 不支持使用 Kaspersky Security Center 的 KL 类别。

- 允许或禁止选定的用户和/或用户组运行应用程序。您可以指定用户和/或用户组，以允许或不允许他们运行指定类别的应用程序。

- 规则触发条件。条件由以下对应关系表示："条件类型 - 条件标准 - 条件值"。根据规则的触发条件，Kaspersky Endpoint Security 可能为应用程序应用规则，也可能不会。这些规则使用包含条件和排除条件：

  - *包含条件*。如果应用程序符合至少一个包含条件，则 Kaspersky Endpoint Security 将规则应用于应用程序。

  - *排除条件*。如果应用程序符合至少一个排除条件或不符合任何包含条件，则 Kaspersky Endpoint Security 不将规则应用于应用程序。

  规则触发条件是使用以下条件创建的：

  - 应用程序的可执行文件的名称。

  - 包含应用程序可执行文件的目录的名称。

  - 应用程序可执行文件的哈希值。仅允许 SHA256。

  对于条件中使用的每个标准，必须指定一个值。

  您可以使用掩码指定文件和目录的名称。

  可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。

  可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如：`/dir/*/file*/` 或 `/dir/file*/`。

  可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 /）。

  如果正在启动的应用程序的设置与包含条件中指定的条件匹配，则会触发规则。在这种情况下，Kaspersky Endpoint Security 将执行规则中指定的操作。如果应用程序设置与排除条件中指定的条件匹配，则 Kaspersky Endpoint Security 不会控制应用程序的启动。

应用程序控制规则可以具有以下*操作状态*之一：

- *已启用*：规则已启用，Kaspersky Endpoint Security 对应用程序控制应用此规则。

- *已禁用*：规则已禁用，不用于应用程序控制。

- *Test* – Kaspersky Endpoint Security 允许启动符合规则标准的应用程序，但在报告中记录有关这些应用程序启动的信息。

规则操作状态的优先级高于规则中指定的操作的优先级。

在 Web Console 中配置“应用程序控制”

在 Web Console 中，您可以在策略属性中配置应用程序控制设置（**应用程序设置→ 安全控制 → 应用程序控制**）。

应用程序控制组件设置

设置	描述
应用程序控制已启用/已禁用	此切换开关可启用或禁用应用程序控制。 默认情况下，切换开关关闭。
应用程序启动被规则阻止时的操作	Kaspersky Endpoint Security 在检测到与配置规则匹配的应用程序启动尝试时执行的操作： • **测试规则**。如果选择此选项，Kaspersky Endpoint Security 会测试规则并生成有关与规则匹配的应用程序启动尝试的事件。 • **应用规则**（默认值）。如果选择此选项，Kaspersky Endpoint Security 将应用应用程序控制规则，并执行规则中指定的操作。
应用程序控制模式	应用程序控制任务操作模式： • **允许列表**。如果选择此选项，Kaspersky Endpoint Security 会阻止所有用户启动除应用程序控制规则中指定的应用程序之外的任何应用程序。 • **拒绝列表**（默认值）。如果选择此选项，Kaspersky Endpoint Security 会允许所有用户启动除应用程序控制规则中指定的应用程序之外的任何应用程序。
应用程序控制规则	单击“**配置规则**”链接将打开“应用程序控制规则”窗口。
应用规则	在下拉列表中，您可以选择如何添加规则： • **使用策略规则替换本地规则**。如果选择此项，应用程序将仅应用策略中指定的规则。 • **将策略规则添加到本地规则**（默认值）。如果选择此项，应用程序将把策略中指定的规则与受保护设备上配置的本地规则一起应用。

“应用程序控制规则”窗口

“**应用程序控制规则**”表具有包含每种操作模式规则的选项卡：**拒绝列表(已激活)**和**允许列表**。默认情况下，“应用程序控制规则”表的两个选项卡均为空。

应用程序控制规则设置

设置	描述
Category	规则使用的应用程序类别的名称。
状态	应用程序控制规则的操作状态： • *已启用* – 该规则已启用，应用程序控制在操作期间应用此规则。

	• *已禁用* – 该规则已禁用，应用程序控制在运行期间不会使用此规则。 • *测试* – 应用程序控制允许启动符合规则标准的应用程序，但在报告中记录有关这些应用程序启动的信息。

您可以添加、修改和删除应用程序控制规则。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

“应用程序控制规则”窗口

在此窗口中，您可以配置应用程序控制规则的设置。

配置应用程序控制规则

设置	描述
规则描述	应用程序控制规则的说明。
状态	您可以选择应用程序控制规则的操作状态： • *已启用* – 该规则已启用，应用程序控制在操作期间应用此规则。 • *已禁用* – 该规则已禁用，应用程序控制在运行期间不会使用此规则。 • *测试* – 应用程序控制允许启动符合规则标准的应用程序，但在报告中记录有关这些应用程序启动的信息。
Category	单击“**选择类别**”链接将打开“应用程序类别”窗口。
用户及其权限	该表包含应用程序控制规则所适用的用户或用户组，以及分配给他们的访问权限类型的列表，其中包含以下列： • **用户或组名称** – 应用程序控制规则应用到的用户名称或用户组名称。 • **访问** – 访问类型（允许或阻止启动应用程序）。此切换开关用于切换访问类型：**允许**启动应用程序或**阻止**启动应用程序。 您可以添加、编辑和删除用户或用户组。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。

“应用程序类别”窗口

在此窗口中，您可以为应用程序控制规则添加新类别或配置类别设置。

Kaspersky Endpoint Security 不支持使用 Kaspersky Security Center 的 KL 类别。

应用程序控制类别

设置	Description
类别名称	已添加应用程序类别的搜索栏。
添加	单击该按钮启动类别创建向导。按照向导的说明进行操作。
编辑	单击此按钮将打开类别属性窗口，您可以在其中更改类别设置。
Remove	单击该按钮可删除选定的类别。无法删除**"黄金映像（本地）"**类别。

"选择用户或组"窗口

在此窗口中，可以指定要为其配置规则的本地或域用户或用户组。

配置应用程序控制规则

设置	描述
手动	如果选择此选项，请在下面的字段中输入应用程序控制规则将适用的本地或域用户或用户组的名称。
组或用户列表	如果选择此选项，您可以在搜索字段中输入搜索条件来搜索应用程序控制规则将适用的用户或用户组的名称，也可以在下面的列表中选择用户组名称。

在管理控制台中配置应用程序控制

在管理控制台中，您可以在策略属性中配置应用程序控制设置（**安全控制 → 应用程序控制**）。

应用程序控制组件设置

设置	Description
启用应用程序控制	该复选框将启用应用程序控制组件。 默认情况下，清除此复选框。
检测到应用程序启动尝试时的操作	Kaspersky Endpoint Security 在检测到与配置规则匹配的应用程序启动尝试时执行的操作： • **应用规则**（默认值）。如果选择此选项，Kaspersky Endpoint Security 将应用应用程序控制规则，并执行规则中指定的操作。 • **测试规则**。如果选择此选项，Kaspersky Endpoint Security 会测试规则并生成有关与规则匹配的应用程序启动尝试的事件。
应用程序控制模式	应用程序控制任务操作模式： • **允许列表**。如果选择此选项，Kaspersky Endpoint Security 会阻止所有用户启动除应用程序控制规则中指定的应用程序之外的任何应用程序。

	• **拒绝列表**（默认值）。如果选择此选项，Kaspersky Endpoint Security 会允许所有用户启动除应用程序控制规则中指定的应用程序之外的任何应用程序。
应用程序控制规则	这组设置包含**配置**按钮。单击此按钮可打开应用程序控制规则窗口。
应用规则	在下拉列表中，您可以选择如何添加规则： • **使用策略规则替换本地规则**。如果选择此项，应用程序将仅应用策略中指定的规则。 • **将策略规则添加到本地规则**（默认值）。如果选择此项，应用程序将把策略中指定的规则与受保护设备上配置的本地规则一起应用。

“应用程序控制规则”窗口

应用程序控制规则表包含应用程序控制组件使用的规则。默认情况下，应用程序控制规则表为空。

应用程序控制规则设置

设置	Description
类别名称	规则使用的应用程序类别的名称。
状态	应用程序控制规则的操作状态： • *已启用* – 该规则已启用，应用程序控制在操作期间应用此规则。 • *已禁用* – 该规则已禁用，应用程序控制在运行期间不会使用此规则。 • *测试* – 应用程序控制允许启动符合规则标准的应用程序，但在报告中记录有关这些应用程序启动的信息。 您可以在“添加新规则/编辑规则”窗口中更改规则状态。

您可以添加、修改和删除应用程序控制规则。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

“添加规则”窗口

在此窗口中，您可以配置应用程序控制规则的设置。

添加应用程序控制规则

设置	Description
Description	应用程序控制规则的说明。
规则状态	在下拉列表中，您可以选择应用程序控制规则的状态：

	• *已启用* – 该规则已启用，应用程序控制在操作期间应用此规则。 • *已禁用* – 该规则已禁用，应用程序控制在运行期间不会使用此规则。 • *测试* – 应用程序控制允许启动符合规则标准的应用程序，但在报告中记录有关这些应用程序启动的信息。
Category	这组设置包含**配置**按钮。单击此按钮可打开"应用程序类别"窗口。
用户及其权限	该表包含应用程序控制规则所适用的用户或用户组，以及分配给他们的访问权限类型的列表，其中包含以下列： • **用户或组名称** – 应用程序控制规则应用到的用户名称或用户组名称。 • **访问权限** – 访问权限的类型：**允许**启动应用程序或**阻止**启动应用程序。 您可以添加、编辑和删除用户或用户组。 单击"**删除**"按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。

"应用程序类别"窗口

在此窗口中，您可以为应用程序控制规则添加新类别或配置类别设置。

Kaspersky Endpoint Security 不支持使用 Kaspersky Security Center 的 KL 类别。

应用程序控制类别

设置	Description
类别名称	添加的应用程序控制类别的列表。
添加	单击该按钮启动类别创建向导。按照向导的说明进行操作。
编辑	单击此按钮将打开类别属性窗口，您可以在其中更改类别设置。

"用户或组"窗口

在此窗口中，可以指定要为其配置规则的本地或域用户或用户组。

添加应用程序控制规则

设置	描述
类型	应用程序控制规则应用到的**用户**或**组**。
用户或组名称	要应用应用程序控制规则的用户或用户组的名称。
Access	访问权限类型：**允许**启动应用程序或**阻止**启动应用程序。

在命令行中配置应用程序控制

在命令行中，您可以使用“应用程序控制”预定义任务 (*Application_Control*) 来管理应用程序控制。

默认情况下，“应用程序控制”任务不运行。您可以手动启动和停止任务。

您可以通过编辑“应用程序控制”预定义任务的设置来配置设备上的应用程序控制。

如果您更改允许的应用程序列表，或者禁止启动所有应用程序或影响 Kaspersky Endpoint Security 操作的应用程序，则在使用配置文件或使用命令行键修改任务设置时，运行带有 `--accept` 标记的 `kesl-control --set-settings` 命令。

您还可以使用应用程序控制命令来配置应用程序控制：

- 创建和编辑类别列表。
- 查看在应用程序中创建的类别列表。
- 配置应用程序控制规则列表。

应用程序控制任务设置

该表介绍了可为“应用程序控制”任务指定的所有设置的全部可用值以及默认值。

应用程序控制任务设置

设置	描述	值
`AppControlMode`	“应用程序控制”任务操作模式。	`AllowList` – Kaspersky Endpoint Security 阻止用户启动应用程序控制规则中未指定的任何应用程序。 `DenyList`（默认值）– Kaspersky Endpoint Security 允许用户启动应用程序控制规则中未指定的任何应用程序。
`AppControlRulesAction`	Kaspersky Endpoint Security 在检测到与配置规则匹配的应用程序启动尝试时执行的操作：	`ApplyRules`（默认值）– Kaspersky Endpoint Security 会应用应用程序控制规则，并执行规则中指定的操作。 `TestRules` – Kaspersky Endpoint Security 测试规则，并生成有关检测到满足规则的应用程序的事件。
[Categories.item_#] 部分包含以下设置：		
`Name`	应用规则的应用程序类别的名称。	
`UseIncludes`	使用包含条件来触发规则。	`Yes` - 如果应用程序匹配至少一个包含条件，则将规则应用于应用程序。 `No`（默认值）- 即使应用程序匹配包含条件，也不将规则应用于应用程序。

`IncludeFileNames.item_#`	触发规则的可执行文件的名称。	您可以使用掩码指定文件名。 可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。 可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如：`/dir/*/file*/` 或 `/dir/file*/`。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 /）。
`IncludeFolders.item_#`	包含触发规则的应用程序可执行文件的目录的名称。	您可以使用掩码指定路径名称。 可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。 可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如：`/dir/*/file*/` 或 `/dir/file*/`。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 /）。
`IncludeHashes.item_#`	触发规则的可执行文件的 SHA256 哈希值。	仅允许 SHA256。
`UseExcludes`	使用排除条件来触发规则。	`Yes` - 如果应用程序匹配至少一个排除条件或不匹配任何包含条件，则不将规则应用于应用程序。 `No`（默认值）- 即使应用程序符合至少一个排除条件，也将规则应用于应用程序。
`ExcludeFileNames.item_#`	触发规则的可执行文件的名称。	您可以使用掩码指定文件名。 可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。 可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如：`/dir/*/file*/` 或 `/dir/file*/`。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 /）。
`ExcludeFolders.item_#`	包含触发规则的应用程序可执行文件的目录的名称。	您可以使用掩码指定路径名称。

		可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。 可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如：`/dir/*/file*/` 或 `/dir/file*/`。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 /）。
`ExcludeHashes.item_#`	触发规则的可执行文件的 SHA256 哈希值。	仅允许 SHA256。
[AllowListRules.item_#] 部分包含 *AllowList* 操作模式的“应用程序控制”规则列表。 每个 [AllowListRules.item_#] 部分均包含以下设置：		
`Description`	应用程序控制规则的说明。	
`AppControlRuleStatus`	应用程序控制规则的操作状态：	`On`（默认值）：规则已启用，Kaspersky Endpoint Security 对“应用程序控制”应用此规则。 `Off`：该规则不用于“应用程序控制”。 `Test` – Kaspersky Endpoint Security 允许启动规则所覆盖的应用程序，但在报告中记录有关这些应用程序启动的信息。
`Category`	应用规则的应用程序类别的名称。 您可以指定“黄金镜像”类别。	
[AllowListRules.item_#.ACL.item_#] 部分包含允许或拒绝运行应用程序的用户列表。		
`Access`	分配给一个用户或用户组的访问类型。	`Allow`（默认值）- 允许运行应用程序。 `Block` – 拒绝运行应用程序。
`Principal`	要应用应用程序控制规则的用户或用户组。	`\Everyone`（默认值）：规则适用于所有用户。 `<用户名>`：规则所适用的用户的名称。 `@<组名称>`：规则所适用的用户组的名称。
[DenyListRules.item_#] 部分包含 *DenyList* 操作模式的“应用程序控制”规则列表。 每个 [DenyListRules.item_#] 部分均包含以下设置：		
`Description`	应用程序控制规则的说明。	
`AppControlRuleStatus`	应用程序控制规则的操作状态：	`On`（默认值）：规则已启用，Kaspersky Endpoint Security 对“应用程序控制”应用此规则。 `Off`：该规则不用于“应用程序控制”。 `Test` – Kaspersky Endpoint Security 允许启动规则所覆盖的应用程序，但在报告中记录有关这些应用程序启动的信息。

Category	应用规则的已创建应用程序类别的名称。 您可以指定"黄金镜像"应用程序列表作为一个类别。	
[DenyListRules.item_#.ACL.item_#] 部分包含允许或拒绝运行应用程序的用户列表。		
Access	分配给一个用户或用户组的访问类型。	Allow – 允许应用程序启动。 Block（默认值）– 不允许应用程序启动。
Principal	要应用应用程序控制规则的用户或用户组。	\Everyone（默认值）：规则适用于所有用户。 < 用户名 >：规则所适用的用户的名称。 @< 组名称 >：规则所适用的用户组的名称。

创建和编辑类别列表

您可以通过两种方式创建新类别：

- 使用"kesl --set-settings"命令和应用程序控制任务设置配置文件（Application_Control）；
- 使用"kesl --set-categories"命令和类别设置配置文件。

要创建应用程序类别，请运行以下命令：

```
kesl-control --set-categories --file < 配置文件路径 >
```

其中：

--file < 配置文件路径 > – 包含类别设置的配置文件的路径。

包含类别设置的文件必须具有以下结构：

```
[
  {
    "Exclude": ["(FilePath like < 可执行文件完整路径 >)", "(FileHash == < 可执行文件哈希 >)"],
    "GUID" : "< 唯一类别 ID >",
    "Include" : [ "(FilePath like < 可执行文件完整路径 >)", "(FileHash == < 可执行文件哈希 >)"
   ],
    "Name" : "< 类别名称 1 >"
  },
  {
    "Exclude": ["(FilePath like < 可执行文件完整路径 >)", "(FileHash == < 可执行文件哈希 >)"],
    "GUID" : "< 唯一类别 ID >",
    "Include" : [ "(FilePath like < 可执行文件完整路径 >)", "(FileHash == < 可执行文件哈希 >)"
   ],
    "Name" : "< 类别名称 2 >"
  }
]
```

要在"排除"和"包含"字段中指定文件名，您可以使用掩码。

可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。

可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如：`/dir/*/file*/` 或 `/dir/file*/`。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 `/`）。

`Name` 设置是必需的。如果不指定类别的名称，则不会创建或删除该类别。`GUID` 设置也需要。如果不指定它，则会显示错误消息，不会创建类别。指定的 `GUID` 设置不得有连字符。

要编辑已创建的应用程序类别的列表，请运行以下命令：

```
kesl-control --set-categories [--names <类别名称 1> <类别名称 2> ... <类别名称 N>] [--file <配置文件路径>]
```

其中：

- `<类别名称 1> <类别名称 2> ... <类别名称 N>` – 您想要更改其信息的类别的名称。如果要更改有关多个类别的信息，请指定类别的名称，用空格分隔。如果不指定类别名称，则现有类别会被删除并从指定文件创建新类别。
- `--file <配置文件路径>` – 包含类别设置的配置文件的路径。

查看已创建类别的列表

在命令行中，您可以使用应用程序控制管理命令查看已创建的应用程序类别列表。

创建的类别列表包含以下类别：

- Kaspersky Security Center 中创建的类别。
- 使用命令行在应用程序控制任务设置中添加的类别。
- 使用“清查”任务（在 Kaspersky Endpoint Security 中或使用命令行）创建的“GoldenImage”类别。

要查看已创建的应用程序类别的列表，请运行以下命令：

```
kesl-control --get-categories [--file <配置文件路径>] [--json]
```

其中：

- `--file <配置文件路径>` – 将输出设置的 JSON 配置文件的完整路径。
- 指定 `--json`，则以 JSON 格式输出设置。如果 --json 键被省略，则设置以 INI 格式输出。

Kaspersky Endpoint Security 显示以下有关每个应用程序类别的信息：

- 类别的唯一标识符 (GUID)

- 类别名称
- 用于触发规则的包含条件列表
- 用于触发规则的排除条件列表

要查看已创建的应用程序类别的列表，请执行以下命令：

```
kesl-control --get-categories [--names <类别名称 1> <类别名称 2> ... <类别名称 N>] [--file <配置文件路径>] [--json]
```

其中：

- <类别名称 1> <类别名称 2> ... <类别名称 N> – 您想要查看其信息的类别的名称。如果要查看有关多个类别的信息，请指定类别的名称，用空格分隔。
- --file <配置文件路径> – 将导出类别列表的JSON 配置文件的完整路径。
- 指定 --json，则以 JSON 格式输出设置。如果 --json 键被省略，则设置以 INI 格式输出。

如果在用于包含或排除规则触发条件的 [Categories.item_#] 部分的"应用程序控制"任务设置中指定指向应用程序文件或包含可执行文件的目录的符号链接，那么在查看这些条件的类别列表时，将显示符号链接所指向的源路径。

配置应用程序控制规则列表

要查看应用程序控制规则的列表，请运行以下命令：

```
kesl-control --get-settings 21 [--file <配置文件的路径>] [--json]
```

其中：

--file <配置文件路径> – 将导出设置的配置文件的完整路径。

--json：以 JSON 格式输出数据。

Kaspersky Endpoint Security 显示以下有关应用程序控制规则的信息：

- 应用程序控制任务操作模式；
- 应用程序控制在检测到尝试启动与配置规则匹配的应用程序时执行的操作：
- 应用程序控制规则的说明（如有）；
- 应用程序控制规则的操作状态；
- 规则应用的应用程序类别的名称；
- 分配给一个用户或用户组的访问类型；

- 要应用应用程序控制规则的用户或用户组。

要编辑应用程序类别和应用程序控制规则的列表，请运行以下命令：

```
kesl-control --set-settings 21 --file <配置文件的路径> [--json]
```

其中：

`--file <配置文件路径>` – 将从其导入设置的配置文件的完整路径。

`--json` – 从 JSON 文件导入数据。

要删除应用程序类别和应用程序控制规则的列表，请运行以下命令：

```
kesl-control --set-settings 21 --set-to-default
```

清查

“清查”任务提供有关客户端设备上存储的所有应用程序可执行文件的信息。例如，获取设备上安装的应用程序的相关信息对于创建应用程序控制规则非常有用。

KESL 容器不支持此功能。

要使用该任务，需要包含相应功能的授权许可。

您还可以配置以下清查设置：

- 选择应用程序在清查时将在设备上检测的对象类型（文件、脚本）。
- 启用或禁用将清查扫描任务在设备上检测到的应用程序添加到“黄金镜像”类别。
- 配置清查范围（搜索可执行应用程序文件的目录路径）。
- 配置清查排除项。

Web Console 中的清查

在 Web Console 中，您可以使用“*清查*”任务对受保护设备的应用程序执行清查。

您可以创建并运行“清查”用户任务。您可以通过编辑这些任务的设置来配置“清查”设置。

Kaspersky Security Center 数据库最多可以存储有关 150,000 个已处理文件的信息。达到此记录数时，将不会再处理新文件。要恢复“清查”任务，请从安装了 Kaspersky Endpoint Security 的设备中删除由于之前的清查而在 Kaspersky Security Center 数据库中注册的文件。

清查任务设置

设置	描述
向“黄金镜像”类别添加文件	该复选框用于启用或禁用将“清查”任务在设备上检测到的应用程序添加到“黄金镜像”类别。如果选中此复选框，则可以在应用程序控制规则中使用“黄金镜像”类别。 默认情况下，清除此复选框。
扫描所有可执行文件	此复选框启用或禁用可执行文件扫描。 默认选中该复选框。
扫描二进制文件	此复选框启用或禁用二进制文件扫描（扩展名为 elf、java 和 pyc）。 默认选中该复选框。
扫描脚本	此复选框启用或禁用脚本扫描。 默认选中该复选框。
清查范围	该表包含应用程序扫描的清查范围。应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个清查范围 – /usr/bin。 您可以在表中添加、配置、删除、上移或下移清查范围。

单击“**下移**”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

单击扫描范围名称将打开“**<扫描范围名称>**”窗口。在此窗口中，可以修改所选扫描范围的设置。

点击“**添加**”按钮将打开“**<新建扫描范围>**”窗口。在此窗口中，可以定义新的扫描范围。

“添加扫描范围”窗口

在此窗口中，您可以为清查任务添加和配置扫描范围。

清查范围设置

设置	Description
范围名称	用于输入清查范围名称的字段。此名称将显示在“**扫描设置**”部分的表格中。 该输入字段不能为空。
使用此范围	此复选框用于启用或禁用在执行任务时扫描此范围。 如果选中此复选框，则应用程序在运行任务时将处理此清查范围。 如果清除此复选框，则应用程序在运行任务时不处理此清查范围。您可以在以后选中此复选框来在任务设置中包括此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定要包含在清查范围中的本地目录路径的输入字段。您可以使用掩码指定路径。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该字段不能为空。默认情况下指定 / 路径 — 应用程序扫描本地文件系统的所有目录。
掩码	此列表包含应用程序在运行任务时扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”部分

在“清查”任务的“**排除范围**”部分中，您可以配置要从扫描中排除的范围。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加排除范围”窗口

在此窗口中，您可以为清查任务添加和配置扫描排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框启用或禁用在执行任务时排除范围的功能。 如果选中此复选框，则应用程序在任务执行期间将排除此范围。 如果清除此复选框，则应用程序将在任务执行期间包含此范围。您可以在以后选中此复选框来从扫描任务中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定在清查中排除的本地目录路径的输入字段。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该字段不能为空。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

管理控制台中的清查

在 Kaspersky Security Center 管理控制台中，您可以使用“*清查*”任务对受保护设备的应用程序执行清查。

您可以创建并运行“清查”用户任务。您可以通过编辑任务的设置来配置扫描设置。

Kaspersky Security Center 数据库最多可以存储有关 150,000 个已处理文件的信息。达到此记录数时，将不会再处理新文件。要恢复“清查”任务，请从安装了 Kaspersky Endpoint Security 的设备中删除由于之前的清查而在 Kaspersky Security Center 数据库中注册的文件。

清查任务设置

设置	描述
向“黄金镜像”类别添加文件	该复选框用于启用或禁用将“清查”任务在设备上检测到的应用程序添加到“黄金镜像”类别。如果选中此复选框，则可以在应用程序控制规则中使用“黄金镜像”类别。 默认情况下，清除此复选框。
扫描所有可执行文件	此复选框启用或禁用可执行文件扫描。 默认选中该复选框。
扫描二进制文件	此复选框启用或禁用二进制文件扫描（扩展名为 elf、java 和 pyc）。 默认选中该复选框。
扫描脚本	此复选框启用或禁用脚本扫描。 默认选中该复选框。
清查范围	这组设置包含**配置**按钮。单击此按钮将打开扫描范围窗口。

在“清查”任务的“**排除范围**”部分中，您还可以配置要从扫描中排除的范围。

“扫描范围”窗口

该表包含扫描范围：应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个扫描范围 - /usr/bin。

清查任务的扫描范围设置

设置	Description
范围名称	扫描范围名称。
Path	应用程序扫描的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“下移”按钮可将所选项目在表中向下移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击“上移”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

<新扫描范围>窗口

在此窗口中，您可以为清查任务添加和配置扫描范围。

清查范围设置

设置	Description
扫描范围名称	用于输入扫描范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于启用或禁用在执行任务时扫描此范围。 如果选中此复选框，则应用程序在运行任务时将处理此扫描范围。 如果清除此复选框，则应用程序在运行任务时不处理此扫描范围。您可以在以后选中此复选框来在任务设置中包括此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定要包含在扫描范围中的本地目录路径的输入字段。您可以使用掩码指定路径。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该字段不能为空。
掩码	此列表包含应用程序在运行任务时扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“删除”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击添加按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除项”部分

扫描排除项设置

设置组	Description
排除范围	这组设置包含配置按钮。单击此按钮将打开排除范围窗口。在此窗口中，您可以定义要从监控中排除的范围列表。

“排除范围”窗口

此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

<新建扫描范围>窗口

在此窗口中，您可以为清查任务添加和配置扫描排除范围。

排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框启用或禁用在执行任务时排除范围的功能。 如果选中此复选框，则应用程序在任务执行期间将排除此范围。 如果清除此复选框，则应用程序将在任务执行期间包含此范围。您可以在以后选中此复选框来从扫描任务中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定在清查中排除的本地目录路径的输入字段。您可以使用掩码指定路径。该字段不能为空。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。
掩码	该列表包含应用程序从扫描中排除的对象的名称掩码。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在命令行中清查

您可以使用命令行来清查受保护设备上的应用程序，如下所示：

- 借助“Inventory_Scan”*预定义任务*。您可以手动启动或停止该任务，并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。
- 借助用户清查任务（*InventoryScan* 类型的任务）。您可以手动启动、停止、暂停或恢复用户任务，并配置任务计划。

您可以使用“应用程序控制”管理命令来查看“清查”任务完成后在设备上检测到的应用程序列表。

清查任务设置

该表介绍了可为清查任务指定的所有设置的全部可用值以及默认值。

清查任务设置

设置	描述	值
`ScanScripts`	启用脚本扫描。	`Yes`（默认值）- 扫描脚本。 `No` - 不扫描脚本。
`ScanBinaries`	启用二进制文件扫描（elf、java 和 pyc）。	`Yes`（默认值）- 扫描二进制文件。 `No` - 不扫描二进制文件。
`ScanAllExecutable`	允许使用可执行位扫描文件。	`Yes`（默认值）- 使用可执行位扫描文件。 `No` - 不使用可执行位扫描文件。
`CreateGoldenImage`	将“清查”任务在设备上检测到的应用程序添加到“黄金镜像”类别。如果 `CreateGoldenImage=Yes`，则可以在应用程序控制规则中使用“黄金映像”应用程序类别。	`Yes` – 将检测到的应用程序添加到“黄金映像”应用程序类别。 `No`（默认值）– 不将检测到的应用程序添加到“黄金映像”应用程序类别。
[ScanScope.item_#] 部分包含以下设置：		

AreaDesc	清查范围的说明；包含有关清查范围的其他信息。使用此设置指定的字符串的最大长度为 4096 个字符。	默认值：All objects。
UseScanArea	启用对指定清查范围的扫描。要运行任务，请启用至少一个清查范围的扫描。	Yes（默认值）- 扫描指定的清查范围。 No - 不扫描指定的清查范围。
AreaMask.item_#	清查范围限制。在清查范围内，应用程序仅扫描使用 shell 格式的掩码指定的文件。 如果未指定此设置，则应用程序会扫描位于清查范围内的所有对象。您可以为此设置指定多个值。	默认值：*（扫描所有对象）。
Path	包含要扫描的对象的目录的路径。	< 本地目录的路径 > — 扫描指定目录中的对象。 默认值：/usr/bin
[ExcludedFromScanScope.item_#] 部分包含以下设置：		
AreaDesc	清查排除范围的说明；包含有关清查范围的其他信息。	默认值为未定义。
UseScanArea	从清查中排除指定的范围。	Yes（默认值）— 排除指定的范围。 No — 不排除指定的范围。
AreaMask.item_#	使用 shell 掩码限制清查排除范围。 如果未指定此设置，则应用程序将排除清查范围内的所有对象。您可以为此设置指定多个值。	默认值：*（排除所有对象）。
路径	包含要排除的对象的目录的路径。	< 本地目录的路径 > — 从扫描中排除指定目录中的对象。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

查看检测到的应用程序列表

要查看在设备上检测到的应用程序列表，请执行以下命令：

```
kesl-control --get-app-list [--json]
```

其中 `--json` 表示以 JSON 格式输出数据。

Kaspersky Endpoint Security 显示以下有关检测到的应用程序的信息：

- **清查的日期和时间**。执行清查任务的日期和时间
- **应用程序数量**。在设备上检测到的应用程序数量
- 包含以下信息的应用程序列表：
  - **路径**。应用程序的路径。
  - **哈希**。应用程序哈希和。
  - **Type**。应用程序类型。例如，`Script`、`Executable`。
  - **类别**。应用程序所属的类别（如果之前已创建）。您可以使用命令 `kesl-control --get-categories` 查看已创建的应用程序类别列表。

添加新类别时，其信息不会在应用程序列表中自动更新。要更新应用程序列表，您需要重新启动清查任务。

设备控制

*设备控制*组件允许您管理用户对已安装到或已连接到客户端设备的设备（例如，硬盘驱动器、摄像头或 Wi-Fi 模块）的访问。访问管理可保护客户端设备在连接外部设备时免受感染，并防止数据丢失或泄露。

KESL 容器不支持此功能。

当 Kaspersky Endpoint Security 启动时，“设备控制”组件会使用默认设置自动启用。

“设备控制”从以下几个方面来控制用户访问：

- 由“设备控制”分类的**设备类型**，例如打印机、可移动驱动器或 CD/DVD 驱动器。下列其中一种访问模式可应用于每种设备类型：
  - *允许*，允许访问此类型的设备。
  - *阻止*，阻止对此类型设备的访问。
  - *基于总线*：根据用于连接设备的总线的访问模式，允许或阻止对设备的访问。
  - *按规则*：根据访问规则，允许或阻止对设备的访问。*设备访问规则*是用于确定哪些用户可以访问已安装在客户端设备上或与其连接的设备，以及在什么时间访问的一组选项。

    当连接禁止的设备时，应用程序将拒绝规则中指定的用户访问该设备并显示通知。尝试在此设备上读取和写入期间，应用程序会静默阻止规则中指定的用户读取/写入。

    如果您尝试对访问模式设置为“*按照规则*”的设备执行操作，但访问时未找到已激活的规则，则该操作将被阻止。
- **连接总线**。*连接总线*是用于将设备连接到客户端设备的接口（例如 USB 或 FireWire）。下列其中一种访问模式可应用于连接总线：
  - *允许*：允许访问通过此连接总线连接的设备。
  - *阻止*：拒绝访问使用此连接总线连接的设备。

  例如，可能拒绝访问所有通过 USB 连接的设备。

默认情况下，所有设备类型均选择*取决于连接总线*访问模式。连接总线选择*允许*访问模式。“设备控制”相应地授予用户对所有设备的完全访问权限。

以下 Linux 内核不支持通过系统设备驱动程序按设备类型或连接总线阻止设备：3.10、5.14、5.15、5.17、6.1。在这些内核上，在*按规则*访问模式下，仅阻止打开文件和读取目录（即获取文件和目录的名称）。在不支持 fanotify 的系统上，也不支持阻止读取目录。

首次启用“设备控制”时，它会为所有检测到的具有已知设备或总线类型的设备生成一个“*DeviceAllowed*”事件。除非这些设备的控制设置发生变化，否则后续组件运行时不会生成重复事件。

当“设备控制”被禁用时，应用程序将解除对被阻止设备的访问的阻止。

您可以启用、禁用和配置“设备控制”：

- 选择当尝试访问设备控制设置禁止访问的设备时应用程序的操作模式：阻止或仅通知有关访问设备的尝试。
- 根据类型选择设备访问模式。

- 为设备连接时使用的总线选择访问模式。
- 通过将单个设备添加到受信任设备的列表中，将其从“设备控制”范围中移除。*受信任设备*是用户拥有完全访问权限的设备。您可以通过标识符或标识符掩码将设备添加到受信任设备的列表中。您还可以限制对特定 USB 设备的访问或仅访问 USB 驱动器；对其他 USB 设备的访问将被拒绝。

  如果您通过命令行管理应用程序，则可以通过在客户端设备上运行 `kesl-control --get-device-list` 来查看连接设备的 ID。

  如果您通过 Kaspersky Security Center 管理应用程序，则有关安装在客户端设备上或与其连接的设备的信息可以发送到管理服务器。默认情况下，信息共享功能处于启用状态。

  > 如果客户端设备受活动策略的控制并与网络代理同步（按照网络代理策略属性中指定的频率执行，默认情况下每 15 分钟一次），则会传输有关设备的信息。

- 定义设备的访问计划：仅硬盘驱动器、可移动驱动器、软盘驱动器和 CD/DVD 驱动器。

  > 在常规应用程序设置中，如果禁用在扫描期间阻止对文件进行访问，则您无法使用设备访问计划来阻止对设备的访问。

- 您可以根据设备的类型定义设备访问规则。在指定时间允许或阻止指定用户的访问。

> “设备控制”忽略挂载点排除项。可以通过“设备控制”设置限制对挂载在排除点的设备的访问。

在 Web Console 中配置设备控制

在 Web Console 中，您可以在策略属性中配置设备控制设置（**应用程序设置→ 安全控制 → 设备控制**）。

设备控制设置

设置	描述
设备控制已启用/已禁用	此切换开关可启用或禁用设备控制。 默认情况下，复选切换开关处于打开状态。
配置受信任设备	单击此链接将打开“**受信任设备**”窗口。在此窗口中，您可以按 ID 或从在客户端设备上检测到的设备列表中选择设备，将设备添加到受信任的设备列表中。
设备控制操作模式	对尝试访问根据设备控制规则受到限制的设备的响应： • **通知**。如果选择此选项，Kaspersky Endpoint Security 将测试选定的访问模式，并生成有关检测到尝试访问设备的事件。 • **阻止**（默认值）。选择此选项后，Kaspersky Endpoint Security 将应用为设备或总线定义的访问模式。
配置设备类型的访问设置	单击此链接将打开“**设备类型**”窗口。在此窗口中，您可以按类型配置对设备的访问。
配置连接总线的访问设置	单击此链接将打开“**连接总线**”窗口。在此窗口中，您可以配置连接总线的访问设置。

“受信任的设备”窗口

该表包含受信任设备的列表。该表默认为空。

受信任设备窗口

设置	Description
设备 ID	受信任设备 ID。
设备名称	受信任设备名称。
设备类型	受信任的设备类型（例如，硬盘驱动器或智能卡读卡器）。
主机名	受信任设备所连接的主机名。
注释	与受信任设备相关的注释。

您可以按设备 ID 或从在用户设备上检测到的设备列表中选择所需设备，将设备添加到受信任设备列表中。

您可以在表中编辑和删除受信任设备。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

还可以单击“**导入**”从文件中导入设备列表，以及单击“**导出**”将所添加的设备列表导出到文件。导入时，系统会提示您替换受信任设备列表或将设备添加到现有列表。

“受信任设备(设备 ID)”窗口

在此窗口中，您可以通过设备的标识符将设备添加到受信任设备列表中。

按 ID 添加设备

设置	Description
设备 ID	设备 ID 或设备 ID 掩码的输入字段。您可以手动指定设备 ID 或从“**主机上检测到的设备**”列表中复制所需设备的 ID。 要指定标识符，可以使用以下通配符：*（任意字符序列）或？（任意单个字符）。例如，您可以指定 USBSTOR* 掩码以允许访问所有 USB 驱动器。
注释	注释的输入字段（可选）。此字段在您输入设备 ID 并单击“**下一步**”按钮后可用。

“受信任设备”窗口（检测到的设备列表）

在此窗口中，您可以通过在现有受管理设备列表中选择设备将其添加到受信任设备列表中。

只有当存在活动策略并且已与网络代理同步（以网络代理策略中指定的频率执行，默认情况下为 15 分钟）时，有关现有设备的信息才可用。如果创建新策略但没有其他活动策略，则该列表将为空。

从列表中添加设备

设置	Description
设备类型	在此下拉列表中，您可以选择要在“主机上检测到的设备”表中显示的设备类型。
设备 ID 掩码	设备 ID 掩码的输入字段。
注释	注释的输入字段（可选）。此字段在您选择设备并单击“下一步”按钮后可用。

单击“筛选”按钮将打开一个窗口，在其中可以设置对显示的有关设备的信息的筛选。

“设备类型”窗口

在此窗口中，您可以为各种类型的设备配置访问规则。

设备类型的访问规则

设置	描述

访问数据存储设备的设置	该表包含以下列：
	• 类型表示设备类型（例如，硬盘驱动器、打印机）。
	• 访问模式表示此类设备的访问模式。您可以选择以下访问模式之一：
	  • 允许，允许访问此类型的设备。
	  • 阻止，阻止对此类型设备的访问。
	  • 取决于总线（默认值），根据用于连接设备的总线的访问模式，允许或阻止对设备的访问。
	  • 按规则 – 允许或阻止对设备的访问，具体取决于访问规则和计划。您可以通过单击所需的设备类型来配置访问规则及其计划。

访问其他设备的设置	该表包含以下列：
	• 类型 – 设备的类型（例如，输入设备、声音适配器）。
	• 访问模式表示此类设备的访问模式。您可以选择以下访问模式之一：
	  • 允许，允许访问此类型的设备。
	  • 阻止，阻止对此类型设备的访问。对于网络适配器，不能选择“阻止”访问模式。
	  • 取决于总线（默认值），根据用于连接设备的总线的访问模式，允许或阻止对设备的访问。

“设备访问设置”窗口

在此窗口中，您可以为所选设备类型配置访问模式和访问规则。

设备访问设置

设置	描述
设备访问模式	所选类型设备的访问模式： • **允许**：允许访问选定类型的设备。 • **阻止**：禁止访问选定类型的设备。 • **取决于总线**（默认值），根据用于连接设备的总线的访问规则，允许或阻止对设备的访问。 • **按规则** – 允许或阻止对设备的访问，具体取决于访问规则和计划。

设备访问规则	该表包含访问规则列表，由以下列组成：
	• **访问计划** – 现有访问计划的名称。
	• **用户和/或用户组** – 访问规则将适用的用户或用户组的名称。
	• **访问** – 计划的访问模式：
	  • **允许**（允许访问选定类型的设备）。
	  • **阻止**（禁止访问选定类型的设备）。
	• **状态** – 访问规则的状态：
	  • **已启用** – 该规则已启用；应用程序控制在运行期间应用此规则。
	  • **已禁用** – 该规则已禁用，应用程序控制在运行期间不会使用此规则。
	默认情况下，该表包含"**默认计划**"访问计划，如果允许通过连接总线访问此类设备，则可以随时向所有用户提供对设备的完全访问权限（在用户和组列表中选择了 **\Everyone** 选项）。
	您可以添加、编辑和删除访问规则。
	单击"**删除**"按钮可将所选项目从表中删除。
	如果在表中选择至少一项，则此按钮可用。

"设备访问规则"窗口

在此窗口中，您可以配置设备访问规则。

设备访问规则

设置	描述
设备访问规则设置	所选类型设备的访问模式： • **允许**（默认值）– 提供对所选类型设备的访问权限。 • **阻止**：禁止访问选定类型的设备。
用户和/或用户组	规则适用的用户或用户组的名称。 默认值为 **\All**（所有用户）。 您可以添加、编辑和删除用户或用户组。

	单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。
状态	访问规则状态： • **已启用** – 该规则已启用；应用程序控制在运行期间应用此规则。 • **已禁用** – 该规则已禁用，应用程序控制在运行期间不会使用此规则。
设备访问计划	指定用户的设备访问计划。默认值为“**默认计划**”。您可以设置不同的计划。

“选择用户或组”窗口

在此窗口中，可以指定要为其配置访问规则的本地或域用户或用户组。

配置访问规则

设置	描述
手动	如果选择此选项，请在下面的字段中输入设备访问规则将适用的本地或域用户或用户组的名称。
组或用户的列表	如果选择此选项，您可以在搜索字段中输入搜索条件来搜索设备访问规则将适用的用户或用户组的名称，也可以在下面的列表中选择用户组名称。

“计划”窗口

在此窗口中，您可以指定所选设备访问规则的计划。

您可以添加、编辑和删除访问计划。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

您不能删除**默认计划**。

访问计划窗口

在此窗口中，您可以配置设备访问计划。您只能为硬盘驱动器、可移动驱动器、软盘和 CD/DVD 驱动器配置计划。

在“常规设置->应用程序设置”部分中，如果清除“扫描期间阻止访问文件”复选框，则无法使用访问计划阻止对设备的访问。

设备访问计划

设置	Description
Name	访问计划名称的输入字段。计划名称必须是唯一的。
时间间隔	在此表格中，您可以选择计划的时间间隔（天和小时）。 以绿色突出显示的时间间隔将包含在计划中。 要从计划中排除时间间隔，请单击相应的单元格。从计划中排除的时间间隔以灰色突出显示。 默认情况下，所有间隔 (24/7) 都包含在计划中。

“连接总线”窗口

在此窗口中，您可以配置连接总线的访问模式。

连接总线的访问模式

设置	描述
连接总线	用于将设备连接到客户端设备的连接总线： • FireWire • USB
访问模式	此切换开关设置使用此总线的设备的访问模式： • 允许（默认）：允许通过此总线访问连接的设备。 • 阻止：拒绝访问使用此连接总线连接的设备。

在管理控制台中配置设备控制

在管理控制台中，您可以在策略属性中配置设备控制设置（安全控制 → 设备控制）。

设备控制设置

设置	描述
启用设备控制	此复选框用于启用或禁用设备控制。 默认选中该复选框。
受信任设备	这组设置包含配置按钮。单击此按钮可打开受信任设备窗口。在此窗口中，您可以按设备 ID 或从在客户端设备上检测到的设备列表中选择设备，将设备添加到受信任的设备列表中。
设备控制操作模式	对尝试访问根据设备控制规则受到限制的设备的响应： • 通知。如果选择此选项，Kaspersky Endpoint Security 将测试选定的访问模式，并生成有关检测到尝试访问设备的事件。

	• **阻止**（默认值）。选择此选项后，Kaspersky Endpoint Security 将应用为设备或总线定义的访问模式。
设备控制设置	这组设置包含打开窗口的按钮，您可以在其中按类型和连接总线配置设备的访问模式。

“受信任的设备”窗口

该表包含受信任设备的列表。该表默认为空。

受信任设备窗口

设置	Description
设备 ID	受信任设备的 ID。
设备名称	受信任设备的名称。
设备类型	受信任的设备类型（例如，硬盘驱动器或智能卡读卡器）。
主机名	受信任设备所连接的主机名。
注释	与受信任设备相关的注释。

您可以按设备 ID 或按掩码或从在用户设备上检测到的设备列表中选择所需设备，将设备添加到受信任设备列表中。

您可以在表中编辑和删除受信任设备。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

还可以单击**高级 -> 导入**将文件中的设备列表导入，单击**高级 -> 导出所选**或**高级 -> 全部导出**可将所添加的设备列表导出到文件。导入时，系统会提示您替换受信任设备列表或将设备添加到现有列表。

“受信任的设备”窗口

在此窗口中，您可以通过设备的标识符将设备添加到受信任设备列表中。

按 ID 添加设备

设置	Description
设备 ID	用于输入要添加到受信任设备列表中的设备的标识符或标识符掩码的字段。 要指定标识符，可以使用以下通配符：*（任意字符序列）或？（任意单个字符）。例如，您可以指定 USBSTOR* 掩码以允许访问所有 USB 驱动器。
在主机上查找	单击该按钮可显示使用指定 ID 或掩码在连接的客户端设备上找到的设备。如果**设备 ID** 字段不为空，则该按钮可用。
找到的	该表包含以下列：

设备	• **设备类型** – 所找到设备的类型（例如，硬盘驱动器或智能卡读卡器）。 • **设备 ID** – 所找到设备的 ID。 • **设备名称** — 所找到设备的名称。 • **主机名称** – 所找到设备连接的客户端设备的名称。
注释	用于为要添加到受信任设备列表中的设备输入注释的字段（可选）。

客户端设备上的设备窗口

在此窗口中，您可以通过在客户端设备上检测到的现有设备列表中选择设备将其添加到受信任设备列表中。

只有当存在活动策略并且已与网络代理同步（在网络代理策略中指定的限制内执行，默认情况下为 15 分钟）时，有关现有设备的信息才可用。如果创建新策略但没有其他活动策略，则该列表将为空。

从列表中添加设备

设置	Description
主机名	用于输入要查找已连接设备的受管理设备的名称或名称掩码的字段。默认掩码为 * – 所有受管理设备。
设备类型	在此下拉列表中，您可以选择要搜索的连接设备的类型（例如，硬盘驱动器或智能卡读卡器）。默认情况下选择**所有设备**选项。
设备 ID	用于输入要查找的设备的标识符或标识符掩码的字段。默认掩码为 * – 即所有设备。
在主机上查找	单击此按钮后，应用程序将以指定设置搜索设备。搜索结果显示在下表中。

“设备类型”窗口

在此窗口中，可以为各种类型的设备配置访问模式。

设备类型的访问模式

设置	Description
设备类型	设备类型（例如，硬盘驱动器、打印机）。
访问模式	设备访问模式。单击鼠标右键将打开一个上下文菜单，您可以在其中选择以下选项之一： • **允许**：允许访问选定类型的设备。 • **阻止**：禁止访问选定类型的设备。 • **取决于总线**（默认值）：根据连接总线的访问模式，允许或阻止对设备的访问。 • **按规则** – 允许或阻止对设备的访问，具体取决于访问规则和计划。

您可以在双击设备类型时打开的“配置设备访问规则”窗口中配置访问规则和计划。

“配置设置访问规则”窗口

在此窗口中，您可以为所选设备类型配置访问规则和计划。

在设备类型窗口中双击设备类型即可打开此窗口。

设备访问规则和计划

设置	描述
用户和/或用户组	该列表包含可以为其配置访问计划的用户和组。 默认情况下，该表包含 **\Everyone** 项目（所有用户）。 您可以添加、编辑和删除用户或用户组。
所选用户组的基于计划的访问规则	此表包含用户和用户组的访问计划。它由以下列组成： • **访问计划** – 现有访问计划的名称。计划旁边的复选框指示组件是否使用此计划。 • **访问权限** – 计划的访问类型：**允许**（授予对所选类型设备的访问权限）或**阻止**（拒绝所选类型设备的访问权限）。 您只能为硬盘驱动器、可移动驱动器、软盘和 CD/DVD 驱动器配置计划。默认情况下，该表包含**默认**访问计划，如果允许通过**连接总线**访问此类设备，则可以随时向所有用户提供对设备的完全访问权限（在**用户和/或用户组**列表中选择了\ Everyone 项）。 您可以添加、编辑和删除所选用户的访问计划。不能修改或移除**默认**计划。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。

“用户或组”窗口

在此窗口中，您可以指定应用设备访问规则的用户或用户组。

配置设备访问规则

设置	描述
类型	应用程序控制规则应用到的**用户**或**组**。
用户或组名称	规则适用的用户或用户组的名称。

访问计划窗口

在此窗口中，您可以配置设备访问计划。

设备访问计划

设置	Description
Name	访问计划名称的输入字段。
时间间隔	在此表格中，您可以选择计划的时间间隔（天和小时）。

	以绿色突出显示的时间间隔将包含在计划中。 要从计划中排除时间间隔，请单击相应的单元格。从计划中排除的时间间隔以灰色突出显示。 默认情况下，所有间隔 (24/7) 都包含在计划中。

“连接总线”窗口

在此窗口中，您可以配置连接总线的访问模式。

连接总线的访问模式

设置	描述
连接总线	用于将设备连接到客户端设备的连接总线： • **FireWire** • **USB**
访问模式	连接总线访问模式。单击鼠标右键将打开一个上下文菜单，您可以在其中选择以下选项之一： • **允许**（默认）：允许通过此总线访问连接的设备。 • **阻止**：拒绝访问使用此连接总线连接的设备。

在命令行上配置设备控制

您可以借助“设备控制”预定义任务 (*Device_Control*) 在命令行中管理设备控制。

“设备控制”任务默认没有运行。您可以手动启动和停止任务。

您可以通过编辑“设备控制”预定义任务的设置来配置设备控制。

您还可以使用设备控制命令查看已连接设备的列表。

设备控制任务设置

该表介绍了可为设备控制任务指定的所有设置的全部可用值以及默认值。

设备控制任务设置

设置	描述	值
OperationMode	对尝试访问根据设备控制规则受到限制的设备的响应。	`Block`（默认值）— 应用程序定义的访问模式。 通知 — 应用程序将测试选定的有关检测到尝试访问设备的事
[DeviceClass] 部分包含设备的访问模式，具体取决于设备的类型。		
HardDrive	连接到客户端设备	`Allow` - 允许用户访问硬盘驱

	的硬盘驱动器的访问模式。	DependsOnBus（默认）：对取决于为连接总线定义的访问 Block—用户对所有硬盘驱动器驱动器，这些驱动器绝不会被访问均被阻止。 ByRule - 对于硬盘驱动器的规则。
RemovableDrive	连接到客户端设备的可移动驱动器的访问模式。	Allow - 允许用户访问可移动 DependsOnBus（默认）：对问取决于为连接总线定义的访 Block - 阻止用户访问可移动 ByRule - 对于可移动驱动器的问规则。
FloppyDrive	连接到客户端设备的软盘驱动器的访问模式。 应用程序不会阻止使用 ISA 总线连接到客户端设备的软盘驱动器。	Allow - 允许用户访问软盘。 DependsOnBus（默认）：对为连接总线定义的访问模式。 Block- 阻止用户访问软盘。 ByRule - 对软盘的访问取决于
OpticalDrive	连接到客户端设备的 CD/DVD 驱动器的访问模式。	Allow - 允许用户访问 CD/DV DependsOnBus（默认）：对访问取决于为连接总线定义的 Block - 阻止用户访问 CD/DV ByRule - 对于 CD /DVD 的访规则。
SerialPortDevice	通过串行端口连接到客户端设备的设备的访问模式。 应用程序不会阻止使用 ISA 总线通过串行端口连接到客户端设备的设备。	Allow - 允许用户访问通过串备。 DependsOnBus（默认）：对的设备的访问取决于总线访问 Block - 阻止用户访问通过串备。
ParallelPortDevice	通过并行端口连接到客户端设备的设备的访问模式。	Allow - 允许用户访问通过并备。 DependsOnBus（默认）：对的设备的访问取决于总线访问 Block - 阻止用户访问通过并备。
Printer	连接到客户端设备的打印机的访问模式。	Allow - 允许用户访问打印机 DependsOnBus（默认）：对于为连接总线定义的访问模式 Block - 阻止用户访问打印机
Modem	连接到客户端设备的调制解调器的访问模式。	Allow - 允许用户访问调制解 DependsOnBus（默认）：对取决于为连接总线定义的访问 Block - 阻止用户访问调制解

TapeDrive	连接到客户端设备的磁带设备的访问模式。	`Allow` - 允许用户访问磁带设 `DependsOnBus`（默认）：对决于为连接总线定义的访问模 `Block` - 阻止用户访问磁带设
MultifuncDevice	连接到客户端设备的多功能设备的访问模式。	`Allow` - 允许用户访问多功能 `DependsOnBus`（默认）：对取决于为连接总线定义的访问 `Block` - 阻止用户访问多功能
SmartCardReader	连接到客户端设备的智能卡读卡器的访问模式。	`Allow` - 允许用户访问智能卡 `DependsOnBus`（默认）：对问取决于为连接总线定义的访 `Block` - 阻止用户访问智能卡
WiFiAdapter	连接到客户端设备的 Wi-Fi 适配器的访问模式。	`Allow` - 允许用户访问 Wi-Fi 适 `DependsOnBus`（默认）：对问取决于连接总线访问模式。 `Block` - 阻止用户访问 Wi-Fi 适
NetworkAdapter	连接到客户端设备的外部网络适配器的访问模式。	`Allow` - 允许用户访问外部网 `DependsOnBus`（默认）：对访问取决于为连接总线定义的 设备控制不允许拒绝访问外以避免客户端设备与网络断
PortableDevice	连接到客户端设备的便携式设备的访问模式。	`Allow` - 允许用户访问便携式 `DependsOnBus`（默认）：对取决于为连接总线定义的访问 `Block` - 阻止用户访问便携式
BluetoothDevice	连接到客户端设备的蓝牙设备的访问模式。	`Allow` - 允许用户访问蓝牙设 `DependsOnBus`（默认）：对决于为连接总线定义的访问模 `Block` - 阻止用户访问蓝牙设
ImagingDevice	连接到客户端设备的成像设备的访问模式。	`Allow`—允许用户访问所有成 `DependsOnBus`（默认）：对决于为连接总线定义的访问模 `Block` – 阻止用户访问所有成
SoundAdapter	连接到客户端设备的声音适配器的访问模式。	`Allow` – 允许用户访问所有声 `DependsOnBus`（默认）：对取决于为连接总线定义的访问 `Block` – 阻止用户访问所有声
InputDevice	连接到客户端设备的输入设备（键盘、鼠标、触摸板和其他设备）的访问模式。	`Allow` - 允许用户访问输入设 `DependsOnBus`（默认）：对决于为连接总线定义的访问模 `Block` - 阻止用户访问输入设

[DeviceBus] 部分包含连接总线的访问模式。		
USB	通过 USB 连接到客户端设备的设备的访问模式。	`Allow`（默认值）- 允许用户 `Block` - 阻止用户访问 USB 设
FireWire	通过 FireWire 连接到客户端设备的设备的访问模式。	`Allow`（默认值）- 允许用户 接口连接的设备。 `Block` - 阻止用户访问通过 Fi 设备。
[TrustedDevices.item_ #] 部分包含受信任设备。		
DeviceId	指定受信任设备的 ID 或 ID 掩码。	您可以使用掩码 *（任意字符 个字符）指示设备 ID。 例如： *要拒绝访问除指定 USB 设备 设备，请指定以下设置：* 在 `[DeviceBus]` 部分中， 在 `[TrustedDevices.ite` 定 `DeviceId=<设备 ID>` *要拒绝访问所有 USB 设备， USB 驱动器，请指定以下设* 在 `[DeviceBus]` 部分中， 在 `[TrustedDevices.ite` 定 `DeviceId=USBSTOR*`
注释	对指定的受信任设备的注释。	—
[Schedules.item_#] 部分包含设备访问计划。您只能为硬盘驱动器、可移动驱动器、软盘和 CD/DVD 驱动器配		
ScheduleName	指定计划名称。 计划名称必须是唯一的。	默认值：`Default`。 如果允许连接总线访问相应的 `Default` 计划使用户在任何时 备。 您不能删除 `Default` 计划。

DaysHours	指定计划的时间间隔。	`All`（默认值）- 计划全天候有
		制）。
		`< week_day >` — 星期几。您可
		几名称或缩写（例如，对于星
		`Mo`、`Mon` 或 `Monday`）。对于
		定间隔时间或特定日子。一周
		< 小时 > — 小时 [0:24]。只能
		例如：
		Schedule_1 的有效期为星期
		晨 0 点至上午 11 点，中午 12
		以及下午 4 点至凌晨 12 点：
		`[Schedules.item_0001]`
		`ScheduleName=schedule_`

		DaysHours=Su-Sa:0..11 Schedule_2 在以下时间段内 午 12 点到下午 2 点，星期五 3 点和下午 4 点到凌晨 12 点 [Schedules.item_0002] ScheduleName=schedule_ DaysHours=Th:12..14;Fr Schedule_3 每周 7 天 24 小 [Schedules.item_0003] ScheduleName=schedule_ DaysHours=All
[HardDrivePrincipals.item_#] 部分包含硬盘驱动器访问规则。 对于硬盘驱动器，必须始终至少启用一个计划。您可以为一个硬盘驱动器分配多个访问规则。另外，可以为用户 个计划。如果用户或组发生访问规则冲突，则授予最低访问权限。		
Principal	指定访问规则所适用的用户或用户组。	\Everyone（默认值）- 访问户。 < 用户名 > — 访问规则所适用 @< 组名 > — 访问规则所适用
[HardDrivePrincipals.item_#.AccessRules.item_#]	访问规则设置。	—
UseRule	指定规则是启用还是禁用。	Yes（默认值）- 访问规则已 No - 访问规则已禁用。
ScheduleName	在 [Schedules.item_#] 部分中指定的计划。	默认值：Default。
Access	指定访问类型。	Allow（默认值）- 允许访问 Block - 阻止访问硬盘驱动器
[RemovableDrivePrincipals.item_#] 部分包含可移动驱动器的访问规则。 对于可移动驱动器，必须始终至少启用一个计划。您可以为一个可移动驱动器分配多个访问规则。另外，可以为 定多个计划。如果用户或组发生访问规则冲突，则授予最低访问权限。		
Principal	指定访问规则所适用的用户或用户组。	\Everyone（默认值）- 访问户。 < 用户名 > — 访问规则所适用 @< 组名 > — 访问规则所适用
[RemovableDrivePrincipals.item_#.AccessRules.item_#]	访问规则设置。	—
UseRule	指定规则是启用还是禁用。	Yes（默认值）- 访问规则已 No - 访问规则已禁用。
ScheduleName	在 [Schedules.item_#] 部分中指定的计划。	默认值：Default。
Access	指定访问类型。	Allow（默认值）— 允许访问 Block — 阻止访问可移动驱动
[FloppyDrivePrincipals.item_#] 部分包含软盘驱动器的访问规则。		

对于软盘驱动器，必须始终至少启用一个计划。您可以为一个软盘驱动器分配多个访问规则。另外，可以为用户 个计划。如果用户或组发生访问规则冲突，则授予最低访问权限。		
Principal	指定访问规则所适用的用户或用户组。	\Everyone（默认值）- 访问 户。 < 用户名 > — 访问规则所适用 @< 组名 > — 访问规则所适用
[FloppyDrivePrincipals.item_#.AccessRules.item_#]	访问规则设置。	—
UseRule	指定规则是启用还是禁用。	Yes（默认值）- 访问规则已 No - 访问规则已禁用。
ScheduleName	在 [Schedules.item_#] 部分中指定的计划。	默认值：Default。
Access	指定访问类型。	Allow（默认值）- 允许访问 Block - 阻止访问软盘驱动器
[OpticalDrivePrincipals.item_#] 部分包含 CD/DVD 驱动器的访问规则。 对于 CD/DVD 驱动器，必须始终至少启用一个计划。您可以为一个 CD/DVD 驱动器分配多个访问规则。另外， 组指定多个计划。如果用户或组发生访问规则冲突，则授予最低访问权限。		
Principal	指定访问规则所适用的用户或用户组。	\Everyone（默认值）- 访问 户。 < 用户名 > — 访问规则所适用 @< 组名 > — 访问规则所适用
[OpticalDrivePrincipals.item_#.AccessRules.item_#]	访问规则设置。	—
UseRule	指定规则是启用还是禁用。	Yes（默认值）- 访问规则已 No - 访问规则已禁用。
ScheduleName	在 [Schedules.item_#] 部分中指定的计划。	默认值：Default。
Access	指定访问类型。	Allow（默认值）-允许访问 C Block - 阻止访问 CD/DVD 驱

在命令行中查看连接设备列表

只有具有 admin 和 audit 角色的用户才能查看已连接设备的列表。

要查看所连接设备的列表，请执行以下命令：

```
kesl-control [-D] --get-device-list
```

Kaspersky Endpoint Security 显示以下有关已连接设备的信息：

- **设备类型**。所连接设备的的类型。例如，`OpticalDrive` 或 `HardDrive`。

- **标识符**。所连接设备的 ID。
- **Name**。所连接设备的名称。
- **路径**。设备在 sysfs 虚拟操作系统中的路径。
- **系统驱动器**。该设置指示所连接的设备是否为系统驱动器（Yes 或 No）。
- **总线**。连接总线。可能值：`UnknownBus`、`USB`、`FireWire`。
- **驱动程序**。sysfs 虚拟操作系统读取的驱动程序名称。

Web 控制

Web 控制控制用户对 Web 资源的访问。这样可以减少流量消耗和对工作时间的不当使用。当用户尝试打开受 Web 控制限制其访问的网站时，Kaspersky Endpoint Security 会阻止访问或显示一条警告消息，告知用户该网站不受欢迎。

Kaspersky Endpoint Security 仅监控 HTTP 和 HTTPS 流量。

Web 控制可让您通过以下方式配置对网站的访问：

- 按内容类别。网站内容基于卡巴斯基安全网络、启发式分析和已知网站数据库（包含在应用程序数据库中）进行分类。例如，您可以限制用户对"社交网络"内容类别或其他类别网站的访问。
- 按数据类型类别。例如，您可以限制用户对网站上数据的访问并隐藏图形。应用程序根据文件格式而不是扩展名来确定数据类型。

  > 应用程序不会扫描压缩文件内的文件。例如，如果图像文件被压缩，应用程序会将数据类型检测为压缩文件而不是图像文件。

- 按网址。您可以指定网址或网址掩码。

您可以同时使用多种方法来规范对网站的访问。例如，您可以仅限制对 "Webmail" 类别网站上的 "Office 应用程序文件"数据类型的访问。

默认情况下，为所有 Web 资源选择的*默认规则*是**"允许"**。根据此规则，如果没有定义其他*Web 资源访问规则*，则 Web 控制允许用户访问 Web 资源。

您可以更改 Web 控制的默认规则，该规则可控制应用程序如何控制对其他规则未涵盖的 Web 资源的访问，并将*默认规则*设置为**阻止**。根据此规则，如果没有定义其他*Web 资源访问规则*，则 Web 控制会阻止用户访问 Web 资源。

关于 Web 资源访问规则

*Web 资源访问规则*是一组筛选器和当用户在规则计划中指定的时间访问规则中描述的 Web 资源时应用程序执行的操作。筛选器可让您指定受 Web 控制组件监控访问的 Web 资源。

以下筛选器可用：

- **按内容类别筛选**。Web 控制可以根据内容对 Web 资源进行分类。您可以控制用户对具有由这些类别定义的内容的 Web 资源的访问。当用户访问属于所选内容类别的 Web 资源时，应用程序将执行规则中指定的操作。
- **按数据类型类别筛选**。Web Control 可以根据数据类型对 Web 资源进行分类。您可以控制用户对位于与某些类型数据相关的 Web 资源上的数据的访问。当用户访问与所选数据类型类别相关的 Web 资源时，应用程序将执行规则中指定的操作。
- **按 Web 资源地址筛选**。您可以控制用户对 Web 资源的所有地址、Web 资源的个别地址和/或 Web 资源的地址组的访问。

  如果您同时定义了按内容类别和/或数据类型类别进行筛选以及按 Web 资源地址进行筛选，并且指定的 Web 资源地址和/或 Web 资源地址组属于选定的内容类别或数据类型类别，则应用程序不会控制对选定内容类别和/或数据类型类别的所有 Web 资源的访问，而只是控制对选定的 Web 资源地址和/或 Web 资源地址组的访问。

- **按用户和用户组名称进行筛选**。您可以定义用户和/或用户组，根据规则控制其对 Web 资源的访问。例如，您可以限制组织中除 IT 部门之外的所有用户使用浏览器对互联网的访问。

- **规则计划**。您可以设置规则计划。规则计划可决定应用程序控制对规则中指定的 Web 资源的访问的时间。例如，您可以限制仅在工作时间时通过浏览器访问互联网。

对于每条规则，您可以指定当用户访问与规则设置匹配的 Web 资源时 Web 控制执行的操作：

- *允许*。Web 控制允许用户访问 Web 资源。

- *阻止*。Web 控制阻止用户对 Web 资源的访问并显示访问被阻止的消息。通过点击阻止消息中的链接，用户可以向企业局域网管理员发送有关错误阻止的投诉消息，并获得对请求的网络资源的访问权限。

- *告知*。Web 控制显示一条警告，提示该 Web 资源不受欢迎。通过点击警告消息中的链接，用户可以向企业局域网管理员发送有关错误警告的投诉消息。在这种情况下，用户对网络资源的访问不会被阻止。

每条规则都有一个优先级。规则在列表中的位置越靠前，其优先级就越高。如果将某个网站添加到多条规则中，Web 控制将按照优先级最高的规则来控制对该网站的访问。例如，应用程序可能将公司门户网站识别为社交网络。要限制对社交网络的访问，同时允许访问公司门户网站，请创建两条规则：一条针对"社交网络"类别的阻止规则和一条针对公司门户网站的允许规则。公司门户网站访问规则的优先级必须高于社交网络访问规则。

如果没有创建阻止规则，则不会解密 HTTPS 流量。

在 Web Console 中配置 Web 控制

在 Web Console 中，您可以在策略属性中配置 Web 控制设置（**应用程序设置→ 安全控制 → Web 控制**）。

Web 控制组件设置

设置	描述
Web 控制已启用/禁用	此切换开关可启用或禁用 Web 控制。 此切换开关默认关闭。

规则列表	该表包含 Web 资源访问规则列表。Web 控制按照表中列出的顺序应用规则。
	该表包含以下列：
	• **规则名称**。Web资源访问规则名称。
	• **状态**。Web 资源访问规则的状态：
	  • *已启用* — 该规则已启用，Web 控制在操作期间应用此规则。
	  • *已禁用* — 该规则已禁用，Web 控制在运行期间不会使用此规则。
	  您可以启用或禁用表中的切换开关，或者在Web 控制规则窗口中选中或清除**使用此规则**复选框。
	• **操作**。当应用程序检测到尝试访问符合规则的 Web 资源时要采取的操作。
	您可以在表中添加、编辑、删除、上移或下移项目。

	单击“**下移**”按钮可将所选项目在表中向下移动。 如果在表中只选择一个项目，则此按钮可用。 单击“**上移**”按钮可将所选项目在表中向上移动。 如果在表中只选择一个项目，则此按钮可用。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 您也可以单击“**导入**”从文件中导入规则列表，单击“**导出**”将所添加的规则列表导出到文件。导入时，系统将提示您替换规则列表或将规则添加到现有列表。
默认规则	您可以选择默认规则来控制应用程序如何管理对其他规则未涵盖的 Web 资源的访问： • **允许规则列表中未指定的所有内容**（默认）以允许访问 Web 资源。 • **阻止规则列表中未指定的所有内容**以阻止对 Web 资源的访问。
模板	**警告**。输入字段包含触发规则时出现的消息模板，该消息警告尝试访问不良 Web 资源。 **阻止消息**。输入字段包含触发阻止访问 Web 资源的规则时出现的消息模板。 **致管理员消息**。输入字段包含当用户认为不应阻止被阻止的 Web 资源时向企业局域网管理员发送投诉的模板。在用户请求访问后，Kaspersky Endpoint Security 会向管理员发送一条关于拒绝访问 Kaspersky Security Center *网页*事件的消息。事件描述包含向管理员发送的消息，其中变量被其值替换。如果您的组织中未部署 Kaspersky Security Center 解决方案或没有与管理服务器连接，则应用程序将向管理员指定的电子邮件地址发送一条消息。

Web 控制规则窗口

在此窗口中，您可以配置 Web 资源访问规则的设置。

添加 Web 资源访问规则

设置	描述
规则名称	用于输入 Web 资源访问规则名称的字段。
状态	您可以选择 Web 资源访问规则的状态： • *已启用* — 该规则已启用，Web 控制在操作期间应用此规则。 • *已禁用* — 该规则已禁用，Web 控制在运行期间不会使用此规则。
操作	您可以选择当 Web 控制检测到尝试访问与规则匹配的 Web 资源时将执行的操作： • **允许**（默认值）— 允许访问 Web 资源。 • **阻止**— 阻止对 Web 资源的访问并显示访问被阻止的消息。

	• **告知** – 显示一条警告，提示该 Web 资源不受欢迎。通过点击警告消息中的链接，用户可以访问所请求的 Web 资源。
按内容类别筛选	此复选框启用或禁用内容类别扫描。如果选中该复选框，则**内容类别**链接可用。单击此链接将打开一个窗口，您可以在其中选择相关内容类别。 默认情况下，清除此复选框。
按数据类型类别筛选	此复选框启用或禁用内容类别扫描。如果选中该复选框，则**数据类型类别**链接可用。单击此链接将打开一个窗口，您可以在其中选择相关数据类型类别。 默认情况下，清除此复选框。
地址	您可以选择 Web 资源地址筛选的使用方式： • **应用于所有地址**（默认）。如果选择此选项，则不使用 Web 资源地址筛选；Web 控制规则将应用于所有 Web 资源地址。 • **应用到指定地址和/或组**。选定此选项后，将显示规则涵盖的 Web 资源地址表以及**"添加地址"**按钮，单击该按钮可以打开一个窗口，您可以在其中添加所需的 Web 资源地址；单击**"添加组"**按钮可以打开**"地址组"**窗口，您可以在其中添加 Web 资源地址组。
用户	您可以选择对 Web 资源访问规则涵盖的用户应用用户筛选的方式： • **应用到所有用户**（默认值）如果选择此选项，则不使用用户筛选器；Web 控制规则将应用于所有用户。 • **应用到指定用户和/或组**。选择此选项后，将会显示规则涵盖的用户和用户组表以及**"添加"**按钮，单击该按钮将打开**"选择用户或组"**窗口，您可以在其中添加用户和/或用户组。
规则计划	Web 控制规则计划。默认情况下，指定**"始终"**作为计划。单击**"始终"**链接将打开**"计划"**窗口，您可以在其中为规则配置不同计划。

地址组窗口

该表包含 Web 资源地址组，这些资源的用户访问受 Web 控制组件控制。该表默认为空。

配置 Web 资源访问规则

设置	描述
组名称	规则适用的 Web 资源地址组的名称。
组中地址的数量	地址组中的地址数量。

您可以在表中添加、编辑和删除项目。

如果要向此窗口的组列表中添加一组新地址，请单击表格上方的**添加**按钮打开**组**窗口。

如果要将一组地址添加到**Web 控制规则**窗口的组列表中，请选中表中组名旁边的复选框，然后单击表格下方的**添加组到规则**按钮。

组窗口

在此窗口中，您可以添加一组 Web 资源地址。

配置 Web 资源访问规则

设置	描述
组名称	新建 Web 资源地址组的名称。
地址	Web 资源地址组中包含的地址表。

您可以在表中添加、编辑和删除项目。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“选择用户或组”窗口

在此窗口中，您可以指定要为其配置 Web 资源访问规则的本地或域用户或用户组。

配置 Web 资源访问规则

设置	描述
手动	如果选择此选项，请在下面的字段中输入 Web 资源访问规则必须应用的本地或域用户或用户组的名称。
组或用户的列表	如果选择此选项，您可以在搜索字段中输入搜索条件来搜索 Web 资源访问规则必须应用的用户或用户组的名称，也可以在下面的列表中选择用户组名称。

“计划”窗口

在此窗口中，您可以指定所选设备访问规则的计划。

您可以添加、编辑和删除访问计划。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

始终默认计划不可删除或编辑。

访问计划窗口

在此窗口中，您可以配置 Web 资源访问计划。

Web 资源访问计划

设置	Description
Name	访问计划名称的输入字段。计划名称必须是唯一的。
时间间隔	在此表格中，您可以选择计划的时间间隔（天和小时）。 以绿色突出显示的时间间隔将包含在计划中。 要从计划中排除时间间隔，请单击相应的单元格。从计划中排除的时间间隔以灰色突出显示。 默认情况下，所有间隔 (24/7) 都包含在计划中。

在管理控制台中配置 Web 控制

在管理控制台中，您可以在策略属性中配置Web 控制设置（**安全控制 → Web 控制**）。

Web 控制组件设置

设置	描述
启用 Web 控制	该复选框将启用 Web 控制组件。 默认情况下，清除此复选框。
Web 控制设置	该表包含 Web 资源访问规则列表。Web 控制按照表中列出的顺序应用规则。 该表包含以下列： • **状态**。Web 资源访问规则的状态： • *已启用* – 该规则已启用，Web 控制在操作期间应用此规则。 • *已禁用* – 该规则已禁用，Web 控制在运行期间不会使用此规则。 您可以选中或清除表中的复选框，也可以选中或清除Web 控制规则窗口中的**使用此规则**复选框。 • **操作**。当应用程序检测到尝试访问符合规则的 Web 资源时要采取的操作。 • **Name**。Web资源访问规则名称。 您可以在表中添加、编辑、删除、上移或下移项目。 单击“**下移**”按钮可将所选项目在表中向下移动。 如果在表中只选择一个项目，则此按钮可用。 单击“**上移**”按钮可将所选项目在表中向上移动。 如果在表中只选择一个项目，则此按钮可用。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。

	您还可以单击**高级 -> 导入**从文件导入规则列表，单击**其他 -> 导出所选**或**其他 -> 全部导出**将所添加的规则列表导出到文件。导入时，系统将提示您替换规则列表或将规则添加到现有列表。
默认规则	在下拉列表中，您可以选择默认规则，该规则规定应用程序如何规范对其他规则未涵盖的 Web 资源的访问： • **允许**（默认值）— 允许访问 Web 资源。 • **阻止**— 阻止访问 Web 资源。
消息模板	这组设置包含**配置**按钮。单击此按钮将打开消息模板窗口。

Web 控制规则窗口

在此窗口中，您可以配置 Web 资源访问规则的设置。

添加 Web 控制规则

设置	描述
规则名称	用于输入 Web 资源访问规则名称的字段。
使用该规则	该复选框可启用或禁用在应用程序运行时使用规则。 如果选中该复选框，则启用规则，Web 控制在运行时应用此规则。 如果清除该复选框，则规则将被禁用，不会在 Web 控制运行时使用。稍后您可以通过选中复选框来启用此 Web 控制规则。 默认选中该复选框。
筛选内容	在下拉列表中，您可以选择 Web 资源的内容筛选器： • **不筛选**（默认值）。如果选择此项，则不使用任何 Web 资源内容筛选。 • **按内容类别**。当选择此项时，**"选择"**按钮将变为可用。单击此按钮将打开选择内容类别窗口。 • **按数据类型类别**。当选择此项时，**"选择"**按钮将变为可用。单击此按钮将打开选择数据类型类别窗口。 • **按内容类别和数据类型类别**。当选择此项时，**"选择"**按钮将变为可用。单击这些按钮将打开窗口，您可以在其中选择必要的类别。
筛选地址	在下拉列表中，您可以选择 Web 资源地址的筛选器： • **任何地址**（默认值）。如果选择此项，则不使用 Web 资源地址筛选；Web 控制规则将应用于所有 Web 资源地址。 • **指定的地址**。当选择此项时，**选择地址**按钮将变为可用。单击此按钮将打开选择地址窗口，您可以在其中选择必要的 Web 资源地址。
应用到用户	在下拉列表中，您可以选择 Web 资源访问规则适用的用户： • **全部用户**（默认值）。如果选择此项，则不使用用户筛选器；Web 控制规则将应用于所有用户。

	• **已选择用户**。当选择此项时，**“选择用户”**按钮将变为可用。单击此按钮将打开**Select users**窗口。
规则计划	在下拉列表中，您可以配置 Web 资源访问规则计划： • **总是**（默认值）。选中此项时，Web 资源访问规则的应用将不受时间限制，即在任何时候都适用。 • **<计划名称>**。当选择此项时，**“删除”**和**“编辑”**按钮将变为可用，您可以单击这些按钮来删除或配置计划。 • **添加新计划**。选中此项将打开**“访问计划”**窗口，您可以在其中配置 Web 资源访问规则的新计划。
规则操作	在下拉列表中，您可以选择当 Web 控制检测到尝试访问与规则匹配的 Web 资源时将执行的操作： • **允许**（默认值）– 允许访问 Web 资源。 • **阻止**– 阻止对 Web 资源的访问并显示访问被阻止的消息。 • **告知** – 显示一条警告，提示该 Web 资源不受欢迎。通过点击警告消息中的链接，用户可以访问所请求的 Web 资源。

内容类别选择窗口

在此窗口中，您可以选择想要控制其访问的内容类别。

为此，请选中相关类别旁边的复选框。

默认情况下，这些复选框均处于未选中状态。

选中任何嵌套内容类别旁边的复选框不会自动选中包含嵌套类别的主内容类别旁边的复选框。

数据类型类别选择窗口

在此窗口中，您可以选择想要控制其访问的类型类别。

为此，请选中相关类别旁边的复选框。

默认情况下，这些复选框均处于未选中状态。

选择地址窗口

在此窗口中，您可以指定想要控制用户访问的 Web 资源的地址。您可以指定多个地址；在新的一行中输入每个地址以方便进行复制。您可以使用掩码指定地址。

如果要指定一组地址，请单击**添加地址组**按钮打开选择地址组窗口。

选择地址组窗口

该表包含 Web 资源地址组，这些资源的用户访问受 Web 控制组件控制。

如果要将一组地址添加到选择地址窗口的组列表中，请选中表中组名旁边的复选框，然后单击表格下方的**添加**按钮。

您可以在表中添加、编辑和删除项目。

> 单击“**删除**”按钮可将所选项目从表中删除。
>
> 如果在表中选择至少一项，则此按钮可用。

如果要向此窗口的组列表中添加一组新地址，请单击表格上方的**添加**按钮打开添加地址组窗口。

该表默认为空。

添加地址组窗口

在此窗口中，您可以指定想要控制用户访问的 Web 资源地址组。您可以在地址组中指定多个地址；在新的一行中输入每个地址以方便进行复制。您可以使用掩码指定地址。

选择用户窗口

该表包含根据规则控制其对 Web 资源的访问的用户和用户组的名称。

您可以在表中添加、编辑和删除项目。

> 单击“**删除**”按钮可将所选项目从表中删除。
>
> 如果在表中选择至少一项，则此按钮可用。

如果要在此窗口的用户列表中添加新用户和/或用户组，请单击表格上方的**添加**按钮以打开用户或组窗口。

该表默认为空。

“用户或组”窗口

在此窗口中，您可以指定应用 Web 资源访问规则的用户或用户组。

配置 Web 资源访问规则

设置	描述
类型	应用程序控制规则应用到的**用户或组**。
用户或组名称	规则适用的用户或用户组的名称。

访问计划窗口

在此窗口中，您可以配置 Web 资源访问计划。

Web 资源访问计划

设置	Description
Name	访问计划名称的输入字段。
时间间隔	在此表格中，您可以选择计划的时间间隔（天和小时）。 以绿色突出显示的时间间隔将包含在计划中。 要从计划中排除时间间隔，请单击相应的单元格。从计划中排除的时间间隔以灰色突出显示。 默认情况下，所有间隔 (24/7) 都包含在计划中。

配置 Web 控制消息模板

根据 Web 控制规则属性中指定的操作，当用户尝试访问 Web 资源时，应用程序将显示以下类型的消息之一（通过将 HTTP 服务器响应替换为包含消息的 HTML 页面）：

- 警告。此类消息警告用户，访问该 Web 资源是不良行为和/或违反公司安全政策。如果在与此 Web 资源匹配的规则设置中选择了**“告知”**操作，则应用程序会显示一条警告消息。

  如果用户认为警告是错误，警告中的链接可以让用户向公司的 LAN 管理员发送自动生成的投诉消息。

- 阻止的 Web 资源消息 如果在与此 Web 资源匹配的规则设置中选择了**阻止**操作，则应用程序会显示一条消息，表明此 Web 资源已被阻止（参见下图）。

  如果用户认为不应阻止该 Web 资源，则被阻止的 Web 资源消息中的链接可让用户向公司的 LAN 管理员发送自动生成的投诉。

提供了警告消息、阻止的 Web 资源消息以及发送给公司 LAN 管理员的投诉消息的模板。您可以编辑其内容。

要在 Web Console 中更改消息模板：

1. 在 Web Console 的主窗口中，选择**“资产（设备）”**→**“策略和策略配置文件”**。

   将打开策略列表。

2. 选择包含应用了策略的设备的管理组。为此，请单击窗口上部的**“当前路径”**字段中的链接，然后在打开的窗口中选择管理组。

   该列表仅显示为所选管理组配置的策略。

3. 单击列表中所需策略的名称。

   将打开策略属性窗口。

4. 在策略属性窗口中，选择**应用程序设置** → **安全控制** → **Web 控制**。

5. 在**模板**部分，在以下选项卡上配置 Web 控制消息模板：

   - **警告**。输入字段包含触发规则时出现的消息模板，该消息警告尝试访问不良 Web 资源。

- **阻止消息**。输入字段包含触发阻止访问 Web 资源的规则时出现的消息模板。
- **致管理员消息**。输入字段包含当用户认为不应阻止被阻止的 Web 资源时向企业局域网管理员发送投诉的模板。在用户请求访问后，Kaspersky Endpoint Security 会向管理员发送一条关于拒绝访问Kaspersky Security Center*网页*事件的消息。事件描述包含向管理员发送的消息，其中变量被其值替换。如果您的组织中未部署 Kaspersky Security Center 解决方案或没有与管理服务器连接，则应用程序将向管理员指定的电子邮件地址发送一条消息。

在**"警告"**和**"阻止消息"**选项卡上，您可以使用**"添加变量"**和**"添加链接"**按钮向用户消息添加变量和链接。您可以通过单击**"默认"**按钮恢复消息模板的文本。

6. 单击"**确定**"。
7. 单击"**保存**"按钮以保存更改。

要在管理控制台中更改消息模板：

1. 在管理控制台树的"**受管理设备**"文件夹中，打开具有所需设备所属的管理组名称的文件夹。
2. 在工作区中选择"**策略**"选项卡。
3. 在策略列表中，选择所需的策略并双击它以打开"**属性：<策略名称>**"窗口。

   您还可以通过使用策略上下文菜单中的"**属性**"项或单击位于策略设置部分中策略列表右侧的"**配置策略设置**"链接来打开策略属性窗口。
4. 在策略窗口中，选择**安全控制→ Web 控制**。
5. 在**消息模板**部分，单击**配置**按钮。
6. 这将打开**消息模板**窗口；在该窗口中，在以下选项卡上配置 Web 控制消息模板：
   - **警告**。输入字段包含触发规则时出现的消息模板，该消息警告尝试访问不良 Web 资源。
   - **阻止消息**。输入字段包含触发阻止访问 Web 资源的规则时出现的消息模板。
   - **向管理员投诉**。输入字段包含当用户认为不应阻止被阻止的 Web 资源时向企业局域网管理员发送投诉的模板。在用户请求访问后，Kaspersky Endpoint Security 会向管理员发送一条关于拒绝访问Kaspersky Security Center*网页*事件的消息。事件描述包含向管理员发送的消息，其中变量被其值替换。您可以使用**用户请求**选择在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织中未部署 Kaspersky Security Center 解决方案或没有与管理服务器连接，则应用程序将向管理员指定的电子邮件地址发送一条消息。

   在**"警告"**和**"阻止消息"**选项卡上，您可以使用**"变量"**和**"插入链接"**按钮向用户消息添加变量和链接。您可以通过单击**"默认"**按钮恢复消息模板的文本。
7. 单击"**确定**"。
8. 单击**应用**。

在命令行中配置 Web 控制

在命令行上，您可以使用 Web 控制预定义任务 (*Web_Control*) 来管理 Web 控制。

默认情况下，Web 控制任务处于停止状态。您可以手动启动和停止任务。

您可以通过更改Web 控制预定义任务的设置来编辑 Web 控制设置。

您还可以使用 Web 控制管理命令查看和编辑 Web 控制设置。

Web 控制任务设置

下表介绍了可为 Web 控制任务指定的所有设置的全部可用值以及默认值。

Web 控制任务设置

设置	描述	值
WebControlDefaultAction	默认规则，即当 Web 控制检测到尝试访问其他规则未涵盖的 Web 资源时执行的操作。	允许（默认值）– 允许访问 W 源。 阻止 – 阻止访问 Web 资源。
ComplaintRecipient	管理员的电子邮件地址，用于接收有关错误阻止网络资源的消息。	
[Rules.item_#] 部分包含以下设置：		
名称	Web 资源访问规则名称。	
WebControlAction	当 Web 控制检测到尝试访问与规则匹配的 Web 资源时将执行该规则的操作。	允许（默认值）– 允许访问 W 源。 阻止 – 阻止访问 Web 资源。 告知 – 显示一条警告，提示 资源不受欢迎。通过点击警告 的链接，用户可以访问所请求 Web 资源。
Enabled	Web 资源访问规则的状态。	Yes – 该规则已启用，Web 操作期间应用此规则。 No（默认值）– 该规则已禁用 Web 控制在运行期间不会使用 则。
ScheduleId	[Schedules.item_#] 部分中使用的计划 ID。	
UseUrls	在规则中使用 Web 资源地址筛选器。	Yes – 在规则中使用 Web 资 筛选器。 No（默认值）– 不使用 Web 址筛选器，将规则应用于所有 资源地址。
Urls.item_#	规则控制访问的 Web 资源的地址。	您可以使用掩码指定 Web 资 址。
UseCategories	在规则中按内容类别和数据类型类别使用筛选器。	None（默认）– 不使用 Web 容筛选器。 ContentOnly – 在规则中使用 类别筛选器。

		FormatOnly – 在规则中使用型类别筛选器。 ContentAndFormat – 在规则内容类别筛选器和数据类型类器。
[Rules.item_#.ContentCategories.item_#]	用于指定内容类别的部分。	–
ContentCategory	内容类别。	AdultContent, AlcoholTobaccoNarcotics Violence, Profanity, We ChatForum, WebMail, OnlineShops, SocialNets, Recruitment HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweeps InternetCommunicationMe CryptocurAndMining, LegislationBE, ECommerce, ComputerGame Religions, News, Torrents, FileSha AudioAndVideo, BankSite Blogs, DatingSites, Legislatio LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAI
[Rules.item_#.FormatCategories.item_#]	用于指定数据类型类别的部分。	–
FormatCategories.item_#.FormatCategory	数据类型类别。	Video– 视频 Audio– 音频数据 OfficeDocument – Office 应文件 Executable– 可执行文件 Archives– 压缩文件 Images– 图像文件 Scripts– 脚本
UsePrincipals	使用受 Web 资源访问规则覆盖的用户筛选器。	Yes– 使用规则中的用户筛选 No（默认值）– 不使用用户筛将规则应用于所有用户。
[Rules.item_#.Principals.item_#]	用于指定受 Web 资源访	

	问规则涵盖的用户的部分。	
名称	Web 资源访问规则涵盖的用户或用户组。	< 用户名 >：规则所适用的用称。 @< 组名称 >：规则所适用的用的名称。 默认值：网页资源访问规则适有用户。
[UrlCategories.item_#] 部分包含以下设置：		
名称	规则控制访问的 Web 资源地址组的名称。	
`Urls.item_#`	属于组的 Web 资源的地址。	您可以使用掩码指定 Web 资址。
[Schedules.item_#] 部分规则计划。		
`Id`	`[Rules.item_#]` 部分中使用的计划 ID。	`1 至 999999` `0` 是 `Default` 计划的 ID，可让受任何时间限制地运行，即在候运行。
名称	指定计划名称。	
`DaysHours`	指定计划的时间间隔。	< week_day > — 星期几。您可用完整的星期几名称或缩写（对于星期一，您可以指定 `Mo` 或 `Monday`）。对于周中日，指定间隔时间或特定日子。一期日开始。 < 小时 > — 小时 [0:24]。只能时间间隔。

查看和编辑 Web 控制设置

要查看 Web 控制设置，请运行以下命令：

```
kesl-control --get-settings 26 [--file <配置文件的路径>] [--json]
```

其中：

`--file <配置文件路径>` – 将导出设置的配置文件的完整路径。

`--json`：以 JSON 格式输出数据。

要编辑 Web 控制设置，请运行以下命令：

```
kesl-control --set-settings 26 --file <配置文件的路径> [--json]
```

其中：

--file <配置文件路径> – 将从其导入设置的配置文件的完整路径。

--json – 从 JSON 文件导入数据。

要删除已配置的设置并将 Web 控制设置重置为默认规则，请运行以下命令：

```
kesl-control --set-settings 26 --set-to-default
```

创建 Web 资源地址掩码的规则

当创建*Web 资源访问规则*时必须输入大量类似的 Web 资源地址时，Web 资源地址掩码（“地址掩码”）会很方便。一个精心构造的地址掩码可以替代大量 Web 资源地址。

创建地址掩码时，使用以下规则：

1. *字符可替换零个或多个字符的任意序列。

   例如，如果您输入地址掩码*abc*，则 Web 资源访问规则将应用于所有包含序列abc的地址。例如：http://www.example.com/page_0-9abcdef.html。

2. 字符序列*.可让您选择地址的所有域，即它代表*域掩码*。域掩码*.可被解释为任何域名、子域名或空字符串。

   示例：以下地址与*.example.com掩码匹配：

   - http://pictures.example.com – 域名掩码*.与pictures匹配。
   - http://user.pictures.example.com – 域名掩码*.匹配pictures.和user.。
   - http://example.com – 域名掩码*.被解释为空字符串。

3. 地址掩码开头的字符序列www.被解释为序列*.。

   例如：地址掩码www.example.com被解释为*.example.com。该掩码与地址www2.example.com和www.pictures.example.com匹配。

4. 如果地址掩码不以*字符开头，则该地址掩码匹配的内容与以*.开头匹配的内容相同。

5. 如果地址掩码以/或*以外的字符结尾，则该地址掩码匹配的内容与以/*结尾匹配的内容相同。

   示例：地址掩码http://www.example.com与http://www.example.com/abc形式的地址匹配，其中a、b、c是任意字符。

6. 如果地址掩码以/字符结尾，则该地址掩码匹配的内容与以/*结尾匹配的内容相同。

7. 地址掩码末尾的字符序列/*被解释为/*或空字符串。

8. 当将 Web 资源地址与地址掩码进行比较时，会考虑协议（http: 或 https:）。

   - 如果地址掩码中没有网络协议，则地址掩码将匹配具有任何网络协议的地址。

     示例：地址掩码example.com与地址http:// example.com和https:// example.com匹配。

   - 如果地址掩码中存在网络协议，则只有具有相同网络协议的地址才会与地址掩码匹配。

示例：地址掩码`http://*.example.com`与地址`http://www.example.com`匹配，但与地址`https://www.example.com`不匹配。

9. 用双引号括起来的地址掩码无需进行任何进一步替换即可解释，但如果`*`字符最初包含在地址掩码中则除外。对于用双引号括起来的地址掩码，不强制执行规则 5 和 7（参见下表中的示例 14–18）。

10. 对 Web 资源地址掩码的评估不考虑用户名和密码、连接端口或大小写。

应用规则构建地址掩码的示例

No.	地址掩码	Web 资源地址	地址是否与地址掩码匹配？	注释
1	*.example.com	http://www.123example.com	否	参见规则 1。
2	*.example.com	http://www.123.example.com	是	参见规则 2。
3	*example.com	http://www.123example.com	是	参见规则 1。
4	*example.com	http://www.123.example.com	是	参见规则 1。
5	http://www.*.example.com	http://www.123example.com	否	参见规则 1。
6	www.example.com	http://www.example.com	是	参见规则 3、2 和 1。
7	www.example.com	https://www.example.com	是	参见规则 3、2 和 1。
8	http://www.*.example.com	http://123.example.com	是	参见规则 3、4 和 1。
9	www.example.com	http://www.example.com/abc	是	参见规则 3、5 和 1。
10	example.com	http://www.example.com	是	参见规则 3 和 1。
11	http://example.com/	http://example.com/abc	是	参见规则 6。
12	http://example.com/*	http://example.com	是	参见规则 7。
13	http://example.com	https://example.com	否	参见规则 8。
14	"example.com"	http://www.example.com	否	参见规则 9。
15	"http://www.example.com"	http://www.example.com/abc	否	参见规则 9。
16	"*.example.com"	http://www.example.com	是	参见规则 1 和 9。
17	"http://www.example.com/*"	http://www.example.com/abc	是	参见规则 1 和 9。
18	"www.example.com"	http://www.example.com; https://www.example.com	是	参见规则 9 和 8。
19	www.example.com/abc/123	http://www.example.com/abc	否	地址掩码比 Web 资源地址包含更多信息。

系统完整性监控

Kaspersky Endpoint Security 实时或按需求监控受保护设备上操作系统的完整性。

- "*系统完整性监控*"会实时跟踪您在组件设置中添加到监控范围的文件和目录的更改。您可以跟踪文件中的更改，这些更改可能表明受保护的设备存在安全漏洞。
- 您可以使用"*系统完整性检查*"任务，通过将受监控对象的当前状态与先前记录的状态进行比较，来检查已添加到监控范围的文件和目录中是否有更改。

使用"系统完整性监控"需要包含此功能的授权许可。

KESL 容器不支持此功能。

当检测到监控范围内的文件或目录出现更改时，Kaspersky Endpoint Security 会生成有关对象访问控制列表更改的事件。"系统完整性监控"不会共享有关所做更改的具体数据。"*系统完整性检查*"任务发送有关修改的属性以及移动的文件和目录的数据。

实时系统完整性监控

系统完整性监控通过实时拦截文件操作来检测监控范围内对象的每次更改。

系统完整性监控运行时，应用程序将监控以下文件设置的更改情况：

- 内容（write, truncate 等）
- 元数据（拥有权 (chmod/chown)）
- 时间戳 (utimensat)
- 扩展属性（(setxattr) 等）

不计算文件校验和。

由于 Linux 操作系统的技术限制，应用程序无法识别对文件进行更改的用户或进程。

默认情况下禁用系统完整性监控。您可以启用、禁用和配置系统完整性监控：

- 定义系统完整性监控的监控范围。应用程序监控系统完整性监控设置中定义的监控范围内的文件操作。您必须指定至少一个监控范围才能使组件正常工作。默认情况下定义 *卡巴斯基内部对象* (/opt/kaspersky/kesl/) 监控范围。

  您可以指定多个监控范围。您可以实时更改监控范围。

  应用程序任务不监控未位于监控范围内的具有硬链接的文件（属性和内容）的更改。

- 您可以按名称掩码配置从监控中排除的对象。

- 设置系统完整性监控的排除范围。为每个监控范围定义排除项，并且仅对指定的范围有效。您可以指定多个监控排除。

  排除项的优先级高于监控范围；即使排除的对象在监控范围内，也会跳过该对象。如果监控范围定义的级别低于排除目录，则应用程序在系统完整性监控期间将跳过该监控范围。

当目录被添加到监控范围或排除范围时，应用程序不会检查该目录是否存在。

在 Web Console 中配置系统完整性监控

在 Web Console 中，您可以在策略属性中配置系统完整性监控设置（**应用程序设置→安全控制 →系统完整性监控**）。

系统完整性监控设置

设置	描述
系统完整性监控已启用/已禁用	此切换开关用于启用或禁用系统完整性监控组件。 默认情况下，切换按钮处于关闭状态。
监控范围	单击“**配置监控范围**”链接将打开“监控范围”窗口。
排除范围	单击“**配置监控排除范围**”链接将打开“排除范围”窗口。
按掩码筛选的排除项	单击“**按掩码配置排除项**”链接将打开“按掩码筛选的排除项”窗口。

“监控范围”窗口

该表包含系统完整性监控组件的监控范围。应用程序会监控位于表中指定路径的文件和目录。默认情况下，该表包含**卡巴斯基内部对象 (/opt/kaspersky/kesl/)** 监控范围。

系统完整性监控的监控范围设置

设置	Description
范围名称	监控范围名称。
Path	应用程序保护的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

“添加监控范围”窗口

在此窗口中，您可以为系统完整性监控组件添加和配置监控范围。

监控范围设置

设置	Description
范围名称	用于输入监控范围名称的字段。此名称将显示在“监控范围”窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将在运行期间控制此监控范围。 如果清除此复选框，应用程序不会在运行期间控制此监控范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定要包含在监控范围中的本地目录路径的输入字段。您可以使用掩码指定路径。该字段不能为空。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下指定 **/** 路径 — 应用程序扫描本地文件系统的所有目录。
掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”窗口

该表包含系统完整性监控组件的监控排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

监控排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从监控中排除的目录的路径。
状态	指示应用程序是否在组件运行期间将此范围排除在监控之外。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加排除范围”窗口

在此窗口中，您可以为系统完整性监控组件添加或配置监控排除范围。

监控排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从监控中排除相应范围。 如果选中此复选框，则应用程序会在组件运行期间将此范围排除在监控之外。

	如果清除此复选框，则应用程序将在组件运行期间监控此范围。您可以在以后选中此复选框来从监控中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	要添加到排除范围的本地目录路径的输入字段。您可以使用掩码指定路径。该字段不能为空。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
掩码	该列表包含应用程序排除在监控范围之外的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从监控中排除的对象。应用程序不会扫描名称中包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
*.txt 掩码表示所有文本文件。
*_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在管理控制台中配置系统完整性监控

在管理控制台中，您可以在策略属性中配置系统完整性监控设置（**安全控制 → 系统完整性监控**）。

系统完整性监控设置

设置	Description
启用系统完整性监控	此复选框启用或禁用系统完整性监控。 默认情况下，清除此复选框。
监控范围	这组设置包含**配置**按钮。单击此按钮将打开“扫描范围”窗口。
监控排除项	这组设置包含**配置**按钮。单击此按钮将打开“排除范围”窗口。
按掩码筛选的排除项	这组设置包含**配置**按钮，用于打开按掩码筛选的排除项窗口。

“扫描范围”窗口

该表包含系统完整性监控组件的监控范围。应用程序会监控位于表中指定路径的文件和目录。默认情况下，该表包含一个**卡巴斯基内部对象** (/opt/kaspersky/kesl/) 监控范围。

监控范围设置

设置	Description
范围名称	监控范围名称。
Path	应用程序保护的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

<新扫描范围>窗口

在此窗口中，您可以为系统完整性监控组件添加和配置监控范围。

监控范围设置

设置	Description
扫描范围名称	用于输入监控范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将在运行期间控制此监控范围。 如果清除此复选框，应用程序不会在运行期间控制此监控范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定要包含在监控范围中的本地目录路径的输入字段。 该字段不能为空。默认路径为 /opt/kaspersky/kesl。
掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”窗口

该表包含系统完整性监控组件的监控排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

监控排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从监控中排除的目录的路径。
状态	指示应用程序是否在组件运行期间将此范围排除在监控之外。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“<排除范围名称>”窗口

在此窗口中，您可以为系统完整性监控组件添加或配置监控排除范围。

监控排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从监控中排除相应范围。 如果选中此复选框，则应用程序会在组件运行期间将此范围排除在监控之外。 如果清除此复选框，则应用程序将在组件运行期间监控此范围。您可以在以后选中此复选框来从监控中排除此范围。 默认选中该复选框。
文件系统，	要添加到排除范围的本地目录路径的输入字段。该字段不能为空。

访问协议和路径	默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
掩码	该列表包含应用程序排除在监控范围之外的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“删除”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击“添加”按钮将打开“对象掩码”窗口。在此窗口中的“定义对象掩码”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从监控中排除的对象。应用程序不会扫描名称中包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“删除”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击“添加”按钮将打开“对象掩码”窗口。在此窗口中的“定义对象掩码”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
*.txt 掩码表示所有文本文件。
*_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在命令行中配置系统完整性监控

您可以使用“系统完整性监控”预定义任务 (*System_Integrity_Monitoring*) 在命令行中实时管理系统完整性监控。任务类型：*OAFIM*。

默认情况下，“系统完整性监控”任务不运行。您可以手动启动和停止任务。

您可以通过编辑“系统完整性监控”预定义任务的设置，在设备上配置系统完整性监控。

访问时文件完整性监控任务设置

设置	描述	值
UseExcludeMasks	对 ExcludeThreats.item_# 设置指定的对象启用监控范围排除项。 仅当为 ExcludeMasks.item_# 设置指定一个值后，此设置才适用。	Yes — 从监控范围中排除由 ExcludeMasks.item_# 设置指定的对象。 No（默认值）— 不从监控范围中排除由 ExcludeMasks.item_# 设置指定的对象。
ExcludeMasks.item_#	按名称或掩码从监控中排除对象。您可以使用此设置来按名称从指定的扫描范围中排除单个文件，或者使用 Shell 格式的掩码一次性排除多个文件。 在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。 您可以指定多个掩码。每个掩码必须在具有新索引的新行上指定。	默认值为未定义。
[ScanScope.item_#] 部分包含系统完整性监控任务的监控范围。必须为任务指定至少一个监控范围。您可以按任意顺序指定多个 [ScanScope.item_#] 部分。应用程序将按索引升序处理范围。 [ScanScope.item_#] 部分包含以下设置：		
AreaDesc	监控范围的说明；包含有关监控范围的其他信息。	默认值为未定义。
UseScanArea	启用指定范围的监控。	Yes（默认值）- 监控指定的范围。 No - 不监控指定的范围。
Path	监控目录的路径。	您可以使用掩码指定路径。

		您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认值：/opt/kaspersky/kesl/
AreaMask.item_#	监控范围限制。在监控范围内，应用程序仅扫描使用 shell 格式的掩码指定的文件。 您可以按任意顺序指定多个 AreaMask.item_# 项目。应用程序将按索引升序处理范围。	默认值：*（将监控所有对象）。
[ExcludedFromScanScope.item_#] 包含要从所有 [ScanScope.item_#] 部分中排除的对象。您可以按任意顺序指定多个 [ExcludedFromScanScope.item_#] 部分。应用程序将按索引升序处理范围。 [ExcludedFromScanScope.item_#] 部分包含以下设置：		
AreaDesc	监控排除范围的说明，其中包含有关监控排除范围的其他信息。	默认值为未定义。
UseScanArea	从监控中排除指定的范围。	Yes（默认值）— 将指定范围排除在监控之外。 No — 不将指定范围排除在监控之外。
路径	包含从监控中排除的对象的目录的路径。	您可以使用掩码指定路径。

		您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认值为未定义。
AreaMask.item_#	监控排除范围的限制。在监控排除范围中，应用程序仅排除使用 shell 格式的掩码指定的对象。 您可以按任意顺序指定多个 AreaMask.item_# 项目。应用程序将按索引升序处理范围。	默认值：*（从监控中排除所有对象）

系统完整性检查

当“*系统完整性检查*”任务运行时，通过比较受监控对象的当前状态和原始状态来发现每个对象的更改情况。可以使用以下比较标准：

- 文件哈希
- 文件更改时间
- 文件大小

受监控对象的初始状态被记录为*基线*。基线包含受监控对象及其元数据的路径。

基线可能也包含个人数据。

设备上首次运行“系统完整性检查”任务时会创建系统基线。如果您创建了多个“系统完整性检查”任务，则会为每个任务创建一个单独的基线。仅当基线包含有关在该任务定义的监控范围内的对象的信息时，才会执行任务。如果基线与监控范围不匹配，则 Kaspersky Endpoint Security 会生成系统完整性违规事件。

如果任务设置更改（例如添加了新的监控范围），会重建基线。

应用程序在受保护设备上创建基线存储。默认情况下，基线的存储位于 /var/opt/kaspersky/kesl/private/fim.db。需要 root 特权才能访问包含基线的数据库。

您可以通过删除相应的“系统完整性检查”任务来删除基线。

您可以根据需要运行系统完整性检查并配置扫描设置：

- 启用或禁用每次系统完整性检查任务完成后重建基线。
- 选择用于比较受监控文件的当前状态与原始状态的标准：使用文件哈希和更改时间，或者仅使用文件大小。
- 配置系统完整性检查的监控范围。
- 配置系统完整性检查的排除范围。您可以指定排除文件和目录的路径，并按名称掩码排除单个对象。

在 Web Console 中配置系统完整性检查

您可以借助“*系统完整性检查*”任务在 Web Console 中运行系统完整性检查。

您可以创建并运行用户系统完整性检查任务。您可以通过编辑任务的设置来配置扫描设置。

“系统完整性检查”任务设置

设置	描述
每次任务启动时重建基线	此复选框用于启用或禁用在每次启动“*系统完整性检查*”任务时重新建立系统基线。 默认情况下，清除此复选框。
检查 SHA256 哈希	此复选框用于启用或禁用在比较文件的当前状态与原始状态时使用文件哈希作为标准。 如果清除此复选框，则应用程序仅比较文件大小（如果文件大小没有变化，则修改时间不被视为关键参数）。 默认情况下，清除此复选框。
跟踪监控范围中的目录	此复选框用于启用或禁用在系统完整性检查运行时监控目录。 默认情况下，清除此复选框。
跟踪文件上次被访问的时间	此复选框用于启用或禁用在系统完整性监控运行时跟踪文件访问时间。 默认情况下，清除此复选框。
监控范围	包含任务扫描的监控范围的表。 默认情况下，该表包含**卡巴斯基内部对象** (/opt/kaspersky/kesl/) 监控范围。 您可以在表中添加、配置、删除、上移或下移监控范围。 单击“**下移**”按钮可将所选项目在表中向下移动。 Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。 如果在表中只选择了就一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

Kaspersky Endpoint Security 会以扫描范围表中列出对象的顺序扫描指定范围内的对象。如果要为子目录配置的安全设置与父目录的安全设置不同，则必须在表中将子目录置于其父目录上方。

如果在表中只选择了就一个项目，则此按钮可用。

单击**删除**按钮会将所选范围排除在扫描范围之外。

如果在表中选择至少一个扫描范围，则此按钮可用。

单击扫描范围名称将打开“**<扫描范围名称>**”窗口。在此窗口中，可以修改所选扫描范围的设置。

点击“**添加**”按钮将打开“**<新建扫描范围>**”窗口。在此窗口中，可以定义新的扫描范围。

“添加扫描范围”窗口

在此窗口中，您可以为“系统完整性检查”任务添加或配置监控范围。

监控范围设置

设置	Description
范围名称	用于输入监控范围名称的字段。此名称将显示在“**扫描设置**”部分的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将在运行期间控制此监控范围。 如果清除此复选框，应用程序不会在运行期间控制此监控范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定要包含在监控范围中的本地目录路径的输入字段。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

	该字段不能为空。 默认情况下指定 **/** 路径 – 应用程序扫描本地文件系统的所有目录。
掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”部分

在“**排除范围**”部分中，您可以为“系统完整性检查”任务配置排除范围和按掩码筛选的排除项。

“排除范围”窗口

该表包含“系统完整性检查”任务的监控排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

监控排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从监控中排除的目录的路径。
状态	指示应用程序是否在任务运行期间将此范围排除在监控之外。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“添加排除范围”窗口

在此窗口中，您可以为“系统完整性检查”任务添加和配置监控排除范围。

监控排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从监控中排除相应范围。 如果选中此复选框，则应用程序会在任务运行期间将此范围排除在监控之外。 如果清除此复选框，则应用程序将在任务运行期间监控此范围。您可以在以后选中此复选框来从监控中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	要添加到排除范围的本地目录路径的输入字段。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该字段不能为空。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
掩码	该列表包含应用程序排除在监控范围之外的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从监控中排除的对象。应用程序不会扫描名称中包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在管理控制台中配置系统完整性检查

您可以在管理控制台中借助“*系统完整性检查*”任务来执行系统完整性检查。

您可以创建并运行用户系统完整性检查任务。您可以通过编辑任务的设置来配置扫描设置。

在系统完整性检查任务属性的**设置**部分中，您可以编辑下表列出的设置。

“系统完整性检查”任务设置

设置	描述
每次任务启动时重建基线	此复选框用于启用或禁用在每次启动系统完整性检查任务时重新建立系统基线。 默认情况下，清除此复选框。
检查 SHA256 哈希	此复选框用于启用或禁用在比较文件的当前状态与原始状态时使用文件哈希作为标准。 如果清除此复选框，则应用程序仅比较文件大小（如果文件大小没有变化，则修改时间不被视为关键参数）。 默认情况下，清除此复选框。
跟踪监控范围中的目录	此复选框用于启用或禁用在系统完整性检查期间对指定监控范围内的目录进行扫描。 默认情况下，清除此复选框。
跟踪文件上次被访问的时间	此复选框用于启用或禁用在系统完整性监控运行时跟踪文件访问时间。 默认情况下，清除此复选框。
监控范围	这组设置包含**配置**按钮。单击此按钮将打开扫描范围窗口。

在“系统完整性检查”属性的“排除范围”中，您可以定义监控排除和按掩码排除。

“扫描范围”窗口

该表包含“系统完整性检查”任务的监控范围。应用程序会监控位于表中指定路径的文件和目录。默认情况下，该表包含一个**卡巴斯基内部对象** (/opt/kaspersky/kesl/) 监控范围。

监控范围设置

设置	Description
范围名称	监控范围名称。
Path	应用程序保护的目录的路径。
状态	该状态指示应用程序是否扫描此范围。

您可以在表中添加、编辑、删除、上移或下移项目。

单击“**下移**”按钮可将所选项目在表中向下移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**上移**”按钮可将所选项目在表中向上移动。

如果在表中只选择一个项目，则此按钮可用。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

Kaspersky Endpoint Security 会以对象在范围列表中的出现顺序扫描指定范围内的对象。如有必要，在列表中将子目录置于其父目录上方，来为子目录配置与父目录的安全设置不同的安全设置。

<新扫描范围>窗口

在此窗口中，您可以为“系统完整性检查”任务添加或配置监控范围。

监控范围设置

设置	Description
扫描范围名称	用于输入监控范围名称的字段。此名称将显示在扫描范围窗口的表格中。 该输入字段不能为空。
使用此范围	此复选框用于允许或禁止应用程序扫描此范围。 如果选中此复选框，应用程序将在运行期间控制此监控范围。

	如果清除此复选框，应用程序不会在运行期间控制此监控范围。您可以在以后选中此复选框，来在组件设置中包含此范围。 默认选中该复选框。
文件系统，访问协议和路径	用于指定要包含在监控范围中的本地目录路径的输入字段。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该字段不能为空。 默认路径为 /opt/kaspersky/kesl。
掩码	该列表包含应用程序扫描的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“删除”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击添加按钮将打开一个窗口，您可以在其中指定新项目设置。

“排除范围”部分

扫描排除项设置

设置组	Description
监控排除项	这组设置包含配置按钮。单击此按钮将打开排除范围窗口。在此窗口中，您可以定义要从监控中排除的范围列表。
按掩码筛选的排除项	这组设置包含“配置”按钮，用于打开“按掩码筛选的排除项”窗口。在此窗口中，您可以配置按名称掩码从监控中排除对象。

“排除范围”窗口

该表包含“系统完整性检查”任务的监控排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

“系统完整性检查”任务的监控排除范围设置

设置	描述
排除范围名称	排除范围名称。
Path	从扫描中排除的目录的路径。
状态	指示应用程序是否在组件运行期间将此范围排除在监控之外。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。

<新建扫描范围>窗口

在此窗口中，您可以为“系统完整性检查”任务添加和配置监控排除范围。

监控排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在排除范围窗口的表格中。该输入字段不能为空。
使用此范围	该复选框启用或禁用在应用程序运行时从监控中排除相应范围。 如果选中此复选框，则应用程序会在任务运行期间将此范围排除在监控之外。 如果清除此复选框，则应用程序将在任务运行期间监控此范围。您可以在以后选中此复选框来从监控中排除此范围。 默认选中该复选框。
文件系统，访问协议和路径	要添加到排除范围的本地目录路径的输入字段。您可以使用掩码指定路径。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该字段不能为空。 默认情况下会指定 / 路径。应用程序将本地文件系统的所有目录排除在扫描范围之外。
掩码	该列表包含应用程序排除在监控范围之外的对象的名称掩码。 默认情况下，该列表包含 * 掩码（所有对象）。 您可以添加、编辑或删除掩码。 单击“**删除**”按钮可将所选项目从表中删除。 如果在表中选择至少一项，则此按钮可用。 所选元素的设置在单独的窗口中更改。 单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。 例如： *.txt 掩码表示所有文本文件。 *_my_file_??.html 掩码表示以任何字符开头，以 _my_file_ 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

“按掩码筛选的排除项”窗口

您可以根据名称掩码配置从监控中排除的对象。应用程序不会扫描名称中包含指定掩码的文件。默认情况下，掩码列表为空。

您可以添加、编辑或删除掩码。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

所选元素的设置在单独的窗口中更改。

单击“**添加**”按钮将打开“**对象掩码**”窗口。在此窗口中的“**定义对象掩码**”字段中，您可以指定 Kaspersky Endpoint Security 排除在扫描范围之外的文件的名称模板。

例如：
`*.txt` 掩码表示所有文本文件。
`*_my_file_??.html` 掩码表示以任何字符开头，以 `_my_file_` 后跟两个任意字符结尾的 html 文件（例如，2020_my_file_09.html）。

在命令行中配置系统完整性检查

您可以使用用户*系统完整性检查*任务（*ODFIM* 任务）在命令行中对设备运行系统完整性检查。

您可以手动启动、停止、暂停或恢复用户任务，并配置任务计划。您可以通过编辑这些任务的设置来配置系统完整性检查。

“系统完整性检查”任务设置

设置	描述	值
`RebuildBaseline`	启用在*系统完整性检查*任务完成后重建基线。	`Yes`：每次*系统完整性检查*任务完成后重建基线。 `No`（默认）：每次*系统完整性检查*任务完成后不重建基线。
`CheckFileHash`	将受监控文件的当前状态与其原始状态进行比较时，使用文件哈希 (SHA256) 作为标准。	`Yes`：检查哈希。 `No`（默认值）- 禁用哈希检查。如果禁用此检查，则应用程序仅比较文件大小（如果文件大小没有变化，则修改时间不被视为关键参数）。
`TrackDirectoryChanges`	启用目录监控。	`Yes`：检查系统完整性时监控目录。 `No`（默认值）- 不监控目录。
`TrackLastAccessTime`	启用跟踪上次文件访问时间。在 Linux 操作系统中，这是 `noatime` 设置。	`Yes` — 跟踪文件上次被访问的时间。 `No`（默认值）— 不跟踪文件上次被访问的时间。
`UseExcludeMasks`	对 `ExcludeMasks.item_#` 设置指定的对象启用监控范围排除项。 仅当为 `ExcludeMasks.item_#` 设置指定一个值后，此设置才适用。	`Yes` — 从监控范围中排除由 `ExcludeMasks.item_#` 设置指定的对象。 `No`（默认值）— 不从监控范围中排除由 `ExcludeMasks.item_#` 设置指定的对象。
`ExcludeMasks.item_#`	按名称或掩码从监控中排除对象。您可以使用此设置来按名称从指定的扫描范围中排除单个文件，或者使用 Shell 格式的掩码一次性排除多个文件。	默认值为未定义。

	在为此设置指定值之前，请确保已启用 `UseExcludeMasks` 设置。 您可以指定多个掩码。每个掩码必须在具有新索引的新行上指定。	
[ScanScope.item_#] 部分包含*系统完整性检查*的监控范围。必须为任务指定至少一个监控范围。您可以按任意顺序指定多个 [ScanScope.item_#] 部分。应用程序将按索引升序处理范围。 [ScanScope.item_#] 部分包含以下设置：		
`AreaDesc`	监控范围的说明；包含有关监控范围的其他信息。	默认值为未定义。
`UseScanArea`	启用指定范围的监控。	`Yes`（默认值）- 监控指定的范围。 `No` - 不监控指定的范围。
`Path`	监控目录的路径。	您可以使用掩码指定路径。 您可以用 `*`（星号）字符来创建文件或目录名称掩码。 您可以指定单个 `*` 字符来表示文件或目录名称中 `/` 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 `*` 字符来表示文件或目录名称中的任意一组字符（包括空集和 `/` 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 `**` 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 可以使用单个 `?` 字符表示文件名或目录名中的任意一个字符。 默认值：/opt/kaspersky/kesl/
`AreaMask.item_#`	监控范围限制。在监控范围内，应用程序仅扫描使用 shell 格式的掩码指定的文件。 您可以按任意顺序指定多个 `AreaMask.item_#` 项目。应用程序将按索引升序处理范围。	默认值：`*`（将监控所有对象）。
[ExcludedFromScanScope.item_#] 部分包含要从所有 [ScanScope.item_#] 部分中排除的对象。您可以按任意顺序指定多个 [ExcludedFromScanScope.item_#] 部分。应用程序将按索引升序处理范围。 [ExcludedFromScanScope.item_#] 部分包含以下设置：		
`AreaDesc`	监控排除范围的说明，其中包含有关监控排除范围的其他信息。	默认值为未定义。
`UseScanArea`	从监控中排除指定的范围。	`Yes`（默认值）— 将指定范围排除在监控之外。

		No — 不将指定范围排除在监控之外。
路径	包含从监控中排除的对象的目录的路径。	您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 默认值为未定义。
AreaMask.item_#	监控排除范围的限制。在监控排除范围中，应用程序仅排除使用 shell 格式的掩码指定的对象。 您可以按任意顺序指定多个 AreaMask.item_# 项目。应用程序将按索引升序处理范围。	默认值：*（从监控中排除所有对象）

行为检测

行为检测组件可让您监控操作系统中应用程序的任何恶意活动。当检测到恶意活动时，Kaspersky Endpoint Security 可以终止执行恶意活动的应用程序进程。

KESL 容器不支持此功能。

当 Kaspersky Endpoint Security 启动时，行为检测组件会使用默认设置自动启用。

您可以启用、禁用和配置“行为检测”：

- 选择 Kaspersky Endpoint Security 在检测到操作系统中的恶意活动时要执行的操作：告知用户或阻止执行恶意活动的应用程序。
- 从扫描范围中排除进程活动。

如果启用了 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 之间的集成，则在检测操作系统中的应用程序行为时将跳过按进程排除。

默认情况下，在 SintezM-Client 操作系统上，auditd 服务配置受到修改保护，即处于`enabled 2`模式。当 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 解决方案集成时，为了确保行为检测组件正常运行，请将配置文件中的 auditd 模式更改为`enabled 1`（无配置阻止）并重新启动操作系统。

在 Web Console 中配置行为检测

在 Web Console 中，您可以在策略属性中配置行为检测设置（**应用程序设置 → 高级威胁防护 → 行为检测**）。

行为检测设置

设置	描述
行为检测已启用/已禁用	此切换开关用于启用或禁用行为检测组件。 默认情况下，复选切换开关处于打开状态。
检测到恶意软件活动时的操作	Kaspersky Endpoint Security 在操作系统中检测到恶意活动时执行的操作： • **告知**用户。Kaspersky Endpoint Security 不终止执行恶意活动的进程；仅在事件日志中记录检测到恶意活动。 • **阻止**执行恶意活动的应用程序（默认值）。Kaspersky Endpoint Security 会终止执行恶意活动的进程，并记录有关检测到的恶意活动的信息。
按进程筛选的排除项	单击“**按进程配置排除项**”链接将打开“按进程筛选的排除项”窗口。在此窗口中，可以排除进程的活动。

“按进程筛选的排除项”窗口

该表包含按进程筛选的排除范围。按进程筛选的排除范围允许您排除指定进程的活动和指定进程修改的文件。默认情况下，该表为空。

如果启用 Kaspersky Endpoint Security 和卡巴斯基托管检测与响应的集成，则不会应用按进程排除。

按进程筛选的排除范围设置

设置	描述
从扫描中排除/不排除受信任的进程	该开关用于在行为检测组件的操作中启用或禁用所配置的按进程筛选的排除项。 默认情况下，切换按钮处于关闭状态。
排除范围名称	排除范围名称。
Path	排除的进程的完整路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

还可以单击“**导入**”从文件中导入排除项列表，以及单击“**导出**”将所添加的排除项列表导出到文件。导入时，系统将提示您替换排除项列表或将排除项添加到现有列表。

“添加进程排除范围”窗口

在此窗口中，可以添加和配置按进程筛选的排除范围。

排除范围设置

设置	描述
基于进程的排除项范围名称	用于输入基于进程的排除项范围名称的字段。此名称将显示在“按进程筛选的排除项”窗口的表格中。 该输入字段不能为空。
使用该排除项	该复选框用于在应用程序运行时启用或禁用此扫描范围排除项。 默认选中该复选框。
排除的进程的路径	要从扫描中排除的进程的完整路径。您可以使用掩码指定路径。

	您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该输入字段不能为空。
应用到子进程	排除“排除的进程的路径”设置中指示的排除进程的子进程。 默认情况下，清除此复选框。

在管理控制台中配置行为检测

在管理控制台中，您可以在策略属性中配置行为检测设置（高级威胁防护 → 行为检测）。

行为检测设置

设置	Description
启用行为检测	此复选框启用或禁用行为检测组件。 默认选中该复选框。
检测到恶意软件活动时的操作	Kaspersky Endpoint Security 在操作系统中检测到恶意活动时执行的操作： • 阻止执行恶意活动的应用程序（默认值）。Kaspersky Endpoint Security 会终止执行恶意活动的进程，并记录有关检测到的恶意活动的信息。 • 告知用户。Kaspersky Endpoint Security 不终止执行恶意活动的进程；仅在事件日志中记录检测到恶意活动。
按进程使用排除项	此复选框用于启用或禁用在行为检测组件的操作中按进程排除。 默认情况下，清除此复选框。 “配置”按钮可打开“按进程筛选的排除项”窗口。在此窗口中，可以排除进程的活动。

“按进程筛选的排除项”窗口

该表包含按进程筛选的排除范围。按进程筛选的排除范围允许您排除指定进程的活动。默认情况下，该表为空。

如果启用 Kaspersky Endpoint Security 和卡巴斯基托管检测与响应的集成，则不会应用按进程排除。

按进程筛选的排除范围设置

设置	描述

排除范围名称	排除范围名称。
Path	排除的进程的完整路径。
状态	该状态指示应用程序是否使用该排除项。

您可以在表中添加、编辑和删除项目。

> 单击“**删除**”按钮可将所选项目从表中删除。
>
> 如果在表中选择至少一项，则此按钮可用。

还可以单击**高级 -> 导入**将文件中的排除项列表导入，单击**高级 -> 导出所选**或**高级 -> 全部导出**可将所添加的排除项列表导出到文件。导入时，系统将提示您替换排除项列表或将排除项添加到现有列表。

“受信任进程”窗口

在此窗口中，可以添加和配置按进程筛选的排除范围。

按进程筛选的排除范围设置

设置	描述
排除范围名称	用于输入排除范围名称的字段。此名称将显示在“按进程筛选的排除项”窗口的表格中。
排除的进程的路径	要从扫描中排除的进程的完整路径。您可以使用掩码指定路径。 > 您可以用 *（星号）字符来创建文件或目录名称掩码。 > > 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 > > 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 > > ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 > > 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 该输入字段不能为空。
应用到子进程	排除“**排除的进程的路径**”设置中指示的排除进程的子进程。 默认情况下，清除此复选框。
使用此范围	该复选框用于启用或禁用此排除范围。 如果选中此复选框，则应用程序排除此范围。 如果清除此复选框，则应用程序包括此范围。您可以在以后选中此复选框来排除此范围。 默认选中该复选框。

在命令行中配置行为检测

您可以使用 *Behavior_Detection* 预定义任务，通过命令行管理操作系统中的应用程序行为检测。

行为检测任务默认运行。您可以手动启动和停止任务。

您可以通过编辑行为检测预定义任务的设置来配置行为检测。

行为检测任务设置

设置	描述	值
TaskMode	在操作系统中检测到恶意活动时应用程序执行的操作。	Block（默认值）– 终止执行恶意活动的应用程序进程。 Notify – 不终止执行恶意活动的进程；仅在事件日志中记录检测到恶意活动。
UseTrustedPrograms	从扫描中排除进程。	Yes – 不扫描指定进程的活动。 No（默认值）– 扫描所有进程。
[TrustedPrograms.item_#] 部分包含从扫描中排除的进程。Kaspersky Endpoint Security 不会监控指定进程的活动。		
ProgramPath	排除的进程的路径。	< 进程的完整路径 > – 不扫描指定本地目录中的进程。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。
ApplyToDescendants	从扫描中排除 ProgramPath 设置指定的排除进程的子进程。	Yes – 从扫描中排除指定的进程及其所有子进程。 No（默认值）– 仅从扫描中排除指定进程，不排除其子进程。
ProgramDesc	排除的进程的描述。	
UseTrustedProgram	启用从扫描中排除指定进程。	Yes（默认值）– 从扫描中排除指定进程。 No – 不从扫描中排除指定进程。

使用卡巴斯基安全网络

在美国境内，为了遵守贸易限制，自 2024 年 9 月 10 日美国东部夏令时间 (EDT) 凌晨 12:00 起，该应用程序将不再提供 KSN 功能。

为了加强对设备和用户数据的保护，Kaspersky Endpoint Security 可以使用卡巴斯基基于云的知识库 - 卡巴斯基安全网络 (KSN) 来检查文件、互联网资源和软件的信誉。使用卡巴斯基安全网络数据可确保更快地响应各种威胁、高保护组件性能和更少的误报。

使用卡巴斯基安全网络是自愿的。您可以随时开始或停止使用 KSN。

KESL 容器不支持 KSN 功能。

卡巴斯基安全网络基础设施解决方案

Kaspersky Endpoint Security 支持以下基础设施解决方案与卡巴斯基的信誉数据库一起使用：

- *卡巴斯基安全网络 (KSN)* – 一种解决方案，从卡巴斯基接收信息并将有关在用户设备上检测到的对象的数据发送到卡巴斯基以供卡巴斯基分析人员进行额外验证并添加到信誉和统计数据库中。
- *卡巴斯基私有安全网络 (KPSN)* – 一种解决方案，允许安装了 Kaspersky Endpoint Security 的设备的用户访问卡巴斯基的信誉数据库以及其他统计数据，而无需从他们的设备向卡巴斯基发送数据。KPSN 专为因例如以下原因而无法使用卡巴斯基安全网络的企业客户所设计：
  - 本地工作场所没有连接到互联网
  - 法律禁止或公司安全限制将任何数据发送到国家或组织的本地网络之外

要在激活新的应用程序授权许可后使用 KPSN，请将新的授权许可密钥告知服务提供商。否则，身份验证错误将阻止与 KPSN 的数据交换。

卡巴斯基安全网络使用选项：

使用 KSN 有两个选项：

- **扩展 KSN 模式** – 您可以从卡巴斯基知识库接收信息，同时 Kaspersky Endpoint Security 会自动向卡巴斯基安全网络发送操作期间获得的统计信息。该应用程序还可以发送给卡巴斯基，针对入侵者可用于损害设备或数据的其他某种文件（或部分文件）进行扫描。
- **基本 KSN 模式** – 您可以从卡巴斯基知识库接收信息，但 Kaspersky Endpoint Security 不会发送有关威胁类型和来源的匿名统计信息和数据。

您可以随时选择不同的卡巴斯基安全网络使用选项。

不会收集、处理或存储任何个人数据。有关在参与 KSN 期间生成的统计信息的存储、销毁和/或提交给卡巴斯基的详细信息，请参阅卡巴斯基安全网络声明和卡巴斯基网站。含有卡巴斯基安全网络声明文本的文件包括在应用程序分发包中。

Kaspersky Endpoint Security 的云模式

*云模式*是 Kaspersky Endpoint Security 的一种运行模式，使用轻量级版本的恶意软件数据库。这样可以减少设备内存的负荷。

卡巴斯基安全网络有助于应用程序使用轻量级恶意软件数据库。

如果 Kaspersky Endpoint Security 在标准模式下运行并使用 KSN，则可以启用云模式。

如果 Kaspersky Endpoint Security 在 Light Agent 模式下运行以保护虚拟环境，则不支持轻量级反恶意软件数据库。该应用程序从 Protection Server 接收 Light Agent 操作所需的特殊数据库。

启用云模式并执行应用程序数据库和模块的最新更新后，Kaspersky Endpoint Security 将切换为使用轻量级版本的恶意软件数据库。如果禁用云模式，Kaspersky Endpoint Security 会在下次更新应用程序数据库和模块时从卡巴斯基服务器下载完整版本的应用程序数据库。

如果不使用 KSN 或禁用云模式，Kaspersky Endpoint Security 将使用完整版本的应用程序数据库。

如果禁用 KSN，将自动禁用云模式。

使用 KSN 代理服务

由管理服务器管理的用户设备可以直接或通过 KSN 代理服务与 KSN 通信。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，KSN 代理服务将支持与 KSN 基础架构的通信。不支持与 KSN 直接通信。如果 KSN 代理不可用，则应用程序不会使用 KSN。

KSN 代理服务器提供以下功能：

- 用户设备可查询 KSN 并将信息提交给 KSN，甚至无需访问互联网即可实现。
- KSN 代理服务器会缓存已处理的数据，从而降低外部网络连接的负载，并提高用户设备所请求信息的接收速度。

可以在“管理服务器”属性中配置 KSN 代理服务器设置。有关 KSN 代理服务器的详细信息，请参阅“Kaspersky Security Center 帮助”。

在 Web Console 中配置使用卡巴斯基安全网络

在 Web Console 中，您可以在策略属性（**应用程序设置** → **高级威胁防护** → **卡巴斯基安全网络**）中配置在 Kaspersky Endpoint Security 中使用卡巴斯基安全网络。

您可以在“卡巴斯基安全网络声明”窗口中阅读**卡巴斯基安全网络声明**的文本，单击**卡巴斯基安全网络声明**链接即可打开该窗口。

Kaspersky Security Center 通过“*资产（设备）*”选项卡上的受管理设备列表中的客户端设备状态（**正常**、**严重**、**警告**）显示有关 KSN 可用性的信息。

卡巴斯基安全网络设置

设置	描述
不使用 KSN	选择此选项即表示您拒绝使用卡巴斯基安全网络。
扩展 KSN 模式	选择此选项，即表示您接受卡巴斯基安全网络的使用条款。您将能够从卡巴斯基在线知识库接收有关文件、Web 资源和软件的信誉的信息。此外，有关各种威胁的类型和来源的匿名统计数据和信息将发送给卡巴斯基，以改进卡巴斯基安全网络。
基本 KSN 模式	选择此选项，即表示您接受卡巴斯基安全网络的使用条款。您将能够从卡巴斯基在线知识库接收有关文件、Web 资源和软件的信誉的信息。
启用云模式	该复选框用于启用或禁用 Kaspersky Endpoint Security 使用轻量级版本恶意软件数据库的运行模式。 如果启用了 KSN，则该复选框可用。 如果您在创建策略时接受了卡巴斯基安全网络声明的条款并在扩展模式下使用 KSN，则该复选框为选中状态。 在下次应用程序数据库更新后，将启用或禁用该模式。 只有在标准模式下使用应用程序时，该设置才适用。
KSN 代理不可用时使用 KSN 服务器	该复选框用于启用或禁用在 KSN 代理服务不可用时直接与 KSN 服务器通信的功能。 默认选中该复选框。 只有在标准模式下使用应用程序时，该设置才适用。
卡巴斯基安全网络声明	此链接将打开“卡巴斯基安全网络声明”窗口，在其中可以阅读卡巴斯基安全网络声明的文本。

卡巴斯基安全网络声明

在此窗口中，您可以阅读卡巴斯基安全网络声明的文本并接受其条款和条件。

卡巴斯基安全网络设置

设置	Description
我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认要使用卡巴斯基安全网络，并且您已完全阅读、理解并接受所显示的卡巴斯基安全网络声明的条款和条件。
我不接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认您不想使用卡巴斯基安全网络。

卡巴斯基专属安全网络声明

在此窗口中，您可以阅读卡巴斯基私有安全网络声明的文本并接受其条款和条件。

卡巴斯基安全网络设置

设置	Description
我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认要加入卡巴斯基安全网络，并且您已完全阅读、理解并接受所显示的卡巴斯基私有安全网络声明的条款和条件。
我不接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认您不想使用卡巴斯基安全网络。

在管理控制台中配置使用卡巴斯基安全网络

在管理控制台中，您可以在策略属性（**高级威胁防护 → 卡巴斯基安全网络**）中配置在 Kaspersky Endpoint Security 中使用卡巴斯基安全网络。

您可以在“卡巴斯基安全网络声明”窗口中阅读**卡巴斯基安全网络声明**的文本，单击**卡巴斯基安全网络声明**链接即可打开该窗口。

Kaspersky Security Center 通过“**设备**”选项卡上的受管理设备列表中的客户端设备状态（*正常*、*严重*、*警告*）显示有关 KSN 可用性的信息。

卡巴斯基安全网络设置

设置	描述
卡巴斯基安全网络声明	单击此链接将打开“**卡巴斯基安全网络声明**”窗口。在此窗口中，可以阅读卡巴斯基安全网络声明的文本。
卡巴斯基安全网络 (KSN)	该块显示有关 KSN 模式的信息或指示 Kaspersky Endpoint Security 未使用 KSN。 单击“**编辑**”按钮会打开一个窗口，在其中可以配置卡巴斯基安全网络的使用。
启用云模式	该复选框用于启用或禁用 Kaspersky Endpoint Security 使用轻量级版本恶意软件数据库的运行模式。 如果启用了 KSN，则该复选框可用。 如果您在创建策略时接受了卡巴斯基安全网络声明的条款并在扩展模式下使用 KSN，则该复选框为选中状态。 在下次应用程序数据库更新后，将启用或禁用该模式。 只有在标准模式下使用应用程序时，该设置才适用。
KSN 代理不可用时使用 KSN 服务器	该复选框用于启用或禁用在 KSN 代理服务不可用时直接与 KSN 服务器通信的功能。 默认选中该复选框。 只有在标准模式下使用应用程序时，该设置才适用。

卡巴斯基安全网络设置

在此窗口中，您可以配置卡巴斯基安全网络加入设置。

卡巴斯基安全网络设置

设置	描述
更多信息...	单击此链接可打开卡巴斯基网站。
不使用卡巴斯基安全网络	选择此选项即表示您拒绝使用卡巴斯基安全网络。
基本 KSN 模式	选择此选项，即表示您接受卡巴斯基安全网络的使用条款。您将能够从卡巴斯基在线知识库接收有关文件、Web 资源和软件的信誉的信息。
扩展 KSN 模式	选择此选项，即表示您接受卡巴斯基安全网络的使用条款。您将能够从卡巴斯基在线知识库接收有关文件、Web 资源和软件的信誉的信息。此外，有关各种威胁的类型和来源的匿名统计数据和信息将发送给卡巴斯基，以改进卡巴斯基安全网络。
卡巴斯基安全网络声明	此链接将打开“卡巴斯基安全网络声明”窗口，在其中可以阅读卡巴斯基安全网络声明的文本。

卡巴斯基安全网络声明

在此窗口中，您可以阅读卡巴斯基安全网络声明的文本并接受其条款和条件。

卡巴斯基安全网络设置

设置	Description
我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认要使用卡巴斯基安全网络，并且您已完全阅读、理解并接受所显示的卡巴斯基安全网络声明的条款和条件。 如果您在“卡巴斯基安全网络设置”窗口中选择了“基本 KSN 模式”或“扩展 KSN 模式”选项，则此选项可用。
我不接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认您不想使用卡巴斯基安全网络。 如果您在“卡巴斯基安全网络设置”窗口中选择了“基本 KSN 模式”或“扩展 KSN 模式”选项，则此选项可用。

卡巴斯基专属安全网络声明

在此窗口中，您可以阅读卡巴斯基私有安全网络声明的文本并接受其条款和条件。

卡巴斯基安全网络设置

设置	Description
我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认要加入卡巴斯基安全网络，并且您已完全阅读、理解并接受所显示的卡巴斯基私有安全网络声明的条款和条件。
我不接受卡巴斯基安全网络声明的条款和条件	选择此选项，即表示您确认您不想使用卡巴斯基安全网络。

在命令行中配置使用卡巴斯基安全网络。

您可以使用常规应用程序设置中的 UseKSN 选项，在命令行中启用或禁用对卡巴斯基安全网络的使用。

您可以借助命令行开关或包含所有常规应用程序设置的配置文件来更改 UseKSN 的值。

要借助命令行开关启用对卡巴斯基安全网络的使用，请运行：

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

其中：

- <Extended/Basic>：卡巴斯基安全网络模式。
- --accept-ksn：表示您同意卡巴斯基安全网络声明中条款的密钥。您确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件。

包含卡巴斯基安全网络声明文本的文件 ksn_license.<语言 ID> 位于目录 /opt/kaspersky/kesl/doc/ 中。

要借助命令行开关禁用对卡巴斯基安全网络的使用，请运行：

```
kesl-control --set-app-settings UseKSN=No
```

要使用配置文件启用或禁用卡巴斯基安全网络，请执行以下命令：

```
kesl-control --set-app-settings --file <配置文件名> [--json] [--accept-ksn]
```

其中：

- --file <配置文件的路径>：配置文件的完整路径，包含所需的常规应用程序设置，其中所需的 UseKSN 值已设置。
- --json：如果您要以 JSON 格式从配置文件导入设置，请指定此键。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。
- --accept-ksn：表示您同意卡巴斯基安全网络声明中条款的密钥。如果要启用对卡巴斯基安全网络的使用，则必须指定密钥。

如果客户端设备上安装的 Kaspersky Endpoint Security 在 Kaspersky Security Center 中分配的策略下运行，则只能使用 Kaspersky Security Center 修改 UseKSN 设置的值。当客户端设备上安装的 Kaspersky Endpoint Security 在策略下停止运行时，以下值将分配给设置：UseKSN=No。

使用命令行检查与卡巴斯基安全网络的连接

要检查与卡巴斯基安全网络的连接，请运行以下命令：

```
kesl-control --app-info
```

“**使用卡巴斯基安全网络**”行显示了与卡巴斯基安全网络的连接状态：

- 如果显示扩展 KSN 模式，Kaspersky Endpoint Security 将使用卡巴斯基安全网络，可以从知识库获取信息，并发送有关威胁类型和来源的匿名统计数据和信息。
- 如果显示基本 KSN 模式，Kaspersky Endpoint Security 将使用卡巴斯基安全网络，可以从知识库获取信息，但是不会发送有关威胁类型和来源的匿名统计数据和信息。
- 如果状态为“已禁用”，则表明 Kaspersky Endpoint Security 未使用卡巴斯基安全网络。

“**卡巴斯基安全网络基础架构**”行显示有关用于与卡巴斯基信誉数据库配合使用的基础架构解决方案的信息：卡巴斯基安全网络或卡巴斯基私人安全网络。

下列原因可导致无法连接到卡巴斯基安全网络：

- 用户设备未连接互联网。
- 卡巴斯基安全网络被禁用。
- 应用程序尚未激活或授权许可已过期。
- 检测到与授权许可密钥有关的问题。例如，密钥在拒绝列表中。

从命令行启用和禁用云模式

*云模式*是 Kaspersky Endpoint Security 的一种运行模式，使用轻量级版本的恶意软件数据库。

如果 Kaspersky Endpoint Security 在 Light Agent 模式下运行以保护虚拟环境，则不支持轻量级反恶意软件数据库。该应用程序从 Protection Server 接收 Light Agent 操作所需的特殊数据库。

您可以在常规应用程序设置中借助“`CloudMode=Yes/No`”选项在命令行中启用或禁用云模式。

您可以使用包含所有常规应用程序设置的配置文件或命令行选项来更改 `CloudMode` 的值。

如果启用对卡巴斯基安全网络的使用，则云模式可用。

高级应用程序设置

您可以配置以下附加应用程序设置：

- 在应用程序中使用代理服务器。
- 全局排除– 将挂载点从文件威胁防护、反加密勒索软件和容器监控组件以及关键区域扫描、容器扫描和可移动驱动器扫描任务的文件操作拦截中排除。
- 从扫描中排除进程内存。
- 文件操作拦截模式。
- 检测威胁入侵者可以用来破坏设备或数据的合法应用程序。
- 应用程序稳定性监控。
- 应用程序启动设置。
- 扫描任务的内存和处理器资源使用限制。
- 应用程序对驻留内存的使用限制。
- 非特权用户可以同时启动的"自定义扫描"任务数量限制。
- 将信息转发至 Kaspersky Security Center 存储的设置。
- 任务管理权限。

配置代理服务器

如果客户端设备的用户使用代理服务器连接到互联网，您可以配置代理服务器设置。Kaspersky Endpoint Security 可使用代理服务器连接到卡巴斯基服务器，例如在更新应用程序数据库和模块时或与卡巴斯基安全网络和 Kaspersky Endpoint Detection and Response (KATA) 通信时。

默认禁用代理服务器。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则不支持使用代理服务器连接卡巴斯基安全网络、SVM 和 Integration Server。

在 Web Console 中配置代理服务器设置

在 Web Console 中，您可以在策略属性中配置代理服务器的使用（**应用程序设置 → 常规设置 → 代理服务器设置**）。

代理服务器设置

设置	Description
不使用代理服务器	如果选择此选项，该应用程序不使用代理服务器。

指定代理服务器设置	如果选择此选项，应用程序将使用指定的代理服务器设置，例如，与 Kaspersky Endpoint Detection and Response (KATA) 进行集成。
Address	用于输入代理服务器的 IP 地址或域名的字段。 如果选择了**使用指定的代理服务器设置**选项，则此字段可用。
Port	用于输入代理服务器端口的字段。 默认值：3128。 如果选择了**使用指定的代理服务器设置**选项，则此字段可用。
使用代理服务器身份验证	启用或禁用使用用户名和密码进行代理服务器身份验证。 如果选择了**"使用指定的代理服务器设置"**选项，则此复选框可用。 默认情况下，清除此复选框。 通过 HTTP 代理连接时，我们建议使用不用于登录其他系统的单独账户。HTTP 代理使用不安全的连接，账户可能会被入侵。
用户名	用于代理服务器身份验证的用户名的输入字段。 如果选中**"使用代理服务器身份验证"**复选框，则该输入字段可用。
编辑	可让您指定用于在代理服务器上进行身份验证的密码。无法编辑**"密码"**字段。默认情况下，密码为空。 要指定密码，请单击**"编辑"**。在打开的窗口中，输入密码，然后单击**"确定"**。 建议确保密码复杂性和反暴力破解机制，使密码无法在 6 个月内被猜出。 单击窗口中的**"显示"**按钮会在密码输入窗口中以明文形式显示密码。 如果选中**"使用代理服务器身份验证"**复选框，则该按钮可用。
使用 Kaspersky Security Center 作为应用程序激活代理服务器	此复选框用于启用或禁用将 Kaspersky Security Center 用作激活应用程序的代理服务器。 如果选中此复选框，则 Kaspersky Endpoint Security 将 Kaspersky Security Center 用作激活应用程序的代理服务器。 默认情况下，清除此复选框。 只有在标准模式下使用应用程序时，该设置才适用。如果在 Light Agent 模式下使用应用程序保护虚拟环境，则授权许可信息由 Protection Server 提供。

在管理控制台中配置代理服务器设置

在管理控制台中，您可以在策略属性中配置代理服务器的使用（**常规设置→代理服务器设置**）。

代理服务器设置

设置	Description

不使用代理服务器	如果选择此选项，该应用程序不使用代理服务器。
指定代理服务器设置	如果选择此选项，该应用程序将使用指定的代理服务器设置（例如）与 Kaspersky Endpoint Detection and Response (KATA) 进行集成。
地址和端口	用于输入代理服务器的 IP 地址或域名及其端口的字段。 默认端口：3128。 如果选择了“**使用指定的代理服务器设置**”选项，则这些字段可用。
使用代理服务器认证	此复选框用于启用或禁用使用用户名和密码进行代理服务器身份验证。 如果选择了“**使用指定的代理服务器设置**”选项，则此复选框可用。 默认情况下，清除此复选框。 通过 HTTP 代理连接时，我们建议使用不用于登录其他系统的单独账户。HTTP 代理使用不安全的连接，账户可能会被入侵。
用户名	用于代理服务器身份验证的用户名的输入字段。 如果选中“**使用代理服务器认证**”复选框，则该输入字段可用。
密码	用于输入代理服务器身份验证的用户密码的输入字段。 建议确保密码复杂性和反暴力破解机制，使密码无法在 6 个月内被猜出。 单击“**显示**”按钮将使用户密码以明文形式显示在“**密码**”字段中。默认情况下，用户密码是隐藏的，并显示为星号。 如果选中“**使用代理服务器身份验证**”复选框，则该文本框和按钮可用。
使用 Kaspersky Security Center 作为应用程序激活代理服务器	此复选框用于启用或禁用将 Kaspersky Security Center 用作激活应用程序的代理服务器。 如果选中此复选框，则 Kaspersky Endpoint Security 将 Kaspersky Security Center 用作激活应用程序的代理服务器。 默认情况下，清除此复选框。 只有在标准模式下使用应用程序时，该设置才适用。如果在 Light Agent 模式下使用应用程序保护虚拟环境，则授权许可信息由 Protection Server 提供。

在命令行中配置代理服务器设置

您可以借助常规应用程序设置中的 `UseProxy` 和 `ProxyServer` 设置，在命令行中启用或禁用应用程序组件对代理服务器的使用。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

`UseProxy` 设置可以使用以下值：

- Yes - 允许使用代理服务器。
- No：禁用代理服务器。

ProxyServer 设置允许您定义代理服务器设置，格式如下：[< 用户 >[:< 密码 >]@]< 代理服务器地址 >[:< 端口 >]，其中：

- < 用户 > 是用于代理服务器认证的用户名。
- < 密码 > 是用于代理服务器认证的用户密码。
- < 代理服务器地址 > 是代理服务器的 IP 地址或域名。
- < 端口 > 是代理服务器端口。

如果连接代理服务器不需要认证，则无需定义 ProxyServer。

> 通过 HTTP 代理连接时，我们建议使用不用于登录其他系统的单独账户。HTTP 代理使用不安全的连接，账户可能会被入侵。

配置全局排除项

您可以配置文件威胁防护和反加密勒索组件的从文件操作拦截中排除挂载点，以及将这些挂载点按恶意软件扫描、关键区域扫描和容器扫描任务从扫描中排除。通过排除挂载点，您可以将挂载在设备上的本地或远程目录排除在文件操作拦截范围之外。此外，全局排除会影响容器监控组件和可移动驱动器扫描任务的运行。

在 Web Console 中配置全局排除项

在 Web Console 中，您可以在策略属性中配置使用全局排除项（**应用程序设置 → 常规设置 → 全局排除项**）。

全局排除部分中的表格包含要从文件操作拦截中排除的挂载点。

"**路径**"列显示排除的挂载点的路径。该表默认为空。

您可以在表中添加、编辑和删除项目。

> 单击"**删除**"按钮可将所选项目从表中删除。
>
> 如果在表中选择至少一项，则此按钮可用。

"添加挂载点排除项"窗口

挂载点设置

设置	描述

文件系统，访问协议和路径	在此下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型： • **本地**：本地挂载点。 • **挂载**：使用 Samba 或 NFS 协议挂载到设备上的远程目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
访问协议	您可以在该下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义** — 在下面的字段中指定的设备文件系统的资源。 如果在文件系统下拉列表中选择**挂载**类型，则此下拉列表可用。
Path	用于输入要从文件操作拦截中排除的挂载点路径的字段。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。 ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。 要排除挂载点 /dir，您需要明确指定 /dir（无星号）。 掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。
共享资源的名称	用于输入要添加到文件操作拦截排除项的目录所在的文件系统共享资源名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在“**访问协议**”下拉列表中选择了“**自定义**”项，则该字段可用。

在管理控制台中配置全局排除项

在管理控制台中，您可以在策略属性中配置使用全局排除项（**常规设置 → 全局排除项**）。

排除的挂载点设置组包含一个“**配置**”按钮。单击此按钮将打开“**排除的挂载点**”窗口。

窗口中的列表包含排除的挂载点的路径。默认情况下，该列表为空。

您可以在列表中添加、编辑和删除项目。

单击“**删除**”按钮可将所选项目从表中删除。

如果在表中选择至少一项，则此按钮可用。

“挂载点路径”窗口

挂载点设置

设置	描述
文件系统，访问协议和路径	该设置块允许您设置挂载点的位置。 在文件系统下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型： • **本地**：本地挂载点。 • **挂载**：使用 Samba 或 NFS 协议挂载到设备上的远程目录。 • **全部远程挂载** – 使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
	如果在文件系统下拉列表中选择**挂载**，则可以在右侧下拉列表中选择远程访问协议： • **NFS**：使用 NFS 协议挂载到设备上的远程目录。 • **Samba**：使用 Samba 协议挂载到设备上的远程目录。 • **自定义**：在下面的字段中指定的设备文件系统的所有资源。
	如果在文件系统下拉列表中选择**本地**，则可以在输入字段中输入要从文件操作拦截中排除的挂载点的路径。您可以使用掩码指定路径。 您可以用 *（星号）字符来创建文件或目录名称掩码。 您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。 您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。 ** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。 要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。 掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。 可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。
文件系统名称	用于输入要从文件操作拦截中排除的目录所在的文件系统名称的字段。 如果在文件系统下拉列表中选择了**挂载**类型，并且在右侧的下拉列表中选择了**自定义**项，则该字段可用。

在命令行中配置全局排除项

您可以通过常规应用程序设置中的 ExcludedMountPoint.item_# 选项在命令行中定义挂载点排除项。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

ExcludedMountPoint.item_# 选项接受以下值：

- AllRemoteMounted – 从文件操作拦截中排除使用 SMB 和 NFS 协议挂载在设备上的所有远程目录。
- Mounted:NFS – 从文件操作拦截中排除使用 NFS 协议挂载在设备上的所有远程目录。
- Mounted:SMB – 从文件操作拦截中排除使用 SMB 协议挂载在计算机上的所有远程目录。
- Mounted:< 文件系统类型 > – 从文件操作拦截中排除具有指定文件系统类型的所有已挂载目录。
- /mnt – 从文件操作拦截中排除 /mnt 挂载点（包括子目录）中的对象。此目录用作可移动驱动器的临时挂载点。
- < 包含 /mnt/user* 或 /mnt/**/user_share> – 从文件操作拦截中排除名称包含指定掩码的挂载点中的对象。

  您可以用 *（星号）字符来创建文件或目录名称掩码。

  您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。

  您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。

  ** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。

  要排除挂载点 /dir，您需要明确指定 /dir（无星号）。

  掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。

  可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

您可以指定要从扫描中排除的多个挂载点。

必须以与 mount 命令输出中所显示的相同方式指定挂载点。

从扫描范围中排除进程内存

您可以从扫描中排除进程内存。应用程序不扫描指定进程的内存。

在 Web Console 中配置排除项

在 Web Console 中，您可以在策略属性中配置从扫描中排除进程内存（**应用程序设置→常规设置→应用程序设置**）。

单击“**从扫描中排除进程内存**”下的“**配置从扫描中排除进程内存**”，将打开“**从扫描中排除进程内存**”窗口，您可以在其中创建排除项列表。

“**从扫描中排除进程内存**”窗口中的列表包含应用程序从进程内存扫描中排除的进程的路径。您可以使用掩码指定路径。默认情况下，该列表为空。

您可以用 * （星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：`/dir/**/file*/` 或 `/dir/file**/`。

** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。

掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

您可以在列表中添加、编辑和删除项目。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从列表中删除所选进程路径。

如果在列表中选择至少一个进程路径，则此按钮可用。

“**编辑**”按钮将打开一个可以在其中更改进程路径的窗口。Kaspersky Endpoint Security 会从扫描中排除指定进程的内存。

“**添加**”按钮将打开一个可以在其中输入进程完整路径的窗口。Kaspersky Endpoint Security 会从扫描中排除指定进程的内存。

在管理控制台中配置排除项

在管理控制台中，您可以在策略属性中配置从扫描中排除进程内存（**常规设置→排除进程内存**）。

单击“**从扫描中排除进程内存**”下的“**配置**”将打开一个窗口，您可以在其中创建排除项列表。

“**从扫描中排除进程内存**”窗口中的列表包含应用程序从进程内存扫描中排除的进程的路径。您可以使用掩码指定路径。默认情况下，该列表为空。

您可以用 *（星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。

** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。

要排除挂载点 /dir，您需要明确指定 /dir（无星号）。

掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

您可以在列表中添加、编辑和删除项目。

单击“**删除**”按钮将使 Kaspersky Endpoint Security 从列表中删除所选进程路径。

如果在列表中选择至少一个进程路径，则此按钮可用。

“**编辑**”按钮将打开一个可以在其中更改进程路径的窗口。Kaspersky Endpoint Security 会从扫描中排除指定进程的内存。

“**添加**”按钮将打开一个可以在其中输入进程完整路径的窗口。Kaspersky Endpoint Security 会从扫描中排除指定进程的内存。

在命令行中配置排除项

您可以通过常规应用程序设置中的 MemScanExcludedProgramPath.item_# 选项，在命令行中配置从扫描中排除进程内存。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

MemScanExcludedProgramPath.item_# 包含本地目录中进程的完整路径。您可以使用掩码指定路径。

您可以用 *（星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。

** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

您可以指定多个要从扫描范围中排除的进程。

选择文件操作拦截模式

文件操作拦截模式会影响文件威胁防护和设备控制组件。

- 在扫描期间，应用程序可以阻止对文件威胁防护组件正在扫描的文件的访问。默认阻止对文件的访问：对所扫描文件的任何访问都必须等到扫描结果出来。如果扫描未检测到文件中存在威胁，应用程序将允许访问该文件。检测感染对象时，应用程序将执行“文件威胁防护”的“**第一个操作**”(`FirstAction`) 和“**第二个操作**” (`SecondAction`) 设置中指定的操作。

  您可以选择不阻止对文件威胁防护组件正在扫描的文件的访问。在这种情况下，则执行异步扫描。

- 当设备控制组件决定是否可以授予对设备的访问权限时，应用程序可以阻止对设备上的文件的访问。默认阻止对文件的访问：对受管理设备上的任何文件的访问都必须等到扫描结果出来。如果扫描后设备控制允许访问包含文件的设备，应用程序将允许访问该文件。

  您可以禁用设备控制组件所监控的设备上的文件访问阻止功能。在这种情况下，设备控制将确定是否允许以异步模式访问设备。

在 Web Console 中配置

在 Web Console 中，您可以在策略属性中配置文件操作拦截模式（**应用程序设置→常规设置→ 应用程序设置、文件操作拦截模式**部分）。

“**扫描期间阻止对文件的访问**”复选框用于启用或禁用在文件威胁防护和设备控制组件扫描文件时阻止对文件的访问。

默认选中该复选框。

如果清除该复选框，则允许在扫描期间访问任何文件，并且扫描以异步模式运行。

在管理控制台中配置

在管理控制台中，您可以在策略属性中配置文件操作拦截模式（**常规设置→ 应用程序设置、文件操作拦截模式**部分）。

“**扫描期间阻止对文件的访问**”复选框用于启用或禁用在文件威胁防护和设备控制组件扫描文件时阻止对文件的访问。

默认选中该复选框。

如果清除该复选框，则允许在扫描期间访问任何文件，并且扫描以异步模式运行。

在命令行中配置

您可以使用常规应用程序设置中的 FileBlockDuringScan设置，在命令行中配置文件操作拦截模式。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

`FileBlockDuringScan` 选项接受以下值：

- `Yes`（默认值） – 在文件威胁防护和设备控制组件扫描文件期间阻止对文件的访问。
- `No` – 在扫描期间允许访问文件。允许请求任何文件，扫描异步完成。

> 这种文件操作拦截模式对系统性能影响较小，但是如果文件在应用程序对文件状态做出决定之前（例如）在扫描过程中更改其名称，则存在文件中的威胁不会被消除或删除的风险。

配置检测黑客可能用来危害的应用程序

您可以启用或禁用对入侵者可以用来破坏设备或数据的合法应用程序的检测。

在 Web Console 中配置

在 Web Console 中，您可以在策略属性中检测入侵者可能用来破坏设备或数据的合法应用程序（**应用程序设置** → **常规设置**→**应用程序设置**、**扫描设置**部分）。

“**检测入侵者可以用来损害设备或数据的合法应用程序**”复选框用于启用或禁用对入侵者可以用来破坏用户设备或数据的合法应用程序的检测。

默认情况下，清除此复选框。

在管理控制台中配置

在管理控制台中，您可以在策略属性中检测入侵者可能用来破坏设备或数据的合法应用程序（**常规设置**→**应用程序设置**、**扫描设置**部分）。

“**检测入侵者可以用来损害设备或数据的合法应用程序**”复选框用于启用或禁用对入侵者可以用来破坏用户设备或数据的合法应用程序的检测。

默认情况下，清除此复选框。

在命令行中配置

在命令行中，您可以使用常规应用程序设置中的DetectOtherObjects设置来启用或禁用检测入侵者可以用来破坏设备或数据的合法应用程序。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

`DetectOtherObjects` 接受以下值：

- `Yes`：启用对入侵者可以用来破坏设备或数据的合法应用程序的检测。
- `No`：不启用对入侵者可以用来破坏设备或数据的合法应用程序的检测。

启用应用程序稳定性监控

您可以启用或禁用 Kaspersky Endpoint Security 稳定性监控，此功能可让您跟踪应用程序异常终止的次数，并将应用程序不稳定运行的情况通知管理员。

在 Web Console 中配置

在 Web Console 中，您可以在策略属性中启用或禁用应用程序稳定性监控（**应用程序设置→常规设置→应用程序设置，高级应用程序设置**部分）。

启用应用程序稳定性监控复选框可启用或禁用对 Kaspersky Endpoint Security 应用程序状态的监控。

默认情况下，清除此复选框。

> 要应用设置，必须重新启动应用程序。

如果应用程序不稳定，则安装了应用程序的设备的属性中会显示以下消息：*自从<日期和时间>以来应用程序异常停止<次数>*。

在管理控制台中配置

在管理控制台中，您可以在策略属性（**常规设置→应用程序设置，高级应用程序设置**部分）中启用或禁用应用程序稳定性监控。

启用应用程序稳定性监控复选框可启用或禁用对 Kaspersky Endpoint Security 应用程序状态的监控。

默认情况下，清除此复选框。

> 要应用设置，必须重新启动应用程序。

如果应用程序不稳定，则安装了应用程序的设备的属性中会显示以下消息：*自从<日期和时间>以来应用程序异常停止<次数>*。

在命令行中配置

在命令行中，您可以使用`kesl.ini` 配置文件中的`TrackProductCrashes` 、 `ProductHealthLogFile`、`WarnThreshold`、`WarnAfter_#_crash`和`WarnRemovingThreshold`设置来配置应用程序稳定性监控。

`TrackProductCrashes`设置可让您启用或禁用应用程序稳定性监控。设置可以使用以下值：

- `Yes/true` – 启用应用程序稳定性监控。
- `No/false` – 不启用应用程序稳定性监控。

`ProductHealthLogFile` 设置可让您指定用于应用程序稳定性监控的文件的路径。默认值：/var/opt/kaspersky/kesl/private/kesl_health.log.

`WarnThreshold` 设置可让您设置应用程序在显示有关不稳定操作的通知之前必须经历指定次数异常停止的时间间隔（以秒为单位）。默认值：3600 秒。

`WarnRemovingThreshold` 设置可让您设置在此后清除应用程序不稳定状态的时间间隔（以秒为单位）。默认值：86400 秒。

`WarnAfter_#_crash` 设置可让您设置在显示有关应用程序不稳定操作的通知之前所需的应用程序异常停止的次数。该设置可采用 0 至 10 之间的值。默认值：10。如果值为 0，则不显示不稳定的应用程序通知。

配置应用程序启动设置

您可以配置应用程序启动设置。

在 Web Console 中设置限制

在 Web Console 中，您可以在策略属性中配置应用程序启动设置（**应用程序设置→常规设置→应用程序设置**，**应用程序启动设置**部分）。

应用程序启动设置

设置	描述
启动应用程序的最大连续不成功尝试次数	启动应用程序的最大连续不成功尝试次数的输入字段。 默认值：5。
等待应用程序启动的最长时间(分钟)	等待应用程序启动的最长时间（以分钟为单位）的输入字段，此后 kesl 进程将重新启动。 默认值：3。

在管理控制台中设置限制

在管理控制台中，您可以在策略属性中配置应用程序启动设置（**常规设置→ 应用程序设置**、**应用程序启动设置**部分）。

在**应用程序启动设置**下，单击**配置**按钮打开**应用程序启动设置**窗口，您可以在其中编辑应用程序启动设置（见下表）。

应用程序启动设置

设置	描述
启动应用程序的最大连续不成功尝试次数	启动应用程序的最大连续不成功尝试次数的输入字段。 默认值：5。
等待应用程序启动的最长时间(分钟)	等待应用程序启动的最长时间（以分钟为单位）的输入字段，此后 kesl 进程将重新启动。

	默认值：3。

在命令行中设置限制

在命令行中，您可以使用`kesl.ini` 配置文件中的`MaxRestartCount`和StartupTimeout设置来配置应用程序启动设置。

`MaxRestartCount`设置可让您设置启动应用程序的不成功连续尝试的最大次数。该设置可采用 1 至 10 之间的值。默认值：5。

`StartupTimeout`设置可让您设置等待应用程序启动的最长时间（以分钟为单位），此后 kesl 进程将重新启动。设置可采用 1 至 60 之间的值。默认值：3。

限制内存和处理器资源的使用

您可以设置扫描任务的 CPU 使用率限制。默认不设置限制。您还可以配置扫描任务的内存使用限制。默认限制为 8192 兆字节。

在 Web Console 中设置限制

在 Web Console 中，您可以启用和禁用 CPU 利用率限制，并在策略属性（**应用程序设置→常规设置→应用程序设置，性能**部分）中配置扫描任务的内存使用限制。

设置

设置	描述
扫描任务的内存使用限制 (MB)	扫描任务的内存使用限制的输入字段（以兆字节为单位）。 默认值：8192。
限制扫描任务的 CPU 使用量 (%)	该复选框用于启用或禁用对恶意软件扫描、关键区域扫描、清查和容器扫描任务的 CPU 利用率限制。 如果选中该复选框，则所有处理器核心的最大利用率将不会超过“**上限 (%)**”中指定的数字。 默认情况下，清除此复选框。

在管理控制台中设置限制

在管理控制台中，您可以启用和禁用 CPU 利用率限制，并在策略属性（**常规设置→应用程序设置，性能**部分）中配置扫描任务的内存使用限制。

在**“性能”**下，单击**“配置”**按钮将打开**CPU 和内存使用**窗口，您可以在其中配置限制（见下表）。

设置

设置	描述
限制扫描任务的 CPU 利用率 (%)	该复选框用于启用或禁用对恶意软件扫描、关键区域扫描、清查和容器扫描任务的 CPU 利用率限制。 如果选中该复选框，则所有处理器核心的最大利用率将不会超过右侧字段中指定的百分比。

	默认情况下，清除此复选框。
扫描任务的内存使用限制 (MB)	扫描任务的内存使用限制的输入字段（以兆字节为单位）。 默认值：8192。

在命令行中设置限制

在命令行中，您可以使用常规应用程序设置中的`UseOnDemandCPULimit`和`OnDemandCPULimit`设置配置*ODS*、*ContainerScan*和*InventoryScan*任务的 CPU 使用率限制。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

`UseOnDemandCPULimit` 接受以下值：

- `Yes`：启用“*ODS*”、“*ContainerScan*”和“*InventoryScan*”任务的 CPU 使用率限制。
- `No`：禁用任务的 CPU 使用率限制。

`OnDemandCPULimit` 选项设置运行 *ODS*、*ContainerScan* 和 *InventoryScan* 任务时所有处理器核心的最大利用率级别（以百分比表示）。该选项接受 10 至 100 之间的值。默认值：100。

在命令行中，您可以使用*kesl.ini 配置文件*中的*ScanMemoryLimit*设置配置*ODS*、`ContainerScan`和InventoryScan任务的内存使用限制。默认值：8192。

限制应用程序对驻留内存的使用

您可以配置应用程序对驻留内存的使用限制。默认情况下，会自动设置限制。

在 Web Console 中设置限制

在 Web Console 中，您可以在策略属性中启用或禁用驻留内存使用限制（**应用程序设置→常规设置→应用程序设置高级应用程序设置**部分）。

在**高级应用程序设置**部分中，**配置内存使用**链接可打开一个窗口，您可以在其中配置驻留内存使用限制（请见下表）。

设置

设置	描述
应用程序的驻留内存使用率	在下拉列表中，您可以选择如何限制驻留内存的使用： • **无限制**。当选择此项时，驻留内存的使用不受限制。 • **限制为总额的百分比**。选择此项后，**“内存使用限制（%）”**字段将可用，您可以在其中以百分比形式指定必要值。 • **限制为以 MB 为单位的值**。选择此项后，**内存使用限制（MB）**字段将可用，您可以在其中指定所需的值（以兆字节为单位）。 • **限制为最低者 (%，MB)**。选择此项后，**内存使用限制 (%)**和**内存使用限制 (MB)**字段将可用，您可以在其中指定必要的值。

	• **限制为最高者 (%，MB)**。选择此项后，**内存使用限制 (%)**和**内存使用限制 (MB)**字段将可用，您可以在其中指定必要的值。 • **自动限制(建议)**。选中此项时，将自动限制驻留内存的使用量（默认值）。
内存使用限制 (%)	内存使用限制的输入字段（作为百分比）。 默认值：50。
内存使用限制 (MB)	内存使用限制的输入字段（以兆字节为单位）。 默认值：2000。

在管理控制台中设置限制

在管理控制台中，您可以在策略属性中配置驻留内存使用限制（**常规设置→ 应用程序设置**）。

在**高级应用程序设置**部分，单击**配置**按钮打开**附加设置**窗口，您可以在其中配置驻留内存使用限制（见下表）。

设置

设置	描述
应用程序内存使用情况	在下拉列表中，您可以选择如何限制驻留内存的使用： • **无限制**。当选择此项时，驻留内存的使用不受限制。 • **自动限制(建议)**。选中此项时，将自动限制驻留内存的使用量（默认值）。 • **限制为总额的百分比**。选择此项后，**“内存使用限制（%）”**字段将可用，您可以在其中以百分比形式指定必要值。 • **限制为以 MB 为单位的值**。选择此项后，**内存使用限制（MB）**字段将可用，您可以在其中指定所需的值（以兆字节为单位）。 • **限制为最低者 (%，MB)**。选择此项后，**内存使用限制 (%)**和**内存使用限制 (MB)**字段将可用，您可以在其中指定必要的值。 • **限制为最高者 (%，MB)**。选择此项后，**内存使用限制 (%)**和**内存使用限制 (MB)**字段将可用，您可以在其中指定必要的值。
内存使用限制 (%)	内存使用限制的输入字段（作为百分比）。 默认值：50。
内存使用限制 (MB)	内存使用限制的输入字段（以兆字节为单位）。 默认值：2000。

在命令行中设置限制

在命令行中，您可以使用`kesl.ini` 配置文件中的MaxMemory设置来配置驻留内存使用限制。

`MaxMemory` 设置可以使用以下值：

- `off` – 驻留集大小不受限制。

- < 值 >% – 介于 1 到 100 之间的值，表示内存的百分比。
- < 值 >MB – 以 MB 为单位的值。
- lowest/< 值 >%/< 值 >MB/ – 以百分比表示的值与以 MB 为单位的值之间的较小值。
- highest/< 值 >%/< 值 >MB/ – 以百分比表示的值与以 MB 为单位的值之间的较大值。
- auto – 最多 50% 的可用内存，但不少于 2 GB 且不超过 16 GB。

默认值：auto。

限制“自定义扫描”任务的数量

您可以对非特权用户能够在设备上同时运行的自定义扫描任务的数量设置限制。具有 root 权限的用户可以运行的任务数量没有限制。

您可以通过常规应用程序设置中的 LimitNumberOfScanFileTasks 选项，在命令行中启用或禁用并发自定义扫描任务的数量限制。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

LimitNumberOfScanFileTasks 接受 0 至 4294967295 之间的值。默认值：0。

如果指定为 0，则非特权用户将无法启动自定义扫描任务。

如果在安装应用程序时安装了图形用户界面包，则“LimitNumberOfScanFileTasks”设置的默认值为 5。

配置将信息发送到 Kaspersky Security Center 备份

在 Kaspersky Security Center 中，您可以启用或禁用将有关未处理的文件和已连接设备的信息转发到 Kaspersky Security Center 存储。

有关未处理文件的信息显示在 Web Console（操作 → 存储 → 活动威胁）和管理控制台（高级 → 存储 → 活动威胁）中的活动威胁列表中。

有关安装在客户端设备上或连接到客户端设备的设备的信息显示在 Web Console（操作 → 存储 → 硬件）和管理控制台（高级 → 存储 → 硬件）的硬件列表中。如果启用了设备控制，则会转发信息。

在 Web Console 中启用或禁用信息转发

在 Web Console 中，您可以在策略属性（应用程序设置→常规设置→存储设置）中启用或禁用发送信息。

将信息转发至 Kaspersky Security Center 存储的设置

设置	描述
已启用/已禁用就未处理文件进行告知	此切换开关用于启用或禁用向管理服务器发送有关扫描期间无法处理的文件的通知。 默认情况下，复选切换按钮处于打开状态。
告知已安装的设备已启用/已禁用	此切换开关可启用或禁用将有关安装在客户端设备上或连接到客户端的设备的信息转发到管理服务器。

	此切换开关默认打开。

在管理控制台中启用和禁用信息转发

在管理控制台中，您可以在策略属性（**常规设置→存储设置**）中启用或禁用发送信息。

将信息转发至 Kaspersky Security Center 存储的设置

设置	Description
通知未处理的文件	此复选框启用或禁用向管理服务器发送有关扫描期间无法处理的文件的通知。 默认选中该复选框。
通知已安装的设备	此复选框启用或禁用将有关安装在客户端设备上或连接到客户端的设备的信息转发到管理服务器。 默认选中该复选框。

配置任务管理的权限

您可以在 Kaspersky Security Center 定义以下用户权限：

- 查看在 Kaspersky Endpoint Security 中创建的任务
- 在客户端设备上查看在 Kaspersky Security Center 中创建的任务

在 Web Console 中配置

在 Web Console 中，您可以在策略属性（**应用程序设置→本地任务→任务管理**）中设置查看任务的权限。

任务管理设置

设置	Description
允许用户查看和管理本地任务	此复选框允许或阻止用户查看在 Kaspersky Endpoint Security 中创建的本地任务，并在受管理客户端设备上控制这些任务。 默认情况下，清除此复选框。
允许用户查看和管理通过 KSC 创建的任务	此复选框允许或禁止用户查看在 Kaspersky Security Center Web Console 中创建的任务，以及在受管理客户端设备上管理这些任务。 默认情况下，清除此复选框。

在管理控制台中配置

在管理控制台中，您可以在策略属性（**本地任务→任务管理**）中设置查看任务的权限。

任务管理设置

设置	Description
允许用户查看和管理本地任务	此复选框允许或阻止用户查看在 Kaspersky Endpoint Security 中创建的本地任务，并在受管理客户端设备上控制这些任务。 默认情况下，清除此复选框。

允许用户查看和管理通过 KSC 创建的任务	此复选框允许或禁止用户查看在 Kaspersky Security Center 中创建的任务，并在受管理客户端设备上管理这些任务。 默认情况下，清除此复选框。

备份

如果 Kaspersky Endpoint Security 在扫描受保护设备时检测到文件中的恶意代码，应用程序会阻止该文件、将其分配为“*已感染*”状态、将副本放入备份并尝试清除该文件。

*备份*会保留在清除过程中被删除或修改的文件的副本。在清除或删除文件之前会创建*备份副本*。文件的备份副本以特定格式保存并且不会带来威胁。

如果文件成功清除，则备份副本的状态将更改为“*已清除*”。有时，在清除过程中无法维护文件的完整性。如果您在清除后部分或完全无法访问已清除文件中的重要信息，则可以尝试将文件的已清除副本恢复到其原始目录。

我们建议，仅当备份副本的状态为“*已清除*”时，才从备份副本中恢复文件。恢复受感染的对象可能会导致设备感染。

文件的备份副本可能包含个人数据。访问备份对象需要 root 权限。

您还可以配置以下备份设置：

- 备份中对象的存储时间。默认情况下，对象保留 90 天。
- 最大备份容量。默认情况下，备份的大小不受限制。
- 文件路径。默认情况下，备份存储位于 /var/opt/kaspersky/kesl/common/objects-backup/ 目录中。

当指定的保留期到期或达到最大备份容量时，应用程序会自动删除任何状态下的备份副本。

您可以手动删除已恢复或未恢复的文件的备份副本。

Kaspersky Security Center 会生成客户端设备上由卡巴斯基应用程序放置在备份中的文件的一般列表，该列表可在管理控制台（**高级→存储→备份**）和 Web Console（**操作→存储→备份**）中查看。您可以查看受保护设备上备份副本的属性、在备份中运行恶意软件扫描以及删除文件。Kaspersky Security Center 不会将文件从备份复制到管理服务器；所有文件都存储在受保护设备上的备份存储中。文件恢复在受保护的设备中进行。

在 Web Console 中配置备份设置

在 Web Console 中，您可以在策略属性（**应用程序设置→常规设置→存储设置**）中配置备份设置。

备份设置

设置	描述
已启用/已禁用有关备份中的文件的通知	此切换开关可启用或禁用向管理服务器发送有关备份存储中文件的通知。 默认情况下，复选切换开关处于打开状态。
存储对象不超过 (天)	用于指定对象在备份存储内的存储期限的输入字段。 可用值：0–3653。 默认值：90。如果指定 0，则对象可在存储内无限期存储。
备份大小限制为 (MB)	用于指定备份存储的最大容量 (MB) 的输入字段。 可用值：0–999999。默认值：0（无限制）。

在管理控制台中配置备份设置

在管理控制台中，您可以在策略属性（**常规设置→存储设置**）中配置备份设置。

备份设置

设置	描述
告知备份中的文件	此复选框启用或禁用向管理服务器发送有关备份存储中的文件的通知。 默认选中该复选框。
存储对象不超过(天)	此复选框用于启用或禁用备份存储中对象的存储期限制（天数）。 可用值：0–3653。 默认值：90。如果指定 0，则对象可在存储内无限期存储。
备份大小限制为 (MB)	此复选框用于启用或禁用最大存储容量 (MB)。 可用值：0–999999。默认值：0（无限制）。

在命令行中配置备份设置

您可以通过“*备份*”预定义任务在命令行中配置备份。

备份管理任务默认启动。您可以手动启动或停止它。

您可以通过编辑“备份管理”预定义任务的设置来配置备份。

备份管理任务设置

设置	Description	值
`DaysToLive`	在备份存储中存储对象的时间段（天数）。 要删除对象保留限制，请设置 0。	0：无限保留。 默认值：90。
`BackupSizeLimit`	最大备份容量 (MB)当达到最大备份存储容量时，应用程序会删除掉最旧的对象。 要移除备份容量限制，请设置 0。	0 – 999999 0：无限制容量。 默认值：0。
`BackupFolder`	备份目录的路径。您可以指定一个与默认目录不同的自定义备份存储目录。您可以使用任何设备上的目录作为备份存储。不推荐分配位于远程设备上的目录，例如通过 Samba 和 NFS 协议挂载的目录。 更改设置并重新启动应用程序后，Kaspersky Endpoint Security 开始将对象移动到指定的目录。 如果指定的目录不存在或不可用，应用程序将使用默认目录。	默认值：/var/opt/kaspersky/kesl/common/objects-backup/ 需要 root 特权才能访问备份存储目录。

在命令行中操作备份对象

您可以在命令行中使用备份管理命令对备份对象执行以下操作：

- 查看备份对象详细信息。
- 从备份中删除部分或全部对象。
- 从备份中恢复对象。

恢复受感染的对象可能会导致设备感染。

查看备份对象详细信息

要查看备份中对象的详细信息，请运行：

```
kesl-control -B --query ["<筛选条件>"] [-n <数量>] [--json]
```

其中：

- <筛选条件>：一个或多个逻辑表达式，格式为 <字段><比较运算符>'<值>'，结合逻辑运算符 and 来限制结果。如果您不指定任何筛选条件，应用程序将显示备份中的所有对象的详细信息。
- <数量>：要显示的最近对象的数量。如果您不指定 -n 开关，则会显示最后 30 个对象。指定 0 则显示所有对象。
- --json：以 JSON 格式输出数据。

ObjectId 行显示应用程序在将对象放入备份时分配给该对象的数字标识符。该 ID 用于对对象执行操作，例如从备份存储中恢复或删除对象。

从备份中恢复对象

要将对象以其原始名称还原到其原始位置，请执行以下命令：

```
kesl-control --restore <对象 ID>
```

其中 <对象 ID> 是应用程序在将对象放入备份时分配给该对象的数字标识符。

要将对象以新名称恢复到指定目录，请执行以下命令：

```
kesl-control --restore <对象 ID> --file <文件名和路径>
```

其中 --file <文件名和路径> 是文件的新名称和要将文件保存到其中的目录的路径。如果指定的目录不存在，应用程序将创建该目录。

从备份中删除对象

要从备份中移除所选对象，请运行：

```
kesl-control --mass-remove --query "< 筛选条件 >"
```

其中 < 筛选条件 > 是一个或多个逻辑表达式，格式为 < 字段 > < 比较运算符 > ‘< 值 >’，结合逻辑运算符 and 来限制结果。

例如：
要移除 ID=15 的对象，请执行以下操作：

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

要移除名称或路径中包含“test”的对象：

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

要从备份中移除所有对象，请运行：

```
kesl-control -B --mass-remove
```

与 Detection and Response 解决方案集成

卡巴斯基的 Detection and Response 解决方案是旨在检测组织基础设施各个层面的高级威胁和攻击迹象的安全系统。Detection and Response 解决方案提供有关检测到的威胁的信息，可让您管理对检测的响应。

Kaspersky Endpoint Security 可与以下 Kaspersky Detection and Response 解决方案进行互操作：

- Kaspersky Anti Targeted Attack Platform（Kaspersky Endpoint Detection and Response 组件）。与 Kaspersky Endpoint Detection and Response (KATA) 的集成由 Kaspersky Endpoint Security 组件 Endpoint Detection and Response (KATA) (EDR (KATA)) 得到促进。
- Kaspersky Endpoint Detection and Response Optimum。Kaspersky Endpoint Security 组件 Endpoint Detection and Response Optimum (EDR Optimum) 促进了集成。
- Kaspersky Managed Detection and Response。Kaspersky Endpoint Security 组件 Managed Detection and Response (MDR) 促进了集成。

如果 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 集成，可以将大量事件写入 systemd 日志。如果要禁用将审计事件记录到 systemd 日志，请禁用 systemd-journald-audit 套接字并重新启动操作系统。

要禁用 systemd-journald-audit 套接字，请运行以下命令：

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket

systemctl mask systemd-journald-audit.socket
```

默认情况下，在 SintezM-Client 操作系统上，auditd 服务配置受到修改保护，即处于`enabled 2`模式。当 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response和Kaspersky Anti Targeted Attack Platform 解决方案集成时，为了行为检测组件能够正确运行，请将配置文件中的 auditd 模式更改为`enabled 1`（无配置阻止）并重新启动操作系统。

关于 Detection and Response 解决方案命令的响应操作

Kaspersky Endpoint Security 可以执行旨在提供安全功能的响应操作：

- 与 Kaspersky Endpoint Detection and Response (KATA) 交互时，这是 Kaspersky Anti Targeted Attack Platform 解决方案的一个组件。
- 与 Kaspersky Endpoint Detection and Response Optimum 交互时。

Kaspersky Anti Targeted Attack Platform 和Kaspersky Endpoint Detection and Response Optimum 的响应操作设置不同。

Kaspersky Endpoint Security 可以执行以下响应操作：

- 从设备获取文件。

  此操作使用*获取文件*任务执行。例如，您可以将应用程序配置为获取第三方程序生成的事件日志文件。

- 从设备中删除文件。

  此操作使用*删除文件*任务执行。

- 在设备上远程运行进程。

  此操作使用*运行流程*任务执行。

  例如，您可以远程运行用于创建设备配置文件的实用程序，然后使用“*获取文件*”来获取该文件。

- 远程终止设备上的进程。

  该操作使用*终止进程*任务执行。

  例如，您可以远程终止使用“运行进程”任务启动的互联网速度测试实用程序。

- 检测设备上的*入侵指标*并执行威胁响应行动。

  此操作使用*IOC 扫描*任务执行。

  *IOC 扫描*任务仅在操作系统的主命名空间中检查 IOC 项（IOC 对象的属性，例如文件哈希）。*IOC 扫描*任务不会计算大于 200 MB 的文件的哈希。

- 启用或禁用设备的网络隔离。

  当 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 交互时，您可以：

  - 在 Web Console 中启用或禁用网络隔离。
  - 在命令行中禁用网络隔离。
  - 在 Web Console 中配置自动禁用网络隔离。

  当 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 交互时，您可以：

  - 在命令行中禁用网络隔离。
  - 在 Kaspersky Endpoint Detection and Response (KATA) 解决方案中启用或禁用网络隔离。

    要了解更多信息，请查看“Kaspersky Anti Targeted Attack Platform 帮助”。

网络隔离限制

使用网络隔离时，我们强烈建议您熟悉下述限制。

要使网络隔离起作用，必须运行 Kaspersky Endpoint Security。如果 Kaspersky Endpoint Security 出现故障（且应用程序未运行），则当 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Endpoint Detection and Response Optimum 启用网络隔离时，无法保证流量阻止。

启用网络隔离的传输流量受到支持，但有限制，并且可能会被过滤。

DHCP 和 DNS 不会自动添加到网络隔离例外中，因此如果在网络隔离期间更改资源的网络地址，Kaspersky Endpoint Security 将无法访问该资源。这同样适用于容错 KATA 服务器的节点。我们建议不要更改它们的地址，这样 Kaspersky Endpoint Security 不会与它们失去联系。

代理服务器也不会被自动添加到网络隔离排除项中，因此您需要手动将其添加到排除项中，以便 Kaspersky Endpoint Security 不会失去与 KATA 服务器的联系。

不支持按名称向网络隔离添加进程和从网络隔离中排除进程。

如果在标准模式下使用 Kaspersky Endpoint Security，我们建议在使用网络隔离时执行以下操作：

- 使用 KSN 代理服务器与卡巴斯基安全网络进行交互。
- 使用 Kaspersky Security Center 作为应用程序激活代理服务器。

  如果无法使用 Kaspersky Security Center 作为代理服务器，请配置所需代理服务器的设置并将其添加到排除项中。
- 指定 Kaspersky Security Center 作为数据库更新源。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，则这些建议不适用。

Kaspersky Endpoint Detection and Response (KATA) 集成

Kaspersky Endpoint Detection and Response (KATA) 是 Kaspersky Anti Targeted Attack Platform 解决方案的一个组件。与 Kaspersky Endpoint Detection and Response (KATA) 组件的集成由 Kaspersky Endpoint Security 组件 Endpoint Detection and Response (KATA) (EDR (KATA)) 得到促进。

Kaspersky Endpoint Security 与 Kaspersky Anti Targeted Attack Platform 解决方案兼容，旨在保护组织的 IT 基础设施并迅速检测威胁，例如零日攻击、针对性攻击和高级持续性威胁 (APT)。要了解更多信息，请查看 "Kaspersky Anti Targeted Attack Platform 帮助"。

KESL 容器不支持此功能。

与 Kaspersky Endpoint Detection and Response (KATA) 交互时，Kaspersky Endpoint Security 可以：

- 将有关设备上事件的数据（遥测数据）发送到具有中央节点组件（"KATA 服务器"）的 Kaspersky Anti Targeted Attack Platform 服务器。Kaspersky Endpoint Security 向 KATA 服务器发送有关进程、打开的网络连接和修改文件的监控数据，以及有关应用程序检测到的威胁的数据和处理这些威胁的结果数据。
- 在接收到 Kaspersky Anti Targeted Attack Platform 的命令时执行响应操作以确保安全。

为了与 Kaspersky Endpoint Detection and Response (KATA) 集成，必须启用行为检测组件。

仅当启用行为检测时，才可以将 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Security 和 EDR (KATA) 集成。否则，无法传输所需的遥测数据。

Kaspersky Endpoint Detection and Response (KATA) 还可以使用从以下组件收到的数据：

- 文件威胁防护。
- 网络威胁防护。
- Web 威胁防护。

当与 Kaspersky Endpoint Detection and Response (KATA) 集成时，具有 Kaspersky Endpoint Security 的设备会通过 HTTPS 协议与 KATA 服务器建立安全连接。为确保安全连接，使用 KATA 服务器颁发的以下证书：

- KATA 服务器证书。使用服务器的 TLS 证书对连接进行加密。您可以通过在 Kaspersky Endpoint Security 端验证服务器证书来提高连接的安全性。为此，请在启用 Kaspersky Endpoint Detection and Response (KATA) 集成之前添加 Integration Server 证书。

- 客户端证书。此证书用于使用双向身份验证对连接进行额外保护（使用 Kaspersky Endpoint Security KATA 服务器扫描设备）。多个设备可以使用同一客户端证书。默认情况下，KATA 服务器不检查客户端证书，但可以在 Kaspersky Anti Targeted Attack Platform 端启用双向身份验证。在这种情况下，您需要在 Kaspersky Endpoint Detection and Response (KATA) 集成设置中启用双向身份验证并添加客户端证书（带证书和私钥的加密容器）。

用于保护与 KATA 服务器的连接的证书由 Kaspersky Anti Targeted Attack Platform 管理员提供。

如果在 Kaspersky Endpoint Security 的常规应用程序设置中配置了使用代理服务器，则使用代理服务器连接到 KATA 服务器。

默认情况下，Kaspersky Endpoint Detection and Response (KATA) 集成被禁用。您可以通过命令行、 Web Console 和管理控制台启用或禁用集成，并配置以下集成设置：

- 添加常规 KATA 服务器连接设置。
- 添加或删除 KATA 服务器证书。
- 配置连接 KATA 服务器时执行双向认证并添加客户端证书。
- 配置事件转发。
- 启用或禁用发送遥测。

  如果启用 Kaspersky Endpoint Security 和 Kaspersky Managed Detection and Response 之间的集成，则发送遥测时不会应用进程排除项。

不支持在 Kaspersky Security Center 云控制台中管理 Kaspersky Endpoint Detection and Response (KATA) 集成设置。

在 Web Console 中配置 Kaspersky Endpoint Detection and Response (KATA) 集成

在 Web Console 中，您可以在策略属性中启用、禁用或配置 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 之间的集成（**应用程序设置 → Detection and Response→Endpoint Detection and Response (KATA)**）。

不支持在 Kaspersky Security Center 云控制台中管理 Kaspersky Endpoint Detection and Response(KATA) 集成设置。

Kaspersky Endpoint Detection and Response (KATA) 集成设置

设置	描述
Endpoint Detection and Response (KATA) 已启用/已禁用	启用或禁用 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response (KATA) 的集成。

	默认情况下，禁用 Integration Server。
服务器连接设置	单击“**配置**”链接将打开一个窗口，您可以在其中配置连接到 KATA 服务器的常规设置，添加服务器证书，并配置连接到 KATA 服务器时的双向认证。
KATA 服务器	该表包含配置了连接的 KATA 服务器的列表。 “**添加**”按钮将打开一个窗口，在其中可以配置与 KATA 服务器的连接。 您可以使用表格上方的按钮来编辑和删除以前配置的连接设置。
发送事件时的最大延时（秒）	向 KATA 服务器发送事件的最大延迟（以秒为单位）。 默认值为 `30`。
启用事件限制	启用或禁用调节发送到 KATA 服务器的事件数。
每小时的最大事件数量	每小时的最大事件数量 默认值为 `3000`。
事件限制阈值（百分比）	事件限制阈值（百分比）。如果一种类型的事件（例如，有关注册表更改的事件）占事件总数的比例超过设置的阈值（以百分比表示），则发送事件将受到限制。 默认值为 `15`。

“服务器连接设置”窗口

在此窗口中，您可以配置连接到 KATA 服务器的常规设置，添加服务器证书，并配置连接到 KATA 服务器时的双向身份验证。

KATA 服务器连接设置

设置	描述
发送同步请求到 KATA 服务器的间隔（分钟）	发送同步请求到 KATA 服务器的间隔（以分钟为单位）。 默认值为 `5`。
等候服务器连接的最长时间（秒）	等待与 KATA 服务器连接的最长时间（以秒为单位）。 默认值为 `10`。
等候服务器响应的最长时间(秒)	等待 KATA 服务器响应的最长时间（以秒为单位）。 默认值为 `10`。
允许发送遥测数据	启用或禁用将有关设备上事件的数据（遥测数据）发送到 KATA 服务器。 默认启用发送遥测数据。
服务器证书	添加服务器证书后，显示有关证书的信息： • 证书序列号 • 证书主题 • 证书颁发者 • 证书开始日期 • 证书到期日期
选择	打开一个标准文件选择窗口，在其中可以指定 KATA 服务器证书的路径。

	如果已添加服务器证书，则在 Kaspersky Endpoint Security 端验证服务器证书。这提高了连接的安全性。
Remove	删除之前添加的服务器证书。 仅当已添加服务器证书时，才会显示该按钮。
附加连接保护	设置部分允许您在连接到 KATA 服务器时启用或禁用双向身份验证和添加客户端证书。
使用双重身份验证	启用或禁用双向身份验证以进一步保护与 KATA 服务器的连接。 必须在 KATA 服务器端启用双向身份验证。 要使用双重身份验证，您需要添加客户端证书。
添加客户端证书	打开一个标准文件选择窗口，在其中可以指定带有客户端证书和私钥的加密容器（PFX 存档）的路径。 如果选中“**使用双重身份验证**”复选框，则该按钮可用。
编辑	允许您为含有客户端证书的加密容器指定密码。无法编辑“**加密容器密码**”字段。默认情况下，密码为空。 要指定密码，请单击“**编辑**”。在打开的窗口中，输入密码，然后单击“**确定**”。单击窗口中的“**显示**”按钮会在密码输入窗口中以明文形式显示密码。 建议确保密码复杂性和反暴力破解机制，使密码无法在 6 个月内被猜出。 如果选中“**使用双重身份验证**”复选框，则该按钮可用。

与 KATA 服务器的连接设置窗口

在此窗口中，可以指定与 KATA 服务器的连接设置。

KATA 服务器连接设置

设置	描述
Address	KATA 服务器地址。可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。 为设备启用网络隔离后，为了确保与 KATA 服务器的通信在应用程序发生故障时不中断，建议指定服务器的 IP 地址。 默认值：`127.0.0.1`。
Port	用于连接到 KATA 服务器的端口。 默认值为 443。

在管理控制台中配置 Kaspersky Endpoint Detection and Response (KATA) 集成

在管理控制台中，您可以在策略属性中启用、禁用或配置 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 之间的集成（**Detection and Response→Endpoint Detection and Response (KATA)**）。

Kaspersky Endpoint Detection and Response (KATA) 集成设置

设置	描述
与 Endpoint Detection and Response (KATA) 集成。	启用或禁用 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response (KATA) 的集成。 默认情况下，禁用 Integration Server。
KATA 服务器	“**配置**”按钮将打开“**KATA 服务器**”窗口。在此窗口中，您可以配置与 KATA 服务器的连接并查看已配置连接的服务器列表。
服务器连接设置	单击“**配置**”按钮将打开一个窗口，您可以在其中配置连接到 KATA 服务器的常规设置，添加服务器证书，并配置连接到 KATA 服务器时的双向认证。
数据传输设置	单击“**配置**”按钮将打开一个窗口，您可以在其中配置传输到 KATA 服务器的数据的设置。

“KATA 服务器”窗口

窗口中的表格显示用于连接到 KATA 服务器的设置列表。对于已配置连接的每个服务器，该表都指示一个 IP 地址（IPv4 或 IPv6）或服务器的完全限定域名 (FQDN) 和端口。

您可以使用表格上方的按钮和菜单执行以下操作：

- 添加 KATA 服务器连接设置
- 编辑或删除以前配置的连接设置
- 导出或导入已配置的连接设置列表

与 KATA 服务器的连接设置窗口

在此窗口中，可以指定与 KATA 服务器的连接设置。

KATA 服务器连接设置

设置	描述
Address	KATA 服务器地址。可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。 为设备启用网络隔离后，为了确保与 KATA 服务器的通信在应用程序发生故障时不中断，建议指定服务器的 IP 地址。 默认值：`127.0.0.1`。
Port	用于连接到 KATA 服务器的端口。 默认值为 `443`。

“服务器连接设置”窗口

在此窗口中，您可以配置连接到 KATA 服务器的常规设置。

KATA 服务器连接设置

设置	描述
发送同步请求到 KATA 服务器的间隔（分钟）	发送同步请求到 KATA 服务器的间隔（以分钟为单位）。 默认值：5。
等候服务器连接的最长时间（秒）	等待与 KATA 服务器连接的最长时间（以秒为单位）。 默认值为 10。
等候服务器响应的最长时间(秒)	等待 KATA 服务器响应的最长时间（以秒为单位）。 默认值为 10。
允许发送遥测数据	启用或禁用将有关设备上事件的数据（遥测数据）发送到 KATA 服务器。 默认启用发送遥测数据。
使用双重身份验证	启用或禁用双向身份验证以进一步保护与 KATA 服务器的连接。 要使用双重身份验证，您需要添加客户端证书。 必须在 KATA 服务器端启用双向身份验证。
添加（客户端证书）	打开“添加客户端证书”窗口，以提高与 KATA 服务器的连接的安全性。 如果尚未添加客户端证书，则会显示该按钮。 如果要为连接配置额外的保护，请在 KATA 服务器端启用客户端证书验证，并在此窗口中选中“**使用双重身份验证**”复选框。
删除（客户端证书）	删除客户端证书。 如果已添加客户端证书，则会显示该按钮。
添加（服务器证书）	打开“添加服务器证书”窗口。 如果尚未添加服务器证书，则会显示该按钮。
删除（服务器证书）	删除服务器证书。 仅当已添加服务器证书时，才会显示该按钮。

“添加服务器证书”窗口

在此窗口中，您可以通过以下方式之一添加 KATA 服务器证书：

- 在“**从文件添加**”字段中指定证书文件的路径。“**浏览**”按钮将打开标准文件选择窗口。指定包含证书的文件（DER 或 PEM 格式）的路径。
- 将证书文件的内容复制到“**输入证书详情**”字段中。

如果已添加服务器证书，则在 Kaspersky Endpoint Security 端验证服务器证书。这提高了连接的安全性。

“添加客户端证书”窗口

在此窗口中，您可以添加客户端证书以进一步保护与 KATA 服务器的连接。

如果要为连接配置额外的保护，请在 KATA 服务器端启用客户端证书验证，并在“服务器连接设置”窗口中选中“**使用双重身份验证**”复选框。

要添加客户端证书，请指定包含客户端证书和私钥的加密容器（PFX 存档）的路径。“**浏览**”按钮将打开标准文件选择窗口。如果存档受密码保护，请在“**加密容器密码**”字段中输入密码。

“数据传输设置”窗口

在此窗口中，您可以配置将数据发送到 KATA 服务器的设置。

将数据发送到 KATA 服务器的设置

设置	描述
发送事件时的最大延时（秒）	向 KATA 服务器发送事件的最大延迟（以秒为单位）。 默认值为 `30`。
启用事件限制	启用或禁用调节发送到 KATA 服务器的事件数。
每小时的最大事件数量	每小时的最大事件数量 默认值为 `3000`。
事件限制阈值（百分比）	事件限制阈值（百分比）。如果一种类型的事件（例如，有关注册表更改的事件）占事件总数的比例超过设置的阈值（以百分比表示），则发送事件将受到限制。 默认值为 `15`。

在命令行上配置 Kaspersky Endpoint Detection and Response (KATA) 集成

您可以在命令行中通过 Kaspersky Endpoint Detection and Response (KATA) 集成(*KATAEDR*) 预定义任务来管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 之间的集成。

Kaspersky Endpoint Detection and Response (KATA) 集成默认不运行。您可以手动启动和停止该任务。

您可以通过编辑预定义任务的设置来配置Kaspersky Endpoint Detection and Response (KATA) 集成设置。

通过使用用于管理 Kaspersky Endpoint Detection and Response (KATA) 集成设置的命令，您可以管理用于连接到 KATA 服务器的证书。

Kaspersky Endpoint Detection and Response (KATA) 集成任务设置

该表描述了所有可用设置以及您可以为 Kaspersky Endpoint Detection and Response (KATA) 集成任务指定的所有设置的默认值。

设置	Description	值
Address	KATA 服务器地址 可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。 为设备启用网络隔离后，为了确保与 KATA 服务器的通信在应用程序发生故障时不中断，建议指定服务器的 IP 地址。	默认值：127.0.0.1。
Port	用于连接到 KATA 服务器的端口。	默认值为 443。
UseClientPinnedCertificate	启用和禁用双向身份验证，以进一步保护与 KATA 服务器的连接。 如果在 KATA 服务器端启用了双向身份验证，您需要在 Kaspersky Endpoint Detection and Response (KATA) 集成任务的设置中启用双向身份验证，并在启动任务前添加客户端证书。	Yes – 使用双重身份验证来进一步保护与 KATA 服务器的连接。 No（默认值）– 不使用双重身份验证。
SynchronizationPeriod	发送同步请求到 KATA 服务器的间隔（以分钟为单位）。	默认值为 5。
ConnectionTimeout	等待与 KATA 服务器连接的最长时间（以秒为单位）。	默认值为 10。
RequestTimeout	等待 KATA 服务器响应的最长时间（以秒为单位）。	默认值为 10。
MaximumDataTransferTime	向 KATA 服务器发送事件的最大延迟（以秒为单位）。	默认值为 30。
UseRequestCountLimits	启用和禁用调节发送到 KATA 服务器的事件数。	Yes（默认值）– 调节发送的事件数。 No – 不调节事件数。
MaximumNumberOfEventsInHour	每小时的最大事件数量	默认值为 3000。
EventLimitExceededPercentage	事件限制阈值（百分比）。如果某种类型的事件占事件总数的比例超过配置的阈值（百分比），则发送事件会受到限制。	默认值为 15。
EnableTelemetry	启用和禁用向 KATA 服务器发送事件数据（遥测数据）。	Yes（默认值）– 向 KATA 服务器发送遥测数据。 No – 不发送遥测数据。

管理用于连接到 KATA 服务器的证书

管理证书需要 root 特权。

您可以使用命令管理用于连接到 KATA 服务器的证书。您可以使用证书做什么：

- 添加或替换服务器证书
- 显示有关服务器证书的信息
- 删除服务器证书
- 添加或替换客户端证书
- 显示有关客户端证书的信息
- 删除客户端证书

要添加或替换服务器证书，请运行以下命令：

```
kesl-control [-R] --add-kataedr-server-certificate <文件名和路径>
```

其中 <文件名和路径> 是包含服务器证书的文件的名称和路径。

要添加或更改客户端证书：

1. 执行命令：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <文件名和路径>
   ```

   其中 <文件名和路径> 是包含客户端证书和私钥的加密容器（PFX 存档）的名称和路径。

2. 如果加密容器受密码保护，请在出现提示时输入密码。

如果在 KATA 服务器设置中启用了客户端证书验证，并且在 Kaspersky Endpoint Detection and Response (KATA) 集成任务设置中 `UseClientPinnedCertificate` 设置的值为`yes`，则客户端证书用于额外保护与 KATA 服务器的连接。

要显示证书信息，请运行以下命令：

- 对于服务器证书：

  ```
  kesl-control [-R] --query-kataedr-server-certificate
  ```

- 对于客户端证书：

  ```
  kesl-control [-R] --query-kataedr-client-certificate
  ```

运行该命令会显示以下证书信息：

- 证书序列号
- 证书主题
- 证书颁发者
- 证书开始日期
- 证书到期日期
- SHA1 和 SHA256 证书指纹

要删除服务器证书信息，请运行以下命令：

```
kesl-control [-R] --remove-kataedr-server-certificate
```

要删除客户端证书信息，请运行以下命令：

```
kesl-control [-R] --remove-kataedr-client-certificate
```

如果在 Kaspersky Endpoint Detection and Response (KATA) 集成任务的设置中配置了证书的使用并且该任务正在运行，则删除此证书会以出错结束。

Kaspersky Endpoint Detection and Response Optimum 集成

Kaspersky Endpoint Detection and Response Optimum 解决方案用于保护组织的 IT 基础设施免受漏洞、勒索软件、无文件攻击以及攻击者用来破坏设备或数据的合法系统工具等威胁。

Kaspersky Endpoint Detection and Response Optimum 监控和分析威胁的演变，并向安全官或管理员提供有关潜在攻击的信息，帮助他们及时采取响应措施。

Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 解决方案的集成由 Kaspersky Endpoint Security 组件 Endpoint Detection and Response Optimum (EDR Optimum) 得到促进。

Kaspersky Endpoint Security 12.1 for Linux 与 Kaspersky Endpoint Detection and Response Optimum 版本 3.0 兼容。

早于 12.1 版的 Kaspersky Endpoint Security for Linux 版本不包含 EDR Optimum 组件。

Kaspersky Endpoint Detection and Response Optimum 使用以下威胁情报工具：

- 卡巴斯基安全网络（以下也称为 KSN）云服务基础设施，提供对卡巴斯基文件、网站和软件信誉在线知识库的访问。
- 与卡巴斯基威胁情报门户集成，门户包含并显示有关文件和网站信誉的信息。
- 卡巴斯基威胁数据库。

与 Kaspersky Endpoint Detection and Response Optimum 交互时，Kaspersky Endpoint Security 可以：

- 将有关设备事件的数据发送到 Kaspersky Security Center。Kaspersky Endpoint Security 向 Kaspersky Security Center 发送有关进程、打开的网络连接和修改文件的监控数据，以及有关应用程序检测到的威胁的数据和处理这些威胁的结果数据。
- 在接收来自 Kaspersky Security Center 的命令时执行响应操作以确保安全。

与 Kaspersky Endpoint Detection and Response Optimum 集成涉及以下步骤：

1. **启用所需的 Kaspersky Endpoint Security 组件**

   确保 Kaspersky Endpoint Security 的以下组件已启用并正在运行：

- 文件威胁防护。
- Web 威胁防护。
- 行为检测。

2. **启用威胁分析工具**

   确保卡巴斯基安全网络在标准或扩展模式下启用。

   > 为了使 Kaspersky Endpoint Detection and Response Optimum 最有效运行，我们建议使用扩展的卡巴斯基安全网络模式。

3. **激活 EDR Optimum 组件**

   确保满足以下条件之一：

   - 您正在使用包含 Kaspersky Endpoint Detection and Response Optimum 功能的授权许可来使用 Kaspersky Endpoint Security。
   - 您已购买使用 Kaspersky Endpoint Detection and Response Optimum 功能的单独授权许可，并且还将EDR Optimum 授权许可密钥添加到了应用程序中。

4. **启用 Kaspersky Endpoint Detection and Response Optimum 集成**

   默认情况下，Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 的集成被禁用。您可以启用、禁用或配置集成：

   - 使用 Web Console。
   - 使用命令行。

     > 不支持使用 Kaspersky Security Center 管理控制台管理 EDR Optimum 组件。

   您可以检查 EDR Optimum 组件的状态：

   - 使用 Web Console 中的*应用程序组件状态报告*。

     Endpoint Detection and Response Optimum组件已被添加到 Kaspersky Endpoint Security 组件列表中。有关报告的详细信息，请参阅"Kaspersky Security Center 帮助"。
   - 在 Web Console 的设备属性中。
   - 使用命令行。

5. **启用到管理服务器的数据传输**

   要使用 Kaspersky Endpoint Detection and Response Optimum 的所有功能，您必须启用以下设置：

   - **已启用/已禁用有关备份中的文件的通知。**

     您可以在**应用程序设置→常规设置→存储设置**下的策略属性中启用此设置。

     通过启用此设置，您允许将 Kaspersky Endpoint Security 已移动到设备备份的文件的相关信息发送到 Kaspersky Security Center。
   - **显示 EDR 警报。**

     您可以在 Kaspersky Security Center Web Console 主窗口的**设置→界面设置**下启用此设置。

通过启用此设置，您可以允许显示警报列表。

在 15.1 之前的 Web Console 版本中不提供**"显示 EDR 警报"**设置。

启用或禁用 Kaspersky Endpoint Detection and Response Optimum 集成

您可以启用或禁用 Kaspersky Endpoint Detection and Response Optimum 集成：

- 使用 Web Console。
- 使用命令行。

管理控制台不支持管理集成 Kaspersky Endpoint Detection and Response Optimum 的设置。

在 Web Console 中启用或禁用 Kaspersky Endpoint Detection and Response Optimum 集成

在 Web Console 中，您可以启用或禁用 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 的集成并配置集成设置：

- 在策略属性中（**应用程序设置→Detection and Response→Endpoint Detection and Response Optimum**）；
- 在设备属性中（**资产（设备）→受管理设备** → <设备名称> 链接 → **应用程序**→< Kaspersky Endpoint Security 应用程序名称> 链接 →**应用程序设置→Detection and Response→Endpoint Detection and Response Optimum**）。

如果策略正在被应用于设备，则无法在设备属性中启用或禁用 Kaspersky Endpoint Security 与Kaspersky Endpoint Detection and Response Optimum 的集成。

Kaspersky Endpoint Detection and Response Optimum 集成设置

设置	描述
Endpoint Detection and Response Optimum 已启用/已禁用	启用或禁用 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Optimum 的集成。 默认情况下，禁用 Integration Server。
网络隔离	**配置设备解除阻止**链接可打开**配置设备解除阻止**窗口，您可以在其中配置设备阻止的持续时间。
排除项	**排除项**链接可打开排除项窗口，您可以在其中配置网络隔离排除项。

在命令行上启用或禁用 Kaspersky Endpoint Detection and Response Optimum 集成

在命令行上，您可以使用常规应用程序设置中的UseEdrOptimum设置启用或禁用与Kaspersky Endpoint Detection and Response Optimum 的集成。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

要使用命令行选项启用 Kaspersky Endpoint Detection and Response Optimum 集成，请运行以下命令：

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

要使用命令行选项禁用 Kaspersky Endpoint Detection and Response Optimum 集成，请运行以下命令：

```
kesl-control --set-app-settings UseEdrOptimum=No
```

查看 Kaspersky Endpoint Detection and Response Optimum 集成状态

在 Web Console 中查看集成状态

您可以通过选择**资产（设备）**部分 →**受管理设备**→ <设备名称> 链接 →**应用程序**→ <Kaspersky Endpoint Security 应用程序名称> 链接 →**常规**→**组件**，在 Web Console 中查看 Kaspersky Endpoint Detection and Response Optimum and Response Optimum 集成的状态。

在命令行上查看集成状态

您可以通过运行`kesl-control --app-info`命令使用命令行查看与 Kaspersky Endpoint Detection and Response Optimum 的集成状态。

集成状态

EDR Optimum 组件将显示以下状态之一：

- *正在运行*。
  当同时满足以下条件时，会显示此状态：
  - 添加了 EDR Optimum 所需的授权许可密钥。
  - 当前日期早于授权许可到期日期。
  - EDR Optimum 所需的一个或多个 Kaspersky Endpoint Security 组件已启用。
  - 设备上已启用 Kaspersky Endpoint Detection and Response Optimum 集成。
- *已停止*。
  在以下情况下显示此状态：

- Kaspersky Endpoint Detection and Response Optimum 集成已被禁用。
- Kaspersky Endpoint Security 应用程序未停止。

- *不受授权许可支持*。
  在以下情况下显示此状态：
  - 当前日期晚于授权许可到期日期。
  - 当前授权许可不包括 EDR Optimum 功能。
- *故障*。
  当同时满足以下条件时，会显示此状态：
  - 当前日期早于授权许可到期日期。
  - EDR Optimum 所需的一个或多个 Kaspersky Endpoint Security 组件遇到错误。

查看有关检测到的威胁和响应操作的信息

要查看有关检测到的威胁的所有信息并执行适当的威胁响应措施，您可以使用警报详情窗口，其中包含：

- 威胁发展链图
- 使用 UI 执行所选操作来应对威胁的建议
- 有关威胁检测的常规信息（例如，检测模式）
- 关于受保护设备的信息
- 有关所检测到的对象的信息
- 设备上出现的文件历史记录
- 有关应用程序执行的威胁响应操作的信息

有关管理警报详情的更多详细信息，请参阅Kaspersky Endpoint Detection and Response Optimum帮助。

IOC 扫描结果保存 30 天。此时间过后，Kaspersky Endpoint Security 会自动删除旧条目。

搜索入侵指标

您可以使用IOC 扫描任务搜索设备上的*入侵指标*并执行威胁响应操作。

为了搜索入侵指标， Kaspersky Endpoint Security 使用用户准备的IOC 文件。IOC 文件必须符合IOC 文件要求。

您可以创建和运行*IoC 扫描*任务，以及在 Web Console 中编辑其设置：

- 在资产（设备）→任务部分
- 在资产（设备）→受管理设备→<设备名称>链接→任务部分
- 在警报详情窗口中

您无法在命令行上创建、运行或配置*IOC 扫描*任务。您无法使用*kesl-control* `--get-task-list`命令在命令行上查看在 Web Console 中创建的`IOC` 扫描任务。

在计划设置中，此任务不提供局域网唤醒功能。为了运行任务，请确保设备已打开电源。

*IOC 扫描*任务设置

设置	描述
重新定义 IOC 文件	此按钮可打开**重新定义 IOC 文件**窗格。 单击**"重新定义 IOC 文件"**面板中的**"添加 IOC 文件"**按钮将打开一个窗口，您可以在其中选择并下载设备上搜索入侵指标所需的 IOC 文件。上传 IOC 文件后，您可以查看 IOC 文件中的指标列表。
导出 IOC 集合	单击此按钮可将 IOC 文件下载到设备。
检测到 IOC 时应用响应操作	此复选框可启用或禁用在检测到入侵指标时应用响应操作。 如果选中该复选框，则当检测到入侵指标时，应用程序将执行您选择的操作： • **将设备从网络中隔离**。 如果选中此复选框，则当检测到入侵指标时，应用程序会将设备与网络隔离，以防止威胁蔓延。您可以配置隔离时长。 • **开始关键区域扫描**。 如果选中此复选框，则当检测到入侵指标时，应用程序将启动*关键区域扫描*任务。默认情况下，Kaspersky Endpoint Security 会扫描内核内存、正在运行的进程和引导扇区。 如果清除该复选框，则应用程序在检测到入侵指标时不会执行任何响应操作。有关检测到的入侵指标的信息显示在警报详情窗口和任务属性中。
扫描范围	显示文件扫描区域：系统磁盘的关键区域和来自 IOC 的路径。

我们不建议在开始此任务后添加或删除 IOC 文件。这可能会导致该任务之前运行的 IOC 扫描结果显示不正确。我们建议添加一个新任务来基于新的 IOC 文件运行 IOC 扫描。

您可以在*资产（设备）*部分→**任务**→<任务名称>→**应用程序设置**→**IOC 扫描结果**中看到**IOC 扫描**的结果。

IOC 扫描结果部分中的表格包含已运行*IOC 扫描*任务的设备列表以及任务的结果。在**设备**下拉列表中，您可以选择管理组中所有受管理设备或特定设备的任务结果。

该表包含以下列：

- **状态**。
  入侵指标检测状态，以图标形式显示。
- **主机**。
  运行*IOC 扫描*任务的设备的名称。

- **时间**。
  执行*IOC 扫描*任务的日期和时间。
- **结果**。
  有关*IOC 扫描*任务结果的信息。已完成的任务可以具有以下状态之一：
  - *检测到 IOC*。
    此状态显示为一个链接；单击链接将打开一个包含警报详情的窗口。
  - *未检测到 IOC*

您也可以在**资产（设备）** →**任务**→ <任务名称> 部分的"**结果**"选项卡的"**描述**"列中查看任务的结果。

IOC 扫描结果保存 30 天。此时间过后，Kaspersky Endpoint Security 会自动删除旧条目。

IOC 文件的要求

创建 IOC 扫描任务时，请考虑以下IOC 文件要求和限制：

- 应用程序支持具有 IOC 和 XML 扩展名的 IOC 文件。这些文件使用开放标准进行 IOC 描述 - OpenIOC 版本 1.0 和 1.1。
- IOC 文件中的语义错误和不受支持的 IOC 术语和标签不会导致任务失败。对于 IOC 文件的此类部分，应用程序会记录不存在匹配项。
- IOC 扫描任务中使用的所有 IOC 文件的 ID必须是唯一的。重复的 ID 可能会影响任务结果的正确性。
- 我们建议为每个威胁创建一个 IOC 文件。这使得*IOC 扫描*任务的结果更易于阅读。

单击下面的链接即可下载该文件，其中包含 OpenIOC 标准的 IOC 术语完整列表。

下载 IOC_TERMS.XLSX

下表列出了应用程序支持 OpenIOC 标准方式的特殊考虑和限制。

OpenIOC 标准版本 1.0 和 1.1 的功能和限制

支持的条件	OpenIOC 1.0： • `is` • `isnot`（作为集合排除项） • `contains` • `containsnot`（作为集合排除项） OpenIOC 1.1： • `is`

	• contains • starts-with • ends-with • matches • greater-than • less-than
支持的条件属性	OpenIOC 1.1： • preserve-case • negate
支持的运算符	AND OR
支持的数据类型	"date": 日期（适用条件：is，greater-than，less-than） "int"：整数（适用条件：is，greater-than，less-than） "string": string（适用条件：is、contains、matches、starts-with 、ends-with） “duration”：持续时间（以秒为单位）（适用术语：is、greater-than、less-than）
解释数据类型的特殊注意事项	"boolean string"、"restricted string"、"md5"、"IP", "sha256"、"base64Binary"数据类型被解释为字符串。 应用程序支持解释被指定为间隔的int和date数据类型的Content参数： • OpenIOC 1.0： 在Content字段中使用TO运算符： <Content type="int">49600 TO 50700</Content> <Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content> <Content type="int">[154192 TO 154192]</Content> • OpenIOC 1.1： • 使用greater-than和less-than条件 • 在Content字段中使用TO运算符 如果指标以ISO 8601、祖鲁时区、UTC格式指定，则应用程序支持date和duration数据类型的解释。

启用或禁用设备网络隔离

您可以通过以下方式为设备启用网络隔离：

- 使用*IOC 扫描*任务。

当创建和配置IOC 扫描任务时，如果在**检测 IOC 时的操作**部分中，您选中了**检测到 IOC 时应用响应操作**和**将设备从网络中隔离**复选框，则当应用程序检测到入侵指标 (IOC) 时，会自动启用网络隔离。

- 在警报详情窗口中
- 在 Web Console 的设备属性中。

仅当启用与 Kaspersky Endpoint Detection and Response Optimum 的集成，并且 EDR Optimum 组件拥有进行中状态时，才可以启用网络隔离。

您可以通过以下方式禁用设备的网络隔离：

- 在 Web Console 的设备属性中手动。
- 在命令行上手动。
- 在警报详情窗口中。
- 通过在设备属性或策略属性中配置自动禁用

无论与 Kaspersky Endpoint Detection and Response Optimum 的集成是否被启用、EDR Optimum 组件是否被启用、或者策略是否已被应用于设备，都可以在设备属性和命令行中禁用网络隔离。

您可以配置在启用网络隔离时不需要隔离的网络连接的排除项。

您可以在命令行上检查网络隔离状态。

启用网络隔离后，应用程序将切断设备上的所有活动网络连接并阻止所有新的 TCP/IP 网络连接，但以下列出的连接除外：

- 在网络隔离排除中指定的连接。
- 由 Kaspersky Endpoint Security 服务发起的连接。
- 由 Kaspersky Security Center 网络代理发起的连接。
- 如果应用程序在 Light Agent 模式下使用，则连接到 SVM 和 Integration Server。

被隔离的 EDR Optimum 设备会自动获取**ISOLATED FROM NETWORK**标签。当网络隔离被禁用时，此标签会被自动删除。

有关按标签获取隔离设备列表的常规信息，请参阅Kaspersky Endpoint Detection and Response Optimum 帮助。

在 Web Console 中手动启用或禁用设备的网络隔离

要启用或禁用设备的网络隔离：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。

将打开受管理设备列表。

2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

3. 在列表中找到您的设备并单击其名称。

4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。

5. 在设备上安装的应用程序列表中，单击 **Kaspersky Endpoint Security 12.1 for Linux** 应用程序的名称。

   应用程序属性窗口将打开。

6. 转到“**应用程序设置**”选项卡。

7. 转到**检测和响应→Endpoint Detection and Response Optimum**部分。

8. 在**网络隔离**下，执行以下操作之一：

   - 要启用设备的网络隔离，请单击**将设备与网络隔离**按钮
   - 要禁用设备的网络隔离，请单击**解除隔离设备**按钮

如果您启用了设备的网络隔离，Kaspersky Endpoint Security 会对该设备分配“**ISOLATED FROM NETWORK**”标签。如果您禁用了设备的网络隔离，Kaspersky Endpoint Security 将从设备中删除此标签。

配置自动禁用网络隔离

您可以将网络隔离配置为在指定的时间段后自动禁用：

- 在设备属性中。

  > 如果策略被应用于设备，则无法在设备属性中配置自动禁用网络隔离。

- 在策略属性中。

  > 策略属性中指定的自动禁用网络隔离设置仅适用于在*IOC 扫描*任务期间因检测到入侵指标 (IOC) 而被隔离的设备。

默认情况下，应用程序在启用网络隔离 5 小时后禁用网络隔离。禁用网络隔离后，设备可以不受限制地在网络上运行。

在设备属性中配置自动禁用网络隔离

配置自动禁用设备网络隔离：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。

   将打开受管理设备列表。

2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

3. 在列表中找到您的设备并单击其名称。

4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。

5. 在设备上安装的应用程序列表中，单击 **Kaspersky Endpoint Security 12.1 for Linux** 应用程序的名称。

   应用程序属性窗口将打开。

6. 转到“**应用程序设置**”选项卡。

7. 转到**Detection and Response→Endpoint Detection and Response Optimum**部分。

8. 在“**网络隔离**”下，单击“**配置设备解除阻止**”。

9. 这将打开**配置设备解除阻止**窗口；在该窗口中，指定设备解锁设置。

设备解锁设置

设置	描述
距离解除阻止被自动隔离的设备：	此复选框可启用或禁用在**“小时”**输入字段中指定的时间段后自动解除阻止隔离设备。 默认选中该复选框。
小时	时间（以小时为单位）的输入字段，在此时间后隔离设备将被自动解除阻止。 仅当选中**“解除对自动隔离设备的阻止”**复选框时，此字段才处于活动状态。

10. 保存更改。

在策略属性中配置自动禁用网络隔离

配置自动禁用设备网络隔离：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**策略和策略配置文件**”。

   将打开策略列表。

2. 选择包含应用了策略的设备的管理组。为此，请单击窗口上部的“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   该列表仅显示为所选管理组配置的策略。

3. 单击列表中所需策略的名称。

   将打开策略属性窗口。

4. 转到“应用程序设置”选项卡。

5. 转到**Detection and Response→Endpoint Detection and Response Optimum**部分。

6. 在“网络隔离”下，单击“配置设备解除阻止”。

7. 这将打开**配置设备解除阻止**窗口；在该窗口中，指定设备解锁设置。

设备解锁设置

设置	描述
距离解除阻止被自动隔离的设备：	此复选框可启用或禁用在**“小时”**输入字段中指定的时间段后自动解除阻止隔离设备。 默认选中该复选框。
小时	时间（以小时为单位）的输入字段，在此时间后隔离设备将被自动解除阻止。 仅当选中**“解除对自动隔离设备的阻止”**复选框时，此字段才处于活动状态。

8. 保存更改。

在命令行中禁用设备的网络隔离

要使用命令行禁用设备的网络隔离，请运行以下命令：

```
kesl-control [-R] --isolation-off
```

您可以通过使用以下命令来检查网络隔离状态并查看网络隔离排除列表：

```
kesl-control [-R] --isolation-stat
```

命令行上显示以下网络隔离状态之一：

- *网络隔离已启用。*
- *网络隔离已禁用。*

配置网络隔离排除

您可以配置排除：

- 在策略属性中

- 在设备属性中

启用网络隔离后，配置的规则所涵盖的网络连接在设备上保持畅通。

默认情况下，如果配置文件由确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备不间断运行的规则组成，则网络配置文件被排除在网络隔离之外。

> 仅当应用程序因为对入侵指标 (IOC) 的检测做出反应自动启用网络隔离时，策略属性中定义的排除项才会被应用。

> 仅当网络隔离在设备属性或警报详情窗口中被手动启用时，设备属性中定义的排除项才会被应用。

活动策略不会阻止应用设备属性中定义的网络隔离排除项。

您可以查看网络隔离排除列表：

- 在策略属性中（**应用程序设置→Detection and Response→Endpoint Detection and Response Optimum→排除**链接）
- 在设备属性中（**资产（设备）→受管理设备** → <设备名称> 链接 → < Kaspersky Endpoint Security 应用程序的名称> 链接 →**应用程序设置→Detection and Response→Endpoint Detection and Response Optimum→排除项**链接）
- 在命令行中

在 Web Console 的策略属性中添加或删除网络隔离排除

在 Web Console中，您可以在策略属性中添加或删除网络隔离排除：**应用程序设置→Detection and Response→Endpoint Detection and Response Optimum→排除**链接。

在**排除**窗口中，您可以单击表格上方的按钮执行以下操作：

- 通过下列方式之一添加有关被排除的网络连接的信息：
  - 单击**添加**并输入有关网络连接的信息
  - 单击**从配置文件添加**，然后从字典中选择一个网络配置文件
- 删除网络连接信息

在设备属性中添加或删除网络隔离排除

> 如果策略已被应用于设备，则无法在设备属性中添加或删除网络隔离排除。

要在设备属性中添加或删除网络隔离排除：

1. 在 Web Console 的主窗口中，选择“资产（设备）”→“受管理设备”。
   将打开受管理设备列表。
2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“当前路径”字段中的链接，然后在打开的窗口中选择管理组。
   列表仅显示所选管理组的受管理设备。
3. 在列表中找到您的设备并单击其名称。
4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“应用程序”选项卡。
5. 在设备上安装的应用程序列表中，单击 **Kaspersky Endpoint Security 12.1 for Linux** 应用程序的名称。
   应用程序属性窗口将打开。
6. 转到“应用程序设置”选项卡。
7. 转到**Detection and Response→Endpoint Detection and Response Optimum**部分。
8. 在**网络隔离**下，单击**排除**以打开**排除**窗口。
9. 在打开的窗口中，使用表格上方的按钮执行必要的操作。
   - 如果想添加有关被排除的网络连接的信息，请通过以下方式之一进行：
     - 单击**添加**按钮并输入有关网络连接的信息。
     - 单击**从配置文件添加**按钮并从字典中选择一个网络配置文件。
   - 如果您想要删除某个被排除的网络连接的信息，请选中要删除的网络连接旁边的复选框，然后单击**删除**。
10. 保存更改。

添加网络隔离排除窗口

在此窗口中，您可以输入有关在启用网络隔离时不想被阻止的网络连接的信息。

网络连接设置

设置	Description
Name	网络连接的名称。
Direction	网络连接方向
协议	网络连接使用的协议。
Number	网络连接的号码。
本地端口/范围	本地端口号或范围。
远程端口/范围	远程端口号或范围。
远程地址	远程设备的 IP 地址

网络配置文件字典窗口

在此窗口中，您可以选择要排除的网络连接的配置文件。

网络连接配置文件

网络连接配置文件	描述
DNS 服务器	通过响应获取 IP 地址的请求和更新 DNS 记录的请求来提供 DNS 名称解析的服务。
DNS 客户端	通过执行 DNS 名称查询来提供 DNS 名称解析的服务。
Active Directory 证书服务	用于创建、验证和撤销供组织内部使用的公钥证书的服务。
Active Directory 联盟服务	用于通过集中存储的统一凭证集授予用户对多个 Web 服务或网络资源的访问权限的服务。
Active Directory 轻型目录服务	提供与 Active Directory 域服务相同功能但不需要创建域或域控制器的服务。
Active Directory Rights Management Services	用于控制用户访问文档的服务。
DHCP	该服务使用动态主机配置协议 (DHCP) 自动分配 IP 地址。
文件传输协议 (FTP)	用于通过网络在客户端和服务器之间传输文件的标准网络协议。
Kerberos 密钥分发中心	用于向 Active Directory 域中的用户和设备提供票证 (TGS) 和临时会话密钥的网络服务。
Secure Shell (SSH)	允许远程控制操作系统和 TCP 连接隧道的协议。
Linux 系统组件	Linux 系统组件。

启动进程

您可以使用*启动进程*任务远程启动设备上的进程和可执行文件。

例如，您可以运行：

- 由于设备上的恶意活动而被停止的进程。
- 被您停止的进程。
  例如，你可以使用终止进程 *任务*远程启动您已停止的任务。
- 脚本。
  例如，您可以运行脚本从设备收集数据来调查威胁。
- 实用程序。
  例如，您可以运行实用程序将设备配置信息保存到文件中。
- 应用程序。

如果 SELinux 以强制模式安装在您的操作系统中，则启动*启动进程*任务需要对 SELinux 进行额外配置。

您可以创建和运行*启动进程*任务，以及在 Web Console 中编辑其设置：

您无法使用命令行创建、运行或配置*启动进程*任务。您无法使用*kesl-control --get-task-list*命令在命令行上查看在 Web Console 中创建的启动进程任务。

启动进程任务设置

设置	描述
可执行命令	用于输入启动进程的命令的字段。 例如，如果您要运行`klnagchk`工具来检查与管理服务器的连接，则需要输入`/ /<工作目录的绝对路径>/klnagchk`命令，然后填写下表中所述的其他字段。 您也可以在**工作目录路径（可选）**字段中输入工作目录的绝对路径。在这种情况下，请不要在**可执行命令**字段中输入工作目录的绝对路径。
命令行参数(可选)	用于输入命令行参数的字段，以便在启动时将附加输入传递给脚本、实用程序或应用程序。 例如，您可以输入`-logfile klnagchk.log`参数。此参数告诉工具将结果保存到名为`klnagchk.log`的文件中。 如果需要传递多个参数，请用空格分隔它们。 例如，您可以输入`-logfile klnagchk.log -savecert certificate.cer`参数。这些参数告诉工具将结果保存到名为`klnagchk.log`的文件中，并将用于检查对管理服务器进行访问的证书保存在`certificate.cer`文件中。
工作目录路径(可选)	用于输入脚本、实用程序或应用程序的可执行文件所在工作目录路径的字段。 例如，您可以输入`/opt/kaspersky/klnagent64/bin/`。 如果您在**可执行命令**字段中输入了工作目录的绝对路径，请不要填写**工作目录路径（可选）**字段。

您可以在**资产（设备）** →**任务**→ <任务名称> 部分的“**结果**”选项卡的“**描述**”列中查看任务的结果。

终止进程

您可以使用*终止进程*任务远程终止设备上的进程。

例如，您可以终止：

- 由于恶意活动而在设备上启动的进程。
- 由您启动的进程。
  例如，您可以远程终止您使用*启动进程*任务启动的进程。
- 脚本。
  例如，您可以远程终止您使用*启动进程*任务启动的脚本。

- 实用程序。

  例如，您可以远程终止您使用“*启动进程*”任务启动的互联网速度测试实用程序。

- 应用程序。

> 您不能终止系统关键对象 (SCO) 的进程。SCO 包含操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。

您可以在 Web Console 中创建和运行*终止进程*任务，以及编辑其设置：您不能在命令行上创建、运行或配置*终止进程*任务。您无法使用*kesl-control --get-task-list*命令在命令行上查看在 Web Console 中创建的终止进程任务。

终止进程任务设置

设置	描述
指定想要终止其进程的文件	在下拉列表中，您可以选择如何指定文件路径： • 按目录路径和校验和 • 按完整路径 • 按 PID 仅对于在设备属性中创建的任务，下拉列表中才会出现“按 PID”值。
文件的完整路径	用于输入文件完整路径的字段。 仅当您在“指定想要终止其进程的文件”下拉列表中选择了“按完整路径”时，此字段才会显示。
校验和类型	在此下拉列表中，您可以选择文件校验和类型： • MD5。 • SHA256。 仅当您在指定要终止其进程的文件下拉列表中选择按目录路径和校验和时，才会出现此下拉列表。
文件校验和	用于输入文件校验和的字段。 仅当您在 指定想要终止其进程的文件下拉列表中选择了按目录路径和校验和， 并且在校验和类型下拉列表中选择了MD5时，此字段才会显示。
目录路径	用于输入文件目录路径的字段。

	仅当您在“**指定想要终止其进程的文件**”下拉列表中选择了“**按目录路径和校验和**”时，此字段才会显示。
进程 ID	进程 ID (PID) 输入字段。 仅当您在“**指定想要终止其进程的文件**”下拉列表中选择了“**按 PID**”时，此字段才会显示。

您可以在**资产（设备）** →**任务**→ <任务名称> 部分的“**结果**”选项卡的“**描述**”列中查看任务的结果。

从设备接收文件

您可以使用*从设备接收文件*任务从用户的设备接收文件。

例如，您可以接收由第三方应用程序生成的事件日志文件。

您可以创建和运行*从设备接收文件*任务，以及在 Web Console 中编辑其设置：

您无法在命令行上创建、运行或配置*从设备接收文件*任务。您无法使用*kesl-control --get-task-list*命令在命令行上查看在 Web Console 中创建的从设备接收文件任务。

应用程序设置选项卡上的**接收文件**表包含以下列：

- **目录路径**。
  设备上文件目录的路径。
- **校验和验证类型**。
  设备上文件的校验和验证类型。

您可以点击表格上方的按钮来添加、编辑或删除设备上文件的数据。针对*接收文件*表中选择的文件执行**从设备接收文件**任务。

单击**添加**按钮将打开**接收文件**窗口，您可以在其中配置*从设备接收文件*任务的设置。

从设备接收文件任务设置

设置	描述
指定要接收的文件	在下拉列表中，您可以选择如何指定文件路径： • **按目录路径和校验和** • **按完整路径**
文件的完整路径	用于输入文件完整路径的字段。 仅当您在“**指定要接收的文件**”下拉列表中选择了“**按完整路径**”时，此字段才会显示。

校验和类型	在此下拉列表中，您可以选择文件校验和类型： • **MD5**。 • **SHA256**。 仅当您在**指定要接收的文件**下拉列表中选择**按目录路径和校验和**时，才会出现此下拉列表。
文件校验和	用于输入文件校验和的字段。 仅当您在“**指定要接收的文件**”下拉列表中选择了**按目录路径和校验和**时，此字段才会显示。
文件目录路径	用于输入文件目录路径的字段。 仅当您在**“指定要接收的文件”**下拉列表中选择了**按目录路径和 校验和**时，此字段才会显示。

作为*从设备接收文件*任务的结果，文件的副本将保存在设备的备份中。您可以使用 Web Console 将此副本从备份下载到您启动下载的设备。

文件大小不得超过 100 MB。

用户设备上的原始文件仍保留在其原始目录中。

无论文件扫描结果如何，通过“*从设备接收文件*”任务接收的所有文件在 Kaspersky Security Center 备份中都将具有“*已感染*”状态。

您可以在**资产（设备）** →**任务**→ <任务名称> 部分的“**结果**”选项卡的“**描述**”列中查看任务的结果。

从设备中删除文件

您可以使用*从设备删除文件*任务从设备删除文件。例如，作为威胁响应的一部分，这可能必不可少。

系统关键对象 (SCO) 无法被删除。SCO 包含操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。

您可以创建和运行*从设备删除文件*任务，以及在 Web Console 中编辑其设置：

您无法在命令行上创建、运行或配置*从设备删除文件*任务。您无法使用*kesl-control --get-task-list*命令在命令行上查看在 Web Console 中创建的从设备中删除文件任务。

从设备任务设置中删除文件

设置	描述
指定要删除的文件	在下拉列表中，您可以选择如何指定被删除的文件的路径： • 按路径和校验和 • 按完整路径
文件的完整路径	用于输入要删除的文件的完整路径的字段。 仅当您在**"指定要删除的文件"**下拉列表中选择了**"按完整路径"**时，此字段才会显示。
校验和类型	在下拉列表中，您可以选择要删除的文件的校验和类型： • **MD5**。 • **SHA256**。 仅当您在**指定要删除的文件**下拉列表中选择**按目录路径和**校验和时，才会出现此下拉列表。
文件校验和	用于输入要删除的文件的校验和的字段。 仅当您在"**指定要删除的文件**"下拉列表中选择了"**按路径和校验和**"时，此字段才会显示。
目录路径	用于输入要删除的文件目录路径的字段。 仅当您在"**指定要删除的文件**"下拉列表中选择了"**按路径和校验和**"时，此字段才会显示。
包括子目录	此复选框可启用或禁用子目录。

如果文件被另一个进程阻止，则任务将显示"*已完成*"状态，但文件本身只有在设备重新启动后才会被删除。重新启动设备后，确保该文件已被删除。

如果您尝试删除正在运行的可执行文件，则*从设备中删除文件*任务可能会以"*访问被拒绝*"错误结束。为该文件创建并运行*终止进程*任务，然后重试。

您可以在**资产（设备）** →**任务**→ <任务名称> 部分的"**结果**"选项卡的"**描述**"列中查看任务的结果。

集成 Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response 服务会持续搜索、检测和消除针对贵组织的威胁。与 Kaspersky Managed Detection and Response 解决方案的集成由 Kaspersky Endpoint Security 组件 Managed Detection and Response (MDR) 得到促进。

与 Kaspersky Managed Detection and Response 交互时，Kaspersky Endpoint Security 可以执行以下功能：

- 将遥测数据发送到 Kaspersky Managed Detection and Response 以进行威胁检测。
- 执行 Kaspersky Managed Detection and Response 命令以提供安全功能。

要配置 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 之间的集成，请执行以下操作：

- 确保“文件威胁防护”和“行为检测”已启用。如果禁用这些组件，设备在 Kaspersky Managed Detection and Response 中将显示红色状态。

  我们还建议启动 Web 威胁防护和网络威胁防护组件。如果禁用这些组件，设备在 Kaspersky Managed Detection and Response 中将呈现黄色状态。

  请参阅“Kaspersky Managed Detection and Response 帮助”部分，了解有关设备状态的更多信息。

- 启用在扩展模式下使用卡巴斯基安全网络。

  您可以在命令行、 Web Console 或管理控制台中启用卡巴斯基安全网络。

- 配置卡巴斯基私人安全网络。发送遥测数据需要使用 KPSN。

  您只能在 Web Console 或管理控制台中配置卡巴斯基私人安全网络。

  > 无法使用 Kaspersky Endpoint Security 命令配置 KPSN。

- 启用 Kaspersky Managed Detection and Response 组件，然后上传 BLOB 配置文件，该文件位于 MDR 配置文件的 ZIP 压缩文件中。

  您可以在命令行、Web Console 或管理控制台中启用托管检测与响应组件并上传 BLOB 配置文件。

配置 KPSN 以启用 Kaspersky Managed Detection and Response 集成

您只能在 Web Console 或管理控制台中配置卡巴斯基私人安全网络，以便与 Kaspersky Managed Detection and Response 集成。

要配置 KPSN，请将卡巴斯基安全网络 .pkcs7 配置文件从 MDR 配置文件的 ZIP 压缩文件上传到 Kaspersky Security Center 管理服务器。

> 一旦下载卡巴斯基安全网络配置文件，即表示您同意安装 Kaspersky Endpoint Security 的设备的数据将自动发送给卡巴斯基进行处理。如果您不同意我们处理将会传输的数据，请不要加载配置文件。有关传输数据的详细说明，请参阅 Kaspersky Managed Detection and Response 文档。

要在 Web Console 中配置 KPSN 以与 Kaspersky Managed Detection and Response 集成：

1. 在 Web Console 的主窗口中，打开管理服务器属性窗口。
2. 在左侧的列表中，选择“**KSN 代理服务器设置**”部分。
3. 开启“**启用管理服务器上的 KSN 代理服务器作为代理服务器**”切换开关以启用 KSN 代理服务器服务。
4. 打开“**使用卡巴斯基私有安全网络**”切换开关。

5. 随即会打开一个窗口，其中显示有关在安装了先前版本网络代理的分发点上使用 KSN 代理服务器的特定方面的警告，单击“**确定**”。

6. 单击“**含有 KSN 代理服务器设置的文件**”按钮。

7. 选择卡巴斯基安全网络 .pkcs7 配置文件并单击“**打开**”。

8. 单击“**保存**”。

要在管理控制台中配置 KPSN 以与 Kaspersky Managed Detection and Response 集成：

1. 在管理控制台树中，打开“管理服务器属性”窗口。

2. 选择 **KSN 代理服务器 → KSN 代理服务器设置**。

3. 选中**使用管理服务器作为代理服务器**复选框，以启用 KSN 代理服务器服务。

4. 选中“**配置私有 KSN**”复选框。

5. 随即会打开一个窗口，其中显示有关在安装了先前版本网络代理的分发点上使用 KSN 代理服务器的特定方面的警告，单击“**确定**”。

6. 单击“**含有 KSN 代理服务器设置的文件**”按钮。

7. 选择卡巴斯基安全网络 .pkcs7 配置文件并单击“**打开**”。

8. 单击“**应用**”。

在 Web Console 中配置 Kaspersky Managed Detection and Response 集成

在 Web Console 中，您可以启用或禁用 Kaspersky Endpoint Security 与Kaspersky Managed Detection and Response 的集成，并在策略属性(**应用程序设置→Detection and Response→Managed Detection and Response**) 中加载 BLOB 配置文件。

MDR 集成设置

设置	描述
托管检测与响应已启用/已禁用	切换开关可启用或禁用托管检测与响应组件，这是将 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 解决方案集成所必需的组件。 默认情况下，切换按钮处于关闭状态。
下载	单击此按钮将打开一个标准窗口，您可以在其中选择 BLOB 配置文件。

BLOB 配置文件位于 Kaspersky Managed Detection and Response 分发包中的 ZIP 压缩文件中。

下载 BLOB 配置文件，即表示您同意安装 Kaspersky Endpoint Security 的设备的数据将自动发送到卡巴斯基以作处理。如果您不同意我们处理将会传输的数据，请不要加载配置文件。有关所传输数据的详细说明，请参阅“Kaspersky Managed Detection and Response 帮助”部分。

在管理控制台中配置 Kaspersky Managed Detection and Response 集成

在管理控制台中，您可以启用或禁用 Kaspersky Endpoint Security 与Kaspersky Managed Detection and Response 的集成，并在策略属性(**Detection and Response→Managed Detection and Response**) 中加载 BLOB 配置文件。

MDR 集成设置

设置	Description
启用 Managed Detection and Response	复选框用于启用托管检测与响应组件，这是将 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 解决方案集成所必需的组件。 默认情况下，清除此复选框。
下载	单击此按钮将打开一个标准的 Microsoft Windows 窗口，您可以在其中选择 BLOB 配置文件。

BLOB 配置文件位于 Kaspersky Managed Detection and Response 分发包中的 ZIP 压缩文件中。

下载 BLOB 配置文件，即表示您同意安装 Kaspersky Endpoint Security 的设备的数据将自动发送到卡巴斯基以作处理。如果您不同意我们处理将会传输的数据，请不要加载配置文件。有关所传输数据的详细说明，请参阅“Kaspersky Managed Detection and Response 帮助”部分。

在命令行上配置 Kaspersky Managed Detection and Response 集成

在命令行中，您可以执行以下操作：

- 启用或禁用托管检测与响应组件。
- 上传或删除集成所需的 BLOB 配置文件。
- 编辑 Kaspersky Endpoint Security 成功与 Managed Detection and Response 集成后自动创建的“*Mdr_Autostart_Scan*”服务任务的启动时间。

建议在管理控制台或 Web Console 中配置 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 之间的集成。

您可以使用常规应用程序设置中的 `UseMDR` 参数启用或禁用托管检测与响应组件。您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

`UseMDR` 接受以下值：

- `Yes` – 启用托管检测与响应组件。
- `No`，禁用托管检测与响应组件。

您可以通过授权许可密钥管理命令上传或删除 BLOB 配置文件。

要加载 BLOB 配置文件，请执行以下命令：

```
kesl-control --load-mdr-blob <MDR BLOB 配置文件路径>
```

要删除 BLOB 配置文件，请执行以下命令：

```
kesl-control --remove-mdr-blob
```

启用集成会创建每天运行一次的“*Mdr_Autostart_Scan*”服务任务。如果需要，您可以设置开始时间。无法编辑其他任务设置或计划选项。

配置在 Light Agent 模式下使用应用程序的设置

仅当在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境时，本节中描述的设置才适用。

在 Light Agent 模式下运行 Kaspersky Endpoint Security 需要 Light Agent 与 SVM 上安装的 Protection Server 持续进行交互。如果没有连接到 Protection Server，Light Agent 无法将文件碎片传输到 Protection Server 进行扫描，因此不会执行扫描。

为了与 Protection Server 进行交互，Light Agent 会与安装了该 Protection Server 的 SVM 建立并保持连接。

您可以在 Web Console 或管理控制台中配置将 Light Agent 连接到 SVM 的设置。您无法在命令行中配置设置；您只能查看有关在 Light Agent 模式下的应用程序使用情况的信息。

您可以配置以下用于将 Light Agent 连接到 SVM 的设置：

- SVM 检测方法。您可以选择 Light Agent 将用来发现可连接的 SVM 的方法。Light Agent 可以通过以下方式之一发现网络上运行的 SVM：
  - 使用 Integration Server。SVM 将自身信息传输到 Integration Server。Integration Server 生成可连接的 SVM 列表并将其提供给 Light Agent。

    要使用此方法检测 SVM，您需要将 SVM 和 Light Agent 连接到 Integration Server。
  - 使用 SVM 地址列表。您可以指定 Light Agent 可以连接的 SVM 地址列表。
- 用于选择要连接的 SVM 的算法。Light Agent 在收到可用 SVM 的信息后，根据 SVM 选择算法选择最佳的 SVM 进行连接。您可以指定 Light Agent 在选择要连接的 SVM 时应使用的算法。
- 连接标签。您可以使用连接标签来控制 Light Agent 与 SVM 的连接。如果使用连接标签，Light Agent 只能连接到配置为使用该连接标签的 SVM。
- Light Agent 与 Protection Server 之间连接的安全。您可以使用加密来保护 Light Agent 与 Protection Server 之间的连接。

有关将 Light Agent 连接到 SVM 的设置的更多信息，请参阅 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的帮助。

在 Web Console 中配置 Light Agent 设置

在 Web Console 中，您可以在策略属性中配置将 Light Agent 连接到 SVM 的设置（**应用程序设置** → **Light Agent 模式**）。

SVM 检测设置

仅当在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境时，本节中描述的设置才适用。

在此窗口中，可以选择 Light Agent 用来发现可连接的 SVM 的方法。

SVM 检测设置

设置	描述
使用 Integration Server	如果选择此选项，Light Agent 将连接到 Integration Server 来获取可连接的 SVM 列表及其详细信息。 如果您希望使用 Integration Server，则需要配置 Light Agent 与 Integration Server 的连接。
使用 SVM 地址的自定义列表	如果选择此选项，您可以指定由此策略管理的 Light Agent 可以连接的 SVM 列表。Light Agent 只会连接到该列表上指定的 SVM。
SVM 地址列表	由策略覆盖的 Light Agent 可以连接的 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN) 的列表。 单击“**添加**”将打开一个窗口，您在其中可以指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。您可以在新行输入 SVM 的多个 IP 地址或 FQDN。 只能指定映射到单个 IP 地址的完全限定域名 (FQDN)。使用与多个 IP 地址对应的完全限定域名可能会导致应用程序出错。 您可以单击“**删除**”按钮来删除在列表中选定的地址。 如果选择“**使用 SVM 地址的自定义列表**”选项，则会显示 SVM 地址列表。

如果选择“**使用自定义的 SVM 地址列表**”选项，Light Agent 使用高级 SVM 选择算法，并且在 SVM 上启用大型基础架构保护模式（有关详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助）），那么只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到该 SVM。在“**SVM 选择算法**”部分中，需要将“**SVM 路径**”设置为“**忽略 SVM 路径**”。如果设置任何其他值，Light Agent 都无法连接到 SVM。

Integration Server 连接设置

仅当在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境时，本节中描述的设置才适用。

如果您希望 Light Agent 通过 Integration Server 接收有关 SVM 的信息，或者要保护 Protection Server 与 Light Agent 之间的连接，则需要连接到 Integration Server。

此窗口显示用于将 Light Agent 连接到 Integration Server 的当前设置：用于连接的地址和端口。单击“**编辑**”按钮将打开“**连接到 Integration Server**”窗口，在其中可以配置与 Integration Server 的连接。

“与 Integration Server 的连接”窗口

在此窗口中，可以指定或更改将 Light Agent 连接到 Integration Server 的设置。

Integration Server 连接设置

设置	描述
Address	安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。

	如果指定 NetBIOS 名称、“localhost”或 127.0.0.1 为地址，则连接 Integration Server 将失败并出现错误。
Port	用于连接到 Integration Server 的端口。 默认情况下使用 7271 端口。
检查	单击该按钮后，Web 插件会检查从 Integration Server 收到的 SSL 证书。 在输入用于连接到 Integration Server 的地址和端口后，该按钮可用。 如果证书包含错误或不受信任，“**与 Integration Server 的连接**”窗口中会显示相应的消息。
查看收到的证书	单击该行可查看有关从 Integration Server 收到的证书的信息。
忽略	选择此选项可保存收到的证书并继续连接到 Integration Server。 如果您遇到 SSL 证书问题，我们建议您确保所使用的数据传输通道是安全的。
取消	选择此选项可终止与 Integration Server 的连接。
密码	Integration Server 管理员账户的密码（admin 账户密码）。 建议确保密码复杂性和反暴力破解机制，使密码无法在 6 个月内被猜出。
检查	单击该按钮会将 Web 插件连接到 Integration Server。 使用管理员权限连接到 Integration Server 后，策略会自动接收代理账户的密码，该账户用于将 Light Agent 连接到 Integration Server。密码以加密形式存储。

SVM 连接标签

在此窗口中，可以启用 Light Agent 使用标签并分配 Light Agent 将用于连接的标签。

确保在 Protection Server 设置中也配置了使用连接标签：有关更多信息，请参阅“Kaspersky Security for Virtualization Light Agent 帮助”。分配了标签的 Light Agent 只能连接到允许与具有该标签的 Light Agent 连接的 SVM。

使用连接标签的设置

设置	描述
使用标签连接 Light Agent	该复选框用于启用或禁用 Light Agent 使用 SVM 连接标签。
标签	分配给 Light Agent 的标签。 您可以输入最多 255 个字符的文本字符串作为标签。可以使用除 ; 字符外的任何字符。 如果选中了“**使用标签连接 Light Agent**”复选框，则该字段可用。

SVM 选择算法

在此窗口中，可以指定 Light Agent for Linux 应使用的 SVM 选择算法，并配置使用高级 SVM 选择算法的设置。

SVM 选择算法

设置	描述
使用标准 SVM 选择算法	如果选择此选项，在虚拟机上安装并运行后，Light Agent 会选择 Light Agent 本地的 SVM 进行连接。有关更多详细信息，请参阅“Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助”。 如果没有可连接的本地 SVM，Light Agent 会选择连接的 Light Agent 数量最少的 SVM，无论该 SVM 在虚拟基础架构中的位置如何。 默认选中该选项。
使用扩展 SVM 选择算法	如果选择此选项，您可以使用“**SVM 路径**”滑块来指定在确定 SVM 相对于 Light Agent 是否为本地时如何考虑 SVM 在虚拟基础架构中的位置。Light Agent 只能连接到本地 SVM。 您还可以指定在选择要连接到的 SVM 时不应考虑虚拟基础架构中的 SVM 路径。 选择 SVM 时，Light Agent 会考虑连接到 SVM 的 Light Agent 数量，以确保 Light Agent 在可连接的 SVM 之间均匀分布。

SVM 路径	可让您指定虚拟基础架构中的 SVM 路径类型，在选择要连接的 SVM 时会考虑该类型：
	• **Hypervisor**。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
	  ◦ SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux 或 Numa vServer 上的虚拟基础架构中）。
	  ◦ SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中（在 OpenStack 平台、VK Cloud 或 TIONIX Cloud 平台管理的虚拟基础架构中）。
	如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 或同一服务器组中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。
	• **集群**。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
	  ◦ SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux 或 Numa vServer 上的虚拟基础架构中）。
	  ◦ SVM 与安装了 Light Agent 的虚拟机部署于同一OpenStack 项目中（在 OpenStack 平台、VK Cloud 或 TIONIX Cloud 平台管理的虚拟基础架构中）。
	如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 集群或同一 OpenStack 项目中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。
	• **数据中心**。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
	  ◦ SVM 与安装了 Light Agent 的虚拟机部署在同一 数据中心中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux 或 Numa vServer 上的虚拟基础架构中）。

- SVM 与安装了 Light Agent 的虚拟机位于同一可用性区域中（在 OpenStack 平台、VK Cloud 或 TIONIX Cloud 平台管理的虚拟基础架构中）。

如果安装了 Light Agent 的虚拟机所在的同一数据中心或可用区中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- **忽略 SVM 路径**。选择 SVM 时，Light Agent 不会考虑其位置。

默认情况下选择“**Hypervisor**”选项。

如果选择“**使用扩展 SVM 选择算法**”选项，则该选项可用。

如果 Light Agent 使用高级 SVM 选择算法，并且选择 SVM 地址列表作为 SVM 检测方法，而且在 SVM 上启用大型基础架构保护模式（有关更多信息，请参阅“Kaspersky Security for Virtualization Light Agent 帮助”），那么只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到该 SVM。您需要将“**SVM 路径**”设置设为“**忽略 SVM 路径**”。如果设置任何其他值，Light Agent 都无法连接到 SVM。

保护连接

在此窗口中，可以启用 Light Agent 和 Protection Server 之间的数据传输通道的加密

确保在 SVM 上的 Protection Server 设置中启用 Light Agent 和 Protection Server 之间的数据传输通道的加密。有关更多详细信息，请参阅“Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助”。

连接保护设置

设置	描述
加密 Light Agent 与 Protection Server 之间的数据通道	使用加密来保护 Light Agent 与 Protection Server 之间的连接。 如果选中该复选框，则会在由策略管理的 Light Agent 与 Light Agent 连接到的 SVM 上的 Protection Server 之间建立安全连接。启用了连接保护的 Light Agent 只能连接到启用了连接保护的 SVM，或者允许与 Protection Server 建立不受保护连接的 SVM。 如果清除该复选框，则会在 Light Agent 与 Light Agent 连接到的 SVM 上的 Protection Server 之间建立不受保护的连接。 默认情况下，清除此复选框。

在管理控制台中配置 Light Agent 设置

在管理控制台中，您可以在策略属性中配置将 Light Agent 连接到 SVM 的设置（**Light Agent 模式**）。

与 Integration Server 的连接

仅当在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境时，本节中描述的设置才适用。

如果您希望 Light Agent 通过 Integration Server 接收有关 SVM 的信息，或者要保护 Protection Server 与 Light Agent 之间的连接，则需要连接到 Integration Server。

此窗口显示用于将 Light Agent 连接到 Integration Server 的当前设置：用于连接的地址和端口。单击“**编辑**”按钮将打开“连接到 Integration Server”窗口，在其中可以配置与 Integration Server 的连接。

“与 Integration Server 的连接”窗口

在此窗口中，可以指定或更改将 Light Agent 连接到 Integration Server 的设置。

Integration Server 连接设置

设置	描述
Address	安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。 如果安装了 Kaspersky Security Center 管理控制台的设备属于某个域，则该字段默认指示该设备的域名。 如果安装了 Kaspersky Security Center 管理控制台的设备不属于某个域，或者 Integration Server 安装在其他设备上，则必须手动填写该字段。 如果指定 NetBIOS 名称、“localhost”或 127.0.0.1 为地址，则连接 Integration Server 将失败并出现错误。
Port	用于连接到 Integration Server 的端口。 默认情况下使用 7271 端口。

验证 Integration Server 证书窗口

如果从 Integration Server 收到的 SSL 证书包含错误或不受信任，则会出现此窗口。

您可以单击窗口中的链接查看收到的证书的详细信息。

如果您遇到 SSL 证书问题，我们建议您确保所使用的数据传输通道是安全的。

要继续连接到 Integration Server，请单击“**忽略**”按钮。收到的证书将作为受信任证书安装到安装了 Kaspersky Security Center 管理控制台的设备上。

“Integration Server 上的身份验证”窗口

如果托管 Kaspersky Security Center 管理控制台的设备不属于某个域，或者您的账户不属于 KLAdmins 本地组或域组或本地管理员组，则会出现此窗口。

指定 Integration Server 管理员的密码（`admin` 账户的密码），然后单击“**确定**”按钮。

建议确保密码复杂性和反暴力破解机制，使密码无法在 6 个月内被猜出。

使用管理员权限连接到 Integration Server 后，策略会自动接收 `agent` 账户的密码，该账户用于将 Light Agent 连接到 Integration Server。

SVM 检测设置

仅当在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境时，本节中描述的设置才适用。

在此窗口中，可以选择 Light Agent 用来发现可连接的 SVM 的方法。

SVM 检测设置

设置	描述
使用 Integration Server	如果选择此选项，Light Agent 将连接到 Integration Server 来获取可连接的 SVM 列表及其详细信息。 如果要使用 Integration Server，则需要配置将 Light Agent 连接到 Integration Server 的设置。
使用 SVM 地址的自定义列表	如果选择此选项，您可以指定由此策略管理的 Light Agent 可以连接的 SVM 列表。Light Agent 只会连接到该列表上指定的 SVM。
SVM 列表	由策略管理的 Light Agent 可以连接的 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN) 的列表。 单击“**添加**”将打开一个窗口，您在其中可以指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。您可以在新行输入 SVM 的多个 IP 地址或 FQDN。 只能指定映射到单个 IP 地址的完全限定域名 (FQDN)。使用与多个 IP 地址对应的完全限定域名可能会导致应用程序出错。 您可以单击“**删除**”按钮来删除在列表中选定的地址。 如果选择“**使用 SVM 地址的自定义列表**”选项，则会显示 SVM 地址列表。

如果选择“**使用自定义的 SVM 地址列表**”选项，Light Agent 使用高级 SVM 选择算法，并且在 SVM 上启用大型基础架构保护模式（有关详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助），那么只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到该 SVM。在“**SVM 选择算法**”部分中，需要将“**SVM 路径**”设置为“**忽略 SVM 路径**”。如果设置任何其他值，Light Agent 都无法连接到 SVM。

SVM 连接标签

在此窗口中，可以启用 Light Agent 使用标签并分配 Light Agent 将用于连接的标签。

确保在 Protection Server 设置中也配置了使用连接标签：有关更多信息，请参阅“Kaspersky Security for Virtualization Light Agent 帮助”。分配了标签的 Light Agent 只能连接到允许与具有该标签的 Light Agent 连接的 SVM。

使用连接标签的设置

设置	描述
使用标签连接 Light Agent	该复选框用于启用或禁用 Light Agent 使用 SVM 连接标签。
标签	分配给 Light Agent 的标签。 您可以输入最多 255 个字符的文本字符串作为标签。可以使用除 ; 字符外的任何字符。 如果选中了“**使用标签连接 Light Agent**”复选框，则该字段可用。

SVM 选择算法

在此窗口中，可以指定 Light Agent for Linux 应使用的 SVM 选择算法，并配置使用高级 SVM 选择算法的设置。

SVM 选择算法

设置	描述
使用标准 SVM 选择算法	如果选择此选项，在虚拟机上安装并运行后，Light Agent 会选择 Light Agent 本地的 SVM 进行连接。有关更多详细信息，请参阅“Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助”。 如果没有可连接的本地 SVM，Light Agent 会选择连接的 Light Agent 数量最少的 SVM，无论该 SVM 在虚拟基础架构中的位置如何。 默认选中该选项。
使用扩展 SVM 选择算法	如果选择此选项，您可以使用“**SVM 路径**”滑块来指定在确定 SVM 相对于 Light Agent 是否为本地时如何考虑 SVM 在虚拟基础架构中的位置。Light Agent 只能连接到本地 SVM。 您还可以指定在选择要连接到的 SVM 时不应考虑虚拟基础架构中的 SVM 路径。 选择 SVM 时，Light Agent 会考虑连接到 SVM 的 Light Agent 数量，以确保 Light Agent 在可连接的 SVM 之间均匀分布。
SVM 路径	可让您指定虚拟基础架构中的 SVM 路径类型，在选择要连接的 SVM 时会考虑该类型： • **Hypervisor**。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）： ◦ SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux 或 Numa vServer 上的虚拟基础架构中）。 ◦ SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中（在 OpenStack 平台、VK Cloud 或 TIONIX Cloud 平台管理的虚拟基础架构中）。 如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 或同一服务器组中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。 • **集群**。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）： ◦ SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux 或 Numa vServer 上的虚拟基础架构中）。 ◦ SVM 与安装了 Light Agent 的虚拟机部署于同一OpenStack 项目中（在 OpenStack 平台、VK Cloud 或 TIONIX Cloud 平台管理的虚拟基础架构中）。

如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 集群或同一 OpenStack 项目中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- **数据中心**。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
  - SVM 与安装了 Light Agent 的虚拟机部署在同一 数据中心中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、Alt Virtualization Server、Astra Linux 或 Numa vServer 上的虚拟基础架构中）。
  - SVM 与安装了 Light Agent 的虚拟机位于同一可用性区域中（在 OpenStack 平台、VK Cloud 或 TIONIX Cloud 平台管理的虚拟基础架构中）。

如果安装了 Light Agent 的虚拟机所在的同一数据中心或可用区中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- **忽略 SVM 路径**。选择 SVM 时，Light Agent 不会考虑其位置。

默认情况下选择“**Hypervisor**”选项。

如果选择“**使用扩展 SVM 选择算法**”选项，则该选项可用。

如果 Light Agent 使用高级 SVM 选择算法，并且选择 SVM 地址列表作为 SVM 检测方法，而且在 SVM 上启用大型基础架构保护模式（有关更多信息，请参阅“Kaspersky Security for Virtualization Light Agent 帮助”），那么只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到该 SVM。您需要将“**SVM 路径**”设置设为“**忽略 SVM 路径**”。如果设置任何其他值，Light Agent 都无法连接到 SVM。

保护连接

在此窗口中，可以启用 Light Agent 和 Protection Server 之间的数据传输通道的加密

确保在 SVM 上的 Protection Server 设置中启用 Light Agent 和 Protection Server 之间的数据传输通道的加密。有关更多详细信息，请参阅“Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助”。

连接保护设置

设置	描述
加密 Light Agent 与 Protection Server 之间的数据通道	使用加密来保护 Light Agent 与 Protection Server 之间的连接。 如果选中该复选框，则会在由策略管理的 Light Agent 与 Light Agent 连接到的 SVM 上的 Protection Server 之间建立安全连接。启用了连接保护的 Light Agent 只能连接到启用了连接保护的 SVM，或者允许与 Protection Server 建立不受保护连接的 SVM。 如果清除该复选框，则会在 Light Agent 与 Light Agent 连接到的 SVM 上的 Protection Server 之间建立不受保护的连接。 默认情况下，清除此复选框。

在命令行中查看有关在 Light Agent 模式下的应用程序使用情况的信息

在命令行中，您可以查看有关在 Light Agent 模式下使用应用程序保护虚拟环境的以下信息：

- 在 Light Agent 模式下使用应用程序的设置
- 连接 Light Agent 到 Integration Server
- 连接 Light Agent 到 SVM

如要查看有关在 Light Agent 模式下使用应用程序的设置信息，请运行以下命令：

```
kesl-control [-V] --ksvla-info
```

该命令向控制台输出以下信息：

- 用于保护虚拟环境的 Light Agent 模式：已启用/已禁用。

  如果启用了 Light Agent 模式，应用程序将被用作 Light Agent （用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。如果禁用了 Light Agent 模式，则在标准模式下使用应用程序。

- VDI 保护模式：已启用/已禁用。

  VDI 保护模式能够优化 Kaspersky Endpoint Security 以在临时虚拟机上运行。如果启用了 VDI 保护模式，则临时虚拟机上不会安装需要重启受保护虚拟机的更新。当接收到需要重新启动的更新时，安装在临时虚拟机上的 Light Agent 会向 Kaspersky Security Center 发送消息，告知需要更新受保护虚拟机模板。

- 受保护虚拟机的类型：临时或持久。
- 受保护虚拟机在虚拟基础架构中的角色：服务器或工作站。
- 受保护虚拟机的标识符 (UUID)。

如要查看有关 Light Agent 连接 Integration Server 的信息，请运行以下命令：

```
kesl-control [-V] --viis-info
```

该命令向控制台输出以下信息：

- Light Agent 连接到的 Integration Server 的地址和端口。
- 与 Integration Server 的连接状态。
- Light Agent 与 Integration Server 之间最后一次连接的日期和时间。

如要查看有关 Light Agent 连接 SVM 的信息，请运行以下命令：

```
kesl-control [-V] --svm-info
```

该命令向控制台输出以下信息：

- Light Agent 连接到的 SVM 的地址，以及虚拟基础架构中 SVM 相对于 Light Agent 的位置：本地或非本地。
- Light Agent 检测 SVM 的方法：使用 Integration Server，或使用手动定义的 SVM 地址列表。
- 如果选择的 SVM 发现方法为 SVM 地址列表，则为 SVM 地址列表。
- 用于将 Light Agent 连接到 SVM 的标签。
- SVM 选择算法：标准或高级。如果使用高级 SVM 选择算法，还会显示 SVM 在虚拟基础架构中的位置类型。

- 保护 Light Agent 与 Protection Server 之间的连接。

有关连接 Light Agent 到 Integration Server 和 SVM 的设置信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

查看事件和报告

在应用程序运行时，可能会发生各种*事件*。这些事件可能是信息性的，也可能包含重要数据。例如，应用程序可以使用事件来通知成功的应用程序数据库更新，或者通知必须消除的应用程序组件操作中的错误。

Kaspersky Endpoint Security 将有关应用程序事件的信息保存到以下日志中：

- 应用程序事件日志。默认情况下，应用程序将有关事件的信息保存到数据库 /var/opt/kaspersky/kesl/private/storage/events.db。您可以在命令行中配置应用程序事件日志。
- 操作系统日志 (syslog)。默认情况下，不使用操作系统日志。您可以启用将事件保存到此日志的功能。

> 访问应用程序事件日志和操作系统日志需要 root 权限。

如果 Kaspersky Endpoint Security 由 Kaspersky Security Center 管理，则有关事件的信息可能会传输到 Kaspersky Security Center 管理服务器。聚合规则适用于某些事件。如果在应用程序运行期间，短时间内生成大量相同类型的事件，则应用程序将切换到事件聚合模式，同时向 Kaspersky Security Center 发送一个聚合事件，并提供事件设置说明。不同的事件可以使用不同的聚合规则。有关事件的更多详细信息，请参阅“Kaspersky Security Center 帮助”。

您可以通过以下方式接收有关应用程序事件的信息：

- 在管理控制台和 Web Console 中
- 在命令行中
- 如果使用 Kaspersky Endpoint Security 图形用户界面，则在应用程序弹出窗口中

某些事件可能包含文件路径。对于输出，文件路径被视为 UTF-8 字符串。如果路径中的任何字节不符合UTF-8编码规则，是否用 ? 字符替换。任何对 Unicode 范围之外的字符代码（大于 0x10FFFF）进行编码的四字节序列也将被替换为 ? 字符。特殊字符将以某种方式转义（替换）。

以下规则适用于输出“`kesl-control -E --query`”中的事件所包含的文件路径中的转义字符：

- '\a'、'\b'、'\t'、'\n'、'\v'、'\f'、'\r' 字符按如下规则被替换为两个字符：
  '\a' -> "\\a"
  '\b' -> "\\b"
  '\t' -> "\\t"
  '\n' -> "\\n"
  '\v' -> "\\v"
  '\f' -> "\\f"
  '\r' -> "\\r"
- 所有其他特殊字符均按原样输出。

以下规则适用于输出“`kesl-control -E --query --json`”中的事件所包含的文件路径中的转义字符：

- 按照 JSON 格式，'\b'、'\f'、'\n'、'\r'、'\t'、'"'、'\\'字符转义如下：
  '\b' -> "\\b"
  '\f' -> "\\f"
  '\n' -> "\\n"

'\r' -> "\\r"
'\t' -> "\\t"
"" -> "\\\""
'\\' -> "\\\\"

- 所有其他特殊字符均按照 JSON 中转义特殊字符的通用规则进行转义（'\a' -> '\u0007 '）。

发送到 syslog 时事件所包含的文件路径中的转义字符规则：

- 按照 JSON 格式，'\b'、'\f'、'\n'、'\r'、'\t'、""、'\\'字符转义如下：
  '\b' -> "\\b"
  '\f' -> "\\f"
  '\n' -> "\\n"
  '\r' -> "\\r"
  '\t' -> "\\t"
  "" -> "\\\""
  '\\' -> "\\\\"
- 所有其他特殊字符均按照 JSON 中转义特殊字符的通用规则进行转义（'\a' -> '\u0007 '）。

在描述规则时，序列中的第一个反斜杠是转义字符。

例如：
'\a' 是一个字符（一个控制字符）。

'\\a' 是两个字符（反斜杠 + a字符）。

'\\' 是一个字符（反斜杠），'\\\\' 是两个字符（反斜杠 + 反斜杠）。

应用程序会根据应用程序运行时发生的事件生成各种类型的*报告*。报告包含有关每个 Kaspersky Endpoint Security 组件的操作、每个任务的结果以及应用程序整体操作情况的信息。

您可以通过以下方式查看报告：

- Kaspersky Security Center 报告可在管理控制台和 Web Console 中获取。您可以使用它们来获取有关受感染文件或密钥和应用程序数据库的使用情况等的信息。有关使用 Kaspersky Security Center 报告的详细信息，请参阅“Kaspersky Security Center 帮助”。
- 应用程序报告可在 Kaspersky Endpoint Security 图形用户界面中获取。

活动和报告可能包含以下个人数据：

- 操作系统用户的用户名和用户 ID
- 用户文件的路径
- 反加密勒索组件扫描的远程设备的 IP 地址
- 防火墙管理组件扫描的网络数据包的发送者和接收者的 IP 地址
- 更新源的网址
- 常规应用程序设置的值

- 命令行任务的名称和设置
- 检测到恶意网址、网络钓鱼网址、广告软件网址以及包含入侵者可以用来破坏设备或数据的合法应用程序的网址
- 容器和映像的名称
- 容器和镜像的路径
- 设备的名称和 ID
- 存储库的网址
- 可执行应用程序文件的文件名、文件路径与哈希和
- 应用程序类别名

将事件日志配置到操作系统日志中

默认情况下，Kaspersky Endpoint Security 运行期间发生的事件不会记录在操作系统日志中。您可以使用 Web Console、管理控制台或命令行启用将事件记录到此日志中的功能。

在 Kaspersky Security Center 中，您还可以选择要保存到操作系统日志的事件。

在 Web Console 中配置

在 Web Console 中，您可以在策略属性（**应用程序设置→常规设置→应用程序设置**）中配置将事件记录到操作系统日志中。

单击“**通知**”部分中的“**配置通知**”链接将打开“**通知**”窗口。在此窗口中，您可以使用复选框选择应用程序在操作系统日志中记录的事件。

您可以选择单个事件类型或具有特定严重性级别的所有事件类型。

默认情况下，这些复选框均处于未选中状态。

在管理控制台中配置

在管理控制台中，您可以在策略属性（**常规设置→应用程序设置**）中配置将事件记录到操作系统日志中。

单击“**通知**”中的“**配置**”将打开“**通知设置**”窗口。在此窗口中，您可以使用复选框选择应用程序在操作系统日志中记录的事件。

您可以选择单个事件类型或具有特定严重性级别的所有事件类型。

默认情况下，这些复选框均处于未选中状态。

在命令行中配置

您可以通过常规应用程序设置中的 `UseSyslog` 选项，在命令行中启用或禁用将事件保存到操作系统日志。

您可以通过命令行开关或包含所有常规应用程序设置的配置文件来编辑该选项。

UseSyslog 接受以下值：

- Yes：启用将事件保存到 syslog。
- No（默认）：禁用将事件保存到 syslog。

配置应用程序事件日志设置

默认情况下，有关事件的信息会保存到设备上的应用程序事件日志中。您可以通过常规应用程序设置在命令行中定义以下应用程序事件日志选项：

- 通过 EventsStoragePath 选项更改应用程序事件日志数据库的路径。默认值：/var/opt/kaspersky/kesl/private/storage/events.db。
- 通过 MaxEventsNumber 选项指定应用程序待存储的最大事件数。默认值：500000。如果超过指定的事件数，应用程序将删除最早的事件。

您可以借助命令行开关或包含所有常规应用程序设置的配置文件来更改设置的值。

在 Kaspersky Security Center 中查看事件

所有 Kaspersky Endpoint Security 事件的列表显示在 Web Console 和管理控制台中。

您可以配置事件通知。*通知*是一种消息，包含有关受保护设备上所发生事件的信息。通知会及时为您提供有关应用程序事件的信息。您可以配置当收到来自应用程序的事件或通过电子邮件收到有关事件的通知时执行脚本。

有关使用 Kaspersky Security Center 通知的详细信息，请参阅“Kaspersky Security Center 帮助”。

在命令行中查看事件

在命令行中，您可以查看：

- 当前应用程序事件
- 应用程序事件日志中的事件

显示当前事件

您可以输出有关所有当前应用程序事件的信息，或与启动或停止指定任务相关的当前事件的信息。您可以使用筛选器输出某些当前事件，例如指定类型的事件。

要输出有关所有当前应用程序事件的信息，请运行：

```
kesl-control -W
```

该命令将返回事件的名称以及有关事件的其他信息。

要仅输出与运行中任务相关的当前事件的信息，请运行：

```
kesl-control --start-task <任务 ID/名称> -W
```

示例：
启用 ID=1 的运行中任务的当前事件的显示：

```
kesl-control --start-task 1 -W
```

要输出符合筛选条件的当前事件信息，请运行：

```
kesl-control -W --query "< 筛选条件 >"
```

筛选条件是通过一个或多个逻辑表达式来设置的，格式为 < 字段 > < 比较运算符 > ‘< 值 >’，结合逻辑运算符 and。

示例：
显示 TaskStateChanged 事件：

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

示例：
显示由“User”用户发起的 TaskSettingsChanged 事件：

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'""
```

显示事件日志中的事件

您可以将有关事件的信息从应用程序事件日志输出到控制台或文件。您可以使用筛选器仅显示某些事件。

要输出有关应用程序事件日志中的所有事件的信息，请运行：

```
kesl-control -E --query [--db < 数据库文件 >]
```

其中：

- < 数据库文件 > 是从中输出事件的事件日志数据库文件的完整路径。默认情况下，应用程序将有关事件的信息保存到数据库 /var/opt/kaspersky/kesl/private/storage/events.db。数据库的位置由 EventsStoragePath `global application setting` 决定。

您可以使用 `less` 命令来浏览显示的事件列表。默认下，应用程序存储多达 500,000 个事件。应用程序存储的最大事件数量取决于 `MaxEventsNumber` 常规应用程序设置。

如果事件日志位于默认数据库中，则可以使用以下命令输出有关所有事件的信息：

```
kesl-control -E
```

要输出应用程序事件日志中符合特定条件的事件的信息，请运行：

```
kesl-control -E --query "< 筛选条件 >" [--db < 数据库文件 >] [-n < 数量 >] [--json] [--reverse]
```

其中：

- < 筛选条件 >：一个或多个逻辑表达式，格式为 < 字段 >< 比较运算符 >'< 值 >'，结合逻辑运算符 and 来限制结果。
- < 数量 > – 要显示的所选内容中最新事件的数量（从所选内容的末尾开始计算的记录数量）。
- --json：以 JSON 格式输出事件。
- --reverse：倒序显示事件（最新事件显示在顶部，最早事件显示在底部）。

要将有关应用程序事件日志中符合特定条件的事件的信息输出到文件，请运行：

```
kesl-control -E --query "< 筛选条件 >" [--db < 数据库文件 >] [-n < 数量 >] --file < 文件名和路径 > [--json]
```

其中 --file < 文件名和路径 > 是输出事件到文件的完整路径。

应用程序组件完整性检查

Kaspersky Endpoint Security 包含许多不同的二进制模块，其形式有动态链接库、可执行文件、配置文件和接口文件。入侵者可以将一个或多个应用程序可执行模块或文件替换为包含恶意代码的其他文件。为了防止模块和文件的替换，Kaspersky Endpoint Security 会检查应用程序组件的完整性。应用程序会检查模块和文件是否有未经授权的更改或损坏。如果某个应用程序模块或文件的校验码不正确，则其被认为已损坏。

如果设备上安装了以下应用程序组件，则会对其进行完整性检查：

- 应用程序包
- 图形用户界面软件包
- Kaspersky Security Center 网络代理程序包
- Kaspersky Endpoint Security 管理插件

该应用程序检查名为*清单文件*的特殊列表中的文件的完整性。每个应用程序组件都有自己的清单文件，其中包含应用程序文件的列表，这些程序文件的完整性对于此应用程序组件的正确工作至关重要。每个组件的清单文件名相同，但清单文件的内容不同。清单文件经过数字签名，其完整性也得到检查。

使用完整性检查实用程序检查应用程序组件的完整性。

> 完整性检查实用程序必须在具有 root 权限的帐户下运行。

要检查完整性，您可以使用随应用程序一起安装的实用程序或经过认证的 CD 上分发的实用程序。

> 推荐从认证的 CD 上运行完整性检查实用程序，以确保该实用程序的完整性。从 CD 运行该实用程序时，请指定清单文件的完整路径。

与应用程序一起安装的完整性检查实用程序位于以下路径中：

- 要检查应用程序软件包、图形用户界面软件包和网络代理：/opt/kaspersky/kesl/bin/integrity_checker。
- 要检查 Kaspersky Endpoint Security 管理插件 – 管理插件的可执行模块 (DLL) 所在的目录：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plug-in version>.plg\integrity_checker.exe – 适用于 32 位操作系统
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plug-in version>.plg\integrity_checker.exe – 适用于 64 位操作系统

清单文件位于以下路径中：

- /opt/kaspersky/kesl/bin/integrity_check.xml – 检查应用程序包的完整性。
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml – 检查图形用户界面软件包的完整性。
- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – 在 32 位操作系统中检查网络代理。
- /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – 在 64 位操作系统中检查网络代理。

要检查应用程序组件的完整性，请运行以下命令：

- 要检查应用程序软件包和图形用户界面软件包：

  `integrity_checker [<清单文件的路径>] --signature-type kds-with-filename`

- 检查 Kaspersky Endpoint Security 管理插件和网络代理：

  `integrity_checker [<清单文件的路径>]`

默认路径表示清单文件与完整性检查实用程序位于同一目录。

您可以使用以下可选设置运行该实用程序：

- `--crl <目录>` – 包含证书吊销列表的目录的路径。
- `--version` – 显示实用程序的版本。
- `--verbose` – 显示有关已执行的操作及其结果的详细信息。如果您未指定此设置，则将仅显示错误、未通过检查的对象以及扫描统计信息摘要。
- `--trace <文件名>`，其中 `<文件名>` 是将以 DEBUG 细节级别记录扫描期间发生的事件的文件的名称。
- `--signature-type kds-with-filename` – 要检查的签名类型（检查应用程序软件包、图形用户界面软件包和网络代理时需要此设置）。
- `--single-file <文件>` – 仅扫描清单中的一个文件；忽略清单中的其他对象。

您可以通过运行 `integrity_checker --help` 命令，查看实用程序选项帮助中所有可用的完整性检查实用程序设置说明。

检查清单文件的结果如下所示：

- `SUCCEEDED` — 已确认文件的完整性（返回码 0）。
- `FAILED` – 未确认文件的完整性（返回码不是 0）。

如果在应用程序启动时检测到应用程序或网络代理的完整性被破坏，Kaspersky Endpoint Security 会在事件日志和 Kaspersky Security Center 中生成 *IntegrityCheckFailed* 事件。

通过图形用户界面进行应用程序管理

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则不支持图形用户界面。

您可以使用 Kaspersky Endpoint Security 图形用户界面执行以下操作：

- 查看有关设备保护状态的信息。
- 启用和禁用应用程序组件：
  - 文件威胁防护。
  - 可移动驱动器扫描。
  - Web 威胁防护。
  - 网络威胁防护。
  - 反加密勒索。
  - 防火墙管理。
  - 应用程序控制。
  - 设备控制。
  - 行为检测。
  - 系统完整性监控。
- 启动和停止扫描任务：
  - 恶意软件扫描。
  - 关键区域扫描。
  - 容器扫描。
- 启动和停止数据库更新和回滚任务。
- 单击要扫描的文件或目录，运行自定义扫描。
- 启用和禁用卡巴斯基安全网络。
- 查看应用程序统计数据和报告。
- 管理应用程序授权许可密钥和查看有关应用程序在其下使用的授权许可以及与授权许可关联的密钥的信息。
- 查看有关放置在备份中的对象的信息。
- 创建应用程序跟踪文件。

如果应用程序组件或任务在"仅通知"模式下运行，则组件或任务的 GUI 将显示警告 *"仅通知"模式已选择*。

图形用户界面

通知区域中的应用程序图标

在设备上安装 Kaspersky Endpoint Security 图形用户界面软件包后，应用程序图标会出现在任务栏通知区域的右侧。

应用程序图标充当上下文菜单和主应用程序窗口的快捷方式。

应用程序图标的上下文菜单包含下列项：

- **Kaspersky Endpoint Security 12.1 for Linux**。打开应用程序的主窗口，其中显示设备的保护状态，并包含用于访问应用程序功能的界面元素。
- **退出**。退出应用程序图形用户界面。

应用程序主窗口

要打开应用程序的主窗口，请执行以下操作之一：

- 右键单击或双击任务栏通知区域中的应用程序图标。
- 在操作系统窗口管理器的应用程序菜单中选择应用程序名称。

应用程序的主窗口分为多个部分：

- 应用程序主窗口的中央部分显示设备的保护状态。单击该窗口的此部分将会打开“**保护中心**”窗口。此窗口显示有关设备保护状态的信息，以及为修复保护问题（如果有）所要执行的操作的相关建议。
- “**扫描**”按钮显示恶意软件扫描任务状态和检测到的威胁数量。单击此按钮将打开“**扫描**”窗口。在此窗口中，您可以启动和停止“*恶意软件扫描*”、“*关键区域扫描*”和“*容器扫描*”任务。您还可以查看这些任务的报告。
- “**更新**”按钮显示“*更新*”任务的状态。单击此按钮将打开“**更新**”窗口。在此窗口中，您可以启动“*更新*”和“*回滚*”任务。您还可以查看这些任务的报告。
- 应用程序主窗口的下部包含以下元素：
  - “**报告**”按钮。单击此按钮将打开“**报告**”窗口，您可以在其中查看组件、任务统计数据和各种报告。
  - **备份**按钮。单击此按钮将打开“**备份**”窗口，其中包含有关备份中对象的信息。
  - “**设置**”按钮。单击此按钮将打开“**设置**”窗口，您可以在其中启用或禁用应用程序组件，以及配置卡巴斯基安全网络的使用。
  - “**支持**”按钮。单击此按钮将打开**支持**窗口，其中显示应用程序的当前版本和以下信息：
    - **密钥**– 添加到应用程序的活动授权许可密钥，或者未添加密钥的消息。单击此字段中的链接将打开**“授权许可”**窗口，其中显示详细的授权许可信息。
    - **密钥状态**– 有关活动授权许可密钥状态的信息，或未添加密钥的消息。

- **数据库发布日期**– 应用程序数据库的状态和发布日期。
- **操作系统**––有关设备操作系统的信息。

支持窗口下部显示卡巴斯基信息资源的链接和打开**跟踪**窗口的链接。在此窗口中，您可以创建应用程序跟踪文件并配置跟踪文件的详细程度。

- 应用程序主窗口的下半部分显示有关授权许可和密钥的信息，以及有关授权许可问题（如果有的话）的信息。单击窗口的此区域将打开**"授权许可"**窗口，其中显示详细的授权许可信息。

  单击此窗口中的**"购买授权许可"**按钮将打开卡巴斯基在线商店，您可以在那里购买授权许可。购买授权许可后，您将收到一个激活码或密钥文件，您需要使用它来激活应用程序。

启用和禁用应用程序组件

您可以使用图形用户界面来启用或禁用应用程序组件。如果启用了组件，则"**禁用**"按钮可用。默认情况下，将启用以下组件：文件威胁防护、设备控制和行为检测。如果允许在设备上本地管理 Web 威胁防护设置（未应用策略或未为策略设置"锁定"）并且在系统上检测到一个受支持的浏览器，则可以自动启用 Web 威胁防护组件。

如果禁用了组件，则"**启用**"按钮将可用。

如要启用或禁用应用程序组件：

1. 打开主应用程序窗口。
2. 在主应用程序窗口下部，单击"**设置**"按钮。

   将打开"**设置**"窗口。
3. 单击该组件的"**启用**"或"**禁用**"。

启动和停止扫描任务

要启动或停止扫描任务：

1. 打开主应用程序窗口。
2. 在主应用程序窗口中，单击**扫描**。

   这将会打开**扫描**窗口。
3. 执行下列操作之一：
   - 如果要启动一项扫描任务，请单击要启动的扫描任务下的**启动**按钮。

     此时将显示正在运行的扫描任务的进度。
   - 如果要停止一项扫描任务，请单击要停止的扫描任务下的**停止**按钮。

     扫描任务将停止，并显示有关已扫描对象和已检测到的威胁的信息。
4. 要查看有关扫描任务的报告，请单击**显示报告**按钮。

当检测到受感染的对象或扫描任务已完成时，在任务栏右侧应用程序图标附近的通知区域中将出现一个弹出窗口。

“**扫描**”窗口还显示临时引导扇区扫描任务 (*Scan_Boot_Sectors_{ID}*) 和临时自定义文件扫描任务 (*Scan_File_{ID}*) 的进度和结果。通过单击十字或关闭“**扫描**”窗口（切换到主窗口或退出应用程序时），可以隐藏有关已完成的临时任务的信息。

启动和停止更新任务

要启动或停止更新任务：

1. 打开主应用程序窗口。
2. 在主应用程序窗口中，单击**更新**。
   更新窗口将打开。
3. 执行下列操作之一：
   - 如果要启动一项任务，请单击要启动的任务下的**启动**按钮。
     此时将显示正在运行的更新任务的进度。
     如果更新任务成功完成，则**回滚更新**链接将变为可用，并且您可以回滚上次成功的数据库更新。
   - 如果要停止一项任务，请单击要停止的任务下的**停止**按钮。
     更新任务将会停止。
4. 要查看有关任务的报告，请单击**显示报告**按钮。

要启动回滚任务：

1. 打开主应用程序窗口。
2. 在主应用程序窗口中，选择**更新**部分。
   更新窗口将打开。
3. 单击**回滚更新**链接以运行回滚任务。

配置卡巴斯基安全网络

您可以通过图形用户界面启用或禁用卡巴斯基安全网络的使用。

要启用卡巴斯基安全网络：

1. 打开主应用程序窗口。
2. 在主应用程序窗口下部，单击“**设置**”按钮。
   将打开“**设置**”窗口。
3. 在“**设置**”窗口中，选择以下选项之一：

- **扩展 KSN 模式** — 如果要使用卡巴斯基安全网络，从知识库中获取信息，并发送有关威胁类型和来源的匿名统计数据和信息。
- **基本 KSN 模式**，如果要使用卡巴斯基安全网络，从知识库中获取信息，但不发送有关威胁类型和来源的匿名统计数据和信息。

4. 单击“**启用**”按钮。

   “**使用卡巴斯基安全网络**”窗口打开。

5. 在“**使用卡巴斯基安全网络**”窗口中，仔细阅读卡巴斯基安全网络声明并选择“**我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件**”选项。

6. 单击“**确定**”。

   如果在“**使用卡巴斯基安全网络**”窗口中未选择任何选项，则“**确定**”按钮不可用。

要禁用卡巴斯基安全网络：

1. 打开主应用程序窗口。
2. 在主应用程序窗口下部，单击“**设置**”按钮。

   将打开“**设置**”窗口。

3. 单击**启用**。
4. 在打开的窗口中，单击“**是**”按钮拒绝使用卡巴斯基安全网络。

查看报告

您可以使用图形用户界面查看应用程序报告。报告包含有关应用程序组件和任务的操作的信息。

报告数据将以表格的形式呈现，该表格中包含一个事件列表。表中的每一行都包含有关单独事件的信息。事件属性将在表格列中显示。各种组件和任务运行时记录的事件具有不同的属性集。

报告中使用以下事件重要级别：

- *严重* — 重要性级别为“严重”的事件，需要予以注意，因为它们表明应用程序操作中存在问题或设备保护中存在漏洞
- *高*
- *中度*
- *低*
- *信息*
- *Error*

单击应用程序主窗口下部的“**报告**”后，将打开一个窗口并在窗口中显示报告。

应用程序中提供以下报告：

- **统计**。此报告包含“文件威胁防护”和扫描任务统计信息。您可以通过单击“**重新加载**”按钮来更新显示的报告。

- **系统审计**。此报告包含有关在应用程序操作期间以及用户与应用程序交互期间发生的事件的信息。
- **威胁防护**。此报告包含有关在运行以下应用程序组件时记录的事件的信息：
  - 文件威胁防护。
  - 可移动驱动器扫描。
  - 反加密勒索。
  - Web 威胁防护。
  - 网络威胁防护。
  - 防火墙管理。
  - 应用程序控制。
  - 设备控制。
  - 行为检测。
  - 系统完整性监控。
- **按需任务**。此报告包含有关扫描任务、更新任务和系统完整性检查记录的事件的信息。

要查看报告：

1. 打开主应用程序窗口。
2. 在主应用程序窗口的下部，单击“**报告**”按钮。
   这将会打开“**报告**”窗口。
3. 在“**报告**”窗口的左侧，选择所需的报告类型。
   包含事件列表的报告将显示在窗口的右侧。
   默认情况下，事件已根据**日期**列的值按照升序进行排序。
4. 要查看有关事件的详细信息，请在报告中选择该事件。
   包含此事件属性的部分将会显示在窗口底部。

为便于处理报告，您可以通过以下几种方法修改数据的显示方式：

- 按发生时间筛选事件列表。
- 使用搜索功能查找特定的事件。
- 在单独的区域中查看所选事件。

查看备份对象

您可以使用图形用户界面对备份对象执行以下操作：

- 查看有关放入设备备份中的对象的信息。
- 将对象从备份恢复到其原始目录。
- 从备份中删除对象。删除的对象以后将无法恢复。

有关恢复和删除对象的信息保存到事件日志中。

如要查看备份中的对象：

1. 打开主应用程序窗口。
2. 在主应用程序窗口的下部，单击**备份**按钮。
   这将打开**备份**窗口。

在此窗口中，会显示有关备份存储中的对象的以下信息：

- 对象名称。
- 对象的完整路径。
- 对象添加到备份中的日期。
- 从备份中删除对象的日期（如果设置了备份保留期，则显示此字段）。
- 对象大小。

管理授权许可密钥

使用图形用户界面，您可以添加和删除应用程序授权许可密钥，并查看有关应用程序所使用的授权许可以及关联的授权许可密钥的信息。

您可以通过添加活动授权许可密钥来激活应用程序。

*激活*是激活授权许可的过程，可让您使用应用程序的完整功能版本，直到授权许可到期。

如果您在不包含Kaspersky Endpoint Detection and Response Optimum功能的授权许可下使用应用程序，则若要激活此功能，您需要添加额外的 Kaspersky Endpoint Detection and Response Optimum 附加授权许可密钥（“EDR Optimum 密钥”）。

您还可以向应用程序添加备用密钥。当与活动密钥关联的授权许可到期或活动密钥被删除时，备用密钥成为活动密钥。备用密钥可避免当授权许可到期时应用程序功能受限。

只有在添加了活动授权许可密钥之后，才可以添加备用授权许可密钥。

添加授权许可密钥

如要将活动密钥添加到应用程序：

1. 打开主应用程序窗口。
2. 执行下列操作之一：
   - 在主应用程序窗口的下半部分，单击显示有关授权许可和密钥信息的区域。
   - 在主应用程序窗口的下半部分，单击**支持**按钮，然后在打开的**支持**窗口中，使用**密钥**字段中的链接打开**授权许可**窗口。

   授权许可窗口将打开。单击此窗口中的**"购买授权许可"**按钮将打开卡巴斯基在线商店，您可以在那里购买授权许可。
3. 您可以在商业授权许可或试用授权许可下激活应用程序。

   要在商业许可下激活应用程序：

   a. 单击**商业密钥**部分中的**添加**按钮，然后执行以下操作，具体取决于您用于添加密钥的方法：
      - 如果您想使用激活码添加密钥，请输入激活码并单击**下一步**按钮。
      - 如果您想使用密钥文件添加密钥，请单击**添加密钥**按钮，然后在打开的窗口中选择一个扩展名为.key的文件。

      该窗口显示有关密钥及其相关授权许可的信息。

   b. 单击**激活**按钮。

   要在试用授权许可下激活应用程序，请单击**试用密钥**部分中的**激活**按钮。该窗口显示有关试用授权许可和相关密钥的信息。

   > 只能在一个试用期内根据试用授权许可使用应用程序。

添加活动应用程序密钥后，您可以添加备用密钥，并且（如果需要）还可以添加 EDR Optimum 附加密钥。要开始添加备用或附加密钥，请使用**授权许可**窗口上部的**添加**按钮。

移除授权许可密钥

要删除已添加到应用程序的授权许可密钥：

1. 打开主应用程序窗口。
2. 执行下列操作之一：
   - 在主应用程序窗口的下半部分，单击显示有关授权许可和密钥信息的区域。
   - 在主应用程序窗口的下半部分，单击**支持**按钮，然后在打开的**支持**窗口中，使用**密钥**字段中的链接打开**授权许可**窗口。

   授权许可窗口将打开。
3. 单击要删除的密钥信息右侧的**"删除"**按钮。

4. 在打开的窗口中确认删除。

查看授权信息

要查看授权许可信息：

1. 打开主应用程序窗口。
2. 执行下列操作之一：
   - 在主应用程序窗口的下半部分，单击显示有关授权许可和密钥信息的区域。
   - 在主应用程序窗口的下半部分，单击**支持**按钮，然后在打开的**支持**窗口中，使用**密钥**字段中的链接打开**授权许可**窗口。

   授权许可窗口将打开。

如果备用密钥已被添加到应用程序，则窗口将显示有关应用程序据此使用的授权许可的信息以及与备用密钥关联的授权许可的信息。单击**更多信息**链接可以查看有关授权许可和密钥的完整信息。

当前授权许可部分显示有关活动密钥和相关授权许可的信息：

- 活动应用程序授权许可的类型、授权许可限制和授权许可期限。
- **"密钥"**是唯一的字母数字序列。
- **密钥状态** – 密钥的状态或密钥相关问题的消息（如果有）。
- **有效自** – 通过添加此密钥激活应用程序的日期。
- **到期** – 授权许可到期前的天数，以及 UTC 格式的授权许可到期日期。
- **应用程序名称** – 为其添加了激活密钥的应用程序的名称。
- **保护** – 有关保护功能限制和更新应用程序数据库的能力的信息。

如果您向应用程序添加了活动的 EDR Optimum 密钥，则有关此密钥及其关联授权许可的信息也会显示在**"当前授权许可"**部分。

备用密钥部分显示有关备用密钥和相关授权许可的信息：

- 备用密钥的类型、授权许可限制以及与该密钥关联的授权许可期限。
- **"密钥"**是唯一的字母数字序列。
- **授权许可类型** – 与备用密钥关联的授权许可类型。
- **应用程序名称** – 为其添加了激活密钥的应用程序的名称。
- **保护** – 有关保护功能限制和更新应用程序数据库的能力的信息。

如果您向应用程序添加了备用 EDR Optimum 密钥，则有关此密钥及其关联授权许可的信息也会显示在**"备用密钥"**部分。

创建跟踪文件

您可以使用图形用户界面来创建应用程序跟踪文件，并定义其中的细节级别。

要创建跟踪文件：

1. 打开主应用程序窗口。
2. 在主应用程序窗口的下部，单击**支持**按钮。
   支持窗口将打开。
3. 单击**跟踪**链接以打开**跟踪**窗口
4. 在"**级别**"下拉列表中，选择跟踪文件的细节级别。
   我们建议您通过卡巴斯基技术支持专家了解所需的细节级别。默认值为**诊断 (300)**。
5. 单击**启用**按钮开始跟踪。
6. 重现导致问题的情况。
7. 单击**禁用**按钮停止跟踪。

创建的跟踪文件存储在 /var/log/kaspersky/kesl/ 目录中。

Kaspersky Endpoint Security 容器应用程序（KESL 容器）

Kaspersky Endpoint Security 分发包包含用于创建容器应用程序（“KESL 容器”）的文件，容器应用程序可嵌入到外部系统，从扫描镜像存储库中的容器镜像。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则不支持 KESL 容器功能。

KESL 容器可让您执行以下操作：

- 扫描位于存储库中的容器镜像。
- 将不包含感染对象的已扫描镜像传输到受信任的存储库。

已部署、激活和配置的 KESL 容器提供以下 Kaspersky Endpoint Security 功能组件和任务：

- 文件威胁防护
- 扫描任务：
  - 恶意软件扫描
  - 关键区域扫描
  - 容器扫描
- 容器监控

KESL 容器中提供以下 Kaspersky Endpoint Security 附加功能：

- 使用密钥文件或激活码来激活应用程序。
- 更新和回滚应用程序数据库。
- 在设备上的备份中保存文件的副本。

您可以通过 REST API 与 KESL 容器通信。您还可以通过 Kaspersky Security Center 中的策略配置 KESL 容器。

为了在 Kaspersky Security Center 中正确操作 KESL 容器，建议将与 KESL 容器对应的设备移动到具有自己策略的单独管理组。在策略属性中，所有 Kaspersky Endpoint Security 功能和设置均可供编辑，但配置 KESL 容器中不支持的设置不会影响 KESL 容器的运行。

不能使用命令行管理 KESL 容器。

如果在部署期间激活了 KESL 容器，并且该容器连接到 Kaspersky Security Center，并配置了自动将授权许可密钥分发到受管理设备，则该密钥将不适用于与 KESL 容器相对应的设备。

部署和激活 KESL 容器

分发包描述

分发包包含以下文件：

- docker-service-<版本>.tgz – 包含创建镜像所需文件的压缩文件
- kesl-<版本>.rpm – Kaspersky Endpoint Security 安装包
- klnagent.rpm – Kaspersky Security Center 网络代理安装包

docker-service-<版本>.tgz 压缩文件包含以下文件：

- kesl-service – 容器应用程序文件的目录。
- Dockerfile – 用于构建 18.06 以下版本的 docker 镜像的文件。
- Dockerfile.1809 – 用于构建 18.05 之后版本的 docker 镜像的文件。
- build.sh.example – 用于构建镜像的脚本示例。
- run.sh.example – 用于启动 KESL 容器的脚本示例。
- kesl-service.config.example – 容器应用程序配置文件的示例。
- klnagent.conf.example – 用于连接到 Kaspersky Security Center 的配置文件示例。
- readme.md – 快速参考。

KESL 容器部署和激活

要准备 KESL 容器以供使用：

1. 解压缩文件 tar -xvf docker-service-<版本>.tgz。
2. 如果要使用 Kaspersky Security Center 配置 KESL 容器设置，请执行以下操作：
   a. 在 klnagent.conf.example 文件中，指定网络代理变量的值。有关详细信息，请参阅“Kaspersky Security Center 帮助”部分（“*在静默模式下安装 Linux 网络代理（带应答文件）*”部分）。
   b. 将 klnagent.conf.example 复制为 kesl-service/klnagent.conf。
3. 使用 build.sh.example 安装脚本构建 KESL 容器 Docker 镜像：
   a. 如果使用代理服务器，请为 COMMON_AGRS 变量指定所需的值。
   b. 如有必要，将目标 kesl-service 镜像的名称更改为所需名称。
   c. 将 build.sh.example 复制为 build.sh 并为其分配一个可执行文件属性。
   d. 运行 build.sh。
4. 通过执行 `docker images -a` 命令确保构建成功完成。
   将显示以下命令执行结果：

```
REPOSITORY TAG IMAGE ID CREATED SIZE
```

```
kesl-service latest <十六进制> <创建时间> <大小>
```

5. 通过以下方式之一激活 KESL 容器：

   - 使用 Kaspersky Security Center。要激活 KESL 容器，您需要将密钥添加到 Web Console 或管理控制台中与 KESL 容器相对应的设备。

     > 为了在 Kaspersky Security Center 中正确操作 KESL 容器，建议将与 KESL 容器对应的设备移动到具有自己策略的单独管理组。KESL 容器停止后，这些设备将自动从管理组中移除，并且用于这些设备的密钥将被释放。

   - 使用配置文件。
   - 使用环境变量（参见步骤 7）。

6. 配置 KESL 容器（配置 KESL 容器、KESL 容器设置）。

7. 使用以下命令启动 KESL 容器：`docker run --privileged --init -p <KESL 容器端口>:<设备端口> \`

   ```
   -e <变量_1> -e <变量_2> ... -e <变量_n> \
   -v <挂载点_1> -v <挂载点_2> ... -v <挂载点_n> \
   <镜像名称>
   ```

   其中：

   - `<KESL 容器端口>` 是 KESL 容器的端口，必须可以从 KESL 容器外部的网络访问。
   - `<设备端口>` – 是安装了 KESL 容器的设备的端口。

   启动 KESL 容器时，可以使用环境变量激活它：

   - 如果您使用激活码，请添加 `KRAS4D_ACTIVATION='<激活码>'` 选项：

     ```
     docker run ... -e KRAS4D_ACTIVATION='<激活码>'
     ```

   - 如果您使用密钥文件，请添加 `KRAS4D_ACTIVATION='<密钥文件>'` 和 `KRAS4D_KEYPATH=/root/kesl-service/keys` 选项：

     ```
     docker run ... -e KRAS4D_ACTIVATION='<密钥文件>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <包含密钥的目录的路径>:/root/kesl-service/keys
     ```

   您可以在文件 run.sh.example 中看到 run 命令的示例。

配置 KESL 容器

KESL 容器设置以多种方式初始化：

- 默认值（除非另外指定）。
- 从配置文件。在这种情况下，配置文件中的值的优先级高于默认值。
- 这些值可以在启动时作为环境变量传递给 KESL 容器。环境变量的优先级高于配置文件中的设置。

- 在扫描请求主体中。请求主体中的设置具有最高优先级，但它们仅在单个请求中有效。

KESL 容器设置

下表介绍了 KESL 容器设置及其默认值。

KESL 容器设置

设置说明	可用值	默认值
用于监听 REST API 的端口		8085
事件严重性级别	debug info warning error critical noset	noset
授权密钥	如果指定了 KRAS4D_XAPIKEY 设置，则会验证每个请求是否存在 x-api-key 标头并且其内容是否与 KRAS4D_XAPIKEY 设置的值匹配。如果不满足这些条件，则拒绝该请求。如果缺少此设置，则不执行验证。	
激活码或密钥文件	要使用激活码激活 KESL 容器，请在运行 KESL 容器时在配置文件中指定激活码或在环境变量中传递激活码： docker run ... -e KRAS4D_ACTIVATION='< 激活码 >' 要使用密钥文件激活 KESL 容器，请在运行 KESL 容器时在配置文件中指定密钥文件或在环境变量中传递密钥文件： docker run ... -e KRAS4D_ACTIVATION='< 密钥文件 >' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v < 包含密钥的目录的路径 >:/root/kesl-service/keys 要使用密钥文件激活 KESL 容器，需要 /root/kesl-service/keys 挂载点。	
其他扫描设置	可选的 KRAS4D_SCANOPTIONS 设置允许您配置“容器扫描”任务的设置： docker run ... -e KRAS4D_SCANOPTIONS='< 设置 >' 其中 < 设置 > 是“容器扫描”任务的设置。	
其他更新设置	可选的 KRAS4D_UPDATEOPTIONS 设置允许您配置“更新”任务的设置。 docker run ... -e KRAS4D_UPDATEOPTIONS='< 设置 >' 其中 < 设置 > 是“更新”任务设置“SourceType”和“ApplicationUpdateMode”以及“CustomSources.item_#”部分中的设置。	
在 KESL 容器启动时更新应用程序数据库	默认情况下，启动 KESL 容器时，应用程序数据库会下载到 /var/opt/kaspersky/kesl/private/updates 目录。 为了实现多个 KESL 容器与一个应用数据库实例的联合操作，并加快 KESL 容器的启动速度，建议通过挂载方式将该目录移至安装了 KESL 容器的设备： docker run ... -v < 数据库目录的路径 >:/var/opt/kaspersky/kesl/private/updates	True

如果目标存储库中已存在镜像，则不处理该镜像。		False
等待应用程序命令运行的最长时间（秒）		600
等待应用程序数据库更新任务运行的最长时间（秒）		600
KESL 容器配置文件的名称		kesl-service.config

环境变量

以下环境变量可用于配置 KESL 容器：

- KRAS4D_PORT – 用于监听 REST API 的端口。
- KRAS4D_LOGLEVEL – 事件严重性级别。
- KRAS4D_XAPIKEY – 请求授权密钥。
- KRAS4D_ACTIVATION – 激活码或密钥文件名。
- KRAS4D_SCANOPTIONS – 其他扫描设置。
- KRAS4D_UPDATEOPTIONS – 其他更新设置。
- KRAS4D_FORCEUPDATE – 在 KESL 容器启动时更新应用程序数据库。
- KRAS4D_SKIPIMAGEIFEXISTS – 如果目标存储库中已存在镜像，则不处理该镜像。
- KRAS4D_GENERALTIMEOUT – 等待应用程序命令运行的最长时间。
- KRAS4D_UPDTASKTIMEOUT – 等待应用程序数据库更新任务运行的最长时间。
- KRAS4D_CFGNAME：KESL 容器配置文件的名称。

配置文件

KESL 容器配置文件采用 yaml 格式。要从文件中读取设置，请在安装了 KESL 容器的设备上挂载 /root/kesl-service/config/ 路径，如果配置文件的名称与默认名称不同，请指定配置文件的名称。因此，您可以为每组 KESL 容器指定单独的配置文件。

```
示例：启动 KESL 容器
docker run ... \
-e KRAS4D_CFGNAME='unique_file_name' \
-v <HOST_PATH>:/root/kesl-service/config \
```

```
kesl-service
```

下表显示了配置文件设置和相应的环境变量。

设置与环境变量之间的对应关系

配置文件设置	环境变量
Common 部分	
port: <监听端口>	# KRAS4D_PORT=8085
sqlpath: <包含扫描结果的数据库文件的完整路径>	# KRAS4D_SQLPATH
certdir: <包含注册表证书的目录的路径>	# KRAS4D_CERTDIR
keypath: <包含授权许可密钥的目录的路径>	# KRAS4D_KEYPATH
tmppath: <临时目录的完整路径>	# KRAS4D_TMPPATH
logpath: <事件日志的完整路径>	# KRAS4D_LOGPATH
loglevel: [noset|debug|info|warning|error|critical]	# KRAS4D_LOGLEVEL
“控制”部分	
xapikey: <请求授权密钥>	# KRAS4D_XAPIKEY=None
forceupdate: <容器启动时强制数据库更新 [True|False]>	# KRAS4D_FORCEUPDATE
activation: </root/kesl-service/config/ 中的激活码或密钥文件名>	# KRAS4D_ACTIVATION
detectaction: [delete|skip]	# KRAS4D_DETECTACTION
scanoptions: <扫描设置 [ScanArchived=yes ScanSfxArchived=yes ...]>	# KRAS4D_SCANOPTIONS
skipimageifexist: <如果要将扫描的镜像复制到的服务器上已存在该镜像，则不扫描该镜像>	# KRAS4D_SKIPIMAGEIFEXIST
generaltimeout: <等待应用程序命令运行的最长时间>	# KRAS4D_GENERALTIMEOUT
updtasktimeout: <等待应用程序数据库更新任务运行的最长时间>	# KRAS4D_UPDTASKTIMEOUT
Repositories 部分	
<server>:<port>：请求验证时需要授权的镜像注册表的地址和端口。	
Credentials 子部分	
user: 镜像注册表中授权的用户名	
pass: 镜像注册表中授权的密码	

配置文件示例

```
common:
    port: 8085
    sqlpath: './data/scans.sqlite'
    tmppath: './tmp/'
    keypath: './keys/'
    certdir: './certificates/'
    logpath: '/var/log/kaspersky/kesl-service/'
    loglevel: 'debug'
control:
    xapikey: 0000
    activation: XXXX-XXXX-XXXX-XXXX or XXXX.key
    scanoptions: 'ScanArchives=yes'
    updateoptions: ''
    forceupdate: True
    skipimageifexists: False
    generaltimeout: 600
    updtasktimeout: 1000
repositories:
    repository.any.com:
        certificate: repository_any_comcert.pem
        credentials:
            user: user
            pass: password
```

可用挂载点

以下挂载点可用于使用 KESL 容器：

- /root/kesl-service/data/scans.sqlite – 包含扫描结果的数据库文件的路径。
- /var/opt/kaspersky/kesl/private/updates – 应用程序数据库的路径。
- /root/kesl-service/certificates – 包含存储库证书的目录的路径。
- /root/kesl-service/keys – 包含授权许可密钥的目录的路径。
- /var/log/kaspersky/ – 包含事件日志的目录的路径。
- /root/kesl-service/config/ – 配置文件的路径。
- /var/lib/containers/vfs-storage – Podman 实用程序正常工作所需的挂载点。

使用 REST API 管理 KESL 容器

使用 REST API 实现与 KESL 容器的交互。您可以使用 REST API 执行以下操作：

- 扫描一个文件或多个文件。为此，请提交一个扫描请求 (POST)。

  示例：
  POST http://<服务器>:<端口>/scans

  一个或多个文件。

- 扫描一个或多个 Docker 镜像。为此，请提交一个扫描请求 (POST)。

  示例：
  POST http://<服务器>:<端口>/scans

  要扫描的 Docker 镜像的链接。

- 扫描一个或多个具有附加设置的 Docker 镜像。为此，请提交一个扫描请求 (POST)。

示例：
POST http://<服务器>:<端口>/scans

某种类型的 JSON。

- 获取扫描会话列表。为此，请发送对扫描会话相关信息的请求 (GET)。
  示例：
  GET http://<服务器>:<端口>/scans
- 获取有关扫描会话的信息。为此，请发送对扫描会话相关信息的请求 (GET)。
  示例：
  GET http://<服务器>:<端口>/scans/<唯一扫描会话标识符>
- 在不重新加载 KESL 容器的情况下添加注册表证书。为此，请提交一个添加注册表证书的请求 (POST)。
  示例：
  POST http://<服务器>:<端口>/addcert
- 获取有关 KESL 容器状态的信息。为此，请发送请求以获取有关 KESL 容器状态的信息 (GET)。
  示例：
  GET http://<服务器>:<端口>/status

扫描请求

用途

扫描请求主体中指定的对象。

可以扫描以下对象：

- 一个文件
- 多个文件
- 位于特定存储库中的一个或多个 Docker 镜像
- 位于特定存储库中的一个或多个具有附加设置的 Docker 镜像

路径

http://<服务器>:<端口>/scans[?wait=1]

设置

可选的 `wait` 设置指定扫描会话的类型。

如果设置值为 `1`，则执行同步扫描，并且应用程序在扫描完成时发送报告。

如果设置值为 0，则执行异步扫描，响应如下：

```
{
  "id"="7d27e9b4-a4d7-469b-bdcf-ebfe953498e4",
  "location"="/scans/7d27e9b4-a4d7-469b-bdcf-ebfe953498e4"
}
```

其中：

- id – 扫描会话的唯一标识符。
- location – 用于请求有关此部分的信息的路径：http://<服务器>:<端口>/scans/<位置>。

请求标头

请求可以包含以下标头：

- Content-Type
  定义提交扫描的对象的类型。
  支持的值：
  - application/octet-stream – 一个文件
  - multipart/form-data – 多个文件
  - text/plain – 位于特定存储库中的一个或多个 Docker 镜像
  - application/json – 位于特定存储库中的一个或多个具有附加设置的 Docker 镜像
- x-api-key（可选）
  KRAS4D_XAPIKEY 环境变量中指定的 API 密钥或配置文件中的 xapikey 变量。

可能的错误

如果在 Content-Type 标头中指定了不受支持的值，应用程序将返回以下错误：

```
{
  "error"={
"code"="NOT_SUPPORTED_CONTENT_TYPE",
"details"="<content type>",
"message"="Not supported Content-Type"
  },
  "status"="error"
```

```
}
```

扫描文件请求

Content-Type

application/octet-stream

请求主体

文件。

响应示例：

```
{
  "completed": "Mon, 01 Mar 2021 06:54:39 GMT",
  "created": "Mon, 01 Mar 2021 06:54:38 GMT",
  "progress": 100,
  "scan_result": {
"noname": {
"started": "2021-03-01 06:54:39",
"stopped": "2021-03-01 06:54:39",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/b8eb4128-8cb4-4964-87cf-b9853e6544ec"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
"infected"
  ]
```

```
}
```

扫描多个文件的请求

Content-Type

multipart/form-data

请求主体

多个文件。

响应示例：

```
{
  "completed": "Mon, 01 Mar 2021 06:55:44 GMT",
  "created": "Mon, 01 Mar 2021 06:55:43 GMT",
  "progress": 100,
  "scan_result": {
"clean": {
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "clean"
},
"corrupted.com": {
"errors": [
{
"error": "Corrupted object",
"object": "/root/kesl-service/tmp/75d28fe6-8154-4361-9382-90a76861518a"
}
],
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "non scanned"
},
"error.com": {
"errors": [
{
```

```
"error": "read error",
"object": "/root/kesl-service/tmp/37f6e0dd-13f9-4d11-899c-5fe0f23e407d"
}
],
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"verdict": "non scanned"
},
"infected.com": {
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/7d664646-bf56-4060-b958-5ce9e746c929"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"clean",
"non scanned",
"infected"
  ]

}
```


扫描 Docker 镜像的请求

Content-Type

text/plain

请求主体

要扫描的 Docker 镜像的链接。

可以是以下值：

- 存储库中镜像的路径（例如，https://index.docker.io/jerbi/eicar:latest）。
- 多个镜像的路径掩码（例如，https://index.docker.io/<名称掩码>:<标签掩码>）。您可以使用 ? 和 * 字符来指定掩码。

响应示例：


```
{
  "completed": "Sun, 31 Jan 2021 10:29:26 GMT",
  "created": "Sun, 31 Jan 2021 10:29:20 GMT",
  "progress": 100,
  "scan_result": {
"jerbi/eicar:latest": {
"started": "2021-01-31 10:29:25",
"stopped": "2021-01-31 10:29:26",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
"infected"
  ]
}
```


可能的错误

一个使用 Docker REST API 的请求被用于按掩码获取镜像列表。

但是，在许多公共服务器上，出于安全原因已将其禁用。尝试在此类服务器上按掩码扫描镜像会导致错误。

错误示例：


```
{
  "completed": "Mon, 01 Mar 2021 07:02:24 GMT",
  "created": "Mon, 01 Mar 2021 07:02:22 GMT",
  "scan_errors": [
{
"code": 401,
"details": {
"context": {
"image_mask": "/jerbi/eic*:latest",
"repository": "index.docker.io",
"repository_base": "index.docker.io"
},
"errors": [
"Unauthorized"
]
},
"message": "Invalid source"
},
[
"Unauthorized"
]
  ],
  "status": "completed"
}
```


扫描具有附加设置的 Docker 镜像的请求

Content-Type

application/json

请求主体

以下类型的 JSON：

```
{
  "source": "https://index.docker.io/jerbi/eicar:latest",
  "params": {
"destination": "https://fake",
"skipimageifexists": true,
"custom_callbacks": {
"on_detect": {
"uri": "http://10.16.42.75:5050",
"content-type": "application/json",
"body": {
"session_id": "100",
"session_init": "20201105T072403+0300",
"infected_items": "$infected"
}
},
"on_complete": {
"body": {
"session_id": "100",
},
"uri": "http://10.16.42.75:5050/on_complete",
}
}
  }
}
```

附加请求设置

`params` 部分可以包含以下设置：

- `destination`（可选）– 扫描的镜像将复制到的服务器。
- `skipimageifexists`（可选）– 如果目标服务器已经有具有相同名称和 SHA256 哈希的镜像，则不扫描或复制镜像。仅当指定 `destination` 设置时，才能指定此设置。
- `custom_callbacks`（可选）– 描述扫描完成时应发送的请求：
  - on_detect – 如果检测到威胁，则发送请求。
  - on_complete – 扫描完成后始终发送请求。

在请求主体的描述中，可以指定 `$infected` 替换变量。受感染对象的列表将替换此变量。

响应示例：


```
{
  "completed": "Mon, 01 Mar 2021 07:13:49 GMT",
  "created": "Mon, 01 Mar 2021 07:13:42 GMT",
  "progress": 100,
  "scan_errors": [
{
"code": 500,
"message": "Unable to get images hash from destination registry"
}
  ],
  "scan_params": {
"destination": "https://fake",
"skipimageifexists": true
  },
  "scan_result": {
"jerbi/eicar:latest": {
"started": "2021-03-01 07:13:48",
"stopped": "2021-03-01 07:13:49",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },
  "status": "completed",
  "verdicts": [
```

```
"infected"
  ]

}
```

对扫描会话相关信息的请求 (GET)

用途

获得有关扫描会话的信息。

路径

http://<服务器>:<端口>/scans[?force] – 请求会话列表。

http://<服务器>:<端口>/scans/<唯一扫描会话标识符>[?force] – 请求有关特定会话的信息。

设置

KESL 容器将有关扫描会话的数据存储在内存中，并将它们写入扫描结果数据库。

如果多个 KESL 容器实例使用同一个数据库，可选的 `?force` 设置会启动从数据库中读取信息。如果缺少此设置，将仅显示由特定 KESL 容器实例启动的会话的信息。

请求扫描会话列表

路径

http://<服务器>:<端口>/scans[?force]

响应示例：

```
{
  "629ae0a9-28de-4e2f-b130-67e87ba4d61d": {

"progress": 100,
"status": "completed"
  },

  "655b96fc-34ca-4915-9c41-d52724a277de": {
```

```
"progress": 100,
"status": "completed"
  },

  "7d27e9b4-a4d7-469b-bdcf-ebfe953498e4": {

"progress": 100,
"status": "completed"
  },

  "c32ca88f-2d24-47ec-b040-0540366bea4b": {

"progress": 100,
"status": "completed"
  },

  "df11ad81-26aa-42f9-94bb-39dee4304807": {

"progress": 0,
"status": "completed"
  },

  "fa25340f-4898-497f-ab59-8df494f4ea47": {

"progress": 100,
"status": "completed"
  }

}
```

请求有关特定会话的信息

路径

http://<服务器>:<端口>/scans/<唯一扫描会话标识符>[?force]

响应示例：

```
{

  "completed": "Mon, 01 Mar 2021 06:45:19 GMT",
```

```
  "created": "Mon, 01 Mar 2021 06:45:19 GMT",

  "progress": 100,

  "scan_result": {

"noname": {
"started": "2021-03-01 06:45:19",
"stopped": "2021-03-01 06:45:19",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/65b55d89-b758-4609-a2f3-f63ef839815d"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"
  ]

}
```


添加注册表证书的请求 (POST)

用途

在不重新加载 KESL 容器的情况下添加注册表证书。

路径

http://<服务器>:<端口>/addcert

请求标头

该请求包含一个 Content-Type 标头。

支持的值：

- application/octet-stream – 一个证书文件
- multipart/form-data – 多个证书文件

请求有关 KESL 容器状态的信息 (GET)

用途

获取有关 KESL 容器当前状态的信息，以及决定 KESL 容器状态的应用状态参数（应用状态、授权许可状态、数据库状态）。

路径

http://<服务器>:<端口>/status

响应示例：

```
{'product info': {'databases_date': '< 数据库发布日期 >', 'databases_loaded': True,
'license_expiration': '< 授权许可到期日期 >', 'license_info': 'The key is valid',
'policy': 'Not applied', 'version': '< 应用程序版本 >'}, 'status': 'service available'}
```

可能的错误

错误示例（应用程序未在 KESL 容器中运行）：

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
```

错误示例（未下载应用程序数据库）：

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': '< 授权许可到期日期 >', 'license_info': 'Inconsistent update',
'policy': 'Not applied', 'version': '< 应用程序版本 >'}, 'status': 'service not
available', 'status_reason': ['Databases not loaded', 'License error: Inconsistent
update']}
```

错误示例（授权许可已过期）：

```
{'product info': {'databases_date': '<数据库发布日期>', 'databases_loaded': True,
'license_expiration': '< 授权许可到期日期 >', 'license_info': 'Expired', 'policy': 'Not
applied', 'version': '<kesl 版本>'}, 'status': 'service not available',
'status_reason': ['License error: Expired']}
```

联系技术支持

如果您在应用程序文档或其他应用程序信息来源中找不到问题的解决方案，建议联系技术支持团队。技术支持专家将回答您关于安装和使用 Kaspersky Endpoint Security 的任何问题。

卡巴斯基为 Kaspersky Endpoint Security 的整个生命周期提供支持（请参阅应用程序生命周期）。与技术支持部门联系之前，请阅读支持规则。

可以通过以下方法之一与技术支持部门联系：

- 访问技术支持网站。
- 通过 Kaspersky CompanyAccount 门户向卡巴斯基技术支持发送请求。

通过 Kaspersky CompanyAccount 获取技术支持

Kaspersky CompanyAccount 是为使用卡巴斯基应用程序的公司提供的门户。Kaspersky CompanyAccount 门户设计用于方便用户与卡巴斯基专家之间通过在线请求进行交互。通过使用 Kaspersky CompanyAccount 门户，您可以跟踪卡巴斯基专家处理电子请求的进度，并存储电子请求的历史记录。

您可以在一个 Kaspersky CompanyAccount 帐户下注册您所有的公司员工。单个帐户使您能够集中管理注册员工向卡巴斯基发送的电子请求，同时通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户提供下列语言：

- 英语
- 西班牙语
- 意大利语
- 德语
- 波兰语
- 葡萄牙语
- 俄语
- 法语
- 日语

要了解有关 Kaspersky CompanyAccount 的更多信息，请访问技术支持网站。

获取技术支持信息

在您将问题告知卡巴斯基技术支持专家后，他们可能会要求您发送*跟踪文件*或*转储文件*。

技术支持专家可能还需要有关操作系统和设备上正在运行的进程的其他信息，以及有关应用程序组件操作的详细报告。

在诊断问题时，技术支持专家可能会要求您将应用程序设置更改为：

- 激活接收高级诊断信息的功能；
- 对无法通过标准用户界面执行的单个应用程序组件执行更详细的配置；
- 更改存储接收到的诊断信息的设置；
- 配置捕获网络流量并存储在文件中。

技术支持专家将告诉您执行这些操作所需的所有信息（步骤顺序、要更改的设置、配置文件、脚本、高级命令行功能、调试模块、特殊实用程序等），以及为诊断目的而收到的信息主体。接收到的高级诊断信息存储在用户设备上。此信息不会自动发送给卡巴斯基。

上面列出的步骤只能在技术支持专家的指导下根据他们提供的说明执行。使用应用程序文档中未描述或技术支持专家未推荐的方式独立更改应用程序文件可能会导致应用程序和操作系统性能不佳和出现故障、减少保护以及数据无法访问和损坏。

应用程序跟踪文件

*跟踪文件*可跟踪应用程序命令的逐步执行情况，并检测错误发生在应用程序操作的哪个阶段。

默认情况下，不会生成应用程序跟踪文件。您可以通过常规应用程序设置和图形用户界面在命令行中启用或禁用应用程序跟踪文件的生成并定义跟踪文件中的详细程度。

如果您启用了应用程序跟踪文件，这些文件将存储在 /var/log/kaspersky/kesl/ 目录中。访问此目录需要 root 权限。

只要应用程序在使用中，跟踪文件就会存储在设备上，并且移除应用程序后会永久删除跟踪文件。跟踪文件不会自动发送到卡巴斯基。

跟踪文件以人类可读的格式保存。建议在将信息发送到卡巴斯基之前保护信息，以避免未经授权的访问。

应用程序跟踪文件内容

跟踪文件包含以下常规数据：

- 事件时间。
- 执行线程的编号。
- 造成一个事件的应用程序组件。
- 事件严重程度（信息性事件、警告、严重事件、错误）。
- 对涉及应用程序组件执行命令的事件的描述以及执行此命令的结果。

除常规数据外，跟踪文件还可能存储以下信息：

- 应用程序组件的状态和它们的操作数据。
- 有关应用程序中用户活动的数据。
- 有关设备上安装的硬件的数据。
- 有关所有操作系统对象和事件的数据，包括有关用户活动的信息。
- 操作系统对象中包含的数据（例如，可能包含任何用户个人数据的文件的内容）。
- 网络流量数据（例如，网站上的输入字段的内容，可能包括银行卡信息或任何其他敏感数据）。
- 从卡巴斯基服务器接收的数据（例如应用程序数据库的版本）。
- 从 KATA 服务器接收的数据。
- 有关消耗的 CPU 资源的数据。
- 有关已消耗 RAM 资源的数据。
- 有关应用程序读取和写入文件操作的数据。
- 有关应用程序运行所需的缓存信息量的数据。

配置应用程序跟踪设置

如果您在通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security 应用程序，则可以使用 Web Console 或管理控制台在 Kaspersky Endpoint Security 策略设置中配置该应用程序的跟踪设置。

如果您在命令行上管理应用程序，则可以在常规应用程序设置中配置应用程序的跟踪设置。

编辑 Web Console 中的跟踪设置

在 Web Console 中，您可以在策略属性中配置应用程序跟踪设置（**应用程序设置→常规设置→应用程序设置跟踪和转储设置**部分）（请见下表）。

应用程序跟踪设置

设置	描述
跟踪文件目录的路径	用于输入跟踪文件的目录路径的字段。 默认值：/var/log/kaspersky/kesl。 如果指定其他目录，请确保运行 Kaspersky Endpoint Security 的帐户对该目录具有读/写权限。需要 root 特权才能访问默认跟踪文件目录。
跟踪文件的最大数量	应用程序跟踪文件最大数量的输入字段。 默认值：10。
跟踪文件最大大小 (MB)	应用程序跟踪最大大小的输入字段（以兆字节为单位）。 默认值：500。

要应用跟踪设置，必须重新启动应用程序。

编辑管理控制台中的跟踪设置

在管理控制台中，您可以在策略属性（**常规设置→应用程序设置**）中配置应用程序跟踪设置。

在“**跟踪和转储设置**”下，单击“**配置**”以打开一个窗口，您可以在其中编辑跟踪设置（请见下表）。

应用程序跟踪设置

设置	描述
跟踪文件目录的路径	用于输入跟踪文件的目录路径的字段。 默认值：/var/log/kaspersky/kesl。 如果指定其他目录，请确保运行 Kaspersky Endpoint Security 的帐户对该目录具有读/写权限。需要 root 特权才能访问默认跟踪文件目录。
跟踪文件最大大小 (MB)	应用程序跟踪最大大小的输入字段（以兆字节为单位）。 默认值：500。
跟踪文件的最大数量	应用程序跟踪文件最大数量的输入字段。 默认值：10。

要应用跟踪设置，必须重新启动应用程序。

在命令行中编辑跟踪设置

在命令行中，您可以使用常规应用程序设置中的`TraceLevel`、`TraceFolder`、`TraceMaxFileCount`和TraceMaxFileSize设置来配置应用程序跟踪设置。

`TraceLevel`设置可让您启用或禁用应用程序跟踪并指定跟踪文件中的详细程度。设置可以使用以下值：

- `Detailed` - 生成详细的跟踪文件。
- `MediumDetailed` – 生成包含信息消息和错误消息的跟踪文件。
- `NotDetailed` - 生成一个包含错误消息的跟踪文件。
- `None`（默认值）- 不生成跟踪文件。

`TraceFolder`设置可让您指定存储应用程序跟踪文件的目录。默认值：/var/log/kaspersky/kesl。如果指定其他目录，请确保运行 Kaspersky Endpoint Security 的帐户对该目录具有读/写权限。需要 root 特权才能访问默认跟踪文件目录。

`TraceMaxFileCount`可让您指定应用程序跟踪文件的最大数量。设置可采用从 1 至 10000 的值。默认值：10。

`TraceMaxFileSize`可让您指定应用程序跟踪文件的最大大小（以兆字节为单位）。设置可采用从 1 至 1000 的值。默认值：500。

您可以使用命令行选项或包含所有常规应用程序设置的配置文件来编辑设置。

更改`TraceFolder`、`TraceMaxFileCount`或`TraceMaxFileSize`设置的值后，需要重新启动应用程序。

应用程序管理插件跟踪文件

管理插件跟踪文件不会自动发送到卡巴斯基。

跟踪文件以人类可读的格式保存。建议在将信息发送到卡巴斯基之前保护信息，以避免未经授权的访问。

MMC 管理插件跟踪文件

如果您使用管理控制台来管理 Kaspersky Endpoint Security，则有关 MMC 管理插件运行时发生的事件的信息可以保存到安装管理服务器的设备上的 Kaspersky Endpoint Security MMC 插件跟踪文件中。文件名包含应用程序版本号、文件创建日期和时间以及进程标识符 (PID)。此文件包含有关 MMC 插件操作期间发生的事件的信息，特别是有关策略和任务的操作信息。

默认情况下，不生成 MMC 插件跟踪文件。您可以使用注册表项创建 MMC 插件跟踪文件。有关如何创建跟踪文件的详细信息，请联系技术支持代表。

MMC 插件创建的所有跟踪文件都位于用户在注册表项配置期间指定的文件夹中。

Web 管理插件跟踪文件

如果您使用 Web Console 管理 Kaspersky Endpoint Security，则有关 Web 管理插件运行时发生的事件的信息可能会写入 Web 插件跟踪文件。

如果在 Web Console 安装向导中启用了 Web Console 活动日志记录，则会自动创建 Web 插件的跟踪文件（有关更多详细信息，请参阅“Kaspersky Security Center 帮助”）。

Web 插件的跟踪文件存储在 Web Console 安装文件夹的“logs”子文件夹中。

管理插件跟踪文件的内容

跟踪文件包含以下常规数据：

- 事件时间。
- 执行线程的编号。
- 造成一个事件的应用程序组件。
- 事件严重程度（信息性事件、警告、严重事件、错误）。
- 对涉及应用程序组件执行命令的事件的描述以及执行此命令的结果。

除了常规数据之外，跟踪文件还可能包含以下信息：

- 个人数据，包括姓氏、名字和中间名（如果此类数据是文件路径的一部分）。

- 用于登录操作系统的账户名（如果用户账户名是文件名的一部分）。

关于转储文件

*转储文件*包含有关在创建转储文件时，Kaspersky Endpoint Security 进程工作内存的所有信息。默认情况下不生成转储文件。您可以启用或禁用应用程序发生故障时的转储。

如果您启用了转储，转储文件将存储在 /var/opt/kaspersky/kesl/common/dumps and /var/opt/kaspersky/kesl/common/dumps-user。

需要 root 特权才能访问转储文件。

只要应用程序在使用中，转储文件就会存储在计算机上，并且删除应用程序后会永久删除转储文件。转储文件不会自动发送到卡巴斯基。

转储文件可能包含个人数据。建议在将信息发送到卡巴斯基之前保护信息，以避免未经授权的访问。

启用或禁用转储日志记录

如果您在通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security 应用程序，则可以使用 Web Console 或管理控制台在 Kaspersky Endpoint Security 策略设置中启用或禁用转储。

如果您使用命令行来管理应用程序，则可以通过 kesl.ini 配置文件启用或禁用转储。

转储文件的最大数量有限。

根据操作系统设置，可能无法创建用户转储文件。确保使用 `sysctl kernel.yama.ptrace_scope=0` 配置系统内核。

在 Web Console 中启用或禁用转储

在 Web Console 中，您可以在策略属性中启用或禁用记录转储文件（**应用程序设置→常规设置→应用程序设置跟踪和转储设置**部分）。

转储文件设置

设置	描述
如果应用程序崩溃，创建转储文件	该复选框用于启用或禁用在应用程序崩溃时创建转储文件。 默认情况下，清除此复选框。
转储文件目录的路径。	用于输入存储文件的目录路径的字段。输入字段限制为 128 个字符。 默认值：/var/opt/kaspersky/kesl/common/dumps。

您必须重新启动应用程序才能应用转储文件设置。

在管理控制台中启用或禁用转储

在管理控制台中，您可以在策略属性（**常规设置→应用程序设置**）中启用或禁用记录转储文件。

在**"跟踪和转储设置"**下，单击**"配置"**以打开一个窗口，您可以在其中编辑转储设置。

转储文件设置

设置	描述
如果应用程序崩溃，创建转储文件	该复选框用于启用或禁用在应用程序崩溃时创建转储文件。 默认情况下，清除此复选框。
转储文件目录的路径。	用于输入存储文件的目录路径的字段。输入字段限制为 128 个字符。 默认值：/var/opt/kaspersky/kesl/common/dumps。

您必须重新启动应用程序才能应用转储文件设置。

在命令行上启用或禁用转储

要通过 kesl.ini 配置文件启用或禁用转储，请执行以下操作：

1. 停止 Kaspersky Endpoint Security。
2. 打开 /var/opt/kaspersky/kesl/common/kesl.ini 文件进行编辑。
3. 在**[常规]**下，设置参数值：
   - `CoreDumps=yes`：启用在发生故障时转储。
   - `CoreDumps=no`：禁用转储。
4. 如果要更改保存转储文件的默认目录，请在 `CoreDumpsPath` 选项中指定目录的路径。
5. 启动 Kaspersky Endpoint Security。

使用 Kaspersky Security Center 进行远程设备诊断

在 Kaspersky Security Center 中，您可以对客户端设备执行远程诊断。远程诊断程序可让您远程执行以下操作：

- 启用和禁用跟踪。
- 更改跟踪级别。
- 下载跟踪文件。
- 下载远程应用程序安装日志。
- 下载系统事件 (syslog) 日志。
- 启动、停止和重启应用程序。

Web Console 中的远程诊断

如果您使用 Web Console 管理 Kaspersky Endpoint Security，则客户端设备的远程诊断将在远程诊断窗口中完成。

要打开设备的远程设备诊断窗口：

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。
   将打开受管理设备列表。
2. 选择您想要远程诊断的设备并单击其名称。
   将打开设备属性窗口。
3. 在“**高级**”选项卡上，选择“**远程诊断**”部分。

在远程设备诊断窗口中，您可以查看远程应用程序安装日志。

要查看设备上的远程应用程序安装日志：

1. 打开远程设备诊断窗口：
2. 在“**事件日志**”选项卡上的“**跟踪文件**”块下，单击“**远程安装日志**”。
   将打开“**设备跟踪事件日志**”窗口。

有关远程诊断的更多信息，请参阅“Kaspersky Security Center 帮助”。

使用管理控制台进行远程诊断

如果您使用管理控制台来管理 Kaspersky Endpoint Security，则远程诊断将使用与管理控制台一起自动安装在设备上的特殊 Kaspersky Security Center 远程诊断实用程序来完成。

要打开远程诊断实用程序的主窗口，请执行以下操作：

1. 在管理控制台树中，进入“**受管理设备**”文件夹，选择包含必要设备的管理组。
2. 在工作区中选择“**设备**”选项卡。
3. 在受管理设备列表中，选择要连接远程诊断实用程序的设备，并在设备上下文菜单中选择**外部工具→远程诊断**。
   Kaspersky Security Center 远程诊断实用程序的主窗口将打开。

您可以使用远程设备诊断实用程序来查看远程安装日志。

要查看设备上的远程应用程序安装日志：

1. 打开远程诊断实用程序的主窗口。
2. 如果需要，配置将实用程序连接到设备的选项。在远程诊断实用程序主窗口中，单击“**登录**”按钮。
3. 在打开的窗口中，在对象树中选择“**远程安装日志**”文件夹。

有关远程诊断实用程序的更多信息，请参阅“Kaspersky Security Center 帮助”部分。

手动检查与管理服务器的连接。Klnagchk 实用程序

网络代理分发包包括 klnagchk 实用程序，该实用程序用于检查与管理服务器的连接。

安装网络代理后，该实用程序位于 32 位操作系统的 /opt/kaspersky/klnagent/bin 目录中，以及 64 位操作系统的 /opt/kaspersky/klnagent64/bin 目录中。根据所使用的键值，网络代理启动时将执行以下操作：

- 写入事件日志文件或显示用于将安装在客户端设备上的网络代理连接到管理服务器的设置值。
- 写入事件日志文件或显示网络代理统计信息（自上次启动以来）和运行该实用程序的结果。
- 尝试在网络代理和管理服务器之间建立连接。
- 如果连接失败，实用程序将发送一个 ICMP 数据包来检查安装了管理服务器的设备的状态。

实用程序语法

```
klnagchk [-logfile <文件名>] [-sp] [-savecert <证书文件的路径>] [-restart]
```

键值说明

- `-logfile <文件名>`：将网络代理与管理服务器的连接设置值和运行实用程序的结果都写入事件日志文件。如果未使用该键值，则设置、结果和错误信息将显示在屏幕上。
- `-sp`：显示用于代理服务器用户身份验证的密码。如果通过代理服务器建立与管理服务器的连接，则使用此设置。
- `-savecert <文件名>`：将用于对访问管理服务器进行身份验证的证书保存在指定的文件中。
- `-restart`：重启网络代理。

手动连接到管理服务器。Klmover 实用程序

网络代理分发包包括 klmover 实用程序，该实用程序用于管理与管理服务器的连接。

安装网络代理后，该实用程序位于 32 位操作系统的 /opt/kaspersky/klnagent/bin 目录中，以及 64 位操作系统的 /opt/kaspersky/klnagent64/bin 目录中。根据所使用的键值，网络代理启动时将执行以下操作：

- 使用指定设置将网络代理连接到管理服务器。
- 写入事件日志文件或显示操作结果。

实用程序语法

```
klmover [-logfile <文件名>] {-address <服务器地址>} [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件路径>] [-silent] [-dupfix]
```

键值说明

- `-logfile <文件名>` – 将运行实用程序的结果写入指定文件。如果不使用此键，结果和错误消息将显示在 stdout 中。
- `-address <服务器地址>` – 用于连接的管理服务器的地址。可以是设备的 IP 地址、NetBIOS 或 DNS 名称。
- `-pn <端口号>` – 将用来建立与管理服务器的非加密连接的端口号。默认情况下使用 14000 端口。
- `-ps <SSL 端口号>` – 将使用 SSL 协议建立与管理服务器的加密连接的 SSL 端口号。默认情况下使用 13000 端口。
- `-nossl` – 与管理服务器之间使用非加密连接。如果未指定此键值，则代理通过加密的 SSL 协议连接到管理服务器。
- `-cert <验证文件的路径>` – 将指定的证书文件用于访问新管理服务器时的身份验证。如果未使用该键值，则网络代理将在首次连接管理服务器时接收证书。
- `-silent` – 以非交互模式启动实用程序。有时候该键值很有用，例如在用户注册期间的启动脚本启动该实用程序时。
- `-dupfix` — 如果网络代理的安装方法与分发包中的安装方法不同，则使用此键值；例如，在从磁盘映像恢复网络代理时。
- `-cloningmode 1` – 切换到克隆模式。
- `-cloningmode 0` – 从克隆模式切换。

附录

本节提供补充主要帮助内容的信息。

附录 1.资源消耗优化

扫描对象时，Kaspersky Endpoint Security 使用处理器资源、磁盘子系统输入/输出和操作系统。

要查看应用程序的资源消耗情况，请执行以下命令：

```
top -bn1|grep kesl
```

加载系统时必须执行该命令。

命令输出会显示已用内存量和处理器时间：

```
651 root 20 0 3014172 2.302g 154360 S 120.0 30.0 0:32.80 kesl
```

第 6 列显示驻留内存量 - `2.302g`。

第 9 列显示处理器核心使用率的百分比 — 120.0，其中每个核心通过 100% 表示。因此，120% 表示一个核心已完全使用，另一个核心的使用率为 20%。

如果 Kaspersky Endpoint Security 在扫描对象时运行会严重降低系统速度，则必须对应用程序进行配置，以优化系统资源的使用量。

确定消耗资源的任务

为了确定哪些应用程序任务正在耗用系统资源，有必要区分文件威胁防护任务（OAS 类型）和按需扫描任务（ODS 和 ContainerScan 类型）的资源消耗量。

如果应用程序由 Kaspersky Security Center 策略管理，则需要在研究期间允许本地任务管理。

文件威胁防护任务操作分析

要分析文件威胁防护任务的运行情况：

1. 停止所有扫描和监控任务。
2. 确保按需扫描任务在扫描期间不会运行或无运行计划。您可以使用 Kaspersky Security Center 或在本地执行以下步骤完成此操作：
   a. 通过执行以下命令获取包含所有应用程序任务的列表：

   ```
   kesl-control --get-task-list
   ```

b. 通过执行以下命令获取恶意软件扫描任务的计划设置：

```
kesl-control --get-schedule <任务 ID>
```

如果命令输出为 `RuleType=Manual`，则任务只能手动启动。

c. 获取所有恶意软件扫描任务的计划设置（如果有），然后通过执行以下命令将其设置为手动启动：

```
kesl-control --set-schedule <任务 ID> RuleType=Manual
```

3. 通过执行以下命令，启用生成具有概要详细信息的应用程序跟踪文件：

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. 如果尚未启动文件威胁防护任务，请执行以下命令启动该任务：

```
kesl-control --start-task 1
```

5. 以导致性能问题的模式加载系统；几个小时的时间就够了。

加载时，应用程序会向跟踪文件写入大量信息；但是默认情况下只存储 5 个 500 MB 的文件，因此旧信息将被覆盖。如果性能和资源消耗问题不再出现，则先前的问题很可能是由按需扫描任务引起的，您可以继续分析 ContainerScan 和 ODS 扫描任务的运行情况。

6. 通过执行以下命令禁用创建应用程序跟踪文件：

```
kesl-control --set-app-settings TraceLevel=None
```

7. 通过运行以下命令确定扫描次数最多的对象的列表：

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -r|less
```

结果将加载到 less 文本查看器实用程序中，扫描次数最多的对象将显示在最前。

8. 确定扫描次数最多的对象是否危险。如有任何困难，请联系技术支持。

例如，如果受信任的进程写入目录和日志文件，则可以认为目录和日志文件是安全的，数据库文件也可以视为安全。

9. 写下您认为安全的对象的路径；在配置扫描范围排除项时需要用到这些路径。

10. 如果各种服务频繁向系统中的文件写入数据，则此类文件会在待处理队列中再次受到扫描。运行以下命令，确定待处理队列中扫描次数最多的路径列表：

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
```

扫描次数最多的文件将显示在列表的最前面。

11. 如果某个文件的计数器在几个小时内超过数千次，则应该确认是否可以信任此文件，以便将其从扫描中排除。

确定逻辑与之前的研究相同（请参阅步骤 8）：日志文件可以视为安全对象，因为它们无法启动。

12. 即使某些文件被实时保护任务排除在扫描范围之外，它们仍然可以被应用程序拦截。如果将某些文件排除在实时保护之外并没有显著提高性能，则可以将这些文件所在的挂载点完全排除在应用程序的拦截范围之外。为此，请执行以下操作：

a. 运行以下命令以获取应用程序拦截的文件列表：

```
grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
```

b. 使用此列表，确定用于大多数文件操作拦截的路径并配置拦截例外。

按需扫描任务操作分析

ODS 和 ContainerScan 类型的任务也会耗用大量资源。对于 ODS 类型的任务，请遵循以下建议：

- 确保多个按需扫描任务不会同时运行。该应用程序允许在此模式下运行，但资源消耗可能会显著增加。在本地检查 ODS 和 ContainerScan 类型的所有任务的计划（如文件威胁防护任务中所述）或使用 Kaspersky Security Center。
- 在服务器负载最低的时间段内运行扫描。
- 确保在指定的扫描路径上没有挂载远程资源 (SMB/NFS)。如果某个远程资源扫描无法直接在提供资源的服务器上执行，请不要在具有关键服务的服务器上执行此资源扫描，因为执行此任务可能需要很长时间（具体取决于连接速度和文件数）。
- 在开始之前优化按需扫描任务的设置。

配置文件威胁防护任务

如果在分析了文件威胁防护任务的运行情况之后，您创建了可以从扫描范围中排除的目录和文件的列表，则需要将它们添加到排除项中。

扫描排除项

要递归排除 /tmp/logs 目录及其所有子目录和文件，请执行以下命令：

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

要在 /tmp/logs 目录中按掩码排除一个或多个特定文件，请执行以下命令：

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

要使用递归掩码排除 /tmp/ 目录和子目录中具有 .log 扩展名的所有文件，请执行以下命令：

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

拦截排除项

如果不仅要从扫描中排除某个目录中的文件，还要从拦截中排除这些文件，则可以排除整个挂载点。

要排除整个挂载点：

1. 如果目录不是挂载点，请通过该目录创建一个挂载点。例如，要从 /tmp 目录创建挂载点，请执行以下命令：

   ```
   mount --bind /tmp/ /tmp
   ```

2. 要在服务器重新启动后保留挂载点，请将以下行添加到 /etc/fstab 文件中：

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. 通过执行以下命令将 /tmp 目录添加到全局例外中：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
```

4. 如果要添加多个目录，请将 item_0000 计数器按 1 递增（例如 item_0001、item_0002 等）。

还建议排除挂载连接不稳定或缓慢的远程资源的挂载点。

更改扫描类型

默认情况下，文件威胁防护任务可以在文件打开或关闭时对其进行扫描。如果对“文件威胁防护”任务性能的分析显示写入的文件过多，则可以运行以下命令，使该任务仅在打开文件时运行：

```
kesl-control --set-set 1 ScanByAccessType=Open
```

在此操作模式下，在下次打开文件之前，不会扫描打开文件后对其所做的更改。

配置按需扫描任务

扫描排除项

您可以为按需 ODS 和 ContainerScan 任务定义扫描排除项。您可以采用与文件威胁防护任务的扫描排除相同的方式对此进行配置。

一个扫描任务的扫描排除项设置不会影响其他扫描任务。必须为每个扫描任务单独配置排除项。

在解包压缩文件时设置内存使用限制

递归扫描压缩文件时，按需扫描任务会耗用 RAM 来解压缩存档。默认情况下，应用程序的限制为所有可用 RAM 的 40%，但不少于 2 GB。因此，如果系统的 RAM 超过 5 GB，则可以手动设置内存使用限制。这对于拥有数百 GB RAM 的服务器特别有用。

设置应用程序内存使用限制

您可以限制 Kaspersky Endpoint Security 在运行 OAS、ODS 和 ContainerScan 扫描任务时使用的 RAM 数量。

默认情况下，应用程序最多使用所有可用 RAM 的 40%。对于具有大量 RAM（超过 5 GB）的系统，内存使用限制可能很有用。

您可以使用 kesl.ini 配置文件中的 `ScanMemoryLimit` 选项来调整应用程序在扫描文件时使用的 RAM 大小。默认值：8192 MB。

此设置仅限制扫描文件时使用的内存量。这意味着应用程序所需的内存总量可能会超过此设置的值。

要指定扫描文件时的内存使用限制：

1. 停止 Kaspersky Endpoint Security。
2. 打开 /var/opt/kaspersky/kesl/common/kesl.ini 文件进行编辑。
3. 在**[常规]**中，在 `ScanMemoryLimit` 中指定所需的 RAM 数量：
   `ScanMemoryLimit=<` 内存量（以 `MB` 为单位） `>`
   最小值为 2048 MB。如果指定的值小于 2048 MB，应用程序将使用最小值。
   如果指定的值超出了系统 RAM 大小，则应用程序最多将使用所有可用 RAM 的 40%。
4. 启动 Kaspersky Endpoint Security。

新的扫描文件内存使用限制将在应用程序重启后生效。

附录 2.用于管理 Kaspersky Endpoint Security 的命令

在命令行中，使用 Kaspersky Endpoint Security 管理命令来管理 Kaspersky Endpoint Security。

您可以通过运行以下命令查看管理命令的帮助：

`kesl-control --help <` 命令组前缀 `>`

其中 < 命令组前缀 > 接受以下值：

- -A：用于管理应用程序控制的命令
- -B：用于管理备份的命令
- -C：用于管理常规容器扫描设置的命令
- -D：用于管理设备控制的命令
- -E：用于管理应用程序事件的命令
- -F：用于管理防火墙的命令
- -H：用于管理受阻止设备的命令
- -L：用于管理授权许可密钥的命令
- -N：用于管理加密连接扫描设置的命令
- -R：用于管理 Kaspersky Endpoint Security 与Kaspersky Endpoint Detection and Response (KATA)以及Kaspersky Endpoint Detection and Response Optimum集成设置的命令
- -S：统计命令
- -T：用于管理应用程序任务和设置的命令
- -U：用于管理用户和角色的命令
- -V：在 Light Agent 模式下用于保护虚拟环境的应用程序命令
- -W：事件显示命令

用于管理应用程序任务和设置的命令

-T 前缀表示该命令属于用于管理应用程序设置和任务的命令组。

-C 前缀表示该命令属于用于管理容器扫描设置的命令组。

-N 前缀表示该命令属于用于管理安全连接扫描设置的命令组。

kesl-control --export-settings

此命令将所有应用程序设置输出到控制台或导出到配置文件。其中包括常规容器扫描设置、加密连接扫描设置、常规应用程序设置和任务设置。

命令语法

```
kesl-control [-T] --export-settings [--file <配置文件路径>] [--json]
```

参数和键

`--file <配置文件路径>` – 将保存应用程序设置的配置文件的完整路径。

指定 `--json`，则以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

kesl-control --import-settings

此命令从配置文件导入所有应用程序设置，包括常规容器扫描设置、加密连接扫描设置、常规应用程序设置和任务设置。

命令语法

```
kesl-control [-T] --import-settings --file <配置文件路径> [--json]
```

参数和键

`--file <配置文件路径>` – 用于将设置导入到应用程序的配置文件的完整路径。

指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json` 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

kesl-control --update-application

此命令安装已下载的应用程序模块更新。

> 仅当应用程序在标准模式下使用时才可执行。

命令语法

```
kesl-control [-T] --update-application
```

管理常规应用程序设置的命令

kesl-control --get-app-settings 命令

该命令将常规应用程序设置的当前值输出到控制台或配置文件。

命令语法

```
kesl-control [-T] --get-app-settings [--file <配置文件路径>] [--json]
```

参数和键

`--file <配置文件路径>` – 将显示应用程序常规设置的配置文件的路径。如果不指定 `--file` 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 `--json`，则以 JSON 格式输出设置。如果未指定 `--json` 键，则设置将以 INI 格式导入。

kesl-control --set-app-settings 命令

该命令使用命令选项或从配置文件导入设置来配置常规应用程序设置。

命令语法

通过命令选项定义设置：

```
kesl-control [-T] --set-app-settings <选项名称>=<选项值> [<选项名称>=<选项值>]
```

通过配置文件定义设置：

```
kesl-control [-T] --set-app-settings --file <配置文件路径> [--json]
```

参数和键

`<选项名称>=<选项值>`：常规应用程序设置的名称和值。

`--file <配置文件路径>` – 用于您想要从其将设置导入到应用程序的配置文件的完整路径。

指定 `--json`，则以 JSON 格式将配置文件中的设置导入应用程序。如果不指定 `--json` 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

管理任务设置的命令

kesl-control --get-settings

此命令将指定任务的当前设置输出到控制台或配置文件。

命令语法

```
kesl-control [-T] --get-settings <任务 ID/名称> [--file <配置文件路径>] [--json]
```

参数和键

<任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

--file <配置文件路径> – 将写入任务设置的配置文件的完整路径。如果不指定 --file 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 --json，则以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

kesl-control --set-settings

此命令通过命令选项或从配置文件导入设置来定义指定任务的设置。

命令语法

通过命令选项定义设置：

```
kesl-control [-T] --set-settings <任务名称/ID> <选项名称>=<选项值> [<选项名称>=<选项值>] [--add-path <路径>] [--del-path <路径>] [--add-exclusion <路径>] [--del-exclusion <路径>]
```

通过配置文件定义设置：

```
kesl-control [-T] --set-settings <任务名称/ID> --file <配置文件路径> [--json]
```

参数和键

<任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

<设置名称>=<设置值>是其中一项任务设置的名称和值。

--add-path <路径>添加要扫描对象的目录路径。

--del-path <路径>删除要扫描对象的目录路径。

--add-exclusion <路径>：添加要从扫描范围中排除的对象的目录路径。

--del-exclusion <路径>删除要排除的对象的目录路径。

--file <配置文件路径> – 将从中导入任务设置的配置文件的完整路径。

指定 --json 后，以 JSON 格式从配置文件中导入设置。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

kesl-control --set-to-default

该命令恢复指定任务的默认设置。

命令语法

```
kesl-control [-T] --set-settings <任务 ID/名称> --set-to-default
```

参数和键

<任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

kesl-control --get-schedule 命令

该命令将指定任务的当前计划输出到控制台或配置文件。

命令语法

```
kesl-control [-T] --get-schedule <任务 ID/名称> [--file <配置文件路径>] [--json]
```

参数和键

<任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

--file <配置文件路径> 是将输出任务运行计划设置的配置文件的路径。如果不指定 --file 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 --json，则以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

kesl-control --set-schedule 命令

该命令通过命令选项或从配置文件导入设置来定义指定任务的计划。

命令语法

通过命令选项定义设置：

```
kesl-control [-T] --set-schedule <任务 ID/名称> <选项名称>=<选项值> [<选项名称>=<选项值>]
```

通过配置文件定义设置：

```
kesl-control [-T] --set-schedule <任务 ID/名称> --file <配置文件路径> [--json]
```

参数和键

<任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

<设置名称>=<设置值> 是其中一项任务计划设置的名称和值。

--file <配置文件路径> – 将从中导入任务计划设置的配置文件的完整路径。

指定 --json 后，以 JSON 格式从配置文件中导入设置。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

管理任务的命令

kesl-control --get-task-list

此命令输出现有任务的列表。

命令语法

```
kesl-control [-T] --get-task-list [--json]
```

参数和键

指定 --json，则以 JSON 格式输出设置。

kesl-control --get-task-state

此命令输出指定任务的状态。

命令语法

```
kesl-control [-T] --get-task-state <任务 ID/名称> [--json]
```

参数和键

<任务 ID/名称>是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

指定 --json，则以 JSON 格式输出设置。

kesl-control --create-task

此命令使用默认设置或配置文件中指定的设置来创建指定类型的任务。

命令语法

使用默认设置创建任务：

```
kesl-control [-T] --create-task <任务名称> --type <任务类型>
```

使用配置文件中的设置创建任务：

```
kesl-control [-T] --create-task <任务名称> --type <任务类型> --file <配置文件路径> [--json]
```

参数和键

<任务名称>是您为新任务指定的名称。

< 任务类型 > 是所创建任务的类型的标识符。

--file < 配置文件路径 >：从中导入设置的配置文件的完整路径。

指定 --json 后，以 JSON 格式从配置文件中导入设置。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

kesl-control --delete-task

此命令删除一项任务。

命令语法

```
kesl-control [-T] --delete-task < 任务 ID/名称 >
```

参数和键

< 任务 ID/名称 > 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

kesl-control --start-task

该命令启动一项任务。

命令语法

```
kesl-control [-T] --start-task < 任务 ID/名称 > [-W] [--progress]
```

参数和键

< 任务 ID/名称 > 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

[-W]：启用当前事件输出。

[--progress]：显示任务进度。

kesl-control --stop-task

该命令停止一项任务。

命令语法

```
kesl-control [-T] --stop-task < 任务 ID/名称 > [-W]
```

参数和键

< 任务 ID/名称 > 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

[-W]：启用当前事件输出。

kesl-control --suspend-task

此命令暂停一项任务。

命令语法

```
kesl-control [-T] --suspend-task <任务 ID/名称>
```

参数和键

<任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

kesl-control --resume-task

此命令恢复一项任务。

命令语法

```
kesl-control [-T] --resume-task <任务 ID/名称>
```

参数和键

<任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

kesl-control --scan-file

此命令创建并运行一项自定义扫描任务。

命令语法

```
kesl-control [-T] --scan-file <路径> [--action <操作>]
```

参数和键

<路径>：要扫描的文件或目录的路径。您可以指定多个路径，用空格分隔。

`--action` <操作> 是应用程序将对受感染对象执行的操作。如果您未指定 `--action` 键，应用程序将执行推荐的操作。

kesl-control --scan-container

此命令创建并运行自定义容器或镜像扫描任务。

命令语法

```
kesl-control [-T] --scan-container <容量/镜像[:标签]>
```

参数和键

<容器/镜像[:标签]>：容器/镜像 ID/名称；您可以使用掩码来扫描多个对象。

您可以用 *（星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如：/dir/*/file 或 /dir/*/*/file。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如：/dir/**/file*/ 或 /dir/file**/。

** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

管理常规容器扫描设置的命令

The kesl-control --get-container-settings 命令

该命令将当前的常规容器扫描设置输出到控制台或配置文件。

命令语法

```
kesl-control [-C] --get-container-settings [--file <配置文件路径>] [--json]
```

参数和键

--file <配置文件路径>：将保存常规容器扫描设置的配置文件路径，如果不指定 --file 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 --json，则以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

The kesl-control --set-container-settings 命令

该命令使用命令选项或从配置文件导入设置来配置常规容器扫描设置。

命令语法

通过命令选项定义设置：

```
kesl-control [-C] --set-container-settings <设置名称>=<设置值> [<设置名称>=<设置值>]
```

通过配置文件定义设置：

```
kesl-control [-C] --set-container-settings --file <配置文件路径> [--json]
```

参数和键

<选项名称> = <选项值>：常规容器扫描设置的名称和值。

--file <配置文件路径>：配置文件的完整路径；此文件中的常规容器扫描设置将被导入应用程序。

指定 --json，则以 JSON 格式将配置文件中的设置导入应用程序。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

用于管理加密连接扫描设置的命令

-N 前缀表示该命令属于用于管理安全连接扫描设置的命令组。

kesl-control -N --query

该命令输出加密连接扫描的排除项列表：

- 用户添加的排除项列表；
- 应用程序添加的排除项列表；
- 从应用程序数据库收到的排除项列表。

命令语法

```
kesl-control -N --query user

kesl-control -N --query auto

kesl-control -N --query kl
```

kesl-control --clear-web-auto-excluded

此命令清除应用程序自动排除在扫描范围之外的域列表。

命令语法

```
kesl-control -N --clear-web-auto-excluded
```

kesl-control --get-net-settings

该命令将当前加密连接扫描设置输出到控制台或配置文件。

命令语法

```
kesl-control [-N] --get-net-settings [--file <配置文件路径>] [--json]
```

参数和键

--file <配置文件路径>：输出加密连接扫描设置的配置文件路径。如果不指定 --file 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 --json，则以 JSON 格式输出设置。如果未指定 --json 键，则设置将以 INI 格式导入。

kesl-control --set-net-settings

该命令使用命令选项或通过从配置文件导入设置来配置加密连接扫描设置。

命令语法

通过命令选项定义设置：

```
kesl-control [-N] --set-net-settings <选项名称>=<选项值> [<选项名称>=<选项值>]
```

通过配置文件定义设置：

```
kesl-control [-N] --set-net-settings --file <配置文件路径> [--json]
```

参数和键

<选项名称> = <选项值>：加密连接扫描选项的名称和值。

--file <配置文件路径>：从中导入加密连接扫描设置的配置文件的完整路径。

指定 --json，则以 JSON 格式将配置文件中的设置导入应用程序。如果不指定 --json 键，应用程序将尝试从 INI 文件导入设置。如果导入失败，将显示错误。

kesl-control --add-certificate

此命令将证书添加到受信任证书列表中。

命令语法

```
kesl-control [-N] -add-certificate <证书路径>
```

参数和键

<证书路径> 是要添加的证书文件（PEM 或 DER 格式）的路径。

kesl-control --remove-certificate

此命令将证书从受信任证书列表中移除。

命令语法

```
kesl-control [-N] --remove-certificate <证书主题>
```

kesl-control --list-certificates

此命令输出受信任证书的列表。

命令语法

```
kesl-control [-N] --list-certificates
```

统计命令

-S 前缀表示该命令属于统计命令组。

kesl-control --app-info

此命令输出有关应用程序的信息。

命令语法

```
kesl-control [-S] --app-info [--json]
```

参数和键

指定 `--json`，则以 JSON 格式输出设置。

kesl-control --omsinfo

此命令创建一个 JSON 文件，以便与 Microsoft Operations Management Suite 集成。

命令语法

```
kesl-control [-S] --omsinfo --file <文件名和路径>
```

用于显示事件的命令

kesl-control -W

该命令将启用当前应用程序事件的显示。该命令将返回事件的名称以及有关事件的其他信息。您可以使用该命令显示所有当前应用程序事件或仅显示与当前运行中任务相关的事件。

命令语法

```
kesl-control -W [--query "<筛选条件>"]
```

参数和键

<筛选条件>：一个或多个逻辑表达式，格式为<字段><比较运算符>'<值>'，结合逻辑运算符 and 来输出具体的当前事件。

用于管理应用程序事件的命令

-E：一个前缀，表示该命令属于用于管理应用程序事件的命令组。

kesl-control -E

此命令输出有关应用程序事件日志中所有事件的信息。您可以使用 `less` 命令在显示的事件列表中导航。

命令语法

```
kesl-control -E
```

kesl-control -E --query

此命令输出有关应用程序事件日志中的事件的信息。您可以使用 `less` 命令在显示的事件列表中导航。您可以使用筛选器来输出特定事件或将事件列表输出到文件。

命令语法

```
kesl-control -E --query "<筛选条件>" [--db <数据库文件>] [-n <数量>] --file <文件名和路径> [--json] [--reverse]
```

参数和键

<数据库文件> 是从中输出事件的事件日志数据库文件的完整路径。默认情况下，应用程序将有关事件的信息保存到数据库 /var/opt/kaspersky/kesl/private/storage/events.db。数据库的位置由 EventsStoragePath `global application setting` 决定。

<筛选条件>：一个或多个逻辑表达式，格式为 <字段><比较运算符>'<值>'，结合逻辑运算符 `and` 来限制结果。

<数量> – 要显示的所选内容中最新事件的数量（从所选内容的末尾开始计算的记录数量）。

`--file` <文件名和路径>：输出事件到文件的完整路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在具有指定名称的文件，则该文件将被覆盖。如果在磁盘上找不到指定目录，则不会创建文件。

如果不指定 `--file` 选项，事件列表将输出到控制台。

`--json`：以 JSON 格式输出事件。

`--reverse`：倒序显示事件（最新事件显示在顶部，最早事件显示在底部）。

用于管理授权许可密钥的命令

-L 前缀表示该命令属于用于管理授权许可密钥的命令组。

> 仅在标准模式下使用应用程序时，才能运行添加和删除授权许可密钥的命令。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则管理授权许可密钥的命令将终止并显示错误。您可以将应用程序作为 Kaspersky Security for Virtualization Light Agent 的一部分进行激活，因此无需单独激活该应用程序。

kesl-control --add-active-key

该命令可让您使用密钥文件或激活码向应用程序添加活动授权许可密钥。

您可以使用此命令添加活动的应用程序授权许可密钥以及活动的 EDR Optimum 授权许可密钥。您不需要在命令中指定密钥的类型。

命令语法

```
kesl-control [-L] --add-active-key <密钥文件路径>

kesl-control [-L] --add-active-key <激活码>
```

参数和键

<密钥文件的路径> – 密钥文件的路径。如果密钥文件位于当前目录中，则仅指定文件名就足够了。

<激活码> – 激活码。

示例：
从 /home/test/00000001.key 文件中添加一个密钥作为活动密钥：

```
kesl-control --add-active-key /home/test/00000001.key
```

kesl-control --add-reserve-key

该命令可让您使用密钥文件或激活码向应用程序添加备用授权许可密钥。

您可以使用此命令添加备用应用程序授权许可密钥以及备用 EDR Optimum 授权许可密钥。您不需要在命令中指定密钥的类型。

如果活动密钥尚未被添加到设备上的应用程序，则命令失败。

命令语法

```
kesl-control [-L] --add-reserve-key <密钥文件路径>

kesl-control [-L] --add-reserve-key <激活码>
```

参数和键

<密钥文件的路径> – 密钥文件的路径。如果密钥文件位于当前目录中，则仅指定文件名就足够了。

<激活码> – 激活码。

示例：
使用 /home/test/00000002.key 文件添加保留密钥：

```
kesl-control --add-reserve-key /home/test/00000002.key
```

kesl-control --remove-active-key

此命令可让您删除活动的授权许可密钥。

命令语法

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

参数和键

`--edr-optimum` – 删除活动的 EDR Optimum 授权许可密钥。如果您不指定`--edr-optimum`选项，Kaspersky Endpoint Security 的活动授权许可密钥将被删除。

kesl-control --remove-reserve-key

此命令可让您删除备用授权许可密钥。

命令语法

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

参数和键

`--edr-optimum` – 删除备用 EDR Optimum 授权许可密钥。如果您不指定`--edr-optimum`选项，Kaspersky Endpoint Security 的备用授权许可密钥将被删除。

kesl-control -L --query

`-L --query` 命令输出关于用于激活应用程序的授权许可以及当前正在使用的授权许可密钥的信息。

命令语法

```
kesl-control -L --query [--json]
```

参数和键

`--json`：以 JSON 格式输出数据。

kesl-control --load-mdr-blob

`--load-mdr-blob` 命令用于下载与 Kaspersky Managed Detection and Response 集成所需的 BLOB 配置文件。

命令语法

```
kesl-control [-L] --load-mdr-blob <MDR BLOB 配置文件路径>
```

kesl-control --remove-mdr-blob

`--remove-mdr-blob` 命令用于移除与 Kaspersky Managed Detection and Response 集成所需的 BLOB 配置文件。

命令语法

```
kesl-control [-L] --remove-mdr-blob
```

用于防火墙管理的命令

-F：前缀，表示该命令属于防火墙管理命令。

kesl-control --add-rule

此命令用于添加一个新的网络数据包规则。

命令语法

```
kesl-control [-F] --add-rule [--name <规则名称>] [--action <操作>] [--protocol <协议>]
[--direction <方向>] [--remote <远程地址>[:<端口范围>]] [--local <本地地址>[:<端口范围>]]
[--at <索引>]
```

参数和键

`--name <规则名称>` 是网络数据包规则的名称。

`--action <操作>` 是对网络数据包规则中指定的连接执行的操作。

`--protocol <协议>` 是要监控其网络活动的数据传输协议的类型。

`--direction <方向>` 是被监控的网络活动的方向。

`--remote <远程地址>[:<端口范围>]`：远程设备的网络地址。

`--local <本地地址>[:<端口范围>]`：已安装 Kaspersky Endpoint Security 的设备的网络地址。

`--at <索引>`：该规则在网络数据包规则列表中的编号。如果未指定 `--at` 键或其值大于列表中的规则数，则新规则会被添加到列表末尾。

命令中未指定值的参数被设置为其默认值。

kesl-control --del-rule

此命令用于删除规则列表中具有指定名称或索引的网络数据包规则。

命令语法

```
kesl-control -F --del-rule --name <规则名称>

kesl-control [-F] --del-rule --index <索引>
```

参数和键

`--name <规则名称>` 是网络数据包规则的名称。

`--index <索引>`：该规则在网络数据包规则列表中的编号。

kesl-control --move-rule

该命令用于更改网络数据包规则的执行优先级。

命令语法

`kesl-control [-F] --move-rule --name <规则名称> --at <索引>`

`kesl-control [-F] --move-rule --index <索引> --at <索引>`

参数和键

`--name <规则名称>` 是网络数据包规则的名称。

`--index < 索引 >`：该规则在网络数据包规则列表中的当前编号。

`--at < 索引 >`：该规则在网络数据包规则列表中的新编号。

kesl-control --add-zone

此命令用于将地址添加到网络区域。

命令语法

`kesl-control [-F] --add-zone --zone <区域> --address <地址>`

参数和键

`--zone <区域>` 是网络区域的预定义名称。

`--address <地址>` 是网络地址或子网。

kesl-control --del-zone

此命令用于从网络区域中移除一个地址。

命令语法

`kesl-control [-F] --del-zone --zone <区域> --address <地址>`

`kesl-control [-F] --del-zone --zone <区域> --index <地址索引>`

参数和键

`--zone <区域>` 是网络区域的预定义名称。

`--address <地址>` 是网络地址或子网。

`--index <地址索引>`：该地址在网络区域中地址的编号。

kesl-control -F --query

此命令用于显示使用 Kaspersky Endpoint Security 创建的防火墙规则。

命令语法

```
kesl-control -F --query
```

用于管理被阻止设备的命令

-H 前缀表示该命令属于用于管理被“反加密勒索”和“网络威胁保护”阻止的设备的命令组。

The kesl-control --get-blocked-hosts 命令

该命令可让您将被阻止设备的列表输出到控制台。

命令语法

```
kesl-control [-H] --get-blocked-hosts
```

The kesl-control --allow-hosts 命令

该命令可让您解除对被阻止设备的阻止。

命令语法

```
kesl-control [-H] --allow-hosts < 地址 >
```

参数和键

< 地址 > 是设备或子网的 IP 地址（IPv4/IPv6，包括缩写形式的地址）。您可以指定设备或子网的多个 IP 地址，用空格分隔。

用于管理设备控制的命令

-D 是一个前缀，表示该命令属于用于管理设备控制的命令组。

kesl-control --get-device-list

该命令向控制台输出安装在客户端设备上或连接到客户端设备的设备列表。

命令语法

```
kesl-control [-D] --get-device-list [--json]
```

参数和键

`--json`：以 JSON 格式输出数据。

用于管理应用程序控制的命令

-A 是一个前缀，表示该命令属于用于管理应用程序控制的命令组。

kesl-control --get-app-list

该命令输出由“清查”任务在客户端设备上找到的应用程序列表。

命令语法

```
kesl-control [-A] --get-app-list [--json]
```

参数和键

`--json`：以 JSON 格式输出数据。

kesl-control --get-categories

该命令输出已创建的应用程序控制类别列表。

命令语法

```
kesl-control [-A] --get-categories [--names <类别名称 1> <类别名称 2> ... <类别名称 N>]
[--file <配置文件路径>] [--json]
```

参数和键

<类别名称 1> <类别名称 2> ... <类别名称 N> – 您想要查看其信息的类别的名称。如果要查看有关多个类别的信息，请指定类别的名称，用空格分隔。

`--file` <配置文件路径> – 将输出设置的 JSON 配置文件的完整路径。

`--json`：以 JSON 格式输出数据。

kesl-control --set-categories

此命令可让您创建或编辑已创建的应用程序控制类别列表。

命令语法

```
kesl-control [-A] --set-categories [--names <类别名称 1> <类别名称 2> ... <类别名称 N>]
[--file <配置文件路径>]
```

参数和键

<类别名称 1> <类别名称 2> ... <类别名称 N> – 您想要更改其信息的类别的名称。如果要更改有关多个类别的信息，请指定类别的名称，用空格分隔。如果您不指定类别名称，该类别将被从列表中删除。

`--file` <配置文件路径> – 包含类别设置的配置文件的完整路径。

kesl-control --get-settings 21

该命令输出已创建的应用程序控制规则列表。

命令语法

```
kesl-control --get-settings 21 [--file <配置文件的路径>] [--json]
```

参数和键

`--file <配置文件路径>` – 将导出设置的配置文件的完整路径。

`--json`：以 JSON 格式输出数据。

kesl-control --set-settings 21

此命令可让您编辑已创建的应用程序类别和应用程序控制规则的列表。

命令语法

```
kesl-control --set-settings 21 [--file <配置文件的路径>] [--json]
```

参数和键

`--file <配置文件路径>` – 将从其导入设置的配置文件的完整路径。

`--json` – 从 JSON 文件导入数据。

kesl-control --set-to-default 21

此命令可让您删除应用程序类别和应用程序控制规则的列表。

命令语法

```
kesl-control --set-settings 21 --set-to-default
```

Web 控制管理命令

kesl-control --get-settings 26

此命令可让您显示指定的 Web 控制设置的列表。

命令语法

```
kesl-control --get-settings 26 [--file <配置文件的路径>] [--json]
```

参数和键

`--file <配置文件路径>` – 将导出设置的配置文件的完整路径。

--json：以 JSON 格式输出数据。

kesl-control --set-settings 26

此命令可让您编辑指定的 Web 控制设置的列表。

命令语法

```
kesl-control --set-settings 26 [--file <配置文件的路径>] [--json]
```

参数和键

--file <配置文件路径> – 将从其导入设置的配置文件的完整路径。

--json – 从 JSON 文件导入数据。

kesl-control --set-to-default 26

此命令可让您删除指定的设置并将 Web 控制设置重置为默认规则。

命令语法

```
kesl-control --set-settings 26 --set-to-default
```

用于管理备份的命令

-B 是一个前缀，表示该命令属于用于管理备份存储的命令组。

kesl-control --mass-remove

该命令从备份中删除部分或全部对象。

命令语法

删除全部对象：

```
kesl-control [-B] --mass-remove
```

删除符合筛选条件的对象：

```
kesl-control [-B] --mass-remove --query "<筛选条件>"
```

参数和键

<筛选条件>：一个或多个逻辑表达式，格式为 <字段><比较运算符>'<值>'，结合逻辑运算符 and 来限制结果。

kesl-control -B --query

此命令输出有关备份对象的信息。

命令语法

输出有关备份中所有对象的信息：

```
kesl-control -B --query [-n <数量>] [--json] [--reverse]
```

输出有关符合筛选条件的备份对象的信息：

```
kesl-control -B --query ["<筛选条件>"] [-n <数量>] [--json] [--reverse]
```

参数和键

<筛选条件>：一个或多个逻辑表达式，格式为 <字段><比较运算符>'<值>'，结合逻辑运算符 and 来限制结果。如果您不指定任何筛选条件，应用程序将显示备份中的所有对象的详细信息。

<数量>：要显示的最近对象的数量。如果您不指定 -n 开关，则会显示最后 30 个对象。指定 0 则显示所有对象。

--json：以 JSON 格式输出数据。

kesl-control --restore

此命令从备份中恢复对象。

命令语法

```
kesl-control [-B] --restore <对象 ID> [--file <文件名和路径>]
```

参数和键

<对象 ID>：备份对象的 ID。

--file <文件名和路径>：文件的新名称和保存到其中的目录的路径。如果不指定 --file 选项，则对象将以其原始名称和原始位置恢复。

用于管理用户和角色的命令

-U 前缀表示该命令属于用于管理用户和角色的命令组。

kesl-control --get-user-list

此命令输出用户和角色的列表。

命令语法

```
kesl-control [-U] --get-user-list
```

kesl-control --grant-role

此命令将角色分配给特定用户。

命令语法

```
kesl-control [-U] --grant-role <角色> <用户>
```

kesl-control --revoke-role

此命令撤销特定用户的角色。

命令语法

```
kesl-control [-U] --revoke-role <角色> <用户>
```

用于管理 Kaspersky Endpoint Detection and Response (KATA) 集成设置的命令

-R 是一个前缀，表示该命令属于用于管理与Kaspersky Endpoint Detection and Response (KATA)和Kaspersky Endpoint Detection and Response Optimum集成的设置的命令组。

kesl-control --add-kataedr-server-certificate

该命令将添加或替换先前添加的 KATA 服务器证书。

命令语法

```
kesl-control [-R] --add-kataedr-server-certificate <文件名和路径>
```

参数和键

<文件名和路径> 是包含服务器证书的文件的名称和路径。

kesl-control --remove-kataedr-server-certificate

该命令将删除 KATA 服务器证书。

命令语法

```
kesl-control [-R] --remove-kataedr-server-certificate
```

kesl-control --query-kataedr-server-certificate

该命令将输出有关 KATA 服务器证书的信息。

命令语法

```
kesl-control [-R] --query-kataedr-server-certificate
```

kesl-control --add-kataedr-client-certificate

该命令将添加或替换先前添加的用于保护与 KATA 服务器连接的客户端证书。

命令语法

```
kesl-control [-R] --add-kataedr-client-certificate < 文件名和路径 >
```

参数和键

< 文件名和路径 > 是包含客户端证书和私钥的加密容器（PFX 压缩文件）的名称和路径。

kesl-control --remove-kataedr-client-certificate

该命令将删除用于保护与 KATA 服务器连接的客户端证书。

命令语法

```
kesl-control [-R] --remove-kataedr-client-certificate
```

kesl-control --query-kataedr-client-certificate

该命令将输出有关客户端证书的信息。

命令语法

```
kesl-control [-R] --query-kataedr-client-certificate
```

kesl-control --isolation-stat

该命令将网络隔离的当前状态输出到控制台：已启用或已禁用。

命令语法

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

此命令可让您禁用设备的网络隔离。

命令语法

```
kesl-control [-R] --isolation-off
```

用于管理 Kaspersky Endpoint Detection and Response Optimum 集成设置的命令

-R 是一个前缀，表示该命令属于用于管理与Kaspersky Endpoint Detection and Response (KATA)和Kaspersky Endpoint Detection and Response Optimum集成的设置的命令组。

您可以使用常规应用程序设置中的UseEdrOptimum设置启用或禁用与 Kaspersky Endpoint Detection and Response Optimum 的集成。

kesl-control --isolation-stat

该命令将网络隔离的当前状态输出到控制台：已启用或已禁用。

命令语法

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

此命令可让您禁用设备的网络隔离。

命令语法

```
kesl-control [-R] --isolation-off
```

Light Agent 模式下用于保护虚拟环境的应用程序命令

-V：前缀，表示该命令属于在 Light Agent 模式下用于保护虚拟环境的 Kaspersky Endpoint Security 命令组（作为 Kaspersky Security for Virtualization Light Agent 的一部分）。

> 仅当在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境时，才能执行以下命令。

kesl-control --ksvla-info

该命令针对在 Light Agent 模式下使用应用程序保护虚拟环境输出有关信息：

命令语法

```
kesl-control --ksvla-info
```

kesl-control --viis-info

该命令针对 Light Agent（Kaspersky Endpoint Security 用作 Light Agent，作为 Kaspersky Security for Virtualization Light Agent 的一部分）连接到 Integration Server 输出有关信息：

命令语法

```
kesl-control --viis-info
```

kesl-control --svm-info

该命令针对 Light Agent（Kaspersky Endpoint Security 用作 Light Agent，作为 Kaspersky Security for Virtualization Light Agent 的一部分）连接到 SVM 输出有关信息：

命令语法

```
kesl-control --svm-info
```

附录 3.配置文件和默认应用程序设置

以下配置文件用于管理 Kaspersky Endpoint Security：

- 包含应用程序初始配置设置的配置文件：
  - autoinstall.ini 配置文件，通过 Kaspersky Security Center 安装应用程序时使用。
  - 通过命令行安装应用程序时使用的配置文件。
- 应用程序初始配置期间自动生成的预设配置文件，包含初始配置时设置的选项。这些设置在运行时应用。
- 您可以使用 Kaspersky Endpoint Security 管理命令创建的配置文件。这些配置文件可能包含任务设置和其他应用程序设置。您可以修改这些文件并导入到应用程序来修改相应选项。

编辑应用程序任务配置文件的规则

编辑配置文件时，请遵循以下规则：

- 在配置文件中指定所有必需的设置。您可以使用命令行指定单个任务设置，而无需文件。
- 如果设置属于特定部分，则仅在此部分中进行指定。您可以在一个部分中按任意顺序指定设置。
- 将各部分的名称括在方括号 [] 中。
- 以 < 设置名称 >=< 设置值 > 的格式输入各设置的值（设置名称与其值之间的空格不会被处理）。

  ```
  示例：
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  字符串值的第一个引号之前和最后一个引号之后的空格和制表符，以及未包含在引号中的字符串值的开始和结尾处的空格和制表符将忽略。
- 如果需要为一个设置指定多个值，请重复该设置，重复次数与您要指定的值的数量相同。

  ```
  示例：
  AreaMask.item_0000=*xml
  AreaMask.item_0001=*doc
  ```
- 输入以下类型设置的值时，区分大小写：
  - 扫描对象和排除对象的名称（掩码）。

- 威胁的名称（掩码）。

其余设置值不区分大小写。

- 按如下方式指定布尔设置值：`Yes/No`。
- 使用引号将包含空格字符的字符串值括起来（例如，文件和目录的名称及其路径、格式为“YYYY-MM-DD HH:MM:SS”的包含日期和时间的表达式）。

  您可以使用或不使用引号来输入其余值。

  ```
  示例：
  AreaDesc=" 扫描电子邮件数据库 "
  ```

  字符串开头或结尾的单引号将被视为错误。

预设配置文件

初始设置后，应用程序会创建以下配置文件：

- /var/opt/kaspersky/kesl/common/agreements.ini

  agreements.ini 配置文件包含与授权许可协议、隐私策略和卡巴斯基安全网络声明相关的设置。
- /var/opt/kaspersky/kesl/common/kesl.ini

  kesl.ini 配置文件包含下表中介绍的设置。

如有必要，您可以编辑这些文件中的设置值。

只有在技术支持专家的监督下并按照他们的说明，才能更改这些文件中的默认值。

kesl.ini 配置文件的设置

设置	描述	值
[General] 部分包含以下设置：		
`Locale`	Kaspersky Endpoint Security 发送到 Kaspersky Security Center 的文本（事件、通知、任务结果等）的本地化所使用的区域设置。 图形界面和应用程序命令行的区域设置取决于 `LANG` 环境变量的值。如果将 Kaspersky Endpoint Security 不支持的区域设置指定为 `LANG` 环境变量的值，则图形界面和命令行将以英语显示。	区域设置采用 RFC 3066 指 如果未指定 `Locale` 设置，置。如果应用程序无法确定不支持操作系统本地化，则 `en_US.utf8`。
`PackageType`	已安装的应用程序软件包的格式。 此设置不会影响应用程序的运行。在初始应用程序配置期间会自动填充该设置的值。	`rpm` – 安装 RPM 软件包。 `deb` – 安装 DEB 软件包。
`UseFanotify`	指示 fanotify 通知的使用。	`true/yes` – 操作系统支持

	此设置不会影响应用程序的运行。在初始应用程序配置期间会自动填充该设置的值。	false/no – 操作系统不支
KsvlaMode	Kaspersky Endpoint Security 使用模式。 此设置不会影响应用程序的运行。在初始应用程序配置期间会自动填充该设置的值。	true/yes – 在 Light Agent 护虚拟环境。 false/no – 在标准模式下
StartupTraces	启用在应用程序启动时生成跟踪文件。	true/yes – 在应用程序启 false/no（默认值）– 在应 踪文件。
RevealSensitiveInfoInTraces	显示跟踪文件中可能包含个人数据（例如，密码）的信息。	true/yes（默认值）– 显 能包含个人数据的信息。 false/no（默认值）– 不 个人数据的信息。
AsyncTraces	启用异步跟踪，其中信息被以异步方式记录到跟踪文件中。	true/yes – 启用异步跟踪 false/no （默认值）– 不
CoreDumps	当应用程序发生故障时，启用创建转储文件。	true/yes – 当应用程序崩 false/no（默认值）– 当应 储文件。
CoreDumpsPath	存储转储文件的目录的路径。	默认 值：/var/opt/kaspersky/ke 需要 root 特权才能访问默认
MinFreeDiskSpace	写入转储文件后剩余的最小磁盘存储空间（以 MB 为单位）。	默认值：300。
ScanMemoryLimit	应用程序的内存使用限制 (MB)。	默认值：8192。
MachineId	用户的唯一设备 ID。	在应用程序安装期间会自动
SocketPath	用于远程连接的套接字的路径，例如连接到图形界面和 kesl-control 实用程序。	默认值：/var/run/bl4contr
MaxInotifyWatches	对 /proc/sys/fs/inotify/max_user_watches 中文件和目录变化的订阅数限制（用户监视）。	默认值：300000。
MaxInotifyInstances	对单个用户的文件和目录变化的订阅数限制。	默认值：2048。
ExecEnvMax	应用程序从命令调用中捕获的环境变量数量。	默认值：50。
ExecArgMax	应用程序从 exec 调用中捕获的参数数量。	默认值：50。
DisableFileAvActions	在安装应用程序组件后禁用应用程序组件的清除和文件删除功能。 如果禁用了清除和文件删除功能并检测到威胁，则应用程序将仅通知用户检测到威胁，不会尝试清除或删除检测到威胁的文件。	true/yes：安装后启动应 删除功能。 false/no（默认值）：安 用清除和文件删除功能。

AdditionalDNSLookup	指示公共 DNS 的使用。 如果通过系统 DNS 访问服务器出错，则应用程序使用公共 DNS。这是更新应用程序数据库和维护设备安全所必需的。应用程序将按顺序使用以下公共 DNS： • Google Public DNS™ (8.8.8.8)。 • Cloudflare® DNS (1.1.1.1)。 • Alibaba Cloud® DNS (223.6.6.6)。 • Quad9® DNS (9.9.9.9)。 • CleanBrowsing (185.228.168.168)。	true/yes – 使用公共 DNS false/no（默认值）– 不使 基服务器。 应用程序的请求可能包含 IP 地址，因为应用程序与 TCP/UDP 连接。例如，在 查 Web 资源的证书需要此 使用公共 DNS 服务器，则 服务的隐私政策约束。如 序使用公共 DNS 服务器， 私有补丁。
[Network] 部分包含以下设置：		
WtpFwMark	iptables 规则中的一个标记，表示将流量转发到应用程序以供 Web 威胁防护组件处理。如果安装了应用程序的设备运行其他使用 TCP 数据包掩码第 9 位的软件并发生冲突，您可能需要更改此标记。	十进制值或带有 0x 前缀的 默认值：0x100。
NtpFwMark	iptables 规则中的一个标记，表示将流量转发到应用程序以供网络威胁防护组件处理。 如果安装了应用程序的设备运行其他使用 TCP 数据包掩码第 9 位的软件并发生冲突，您可能需要更改此标记。	十进制值或带有 0x 前缀的 默认值：0x200。
BypassFwMark	用于指示应用程序创建或扫描的数据包的标记，以便应用程序不会再次扫描这些数据包。	十进制值或带有 0x 前缀的 默认值：0x400。
BypassNFlogMark	一个标记，用于指示应用程序创建或扫描的软件包，防止它们被 iptable 实用程序记录。	十进制值或带有 0x 前缀的 默认值：0x800。
ProxyRouteTable	路由表编号。	默认值：101。
[Virtualization] 部分包含以下设置：		
ServerMode	在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境的受保护虚拟机的角色：服务器或工作站。 此设置不会影响应用程序的运行。在初始应用程序配置期间会自动填充该设置的值。	true/yes – 受保护虚拟机 false/no – 受保护虚拟机
VdiMode	在 Light Agent 模式下使用应用程序保护虚拟环境时启用 VDI 保护模式。 此设置不会影响应用程序的运行。在初始应用程序配置期间会自动填充该设置的值。	true/yes – 启用 VDI 保护 false/no – 禁用 VDI 保护
[Watchdog] 部分包含以下设置：		
TimeoutAfterHeadshot	等待 kesl 进程完成的最长时间，从 Watchdog 服务器向 kesl 进程发送	默认值：2 分钟。

	HEADSHOT 信号的一刻开始计算。	
`StartupTimeout`	等待应用程序启动的最长时间（以分钟为单位），此后 kesl 进程将重新启动。	默认值：3 分钟。
`TimeoutAfterKill`	等待受控 kesl 进程完成的最长时间，从 Watchdog 服务器向 kesl 进程发送 SIGKILL 信号的一刻开始计算。 如果 kesl 进程在此时间结束之前没有完成，将执行 --failed-kill 设置指定的操作。	默认值：2 天。
`PingInterval`	应用程序尝试向服务器发送 PONG 消息以响应收到的 PING 消息的时间间隔。	默认值：2000 ms。
`MaxRestartCount`	连续尝试启动应用程序失败的最大次数。	默认值：5。
`ActivityTimeout`	应用程序应向 Watchdog 服务器发送消息的最大时间间隔。 如果在此时间间隔内没有从应用程序收到消息，Watchdog 服务器将开始终止 kesl 进程的程序。	默认值：2 分钟。
`ConnectTimeout`	从 kesl 进程启动到应用程序与 Watchdog 服务器建立连接的最长时间。 如果应用程序在此时间间隔内没有建立连接，Watchdog 服务器将开始终止 kesl 进程的程序。	默认值：3 分钟。
`RegisterTimeout`	从应用程序连接到 Watchdog 服务器到服务器收到 REGISTER 消息的最长时间。	默认值：500 ms。
`TimeoutAfterShutdown`	等待 kesl 进程完成的最长时间，从 Watchdog 服务器向 kesl 进程发送 SHUTDOWN 信号的一刻开始计算。	默认值：2 分钟。
`MaxMemory`	kesl 进程的驻留内存的使用限制。 如果 kesl 进程使用的驻留内存超过此限制，Watchdog 服务器将开始终止 kesl 进程的程序。	`off` – 驻留集大小不受限制 < 值 `>%` – 介于 1 到 100 之间比。 < 值 `>MB` – 以 MB 为单位的 `lowest/`< 值 `>%/`< 值 `>MB/` MB 为单位的值之间的较小 `highest/`< 值 `>%/`< 值 `>MB` 以 MB 为单位的值之间的较 `auto` – 最多 50% 的可用内超过 16GB。 默认值：`auto`。
`MaxVirtualMemory`	kesl 进程的虚拟内存的使用限制。 如果 kesl 进程使用的虚拟内存超过此限制，Watchdog 服务器将开始终止 kesl 进程的程序。	`off`（默认值）– 虚拟内存 < 值 `>MB` – 以 MB 为单位的
`MaxSwapMemory`	kesl 进程的交换文件的大小限制。	`off`（默认值）– 交换文件

	如果 kesl 进程的交换文件超过此限制，Watchdog 服务器将开始终止 kesl 进程的程序。	< 值 >% – 介于 0 到 100 之间 比。 < 值 >MB – 以 MB 为单位的 lowest/< 值 >%/< 值 >MB/ MB 为单位的值之间的较小 highest/< 值 >%/< 值 >MB 以 MB 为单位的值之间的较
TrackProductCrashes	启用应用程序稳定性监控。 如果启用了应用程序稳定性监控，Watchdog 服务器会跟踪应用程序异常停止的次数。	true/yes – 启用应用程序 false/no （默认值）– 禁
ProductHealthLogFile	用于应用程序稳定性监控的文件路径。	默认 值：/var/opt/kaspersky/ke
WarnThreshold	应用程序在显示有关不稳定操作的通知之前必须经历指定次数异常停止的时间间隔（以秒为单位）。	默认值：3600 秒。
WarnAfter_#_crash	在显示有关应用程序运行不稳定的通知之前，需要应用程序异常停止的次数。	默认值：10。 如果值为 0，则不显示不稳
WarnRemovingThreshold	应用程序不稳定状态在此后被清除的时间间隔（以秒为单位）。	默认值：86400 秒。
默认情况下，配置文件中没有**[Environment]**部分。		
ExperimentalContainerdSupport	在运行容器监控组件时启用对 containerd 环境的支持。 默认情况下，配置文件中不存在此部分。如果要在容器监控组件运行时使用 containerd 环境，您需要手动添加 [Environment] 部分到配置文件 和其内的 ExperimentalContainerdSupport 设置。	true/yes – 在容器监控组 containerd 环境的支持。 false/no – 在容器监控组 containerd 环境的支持。

默认命令行任务设置

本节包含用于通过命令行管理 Kaspersky Endpoint Security 的所有预定义任务的默认选项。

"*回滚*"和"*授权许可*"任务没有设置。

File_Threat_Protection 任务（ID：1）的默认设置

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No
```

```
ScanPlainMail=No

SkipPlainTextFiles=No

TimeLimit=60

SizeLimit=0

FirstAction=Recommended

SecondAction=Block

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Scan_My_Computer 任务（ID：2）的默认设置

```
ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes
```

```
ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Scan_File 任务（ID：3）的默认设置

```
ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No
```

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Critical_Areas_Scan 任务（ID：4）的默认设置

```
ScanFiles=No

ScanBootSectors=Yes
```

```
ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Update 任务（ID：6）的默认设置

```
SourceType="KLServers"

UseKLServersWhenUnavailable=Yes

ApplicationUpdateMode=DownloadOnly

ConnectionTimeout=10
```

Backup 任务（ID：10）的默认设置

```
DaysToLive=90

BackupSizeLimit=0

BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

System_Integrity_Monitoring 任务（ID：11）的默认设置

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Firewall_Management 任务（ID：12）的默认设置

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Anti_Cryptor 任务（ID：13）的默认设置

```
ActionOnDetect=Block

BlockTime=30
```

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Web_Threat_Protection 任务（ID：14）的默认设置

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Device_Control 任务（ID：15）的默认设置

```
OperationMode=Block

[DeviceClass]

HardDrive=DependsOnBus

RemovableDrive=DependsOnBus

Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus

Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus
```

```
PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus

NetworkAdapter=DependsOnBus

BluetoothDevice=DependsOnBus

ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone

[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]
```

```
Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Removable_Drives_Scan 任务（ID：16）的默认设置

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Network_Threat_Protection 任务（ID：17）的默认设置

```
ActionOnDetect=Block

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Container_Scan 任务（ID：18）和 Custom_Container_Scan（ID：19）任务的默认设置

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No
```

```
TimeLimit=0

SizeLimit=0

FirstAction=Recommended

SecondAction=Skip

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*

DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes
```

> 您还可以将此配置文件中的选项用于自定义容器扫描任务。

Behavior_Detection 任务（ID：20）的默认设置

```
UseTrustedPrograms=No

TaskMode=Block
```

Application_Control 任务（ID：21）的默认设置

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Inventory_Scan 任务（ID：22）的默认设置

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

CreateGoldenImage=No

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

KATAEDR 任务（ID：24）的默认设置

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Web_Control 任务（ID：26）的默认设置

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

常规应用程序设置

常规应用程序设置定义了应用程序整体的运行以及各个功能的操作。

常规应用程序设置

设置	描述	值
SambaConfigPath	存储 Samba 配置文件的目录。需要 Samba 配置文件以确保可将 AllShared 或 Shared:SMB 值用于 Path 设置。	默认情况下，将在计算机上指目录。 默认值：/etc/samba/smb.con 更改此设置后，必须重新启动
NfsExportPath	存储 NFS 配置文件的目录。需要 NFS 配置文件以确保可将 AllShared 或 Shared:NFS 值用于 Path 设置。	默认情况下，将在计算机上指录。 默认值：/etc/exports。 更改此设置后，必须重新启动
TraceLevel	启用应用程序跟踪和跟踪文件的细节级别。	Detailed - 生成详细的跟踪文 MediumDetailed – 生成包含文件。 NotDetailed - 生成一个包含 None（默认值）- 不生成跟踪
TraceFolder	存储应用程序跟踪文件的目录。	默认值：/var/log/kaspersky/k 如果指定其他目录，请确保运 Security 的帐户对该目录具有才能访问默认跟踪文件目录。 更改此设置后，必须重新启动
TraceMaxFileCount	应用程序跟踪文件的最大数量。	1–10000 默认值：10。 更改此设置后，必须重新启动
TraceMaxFileSize	指定应用程序跟踪文件的最大大小（以兆字节为单位）。	1–1000 默认值：500。 更改此设置后，必须重新启动
BlockFilesGreaterMaxFileNamePath	阻止对其完整路径长度超过已定义设置值（以字节为单位指定）的文件的访问。如果扫描文件的完整路径长度超过此设置的值，则扫描任务会在扫描过程中跳过此文件。 此设置不适用于使用 fanotify 技术的操作系统。	4096–33554432 默认值：16384。 更改此设置的值后，需要重新

DetectOtherObjects	启用对入侵者可以用来破坏设备或数据的合法应用程序的检测。	Yes：启用对入侵者可以用来 程序的检测。 No（默认）：禁用对入侵者可 合法应用程序的检测。
NamespaceMonitoring	启用对命名空间和容器的扫描。 除非操作系统中安装了用于使用容器和命名空间的组件，否则应用程序不会扫描命名空间和容器。	Yes（默认值）- 启用命名空间 No - 禁用对命名空间和容器的
FileBlockDuringScan	启用文件操作拦截模式，在扫描期间阻止对文件的访问。文件操作拦截模式会影响文件威胁防护和设备控制组件。	Yes（默认值）– 在扫描期间阻 No – 在扫描期间允许访问文件 描异步完成。这种文件操作拦 小，但是如果文件在应用程序 （例如）在扫描过程中更改其 不会被消除或删除的风险。
UseKSN	启用卡巴斯基安全网络：	Basic – 在标准模式下使用卡 Extended – 在扩展模式下使用 No（默认值）– 禁用卡巴斯基
CloudMode	启用云模式。如果启用了KSN，则云模式可用。 如果您计划使用云模式，请确保在您的设备上可以使用KSN。 只有在标准模式下使用应用程序时，该设置才适用。	Yes – 启用 Kaspersky Endpoin 的恶意软件数据库的运行模式 No（默认值）– 使用完整版本 如果禁用 KSN，将自动禁用
UseMDR	启用托管检测与响应组件，以便与 Kaspersky Managed Detection and Response 集成。	Yes – 启用托管检测与响应组 No（默认值）– 禁用托管检测
UseProxy	允许 Kaspersky Endpoint Security 组件使用代理服务器。代理服务器可以用于与卡巴斯基安全网络和 Kaspersky Endpoint Detection and Response (KATA) 通信以激活应用程序，以及更新应用程序数据库和模块时。 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则不支持使用代理服务器连接卡巴斯基安全网络、SVM 和 Integration Server。	Yes - 允许使用代理服务器。 No（默认）- 禁用代理服务器 如果选择 Yes，则通过代理服 Detection and Response(KATA

ProxyServer	代理服务器选项的格式为：[<用户>[:<密码>]@]<代理服务器地址>[:<端口>]。 通过 HTTP 代理连接时，我们建议使用不用于登录其他系统的单独账户。HTTP 代理使用不安全的连接，账户可能会被入侵。	—
MaxEventsNumber	应用程序存储的事件的最大数量。如果超过指定的事件数，应用程序将删除最早的事件。	默认值：500000。 如果指定 0，则不保存事件。
LimitNumberOfScanFileTasks	非特权用户可以同时在设备上启动的自定义扫描任务的最大数量。此设置不限制具有 root 特权的用户可以启动的任务数。	0–4294967295 默认值：0。 如果指定为 0，则非特权用户 务。 如果在安装应用程序时安装了 LimitNumberOfScanFileTas
UseSyslog	启用将有关事件的信息记录到 syslog 访问 syslog 需要 root 特权。	Yes - 启用将有关事件的信息 No（默认值）- 禁用将有关事
EventsStoragePath	应用程序保存事件信息的数据库目录。 需要 root 权限才能访问默认事件数据库。	默认 值：/var/opt/kaspersky/kesl/
ExcludedMountPoint.item_#	要从扫描范围中排除的挂载点。排除适用于文件威胁防护、反加密勒索和容器监控组件以及可移动驱动器扫描任务的操作，还在 ODS 和 ContainerScan 扫描任务的操作中得到了配置。 您可以指定要从扫描中排除的多个挂载点。 必须以与 mount 命令输出中所显示的相同方式指定挂载点。 ExcludedMountPoint.item_# 设置默认未指定。	AllRemoteMounted – 从文件 和 NFS 协议挂载在设备上的所 Mounted:NFS – 从文件操作拦 载在设备上的所有远程目录。 Mounted:SMB – 从文件操作拦 载在计算机上的所有远程目录 Mounted:<文件系统类型> – 指定文件系统类型的所有已挂 /mnt – 从文件操作拦截中排除 录）中的对象。此目录用作可 <包含 /mnt/user* 或 /mn 件操作拦截中排除名称包含指

		您可以用 *（星号）字符来 码。 您可以指定单个 * 字符来表 字符前面的任意一组字符（ 如：/dir/*/file 或 /dir 您可以指定两个连续的 * 字 称中的任意一组字符（包括 如：/dir/**/file*/ 或 / ** 掩码在目录名称中只能使 如，/dir/**/**/file 是不 要排除挂载点 /dir，您需要 号）。 掩码 /dir/* 会排除 /dir 下 但不会排除 /dir 本身。掩码 级别下面的所有挂载点，但 可以使用单个 ? 字符表示文 一个字符。
MemScanExcludedProgramPath.item_#	从扫描中排除进程内存。 应用程序不扫描指定进程的内存。	< 进程的完整路径 > – 不扫描指 可以使用掩码指定路径。 您可以用 *（星号）字符来 码。 您可以指定单个 * 字符来表 字符前面的任意一组字符（ 如：/dir/*/file 或 /dir 您可以指定两个连续的 * 字 称中的任意一组字符（包括 如：/dir/**/file*/ 或 / ** 掩码在目录名称中只能使 如，/dir/**/**/file 是不 可以使用单个 ? 字符表示文 一个字符。
UseOnDemandCPULimit	启用 *ODS*、*ContainerScan* 和 *InventoryScan* 类型任务的 CPU 使用率限制。	Yes：启用 *ODS*、*ContainerS* 的 CPU 使用率限制。 No（默认）：禁用任务的 CPU
OnDemandCPULimit	运行 *ODS*、*ContainerScan* 和 *InventoryScan* 类型的任务时所有处理器核心上的最大利用率（百分比形式）。	10–100 默认值：100。
UseEdrOptimum	启用 EDR Optimum 组件以便与	Yes – 启用 EDR Optimum 组件

	Kaspersky Endpoint Detection and Response Optimum集成。	No（默认）– 禁用 EDR Optim

常规容器扫描设置

容器扫描常规设置在实时扫描命名空间和容器时使用。

常规容器和命名空间扫描设置

设置	描述	值
OnAccessContainerScanAction	检测到受感染对象时要对容器执行的操作。 在支持此功能的授权许可下使用应用程序时，此设置可用。 “文件威胁防护”任务设置在扫描容器内的对象时使用。检测到受感染对象时对容器执行的操作还取决于文件威胁防护任务设置（请参阅下表）。	StopContainerIfFailed（默认值）- 如果无法清除或删除受感染对象，则停止容器。 StopContainer — 检测到受感染对象时停止容器。 Skip — 检测到受感染的对象时，不对容器执行任何操作。
UseDocker	使用 Docker 环境。	Yes（默认值）— 使用 Docker 环境。 No — 不使用 Docker 环境。
DockerSocket	Docker 套接字路径或 URI（通用资源标识符）。	默认值：/var/run/docker.sock.
UseCrio	使用 CRI-O 环境。	Yes（默认值）— 使用 CRI-O 环境。 No — 不使用 CRI-O 环境。
CrioConfigFilePath	CRI-O 配置文件的路径。	默认值：/etc/crio/crio.conf。
UsePodman	使用 Podman 实用程序。	Yes（默认值）— 使用 Podman 实用程序。 No — 不使用 Podman 实用程序。
PodmanBinaryPath	Podman 实用程序可执行文件的路径。	默认值：/usr/bin/podman。
PodmanRootFolder	容器存储的根目录的路径。	默认值：/var/lib/containers/storage。
UseRunc	使用 runc 实用程序。	Yes（默认值）— 使用 runc 实用程序。 No：不使用 runc 实用程序。
RuncBinaryPath	runc 实用程序可执行文件的路径。	默认值：/usr/bin/runc。
RuncRootFolder	容器状态存储的根目录的路径。	默认值：/run/runc。

检测到感染对象后对容器执行的操作可能因文件威胁防护任务的FirstAction和SecondAction参数的指定值而异。

对容器执行的操作与对受感染对象执行的指定操作之间的关系

FirstAction / SecondAction 设置的值	选择 StopContainerIfFailed 操作时对容器执行的操作
Disinfect	如果对受感染物体的清除失败，停止容器。
Remove	如果删除受感染的对象失败，停止容器。

加密连接扫描设置

加密连接扫描设置

设置	描述	值
EncryptedConnectionsScan	启用或禁用加密流量扫描。 对于 FTP 协议，默认情况下禁用安全连接扫描。	Yes（默认值）—启用安全连接扫描。 No：禁用加密连接扫描。应用程序不会解密已经加密的流量。
EncryptedConnectionsScanErrorAction	指定在网站上发生安全连接扫描错误时要执行的操作。	AddToAutoExclusions（默认值）- 将发生错误的域添加到存在扫描错误的域列表中。应用程序在访问此域时不会监视加密的网络流量。 Disconnect - 阻止网络连接。
CertificateVerificationPolicy	指定 Kaspersky Endpoint Security 检查证书的方式。 如果证书是自签名的，应用程序将不执行额外的验证。	FullCheck（默认值）- 应用程序使用互联网检查和下载验证证书所需的缺失链。 LocalCheck - 应用程序不使用互联网来验证证书。
UntrustedCertificateAction	检测到未确认的证书时要执行的操作。	Allow（默认值）- 允许在使用非可信证书访问域时建立网络连接。 Block - 阻止在使用非可信证书访问域时建立的网络连接。
ManageExclusions	扫描加密流量时使用排除项。	Yes：不扫描 [Exclusions.item_#] 下指定的网站（见下文）。 No（默认值）- 扫描所有网站。
MonitorNetworkPorts	指定 Kaspersky Endpoint Security 监控网络端口的方式。	Selected（默认值）- 仅监视在 [NetworkPorts.item_#] 部分中指定的网络端口（见下文）。 All - 监控所有网络端口。 指定此值可能会大大增加操作系统负载。

[Exclusions.item_#] 部分包含排除在扫描范围之外的域。应用程序不会扫描访问指定域时建立的安全连接。		
DomainName	指定域名。您可以使用掩码指定域。	默认值为未定义。
[NetworkPorts.item_#] 部分包含由应用程序监视的网络端口。		
PortName	网络端口描述。	默认值为未定义。
Port	应用程序要监控的网络端口号。	1 – 65535 默认值为未定义。

任务计划设置

任务启动计划设置

设置	描述	值
RuleType	任务启动计划。	Once：运行一次任务。 Monthly：每月在指定的日期和时间运行任务。 Weekly：每周在指定的日期和时间运行任务。 Daily：按照指定的天数间隔定期运行任务。 Hourly：从指定的日期和时间开始，按照指定的小时间隔定期运行任务。 Minutely：从指定的时间开始，按照指定的分钟间隔定期运行任务。 Manual – 手动启动任务。 PS - 启动应用程序后启动任务。 BR - 在应用程序数据库更新后启动任务。
StartTime	任务开始日期和时间。 如果 RuleType 选项设置为 Once、Monthly、Weekly、Daily、Hourly 或 Minutely 中的一项，则 StartTime 是必需选项。	[< 年 >/< 月 >/< 日 >] [时]:[分]:[秒]；[< 一个月中的第几天 >|< 一周中的第几天 >]；[< 启动周期 >]。
RandomInterval	从 0 到指定值（以分钟为单位）的时间间隔，将添加到任务开始时间以避免同时启动任务。	
RunMissedStartRules	在应用程序启动后运行漏掉的任务。	Yes：启用在应用程序启动后运行漏掉的任务。 No：禁用在应用程序启动后运行漏掉的任务。

附录 4.命令行返回代码

Kaspersky Endpoint Security 具有以下命令行返回码：

0 – 命令/任务成功完成。

1 – 命令参数中存在一般错误。

2 – 所传递的应用程序设置中存在错误。

64 — Kaspersky Endpoint Security 未运行。

66 – 未下载应用程序数据库（仅由 `kesl-control --app-info` 命令使用）。

67 – 由于网络问题，激活 2.0 终止并显示错误。

68 – 命令无法执行，因为应用程序正按照某项策略运行。

69 – 应用程序位于 Amazon 付费 Ami 基础设施中。

70 – 尝试启动正在运行的任务、删除正在运行的任务、更改正在运行的任务的设置、停止已停止的任务、暂停已暂停的任务或继续正在运行的任务。

71 – 尚未接受卡巴斯基安全网络声明。

72 — 在执行"自定义扫描"或"自定义容器扫描"任务期间检测到威胁。

73 — 尝试指定影响应用程序操作的"应用程序控制"任务设置，但未使用 `--accept` 标志确认这些设置。

74 – 更新后必须重新启动 Kaspersky Endpoint Security。

75 – 必须重启设备。

76 — 禁止连接，因为只有具有 root 权限的用户才拥有指定路径的写访问权限。

77 — 指定的授权许可密钥已在设备上使用。

128 – 未知错误。

65 – 所有其他错误。

附录 5.配置与 Kaspersky Anti-Virus for Linux Mail Server 的交互

要配置 Kaspersky Endpoint Security 和 Kaspersky Anti-Virus for Linux Mail Server 的联合操作：

1. 使用以下命令将文件威胁防护任务设置保存到配置文件中：
   `kesl-control --get-settings 1 --file <文件的完整路径>`
2. 打开创建的配置文件进行编辑。
3. 在创建的文件中添加以下部分：
   `[ExcludedFromScanScope.item_<项目号>]`
   `Path=/var/opt/kaspersky/klms`

4. 对与 Kaspersky Anti-Virus for Linux Mail Server 集成的所有邮件代理重复上面指定的部分。

5. 要从扫描中排除过滤器的临时目录和 Kaspersky Anti-Virus for Linux Mail Server，请将以下部分添加到创建的文件中：

   ```
   [ExcludedFromScanScope.item_<项目号>]
   Path=/tmp/klmstmp
   ```

6. 将更改保存在配置文件中。

7. 使用以下命令将设置从配置文件导入到文件威胁防护任务：

   ```
   kesl-control --set-settings 1 --file <文件的完整路径>
   ```

有关 Kaspersky Endpoint Security 的信息来源

知识库中的 Kaspersky Endpoint Security 页面

*知识库*是卡巴斯基技术支持网站的一部分。

在知识库中的 Kaspersky Endpoint Security 页面上，您可以阅读到提供有用信息的文章、推荐以及有关如何购买、安装和使用应用程序的常见问题的答案。

知识库中的文章可能提供关于 Kaspersky Endpoint Security 和其他卡巴斯基应用程序的问题的答案。知识库中的文章也可能包含技术支持新闻。

在论坛上讨论卡巴斯基应用程序

如果您的问题不需要立即回答，您可以在论坛中与卡巴斯基专家和其他用户一起进行讨论。

在论坛上可以查看讨论主题、发表评论和创建新的讨论主题。

术语表

Integration Server

Kaspersky Endpoint Security for Virtualization Light Agent 组件。在 Kaspersky Endpoint Security 组件和虚拟基础架构之间交互。

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent 组件。已安装到每个需要保护的虚拟机。

SIEM 系统

*SIEM（安全信息和事件管理）*系统是管理组织安全系统内的信息和事件的解决方案。

SVM

安全虚拟机 – 安装了扫描服务器服务（保护虚拟机，即 Kaspersky Endpoint Security for Virtualization Light Agent 的组件）的特殊虚拟机。

代理服务器

允许用户对其他网络服务发起间接请求的一种计算机网络服务。首先，用户连接到代理服务器并请求获取位于另一台服务器上的资源（例如文件）。然后，代理服务器要么连接到指定的服务器并从中获取该资源，要么从其自己的缓存中（如果代理具有自己的缓存）返回该资源。在某些情况下，出于某种目的，代理服务器可能会修改用户的请求或服务器的响应。

卡巴斯基更新服务器

卡巴斯基 HTTP 和 FTP 服务器，卡巴斯基应用程序从中下载数据库和应用程序模块更新。

受信任设备

在受信任设备设置下列出，可供用户随时完整访问的设备。

受感染的对象

包含与某个已知恶意软件代码部分完全匹配的部分代码的对象。卡巴斯基专家不推荐访问此类对象。

启动对象

计算机上安装的操作系统和软件正常启动和运行所需的一组应用程序。每次启动操作系统时，都会执行这些对象。有些病毒专门感染此类对象，例如，可能会导致操作系统无法启动。

备用密钥

证明具有使用应用程序的权限但当前未使用的密钥。

对象清除

处理已感染对象的一种方法，清除后可完全或部分恢复数据。并非所有已感染对象都可以清除。

应用程序数据库

包含在数据库发布之时，卡巴斯基已知的计算机安全威胁信息的数据库。应用程序数据库由 Kaspersky 专家创建并且每小时都会更新。

应用程序激活

将应用程序切换到全功能模式。应用程序激活在应用程序安装期间或之后执行。您需要提供激活码或密钥文件才能激活应用程序。

应用程序设置

对所有任务类型通用并且管辖应用程序总体操作情况的应用程序设置，例如应用程序性能设置、报告设置和备份设置。

恶意网址数据库

其内容可能被视为危险的 Web 资源列表。该列表由卡巴斯基专家创建；它会定期更新，并包含在卡巴斯基应用程序的分发包中。

授权许可

根据最终用户授权许可协议授予的在有限时间内使用本应用程序的权限。

授权许可证书

您从卡巴斯基收到的文档，其中含有密钥文件或激活码。此文档包含有关所提供授权许可的信息。

排除

*排除项*是从卡巴斯基应用程序扫描中排除的对象。您可以根据病毒百科全书的分类，按名称从扫描文件中排除某些格式、文件掩码、特定区域（例如文件夹或应用程序）、应用程序进程或对象。可以为每个任务分配一组排除项。

文件掩码

使用通配符表示文件名。文件掩码中使用的标准通配符为 * 和 ?，其中 * 代表任意数量的任意字符，? 代表单个任意字符。

活动密钥

应用程序当前使用的密钥。

活动策略

应用程序当前用于控制数据泄漏的策略。应用程序可以同时使用多个策略。

策略

在管理组内，策略决定应用程序的设置并管理对设备上安装的应用程序的配置的访问。必须为每个应用程序创建单独策略。您可以在每个管理组内为设备上安装的应用程序创建无限数量的不同策略，但在一个管理组内一次只能对每个应用程序应用一个策略。

管理服务器

Kaspersky Security Center 的一个组件，可集中存储公司网络内安装的所有卡巴斯基应用程序的信息。它也可用于管理这些应用程序。

管理组

根据设备执行的功能和安装在其上的卡巴斯基应用程序集合，在 Kaspersky Security Center 内分组在一起的一组设备。由于设备组可以作为单个实体进行管理，因此我们对设备进行分组以便简化管理。一个管理组可以包含其他组。对于管理组中已安装的每个应用程序，都可以创建组策略和组任务。

组任务

分配给管理组并在此管理组中包括的所有受管理设备上执行的任务。

组策略

请参阅策略。

网络钓鱼网址数据库

由卡巴斯基专家确定为网络钓鱼的 Web 资源地址列表。该数据库会定期更新，并包含在卡巴斯基应用程序的分发包中。

订阅

以选定设置（到期日期和设备数量）启用应用程序。您可以暂停或继续订阅、自动续订或取消订阅。

误报

卡巴斯基应用程序将非感染对象认为是受感染的情况，因为该对象的代码类似于病毒的代码。

有关第三方代码信息

有关第三方代码信息包含在文件 legal_notices.txt 中，该文件位于应用程序安装文件夹中。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

Amazon 是 Amazon.com, Inc. 或其子公司的商标。

FireWire 是 Apple Inc. 的商标。

Arm 是 Arm Limited（或其子公司）在美国和/或其他地区的注册商标。

蓝牙 (Bluetooth) 文字、商标和徽标归 Bluetooth SIG, Inc. 所有。

Ubuntu 和 LTS 是 Canonical Ltd. 的注册商标。

Citrix、XenServer 是 Citrix Systems, Inc. 和/或其一个或多个子公司的商标，可能在美国专利及商标局以及其他国家/地区注册。

Cloudflare、Cloudflare 徽标和 Cloudflare Workers 是 Cloudflare, Inc. 在美国和其他司法管辖区的商标和/或注册商标。

Docker 和 Docker 徽标是 Docker, Inc. 在美国和/或其他国家/地区的商标或注册商标。Docker, Inc. 和其他各方也可能拥有本文中使用的其他术语的商标权。

Chrome、Google Public DNS 是 Google LLC 的商标。

HUAWEI、EulerOS 和 FusionSphere 是华为技术有限公司的商标。

Intel、Core 是 Intel Corporation 在美国和/或其他国家/地区的商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft、Active Directory、Hyper-V、Outlook、Visual C++ 和 Windows 是 Microsoft 公司集团的商标。

OpenStack 是 OpenStack Foundation 在美国和其他国家/地区的注册商标。

Oracle 和 JavaScript 是 Oracle 和/或其附属公司的注册商标。

Red Hat、Red Hat Enterprise Linux 和 CentOS 是 Red Hat Inc. 或其子公司在美国和其他国家/地区的商标或注册商标。

Debian 是 Public Interest, Inc. 的软件注册商标

SUSE 是 SUSE LLC 在美国和其他国家/地区的注册商标。

VMware、VMware NSX、VMware NSX Manager、VMware Tools、VMware vCenter、VMware vSphere 是 VMware, Inc. 在美国和其他司法管辖区的商标或注册商标。

UNIX 是在美国和其他国家/地区的注册商标，通过 X/Open Company Limited 独家授权。