kaspersky

# Kaspersky Endpoint Security for Linux 12.5.0

© 2026 AO Kaspersky Lab

# 目录


Kaspersky Endpoint Security for Linux
关于应用程序
主要功能
版本 12.5 的新功能
已修复问题
硬件和软件要求
分发包
与其他应用程序的兼容性
卡巴斯基解决方案之间的功能比较
部署和初始配置
模式和部署方案
准备应用程序安装环境
选择系统事件拦截机制
准备分发包
Kaspersky Security Center 中的准备操作
使用 Kaspersky Security Center 安装应用程序
使用命令行安装应用程序
某些操作系统中安装后的其他配置步骤
使用快速安装脚本迁移到 Kaspersky Security Center Linux 的方案
从先前的版本更新应用程序
更新 Kaspersky Endpoint Security 管理插件
升级后的应用程序设置
卸载应用程序
使用应用程序
授权许可
如何切换到其他卡巴斯基解决方案
管理授权许可密钥
查看授权许可密钥信息
应用程序的管理界面
使用 Kaspersky Security Center 管理应用程序
Kaspersky Security Center 策略
策略管理
导出和导入策略设置
在 Kaspersky Security Center 中创建的 Kaspersky Endpoint Security 任务
登录和注销 Web Console 和云控制台
使用命令行管理应用程序
Kaspersky Endpoint Security 本地任务
编辑任务设置
配置任务计划
管理常规应用程序设置
使用筛选器来限制查询结果
导出和导入应用程序设置
通过图形界面管理应用程序

保护状态监控
- 实时保护状态
- 事件和报告
  - 将事件日志配置到操作系统日志中
  - 配置应用程序事件日志设置
  - 查看应用程序事件
  - 查看报告
- 获取系统性能指标
- 应用程序稳定性监控
- 应用程序组件完整性检查

应用程序访问控制
- 预定义角色
- 如何分配或撤销用户角色
- Kaspersky Security Center 中的 RBAC 功能区域

受保护设备典型角色的建议

更新应用程序数据库和模块
- 如何选择更新源和更新分发方案
- 如何配置数据库更新任务
- 如何使用卡巴斯基更新实用程序进行更新
- 如何回滚数据库和应用程序模块的更新

主机威胁防护
- 文件威胁防护
  - 如何创建保护范围
  - 如何选择检测到文件威胁后的操作
  - 什么是文件扫描的智能模式
  - 如何优化文件扫描
  - 扫描符号链接和硬链接的特殊注意事项
- 恶意软件扫描
  - 如何创建扫描范围
  - 如何配置扫描计划
  - 如何扫描单个文件或目录
  - 如何优化自定义扫描任务
- 关键区域扫描
- 容器扫描
  - 如何配置与容器管理工具的集成
  - 如何为容器和镜像创建按需扫描范围
  - 如何优化容器扫描
  - 如何选择检测到受感染对象时要对容器执行的操作
  - 如何运行容器和镜像的自定义扫描
- 可移动驱动器扫描
- 行为检测
- 漏洞利用防御
- 反加密
  - 如何选择检测到恶意加密时的操作
  - 如何创建保护范围

- BadUSB 攻击防护
  - 如何配置 USB 设备授权
  - 如何允许使用屏幕键盘连接 USB 设备
  - 如何允许使用条形码扫描器连接 USB 设备
- 通信和 Web 保护
  - 邮件威胁防护
    - 检测到邮件威胁时该怎么办
    - 如何优化邮件附件扫描
    - 电子邮件附件过滤器的用途
  - Web 威胁防护
    - 如何选择检测到 Web 威胁时的操作
    - 什么是反钓鱼
  - 网络威胁防护
    - 如何选择检测到网络威胁时的操作
    - 如何管理被阻止的设备
  - 防火墙管理
    - 如何创建网络包规则
    - 网络包规则使用示例
    - 如何将 IP 地址添加到网络区域：公共、本地、受信任
    - 什么是动态规则
    - 如何创建连接到 Kaspersky Security Center 的规则
- 安全控制
  - 设备控制
    - 如何在命令行中管理受信任设备列表
    - 如何配置设备访问模式
    - 如何配置设备访问规则
    - 如何配置设备控制消息模板
    - 授予设备临时访问权限
  - Web 控制
    - 如何创建 Web 资源访问规则
    - 如何修改 Web 控制消息模板
    - 创建 Web 资源地址掩码的规则
  - 应用程序控制
    - 应用程序清查
    - 如何配置应用程序控制的操作模式
    - 创建应用程序类别
    - 黄金镜像
    - 关于应用程序控制规则
    - 应用程序控制规则测试模式
  - 系统完整性监控
    - 实时系统完整性监控
    - 系统完整性检查
- 信任区域
  - 如何添加保护排除项
  - 如何添加受信任网址
  - 如何添加计算机的受信任 IP 地址
  - 如何选择受监控的网络端口

- 如何将证书添加到受信任根证书列表
- 如何添加受信任域
- 如何排除挂载点
- 如何添加受信任的应用程序
- 如何添加受信任设备

常规设置

- 检测设置
- 卡巴斯基安全网络
  - 如何启用或禁用卡巴斯基安全网络
  - 什么是应用程序的云模式
  - KSN 代理的用途是什么
- 配置数据传输到 Kaspersky Security Center 存储
- 如何配置应用程序启动
- 配置任务管理的权限
- 密码保护
  - 关于自定义权限
  - 默认用户权限
- 性能设置
- 网络设置
  - 如何管理代理设置
  - 应用程序如何拦截流量
  - 如何配置证书验证策略
  - 如何配置受监控的端口
  - 使用操作系统工具排除流量拦截
- 文件操作拦截
- 配置系统事件拦截
- 管理附加遥测设置
- 备份

防御高级威胁和定向攻击

- 响应操作
  - 搜索入侵指标
  - 网络隔离
    - 在 Web Console 中手动启用或禁用设备的网络隔离
    - 配置自动网络隔离的持续时间
    - 手动配置网络隔离
    - 在 Web Console 中配置网络隔离排除项
  - 隔离文件
  - 从设备接收文件
  - 从设备删除文件
  - 启动进程
  - 终止进程
  - 对象的执行防护
  - 管理隔离区
- Endpoint Detection and Response Optimum
  - 如何启用 EDR Optimum 集成
  - 如何验证 EDR Optimum 集成是否正常运行
  - Cloud Sandbox

Endpoint Detection and Response Expert (on-premises)
如何准备用于与 EDR Expert (on-premises) 正确集成的参考镜像
如何配置 EDR Expert (on-premises) 集成
如何验证 EDR Expert (on-premises) 集成已启动并正在运行
Endpoint Detection and Response Expert (cloud)
如何配置内置代理与 EDR Expert (cloud) 的集成
如何优化 EDR Expert (cloud) 遥测传输
如何配置 EDR Expert (cloud) 遥测排除项
如何导出或导入 EDR Expert (cloud) 事件过滤器
Kaspersky Anti Targeted Attack Platform
如何配置 EDR (KATA) 集成
如何配置 NDR (KATA) 集成
如何验证 KATA 整合是否已启动并正常运行
Sandbox
如何配置 Sandbox 整合
如何验证 Sandbox 整合是否已启动并运行
如何手动将文件发送到沙盒
Kaspersky Managed Detection and Response
有关创建用于与 MDR 正确集成的参考镜像的建议
上传 KPSN 配置文件
如何配置 MDR 集成
如何验证 MDR 集成是否已启用
Kaspersky Unified Monitoring and Analysis Platform
如何配置 KUMA 集成
如何验证 KUMA 整合是否已启动并正常运行
虚拟环境保护
如何配置 SVM 发现
Light Agent 如何选择 SVM
如何平衡 SVM 之间的 Light Agent 连接
保护 Light Agent 与 SVM 之间的连接
如何查看 Light Agent 的状态
最佳实践
优化应用程序的资源消耗
设备端应用程序性能分析
针对文件威胁防护任务和扫描任务的建议
针对 Web 威胁防护任务和网络威胁防护任务的建议。
行为检测建议
与卡巴斯基解决方案的互操作性
Kaspersky Security Center Linux
Network Detection and Response (KATA)
Kaspersky Unified Monitoring and Analysis Platform
应用程序组件参考
用于管理 Kaspersky Endpoint Security 的命令
用于管理授权许可密钥的命令
用于管理用户和角色的命令

- 管理应用程序任务和设置
  - 管理常规应用程序设置的命令
  - 管理任务设置的命令
  - 管理任务的命令
  - 管理常规容器扫描设置的命令
  - 用于管理网络流量扫描设置的命令
- 状态和保护监控
  - 统计命令
  - 用于显示事件的命令
  - 用于管理应用程序事件的命令
  - 用于管理系统性能指标的命令
- 安全控制
  - 用于管理设备控制的命令
  - 用于管理应用程序控制的命令
  - Web 控制管理命令
- 网络连接保护
  - 用于管理被阻止设备的命令
  - 用于防火墙管理的命令
- 防御高级威胁和定向攻击
  - 用于管理隔离区的命令
  - 用于管理 EDR Expert (on-premises) 组件的命令
  - 用于管理 EDR Expert (cloud) 组件的命令
  - 用于管理 NDR (KATA) 组件的命令
  - 用于管理设备网络隔离的命令
  - 用于管理 KUMA 集成设置的命令
  - 用于管理 Sandbox 集成设置的命令
  - 用于管理 IOC 扫描的命令
- Light Agent 模式下的应用程序命令

应用程序命令行选项

- 更新任务
- 主机威胁防护
  - 文件威胁防护任务
  - 优化网络目录扫描
  - 恶意软件扫描
    - 恶意软件扫描任务
    - 自定义扫描任务
  - 关键区域扫描任务
  - “可移动驱动器扫描”任务
  - 容器扫描
    - 容器扫描设置
    - 容器扫描任务
    - 与 Jenkins 整合
  - 反加密勒索任务
  - 行为检测任务
  - 漏洞利用防御

- 使用卡巴斯基安全网络
  - 连接到卡巴斯基安全网络
  - 启用或禁用云模式
- BadUSB 攻击防护任务

通信和 Web 保护
- Web 威胁防护任务
- 扫描网络流量
  - 查看和编辑网络流量扫描设置
  - 查看加密连接扫描的排除项
  - 管理受信任根证书列表
  - 配置和查看流量拦截排除
- 网络威胁防护任务
- 防火墙管理
  - 配置网络包规则列表
  - 配置网络区域

安全控制
- 设备控制任务
- Web 控制
  - Web 控制任务
  - 查看和编辑 Web 控制设置
- 应用程序控制
  - 应用程序控制任务
  - 创建和编辑类别列表
  - 查看类别列表
  - 配置应用程序控制规则列表
- 配置清查
  - 清查任务
  - 查看检测到的应用程序列表
- 系统完整性监控任务
- 系统完整性检查任务

防御高级威胁和定向攻击
- Kaspersky Endpoint Detection and Response Expert (on-premises) 集成
  - Kaspersky Endpoint Detection and Response Expert (on-premises) 整合设置
  - 管理用于连接到 OSMP EDR Expert (on-premises) 服务器的证书
- Kaspersky Endpoint Detection and Response Expert (cloud) 集成
  - Kaspersky Endpoint Detection and Response Expert (cloud) 集成设置
  - 管理 OSMP EDR Expert 服务器 (cloud) 连接证书
- Kaspersky Endpoint Detection and Response (KATA) 整合
  - Kaspersky Endpoint Detection and Response (KATA) 集成设置
  - 管理用于连接到 Expert 服务器的证书
- Kaspersky Network Detection and Response (KATA) 整合
  - Kaspersky Network Detection and Response (KATA) 集成设置
  - 管理用于连接到 NDR 服务器的证书
- Sandbox 集成
  - Sandbox 集成设置
  - 管理用于连接到 Sandbox 服务器的证书
- 启用或禁用 Kaspersky Endpoint Detection and Response Optimum 整合

- 配置 Kaspersky Managed Detection and Response 集成
- 管理设备网络隔离
- 管理隔离区设置
- 通过命令行管理隔离文件
- 搜索入侵指标
- 管理执行防护
- 配置 KUMA 整合
  - Kaspersky Unified Monitoring and Analysis Platform 整合任务
  - 管理用于连接到 KUMA 服务器的证书
- 常规设置
  - 常规应用程序设置
  - 任务计划
  - 配置代理服务器设置
  - 配置备份设置
  - 网络流量扫描设置
  - 配置全局排除项
  - 密码保护设置
- 管理控制台中的应用程序设置
  - 数据库更新
  - 主机威胁防护
    - 文件威胁防护
      - “扫描范围”窗口
      - “新建扫描范围”窗口
      - “扫描设置”窗口
      - “检测到威胁后的操作”窗口
      - 文件威胁防护排除项
        - “排除范围”窗口
        - “新排除范围”窗口
        - “按掩码筛选的排除项”窗口
        - “按威胁名称筛选的排除项”窗口
        - “按进程筛选的排除项”窗口
        - “受信任进程”窗口
    - 恶意软件扫描
      - “扫描范围”窗口
      - <新扫描范围>窗口
      - “扫描范围设置”窗口
      - “扫描范围”窗口
      - “扫描设置”窗口
      - “检测到威胁后的操作”窗口
      - “排除项”部分
      - “排除范围”窗口
      - “新排除范围”窗口
      - “按掩码筛选的排除项”窗口
      - “按威胁名称筛选的排除项”窗口
    - 关键区域扫描
      - “扫描范围”窗口
      - “新建扫描范围”窗口

“扫描范围设置”窗口
“扫描范围”窗口
“扫描设置”窗口
“检测到威胁后的操作”窗口
“排除项”部分
“排除范围”窗口
“新排除范围”窗口
“按掩码筛选的排除项”窗口
“按威胁名称筛选的排除项”窗口
容器监控
“容器扫描设置”窗口
容器扫描
“容器扫描设置”窗口
“扫描设置”窗口
“检测到威胁后的操作”窗口
“排除项”部分
“按掩码筛选的排除项”窗口
“按威胁名称筛选的排除项”窗口
可移动驱动器扫描
行为检测
“按进程筛选的排除项”窗口
“受信任进程”窗口
漏洞利用防御
漏洞利用防御排除窗口
漏洞利用防御排除窗口
反加密
“扫描范围”窗口
“新建扫描范围”窗口
“保护设置”窗口
“排除范围”窗口
“新排除范围”窗口
“按掩码筛选的排除项”窗口
卡巴斯基安全网络
卡巴斯基安全网络设置
卡巴斯基安全网络声明
卡巴斯基私人安全网络声明
BadUSB 攻击防护
通信和 Web 保护
邮件威胁防护
邮件威胁防护设置窗口
附件筛选窗口
Web 威胁防护
“受信任网址”窗口
“扫描设置”窗口
网络威胁防护
“排除项”窗口

- 防火墙管理
  - “网络数据包规则”窗口
  - “添加网络数据包规则”窗口
  - 添加 IP 地址窗口
  - “可用网络”窗口
  - “网络连接”窗口
- 安全控制
  - 设备控制
    - “受信任的设备”窗口
    - “受信任设备(设备 ID)”窗口
    - 客户端设备上的设备窗口
    - 基于设备控制事件窗口的设备列表
    - 访问受信任设备窗口
    - “用户或组”窗口
    - “设备类型”窗口
    - “配置设置访问规则”窗口
    - “用户或组”窗口
    - 访问计划窗口
    - “连接总线”窗口
  - Web 控制
    - Web 控制规则窗口
    - 内容类别选择窗口
    - 数据类型类别选择窗口
    - 选择地址窗口
    - 选择地址组窗口
    - 添加地址组窗口
    - 选择用户窗口
    - “用户或组”窗口
    - 访问计划窗口
  - 应用程序控制
    - “应用程序控制规则”窗口
    - “添加规则”窗口
    - “应用程序类别”窗口
    - “用户或组”窗口
    - 清查
      - “扫描范围”窗口
      - “新建扫描范围”窗口
      - “排除项”部分
      - “排除范围”窗口
      - “新排除范围”窗口
  - 系统完整性监控
    - “扫描范围”窗口
    - “新建扫描范围”窗口
    - “排除范围”窗口
    - “新排除范围”窗口
    - “按掩码筛选的排除项”窗口

- 系统完整性检查
  - “扫描范围”窗口
  - “新建扫描范围”窗口
  - “排除项”部分
  - “排除范围”窗口
  - “新排除范围”窗口
  - “按掩码筛选的排除项”窗口
- 本地任务
  - 任务管理
- 防御高级威胁和定向攻击
  - 与 Kaspersky Managed Detection and Response 整合
  - 卡巴斯基 Endpoint Detection and Response (on-premises) 集成
    - 配置 KATA 服务器连接
    - 管理 KATA 服务器连接常规设置
    - 配置数据传输到 KATA 服务器
  - Kaspersky Network Detection and Response (KATA) 整合
    - 配置 NDR 服务器连接
    - 管理 NDR 服务器连接常规设置
    - 配置数据传输到 NDR 服务器
  - 与 KUMA 的整合
    - “KUMA 服务器”窗口
    - “KUMA 服务器”窗口
    - “KUMA 服务器连接设置”窗口
    - “添加服务器证书”窗口
    - “添加客户端证书”窗口
  - 隔离
  - 对象的执行防护
- 常规设置
  - 代理服务器
    - 代理服务器排除项窗口
  - 扫描任务的 CPU 使用量
  - 使用电池供电时运行任务
  - 启动应用程序
  - 收到关键更新时自动重启
  - 密码保护
  - 跟踪和转储设置
  - 应用程序的常驻内存使用率
  - 加密连接扫描
    - “受信任域”窗口
    - “受信任的证书”窗口
    - 流量拦截排除窗口
    - 流量拦截排除窗口
    - 被监控的端口
  - 全局排除项
    - “挂载点路径”窗口
  - 从扫描中排除进程内存
  - 备份

检测黑客可能用来造成危害的应用程序
文件操作拦截
将信息发送至 Kaspersky Security Center 存储
系统事件拦截
附加遥测设置
Light Agent 模式
与 Integration Server 的连接
"与 Integration Server 的连接"窗口
验证 Integration Server 证书窗口
"Integration Server 上的身份验证"窗口
SVM 检测设置
SVM 连接标签
SVM 选择算法
保护连接
已知问题和限制
联系技术支持
通过 Kaspersky CompanyAccount 获取技术支持
获取技术支持信息
如何启用和配置跟踪文件创建
如何启用和配置转储
使用 Kaspersky Security Center 进行远程设备诊断
附录
附录 1.配置文件和默认应用程序设置
编辑任务配置文件的规则
初始配置文件
安装包中的初始配置设置
预设配置文件
命令行任务的默认设置
File_Threat_Protection 任务（ID：1）的默认设置
Scan_My_Computer 任务（ID：2）的默认设置
Default settings for the Scan_File task (ID:3)
Critical_Areas_Scan 任务（ID：4）的默认设置
更新任务（ID：6）的默认设置
System_Integrity_Monitoring 任务（ID：11）的默认设置
Firewall_Management 任务（ID：12）的默认设置
Anti_Cryptor 任务（ID：13）的默认设置
Web_Threat_Protection 任务（ID：14）的默认设置
Device_Control 任务（ID：15）的默认设置
Removable_Drives_Scan 任务（ID：16）的默认设置
Network_Threat_Protection 任务（ID：17）的默认设置
Container_Scan 任务（ID：18）和 Custom_Container_Scan（ID：19）任务的默认设置
Behavior_Detection 任务（ID：20）的默认设置
Application_Control 任务（ID：21）的默认设置
Inventory_Scan 任务（ID：22）的默认设置
KATAEDR 任务（ID：24）的默认设置
Web_Control 任务（ID：26）的默认设置
Standalone_Sandbox 任务（ID：29）的默认设置

KATANDR 任务（ID：31）的默认设置
KUMA 任务（ID：33）的默认设置
邮件威胁防护任务（ID: 35）的默认设置
BadUSB 攻击防护任务（ID: 37）的默认设置
KATANDR 任务（ID：31）的默认设置
附录 2.配置与 Kaspersky Anti-Virus for Linux Mail Server 的交互
附录 3.与外部服务交互的设置
附录 4.快速可移动驱动器扫描的文件扩展名
附录 5.消息模板中的变量
附录 6.应用程序事件
严重
警告
信息性消息
附录 7.返回代码
附录 8.准备包含应用程序数据库的存档文件
附录 9.IOC 文件的要求
法律通告
数据提供
使用激活码时提供的数据
从卡巴斯基更新服务器下载更新时提供的数据
在 Light Agent 模式下使用应用程序时传输的数据
发送到 Kaspersky Security Center 的数据
在应用程序界面中点击链接时提供的数据
使用卡巴斯基安全网络时提供的数据
与 Kaspersky Endpoint Detection and Response Optimum 集成时提供的数据
与 Kaspersky Endpoint Detection and Response (KATA) 组件集成时提供的数据
与 Kaspersky Endpoint Detection and Response Expert (on-premises) 组件集成时提供的数据
与 Kaspersky Endpoint Detection and Response Expert (cloud) 组件集成时提供的数据
与 Kaspersky Network Detection and Response (KATA) 组件集成时提供的数据
与 Kaspersky Unified Monitoring and Analysis Platform 集成时提供的数据
有关第三方代码的信息
商标通知

# Kaspersky Endpoint Security for Linux

### 浏览

Kaspersky Endpoint Security for Linux
版本 12.5 的新功能
典型部署方案
功能比较
已知问题和限制

### 快速入门

硬件和软件要求
兼容性
准备分发包
准备用于安装的环境
部署应用程序
迁移到 Kaspersky Security Center Linux 的方案

### 使用应用程序

激活
更新数据库
使用 Kaspersky Update Utility 进行更新
文件威胁防护
信任区域
优化资源

### 在命令行中配置

使用命令行管理应用程序
管理命令
应用程序命令行选项

### 支持

保护状态监控
从以前版本的应用程序升级
联系技术支持

# 关于应用程序

Kaspersky Endpoint Security for Linux 为 Linux 设备提供高级全面保护，并可预防、检测和响应各种类型的威胁、网络攻击和欺诈行为。该应用程序包含在许多卡巴斯基多平台解决方案中，并且可以灵活配置，以应对您组织的 IT 基础架构面临的挑战。

您可以在本地管理安装在受保护设备上的 Kaspersky Endpoint Security，也可以使用 Kaspersky Security Center 对其进行集中管理。

该应用程序不适用于涉及自动化控制系统的工业流程。为了保护这些系统中的设备，我们建议使用 Kaspersky Industrial CyberSecurity for Linux Nodes。

# 主要功能

### 防御大规模网络威胁

基于先进技术的保护是您的 IT 安全的基础。Kaspersky Endpoint Security 可防止用户设备的文件系统受到感染，监控可移动驱动器与设备的连接并扫描其中的病毒。它会监控应用程序的恶意活动，并保护文件免受恶意远程加密。包含有关新型全球威胁（例如病毒、木马程序、加密程序、黑客攻击）信息的数据库会定期自动更新。

### 通信和 Web 保护

Kaspersky Endpoint Security 可以可靠地保护您组织的网络环境：它会在您打开电子邮件、网站和下载的文件之前，扫描其中是否存在病毒、网络蠕虫和其他威胁。该应用程序允许扫描传入网络流量中可能表明存在网络攻击的活动，监控操作系统防火墙的设置并过滤网络活动。

### 工作场所安全控制

通过使用 Kaspersky Endpoint Security 控制用户在工作场所对应用程序、Web 资源和已连接设备的访问，您可以为您的组织提供另一层安全保障。这有助于保护设备免受感染，并防止数据丢失或泄露。

### 防御高级威胁和定向攻击

该应用程序可以与卡巴斯基 Detection and Response 解决方案交互，即 Kaspersky Managed Detection and Response (MDR) 和 Kaspersky Anti Targeted Attack Platform (KATA)。卡巴斯基 SIEM 解决方案 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 也受支持。Kaspersky Endpoint Security 会监控用户设备上运行的进程、打开的网络连接以及正在修改的文件。与 Detection and Response 解决方案的交互可防御漏洞利用、勒索软件、无文件攻击以及黑客可用来破坏设备或数据的合法系统工具等威胁。

### 保护虚拟和云环境

Kaspersky Endpoint Security 作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分，可为在各种服务器虚拟化平台和 VDI 平台上运行 Linux 客户操作系统的虚拟机提供保护。对象病毒扫描由安装在单独虚拟机（即 SVM (Secure Virtual Machine)）上的特殊组件执行。因此，该应用程序使用 SVM 的资源而不是虚拟机的资源来提供安全性，再结合智能优化（例如使用共享缓存），可最大限度地减少 IT 基础设施的总体负载。

# 版本 12.5 的新功能

Kaspersky Endpoint Security 12.5 for Linux 引入了以下功能和改进：

- 支持在配备 Elbrus CPU 的设备上安装 Kaspersky Endpoint Security 12.5 for Linux。该应用程序为 Elbrus CPU 提供 有限支持。
- 已实现与 Kaspersky Endpoint Detection and Response Expert (cloud) 的集成。该云解决方案旨在保护组织的 IT 基础架构免受高级网络威胁侵害，包括无法由安装在企业资产上的 EPP 应用程序检测到的威胁。该解决方案通过利用各种响应工具和数据源（包括端点资产、网络数据和云环境数据）提供全面的可见性、关联分析和自动化，并通过单一界面中的集成组件和端到端工作流实现统一的检测和响应流程，从而提高安全专家的工作效率。

  在 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案推出之前，Kaspersky Endpoint Security for Linux 与该解决方案的集成暂时不可用；该解决方案计划于 2026 年底推出。之后，我们预计该集成功能将可用于此版本的 Kaspersky Endpoint Security，无需额外升级。

- Kaspersky Endpoint Security 应用程序中某些操作的密码保护。密码保护允许您根据授予用户的权限，限制用户可对 Kaspersky Endpoint Security 应用程序执行的操作。限制对应用程序设置的访问可降低未经授权或无意更改应用程序的风险。
- 设备控制组件得到了改进。现在，您可以将受信任设备列表导出到文件，也可以从文件导入该列表。
- 改进了 BadUSB 攻击防护 组件。现在，当您连接条形码扫描器时，可以扫描屏幕上的条形码来授权扫描器，而无需输入授权码来解锁设备。
- 对可更新内核模块 (ULKM)的改进：
  - 新增了对在启用 Secure Boot 的系统上基于可更新内核模块 (ULKM)进行系统事件拦截的支持。
  - 该应用程序现在支持更多可使用可更新内核模块拦截事件的操作系统。
  - 我们为反加密勒索和设备控制组件添加了对可更新内核模块的支持。
- 我们改进了 Astra Linux Special Edition 的封闭软件环境模式下的安装过程。现在，如果安装了兼容性包，则在配备 Astra Linux Special Edition 操作系统的设备上安装 Kaspersky Endpoint Security 应用程序后，用户无需手动执行其他操作即可启动该应用程序。
- 现在，安装应用程序时，您可以使用 autoinstall.ini 配置文件修改 kesl.ini 配置文件的设置。
- 改进了应用程序安装和卸载期间的错误诊断：
  - 返回代码更加详细，有助于更清楚地了解任何潜在问题。
  - 我们添加了有关缺少安装和应用程序正常运行所需的依赖项（外部库、组件、实用程序或其他程序）的新消息。
  - 我们添加了有关系统目录访问权限配置不正确的新消息。

- Kaspersky Security Center 显示新的和更明确的错误消息。
- 现在，您可以在安装应用程序时忽略软件包管理器错误。

- 首次更新应用程序数据库和模块后，应用程序现在会在安装过程中自动重新启动。现在，您可以将应用程序配置为在收到关键更新时自动重新启动，此设置在安装应用程序 24 小时后生效。您可以通过命令行、在常规应用程序设置中，或使用 Web Console 或管理控制台在策略属性中配置应用程序自动重启。
- 现在，与检测和响应解决方案集成时，您可以使用 `UseIncreasedXdrEventsCache` 设置在 kesl.ini 配置文件中管理事件缓存。高性能与 RAM 占用之间需要权衡。
- 现在，在停止或重新启动应用程序时，您可以使用 kesl.ini 配置文件中的 `FastShutdown` 设置快速关闭 kesl 进程，这有助于最大限度地缩短高负载系统上的应用程序停机时间，并防止资源消耗过多。
- 现在，您可以使用 `ReduceSWMemoryConsumption` 设置（来自 kesl.ini 配置文件）限制行为分析组件处理事件队列时的内存消耗。使用此设置可能会影响保护级别。请务必查看文档。
- 我们提高了网络访问的稳定性。现在，如果 kesl 进程异常终止，Watchdog 服务器会删除应用程序在 Web 威胁防护和网络威胁防护组件启动时添加的防火墙规则，从而避免互联网连接中断，并快速恢复设备上的网络访问。
- 现在，您可以防止多个扫描任务同时运行，以优化应用程序性能。现在，启用该选项后，如果同时启动多个扫描任务，这些任务将进入队列。
- 文件威胁防护排除项现在可以处理符号链接。路径现在会转换为最终文件地址。
- 现在，您可以使用用于管理常规应用程序设置的命令启用和配置转储文件目录，而无需重新启动应用程序。这些转储文件配置设置已从 kesl.ini 配置文件中删除。
- 现在，与 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Anti Targeted Attack Platform 和 Kaspersky Unified Monitoring and Analysis Platform 解决方案集成时，必须使用密码。现在，在配置集成时，您必须为客户端证书指定密码。
- 现在，在 Kaspersky Unified Monitoring and Analysis Platform 整合过程中发送遥测事件时，应用程序可以压缩流量，这有助于节省带宽。
- 我们更新了支持的操作系统列表，包括支持 CentOS 5.2、5.4、6.4 和 6.6 的 64 位版本。
- 应用程序界面现已支持新语言：西班牙语（墨西哥）和葡萄牙语（巴西）。

## 旧版本中的更改

### 版本 12.4

Kaspersky Embedded Systems Security 12.4 for Linux 现在具有以下新功能和改进：

- 新增功能组件：邮件威胁防护。该组件会扫描收发电子邮件的附件，以检测病毒和其他威胁性应用程序。
- 新增功能组件：BadUSB 攻击防护。该组件可阻止将伪装成键盘的受感染 USB 设备连接到客户端设备。
- 设备控制组件得到了改进。现在，您可以根据用户请求授予对被阻止设备的临时访问权限。
- 对漏洞利用防御组件的改进。现在，您可以为对象配置特定于组件的扫描排除项。

- 对可更新内核模块的改进：
  - 现在，可更新内核模块可帮助优化文件操作拦截。应用程序性能通过使用无需扫描的文件和进程缓存得到提高。
  - 现在，通过使用可更新内核模块，您可以更精细地配置全局排除项。如果您使用的是基于 fanotify 技术的拦截机制，指定的挂载点将被从文件操作拦截中完全排除。使用可更新内核模块，您可以排除设备上挂载的特定本地或远程目录。
- 提供与 Kaspersky Endpoint Detection and Response (KATA) 集成的 EDR (KATA) 组件已重命名为 EDR Expert (on-premises)。该组件还提供 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成。集成任务已重命名为 *Kaspersky Endpoint Detection and Response Expert (on-premises) 集成* (KATAEDR, ID: 24)。
- 现在，您可以设置与 Kaspersky Endpoint Detection and Response Expert (on-premises) 的集成，这是一款企业级网络安全解决方案，能够抵御大多数网络安全风险，并涵盖威胁传播的主要场景。Kaspersky Endpoint Detection and Response Expert (on-premises) 的组件部署在 Open Single Management Platform (OSMP) 上。与 Kaspersky Endpoint Detection and Response Expert (on-premises) 的集成支持 Kaspersky Endpoint Detection and Response (KATA) 集成的所有功能，并支持以下新功能：
  - 启动 YARA 扫描。在 *YARA 扫描*期间， Kaspersky Endpoint Security 使用 YARA 文件搜索设备上的恶意活动特征。
  - 收集取证数据，即在调查涉及网络犯罪和数据泄漏的事件时可能会有用的数字数据。
  - 将关于设备上事件的扩展数据（遥测数据）发送到 OSMP 平台上的遥测服务器。
  - 仅发送包含攻击指标 (IOA) 的遥测数据。现在，您还可以在 Web Console 策略中配置自定义过滤器。
  - 通过添加授权许可密钥，激活 EDR Expert (on-premises) 组件，该组件提供 与 Kaspersky Endpoint Detection and Response Expert (on-premises) 的集成以及与 Kaspersky Endpoint Detection and Response (KATA) 的集成。
  - 在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 集成*任务的设置中（通过命令行或在 Web Console 的策略属性中）选择集成模式。
- 应用程序可在 Endpoint Detection and Response Agent 模式下使用，以支持 Kaspersky Detection and Response 解决方案与受保护设备上的第三方反病毒解决方案协同工作。在此模式下，设备将不受标准保护和 Kaspersky Endpoint Security 控制组件的保护。第三方应用程序负责设备的标准保护。
- 您可以在安装后首次启动应用程序时创建跟踪文件。现在，您可以在 Web Console、管理控制台或初始配置文件设置中启用首次启动应用程序时创建跟踪文件的功能。
- Web Console 中的策略管理接口已更新。策略中的章节结构已经过重新设计，以帮助您更快找到所需功能。
- 现在，您可以选择流量拦截模式：eBPF 技术或 iptables 实用程序。
- 现在，您可以选择遥测源（仅限 eBPF 或 eBPF 加 auditd）。对于 auditd，您还可以选择运行模式（独占模式或组播模式）。
- 现在，您可以选择将文件和目录发送到沙盒进行扫描的模式：手动、仅自动、自动和手动。

- 在 Light Agent 模式下使用应用程序时，可以使用更多功能：
  - 基于可更新内核模块的系统事件拦截机制可用。
  - 漏洞利用防御功能组件可用。
  - 威胁检测得到了改进。
- 现在，您可以直接使用卡巴斯基私人安全网络 (KPSN)，而无需在管理服务器上使用 KSN 代理服务。
- 现在，您可以在 Web Console 和管理控制台中创建漫游策略。漫游策略会在设备离开组织网络时生效。
- 在 Web Console 或管理控制台中查看和导出挂载点列表，或在命令行中查看此列表时，现在还会显示有关在命名空间中找到的挂载点的信息。
- 我们改进了在 64 位操作系统（内核版本为 4.18 或更高版本，且支持 eBPF）上行为检测组件用于获取系统遥测数据的替代机制，该机制可释放 auditd 内核审计子系统的资源。
- 现在，当与 Kaspersky Managed Detection and Response 集成时，您可以将以下信息包含在遥测数据中：
  - 容器中发生的事件指示
  - 容器命名空间 ID
  - 容器名称
- 我们更新了支持的操作系统列表。

**版本 12.3**

Kaspersky Embedded Systems Security 12.3 for Linux 现在具有以下新功能和改进：

- 我们添加了基于可更新内核模块拦截系统事件的机制（在 Light Agent 模式下不可用）。如果设备的操作系统支持 fanotify 并且满足安装可更新内核模块的其他要求，则您可以配置应用程序以使用可更新内核模块。使用可更新内核模块可优化 Kaspersky Endpoint Security 对已启动进程的拦截。可更新内核模块包含在应用程序的分发包中。
- 可更新内核模块改进了 反加密勒索 组件的功能（在 Light Agent 模式下不可用）。应用程序现在可以检测更多类型的勒索软件。
- 我们添加了一个新的功能组件：漏洞利用防御（在 Light Agent 模式下不可用）。漏洞利用防御会监控利用设备漏洞来获取管理权限或执行恶意操作的代码。
- 设备控制组件得到了改进：
  - 我们添加了一项配置用户或用户组列表的功能，添加的设备在这些用户或用户组中被视为可信。
  - 我们增加了允许对存储设备进行只读访问的功能。
  - 我们还改进了通过事件向用户发出通知的方式，添加了新事件，并明确和系统化了插件及命令行中的事件文本。

- 扩展了与 Kaspersky Managed Detection and Response 解决方案的整合：
  - 现在您可以将设备从网络隔离。
  - 您可以隔离文件或从隔离区恢复文件。
  - 您可以启动或终止一个进程。
- 我们添加了通过添加授权许可密钥来激活 MDR 组件的功能，该组件提供与 Kaspersky Managed Detection and Response 的集成。
- 行为检测组件得到了改进。现在，您可以启用或禁用将进程从 MDR 和 EDR (KATA) 扫描范围中排除。
- 现在，您可以配置代理服务器排除项。您可以指定哪些 Kaspersky Endpoint Security 组件必须绕过代理服务器，还可以创建一个不会为其使用代理服务器的地址列表。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。
- 现在，您可以配置流量拦截排除项目。现在，您可以使用应用程序的管理插件或命令行来指定应用程序应从流量拦截中排除的连接。
- 现在，您可以暂时将数据库日志文件从扫描中排除，以优化文件威胁防护扫描。如果数据库日志文件在上次扫描后的 10 分钟内被同一进程重复使用，则应用程序将跳过对该日志文件的扫描。
- 现在，您可以在继承父策略的设置时启用合并父策略及其子策略中的排除列表项。
- 现在，您可以使用管理 Web 插件来导出和导入策略和任务中的排除列表。
- 我们添加了在创建安装包时或在安装包的属性中在 Kaspersky Security Center 管理控制台中配置 Kaspersky Endpoint Security 应用程序的初始配置设置的功能。
- 现在，您可以配置在使用电池供电的设备上取消计划的任务。
- 我们添加了当 Kaspersky Endpoint Security 与 KSN 服务器交互时启用或禁用 KSN 代理服务器的功能（在 Light Agent 模式下不可用）。如果启用了 KSN 代理服务器，Kaspersky Endpoint Security 将使用管理服务器上的 KSN 代理服务与 KSN 服务器进行通信。如果禁用 KSN 代理服务器，Kaspersky Endpoint Security 将直接与 KSN 服务器交互。
- 在命令行中，您可以使用一个命令，该命令可显示应用程序功能列表、有关其状态（已使用或未使用）的信息，以及用于实现这些应用程序功能的 Linux 技术。
- 我们添加了在命令行和图形界面中显示设备上生效的策略和策略配置文件相关信息的功能。
- 现在，您可以使用命令行在未安装 Perl 解释器的设备上安装应用程序。
- 我们改进了流量拦截。现在本地流量（同一设备上进程之间的流量）不会被拦截。
- 现在，您可以在与 Kaspersky Managed Detection and Response 集成时传递发送遥测所需的必要设置，而无需使用 KPSN 配置文件。如果您正在使用卡巴斯基安全网络基础设施解决方案，或者您的唯一租户是根租户，则不需要 KPSN 配置文件即可与 Kaspersky Managed Detection and Response 整合。
- 优化了应用程序事件日志中大量事件的存储。现在，打开和关闭事件数据库以及检索事件的操作速度更快了。

- 我们改进了应用程序的图形界面（如果应用程序在 Light Agent 模式下使用，则不支持图形界面）：
  - 现在，您可以启用或禁用 Web 控制 组件。
  - 我们重新设计了图形界面的样式（新颜色、所有窗口的圆角）。
- 更改了文件威胁防护设置和扫描任务中可应用于受感染对象的操作名称。
- 添加了在 64 位操作系统（内核版本为 5.3 或更高版本，且支持 eBPF）上在行为检测组件中获取系统遥测数据的替代机制，可释放 auditd 内核审计子系统的资源。如果操作系统满足要求，应用程序在 Light Agent 模式下也会自动使用 eBPF。
- 所有应用程序管理接口（命令行接口除外）中的日期和时间均以符合 RFC 3339 标准的统一格式显示，例如，2023-12-25 23:55:59。
- 我们更新了支持的操作系统列表。

**版本 12.2**

Kaspersky Embedded Systems Security 12.2 for Linux 现在具有以下新功能和改进：

- 增加了对与 Kaspersky Network Detection and Response (KATA) 进行集成的支持，KATA 是 Kaspersky Anti Targeted Attack Platform 解决方案的一个组件，它可以保护公司内部网络，并允许将有关设备上发生的事件的信息（遥测）发送到带有中央节点组件的 Kaspersky Anti Targeted Attack Platform 服务器（以下也称为 NDR 服务器）。
- 增加了对与 Kaspersky Anti Targeted Attack Platform 解决方案的组件 KATA Sandbox 进行集成的支持，该解决方案允许您使用部署了操作系统虚拟映像的特殊服务器来分析和扫描对象，以检测针对企业 IT 基础设施的恶意活动和针对性攻击指标。
- 增加了对与 Kaspersky Unified Monitoring and Analysis Platform 进行集成的支持， Kaspersky Unified Monitoring and Analysis Platform 是一个全面的软件解决方案，结合了以下功能：接收、处理和存储信息安全事件；分析和关联传入数据；搜索收到的事件，以及创建有关检测信息安全威胁指标的通知。
- 扩展了与 Kaspersky Endpoint Detection and Response (KATA) 进行集成的功能，这是 Kaspersky Anti Targeted Attack Platform 解决方案的一个组件。
  - 新的对象执行预防功能。
  - 新的文件隔离功能。
  - 扩展了有关设备事件（遥测）的信息。
- 扩展了 Endpoint Detection and Response Optimum 集成功能：
  - 新的对象执行预防功能。
  - 新的文件隔离功能。
  - 现在您可以按照进程名称将进程从网络隔离中排除。
- 现在您可以使用 Cloud Sandbox 技术，它可以检测设备上的复杂威胁。Kaspersky Endpoint Security 应用程序会自动将检测到的文件发送到 Cloud Sandbox 进行分析。Cloud Sandbox 在隔离环境中运行这些文件以检测恶意活动并确定这些文件的信誉。

- 现在，您可以查看有关最常扫描的文件和应用程序的统计数据以及受保护设备上的挂载点列表。为了提高性能，您现在可以排除文件威胁防护组件最常扫描的文件、行为检测组件最常扫描的应用程序路径以及设备上检测到的挂载点。

- 现在，您可以收集应用程序性能指标，这些指标可帮助分析 Kaspersky Endpoint Security 对操作系统性能的影响。

- 改进了防火墙管理组件。现在，您可以为网络包规则指定多个 IP 地址或 IP 地址范围。

- 用于跟踪操作系统冻结的新机制。此机制会检查某些系统功能的冻结情况，其中包括 execve 函数。每隔三秒，wdserver Watchdog 服务器进程会启动另一个 wdserver 进程，并在该进程中调用这些系统函数（一个 execve 函数调用至少会启动一个额外的 wdserver 进程）。如果 wdserver 检测到无响应的系统功能，Watchdog 服务器过载机制会重启 kesl 进程。

- 现在，您可以在管理应用程序的图形用户界面时配置弹出通知的显示。现在，您可以使用 Web Console、管理控制台或命令行启用或禁用 GUI 中弹出通知的显示。

- 改进了任务计划的命令行选项。现在，您可以配置任务在达到最大允许执行时间时停止。

- 更改了创建 Kaspersky Security Center 策略配置文件时的“挂锁”属性的状态。现在，创建配置文件时，所有“挂锁”默认打开，这意味着默认情况下，配置文件设置不会覆盖“基本”策略的设置。

- 添加了在 64 位操作系统（内核版本 5.3 或更高版本，带有支持 BTF 的 eBPF）上获取系统遥测的替代机制，这样可释放 auditd 内核审计子系统的资源。如果操作系统满足指定要求，该应用程序将自动与 eBPF 一起工作。

- 所有管理插件中的日期和时间均以符合 RFC 3339 标准的统一格式显示，例如，2023-12-25 23:55:59。

- 我们更新了支持的操作系统列表。

**版本 12.1**

Kaspersky Embedded Systems Security 12.1 for Linux 现在具有以下新功能和改进：

- 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设置。

- 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。

- 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上或连接到客户端设备的所有设备（包括以前安装和连接过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。
- 我们更新了支持的操作系统列表。

# 已修复问题

下表列出了在 Kaspersky Endpoint Security 先前版本中发现并已在当前版本中修复的所有问题。

## 版本 12.5 中修复的问题列表

| 标识符 | 描述 |
| --- | --- |
| 10306343 | 检查当前授权许可密钥的状态时，错误地生成了有关删除和安装授权许可密钥的通知。 |
| 10295949 | 当前策略配置文件中为设备控制组件指定的设置未应用。因此，该组件继续使用策略中指定的设置运行。 |
| 10171454 | 如果设置中指定的第一个更新源不可用，则会错误地显示有关更新问题的消息。 |
| 10109293 | 如果选择了 iptables 网络流量拦截模式（`NetInterceptorMode=UseIPTables`），则来自打开了与特定网络接口绑定的网络套接字的应用程序的流量处理不正确。 |
| 10024219 | Kaspersky Security Center 管理控制台错误地显示受管理设备上可更新内核模块的状态。 |
| 9995631 | 应用程序对常驻 RAM 使用量的限制（`MaxMemory` 设置）在没有交换分区的系统上无法正常工作。现在，当达到设置的限制时，Kaspersky Endpoint Security 会重新启动。 |
| 9937329 | 在禁用设备控制 (Device_Control) 任务的系统上错误地生成了 *设备已连接* 和 *设备已断开连接*。 |
| 9934846 | 该应用程序在高负载系统上无法启动。应用程序连接到 Watchdog 服务器的超时时间已增加。 |
| 9846405 | 在配置了 EFI 引导加载程序的系统上错误地生成了 *对象未处理* 事件。 |
| 9815051 | 在 eBPF 网络流量拦截模式（`NetInterceptorMode=UseEBPF`）下，在受管理设备上运行 Web 威胁防护 (Web_Threat_Protection) 和网络威胁防护 (Network_Threat_Protection) 任务时，之前建立的网络连接可能会挂起。现在，当尝试传输数据时，此类连接会被终止。 |
| 9807202 | 在某些 ROSA 操作系统上，使用 mkfs.ext2 实用程序进行安装时遇到问题。 |
| 9704644 | 当应用程序以 EDR 代理模式使用时，设备状态显示不正确。当应用程序以 EDR Agent 模式使用时，已更改设备保护状态的值。 |
| 9643969 | 在某些情况下，在 eBPF 模式下使用网络流量拦截时，Scylla 主机之间的网络连接可能会出现问题。 |
| 9633030 | 当策略中取消选中 **启用对象执行防护** 复选框时，对象执行防护 (EDR Expert (on-premises)) 任务会运行。 |
| 9627894 | 在禁用 IPv6 的操作系统上，基于 eBPF 技术的网络流量拦截模式无法正常工作。 |
| 9606448 | 使用 Kaspersky Security Center 管理服务器作为代理服务器访问卡巴斯基激活服务器来激活应用程序时出现问题（当在策略中选中 **将 Kaspersky Security Center 用作代理服务器以进行激活** 复选框时）。 |
| 9508605 | 启用 Kaspersky Endpoint Detection and Response Expert 集成后，该应用程序在具有容器环境的系统上会占用大量内存。 |
| 9456741 | 由于在拦截新进程启动时无法确定文件解释器，应用程序崩溃。 |

Web 插件 6.1 版本中修复的问题列表

| 标识符 | 描述 |
| --- | --- |
| 9558745 | 策略属性（**应用程序设置** → **常规设置** → **事件设置** → **高级设置**）中未显示用于配置 Kaspersky Endpoint Security 图形界面中通知显示的 **在图形用户界面中显示弹出通知** 设置。 |
| 9622658 | 按对象哈希值添加恶意软件扫描排除项时，这些排除项未保存。 |
| 9798821 | 将单个网站添加到 Web 控制规则时，策略更改未保存。 |
| 9990129 | 在添加受信任应用程序的表单中显示了不相关的 **注释** 字段。 |
| 9977884 | 在邮件威胁防护组件的设置中显示了不相关的 **安全级别** 切换开关。 |
| 9944635 | **扫描电子邮件数据库** 标志的名称重复。现在显示正确的名称：**扫描电子邮件数据库** 和 **扫描电子邮件格式文件**。 |
| 10010439 | 创建 Web 控制规则时，从 Active Directory 列表中分配给该规则的用户未正确添加。 |
| 10218308 | 更改策略设置时，卡巴斯基安全网络模式被重置。 |

# 硬件和软件要求

最低硬件要求

**应用程序安装**

- 采用 AMD64 架构、2 GHz 或更高频率、两个或更多核心且支持 SSE2 指令集的 CPU。
- 至少 1 GB 的交换空间
- RAM：
  - 对于 64 位操作系统：可供应用程序使用的 RAM 为 2 GB
  - 对于 32 位操作系统：可供应用程序使用的 RAM 为 1 GB
- 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

  需要额外的磁盘空间来存储跟踪文件和应用程序内存转储文件。

  当使用 `ScanArchived=Yes` 和/或 `ScanSfxArchived=Yes` 扫描压缩文件和复合对象时（默认情况下，对于扫描任务设置为 `Yes`，对于文件威胁防护为 `No`），文件威胁防护和扫描任务需要额外的磁盘空间，具体取决于此类对象的类型和解压大小。

  我们建议确保 /tmp 目录中有足够的可用空间来扫描压缩文件和复合对象。您还可以通过为每个任务指定 `SizeLimit` 来限制可扫描的压缩文件的大小（处于存档状态）。

**安装图形用户界面**

- 能够显示宽度为 1000 像素、高度为 600 像素的窗口的显示器。如果应用了屏幕缩放，这些尺寸也会相应缩放。

## Arm 架构的最低硬件要求

**应用程序安装**

- Armv8.2-A Kunpeng 920 或 Armv8-A Baikal-M (BE-M1000) CPU 或 m-TrusT 终端平台
- 至少 1 GB 的交换分区
- 应用程序有 2 GB 的 RAM 可用
- 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

  需要额外的磁盘空间来存储跟踪文件和应用程序内存转储文件。

  当使用 `ScanArchived=Yes` 和/或 `ScanSfxArchived=Yes` 扫描压缩文件和复合对象时（默认情况下，对于扫描任务设置为 `Yes`，对于文件威胁防护为 `No`），文件威胁防护和扫描任务需要额外的磁盘空间，具体取决于此类对象的类型和解压大小。

  我们建议确保 /tmp 目录中有足够的可用空间来扫描压缩文件和复合对象。您还可以通过为每个任务指定 `SizeLimit` 来限制可扫描的压缩文件的大小（处于存档状态）。

**安装图形用户界面**

- 能够显示宽度为 1000 像素、高度为 600 像素的窗口的显示器。如果应用了屏幕缩放，这些尺寸也会相应缩放。

## Elbrus (E2K) 架构的最低硬件要求

**应用程序安装**

- CPU v3：Elbrus-4S；v4：Elbrus-8S 或 Elbrus-1S+
- 至少 2 GB 的交换分区
- 应用程序有 2 GB 的 RAM 可用
- 2 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

**安装图形用户界面**

- 能够显示宽度为 1000 像素、高度为 600 像素的窗口的显示器。如果应用了屏幕缩放，这些尺寸也会相应缩放。

## 软件要求

要安装 Kaspersky Endpoint Security，设备上必须安装表中列出的操作系统之一：

本文列出了应用程序已经过测试并保证能够正常运行的软件版本。应用程序也可能适用于其他软件版本，但这些配置尚未经过完整测试周期，因此未包含在保证支持的版本列表中。

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

如果操作系统管理员未完成其他步骤，则通过 FUSE 技术对挂载点进行文件威胁防护会受到限制。您可以将 user_allow_other 设置添加到 /etc/fuse.conf 文件，并为每个挂载点添加 allow_root 挂载选项，以允许应用程序监控这些挂载点的文件事件。

| 64 位操作系统 | Arm 架构的 64 位操作系统 | Elbrus (E2K) 架构的 64 位操作系统 | 32 位操作系统 |
| --- | --- | --- | --- |
| • AlmaLinux OS 8.6、8.7、8.8、8.9。<br>• AlmaLinux OS 9.4、9.5、9.6。<br>• AlterOS® 2025。<br>• Amazon™ Linux 2023。<br>• Astra Linux Common Edition 2.12。<br>• Astra Linux Special Edition RUSB.10015-01（操作更新 1.5、1.6、1.7、1.8）。<br>• Astra Linux Special Edition RUSB.10015-03 (operational update 7.6)。<br>• Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)。<br>• Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3)。<br>• Astra Linux Special Edition RUSB.10015-37 (operational update 7.7)。<br>"移动"模式下的 Astra Linux 操作系统仅在桌面模式下受支持。<br>• CentOS 5.2、5.4、6.4、6.6、7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9。<br>在 Kaspersky Endpoint Security Cloud 解决方案中，应用程序不支持在 CentOS 5.2、5.4、6.4、6.6 设备上运行。<br>在 Kaspersky Security Center 云控制台中，应用程序不支持在 CentOS 5.2、5.4、6.4、6.6 设备上运行。<br>• CentOS Stream 8、9、10。<br>• Debian GNU/Linux 12.8、12.9、12.10、12.11、12.12、12.13。<br>• Debian GNU/Linux 13.1、13.2、13.3。<br>• EMIAS 1.0。<br>• EulerOS 2.0 SP10。<br>• Fedora Linux 41。<br>• Kylin Desktop OS V10 SP1。<br>• Linux Mint 21.3。<br>• Linux Mint 22.2。<br>• Mostech 12 版本 2021.1。<br>• openSUSE Leap 15.6。<br>• Oracle Linux 7.3、7.4、7.5、7.6、7.7、7.8、7.9。<br>• Oracle Linux 8.5、8.6、8.7、8.8、8.9。<br>• Oracle Linux 9.4、9.5、9.6。<br>• Red Hat Enterprise Linux 7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9。<br>• Red Hat Enterprise Linux 8.5、8.6、8.7、8.8、8.9、8.10。<br>• Red Hat Enterprise Linux 9.4、9.5、9.6。<br>• Red Hat Enterprise Linux 10.0, 10.1。<br>• Rocky Linux 8.6、8.7、8.8、8.9。<br>• Rocky Linux 9.4、9.5、9.6。<br>• SberLinux 8.10、9.1、9.5、9.6、9.7。<br>• SberOS 3.4.0、3.5.0、3.6.1。<br>• SUSE Linux Enterprise Server 12.5、12.6、12.7。<br>• SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7。<br>• Ubuntu® 24.04 LTS。<br>• Ubuntu 26.04 LTS。<br>• ALT Education 10、11。<br>• ALT Workstation 11。<br>• ALT Server 11。<br>• ALT SP Workstation 版本 10。 | • Astra Linux Special Edition RUSB.10152-02 (operational update 4.7)。<br>• CentOS Stream 9。<br>• EulerOS 2.0 SP10。<br>• SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7。<br>• Ubuntu 26.04 LTS。<br>• ALT Workstation 11.2。<br>• ALT Server 11.1。<br>• ALT SP Workstation 版本 10。<br>• ALT SP Server 版本 10。<br>• RED OS 8.0。 | • OS Elbrus 9.3.6。<br>• Astra Linux Special Edition RUSB.10015-16 (release 2) (operational update 8.1)。<br>• Astra Linux Special Edition RUSB.10265-01 (operational update 8.1)。<br>• ALT SP Workstation 版本 8、10。<br>• ALT SP Server 版本 8、10。 | • Debian GNU/Linux 12.8、12.9、12.10、12.11、12.12、12.13。 |

| 64 位操作系统 | Arm 架构的 64 位操作系统 | Elbrus (E2K) 架构的 64 位操作系统 | 32 位操作系统 |
| --- | --- | --- | --- |
| • ALT SP Server 版本 10。<br>• Atlant，Alcyone build，版本 2022.02。<br>• GosLinux 7.2。<br>• M OS 12 Server 版本 2021.1。<br>• Mos OS 15.5 Arbat。<br>• MSVSphere 9.5 Workstation。<br>• MSVSphere 9.5 Server。<br>• MES OS 12 Panel 版本 2025。<br>• MES OS 12 Desktop 版本 2025。<br>• OSnova 3.1。<br>• RED OS® 7.3。<br>• RED OS 8.0。<br>• ROSA "Cobalt" 7.9 Workstation。<br>• ROSA "Cobalt" 7.9 Server。<br>• ROSA "Chrome" 12 Workstation。<br>• ROSA "Chrome" 12 Server。<br>• SintezM-Client 8.6。<br>• SintezM-Server 8.6。 | | | |

## Light Agent 模式的其他软件和硬件要求

Kaspersky Endpoint Security 可以作为Kaspersky Security for Virtualization Light Agent 6.5的一部分用作Light Agent。您可以在Kaspersky Security for Virtualization Light Agent 帮助中查看应用程序在 Light Agent 模式下的虚拟基础架构要求。

### 虚拟机

Kaspersky Endpoint Security 的软件和硬件要求在以下限制下适用于以 Light Agent 模式运行 Kaspersky Endpoint Security 的虚拟机：

- 必须具有一个带宽为 100 Mbps 的虚拟化网络接口
- 在 Arm 设备上，不支持以 Light Agent 模式运行 Kaspersky Endpoint Security。
- 不支持在处于强制访问控制模式和封闭软件环境模式的 Astra Linux Special Edition 操作系统中以 Light Agent 模式运行应用程序。

虚拟机上的 BIOS 必须支持 SMBIOS 规范版本 2.1 或更高版本。

根据您的虚拟基础架构，虚拟机必须安装以下组件：

- 在 Microsoft Hyper-V 基础架构中，必须安装 Integration Services 包。
- 在 VMware vSphere 基础架构中，必须安装 VMware Tools 包。
- 在 XenServer 基础架构中，必须安装 XenTools 软件。
- 在 HUAWEI FusionSphere 基础架构中，必须安装 HUAWEI Tools 包。
- 在 KVM（基于内核的虚拟机）基础架构中，必须安装 QEMU Guest Agent。

### 支持的终端服务器类型

- Astra Linux 3.0.5 终端服务器。

# 分发包

Kaspersky Endpoint Security 分发套件包含以下文件：

**主应用程序文件**

- 对于使用 32 位操作系统的处理器：
  `kesl-12.5.0-<build number>.i386.rpm`
  `kesl_12.5.0-<build number>_i386.deb`
- 对于使用 64 位操作系统的处理器：
  `kesl-12.5.0-<build number>.x86_64.rpm`
  `kesl_12.5.0-<build number>_amd64.deb`
- 对于使用 64 位操作系统的 Arm® 处理器：
  `kesl-12.5.0-<build number>.aarch64.rpm`
  `kesl_12.5.0-<build number>_arm64.deb`
- 对于 Elbrus CPU：
  `kesl-12.5.0-<build number>.e2k.rpm`
  `kesl_12.5.0-<build number>_e2k.deb`

**应用程序的图形界面**

- 对于使用 32 位操作系统的处理器：
  `kesl-gui-12.5.0-<build number>.i386.rpm`
  `kesl-gui_12.5.0-<build number>_i386.deb`
- 对于使用 64 位操作系统的处理器：
  `kesl-gui-12.5.0-<build number>.x86_64.rpm`
  `kesl-gui_12.5.0-<build number>_amd64.deb`
- 对于使用 64 位操作系统的 Arm® 处理器：
  `kesl-gui-12.5.0-<build number>.aarch64.rpm`
  `kesl-gui_12.5.0-<build number>_arm64.deb`
- 对于 Elbrus CPU：
  `kesl-gui-12.5.0-<build number>.e2k.rpm`
  `kesl-gui_12.5.0-<build number>_e2k.deb`

要在支持有限的操作系统（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）上安装 Kaspersky Endpoint Security 应用程序，请选择标记为 `OLD` 的分发包。

**用于使用 Kaspersky Security Center 远程安装应用程序的存档**

`kesl-12.5.0.<build number>.zip`

该存档还包含用户协议文本。

**用户协议文本**

- `ksn_license.<language ID>` 包含卡巴斯基安全网络声明的文本。
- `license.<language ID>` 包含最终用户授权许可协议的文本。最终用户授权许可协议规定了使用该应用程序的条款。

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。

# 与其他应用程序的兼容性

## 支持的 Kaspersky Security Center 版本

根据 Kaspersky Endpoint Security 的模式，您可以使用表中列出的 Kaspersky Security Center 版本管理应用程序。

| 模式 | Kaspersky Security Center 版本 |
| --- | --- |
| 标准模式下的 Kaspersky Endpoint Security | Kaspersky Security Center Windows 14.2、15.1。<br>使用 MMC 管理插件通过管理控制台进行管理，以及使用 Web 管理插件通过 Kaspersky Security Center Web Console 进行管理。<br>Kaspersky Security Center Linux 15.1、15.2、15.3、15.4、16.0、16.1、16.2、16.3。<br>使用 Web 管理插件通过 Kaspersky Security Center Web Console 进行管理。 |
| 标准模式下带有 Endpoint Detection and Response Optimum 组件的 Kaspersky Endpoint Security | Kaspersky Security Center Windows 15.1。<br>Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2。 |
| Light Agent 模式下的 Kaspersky Endpoint Security | Kaspersky Security Center Windows 15.1。<br>Kaspersky Security Center Linux 16.1、16.2、16.3。 |
| EDR Agent 模式下的 Kaspersky Endpoint Security | Kaspersky Security Center Windows 14.2、15.1。<br>Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2、16.3。 |

## Kaspersky Security for Virtualization Light Agent 的受支持版本

Kaspersky Endpoint Security 可以作为Kaspersky Security for Virtualization Light Agent 6.5的一部分用作Light Agent 。

### KATA 和 OSMP 平台上支持的解决方案版本

Kaspersky Endpoint Security 与以下版本的 基于 Kaspersky Anti Targeted Attack Platform 的解决方案和 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案兼容：

- Kaspersky Anti Targeted Attack Platform 6.0、6.1、7.0、7.1（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)，包括将文件发送到沙盒进行扫描的场景）。
- Kaspersky Anti Targeted Attack Platform 8.0（Kaspersky Network Detection and Response (KATA)，包括将文件发送到沙盒进行扫描的场景）。

  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。
- Open Single Management Platform（以下简称 OSMP）上的 Kaspersky Endpoint Detection and Response Expert (on-premises) 8.0、8.1，包括将文件发送到沙盒进行扫描的场景。

  有关 Kaspersky Endpoint Detection and Response Expert (on-premises) 的更多信息，请参阅 Kaspersky Endpoint Detection and Response Expert (on premise) 帮助。

### 支持的用于与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成的网络代理版本

要将应用程序与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成，您需要用于 Kaspersky Security Center 云控制台的特定版本的网络代理，这些版本在 Kaspersky Security Center 云控制台帮助 中说明。

### 与第三方解决方案的兼容性

EDR Agent 模式下的 Kaspersky Endpoint Security 可以与 Dr. Web 反病毒应用程序协同工作。

# 卡巴斯基解决方案之间的功能比较

Kaspersky Endpoint Security 包含在许多卡巴斯基多平台解决方案中。可用的应用程序功能取决于您从所在地区的服务提供商处购买的解决方案。

| 功能 | Kaspersky Next EDR Foundations | Kaspersky Next EDR Optimum | Kaspersky Next XDR Optimum | Kaspersky Next MXDR Optimum | Kaspersky Next EDR Expert | Kaspersky Next XDR Expert | Kaspersky Hybrid Cloud Security，桌面版 | Kaspersky Hybrid Cloud Security Enterprise 桌面版/CPU 版/服务器版 | Kaspersky Hybrid Cloud Security 核心版/CPU 版/服务器版 |
|---|---|---|---|---|---|---|---|---|---|
| 文件威胁防护 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 邮件威胁防护 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Web 威胁防护 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 网络威胁防护 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 防火墙管理 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 行为检测 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| BadUSB 攻击防护 | – | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 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 | – | – | – | – | – | ✓ | – | ✓ | – |
| 应用程序控制 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – |
| Web 控制 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 与 Kaspersky Unified Monitoring and Analysis Platform 整合 | – | – | – | – | – | ✓ | – | – | – |
| 与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成 | – | – | – | – | ✓ | ✓ | – | – | – |
| 与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成 | – | – | – | – | ✓ | ✓ | – | – | – |
| Kaspersky Endpoint Detection and Response Optimum | ✓ | ✓ | ✓ | ✓ | – | – | – | – | – |
| 与 Kaspersky Managed Detection and Response 整合 | – | – | – | ✓ | – | – | – | – | – |

# 部署和初始配置

您可以按照此方案部署 Kaspersky Endpoint Security 应用程序并做好使用准备。

## 1 选择应用程序使用模式

在 卡巴斯基官方网站 或从我们的某个合作伙伴处购买卡巴斯基解决方案后，您将在购买期间指定的电子邮件地址收到一封邮件。此消息将包含激活码以及有关如何获取密钥文件的信息。如果您的组织不支持使用激活码在线激活应用程序，您可能需要密钥文件。

您选择的解决方案决定了您可以使用该应用程序的模式：

- 如果您拥有 Kaspersky Endpoint Security 授权许可，则可以在标准模式下使用该应用程序。
- 如果您拥有 Kaspersky Security for Virtualization Light Agent 授权许可，则可以在 Light Agent 模式下使用该应用程序。
- 如果您拥有 Kaspersky Endpoint Detection and Response Expert (on-premises) 授权许可，则可以在 EDR agent 模式下使用该应用程序。

应用程序部署取决于所选模式。

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

## 2 准备环境

根据您的基础设施完成必要的准备操作。

## 3 选择系统事件拦截机制

如果设备的操作系统支持 fanotify，则在安装期间，您可以选择用于拦截系统事件的机制。

## 4 准备分发包

下载安装应用程序所需的文件。您需要哪些文件取决于受保护设备的操作系统和应用程序部署方法。

## 5 Kaspersky Security Center 中的准备操作

在 Kaspersky Security Center 中执行准备操作。我们建议使用 Kaspersky Security Center 集中管理您组织的防护。如果您将在 EDR agent 模式或 Light Agent 模式下使用 Kaspersky Endpoint Security，则还需要 Kaspersky Security Center。

## 6 安装应用程序

使用适合您组织需求的方法将应用程序安装到设备上：

- 使用 Kaspersky Security Center 安装应用程序
- 使用命令行安装应用程序

## 7 在某些操作系统中安装后执行其他配置步骤

某些 Linux 操作系统在安装 Kaspersky Endpoint Security 后需要额外配置。

# 模式和部署方案

Kaspersky Endpoint Security 是众多卡巴斯基解决方案的一部分。您选择的解决方案决定应用程序的运行模式和部署方案。

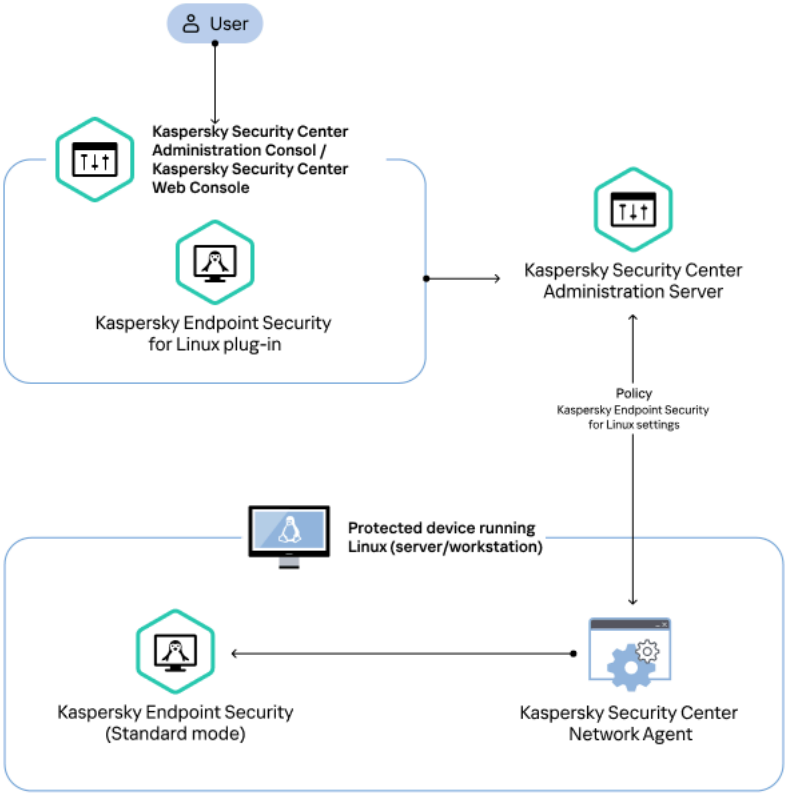
### 标准模式

应用程序的默认模式。Kaspersky Endpoint Security 为 Linux 工作站和服务器提供针对各种类型的威胁、网络攻击和欺诈的全面保护。

在此模式下，应用程序使用设备保护和控制组件（例如 文件威胁防护 或 行为检测）以及 内置代理 来抵御高级威胁和定向攻击。

您可以在此模式下安装该应用程序作为 Kaspersky EPP 解决方案（Endpoint Protection Platform)的一部分。例如，标准模式下的 Kaspersky Endpoint Security 是 Kaspersky Endpoint Security for Business 的一部分。

Kaspersky Endpoint Security 的主流部署方案是通过 Kaspersky Security Center 集中部署。在每台受保护设备上，您需要安装 Kaspersky Endpoint Security 和 Kaspersky Security Center 网络代理组件。该组件将设备连接到 Kaspersky Security Center 管理服务器，并允许使用 Kaspersky Security Center 管理设备。




Kaspersky Endpoint Security 在标准模式下的部署方案

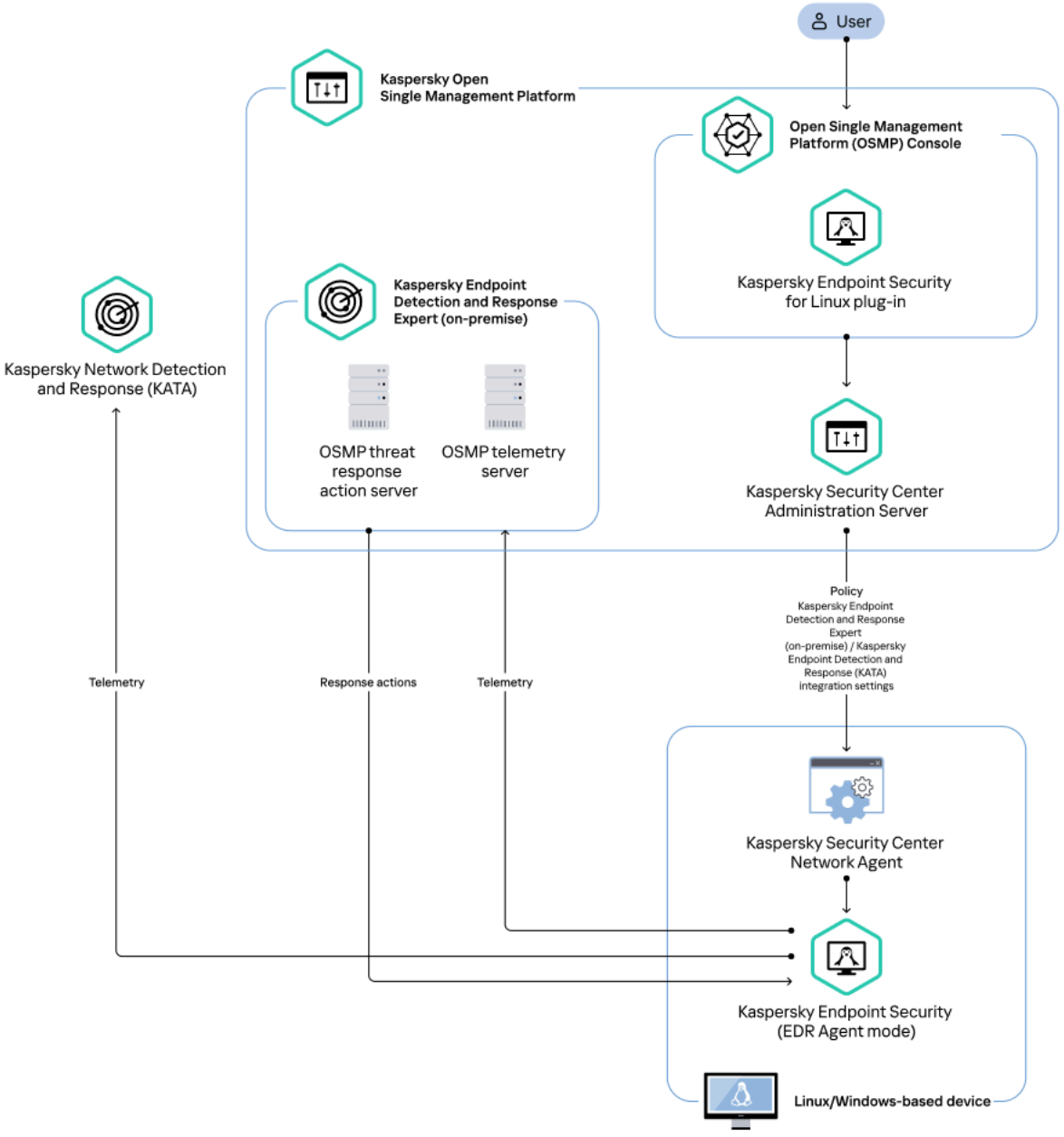
## Endpoint Detection and Response Agent (EDR Agent) 模式

此模式允许将卡巴斯基 Detection and Response 解决方案与第三方反病毒解决方案一起部署。Detection and Response 解决方案包括：

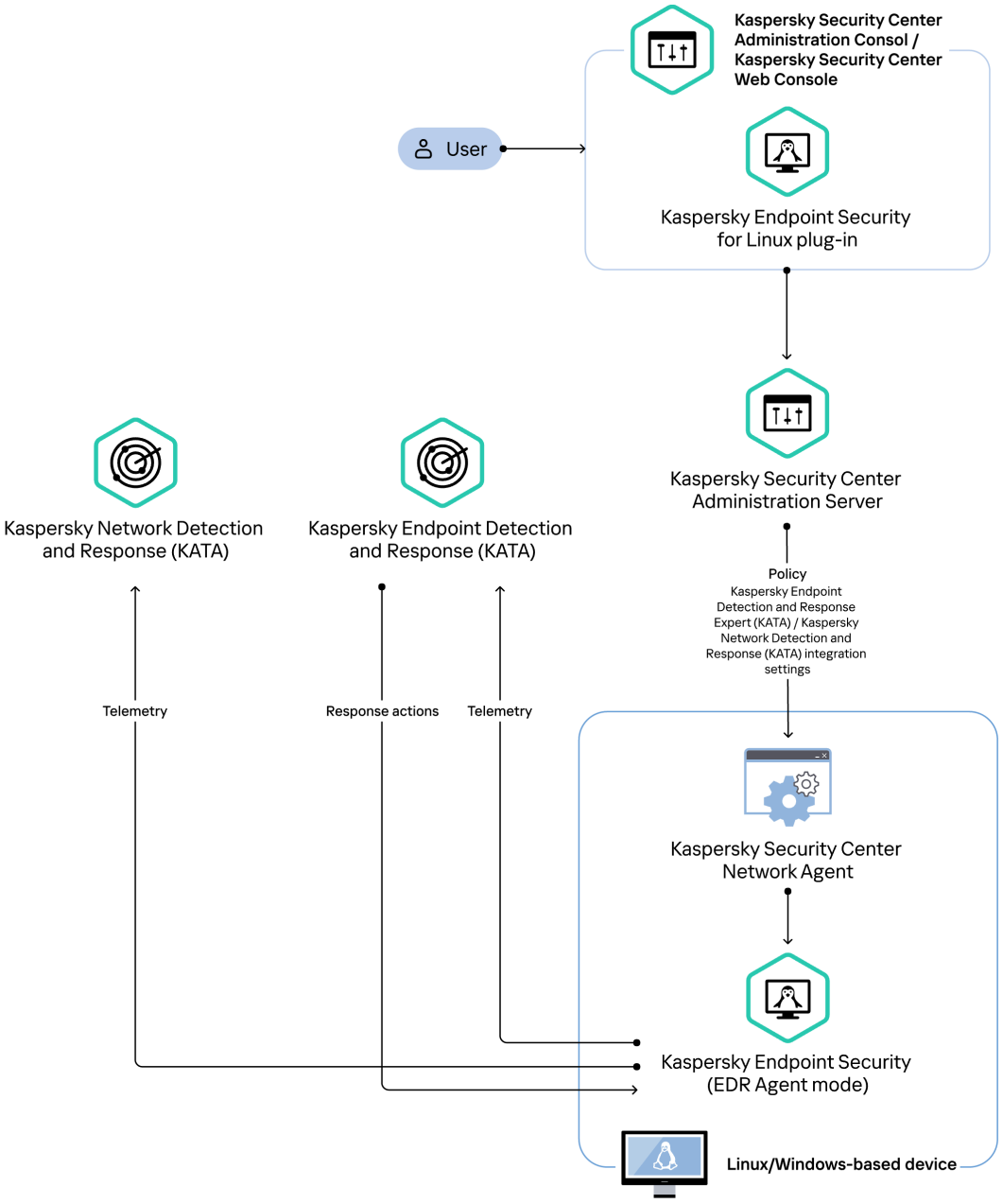
- Open Single Management Platform 上的 Kaspersky Endpoint Detection and Response Expert (on-premises)（以下也称为“OSMP”）。
- Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 基于 Kaspersky Anti Targeted Attack Platform（以下也称为“KATA”）。

在 EDR Agent 模式下，文件威胁防护或 Web 威胁防护等保护和控制组件不可用。设备由第三方反病毒应用程序保护。EDR 代理持续监控这些设备上运行的进程、打开的网络连接和修改的文件，并与 Detection and Response 解决方案交互，以抵御高级威胁和定向攻击。

要使 Kaspersky Endpoint Security 在 EDR Agent 模式下运行，您必须部署相应的基础架构；有关详细信息，请参阅您所选 Detection and Response 解决方案的帮助。请参阅已知问题和限制文章，详细了解 EDR Agent 模式的特殊方面。




Kaspersky Endpoint Security 在 EDR Agent 模式下与 Kaspersky Endpoint Detection and Response Expert (on-premises) 配合使用的部署方案



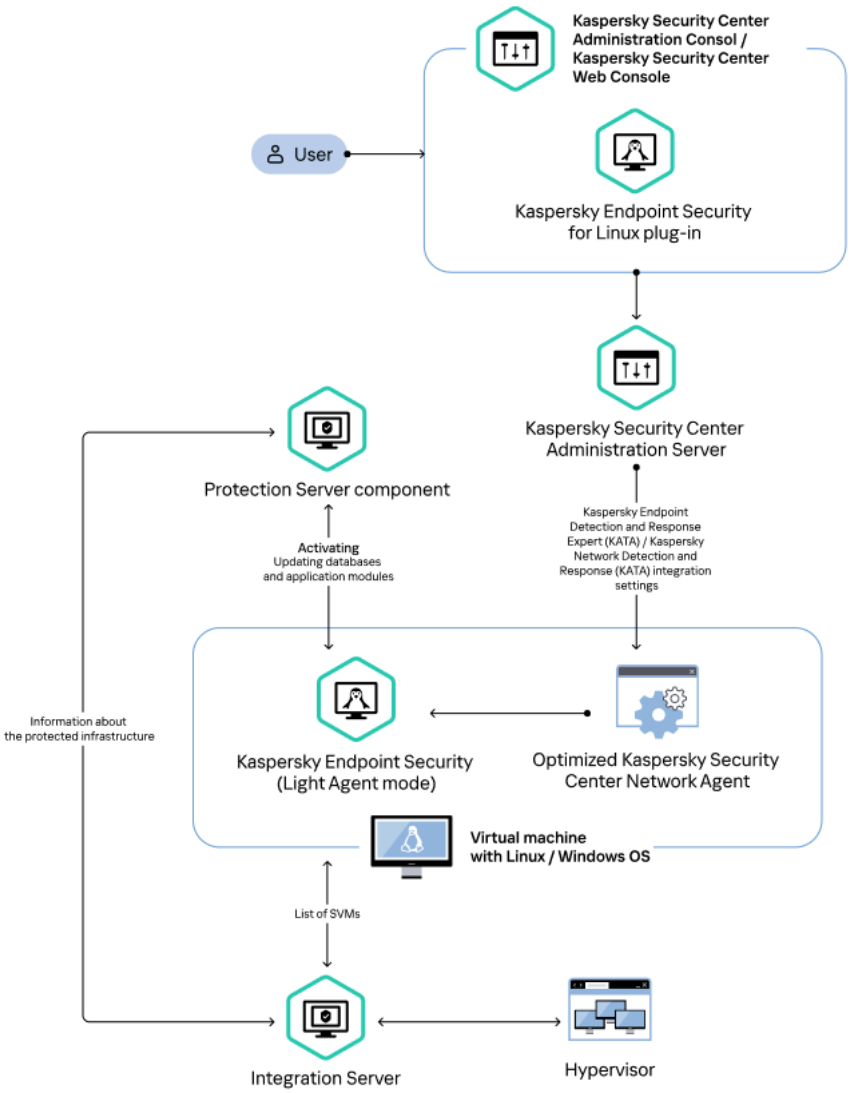

Kaspersky Endpoint Security 在 EDR Agent 模式下与 Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 配合使用的部署方案

## Light Agent 模式

Light Agent 模式下的 Kaspersky Endpoint Security 是 Kaspersky Security for Virtualization Light Agent 解决方案的一部分，该解决方案用于保护运行 Linux 客户机操作系统的虚拟机。

此模式中提供的保护和控制组件与标准模式中相同。不同之处在于，对象的病毒和其他恶意软件扫描、授权许可密钥添加以及数据库和模块更新均由安装在单独虚拟机上的特殊解决方案组件 SVM（Secure Virtual Machine）执行。这有助于减轻虚拟机监控程序的负载，因为 Light Agent 模式下的应用程序使用 SVM 的资源而不是虚拟机的资源来保护基础架构。

要使 Kaspersky Endpoint Security 在 Light Agent 模式下运行，您必须部署相应的基础架构；有关更多信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。在已知问题和限制文章中了解有关 Light Agent 模式特殊之处的更多信息。




Kaspersky Endpoint Security 在 Light Agent 模式下的部署方案

选择应用程序模式后，您可以返回部署场景，并从准备环境步骤继续。

# 准备应用程序安装环境

## 准备基础架构

### Kaspersky Security Center

如果您打算使用 Kaspersky Security Center 集中管理应用程序，请在您的基础架构中安装 Kaspersky Security Center。如果您已安装 Kaspersky Security Center Windows 并计划迁移到 Kaspersky Security Center Linux，请遵循以下说明：将数据迁移到 Kaspersky Security Center Linux。

### EDR Agent 模式下的 Kaspersky Endpoint Security

要使 Kaspersky Endpoint Security 在 EDR Agent 模式下运行，您必须部署相应的基础架构；有关详细信息，请参阅您所选 Detection and Response 解决方案的帮助。

**Light Agent 模式下的 Kaspersky Endpoint Security**

要使 Kaspersky Endpoint Security 在 Light Agent 模式下运行，您需要部署 Kaspersky Security for Virtualization Light Agent 解决方案：

1. 安装 Kaspersky Security for Virtualization Light Agent 解决方案的组件，即 Integration Server 和 Protection Server。
2. 通过激活解决方案并为 Protection Server 和 Light Agent 配置数据库更新，使 Protection Server 做好运行准备。

   有关解决方案组件的安装和配置的更多详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。
3. 确保要保护的虚拟机满足Light Agent 模式要求。
4. 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。Light Agent 使用的端口列于Kaspersky Security for Virtual Environment Light Agent 帮助中。

Kaspersky Endpoint Security 的 Light Agent 模式不支持基于 Arm 架构的设备以及配备 Elbrus CPU 的设备。

## 准备设备以进行安装

- 检查您的设备是否满足应用程序的硬件和软件要求。
- 如果您想以标准模式或 Light Agent 模式安装 Kaspersky Endpoint Security，请确保您的设备上未安装任何第三方反病毒软件。在 EDR Agent 模式下，Kaspersky Endpoint Security 可以与 Dr. 应用程序协同工作。Web 反病毒应用程序。
- 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，请将其卸载。
- 确保您的设备上已安装 iptables 实用程序。应用程序需要使用 iptables 实用程序来拦截网络流量。
- 确保 root 是以下目录的所有者，并且只有所有者拥有写入权限：/var、/var/opt、/opt、/usr/bin、/usr/lib、/usr/lib64。这是应用程序启动和正常运行所必需的。
- 当应用程序运行时，操作系统使用的文件描述符数量可能会显著增加。确保文件描述符数量限制足够高。要检查限制，请运行命令`cat /proc/sys/fs/file-max`。通常，我们建议通过在 /etc/sysctl.conf 文件中指定`fs.file-max=9223372036854775807` 来禁用该限制。完成此更改后，请重启操作系统。
- 确保操作系统中设置了 `kernel.yama.ptrace_scope=0`。`kernel.yama.ptrace_scope` 参数的其他值可能会影响 Kaspersky Endpoint Security 应用程序的运行；有关更多详细信息，请参阅已知问题和限制部分。

此外，要安装应用程序的图形界面：

- 您安装的 kesl-gui 软件包的版本必须与 kesl 软件包的版本匹配。
- 要使 Kaspersky Endpoint Security 的图形界面正常工作，您的操作系统中必须安装 Zenity 实用程序。
- 如果您的设备可以访问软件包管理器的存储库，则在安装应用程序的图形界面期间，所有必要的依赖项都会自动安装。如果设备位于私有网段且无法访问软件包管理器的存储库：

  1. 检查参考设备上的依赖项列表（libice6、libsm6、zlib1g、kesl）。
  2. 执行下列操作之一：
     - 在安装图形界面之前，请先将软件包下载到所有设备，然后使用软件包管理器进行安装。
     - 确保在安装图形界面期间将软件包下载到设备。

### MMC 插件支持的附加要求

如果您打算使用 Kaspersky Security Center 管理控制台来管理应用程序，请在安装了管理服务器的设备上安装 Microsoft® Visual C++® 2015 Redistributable Update 3 RC（请参见 https://www.microsoft.com/en-us/download/details.aspx?id=52685）。这是 Kaspersky Endpoint Security MMC 管理插件正常工作所必需的。

### 某些操作系统的附加要求

**封闭软件环境模式下的 Astra Linux**

**安装兼容包**

在以下情况下，您需要安装兼容包：

- 在封闭软件环境模式下安装应用程序之前。
- 在应用程序已安装的情况下，将操作系统切换到封闭软件环境模式时。

安装软件包

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

这样即可在 Astra Linux Special Edition 操作系统（Arm 架构的更新 4.7 以及更新 1.6、1.7 和 1.8）中以封闭软件环境模式运行该应用程序。

**重新允许 ptrace**

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。为了使 Kaspersky Endpoint Security 正常工作，建议在安装 Astra Linux 时解除对 ptrace 的阻止。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**”）。

#### SUSE Linux Enterprise Server 15

在将应用程序安装到运行 SUSE Linux Enterprise Server 15 操作系统的设备上之前，必须安装 insserv-compat 软件包。

#### 封闭软件环境模式下的 ALT SP

在封闭软件环境模式下将应用程序安装到运行 ALT SP 操作系统的设备上之前：

1. 禁用封闭软件环境模式：

```
integrity-remover
```

2. 创建 kesl 组，以便进一步更改 IMA 策略：

```
groupadd kesl
```

3. 查找所创建组的唯一标识符（GID）：

```
cat /etc/group | grep kesl
```

4. 使用该实用程序编辑 IMA 策略，将 kesl 组从应用程序组件完整性检查中排除，以确保应用程序正常工作。为此，请执行下列操作：

   a. 复制 /usr/share/integrity/policy 文件：

   ```
   cp /usr/share/integrity/policy /etc/integrity/policy
   ```

   b. 在文本编辑器（例如 vim）中打开 /etc/integrity/policy 文件进行编辑：

   ```
   vim /etc/integrity/policy
   ```

   c. 在 `dont_measure fsmagic=0xf97cff8c` 行之后（通常，这是 `dont_measure` 部分的最后一行），添加以下行：

   ```
   dont_measure fgroup=<GID>
   ```

   其中，`<GID>` 是在这些说明的步骤 2 中创建的组的唯一 ID。

   d. 在 `dont_appraise fsmagic=0x27e0eb` 行之后（通常，这是 `dont_appraise` 部分的最后一行），添加以下行：

   ```
   dont_appraise fgroup=<GID>
   ```

   其中，`<GID>` 是在这些说明的步骤 2 中创建的组的唯一 ID。

   e. 保存更改。

5. 在 /usr/sbin/integrity-sign 文件中，编辑 list_all_files 函数，将 Kaspersky Endpoint Security 应用程序添加到允许在封闭环境模式下运行的应用程序允许列表中。为此，请执行下列操作：

   a. 在文本编辑器（例如 vim）中打开 /usr/sbin/integrity-sign 文件进行编辑：

   ```
   vim /usr/sbin/integrity-sign
   ```

   b. 找到 list_all_files 函数，在函数体中，在以`find -P`开头的行中，将 Kaspersky Endpoint Security 应用程序在 /var/opt 和 /opt 下的目录添加到每个目录枚举的末尾。

   c. 保存更改。

在应用程序初始配置期间，不要启动应用程序数据库更新。

安装完成后，启用封闭软件环境模式并执行启动应用程序所需的操作。

**OSnova**

如果您打算使用 Kaspersky Security Center 安装和管理应用程序，请在安装应用程序之前准备设备以安装网络代理：

1. 打开 /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf 文件进行编辑，并在 `[Login]` 部分中注释掉 KillUserProcesses=yes 行。

   ```
   #KillUserProcesses=yes
   ```

2. 打开 /usr/lib/NESS/pam-user-session 文件进行编辑，并注释掉 loginctl terminate-session "$XDG_SESSION_ID" 行。

   ```
   #loginctl terminate-session "$XDG_SESSION_ID"
   ```

**支持 SELinux 的操作系统**

如果您的操作系统中未安装 semanage 实用程序，请在安装应用程序之前根据软件包管理器安装 policycoreutils-python 或 policycoreutils-python-utils 软件包。

policycoreutils-python-utils 软件包可用于以下软件包管理器：适用于 Fedora、Debian、Ubuntu 以及 RHEL 7 和更高版本的 dnf、apt 和 yum。

policycoreutils-python 软件包适用于以下类型的软件包管理器：适用于 CentOS/RHEL 7 及更早版本的 yum。

**麒麟操作系统**

在麒麟操作系统设备上安装应用程序之前：

1. 在 UKUI（Ubuntu Kylin 用户界面）中，关闭 Firewall。为此，请转到 **麒麟安全中心** → **防火墙和网络保护**部分，并在 **Firewall** 下，禁用 **公共网络**和 **专用网络**切换开关。

2. 在 UKUI 中，禁用应用程序网络控制。为此，请转到 **麒麟安全中心** → **防火墙和网络保护**部分，并在 **应用程序网络控制**下，选择 **禁用**。

3. 在 UKUI 中，禁用应用程序来源检查。为此，请转到 **麒麟安全中心 → 应用程序保护**部分，并在 **应用程序来源检查**下，选择 **禁用**。

4. 禁用 KYSEC 安全机制。为此，请在终端中执行以下操作：

   a. 检查当前状态：

   ```
   getstatus
   ```

   b. 禁用 KYSEC 安全机制：

   ```
   setstatus disable -p
   ```

   c. 确认 KYSEC 安全机制已禁用：

   ```
   getstatus
   ```

5. 卸载内置反病毒应用程序。为此，请在终端中运行以下命令：

   ```
   sudo dpkg -P pksav
   ```

6. 如果您的设备上安装了 Qaxsafe 反病毒软件，则需要将其卸载。为此，请执行下列操作：

   a. 禁用自我保护：

      1. 在任务栏的通知区域中找到应用程序图标，然后双击该应用程序图标以打开上下文菜单。
      2. 在上下文菜单中，选择 **设置 → 保护中心**。
      3. 此时会打开一个窗口；在该窗口中，取消选中 **启用自我保护** 复选框，并在出现提示时输入密码。

   b. 卸载 Qaxsafe 反病毒软件。为此，请在终端中运行以下命令：

   ```
   sudo dpkg -P qaxsafe
   ```

   c. 删除所有残留文件。为此，请在终端中运行以下命令：

   ```
   sudo rm -rf /opt/qaxsafe
   ```

**不支持 fanotify 的操作系统**

在继续安装应用程序之前，请确保设备上已安装以下软件：

- 用于编译应用程序和运行任务的软件包（gcc、binutils、glibc、glibc-devel、make）
- 包含操作系统内核头文件的软件包，用于编译 Kaspersky Endpoint Security 模块

实用文章

麒麟操作系统问题排查

准备好安装环境后，您可以返回部署场景，并从 选择系统事件拦截机制 步骤继续。

# 选择系统事件拦截机制

为确保正常运行，应用程序必须拦截文件操作和进程启动的系统事件。所有应用程序模式（标准模式、Light Agent 模式和 EDR 代理模式）都需要系统事件拦截。如果应用程序不使用系统事件拦截，则不会执行文件实时扫描，从而降低设备的保护级别。

## 系统事件拦截机制

应用程序可以使用以下机制来拦截系统事件：

- **基于 fanotify 的系统拦截机制。** *Fanotify* 是 Linux 内核的一个子系统，用于监控文件系统中的事件（例如打开、读取、写入或关闭文件），并允许应用程序实时拦截这些事件。
- **基于可更新内核模块的拦截机制。** *可更新内核模块*与基于 fanotify 技术的系统拦截机制协同工作。这使 Kaspersky Endpoint Security 能够通过在 kernel space 而非 user space 中处理系统事件，优化对文件操作和进程启动的拦截。可更新内核模块会在文件被打开、重命名或修改时拦截文件操作。由于采用了文件和进程扫描结果缓存，应用程序性能得到了提升。

  可更新内核模块还用于以下任务和组件：

  - 文件威胁防护
  - 反加密
  - 漏洞利用防御
  - 行为检测
  - 应用程序控制
  - 对象的执行防护（与 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Optimum 集成时）

  通过使用可更新内核模块，您可以更精细地配置全局排除项。基于 fanotify 技术的拦截机制允许完全排除对指定挂载点的文件操作拦截。使用可更新内核模块，您可以排除设备上挂载的特定本地或远程目录。

  可更新内核模块包含在应用程序的分发包中。
- **适用于没有 fanotify 的操作系统的文件威胁防护内核模块。**如果设备上的操作系统不支持 fanotify 技术（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6），应用程序会编译并使用特殊模块来拦截系统事件。当启动文件威胁防护时，如果所有依赖项和构建工具都可用，则会自动编译此模块。

如何选择系统事件拦截机制

如果操作系统支持 fanotify，您可以在部署应用程序时选择系统事件拦截机制：仅 fanotify，或可更新内核模块加 fanotify。默认设置为 fanotify。安装后，您可以在应用程序设置中更改系统事件拦截机制。

对于不支持 fanotify 的操作系统，无法选择拦截机制。

如果操作系统满足安装可更新内核模块的要求，则应用程序可以使用基于可更新内核模块的拦截机制。

**可更新内核模块的安装要求**

要安装和使用可更新内核模块，设备必须安装以下 64 位操作系统中的一种：

- Astra Linux Special Edition RUSB.10015-01（operational update 1.6.5、1.6.6）。
- Astra Linux Special Edition RUSB.10015-01（operational update 1.7.3、1.7.4、1.7.6、1.7.7、1.7.8、1.7.9）。
- Astra Linux Special Edition RUSB.10015-01（operational update 1.8.2、1.8.3、1.8.4、1.8.5）。

  如果在基本模式下使用 Kaspersky Endpoint Security 应用程序，则可更新内核模块可在封闭软件环境模式下在运行 Astra Linux 操作系统的设备上使用。

- CentOS 7.x。
- CentOS 8.x。
- Debian GNU/Linux 12.7、12.8、12.9、12.10、12.11、12.12。
- Red Hat Enterprise Linux 7.4。
- Red Hat Enterprise Linux 8.10。
- SberLinux 8.10。
- SberLinux 9.0.1。
- SberLinux 9.1。
- SberLinux 9.6。
- SberLinux 9.7。
- SberOS 3.4。
- SberOS 3.5。
- Ubuntu 16.04 LTS。
- Ubuntu 18.04 LTS。
- Ubuntu 20.04 LTS。

- Ubuntu 22.04 LTS。
- Ubuntu 24.04 LTS。
- ALT SP Workstation 版本 10。
- ALT SP Server 版本 10。
- ALT Education 10。
- ALT Workstation 11。
- ALT Server 11。
- ALT Education 11。
- RED OS 7.3。
- RED OS 8.0。
- ROSA "Cobalt" 7.9 Workstation。
- ROSA "Cobalt" 7.9 Server。
- ROSA "Chrome" 12 Workstation。
- ROSA "Chrome" 12 Server。

不支持 32 位操作系统、Arm 架构操作系统和 Elbrus 架构操作系统。

可更新内核模块可能会与某些版本的 Linux 内核和某些第三方应用程序发生冲突。

## 检查是否可以安装可更新内核模块

可更新内核模块的版本不依赖于 Kaspersky Endpoint Security 的版本。作为 Kaspersky Endpoint Security 数据库和应用程序模块更新的一部分，已更新内核模块的功能会定期扩展。因此，上面列出的支持的操作系统可能并不完整。要验证您的设备是否满足安装可更新内核模块的要求，请使用卡巴斯基 ULKM 工具。

**如何使用 Web Console 或管理控制台进行远程检查**

1. 进入应用程序下载页面，在“**Kaspersky Endpoint Security for Linux**”部分下载 ulkmtool.zip 压缩文件。
2. 创建该实用程序的安装包。

**如何在 Web Console 中创建安装包**

1. 将下载的 ulkmtool.zip 压缩文件放入 Kaspersky Security Center 管理服务器可访问的文件夹。
2. 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。
3. 单击“**添加**”按钮。
   创建安装包的向导将启动。
4. 选择“**从文件创建安装包**”作为安装包创建方法。
5. 输入新安装包的名称，点击“**浏览**”按钮并指定已下载的 ulkmtool.zip 压缩文件的路径。
6. 结束向导。

   安装包将被创建并添加到安装包列表中。

**如何在管理控制台中创建安装包**

1. 将 ulkmtool.zip 压缩文件解压到可供 Kaspersky Security Center Administration Server 访问的一个文件夹中。
2. 在控制台树中，选择**附加 → 远程安装 → 安装包**。
   将打开管理服务器上可用的安装包列表。
3. 单击“**创建安装包**”按钮。
   创建安装包的向导将启动。
4. 点击“**创建卡巴斯基应用程序的安装包**”按钮。
5. 指定新安装包的名称并继续执行向导的下一步。
6. 点击“**浏览**”按钮并指定 ulkmtool.kud 文件的路径。该文件位于 ulkmtool.zip 压缩文件所解压到的文件夹中。
   继续执行向导的下一步。
7. 等待文件下载完成并结束向导。

   安装包将被创建并添加到安装包列表中。

3. 在要检查是否满足可更新内核模块要求的设备上安装 Kaspersky Security Center 网络代理。有关详细信息，请参见 Kaspersky Security Center 帮助。
4. 在 Kaspersky Security Center Web Console 或管理控制台中，在要检查其是否满足可更新内核模块要求的设备上创建并运行远程安装任务。在任务设置中，选择您创建的安装包。
   每个设备的任务结果会显示该设备是否支持安装和运行可更新内核模块。

根据任务结果，每个设备将获得一个标签：

- *UpdatableKernelModule=No* 表示设备不支持安装可更新内核模块。
- *UpdatableKernelModule=Yes* 表示设备满足安装和运行可更新内核模块的要求。

您可以使用这些标签来创建设备选择方案。例如，您可以选择满足可更新内核模块安装要求的设备，并在这些设备上安装带有可更新内核模块的 Kaspersky Endpoint Security。

**如何在设备本地进行检查**

1. 进入应用程序下载页面，在“**Kaspersky Endpoint Security for Linux**”部分下载 ulkmtool.zip 压缩文件。
2. 在要检查是否满足可更新内核模块要求的设备上安装 Kaspersky Security Center 网络代理。有关详细信息，请参见 Kaspersky Security Center 帮助。
3. 在要扫描的设备上本地运行 Kaspersky ULKM tool 实用程序。

   ```
   ulkmtool --check remote
   ```

4. 检查返回代码。

   ```
   echo $?
   ```

   该实用程序在命令行返回以下代码：

   *0 = Success* 表示设备满足安装和运行可更新内核模块的要求。

   *1 = NotSupported* 表示设备不支持安装可更新内核模块。

## 检查可更新内核模块的状态

在 Kaspersky Security Center Web Console 或管理控制台中，您可以检查安装了 Kaspersky Endpoint Security 的设备上的可更新内核模块状态。为此，您可以查看分配给设备的标签：

- *UpdatableKernelModule=Use* 表示可更新内核模块已在设备上安装并运行。
- *UpdatableKernelModule = Error*表示设备上安装了可更新内核模块，但是启动该模块时发生错误，模块未运行。

有关查看分配给设备的标签的详细信息，请参阅 Kaspersky Security Center 帮助。

## 安全启动支持

可更新内核模块支持 Secure Boot。要在启用了 Secure Boot 的操作系统上使用基于可更新内核模块的拦截机制，您需要将用于签署该模块的 Kaspersky Endpoint Security 公共证书添加到操作系统，然后重新启动操作系统。

**下载证书**

**为 Ubuntu 添加证书的示例**

1. 确保已在您的操作系统中启用安全启动：

```
mokutil --sb-state
```

2. 使用 mokutil 实用程序将已下载的证书添加到您的操作系统：

```
mokutil --import <path to certificate>
```

3. 重新启动 Kaspersky Endpoint Security。

4. 运行以下命令，检查可更新内核模块是否正在工作：

```
kesl-control --app-info
```

选择系统事件拦截机制后，您可以返回部署场景，并从准备分发包步骤继续。

# 准备分发包

*Kaspersky Endpoint Security 分发包*是一组用于安装和更新应用程序的文件，以及用户协议文本（最终用户授权许可协议、隐私策略和卡巴斯基安全网络声明）。您还可以单独下载包含图形界面的分发包，以便在本地管理和监控应用程序。

您需要使用分发包来创建安装包，以便使用 Kaspersky Security Center 在企业网络中的设备上部署应用程序，以及使用命令行部署应用程序。

要使用 Kaspersky Security Center 进行部署，您还需要*用于远程安装应用程序的分发包*。此分发包包含远程部署应用程序所需的文件以及用户协议文本。

> 用户协议文本可在卡巴斯基网站（**最终用户授权许可协议**区域）以及安装应用程序后的 `/opt/kaspersky/kesl/doc/` 目录中获取。

在创建安装包步骤中，您可以选择用于自行部署 Kaspersky Endpoint Security 或使用 Kaspersky Security Center 部署 Kaspersky Endpoint Security 的分发包。

## 如何选择用于部署 Kaspersky Endpoint Security 的分发包

分发包的选择取决于以下因素：

- Kaspersky Endpoint Security 版本：已认证或未认证
- 部署方法：使用 Kaspersky Security Center 或使用命令行
- 取决于操作系统的包格式

- 操作系统架构和 CPU 类型
- Kaspersky Endpoint Security 管理方法
- 是否需要安装应用程序的图形用户界面

**1 确定应用程序版本：已认证或未认证**

- 如果您需要**已认证**版本，请从企业应用程序支持生命周期页面下载分发包集。
  已认证版本包含主应用程序文件和图形界面文件（`kesl` 目录）、用于远程安装应用程序的存档（`remote install` 目录）、MMC 插件（`SCPlugin`）和 Web 插件（`web plugin`）。
  转至步骤 3。
- 如果您需要**未认证**版本，请转到下一步。

**2 确定部署方法：使用 Kaspersky Security Center 或使用命令行**

要**使用 Kaspersky Security Center 部署**，请从以下来源之一下载分发包：

- 从卡巴斯基网站
- 如果您有 Kaspersky CompanyAccount，则通过向技术支持提交请求

要**使用命令行部署**，请从卡巴斯基网站下载分发包：

- 主应用程序分发包（`Distributive`）
- 如有必要，包含图形用户界面的分发包（`Product GUI`）

如果您想从卡巴斯基网站下载分发包，您将需要以下文件：

- 主应用程序分发包（`Distributive`）
- 如有必要，包含图形用户界面的分发包（`Product GUI`）
- 用于使用 Kaspersky Security Center 远程安装应用程序的分发包（**附加分发包** → `Files for Product remote installation`）
- Kaspersky Security Center 网络代理的分发包（Kaspersky Security Center 分发部分 → `Network agent`）

> 应用程序的分发包对于所有本地化版本都是相同的。Kaspersky Endpoint Security 的语言是在应用程序初始配置期间选择的。本地化支持取决于操作系统中安装的语言。

**3 根据受保护设备的操作系统确定软件包格式**

| 操作系统 | 软件包格式 |
| --- | --- |
| Debian、Ubuntu、Astra Linux、Linux Mint | `.deb` |
| Red Hat Enterprise Linux、CentOS、Oracle Linux、RED OS、SUSE Linux Enterprise、openSUSE、Rocky Linux、AlmaLinux、ALT 系列操作系统、GosLinux、Rosa 系列操作系统、Amazon Linux 2023 | `.rpm` |

如果您的操作系统未列出，请根据操作系统的文档选择软件包格式。

**4 确定操作系统架构和 CPU 类型**

| CPU 类型和操作系统位数 | 分发包 |
| --- | --- |
| Arm CPU，64 位操作系统 | `arm64`<br>`aarch64` |
| Elbrus CPU | `e2k` |
| 其他处理器，32 位操作系统 | `i386` |
| 其他处理器，64 位操作系统 | `x86_64`<br>`x64`<br>`amd64` |

要在支持有限的操作系统（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）上安装 Kaspersky Endpoint Security 应用程序，请选择标记为 `OLD` 的分发包。

以应用程序文档中未描述的方式或技术支持未推荐的方式在您的设备上编辑该应用程序的配置文件，可能会导致应用程序和操作系统性能下降及出现故障、设备的防护能力降低、数据无法访问并损坏，还可能会开启向 KSN 发送额外统计信息的功能。

准备好分发包后，您可以返回部署方案，并从 Kaspersky Security Center 中的准备工作 步骤继续。

# Kaspersky Security Center 中的准备操作

在安装 Kaspersky Endpoint Security 应用程序之前，建议您在 Kaspersky Security Center 中执行以下操作。

## 1 配置设备的管理组

要使用 Kaspersky Security Center 管理该应用程序，您需要将安装了该应用程序的设备放入管理组。默认情况下，Kaspersky Security Center 会将所有已安装管理代理并连接到管理服务器的设备移至 **未分配的设备** 组。

建议预先在管理组中配置设备自动分配规则，并根据设备的类型将设备分配到组中，即为每种设备类型创建单独的组。这样，您可以根据设备应用不同的应用程序设置。

您也可以手动将设备放入管理组。

## 2 网络代理的安装和初始配置

网络代理有助于设备连接到 Kaspersky Security Center 管理服务器。必须在将连接到 Kaspersky Security Center 的每台设备上安装它。

1. 准备您的 Linux 设备以安装网络代理。该过程取决于操作系统。
2. 执行网络代理的安装和初始配置。有关说明，请参见 Kaspersky Security Center 帮助。

因此，安装了网络代理的设备会显示在与为这些设备配置的移动规则相对应的组中。如果您尚未配置任何移动规则，设备将显示在 **未分配的设备** 组中。

## 3 安装 Kaspersky Endpoint Security 管理插件

根据您使用的 Kaspersky Security Center 管理控制台，安装 Kaspersky Endpoint Security 管理插件：

- **Kaspersky Endpoint Security 管理 MMC 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。

  **如何安装 Kaspersky Endpoint Security MMC 插件**

  > 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：*

  1. 从 应用程序下载页面 的 **Kaspersky Endpoint Security for Linux** 部分（**构建 → 管理插件**）下载 klcfginst.msi 文件。
  2. 在安装 Kaspersky Security Center 管理控制台的设备上，运行 klcfginst.msi 文件。

  安装后，MMC 管理插件将显示在 Kaspersky Security Center 管理服务器属性中已安装的 MMC 管理插件列表中。

  *如要查看已安装的管理 MMC 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：
     - 打开 **管理服务器 <服务器名称>** 节点的上下文菜单，然后选择 **属性** 项。
     - 在 **管理服务器** 部分中，单击 **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 的管理 MMC 插件：**Kaspersky Endpoint Security <版本号> for Linux**。

如果您使用 Kaspersky Security Center 管理控制台来管理 Kaspersky Endpoint Security 应用程序，并且安装了该应用程序的多个版本，则需要为每个版本的 Kaspersky Endpoint Security 应用程序安装一个管理插件。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。

- **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。Web 插件安装在已安装 Kaspersky Security Center Web Console 的设备上。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。

  **如何安装 Kaspersky Endpoint Security Web 插件**

  您可以通过以下方式安装 Web 插件：

  - 使用 Kaspersky Security Center Web Console 的快速启动向导。

    首次将 Kaspersky Security Center Web Console 连接到管理服务器时，Kaspersky Security Center Web Console 会自动提示您运行快速启动向导。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 → 快速启动向导**）。快速启动向导还可以检查已安装的 Web 插件是否为最新，并下载必需的更新。有关 Kaspersky Security Center Web Console 快速启动向导的详细信息，请参阅 Kaspersky Security Center 帮助。

  - 手动安装，使用卡巴斯基 Web 插件列表中的分发包或来自文件的分发包。

  *如要从 Kaspersky Security Center 手动安装 Kaspersky Endpoint Security Web 插件：*

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

     已安装的 Web 插件列表将打开。

  2. 单击“**添加**”按钮。

     这将打开可用管理插件列表。当新版本的 Web 插件发布后，该列表会自动更新。

  3. 在可用插件列表中，选择 **Kaspersky Endpoint Security <version number> for Linux Web 插件**。

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

  5. 等待安装完成，然后在信息窗口中单击“**确定**”。

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

  *如要从文件手动安装 Kaspersky Endpoint Security Web 插件：*

  1. 从 应用程序下载页面 的 **Kaspersky Endpoint Security for Linux** 部分（**附加分发包 → Web Console 插件**）下载包含 Web 插件的压缩包。

  2. 将下载的压缩包解压到本地。

  3. 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。

  4. 单击“**从文件添加**”按钮。

  5. 这将打开一个窗口；在该窗口中，指定 plugin.zip 文件的路径和 signature.txt 文件的路径。这些文件位于您将 Web 插件压缩包解压到的文件夹中。

6. 单击“**添加**”按钮。

7. 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。

*视频：使用向导安装管理 Web 插件*




*视频：在隔离网络中安装管理 Web 插件*




## 4 创建 Kaspersky Endpoint Security 策略

在 Kaspersky Security Center Web Console 或管理控制台中为 Kaspersky Endpoint Security 创建策略（具体取决于您使用的 Kaspersky Security Center 管理控制台）。

根据您希望使用应用程序的模式管理以下设置：

**对于标准模式**

如果您已在管理控制台向导中创建策略，请指定应用程序使用模式：**标准模式或 Endpoint Detection and Response Agent 模式**。如果您已在 Kaspersky Security Center Web Console 向导中创建策略，请跳过应用程序模式选择。

**对于 EDR 代理模式**

1. 如果您已在管理控制台向导中创建策略，请指定应用程序使用模式：**标准模式或 Endpoint Detection and Response Agent 模式**。如果您已在 Kaspersky Security Center Web Console 向导中创建策略，请跳过应用程序模式选择。

2. 按照向导的说明完成策略创建。

3. 在 Kaspersky Security Center Web Console 或管理控制台中打开已创建策略的属性，并启用与您要用于保护设备的检测和响应解决方案的集成：

   - 对于 OSMP 平台上的 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合，您需要启用并配置 EDR Expert (on-premises) 组件。这些设置位于 Kaspersky Security Center Web Console 中

   - 要与 Kaspersky Anti Targeted Attack Platform 上的 Kaspersky Endpoint Detection and Response 集成，您需要启用并配置 EDR Expert (on-premises) 组件。这些设置位于 Kaspersky Security Center Web Console 和 管理控制台 中。

   - 要与 Kaspersky Anti Targeted Attack Platform 上的 Kaspersky Network Detection and Response 集成，您需要启用并配置 NDR (KATA) 组件。这些设置位于 Kaspersky Security Center Web Console 和 管理控制台 中。

**对于 Light Agent 模式**

在新策略向导中：

1. 指定 **用于保护虚拟环境的 Light Agent 模式**。

2. 管理 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 SVM 地址的自定义列表** 选项，Light Agent 使用扩展 SVM 选择算法，并且在某个 SVM 上启用了大型基础架构保护模式，则只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到此 SVM。在 **SVM 选择算法** 区域中，您需要将 **SVM 路径** 设置设为 **忽略**。如果设置任何其他值，Light Agent 都无法连接到 SVM。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

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，请指定新的连接设置：IPv4 地址或完全限定域名 (FQDN)，以及用于连接到 Integration Server 的端口。

> 如果您的基础架构中部署了基于 Linux 的高可用性 Integration Server 集群，则需要将负载均衡器的地址和端口指定为连接到 Integration Server 的地址和端口。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

c. 如果您选择手动定义的 SVM 地址列表，请创建由此策略管理的 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)。您可以使用换行输入来隔开多个 IP 地址或 SVM 的完全限定域名。

> 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。

对于其余策略设置，您可以保留默认值。默认设置提供基本级别的保护。安装 Kaspersky Endpoint Security 后，您可以根据组织的要求配置策略。为此，您可以使用 管理应用程序 帮助部分中的组件配置方案。

*视频：创建策略*




## 5 配置应用程序数据库和模块的集中式更新

默认情况下，Kaspersky Endpoint Security 安装在没有反病毒数据库的设备上。只有将数据库下载到设备后，应用程序才能正常运行。要确保在安装应用程序后立即开始保护，请配置集中式数据库更新。

在 Kaspersky Security Center Web Console 或管理控制台中（取决于您使用的 Kaspersky Security Center 管理控制台）：

1. 启动管理服务器任务 *将更新下载至管理服务器存储库*。该任务由管理服务器快速启动向导自动创建。

   该任务会将 Kaspersky Endpoint Security 的更新包下载到管理服务器上的更新目录。

2. 为 Kaspersky Endpoint Security 应用程序创建 *更新* 类型的组任务。在 任务设置 中，指定：

- 更新源：Kaspersky Security Center。
- 任务计划：至少每天一次。建议每天运行该任务 4 到 6 次。

*视频：配置集中式数据库更新*




## 6 添加授权许可密钥并创建激活任务

要在标准模式下激活应用程序，您必须向应用程序添加授权许可密钥。如果某些组件不在您的授权许可涵盖范围内，您可能需要另一个授权许可密钥：

要在 EDR 代理模式下激活 Kaspersky Endpoint Security 应用程序，您需要 EDR Expert (on-premises) 授权许可密钥。

您可以根据基础架构和组织的要求选择激活方法：

- 如果所有设备上都安装了具有相同功能集的应用程序，请使用授权许可密钥的自动分发。要分发的授权许可密钥必须先使用密钥文件或激活码添加到 Kaspersky Security Center 密钥库中。有关更多信息，请参阅 Kaspersky Security Center 帮助。
- 如果各设备的应用程序功能集不同，则需要使用不同的授权许可密钥进行激活。在这种情况下，请将受保护设备置于不同的管理组中，并为每个管理组配置用于添加密钥的 组任务。

在连接到 SVM 后，Light Agent 模式下的 Kaspersky Endpoint Security 会从 Protection Server 接收授权许可信息。您无需单独激活 Light Agent 模式下的 Kaspersky Endpoint Security。

*视频：使用激活码激活应用程序*




*视频：使用密钥文件激活应用程序*




准备好 Kaspersky Security Center 后，您可以返回部署场景，并从 安装应用程序 步骤继续。

# 使用 Kaspersky Security Center 安装应用程序

**安装涉及的特殊注意事项：**

- Kaspersky Endpoint Security 的 EDR Agent 模式和 Light Agent 模式在配备 Elbrus CPU 的设备上不受支持。
- 在 Arm 设备上，不支持以 Light Agent 模式运行 Kaspersky Endpoint Security。

使用 Kaspersky Security Center 安装应用程序的推荐方案包括以下步骤：

您还可以使用 快速入门向导 和 保护部署向导，通过 Kaspersky Security Center 安装 Kaspersky Endpoint Security 应用程序。

## 1 创建安装包

Kaspersky Endpoint Security 应用程序的安装包包含以下内容：

- 主分发包
- 用于远程安装应用程序的分发包
- 包含应用程序图形界面的分发包
- 在安装过程中应用的 初始配置设置

您可以通过以下方式创建安装包：

- **使用卡巴斯基服务器上托管的分发包**。在 Kaspersky Security Center 中，系统会自动根据指定的分发包创建安装包。

  *视频：在 Kaspersky Security Center 中自动创建安装包*




  要在支持有限的操作系统（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）上安装 Kaspersky Endpoint Security 应用程序，请选择标记为 `for legacy OS` 的分发包。

- **手动，使用在 准备分发包 步骤中准备的文件**。如果您想使用 配置文件 指定初始配置设置，或者想要将创建的安装包用于不同的操作系统或不同的包管理器，建议使用此方法。

*视频：在 Kaspersky Security Center 中手动创建安装包*




您可以将预下载的应用程序数据库添加到安装包中。如果您使用的是带有集成数据库的安装包，则应用程序和数据库一起安装；在这种情况下，您不需要在安装后立即更新数据库。

您可以多次使用相同的安装包。

**如何手动准备安装包**

1. 在本地解压包含用于远程安装 Kaspersky Endpoint Security 的文件的存档。
2. 将包含主应用程序文件的软件包放在同一目录中。

   如果您想将创建的安装包用于不同的操作系统或包管理器，请将所需的所有操作系统和包管理器类型的分发包放在该目录中。
3. 如果您想使用应用程序的图形界面，请将图形界面软件包放在同一目录中。

   在已创建安装包的属性中，或者在 autoinstall.ini 配置文件中编辑相应设置（`USE_GUI=Yes`），以启用图形界面。默认情况下，不安装图形界面。

   > 如果 Kaspersky Endpoint Security 在 Light Agent 模式下使用，则不支持图形用户界面。

4. 如果您想使用配置文件设置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 文件位于您将包含用于远程安装 Kaspersky Endpoint Security 的文件的存档解压到的文件夹中。

   a. 默认在标准模式下使用应用程序。

   若要以 EDR Agent 模式使用应用程序，请设置 `ENDPOINT_AGENT_MODE=Yes`。

   若要以 Light Agent 模式使用应用程序，请设置 `KSVLA_MODE=Yes`。

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

   b. 若要以 Light Agent 模式安装应用程序：

   - 如果您要将应用程序安装在用于创建临时虚拟机的模板上，请设置 `VDI_MODE=Yes`。此设置会启用 VDI 保护模式，以优化应用程序在临时虚拟机上的性能。
   - 指定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）（`SERVER_MODE=Yes|No`）。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。

稍后，您也可以在已创建安装包的属性中的“**设置**”选项卡上更改应用程序的初始配置。

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。

**如何在 Web Console 中创建安装包**

1. 在 Web Console 主窗口中，选择以下任一部分：

   - **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**”按钮。
   创建安装包的向导将启动。

3. 如果您使用的是 Web Console，请选择创建安装包的方式：

   - “**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。
   - “**为卡巴斯基应用程序创建安装包**”。将从卡巴斯基服务器上的分发包创建安装包。

   如果您使用的是 Kaspersky Security Center 云控制台，则安装包是从托管在卡巴斯基服务器上的分发包创建的。

4. 根据软件包创建方法：

   - 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，然后单击 **下载并创建安装包** 按钮。安装包创建过程启动。

5. 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，请确认您已阅读并接受最终用户授权许可协议和隐私策略的完整条款。

6. 结束向导。
   安装包将被创建并添加到安装包列表中。

7. 打开安装包的属性，然后转到“**设置**”选项卡。

   - 如果您要以 EDR Agent 模式安装应用程序，请为 **使用模式** 设置选择 **Endpoint Detection and Response Agent**。
   - 如果您正在以 Light Agent 模式安装应用程序，请指定以下设置：
     **使用模式**，选择 **用于保护虚拟环境的 Light Agent** 选项。
     “**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。默认情况下已清空该复选框。
     “**受保护的虚拟机被用作服务器**”。要安装应用程序的虚拟机的角色：服务器或工作站。此复选框默认处于选中状态（虚拟机在虚拟基础架构中用作服务器）。
   - 如有必要，管理其他初始配置设置。
     有关安装包中应用程序所有初始配置设置的说明，请参阅 附录 1。

**如何在管理控制台中创建安装包**

*若要使用准备好的文件创建安装包：*

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. 点击"**创建卡巴斯基应用程序的安装包**"按钮。
4. 指定新安装包的名称并继续执行向导的下一步。
5. 指定 kesl.kud 文件的路径。该文件位于您在 准备分发包 步骤中将包含应用程序安装文件 (kesl.zip) 的压缩文件解压到的文件夹中。

   应用程序的名称和版本将显示在窗口中。继续执行向导的下一步。
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，请确认您已阅读并接受最终用户授权许可协议和隐私策略的完整条款。要进行确认，请在打开的窗口中选中两个复选框。

   继续执行向导的下一步。
7. 该向导下载将应用程序安装到 Kaspersky Security Center Administration Server 所需的文件。等待下载完成并结束向导。
8. 打开安装包的属性，然后转到"**应用程序设置**"选项卡。

   - 如果您要以 EDR Agent 模式安装应用程序，请为 **应用程序模式** 设置选择 **Endpoint Detection and Response Agent**。
   - 如果您正在以 Light Agent 模式安装应用程序，请指定以下设置：

     "**应用程序模式**"。请选择**用于保护虚拟环境的 Light Agent**选项。

     "**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。默认情况下已清空该复选框。

     "**受保护的虚拟机被用作服务器**"。要安装应用程序的虚拟机的角色：服务器或工作站。默认情况下已选定该选框。

     Light Agent 模式下不可用：

     - 配置应用程序数据库的更新源并启动更新
     - 配置代理服务器设置
     - 应用程序激活

     Light Agent 模式下的应用程序在连接到 SVM 后，会从 Protection Server 接收数据库更新和授权许可信息。您无需单独激活 Kaspersky Endpoint Security 或配置数据库更新。
   - 如有必要，管理其他初始配置设置。

     有关安装包中应用程序所有初始配置设置的说明，请参阅 附录 1。

   您可以稍后在已创建安装包的属性中的"**应用程序设置**"部分执行应用程序的初始配置。

*该向导会根据卡巴斯基服务器上的分发包创建安装包。*

1. 在控制台树中，选择**附加 → 远程安装 → 安装包**。
2. 单击“**其他操作**”→“**查看卡巴斯基应用程序的当前版本**”按钮。
3. 从列表中选择 Kaspersky Endpoint Security 分发包，然后单击“**下载并创建安装包**”按钮。
4. 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，请确认您已阅读并接受最终用户授权许可协议和隐私策略的完整条款。要确认，请在确认窗口中选中两个复选框，然后单击“**全部接受**”按钮。
5. 等待下载完成。安装包将被创建并添加到安装包列表中。
6. 打开安装包的属性，然后转到“**应用程序设置**”部分。

   - 如果您要以 EDR Agent 模式安装应用程序，请为 **应用程序模式** 设置选择 **Endpoint Detection and Response Agent**。
   - 如果您正在以 Light Agent 模式安装应用程序，请指定以下设置：

     “**应用程序模式**”。请选择**用于保护虚拟环境的 Light Agent**选项。

     “**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。默认情况下已清空该复选框。

     “**受保护的虚拟机被用作服务器**”。要安装应用程序的虚拟机的角色：服务器或工作站。默认情况下已选定该选框。

     以下设置在 Light Agent 模式下不可用：

     - 配置应用程序数据库的更新源并启动更新
     - 配置代理服务器设置
     - 应用程序激活

     Light Agent 模式下的应用程序在连接到 SVM 后，会从 Protection Server 接收数据库更新和授权许可信息。您无需单独激活 Kaspersky Endpoint Security 或配置数据库更新。
   - 如有必要，管理其他初始配置设置。

     有关安装包中应用程序所有初始配置设置的说明，请参阅 附录 1。

   您可以稍后在已创建安装包的属性中的“**应用程序设置**”部分执行应用程序的初始配置。

## 2 在企业网络中的设备上安装应用程序

您可以通过 Kaspersky Security Center 使用 远程应用程序安装任务 来安装应用程序。

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。

应用程序的初始配置会根据在 安装包 属性中所做的设置或安装包中包含的配置文件自动执行。

*视频：安装、更新数据库并检查 Kaspersky Endpoint Security 的性能*




## 3 应用程序数据库更新

如果您已以标准模式或 EDR Agent 模式安装应用程序，请在 Web Console 或管理控制台（取决于您使用的 Kaspersky Security Center 管理控制台）中，运行在“配置应用程序数据库和模块的集中更新”步骤创建的 *Update* 组任务。有关更新 Kaspersky Endpoint Security 数据库的更多信息，请参阅 更新应用程序数据库和模块 部分。

## 4 应用程序运行状况检查

因此，Kaspersky Endpoint Security 应用程序已安装并激活，且应用程序数据库已更新。安装后，应用程序会自动启动。默认情况下，以下组件处于启用状态：

- 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。

请确认应用程序已准备就绪，可以使用。

**如何在 Web Console 中检查设备的保护状态**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
   列表仅显示所选管理组的受管理设备。

3. 单击设备名称。

   这将打开受管理设备的属性窗口。

4. 在“**常规**”选项卡上，选择“**保护**”部分。“**设备状态**”字段应显示 *OK*。

   如果“**设备状态**”字段显示有关系统目录权限不足的信息，请在此设备本地检查以下目录的权限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。请确保所有者为 root，并且只有所有者拥有对这些目录的写入权限。

5. 转到“**应用程序**”选项卡。

6. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。

   应用程序属性窗口将打开。

7. 在“**常规**”选项卡的“**信息**”部分中，查看“**应用程序数据库**”。请确保应用程序数据库为最新。

8. 转到“**常规**”选项卡上的“**授权许可**”部分，并确保应用程序已激活。

9. 如果您已以 EDR Agent 模式安装应用程序，请转到“**常规**”选项卡上的“**组件**”部分，并确保您在“创建 Kaspersky Endpoint Security 策略”步骤配置的集成具有“*正在运行*”状态。

10. 如果您已以 Light Agent 模式安装应用程序，请转到“**常规**”选项卡上的“**组件**”部分，并确保“**用于保护虚拟环境的 Light Agent 模式**”行显示状态为“*正在运行*”。这意味着应用程序正以 Light Agent 模式使用。

**如何在管理控制台中检查设备的保护状态**

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。

   这将打开受管理设备的属性窗口。

4. 选择“**保护**”部分。“**设备状态**”字段应显示 *OK/在网络中可见*。

   如果“**设备状态**”字段显示有关系统目录权限不足的信息，请在此设备本地检查以下目录的权限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。请确保所有者为 root，并且只有所有者拥有对这些目录的写入权限。

5. 转至“**应用程序**”部分。

6. 在设备上安装的应用程序列表中，选择 Kaspersky Endpoint Security 应用程序并双击以打开应用程序属性窗口。

7. 在“**常规**”部分中，查看“**应用程序数据库**”字段。请确保应用程序数据库为最新。

8. 转到“**授权许可密钥**”部分，并确认应用程序已激活。

9. 如果您已以 EDR Agent 模式安装应用程序，请转到“**组件**”部分，并确保您在“创建 Kaspersky Endpoint Security 策略”步骤配置的集成具有“*正在运行*”状态。

10. 如果您已以 Light Agent 模式安装应用程序，请转到“**组件**”部分，并确保“**用于保护虚拟环境的 Light Agent 模式**”行显示“*正在运行*”状态。这意味着应用程序正以 Light Agent 模式使用。

实用文章

任务未运行或策略未应用时该怎么办

设备状态为“无效的策略设置。策略尚未应用”时该怎么办

错误：“当前版本的 Kaspersky Security Center Web Console 不支持该应用程序，或者未安装应用程序 Web 插件”

排查安装 GUI 时的问题

安装错误代码说明

Kaspersky Endpoint Security 安装后出现的错误

安装 Kaspersky Endpoint Security 后，您可以返回部署方案，并从 某些操作系统中安装后的其他配置步骤 步骤继续。

# 使用命令行安装应用程序

**安装涉及的特殊注意事项：**

- Kaspersky Endpoint Security 的 EDR Agent 模式和 Light Agent 模式在配备 Elbrus CPU 的设备上不受支持。
- 在 Arm 设备上，不支持以 Light Agent 模式运行 Kaspersky Endpoint Security。
- 您需要 root 权限才能安装应用程序和图形界面。
- 您必须以 root 用户身份运行初始设置向导。
- 如果 apt 软件包管理器的版本低于 1.1.X，您需要使用 dpkg 软件包管理器（取决于操作系统）进行安装。

使用命令行安装应用程序的推荐方案包括以下步骤：

## 1 安装 Kaspersky Endpoint Security 应用程序

开始安装之前，请将下载的包含应用程序主文件的软件包放置在设备上的 /tmp 目录中。

## 如何从 RPM 软件包安装应用程序

在 32 位操作系统上

```
yum install kesl-12.5.0-<build number>.i386.rpm
```

在 64 位操作系统上

```
yum install kesl-12.5.0-<build number>.x86_64.rpm
```

在 64 位 ALT 操作系统上

```
apt-get install kesl-12.5.0-<build number>.x86_64.rpm
```

在 Arm 架构的 64 位操作系统上

```
yum install kesl-12.5.0-<build number>.aarch64.rpm
```

在 Arm 架构的 64 位 ALT 操作系统上

```
apt-get install kesl-12.5.0-<build number>.aarch64.rpm
```

在 Elbrus 架构的 64 位操作系统上

```
yum install kesl-12.5.0-<build number>.2ek.rpm
```

在 Elbrus 架构的 64 位 ALT 操作系统上

```
apt-get install kesl-12.5.0-<build number>.2ek.rpm
```

在支持有限的 64 位操作系统上（CentOS 5.2、CentOS 5.4、CentOS 6.4、CentOS 6.6）

```
rpm -i kesl-12.5.0-<build number>.x86_64.rpm
```

要在 CentOS 5.2、CentOS 5.4、CentOS 6.4 或 CentOS 6.6 上安装应用程序，您需要从网站下载标记为 OLD 的分发包。

## 如何从 DEB 软件包安装应用程序

在 32 位操作系统上

```
apt-get install ./kesl_12.5.0-<build number>_i386.deb
```

在 64 位操作系统上

```
apt-get install ./kesl_12.5.0-<build number>_amd64.deb
```

在 Arm 架构的 64 位操作系统上

```
apt-get install ./kesl_12.5.0-<build number>_arm64.deb
```

在 Elbrus 架构的 64 位操作系统上

```
apt-get install ./kesl_12.5.0-<build number>_2ek.deb
```

## ❷ 安装应用程序的图形界面

如果您想要使用图形界面管理应用程序，需要将图形界面安装在与应用程序相同的设备上。

应用程序图形界面的特殊功能：

- 您无法在未安装 Kaspersky Endpoint Security 应用程序的设备上安装图形界面。
- 如果应用程序在 Light Agent 模式下使用，则不支持图形用户界面。

开始安装之前，请将下载的包含应用程序图形界面文件的软件包放置在设备上的 /tmp 目录中。

**如何从 RPM 软件包安装应用程序的图形界面**

在 32 位操作系统上

```
yum install kesl-gui-12.5.0-<build number>.i386.rpm
```

在 64 位操作系统上

```
yum install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

在 64 位 ALT 操作系统上

```
apt-get install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

在 Arm 架构的 64 位操作系统上

```
yum install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

在 Arm 架构的 64 位 ALT 操作系统上

```
apt-get install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

在 Elbrus 架构的 64 位操作系统上

```
yum install kesl-gui-12.5.0-<build number>.2ek.rpm
```

在 Elbrus 架构的 64 位 ALT 操作系统上

```
apt-get install kesl-gui-12.5.0-<build number>.2ek.rpm
```

在支持有限的 64 位操作系统上（CentOS 6.4、CentOS 6.6）

```
rpm -i kesl-gui-12.5.0-<build number>.x86_64.rpm
```

要在 CentOS 6.4 或 CentOS 6.6 上安装应用程序，您需要从网站下载标记为 OLD 的分发包。

**如何从 DEB 软件包安装应用程序的图形界面**

在 32 位操作系统上

```
apt-get install ./kesl-gui_12.5.0-<build number>_i386.deb
```

在 64 位操作系统上

```
apt-get install ./kesl-gui_12.5.0-<build number>_amd64.deb
```

在 Arm 架构的 64 位操作系统上

```
apt-get install ./kesl-gui_12.5.0-<build number>_arm64.deb
```

在 Elbrus 架构的 64 位操作系统上

```
apt-get install ./kesl-gui_12.5.0-<build number>_2ek.deb
```

## 3 应用程序的初始设置

该应用程序需要初始配置以准备运行并启用客户端设备的保护。

如果应用程序在设备上的初始配置尚未完成，则您无法在该设备上使用或更新该应用程序。

应用程序的初始配置使用 Kaspersky Endpoint Security 分发包中的初始配置向导执行。您可以在交互模式或自动模式下执行初始配置。

**如何以交互方式执行应用程序的初始配置。**

**步骤 1. 启动向导**

启动初始配置向导

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

根据向导提示，逐步指定 Kaspersky Endpoint Security 初始配置设置的值。

如果设备上安装了网络代理，并且您正在以标准模式或 EDR Agent 模式安装应用程序，则可以跳过与更新应用程序数据库和激活应用程序相关的初始配置向导步骤。

**步骤 2. 选择标准模式或 Light Agent 模式**

输入 yes 以在 Light Agent 模式下使用应用程序。

输入 no 以在标准模式下使用应用程序。

如果您打算在 EDR Agent 模式下使用应用程序，则在此步骤中，您需要输入 no 并在下一步中选择 EDR Agent 模式。

初始配置完成后，即无法更改应用程序使用模式。

**步骤 3. 选择模式：标准模式或 Endpoint Detection and Response Agent**

如果您在步骤 2 中选择在标准模式下使用应用程序，则会显示此步骤。

输入 yes 以在 EDR Agent 模式下使用应用程序。

输入 no 以在标准模式下使用应用程序。

初始配置完成后，即无法更改应用程序使用模式。

**步骤 4. Kaspersky Endpoint Detection and Response Expert (cloud) 集成**

如果您在步骤 3 中选择在标准模式下使用应用程序，则会显示此步骤。

输入 yes 以使用 Kaspersky Endpoint Detection and Response Expert (cloud) 集成。

输入 no 以使用 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成。

**步骤 5. 选择虚拟机的角色**

如果您在步骤 2 中选择在 Light Agent 模式下使用应用程序，则会显示此步骤。

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yes。
- 如果要将虚拟机作为工作站，请输入no。

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。

**步骤 6. 启用 VDI 保护模式**

如果您在步骤 2 中选择在 Light Agent 模式下使用应用程序，则会显示此步骤。

VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 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的虚拟机模板。

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。

**步骤 7. 选择区域设置**

在此步骤中，向导以 RFC 3066 格式显示支持的区域设置列表。

请按照此处所列指定区域设置。此区域设置用于以下目的：

- 对安装过程中显示的《最终用户授权许可协议》、《隐私策略》和《卡巴斯基安全网络声明》的文本进行本地化。
- 对发送到 Kaspersky Security Center 的应用程序事件进行本地化。

图形界面和应用程序命令行的区域设置取自 LANG 环境变量。如果应用程序不支持此本地化，则默认使用英语本地化。

**步骤 8. 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订立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。

**步骤 9.接受最终用户授权许可协议**

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和条件，Kaspersky Endpoint Security 安装过程将中止。

**步骤 10.接受隐私策略**

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）。

如果您不接受隐私策略的条款和条件，Kaspersky Endpoint Security 设置过程将中止。

**步骤 11.使用卡巴斯基安全网络**

在此步骤中，接受或拒绝 卡巴斯基安全网络 的使用条款：

- 如果您接受卡巴斯基安全网络声明的条款和条件，请输入 yes（或 y）。这将启用扩展 KSN 模式。
- 如果您不接受卡巴斯基安全网络声明的条款和条件，请输入 no（或 n）。

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。

拒绝参与卡巴斯基安全网络不会中断 Kaspersky Endpoint Security 的初始配置。您可以随时启用、禁用或更改卡巴斯基安全网络模式。

如果启用了卡巴斯基安全网络，则会自动启用云模式，在该模式下，Kaspersky Endpoint Security 使用轻量级版本的恶意软件数据库。

**步骤 12. 从特权组中删除用户**

如果在 kesladmin 和/或 keslaudit 组中检测到用户，则会显示此步骤。

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 yes。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 no。

**步骤 13. 将管理员角色分配给一位用户**

在此步骤中，向导会提示您授予管理员角色（admin）。

输入要向其授予管理员角色的用户的名称。您需要具备管理员角色，才能在应用程序的图形界面和命令行中管理应用程序设置和任务设置，而无需使用 sudo 命令。

完成初始配置后，您可以稍后将管理员角色分配给用户。

**步骤 14.配置系统事件拦截机制**

如果操作系统满足安装可更新内核模块的要求，则应用程序可以使用基于可更新内核模块的拦截机制。如果操作系统不满足这些要求但支持 fanotify 技术，则应用程序会使用 fanotify 拦截系统事件。如果操作系统不支持 fanotify 技术，则应用程序将编译并使用一个特殊内核模块，以便为文件威胁防护拦截系统事件。如果安装了所有必需的软件包，则会在文件威胁防护启动时自动开始编译内核模块。如果未在设备上发现任何依赖项，Kaspersky Endpoint Security 应用程序会建议安装相关软件包。如果软件包下载失败，将显示一条错误消息。

- 如果您希望使用可更新内核模块，请输入“yes”。
- 如果您希望使用 fanotify，请输入“no”。

如果选择可更新内核模块作为拦截机制，请指定以下设置：

- 如果可更新内核模块启动失败，应用程序执行的操作：
  - 如果您希望应用程序在可更新内核模块启动失败时回退到使用 fanotify 进行系统事件拦截，请输入“yes”。
  - 如果您希望应用程序在可更新内核模块启动失败时继续运行而不进行系统事件拦截，请输入“no”。

    如果应用程序不使用系统事件拦截，则不会执行文件实时扫描，从而降低设备的保护级别。

- 切换到使用可更新内核模块时的应用程序重启模式。要运行该模块，必须自动或手动重启应用程序。

  我们建议自动重启应用程序以切换到使用可更新的内核模块。重新启动应用程序后手动启动可更新的内核模块可能会导致应用程序错误。

如果您希望允许自动重启应用程序来运行模块，请输入“yes”。

**步骤 15. 启用 SELinux 的自动配置**

如果您的操作系统中安装了 SELinux 访问控制系统，则会显示此步骤。

输入 yes 可自动配置 SELinux，以便与 Kaspersky Endpoint Security 配合使用。如果应用程序无法自动配置 SELinux（例如，如果缺少 semanage 实用程序），则向导会显示错误消息并提示用户手动配置 SELinux。

如果您不想执行 SELinux 系统的自动配置，请输入 no。

默认情况下，向导建议使用 yes。

如有必要，在应用程序的初始配置完成后，您可以稍后手动配置 SELinux，以便与应用程序配合使用。

**步骤 16.配置更新源**

如果您正在以标准模式或 EDR Agent 模式安装 Kaspersky Endpoint Security，则会显示此步骤。

指定数据库和应用程序模块的更新源。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。

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。
- Custom：应用程序从自定义源下载更新。您可以将自定义更新源的地址指定为本地目录（例如，/home/databases）或远程 HTTP 或 HTTPS 服务器（例如，http://example.com/databases/）。

**步骤 17.配置代理服务器设置**

如果您正在以标准模式或 EDR Agent 模式安装 Kaspersky Endpoint Security，则会显示此步骤。

如果使用代理服务器进行互联网连接，请使用以下格式之一输入代理服务器的地址：

- [<connection protocol>://]<address of proxy server>:<port>，如果连接到代理服务器不需要身份验证；
- [<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>，如果连接到代理服务器时需要身份验证。指定 IPv6 地址时，请将其输入方括号中。

  不支持通过 HTTPS 连接到代理服务器。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。

如果您不使用代理服务器，请输入 no。

默认情况下，应用程序建议为 no。

完成初始配置后，您可以稍后管理代理服务器设置。

**步骤 18. 启动应用程序数据库更新**

如果您正在以标准模式或 EDR Agent 模式安装 Kaspersky Endpoint Security，则会显示此步骤。

在此步骤中，向导会提示您在安装后立即在客户端设备上运行应用程序数据库更新任务。

如果您不想开始下载应用程序数据库，请输入 no。

默认情况下，向导建议使用 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。

完成初始配置后，您可以稍后运行更新任务。

**步骤 19. 启用应用程序数据库自动更新**

如果您正在以标准模式或 EDR Agent 模式安装 Kaspersky Endpoint Security，则会显示此步骤。

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。

完成初始配置后，您可以通过配置更新任务计划来稍后启用自动更新数据库。

**步骤 20.应用程序激活**

如果您正在以标准模式或 EDR Agent 模式安装 Kaspersky Endpoint Security，则会显示此步骤。

如果您想在安装后立即激活应用程序，请输入激活码或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。

完成初始配置后，您可以稍后激活应用程序。

**如何在自动模式下执行初始配置**

1. 创建一个包含初始配置设置的配置文件。您可以从用于通过 Kaspersky Security Center 远程安装应用程序的 autoinstall.ini 配置文件中复制设置，并根据需要进行更改。
2. 在配置文件中指定以下必需设置：
   - 接受最终用户授权许可协议 (EULA) 和隐私策略：

     `EULA_AGREED=Yes`

     `PRIVACY_POLICY_AGREED=Yes`

     您可以在 应用程序分发包中包含的 license.<language ID> 文件中阅读最终用户授权许可协议和隐私策略的条款和条件：

     如果您不接受最终用户授权许可协议和隐私策略的条款和条件，安装过程将中止。

   - 默认情况下，卡巴斯基安全网络应用程序使用标准模式。

     要在 EDR Agent 模式下使用应用程序，请指定以下设置：

     `ENDPOINT_AGENT_MODE=Yes`

     要在 Light Agent 模式下使用应用程序，请指定以下设置：

     `KSVLA_MODE=Yes`

- 使用卡巴斯基安全网络。接受或拒绝卡巴斯基安全网络的使用条款：

  `USE_KSN=Yes|No`

  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。如果您接受卡巴斯基安全网络声明的条款和条件，则会启用扩展 KSN 模式。您可以随时启用、禁用或更改卡巴斯基安全网络模式。

  > 如果启用了卡巴斯基安全网络，则会自动启用云模式，在该模式下，Kaspersky Endpoint Security 使用轻量级版本的恶意软件数据库。

- 在安装应用程序之前，自动从 kesladmin 和 keslaudit 特权组中移除用户：

  `GROUP_CLEAN=Yes|No`

3. 选择 Kaspersky Endpoint Security 使用的系统事件拦截机制。如果要使用可更新内核模块拦截系统事件，请设置以下值：

   `INTERCEPTOR_MODE=UseUpdatableKernelModule`

   默认情况下，fanotify 技术用于拦截系统事件。

4. 如果您正在以标准模式或 EDR Agent 模式安装应用程序，请指定以下设置：

   - 代理服务器设置。如果使用代理服务器进行互联网连接，请使用以下格式之一输入代理服务器的地址：

     - `PROXY_SERVER=[<connection protocol>://]<address of proxy server>:<port>`，如果连接到代理服务器不需要身份验证；
     - `PROXY_SERVER=[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`，如果连接到代理服务器时需要身份验证。指定 IPv6 地址时，请将其输入方括号中。

     > 不支持通过 HTTPS 连接到代理服务器。

   - 安装并使用应用程序的图形界面：

     `USE_GUI=Yes|No`

5. 如果您正在以 Light Agent 模式安装应用程序，请指定以下设置：

   - 受保护的虚拟机的角色：

     - 如果受保护的虚拟机用作服务器，请输入 `SERVER_MODE=Yes`；
     - 如果受保护的虚拟机用作工作站，请输入 `SERVER_MODE=No`。

   - 启用 VDI 保护模式，以优化临时虚拟机上的应用程序性能。如果要将应用程序安装在用于创建临时虚拟机的虚拟机模板上，请设置以下值：

     `VDI_MODE=Yes`

6. 启动初始配置向导：

   ```
   /opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<initial configuration file>
   ```

   其中，`<initial configuration file>` 是包含初始配置设置的配置文件的路径。

当完成初始设置向导并释放控制台后，应用程序的安装后配置完成。

检查返回代码

```
echo $?
```

如果命令返回 0，则表示应用程序的安装后配置已成功完成。

## 4 应用程序运行状况检查

因此，Kaspersky Endpoint Security 应用程序已安装并激活，且应用程序数据库已更新。安装后，应用程序会自动启动。默认情况下，以下组件处于启用状态：

- 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。

### 检查标准模式下的设备保护状态

要检查设备的保护状态，请运行以下命令：

```
kesl-control --app-info [--json]
```

其中 `--json` 表示以 JSON 格式输出数据。如果不指定 `--json` 选项，设置将输出到控制台。

请确保：

- 应用程序已激活（**应用程序授权许可信息** 行）。
- 应用程序数据库为最新（**应用程序数据库已加载** 和 **数据库的上次发布日期** 行）。
- 文件威胁防护已启用（**文件威胁防护** 行）。
- **应用程序状态** 行显示 OK。

  如果 **应用程序状态** 行显示有关系统目录权限不足的信息，请在此设备本地检查以下目录的权限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。请确保所有者为 root，并且只有所有者拥有对这些目录的写入权限。

### 检查 EDR Agent 模式下的设备保护状态

要检查设备的保护状态，请运行以下命令：

```
kesl-control --app-info [--json]
```

其中 `--json` 表示以 JSON 格式输出数据。如果不指定 `--json` 选项，设置将输出到控制台。

请确保：

- 应用程序已激活（**EDR Expert (on-premises) 授权许可信息** 行）
- 应用程序数据库为最新（**应用程序数据库已加载** 和 **数据库的上次发布日期** 行）。
- 应用程序以 EDR Agent 模式使用（**Endpoint Detection and Response Agent 模式** 行）。
- 对于您在策略中配置的集成，会显示“可用且正在运行”状态。
- **应用程序状态** 行显示 OK。

  如果 **应用程序状态** 行显示有关系统目录权限不足的信息，请在此设备本地检查以下目录的权限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。请确保所有者为 root，并且只有所有者拥有对这些目录的写入权限。

**检查 Light Agent 模式下的设备保护状态**

1. 运行以下命令：

   ```
   kesl-control --ksvla-info
   ```

   确保应用程序以 Light Agent 模式使用（**用于保护虚拟环境的 Light Agent 模式** 行）。

2. 如果您已在策略中选择 Integration Server 来检测可供连接的 SVM，请运行以下命令：

   ```
   kesl-control --viis-info
   ```

   确保 Light Agent 已连接到 Integration Server（**Integration Server 的连接状态** 行）。

3. 运行以下命令：

   ```
   kesl-control --svm-info
   ```

   请确保 Light Agent 已连接到 SVM：会显示与其建立连接的 SVM 的相关信息。

4. 运行以下命令：

   ```
   kesl-control --app-info [--json]
   ```

   其中 `--json` 表示以 JSON 格式输出数据。如果不指定 `--json` 选项，设置将输出到控制台。

   请确保：

   - Light Agent 会接收有关用于激活 Kaspersky Security for Virtualization Light Agent 的授权许可的信息（**应用程序授权许可信息** 行）。
   - 应用程序数据库为最新（**应用程序数据库已加载** 和 **数据库的上次发布日期** 行）。
   - **应用程序状态** 行显示 OK。

     如果 **应用程序状态** 行显示有关系统目录权限不足的信息，请在此设备本地检查以下目录的权限：/var/opt/kaspersky、/var/log/kaspersky 和 /opt/kaspersky。请确保所有者为 root，并且只有所有者拥有对这些目录的写入权限。

实用文章

任务未运行或策略未应用时该怎么办

设备状态为“无效的策略设置。策略尚未应用”时该怎么办

错误：“当前版本的 Kaspersky Security Center Web Console 不支持该应用程序，或者未安装应用程序 Web 插件”

排查安装 GUI 时的问题

安装错误代码说明

Kaspersky Endpoint Security 安装后出现的错误

安装 Kaspersky Endpoint Security 后，您可以返回部署方案，并从 某些操作系统中安装后的其他配置步骤 步骤继续。

# 某些操作系统中安装后的其他配置步骤

在为 Kaspersky Endpoint Security 安装准备环境并安装应用程序后，某些操作系统需要进行其他配置。

**手动配置 SELinux 以与应用程序配合使用**

如果您的操作系统在 `Enforcing` 模式下使用 SELinux 访问控制系统，则默认会在安装期间自动将其配置为与应用程序配合使用。

如果应用程序无法自动配置 SELinux（例如，缺少 semanage 实用程序），则向导会显示错误消息并提示用户手动配置 SELinux。在这种情况下，或者如果您拒绝了自动配置，请在完成应用程序的初始配置后，手动配置 SELinux 系统以与 Kaspersky Endpoint Security 应用程序配合使用。

此配置需要 root 权限。

*要手动配置 SELinux 以使用应用程序：*

1. 将 SELinux 切换为宽容模式：
   - 如果启用了 SELinux，请运行以下命令：

     ```
     setenforce Permissive
     ```

   - 如果 SELinux 已禁用，请在 /etc/selinux/config 配置文件中设置 `SELINUX=permissive`，然后重启操作系统。
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“targeted”策略，请根据您的 SELinux 策略为每个原始 Kaspersky Endpoint Security 可执行文件分配标签。

```
semanage fcontext -a -t bin_t <executable file>
restorecon -v <executable file>
```

其中 `<executable file>` 为：

- /var/opt/kaspersky/kesl/<内部版本号_*>/opt/kaspersky/kesl/libexec/kesl
- /var/opt/kaspersky/kesl/<内部版本号_*>/opt/kaspersky/kesl/bin/kesl-control
- /var/opt/kaspersky/kesl/<内部版本号_*>/opt/kaspersky/kesl/libexec/kesl-gui
- /var/opt/kaspersky/kesl/<内部版本号_*>/opt/kaspersky/kesl/shared/kesl
- /var/opt/kaspersky/kesl/<内部版本号_*>/opt/kaspersky/kesl/bin/response

4. 运行以下任务：

运行“文件威胁防护”任务

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

运行“关键区域扫描”任务

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

建议运行您将来打算运行的所有 Kaspersky Endpoint Security 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。

查看 audit.log 文件

```
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，然后重新启动您计划将来运行的所有任务。

根据阻止记录创建并加载新的规则模块：

```
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 切换为强制模式。

```
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 以执行响应操作**

如果您计划在操作系统中以 `Enforcing` 模式使用 SELinux，则要在与 Detection and Response 解决方案集成时执行响应操作，您需要额外管理 SELinux 设置。

此 SELinux 配置需要 root 权限。

*要为响应操作配置 SELinux：*

1. 将 SELinux 切换为宽容模式：
   - 如果 SELinux 已启用，请运行以下命令：

     ```
     将 SELinux 切换为宽容模式
     setenforce Permissive
     ```

   - 如果 SELinux 已禁用，请在 /etc/selinux/config 配置文件中设置 `SELINUX=permissive`，然后重启操作系统。
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. 运行所有任务，以执行您希望在与 Detection and Response 解决方案集成时使用的响应操作。
4. 要使用“获取内存转储”任务和“获取进程内存转储”任务收集取证信息，请在 SELinux 中允许 Kaspersky Endpoint Security 应用程序访问任务中指定的 SMB 服务器。
5. 确保 audit.log 文件中没有错误。

   ```
   查看 audit.log 文件
   grep kesl /var/log/audit/audit.log
   ```

6. 如果 audit.log 文件中存在任何错误，请根据阻止记录创建并加载新的规则模块以修复错误，然后再次运行响应操作任务。

   ```
   根据阻止记录创建并加载新的规则模块：
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

7. 将 SELinux 切换为强制模式。

   ```
   setenforce Enforcing
   ```

**在 OSnova 操作系统中配置应用程序启动**

安装应用程序后，请按照以下步骤配置应用程序及其图形界面的启动：

1. 打开 `/etc/NESS/systemd/kesl.service.config` 文件并设置 `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"`。

2. 打开 `/etc/sysctl.d/30-disable-ptrace.conf` 文件并设置 `kernel.yama.ptrace_scope=0`。`kernel.yama.ptrace_scope` 参数的其他值可能会影响 Kaspersky Endpoint Security 应用程序的运行；有关更多详细信息，请参阅已知问题和限制部分。

3. 如果要运行进程内存和内核内存扫描，需要禁用内核中的 mprotect（或 PaX）内存保护机制。为此，请将 `mprotect=off` 选项添加到内核命令行。更多详情，请参考OSnova 文档。

4. 重新启动操作系统。

**配置在封闭软件环境模式下的 ALT SP 上启动应用程序**

安装应用程序后，请按照以下步骤启动应用程序：

1. 为 Kaspersky Endpoint Security 的可更新组件分配 kesl 组和目录权限的继承：

```
cd /var/opt/kaspersky/kesl/<build number_*>/var/opt/kaspersky/kesl/private
chown -R root:kesl updates/
find updates -type d -exec chmod g+s {} \;
cd /opt/kaspersky/kesl/lib64
chown -R root:kesl updatable_modules/
find updatable_modules -type d -exec chmod g+s {} \;
cd /var/opt/kaspersky/kesl/common/
chown -R root:kesl temp/
find temp -type d -exec chmod g+s {} \;
```

2. 为网络代理的可更新组件分配 kesl 组和目录权限的继承：

```
cd /var/opt/kaspersky/
chown -R root:kesl klnagent/
find klnagent/ -type d -exec chmod g+s {} \;
cd /opt/kaspersky/
chown -R root:kesl klnagent64/
find klnagent64/ -type d -exec chmod g+s {} \;
```

3. 通过启动系统签名来启用封闭软件环境模式：

```
integrity-applier -i -A
```

4. 确保 IMA 子系统已激活：

```
cat /proc/cmdline
```

该命令的输出应包含以下行 `lsm=integrity ima_hash=sha512 ima_appraise=enforce`。

5. 运行数据库更新任务：

```
kesl-control --start 6 -W
```

如果数据库更新任务的输出包含 *EventType=BasesApplied* 事件，则表示数据库更新已正确执行。

6. 重启应用程序：

```
systemctl restart kesl
```

# 使用快速安装脚本迁移到 Kaspersky Security Center Linux 的方案

本方案包含将解决方案及其数据迁移到新的管理服务器设备的以下用例示例：

- 从 Kaspersky Security Center Windows（MS SQL 和 PostgreSQL）迁移到 Kaspersky Security Center Linux（PostgreSQL）。
- 因硬件更换而迁移 Kaspersky Security Center Linux（PostgreSQL）。

使用快速安装脚本部署新的管理服务器。

有关其他数据传输方式，请参见迁移到 Kaspersky Security Center Linux 部分。

## 1 创建备份副本的先决条件

此步骤包含相关说明，用于准备先前已配置的管理服务器，以便随后迁移到新的 Kaspersky Security Center Linux 管理服务器。准备过程包括以下步骤：

1. 检查管理服务器的版本，以创建与 Kaspersky Security Center Linux 兼容的备份副本。

   **Kaspersky Security Center Linux** 的所有当前版本均支持在将应用程序升级到较新版本的同时进行数据迁移。备份副本只能在同一数据库管理系统类型内创建和还原。

   对于 **Kaspersky Security Center Windows**，您需要在 **属性** → **常规** → **版本** 中检查管理服务器的版本。如果版本低于 15.1.0.22239，请将 Kaspersky Security Center Windows 升级到最新版本。

   **将 Kaspersky Security Center for Windows 升级到最新版本。**

   1. 在 卡巴斯基网站 上，下载与已安装管理服务器的本地化语言匹配的分发包：`Version 15.1.0.22239 | Windows | Full distributive`。

      可执行文件将以下列名称保存到 **下载** 文件夹：`ksc_15.1_<build number>_full_<language>.exe`。

   2. 将分发包复制到管理服务器。

   3. 以管理员身份运行 `ksc_15.1_<build number>_full_<language>.exe` 可执行文件。

   4. 在显示的窗口中，单击 **安装 Kaspersky Security Center** 链接。

      管理服务器安装向导将启动。

   5. 查看最终用户授权许可协议和隐私策略的条款。如果您同意最终用户授权许可协议和隐私策略的所有条款和条件，请在 **我确认我已完整阅读、理解并接受以下条款和条件** 部分中选中以下复选框：

      - “**该 EULA 的条款和条件**”。
      - “**描述数据处理的隐私策略**”。

6. 选择 **升级管理服务器和基于 Web 的控制台(推荐)** 并转到下一步。

7. 创建新的备份副本，选择 **我要创建数据备份副本** 选项，然后按照备份向导中的步骤操作。

8. 单击“**升级**”。

9. 在升级期间，在 Web Console 安装向导中确认升级版本所需的所有步骤。

   安装管理服务器升级需要一些时间。安装向导完成后，管理控制台在数据库初始化完成之前可能不接受连接。

10. 等待升级完成。

2. 验证管理服务器证书是否符合要求。

   创建备份副本之前，您需要确保证书包含 Subject Alternative Name (SAN)。如果不包含，请务必替换证书，否则从备份恢复后，您将无法登录 Web Console。

   *要验证证书是否包含使用者备用名称*：

   - 对于运行 Windows 的设备：

     a. 在管理控制台中，选择要检查的管理服务器。

     b. 在上下文菜单中，选择 **属性 → 常规 → 查看管理服务器证书**。

     c. 这将打开一个窗口；在该窗口中，检查 **使用者备用名称** 项的值。

   - 对于 Linux 设备，请运行以下命令：

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   确保使用者备用名称包含管理服务器设备的域名 (DNS)。

   如果该值仅包含外部 IP 地址而不包含域名 (DNS)，或者该值完全缺失，请手动将证书替换为符合Kaspersky Security Center Linux 要求的证书。使用 klsetsrvcert 实用程序替换管理服务器的通用证书。

   **使用 klsetsrvcert 实用程序替换管理服务器的通用证书**

   1. 通过运行以下命令，在设备上创建具有推迟开始日期的新证书：

      - 对于 Kaspersky Security Center Windows：

        ```
        "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
        <oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      - 对于 Kaspersky Security Center Linux：

        ```
        /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
        ```

      其中，`"<oldksc.example.internal>"` 是用于连接到管理服务器的 FQDN。

      请勿将 IP 地址用于此值。

2. 运行以下命令，为所有设备上的新证书设置开始日期：

   - 对于 Kaspersky Security Center Windows：

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - 对于 Kaspersky Security Center Linux：

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   其中，`"DD-MM-YYYY hh:mm"` 是比当前日期至少晚 30 天的日期。默认情况下，新证书 (`CR`) 的分发期限为 90 天。

   > 到了设置的时间后，您需要重新安装 Web Console 以恢复对其的访问并更新其证书。

3. 如有必要，在迁移到新的管理服务器后，请运行 klmover 实用程序 以恢复设备与管理服务器的连接。如果设备在整个证书分发期限内一直处于关闭状态，或者从未连接到管理服务器，您可能需要启动此实用程序。

## 2 创建先前管理服务器安装的备份副本

### 创建 Kaspersky Security Center Windows 的备份副本

1. 从 **开始菜单** → **Kaspersky Security Center** → **Kaspersky Backup 实用程序**，运行位于 Kaspersky Security Center Linux 安装文件夹中的 `klbackup.exe` 实用程序。

   “安装向导”将启动。在以 Server Core 模式运行的 Microsoft Windows 上，请使用klbackup 实用程序的控制台版本。

2. 第一步，选择 **执行管理服务器数据备份**。

3. 在 **备份设置** 步骤：

   a. 单击 **浏览** 按钮并创建一个新文件夹，将备份副本与默认目录分开保存，例如 `C:\kscbackups`。

   b. 如果您使用 Microsoft SQL Server，请选择**迁移数据库** → **迁移到 Postgres**选项，以便与快速安装脚本配合使用。使用标准方法部署 Kaspersky Security Center Linux 时，还可以将数据迁移到 MySQL/MariaDB 数据库。

   c. 为备份副本设置密码，以防止未经授权访问数据。

4. 等待备份副本创建完成并退出该实用程序。

将在指定目录中创建一个带有备份时间戳的新子目录。

**创建 Kaspersky Security Center Linux 的备份副本**

1. 在管理服务器设备上，在命令行中运行以下命令：

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. 等待备份过程完成。

将在 `-path` 选项中指定的目录中创建一个带有备份时间戳的新子目录。

创建旧管理服务器的备份副本后，请停用管理服务器设备。

**停用管理服务器设备**

1. 将获取的用于数据迁移的备份副本复制到管理员的设备。
2. 关闭管理服务器的操作系统。
3. 从企业网络中拔下网络适配器。
4. 如果您计划将该设备的 IP 地址重新用于新安装的 Kaspersky Security Center Linux，请释放该设备的 IP 地址。
5. 确保设备已完全关机。

网络中仍存在的旧管理服务器可能会导致设备管理故障并干扰新管理服务器的 Web Console 登录过程，还可能使网络代理安装任务在启动时连接到旧服务器。

## 3 使用快速安装脚本初始部署 Kaspersky Security Center Linux

本指南介绍如何使用快速安装脚本初始部署 Kaspersky Security Center Linux 实例。

**特殊注意事项：**

- Kaspersky Security Center 的所有组件都安装在与管理服务器相同的设备上。
- 管理服务器的操作系统必须为以下系统之一：
  - Astra Linux Special Edition RUSB.10015-01（操作更新 1.8.5），配备 PostgreSQL 15
  - Ubuntu Server 26.04 LTS，配备 PostgreSQL 18
  - CentOS Stream 10 搭配 PostgreSQL 18
  - RED OS 8.0 搭配 PostgreSQL 16
- 快速安装脚本仅自动执行 Kaspersky Security Center 应用程序的配置和安装。管理员必须采取措施，在操作系统中配置管理服务器设备的名称，在操作系统级别配置网络适配器和安全防火墙，并配置硬件。

使用快速安装脚本初始部署 Kaspersky Security Center Linux 实例包括以下步骤：

### 1.准备部署

在继续执行安装步骤之前，您必须准备：

- 操作系统安装磁盘映像和应用程序软件包存储库。
- 用于登录 Web Console 时进行 双因素身份验证 (2FA) 的身份验证器应用程序。
- 新的 FQDN（例如 *ksclinux.example.com*）。如果您在配置解决方案方面拥有足够的经验，则可以在安装过程中使用自己的脚本将原 FQDN 分配给新服务器。在这种情况下，请在步骤 5“从备份副本恢复后配置应用程序”中跳过步骤 4“恢复受管理设备与原管理服务器 FQDN 的连接”。
- 配备浏览器的管理员设备，用于通过互联网下载分发包和管理 Web Console。
- 确保应用程序组件可以使用 DNS 和时间服务器 (NTP)。
- 根据您的方案，如果原 IP 地址曾用于连接受管理设备，请释放该 IP 地址。
- 根据要求配置网络设备和代理服务器：
  - 应用程序组件之间通信所用的端口。
  - 对卡巴斯基服务器的访问权限。
  - 加固指南的建议。

### 2.操作系统容量规划和配置

1. 根据管理服务器将管理的设备数量配置设备。

   每次容量规划计算都会考虑卡巴斯基应用程序的可用资源。该计算考虑了管理服务器、网络代理、DBMS、Web Console 服务器以及 Kaspersky Endpoint Security for Linux 全部在同一设备上运行的情况。但是，该计算未考虑管理服务器备份副本的存储。

   > 使用外部文件共享作为挂载点，以便在单独的设备上存储备份副本，或者在考虑备份存储的情况下提高可用硬盘空间要求。

   我们建议为操作系统增加 4–6 GB 的 RAM 和 20 GB 的可用硬盘空间。

   根据受管理设备的数量确定设备容量：

   - **S**（最多 1000 台设备）：8 个 CPU 核心、16 GB 的 RAM、用于 `/var` 目录的 70 GB 可用硬盘空间、300 IOPS 或更高。
   - **M**（最多 10,000 台设备）：12 个 CPU 核心、24 GB 的 RAM、用于 `/var` 目录的 340 GB 可用硬盘空间、300 IOPS 或更高。
   - **L**（最多 30,000 台设备）：20 个 CPU 核心、40 GB 的 RAM、用于 `/var` 目录的 490 GB 可用硬盘空间、300 IOPS 或更高。
   - **XL**（最多 50,000 台设备）：28 个 CPU 核心、54 GB 的 RAM、用于 `/var` 目录的 640 GB 可用硬盘空间、300 IOPS 或更高。

2. 根据选定的规格，为 Kaspersky Security Center 服务器准备硬件。
3. 在 Kaspersky Security Center 服务器上安装操作系统。

如果您打算通过命令行远程管理管理服务器设备，请在安装期间启用 **SSH 远程连接工具** 选项。

> 安装 Astra Linux 时必须禁用 **强制访问控制** 选项。此外，为了使 Kaspersky Endpoint Security for Linux 正常工作，请禁用 **阻止 ptrace 跟踪** 选项。

4. 如果 `/var` 目录是单独挂载的，请检查该目录的可用磁盘空间；否则，请检查根目录 `/` 的可用磁盘空间。

   M 配置示例：

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                 Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                         Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. 如果先前的管理服务器使用 IP 地址连接受管理设备，请在新服务器上配置该管理服务器的 IP 地址。

*视频：配置操作系统*




### 3.下载分发文件

1. 从卡巴斯基网站下载所需区域设置对应的分发包，并将其保存在单独的目录中（例如，*kscdistr*）。

   **适用于 Ubuntu 和 Astra Linux**

   - 管理服务器的 deb 格式分发包：

     `Version 16.3.0.1207 | Debian x64 | Administration server`

   - Web Console 的 deb 格式分发包：

     `Version 16.3.0.1207 | Debian x64 | Web console`

   - 快速安装脚本：

     `Version 16.3.0.1207 | Linux | KSC installation script`

**适用于 CentOS 和 RED OS**

- 管理服务器的 rpm 格式分发包：
  `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`
- Web Console 的 rpm 格式分发包：
  `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`
- 快速安装脚本：
  `Version 16.3.0.1207 | Linux | KSC installation script`

2. 为了使卡巴斯基应用程序能够在 Astra Linux 的封闭软件环境模式下运行，请下载公钥文件 kaspersky_astra_pub_key.gpg。

3. 使用可移动介质或通过网络将下载的文件复制到新的 Kaspersky Security Center 管理服务器设备。
   以下是使用命令行通过网络复制文件的操作。

   是否可以使用 scp 工具复制文件，取决于管理服务器设备的操作系统中是否正在运行 SSH 服务，以及您组织的安全策略。

   a. 在命令行中，使用 cd 命令切换到 *kscdistr* 目录的上一级目录，例如：

   对于 Linux
   ```
   cd /home/administrator/Desktop
   ```

   对于 Windows
   ```
   cd C:\Users\Administrator\Downloads
   ```

   b. 使用 scp 实用程序通过网络复制分发文件：

   ```
   scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
   ```

   其中：
   `<kscdistr>` 是包含已下载 Kaspersky Security Center 分发包的本地目录。
   `<administrator>` 是新管理服务器上的超级用户，有权使用 SSH 连接。
   `<ksclinux.example.com>` 是新管理服务器的 FQDN 地址。

   文件将复制到指定用户主目录的根级别。

**4.配置安装设置**

1. 在新管理服务器设备上，以超级用户身份登录并打开终端。

2. 转到包含已复制分发包的目录。

   示例
   ```
   cd ~/kscdistr
   ```

3. 将快速安装脚本的压缩包解压到当前包含分发文件的目录中。

示例

```
tar -xf ./ksc_fast_install.tar.gz
```

4. 运行以下命令检查所有文件是否都存在：

```
ls -la
```

ls -la 命令输出示例

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. 在包含分发包的目录中，打开包含安装脚本设置的文本文件进行编辑，例如：

```
nano ./params.txt
```

6. 设置先前准备的值，并移除相关行中的第一个注释字符（#），或添加包含以下值的新行：

- 设备规模（S/M/L/XL 配置的值）。

  示例

  ```
  klfi_netsize=S
  ```

- 文件中两个设置项里的管理服务器 FQDN 地址。

  ```
  klfi_klserver_address=ksclinux.example.com
  ```

  ```
  klfi_kliam_address=ksclinux.example.com
  ```

已安装的管理服务器所使用的语言取决于所下载分发包的区域设置。

7. 检查管理服务器的 FQDN 是否在新管理服务器的操作系统中正确解析为环回 IP 地址。为此，请执行下列操作：

   a. 使用新管理服务器的地址运行 `ping` 命令。

   成功获取环回 IP 地址的示例

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. 如果未获取到地址或获取到的是外部 IP 地址，请将管理服务器的地址添加到新管理服务器上操作系统的 `/etc/hosts` 文件中。

   为此，请执行下列操作：

   - 运行以下命令，打开 `/etc/hosts` 文件进行编辑：

     ```
     sudo nano /etc/hosts
     ```

   - 输入管理服务器设备的 FQDN 作为服务器地址，例如：

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

在受管理设备上，管理服务器的 FQDN 必须解析为服务器的外部 IP 地址。请确保 DNS 服务器上的记录已正确设置。

**5.启动快速安装脚本**

*要运行快速安装脚本：*

1. 重新启动设备后，返回到包含分发包的目录：

   ```
   cd ~/kscdistr
   ```

2. 运行以下命令使文件可执行：

   ```
   chmod +x ./ksc_fast_install.py
   ```

3. 在运行脚本之前，请阅读采用您的本地化语言编写的 最终用户授权许可协议，因为快速安装脚本本身仅提供英文版本。

4. 将网络软件包存储库连接到操作系统，或连接操作系统安装磁盘映像，以便在安装过程中下载软件包。

5. 运行快速安装脚本：

   ```
   sudo ./ksc_fast_install.py
   ```

6. 按照安装向导的步骤操作。

> 如果脚本在资源检查步骤中错误地声称您没有足够的 RAM，请在安装过程中禁用动态 RAM 分配。

7. 等待安装完成。从脚本的文本输出中，保存 Web Console 的用户名（`User`）和密码（`Pass`）。

示例

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

*视频：在 Ubuntu 上运行快速安装脚本*




### 6.首次登录 Web Console

1. 在浏览器中打开 Web Console 地址： `https://<FQDN>:8080`
   其中 `<FQDN>` 是安装脚本设置中的管理服务器地址，例如 *https://ksclinux.example.com:8080*。

2. 使用脚本输出中的用户名和密码登录 Web Console。

3. 配置身份验证器应用程序：

   a. 将用于获取一次性确认码的密钥复制到应用程序，或扫描 Web Console 身份验证向导中的二维码。

   b. 输入生成的确认码以进行身份验证并登录 Web Console。

4. 查看并确认 加固指南。

5. 如果您不打算从备份副本恢复管理服务器的数据，请在 初始配置向导 中配置管理服务器。

## 4 恢复管理服务器的备份副本

在从 Kaspersky Security Center Windows 迁移，或将 Kaspersky Security Center Linux 数据迁移到新硬件的场景中，您可能需要从管理服务器旧安装中创建的备份副本恢复数据。

新服务器上的 PostgreSQL 版本必须至少与备份副本中的版本一致。

如果不需要恢复数据，请跳过此步骤。

如果之前尚未创建备份副本：

- 创建管理服务器旧安装的备份副本，并将数据格式类型设置为 PostgreSQL。
- 安装新的 Kaspersky Security Center Linux 服务器，并首次登录 Web Console。

从备份副本恢复管理服务器包括以下步骤：

**1.将备份副本放置在管理服务器上**

使用可移动介质或网络将旧管理服务器的备份副本放置到新管理服务器设备上。

*要通过网络将备份副本复制到管理服务器：*

是否可以使用 scp 工具复制文件，取决于管理服务器设备的操作系统中是否正在运行 SSH 服务，以及您组织的安全策略。

1. 在命令行中，使用 *cd* 命令转到包含先前管理服务器备份文件的目录，例如：

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. 使用 scp 工具复制包含备份文件的目录：

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   其中：

   `<klbackup202x-xx-xx>` 是存储备份文件的目录。

   `<administrator>` 是新管理服务器上的超级用户，有权使用 SSH 连接。

   `<ksclinux.example.com>` 是新管理服务器的 FQDN 地址。

   包含备份副本的目录将复制到指定用户的主目录。

### 2.从备份恢复的过程

1. 在新管理服务器设备上，打开终端。
2. 从备份副本恢复数据时，请向管理服务器用于连接数据库的标准 klserver 和 kliam 账户授予 PostgreSQL 超级用户权限：

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

3. 使用 klbackup 工具从旧管理服务器的备份副本启动数据恢复：

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
```

其中，`</home/administrator/klbackup202x-xx-xx>` 是包含备份文件的目录的完整路径。

4. 如果未为备份设置密码，则在系统提示输入备份密码时，不输入密码直接按 **Enter** 键。
5. 等待该工具完成运行。
   大型安装环境可能需要很长时间。
6. 恢复管理服务器用于连接数据库的 PostgreSQL 账户的原始权限。

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

## 5 从备份副本恢复后配置应用程序

如果您没有从备份副本恢复数据，请跳过此步骤。

从备份副本恢复后配置应用程序包括以下步骤：

### 1.恢复 Web Console

1. 从 IAM Server 配置文件中获取旧服务器的地址：

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

示例

```
ksc_address: "oldksc.example.internal"
```

2. 检查旧管理服务器的 FQDN 是否正确解析为新管理服务器的环回 IP 地址。为此，请执行下列操作：

a. 使用旧管理服务器的地址运行 `ping` 命令。

成功获取环回 IP 地址的示例

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

b. 如果未获取到地址或获取到的是外部 IP 地址，请将管理服务器的地址添加到新管理服务器上操作系统的 `/etc/hosts` 文件中。为此，请执行下列操作：

- 打开 /etc/hosts 文件进行编辑：

```
sudo nano /etc/hosts
```

- 输入旧服务器的名称作为管理服务器设备地址的附加别名。

示例

```
127.0.0.1       localhost
127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
<...>
```

3. 重新安装 Web Console：

a. 卸载本地 Web Console 服务器：

根据您的 Kaspersky Security Center Linux 分发包，运行以下命令之一：

- 在基于 Debian 的操作系统上：

```
sudo apt remove ksc-web-console -y
```

- 在运行基于 Red Hat Enterprise Linux 的操作系统的设备上：

```
sudo dnf remove ksc-web-console -y
```

b. 从包含分发包的目录安装 Web Console 软件包：

- 在基于 Debian 的操作系统上：

```
sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
```

- 在运行基于 Red Hat Enterprise Linux 的操作系统的设备上：

```
sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
```

**2.从 Kaspersky Security Center Windows 迁移时恢复 kscadmin 用户的访问权限**

用户数据库已被覆盖；请重新创建 kscadmin 用户并配置双因素身份验证。

1. 在管理服务器设备的操作系统中打开终端，并运行以下命令来创建用户：

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   按 **Enter** 键后，输入密码，然后再次输入。

2. 在浏览器中打开 Web Console 地址：

   ```
   https://<FQDN>:8080
   ```

   其中 <FQDN> 是安装脚本设置中的管理服务器地址，例如 *https://ksclinux.example.com:8080*。

3. 使用创建的用户名和密码登录 Web Console。

4. 配置身份验证器应用程序。为此，请执行下列操作：

   a. 在恢复管理服务器的备份副本之前，请从身份验证器应用程序中删除旧的 kscadmin 用户配置文件。

   b. 将用于获取一次性确认码的密钥复制到应用程序，或扫描 Web Console 身份验证向导中的二维码。

   c. 输入生成的确认码以进行身份验证并登录 Web Console。

**3.测试管理服务器**

1. 验证以 kscadmin 和其他用户身份登录时，Web Console 界面是否正常工作。

2. 依次运行以下任务：

   - 将更新下载至管理服务器存储库
   - 管理服务器维护
   - 管理服务器数据备份

   将任务设置中的 Windows 路径替换为新管理服务器上的 Linux 目录，或者删除任务并从头开始配置。

3. 检查任务结果，并在必要时更改任务设置、管理策略和管理服务器设置。

**4.恢复受管理设备与先前管理服务器的 FQDN 的连接**

如果您已为新管理服务器分配新的 FQDN（例如 ksclinux.example.com），请添加以下类型的 DNS 记录之一：

- 一条将管理服务器的旧名称与管理服务器的新名称相匹配的 CNAME 记录。
  有关如何配置必要记录的详细信息，请参阅您的 DNS 服务器文档。
- 适用于先前管理服务器地址并指向管理服务器新 IP 地址的 A 和 AAAA 记录。
  对于基于 Windows Server 的 DNS 服务，请使用适用于您基础架构的值运行命令。

*要为基于 Windows Server 的 DNS 服务添加 DNS A 记录，请使用适用于您基础架构的值运行命令：*

1. 连接到您的 DNS 服务器。
2. 打开 PowerShell，并运行以下命令从现有的 A 记录中获取 IP 地址：

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. 运行以下命令更改 A 记录中的 IP 地址：

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. 运行以下命令，验证 A 记录中的 IP 地址是否已更新：

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

该命令的输出结果包括 Kaspersky Security Center Linux 管理服务器的 IP 地址。本地 DNS 缓存更新后，受管理设备将重新连接。

## 6 配置管理服务器的反病毒保护

要遵循《强化指南》的建议，为管理服务器提供反病毒保护，请在管理服务器上安装卡巴斯基应用程序并配置管理策略。要部署 Kaspersky Endpoint Security for Linux，请参阅部署指南。

安装和配置包括以下步骤：

### 1.创建单独的管理组

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**组层级**”。
2. 选中 **受管理设备** 组旁边的复选框。
3. 单击“**添加**”。
4. 在显示的窗口中，为新组指定名称（例如 *kscserver*），然后单击 **添加** 按钮确认创建。

### 2.创建不继承设置的网络代理策略

1. 在 Web Console 的主窗口中，转到“**资产管理** → **策略**”部分。
2. 单击“**添加**”按钮。

3. 在新策略向导中，选择 **Kaspersky Security Center 网络代理** 应用程序，然后单击 **下一步**。

4. 禁用 **从父策略继承设置** 选项，然后单击 **保存**。

**3.从 Kaspersky Security Center 安装 Kaspersky Endpoint Security for Linux 管理插件或手动安装**

您可以通过以下方式安装 Kaspersky Endpoint Security for Linux 管理插件：

- 从 Web Console 中可用的分发包列表安装。
- 从文件手动安装。

*要从 Web Console 中可用的分发包列表安装 Kaspersky Endpoint Security 管理插件：*

1. 在 Web Console 的主窗口中，选择“**设置** → **Web 插件**”。
   已安装的 Web 插件列表将打开。

2. 单击“**添加**”按钮。
   这将打开可用管理插件列表。当新版本的 Web 插件发布后，该列表会自动更新。

3. 在可用插件列表中，选择最新可用版本的 Kaspersky Endpoint Security for Linux Web 插件。

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

5. 等待安装完成，然后在信息窗口中单击“**确定**”。

新插件将显示在已安装的 Web 插件列表中。

*视频：使用向导安装管理 Web 插件*




*要从文件手动安装 Kaspersky Endpoint Security 管理插件：*

1. 从应用程序下载页面的 Kaspersky Endpoint Security for Linux 部分下载包含 Web 插件的压缩包：**应用程序控制插件** → **Web Console 插件**。

2. 将下载的压缩包解压到本地。

3. 在 Web Console 的主窗口中，选择“**设置** → **Web 插件**”。
   已安装的 Web 插件列表将打开。

4. 单击“**从文件添加**”按钮。

5. 这将打开一个窗口；在该窗口中，指定 plugin.zip 文件的路径和 signature.txt 文件的路径。
   这些文件位于您将 Web 插件压缩包解压到的文件夹中。

6. 单击“**添加**”按钮。

7. 等待安装完成，然后在信息窗口中单击“**确定**”。

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

*视频：在隔离网络中安装管理 Web 插件*




### 4.创建不继承设置的 Kaspersky Endpoint Security for Linux 策略

将 Kaspersky Endpoint Security for Linux 与 Kaspersky Security Center Linux 配合使用时，您需要按照卡巴斯基专家的建议管理策略设置。

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。

2. 为管理服务器选择一个管理组。

3. 单击“**添加**”。
   “策略向导”将启动。

4. 在显示的窗口中，从列表中选择 Kaspersky Endpoint Security for Linux。

5. 指定 Kaspersky Endpoint Security for Linux 应用程序的 **标准模式或 Endpoint Detection and Response Agent 模式**。

6. 决定是否要参与卡巴斯基安全网络。

7. 查看受管理设备的优化建议。

8. 在策略名称中，指明该策略属于管理服务器。

9. 禁用 **从父策略继承** 选项。

10. 保存更改。

*视频：创建策略*




**5.创建 Kaspersky Endpoint Security for Linux 的更新组任务**

1. 在 Web Console 的主窗口中，选择“**任务**”部分。

2. 为管理服务器选择一个管理组。

3. 单击“**添加**”。
   “任务向导”将启动。

4. 在显示的窗口中，从列表中选择 Kaspersky Endpoint Security for Linux。

5. 指定 *更新* 任务类型，然后执行后续步骤，无需更改设置。
   任务属性窗口将打开。

6. 在 **应用程序设置** → **更新源** 部分中，启用 Kaspersky Security Center 源并提高其优先级。

在隔离网络中，使用卡巴斯基更新实用程序为更新任务创建存储库。

*视频：配置集中式数据库更新*




**6.将授权许可密钥添加到具有自动密钥分发功能的管理服务器存储库**

1. 在 Kaspersky Security Center Web Console 主窗口中，转到“**授权许可**”部分。
2. 单击“**添加**”。
3. 指定“**激活码**”选项，然后单击“**发送**”。
   在隔离网络中，使用可通过 https://keyfile.kaspersky.com/en-US 服务请求的密钥文件。
4. 在授权许可列表中，单击授权许可的名称。
5. 选择**自动分发授权许可密钥到受管理设备**复选框。
6. 保存更改。

*视频：使用激活码激活应用程序*



*视频：使用密钥文件激活应用程序*




**7.为网络代理和 Kaspersky Endpoint Security for Linux 创建安装包**

1. 在 Web Console 的主窗口中，选择“**软件管理**” → “**安装包**”。
2. 单击“**添加**”。
   创建安装包的向导将启动。
3. 选择“**为卡巴斯基应用程序创建安装包**”。
4. 在应用程序列表中，找到最新版本的 Kaspersky Endpoint Security for Linux，然后单击其名称。
5. 在侧边栏中，单击“**下载并创建安装包**”按钮开始下载。
   阅读并接受最终用户授权许可协议，以开始使用应用程序。
6. 返回应用程序列表，然后下载适用于 Linux 的网络代理的最新版本。
   阅读并接受最终用户授权许可协议，以开始使用应用程序。
7. 在 Web Console 主窗口的已下载应用程序列表中，单击应用程序的名称。

在隔离网络中，从卡巴斯基网站下载分发包，然后在新安装包向导中选择“**从文件创建安装包**”选项。

*视频：在 Kaspersky Security Center 中自动创建安装包*



*视频：在 Kaspersky Security Center 中手动创建安装包*




### 8.安装适用于 Linux 的网络代理

1. 在 Web Console 主窗口中，选择**“软件管理”** → **“安装包”**。
2. 选中 **卡巴斯基网络代理 for Linux** 安装包旁边的复选框。
3. 单击**“展开”**。
   保护部署向导将启动。
4. 选择**“使用独立安装包”**选项。
5. 在**“将设备移动到受管理设备文件夹”**步骤，跳过配置用于将设备移动到管理组的规则。此选项不适用于管理服务器设备。
6. 在**“创建独立安装包的结果”**步骤，选择并复制应用程序安装脚本的完整路径。
7. 在管理服务器的操作系统中，打开命令行。
8. 开始安装独立安装包：

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   其中，`</var/opt/.../stand-alone_package_sh>` 是此前复制的应用程序独立安装包脚本文件的完整路径。
   如果安装成功，将显示相应的通知。
9. 将管理服务器设备（例如 *ksclinux*）从 **受管理设备** 组移动到之前准备好的管理组（例如 *kscserver*）。

### 9.安装 Kaspersky Endpoint Security for Linux

1. 在 Web Console 主窗口中，选择**“软件管理”** → **“安装包”**。
2. 选中 Kaspersky Endpoint Security for Linux 安装包旁边的复选框。
3. 单击**“展开”**。
   保护部署向导将启动。
4. 选择**“使用独立安装包”**选项。

5. 在**“创建独立安装包的结果”**步骤，选择并复制应用程序安装脚本的完整路径。
6. 在管理服务器的操作系统中，打开命令行。
7. 开始安装独立安装包：

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

其中，`</var/opt/.../stand-alone_package_sh>` 是此前复制的应用程序独立安装包脚本文件的完整路径。

如果安装成功，将显示相应的通知。

8. 在 Web Console 主窗口的**“任务”**区域中，选择管理组列表中以管理服务器名称命名的根节点。
9. 在管理服务器任务列表中，按顺序启动以下任务：
   - 将更新下载至管理服务器存储库
   - Update (Kaspersky Endpoint Security for Linux)
10. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（设备）**”。
11. 单击管理服务器设备对象的名称。
12. 检查设备状态的主要指标：
    - 反病毒数据库的上次更新（当前）。
    - 已连接到管理服务器（当前）。
    - 保护状态（正在运行）。
    - *成功添加密钥*事件（存在）。

使用 Kaspersky Endpoint Security for Linux 部署指南在网络中的设备上部署安全解决方案。

# 从先前的版本更新应用程序

可以通过在受保护设备上远程或本地安装应用程序的新版本来升级 Kaspersky Endpoint Security 应用程序。

您只能从 Kaspersky Endpoint Security 12.4 for Linux 升级到 Kaspersky Endpoint Security 12.5 for Linux。

不支持将更早的 Kaspersky Endpoint Security 版本升级到版本 12.5。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 12.5 for Linux。

您可以按照以下步骤升级应用程序。

## 1 准备环境

在开始升级 Kaspersky Endpoint Security 之前，请根据您的基础架构完成必要的准备步骤。

## 2 准备分发包

选择分发包，具体取决于您的操作系统、其架构和 CPU 类型。

## 3 更新 Kaspersky Endpoint Security 管理插件

如果您使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security，请更新 Kaspersky Endpoint Security 管理 Web 插件或 MMC 插件，具体取决于您用于管理 Kaspersky Security Center 的控制台。

## 4 更新受保护设备上的应用程序和图形界面

在受保护设备上安装应用程序的新版本。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。

如果您在基本模式或 EDR Agent 模式下使用 Kaspersky Endpoint Security，并且使用应用程序的图形界面，也请更新图形界面。

您可以通过以下方式更新应用程序和应用程序的图形界面：

- 使用 Kaspersky Security Center 远程执行
- 通过命令行在本地执行

**如何使用命令行从 RPM 包升级应用程序**

在命令行上升级应用程序相当于在设备上安装新版本的应用程序。

> 您需要 root 权限才能更新应用程序。

*要升级应用程序，运行以下命令：*

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] rpm -U --replacefiles --
replacepkgs kesl-12.5.0-<build number>.<arch>.rpm [kesl-gui-12.5.0-<build number>.<arch>.rpm]
```

Kaspersky Endpoint Security 将自动重启。

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| KESL_EULA_AGREED=yes | 接受最终用户授权许可协议的条款和条件。 |
| KESL_PRIVACY_POLICY_AGREED=yes | 接受隐私策略的条款和条件。 |
| KESL_USE_KSN=yes/no | 使用卡巴斯基安全网络：<br>yes – 接受卡巴斯基安全网络声明的条款并启用卡巴斯基安全网络。<br>no – 拒绝卡巴斯基安全网络声明的条款并禁用卡巴斯基安全网络。 |

| 设置 | 描述 |
| --- | --- |
| <arch> | 架构类型：<br>i386 – 适用于 32 位操作系统<br>x86_64 – 适用于 64 位操作系统<br>aarch64 – 适用于 Arm 架构 64 位操作系统 |

Kaspersky Endpoint Security 将自动重启。

**示例：**

更新适用于 64 位操作系统的带有 GUI 包的 RPM 应用程序包：

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.5.0-<build number>.x86_64.rpm kesl-gui-12.5.0-<build number>.x86_64.rpm
```

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。

### 如何使用命令行从 DEB 包升级应用程序

在命令行上升级应用程序相当于在设备上安装新版本的应用程序。

您需要 root 权限才能更新应用程序。

*要升级应用程序，运行以下命令：*

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] apt-get install ./kesl_12.5.0-<build number>_<arch>.deb [./kesl-gui_12.5.0-<build number>_<arch>.deb]
```

Kaspersky Endpoint Security 将自动重启。

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| KESL_EULA_AGREED=yes | 接受最终用户授权许可协议的条款和条件。 |
| KESL_PRIVACY_POLICY_AGREED=yes | 接受隐私策略的条款和条件。 |
| KESL_USE_KSN=yes/no | 使用卡巴斯基安全网络：<br>yes – 接受卡巴斯基安全网络声明的条款并启用卡巴斯基安全网络。<br>no – 拒绝卡巴斯基安全网络声明的条款并禁用卡巴斯基安全网络。 |
| <arch> | 架构类型：<br>i386 – 适用于 32 位操作系统<br>amd64 – 适用于 64 位操作系统<br>arm64 – 适用于 Arm 架构 64 位操作系统 |

**示例：**

更新适用于 64 位操作系统的带有 GUI 包的 DEB 应用程序包：

```
# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes apt-get install ./kesl_12.5.0-<build number>_amd64.deb [./kesl-gui_12.5.0-<build number>_amd64.deb]
```

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。

### 5 更新 Kaspersky Security Center 网络代理

可选步骤。如果您使用 Kaspersky Security Center 集中管理 Kaspersky Endpoint Security，请更新受保护设备上的网络代理。升级是通过安装新版本的网络代理来执行的。

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。有关更多详细信息，请参阅 Kaspersky Security Center 帮助。

在网络代理更新期间，应用程序将继续正常工作。

升级应用程序以前版本的特点

- 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。
- 在包管理器类型为 `rpm` 的操作系统上，如果同时安装了应用程序包和 GUI 包，我们不建议只更新其中一个包而不更新另一个。

  在包管理器类型为 `dpkg` 的操作系统上，如果同时安装了应用程序包和 GUI 包，则两个包必须同时更新。
- 如果新版本的应用程序更改了最终用户授权许可协议和/或隐私策略的条款和条件，您必须在更新期间接受新条款和条件。用户协议文本可在 卡巴斯基网站（**EULA** 部分）以及 `~/.kesl/12.5/license.<language ID>` 目录中获取。

  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。您可以在 ~/.kesl/12.5/ksn_license.<language ID> 中找到卡巴斯基安全网络声明的文本。拒绝使用卡巴斯基安全网络不会中断更新过程。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。
- 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。

- 当您更新应用程序时，先前版本的事件日志文件将成为当前版本文件集中的第一个事件文件。该文件将一直保留，直到剩余文件中的事件数达到指定的最大数量（`MaxEventsNumber`设置）。因此，可能会出现一种暂时的情况，即应用程序存储的事件数量是`MaxEventsNumber`设置中指定的两倍。

- 如果 Kaspersky Endpoint Security 在基本模式或 EDR Agent 模式下使用，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

**如何安装管理 Web 插件**

您可以通过以下方式安装 Web 插件：

- 使用 Kaspersky Security Center Web Console 的快速启动向导。

  首次将 Kaspersky Security Center Web Console 连接到管理服务器时，Kaspersky Security Center Web Console 会自动提示您运行快速启动向导。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 → 快速启动向导**）。快速启动向导还可以检查已安装的 Web 插件是否为最新，并下载必需的更新。有关 Kaspersky Security Center Web Console 快速启动向导的详细信息，请参阅 Kaspersky Security Center 帮助。

- 手动安装，使用卡巴斯基 Web 插件列表中的分发包或来自文件的分发包。

*如要从 Kaspersky Security Center 手动安装 Kaspersky Endpoint Security Web 插件：*

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

   已安装的 Web 插件列表将打开。

2. 单击“**添加**”按钮。

   这将打开可用管理插件列表。当新版本的 Web 插件发布后，该列表会自动更新。

3. 在可用插件列表中，选择 **Kaspersky Endpoint Security <version number> for Linux Web 插件**。

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

5. 等待安装完成，然后在信息窗口中单击“**确定**”。

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

*如要从文件手动安装 Kaspersky Endpoint Security Web 插件：*

1. 从 应用程序下载页面 的 **Kaspersky Endpoint Security for Linux** 部分（**附加分发包 → Web Console 插件**）下载包含 Web 插件的压缩包。

2. 将下载的压缩包解压到本地。

3. 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。

4. 单击“**从文件添加**”按钮。

5. 这将打开一个窗口；在该窗口中，指定 plugin.zip 文件的路径和 signature.txt 文件的路径。这些文件位于您将 Web 插件压缩包解压到的文件夹中。

6. 单击“**添加**”按钮。

7. 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。

**如何安装 MMC 管理插件**

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：*

1. 从 应用程序下载页面 的 **Kaspersky Endpoint Security for Linux** 部分（**构建** → **管理插件**）下载 klcfginst.msi 文件。

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

安装后，MMC 管理插件将显示在 Kaspersky Security Center 管理服务器属性中已安装的 MMC 管理插件列表中。

*如要查看已安装的管理 MMC 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：

   - 打开 **管理服务器 <服务器名称>** 节点的上下文菜单，然后选择 **属性** 项。
   - 在 **管理服务器** 部分中，单击 **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 的管理 MMC 插件：**Kaspersky Endpoint Security <版本号> for Linux**。

转换策略和任务

为先前版本的 Kaspersky Endpoint Security 配置的策略和任务与应用程序的更新版本不兼容。如果使用 Kaspersky Security Center 管理控制台来管理应用程序，则在更新 MMC 管理插件后，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）。

转换后的策略和任务命名为“*<原始策略或任务的名称>（已转换）*”。

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。

您无法在 Kaspersky Security Center Web Console 中转换策略和任务。

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。

管理插件的特殊注意事项

- 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。

- 为同一版本的应用程序安装新的 MMC 管理插件时，您必须先卸载当前已安装的该版本 MMC 插件，然后再安装该版本的新 MMC 插件。

# 升级后的应用程序设置

如果您使用 Kaspersky Security Center 管理控制台管理应用程序，则可以*转换策略*，使新版本使用为该应用程序的先前版本指定的策略设置值（有关更多信息，请参阅 Kaspersky Security Center 帮助）。

您无法在 Kaspersky Security Center Web Console 中转换策略。

使用命令行更新应用程序后，大多数设置都会从应用程序的先前版本延续下来。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。

### 系统事件拦截设置

如果在应用程序的先前版本中选择了基于可更新内核模块的系统事件拦截机制，则更新后应用程序将切换到使用 fanotify 拦截系统事件。然后，在更新数据库和应用程序程序模块并自动重启后，应用程序将再次恢复使用可更新内核模块。

### 卡巴斯基安全网络设置

在 MMC 插件中转换策略后，策略属性中的卡巴斯基安全网络设置取决于您是接受还是拒绝策略和任务批量转换向导中的卡巴斯基安全网络声明的条款：

- 如果您接受本声明的条款，则选择**扩展 KSN 模式**选项。
- 如果您拒绝该声明的条款，请选择**"不使用 KSN"**选项。

通过命令行更新应用程序后，`UseKSN` 设置将修改如下：

- 如果您在升级期间设置 `KESL_USE_KSN=No`，则 `UseKSN=No`。
- 如果您在升级期间设置 `KESL_USE_KSN=Yes`，则 `UseKSN=Extended`。
- 在其他情况下，`UseKSN`设置的值在更新后不会改变。

## 云模式设置

在 MMC 插件中转换策略后，云模式使用设置可能会发生变化，具体取决于您是否接受或拒绝策略和任务批量转换向导中的卡巴斯基安全网络声明的条款：

- 如果您接受声明的条款，则**启用云模式**复选框将被选中。
- 如果您拒绝声明的条款，则**启用云模式**复选框将被清除。

在命令行上更新应用程序后，`CloudMode` 将被设置为：

- `CloudMode=No`：如果更新后设置了 `UseKSN=No`。
- 如果在更新后设置了 `UseKSN=Basic/Extended`，并且在更新前设置了 `CloudMode=Yes`，则为 `CloudMode=Yes`。

如果启用了 KSN，则云模式可用。要启用云模式：

- 在管理控制台或 Web Console 中，选择**扩展 KSN 模式**选项并选中**启用云模式**复选框。
- 在命令行中，设置以下设置：

```
UseKSN=<Basic|Extended>
CloudMode=Yes
```

### Kaspersky Managed Detection and Response 整合设置

如果已启用 MDR 组件，则在 MMC 插件中转换策略后，MDR 组件的状态取决于您在策略和任务转换向导中是接受还是拒绝了卡巴斯基安全网络声明的条款：

- 如果您接受了该声明的条款，MDR 组件将保持启用状态（“**启用 Managed Detection and Response**”复选框被选中）。
- 如果您拒绝了该声明的条款，则“**启用 Managed Detection and Response**”复选框将被清除。

在命令行上更新应用程序后，`UseMDR` 将被设置为：

- `UseMDR=No`：如果更新后设置了 `UseKSN=No`。
- 如果在更新后设置了 `UseKSN=Basic/Extended`，并且在更新前设置了 `UseMDR=Yes`，则为 `UseMDR=Yes`。

如果您想使用 Kaspersky Managed Detection and Response 功能，则需要启用卡巴斯基安全网络的扩展模式。

### Endpoint Detection and Response Expert 集成设置

新版应用程序提供 Kaspersky Endpoint Detection and Response Expert (cloud) 集成模式。

Kaspersky Endpoint Security for Linux 与 Kaspersky Endpoint Detection and Response Expert (cloud) 的集成暂时不可用。计划在 2026 年底之前支持此功能。请关注我们的发行说明，以了解应用程序升级和新功能。

在 MMC 插件中转换策略后，与 Endpoint Detection and Response Expert (cloud) 的集成将被禁用（**启用 Endpoint Detection and Response Expert (cloud)** 复选框将被取消选中）。应用程序使用 Endpoint Detection and Response Expert (on-premises) 集成。

通过命令行更新应用程序后，`EDR_EXPERT_CLOUD_MODE` 设置为：`EDR_EXPERT_CLOUD_MODE=No`（默认值）。

### 用户权限设置

新版应用程序支持密码保护。

在 MMC 插件中转换策略后，密码保护将被禁用。

通过命令行升级应用程序后，将根据应用程序先前版本中配置的用户角色（*kesladmin*、*kesluser*、*keslaudit*、*nokesl*）保留用户权限。

# 卸载应用程序

您可以按照以下步骤卸载 Kaspersky Endpoint Security。

## 卸载 Kaspersky Endpoint Security for Linux 的特殊注意事项

- 卸载应用程序时，设备上的所有 Kaspersky Endpoint Security 任务都会停止。
- 卸载应用程序后，应用程序保存的所有信息都将被删除，包括已安装的任何应用程序证书。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。唯一计算机 ID（SensorID）也会被保存。
- 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。

## 1 卸载应用程序及其图形界面

从受保护设备卸载应用程序软件包和图形界面软件包。

您可以同时卸载应用程序软件包和图形界面软件包，或者仅卸载图形界面软件包。如果安装了图形界面软件包，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界面：

使用 Kaspersky Security Center 远程执行

**通过命令行在本地执行**

卸载需要 root 权限。

卸载过程完成后，会显示有关卸载结果的消息。

**移除应用程序包和图形用户界面软件包**

卸载从 RPM 软件包安装的应用程序和图形界面

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

卸载从 DEB 软件包安装的应用程序和图形用户界面

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

### 移除在不使用图形界面的情况下使用的应用程序包

删除通过 RPM 包安装的应用程序

```
rpm -e kesl
```

删除通过 DEB 包安装的应用程序

```
apt-get purge kesl
```

### 移除图形用户界面软件包

卸载从 RPM 软件包安装的应用程序的图形界面

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

卸载从 DEB 软件包安装的应用程序的图形界面

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

卸载在后台进行。

## 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

### 通过命令行在本地执行

卸载需要 root 权限。

卸载过程完成后，会显示有关卸载结果的消息。

卸载从 RPM 软件包安装到 32 位操作系统上的网络代理

```
rpm -e klnagent
```

卸载从 RPM 软件包安装到 64 位操作系统上的网络代理

```
rpm -e klnagent64
```

卸载从 DEB 软件包安装到 32 位操作系统上的网络代理

```
apt-get purge klnagent
```

卸载从 DEB 软件包安装到 64 位操作系统上的网络代理

```
apt-get purge klnagent64
```

### ❸ 卸载 Kaspersky Endpoint Security 管理插件

如果您使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security，则必须卸载 Kaspersky Endpoint Security 管理 Web 插件或 MMC 插件，具体取决于您用于管理 Kaspersky Security Center 的控制台。

**如何移除 Kaspersky Endpoint Security MMC 管理插件**

1. 关闭 Kaspersky Security Center 管理控制台。
2. 在安装了 Kaspersky Security Center 管理控制台的设备上，打开 Windows 注册表编辑器并转到：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   此项包含有关管理控制台中安装的所有管理插件的信息。受管理应用程序的名称位于 **DisplayName** 值中。
3. 选择与 Kaspersky Endpoint Security 应用程序插件相关版本对应的部分。
4. 打开并复制 **UninstallString** 值。
5. 以管理员身份打开命令提示符，粘贴复制的值并按 **Enter**。

**如何移除 Kaspersky Endpoint Security 管理 Web 插件**

1. 在 Kaspersky Security Center Web Console 的主窗口中，选择 **设置** → **Web 插件**。
   已安装的 Web 插件列表将打开。
2. 选中 **Kaspersky Endpoint Security <version number> for Linux** 复选框。
3. 单击“**删除**”。
   确认卸载该 Web 插件。

# 使用应用程序

默认情况下，引导操作系统时，Kaspersky Endpoint Security 会自动启动（处于每个操作系统的默认执行级别）。

当应用程序以默认配置启动时，将启动以下组件：

- 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，会在设备上自动启动服务任务，以确保其他应用程序功能的运行：应用程序激活功能和备份区功能。

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。在 PS 运行模式下中断的用户任务无法从中断处继续执行。下次启动应用程序时，此类任务将从头开始执行，而不会从中断处继续执行。有关任务类型的更多信息，请参阅 Kaspersky Endpoint Security 本地任务部分。

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。

**如何使用 Web Console 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 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/控制板**”窗口中的“**保护状态**”小部件来监控应用程序运行状态。

### 如何使用管理控制台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”。
6. 执行下列操作之一：
    – 启动应用程序。
    – 停止应用程序。
   您还可以通过上下文菜单管理应用程序。

### 如何使用命令行启动或停止应用程序

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、/u

#### 使用 systemd 的操作系统

启动应用程序

```
systemctl start kesl
```

停止应用程序

```
systemctl stop kesl
```

重启应用程序

```
systemctl restart kesl
```

显示应用程序的当前状态

```
systemctl status kesl
```

### 使用 init 的操作系统

启动应用程序

```
service kesl start
```

停止应用程序

```
service kesl stop
```

重启应用程序

```
service kesl restart
```

显示应用程序的当前状态

```
service kesl status
```

# 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。

### 授权许可类型

#### 免费

- *试用版* – 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。

  您只能使用试用授权许可激活应用程序一次。应用程序在使用商业授权许可激活后，不能再使用试用授权许可激活。

- *Kaspersky Security Center 云控制台试用授权许可*是一种用于评估云控制台的授权许可。使用此授权许可，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。

  30 天期限到期后，该试用工作区及其所有内容都将被自动删除。

#### 付费

- *商业* - 购买应用程序时提供的付费授权许可。

  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。

- *订阅*是应用程序的购买订单，具有特定参数（订阅到期日期、受保护设备数量）。您可以从您所在地区的服务提供商处购买订阅。

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）。有限订阅过期时，您可能得到订阅续费宽限期，在此期间应用程序继续运行。服务提供商决定是否提供宽限期，如果提供的话，还将确定宽限期期限。

您可以在服务提供商的网站上管理您的订阅，包括取消订阅。

## 授权许可如何运作

### 1 您将收到激活码

在 卡巴斯基官方网站 或从我们的某个合作伙伴处购买卡巴斯基解决方案后，您将在购买期间指定的电子邮件地址收到一封邮件。此消息将包含激活码以及有关如何获取密钥文件的信息。如果您的组织不支持使用激活码在线激活应用程序，您可能需要密钥文件。

如果您已购买 Kaspersky Endpoint Security 订阅，服务提供商将只向您提供激活码。

### 2 激活应用程序

接下来，您需要*激活应用程序*，即使应用程序授权许可生效。为此，您需要使用激活码或密钥文件将授权许可密钥添加到应用程序中。

提供以下激活方法：

- 使用 Kaspersky Security Center 远程激活
- 在命令行上
- 通过图形界面

**标准模式**

要在标准模式下使用应用程序，您可以使用涵盖不同功能范围的授权许可。如果您的授权许可未涵盖某些组件，您可能需要另一个授权许可密钥：

- Kaspersky Endpoint Detection and Response Optimum 附加模块授权许可密钥（下文亦称为 *EDR Optimum 密钥*），用于激活 Kaspersky EDR Optimum 组件
- Kaspersky Unified Monitoring and Analysis Platform 附加模块授权许可密钥（下文亦称为 *KUMA 密钥*），用于激活与 Kaspersky Unified Monitoring and Analysis Platform 功能的集成
- Kaspersky Managed Detection and Response Optimum/Expert 附加模块授权许可密钥（下文亦称为 *MDR 密钥*），用于激活 Kaspersky MDR 组件
- Kaspersky Endpoint Detection and Response Expert (on-premises) 附加模块授权许可密钥（下文亦称为 *EDR Expert (on-premises) 密钥*），用于激活 EDR Expert (on-premises) 组件
- Kaspersky Endpoint Detection and Response Expert (cloud) 附加模块授权许可密钥（下文亦称为 *EDR Expert (cloud) 密钥*），用于激活 EDR Expert (cloud) 组件
- Kaspersky Workload Security Module 附加模块授权许可密钥（下文亦称为 *KWSM 密钥*），用于激活 系统完整性监控 和 容器扫描 组件

如果您的授权许可未涵盖这些组件，您只能在激活 Kaspersky Endpoint Security 应用程序本身后激活它们。

**EDR Agent 模式**

如果您在 EDR Agent 模式下使用 Kaspersky Endpoint Security 应用程序，则需要 EDR Expert (on-premises) 授权许可密钥才能将其激活。

**Light Agent 模式**

如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security，则无需向应用程序添加密钥。您需要在 Protection Server 端激活 Kaspersky Security for Virtualization Light Agent。

Endpoint Detection and Response Optimum 组件以及用于与卡巴斯基解决方案集成的组件也在 Protection Server 端激活。

排查应用程序激活问题

3. **续订授权许可或订阅**

我们建议您留意授权许可或订阅，以便及时续订。我们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。

为及时续订授权许可，您可以使用备用密钥。您可以在服务提供商的网站上手动或自动续订订阅。如果已按时对供应商的服务进行预付，无限期订阅会自动续订。

**添加密钥时的特殊注意事项**

- 试用授权许可密钥或订阅密钥不能作为备用密钥添加。
- 备用密钥的到期日期必须晚于活动密钥的到期日期。
- 如果应用程序中已添加活动密钥和备用密钥，而您又添加新的活动密钥，则新密钥会替换之前添加的活动密钥；如果您添加新的备用密钥，则会替换之前添加的备用密钥。
- 如果应用程序中已添加活动密钥以及用于激活 Endpoint Detection and Response Optimum 组件和用于与卡巴斯基解决方案集成的组件的密钥，并且您已为同样涵盖 Endpoint Detection and Response Optimum 组件和用于与卡巴斯基解决方案集成的组件的授权许可添加了一个备用密钥，则在活动密钥过期后，该备用密钥将变为活动密钥并释放其他活动密钥。然后，您可以使用这些密钥在另一台设备上激活 Endpoint Detection and Response Optimum 组件和集成组件。

4. **查看有关已添加的授权许可密钥的信息**

您可以使用 Kaspersky Security Center 远程查看有关添加到应用程序的授权许可密钥的信息，也可以在受保护设备上使用命令行或图形界面在本地查看。

## 实用文章

### 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。

您可以阅读最终用户授权许可协议和隐私策略，其中描述了数据处理和提供：

- 安装应用程序之前，请阅读 license.<语言标识符> 文件。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）或在初始应用程序配置期间（如果使用命令行安装）确认您同意最终用户授权许可协议和隐私策略的条款和条件，即表示您接受最终用户授权许可协议和隐私策略的条款和条件。如果您不接受最终用户授权许可协议或隐私策略的条款，则必须取消应用程序安装，且不得使用该应用程序。

- 应用程序安装后，包含卡巴斯基应用程序最终用户授权许可协议和隐私策略文本的文件位于受保护设备的 /opt/kaspersky/kesl/doc/license.<语言 ID> 目录中。

**激活码**

*激活码*是由 20 个字母数字字符组成的唯一序列。

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。

**密钥文件**

*密钥文件*是您从 Kaspersky 接收到的 .key 扩展名的文件。要使用密钥文件激活应用程序，您不需要连接到卡巴斯基激活服务器。

如果意外删除了密钥文件，您可以将其恢复。您可能需要密钥文件注册诸如 Kaspersky CompanyAccount 之类的服务。

要恢复密钥文件，请执行以下任一操作：

- 联系授权许可销售商。
- 基于您现有的激活码在卡巴斯基网站上获取密钥文件。

**授权许可密钥**

*授权许可密钥*是一个位序列，可用于按照最终用户授权许可协议条款激活和使用应用程序。授权许可密钥由卡巴斯基专家生成。

应用程序当前用于激活的密钥将成为*活动授权许可密钥*。作为活动密钥，您可以添加试用授权许可密钥、商业授权许可密钥（商业密钥）或订阅密钥。

**备用密钥**

*备用授权许可密钥*是允许用户使用应用程序但当前未使用的授权许可密钥。与当前活动的授权许可密钥相关联的授权许可过期时，备用授权许可密钥将自动成为活动授权许可密钥。只有在添加活动密钥后，才能添加备用密钥。

试用授权许可密钥只能作为活动授权许可密钥添加。无法将试用授权许可密钥添加为备用授权许可密钥。

# 如何切换到其他卡巴斯基解决方案

如果应用程序在 Light Agent 模式下使用，则授权许可密钥在 Kaspersky Security for Virtualization Light Agent 解决方案中管理。

如果您的组织已部署卡巴斯基解决方案，Kaspersky Endpoint Security 在标准模式或 EDR Agent 模式下使用，并且您需要切换到其他卡巴斯基解决方案，请执行以下步骤。

1. **准备新授权许可**

   在 卡巴斯基网站 或通过我们的合作伙伴购买其他卡巴斯基解决方案。您将在购买时指定的电子邮件地址收到一封电子邮件。此消息将包含激活码以及有关如何获取密钥文件的信息。

   如果您之前使用激活码激活了 Kaspersky Endpoint Security 应用程序，则这次也需要使用激活码。如果您之前使用密钥文件激活了应用程序，则需要使用密钥文件。

2. **替换您的授权许可**

   您可以通过以下方式替换授权许可：

   - 使用 Kaspersky Security Center 远程执行。将授权许可密钥添加到管理服务器存储库，并将其分发到受保护设备。
   - 在 命令行 上使用以下命令：`kesl-control [-L] --add-active-key <path to key file / activation code>`。
   - 在 图形界面 中，删除当前应用于应用程序的密钥并添加新密钥。

3. **确保授权许可已成功替换**

   为此，请查看授权许可密钥的详细信息，该密钥用于您的受保护设备。

实用文章

**激活码**

*激活码*是由 20 个字母数字字符组成的唯一序列。

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。

**密钥文件**

*密钥文件*是您从 Kaspersky 接收到的 .key 扩展名的文件。要使用密钥文件激活应用程序，您不需要连接到卡巴斯基激活服务器。

如果意外删除了密钥文件，您可以将其恢复。您可能需要密钥文件注册诸如 Kaspersky CompanyAccount 之类的服务。

要恢复密钥文件，请执行以下任一操作：

- 联系授权许可销售商。
- 基于您现有的激活码在卡巴斯基网站上获取密钥文件。

# 管理授权许可密钥

如果应用程序在 Light Agent 模式下使用，则授权许可密钥在 Kaspersky Security for Virtualization Light Agent 解决方案中管理。授权许可密钥管理命令返回错误。

## 使用 Kaspersky Security Center 管理密钥

在 Kaspersky Security Center 中，您可以通过以下方式向受管理设备添加密钥：

- 使用“*添加密钥*”任务。此方法允许向单个设备上的应用程序或管理组中包含的所有设备上的应用程序添加密钥。创建任务时，它使用添加到 Kaspersky Security Center 密钥存储的密钥。您可以提前或在创建“添加密钥”任务时将授权许可密钥添加到密钥存储中。
- 将存储在 Kaspersky Security Center 管理服务器上的密钥分发到设备。使用此方法可以自动向已连接到 Kaspersky Security Center 的受管理设备和新的受管理设备添加密钥。要使用此方法，先将密钥添加到 Kaspersky Security Center 密钥存储中。

  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。

**如何使用 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**”按钮。
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**”按钮。

添加的密钥将出现在密钥列表中。

### 如何使用“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“**任务**”。
   任务列表打开。
2. 单击“**添加**”按钮。
   “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**”。
   这将打开 **选择授权许可** 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. 如果您需要的密钥不在密钥存储中，请单击 **添加新的授权许可密钥** 链接。
   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. 在 **应用程序设置** 选项卡上，您可以选中 **用作备用密钥** 复选框。添加为备用密钥的密钥将在当前密钥过期后变为活动状态。
9. 结束向导。
   在任务列表中将显示一个新任务。
10. 选中该任务旁边的复选框。单击**启动**按钮。

### 如何使用 Web Console 通过将密钥分发到设备来向应用程序添加密钥

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**”按钮。

授权许可密钥将自动分发到相应的客户端设备。

仅当应用程序尚未在设备上激活或距离授权许可到期不足 14 天时，新的授权许可密钥才会被添加到设备。

在命令行中管理密钥

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。

### 如何向应用程序添加密钥

您可以使用这些命令添加用于激活应用程序的密钥，以及用于激活授权许可未涵盖的组件的密钥。您不需要在命令中指定密钥的类型。

将活动授权许可密钥添加到应用程序

```
kesl-control [-L] --add-active-key <path to key file / activation code>
```

其中：

- `path to key file` 是密钥文件的路径。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` 是激活码。

将备用授权许可密钥添加到应用程序

```
kesl-control [-L] --add-reserve-key <path to key file / activation code>
```

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。

### 如何删除密钥

有多种命令可用于删除密钥。

删除活动密钥

```
kesl-control [-L] --remove-active-key
```

删除备用密钥

```
kesl-control [-L] --remove-reserve-key
```

删除活动 EDR Optimum 密钥

```
kesl-control [-L] --remove-active-key --edr-optimum
```

删除备用 EDR Optimum 密钥

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

删除活动 KUMA 密钥

```
kesl-control [-L] --remove-active-key --kuma
```

删除备用 KUMA 密钥

```
kesl-control [-L] --remove-reserve-key --kuma
```

删除活动 MDR 密钥

```
kesl-control [-L] --remove-active-key --mdr
```

删除备用 MDR 密钥

```
kesl-control [-L] --remove-reserve-key --mdr
```

删除活动 EDR Expert (on-premises) 授权许可密钥

```
kesl-control [-L] --remove-active-key --edr-kata
```

删除备用 EDR Expert (on-premises) 授权许可密钥

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

删除活动 EDR Expert (cloud) 密钥

```
kesl-control [-L] --remove-active-key --cxdr
```

删除备用 EDR Expert (cloud) 密钥

```
kesl-control [-L] --remove-reserve-key --cxdr
```

删除活动 KWSM 密钥

```
kesl-control [-L] --remove-active-key --khcs
```

删除备用 KWSM 密钥

```
kesl-control [-L] --remove-reserve-key --khcs
```

在图形界面中管理密钥

**如何添加活动授权许可密钥**

1. 打开应用程序图形界面的主窗口。
2. 执行下列操作之一：
   - 在主窗口的下部，点击显示授权许可和密钥相关信息的区域。
   - 在主窗口的下部，点击“**支持**”按钮将打开“**支持**”窗口，然后在该窗口中点击“**授权许可密钥**”或窗口下部的“**授权许可**”链接。

   这将打开**授权许可**窗口。
   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. 如果要在商业许可下激活应用程序：
   a. 单击**商业版密钥**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。
      - 如果您想要使用密钥文件添加密钥，请单击**选择密钥文件**链接打开文件选择窗口，在该窗口中选择扩展名为 .key 的文件。

      此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。
4. 如果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。此窗口显示有关试用授权许可及其相关密钥的信息。

**如何添加备用授权许可密钥**

1. 打开应用程序图形界面的主窗口。
2. 执行下列操作之一：
   - 在主窗口的下部，点击显示授权许可和密钥相关信息的区域。
   - 在主窗口的下部，点击“**支持**”按钮将打开“**支持**”窗口，然后在该窗口中点击“**授权许可密钥**”或窗口下部的“**授权许可**”链接。

   这将打开**授权许可**窗口。该窗口将显示有关先前添加的授权许可密钥的信息。
3. 单击**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。
   - 如果您想要使用密钥文件添加密钥，请单击**选择密钥文件**链接打开文件选择窗口，在该窗口中选择扩展名为 .key 的文件。

此窗口显示有关密钥及其相关授权许可的信息。

4. 单击“**添加**”按钮。

**如何删除授权许可密钥**

1. 打开应用程序图形界面的主窗口。
2. 执行下列操作之一：
   - 在主窗口的下部，点击显示授权许可和密钥相关信息的区域。
   - 在主窗口的下部，点击“**支持**”按钮将打开“**支持**”窗口，然后在该窗口中点击“**授权许可密钥**”或窗口下部的“**授权许可**”链接。

   这将打开**授权许可**窗口。该窗口将显示有关先前添加的授权许可密钥的信息。
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。

实用文章

排查应用程序激活问题

# 查看授权许可密钥信息

Kaspersky Security Center 中的授权许可密钥信息

您可以通过以下方式查看有关 Kaspersky Endpoint Security 正在使用的授权许可密钥的信息：

- 在用于激活应用程序的 *添加密钥* 任务的属性中，您可以找到有关此任务添加到应用程序的密钥的信息。
- 在安装在客户端设备上的卡巴斯基应用程序的属性中，您可以找到有关添加到此设备上的应用程序的活动密钥和备用密钥的信息。

  **如何使用 Web Console 查看设备上的授权许可密钥信息**

  1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
     列表仅显示所选管理组的受管理设备。
  3. 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. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。

6. 这将打开应用程序属性窗口；在该窗口中，转到 **常规** 选项卡上的 **授权许可** 部分。
   此部分显示有关添加到应用程序的授权许可密钥以及与这些密钥关联的授权许可的信息。

   - **授权许可密钥状态**是密钥类型：活动密钥或备用密钥。
   - **应用程序名称**是与密钥关联的授权许可的名称以及有关此授权许可的信息。
   - **授权许可密钥**就是授权许可密钥，一个唯一的字母数字序列。
   - **授权许可类型**可以是试用版、商业版或订阅。
   - **激活日期**是添加此密钥的日期。
   - **到期日期**是您使用通过添加此密钥激活的应用程序的权利到期的日期。

**如何使用管理控制台查看设备上的授权许可密钥信息**

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 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。
6. 这将打开一个窗口；在该窗口中，转到**授权许可密钥**部分。
   此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。
   - **状态**：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**：您可以使用通过添加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。

- 授权许可密钥使用报告显示有关使用 Kaspersky Security Center 添加的所有密钥的信息。您可以使用 Web Console（**监控和报告 → 报告**）以及管理控制台（**报告** 选项卡）查看授权许可密钥使用报告。要查看报告，您需要在报告列表中选择“授权许可密钥使用情况报告”模板并开始生成报告。

- Kaspersky Security Center 授权许可密钥存储显示有关添加到 Kaspersky Security Center 管理服务器的所有密钥的信息。您可以使用 Web Console（**操作→卡巴斯基授权许可**）或使用管理控制台（**卡巴斯基授权许可**文件夹）打开密钥存储。

您还可以使用有关 Kaspersky Security Center 事件的通知来获取有关已使用的授权许可密钥及其关联的授权许可的信息。该应用程序将有关过期授权许可和授权许可违规的信息发送到 Kaspersky Security Center 管理服务器。

受保护设备上的授权许可密钥信息

**如何在命令行中查看授权许可密钥信息**

查看设备上的授权许可密钥和授权许可信息

```
kesl-control -L --query [--json]
```

其中 `--json` 表示以 JSON 格式输出数据。如果不指定 `--json` 选项，设置将输出到控制台。

该命令向控制台输出以下信息：

- 有关活动授权许可密钥的信息：
  - 授权许可到期日期和时间。
  - 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（仅对激活 Kaspersky Endpoint Security 应用程序所使用的密钥显示此行）。
  - 有关应用程序数据库更新限制的信息。
  - 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。
- 有关备用授权许可密钥的信息。如果应用程序在标准模式或 EDR Agent 模式下使用，并且已添加备用密钥，则显示此信息。如果应用程序在 Light Agent 模式下使用，则不显示备用密钥信息。
  - 授权许可到期日期和时间。
  - 有关保护功能限制的信息（仅对可用于激活 Kaspersky Endpoint Security 应用程序的密钥显示此行）。
  - 有关应用程序数据库更新限制的信息。
  - 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。

- 备用授权许可密钥（唯一的字母数字序列）。
- 与活动密钥关联的授权许可到期的日期和时间（UTC）。

在查看应用程序详细信息时，您还可以获取有关应用程序所依据的授权许可的信息：

```
kesl-control --app-info
```

**如何在应用程序的图形界面中查看授权许可和密钥信息**

1. 打开应用程序图形界面的主窗口。
2. 执行下列操作之一：
   - 在主窗口的下部，点击显示授权许可和密钥相关信息的区域。
   - 在主窗口的下部，点击“**支持**”按钮将打开“**支持**”窗口，然后在该窗口中点击“**授权许可密钥**”或窗口下部的“**授权许可**”链接。

   这将打开**授权许可**窗口。
   该窗口将显示有关添加到应用程序的活动密钥和备用密钥的信息。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**部分显示有关已添加的活动密钥和相关授权许可的信息：

- 授权许可类型、授权许可限制和授权许可期限。
- **授权许可密钥** — 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，以及授权许可到期日期 (UTC)。
- **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。

**备用密钥**部分显示有关已添加的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。
- **授权许可密钥** — 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。
- **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。

如果您在标准模式或 EDR Agent 模式下使用 Kaspersky Endpoint Security 应用程序，并且使用 Kaspersky Security Center 管理该应用程序，则默认情况下，有关添加和删除授权许可密钥以及授权许可期限到期的信息将记录在操作系统日志中。

# 应用程序的管理界面

要管理 Kaspersky Endpoint Security，您可以使用：

- Kaspersky Security Center
- 命令行
- 应用程序的图形界面

> 您只能使用 Kaspersky Endpoint Security 图形界面执行有限的一部分操作。

如果 Kaspersky Endpoint Security 以用于保护虚拟环境的 Light Agent 模式使用，则无法使用 Kaspersky Security Center 云控制台和应用程序的图形界面管理应用程序。

如果应用程序以 EDR Agent 模式使用，则只有有限的应用程序组件和任务可用。您可以管理某些防护组件、激活应用程序以及更新数据库。请参阅已知问题和限制文章，详细了解 EDR Agent 模式的特殊方面。

请根据组织的 IT 基础架构以及管理员的角色和工作流程选择管理工具。我们建议使用 Kaspersky Security Center 以集中方式远程管理客户端设备上的应用程序。

# 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。

## Kaspersky Security Center 管理组

要使用 Kaspersky Security Center 管理安装在设备上的 Kaspersky Endpoint Security，您需要将这些设备添加到*管理组*中。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。您还可以在安装应用程序后手动将设备移动到管理组（有关详细信息，请参阅 Kaspersky Security Center 帮助）。

## 管理控制台和管理插件

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 Kaspersky Endpoint Security MMC 管理插件（以下也称为“MMC 插件”）提供。

必须在安装了 Kaspersky Security Center 管理控制台的设备上安装 MMC 插件。

- 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。您可以使用任何设备上的浏览器在 Kaspersky Security Center Web Console 中工作。

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

  必须在安装了 Kaspersky Security Center Web Console 的设备上安装 Web 插件。

- 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。

  如果以 Light Agent 模式使用 Kaspersky Endpoint Security，则无法使用 Kaspersky Security Center 云控制台管理应用程序。

Kaspersky Endpoint Security 是 Kaspersky Next Pro View 解决方案的一部分。关于此解决方案中应用程序可用功能的更多信息，请参阅Kaspersky Next 帮助。

### Kaspersky Security Center 策略和任务

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）。

## 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。策略具有以下状态之一：

策略状态

| 状态 | 描述 |
| --- | --- |
| 活动 | 应用于设备的当前策略。 |
| 不活动 | 当前未应用于设备的策略。 |
| 漫游 | 如果选择此选项，当设备离开组织网络时，该策略变为活动状态。 |

策略遵循以下规则：

- 您可以为一个应用程序配置多个具有不同设置的策略。
- 每个应用程序只能有一个活动策略。
- 策略可以有子策略。

锁定设置

每个策略设置都有“挂锁”属性。此属性的状态决定了该设置是否会传递给管理组中的受管理设备。

- 如果“挂锁”已关闭（🔒），则表示该设置会应用于已应用该策略的设备。用户无法在受管理应用程序的用户界面中更改此类设置。此类设置被称为*已锁定*。
- 如果“挂锁”已打开（🔓），则表示策略中未指定该设置。用户可以在受管理应用程序的用户界面中更改此类设置。此类设置被称为*已解锁*。

建议您锁定要应用于受管理设备的策略设置。已解锁的策略设置可以在受管理设备上被覆盖。

Web Console 和管理控制台中带有“挂锁”的设置数量可能不同。

策略配置文件

例如，如果只有少数设置应可更改，您可以使用策略配置文件，以避免必须支持大量策略。

*策略配置文件*是一组与“基本”策略设置不同的单独策略设置，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应用程序设置。

使用“挂锁”锁定的配置文件设置将覆盖策略设置。也就是说，如果用“挂锁”锁定的配置文件设置与策略设置不同，则应用程序将应用配置配置文件中的设置。但是，设置列表会合并，互相补充。也就是说，如果配置文件列表中的设置在“基本”策略中缺失，则这些设置将被添加到结果设置列表中。

策略配置文件遵循以下规则：

- 策略配置文件会在满足特定激活条件时生效。
- 策略配置文件包含与策略中设置的值不同的设置值。
- 激活策略配置文件会更改受管理设备的有效设置（当前应用于设备的设置）。
- 一个策略最多可以有 100 个配置文件。

设置继承

策略具有层次结构，类似于管理组。*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。

默认情况下，子策略会继承父策略的设置。如果父策略中的设置已锁定（🔒），则子策略和应用程序的本地设置会获得相同的值，并且该设置会被锁定。如果必要，您可以禁用从父策略继承设置。漫游策略不通过管理组的层次结构影响其他策略。

如果子策略的设置被锁定（*访问被拒绝* 错误），请检查用户的访问权限。如果用户有权编辑策略设置，请启动 Kaspersky Security Center 的 *将更新下载至管理服务器存储库* 任务并重复授权。在 Kaspersky Security Center 中升级管理插件后可能会出现此错误：下载更新后，应用程序会获取新版管理插件所需的文件。

对于某些以列表作为值的设置（例如规则列表、排除列表），您可以启用列表项合并。要合并列表项，您需要执行以下操作：

- 在子策略属性的 **常规** 选项卡上，启用 **从父策略继承设置** 设置。
- 在父策略的属性中，点击挂锁（🔒）图标将其“锁定”。
- 在父策略的属性中，通过选中**合并继承的值**复选框来启用设置合并。如果选中该复选框，则 Kaspersky Security Center 的父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。如果清除该复选框，则继承策略设置时不会合并列表项。

您不能删除或修改子策略中继承的列表项。继承时已被合并的列表项只能在父策略中删除或修改。可以在较低级别添加、修改或删除列表项。因此，您可以在父策略中配置列表，该列表将应用于所有子策略，并且您还可以在子策略中向列表添加更多项。

如果从父策略中通过继承合并的列表中删除某个项目，则不会从子策略中删除该项目。要从子策略中删除此项目，您必须打开这些策略的属性并手动删除该项目。

有些列表未合并。如果发生这种情况，配置文件中的设置将覆盖“基本”策略的设置：

- 文件威胁防护和行为检测组件中的进程排除项
- 文件威胁防护和反加密勒索组件中的保护范围
- 系统完整性监控组件中的监控范围
- 应用程序控制组件中的规则列表（在**应用程序控制规则**窗口中）
- Web 控制中的规则列表
- 应用程序设置中的进程内存排除项
- 网络设置中的受信任域
- 网络设置中的受信任根证书

- 网络设置中的监控端口
- SVM 检测设置中的 SVM 地址列表

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以及设置继承机制的更多信息，请参阅 Kaspersky Security Center 帮助。

# 策略管理

**如何在 Web Console 中创建策略**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
   将打开策略和策略配置文件的列表。
2. 选择要应用该策略的管理组。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
3. 单击“**添加**”。
   “策略向导”将启动。
4. 在显示的窗口中，从列表中选择 Kaspersky Endpoint Security。
   继续执行向导的下一步。
5. 指定 Kaspersky Endpoint Security 使用模式：
   - 在 **标准模式或 Endpoint Detection and Response Agent 模式** 下，该应用程序作为独立应用程序使用，或作为支持卡巴斯基 Detection and Response 解决方案与第三方反病毒解决方案协同工作的应用程序，用于保护 Linux 设备。
     要选择此模式，请转到向导的下一步。
   - **用于保护虚拟环境的 Light Agent** – 作为卡巴斯基 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 客户机操作系统的虚拟机。
6. 如果您在 Light Agent 模式下使用该应用程序，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 SVM 地址的自定义列表** 选项，Light Agent 使用扩展 SVM 选择算法，并且在某个 SVM 上启用了大型基础架构保护模式，则只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到此 SVM。在 **SVM 选择算法** 区域中，您需要将 **SVM 路径** 设置设为 **忽略**。如果设置任何其他值，Light Agent 都无法连接到 SVM。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

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：

- "**地址**"。安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。如果将地址指定为 NetBIOS 名称、localhost 或 127.0.0.1，则与 Integration Server 的连接将以错误完成。
- "**端口**"。用于连接到 Integration Server 的端口。默认情况下，指定端口为 7271。

如果您的基础架构中部署了基于 Linux 的高可用性 Integration Server 集群，则需要将负载均衡器的地址和端口指定为连接到 Integration Server 的地址和端口。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

b. 单击"**检查**"。

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，则会在 **Integration Server 连接错误** 窗口中显示相应的消息。

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，请创建由此策略管理的 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)。您可以使用换行输入来隔开多个 IP 地址或 SVM 的完全限定域名。

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：

- 如果您同意本声明的所有条款和条件，并希望将卡巴斯基安全网络与该应用程序一起使用，请选择 **我同意使用卡巴斯基安全网络**。
- 如果您不想使用卡巴斯基安全网络，请选择 **我不同意使用卡巴斯基安全网络**，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. 系统将提示您阅读有关配置 Kaspersky Endpoint Security 的建议。检查允许应用程序优化系统资源使用的设置。

   继续执行向导的下一步。

9. 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。默认情况下已选定该选项。
     - **不活动**。如果选择此选项，则策略不会被应用于设备，但仍保留在**策略**文件夹中。您可以稍后激活非活动策略。
     - **漫游**。如果选择此选项，当设备离开组织网络时，该策略变为活动状态。

       在设备上处于活动状态的网络代理策略的**网络** → **连接配置文件**部分中，必须启用**管理服务器不可用时启用漫游模式**设置。

   - 策略设置继承：
     - “**从父策略继承**”。如果启用此拨动开关，策略设置将从上级组策略继承。父策略中被用“挂锁”（🔒）锁定的设置不可编辑。默认情况下，拨动开关处于打开状态。
     - “**子策略的强制继承**”。如果启用此切换开关，策略设置将传播到子策略。在子策略的属性中，“**从父策略继承**”切换按钮将自动打开，且无法关闭。子策略的设置将从父策略继承，但带有打开“挂锁”（🔓）图标的设置除外。默认情况下，切换按钮处于关闭状态。

   有关策略设置的一般信息，请参阅 Kaspersky Security Center 帮助。

10. 如果您想管理其他策略设置，请转到 **应用程序设置** 选项卡并根据需要进行更改。

    您也可以稍后更改策略设置。

11. 单击“**保存**”按钮。

**如何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，在列表中选择 Kaspersky Endpoint Security。

   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：

   - 在**标准模式或 Endpoint Detection and Response Agent 模式下**，应用程序作为独立应用程序或支持与 Kaspersky Detection and Response 解决方案和第三方反病毒解决方案协同工作的应用程序以保护 Linux 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，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 SVM 地址的自定义列表** 选项，Light Agent 使用扩展 SVM 选择算法，并且在某个 SVM 上启用了大型基础架构保护模式，则只有在忽略 SVM 路径的情况下，才能将 Light Agent 连接到此 SVM。在 **SVM 选择算法** 区域中，您需要将 **SVM 路径** 设置设为 **忽略**。如果设置任何其他值，Light Agent 都无法连接到 SVM。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

   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：

         - **地址**。安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。如果将地址指定为 NetBIOS 名称、localhost 或 127.0.0.1，则与 Integration Server 的连接将以错误完成。
         - **端口**。用于连接到 Integration Server 的端口。默认情况下，指定端口为 7271。

如果您的基础架构中部署了基于 Linux 的高可用性 Integration Server 集群，则需要将负载均衡器的地址和端口指定为连接到 Integration Server 的地址和端口。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

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，请创建由此策略管理的 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)。您可以使用换行输入来隔开多个 IP 地址或 SVM 的完全限定域名。

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. 选择策略状态：

- **活动策略**。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。默认情况下已选定该选项。
- **非活动策略**。如果选择此选项，则策略不会被应用于设备，但仍保留在**策略**文件夹中。您可以稍后激活非活动策略。

- **漫游策略**。如果选择此选项，当设备离开组织网络时，该策略变为活动状态。

  在设备上处于活动状态的网络代理策略的**网络 → 连接配置文件**部分中，必须启用**管理服务器不可用时启用漫游模式**设置。

15. 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。

有关管理策略的一般信息，请参阅 Kaspersky Security Center 帮助。

实用文章

任务未运行或策略未应用时该怎么办

设备状态为“无效的策略设置。策略尚未应用”时该怎么办

错误：“当前版本的 Kaspersky Security Center Web Console 不支持该应用程序，或者未安装应用程序 Web 插件”

# 导出和导入策略设置

Kaspersky Endpoint Security 允许将策略及其设置和配置文件导出到 KLP 文件。然后，您可以使用策略导出/导入功能来备份策略、将策略迁移到另一台服务器，或者，例如，将策略从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux。有关管理策略的详细信息，请参阅 Kaspersky Security Center 帮助。

**如何在管理控制台 (MMC) 中导出和导入策略**

1. 打开 Kaspersky Security Center 管理控制台。
2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择“**策略**”选项卡。
4. 要导出策略：
   a. 单击要导出的策略。
   b. 单击窗口右侧的“**导出策略到文件**”链接。
   c. 在打开的窗口中，指定您要将策略导出到的 KLP 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
5. 要导入策略：
   a. 单击“**从文件导入策略**”。
   b. 在打开的窗口中，选择您要导入的 KLP 策略文件。
   c. 打开文件。

这增加了一个具有“*非活动策略*”状态的新策略。

**如何在 Web Console 中导出和导入策略**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 要导出策略：
   a. 选中要导出的策略旁边的复选框。
   b. 单击“**导出**”按钮。
   c. 在打开的窗口中，指定您要将策略导出到的 KLP 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
3. 要导入策略：
   a. 单击“**导入**”。
   b. 选择要导入的 KLP 策略文件。
   c. 策略成功处理后，选择要应用该策略的管理组。
   d. 单击“**完成**”按钮完成导入策略。

   这增加了一个具有“*不活动*”状态的新策略。

在 Web Console 中导出和导入特定策略设置

在 Web Console 中，您可以将各个策略设置导出到 JSON 文件，并从文件导入此类设置。例如，您可以导出 Web 控制规则列表或文件威胁防护的保护范围列表。

以下设置可用于导出和导入：

- 文件威胁防护的保护范围
- 邮件威胁防护的附件过滤器
- 网络数据包规则
- Web 控制规则
- 应用程序控制规则
- 系统完整性监控的监控范围和排除范围
- 遥测设置
- 特定“信任区域”排除

*要在 Web Console 中导出或导入设置：*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到要从中导出或导入设置的区域。
5. 单击 按钮。
6. 选择操作：**导入** 或 **导出**。
7. 如果要导入设置，请选择要从中导入设置的文件。

# 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；
- 设备选择任务，用于在多台设备上运行，而不论这些设备是否属于管理组。

您可以创建任意数量的任务。

有关在 Kaspersky Security Center 中创建的任务的一般信息，请参阅 Kaspersky Security Center 帮助。

## 任务类型

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，并管理黄金镜像。
- *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。

在 Web Console 中管理任务

### 如何在 Web Console 中为设备组或设备选择创建任务

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

2. 单击“**添加**”按钮。
   “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，选择应用程序名称：Kaspersky Endpoint Security。

   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. 要在创建任务后立即管理任务设置，请在向导的最后一步选中 **创建完成后打开任务详细信息** 复选框。使用默认设置创建任务。

6. 结束向导。

在任务列表中将显示一个新任务。

### 如何在 Web Console 中创建本地任务

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的 **显示层次结构** 按钮，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，找到要为其创建任务的设备，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“**任务**”选项卡。

   为此设备创建的任务列表将显示。

5. 单击“**添加**”按钮。

   “任务向导”将启动。

6. 在向导的第一步，执行以下操作：

   a. 在“**应用程序**”下拉列表中，选择应用程序名称：Kaspersky Endpoint Security。

   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。

7. 要在创建任务后立即管理任务设置，请在向导的最后一步选中 **创建完成后打开任务详细信息** 复选框。使用默认设置创建任务。

8. 结束向导。

在任务列表中将显示一个新任务。

### 如何在 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**”。

   任务列表打开。

2. 执行下列操作之一：

   - 要启动或停止在特定管理组所包含的所有设备上运行的任务，请单击窗口上部的 **显示层次结构** 按钮，然后在显示的窗口中选择该管理组。

     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），请单击窗口上部的 **显示层次结构** 按钮，然后在显示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。

> “*更新*”任务无法暂停或继续，只能启动或停止。

在管理控制台中管理任务

**要在管理控制台中为设备组或设备选择创建任务**

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 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）。

   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. 结束向导。

   在任务列表中将显示一个新任务。

**如何在管理控制台中创建本地任务**

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“**任务**”部分。
   为此设备创建的任务列表将显示。

5. 单击“**添加**”按钮。
   “任务向导”将启动。

6. 在向导的第一步中，选择 Kaspersky Endpoint Security 和任务类型。
   继续执行向导的下一步。

7. 输入新任务的名称并按照向导的说明配置可用的任务设置。

8. 结束向导。
   在任务列表中将显示一个新任务。

**如何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。

> “*更新*”任务无法暂停或继续，只能启动或停止。

在任务列表中，您可以监控任务执行结果：查看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的执行情况。有关事件选择的更多详细信息，请参阅 Kaspersky Security Center 帮助。

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

管理和运行任务时的特殊注意事项

- 设备集的任务仅在该任务中指定的设备上执行。如果向已创建任务的设备集添加新设备，则不会对这些设备执行该任务。在这种情况下，您需要创建新任务或编辑现有任务。

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

- 如果设备受策略管理，则可能无法使用命令行或应用程序的图形界面来查看和管理在 Kaspersky Security Center 中创建的任务。

- 对于 Kaspersky Security Center 中的 Kaspersky Endpoint Security 应用程序，您可以创建所有类型的任务。在受保护设备上应用和运行任务取决于设备上的 应用程序模式。例如，如果应用程序以 Light Agent 模式运行，则 *添加密钥*、*更新* 和 *回滚* 任务不会应用到设备上。

# 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。

您可以使用以下方法之一登录 Kaspersky Security Center Web Console：

- 域身份验证（单点登录）
- 域用户的用户名和密码
- 内部用户的用户名和密码

有关登录和退出 Kaspersky Security Center Web Console 的更多详细信息，请参阅 Kaspersky Security Center 帮助。

*要通过指定用户名和密码登录 Web Console：*

1. 在浏览器中，转到：

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   这将打开用于选择管理服务器的页面。

2. 如果您添加了多个受信任的管理服务器，请从列表中选择要连接的管理服务器。
   如果您只添加了一个管理服务器，则不会显示管理服务器列表。
   浏览器将重定向到 `https://<Administration Server address>:4444`。

3. 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。

4. 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。

5. 输入移动设备上的身份验证应用中生成的一次性安全代码。
   如果是首次登录，请为您的账户配置两步身份验证。

登录后，将以上次使用的语言和主题显示控制板。

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

*要登出 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 云控制台，请在云控制台门户上使用 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。

# 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，并在本地管理应用程序。

组件和任务

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。要在设备上启用或禁用应用程序的功能组件，您需要在命令行中启动或停止相应的 Kaspersky Endpoint Security 任务。

要对设备执行一次扫描，您还需要启动相应的 Kaspersky Endpoint Security 任务。

要管理设备上功能组件的设置或设备扫描设置，您需要管理相应 Kaspersky Endpoint Security 任务的设置。

常规设置

除各个 Kaspersky Endpoint Security 任务的特定设置外，还有一些常规设置：

- 常规容器扫描设置。用于实时扫描容器和命名空间（容器监控）。
- 网络流量扫描设置。由 Web 威胁防护、网络威胁防护、邮件威胁防护 和 Web 控制 组件使用。
- 常规应用程序设置。这些设置控制应用程序的整体运行以及各个功能的运行。

管理命令

您可以在命令行中使用 *kesl-control 实用程序* 管理 Kaspersky Endpoint Security 任务和设置。

只能创建或删除用户任务。无法创建或删除预定义任务。

根据应用程序模式，可以创建以下类型的用户任务：

- 标准模式：*ODS*、*更新*、*回滚*、*ODFIM*，*ContainerScan* 和 *InventoryScan*；
- Light Agent 模式：*ODS*、*ODFIM*、*ContainerScan* 和 *InventoryScan*。

您可以启动和停止所有预定义任务和用户任务，但 *License* 类型的任务除外。

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

## Kaspersky Endpoint Security 本地任务

下表列出了可用于通过命令行管理 Kaspersky Endpoint Security 的任务：

每个应用程序任务都有一个在命令行中使用的名称、一个 ID 和一个类型。

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 | 任务描述 | 命令行中的任务名称 | 任务 ID | 任务类型 |
|---|---|---|---|---|
| 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。如果启用文件威胁防护，该任务将在应用程序启动时自动运行 | File_Threat_Protection | 1 | OAS |
| 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。 | 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 | 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所用的设置。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。 | Scan_File | 3 | ODS |
| 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。 | Critical_Areas_Scan | 4 | ODS |
| 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。 | Update | 6 | Update |
| 更新（用户任务） | | 用户自定义 | 从 100 开始 | Update |
| 回滚 | 您可以使用此任务回滚应用程序数据库和模块的上一次更新。 | Rollback | 7 | Rollback |
| 回滚（用户任务） | | 用户自定义 | 从 100 开始 | Rollback |
| 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。 | License | 9 | License |
| 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。 | System_Integrity_Monitoring | 11 | OAFIM |
| 系统完整性检查（用户任务） | | 用户自定义 | 从 100 开始 | ODFIM |

| 任务 | 任务描述 | 命令行中的任务名称 | 任务 ID | 任务类型 |
| --- | --- | --- | --- | --- |
| 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。 | Firewall_Management | 12 | Firewall |
| 反加密 | 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。 | Anti_Cryptor | 13 | AntiCryptor |
| 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。如果启用 Web 威胁防护，该任务将在应用程序启动时自动运行 | Web_Threat_Protection | 14 | WTP |
| 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。如果启用设备控制，该任务将在应用程序启动时自动运行。 | Device_Control | 15 | DeviceControl |
| 可移动驱动器扫描 | 此任务允许您实时监控可移动介质与设备的连接，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。 | Removable_Drives_Scan | 16 | RDS |
| 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。 | Network_Threat_Protection | 17 | NTP |
| 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。 | 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 | 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所用的设置。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。 | Custom_Container_Scan | 19 | ContainerScan |
| 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。如果启用行为检测，该任务将在应用程序启动时自动运行。 | Behavior_Detection | 20 | BehaviorDetection |
| 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。 | Application_Control | 21 | AppControl |
| 清查 | 此任务允许获取设备上应用程序的所有可执行文件的信息，并管理应用程序的"黄金镜像"类别。 | 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 Expert (on-premises) 集成。 | 此任务允许启用或禁用与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 的集成，并管理集成设置。 | KATAEDR | 24 | KATAEDR |
| 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。 | Web_Control | 26 | WebControl |
| Sandbox 集成 | 此任务可启用和禁用与 Sandbox 的集成并指定集成设置。 | Standalone_Sandbox | 29 | StandaloneSandbox |
| 对象的执行防护 (EDR Expert (on-premises)) | 此任务允许您启用或禁用 Endpoint Detection and Response Expert (on-premises) 执行防护规则的使用，并查看这些规则的列表。 | KATAEDR_Prevention | 30 | KATAEDRPrevention |
| Kaspersky Network Detection and Response (KATA) 整合 | 此任务允许您启用或禁用与 Kaspersky Network Detection and Response (KATA) 的集成，并指定集成设置。 | KATANDR | 31 | KATANDR |

| 任务 | 任务描述 | 命令行中的任务名称 | 任务 ID | 任务类型 |
| --- | --- | --- | --- | --- |
| 对象的执行防护 (EDR Optimum) | 此任务可让您启用和禁用 Endpoint Detection and Response Optimum 执行防护规则的使用，还可以查看这些规则的列表。 | EDRO_Prevention | 32 | Prevention |
| KUMA 整合 | 此任务可启用和禁用与Kaspersky Unified Monitoring and Analysis Platform的整合并指定整合设置。 | KUMA | 33 | KUMA |
| 邮件威胁防护 | 此任务允许您扫描传入和传出电子邮件的附件，以查找病毒和其他威胁性应用程序。如果启用邮件威胁防护，该任务将在应用程序启动时自动运行 | Mail_Monitoring | 35 | MailMonitoring |
| BadUSB 攻击防护 | 此任务允许您阻止将伪装成键盘的受感染 USB 设备连接到客户端设备。 | Bad_USB | 37 | BadUSB |
| Kaspersky Endpoint Detection and Response Expert (cloud) 集成 | 此任务允许您启用或禁用与 Kaspersky Endpoint Detection and Response Expert (cloud) 的集成，并指定集成设置。 | EDRExpertCloud | 39 | EDRExpertCloud |

# 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的设置，但 *回滚* 和 *授权许可* 类型的任务除外（这些任务没有设置）。如果在 Light Agent 模式下使用应用程序，则也无法编辑预定义的 *更新* 任务的设置。

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。

您可以通过以下方式编辑任务设置：

- 使用配置文件。此方法允许同时修改所有任务设置。您可以使用用于输出任务设置的命令获取要编辑的配置文件。
- 使用 <setting name>=<setting value> 格式的命令行选项。此方法允许更改单个任务设置。您可以使用用于输出任务设置的命令查看任务设置的当前值。

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。

### 如何输出任务设置的当前值

您可以将任务设置的当前值输出到控制台或配置文件。然后，您可以编辑此文件以修改任务设置。

将任务设置的当前值输出到控制台

```
kesl-control --get-settings <task ID|name>
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

将任务设置的当前值输出到配置文件

```
kesl-control --get-settings <task ID/name> --file <path to configuration file> [--json]
```

其中：

- `--file <path to configuration file>` 是要将任务设置输出到的配置文件的路径。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`选项，则设置以 INI 格式输出。

**如何使用配置文件修改任务设置：**

1. 使用以下命令将任务设置输出到配置文件：

   ```
   kesl-control --get-settings --file <path to configuration file> [--json]
   ```

   其中：

   - `--file <path to configuration file>` 是配置文件的完整路径，您希望从该配置文件导入任务设置。
   - 如果要将设置输出到 JSON 配置文件，请指定 `--json` 选项。如果未指定 `--json` 选项，应用程序会将设置输出到 INI 文件。

2. 打开生成的配置文件，根据需要编辑设置，然后保存更改。

   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，请向文件中添加包含以下设置的 `[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` 是包含要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` 是包含要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. 运行以下命令：

```
kesl-control --set-settings <task ID/name> --file <path to configuration file> [--json]
```

其中：

- <task ID/name> 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- --file <path to configuration file> 是配置文件的完整路径，您希望从该配置文件导入任务设置。
- 如果要从 JSON配置文件导入设置，请指定 --json 选项。如果不指定 --json选项，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 --set-settings 选项的 --accept 命令。

**如何使用命令行选项更改单个任务设置**

请执行命令：

```
kesl-control --set-settings <task ID|name> <setting name >=<setting value> [<setting name >=<setting value>]
```

其中：

- <task ID|name> 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- <setting name >=<setting value> 是某个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 --set-settings 选项的 --accept 命令。

**如何使用命令行选项添加或删除扫描范围**

使用命令行选项添加扫描范围

```
kesl-control --set-settings <task ID|name> --add-path <path>
```

其中：

- <task ID|name> 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- <path> 是包含要扫描对象的目录的路径。

此命令会向任务设置添加新的 [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。

将 /home 目录添加到 ID=100 的任务扫描范围的示例

```
kesl-control --set-settings 100 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.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=*
```

使用命令行选项删除扫描范围

```
kesl-control --set-settings <task ID|name> --del-path <path>
```

此命令会从任务设置中删除包含指定路径的 [ScanScope.item_#] 部分。应用程序将不会扫描指定目录中的对象。

**如何使用命令行选项添加或删除排除范围**

使用命令行选项添加排除范围

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

其中：

- <task ID|name> 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- <path> 是包含要排除对象的目录的路径。

此命令会向任务设置添加新的 [ExcludedFromScanScope.item_#] 部分。应用程序会从扫描中排除 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。

使用命令行选项删除排除范围

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

此命令会从任务设置中删除包含指定路径的 [ExcludedFromScanScope.item_#] 部分。应用程序不会从扫描中排除指定目录中的对象。

**如何恢复默认任务设置**

请执行命令：

```
kesl-control --set-settings <task ID|name> --set-to-default
```

其中，`<task ID|name>` 是任务创建时分配给任务的 ID，或者是命令行上的任务名称。

应用程序将设置值改为默认值。

# 配置任务计划

根据应用程序的模式，您可以为以下类型的任务配置计划：

- 标准模式：*ODS*、*更新*、*回滚*、*ODFIM*，*ContainerScan* 和 *InventoryScan*；
- Light Agent 模式：*ODS*、*ODFIM*、*ContainerScan* 和 *InventoryScan*。

您可以通过以下方式编辑任务计划：

- 使用配置文件。此方法允许同时修改所有任务计划设置。您可以使用输出计划设置的命令获取要编辑的配置文件。
- 使用 <setting name>=<setting value> 格式的命令行选项。此方法允许修改单个任务计划设置。您可以使用输出计划设置的命令查看任务设置的当前值。

### 如何输出当前计划设置

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。随后，您可以编辑此文件以修改设置。

将当前任务计划设置输出到控制台

```
kesl-control --get-schedule <task ID|name> [--json]
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- 指定 `--json`，则以 JSON 格式输出设置。如果 --json 选项被省略，则设置以 INI 格式输出。

将当前任务计划设置输出到配置文件

```
kesl-control --get-schedule <task ID|name> --file <path to configuration file> [--json]
```

其中 `--file <path to configuration file>` 是要将任务计划设置输出到其中的配置文件的路径。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。

将更新任务计划设置输出到名为 `update_schedule.ini` 的文件并将创建的文件保存到当前目录的示例

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

将更新任务计划写入终端的示例

```
kesl-control --get-schedule 6
```

### 如何使用配置文件配置任务计划

```
kesl-control --set-schedule <task ID|name> --file <path to configuration file> [--json]
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `--file <path to configuration file>` 是配置文件的完整路径，您希望从该配置文件导入任务计划设置。
- 如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果不指定 `--json`选项，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。

从配置文件 `/home/test/on_demand_schedule.ini` 将计划设置导入 `ID=2` 的任务的示例

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

### 如何使用命令行选项修改任务计划设置：

```
kesl-control --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `<setting name>=<setting value>` 是某个 任务计划设置 的名称和值。

配置任务每 `10` 小时运行一次的示例

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

配置任务每 `10` 分钟运行一次的示例

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

配置任务在每月 `15` 日运行的示例

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

配置任务每周二运行的示例

```
RuleType=Weekly
StartTime=18:01:30;Tue
RandomInterval=99
RunMissedStartRules=No
```

配置任务每 `11` 天运行一次的示例

```
RuleType=Daily
RunMissedStartRules=No
```

```
StartTime=23:15:00;11
RandomInterval=0
```

# 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。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的使用和反恶意软件数据库精简版。
- 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）。
- 配置进程内存扫描的排除项。
- 启用或禁用实时容器监控。
- 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。
- 启用或禁用与 Kaspersky Managed Detection and Response 的整合。
- 配置事件日志的使用。
- 配置扫描任务（ODS 类型）的 CPU 资源使用限制。
- 限制非特权用户可以同时启动的用户扫描任务的数量。

您可以通过以下方式使用特殊管理命令来管理常规应用程序设置：

- 使用配置文件。此方法允许同时更改所有常规应用程序设置。您可以使用常规应用程序设置输出命令获取要编辑的配置文件。
- 使用 <setting name>=<setting value> 格式的命令行选项。此方法允许更改单个设置。您可以使用常规应用程序设置输出命令获取各设置的当前值。

### 如何输出常规应用程序设置的当前值

您可以将常规应用程序设置的当前值输出到控制台或配置文件。然后，您可以使用此文件来编辑设置。

将应用程序常规设置的当前值输出到控制台

```
kesl-control --get-app-settings [--json]
```

其中指定 `--json` 后，将以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

将应用程序常规设置的当前值输出到配置文件

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

其中 `--file <path to configuration file>` 是要将应用程序常规设置输出到的配置文件的路径。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。

将常规应用程序设置写入当前目录中的 kesl_config.ini 文件的示例

```
kesl-control --get-app-settings --file kesl_config.ini
```

**如何使用配置文件编辑任务设置：**

1. 使用 `kesl-control --get-app-settings` 命令将常规应用程序设置输出到配置文件。
2. 打开生成的配置文件，根据需要编辑设置，然后保存更改。
3. 运行以下命令：

   ```
   kesl-control --set-app-settings --file <path to configuration file> [--json]
   ```

   其中：

   - `--file <path to configuration file>` 是包含常规应用程序设置的配置文件的完整路径。如果删除配置文件中的任何参数，则执行命令后将显示该参数的默认值。
   - 如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果不指定 `--json`选项，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。

从 /home/test/kesl_config.ini 配置文件将常规设置导入应用程序的示例

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

**如何使用命令行选项更改常规设置**

使用命令行选项更改常规设置

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name >=<setting value>]
```

其中 `<setting name>=<setting value>` 是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。

设置跟踪文件的低详细程度的示例

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

添加挂载点排除以避免文件操作拦截的示例

```
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：

您可以将过滤器用于以下目的：

显示有关应用程序某些当前事件的信息

```
kesl-control -W --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

在事件日志中显示有关某些应用程序事件的信息

```
kesl-control -E --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

显示备份区中某些对象的信息

```
kesl-control -B --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

从备份区中删除某些对象

```
kesl-control -B --mass-remove --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

其中：

- `<field>` 是数据库字段的名称。
- `<comparison operator>` 是以下比较运算之一：
  - `>` 表示“大于”
  - `<` 表示“小于”
  - `like` 与指定值匹配。指定值时，可以使用 % 掩码：例如，逻辑表达式 `"FileName like '%etc%'"` 设置了“FileName 字段中包含文本 ‘etc’”这一限制条件

    > `like`比较操作仅适用于数据库中存储为文本类型的字段。`like`操作不适用于包含日期、时间、数字或其他非文本数据类型的字段。

  - `==` 表示“等于”
  - `!=`表示“不等于”
  - `>=` 表示“大于或等于”
  - `<=` 表示“小于或等于”

- <value> 是字段的值。该值必须用单引号 (') 括起来。

  您可以将日期值指定为 UNIX™ 时间（自 1970 年 1 月 1 日 00:00:00 (UTC) 起经过的秒数），或者采用 YYYY-MM-DD hh:mm:ss 的格式。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。

FileName 字段中包含文本“etc”的事件信息的输出示例

```
kesl-control -E --query "FileName like '%etc%'"
```

ThreatDetected 类型的事件信息的输出示例

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

由 ODS 类型的任务创建的 ThreatDetected 类型事件信息的输出示例

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

在 UNIX 时间戳系统中指定的日期之后生成的事件信息的输出示例（自 1970 年 1 月 1 日 00:00:00 (UTC) 起经过的秒数）

```
kesl-control -E --query "Date > '1583425000'"
```

以 YYYY-MM-DD hh:mm:ss 格式指定的日期之后生成的事件信息的输出示例

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

备份区中严重级别为“高”的文件信息的输出示例

```
kesl-control -B --query "DangerLevel == 'High'"
```

# 导出和导入应用程序设置

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。

仅允许受信任的用户访问配置文件。在将设置导入应用程序之前，请验证目录、配置文件、可执行文件和隔离区的路径。请勿从不受信任的来源导入配置文件。配置文件遭到破坏可能会影响组织基础设施的安全性、完整性或功能，还可能影响用户数据。

## 导出设置

导出设置时，所有应用程序设置（包括常规“容器扫描”设置、网络流量扫描设置、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随后将设置导入应用程序。

导出应用程序设置

```
kesl-control --export-settings --file <configuration file path> [--json]
```

其中：

- `--file <configuration file path>` 是要将应用程序设置保存到其中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` 选项，设置将导出到 INI 文件。

导入设置

1. 运行以下命令：

   ```
   kesl-control --import-settings --file <configuration file path> [--json]
   ```

   其中：

   - `--file <configuration file path>` 是要从中导入应用程序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`选项，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。

2. 重启应用程序。

导出和导入设置时的特殊注意事项和限制

- 在导入或导出设置时，必须启动应用程序。
- 如果 Kaspersky Endpoint Security 在 Light Agent 模式下使用，则无法导出或导入 `Update` 类型的预定义任务的设置。
- 如果策略禁止更改设置，则无法导入设置。
- 如果将从旧版本应用程序导出的设置导入到较新版本中，则旧版本中不存在的设置将设置为默认值。
- 无法将设置从较新版本导入到较旧版本。
- 某些策略和任务设置无法从应用程序 Web 插件版本 12.3 和 12.4 导入到应用程序版本 12.5 中。此限制适用于以下策略和任务设置：
  - 文件威胁防护和反加密勒索的保护范围和排除范围
  - 行为分析扫描的进程排除项
  - 设备控制的受信任设备
  - 系统完整性监控的扫描范围和排除范围
  - Web 控制规则
  - 代理服务器设置

- 进程内存扫描排除项
- 全局排除项（从扫描中排除的挂载点）
- *ODS*，*ContainerScan*、*InventoryScan*、*ODFIM* 任务的扫描范围。

- 导入设置后，将关闭以下功能：卡巴斯基安全网络（`UseKSN=No`）、云模式（`CloudMode=No`）和 MDR 集成（`UseMDR=No`）。如果要使用此功能，请管理相关设置。
- 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。
- 与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成时，将导出所有设置，包括从 Kaspersky Endpoint Detection and Response Expert (cloud) 接收的设置：
  - 遥测服务器的地址和端口
  - 响应服务器的地址和端口
  - 响应服务器的连接超时
  - 响应服务器的响应超时
  - 遥测服务器的连接超时
  - 遥测服务器的响应超时
  - 遥测服务器的客户端证书
  - 遥测服务器的服务器证书
  - 响应服务器的客户端证书
  - 响应服务器的服务器证书

  导入时，上述设置不会导入到设备。

# 通过图形界面管理应用程序

通过图形界面管理应用程序需要 管理员 (admin) 角色的权限。

如果 Kaspersky Endpoint Security 以 Light Agent 模式运行，则不支持图形界面。

在应用程序的 **标准模式**下，您可以使用图形界面执行以下操作：

- 查看有关设备保护状态的信息。
- 配置应用程序组件。

**选择树**

- 文件威胁防护。
- 防火墙管理。
- 反加密勒索。
- 可移动驱动器扫描。
- Web 威胁防护。
- 邮件威胁防护。
- 设备控制。
- 网络威胁防护。
- BadUSB 攻击防护。
- 行为检测。
- 漏洞利用防御。
- 应用程序控制。
- Web 控制。
- 系统完整性监控。

- 扫描文件和目录，包括将文件发送到沙盒进行扫描。
- 启动更新并回滚数据库更新。
- 为应用程序启用或禁用卡巴斯基安全网络。
- 向组织本地网络的管理员请求并获取对被阻止设备的临时访问权限。
- 管理应用程序授权许可密钥并查看有关当前使用的授权许可和密钥的信息。
- 查看有关放置在备份中的对象的信息。
- 查看应用程序报告。
- 创建应用程序跟踪文件。

通知区域中的应用程序图标

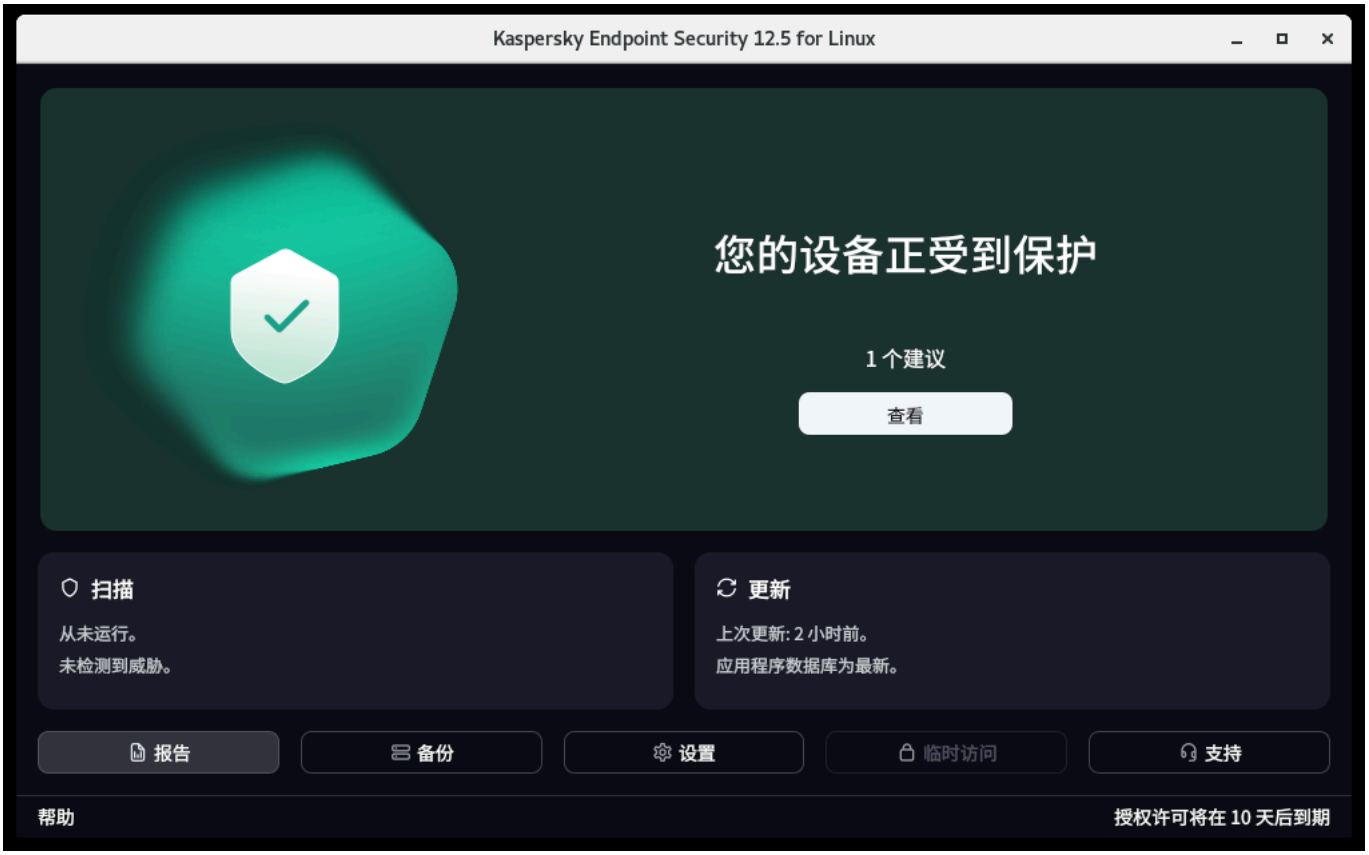
使用托盘中的 Kaspersky Endpoint Security 图标可以访问上下文菜单和应用程序图形界面的主窗口。

在某些操作系统中，安装应用程序图形界面软件包后，可能会丢失默认的应用程序图标。

应用程序图标的上下文菜单包含下列项：

- **Kaspersky Endpoint Security 12.5 for Linux**。打开应用程序图形界面的主窗口。
- **退出**。退出图形界面。

## 应用程序图形界面的主窗口




主应用程序窗口

| | |
|---|---|
| **保护状态** | 有关设备保护状态的信息。显示在主窗口的上半部分。<br>您可以点击 **查看** 按钮打开 **保护中心** 窗口。此窗口显示为修复保护问题（如有）而需执行的操作建议。 |
| **扫描** | 有关恶意软件扫描任务状态和检测到的威胁数量的信息。<br>您可以点击此部分打开 **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，并查看这些任务的报告。 |
| **更新** | 有关数据库更新任务状态的信息。<br>您可以点击此部分打开 **更新** 窗口。在此窗口中，您可以启动 *更新* 和 *回滚* 任务，并查看这些任务的报告。 |
| **报告** | 查看组件和任务的 报告 和统计信息。 |
| **备份** | 查看 备份区 中的对象详细信息。<br>如果按钮处于非活动状态该怎么办 |
| **设置** | 启用或禁用应用程序组件，配置 卡巴斯基安全网络。<br>如果按钮处于非活动状态该怎么办 |
| **临时访问** | 请求并获取对被阻止设备的临时访问权限。 |

| | |
|---|---|
| **支持** | 应用程序相关信息：Kaspersky Endpoint Security 的当前版本、数据库发布日期、密钥和其他信息。<br>您还可以访问卡巴斯基资源以获取有用信息或联系技术支持。 |
| **授权许可期限** | 剩余授权许可期限<br>您可以点击此区域打开 **授权许可** 窗口。在此窗口中，您可以查看 有关您的授权许可的详细信息，或访问卡巴斯基网站购买新的授权许可。 |

# 保护状态监控

## Kaspersky Security Center 客户端设备的保护状态

您可以使用客户端设备状态在 Kaspersky Security Center 中获取有关设备保护状态的信息。在 Kaspersky Security Center 中，客户端设备是指安装了 Kaspersky Security Center 网络代理的设备。

客户端设备状态可根据 Kaspersky Security Center 中配置的规则更改为 *严重* 或 *警告*。例如，如果设备上未安装保护应用程序、长时间未执行病毒扫描、应用程序数据库已过期、授权许可已过期，或者 Kaspersky Security Center 已从受管理应用程序接收到设备状态，则状态可能会发生变化。

有关状态更改原因和配置状态分配条件的更多详细信息，请参阅 Kaspersky Security Center 帮助。

**如何在 Web Console 中检查设备的保护状态**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
   列表仅显示所选管理组的受管理设备。
3. 单击设备名称。
4. 此时将打开受管理设备的属性窗口；在该窗口的“**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全盘扫描任务的日期和时间。
- **检测到病毒**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。

**如何在管理控制台中检查设备的保护状态**

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。

有关客户端设备状态的详细信息，请参阅 Kaspersky Security Center 帮助。

## 设备上应用程序运行的常规信息

**如何在 Web Console 中查看应用程序的常规信息**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。

   列表仅显示所选管理组的受管理设备。
3. 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. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。

   应用程序属性窗口将打开。

6. 在“**常规**”选项卡的“**信息**”部分中查看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**：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**”是设备上应用程序的状态，例如“*正在运行*”或“*已停止*”。
   - **已安装的更新**块包含有关已安装的应用程序更新版本的信息。
   - 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。

7. 在“**常规**”选项卡的“**组件**”部分中查看有关应用程序功能组件的信息。将显示每个组件的状态（例如，*“已停止”*、*“已暂停”*、“*未安装*”）和版本。

8. 在“**事件**”选项卡上查看设备上的应用程序事件列表。

**如何在管理控制台中查看应用程序的常规信息**

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 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。

   应用程序属性窗口将打开。

6. 在“**常规**”部分中查看应用程序行的常规信息。

   - **版本号**：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。
   - **当前状态**是应用程序（kesl 服务）的状态。应用程序可以具有“*正在运行*”或“*已暂停*”等状态。
   - **上次软件更新**：Kaspersky Endpoint Security 软件模块上次更新的日期和时间。
   - **已安装的更新**是有关已安装的应用程序更新版本的信息。
   - **应用程序数据库**是应用程序数据库更新发布的日期和时间。

7. 在“**组件**”部分中查看有关应用程序功能组件的信息。将显示每个组件的状态（例如，*“已停止”*、*“已暂停”*、“*未安装*”）和版本。

### 如何在命令行上查看应用程序的常规信息

运行以下命令：

```
kesl-control --app-info [--json] [--check-permissions]
```

其中：

`--json`：以 JSON 格式输出数据。

`--check-permissions` 显示权限配置不正确的应用程序目录的路径。

命令执行的结果会在控制台中显示如下信息：

- "**名称**"。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。
- 关于设备上应用的策略的扩展信息：
  - 策略名称。
  - 策略上次在设备上应用或更新时的日期和时间。
  - 该设备所属的 Kaspersky Security Center 管理组。
  - 设备上应用的策略配置文件列表（如有）。

  如果设备上安装的网络代理的"**允许应用程序检索设备上的策略扩展数据**"设置允许从 Kaspersky Endpoint Security 检索策略扩展数据，则会显示扩展的策略信息。默认禁用此选项。有关网络代理设置的详细信息，请参阅 Kaspersky Security Center 帮助。
- 有关应用程序使用的授权许可的信息：
  - "**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。
  - **Kaspersky Endpoint Security 授权许可到期日期**。应用程序授权许可到期日期和时间 (UTC)。
- Endpoint Detection and Response Optimum 组件以及用于与卡巴斯基解决方案集成的组件的授权许可信息。如果受保护设备上激活了以下组件，则会显示这些字段：
  - **EDR Optimum 授权许可信息**。有关激活 Endpoint Detection and Response Optimum 组件所用的授权许可的信息，或 EDR Optimum 授权许可密钥的状态。
  - **EDR Optimum 授权许可到期日期。**授权许可到期日期和时间 (UTC)。
  - **KUMA 授权许可信息**。有关据其使用 Kaspersky Unified Monitoring and Analysis Platform 功能的授权许可的信息，或 KUMA 授权许可密钥的状态。
  - **KUMA 授权许可到期日期**。授权许可到期日期和时间 (UTC)。
  - **MDR 授权许可信息**。有关激活 Managed Detection and Response 组件所用的授权许可或 MDR 授权许可密钥状态的信息。

- **MDR 授权许可到期日期**。授权许可到期日期和时间 (UTC)。
- **EDR Expert (on-premises) 授权许可信息**。有关激活 Endpoint Detection and Response Expert (on-premises) 组件所用的授权许可信息，或 EDR Expert (on-premises) 授权许可密钥状态。
- **EDR Expert (on-premises) 的授权许可到期日期**。授权许可到期日期和时间 (UTC)。
- **EDR Expert (cloud) 授权许可信息**。有关激活 Endpoint Detection and Response Expert (on-premise) 组件所用的授权许可信息，或 EDR Expert (cloud) 授权许可密钥状态。
- **EDR Expert (cloud) 的授权许可到期日期**。授权许可到期日期和时间 (UTC)。

- "**订阅状态**"。订阅的状态。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 整合的 MDR BLOB 文件的状态。
- "**MDR BLOB 文件中的授权许可到期日期**"。Kaspersky Managed Detection and Response 授权许可到期日期和时间 (UTC)。如果已为 Kaspersky Managed Detection and Response 整合加载了 BLOB配置文件，则会显示此字段。
- "**备份区状态**"。关于备份区状态的信息。
- "**备份区使用情况**"。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。
- "**应用程序数据库已加载**"。有关应用程序数据库是否已下载的信息。
- "**可更新的内核模块状态**"。关于可更新内核模块状态的信息。
- "**卡巴斯基安全网络使用**"。有关使用卡巴斯基安全网络的信息：`扩展 KSN 模式`、`基本 KSN 模式`或`已禁用`。
- **Light Agent 模式**。有关以 Light Agent 模式使用的应用程序的信息。如果应用程序以标准模式或 Endpoint Detection and Response Agent 模式使用，则不会显示此行。
- **Endpoint Detection and Response Agent 模式**。有关以 EDR Agent 模式 使用的应用程序的信息。如果应用程序在基本模式或 Light Agent 模式下使用，则不会显示此行。
- "**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：`Kaspersky Security Network`或`Kaspersky Private Security Network`。
- **Kaspersky Managed Detection and Response 集成**。Kaspersky Managed Detection and Response 集成状态。
- **Kaspersky Endpoint Detection and Response Optimum 整合**。与 Kaspersky Endpoint Detection and Response Optimum 整合的状态。
- **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。
- **BadUSB 攻击防护**。BadUSB 攻击防护组件状态。
- **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 Expert (on-premises) 集成**。与Kaspersky Endpoint Detection and Response Expert (on-premises)或与Kaspersky Endpoint Detection and Response (KATA)的集成状态。
- **Kaspersky Endpoint Detection and Response Expert (cloud) 集成**。Kaspersky Endpoint Detection and Response Expert (cloud) 集成状态。
- **Sandbox 集成**。Sandbox 集成状态。
- **Kaspersky Unified Monitoring and Analysis Platform 整合**。Kaspersky Unified Monitoring and Analysis Platform 整合状态。
- **Kaspersky Network Detection and Response (KATA) 整合** Kaspersky Network Detection and Response (KATA) 整合状态。
- **邮件威胁防护**。邮件威胁防护组件状态。
- "**更新后操作**"。应用程序更新操作和用户要执行的操作。
- "**应用程序不稳定**"。有关应用程序崩溃时生成转储的信息。如果在转储目录中找到任何文件，则会显示此字段。
- "**应用程序状态**"。有关网络代理连接状态和系统目录权限的信息：
  - "*正常*"。网络代理已连接，系统目录权限已正确配置。
  - "*严重。未连接到网络代理*"。
  - "*严重。系统目录的权限配置不正确*"。
  - "*严重。未连接到网络代理。系统目录的权限配置不正确*"。

**如何在图形界面中查看应用程序的常规信息**

1. 打开应用程序图形界面的主窗口。
2. 在主窗口下部，单击“**支持**”按钮。
   **支持**窗口将打开。
3. 查看设备和已安装应用程序的常规信息：
   - 应用程序版本。
   - **授权许可密钥**显示添加到应用程序的活动授权许可密钥，或者说未添加密钥的消息。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**显示有关活动主授权许可密钥状态的信息，或者说未添加密钥的消息。
   - **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。
   - **应用程序管理** – 有关设备是否受策略管理的信息。

   如果在网络代理策略中启用了“**允许应用程序检索设备上的策略扩展数据**”选项，则该窗口还会显示在应用程序安装设备上应用的策略的以下信息。
   - “**策略名称**”是指应用于应用程序安装设备的策略名称。
   - **应用日期** – 在安装了应用程序的设备上最后应用或更新策略的日期和时间。
   - “**管理组**”是指包含应用程序安装设备且受策略管理的管理组的名称。
   - “**活动策略配置文件**”是指设备上应用的活动策略配置文件列表（如有）。

## 应用程序统计信息

您可以查看扫描频率最高的文件和启动的进程的统计信息。

您可以在 `[ScannerImpactStats]` 部分的 kesl.ini 配置文件中配置应用程序计算和显示统计信息的方式。

**如何在 Web Console 中查看扫描统计信息**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
   列表仅显示所选管理组的受管理设备。
3. 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. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。

6. 在打开的应用程序属性窗口中，在**应用程序设置**选项卡上，选择**统计数据 → 扫描统计**。

7. 在“**扫描统计信息**”窗口中查看应用程序统计信息：

   - **最常扫描的应用程序（文件威胁防护）**块显示文件威胁防护组件最常扫描的应用程序的路径，以及该组件访问这些应用程序的次数。文件按访问次数的降序显示。
   - 在**最常启动的进程**下，您可以找到 Kaspersky Endpoint Security 最常检测的进程的路径以及此类进程启动的数量。进程路径按进程启动数量降序排列。

   您可以单击每个区域上部的“**导出**”按钮，将相应统计信息导出到文本文件。

**如何在管理控制台中查看扫描统计信息**

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 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。

6. 在打开的窗口中，选择**统计数据 → 扫描统计**。

7. 查看应用程序统计信息：

   - **最常扫描的应用程序（文件威胁防护）**块显示文件威胁防护组件最常扫描的应用程序的路径，以及该组件访问这些应用程序的次数。文件按访问次数的降序显示。
   - 在**最常启动的进程**下，您可以找到 Kaspersky Endpoint Security 最常检测的进程的路径以及此类进程启动的数量。进程路径按进程启动数量降序排列。

   您可以单击每个区域下方的“**导出**”按钮，将相应统计信息导出到文本文件。

**如何在命令行中查看扫描统计信息**

运行以下命令：

```
kesl-control [-S] --get-statistic [--files] [--processes]
```

其中：

- `--files`：文件威胁防护组件扫描最频繁的文件的统计数据，以及组件访问这些文件的次数。
- `--processes`：Kaspersky Endpoint Security 最常检测的进程启动的统计信息，以及此类启动的数量。

> 将进程从行为检测组件的扫描范围中排除，不会将这些进程从统计信息中移除，但可以提升Kaspersky Endpoint Security 应用程序的性能。

如果您不指定任何选项，应用程序将显示三个列表：有关最常扫描的文件的统计数据、有关最常启动的进程的统计数据以及在设备上找到的挂载点列表。

在 CentOS 5.2、5.4、6.4 和 6.6 上，不会收集扫描频率最高的文件的统计信息。

发现的挂载点

您可以查看在设备上找到的挂载点列表。该列表显示挂载点是否已添加到扫描排除项的信息。

**如何在 Web Console 中查看挂载点列表**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
   列表仅显示所选管理组的受管理设备。
3. 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. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。
6. 在打开的应用程序属性窗口中，在**应用程序设置**选项卡上，选择**统计数据 → 挂载点**。
   这将打开“**挂载点**”窗口。
7. 在表中查看挂载点信息：
   - **挂载点路径**是设备上检测到的挂载点的路径。
   - **命名空间**指示挂载点是否位于命名空间中。
   - **已排除**指示挂载点是否已被添加到扫描排除项中。

   挂载点路径按以下方式排序：
   - 静态、系统、服务和其他挂载点
   - 其命名空间中的已挂载 snap 包和挂载点
   - Docker 容器管理系统创建的挂载点

   通过单击窗口上部列表上方的“**导出**”按钮，您可以将挂载点列表导出到文本文件。该文件包含挂载点路径列表，以及**[Namespace]** 和 **[Excluded]**标签。

**如何在管理控制台中查看挂载点列表**

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 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。

6. 这将打开应用程序属性窗口；在该窗口中，选择“**统计信息**”→“**挂载点**”部分。

7. 在“**挂载点列表**”表中查看挂载点信息：

   - **挂载点路径**是设备上检测到的挂载点的路径。
   - **命名空间**指示挂载点是否位于命名空间中。
   - **已排除**指示挂载点是否已被添加到扫描排除项中。

   挂载点路径按以下方式排序：

   - 静态、系统、服务和其他挂载点
   - 其命名空间中的已挂载 snap 包和挂载点
   - Docker 容器管理系统创建的挂载点

   通过单击列表下方的**导出**按钮，您可以将挂载点列表导出为文本格式的文件。该文件包含挂载点路径列表，以及 `[Namespace]` 和 `[Excluded]` 标签。

**如何在命令行中查看挂载点列表**

运行以下命令：

```
kesl-control [-S] --get-statistic --mountpoints
```

输出包含以下信息：

- `[excluded]` 表示挂载点是否已添加到扫描排除项。
- `[namespace]`，指示挂载点是否位于命名空间中。
- 在设备上发现的挂载点的路径。

挂载点路径按以下方式排序：

- 静态、系统、服务和其他挂载点
- 其命名空间中的已挂载 snap 包和挂载点
- Docker 容器管理系统创建的挂载点

## 功能和技术列表

在命令行中，您可以查看应用程序功能列表及其状态信息（使用中或未使用），以及用于实现这些应用程序功能的 Linux 技术。

查看功能和技术列表

```
kesl-control --supported-tech-info
```

命令执行的结果会在控制台中显示如下信息：

文件操作拦截：

状态：使用中或未使用

技术：fanotify、文件威胁防护内核模块、可更新内核模块。

进程启动拦截：

状态：使用中或未使用

技术：eBPF、kprobe、netlink、未定义、可更新内核模块。

扫描网络流量：

状态：使用中或未使用

技术：eBPF、iptables、未定义。

iptables 工具：

状态：使用中或未使用

技术：ipv6、未定义、timeout、支持规则中的多个标签。

网络隔离：

状态：使用中或未使用

技术：eBPF、iptables、未定义。

漏洞利用防御：

状态：使用中或未使用

技术：未定义、可更新内核模块。

# 实时保护状态

实时计算机保护状态决定文件威胁防护组件的状态。文件威胁防护为计算机提供最低级别的安全保护。该组件随 Kaspersky Endpoint Security 一起启动，并实时扫描文件。

实时保护状态

| Kaspersky Security Center 中的状态 | 命令行中的状态 | 描述 |
|---|---|---|
| 运行中 | 已启动 | “文件威胁防护”任务已启动并正在运行。 |
| 正在启动 | 正在启动 或 正在恢复 | 尝试运行“文件威胁防护”任务。等待任务启动。 |
| 已停止 | 已停止 或 停止 | “文件威胁防护”任务已手动停止。在 Kaspersky Security Center 中或在计算机本地运行该任务。<br>如果应用程序安装在 Light Agent 模式下，当与 SVM 无连接时，设备将获得此状态。 |
| 已暂停 | 正在暂停 或 被暂停 | “文件威胁防护”任务已手动暂停。在 Kaspersky Security Center 中或在计算机本地运行该任务。 |
| 未设置 | | 应用程序已安装为 EDR Agent 模式。文件威胁防护组件在 Inform 模式下运行。 |
| 未知 | | 未知错误。 |

## 如何查看实时计算机保护状态

您可以在 Kaspersky Security Center 控制台的受管理设备列表中 或计算机本地查看实时计算机保护状态。

### 如何在 Web Console 中查看实时计算机保护状态

在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

当前保护状态显示在设备列表的 **实时保护状态** 列中。如果缺少 **实时保护状态** 列，请管理列设置（ ）。

### 如何在命令行中查看实时计算机保护状态

运行以下命令：

```
kesl-control --get-task-state 1
```

随后，Kaspersky Endpoint Security 将按以下格式显示有关文件威胁防护运行情况的信息：

| 名称: File_Threat_Protection | |
|---|---|
| ID | : 1 |
| 类型 | : OAS |
| 状态 | : <protection status> |

如果实时计算机保护状态不是 运行中，该怎么办

1. 确保已在策略属性中启用文件威胁防护。
2. 确保应用程序已激活。
3. 尝试运行“文件威胁防护”任务：

   **如何在 Web Console 中运行“文件威胁防护”任务**

   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
      将打开受管理设备列表。
   2. 在列表中找到您的设备并单击其名称。
   3. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**任务**”选项卡。
      这将打开设备上的所有任务列表。
   4. 选择 **文件威胁防护** 任务，然后单击 **运行** 按钮。

   **如何在命令行中运行“文件威胁防护”任务**

   运行以下命令：

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

# 事件和报告

在应用程序运行时，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应用程序数据库更新成功，或者通知应用程序组件出现需要修复的错误。

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，应用程序将事件信息存储在位于 /var/opt/kaspersky/kesl/private/storage 目录中的事件日志数据库文件中。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
- 使用应用程序的图形用户界面时 – 如果在策略属性或应用程序的常规设置中启用了显示通知，则在弹出通知中

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。
- Kaspersky Endpoint Security 的图形用户界面会显示应用程序、其组件和任务的报告。

## 报告和事件的内容

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
- 应用程序类别名称
- 存储库的网址
- 应用程序可执行文件的文件名、路径和哈希值

### 文件路径中字符转义的规则

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）。

# 将事件日志配置到操作系统日志中

Kaspersky Endpoint Security 运行期间发生的事件可以记录在操作系统日志 (syslog) 中。您可以使用 Web Console、管理控制台或命令行启用或禁用将事件记录到此日志中。

默认情况下，操作系统日志中的事件记录功能处于禁用状态。

如果 Kaspersky Endpoint Security 以标准模式或 EDR Agent 模式运行，并由 Kaspersky Security Center 中的策略进行管理，则默认情况下，有关添加和删除授权许可密钥以及授权许可到期的信息会记录在操作系统日志中。您可以在应用于应用程序的策略的属性中选择想要记录在操作系统日志中的事件。

### 如何在 Web Console 中配置将事件记录到 syslog

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**策略**”。
2. 单击 Kaspersky Endpoint Security for Linux 策略的名称。

   策略属性窗口将打开。
3. 转到“**应用程序设置**”选项卡。
4. 选择“**常规设置 → 事件设置**”。

   事件类型按严重级别分组显示。
5. 在名称为与要配置其操作系统日志记录的事件相对应的严重级别的块中，单击 **设置** 按钮。

   这将打开一个窗口，其中列出了所选严重级别的所有事件。您可以为每个事件单独启用或禁用记录到操作系统日志。
6. 在 **事件** 列中，单击要为其配置操作系统日志记录的事件名称。
7. 转到“**通知**”选项卡。
8. 选中或清除 **保存到操作系统事件日志中** 复选框。




事件通知设置

### 如何在管理控制台中配置将事件记录到 syslog

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。
4. 转到“**常规设置**”→“**界面**”区域。
5. 在“**通知**”下，单击“**配置**”。
   “**通知设置**”窗口打开。
6. 使用复选框选择应用程序在操作系统日志中记录的事件。
   您还可以选择特定严重级别的所有事件：
   - *严重事件*会对设备安全构成严重威胁（检测到恶意的对象、漏洞、应用程序运行问题）。关键事件需要您立即关注。我们建议不要禁用严重事件通知。
   - *功能失败*是指应用程序出现故障（处理错误、任务配置错误）。此类事件不会直接威胁设备安全，但需要您采取措施才能使应用程序正常运行。
   - *警告*不需要您立即采取行动，但可能表明设备安全存在潜在的未来威胁。
   - *信息消息*对应于信息性质的事件。

### 如何在命令行中配置将事件记录到 syslog

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。

启用或禁用将事件记录到 syslog

```
kesl-control --set-app-settings UseSyslog=<Yes|No>
```

其中：

- `Yes`：启用将所有事件保存到 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。

事件日志数据库包含以下文件：

- 几个包含事件的文件。文件数量取决于事件日志中的当前事件数以及应用程序被配置用来存储的最大事件数（`MaxEventsNumber`设置）。

  包含事件的文件的名称包括其序列号（例如，events.db.0001）。当文件写满时，会创建一个新文件。如果除最早文件外的所有事件文件中的最大事件数达到`MaxEventsNumber`值，则删除最早的文件。这意味着应用程序可能存储比设置更多的事件。

- 用于管理事件文件的数据库的主文件，用于存储关于事件日志文件的信息。此文件无法删除。

您可以通过常规应用程序设置在命令行上管理以下应用程序事件日志选项：

- 使用 `EventsStoragePath` 设置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。

您可以在命令行或配置文件中查看常规应用程序设置的当前值。

将应用程序常规设置的当前值输出到控制台

```
kesl-control --get-app-settings [--json]
```

其中指定 `--json` 后，将以 JSON 格式输出设置。

将应用程序常规设置的当前值输出到配置文件

```
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

其中 `--file <path to configuration file>` 是要将应用程序常规设置输出到的配置文件的路径。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。

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。

使用命令行选项修改事件设置

```
kesl-control --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

其中 <设置名称>=<设置值> 是其中一项设置的名称和值。

使用配置文件更改事件设置

```
kesl-control --set-app-settings --file <path to configuration file> [--json]
```

其中：

- `--file <path to configuration file>` 是包含常规应用程序设置的配置文件的完整路径。如果删除配置文件中的任何参数，则执行命令后将显示该参数的默认值。
- 如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果未指定 --json 选项，应用程序将尝试从 INI 文件导入。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。

# 查看应用程序事件

### 在 Kaspersky Security Center 中查看 Kaspersky Endpoint Security 应用程序的所有事件

Kaspersky Endpoint Security 应用程序的事件按严重程度分为以下几种类型：

- *严重事件*会对设备安全构成严重威胁（检测到恶意的对象、漏洞、应用程序运行问题）。关键事件需要您立即关注。我们建议不要禁用严重事件通知。
- *功能失败*是指应用程序出现故障（处理错误、任务配置错误）。此类事件不会直接威胁设备安全，但需要您采取措施才能使应用程序正常运行。
- *警告*不需要您立即采取行动，但可能表明设备安全存在潜在的未来威胁。
- *信息消息*对应于信息性质的事件。

所有 Kaspersky Endpoint Security 事件的列表显示在 Web Console 和管理控制台中。

### 如何在 Web Console 中查看所有事件列表

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 转到“**事件配置**”选项卡。

   将显示按严重级别筛选的所有事件列表。
4. 使用左侧菜单查看其他严重级别的所有事件。

**如何在管理控制台中查看所有事件列表**

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。
4. 转到“**常规设置**”→“**通知设置**”部分。
5. 在“**通知**”下，单击“**配置**”。
   “**通知设置**”窗口打开。

您可以配置事件通知。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。

在应用程序的图形界面中查看事件

默认情况下，在应用程序的图形界面中，信息事件会以弹出通知的形式显示。

**如何在 Web Console 中配置弹出式通知**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**策略**”。
2. 单击 Kaspersky Endpoint Security for Linux 策略的名称。
   策略属性窗口将打开。
3. 转到“**应用程序设置**”选项卡。
4. 选择“**常规设置 → 事件设置**”。
5. 单击 **附加设置** 链接。
   “**附加设置**”窗口打开。
6. 选中或清除“**在图形用户界面中显示弹出式通知**”复选框。默认情况下已选定该选框。
7. 保存更改。

**如何在管理控制台中配置弹出式通知**

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。
4. 转到“**常规设置**”→“**通知设置**”部分。
5. 选中或清除“**在图形用户界面中显示弹出式通知**”复选框。默认情况下已选定该选框。

### 如何在命令行配置弹出式通知

在命令行中，您可以使用ShowPopUpNotifications中的 ShowPopUpNotifications 设置启用或禁用图形界面中的弹出通知。

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该设置的值。

允许在图形界面中显示弹出式通知

```
kesl-control --set-app-settings ShowPopUpNotifications=<Yes|No>
```

其中：

- Yes （默认值）— 在图形用户界面中显示弹出通知。
- No — 不在图形用户界面中显示弹出通知。

在命令行中查看 Kaspersky Endpoint Security 应用程序的当前事件

在命令行中，您可以输出有关应用程序中所有当前事件或与指定任务相关的事件的信息。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。

在控制台中显示有关所有当前应用程序事件的信息

```
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。

运行任务，并将与其关联的当前事件信息输出到控制台

```
kesl-control --start-task <task ID|name> -W
```

其中 <task ID|name> 是创建任务时分配给该任务的 ID，或者是命令行中的任务名称。

该命令会启动具有指定 ID 或名称的任务，并启用与该任务关联的当前事件的输出。事件一旦由该任务生成，就会立即输出。

启动 ID=1 的任务并启用其事件输出的示例

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

在控制台中显示有关符合筛选条件的当前事件的信息

```
kesl-control -W --query "<filter conditions>"
```

其中，<filter conditions> 是采用 <field> <comparison operation> '<value>' 格式并由 and 逻辑运算符组合的一个或多个 逻辑表达式。

TaskStateChanged 事件输出示例

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

由“User”用户发起的 TaskSettingsChanged 事件输出示例

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

显示应用程序事件日志中的事件

您可以使用命令行将应用程序事件日志中的事件信息输出到控制台或文件。要输出事件子集，请使用 筛选。

将应用程序事件日志中所有事件的信息输出到控制台

```
kesl-control -E --query [--db <database file>]
```

其中，<database file> 是要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，应用程序将事件信息存储在 /var/opt/kaspersky/kesl/private/storage/events.db 数据库中。数据库的位置由 EventsStoragePath 常规应用程序设置决定。

如果事件日志位于默认数据库中，请使用以下命令将事件输出到控制台：

```
kesl-control -E
```

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。

在控制台中显示应用程序事件日志中符合特定条件的事件信息

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

其中：

- <filter conditions> 指定一个或多个采用 <field> <comparison operator> '<value>' 格式且使用逻辑运算符 and 组合的 逻辑表达式，以限制查询结果。
- <number> 是选择中要输出的最新事件数（即从选择末尾开始计数的记录数）。
- --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）。

将应用程序事件日志中所有事件的信息输出到文件

```
kesl-control -E --query "<>" [--db <database file>] [-n <number>] --file <path to file> [--json]
```

其中，--file <path to file> 是要将事件输出到的文件的完整路径。

实用文章

如何处理误报

# 查看报告

只有在应用程序的图形界面中才能查看报告。

有关每个 Kaspersky Endpoint Security 组件的运行、每个扫描任务的执行情况、更新任务和完整性检查任务以及应用程序整体运行的信息都记录在*报告*中。

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*

应用程序中提供以下报告：

- **统计**。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**。有关应用程序运行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**。有关以下应用程序组件运行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
  - Web 威胁防护
  - 邮件威胁防护
  - 网络威胁防护
  - BadUSB 攻击防护
  - 防火墙管理

- 应用程序控制
- 设备控制
- 行为检测
- 漏洞利用防御
- 系统完整性监控
- Web 控制

- **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任务记录的事件的信息。
- **执行防护** 此报告包含有关 EDR Expert (on-premises) 和 EDR Optimum 组件执行对象执行防护期间记录的事件的信息。

**如何在应用程序界面中查看报告**

1. 打开应用程序图形界面的主窗口。
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。

   报告将显示在窗口的右侧。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。

   默认情况下，事件按**日期和时间**列中的值升序排序。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。
4. 要查看事件的相关详细信息，请在报告中选择事件。

   包含此事件属性的部分将会显示在窗口底部。

# 获取系统性能指标

Kaspersky Endpoint Security 会影响操作系统。为了帮助您分析影响，应用程序可以获取与应用程序性能相关的指标。

您可以使用 Grafana 等数据可视化工具分析指标。您可以将导出的指标发布到 Prometheus 和 Zabbix 等监控系统。

配置应用程序所用操作系统资源的指标收集

```
kesl-control [-J] --export-metrics [--period <interval in seconds between outputs>|--interactive]
```

其中：

`--period` 启用定期向命令行输出结果（输出间隔以秒为单位指定）。

`--interactive`可启用交互式输出（按下**Enter**键时）。

此命令可将指标列表输出到控制台。

指标列表

| 指标的内部名称；指标的标签和类型 | 描述和推荐阈值设置 |
| --- | --- |
| lfs_system_descriptor_opened_count<br>Gauge | kesl 进程当前打开的描述符的数量。<br>如果描述符的数量每小时增长超过 250 个，我们建议联系技术支持。 |
| lfs_system_uptime_milliseconds<br>计数器 | 从操作系统启动到现在的毫秒数。 |
| lfs_system_memory_usage_bytes<br>'type=virtual' 标签<br>Gauge | kesl 进程当前使用的虚拟化内存量。<br>我们建议采取措施根据系统信息设置阈值。您可以手动或使用脚本获取此信息。如需示例脚本，您可以联系技术支持。 |
| lfs_system_memory_usage_bytes<br>'type=resident' 标签<br>Gauge | kesl 进程当前使用的驻留内存量。<br>我们建议采取措施根据系统信息设置阈值。您可以手动或使用脚本获取此信息。如需示例脚本，您可以联系技术支持。 |
| lfs_system_memory_usage_bytes<br>'type=swap' 标签<br>Gauge | kesl 进程当前使用的交换空间量。<br>我们建议采取措施根据系统信息设置阈值。您可以手动或使用脚本获取此信息。如需示例脚本，您可以联系技术支持。 |
| lfs_system_memory_wd_limits_bytes<br>'type=virtual' 标签<br>Gauge | kesl 进程的虚拟内存的使用限制。 |
| lfs_system_memory_wd_limits_bytes<br>'type=resident' 标签<br>Gauge | kesl 进程的驻留内存的使用限制。 |
| lfs_system_memory_wd_limits_bytes<br>'type=swap' 标签<br>Gauge | 限制 kesl 进程使用交换空间。 |
| lfs_system_cpu_usage_milliseconds<br>'type=user' 标签<br>计数器 | 从 kesl 进程启动到现在，kesl 进程在用户空间使用的 CPU 时间（毫秒）。<br>我们建议采取措施根据系统信息设置阈值。您可以手动或使用脚本获取此信息。如需示例脚本，您可以联系技术支持。 |
| lfs_system_cpu_usage_milliseconds<br>'type=kernel' 标签<br>计数器 | 从 kesl 进程启动到现在，kesl 进程在内核空间中使用的 CPU 时间（毫秒）。<br>我们建议采取措施根据系统信息设置阈值。您可以手动或使用脚本获取此信息。如需示例脚本，您可以联系技术支持。 |
| lfs_system_cpu_usage_milliseconds<br>'type=total' 标签<br>计数器 | 从 kesl 进程启动到现在，kesl 进程在用户空间和内核空间中使用的 CPU 时间（毫秒）。<br>如果 kesl 进程使用的 CPU 时间超过了其余工作负载，我们建议联系技术支持。 |
| lfs_tcpSynInterceptor_connection_hanging_count<br>计数器 | 从 kesl 进程启动到现在，在服务器和客户端之间的 TCP 网络中握手阶段挂起的网络连接总数（如果网络连接一直在等待远程服务器允许连接，则视为挂起，时间介于 1 秒到 2 分钟之间，具体取决于 /proc/sys/net/ipv4/tcp_syn_retries 中的系统设置）。<br>该指标的增加可能是由于远程服务器无法访问或丢失造成的。如果挂起的网络连接数量每分钟增加超过 10 个，我们建议联系技术支持。 |
| lfs_tcpSynInterceptor_connection_count<br>Gauge | 当前等待连接到远程服务器的网络连接数。 |
| lfs_tcpSynInterceptor_verdict_count<br>“verdict=allow”标签<br>计数器 | 从 kesl 进程启动到现在，已建立的被拦截连接总数。 |
| lfs_tcpSynInterceptor_verdict_count<br>‘verdict=drop’ 标签<br>计数器 | 从 kesl 进程启动到现在，已拦截的尚未建立的连接总数。 |

| 指标的内部名称；指标的标签和类型 | 描述和推荐阈值设置 |
| --- | --- |
| lfs_tcpSynInterceptor_verdict_count<br>'verdict=unknown' 标签<br>计数器 | 从 kesl 进程启动到现在远程服务器的解决方法无法处理的网络连接总数。 |
| lfs_tcpSynInterceptor_verdict_latency_milliseconds<br>直方图 | 从拦截 SYN 数据包到对其发出解析、远程服务器对连接做出判决所用时间的直方图。 |
| lfs_tproxy_connection_count<br>'direction=inbound' 标签<br>Gauge | 当前拦截的入站网络连接数。 |
| lfs_tproxy_connection_count<br>'direction=outbound' 标签<br>Gauge | 当前拦截的出站网络连接数。 |
| lfs_tproxy_connection_processed_count<br>'direction=inbound' 标签<br>计数器 | 拦截的入站网络连接总数。 |
| lfs_tproxy_connection_processed_count<br>'direction=outbound' 标签<br>计数器 | 拦截的出站网络连接总数。 |
| lfs_tproxy_connection_orphaned_count<br>计数器 | Kaspersky Endpoint Security 拦截的连接总数（从 Web 威胁防护、网络威胁防护和 Web 控制保护组件启动开始），尽管这些拦截并非有意为之（例如，由于 iptables 配置不兼容或应用程序没有时间处理新的拦截配置）。此类连接将被拒绝。<br>如果此类连接的总数超过 10 个，这可能表明应用程序或系统运行不正确，我们建议联系技术支持。 |
| lfs_tproxy_threadPool_task_count<br>计数器 | 自 Web 威胁防护、网络威胁防护和 Web 控制保护组件启动以来，已添加到线程池的任务总数（新连接、新一批数据、已发送的数据等）。<br>如果已建立但未完成的任务总数不断增加，则需要添加资源、配置排除项或联系技术支持。 |
| lfs_tproxy_threadPool_thread_count<br>Gauge | 为网络拦截器的 MITM 机制提供服务的线程数。线程由线程管理器创建，用于处理连接。所有线程都执行相同的代码，并在其中等待网络事件，例如新连接以及已建立连接上的传入数据包。 |
| lfs_tproxy_threadPool_thread_waiting<br>Gauge | lfs_tproxy_threadPool_thread_count 中的空闲线程数。网络拦截器的 MITM 机制中等待 poll 的线程。 |
| lfs_tproxy_threadPool_task_duration_milliseconds<br>直方图 | 处理被拦截连接的任务执行时间的直方图。<br>如果 95% 的任务执行时间超过 1 秒，则需要添加资源、配置排除项或联系技术支持。 |
| lfs_tproxy_socket_count<br>Gauge | 当前套接字数量（监听套接字和连接套接字）。被拦截的连接有 2 个连接套接字。 |
| lfs_trafficScanning_object_hanging_count<br>Gauge | 当前拦截流量中挂起对象扫描的数量（持续时间超过 1 分钟的扫描被视为挂起）。<br>挂起对象扫描总数超过 35 表示应用程序数据库存在问题。在这种情况下，我们建议联系技术支持。 |
| lfs_trafficScanning_object_duration_milliseconds<br>直方图 | 被拦截流量扫描持续时间的直方图。<br>如果 95% 的对象的扫描时间超过 1 秒，则需要添加资源、更新应用程序数据库或联系技术支持。<br>如果拦截流量中数据包扫描的增长率为 0，且 lfs_tproxy_threadPool_task_count 指标的值不为 0，则需要更新应用程序数据库或联系技术支持。 |
| lfs_fileMonitor_cache_size<br>Gauge | 文件监视器（文件修订缓存）的当前大小，用于监视文件修改。<br>如果当前文件监视器缓存大小大于 50,000，我们建议联系技术支持。 |
| lfs_fileMonitor_cache_hit_count<br>计数器 | 文件监视器缓存（文件修订缓存）的命中次数，用于监视文件修改。 |

| 指标的内部名称；指标的标签和类型 | 描述和推荐阈值设置 |
| --- | --- |
| lfs_fileMonitor_cache_miss_count<br>计数器 | 文件监视器缓存（文件修订缓存）的未命中计数，用于监视文件修改。 |
| lfs_faCache_file_count<br>Gauge | 当前不需要扫描的 fanotify 拦截器文件的缓存大小。<br>如果当前文件缓存大小大于 100,000，我们建议联系技术支持。 |
| lfs_faCache_file_hit_count<br>计数器 | 不需要扫描的 fanotify 拦截器文件缓存的命中次数。 |
| lfs_faCache_file_miss_count<br>计数器 | 不需要扫描的 fanotify 拦截器文件缓存未命中次数。 |
| lfs_faCache_volume_count<br>Gauge | fanotify 拦截器挂载点缓存的当前大小。 |
| lfs_oas_cache_file_count<br>Gauge | 当前不需要扫描的文件威胁防护文件的缓存大小。<br>如果当前文件缓存大小大于 100,000，我们建议联系技术支持。 |
| lfs_oas_cache_file_hit_count<br>计数器 | 不需要扫描的文件威胁防护文件缓存的命中次数。 |
| lfs_oas_cache_file_miss_count<br>计数器 | 不需要扫描的文件威胁防护文件缓存的未命中次数。 |
| lfs_oas_cache_volume_count<br>Gauge | 文件威胁防护装载点缓存的当前大小。 |
| lfs_processManager_cache_size<br>Gauge | 系统中当前已缓存的活动进程数。 |
| lfs_processManager_cache_hit_count<br>计数器 | 系统进程缓存的命中计数。 |
| lfs_processManager_cache_miss_count<br>计数器 | 系统进程缓存的未命中计数。 |
| lfs_blockingProcessInterceptor_cache_size<br>Gauge | 可用于启动进程的解释器缓存的当前大小。<br>这个数字取决于脚本在特定设备上运行的强度。如果当前文件缓存大小大于 10000，我们建议联系技术支持。 |
| lfs_blockingProcessInterceptor_cache_hit_count<br>计数器 | 解释器缓存的命中次数。 |
| lfs_blockingProcessInterceptor_cache_miss_count<br>计数器 | 解释器缓存的未命中计数。 |
| lfs_doc_prevention_cache_file_count<br>Gauge | 不需要扫描的对象的 *对象的执行防护* 任务文件缓存的当前大小（打开文档时）。 |
| lfs_script_prevention_cache_file_count<br>Gauge | 不需要扫描的对象的 *对象的执行防护* 任务文件缓存的当前大小（运行脚本时）。 |
| lfs_doc_prevention_cache_file_hit_count<br>计数器 | 不需要扫描的对象的 *对象的执行防护* 任务文件缓存中的命中次数（打开文档时）。 |
| lfs_script_prevention_cache_file_hit_count<br>计数器 | 不需要扫描的对象的 *对象的执行防护* 任务文件缓存中的命中次数（运行脚本时）。 |
| lfs_doc_prevention_cache_file_miss_count<br>计数器 | 不需要扫描的对象的 *对象的执行防护* 任务文件缓存中的未命中次数（打开文档时）。 |
| lfs_script_prevention_cache_file_miss_count<br>计数器 | 不需要扫描的对象的 *对象的执行防护* 任务文件缓存中的未命中次数（运行脚本时）。 |
| lfs_doc_prevention_cache_volume_count<br>Gauge | 文档的“对象的执行防护”任务的挂载点缓存的当前大小。 |
| lfs_script_prevention_cache_volume_count<br>Gauge | 脚本的“对象的执行防护”任务的挂载点缓存的当前大小。 |

| 指标的内部名称；指标的标签和类型 | 描述和推荐阈值设置 |
| --- | --- |
| eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds<br>Gauge | 注册表中注册的所有客户端的当前指标更新花费了多长时间（以毫秒为单位）。 |
| eka_telemetry_metrics_registry_registered_callbacks<br>Gauge | MetricsRegistry 为所有注册客户端执行的指标更新回调的当前数量。 |
| eka_telemetry_metrics_registry_scrape_duration_milliseconds<br>Gauge | 获取所有注册表指标花了多长时间（以毫秒为单位）。<br>如果该指标的 99% 的值在 10 分钟内超过 1 秒，我们建议联系技术支持。 |

# 应用程序稳定性监控

Kaspersky Endpoint Security 应用程序稳定性监控会跟踪应用程序异常停止的次数，并在应用程序性能不稳定时通知管理员。

**如何在 Web Console 中配置应用程序稳定性监控**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**策略**”。
2. 单击 Kaspersky Endpoint Security for Linux 策略的名称。
   策略属性窗口将打开。
3. 转到“**应用程序设置**”选项卡。
4. 选择“**常规设置**” → “**性能**”。
5. 选中或清除 **启用应用程序稳定性监控** 复选框。默认情况下已清空该复选框。

**如何在管理控制台中配置应用程序稳定性监控**

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。
4. 转到“**常规设置**”→“**应用程序设置**”部分。
5. 选中或清除 **启用应用程序稳定性监控** 复选框。默认情况下已清空该复选框。

要应用此设置，必须重启应用程序和网络代理。

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>*。

**如何在命令行中配置应用程序稳定性监控**

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 Kaspersky Endpoint Security 稳定性监控。

`TrackProductCrashes` 用于在应用程序不稳定时将设备状态信息从 Kaspersky Endpoint Security 发送到 Kaspersky Security Center。设置可以使用以下值：

- `Yes/true` 可启用将设备状态信息从 Kaspersky Endpoint Security 发送到 Kaspersky Security Center。
- `No/false` 可禁用将设备状态信息从 Kaspersky Endpoint Security 发送到 Kaspersky Security Center。

`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`设置允许您设置应用程序异常停止的次数，超过此次数后会显示关于应用程序不稳定的通知。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。

修改此文件后，请重启 Kaspersky Endpoint Security。

# 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。黑客可以将应用程序的一个或多个可执行模块或文件替换为包含恶意代码的其他文件。为防止此类模块和文件替换，Kaspersky Endpoint Security 可以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。如果应用程序模块或文件的校验和不正确，则认为其已损坏。

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 Web 插件
- Kaspersky Endpoint Security MMC 管理插件

使用完整性检查实用程序检查应用程序组件的完整性。该实用程序检查名为*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。清单文件经过数字签名，其完整性也得到检查。

要在 Linux 设备上运行完整性检查实用程序，需要具有 root 权限的账户。

完整性检查实用程序与应用程序一起安装，位于以下路径中：

- 作为应用程序包（integrity_checker）的一部分：/opt/kaspersky/kesl/bin/integrity_checker。
- 作为 Kaspersky Endpoint Security 的 MMC 管理插件 (integrity_checker.exe) 的一部分：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<版本编号>.plg\integrity_checker.exe – 适用于 32 位操作系统
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<版本编号>.plg\integrity_checker.exe — 适用于 64 位操作系统

清单文件位于以下路径中：

- 要检查应用程序包的完整性：/opt/kaspersky/kesl/bin/integrity_check.xml。
- 要检查图形用户界面包的完整性：/opt/kaspersky/kesl/bin/gui_integrity_check.xml。
- 检查网络代理：
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – 适用于 32 位操作系统
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – 适用于 64 位操作系统
- 检查 Kaspersky Endpoint Security MMC 管理插件：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<插件版本>.plg\integrity_check.xml – 适用于 32 位操作系统
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<插件版本>.plg\integrity_check.xml – 适用于 64 位操作系统

要检查解决方案组件的完整性，您需要从该组件工具的文件夹运行该工具。

检查应用程序软件包的完整性

```
integrity_checker [<path to manifest file>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type
kds-with-filename
```

检查图形界面软件包的完整性

```
integrity_checker <path to manifest file> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-
with-filename
```

检查 Kaspersky Endpoint Security MMC 管理插件的完整性

```
integrity_checker.exe [<path to manifest file>]
```

检查网络代理的完整性

```
integrity_checker <path to manifest file>
```

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 <directory>` 是包含证书吊销列表的目录的路径。
- `--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数据摘要。
- `--trace <file name>` 将扫描期间发生的事件以 DEBUG 日志级别写入指定文件。
- `--signature-type kds` 是要验证的签名类型（检查 Kaspersky Endpoint Security 管理 Web 插件时需要此选项）。
- `--signature-type kds-with-filename` 是要验证的签名类型（检查应用程序软件包和图形界面软件包时需要此设置）。
- `--single_file <file name>` 仅检查清单中的指定文件，并忽略清单中的所有其他对象。
- `--version` – 显示实用程序的版本，但不执行完整性检查。

查看完整性检查工具的所有可用选项

```
integrity_checker --help
```

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 中生成相应的事件。

# 应用程序访问控制

Kaspersky Endpoint Security 中的访问控制基于Role Based Access Control (RBAC) 策略。要向用户授予特定权限或资源访问权限，您需要分配相应的角色。*角色*是用于管理应用程序的一组权限和特权。

用户角色使访问权限的日常管理更加轻松快捷。角色的访问权限根据用户的典型任务和岗位职责进行配置。

应用程序需要操作系统中的提升权限才能保护设备。应用程序需要 root 权限才能执行其部分基本安全功能。

应用程序基于角色的访问模型包括 管理员 (admin) 角色。在某些情况下，具有管理员角色的用户所执行的操作可能会导致以操作系统超级用户 (root) 的权限执行操作。

管理员角色只能授予受信任的用户。此管理员角色遭到入侵或被滥用会导致整个设备失陷，并可能影响组织基础设施以及用户数据的安全性、完整性或性能。

授予管理员角色是系统所有者的责任，并且应根据您组织的访问控制策略以及对相关用户的信任级别来执行。

# 预定义角色

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。

操作系统中会创建四个系统用户组：

- kesladmin
- kesluser
- keslaudit
- nokesl

当您向系统用户分配应用程序角色时，该用户将被添加到相应组中（请参见下表）。当您撤消用户的角色时，该用户将从相应组中移除。

分配或撤消角色后，您必须重启应用程序（kesl 进程）及其图形界面（kesl-gui 进程）。

角色和用户组

| 角色名 | 应用程序中的角色 | 操作系统用户组 | 权限 |
|---|---|---|---|
| 管理员 | admin | kesladmin | 无需使用 sudo 命令，即可在应用程序的图形界面和命令行中管理应用程序设置和任务设置。<br>管理应用程序授权许可。<br>为用户分配角色。<br>撤销用户的角色（管理员无法撤销自己的 admin 角色）。<br>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。<br>启动和停止更新任务。<br>将文件发送到沙盒进行扫描<br>查看此用户创建的任务的报告。<br>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<br>查看应用程序状态。<br>查看所有任务、其设置和开始计划。<br>查看所有活动。<br>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。 |

# 如何分配或撤销用户角色

角色定义用户在系统中的权限以及用户可以执行的操作。只有具有管理员 (kesladmin) 角色的用户才能管理角色。建议在受保护设备上至少创建一个具有管理员角色的用户，以避免由具有 root 权限的用户管理应用程序。

查看用户和角色列表

```
kesl-control --get-user-list
```

为用户分配角色

```
kesl-control --grant-role <admin|user|audit> <user name>
```

为用户 test15 分配 audit 角色的示例

```
kesl-control --grant-role audit test15
```

撤销用户的角色

```
kesl-control --revoke-role <role> <user name>
```

为用户 test15 撤销 audit 角色的示例

```
kesl-control --revoke-role audit test15
```

# Kaspersky Security Center 中的 RBAC 功能区域

默认情况下，Kaspersky Security Center 管理系统中具有“Kaspersky Endpoint Security 管理员”角色的用户可以访问 Kaspersky Endpoint Security 的所有功能。

您可以为 Kaspersky Endpoint Security 用户或组选择以下预定义的 Kaspersky Endpoint Security 功能访问级别之一：

- **读取**允许查看 Kaspersky Endpoint Security 的常规设置和 Kaspersky Endpoint Security 组件的设置。
- **编辑**允许查看和编辑 Kaspersky Endpoint Security 的常规设置以及 Kaspersky Endpoint Security 组件的设置。
- **执行**允许启动和停止 Kaspersky Endpoint Security 任务。
- **对设备选择执行操作**允许对选定设备启动和停止 Kaspersky Endpoint Security 任务。

您还可以配置高级访问权限：允许或拒绝访问 Kaspersky Endpoint Security 功能。

*如何在 Web Console 中配置应用程序功能的访问权限*

1. 在 Web Console 的主窗口中，选择“**用户和角色**” → “**角色**”。
2. 选择要为其配置功能区域的角色。
   如有必要，您可以添加新角色。有关详细信息，请参见 Kaspersky Security Center 帮助。

3. 配置 Kaspersky Endpoint Security 应用程序的访问权限。

4. 单击“**保存**”按钮。

Kaspersky Endpoint Security 功能的访问权限

| 功能区域 | Kaspersky Endpoint Security 功能 |
| --- | --- |
| 基本功能 | 更新应用程序数据库和模块<br>回滚<br>清查<br>BadUSB 攻击防护<br>系统完整性监控<br>系统完整性检查<br>检测设置<br>卡巴斯基安全网络<br>用户交互<br>性能<br>网络设置<br>容器扫描<br>技术支持<br>报告和存储<br>与 KSC 的整合<br>遥测源和 auditd 模式（操作系统交互设置）<br>事件设置<br>Light Agent 模式<br>添加密钥 |
| 应用程序控制 | 应用程序控制 |
| 设备控制 | 设备控制 |
| 数据加密 | 授予对设备的临时访问权限（设备控制） |
| 信任区域 | 受信任区域：<br>• 指定受信任的网址<br>• 受信任的 IP 地址<br>• 被监控的端口<br>• 受信任的根证书<br>• 受信任域<br>• 受信任的挂载点<br>• 流量拦截排除<br>• 受信任的应用程序<br>• 恶意软件扫描排除项<br>• 受信任设备 |
| Detection and Response | 内置代理：<br>• Managed Detection and Response<br>• Endpoint Detection and Response<br>• Endpoint Detection and Response Expert (on-premises)<br>• Endpoint Detection and Response Expert (cloud)<br>• Network Detection and Response (KATA)<br>• Sandbox<br>• 与 KUMA 的整合。<br>响应操作：<br>• 终止进程<br>• 启动进程<br>• IOC 扫描<br>• 从设备接收文件<br>• 移动文件到隔离区<br>• 从设备删除文件<br>• 网络隔离<br>• 对象的执行防护<br>• 遥测设置 |

| 功能区域 | Kaspersky Endpoint Security 功能 |
| --- | --- |
| 主机入侵防御 | 行为检测<br>漏洞利用防御<br>反加密<br>网络威胁防护<br>防火墙管理 |
| 保护组件 | 恶意软件扫描<br>关键区域扫描<br>文件威胁防护<br>邮件威胁防护<br>可移动驱动器扫描<br>Web 威胁防护 |
| Web 控制 | Web 控制 |

# 受保护设备典型角色的建议

### 工作站

如果您在工作站上安装应用程序，建议您同时安装该应用程序的图形界面。

安装应用程序后：

- 启用 Web 威胁防护。
- 如果设备未直接连接到互联网，请在网络流量扫描设置中使用以下选项之一选择本地证书验证：
  - 在 Web Console 中，在 **加密连接扫描** 下，单击 **设置** 按钮，然后将 **证书验证策略** 设置为 **本地检查**。
  - 在管理控制台中，在 **加密连接设置** 下，将 **证书验证策略** 设置为 **本地检查**。
  - 在设备本地使用命令行：

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

    应用程序不使用互联网来验证证书。
- 为使用 Samba 和 NFS 协议挂载在设备上的所有远程目录配置文件操作拦截排除项（全局排除项）。

### 文件服务器

安装应用程序后：

1. 确保在 文件威胁防护 设置中禁用压缩文件扫描。默认情况下已选定该选项。
2. 使用以下设置创建一个 *恶意软件扫描* 任务：
   - 扫描压缩文件：已启用
   - 任务计划：在最低负载时段

### Web 服务器

Kaspersky Endpoint Security 不适用于 Web 服务器保护。为了保护 Web 服务器，建议使用 Kaspersky NGFW 和 Kaspersky Web Traffic Security。

如果您在 Web 服务器上使用 Kaspersky Endpoint Security，且该服务器使用 HTTPS 协议并具有较高的客户端负载，则 Web 威胁防护 可能会显著增加系统资源使用率。这是由于应用程序解密和 HTTPS 流量扫描造成的。

分析 Web 威胁防护运行期间 Web 服务器负载的变化。您可以配置排除项以优化设置并消除兼容性问题。

**代理服务器**

安装应用程序后，在充当代理服务器或负载均衡器的设备上禁用 Web 威胁防护 和 网络威胁防护 组件。

**支持容器化的服务器**

安装应用程序后，在用于容器化服务的服务器上禁用 Web 威胁防护、网络威胁防护 和 防火墙管理 组件。为了保护容器环境，您可以使用卡巴斯基容器安全应用程序。

**数据库服务器**

为数据库管理系统的工作目录配置全局排除项。

请向 DBMS 管理员确认您的基础架构中的工作目录列表。

以下示例路径适用于 Ubuntu 操作系统。在其他操作系统中，目录可能有所不同。

**常用 DBMS 的建议**

**PostgreSQL**。彻底消除数据文件和预写日志（WAL 文件）文件操作的任何延迟至关重要。我们还建议排除 PostgreSQL 进程和表空间的文件操作（请参见下面的示例）。在典型的 PostgreSQL 安装中，这些文件位于以下目录中：

- 统计信息和并行查询：`/dev/shm`
- 数据：`/var/lib/postgresql/<PostgreSQL version>/main`
- WAL 文件：`/var/lib/postgresql/<PostgreSQL version>/main/pg_wal`
- 可执行文件：`/usr/lib/postgresql/<PostgreSQL version>/bin/`。

**Postgres Pro**。请遵循 PostgreSQL 的指导原则。此外，请将 `/var/lib/pgpro/<Postgres Pro version>/data` 目录添加到排除项中。

**Oracle Database**。您可以从 `/etc/oratab` 配置文件中获取所有数据库的工作目录列表。

**ScyllaDB**。使用 Web 威胁防护和网络威胁防护组件时，请使用 eBPF 流量拦截模式。要管理 Detection and Response 解决方案的缓存模式，请使用 kesl.ini 配置文件中 `UseIncreasedXdrEventsCache=yes` 设置的默认值。

**配置 PostgreSQL 工作目录的全局排除项的示例**

如果您使用基于 *fanotify 技术*的机制来拦截系统事件，则 DBMS 文件目录必须是挂载点。如果您使用*可更新内核模块*来拦截系统事件，则无需创建挂载点。

*要创建挂载点：*

1. 检查包含数据库文件的目录是否为挂载点：

   ```
   mount
   ```

   如果 mount 命令的输出中没有这些目录：

   a. 创建挂载点：

   ```
   mount --bind /var/lib/postgresql/<PostgreSQL version>/main/ /var/lib/postgresql/<PostgreSQL version>/main
   ```

   您无需为包含 WAL 文件的目录创建单独的挂载点，因为该目录嵌套在数据目录中。

   b. 将以下行添加到 /etc/fstab 文件，以使新创建的挂载点在系统重启后仍保留：

   ```
   /var/lib/postgresql/<PostgreSQL version>/main /var/lib/postgresql/<PostgreSQL version>/main none
   defaults,bind 0 0
   ```

2. 重启 PostgreSQL 服务：

   ```
   systemctl restart postgresql
   ```

*要配置工作目录的全局排除项：*

1. 将目录添加到全局排除项：

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/var/lib/postgresql/<PostgreSQL version>/main
   kesl-control --set-app-settings ExcludedMountPoint.item_0001=/var/lib/postgresql/<PostgreSQL
   version>/main/pg_wal
   kesl-control --set-app-settings ExcludedMountPoint.item_0002=/usr/lib/postgresql/<PostgreSQL version>/bin/
   kesl-control --set-app-settings ExcludedMountPoint.item_0003=/usr/lib/postgresql/<PostgreSQL version>
   ```

2. 如果使用表空间，也请将其添加到排除项中：

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=<tablespace directory>
   ```

3. 重启应用程序以应用全局排除项：

   ```
   systemctl restart kesl
   ```

# 更新应用程序数据库和模块

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。新病毒和其他类型的恶意软件每天都在全世界出现。Kaspersky Endpoint Security 数据库包含有关威胁的信息和使其失效的方法。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。

如果 应用程序部署 成功，并且您在初始配置阶段选择了更新数据库，则安装应用程序后，数据库为最新状态。在 Kaspersky Security Center 中查看设备保护状态时，您可以通过查看客户端设备的状态以及在命令行中使用 `kesl-control --app-info` 命令，获取有关数据库状态的信息。如果数据库不是最新状态，您需要配置并启动数据库更新。

## 配置数据库和模块更新

1. **选择更新分发方案和更新源**

   *更新源*是包含 Kaspersky Endpoint Security 数据库和应用程序模块更新的资源。更新源可以是以下任一项：卡巴斯基更新服务器；Kaspersky Security Center 管理服务器存储；FTP、HTTP 或 HTTPS 服务器；用户使用 Samba 或 NFS 协议挂载的本地或网络目录。

   如果 Kaspersky Endpoint Security 在 Light Agent 模式 下使用，则受保护的虚拟机上的数据库将从 SVM 上的目录更新。

2. **配置数据库更新任务**

   *Update* 任务下载更新包，并在设备上安装数据库和应用程序模块更新。

应用程序可能无法在美国境内提供更新功能（包括反病毒签名更新和代码库更新）。

更新期间，以下对象将下载并安装到您的设备中：

- Kaspersky Endpoint Security 数据库。应用程序数据库包括恶意软件检测规则、网络攻击描述、恶意网址和钓鱼网址数据库、广告栏数据库、垃圾邮件数据库以及其他数据。
- 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。模块更新可能更改应用程序组件的行为和添加新功能。

您还可以接收自动安装的应用程序更新（自动补丁）。自动补丁包含应用程序的修复和改进。

更新时，您计算机上的应用程序模块和数据库将与 更新源 中的最新版本进行比较。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。

## 实用文章

应用程序数据库和模块更新故障排除

收到以下状态时该怎么办：“已安装应用程序更新或 cryptossl 模块更新。重启应用程序。”

# 如何选择更新源和更新分发方案

## 选择 Kaspersky Endpoint Security 更新源

*更新源*是包含 Kaspersky Endpoint Security 数据库和应用程序模块更新的资源。

更新源可以是以下之一：卡巴斯基更新服务器、Kaspersky Security Center 管理服务器的存储、用户挂载的本地或网络 (SMB/NFS) 目录、FTP、HTTP 或 HTTPS 服务器。选择您自己的 HTTPS 服务器作为更新源时，需要确保它具有正确的证书链。自签名证书只能用作证书链中的根证书。在这种情况下，您需要将其添加到设备上的受信任证书列表中。

如果 Kaspersky Endpoint Security 在 Light Agent 模式 下使用，则受保护的虚拟机上的数据库将从 SVM 上的目录更新。

如果选择了多个资源作为更新源，Kaspersky Endpoint Security 将尝试从列表顶端开始依次连接这些资源，并通过从第一个可用源检索更新包来执行更新任务。您可以在尝试连接所选更新源时，配置所选更新源的响应超时。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。

## 选择更新分发方案

Kaspersky Endpoint Security 支持以下数据库和应用程序模块更新分发方案：

### 集中更新

如果您使用 Kaspersky Security Center 集中管理组织中的设备保护，我们建议设置集中式数据库更新。集中更新可减少外部 Internet 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。

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 作为更新源。

### 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。有关卡巴斯基更新服务器的更多信息，请参阅技术支持知识库。

### 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

自定义更新源必须包含预先下载的更新包（例如，可以使用 Kaspersky Update Utility 预先下载这些更新包）。选择您自己的 HTTPS 服务器作为更新源时，需要确保它具有正确的证书链。自签名证书只能用作证书链中的根证书。在这种情况下，您需要将其添加到设备上的受信任证书列表中。您可以在“*更新*”任务设置中指定自定义更新源。有关创建自定义更新源的详细信息，请参阅 Kaspersky Security Center 帮助。

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，请指定代理服务器设置。

# 如何配置数据库更新任务

*Update* 任务下载更新包，并在设备上安装数据库和应用程序模块更新。

## 在 Kaspersky Security Center 中更新数据库

在 Kaspersky Security Center 中，*Update* 任务由管理服务器快速启动向导自动创建。要在运行向导时创建 *Update* 任务，您需要安装 Kaspersky Endpoint Security 管理插件。

您可以使用自动创建的 *Update* 组任务，也可以使用 Web Console 或管理控制台创建并运行自定义组更新任务和本地更新任务。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，则受保护的虚拟机上的数据库将使用特殊的 *Update* 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。

### 如何在 Web Console 中配置和运行更新任务

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 在任务列表中，选择 Kaspersky Endpoint Security 更新任务，然后单击任务名称。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在 **更新源** 区域中，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。

   更新源列表包含两个源：卡巴斯基更新服务器和 Kaspersky Security Center。**状态**列指示应用程序在运行任务时是否正在使用此更新源。您可以单击**添加**按钮将其他更新源添加到列表中。作为更新源，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。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. 在任务属性窗口中，选择 **计划** 选项卡，并配置更新任务的运行计划。默认情况下，为该任务选择手动启动模式。

   如果您已选择 **Kaspersky Security Center** 作为更新源，请从“**启动计划**”下拉列表中选择“**当下载更新到存储库时**”。有关任务计划的详细信息，请参阅 Kaspersky Security Center 帮助。

6. 保存更改。

任务将根据配置的计划启动。您也可以手动运行该任务。

**如何在管理控制台中配置和运行更新任务**

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，选择更新任务并双击该任务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. 在表格中，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。

   更新源列表包含两个源：卡巴斯基更新服务器和 Kaspersky Security Center。**状态**列指示应用程序在运行任务时是否正在使用此更新源。您可以单击**添加**按钮将其他更新源添加到列表中。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**”选项卡并配置运行更新任务的计划。默认情况下，为该任务选择手动启动模式。

   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**”。有关任务计划的详细信息，请参阅 Kaspersky Security Center 帮助。

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。您也可以手动运行该任务。

在命令行中更新数据库

在命令行中，您可以使用 *Update* 预定义任务更新数据库和应用程序模块，或创建 Update 类型的用户任务。

您可以管理手动更新任务（启动、停止、暂停和恢复）、配置任务计划，并通过更改任务设置来管理更新设置。

**如何在命令行中创建和配置更新任务**

在命令行中，您可以通过两种方式创建和配置自定义更新任务：

- 通过在配置文件中指定任务的所有设置来创建任务。
- 创建具有默认设置的任务，然后配置其设置。

使用配置文件中的设置创建更新任务

```
kesl-control --create-task <task name> --type <task type> --file <path to file> [--json]
```

其中：

- `<path to file>` 是配置文件的完整路径，该配置文件包含您要用于该任务的设置。
- 指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json`选项，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。

  配置文件示例

  ```
  ConnectionTimeout=10
  ApplicationUpdateMode=DownloadOnly
  [Sources.item_0000]
  Enabled=Yes
  SourceType=Custom
  URL=https://s00.upd.kaspersky.com
  ```

*要创建并配置具有默认设置的更新任务：*

1. 运行以下命令创建任务：

   ```
   kesl-control --create-task <更新任务名称> --type Update
   ```

   其中 `<update task name>` 是要为新更新任务设置的名称。

   此命令将创建具有默认设置的更新任务。

2. 如有必要，请运行以下命令管理更新任务设置：

   ```
   kesl-control --set-settings <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

3. 如有必要，请运行以下命令管理更新任务计划设置：

   ```
   kesl-control --set-schedule <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

4. 运行以下命令检查任务设置的当前值：

   ```
   kesl-control --get-settings <update task ID|name>
   ```

在应用程序的图形界面中更新数据库

**如何在图形界面中启动或停止更新任务**

1. 打开应用程序图形界面的主窗口。
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。

# 如何使用卡巴斯基更新实用程序进行更新

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。

*要配置 Kaspersky Security Center 使用 Kaspersky Update Utility 从共享目录更新数据库：*

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 Kaspersky 知识库。
3. 配置从组织的本地网络中其他设备上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。
   d. 在“更新源”表中，单击“**添加**”按钮并指定共享目录的路径。

      更新源的地址必须与 Kaspersky Update Utility 设置中指定的地址相匹配。

   e. 选中“**使用此源**”复选框，单击“**确定**”。
   f. 在表中，使用“**向上**”和“**向下**”按钮设置更新源的顺序。
   g. 将更改保存到任务设置中。

*要配置 Kaspersky Security Center 使用命令行从共享目录更新数据库：*

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 Kaspersky 知识库。

3. 将应用程序数据库和模块配置为从组织本地网络中其他设备上的指定共享目录进行更新：在 `Update` 任务设置 中，设置 `SourceType=Custom`，并在 `[Sources.item_#]` 部分中指定共享目录的路径。

   更新源的地址必须与 Kaspersky Update Utility 设置中指定的地址相匹配。

# 如何回滚数据库和应用程序模块的更新

在数据库和应用程序模块进行第二次更新以后，可以使用将数据库和应用程序模块回滚至其先前版本的功能。

每次用户开始更新程序时，Kaspersky Endpoint Security 会为当前数据库和程序模块创建一个备份副本。让您能够在必要时将数据库和程序模块回滚至它们的前一版本。回滚上次更新是有用的，例如，如果新的数据库版本导致误报，从而导致 Kaspersky Endpoint Security 阻止安全应用程序。

如果 Kaspersky Endpoint Security 在 Light Agent 模式下使用，则无法使用该任务回滚数据库更新。

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。

在命令行上，您可以通过以下方式回滚数据库更新：

- 运行 *回滚*预定义任务。
- 创建并运行*回滚*自定义任务。

“*回滚*”任务没有任何设置。

**如何在 Web Console 中回滚数据库和应用程序模块的更新**

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

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，选择应用程序的名称。

   b. 在“**任务类型**”下拉列表中，选择“**回滚**”。

   c. 在 **任务名称** 字段中，输入新任务的名称。

   d. 在 **要对其分配任务的设备** 下，选择要如何定义任务范围。

4. 根据您首选的任务范围定义方法选择设备。

5. 结束向导。
   在任务列表中将显示一个新任务。

6. 选中任务旁边的复选框，然后单击“**开始**”按钮。

**如何在管理控制台中回滚数据库和应用程序模块的更新**

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，在列表中选择 Kaspersky Endpoint Security 和 **回滚** 任务类型。

3. 如果您正在为一组设备创建任务，向导会提示您选择要将任务分配给的设备。选择您要如何定义任务范围。

4. 根据您首选的任务范围定义方法选择设备。

5. 配置任务的计划。

6. 输入新任务的名称。

7. 结束向导。
   在任务列表中将显示一个新任务。

8. 在任务列表中，选择该任务，打开该任务的上下文菜单，然后选择 **启动**。

**如何在命令行上回滚数据库和应用程序模块的更新**

请执行命令：

回滚数据库和模块更新

```
kesl-control --start-task 7
```

**如何在图形界面中回滚数据库和应用程序模块的更新**

1. 打开应用程序图形界面的主窗口。

2. 在主应用程序窗口中，单击**更新**。
   **更新**窗口将打开。

3. 单击 **回滚更新** 链接以回滚数据库更新。

# 主机威胁防护

# 文件威胁防护

文件威胁防护为计算机提供最低级别的安全保护。该组件随 Kaspersky Endpoint Security 一起启动，并实时扫描文件。

## 文件威胁防护的工作原理

1. **应用程序会拦截文件操作事件，并阻止相关操作，直到扫描完成。**

   该应用程序使用文件操作拦截机制，并在扫描完成之前阻止对该文件的所有访问。

2. **应用程序扫描文件**

   文件威胁防护使用以下技术扫描文件：

   - 反病毒数据库。
   - 卡巴斯基安全网络的云服务。
   - 启发式分析技术能够检测卡巴斯基数据库尚未涵盖的威胁。

3. **扫描完成**

   扫描完成后，应用程序会允许该操作，或者阻止该操作并执行在检测到威胁时指定的操作。

## 文件威胁防护的初始配置

初始配置包括基本端点保护所需的必要步骤。

1. **选择系统事件拦截机制**

   文件威胁防护会拦截文件操作事件，并阻止相关操作，直到扫描完成。

   安装应用程序时，您选择了系统事件拦截机制：

   - 基于可更新内核模块的拦截机制
   - 基于 fanotify 的系统事件拦截机制
   - 适用于没有 fanotify 的操作系统的文件威胁防护内核模块

   系统事件拦截机制的选择取决于计算机的配置。提供最高性能的拦截技术是可更新内核模块。您可以在应用程序设置中启用此机制。

2. **配置文件威胁防护**

   默认情况下，文件威胁防护已启用，并使用卡巴斯基专家建议的设置运行。默认设置提供建议的保护级别和最佳资源使用。如果您对基础设施安全有特殊要求，可以更改这些设置。

### 3 配置保护范围

默认情况下，应用程序会扫描受保护设备上的所有文件。如果您只需扫描单个目录（例如，从外部源自动下载文件的目录），可以仅将该目录指定为保护范围。在其他情况下，我们建议保留默认保护范围，并使用排除项来微调范围。

### 4 从扫描中排除挂载点

从扫描中排除挂载点可让您避免拦截特定目录中的文件操作。例如，您可以从扫描中排除共享网络资源，并使用 Kaspersky Endpoint Security 在实际存储这些资源的设备上对其进行保护。您还可以参考文件威胁防护和扫描任务建议。

### 5 添加排除项

排除项有助于平衡系统安全性和性能。为了保证第三方软件稳定运行，请将相应软件文档中列出的文件和目录添加到排除项。

我们建议排除以下对象：

- 数据库。扫描大型数据库需要大量资源。频繁访问数据库文件会触发频繁扫描。
- 资源密集型进程使用的文件。扫描此类文件会降低计算机运行速度。
- 包含日志文件的目录。操作系统会持续向日志文件写入信息。因此，文件威胁防护会浪费计算机资源来扫描日志。

> 如果某个对象已被文件威胁防护组件排除在扫描范围之外，我们建议使用*恶意软件扫描*任务扫描此类对象。

## 高负载服务器的附加配置

附加配置包括微调文件威胁防护的步骤。完成初始配置后，如果遇到任何延迟或正在配置高负载服务器，请按照以下步骤操作：

### 1 在扫描期间禁用文件访问阻止

默认情况下，文件威胁防护会阻止对正在扫描的文件的所有访问，直到扫描完成。如果禁用阻止模式，文件威胁防护将以通知模式运行。这种文件操作拦截模式在扫描时对系统性能的影响较小，但存在文件中的威胁可能无法清除或删除的风险。

> 如果禁用阻止模式，设备控制、对象执行防护操作和可移动驱动器扫描任务也会以通知模式运行。

### 2 收集文件扫描统计信息

监控计算机的主要性能指标：CPU 负载、第三方软件性能或其他指标。这将帮助您确定如何降低系统负载。

您可以使用应用程序性能分析工具获取文件扫描统计信息。您也可以使用自己的监控工具。

### 3 优化应用程序性能

分析收集到的信息后，优化应用程序性能：

- 添加全局排除项
- 添加排除项
- 优化应用程序设置

4. **在扫描期间启用文件访问阻止**

   启用扫描期间的文件访问阻止。当检测到感染对象时，应用程序将执行选定的操作。

特殊注意事项和限制

- 如果 root 用户无权访问通过 NFS4 协议挂载到设备上的远程目录中的文件，应用程序将阻止所有用户访问此类文件。
- 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命名空间和容器。

# 如何创建保护范围

*保护范围*是 Kaspersky Endpoint Security 为检测威胁而扫描的对象路径列表。默认情况下，应用程序会扫描受保护设备上的所有文件。如果您只需要扫描单个目录（例如，从外部源自动下载文件的目录），则可以将此目录指定为保护范围。在其他情况下，我们建议保留默认保护范围，并使用排除项来微调范围。

Kaspersky Endpoint Security 会按照对象在对象列表中的显示顺序扫描对象。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。

**如何在 Web Console 中创建保护范围**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

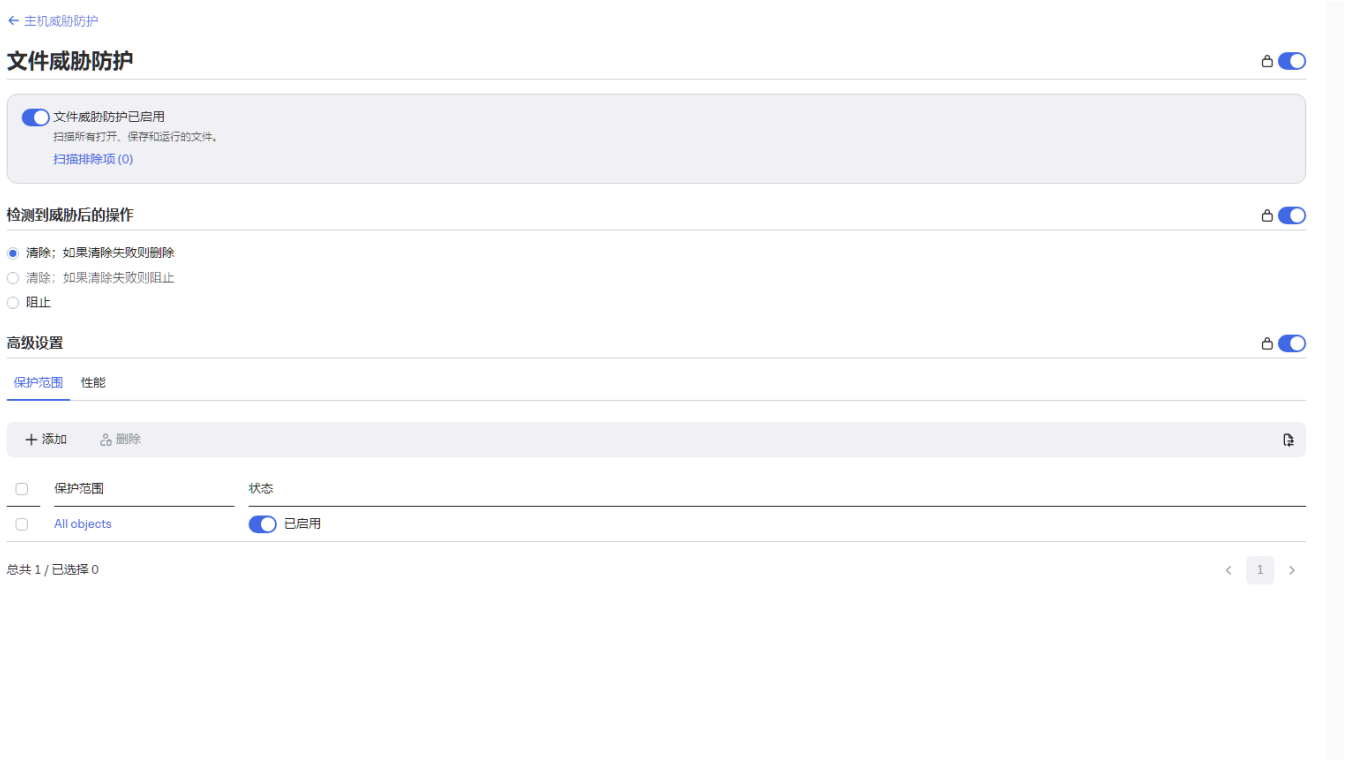
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**主机威胁防护 → 文件威胁防护**”。
5. 在**保护范围**块，单击**添加**。
6. 这将打开一个窗口；在该窗口中，选择文件系统类型：
   - “**本地**”。无需网络连接即可访问的硬盘目录。
   - “**挂载**”。已挂载的远程或本地目录。
   - “**共享**”。可通过 Samba (SMB) 或 NFS 协议访问的计算机目录。
   - “**全部远程挂载**”。使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。
   - “**全部共享**”。通过 Samba 和 NFS 协议访问的所有计算机目录。

7. 对于本地文件系统，请指定目录路径（例如，`/path/to/folder`）。如有必要，选中“**包括子文件夹**”复选框。

8. 指定已挂载或共享文件系统的访问协议。

9. 为对象扩展名指定掩码（例如，`*.txt`）。用逗号分隔各个掩码。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




文件威胁防护

## 如何在命令行创建保护范围

1. 运行以下命令：

```
kesl-control --set-settings 1 --add-path <path>
```

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。

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 1
```

示例

```
kesl-control --set-settings 1 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

以下保护范围设置将添加到任务中：

```
[ScanScope.item_0001]
AreaDesc=All object
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

# 如何选择检测到文件威胁后的操作

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。在文件威胁防护设置中，您可以选择 Kaspersky Endpoint Security 在检测到威胁时执行的操作。

### 如何在 Web Console 中配置检测到威胁后的操作

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**主机威胁防护 → 文件威胁防护**”。
5. 在 **检测到威胁后的操作** 下，选择应用程序在检测到威胁时将执行的操作：
   - **清除；如果清除失败则删除**（默认）。如果选择该选项，应用程序将自动尝试对已检测到的受感染文件执行清除操作。如果清除失败，应用程序将删除文件。
   - “**清除；如果清除失败则阻止**”。如果选择该选项，应用程序将自动尝试对已检测到的受感染文件执行清除操作。如果清除失败，应用程序将阻止这些文件。
   - “**阻止**”。如果选择该选项，应用程序将自动阻止受感染的文件，而不试图对其进行清除或删除。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行中配置检测到威胁后的操作

1. 运行以下命令：

```
kesl-control --set-settings 1 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 1
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ActionOnThreat` | 检测到威胁后的操作：<br>• `DisinfectDeleteIfNotPossible`（默认）。如果选择该选项，应用程序将自动尝试对已检测到的受感染文件执行清除操作。如果清除失败，应用程序将删除文件。<br>• `DisinfectBlockIfNotPossible`。如果选择该选项，应用程序将自动尝试对已检测到的受感染文件执行清除操作。如果清除失败，应用程序将阻止这些文件。<br>• `Block`。如果选择该选项，应用程序将自动阻止受感染的文件，而不试图对其进行清除或删除。 |

# 什么是文件扫描的智能模式

文件威胁防护会扫描所有打开、保存或执行的文件。默认情况下，文件威胁防护以智能模式扫描文件。在 *智能模式*下，当尝试打开文件时，文件威胁防护会扫描该文件。如果某个进程在一段时间内反复访问并修改某个文件，文件威胁防护只会在该进程关闭该文件时重新扫描该文件。这可在提供高级别保护的同时，最大限度地减少应用程序对系统性能的影响。

要使智能模式正常工作，必须选择并启动可更新内核模块。

您无法在 Web Console 中更改文件扫描模式。

*如何在命令行中选择文件扫描模式*

1. 运行以下命令：

```
kesl-control --set-settings 1 ScanByAccessType=<SmartCheck|OpenAndModify|Open>
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 1
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ScanByAccessType` | 文件扫描模式：<br>• `SmartCheck`（默认值）。文件威胁防护以智能模式扫描文件。Kaspersky Endpoint Security 会在文件打开时扫描该文件，如果该文件已被修改，还会在文件关闭时扫描该文件。<br>如果智能模式不可用，应用程序会在文件打开时以及每次修改文件时扫描文件（`OpenAndModify`）。例如，如果可更新内核模块已停止，智能模式可能不可用。<br>• `OpenAndModify`。Kaspersky Endpoint Security 会在文件打开时以及每次修改文件时扫描该文件，而不仅在文件关闭时扫描。<br>• `Open`。Kaspersky Endpoint Security 会在尝试打开文件进行读取、执行或修改时扫描该文件。 |

# 如何优化文件扫描

配置文件扫描以优化文件威胁防护组件。这有助于降低受保护设备的 CPU 使用率。您可以限制压缩文件扫描，设置可扫描对象的最大大小，以及设置对象扫描的最长持续时间。

### 如何在 Web Console 中配置文件扫描

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 转到“**主机威胁防护 → 文件威胁防护**”。

5. 在 **高级设置** 下，选择 **性能** 选项卡并配置文件扫描：

   - “**扫描压缩包**”。这包括扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他类型的压缩文件。应用程序不仅可通过扩展名识别文件，还可通过格式识别文件。在扫描压缩文件时，应用程序会递归解包。这样就可以检测嵌套压缩文件（压缩文件中的压缩文件）中的威胁。默认情况下，扫描处于禁用状态。

   - “**扫描分发包和自解压存档文件**”。扫描第三方应用程序的安装包和自解压存档。自解压缩文件是包含可执行解压模块的压缩文件。默认情况下，扫描处于禁用状态。

   - “**扫描电子邮件数据库**”。扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件客户端的电子邮件数据库。默认情况下，扫描处于禁用状态。

   - “**扫描电子邮件格式文件**”。扫描纯文本电子邮件。默认情况下，扫描处于禁用状态。

   - “**不扫描大小大于该值(MB)的压缩包**”。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。

   - “**跳过扫描时间超过以下值的文件(秒)**”。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。默认情况下，应用程序会尝试在一分钟内扫描对象。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行中配置文件扫描

1. 运行以下命令：

```
kesl-control --set-settings 1 ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<Object size (MB)>
TimeLimit=<Scan time (sec)>
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 1
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| ScanArchived | 这包括扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他类型的压缩文件。应用程序不仅可通过扩展名识别文件，还可通过格式识别文件。在扫描压缩文件时，应用程序会递归解包。这样就可以检测嵌套压缩文件（压缩文件中的压缩文件）中的威胁。默认情况下，扫描处于禁用状态。 |
| ScanSfxArchived | 扫描第三方应用程序的安装包和自解压存档。自解压缩文件是包含可执行解压模块的压缩文件。默认情况下，扫描处于禁用状态。 |
| ScanMailBases | 扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件客户端的电子邮件数据库。默认情况下，扫描处于禁用状态。 |
| ScanPlainMail | 扫描纯文本电子邮件。默认情况下，扫描处于禁用状态。 |

| 设置 | 描述 |
| --- | --- |
| `SkipPlainTextFiles` | 从扫描中临时排除纯文本格式的文件。如果文本文件在最近一次扫描后 10 分钟内被同一进程重复使用，应用程序不会扫描这些文本文件。默认情况下，扫描排除处于禁用状态。<br>此设置适用于支持 fanotify 系统事件拦截机制的设备。在具有可更新内核模块的设备上，应用程序使用扫描结果缓存来优化负载。 |
| `SkipDatabaseJournals` | 暂时将数据库日志文件排除在扫描范围之外。如果数据库日志文件在最近一次扫描后 10 分钟内被同一进程重复使用，应用程序不会扫描该文件。默认情况下，扫描排除处于禁用状态。<br>此设置适用于支持 fanotify 系统事件拦截机制的设备。在具有可更新内核模块的设备上，应用程序使用扫描结果缓存来优化负载。 |
| `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。（值 `0`）。 |
| `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。默认情况下，应用程序会尝试在一分钟内扫描对象。（值 `60`）。 |

# 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。

*符号链接*（也称为 Soft link）是指向另一个文件或目录的文件。符号链接及其指向的文件可以位于不同的文件系统中。此外，此类链接可能指向不存在的文件。删除目标文件时，链接不会被删除，但会停止工作。

*Hard link* 本质上是文件的另一个名称。硬链接指向文件的索引描述符 (inode)，其中包含该文件的元数据。只要至少存在一个指向该文件的硬链接，该文件就会继续存在于文件系统中。

## 扫描符号链接

仅当符号链接指向的文件位于文件威胁防护的保护范围内时，应用程序才会扫描符号链接。

如果文件位于保护范围之外，应用程序不会沿符号链接扫描文件的内容。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

如果在有多个硬链接指向的文件中检测到恶意代码，应用程序将清除原始文件。如果无法清除，应用程序将删除该硬链接，并在备份区中创建源文件的副本，副本名称与已删除链接的名称相同。应用程序仅删除正在处理的硬链接，其他可能指向相同数据的硬链接保持不变。

从 备份区 恢复硬链接时，应用程序会在原始位置创建原始文件的副本，副本名称与正在恢复的硬链接名称相同。恢复后的链接不会成为指向原始文件的硬链接，并且与指向同一文件的其他硬链接保持独立。

### 解析按进程排除中的符号链接

如果 `ExcludedForProgram` 部分的 `ProgramPath` 参数中指定的路径是指向二进制可执行文件的符号链接，应用程序会将排除应用于目标文件的路径。此规则适用于指向此文件的所有链接，而不仅仅是明确指定的链接。此参数使用程序映像的路径，因此不会解析指向脚本的符号链接（例如，`.sh`）。

运行任务并应用设置时，将确定目标文件。如果链接指向不存在的文件，则链接本身的路径将包含在排除中。如果随后将该链接替换为同名的普通可执行文件，则排除将应用于该文件。

包含符号链接的排除示例

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/md5sum
UseExcludedForProgram=Yes
Path=/root/s1
```

启动任务时，`/usr/bin/md5sum` 链接指向 `/bin/coreutils`，因此 `/bin/coreutils` 将添加到排除中。如果该链接之后重定向到 `/bin/false`，则排除将继续应用于 `/bin/coreutils`，直到任务重新启动，而不会应用于 `/bin/false`。任务重新启动后，排除将应用于 `/bin/false`，而不再应用于 `/bin/coreutils`。

# 恶意软件扫描

恶意软件扫描对于计算机安全至关重要。定期进行恶意软件扫描有助于防止因安全级别设置过低或者其他原因导致保护组件未能检测到的恶意软件进行传播。

Kaspersky Endpoint Security 预定义了“*恶意软件扫描*”标准任务。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。

管理服务器初始配置向导会自动创建“*恶意软件扫描*”任务。要创建“*恶意软件扫描*”任务，请在运行该向导时安装 Kaspersky Endpoint Security for Linux 管理插件。如有必要，您可以创建“*恶意软件扫描*”类型的用户任务。

### 恶意软件扫描 任务设置

1. **配置任务运行计划**

   扫描期间，Kaspersky Endpoint Security 可能会比平时占用更多计算机资源。我们建议计划扫描任务在计算机负载最低时运行。

2. **优化扫描对系统造成的负载**

   运行“恶意软件扫描”任务时，您可以限制 CPU 使用率。这可能会增加扫描计算机所需的时间。

   Kaspersky Endpoint Security 允许在笔记本电脑使用电池供电时取消计划任务。

### 3 配置“恶意软件扫描”任务设置

默认情况下，“恶意软件扫描”任务使用卡巴斯基专家建议的设置。默认设置提供建议的保护级别和最佳资源使用。如果您对基础设施安全有特殊要求，可以更改这些设置。

默认情况下，应用程序会扫描压缩文件。为此，应用程序会将压缩文件解压缩到 /tmp 目录。请确保计算机上有足够的可用空间来解压缩压缩文件。

### 4 配置扫描范围

默认情况下，应用程序会扫描受保护设备上的所有文件。如果您只需扫描单个目录（例如，从外部来源自动下载文件的目录），可以仅将该目录指定为扫描范围。在其他情况下，我们建议保留默认扫描范围，并使用排除项来微调该范围。

要扫描服务器，我们建议将扫描范围划分为多个子范围，并为每个子范围创建单独的“恶意软件扫描”任务。为分散负载，请为每个任务计划不同的开始时间。

### 5 添加扫描排除项

设置排除范围：

- **扫描排除项**。排除项有助于平衡系统安全性和性能。为确保第三方软件稳定运行，请将相应软件文档中列出的文件和目录添加到排除项中。

  如果您已为文件威胁防护组件创建了排除范围，也可以将这些排除项应用于“恶意软件扫描”任务。

- **全局排除项**。排除挂载点（全局排除项）可让您避免拦截特定目录中的文件操作。从扫描范围中排除共享网络资源。要保护共享网络资源，请在物理存储资源的设备上使用 Kaspersky Endpoint Security 应用程序。

### 6 运行“恶意软件扫描”任务

**如何在 Web Console 中运行恶意软件扫描任务**

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“*恶意软件扫描*”任务。

   任务属性窗口将打开。

   “*恶意软件扫描*”任务由管理服务器快速启动向导自动创建。要创建“*恶意软件扫描*”任务，请在运行该向导时安装 Kaspersky Endpoint Security for Linux 管理插件。

   如有必要，您可以创建“*恶意软件扫描*”类型的用户任务。

3. 在**设置**选项卡上，管理任务设置。

4. 在**应用程序设置**选项卡上，配置应用程序的高级设置（参见下表）。

5. 在**计划**选项卡上，配置任务的启动方式。

   默认情况下，Kaspersky Endpoint Security 配置为手动运行该任务。

6. 保存更改。

7. 运行任务。

*恶意软件扫描*任务设置

| 设置 | 描述 |
| --- | --- |
| **扫描范围** | 包含任务扫描的范围的表。默认情况下，只有一个扫描范围处于活动状态；该范围包括本地文件系统的所有目录。您可以手动添加扫描范围。 |
| **检测到威胁后的操作** | • **清除；如果清除失败则删除**（默认值）。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>• "**清除；如果清除失败则通知**"。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>• "**通知**"。如果选择此操作，应用程序会在日志中创建关于感染对象的记录。 |
| **扫描压缩包** | 如果启用此选项，应用程序将扫描压缩文件。<br>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。<br>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。您可以通过指定"**跳过扫描时间超过以下值的文件(秒)**"和"**不扫描大小大于该值(MB)的文件**"设置来缩短压缩文件扫描时间。<br>默认情况下已禁用该选项。 |
| **扫描分发包和自解压存档文件** | 如果启用此选项，应用程序将扫描自解压压缩文件。自解压缩文件是包含可执行解压模块的压缩文件。<br>默认情况下已禁用该选项。 |
| **扫描电子邮件格式文件** | 如果启用此选项，应用程序将扫描文本格式的电子邮件。<br>默认情况下，该功能处于禁用状态。 |
| **扫描电子邮件数据库** | 如果启用此选项，应用程序将扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。<br>默认情况下，该功能处于禁用状态。 |
| **不扫描大小大于该值(MB)的文件** | 您可以指定可扫描文件的最大大小，单位为兆字节。<br>可用值：1-999999。默认情况下，此限制处于禁用状态。 |
| **跳过扫描时间超过以下值的文件(秒)** | 您可以指定文件的最长扫描时间，单位为秒。在指定时间后，应用程序将停止扫描该文件。<br>可用值：1-9999。默认情况下，此限制处于禁用状态。 |
| **不同时运行多个扫描任务** | 如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。<br>默认情况下，该功能处于禁用状态。 |
| **使用 iChecker 技术** | 如果启用此选项，应用程序将仅扫描新增文件以及上次扫描后修改过的文件。<br>如果禁用此选项，应用程序将扫描文件，而不考虑文件的创建或修改日期。<br>默认情况下已禁用该选项。 |

## 如何在命令行运行"恶意软件扫描"任务

1. 默认情况下，应用程序有一个*恶意软件扫描*（*Scan_My_Computer*）任务。如果您想要创建新的*恶意软件扫描*任务，请运行以下命令：

```
kesl-control --create-task <task name> --type ODS
```

其中 `<task name>` 是您要为新任务设置的名称。

此命令返回已创建任务的 ID。

2. 如有必要，请使用以下命令更改任务设置（见下表）：

```
kesl-control --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

更改任务设置的示例

```
kesl-control --set-settings 101 ScanFiles=No
```

您还可以使用配置文件管理任务设置。

3. 如有必要，请配置任务计划。默认情况下，该任务手动启动。

4. 要检查任务设置的当前值，请运行以下命令：

```
kesl-control --get-settings <task ID|name>
```

5. 要运行 *恶意软件扫描* 任务，请运行以下命令：

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

命令示例

```
kesl-control --start-task 2 -W
```

6. 要停止 *恶意软件扫描* 任务，请运行以下命令：

```
kesl-control --stop-task <task ID|name> [-W]
```

## 符号

恶意软件扫描 任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| ScanFiles | 启用文件扫描。 | Yes（默认值）— 扫描文件。<br>No — 不扫描文件。 |
| ScanBootSectors | 启用引导扇区扫描。 | Yes（默认值）— 扫描引导扇区。<br>No — 不扫描引导扇区。 |
| ScanComputerMemory | 启用进程内存和内核内存扫描。 | Yes（默认值）— 扫描进程内存和内核内存。<br>No — 不扫描进程内存和内核内存。 |
| ScanStartupObjects | 启用启动对象扫描。 | Yes（默认值）— 扫描启动对象。<br>No — 不扫描启动对象。 |
| ScanArchived | 启用存档扫描（包括 SFX 自解压存档）。<br>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（默认值）— 扫描压缩文件。<br>如果将 ActionOnThreat 设置为 DisinfectDeleteIfNotPossible 并且无法清除，则应用程序将根据压缩文件类型，删除感染对象或包含威胁的整个压缩文件。<br>No — 不扫描压缩文件。 |
| ScanSfxArchived | 仅启用对self-extracting archives的扫描（包含可执行提取模块的压缩文件）。 | Yes（默认值）— 扫描自解压存档。<br>No — 不扫描自解压存档。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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 — 扫描电子邮件数据库的文件。<br>No（默认值）— 不扫描电子邮件数库的文件。 |
| ScanPlainMail | 启用对plain text电子邮件的扫描。 | Yes — 扫描纯文本电子邮件。<br>No（默认值）— 不扫描纯文本电子件。 |
| 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 至 999999<br>0 — 应用程序扫描任意大小的对象。<br>默认值：0。 |
| 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 至 9999<br>0 — 对象扫描时间不受限制。<br>默认值：0。 |
| QueueScanTasks | 如果先前启动的计划扫描仍在运行，则延迟计划扫描任务。如果当前扫描仍在运行，Kaspersky Endpoint Security 会将计划扫描任务加入队列。这有助于优化计算机上的负载。例如，扫描任务计划在 18:00 和 20:00 运行。如果 18:00 的扫描仍在运行，则计划在 20:00 运行的扫描任务将被延迟。延迟的任务将在 18:00 的任务完成后运行。 | Yes，如果当前扫描仍在运行，则将计划扫描任务加入队列。<br>No（默认值），即使当前扫描仍在行，也运行计划扫描任务。 |
| ActionOnThreat | 选择应用程序将对感染对象执行的操作。 | DisinfectDeleteIfNotPossible（清除；如果无法清除则删除）表应用程序将对象副本保存到备份区尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型对象中的威胁类型），则应用程序删除感染对象。<br>DisinfectInformIfNotPossible（清除；如果无法清除则通知）表应用程序将对象副本保存到备份区尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型对象中的威胁类型），则应用程序在日志中创建记录。<br>Inform 表示应用程序不会尝试清或删除感染对象。受感染对象的信会予以记录。<br>默认值：DisinfectDeleteIfNotPossible |
| UseExcludeMasks | 启用从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 | Yes — 从扫描中排除 ExcludeMasks.item_# 设置指定对象。<br>No（默认值）— 不从扫描中排除 ExcludeMasks.item_# 设置指定对象。 |
| 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。<br>在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。 | 默认值为未定义。<br>示例<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |
| UseExcludeThreats | 允许从扫描中排除包含 ExcludeThreats.item_# 设置所指定威胁的对象。 | Yes — 从扫描中排除包含 ExcludeThreats.item_# 设置指的威胁的对象。<br>No（默认值）：不从扫描中排除包 ExcludeThreats.item_# 设置指的威胁的对象。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。<br>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。<br>例如，您可能正在使用实用程序来获取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。<br>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。 | 该设置值区分大小写。<br>默认值为未定义。<br>示例<br>UseExcludeThreats=Yes<br>ExcludeThreats.item_0000=EICAR-Test-*<br>ExcludeThreats.item_0001=?rojan.Linux |
| UseGlobalExclusions | 针对扫描启用全局排除项。 | Yes （默认值）— 使用全局排除项。<br>No — 不使用全局排除项。 |
| UseOASExclusions | 针对扫描启用文件威胁防护排除项。 | Yes （默认值）— 使用文件威胁防护排除项。<br>No — 不使用文件威胁防护排除项。 |
| 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。<br>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 — 记录有关未感染的对象的信息。<br>No （默认值）—不记录有关未感染对象的信息。 |
| 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。<br>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 — 记录有关存档中已扫描对象信息。<br>No （默认值）— 不记录有关存档中扫描对象的信息。 |
| ReportUnprocessedObjects | 启用记录由于某种原因尚未处理的对象的有关信息。 | Yes — 记录有关未处理对象的信息。<br>No （默认值）—不记录有关未处理对象的信息。 |
| UseAnalyzer | 启用启发式分析。<br>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 （默认值）— 启用启发式分析器。<br>No — 禁用启发式分析器。 |
| HeuristicLevel | 指定启发式分析级别。<br>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 — 扫描最不全面，系统负载小。<br>Medium — 中度启发式分析级别，操作系统负载均衡。<br>Deep — 最全面的扫描，操作系统负载最大。<br>Recommended （默认值）— 推荐值 |
| UseIChecker | 启用 iChecker 技术。 | Yes （默认值）— 启用 iChecker 技术。<br>No — 禁用 iChecker 技术。 |
| DeviceNameMasks.item_# | 设备名称列表。应用程序将扫描这些设备的引导扇区。<br>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。 | AllObjects – 扫描所有设备的引导扇区。<br><device name mask> – 扫描名称指定掩码匹配的设备的引导扇区。<br>默认值： /** – 设备名称中的任意一组字符，包括 / 字符）。 |
| **[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： All objects。<br>示例<br>AreaDesc="Mail bases scan" |
| 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 （默认值）— 扫描指定的范围。<br>No — 不扫描指定的范围。 |
| 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。<br>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： * （扫描所有对象）。<br>示例<br>AreaMask.item_0000=*doc |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `Path` | 包含要扫描的对象的目录的路径。 | `<path to local directory>` – 扫描指定目录中的对象。默认情况下指定 `/` 路径 – 应用程序扫描本地文件统的所有目录。<br>`Shared:NFS` – 扫描可通过 NFS 协访问的设备文件系统资源。<br>`Shared:SMB` – 扫描可通过 Samba 议访问的设备文件系统资源。<br>`Mounted:NFS` – 扫描使用 NFS 协挂载到设备上的远程目录。<br>`Mounted:SMB` – 扫描使用 Samba 议挂载到设备上的远程目录。<br>`AllRemoteMounted` – 扫描使用 Samba 和 NFS 协议挂载到设备上的有远程目录。<br>`AllShared` – 扫描可通过 SMB 和 NFS 协议访问的所有设备文件系统源。<br>`<file system type>` – 扫描指定件系统设备的所有资源。 |
| **[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。 | 默认值为未定义。 |
| `UseScanArea` | 从扫描中排除指定的范围。 | `Yes`（默认值）– 排除指定的范围。<br>`No` – 不排除指定的范围。 |
| `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。<br>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：`*`（排除所有对象）。 |
| `Path` | 包含要排除的对象的目录的路径。 | `<path to local directory>` – 扫描中排除指定目录（包括子目录）中的对象。您可以使用掩码指定路径。<br>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，以添加以下排除项：`/.snapshots/*/snapshot/`。<br>默认情况下会指定 `/` 路径。应用程将本地文件系统的所有目录排除在扫描范围之外。<br>`Mounted:NFS` – 从扫描中排除使用 NFS 协议在设备上挂载的远程目录。<br>`Mounted:SMB` – 从扫描中排除使用 SMB 协议在设备上挂载的远程目录。<br>`AllRemoteMounted` – 在扫描中排使用 SMB 和 NFS 协议挂载在设备上的所有远程目录。<br>`<file system type>` – 从扫描中除指定文件系统设备的所有资源。<br>仅当远程目录在任务启动之前安装时，应用程序才会将其排除在扫描之外。任务启动后安装的远程目录不会被排除在扫描之外。 |

**如何从图形界面运行恶意软件扫描任务**

1. 打开应用程序图形界面的主窗口。
2. 单击“**扫描**”。
   “**扫描**”窗口将打开。
3. 要启动扫描任务，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。
4. 要停止扫描任务，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。
5. 要查看扫描任务的报告，请单击 **显示报告** 按钮。

检测到受感染对象或扫描任务完成时，将显示相应通知。

“**扫描**扫描”窗口还会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。

7 **收集计算机扫描统计信息**

您可以使用报告获取计算机的扫描统计数据。请确保扫描持续时间在可接受的范围内。检查检测到的对象，如果这些对象可信，请将它们添加到排除中。

特殊注意事项和限制

- 如果 root 用户无权访问通过 NFSv4 协议挂载到设备上的远程目录，应用程序将在扫描期间跳过该文件。
- 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”属性将不予以保留。
- 如果用户或监控服务在恶意软件扫描期间重新启动了应用程序，或者计算机在扫描期间重新启动，则扫描将停止。下次启动恶意软件扫描时，它将从头开始。

实用文章

设备可用磁盘空间不足时该怎么办

# 如何创建扫描范围

*扫描范围*是 Kaspersky Endpoint Security 为查找威胁而扫描的对象路径列表。默认情况下，应用程序会扫描受保护设备上的所有文件。如果您只需要扫描单个目录（例如，从外部源自动下载文件的目录），则可以将此目录指定为扫描范围。

Kaspersky Endpoint Security 会按照对象在对象列表中的显示顺序扫描对象。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。

在使用专用 parsecfs 文件系统（Astra Linux Special Edition）的操作系统上运行时，我们建议将此文件系统的挂载路径添加到扫描排除项中。

**如何在 Web Console 中创建扫描范围**

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击扫描任务。
   任务属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**扫描范围**”区域中单击“**添加**”。
5. 在“**文件系统，访问协议和路径**”下拉列表中，选择文件系统类型：
   - “**本地**”。无需网络连接即可访问的硬盘目录。
   - “**挂载**”。已挂载的远程或本地目录。
   - “**共享**”。可通过 Samba (SMB) 或 NFS 协议访问的计算机目录。
   - “**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。
   - “**全部共享**”。通过 Samba 和 NFS 协议访问的所有计算机目录。
6. 对于 **挂载** 和 **共享** 文件系统类型，请选择访问协议：
   - **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**。设备上类型不是 NFS 或 Samba 的文件系统资源（例如，`ext4` 或 `parsecfs`）。
7. 指定目录路径或路径掩码。
8. 如有必要，请指定对象名称的掩码（例如，`*.txt` 或 `report_*`）。用逗号分隔各个掩码。
9. 单击“**添加**”。
   新对象已添加到扫描范围。您可以将对象从扫描范围中排除，而不必将其从对象列表中删除。为此，请关闭对象旁边的切换开关。
10. 如有必要，启用或禁用扫描范围内的预定义对象：
    - **内核内存**。**运行中进程的内存**。
    - “**正在运行的进程和启动对象**”。
    - “**磁盘引导扇区**”。

- “**所有硬盘驱动器**”。
- “**所有网络驱动器**”。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中创建扫描范围**

1. 运行以下命令：

```
kesl-control --set-settings 2 --add-path <path>
```

任务设置中将添加一个新的 `[ScanScope.item_#]` 部分。应用程序将扫描指定目录中的对象。

示例

```
kesl-control --set-settings 2 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=All objects
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

2. 如果要将已挂载的特定类型（NFS 或 Samba 除外）文件系统中的资源（例如， `parsecfs`）纳入扫描范围，请在 `Path` 参数中指定文件系统类型：Path=<文件系统类型>

应用程序将扫描指定设备文件系统的所有资源。

示例

```
kesl-control --set-settings 2 ScanScope.item_0002.UseScanArea=Yes ScanScope.item_0002.Path=parsecfs
```

以下扫描范围设置将添加到任务中：

```
[ScanScope.item_0002]
AreaDesc=All objects
UseScanArea=Yes
Path=parsecfs
AreaMask.item_0000=*
```

3. 要检查任务设置的当前值，请运行以下命令：

```
kesl-control --get-settings 2
```

# 如何配置扫描计划

运行任务 *恶意软件扫描* 可能会增加计算机上的资源利用率。为了最大限度地减少 Kaspersky Endpoint Security 对用户计算机在使用中性能的影响，您可以将该任务计划在最合适的时间运行。

例如，如果贵公司员工按固定时间表工作，您可以配置扫描在夜间或周末运行。如果由于任何原因无法运行扫描（例如，当时计算机处于关机状态），则可以配置跳过的任务，使其在条件允许时尽快自动运行。

如果无法确定运行计算机扫描的最佳计划，您不仅可以在特定时间运行 *恶意软件扫描* 任务，还可以根据特定条件运行该任务，例如启动应用程序、将更新下载到存储库、检测到病毒攻击或完成其他任务时。您还可以使用 Wake-on-LAN 功能，在任务开始前不久启动已关机的计算机。您可以仅为 Kaspersky Security Center 的“*恶意软件扫描*”任务配置使用“Wake-on-LAN”运行扫描。无法在应用程序界面中启用“Wake-on-LAN”以扫描计算机。

### 如何在 Web Console 中运行恶意软件扫描任务

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击扫描任务。
   任务属性窗口将打开。
3. 在任务属性窗口中，选择“**计划**”选项卡。
4. 配置扫描任务计划。
5. 根据选定的频率，配置指定任务运行计划的高级设置（参见下表）。
6. 保存更改。

扫描计划设置

| 设置 | 描述 |
| --- | --- |
| **启动任务** | “**手动**”。您可以在方便时手动启动扫描的运行模式。<br>根据计划。在该扫描任务运行模式下，应用程序将按照您创建的计划启动扫描任务。如果选择该扫描任务运行模式，您也可以手动启动扫描任务。 |
| **运行错过的任务** | 如果选中该复选框，Kaspersky Endpoint Security 将在可能的情况下尽快启动已忽略的任务。任务在某些情况下可能被略过，例如，计算机在启动计划任务时处于关闭状态。当应用程序有机会执行略过的任务时，它会在一定的时间间隔内随机运行任务，以分配计算机上的负载。<br>如果清除该复选框，Kaspersky Endpoint Security 不会运行已略过的任务。它将按照当前计划运行下一次任务。 |
| **使用任务启动自动随机延迟** | 如果选中该复选框，则任务不会严格按计划运行，而是在一定的时间间隔内随机运行，即任务的开始时间是分散的。随机开始时间有助于避免任务按计划运行时大量计算机同时访问管理服务器。<br>随机开始时间的范围在创建任务时自动计算，具体取决于分配任务的计算机数量。随后，任务始终在其计算的开始时间运行。然而，无论何时修改任务设置或手动运行任务，计算的开始时间都会更改。<br>如果清除该复选框，则任务将完全在计划时间运行。 |
| **使用任务启动自动随机延迟间隔** | 如果选中此复选框，则会在一定时间范围内的随机时间在计算机上运行任务。随机开始时间有助于避免任务按计划运行时大量计算机同时访问管理服务器。<br>如果清除该复选框，则任务将完全在计划时间运行。 |
| **使用 Wake-On-LAN 功能在任务启动之前开启设备** | 如果选中该复选框，则在运行任务之前，计算机的操作系统将有一个指定的提前期来完成启动。默认提前期为 5 分钟。<br>如果要在所有计算机（包括已关机的计算机）上运行任务，请选中该复选框。 |
| **任务完成后关闭设备** | 如果选中此复选框，计算机将在任务完成后关机。例如，您可以启用此功能在星期五下班后扫描计算机。当任务完成后，应用程序会在周末关闭计算机。 |
| **如果任务运行超过该时间则停止** | 限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。 |

### 如何在命令行中计划恶意软件扫描任务

要在特定时间运行一次该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=Once StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>'
```

要每月运行该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='<hh>:<mm>:<ss>;<day of the month>'
```

要在一周中的特定某一天运行该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='<hh>:<mm>:<ss>;<day of the week>'
```

要按天以固定间隔运行该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=Daily StartTime='<hh>:<mm>:<ss>;<interval between runs (in days)>'
```

要从特定日期开始按小时以固定间隔运行该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>;
<interval between runs (in hours)>'
```

要从特定日期开始按固定间隔运行该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=Minutely StartTime='<hh>:<mm>:<ss>;<interval between runs (in minutes)>'
```

要在应用程序启动后立即运行该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=PS
```

要在数据库更新后立即运行该任务，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=BR
```

要禁用该任务的计划，请运行以下命令：

```
kesl-control --set-schedule 2 RuleType=Manual
```

要管理其他任务计划设置，请运行以下命令：

```
kesl-control --set-schedule 2 RandomInterval=<time interval (minutes)> RunMissedStartRules=<Yes|No>
UseWorkingTimeout=<Yes|No> WorkingTimeout=<maximum task completion time (minutes)> QueueScanTasks=<Yes|No>
```

要检查任务设置的当前值，请运行以下命令：

```
kesl-control --get-schedule 2
```

## 符号

任务启动计划设置

| 设置 | 描述 |
| --- | --- |
| RuleType | 任务启动计划。<br>• Once：运行一次任务。<br>• Monthly：每月在指定的日期和时间运行任务。<br>• Weekly：每周在指定的日期和时间运行任务。<br>• Daily：按照指定的天数间隔定期运行任务。<br>• 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。<br>• Minutely：从指定的时间开始，按照指定的分钟间隔定期运行任务。<br>• Manual – 手动启动任务。<br>• PS – 启动应用程序后启动任务。<br>• BR – 在应用程序数据库更新后启动任务。 |

| 设置 | 描述 |
| --- | --- |
| StartTime | 任务开始日期和时间。此设置的格式取决于 RuleType。<br>可能的值：<br>• <year>:1970 至 2099<br>• <month>:JAN，FEB，MAR，APR，MAY，JUN，JUL，AUG，SEP，OCT，NOV，DEC。<br>• <day of the month>:1 至 31<br>• <day of the week>:Mon，Tue，Wed，Thu，Fri，Sat，Sun。<br>• <hh>:0 至 23<br>• <mm>:0 至 59<br>• <ss>:0 至 59<br>• <interval between runs (in days)>:0 至 364<br>• <interval between runs (in hours)>:0 至 23<br>• <interval between runs (in minutes)>:0 至 59 |
| RandomInterval | 在一定时间间隔内（从 0 到指定值），随机在计算机上运行该任务。这样可以避免多个任务同时启动。<br>默认值：99 分钟。<br>可能值：0 – 999。 |
| RunMissedStartRules | 在应用程序启动后运行漏掉的任务。<br>• Yes（默认值）表示已启用运行错过的任务。如果在计划任务运行时应用程序停止运行或计算机断电，Kaspersky Endpoint Security 会在应用程序启动后立即启动该任务。这有助于确保绝不会错过关键任务。<br>• No 表示已禁用运行错过的任务。如果在计划任务运行时应用程序停止运行或计算机断电，应用程序将跳过该任务。这有助于避免在启动应用程序时产生额外负载。 |
| UseWorkingTimeout | 达到 WorkingTimeout 设置指定的最大任务执行时间时停止任务。即使未完成，任务也会停止。下次任务启动将按照计划进行。<br>• Yes – 当达到最大任务执行时间时停止任务。<br>• No（默认值）– 达到最大任务执行时间时不停止任务。 |
| WorkingTimeout | 如果 UseWorkingTimeout=Yes，则应用程序停止执行任务后的最大任务执行时间（以分钟为单位）。<br>默认值：120 分钟。<br>可能值：1 – 999。 |

每 10 小时运行一次扫描任务的示例

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='2030/May/28 12:00:00;10'
```

每月 15 日运行扫描任务的示例

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='12:00:00;15'
```

每周二运行任务的示例

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='12:00:00;Tue'
```

# 如何扫描单个文件或目录

Kaspersky Endpoint Security 允许您使用命令行运行单个文件扫描来查找病毒和其他恶意软件。例如，您可以有选择地扫描默认情况下禁用文件威胁防护扫描的归档文件。

默认情况下，应用程序使用卡巴斯基专家推荐的*Scan_File (ID: 3)*任务设置扫描文件。默认设置提供建议的保护级别和最佳资源使用。默认情况下，应用程序会将受感染对象的副本保存到备份区，并尝试清除该对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。您可以选择其他检测到威胁后的操作，并管理其他任务设置。

如何在命令行中开始扫描单个文件或目录

```
kesl-control --scan-file <path to the file or directory>
```

因此，Kaspersky Endpoint Security 会生成以下格式的报告：

已扫描对象：N

检测到的对象总数：N

受感染对象和其它对象：N

已清除对象：N

已移动至备份区：N

已删除对象：N

未清除对象：N

扫描错误：N

受密码保护的对象：N

已跳过的对象：N

由 Cloud Sandbox 检测：N

# 如何优化自定义扫描任务

要优化 自定义扫描，您可以限制同时启动多个任务。如果用户尝试同时运行过多的自定义扫描任务，应用程序将不会运行超出限制的任务。这样，您可以控制客户端设备的资源利用率，并且例如避免服务器负载过高。默认情况下，自定义扫描任务的数量限制设置为 100。

Kaspersky Endpoint Security 仅对非特权用户限制任务。具有 root 权限的用户可以不受限制地运行自定义扫描任务。

您可以在命令行中使用 常规应用程序设置配置自定义扫描任务限制。您无法在管理控制台或 Web Console 中配置任务限制。

如何在命令行中优化自定义扫描任务

```
kesl-control --set-app-settings LimitNumberOfScanFileTasks=<number of tasks>
```

# 关键区域扫描

通过特殊扫描任务，您可以仅扫描计算机的关键区域：*关键区域扫描*。"*关键区域扫描*"会快速扫描计算机中最常发现恶意软件的区域。此任务的扫描范围包括引导扇区、启动对象、内核内存和正在运行的进程。

成功入侵计算机关键区域的恶意软件可以在逃避检测的同时执行其功能。默认情况下，应用程序使用卡巴斯基专家推荐的设置运行该任务。默认设置提供建议的保护级别和最佳资源使用。

卡巴斯基专家不建议更改“*关键区域扫描*”任务的默认设置。

如果 root 用户无权访问通过 NFSv4 协议挂载到设备上的远程目录，应用程序将在扫描期间跳过该文件。

管理服务器初始配置向导会自动创建“*关键区域扫描*”任务。要创建“*关键区域扫描*”任务，请在运行该向导时安装 Kaspersky Endpoint Security for Linux 管理插件。如有必要，您可以创建“*关键区域扫描*”类型的用户任务。

**如何在 Web Console 中运行关键区域扫描**

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
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“**Kaspersky Endpoint Security for Linux**”。
   b. 在“**任务类型**”下拉列表中，选择“**关键区域扫描**”。
   c. 在“**任务名称**”字段中，输入简要说明，例如“*计算机感染后的关键区域扫描*”。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。继续下一步。
5. 结束向导。
6. 单击扫描任务。
   任务属性窗口将打开。
7. 选择**应用程序设置**选项卡。
8. 配置扫描任务（参见下表）。
9. 如有必要，请在“**计划**”选项卡上配置任务启动计划设置。
10. 保存更改。
11. 运行扫描任务。

关键区域扫描 任务设置

| 设置 | 描述 |
| --- | --- |
| **扫描范围** | 包含任务扫描的范围的表。默认情况下，扫描范围包括本地文件系统的所有目录、内核内存、正在运行的进程的内存、启动对象和引导扇区。 |
| **检测到威胁后的操作** | • **清除；如果清除失败则删除**（默认）。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>• "**清除；如果清除失败则通知**"。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>• "**通知**"。如果选择此操作，应用程序会在日志中创建关于感染对象的记录。 |
| **扫描压缩包** | 如果启用此选项，应用程序将扫描压缩文件。<br>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。<br>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。您可以通过指定"**跳过扫描时间超过以下值的文件(秒)**"和"**不扫描大小大于该值(MB)的文件**"设置来缩短压缩文件扫描时间。<br>默认情况下已禁用该选项。 |
| **扫描分发包和自解压存档文件** | 如果启用此选项，应用程序将扫描自解压压缩文件。自解压缩文件是包含可执行解压模块的压缩文件。<br>默认情况下已禁用该选项。 |
| **扫描电子邮件格式文件** | 扫描纯文本电子邮件。<br>默认情况下，该功能处于禁用状态。 |
| **扫描电子邮件数据库** | 如果启用此选项，应用程序将扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件应用程序的邮件数据库。<br>默认情况下，该功能处于禁用状态。 |
| **不扫描大小大于该值(MB)的文件** | 您可以指定可扫描文件的最大大小，单位为兆字节。<br>可用值：0-9999。如果该值设置为 0，则应用程序将扫描任何大小的文件。<br>默认情况下，该功能处于禁用状态。 |
| **跳过扫描时间超过以下值的文件(秒)** | 您可以指定文件的最长扫描时间，单位为秒。在指定时间后，应用程序将停止扫描该文件。<br>可用值：0-9999。如果该值设置为 0，则扫描时间不受限制。<br>默认情况下，该功能处于禁用状态。 |
| **不同时运行多个扫描任务** | 如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。<br>默认情况下，该功能处于禁用状态。 |
| **使用 iChecker 技术** | 如果启用此选项，应用程序将仅扫描新增文件以及上次扫描后修改过的文件。<br>如果禁用此选项，应用程序将扫描文件，而不考虑文件的创建或修改日期。<br>默认情况下已禁用该选项。 |

## 如何在命令行运行关键区域扫描任务

1. 如有必要，请配置任务设置（请参见下表）。

```
kesl-control --set-settings 4 <setting name>=<setting value>
```

2. 如有必要，请配置任务计划。

3. 要检查任务设置的当前值，请运行以下命令：

```
kesl-control --get-settings 4 [--json]
```

其中 `--json` 表示以 JSON 格式输出数据。

4. 要运行该任务，请运行以下命令：

```
kesl-control --start-task 4 [-W] [--progress]
```

其中：

- `[-W]` 启用与该任务相关的当前事件的输出。
- `[--progress]`：显示任务进度。

如有必要，您可以创建用户任务，类型为 *关键区域扫描*。

关键区域扫描 任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `ScanFiles` | 启用文件扫描。 | `Yes` — 扫描文件。<br>`No`（默认值）— 不扫描文件。 |
| `ScanBootSectors` | 启用引导扇区扫描。 | `Yes`（默认值）— 扫描引导扇区。<br>`No` — 不扫描引导扇区。 |
| `ScanComputerMemory` | 启用进程内存和内核内存扫描。 | `Yes`（默认值）— 扫描进程内存和内核内存。<br>`No` — 不扫描进程内存和内核内存。 |
| `ScanStartupObjects` | 启用启动对象扫描。 | `Yes`（默认值）— 扫描启动对象。<br>`No` — 不扫描启动对象。 |
| `ScanArchived` | 启用存档扫描（包括 SFX 自解压存档）。<br>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`（默认值）— 扫描压缩文件。<br>如果将 `ActionOnThreat` 设置为 `DisinfectDeleteIfNotPossible`，并且无法清除，则应用程序将根据压缩文件类型，删除感染对象或包含威胁的整个压缩文件。<br>`No` — 不扫描压缩文件。 |
| `ScanSfxArchived` | 仅启用对self-extracting archives的扫描（包含可执行提取模块的压缩文件）。 | `Yes`（默认值）— 扫描自解压存档。<br>`No` — 不扫描自解压存档。 |
| `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` — 扫描电子邮件数据库的文件。<br>`No`（默认值）— 不扫描电子邮件数据库的文件。 |
| `ScanPlainMail` | 启用对plain text电子邮件的扫描。 | `Yes` — 扫描纯文本电子邮件。<br>`No`（默认值）— 不扫描纯文本电子邮件。 |
| `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 至 999999<br>0 — 应用程序扫描任意大小的对象。<br>默认值：0。 |
| `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 至 9999<br>0 — 对象扫描时间不受限制。<br>默认值：0。 |
| `QueueScanTasks` | 如果先前启动的计划扫描仍在运行，则延迟计划扫描任务。如果当前扫描仍在运行，Kaspersky Endpoint Security 会将计划扫描任务加入队列。这有助于优化计算机上的负载。例如，扫描任务计划在 18:00 和 20:00 运行。如果 18:00 的扫描仍在运行，则计划在 20:00 运行的扫描任务将被延迟。延迟的任务将在 18:00 的任务完成后运行。 | `Yes`，如果当前扫描仍在运行，则将计划扫描任务加入队列。<br>`No`（默认值），即使当前扫描仍在运行，也运行计划扫描任务。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ActionOnThreat | 选择应用程序将对感染对象执行的操作。 | DisinfectDeleteIfNotPossible（清除；如果无法清除则删除）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>DisinfectInformIfNotPossible（清除；如果无法清除则通知）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>Inform 表示应用程序不会尝试清除或删除感染对象。受感染对象的信息会予以记录。<br>默认值：DisinfectDeleteIfNotPossible。 |
| UseExcludeMasks | 启用从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 | Yes — 从扫描中排除 ExcludeMasks.item_# 设置指定的对象。<br>No（默认值）— 不从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 |
| 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。<br>在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。 | 默认值为未定义。<br>示例<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |
| UseExcludeThreats | 允许从扫描中排除包含 ExcludeThreats.item_# 设置所指定威胁的对象。 | Yes — 从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。<br>No（默认值）：不从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。 |
| 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。<br>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。<br>例如，您可能正在使用实用程序来获取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。<br>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。 | 该设置值区分大小写。<br>默认值为未定义。<br>示例<br>UseExcludeThreats=Yes<br>ExcludeThreats.item_0000=EICAR-Test-*<br>ExcludeThreats.item_0001=?rojan.Linux |
| UseGlobalExclusions | 针对扫描启用全局排除项。 | Yes（默认值）— 使用全局排除项。<br>No — 不使用全局排除项。 |
| UseOASExclusions | 针对扫描启用文件威胁防护排除项。 | Yes（默认值）— 使用文件威胁防护排除项。<br>No — 不使用文件威胁防护排除项。 |
| 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。<br>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 — 记录有关未感染的对象的信息。<br>No（默认值）—不记录有关未感染的对象的信息。 |
| 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。<br>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 — 记录有关存档中已扫描对象的信息。<br>No（默认值）— 不记录有关存档中已扫描对象的信息。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ReportUnprocessedObjects | 启用记录由于某种原因尚未处理的对象的有关信息。 | Yes — 记录有关未处理对象的信息。<br>No（默认值）—不记录有关未处理对象的信息。 |
| UseAnalyzer | 启用启发式分析。<br>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（默认值）— 启用启发式分析器。<br>No — 禁用启发式分析器。 |
| HeuristicLevel | 指定启发式分析级别。<br>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 — 扫描最不全面，系统负载最小。<br>Medium — 中度启发式分析级别，操作系统负载均衡。<br>Deep — 最全面的扫描，操作系统负载最大。<br>Recommended（默认值）— 推荐值。 |
| UseIChecker | 启用 iChecker 技术。 | Yes（默认值）— 启用 iChecker 技术。<br>No — 禁用 iChecker 技术。 |
| DeviceNameMasks.item_# | 设备名称列表。应用程序将扫描这些设备的引导扇区。<br>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。 | AllObjects – 扫描所有设备的引导扇区。<br><device name mask> – 扫描名称与指定掩码匹配的设备的引导扇区。<br>默认值：/** – 设备名称中的任意一组字符，包括 / 字符）。 |
| [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：All objects。<br>示例<br>AreaDesc="Mail bases scan" |
| 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（默认值）— 扫描指定的范围。<br>No — 不扫描指定的范围。 |
| 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。<br>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：*（扫描所有对象）。<br>示例<br>AreaMask.item_<item number>=*doc |
| Path | 包含要扫描的对象的目录的路径。 | <path to local directory> – 扫描指定目录中的对象。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。<br>Shared:NFS — 扫描可通过 NFS 协议访问的设备文件系统资源。<br>Shared:SMB – 扫描可通过 Samba 协议访问的设备文件系统资源。<br>Mounted:NFS — 扫描使用 NFS 协议挂载到设备上的远程目录。<br>Mounted:SMB — 扫描使用 Samba 协议挂载到设备上的远程目录。<br>AllRemoteMounted — 扫描使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。<br>AllShared — 扫描可通过 SMB 和 NFS 协议访问的所有设备文件系统资源。<br><file system type> – 扫描指定文件系统设备的所有资源。 |
| [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。 | 默认值为未定义。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseScanArea | 从扫描中排除指定的范围。 | Yes（默认值）— 排除指定的范围。<br>No — 不排除指定的范围。 |
| 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。<br>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：*（排除所有对象）。 |
| Path | 包含要排除的对象的目录的路径。 | <path to local directory> – 从扫描中排除指定目录（包括子目录）中的对象。您可以使用掩码指定路径。<br>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，可以添加以下排除项：/.snapshots/*/snapshot/。<br>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。<br>Mounted:NFS — 从扫描中排除使用 NFS 协议在设备上挂载的远程目录。<br>Mounted:SMB — 从扫描中排除使用 SMB 协议在设备上挂载的远程目录。<br>AllRemoteMounted — 在扫描中排除使用 SMB 和 NFS 协议挂载在设备上的所有远程目录。<br><file system type> – 从扫描中排除指定文件系统设备的所有资源。<br>仅当远程目录在任务启动之前安装时，应用程序才会将其排除在扫描之外。任务启动后安装的远程目录不会被排除在扫描之外。 |

实用文章

### 如何指定掩码

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。

# 容器扫描

Kaspersky Endpoint Security 可以实时或按需扫描容器和镜像中是否存在恶意软件。

要使用"容器扫描"功能，需要包含此功能的授权许可。

该组件不适用于配备 Elbrus CPU 的设备。

## 容器监控

*容器监控*组件实时扫描正在运行的容器和命名空间。容器监控组件默认处于启用状态。

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应用文件威胁防护设置。

建议的容器监控配置方案包括以下步骤：

1. **配置应用程序与容器管理工具的集成**

   应用程序支持与Docker 容器管理系统、CRI-O 环境以及 Podman 和 runc 工具集成。

2. **创建保护范围**

   确定要扫描容器和命名空间的设备。

3. **在容器监控设置中，选择"跳过容器"操作**

   在容器中检测到受感染对象时，Kaspersky Endpoint Security 可以立即停止该容器、不执行任何操作，或者在无法清除对象或消除威胁时停止该容器。选择**跳过容器**操作来测试组件。检测到受感染对象时，应用程序不会对容器执行任何操作，但会记录有关检测到的威胁的信息。

4. **收集容器监控统计信息**

   您可以使用报告获取容器监控统计信息。

5. **选择检测到受感染对象时要对容器执行的操作。**

   选择应用程序在检测到受感染对象时对容器执行的操作。

## 容器按需扫描

应用程序可以按需扫描容器和镜像中的病毒及其他恶意软件。此操作使用预定义的*容器扫描 (Container_Scan)*任务执行。您可以通过命令行、Web Console 或管理控制台配置预定义任务，或创建用于扫描容器的用户任务。

应用程序可以同时运行多个"容器扫描"任务。

建议的容器扫描配置方案包括以下步骤：

1. **配置应用程序与容器管理工具的集成**

   应用程序支持与Docker 容器管理系统、CRI-O 环境以及 Podman 和 runc 工具集成。

2. **设置扫描范围**

   默认情况下，应用程序会扫描受保护设备上的所有容器。如果您只需扫描特定容器，可以指定其名称或名称掩码。

3. **在容器扫描设置中，选择"跳过容器"和"跳过镜像"操作**

   在容器中检测到受感染对象时，Kaspersky Endpoint Security 可以立即停止该容器、不执行任何操作，或者在无法清除对象或消除威胁时停止该容器。如果在容器镜像中检测到受感染对象，Kaspersky Endpoint Security 可以删除容器镜像，或不对容器镜像执行任何操作。选择**跳过容器**和**跳过镜像**操作来测试任务。检测到受感染对象时，应用程序不会对容器及其镜像执行任何操作，但会记录有关检测到的威胁的信息。

4. **收集容器扫描统计信息**

   您可以使用报告获取容器扫描统计信息。

5. **优化应用程序性能**

   分析收集到的信息后，优化应用程序性能：

   - 添加全局排除项
   - 添加扫描排除项
   - 优化容器扫描

6. **选择检测到受感染对象时要对容器及其镜像执行的操作**

   选择操作，即应用程序在检测到受感染对象时对容器及其镜像执行的操作。

## 自定义容器扫描

*自定义容器扫描*任务允许配置并存储在使用以下命令扫描指定容器和镜像时所用的设置：

```
kesl-control --scan-container
```

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。

该命令会创建并运行用于扫描容器和镜像的临时任务，该任务会在完成后自动删除。在这种情况下，扫描结果将输出到控制台。

特殊注意事项和限制

- 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“任务可用但未运行”，而在 Kaspersky Security Center 中则显示为“已停止”。
- 仅当应用程序的授权许可包含此功能时，才能选择容器监控操作。

# 如何配置与容器管理工具的集成

应用程序支持与 Docker 容器管理系统、CRI-O 环境以及 Podman 和 runc 工具集成。您可以配置与这些容器管理工具的集成。

**如何在 Web Console 中配置与容器管理工具的集成**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到 **常规设置** → **容器扫描设置**。
5. 确保容器监控组件的切换开关处于 **命名空间和容器监控已启用** 位置。
6. 在“**容器扫描设置**”块中单击“**配置**”按钮。
7. 此时将打开 **扫描设置** 窗口；在该窗口中，选中受保护设备的操作系统中已安装并使用的容器管理工具旁边的复选框，然后根据需要管理设置：
   - **使用 Docker** 复选框用于启用 Docker 容器管理系统。默认情况下已选定该选框。
     - **Docker 套接字路径** 是用于指定 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** 复选框用于启用 CRI-O 环境。默认情况下已选定该选框。
     - **文件路径** 是用于指定 CRI-O 配置文件路径的输入字段。默认值：/etc/crio/crio.conf。
   - **使用 Podman** 复选框用于启用 Podman 实用程序。默认情况下已选定该选框。
     - **文件路径** 是用于指定 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** 是用于指定容器存储根目录路径的输入字段。

- **使用 runc** 复选框用于启用 runc 实用程序。默认情况下已选定该选框。
  - **文件路径** 是用于指定 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** 是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。

8. 保存更改。

**如何在命令行中配置与容器管理工具的集成**

在命令行中，您可以使用常规应用程序设置中的 `NamespaceMonitoring=<Yes|No>` 设置启用或禁用对命名空间和容器的实时监控。

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选项来编辑设置 `NamespaceMonitoring` 的值。

使用命令行选项启用对命名空间和容器的监控

```
kesl-control --set-app-settings NamespaceMonitoring=Yes
```

实时扫描命名空间和容器时，会应用 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编辑所有容器扫描设置。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 `<setting name>=<setting value>` 格式的命令行选项管理各项设置。您可以使用用于输出容器扫描设置的命令获取设置的当前值。

将容器扫描设置的当前值输出到控制台

```
kesl-control --get-container-settings [--json]
```

其中指定 `--json` 后，将以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

将容器扫描设置的当前值输出到文件

```
kesl-control --get-container-settings --file <path to configuration file> [--json]
```

其中：

- `--file <path to configuration file>` 是要保存容器扫描设置的文件的路径。如果您指定文件名而不指定其路径，则将在当前目录中创建文件。如果指定路径中已存在具有指定名称的文件，则它将被覆盖。如果在磁盘上找不到指定目录，则不会创建文件。
- 指定 `--json`，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

*要使用配置文件修改容器扫描设置的值：*

1. 如上所述，将容器扫描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. 运行以下命令：

```
kesl-control --set-container-settings --file <path to configuration file> [--json]
```

其中：

- `--file <path to configuration file>` 是包含容器扫描设置的配置文件的完整路径。
- 如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果不指定 `--json`选项，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。

文件中指定的所有容器扫描设置的值都将导入到应用程序中。

使用命令行选项修改容器扫描设置的值

```
kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

其中，`<setting name>=<setting value>` 是容器扫描设置的名称和值。

指定的容器扫描设置的值已修改。

# 如何为容器和镜像创建按需扫描范围

扫描范围

*扫描范围* 是 Kaspersky Endpoint Security 在运行 *容器扫描* 任务时扫描的容器名称列表。

默认情况下，*容器扫描* 任务会扫描受保护设备上的所有容器。如果您只需扫描特定容器，可以指定其名称或名称掩码。

**如何在 Web Console 中创建扫描范围**

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 在任务列表中，选择 Kaspersky Endpoint Security 容器扫描任务，然后单击该任务的名称。
   任务属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在 **高级扫描设置** → **容器扫描设置** 下，在 **名称掩码** 字段中，输入要扫描的容器的名称或名称掩码。默认情况下，会扫描所有容器。
5. 在 **高级扫描设置** → **镜像扫描设置** 下，在 **名称掩码** 字段中，输入要扫描的容器镜像的名称或名称掩码。默认情况下，会扫描所有镜像。
6. 保存更改。

**如何在命令行中创建扫描范围**

1. 使用以下命令配置扫描范围：

```
kesl-control --set-settings <task ID|name> ScanContainers=Yes ContainerNameMask=<container name or mask>
ScanImages=Yes ImageNameMask=<image name or mask>
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `<container name or mask>` 是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 `*` 符号。默认情况下，会扫描所有容器。
- `<image name or mask>` 是要扫描的镜像的名称或名称掩码。掩码以命令 Shell 格式指定。您可以使用 `?` 和 `*` 符号。默认情况下，会扫描所有镜像。

2. 您还可以使用配置文件配置扫描范围：

   a. 运行以下命令，将任务设置输出到配置文件：

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. 打开配置文件进行编辑。

   c. 将以下设置添加到文件中：

   - `ScanContainers=Yes` 启用对指定容器的扫描。
   - `ContainerNameMask=<container name or mask>` 是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 `*` 符号。默认情况下，会扫描所有容器。
   - `ScanImages=Yes` 启用对指定镜像的扫描。
   - `ImageNameMask=<image name or mask>` 是要扫描的镜像的名称或名称掩码。掩码以命令 Shell 格式指定。您可以使用 `?` 和 `*` 符号。默认情况下，会扫描所有镜像。

   对名为 my_container 的容器执行容器扫描的示例

   ```
   ContainerNameMask=my_container
   ```

   扫描名称以 my_container 开头的所有容器的示例

   ```
   ContainerNameMask=my_container*
   ```

   对所有符合以下条件的容器执行容器扫描的示例：名称以 my_ 开头，后接任意五个字符，再接 _container，并以任意字符序列结尾

   ```
   ContainerNameMask=my_?????_container*
   ```

   对名称为“my_image”且标签为“latest”的镜像执行镜像扫描的示例

   ```
   ImageNameMask=my_image:latest
   ```

   对名称以 my_image_ 开头且带有任意标签的所有镜像执行镜像扫描的示例

   ```
   ImageNameMask=my_image*
   ```

   d. 将更改保存在配置文件中。

e. 使用以下命令，将设置从配置文件导入到任务中：

```
kesl- <task ID|name> --file <path> [--json]
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `--file <path>` 是配置文件的完整路径，您希望从该配置文件导入任务设置。
- 如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果未指定 --json 选项，应用程序将尝试从 INI 文件导入。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。

扫描排除项

"*扫描排除项*"是一组条件，必须满足这些条件，Kaspersky Endpoint Security 才不会扫描特定对象是否存在病毒和其他威胁。扫描排除项可让您使用入侵者可以用来破坏计算机或用户数据的合法应用程序。此类应用程序不一定具有恶意目的，但可能会被黑客利用。有关入侵者可以用来破坏计算机或用户数据的合法应用程序的详细信息，请访问 卡巴斯基百科全书网站。

您还可以将某些受信任的目录从扫描范围中排除，以优化应用程序性能。

可以使用以下方法从扫描中排除对象：

- **按掩码筛选的排除项**。输入带掩码的文件名。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

  使用掩码：

  - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和目录路径中的文件和目录名称的分隔符）。例如，掩码 `/dir/*/*.txt` 将包括位于 dir 目录内各目录中（但不包括这些目录的子目录中）的所有 TXT 扩展名文件的路径。
  - 两个连续的 `*` 字符在文件或目录名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和目录路径中的文件和目录名称的分隔符）。例如，掩码 `/dir/**/*.txt` 将包括位于 dir 目录内嵌套目录中的所有 TXT 扩展名文件的路径，但不包括 dir 目录本身。
  - `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和目录路径中的文件和目录名称的分隔符）。例如，`/dir/???.txt` 掩码将包括位于 dir 目录中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

- **按威胁名称筛选的排除项** 根据 卡巴斯基百科全书的分类输入对象类型名称（例如，`Email-Worm`、`Rootkit` 或 `RemoteAdmin`）。您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，应用程序从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

Kaspersky Endpoint Security 还允许从扫描中排除某些格式的文件：压缩文件、电子邮件数据库、文本文件、数据库日志文件。

### 如何在 Web Console 中添加扫描排除项

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 在任务列表中，选择 Kaspersky Endpoint Security 容器扫描任务，然后单击该任务的名称。
   任务属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**排除范围**区域。
5. 如有必要，按掩码添加排除项：
   a. 在“**按掩码的排除项**”块中单击“**添加**”按钮。
   b. 这将打开一个窗口；在该窗口中，指定希望 Kaspersky Endpoint Security 从扫描中排除的文件名称模板。
   c. 单击“**添加**”。
   排除项将添加到列表中。
6. 如有必要，按威胁名称添加排除项：
   a. 在“**按威胁名称筛选的排除项**”块中单击“**添加**”按钮。
   b. 这将打开一个窗口；在该窗口中，指定威胁名称模板。应用程序不会阻止指定的威胁。

   例如，如果您使用某个工具扫描网络，请将其完整威胁名称添加到要从扫描中排除的威胁列表中。
   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。
7. 如有必要，您可以导入或导出每个列表的排除项：
   - 要导出排除项列表，请单击 **导出** 按钮。
     Kaspersky Endpoint Security 会将 export.json 文件保存到标准下载文件夹中。
   - 要导入排除项列表：
     a. 单击“**导入**”。
     b. 选择要从中导入排除范围的 JSON 文件。
     c. 打开文件。
     d. 选择导入方法：将排除项添加到现有列表，或替换排除项列表。
     e. 保存更改。
     JSON 文件中的规则会显示在列表中。
8. 保存更改。

### 如何在命令行中添加扫描排除项

1. 使用以下命令添加排除范围：

```
kesl-control --set-settings <任务 ID|名称> --add-exclusion <路径>
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `--add-exclusion <path>` 添加要从扫描中排除的对象所在目录的路径。

任务设置中将添加一个新的 `[ExcludedFromScanScope.item_#]` 部分。应用程序会从扫描中排除 `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。

2. 您还可以使用配置文件添加排除范围：

   a. 通过运行以下命令将任务设置输出到配置文件：

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. 打开配置文件进行编辑。

   c. 向文件添加一个 `[ExcludedFromScanScope.item_#]` 部分，并包含以下设置：

   - `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` 是包含要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=*
     ```

   d. 您可以指定多个 `[ExcludedFromScanScope.item_#]` 部分。

   应用程序将按索引升序处理范围。

   e. 将更改保存在配置文件中。

f. 使用以下命令，将设置从配置文件导入到任务中：

```
kesl-control --set-settings <task ID|name> --file <path>
```

3. 如有必要，您可以通过运行以下命令删除排除范围：

```
kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `--del-exclusion <path>` 删除包含要从扫描中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。

# 如何优化容器扫描

配置文件扫描以优化任务的性能。这有助于降低受保护设备的 CPU 使用率。您可以限制压缩文件扫描，设置可扫描对象的最大大小，以及设置对象扫描的最长持续时间。Kaspersky Endpoint Security 还允许从扫描中排除某些格式的文件：压缩文件、电子邮件数据库、文本文件和纯文本电子邮件。

### 如何在 Web Console 中配置文件扫描

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 在任务列表中，选择 Kaspersky Endpoint Security 容器扫描任务，然后单击该任务的名称。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在 **扫描设置**下，配置文件扫描：

   - “**扫描压缩包**”。这包括扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他类型的压缩文件。应用程序不仅可通过扩展名识别文件，还可通过格式识别文件。在扫描压缩文件时，应用程序会递归解包。这样就可以检测嵌套压缩文件（压缩文件中的压缩文件）中的威胁。默认情况下，扫描处于禁用状态。
   - “**扫描 SFX 压缩文件**”。扫描包含可执行解压缩模块的自解压压缩文件。默认情况下，扫描处于禁用状态。
   - “**扫描邮件数据库**”。扫描 Microsoft Outlook、Outlook Express、The Bat! 和其他邮件客户端的电子邮件数据库。默认情况下，扫描处于禁用状态。
   - “**扫描邮件格式文件**”。扫描纯文本电子邮件。默认情况下，扫描处于禁用状态。
   - “**跳过扫描时间超过以下值的文件(秒)**”。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。默认情况下，应用程序会尝试在一分钟内扫描对象。

- “**跳过大于以下大小的文件 (MB)**”。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。

- “**跳过大于以下大小的文件 (MB)**”。如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。

5. 保存更改。

**如何在命令行中配置文件扫描**

1. 运行以下命令：

```
kesl --set-settings <task ID|name> ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<object size (MB)>
TimeLimit=<scan time (sec)> QueueScanTasks=<Yes|No>
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

- `<object size (MB)>` 是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。默认值：`0`。

- `<scan time (sec)>` 是对象扫描的最长持续时间（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。默认值：`0`。

2. 您还可以使用配置文件配置设置：

   a. 运行以下命令，将任务设置输出到配置文件：

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. 打开配置文件进行编辑。

   c. 在此文件中，添加以下适用于容器和镜像内对象的 *容器扫描*任务设置：`ScanArchived`、`ScanSfxArchived`、`ScanMailBases`、`ScanPlainMail`、`SizeLimit`、`TimeLimit`、`QueueScanTasks`。

   d. 将更改保存在配置文件中。

   e. 使用以下命令，将设置从配置文件导入到任务中：

   ```
   kesl-control --set-settings <task ID|name> --file <path> [--json]
   ```

   其中：

   - `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

   - `--file <path>` 是配置文件的完整路径，您希望从该配置文件导入任务设置。

   - 如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果不指定 `--json`选项，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。

## 如何选择检测到受感染对象时要对容器执行的操作

在容器中检测到受感染对象时，Kaspersky Endpoint Security 可以立即停止该容器、不执行任何操作，或者在无法清除对象或消除威胁时停止该容器。您可以选择当 *容器监控* 组件执行实时扫描或按需 *容器扫描* 任务时检测到受感染对象后，Kaspersky Endpoint Security 对容器执行的操作。

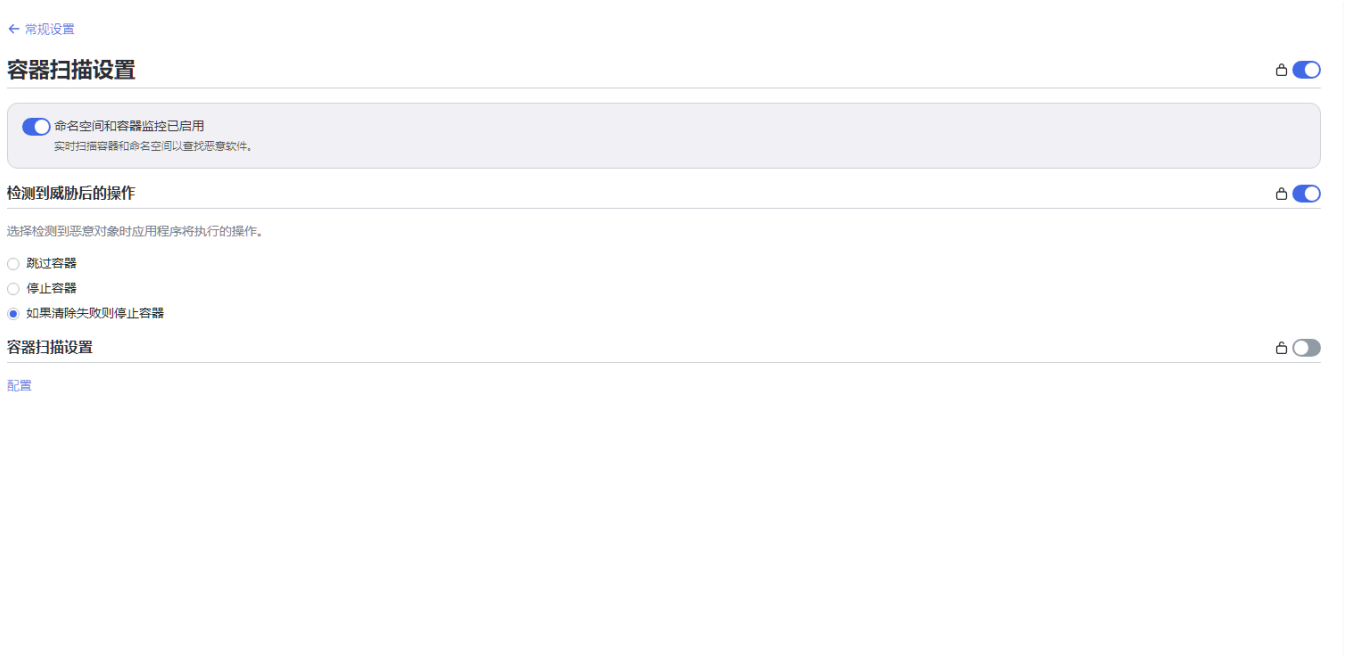
如果在容器镜像中检测到受感染对象，Kaspersky Endpoint Security 可以删除该镜像，或者不对该镜像执行任何操作。您可以选择在按需 *容器扫描* 任务中检测到受感染对象时，Kaspersky Endpoint Security 对容器镜像执行的操作。

**如何在 Web Console 中选择容器监控检测到威胁后的操作**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **容器扫描设置**。
5. 确保容器监控组件的切换开关处于 **命名空间和容器监控已启用** 位置。
6. 在 **检测到威胁后的操作** 下，选择在容器中检测到受感染对象时应用程序将执行的操作：
   - “**跳过容器**”。当在容器中检测到受感染对象时，应用程序不会对容器执行任何操作。
   - “**停止容器**”。当在容器中检测到受感染对象时，应用程序将停止容器。
   - **如果清除失败则停止容器**（默认）。当在容器中检测到受感染对象时，应用程序会尝试清除受感染对象。如果无法清除感染对象，应用程序将停止容器。

     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。

7. 保存更改。




容器扫描设置

### 如何在命令行中选择容器监控检测到威胁后的操作

1. 运行以下命令：

```
kesl-control --set-container-settings OnAccessContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
```

> 仅在使用具有支持此功能的授权许可的应用程序时，才能配置此设置。

2. 要查看容器扫描设置的当前值，请运行以下命令：

```
kesl-control --get-settings container-settings
```

### 如何在 Web Console 中选择容器扫描检测到威胁后的操作

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 在任务列表中，选择 Kaspersky Endpoint Security 容器扫描任务，然后单击该任务的名称。
   任务属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在 **高级扫描设置** → **容器扫描设置** → **检测到威胁后的操作** 下，选择当在容器中检测到受感染对象时应用程序将执行的操作：
   - “**跳过容器**”。当在容器中检测到受感染对象时，应用程序不会对容器执行任何操作。
   - “**停止容器**”。当在容器中检测到受感染对象时，应用程序将停止容器。

- **如果清除失败则停止容器**（默认）。当在容器中检测到受感染对象时，应用程序会尝试清除受感染对象。如果无法清除感染对象，应用程序将停止容器。

  > 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。

5. 在 **高级扫描设置 → 镜像扫描设置 → 检测到威胁后的操作** 下，选择当在容器中检测到受感染对象时应用程序将执行的操作：

   - **跳过镜像**（默认）。当在镜像中检测到受感染对象时，应用程序不会对镜像执行任何操作。
   - **删除镜像**（不推荐）。当在镜像中检测到受感染对象时，应用程序将删除该镜像。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。

6. 保存更改。

**如何在命令行中选择容器扫描检测到威胁后的操作**

1. 运行以下命令：

   ```
   kesl-control --set-settings <task ID|name> ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
   ImageAction=<Skip|Delete>
   ```

   其中，`<task ID|name>` 是任务创建时分配给任务的 ID，或者是命令行上的任务名称。

   > 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。

2. 您还可以使用配置文件配置该操作：

   a. 运行以下命令，将任务设置输出到配置文件：

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. 打开配置文件进行编辑。

   c. 将 *容器扫描* 任务的以下设置添加到文件：

   - `ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>` – 检测到受感染对象时要对容器执行的操作。默认值：`StopContainerIfFailed`。
   - `ImageAction=<Skip|Delete>` – 检测到受感染对象时要对容器镜像执行的操作。默认值：`Skip`。

   d. 将更改保存在配置文件中。

   e. 使用以下命令，将设置从配置文件导入到任务中：

   ```
   kesl-control --set-settings <task ID|name> --file <path> [--json]
   ```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `--file <path>` 是配置文件的完整路径，您希望从该配置文件导入任务设置。
- 如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果不指定 `--json`选项，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。

## 如何运行容器和镜像的自定义扫描

*要在命令行中启动"自定义容器扫描"任务，请运行以下命令：*

```
kesl-control --scan-container <id|name[:tag]>
```

其中 `<id|name[:tag]>` 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。

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。

对名为 `my_container` 的容器执行容器扫描的示例

```
kesl-control --scan-container my_container
```

对名为 `my_image` 的镜像执行镜像扫描的示例（所有标签）

```
kesl-control --scan-container my_image*
```

实用文章

**如何指定掩码**

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。

# 可移动驱动器扫描

Kaspersky Endpoint Security 扫描您执行或复制的所有文件，即使该文件位于可移动驱动器上。应用程序会扫描 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上的文件。默认情况下，可移动驱动器扫描处于禁用状态。

## 可移动驱动器扫描的工作原理

连接可移动驱动器时，应用程序会自动创建并启动以下使用默认设置的扫描任务：*关键区域扫描* 用于快速扫描，*恶意软件扫描* 用于详细扫描。这些任务无法停止。在可移动驱动器上检测到威胁时，Kaspersky Endpoint Security 会尝试清除受感染的对象。如果无法清除，应用程序会删除受感染的对象。扫描完成后，应用程序会自动删除这些任务。

## 扫描类型

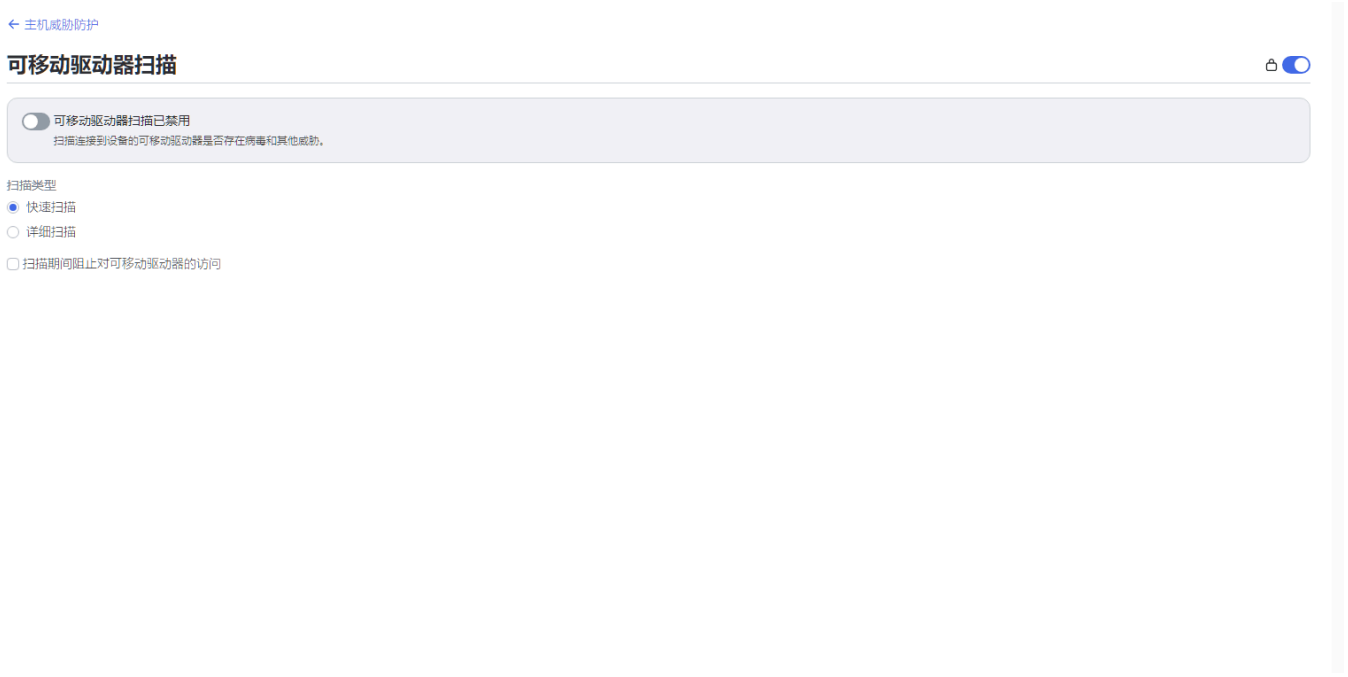
- “**快速扫描**”。Kaspersky Endpoint Security 仅扫描 具有指定扩展名的文件，并且不会解包复合对象。应用程序使用 *关键区域扫描* 任务的默认设置执行快速扫描。
- “**详细扫描**”。Kaspersky Endpoint Security 会扫描可移动驱动器上的所有文件。应用程序使用 *恶意软件扫描* 任务的默认设置执行详细扫描。

**如何在 Web Console 中选择可移动驱动器扫描类型**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护 → 可移动驱动器扫描**。
5. 确保该组件的切换开关处于 **可移动驱动器扫描已启用** 位置。
6. 在 **扫描类型** 下，选择可移动驱动器扫描的类型：**快速扫描** 或 **详细扫描**。
7. 如有必要，选中“**扫描期间阻止访问文件**”复选框。
   阻止对文件的访问可防止用户在扫描过程中运行恶意软件。

   扫描引导扇区时，应用程序不会阻止任何文件。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




可移动驱动器扫描

## 如何在命令行中选择可移动驱动器扫描类型

1. 连接可移动驱动器时，请选择要执行的扫描类型：

```
kesl-control --set-settings 16 ScanRemovableDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

2. 插入 CD/DVD 驱动器或蓝光光盘时，请选择要执行的扫描类型：

```
kesl-control --set-settings 16 ScanOpticalDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

3. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 16
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ScanRemovableDrives` | 连接可移动驱动器时的扫描类型：<br>• `DetailedScan`。详细扫描。<br>• `QuickScan`。快速扫描。<br>• `NoScan`（默认）。应用程序不执行扫描。 |
| `ScanOpticalDrives` | 插入 CD/DVD 驱动器或蓝光光盘时要执行的扫描类型：<br>• `DetailedScan`。详细扫描。<br>• `QuickScan`。快速扫描。<br>• `NoScan`（默认）。应用程序不执行扫描。 |
| `BlockDuringScan` | 扫描期间阻止对已连接磁盘上文件的访问。默认情况下，应用程序不会阻止对文件的访问。阻止对文件的访问可防止用户在扫描过程中运行恶意软件。<br>扫描引导扇区时，应用程序不会阻止任何文件。 |

# 行为检测

行为检测组件允许监控可能危害计算机或用户数据的应用程序的活动（打开文件、建立连接等）。该组件监控应用程序行为，以查找危险模式。如果应用程序活动匹配此类模式之一，Kaspersky Endpoint Security 将执行选定的响应操作。Kaspersky Endpoint Security 的此功能可为计算机提供主动防护。

为了使行为检测组件达到最佳运行状态，建议启用 Web 威胁防护组件。

## 行为检测的工作原理

1. **应用程序监控操作系统中的事件**

   应用程序接收由事件组成的遥测流：进程创建和终止、打开的文件、建立的连接等。应用程序还会为事件补充相关元数据（进程名称、PID、IP 地址等）。

2. **应用程序将遥测流与危险行为模式进行比较**

   如果第三方应用程序的操作与危险行为模式匹配，Kaspersky Endpoint Security 会执行威胁响应操作（例如，可以停止该第三方应用程序）。

3. **应用程序将遥测发送到 KSN**

   应用程序会过滤事件并将其发送到 KSN 以供进一步分析。

## 配置行为检测

1. **在行为检测设置中，选择“通知”操作**

   默认情况下，行为检测组件处于启用状态。在行为检测设置中，我们建议选择 **通知** 作为检测到威胁后的操作，并检查已安装的应用程序能否正常运行。Kaspersky Endpoint Security 允许所有应用程序活动，并记录组件的运行日志。

   **如何在 Web Console 中选择检测到恶意软件活动时执行的操作**

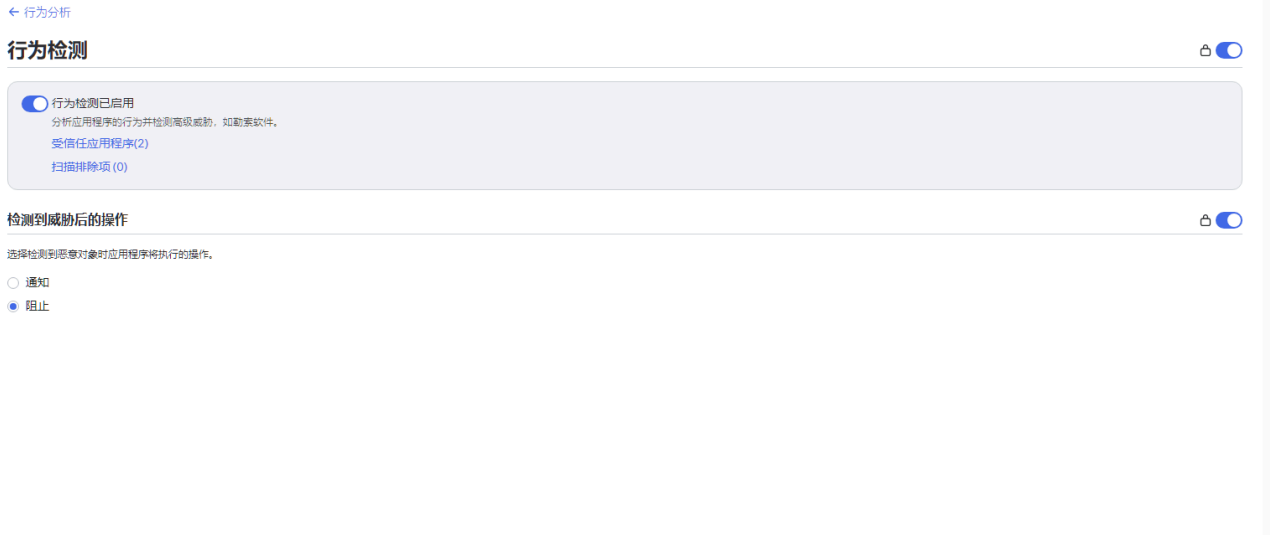
   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
   2. 单击 Kaspersky Endpoint Security 策略的名称。

      策略属性窗口将打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择 **主机威胁防护 → 行为分析 → 行为检测**。

5. 在“**检测到威胁后的操作**”块中选择相关操作：

   - “**通知**”。如果检测到恶意活动，Kaspersky Endpoint Security 不会停止此应用程序，而只会在事件日志中记录有关检测到恶意活动的事件。
   - “**阻止**”。如果检测到恶意活动，Kaspersky Endpoint Security 会停止正在执行恶意活动的应用程序的进程，并记录有关检测到的恶意活动的信息。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




行为检测

### 如何在命令行中选择检测到恶意软件活动时执行的操作

1. 运行以下命令：

```
kesl-control --set-settings 20 TaskMode=<Block|Notify>
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 20
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| TaskMode | 检测到恶意软件活动时的操作：<br>• Block （默认）。如果检测到恶意活动，Kaspersky Endpoint Security 会停止正在执行恶意活动的应用程序的进程，并记录有关检测到的恶意活动的信息。<br>• Notify。如果检测到恶意活动，Kaspersky Endpoint Security 不会停止此应用程序，而只会在事件日志中记录有关检测到恶意活动的事件。 |

## 2 收集行为检测统计信息

您可以使用 报告 获取行为检测统计信息。

## 3 优化应用程序性能

分析收集到的信息后，优化应用程序性能并添加排除项。

4. **在行为检测设置中，选择“阻止”操作**

   启用对应用程序恶意活动的阻止。之后，Kaspersky Endpoint Security 将停止正在执行恶意活动的应用程序的进程。

特殊注意事项和限制

- 为了确保在 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 解决方案集成时行为检测组件正常运行，请确保配置文件中的 auditd 设置为无配置阻止模式 `enabled 1`。

# 漏洞利用防御

漏洞利用防御会监控利用设备上的漏洞来获取管理权限或执行恶意操作的代码。

要使漏洞利用防御组件正常工作，必须启用以下组件：

- 行为检测
- 可更新内核模块

> 该组件不适用于配备 Elbrus CPU 的设备。

漏洞利用防御的工作原理

1. **应用程序监控操作系统中的事件**

   应用程序接收由事件组成的遥测流：进程创建和终止、打开的文件、建立的连接等。应用程序还会为事件补充相关元数据（进程名称、PID、IP 地址等）。

2. **应用程序将遥测流与危险行为模式进行比较**

   如果第三方应用程序的操作与危险行为模式匹配，Kaspersky Endpoint Security 会执行威胁响应操作（例如，可以停止该第三方应用程序）。

配置漏洞利用防御

1. **在漏洞利用防御设置中，选择“通知”操作**

   默认情况下，漏洞利用防御组件处于禁用状态。在漏洞利用防御设置中，选择**通知**作为检测到威胁后的操作，并检查已安装的应用程序能否正常工作。Kaspersky Endpoint Security 允许应用程序执行所有活动，并记录有关检测到的威胁的信息。

**如何在 Web Console 中选择检测到漏洞利用后的操作**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护 → 行为分析 → 漏洞利用防御**。
5. 使用**漏洞利用防御**开关启用或禁用组件。
6. 在“**检测到威胁后的操作**”块中选择相关操作：
   - “**阻止**”。如果选择此项，在检测到漏洞时，Kaspersky Endpoint Security 会阻止此漏洞的操作，并生成一条包含此漏洞相关信息的日志条目。
   - “**通知**”。如果选择此项目，Kaspersky Endpoint Security 将在检测到漏洞时记录包含漏洞相关信息的条目，并将此漏洞的相关信息添加至活动威胁列表。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中选择检测到威胁后的操作**

1. 要启用漏洞利用防御，请运行以下命令：

```
kesl-control --set-settings 20 UseAEP=Yes
```

2. 选择检测到漏洞利用后的操作：

```
kesl-control --set-settings 20 AEPMode=<Block|Notify>
```

3. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 20
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `UseAEP` | 启用组件：<br>• `Yes` 启用漏洞利用防御。<br>• `No`（默认）禁用漏洞利用防御。 |
| `AEPMode` | 检测到漏洞利用后的操作：<br>• `Block`（默认）。Kaspersky Endpoint Security 会阻止此漏洞利用的操作，并生成一条包含此漏洞利用相关信息的日志记录。<br>• `Notify`。Kaspersky Endpoint Security 检测到漏洞利用时，会生成一条包含该漏洞利用相关信息的日志记录，并将此漏洞利用的信息添加到活动威胁列表。 |

## 2 收集漏洞利用防御统计信息

您可以使用报告获取漏洞利用防御统计信息。

3. **优化应用程序性能**

   分析收集到的信息后，优化应用程序性能：

   - 添加全局排除项
   - 添加排除项

4. **在漏洞利用防御设置中，选择“阻止”操作**

   启用阻止操作系统中应用程序恶意活动的功能。

# 反加密

反加密勒索组件通过分析计算机共享网络目录中远程设备的活动，提供针对远程加密的保护。反加密勒索会分析通过 NFS 和 SMB 协议传输到受保护计算机的文件。

如果活动与外部加密的典型行为流签名匹配，Kaspersky Endpoint Security 将阻止此活动或向您发出通知。

## 反加密勒索的工作原理

1. **应用程序拦截 NFS 和 SMB 请求**

   应用程序会接收通过 NFS 和 SMB 协议传输的文件的创建和修改相关遥测数据流。

2. **应用程序会将遥测数据流与签名数据库进行比较。**

   如果第三方应用程序的操作与勒索软件的操作匹配，Kaspersky Endpoint Security 会执行选定的检测到威胁后的操作（例如，阻止与远程计算机的连接）。

## 配置反加密勒索

1. **配置保护范围**

   默认情况下，应用程序会扫描所有共享目录。如果您只需扫描单个目录（例如，从外部源自动下载文件的目录），可以仅将该目录指定为保护范围。在其他情况下，我们建议保留默认保护范围，并使用排除项来微调范围。

2. **在反加密勒索设置中，选择“通知”操作**

   默认情况下，反加密勒索处于禁用状态。建议启用反加密勒索，并将检测到威胁后的操作设置为**通知**，然后检查对所有企业资源的访问。Kaspersky Endpoint Security 允许访问共享目录中的所有资源，并记录有关检测到的威胁的信息。

3. **收集反加密勒索统计信息**

   您可以使用报告获取反加密勒索统计信息。

4. **优化应用程序性能**

分析收集到的信息后，优化应用程序性能：

- 添加全局排除项。
- 添加排除项。

5. **在反加密勒索设置中，选择"阻止连接"操作**

   启用阻止来自远程攻击设备的网络流量。

特殊注意事项和限制

- 反加密勒索组件可以与 SMB1、SMB2、SMB3、NFS3、TCP/UDP 和 IP 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，以保证不能使用 NFS2 和 NFS4 协议挂载资源。
- 为了保证反加密勒索组件正常工作，必须在操作系统中安装至少一项服务（Samba 或 NFS）。对于 NFS 服务，必须安装 rpcbind 软件包。
- 在将远程设备的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。

## 如何选择检测到恶意加密时的操作

如果检测到恶意加密，应用程序可以阻止远程攻击设备的网络流量，或者仅通知检测到恶意加密。

为了阻止网络流量，Kaspersky Endpoint Security 会创建一条动态防火墙规则。防火墙会临时阻止攻击设备的网络流量。应用程序还会将攻击设备添加到已阻止设备列表。被阻止的设备无法访问共享网络目录。

为了通知管理员检测到恶意加密，应用程序会生成 *检测到加密* 事件。

默认情况下，应用程序会阻止攻击设备的网络流量 60 分钟。阻止时间到期后，应用程序会将受感染的设备从已阻止设备列表中移除，并自动恢复该设备对网络文件资源的访问权限。

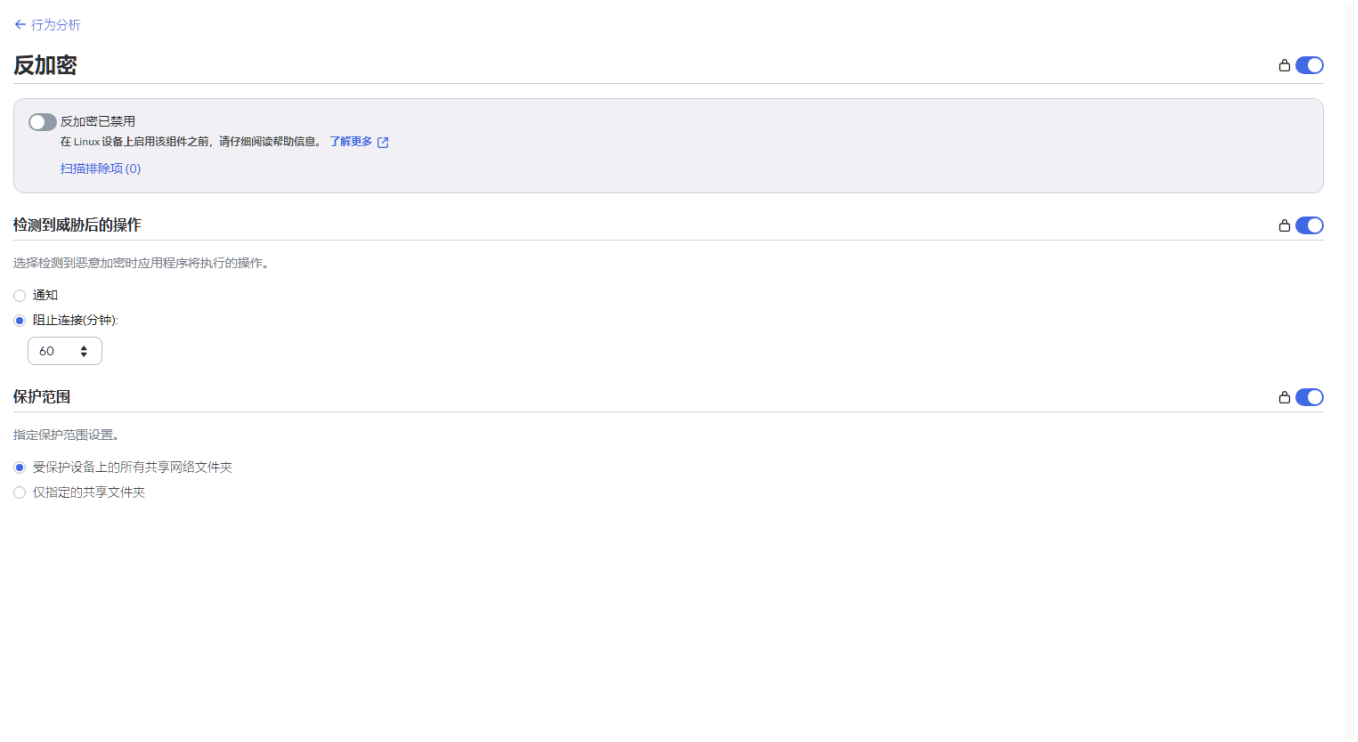
您可以在用户计算机本地查看已阻止设备列表，并手动解除对这些设备的阻止。除 *检测到加密* 事件外，Kaspersky Security Center 不提供用于监控和管理已阻止设备的工具。

**如何在 Web Console 中配置检测到恶意加密时的操作**

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**策略**"。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护 → 行为分析 → 反加密**。
5. 确保该组件的切换开关处于 **反加密已启用** 位置。
6. 在 **检测到威胁后的操作** 下，选择应用程序在检测到威胁时将执行的操作：**通知** 或 **阻止连接(分钟)**。
7. 如果选择了 **阻止连接(分钟)**，请设置攻击设备的阻止时间（分钟）。默认情况下，设备会被阻止 60 分钟。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




反加密

## 如何在命令行中配置检测到恶意加密时的操作

1. 运行以下命令：

```
kesl-control --set-settings 13 ActionOnDetect=<Block|Notify>
```

2. 选择 `Block` 操作的阻止时间。

```
kesl-control --set-settings 13 BlockTime=<Blocking period>
```

3. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 13
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ActionOnDetect` | 检测到外部加密时的操作：<br>• `Block`（默认）会阻止攻击设备的网络流量并创建 *检测到加密* 事件。<br>• `Notify` 创建 *检测到加密* 事件，但不阻止网络流量。 |
| `BlockTime` | 攻击设备的阻止时间（分钟）。 |

# 如何创建保护范围

*保护范围*是 Kaspersky Endpoint Security 监控文件活动的共享网络目录路径列表。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。默认情况下，应用程序会自动识别共享网络目录并监控这些目录中的文件活动。

如有必要，您可以将针对恶意加密的文件活动监控限制为部分目录。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。

如果您的组织在通过共享网络目录交换文件时使用数据加密，则从保护范围中排除目录可以减少误报量。例如，当用户处理共享文件夹中扩展名为 ENC 的文件时，反加密勒索可能会引发误报。这种活动与外部加密的典型行为模式相匹配。如果您在共享网络目录中有用于保护数据的加密文件，请将该目录添加到排除项。

**如何在 Web Console 中创建保护范围**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **行为分析** → **反加密**。
5. 确保该组件的切换开关处于 **反加密已启用** 位置。
6. 在“**保护范围**”下，选择“**仅指定的共享文件夹**”。
7. 在目录列表中，单击“**添加**”。
8. 这将打开一个窗口；在该窗口中，选择文件系统类型：
   - “**本地**”。无需网络连接即可访问的硬盘目录。
   - “**共享**”。可通过 Samba (SMB) 或 NFS 协议访问的计算机目录。
   - “**全部共享**”。通过 Samba 和 NFS 协议访问的所有计算机目录。
9. 对于本地文件系统，请指定目录路径（例如，`/path/to/folder`）。
10. 为对象扩展名指定掩码（例如，`*.txt`）。用逗号分隔各个掩码。
11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行创建保护范围**

1. 运行以下命令：

```
kesl-control --set-settings 13 ScanScope.item_#.UseScanArea=Yes \
        [ScanScope.item_#.AreaDesc=<description of the area>] \
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>] \
        [ScanScope.item_#.Path=<path to the directory>]
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 13
```

### 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ScanScope.item_#.UseScanArea=Yes` | 启用编号为 `#` 的保护范围。<br>您可以临时排除某个保护范围，而不是将其删除。为此，请设置 `ScanScope.item_#.UseScanArea=No`。 |
| `ScanScope.item_#.AreaDesc` | 保护范围的说明；包含有关 `#` 保护范围的其他信息。 |
| `ScanScope.item_#.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。<br>示例<br>`ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt.` |
| `ScanScope.item_#.Path` | 包含要保护的对象的目录的路径。可能的值：<br>• `AllShared`（默认）。通过 Samba 和 NFS 协议访问的所有计算机目录。<br>• `Shared:SMB`。可通过 Samba (SMB) 协议访问的目录。<br>• `Shared:NFS`。可通过 NFS 协议访问的目录。<br>• `<path to local directory>`。无需网络连接即可访问的硬盘目录。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |

仅包含 `/home` 目录的保护范围示例

```
kesl-control --set-settings 13 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

# BadUSB 攻击防护

攻击者可以利用 USB 设备（例如闪存驱动器）固件中的漏洞，对该设备重新编程，使操作系统在连接时将该设备识别为键盘。因此，受感染的 USB 设备可能会用您的用户账户执行命令，例如下载恶意软件。

BadUSB 攻击防护组件可以阻止受感染的 USB 设备连接。

该组件不适用于配备 Elbrus CPU 的设备。

## BadUSB 攻击防护的工作原理

1. **应用程序会提示您授权 USB 设备**

   当 USB 设备连接到设备时，应用程序会提示用户输入应用程序生成的数字代码。此过程称为 *授权*。

2. **用户输入授权码**

   用户可以使用连接的 USB 设备本身（键盘或条形码扫描器）或屏幕键盘（如果可用）输入该代码。您无法使用已连接的 USB 设备输入该代码。

3. **应用程序允许已授权的 USB 设备，并阻止未授权的 USB 设备**

   如果数字代码输入正确，应用程序会将识别参数（即 USB 设备的 VID/PID 及其连接的端口号）保存到已授权 USB 设备列表中。如果重新连接此 USB 设备或重启操作系统，则无需再次授权。

   如果输入的数字代码不正确，应用程序将生成一个新代码。您可以配置输入数字代码的最大尝试次数。如果多次输入错误的数字代码，应用程序将在一定时间内阻止来自此 USB 设备的输入。等待 USB 设备锁定时间结束后，您可以再次尝试授权 USB 设备。您可以配置多长时间后可以继续尝试输入授权码。

当已授权的 USB 设备连接到不同的 USB 端口时，应用程序会要求重新授权。

配置 BadUSB 攻击防护

1. **启用 BadUSB 攻击防护**

   默认情况下，BadUSB 攻击防护保护组件处于禁用状态。确定不受信任的人员可以实际接触且需要防范外部攻击者的设备，并在这些设备上启用 BadUSB 攻击防护组件。启用 BadUSB 攻击防护后，应用程序将要求对连接的 USB 设备进行授权，在获得授权之前，用户将无法使用未授权的 USB 设备。但是，在启用 BadUSB 攻击防护之前连接的 USB 设备默认被视为已授权，无需授权。

   在启用并配置 BadUSB 攻击防护之前，请勿将任何不受信任的 USB 设备连接到设备。

2. **配置 BadUSB 攻击防护**

   根据所连接的 USB 设备类型（键盘或条形码扫描器），配置授权码的显示方式：显示为条形码或数字代码（默认设置）。

   如有必要，请配置 USB 设备授权：

   - 输入授权码的最大尝试次数
   - 达到最大尝试次数时的 USB 设备阻止持续时间。

# 如何配置 USB 设备授权

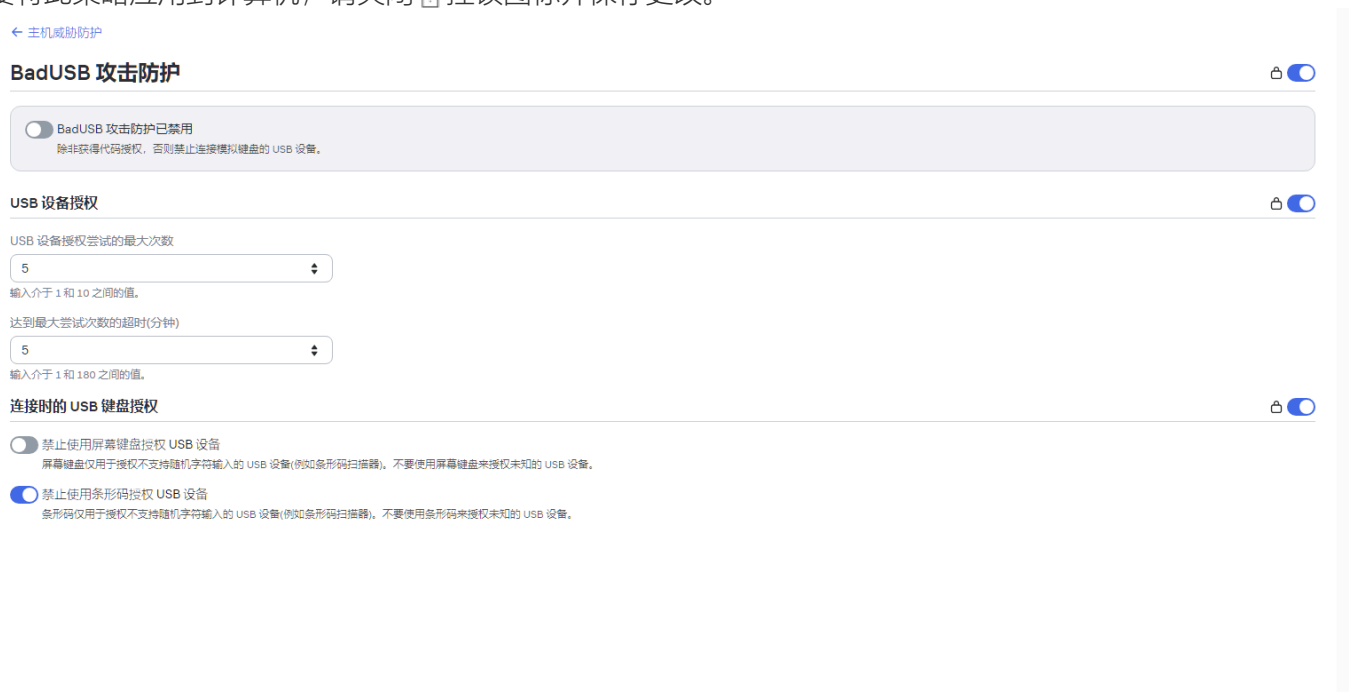
当操作系统识别为输入设备的 USB 设备连接到受管理设备时，应用程序会建议使用数字代码或条形码授权该 USB 设备。如果授权代码输入错误，应用程序将生成新代码。如果授权代码多次输入错误或授权窗口关闭，应用程序将阻止来自此 USB 设备的输入。当 USB 设备阻止时间结束或操作系统重新启动后，应用程序将提示用户再次执行授权。

Kaspersky Endpoint Security 允许您配置 USB 设备授权

- 最大授权尝试次数。
- 达到最大尝试次数时的 USB 设备阻止持续时间。

### 如何在 Web Console 中配置 USB 设备授权

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **BadUSB 攻击防护**。
5. 确保该组件的切换开关处于 **BadUSB 攻击防护已启用** 位置。
6. 在 **USB 设备授权** 下，配置授权设置：
   - “**USB 设备授权尝试的最大次数**”。如果授权码输入错误达到指定次数，则自动锁定 USB 设备。有效值为 1 到 10。例如，如果允许 5 次尝试输入授权码，则在第五次尝试失败后，应用程序将阻止 USB 设备。Kaspersky Endpoint Security会显示 USB 设备被阻止的时间。此时间过后，您还可以再尝试 5 次输入授权代码。
   - “**达到最大尝试次数的超时(分钟)**”。在指定次数的授权码输入失败后，USB 设备将被阻止。可能的值：1 到 180（分钟）
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




BadUSB 攻击防护

### 如何在命令行配置 USB 设备授权

1. 运行以下命令：

```
kesl-control --set-settings 37 MaxAuthAttempts=<number of attempts> TimeoutAfterAttempts=<timeout (minutes)>
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 37
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| MaxAuthAttempts | 如果授权码输入错误达到指定次数，则自动锁定 USB 设备。有效值为 1 到 10。例如，如果允许 5 次尝试输入授权码，则在第五次尝试失败后，应用程序将阻止 USB 设备。Kaspersky Endpoint Security会显示 USB 设备被阻止的时间。此时间过后，您还可以再尝试 5 次输入授权代码。<br>默认值：5。 |
| TimeoutAfterAttempts | 在指定次数的授权码输入失败后，USB 设备将被阻止。可能的值：1 到 180（分钟）<br>默认值：5 分钟。 |

# 如何允许使用屏幕键盘连接 USB 设备

屏幕键盘应仅用于不支持随机字符输入的 USB 设备的授权（例如条形码扫描器）。不建议使用屏幕键盘授权未知的 USB 设备。默认情况下，允许使用屏幕键盘。

我们建议仅使用屏幕键盘授权用户已知的 USB 设备。

### 如何在 Web Console 中使用屏幕键盘启用 USB 设备授权

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **BadUSB 攻击防护**。
5. 确保该组件的切换开关处于 **BadUSB 攻击防护已启用** 位置。
6. 确保“**禁止使用屏幕键盘授权 USB 设备**”开关已关闭。默认情况下，切换按钮处于关闭状态。
7. 要将策略应用到设备，请关闭 挂锁图标并保存更改。

### 如何在命令行中使用屏幕键盘启用 USB 设备授权

请执行命令：

```
kesl-control --set-settings 37 ProhibitOnScreenKeyboard=No
```

# 如何允许使用条形码扫描器连接 USB 设备

将条形码扫描器连接到设备时，BadUSB 攻击防护组件会将此扫描器识别为输入设备，并提示您执行授权。要授权条形码扫描器，您必须扫描屏幕上显示的条形码。应用程序会生成 Code39 格式的条形码。大多数条形码扫描器和二维码扫描器都支持此格式。

应用程序还支持另一种对条形码扫描器进行授权的方式。如果您使用触摸屏设备，则可以使用屏幕键盘输入代码。为此，您需要允许使用屏幕键盘。例如，对于收银机内置的固定条形码扫描器，这种方法很方便。禁止使用其他条形码扫描器授权方法。默认情况下，应用程序不使用条形码来授权 USB 设备。

**如何在 Web Console 中使用条形码扫描器启用 USB 设备授权**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **BadUSB 攻击防护**。
5. 确保该组件的切换开关处于 **BadUSB 攻击防护已启用** 位置。
6. 禁用 **禁止使用条形码授权 USB 设备** 切换开关。
7. 要将策略应用到设备，请关闭 挂锁图标并保存更改。

**如何在命令行中使用条形码扫描器启用 USB 设备授权**

请执行命令：

```
kesl-control --set-settings 37 ProhibitBarcodeScanner=No
```

# 通信和 Web 保护

## 邮件威胁防护

邮件威胁防护组件会扫描收发电子邮件的附件，以检测病毒和其他威胁性应用程序。该组件使用反病毒数据库、卡巴斯基安全网络云服务和启发式分析来保护设备。

邮件威胁防护可以扫描收件和发件。该应用程序在以下邮件客户端中支持 POP3、SMTP 和 IMAP：该应用程序还支持协议的扩展版本：POP3S、SMTPS 和 IMAPS。

如果在浏览器中打开邮件客户端，“邮件威胁防护”组件不会扫描邮件。

> 要使邮件威胁防护组件正常工作，必须在网络设置中监控网络端口 25、110、143、465、587、993 和 995。这些网络端口默认已添加到监控端口列表中。从列表中移除这些端口可能会导致组件无法正常工作。

邮件威胁防护组件默认启用。

## 邮件威胁防护的工作原理

安装 Kaspersky Endpoint Security 时，应用程序会添加一个自签名证书 *卡巴斯基反病毒个人根证书*。应用程序会将此证书放入本地受信任证书存储区 (`/etc/ssl/certs`)。每次应用程序启动时，都会检查证书是否存在。如果证书已被删除，应用程序会自动恢复该证书。

1. **应用程序拦截邮件流量**

   Kaspersky Endpoint Security 通过 POP3、SMTP 和 IMAP 协议检查连接。

2. **应用程序扫描传入和传出的邮件**

   邮件威胁防护使用以下技术扫描流量：

   - 反病毒数据库。
   - 卡巴斯基安全网络的云服务。
   - 启发式分析技术能够检测卡巴斯基数据库尚未涵盖的威胁。

3. **应用程序完成扫描**

   如果传入邮件的附件或邮件正文中包含威胁，Kaspersky Endpoint Security 会执行检测到威胁后的操作。如果在传出邮件中检测到威胁，邮件威胁防护会阻止发送此类邮件。

## 配置邮件威胁防护

1. **定义用于组件测试部署的组**

   划分出一小组设备，用于测试邮件威胁防护组件的配置。这样，您可以确认组件已正确配置，并确保邮件客户端稳定运行，避免可能的故障。

2. **配置附件过滤器**

   默认情况下，由卡巴斯基配置的邮件威胁防护过滤器可提供推荐的防护级别。如果您对邮件安全有特殊要求，您可以更改附件过滤器设置。

3. **配置邮件扫描**

   如有必要，请根据邮件服务器的参数配置电子邮件扫描。例如，您可以限制所扫描压缩文件的大小，以降低邮件服务器的负载。

4. **验证邮件威胁防护是否正常工作**

   生成一封带有恶意附件的测试邮件。将该邮件发送到您选择的设备组，并验证邮件中的恶意内容是否已按照组件设置进行处理。

   您还可以通过运行以下命令，验证应用程序是否已生成相应的 *检测到威胁* 事件：

   ```
   kesl-control -E -q "TaskName == 'Mail_Monitoring'"
   ```

5. **将邮件威胁防护设置应用到组织中的所有设备**

特殊注意事项和限制

- 如果受保护设备上的邮件客户端不使用本地受信任证书存储区，请手动将 *卡巴斯基反病毒个人根证书* 证书添加到邮件客户端的受信任证书存储区。有关添加证书的更多信息，请参阅您的邮件客户端的官方文档。
- 邮件威胁防护不会尝试清除传出邮件中的恶意附件。带有恶意附件的传出邮件会被完全阻止或允许通过。

# 检测到邮件威胁时该怎么办

当在*外发邮件*的附件中检测到受感染对象时，应用程序会阻止发送该邮件。

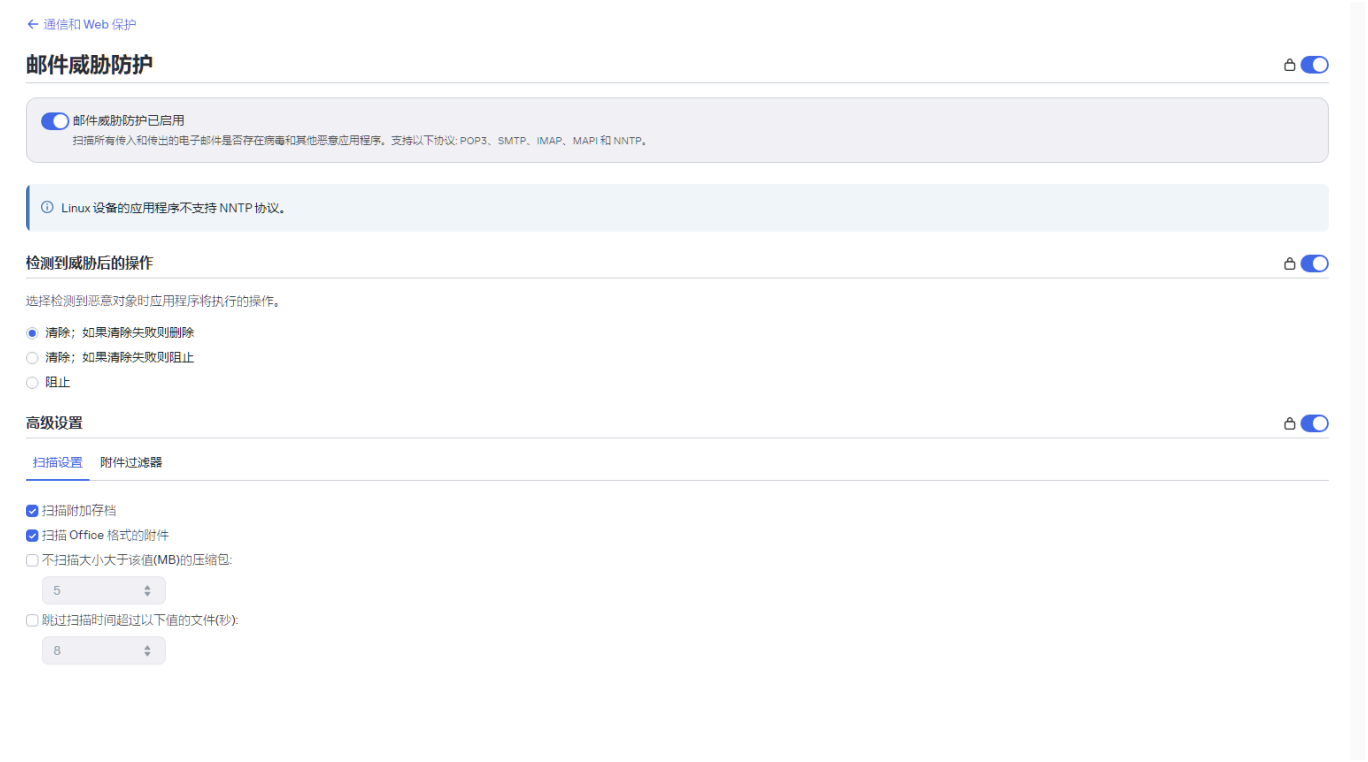
如果在*传入邮件*中检测到受感染对象，应用程序可以尝试清除该对象，然后删除该对象或阻止访问该对象。Kaspersky Endpoint Security 还会将有关已执行操作的信息添加到邮件主题中，例如，*[邮件已被处理] <邮件主题>*。

配置邮件威胁防护时，您可以选择当在电子邮件中检测到威胁时 Kaspersky Endpoint Security 将执行的操作。

**如何在 Web Console 中配置检测到威胁时的操作**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护 → 邮件威胁防护**。
5. 在 **检测到威胁后的操作** 下，选择应用程序在检测到威胁时将执行的操作：
   - “**清除；如果清除失败则删除**”。当在传入邮件中检测到感染对象时，应用程序会尝试清除该对象。然后带有安全附件的邮件将被提供给用户。如果清除失败，应用程序会删除感染对象。应用程序会在邮件主题中添加关于已执行操作的信息，例如*[邮件已处理] <邮件主题>*。如果在发送邮件中检测到感染对象，应用程序会阻止该邮件，邮件客户端会显示错误。
   - “**清除；如果清除失败则阻止**”。当在传入邮件中检测到感染对象时，应用程序会尝试清除该对象。然后带有安全附件的邮件将被提供给用户。如果清除失败，应用程序会在邮件主题中添加警告信息。然后，带有原始附件的邮件将被提供给用户。如果在发送邮件中检测到感染对象，应用程序会阻止该邮件，邮件客户端会显示错误。
   - “**阻止**”。如果在传入邮件中检测到感染对象，应用程序会在邮件主题中添加警告。然后，带有原始附件的邮件将被提供给用户。如果在发送邮件中检测到感染对象，应用程序会阻止该邮件，邮件客户端会显示错误。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




邮件威胁防护

## 如何在命令行中配置检测到威胁时的操作

1. 确保邮件威胁防护组件已启用：

```
kesl-control --get-task-state 35
```

组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

```
kesl-control --start-task 35
```

3. 选择在传入邮件中检测到邮件威胁时要执行的操作：

```
kesl-control --set-settings 35 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

4. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 35
```

符号

| 设置 | 描述 |
| --- | --- |
| `ActionOnThreat` | 检测到威胁后的操作：<br>• `DisinfectDeleteIfNotPossible`（默认）。当在传入邮件中检测到感染对象时，应用程序会尝试清除该对象。然后带有安全附件的邮件将被提供给用户。如果清除失败，应用程序会删除感染对象。应用程序会在邮件主题中添加关于已执行操作的信息，例如*[邮件已处理]<邮件主题>*。如果在发送邮件中检测到感染对象，应用程序会阻止该邮件，邮件客户端会显示错误。<br>• `DisinfectBlockIfNotPossible`。当在传入邮件中检测到感染对象时，应用程序会尝试清除该对象。然后带有安全附件的邮件将被提供给用户。如果清除失败，应用程序会在邮件主题中添加警告信息。然后，带有原始附件的邮件将被提供给用户。如果在发送邮件中检测到感染对象，应用程序会阻止该邮件，邮件客户端会显示错误。<br>• `Block`。如果在传入邮件中检测到感染对象，应用程序会在邮件主题中添加警告。然后，带有原始附件的邮件将被提供给用户。如果在发送邮件中检测到感染对象，应用程序会阻止该邮件，邮件客户端会显示错误。 |

# 如何优化邮件附件扫描

配置邮件附件扫描以优化邮件威胁防护组件。这有助于降低受保护设备的 CPU 使用率。您可以限制对附件中压缩文件的扫描，设置可扫描附件的最大大小，以及设置对象扫描的最长持续时间。

### 如何在 Web Console 中优化附件扫描

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护 → 邮件威胁防护**。
5. 在“**高级设置**”下，选择“**扫描设置**”选项卡。
6. 配置附件扫描：

   - “**扫描附加存档**”。这包括扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他类型的压缩文件。应用程序不仅可通过扩展名识别文件，还可通过格式识别文件。在扫描压缩文件时，应用程序会递归解包。这样就可以检测嵌套压缩文件（压缩文件中的压缩文件）中的威胁。
   - “**扫描 Office 格式的附件**”。扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。无论是否选中此复选框，应用程序都会扫描小于 1 MB 的 Office 格式附件。
   - “**不扫描大小大于该值(MB)的压缩包**”。如果选中此复选框，邮件威胁防护将不会扫描任何大于指定限制的压缩文件附件。如果取消选中此复选框，邮件威胁防护将扫描任何大小的压缩文件附件。
   - “**跳过扫描时间超过以下值的文件(秒)**”。如果选中此复选框，则会限制电子邮件附件中压缩文件的扫描持续时间。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行上优化附件扫描

1. 确保邮件威胁防护组件已启用：

```
kesl-control --get-task-state 35
```

2. 该组件必须处于 `Started` 状态。

3. 如果组件已禁用，请运行以下命令：

```
kesl-control --start-task 35
```

4. 选择在传入邮件中检测到邮件威胁时要执行的操作：

```
kesl-control --set-settings 35 [ScanFileArchive=<Yes|No>] [UseSizeLimit=<Yes|No>] [SizeLimit=<archive size (MB)>] [UseTimeLimit=<Yes|No>] [TimeLimit=<scan time (sec)>] [ScanFileOffice=<Yes|No>]
```

5. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 35
```

### 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ScanFileArchive` | 这包括扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他类型的压缩文件。应用程序不仅可通过扩展名识别文件，还可通过格式识别文件。在扫描压缩文件时，应用程序会递归解包。这样就可以检测嵌套压缩文件（压缩文件中的压缩文件）中的威胁。默认情况下，应用程序会扫描附件中的压缩文件。 |
| `UseSizeLimit`<br>`SizeLimit` | 限制可扫描的附件中压缩文件的大小。如果附件中压缩文件的大小超过指定值，邮件威胁防护会在扫描时跳过该压缩文件。默认情况下，应用程序会扫描任意大小的压缩文件。 |
| `UseTimeLimit`<br>`TimeLimit` | 扫描附件中压缩文件的时间限制。默认情况下，扫描附件中压缩文件的时间不受限制。 |
| `ScanFileOffice` | 扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。无论是否选中此复选框，应用程序都会扫描小于 1 MB 的 Office 格式附件。默认情况下，应用程序会扫描附件中的 Office 格式文件。 |

## 电子邮件附件过滤器的用途

附件过滤器不适用于传出电子邮件。

恶意应用程序会以电子邮件附件的形式传播。您可以根据邮件附件类型配置筛选，银边指定类型的文件可以被自动重命名或删除。通过重命名某种类型的附件，Kaspersky Endpoint Security 可以保护您的计算机，防御恶意应用程序的自动执行。

例如，您可以为 HTML 文件配置附件过滤。HTML 文件可能包含恶意脚本。如果应用程序重命名此类文件，用户将无法通过双击电子邮件中的该文件来打开 HTML 页面。要打开 HTML 文件，用户需要下载该文件并对其重命名。这样，用户就有时间分析收到的邮件，并阻止恶意脚本启动。

默认情况下，应用程序会重命名扩展名为 CMD、COM、EXE、JS、JSE、MSI、SCR、VBE、VBS 和 SH 的文件。应用程序会将指定文件类型的扩展名最后一个字符替换为下划线字符（例如，attachment.doc_）。

### 如何在 Web Console 中配置附件过滤器

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护 → 邮件威胁防护**。
5. 在“**高级设置**”下，选择“**附件过滤器**”选项卡。
6. 选择应用程序将对电子邮件附件执行的操作：
   - “**不修改附件**”。如果选择此选项，邮件威胁防护将不会筛选电子邮件附件。
   - “**重命名选定类型的附件**”。如果选择此选项，邮件威胁防护会将指定文件类型的扩展名的最后一个字符替换为下划线字符（例如 attachment.doc_）。因此，用户需要重命名文件才能打开它。
   - “**删除选定类型的附件**”。如果选择此选项，邮件威胁防护将从电子邮件中删除指定类型的附件。
7. 如果在上一步中选择了 **重命名选定类型的附件** 或 **删除选定类型的附件** 选项，请选中相关文件类型对应的复选框。
8. 如果未列出您需要的文件类型，请添加新的附件类型：
   a. 单击“**添加**”。
      这将打开用于添加新附件类型的表单。
   b. 在 **附件类型** 字段中，以 `*.<extension>`（例如，`*.doc`）格式指定扩展名掩码。
      如果要指定多个文件类型，请在新行输入每种文件类型。
9. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行配置附件过滤器

1. 确保邮件威胁防护组件已启用：

```
kesl-control --get-task-state 35
```

2. 该组件必须处于 `Started` 状态。
3. 如果组件已禁用，请运行以下命令：

```
kesl-control --start-task 35
```

4. 选择应用程序将对电子邮件附件执行的操作：

```
kesl-control --set-settings 35 ExtensionFilter=<Disable|Rename|Delete>
ExtensionMasks.item_#.UseExtensionMask=Yes\
[ExtensionMasks=*.<extention>]
```

5. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 35
```

### 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ExtensionFilter` | 应用程序将对电子邮件附件执行的操作：<br>`Disable`。如果选择此选项，邮件威胁防护将不会筛选电子邮件附件。<br>`Rename`（默认）。如果选择此选项，邮件威胁防护会将指定文件类型的扩展名的最后一个字符替换为下划线字符（例如 attachment.doc_）。因此，用户需要重命名文件才能打开它。<br>`Delete`。如果选择此选项，邮件威胁防护将从电子邮件中删除指定类型的附件。 |
| `UseExtensionMask=Yes` | 将文件类型添加到附件过滤器。<br>您可以暂时从附件过滤器中排除某种文件类型，而不是删除该文件类型。为此，请设置 `ExtensionMasks.item_#.UseExtensionMask=No` |
| `ExtensionMasks=*.<extention>` | 要重命名或从电子邮件中删除的附件类型的扩展名。 |

# Web 威胁防护

“Web 威胁防护”组件可防止从 Internet 下载恶意文件，同时阻止连接到恶意网站和钓鱼网站。该组件借助反病毒数据库、卡巴斯基安全网络云服务和启发式分析来提供计算机保护。

## Web 威胁防护的工作原理

安装 Kaspersky Endpoint Security 时，应用程序会添加一个自签名证书 *卡巴斯基反病毒个人根证书*。应用程序会将此证书放入本地受信任的证书存储区 (`/etc/ssl/certs`) 和 Web 浏览器的证书存储区中。每次应用程序启动时，都会检查证书是否存在。如果证书已被删除，应用程序会自动恢复该证书。

1. **拦截传出连接**

   第三方应用程序（例如浏览器）发起与服务器的连接。Kaspersky Endpoint Security 会将服务器证书替换为由卡巴斯基反病毒个人根证书签名的自有证书。接下来，应用程序会拦截加密密钥并解密通信会话。Kaspersky Endpoint Security 会在不提醒用户的情况下执行此操作，因为卡巴斯基反病毒个人根证书位于受信任的证书存储区中。

2. **扫描网络流量**

   Web 威胁防护使用以下技术扫描流量：

   - 反病毒数据库。
   - 卡巴斯基安全网络的云服务。
   - 启发式分析技术能够检测卡巴斯基数据库尚未涵盖的威胁。

3. **扫描完成**

   如果某个网站被归类为恶意网站或网络钓鱼网站，Kaspersky Endpoint Security 会执行 Web 威胁防护组件设置中指定的操作：阻止连接或显示警告。

Web 威胁防护设置

### 1 配置操作系统的 Firewall 规则

如果系统已配置自己的网络规则或包含 Drop 策略的 firewalld 规则，则为了确保应用程序正常工作，您需要添加一条规则，以允许来自本地设备（环回）的传入连接：

iptables 的命令示例：

```
iptables -A INPUT -i lo -j ACCEPT
```

### 2 选择网络流量拦截模式

收到网络数据包时，Web 威胁防护会提取数据以扫描威胁。网络流量拦截可以使用以下模式：

- eBPF
- iptables（默认）

网络流量拦截模式的选择取决于组织的基础设施。在封闭边界中，我们建议使用 eBPF。在其他场景下，请使用 iptables。

我们建议根据网络流量拦截模式将设备分组到不同的管理组中。

### 3 配置证书验证策略

默认情况下，Web 威胁防护会解密并扫描通过加密连接发送的网络流量。在此过程中，组件会利用互联网进行验证，并下载验证证书所需的缺失证书链。如果设备无法直接访问互联网，则必须选择本地证书验证方法（不使用互联网）或使用代理服务器访问互联网。

证书验证策略还包括以下设置：

- 访问使用不受信任证书的网站
- 访问存在证书验证错误的网站

默认情况下，Kaspersky Endpoint Security 允许导航到带有不受信任证书的网站，并将带有证书验证错误的域添加到排除项。例如，使用银行应用程序或云存储时可能会发生证书验证错误。这些服务所属的域可能会拒绝卡巴斯基反病毒个人根证书。您可以配置自己的证书验证策略。

### 4 添加受信任证书

如果您的组织使用私有证书颁发机构为内部服务器颁发证书，Kaspersky Endpoint Security 可能会因证书验证错误而阻止对 Web 资源的访问。请将这些证书添加到受信任列表，以从加密连接扫描中排除 Web 资源。

### 5 在 Web 威胁防护设置中，选择“通知”操作

默认情况下，“Web 威胁防护”任务被禁用。建议启用 Web 威胁防护，并将检测到威胁后的操作设置为**通知**，然后检查对所有企业资源的访问。Kaspersky Endpoint Security 允许访问所有网站，并记录有关检测到的威胁的信息。

### 6 收集 Web 威胁防护认为不安全的网站的统计信息

您可以使用报告获取 Web 威胁防护认为不安全的网站的统计信息。

7. **添加受信任的网址**

   查看 Web 威胁防护报告后，您需要将信任的网址添加到受信任列表。如果受信任的网址列表不足以解决 Kaspersky Endpoint Security 应用程序与第三方应用程序之间的冲突，您可以使用特殊的允许规则链 kesl_bypass。*kesl_bypass 链*是 Kaspersky Endpoint Security 在操作系统防火墙的 mangle 表（iptables/ip6tables）中创建的特殊规则列表。

8. **在 Web 威胁防护设置中，选择“阻止”操作**

   启用阻止 Web 流量中的受感染对象。

特殊注意事项和限制

- 应用程序会扫描 TCP 端口上的传入流量，并使用 localhost 上的 9879 端口拦截连接。如果 9879 端口已被占用，应用程序会自动选择任一可用端口来拦截连接。
- 启用或禁用应用程序以及启用或禁用 Web 威胁防护和网络威胁防护组件会终止被拦截端口上的连接。
- Kaspersky Endpoint Security 扫描 HTTP 和 HTTPS 流量。Kaspersky Endpoint Security 扫描 URL 和 IP 地址。
- 应用程序支持以下浏览器可执行文件，包括 snap 格式的可执行文件：
  - chrome
  - chromium
  - chromium-browser
  - firefox
  - firefox-esr
  - google-chrome
  - opera
  - yandex-browser
- 如果用户尝试访问恶意网站，应用程序将执行以下操作：
  - **HTTP**。应用程序会阻止访问并显示警告。
  - **HTTPS**。应用程序会阻止访问；浏览器显示错误页面。
- 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。

实用文章

收到“正在访问证书不受信任的域”警告时该怎么办

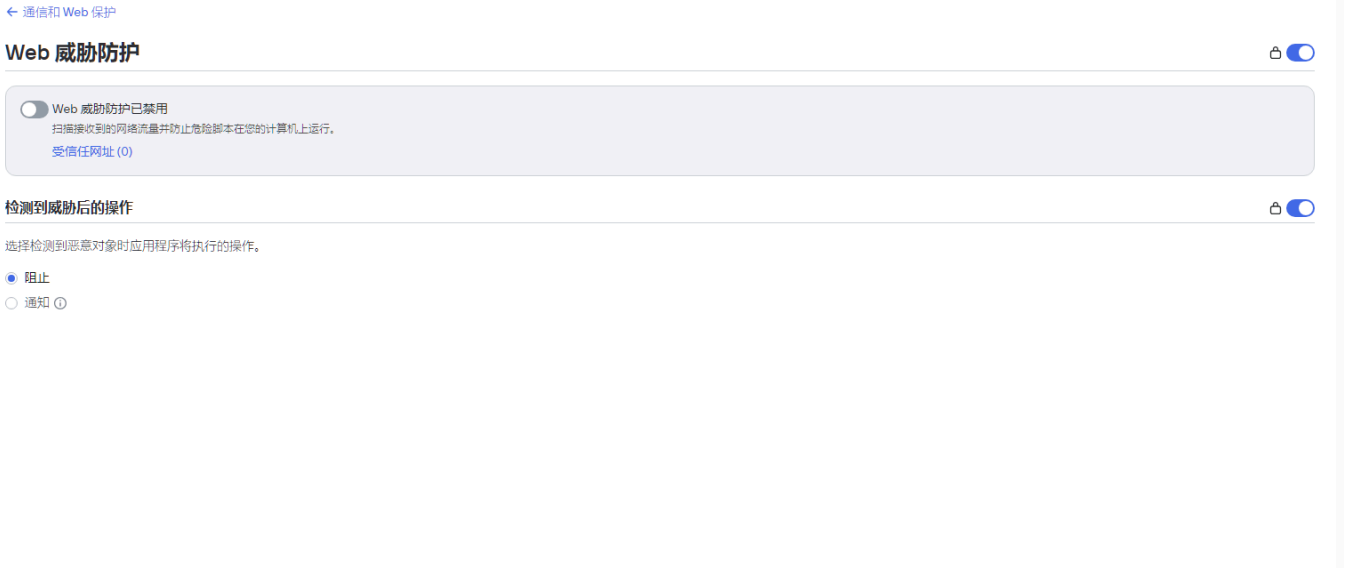
# 如何选择检测到 Web 威胁时的操作

检测到 Web 威胁时，Kaspersky Endpoint Security 可以阻止对危险对象的访问，或仅通知检测到危险对象。

### 如何在 Web Console 中配置检测到 Web 威胁时的操作

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **Web 威胁防护**。
5. 在 **检测到威胁后的操作** 下，选择应用程序在检测到威胁时将执行的操作：
   - “**阻止**”。如果选择此选项并且在 Web 流量中检测到受感染对象，“Web 威胁防护”组件将阻止访问对象并在浏览器中显示一条消息。
   - “**通知**”。Kaspersky Endpoint Security 会通知用户在 Web 流量中检测到受感染对象。Web 威胁防护允许将此对象下载到设备。同时，应用程序记录关于受感染对象的信息并将其添加到活动威胁列表中。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




Web 威胁防护

### 如何在命令行中配置检测到威胁时的操作

1. 运行以下命令：

```
kesl-control --set-settings 14 ActionOnDetect=<Block|Notify>
```

2. 选择要用于扫描链接的数据库：

```
kesl-control --set-settings 14 CheckMalicious=<Yes|No> CheckAdware=<Yes|No> CheckOther=<Yes|No>
```

3. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 14
```

### 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ActionOnDetect` | 检测到威胁后的操作：<br>• `Block`（默认）。如果选择此选项并且在 Web 流量中检测到受感染对象，“Web 威胁防护”组件将阻止访问对象并在浏览器中显示一条消息。<br>• `Notify`。如果选择此选项并在 Web 流量中检测到受感染对象，Kaspersky Endpoint Security 将允许将该对象下载到计算机，但会将受感染对象的相关信息添加到活动威胁列表中。 |
| `CheckMalicious` | 扫描链接以决定它们是否被包含在恶意网址数据库中，这样您可以跟踪被列入拒绝列表的网站。恶意网址数据库由 Kaspersky 维护，包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。默认情况下启用扫描（`Yes`）。 |
| `CheckAdware` | 根据广告网址数据库检查链接。默认情况下禁用扫描（`No`）。 |
| `CheckOther` | 根据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数据库检查链接。默认情况下禁用扫描（`No`）。 |

## 什么是反钓鱼

Web 威胁防护检查链接以查看它们是否属于钓鱼网址。这将帮助防止*钓鱼攻击*。钓鱼攻击常常带有伪装，比如从您银行发来的带有银行官方网站链接的电子邮件消息。单击此链接，您将进入银行网站的完整复制网站，甚至可以在浏览器地址栏看到其真实地址，即使您在假网站上。从此刻起，您在网站上的所有操作都将被跟踪，进而用来窃取您的金钱。

由于钓鱼网站的链接不仅能通过电子邮件消息传送，而且还可能来自其他来源（例如聊天软件），因此“Web 威胁防护”组件将在 Web 流量扫描级别监视访问钓鱼网站的尝试并阻止对此类网站的访问。Kaspersky Endpoint Security 分发套装中包含了钓鱼网址列表。

您只能通过命令行配置反钓鱼功能。您无法在 Web Console 中配置反钓鱼。默认下，带有启发式分析的反钓鱼被启用。

*如何通过命令行启用反钓鱼*

1. 确保已启用 Web 威胁防护组件：

```
kesl-control --get-task-state 14
```

组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

```
kesl-control --start-task 14
```

3. 启用反钓鱼：

```
kesl-control --set-settings 14 CheckPhishing=Yes
```

4. 配置启发式分析以扫描网页中的钓鱼链接：

```
kesl-control --set-settings 14 UseHeuristicForPhishing=<Yes|No>
```

此设置不适用于配备 Elbrus CPU 的设备。

5. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 14
```

# 网络威胁防护

*网络威胁防护组件*组件（也称Intrusion Detection System，IDS）监控入站网络流量以查找网络攻击的活动特征。当应用程序在用户计算机上检测到网络攻击企图时，它将阻止与攻击计算机的网络连接。应用程序数据库提供了当前已知类型的网络攻击以及应对方法的描述。“网络威胁防护”组件检测到的网络攻击列表在数据库和应用程序模块更新期间更新。

## 网络威胁防护的工作原理

1. **应用程序分析传入数据包**

   为了扫描传入流量，“网络威胁防护”组件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 iptables 流量拦截模式下执行网络扫描期间，设备上可能看起来存在开放端口，即使系统上没有任何应用程序正在侦听此端口。我们建议通过 Firewall 关闭未使用的端口。

2. **应用程序扫描传入流量**

   网络威胁防护使用以下技术扫描传入流量：

   - 反病毒数据库。
   - 卡巴斯基安全网络的云服务。
   - 启发式分析技术能够检测卡巴斯基数据库尚未涵盖的威胁。

3. **扫描完成**

   当检测到网络威胁时，应用程序会在指定时间内阻止来自攻击设备的所有网络连接。

网络威胁防护设置

### 1 配置操作系统的 Firewall 规则

为确保 REDIRECT 规则（例如，从端口 443 重定向到 8443）与网络威胁防护的拦截规则兼容，您需要删除 REDIRECT 规则并添加拦截规则。

删除 REDIRECT 规则的命令示例：

```
iptables -t nat -D PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
```

添加拦截规则的命令示例：

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
```

```
iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT -
-to-destination :8443
```

### 2 创建受监控网络端口的列表

默认情况下，应用程序会监控已知和已注册的端口，例如，用于 HTTPS 连接的端口 443、用于 IMAP 邮件协议的端口 143。默认设置提供建议的保护级别和最佳资源使用。如有必要，您可以更改受监控端口的列表或启用对所有端口的监控。

### 3 选择流量拦截模式

收到网络数据包时，网络威胁防护会提取数据以扫描威胁。可以使用以下模式拦截传入流量：

- eBPF
- iptables（默认）

流量拦截模式的选择取决于组织的基础设施。在封闭边界中，我们建议使用 eBPF。在其他场景下，请使用 iptables。

> 我们建议根据流量拦截模式将设备分组到不同的管理组中。

### 4 以通知模式启用 Web 威胁防护

默认情况下，网络威胁防护处于禁用状态。以阻止模式启用网络威胁防护之前，我们建议以通知模式启用该组件。这样，Kaspersky Endpoint Security 便可检测可疑的网络活动，并记录有关检测到的网络攻击的信息，而不会中断网络连接。检查第三方企业应用程序对网络资源的访问权限。确保网络端口控制不会降低这些应用程序的运行速度。

### 5 收集网络威胁防护观察到可疑网络活动的 IP 地址统计信息

您可以查看报告，以获取网络威胁防护认为不安全的 IP 地址的统计信息。应用程序生成 *检测到网络攻击* 事件。

### 6 添加受信任的 IP 地址

查看网络威胁防护报告后，您需要将您信任其网络连接的设备的 IP 地址添加到受信任列表。您可以将单个设备或子网的地址添加到排除列表。网络威胁防护不会拦截或扫描来自此类设备的数据包。

7. **以阻止模式启用网络威胁防护**

   将受信任设备的 IP 地址添加到排除列表后，以阻止模式启用该组件。不受信任设备的网络活动会被阻止，相关信息会显示在报告中。

特殊注意事项和限制

- 应用程序会扫描 TCP 端口的传入流量。应用程序使用 localhost 上的固定端口 9789 来拦截连接。
- 启用或禁用应用程序以及启用或禁用 Web 威胁防护和网络威胁防护组件会终止被拦截端口上的连接。
- 由于缺少 TProxy 支持，网络威胁防护无法在运行 CentOS 5.2 和 5.4 的计算机上运行。

# 如何选择检测到网络威胁时的操作

如果检测到对受保护设备的网络攻击企图，应用程序会阻止来自攻击设备的网络活动并创建 *检测到网络攻击* 事件。

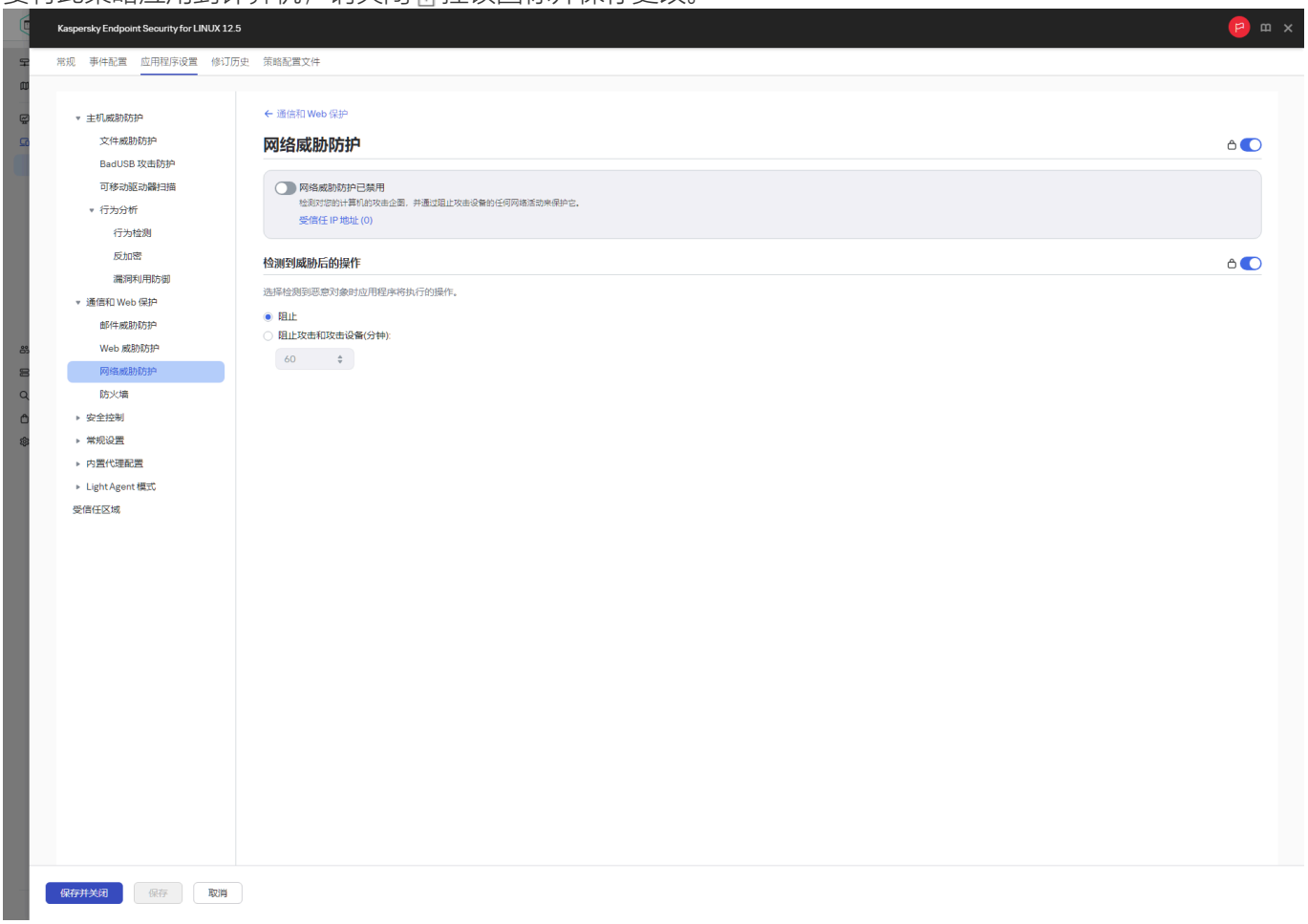
为了阻止网络流量，Kaspersky Endpoint Security 会创建一条动态防火墙规则。防火墙会临时阻止攻击设备的网络流量。该应用程序还会将受侵设备添加到被阻止设备列表。被阻止的设备无法访问共享网络目录。

**如何在 Web Console 中配置检测到网络攻击时的操作**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护 → 网络威胁防护**。
5. 确保该组件的切换开关处于 **网络威胁防护已启用** 位置。
6. 选择**为 Linux 设备启用网络威胁防护**复选框。
7. 在 **检测到威胁后的操作** 下，选择应用程序在检测到威胁时将执行的操作：**阻止** 或 **阻止攻击和攻击设备(分钟)**。
8. 如果选择了 **阻止攻击和攻击设备(分钟)**，请设置受侵设备的阻止持续时间（以分钟为单位）。默认情况下，设备会被阻止 60 分钟。有效值为 1 到 999。

9. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




网络威胁防护

## 如何在命令行中配置检测到网络攻击时的操作

1. 确保已启用网络威胁防护组件：

```
kesl-control --get-task-state 17
```

组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

```
kesl-control --start-task 17
```

3. 选择检测到网络威胁时的操作：

```
kesl-control --set-settings 17 ActionOnDetect=<Block|Notify>
```

4. 配置对受侵设备的阻止：

```
kesl-control --set-settings 17 BlockAttackingHosts=<Yes|No>
```

5. 选择 `BlockAttackingHosts=Yes` 操作的阻止时长：

```
kesl-control --set-settings 17 BlockDurationMinutes=<Blocking period>
```

6. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 17
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ActionOnDetect` | 检测到网络威胁时的操作：<br>• `Block`（默认）阻止受侵设备的网络流量并创建 *检测到网络攻击* 事件。<br>• `Notify` 创建 *检测到网络攻击* 事件，但不阻止网络流量。 |
| `BlockAttackingHosts` | 阻止攻击设备的网络活动。默认情况下，已启用设备阻止。 |
| `BlockDurationMinutes` | 配置涉及恶意活动或恶意数据加密的远程设备的阻止时长。 |

# 如何管理被阻止的设备

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。反加密勒索和 网络威胁防护 组件保护设备免受此类威胁。Kaspersky Endpoint Security 会在一段时间内阻止网络流量。当阻止期结束时，Kaspersky Endpoint Security 允许网络流量恢复。默认情况下，应用程序会阻止攻击设备的网络流量 60 分钟。当阻止时间到期时，应用程序会将此设备从被阻止的设备列表中移除。

如果 Kaspersky Endpoint Security 阻止了受信任设备，您需要将此设备的 IP 地址添加到 排除列表。

如何查看被阻止的设备列表

```
kesl-control -H --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。

被阻止的设备列表

```
Blocked devices: 1
Host                : 10.69.119.234
Block date          : 2026-04-29 15:44
Will be unblocked   : 2026-04-29 16:44
Task name           : Network_Threat_Protection
```

如何取消阻止设备

```
kesl-control -H --allow-hosts <address>
```

其中 `<address>` 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。

# 防火墙管理

操作系统的防火墙控制设备的所有网络活动，无论是互联网上的活动还是本地网络上的活动。防火墙保护设备上的数据免遭未经授权的访问，并阻止大多数威胁，例如来自网络的设备攻击。防火墙可以检测用户设备上的所有网络连接，并获取这些网络连接的 IP 地址列表。

应用程序使用防火墙管理组件来管理操作系统的防火墙。该组件会向操作系统的防火墙添加 网络包规则，以监控设备的网络活动。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。

默认禁用防火墙管理组件。

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。

如果启用了防火墙管理，Kaspersky Endpoint Security 会每 60 秒检查一次操作系统的防火墙。如果检查发现第三方应用程序或实用程序添加或删除了网络包规则，Kaspersky Endpoint Security 将恢复使用本应用程序创建的防火墙规则集。

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恢复动态规则。

启用 Firewall 管理组件之前，请执行以下操作：

- 禁用其他管理操作系统防火墙的工具。
- 在启用防火墙管理组件之前，请保存并备份所有已配置的自定义防火墙规则。

# 如何创建网络包规则

Firewall 根据*网络包规则*过滤受保护设备上的所有网络活动。网络包规则会限制网络包或连接，而不考虑应用程序。规则根据以下条件允许或拒绝网络活动：

- 连接协议和端口
- 流量方向
- 发送或接收网络流量的设备的 IP 地址

## 网络包规则的优先级

默认情况下，所有传出数据包和连接。默认规则的优先级最低：如果未触发其他网络包规则，或者未指定其他网络包规则，则允许该活动。

Firewall 按优先级顺序应用网络包规则。规则的优先级是其在列表中的位置，从上到下排列。Firewall 按列表中的第一条规则过滤网络连接，并允许或阻止网络活动。如果规则不匹配，Firewall 将应用列表中的下一条规则，依此类推，直至列表末尾。然后，该组件会忽略该连接的匹配规则之后的所有网络包规则。

创建网络包规则的建议

要在命令行中创建网络包规则，可以使用命令行选项或配置文件。如果要添加多条规则，请使用配置文件进行添加。

使用命令行选项逐条添加大量规则可能会导致 CPU 负载激增。

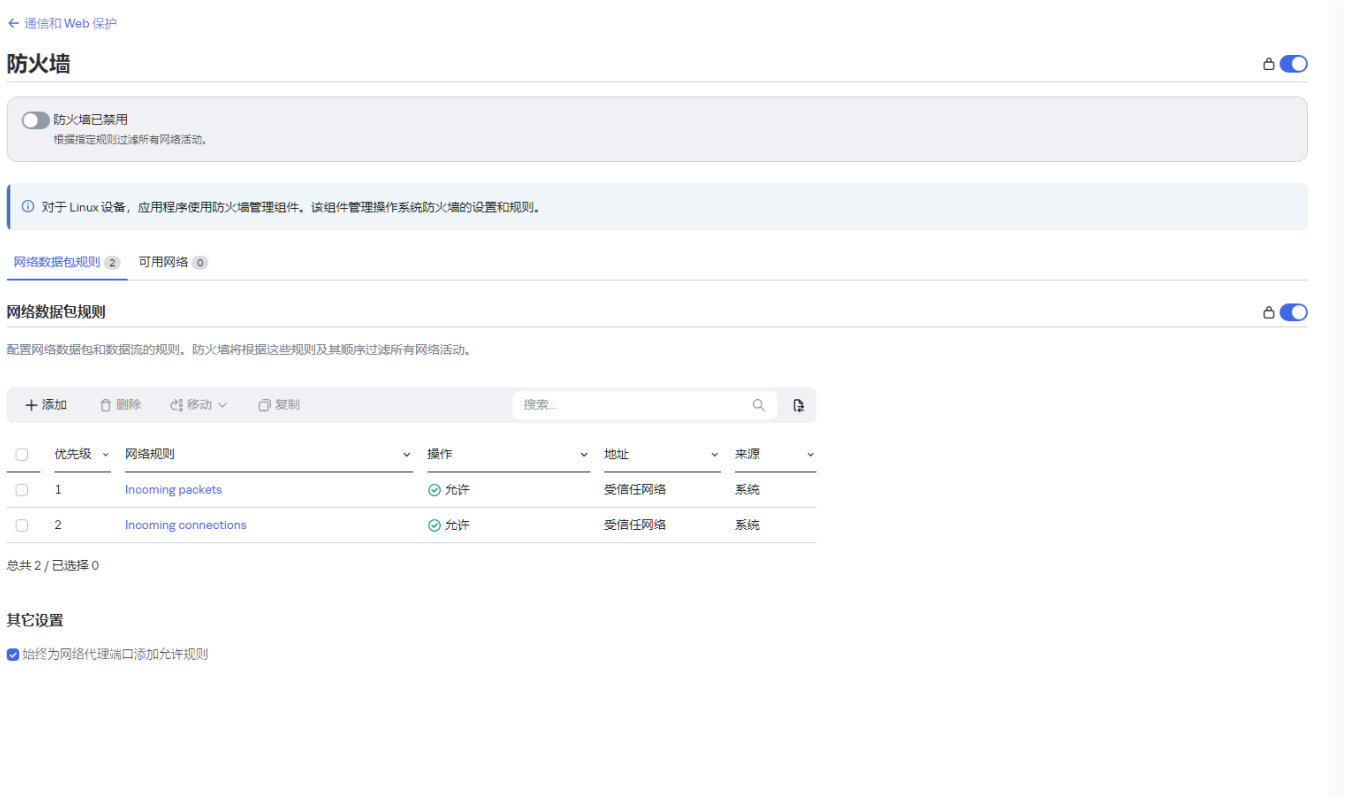
**如何在 Web Console 中创建网络包规则**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择“**通信和 Web 保护**”→“**防火墙**”。
5. 确保该组件的切换开关处于 **防火墙已启用** 位置。
6. 在“**网络数据包规则**”选项卡上单击“**添加**”按钮。
   这将打开新的网络规则表单（见下图）。
7. 在“**规则名称**”字段中输入规则的名称。
   您可以通过单击**选择规则模板**链接选择预定义的规则模板。规则模板包含最常用网络连接的设置。
   除优先级以及 Firewall 对连接应用的操作外，网络规则的所有设置都会自动填充。
8. 在“**优先级**”字段中，指定规则的优先级。默认情况下，将以最高优先级创建规则。
9. 在“**操作**”下，选择触发规则时希望 Firewall 如何处理网络活动：**允许** 或 **阻止**。
10. 在“**方向**”字段中，选择希望规则应用于哪些网络活动：
    - “**入站**”。防火墙应用网络规则到所有入站网络包。
    - “**入站(包)**”。防火墙应用网络规则到所有通过由远程计算机发起的网络连接发送的网络包。
    - “**入站/出站**”。防火墙将为接收和发送的网络数据包应用网络规则，与该网络连接的发起者是用户计算机还是远程计算机无关。
    - “**出站(包)**”。防火墙应用网络规则到所有出站网络包。
    - “**出站**”。防火墙应用网络规则到所有通过由用户计算机发起的网络连接发送的网络包。
    - “**入站/出站(包)**”。防火墙应用网络规则到所有入站和出站网络包。
11. 如果您希望将网络规则的操作反映在报告中，请选中“**记录事件**”复选框。根据规则的操作，应用程序会创建 *网络活动已阻止* 或 *网络活动已允许* 事件。
12. 在“**协议设置**”选项卡上，选择希望规则过滤其网络活动的协议。
13. 转到“**远程网络地址**”选项卡。

14. 在“**远程**”字段中，指定可以发送和接收网络包的远程计算机的网络地址：Firewall 会将规则应用于指定的地址。

15. 在“**本地**”字段中，指定安装了 Kaspersky Endpoint Security 且可以发送和接收网络包的计算机的网络地址：Firewall 会将规则应用于指定的地址。

16. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




防火墙

## 如何在命令行中创建网络包规则

1. 确保已启用防火墙管理：

   ```
   kesl-control --get-task-state 12
   ```

   组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

   ```
   kesl-control --start-task 12
   ```

3. 添加新的网络包规则：

   ```
   kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
   <direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
   ```

   如果要添加多条规则，请使用配置文件进行添加：

   a. 将该组件的设置输出到配置文件：

      ```
      kesl-control --get-settings 12 --file <path to file> [--json]
      ```

b. 打开配置文件，并添加包含以下节的网络包规则：

```
[PacketRules.item_#]
Name=<rule name>
FirewallAction=<Allow|Block>
Protocol=<protocol>
Direction=<direction>
RemoteAddress=<remote address>
LocalAddress=<local address>
LogAttempts=<Yes|No>
```

c. 将配置文件中的设置导入到应用程序中：

```
kesl-control --set-settings 12 --file <path to file> [--json]
```

4. 要查看网络包规则列表，请运行以下命令：

```
kesl-control -F --query
```

应用程序会按以下格式显示所有网络包规则的列表：`<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`。

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `--name <rule name>`<br>`Name` | 网络数据包规则名称。默认情况下为 `Packet rule #<n>`。 |
| `--action`<br>`FirewallAction` | 将针对此网络数据包规则中指定的连接执行的操作。<br>• `Allow`（默认）允许连接。<br>• `Block` 阻止连接。 |
| `--protocol`<br>`Protocol` | 要监控其网络活动的协议类型。<br>• `Any`（默认）表示 Firewall 控制所有网络活动<br>• `TCP`<br>• `UDP`<br>• `ICMP`<br>• `ICMPv6`<br>• `IGMP`<br>• `GRE` |
| `--direction`<br>`Direction` | 受监控网络活动的方向：<br>• `IncomingOutgoing` 或 `InOut`（默认）。防火墙应用网络规则到所有入站和出站网络包。<br>• `Incoming` 或 `In`。防火墙应用网络规则到所有通过由远程计算机发起的网络连接发送的网络包。<br>• `Outgoing` 或 `Out`。防火墙应用网络规则到所有通过由用户计算机发起的网络连接发送的网络包。<br>• `IncomingPacket` 或 `InPacket`。防火墙应用网络规则到所有入站网络包。<br>• `OutgoingPacket` 或 `OutPacket`。防火墙应用网络规则到所有出站网络包。<br>• `IncomingOutgoingPacket` 或 `InOutPacket`。防火墙将为接收和发送的网络数据包应用网络规则，与该网络连接的发起者是用户计算机还是远程计算机无关。 |

| 设置 | 描述 |
| --- | --- |
| `--remote <remote address[:<port>]>`<br>`RemoteAddress=<remote address>` | 远程设备的 IP 地址：<br>• `Any`（默认）启用对具有任意 IP 地址的远程设备发送和/或接收的网络数据包的监控。<br>• `Trusted` 是为可信网络配置的网络区域。<br>• `Local` 是为本地网络配置的网络区域。<br>• `Public` 是为公用网络配置的网络区域。<br>• `d.d.d.d` 是 IPv4 地址，其中 d 是 0 到 255 之间的十进制数。<br>• `d.d.d.d – d.d.d.d` 是 IPv4 地址范围。<br>• `d.d.d.d/p` 是 IPv4 子网，其中 p 是 0 到 32 之间的数字。<br>• `x:x:x:x:x:x:x:x` 是 IPv6 地址，其中 x 是 0 到 ffff 之间的十六进制数。<br>• `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` 是 IPv6 地址范围。<br>• `x:x:x:x:x:x:x:x/p` 是 IPv6 地址子网，其中 p 是 0 到 128 之间的数字；为简洁起见，您可以使用 `::`。<br>您还可以指定远程端口：<br>• `Any`（默认）用于监控所有远程端口<br>• `0 – 65535`。 |
| `--local <local address[:<port>]>`<br>`LocalAddress=<local address>` | 安装了 Kaspersky Endpoint Security 的设备的网络地址：<br>• `Any`（默认）用于监控具有任意 IP 地址的本地设备发送和/或接收的网络数据包。<br>• `Trusted` 是为可信网络配置的网络区域。<br>• `Local` 是为本地网络配置的网络区域。<br>• `Public` 是为公用网络配置的网络区域。<br>• `d.d.d.d` 是 IPv4 地址，其中 d 是 0 到 255 之间的十进制数。<br>• `d.d.d.d – d.d.d.d` 是 IPv4 地址范围。<br>• `d.d.d.d/p` 是 IPv4 子网，其中 p 是 0 到 32 之间的数字。<br>• `x:x:x:x:x:x:x:x` 是 IPv6 地址，其中 x 是 0 到 ffff 之间的十六进制数。<br>• `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` 是 IPv6 地址范围。<br>• `x:x:x:x:x:x:x:x/p` 是 IPv6 地址子网，其中 p 是 0 到 128 之间的数字；为简洁起见，您可以使用 `::`。<br>您还可以指定本地端口：<br>• `Any`（默认）用于监控所有本地端口<br>• `0 – 65535`。 |
| `--at <index>` | 规则在网络数据包规则列表中的索引。如果未指定 `--at` 选项或其值大于列表中的规则数，则新规则将添加到列表末尾。 |
| `LogAttempts` | 在报告中包含网络规则操作的记录。<br>• `Yes`—在报告中记录操作。<br>• `No`（默认值）—不在报告中记录操作。 |

阻止到 TCP 端口 23 的所有传入和已建立的连接的规则示例

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote any
```

阻止公用网络区域通过 TCP 端口 23 的传入和已建立的连接的规则示例

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote Public
```

# 网络包规则使用示例

### 1 仅允许本地网络中的一台特定计算机访问互联网，并阻止所有其他计算机访问

允许计算机 (192.168.2.22) 通过 TCP 协议访问互联网的规则：

```
kesl-control --add-rule --name InternetAccess --action Allow --protocol TCP --local 192.168.2.22
```

用于互联网访问被阻止的其他计算机的规则：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.1.0/24
```

**2 仅阻止本地网络上的一台特定计算机访问互联网**

用于互联网访问被阻止的计算机 (192.168.2.23) 的规则：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.23
```

**3 阻止从本地网络访问特定网站**

本地网络上的计算机被拒绝通过 HTTP 访问 example.com (91.198.174.192) 的规则：

```
kesl-control --add-rule --name ExampleHTTP --action Block --protocol TCP --remote 91.198.174.192:80
```

本地网络上的计算机被拒绝通过 HTTPS 访问 example.com (91.198.174.192) 的规则：

```
kesl-control --add-rule --name ExampleHTTPS --action Block --protocol TCP --remote 91.198.174.192:443
```

**4 仅允许本地网络上的一台特定计算机访问一个指定网站**

允许计算机 (192.168.2.24) 通过 HTTP 访问 example.com (91.198.174.192) 的规则：

```
kesl-control --add-rule --name ExampleHTTP --action Allow --protocol TCP --remote 91.198.174.192:80 --local
192.168.2.24
```

允许计算机 (192.168.2.25) 通过 HTTPS 访问 example.com (91.198.174.192) 的规则：

```
kesl-control --add-rule --name ExampleHTTPS --action Allow --protocol TCP --remote 91.198.174.192:443 --local
192.168.2.25
```

用于阻止计算机 (192.168.2.26) 访问互联网的规则：

```
kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.26
```

# 如何将 IP 地址添加到网络区域：公共、本地、受信任

防火墙允许监控*网络区域*的网络活动。网络区域是指归入同一种网络连接类型的一组 IP 地址或子网。您可以使用预定义的网络区域，对多个 IP 地址或子网重复使用规则，而无需为每个 IP 地址或子网创建单独的规则。

Kaspersky Endpoint Security 区分三种网络区域：

- “**公用网络**”。网络不受反病毒应用程序、防火墙或过滤器保护（例如咖啡馆中的 Wi-Fi）。当用户操作连接到此类网络的计算机时，防火墙会阻止访问此计算机的文件和打印机。外部用户也无法通过共享文件夹访问数据和远程访问该计算机的桌面。
- “**本地网络**”。为对此计算机上的文件和打印机具有受限访问权限的用户提供的网络（例如企业 LAN 或家庭网络）。
- “**受信任网络**”。其中的计算机不会暴露于攻击或未经授权的数据访问尝试的安全网络。防火墙允许在具有此状态的网络中进行任何网络活动。

**如何在 Web Console 中将 IP 地址添加到网络区域**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择“**通信和 Web 保护**”→“**防火墙**”。
5. 转到“**可用网络**”选项卡。
6. 单击“**添加**”。
   这将打开用于添加新网络连接的表单。
7. 在“**名称**”字段中，输入网络连接的名称。
8. 在“**网络类型**”字段中，选择网络连接所属的网络区域：**公用网络**、**本地网络**、**受信任网络**。
9. 在“**IP 地址**”字段中，指定将与网络连接关联的 IP 地址或子网。
10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中将 IP 地址添加到网络区域**

1. 确保已启用防火墙管理：

   ```
   kesl-control --get-task-state 12
   ```

   组件必须处于 **已启动** 状态。
2. 如果组件已禁用，请运行以下命令：

   ```
   kesl-control --start-task 12
   ```

3. 将地址添加到网络区域：

   ```
   kesl-control -F --add-zone <Public|Local|Trusted> --address <IP address>
   ```

   要查看网络数据包规则列表，请运行以下命令：

   ```
   kesl-control -F --query
   ```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `--add-zone` | 预定义网络区域：<br>• `Public`。公共网络。<br>• `Local`。本地网络。<br>• `Trusted`。受信任网络。 |
| `--address` | 网络地址或子网。 |

示例

```
kesl-control -F --add-zone Local --address 10.28.0.0/24
```

# 什么是动态规则

Kaspersky Endpoint Security 允许添加或删除应用程序正常运行所需的 Firewall *动态规则*。例如：

- 网络代理会添加允许连接到 Kaspersky Security Center的动态规则。
- 反加密勒索组件会添加用于拦截通过 NFS 和 SMB 文件传输和存储协议传输的流量的动态规则。这使该组件能够阻止那些其操作被应用程序解释为恶意加密的设备的网络流量。
- 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 会自动创建动态规则，允许应用程序组件访问网络资源。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。如果动态规则集中的任何规则被删除（例如，使用 iptables 实用程序删除），应用程序会恢复该动态规则集。如果 kesl 进程被 Watchdog 服务器终止，则应用程序在运行期间创建的所有规则链链接（kesl-bypass 除外）都会从 iptables 中删除。

您可以使用以下命令查看动态规则集：

```
kesl-control -F --query
```

应用程序会按以下格式显示所有网络包规则的列表：`<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`。动态规则被划分到单独的链中：`kesl_input`、`kesl_output`、`kesl_prerouting`、`kesl_postrouting`、`kesl_forward`。

您无法管理动态规则的设置。

示例

```
ipv4 mangle kesl_output -p tcp -m tcp --dport 80 -m mark ! --mark 0x400/0x400 -m conntrack --ctdir ORIGINAL -m
addrtype ! --dst-type LOCAL -j MARK --set-xmark 0x100/0x100 tag WebAv
```

# 如何创建连接到 Kaspersky Security Center 的规则

网络代理被用于与 Kaspersky Security Center 的交互。为了在网络代理与 Kaspersky Security Center 之间建立永久连接，您需要为网络代理的端口添加允许规则。在这种情况下，即使您错误配置了防火墙并意外阻止了所有连接，也可以在 Kaspersky Security Center 控制台中远程配置防火墙。

端口集取决于计算机的角色（例如，分发点）。要了解要在计算机上打开的端口，请参阅 Kaspersky Security Center 帮助。

**如何在 Web Console 中为网络代理添加允许规则**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择“**通信和 Web 保护**”→“**防火墙**”。
5. 确保该组件的切换开关处于 **防火墙已启用** 位置。
6. 选择**始终为网络代理端口添加允许规则**复选框。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中为网络代理添加允许规则**

1. 确保已启用防火墙管理：

   ```
   kesl-control --get-task-state 12
   ```

   组件必须处于 **已启动** 状态。
2. 如果组件已禁用，请运行以下命令：

   ```
   kesl-control --start-task 12
   ```
3. 运行以下命令：

   ```
   kesl-control --set-settings 12 OpenNagentPorts=Yes
   ```
4. 要检查组件设置的当前值，请运行以下命令：

   ```
   kesl-control --get-settings 12
   ```

# 安全控制

## 设备控制

*设备控制*管理用户对安装在客户端设备上或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。

## 设备控制的工作原理

默认情况下，设备控制组件已启用并使用默认设置。

1. **用户尝试访问设备**
2. **“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。可以为每种设备类型应用以下*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。
     - *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。
     - *自定义*：根据设备访问规则允许或阻止对设备的访问。
     - *只读*：允许对所选类型的设备进行只读访问，同时阻止写入访问。
   - **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。
3. **扫描完成**

   如果用户尝试访问的设备对该用户而言不是受信任设备，或者用户没有根据访问模式获得访问该设备的权限，则应用程序会阻止该用户访问该设备。

   如果用户认为访问被错误阻止，可以向组织管理员发送申诉请求，或者请求临时访问该设备。

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。

## 配置设备控制

1. **配置受信任设备**

   *受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。您可以向单个用户、用户组或组织的所有用户授予对受信任设备的访问权限。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。
2. **配置访问模式**

   您可以为设备类型和连接总线配置访问模式。默认情况下，所有设备类型均选择*取决于总线*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。
3. **配置访问规则**

   对于存储设备（硬盘驱动器、可移动驱动器、软盘驱动器和 CD/DVD 驱动器），您可以配置*访问规则*。

4. **配置消息模板**

   如有必要，您可以自定义消息的模板文本，该消息用于通知用户访问设备被阻止或对设备执行的操作被禁止。

5. **配置对设备的临时访问权限**

   如有必要，允许用户获取对被阻止设备的临时访问权限。

特殊注意事项和限制

- 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。
- 设备控制不会阻止系统驱动器。如果应用程序无法自动检测系统驱动器，设备控制组件将因错误而终止。
- 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、6.8。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。
- “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，则您无法使用访问设备的计划来阻止对设备的访问。

# 如何在命令行中管理受信任设备列表

受信任设备列表包含允许被访问的设备（针对特定用户或组）的信息。

在命令行中，您可以查看受信任设备列表、从列表中添加和删除设备，以及从文件导入受信任设备列表。

查看受信任设备列表

```
kesl-control --trusted-devices --list
```

将设备添加到受信任设备列表

```
kesl-control --trusted-devices --add <device id or mask>
```

其中，`<device id or mask>` 是设备 ID 或设备 ID 掩码。

从受信任设备列表中删除设备

```
kesl-control --trusted-devices --delete <device id or mask>
```

其中，`<device id or mask>` 是设备 ID 或设备 ID 掩码。

从文件导入受信任设备列表

```
kesl-control --trusted-devices --merge|--add|--replace --file <file>
```

其中：

- `--merge`可合并受信任设备列表。如果当前列表和导入的列表中包含具有相同 ID 的设备条目，则会更新现有条目。对于不在当前列表中的设备，会添加条目。
- `--add`会在导入时添加当前受信任设备列表。仅将之前不在设备列表中的设备条目添加到列表中。
- `--replace`可替换当前受信任设备列表。现有受信任设备列表将被导入的列表替换。
- `--file <file>` 是将从中导入受信任设备列表的 JSON 文件的完整路径。

# 如何配置设备访问模式

对于每种设备类型（根据“设备控制”组件的分类，例如打印机、可移动驱动器、CD/DVD 驱动器），可以应用以下*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。
- *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。
- *自定义*：根据设备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。此访问模式仅可针对存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）进行指定。
- *只读*：允许对所选类型的设备进行只读访问，同时阻止写入访问。此访问模式仅可针对存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）进行指定。如果设备具有“只读”访问类型，则当将受信任设备被分配给特定用户时，被分配的用户将被忽略，所有用户都可以写入该设备。

**如何在 Web Console 中为设备类型配置设备访问模式**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

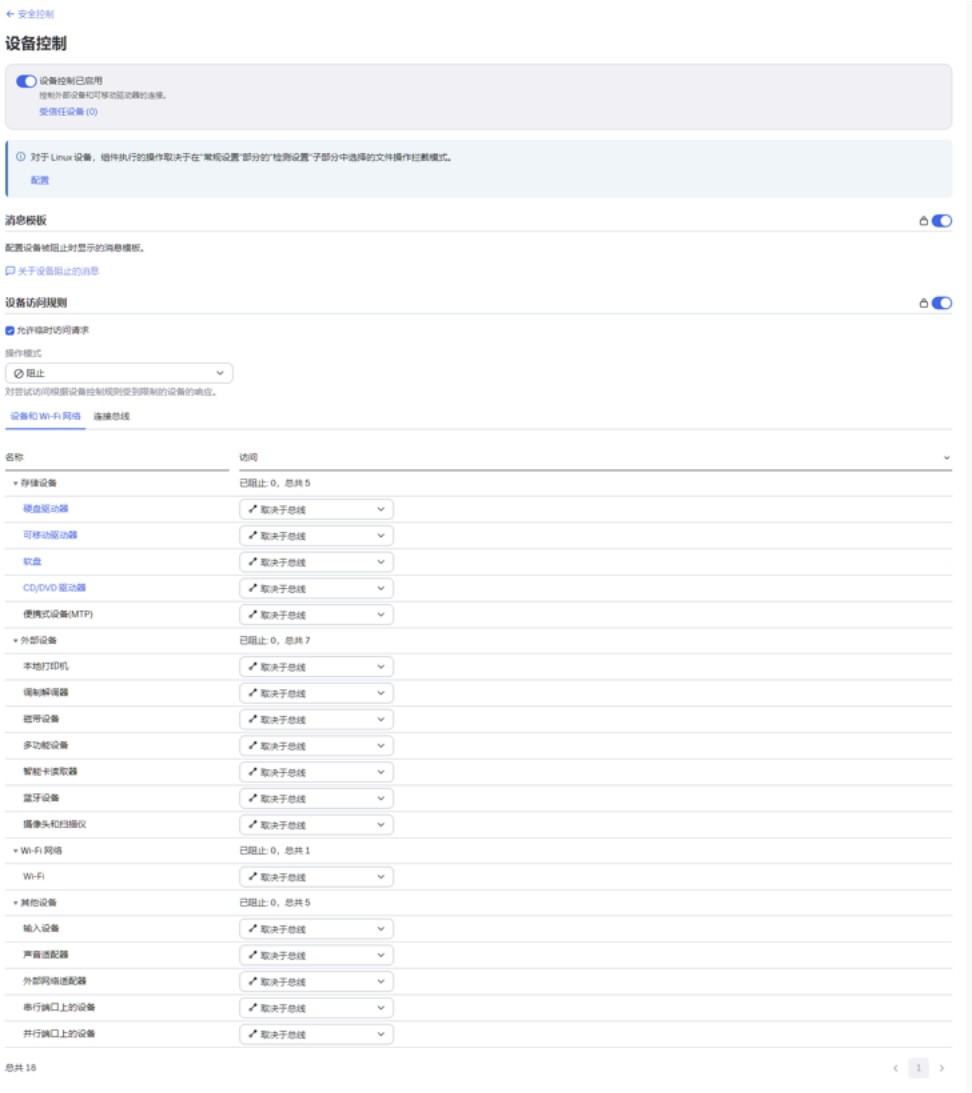
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **设备控制**。
5. 确保该组件的切换开关处于 **设备控制已启用** 位置。
6. 在“**设备访问规则**”下的表格中，选择“**设备和 Wi-Fi 网络**”选项卡。
7. 在“**名称**”列中，选择要为其配置访问模式的设备类型。
8. 在“**访问权限**”下拉列表中，选择以下访问模式之一：
   - **允许**：允许访问所选类型的设备。
   - **阻止**：禁止访问选定类型的设备。

- **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。
- **自定义**：根据访问规则和计划允许或阻止对设备的访问。此选项仅适用于存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）。
- **只读**：允许对所选类型的设备进行只读访问。此选项仅适用于存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）。

9. 在下表中，单击“**添加**”按钮。

   这将打开添加新访问规则的窗口。

10. 在“**优先级**”字段中，设置访问规则优先级。
11. 选择此访问规则将应用到的用户或用户组。默认情况下，该规则适用于所有用户。
12. 如有必要，请设置访问计划。默认情况下，该规则始终适用。
13. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




设备控制

### 如何在命令行中为设备类型配置设备访问模式

1. 请确保设备控制组件正在运行：

   ```
   kesl-control --get-task-list
   ```

   组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

   ```
   kesl-control --start-task 15
   ```

3. 选择在尝试访问根据设备控制规则受到限制的设备时的操作模式：

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

4. 为以下任一设备类型指定访问模式：`HardDrive`、`RemovableDrive`、`FloppyDrive`、`OpticalDrive`、`SerialPortDevice`、`ParallelPortDevice`、`Printer`、`Modem`、`TapeDrive`、`MultifuncDevice`、`SmartCardReader`、`WiFiAdapter`、`NetworkAdapter`、`PortableDevice`、`PortableDevice`、`BluetoothDevice`、`ImagingDevice`、`SoundAdapter`、`InputDevice`

   ```
   kesl-control --set-settings 15 DeviceClass.<device type>=<Allow|Block>
   ```

5. 要查看 设备控制设置，请运行以下命令：

   ```
   kesl-control --get-settings 15
   ```

### 如何在 Web Console 中配置连接总线访问模式

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **设备控制**。
5. 确保该组件的切换开关处于 **设备控制已启用** 位置。
6. 在“**设备访问规则**”下的表格中，选择“**连接总线**”选项卡。
7. 在“**名称**”列中，选择要为其配置访问模式的总线。
8. 在“**访问权限**”下拉列表中，选择以下访问模式之一：
   - **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。
9. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行中配置连接总线访问模式

1. 请确保设备控制组件正在运行：

   ```
   kesl-control --get-task-list
   ```

   组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

   ```
   kesl-control --start-task 15
   ```

3. 选择在尝试访问根据设备控制规则受到限制的设备时的操作模式：

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

4. 指定连接总线的访问模式：

   ```
   kesl-control --set-settings 15 DeviceBus.USB=<Allow|Block>
   kesl-control --set-settings 15 DeviceBus.FireWire=<Allow|Block>
   ```

5. 要查看 设备控制设置，请运行以下命令：

   ```
   kesl-control --get-settings 15
   ```

## 如何配置设备访问规则

对于存储设备（硬盘驱动器、可移动驱动器、软盘驱动器和 CD/DVD 驱动器），您可以配置访问规则。*设备访问规则*是一组选项，用于确定哪些用户可以访问安装在客户端设备上或连接到客户端设备的设备，以及可以在什么时间访问。此访问模式仅可针对存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）进行指定。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，但访问时未发现任何有效规则，则该操作将被阻止。

### 如何在 Web Console 中配置设备访问规则

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **设备控制**。
5. 确保该组件的切换开关处于 **设备控制已启用** 位置。
6. 在“**设备访问规则**”下的表格中，选择“**设备和 Wi-Fi 网络**”选项卡。

7. 在“**名称**”列中，选择要为其添加访问规则的存储设备类型（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）。

8. 在打开的窗口中，在“**设备访问规则**”下，选择“**自定义**”。

9. 在下表中，单击“**添加**”按钮。
   这将打开添加新访问规则的窗口。

10. 在“**优先级**”字段中，设置访问规则优先级。

11. 选择此访问规则将应用到的用户或用户组。默认情况下，该规则适用于所有用户。

12. 如有必要，请设置访问计划。默认情况下，该规则始终适用。

13. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行配置设备访问规则**

1. 请确保设备控制组件正在运行：

   ```
   kesl-control --get-task-list
   ```

   组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

   ```
   kesl-control --start-task 15
   ```

3. 要查看 设备控制设置，请运行以下命令：

   ```
   kesl-control --get-settings 15
   ```

4. 选择在尝试访问根据设备控制规则受到限制的设备时的操作模式：

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

5. 为以下设备类型之一添加新的访问规则：`HardDrivePrincipals.item_#.AccessRules.item_#`、`RemovableDrivePrincipals.item_#.AccessRules.item_#`、`FloppyDrivePrincipals.item_#.AccessRules.item_#` 或 `OpticalDrivePrincipals.item_#.AccessRules.item_#`。

   - 启用该规则并指定默认计划：

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.UseRule=Yes
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.ScheduleName=Default
     ```

     示例

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - 设置规则触发时的设备控制操作：

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.Access=Allow|Block
     ```

     示例

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.Access=Allow
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - 如有必要，请指定该规则将应用到的用户：

     ```
     kesl-control --set-settings 15 <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.Principal=<Name>=
     <\Everyone|user name|@group name>
     ```

     示例

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.Principal=\Everyone
     ```

   - 如有必要，请编辑规则计划：

     ```
     kesl-control --set-settings 15 Schedules.item_#.ScheduleName=<Name> Schedules.item_#.DaysHours=<All|day of
     the week|hour>
     ```

     示例

     ```
     kesl-control --set-settings 15 Schedules.item_0001.ScheduleName=Default Schedules.item_0001.DaysHours=All
     ```

# 如何配置设备控制消息模板

当用户尝试访问被阻止的设备时，应用程序会显示一条关于访问被拒绝或设备操作被阻止的消息。

拒绝访问消息基于一个描述阻止原因的模板。您可以在消息模板中使用特殊变量（例如，%USER_NAME%）。这些变量可让您对不同设备使用相同的消息模板。生成消息时，应用程序会将与特定设备、用户和事件对应的变量值带入到消息中。

您可以编辑消息模板。

**如何在 Web Console 中编辑消息模板**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制 → 设备控制**。
5. 在 **消息模板** 下，单击 **关于设备阻止的消息** 链接。

   这将打开消息模板配置窗口。
6. 在 **给用户的消息** 选项卡上配置设备控制消息模板。
7. 您可以通过单击**添加变量**和**添加链接**按钮，向用户消息正文中添加变量和链接。要向模板添加变量，请将光标放在文本中的所需位置，单击**添加变量**按钮，然后从下拉列表中选择一个变量。要向模板添加链接，请将光标放在文本中的所需位置，然后单击**添加链接**按钮。

   如果要恢复消息模板的文本，请单击 **恢复默认** 按钮。
8. 单击“**确定**”。
9. 单击“**保存**”按钮以保存更改。

**如何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→ 设备控制**。
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**阻止消息**选项卡上配置设备控制消息模板。

   您可以通过单击**变量**和**链接**按钮，向用户消息正文中添加变量和链接。要向模板添加变量，请将光标放在文本中的所需位置，单击**变量**按钮，然后从下拉列表中选择一个变量。要向模板添加链接，请将光标放在文本中的所需位置，然后单击**链接**按钮。

   您也可以通过单击“**默认**”按钮恢复消息模板的文本。
7. 单击“**确定**”。
8. 单击**应用**。

# 授予设备临时访问权限

配置设备控制时，管理员可能会错误阻止用户访问工作所需的设备。如果用户认为对设备的访问或对设备内容的操作被错误阻止，用户可以向公司本地网络管理员请求临时访问被阻止的设备。

如果管理员允许用户请求临时访问权限，则用户可以这样做。管理员可以在 Web Console 的策略属性中、管理控制台中或设备控制任务的设置中配置此权限。

授予对被阻止设备的访问权限涉及以下步骤：

1. 用户创建*访问请求文件*并将其发送给管理员，例如通过电子邮件或任何可用的方式（管理员可以在阻止消息模板中配置此设置）。用户可以在应用程序的图形界面或命令行中请求临时访问被阻止的设备。
2. 管理员根据访问请求文件创建*访问密钥*，并将其传递给用户，例如通过电子邮件或其他方式。对被阻止设备的访问权限在 Web Console 中授予。
3. 用户上传访问密钥，即可临时访问被阻止的设备。用户可以在应用程序的图形用户界面或命令行中上传访问密钥。

只有当组织中部署了 Kaspersky Security Center 16.1 并且客户端设备能够与管理服务器建立连接时，才能授予对被阻止设备的访问权限。

**如何在 Web Console 中为被阻止的设备创建访问密钥**

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. 选择包含相关设备的管理组，然后选中设备名称旁边的复选框。
3. 在受管理设备列表上方，单击**授予对离线模式下设备的访问权限**按钮。如果设备列表上方未显示此按钮，请单击三个点按钮，然后从菜单中选择**授予对离线模式下设备的访问权限**命令。
4. 这将打开**“应用程序设置”**窗口；在该窗口的**“设备控制”**部分，点击“**浏览**”按钮并下载从用户处收到的访问请求文件。

   用户请求访问但被阻止的设备信息将显示。
5. 如有必要，请在**访问持续时间**字段中更改持续时间（以小时为单位）。

   默认情况下，**访问持续时间**设置为用户在生成访问请求文件时指定的值。
6. 如有必要，请更改**指定访问密钥在客户端设备上可使用的时长（以小时为单位）**字段中的值。

   此字段包含用户可以上传访问密钥的时间段。
7. 单击**创建密钥**按钮。
8. 将访问密钥文件以 *.acode 扩展名保存。

**如何在命令行中请求并获得临时访问权限**

如果用户认为对设备的访问被错误阻止或对设备内容的操作被错误禁止，则可以使用以下设备控制管理命令向组织本地网络的管理员请求对被阻止设备的临时访问权限：

请求对被阻止设备的临时访问权限

```
kesl-control --request-temporary-device-access --device-id <device identifier>  --access-duration <access duration> --path <path to the access request file>
```

其中：

`--device-id <device identifier>` 是要访问的被阻止设备的 ID。

`--access-duration <access duration>` 是您希望获得设备访问权限的时间段（以小时为单位）。可能的值：1 到 100

`--path <path to the access request file>` 是要保存扩展名为 .akey 的访问请求文件的目录路径。

此命令会创建一个访问请求文件，该文件必须发送给管理员，例如通过电子邮件或其他方式（管理员可以在阻止消息模板中描述首选方法）。

从管理员处收到访问密钥后，您必须输入访问密钥，才能获得设备的临时访问权限。

上传被阻止设备的访问密钥

```
kesl-control --upload-temporary-device-access-key --path <path to the file with the access key>
```

其中：

`--path <path to the file with the access key>` 是包含设备访问密钥的文件路径（扩展名为 .acode 的文件）。

该命令会输出关于已授予的设备访问权限和访问持续时间的信息。

**如何在图形界面中请求并获得临时访问权限**

当设备连接后，如果设备控制拒绝访问该设备，则会显示一个窗口，其中包含关于阻止访问该设备的消息。

您可以使用图形界面向您所在组织的本地网络管理员申请临时访问被阻止的设备：

- 在显示设备访问被阻止消息的窗口中，单击**确定**
- 从应用程序图形界面的主窗口

*请求对被阻止设备的临时访问权限：*

1. 打开应用程序图形界面的主窗口。
2. 在主窗口下部，单击**临时访问权限**按钮。
   这将打开**临时访问权限**窗口。
   您也可以从显示设备访问被阻止消息的窗口中单击**确定**打开**临时访问权限**窗口。
3. 在“**请求访问被阻止的设备**”部分，在已连接设备列表中，选择要访问的设备。
4. 在**设备访问持续时间（小时）**字段中，指定您希望访问设备的时间段（以小时为单位）。
5. 单击**创建请求访问文件**按钮。

6. 在打开的窗口中，指定要保存扩展名为 .akey 的访问请求文件的目录路径。

7. 将访问请求文件发送给管理员，例如通过电子邮件或任何可用的方式（管理员可以在阻止消息模板中配置此设置）。

从管理员处获得访问密钥后，您可以上传该访问密钥以获得对被阻止设备的临时访问权限。

*获取对被阻止设备的临时访问权限：*

1. 打开应用程序图形界面的主窗口。

2. 在主窗口下部，单击**临时访问权限**按钮。

   这将打开**临时访问权限**窗口。

3. 在“**获取设备访问权限**”部分，单击“**上传访问密钥**”按钮。

4. 在打开的窗口中，选择从组织本地网络管理员处收到的设备访问密钥文件（扩展名为 .acode 的文件）。

5. 此时将显示一个窗口，其中包含关于已授予访问权限的设备及访问持续时间的信息。

6. 单击“**确定**”。

# Web 控制

“Web 控制”管理用户对 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。

Web 控制允许按内容类别和数据类型限制对 Web 资源的访问，以及阻止访问单个网站。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。应用程序根据文件格式而不是扩展名来确定数据类型。

## Web 控制的工作原理

1. **应用程序检查对 Web 资源的请求**

   Web 控制使用以下技术确定网站的内容类别和数据类型：

   - 反病毒数据库。
   - 卡巴斯基安全网络的云服务。
   - 启发式分析技术能够检测卡巴斯基数据库尚未涵盖的威胁。

2. **应用程序应用规则**

   应用程序按优先级顺序应用 Web 控制规则。优先级编号越低，规则的优先级越高。如果多条规则适用于某个网站，Web 控制将应用优先级最高的规则。

   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并提供对公司 Web 门户的访问权限，请创建两条规则：一条针对“*社交网络*”网站类别的阻止规则和一条针对公司 Web 门户的允许规则。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。

### 3 扫描完成

如果规则阻止访问 Web 资源，应用程序会在浏览器中显示阻止消息。该资源将不可用。

如果用户认为网页被误拦截，可以向组织的管理员发送有关误拦截的请求。

## 配置 Web 控制

### 1 配置 Web 控制规则

Web 控制通过使用*访问规则*管理用户对网站的访问。这些规则允许限制单个用户对网站的访问，以及配置访问计划。

例如，您可以限制组织中除 IT 部门以外的所有用户访问 *互联网通信* 类别中的网站。

### 2 配置消息模板

根据访问规则的操作，Web 控制会向用户显示有关访问不受欢迎的网站的消息或阻止消息。当网站被阻止时，用户可以向本地网络的管理员发送有关误拦截的消息。

针对此类消息提供了模板。

无法在命令行中编辑模板。

### 3 启用 Web 控制

默认情况下，Web 控制处于禁用状态。使用切换开关在 Web Console 或管理控制台中启用该组件，或使用以下命令在命令行中启用该组件：

```
kesl-control --start-task 26
```

## 特殊注意事项和限制

- 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。
- Kaspersky Endpoint Security 仅监控 HTTP 和 HTTPS 流量。
- 当 Web 威胁防护和 Web 控制同时运行时，Web 威胁防护设置将应用于 Web 资源。这意味着，即使 Web 控制规则允许访问恶意网站或钓鱼网站，也会将其阻止。

# 如何创建 Web 资源访问规则

*Web 资源访问规则*是 Kaspersky Endpoint Security 在用户访问 Web 资源时应用的一组过滤器和操作。访问规则可以包括规则计划。

规则通过以下筛选条件限制对 Web 资源的访问：

- “**内容类别**”。Web 控制按内容和数据类型对 Web 资源进行分类。这允许限制用户访问具有特定内容类别（例如，*支付系统*）和/或特定数据类型（例如，*可执行文件*）的网站。
- “**个别网站**”。Web 控制允许限制用户访问 Web 资源的单个网址或网址组。

  网址的域名不区分大小写。如果规则包含 `examPLE.com` 等网址，Web 控制将限制对 `example.com` 的访问。

  如果在访问规则中同时配置了内容类别筛选条件和单个网站筛选条件，Web 控制不会限制对指定内容类别的所有网站的访问，而只会限制对指定网址的访问。
- **按用户和用户组名称进行筛选**。Web 控制允许限制单个用户或用户组访问 Web 资源。例如，您可以限制组织中除 IT 部门外的所有用户访问社交媒体网站。
- **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，您可以仅在工作时间限制对不受欢迎的网站的访问。

如果没有创建阻止规则，则不会解密 HTTPS 流量。

**如何在 Web Console 中创建访问规则**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **Web 控制**。
5. 确保该组件的切换开关处于 **Web 控制已启用** 位置。
6. 在 **规则列表** 下，选择默认的 Web 控制操作：
   - **允许除规则列表外的所有内容**
   - **阻止除规则列表外的所有内容**
7. 单击“**添加**”。

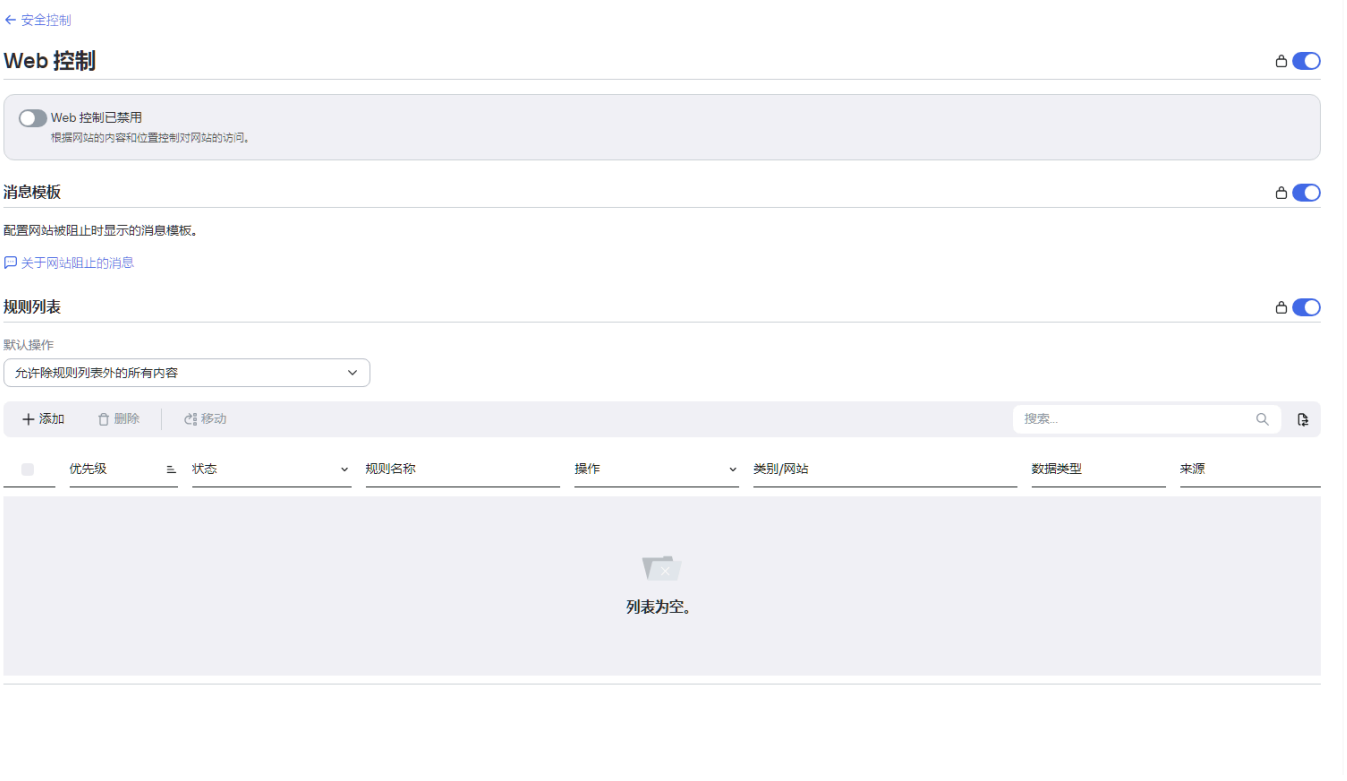
   这将打开用于添加新访问规则的表单。
8. 在“**规则名称**”字段中输入规则名称。规则名称必须唯一。
9. 在“**优先级**”字段中，设置访问规则优先级。
10. 选择当规则触发时您希望 Web 控制应用于 Web 资源的操作：
    - “**允许**”。Web 控制允许用户访问 Web 资源。
    - “**阻止**”。Web 控制阻止用户对 Web 资源的访问并显示访问被阻止的消息。通过点击阻止消息中的链接，用户可以向本地网络管理员发送消息，以报告阻止错误。
    - “**通知**”。Web 控制会显示关于访问不受欢迎的 Web 资源的警告。如果用户认为警告不正确，则可通过警告中的链接前往网页或向组织的本地网络管理员发送请求。

11. 选择访问规则筛选条件：

    - “**内容类别**”。指定您希望访问规则控制的内容类别。您可以选择多个类别。
    - “**个别网站**”。指定一个网址或一组网址。

    > 在 Web Console 中，您无法同时按内容类别和单个网站设置筛选条件。

12. 如有必要，请指定您希望应用程序筛选的数据类型。
13. 选择此访问规则将应用到的用户或用户组。默认情况下，该规则适用于所有用户。
14. 如有必要，请设置访问计划。默认情况下，该规则始终适用。
15. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




Web 控制

### 如何在命令行创建访问规则

1. 确保已启用 Web 控制组件：

   ```
   kesl-control --get-settings 26
   ```

   组件必须处于 **已启动** 状态。

2. 如果组件已禁用，请运行以下命令：

   ```
   kesl-control --start-task 26
   ```

3. 选择默认 Web 控制操作：

```
kesl-control --set-settings 26 WebControlDefaultAction=<Allow|Block>
```

4. 添加 ID 为 # 的新访问规则：

a. 启用该规则：

```
kesl-control --set-settings 26 Rules.item_#.Enabled=Yes
```

b. 输入规则名称：

```
kesl-control --set-settings 26 Rules.item_#.Name=<rule name>
```

c. 指定当规则触发时您希望 Web 控制应用于 Web 资源的操作：

```
kesl-control --set-settings 26 Rules.item_#.WebControlAction=<Allow|Block|Notify>
```

d. 如果需要按内容类别筛选 Web 资源：

```
kesl-control --set-settings 26 Rules.item_#.UseCategories=<ContentOnly|FormatOnly|ContentAndFormat>
kesl-control --set-settings 26 Rules.item_#.ContentCategories.item_#.ContentCategory=<category>
[Rules.item_#.FormatCategories.item_#.FormatCategory=<format>]
```

e. 如果需要筛选单个 Web 资源：

```
kesl-control --set-settings 26 Rules.item_#.UseUrls=Yes
kesl-control --set-settings 26 Rules.item_#.Urls.item_#=<web address>
```

f. 如有必要，请指定该规则适用的用户：

```
kesl-control --set-settings 26 Rules.item_#.UsePrincipals=Yes
kesl-control --set-settings 26 Rules.item_#.Principals.item_#.Name=<user name|@group name>
```

g. 如有必要，请指定规则的计划：

```
kesl-control --set-settings 26 Rules.item_#.Schedules.item_#.Id=<ID> Rules.item_#.Schedules.item_#.Name=
<schedule name> Rules.item_#.Schedules.item_#.DaysHours=<day of the week|hour>
```

5. 要查看 Web 控制规则列表，请运行以下命令：

```
kesl-control --get-settings 26
```

符号

| 设置 | 描述 |
| --- | --- |
| WebControlDefaultAction | Web 控制对未在任何访问规则中指定的 Web 资源应用的操作。 |
| Enabled=Yes | 启用 ID 为 # 的访问规则。 |
| Name | 规则名称。规则名称必须唯一。 |
| WebControlAction | 规则触发时 Web 控制对 Web 资源应用的操作：<br>Allow（默认值）— 允许访问 Web 资源。<br>Block — 阻止访问 Web 资源。<br>Notify – 显示有关访问不需要的 Web 资源的警告。通过单击警告消息中的链接，用户可以访问所请求的 Web 资源。 |
| UseCategories | 在规则中按内容类别和数据类型类别使用筛选器：<br>None（默认）— 不使用 Web 资源内容筛选器。<br>ContentOnly — 在规则中使用内容类别筛选器。<br>FormatOnly — 在规则中使用数据类型类别筛选器。<br>ContentAndFormat — 在规则中使用内容类别筛选器和数据类型类别筛选器。 |
| ContentCategories.item_#.ContentCategory | 内容类别。 |
| FormatCategories.item_#.FormatCategory | 数据类型类别：<br>Video – 视频文件<br>Audio – 音频文件<br>OfficeDocument — Office 应用程序文件<br>Executable – 可执行文件<br>Archives – 压缩文件<br>Images – 图像文件<br>Scripts – 脚本 |
| UseUrls=Yes | 在筛选规则中使用单个网站。 |
| 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 资源地址。 |
| UsePrincipals=Yes | 使用受 Web 资源访问规则覆盖的用户筛选器。 |
| Principals.item_#.Name | Web 资源访问规则涵盖的用户或用户组：<br><user name> 是规则适用的用户的名称。<br>@<group name> 是规则适用的用户组的名称。 |
| Schedules.item_#.Id | 计划 ID。 |
| Schedules.item_#.Name | 指定计划名称。 |
| Schedules.item_#.DaysHours | 指定计划的时间间隔：<br><day of week> 是星期几。您可以使用完整的星期几名称或缩写（例如，对于星期一，您可以指定 Mo、Mon 或 Monday）。对于周中日，您可以指定间隔时间或特定日子。一周从星期日开始。<br><hour> – 小时 [0:24]。只能指定小时间隔。 |

# 如何修改 Web 控制消息模板

根据访问规则中指定的操作，当用户尝试访问 Web 资源时，Web 控制会向用户显示一条消息（通过将 HTTP 服务器响应替换为包含消息的 HTML 页面）：

- **警告。**当用户尝试访问不需要的资源时，向其显示的消息。如果为规则选择了 **通知** 操作，应用程序将显示此消息。

  如果用户认为警告不正确，则可通过警告中的链接前往网页或向组织的本地网络管理员发送请求。

- **Web 资源被阻止消息** 当不需要的 Web 资源被阻止时向用户显示的消息。如果为规则选择了 **阻止** 操作，应用程序将显示此消息。

  如果用户认为某个 Web 资源被错误地阻止，则可通过 Web 资源阻止消息中的链接向组织的本地网络管理员提交请求。

提供了警告消息、关于阻止 Web 资源的消息以及向组织的本地网络管理员发送的请求的模板。提供了特殊变量来管理消息模板（例如，`%USER_NAME%`）。变量允许将单个消息模板用于不同的计算机。生成消息时，Kaspersky Endpoint Security 从操作系统设置中检索变量的值，并将其插入到与特定计算机、用户和事件匹配的消息中。

无法在命令行中编辑模板。

**如何在 Web Console 中编辑消息模板**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **Web 控制**。
5. 在 **消息模板** 下，单击 **关于网站阻止的消息** 链接。

   这将打开包含消息模板的窗口。
6. 配置 Web 控制消息模板：
   - “**警告**”。当用户尝试访问不需要的资源时，向其显示的警告模板。
   - “**阻止消息**”。当不需要的网页或网站被阻止时显示的消息模板。
   - “**给管理员的消息**”。向管理员发送的消息模板。如果用户认为网页被错误地阻止，则使用此模板。用户请求访问权限后，应用程序会向 Kaspersky Security Center 发送 *发送给管理员的网页访问阻止消息* 事件。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。

   如果您要恢复消息模板的文本，请单击 **重置为默认文本** 按钮。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何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**。该条目字段包含某个阻止访问网页资源的规则被触发时要显示的消息的模板。
   - **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 管理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“**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**。

## 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 `/*` 将被解释为 `/*` 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;<br>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。 |

# 应用程序控制

应用程序控制管理用户设备上第三方应用程序的启动。这可以降低受保护设备感染恶意软件的风险。

要使用该组件，需要包含相应功能的授权许可。

## 应用程序控制的工作原理

1. **用户尝试运行第三方应用程序**
2. **应用程序控制应用规则**

   应用程序控制按顺序将规则应用于正在启动的应用程序。根据所选的规则模式，该组件会*控制*正在启动的应用程序或*测试*规则。阻止规则的优先级高于允许规则的优先级。
3. **扫描完成**

   如果规则阻止应用程序执行，该组件会阻止此应用程序启动并生成一个 *已禁止应用程序启动* 事件。在测试模式下，该组件不会阻止此应用程序启动，并会生成 *禁止应用程序在测试模式下启动* 事件。

## 配置应用程序控制

1. **清查应用程序**

   使用 清查 任务获取受保护设备上已安装应用程序的列表。根据此信息，创建要阻止其运行的应用程序列表。
2. **选择应用程序控制的操作模式**

   应用程序控制组件有两种运行模式可选：

   - "*允许除规则列表外的所有内容*"。应用程序控制允许用户运行任何第三方应用程序，但规则禁止的应用程序除外。
   - "*阻止除规则列表外的所有内容*"。应用程序控制允许用户运行任何第三方应用程序，但规则允许且未禁止的应用程序除外。

   应用程序控制模式的选择取决于您组织的安全策略以及您要控制的应用程序数量。
3. **创建应用程序类别**

   定义允许或拒绝的应用程序类别。应用程序类别适用于公司网络中的所有设备，无论所属管理组如何。应用程序类别可让您针对一组应用程序配置规则，而不是基于包含和排除条件配置规则。

   建议您创建涵盖公司内所使用的标准应用程序集的"工作应用程序"类别。如果工作中不同的用户组使用不同的应用程序集，则可以为每个用户组创建单独的应用程序类别。

   我们建议在 Kaspersky Security Center 中配置应用程序类别。

### 4 配置应用程序控制规则

该组件根据 *应用程序控制规则* 控制应用程序的启动，这些规则定义了应用程序控制在何种条件下允许或拒绝选定用户组启动第三方应用程序。

### 5 测试应用程序控制规则

默认情况下，“应用程序控制”被禁用。我们建议在测试模式下启用应用程序控制，并测试已创建的应用程序控制规则。该应用程序不会阻止第三方应用程序运行，但会将有关其启动的通知发送到管理服务器。

### 6 了解应用程序控制规则的工作原理

查看应用程序控制在测试模式下运行情况的 报告。查看信息后，根据需要调整应用程序控制规则。

### 7 启用应用程序控制规则

在此模式下，如果规则不允许运行第三方应用程序，Kaspersky Endpoint Security 将阻止执行这些应用程序。

**如何在 Web Console 中启用应用程序控制规则**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **应用程序控制**。
5. 确保该组件的切换开关处于 **应用程序控制已启用** 位置。
6. 在 **启动应用程序时的操作** 下，选择应用程序控制的 **应用规则** 操作。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中启用应用程序控制规则**

要为应用程序控制选择测试模式，请运行以下命令：

```
kesl-control --set-settings 21 AppControlRulesAction=ApplyRules
```

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。

特殊注意事项和限制

- 应用程序控制不控制 Snap、Flatpak 或 AppImage 应用程序的启动。
- 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。
- 如果规则允许解释器运行，则应用程序控制不会阻止从该解释器启动的脚本。如果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。

# 应用程序清查

要创建最佳应用程序控制规则，建议首先了解公司 LAN 上受保护设备中使用的应用程序。*清查*任务可让您获取以下信息：

- 第三方应用程序的名称和版本
- 简短描述

要使用该任务，需要包含相应功能的授权许可。

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。达到限制后，将不再处理新文件。要恢复清查，您需要从受保护设备中删除在上一次清查期间已添加到 Kaspersky Security Center 数据库的文件。

配置并运行清查任务

1. **创建清查任务**

   **如何在 Web Console 中创建清查任务**

   1. 在 Web Console 的主窗口中，选择“**任务**”。
      任务列表打开。
   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“**Kaspersky Endpoint Security for Linux 12.5**”。
      b. 在“**任务类型**”下拉列表中，选择“**Inventory**”。

c. 在 **任务名称** 字段中，输入任务名称。

d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。

5. 结束向导。

**如何在命令行创建清查任务**

要创建任务，请运行以下命令：

```
kesl-control --create-task <task name> --type InventoryScan
```

其中，`<task name>` 是新任务的名称。

此命令返回已创建任务的 ID。

命令执行结果示例：

已创建任务（任务 ID：100）

2 **配置清查范围**

要启动任务，必须指定至少一个清查范围。默认情况下，已设置 *可执行命令* – `/usr/bin` 范围。

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。

**如何在 Web Console 中配置清查范围**

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击已创建的清查任务。
   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到**清查范围**区域。

5. 单击“**添加**”。
   将打开用于添加清查范围的窗口。

6. 在 **范围名称** 字段中，输入清查范围的名称，例如 *桌面上的文件*。

7. 在 **路径** 字段中，指定单个文件或目录的路径，例如 `/path/to/folder`。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

8. 如有必要，请以命令 shell 格式指定对象名称掩码，例如 `*.txt`、 `file?.*`。逐个添加掩码。

9. 保存更改。

### 如何在命令行配置清查范围

1. 运行以下命令：

```
kesl-control --set-settings <task name | task ID> ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 要检查当前设置，请运行以下命令：

```
kesl-control --get-settings <task name | task ID>
```

### 符号

清查任务设置

| 设置 | 描述 |
| --- | --- |
| `UseScanArea=Yes` | 启用 ID 为 `#` 的清查范围。<br>您可以暂时禁用清查范围扫描，而不是删除该范围。为此，请设置 `ScanScope.item_#.UseScanArea=No`。 |
| `AreaDesc` | 清查范围的描述。使用此设置指定的字符串的最大长度为 4096 个字符。 |
| `AreaMask.item_#` | 库存扫描范围限制。在清查范围内，应用程序仅扫描使用 shell 格式的掩码指定的对象。<br>您可以按任意顺序指定多个 `ScanScope.item_#.AreaMask.item_#` 项目。应用程序将按索引升序处理范围。<br>例如，`ScanScope.item_0001.AreaMask.item_0001=*.exe`<br>`ScanScope.item_0001.AreaMask.item_0002=*.txt`。 |
| `Path` | 包含要扫描的对象的目录的路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。<br>默认值：`/usr/bin` |

## 3 如有必要，请编辑任务设置

### 如何在 Web Console 中配置清查任务

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击已创建的清查任务。
   任务属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**清查设置**区域。
5. 选择要对“黄金镜像”应用程序类别执行的操作：

   - **无更改** – 完成清查后，不更改“黄金镜像”类别。这是默认选择。如果您想获取设备上使用的第三方应用程序列表，但不想将它们添加到“黄金镜像”类别，请使用此选项。
   - **更新或创建(如果不存在)** – 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。如果该类别不存在，则创建该类别。如果该类别已存在，则更新该类别的应用程序列表。
   - **删除** – 清除“黄金镜像”应用程序类别。任务启动后会立即清除此类别，而不会对设备上的文件进行清查。

6. 如有必要，请选中以下复选框：

   - “**脚本文件清查**”。检查清查范围内是否存在脚本。应用程序会将此信息发送到 Kaspersky Security Center。
   - “**扫描所有可执行文件**”。
   - “**扫描二进制文件**”。扫描二进制文件（扩展名为 .elf、.java 和 .pyc 的文件）。

7. 保存更改。

**如何在命令行配置清查任务**

请执行命令：

```
kesl-control --set-settings <task name | task ID> ScanScripts=<Yes|No> ScanBinaries=<Yes|No>
ScanAllExecutable=<Yes|No> GoldenImageAction=<DoNothing|Create|Remove>
```

符号

*清查任务设置*

| 设置 | 描述 |
| --- | --- |
| `ScanScripts` | 检查清查区域内是否存在脚本：<br>`Yes`（默认值）– 扫描脚本。<br>`No` – 不扫描脚本。 |
| `ScanBinaries` | 扫描二进制文件（扩展名为 .elf、.java 和 .pyc 的文件）：<br>`Yes`（默认值）– 扫描二进制文件。<br>`No` – 不扫描二进制文件。 |
| `ScanAllExecutable` | 扫描可执行文件：<br>`Yes`（默认值）– 使用可执行位扫描文件。<br>`No` – 不使用可执行位扫描文件。 |
| `GoldenImageAction` | 完成清查任务后，Kaspersky Endpoint Security 必须对“黄金镜像”应用程序类别执行的操作：<br>`DoNothing`（默认）– 不更改“黄金镜像”应用程序类别。<br>`Create` – 将检测到的应用程序添加到“黄金镜像”应用程序类别。如果该类别不存在，则创建该类别。如果该类别已存在，则更新该类别的应用程序列表。<br>`Remove` – 清除“黄金镜像”应用程序类别。任务启动后会立即清除此类别，而不会对设备上的文件进行清查。 |

### 4 配置排除项范围

排除项的优先级高于清查范围。即使排除的对象位于清查范围内，也不会对其进行扫描。如果清查范围定义的级别低于排除目录，则应用程序在运行任务时会跳过该清查范围。

**如何在 Web Console 中配置排除范围**

1. 在 Web Console 的主窗口中，选择“**任务**”。
2. 任务列表打开。
3. 单击已创建的清查任务。
   任务属性窗口将打开。
4. 选择**应用程序设置**选项卡。
5. 转到**排除范围**区域。

6. 单击“**添加**”。

   这将打开用于添加排除范围的窗口。

7. 在 **范围名称** 字段中，指定排除范围的名称，例如 *系统文件*。

8. 在 **路径** 字段中，指定单个文件或目录的路径（例如 `/path/to/folder`）。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

9. 以命令 shell 格式指定对象名称掩码（例如 `*.txt` 或 `file?.*`）。逐个添加掩码。

10. 保存更改。

**如何在命令行配置排除范围**

1. 运行以下命令：

```
kesl-control --set-settings <task name | task ID>       ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 要检查当前设置，请运行以下命令：

```
kesl-control --get-settings <task name | task ID>
```

符号

清查任务设置

| 设置 | 描述 |
| --- | --- |
| `UseScanArea` | 从清查中排除指定的范围。<br>您可以暂时禁用排除范围，而不是删除该范围。为此，请设置 `ExcludedFromScanScope.item_#.UseScanArea=No`。 |
| `AreaDesc` | 清查排除范围的说明。 |
| `AreaMask.item_#` | 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 格式的掩码指定的对象。<br>您可以按任意顺序指定多个 `ExcludedFromScanScope.item_#.AreaMask.item_#` 项目。应用程序将按索引升序处理范围。<br>例如，`ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`。 |
| `Path` | 要从清查中排除的目录的路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |

从清查中排除 `/tmp` 目录的示例：

```
kesl-control --set-settings 100 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

## 5 运行任务

**如何在 Web Console 中运行“清查”任务**

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 选中已创建任务旁边的复选框。

3. 单击“**开始**”。

**如何在命令行运行清查任务**

要运行任务，请运行以下命令：

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `[-W]` 启用与此任务相关的当前事件的输出。
- `[--progress]` 启用任务进度的显示。

查看检测到的应用程序列表

*要在 Web Console 中查看在设备上检测到的应用程序列表：*

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击已创建的清查任务。
   任务属性窗口将打开。
3. 选择**结果**选项卡。

查看在客户端设备上检测到的应用程序列表

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

Kaspersky Endpoint Security 显示以下有关检测到的应用程序的信息：

- 清查日期和时间
- 应用程序数量
- 包含以下信息的应用程序列表：
  - 应用程序的路径。
  - 应用程序哈希和。
  - 应用程序类型。例如，`Script`、`Executable`。
  - 应用程序所属的类别（如果之前已创建）。您可以使用以下 命令 查看已创建的应用程序类别列表：

    ```
    kesl-control --get-categories
    ```

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，您必须再次运行清查任务。

## 如何配置应用程序控制的操作模式

应用程序控制组件有两种运行模式可选：

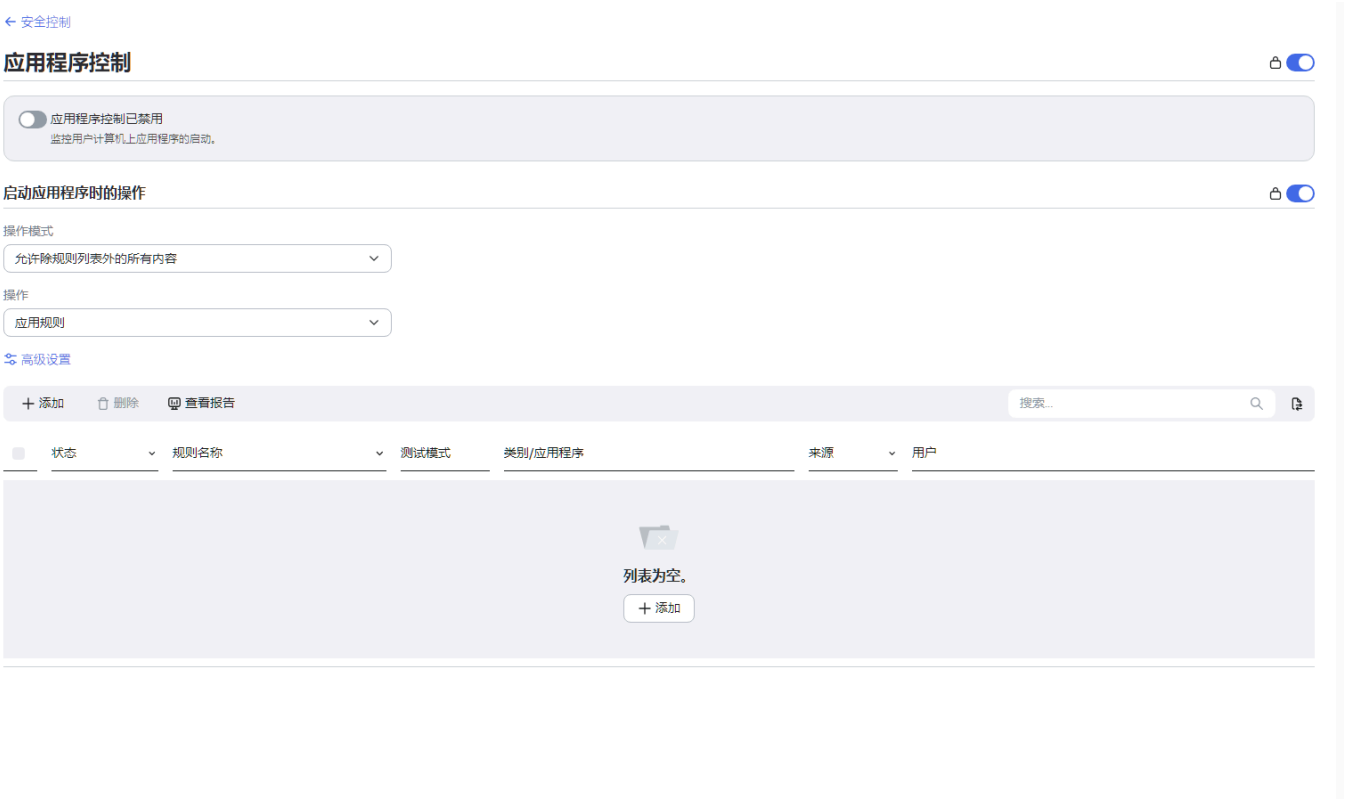
- "*允许除规则列表外的所有内容*"。应用程序控制允许用户运行任何第三方应用程序，但规则禁止的应用程序除外。
- "*阻止除规则列表外的所有内容*"。应用程序控制允许用户运行任何第三方应用程序，但规则允许且未禁止的应用程序除外。

应用程序控制模式的选择取决于您组织的安全策略以及您要控制的应用程序数量。

**如何在 Web Console 中配置应用程序控制的操作模式**

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**策略**"。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **应用程序控制**。
5. 确保该组件的切换开关处于 **应用程序控制已启用** 位置。
6. 在 **启动应用程序时的操作** 下，选择应用程序控制的操作模式：
   - **允许除规则列表外的所有内容**
   - **阻止除规则列表外的所有内容**

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




应用程序控制

### 如何在命令行中配置应用程序控制的操作模式

请执行命令：

```
kesl-control --set-settings 21 AppControlMode=<AllowList|DenyList>
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `AppControlMode` | `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。<br>`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。 |

## 创建应用程序类别

您可以创建*应用程序类别*，以便更方便地创建应用程序控制规则。

Kaspersky Endpoint Security 使用以下技术确定应用程序的类别：

- 反病毒数据库。
- 卡巴斯基安全网络的云服务。
- 启发式分析技术能够检测卡巴斯基数据库尚未涵盖的威胁。

在 Kaspersky Endpoint Security for Linux 中，可以根据以下参数创建类别：

- 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。仅可使用 SHA256。

  您可以使用掩码指定文件和目录的名称。

  **指定掩码的规则**

  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 `/`）。

建议您创建涵盖公司内所使用的标准应用程序集的“工作应用程序”类别。如果工作中不同的用户组使用不同的应用程序集，则可以为每个用户组创建单独的应用程序类别。

Kaspersky Endpoint Security for Linux 不支持 KL 类别。

*要在 Kaspersky Security Center 中创建应用程序类别：*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**第三方应用程序**” → “**应用程序类别**”。
2. 单击“**添加**”。

   用户类别创建向导将启动。
3. 按照用户类别创建向导的说明进行操作。

步骤 1.

在此步骤中，指定应用程序类别的名称，并选择以下应用程序类别类型之一：

- “*含有手动添加内容的类别。可执行文件的数据被手动添加到该类别中*”。如果您选择了此类类别，则在“*条件*”和“*排除项*”步骤，您将能够定义将可执行文件纳入类别的标准。
- “*包含指定文件夹内可执行文件的类别。复制到指定文件夹的应用程序可执行文件被自动处理，它们的度量数据被添加到类别中*”。如果选择此类型的类别，您可以在下一步中指定一个文件夹，该文件夹中的可执行文件将自动包括在类别中。
- “*包含所选设备上可执行文件的类别。这些可执行文件被自动处理，它们的度量数据被添加到类别中*”。如果选择此类型的类别，您可以在下一步中指定将自动包括在该类别中的可执行文件所属的计算机。

步骤 2.

如果您选择了以下类别类型，则可以执行此步骤：**含有手动添加内容的类别。可执行文件的数据被手动添加到该类别中。**

在此步骤中，请选择将应用程序纳入此类别的标准：

- **从 KL 类别**

  如果选择此选项，您可以将卡巴斯基应用程序类别指定为将应用程序添加到自定义类别的条件。*KL 类别*是具有相同主题属性的应用程序列表。该列表由 Kaspersky 专家维护。例如，“Office 应用程序”KL 类别就包含了 Microsoft Office 套装的所有应用程序、Adobe Acrobat 和其他应用程序。

  您可以选择所有 KL 类别来生成受信任应用程序的扩展列表。

- **从存储库选择证书**

  如果选择此选项，您可以从证书商店指定证书。该类别条件仅匹配使用指定证书签名的可执行文件。

  如果您已选择证书作为规则触发条件，请确保将此证书添加到计算机上的受信任系统存储中，并检查应用程序中的受信任系统存储使用设置。

- **指定应用程序路径 (支持掩码)**

  如果选择此选项，您可以指定客户端设备上的文件或文件夹，可执行文件将从中添加到自定义应用程序类别。您可以使用正则表达式，例如：`C:\path_to_exe\*`，例如：`C:\Program Files\Internet Explorer\*`。

- **可移动驱动器**

  如果选择此选项，您可以指定启动应用程序的媒体类型（任何介质或可移动驱动器）。从选定类型的媒体启动的应用程序将被添加到自定义应用程序类别中。

- **哈希、元数据或证书**：

  - **从可执行文件列表选择**

    如果选择此选项，您可以从客户端设备上的可执行文件列表中选择要添加到该类别的应用程序。

  - **从应用程序注册表中选择**

    如果选择此选项，则会显示应用程序注册表。从注册表中选择应用程序后，将打开一个窗口，其中预先填充了所选应用程序的元数据设置：

    - 文件名
    - 文件版本 您可以指定确切的版本，或者输入条件，例如“大于 5.0”。
    - 应用程序名称。

- 应用程序版本。您可以指定确切的版本，或者输入条件，例如“大于 5.0”。
- “供应商”。

请注意，只会阻止符合指定参数的可执行文件，但不会阻止所选应用程序本身的启动。如果所选元数据与启动应用程序时启动的可执行文件的元数据匹配，则可以继续执行下一步。否则，您需要手动编辑这些值，使它们与可执行文件的元数据相匹配。

- **手动设置**

  如果选择此选项，则需要指定文件哈希值、元数据或证书作为将应用程序添加到自定义类别的条件。

  **文件哈希**

  根据网络中设备上安装的安全应用程序版本，您需要选择 Kaspersky Endpoint Security 应用于该类别文件的哈希算法。哈希函数计算出的哈希值信息存储在管理服务器的数据库中。

  SHA256 是一种加密哈希函数，其算法没有已知的弱点；它目前被认为是安全性最高的哈希函数。Kaspersky Endpoint Security 10 及更高版本支持 SHA256。Kaspersky Endpoint Security 10 之前的版本支持 MD5 哈希函数。

  选择您希望 Kaspersky Endpoint Security 应用于该类别文件的哈希函数之一：

  - 如果您的网络中安装的所有安全应用程序实例都是 Kaspersky Endpoint Security 10 或更高版本，请选择“**SHA256**”复选框。我们不建议基于 Kaspersky Endpoint Security 10 或更早版本的可执行文件的 SHA256 哈希值创建类别。这可能会导致安全应用程序出现故障。在这种情况下，您可以对该类别的文件使用 MD5 加密哈希函数。
  - 如果您的网络中安装了早于 Kaspersky Endpoint Security 10 的版本，请选择“**MD5 哈希**”复选框。对于 Kaspersky Endpoint Security 10 或更高版本，无法根据可执行文件的 MD5 哈希值添加类别。在这种情况下，您可以对该类别的文件使用 SHA256 加密哈希函数。
  - 如果您的网络中包含使用 Kaspersky Endpoint Security 10 更早及更高版本的设备，请同时选择 **SHA256** 复选框和 **MD5 哈希** 复选框。

  **元数据**

  如果选择此选项，您可以指定文件元数据，例如文件名、文件版本和供应商。类别条件仅匹配元数据相同的可执行文件。

  **证书**

  如果选择此选项，您可以从证书商店指定证书。该类别条件仅匹配使用指定证书签名的可执行文件。

- **从 MSI 包/存档文件夹**

  如果选择此选项，您可以将 MSI 安装程序文件指定为将应用程序添加到自定义类别的条件。应用程序安装程序的元数据被发送到管理服务器。安装程序元数据与指定 MSI 安装程序匹配的应用程序将被添加到自定义应用程序类别中。

步骤 3.

如果您选择了以下类别类型，则可以执行此步骤：**含有手动添加内容的类别。可执行文件的数据被手动添加到该类别中**。

在此步骤指定的应用程序将从类别中排除，即使在“配置将应用程序包括在类别中的条件”步骤指定了这些应用程序。

在此步骤中，选择从类别中排除应用程序的标准：

- **从 KL 类别**

  如果选择此选项，您可以将卡巴斯基应用程序类别指定为将应用程序添加到自定义类别的条件。*KL 类别*是具有相同主题属性的应用程序列表。该列表由 Kaspersky 专家维护。例如，“Office 应用程序”KL 类别就包含了 Microsoft Office 套装的所有应用程序、Adobe Acrobat 和其他应用程序。

  您可以选择所有 KL 类别来生成受信任应用程序的扩展列表。

- **从存储库选择证书**

  如果选择此选项，您可以从证书商店指定证书。该类别条件仅匹配使用指定证书签名的可执行文件。

  如果您已选择证书作为规则触发条件，请确保将此证书添加到计算机上的受信任系统存储中，并检查应用程序中的受信任系统存储使用设置。

- **指定应用程序路径 (支持掩码)**

  如果选择此选项，您可以指定客户端设备上的文件或文件夹，可执行文件将从中添加到自定义应用程序类别。您可以使用正则表达式，例如：`C:\path_to_exe\*`，例如：`C:\Program Files\Internet Explorer\*`。

- **可移动驱动器**

  如果选择此选项，您可以指定启动应用程序的媒体类型（任何介质或可移动驱动器）。从选定类型的媒体启动的应用程序将被添加到自定义应用程序类别中。

- **哈希、元数据或证书**：

  - **从可执行文件列表选择**

    如果选择此选项，您可以从客户端设备上的可执行文件列表中选择要添加到该类别的应用程序。

  - **从应用程序注册表中选择**

    如果选择此选项，则会显示应用程序注册表。从注册表中选择应用程序后，将打开一个窗口，其中预先填充了所选应用程序的元数据设置：

    - 文件名
    - 文件版本 您可以指定确切的版本，或者输入条件，例如“大于 5.0”。

- 应用程序名称。
- 应用程序版本。您可以指定确切的版本，或者输入条件，例如“大于 5.0”。
- “供应商”。

请注意，只会阻止符合指定参数的可执行文件，但不会阻止所选应用程序本身的启动。如果所选元数据与启动应用程序时启动的可执行文件的元数据匹配，则可以继续执行下一步。否则，您需要手动编辑这些值，使它们与可执行文件的元数据相匹配。

- **手动设置**

  如果选择此选项，则需要指定文件哈希值、元数据或证书作为将应用程序添加到自定义类别的条件。

  **文件哈希**

  根据网络中设备上安装的安全应用程序版本，您需要选择 Kaspersky Endpoint Security 应用于该类别文件的哈希算法。哈希函数计算出的哈希值信息存储在管理服务器的数据库中。

  SHA256 是一种加密哈希函数，其算法没有已知的弱点；它目前被认为是安全性最高的哈希函数。Kaspersky Endpoint Security 10 及更高版本支持 SHA256。Kaspersky Endpoint Security 10 之前的版本支持 MD5 哈希函数。

  选择您希望 Kaspersky Endpoint Security 应用于该类别文件的哈希函数之一：

  - 如果您的网络中安装的所有安全应用程序实例都是 Kaspersky Endpoint Security 10 或更高版本，请选择“**SHA256**”复选框。我们不建议基于 Kaspersky Endpoint Security 10 或更早版本的可执行文件的 SHA256 哈希值创建类别。这可能会导致安全应用程序出现故障。在这种情况下，您可以对该类别的文件使用 MD5 加密哈希函数。
  - 如果您的网络中安装了早于 Kaspersky Endpoint Security 10 的版本，请选择“**MD5 哈希**”复选框。对于 Kaspersky Endpoint Security 10 或更高版本，无法根据可执行文件的 MD5 哈希值添加类别。在这种情况下，您可以对该类别的文件使用 SHA256 加密哈希函数。
  - 如果您的网络中包含使用 Kaspersky Endpoint Security 10 更早及更高版本的设备，请同时选择 **SHA256** 复选框和 **MD5 哈希** 复选框。

  **元数据**

  如果选择此选项，您可以指定文件元数据，例如文件名、文件版本和供应商。类别条件仅匹配元数据相同的可执行文件。

  **证书**

  如果选择此选项，您可以从证书商店指定证书。该类别条件仅匹配使用指定证书签名的可执行文件。

- **从 MSI 包/存档文件夹**

  如果选择此选项，您可以将 MSI 安装程序文件指定为将应用程序添加到自定义类别的条件。应用程序安装程序的元数据被发送到管理服务器。安装程序元数据与指定 MSI 安装程序匹配的应用程序将被添加到自定义应用程序类别中。

步骤 4. 设置

如果您选择了以下类别类型，则可以执行此步骤：**包含所选设备上可执行文件的类别。这些可执行文件被自动处理，它们的度量数据被添加到类别中**。

在此步骤中，单击“**添加**”按钮并指定 Kaspersky Security Center 将其可执行文件添加到应用程序类别的计算机。

在此步骤中，配置以下设置：

- **哈希函数计算的算法**

  根据网络中设备上安装的安全应用程序版本，您需要选择 Kaspersky Security Center 应用于该类别文件的哈希算法。哈希函数计算出的哈希值信息存储在管理服务器的数据库中。

  *SHA256 是一种加密哈希函数，其算法没有已知的弱点；它目前被认为是安全性最高的哈希函数*。Kaspersky Endpoint Security for Linux 支持 SHA256。

  选择要应用于该类别文件的哈希算法之一：

  - 如果您在受保护的设备上使用 Kaspersky Endpoint Security for Linux，请选中 **为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)** 复选框。
  - 如果您在受保护的设备上使用 Kaspersky Endpoint Security for Windows，请选中 **为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)** 复选框。

  如果您在网络上同时使用 Windows 和 Linux 应用程序，请选中这两个复选框。

- **将数据与管理服务器存储同步**

  如果您希望管理服务器定期检查指定的文件夹（或多个文件夹）中的更改，请选择此选项。

  默认禁用此选项。

  如果启用此参数，请指定检查指定文件夹（或多个文件夹）的更改的时间段（以小时为单位）。默认情况下，时间段被设置为 24 小时。

- **文件类型**

  在此区域中，您可以指定要用于创建应用程序类别的文件类型。

  “**所有文件**”。该类别将匹配所有文件。默认情况下已启用此选项。

  “**仅应用程序类别之外的文件**”。该类别将仅匹配应用程序类别之外的文件。

- **文件夹**

  在此区域中，您可以指定选定计算机的文件夹，其中包含要用于创建应用程序类别的文件。

  “**所有文件夹**”。该类别将匹配所有文件夹。默认情况下已启用此选项。

  “**指定文件夹**”。该类别将仅与指定的文件夹匹配。如果选择此选项，则需要指定文件夹路径。

步骤 5.

如果您选择了以下类别类型，则可以执行此步骤：**包含指定文件夹内可执行文件的类别。复制到指定文件夹的应用程序可执行文件被自动处理，它们的度量数据被添加到类别中。**

在此步骤中，指定一个文件夹，该文件夹中的可执行文件将用于创建类别。

管理以下设置：

- **包含动态链接库 (DLL) 到该类别**

  应用程序类别包括动态链接库（DLL 格式的文件），应用程序控制组件会记录在系统中运行的此类库的操作。在应用程序类别中包含 DLL 文件可能降低 Kaspersky Security Center的性能。

  默认情况下已清空该复选框。

- **包含脚本数据到该类别**

  应用程序类别包括脚本数据，并且 Web 威胁防护不会阻止脚本。在类别中包含脚本数据可能会降低 Kaspersky Security Center 的性能。

  默认情况下已清空该复选框。

- **哈希函数计算的算法**

  根据网络中设备上安装的安全应用程序版本，您需要选择 Kaspersky Security Center 应用于该类别文件的哈希算法。哈希函数计算出的哈希值信息存储在管理服务器的数据库中。

  *SHA256 是一种加密哈希函数，其算法没有已知的弱点；它目前被认为是安全性最高的哈希函数。*Kaspersky Endpoint Security for Linux 支持 SHA256。

  选择要应用于该类别文件的哈希算法之一：

  - 如果您在受保护的设备上使用 Kaspersky Endpoint Security for Linux，请选中 **为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)** 复选框。
  - 如果您在受保护的设备上使用 Kaspersky Endpoint Security for Windows，请选中 **为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)** 复选框。

  如果您在网络上同时使用 Windows 和 Linux 应用程序，请选中这两个复选框。

- **强制扫描文件夹以查找更改**

  如果启用此选项，应用程序将定期检查用于添加类别内容的文件夹是否有更改。您可以在复选框旁边的输入字段中指定检查频率（以小时为单位）。默认情况下，强制检查之间的时间间隔为 24 小时。

  如果禁用此选项，应用程序不会强制对该文件夹执行任何检查。服务器会尝试访问已被修改、添加或删除的文件。

  默认情况下已清空该复选框。

步骤 6.

结束向导。向导完成后，即可创建新的应用程序类别。您可以使用应用程序控制规则控制该类别中的应用程序。

## 黄金镜像

您可以使用清查来添加 Golden Image 应用程序类别。默认情况下，该类别为空。“黄金镜像”类别包括随操作系统一起交付到设备的应用程序。此类别中的应用程序被视为受信任。如有必要，您可以将第三方应用程序添加到该类别。

完成清查任务后，应用程序可以按如下方式修改“黄金镜像”类别：

- **无更改** – 完成清查后，不更改“黄金镜像”类别。这是默认选择。如果您想获取设备上使用的第三方应用程序列表，但不想将它们添加到“黄金镜像”类别，请使用此选项。
- **更新或创建(如果不存在)** – 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。如果该类别不存在，则创建该类别。如果该类别已存在，则更新该类别的应用程序列表。
- **删除** – 清除“黄金镜像”应用程序类别。任务启动后会立即清除此类别，而不会对设备上的文件进行清查。

  这在以下场景中可能很有用：

  - 如果您需要阻止设备上“黄金镜像”类别中的应用程序在设备上启动，但无法禁用应用程序控制规则。
  - 如果您将包含与当前策略不同的应用程序控制规则的新策略应用于设备，或者将设备移动到子策略时。在这种情况下，建议清除“黄金镜像”类别，以避免错误阻止允许的应用程序。

### 基于基线计算机配置“黄金镜像”类别

您可以使用基线计算机创建包含所需应用程序集的“黄金镜像”类别。然后，您可以使用此类别创建应用程序控制允许规则。

基于基线计算机配置“黄金镜像”类别涉及以下步骤：

1. **配置参考计算机**

   安装并配置设备在企业网络上运行所需的所有软件，包括 Kaspersky Endpoint Security for Linux 和网络代理。

2. **创建清查任务**

   在 Web Console 或命令行中创建任务，并管理以下设置：

   - 对“黄金镜像”应用程序类别执行的操作:**更新或创建(如果不存在)**；

     ```
     GoldenImageAction=Create
     ```

   - 清查范围为参考计算机。

3. **运行清查任务并等待其完成。**

   该任务会生成“黄金镜像”应用程序类别。

4. **将类别列表导出到文件。**

   > 您无法在 Web Console 中导出类别列表。

   请执行命令：

   ```
   kesl-control [-A] --get-categories --file <path to file> --json
   ```

   其中，`<path to file>` 是要将任务设置输出到的配置文件的路径。

5. **如有必要，请调整“黄金镜像”类别**

   查看包含应用程序类别列表的配置文件。如有必要，请在“黄金镜像”类别中调整应用程序列表。

6. **从配置文件导入设置。**

   如果您已修改包含应用程序类别列表的配置文件，请将其导入应用程序：

   ```
   kesl-control [-A] --set-categories --names GoldenImage [<category name 1> <category name 2> ... <name of category N>] --file <path to file>
   ```

   其中，`<category name 1> <category name 2> ... <category name N>` 是除“黄金镜像”类别之外、您想要更改其信息的类别的名称。

   `<path to file>` 是要将任务设置输出到的配置文件的路径。

因此，您可以使用“黄金镜像”类别创建应用程序控制规则。

# 关于应用程序控制规则

*应用程序控制规则*是一组条件，用于确定应用程序控制是允许还是拒绝为选定用户组启动第三方应用程序。

这些规则根据以下条件限制第三方应用程序的启动：

- **应用程序类别**。应用程序是否属于应用程序类别。

  > 每个类别只能在一条规则中使用。

- **用户和用户组**。应用程序控制允许限制单个用户或用户组访问第三方应用程序。例如，您可以限制组织中除 IT 部门用户以外的所有用户访问远程管理应用程序。

应用程序控制规则可以具有以下*操作状态*之一：

- **已启用**。应用程序控制应用该规则。
- **已禁用**。应用程序控制不应用该规则。
- **测试**。应用程序控制不会阻止第三方应用程序运行，但会将有关其启动的通知发送到管理服务器。

### 如何在 Web Console 中添加应用程序控制规则

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **应用程序控制**。
5. 确保该组件的切换开关处于 **应用程序控制已启用** 位置。
6. 在“**启动应用程序时的操作**”块中单击“**添加**”按钮。
   这将打开用于添加应用程序控制规则的表单。
7. 在“**状态**”字段中设置规则的状态。
8. 如果要测试该规则，请将此切换开关设置为 **已启用**，并选中 **测试模式** 复选框。
9. 在“**规则名称**”字段中输入规则名称。规则名称必须唯一。
10. 选择要应用该规则的应用程序类别。如果未指定类别，则无法保存规则。
11. 选择用户或用户组及其运行应用程序的权限。
12. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行中添加应用程序控制规则

1. 将应用程序控制规则列表输出到文件：

   ```
   kesl-control --get-settings 21 --file <path to file> [--json]
   ```

2. 打开配置文件，并根据应用程序控制模式，为 ID 为 `#` 的规则添加一个部分：

   a. 如果选择了 `AppControlMode=AllowList`：

   ```
   [AllowListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [AllowListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   模式

b. 如果选择了 `AppControlMode=DenyList`：

```
[DenyListRules.item_#]
Description=<rule name>
AppControlRuleStatus=<On|Off|Test>
Category=<category name>
[DenyListRules.item_#.ACL.item_#]
Access=<Allow|Block>
Principal=<user>
```

模式

3. 将配置文件中的设置导入到应用程序中：

```
kesl-control --set-settings 21 --file <path to file> [--json]
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `[AllowListRules.item_#]`<br>`[DenyListRules.item_#]` | ID 为 `#` 的应用程序控制规则。 |
| `[AllowListRules.item_#.ACL.item_#]`<br>`[DenyListRules.item_#.ACL.item_#]` | ID 为 `#` 的应用程序控制规则适用的用户列表。 |
| `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：<br>`On`（默认值）– 规则已启用，Kaspersky Endpoint Security 对"应用程序控制"应用此规则。<br>`Off` – 该规则不用于"应用程序控制"。<br>`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。<br>您可以指定 `Golden Image` 类别。 |
| `Access` | 分配给用户或用户组的访问类型：<br>`Allow`（默认值）– 允许运行应用程序。<br>`Block` – 拒绝运行应用程序。 |
| `Principal` | 应用程序控制规则适用的用户或用户组：<br>`\Everyone`（默认值）：规则适用于所有用户。<br>`<user>` 是规则适用的用户的名称。<br>`@<group name>` 是规则适用的用户组的名称。 |

# 应用程序控制规则测试模式

为确保应用程序控制不会阻止运行所需的应用程序，建议您测试应用程序控制规则。在测试模式下，Kaspersky Endpoint Security 会阻止第三方应用程序运行，并将有关其启动的通知发送到管理服务器。

默认情况下，应用程序控制允许所有第三方应用程序运行，但规则禁止的应用程序除外。

测试应用程序控制规则

1. **创建应用程序控制规则**

   配置并启用应用程序控制规则，以便进行测试。例如，您可以创建规则，以阻止执行任何第三方应用程序，但“黄金镜像”和“工作应用程序”类别中的应用程序除外。

2. **在测试模式下启用应用程序控制**

   **如何在 Web Console 中启用应用程序控制的测试模式**

   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
   2. 单击 Kaspersky Endpoint Security 策略的名称。
      策略属性窗口将打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择 **安全控制** → **应用程序控制**。
   5. 确保该组件的切换开关处于 **应用程序控制已启用** 位置。
   6. 在 **启动应用程序时的操作** 下，选择应用程序控制的 **通知** 操作。
   7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

   **如何在命令行中启用应用程序控制的测试模式**

   要为应用程序控制选择测试模式，请运行以下命令：

   ```
   kesl-control --set-settings 21 AppControlRulesAction=TestRules
   ```

3. **查看测试结果**

   查看发送到 Kaspersky Security Center 的应用程序控制报告和该组件的事件。

   **如何在 Web Console 中查看应用程序控制报告**

   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
   2. 单击 Kaspersky Endpoint Security 策略的名称。
      策略属性窗口将打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择 **安全控制** → **应用程序控制**。
   5. 确保该组件的切换开关处于 **应用程序控制已启用** 位置。
   6. 在应用程序控制规则表中，单击“**查看报告**”按钮。
   7. “**测试模式中禁止的应用程序报告**”窗口将打开。
   8. 查看有关在测试模式下启动被禁止应用程序的信息。

**如何查看应用程序控制测试运行产生的事件**

1. 在 Web Console 的主窗口中，选择“**监控**” → “**事件分类**”。
2. 单击“**添加**”。
3. 在打开的 **新事件分类** 窗口中，指定该选择的名称。例如，“应用程序控制规则测试”。
4. 转到 **事件** 区域并管理以下设置：
   - **应用程序名称** – Kaspersky Endpoint Security for Linux。
   - **严重级别** – **信息**。
   - 请选择**包含所选常规事件**选项。
   - 选中 **禁止应用程序在测试模式下启动** 和 **允许应用程序在测试模式下启动** 事件对应的复选框。
5. 如有需要，配置其余设置。
6. 保存更改。
7. 单击选择的名称以查看事件选择结果。

4 **调整规则**

如果对于计算机用户工作所需的所有应用程序，测试模式都不会产生阻止启动事件，则说明创建了正确的规则。

否则，请编辑已创建规则的设置，创建附加规则或删除现有规则。

# 系统完整性监控

系统完整性监控组件监控操作系统中可能预示计算机安全漏洞的变化。当检测到此类变化时，Kaspersky Endpoint Security 会生成相应的事件并向管理员发出警报。

## 系统完整性监控的工作原理

系统完整性监控可以实时或按需运行：

- *系统完整性监控* 组件允许您*实时*监控已纳入监控范围的文件和目录的更改。
- *系统完整性检查* 功能允许您将已纳入监控范围的对象的当前状态与其记录状态进行比较，可以*按计划或按需*进行。

“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。

### 特殊注意事项和限制

- 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。
- 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。

## 实时系统完整性监控

系统完整性监控允许实时检测监控范围内对象的更改。

### 系统完整性监控的工作原理

1. **应用程序拦截文件操作事件**

   应用程序使用一种特殊的拦截机制，该机制对正在扫描的文件具有只读访问权限。

2. **应用程序会检查文件是否已被修改。**

   系统完整性监控会跟踪以下文件属性的更改：

   - 内容（`write ()`、`truncate ()` 和其他修改）
   - 元数据（使用 `chmod` 或 `chown` 命令更改访问权限）
   - 时间戳（`utimensat`）
   - 扩展属性（`setxattr`）及其他

3. **扫描完成**

   如果文件已被修改，应用程序会生成一个 *系统完整性检查失败* 事件。

### 配置系统完整性监控

1. **启用系统完整性监控**

   默认情况下禁用系统完整性监控。选择要实时监控文件更改的设备，并在这些设备上启用系统完整性监控组件。

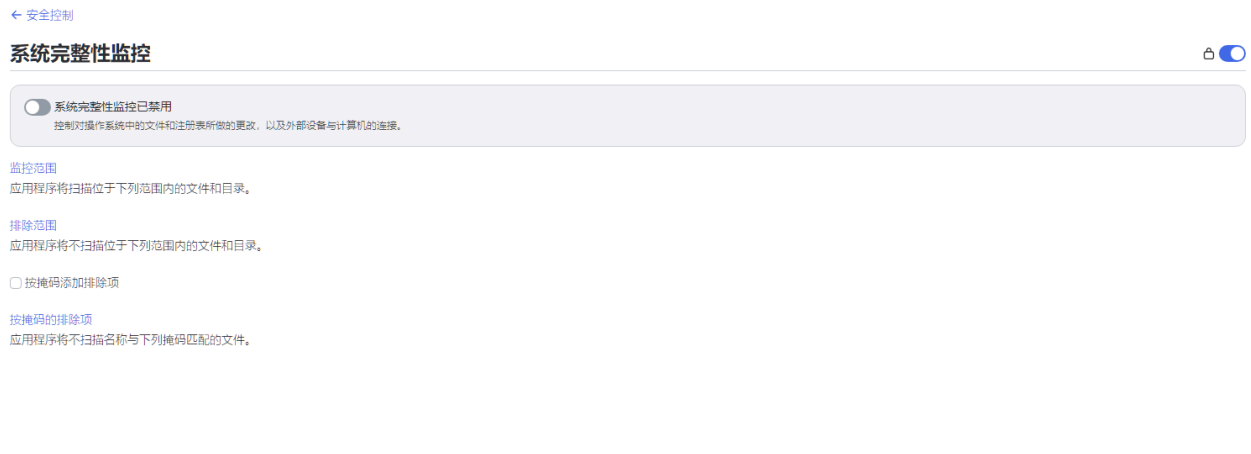
2. **配置监控范围**

   要使该组件正常工作，必须至少指定一个监控范围。默认设置 *卡巴斯基内部对象*（`/opt/kaspersky/kesl/`）监控范围。

   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。

### 如何在 Web Console 中配置监控范围

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **系统完整性监控**。
5. 单击**监控范围**链接。
   这将打开一个包含扫描范围表的窗口。
6. 单击“**添加**”。
   这将打开用于添加扫描范围的窗口
7. 在 **名称** 字段中，指定监控范围的名称，例如 *关键对象*。
8. 在 **路径** 字段中，指定单个文件或目录的路径（例如 `/path/to/folder`）。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。
9. 如有必要，请以命令 shell 格式指定对象名称掩码（例如 `*.txt` 或 `file?.*`）。逐个添加掩码。
10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




系统完整性监控

### 如何在命令行上配置监控范围

1. 运行以下命令：

```
kesl-control --set-settings 11  ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 11
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `UseScanArea=Yes` | 启用 ID 为 `#` 的监控范围。<br>您可以暂时禁用监控范围扫描，而不是删除该范围。为此，请设置 `ScanScope.item_#.UseScanArea=No`。 |
| `AreaDesc` | 监控范围的说明；包含有关监控范围的其他信息。 |
| `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。<br>例如，`ScanScope.item_0001.AreaMask.item_0001=*.exe`<br>`ScanScope.item_0001.AreaMask.item_0002=*.txt`。 |
| `Path` | 监控目录的路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |

示例

仅包含 `/etc` 目录的监控范围：

```
kesl-control --set-settings 11 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

### 3 配置排除项范围

排除项的优先级高于监控范围。即使排除的对象位于监控范围内，也不会对其进行扫描。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。

**如何在 Web Console 中配置排除范围**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制 → 系统完整性监控**。

您可以按路径或文件名掩码指定排除项。应用程序可以从扫描中排除整个目录（或单个文件），也可以排除监控范围内文件名掩码匹配的文件。

*要按路径添加排除项：*

1. 单击**排除范围**链接。
   这将打开一个包含排除范围表的窗口。
2. 单击“**添加**”。
   这将打开用于添加排除范围的窗口。
3. 在 **名称** 字段中，指定排除范围的名称，例如 *系统文件*。
4. 在 **路径** 字段中，指定单个文件或目录的路径（例如 `/path/to/folder`）。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

5. 以命令 shell 格式指定对象名称掩码（例如 `*.txt` 或 `file?.*`）。逐个添加掩码。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

*要按文件名掩码添加排除项：*

1. 选择**按掩码添加排除项**复选框。

2. 单击**按掩码的排除项**链接。
   这将打开按掩码指定的排除范围表。

3. 单击“**添加**”。
   这将打开用于按掩码添加排除范围的窗口。

4. 以命令 shell 格式指定文件名掩码（例如 `*.txt` 或 `file?.*`）。逐个添加掩码。

5. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行配置排除范围**

1. 运行以下命令：

```
kesl-control --set-settings 11  ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 11
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `UseScanArea=Yes` | 从监控中排除具有 `#` ID 的指定范围。<br>您可以暂时禁用排除范围，而不是删除该范围。为此，请设置 `ExcludedFromScanScope.item_#.UseScanArea=No`。 |
| `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。 |
| `AreaMask.item_#` | 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 格式的掩码指定的对象。<br>例如，`ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`。 |
| `Path` | 要从扫描中排除的目录的路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |

示例

仅包含 `/tmp` 目录的排除范围：

```
kesl-control --set-settings 11 ExcludedFromScanScope.item_0001.UseScanArea=Yes
```

```
ScanScope.item_0001.Path=/tmp
```

# 系统完整性检查

运行 *系统完整性检查* 任务时，应用程序会将每个对象的当前状态与其原始状态（即基线）进行比较。基线包含受监控对象及其元数据的路径。这允许跟踪监控范围内所包含文件和目录的变化。

> 基线可能也包含个人数据。

与 系统完整性监控 组件相比，*系统完整性检查* 任务有助于限制事件数量，并允许您生成操作系统变化的摘要报告。

## 系统完整性检查的工作原理

1. **应用程序创建系统快照**

   系统基线在首次运行任务时创建。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。对于 Linux 设备，当任务设置发生更改（例如，添加新的监控范围）时，以及在启用 **每次任务启动时重建基线** 设置的情况下启动任务时，都会重建基线。

   基线存储位于 `/var/opt/kaspersky/kesl/private/fim.db`。需要 root 特权才能访问包含基线的数据库。基线会随关联的系统完整性检查任务一起删除。

2. **应用程序查找系统状态的变化**

   应用程序采用以下条件来比较监控范围内所含对象的信息：

   - 文件的 SHA256 哈希值（用于完整检查）
   - 文件更改时间
   - 文件大小

3. **扫描完成**

   如果系统的当前状态与基线不同，Kaspersky Endpoint Security 将生成系统完整性违规事件：*系统完整性检查失败*。

## 配置并运行系统完整性检查任务

1. **创建系统完整性检查任务**

   **如何在 Web Console 中创建系统完整性检查任务**

   1. 在 Web Console 的主窗口中，选择“**任务**”。

      任务列表打开。

   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“**Kaspersky Endpoint Security for Linux 12.5**”。

   b. 在“**任务类型**”下拉列表中，选择“**系统完整性检查**”。

   c. 在“**任务名称**”字段中，输入简要说明，例如“*每周系统完整性检查*”。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。

5. 结束向导。

**如何在命令行上创建系统完整性检查任务**

要创建任务，请运行以下命令：

```
kesl-control --create-task <task name> --type ODFIM
```

其中，`<task name>` 是新任务的名称。

此命令返回已创建任务的 ID。

**命令执行结果示例**：

已创建任务（任务 ID：115）

2. **如有必要，请编辑任务设置**

   **如何在 Web Console 中配置系统完整性检查任务**

   1. 在 Web Console 的主窗口中，选择“**任务**”。
      任务列表打开。

   2. 单击新创建的系统完整性检查任务。
      任务属性窗口将打开。

   3. 选择**应用程序设置**选项卡。

   4. 选择扫描类型：

      - “**全盘扫描**”。应用程序会将文件当前状态下的 SHA256 哈希值与系统快照中的哈希值进行比较。
      - “**快速扫描**”。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。

5. 在“**系统完整性检查设置**”区域中，选中以下复选框：

   - “**每次任务启动时重建基线**”。如果选中此复选框，应用程序会在每次启动任务时重新构建基线。
   - “**跟踪监控范围中的目录**”。如果选中此复选框，应用程序将检查用户指定的目录。如果清除此复选框，则应用程序仅扫描默认扫描范围 – *Kaspersky 内部对象* (`/opt/kaspersky/kesl/`)。
   - “**跟踪每次任务启动时上次访问文件的时间**”。如果选中此复选框，则每次运行任务时，应用程序都会检查文件的最后访问时间（`noatime` 参数）。

6. 保存更改。

**如何在命令行上配置系统完整性检查任务**

请执行命令：

```
kesl-control --set-settings <task ID|name> RebuildBaseline=<Yes|No> [CheckFileHash=<Yes|No>]
[TrackDirectoryChanges=<Yes|No>] [TrackLastAccessTime=<Yes|No>] [UseExcludeMasks=<Yes|No>]
[ExcludeMasks.item_#=<object mask>]
```

符号

*系统完整性检查任务设置*

| 设置 | 描述 |
|---|---|
| `RebuildBaseline` | 每次任务启动时重新构建基线。 |
| `CheckFileHash` | 扫描文件的 SHA256 哈希值。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` | 扫描用户指定的目录。如果禁用此设置，应用程序仅扫描默认范围（`/opt/kaspersky/kesl/`）。 |
| `TrackLastAccessTime` | 检查文件的最后访问时间（`noatime` 选项）。 |
| `UseExcludeMasks` | 监控排除项。任务设置中将添加一个新的 `[ExcludeMasks.item_#]` 部分。应用程序将不会扫描此部分中指定的对象。<br>仅当指定 `ExcludeMasks.item_#` 设置时，此设置才适用。 |
| `ExcludeMasks.item_#=<object mask>` | 从监控范围中排除对象。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，或者使用命令 Shell 格式的掩码一次性排除多个文件。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。<br>只有启用 `UseExcludeMasks` 参数时，才能管理此设置。<br>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。<br>示例：`ExcludeMasks.item_0000=<eicar1.*>` |

### 3 配置监控范围

要启动任务，必须指定至少一个监控范围。默认设置 *卡巴斯基内部对象*（`/opt/kaspersky/kesl/`）监控范围。

仅当基线包含有关属于任务监控范围的对象的信息时，才会运行任务。

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。

**如何在 Web Console 中配置监控范围**

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击新创建的系统完整性检查任务。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 确保“**跟踪监控范围中的目录**”复选框被选中。

5. 在“**监控和排除范围**”区域，单击“**监控范围**”链接。
   这将打开一个包含扫描范围表的窗口。

6. 单击“**添加**”。
   这将打开用于添加扫描范围的窗口

7. 在 **名称** 字段中，输入监控范围的名称，例如 *桌面上的文件*。

8. 在 **路径** 字段中，指定单个文件或目录的路径（例如 `/path/to/folder`）。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

9. 如有必要，请以命令 shell 格式指定对象名称掩码（例如，`*.txt`、`file?.*`）。逐个添加掩码。

10. 保存更改。

**如何在命令行上配置监控范围**

1. 运行以下命令：

```
kesl-control --set-settings <task ID|name> TrackDirectoryChanges=Yes ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. 要检查当前设置，请运行以下命令：

```
kesl-control --get-settings <task ID|name>
```

符号

*系统完整性检查任务设置*

| 设置 | 描述 |
|---|---|
| `UseScanArea=Yes` | 启用 ID 为 `#` 的监控范围。<br>您可以暂时禁用监控范围扫描，而不是删除该范围。为此，请设置 `ScanScope.item_#.UseScanArea=No`。 |
| `AreaDesc` | 监控范围的说明；包含有关监控范围的其他信息。 |
| `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。<br>您可以按任意顺序指定多个 `ScanScope.item_#.AreaMask.item_#` 项目。应用程序将按索引升序处理范围。<br>例如，`ScanScope.item_0001.AreaMask.item_0001=*.exe`<br>`ScanScope.item_0001.AreaMask.item_0002=*.txt`。 |
| `Path` | 监控目录的路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |

**示例**

仅包含 `/etc` 目录的监控范围：

```
kesl-control --set-settings 115 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

### 4 配置排除项范围

排除项的优先级高于监控范围。即使排除的对象位于监控范围内，也不会对其进行扫描。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。

**如何在 Web Console 中配置排除范围**

1. 在 Web Console 的主窗口中，选择“**任务**”。
2. 任务列表打开。
3. 单击新创建的系统完整性检查任务。
   任务属性窗口将打开。
4. 选择**应用程序设置**选项卡。

您可以按路径或文件名掩码指定排除项。应用程序可以从扫描中排除整个目录（或单个文件），也可以排除监控范围内文件名掩码匹配的文件。

*要按路径添加排除项：*

1. 在“**监控和排除范围**”区域，单击“**排除范围**”链接。
   这将打开一个包含排除范围表的窗口。
2. 单击“**添加**”。
   这将打开用于添加排除范围的窗口。
3. 在 **名称** 字段中，指定排除范围的名称，例如 *系统文件*。
4. 在 **路径** 字段中，指定单个文件或目录的路径（例如 `/path/to/folder`）。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。
5. 以命令 shell 格式指定对象名称掩码（例如 `*.txt` 或 `file?.*`）。逐个添加掩码。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

*要按文件名掩码添加排除项：*

1. 在“**监控和排除范围**”区域，单击“**按掩码的排除项**”链接。
   这将打开按掩码指定的排除范围表。
2. 单击“**添加**”。
   这将打开用于按掩码添加排除范围的窗口。
3. 以命令 shell 格式指定文件名掩码（例如 `*.txt` 或 `file?.*`）。逐个添加掩码。
4. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行配置排除范围**

1. 运行以下命令：

```
kesl-control --set-settings <task ID|name>      ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. 要检查当前设置，请运行以下命令：

```
kesl-control --get-settings <task ID|name>
```

符号

*系统完整性检查任务设置*

| 设置 | 描述 |
| --- | --- |
| `UseScanArea=Yes` | 从监控中排除具有 `#` ID 的指定范围。<br>您可以暂时禁用排除范围，而不是删除该范围。为此，请设置 `ExcludedFromScanScope.item_#.UseScanArea=No`。 |
| `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。 |
| `AreaMask.item_#` | 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 格式的掩码指定的对象。<br>您可以按任意顺序指定多个 `ExcludedFromScanScope.item_#.AreaMask.item_#` 项目。应用程序将按索引升序处理范围。<br>例如，`ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`。 |
| `Path` | 要从扫描中排除的目录的路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |

**示例**

仅包含 `/tmp` 目录的排除范围：

```
kesl-control --set-settings 115 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

### 5 运行任务

**如何在 Web Console 中运行系统完整性检查任务**

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 选中已创建任务旁边的复选框。
3. 单击“**开始**”。

**如何在命令行运行系统完整性检查任务**

要运行任务，请运行以下命令：

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

其中：

- `<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。
- `[-W]` 启用与此任务相关的当前事件的输出。
- `[--progress]` 启用任务进度的显示。

# 信任区域

受*信任区域*是由系统管理员配置的、Kaspersky Endpoint Security 在活动期间不予监控的对象和应用程序的列表。

考虑到所处理对象的特点和安装在计算机上的应用程序，管理员可以自主创建受信任区域。当 Kaspersky Endpoint Security 阻止访问特定对象或应用程序时，如果您确定此对象或应用程序是无害的，则有必要将其包含在受信任区域中。

受信任区域设置

| 设置 | 描述 |
| --- | --- |
| **网址** | Web 威胁防护组件认为受信任的网址。该组件不会扫描来自这些地址的传入和传出流量以检测威胁。如果该组件干扰从已知网站下载文件，则可以使用受信任地址列表。<br><br>有关更多信息，请参阅 如何添加受信任的网址 一文 |
| **IP 地址** | 受信任设备的 IP 地址。网络威胁防护组件不会阻止来自这些地址的网络活动。<br>应用程序也不会记录有关来自排除列表中的 IP 地址的网络攻击的信息。<br>有关更多信息，请参阅 如何添加计算机的受信任 IP 地址 一文 |
| **网络端口** | 网络威胁防护组件排除扫描的网络端口列表。<br>有关更多信息，请参阅 如何选择受监控的网络端口 一文 |
| **根证书** | Kaspersky Endpoint Security 认为受信任的根证书。当 Web 威胁防护、邮件威胁防护 和 Web 控制 组件扫描加密连接（HTTPS 连接）时，将使用受信任的根证书列表。<br>有关更多信息，请参阅 如何将证书添加到受信任的根证书列表 一文 |
| **域** | 受信任域列表。Web 威胁防护和Web 控制组件不会控制与这些域的加密连接。<br>有关更多信息，请参阅 如何添加受信任域 一文 |
| **挂载点** | 受信任挂载点列表。文件威胁防护、反加密勒索和容器扫描组件会将指定的挂载点排除在扫描范围之外。<br><br>必须以与 `mount` 命令输出中所显示的相同方式指定挂载点。<br><br>有关更多信息，请参阅"如何排除挂载点"一文 |
| **应用程序** | Kaspersky Endpoint Security 不会控制其文件和网络活动或系统注册表访问的应用程序。保护组件（例如 文件威胁防护 或 行为检测）不会控制指定应用程序的活动。<br>有关更多信息，请参阅 如何添加受信任的应用程序 一文 |
| **恶意软件扫描排除项** | 被所有或部分应用程序组件排除在扫描范围之外的文件或文件夹，以及对象类型（根据 病毒百科全书 ）。<br>有关更多信息，请参阅 如何添加保护排除项 一文 |
| **设备** | 设备控制组件始终允许所选用户或组完全访问的设备。<br>有关更多信息，请参阅 如何添加受信任设备 一文 |

# 如何添加保护排除项

*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。

可以使用以下方法从扫描中排除对象：

- **排除**。目录路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。例如：`/.snapshots/*/snapshot/`。

  要指定容器或镜像中的路径，请使用标签。

**如何使用标签**

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名称

`<path to local directory>` 是本地目录的路径。

您还可以使用唯一的标签组合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

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:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

- **按掩码筛选的排除项**。使用掩码指定的文件名。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。示例：`*.txt` 掩码会涵盖所有文本文件。

使用掩码：

- `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和目录路径中的文件和目录名称的分隔符）。例如，掩码 `/dir/*/*.txt` 将包括位于 dir 目录内各目录中（但不包括这些目录的子目录中）的所有 TXT 扩展名文件的路径。

- 两个连续的 `*` 字符在文件或目录名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和目录路径中的文件和目录名称的分隔符）。例如，掩码 `/dir/**/*.txt` 将包括位于 dir 目录内嵌套目录中的所有 TXT 扩展名文件的路径，但不包括 dir 目录本身。

- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和目录路径中的文件和目录名称的分隔符）。例如，`/dir/???.txt` 掩码将包括位于 dir 目录中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

- **按威胁名称筛选的排除项** 根据 卡巴斯基百科全书 分类的对象类型名称（例如，`Email-Worm`、`Rootkit` 或 `RemoteAdmin`）。您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，应用程序从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

- **按进程筛选的排除项** 进程路径。

Kaspersky Endpoint Security 还允许排除某些格式的文件：压缩文件、电子邮件数据库、文本文件、数据库日志文件。

**如何在 Web Console 中添加保护排除项**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**主机威胁防护 → 文件威胁防护**”。
5. 单击**扫描排除项**链接。
6. 在打开的窗口中，单击“**添加**”按钮。
7. 选中要用于保护排除项的条件对应的复选框：

   - “**文件或文件夹路径**”。指定文件或目录路径，或者文件名掩码。要指定容器或镜像中的路径，请使用标签。

     对于本地文件系统，请指定目录路径（例如，`/path/to/folder/`）。对于已挂载的文件系统或所有远程挂载的文件系统，请输入文件名掩码。对于已挂载的文件系统，还要指定访问协议（NFS、Samba 或自定义）。

   - “**对象类型**”。指定威胁名称。

   - “**对象哈希**”。输入对象的 SHA256 哈希值。您还可以添加文件或指定事件，以便从中获取用于排除项的 SHA256 哈希值。

8. 选择要应用排除项的保护组件：

- “**所有保护组件**”。该排除项将应用于受 **恶意软件扫描排除项** 影响的所有保护组件。
- “**所选保护组件**”。选择要应用排除项的组件：文件威胁防护、反加密勒索、漏洞利用防御。

9. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中添加保护排除项**

1. 要按路径添加排除项，请运行以下命令：

```
kesl-control --set-settings 1 --add-exclusion <path>
```

2. 要按掩码添加排除项，请按照以下步骤操作：

   a. 启用按掩码排除文件：

   ```
   kesl-control --set-settings 1 UseExcludeMasks=Yes
   ```

   b. 添加文件掩码：

   ```
   kesl-control --set-settings 1 ExcludeMasks.item_#=<file mask>
   ```

3. 要按威胁名称添加排除项，请按照以下步骤操作：

   a. 启用按威胁名称排除文件：

   ```
   kesl-control --set-settings 1 UseExcludeThreats=Yes
   ```

   b. 添加威胁名称：

   ```
   kesl-control --set-settings 1 ExcludeThreats.item_#=<threat name>
   ```

4. 要检查组件设置的当前值，请运行以下命令：

```
kesl-control --get-settings 1
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `--add-exclusion` | 从扫描中排除目录。任务设置中将添加一个新的 `[ExcludedFromScanScope.item_#]` 部分。应用程序会从扫描中排除 `path` 设置指定的目录中的对象。 |
| `ExcludeMasks.item_#` | 按名称或掩码在扫描中排除对象。使用 shell 格式的掩码输入文件名。例如：`ExcludeMasks.item_0000=*_my_file_??.html`。 |
| `ExcludeThreats.item_#` | 按对象中检测到的威胁的名称从扫描中排除对象。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。<br>例如，您可能正在使用实用程序来获取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。例如：`ExcludeThreats.item_0000=EICAR-Test-*`。 |

# 如何添加受信任网址

除了恶意和钓鱼网站，Web 威胁防护还可以阻止其他网站。例如，Web 威胁防护阻止不满足 RFC 标准的 HTTP 流量。您可以为您信任其内容的网址创建一个列表。“Web 威胁防护”组件不会分析来自受信任网址的信息，不会检查它们中是否含有病毒或其他威胁。在一些情况下本选项十分有用，例如，当“Web 威胁防护”组件干扰您从一个已知网站上下载文件时。

### 如何在 Web Console 中添加受信任网址

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**受信任区域**区域。
5. 在打开的窗口中，单击“**网址**”链接。
   这将打开一个包含受信任网址列表的窗口。
6. 为您信任其内容的网页或网址创建列表。
   输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。
   您也可以从 JSON 文件导入受信任网址列表。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行中添加受信任网址

1. 要启用受信任网址列表，请运行以下命令：

   ```
   kesl-control --set-settings 14 UseTrustedAddresses=Yes
   ```

2. 要添加受信任网址，请运行以下命令：

   ```
   kesl-control --set-settings 14 TrustedAddresses.item_#=<trusted web address>
   ```

3. 要检查组件设置的当前值，请运行以下命令：

   ```
   kesl-control --get-settings 14
   ```

### 示例

```
kesl-control --set-settings 14 TrustedAddresses.item_001=https://example.com/
```

# 如何添加计算机的受信任 IP 地址

Kaspersky Endpoint Security 可以识别网络攻击并阻止不安全的传输大量数据包的网络连接（例如，从摄像头）。要使用收信人设备，您可以添加这些设备的 IP 地址到排除项列表。受信任的网址会影响 网络威胁防护 组件。

### 如何在 Web Console 中配置从阻止中排除的地址

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**受信任区域**区域。
5. 在打开的窗口中，单击“**IP 地址**”链接。
   这将打开一个包含受信任 IP 地址列表的窗口。
6. 在打开的窗口中，单击“**添加**”按钮。
7. 输入不阻止网络攻击的计算机的 IP 地址。
   如有必要，请指定子网。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行配置从阻止中排除的地址

1. 要应用受信任 IP 地址，请运行以下命令：

   ```
   kesl-control --set-settings 17 UseExcludeIPs=Yes
   ```

2. 要添加受信任 IP 地址，请运行以下命令：

   ```
   kesl-control --set-settings 17 ExcludeIPs.item_#=<IP address>
   ```

3. 要扫描受信任 IP 地址列表，请运行以下命令：

   ```
   kesl-control --get-settings 17 TrustedIPAddresses
   ```

### 示例

```
kesl-control --set-settings 17 ExcludeIPs.item_0000="192.168.2.0/24"
```

# 如何选择受监控的网络端口

Kaspersky Endpoint Security 会监控通过特定协议传输并通过用户计算机上特定开放 TCP 端口的数据流。默认情况下，应用程序会监控已知和已注册的端口，例如，用于 HTTPS 连接的端口 443、用于 IMAP 邮件协议的端口 143。

*受信任的网络端口*是指被 网络威胁防护 组件从扫描中排除的网络端口。必须执行此操作，才能将 Kaspersky Endpoint Security 配置为与受信任的第三方服务和应用程序兼容，并优化性能。例如，您可以为内部备份服务指定网络端口，以便应用程序不会干扰备份副本的下载或上传。

请务必记住，将网络端口从扫描中排除会降低设备的受保护程度。请尽量减少排除。

### 如何在 Web Console 中将网络端口从扫描中排除

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **受信任区域 → 网络端口**。
   这将打开一个包含受监控网络端口列表的窗口。
5. 关闭要从扫描中排除的端口的切换开关。
   如果所需端口未列出，则表示应用程序不会扫描该端口。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

### 如何在命令行中将网络端口从扫描中排除

1. 运行以下命令获取受监控端口列表：

   ```
   kesl-control --get-net-setting
   ```

2. 如果已启用所有端口的监控（`MonitorNetworkPorts=All`），请运行以下命令：

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=Selected
   ```

   这会添加一个包含受监控网络端口的 `[NetworkPorts.item_#]` 节。

3. 如果该节包含您要从扫描中排除的端口，请执行以下步骤：

   a. 要将网络流量扫描设置输出到文件，请运行以下命令：

   ```
   kesl-control --get-net-setting --file <path to file>
   ```

   b. 在该文件中，删除包含您不想监控的网络端口的 `[NetworkPorts.item_#]` 节。

c. 要应用您的设置，请运行以下命令：

```
kesl-control --set-net-settings --file <path to file>
```

修改后的设置将导入到应用程序中。

# 如何将证书添加到受信任根证书列表

Kaspersky Endpoint Security 允许您在用户计算机上安装受信任的根证书，例如，如果您需要部署新的证书中心。该应用程序允许您将证书添加到特殊的 Kaspersky Endpoint Security 证书存储中。在这种情况下，证书仅被认为是 Kaspersky Endpoint Security 应用程序的受信任证书。换句话说，用户可以通过浏览器中的新证书访问网站。如果另一个应用程序试图访问该网站，您可能会因为证书问题而出现连接错误。

以下组件使用受信任根证书：

- Web 威胁防护
- 邮件威胁防护
- Web 控制

支持 CER、CRT、PEM 和 DER 格式的受信任证书。受信任证书的最大文件大小为 2 MB。

**如何在 Web Console 中安装受信任根证书**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **受信任区域 → 根证书**。
   这将打开一个包含受信任根证书列表的窗口。
5. 单击“**添加**”。
   这将打开用于添加证书的表单。
6. 上传证书。
7. 如有必要，请在 **注释** 字段中输入证书描述。
8. 保存更改。

在受信任证书列表中，序列号用作证书名称。

**如何在命令行中安装受信任根证书**

1. 要添加证书，请运行以下命令：

```
kesl-control --add-certificate <path to certificate>
```

2. 要查看受信任根证书列表，请运行以下命令：

```
kesl-control --list-certificates
```

将显示每个证书的以下信息：

- 证书主题
- 序列号
- 证书发布者
- 证书开始日期
- 证书到期日期
- SHA256 证书指纹

3. 要从列表中移除证书，请运行以下命令：

```
kesl-control --remove-certificate <certificate subject>
```

# 如何添加受信任域

Kaspersky Endpoint Security 包含一个受信任域列表，不会扫描这些域的加密连接。受信任域会影响 Web 威胁防护 和 Web 控制。将域排除在扫描范围之外，可避免阻止来自已知来源的流量。

指定域名。系统会忽略 `example.com/*` 或 `https://example.com` 等网址。

### 如何在 Web Console 中指定受信任域

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **受信任区域** → **受信任域**。
   这将打开一个包含受信任域列表的窗口。
5. 单击“**添加**”。
   这将打开用于添加域的表单。
6. 指定域名或域掩码。例如，`*example.com`。
7. 保存更改。

### 如何在命令行中指定受信任域

1. 要添加域，请运行以下命令：

   ```
   kesl-control --set-net-settings ManageExclusions=Yes Exclusions.item_#.DomainName=<domain name>
   ```

2. 要测试您的设置，请运行以下命令：

   ```
   kesl-control --get-net-settings
   ```

   受信任域应列在 `[Exclusions.item_#]` 部分中。

### 示例

```
kesl-control --set-net-settings Exclusions.item_0000.DomainName=example.com
```

# 如何排除挂载点

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。此类排除称为 *全局排除*。应用程序会将挂载在设备上的受信任本地或远程目录排除在扫描和文件操作拦截之外。例如，您可以排除包含临时文件的挂载点，以降低系统负载并使扫描更快完成。

挂载点排除会影响以下组件：

- 文件威胁防护
- 反加密
- 容器扫描

以下任务也会将受信任的挂载点排除在扫描范围之外：

- 恶意软件扫描
- 关键区域扫描
- 容器扫描
- 可移动驱动器扫描

> 必须以与 `mount` 命令输出中所显示的相同方式指定挂载点。

### 如何在 Web Console 中指定受信任的挂载点

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。
4. 选择 **受信任区域 → 挂载点**。
   这将打开一个包含受信任挂载点列表的窗口。
5. 单击“**添加**”。
   这将打开用于添加挂载点的表单。
6. 在文件系统下拉列表中，选择要排除的目录所在的文件系统类型：**本地**、**挂载**、**全部远程挂载**。
   Kaspersky Endpoint Security 支持用于远程目录的 Samba 和 NFS 协议。

   > 必须以与 `mount` 命令输出中所显示的相同方式指定挂载点。

7. 输入包含要排除的目录的文件系统名称。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中指定受信任的挂载点**

1. 如果目录不是挂载点，请运行以下命令将其创建为挂载点：

   ```
   mount --bind <path to dir> <path to dir>
   ```

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：

   ```
   <path to dir> <path to dir> none defaults,bind 0 0
   ```

3. 重新启动 Kaspersky Endpoint Security：

   ```
   systemctl restart kesl
   ```

4. 要添加受信任的挂载点，请运行以下命令：

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_#=<path to mount point>
   ```

5. 重启应用程序以应用全局排除项：

   ```
   systemctl restart kesl
   ```

**示例**

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/tmp"
```

# 如何添加受信任的应用程序

*受信任应用程序列表*是一个应用程序列表，对于该列表中的应用程序，Kaspersky Endpoint Security 不会监控其文件和进程活动（包括恶意活动）或进程内存。默认情况下，Kaspersky Endpoint Security 会监控由任何应用程序进程打开、执行或保存的对象，并控制所有应用程序的活动。

受信任应用程序会影响以下组件：

- 文件威胁防护
- 行为检测

以及进程内存扫描排除项。

**如何在 Web Console 中指定受信任应用程序**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **受信任区域 → 受信任应用程序**。
   这将打开包含受信任应用程序列表的窗口。
5. 如果要为公司内的所有计算机创建受信任应用程序的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的受信任应用程序列表。父策略中的应用程序在子策略中仅显示供查看，无法修改或删除。

   > 要合并这些列表，必须启用父策略设置的继承。

6. 单击“**添加**”。
   这将打开用于添加应用程序的表单。
7. 指定应用程序的路径或路径掩码。
8. 配置受信任应用程序设置：
   - “**不扫描此应用程序打开的文件**”。应用程序打开的所有文件被从 Kaspersky Endpoint Security 的扫描中排除。
   - “**不监控应用程序活动**”。Kaspersky Endpoint Security 不会监控操作系统中受信任应用程序的文件和网络活动。
     您还可以通过选中 **不监控 Managed Detection and Response 和 Endpoint Detection and Response** 复选框，分别为 MDR 和 EDR (KATA) 组件配置应用程序活动监控。

- "**不监控子程序活动**"。Kaspersky Endpoint Security 不会监控由受信任应用程序启动的应用程序的文件和网络活动。
- "**不扫描指定应用程序的内存**"。Kaspersky Endpoint Security 不会扫描由受信任应用程序生成的进程的内存。

> 在 Web Console 中，**注释** 设置不适用于 Kaspersky Endpoint Security for Linux。

9. 保存更改。

**如何在命令行中指定受信任应用程序**

1. 要将受信任应用程序的文件活动排除在扫描范围之外，请运行以下命令：

```
kesl-control --set-settings 1 ExcludedForProgram.item_#.UseExcludedForProgram=Yes
ExcludedForProgram.item_#.ProgramPath=<path to app> ExcludedForProgram.item_#.AreaDesc=<trusted app name>
[ExcludedForProgram.item_#.ApplyToDescendants=Yes]
```

2. 要将受信任应用程序的进程活动排除在扫描范围之外，请运行以下命令：

```
kesl-control --set-set 20 UseTrustedPrograms=Yes TrustedPrograms.item_#.UseTrustedProgram=Yes
TrustedPrograms.item_#.ProgramPath=<path to app> TrustedPrograms.item_#.ProgramDesc=<trusted app name>
[TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes] [TrustedPrograms.item_#.ApplyToDescendants=Yes]
```

3. 要将受信任应用程序的进程内存排除在扫描范围之外，请运行以下命令：

```
kesl-control --set-app-settings MemScanExcludedProgramPath.item_#=<path to app>
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `ExcludedForProgram.item_#.UseExcludedForProgram=Yes` | 将受信任应用程序的文件活动排除在文件威胁防护组件的扫描范围之外。 |
| `ExcludedForProgram.item_#.ProgramPath` | ID 为 `#` 的受信任应用程序的路径。文件威胁防护组件不会扫描指定应用程序的进程。<br>如果使用可更新内核模块进行系统事件拦截，则指定进程将被排除在所有命名空间的拦截之外。 |
| `ExcludedForProgram.item_#.AreaDesc` | ID 为 `#` 的受信任应用程序名称。 |
| `ExcludedForProgram.item_#.ApplyToDescendants=Yes` | 将受信任应用程序的子进程排除在文件威胁防护组件的扫描范围之外。 |
| `UseTrustedPrograms=Yes` | 将受信任应用程序进程的活动排除在行为检测组件的扫描范围之外。 |
| `TrustedPrograms.item_#.UseTrustedProgram=Yes` | 将 ID 为 `#` 的受信任应用程序的活动排除在扫描范围之外。 |
| `TrustedPrograms.item_#.ProgramPath` | ID 为 `#` 的受信任应用程序的路径。行为检测组件不会扫描指定应用程序的进程。<br>输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |
| `TrustedPrograms.item_#.ProgramDesc` | ID 为 `#` 的受信任应用程序名称。 |

| 设置 | 描述 |
| --- | --- |
| `TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes` | 将受信任应用程序的活动排除在 Managed Detection and Response 和 Endpoint Detection and Response Expert (on-premises) 组件的遥测数据收集范围之外。 |
| `TrustedPrograms.item_#.ApplyToDescendants=Yes` | 将受信任应用程序的子进程排除在行为检测组件的扫描范围之外。 |
| `MemScanExcludedProgramPath.item_#` | ID 为 `#` 的受信任应用程序的路径。应用程序不会检查受信任应用程序进程的内存。 |

# 如何添加受信任设备

*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

要使用受信任设备，您可以为单个用户、一组用户或组织的所有用户授予访问权限。例如，如果您的组织不允许使用可移动驱动器，但是管理员在工作中使用可移动驱动器，您可以仅允许一组管理员使用可移动驱动器。为此，请将可移动驱动器添加到受信任列表，并配置用户访问权限。

您可以根据以下数据添加受信任设备：

- “**ID**”。每个设备都有唯一标识符（Hardware ID，也称为 HWID）。您可以使用操作系统工具在设备属性中查看 ID。设备 ID 示例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。如果要添加多个特定设备，则按 ID 添加设备很方便。
- **按 ID 掩码**。如果您使用具有相似 ID 的多个设备，则可以使用掩码将设备添加到受信任列表中。`*` 字符可替换任意一组字符。`?` 字符可替换任意单个字符。例如，`WDC_C*`。

**如何在 Kaspersky Security Center Web Console 中添加受信任设备**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **设备控制** → **受信任设备**。

   这将打开包含受信任设备列表的窗口。
5. 单击“**添加**”。

   这将打开用于添加设备的表单。
6. 在 **用户或组** 下，指定将其视为受信任设备的用户或用户组。

   您可以在 Kaspersky Security Center 的账户列表中选择用户，或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   默认情况下，允许 Everyone 组访问受信任设备。
7. 在 **设备类型** 下，从下拉列表中选择设备类型（例如 **可移动驱动器**）。
8. 如果要基于 ID 掩码添加设备，请选中 **使用掩码** 复选框。
9. 在 **搜索受信任的设备** 字段中，输入设备 ID 或 ID 掩码。

   该表显示满足定义条件的设备列表。

10. 选中您想要添加到受信任列表中的设备名称旁边的复选框。
11. 如有必要，请在 **注释** 选项卡上描述将设备添加到受信任列表的原因。
12. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行添加受信任设备**

1. 要添加受信任设备，请运行以下命令：

```
kesl-control --trusted-devices --add <device ID>
```

2. 要扫描该组件的受信任设备列表，请运行以下命令：

```
kesl-control --trusted-devices --list
```

**示例**

```
kesl-control --trusted-devices --add WDC_C*
```

# 常规设置

# 检测设置

检测其他类型的对象

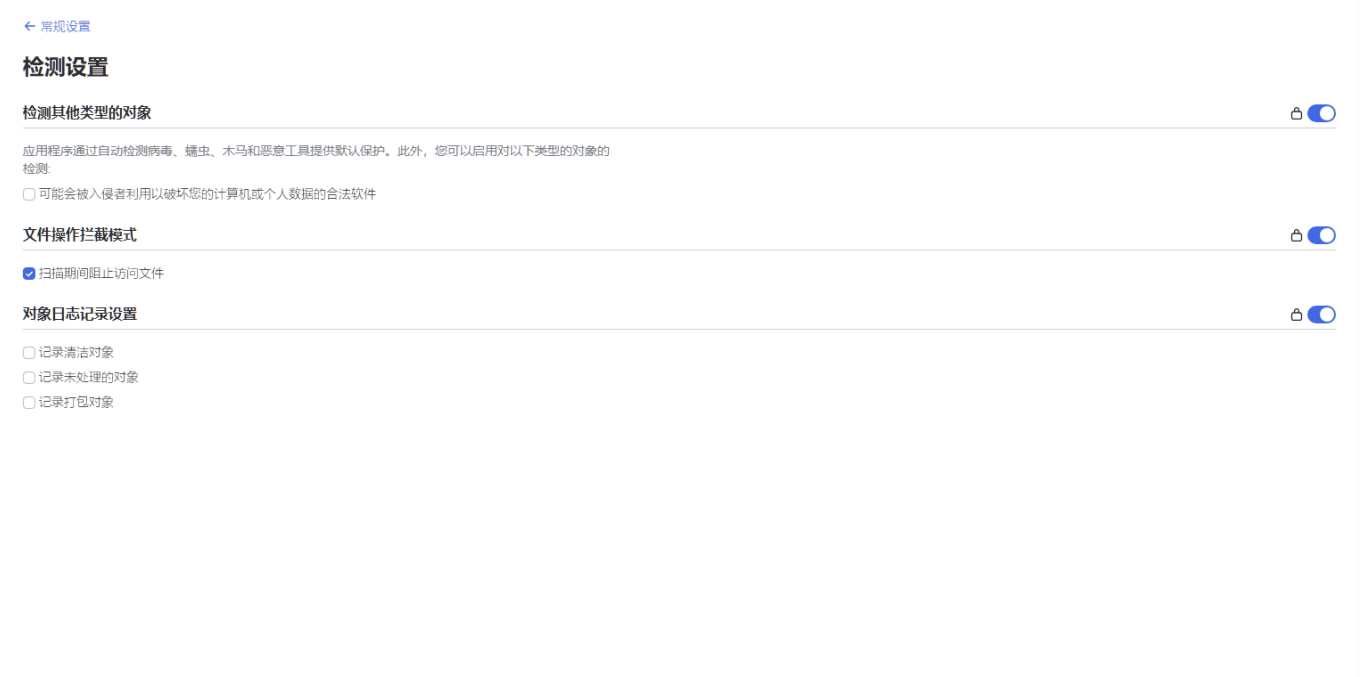
不管应用程序设置的配置如何，Kaspersky Endpoint Security 始终会检测并阻止病毒、蠕虫和木马。它们可能会给计算机带来巨大的损害。

您还可以启用对入侵者可以用来破坏计算机或用户数据的合法应用程序的检测。此类应用程序不一定具有恶意目的，但可能会被黑客利用。有关入侵者可以用来破坏计算机或用户数据的合法应用程序的详细信息，请访问 卡巴斯基百科全书网站。

**如何在 Web Console 中配置对入侵者可以用来破坏设备或数据的应用程序的检测**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**常规设置 → 检测设置**”。
5. 在“**检测其他类型的对象**”块中，选中“**可能会被入侵者利用以破坏您的计算机或个人数据的合法软件**”复选框。

6. 保存更改。




检测设置

### 如何在命令行中配置对入侵者可以用来破坏设备或数据的应用程序的检测

1. 要配置对攻击者可以用来破坏设备或数据的应用程序的检测，请对应用程序保护组件运行以下命令：

```
kesl-control --set-app-settings DetectOtherObjects=<Yes|No>
```

2. 要根据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数据库检查链接，请在 Web 威胁防护组件中运行以下命令：

```
kesl-control --set-settings 14 CheckOther=<Yes|No>
```

3. 要检查当前应用程序设置，请运行以下命令：

```
kesl-control --get-app-settings
```

4. 要检查当前的 Web 威胁防护设置，请运行以下命令：

```
kesl-control --get-settings 14
```

事件日志记录设置

默认情况下，Kaspersky Endpoint Security 不会记录处理打包对象和未感染对象的事件，也不会记录有关未由文件威胁防护组件处理的对象的事件。

您可以启用此类事件的日志记录，使应用程序生成 *检测到打包对象*、*对象未处理*、*对象已处理* 事件。此类事件在配置组件以及调试或排查应用程序故障时可能很有用。这可确保此类对象已由应用程序扫描，而不是因错误被跳过。

**如何在 Web Console 中启用对象处理事件日志记录**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**常规设置** → **检测设置**”。
5. 在 **对象日志记录设置** 下，选中相关事件类型旁边的复选框。
   - **记录清洁对象**
   - **记录未处理的对象**
   - **记录打包对象**
6. 保存更改。

**如何在命令行中启用有关处理对象的事件日志记录**

1. 要记录有关未感染对象的事件，请运行以下命令：

```
kesl-control --set-settings 1 ReportCleanObjects=Yes
```

2. 要记录有关未处理对象的事件，请运行以下命令：

```
kesl-control --set-settings 1 ReportUnprocessedObjects=Yes
```

3. 要记录有关已打包对象的事件，请运行以下命令：

```
kesl-control --set-settings 1 ReportPackedObjects=Yes
```

4. 要检查文件威胁防护设置的当前值，请运行以下命令：

```
kesl-control --get-settings 1
```

# 卡巴斯基安全网络

为了更有效地保护您的计算机，Kaspersky Endpoint Security 使用从全球用户处接收的数据。卡巴斯基安全网络设计用于收集此数据。

应用程序可能无法在美国境内使用 KSN 功能。

*卡巴斯基安全网络 (KSN)* 是一种云服务基础架构，提供对 Kaspersky 在线知识库（其中包含文件声誉、网页资源和软件的相关信息）的访问。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。如果您正在参与卡巴斯基安全网络，KSN 服务为 Kaspersky Endpoint Security 提供有关已扫描网址的信誉的信息，以及有关已扫描文件的类别和信誉的信息。有关 KSN 配置的详细信息，请参阅 Kaspersky Security Center 帮助。

卡巴斯基安全网络的使用是自愿的。应用程序将在初始配置期间提示您使用 KSN。用户可以随时开始或停止加入 KSN。

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。包含卡巴斯基安全网络声明文本的 ksn_license.<language ID> 文件包含在应用程序分发包中，并且位于 /opt/kaspersky/kesl/doc 目录中。

## 卡巴斯基信誉数据库的基础设施

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）*是大多数卡巴斯基应用程序使用的解决方案。KSN 参与者从卡巴斯基接收信息，并向卡巴斯基发送用户计算机上检测到的对象的信息，以便 卡巴斯基分析人员进行额外分析，并包括在卡巴斯基安全网络的信誉和统计数据库中。
- *卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。KPSN 专为因以下任一原因无法参与卡巴斯基安全网络的公司客户所设计：
  - 本地工作站未连接 Internet。
  - 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

要在使用新的授权许可激活应用程序后使用 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。

## 卡巴斯基私有安全网络的限制

卡巴斯基私有安全网络允许您使用自己的本地信誉数据库来检查对象（文件或网址）的信誉。添加到本地信誉数据库的对象的信誉比添加到 KSN/KPSN 的对象的信誉具有更高的优先级。例如，假设 Kaspersky Endpoint Security 正在扫描计算机并请求 KSN/KPSN 中文件的信誉。如果文件在本地信誉数据库中具有“*不信任*”的信誉，但在 KSN/KPSN 中具有“*受信任*”信誉，Kaspersky Endpoint Security 将检测到该文件为“*不信任*”，并将采取为检测到的威胁定义的操作。

但是，在某些情况下，Kaspersky Endpoint Security 可能不会请求 KSN/KPSN 中对象的信誉。如果是这种情况，Kaspersky Endpoint Security 将不会从 KPSN 的本地信誉数据库接收数据。Kaspersky Endpoint Security 可能不会请求 KSN/KPSN 中对象的信誉，原因如下：

- Kaspersky 应用程序正在使用离线信誉数据库。离线信誉数据库旨在优化 Kaspersky 应用程序运行期间的资源，并保护计算机上至关重要的对象。离线信誉数据库由 Kaspersky 专家根据卡巴斯基安全网络的数据创建。Kaspersky 应用程序使用特定应用程序的防病毒数据库更新脱机信誉数据库。如果脱机信誉数据库包含有关正在扫描的对象的信息，则应用程序不会从 KSN/KPSN 请求此对象的信誉。
- 扫描排除（受信任区域）在应用程序设置中配置。如果是这种情况，则应用程序不会考虑对象在本地信誉数据库中的信誉。
- 应用程序使用扫描优化技术，例如 iChecker 或缓存发送到 KSN / KPSN 的信誉请求。如果是这种情况，应用程序可能不会请求以前扫描的对象的信誉。
- 为了优化其工作负载，应用程序扫描特定格式和大小的文件。相关格式和尺寸限制列表由 Kaspersky 专家确定。该列表与应用程序的反病毒数据库一起更新。您还可以在应用程序界面中配置扫描优化设置，例如文件威胁保护组件。
- Light Agent 模式下的 Kaspersky Endpoint Security 通过 KSN 代理服务器与 KSN 服务器通信。不支持与 KSN 直接通信。

# 如何启用或禁用卡巴斯基安全网络

默认情况下，Kaspersky Endpoint Security 使用扩展 KSN 模式。*扩展 KSN 模式*是 Kaspersky Endpoint Security 用来向卡巴斯基发送附加数据的一种模式。

不会获取、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。

### 如何在 Web Console 中启用或禁用 KSN

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **卡巴斯基安全网络**。
5. 使用 **卡巴斯基安全网络 (KSN) 使用** 切换开关启用或禁用该组件。
6. 如果您启用了 KSN，**卡巴斯基安全网络声明** 窗口将打开。如果您同意，请阅读并接受卡巴斯基安全网络 (KSN) 声明使用条款。
7. 如有需要，请选中或清除 **使用扩展 KSN 模式** 复选框。

8. 保存更改。




卡巴斯基安全网络

## 如何在命令行中启用或禁用 KSN

1. 检查卡巴斯基安全网络的状态：

```
kesl-control --app-info
```

应用程序在 **卡巴斯基安全网络使用** 行中显示 KSN 状态：

- **已禁用**
- **基本 KSN 模式**
- “**扩展 KSN 模式**”。

2. 要启用卡巴斯基安全网络的标准模式，请运行以下命令：

```
kesl-control --set-app-settings UseKSN=Basic --accept-ksn
```

3. 要启用卡巴斯基安全网络的扩展模式，请运行以下命令：

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

4. 要禁用卡巴斯基安全网络，请运行以下命令：

```
kesl-control --set-app-settings UseKSN=No
```

**如何在应用程序界面中启用或禁用 KSN 使用**

1. 打开主应用程序窗口。
2. 在主应用程序窗口的下部，单击 **设置** 按钮。
3. 在打开的窗口中，选择以下选项之一：
   - **扩展 KSN 模式**，如果您想使用卡巴斯基安全网络、从知识库获取信息，并发送匿名统计信息以及有关威胁类型和来源的信息。
   - **基本 KSN 模式**，如果您想使用卡巴斯基安全网络、从知识库获取信息，但不发送匿名统计信息以及有关威胁类型和来源的信息。
4. 单击“**启用**”。
5. 在 **卡巴斯基安全网络使用** 窗口中，仔细阅读卡巴斯基安全网络声明，然后选择以下选项之一：
   - “**我确认我已完整阅读、理解并接受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**”。
6. 单击“**确定**”。

结果，如果启用 KSN，Kaspersky Endpoint Security 使用从卡巴斯基安全网络接收的文件、Web 资源的信誉信息。

Kaspersky Endpoint Security 使用以下网络设置与外部服务交互：

| 地址 | 协议 | 端口 |
|---|---|---|
| ds.kaspersky.com | HTTPS | 443 |
| ksn-a-stat-geo.kaspersky-labs.com | KSN | 443, 1443 |
| ksn-file-geo.kaspersky-labs.com | KSN | 443, 1443 |
| ksn-verdict-geo.kaspersky-labs.com | KSN | 443, 1443 |
| ksn-url-geo.kaspersky-labs.com | KSN | 443, 1443 |
| ksn-a-p2p-geo.kaspersky-labs.com | KSN | 443, 1443 |
| ksn-cinfo-geo.kaspersky-labs.com | KSN | 443, 1443 |

# 什么是应用程序的云模式

在 *云模式*下，Kaspersky Endpoint Security 使用轻量版反病毒数据库，这会使计算机 RAM 的负载大约减半。

只有启用卡巴斯基安全网络后，才能使用云模式。如果您未参与卡巴斯基安全网络或已禁用云模式，Kaspersky Endpoint Security 会从 Kaspersky 服务器下载完整版本的反病毒数据库。默认情况下已启用云模式。

如果应用程序正在 Light Agent 模式下运行，则云模式不可用。

**如何在 Web Console 中启用或禁用云模式**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **卡巴斯基安全网络**。
5. 使用**使用云模式**开关启用或禁用组件。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中启用或禁用云模式**

1. 运行命令以显示应用程序的常规设置，了解应用程序的当前状态：

   ```
   kesl-control --get-app-settings
   ```

   应用程序会在 `CloudMode` 行中显示其状态。
2. 要启用或禁用云模式，请运行以下命令：

   ```
   kesl-control --set-app-settings CloudMode=<Yes|No>
   ```

结果，Kaspersky Endpoint Security 在下一次更新中下载轻量版本或完整版本的反病毒数据库。

如果反病毒数据库的轻量级版本不可用，Kaspersky Endpoint Security 会自动切换到反病毒数据库的高级版本。

# KSN 代理的用途是什么

受 Kaspersky Security Center 管理服务器管理的用户计算机可以直接或通过“KSN Proxy”服务与 KSN 交互。

> 如果应用程序在 Light Agent 模式下运行，则不支持与 KSN 直接通信。Kaspersky Endpoint Security 通过 KSN 代理服务器与 KSN 服务器通信。

KSN Proxy服务提供以下功能：

- 用户计算机可查询 KSN 并将信息提交给 KSN，甚至无需访问互联网即可实现。
- KSN Proxy服务会缓存已处理的数据，从而降低外部网络通信信道的负载，并提高用户计算机所请求信息的接收速度。

默认情况下，在启用 KSN 并接受 KSN 声明后，应用程序使用代理服务器连接到卡巴斯基安全网络。应用程序使用的代理服务器是通过 TCP 端口 13111 的 Kaspersky Security Center 管理服务器。

您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。

无法使用命令行配置与 KSN 代理服务器的连接设置。

**如何在 Web Console 中通过代理服务器配置 KSN 连接**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **卡巴斯基安全网络**。
5. 使用“**使用管理服务器作为 KSN 代理服务器**”复选框启用或禁用 KSN 代理的使用。
6. 如有必要，选中或清除“**如果 KSN 代理服务器不可用则使用卡巴斯基安全网络服务器**”复选框。默认情况下已选定该选框。
   如果启用此选项，当 KSN 代理服务不可用时，Kaspersky Endpoint Security 将直接使用 KSN 服务器。KSN 服务器可以位于卡巴斯基侧，也可以位于第三方一侧（使用卡巴斯基私有安全网络）。
7. 保存更改。

# 配置数据传输到 Kaspersky Security Center 存储

在 Kaspersky Security Center 中，您可以启用或禁用将有关备份中的文件、隔离文件、未处理的文件和已连接设备的信息传输到 Kaspersky Security Center 存储。

**如何在客户端设备上查看已隔离文件**

卡巴斯基应用程序在客户端设备上隔离的文件总列表保存在 Kaspersky Security Center 中。

1. 在 Web Console 的主窗口中，选择 **操作** → **存储库**。
2. 转到 **隔离区** 文件夹。
3. 有关已隔离对象的信息显示在控制台的右侧窗格中。

**如何在客户端设备上查看备份区中的文件**

卡巴斯基应用程序在客户端设备上放入备份区的文件总列表保存在 Kaspersky Security Center 中。

1. 在 Web Console 的主窗口中，选择 **操作** → **存储库**。
2. 转到 **文件备份** 文件夹。
3. 有关放入备份区的对象的信息显示在控制台的右侧窗格中。

**如何查看活动威胁列表中未处理文件的相关信息**

1. 在 Web Console 的主窗口中，选择 **操作** → **存储库**。
2. 转到 **活动威胁** 文件夹。
3. 活动威胁列表中未处理文件的相关信息显示在控制台的右侧窗格中。

**如何查看连接到客户端设备的硬件的相关信息**

1. 在 Web Console 的主窗口中，选择 **操作** → **存储库**。
2. 转到 **硬件** 文件夹。
3. 有关设备的信息显示在控制台的右侧窗格中。

如果启用了设备控制，则会传输数据。

**如何查看客户端设备上的应用程序相关信息**

1. 在 Web Console 的主窗口中，选择 **操作** → **第三方应用程序**。
2. 转到 **应用程序注册表** 文件夹。
3. 有关应用程序的信息显示在控制台的右侧窗格中。

如果启用了应用程序控制，则会传输数据。

**如何配置与管理服务器的集成**

*要在策略属性中配置管理服务器集成：*

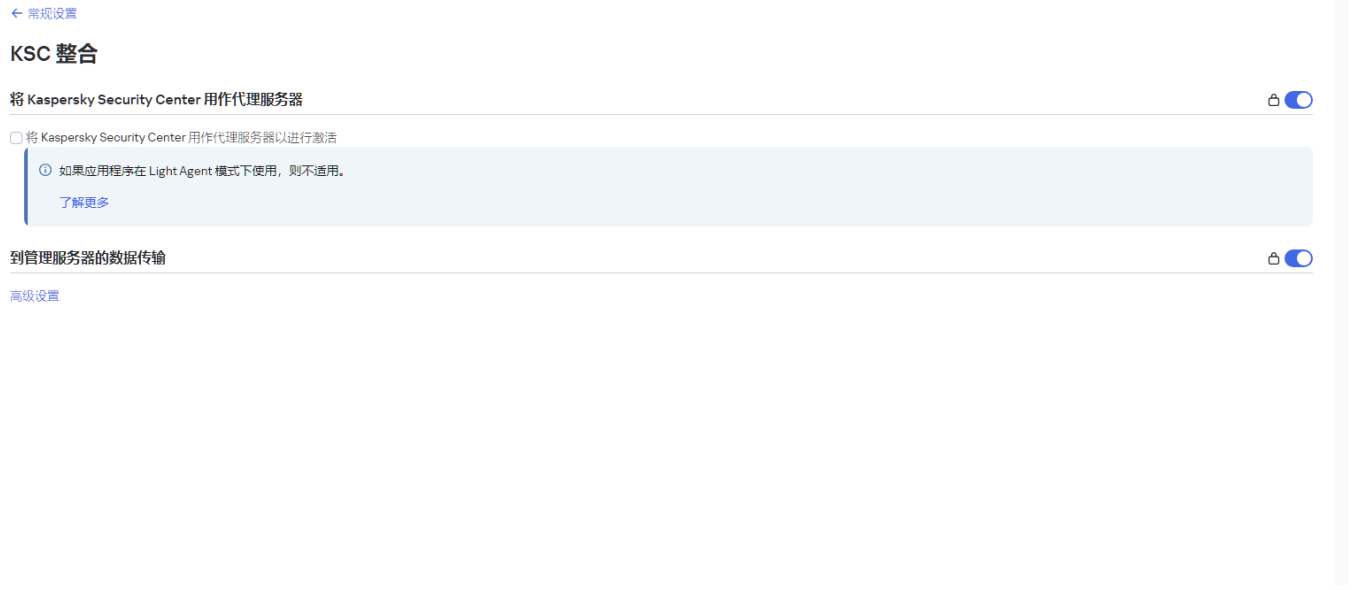
1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **KSC 整合**。
5. 单击 **附加设置** 链接。
6. 选择客户端计算机上必须将其信息发送到管理服务器的事件类别：
   - **关于隔离区中的文件** 此复选框可启用或禁用将隔离文件的相关数据传输到管理服务器。
   - **关于备份区中的文件**。此复选框可启用或禁用将备份中的文件数据传输到管理服务器。
   - **关于未处理的文件**。此复选框用于启用或禁用向管理服务器发送扫描期间未处理文件的相关通知。

- **关于已安装的设备**。此复选框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数据传输到管理服务器。
- **关于已启动的应用程序**。此复选框用于启用或禁用将清查任务在客户端设备上发现的应用程序列表发送到管理服务器。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

*要在受管理设备的属性中配置管理服务器集成：*

1. 在 Web Console 的主窗口中，选择 **资产管理** → **资产（设备）** → **受管理设备**。
2. 单击 **<设备名称>** 链接。
3. 选择 **应用程序** 选项卡，然后单击 **Kaspersky Endpoint Security** 链接。
4. 在 **应用程序设置** 选项卡上，转到 **存储设置** 部分。
5. 在 **向管理服务器传输数据的设置** 下，单击 **配置** 按钮。
6. 在 **数据传输设置** 窗口中，您可以启用或禁用向管理服务器发送信息：
   - **通知备份区中的文件**。此复选框可启用或禁用将备份中的文件数据传输到管理服务器。
   - **通知隔离区中的文件**。此复选框可启用或禁用将隔离文件的有关数据传输到管理服务器。
   - **通知未处理的文件**。此复选框用于启用或禁用向管理服务器发送扫描期间未处理文件的相关通知。
   - **通知已安装的设备**。此复选框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数据传输到管理服务器。
   - **通知设备上发现的应用程序**。此复选框用于启用或禁用将清查任务在客户端设备上发现的应用程序列表发送到管理服务器。
7. 保存更改。



# 如何配置应用程序启动

## 配置应用程序启动

您可以配置 Kaspersky Endpoint Security 的启动尝试失败的最大次数以及启动超时时间。如果应用程序长时间无法启动，这可以降低系统负载。默认情况下，连续启动应用程序失败的最大尝试次数为 5 次，最大超时时间为 3 分钟。

**如何在 Web Console 中配置应用程序启动**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **用户交互**。
5. 在“**应用程序启动设置**”下，在以下字段中输入值：
   - “**启动应用程序的最大连续不成功尝试次数**”。默认值：5。
   - “**等待应用程序启动的最长时间(分钟)**”。默认值：3。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行配置应用程序启动**

在命令行中，您可以使用`MaxRestartCount`中的`StartupTimeout`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。该设置可采用 1 至 60 之间的值。默认值：3。

## 应用关键更新

您可以将应用程序配置为在安装应用程序后的前 24 小时过后收到关键更新时自动重新启动。安装后的前 24 小时内，应用程序收到关键更新时会自动重新启动，无需额外配置。

**如何在 Web Console 中配置应用程序自动重新启动**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **用户交互**。
5. 在“**应用关键更新**”块中，选中“**收到关键更新时自动重新启动应用程序**”复选框。
   Kaspersky Endpoint Security 应用程序将在安装一天后收到关键更新时重新启动。
6. 保存更改。

**如何在命令行配置应用程序自动重新启动**

您可以使用常规应用程序设置中的 `UrgentUpdateRestartEnabled` 设置在命令行配置应用程序自动重新启动。

要在安装关键更新时自动重新启动应用程序，请运行以下命令：

```
kesl-control --set-app-settings UrgentUpdateRestartEnabled=Yes
```

# 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 中创建的本地任务。如果 Kaspersky Security Center 策略阻止用户查看、编辑、创建和删除本地任务，则有关 Scan_My_Computer、Critical_Areas_Scan、Container_Scan、Inventory_Scan、Update（在标准模式下）和 Rollback（在标准模式下）任务的信息不可用。
- 在客户端设备上查看和管理在 Kaspersky Security Center 中创建的任务。

*要在 Web Console 中配置任务管理权限：*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **用户交互**。

5. 在 **允许的操作** 下，选择允许用户在其设备上执行的操作：

- "**访问本地任务**"。如果选择此复选框，本地任务将显示在 Kaspersky Endpoint Security 的本地界面上。如果没有其他策略限制阻止此操作，用户可以在应用程序的图形界面或命令行中配置、运行、创建和删除可用的本地任务。
- "**管理组任务**"。如果选中此复选框，用户可以在客户端设备上管理在 Kaspersky Security Center 中配置的组任务。可以从应用程序的图形界面或命令行运行任务。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

# 密码保护

密码保护允许您根据授予的权限（例如，查看应用程序报告的权限）限制用户对 Kaspersky Endpoint Security 进行修改的访问权限。限制对应用程序设置的访问可降低未经授权或无意更改应用程序的风险。

## 密码保护的工作原理

1. **用户尝试执行由该组件控制的操作**

   例如，禁用保护组件或查看 Kaspersky Endpoint Security 报告。

2. Kaspersky Endpoint Security **检查用户权限**

   如果用户拥有相应的权限，则操作成功执行。如果用户没有相应的权限，应用程序将阻止该操作并显示错误。

   在 Kaspersky Endpoint Security 的图形界面中，无法查看或编辑禁止的操作。

## 配置密码保护

1. **启用密码保护**

   默认情况下，密码保护处于禁用状态。在 Web Console 或管理控制台中启用该组件，或者使用以下命令在命令行中启用该组件：

   ```
   kesl-control --set-permission-manager-settings Enabled=Yes
   ```

2. **配置用户权限**

   默认情况下，应用程序已为预定义用户组配置用户权限：*kesladmin*、*kesluser*、*keslaudit*。

   为这些组配置用户权限，或者创建新用户或用户组。

   > 为了使应用程序正常运行，我们建议至少为一个组配置权限。

### 如何在 Web Console 中配置自定义权限

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **自我保护**。
5. 确保该组件的切换开关处于 **密码保护已启用** 位置。
6. 单击**用户权限**链接。
   这将打开一个包含用户及其权限的窗口。
7. 如果要更改预定义组的权限，请单击组名称。
   如果要更改其他用户或组的权限：
   a. 单击“**添加**”。
   b. 从 Active Directory 中选择用户或组，或手动输入名称。
8. 选中要授予用户或组的权限旁边的复选框。
9. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




自我保护

### 如何在命令行配置自定义权限

1. 要查看当前密码保护设置列表，请运行以下命令：

```
kesl-control --get-permission-manager-settings
```

2. 要更改用户或组的权限，请运行以下命令：

```
kesl-control --set-permissions <principal> [--group] <permissions>=<Yes|No> [--file <file name>] [--
json]
```

3. 要删除已配置权限的用户或组，请运行以下命令：

```
kesl-control --remove-permissions <principal> [--group]
```

### 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `--group` | 该设置适用于组。如果未指定 `--group` 选项，则该设置适用于单个用户。 |
| `--file <file name>` | 将参数输出到文件或从文件导入参数。输入 `<file name>`。 |
| `--json` | 将参数输出到 JSON 文件或从 JSON 文件导入参数。<br>仅当指定 `--file <file name>` 选项时，才能指定此选项。 |
| `principal` | 用户或用户组名称。 |
| `permissions` | 自定义权限。指定 `Yes` 以允许用户执行操作，或指定 `No` 以拒绝。<br>• `StopProtection`。禁用保护组件。<br>• `StopSecurityControl`。禁用控制组件<br>• `StartProtection`。启用保护组件。<br>• `StartSecurityControl`。启用控制组件<br>• `ApplicationSettings`。配置应用程序<br>• `ViewReports`。查看报告<br>• `RestoreFromBackup`。从备份区恢复<br>• `RemoveLicenseKey`。删除密钥<br>• `AddLicense`。添加密钥<br>• `DisablePolicy`。禁用 Kaspersky Security Center 策略 |

**示例**

撤销 *kesluser* 组查看报告的权限：

```
kesl-control --set-permissions kesluser --group ViewReports=No
```

允许 *new-user* 管理控制组件：

```
kesl-control --set-permissions new-user startSecurityControl=Yes StopSecurityControl=Yes
```

密码保护的特殊注意事项

- 如果禁用了密码保护，则用户是否可以管理应用程序由 用户角色 决定。
- 如果用户的访问级别同时受组权限和个人权限控制，则个人权限优先于组权限。也就是说，即使用户的个人权限比该用户的组权限更严格，也以更严格的权限为准。

  例如，如果禁止 *kesluser* 组管理应用程序，您仍然可以允许该组的某个用户管理应用程序。即使组权限不允许，此类用户仍然可以管理应用程序。
- 如果启用了密码保护，并且用户既没有个人权限也没有组权限，则禁止所有操作。

# 关于自定义权限

如果启用了密码保护，则使用 *用户权限*控制对 Kaspersky Endpoint Security 管理功能的访问。用户权限定义用户的权限（请参见下表）。

自定义权限

| 权限 | 权限 |
| --- | --- |
| 配置应用程序 | 查看和编辑应用程序设置。<br>无需使用 `sudo` 命令，即可在应用程序的 图形界面和命令行中管理任务设置。<br>为用户分配角色。<br>撤销用户角色（管理员无权撤销自己的管理员角色）。<br>管理 *回滚* 任务。<br>管理组件：<br>• Managed Detection and Response<br>• Endpoint Detection and Response Optimum |
| 启用保护组件。 | 管理组件：<br>• 文件威胁防护<br>• 可移动驱动器扫描<br>• 行为检测<br>• 反加密<br>• BadUSB 攻击防护<br>• 邮件威胁防护<br>• Web 威胁防护<br>• 网络威胁防护<br>• 防火墙管理<br>• 系统完整性监控<br>• 对象的执行防护 (EDR Optimum)（*EDRO_Prevention*）<br>• Endpoint Detection and Response Expert (on-premises)<br>• Endpoint Detection and Response Expert (cloud)<br>• Network Detection and Response (KATA)<br>• Sandbox<br>• 与 KUMA 的整合 |
| 禁用保护组件 | |
| 启用控制组件 | 管理组件：<br>• 设备控制<br>• 应用程序控制<br>• Web 控制 |
| 禁用控制组件 | |
| 查看报告 | 查看任务报告<br>查看事件 |
| 从备份区恢复 | 查看和管理用户的存储。 |
| 删除密钥 | 管理应用程序授权许可。 |
| 添加密钥 | |
| 禁用 Kaspersky Security Center 策略 | 在设备上禁用或启用 Kaspersky Security Center 策略。 |

## 自定义权限相关的特殊注意事项

- 用户权限不会影响查看任务列表、查看备份区中的对象，以及查看应用程序的设置和状态。
  所有用户均可管理以下任务：
  - 扫描任务（*自定义扫描*、*容器扫描*、*自定义容器扫描*、*关键区域扫描*、*恶意软件扫描*）
  - *清查*

- *数据库和应用程序模块更新*
- *系统完整性检查*
- *IoC 搜索*

- 如果设备受 Kaspersky Security Center 策略控制，则无法在图形界面中添加或删除主授权许可密钥。拥有 *添加密钥* 和 *删除密钥* 权限的用户可以 添加备用密钥 或添加用于激活其他卡巴斯基解决方案（附加组件）的授权许可密钥。

  如果设备不受策略管理，用户可以删除或添加主授权许可密钥。

## 默认用户权限

默认情况下，应用程序已为预定义用户组配置用户权限：*kesladmin*、*kesluser*、*keslaudit*。对于不属于这些组的用户，禁止其对应用程序执行任何操作。

预定义组的用户权限

| 权限 | kesladmin | kesluser | keslaudit |
|---|---|---|---|
| 配置应用程序 | ✓ | – | – |
| 启用保护组件。 | ✓ | – | – |
| 禁用保护组件 | ✓ | – | – |
| 启用控制组件 | ✓ | – | – |
| 禁用控制组件 | ✓ | – | – |
| 查看报告 | ✓ | – | ✓ |
| 从备份区恢复 | ✓ | – | – |
| 删除密钥 | ✓ | – | – |
| 添加密钥 | ✓ | – | – |
| 禁用 Kaspersky Security Center 策略 | ✓ | – | – |

# 性能设置

使用 Kaspersky Endpoint Security 应用程序扫描计算机可能会占用大量系统资源。要优化系统负载，您可以：

- 使用电池供电时推迟或跳过计划任务
- 限制扫描任务的 CPU 使用量 (%)
- 限制应用程序的常驻内存使用量
- 将某些进程的内存从扫描中排除

使用电池供电时推迟或跳过计划任务

如果您的设备正在使用电池供电，并且您希望减少 Kaspersky Endpoint Security 的资源使用量，可以跳过计划任务：

- 所有扫描任务（自定义扫描、容器扫描、自定义容器扫描、关键区域扫描、*恶意软件扫描*）
- *Inventory*
- *数据库和应用程序模块更新*
- *应用程序完整性检查*
- *IOC 扫描*

您可以根据需要手动运行任务。

**如何使用 Web Console 在使用电池供电时取消计划任务**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **性能**。
5. 启用 **使用电池供电时推迟或跳过计划任务** 功能。
   Kaspersky Endpoint Security *取消*计划任务。
6. 保存更改。

**如何使用命令行在使用电池供电时取消计划任务**

您可以使用常规应用程序设置中的“PowerSaveMode”设置在命令行上配置取消计划任务。

要在设备使用电池供电时取消计划任务，请运行以下命令：

```
kesl-control --set-app-settings PowerSaveMode=Yes
```

限制扫描任务的 CPU 使用量 (%)

您可以限制*恶意软件扫描*、*关键区域扫描*、*清查*和*容器扫描*任务（属于 ODS、ContainerScan 和 InventoryScan 类型）的 CPU 使用率和内存使用量。默认情况下，内存使用限制设置为 8192 MB。未设置 CPU 使用率限制。

建议您将扫描任务的内存使用限制设置为低于驻留内存使用限制的值，以免扫描任务消耗所有可用 RAM 并导致应用程序重新启动。

请注意，所有 CPU 核心的总容量被视为 100%。

在`top`实用程序的输出中，100% 对应于单个核心的完全利用。因此，对于 10 核 CPU（ `top`实用程序报告为总共 1000%），400% 的值意味着整个 CPU（所有核心加在一起）的使用率为 40%。如果您希望在相同 10 个核心上， `top` 实用程序输出中的值永不超过 150%，请将 CPU 使用率限制设置为 `15%`。

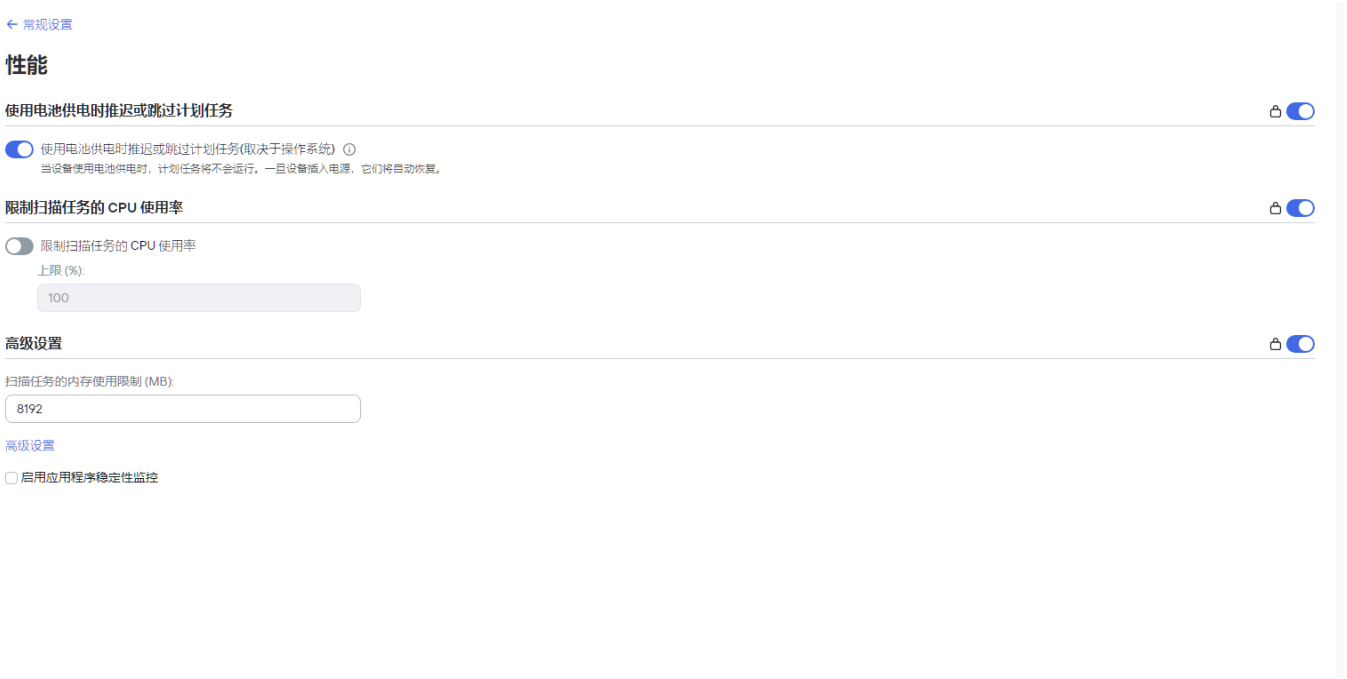
CPU 使用率限制适用于 *恶意软件扫描*、*关键区域扫描*、*清查* 和 *容器扫描* 任务，这意味着 CPU 使用率可能会超过配置的值。

限制 CPU 使用率在运行 CentOS 5.2 和 5.4 的设备上无法实现。

**如何在 Web Console 中限制内存和 CPU 资源使用量**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **性能**。
5. 启用 **限制扫描任务的 CPU 使用率** 功能。
6. 在 **上限 (%)** 字段中指定所有 CPU 核心的最大负载。该值必须是 10 到 100 之间的整数。
7. 在 **高级设置** 下，在相应字段中指定扫描任务的内存使用限制（MB）。默认值：8192。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




性能

### 如何使用命令行限制内存和 CPU 资源使用量

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，配置扫描任务的 CPU 资源使用限制。

1. 运行以下命令启用扫描任务的 CPU 使用率限制:

```
kesl-control --set-app-settings UseOnDemandCPULimit = Yes
```

2. 运行以下命令设置 CPU 使用率限制:

```
kesl-control --set-app-settings OnDemandCPULimit =<value>
```

限制值以百分比形式设置；可用值为 10 到 100 之间的整数。

3. 通过管理 kesl.ini 配置文件中的 `ScanMemoryLimit` 设置，指定扫描任务的内存使用限制。

## 限制应用程序的常驻内存使用量

您可以限制应用程序的常驻内存使用量。默认情况下，该限制设置为最多占用 50% 的内存，但不低于 2 GB 且不高于 16 GB。

### 如何在 Web Console 中限制驻留内存使用量

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **性能**。

5. 在 **高级设置** 下，单击 **高级设置** 链接，并在显示的窗口中选中 **限制应用程序内存使用** 复选框。
   在下拉列表中，您可以选择如何限制驻留内存的使用：

   - “**设置一个精确值 (%)**”。选择此项后，**精确值 (%)** 字段将变为可用，您可以在其中指定百分比值。默认值为 50%
   - “**设置一个精确值 (MB)**”。选择此项后，**精确值 (MB)** 字段将变为可用，您可以在其中指定以兆字节为单位的值。默认值为 2000 MB。
   - “**使用两个值中的最高值 (% 或 MB)**”。选择此项后，**精确值 (%)** 和 **精确值 (MB)** 字段将变为可用，您可以在其中指定所需的值。
   - “**使用两个值中的最低值 (% 或 MB)**”。选择此项后，**精确值 (%)** 和 **精确值 (MB)** 字段将变为可用，您可以在其中指定所需的值。
   - “**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）。

6. 保存更改。

要使更改生效，请在应用策略后重新启动受管理设备上的 Kaspersky Endpoint Security 应用程序。

**如何使用命令行限制驻留内存使用量**

无法在命令行中管理 `MaxMemory` 设置。使用 kesl.ini 配置文件配置驻留内存限制。

仅建议在技术支持专家的监督下并根据其说明更改默认值。

`MaxMemory` 参数可以采用以下值：

- `off` — 驻留集大小不受限制。
- `<value>%` – RAM 的 1% 到 100% 之间的值。
- `<value>MB` – 以兆字节为单位的值。
- `lowest/<value>%/<value>MB` – 百分比值和以兆字节为单位的绝对值中的较小值。
- `highest/<value>%/<value>MB` – 百分比值和以兆字节为单位的绝对值中的较大值。
- `auto`（默认）– 自动限制。

从扫描中排除进程内存

您可以将选定进程的内存从扫描中排除。

**如何在 Web Console 中将进程内存从扫描中排除**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **性能**。
5. 在“**高级设置**”区域，单击“**配置从扫描中排除进程内存**”链接。
6. 这将打开一个窗口；在该窗口中，单击 **添加** 按钮，并指定进程的可执行文件的路径。
   路径要求：
7. 必须以 `/` 开头（绝对路径）
   a. 不得包含禁用字符：
   - `\0`（空字节）：操作系统禁止使用。
   - 文件或目录名称中的斜杠（`/`）：用作分隔符。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中将进程内存从扫描中排除**

您可以通过`MemScanExcludedProgramPath.item_#`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该设置的值。

`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。

您可以指定多个要从扫描范围中排除的进程。

实用文章

**如何指定掩码**

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。

优化应用程序的资源消耗

# 网络设置

您可以配置用于连接互联网的代理服务器，选择网络端口监控模式，并设置加密连接扫描。

## 如何管理代理设置

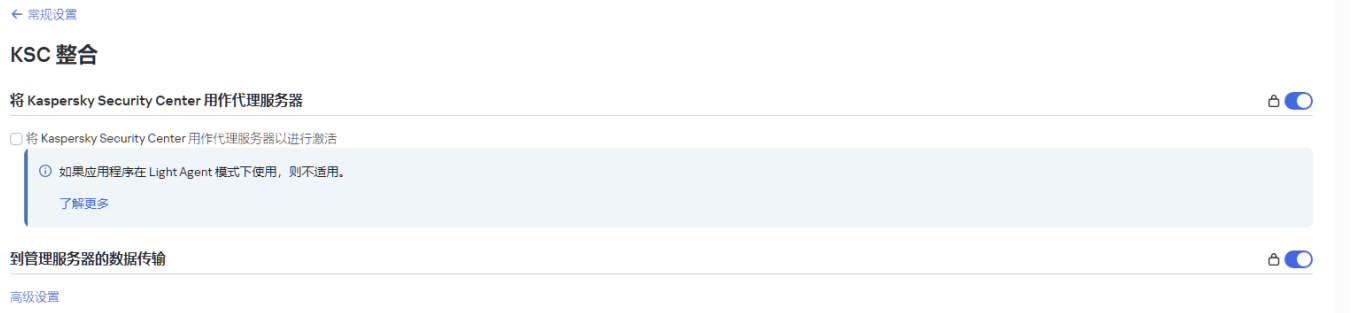
如果客户端设备的用户使用代理服务器连接到互联网，您可以配置代理服务器设置。Kaspersky Endpoint Security 应用程序可以使用代理服务器连接到卡巴斯基激活服务器、数据库和应用程序模块的更新源、卡巴斯基安全网络，并且在使用 Web 威胁防护组件验证网站证书时也会使用这些设置。

默认不适用代理服务器。

如果您在无法接入互联网的隔离网段中使用激活码来激活设备，则可以将 Kaspersky Security Center 管理服务器用作访问卡巴斯基激活服务器的代理服务器。

**如何在 Web Console 中配置使用 Kaspersky Security Center 作为代理服务器激活应用程序**

1. 在 Web Console 的主窗口中，选择“**资产管理** → **策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择“**应用程序设置**”选项卡。
4. 转到“**常规设置**” → “**KSC 集成**”部分。
5. 选中“**使用 Kaspersky Security Center 作为激活代理服务器**”复选框。
6. 单击“**保存**”按钮。

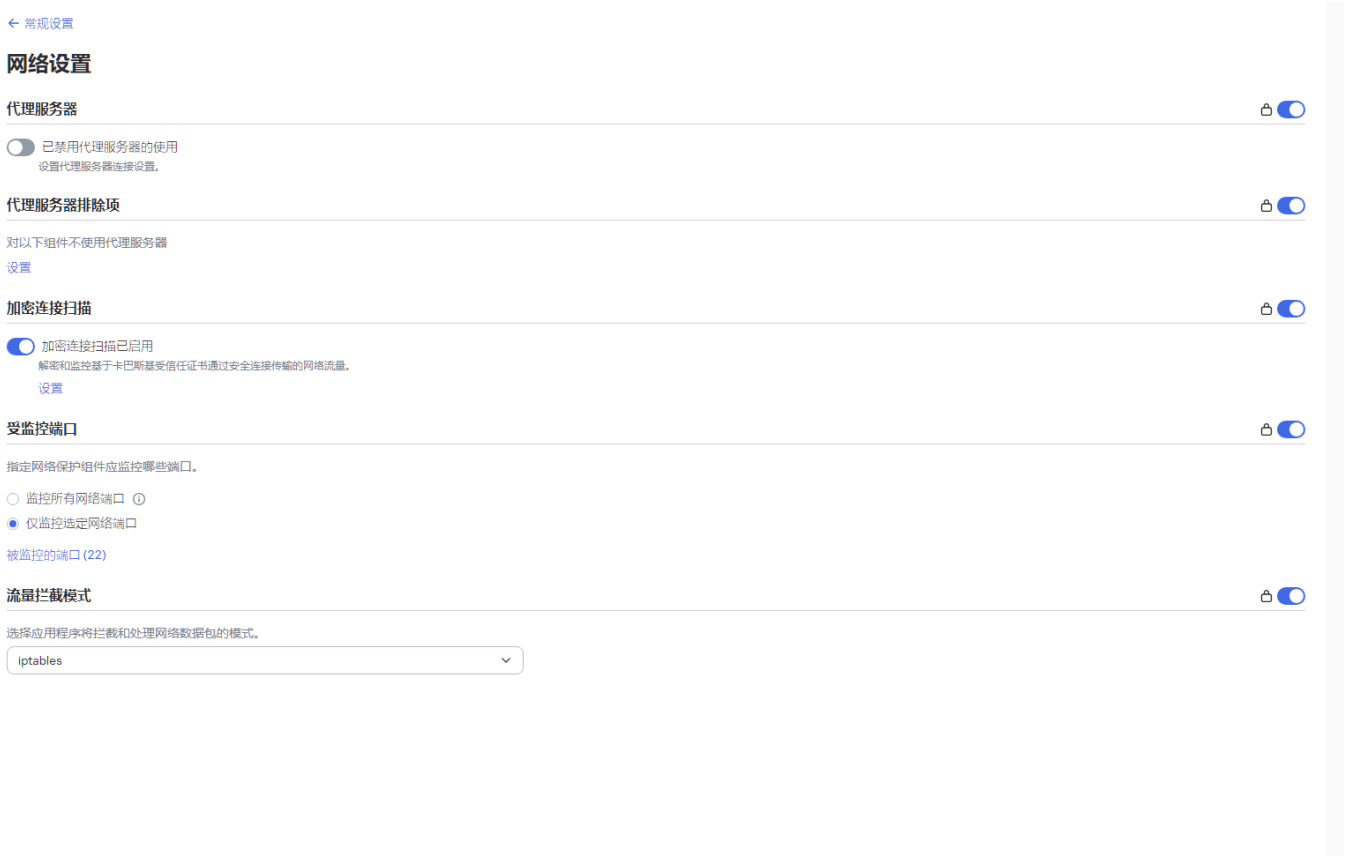


如果 Kaspersky Endpoint Security 以 Light Agent 模式使用，则不支持使用代理服务器连接卡巴斯基安全网络、SVM 和 Integration Server。此外，在 Light Agent 模式下不支持使用管理服务器作为访问卡巴斯基激活服务器的代理服务器。

**如何在 Web Console 中管理代理设置**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**常规设置 → 网络设置**”。
5. 将切换开关设置为 **已启用代理服务器的使用**。
6. 在显示的窗口中，填写以下字段：
   - “**代理服务器地址**”。
   - “**代理服务器端口**”。
7. 如有必要，启用代理服务器身份验证：
   a. 选择**使用代理服务器身份验证**复选框。
   b. 填写以下字段：
      - “**用户名**”。
      - “**密码**”。

8. 保存更改。




网络设置

## 如何在命令行管理代理设置

1. 要启用使用代理服务器，请运行以下命令：

```
kesl-control --set-net-settings UseProxy=Yes ProxyServer=<proxy server address>
```

2. 要检查网络设置的当前值，请运行以下命令：

```
kesl-control --get-net-settings
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| ProxyServer | 用于连接到互联网的代理服务器的地址。<br>代理服务器的地址采用以下格式之一：<br>• [<connection protocol>://]<address of the proxy server>:<port>，如果连接到代理服务器不需要身份验证；<br>• [<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>，如果连接到代理服务器时需要身份验证。指定 IPv6 地址时，请将其输入方括号中。<br>不支持通过 HTTPS 连接到代理服务器。<br>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。 |

代理服务器排除项

如果连接到某些地址时不需要使用代理服务器，可以将这些地址添加到排除中。

您还可以为提供与 Detection and Response 解决方案集成的 EDR Expert (on-premises)、NDR (KATA) 和沙盒组件禁用代理服务器。连接到这些组件的集成服务器时，将不会使用代理服务器。

**如何在 Web Console 中配置代理服务器排除**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**常规设置 → 网络设置**”。
5. 在“**代理服务器排除项**”区域，单击“**设置**”链接。
   这将打开代理服务器排除窗口
6. 选中不希望使用代理服务器的组件对应的复选框：
   - **Endpoint Detection and Response Expert (on-premises)**
   - “KATA Sandbox”。
   - “Network Detection and Response (KATA)”。
7. 添加不希望使用代理服务器的 IP 地址。例如：`1.2.3.4/24`、`1234::cdef/96`。
8. 保存更改。

**如何在命令行中配置代理服务器排除**

1. 要添加不希望使用代理服务器的地址，请运行以下命令：

```
kesl-control --set-net-settings ProxyBypass=<address:port>
```

2. 要为与卡巴斯基 Detection and Response 解决方案的集成绕过代理服务器，请运行以下命令：

```
kesl-control --set-net-settings [ProxyBypassEdr=<Yes|No>] [ProxyBypassNdr=<Yes|No>] [ProxyBypassSandbox=
<Yes|No>]
```

3. 要检查网络设置的当前值，请运行以下命令：

```
kesl-control --get-net-settings
```

符号

| 设置 | 描述 |
| --- | --- |
| ProxyBypass | 需绕过代理服务器的地址列表。<br>地址以 <address>[:<port>] 格式指定。要指定地址，您可以使用掩码（* 符号）以及 \ 符号后的注释。 |
| ProxyBypassEdr | 连接到 Kaspersky Endpoint Detection and Response Expert (on-premises) Integration Server 时是否使用代理服务器。默认不使用代理服务器（No）。 |
| ProxyBypassNdr | 连接到 Kaspersky Network Detection and Response (KATA) Integration Server 时是否使用代理服务器。默认不使用代理服务器（No）。 |
| ProxyBypassSandbox | 连接到提供与 Sandbox 交互的服务器时是否使用代理服务器。默认不使用代理服务器（No）。 |

# 应用程序如何拦截流量

应用程序可以采用以下两种网络流量拦截模式之一：eBPF 或 iptables。默认情况下会选择 iptables 模式。

此设置不适用于配备 Elbrus CPU 的设备。

## 关于 eBPF 网络流量拦截

在 eBPF 模式下，应用程序会创建自己的独立网络命名空间 (network linux namespace)，并使用与本地网络接口的 tc (linux traffic control) 队列关联的 eBPF 程序重定向网络数据包。重定向的网络流量随后会根据活动的网络任务得到分析，然后返回到原始网络接口。

命名空间之间的通信使用veth对虚拟化网络接口（每对接口的两端都位于各自的网络命名空间中）：

- kesl_in – kesl_worm_in 对传输入站连接的网络流量。
- kesl_out – kesl_worm_out 对传输出站连接的网络流量。

通过这些接口对，网络流量从默认命名空间发送到应用程序创建的命名空间进行扫描，并通过相同的接口在分析后返回。

只有当应用程序正在运行且启用网络拦截时，网络流量才能从系统中的其他网络接口到达这些接口。这些接口不能用于远程设备之间的网络数据传输。

## 关于 iptables 网络流量拦截

在 iptables 模式下，将使用 tproxy 内核机制执行拦截。

将在 mangle 表的 PREROUTING 链中创建相应的规则，以将流量转发到应用程序打开的特殊端口。应用程序还会向操作系统 Firewall 的各个表添加 额外规则，以将数据包转发到 tproxy。应用程序的网络拦截器位于客户端和服务器之间，并与二者分别建立单独的连接，然后扫描并传输二者之间的流量。

拦截到的入站和出站连接会使用不同的标签进行标记，您可以在 kesl.ini 配置文件中更改这些标签。

对于出站连接，会引入额外的路由规则，以将 拦截端口的出站流量重定向到 tproxy 中的回环接口。

选择流量拦截模式

**如何在 Web Console 中选择网络流量拦截模式**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **网络设置**。
5. 在 **流量拦截模式** 下，选择应用程序的流量拦截模式：
   - “**iptables**”。默认选中。应用程序使用 iptables 工具拦截流量。
   - “**eBPF**”。应用程序使用 eBPF 技术拦截流量。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中选择网络流量拦截模式**

1. 运行以下命令：

   ```
   kesl-control --set-net-settings NetInterceptorMode=<UseEBPF|UseIPTables>
   ```

2. 要检查网络设置的当前值，请运行以下命令：

   ```
   kesl-control --get-net-setting
   ```

特殊注意事项和限制

- 要更改流量拦截模式，您需要重启应用程序。重启会断开已连接的网络连接。
- 如果应用程序无法使用 eBPF 模式拦截网络流量，则会改用 iptables 模式。

# 如何配置证书验证策略

网络流量扫描设置由Web 威胁防护、网络威胁防护、邮件威胁防护和Web 控制使用。

默认情况下，Web 威胁防护会解密并扫描通过加密连接发送的网络流量。为此，应用程序会验证整个证书链。

证书验证策略包括以下设置：

- 验证方法（本地或通过互联网）
- 访问使用不受信任证书的网站
- 访问存在证书验证错误的网站

如果设备没有直接的互联网连接，您可以选择本地证书验证方法。

默认情况下，应用程序允许与具有不受信任证书的域建立网络连接。应用程序会显示一个 HTML 页面，其中包含警告以及有关不建议访问相关域的原因的信息（请参见下图）。用户可以单击 HTML 警告页面中的链接来获取对所请求 Web 资源的访问权限。

如果第三方应用程序或服务与具有不受信任证书的域建立连接，应用程序将创建自己的证书来扫描流量。新证书具有*不受信任*状态。这对于警告第三方应用程序不受信任的连接是必要的，因为在这种情况下无法显示 HTML 页面，并且连接可以在后台模式下建立。

证书验证可能会以错误结束。例如，在使用云存储或验证自签名证书时。默认情况下，应用程序会将此类网站的域名添加到排除列表中，并且在访问该域名时不会控制加密的网络流量。应用程序还会为加密连接扫描错误生成事件。

> 您只能在应用程序的本地界面中查看具有加密连接扫描错误的域列表。

**如何在 Web Console 中配置证书验证策略**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **网络设置**。
5. 在 **加密连接扫描** 下，确保切换开关处于 **加密连接扫描已启用** 位置。
   如果禁用此切换开关，Kaspersky Endpoint Security 将无法访问地址以 `https://` 开头的网站的内容。
6. 单击 **设置** 链接并配置证书验证策略：
   - “**访问带有不受信任证书的域**”。遇到不受信任的证书时的操作
     - “**允许连接**”。应用程序允许连接到具有不受信任证书的域。应用程序会显示一个 HTML 页面，其中包含警告以及有关不建议访问相关域的原因的信息（请参见下图）。用户可以单击 HTML 警告页面中的链接来获取对所请求 Web 资源的访问权限。
     - “**阻止连接**”。访问具有不受信任证书的域时，Kaspersky Endpoint Security 会阻止网络连接，并显示一个 HTML 页面，其中显示阻止该域的原因。

- “**访问带有加密连接扫描错误的域**”。加密连接扫描出错时的操作：
  - “**允许并添加域到排除项**”。当发生加密连接扫描错误时，应用程序会将导致该错误的域添加到排除列表，并且在访问此域时不监控加密网络流量。
  - “**阻止连接**”。发生加密连接扫描错误时，Kaspersky Endpoint Security 会阻止网络连接。
- “**证书验证策略**”。应用程序如何验证证书：
  - “**完整检查**”。应用程序使用互联网检查并下载验证证书所需的缺失链。
  - “**本地检查**”。应用程序会在计算机本地验证证书。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行配置证书验证策略**

1. 要启用加密连接扫描，请运行以下命令：

```
kesl-control --set-net-settings EncryptedConnectionsScan=Yes
```

2. 要选择证书验证方法，请运行以下命令：

```
kesl-control --set-net-settings CertificateVerificationPolicy=<FullCheck|LocalCheck>
```

3. 要选择在发现不受信任的证书时要执行的操作，请运行以下命令：

```
kesl-control --set-net-settings UntrustedCertificateAction=<Allow|Block>
```

4. 要选择在加密连接扫描期间发生错误时要执行的操作，请运行以下命令：

```
kesl-control --set-net-setting EncryptedConnectionsScanErrorAction=<AddToAutoExclusions|Disconnect>
```

5. 要检查网络设置的当前值，请运行以下命令：

```
kesl-control --get-net-setting
```

## 符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `EncryptedConnectionsScan` | 加密连接扫描模式：<br>`Yes`（默认）。加密连接扫描已启用。<br>`No`。加密连接扫描已禁用。 |
| `CertificateVerificationPolicy` | 证书验证策略：<br>`FullCheck`（默认）。应用程序使用互联网检查并下载验证证书所需的缺失链。<br>`LocalCheck`。应用程序会在计算机本地验证证书。 |

| 设置 | 描述 |
| --- | --- |
| `UntrustedCertificateAction` | 遇到不受信任的证书时的操作<br>`Allow`（默认）。应用程序允许连接到具有不受信任证书的域。应用程序会显示一个 HTML 页面，其中包含警告以及有关不建议访问相关域的原因的信息（请参见下图）。用户可以单击 HTML 警告页面中的链接来获取对所请求 Web 资源的访问权限。<br>`Block`。当访问具有不受信任证书的域时，Kaspersky Endpoint Security 会阻止网络连接。在浏览器中打开具有未受信任证书的域时，Kaspersky Endpoint Security 会显示一个 HTML 页面，其中显示阻止该域的原因。 |
| `EncryptedConnectionsScanErrorAction` | 加密连接扫描出错时的操作：<br>`AddToAutoExclusions`（默认）。当发生加密连接扫描错误时，应用程序会将导致该错误的域添加到排除列表，并且在访问此域时不监控加密网络流量。<br>`Disconnect`。发生加密连接扫描错误时，Kaspersky Endpoint Security 会阻止网络连接。 |

# 如何配置受监控的端口

Kaspersky Endpoint Security 运行时，网络威胁防护组件会监控通过某些网络端口传输的数据。应用程序监控的网络端口列表根据卡巴斯基专家的建议进行配置。

行为检测和漏洞利用防御组件还会监控可能威胁计算机安全的应用程序进程的网络端口。应用程序通过反病毒数据库获取有关此类进程的信息。

您可以配置希望应用程序监控的端口：

- “**监控所有网络端口**”。在此网络端口监控模式下，应用程序会监控通过计算机任何开放网络端口的数据流。

  > 指定此值可能会大大增加操作系统负载。

- “**仅监控选定网络端口**”。在该网络端口监控模式中，保护组件监控应用程序的所选端口和所选应用程序的网络活动。

> 如果要拦截与 NFS 服务器的网络连接，则需要确保 NFS 服务器以 `insecure` 选项启动（以便接受来自 1–1024 范围之外的端口的连接），否则 NFS 服务器可能会拒绝此类连接。

### 如何在 Web Console 中配置受监控端口

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**常规设置 → 网络设置**”。
5. 在 **受监控端口** 下，选择应用程序端口监控模式：
   - “**监控所有网络端口**”。
   - **仅监控选定网络端口**（默认值）。

6. 如果您选择了 **仅监控选定网络端口** 选项，请配置要监控的端口列表：

   a. 单击**被监控的端口**链接。

   b. 编辑受监控端口列表。

   要使邮件威胁防护组件正常工作，必须在网络设置中监控网络端口 25、110、143、465、587、993 和 995。这些网络端口默认已添加到监控端口列表中。从列表中移除这些端口可能会导致组件无法正常工作。

7. 保存更改。

**如何在命令行配置受监控端口**

1. 要选择端口监控模式，请运行以下命令：

```
kesl-control --set-net-settings MonitorNetworkPorts=<All|Selected>
```

2. 如果您选择仅监控选定端口 (`MonitorNetworkPorts=Selected`)，请指定要监控的端口列表：

```
kesl-control --set-net-settings NetworkPorts.item_#.PortName=<port name> NetworkPorts.item_#.Port=<port number>
```

   要从监控列表中移除端口，请使用 配置文件编辑该列表。

3. 要检查网络设置的当前值，请运行以下命令：

```
kesl-control --get-net-settings
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `MonitorNetworkPorts` | `Selected`（默认值）– 仅监视在 `[NetworkPorts.item_#]` 部分中指定的网络端口（见下文）。<br>`All` – 监控所有网络端口。<br>指定此值可能会大大增加操作系统负载。 |
| `PortName` | 网络端口描述。 |
| `Port` | 应用程序要监控的网络端口号。可能的值：`1 – 65535`。<br>要使邮件威胁防护组件正常工作，必须在网络设置中监控网络端口 25、110、143、465、587、993 和 995。这些网络端口默认已添加到监控端口列表中。从列表中移除这些端口可能会导致组件无法正常工作。 |

# 使用操作系统工具排除流量拦截

在 Kaspersky Endpoint Security 设置中，您可以按流量方向、目标 IP地址和端口来配置流量拦截排除项。如果此类排除项不足以解决 Kaspersky Endpoint Security 应用程序与客户端应用程序之间的冲突，您可以使用特殊的允许规则链 kesl_bypass。

kesl_bypass 链是 Kaspersky Endpoint Security 在操作系统防火墙的 mangle 表（iptables/ip6tables）中创建的特殊规则列表。kesl_bypass 链的规则允许从 Kaspersky Endpoint Security 的拦截中排除流量。kesl_bypass 链被添加到网络包处理进程的顶部，这意味着 kesl_bypass 规则会在所有其他 iptables 规则之前得到处理。

与 Kaspersky Endpoint Security 设置中可连接的排除项不同，kesl_bypass 链不仅允许按流量方向、目标 IP 地址和端口配置排除项，还允许按其他连接参数配置排除项。

kesl_bypass 链中的规则可以通过操作系统进行更改。

例如，您可以通过运行以下命令向 kesl_bypass 链添加规则：

```
iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT
```

此规则允许将任何 IP 地址上端口 80 的入站和出站 HTTP 流量排除在 Kaspersky Endpoint Security 的拦截之外。这有助于避免与您信任的 Web 服务发生潜在冲突。

如果在链中配置了流量排除规则，这些规则会影响Web 威胁防护、网络威胁防护和Web 控制组件。

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。

# 文件操作拦截

文件操作拦截模式会影响文件威胁防护和设备控制组件、对象的执行防护操作以及可移动驱动器扫描任务。

**如果启用了文件操作拦截的阻止模式**

- 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。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。检测到感染对象时，应用程序会执行文件威胁防护组件的 **针对威胁检测的操作** (`ActionOnThreat`) 设置中指定的操作。
- 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。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。
- 当“对象的执行阻止”操作确定是否可以执行设备上的文件时，应用程序可能会阻止这些文件。如果扫描结果显示“对象的执行阻止”操作允许这些文件运行，应用程序将允许其运行。
- 扫描期间，应用程序可能会阻止访问可移动驱动器上的文件。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。检测到感染对象时，应用程序会执行文件威胁防护组件的 **针对威胁检测的操作** (`ActionOnThreat`) 设置中指定的操作。

**如果禁用了文件操作拦截的阻止模式**

- 无论选择何种运行模式，文件威胁防护组件均以通知模式运行，允许访问文件并异步执行扫描。
- 无论选择何种运行模式，设备控制组件均以通知模式运行，并始终允许访问设备。

- 无论选择何种运行模式，“对象的执行阻止”操作均以通知模式运行，并始终允许执行对象。
- 应用程序始终允许访问可移动驱动器上的文件，并以异步方式执行扫描。

这种文件操作拦截模式在扫描时对系统性能的影响较小，但存在文件中的威胁可能无法清除或删除的风险。如果在扫描期间，与此文件关联的进程在应用程序能够判定此文件的状态之前成功重命名了此文件，则可能会发生这种情况。

默认情况下，文件操作拦截阻止模式已启用。

**如何在 Web Console 中配置文件操作拦截模式**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**常规设置** → **检测设置**”。
5. 在 **文件操作拦截模式** 下，取消选中或选中 **扫描期间阻止访问文件** 复选框。默认情况下已选定该选框。
6. 保存更改。

**如何在命令行中配置文件操作拦截模式**

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。

要选择文件操作拦截模式，请运行以下命令：

```
kesl-control --set-app-settings FileBlockDuringScan=<Yes|No>
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `FileBlockDuringScan` | `Yes`（默认值），用于在 文件威胁防护 和 设备控制 组件、执行防护操作以及 可移动驱动器扫描 任务扫描文件期间阻止访问文件。<br>`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。 |

# 配置系统事件拦截

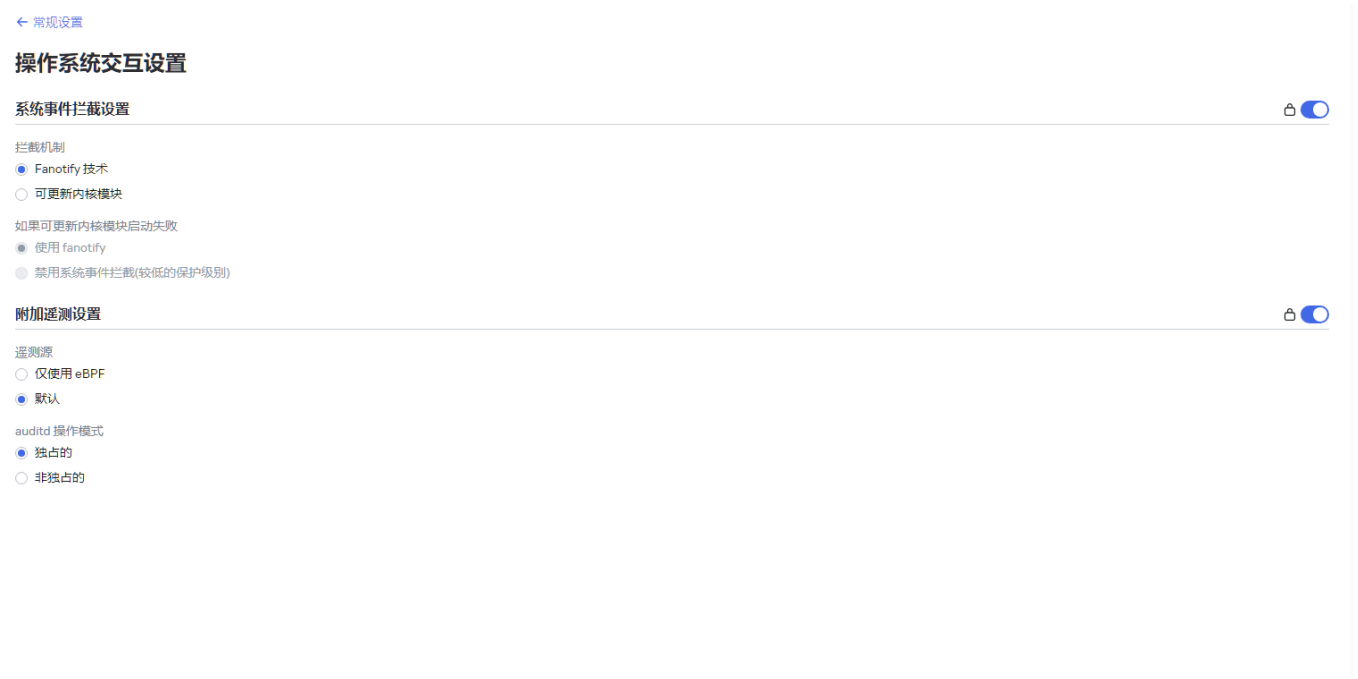
您可以在 Web Console 中、命令行中或 管理控制台 中选择系统事件拦截机制。

只有在操作系统支持 fanotify 技术的设备上，才能管理系统事件拦截设置。

对于配备 Elbrus CPU 的设备，无法配置系统事件拦截。

### 如何在 Web Console 中配置系统事件拦截机制

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到 **常规设置** → **操作系统交互设置**。
5. 在 **系统事件拦截设置** 下，选择一种系统事件拦截机制：
   - “**Fanotify 技术**”。
   - “**可更新内核模块**”。如果选中此选项，请选择当可更新内核模块无法启动时应用程序将执行的操作：
     - “**使用 fanotify**”。
     - “**禁用系统事件拦截(较低的保护级别)**”。




操作系统交互设置

### 如何在命令行中配置系统事件拦截机制

1. 要选择系统事件拦截机制，请运行以下命令：

```
kesl-control --set-app-settings InterceptorMode=<UseFanotify|UseUpdatableKernelModule>
```

2. 要指定可更新内核模块启动失败时应用程序执行的操作，请运行以下命令：

```
kesl-control --set-app-settings InterceptorFallbackStrategy=<FallbackToFanotify|FallbackToLimitedMode>
```

3. 如果可更新内核模块启动失败，要使应用程序重新启动，请运行以下命令：

```
kesl-control --set-app-settings InterceptorApplyStrategy=<RestartServiceAutomatically|RestartServiceManually>
```

4. 要检查当前应用程序设置，请运行以下命令：

```
kesl-control --get-app-settings [--json]
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `InterceptorMode` | `UseFanotify`（默认）— 使用 fanotify 技术来拦截系统事件。<br>`UseUpdatableKernelModule` — 用于通过可更新内核模块来拦截系统事件。 |
| `InterceptorFallbackStrategy` | `FallbackToFanotify`（默认）— 切换到 fanotify 进行系统事件拦截。<br>`FallbackToLimitedMode` — 不使用系统事件拦截。如果应用程序不使用系统事件拦截，则不会执行文件实时扫描，从而降低设备的保护级别。 |
| `InterceptorApplyStrategy` | `RestartServiceAutomatically` 自动重启应用程序以启动可更新内核模块。建议使用此设置。<br>`RestartServiceManually`（默认）在用户手动重启应用程序后启动可更新内核模块。 |

如果操作系统满足安装可更新内核模块的要求，则应用程序可以使用基于可更新内核模块的拦截机制。

如果选择了基于可更新的内核模块的拦截机制，则可以配置在可更新的内核模块启动而模块没有启动时发生错误的应用程序的行为。在此情况下，应用程序可以回退到 fanotify 或禁用系统事件拦截。

如果在安装应用程序期间无法安装可更新内核模块，则可以在您的操作系统获得支持后再进行安装。为此，请执行下列操作：

1. 更新应用程序数据库和模块。可更新内核模块会作为常规更新过程的一部分进行安装。
2. 根据可更新内核模块选择拦截机制。

应用程序可以在以下情况下切换到使用可更新的内核模块：

- 在应用程序设置中，您已将拦截系统事件的机制更改为可更新的内核模块。
- 在未启动可更新的内核模块的设备上，数据库和模块更新引入了支持可更新内核模块的更新。

关于可更新内核模块状态的信息

关于可更新内核模块的状态和可用性的信息以状态形式显示：

- “**正在运行**”表示模块已安装并且正在运行。
- “**已停止**”表示模块已安装但未运行。

- “**不可用**”表示设备不支持此模块。
- “**故障**”表示启动模块时发生错误，模块未运行。

您可以在 Web Console 和命令行中查看设备上可更新内核模块的状态。

**如何在 Web Console 中查看可更新内核模块的状态**

1. 在 Web Console 的主窗口中，选择“**资产管理**”→“**资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
   列表仅显示所选管理组的受管理设备。
3. 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. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。
6. 查看“**可更新内核模块**”功能组件的状态。

**如何在命令行中查看可更新内核模块的状态**

*要查看可更新内核模块的状态，请运行以下命令：*

```
kesl-control --app-info [--json]
```

其中 `--json` 表示以 JSON 格式输出数据。如果不指定 `--json` 选项，设置将输出到控制台。

## 当使用可更新内核模块时的“安全”模式

如果使用可更新内核模块时应用程序不稳定，则在达到指定的最大异常停止次数后，应用程序会自动切换到“安全”模式（在kesl.ini 配置文件中设置 `SafeMode=yes`）。默认情况下，应用程序在三次异常停止后进入“安全”模式。异常停止的最大次数在 kesl.ini 配置文件中的 `PanicThreshold` 设置中进行配置。

如果应用程序在“安全”模式下运行，可更新内核模块不会启动，应用程序将切换到 fanotify 来拦截系统事件。应用程序会将 `UpdatableKernelModule=Error` 标签发送到 Kaspersky Security Center。

要在解决应用程序问题后继续使用可更新内核模块，您需要禁用“安全”模式。

**如何在命令行中禁用应用程序的安全模式**

1. 打开 /var/opt/kaspersky/kesl/common/kesl.ini 文件进行编辑。
2. 在 `[General]` 部分中，设置 `SafeMode=no` 。
3. 重新启动 Kaspersky Endpoint Security：

   ```
   systemctl restart kesl
   ```

安全模式已禁用。

# 管理附加遥测设置

您可以管理以下高级设置，用于在与以下内容集成时收集发送到 Detection and Response 解决方案的遥测数据：

- 遥测来源。您可以使用 eBPF 技术和 auditd 服务获取遥测数据，也可以单独使用 eBPF 技术。
- auditd 服务的模式。Kaspersky Endpoint Security 可以在独占模式或组播模式下使用 auditd 服务。

**如何在 Web Console 中配置其他遥测设置**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **操作系统交互设置**。
5. 在**遥测设置**下，指定 Kaspersky Endpoint Security 用于收集遥测数据的来源：
   - **仅使用 eBPF** 表示仅使用 eBPF 技术获取遥测数据。

     如果选择了 **仅使用 eBPF** 选项，则检测和响应解决方案的遥测功能可能会受到限制。

   - **默认**表示使用 eBPF 技术和 auditd 服务获取遥测数据。
6. 还要指定 auditd 服务的模式：
   - **独占**表示 Kaspersky Endpoint Security 以独占模式使用 auditd 服务。
   - **非独占**表示 auditd 服务以非独占模式使用。

     仅当 **遥测来源** 设置为 **默认** 时，才会应用此设置。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行配置其他遥测设置**

在命令行中，您可以使用 Behavior_Detection 预定义任务的 `TelemetrySource` 和 `UseTelemetryMonopolyMode` 设置来管理其他遥测设置。

1. 要启用遥测来源，请运行以下命令：

```
kesl-control --set-settings 20 TelemetrySource=<Default|OnlyEBPF>
```

2. 要为 auditd 服务选择模式，请运行以下命令：

```
kesl-control --set-settings 20 UseTelemetryMonopolyMode=<True|False>
```

符号

命令选项

| 设置 | 描述 |
| --- | --- |
| `TelemetrySource` | `Default`（默认）表示使用 eBPF 技术和 auditd 服务来获取遥测数据。<br>`OnlyEBPF` 表示仅使用 eBPF 技术获取遥测数据。 |
| `UseTelemetryMonopolyMode` | `True`（默认值）表示 Kaspersky Endpoint Security 以独占模式使用 auditd 服务。<br>`False` 表示 auditd 服务以非独占模式使用。<br>仅当 `UseTelemetryMonopolyMode` 被设置为 `TelemetrySource` 时，`Default` 设置才应用。 |

# 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。

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，可以尝试从备份副本恢复文件。

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。

## 配置备份设置

您可以在 Web Console、管理控制台中或使用命令行管理设备上的备份区设置。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 30 天。最长存储期限到期后，Kaspersky Endpoint Security 将删除备份区中最旧的文件。
- **最大备份容量。**默认情况下，配置以下备份区最大大小：
  - 如果未应用策略，则为 0 MB
  - 如果应用了策略，则为 1024 MB

为避免超过最大存储大小，当达到最大存储大小时，Kaspersky Endpoint Security 将自动删除存储中的最早文件。

- **存储备份区和隔离区对象的目录路径**（只能在命令行中配置）。默认情况下，/var/opt/kaspersky/kesl/common/objects-backup/ 目录用于存储文件的备份副本和隔离的文件。

**如何在 Web Console 中配置备份区设置**

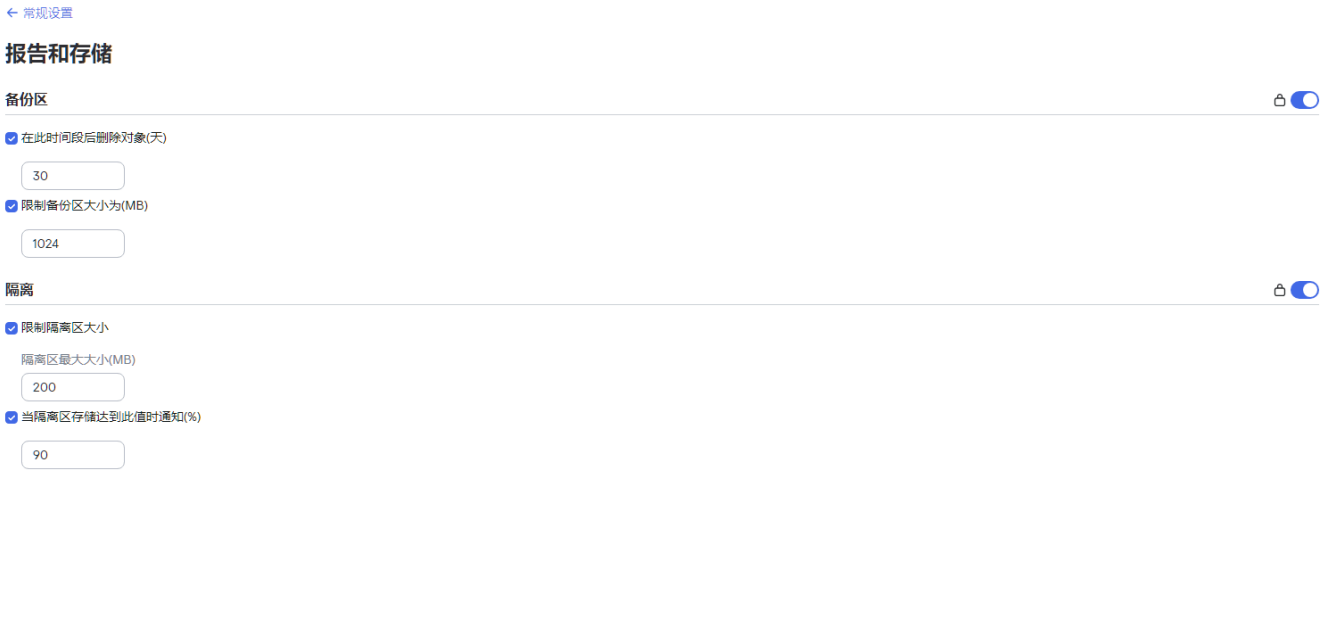
*要在策略属性中管理备份区设置：*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到 **常规设置** → **报告和存储** 部分。
5. 在 **备份区** 部分中，配置以下设置：
   - “**在此时间段后删除对象(天)**”。如果选中该复选框，则最大文件存储期限制为定义的时间间隔。默认情况下已选定该选框。
     有效值为 0 到 10000。
   - “**限制备份区大小为(MB)**”。如果选中该复选框，则最大存储大小限制为定义值。默认情况下已选定该选框。
     有效值为 1 到 4000。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

*要在受管理设备的属性中管理备份区设置：*

1. 在 Web Console 的主窗口中，选择 **资产管理** → **资产（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。要选择嵌套组，请单击窗口上方的 **显示层次结构** 按钮。
   列表仅显示所选管理组的受管理设备。
3. 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. 选择 Kaspersky Endpoint Security
6. 转到 **应用程序设置** → **存储设置**。
   - “**在此时间段后删除对象(天)**”。如果选中该复选框，则最大文件存储期限制为定义的时间间隔。默认情况下已选定该选框。
     有效值为 1 到 10000。
   - “**限制备份区大小为(MB)**”。如果选中该复选框，则最大存储大小限制为定义值。默认情况下已选定该选框。
     有效值为 1 到 4000。

7. 保存更改。




报告和存储

## 如何在命令行中配置备份区

在命令行中，您可以使用常规应用程序设置中的 `BackupDaysToLive`,、 `BackupSizeLimit` 和 `QuarantineBackupFolder` 设置来配置备份设置。

1. 要配置备份区中对象的保留期限，请运行以下命令：

```
kesl-control --set-app-settings BackupDaysToLive=<days>
```

2. 要配置备份区的最大大小，请运行以下命令：

```
kesl-control --set-app-settings BackupSizeLimit=<Backup size>
```

3. 要配置存储备份区和隔离区对象的目录，请运行以下命令：

```
kesl-control --set-app-settings QuarantineBackupFolder=<path to folder>
```

4. 要检查当前应用程序设置，请运行以下命令：

```
kesl-control --get-app-settings
```

命令选项

| 设置 | 描述 |
| --- | --- |
| `BackupDaysToLive` | 在备份存储中存储对象的时间段（天数）。指定时间过去后，应用程序将删除文件的最旧备份副本。<br>要删除对象保留限制，请设置 0。 |
| `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备份副本。<br>要移除备份容量限制，请设置 0。 |

| 设置 | 描述 |
| --- | --- |
| `QuarantineBackupFolder` | 存储备份和隔离对象的目录的路径。您可以指定一个与默认目录不同的目录。您可以使用任何设备上的目录作为存储备份和隔离对象的目录。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。<br>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。<br>默认值：`/var/opt/kaspersky/kesl/common/objects-backup/`<br>访问默认目录需要 root 特权。 |

查看备份对象

客户端设备上由卡巴斯基应用程序放置在备份区中的文件的通用列表在 Kaspersky Security Center 中生成，可在 Web Console 和管理控制台（**高级 → 存储库 → 备份区**）中查看。

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中。

**如何在 Web Console 中查看备份区中对象的信息**

1. 在 Web Console 主窗口中，选择 **存储库 → 文件备份**。

   这将打开客户端设备上由卡巴斯基应用程序放置在备份区中的文件列表。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中。

2. 查看受保护设备上备份区中文件的属性：

   - **文件名**
   - **状态**：
     - *警告*
     - *可能已感染*
     - *由用户添加*
     - *误报*
     - *已清除*
     - *未感染*
     - *受密码保护*
     - *已删除*
     - *必须发送给卡巴斯基*
   - **设备名称**

- **执行的操作**：
  - *删除*
  - *清除*
  - *扫描*
  - *正在恢复*
- **对象**
- **已放入存储库**
- **条目添加者**
- **大小（字节）**
- **文件夹已恢复**
- **用户**
- **描述**
- **虚拟管理服务器的名称**

**如何在命令行中查看备份区对象的信息**

要查看备份中对象的详细信息，请运行：

```
kesl-control -B --query ["<filter conditions>"] [-n <objects number>] [--json]
```

其中：

- `<filter conditions>` 指定一个或多个采用 `<field> <comparison operator> '<value>'` 格式且使用逻辑运算符 `and` 组合的 逻辑表达式，以限制查询结果。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。
- `<objects number>` 指定要显示的存储中最新对象的数量。如果您不指定 `-n` 选项，应用程序将显示最近 30 个对象的信息。如果您要显示所有对象的信息，请指定 `0`。
- `--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。

**如何在图形界面中查看备份区对象的信息**

1. 打开应用程序图形界面的主窗口。
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。

从备份中恢复对象

文件将根据指定的设置从备份区恢复到其原始位置。恢复操作会保留 MAC 标签（仅限 Astra Linux 设备）和原始文件的属性（不可变属性和仅追加属性除外）。

在 Astra Linux 设备上，从备份区恢复文件在以下情况下会出错：

- 文件的 MAC 标签高于要将文件恢复到的目录的 MAC 标签。
- 文件的 MAC 标签低于要将文件恢复到的目录的 MAC 标签，并且未为此目录设置 ccnr 标志。
- 在 Astra Linux 设备上的封闭软件环境模式下，您只能使用将文件放入备份区时所用的同一帐户来恢复文件。恢复文件时，应用程序会创建一个 MAC 标签为 3（cnnr 标志）的目录。

要管理 Kaspersky Security Center 的备份中的文件，您需要启用将备份文件相关数据传输到管理服务器的功能。

恢复受感染的对象可能会导致设备感染。

**如何在 Web Console 中从备份区恢复对象**

1. 在 Web Console 主窗口中，选择 **存储库 → 文件备份**。

   这将打开客户端设备上由卡巴斯基应用程序放置在备份区中的文件列表。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中。

2. 选中要恢复的文件旁边的复选框。
3. 点击 **恢复**。

客户端设备上的备份区对象已恢复。

**如何在命令行中从备份区恢复对象**

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 -B --restore <object id>
```

其中 `<object id>` 是应用程序在将对象放入备份区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 -B --restore <object id> --file <path to file>
```

其中 `--file <path to file>` 是文件的新名称以及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。

在 Astra Linux 设备上的封闭软件环境模式下，您只能使用将文件放入备份区时所用的同一帐户来恢复文件。

**如何在图形界面中从备份区恢复对象**

*要将对象从备份区恢复到其原始目录：*

1. 打开应用程序图形界面的主窗口。
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。
3. 选择要恢复的对象。
4. 点击 **恢复**。

备份区中的对象已恢复，并可在原始目录中使用。

有关恢复和删除对象的信息保存到事件日志中。

从备份中删除对象

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最旧的备份副本。

您可以手动删除已恢复或未恢复的文件的备份副本。

**如何在 Web Console 中删除备份区对象**

1. 在 Web Console 主窗口中，选择 **存储库 → 文件备份**。
   这将打开客户端设备上由卡巴斯基应用程序放置在备份区中的文件列表。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中。
2. 选中要删除的文件旁边的复选框。
3. 单击“**删除**”按钮。

   客户端设备上的备份区对象已删除。

**如何在命令行中删除备份区对象**

*要从备份中移除所选对象，请运行：*

```
kesl-control -B --mass-remove --query "<filter conditions>"
```

其中 `<filter conditions>` 指定一个或多个 逻辑表达式，这些表达式采用 `<field> <comparison operator> '<value>'` 格式，并使用逻辑运算符 `and` 组合以限制查询结果。

**例如：**

移除 ID=15 的对象

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

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
```

**如何在图形界面中删除备份区对象**

1. 打开应用程序图形界面的主窗口。
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。
3. 选择要删除的对象。
4. 单击“**删除**”按钮。

备份区对象将被删除。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。

# 防御高级威胁和定向攻击

Kaspersky Detection and Response 解决方案是用于检测组织基础设施不同级别的高级威胁和攻击指标的安全系统。Detection and Response 解决方案提供有关检测到的威胁的信息，并允许您管理对检测结果的响应。

Kaspersky Endpoint Security 可与以下 Kaspersky Detection and Response 解决方案进行互操作：

- Open Single Management Platform (OSMP) 上的 Kaspersky Endpoint Detection and Response Expert (on-premises)。集成由 Kaspersky Endpoint Security 应用程序组件 Endpoint Detection and Response Expert (on-premises)（以下简称 *EDR Expert (on-premises)*）提供。
- Open Single Management Platform (OSMP) 上的 Kaspersky Endpoint Detection and Response Expert (cloud)。集成由 Kaspersky Endpoint Security 应用程序组件 Endpoint Detection and Response Expert (cloud)（以下简称 *EDR Expert (cloud)*）提供。

- Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 组件位于 Kaspersky Anti Targeted Attack Platform上。集成由 Kaspersky Endpoint Security 应用程序的以下组件提供：
  - Endpoint Detection and Response Expert (on-premises)（以下简称 *EDR Expert (on-premises)*）。
  - Network Detection and Response (KATA)（以下也称为 *NDR (KATA)*）。
- 在 Open Single Management Platform (OSMP) 或 Kaspersky Anti Targeted Attack Platform 上的Sandbox 。集成由以下 Kaspersky Endpoint Security 组件提供： *Sandbox* 。
- Kaspersky Unified Monitoring and Analysis Platform。
- Kaspersky Endpoint Detection and Response Optimum。Kaspersky Endpoint Security 组件 Endpoint Detection and Response Optimum (*EDR Optimum*) 可促进集成。
- Kaspersky Managed Detection and Response。Kaspersky Endpoint Security 组件 Managed Detection and Response (*MDR*) 可促进集成。

### Detection and Response 解决方案集成功能

- 如果您在 EDR Agent 模式下使用 Kaspersky Endpoint Security，则仅支持与 Open Single Management Platform (OSMP) 上的 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，以及与 Kaspersky Anti Targeted Attack Platform 上的 Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 组件集成。
- 当 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 集成时，内置代理可能会将大量事件记录到 systemd-journald 日志中。如果要禁用将审计事件记录到 systemd-journald 日志中，请禁用 systemd-journald-audit 套接字并重启操作系统。

  禁用 systemd-journald-audit 套接字

  ```
  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 操作系统中，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。
- Detection and Response 解决方案在从安装了 Kaspersky Endpoint Security for Linux 的镜像创建的虚拟机上可能无法正常工作。与 Detection and Response 解决方案集成时，会使用计算机的唯一 ID（Sensor ID）。应用程序在初始安装过程中会生成此 ID，即使卸载应用程序后也会保留此 ID。克隆镜像时，虚拟机会继承 Sensor ID，这可能会导致 Detection and Response 解决方案将多个虚拟机识别为同一设备。

  有关创建参考镜像以正确集成 MDR 的建议

  如何准备用于与 EDR Expert (on-premises) 正确集成的参考镜像

# 响应操作

与 Detection and Response 解决方案集成时，Kaspersky Endpoint Security 可以执行威胁响应操作以维护安全功能。如果在 Detection and Response 解决方案的设置中启用了此功能，则可以在 Detection and Response 解决方案端生成威胁响应操作，并在 Kaspersky Endpoint Security 设备上自动执行。您还可以手动配置和执行威胁响应操作。

威胁响应操作的设置取决于与 Kaspersky Endpoint Security 集成的 Detection and Response 解决方案。

Kaspersky Endpoint Security 可以执行以下威胁响应操作：

- 将设备与网络隔离。

  当与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，网络隔离会在 Detection and Response 解决方案端启用或禁用。您可以手动禁用设备的网络隔离。

  与 Kaspersky Endpoint Detection and Response Optimum 集成时，可以自动或手动将设备与网络隔离。您可以配置网络隔离或手动禁用设备的网络隔离。

- 隔离文件。

  操作使用*隔离区文件*任务执行。

  当与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务会在 Detection and Response 解决方案端创建并运行。

  与 Kaspersky Endpoint Detection and Response Optimum 集成时，可以根据检测到的入侵指标自动隔离文件。

  当与 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Managed Detection and Response 集成时，您也可以手动隔离文件。

- 从隔离区恢复文件。

  当与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，威胁响应操作会在 Detection and Response 解决方案端生成。您也可以使用 Kaspersky Security Center 或命令行手动执行该操作。

  与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以使用 Kaspersky Security Center 或命令行手动执行该操作。

- 从隔离区删除文件。

  当与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，威胁响应操作会在 Detection and Response 解决方案端生成。您也可以使用 Kaspersky Security Center 或命令行手动执行该操作。

  与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以使用 Kaspersky Security Center 或命令行手动执行该操作。

- 从隔离区获取文件。

当与 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，威胁响应操作会在 Detection and Response 解决方案端生成。

与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以使用 Kaspersky Security Center 手动执行该操作。

- 从设备接收文件。

  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应用程序生成的事件日志文件。

  当与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务会在 Detection and Response 解决方案端创建并运行。

  与 Kaspersky Endpoint Detection and Response Optimum 解决方案集成时，您可以在 Web Console 中创建"获取文件"任务。

- 从设备删除文件。

  此操作使用*删除文件*任务执行。

  当与 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response Expert (cloud) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，任务会在 Detection and Response 解决方案端创建并运行。

  与 Kaspersky Endpoint Detection and Response Optimum 解决方案集成时，您可以在 Web Console 中创建"删除文件"任务。

- 远程在设备上运行进程。

  此操作使用*运行应用程序*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*"任务检索所创建的文件。

  当与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务会在 Detection and Response 解决方案端创建并运行。

  与 Kaspersky Endpoint Detection and Response Optimum 解决方案集成时，您可以在 Web Console 中创建并执行"运行进程"任务。

- 远程终止设备上的进程。

  该操作使用*Kill 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。

  当与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务会在 Detection and Response 解决方案端创建并运行。

  与 Kaspersky Endpoint Detection and Response Optimum 解决方案集成时，您可以在 Web Console 中创建并执行"Kill 进程"任务。

- 检测设备上的入侵指标 (IOC)。

  *入侵指标 (IOC)* 是一组有关对象或活动的数据，指示对设备的未经授权访问（入侵数据）。例如，入侵指标可能是很大的失败登录尝试次数。

- 启动 *YARA 扫描*。

  在*YARA 扫描*期间， Kaspersky Endpoint Security 使用 YARA 文件搜索设备上的恶意活动特征。*YARA 文件*是扩展名为 YARA 或 YAR 的文件，其中包含 YARA 规则。*YARA 规则*描述针对企业 IT 基础设施的定向攻击和入侵的特征。Kaspersky Endpoint Security 使用这些规则扫描对象。如果满足规则的条件，分析器会判定感染正在进行，并将详细信息记录在日志中。扫描会在本地驱动器上递归执行。不支持扫描网络、可移动和云资源。

  在 Kaspersky Endpoint Security 设备上执行 YARA 扫描的命令会在 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案端创建并运行。

- 执行防护

- 获取取证信息。

  当与 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Expert (cloud) 集成时，您可以收集数字数据，这些数据在调查与网络犯罪和数据泄漏相关的事件时可能会有用。

  此操作可以使用以下任务执行：

  - *获取取证*任务，该任务收集以下类型的信息：
    - 文件列表
    - 进程列表
    - 自动运行点列表
  - *获取内存转储*任务
  - *获取进程内存转储*任务
  - *获取磁盘镜像*任务

  任务会在 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案端创建并运行。

## 搜索入侵指标

*妥协的指标 (IOC)* 是一组关于对象或活动的数据，表示未经授权访问计算机（数据泄露）。例如，入侵指标可能是很大的失败登录尝试次数。*IOC 扫描*任务允许在计算机上查找妥协的指标，并采取威胁响应措施。

如果满足以下任一条件，则可以使用 Kaspersky Endpoint Security 应用程序的 IOC 扫描功能：

- Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 解决方案的整合已启用，且 EDR Optimum 组件已激活。

  在这种情况下，IOC 搜索是使用 *IOC 扫描*任务执行的。

- 已启用 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，并且已激活 EDR Expert (on-premises) 组件。

  在这种情况下，IOC 扫描在相应解决方案端执行。

*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*任务不计算大于 200 MB 的文件的哈希。

为了搜索入侵指标，Kaspersky Endpoint Security 使用用户准备的 IOC 文件。如果您想手动添加入侵指标，请参阅IOC 文件要求。如果 IOC 文件不符合要求，应用程序将无法使用它。

IOC 扫描任务中使用的所有 IOC 文件的 ID必须是唯一的。如果加载具有相同 ID 的多个 IOC 文件，则应用程序仅使用其中一个 IOC 文件。其他 IOC 文件将被自动排除。

创建一个“IOC 扫描”任务

您可以手动创建 *IOC 扫描*任务：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

- 使用任务向导。

- 在本地命令行中进行。

**如何在 Web Console 中创建“IOC 扫描”任务**

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

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“**Kaspersky Endpoint Security for Linux 12.5**”。

   b. 在“**任务类型**”下拉列表中，选择“**IOC 扫描**”。

   c. 在 **任务名称** 字段中，输入新任务的名称。

   d. 在 **要对其分配任务的设备** 下，选择要如何定义任务范围。

4. 根据您首选的任务范围定义方法选择设备。继续下一步。

5. 结束向导。

   在任务列表中将显示一个新任务。

6. 单击新任务。

   任务属性窗口将打开。

7. 选择**应用程序设置**选项卡。

8. 转到**威胁扫描**区域。

9. 上传 IOC 文件以搜索入侵指标。

   上传 IOC 文件后，应用程序会显示有关该文件的摘要信息，包括未通过检查的指标列表。上传 IOC 文件后，您可以直接在任务属性中手动在内置编辑器中编辑文件。Kaspersky Endpoint Security 支持编辑符合 OpenIOC 1.1 标准的 IOC 文件。无法修改符合 OpenIOC 1.0 版本的 IOC 文件的内容。

   Kaspersky Endpoint Security 将 IOC 文件添加到 IOC 收集中。如有必要，您可以暂时将 IOC 文件排除在任务范围之外。

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。

10. 转到**扫描设置**区域。

11. 如有必要，配置回顾性 IOC 扫描。

    *回顾性 IOC 扫描*是 *IOC 扫描* 任务的一种模式，在该模式下，Kaspersky Endpoint Security 使用特定时间段的数据扫描入侵指标。此模式旨在通过受保护计算机的遥测数据（例如网络活动、进程、文件和其他遥测数据）来搜索入侵指标。Kaspersky Endpoint Security 分析计算机上的操作系统日志和浏览器日志中的数据。回顾性 IOC 扫描分析以下浏览器的日志：Google Chrome、Mozilla Firefox、Microsoft Edge（版本 79 或更高版本）。

    a. 在 **IOC 追溯扫描** 下，转到搜索设置。

    b. 启用 **IOC 追溯扫描** 切换开关。

    c. 设置回顾性 IOC 扫描的时间间隔。

12. 选择作为任务的一部分必须被分析的数据类型 (IOC 文档)。

    Kaspersky Endpoint Security 根据加载的 IOC 文件的内容自动选择"*IOC 扫描*"任务的数据类型（IOC 文档）。不建议取消选择数据类型。

    此外，您可以配置 **文件 – FileItem** 数据类型的搜索范围。使用预设范围在计算机上设置 IOC 扫描范围。

13. 转到**响应设置**区域。

14. 选择任务运行模式：**仅警报** 或 **警报和响应**。

15. 选择检测到 IOC 时的响应操作：

    - "**运行关键区域扫描**"。如果选择此选项，Kaspersky Endpoint Security 运行*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。

      **Kaspersky Endpoint Security 扫描的关键区域**

      - /lib/systemd
      - /lib/udev
      - /lib/dbus-1.0
      - /usr/local/lib/systemd/user
      - /usr/share/dbus-1
      - /usr/share/gdm/autostart
      - /usr/share/gnome/autostart
      - /var/spool/at
      - /var/spool/at/spool

- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

- "**将副本移动到隔离区，删除对象**"。如果选择此选项，Kaspersky Endpoint Security 删除在计算机上发现的恶意对象。在删除对象之前，Kaspersky Endpoint Security 会创建它的备份副本，以防您稍后需要恢复该对象。Kaspersky Endpoint Security 移动备份副本到隔离区。

  如果清除此复选框，您可以在手动运行任务后手动隔离该文件。如果"*IOC 扫描*"任务检测到可能危及数据的文件，您可以直接从 IOC 扫描结果中隔离此文件（**应用程序设置 → IOC 扫描结果**）。因此，Kaspersky Endpoint Security 将使用检测到的文件的预设数据启动任务创建向导。您只需要管理额外的任务设置，例如设置任务计划。

- “**将设备与网络隔离**”。如果选择此选项，Kaspersky Endpoint Security 将计算机与网络隔离，以防止威胁扩散。您可以在 Endpoint Detection and Response 组件设置中配置隔离的持续时间。

  如果清除此复选框，您可以在手动运行任务后将计算机与网络隔离。如果“*IOC 扫描*”任务检测到可能危及数据的文件，您可以直接从 IOC 扫描结果中隔离此文件（**应用程序设置** → **IOC 扫描结果**）。因此，Kaspersky Endpoint Security 将使用检测到的文件的预设数据启动任务创建向导。您只需要管理额外的任务设置，例如设置任务计划。

16. 在任务属性窗口中，选择“**计划**”选项卡。

17. 配置任务计划。

    “Wake-on-LAN”不可用于此任务。确保计算机已打开以运行任务。

18. 保存更改。

19. 选中该任务旁边的复选框。

20. 单击“**开始**”。

    您可以在 Web Console 中任务属性的 **IOC 扫描结果** 下查看 *IOC 扫描* 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。

### 如何在命令行中创建“IOC 扫描”任务

请执行命令：

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

符号

恶意软件扫描任务的设置

| 设置 | 描述 |
| --- | --- |
| `--path` | IOC 文件或包含 .IOC 或 .XML 扩展名 IOC 文件的目录的路径，该路径应用于执行扫描。*IOC 文件*是包含应用程序尝试匹配以计数检测的指标集的文件。IOC 文件必须符合 OpenIOC 标准。<br>您可以指定多个路径，用空格分隔。您还可以指定两种类型的路径（文件路径和目录路径）。 |
| `--process` | 执行 IOC 扫描时分析进程数据（ProcessItem 术语）。<br>如果参数的值为“`off`”，则在执行扫描时，Kaspersky Endpoint Security 不会分析计算机上运行的进程。如果 IOC 文件包含 ProcessItem IOC 文档的 IOC 术语，则忽略这些术语（检测为不匹配）。<br>如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 ProcessItem IOC 文档时，Kaspersky Endpoint Security 才会分析进程数据。 |
| `--hint` | 执行 IOC 扫描时分析文件数据（ProcessItem 和 FileItem 术语）。<br>您可以采用以下方式之一选择文件：<br>• `<full path to the executable file of the process>` – ProcessItem 术语；<br>• `<full path to the file>` – FileItem 术语。 |
| `--arpentry` | 执行 IOC扫描（ArpEntryItem术语）时，分析有关 ARP 表中记录的数据。<br>如果参数的值为 `off`，Kaspersky Endpoint Security 不会扫描 ARP 表。如果 IOC 文件包含 ArpEntryItem IOC 文档术语，则忽略这些术语（检测为不匹配）。<br>如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 ArpEntryItem IOC 文档时，Kaspersky Endpoint Security 才会分析 ARP 表。 |

| 设置 | 描述 |
| --- | --- |
| `--ports` | 分析有关在执行 IOC 扫描时打开以进行侦听的端口的数据（PortItem 术语）。<br>如果参数的值为 `off`，Kaspersky Endpoint Security 不会扫描设备上的活动连接表。如果 IOC 文件包含 PortItem IOC 文档术语，则忽略这些术语（检测为不匹配）。<br>如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 PortItem IOC 文档时，Kaspersky Endpoint Security 才会分析设备上的活动连接表。 |
| `--system` | 执行 IOC 扫描时分析环境数据（SystemInfoItem 术语）。<br>如果参数的值为 `off`，Kaspersky Endpoint Security 不会分析环境数据。如果 IOC 文件包含 SystemInfoItem IOC 文档术语，则忽略这些术语（检测为不匹配）。<br>如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 SystemInfoItem IOC 文档时，Kaspersky Endpoint Security 才会分析环境数据。 |
| `--files` | 执行 IOC 扫描时分析文件数据（FileItem 术语）。<br>如果参数的值为 `off`，Kaspersky Endpoint Security 不会分析文件数据。如果 IOC 文件包含 FileItem IOC 文档术语，则忽略这些术语（检测为不匹配）。<br>如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 FileItem IOC 文档时，Kaspersky Endpoint Security 才会分析文件数据。 |
| `--drives` | 在分析 FileItem IOC 文档的数据时设置 IOC 扫描范围。<br>您可以为扫描范围设置以下值：<br>• `<all>` 用于所有可用的文件范围。<br>• `<system>` 用于安装操作系统的文件夹中的文件。<br>• `<critical>` 用于用户和系统文件夹中的临时文件。<br>• `<custom>` 用于用户定义的范围（`/scope=<list of folders to scan>`）。<br>如果未指定参数，则对关键区域执行扫描。 |
| `--excludes` | 在分析 FileItem IOC 文档的数据时设置排除范围。您可以指定多个由空格分隔的路径。 |
| `--scope` | 在分析 FileItem IOC 文档的数据时设置的用户定义的 IOC 扫描范围（`/drives=custom`）。您可以指定多个由空格分隔的路径。 |
| `--action` | 检测到入侵指标时执行的操作：<br>• `Skip`。如果选择此选项，Kaspersky Endpoint Security 仅检测可能导致数据泄露的文件。<br>• `QuarantineFile`。如果选择此选项，Kaspersky Endpoint Security 删除在计算机上发现的恶意对象。在删除对象之前，Kaspersky Endpoint Security 会创建它的备份副本，以防您稍后需要恢复该对象。Kaspersky Endpoint Security 移动备份副本到隔离区。<br>• `IsolateHost`。如果选择此选项，Kaspersky Endpoint Security 将计算机与网络隔离，以防止威胁扩散。<br>• `ScanCriticalAreas`。如果选择此选项，Kaspersky Endpoint Security 运行*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。 |

# 网络隔离

与 Detection and Response 解决方案集成时，设备可以与网络隔离，作为威胁响应操作。

## 与网络隔离相关的特殊注意事项

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：

- 在网络隔离排除项中指定的连接
- 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。
- KSN 连接（与 Kaspersky Managed Detection and Response 集成时）

当满足以下条件之一时，可以应用网络隔离：

- Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 解决方案的整合已启用，且 EDR Optimum 组件已激活。
- 已启用 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，并且已激活 EDR Expert (on-premises) 组件。
- Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 解决方案的整合已启用，且 MDR 组件已激活。

与 Kaspersky Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 以及 Kaspersky Managed Detection and Response 集成时，可启用或禁用设备的网络隔离，并在 Detection and Response 解决方案端配置网络隔离排除项。详情请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助、Kaspersky Anti Targeted Attack Platform 帮助或 Kaspersky Managed Detection and Response 帮助。必要时，您可以手动禁用设备的网络隔离：

- 在 Web Console 的设备属性中（仅当与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时）
- 在命令行上

无论是否启用与 Detection and Response 解决方案的整合，也无论是否将策略应用于设备，都可以手动禁用网络隔离。

与 Kaspersky Endpoint Detection and Response Optimum 集成时，可以采用以下模式之一应用网络隔离：

- 自动网络隔离模式。检测到入侵指标后，可以自动将设备与网络隔离。在“**检测到 IOC 后的操作**”部分创建和配置 *IOC 扫描*任务设置时，如果选中“**检测到 IOC 时应用响应操作**”和“**将设备与网络隔离**”复选框，则当应用程序检测到入侵指标时，会自动启用网络隔离。

  您可以管理以下自动网络隔离设置：

  - 更改自动禁用网络隔离的持续时间。
  - 为自动隔离的设备配置网络隔离排除项。

  > 如果被自动隔离的设备符合某项策略，则会应用该策略中指定的设置。如果未应用某项策略，则应用设备属性中指定的设置。

- 手动网络隔离模式。在调查检测到的威胁时，您可以将设备与网络隔离。您可以在警报详情窗口和 Web Console 的设备属性中手动为设备启用网络隔离。

  您可以管理以下手动网络隔离设置：

  - 更改自动禁用网络隔离的持续时间。
  - 为手动隔离的设备配置网络隔离排除项。

与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以在 Web Console 上的设备属性中和命令行上手动禁用设备的网络隔离。

您可以在命令行上检查设备的网络隔离状态。

隔离设备会被被自动分配“**已从网络隔离**”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。

网络隔离限制

使用网络隔离时，我们强烈建议您熟悉相关限制。

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（并且该应用程序未运行），当 Kaspersky Managed Detection and Response 启用网络隔离时，流量可能不会被阻止。

DHCP 和 DNS 不会自动添加到网络隔离排除项中，因此如果在网络隔离期间变更资源的网络地址，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 不会失去与提供基础的服务器的联系。

在内核版本为 4.18 或更高版本且支持 eBPF 和 BTF、并启用了内核跟踪的跟踪点和 kprobes 功能的设备上，支持按名称将进程从网络隔离中排除。

如果 Kaspersky Endpoint Security 在标准模式或 EDR Agent 模式下使用，则在使用网络隔离时，建议执行以下操作：

- 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，则必须配置要使用的代理服务器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。

## 在 Web Console 中手动启用或禁用设备的网络隔离

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以使用 Web Console 为设备启用网络隔离。

与 Kaspersky Endpoint Detection and Response Optimum 集成时手动启用和禁用设备的网络隔离

*要手动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. 如有必要，请选择一个管理组，找到您的设备，然后单击其名称。

3. 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。

4. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。

5. 在打开的应用程序属性窗口中，在**应用程序设置**选项卡上，选择**内置代理 → Endpoint Detection and Response**。

6. 这将打开一个窗口；在该窗口中，在**网络隔离**下执行以下操作之一：

   - 单击**将设备从网络中隔离**按钮，启用设备的网络隔离。仅当**Endpoint Detection and Response**拨动开关已启用时，该按钮才可用。

     单击此按钮时，设备将在*启用网络隔离 (NetworkIsolationStart)*任务的属性中指定的时间段内被隔离。

   - 单击“**解除阻止隔离的设备**”按钮可禁用该设备的网络隔离。无论**Endpoint Detection and Response**拨动开关处于启用还是禁用状态，该按钮均可用。

7. 单击“**确定**”。

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。

在与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，手动禁用设备的网络隔离

*要手动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。

6. 在打开的应用程序属性窗口的“**应用程序设置**”选项卡上，选择“**Detection and Response**”部分。

7. 在 **网络隔离 (EDR Expert (on-premises))** 下，单击 **解除阻止隔离的设备** 按钮以禁用设备的网络隔离。

禁用设备的网络隔离后，Kaspersky Endpoint Security 将从设备上移除“**ISOLATED FROM NETWORK**”标签。

## 配置自动网络隔离的持续时间

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以配置自动网络隔离的持续时间：

对于由 *IOC 扫描*任务隔离的设备，其网络隔离会在一段时间后自动禁用。您可以通过 Web Console，在设备属性和策略属性中配置此超时时间。Web Console 策略属性中的网络隔离设置详见附录 5。下表描述了受管理设备属性中的网络隔离设置。

如果将策略应用于设备，则会应用策略中指定的设置；而无法在设备属性中配置自动网络隔离超时时间。如果该策略不适用于设备，则应用设备属性中指定的设置。

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。

6. 在打开的应用程序属性窗口中，在**应用程序设置**选项卡上，选择**Detection and Response** 然后单击 **Endpoint Detection and Response Optimum**链接。

7. 在“**网络隔离**”下，单击“**配置设备解除阻止**”。

8. 这将打开**配置设备解除封锁**窗口；在该窗口中，选中**在此后解除封锁被自动隔离的设备：**复选框，并在其下方的输入字段中，指定此后设备必须被自动解除封锁的时间段（以小时为单位）。

9. 保存更改。

## 手动配置网络隔离

要手动将设备与网络隔离，则需要与 Kaspersky Endpoint Detection and Response Optimum 整合。

如果手动为设备启用网络隔离，则可以使用“*启用网络隔离*”(*NetworkIsolationStart*) 本地任务预先配置网络隔离。您可以配置设备的网络隔离排除项和网络隔离持续时间。

“*启用网络隔离*”是一项预定义任务，仅在以下情况下自动运行：

- 点击设备属性中的“**将设备与网络隔离**”按钮。
- 如果您在警报详情窗口中启用设备的网络隔离。

点击“**添加**”按钮无法创建“*启用网络隔离*”任务的新实例，点击“**开始**”按钮也无法运行该任务。此任务仅在设备属性中可用，您可以在启用设备的网络隔离之前，在设备属性中更改其设置。

无论策略是否应用于设备，“*启用网络隔离*”任务设置均适用。

*要配置设备的网络隔离参数：*

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“**任务**”选项卡。
5. 在任务列表中，点击“*启用网络隔离*”任务。
   任务属性窗口将打开。
6. 转到“**应用程序设置**”选项卡。
7. 单击“**配置排除项**”链接打开“**排除项**”窗口。
8. 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，然后从词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**按钮。
9. 单击“**确定**”。
10. 在**隔离设备**字段中，输入设备网络隔离的所需持续时间（以小时为单位）。
    网络隔离默认时长为 5 小时。
    网络隔离最短时长为 1 小时。
11. 单击“**保存**”按钮以保存更改。

## 在 Web Console 中配置网络隔离排除项

当 Kaspersky Endpoint Security 与 Endpoint Detection and Response Expert (on-premises)、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，网络隔离排除项在 Detection and Response 解决方案端配置。详情请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助、Kaspersky Anti Targeted Attack Platform 帮助或 Kaspersky Managed Detection and Response 帮助。

当 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以通过以下方式配置网络隔离排除项：

- 在 Web Console 的策略属性中。当为应用该策略的设备自动启用网络隔离时，将应用策略中配置的排除项。
- 在 Web Console 的设备属性中。当为未应用任何策略的设备自动启用网络隔离时，将应用设备属性中配置的排除项。
- 在“*启用网络隔离*”(*NetworkIsolationStart*) 本地任务的设置中配置。当您手动为设备启用网络隔离时，将应用此任务属性中配置的排除项。无论策略是否应用于设备，*启用网络隔离*任务设置均适用。

应用程序提供了*标准网络配置文件*列表，用于配置网络隔离排除项。网络配置文件由一系列规则组成，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。您可以管理标准网络配置文件的设置并手动配置排除项。

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。

**如何在 Web Console 中添加网络隔离排除项**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 在“**网络隔离**”区域，单击“**排除项**”链接。
   这将打开一个包含网络隔离排除项列表的窗口。
6. 您可以通过以下方式排除网络连接：
   - 单击 **添加**，然后输入网络连接信息。

     您可以添加一个应用程序，组件将不会阻止该应用程序的网络连接。此设置适用于内核版本为 4.18 或更高版本、支持 eBPF 和 BTF，并且启用了用于内核跟踪的 tracepoints 和 kprobes 功能的设备。

   - 单击 **从配置文件添加** 按钮，然后从词典中选择网络配置文件。
7. 保存更改。

**如何在 Web Console 中删除网络隔离排除项**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。

5. 在“**网络隔离**”区域，单击“**排除项**”链接。

   这将打开一个包含网络隔离排除项列表的窗口。

6. 选中网络连接旁边的复选框，然后单击 **删除**。

7. 保存更改。

# 隔离文件

在应对威胁时，Kaspersky Endpoint Detection and Response 可以创建*移动文件到隔离区*任务。这对于将威胁的后果降至最低是必要的。*隔离区*是计算机上的一个特别的本地存储区。用户可以隔离用户认为对计算机有危险的文件。隔离的文件以加密形式存储，不会威胁设备的安全。

您可以用以下方式创建*移动文件到隔离区*任务：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。您可以直接从警报详情中选择要删除的文件。因此，Kaspersky Endpoint Security 将使用检测到的文件的预设数据启动任务创建向导。您只需要管理额外的任务设置，例如设置任务计划。

- 使用任务向导。

  新任务向导允许手动输入要删除的文件或目录的路径以及要删除文件的哈希值。您还可以管理其他任务设置，例如设置任务计划。

- 在“*IOC 扫描*”任务设置中。

  如果“*IOC 扫描*”任务检测到可能危及数据的文件，您可以直接从 IOC 扫描结果中隔离此文件（**应用程序设置 → IOC 扫描结果**）。因此，Kaspersky Endpoint Security 将使用检测到的文件的预设数据启动任务创建向导。您只需要管理额外的任务设置，例如设置任务计划。

文件大小不得超过 100 MB。

*如何创建 移动文件到隔离区 任务*

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

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“**Kaspersky Endpoint Security for Linux**”。

   b. 在“**任务类型**”下拉列表中，选择“**移动文件到隔离区**”。

   c. 在“**任务名称**”字段中，输入简要说明。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。单击“**下一步**”。

5. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。
6. 单击新任务。
7. 任务属性窗口将打开。
8. 选择**应用程序设置**选项卡。
9. 在文件列表中，单击“**添加**”。
   文件添加向导将启动。
10. 要添加文件，您需要输入文件路径或目录路径以及文件哈希值。
11. 在任务属性窗口中，选择“**计划**”选项卡。
12. 配置任务计划。
13. 保存更改。
14. 选中该任务旁边的复选框。
15. 单击“**开始**”。

结果，Kaspersky Endpoint Security 将文件移动到隔离区。

如果文件被其他进程锁定，则任务显示为*已完成*，但文件本身只有在计算机重新启动后才会被隔离。重新启动计算机后，确认文件已删除。

如果试图隔离当前正在运行的可执行文件，则“*移动文件到隔离区*”任务可能会以“*访问被拒绝*”错误结束。为该文件创建终止进程任务，然后重试。

如果试图隔离太大的文件，则“*移动文件到隔离区*”任务可能会以“*隔离区存储空间不足*”错误结束。清除隔离区或增加隔离区的容量。然后再次尝试。

# 从设备接收文件

您可以从用户计算机获取文件。例如，您可以将应用程序配置为获取第三方应用程序生成的事件日志文件。执行任务后，文件副本将保存在隔离区中。*隔离区*是计算机上的一个特别的本地存储区。您可以使用 Web Console 将此文件从隔离区下载到您的计算机（**操作 → 存储库 → 隔离**）。用户设备上的原始文件仍保留在其原始目录中。

在 Kaspersky Security Center 的隔离文件列表中，无论文件扫描结果如何，通过 *获取文件* 任务接收的所有文件都将具有 *被感染* 状态。

文件大小不得超过 100 MB。

*如何创建 获取文件 任务*

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
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“**Kaspersky Endpoint Security for Linux**”。
   b. 在“**任务类型**”下拉列表中，选择“**获取文件**”。
   c. 在“**任务名称**”字段中，输入简要说明。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。单击“**下一步**”。
5. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。
6. 单击新任务。
7. 任务属性窗口将打开。
8. 选择**应用程序设置**选项卡。
9. 在文件列表中，单击“**添加**”。
   文件添加向导将启动。
10. 要添加文件，您需要输入文件路径或目录路径以及文件哈希值。
11. 在任务属性窗口中，选择“**计划**”选项卡。
12. 配置任务计划。
13. 保存更改。
14. 选中该任务旁边的复选框。
15. 单击“**开始**”。

结果，Kaspersky Endpoint Security 创建文件的副本并将其移动到隔离区。您可以在 Web Console 中从隔离区下载文件。

在以下情况下，*获取文件* 任务将以错误结束：

- 未找到指定的文件。
- 指定了不正确的文件信息（文件名或校验和）。
- 权限不足，无法管理指定的文件。

- 指定的文件已被阻止。
- 隔离区空间不足。
- 指定的文件太大（超过 100 MB）。

## 从设备删除文件

您可以使用“*删除文件*”任务远程删除文件。例如，您可以在响应威胁时远程删除文件。

*如何创建 删除文件 任务*

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
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“**Kaspersky Endpoint Security for Linux**”。
   b. 在“**任务类型**”下拉列表中，选择“**删除文件**”。
   c. 在“**任务名称**”字段中，输入简要说明。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。单击“**下一步**”。
5. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。
6. 单击新任务。
7. 任务属性窗口将打开。
8. 选择**应用程序设置**选项卡。
9. 要添加文件，您需要输入目录路径和文件哈希值。
10. 在任务属性窗口中，选择“**计划**”选项卡。
11. 配置任务计划。
12. 保存更改。
13. 选中该任务旁边的复选框。
14. 单击“**开始**”。

结果，Kaspersky Endpoint Security 将从计算机删除文件。如果文件被其他进程锁定，则任务显示为*已完成*，但文件本身只有在计算机重新启动后才会被删除。重新启动计算机后，确认文件已删除。

# 启动进程

您可以使用"*进程启动*"任务远程运行文件。例如，您可以远程运行创建计算机配置文件的实用程序。下一步，您可以使用 *获取文件* 任务在 Kaspersky Security Center Web Console 中接收所创建的文件。

如果操作系统中的 SELinux 处于 `Enforcing` 模式，则要启动 *进程启动* 任务，您需要对 SELinux 执行额外配置。

### 如何配置 SELinux 以运行"启动进程"任务

如果您计划在操作系统中以 `Enforcing` 模式使用 SELinux，则要在与 Detection and Response 解决方案集成时执行响应操作，您需要额外管理 SELinux 设置。

此 SELinux 配置需要 root 权限。

*要为响应操作配置 SELinux：*

1. 将 SELinux 切换为宽容模式：
   - 如果 SELinux 已启用，请运行以下命令：

     将 SELinux 切换为宽容模式

     ```
     setenforce Permissive
     ```

   - 如果 SELinux 已禁用，请在 /etc/selinux/config 配置文件中设置 `SELINUX=permissive`，然后重启操作系统。
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. 运行所有任务，以执行您希望在与 Detection and Response 解决方案集成时使用的响应操作。
4. 确保 audit.log 文件中没有错误。

   查看 audit.log 文件

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

5. 如果 audit.log 文件中存在任何错误，请根据阻止记录创建并加载新的规则模块以修复错误，然后再次运行响应操作任务。

   根据阻止记录创建并加载新的规则模块：

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

6. 将 SELinux 切换为强制模式。

```
setenforce Enforcing
```

*如何创建 进程启动 任务*

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

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“**Kaspersky Endpoint Security for Linux**”。

   b. 在“**任务类型**”下拉列表中，选择“**进程启动**”。

   c. 在“**任务名称**”字段中，输入简要说明。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。单击“**下一步**”。

5. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。

6. 单击新任务。

7. 任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 输入进程启动命令：

   - “**可执行命令**”。用于输入启动进程的命令的字段。
     例如，如果您想运行用于检查与管理服务器连接的 `klnagchk` 实用程序，请输入 `/opt/kaspersky/klnagent/bin/klnagchk`。

   - “**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 /tmp/klnagchk.log` 参数。此参数指示该工具将结果保存到 `/tmp` 中名为 `klnagchk.log` 的文件。如果需要传递多个参数，请用空格分隔它们。

   - “**工作文件夹路径(可选)**”。用于输入工作目录路径的字段，进程会在该工作目录中放置文件。
     例如，您可以输入 `/tmp`，并使用以下参数运行 `klnagchk` 实用程序：`-logfile klnagchk.log -savecert certificate.cer`。在这种情况下，两个文件均在 `tmp` 中创建。

10. 在任务属性窗口中，选择“**计划**”选项卡。

11. 配置任务计划。

12. 保存更改。

13. 选中该任务旁边的复选框。

14. 单击“**开始**”。

结果，Kaspersky Endpoint Security 在静默模式下运行命令并启动进程。您可以在“**执行结果**”部分的“任务属性”中查看任务结果。

## 终止进程

您可以使用“*终止进程*”任务远程终止进程。例如，您可以远程终止因恶意活动而启动的进程。

如果您要禁止运行一个文件，您可以配置执行防护组件。您可以禁止执行可执行文件、脚本、Office 格式文件。

*如何创建 终止进程 任务*

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

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“**Kaspersky Endpoint Security for Linux**”。

   b. 在“**任务类型**”下拉列表中，选择“*终止进程*”。

   c. 在“**任务名称**”字段中，输入简要说明。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。单击“**下一步**”。

5. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。

6. 单击新任务。

7. 任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 要终止该进程，您必须选择要终止的进程的文件。您可以采用以下方式之一选择文件：

   - 输入文件的全名。
   - 输入文件的哈希值和文件的路径。
   - 输入进程的 PID（仅适用于本地任务）。
   - 如果文件位于网络驱动器上，请输入以“`\\`”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现“*未找到文件*”错误。

10. 在任务属性窗口中，选择“**计划**”选项卡。

11. 配置任务计划。

12. 保存更改。

13. 选中该任务旁边的复选框。

14. 单击“**开始**”。

结果，Kaspersky Endpoint Security 将在计算机上终止该进程。您可以在“**结果**”部分的“任务属性”中查看任务结果。

# 对象的执行防护

在与卡巴斯基 Detection and Response 解决方案集成时，您可以应用此响应操作，Kaspersky Endpoint Security 将从这些解决方案接收执行防护规则。

如果某个对象与规则匹配，Kaspersky Endpoint Security 会阻止执行该对象。

## 对象的执行防护 EDR Expert (on-premises)

与 Kaspersky Endpoint Detection and Response Expert (on-premise)、Kaspersky Endpoint Detection and Response Expert (cloud) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，您可以在相应解决方案的控制台中配置规则，以阻止对象的执行。

如果已启用与 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，您可以在策略属性（**应用程序设置** → **内置代理配置** → **Endpoint Detection and Response Expert (on-premises)**）中启用或禁用对象的执行防护。

要启用对象的执行防护，请将切换开关设置为 **执行防护已启用**。

## 对象的执行防护 (EDR Optimum)

与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以在 Web Console 中配置对象的执行防护和执行防护规则。

**如何在 Kaspersky Security Center 策略中启用对象的执行防护**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。

2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **Endpoint Detection and Response**。

5. 转到“**执行防护**”选项卡。

6. 将切换开关设置为 **执行防护已启用**。

7. 选择启动或打开对象时的操作

   - "**阻止并添加到事件日志**"。应用程序会阻止执行符合防护规则条件的对象或打开符合防护规则条件的文档，并在事件日志中记录有关尝试运行对象或打开文档的事件。

   - "**添加到事件日志**"。应用程序会记录有关尝试运行符合防护规则条件的可执行对象或打开符合防护规则条件的文档的事件，但不会实际阻止其执行或打开。

8. 保存更改。

**如何在受管理设备属性中启用对象的执行防护**

1. 在 Web Console 中，转到 **资产管理 → 资产（设备）**。

2. 单击带有所需设备名称的链接。

3. 这将打开所选设备的属性窗口；在该窗口中，转到 **应用程序** 选项卡，然后单击 <**Kaspersky Endpoint Security** 应用程序名称> 链接。

   1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**策略**"。

   2. 单击 Kaspersky Endpoint Security 策略的名称。

      策略属性窗口将打开。

   3. 选择**应用程序设置**选项卡。

   4. 选择 **内置代理配置 → Endpoint Detection and Response**。

   5. 转到"**执行防护**"选项卡。

   6. 将切换开关设置为 **执行防护已启用**。

   7. 选择启动或打开对象时的操作

      - "**阻止并添加到事件日志**"。应用程序会阻止执行符合防护规则条件的对象或打开符合防护规则条件的文档，并在事件日志中记录有关尝试运行对象或打开文档的事件。

      - "**添加到事件日志**"。应用程序会记录有关尝试运行符合防护规则条件的可执行对象或打开符合防护规则条件的文档的事件，但不会实际阻止其执行或打开。

   8. 保存更改。

4. 选择**应用程序设置**选项卡。

5. 选择 **内置代理配置 → Endpoint Detection and Response**。

6. 转到 **执行防护** 子部分。

7. 将切换开关设置为 **执行防护已启用**。

8. 选择对象的执行防护模式：

   - **阻止**。在此模式下，应用程序会阻止执行符合预防规则标准的对象或打开文档，并在事件日志中记录有关尝试运行对象或打开文档的事件。
   - **通知**。在这种模式下，应用程序会在事件日志中记录有关尝试运行可执行对象或打开满足预防规则标准的文档的事件，但实际上并不会阻止它们的执行或打开。默认情况下已选择此模式。

9. 保存更改。

如果将策略应用于设备，则无法在设备属性中启用或禁用对象执行防护。

**如何在 Web Console 中添加 EDR Optimum 组件的对象的执行防护规则**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 如有必要，选中“**使用区分大小写的路径**”复选框。
5. 在策略或受管理设备的属性中，单击对象的执行防护规则列表上方工具栏中的 **添加** 按钮。
6. 这将打开一个窗口；在该窗口中，输入执行防护规则的名称。
7. 通过将开关设置到相应位置来指定执行防护规则的状态。
8. 在 **类型** 下拉列表中，选择要阻止的对象类型：

   - “**可执行文件**”。
   - “**脚本**”。
   - “Office **应用程序文件**”。

   如果选择了错误的对象类型，应用程序将无法阻止该文件或脚本。

9. 要添加对象，请在相应字段中指定对象路径和/或对象的校验和（文件的 SHA256 或 MD5 哈希值）。
10. 保存更改。
    创建的规则将被添加到**对象的执行防护**设置块的规则列表中。

Kaspersky Endpoint Security 控制设备上可执行文件和脚本的执行，以及办公应用程序文件的打开。对象的执行防护支持特定的一组办公应用程序文件扩展名和特定的一组脚本解释器。通过阻止启动对象，您可以阻止威胁蔓延。

如果满足以下条件之一，则 Kaspersky Endpoint Security 应用程序中可使用执行防护功能：

- 与 Kaspersky Endpoint Detection and Response Optimum 解决方案的集成已启用，并且 EDR Optimum 组件已激活。
- 已启用与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 组件 的集成，并且 EDR Expert (on-premises) 组件已激活。
- 已启用与 Kaspersky Endpoint Detection and Response Expert (cloud) 的集成，并且 EDR Expert (cloud) 组件已激活。

如果未启用文件操作拦截的阻止模式，则对象执行防护功能将以通知模式运行，与配置的运行模式无关。

默认情况下，对象的执行防护被禁用。启用对象的执行防护可能会影响操作系统中应用程序的启动速度。

为确保对象执行防护功能生效，您需要启用执行防护规则。

对象执行防护的限制和特殊注意事项

**对象的执行防护的限制**

对象的执行防护规则存在以下限制：

- Kaspersky Endpoint Security 应用程序在应用程序启动之前不会阻止执行防护规则中指定的对象。
- Kaspersky Endpoint Security 应用程序不会阻止在创建或修改预防规则之前打开的文件。
- Kaspersky Endpoint Security 应用程序不会阻止在创建或修改执行防护规则以覆盖这些对象之前执行的执行防护规则所涵盖的对象。
- 某些文件可能对于操作系统和应用程序的运行至关重要。阻止此类文件的执行可能会扰乱系统运行。

我们建议创建不超过 50000 条执行防护规则，因为这可能会导致系统不稳定。

**与 Kaspersky Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response (KATA) 集成时对象执行防护涉及的特殊注意事项**

当 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，该应用程序将使用 *EDR Expert (on-premises) 组件的执行防护规则*。应用程序会从 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 获取这些规则。

当与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，您可以：

- 在 Web Console 或管理控制台中启用或禁用 EDR Expert (on-premises) 组件的对象执行防护规则的应用。

  当执行防护规则被触发时，Kaspersky Endpoint Security 会向 Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Anti Targeted Attack Platform 发送报告。有关详细信息，请参阅相关解决方案的帮助文档。
- 在命令行中查看 EDR Expert (on-premises) 组件的对象执行防护规则列表。

### 与 Kaspersky Endpoint Detection and Response Optimum 集成时对象执行防护的特殊注意事项

当 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 解决方案集成时，应用程序将使用 *EDR Optimum 组件的对象执行防护规则*。您可以在 Web Console 中手动创建这些规则。您还可以在警报详情窗口中自动创建执行防护规则。

与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以：

- 在 Web Console 中启用或禁用 EDR Optimum 组件的对象执行防护规则的应用。
- 在 Web Console 中为对象创建和配置 EDR Optimum 执行防护规则。

  您还可以通过在警报详情窗口中阻止文件执行来自动为对象创建执行防护规则。执行防护规则被添加到设备所属管理组的策略中。

  > 仅当策略应用于设备时，您才可以在警报详情窗口中阻止文件的执行。

- 在命令行上查看 EDR Optimum 组件的对象执行防护规则列表。

与 Kaspersky Endpoint Detection and Response Optimum 集成时，对象执行防护可以采用以下两种模式之一运行：

- **阻止**。在此模式下，应用程序会阻止执行符合预防规则标准的对象或打开文档，并记录有关尝试运行对象或打开文档的事件。

  > Kaspersky Endpoint Security 应用程序会阻止执行被运行预防规则禁止的脚本，即使该脚本由允许的脚本导入。

- **通知**。在这种模式下，应用程序会记录有关尝试运行可执行对象或打开满足预防规则标准的文档的事件，但实际上并不会阻止它们的执行或打开。默认情况下已选择此模式。

## 管理隔离区

*隔离区*是设备上的一个特殊存储区，用于存储可能感染病毒或被检测到但无法清除的文件。隔离区用于隔离文件以待进一步调查。隔离的文件以加密形式存储，不会威胁设备的安全。与隔离区相反，备份区存储在清除过程中检测到恶意代码并被删除或修改的文件的备份副本。

该应用程序仅在与 Detection and Response 解决方案集成时使用隔离区来执行建议的威胁响应操作。当应用程序与 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Managed Detection and Response 集成时，您还可以手动隔离您认为会危害设备安全的文件。

默认情况下，/var/opt/kaspersky/kesl/common/objects-backup/ 目录用于存储被隔离文件。该目录还包含备份对象。您可以使用命令行更改存储备份和隔离对象的目录。

被隔离的文件可能包含个人数据。访问被隔离文件需要 root 特权。

您可以在 Web Console 或 管理控制台 中使用策略，或使用 命令行在设备上配置隔离区设置。您还可以配置以下隔离区设置：

- 隔离区百分比，百分比必须达到 100% 才会生成隔离区已满的事件。默认情况下，当隔离区已满 90% 时，就会生成事件。
- 隔离区的最大大小（以兆字节为单位）。当达到最大隔离区大小时，应用程序会自动删除掉最旧的隔离文件。默认情况下，如果应用程序在标准模式或 EDR Agent 模式下使用，则隔离区的最大大小为 200 MB；如果应用程序在 Light Agent 模式下使用，则为 100 MB。
- 存储备份和隔离对象的目录路径（只能在命令行上配置）。

**如何在 Web Console 中管理隔离区设置**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **报告和存储**。
5. 在 **隔离** 部分中，配置以下设置：
   - “**限制隔离区大小**”。将隔离区限制为指定大小（以兆字节为单位）。默认情况下已选定该选框。
   - “**隔离区最大大小(MB)**”。如果启用 **限制隔离区大小** 设置，您可以指定隔离区的最大大小（以兆字节为单位，默认为 200 MB）。隔离区大小不得超过 999,999 MB。
   - “**隔离区已满时通知**”。隔离区达到此占用百分比时的通知。默认情况下已选定该选框。
     您可以指定达到哪个百分比后发送通知（默认为 90%）。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

隔离文件

某些文件可能对于操作系统和应用程序的运行至关重要。隔离此类文件可能会扰乱系统的运行。

仅当满足以下条件之一时，才可以将文件置于隔离区：

- 已启用 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 的集成，并且已激活 EDR Optimum 组件。
- 已启用 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，并且已激活 EDR Expert (on-premises) 组件。
- 已启用 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 的集成，并且已激活 MDR 组件。

存储隔离对象的目录必须可写。

当与 Kaspersky Endpoint Detection and Response (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，可以通过以下方式之一将文件隔离：

- 通过在 Detection and Response 解决方案侧配置的任务。有关详情，请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助 或 Kaspersky Anti Targeted Attack Platform 帮助。
- 因对进程内存执行 IOC 扫描任务而被隔离。

与 Kaspersky Managed Detection and Response 集成时，文件将通过以下方式之一被隔离：

- 由于执行在 Kaspersky Managed Detection and Response 端配置的任务。
- 由于在设备上执行管理隔离区的命令。

有关与 Kaspersky Endpoint Detection and Response Optimum 集成时使用隔离区的更多信息，请参阅 Kaspersky Endpoint Detection and Response 帮助。

与 Kaspersky Endpoint Detection and Response 集成时，文件将通过以下方式之一被隔离：

- 由于检测到入侵指标自动执行。
- 作为*隔离*任务的结果，您可以在Web 控制台中创建该任务。
- 由于在设备上执行管理隔离区的命令。
- 因遵循警报详情中的建议而被隔离。

有关与 Kaspersky Endpoint Detection and Response Optimum 集成时管理隔离区的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

管理隔离文件

您可以管理隔离文件：

- 在 Kaspersky Security Center 中，在由卡巴斯基应用程序隔离的文件通用列表中。

  要在 Kaspersky Security Center 中管理隔离文件，您需要启用将隔离文件的数据传输到管理服务器的功能。

- 在设备本地使用命令行。

您可以查看有关隔离文件的信息，以及删除和恢复隔离区中的文件。

无论是否启用与 Detection and Response 解决方案的整合，也无论是否将策略应用于设备，都可以从隔离区中恢复、删除和检索文件。

客户端设备上卡巴斯基应用程序隔离的文件的常规列表保存在 Kaspersky Security Center 中，可在管理控制台（**高级 →存储库→隔离区**）和 Web Console（**操作 →存储库→隔离区**）中获取。Kaspersky Security Center 不会将文件从隔离区存储复制到管理服务器；所有文件都存储在客户端设备上的隔离区存储中。有关在 Kaspersky Security Center 中管理隔离文件的详细信息，请参阅 Kaspersky Security Center 帮助。

隔离的文件将根据指定设置被恢复到其原始位置。恢复操作会保留 MAC 标签（仅限 Astra Linux 设备）和原始文件的属性（包括不可变属性和仅追加属性）。具有不可变和仅追加属性的文件只有在原始文件不存在时才能恢复到该位置，或者恢复到原始位置，但使用不同的名称。要将文件从隔离区恢复到不同的目录或使用不同的名称恢复到原始位置，需要 root 权限。

恢复过程完成后，应用程序将删除恢复文件的隔离副本。

在以下情况下，从隔离区恢复文件会失败：

- 在隔离存储中未找到要恢复的文件。
- 正在恢复的文件的名称指定不正确或大小写错误。
- 文件 ID 指定不正确。
- 目标目录已被删除、移动、重命名，或者您没有目录的访问权限。

  在这种情况下，应用程序将文件移动到 /var/opt/kaspersky/kesl/common/restored/ 目录。您可以手动将文件从该目录移动到您选择的目录。
- 指定路径下已存在同名文件。
- 设备没有足够的空间。
- 仅在 Astra Linux 设备上：文件的 MAC 标签高于要将文件恢复到的目录的 MAC 标签。
- 仅在 Astra Linux 设备上：文件的 MAC 标签低于要将文件恢复到的目录的 MAC 标签，并且未为此目录设置 ccnr 标志。

在下列情况下，从隔离区删除文件会失败：

- 在隔离存储中未找到要删除的文件。
- 被删除的文件的名称指定不正确或大小写错误。
- 文件 ID 指定不正确。

# Endpoint Detection and Response Optimum

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 Security 12.5 for Linux 与 Kaspersky Endpoint Detection and Response Optimum 版本 3.1 兼容。

Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 解决方案的整合由 Kaspersky Endpoint Security 组件 Endpoint Detection and Response Optimum (*EDR Optimum*) 得到促进。

要使用 EDR Optimum 组件集中管理 Kaspersky Endpoint Security 应用程序，请使用 Kaspersky Security Center Windows 15.1 或 Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2。

该组件不适用于配备 Elbrus CPU 的设备。

## Kaspersky Endpoint Detection and Response Optimum 的工作原理

Kaspersky Endpoint Detection and Response Optimum 可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，帮助他们及时执行威胁响应操作。

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 的命令时执行威胁响应操作以维护安全。

配置 Kaspersky Endpoint Detection and Response Optimum 集成

**先决条件**

配置 Kaspersky Endpoint Detection and Response Optimum 集成之前：

- 如果您购买了单独的授权许可来使用此功能，请将 EDR Optimum 授权许可密钥添加到应用程序。

  如果您使用的 Kaspersky Endpoint Security 授权许可包含 Kaspersky Endpoint Detection and Response Optimum，则无需执行任何操作。

  > 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，则授权许可密钥将添加到 SVM。

- 请确保已启用以下项并且其正常运行：

  - 卡巴斯基安全网络（标准模式或扩展模式）：

    > 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。

  - Kaspersky Endpoint Security 应用程序的以下组件：

    - 文件威胁防护。
    - 行为检测。

  为了确保遥测数据完整，并在 Kaspersky Security Center 中构建威胁发展链，您还需要启用 Web 威胁防护。

  您还可以启用对象的执行防护。

**基本配置步骤**

1. **安装 Kaspersky Endpoint Detection and Response Optimum 管理插件**

   Kaspersky Endpoint Detection and Response Optimum 管理插件是管理 Windows、Mac 和 Linux 操作系统上的代理的统一插件；该插件对于显示警报和查看警报详细信息必不可少。有关安装过程的说明，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

   如果您的基础设施使用 Kaspersky Security Center 云控制台 来管理 Kaspersky Endpoint Detection and Response Optimum，则默认安装该插件。

2. **配置 Kaspersky Endpoint Detection and Response Optimum 集成设置**

   您可以通过以下方式进行配置：

   - 使用 Web Console（Kaspersky Security Center 控制台和/或 OSMP 控制台）。
   - 使用命令行。

     > 不支持使用 Kaspersky Security Center 管理控制台管理 EDR Optimum 组件。

3. **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，您必须配置以下内容：

- 启用将备份和隔离区中的文件信息发送到Kaspersky Security Center 存储。为此，您需要在策略属性中选中以下复选框：
  - **关于备份区中的文件**
  - **关于隔离区中的文件**
- 允许显示警报列表 为此，您可以在 Kaspersky Security Center Web Console 主窗口的**设置→界面设置**下启用**显示 EDR 警报**拨动开关。

  在 15.1 之前的 Web Console 版本中不提供**"显示 EDR 警报"**设置。在 Kaspersky Security Center 控制台中，您可以从"威胁报告"导航到 EDR 警报。
- 启用传输受管理设备上第三方应用程序事件相关信息。为此，请在受管理设备上运行以下命令：

  ```
  kesl-control --set-app-settings SystemEventsTransmission=Yes
  ```

  启用此设置可能会显著增加操作系统负载。

4. **确保已成功建立与 Kaspersky Endpoint Detection and Response Optimum 的连接**

   检查 Kaspersky Endpoint Detection and Response Optimum 的状态以任何方便的方式。
Kaspersky Endpoint Detection and Response Optimum 集成已配置。检测到威胁时，会生成警报。在警报详情窗口中，您可以查看有关威胁的信息并执行响应操作。

# 如何启用 EDR Optimum 集成

在 Web Console 中，您可以在策略属性中启用或禁用 EDR Optimum 组件，并配置与 Kaspersky Endpoint Detection and Response Optimum 的集成。

**如何在 Web Console 中启用 Kaspersky Endpoint Detection and Response Optimum 集成**

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**策略**"选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 启用 **Endpoint Detection and Response 已启用** 切换开关。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行上启用 Kaspersky Endpoint Detection and Response Optimum 集成**

要启用 EDR Optimum 组件，请运行以下命令：

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

1. 在 Web Console 主窗口中，选择 **资产管理** → **资产（设备）** 部分。
2. 单击带有所需设备名称的链接。
3. 这将打开所选设备的属性窗口；在该窗口中，转到 **应用程序** 选项卡，然后单击 <Kaspersky Endpoint Security application name> 链接。
4. 转到 **应用程序设置** 选项卡，单击 **检测和响应** 区域，然后单击 **Endpoint Detection and Response Optimum** 链接。
5. 这将打开一个窗口；在该窗口中，将切换开关设置为 **Endpoint Detection and Response Optimum 已启用** 以启用集成。
6. 如有必要，请管理以下设置：
   - 自动网络隔离过程中设备被阻止的持续时间。
     单击 **配置设备解除阻止** 链接并指定阻止时间。
   - 自动网络隔离排除项
7. 保存更改。

受管理设备已配置为与 Kaspersky Endpoint Detection and Response Optimum 集成。

## 如何验证 EDR Optimum 集成是否正常运行

阅读有关可能的集成状态及其显示时间的信息。

您可以通过以下方式测试 EDR Optimum 组件：

- 在命令行中使用以下 命令：

  ```
  kesl-control --app-info
  ```

  EDR Optimum 集成显示为 **正在运行** 状态。

- 在 Web Console 中：
  - 使用 *有关应用程序组件状态的报告*。有关报告的详细信息，请参阅“Kaspersky Security Center 帮助”。
  - 转到 **资产管理** → **资产** 部分 → <设备名称> 链接 → **应用程序** 选项卡 → <Kaspersky Endpoint Security 应用程序名称> 链接 → **常规** 选项卡 → **组件**。
    Endpoint Detection and Response Optimum 组件显示为 **正在运行** 状态。

## Cloud Sandbox

*Cloud Sandbox* 是一种可以让您检测计算机上的高级威胁的技术。Kaspersky Endpoint Security 自动将检测到的文件转发到 Cloud Sandbox 进行分析。Cloud Sandbox 在隔离环境中运行这些文件以检测恶意活动并确定这些文件的信誉。这些文件上的数据随后被发送到卡巴斯基安全网络。因此，如果 Cloud Sandbox 检测到恶意文件，Kaspersky Endpoint Security 将在检测到此文件的所有计算机上执行适当的操作以消除此威胁。

要运行 Cloud Sandbox，您必须启用卡巴斯基安全网络。

如果您使用卡巴斯基私人安全网络，则 Cloud Sandbox 技术不可用。

Cloud Sandbox 技术始终处于启用状态，可供卡巴斯基安全网络的所有用户使用，无论授权许可类型如何。如果您已经部署了 Endpoint Detection and Response Optimum 解决方案，您可以为 Cloud Sandbox 检测到的威胁启用单独的计数器。您可以使用此计数器在分析检测到的威胁时汇总统计信息。Kaspersky Endpoint Security 会在 Kaspersky Security Center 控制台的 *威胁报告* 中指示 Cloud Sandbox 威胁检测技术。

*如何在 Web Console 中启用 Cloud Sandbox 计数器*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 选择**Cloud Sandbox**选项卡。
6. 启用 **Cloud Sandbox 已启用** 切换开关。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

# Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Detection and Response Expert (on-premises) 是一款企业级网络安全解决方案，能够防御大多数网络安全风险，并涵盖威胁传播的主要场景。Kaspersky Endpoint Detection and Response Expert (on-premises) 的组件部署在 Open Single Management Platform (OSMP) 上。有关该解决方案和平台的更多信息，请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助。

与 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案的集成由 Kaspersky Endpoint Security 应用程序组件 Endpoint Detection and Response Expert (on-premises)（以下简称 *EDR Expert (on-premises)*）提供。

该组件不适用于配备 Elbrus CPU 的设备。

Endpoint Detection and Response Expert (on-premises) 的工作原理

1. **安装了 Kaspersky Endpoint Security 的设备与 OSMP 威胁响应操作服务器和 OSMP 遥测收集服务器建立安全连接**
2. **Kaspersky Endpoint Security 将数据发送到 OSMP 平台上的遥测收集服务器**

   传输以下信息：

   - 设备上的事件信息
   - 应用程序检测到的威胁信息
   - 处理这些威胁的结果信息
   - 进程、开放的网络连接和已修改文件的监控数据
3. **Kaspersky Endpoint Security 执行威胁响应操作**

   响应操作根据 OSMP 平台上的威胁响应操作服务器发出的命令执行。

配置 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成

**先决条件**

在配置与 Kaspersky Endpoint Detection and Response Expert (on-premises) 的集成之前：

- 允许在端口 443 和 8443 上连接。
- 启用 行为检测 组件以传输必要的遥测数据。

  如果要获取其他保护组件检测到的威胁信息，请启用以下组件：

  - 文件威胁防护。
  - 网络威胁防护。
  - Web 威胁防护。
  - 反加密勒索。
  - 应用程序控制。
  - 设备控制。
  - 系统完整性监控。

  如果行为检测使用 eBPF 机制获取系统遥测数据（在内核版本 4.18 及更高版本且支持 eBPF 的 64 位操作系统上可用），则遥测数据更加全面。

- 如果您已购买单独的授权许可来使用此功能，请将 EDR Expert (on-premises) 授权许可密钥添加到应用程序中。

  如果您使用的 Kaspersky Endpoint Security 授权许可包含 Kaspersky Endpoint Detection and Response Expert (on-premises)，则无需执行任何操作。

  如果应用程序在 Light Agent 模式下使用，则会将 EDR Expert (on-premises) 授权许可密钥添加到 SVM。

- 此外，您还需要在 OSMP 平台上配置收集器、关联器和存储。

**基本配置步骤**

1. **获取并处理 OSMP 服务器颁发的证书**

   与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成时，运行 Kaspersky Endpoint Security 的设备会与 OSMP 威胁响应服务器和 OSMP 遥测服务器建立加密的 HTTPS 连接。

   > 如果在 Kaspersky Endpoint Security 应用程序的常规设置中配置了使用代理服务器，则代理服务器将用于连接到 OSMP 服务器。

   用于保护与 OSMP 服务器连接的证书必须由 OSMP 平台管理员提供。

   要处理证书，请按照 将 PFX 证书转换为 PEM 格式一文中所述步骤操作。

   您可以使用服务器证书和/或客户端证书。选择取决于贵组织的安全策略。

2. **配置 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成设置**

   您可以通过以下方式进行配置：

   - 使用 Web Console（Kaspersky Security Center 控制台和/或 OSMP 控制台）。
   - 使用命令行。

   如果您想对对象使用执行防护，可以启用 EDR Expert (on-premises) 组件的对象执行防护规则。

3. **确认已成功建立与 Endpoint Detection and Response Expert (on-premises) 平台的连接**

   使用任何方便的方式检查 EDR Expert (on-premises) 的状态。

4. **必要时管理其他设置**

   - 如果您的操作系统上的 SELinux 配置为 Enforcing 模式，则需要额外配置 SELinux以执行响应操作。
   - 要执行**内存转储**或**进程转储**响应操作，请解除 ptrace 阻止。
   - 查看网络隔离的限制。
   - 启用传输受管理设备上第三方应用程序事件相关信息。为此，请在受管理设备上运行以下命令：

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     > 启用此设置可能会显著增加操作系统负载。

# 如何准备用于与 EDR Expert (on-premises) 正确集成的参考镜像

在准备映像之前，请确保参考设备上不存在 `/var/opt/kaspersky/.ids_generated` 文件。

*要准备用于与 Kaspersky Endpoint Detection and Response Expert (on-premises) 正确集成的参考镜像：*

按照这些说明操作时，请勿重启参考设备或重新启动 Kaspersky Endpoint Security 应用程序。

1. 以 root 用户身份运行以下命令：

   ```
   systemctl stop kesl
   systemctl edit kesl
   ```

2. 在编辑器中，在 `### Anything between here and the comment below will become the contents of the drop-in file` 和 `### Edits below this comment will be discarded` 两行之间添加以下配置之一：

   - 每次在临时虚拟机上启动应用程序时更新 SensorID

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -a
     ```

   - 仅在持久性虚拟机上更新一次 SensorID

     ```
     [Service]
     ExecStartPre=-/usr/bin/uuid-regen.sh -b
     ```

3. 保存更改并关闭编辑器。

   已创建 `/etc/systemd/system/kesl.d/override.conf` 文件。检查其内容，确保其与添加的配置相符。

4. 运行以下命令重新加载 systemd 服务：

   ```
   systemctl daemon-reload
   ```

5. 创建包含以下内容的 `/usr/bin/uuid-regen.sh` 文件：

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ------------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode -------------------------------------------------
MODE="a"
# ----- parse command-line arguments ---------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file --------------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini ------------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ---------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. 使用以下命令更改 `/usr/bin/uuid-regen.sh` 文件的权限：

```
chmod 700 /usr/bin/uuid-regen.sh
```

参考设备现已准备就绪，可以创建操作系统镜像。

# 如何配置 EDR Expert (on-premises) 集成

在 Web Console 中，您可以启用或禁用 EDR Expert (on-premises) 组件，并在 Kaspersky Endpoint Security 策略属性中配置 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Expert (on-premises) 的集成。

**如何在 Web Console 中配置 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premises)**。
5. 选择 **Endpoint Detection and Response Expert 版本 8.0 或更高版本** 选项。
6. 添加遥测采集服务器和响应服务器。
   为此，在 **连接到遥测采集服务器** 和 **连接到威胁响应服务器** 部分中，单击 **添加** 按钮。在打开的窗口中，指定服务器地址（IPv4、IPv6）和用于连接到服务器的端口。
7. 通过单击 **连接到遥测采集服务器** 和 **连接到威胁响应服务器** 部分中的 **连接设置** 链接来添加证书；然后在显示的窗格中执行以下操作：
   a. 通过单击相应部分中的 **上传** 按钮来添加服务器证书。
   b. 如果需要额外保护，请创建加密容器。
      为此，请在 **附加连接保护** 部分中执行以下操作：
      1. 选中 **使用双向身份验证** 复选框。
      2. 单击 **上传** 按钮，并添加您在完成 主要集成场景 时收到的客户端证书。
      3. 在相应字段中输入加密容器的密码。

      > **加密容器密码** 字段为必填字段。不输入客户端证书（加密容器）的密码，就无法保存设置。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中配置 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成**

1. 要添加响应服务器证书，请运行以下命令：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

2. 要添加遥测服务器证书，请运行以下命令：

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

3. 要配置集成设置，请运行以下命令：

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

设置及其可能的值列于下表中。

4. 要添加用于连接到响应服务器的客户端证书，请运行以下命令：

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
```

5. 要添加用于连接到遥测服务器的客户端证书，请运行以下命令：

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

6. 要启用与 EDR Expert (on-premises) 的集成，请运行以下命令：

```
kesl-control --start-task 24
```

Kaspersky Endpoint Detection and Response Expert (on-premises) 整合设置

| 设置 | 描述 | 值 |
|---|---|---|
| `Mode` | 集成模式。<br>对于 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，Kaspersky Endpoint Security 应用程序会与 OSMP 平台上的服务器交互。<br>对于 Kaspersky Endpoint Detection and Response (KATA) 集成，Kaspersky Endpoint Security 应用程序与 Kaspersky Anti Targeted Attack Platform 上的服务器进行交互。 | `EDRKATA`（默认）是 EDR (KATA) 集成模式。允许启用与 Kaspersky Endpoint Detection and Response (KATA) 进行集成，这是 Kaspersky Anti Targeted Attack Platform 的一个组件。<br>`EDRExpertOnPrem` 是 EDR Expert (on-premises) 集成模式。启用 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成 |
| `UseClientPinnedCertificate` | 启用或禁用双向身份验证，以增强与 OSMP 威胁响应操作服务器连接的安全性。<br>如果在 OSMP 威胁响应服务器端启用了双向身份验证，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 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` 启用双向身份验证，以增强与 OSMP 威胁响应操作服务器连接的安全性。<br>`No`（默认值）— 不使用双向身份验证。 |
| `SynchronizationPeriod` | 向 OSMP 威胁响应操作服务器发送同步请求的周期（以分钟为单位）。 | 默认值：`5`。 |
| `ConnectionTimeout` | 等待连接到 OSMP 威胁响应操作服务器的最长时间（以秒钟为单位）。 | 默认值：`10`。 |
| `RequestTimeout` | 等待 OSMP 威胁响应操作服务器响应的最长时间（以秒钟为单位）。 | 默认值：`10`。 |
| `EnableTelemetry` | 将设备上的事件数据（遥测）发送到 OSMP 遥测收集服务器。 | `Yes`（默认值）启用向 OSMP 遥测服务器发送遥测数据。<br>`No`禁用传送遥测数据。 |
| **[Endpoints.item_#]** 部分包含 OSMP 威胁响应操作服务器的地址和端口。您可以添加多台服务器。 | | |
| `Address` | OSMP 威胁响应操作服务器地址。<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>为确保在设备上启用网络隔离的情况下应用程序发生故障时与服务器的通信不会中断，我们建议指定服务器的 IP 地址。 | 默认值：`127.0.0.1`。 |
| `Port` | 用于连接到 OSMP 威胁响应服务器的端口。 | 默认值：`443`。 |
| **[TelemetrySettings]**部分包含用于连接到 OSMP 遥测服务器的常规设置。 | | |
| `UseClientPinnedCertificate` | 启用或禁用双向身份验证，以增强与 OSMP 遥测服务器连接的安全性。<br>如果在 OSMP 遥测服务器端启用了双向身份验证，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 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` 启用双向身份验证，以增强与 OSMP 遥测服务器连接的安全性。<br>`No`（默认值）— 不使用双向身份验证。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ConnectionTimeout | 等待连接到 OSMP 遥测服务器的最长时间（以秒钟为单位）。 | 默认值：10。 |
| RequestTimeout | 等待 OSMP 遥测服务器响应的最长时间（以秒钟为单位）。 | 默认值：10。 |
| OnlyTaggedEvents | 仅发送包含 IOA 的遥测。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。 | Yes — 仅发送包含攻击指标 (IOA) 的遥测数据。<br>No（默认值）— 发送所有遥测数据。 |
| **[TelemetrySettings.Endpoints.item_#]**部分包含 OSMP 遥测服务器的地址和端口。您可以添加多台服务器。 | | |
| Address | OSMP 遥测服务器证书地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>为确保在设备上启用网络隔离的情况下应用程序发生故障时与服务器的通信不会中断，我们建议指定服务器的 IP 地址。 | 默认值：127.0.0.1。 |
| Port | 用于连接到 OSMP 遥测服务器的端口。 | 默认值：443。 |
| **[TelemetrySettings.EventTransferSettings]**部分包含用于向 OSMP 遥测服务器传输数据的设置。 | | |
| MaximumDataTransferTime | 向 OSMP 遥测服务器发送事件的最大延迟（以秒钟为单位）。 | 默认值：30。 |
| UseRequestCountLimits | 限制请求数量。该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制传输的事件。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。 | Yes（默认值）– 调节发送的事件数。<br>No – 不调节事件数。 |
| MaximumNumberOfEventsInHour | 每小时的最大事件数量 | 默认值：3000。 |
| MaximumNumberOfEventsInPackage | 一个数据包中的最大事件数量。 | 默认值：1024。 |
| EventLimitExceededPercentage | 事件数量超过限制（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：15。 |

对于 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的设置，层次结构中的嵌套策略允许指定独立值，即使所有其他策略设置都是继承的。

如果在父策略中启用了 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，并且在子策略中启用了设置继承，则默认情况下，子策略的集成设置也会被继承，并且无法更改。如果要配置独立的集成设置，请从下拉列表中选择 **使用自定义连接设置**。这样就可以编辑 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成设置了。

如果使用 Web Console 或命令行，要与 Kaspersky Endpoint Detection and Response (on-premises) 集成，您需要在 EDR Expert (on-premises) 组件的设置中选择 EDR (on-premises) 集成模式：

- 如果您使用的是 Web Console，请在策略设置中选择**Endpoint Detection and Response Expert（版本 8.0 或更高版本）** 。要在设备上配置与 Kaspersky Endpoint Detection and Response (on-premises) 的集成，您需要在 Web Console 中针对任一版本（版本 8.0 及更高版本和版本 7.1 及更早版本）管理“挂锁”。
- 如果您使用命令行，请在任务设置中设置Mode=EDRExpertOnPrem。

## 如何验证 EDR Expert (on-premises) 集成已启动并正在运行

如何测试 EDR Expert (on-premises) 组件：

- 在命令行中使用以下 命令：

```
kesl-control --app-info
```

- 在 Web Console 中。
  - 在 Kaspersky Security Center 控制台中：
    使用 *有关应用程序组件状态的报告*。有关报告的详细信息，请参阅“Kaspersky Security Center 帮助”。
  - 在 OSMP 控制台中：
    - 使用 *有关应用程序组件状态的报告*。
    - 转到 **资产管理** → **资产** 区域，然后选择 **分析和响应** 选项卡。
      该设备会显示在列表中，遥测状态为 **正常活动**。
    - 转到 **威胁搜索** 区域。
      来自该设备的遥测事件会显示在事件列表中。

# Endpoint Detection and Response Expert (cloud)

Kaspersky Endpoint Security for Linux 与 Kaspersky Endpoint Detection and Response Expert (cloud) 的集成暂时不可用。计划在 2026 年底之前支持此功能。请关注我们的发行说明，以了解应用程序升级和新功能。

Kaspersky Endpoint Security for Linux 支持与 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案集成。*Kaspersky Endpoint Detection and Response Expert (cloud)* 是一款基于云的企业网络安全解决方案，其中包括卡巴斯基应用程序，可帮助组织防御大多数类型的网络风险并涵盖最重要的威胁传播场景。EDR Expert (cloud) 组件部署在 Open Single Management Platform (OSMP) 上。该平台可在单一界面中运行跨平台方案，并允许将卡巴斯基应用程序与第三方应用程序集成到全面的安全系统中。

解决方案的核心要素之一是 *SIEM*。SIEM 跟踪来自所有组件的事件，并使用供应商和用户定义的规则将这些事件相互关联起来。EDR Expert (cloud) 会查看从企业基础设施接收的日志和遥测数据，以自动检测攻击，并允许使用统一的调查图来调查事件，该调查图结合了 EDR Expert (cloud) 中采集的所有事件，包括来自卡巴斯基应用程序和第三方信息安全产品的事件。

对于高级事件的响应，EDR Expert (cloud) 使用预设方案和用户自定义方案。您还可以使用来自第三方应用程序的响应操作以及涉及多个应用程序的响应方案。

### 威胁情报工具

Kaspersky Endpoint Detection and Response 使用以下 Threat Intelligence 工具：

- 与卡巴斯基威胁情报门户集成，该系统包含并显示有关文件和网址信誉的信息。
- 卡巴斯基威胁数据库。
- 卡巴斯基安全网络（以下也称为"KSN"）云服务基础设施，提供对 Kaspersky 知识库中实时文件、网站和软件信誉信息的访问。使用卡巴斯基安全网络的数据可确保 Kaspersky 应用程序能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。

### 解决方案的工作原理

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。

计算机事件信息（遥测数据）被发送到 EDR Expert (cloud) 服务器。在这种情况下，Kaspersky Endpoint Security 还会将应用程序发现的威胁信息以及这些威胁的处理结果信息发送到遥测采集服务器。

EDR Expert (cloud) 集成在 Kaspersky Security Center 控制台中配置。然后使用 Open Single Management Platform (OSMP) 管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

### EDR Expert (cloud) 的限制

- Kaspersky Endpoint Security 在 Light Agent 模式下不支持与 EDR Expert (cloud) 集成。
- EDR Expert (cloud) 不适用于配备 Elbrus CPU 的设备。
- EDR Expert (cloud) 不支持基于 Arm 架构的设备。
- EDR Expert (cloud) 不适用于运行 64 位操作系统的计算机。

## 如何配置内置代理与 EDR Expert (cloud) 的集成

要与 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案集成，您需要启用 Endpoint Detection and Response Expert (cloud) 组件，并配置与遥测采集服务器和响应服务器的连接。

*遥测采集服务器* 是 SIEM 解决方案的一部分，用于收集、规范化、关联、分析和存储有关计算机上发生的事件的信息。

*响应服务器* 是一个用于接收和扫描数据、研究对象行为和发布此类研究结果的服务器。

> *Endpoint Detection and Response (cloud)* 和 *Endpoint Detection and Response Expert (on-premises)* 组件彼此不兼容。

EDR Expert (cloud) 运行条件

要使 EDR Expert (cloud) 正常工作，必须满足以下条件：

- Kaspersky Endpoint Detection and Response Expert (cloud) 基础设施已在您所在的地区推出。如需了解您所在地区 EDR Expert (cloud) 基础设施的可用性信息，请联系技术支持。
- OSMP（Open Single Management Platform 已安装。
- Kaspersky Endpoint Security 以标准模式安装。
- Kaspersky Endpoint Security 应用程序已激活，授权许可涵盖了该功能。
- 您已接受 Kaspersky Endpoint Detection and Response Expert (cloud) 数据处理协议的条款。
- “Endpoint Detection and Response Expert (cloud)”组件已启用。
- 用于传输必要遥测数据的 行为检测 组件已启用。
  如果要获取其他保护组件检测到的威胁信息，请启用以下组件：
  - 文件威胁防护。
  - 网络威胁防护。
  - Web 威胁防护。
  - 反加密勒索。
  - 应用程序控制。
  - 设备控制。
  - 系统完整性监控。

与 EDR Expert (cloud) 集成的步骤

设置 EDR Expert (cloud) 集成涉及以下步骤：

1. **选择 EDR Expert 模式**

   Kaspersky Endpoint Security 支持两种 EDR Expert 模式：本地部署和云。要与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成，您需要在安装应用程序期间启用相应模式。默认情况下，应用程序使用 Endpoint Detection and Response Expert (on-premises) 集成。

2. **激活 Kaspersky Endpoint Detection and Response Expert (cloud)**

   您需要为 Kaspersky Endpoint Detection and Response Expert (cloud) 购买单独的授权许可。

   该功能将在为 Kaspersky Endpoint Detection and Response Expert (cloud) 添加单独密钥后可用。因此，计算机上将添加两个密钥：Kaspersky Endpoint Security 密钥和 Kaspersky Endpoint Detection and Response Expert (cloud) 密钥。

   独立 Endpoint Detection and Response Expert (cloud) 功能的授权许可与 Kaspersky Endpoint Security 的相同。

确保您的授权许可涵盖 EDR Expert (cloud) 功能，并且该功能可在 Kaspersky Security Center 中或受保护设备上运行。

### 3 配置与遥测采集服务器和响应服务器的连接

Kaspersky Endpoint Detection and Response Expert (cloud) 要求在 Kaspersky Endpoint Security 与两台服务器（遥测采集服务器和响应服务器）之间建立可信连接。接受 Kaspersky Endpoint Detection and Response Expert (cloud) 数据处理协议的条款和条件后，应用程序会自动接收用于建立可信连接的服务器地址和证书。因此，您只需管理用于连接到服务器的高级设置：是否使用 TCP 隧道，以及发送与服务器同步的请求的周期。

**如何在 Web Console 中配置 Kaspersky Endpoint Security 与 EDR Expert (cloud) 连接的其他设置**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (cloud)**。
5. 使用“**Endpoint Detection and Response Expert (cloud) 已禁用**”拨动开关启用该组件。
6. 如果当前策略是子策略，且父策略禁止更改 EDR Expert (cloud) 集成设置（闭合的“锁”图标），则可以在“**继承**”部分中配置设置继承：
   - **从策略继承连接设置**（默认值）。连接设置将继承自父策略。您将无法编辑这些设置。
   - “**使用自定义连接设置**”。您可以手动配置连接设置。
7. “**响应服务器**”选项卡显示响应服务器的完全限定域名和端口，这些信息会自动检索。如果您的基础架构中的安全策略不允许您直接连接到 EDR Expert (cloud) 服务器，您可以通过 TCP 隧道建立连接：
   a. 选择**使用 TCP 隧道进行响应**复选框。
   b. 指定服务器地址（IPv4、IPv6）和连接到隧道的端口。
8. 如有必要，请在“**发送同步请求到服务器的间隔(分钟)**”字段设置向服务器发送同步请求的频率。在同步过程中，Kaspersky Endpoint Security 接收威胁响应任务并发送任务结果。
9. 转到“**遥测采集服务器**”选项卡。
10. 配置遥测采集服务器连接设置：
    a. 单击**编辑**链接。
    b. 这将打开一个窗口；在该窗口中，从列表中选择一个遥测采集服务器。KUMA 收集器在 EDR Expert (cloud) 中用作遥测采集服务器。有关更多详细信息，请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助。

       如果在连接到遥测采集服务器时发生错误，请选择其他服务器。如果您无法连接到遥测采集服务器，请联系技术支持。
    c. 如有必要，您可以像为响应服务器配置连接一样，通过 TCP 隧道配置与遥测采集服务器的连接。
11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何通过命令行查看证书信息**

1. 要查看有关客户端证书的信息，请运行以下命令：

```
kesl-control --query-cloudxdr-client-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-client-certificate --server-type response
```

2. 要查看有关服务器证书的信息，请运行以下命令：

```
kesl-control --query-cloudxdr-server-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-server-certificate --server-type response
```

因此，Kaspersky Endpoint Security 将按如下方式显示证书信息：

```
Serial number: 12 34 56 78 AB CD EF GH
Subject: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Issuer: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Valid from: 2022-07-27 13:25:35
Expires on: 2072-07-14 13:25:35
SHA1 fingerprint: a14f12df23fg3465bgh6345g567df
```

通过查看*应用程序组件状态报告*检查组件的操作状态。您还可以查看受保护设备上组件的状态。

# 如何优化 EDR Expert (cloud) 遥测传输

*遥测*是受保护计算机上发生的事件的列表。Kaspersky Endpoint Security 在同步期间分析遥测数据并将其发送到遥测采集服务器。遥测事件几乎连续不断地到达服务器。当满足以下任一条件时，Kaspersky Endpoint Security 启动与服务器的同步：

- 同步间隔已用完。
- 缓冲区中的事件数超过上限。

因此，默认情况下，应用程序每 30 秒或每当缓冲区包含 1024 个事件时同步一次。您可以在 Kaspersky Endpoint Security 策略中配置同步行为并选择最佳值以匹配您的网络负载（请参阅下面的说明）。

如果 Kaspersky Endpoint Security 与服务器之间没有连接，应用程序将对新事件进行排队。当连接恢复时，Kaspersky Endpoint Security 以正确的顺序将排队的事件发送到服务器。为避免服务器过载，Kaspersky Endpoint Security 可能会跳过一些事件。要启用此功能，您可以优化事件传输设置，例如，设置每小时最大事件数值（请参阅下面的说明）。

**如何在 Web Console 中优化遥测传输**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (cloud)**。

5. 在打开的窗口中，选择“**数据传输设置**”选项卡。

6. 确保“**发送遥测已启用**”复选框被选中。

7. 如果需要，请启用 **仅发送带有 IOA 的遥测** 功能。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。默认情况下，该功能处于禁用状态。

8. 如有必要，请配置服务器同步设置：

   - “**最大事件传输延迟(秒)**”。应用程序在同步间隔到期后与服务器同步以发送事件。默认设置是 30 秒。
   - “**事件包的最大数量**”。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。

9. 转到“**请求限制**”选项卡。

10. 如有必要，请使用 **请求限制已启用** 切换开关禁用请求限制。

    该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制传输的事件。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。默认情况下已禁用该选项。

11. 配置用于将事件发送到服务器的优化设置：

    - “**每小时最大事件数**”。如果事件流超过配置的每小时事件数限制，应用程序会分析遥测数据流并限制事件的发送。Kaspersky Endpoint Security 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。
    - “**超出事件限制的百分比 (%)**”。该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Endpoint Security 将恢复发送事件。默认设置为 15%。

12. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**如何在命令行中优化遥测传输**

1. 要启用发送遥测，请运行以下命令：

```
kesl-control --set-settings 39 [EnableTelemetry=<Yes|No>] [TelemetrySettings.OnlyTaggedEvents=<Yes|No>]
```

2. 要配置与服务器的同步设置，请运行以下命令：

```
kesl-control --set-settings 39 [TelemetrySettings.EventTransferSettings.UseRequestCountLimits=<Yes|No>]
[TelemetrySettings.EventTransferSettings.MaximumDataTransferTime=<delay in sending events in seconds>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInHour=<number of events>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInPackage=<number of event packages>]
[TelemetrySettings.EventTransferSettings.EventLimitExceededPercentage=<percentage of exceeding the event
limit>]
```

| 设置 | 描述 |
| --- | --- |
| `EnableTelemetry` | 将设备上的事件数据（遥测）发送到 OSMP 遥测收集服务器。<br>默认情况下，发送遥测已启用（`Yes`）。 |
| `TelemetrySettings.OnlyTaggedEvents` | 仅发送包含 IOA 的遥测。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。<br>默认情况下，仅发送包含 IOA 的遥测处于禁用状态（`No`）。 |
| `[TelemetrySettings.EventTransferSettings]` 部分包含用于连接到 OSMP 遥测服务器的常规设置。 | |
| `UseRequestCountLimits` | 请求限制。该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制传输的事件。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。<br>默认情况下已禁用该选项。 |
| `MaximumDataTransferTime` | 最大事件传输延迟(秒)。应用程序在同步间隔到期后与服务器同步以发送事件。默认设置是 30 秒。 |
| `MaximumNumberOfEventsInHour` | 每小时最大事件数。如果事件流超过配置的每小时事件数限制，应用程序会分析遥测数据流并限制事件的发送。Kaspersky Endpoint Security 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。 |
| `MaximumNumberOfEventsInPackage` | 数据包中的最大事件数量。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。 |
| `EventLimitExceededPercentage` | 超出事件限制的百分比 (%)。该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Endpoint Security 将恢复发送事件。默认设置为 15%。 |

# 如何配置 EDR Expert (cloud) 遥测排除项

要提高性能并优化到遥测采集服务器的数据传输，您可以配置遥测排除项。例如，您可以选择不发送单个应用程序的网络通信数据。

使用过多规则会增加遥测采集服务器的负载并降低计算机性能。我们建议只添加必要的规则。

*要在 Web Console 中创建遥测排除项：*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **遥测设置**。
5. 选择**EDR Expert (cloud) 遥测**选项卡。
6. 在“**常规排除项**”块中单击“**添加**”按钮。
   这将打开用于添加遥测排除规则的窗口。

7. 配置遥测排除规则：

   a. 如有必要，可更改规则状态。默认情况下，规则已启用。

   b. 输入规则的名称。

   c. 选择触发规则时要执行的操作：

   - “**不采集**”。被过滤的事件将从发送的遥测数据中排除。
   - “**排除 IOA**”。IOA 规则触发器事件将从发送的遥测数据中排除。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。

   d. 如果选中“**排除 IOA**”选项，请指定要添加到排除项中的 IOA 规则：

   - “**全部排除**”。当满足指定条件时，应用程序将从遥测数据中排除基于所有 IOA 规则生成的事件。
   - “**按 GUID 排除**”。指定 IOA 规则的 GUID。您可以使用“`,`”指定多个 GUID。有关 IOA 规则的详细信息，请参阅 EDR Expert (cloud) 帮助。

   e. 指定过滤条件：

   如有必要，您可以使用 **且**、**或** 和 **非** 运算符，通过添加多个过滤条件和条件组来创建复杂的过滤条件。您还可以向条件组中添加嵌套条件和条件组。

8. 如有必要，在“**所有事件类型**”下，按事件类型添加遥测排除项。

   a. 点击事件类型名称。

   b. 在打开的窗口中，单击“**手动设置**”按钮。

   c. 在“**排除规则**”块中单击“**添加**”按钮。

   这将打开用于添加遥测排除规则的窗口。在遥测排除规则中，已预设与事件类型相对应的 `EventType` 过滤条件。

   d. 指定过滤条件：

9. 要将该策略应用于计算机，请确保锁形图标已关闭 (🔓)，然后保存更改。

## 如何导出或导入 EDR Expert (cloud) 事件过滤器

可以将排除列表导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。还可以使用导出/导入功能备份事件过滤器或将列表迁移到其他服务器。

使用过多规则会增加遥测采集服务器的负载并降低计算机性能。我们建议只添加必要的规则。

*要在 Web Console 中导出和导入事件过滤器：*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **遥测设置**。
5. 选择**EDR Expert (cloud) 遥测**选项卡。
6. 要导出事件过滤器：
   a. 单击“**导出**”。
   b. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。
   c. 保存文件。
      Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。
7. 要导入事件过滤器：
   a. 单击“**导入**”。
   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。
   c. 选择您希望如何导入事件过滤规则：添加到现有规则或丢弃现有规则并用新规则替换。
   d. 打开文件。
8. 要将该策略应用于计算机，请确保锁形图标已关闭 (🔒)，然后保存更改。
   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
   2. 单击 Kaspersky Endpoint Security 策略的名称。
      策略属性窗口将打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择 **常规设置** → **遥测设置**。
   5. 选择**EDR Expert (cloud) 遥测**选项卡。
   6. 要导出事件过滤器：
      a. 单击“**导出**”。
      b. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。
      c. 保存文件。
         Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。

7. 要导入事件过滤器：

   a. 单击“**导入**”。

   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。

   c. 选择您希望如何导入事件过滤规则：添加到现有规则或丢弃现有规则并用新规则替换。

   d. 打开文件。

8. 要将该策略应用于计算机，请确保锁形图标已关闭 (🔒)，然后保存更改。

# Kaspersky Anti Targeted Attack Platform

*Kaspersky Anti Targeted Attack Platform* 是一款用于保护组织 IT 基础设施并及早检测零日攻击、定向攻击和高级持续性威胁（以下简称 APT）等威胁的解决方案。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

Kaspersky Endpoint Security 应用程序可以与 Kaspersky Anti Targeted Attack Platform 上的以下组件集成：

**Kaspersky Endpoint Detection and Response (KATA)**

该保护组件可保护组织本地网络中的设备。与 Kaspersky Endpoint Detection and Response (KATA) 集成时，Kaspersky Endpoint Security 执行以下功能：

- 将设备上发生的事件的相关信息（遥测数据）发送到中央节点服务器，该服务器提供与 Kaspersky Endpoint Detection and Response (KATA) 的交互功能（以下简称 *KATA 服务器*）。

  Kaspersky Endpoint Security 会向中央节点组件发送有关进程、打开的网络连接和修改后的文件的监控数据，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 威胁响应操作 以确保安全。

支持与 Kaspersky Endpoint Detection and Response (KATA) 7.1 及更早版本集成。

**Network Detection and Response (KATA)**

该组件用于保护组织的内部网络。与 Kaspersky Network Detection and Response (KATA) 集成时，Kaspersky Endpoint Security 可以将关于设备事件的信息（遥测数据）发送到提供 Kaspersky Network Detection and Response (KATA) 交互功能的 Central Node 服务器（下文亦称“*NDR 服务器*”）。

**Sandbox**

Kaspersky Endpoint Security 应用程序将文件发送到中央节点服务器进行扫描，该服务器负责处理与 沙盒 的交互。

Kaspersky Endpoint Security 的以下组件支持与 Kaspersky Anti Targeted Attack Platform 集成：

- Endpoint Detection and Response Expert (on-premises)，以下简称 *EDR Expert (on-premises)*。

  从 Kaspersky Endpoint Security 12.4 for Linux 开始，Endpoint Detection and Response (KATA) 组件已重命名为 Endpoint Detection and Response Expert (on-premises)。现在，该组件不仅提供与 Kaspersky Endpoint Detection and Response (KATA)（Kaspersky Anti Targeted Attack Platform 的一个组件）的集成，还提供与 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案的集成。

- Network Detection and Response (KATA)，以下简称 *NDR (KATA)*。
- Sandbox。

您可以配置 Kaspersky Endpoint Security 应用程序与 Kaspersky Anti Targeted Attack Platform 解决方案的所有组件的整合，也可以单独配置与每个组件的整合。

该组件不适用于配备 Elbrus CPU 的设备。

配置 Kaspersky Anti Targeted Attack Platform 集成

**先决条件**

在配置 Kaspersky Network Detection and Response (KATA) 集成之前，请允许端口 8085 上的连接。

在配置与 Kaspersky Endpoint Detection and Response (KATA) 组件的集成之前：

- 允许通过端口 443、8443 进行连接。
- 启用 行为检测 组件以传输必要的遥测数据。

  行为分析组件适用于内核版本 3.13 及更高版本的设备。

  如果要获取其他保护组件检测到的威胁信息，请启用以下组件：

  - 文件威胁防护。
  - 网络威胁防护。
  - Web 威胁防护。
  - 反加密勒索。
  - 应用程序控制。
  - 设备控制。
  - 系统完整性监控。

启用 eBPF 网络流量拦截模式可使遥测数据更加全面。eBPF 技术适用于运行 64 位操作系统且内核版本为 4.18 或更高版本并支持 eBPF 的计算机。

建议检查您的计算机是否支持发送遥测数据所需的组件。

- 如果您已购买单独的授权许可来使用此功能，请将 EDR Expert (on-premises) 授权许可密钥添加到应用程序。

  如果您使用的 Kaspersky Endpoint Security 授权许可包含 Kaspersky Endpoint Detection and Response Expert (on-premises)，则无需执行任何操作。

  如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security，则需要向 SVM 添加用于激活附加功能的授权许可密钥。

**基本配置步骤**

1. **获取并处理中央节点服务器颁发的证书**

   与 Kaspersky Anti Targeted Attack Platform 集成时，运行 Kaspersky Endpoint Security 的设备会与提供集成的 Central Node 服务器建立加密的 HTTPS 连接。

   如果 Kaspersky Endpoint Security 的常规设置规定必须使用代理服务器，则与处理 Kaspersky Anti Targeted Attack Platform 组件交互的服务器的连接将通过代理服务器建立。

   用于保护处理 Kaspersky Anti Targeted Attack Platform 组件交互的服务器连接的证书必须由 Kaspersky Anti Targeted Attack Platform 管理员提供。

   要处理证书，请按照 将 PFX 证书转换为 PEM 格式一文中所述步骤操作。

   您可以使用服务器证书和/或客户端证书。选择取决于贵组织的安全策略。

2. **配置 Kaspersky Anti Targeted Attack Platform 集成设置**

   您可以通过以下方式进行配置：

   - 使用 Web Console（Kaspersky Security Center 控制台中的 EDR (KATA) 和 NDR (KATA) 和/或 OSMP 控制台）。
   - 使用 Kaspersky Security Center 管理控制台（EDR (KATA) 和 NDR (KATA)）。
   - 使用命令行（EDR (KATA) 和 NDR (KATA)）。

3. **验证是否已成功建立与 Kaspersky Anti Targeted Attack Platform 的连接。**

   以任何方便的方式检查 Kaspersky Anti Targeted Attack Platform 组件的状态。

4. **必要时管理其他设置**

   - 如果您的操作系统上的 SELinux 配置为 Enforcing 模式，则需要额外配置 SELinux，以执行响应操作。
   - 查看网络隔离的限制。

# 如何配置 EDR (KATA) 集成

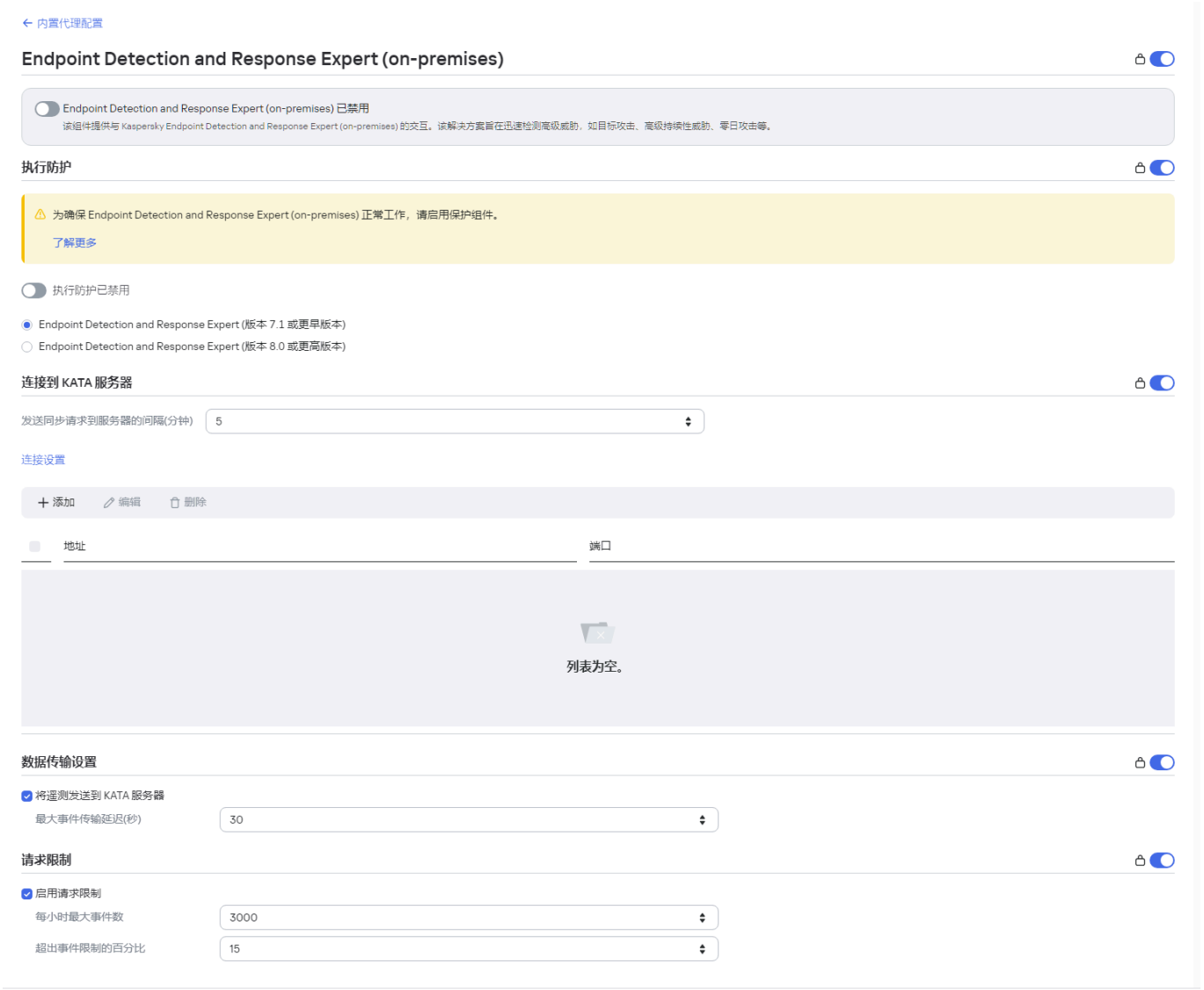
在 Web Console 中，您可以启用或禁用 Kaspersky Endpoint Detection and Response (KATA) 组件，并配置 Kaspersky Endpoint Security 应用程序与此组件的集成。

**如何在 Web Console 中配置 Kaspersky Endpoint Detection and Response (KATA) 集成**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在打开的策略属性窗口中，选择“**应用程序设置**”选项卡。
5. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premises)**。
6. 在屏幕右侧：
   a. 选择“**Endpoint Detection and Response Expert 版本 7.1 或更早版本**”选项。
   b. 在 **连接到遥测收集服务器** 部分中，通过单击工具栏中的 **添加** 按钮来选择遥测收集服务器，然后单击 **选择服务器**。
   c. 在 **连接到响应服务器** 部分中，通过单击工具栏中的 **添加** 按钮来选择响应服务器，然后单击 **选择服务器**。
   d. 在 **连接到遥测收集服务器** 和 **连接到威胁响应服务器** 部分中，单击 **连接设置** 链接，然后在显示的窗格中：
      1. 通过单击 **上传** 按钮添加服务器证书。
      2. 如果需要额外保护，请创建加密容器。
         为此，请在 **附加连接保护** 部分中执行以下操作：
         - 选中 **使用双向身份验证** 复选框。
         - 单击 **上传** 按钮，并添加您在主场景步骤 1 中获得的客户端证书。
         - 在相应字段中输入加密容器的密码。

         **加密容器密码** 字段为必填字段。不输入客户端证书（加密容器）的密码，就无法保存设置。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




Endpoint Detection and Response Expert (on-premises)

## 如何在命令行上配置 Kaspersky Endpoint Detection and Response (KATA) 集成

1. 要选择 EDR (KATA) 集成模式，请运行以下命令：

```
kesl-control --set-settings 24 Mode=EDRKATA
```

2. 要添加 Central Node 服务器，请运行以下命令：

```
kesl-control --set-settings 24 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

3. 要添加响应服务器证书，请运行以下命令：

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

4. 要配置集成设置，请运行以下命令：

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

设置及其可能的值列于下表中。

5. 要添加用于连接到响应服务器的客户端证书，请运行以下命令：

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

6. 要启用与 EDR (KATA) 的集成，请运行以下命令：

```
kesl-control --start-task 24
```

Kaspersky Endpoint Detection and Response (KATA) 集成设置

| 设置 | 描述 | 值 |
|---|---|---|
| Mode | 集成模式。<br>对于 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，Kaspersky Endpoint Security 应用程序会与 OSMP 平台上的服务器交互。<br>对于 Kaspersky Endpoint Detection and Response (KATA) 集成，Kaspersky Endpoint Security 应用程序与 Kaspersky Anti Targeted Attack Platform 上的服务器进行交互。 | EDRKATA（默认）是 EDR (KATA) 集成模式。允许启用与 Kaspersky Endpoint Detection and Response (KATA) 进行集成，这是 Kaspersky Anti Targeted Attack Platform 的一个组件。<br>EDRExpertOnPrem 是 EDR Expert (on-premises) 集成模式。启用 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成 |
| 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。<br>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 Expert (on-premises) 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 – 使用双向身份验证来进一步保护与 KATA 服务器的连接。<br>No （默认值）— 不使用双向身份验证。 |
| SynchronizationPeriod | 发送同步请求到 KATA 服务器的间隔（以分钟为单位）。 | 默认值：5。 |
| ConnectionTimeout | 等待与 KATA 服务器连接的最长时间（以秒为单位）。 | 默认值：10。 |
| RequestTimeout | 等待 KATA 服务器响应的最长时间（以秒为单位）。 | 默认值：10。 |
| EnableTelemetry | 向 KATA 发送事件数据（遥测）。 | Yes （默认值）– 向 KATA 服务器发送遥测数据。<br>No禁用传送遥测数据。 |
| **[Endpoints.item_#]** 部分包含 KATA 服务器的地址和端口。您可以添加多台服务器。 | | |
| Address | KATA 服务器地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>为确保在设备上启用网络隔离的情况下应用程序发生故障时与服务器的通信不会中断，我们建议指定服务器的 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：443。 |
| **[EventTransferSettings]** 部分包含将数据发送到 KATA 服务器的设置。 | | |
| MaximumDataTransferTime | 向 KATA 服务器发送事件的最大延迟（以秒为单位）。 | 默认值：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。<br>No – 不调节事件数。 |
| MaximumNumberOfEventsInHour | 每小时的最大事件数量 | 默认值：3000。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `MaximumNumberOfEventsInPackage` | 一个数据包中的最大事件数量。 | 默认值：`1024`。 |
| `EventLimitExceededPercentage` | 事件数量超过限制（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：`15`。 |

如果使用 Web Console 或命令行，要与 Kaspersky Endpoint Detection and Response (KATA) 集成，您需要在 EDR Expert (on-premises) 组件的设置中选择 *EDR (KATA)* 集成模式：

- 如果您使用的是 Web Console，请在策略设置中选择 **Endpoint Detection and Response Expert (版本 7.1 或更早版本)** 选项。要在设备上配置与 Kaspersky Endpoint Detection and Response (KATA) 的集成，您需要在 Web Console 中为任一版本（8.0 及更高版本，以及 7.1 及更早版本）管理“锁定”。
- 如果您使用命令行，请在任务设置中设置`Mode=EDRKATA`。

# 如何配置 NDR (KATA) 集成

在 Web Console 中，您可以启用或禁用 Kaspersky Network Detection and Response (KATA) 组件，并配置 Kaspersky Endpoint Security 应用程序与此组件的集成。

**如何在 Web Console 中配置 Kaspersky Network Detection and Response (KATA) 集成**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Network Detection and Response (KATA)**。
5. 启用 **Network Detection and Response (KATA)** 切换开关。
6. 单击“**连接设置**”。
7. 配置服务器连接：
   - “**超时(秒)**”。最大 Central Node 服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的 Central Node 服务器。
   - “**服务器证书**”。用于与 Central Node 服务器建立可信连接的 TLS 证书。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Anti Targeted Attack Platform 帮助 中的说明）。
   - “**使用双向身份验证**”。在 Kaspersky Endpoint Security 和 Central Node 之间建立安全连接时进行双向身份验证。要使用双向身份验证，您需要在 Central Node 服务器设置中启用双向身份验证，然后获取加密容器并设置密码以保护加密容器。*加密容器*是带有证书和私钥的 PFX 存档。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获得一个加密容器（请参阅 Kaspersky Anti Targeted Attack Platform 帮助 中的说明）。配置 Central Node 设置后，您还需要在 Kaspersky Endpoint Security 设置中启用双向身份验证并加载受密码保护的加密容器。

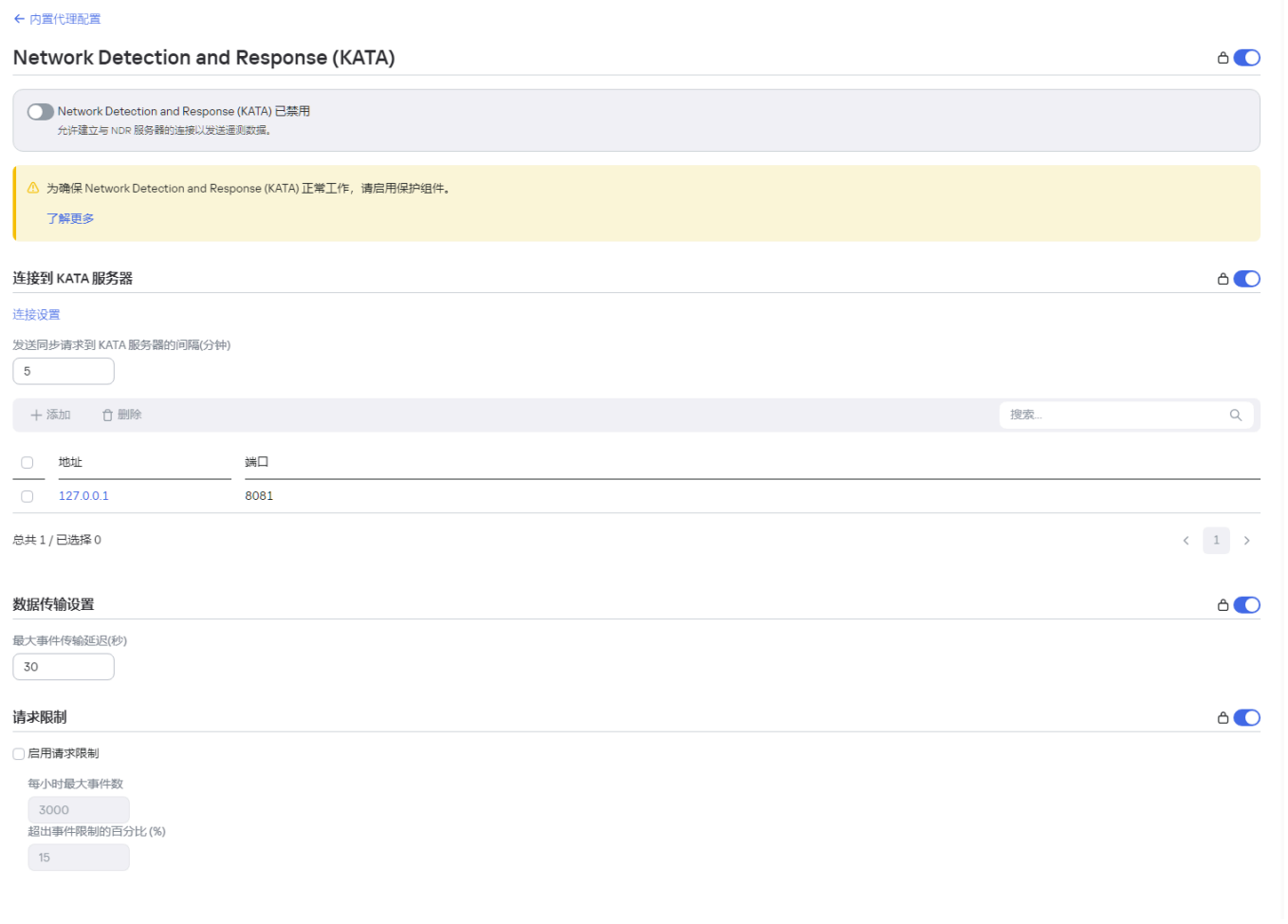
     加密容器必须受密码保护。无法添加密码为空的加密容器。

8. 单击“**确定**”。

9. 添加 Central Node 服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

10. 您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




Network Detection and Response (KATA)

## 如何在命令行上配置 Kaspersky Network Detection and Response (KATA) 集成

1. 要添加 Central Node 服务器，请运行以下命令：

```
kesl-control --set-settings 31 Endpoints.item_001.Address=<cenral node server address> Endpoints.item_001.Port=
<central node server port>
```

2. 要添加响应服务器证书，请运行以下命令：

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

3. 要配置集成设置，请运行以下命令：

```
kesl-control --set-settings 31 [<setting name>=<setting value>]
```

设置及其可能的值列于下表中。

4. 要添加用于连接到响应服务器的客户端证书，请运行以下命令：

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

5. 要启用与 NDR (KATA) 的集成，请运行以下命令：

```
kesl-control --start-task 31
```

Kaspersky Network Detection and Response (KATA) 整合任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `UseClientPinnedCertificate` | 启用和禁用双向身份验证，以进一步保护与 NDR 服务器的连接。<br>如果在 NDR 服务器端启用了客户端证书验证，请在启动 *Kaspersky Network Detection and Response (KATA) 整合*任务之前启用客户端证书的使用并添加客户端证书。 | `Yes` – 使用双向身份验证来进一步保护与 NDR 服务器的连接。<br>`No`（默认值）– 不使用双向身份验证。 |
| `SynchronizationPeriod` | 发送同步请求到 NDR 服务器的间隔（以分钟为单位）。 | 默认值：`5`。 |
| `ConnectionTimeout` | 等待与 NDR 服务器连接的最长时间（以秒为单位）。 | 默认值：`10`。 |
| `RequestTimeout` | 等待 NDR 服务器响应的最长时间（以秒为单位）。 | 默认值：`10`。 |
| **[Endpoints.item_#]** 部分包含 NDR 服务器的地址和端口。 | | |
| `Address` | NDR 服务器地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。 | 默认值：`127.0.0.1`。 |
| `Port` | 用于连接到 NDR 服务器的端口。 | 默认值：`8081`。 |
| **[EventTransferSettings]** 部分包含将事件发送到 NDR 服务器的设置。 | | |
| `MaximumDataTransferTime` | 向 NDR 服务器发送事件的最大延迟（以秒为单位）。 | 默认值：`30`。 |
| `MaximumNumberOfEventsInPackage` | 一个数据包中的最大事件数量。 | 默认值：`1024`。 |
| `UseRequestCountLimits` | 启用和禁用调节发送到 NDR 服务器的事件数。 | `Yes`（默认值）– 调节发送的事件数。<br>`No` – 不调节事件数。 |
| `MaximumNumberOfEventsInHour` | 每小时的最大事件数量 | 默认值：`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：`15`。 |
| `PingPeriod` | NDR 服务器轮询周期（秒）。 | 默认值：`450`。 |

# 如何验证 KATA 整合是否已启动并正常运行

您可以通过以下方式测试 Kaspersky Anti Targeted Attack Platform 组件：

- 在命令行中使用以下 命令：

```
kesl-control --app-info
```

对于与 EDR (on-premises) 和 NDR (KATA) 组件的集成，系统会显示**可用并正在运行**状态。

- 在 Web Console 中：
  - 在 Kaspersky Security Center 控制台中，使用*应用程序组件状态报告*。有关报告的详细信息，请参阅“Kaspersky Security Center 帮助”。
  - 在 OSMP 控制台中：
    - 使用 *有关应用程序组件状态的报告*。
    - 转到**资产管理** → **资产**区域，选择 **分析和响应**选项卡。
      该设备以 **正常活动**遥测状态显示在列表中。
    - 转到 **威胁搜索**区域。
      来自该设备的遥测事件会显示在事件列表中。
- 在 Kaspersky Anti Targeted Attack Platform 中：
  转到 **资产** → **设备** 区域。设备会显示在表中。如有必要，您可以按 **EPP 应用程序**、**EPP 连接**、**上次连接到 EPP** 筛选表格。
  单击设备名称会打开一个窗格。在**端点代理**区域中，连接状态为**活动**。

# Sandbox

Sandbox 技术能够分析和扫描部署了操作系统虚拟镜像的特殊服务器上的对象，以检测恶意活动和针对企业 IT 基础设施的定向攻击的迹象。

Kaspersky Endpoint Security 应用程序可以通过 Open Single Management Platform (OSMP) 或 Kaspersky Anti Targeted Attack Platform 与沙盒进行交互。

该组件不适用于配备 Elbrus CPU 的设备。

## 如何配置 Sandbox 整合

开始配置 Sandbox 整合之前：

- 允许以下入站和出站连接：
  - 入站（管理接口）：
    - TCP 22
    - TCP 443
    - TCP 8443
  - 出站（管理接口）：
    - TCP 80 或 TCP 443

- 出站和相应的入站方向（用于访问已处理对象的接口）：
  任意端口。

- 如果您想通过文件或目录的上下文菜单手动将文件发送到沙盒，请安装图形界面（kesl-gui 软件包）。

**基本配置步骤**

1. **在平台中创建沙盒服务器连接请求，然后在沙盒管理控制台中确认连接**

   有关详细信息，请参阅相应解决方案的帮助：

   - Kaspersky Anti Targeted Attack Platform
   - Open Single Management Platform

   以任何方便的方式保存沙盒服务器的 IP 地址。后续配置整合时将需要用到它。

2. **获取并处理由 OSMP 服务器或 中央节点 服务器颁发的证书**

   与 Sandbox 集成时，运行 Kaspersky Endpoint Security 的设备会与 Integration Server 建立加密的 HTTPS 连接。

   > 如果在 Kaspersky Endpoint Security 应用程序的常规设置中配置了使用代理服务器，则代理服务器将用于连接到处理 Sandbox 交互的服务器。

   用于保护处理 Sandbox 交互的服务器的连接的证书，必须由 OSMP 平台或 Kaspersky Anti Targeted Attack Platform 的管理员提供。

   要处理证书，请按照 将 PFX 证书转换为 PEM 格式一文中所述步骤操作。

   您可以使用服务器证书和/或客户端证书。选择取决于贵组织的安全策略。

3. **管理 Sandbox 整合设置**

   要发送文件进行扫描，您必须启用与 KATA Sandbox 的集成并添加部署在解决方案内部的 Central Node 服务器。

   **如何在 Web Console 中配置 Sandbox 整合**

   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
   2. 单击 Kaspersky Endpoint Security 策略的名称。
      策略属性窗口将打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择 **内置代理配置** → **Sandbox**。
   5. 在“**提交扫描的文件类型**”下拉列表中，选择所需方法：

      - “**手动**”。在此模式下，您可以使用命令手动将对象发送到沙盒进行扫描，或从 **在 Sandbox 中扫描** 上下文菜单发送。

        > 如果您的沙盒版本低于 8.0，我们建议选择此类型。

- “**自动**”。应用程序会自动发送对象进行扫描，无法手动发送对象供 Sandbox 进行扫描。
- “**组合的**”。应用程序会自动发送对象进行扫描，但您也可以使用命令或图形接口手动将对象发送到 Sandbox 。

6. 在“**连接到 Sandbox 服务器**”部分中：

- 通过单击工具栏中的“**添加**”按钮来添加 Integration Server。

  您可以指定 KATA / OSMP 平台的 IP 地址或其 FQDN 作为地址。

  如果沙盒服务器连接到 OSMP，则只能指定代理服务器的 FQDN。

- 添加 Kaspersky Anti Targeted Attack Platform 或 OSMP 的服务器证书，该证书是您在主要场景的步骤 2 中收到的。

  要执行此操作，请单击“**服务器连接设置**”链接，然后在显示的窗格中的“**服务器 TLS 证书**”部分中，单击“**上传**”按钮。

- 如果需要额外保护，请创建加密容器。

  为此，请在“**附加连接安全**”部分中：

  - 选择**使用双向身份验证**复选框。
  - 单击“**上传**”按钮并添加客户端证书。
  - 在相应字段中输入加密容器的密码。

  “**加密容器密码**”字段为必填字段。不输入客户端证书（加密容器）的密码，就无法保存设置。

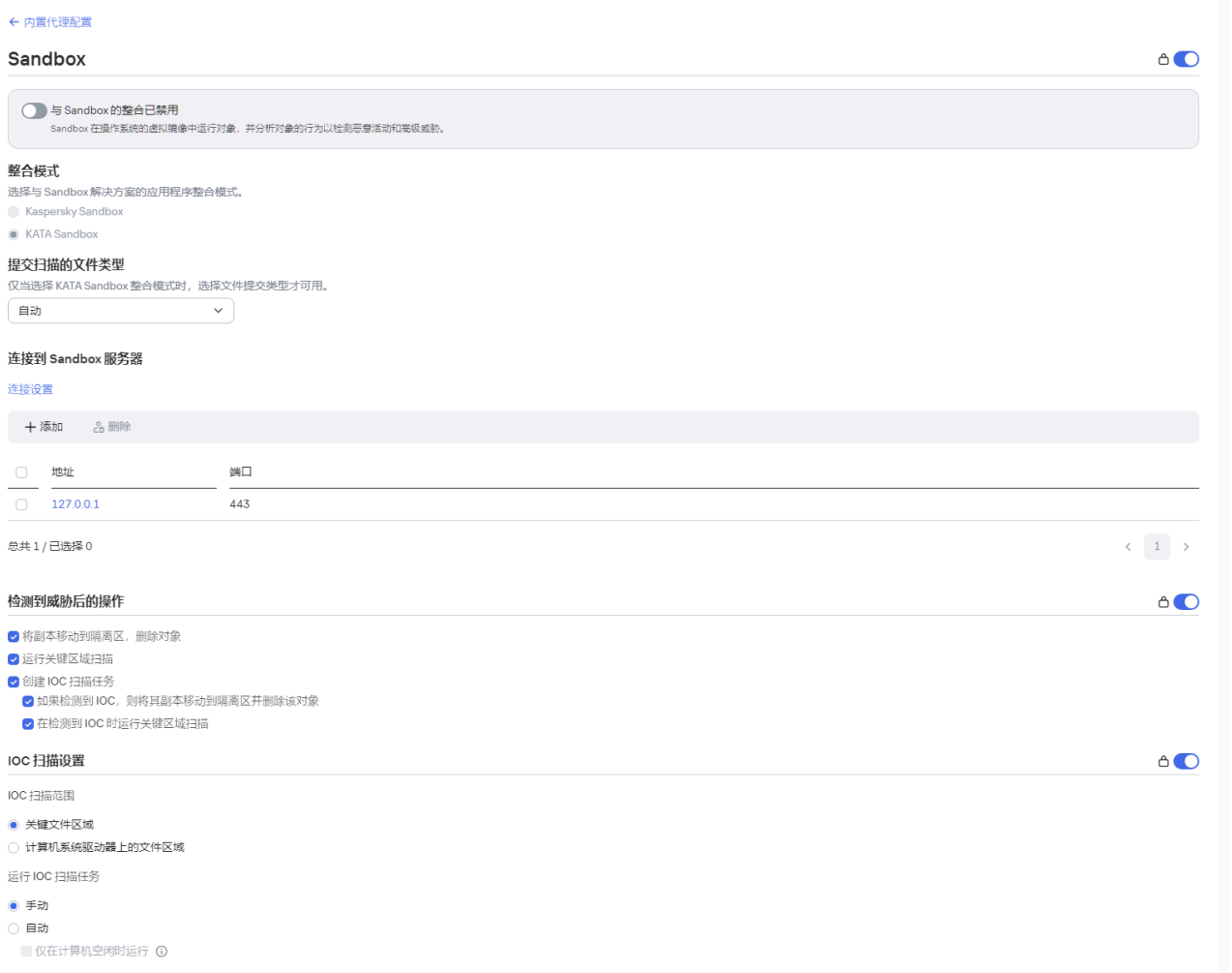
7. 在“**检测到威胁后的操作**”块中选择相关操作：

- “**将副本移动到隔离区，删除对象**”。如果选择此选项，Kaspersky Endpoint Security 删除在计算机上发现的恶意对象。在删除对象之前，Kaspersky Endpoint Security 会创建它的备份副本，以防您稍后需要恢复该对象。Kaspersky Endpoint Security 移动备份副本到隔离区。
- “**运行关键区域扫描**”。如果选择此选项，Kaspersky Endpoint Security 运行*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。
- “**创建 IOC 扫描任务**”。如果选择此选项，Kaspersky Endpoint Security 将自动创建 *IOC 扫描(自主 IOC 扫描任务)*。对于此任务，您可以配置运行模式、扫描范围以及检测到 IOC 时执行的操作（*将副本移动到隔离区，删除对象* 或 *运行关键区域扫描*）。要修改 *IOC 扫描*任务的其他设置，请转到任务设置。

8. 如有必要，在“**IOC 扫描范围**”块配置“*IOC 扫描*”任务设置。

- “**关键文件区域**”。如果选择此选项，Kaspersky Endpoint Security 仅在用户目录和系统目录中扫描 IOC。
- “**计算机系统驱动器上的文件区域**”。如果选择此选项，Kaspersky Endpoint Security 将扫描根文件系统中的所有文件以查找 IOC。

9. 如有必要，在“**运行 IOC 扫描任务**”块配置“*IOC 扫描*”任务设置。
   - “**手动**”。您可以在方便时手动启动“*IOC 扫描*”任务的运行模式。
   - “**自动**”。在此运行模式下，Kaspersky Endpoint Security 会在检测到威胁后自动运行 *IOC 扫描* 任务。
10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。




Sandbox

## 如何在命令行上配置 Sandbox 整合

1. 要添加服务器证书，请运行以下命令：

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

2. 要添加中央节点或 OSMP 服务器，请运行以下命令：

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port>
```

3. 要配置集成设置，请运行以下命令：

```
kesl-control --set-settings 29 [<setting name>=<setting value>]
```

设置及其可能的值列于下表中。

4. 要添加客户端证书，请运行以下命令：

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

5. 要启用 Sandbox 整合，请运行以下命令：

```
kesl-control --start-task 29
```

Sandbox 集成任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| `UseClientCertificate` | 启用和禁用双向身份验证，以进一步保护与 Sandbox 服务器的连接。<br>如果在 Sandbox 服务器端启用了客户端证书验证，请在启动 *Sandbox 集成*任务之前启用客户端证书的使用并添加客户端证书。 | `Yes` — 使用双向身份验证来进一步保护与 Sandbox 服务器的连接。<br>`No`（默认值）— 不使用双向身份验证。 |
| `ConnectionTimeout` | 等待与服务器连接的最长时间（以秒为单位）。 | 默认值：`10`。 |
| `RequestTimeout` | 等待服务器响应的最长时间（以秒为单位）。 | 默认值：`10`。 |
| `SendingMode` | 将对象发送到 Sandbox 进行扫描的模式 | `AutoOnly`（默认值）– 当尝试访问文件时，自动发送文件进行扫描。<br>`Manual` – 手动发送文件进行扫描。<br>`AutoAndManual` – 自动和手动发送文件进行扫描。 |
| `QuarantineFile` | 当检测到威胁时，将文件进行隔离。 | `Yes`（默认值）– 如果检测到威胁，则删除原始文件，并将文件副本放入隔离区。<br>`No` – 检测到威胁时，不将文件进行隔离。 |
| `ScanCriticalAreas` | 检测到威胁时，执行关键区域扫描。 | `Yes`（默认值）– 检测到威胁时启动关键区域扫描。<br>`No` – 检测到威胁时不启动关键区域扫描。 |
| `CreateIocScanTask` | 检测到威胁时创建IOC 扫描任务。 | `Yes`（默认值）– 检测到威胁时创建 IOC 扫描任务。<br>`No` – 检测到威胁时不创建 IOC 扫描任务。 |
| `QuarantineFileOnIocDetected` | 检测到入侵指标时隔离对象。 | `Yes`（默认值）– 如果检测到入侵指标，则删除原始对象，并将对象副本放入隔离区。<br>`No` — 检测到入侵指标时不隔离对象。 |
| `ScanCriticalAreasOnIocDetected` | 检测到入侵指标时，执行关键区域扫描。 | `Yes`（默认值）– 检测到入侵指标时启动关键区域扫描。<br>`No` – 检测到入侵指标时不启动关键区域扫描。 |
| `Drives` | IoC 扫描范围。 | `Critical`（默认）— 扫描用户和系统目录中的文件。<br>`System` — 扫描根文件系统中的所有文件。 |
| `ScheduleMode` | IOC 扫描任务启动模式。 | `Manually`（默认）– 手动启动 IOC 扫描任务。<br>`AfterTreatDetected` – 检测到威胁后启动 IOC 扫描任务。 |
| **[Servers.item_#]** 部分包含 Sandbox 服务器的设置。 | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `Address` | 服务器的地址。<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。 | 默认值：`127.0.0.1`。 |
| `Port` | 用于连接到服务器的端口。 | 默认值：`443`。 |
| **[SandboxTransferSettings]** 部分包含发送文件以在 Sandbox 中进行扫描的设置。 | | |
| `SandboxQueue` | 扫描请求队列的最大大小（以 MB 为单位）。 | 默认值：`1024`。 |

4. **验证是否已成功建立与沙盒的连接**

   以任何方便的方式检查沙盒的状态。

# 如何验证 Sandbox 整合是否已启动并运行

您可以通过以下方式测试沙盒组件：

- 在命令行中使用以下 命令：

  ```
  kesl-control --app-info
  ```

  与沙盒的集成显示为 **可用且正在运行** 状态。

- 在 Web Console 中：
  - 在 Kaspersky Security Center 控制台中：

    使用 *有关应用程序组件状态的报告*。有关报告的详细信息，请参阅“Kaspersky Security Center 帮助”。
  - 在 OSMP 控制台中：
    - 使用 *有关应用程序组件状态的报告*。
    - 转到 **威胁搜索**区域。

      成功建立沙盒连接的事件会显示在事件列表中。
- 在 Kaspersky Anti Targeted Attack Platform 中：

  转到 **资产** → **设备** 区域。设备会显示在表中。如有必要，您可以按 **EPP 应用程序**、**EPP 连接**、**上次连接到 EPP** 筛选表格。

  单击设备名称会打开一个窗格。在 Endpoint Agent 区域中，连接状态为**活动**。

# 如何手动将文件发送到沙盒

Kaspersky Endpoint Security 允许用户从上下文菜单手动发送文件或目录到沙盒进行扫描。

要将文件发送到沙盒进行扫描，必须满足以下条件：

- 必须安装 Kaspersky Endpoint Security 的图形界面。
- Kaspersky Endpoint Security 必须与沙盒集成。
- 必须将发送文件进行扫描的模式设置为 **手动** 或 **组合的**。

*要将文件或目录发送到沙盒进行扫描：*

1. 打开要扫描的文件或目录的上下文菜单。
2. 选择 **Kaspersky Endpoint Security 12.5 for Linux** 作为用于打开文件或目录的应用程序。

   根据桌面环境，上下文菜单命令的名称可能会有所不同。

3. 然后在上下文菜单中，选择 **在 Sandbox 中扫描**。

# Kaspersky Managed Detection and Response

Kaspersky Endpoint Security 包含一个内置代理，用于与 Kaspersky Managed Detection and Response 解决方案集成。*Kaspersky Managed Detection and Response (MDR)* 解决方案自动检测和分析您基础架构中的安全事故。为此，MDR 使用从端点和机器学习接收的遥测数据。MDR 发送事故数据到 Kaspersky 专家。然后专家便可以处理事故，例如，添加新条目到反病毒数据库。或者，专家可以发布处理事件的建议，例如，建议将计算机从网络隔离。对于该解决方案如何工作的详情，请参考 Kaspersky Managed Detection and Response 帮助。

Kaspersky Endpoint Security 组件 Managed Detection and Response (MDR) 促进了整合。必须通过集成方案中描述的方式之一激活该组件。

该组件不适用于配备 Elbrus CPU 的设备。

Kaspersky Endpoint Security 与 MDR 集成的配置

以下配置可用于与 MDR 配合使用：

- **[KES+内置代理]**。在此配置中，Kaspersky Endpoint Security 既充当确保计算机安全的应用程序，又充当使用 MDR 的应用程序。
- **[第三方 EPP+EDR Agent]**。在此配置中，IT 基础设施的安全性由第三方 Endpoint Protection Platform（EPP）提供。与 MDR 的交互由 Kaspersky Endpoint Security 在 Endpoint Detection and Response Agent (EDR Agent) 配置下提供。在此配置中，EDR Agent 与第三方 EPP 应用程序兼容。

# 有关创建用于与 MDR 正确集成的参考镜像的建议

我们不建议将 Kaspersky Endpoint Security for Linux 应用程序包含在参考镜像中。

如果参考镜像中包含 Kaspersky Endpoint Security for Linux，请在基于该镜像的每台设备上执行以下步骤：

1. 要创建新的 UUID，请运行以下命令：

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid
uuidgen > /var/opt/kaspersky/epagent/install_id
```

2. 卸载 Kaspersky Endpoint Security for Linux，然后重新安装。

如果不执行这些步骤，设备可能无法被正确识别。

# 上传 KPSN 配置文件

如果您的配置不满足无需 KPSN 配置文件即可运行的要求，则要与 Kaspersky Managed Detection and Response 集成，您需要将 *KPSN 配置文件*上传到 Kaspersky Security Center 管理服务器。该文件包含必要的遥测设置。扩展名为 pkcs7 的 KPSN 配置文件位于 MDR 配置文件（ZIP 压缩文件格式）中。有关详细信息，请参阅 Kaspersky Managed Detection and Response 帮助。

您可以在 Web Console 或管理控制台中上传 KPSN 配置文件。

上传 KPSN 配置文件，即表示您同意在安装 Kaspersky Endpoint Security 的设备中，数据将自动发送到卡巴斯基进行处理。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，请参阅卡巴斯基 Managed Detection and Response 文档。

**如何在 Web Console 中上传 KPSN 配置文件**

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**”拨动开关以启用 KSN 代理服务器服务。
4. 打开“**使用卡巴斯基私人安全网络**”拨动开关。
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 KSN 配置文件（扩展名为 pkcs7），然后点击“**打开**”。
8. 接受 KPSN 声明的条款和条件，然后点击“**保存**”按钮。

**如何在管理控制台 (MMC) 中上传 KPSN 配置文件**

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 KPSN** 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 KSN 配置文件（扩展名为 pkcs7），然后点击“**打开**”。

8. 接受 KPSN 声明的条款和条件，然后点击“**应用**”按钮。

**如何在命令行上传 KPSN 配置文件**

请执行命令：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

# 如何配置 MDR 集成

在配置 Kaspersky Managed Detection and Response 集成之前：

- 允许在端口 443 和 1443 上连接。
- 允许连接到以下地址：
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

  地址列表可能会发生变化。要获取确切地址，您可以联系技术支持。
- 请确保已启用以下项并且其正常运行：
  - 卡巴斯基安全网络处于扩展模式：
  - 行为检测。

    为确保遥测数据完整，您还可以启用以下组件：Web 威胁防护、网络威胁防护、文件威胁防护和 邮件威胁防护。

**基本配置步骤**

1. **通过以下方式之一激活 MDR 组件**
   - 使用授权许可密钥。

     如果您已购买单独的授权许可来使用此功能，请将 MDR 授权许可密钥添加到应用程序。

     如果您根据包含 Kaspersky Managed Detection and Response 的授权许可使用 Kaspersky Endpoint Security，则无需执行任何操作。

     如果 Kaspersky Endpoint Security 在 Light Agent 模式下使用，则 MDR 授权许可密钥会添加到 SVM。

- 使用 MDR BLOB 文件。

  在 MDR 控制台中，下载 MDR 配置文件。此文件是一个 ZIP 压缩文件，其中包含 MDR BLOB 文件和 KPSN 配置文件。

  然后，在 Web Console、管理控制台中或通过命令行上传 BLOB 文件。

Kaspersky Endpoint Security 应用程序的版本决定 MDR 组件的激活方法以及是否需要使用 KPSN 配置文件。有关详细信息，请参阅 Kaspersky Managed Detection and Response 帮助。

如果 Kaspersky Security Center 管理服务器按层级结构组织，并且辅助服务器没有直接 Internet 访问权限，即使主要管理服务器可以访问 Internet，Kaspersky Managed Detection and Response 也无法工作。

### 2 上传 KPSN 配置文件

如果您的组织有多个租户，或者您已使用 MDR BLOB 激活 MDR 组件，请将 KPSN 文件上传到 Kaspersky Security Center 管理服务器。此文件包含发送遥测数据所需的设置；您可以在包含 MDR 配置文件的 ZIP 压缩文件中找到它。

### 3 配置 Kaspersky Managed Detection and Response 集成设置

**如何在 Web Console 中启用 Kaspersky Managed Detection and Response 集成**

1. 在 Web Console 的主窗口中，选择“**资产管理** → **策略**”部分。
2. 单击所需的 Kaspersky Endpoint Security 策略。
3. 在打开的策略属性窗口中，选择“**应用程序设置**”选项卡。
4. 在“**内置代理配置**”部分中，选择“**Managed Detection and Response**”，然后在屏幕右侧管理以下设置：
   - 将切换开关设置为 **Managed Detection and Response 已启用**。
   - 如果您有租户，或者您已使用 MDR BLOB 文件激活 MDR 组件，请单击“**上传**”按钮以添加 MDR BLOB 文件。
5. 保存设置。




Managed Detection and Response

**如何通过命令行启用 Kaspersky Managed Detection and Response 集成**

1. 要启用 MDR 组件，请运行以下命令：

```
kesl-control --set-app-settings UseMDR=Yes
```

2. 要添加 BLOB 文件，请运行以下命令：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

4. **配置 KSN 策略**

**如何在 Web Console 中管理 KSN 设置**

1. 在 Kaspersky Endpoint Security 策略的“**应用程序设置**”选项卡上，转到“**常规设置**”部分。
2. 选择“**卡巴斯基安全网络**”，然后在屏幕右侧指定以下设置：
   a. 将切换开关设置为 **使用卡巴斯基安全网络 (KSN) 已启用**。
   b. 在“**KSN 设置**”子部分中，选中“**使用扩展 KSN 模式**”复选框。
   c. 在“**KSN 代理服务器**”子部分中，选中以下复选框：
      - **使用管理服务器作为 KSN 代理服务器**
      - **如果 KSN 代理服务器不可用则使用卡巴斯基安全网络服务器**

   将根据配置的选项是否可用，从管理服务器或设备收集遥测。
3. 保存设置。

**如何通过命令行配置 KSN 设置**

要在扩展模式下启用 KSN，请运行以下命令：

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

5. **启用 KSN**

**如何在 Web Console 中启用 KSN**

1. 在主菜单中，单击管理服务器的名称。
2. 在打开的窗口中的“**常规**”选项卡上，选择“**KSN 代理**”部分。
3. 将切换开关设置为 **在管理服务器上启用 KSN 代理 已启用**。

4. 根据您使用的 KSN 基础设施解决方案，启用相应的切换开关：

   - “**使用卡巴斯基安全网络已启用**”。
   - “**使用卡巴斯基私人安全网络已启用**”，然后上传 KPSN 配置文件。

5. 保存设置。

6. **确保已成功建立与 Kaspersky Managed Detection and Response 的连接**

   以任意方便的方式检查 Kaspersky Managed Detection and Response 的状态。

## 如何验证 MDR 集成是否已启用

您可以通过以下方式检查 Kaspersky Managed Detection and Response 组件的运行状况：

- 在命令行中使用以下 命令：

  ```
  kesl-control --app-info
  ```

  Kaspersky Managed Detection and Response 集成显示为 **可用且正在运行** 状态。

- 在 MDR 控制台中，转到 **资产** 部分。设备显示为 **正常**（绿色）状态。

如果组件已禁用：

1. 更新应用程序反病毒数据库。
2. 确保卡巴斯基安全网络已启用并以扩展模式运行。
3. 检查 Kaspersky Endpoint Security 和 MDR 的授权许可密钥。
4. 确保 BLOB 文件已添加到策略中。
5. 验证 MDR 所需的组件是否正常工作。

# Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Linux 支持 Kaspersky Unified Monitoring and Analysis Platform 解决方案。*Kaspersky Unified Monitoring and Analysis Platform (KUMA)* 是针对组织 IT 基础设施的安全信息和事件管理 (SIEM) 解决方案。KUMA 可以在安全威胁造成危害之前检测、分析和减轻它们。

有关该解决方案的更多信息，请参阅Kaspersky Unified Monitoring and Analysis Platform 帮助。

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。有关计算机上事件的信息（遥测数据）被发送到 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 服务器。

该组件不适用于配备 Elbrus CPU 的设备。

# 如何配置 KUMA 集成

在配置 Kaspersky Unified Monitoring and Analysis Platform 整合之前：

- 允许在端口 443 和 1443 或 KUMA 收集器端配置的端口上进行连接。
- 如果您已购买单独的授权许可来使用此功能，请将 KUMA 授权许可密钥添加到应用程序。

  如果您通过包含 Kaspersky Unified Monitoring and Analysis Platform 的授权许可使用 Kaspersky Endpoint Security，则无需执行任何操作。

  如果应用程序在 Light Agent 模式下使用，则将 KUMA 授权许可密钥添加到 SVM。

**基本配置步骤**

1. **在 KUMA 中，配置收集器和规范化器。**

   如果您要使用客户端证书，请在 **传输** 选项卡上配置收集器时，选择 tcp 连接器类型。接下来，在 **高级设置**选项卡上，在 **TLS 模式** 下拉列表中，选择 **带客户端身份验证的自定义 PFX**。

2. **复制要连接的收集器地址**

   在 **资源** → **活动服务**部分的服务表中，以任何方便的方式复制并保存 **FQDN / IP 地址**和**端口**列中的值。

   如果使用 TLS 进行连接，请仅指定完全限定域名 (FQDN)。该设置值区分大小写。

3. **获取并处理 KUMA 服务器颁发的证书**

   对于与 KUMA 服务器的 UDP 连接，不支持使用证书来保护连接安全。

   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 KUMA 服务器。

   获取服务器证书（微服务 CA 证书），请参阅下载 CA 证书。要处理该证书，请按照将 PFX 证书转换为 PEM 格式一文中的步骤，将其转换为 DER 或 PEM 格式。

   为了加强保护，您还可以使用配置收集器时获得的客户端证书，请参阅步骤 1。

4. **配置 Kaspersky Unified Monitoring and Analysis Platform 整合设置**

   **如何在 Kaspersky Security Center Web Console 中配置 KUMA 整合**

   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
   2. 单击 Kaspersky Endpoint Security 策略的名称。

      策略属性窗口将打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择 **内置代理配置** → **KUMA 整合**。

5. 启用 **KUMA 整合已启用** 切换开关。

6. 添加 KUMA 服务器：

   a. 单击“**添加**”。

   这将打开一个表单，您可以在其中添加 KUMA 服务器。

   b. 选择连接到 KUMA 服务器的协议：**HTTP/HTTPS**、**TCP**、**UDP**。

   Kaspersky Endpoint Security 中用于连接到收集器的协议必须与 KUMA 中的连接器类型匹配：**http**、**tcp** 或 **udp**。

   如果您选择 **HTTP/HTTPS** 协议，默认情况下，应用程序使用 HTTPS 连接到 KUMA 服务器。要使用 HTTP，您需要在服务器地址中手动指定此协议（例如，`http://server.com`）。

   c. 请输入服务器地址（IPv4、IPv6）和用于连接到服务器的端口（默认指定端口 443）。

   您可以在 KUMA 控制台的连接器属性中查看服务器地址。有关 KUMA 连接器的更多信息，请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助。

   d. 单击“**确定**”。

   Kaspersky Endpoint Security 连接到列表中第一个 KUMA 服务器。如果连接失败，Kaspersky Endpoint Security 将连接到列表中的第二个 KUMA 服务器，依此类推。

7. 如有必要，在“**服务器连接设置**”块配置“**发送事件时的最大延时（秒）**”设置。指定的时间结束后，Kaspersky Endpoint Security 会尝试连接到同一个收集器；如果有多个收集器，则会连接到列表中的下一个收集器。默认设置是 30 秒。

8. 保存更改。

**如何在命令行上配置 KUMA 整合**

1. 要添加 KUMA 服务器，请运行以下命令：

```
kesl-control --set-settings 33 Servers.item_001.ServerAddress=<kuma server address>
Servers.item_001.Port=<kuma server port> Servers.item_001.ServerProtocol=<tcp|HTTPWithCompression|udp>
```

2. 要添加 KUMA 服务器证书，请运行以下命令：

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

3. 要配置集成设置，请运行以下命令：

```
kesl-control --set-settings 33 [<setting name>=<setting value>]
```

设置及其可能的值列于下表中。

4. 要添加用于连接到响应服务器的客户端证书，请运行以下命令：

```
kesl-control [-M] --add-kuma-client-certificate <path to the file>
```

5. 要启用与 EDR (KATA) 的集成，请运行以下命令：

```
kesl-control --start-task 33
```

Kaspersky Unified Monitoring and Analysis Platform 整合任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| `UseTls` | 启用或禁用服务器证书验证，以对与 KUMA 服务器的连接提供额外保护。 | `Yes` — 使用证书来进一步保护与 KUMA 服务器的连接。<br>`No`（默认）— 不使用证书来保护与 KUMA 服务器的连接。 |
| `UseClientCertificate` | 启用和禁用双向身份验证，以进一步保护与 KUMA 服务器的连接。<br>如果在 KUMA 服务器端启用了客户端证书验证，请在启动 Kaspersky Unified Monitoring and Analysis Platform 整合任务之前启用客户端证书的使用并添加客户端证书。 | `Yes` – 使用双向身份验证来进一步保护与 KUMA 服务器的连接。<br>`No`（默认值）— 不使用双向身份验证。 |
| `ConnectionTimeout` | 等待与 KUMA 服务器连接的最长时间（以秒为单位）。 | 默认值：`5`。 |
| **[Servers.item_#]** 部分包含 KUMA 服务器的设置。 | | |
| `ServerAddress` | KUMA 服务器地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>如果设置`UseTls=Yes`，则必须从购买授权许可时收到的证书中指定服务器的完全限定域名 (FQDN) 才能使用 KUMA。 | 默认值：`127.0.0.1`。 |
| `ServerPort` | 用于连接到 KUMA 服务器的端口。 | 默认值：`443`。 |
| `ServerProtocol` | 用于连接到 KUMA 服务器的端口。 | `tcp`（默认值）— 使用 TCP 协议连接到 KUMA 服务器。<br>`HTTPWithCompression` — 使用带事件压缩的 HTTP 协议连接到 KUMA 服务器。<br>`udp` — 使用 UDP 协议连接到 KUMA 服务器。<br>当选择 UDP 协议时，不支持使用证书提供连接保护（`UseTls`、`UseClientCertificate` 和 `ConnectionTimeout` 设置的值将被忽略），并且不会生成有关与 KUMA 服务器连接的事件。 |
| **[KumaTransferSettings]** 部分包含向 KUMA 服务器发送事件的设置。 | | |
| `EventTransferTimeMax` | 向 KUMA 服务器发送事件的最大延迟（以秒为单位）。 | 默认值：`30`。 |

**5 确保已成功建立与 Kaspersky Unified Monitoring and Analysis Platform 的连接**

使用任何方便的方式检查 KUMA 的状态。

# 如何验证 KUMA 整合是否已启动并正常运行

您可以通过以下方式测试 KUMA 组件：

- 在命令行中使用以下 命令：

```
kesl-control --app-info
```

与 KUMA 的整合显示为**可用且运行中**状态。

- 在 Web Console（OSMP Console）中：

  转到**威胁搜索**区域：事件列表中会显示相关设备状态为"已建立与 KUMA 的连接"的遥测事件。

- 在 Kaspersky Unified Monitoring and Analysis Platform 中：

  在 KUMA 控制台的主菜单中，转到**事件**区域：列表中会显示 Kaspersky Endpoint Security 遥测事件。

# 虚拟环境保护

Kaspersky Endpoint Security 支持 Light Agent 模式，可作为 Kaspersky Security for Virtualization Light Agent 的一部分运行。*Kaspersky Security for Virtualization Light Agent* 解决方案是一款集成解决方案，可为虚拟机提供全面保护，使其免受各种类型的信息安全威胁、网络攻击和网络钓鱼攻击。要使用此解决方案，您必须以 Light Agent 模式安装该应用程序。

启动 Light Agent 时，它会建立并维护与虚拟机 SVM 的连接 (Secure Virtual Machine）。Protection Server 部署在 SVM 上。*Protection Server* 是 Kaspersky Security for Virtualization Light Agent 解决方案组件，可扫描文件以查找病毒和其他恶意软件、更新反病毒数据库和管理授权许可密钥。Light Agent 将需要扫描的文件或其片段发送到 SVM。扫描结果适用于所有安装了 Light Agent 的虚拟机（SharedCache 技术）。此技术提高了解决方案效率，并能更快地应对威胁。

组织的基础架构可能包含许多安装了 Light Agent 的虚拟机和许多 SVM。集成服务器处理虚拟机和 SVM 之间的交互。*集成服务器*是 Kaspersky Security for Virtualization Light Agent 解决方案的一个组件，它生成可用 SVM 列表并将此数据传输到 Light Agent，参与 Light Agent 对 SVM 的发现，保护 Light Agent 和 SVM 之间的连接，并执行其他功能。

## 将 Light Agent 连接至 SVM

1. **获取可用 SVM 的列表**

   Light Agent 获取可用 SVM 列表。

2. **选择最佳 Protection Server (SVM)**

   Light Agent 根据 SVM 选择算法决定一个对连接最优的可用 Protection Server (SVM)。

3. **检查其他连接设置**

   Light Agent 检查其他 SVM 连接设置：标签、连接保护状态、授权许可涵盖的应用程序功能。

4. **将 Light Agent 连接至 SVM**

   Light Agent 与选定的 SVM 建立并保持连接。

# 如何配置 SVM 发现

您可以为 Light Agent 选择 SVM 检测方法之一：

- 使用 Integration Server (VIIS)。

  *集成服务器* 是一种解决方案组件，可支持 Kaspersky Security for Virtualization Light Agent 与虚拟基础架构交互，并生成可供连接的 SVM 列表。Light Agent 与Integration Server 建立连接并获取 SVM 地址列表。

集成服务器尤其适用于大型虚拟基础架构，因为它会自动平衡 SVM 之间的负载，获取有关可用 SVM 的信息，分析这些信息，并向 Light Agent 提供最适合连接的保护服务器 (SVM) 列表。

为了使 Light Agent 能够获取 SVM 列表，您只需输入 Integration Server 的地址。

- 使用 Integration Server 高可用性集群。

  Kaspersky Security for Virtualization Light Agent 6.4 支持部署 Integration Server 高可用性集群。当主要 Integration Server 发生故障时，SVM 和 Light Agent 会故障转移到备用 Integration Server，因此 Integration Server 高可用性集群可为虚拟环境提供不间断的保护。一个特殊的集群组件（*负载均衡器*）负责服务器故障转移。有关 Integration Server 高可用性集群的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

  要使 Light Agent 获取 SVM 列表，您需要输入安装了负载均衡器的设备地址。

- 使用 SVM 地址的列表。

  如果需要指定 Light Agent 想要连接的各个 SVM，您可以手动准备一个列表。

  您需要列出 Light Agent 可以连接的可用 SVM 的地址。

**如何在 Web Console 中配置 Light Agent 的 SVM 发现**

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **SVM 发现设置**。
5. 选择 SVM 发现方法。
   - “**使用 Integration Server**”。根据您的基础架构，输入 Integration Server 连接设置：
     - **单个 Integration Server**。输入 Integration Server 连接设置：设备的 IPv4 地址或完全限定域名 (FQDN)。
     - **Integration Server 高可用性集群**。输入集群中负载均衡器的 IP 地址和端口。
   - “**使用 SVM 地址的自定义列表**”。创建 Light Agent 可连接到的 SVM 的列表。指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。每个列表项必须另起一行，或者用分号 (`;`) 与前一项分隔开。

     在 SVM 地址列表中，仅指定与单个 IP 地址匹配的完全限定域名（FQDN）。使用与多个 IP 地址对应的完全限定域名可能会导致解决方案出错。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

**要在命令行中查看有关 Light Agent 连接到 Integration Server 的信息：**

1. 确保应用程序以 Light Agent 模式安装：

   ```
   kesl-control -V --ksvla-info
   ```

   该组件的状态必须为 **开启**。

2. 输出有关 Light Agent 与 Integration Server 的连接信息：

```
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。

**如何在命令行中查看 Light Agent 与 Integration Server 的连接信息**

1. 确保应用程序以 Light Agent 模式安装：

```
kesl-control -V --ksvla-info
```

该组件的状态必须为 **开启**。

2. 输出有关 Light Agent 与 Integration Server 的连接信息：

```
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 使用的 SVM 发现方法：使用 Integration Server 或使用 SVM 地址的自定义列表。
- 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。如果使用扩展 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。

# Light Agent 如何选择 SVM

组织的基础架构可能已部署多个 SVM，Light Agent 可以连接到这些 SVM。为了平衡网络和虚拟基础架构资源的负载，需要在 SVM 之间分发 Light Agent。

SVM 选择算法

Light Agent 可以应用以下 SVM 选择算法进行连接：标准算法（默认）和扩展算法。

| 标准算法 | 扩展算法 |
| --- | --- |
| 如果使用此算法，则在安装和启动后，虚拟机上的 Light Agent 选择连接到相对于 Light Agent 是*本地*的 SVM。<br>如果找不到适合连接的本地 SVM，则 Light Agent 会选择连接 Light Agent 数量最少的 SVM，而不管 SVM 在虚拟基础架构中的位置如何。<br>如果在 SVM 上为 Protection Server 启用了大型基础架构保护模式，则应用程序无法确定 SVM 相对于 Light Agent 是否为本地。在这种情况下，建议使用扩展 SVM 选择算法并选择 Integration Server 作为 SVM 发现方法。<br>SVM 是否为 Light Agent 的本地 SVM，取决于虚拟基础架构的类型。 | 如果应用此算法，您可以定义以下 SVM 选择设置：<br>• 在选择用于连接的 SVM 时是否考虑或忽略基础架构中的 SVM 位置<br>• 如果考虑 SVM 的位置，则确定 SVM 相对于 Light Agent 的本地性的方法<br>如果 Light Agent 忽略基础架构中 SVM 的位置，则 Light Agent 将能够连接到任何可供连接的 SVM。<br>如果 Light Agent 必须考虑基础架构中 SVM 的位置，则需要选择在确定相对于 Light Agent 的 SVM 位置时要考虑的 SVM 路径类型。SVM 是否为 Light Agent 的本地 SVM，取决于虚拟基础架构的类型。<br>如果 Light Agent 在选择连接哪个 SVM 时考虑 SVM 在基础架构中的位置，则 Light Agent 只能连接到本地的 SVM。<br>例如，如果您将 Hypervisor 集群指定为 SVM 路径类型，则部署在该 Hypervisor 集群上的所有 SVM 都将被视为对 Light Agent 而言是本地的，而 Light Agent 只能连接到其中一个 SVM。如果运行 Light Agent 的同一集群中没有 SVM 可供连接，则 Light Agent 将不连接到 SVM。<br>在选择 SVM 时，Light Agent 将考虑已连接的 Light Agent 数量，以确保在可供连接的 SVM 之间平均分布 Light Agent。<br>如果 Light Agent 使用扩展 SVM 选择算法，选择 SVM 地址列表作为 SVM 发现方法，并且 SVM 上启用了大型基础架构保护模式，则只有在忽略 SVM 路径的情况下才可以将 Light Agent 连接到该 SVM。 |
| **Basis Dynamix Enterprise** | |
| 在基于 Basis Dynamix Enterprise 的虚拟基础架构中，部署在与安装了 Light Agent 的虚拟机相同节点上的 SVM 会被视为 Light Agent 的本地 SVM。 | 在基于 Basis Dynamix Enterprise 的虚拟基础架构中，在以下情况之一，SVM 可被视为 Light Agent 的本地 SVM：<br>• SVM 与安装了 Light Agent 的虚拟机部署在同一节点上。<br>• SVM 与安装了 Light Agent 的虚拟机部署在同一区域中。<br>• SVM 与安装了 Light Agent 的虚拟机部署在同一数据中心中。 |
| **Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 和 Basis Dynamix Standard** | |
| 在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中，部署在与安装了 Light Agent 的虚拟机相同 Hypervisor 上的 SVM 会被视为 Light Agent 的本地 SVM。 | 在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中，在以下任何一种情况下，SVM 可被视为 Light Agent 的本地 SVM：<br>• SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上。<br>• SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群上。<br>• SVM 与安装了 Light Agent 的虚拟机部署在同一数据中心中。 |
| **OpenStack 和 VK Private Cloud SVM** | |

| 标准算法 | 扩展算法 |
| --- | --- |
| 在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中，您可以使用 Integration Server 配置文件 appsettings.json 中 `HypervisorSpecificSettings:Openstack` 部分的 `StandardAlgorithmSvmLocality` 参数，指定如何确定 SVM 相对于 Light Agent 的本地性。根据 Integration Server 的版本，文件位于以下路径之一：<br>• /var/opt/kaspersky/viis/common/ - 对于基于 Linux 的 Integration Server<br>• %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ - 对于基于 Windows 的 Integration Server<br>`StandardAlgorithmSvmLocality` 参数可以采用以下值：<br>• `ServerGroup` – 如果选择此值，只要 SVM 与安装了 Light Agent 的虚拟机位于同一服务器组内，则该 SVM 被视为 Light Agent 的本地 SVM。默认情况下使用此值。<br>• `Project` – 如果选择此值，只要 SVM 与安装了 Light Agent 的虚拟机部署在同一个 OpenStack 项目中，则该 SVM 被视为 Light Agent 的本地 SVM。<br>• `AvailabilityZone` – 如果选择此值，只要 SVM 与安装了 Light Agent 的虚拟机位于同一可用域内，则该 SVM 被视为 Light Agent 的本地 SVM。 | 在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中，在以下情况之一，SVM 可被视为 Light Agent 的本地 SVM：<br>• SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中。<br>• SVM 与安装了 Light Agent 的虚拟机部署在同一 OpenStack 项目中。<br>• SVM 与安装了 Light Agent 的虚拟机位于同一可用域中。 |

除了 SVM 连接算法之外，您还可以使用标签来管理 Light Agent 与 SVM 的连接。

*如何在 Web Console 中为 Light Agent 配置 SVM 选择算法*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **SVM 选择算法**。
5. 选择算法：
   - “**使用标准 SVM 选择算法**”。Light Agent 选择部署在同一个 Hypervisor 中的 SVM。
   - “**使用扩展 SVM 选择算法**”。Light Agent 选择部署在选定 SVM 路径类型的 SVM（默认情况下，**Hypervisor**）。
6. 如果需要，为扩展的 SVM 选择算法选择 SVM 路径：
   - “**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（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、 Astra Linux、 Numa vServer 或 Basis Dynamix Standard 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 或 VK Private Cloud 平台上运行的虚拟基础架构中）。
     - SVM 与安装了 Light Agent 的虚拟机托管在同一计算节点上（在 Basis Dynamix Enterprise 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（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机部署在同一 OpenStack 项目中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机位于同一区域中（在 Bais Dynamix Enterprise 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（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 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区中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机位于同一数据中心中（在 Dynamix Enterprise Basis 的虚拟基础架构中）。

  如果带有 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**”。Light Agent 会忽略用于连接 Protection Server 的 SVM 路径。Light Agents 考虑了其他标准：标签、连接到 SVM 的 Light Agents 数量等等。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

# 如何平衡 SVM 之间的 Light Agent 连接

多个 Light Agent 可以连接到一个 SVM。要平衡 Light Agent 连接，您可以指定单独的 SVM 列表。如果您使用 Integration Server 进行 SVM 发现，则可以使用“*标签*”平衡 Light Agent 与 SVM 的连接。也就是说，对于 Light Agent，您可以分配一个 SVM 列表，以便使用标签进行连接。为此，您必须为 Light Agent 分配一个标签，并在 SVM 设置中指定此标签。有关在 SVM 设置中指定标签的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

示例：Kaspersky Endpoint Detection and Response Optimum 解决方案部署在您的基础设施中，用于指定的虚拟机主机。在这种情况下，您可以分配“`[EDROptimum]`”标签到 Light Agent，使其连接到已添加 EDR Optimum（EDR Optimum 插件）授权许可密钥的 SVM。因此，您可以在带有 Light Agent 的虚拟机上使用 EDR Optimum 功能。当将 Light Agent 连接到没有 EDR Optimum 授权许可密钥的 SVM 时， Kaspersky Endpoint Detection and Response Optimum 功能不可用。

*如何在 Web Console 中将 SVM 连接标签分配给 Light Agent*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **SVM 连接标签**。
5. 选择“**使用连接标签**”复选框并输入 SVM 连接标签。
   对于标签，可以输入最长 255 个字符的文本字符串。可以使用除 `;` 字符外的任何字符。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

# 保护 Light Agent 与 SVM 之间的连接

您可以配置 Light Agent 和 Protection Server 之间的连接加密。为此，您需要在 SVM 上的 Protection Server 设置和 Light Agent 设置中启用 Light Agent 和 Protection Server 之间的数据通道加密。

启用了连接保护的 Light Agent 只能连接到在 Light Agent 与 Protection Server 之间启用了数据通道加密的 SVM。禁用了连接保护的 Light Agent 只能连接到禁用了通道加密或允许 Protection Server 与 Light Agent 之间建立不安全连接的 SVM。

有关在 Protection Server 上配置连接保护的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

使用加密保护连接可能会降低 Kaspersky Security for Virtualization Light Agent 的性能。

*如何在 Web Console 中配置 Light Agent 中的连接保护*

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **连接保护**。
5. 选择**加密 Light Agent 与 Protection Server 之间的数据通道**复选框。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

# 如何查看 Light Agent 的状态

在命令行中，您可以查看有关在 Light Agent 模式下使用的应用程序的以下信息：

- 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

## 查看在 Light Agent 模式下使用应用程序的设置信息

```
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：开 或 关。

  如果启用了 Light Agent 模式，应用程序将被用作 Kaspersky Security for Virtualization Light Agent 解决方案的一部分。

- VDI 保护模式：开 或 关。

  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的虚拟机的更新。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的虚拟机模板。

- 虚拟机类型：持久或非持久。
- 虚拟机角色：服务器 或 工作站。
- 虚拟机 ID – UUID。

## 查看 Light Agent 与 Integration Server 的连接信息

```
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。

如果您的基础架构具有基于 Linux 的高可用性集群，则会显示负载均衡器的地址和端口。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

查看 Light Agent 与 SVM 的连接信息

```
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 使用的 SVM 发现方法：使用 Integration Server 或使用 SVM 地址的自定义列表。
- 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。如果使用扩展 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。

# 最佳实践

部署 Kaspersky Endpoint Security for Linux 时，您可以使用本节中所述的建议来配置计算机保护并优化性能。有关处理计算机性能问题的更多信息，请参阅技术支持知识库。

# 优化应用程序的资源消耗

以默认设置运行的应用程序可能会影响某些设备的系统性能，因为应用程序和 Kaspersky Endpoint Security 使用相同的资源。

优化应用程序系统资源消耗的建议配置方案：

1. **根据基础设施中每个设备的角色，将设备归入管理组中。**

   对设备及其执行的功能进行清查，并根据这些功能将其归入不同的管理组中。例如，您可以设置一个包含 Web 服务器的管理组、另一个包含数据库服务器的管理组、还有一个包含用户工作站的管理组等。

2. **针对典型的服务器角色配置应用程序。**

   按照建议，根据设备在基础设施中的角色配置设备上的应用程序。

3. **分析试点设备的性能。**

   在每个管理组中挑选一到两个试点设备。对于每个设备，分析 Kaspersky Endpoint Security 对系统资源的使用情况以及对已安装应用程序的性能的影响情况。

4. **根据性能分析的结果，在试点设备上配置应用程序。**

   如果应用程序的性能显著下降，或 Kaspersky Endpoint Security 消耗的系统资源量对于操作系统和应用程序的运行产生重要影响，请按照建议来配置文件威胁防护和扫描任务。

   为了减少 Web 威胁防护、网络威胁防护 和 行为检测 组件对应用程序性能的影响，请优化这些组件的性能。

5. **在所有设备上配置应用程序。**

   如果上述步骤有助于提高试点设备的性能，请在其他同类型的设备上进行相同的更改。

# 设备端应用程序性能分析

扫描对象时，Kaspersky Endpoint Security 使用 CPU 资源、磁盘子系统输入/输出和 RAM。

查看应用程序的资源消耗信息

```
top -bn1|grep kesl
```

该命令必须在系统处于负载状态时执行。

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 列显示常驻内存量：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%。

要获取有关应用程序性能的信息，您还可以配置应用程序所用操作系统资源的指标收集。

如果 Kaspersky Endpoint Security 严重降低系统速度，您需要查明是哪些应用程序组件和任务正在占用系统资源。

为此，请在设备上执行以下实验：

1. **分析文件威胁防护任务（OAS 类型的任务）的资源消耗情况**

   通过这种方式，您可以了解性能问题是否与文件威胁防护任务或扫描任务（ODS 和 ContainerScan 类型的任务）有关，并遵循针对相关任务的建议。

   **如何分析文件威胁防护任务的资源消耗情况**

   1. 停止所有扫描和监控任务。
   2. 确保在调查期间未计划运行按需扫描任务（ODS 和 ContainerScan 类型的任务）：
      a. 获取所有应用程序任务的列表：

      ```
      kesl-control --get-task-list
      ```

      b. 获取所有 ODS 和 ContainerScan 类型任务的计划设置：

      ```
      kesl-control --get-schedule <task ID |name>
      ```

      如果命令输出为 `RuleType=Manual`，则任务只能手动启动。

      c. 对于所有 `RuleType` 不同于 `Manual` 的任务，请更改计划：

      ```
      kesl-control --set-schedule <task ID |name> RuleType=Manual
      ```

   3. 启用生成高详细级别的应用程序跟踪文件：

   ```
   kesl-control --set-app-settings TraceLevel=Detailed
   ```

   4. 如果文件威胁防护任务未运行，请启动该任务：

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

   5. 以导致性能问题的相同模式对系统施加负载。几个小时就足够了。

6. 分析生成的跟踪文件。默认情况下，跟踪文件存储在 /var/log/kaspersky/kesl/ 目录中。

> 在负载情况下，应用程序会将大量信息写入跟踪文件；但仅保留 10 个文件（每个文件的大小为 500 MB），这意味着旧信息会被覆盖。

如果性能和资源消耗问题仍然存在，您可能需要优化文件威胁防护。

如果性能和资源消耗问题不再出现，则这些问题最可能由按需扫描任务（ODS 和 ContainerScan 类型的任务）或行为检测任务引起。您需要优化扫描任务或分析行为检测任务的性能。

7. 禁用创建应用程序跟踪文件：

```
kesl-control --set-app-settings TraceLevel=None
```

2. **分析行为检测任务（Behavior_Detection 类型的任务）的资源使用情况。**

通过这种方式，您可以了解性能问题是否与行为检测任务或扫描任务（ODS 和 ContainerScan 类型的任务）有关，并遵循针对相关任务的建议。

**如何分析行为检测任务的资源使用情况**

1. 停止所有扫描和监控任务。
2. 确保在调查期间未计划运行按需扫描任务（ODS 和 ContainerScan 类型的任务）：
   a. 获取所有应用程序任务的列表：

   ```
   kesl-control --get-task-list
   ```

   b. 获取所有 ODS 和 ContainerScan 类型任务的计划设置：

   ```
   kesl-control --get-schedule <task ID|name>
   ```

   如果命令输出为 `RuleType=Manual`，则任务只能手动启动。

   c. 对于所有 `RuleType` 不同于 `Manual` 的任务，请更改计划：

   ```
   kesl-control --set-schedule <task ID|name> RuleType=Manual
   ```

3. 启用生成高详细级别的应用程序跟踪文件：

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. 如果行为检测任务未运行，请启动该任务：

```
kesl-control --start-task 20
```

5. 以导致性能问题的相同模式对系统施加负载。几个小时就足够了。
6. 分析生成的跟踪文件。默认情况下，跟踪文件存储在 /var/log/kaspersky/kesl/ 目录中。

在负载情况下，应用程序会将大量信息写入跟踪文件；但仅保留 10 个文件（每个文件的大小为 500 MB），这意味着旧信息会被覆盖。

如果性能和资源消耗问题仍然存在，您可能需要优化行为检测。

如果性能和资源消耗问题不再出现，则这些问题最可能由按需扫描任务（ODS 和 ContainerScan 类型的任务）引起。这意味着您需要优化这些任务。

7. 禁用创建应用程序跟踪文件：

```
kesl-control --set-app-settings TraceLevel=None
```

### 3 识别最常扫描的对象

您可以从扫描中排除无危险的频繁扫描对象和文件，以便优化文件威胁防护和扫描任务的性能。

确定扫描次数最多的对象是否危险。例如，如果写入操作由受信任进程执行，则数据库文件、目录和日志文件可被视为是安全的。如有任何困难，请联系技术支持。

**如何识别最常扫描的对象**

1. 获取扫描次数最多的对象列表：

```
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。

如果需要从根目录 / 开始，聚合向下到特定深度的子目录中的对象扫描统计信息，您可以向命令添加 `cut -d/ -f 1-X`，其中 X 是嵌套深度。例如：

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c |
sort -k1 -n -r|less
```

2. 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。获取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 $10}' |
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。

如果需要从根目录 / 开始，聚合向下到特定深度的子目录中的对象扫描统计信息，您可以向命令添加 `cut -d/ -f 1-X`，其中 X 是嵌套深度。例如：

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
tr -d ',' |  cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

### 4 识别 Kaspersky Endpoint Security 检测到启动最频繁的进程

您可以从扫描中排除无危险的、频繁启动的进程，以便优化行为检测的性能。

**如何识别最常启动的进程**

请执行命令：

```
kesl-control --get-statistic --processes
```

此命令输出 Kaspersky Endpoint Security 最频繁检测到启动的进程列表，以及这些进程的启动次数。

5 **识别发生文件操作拦截次数最多的路径**

您可以从文件操作拦截中排除目录，以便优化文件威胁防护和扫描任务的性能。

**如何获取有关文件操作拦截的信息**

您可以通过以下方式获取有关文件操作拦截的信息：

- 获取文件威胁防护组件最常扫描的文件的统计信息：

  ```
  kesl-control --get-statistic --files
  ```

  此命令可显示过去 24 小时的文件操作拦截统计信息。

- 使用应用程序跟踪文件进行更详细的分析。通过分析跟踪文件，可以获取应用程序拦截的文件列表，并识别与大量文件操作拦截相关的路径。

  默认情况下，应用程序不会生成跟踪文件。

  启用跟踪文件创建

  ```
  kesl-control --set-app-settings TraceLevel=Detailed
  ```

  > 启用跟踪可能会影响整体系统性能。当您不再需要跟踪文件时，建议禁用跟踪。

  禁用跟踪文件创建

  ```
  kesl-control --set-app-settings TraceLevel=None
  ```

- 获取已拦截文件的列表：

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'|sort | uniq -c | sort -k1 -n -r
  ```

  如果需要从根目录 / 开始，聚合向下到特定深度的子目录中的文件操作拦截统计信息，您可以向命令添加 `cut -d/ -f 1-X`，其中 X 是嵌套深度。例如：

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
  ```

> 您可以在命令行上分析应用程序的性能。如果设备受 Kaspersky Security Center 策略管理，请在进行调查时允许本地任务管理。

# 针对文件威胁防护任务和扫描任务的建议

一般建议

**扫描排除项**

扫描排除有助于平衡系统安全性和性能。

我们建议将以下内容排除在扫描范围之外：

- 数据库的数据文件和索引文件。卡巴斯基的病毒专家认为，病毒不会通过此类文件传播。
- 最常扫描对象列表中的安全对象。

您可以通过文件路径（还可以指定挂载类型）、文件掩码、威胁类型和执行文件操作的进程路径配置排除项。

> 应用程序不会扫描排除在扫描范围之外的对象，但文件操作依然有轻微延迟，因为应用程序仍会执行文件操作拦截和阻止操作。如果您需要避免哪怕是最轻微的延迟，建议配置文件操作拦截排除项。

如何配置排除项：

- 您可以使用 Web Console 或管理控制台在策略中配置文件威胁防护排除项，或者在设备本地使用命令行进行配置。
- 您可以在 Kaspersky Security Center 的任务设置中为 ODS 和 ContainerScan 类型的扫描任务配置排除项，也可以在设备本地使用命令行进行配置。

  > 为一个扫描任务配置的排除项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。

在命令行上配置的文件威胁防护排除项示例

递归排除 /tmp/logs 目录及其所有子目录和文件

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

按掩码排除 /tmp/logs 目录中的一个或多个特定文件

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

使用递归掩码排除 /tmp 目录及子目录中扩展名为 .log 的所有文件

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

**文件操作拦截排除项**

在执行文件威胁防护和扫描任务期间，应用程序仍可能会拦截排除在扫描范围之外的文件。应用程序会拦截文件操作事件，并在这些事件得到处理之前阻止相关操作。扫描完成后，应用程序可以：

- 解除阻止并允许操作。
- 阻止操作并执行保护或验证设置中指定的操作。

拦截事件需要时间，这会影响其他应用程序和操作系统的性能。

如果您的操作系统支持 fanotify 技术并满足要求，请为应用程序配置可更新内核模块。可更新内核模块包含在应用程序的分发包中。可更新内核模块可以优化文件操作拦截。

要将某个目录中的文件不仅从扫描中排除，还从拦截中排除，请为挂载点配置排除项（全局排除项）。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。

您可以使用 Web Console、管理控制台或命令行查看设备上检测到的挂载点列表。该列表显示挂载点是否已添加到扫描排除项的信息。

卡巴斯基专家建议在以下情况下使用全局排除：

- 与已挂载的远程资源（例如 NFS 或 SMB）的连接速度缓慢。
- 即使是轻微的滞后也无法接受。

您可以指定挂载点类型（Local、AllRemoteMounted、Mounted:NFS、Mounted:SMB 或 Mounted:Custom）或特定挂载点。应用程序不会监控已排除的范围。

要保护共享网络资源，请在物理存储资源的设备上使用 Kaspersky Endpoint Security 应用程序。

如果您使用可更新内核模块进行系统事件拦截，则可以从拦截中排除设备上挂载的单个本地或远程目录，而不只是整个挂载点。

如果您使用 fanotify 进行系统事件拦截，则全局排除项不适用于不是挂载点的路径。

您可以使用 Web Console 或管理控制台在策略中配置全局排除项，或者在设备本地使用命令行进行配置。

### 使用命令行为 /tmp 目录配置全局排除项的示例

*要将 /tmp 目录中的所有文件排除在拦截范围之外：*

1. 如果您使用 fanotify 进行系统事件拦截，请检查 /tmp 目录是否为挂载点：

   ```
   mount
   ```

如果 mount 命令的输出中没有该目录：

a. 创建挂载点：

```
mount --bind /tmp/ /tmp
```

b. 将以下行添加到 /etc/fstab 文件，以使新创建的挂载点在系统重启后仍保留：

```
/tmp /tmp none defaults,bind 0 0
```

如果您使用可更新内核模块进行系统事件拦截，请跳过此步骤。

2. 将 /tmp 目录添加到全局排除项：

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
```

3. 重启应用程序以应用全局排除项：

```
systemctl restart kesl
```

**限制应用程序的 RAM 使用量**

您可以限制 Kaspersky Endpoint Security 使用文件威胁防护组件扫描文件以及执行 ODS 和 ContainerScan 类型的扫描任务时使用的 RAM 量。

对于具有大量 RAM（超过 5 GB）的系统，限制内存使用可能会有用。

默认情况下，该应用程序最多可使用的 RAM 为 8192 MB。您可以调整应用程序使用的 RAM 大小：

- 在策略中，使用“**扫描任务的内存使用限制 (MB)**”设置。
- 在设备本地使用 kesl.ini 配置文件中的 `ScanMemoryLimit` 设置。

如果指定的值小于 2 MB，应用程序使用最小值 (2 MB)。如果指定的值大于设备上的可用 RAM 容量，则应用程序最多可使用 25% RAM。该值无法更改。

> 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。

文件威胁防护的其他建议

**仅在打开文件时扫描**

将文件扫描模式更改为仅在打开文件时扫描文件。默认情况下，当有人试图打开文件时，应用程序会扫描该文件；如果文件已被修改，当有人试图关闭该文件时，应用程序会再次扫描该文件。

您可以在文件威胁防护设置中更改文件扫描模式：

- 在策略中，使用 Web Console 或管理控制台将**文件威胁防护模式**设置为“**打开时**”。
- 在设备本地：

```
kesl-control --set-set 1 ScanByAccessType=Open
```

文件打开后对其所做的更改，在下次打开文件后才会被扫描。

**扫描压缩文件**

确保已禁用压缩文件扫描（默认设置）。扫描压缩文件会影响性能，因为在将文件解压到 /tmp 临时目录并进行扫描时，对压缩文件的访问会被阻止。压缩文件的定义包括传统的压缩文件以及 .jar 等格式的打包对象。

您可以使用 Web Console 或管理控制台（**扫描压缩文件**设置）或在设备本地使用命令行（ `ScanArchived` 设置）来启用或禁用压缩文件扫描。

**扫描从网络目录复制的文件**

为从网络目录复制的文件配置扫描排除项。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_#]` 部分来按进程配置排除项。

扫描任务的其他建议

**任务启动计划**

计划扫描任务，避免任务重叠。该应用程序允许同时运行扫描任务，但这可能会显著增加资源消耗。在设备本地或 Kaspersky Security Center 中检查所有 ODS 和 ContainerScan 任务的计划。

在服务器负载最低的时间段内运行扫描。

**扫描远程目录**

确保扫描任务的范围不包括通过 SMB 或 NFS 挂载在设备上的任何远程目录。

建议直接在提供资源的设备上扫描此类目录。如果不可行，则不要在运行关键服务的服务器上运行扫描，因为此类任务可能会花费很长时间（取决于连接速度和文件数量）。

**使用全局排除项和文件威胁防护排除项**

确保已为恶意软件扫描任务启用以下设置：

- **使用全局排除项**（`UseGlobalExclusions`），以从扫描中排除全局排除项中指定的挂载点。
- **使用文件威胁防护排除项**（`UseOASExclusions`），以在扫描期间使用已配置的文件威胁防护排除项。

默认情况下，这两个设置均已启用。

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/`。

# 针对 Web 威胁防护任务和网络威胁防护任务的建议。

一般建议

### 操作系统的 Firewall

如果系统已配置了自己的网络规则（或 firewalld 规则）且包含 Drop 策略，为确保应用程序正常工作，请添加一条 accept 规则以允许来自本地设备（环回接口）的传入连接：

```
iptables 命令示例
iptables -A INPUT -i lo -j ACCEPT
```

### 受监控网络端口列表

限制应用程序监控的网络端口列表。默认情况下，应用程序仅监控所选网络端口。如果设备使用 SMB 连接，请确保使用默认值：

- 在 Web Console 或管理控制台中的策略中：在网络流量扫描设置中，已选中“**仅监控所选网络端口**”选项。
- 在设备本地：`MonitorNetworkPort` 网络流量扫描设置设为“`Selected`”。

### 将应用程序与 HAProxy 结合使用

将应用程序与 HAProxy 负载均衡器结合使用时：

1. 打开 /var/opt/kaspersky/kesl/common/kesl.ini 配置文件，创建 `[Environment]` 部分并添加 `TcpSynInterceptDisabled=1` 设置。
2. 重启应用程序：

```
systemctl restart kesl
```

### 将应用程序与 Kubernetes 结合使用

为了使 Web 威胁防护和网络威胁防护组件能够与使用 Calico 和 Cilium 网络插件的 Kubernetes 集群协同工作，请管理 kesl.ini 配置文件中的 `WtpFwMark`、`NtpFwMark`、`BypassFwMark` 和 `BypassNflogMark` 设置。

出现“应用程序模块完整性检查失败”错误时该怎么办

Web 威胁防护建议

### 证书验证策略

默认情况下，Web 威胁防护组件会解密并扫描通过加密连接发送的网络流量。在此过程中，组件会利用互联网进行验证，并下载验证证书所需的缺失证书链。

如果设备无法直接访问互联网，请执行以下操作之一：

- 在网络流量扫描设置中选择本地证书验证方法：
  - 在策略中，使用 Web Console 或管理控制台将**证书验证策略**设置为“**本地检查**”。
  - 在设备本地使用命令行：

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  应用程序不使用互联网来验证证书。
- 配置通过代理服务器访问互联网：
  - 在策略中，使用 Web Console 或 管理控制台：配置代理设置。
  - 在设备本地使用命令行：

    启用使用需要身份验证的代理服务器

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<user name>:<password>@<IP address of the proxy server>:<port number>
    ```

    启用使用无需身份验证的代理服务器

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<IP address of the proxy server>:<port number>
    ```

网络威胁防护建议

### 与 REDIRECT 规则的兼容性

为确保网络威胁防护组件的拦截规则与 REDIRECT 规则兼容（例如，从端口 443 重定向到 8443）：

1. 删除该规则：

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

2. 将其替换为以下规则：

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports
8443
iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT
--to-destination :8443
```

# 行为检测建议

我们建议将行为检测组件扫描频率最高的进程的活动排除在扫描范围之外。

*要找出哪些进程启动最频繁，请运行以下命令：*

```
kesl-control --get-statistic --processes
```

此命令输出 Kaspersky Endpoint Security 最频繁检测到启动的进程列表，以及这些进程的启动次数。

您可以使用 Web Console 或管理控制台在策略中配置排除项，或者在设备本地使用 命令行进行配置。

默认情况下，仅指定的进程会被排除在扫描之外；行为检测会继续扫描被排除进程的子进程。

在命令行中配置排除项的示例

将 my_program1 和 my_program2 的活动排除在扫描范围之外

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0001.ProgramPath=/bin/my_program2
```

将 my_program1 及其子进程的活动排除在扫描范围之外

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0000.ApplyToDescendants=Yes
```

# 与卡巴斯基解决方案的互操作性

Kaspersky Endpoint Security 应用程序支持与某些卡巴斯基解决方案的互操作性。为实现应用程序的最佳互操作性，请遵循本节中的指南。

## Kaspersky Security Center Linux

将 Kaspersky Endpoint Security for Linux 与 Kaspersky Security Center Linux 配合使用时，建议使用本文中所述的设置。

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 文件威胁防护 | Enabled | 添加保护排除项：<br>• `/opt/kaspersky/klnagent/sbin/klnagent`<br>• `/opt/kaspersky/klnagent64/sbin/klnagent`<br>• `/var/lib/postgresql/<PostgreSQL version>` |
| 恶意软件扫描 | Enabled | |
| 可移动驱动器扫描 | 已禁用 | – |
| 行为检测 | Enabled | 使用默认设置。 |
| 网络威胁防护 | Enabled | 选择 eBPF 网络流量拦截模式<br>`NetInterceptorMode=UseEBPF` |
| Web 威胁防护 | Enabled | 使用默认设置。 |
| 反加密 | 已禁用 | – |
| 容器扫描 | 已禁用 | – |
| 清查 | 已禁用 | – |
| 设备控制 | 已禁用 | – |
| 应用程序控制 | 已禁用 | – |
| 防火墙 | 已禁用 | – |
| Web 控制 | 已禁用 | – |
| 系统完整性监控 | Enabled | 添加扫描范围：<br>• /etc<br>• /opt/kaspersky/kesl/<br>• /opt/kaspersky/ksc64 |
| 系统完整性检查 | 已禁用 | – |
| Endpoint Detection and Response Expert (on-premises) | Enabled | 使用默认设置。 |
| Endpoint Detection and Response Expert (cloud) | 已禁用 | – |
| Managed Detection and Response | Enabled | 使用默认设置。 |
| Network Detection and Response (KATA) | 已禁用 | – |
| 与 KUMA 的整合 | 已禁用 | – |
| Sandbox | 已禁用 | – |
| 响应操作 | 存在一些限制 | 对于响应操作，您不能排除 Kaspersky Endpoint Security for Linux 所需的对象以及关键系统对象。启动响应操作时，请确保这些操作不会中断系统和您使用的应用程序。 |
| 图形界面 | 未设置 | – |
| Kaspersky Endpoint Security for Linux 管理 Web 插件 | 已安装 | 使用默认设置。 |
| Kaspersky Endpoint Security for Linux MMC 管理插件 | 已安装 | 使用默认设置。 |
| 网络代理 | 已安装 | 使用默认设置。 |
| 文件操作拦截机制 | 基于 fanotify 的系统拦截机制 | 使用默认设置。 |
| 系统事件遥测源 | eBPF+auditd | `TelemetrySource=Default` |
| 漏洞利用防御 | 已禁用 | – |
| 使用卡巴斯基安全网络 | Enabled | 使用默认设置。 |
| 邮件威胁防护 | Enabled | 使用默认设置。 |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| BadUSB 攻击防护 | 已禁用 | – |
| 全局排除项 | 已配置 | 如果您使用快速安装脚本安装 Kaspersky Security Center，请将挂载点添加到排除项：<br>`/var/lib/postgresql/<PostgreSQL version>/main`<br>其中，`<PostgreSQL version>` 是您使用的 PostgreSQL 数据库管理系统的版本号。 |

# Network Detection and Response (KATA)

将 Kaspersky Endpoint Security for Linux 与 Network Detection and Response (KATA) 结合使用时，我们建议使用本文中所述的设置。

另请参阅 Kaspersky Anti Targeted Attack (KATA) Platform 解决方案文档。

## 安装 Sensor 组件的服务器上的 Kaspersky Endpoint Security for Linux 设置

Sensor 服务器的推荐设置

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 文件威胁防护 | Enabled | 添加保护排除项：<br>• `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-collector/spool`<br>• `[container-name:*kata_scanner*]/data/var/opt/kaspersky/apt-collector/spool`<br>• `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool`<br>• `[container-name:*preprocessor_icap*]/tmp/content`<br>• `[container-name:*preprocessor_span*]/tmp/suricata`<br>• `[container-name:*preprocessor_span*]/mnt/kaspersky/nta`<br>• `[container-name:*preprocessor_smtp*]/tmp/`<br>• `[container-name:*preprocessor_pop*]/tmp/`<br>• `[container-name:*sandbox_scan*]/tmp/`<br>• `[container-name:*]/var/log/kaspersky` |
| 恶意软件扫描 | 已禁用 | – |
| 可移动驱动器扫描 | 已禁用 | – |
| 行为检测 | Enabled | 使用默认设置。 |
| 网络威胁防护 | 已禁用 | – |
| Web 威胁防护 | 已禁用 | – |
| 反加密 | 已禁用 | – |
| 容器扫描 | Enabled | 启用容器监控以实时扫描正在运行的容器和命名空间<br>`NamespaceMonitoring=Yes` |
| 清查 | 已禁用 | – |
| 设备控制 | 已禁用 | – |
| 应用程序控制 | 已禁用 | – |
| 防火墙 | 已禁用 | – |
| Web 控制 | 已禁用 | – |
| 系统完整性监控 | 已禁用 | – |
| 系统完整性检查 | 已禁用 | – |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| Endpoint Detection and Response Expert (on-premises) | 已禁用 | – |
| Endpoint Detection and Response Expert (cloud) | 已禁用 | – |
| Managed Detection and Response | 已禁用 | – |
| Network Detection and Response (KATA) | 已禁用 | – |
| 与 KUMA 的整合 | 已禁用 | – |
| Sandbox | 已禁用 | – |
| 响应操作 | 已禁用 | – |
| 图形界面 | 未设置 | – |
| 网络代理 | 已安装 | 使用默认设置。 |
| 文件操作拦截机制 | 基于 fanotify 的系统拦截机制 | 使用默认设置。 |
| 系统事件遥测源 | eBPF+auditd | `TelemetrySource=Default` |
| 漏洞利用防御 | 已禁用 | – |
| 使用卡巴斯基安全网络 | Enabled | 使用默认设置。 |
| 邮件威胁防护 | 已禁用 | – |
| BadUSB 攻击防护 | 已禁用 | – |
| 跟踪文件 | – | 将跟踪文件的目录更改为 `/var/log/kaspersky` 目录之外的目录。例如，使用 `/var/log/kesl` 目录。 |
| 全局排除项 | 已配置 | 排除以下挂载点：<br>• `/apt_spool`<br>• `/storage`<br>• `/var/lib/postgresql`<br>• `/var/lib/clickhouse`<br>• `/tmp/apttmp/*`<br>• `/tmp/suricata/*`<br>• `/tmp/traffic/*`<br>• `/tmp/apt_certs/*`<br>对 tmp/apttmp/*、/tmp/suricata/*、/tmp/traffic/* 和 /tmp/apt_certs/* 挂载点的排除适用于 8.0 及更早版本的 NDR (KATA) 服务器。<br>• `/varog/kaspersky`<br>• `/var/opt/kaspersky`<br>• `/data`<br>• `/data/volumes/dumps` |

# 安装 Central Node 组件的服务器上的 Kaspersky Endpoint Security for Linux 设置

Central Node 服务器的推荐设置

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 文件威胁防护 | Enabled | 添加保护排除项：<br>• [container-name:*edr_synchronizer*]/tmp/<br>• [container-name:*ids_alert_syncer*]/tmp/<br>• [container-name:kata_product_main_1_kata_scanner]/storage<br>• [container-name:kata_product_main_1_postgresql_server]/var/lib/postgresql<br>• [container-name:kata_product_main_1_clickhouse]/var/lib/clickhouse<br>• [container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool<br>• [container-name:*kata_scanner*]/var/opt/kaspersky/apt-agents<br>• [container-name:*kata_scanner*]/var/lib/nginx/body<br>• [container-name:*kata_scanner*]/apt_spool<br>• [container-name:*kata_scanner*]/tmp/<br>• [container-name:*kafka*]/tmp/<br>• [container-name:*ksn_proxy*]/tmp/<br>• [container-name:*preprocessor_smtp*]/tmp/<br>• [container-name:*preprocessor_pop*]/tmp/<br>• [container-name:*preprocessor_icap*]/tmp/<br>• [container-name:*preprocessor_span*]/tmp/<br>• [container-name:*sandbox_scan*]/tmp/<br>• [container-name:*statistics_clickhouse_importer*]/tmp/<br>• [container-name:*updates_consistency_checker*]/tmp/<br>• [container-name:*web_backend*]/tmp/<br>• [container-name:*]/var/opt/kaspersky<br>• /tmp/<br>• /var/log/kaspersky |
| 恶意软件扫描 | 已禁用 | – |
| 可移动驱动器扫描 | 已禁用 | – |
| 行为检测 | Enabled | 使用默认设置。 |
| 网络威胁防护 | 已禁用 | – |
| Web 威胁防护 | 已禁用 | – |
| 反加密 | 已禁用 | – |
| 容器扫描 | Enabled | 启用容器监控以实时扫描正在运行的容器和命名空间<br>`NamespaceMonitoring=Yes` |
| 清查 | 已禁用 | – |
| 设备控制 | 已禁用 | – |
| 应用程序控制 | 已禁用 | – |
| 防火墙 | 已禁用 | – |
| Web 控制 | 已禁用 | – |
| 系统完整性监控 | 已禁用 | – |
| 系统完整性检查 | 已禁用 | – |
| Endpoint Detection and Response Expert (on-premises) | 已禁用 | – |
| Endpoint Detection and Response Expert (cloud) | 已禁用 | – |
| Managed Detection and Response | 已禁用 | – |
| Network Detection and Response (KATA) | 已禁用 | – |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 与 KUMA 的整合 | 已禁用 | – |
| Sandbox | 已禁用 | – |
| 响应操作 | 已禁用 | – |
| 图形界面 | 未设置 | – |
| 网络代理 | 已安装 | 使用默认设置。 |
| 文件操作拦截机制 | 基于 fanotify 的系统拦截机制 | 使用默认设置。 |
| 系统事件遥测源 | eBPF+auditd | `TelemetrySource=Default` |
| 漏洞利用防御 | 已禁用 | – |
| 使用卡巴斯基安全网络 | Enabled | 使用默认设置。 |
| 邮件威胁防护 | 已禁用 | – |
| BadUSB 攻击防护 | 已禁用 | – |
| 跟踪文件 | – | 将跟踪文件的目录更改为 `/var/log/kaspersky` 目录之外的目录。例如，使用 `/var/log/kesl` 目录。 |
| 全局排除项 | 已配置 | 将挂载点添加到排除项：<br>• `/apt_spool`<br>• `/storage`<br>• `/var/lib/postgresql`<br>• `/var/lib/clickhouse`<br>• `/tmp/apttmp/*`<br>• `/tmp/suricata/*`<br>• `/tmp/traffic/*`<br>• `/tmp/apt_certs/*`<br>对 tmp/apttmp/*、/tmp/suricata/*、/tmp/traffic/* 和 /tmp/apt_certs/* 挂载点的排除适用于 8.0 及更早版本的 NDR (KATA) 服务器。<br>• `/var/log/kaspersky`<br>• `/var/opt/kaspersky`<br>• `/data` |

# Kaspersky Unified Monitoring and Analysis Platform

将 Kaspersky Endpoint Security for Linux 与 Kaspersky Unified Monitoring and Analysis Platform 一起使用时，建议使用本文所述的设置。

建议设置

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 文件威胁防护 | Enabled | 添加保护排除项：<br>• `/opt/kaspersky/kuma`<br>• `/opt/kaspersky/klnagent/sbin/klnagent`<br>• `/opt/kaspersky/klnagent64/sbin/klnagent` |
| 恶意软件扫描 | 已禁用 | – |
| 可移动驱动器扫描 | 已禁用 | – |
| 行为检测 | Enabled | 从扫描中排除该进程<br>`/opt/kaspersky/kuma` |
| 网络威胁防护 | Enabled | 禁用阻止受感染设备<br>`BlockAttackingHosts=No` |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| Web 威胁防护 | 已禁用 | – |
| 反加密 | 已禁用 | – |
| 容器扫描 | 已禁用 | – |
| 清查 | 已禁用 | – |
| 设备控制 | 已禁用 | – |
| 应用程序控制 | 已禁用 | – |
| 防火墙 | 已禁用 | – |
| Web 控制 | 已禁用 | – |
| 系统完整性监控 | 已禁用 | – |
| 系统完整性检查 | 已禁用 | – |
| Endpoint Detection and Response Expert (on-premises) | 已禁用 | – |
| Endpoint Detection and Response Expert (cloud) | 已禁用 | – |
| Managed Detection and Response | 已禁用 | – |
| Network Detection and Response (KATA) | 已禁用 | – |
| 与 KUMA 的整合 | 已禁用 | – |
| Sandbox | 已禁用 | – |
| 响应操作 | 已禁用 | – |
| 图形界面 | 未设置 | – |
| 网络代理 | 已安装 | 使用默认设置。 |
| 文件操作拦截机制 | 基于 fanotify 的系统拦截机制 | 使用默认设置。 |
| 系统事件遥测源 | eBPF+auditd | `TelemetrySource=Default` |
| 漏洞利用防御 | 已禁用 | – |
| 使用卡巴斯基安全网络 | Enabled | 使用默认设置。 |
| 邮件威胁防护 | 已禁用 | – |
| BadUSB 攻击防护 | 已禁用 | – |

# 应用程序组件参考

## 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 <prefix of command group>
```

其中 `<prefix of command group>` 可以采用以下值：

- `-A`：用于管理应用程序控制的命令
- `-B`：用于管理备份区的命令
- `-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`：用于查看当前应用程序事件的命令
- `-F`：用于防火墙管理的命令
- `-H`：用于管理被反加密勒索和网络威胁防护阻止的设备的命令
- `-J`：用于管理系统性能指标获取的命令
- `-L`：用于管理授权许可密钥的命令
- `-M`：用于管理 Kaspersky Endpoint Security 应用程序与 Kaspersky Unified Monitoring and Analysis Platform 的集成设置的命令
- `-N`：用于管理加密连接扫描设置的命令
- `-Q`：用于管理隔离区的命令
- `-R`：用于管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert (cloud) 和 Kaspersky Endpoint Detection and Response Optimum 的集成设置的命令
- `-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`：Light Agent 模式下的应用程序命令

- `-W`：用于显示应用程序事件日志中的事件的命令
- `-X`：用于管理 Kaspersky Endpoint Security 应用程序与 沙盒 的集成设置的命令

在 bash shell 中，您可以为 kesl-control 命令启用自动补全。

在当前 bash 会话中为 kesl-control 命令启用自动补全

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

为所有新的 bash 会话启用自动补全

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

# 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。

> 如果应用程序以标准模式或 EDR Agent 模式运行，则可以使用用于添加或移除授权许可密钥的命令。如果应用程序在 Light Agent 模式下使用，密钥管理命令会返回错误。

## 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用于激活应用程序的密钥，以及用于激活授权许可未涵盖组件的密钥。您不需要在命令中指定密钥的类型。

使用密钥文件添加授权许可密钥

```
kesl-control [-L] --add-active-key <key file path>
```

使用激活码添加授权许可密钥

```
kesl-control [-L] --add-active-key <activation code>
```

其中：

`<key file path>` 是密钥文件的路径。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>` 是激活码。

使用 /home/test/00000001.key 文件作为活动密钥添加密钥的示例

```
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用于激活应用程序的密钥，以及用于激活授权许可未涵盖组件的密钥。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。

使用密钥文件添加备用授权许可密钥

```
kesl-control [-L] --add-reserve-key <key file path>
```

使用激活码添加备用授权许可密钥

```
kesl-control [-L] --add-reserve-key <activation code>
```

其中：

`<key file path>` 是密钥文件的路径。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>` 是激活码。

使用 `/home/test/00000002.key` 文件添加备用密钥的示例

```
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。

删除活动的 EDR Optimum 授权许可密钥

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

删除活动的 KUMA 授权许可密钥

```
kesl-control [-L] --remove-active-key [--kuma]
```

删除活动的 MDR 授权许可密钥

```
kesl-control [-L] --remove-active-key [--mdr]
```

删除活动的 EDR Expert (on-premises) 授权许可密钥

```
kesl-control [-L] --remove-active-key [--edr-kata]
```

删除活动的 EDR Expert (cloud) 授权许可密钥

```
kesl-control [-L] --remove-active-key [--cxdr]
```

删除活动的 KWSM 授权许可密钥

```
kesl-control [-L] --remove-active-key [--khcs]
```

其中：

`--edr-optimum` – 删除活动的 EDR Optimum 授权许可密钥。

`--kuma` – 删除活动的 KUMA 授权许可密钥。

`--mdr` – 删除活动的 MDR 授权许可密钥。

`--edr-kata` – 删除活动的 EDR Expert (on-premises) 授权许可密钥。

`--cxdr` – 删除活动的 EDR Expert (cloud) 授权许可密钥。

`--khcs` – 删除活动的 KWSM 授权许可密钥。

如果未在命令行中指定 `--edr-optimum`、`--kuma`、`--mdr`、`--edr-kata`、`--cxdr` 或 `--khcs` 选项，该命令将删除用于激活应用程序的活动密钥。

kesl-control --remove-reserve-key

此命令可让您删除备用授权许可密钥。

删除备用 EDR Optimum 授权许可密钥

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

删除备用 KUMA 授权许可密钥

```
kesl-control [-L] --remove-reserve-key [--kuma]
```

删除备用 MDR 授权许可密钥

```
kesl-control [-L] --remove-reserve-key [--mdr]
```

删除备用 EDR Expert (on-premises) 授权许可密钥

```
kesl-control [-L] --remove-reserve-key [--edr-kata]
```

删除备用 EDR Expert (cloud) 授权许可密钥

```
kesl-control [-L] --remove-reserve-key [--cxdr]
```

删除备用 KWSM 授权许可密钥

```
kesl-control [-L] --remove-reserve-key [--khcs]
```

其中：

`--edr-optimum` – 删除备用 EDR Optimum 授权许可密钥。

`--kuma` – 删除备用 KUMA 授权许可密钥。

`--mdr` – 删除备用 MDR 授权许可密钥。

`--edr-kata` – 删除备用 EDR Expert (on-premises) 授权许可密钥。

`--cxdr` – 删除备用 EDR Expert (cloud) 授权许可密钥。

`--khcs` – 删除备用 KWSM 授权许可密钥。

如果未在命令行中指定 `--edr-optimum`、`--kuma`、`--mdr`、`--edr-kata`、`--cxdr` 或 `--` 选项，该命令将从应用程序中删除备用密钥。

### kesl-control -L --query

该命令输出有关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。

```
kesl-control -L --query [--json]
```

其中：

`--json`：以 JSON 格式输出数据。

### kesl-control --load-mdr-blob

该命令允许您将可用于与 Kaspersky Managed Detection and Response 集成的 BLOB 文件上传到设备。您可以在 MDR 配置文件（ZIP 压缩文件格式）中找到 BLOB 文件。

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB file>
```

### kesl-control --remove-mdr-blob

该命令允许您从设备中删除用于与 Kaspersky Managed Detection and Response 集成的 BLOB 文件。

```
kesl-control [-L] --remove-mdr-blob
```

## 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。

## 管理用户角色

显示用户和角色列表

```
kesl-control [-U] --get-user-list
```

为指定用户分配角色

```
kesl-control [-U] --grant-role <role> <user>
```

撤销用户角色

```
kesl-control [-U] --revoke-role <role> <user>
```

其中：

`<user>` 是用户或用户组名称。

`<role>` 是用户或用户组角色。

## 密码保护设置

您可以使用命令管理 密码保护。

启用或禁用密码保护

```
kesl-control --set-permission-manager-settings Enabled=<Yes|No>
```

查看当前密码保护设置

```
kesl-control --get-permission-manager-settings
```

编辑用户或组的权限

```
kesl-control --set-permissions <user> [--group] <permissions>=<Yes|No> [--file <file name>] [--json]
```

查看用户或组的当前权限

```
kesl-control --get-permissions <user> [--group] [--file <file name>] [--json]
```

移除已配置权限的用户或用户组

```
kesl-control --remove-permissions <user> [--group]
```

其中：

`<user>` 是用户或用户组名称。

`<permissions>` 用于自定义权限。

`--group` 将该设置应用于一组用户。如果未指定此选项，则该设置将应用于单个用户。

`--file <path to file>` 将设置保存或导出到配置文件。如果未指定此选项，则命令结果将写入标准输出。

指定 `--json`，则以 JSON 格式输出设置。

### 管理设备上的策略

要在设备上禁用策略，用户需要拥有 禁用 Kaspersky Security Center 策略 权限。

如果用户已在设备上禁用策略，则策略会在设备或 Kaspersky Endpoint Security 重新启动后重新生效。

在设备上禁用策略

```
kesl-control --disable-policy
```

将策略应用于设备

```
kesl-control --enable-policy
```

# 管理应用程序任务和设置

`-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网络流量扫描设置的命令组。

### 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。

```
kesl-control [-T] --export-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是要将应用程序设置保存到其中的配置文件的完整路径。

指定 `--json`，则以 JSON 格式输出设置。

### kesl-control --import-settings

仅允许受信任的用户访问配置文件。在将设置导入应用程序之前，请验证目录、配置文件、可执行文件和隔离区的路径。请勿从不受信任的来源导入配置文件。配置文件遭到破坏可能会影响组织基础设施的安全性、完整性或功能，还可能影响用户数据。

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。

```
kesl-control [-T] --import-settings --file <path to configuration file> [--json]
```

其中：

`--file <path to file>` 是要从中导入应用程序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` 选项，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。

如果应用程序正在以 Light Agent 模式使用，则无法运行此命令。

```
kesl-control [-T] --update-application
```

## 管理常规应用程序设置的命令

### kesl-control --get-app-settings

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。

```
kesl-control [-T] --get-app-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是要将应用程序的常规设置输出到的配置文件的路径。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。

### kesl-control --set-app-settings

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。

使用命令行选项指定设置：

```
kesl-control [-T] --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

使用配置文件指定设置：

```
kesl-control [-T] --set-app-settings --file <path to file> [--json]
```

其中：

`<setting name>=<setting value>` 是应用程序常规设置的名称和值。

`--file <path to file>` 是要从中导入应用程序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`选项，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。

```
kesl-control [-T] --get-settings <task ID|name> [--file <path to file>] [--json]
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

`--file <path to file>` 是要将任务设置输出到的配置文件的路径。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。

### 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。

使用命令行选项指定设置：

```
kesl-control [-T] --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>] [--add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

使用配置文件指定设置：

```
kesl-control [-T] --set-settings <task ID/name> --file <path to file> [--json]
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

`<setting name>=<setting value>` 是某个任务设置的名称和值。

`--add-path <path>` 添加包含要扫描的对象的目录路径。

`--del-path <path>` 删除包含要扫描的对象的目录路径。

`--add-exclusion <path>` 添加包含要从扫描中排除的对象的目录路径。

`--del-exclusion <path>` 删除包含要从扫描中排除的对象的目录路径。

`--file <path to file>` 是配置文件的完整路径，您希望从该配置文件导入任务设置。

指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json`选项，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。

```
kesl-control [-T] --set-settings <task ID|name> --set-to-default
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

### kesl-control --get-schedule

该命令将指定任务的当前计划输出到控制台或配置文件。

```
kesl-control [-T] --get-schedule <task ID|name> [--file <path to file>] [--json]
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

`--file <path to file>` 是要将任务计划设置输出到的配置文件的路径。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。

### kesl-control --set-schedule

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。

使用命令行选项指定设置：

```
kesl-control [-T] --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

使用配置文件指定设置：

```
kesl-control [-T] --set-schedule <task ID|name> --file <path to file> [--json]
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

`<setting name>=<setting value>` 是某个 任务计划设置 的名称和值。

`--file <path to file>` 是配置文件的完整路径，您希望从该配置文件导入任务计划设置。

指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json`选项，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。

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

其中：

指定 `--json`，则以 JSON 格式输出设置。

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 策略禁止用户查看和编辑本地任务，则有关 `Scan_My_Computer`、`Critical_Areas_Scan`、`Container_Scan`、`Inventory_Scan`、`Update` 和 `Rollback` 任务的信息不可用。

## kesl-control --get-task-state

此命令输出指定任务的状态。

```
kesl-control [-T] --get-task-state <task ID|name> [--json]
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

指定 `--json`，则以 JSON 格式输出设置。

应用程序任务可以处于以下状态：

- `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` 类型的任务还可以具有以下状态之一：

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

### kesl-control --create-task

此命令使用默认设置或配置文件中指定的设置创建指定类型的任务。

只能创建用户任务。无法创建预定义任务。

根据应用程序模式，可以创建以下类型的用户任务：

- 标准模式：`ODS`、`Update`、`Rollback`、`ODFIM`、`ContainerScan` 和 `InventoryScan`。
- Light Agent 模式：`ODS`、`ODFIM`、`ContainerScan` 和 `InventoryScan`。

使用默认设置创建任务

```
kesl-control [-T] --create-task <task name> --type <task type>
```

使用配置文件中的设置创建任务

```
kesl-control [-T] --create-task <task name> --type <task type> [--file <path to file>] [--json]
```

其中：

`<task name>` 是您为新任务指定的名称。

`<task type>` 指定您要创建的任务类型。

`--file <path to file>` 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`选项，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。

只能删除用户任务。无法删除预定义任务。

```
kesl-control [-T] --delete-task <task ID|name>
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

### kesl-control --start-task

此命令启动一项任务。

您可以启动和停止所有预定义任务和用户任务，但 `License` 类型的任务除外。

```
kesl-control [-T] --start-task <task ID|name> [-W] [--progress]
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

`-W`：启用当前事件输出。

`--progress`：显示任务进度。

运行 ID 为 1 的任务并启用与该任务相关的当前事件显示的示例

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

如果在启动任务时出现错误，导致任务没有启动，则在应用程序重启后，会尝试再次启动该任务。

### kesl-control --stop-task

此命令停止一项任务。

您可以启动和停止所有预定义任务和用户任务，但 `License` 类型的任务除外。

```
kesl-control [-T] --stop-task <task ID|name> [-W]
```

其中：

`<task ID|name>` 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

`-W`：启用当前事件输出。

### kesl-control --suspend-task

此命令暂停一项任务。

您只能暂停 ODS、ODFIM 和 InventoryScan 任务。

```
kesl-control [-T] --suspend-task <task ID|name>
```

其中：

<task ID|name> 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

### kesl-control --resume-task

此命令恢复一项任务。

您只能恢复 ODS、ODFIM 和 InventoryScan 任务。

```
kesl-control [-T] --resume-task <task ID|name>
```

其中：

<task ID|name> 是在创建任务时分配给任务的 ID，或者是命令行上的任务名称。

### kesl-control --scan-file

此命令创建并运行一项自定义扫描任务。

```
kesl-control [-T] --scan-file <path> [--action <action>]
```

其中：

<path> 是您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 <action> 是您希望应用程序对受感染对象执行的操作。如果您未指定 --action 选项，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。

```
kesl-control [-T] --scan-container <ID|name[:tag]>
```

其中：

`<ID|name[:tag]>` 是容器或镜像的名称或 ID。您可以使用掩码扫描多个对象。

实用文章

**如何指定掩码**

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

kesl-control --get-container-settings

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。

```
kesl-control [-C] --get-container-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是要将容器扫描的常规设置输出到其中的配置文件的路径。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。

### kesl-control --set-container-settings

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。

使用命令行选项指定设置：

```
kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

使用配置文件指定设置：

```
kesl-control [-C] --set-container-settings --file <path to file> [--json]
```

其中：

`<setting name>=<setting value>` 是容器扫描常规设置的名称和值。

`--file <path to file>` 是要从中导入容器扫描常规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`选项，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。

## 用于管理网络流量扫描设置的命令

`-N` 前缀表示该命令属于用于管理网络流量扫描设置的命令组。

### 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。

显示用户添加的排除项列表

```
kesl-control -N --query user
```

显示应用程序添加的排除项列表

```
kesl-control -N --query auto
```

显示从应用程序数据库收到的排除项列表

```
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。

```
kesl-control -N --clear-web-auto-excluded
```

### kesl-control --get-net-settings

该命令将当前的网咯流量扫描设置输出到控制台或配置文件。

```
kesl-control [-N] --get-net-settings [--file <path to file>] [--json]
```

其中：

`--file <path to file>` 是要将网络流量扫描设置输出到的配置文件的路径。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。

### kesl-control --set-net-settings

该命令使用命令选项或从配置文件导入设置来配置网咯流量扫描设置。

使用命令行选项指定设置：

```
kesl-control [-N] --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

使用配置文件指定设置：

```
kesl-control [-N] --set-net-settings --file <path to file> [--json]
```

其中：

`<setting name>=<setting value>` 是 网络流量扫描设置的名称和值。

`--file <path to file>` 是要从中导入网络流量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`选项，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 --list-certificates

此命令输出受信任根证书列表。

```
kesl-control [-N] --list-certificates
```

### kesl-control --add-certificate

此命令将证书添加到受信任根证书列表中。

```
kesl-control [-N] --add-certificate <path to certificate>
```

其中：

`<path to certificate>` 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根证书列表中移除。

```
kesl-control [-N] --remove-certificate <certificate subject>
```

### kesl-control --add-bypass-endpoints

此命令可让您添加流量拦截排除。

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

其中：

`<in|out>` 是被排除连接中的流量方向：出站或入站。

`<remote IP address>` 是远程设备的 IPv4 或 IPv6 地址。如果您将入站流量排除在拦截之外，则来自指定 IP 地址的流量也将被排除。如果您将出站流量排除在拦截之外，那么前往指定 IP 地址的流量也将被排除。

`<destination port>` 是受保护设备上的端口（入站流量排除项）或远程设备上的端口（出站流量排除项）。到此端口的流量不被拦截。

### kesl-control --list-bypass-endpoints

此命令可让您查看已配置的流量拦截排除列表。

```
kesl-control [-N] --list-bypass-endpoints
```

### kesl-control --remove-bypass-endpoints

此命令可让您移除流量拦截排除。

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

其中：

`<in|out>` 是被排除连接中的流量方向：出站或入站。

`<remote IP address>` 是远程设备的 IPv4 或 IPv6 地址，该设备的流量被排除在拦截范围之外（取决于流量方向）。

`<destination port>` 是受保护设备上的端口（入站流量排除项）或远程设备上的端口（出站流量排除项）。

# 状态和保护监控

## 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。

```
kesl-control [-S] --app-info [--json] [--check-permissions]
```

其中：

指定 `--json`，则以 JSON 格式输出设置。

`--check-permissions` 显示权限配置不正确的应用程序目录的路径。

### kesl-control --supported-tech-info

此命令显示应用程序功能的列表、功能状态信息（使用或未使用）以及实现这些应用程序功能所采用的 Linux 技术。

```
kesl-control [-S] --supported-tech-info [--json]
```

其中：

`--json`：以 JSON 格式输出功能。

### kesl-control --get-statistic

该命令允许您显示有关应用程序操作的统计信息和在设备上找到的挂载点列表。

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

其中：

`--files`：文件威胁防护组件扫描最频繁的文件的统计数据，以及组件访问这些文件的次数。

`--processes`：Kaspersky Endpoint Security 最常检测的进程启动的统计信息，以及此类启动的数量。

> 将进程从行为检测组件的扫描范围中排除，不会将这些进程从统计信息中移除，但可以提升Kaspersky Endpoint Security 应用程序的性能。

`--mountpoints`:挂载点列表。在输出中，挂载点路径按以下方式排序：

- 静态、系统、服务和其他挂载点
- 其命名空间中的已挂载 snap 包和挂载点
- Docker 容器管理系统创建的挂载点

您可以以任意组合指定一个或多个选项，或者根本不指定任何选项。如果您不指定任何选项，应用程序将显示三个列表：有关最常扫描的文件的统计数据、有关最常启动的进程的统计数据以及在设备上找到的挂载点列表。

### kesl-control --omsinfo

此命令创建一个 JSON 文件，以便与 Microsoft Operations Management Suite 整合。

```
kesl-control [-S] --omsinfo --file <path to file>
```

# 用于显示事件的命令

`-W` 前缀表示用于显示应用程序事件日志中的事件的命令。

### 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。

```
kesl-control -W [--query "<filter conditions>"]
```

其中：

`<filter conditions>` 指定一个或多个 逻辑表达式，这些表达式采用 `<field> <comparison operation> '<value>'` 格式，并使用逻辑运算符 `and` 组合，以输出某些当前事件。

# 用于管理应用程序事件的命令

-E 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。

```
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。

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--file <path to file>] [--
json] [--reverse]
```

其中：

`<database file>` 是要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` 常规应用程序设置决定。

`<filter conditions>` 指定一个或多个采用 `<field> <comparison operator> '<value>'` 格式且使用逻辑运算符 `and` 组合的 逻辑表达式，以限制查询结果。

`<number>` 是选择中要输出的最新事件数（即从选择末尾开始计数的记录数）。

`--file <path to file>` 是要将事件输出到其中的文件的完整路径。如果您指定文件名而不指定其路径，则将在当前目录中创建文件。如果指定路径中已存在具有指定名称的文件，则它将被覆盖。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）。

## 用于管理系统性能指标的命令

kesl-control --export-metrics

此命令可配置操作系统性能指标的获取。

```
kesl-control [-J] --export-metrics [--period <interval in seconds between exports>|--interactive]
```

其中：

`--period`可启用定期输出结果。

`<interval in seconds between exports>` 指定命令结果输出到命令行控制台的频率（以秒为单位）

`--interactive`可启用交互式输出（按下**Enter**键时）。

# 安全控制

## 用于管理设备控制的命令

-D 前缀表示该命令属于用于管理设备控制的命令组。

管理设备控制设置

查看当前设备控制设置

```
kesl-control --get-settings 15 [--file <path to file>] [--json]
```

修改应用程序控制设置

```
kesl-control --set-settings 15 [<setting>=<value>] [--file <path to file>] [--json]
```

其中：

`<setting>=<value>` 指定设备控制设置及其值。

--file <文件路径> 将设置保存或导出到配置文件。如果未指定此选项，则命令结果将写入标准输出。

`--json`：以 JSON 格式输出数据。

管理设备

查看已连接设备列表

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

其中：

`--all`列出所有已连接的设备。

`--json`列出已连接的 JSON 格式设备。

`--export <file>` 将已连接设备列表导出到 JSON 文件。已导出已连接设备列表。

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。

受信任设备

该命令行可让您查看受信任设备列表、从列表中添加和删除设备，以及从文件导入受信任设备列表。

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <file>]
```

其中：

`--list` – 显示受信任设备列表。

`--add <ID>` 按照设备 ID 或设备 ID 掩码将设备添加到受信任设备列表中。

`--delete <ID>` 按照设备 ID 或设备 ID 掩码从受信任设备列表中删除设备。

`--merge`可合并受信任设备列表。如果当前列表和导入的列表中包含具有相同 ID 的设备条目，则会更新现有条目。对于不在当前列表中的设备，会添加条目。

`--add`会在导入时添加当前受信任设备列表。仅将之前不在设备列表中的设备条目添加到列表中。

`--replace`可替换当前受信任设备列表。现有受信任设备列表将被导入的列表替换。

`--file <file>` 从指定文件导入受信任设备列表。您需要指定 JSON 文件的完整路径。

临时访问被阻止的设备

这些命令允许您创建访问请求文件并上传访问密钥，以获取临时访问被阻止设备的权限：

创建访问请求文件

```
kesl-control [-D] --request-temporary-device-access --device-id <device ID> --access-duration <access duration> --path <path to access request file>
```

上传访问密钥

```
kesl-control [-D] --upload-temporary-device-access-key --path <access key>
```

其中：

`--device-id <device ID>` 是要访问的被阻止设备的 ID。

`--access-duration <access duration>` 是您要访问设备的时长（以小时为单位）。可能的值：1 到 100

`--path <path to access request file>` 是要保存扩展名为 .akey 的访问请求文件的目录路径。

`--path <access key>` 是包含设备访问密钥的文件路径（扩展名为 .acode 的文件）。

# 用于管理应用程序控制的命令

-A 前缀表示该命令属于用于管理应用程序控制的命令组。

## 管理清查任务

查看在客户端设备上检测到的应用程序列表

```
kesl-control [-A] --get-app-list [--json]
```

其中：

`--json`：以 JSON 格式输出数据。

## 查看应用程序类别

查看已创建的应用程序控制类别列表

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [--file <path to file>] [--json]
```

其中：

`<category name 1> <category name 2> ... <category name N>` 为类别名称。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 <path to file>` 将设置保存或导出到配置文件。如果未指定此选项，则命令结果将写入标准输出。

`--json`：以 JSON 格式输出数据。

## 管理应用程序类别

要创建应用程序类别：

1. 将应用程序类别列表写入配置文件：

   ```
   kesl-control --set-categories --file <path to file>
   ```

2. 按如下方式添加应用程序类别：

```
[
   {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 2>"
   }
]
```

要在 `Exclude` 和 `Include` 字段中指定文件路径，可以使用掩码。

3. 将类别列表导入应用程序：

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --
file <path to file>
```

编辑应用程序控制类别列表

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --file
<path to file>
```

其中：

`FilePath like <application>` 是应用程序可执行文件的完整路径。

`FileHash == <hash>` 是应用程序可执行文件的 SHA256 哈希值。

`<category ID>` 是唯一的类别 ID。必要设置。输入不带连字符的 `GUID`。

`<category name 1> <category name 2> ... <category name N>` 为类别名称。必要设置。

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。如果未指定类别名称，则不会创建该类别，或会将其从现有类别列表中删除。

`--file <path to file>` 将设置保存或导出到 JSON 配置文件。

管理应用程序控制设置

查看当前应用程序控制设置

```
kesl-control --get-settings 21 [--file <path to file>] [--json]
```

修改应用程序控制设置

```
kesl-control --set-settings 21 [<setting>=<value>] [--file <path to file>] [--json]
```

其中：

`<setting>=<value>` 指定应用程序控制的设置及其值。

`--file <path to file>` 将设置保存或导出到配置文件。如果未指定此选项，则命令结果将写入标准输出。

`--json`：以 JSON 格式输出数据。

将设置重置为默认值

删除应用程序类别和应用程序控制规则列表并恢复默认设置

```
kesl-control --set-settings 21 --set-to-default
```

实用文章

**如何指定掩码**

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 `/`）。

# Web 控制管理命令

管理 Web 控制设置

查看当前 Web 控制设置

```
kesl-control --get-settings 26 [--file <path to file>] [--json]
```

修改 Web 控制设置

```
kesl-control --set-settings 26 [<setting>=<value>] [--file <path to file>] [--json]
```

其中：

`<setting>=<value>` 是 Web 控制的设置及其值。您可以修改任意数量的设置。

`--file <path to file>` 将设置保存或导出到配置文件。如果未指定此选项，则命令结果将写入标准输出。

`--json`：以 JSON 格式输出数据。

将设置重置为默认值

删除已配置的设置并恢复默认 Web 控制设置

```
kesl-control --set-settings 26 --set-to-default
```

# 网络连接保护

## 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 网络威胁防护 阻止的设备的命令组。

### kesl-control --get-blocked-hosts

该命令可让您将被阻止设备的列表输出到控制台。

```
kesl-control [-H] --get-blocked-hosts
```

### kesl-control --allow-hosts

该命令可让您解除对被阻止设备的阻止。

```
kesl-control [-H] --allow-hosts <address>
```

其中：

<address> 是设备或子网的 IP 地址（IPv4/IPv6，包括短格式地址）。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。

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

其中：

`--name <rule name>` 是网络数据包规则的名称。

`--action <Allow|Block>` 是要对在此网络数据包规则中指定的连接执行的操作。

`--protocol <protocol>` 是您要监控其网络活动的协议。

`--direction <direction>` 是受监控网络活动的方向。

`--remote <remote address>:<port>` 是远程设备的网络地址。

`--local <local address>:<port>` 是安装了 Kaspersky Endpoint Security 的设备的网络地址。

`--at <index>` 是网络数据包规则列表中的规则编号。如果未指定 `--at` 选项或其值大于列表中的规则数，则新规则将添加到列表末尾。

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。

按规则名称删除网络数据包规则

```
kesl-control [-F] --del-rule --name <rule name>
```

按规则编号删除网络数据包规则

```
kesl-control [-F] --del-rule --index <index>
```

其中：

`--name <rule name>` 是网络数据包规则的名称。

`--index <index>` 是网络数据包规则列表中的规则编号。

### kesl-control --move-rule

该命令用于更改网络数据包规则的执行优先级。

按规则名称更改网络数据包规则的优先级

```
kesl-control [-F] --move-rule --name <rule name> --at <index>
```

按规则编号更改网络数据包规则的优先级

```
kesl-control [-F] --move-rule --index <index> --at <index>
```

其中：

`--name <rule name>` 是网络数据包规则的名称。

`--index <index>` 是网络数据包规则列表中规则的当前编号。

`--at <index>` 是网络数据包规则列表中规则的新编号。

### kesl-control --add-zone

此命令用于将地址添加到网络区域。

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

其中：

`--zone <zone>` 是网络区域的预定义名称。

`--address <address>` 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。

按地址或子网从网络区域中删除地址

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

按规则编号从网络区域中删除地址

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

其中：

`--zone <zone>` 是网络区域的预定义名称。

`--address <address>` 是网络地址或子网。

`--index <address index>` 是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。

```
kesl-control -F --query
```

# 防御高级威胁和定向攻击

## 用于管理隔离区的命令

-Q 前缀表示该命令属于用于管理隔离区的命令组。

### kesl-control -Q --mass-remove

该命令可从隔离区中删除部分或全部文件。

删除所有文件

```
kesl-control -Q --mass-remove
```

删除符合筛选条件的文件

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

其中：

`<filter conditions>` 指定一个或多个采用 `<field> <comparison operator> '<value>'` 格式且使用逻辑运算符 `and` 组合的逻辑表达式，以限制查询结果。

### kesl-control --put

此命令仅当 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Managed Detection and Response 集成时可用。

该命令允许隔离文件。

```
kesl-control [-Q] --put <file path> [--md5] [--sha256] [--save-original-file]
```

其中：

`<file path>` 是要隔离的文件的路径。

`--md5` 是您要隔离的文件的 MD5 哈希值。

`--sha256` 是您要隔离的文件的 SHA256 哈希值。

`--save-original-file` 保留原始文件。如果不指定此选项，则原始文件将被删除。

### kesl-control -Q --query

此命令输出有关隔离文件的信息。

输出所有已隔离文件的信息

```
kesl-control -Q --query [-n <number>] [--json]
```

显示符合筛选条件的已隔离文件的信息

```
kesl-control -Q --query ["<filter conditions>"] [-n <number>]
```

其中：

`<filter conditions>` 指定一个或多个采用 `<field> <comparison operator> '<value>'` 格式且使用逻辑运算符 `and` 组合的 逻辑表达式，以限制查询结果。如果您不指定任何筛选条件，应用程序将显示隔离文件的详细信息。

`<number>` 是要显示的最近隔离文件的数量。如果您不指定 `-n`选项，则会显示最后 30 个文件。要显示所有文件，请指定 0。

`--json`：以 JSON 格式输出数据。

### kesl-control -Q --restore

该命令可让您从隔离区恢复文件。

```
kesl-control -Q --restore <file ID> [--file <file path>]
```

**其中：**

`<file ID>` 是已隔离文件的 ID。

`--file <file path>` 是文件的新名称以及要将其保存到的目录的路径。如果不指定 `--file` 选项，则文件将以其原始名称和原始位置恢复。如果目录被删除或者用户没有访问权限，应用程序会将文件放在 /var/opt/kaspersky/kesl/common/restored/ 目录中。您可以手动将文件从该目录移动到您选择的目录。

# 用于管理 EDR Expert (on-premises) 组件的命令

-R 前缀表示该命令属于用于管理与卡巴斯基 Detection and Response 解决方案的集成设置的命令组。

## kesl-control --add-kataedr-server-certificate

此命令可让您添加或替换先前添加的KATA 服务器、OSMP 威胁响应服务器或 OSMP 遥测服务器的证书（取决于集成模式）。

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type <response|telemetry>]
```

其中：

`<file>` 是包含服务器证书的文件的路径。

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (on-premises) 集成模式下为其添加或替换证书的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

如果您要添加或替换 KATA 服务器证书，请省略`--server-type`选项。

## kesl-control --remove-kataedr-server-certificate

此命令可让您移除先前添加的KATA 服务器、OSMP 威胁响应服务器或 OSMP 遥测服务器的证书（取决于集成模式）。

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (on-premises) 集成模式下从中移除证书的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

如果要删除 KATA 服务器证书，请省略`--server-type`选项。

### kesl-control --query-kataedr-server-certificate

此命令可让您查看先前添加的KATA 服务器、OSMP 威胁响应服务器或 OSMP 遥测服务器（取决于集成模式）的证书信息。

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (on-premises) 集成模式下查看其证书信息的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

如果要查看关于 KATA 服务器证书的信息，请省略`--server-type`选项。

### kesl-control --add-kataedr-client-certificate

此命令可让您添加或替换先前添加的客户端证书，该证书用于保护与KATA 服务器、OSMP威胁响应服务器或 OSMP 遥测服务器的连接（取决于集成模式）。

```
kesl-control [-R] --add-kataedr-client-certificate <file>  [--server-type <response|telemetry>]
```

其中：

`<file>` 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

> 您必须指定加密容器的密码。否则，当您单击**输入**时，会显示 `Certificate password is required and cannot be empty` 错误。

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (on-premises) 集成模式下为其添加客户端证书的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

如果您要添加或替换用于与 KATA 服务器连接的客户端证书，请省略`--server-type`选项。

### kesl-control --remove-kataedr-client-certificate

此命令可让您移除先前添加的客户端证书，该证书用于保护与KATA 服务器、OSMP威胁响应服务器或 OSMP 遥测服务器的连接（取决于集成模式）。

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (on-premises) 集成模式下从中移除客户端证书的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

如果您要移除用于与 KATA 服务器连接的客户端证书，请省略`--server-type`选项。

### kesl-control --query-kataedr-client-certificate

此命令可让您查看先前添加的客户端证书的信息，该证书用于保护与KATA 服务器、OSMP威胁响应服务器或 OSMP 遥测服务器的连接（取决于集成模式）。

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

其中：

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (on-premises) 集成模式下查看客户端证书信息的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

如果要查看用于与 KATA 服务器连接的客户端证书信息，请省略`--server-type`选项。

## 用于管理 EDR Expert（云）组件的命令

-R 前缀表示该命令属于用于管理与卡巴斯基 Detection and Response 解决方案的集成设置的命令组。

### kesl-control --query-cloudxdr-server-certificate

此命令可让您查看OSMP 威胁响应服务器或 OSMP 遥测收集服务器的证书信息。

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type <response|telemetry>
```

其中：

`--server-type <response|telemetry>`可让您在 EDR Expert (cloud) 集成模式下选择要查看其证书信息的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

### kesl-control --query-cloudxdr-client-certificate

此命令可让您查看先前添加的客户端证书的信息，该证书用于保护与OSMP 威胁响应服务器或 OSMP 遥测服务器的连接。

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type <response|telemetry>
```

其中：

`--server-type <response|telemetry>`可让您在 EDR Expert (cloud) 集成模式下选择要查看其客户端证书信息的服务器类型：

- `response` — OSMP 威胁响应操作服务器
- `telemetry` – OSMP 遥测服务器

## 用于管理 NDR (KATA) 组件的命令

-R 前缀表示该命令属于用于管理与卡巴斯基 Detection and Response 解决方案的集成设置的命令组。

### kesl-control --add-katandr-server-certificate

该命令将添加或替换先前添加的 NDR 服务器证书。

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

其中：

`<file>` 是包含服务器证书的文件的路径。

### kesl-control --remove-katandr-server-certificate

此命令可删除 NDR 服务器证书。

```
kesl-control [-R] --remove-katandr-server-certificate
```

### kesl-control --query-katandr-server-certificate

该命令将输出有关 NDR 服务器证书的信息。

```
kesl-control [-R] --query-katandr-server-certificate
```

### kesl-control --add-katandr-client-certificate

该命令将添加或替换先前添加的用于保护与 NDR 服务器连接的客户端证书。

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

其中：

`<file>` 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

> 您必须指定加密容器的密码。否则，当您单击**输入**时，会显示 `Certificate password is required and cannot be empty` 错误。

### kesl-control --remove-katandr-client-certificate

该命令将删除用于保护与 NDR 服务器连接的客户端证书。

```
kesl-control [-R] --remove-katandr-client-certificate
```

### kesl-control --query-katandr-client-certificate

该命令将输出有关客户端证书的信息。

```
kesl-control [-R] --query-katandr-client-certificate
```

## 用于管理设备网络隔离的命令

-R 前缀表示该命令属于用于管理与卡巴斯基 Detection and Response 解决方案的集成设置的命令组。与指定的 Detection and Response 解决方案集成时，设备的网络隔离将作为检测到威胁后的威胁响应操作。

### 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。

```
kesl-control [-R] --isolation-stat
```

### kesl-control --isolation-off

此命令可让您禁用设备的网络隔离。

```
kesl-control [-R] --isolation-off
```

## 用于管理 KUMA 集成设置的命令

-M 前缀表示该命令属于用于管理 Kaspersky Unified Monitoring and Analysis Platform 设置的命令组。

### kesl-control --add-kuma-server-certificate

该命令将添加或替换先前添加的 KUMA 服务器证书。

```
kesl-control [-M] --add-kuma-server-certificate <path to file>
```

其中：

`<path to file>` 是包含 DER 或 PEM 格式的服务器证书的文件路径。

### kesl-control --remove-kuma-server-certificate

此命令可删除 KUMA 服务器证书。

```
kesl-control [-M] --remove-kuma-server-certificate
```

### kesl-control --query-kuma-server-certificate

该命令将输出有关 KUMA 服务器证书的信息。

```
kesl-control [-M] --query-kuma-server-certificate
```

### kesl-control --add-kuma-client-certificate

该命令将添加或替换先前添加的用于保护与 KUMA 服务器连接的客户端证书。

```
kesl-control [-M] --add-kuma-client-certificate <path to file>
```

其中：

`<path to file>` 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

> 您必须指定加密容器的密码。否则，当您单击**输入**时，会显示 `Certificate password is required and cannot be empty` 错误。

### kesl-control --remove-kuma-client-certificate

该命令将删除用于保护与 KUMA 服务器连接的客户端证书。

```
kesl-control [-M] --remove-kuma-client-certificate
```

### kesl-control --query-kuma-client-certificate

该命令将输出有关客户端证书的信息。

```
kesl-control [-M] --query-kuma-client-certificate
```

## 用于管理 Sandbox 集成设置的命令

-X 前缀表示该命令属于用于管理 Sandbox 整合设置的命令组。

### kesl-control --add-sandbox-server-certificate

此命令将添加或替换负责与 Sandbox 交互的服务器的先前已添加证书。

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

其中：

`<file>` 是包含 DER 或 PEM 格式的服务器证书的文件路径。

### kesl-control --remove-sandbox-server-certificate

此命令将删除负责与 Sandbox 交互的服务器的证书。

```
kesl-control [-X] --remove-sandbox-server-certificate
```

### kesl-control --query-sandbox-server-certificate

此命令将显示负责与 Sandbox 交互的服务器的证书信息。

```
kesl-control [-X] --query-sandbox-server-certificate
```

### kesl-control --add-sandbox-client-certificate

此命令将添加或替换先前已添加的客户端证书，该证书用于为连接到负责与 Sandbox 交互的服务器提供保护。

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

其中：

`<file>` 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

> 您必须指定加密容器的密码。否则，当您单击**输入**时，会显示 `Certificate password is required and cannot be empty` 错误。

### kesl-control --remove-sandbox-client-certificate

此命令将删除用于为连接到负责与 Sandbox 交互的服务器提供保护的客户端证书。

```
kesl-control [-X] --remove-sandbox-client-certificate
```

### kesl-control --query-sandbox-client-certificate

该命令将输出有关客户端证书的信息。

```
kesl-control [-X] --query-sandbox-client-certificate
```

### kesl-control --sandbox

此命令可将要扫描的文件发送到 Sandbox。

```
kesl-control [-X] --sandbox <path 1> <path 2>
```

其中：

`<path>` 是您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。

# 用于管理 IOC 扫描的命令

`-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。

kesl-control --scan-ioc

该命令可启动搜索设备上的入侵指标 (IOC)。

```
kesl-control [-T] --scan-ioc --path <path to directory or file> [--process on|off] [--hint <regular expression>]
[--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--
excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

其中：

`--path <path to directory or file>` 是用于执行扫描的 IOC 文件的路径，或包含扩展名为 .IOC 或 .XML 的 IOC 文件的目录。

> 您可以指定多个路径，用空格分隔。您还可以指定两种类型的路径（文件路径和目录路径）。

`--process` — 启用对设备上运行的进程的分析。

可能的参数：

- `on` — 启用对设备上运行的进程的分析（默认值）。
- `off` — 禁用对设备上运行的进程的分析。

如果不指定 `--process` 选项，则仅当使用的IOC 文件指定了这些进程的详细信息（`ProcessItem`）时，应用程序才会分析进程。

`--hint <regular expression>` 是与要分析的文件 (`FileItem`) 或进程的可执行文件 (`ProcessItem`) 的完整路径匹配的正则表达式。

您可以使用以下正则表达式元素：

- 元字符：`.` `^` `$` `|`
- 字符类：`digit`，`alpha`，`lower`，`upper`，`cntrl`
- 量词：`*` `+` `?` `{n}` `{n,}` `{n, m}`
- 否定：`'[^a-c]'`
- 转义字符：`\a` `\e` `\f`, `\n` `\r` `\t` `\v` `\b`

`--arpentry` — 启用 ARP 表 (`ArpEntryItem`) 中的条目分析。

可能的参数：

- `on` — 启用 ARP 表中条目的分析（默认值）。
- `off` — 禁用 ARP 表中条目的分析。

如果不指定 `--arpentry` 选项，则仅当使用的 IOC 文件指定了 ARP 表（`ArpEntryItem`）的详细信息时，应用程序才会分析 ARP 表。

`--ports` — 启用对连接开放的端口的分析。

可能的参数：

- `on` — 启用对连接开放的端口的分析并扫描设备上的活动连接（默认值）。
- `off` — 禁用对连接开放的端口的分析并且不扫描设备上的活动连接。

如果不指定 `--ports` 选项，则仅当使用的IOC 文件指定了这些端口的详细信息（`PortItem`）时，应用程序才会分析端口。

`--system` — 启用系统环境分析。

可能的参数：

- `on` — 启用系统环境分析（默认值）。
- `off` — 禁用系统环境分析。

如果不指定 `--system` 选项，则仅当使用的IOC 文件指定了系统环境（`SystemInfoItem`）的详细信息时，应用程序才会分析系统环境。

`--files` — 启用文件分析。

可能的参数：

- `on` — 启用文件分析（默认值）。
- `off` — 禁用文件分析。

如果不指定 `--files` 选项，则仅当使用的 IOC 文件指定了这些文件的详细信息 (`FileItem`) 时，应用程序才会分析文件。

`--drives` — 要扫描的区域。

可能的参数：

- `all` — 检查所有可用的文件区域。
- `system` — 扫描根文件系统中的所有文件。
- `critical` — 扫描用户和系统目录中的文件（默认值）。
- `custom` — 仅扫描您指定的区域中的文件。

如果您未指定 `--drives` 选项，应用程序将分析用户和系统目录中的文件。

`--excludes <list of exclusions>` 是排除在扫描范围之外的路径列表。

此选项指定的排除项为全局选项，无论范围类型或目录列表如何均有效。这些排除项优先于其他命令行选项，包括`--hint`和`--scope`。

> 排除项被指定为路径，但不能包含递归元素或通配符（例如`*`）。

如果不指定`--excludes`选项，则执行扫描时不进行排除。

您可以指定多个排除项，用空格分隔。

`--scope <list of directories>` 是要扫描的其他目录列表。

> 如果您为`custom`选项指定了`--drives`参数，则需要此选项。

`--action`— 当检测到入侵指标时执行的操作。

可能的参数：

- `Skip` — 应用程序不会对检测到的对象执行任何操作，但有关它的信息将保存在任务执行结果中（默认值）。
- `QuarantineFile` — 应用程序将隔离检测到的对象。
- `IsolateHost`— 应用程序对在其上检测到对象的设备实施网络隔离。
- `ScanCriticalAreas` – 应用程序将执行关键区域扫描。

**Kaspersky Endpoint Security 扫描的关键区域**

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot

- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

您可以指定多个操作，用逗号分隔。

如果指定 `Skip` 参数，请不要添加任何其他参数。`Skip` 参数只能单独使用。

kesl-control --get-response-task-list

此命令显示设备上正在运行的 *IOC 扫描* 任务的相关信息。

```
kesl-control [-T] --get-response-task-list
```

因此，应用程序会以下列形式显示有关正在运行的任务的信息：

任务 ID：<任务 ID>
响应操作：IocScan

创建日期：<任务创建日期和时间>

启动任务：<任务启动计划>

状态：<任务状态>

Kaspersky Endpoint Security 在每次与服务器同步时更新有关正在运行的 *IOC 扫描* 任务的信息。您可以在与卡巴斯基检测和响应解决方案集成的设置中配置同步周期 (`SynchronizationPeriod`)。默认情况下，应用程序每 5 分钟与服务器同步一次。

kesl-control --delete-response-task <任务 ID>

此命令按 ID 删除 *IOC 扫描* 任务。应用程序会在计算机本地删除该任务。如果您尚未在 Web Console 或 OSMP Console 中删除该任务，应用程序会在下一次与服务器同步时恢复此任务。

```
kesl-control [-T] --delete-response-task-list <task ID>
```

# Light Agent 模式下的应用程序命令

-V 前缀表示该命令属于 Kaspersky Endpoint Security 在 Light Agent 模式下使用的命令组。

仅当 Kaspersky Endpoint Security 在 Light Agent 模式下使用时，才能执行这些命令。

kesl-control --ksvla-info

该命令输出有关在 Light Agent 模式下使用应用程序的信息。

```
kesl-control --ksvla-info
```

kesl-control --viis-info

该命令输出信息，内容涉及在 Light Agent 模式下将应用程序连接到 Integration Server。

```
kesl-control --viis-info
```

kesl-control --svm-info

该命令输出信息，内容涉及在 Light Agent 模式下将应用程序连接到 SVM。

```
kesl-control --svm-info
```

# 应用程序命令行选项

# 更新任务

下表介绍了可为 `Update` 任务指定的所有设置的全部可用值和默认值。

更新任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。<br>默认值：10。 |
| `ApplicationUpdateMode` | 如何下载和安装自动安装的应用程序更新（自动补丁）。 | `Disabled`：不下载或安装自动补丁。<br>`DownloadOnly`（默认）：下载自动补丁，但不安装。<br>`DownloadAndInstall`：自动下载并安装自动补丁。安装自动补丁后，应用程序将自动重启。 |
| **[Sources.item_#]** 部分包含以下设置： | | |
| `Enabled` | 使用 `SourceType` 设置中指定的更新源。<br>要运行该任务，需要启用至少一个更新源。 | `Yes` – 应用程序正在使用更新源。<br>`No`（默认）– 应用程序未使用更新源。 |
| `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。<br>`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。<br>`Custom`。应用程序从 `URL` 设置中指定的自定义源下载更新。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。 |
| `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。<br>例如：<br>`URL=http://example.com/bases/` – 包含更新的目录的 HTTP 服务器地址。<br>`URL=/home/bases/` – 受保护的计算机上包含应用程序数据库的目录。 |

# 主机威胁防护

## 文件威胁防护任务

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。

下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能值和默认值。

“文件威胁防护任务”设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `ScanArchived` | 启用存档扫描（包括 SFX 自解压存档）。<br>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。<br>我们不建议启用此设置，因为扫描压缩文件会影响性能，因为在将文件解压到临时目录并进行扫描时，对压缩文件文件的访问会被阻止。 | `Yes` – 扫描压缩文件。<br>如果将 `ActionOnThreat` 设置为 `DisinfectDeleteIfNotPossible`，并且无法清除，则应用程序将根据压缩文件类型，删除感染对象或包含威胁的整个压缩文件。<br>`No`（默认值）– 不扫描压缩文件。 |
| `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` – 扫描自解压存档。<br>`No`（默认值）– 不扫描自解压存档。 |
| `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` – 扫描电子邮件数据库的文件。<br>`No`（默认值）– 不扫描电子邮件数据库的文件。 |
| `ScanPlainMail` | 启用对纯文本电子邮件的扫描。 | `Yes` – 扫描纯文本电子邮件。<br>`No`（默认值）– 不扫描纯文本电子邮件。 |
| `SkipPlainTextFiles` | 从扫描中临时排除纯文本格式的文件。此设置使优化应用程序日志扫描成为可能。<br>如果您使用基于 fanotify 的系统事件拦截机制，则会应用此设置。使用可更新内核模块时，会利用扫描结果缓存优化扫描。 | `Yes` – 如果文本文件在最近一次扫描后 10 分钟内被同一进程重复使用，则不扫描这些文本文件。<br>`No`（默认值）– 扫描纯文本格式的文件。 |
| `SkipDatabaseJournals` | 暂时将数据库日志文件排除在扫描范围之外。此设置能够优化数据库日志文件的扫描。<br>如果您使用基于 fanotify 的系统事件拦截机制，则会应用此设置。使用可更新内核模块时，会利用扫描结果缓存优化扫描。 | `Yes` – 如果数据库日志文件在最近一次扫描后的 10 分钟内由同一进程重复使用，则不会扫描这些文件。<br>`No`（默认）– 扫描数据库日志文件。 |

| 设置 | 描述 | 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 至 999999<br>0 – 应用程序扫描任意大小的对象。<br>默认值：0。 |
| TimeLimit | 最长对象扫描持续时间（以秒为单位）。<br>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 至 9999<br>0 – 对象扫描时间不受限制。<br>默认值：60。 |
| ActionOnThreat | 选择应用程序将对感染对象执行的操作。 | DisinfectDeleteIfNotPossible（清除；如果无法清除则删除）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>DisinfectBlockIfNotPossible（清除；如果无法清除则阻止）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将阻止访问感染对象。<br>Block – 应用程序阻止访问受感染对象。<br>默认值：DisinfectDeleteIfNotPossible。 |
| UseExcludeMasks | 启用从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 | Yes – 从扫描中排除 ExcludeMasks.item_# 设置指定的对象。<br>No（默认值）– 不从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 |
| ExcludeMasks.item_# | 按名称或掩码在扫描中排除对象。<br>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。<br>示例<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |
| UseExcludeThreats | 允许从扫描中排除包含 ExcludeThreats.item_# 设置所指定威胁的对象。 | Yes – 从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。<br>No（默认值）：不从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。 |
| 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。<br>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。<br>例如，您可能正在使用实用程序来获取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。<br>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。 | 该设置值区分大小写。<br>默认值为未定义。<br>示例<br>UseExcludeThreats=Yes<br>ExcludeThreats.item_0000=EICAR-Test-*<br>ExcludeThreats.item_0001=?rojan.Linux |
| 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。<br>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 – 记录有关未感染的对象的信息。<br>No（默认值）–不记录有关未感染的对象的信息。 |
| 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。<br>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 – 记录有关存档中已扫描对象的信息。<br>No（默认值）– 不记录有关存档中已扫描对象的信息。 |
| ReportUnprocessedObjects | 启用记录由于某种原因尚未处理的对象的有关信息。 | Yes – 记录有关未处理对象的信息。<br>No（默认值）–不记录有关未处理对象的信息。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseAnalyzer | 启用启发式分析。<br>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。<br>此设置不适用于配备 Elbrus CPU 的设备。 | Yes（默认值）— 启用启发式分析器。<br>No — 禁用启发式分析器。 |
| HeuristicLevel | 指定启发式分析级别。<br>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。<br>此设置不适用于配备 Elbrus CPU 的设备。 | Light — 扫描最不全面，系统负载最小。<br>Medium — 中度启发式分析级别，操作系统负载均衡。<br>Deep — 最全面的扫描，操作系统负载最大。<br>Recommended（默认值）— 推荐值。 |
| UseIChecker | 启用 iChecker 技术。 | Yes（默认值）— 启用 iChecker 技术。<br>No — 禁用 iChecker 技术。 |
| 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。 | SmartCheck（默认值）- 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。如果某个进程在其操作过程中多次访问该对象并对其进行修改，则仅当该进程最后一次关闭该对象时，应用程序才会再次扫描该对象。<br>OpenAndModify – 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。<br>Open – 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。 |
| **[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。<br>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。<br>示例<br>AreaDesc="Scanning of email databases" |
| 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（默认值）— 扫描指定的范围。<br>No — 不扫描指定的范围。 |
| 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。<br>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：*（扫描所有对象）。<br>示例<br>AreaMask_item_<item number>=*doc |
| Path | 包含要扫描的对象的目录的路径。 | <path to local folder> – 扫描指定目录中的对象。您可以使用掩码和标签指定路径。<br>Shared:NFS — 扫描可通过 NFS 协议访问的设备文件系统资源。<br>Shared:SMB – 扫描可通过 Samba 协议访问的设备文件系统资源。<br>Mounted:NFS — 扫描使用 NFS 协议挂载到设备上的远程目录。<br>Mounted:SMB — 扫描使用 Samba 协议挂载到设备上的远程目录。<br>AllRemoteMounted — 扫描使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。<br>AllShared — 扫描可通过 SMB 和 NFS 协议访问的所有设备文件系统资源。<br><file system type> – 扫描指定文件系统设备的所有资源。 |
| **[ExcludedFromScanScope.item_#]** 部分包含以下设置： | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 | 默认值为未定义。 |
| UseScanArea | 从扫描中排除指定的范围。 | Yes（默认值）— 排除指定的范围。<br>No — 不排除指定的范围。 |
| 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。<br>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：*（从扫描中排除所有对象） |
| Path | 包含要排除的对象的目录的路径。 | <path to local folder> – 从扫描中排除指定目录（包括子目录）中的对象。您可以使用掩码和标签指定路径。<br>Mounted:NFS — 从扫描中排除使用 NFS 协议在设备上挂载的远程目录。<br>Mounted:SMB — 从扫描中排除使用 SMB 协议在设备上挂载的远程目录。<br>AllRemoteMounted — 在扫描中排除使用 SMB 和 NFS 协议挂载在设备上的所有远程目录。<br><file system> – 从扫描中排除指定文件系统设备的所有资源。 |
| **[ExcludedForProgram.item_#]** 部分包含以下设置： | | |
| ProgramPath | 排除的进程的路径。<br>如果使用可更新内核模块进行系统事件拦截，则指定进程将被排除在所有命名空间的拦截之外。 | <path to process> — 从扫描中排除指定目录中的对象。 |
| 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。<br>No（默认值）– 仅从扫描中排除指定进程，不排除其子进程。 |
| AreaDesc | 进程排除范围的说明。 | 默认值：All objects。 |
| UseExcludedForProgram | 从扫描中排除指定的范围。 | Yes（默认值）— 排除指定的范围。<br>No — 不排除指定的范围。 |
| 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。<br>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：*（从扫描中排除所有对象） |
| Path | 包含由进程修改的文件的目录的路径。 | <path to local folder> — 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。<br>Shared:NFS — 在扫描中排除可通过 NFS 协议访问的设备文件系统资源。<br>Shared:SMB — 在扫描中排除可通过 Samba 协议访问的设备文件系统资源。<br>Mounted:NFS — 从扫描中排除使用 NFS 协议在设备上挂载的远程目录。<br>Mounted:SMB — 从扫描中排除使用 SMB 协议在设备上挂载的远程目录。<br>AllRemoteMounted — 在扫描中排除使用 SMB 和 NFS 协议挂载在设备上的所有远程目录。<br>AllShared — 从扫描中排除可通过 SMB 和 NFS 协议访问的所有设备文件系统资源。<br><file system type> – 从扫描中排除指定文件系统设备的所有资源。 |

实用文章

**如何指定掩码**

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。

**如何使用标签**

您可以使用特殊标签来指定容器或镜像：

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名称

<path to local directory> 是本地目录的路径。

您还可以使用唯一的标签组合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

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:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>

- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

# 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 <full path to the configuration file> [--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_#` 是要从扫描中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. 运行以下命令：

```
kesl-control --set-settings 1 --file <full path to the configuration file> [--json]
```

如果要以 JSON 格式从配置文件导入设置，请指定 `--json` 选项。如果不指定此选项，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。

# 恶意软件扫描

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。
- 使用恶意软件扫描自定义任务（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。

您可以使用以下命令对指定的文件和目录执行*自定义扫描*：

```
kesl-control --scan-file
```

## 恶意软件扫描任务

该表介绍了可为恶意软件扫描任务（Scan_My_Computer）指定的所有设置的全部可能值和默认值。

恶意软件扫描任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ScanFiles | 启用文件扫描。 | Yes（默认值）— 扫描文件。<br>No — 不扫描文件。 |
| ScanBootSectors | 启用引导扇区扫描。 | Yes（默认值）— 扫描引导扇区。<br>No — 不扫描引导扇区。 |
| ScanComputerMemory | 启用进程内存和内核内存扫描。 | Yes（默认值）— 扫描进程内存和内核内存。<br>No — 不扫描进程内存和内核内存。 |
| ScanStartupObjects | 启用启动对象扫描。 | Yes（默认值）— 扫描启动对象。<br>No — 不扫描启动对象。 |
| ScanArchived | 启用存档扫描（包括 SFX 自解压存档）。<br>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（默认值）— 扫描压缩文件。<br>如果将 ActionOnThreat 设置为 DisinfectDeleteIfNotPossible，并且无法清除，则应用程序将根据压缩文件类型，删除感染对象或包含威胁的整个压缩文件。<br>No — 不扫描压缩文件。 |
| 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（默认值）— 扫描自解压存档。<br>No — 不扫描自解压存档。 |
| 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 — 扫描电子邮件数据库的文件。<br>No（默认值）— 不扫描电子邮件数据库的文件。 |
| ScanPlainMail | 启用对纯文本电子邮件的扫描。 | Yes — 扫描纯文本电子邮件。<br>No（默认值）— 不扫描纯文本电子邮件。 |
| 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 至 999999<br>0 — 应用程序扫描任意大小的对象。<br>默认值：0。 |

| 设置 | 描述 | 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 至 9999<br>0 — 对象扫描时间不受限制。<br>默认值：0。 |
| QueueScanTasks | 如果先前启动的计划扫描仍在运行，则延迟计划扫描任务。如果当前扫描仍在运行，Kaspersky Endpoint Security 会将计划扫描任务加入队列。这有助于优化计算机上的负载。例如，扫描任务计划在 18:00 和 20:00 运行。如果 18:00 的扫描仍在运行，则计划在 20:00 运行的扫描任务将被延迟。延迟的任务将在 18:00 的任务完成后运行。 | Yes，如果当前扫描仍在运行，则将计划扫描任务加入队列。<br>No（默认值），即使当前扫描仍在运行，也运行计划扫描任务。 |
| ActionOnThreat | 选择应用程序将对感染对象执行的操作。 | DisinfectDeleteIfNotPossible（清除；如果无法清除则删除）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>DisinfectInformIfNotPossible（清除；如果无法清除则通知）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>Inform 表示应用程序不会尝试清除或删除感染对象。受感染对象的信息会予以记录。<br>默认值：DisinfectDeleteIfNotPossible。 |
| UseExcludeMasks | 启用从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 | Yes — 从扫描中排除 ExcludeMasks.item_# 设置指定的对象。<br>No（默认值）— 不从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 |
| 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。<br>在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。 | 默认值为未定义。<br>示例<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |
| UseExcludeThreats | 允许从扫描中排除包含 ExcludeThreats.item_# 设置所指定威胁的对象。 | Yes — 从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。<br>No（默认值）：不从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。 |
| 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。<br>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。<br>例如，您可能正在使用实用程序来获取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。<br>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。 | 该设置值区分大小写。<br>默认值为未定义。<br>示例<br>UseExcludeThreats=Yes<br>ExcludeThreats.item_0000=EICAR-Test-*<br>ExcludeThreats.item_0001=?rojan.Linux |
| UseGlobalExclusions | 针对扫描启用全局排除项。 | Yes（默认值）— 使用全局排除项。<br>No — 不使用全局排除项。 |
| UseOASExclusions | 针对扫描启用文件威胁防护排除项。 | Yes（默认值）— 使用文件威胁防护排除项。<br>No — 不使用文件威胁防护排除项。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。<br>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 — 记录有关未感染的对象的信息。<br>No（默认值）—不记录有关未感染的对象的信息。 |
| 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。<br>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 — 记录有关存档中已扫描对象的信息。<br>No（默认值）— 不记录有关存档中已扫描对象的信息。 |
| ReportUnprocessedObjects | 启用记录由于某种原因尚未处理的对象的有关信息。 | Yes — 记录有关未处理对象的信息。<br>No（默认值）—不记录有关未处理对象的信息。 |
| UseAnalyzer | 启用启发式分析。<br>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（默认值）— 启用启发式分析器。<br>No — 禁用启发式分析器。 |
| HeuristicLevel | 指定启发式分析级别。<br>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 — 扫描最不全面，系统负载最小。<br>Medium — 中度启发式分析级别，操作系统负载均衡。<br>Deep — 最全面的扫描，操作系统负载最大。<br>Recommended（默认值）— 推荐值。 |
| UseIChecker | 启用 iChecker 技术。 | Yes（默认值）— 启用 iChecker 技术。<br>No — 禁用 iChecker 技术。 |
| DeviceNameMasks.item_# | 设备名称列表。应用程序将扫描这些设备的引导扇区。<br>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。 | AllObjects – 扫描所有设备的引导扇区。<br><device name mask> – 扫描名称与指定掩码匹配的设备的引导扇区。<br>默认值：/** – 设备名称中的任意一组字符，包括 / 字符）。 |
| **[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：All objects。<br>示例<br>AreaDesc="Mail bases scan" |
| 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（默认值）— 扫描指定的范围。<br>No — 不扫描指定的范围。 |
| 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。<br>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：*（扫描所有对象）。<br>示例<br>AreaMask.item_0000=*doc |
| Path | 包含要扫描的对象的目录的路径。 | <path to local directory> – 扫描指定目录中的对象。<br>Shared:NFS — 扫描可通过 NFS 协议访问的设备文件系统资源。<br>Shared:SMB – 扫描可通过 Samba 协议访问的设备文件系统资源。<br>Mounted:NFS — 扫描使用 NFS 协议挂载到设备上的远程目录。<br>Mounted:SMB — 扫描使用 Samba 协议挂载到设备上的远程目录。<br>AllRemoteMounted — 扫描使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。<br>AllShared — 扫描可通过 SMB 和 NFS 协议访问的所有设备文件系统资源。<br><file system type> – 扫描指定文件系统设备的所有资源。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| **[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。 | 默认值为未定义。 |
| UseScanArea | 从扫描中排除指定的范围。 | Yes（默认值）— 排除指定的范围。<br>No — 不排除指定的范围。 |
| 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。<br>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：*（排除所有对象）。 |
| Path | 包含要排除的对象的目录的路径。 | <path to local directory> – 从扫描中排除指定目录（包括子目录）中的对象。您可以使用掩码指定路径。<br>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，可以添加以下排除项：/.snapshots/*/snapshot/。<br>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。<br>Mounted:NFS — 从扫描中排除使用 NFS 协议在设备上挂载的远程目录。<br>Mounted:SMB — 从扫描中排除使用 SMB 协议在设备上挂载的远程目录。<br>AllRemoteMounted — 在扫描中排除使用 SMB 和 NFS 协议挂载在设备上的所有远程目录。<br>< file system type> – 从扫描中排除指定文件系统设备的所有资源。<br>仅当远程目录在任务启动之前安装时，应用程序才会将其排除在扫描之外。任务启动后安装的远程目录不会被排除在扫描之外。 |

实用文章

### 如何指定掩码

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。

# 自定义扫描任务

该表介绍了可为自定义扫描任务指定的所有设置的全部可用值以及默认值（Scan_File）。

自定义扫描任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ScanFiles | 启用文件扫描。 | Yes（默认值）— 扫描文件。<br>No — 不扫描文件。 |
| ScanBootSectors | 启用引导扇区扫描。 | Yes — 扫描引导扇区。<br>No（默认值）— 不扫描引导扇区。 |
| ScanComputerMemory | 启用进程内存和内核内存扫描。 | Yes — 扫描进程内存和内核内存。<br>No（默认值）— 不扫描进程内存和内核内存。 |
| ScanStartupObjects | 启用启动对象扫描。 | Yes — 扫描启动对象。<br>No（默认值）— 不扫描启动对象。 |
| ScanArchived | 启用存档扫描（包括 SFX 自解压存档）。<br>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（默认值）— 扫描压缩文件。<br>如果将 ActionOnThreat 设置为 DisinfectDeleteIfNotPossible，并且无法清除，则应用程序将根据压缩文件类型，删除感染对象或包含威胁的整个压缩文件。<br>No — 不扫描压缩文件。 |
| 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（默认值）— 扫描自解压存档。<br>No — 不扫描自解压存档。 |
| 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 — 扫描电子邮件数据库的文件。<br>No（默认值）— 不扫描电子邮件数据库的文件。 |
| ScanPlainMail | 启用对纯文本电子邮件的扫描。 | Yes — 扫描纯文本电子邮件。<br>No（默认值）— 不扫描纯文本电子邮件。 |
| 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 至 999999<br>0 — 应用程序扫描任意大小的对象。<br>默认值：0。 |
| 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 至 9999<br>0 — 对象扫描时间不受限制。<br>默认值：0。 |
| QueueScanTasks | 如果先前启动的计划扫描仍在运行，则延迟计划扫描任务。如果当前扫描仍在运行，Kaspersky Endpoint Security 会将计划扫描任务加入队列。这有助于优化计算机上的负载。例如，扫描任务计划在 18:00 和 20:00 运行。如果 18:00 的扫描仍在运行，则计划在 20:00 运行的扫描任务将被延迟。延迟的任务将在 18:00 的任务完成后运行。 | Yes，如果当前扫描仍在运行，则将计划扫描任务加入队列。<br>No（默认值），即使当前扫描仍在运行，也运行计划扫描任务。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ActionOnThreat | 选择应用程序将对感染对象执行的操作。 | DisinfectDeleteIfNotPossible（清除；如果无法清除则删除）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>DisinfectInformIfNotPossible（清除；如果无法清除则通知）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>Inform 表示应用程序不会尝试清除或删除感染对象。受感染对象的信息会予以记录。<br>默认值：DisinfectDeleteIfNotPossible。 |
| UseExcludeMasks | 启用从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 | Yes — 从扫描中排除 ExcludeMasks.item_# 设置指定的对象。<br>No（默认值）不从扫描中排除由 ExcludeMasks.item_# 设置指定的对象。 |
| 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。 | 默认值为未定义。<br>示例<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |
| UseExcludeThreats | 允许从扫描中排除包含 ExcludeThreats.item_# 设置所指定威胁的对象。 | Yes — 从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。<br>No（默认值）：不从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。 |
| 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。<br>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。<br>例如，您可能正在使用实用程序来获取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。<br>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。 | 该设置值区分大小写。<br>默认值为未定义。<br>示例<br>UseExcludeThreats=Yes<br>ExcludeThreats.item_0000=EICAR-Test-*<br>ExcludeThreats.item_0001=?rojan.Linux |
| UseGlobalExclusions | 针对扫描启用全局排除项。 | Yes（默认值）使用全局排除项。<br>No — 不使用全局排除项。 |
| UseOASExclusions | 针对扫描启用文件威胁防护排除项。 | Yes（默认值）使用文件威胁防护排除项。<br>No — 不使用文件威胁防护排除项。 |
| 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。<br>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 — 记录有关未感染的对象的信息。<br>No（默认值）不记录有关未感染对象的信息。 |
| 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。<br>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 — 记录有关存档中已扫描对象的信息。<br>No（默认值）不记录有关存档中已扫描对象的信息。 |
| ReportUnprocessedObjects | 启用记录由于某种原因尚未处理的对象的有关信息。 | Yes — 记录有关未处理对象的信息。<br>No（默认值）不记录有关未处理对象的信息。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseAnalyzer | 启用启发式分析。<br>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（默认值）启用启发式分析器。<br>No — 禁用启发式分析器。 |
| HeuristicLevel | 指定启发式分析级别。<br>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 — 扫描最不全面，系统负载最小。<br>Medium — 中度启发式分析级别，操作系统负载均衡。<br>Deep — 最全面的扫描，操作系统负载最大。<br>Recommended（默认值）– 推荐值。 |
| UseIChecker | 启用 iChecker 技术。 | Yes（默认值）启用 iChecker 技术。<br>No — 禁用 iChecker 技术。 |
| DeviceNameMasks.item_# | 设备名称列表。应用程序将扫描这些设备的引导扇区。<br>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。 | AllObjects – 扫描所有设备的引导扇区。<br><device name mask> – 扫描名称与指定掩码匹配的设备的引导扇区。<br>默认值：/** – 设备名称中的任意一组字符，包括 / 字符）。 |

# 关键区域扫描任务

下表介绍了您可以为关键区域扫描任务（Critical_Areas_Scan）指定的所有设置的全部可用值和默认值。

关键区域扫描任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ScanFiles | 启用文件扫描。 | Yes — 扫描文件。<br>No（默认值）— 不扫描文件。 |
| ScanBootSectors | 启用引导扇区扫描。 | Yes（默认值）— 扫描引导扇区。<br>No — 不扫描引导扇区。 |
| ScanComputerMemory | 启用进程内存和内核内存扫描。 | Yes（默认值）— 扫描进程内存和内核内存。<br>No — 不扫描进程内存和内核内存。 |
| ScanStartupObjects | 启用启动对象扫描。 | Yes（默认值）— 扫描启动对象。<br>No — 不扫描启动对象。 |
| ScanArchived | 启用存档扫描（包括 SFX 自解压存档）。<br>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（默认值）— 扫描压缩文件。<br>如果将 ActionOnThreat 设置为 DisinfectDeleteIfNotPossible，并且无法清除，则应用程序将根据压缩文件类型，删除感染对象或包含威胁的整个压缩文件。<br>No — 不扫描压缩文件。 |
| 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（默认值）— 扫描自解压存档。<br>No — 不扫描自解压存档。 |
| 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 — 扫描电子邮件数据库的文件。<br>No（默认值）— 不扫描电子邮件数据库的文件。 |
| ScanPlainMail | 启用对纯文本电子邮件的扫描。 | Yes — 扫描纯文本电子邮件。<br>No（默认值）— 不扫描纯文本电子邮件。 |

| 设置 | 描述 | 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 至 999999<br>0 — 应用程序扫描任意大小的对象。<br>默认值：0。 |
| 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 至 9999<br>0 — 对象扫描时间不受限制。<br>默认值：0。 |
| QueueScanTasks | 如果先前启动的计划扫描仍在运行，则延迟计划扫描任务。如果当前扫描仍在运行，Kaspersky Endpoint Security 会将计划扫描任务加入队列。这有助于优化计算机上的负载。例如，扫描任务计划在 18:00 和 20:00 运行。如果 18:00 的扫描仍在运行，则计划在 20:00 运行的扫描任务将被延迟。延迟的任务将在 18:00 的任务完成后运行。 | Yes，如果当前扫描仍在运行，则将计划扫描任务加入队列。<br>No（默认值），即使当前扫描仍在运行，也运行计划扫描任务。 |
| ActionOnThreat | 选择应用程序将对感染对象执行的操作。 | DisinfectDeleteIfNotPossible（清除；如果无法清除则删除）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>DisinfectInformIfNotPossible（清除；如果无法清除则通知）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>Inform 表示应用程序不会尝试清除或删除感染对象。受感染对象的信息会予以记录。<br>默认值：DisinfectDeleteIfNotPossible。 |
| UseExcludeMasks | 启用从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 | Yes — 从扫描中排除 ExcludeMasks.item_# 设置指定的对象。<br>No（默认值）— 不从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 |
| 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。<br>在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。 | 默认值为未定义。<br>示例<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |
| UseExcludeThreats | 允许从扫描中排除包含 ExcludeThreats.item_# 设置所指定威胁的对象。 | Yes — 从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。<br>No（默认值）：不从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。 |
| 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。<br>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。<br>例如，您可能正在使用实用程序来获取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。<br>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。 | 该设置值区分大小写。<br>默认值为未定义。<br>示例<br>UseExcludeThreats=Yes<br>ExcludeThreats.item_0000=EICAR-Test-*<br>ExcludeThreats.item_0001=?rojan.Linux |
| UseGlobalExclusions | 针对扫描启用全局排除项。 | Yes（默认值）— 使用全局排除项。<br>No — 不使用全局排除项。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseOASExclusions | 针对扫描启用文件威胁防护排除项。 | Yes（默认值）– 使用文件威胁防护排除项。<br>No – 不使用文件威胁防护排除项。 |
| 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。<br>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 – 记录有关未感染的对象的信息。<br>No（默认值）–不记录有关未感染的对象的信息。 |
| 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。<br>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 – 记录有关存档中已扫描对象的信息。<br>No（默认值）– 不记录有关存档中已扫描对象的信息。 |
| ReportUnprocessedObjects | 启用记录由于某种原因尚未处理的对象的有关信息。 | Yes – 记录有关未处理对象的信息。<br>No（默认值）–不记录有关未处理对象的信息。 |
| UseAnalyzer | 启用启发式分析。<br>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（默认值）– 启用启发式分析器。<br>No – 禁用启发式分析器。 |
| HeuristicLevel | 指定启发式分析级别。<br>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 – 扫描最不全面，系统负载最小。<br>Medium – 中度启发式分析级别，操作系统负载均衡。<br>Deep – 最全面的扫描，操作系统负载最大。<br>Recommended（默认值）– 推荐值。 |
| UseIChecker | 启用 iChecker 技术。 | Yes（默认值）– 启用 iChecker 技术。<br>No – 禁用 iChecker 技术。 |
| DeviceNameMasks.item_# | 设备名称列表。应用程序将扫描这些设备的引导扇区。<br>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。 | AllObjects – 扫描所有设备的引导扇区。<br><device name mask> – 扫描名称与指定掩码匹配的设备的引导扇区。<br>默认值：/** – 设备名称中的任意一组字符，包括 / 字符）。 |
| **[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：All objects。<br>示例<br>AreaDesc="Mail bases scan" |
| 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（默认值）– 扫描指定的范围。<br>No – 不扫描指定的范围。 |
| 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。<br>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：*（扫描所有对象）。<br>示例<br>AreaMask.item_0000=*doc |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `Path` | 包含要扫描的对象的目录的路径。 | `<path to local directory>` – 扫描指定目录中的对象。<br>`Shared:NFS` — 扫描可通过 NFS 协议访问的设备文件系统资源。<br>`Shared:SMB` – 扫描可通过 Samba 协议访问的设备文件系统资源。<br>`Mounted:NFS` — 扫描使用 NFS 协议挂载到设备上的远程目录。<br>`Mounted:SMB` — 扫描使用 Samba 协议挂载到设备上的远程目录。<br>`AllRemoteMounted` — 扫描使用 Samba 和 NFS 协议挂载到设备上的所有远程目录。<br>`AllShared` — 扫描可通过 SMB 和 NFS 协议访问的所有设备文件系统资源。<br>`<file system type>` – 扫描指定文件系统设备的所有资源。 |
| **[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。 | 默认值为未定义。 |
| `UseScanArea` | 从扫描中排除指定的范围。 | `Yes`（默认值）— 排除指定的范围。<br>`No` — 不排除指定的范围。 |
| `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。<br>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：`*`（排除所有对象）。 |
| `Path` | 包含要排除的对象的目录的路径。 | `<path to local directory>` – 从扫描中排除指定目录（包括子目录）中的对象。您可以使用掩码指定路径。<br>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，可以添加以下排除项：`/.snapshots/*/snapshot/`。<br>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。<br>`Mounted:NFS` — 从扫描中排除使用 NFS 协议在设备上挂载的远程目录。<br>`Mounted:SMB` — 从扫描中排除使用 SMB 协议在设备上挂载的远程目录。<br>`AllRemoteMounted` — 在扫描中排除使用 SMB 和 NFS 协议挂载在设备上的所有远程目录。<br>`<file system type>` – 从扫描中排除指定文件系统设备的所有资源。<br>仅当远程目录在任务启动之前安装时，应用程序才会将其排除在扫描之外。任务启动后安装的远程目录不会被排除在扫描之外。 |

实用文章

**如何指定掩码**

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。

# “可移动驱动器扫描”任务

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*不运行。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。

如果修改“*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` | 启用在可移动介质连接到设备时对其进行扫描的功能。<br>此设置不适用于 CD/DVD 驱动器和蓝光光盘（请参阅 `ScanOpticalDrives` 设置）。 | `DetailedScan`。扫描可移动介质（不包括 CD/DVD 和蓝光光盘）上的所有文件。<br>使用 `Scan_File` 任务（ID：3）的默认设置执行详细扫描。<br>`QuickScan`。仅扫描可移动介质（不包括 CD/DVD 和蓝光光盘）上的**特定类型**文件。<br>在可移动介质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、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。<br>使用 Critical_Areas_Scan 任务（ID：4）的`Critical_Areas_Scan` 设置执行快速扫描。<br>`NoScan`（默认值）– 当可移动介质连接到设备时不扫描该介质。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。<br>使用 Scan_File 任务（ID：3）的默认设置执行详细扫描。<br>QuickScan。仅扫描 CD/DVD 驱动器和蓝光光盘上的**特定类型**文件。<br>在可移动介质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、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。<br>使用 Critical Areas Scan 任务（ID：4）的Critical_Areas_Scan 设置执行快速扫描。<br>NoScan （默认值）。连接 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。<br>No （默认值）– 扫描过程中不阻止文件。 |

# 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此任务，并配置任务计划。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，并配置任务计划。
- 使用以下命令，您可以对指定的容器和镜像执行*自定义扫描*：

```
kesl-control --scan-container
```

## 容器扫描设置

下表介绍了在实时扫描命名空间和容器时使用的容器扫描设置。

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。<br>在支持此功能的授权许可下使用应用程序时，此设置可用。<br>“文件威胁防护”任务设置在扫描容器内的对象时使用。 | StopContainerIfFailed （默认值）- 如果无法清除或删除受感染对象，则停止容器。如果指定了此值，则对容器执行的操作还取决于ActionOnThreat 的 ActionOnThreat设置。如果将ActionOnThreat 设置为 DisinfectDeleteIfNotPossible，且应用程序在执行操作时无法清除或删除受感染对象，则容器将被停止。<br>StopContainer — 检测到受感染对象时停止容器。<br>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 容器管理系统。 | Yes （默认）启用 Docker 容器管理系统。<br>No 禁用 Docker 容器管理系统。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。<br>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。<br>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。<br>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。 |

## 容器扫描任务

该表介绍了可为容器扫描任务 (Container_Scan) 指定的所有设置的全部可用值和默认值。

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。<br>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。<br>掩码以命令 Shell 格式指定。您可以使用 ? 和 * 符号。<br>在指定此设置之前，请确保 ScanContainers=Yes。 | 默认值：*（扫描所有容器）。<br>对名为 my_container 的容器执行容器扫描的示例<br>ContainerNameMask=my_container<br>扫描名称以 my_container 开头的所有容器的示例<br>ContainerNameMask=my_container*<br>对所有符合以下条件的容器执行容器扫描的示例：名称以 my_ 开头，后接任意五个字符，再接 _container，并以任意字符序列结尾<br>ContainerNameMask=my_?????_container* |
| ScanImages | 扫描按掩码指定的镜像。您可以使用 ImageNameMask 设置指定掩码。 | Yes （默认值）— 扫描由掩码定义的镜像。<br>No — 不扫描由掩码定义的镜像。 |
| ImageNameMask | 指定定义要扫描的镜像的名称或名称掩码。<br>在指定此设置之前，请确保 ScanImages 设置值已设为 Yes。<br>掩码以命令 Shell 格式指定。<br>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：*（扫描所有镜像）。<br>对名称为“my_image”且标签为“latest”的镜像执行镜像扫描的示例<br>ImageNameMask=my_image:latest<br>对名称以 my_image_ 开头且带有任意标签的所有镜像执行镜像扫描的示例<br>ImageNameMask=my_image* |
| DeepScan | 检查所有镜像层和正在运行的容器。 | Yes — 扫描所有层。<br>No （默认值）— 不扫描任何层。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。如果选择此值，则对容器执行的操作还取决于ActionOnThreat设置，该设置应用于容器和镜像内的对象（参见下表）。如果将ActionOnThreat设置为DisinfectDeleteIfNotPossible，且应用程序在执行操作时无法清除或删除受感染对象，则容器将被停止。<br>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。<br>StopContainer — 检测到受感染的对象时，应用程序会停止容器。<br>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镜像执行的操作。下面介绍了对镜像内受感染对象的操作。 | Skip（默认值）– 检测到受感染的对象时，应用程序不会对镜像执行任何操作。<br>Delete — 当检测到受感染的对象时，应用程序会删除镜像（不推荐）。<br>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 | 值 |
| --- | --- | --- |
| ScanArchived | 启用存档扫描（包括 SFX 自解压存档）。<br>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（默认值）— 扫描压缩文件。<br>如果将 ActionOnThreat 设置为 DisinfectDeleteIfNotPossible，并且无法清除，则应用程序将根据压缩文件类型，删除感染对象或包含威胁的整个压缩文件。<br>No — 不扫描压缩文件。 |
| 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（默认值）— 扫描自解压存档。<br>No — 不扫描自解压存档。 |
| 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 — 扫描电子邮件数据库的文件。<br>No（默认值）— 不扫描电子邮件数据库的文件。 |
| ScanPlainMail | 启用对纯文本电子邮件的扫描。 | Yes — 扫描纯文本电子邮件。<br>No（默认值）— 不扫描纯文本电子邮件。 |
| 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 至 9999<br>0 — 对象扫描时间不受限制。<br>默认值：0。 |
| 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 至 999999<br>0 — 应用程序扫描任意大小的对象。<br>默认值：0。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ActionOnThreat | 选择应用程序将对感染对象执行的操作。 | DisinfectDeleteIfNotPossible（清除；如果无法清除则删除）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>DisinfectInformIfNotPossible（清除；如果无法清除则通知）表示应用程序将对象副本保存到备份区后尝试清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>Inform 表示应用程序不会尝试清除或删除感染对象。受感染对象的信息会予以记录。<br>默认值：DisinfectDeleteIfNotPossible。 |
| UseExcludeMasks | 对 ExcludeMasks.item_# 设置指定的对象使用扫描排除项。 | Yes — 从扫描中排除 ExcludeMasks.item_# 设置指定的对象。<br>No（默认值）— 不从扫描中排除 ExcludeMasks.item_# 设置指定的对象。 |
| 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。 | 默认值为未定义。<br>示例<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |
| UseExcludeThreats | 对包含 ExcludeThreats.item_# 设置指定的威胁的对象使用扫描排除项。 | Yes — 从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。<br>No（默认值）：不从扫描中排除包含 ExcludeThreats.item_# 设置指定的威胁的对象。 |
| 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。<br>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。<br>例如，您可能正在使用实用程序来获取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。<br>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。 | 该设置值区分大小写。<br>默认值为未定义。<br>示例<br>UseExcludeThreats=Yes<br>ExcludeThreats.item_0000=EICAR-Test-*<br>ExcludeThreats.item_0001=?rojan.Linux |
| UseGlobalExclusions | 针对扫描启用全局排除项。 | Yes（默认值）— 使用全局排除项。<br>No — 不使用全局排除项。 |
| 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。<br>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 — 记录有关未感染的对象的信息。<br>No（默认值）—不记录有关未感染的对象的信息。 |
| 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。<br>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 — 记录有关存档中已扫描对象的信息。<br>No（默认值）— 不记录有关存档中已扫描对象的信息。 |
| ReportUnprocessedObjects | 启用记录由于某种原因尚未处理的对象的有关信息。 | Yes — 记录有关未处理对象的信息。<br>No（默认值）—不记录有关未处理对象的信息。 |
| UseAnalyzer | 启用启发式分析。<br>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（默认值）— 启用启发式分析器。<br>No — 禁用启发式分析器。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `HeuristicLevel` | 指定启发式分析级别。<br>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` — 扫描最不全面，系统负载最小。<br>`Medium` — 中度启发式分析级别，操作系统负载均衡。<br>`Deep` — 最全面的扫描，操作系统负载最大。<br>`Recommended`（默认值）— 推荐值。 |
| `UseIChecker` | 启用 iChecker 技术。 | `Yes`（默认值）— 启用 iChecker 技术。<br>`No` — 禁用 iChecker 技术。 |
| `QueueScanTasks` | 如果先前启动的计划扫描仍在运行，则延迟计划扫描任务。如果当前扫描仍在运行，Kaspersky Endpoint Security 会将计划扫描任务加入队列。这有助于优化计算机上的负载。例如，扫描任务计划在 18:00 和 20:00 运行。如果 18:00 的扫描仍在运行，则计划在 20:00 运行的扫描任务将被延迟。延迟的任务将在 18:00 的任务完成后运行。 | `Yes`，如果当前扫描仍在运行，则将计划扫描任务加入队列。<br>`No`（默认值），即使当前扫描仍在运行，也运行计划扫描任务。 |

## 与 Jenkins 整合

Kaspersky Endpoint Security 支持与 Jenkins 整合。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：

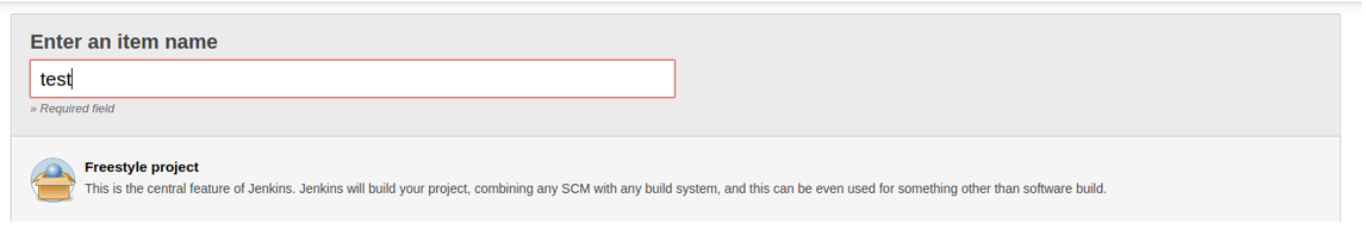
   ```
   kesl-control --grant-role admin <Jenkins user name>
   ```

4. 将 Jenkins 用户添加到 docker 组：

   ```
   sudo usermod -aG docker <Jenkins user name>
   ```

   通常使用 jenkins 这一名称。

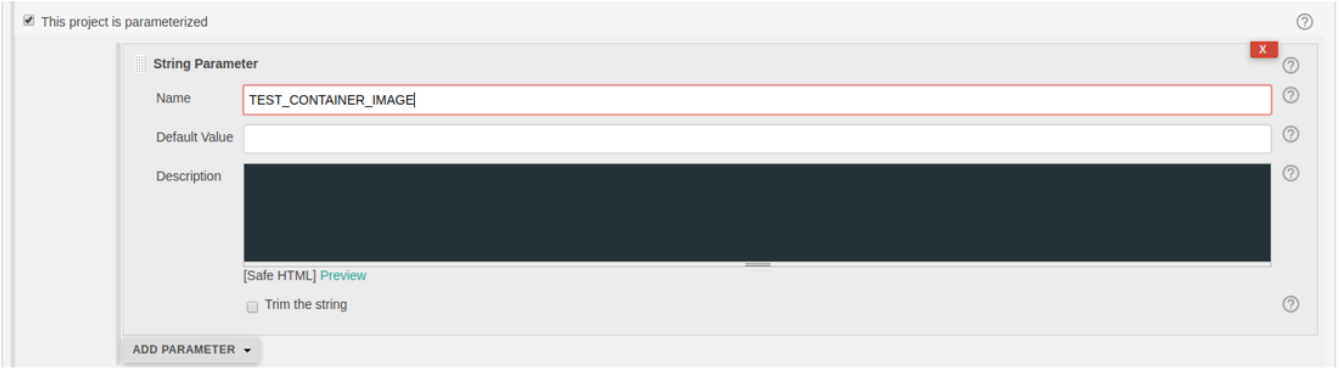
5. 在 Jenkins 中，创建一个名为 `test` 的新构建作业（**新建项目** → **输入项目名称**）。




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 插件或其他方式启动 Docker 容器，请将正在运行的 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. 要扫描存储库中的 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。

# 反加密勒索任务

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。<br>`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）。<br>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。<br>默认值：30。 |
| `UseExcludeMasks` | 启用从保护范围中排除 `ExcludeMasks.item_#` 设置指定的对象。<br>仅当指定 `ExcludeMasks.item_#` 设置时，此设置才适用。 | `Yes` – 从保护范围中排除 `ExcludeMasks.item_#` 设置指定的对象。<br>`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。<br>在为此设置指定值之前，请确保已启用 `UseExcludeMasks` 设置。<br>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。 | 默认值为未定义。 |
| **[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。<br>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。<br>[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。<br>`No` – 不保护指定的范围。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。<br>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）。 |
| `Path` | 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。<br>`AllShared`（默认值）– 保护可通过 SMB/NFS 访问的所有资源。<br>`Shared:SMB` – 保护可通过 SMB 访问的资源。<br>`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。<br>[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。<br>`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。<br>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）。 |
| `Path` | 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。<br>`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。<br>`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。<br>`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。 |

实用文章

**如何指定掩码**

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。

# 行为检测任务

您可以使用行为检测预定义任务（`Behavior_Detection`），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 |
| --- | --- | --- |
| UseTrustedPrograms | 从扫描中排除进程。 | Yes – 不扫描指定进程的活动。<br>No（默认值）– 扫描所有进程。 |
| 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。<br>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。 |
| TelemetrySource | 与 Detection and Response 解决方案集成时，用于收集发送到此类解决方案的遥测数据的其他设置。<br>仅当UseTelemetryMonopolyMode被设置为TelemetrySource时，Default设置才应用。 | Default（默认）表示使用 eBPF 技术和 auditd 服务来获取遥测数据。<br>OnlyEBPF 表示仅使用 eBPF 技术获取遥测数据。 |
| UseTelemetryMonopolyMode | 此设置不适用于配备 Elbrus CPU 的设备。 | True（默认值）表示 Kaspersky Endpoint Security 以独占模式使用 auditd 服务。<br>False表示 auditd 服务以非独占模式使用。 |
| **[TrustedPrograms.item_#]** 部分包含从行为检测扫描中排除的进程。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。 |
| 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。<br>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 | 将指定进程的活动排除在扫描范围之外。 | Yes（默认值）— 将指定进程的活动排除在扫描范围之外。<br>No — 不将指定进程的活动排除在扫描范围之外。 |
| UseTrustedProgramForDetects | 将某个进程的活动排除在行为检测的扫描范围之外。 | 如果设置为Yes，则指定进程的活动将被排除在行为检测的扫描范围之外。<br>如果设置为No（默认），则指定进程的活动不会被排除在行为检测的扫描范围之外。 |
| UseTrustedProgramForMDRAndEDR | 将进程从 MDR 和 EDR Expert (on-premises) 组件收集的遥测数据中排除。<br>此设置不适用于配备 Elbrus CPU 的设备。 | Yes – 将此进程的活动从 MDR 和 EDR Expert (on-premises) 组件收集的遥测数据中排除。<br>No（默认值）— 不将此进程的活动从遥测中排除。 |

实用文章

## 如何指定掩码

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。

# 漏洞利用防御

在命令行上，您可以使用行为检测预定义任务 (Behavior_Detection) 的设置来管理漏洞利用防御。

您可以通过编辑行为检测预定义任务的设置来配置漏洞利用防御（请见下表）。

漏洞利用防御设置

| 设置 | 描述 | 值 |
|---|---|---|
| UseAEP | 启用漏洞利用防御组件。 | Yes 启用漏洞利用防御。<br>No （默认）禁用漏洞利用防御。 |
| AEPMode | 检测到漏洞利用时要执行的操作。 | 如果设置为 Block （默认），则会阻止漏洞利用的恶意活动并记录事件日志。<br>如果设置为 Notify，则不会阻止漏洞利用活动，只有关于检测到的漏洞利用的信息会记录在事件日志中。 |
| [AEPExclusions.item_#]部分包含漏洞利用防御组件的扫描排除项。 | | |
| Enabled | 启用漏洞利用防御保护组件的扫描排除。 | Yes （默认值）– 使用漏洞利用防御排除。<br>No – 不使用漏洞利用防御排除。 |
| DetectName | 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 UseDetectName 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。<br>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。 |
| Hash | 排除通过哈希值检测到威胁的对象。在为此设置指定值之前，请确保已启用 UseHash 设置。 | |
| HashType | 您想要使用 Hash 参数排除文件扫描的文件哈希类型。 | Md5 – MD5 哈希值<br>Sha256 – SHA256 哈希值 |
| Path | 排除按照路径检测到威胁的对象。在为此设置指定值之前，请确保已启用 UsePath 设置。 | < 文件或本地目录的完整路径 > – 从扫描中排除指定目录（包括子目录）中的文件或对象。路径中可以使用 * 和 ? 字符。 |
| UseDetectName | 允许从扫描中排除包含 DetectName 设置所指定威胁的对象。 | Yes （默认值）– 从扫描中排除包含 DetectName 设置指定的威胁的对象。<br>No – 不从扫描中排除包含使用 DetectName 设置指定的威胁的对象 |
| UseHash | 根据哈希值排除检测到威胁的文件。文件哈希值在 Hash 参数中指定。 | Yes （默认值）– 通过哈希值排除检测到威胁的文件。<br>No – 不按哈希值排除检测到威胁的文件。 |
| UsePath | 根据路径排除检测到威胁的文件。文件路径通过 Path 参数指定。 | Yes （默认值）– 按路径排除检测到威胁的文件。<br>No – 不按路径排除检测到威胁的文件。 |

# 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更改 UseKSN 设置的值。

*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`：一个选项，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 <path to the configuration file> [--json] [--accept-ksn]
```

其中：

`--file <path to the configuration file>` 是包含常规应用程序设置的配置文件的完整路径，在该文件中配置了所需的 UseKSN 值。

如果要从 JSON配置文件导入设置，请指定 `--json` 选项。如果不指定 `--json`选项，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`：一个选项，表示您同意卡巴斯基安全网络声明中条款的密钥。如果您要启用卡巴斯基安全网络，则必须指定该选项。

如果客户端设备上安装的 Kaspersky Endpoint Security 在 Kaspersky Security Center 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`。

## 连接到卡巴斯基安全网络

*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* 状态，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* 状态，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。
- 如果显示 *KSN 未在使用中* 状态，则 Kaspersky Endpoint Security 不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：*KSN* 或*KPSN*。

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。
- 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。

### 启用或禁用云模式

*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。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则不支持使用轻量级恶意软件数据库。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` 设置。

如果启用对卡巴斯基安全网络的使用，则云模式可用。

## BadUSB 攻击防护任务

在命令行中，您还可以使用预定义的 BadUSB 攻击防护预定义任务 (`Bad_USB`) 来管理 BadUSB 攻击防护。

BadUSB 攻击防护任务默认不启动。您可以手动启动和停止该任务。

要从命令行启动和停止 BadUSB 攻击防护任务，需要管理员角色权限。

您可以通过编辑BadUSB 攻击防护预定义任务的设置来管理 BadUSB 攻击防护设置。

下表描述了您可以为 BadUSB 攻击防护任务指定的设置的可用值和默认值。

BadUSB 攻击防护任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `MaxAuthAttempts` | USB 设备授权尝试的最大次数，此后应用程式将在 `TimeoutAfterAttempts` 参数中指定的时长内阻止 USB 设备和继续授权 USB 设备的尝试。 | 可能的值：1 到 10<br>默认值：5。 |
| `TimeoutAfterAttempts` | 在 `MaxAuthAttempts` 次输入授权码失败后阻止 USB 设备的时长。 | 可能的值：1 到 180 分钟。默认值：5 分钟。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ProhibitOnScreenKeyboard | 禁止或允许使用屏幕键盘授权 USB 设备。 | 如果设置为 Yes，则应用程序不允许使用屏幕键盘对无法输入授权码的 USB 设备进行键盘授权。<br>如果设置为No，则应用程序允许使用屏幕键盘对无法输入授权码的 USB 设备进行键盘授权。 |
| ProhibitBarcodeScanner | 启用或禁用将授权码显示为条形码，以便授权无法输入授权码的 USB 设备。 | Yes （默认）禁止将授权码显示为条形码。<br>No 允许将授权码显示为条形码。 |

# 通信和 Web 保护

## Web 威胁防护任务

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。 | Notify – 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。<br>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 | 根据恶意网址数据库检查链接。 | Yes （默认值） – 检查链接是否列在恶意链接数据库中。<br>No – 不检查链接是否列在恶意链接数据库中。 |
| CheckPhishing | 根据网络钓鱼网址数据库检查链接。 | Yes （默认值） – 检查链接是否列在网络钓鱼链接数据库中。<br>No – 不检查链接是否列在网络钓鱼链接数据库中。 |
| UseHeuristicForPhishing | 使用启发式分析扫描网页中的钓鱼链接。<br>此设置不适用于配备 Elbrus CPU 的设备。 | 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。<br>No – 不使用启发式分析来检测钓鱼链接。 |
| CheckAdware | 根据广告网址数据库检查链接。 | Yes – 检查链接是否列在广告软件链接数据库中。<br>No （默认值） – 不检查链接是否列在广告软件链接数据库中。 |
| CheckOther | 根据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数据库检查链接。 | 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。<br>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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseTrustedAddresses | 使用受信任网址列表。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_# 设置指定受信任网址。 | Yes（默认值）– 使用受信任网址列表。<br>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。<br>您可以使用掩码指定网址。<br>不支持使用掩码指定 IP 地址。 |

实用文章

**如何指定掩码**

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）。

# 扫描网络流量

在命令行上，您可以使用特殊的管理命令来管理网络流量扫描设置。您可以使用网络流量扫描设置管理命令来执行以下操作：

- 管理网络流量扫描设置。
- 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。
- 配置应用程序在扫描加密连接时使用的受信任根证书列表。
- 配置和查看流量拦截排除。

## 查看和编辑网络流量扫描设置

您可以使用特殊的网络流量扫描设置管理命令来：

- 将网络流量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。
- 使用配置文件管理所有网络流量扫描设置。您可以获取一个配置文件，可以使用显示网络流量扫描设置输出命令对其进行编辑。
- 使用命令行选项以 < 设置名称 >=< 设置值 > 格式编辑单个设置。您可以使用输出网络流量扫描设置的命令获取设置的当前值。

*要将当前网络流量扫描设置输出到控制台，请执行以下命令：*

```
kesl-control --get-net-settings [--json]
```

其中指定 `--json` 后，将以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

*要将当前网络流量扫描设置输出到文件，请运行以下命令：*

```
kesl-control --get-net-settings --file <path to configuration file> [--json]
```

其中：

- `--file <path to the configuration file>` 是将保存网络流量扫描设置的文件的路径。如果您指定文件名而不指定其路径，则将在当前目录中创建文件。如果指定路径中已存在具有指定名称的文件，则它将被覆盖。如果在磁盘上找不到指定目录，则不会创建文件。
- 指定 `--json`，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

*要使用配置文件管理网络扫描设置：*

1. 将网络流量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. 运行以下命令：

   ```
   kesl-control --set-net-settings --file <path to the configuration file> [--json]
   ```

   其中：

   - `--file <path to the configuration file>` 是包含网络流量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`选项，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。

   文件中配置的所有网络流量扫描设置都将被导入到应用程序中。

*要在命令行上编辑网络流量扫描设置，请运行以下命令：*

```
kesl-control --set-net-settings <parameter name>=<parameter value> [<parameter name>=<parameter value>]
```

其中 `<parameter name>=<parameter value>` 是 网络流量扫描设置的名称和值。

指定设置的值已被修改。

## 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加密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加密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加密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
```

## 管理受信任根证书列表

*要将证书添加到受信任的根证书列表，请运行以下命令：*

```
kesl-control --add-certificate <path to the certificate>
```

其中：

`<path to the certificate>` 是要添加的证书文件（PEM 或 DER 格式）的路径。

*要将证书从受信任的根证书列表中移除，请运行以下命令：*

```
kesl-control --remove-certificate <subject of the certificate>
```

*要查看受信任的根证书列表，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
- 证书发布者
- 证书开始日期

- 证书到期日期
- SHA256 证书指纹

## 配置和查看流量拦截排除

*要添加流量拦截排除项，请运行以下命令：*

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port <destination
port>
```

其中：

- `<in|out>` 是被排除连接中的流量方向。您可以为入站流量或出站流量配置排除项。
- `<remote IP address>` 是远程设备的 IPv4 或 IPv6 地址。根据流量方向，来自指定 IP 地址的流量（入站流量排除项）或去往指定 IP 地址的流量（传出流量排除项）被排除。
- `<destination port>` 是以下项，具体取决于流量方向：
  - 受保护设备上的端口（入站流量排除项）。从远程设备到此端口的流量不被拦截。
  - 远程设备上的端口（出站流量排除项）。从受保护设备到此端口的流量不被拦截。

在排除项中，您可以指定没有端口的远程设备的 IP 地址或没有 IP 地址的目标端口。

如果在入站流量排除项中仅指定远程设备的 IP 地址（未指定受保护设备上的端口），则来自远程设备的所有流量都将被排除在拦截之外。我们建议仅为来自您信任的设备的流量配置此排除项。

*要查看已配置的流量拦截排除列表，请运行以下命令：*

```
kesl-control --list-bypass-endpoints
```

将显示每个排除项的以下信息：

- 排除项序列号
- 流量方向
- 远程设备的 IP 地址
- 端口号

*要删除流量拦截排除项，请运行以下命令：*

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

其中：

- `<in|out>` 是被排除连接中的流量方向。
- `<remote IP address` 是远程设备的 IPv4 或 IPv6 地址，该设备的流量被排除在拦截范围之外（取决于流量方向）。
- `<destination port>` 是受保护设备上的端口（入站流量排除项）或远程设备上的端口（出站流量排除项）。

## 网络威胁防护任务

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` | 当检测到具有网络攻击典型特征的网络活动时所执行的操作。<br>将此设置的值从 `Block` 更改为 `Notify` 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。<br>`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。<br>`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 至 32768<br>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。<br>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。<br>`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。<br>`d.d.d.d/p` – IPv4 地址子网，其中 p 是介于 0 到 32 之间的数字。<br>`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。<br>`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。<br>默认值为未定义。 |

## 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。

您可以通过编辑防火墙管理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。
- 使用以下命令查看应用程序中创建的防火墙规则：

```
kesl-control -F --query
```

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。<br>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。<br>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。<br>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。<br>每个 [PacketRules.item_#] 部分均包含以下设置：<br> | | |
| 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。<br>Block – 阻止网络连接。 |
| Protocol | 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。<br>TCP<br>UDP<br>ICMP<br>ICMPv6<br>IGMP<br>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。<br>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。<br>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。<br>只有将 Protocol 设置设为 TCP 或 UDP 时，才能指定此设置。 | Any（默认值） – 监控所有本地端口。<br>0 – 65535。 |
| ICMPType | ICMP 数据包类型。<br>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。<br>符合数据传输协议规范的一个整数。 |
| ICMPCode | ICMP 数据包代码。<br>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。<br>符合数据传输协议规范的一个整数。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。<br>`Incoming` 或 `In` – 仅监控入站连接。<br>`Outgoing` 或 `Out` – 仅监控出站连接。<br>`IncomingPacket` 或 `InPacket` – 仅监控传入数据包。<br>`OutgoingPacket` 或 `OutPacket` – 仅监控传出数据包。<br>`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。<br>`Trusted` – 可信网络的预定义网络区域。<br>`Local` – 本地网络的预定义网络区域。<br>`Public` – 公用网络的预定义网络区域。<br>`d.d.d.d` – IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。<br>`d.d.d.d – d.d.d.d` – IPv4 地址范围。<br>`d.d.d.d/p` – IPv4 地址子网，其中 p 是介于 0 到 32 之间的数字。<br>`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。<br>`x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – IPv6 地址范围。<br>x:x:x:x:x:x:x:x/p – IPv6 地址子网，其中 p 是 0 到 128 之间的数字；为了简洁起见，可以使用 ::。 |
| `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。<br>`d.d.d.d` – IPv4 地址，其中 d 是十进制数字，范围为 0 至 255。<br>`d.d.d.d – d.d.d.d` – IPv4 地址范围。<br>`d.d.d.d/p` – IPv4 地址子网，其中 p 是介于 0 到 32 之间的数字。<br>`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。<br>`x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` – IPv6 地址范围。<br>x:x:x:x:x:x:x:x/p – IPv6 地址子网，其中 p 是 0 到 128 之间的数字；为了简洁起见，可以使用 ::。 |
| `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。<br>`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。<br>`d.d.d.d/p` – IPv4 地址子网，其中 p 是介于 0 到 32 之间的数字。<br>`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。<br>`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。<br>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。 | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。<br>`d.d.d.d/p` — IPv4 地址子网，其中 p 是介于 0 到 32 之间的数字。<br>`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。<br>`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。<br>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。<br>`d.d.d.d/p` — IPv4 地址子网，其中 p 是介于 0 到 32 之间的数字。<br>`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。<br>`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。<br>默认值：`""`（此区域中没有网络地址） |

## 配置网络包规则列表

*要添加网络数据包规则，请执行以下命令：*

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

其中：

- `--name <rule name>` 是网络数据包规则的名称。
- `--action <Allow|Block>` 是要对在此网络数据包规则中指定的连接执行的操作。
- `--protocol <protocol>` 是您要监控其网络活动的协议。
- `--direction <direction>` 是受监控网络活动的方向。
- `--remote <remote address>:<port>` 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 <local address>:<port>` 是安装了 Kaspersky Endpoint Security 的设备的网络地址。
- `--at <index>` 是规则在网络数据包规则列表中的索引。如果未指定 `--at` 选项或其值大于列表中的规则数，则新规则将添加到列表末尾。

命令中未指定值的参数被设置为其默认值。

创建阻止所有到 TCP 端口 23 的传入连接和已建立连接的规则的示例

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

创建规则以针对公共网络区域阻止通过 TCP 端口 23 的传入连接和已建立连接的示例

```
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 <rule name>
```

或

```
kesl-control --del-rule --index <current index>
```

其中：

- `--name <rule name>` 是网络数据包规则的名称。
- `--index <current index>` 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 <rule name> --at < new index>
```

或

```
kesl-control --move-rule --index <current index> --at <new index>
```

其中：

- `--name <rule name>` 是网络数据包规则的名称。
- `--index <current index>` 是网络数据包规则列表中的当前规则索引。
- `--at <new index>` 是网络数据包规则列表中的新规则索引。

## 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> --address <address>
```

其中：

- <zone> 是网络区域的预定义名称。可能的值：Public、Local、Trusted。
- <address> 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> --address <address>
```

或

```
kesl-control --del-zone <zone> --index <address index in the zone>
```

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。

# 安全控制

## 设备控制任务

该表介绍了可为设备控制任务（Device_Control）指定的所有设置的全部可能值和默认值。

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）— 应用程序应用为设备或总线定义的访问模式。<br>Notify — 应用程序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。 |
| AllowToRequestTemporaryAccess | 允许请求对被阻止设备的临时访问权限。<br>只有当组织中部署了 Kaspersky Security Center 16.1 并且客户端设备能够与管理服务器建立连接时，才能授予对被阻止设备的访问权限。 | Yes – 允许用户在应用程序的图形界面或命令行中请求临时访问被阻止的设备。<br>No（默认）— 不允许用户请求对被阻止设备的临时访问权限。 |
| **[DeviceClass]** 部分包含设备的访问模式，具体取决于设备的类型。 | | |
| HardDrive | 连接到客户端设备的硬盘驱动器的访问模式。 | Allow – 允许用户访问硬盘驱动器。<br>DependsOnBus（默认）：对硬盘驱动器的访问取决于为连接总线定义的访问模式。<br>Block—用户对所有硬盘驱动器（除了系统硬盘驱动器，这些驱动器绝不会被设备控制阻止）的访问均被阻止。<br>ByRule – 对于硬盘驱动器的访问权限取决于访问规则。<br>ReadOnly — 用户对硬盘驱动器具有只读权限，写入被阻止。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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驱动器。<br>DependsOnBus（默认）– 对可移动驱动器的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问可移动驱动器。<br>ByRule – 对于可移动驱动器的访问权限取决于访问规则。<br>ReadOnly — 用户对可移动驱动器具有只读权限，写入被阻止。 |
| FloppyDrive | 连接到客户端设备的软盘驱动器的访问模式。<br>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 — 允许用户访问软盘驱动器。<br>DependsOnBus（默认）：对软盘驱动器的访问取决于为其所连接的总线定义的访问模式。<br>Block — 阻止用户访问软盘驱动器。<br>ByRule — 对软盘驱动器的访问取决于访问规则。<br>ReadOnly — 用户对软盘驱动器具有只读权限，写入操作被阻止。 |
| 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/DVD。<br>DependsOnBus（默认）– 对 CD/DVD 驱动器的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问 CD/DVD 驱动器。<br>ByRule – 对于 CD /DVD 的访问权限取决于访问规则。<br>ReadOnly — 用户对 CD/DVD 驱动器具有只读权限，写入被阻止。 |
| SerialPortDevice | 通过串行端口连接到客户端设备的设备的访问模式。<br>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行端口连接的设备。<br>DependsOnBus（默认）– 对通过串行端口连接的设备的访问取决于总线访问模式。<br>Block – 阻止用户访问通过串行端口连接的设备。 |
| 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行端口连接的设备。<br>DependsOnBus（默认）– 对通过并行端口连接的设备的访问取决于总线访问模式。<br>Block – 阻止用户访问通过并行端口连接的设备。 |
| 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。<br>DependsOnBus（默认）– 对打印机的访问取决于为连接总线定义的访问模式。<br>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调器。<br>DependsOnBus（默认）– 对调制解调器的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问调制解调器。 |
| 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备。<br>DependsOnBus（默认）– 对磁带设备的访问取决于为连接总线定义的访问模式<br>Block – 阻止用户访问磁带设备。 |
| 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设备。<br>DependsOnBus（默认）– 对多功能设备的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问多功能设备。 |
| 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读卡器。<br>DependsOnBus（默认）– 对智能卡读卡器的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问智能卡读卡器。 |
| 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 适配器。<br>DependsOnBus（默认）– 对 Wi-Fi 适配器的访问取决于连接总线访问模式。<br>Block – 阻止用户访问 Wi-Fi 适配器。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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络适配器。<br>DependsOnBus （默认）– 对外部网络适配器的访问取决于为连接总线定义的访问模式。<br>设备控制不允许拒绝访问外部网络适配器，以免客户端设备与网络断开连接。 |
| 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设备。<br>DependsOnBus （默认）– 对便携式设备的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问便携式设备。 |
| 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备。<br>DependsOnBus （默认）– 对蓝牙设备的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问蓝牙设备。 |
| 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像设备。<br>DependsOnBus （默认）– 对成像设备的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问所有成像设备。 |
| 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音适配器。<br>DependsOnBus （默认）– 对声音适配器的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问所有声音适配器。 |
| 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备。<br>DependsOnBus （默认）– 对输入设备的访问取决于为连接总线定义的访问模式。<br>Block – 阻止用户访问输入设备。 |
| **[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） – 允许用户访问 USB 设备。<br>Block – 阻止用户访问 USB 设备。 |
| FireWire | 通过 FireWire 连接到客户端设备的设备的访问模式。 | Allow （默认值） – 允许用户访问通过 FireWire 接口连接的设备。<br>Block – 阻止用户访问通过 FireWire 接口连接的设备。 |
| **[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 *（任意字符序列）或？（任意一个字符）指示设备 ID。<br>例如：<br>*要拒绝访问除指定 USB 设备之外的所有 USB 设备，请指定以下设置：*<br>在 [DeviceBus] 部分中，指定 USB=Block<br>在 [TrustedDevices.item_#] 部分中，指定 DeviceId=<device ID><br>*要拒绝访问所有 USB 设备，但允许访问所有 USB 驱动器，请指定以下设置：*<br>在 [DeviceBus] 部分中，指定 USB=Block<br>在 [TrustedDevices.item_#] 部分中，指定 DeviceId=USBSTOR* |
| Comment | 对指定的受信任设备的注释。 | — |
| **[TrustedDevices.item_#.Principals.item_#]** 部分包含访问受信任设备的规则。 | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| Principal | 受信任设备的用户或用户组。<br>如果设备具有"只读"访问类型，则当将受信任设备被分配给特定用户时，被分配的用户将被忽略，所有用户都可以写入该设备。 | \Everyone（默认）：设备被设置为对所有用户均为受信任设备。<br><user name> 是设备受信任所针对的本地用户或域用户的名称（如果系统允许以此格式输入用户名，则无需指定带域的全名；也可以采用 <域名>\<user name> 或 <user name>@<域名> 格式）。<br>@<group name> 是设备受信任所针对的（本地或域）用户组的名称。 |
| **[Schedules.item_#]** 部分包含访问设备的计划。您只能为硬盘驱动器、可移动驱动器、软盘驱动器和 CD/DVD 驱动器配置计划。 | | |
| ScheduleName | 指定计划名称。<br>计划名称必须是唯一的。 | 默认值：Default。<br>如果允许连接总线访问相应的设备类型，Default 计划使用户在任何时候都能完全访问设备。<br>您不能删除 Default 计划。 |
| DaysHours | 指定计划的时间间隔。 | All（默认值）– 计划全天候有效（没有时间限制）。<br><weekday> – 星期几。您可以使用完整的星期几名称或缩写（例如，对于星期一，您可以指定 Mo、Mon 或 Monday）。对于周中日，您可以指定间隔时间或特定日子。一周从星期日开始。<br><hour> – 小时 [0:24]。对于小时，您仅能指定间隔时间。<br>以下是 schedule_1 示例，该计划在星期日至星期六的凌晨 0 点至上午 11 点、中午 12 点至下午 3 点以及下午 4 点至凌晨 12 点有效。<br>[Schedules.item_0001]<br>ScheduleName=schedule_1<br>DaysHours=Su-Sa:0..11,12..15,16..24<br>以下是 schedule_2 示例，该计划在以下时间段内有效：星期四中午 12 点到下午 2 点，星期五凌晨 2 点到下午 3 点和下午 4 点到凌晨 12 点。<br>[Schedules.item_0002]<br>ScheduleName=schedule_2<br>DaysHours=Th:12..14;Fr:2..15,16..24<br>以下是 schedule_3 示例，该计划每周 7 天 24 小时有效<br>[Schedules.item_0003]<br>ScheduleName=schedule_3<br>DaysHours=All |
| **[HardDrivePrincipals.item_#]** 部分包含硬盘驱动器访问规则。<br>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，可以为用户或用户组指定多个计划。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）– 访问规则适用于所有用户。<br><user name> 是访问规则所适用的本地用户的名称。<br>@<group name> 是访问规则所适用的用户组的名称。 |
| [HardDrivePrincipals.item_#.AccessRules.item_#] 包含访问规则设置。 | | |
| UseRule | 指定规则是启用还是禁用。 | Yes（默认值）– 访问规则已启用。<br>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）– 允许访问硬盘驱动器。<br>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。<br>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，可以为用户或用户组指定多个计划。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）– 访问规则适用于所有用户。<br><user name> 是访问规则所适用的本地用户的名称。<br>@<group name> 是访问规则所适用的用户组的名称。 |
| [RemovableDrivePrincipals.item_#.AccessRules.item_#] 包含访问规则设置。 | | |
| UseRule | 指定规则是启用还是禁用。 | Yes（默认值）– 访问规则已启用。<br>No – 访问规则已禁用。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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）— 允许访问可移动驱动器。<br>Block — 阻止访问可移动驱动器。 |
| **[FloppyDrivePrincipals.item_#]** 部分包含软盘驱动器的访问规则。<br>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，可以为用户或用户组指定多个计划。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）— 访问规则适用于所有用户。<br><user name> 是访问规则所适用的本地用户的名称。<br>@<group name> 是访问规则所适用的用户组的名称。 |
| [FloppyDrivePrincipals.item_#.AccessRules.item_#] 包含访问规则设置。 | | |
| UseRule | 指定规则是启用还是禁用。 | Yes（默认值）– 访问规则已启用。<br>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）– 允许访问软盘驱动器。<br>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。<br>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，可以为用户或用户组指定多个计划。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）— 访问规则适用于所有用户。<br><user name> 是访问规则所适用的本地用户的名称。<br>@<group name> 是访问规则所适用的用户组的名称。 |
| [OpticalDrivePrincipals.item_#.AccessRules.item_#] 包含访问规则设置。 | | |
| UseRule | 指定规则是启用还是禁用。 | Yes（默认值）– 访问规则已启用。<br>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 CD/DVD 驱动器。<br>Block – 阻止访问 CD/DVD 驱动器。 |

# 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

下表介绍了可为 Web 控制任务 (Web_Control) 指定的所有设置的全部可用值和默认值。

| 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。 | Allow（默认值）— 允许访问 Web 资源。<br>Block — 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： | | |
| Name | Web 资源访问规则名称。规则名称必须唯一。 | |
| 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。 | Allow（默认值）— 允许访问 Web 资源。<br>Block — 阻止访问 Web 资源。<br>Notify — 显示一条警告，提示该 Web 资源不受欢迎。通过单击警告消息中的链接，用户可以访问所请求的 Web 资源。 |
| Enabled | Web 资源访问规则的状态。 | Yes — 该规则已启用，Web 控制在操作期间应用此规则。<br>No（默认值）— 该规则已禁用，Web 控制在运行期间不会使用此规则。 |
| 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 资源地址筛选器。<br>No（默认值）— 不使用 Web 资源地址筛选器，将规则应用于所有 Web 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 资源地址。 |
| 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 资源内容筛选器。<br>ContentOnly — 在规则中使用内容类别筛选器。<br>FormatOnly — 在规则中使用数据类型类别筛选器。<br>ContentAndFormat — 在规则中使用内容类别筛选器和数据类型类别筛选器。 |
| [Rules.item_#.ContentCategories.item_#] | 用于指定内容类别的部分。 | – |
| ContentCategory | 内容类别。 | AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weapons, ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepstakes, InternetCommunicationMedia, CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileSharing, AudioAndVideo, BankSites, Blogs, DatingSites, LegislationRF, LegislationGlobal, SexuallyExplicit, Sexuality, AITools |
| [Rules.item_#.FormatCategories.item_#] | 用于指定数据类型类别的部分。 | – |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| FormatCategory | 数据类型类别。 | Video – 视频<br>Audio – 音频数据<br>OfficeDocument – Office 应用程序文件<br>Executable – 可执行文件<br>Archives – 压缩文件<br>Images – 图像文件<br>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器。<br>No （默认值）– 不使用用户筛选器，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。 | |
| Name | Web 资源访问规则涵盖的用户或用户组。 | <username> 是规则适用的用户的名称。<br>@<groupname> 是规则适用的用户组的名称。<br>默认值：网页资源访问规则适用于所有用户。 |
| **[UrlCategories.item_#]** 部分包含以下设置： | | |
| Name | 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 资源地址。 |
| **[Schedules.item_#]** 部分规则计划。 | | |
| Id | [Rules.item_#] 部分中使用的计划 ID。 | 1 – 999999<br>0 是 Default 计划的 ID，可让规则不受任何时间限制地运行，即在任何时候运行。 |
| Name | 指定计划名称。 | |
| DaysHours | 指定计划的时间间隔。 | <weekday> – 星期几。您可以使用完整的星期几名称或缩写（例如，对于星期一，您可以指定 Mo、 Mon 或 Monday）。对于周中日，您可以指定间隔时间或特定日子。一周从星期日开始。<br><hour> – 小时 [0:24]。只能指定小时间隔。 |

## 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 <path to the configuration file>] [--json]
```

其中：

--file <path to the configuration file> 是要将设置输出到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 <path to the configuration file>] [--json]
```

其中：

`--file <path to the configuration file>` 是要从中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
```

# 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 运行的应用程序，则在使用配置文件或使用命令行选项修改任务设置时，请运行以下命令：

```
kesl-control --set-settings --accept
```

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

该表介绍了可为应用程序控制任务 (`Application_Control`) 指定的所有设置的所有可能值和默认值。

“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。<br>`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。<br>`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。<br>`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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |
| 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目录名称。 |
| IncludeHashes.item_# | 触发规则的可执行文件的 SHA256 哈希值。 | 仅可使用 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。<br>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。 |
| 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目录名称。 |
| ExcludeHashes.item_# | 触发规则的可执行文件的 SHA256 哈希值。 | 仅可使用 SHA256。 |
| **[AllowListRules.item_#]** 部分包含 *AllowList* 操作模式的“应用程序控制”规则列表。<br>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。<br>Off — 该规则不用于“应用程序控制”。<br>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。<br>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。<br>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。<br>< 用户名 > 是规则所适用的用户的名称。<br>@< 组名称 > 是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。<br>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。<br>Off — 该规则不用于“应用程序控制”。<br>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。<br>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。<br>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。<br>< 用户名 > 是规则所适用的用户的名称。<br>@< 组名称 > 是规则所适用的用户组的名称。 |

实用文章

## 如何指定掩码

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 /）。

## 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 <path to the configuration file>
```

其中：

`--file <path to the configuration file>` 是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 <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 2>"
   }
]
```

要在 `Exclude` 和 `Include` 字段中指定文件名，您可以使用掩码。

`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 <category name 1> <category name 2> ... <category name N>] --file <path to the configuration file>
```

其中：

- `<category name 1> <category name 2> ... <category name N>` 是您要编辑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 <path to the configuration file>` 是包含类别设置的配置文件的路径。

实用文章

**如何指定掩码**

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 `/`）。

## 查看类别列表

在命令行上，您可以使用应用程序控制管理命令`kesl-control --get-categories`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 <path to the configuration file>] [--json]
```

其中：

- `--file <path to the configuration file>` 是要将设置输出到的配置文件的完整路径。
- 指定 `--json`，则以 JSON 格式输出设置。

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

*要查看单独应用程序类别的列表，请执行以下命令：*

```
kesl-control --get-categories [--names <category name 1> <category name 2> ... <category name N>] [--file <path to the configuration file>] [--json]
```

其中：

- `<category name 1> <category name 2> ... <category name N>` 是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 <path to the configuration file>` – 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 <path to the configuration file>] [--json]
```

其中：

- `--file <path to the configuration file>` 是要将设置输出到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的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。
- 该规则适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。
- 应用程序控制规则适用的用户或用户组。

*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 <path to the configuration file>] [--json]
```

其中：

- `--file <path to the configuration file>` 是要从中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
```

# 配置清查

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：

- 借助清查预定义任务 (`Inventory_Scan`)。您可以手动启动或停止此任务，并配置任务计划。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

该表介绍了可为清查任务（`Inventory_Scan`）指定的所有设置的全部可能值和默认值。

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。<br>`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。<br>`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。<br>`No` – 不使用可执行位扫描文件。 |
| `GoldenImageAction` | 完成清查任务后，Kaspersky Endpoint Security 必须对"黄金镜像"应用程序类别执行的操作：<br>您可以在应用程序控制规则中使用"黄金镜像"类别。 | `DoNothing`（默认）– 完成清查后不更改"黄金镜像"应用程序类别。<br>`Create` – 将检测到的应用程序添加到"黄金镜像"应用程序类别。如果该类别不存在，则创建该类别。如果该类别已存在，则更新该类别的应用程序列表。<br>`Remove` – 清除"黄金镜像"应用程序类别。任务启动后会立即清除此类别，而不会对设备上的文件进行清查。 |
| **[ScanScope.item_#]** 部分包含以下设置： | | |
| `AreaDesc` | 清查范围的描述。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。<br>`No` – 不扫描指定的清查范围。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| AreaMask.item_# | 库存扫描范围限制。在清查扫描范围内，应用程序仅扫描使用 shell 格式的掩码指定的文件。<br>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。<br>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。 | 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。<br>No — 不排除指定的范围。 |
| AreaMask.item_# | 使用 shell 掩码限制清查排除范围。<br>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）。 |
| Path | 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。 |

实用文章

**如何指定掩码**

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）。您可以使用以下命令查看已创建的应用程序类别列表：

```
kesl-control --get-categories
```

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。

## 系统完整性监控任务

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。`OAFIM`：任务类型。

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。

访问时系统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。<br>仅当指定 `ExcludeMasks.item_#` 设置时，此设置才适用。 | `Yes` — 从监控范围中排除 `ExcludeMasks.item_#` 设置指定的对象。<br>`No`（默认值）— 不从监控范围中排除 `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。<br>在为此设置指定值之前，请确保已启用 `UseExcludeMasks` 设置。<br>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。<br>[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。<br>`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。<br>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。<br>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：`*`（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。<br>[ExcludedFromScanScope.item_#] 部分包含以下设置： | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。<br>No – 不将指定范围排除在监控之外。 |
| Path | 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。<br>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。<br>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）。 |

实用文章

**如何指定掩码**

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。

# 系统完整性检查任务

您可以使用自定义系统完整性检查任务（System_Integrity_Monitoring 类型的任务），在命令行中对设备运行系统完整性检查。ODFIM：任务类型。

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。<br>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。<br>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。<br>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 – 跟踪上次文件访问时间。<br>No（默认值）– 不跟踪上次文件访问时间。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseExcludeMasks | 对 ExcludeMasks.item_# 设置指定的对象启用监控范围排除项。<br>仅当指定 ExcludeMasks.item_# 设置时，此设置才适用。 | Yes — 从监控范围中排除 ExcludeMasks.item_# 设置指定的对象。<br>No（默认值）— 不从监控范围中排除 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。<br>在为此设置指定值之前，请确保已启用 UseExcludeMasks 设置。<br>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。<br>[ScanScope.item_#] 部分包含以下设置：<br>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。<br>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。<br>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。<br>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：*（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。<br>[ExcludedFromScanScope.item_#] 部分包含以下设置：<br>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。<br>No — 不将指定范围排除在监控之外。 |
| Path | 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。<br>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。<br>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）。 |

实用文章

### 如何指定掩码

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。

# 防御高级威胁和定向攻击

## Kaspersky Endpoint Detection and Response Expert (on-premises) 集成

您可以在命令行上通过 *Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR)* 预定义任务管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案之间的集成。

此任务还可让您管理 Kaspersky Endpoint Detection and Response (KATA) 集成设置。对于 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，您需要选择 *EDR Expert (on-premises)* 集成模式，并根据需要管理集成设置。

您可以通过编辑预定义任务的设置来管理 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成设置。

*Kaspersky Endpoint Detection and Response Expert (on-premises) 集成*任务默认不运行。您可以手动启动和停止任务。

您可以使用 EDR Expert (on-premises) 组件管理命令管理用于连接到 OSMP 服务器的证书。

### Kaspersky Endpoint Detection and Response Expert (on-premises) 整合设置

下表介绍了 Kaspersky Endpoint Detection and Response Expert (on-premises)（KATAEDR）集成预定义任务的设置，您可以在与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成时管理这些设置。

此任务还可让您管理 Kaspersky Endpoint Detection and Response (KATA) 集成设置。对于 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，您需要在任务设置中选择 *EDR Expert (on-premises)* 集成模式 (`Mode=EDRExpertOnPrem`)。

Kaspersky Endpoint Detection and Response Expert (on-premises) 整合设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `Mode` | 集成模式。<br>对于 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，Kaspersky Endpoint Security 应用程序会与 OSMP 平台上的服务器交互。<br>对于 Kaspersky Endpoint Detection and Response (KATA) 集成，Kaspersky Endpoint Security 应用程序与 Kaspersky Anti Targeted Attack Platform 上的服务器进行交互。 | `EDRKATA`（默认）是 EDR (KATA) 集成模式。允许启用与 Kaspersky Endpoint Detection and Response (KATA) 进行集成，这是 Kaspersky Anti Targeted Attack Platform 的一个组件。<br>`EDRExpertOnPrem` 是 EDR Expert (on-premises) 集成模式。启用 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成 |
| `UseClientPinnedCertificate` | 启用或禁用双向身份验证，以增强与 OSMP 威胁响应操作服务器连接的安全性。<br>如果在 OSMP 威胁响应服务器端启用了双向身份验证，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 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` 启用双向身份验证，以增强与 OSMP 威胁响应操作服务器连接的安全性。<br>`No`（默认值）— 不使用双向身份验证。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| SynchronizationPeriod | 向 OSMP 威胁响应操作服务器发送同步请求的周期（以分钟为单位）。 | 默认值：5。 |
| ConnectionTimeout | 等待连接到 OSMP 威胁响应操作服务器的最长时间（以秒钟为单位）。 | 默认值：10。 |
| RequestTimeout | 等待 OSMP 威胁响应操作服务器响应的最长时间（以秒钟为单位）。 | 默认值：10。 |
| EnableTelemetry | 将设备上的事件数据（遥测）发送到 OSMP 遥测收集服务器。 | Yes（默认值）启用向 OSMP 遥测服务器发送遥测数据。<br>No 禁用传送遥测数据。 |
| **[Endpoints.item_#]** 部分包含 OSMP 威胁响应操作服务器的地址和端口。您可以添加多台服务器。 | | |
| Address | OSMP 威胁响应操作服务器地址。<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>为确保在设备上启用网络隔离的情况下应用程序发生故障时与服务器的通信不会中断，我们建议指定服务器的 IP 地址。 | 默认值：127.0.0.1。 |
| Port | 用于连接到 OSMP 威胁响应服务器的端口。 | 默认值：443。 |
| **[TelemetrySettings]**部分包含用于连接到 OSMP 遥测服务器的常规设置。 | | |
| UseClientPinnedCertificate | 启用或禁用双向身份验证，以增强与 OSMP 遥测服务器连接的安全性。<br>如果在 OSMP 遥测服务器端启用了双向身份验证，您需要在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 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 启用双向身份验证，以增强与 OSMP 遥测服务器连接的安全性。<br>No（默认值）— 不使用双向身份验证。 |
| ConnectionTimeout | 等待连接到 OSMP 遥测服务器的最长时间（以秒钟为单位）。 | 默认值：10。 |
| RequestTimeout | 等待 OSMP 遥测服务器响应的最长时间（以秒钟为单位）。 | 默认值：10。 |
| OnlyTaggedEvents | 仅发送包含 IOA 的遥测。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。 | Yes — 仅发送包含攻击指标 (IOA) 的遥测数据。<br>No（默认值）— 发送所有遥测数据。 |
| **[TelemetrySettings.Endpoints.item_#]**部分包含 OSMP 遥测服务器的地址和端口。您可以添加多台服务器。 | | |
| Address | OSMP 遥测服务器证书地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>为确保在设备上启用网络隔离的情况下应用程序发生故障时与服务器的通信不会中断，我们建议指定服务器的 IP 地址。 | 默认值：127.0.0.1。 |
| Port | 用于连接到 OSMP 遥测服务器的端口。 | 默认值：443。 |
| **[TelemetrySettings.EventTransferSettings]**部分包含用于向 OSMP 遥测服务器传输数据的设置。 | | |
| MaximumDataTransferTime | 向 OSMP 遥测服务器发送事件的最大延迟（以秒钟为单位）。 | 默认值：30。 |
| UseRequestCountLimits | 限制请求数量。该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制传输的事件。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。 | Yes（默认值）– 调节发送的事件数。<br>No – 不调节事件数。 |
| MaximumNumberOfEventsInHour | 每小时的最大事件数量 | 默认值：3000。 |
| MaximumNumberOfEventsInPackage | 一个数据包中的最大事件数量。 | 默认值：1024。 |
| EventLimitExceededPercentage | 事件数量超过限制（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：15。 |

## 管理用于连接到 OSMP EDR Expert (on-premises) 服务器的证书

管理证书需要具有管理员 (admin) 角色的用户权限。

您可以使用命令来管理用于连接到 OSMP 服务器的证书。您可以使用证书执行以下操作：

- 添加或替换 OSMP 服务器（威胁响应服务器和遥测服务器）的证书
- 显示有关服务器证书的信息
- 删除服务器证书
- 添加或替换用于保护与 OSMP 服务器（威胁响应服务器和遥测服务器）连接的客户端证书
- 显示有关客户端证书的信息
- 删除客户端证书

管理与 OSMP 威胁响应服务器连接的证书

*要添加或替换威胁响应操作服务器证书，请运行以下命令：*

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

其中 `<file>` 是包含服务器证书的文件的路径。

*要添加或替换用于威胁响应服务器连接的客户端证书：*

1. 运行以下命令：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
   ```

   其中 `<file>` 是包含客户端证书和私有密钥的加密容器（PFX 存档）的路径。

2. 输入加密容器密码

如果在 OSMP 服务器设置中启用了客户端证书验证，并且在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 集成* 任务设置中，`[KATAEDR]` 部分中的 `UseClientPinnedCertificate` 设置的值为 `yes`，则客户端证书用于为与 OSMP 服务器的连接提供额外保护。

*要显示关于威胁响应操作服务器证书的信息，请运行以下命令：*

```
kesl-control [-R] --query-kataedr-server-certificate --server-type response
```

*要显示关于用于保护与威胁响应操作服务器连接的客户端证书的信息，请运行以下命令：*

```
kesl-control [-R] --query-kataedr-client-certificate --server-type response
```

运行该命令会显示以下证书信息：

- 证书序列号
- 证书主题
- 证书发布者
- 证书开始日期
- 证书到期日期
- SHA1 和 SHA256 证书指纹

*要删除威胁响应操作服务器证书，请运行以下命令：*

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

*要删除用于保护威胁响应操作服务器连接的客户端证书，请运行以下命令：*

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

管理用于连接到 OSMP 遥测服务器的证书

*要添加或替换遥测服务器的证书，请运行以下命令：*

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

其中 `<file>` 是包含服务器证书的文件的路径。

*要添加或替换遥测服务器连接的客户端证书：*

1. 运行以下命令：

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
   ```

   其中 `<file>` 是包含客户端证书和私有密钥的加密容器（PFX 存档）的路径。

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 OSMP 服务器设置中启用了客户端证书验证，并且在 *Kaspersky Endpoint Detection and Response Expert (on-premises) 集成* 任务设置中，`[TelemetrySettings]` 部分中的 `UseClientPinnedCertificate` 设置的值为 `yes`，则客户端证书用于为与 OSMP 服务器的连接提供额外保护。

*要显示关于遥测服务器证书的信息，请运行以下命令：*

```
kesl-control [-R] --query-kataedr-server-certificate --server-type telemetry
```

*要显示关于用于保护遥测服务器连接的客户端证书的信息，请运行以下命令：*

```
kesl-control [-R] --query-kataedr-client-certificate --server-type telemetry
```

运行该命令会显示以下证书信息：

- 证书序列号
- 证书主题
- 证书发布者
- 证书开始日期
- 证书到期日期
- SHA1 和 SHA256 证书指纹

*要删除遥测服务器证书信息，请运行以下命令：*

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

*要删除用于保护遥测服务器连接的客户端证书，请运行以下命令：*

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

## Kaspersky Endpoint Detection and Response Expert (cloud) 集成

您可以在命令行中通过 *Kaspersky Endpoint Detection and Response Expert (cloud) 集成* 预定义任务 管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案之间的集成。

您可以通过编辑预定义任务的设置来管理 Kaspersky Endpoint Detection and Response Expert (cloud) 集成设置。

*Kaspersky Endpoint Detection and Response Expert (cloud) 集成*任务默认不运行。您可以手动启动和停止任务。

# Kaspersky Endpoint Detection and Response Expert (cloud) 集成设置

下表介绍 Kaspersky Endpoint Detection and Response Expert (cloud) 集成预定义任务 (`EDRExpertCloud`) 的设置。

如何获取任务设置的当前值

```
kesl-control --get-settings 39
```

如何配置任务设置

```
kesl-control --set-settings 39 <parameter>=<value>
```

Kaspersky Endpoint Detection and Response Expert (cloud) 集成设置

| 设置 | 描述 |
| --- | --- |
| **响应服务器集成设置** | |
| `UseTunnel` | 使用 TCP 隧道连接到响应服务器。如果您的基础架构中的安全策略不允许您直接连接到服务器，则使用 TCP 隧道连接到服务器。<br>默认情况下，使用 TCP 隧道处于禁用状态 (`No`)。 |
| `TunnelAddress` | 用于连接到隧道的服务器地址（IPv4 或 IPv6）。 |
| `TunnelPort` | 用于连接到隧道的服务器端口。 |
| `SynchronizationPeriod` | 向 OSMP 威胁响应操作服务器发送同步请求的周期（以分钟为单位）。<br>默认值： `5`。 |
| **遥测收集服务器集成设置**<br>`[TelemetrySettings]` 部分包含用于连接到 OSMP 遥测服务器的常规设置。 | |
| `EnableTelemetry` | 将设备上的事件数据（遥测）发送到 OSMP 遥测收集服务器。<br>默认情况下，发送遥测已启用（`Yes`）。 |
| `OnlyTaggedEvents` | 仅发送包含 IOA 的遥测。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。<br>默认情况下，仅发送包含 IOA 的遥测处于禁用状态（`No`）。 |
| `UseTunnel` | 使用 TCP 隧道连接到遥测数据收集服务器。如果您的基础架构中的安全策略不允许您直接连接到服务器，则使用 TCP 隧道连接到服务器。<br>默认情况下，使用 TCP 隧道处于禁用状态 (`No`)。 |
| `TunnelAddress` | 用于连接到隧道的服务器地址（IPv4 或 IPv6）。 |
| `TunnelPort` | 用于连接到隧道的服务器端口。 |
| `[TelemetrySettings.EventTransferSettings]` 部分包含用于连接到 OSMP 遥测服务器的常规设置。 | |
| `UseRequestCountLimits` | 限制请求数量。该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制传输的事件。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。<br>默认情况下已禁用该选项。 |
| `MaximumDataTransferTime` | 发送事件时的最大延迟。应用程序在同步间隔到期后与服务器同步以发送事件。默认设置是 30 秒。 |
| `MaximumNumberOfEventsInHour` | 每小时最大事件数 应用程序会分析遥测数据流，并在事件流超过配置的每小时事件数限制时限制事件的发送。Kaspersky Endpoint Security 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。 |
| `MaximumNumberOfEventsInPackage` | 数据包中的最大事件数量。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。 |
| `EventLimitExceededPercentage` | 事件限制阈值（百分比）。该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Endpoint Security 将恢复发送事件。默认设置为 15%。 |

# 管理 OSMP EDR Expert 服务器（云）连接证书

管理证书需要具有管理员 (admin) 角色的用户权限。

接受 Kaspersky Endpoint Detection and Response Expert (cloud) 数据处理协议的条款和条件后，应用程序会自动接收用于建立可信连接的服务器地址和证书。因此，您无法使用命令添加或删除证书。您只能在命令行显示证书信息。

管理与 OSMP 威胁响应服务器连接的证书

要显示有关威胁响应服务器证书的信息

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type response
```

要显示有关威胁响应服务器连接的客户端证书的信息

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type response
```

运行该命令会显示以下证书信息：

- 证书序列号
- 证书主题
- 证书发布者
- 证书开始日期
- 证书到期日期
- SHA1 和 SHA256 证书指纹

管理用于连接到 OSMP 遥测服务器的证书

显示有关遥测收集服务器证书的信息

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type telemetry
```

要显示有关遥测服务器连接的客户端证书的信息

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type telemetry
```

运行该命令会显示以下证书信息：

- 证书序列号
- 证书主题
- 证书发布者
- 证书开始日期

- 证书到期日期
- SHA1 和 SHA256 证书指纹

# Kaspersky Endpoint Detection and Response (KATA) 整合

您可以在命令行中通过 *Kaspersky Endpoint Detection and Response Expert (on-premises) 整合 (KATAEDR)* 预定义任务管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 组件之间的整合。

此任务还允许您管理 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成设置。要与 Kaspersky Endpoint Detection and Response (KATA) 整合，您需要在任务设置中选择 EDR (KATA) 整合模式，并根据需要管理整合设置。

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。

*Kaspersky Endpoint Detection and Response Expert (on-premises) 集成*任务默认不运行。您可以手动启动和停止任务。

您可以使用 EDR Expert (on-premises) 组件管理命令管理用于连接到 KATA 服务器的证书。

## Kaspersky Endpoint Detection and Response (KATA) 集成设置

下表介绍了 Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR) 整合预定义任务的设置，您可以在与 Kaspersky Endpoint Detection and Response (KATA) 整合时管理这些设置。

此任务还允许您管理 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成设置。要与 Kaspersky Endpoint Detection and Response (KATA) 集成，您需要在任务设置中选择*EDR (KATA)* 集成模式 (`Mode=EDRKATA`)。

Kaspersky Endpoint Detection and Response (KATA) 集成设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `Mode` | 集成模式。<br>对于 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成，Kaspersky Endpoint Security 应用程序会与 OSMP 平台上的服务器交互。<br>对于 Kaspersky Endpoint Detection and Response (KATA) 集成，Kaspersky Endpoint Security 应用程序与 Kaspersky Anti Targeted Attack Platform 上的服务器进行交互。 | `EDRKATA`（默认）是 EDR (KATA) 集成模式。允许启用与 Kaspersky Endpoint Detection and Response (KATA) 进行集成，这是 Kaspersky Anti Targeted Attack Platform 的一个组件。<br>`EDRExpertOnPrem` 是 EDR Expert (on-premises) 集成模式。启用 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成 |
| `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。<br>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 Expert (on-premises) 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` – 使用双向身份验证来进一步保护与 KATA 服务器的连接。<br>`No`（默认值）– 不使用双向身份验证。 |
| `SynchronizationPeriod` | 发送同步请求到 KATA 服务器的间隔（以分钟为单位）。 | 默认值：`5`。 |
| `ConnectionTimeout` | 等待与 KATA 服务器连接的最长时间（以秒为单位）。 | 默认值：`10`。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `RequestTimeout` | 等待 KATA 服务器响应的最长时间（以秒为单位）。 | 默认值：`10`。 |
| `EnableTelemetry` | 向 KATA 发送事件数据（遥测）。 | `Yes`（默认值）– 向 KATA 服务器发送遥测数据。<br>`No` 禁用传送遥测数据。 |
| **[Endpoints.item_#]** 部分包含 KATA 服务器的地址和端口。您可以添加多台服务器。 | | |
| `Address` | KATA 服务器地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>为确保在设备上启用网络隔离的情况下应用程序发生故障时与服务器的通信不会中断，我们建议指定服务器的 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：`443`。 |
| **[EventTransferSettings]** 部分包含将数据发送到 KATA 服务器的设置。 | | |
| `MaximumDataTransferTime` | 向 KATA 服务器发送事件的最大延迟（以秒为单位）。 | 默认值：`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。<br>`No` – 不调节事件数。 |
| `MaximumNumberOfEventsInHour` | 每小时的最大事件数量 | 默认值：`3000`。 |
| `MaximumNumberOfEventsInPackage` | 一个数据包中的最大事件数量。 | 默认值：`1024`。 |
| `EventLimitExceededPercentage` | 事件数量超过限制（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：`15`。 |

## 管理用于连接到 Expert 服务器的证书

管理证书需要具有管理员 (admin) 角色的用户权限。

您可以使用命令管理用于连接到 KATA 服务器的证书。您可以使用证书执行以下操作：

- 添加或替换 KATA 服务器证书
- 显示有关服务器证书的信息
- 删除服务器证书
- 删除或替换用于保护与 KATA 服务器连接的客户端证书
- 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 <file>
```

其中 `<file>` 是包含服务器证书的文件的路径。

*要添加或更改客户端证书：*

1. 运行以下命令：

```
kesl-control [-R] --add-kataedr-client-certificate <file>
```

其中 `<file>` 是包含客户端证书和私有密钥的加密容器（PFX 存档）的路径。

2. 输入加密容器密码

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 Expert (on-premises) 集成任务设置*中，`UseClientPinnedCertificate` 设置为 `yes`，则客户端证书用于为与 KATA 服务器的连接提供额外保护。

*要显示服务器证书信息，请运行以下命令：*

```
kesl-control [-R] --query-kataedr-server-certificate
```

*要显示客户端证书信息，请运行以下命令：*

```
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
- 证书发布者
- 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
```

# Kaspersky Network Detection and Response (KATA) 整合

您可以在命令行中通过 *Kaspersky Network Detection and Response (KATA) 整合*（`KATANDR`）预定义任务管理 Kaspersky Network Security 与 Kaspersky Endpoint Detection and Response (KATA) 之间的集成：

*Kaspersky Network Detection and Response (KATA) 集成*默认不运行。您可以手动启动和停止任务。

您可以通过编辑预定义任务的设置来配置Kaspersky Network Detection and Response (KATA) 集成设置。

您可以使用NDR (KATA) 组件管理命令来管理用于连接到 NDR 服务器的证书。

## Kaspersky Network Detection and Response (KATA) 集成设置

该表介绍了可为 Kaspersky Network Detection and Response (KATA) 整合任务 (`KATANDR`) 指定的所有可用设置及其默认值。

Kaspersky Network Detection and Response (KATA) 整合任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| `UseClientPinnedCertificate` | 启用和禁用双向身份验证，以进一步保护与 NDR 服务器的连接。<br>如果在 NDR 服务器端启用了客户端证书验证，请在启动 *Kaspersky Network Detection and Response (KATA) 整合*任务之前启用客户端证书的使用并添加客户端证书。 | `Yes` – 使用双向身份验证来进一步保护与 NDR 服务器的连接。<br>`No`（默认值）– 不使用双向身份验证。 |
| `SynchronizationPeriod` | 发送同步请求到 NDR 服务器的间隔（以分钟为单位）。 | 默认值：`5`。 |
| `ConnectionTimeout` | 等待与 NDR 服务器连接的最长时间（以秒为单位）。 | 默认值：`10`。 |
| `RequestTimeout` | 等待 NDR 服务器响应的最长时间（以秒为单位）。 | 默认值：`10`。 |
| **[Endpoints.item_#]** 部分包含 NDR 服务器的地址和端口。 | | |
| `Address` | NDR 服务器地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。 | 默认值：`127.0.0.1`。 |
| `Port` | 用于连接到 NDR 服务器的端口。 | 默认值：`8081`。 |
| **[EventTransferSettings]** 部分包含将事件发送到 NDR 服务器的设置。 | | |
| `MaximumDataTransferTime` | 向 NDR 服务器发送事件的最大延迟（以秒为单位）。 | 默认值：`30`。 |
| `MaximumNumberOfEventsInPackage` | 一个数据包中的最大事件数量。 | 默认值：`1024`。 |
| `UseRequestCountLimits` | 启用和禁用调节发送到 NDR 服务器的事件数。 | `Yes`（默认值）– 调节发送的事件数。<br>`No` – 不调节事件数。 |
| `MaximumNumberOfEventsInHour` | 每小时的最大事件数量 | 默认值：`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：`15`。 |
| `PingPeriod` | NDR 服务器轮询周期（秒）。 | 默认值：`450`。 |

## 管理用于连接到 NDR 服务器的证书

管理证书需要具有管理员 (admin) 角色的用户权限。

您可以使用命令管理用于连接到 NDR 服务器的证书。您可以使用证书执行以下操作：

- 添加或替换 NDR 服务器证书
- 显示有关服务器证书的信息
- 删除服务器证书
- 删除或替换用于保护与 NDR 服务器连接的客户端证书
- 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-katandr-server-certificate <file>
```

其中 `<file>` 是包含服务器证书的文件的路径。

*要添加或更改客户端证书：*

1. 运行以下命令：

   ```
   kesl-control [-R] --add-katandr-client-certificate <file>
   ```

   其中 `<file>` 是包含客户端证书和私有密钥的加密容器（PFX 存档）的路径。

2. 输入加密容器密码

如果在 NDR 服务器设置中启用了客户端证书验证，并且在 *Kaspersky Network Detection and Response (KATA) 集成* 任务设置中，`UseClientPinnedCertificate` 设置设为 `yes`，则客户端证书用于额外保护与 NDR 服务器的连接。

*要显示服务器证书信息，请运行以下命令：*

```
kesl-control [-R] --query-katandr-server-certificate
```

*要显示客户端证书信息，请运行以下命令：*

```
kesl-control [-R] --query-katandr-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
- 证书发布者

- 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-katandr-server-certificate
```

*要删除客户端证书信息，请运行以下命令：*

```
kesl-control [-R] --remove-katandr-client-certificate
```

## Sandbox 集成

在命令行上，您可以使用*Sandbox 集成*预定义任务管理 Kaspersky Endpoint Security 应用程序与 Sandbox 组件的集成。

默认情况下，*Sandbox 集成*任务未运行。您可以手动启动和停止该任务。

*要启动 Sandbox 集成 任务，请执行以下命令：*

```
kesl-control --start-task 29
```

如果尚未添加服务器证书，则无法启动*与 Sandbox 集成*任务。

如果 *Sandbox 集成* 任务已启动，并且所选模式允许手动发送文件进行扫描（`Manual` 或 `AutoAndManual`），则可以通过命令行将文件发送到沙盒进行扫描。

如何将文件发送到沙盒进行扫描

```
kesl-control [-X] --sandbox <path>
```

其中 `<path>` 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。

您可以通过编辑预定义任务的设置来管理 Sandbox 集成设置。

通过使用用于管理 Sandbox 集成设置的命令，您可以管理证书，该证书用于连接到负责与 Sandbox 服务器交互的服务器。

### Sandbox 集成设置

下表介绍了可为 Sandbox 整合任务 (`Standalone_Sandbox`) 指定的所有可用设置及其默认值。

如何配置 Sandbox 集成设置

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port> [<setting name>=
```

```
<setting value>]
```

Sandbox 集成任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| UseClientCertificate | 启用和禁用双向身份验证，以进一步保护与 Sandbox 服务器的连接。<br>如果在 Sandbox 服务器端启用了客户端证书验证，请在启动 *Sandbox 集成*任务之前启用客户端证书的使用并添加客户端证书。 | Yes — 使用双向身份验证来进一步保护与 Sandbox 服务器的连接。<br>No （默认值）— 不使用双向身份验证。 |
| ConnectionTimeout | 等待与服务器连接的最长时间（以秒为单位）。 | 默认值：10。 |
| RequestTimeout | 等待服务器响应的最长时间（以秒为单位）。 | 默认值：10。 |
| SendingMode | 将对象发送到 Sandbox 进行扫描的模式 | AutoOnly （默认值）– 当尝试访问文件时，自动发送文件进行扫描。<br>Manual – 手动发送文件进行扫描。<br>AutoAndManual – 自动和手动发送文件进行扫描。 |
| QuarantineFile | 当检测到威胁时，将文件进行隔离。 | Yes （默认值）– 如果检测到威胁，则删除原始文件，并将文件副本放入隔离区。<br>No – 检测到威胁时，不将文件进行隔离。 |
| ScanCriticalAreas | 检测到威胁时，执行关键区域扫描。 | Yes （默认值）– 检测到威胁时启动关键区域扫描。<br>No – 检测到威胁时不启动关键区域扫描。 |
| CreateIocScanTask | 检测到威胁时创建IOC 扫描任务。 | Yes （默认值）– 检测到威胁时创建 IOC 扫描任务。<br>No – 检测到威胁时不创建 IOC 扫描任务。 |
| QuarantineFileOnIocDetected | 检测到入侵指标时隔离对象。 | Yes （默认值）– 如果检测到入侵指标，则删除原始对象，并将对象副本放入隔离区。<br>No — 检测到入侵指标时不隔离对象。 |
| ScanCriticalAreasOnIocDetected | 检测到入侵指标时，执行关键区域扫描。 | Yes （默认值）– 检测到入侵指标时启动关键区域扫描。<br>No – 检测到入侵指标时不启动关键区域扫描。 |
| Drives | IoC 扫描范围。 | Critical （默认）— 扫描用户和系统目录中的文件。<br>System — 扫描根文件系统中的所有文件。 |
| ScheduleMode | IOC 扫描任务启动模式。 | Manually （默认）– 手动启动 IOC 扫描任务。<br>AfterTreatDetected – 检测到威胁后启动 IOC 扫描任务。 |
| **[Servers.item_#]** 部分包含 Sandbox 服务器的设置。 | | |
| Address | 服务器的地址。<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。 | 默认值：127.0.0.1。 |
| Port | 用于连接到服务器的端口。 | 默认值：443。 |
| **[SandboxTransferSettings]** 部分包含发送文件以在 Sandbox 中进行扫描的设置。 | | |
| SandboxQueue | 扫描请求队列的最大大小（以 MB 为单位）。 | 默认值：1024。 |

## 管理用于连接到 Sandbox 服务器的证书

管理证书需要具有管理员 (admin) 角色的用户权限。

您可以使用命令管理用于连接到 OSMP 服务器或负责与沙盒交互的 Central Node 服务器（以下简称"沙盒服务器"）的证书。您可以使用证书执行以下操作：

- 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 [-X] --add-sandbox-server-certificate <file>
```

其中 `<file>` 是包含服务器证书的文件的路径。

*要添加或更改客户端证书：*

1. 运行以下命令：

   ```
   kesl-control [-X] --add-sandbox-client-certificate <file>
   ```

   其中 `<file>` 是包含客户端证书和私有密钥的加密容器（PFX 存档）的路径。

2. 输入加密容器密码

如果在沙盒服务器设置中启用了客户端证书验证，并且在 *Sandbox 集成* 任务的 设置 中将 `UseClientCertificate` 设置为 `yes`，则客户端证书用于为与沙盒服务器的连接提供额外保护。

*要显示证书信息，请运行以下命令：*

- 对于服务器证书：

  ```
  kesl-control [-X] --query-sandbox-server-certificate
  ```

- 对于客户端证书：

  ```
  kesl-control [-X] --query-sandbox-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

- 证书发布者
- 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 [-X] --remove-sandbox-server-certificate
```

*要删除客户端证书信息，请运行以下命令：*

```
kesl-control [-X] --remove-sandbox-client-certificate
```

## 启用或禁用 Kaspersky Endpoint Detection and Response Optimum 整合

您可以使用常规应用程序设置中的“`UseEdrOptimum`”设置来启用或禁用 EDR Optimum 组件。

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该设置的值。

*要使用命令行选项启用 EDR Optimum 组件：*

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

*要使用命令行选项禁用 EDR Optimum 组件：*

```
kesl-control --set-app-settings UseEdrOptimum=No
```

## 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 MDR 组件。
- 上传或删除包含 Kaspersky Managed Detection and Response 授权许可信息的 MDR BLOB 文件。

  如果使用授权许可密钥激活了 MDR 组件，则无需上传 MDR BLOB 文件。

建议在管理控制台或 Web Console 中配置 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 之间的整合。

您可以通过编辑常规应用程序设置中的 UseMDR 选项来启用或禁用 MDR 组件。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该设置的值。

UseMDR 参数可以采用以下值：

- "Yes"表示启用 MDR 组件。
- "No"表示禁用 MDR 组件。

如果启用 MDR 组件，并且卡巴斯基安全网络被禁用或在基本模式下使用，则会显示错误消息并且不会启用 MDR 组件。要启用 MDR 组件，您必须在扩展模式下启用 KSN。

您可以使用授权许可密钥管理命令来上传或删除 MDR BLOB 文件。您可以在 MDR 配置文件（ZIP 压缩文件格式）中找到 BLOB 文件。

要上传 BLOB 文件，请执行以下命令：

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

要删除 BLOB 文件，请执行以下命令：

```
kesl-control --remove-mdr-blob
```

启用整合会创建每天运行一次的"Mdr_Autostart_Scan"服务任务。

## 管理设备网络隔离

与 Detection and Response 解决方案集成时，在命令行上，您可以：

- 检查设备的网络隔离状态并查看网络隔离排除项列表。
- 禁用设备的网络隔离。

*要禁用设备的网络隔离，请运行以下命令：*

```
kesl-control [-R] --isolation-off
```

*要检查网络隔离状态并查看网络隔离排除项列表，请运行以下命令：*

```
kesl-control [-R] --isolation-stat
```

显示以下网络隔离状态中的一种：

- *网络隔离已启用。*
- *网络隔离已禁用。*

# 管理隔离区设置

在命令行中，您可以使用常规应用程序设置中的`QuarantineSizeLimit`、`QuarantineFillingNotification`和`QuarantineBackupFolder`设置来配置隔离区。

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。

隔离设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `QuarantineFillingNotification` | 隔离区百分比，百分比必须达到 100% 才会生成隔离区已满的事件。<br>要禁用生成有关已满隔离区的事件，请输入 0。 | 0 至 100<br>0 – 禁用生成有关已满隔离区的事件。<br>默认值：90。 |
| `QuarantineSizeLimit` | 隔离区的最大大小（以兆字节为单位）。当达到最大隔离区大小时，应用程序会删除掉最旧的文件。<br>要使隔离区的大小不受限制，请输入 0。 | 0 至 4000<br>0 表示隔离区大小不受限制。<br>如果应用程序在标准模式或 EDR Agent 模式下使用，则默认值为 200；如果应用程序在 Light Agent 模式下使用，则默认值为 100。 |
| `QuarantineBackupFolder` | 存储备份和隔离对象的目录的路径。您可以指定一个与默认目录不同的目录。您可以使用任何设备上的目录作为存储备份和隔离对象的目录。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。<br>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/<br>访问默认目录需要 root 特权。 |

# 通过命令行管理隔离文件

与 Detection and Response 解决方案集成时，您可以在命令行上使用隔离区管理命令来执行以下操作：

- 将文件放入隔离区（仅当与Kaspersky Endpoint Detection and Response Optimum或Kaspersky Managed Detection and Response集成时）。
- 查看有关隔离文件的信息。
- 从隔离区中删除所有文件或指定的文件。
- 从隔离区恢复文件。

恢复受感染的文件可能会导致设备感染。

隔离文件

*要隔离文件，请运行以下命令：*

```
kesl-control [-Q] --put <path to the file> [--md5] [--sha256] [--save-original-file]
```

其中：

- `<path to the file>` 是要隔离的文件的路径。
- `--md5` 是您要隔离的文件的 MD5 哈希值。
- `--sha256` 是您要隔离的文件的 SHA256 哈希值。
- `--save-original-file` 保留原始文件。如果不指定此选项，则原始文件将被删除。

> 仅当用户账户具有删除对象的权限时，才会删除原始文件。如果权限不足，则会显示文件删除错误信息。

> 仅当与Kaspersky Endpoint Detection and Response Optimum或Kaspersky Managed Detection and Response集成时，您才可以使用此命令。

查看有关隔离文件的信息

*要查看有关隔离文件的信息，请运行以下命令：*

```
kesl-control -Q --query ["<filter conditions>"] [-n <number of files>] [--json]
```

其中：

- `<filter conditions>` 指定一个或多个逻辑表达式，采用 `< 字段 > < 比较运算 > '< 值 >'` 格式，并使用 `and` 逻辑运算符组合，用于限制查询结果。如果您不指定任何筛选条件，应用程序将显示隔离文件的详细信息。
- `<number of files>` 是要显示的最近隔离文件的数量。如果您不指定 `-n`选项，则会显示最后 30 个文件。指定 0 则显示所有文件。
- `--json`：以 JSON 格式输出数据。

`ObjectId` 行显示应用程序在隔离对象时分配给该对象的数字标识符。此 ID 用于对文件执行操作，例如还原文件或将其从隔离区中删除。

从隔离区恢复文件

*要将文件以原始名称从隔离区恢复到其原始位置，请执行以下命令：*

```
kesl-control -Q --restore <object identifier>
```

其中 `<object identifier>` 是应用程序在隔离文件时分配给文件的数字 ID。

*要将文件以新名称从隔离区恢复到指定目录，请执行以下命令：*

```
kesl-control -Q --restore <object identifier> --file <path to the file>
```

其中 --file <path to the file> 是文件的新名称以及要保存文件的目录的路径。

仅当您的用户拥有 root 权限时，您才可以将文件从隔离区恢复到其他目录。如果您的用户权限不足，则只能将文件恢复到其原始位置。

在 Astra Linux 设备上的封闭软件环境模式下，您只能使用将文件放入备份区时所用的同一帐户来恢复文件。恢复文件时，应用程序会创建一个 MAC 标签为 3（cnnr 标志）的目录。

从隔离区中删除文件

*要从隔离区中删除选定的文件，请运行以下命令：*

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

其中 <filter conditions> 指定一个或多个逻辑表达式，采用 <field><comparison operation>'<value>' 格式，并使用 "and" 逻辑运算符组合，用于限制查询结果。

删除名称或路径中包含“test”的文件的示例

```
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

*要从隔离区中删除所有文件，请运行以下命令：*

```
kesl-control -Q --mass-remove
```

# 搜索入侵指标

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以在命令行上通过使用 IOC 扫描任务来扫描入侵指标。当与 Kaspersky Endpoint Detection and Response (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，IOC 扫描将在相应的 Detection and Response 解决方案端执行。

*要从命令行创建、配置和运行IOC 扫描任务，请运行以下命令：*

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

其中：

- `--path <path to the directory or file>` 是用于执行扫描的 IOC 文件的路径，或包含扩展名为 .IOC 或 .XML 的 IOC 文件的目录。

  > 您可以指定多个路径，用空格分隔。您还可以指定两种类型的路径（文件路径和目录路径）。

- `--process` — 启用对设备上运行的进程的分析。

  可能的参数：

  - `on` — 启用对设备上运行的进程的分析（默认值）。
  - `off` — 禁用对设备上运行的进程的分析。

  如果不指定 `--process` 选项，则仅当使用的IOC 文件指定了这些进程的详细信息（`ProcessItem`）时，应用程序才会分析进程。

- `--hint <regular expression>` 是与要分析的文件 (`FileItem`) 或进程的可执行文件 (`ProcessItem`) 的完整路径匹配的正则表达式。

  您可以使用以下正则表达式元素：

  - 元字符： `. ^ $ |`
  - 字符类：数字、字母、小写、大写、cntrl
  - 量词： `* + ? {n} {n,} {n, m}`
  - 否定：`'[^a-c]'`
  - 转义字符： `\a \e \f, \n \r \t \v \b`

- `--arpentry` — 启用 ARP 表 (`ArpEntryItem`) 中的条目分析。

  可能的参数：

  - `on` — 启用 ARP 表中条目的分析（默认值）。
  - `off` — 禁用 ARP 表中条目的分析。

  如果不指定 `--arpentry` 选项，则仅当使用的 IOC 文件指定了 ARP 表（`ArpEntryItem`）的详细信息时，应用程序才会分析 ARP 表。

  `--ports` — 启用对连接开放的端口的分析。

  可能的参数：

  - `on` — 启用对连接开放的端口的分析并扫描设备上的活动连接（默认值）。
  - `off` — 禁用对连接开放的端口的分析并且不扫描设备上的活动连接。

  如果不指定 `--ports` 选项，则仅当使用的IOC 文件指定了这些端口的详细信息（`PortItem`）时，应用程序才会分析端口。

- `--system` — 启用系统环境分析。

可能的参数：

- `on` — 启用系统环境分析（默认值）。
- `off` — 禁用系统环境分析。

如果不指定 `--system` 选项，则仅当使用的IOC 文件指定了系统环境（`SystemInfoItem`）的详细信息时，应用程序才会分析系统环境。

- `--files` — 启用文件分析。

  可能的参数：

  - `on` — 启用文件分析（默认值）。
  - `off` — 禁用文件分析。

  如果不指定 `--files` 选项，则仅当使用的 IOC 文件指定了这些文件的详细信息(`FileItem`)时，应用程序才会分析文件。

- `--drives` — 要扫描的区域。

  可能的参数：

  - `all` — 检查所有可用的文件区域。
  - `system` — 扫描根文件系统中的所有文件。
  - `critical` — 扫描用户和系统目录中的文件（默认值）。
  - `custom` — 仅扫描您指定的区域中的文件。

  如果您未指定 `--drives` 选项，应用程序将分析用户和系统目录中的文件。

- `--excludes <list of exclusions>` 是排除在扫描范围之外的路径列表。

  此选项指定的排除项为全局选项，无论范围类型或目录列表如何均有效。这些排除项优先于其他命令行选项，包括`--hint` 和`--scope`。

  > 排除项被指定为路径，但不能包含递归元素或通配符（例如 *）。

  如果不指定 `--excludes` 选项，则执行扫描时不进行排除。

  您可以指定多个排除项，用空格分隔。

- `--scope <list of directories>` 是要扫描的其他目录列表。

  > 如果您为 `custom` 选项指定了 `--drives` 参数，则需要此选项。

- `--action` — 当检测到入侵指标时执行的操作。

可能的参数：

- `Skip` — 应用程序不会对检测到的对象执行任何操作，但有关它的信息将保存在任务执行结果中（默认值）。
- `QuarantineFile` — 应用程序将隔离检测到的对象。
- `IsolateHost` — 应用程序对在其上检测到对象的设备实施网络隔离。
- `ScanCriticalAreas` – 应用程序将执行关键区域扫描。

  **Kaspersky Endpoint Security 扫描的关键区域**

  - /lib/systemd
  - /lib/udev
  - /lib/dbus-1.0
  - /usr/local/lib/systemd/user
  - /usr/share/dbus-1
  - /usr/share/gdm/autostart
  - /usr/share/gnome/autostart
  - /var/spool/at
  - /var/spool/at/spool
  - /var/spool/anacron
  - /var/spool/cron
  - /boot
  - /bin
  - /sbin
  - /lib
  - /lib32
  - /lib64
  - /libx32
  - /usr/lib
  - /usr/lib32
  - /usr/lib64
  - /usr/libx32

- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

您可以指定多个操作，用逗号分隔。

如果指定 `Skip` 参数，请不要添加任何其他参数。`Skip` 参数只能单独使用。

## 管理执行防护

执行防护允许管理可执行文件和脚本的运行，以及打开 office 格式的文件。执行防护使用执行防护规则管理用户对文件的访问。

对象的执行防护包括以下任务：

- *对象的执行防护 (EDR Expert (on-premises))*(`KATAEDR_Prevention`)
- *对象的执行防护 (EDR Expert (cloud))*(`EDRExpertCloud_Prevention`)
- *对象的执行防护 (EDR Optimum)*(`EDRO_Prevention`)

默认情况下，*对象的执行防护*任务不会启动。如果您至少添加了一个 执行防护规则，应用程序将启动该任务。

*要查看执行防护规则列表，请运行以下命令：*

```
kesl-control [-T] --get-prevention-state [--kata|cxdr|edro]
```

其中：

`--kata`：EDR Expert (on-premises) 组件的执行防护规则列表
`--cxdr`：EDR Expert (cloud) 组件的执行防护规则列表
`--edro`：EDR Optimum 组件的执行防护规则列表

## 配置 KUMA 整合

在命令行上，您可以使用预定义任务管理 Kaspersky Endpoint Security 与 Kaspersky Unified Monitoring and Analysis Platform 的整合：*Kaspersky Unified Monitoring and Analysis Platform 整合*。

默认情况下，*Kaspersky Unified Monitoring and Analysis Platform 整合*任务未运行。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 Unified Monitoring and Analysis Platform 整合设置。

通过使用用于管理 Kaspersky Unified Monitoring and Analysis Platform 整合设置的命令，您可以管理用于连接到 KUMA 服务器的证书。

## Kaspersky Unified Monitoring and Analysis Platform 整合任务

该表介绍了可为 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 整合任务指定的所有可用设置及其默认值。

Kaspersky Unified Monitoring and Analysis Platform 整合任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| UseTls | 启用或禁用服务器证书验证，以对与 KUMA 服务器的连接提供额外保护。 | Yes — 使用证书来进一步保护与 KUMA 服务器的连接。<br>No（默认）— 不使用证书来保护与 KUMA 服务器的连接。 |
| UseClientCertificate | 启用和禁用双向身份验证，以进一步保护与 KUMA 服务器的连接。<br>如果在 KUMA 服务器端启用了客户端证书验证，请在启动 Kaspersky Unified Monitoring and Analysis Platform 整合任务之前启用客户端证书的使用并添加客户端证书。 | Yes – 使用双向身份验证来进一步保护与 KUMA 服务器的连接。<br>No（默认值）— 不使用双向身份验证。 |
| ConnectionTimeout | 等待与 KUMA 服务器连接的最长时间（以秒为单位）。 | 默认值：5。 |
| **[Servers.item_#]** 部分包含 KUMA 服务器的设置。 | | |
| ServerAddress | KUMA 服务器地址<br>可以指定 Integration Server 的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。<br>如果设置 UseTls=Yes，则必须从购买授权许可时收到的证书中指定服务器的完全限定域名 (FQDN) 才能使用 KUMA。 | 默认值：127.0.0.1。 |
| ServerPort | 用于连接到 KUMA 服务器的端口。 | 默认值：443。 |
| ServerProtocol | 用于连接到 KUMA 服务器的端口。 | tcp（默认值）— 使用 TCP 协议连接到 KUMA 服务器。<br>HTTPWithCompression — 使用带事件压缩的 HTTP 协议连接到 KUMA 服务器。<br>udp — 使用 UDP 协议连接到 KUMA 服务器。<br>当选择 UDP 协议时，不支持使用证书提供连接保护（UseTls、UseClientCertificate 和 ConnectionTimeout 设置的值将被忽略），并且不会生成有关与 KUMA 服务器连接的事件。 |
| **[KumaTransferSettings]** 部分包含向 KUMA 服务器发送事件的设置。 | | |
| EventTransferTimeMax | 向 KUMA 服务器发送事件的最大延迟（以秒为单位）。 | 默认值：30。 |

## 管理用于连接到 KUMA 服务器的证书

选择 UDP 协议时，不支持使用证书提供连接保护。

管理证书需要具有管理员 (admin) 角色的用户权限。

您可以使用命令管理用于连接到 KUMA 服务器的证书。您可以使用证书执行以下操作：

- 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 [-M] --add-kuma-server-certificate <path to the file>
```

其中 `<path to the file>` 是包含 DER 或 PEM 格式服务器证书的文件路径。

*要添加或更改客户端证书：*

1. 运行以下命令：

   ```
   kesl-control [-M] --add-kuma-client-certificate <path to the file>
   ```

   其中 `<path to the file>` 是包含客户端证书和私有密钥的加密容器（PFX 存档）的路径。

2. 输入加密容器密码

如果在 KUMA 服务器设置中启用了客户端证书验证，并且在*Kaspersky Unified Monitoring and Analysis Platform 集成任务设置*中，`UseClientCertificate` 设置被设为`yes`，则客户端证书用于对与 KUMA 服务器的连接进行额外保护。

*要显示证书信息，请运行以下命令：*

- 对于服务器证书：

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- 对于客户端证书：

  ```
  kesl-control [-M] --query-kuma-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
- 证书发布者
- 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 [-M] --remove-kuma-server-certificate
```

*要删除客户端证书信息，请运行以下命令：*

```
kesl-control [-M] --remove-kuma-client-certificate
```

# 常规设置

在管理控制台中，您可以在策略属性（**常规设置**）中管理用于定义应用程序整体运行以及各项功能运行的常规应用程序设置。

## 常规应用程序设置

下表介绍用于控制整个应用程序运行以及各个功能运行的常规应用程序设置。

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。<br>更改此设置后，必须重新启动应用程序。 | 默认情况下，将在计算机上指定 SAMBA 配置文件的录。<br>默认值：/etc/samba/smb.conf。 |
| 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。<br>更改此设置后，必须重新启动应用程序。 | 默认情况下，将在计算机上指定 NFS 配置文件的标<br>默认值：/etc/exports。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| TraceFolder | 存储应用程序跟踪文件的目录。<br>更改此设置后，必须重新启动应用程序。 | 默认值：/var/log/kaspersky/kesl。<br>需要 root 特权才能访问默认跟踪文件目录。如果您目录，请确保只有 root 用户具有此目录的读写权限 rwx-------- 权限）。 |
| TraceLevel | 启用应用程序跟踪和跟踪文件的细节级别。<br>此设置仅启用应用程序跟踪文件的生成。要为图形界面和 kesl-control 命令行实用程序生成跟踪文件，您需要设置 LFS_ENABLE_ALL_COMPONENTS_LOGGING 环境变量。 | Detailed – 生成详细的应用程序跟踪文件。<br>MediumDetailed – 生成包含信息消息和错误消息跟踪文件。<br>NotDetailed – 生成包含错误消息的应用程序跟踪<br>None （默认值）– 不生成应用程序跟踪文件。 |
| TraceMaxFileCount | 应用程序跟踪文件的最大数量。<br>更改此设置后，必须重新启动应用程序。 | 1–10000<br>默认值：10。 |
| TraceMaxFileSize | 指定应用程序跟踪文件的最大大小（以兆字节为单位）。<br>更改此设置后，必须重新启动应用程序。 | 1–1000<br>默认值：500。 |
| WdTraceLevel | 启用Watchdog 服务器跟踪并设置跟踪文件的详细级别。 | Detailed – 生成详细的 Watchdog 服务器跟踪文件<br>MediumDetailed – 生成包含信息消息和错误消息 Watchdog 服务器跟踪文件。<br>NotDetailed – 生成包含错误消息的 Watchdog 服文件。<br>None – 不生成 Watchdog 服务器跟踪文件。<br>Product （默认值）– 将该值设置为等于 TraceLe |
| 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。<br>此设置仅适用于不支持 fanotify 的操作系统。<br>更改此设置的值后，需要重新启动文件威胁防护任务。 | 4096–33554432<br>默认值：16384。 |
| 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破坏设备或数据的合的检测。<br>No （默认）：禁用对入侵者可以用来破坏设备或数应用程序的检测。 |
| NamespaceMonitoring | 启用对命名空间和容器的扫描。<br>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）启用对命名空间和容器的扫描。<br>No 禁用对命名空间和容器的扫描。 |
| 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、对象的执行防护操作以及可移动驱动器扫描任务。 | Yes （默认值）– 在扫描期间阻止对文件的访问。<br>No – 在扫描期间允许访问文件。允许请求任何文件步完成。这种文件操作拦截模式在扫描时对系统性小，但存在文件中的威胁可能无法清除或删除的风扫描期间，与此文件关联的进程在应用程序能够判状态之前成功重命名了此文件，则可能会发生这种是，文件威胁防护、设备控制、执行防护组件以及器扫描任务均以通知模式运行，而不考虑所选的运 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `UseKSN` | 为应用程序配置卡巴斯基安全网络。 | `Basic` — 启用以标准模式使用卡巴斯基安全网络。<br>`Extended` — 启用以扩展模式使用卡巴斯基安全网<br>`No`（默认值）— 不使用卡巴斯基安全网络。 |
| `CloudMode` | 启用云模式。如果启用了 KSN，则云模式可用。<br>如果您计划使用云模式，请确保在您的设备上可以使用 KSN。<br>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）— 启用一种运行模式，在该模式下 Endpoint Security 使用轻量级版本的恶意软件数据<br>`No`（默认值）— 使用恶意软件数据库的完整版本。<br>如果禁用 KSN，将自动禁用云模式。 |
| `UseMDR` | 启用 Managed Detection and Response 组件，以便与 Kaspersky Managed Detection and Response 整合。<br>如果启用 MDR 组件，并且卡巴斯基安全网络被禁用或在基本模式下使用，则会显示错误消息并且不会启用 MDR 组件。要启用 MDR 组件，您必须在扩展模式下启用 KSN。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `Yes` — 启用 Managed Detection and Response 组件<br>`No`（默认值）— 禁用 Managed Detection and Resp<br>件。 |
| `UseEdrOptimum` | 启用 EDR Optimum 组件以便与Kaspersky Endpoint Detection and Response Optimum整合。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `Yes` — 启用 EDR Optimum 组件。<br>`No`（默认）— 禁用 EDR Optimum 组件。 |
| `UseProxy` | 允许 Kaspersky Endpoint Security 组件使用代理服务器。代理服务器可用于访问卡巴斯基激活服务器、数据库和应用程序模块的更新源、卡巴斯基安全网络，以及使用 Web 威胁防护组件验证网站证书时。<br>如果 Kaspersky Endpoint Security 以 Light Agent 模式使用，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`：启用代理服务器的使用。<br>`No`（默认）— 禁用代理服务器的使用。 |
| `ProxyServer` | 用于连接到互联网的代理服务器的地址。<br>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。 | 代理服务器的地址采用以下格式之一：<br>• `[<connection protocol>://]<address o`<br>`proxy server>:<port>`，如果连接到代理服<br>身份验证；<br>• `[<connection protocol>://][<user name`<br>`[<password>]@]<address of the proxy s`<br>`<port>`，如果连接到代理服务器时需要身份验<br>IPv6 地址时，请将其输入方括号中。<br>不支持通过 HTTPS 连接到代理服务器。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| ProxyBypass | 需绕过代理服务器的地址列表。 | 地址以 <address>[:<port>]格式指定。要指定地<br>以使用掩码（*符号）以及\符号后的注释。 |
| ProxyBypassEdr | 连接到 Kaspersky Endpoint Detection and Response Expert (on-premises) Integration Server 时是否使用代理服务器。<br>此设置不适用于配备 Elbrus CPU 的设备。 | Yes 在连接到 Kaspersky Endpoint Detection and R<br>Expert (on-premise) Integration Server 时不使用代<br>No （默认值）在连接到 Kaspersky Endpoint Detec<br>Response Expert (on-premise) Integration Server 时<br>服务器。 |
| ProxyBypassNdr | 连接到 Kaspersky Network Detection and Response (KATA) Integration Server 时是否使用代理服务器。<br>此设置不适用于配备 Elbrus CPU 的设备。 | Yes — 连接到 Kaspersky Network Detection and Re<br>（KATA）Integration Server 时不使用代理服务器。<br>No （默认值）– 连接到 Kaspersk Network Detectio<br>Response (KATA) Integration Server 时使用代理服务 |
| ProxyBypassSandbox | 连接到提供与 Sandbox 交互的服务器时是否使用代理服务器。<br>此设置不适用于配备 Elbrus CPU 的设备。 | Yes，在连接到提供与 Sandbox 交互的服务器时绕<br>器。<br>No （默认值），在连接到提供与 Sandbox 交互的服<br>用代理服务器。 |
| 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。<br>如果值为 0，则不保存新事件，并删除旧事件。 |
| 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 特权或 kesladmin 角色的用户可以启动的任务数。 | 0–100000<br>0 表示非特权用户无法启动自定义扫描任务。<br>默认值：100。 |
| UseSyslog | 启用将应用程序事件记录到 syslog。<br>访问 syslog 需要 root 特权。 | Yes：启用将事件保存到 syslog。<br>No （默认）：禁用将事件保存到 syslog。 |
| EventsStoragePath | 事件日志数据库主文件的路径。<br>需要 root 权限才能访问默认事件数据库。 | 默认值：<br>/var/opt/kaspersky/kesl/private/storage/ |
| 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。<br>您可以指定要从扫描中排除的多个挂载点。<br>必须以与 mount 命令输出中所显示的相同方式指定挂载点。<br>ExcludedMountPoint.item_# 设置默认未指定。 | AllRemoteMounted – 从文件操作拦截中排除使用<br>NFS 协议挂载在设备上的所有远程目录。<br>Mounted:NFS – 从文件操作拦截中排除使用 NFS 协<br>计算机上的所有远程目录。<br>Mounted:SMB – 从文件操作拦截中排除使用 SMB<br>计算机上的所有远程目录。<br>Mounted:<file system type>：从文件操作拦截<br>有指定文件系统类型的所有已挂载目录。<br>/mnt – 从文件操作拦截中排除 /mnt 挂载点（包括<br>的对象。此目录用作可移动驱动器的临时挂载点。<br><path that contains the /mnt/user*\|/mnt/**/user_share>：从文件操作<br>除挂载点中名称包含指定掩码的对象。 |
| MemScanExcludedProgramPath.item_# | 从扫描中排除进程内存。<br>应用程序不扫描指定进程的内存。 | <full path to process> — 从扫描中排除指定目<br>象。您可以使用掩码指定路径。 |
| PowerSaveMode | 设备使用电池供电时取消计划任务。 | Yes （默认值）：当设备使用电池供电时会跳过计<br>No：无论设备是否使用电池供电，都会运行计划任 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `UseOnDemandCPULimit` | 启用 *ODS*、*ContainerScan* 和 *InventoryScan* 类型任务的 CPU 使用率限制。 | `Yes`：启用 *ODS*、*ContainerScan* 和 *InventoryScan* CPU 使用率限制。<br>`No`（默认）：禁用任务的 CPU 使用率限制。 |
| `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 到 100 之间的整数值。<br>默认值：100。 |
| `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备份副本。<br>要移除备份容量限制，请设置 0。 | 0 至 4000<br>0 — 无限制容量。<br>默认值：0。 |
| `BackupDaysToLive` | 在备份存储中存储对象的时间段（天数）。指定时间过去后，应用程序将删除文件的最旧备份副本。<br>要删除对象保留限制，请设置 0。 | 0 至 10000<br>0 — 无限保留。<br>默认值：30。 |
| `QuarantineSizeLimit` | 隔离区的最大大小（以兆字节为单位）。当达到最大隔离区大小时，应用程序会删除掉最旧的文件。<br>要使隔离区的大小不受限制，请输入 0。<br>此设置不适用于配备 Elbrus CPU 的设备。 | 0 至 999999<br>0 表示隔离区大小不受限制。<br>如果应用程序以标准模式使用，则默认值为 200；序以 Light Agent 模式使用，则默认值为 100。 |
| `QuarantineFillingNotification` | 隔离区百分比，百分比必须达到 100% 才会生成隔离区已满的事件。<br>要禁用生成有关已满隔离区的事件，请输入 0。<br>此设置不适用于配备 Elbrus CPU 的设备。 | 0 至 100<br>0 – 禁用生成有关已满隔离区的事件。<br>默认值：90。 |
| `QuarantineBackupFolder` | 存储文件备份副本和隔离文件的目录的路径。<br>您可以更改默认目录。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。<br>此设置不适用于配备 Elbrus CPU 的设备。使用 `BackupFolder` 设置。 | 默认值：<br>`/var/opt/kaspersky/kesl/common/objects-b`<br>访问默认目录需要 root 特权。 |
| `BackupFolder` | 备份目录的路径。<br>您可以更改默认目录。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/ob backup/`<br>需要 root 特权才能访问备份存储目录。 |
| `ShowPopUpNotifications` | 允许在图形用户界面中显示弹出通知。 | `Yes`（默认值）— 在图形用户界面中显示弹出通知<br>`No` — 不在图形用户界面中显示弹出通知。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| InterceptorMode | Kaspersky Endpoint Security 使用的系统事件拦截机制：<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br>此设置不适用于配备 Elbrus CPU 的设备。 | UseFanotify （默认）— 使用 fanotify 技术来拦截<br>UseUpdatableKernelModule — 用于通过可更新内拦截系统事件。 |
| InterceptorFallbackStrategy | 如果可更新内核模块启动失败，应用程序执行的操作。<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。 | FallbackToFanotify （默认）— 切换到 fanotify 件拦截。<br>FallbackToLimitedMode — 不使用系统事件拦截程序不使用系统事件拦截，则不会执行文件实时扫低设备的保护级别。 |
| InterceptorApplyStrategy | 如果应用程序切换到使用可更新内核模块，则必须重启应用程序才能启动该模块。此设置允许您指定是希望自动重启应用程序还是希望手动重启应用程序。<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。 | RestartServiceAutomatically 自动重启应用程可更新内核模块。建议使用此设置。<br>RestartServiceManually （默认）在用户手动重序后启动可更新内核模块。 |
| SystemEventsTransmission | 启用传输来自第三方应用程序（非卡巴斯基解决方案）的事件信息。如果启用此设置，除了自身事件外，Kaspersky Endpoint Security 还会将第三方应用程序的 systemd-journald 事件发送到应用程序事件日志。<br>访问 systemd-journald 需要 root 权限。 | Yes 启用将第三方应用程序的 systemd-journald 事到应用程序事件日志。<br>No （默认）禁用将第三方应用程序的 systemd-jou信息传输到应用程序事件日志。 |
| UrgentUpdateRestartEnabled | 安装应用程序后的前 24 小时过后，收到关键更新时自动重启应用程序。 | Yes 表示收到关键更新时自动重启应用程序。<br>No （默认值）表示收到关键更新时不重启应用程序 |
| CoreDumps | 当应用程序发生故障时，启用创建转储文件。 | Yes 表示应用程序崩溃时创建转储文件。<br>No （默认值）表示应用程序崩溃时不创建转储文件 |
| CoreDumpsPath | 存储转储文件的目录的路径。 | 默认值：<br>/var/opt/kaspersky/kesl/common/dumps<br>需要 root 特权才能访问默认转储文件目录。 |

实用文章

### 如何指定掩码

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。

# 任务计划

下表介绍了可为所有应用程序任务管理的任务计划设置。

任务启动计划设置

| 设置 | 描述 |
| --- | --- |
| RuleType | 任务启动计划。<br>• Once：运行一次任务。<br>• Monthly：每月在指定的日期和时间运行任务。<br>• Weekly：每周在指定的日期和时间运行任务。<br>• Daily：按照指定的天数间隔定期运行任务。<br>• 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。<br>• Minutely：从指定的时间开始，按照指定的分钟间隔定期运行任务。<br>• Manual – 手动启动任务。<br>• PS – 启动应用程序后启动任务。<br>• 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。此设置的格式取决于 RuleType。<br>可能的值：<br>• <year>:1970 至 2099<br>• <month>:JAN，FEB，MAR，APR，MAY，JUN，JUL，AUG，SEP，OCT，NOV，DEC。<br>• <day of the month>:1 至 31<br>• <day of the week>:Mon，Tue，Wed，Thu，Fri，Sat，Sun。<br>• <hh>:0 至 23<br>• <mm>:0 至 59<br>• <ss>:0 至 59<br>• <interval between runs (in days)>:0 至 364<br>• <interval between runs (in hours)>:0 至 23<br>• <interval between runs (in minutes)>:0 至 59 |
| RandomInterval | 在一定时间间隔内（从 0 到指定值），随机在计算机上运行该任务。这样可以避免多个任务同时启动。<br>默认值：99 分钟。<br>可能值：0 – 999。 |
| RunMissedStartRules | 在应用程序启动后运行漏掉的任务。<br>• Yes（默认值）表示已启用运行错过的任务。如果在计划任务运行时应用程序停止运行或计算机断电，Kaspersky Endpoint Security 会在应用程序启动后立即启动该任务。这有助于确保绝不会错过关键任务。<br>• No 表示已禁用运行错过的任务。如果在计划任务运行时应用程序停止运行或计算机断电，应用程序将跳过该任务。这有助于避免在启动应用程序时产生额外负载。 |
| UseWorkingTimeout | 达到 WorkingTimeout 设置指定的最大任务执行时间时停止任务。即使未完成，任务也会停止。下次任务启动将按照计划进行。<br>• Yes – 当达到最大任务执行时间时停止任务。<br>• No（默认值）– 达到最大任务执行时间时不停止任务。 |
| WorkingTimeout | 如果 UseWorkingTimeout=Yes，则应用程序停止执行任务后的最大任务执行时间（以分钟为单位）。<br>默认值：120 分钟。<br>可能值：1 – 999。 |

# 配置代理服务器设置

在命令行中，您可以使用 `UseProxy`、`ProxyServer`、`ProxyBypass`、`ProxyBypassEdr`、`ProxyBypassNdr` 和 `ProxyBypassSandbox` 常规应用程序设置来管理应用程序组件的代理服务器设置。

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。

`UseProxy` 参数可以采用以下值：

- `Yes` 启用代理服务器的使用。
- `No` 禁用代理服务器。

ProxyServer 设置允许以 `<connection protocol>://[<user>[:<password>]@]<proxy server address>:<port number>` 格式指定代理服务器设置，其中：

- `<user>` 是用于在代理服务器上进行身份验证的用户名。
- `<password>` 是用于在代理服务器上进行身份验证的用户密码。
- `<proxy server address>` 是代理服务器的 IP 地址或域名。
- `<port number>` 是代理服务器的端口号。

不支持通过 HTTPS 连接到代理服务器。

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。

`ProxyBypass` 设置允许您指定无需代理服务器即可连接的地址列表。地址以 `<address>[:<port number>]` 格式指定。要指定地址，您可以使用掩码（ `*`符号）和注释（在 `\` 符号之后）。

以下设置可用于配置 EDR Expert (on-premises)、NDR (KATA) 和沙盒组件对代理服务器的使用，这些组件提供与 Detection and Response 解决方案的集成：

- 在连接到提供与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成的服务器时， `ProxyBypassEdr` 设置可启用或禁用代理服务器的使用。
- `ProxyBypassNdr`设置可启用或禁用当连接到提供与 Kaspersky Network Detection and Response (KATA) 进行集成的服务器时使用代理服务器。
- `ProxyBypassSandbox` 设置可启用或禁用当连接到提供与 Sandbox 进行交互的服务器时使用代理服务器。

设置可以使用以下值：

- `Yes` 启用代理服务器的使用。
- `No` 禁用代理服务器。

# 配置备份设置

在命令行中，您可以使用常规应用程序设置中的 `BackupDaysToLive`、、 `BackupSizeLimit` 和 `QuarantineBackupFolder` 设置来配置备份设置。

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。

备份设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `BackupDaysToLive` | 在备份存储中存储对象的时间段（天数）。指定时间过去后，应用程序将删除文件的最旧备份副本。<br>要删除对象保留限制，请设置 0。 | 0 至 10000<br>0 — 无限保留。<br>默认值：30。 |
| `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备份副本。<br>要移除备份容量限制，请设置 0。 | 0 至 4000<br>0 — 无限制容量。<br>默认值：0。 |
| `QuarantineBackupFolder` | 存储文件备份副本和隔离文件的目录的路径。<br>您可以更改默认目录。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。<br>此设置不适用于配备 Elbrus CPU 的设备。使用 `BackupFolder` 设置。 | 默认值：`/var/opt/kaspersky/kesl/common/objects-backup/`<br>访问默认目录需要 root 特权。 |
| `BackupFolder` | 备份目录的路径。<br>您可以更改默认目录。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/`<br>需要 root 特权才能访问备份存储目录。 |

# 网络流量扫描设置

网络流量扫描设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `EncryptedConnectionsScan` | 启用或禁用对加密连接的扫描。<br>对于 FTP 协议，默认情况下禁用加密连接扫描。 | `Yes`（默认值）- 启用加密连接扫描。<br>`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` | 指定在网站上发生加密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。<br>`Disconnect` – 阻止网络连接。 |
| `CertificateVerificationPolicy` | 指定 Kaspersky Endpoint Security 检查证书的方式。<br>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。<br>`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。<br>`Block` – 阻止在使用非可信证书访问域时建立的网络连接。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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）。<br>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）。<br>All – 监控所有网络端口。<br>指定此值可能会大大增加操作系统负载。 |
| NetInterceptorMode | Kaspersky Endpoint Security 应用程序的流量拦截模式。<br>此设置不适用于配备 Elbrus CPU 的设备。 | UseEBPF — 使用 eBPF 技术拦截流量。<br>UseIPTables（默认值）— 使用 iptables 实用程序拦截流量。<br>要更改流量拦截模式，您需要重启应用程序。重启会断开已连接的网络连接。 |
| **[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连接。 | | |
| DomainName | 指定域名。 | 您可以在指定域时使用掩码。 |
| **[IncomingEndpointsExclusions.item_#]**部分包含入站流量的排除项。 | | |
| RemoteIp | 远程设备的 IP 地址，其流量将被排除在拦截范围之外。 | |
| DestinationPort | 受保护设备上的端口，来自远程设备的流量将被排除在拦截范围之外。 | |
| **[OutgoingEndpointsExclusions.item_#]**部分包含出站流量的排除项。 | | |
| RemoteIp | 远程设备的 IP 地址，其流量将被排除在拦截范围之外。 | |
| DestinationPort | 远程设备上的端口，来自受保护设备的流量将被排除在拦截范围之外。 | |
| **[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。 | |
| Port | 应用程序要监控的网络端口号。 | 1 – 65535。<br>默认值为未定义。 |

# 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该设置的值。

ExcludedMountPoint.item_# 参数可以采用以下值：

- 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 协议挂载在计算机上的所有远程目录。
- 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:<file system type>`：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。
- `<path containing the mask /mnt/user* or /mnt/**/user_share>`：从文件操作拦截中排除挂载点中名称包含指定掩码的对象。

> 必须以与 `mount` 命令输出中所显示的相同方式指定挂载点。

您可以指定要从扫描中排除的多个挂载点。

实用文章

**如何指定掩码**

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。

# 密码保护设置

您可以使用命令行选项或通过编辑配置文件来更改设置，以授予或撤销管理应用程序的权限。

密码保护设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `StopProtection` | 禁用保护组件。 | `Yes` 允许用户执行该操作。<br>`No` 禁止用户执行操作。 |
| `StopSecurityControl` | 禁用控制组件 | |
| `StartProtection` | 启用保护组件 | |
| `StartSecurityControl` | 启用控制组件 | |
| `ApplicationSettings` | 配置应用程序 | |
| `ViewReports` | 查看报告 | |
| `RestoreFromBackup` | 从备份区恢复 | |
| `RemoveLicenseKey` | 删除密钥 | |
| `AddLicense` | 添加密钥 | |
| `DisablePolicy` | 禁用 Kaspersky Security Center 策略 | |

# 管理控制台中的应用程序设置

您使用策略来配置 Kaspersky Endpoint Security。有关应用程序组件的详细信息，请参见相应章节。

# 数据库更新

在管理控制台中，您可以使用“更新”任务更新数据库。

您可以创建并运行“更新”用户任务。您可以通过编辑任务设置来管理更新设置。

在“更新”任务的属性的**更新源**和**设置**区域中，您可以管理下表中列出的设置。

Update 任务部分的更新源

| 设置 | 描述 |
| --- | --- |
| **更新源** | 此表包含数据库更新源列表。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。<br>该表包含以下列：<br>• **源地址**是更新源的地址：<br>  • **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）。<br>  • **Kaspersky Security Center** – Kaspersky Security Center 管理服务器。<br>  • 用户添加的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。<br>• **状态**指示更新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。<br>您可以在表中添加、编辑、删除、上移或下移更新源。 |

Update 任务设置部分

| 设置 | 描述 |
| --- | --- |
| **更新源响应超时（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。<br>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。<br>默认值：10 秒。 |
| **应用程序更新下载模式** | 在下拉列表中，您可以选择自动安装的更新（自动补丁）的下载方式：<br>• **不下载**。选择此项时，不会自动下载自动补丁。<br>• **仅下载**。选择此列表项时，将自动下载自动补丁，但不安装在客户端设备上（默认设置）。<br>• **下载并安装**。选中此列表项后，自动补丁会被自动下载并安装到客户端设备上。安装自动补丁后，应用程序将自动重启。 |

# 主机威胁防护

## 文件威胁防护

在管理控制台中，您可以在策略属性（**基本威胁防护 → 文件威胁防护**）中管理文件威胁防护。

文件威胁防护组件设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>默认情况下已选定该选框。 |
| **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：<br>• **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。<br>• **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。<br>• **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。 |
| **检测到威胁后的操作** | 这组设置包含**配置**按钮。点击此按钮将打开"**检测到威胁后的操作**"窗口，您可以在其中配置应用程序对检测到的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 | 描述 |
| --- | --- |
| **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。

# “新建扫描范围”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 | 描述 |
| --- | --- |
| **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。<br>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。<br>如果选中此复选框，应用程序将处理此扫描范围。<br>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。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 该设置块可让您设置扫描范围。<br>您可以在文件系统下拉列表中选择文件系统类型：<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。<br>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。<br>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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

## 如何指定掩码

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。

## 如何使用标签

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名称

`<path to local directory>` 是本地目录的路径。

您还可以使用唯一的标签组合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

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:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

## “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 | 描述 |
| --- | --- |
| **扫描压缩文件** | 此复选框用于启用或禁用压缩文件扫描。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将扫描压缩文件。<br>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“**跳过扫描时间超过以下值的文件（秒）**”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。<br>如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描压缩文件。<br>默认情况下已清空该复选框。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将扫描自解压缩文件。<br>如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描自解压缩文件。<br>如果清除**扫描压缩文件**复选框，则此复选框可用。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将扫描邮件数据库文件。<br>如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描邮件数据库文件。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将扫描纯文本邮件。<br>如果清除此复选框，则 Kaspersky Endpoint Security 不会扫描纯文本邮件。<br>默认情况下已清空该复选框。 |
| **跳过文本文件** | 从扫描中临时排除纯文本格式的文件。<br>如果选中该复选框，Kaspersky Endpoint Security 将不扫描文本文件，前提是它们在最近一次扫描后 10 分钟内被同一进程使用。此设置使优化应用程序日志扫描成为可能。<br>如果取消选中此复选框，Kaspersky Endpoint Security 将扫描文本文件。<br>默认情况下已清空该复选框。<br>如果您使用基于 fanotify 的系统事件拦截机制，则会应用此设置。使用可更新内核模块时，会利用扫描结果缓存优化扫描。 |
| **跳过数据库日志文件** | 暂时将数据库日志文件排除在扫描范围之外。<br>如果选中该复选框，并且数据库日志文件在最近一次扫描后的 10 分钟内由同一进程重复使用，则应用程序不会扫描这些文件。此设置能够优化数据库日志文件的扫描。<br>如果清除此复选框，则应用程序将扫描数据库日志文件。<br>默认情况下已清空该复选框。<br>如果您使用基于 fanotify 的系统事件拦截机制，则会应用此设置。使用可更新内核模块时，会利用扫描结果缓存优化扫描。 |
| **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。<br>可用值：0-9999。如果该值设置为 0，则扫描时间不受限制。<br>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）。<br>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。<br>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。<br>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。<br>如果清除此复选框，则 Kaspersky Endpoint Security 不会记录 *ObjectProcessed* 类型事件。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将记录 *ObjectNotProcessed* 类型事件。<br>如果清除此复选框，则 Kaspersky Endpoint Security 不会记录 *ObjectNotProcessed* 类型事件。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将记录 *PackedObjectDetected* 类型事件。<br>如果清除此复选框，则 Kaspersky Endpoint Security 不会记录 *PackedObjectDetected* 类型事件。<br>默认情况下已清空该复选框。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>默认情况下已选定该选框。 |
| **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：<br>• **轻度**是详细程度最低的扫描，系统负载最小。<br>• **中度**是中度扫描，系统负载平衡。<br>• **深度**是最详细的扫描，系统负载最大。<br>• **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。 |

## “检测到威胁后的操作”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 | 描述 |
| --- | --- |
| **检测到威胁后的操作** | 您可以选择应用程序对检测到的感染对象执行的操作：<br>• **清除；无法清除则删除**（默认）。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>• **清除；清除失败则阻止**。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将阻止访问感染对象。<br>• **阻止**。如果选择此操作，则应用程序将阻止访问感染对象。<br>当感染对象被清除或删除后，感染对象的副本将被保存在备份区中。 |

## 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（**基本威胁防护 → 文件威胁防护排除项**）中配置文件威胁防护排除项。

扫描排除项设置

| 设置组 | 描述 |
| --- | --- |
| **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

此窗口包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。

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。 |

默认情况下，排除范围表为空。您可以在表中添加、编辑和删除项目。

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。

## “新排除范围”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。<br>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。<br>如果选中此复选框，则应用程序在扫描期间将排除此区域。<br>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。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 该设置块可让您设置排除范围。<br>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：<br>• “**本地**”，表示本地目录。<br>• **挂载**– 已挂载的目录。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。<br>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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

**如何使用标签**

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名称

`<path to local directory>` 是本地目录的路径。

您还可以使用唯一的标签组合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

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:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

## “按掩码筛选的排除项”窗口

您可以按名称掩码配置对象的扫描排除项。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“**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）。

您可以启用合并子策略继承时的排除列表。如果要合并列表项，请选中**合并继承的值**复选框。如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。如果清除此复选框，则继承策略设置时不会合并列表项。默认情况下已清空该复选框。

## “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。

您可以启用合并子策略继承时的排除列表。如果要合并列表项，请选中**合并继承的值**复选框。如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。如果清除此复选框，则继承策略设置时不会合并列表项。默认情况下已清空该复选框。

## “按进程筛选的排除项”窗口

此窗口包含按进程进行的排除范围。通过按进程进行排除的排除范围，您可以从扫描中排除指示进程的活动以及被指示进程修改的文件。默认情况下，该列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 |
| --- | --- |
| **合并继承的值** | 此复选框可启用或禁用在子策略中继承时合并列表。<br>如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。<br>如果清除该复选框，则继承策略设置时不会合并列表项。<br>默认情况下已清空该复选框。 |
| **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、编辑或删除项目。

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。<br>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。<br>如果使用可更新内核模块进行系统事件拦截，则指定进程将被排除在所有命名空间的拦截之外。 |
| **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。<br>默认情况下已清空该复选框。 |
| **使用此范围** | 该复选框用于启用或禁用此排除范围。<br>如果选中此复选框，则应用程序在扫描期间将排除此区域。<br>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。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>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：<br>• "**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。<br>• **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。<br>• **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。<br>• **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。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。 |
| **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。<br>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。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

## 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，也可以创建并运行用于扫描的用户任务。您可以通过编辑任务设置来管理扫描设置。

在 *搜索恶意软件* 任务的属性中，在 **设置** 部分，您可以管理下表列出的设置。

恶意软件扫描任务设置

| 设置 | 描述 |
| --- | --- |
| **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。 |
| **检测到威胁后的操作** | 这组设置包含**配置**按钮。点击此按钮将打开"**检测到威胁后的操作**"窗口，您可以在其中配置应用程序对检测到的感染对象执行的操作。 |

在 *搜索恶意软件* 任务的属性中，在 **排除项** 部分，您可以自定义排除范围、按掩码排除和按威胁名称排除。

## “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 | 描述 |
| --- | --- |
| **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 | 描述 |
| --- | --- |
| **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。<br>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。<br>如果选中此复选框，应用程序将处理此扫描范围。<br>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。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| **文件系统，访问协议和路径** | 该设置块可让您设置扫描范围。<br>您可以在文件系统下拉列表中选择文件系统类型：<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。<br>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。<br>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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

### 如何使用标签

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名称

`<path to local directory>` 是本地目录的路径。

您还可以使用唯一的标签组合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

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:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

## “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 | 描述 |
| --- | --- |
| **扫描文件** | 此复选框启用或禁用文件扫描。<br>如果选中该复选框，应用程序将扫描文件。<br>如果清除了该复选框，则应用程序不会扫描文件。<br>默认情况下已选定该选框。 |
| **扫描启动扇区** | 此复选框启用或禁用引导扇区扫描。<br>如果选中该复选框，应用程序将扫描引导扇区。<br>如果清除该复选框，则应用程序不扫描引导扇区。<br>默认情况下已清空该复选框。 |
| **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。<br>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。<br>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。<br>默认情况下已清空该复选框。 |
| **扫描启动对象** | 此复选框启用或禁用启动对象扫描。<br>如果选中该复选框，应用程序将扫描启动对象。<br>如果清除了该复选框，则应用程序不会扫描启动对象。<br>默认情况下已清空该复选框。 |
| **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。<br>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。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>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。<br>默认情况下已选定该选框。 |

## “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。

## “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 | 描述 |
| --- | --- |
| **扫描压缩文件** | 此复选框用于启用或禁用压缩文件扫描。<br>如果选中该复选框，应用程序将扫描压缩文件。<br>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。您可以通过在 **常规扫描设置** 部分中配置 **跳过扫描时间超过以下值的文件（秒）** 和 **跳过大于以下大小的文件 (MB)** 设置，缩短压缩文件扫描的持续时间。<br>如果清除该复选框，应用程序不会扫描压缩文件。<br>默认情况下已选定该选框。 |
| **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。<br>如果选中该复选框，应用程序将扫描自解压存档。<br>如果清除了该复选框，则应用程序不会扫描自解压存档。<br>如果清除 **扫描压缩文件** 复选框，则此复选框可用。<br>默认情况下已选定该选框。 |
| **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。<br>如果选中该复选框，应用程序将扫描邮件数据库文件。<br>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。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，则应用程序将扫描纯文本邮件。<br>如果清除此复选框，则应用程序不会扫描纯文本邮件。<br>默认情况下已清空该复选框。 |
| **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。<br>可用值：0-9999。如果该值设置为 0，则扫描时间不受限制。<br>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）。<br>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。<br>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。<br>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。<br>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。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。<br>如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。<br>默认情况下已清空该复选框。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。<br>如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。<br>默认情况下已清空该复选框。 |
| **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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>默认情况下已选定该选框。 |
| **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：<br>• **轻度** 是详细程度最低的扫描，系统负载最小。<br>• **中度** 是中度扫描，系统负载平衡。<br>• **深度** 是最详细的扫描，系统负载最大。<br>• **推荐**（默认）是卡巴斯基专家推荐的最佳级别。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。 |
| **不同时运行多个扫描任务** | 如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。<br>默认情况下已清空该复选框。 |

## "检测到威胁后的操作"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 | 描述 |
| --- | --- |
| **检测到威胁后的操作** | 您可以选择应用程序对检测到的受感染对象执行的操作：<br>• **清除；无法清除则删除**（默认）。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>• **清除；清除失败则通知**。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>• **通知**。如果选择此操作，应用程序会在日志中创建关于感染对象的记录。 |

## "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 | 描述 |
| --- | --- |
| **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

此窗口包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。

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。 |

默认情况下，排除范围表为空。您可以在表中添加、编辑和删除项目。

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。

## “新排除范围”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。<br>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。<br>如果选中此复选框，则应用程序在扫描期间将排除此区域。<br>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。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 该设置块可让您设置排除范围。<br>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：<br>• “**本地**”，表示本地目录。<br>• **挂载**– 已挂载的目录。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。<br>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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

**如何使用标签**

您可以使用特殊标签来指定容器或镜像：

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名称

<path to local directory> 是本地目录的路径。

您还可以使用唯一的标签组合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

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:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

您可以在名称和标识符中使用掩码（? 和 * 字符）。

## “按掩码筛选的排除项”窗口

您可以按名称掩码配置对象的扫描排除项。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“**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。

## 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。

您可以创建并运行自定义关键区域扫描任务。您可以通过编辑任务设置来管理扫描设置。

在 *关键区域扫描* 任务的属性中，在 **设置** 部分，您可以管理下表中列出的设置。

关键区域扫描任务设置

| 设置 | 描述 |
| --- | --- |
| **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。 |
| **检测到威胁后的操作** | 这组设置包含**配置**按钮。点击此按钮将打开“**检测到威胁后的操作**”窗口，您可以在其中配置应用程序对检测到的感染对象执行的操作。 |

在 *关键区域扫描* 任务的属性中，在 **排除** 部分，您可以自定义 排除范围、按掩码排除项和按威胁名称排除项。

### “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 | 描述 |
| --- | --- |
| **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。

## “新建扫描范围”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 | 描述 |
| --- | --- |
| **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。<br>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。<br>如果选中此复选框，应用程序将处理此扫描范围。<br>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。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 该设置块可让您设置扫描范围。<br>您可以在文件系统下拉列表中选择文件系统类型：<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。<br>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。<br>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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

**如何使用标签**

您可以使用特殊标签来指定容器或镜像：

- [container-id:<id>]/<path to local directory>
- [container-name:<name>]/<path to local directory>
- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

其中：

<id> 是容器 ID。

<name> 是容器名称

<path to local directory> 是本地目录的路径。

您还可以使用唯一的标签组合：[container-id:<id>]、[container-name:<name>]、[image-id:<id>] 和 [image-name:<name>]/path to local directory>。

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:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

您可以在名称和标识符中使用掩码（? 和 * 字符）。

## “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 | 描述 |
| --- | --- |
| **扫描文件** | 此复选框启用或禁用文件扫描。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将扫描文件。<br>如果取消选中此复选框，则 Kaspersky Endpoint Security 不会扫描文件。<br>默认情况下已清空该复选框。 |
| **扫描启动扇区** | 此复选框启用或禁用引导扇区扫描。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将扫描引导扇区。<br>如果取消选中此复选框，则 Kaspersky Endpoint Security 不会扫描引导扇区。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **扫描启动对象** | 此复选框启用或禁用启动对象扫描。<br>如果选中此复选框，则 Kaspersky Endpoint Security 将扫描启动对象。<br>如果取消选中此复选框，则 Kaspersky Endpoint Security 不会扫描启动对象。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>默认情况下已选定该选框。 |

## “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。

## “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 | 描述 |
| --- | --- |
| **扫描压缩文件** | 此复选框用于启用或禁用压缩文件扫描。<br>如果选中该复选框，应用程序将扫描压缩文件。<br>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。您可以通过在 **常规扫描设置** 部分中配置 **跳过扫描时间超过以下值的文件（秒）** 和 **跳过大于以下大小的文件 (MB)** 设置，缩短压缩文件扫描的持续时间。<br>如果清除该复选框，应用程序不会扫描压缩文件。<br>默认情况下已选定该选框。 |
| **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。<br>如果选中该复选框，应用程序将扫描自解压存档。<br>如果清除了该复选框，则应用程序不会扫描自解压存档。<br>如果清除 **扫描压缩文件** 复选框，则此复选框可用。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>如果选中该复选框，应用程序将扫描邮件数据库文件。<br>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。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，则应用程序将扫描纯文本邮件。<br>如果清除此复选框，则应用程序不会扫描纯文本邮件。<br>默认情况下已清空该复选框。 |
| **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。<br>可用值：0-9999。如果该值设置为 0，则扫描时间不受限制。<br>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）。<br>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。<br>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。<br>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。<br>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。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。<br>如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。<br>如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。<br>默认情况下已清空该复选框。 |
| **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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>默认情况下已选定该选框。 |
| **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：<br>• **轻度** 是详细程度最低的扫描，系统负载最小。<br>• **中度** 是中度扫描，系统负载平衡。<br>• **深度** 是最详细的扫描，系统负载最大。<br>• **推荐**（默认）是卡巴斯基专家推荐的最佳级别。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。 |
| **不同时运行多个扫描任务** | 如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。<br>默认情况下已清空该复选框。 |

## “检测到威胁后的操作”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 | 描述 |
| --- | --- |
| **检测到威胁后的操作** | 您可以选择应用程序对检测到的受感染对象执行的操作：<br>• **清除；无法清除则删除**（默认）。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>• **清除；清除失败则通知**。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>• **通知**。如果选择此操作，应用程序会在日志中创建关于感染对象的记录。 |

## “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 | 描述 |
| --- | --- |
| **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

此窗口包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。

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。 |

默认情况下，排除范围表为空。您可以在表中添加、编辑和删除项目。

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。

## “新排除范围”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。<br>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。<br>如果选中此复选框，则应用程序在扫描期间将排除此区域。<br>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。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| **文件系统，访问协议和路径** | 该设置块可让您设置排除范围。<br>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：<br>• “**本地**”，表示本地目录。<br>• **挂载**– 已挂载的目录。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。<br>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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

### 如何使用标签

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名称

`<path to local directory>` 是本地目录的路径。

您还可以使用唯一的标签组合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

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:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

### “按掩码筛选的排除项”窗口

您可以按名称掩码配置对象的扫描排除项。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“**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。

## 容器监控

在管理控制台中，您可以在策略属性（**常规设置** → **容器扫描设置**）中配置容器监控组件。

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。<br>默认情况下已选定该选框。 |
| **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：<br>• **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。<br>• **停止容器**：如果检测到受感染的对象，应用程序将停止容器。<br>• **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。<br>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 | 描述 |
| --- | --- |
| **使用 Docker** | 该复选框可启用或禁用 Docker 容器管理系统。<br>默认情况下已选定该选框。 |
| **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。<br>默认值：/var/run/docker.sock. |
| **使用 CRI-O** | 该复选框启用或禁用 CRI-O 环境。<br>默认情况下已选定该选框。 |
| **文件路径** | 用于指定 CRI-O 配置文件路径的输入字段。<br>默认值：/etc/crio/crio.conf。 |
| **使用 Podman** | 该复选框启用或禁用 Podman 实用程序。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>默认值：/var/lib/containers/storage |
| **使用 runc** | 该复选框启用或禁用 runc 实用程序。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>默认值：/run/runc。 |

# 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。

您可以创建并运行自定义容器扫描任务。您可以通过编辑任务设置来管理扫描设置。

在 *容器扫描* 任务的属性中，在 **设置** 部分，您可以管理下表中列出的设置。

容器扫描任务设置

| 设置 | 描述 |
| --- | --- |
| **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。 |
| **检测到威胁后的操作** | 这组设置包含**配置**按钮。点击此按钮将打开"**检测到威胁后的操作**"窗口，您可以在其中配置应用程序对检测到的感染对象执行的操作。 |

在 *容器扫描* 任务的属性中，在 **排除** 部分，您还可以配置按掩码排除项和按威胁名称排除项。

## "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 | 描述 |
| --- | --- |
| **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。<br>默认情况下已选定该选框。 |
| **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。<br>默认情况下，指定 * 掩码 – 将扫描所有容器。 |
| **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容器执行的操作：<br>• **跳过容器** – 检测到受感染的对象时，不对容器执行任何操作。<br>• **停止容器** – 检测到受感染对象时停止容器。<br>• **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。<br>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。 |
| **扫描镜像** | 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。<br>默认情况下已选定该选框。 |
| **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。<br>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：<br>• **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。<br>• 检测到受感染对象时**删除镜像**（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。<br>默认情况下已清空该复选框。 |

## "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 | 描述 |
| --- | --- |
| **扫描压缩文件** | 此复选框用于启用或禁用压缩文件扫描。<br>如果选中该复选框，应用程序将扫描压缩文件。<br>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。您可以通过在 **常规扫描设置** 部分中配置 **跳过扫描时间超过以下值的文件（秒）** 和 **跳过大于以下大小的文件 (MB)** 设置，缩短压缩文件扫描的持续时间。<br>如果清除该复选框，应用程序不会扫描压缩文件。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>如果选中该复选框，应用程序将扫描自解压存档。<br>如果清除了该复选框，则应用程序不会扫描自解压存档。<br>如果清除 **扫描压缩文件** 复选框，则此复选框可用。<br>默认情况下已选定该选框。 |
| **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。<br>如果选中该复选框，应用程序将扫描邮件数据库文件。<br>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。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，则应用程序将扫描纯文本邮件。<br>如果清除此复选框，则应用程序不会扫描纯文本邮件。<br>默认情况下已清空该复选框。 |
| **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。<br>可用值：0-9999。如果该值设置为 0，则扫描时间不受限制。<br>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）。<br>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。<br>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。<br>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。<br>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。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，应用程序将记录 *ObjectNotProcessed* 类型的事件。<br>如果清除此复选框，应用程序不会记录 *ObjectNotProcessed* 类型的事件。<br>默认情况下已清空该复选框。 |
| **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。<br>如果选中此复选框，应用程序将记录 *PackedObjectDetected* 类型的事件。<br>如果清除此复选框，应用程序不会记录 *PackedObjectDetected* 类型的事件。<br>默认情况下已清空该复选框。 |
| **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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>默认情况下已选定该选框。 |
| **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：<br>• **轻度** 是详细程度最低的扫描，系统负载最小。<br>• **中度** 是中度扫描，系统负载平衡。<br>• **深度** 是最详细的扫描，系统负载最大。<br>• **推荐**（默认）是卡巴斯基专家推荐的最佳级别。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。 |
| **不同时运行多个扫描任务** | 如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。<br>默认情况下已清空该复选框。 |

## “检测到威胁后的操作”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 | 描述 |
| --- | --- |
| **检测到威胁后的操作** | 您可以选择应用程序对检测到的受感染对象执行的操作：<br>• **清除；无法清除则删除**（默认）。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序将删除感染对象。<br>• **清除；清除失败则通知**。如果选择此操作，应用程序将尝试通过将对象副本保存到备份区中来清除感染对象。如果无法清除（例如，如果无法清除此对象类型或对象中的威胁类型），则应用程序会在日志中创建记录。<br>• **通知**。如果选择此操作，应用程序会在日志中创建关于感染对象的记录。 |

## “排除项”部分

扫描排除项设置

| 设置组 | 描述 |
| --- | --- |
| **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。<br>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。<br>默认情况下已选定该选框。 |

## “按掩码筛选的排除项”窗口

您可以按名称掩码配置对象的扫描排除项。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“**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。

# 可移动驱动器扫描

在管理控制台中，您可以在策略属性（**本地任务 → 可移动驱动器扫描**）中配置可移动驱动器扫描的设置。

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。<br>默认情况下已清空该复选框。 |
| **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：<br>• 连接可移动驱动器时**不扫描**（默认值）。<br>• **快速扫描**：仅扫描可移动驱动器（CD/DVD 驱动器和蓝光光盘除外）上的特定类型文件，并且不解压复合对象。快速扫描使用"*关键区域扫描*"任务的默认设置执行。<br>• **详细扫描**：扫描可移动驱动器（CD/DVD 驱动器和蓝光光盘除外）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：<br>• 连接 CD/DVD 驱动器和蓝光光盘时**不扫描**（默认值）。<br>• **快速扫描**：仅扫描 CD/DVD 驱动器和蓝光光盘上的特定类型文件。快速扫描使用"*关键区域扫描*"任务的默认设置执行。<br>• **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。<br>默认情况下已清空该复选框。 |

实用文章

### 快速扫描的文件类型

在可移动介质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、emf、ico、ov?、xl*、xlsb、pp*、md*、sldx、sldm、thmx。

## 行为检测

在管理控制台中，您可以在策略属性（**高级威胁防护 → 行为检测**）中管理行为检测设置。

行为检测组件设置

| 设置 | 描述 |
| --- | --- |
| **启用行为检测** | 此复选框启用或禁用行为检测组件。<br>默认情况下已选定该选框。 |
| **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：<br>• **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。<br>• **通知**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。<br>默认情况下已清空该复选框。<br>"**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

此窗口包含按进程进行的排除范围。通过进程排除的排除范围可让您排除指定进程的活动。

按进程筛选的排除范围设置

| 设置 | 描述 |
| --- | --- |
| **合并继承的值** | 此复选框可启用或禁用在子策略中继承时合并列表。<br>如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。<br>如果清除该复选框，则继承策略设置时不会合并列表项。<br>默认情况下已清空该复选框。 |
| **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。 |

默认情况下，排除范围表为空。您可以在表中添加、编辑或删除项目。

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。 |
| **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。<br>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。<br>默认情况下已清空该复选框。 |
| **使用此范围** | 该复选框用于启用或禁用此排除范围。<br>如果选中此复选框，则应用程序排除此范围。<br>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。<br>默认情况下已选定该选框。 |
| **从行为检测扫描中排除进程** | 此复选框用于启用或禁用将进程从行为检测扫描范围中排除。<br>默认情况下已清空该复选框。 |
| **将进程从 MDR 和 EDR Expert (on-premises) 遥测中排除** | 此复选框可启用或禁用将进程从 MDR 和 EDR Expert (on-premises) 组件收集的遥测数据中排除。<br>默认情况下已清空该复选框。 |

实用文章

### 如何指定掩码

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。

# 漏洞利用防御

在管理控制台中，您可以在策略属性（**高级威胁防护 → 行为检测**）中配置漏洞利用防御。

漏洞利用防御组件设置

| 设置 | 描述 |
| --- | --- |
| **启用漏洞利用防御** | 此复选框用于启用或禁用漏洞利用防御。<br>默认情况下已清空该复选框。 |
| **漏洞利用防御** | 单击**配置**按钮将打开**漏洞利用防御排除项**窗口，您可以在其中配置漏洞利用防御组件的扫描排除项。 |
| **检测到漏洞后的操作** | 应用程序在检测到漏洞利用时将执行的操作：<br>• **阻止**（默认值）。应用程序会阻止漏洞利用攻击的恶意活动，并在事件日志中记录相关信息。<br>• "**通知**"。应用程序不会阻止漏洞利用攻击活动，只会在事件日志中记录关于漏洞利用检测的信息。 |

## 漏洞利用防御排除窗口

在此窗口中，您可以配置从漏洞利用防御扫描中排除对象。应用程序不会扫描指定对象。默认情况下，对象列表为空。

漏洞利用防御排除设置

| 设置 | 描述 |
| --- | --- |
| **合并继承的值** | 此复选框可启用或禁用在子策略中继承时合并列表。<br>如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。<br>如果清除该复选框，则继承策略设置时不会合并列表项。<br>默认情况下已清空该复选框。 |
| **状态** | 该状态指示应用程序是否使用该排除项。 |
| **威胁名称。** | 要从扫描中排除的威胁名称。 |
| **文件或目录路径** | 从扫描中排除的文件或目录的完整路径。 |
| **文件哈希** | 要从扫描中排除的文件的哈希值。 |
| **注释** | 扫描排除项的注释。 |

默认情况下，排除项表为空。您可以在表中添加、编辑或删除项目。

## 漏洞利用防御排除窗口

在此窗口中，您可以添加或配置漏洞利用防御扫描的排除对象。

漏洞利用防御排除设置

| 设置 | 描述 |
| --- | --- |
| **使用威胁名称** | 此复选框用于启用或禁用按对象中检测到的威胁名称排除扫描。<br>默认情况下已选定该选框。 |
| **威胁名称。** | 在此字段中，您可以输入对象中检测到的威胁名称。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。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。<br>如果选中了"**使用威胁名称**"复选框，则该字段可用。 |
| **使用文件哈希** | 此复选框用于启用或禁用按文件哈希值排除扫描。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| 文件哈希值和类型 | 在此下拉列表中，您可以选择要用于排除文件扫描的文件哈希值类型：<br>• MD5<br>• SHA256<br>如果选中**使用文件哈希**复选框，则此下拉列表可用。 |
| **文件哈希和** | 在此字段中，您可以输入要从扫描中排除的文件的哈希值。<br>如果选中**使用文件哈希**复选框，则此字段可用。 |
| **使用文件或目录路径** | 此复选框用于启用或禁用按照路径排除检测到威胁的文件。<br>默认情况下已选定该选框。 |
| **文件或目录路径** | 用于指定要从扫描中排除的文件或者目录路径的输入字段。路径中可以使用 * 和 ? 字符。<br>如果选中了**使用文件或目录路径**复选框，则该字段可用。 |
| **注释** | 注释的输入字段（可选）。 |
| **使用该排除项** | 该复选框可启用或禁用在应用程序运行时使用此排除项。<br>默认情况下已选定该选框。 |

# 反加密

在管理控制台中，您可以在策略属性（**高级威胁防护 → 反加密勒索**）中管理反加密勒索设置。

反加密组件设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>默认情况下已清空该复选框。 |
| **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 | 描述 |
| --- | --- |
| **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。

## “新建扫描范围”窗口

在此窗口中，您可以添加或配置反加密勒索组件的保护范围。

保护范围设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 该设置块可让您设置扫描范围。<br>您可以在文件系统下拉列表中选择文件系统类型：<br>• “**本地**”，表示本地目录。<br>• **共享**显示可通过 Samba 或 NFS 协议访问的服务器文件系统资源。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **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。<br>该字段不能为空。 |
| **掩码** | 该列表包含应用程序在反加密勒索组件工作期间扫描的对象的名称掩码。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

## “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：<br>• **通知**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。<br>• **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，您可以指定不受信任主机阻止持续时间（以分钟为单位）。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。<br>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。<br>可能的值：从 1 到 2147483647 的整数。<br>默认值：30。 |

## “排除范围”窗口

此窗口包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。

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。 |

默认情况下，排除范围表为空。您可以在表中添加、编辑和删除项目。

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。

## “新排除范围”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。<br>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。<br>如果选中此复选框，则应用程序在扫描期间将排除此区域。<br>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。<br>默认情况下已选定该选框。 |

| 设置 | 描述 |
| --- | --- |
| **文件系统，访问协议和路径** | 该设置块可让您设置排除范围。<br>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：<br>• **本地** 用于本地目录。<br>• **挂载** 用于已挂载的目录。<br>• **全部远程挂载** 用于使用 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了 **挂载**，则可以在右侧的下拉列表中选择远程访问协议：<br>• **NFS** 用于使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba** 用于使用 Samba 协议挂载到设备上的远程目录。<br>• **自定义** 用于在下面字段中指定的设备文件系统资源。 |
| | 如果在文件系统下拉列表中选择了 **本地**，则可以在输入字段中输入要添加到排除范围的目录路径。您可以使用掩码和标签指定路径。<br>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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

### 如何使用标签

您可以使用特殊标签来指定容器或镜像：

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

其中：

`<id>` 是容器 ID。

`<name>` 是容器名称

`<path to local directory>` 是本地目录的路径。

您还可以使用唯一的标签组合：`[container-id:<id>]`、`[container-name:<name>]`、`[image-id:<id>]` 和 `[image-name:<name>]/path to local directory>`。

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:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。

### “按掩码筛选的排除项”窗口

您可以按名称掩码配置对象的扫描排除项。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“**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）。

您可以启用合并子策略继承时的排除列表。如果要合并列表项，请选中**合并继承的值**复选框。如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。如果清除此复选框，则继承策略设置时不会合并列表项。默认情况下已清空该复选框。

## 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 Kaspersky Endpoint Security 对卡巴斯基安全网络的使用。

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。<br>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** | 在 *云模式*下，Kaspersky Endpoint Security 使用轻量版反病毒数据库，这会使计算机 RAM 的负载大约减半。<br>如果启用了 KSN，则该复选框可用。<br>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。<br>在下次应用程序数据库更新后，将启用或禁用该模式。<br>只有在标准模式下使用应用程序时，该设置才适用。 |
| **使用管理服务器作为 KSN 代理服务器** | 如果选中此复选框，Kaspersky Endpoint Security 将使用管理服务器上的 KSN 代理服务与 KSN 服务器进行通信。<br>默认情况下已选定该选框。<br>只有在标准模式下使用应用程序时，该设置才适用。在 Light Agent 模式下，应用程序只能通过 KSN 代理服务器与 KSN 基础设施进行通信。 |
| **KSN 代理不可用时使用 KSN 服务器** | 如果选中此复选框，当 KSN 代理服务不可用时，Kaspersky Endpoint Security 会直接与 KSN 服务器通信。<br>默认情况下已选定该选框。<br>如果选中了"**使用管理服务器作为 KSN 代理服务器**"复选框，则此复选框可用。<br>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 | 描述 |
| --- | --- |
| **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。<br>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。<br>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。 |

## 卡巴斯基私人安全网络声明

在此窗口中，您可以阅读卡巴斯基私人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 | 描述 |
| --- | --- |
| **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人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。 |

# BadUSB 攻击防护

在管理控制台中，您可以在策略属性（**基本威胁防护** → **BadUSB 攻击防护**）中管理 Web 威胁防护设置。

BadUSB 攻击防护组件设置

| 设置 | 描述 |
| --- | --- |
| **启用 BadUSB 攻击防护** | 此复选框启用或禁用 BadUSB 攻击防护组件。<br>默认禁用此组件。 |
| **最大 USB 设备授权尝试次数** | 如果授权码输入错误达到指定次数，则自动锁定 USB 设备。有效值为 1 到 10。例如，如果允许 5 次尝试输入授权码，则在第五次尝试失败后，应用程序将阻止 USB 设备。Kaspersky Endpoint Security会显示 USB 设备被阻止的时间。此时间过后，您还可以再尝试 5 次输入授权代码。 |
| **达到最大授权尝试次数时的阻止持续时间(分钟)** | 在指定次数的授权码输入失败后，USB 设备将被阻止。可能的值：1 到 180（分钟） |
| **授权 USB 设备时不允许使用屏幕键盘** | 如果此切换按钮被打开，应用程序将阻止使用屏幕键盘认证无法输入认证码的 USB 设备。 |
| **禁止使用条形码授权 USB 设备** | 如果启用此拨动开关，则应用程序不允许使用条形码对无法用于输入授权码的 USB 设备进行授权。 |

# 通信和 Web 保护

## 邮件威胁防护

在管理控制台中，您可以在策略属性（**基本威胁防护** → **邮件威胁防护**）中管理 Web 威胁防护设置。

邮件威胁防护组件设置

| 设置 | 描述 |
| --- | --- |
| **邮件威胁防护** | 此复选框用于启用或禁用邮件威胁防护。<br>此组件默认启用。 |
| **配置 (保护设置)** | 单击此按钮将打开**邮件威胁防护设置**窗口，您可以在其中配置邮件威胁防护范围和复合文件的扫描设置。 |
| **配置 (附件过滤器)** | 单击此按钮将打开**附件过滤器**窗口，您可以在其中配置电子邮件附件的过滤。 |
| **使用启发式分析器**<br>**启发式分析级别** | 该复选框可启用或禁用启发式分析器。<br>扫描文件查找恶意代码时，启发式分析器会执行可执行文件中的指令。启发式分析器执行的指令数量取决于指定的启发式分析级别。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启发式分析持续时间之间建立平衡。<br>默认情况下，启发式分析器已启用，并选择了中等启发式分析级别。 |
| **针对威胁检测的操作** | 当在电子邮件中检测到威胁时，邮件威胁防护将执行以下操作：<br>• "**清除；无法清除则删除**"。当在传入邮件中检测到感染对象时，应用程序会尝试清除该对象。然后带有安全附件的邮件将被提供给用户。如果清除失败，应用程序会删除感染对象。应用程序会在邮件主题中添加关于已执行操作的信息，例如*[邮件已处理] <邮件主题>*。默认情况下已选择此操作。<br>• "**清除；清除失败则阻止**"。当在传入邮件中检测到感染对象时，应用程序会尝试清除该对象。然后带有安全附件的邮件将被提供给用户。如果清除失败，应用程序会在邮件主题中添加警告信息。然后，带有原始附件的邮件将被提供给用户。<br>• "**阻止**"。如果在传入邮件中检测到感染对象，应用程序会在邮件主题中添加警告。然后，带有原始附件的邮件将被提供给用户。<br>此设置不适用于传出邮件。如果在发送的消息中检测到感染对象，应用程序将阻止该消息的发送。 |

## 邮件威胁防护设置窗口

在此窗口中，您可以配置邮件威胁防护范围和复合文件扫描设置。

邮件威胁防护设置

| 设置 | 描述 |
| --- | --- |
| **保护范围** | *保护范围*指定组件必须扫描的对象：接收和发送邮件，还是仅接收邮件。<br>默认**传入和传出邮件**选项处于选中状态。 |
| **扫描存档附件** | 启用或禁用对压缩文件附件的扫描。<br>这包括扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他类型的压缩文件。应用程序不仅可通过扩展名识别文件，还可通过格式识别文件。在扫描压缩文件时，应用程序会递归解包。这样就可以检测嵌套压缩文件（压缩文件中的压缩文件）中的威胁。<br>默认情况下已选定该选框。 |
| **扫描附带的 Office 应用程序文件** | 启用或禁用扫描 Office 格式的附件。无论是否选中此复选框，应用程序都会扫描小于 1MB 的 Office 格式附件。<br>默认情况下已选定该选框。 |
| **不扫描大于此值的存档(MB)** | 如果选中此复选框，邮件威胁防护将不会扫描任何大于指定限制的压缩文件附件。如果取消选中此复选框，邮件威胁防护将扫描任何大小的压缩文件附件。<br>默认情况下已清空该复选框。 |
| **限制存档扫描持续时间为(秒)** | 如果选中此复选框，则会限制电子邮件附件中压缩文件的扫描持续时间。<br>默认情况下已清空该复选框。 |

## 附件筛选窗口

在此窗口中，您可以配置电子邮件附件筛选。

附件筛选设置

| 设置 | 描述 |
| --- | --- |
| **不应用过滤器** | 如果选择此选项，邮件威胁防护将不会筛选电子邮件附件。 |
| **重命名指定类型的附件** | 如果选择此选项，邮件威胁防护会将指定文件类型的扩展名的最后一个字符替换为下划线字符（例如 attachment.doc_）。因此，用户需要重命名文件才能打开它。<br>默认选中。 |
| **删除指定类型的附件** | 如果选择此选项，邮件威胁防护将从电子邮件中删除指定类型的附件。<br>您可以在文件掩码列表中指定要从电子邮件中重命名或删除的附件类型。 |
| **合并继承的值** | 此复选框可启用或禁用在子策略中继承时合并列表。<br>如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。<br>如果清除该复选框，则继承策略设置时不会合并列表项。<br>默认情况下已清空该复选框。 |
| **附件类型表** | 此表列出了要从电子邮件中重命名或删除的附件类型。<br>您可以使用相应按钮添加、编辑或删除附件类型。 |

# Web 威胁防护

在管理控制台中，您可以在策略属性（**基本威胁防护** → **Web 威胁防护**）中配置 Web 威胁防护设置。

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。<br>默认情况下已清空该复选框。 |
| **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。 |
| **检测到威胁后的操作** | 应用程序对在其中检测到危险对象的 Web 资源执行的操作：<br>• **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）。<br>• 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。您可以在列表中添加、编辑和删除网址。

实用文章

### 如何指定掩码

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 | 描述 |
| --- | --- |
| **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。<br>默认情况下已选定该选框。 |
| **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。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>默认情况下已清空该复选框。 |
| **检测入侵者可以用来破坏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。<br>默认情况下已清空该复选框。 |

# 网络威胁防护

在管理控制台中，您可以在策略属性（**基本威胁防护 → 网络威胁防护**）中管理“网络威胁防护”设置。

网络威胁防护组件设置

| 设置 | 描述 |
| --- | --- |
| **启用网络威胁防护** | 此复选框启用或禁用网络威胁防护。<br>默认情况下已清空该复选框。 |
| **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。<br>• **通知**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。<br>• **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。<br>默认情况下已选定该选框。 |
| **阻止攻击设备的时间（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。<br>可能的值：从 1 到 32768 的整数。<br>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。您可以指定 IPv4 和 IPv6 版本的 IP 地址。

# 防火墙管理

在管理控制台中，您可以在策略属性（**基本威胁防护 → 防火墙管理**）中配置防火墙管理设置。

防火墙管理设置

| 设置 | 描述 |
| --- | --- |
| **启用防火墙管理** | 此复选框用于启用或禁用防火墙管理。<br>默认情况下已清空该复选框。 |
| **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：<br>• **允许**网络连接（默认值）。<br>• **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：<br>• **允许**传入的数据包（默认值）。<br>• **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代理端口的自动添加允许规则。<br>默认情况下已选定该选框。 |

## “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 | 描述 |
| --- | --- |
| 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。<br>如果值为 **Yes**，应用程序将记录网络数据包规则的操作。<br>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。

## “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 | 描述 |
| --- | --- |
| **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：<br>• **任何**（默认值）<br>• GRE<br>• ICMP<br>• ICMPv6<br>• IGMP<br>• TCP<br>• UDP |
| Direction | 您可以指定被监控的网络活动的方向：<br>• **传入数据包**。如果选择此选项，防火墙管理组件将仅监控传入数据包。<br>• **传入**。如果选择此选项，防火墙管理组件将仅监控传入连接。<br>• **传入/传出**（默认设置）。如果选择此选项，防火墙管理组件将监控传入和传出连接。<br>• **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。<br>• **传出数据包**。如果选择此选项，防火墙管理组件将仅监控传出数据包。<br>• **传出**。如果选择此选项，防火墙管理组件将仅监控传出连接。 |
| 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。<br>如果选择了**指定的**选项，则将显示用于输入 ICMP 类型的字段。<br>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、代码在**ICMP 代码**字段中指定的类型的消息。<br>如果选择了**指定的**选项，则将显示用于输入 ICMP 代码的字段。<br>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或者端口范围。<br>如果选择了**指定的**选项，则将显示用于输入端口号的字段。<br>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或者端口范围。<br>如果选择了**指定的**选项，则将显示用于输入端口号的字段。<br>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：<br>• **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。<br>• **指定的地址或地址范围**。如果选择此选项，则网络规则将控制具有在下面表格中指定的 IP 地址的远程设备的网络数据包发送和接收。单击表格上方的**添加**按钮将打开**添加 IP 地址**窗口，您可以在其中指定设备的 IP 地址、网络地址或 IP 地址范围。<br>• **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：<br>• **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。<br>• **指定的地址或地址范围**。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表格中指定。单击表格上方的**添加**按钮将打开**添加 IP 地址**窗口，您可以在其中指定设备的 IP 地址、网络地址或 IP 地址范围。 |
| **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：<br>• **阻止**网络活动。<br>• **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。 |

## 添加 IP 地址窗口

在此窗口中，您可以指定设备的 IP 地址、网络地址或 IP 地址范围。

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。

### “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 | 描述 |
| --- | --- |
| **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。

### “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 | 描述 |
| --- | --- |
| **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：<br>• **公用**<br>• **本地**<br>• **受信任** |

# 安全控制

## 设备控制

在管理控制台中，您可以在策略属性（**安全控制** → **设备控制**）中管理设备控制设置。

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。<br>默认情况下已选定该选框。 |
| **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，您可以将设备添加到受信任设备列表中。 |
| **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：<br>• **通知**。如果选择此选项，Kaspersky Endpoint Security 将测试选定的访问模式，并为检测到的设备访问尝试生成事件。<br>• **阻止**（默认值）。如果选择此选项，Kaspersky Endpoint Security 将应用为设备或总线设置的访问模式。 |
| **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。 |
| **允许请求临时访问权限** | 如果选中此复选框，用户可以在应用程序的图形界面或命令行中请求临时访问被阻止的设备。 |
| **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。 |

## “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 | 描述 |
| --- | --- |
| **设备 ID** | 受信任设备的 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** | 受信任设备连接到的客户端设备的名称。 |
| **用户或组名称** | 受信任设备的用户或用户组名称。 |
| **注释** | 与受信任设备相关的注释。 |

您可以使用**添加**按钮将设备添加到受信任设备列表，具体操作如下：

- 指定设备 ID 或设备 ID 掩码（**添加→ 按 ID 或掩码添加设备**）。
- 从受管理设备上检测到的设备列表中选择所需设备（**添加→ 从在主机上检测到的设备列表中选择设备**）。
- 从Kaspersky Security Center 的设备控制事件中检测到的设备列表中选择所需设备（**添加 → 基于事件添加设备**）。

您可以在表中编辑和删除受信任设备。

您还可以通过单击**高级 → 导出所选**或**高级 → 导出全部**按钮将已添加的设备列表导出到文件，通过单击**高级 → 导入**按钮从 JSON 文件导入设备列表。

有三种导入模式：

- **与现有列表结合**以在导入时合并受信任设备列表。如果文件中已存在此设备 ID 的条目，则会更新现有条目的设置。对于之前不在列表中的设备，将添加条目。
- **添加到现有列表**以在导入时将设备添加到受信任设备列表中。仅将之前不在设备列表中的设备条目添加到列表中。
- **替换现有列表**以替换受信任设备列表。现有受信任设备列表将被文件中的列表替换。

## “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 | 描述 |
| --- | --- |
| **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。<br>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。 |

| 设置 | 描述 |
| --- | --- |
| **找到的设备** | 该表包含以下列：<br>• **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）。<br>• **设备 ID** – 所找到设备的 ID。<br>• **设备名称** — 所找到设备的名称。<br>• **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）。 |
| **允许以下用户和/或用户组访问** | 此字段显示受信任设备的用户和/或用户组的名称。默认值为"**\Everyone**"（所有用户）。 |
| **配置** | 单击此按钮将打开"**访问受信任设备**"窗口。 |

## 客户端设备上的设备窗口

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。

仅当已创建活动策略并且已执行与网络代理的同步时，才可获得关于现有设备的信息（同步间隔在网络代理策略中指定；默认为 15 分钟）。

如果您新创建了不活动的策略，则列表为空。

从受管理客户端设备上检测到的设备列表中添加设备

| 设置 | 描述 |
| --- | --- |
| **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，应用程序将搜索具有指定参数的设备。搜索结果显示在下表中。 |
| 检测到的设备列表 | 该表包含以下列：<br>• **主机名称** – 所找到设备连接的客户端设备的名称。<br>• **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）。<br>• **设备名称** — 所找到设备的名称。<br>• **设备 ID** – 所找到设备的 ID。 |

## 基于设备控制事件窗口的设备列表

在此窗口中，您可以创建在 Kaspersky Security Center 的设备控制事件中检测到的设备列表。然后您可以将此列表中的设备添加到受信任设备列表中。

您可以选择一个或多个设备添加到受受信任设备列表中。

如果启用了设备控制、存在活动策略、并且已与网络代理执行同步（同步按网络代理策略中指定的频率执行；默认每 15 分钟一次），则可以获取关于设备的信息。

如果您新创建了不活动的策略，则列表为空。

从 Kaspersky Security Center 事件中检测到的设备列表中添加设备

| 设置 | 描述 |
| --- | --- |
| **事件类型** | 您可以使用复选框选择发送到 Kaspersky Security Center 的设备控制事件类型。列表包含在指定类型事件中检测到的设备。<br>默认选择所有复选框。 |
| **管理组** | 此字段用于输入管理组的名称，管理组包含检测到的设备连接的客户端设备。列表中仅包含已连接到指定管理组中的客户端设备的设备。<br>您可以指定部分组名称。<br>默认情况下，列表包含连接到任何管理组中的客户端设备的设备。 |
| **事件时间段** | 在下拉列表中，您可以选择事件发生的时间段。列表包含在指定时间段内发送到 Kaspersky Security Center 的事件中检测到的设备。<br>默认情况下，列表包含过去一个月内事件中检测到的设备。 |
| **搜索设备** | 单击此按钮后，应用程序将搜索具有指定参数的设备。搜索结果显示在下表中。 |
| **找到的设备** | 该表包含以下列：<br>• **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）。<br>• **设备 ID** – 所找到设备的 ID。<br>• **设备名称** — 所找到设备的名称。<br>• **主机名称** – 所找到设备连接的客户端设备的名称。<br>• **连接日期**是被发现设备所连接的日期。<br>• **管理组**是管理组的名称，管理组包含检测到的设备所连接的客户端设备。 |
| **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）。 |
| **允许以下用户和/或用户组访问** | 此字段显示受信任设备的用户和/或用户组的名称。默认值为"**\Everyone**"（所有用户）。 |
| **配置** | 单击此按钮将打开"**访问受信任设备**"窗口。 |

## 访问受信任设备窗口

在此窗口中，您可以配置用户或用户组对选定的受信任设备的访问权限。

对受信任设备的访问

| 设置 | 描述 |
| --- | --- |
| **用户和/或用户组** | 您想要使所添加设备受信任的用户和组的列表。<br>默认情况下，该表包含 **\Everyone** 项目（所有用户）。<br>您可以添加、编辑或删除用户或用户组。 |

## "用户或组"窗口

在此窗口中，可以指定要为其使设备受信任的用户或用户组。

受信任设备窗口

| 设置 | 描述 |
| --- | --- |
| **类型** | 您想要使设备受信任的**用户**或**组**。 |
| **用户或组名称** | 本地用户或域用户的名称（如果系统允许以这种格式输入用户名，则无需指定带有域的完整名称，或者采用 <域名>\<用户名> 或 <用户名>@<域名>）格式，或者是想要使设备受信任的用户组的名称。 |

## "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 | 描述 |
| --- | --- |
| **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项之一：<br>• **允许**：允许访问所选类型的设备。<br>• **阻止**：禁止访问选定类型的设备。<br>• **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。<br>• **按规则**：根据访问规则和计划，允许或阻止对设备的访问。此菜单命令仅适用于存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）。<br>• **只读**：允许对所选类型的设备进行只读访问。此菜单命令仅适用于存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）。 |

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。<br>默认情况下，该表包含 **\Everyone** 项目（所有用户）。<br>您可以添加、编辑或删除用户或用户组。 |
| **设备访问规则** | 此表包含用户和用户组的访问计划。它由以下列组成：<br>• **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。<br>• **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）。<br>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）。<br>您可以添加、编辑或删除所选用户的访问计划。不能修改或移除**默认**计划。 |

## “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** | 规则所适用的本地用户名或用户组名称。 |

## 访问计划窗口

在此窗口中，您可以配置访问设备的计划。

访问设备的计划

| 设置 | 描述 |
| --- | --- |
| **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）。<br>以绿色突出显示的时间间隔将包含在计划中。<br>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。<br>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：<br>• **FireWire**<br>• **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项之一：<br>• **允许**（默认）：允许通过此总线访问连接的设备。<br>• **阻止**：拒绝访问使用此连接总线连接的设备。 |

# Web 控制

在管理控制台中，您可以在策略属性（**安全控制** → **Web 控制**）中管理 Web 控制设置。

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。<br>默认情况下已清空该复选框。 |
| **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。<br>该表包含以下列：<br>• **状态**。Web 资源访问规则的状态：<br>  • *已启用* – 该规则已启用，Web 控制在操作期间应用此规则。<br>  • *已禁用* – 该规则已禁用，Web 控制在运行期间不会使用此规则。<br>  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。<br>• **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。<br>• **Name**。Web资源访问规则名称。<br>您可以在表中添加、编辑、删除、上移和下移项目。<br>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：<br>• **Allow**（默认值）– 允许访问 Web 资源。<br>• **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。

| 设置 | 描述 |
| --- | --- |
| **规则名称** | 用于输入 Web 资源访问规则名称的字段。规则名称必须唯一。 |
| **使用此规则** | 该复选框可启用或禁用在应用程序运行时使用规则。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **过滤内容** | 在下拉列表中，您可以选择 Web 资源的内容筛选器：<br>• **不扫描**（默认值）。如果选择此项，则不使用任何 Web 资源内容筛选。<br>• **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**内容类别选择**窗口。<br>• **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**数据类型类别选择**窗口。<br>• **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。 |
| **过滤器地址** | 在下拉列表中，您可以选择 Web 资源地址的筛选器：<br>• **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。<br>• **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：<br>• **所有用户**（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。<br>• **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**选择用户**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：<br>• **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。<br>• **<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。<br>• **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：<br>• **Allow**（默认值）– 允许访问 Web 资源。<br>• **阻止** – 阻止对 Web 资源的访问并显示访问被阻止的消息。<br>• **通知** – 显示一条警告，提示该 Web 资源不受欢迎。通过单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。

选中所有嵌套内容类别的复选框不会自动选中父内容类别的复选框。

## 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、编辑或删除项目。

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**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、编辑或删除项目

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 | 描述 |
| --- | --- |
| **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）。<br>以绿色突出显示的时间间隔将包含在计划中。<br>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。<br>默认情况下，所有间隔 (24/7) 都包含在计划中。 |

# 应用程序控制

在管理控制台中，您可以在策略属性（**安全控制 → 应用程序控制**）中管理应用程序控制设置。

应用程序控制组件设置

| 设置 | 描述 |
| --- | --- |
| **启用应用程序控制** | 该复选框将启用应用程序控制组件。<br>默认情况下已清空该复选框。 |
| **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：<br>• **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。<br>• **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：<br>• **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。<br>• **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：<br>• **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。<br>• **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配置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 | 描述 |
| --- | --- |
| **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：<br>• *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。<br>• *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。<br>• *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。<br>您可以在**添加新规则**窗口中更改规则状态。 |

您可以添加、修改或删除应用程序控制规则。

## “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 | 描述 |
| --- | --- |
| **描述** | 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：<br>• *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。<br>• *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。<br>• *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：<br>• **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。<br>• **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。<br>您可以添加、编辑或删除用户或用户组。 |

## "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 | 描述 |
| --- | --- |
| **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。<br>有关创建类别的详细信息，请参阅"Kaspersky Security Center 帮助"。 |
| **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。无法编辑"**黄金镜像（本地）**"类别。 |

## "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。 |

## 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设置来管理扫描设置。

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 |
| --- | --- |
| **任务完成后，对“黄金镜像”类别执行的操作** | 在下拉列表中，您可以选择 Kaspersky Endpoint Security 在“清查”任务完成后必须对“黄金镜像”应用程序类别执行的操作：<br>• **无更改** — 完成清查后，不更改“黄金镜像”应用程序类别。这是默认值。<br>• **更新或创建（如果不存在）** — 将“清查”任务在设备上发现的应用程序添加到“黄金镜像”类别。如果该类别不存在，则创建该类别。如果该类别已存在，则更新该类别的应用程序列表。<br>• **删除** — 清空“黄金镜像”应用程序类别。任务启动后会立即清除此类别，而不会对设备上的文件进行清查。<br>您可以在应用程序控制规则中使用“黄金镜像”类别。 |
| **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。<br>默认情况下已选定该选框。 |
| **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 的文件）。<br>默认情况下已选定该选框。 |
| **扫描脚本** | 此复选框启用或禁用脚本扫描。<br>默认情况下已选定该选框。 |
| **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“**排除项**”部分，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 | 描述 |
| --- | --- |
| **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。

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范围。

清查范围设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

### 如何指定掩码

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。

## “排除项”部分

扫描排除项设置

| 设置组 | 描述 |
| --- | --- |
| **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

此窗口包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。

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。 |

默认情况下，排除范围表为空。您可以在表中添加、编辑和删除项目。

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。

## “新排除范围”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。<br>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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。 |
| **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。<br>您可以添加、编辑或删除掩码。 |

实用文章

**如何指定掩码**

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。

# 系统完整性监控

在管理控制台中，您可以在策略属性（**安全控制** → **系统完整性监控**）中配置系统完整性监控设置。

系统完整性监控设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>默认情况下已清空该复选框。 |
| **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 | 描述 |
| --- | --- |
| **合并继承的值** | 此复选框可启用或禁用在子策略中继承时合并列表。<br>如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。<br>如果清除该复选框，则继承策略设置时不会合并列表项。<br>默认情况下已清空该复选框。 |
| **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。

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。

## “新建扫描范围”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 | 描述 |
| --- | --- |
| **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。<br>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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

## “排除范围”窗口

该窗口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。

监控排除范围设置

| 设置 | 描述 |
| --- | --- |
| **合并继承的值** | 此复选框可启用或禁用在子策略中继承时合并列表。<br>如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。<br>如果清除该复选框，则继承策略设置时不会合并列表项。<br>默认情况下已清空该复选框。 |
| **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。 |

默认情况下，排除范围表为空。您可以在表中添加、编辑或删除项目。

您还可以点击“**导入**”从文件中导入排除范围列表，或点击“**导出**”将排除范围列表以 JSON 格式导出到文件。导入时，系统将提示您替换排除范围列表或将排除范围添加到现有列表。

## “新排除范围”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项。

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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。该字段不能为空。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。<br>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 排除在监控范围之外的文件的名称模板。<br>例如：<br>`*.txt` 掩码表示所有文本文件。<br>`*_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“**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 排除在监控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）。

您还可以使用 **导入** 按钮从文件中导入排除列表，并使用 **导出** 按钮将排除列表导出到 JSON 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。

您可以启用合并子策略继承时的排除列表。如果要合并列表项，请选中**合并继承的值**复选框。如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。如果清除此复选框，则继承策略设置时不会合并列表项。默认情况下已清空该复选框。

## 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。

您可以创建并运行自定义系统完整性检查任务。您可以通过编辑任务设置来管理扫描设置。

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建系统基线。<br>默认情况下已清空该复选框。 |
| **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。<br>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）。<br>默认情况下已清空该复选框。 |
| **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。<br>默认情况下已清空该复选框。 |
| **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检查运行时跟踪文件访问时间。<br>默认情况下已清空该复选框。 |
| **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**部分中，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 | 描述 |
| --- | --- |
| **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。

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范围。

监控范围设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>该字段不能为空。<br>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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。 |

实用文章

### 如何指定掩码

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。

## “排除项”部分

扫描排除项设置

| 设置组 | 描述 |
| --- | --- |
| **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”组件的扫描排除范围。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。

“系统完整性检查”任务的扫描排除范围设置

| 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、编辑或删除项目。

## “新排除范围”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项。

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。<br>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。<br>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。<br>默认情况下已选定该选框。 |
| **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。<br>该字段不能为空。<br>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。 |

| 设置 | 描述 |
| --- | --- |
| **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。<br>默认情况下，该列表包含 * 掩码（所有对象）。<br>您可以添加、编辑或删除掩码。<br>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。<br>例如：<br>`*.txt` 掩码表示所有文本文件。<br>`*_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）。 |

实用文章

### 如何指定掩码

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。

## “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“**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）。

# 本地任务

## 任务管理

在管理控制台中，您可以在策略属性（**本地任务 → 任务管理**）中设置查看和管理任务的权限。

任务管理设置

| 设置 | 描述 |
| --- | --- |
| **允许本地任务** | 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。<br>如果选中此复选框，用户可以在应用程序的图形界面和命令行中配置和运行任务。<br>如果清除此复选框，则不使用本地任务。计划的本地任务不会运行。无法在应用程序的图形界面或命令行中运行或配置任务。<br>默认情况下已清空该复选框。 |
| **允许查看和管理通过 KSC 创建的任务** | 此复选框用于允许或禁止用户查看在 Kaspersky Security Center 中创建的本地任务，以及在客户端设备上管理这些任务。<br>如果选中此复选框，则在 Kaspersky Security Center 中创建的任务将显示在应用程序的图形界面中。用户可以通过应用程序的图形界面和命令行启动和停止这些任务。<br>如果清除此复选框，则无法在应用程序的图形界面中或通过命令行来查看或管理在 Kaspersky Security Center 中创建的任务。<br>默认情况下已清空该复选框。 |

# 防御高级威胁和定向攻击

## 与 Kaspersky Managed Detection and Response 整合

在管理控制台中，您可以在策略属性（**Detection and Response → Managed Detection and Response**）中启用或禁用 MDR 组件并上传 MDR BLOB 文件。

MDR 整合设置

| 设置 | 描述 |
| --- | --- |
| **启用 Managed Detection and Response** | 此复选框用于启用或禁用 MDR 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。<br>默认禁用此组件。<br>如果您启用 MDR 组件并且卡巴斯基安全网络被禁用或在标准模式下使用，系统将提示您接受卡巴斯基安全网络声明以在扩展模式下启用卡巴斯基安全网络。<br>如果父策略禁止更改 KSN 设置，则会显示错误消息，并且不会启用 MDR 组件。 |
| **上传** | 点击此按钮将打开一个标准的 Microsoft Windows 窗口，您可以在其中选择要上传的 MDR BLOB 文件。<br>如果您有租户，或者已使用 MDR BLOB 文件激活 MDR 组件，则必须执行此操作。 |

BLOB 文件位于 Kaspersky Managed Detection and Response 分发包所含的 MDR 配置文件（ZIP 压缩文件格式）中。

上传 BLOB 文件，即表示您同意在安装 Kaspersky Endpoint Security 的设备中，数据将自动发送到卡巴斯基进行处理。如果您不同意处理传输的数据，请勿上传该文件。有关所传输数据的详细说明，请参阅“Kaspersky Managed Detection and Response 帮助”部分。

# 卡巴斯基 Endpoint Detection and Response (on-premises) 集成

在管理控制台中，您可以启用或禁用 EDR Expert (on-premises) 组件，并在策略属性（**检测和响应 → EDR Expert (on-premises)**）中管理 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response (KATA) 组件集成的设置。

如果在 Web Console 中为 EDR Expert (on-premises) 组件选择了 **Endpoint Detection and Response Expert（版本 8.0 及更高版本）**，即选择了 EDR Expert (on-premises) 集成模式，则管理控制台会显示警告，并且 Kaspersky Endpoint Detection and Response (KATA) 集成的设置不可用。您可以在 Web Console 中更改集成模式。

卡巴斯基 Endpoint Detection and Response (on-premises) 集成设置

| 设置 | 描述 |
| --- | --- |
| **Enable Endpoint Detection and Response Expert (on-premises)** | 此复选框可启用或禁用 EDR Expert (on-premises) 组件，该组件提供与 Kaspersky Endpoint Detection and Response (KATA) 的集成。<br>默认禁用此组件。 |
| **启用对象的执行防护** | 此复选框可启用或禁用用于 对象执行防护 的 EDR Expert (on-premises) 规则。 |
| **KATA 服务器** | **配置**按钮会打开一个窗口，您可以在其中配置与 KATA 服务器的连接，以及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数据到 KATA 服务器的设置。 |

## 配置 KATA 服务器连接

该表格列出了 KATA 服务器的连接设置。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

服务器连接设置

| 设置 | 描述 |
| --- | --- |
| **地址** | 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)。<br>为确保在设备上启用网络隔离的情况下应用程序发生故障时与服务器的通信不会中断，我们建议指定服务器的 IP 地址。<br>默认值：`127.0.0.1`。 |
| **端口** | 用于连接到 KATA 服务器的端口。<br>默认值：`443`。 |

## 管理 KATA 服务器连接常规设置

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）。<br>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）。<br>默认值：`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）。<br>默认值：`10`。 |
| **允许发送遥测数据** | 此复选框可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。<br>默认启用发送遥测数据。 |
| **服务器证书** | 该部分包含用于添加或删除服务器证书的按钮：<br>• **添加**会打开一个窗口，您可以在其中添加服务器证书。如果尚未添加服务器证书，则会显示该按钮。<br>在证书添加窗口中，您可以通过以下方式之一添加 KATA 服务器证书：<br>  • 在**从文件添加**字段中，指定包含 DER 或 PEM 格式证书的证书文件的路径。"**浏览**"按钮将打开标准文件选择窗口。<br>  • 将证书文件的内容复制到"**输入证书详情**"字段中。<br>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。<br>• **删除**会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** | 本节包含使用双向身份验证配置连接的额外安全性的控制：<br>• **使用双向身份验证**可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。要使用双向身份验证，您需要添加客户端证书。<br>必须在 KATA 服务器端启用双向身份验证。<br>• **添加**可打开"添加客户端证书"窗口，以提高与 KATA 服务器的连接的安全性。如果选中**使用双向身份验证**复选框并且尚未添加客户端证书，则会显示此按钮。<br>要添加客户端证书，请在证书添加窗口中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。接下来，在 **加密容器密码** 字段中输入客户端证书密码。<br>此字段为必填字段。如果您尝试在未输入密码的情况下保存设置，则会显示错误消息。<br>如果密码正确，**确定** 按钮将变为活动状态。您可以保存设置。<br>• **删除**会删除之前添加的客户端证书。该按钮仅在已添加客户端证书的情况下才会显示。 |

# 配置数据传输到 KATA 服务器

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）。<br>默认值：`30`。 |
| **启用事件限制** | 启用或禁用调节发送到 KATA 服务器的事件数量。 |
| **每小时的最大事件数量** | 每小时的最大事件数量<br>默认值：`3000`。 |
| **事件数量超过限制（百分比）** | 事件数量超过限制（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。<br>默认值：`15`。 |

# Kaspersky Network Detection and Response (KATA) 整合

在管理控制台中，您可以启用或禁用 NDR (KATA) 组件，并在策略属性（**Detection and Response → Network Detection and Response (KATA)**）中管理将 Kaspersky Endpoint Security 应用程序与 Kaspersky Network Detection and Response (KATA) 组件集成的设置。

Kaspersky Network Detection and Response (KATA) 集成设置

| 设置 | 描述 |
| --- | --- |
| **启用 Network Detection and Response (KATA)** | 此复选框可启用或禁用 NDR (KATA) 组件。<br>默认禁用此组件。 |
| **NDR 服务器** | **配置**按钮会打开一个窗口，您可以在其中配置与 NDR 服务器的连接，以及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 NDR 服务器的常规设置，添加服务器证书，并配置连接到 NDR 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数据到 NDR 服务器的设置。 |

## 配置 NDR 服务器连接

该表格列出了 NDR 服务器的连接设置。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 NDR 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

服务器连接设置

| 设置 | 描述 |
| --- | --- |
| **地址** | NDR 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)。<br>默认值：`127.0.0.1`。 |
| **端口** | 用于连接到 NDR 服务器的端口。<br>默认值：`443`。 |

## 管理 NDR 服务器连接常规设置

在此窗口中，您可以配置连接到 NDR 服务器的常规设置。

NDR 服务器连接设置

| 设置 | 描述 |
| --- | --- |
| **发送同步请求到 NDR 服务器的间隔（分钟）** | 发送同步请求到 NDR 服务器的间隔（以分钟为单位）。<br>默认值：`5`。 |
| **等候服务器连接的最长时间（秒）** | 等待与 NDR 服务器连接的最长时间（以秒为单位）。<br>默认值：`10`。 |

| 设置 | 描述 |
| --- | --- |
| **等候服务器响应的最长时间(秒)** | 等待 NDR 服务器响应的最长时间（以秒为单位）。<br>默认值：`10`。 |
| **服务器证书** | 该部分包含用于添加或删除服务器证书的按钮：<br>• **添加**会打开一个窗口，您可以在其中添加服务器证书。如果尚未添加服务器证书，则会显示该按钮。<br>在证书添加窗口中，您可以通过以下方式之一添加 NDR 服务器证书：<br>  • 在**从文件添加**字段中，指定包含 DER 或 PEM 格式证书的证书文件的路径。"**浏览**"按钮将打开标准文件选择窗口。<br>  • 将证书文件的内容复制到"**输入证书详情**"字段中。<br>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。<br>• **删除**会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** | 本节包含使用双向身份验证配置连接的额外安全性的控制：<br>• **使用双向身份验证**可启用或禁用双向身份验证以进一步保护与 NDR 服务器的连接。要使用双向身份验证，您需要添加客户端证书。<br>必须在 NDR 服务器端启用双向身份验证。<br>• **添加**可打开"添加客户端证书"窗口，以提高与 NDR 服务器的连接的安全性。如果选中**使用双向身份验证**复选框并且尚未添加客户端证书，则会显示此按钮。<br>要添加客户端证书，请在证书添加窗口中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。接下来，在 **加密容器密码** 字段中输入客户端证书密码。<br>此字段为必填字段。如果您尝试在未输入密码的情况下保存设置，则会显示错误消息。<br>如果密码正确，**确定** 按钮将变为活动状态。您可以保存设置。<br>• **删除**会删除之前添加的客户端证书。该按钮仅在已添加客户端证书的情况下才会显示。 |

## 配置数据传输到 NDR 服务器

在此窗口中，您可以配置将数据发送到 NDR 服务器的设置。

将数据发送到 NDR 服务器的设置

| 设置 | 描述 |
| --- | --- |
| **发送事件时的最大延时（秒）** | 向 NDR 服务器发送事件的最大延迟（以秒为单位）。<br>默认值：`30`。 |
| **数据包中的最大事件数量** | 一个数据包中的最大事件数量。<br>默认值：`1024`。 |
| **服务器轮询频率** | 发送同步请求到 NDR 服务器的间隔（以秒钟为单位）。<br>默认值：`450`。 |
| **启用事件限制** | 启用或禁用调节发送到 NDR 服务器的事件数量。 |
| **每小时的最大事件数量** | 每小时的最大事件数量<br>默认值：`3000`。 |
| **事件数量超过限制（百分比）** | 事件数量超过限制（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。<br>默认值：`15`。 |

# 与 KUMA 的整合

在管理控制台中，您可以启用或禁用 Kaspersky Endpoint Security 与 Kaspersky Unified Monitoring and Analysis Platform 的集成，并在策略属性（**KUMA 集成** → **KUMA 集成**）中管理集成设置。

与 Kaspersky Unified Monitoring and Analysis Platform 的整合设置

| 设置 | 描述 |
| --- | --- |
| **启用 KUMA 整合** | 启用或禁用 Kaspersky Endpoint Security 应用程序与 Kaspersky Unified Monitoring and Analysis Platform 解决方案的整合。<br>默认禁用 KUMA 整合。 |
| **使用加密连接** | 该复选框可启用或禁用服务器证书验证，为与 KUMA 服务器的连接提供额外保护。<br>要验证服务器证书，您需要选中此复选框并在 **KUMA 服务器**窗口中添加服务器证书。<br>默认情况下已清空该复选框。 |
| **KUMA 服务器** | "**配置**"按钮将打开"**KUMA 服务器**"窗口。在此窗口中，您可以配置与 KUMA 服务器的连接并查看已配置连接的服务器列表。 |
| **KUMA 服务器连接设置** | 单击"**配置**"按钮将打开"**服务器连接设置**"窗口，您可以在其中配置连接到 KUMA 服务器的常规设置，添加服务器证书，并配置连接到 KUMA 服务器时的双向身份验证。 |
| **发送事件时的最大延时（秒）** | 向 KUMA 服务器发送事件的最大延迟（以秒为单位）。<br>默认值：`30`。 |

## "KUMA 服务器"窗口

窗口中的表格显示用于连接到 KUMA 服务器的设置列表。对于配置了连接的每台服务器，该表指示：

- 服务器的 IP 地址（IPv4 或 IPv6）或完全限定域名 (FQDN)。如果您在 **KUMA 整合设置**窗口中选中了使用加密连接复选框，则必须从购买授权许可时收到的证书中指定服务器的完全限定域名(FQDN) 才能使用 KUMA。
- 用于连接到 KUMA 服务器的端口。
- 用于连接到 KUMA 服务器的协议。

您可以使用表格上方的按钮和菜单执行以下操作：

- 添加 KUMA 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

## "KUMA 服务器"窗口

在此窗口中您可以指定 KUMA 服务器连接设置。

KUMA 服务器连接设置

| 设置 | 描述 |
| --- | --- |
| **地址** | KUMA 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)。如果您在 **KUMA 整合设置**窗口中选中了使用加密连接复选框，则必须从购买授权许可时收到的证书中指定服务器的完全限定域名(FQDN) 才能使用 KUMA。 |
| **端口** | 用于连接到 KUMA 服务器的端口。<br>默认值：`443`。 |
| **协议** | 用于连接 KUMA 服务器的协议：TCP、UDP 或带压缩的 HTTP/HTTPS。<br>选择 UDP 协议时，不支持使用证书提供连接保护，没有有关与 KUMA 服务器连接的事件。<br>默认为 TCP。 |

## “KUMA 服务器连接设置”窗口

在此窗口中，您可以配置连接到 KUMA 服务器的常规设置。

KUMA 服务器连接设置

| 设置 | 描述 |
| --- | --- |
| **等候服务器连接的最长时间（秒）** | 等待与 KUMA 服务器连接的最长时间（以秒为单位）。<br>默认值：5。 |
| **服务器证书** | 该部分包含用于添加或删除服务器证书的按钮。 |
| **添加**（服务器证书） | 打开“添加服务器证书”窗口。<br>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。<br>仅当已添加服务器证书时，才会显示该按钮。 |
| **附加连接保护** | 本节包含使用双向身份验证配置连接的额外安全性的控制。 |
| **使用双向身份验证** | 该复选框可启用或禁用双向身份验证，以对与 KUMA 服务器的连接提供额外保护。<br>要使用双向身份验证，您需要添加客户端证书。<br>必须在 KUMA 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 KUMA 服务器连接的安全性。<br>如果尚未添加客户端证书，则会显示该按钮。<br>如果要为连接配置额外的保护，请在 KUMA 服务器端启用客户端证书验证，并在此窗口中选中“**使用双向身份验证**”复选框。 |
| **删除**（客户端证书） | 删除客户端证书。<br>如果已添加客户端证书，则会显示该按钮。 |

## “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 KUMA 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 KUMA 服务器的连接。

如果要为连接配置额外的保护，请在 KUMA 服务器端启用客户端证书验证，并在 **KUMA 服务器连接设置**窗口中选中“**使用双向身份验证**”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。接下来，在 **加密容器密码** 字段中输入客户端证书密码。

此字段为必填字段。如果您尝试在未输入密码的情况下保存设置，则会显示错误消息。

如果密码正确，**确定** 按钮将变为活动状态。您可以保存设置。

## 隔离

在管理控制台中，您可以在策略属性（**常规设置** → **存储设置**）和受管理设备属性（**受管理设备** → **设备**选项卡 → 设备属性窗口 → **应用程序**区域 → 应用程序属性窗口 → **存储设置**）中管理隔离区设置。

隔离设置

| 设置 | 描述 |
| --- | --- |
| **隔离区大小限制为 (MB):** | 此复选框可启用或禁用将隔离区的最大容量限制为指定值（以兆字节为单位）。如果清除该复选框，则隔离区的大小不受限制。<br>可用值：1-999999。<br>如果应用程序在标准模式或 EDR Agent 模式下使用，则默认值为 200；如果应用程序在 Light Agent 模式下使用，则默认值为 100。 |
| **隔离区已满 (%) 时通知:** | 此复选框可启用或禁用对隔离区已满百分比的限制，达到此百分比会生成有关隔离区已满的事件。如果清除该复选框，则不会生成有关隔离区已满的事件。<br>可用值：1-100。<br>默认值：90。 |

## 对象的执行防护

只有在启用了与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或与 Kaspersky Endpoint Detection and Response (KATA) 的集成后，才能在管理控制台中启用或禁用对象执行防护。

您可以在策略属性（**应用程序设置** → **Detection and Response** → **EDR Expert (on-premises)**）中启用或禁用对象执行防护。

**对象的执行防护** 下的 **启用对象的执行防护** 复选框用于启用或禁用对象执行防护的 EDR Expert (on-premises) 规则。

# 常规设置

在管理控制台中，您可以在策略属性（**常规设置**）中管理用于定义应用程序整体运行以及各项功能运行的常规应用程序设置。

## 代理服务器

在管理控制台中，您可以在策略属性（**常规设置** → **代理服务器设置**）中管理代理服务器设置。

代理服务器设置

| 设置 | 描述 |
| --- | --- |
| **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。 |
| **使用指定的代理服务器设置** | 如果选择此选项，应用程序将使用指定的代理服务器设置连接到卡巴斯基激活服务器、数据库和应用程序模块的更新源、卡巴斯基安全网络，并且在使用Web 威胁防护组件验证网站证书时也会使用这些设置。 |
| **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。<br>默认端口：3128。<br>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。 |
| **使用代理服务器身份验证** | 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。<br>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。<br>默认情况下已清空该复选框。<br>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。<br>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。 |
| **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。<br>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。<br>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。<br>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** | 启用或禁用将 Kaspersky Security Center 管理服务器作为访问卡巴斯基激活服务器的代理服务器。当在没有互联网接入的隔离网段中使用激活码激活应用程序时，必须执行此操作。<br>如果选中此复选框，应用程序将通过能够接入互联网的管理服务器来访问激活服务器。<br>默认情况下已清空该复选框。<br>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，则授权许可信息由 Protection Server 提供。 |
| **代理服务器排除项** | 这组设置包含"**配置**"按钮，用于打开"**代理服务器排除项**"窗口。 |

# 代理服务器排除项窗口

在此窗口中，您可以配置与 Kaspersky Anti Targeted Attack Platform 解决方案组件集成时使用代理服务器，以及您想要绕过代理服务器的地址列表。

代理服务器排除项

| 设置 | 描述 |
| --- | --- |
| **对组件不使用代理服务器** | 选中您不想使用代理服务器的应用程序组件旁边的复选框：<br>• **Endpoint Detection and Response Expert (on-premises)** – 连接到提供与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成的服务器时，不使用代理服务器。<br>• **Sandbox** – 连接到提供与 Sandbox 交互的服务器时，不使用代理服务器。<br>• **Network Detection and Response (KATA)** – 连接到 Kaspersky Network Detection and Response (KATA) Integration Server 时，不使用代理服务器。 |
| **对地址不使用代理服务器。** | 该表包含绕过代理服务器进行连接的地址列表。<br>• **IP 地址/DNS 名称**是您想要在不使用代理服务器的情况下连接的 IP 地址或域名。您可以使用掩码（"*"和"?"字符）来指定地址。<br>• 您可以选择在"**注释**"字段中输入注释。<br>您可以在表中添加、编辑或删除地址。 |

# 扫描任务的 CPU 使用量

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**，**性能** 部分）中启用或禁用 CPU 利用率限制，并配置扫描任务的内存使用限制。

单击 **性能** 下的 **配置** 将打开 **扫描任务的性能设置** 窗口，您可以在该窗口的 **CPU 和内存使用情况** 部分中配置限制（请参见下表）。

CPU 和内存使用设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>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。字段中的值必须是 10 到 100 之间的整数。<br>默认情况下已清空该复选框。 |
| **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）。<br>默认值：8192。 |

# 使用电池供电时运行任务

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**的 **性能**区域）中配置计划任务的取消。

使用电池供电运行时的任务设置

| 设置 | 描述 |
| --- | --- |
| **使用电池供电运行时跳过计划任务** | 该复选框可启用或禁用计划任务的取消。<br>默认情况下已选定该选框。<br>如果清除此复选框，则所有任务都会按计划运行，无论设备是否使用电池供电。 |

# 启动应用程序

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**，**应用程序启动设置**部分）中管理应用程序启动设置。

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。<br>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。<br>默认值：3。 |

# 收到关键更新时自动重启

在管理控制台中，您可以在策略属性中配置安装关键更新时应用程序自动重启（**常规设置 → 应用程序设置**）。

在**高级应用程序设置**部分中，单击**配置**按钮会打开**其他设置**窗口，您可以在该窗口中配置应用程序在收到关键更新时重启（见下表）。

应用关键更新的设置

| 设置 | 描述 |
| --- | --- |
| **收到关键更新时自动重启应用程序** | 该复选框用于启用或禁用在应用程序安装 24 小时后收到关键更新时自动重启应用程序。<br>默认情况下已清空该复选框。<br>如果选中此复选框，则在应用程序安装后已过去 24 小时的情况下，应用程序会在收到关键更新后重启。 |

# 密码保护

在管理控制台中，您可以在策略属性（**常规设置 → 界面**，**密码保护**部分）中配置密码保护设置。

在 **密码保护** 下，单击 **配置** 按钮可打开 **密码保护设置** 窗口，您可以在该窗口中编辑密码保护设置（见下表）。

应用程序启动设置

| 设置 | 描述 |
| --- | --- |
| **启用密码保护** | 此复选框用于启用或禁用应用程序设置的密码保护。<br>默认情况下已清空该复选框。 |
| **权限** | 此表包含可为其配置应用程序设置更改权限的用户和组。该表包含以下列：<br>• **用户/组** 是本地用户或域用户的名称，或者已配置权限的用户组的名称。<br>• **类型** 是已配置权限的 **用户** 或 **组**。<br>• **权限** 是允许用户或用户组执行的操作列表。<br>您可以添加、编辑和删除用户或用户组。<br>您可以单击 **添加** 按钮打开 **用户/组权限** 窗口，在该窗口中可以添加用户或组，并设置更改应用程序设置的权限。 |

# 跟踪和转储设置

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**，**跟踪和转储设置**部分）中管理跟踪和转储设置。

在 **跟踪和转储设置**下，单击 **配置**可打开 **跟踪和转储设置**窗口，您可以在其中编辑跟踪转储设置（请参见下表）。

跟踪和转储设置

| 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。<br>默认值：/var/log/kaspersky/kesl。<br>如果指定了不同的目录，请确保运行 Kaspersky Endpoint Security 的用户对该目录具有读取和写入权限。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)** | 在此字段中，可以输入应用程序跟踪文件的最大大小（以 MB 为单位）。<br>默认值：500。 |
| **跟踪文件的最大数量** | 在此字段中，您可以输入应用程序跟踪文件的最大数量。<br>默认值：10。 |
| **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。<br>默认情况下已清空该复选框。 |
| **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。<br>默认值：/var/opt/kaspersky/kesl/common/dumps。 |

# 应用程序的常驻内存使用率

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**）中配置常驻内存使用限制。

在**高级应用程序设置**部分，单击**配置**按钮打开**其他设置**窗口，您可以在其中配置驻留内存使用限制（见下表）。

要使更改生效，请在应用策略后重新启动受管理设备上的 Kaspersky Endpoint Security 应用程序。

应用程序的常驻内存使用设置

| 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：<br>• **无限制**。如果选择此选项，驻留内存的使用不受限制。<br>• **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）。<br>• **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。<br>• **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）。<br>• **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。<br>• **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）。<br>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）。<br>默认值：2000。 |

# 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**）中管理网络流量扫描设置。

加密连接扫描设置

| 设置 | 描述 |
| --- | --- |
| **启用加密连接扫描** | 此复选框启用或禁用对加密连接的扫描。<br>默认情况下已选定该选框。 |
| **加密连接的设置** | 本节包含加密连接扫描设置：<br>• **访问包含不受信任的证书的域**可指定在访问具有不受信任证书的域时应用程序必须执行的操作：<br>  • “**允许**”（默认值）– 允许连接到具有不受信任证书的域。<br>  • “**阻止**”– 阻止连接到具有不受信任证书的域。<br>• **访问具有网络流量扫描错误的域**可指定访问具有网络流量扫描错误的域时应用程序必须执行的操作：<br>  • “**允许并将域添加到排除项**”（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。<br>  • “**阻止**”– 阻止连接到存在扫描错误的域。<br>• **证书验证策略**是应用程序用来验证证书的方法：<br>  • **本地检查**：应用程序不使用互联网来验证证书。<br>  • **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。单击此按钮将打开“**受信任的根证书**”窗口。在此窗口中，您可以配置 Kaspersky Endpoint Security在扫描加密连接时必须视为受信任的根证书列表。 |

| 设置 | 描述 |
| --- | --- |
| **流量拦截排除** | 这组设置包含**配置**按钮，您可以点击该按钮打开**流量拦截排除**窗口。在此窗口中，您可以管理应用程序排除在流量拦截之外的连接的设置。 |
| **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。 |
| **高级设置** | 这组设置包含**配置**按钮，您可以单击该按钮打开**流量拦截模式**窗口。在此窗口中，您可以配置流量拦截模式：<br>• **使用 eBPF**。如果选择此选项，应用程序将使用 eBPF 技术来拦截流量。<br>• **使用 iptables**（默认）。如果选择此选项，应用程序将使用 iptables 技术来拦截流量。<br>要更改流量拦截模式，您需要重启应用程序。重启会断开已连接的网络连接。 |

## “受信任域”窗口

此列表包含将从扫描中排除的域名和域名掩码。应用程序不会扫描访问指定域时建立的连接。

例如：`*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、编辑或移除域。

## “受信任的证书”窗口

您可以配置 Kaspersky Endpoint Security 认为可信任的根证书列表。扫描加密连接时，将使用受信任的根证书列表。

将显示每个证书的以下信息：

- 证书主题
- 证书序列号
- 证书发布者
- 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。

您可以添加或移除证书。

单击**添加**按钮会打开一个窗口，您可以在其中通过以下方式之一将证书添加到受信任证书列表中：

- 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。

## 流量拦截排除窗口

该表包含应用程序排除在流量拦截之外的连接的设置：

- **远程 IP 地址**是被排除在拦截之外的流量去往或来自的 IP 地址（取决于流量的方向）。
- **目标端口**是受保护设备上的端口（在入站流量拦截排除中）或远程设备上的端口（在出站流量拦截排除中）。
- **流量方向**是连接中的流量方向：入站或出站。

您可以添加、编辑或删除排除项。

## 流量拦截排除窗口

在此窗口中，您可以添加流量拦截排除项。为此，您需要指定以下连接设置：

- **远程 IP 地址**是远程设备的 IPv4 或 IPv6 地址。根据流量方向，来自指定 IP 地址的流量（入站流量排除项）或去往指定 IP 地址的流量（传出流量排除项）被排除。
- **目标端口**，取决于流量方向：
  - 受保护设备上的端口（入站流量排除项）。从远程设备到此端口的流量不被拦截。
  - 远程设备上的端口（出站流量排除项）。从受保护设备到此端口的流量不被拦截。
- **流量方向**是被排除连接中的流量方向。您可以为入站流量或出站流量配置排除项。

在排除项中，您可以指定没有端口的远程设备的 IP 地址或没有 IP 地址的目标端口。

> 如果在入站流量排除项中仅指定远程设备的 IP 地址（未指定受保护设备上的端口），则来自远程设备的所有流量都将被排除在拦截之外。我们建议仅为来自您信任的设备的流量配置此排除项。

## 被监控的端口

网络端口设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>默认情况下已选定该选项。 |
| **网络端口设置** | 如果选择了**仅监控所选网络端口**选项，则此表包含应用程序监控的网络端口。该表包含两列：<br>• **端口** – 受监控的端口。<br>• **描述** — 受监控端口的描述。<br>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。<br>您可以在表中添加、编辑和删除项目。 |

# 全局排除项

在管理控制台中，您可以在策略属性（**常规设置 → 全局排除**）中配置全局排除。

**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。

## “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。<br>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：<br>• **本地**：本地挂载点。<br>• **挂载**：使用 Samba 或 NFS 协议挂载到设备上的远程目录。<br>• **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：<br>• **NFS**：使用 NFS 协议挂载到设备上的远程目录。<br>• **Samba**：使用 Samba 协议挂载到设备上的远程目录。<br>• **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。<br>必须以与 `mount` 命令输出中所显示的相同方式指定挂载点。 |
| **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。<br>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。 |

实用文章

### 如何指定掩码

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。

# 从扫描中排除进程内存

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。

您可以启用合并子策略继承时的排除列表。要合并列表项，请在**从扫描中排除进程内存**窗口中选中**合并继承的值**复选框。如果选中该复选框，则父策略列表中的项目将显示在子策略中，并且可以将项目添加到子策略列表中。如果清除此复选框，则继承策略设置时不会合并列表项。默认情况下已清空该复选框。

实用文章

**如何指定掩码**

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。

# 备份

在管理控制台中，您可以在策略属性（**常规设置** → **存储设置**）和受管理设备属性（**受管理设备** → **设备**选项卡 → 设备属性窗口 → **应用程序**区域 → 应用程序属性窗口 → **存储设置**）中管理备份区设置。

备份设置

| 设置 | 描述 |
| --- | --- |
| **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）。<br>可用值：0-10000。 如果指定 0，则对象可在存储内无限期存储。<br>默认值：30。 |
| **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)。<br>可用值：1-4000。如果清除该复选框，则备份的大小将不受限制。<br>默认情况下已清空该复选框。 |

# 检测黑客可能用来造成危害的应用程序

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**，**扫描设置**部分）中配置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。

入侵者可以用来破坏设备或数据的应用程序检测设置

| 设置 | 描述 |
| --- | --- |
| **检测入侵者可以用来破坏设备或数据的合法应用程序** | 此复选框用于启用或禁用对可能被黑客用来损害计算机或用户数据的合法应用程序的检测。<br><br>默认情况下已清空该复选框。 |

# 文件操作拦截

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**的 **文件操作拦截模式**区域）中配置文件操作拦截模式。

文件操作拦截设置

| 设置 | 描述 |
| --- | --- |
| **扫描期间阻止访问文件** | 该复选框可启用或禁用在文件由文件威胁防护和设备控制组件、执行防护操作以及可移动驱动器扫描任务扫描期间阻止对文件的访问。<br><br>默认情况下已选定该选框。<br><br>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。 |

# 将信息发送至 Kaspersky Security Center 存储

在 Kaspersky Security Center 中，您可以启用或禁用将有关备份中的文件、隔离文件、未处理的文件和已连接设备的信息传输到 Kaspersky Security Center 存储。

客户端设备上由卡巴斯基应用程序隔离的文件的常规列表保存在 Kaspersky Security Center 中，也可在管理控制台（**高级** → **存储库** → **隔离区**）中查看。

Kaspersky Security Center 会生成客户端设备上由卡巴斯基应用程序放入备份区的文件的常规列表，该列表可在管理控制台（**高级** → **存储库** → **备份区**）中查看。

未处理文件的信息显示在管理控制台的活动威胁列表中（**高级** → **存储库** → **活动威胁**）。

安装在客户端设备上或连接到客户端设备的设备信息显示在管理控制台的硬件列表中（**高级** → **存储库** → **硬件**）。如果启用了设备控制，则会传输数据。

在客户端设备上检测到的应用程序的信息也显示在管理控制台的应用程序列表中（**高级** → **应用程序管理** → **应用程序注册表**）。如果启用了应用程序控制，则会传输数据。

### 在管理控制台中启用或禁用数据传输

在管理控制台中，您可以在策略属性（**常规设置** → **存储设置**，**将数据传输到管理服务器**）或受管理设备的属性（**受管理设备** → **设备**选项卡 → 设备属性窗口 → **应用程序**部分 → 应用程序属性窗口 → **存储设置**，**将数据传输到管理服务器**部分）中启用或禁用向管理服务器传输数据。

单击“**将数据传输到管理服务器**”部分中的“**配置**”将打开**数据传输设置**，您可以在其中启用或禁用将数据传输到管理服务器。

向管理服务器传输数据的设置

| 设置 | 描述 |
| --- | --- |
| **关于隔离区中的文件** | 此复选框可启用或禁用将隔离文件的有关数据传输到管理服务器。<br>默认情况下已选定该选框。 |
| **关于备份区中的文件** | 此复选框可启用或禁用将备份中的文件数据传输到管理服务器。<br>默认情况下已选定该选框。 |
| **关于未处理的文件** | 此复选框用于启用或禁用向管理服务器发送扫描期间未处理文件的相关通知。<br>默认情况下已选定该选框。 |
| **关于已安装的设备** | 此复选框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数据传输到管理服务器。<br>默认情况下已选定该选框。 |
| **关于设备上发现的应用程序** | 此复选框用于启用或禁用将清查任务在客户端设备上发现的应用程序列表发送到管理服务器。<br>默认情况下已选定该选框。 |

## 系统事件拦截

在管理控制台中，您可以在策略属性（**常规设置** → **操作系统交互设置**，**系统事件拦截设置**区域）中配置系统事件拦截。

这些设置仅适用于运行支持 fanotify 技术的操作系统的设备。

系统事件拦截设置

| 设置 | 描述 |
| --- | --- |
| **拦截机制** | 应用程序使用的系统事件拦截机制：<br>• **fanotify 技术**（默认）。如果选择此选项，应用程序使用 fanotify 技术进行系统事件拦截。<br>• **可更新内核模块**。如果选择此选项，应用程序使用可更新内核模块进行系统事件拦截。 |
| **如果可更新内核模块启动失败** | 可更新内核模块启动失败时应用程序执行的操作：<br>• **使用 fanotify**（默认）。如果选择此选项，应用程序切换到 fanotify 技术进行系统事件拦截。<br>• **禁用系统事件拦截**如果应用程序不使用系统事件拦截，则不会执行实时文件扫描，并且设备的保护级别会降低。<br>如果选择了“**可更新内核模块**”拦截机制，则此选项可用。 |

## 附加遥测设置

在管理控制台中，您可以在策略属性（**常规设置** → **操作系统交互设置**，**附加遥测设置**部分）中管理附加遥测设置。

附加遥测设置

| 设置 | 描述 |
| --- | --- |
| **遥测来源** | Kaspersky Endpoint Security 用于收集遥测数据的来源：<br>• **仅使用 eBPF** 表示仅使用 eBPF 技术获取遥测数据。<br>• **使用 eBPF 和 auditd**（默认）表示使用 eBPF 技术和 auditd 服务获取遥测数据。 |
| **使用 auditd** | auditd 服务的模式：<br>• **在独占模式下使用 auditd**（默认）表示Kaspersky Endpoint Security 以独占模式使用 auditd 服务。<br>• **非独占模式**表示 auditd 服务以非独占模式使用。<br>此设置仅在**遥测来源**被设置为**使用 eBPF 和 auditd**时应用。 |

# Light Agent 模式

在管理控制台中，您可以在策略属性（**Light Agent 模式**）中管理用于将 Light Agent 连接到 SVM 的设置。

## 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 |
| --- | --- |
| **地址** | 安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。<br>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。<br>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。<br>如果将地址指定为 NetBIOS 名称、localhost 或 127.0.0.1，则与 Integration Server 的连接将以错误完成。 |
| **端口** | 用于连接到 Integration Server 的端口。<br>默认情况下，指定端口为 7271。 |

如果您的基础架构中部署了基于 Linux 的高可用性 Integration Server 集群，则需要将负载均衡器的地址和端口指定为连接到 Integration Server 的地址和端口。有关更多详细信息，请参阅卡巴斯基 Security for Virtualization Light Agent 帮助。

### 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 Kaspersky Endpoint Security 在 Light Agent 模式下使用时，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。<br>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。 |

| 设置 | 描述 |
| --- | --- |
| **SVM 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。<br>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)。您可以使用换行输入来隔开多个 IP 地址或 SVM 的完全限定域名。<br>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。<br>您可以单击"**删除**"按钮来删除在列表中选定的地址。<br>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 SVM 地址的自定义列表**"选项，Light Agent 使用扩展 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**"。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 |
| --- | --- |
| **使用连接标签** | 该复选框可启用或禁用 Light Agent 使用 SVM 连接标签。 |
| **标签** | 分配给 Light Agent 的标签。<br>对于标签，可以输入最长 255 个字符的文本字符串。可以使用除 **;** 字符外的任何字符。<br>如果选中了"**使用连接标签**"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 必须使用的 SVM 选择算法，并配置使用扩展 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。<br>如果找不到适合连接的本地 SVM，则 Light Agent 会选择连接 Light Agent 数量最少的 SVM，而不管 SVM 在虚拟基础架构中的位置如何。<br>默认情况下已选定该选项。 |
| **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。<br>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。<br>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。 |

| 设置 | 描述 |
| --- | --- |
| **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：<br>• **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）：<br>  • SVM 部署在与安装了 Light Agent 的虚拟机相同的 Hypervisor 上（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 上的虚拟基础架构中）。<br>  • SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。<br>  • SVM 与安装了 Light Agent 的虚拟机托管在同一计算节点上（在 Basis Dynamix Enterprise 的虚拟基础架构中）。<br>  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。<br>• **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）：<br>  • SVM 部署在与安装了 Light Agent 的虚拟机相同的 Hypervisor 集群中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 上的虚拟基础架构中）。<br>  • SVM 与安装了 Light Agent 的虚拟机部署在同一个 OpenStack 项目中（在 OpenStack 平台或 VK Private Cloud 上运行的虚拟基础架构中）。<br>  • SVM 与安装了 Light Agent 的虚拟机位于同一区域中（在 Bais Dynamix Enterprise 的虚拟基础架构中）。<br>  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。<br>• **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）：<br>  • SVM 部署在与安装了 Light Agent 的虚拟机相同的数据中心中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 上的虚拟基础架构中）。<br>  • SVM 与安装了 Light Agent 的虚拟机位于同一可用区中（在 OpenStack 平台或 VK Private Cloud 上运行的虚拟基础架构中）。<br>  • SVM 与安装了 Light Agent 的虚拟机位于同一数据中心中（在 Dynamix Enterprise Basis 的虚拟基础架构中）。<br>  如果带有 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。<br>• **忽略**。选择 SVM 时，Light Agent 不会考虑其位置。<br>默认情况下选择“**Hypervisor**”选项。<br>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 使用扩展 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。您必须将 **SVM 路径**设置设为**忽略**。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。<br>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 之间建立加密连接。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。<br>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。<br>默认情况下已清空该复选框。 |

# 已知问题和限制

## 应用程序限制

Kaspersky Endpoint Security 在以下情况下不受支持：

- 在 OSnova 操作系统的封闭软件环境模式和强化内核模式下。
- 在基于 Red Hat Enterprise Linux 且使用 IMA 子系统的操作系统上。
- 在基于 Red Hat Enterprise Linux 且处于 FIPS 模式的操作系统上。
- 在 Ubuntu 操作系统以及基于 SUSE Linux Enterprise Server 且使用 AppArmor 强制访问控制系统的操作系统上。
- 使用 Grsecurity 安全系统时（在所有操作系统上）。
- 使用 seccomp 机制时（在所有操作系统上）。
- 使用 WSL1 和 WSL2 技术时（在所有操作系统上）。
- 使用某些文件系统挂载选项时（例如，noexec、nosuid）。
- 当 Kaspersky Endpoint Security 安装在容器内时。

Detection and Response 解决方案在从安装了 Kaspersky Endpoint Security for Linux 的镜像创建的虚拟机上可能无法正常工作。与 Detection and Response 解决方案集成时，会使用计算机的唯一 ID（Sensor ID）。应用程序在初始安装过程中会生成此 ID，即使卸载应用程序后也会保留此 ID。克隆镜像时，虚拟机会继承 Sensor ID，这可能会导致 Detection and Response 解决方案将多个虚拟机识别为同一设备。

## 应用程序在某些架构上的限制

应用程序在以下处理器架构上运行时存在限制：

**厄尔布鲁士**

- Light Agent 模式：不受支持。
- EDR 代理模式：不受支持。
- BadUSB 攻击防护：无法正常工作。
- 漏洞利用防御：无法正常工作。
- Web 威胁防护：扫描网页中的网络钓鱼链接时，启发式分析不可用。
- Kaspersky Endpoint Detection and Response Optimum 集成：无法正常工作。

- Kaspersky Endpoint Detection and Response Expert (cloud) 集成：无法正常工作。
- Kaspersky Endpoint Detection and Response (KATA) 整合：无法正常工作。
- Kaspersky Managed Detection and Response 整合：无法正常工作。
- 沙盒：无法正常工作。
- KUMA 整合：无法正常工作。
- 容器扫描：无法正常工作。
- 可更新内核模块：不支持。
- 管理图形用户界面：用户无法在沙盒中提交文件进行扫描，因为不支持沙盒组件。

## 应用程序在某些操作系统上的限制

在以下操作系统上运行时，应用程序存在限制：

**Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)**

- BadUSB 攻击防护：无法正常工作，因为操作系统中缺少 systemd-logind 服务。
- 恶意软件扫描、关键区域扫描、清查和容器扫描任务的 CPU 资源使用限制在“4.2.0-23-generic”内核上不起作用。

**CentOS 5.2 和 5.4**

- 行为检测：由于无法同步拦截进程启动，因此无法保证该组件正常工作。
- 邮件威胁防护：无法正常工作。
- Web 威胁防护：无法正常工作，因为不支持 TProxy 机制。
- 网络威胁防护：无法正常工作，因为不支持 TProxy 机制。
- 反加密勒索：无法正常工作，因为不支持 TProxy 机制。
- BadUSB 攻击防护：无法正常工作，因为操作系统中缺少 systemd-logind 服务。
- 容器扫描：无法正常工作，因为操作系统不支持容器。
- 设备控制：仅当在应用程序中激活该模式后连接设备时，设备的只读模式才会生效。对于在激活此模式之前连接的设备，访问模式保持不变。
- 应用程序控制：无法正常工作，因为不支持同步拦截进程启动所需的 fanotify 技术。
- 防火墙管理：无法正常工作，因为不支持向 iptables 添加链。
- Web 控制：无法正常工作，因为不支持 TProxy 机制。

- 可更新内核模块：不支持。
- 网络隔离：无法正常工作，因为不支持 TProxy 机制。
- 对象执行防护无法正常工作，因为无法同步拦截进程启动。
- Kaspersky Endpoint Detection and Response Optimum 集成：无法正常工作。
- Kaspersky Endpoint Detection and Response Expert (cloud) 集成：无法正常工作。
- Kaspersky Endpoint Detection and Response (KATA) 集成：eBPF 遥测源不可用。
- Kaspersky Managed Detection and Response 集成：auditd 遥测源不可用。
- 图形用户界面：无法正常工作，因为操作系统中缺少 libxcb 库。
- Kaspersky Security Center 网络代理：需要额外的设备配置。请参阅 Kaspersky Security Center 帮助。
- 安装/删除：该应用程序与这些版本的操作系统中的 SELinux 不兼容。可能的解决方案：将 SELinux 设置为非阻止模式（宽容模式）、禁用 SELinux，或手动配置 SELinux。
- 恶意软件扫描：在 glibc 版本低于 2.11 的操作系统中，位于路径长度超过 4096 个字符的目录中的文件不会被清除或删除。
- 恶意软件扫描、关键区域扫描、清查和容器扫描任务的 CPU 资源使用限制无法正常工作。
- 不支持 Light Agent 模式，因此在安装应用程序时，KSVLA_MODE、SERVER_MODE、VDI_MODE 设置不适用。
- 不支持应用程序在 EDR Agent 模式下运行。
- Kaspersky Security Center 云控制台不支持该应用程序。
- 该应用程序不支持基于 FUSE 技术的文件系统。
- 扫描频率最高的文件统计信息不会被收集。
- 在某些情况下，作为与 Kaspersky Endpoint Detection and Response (KATA) 集成的一部分而传输的遥测数据可能包含有关系统事件日志中事件的不完整信息。

**CentOS 6.4 和 6.6**

- 行为检测：由于无法同步拦截进程启动，因此无法保证该组件正常工作。
- Web 威胁防护：IPv6 流量拦截无法正常工作。
- 网络威胁防护：IPv6 流量拦截无法正常工作。
- 反加密勒索：IPv6 流量拦截无法正常工作。
- BadUSB 攻击防护：无法正常工作，因为操作系统中缺少 systemd-logind 服务。
- 容器扫描：无法正常工作，因为操作系统不支持容器。
- 应用程序控制：无法正常工作，因为不支持同步拦截进程启动所需的 fanotify 技术。

- 防火墙管理：Firewall 的 IPv6 规则无法正常工作。
- Web 控制：IPv6 流量拦截无法正常工作。
- 可更新内核模块：不支持。
- 对象执行防护无法正常工作，因为无法同步拦截进程启动。
- Kaspersky Endpoint Detection and Response Optimum：威胁发展链不会显示网络活动，因为不支持 TProxy。仅提供有关文件操作的遥测事件。对象执行防护无法正常工作，因为无法同步拦截进程启动。
- Kaspersky Endpoint Detection and Response Expert (cloud) 集成：无法正常工作。
- Kaspersky Endpoint Detection and Response (KATA) 集成：eBPF 遥测源不可用。
- Kaspersky Managed Detection and Response 集成：auditd 遥测源不可用。
- Kaspersky Security Center 网络代理：需要额外的设备配置。请参阅 Kaspersky Security Center 帮助。
- 安装/删除：该应用程序与这些版本的操作系统中的 SELinux 不兼容。可能的解决方案：将 SELinux 设置为非阻止模式（宽容模式）、禁用 SELinux，或手动配置 SELinux。
- 恶意软件扫描：在 glibc 版本低于 2.11 的操作系统中，位于路径长度超过 4096 个字符的目录中的文件不会被清除或删除。
- 不支持应用程序在 Light Agent 模式和 EDR Agent 模式下运行。
- Kaspersky Security Center 云控制台不支持该应用程序。
- 扫描频率最高的文件统计信息不会被收集。
- 在某些情况下，作为与 Kaspersky Endpoint Detection and Response (KATA) 集成的一部分而传输的遥测数据可能包含有关系统事件日志中事件的不完整信息。

## 与 ptrace 设置值相关的限制

操作系统的 `kernel.yama.ptrace_scope` 设置值可能会影响 Kaspersky Endpoint Security：

- 1（受限 ptrace）。进程只能连接到它所启动的进程。连接到其他进程需要特殊权限。该应用程序的功能存在以下限制：
  - 行为检测组件无法获取进程的环境参数。
  - 在内核版本高于 5.7 的操作系统上，应用程序控制组件无法读取进程的命令行参数和环境变量，因为禁止读取 /proc/<pid>/syscall 和 /proc/<pid>/mem。在内核版本为 5.0 的操作系统上，应用程序控制组件无法正常运行。
  - 进程内存和内核内存扫描无法在扫描任务中正常工作，因为禁止读取 /proc/<pid>/mem。
  - 无法保证对进程内存进行 YARA 扫描，因为不允许读取 /proc/<pid>/mem。

- 2（管理员 ptrace）。只有具有 CAP_SYS_PTRACE 权限的进程（通常是 root）才能使用 ptrace 或访问 /proc 中的进程（/proc/<pid>/mem）。故障排除受到限制，因为崩溃转储不适用于用户进程（例如 kesl-control 和 kesl-gui），但转储适用于 kesl 进程本身。
- 3（禁止 ptrace）：在操作系统级别完全禁止 ptrace。该应用程序的功能存在以下限制：
  - 崩溃转储不适用于 kesl 进程或用户进程（例如 kesl-control 和 kesl-gui）。
  - 行为检测组件无法获取进程的环境参数。
  - 不支持应用程序控制组件。
  - 因为无法读取 /proc/<pid>/mem 目录：
    - 扫描任务中无法对进程内存和内核内存进行扫描。
    - 与检测和响应解决方案集成时，获取内存转储和获取进程内存转储任务无法运行。
    - 与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成时，无法保证在强制访问控制模式下对进程内存进行 YARA 扫描。

## 可更新内核模块的限制

可更新内核模块不支持以下内核类型和版本：

**Ubuntu**

- `*-kvm`
- `*-gkeop 5.15.0-100[1234] (bionic/jammy)`
- `focal 5.10.0-1002-oem`
- `noble 6.8.0-1014-ibm`
- `*-realtime`
- `*-uc-*`
- `kinetic 5.18.0-100(1|2)-(ibm|gcp|oracle)`

**Astra**

- `6.1.90-1-generic-*, 6.6.28-1-generic-*`
- `*-hardened`

**Debian**

- `*-rt`
- `5.14.0-1-(cloud-amd64|amd64)-5.14.6-2`

- `6.1.0-36-(cloud-amd64|amd64)-6.1.139-1`
- `6.5.0-5-*amd64-6.5.13-1`
- `6.6.*`

**RED OS 7.3**

- `kernel-ml-5.14.9-1.el7`

**RED OS 8.0**

- `6.6.26-1.red80`
- `6.6.34-1.red80`
- `6.6.51-1.red80`
- `6.6.76-1.red80`
- `6.6.6-1.red80`

## 使用 eBPF 技术的限制

要使用 eBPF 技术拦截网络流量，您需要使用以下选项编译的 Linux 4.18 或更高版本内核：

- `CONFIG_DEBUG_INFO_BTF=y` 或 `m`（支持带 BTF 的 eBPF）
- `CONFIG_KPROBES= y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_FSNOTIFY=y`

要在与 Detection and Response 解决方案集成时使用 eBPF 发送遥测数据，您需要使用以下选项编译的 Linux 4.18 或更高版本内核：

- `CONFIG_BPF=y`
- `CONFIG_BPF_SYSCALL=y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_KPROBES=y`
- `CONFIG_KPROBES_ON_FTRACE=y`
- `CONFIG_KRETPROBES=y`
- `CONFIG_HAVE_SYSCALL_TRACEPOINTS=y`

- `CONFIG_FTRACE=y`
- `CONFIG_FUNCTION_TRACER=y`
- `CONFIG_DYNAMIC_FTRACE=y`
- `CONFIG_DYNAMIC_FTRACE_WITH_REGS=y`
- `CONFIG_FTRACE_SYSCALLS=y`
- `CONFIG_KPROBE_EVENTS=y`
- `CONFIG_FSNOTIFY=y`

## 特殊注意事项

- 该应用程序不能同时在 Light Agent 模式和 EDR Agent 模式下使用。
- 在使用 auditd 3.0.7 和 Linux 内核 4.18 的操作系统中，使用行为检测组件可能会导致应用程序和 ssh 连接冻结。
- 在 Kylin Desktop V10 SP1 2303 操作系统上，行为检测组件可能会导致操作系统冻结。为解决此问题，我们建议更新操作系统内核。

## Light Agent 模式的特殊注意事项

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

- 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。

## EDR Agent 模式的特殊注意事项

如果 Kaspersky Endpoint Security 以 EDR Agent 模式运行，则仅有一部分应用程序组件和任务可用。安装后，应用程序设置如下：

- 不支持与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成。
- 以下组件提供与检测和响应解决方案的集成，完全可管理：
  - EDR Expert (on-premises)
  - NDR (KATA)

  这些组件默认处于禁用状态，您需要启用它们才能使应用程序在 EDR Agent 模式下运行。您可以管理集成设置，包括对象执行防护功能。
- 扫描期间不会阻止对文件的访问：**扫描期间阻止对文件的访问**复选框已清除（`FileBlockDuringScan=No`）。此设置可以修改，但不会应用到受保护的设备上。
- 文件威胁防护和反加密勒索防护组件以功能受限模式运行：当检测到威胁时，这些组件不会尝试清除或删除恶意对象，也不会阻止访问或应用程序活动，而只会将威胁检测信息发送到提供与 Detection and Response 解决方案进行集成的 Integration Server。

  您可以启用或禁用文件威胁防护和反加密勒索功能，并管理组件设置，但“检测到威胁后的操作”除外。以下设置不会应用到受保护的设备上：
  - 文件威胁防护：**检测到威胁后的操作**为**跳过**（`ActionOnThreat=Skip`）。
  - 反加密勒索：**检测到加密时的操作**为**通知**（`ActionOnDetect=Notify`）。
- 行为检测组件完全可管理。
- 所有其他保护和控制组件均已禁用，且无法管理。

当与 Kaspersky Endpoint Detection and Response Expert (on-premises) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，作为威胁响应操作的一部分，Kaspersky Endpoint Security 可以控制设备上可执行文件和脚本的启动。对象执行防护功能存在以下限制：

- 如果从解释器启动了脚本，则应用程序无法控制脚本的启动。
- 应用程序无法控制设备上办公软件文件的打开。

# 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。

卡巴斯基在 Kaspersky Endpoint Security 每个版本的生命周期内为其提供支持（请参阅应用程序生命周期页面）。与技术支持部门联系之前，请阅读支持规则。

您可以采用以下方式之一联系技术支持：

- 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 允许使用卡巴斯基应用程序的组织通过电子邮件请求联系卡巴斯基技术支持。在该门户上，您可以创建新请求、监控其进度并保留请求处理历史记录。

在 Kaspersky CompanyAccount 中，将贵组织的所有员工注册到同一账户下。这样，您便可以集中管理向卡巴斯基提交的电子请求，并控制用户对 Kaspersky CompanyAccount 的访问权限。

Kaspersky CompanyAccount 门户支持以下语言：

- 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 Kaspersky CompanyAccount 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。

# 如何启用和配置跟踪文件创建

*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。您可以在命令行、常规应用程序设置或图形用户界面中启用或禁用跟踪文件创建，并选择跟踪级别。

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 策略设置中管理该应用程序的跟踪设置。

**如何在 Web Console 中管理跟踪设置**

1. 在 Web Console 的主窗口中，选择 **资产管理** → **策略**。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到 **常规设置** → **技术支持** 部分，然后查看 **跟踪设置** 下的内容。

5. 如果要更改应用程序的跟踪文件默认保存的目录，请在 **跟踪文件夹路径** 字段中指定用于存储跟踪文件的目录。默认值：/var/log/kaspersky/kesl。需要 root 特权才能访问默认跟踪文件目录。如果您指定其他目录，请确保只有 root 用户具有此目录的读写权限（`700` 或 `rwx--------` 权限）。

6. 如有必要，请在 **跟踪文件最大大小 (MB)** 字段中指定应用程序跟踪文件的最大大小（以 MB 为单位）。默认值：500。

7. 如有必要，请在 **跟踪文件的最大数量** 字段中指定应用程序跟踪文件的最大数量。默认值：10。

8. 保存更改。

9. 重启应用程序以应用跟踪设置。

**如何在管理控制台中管理跟踪设置**

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. 转到“**常规设置**”→“**应用程序设置**”部分。

5. 在 **跟踪和转储设置** 下，单击 **配置**。

6. 将打开 **跟踪和转储设置** 窗口。

7. 如果要更改应用程序的跟踪文件默认保存的目录，请在 **跟踪文件目录的路径** 字段中指定用于存储跟踪文件的目录。默认值：/var/log/kaspersky/kesl。需要 root 特权才能访问默认跟踪文件目录。如果您指定其他目录，请确保只有 root 用户具有此目录的读写权限（`700` 或 `rwx--------` 权限）。

8. 如有必要，请在 **最大跟踪文件大小 (MB)** 字段中指定应用程序跟踪文件的最大大小（以 MB 为单位）。默认值：500。

9. 如有必要，请在 **跟踪文件的最大数量** 字段中指定应用程序可以创建的跟踪文件的最大数量。默认值：10。

10. 在 **跟踪和转储设置** 窗口中单击 **确定**。

11. 单击**应用**。

12. 重启应用程序以应用跟踪设置。

**如何在命令行中启用跟踪并管理跟踪设置**

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` 设置来配置跟踪。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。

*要在命令行中创建跟踪文件并配置跟踪设置：*

1. 启用跟踪文件创建并选择跟踪级别：

```
kesl-control --set-app-settings TraceLevel=Detailed | MediumDetailed | NotDetailed
```

其中：

- `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。

2. 如果要更改应用程序的跟踪文件默认保存的目录，请指定用于存储跟踪文件的目录：

```
kesl-control --set-app-settings TraceFolder=<path to trace files directory>
```

其中 `<path to trace files directory>` 是存储跟踪文件的目录路径。默认值：/var/log/kaspersky/kesl。需要 root 特权才能访问默认跟踪文件目录。如果您指定其他目录，请确保只有 root 用户具有此目录的读写权限（`700` 或 `rwx--------` 权限）。

3. 如有必要，请指定跟踪文件的最大数量：

```
kesl-control --set-app-settings TraceMaxFileCount=<number of application trace files>
```

其中 `<number of application trace files>` 是应用程序跟踪文件的最大数量。可能的值：1 到 10000。默认值：10。

4. 如有必要，请指定应用程序跟踪文件的最大大小（以 MB 为单位）：

```
kesl-control --set-app-settings TraceMaxFileSize=<size of an application trace file>
```

其中 `<size of an application trace file>` 是跟踪文件的最大大小（以 MB 为单位）。可能的值：1 到 1000。默认值：500。

更改`TraceFolder`、`TraceMaxFileCount`或`TraceMaxFileSize`设置的值后，需要重新启动应用程序。

要禁用跟踪文件创建，请运行以下命令：

```
kesl-control --set-app-settings TraceLevel=None
```

### 如何在图形界面中启用跟踪并管理跟踪设置

要创建跟踪文件并配置其详细程度，您需要具有管理员角色(admin) 的用户。

1. 打开应用程序图形界面的主窗口。
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：

   - **诊断 (300)** – 仅错误消息。
   - **信息 (700)** – 信息性消息和错误消息。
   - **调试 (800)** – 详细的跟踪文件。

   我们建议您向卡巴斯基技术支持专家确认所需的细节级别。默认设置为 **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。

您还可以启用和配置 Watchdog 服务器跟踪文件的创建。

**如何在命令行中启用跟踪并管理 Watchdog 服务器跟踪设置**

在命令行中，您可以使用 常规应用程序设置中的 `WdTraceLevel` 设置来配置 Watchdog 服务器跟踪。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更改设置的值。

从命令行创建 Watchdog 服务器跟踪文件并配置跟踪设置

```
kesl-control --set-app-settings WdTraceLevel=Detailed | MediumDetailed | NotDetailed | Product
```

其中：

- `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。
- `Product` – 将该值设置为等于 常规应用程序设置中 `TraceLevel` 设置的值。如果 `TraceLevel=None`，则不会生成跟踪文件。

禁用 Watchdog 服务器跟踪文件的创建并从命令行配置跟踪设置

```
kesl-control --set-app-settings WdTraceLevel=None
```

默认情况下，创建的跟踪文件存储在 /var/log/kaspersky/kesl/ 目录中。访问此目录需要 root 权限。您可以指定其他目录来存储跟踪文件。如果您指定其他目录，请确保只有 root 用户具有此目录的读写权限（`700` 或 `rwx------` 权限）。

图形界面和 kesl-control 命令行实用程序的跟踪文件存储在 /var/log/kaspersky/kesl-user 目录中。要启用这些跟踪文件的创建，您需要设置 LFS_ENABLE_ALL_COMPONENTS_LOGGING 环境变量。

为了存储跟踪文件，应用程序除了最低硬件要求中列出的磁盘空间外，还需要额外的磁盘空间。

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。

**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，则有关管理 MMC 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。

**管理 Web 插件跟踪文件**

如果您使用 Web Console 管理 Kaspersky Endpoint Security，则有关管理 Web 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。

**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。
- 执行线程编号。
- 引起该事件的应用程序组件。
- 事件严重程度（通知性事件、警告、严重事件、错误）。
- 关于应用程序组件命令执行和命令执行结果的事件说明。

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。
- 应用程序中的用户活动的数据。
- 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、OSMP 服务器、NDR 服务器以及提供与 Sandbox 交互的服务器接收的数据。
- 有关消耗的 CPU 资源的数据。
- 有关消耗的 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。

**管理插件跟踪文件的内容**

管理插件的跟踪文件包含以下常规数据：

- 事件时间。
- 执行线程编号。
- 引起该事件的应用程序组件。
- 事件严重程度（通知性事件、警告、严重事件、错误）。
- 关于应用程序组件命令执行和命令执行结果的事件说明。

除了常规数据之外，管理插件的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）。

# 如何启用和配置转储

*转储文件*包含有关在创建转储文件时 Kaspersky Endpoint Security 进程的工作内存的所有信息。

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。

默认情况下不生成转储文件。您可以在应用程序发生故障时启用或禁用转储。

如果您通过 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并对其进行配置。

如果您使用命令行管理应用程序，则可以通过 常规应用程序设置 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。

**如何在 Web Console 中启用和配置转储**

*要在 Web Console 中启用和配置转储：*

1. 在 Web Console 的主窗口中，选择 **资产管理 → 策略**。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**常规设置 → 技术支持**”部分中的“**调试信息**”。
5. 如果您希望在应用程序崩溃时生成转储文件，请启用“**转储写入已启用**”切换开关。
6. 如果要更改默认保存 kesl 进程转储文件的目录，请在“**代码转储路径**”字段中指定用于存储转储文件的目录。默认值：/var/opt/kaspersky/kesl/common/dumps。需要 root 特权才能访问默认转储文件目录。如果您指定其他目录，请确保只有 root 用户具有此目录的读写权限（`700` 或 `rwx--------` 权限）。
7. 保存更改。

**如何在管理控制台中启用和配置转储**

*要在管理控制台中启用和配置转储：*

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. 转到“**常规设置**”→“**应用程序设置**”部分。
5. 在 **跟踪和转储设置** 下，单击 **配置**。
6. 将打开 **跟踪和转储设置** 窗口。
7. 如果您希望在应用程序崩溃时生成转储文件，请选中“**应用程序崩溃时创建转储文件**”复选框。
8. 如果要更改默认保存 kesl 进程转储文件的目录，请在“**转储文件目录的路径**”字段中指定用于存储转储文件的目录。默认值：/var/opt/kaspersky/kesl/common/dumps。访问默认转储文件目录需要 root 权限（`700` 或 `rwx-------` 权限）。如果指定其他目录，请确保只有 root 用户对此目录具有读写权限。
9. 在 **跟踪和转储设置** 窗口中单击 **确定**。
10. 单击**应用**。

**如何在命令行中启用和配置转储**

在命令行中，您可以使用常规应用程序设置中的 `CoreDumps` 和 `CoreDumpsPath` 设置启用、禁用和配置转储。

*要启用和配置转储：*

1. 运行以下命令启用转储：

```
kesl --set-app-settings CoreDumps=Yes
```

2. 如果要更改保存转储文件的目录，请在 `CoreDumpsPath` 设置中指定目录的路径。

```
kesl --set-app-settings CoreDumpsPath=<path to directory with dump files>
```

其中，`<path to directory with dump files>` 是存储转储文件的目录路径。默认值：/var/opt/kaspersky/kesl/common/dumps。访问默认转储文件目录需要 root 权限（`700` 或 `rwx--------` 权限）。如果指定其他目录，请确保只有 root 用户对此目录具有读写权限。

*要禁用转储，请运行以下命令：*

```
kesl --set-app-settings CoreDumps=No
```

如果已启用转储，默认情况下，转储文件存储在以下目录中：

- /var/opt/kaspersky/kesl/common/dumps（kesl 进程的转储文件）
- /var/opt/kaspersky/kesl/common/dumps-user（用户进程的转储文件）。

需要 root 特权才能访问默认转储文件目录。您可以指定不同的目录来存储 kesl 进程的转储文件。如果您指定其他目录，请确保只有 root 用户具有此目录的读写权限（`700` 或 `rwx--------` 权限）。

为了存储转储文件，应用程序除了最低硬件要求中列出的磁盘空间外，还需要其他磁盘空间。

只要应用程序在使用中，就会在计算机中存储转储文件，当应用程序被卸载后，转储文件将被永久删除。转储文件不会自动发送到卡巴斯基。

# 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<设备名称>链接。
   设备属性窗口将打开。
3. 在“**高级**”选项卡上，选择“**远程诊断**”部分。

在设备远程诊断窗口中，您可以查看远程安装日志。

*要查看设备上的远程安装日志，请执行以下操作：*

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安装日志，请执行以下操作：*

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。

# 附录

本节提供补充主要帮助内容的信息。

# 附录 1.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：
- 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 > 格式指定设置值（不处理设置名称与其值之间的空格）。

  例如：

  ```
  [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。

  例如：

  ```
  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。

  例如：
  `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。

# 初始配置文件

您可以使用配置文件指定应用程序的初始配置设置：

- 如果您使用 Kaspersky Security Center 安装应用程序，则可以在用于远程应用程序安装的存档中找到 autoinstall.ini 配置文件。您可以在创建安装包之前在此文件中指定设置。Kaspersky Security Center 会在应用程序安装过程中应用这些设置。
- 如果您使用命令行安装应用程序，则需要创建配置文件，并在启动初始配置向导时指定该文件的路径。您可以从 autoinstall.ini 配置文件复制此文件的结构。

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。已为 autoinstall.ini 文件指定默认值。

某些设置的有效值取决于您是通过 Kaspersky Security Center 远程安装，还是通过命令行安装。

要更改配置文件中的设置，请以 <setting name>=<value> 格式指定其值。

示例

```
UPDATER_SOURCE=KLServers
```

| 设置 | 描述 | 值 |
| --- | --- | --- |
| **[CustomSettings]** 部分 | 在远程安装过程中对应用程序进行微调。允许您更改 kesl.ini 文件中的部分设置以及 跟踪级别。<br><br>您只能在初始安装期间使用此部分配置应用程序。<br><br>如果 `[CustomSettings]` 部分重复 autoinstall.ini 文件的设置，则会将 autoinstall.ini 设置应用于应用程序。 | • kesl.ini 配置文件中采用 <setting section>.<setting name>=<value> 格式的任何设置<br>**示例**<br>`[CustomSettings]`<br>`General.Locale=ru_RU.utf8`<br>`Network.ProxyRouteTable=202`<br>`Watchdog.MaxMemory=20MB`<br>• `TraceLevel`，应用程序跟踪文件的详细级别：<br>  • `Detailed` – 生成详细的应用程序跟踪文件。<br>  • `MediumDetailed` – 生成包含信息消息和错误消息的应用程序跟踪文件。<br>  • `NotDetailed` – 生成包含错误消息的应用程序跟踪文件。<br>  • `None`（默认值）– 不生成应用程序跟踪文件。<br>• `WdTraceLevel`，Watchdog 服务器跟踪文件的详细级别：<br>  • `Detailed` 生成详细的 Watchdog 服务器跟踪文件。<br>  • `MediumDetailed` 生成包含信息消息和错误消息的 Watchdog 服务器跟踪文件。<br>  • `NotDetailed` 生成包含错误消息的 Watchdog 服务器跟踪文件。<br>  • `None` 不生成 Watchdog 服务器跟踪文件。<br>  • `Product`（默认值）将值设置为等于 `TraceLevel` 的值。 |
| EULA_AGREED | 必要设置。<br>接受最终用户授权许可协议的条款。 | `Yes`（默认）– 接受最终用户授权许可协议的条款和条件。<br>`No` – 不接受最终用户授权许可协议的条款和条件。应用程序安装将终止。 |
| PRIVACY_POLICY_AGREED | 必要设置。<br>接受隐私策略条款。 | `Yes`（默认）– 接受隐私策略的条款和条件。<br>`No` – 不接受隐私策略的条款和条件。应用程序安装将终止。 |
| USE_KSN | 必要设置。<br>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。<br><br>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。 | `Yes` – 接受卡巴斯基安全网络声明的条款并启用 KSN。<br>`No`（默认值）– 不接受卡巴斯基安全网络声明的条款和条件。退出 KSN 不会中止应用程序安装过程。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| LOCALE | 发送到 Kaspersky Security Center 的应用程序事件使用的区域设置。<br><br>图形界面和应用程序命令行的区域设置取自 `LANG` 环境变量。如果应用程序不支持此本地化，则默认使用英语本地化。 | RFC 3066 格式的区域设置。可能的值：<br>• `de_DE.UTF-8` — 德语<br>• `en_US.UTF-8` – 英语（美国）<br>• `es_MX.UTF-8` – 西班牙语（墨西哥）<br>• `fr_FR.UTF-8` — 法语<br>• `ja_JP.UTF-8` — 日语<br>• `pt_BR.UTF-8` – 葡萄牙语（巴西）<br>• `ru_RU.UTF-8` — 俄语<br>• `zh_TW.UTF-8` — 繁体中文<br>• `zh_CN.UTF-8` — 简体中文<br>如果未指定 `LOCALE` 设置，则使用操作系统区域设置。<br><br>如果应用程序无法检测操作系统的区域设置或不支持该区域设置，则使用英语（RFC 3066 格式的 en_US.UTF-8）对事件进行本地化。 |
| INSTALL_LICENSE | 在 autoinstall.ini 配置文件中：用于向应用程序添加授权许可密钥的激活码。<br>在命令行配置文件中，您还可以指定密钥文件的路径，以便向应用程序添加授权许可密钥。<br><br>只有在标准模式下使用应用程序时，该设置才适用。 | `<activation code>`，如果您希望通过 Kaspersky Security Center 或在命令行安装时使用激活码激活应用程序。<br>`<full path to key file>`，如果您希望在命令行安装期间使用密钥文件激活应用程序。<br>`None`，如果您不想在安装期间激活应用程序，例如，如果您在没有互联网访问的独立网络段中安装应用程序。 |
| UPDATER_SOURCE | 数据库和应用程序模块的更新源。<br><br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 | `SCServer` —使用 Kaspersky Security Center 管理服务器作为更新源。<br>`KLServers`（默认）– 使用卡巴斯基服务器作为更新源。<br>`<update source address>`，可以是本地目录（例如 /home/bases），也可以是远程 HTTP 或 HTTPS 服务器（例如 http://example.com/bases/）。 |
| PROXY_SERVER | 用于连接到互联网的代理服务器的地址。<br><br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 | 代理服务器的地址采用以下格式之一：<br>• `[<connection protocol>://]<address of the proxy server>:<port>`，如果连接到代理服务器不需要身份验证；<br>• `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。指定 IPv6 地址时，请将其输入方括号中。<br><br>不支持通过 HTTPS 连接到代理服务器。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UPDATE_EXECUTE | 在初始配置期间启动应用程序数据库更新任务。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 | `Yes`（默认值）– 启动更新任务。<br>`No` — 不启动更新任务。 |
| KERNEL_SRCS_INSTALL | 启动文件威胁防护时自动编译内核模块。<br>此设置仅适用于不支持 fanotify 的操作系统。 | `Yes`（默认） — 在文件威胁防护任务启动时编译内核模块。<br>`No` – 不编译内核模块。 |
| USE_GUI | 安装并使用应用程序的图形界面。<br>仅当应用程序以标准模式或 EDR 代理模式使用时，才应用此参数。 | `Yes` — 安装并使用应用程序的图形界面（必须将用于安装图形界面的文件添加到安装包中）。<br>`No`（默认）– 不使用图形界面。 |
| GROUP_CLEAN | 必要设置。<br>在安装应用程序之前，自动从 kesladmin 和 keslaudit 特权组中移除用户。 | `Yes` – 从特权组中删除用户。如果值为“`Yes`”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。<br>`No`（默认）– 不从特权组中删除用户。 |
| ADMIN_USER | 被分配了管理员角色 (admin) 的用户。<br>管理员角色允许在应用程序的图形界面和命令行中管理应用程序设置和任务设置，而无需使用 `sudo` 命令。 | |
| 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。<br>`No` – 不执行 SELinux 自动配置。 |
| DISABLE_PROTECTION | 安装后禁用应用程序的功能组件。<br>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。<br>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。 | `Yes` – 在安装后启动应用程序时，禁用保护组件和扫描任务。<br>`No` – 在安装后启动应用程序时，不禁用保护组件和扫描任务。 |
| ENDPOINT_AGENT_MODE | 在 EDR Agent 模式下使用 Kaspersky Endpoint Security。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `Yes` – Kaspersky Endpoint Security 以 EDR 代理模式使用，以支持 Kaspersky Detection and Response 解决方案与受保护设备上的第三方反病毒解决方案协同工作。<br>`No`（默认值）– Kaspersky Endpoint Security 以标准模式或 Light Agent 模式运行（请参阅 KSVLA_MODE 设置）。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| EDR_EXPERT_CLOUD_MODE | 选择 Endpoint Detection and Response Expert 组件的模式。<br>只有在标准模式下使用应用程序时，该设置才适用。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `Yes` 表示应用程序使用 Kaspersky Endpoint Detection and Response Expert (cloud) 整合。<br>`No`（默认值）表示应用程序使用 Kaspersky Endpoint Detection and Response Expert (on-premises) 整合。 |
| KSVLA_MODE | 在 Light Agent 模式下使用 Kaspersky Endpoint Security。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `Yes` - Kaspersky Endpoint Security 以 Light Agent 模式使用（作为 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。<br>`No`（默认值）– Kaspersky Endpoint Security 以标准模式或 EDR 代理模式使用（请参阅 ENDPOINT_AGENT_MODE 设置）。 |
| SERVER_MODE | 受保护的虚拟机的角色（服务器或工作站）。<br>仅当在 Light Agent 模式下使用应用程序时，才应用此设置。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `Yes` – 受保护的虚拟机被用作服务器。<br>`No` – 受保护的虚拟机被用作工作站。 |
| 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。<br>仅当在 Light Agent 模式下使用应用程序时，才应用此设置。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `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。<br>`No` – 不启用 VDI 保护模式。 |
| INTERCEPTOR_MODE | Kaspersky Endpoint Security 使用的系统事件拦截机制：<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `UseFanotify`（默认）— 使用 fanotify 技术来拦截系统事件。<br>`UseUpdatableKernelModule` — 用于通过可更新内核模块来拦截系统事件。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| INTERCEPTOR_FALLBACK_STRATEGY | 如果可更新内核模块启动失败，应用程序执行的操作。<br><br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br><br>此设置不适用于配备 Elbrus CPU 的设备。 | `FallbackToFanotify`（默认）— 切换到 fanotify 进行系统事件拦截。<br><br>`FallbackToLimitedMode` — 不使用系统事件拦截。这一操作会导致无法进行实时文件扫描，降低了设备的保护级别。 |
| INTERCEPTOR_APPLY_STRATEGY | 如果应用程序切换到使用可更新内核模块，则必须重启应用程序才能启动该模块。此设置允许您指定是希望自动重启应用程序还是希望手动重启应用程序。<br><br>此设置仅适用于通过 Kaspersky Security Center 安装的情况。<br><br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br><br>此设置不适用于配备 Elbrus CPU 的设备。 | `RestartServiceAutomatically`（默认值）自动重启应用程序以启动可更新内核模块。<br><br>`RestartServiceManually` 会在用户手动重启应用程序后，启动可更新内核模块。<br><br>我们建议自动重启应用程序以切换到使用可更新的内核模块。重新启动应用程序后手动启动可更新的内核模块可能会导致应用程序错误。 |
| ENABLE_TRACES_ON_FIRST_STARTUP | 在安装后首次启动应用程序时创建跟踪文件。<br><br>为了创建跟踪文件，系统会在 /var/log/kaspersky/kesl 目录下自动创建一个名为 kesl_startup.log 的文件。常规应用程序跟踪文件的大小限制不适用于此文件。跟踪在五分钟后或文件威胁防护任务启动后停止。 | `Yes` — 在安装后首次启动应用程序时创建跟踪文件。<br><br>`No`（默认值）– 在首次启动应用程序时不创建跟踪文件。 |
| AK_FORCED_PACKAGE_MANAGER_OPERATIONS_AS_FALLBACK | 使用忽略软件包管理器错误的应用程序安装模式。<br><br>如果无法正常安装应用程序，可以使用此模式。<br><br>此设置仅适用于通过 Kaspersky Security Center 安装的情况。<br><br>仅建议在技术支持专家的监督下并根据其说明更改默认值。 | `No`（默认值）正常安装应用程序。<br><br>`Yes` 在忽略系统错误的情况下安装应用程序。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| AK_REMOVE_PARTIALLY_INSTALLED_PACKAGE | 如果应用程序安装包仅部分安装，则自动将其删除。<br>如果无法正常安装应用程序，请禁用此设置。<br>此设置仅适用于通过 Kaspersky Security Center 安装的情况。<br>仅建议在技术支持专家的监督下并根据其说明更改默认值。 | `Yes`（默认值）删除部分安装的应用程序安装包。<br>`No` 在忽略部分安装的安装包的情况下安装应用程序。 |
| AK_PACKAGE_MANAGER_DEBUG_LOG_OUTPUT | 启用软件包管理器的调试日志。<br>如果无法正常安装应用程序，可以使用此设置。<br>此设置仅适用于通过 Kaspersky Security Center 安装的情况。<br>仅建议在技术支持专家的监督下并根据其说明更改默认值。 | `Yes` 启用软件包管理器的调试日志。<br>`No`（默认值）不启用软件包管理器的调试日志。 |

# 安装包中的初始配置设置

您可以在通过 Kaspersky Security Center 安装应用程序所用的安装包中指定应用程序的初始配置设置。

在 Kaspersky Security Center Web Console 中，您可以在安装包属性中的“**设置**”选项卡上指定 Kaspersky Endpoint Security 的初始配置设置。创建的安装包可在 Web Console 主窗口的以下任一部分中找到：

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

在 Kaspersky Security Center 管理控制台中，您可以在创建安装包时或在安装包属性的“**设置**”部分中指定 Kaspersky Endpoint Security 的初始配置设置。已创建的安装包可在管理控制台的树形结构中找到：**附加 → 远程安装 → 安装包**文件夹。

适用的设置集取决于应用程序的使用模式。

### 在 Web Console 中进行初始配置设置

| 设置 | 描述 |
| --- | --- |
| **使用模式** | • **用于保护工作站和服务器的标准模式**（默认值）。如果选中此选项，则应用程序将作为独立应用程序用于保护 Linux 工作站和服务器。<br>• "**Endpoint Detection and Response Agent**"。如果选择此选项，则应用程序将用于支持 Kaspersky Detection and Response 解决方案与受保护设备上的第三方反病毒解决方案协同工作。<br>• "**用于保护虚拟环境的 Light Agent**"。如果选择此选项，则应用程序将在 Light Agent 模式下使用（作为 Kaspersky Security for Virtualization Light Agent 的一部分）。<br><br>EDR Agent 模式和 Light Agent 模式不适用于配备 Elbrus CPU 的设备。 |
| **启用 Endpoint Detection and Response Expert (cloud)** | 选中此复选框以使用 Endpoint Detection and Response Expert (cloud) 集成。<br><br>在标准模式下，应用程序支持与 Endpoint Detection and Response Expert (cloud) 和 Endpoint Detection and Response Expert (on-premises) 集成。如果清除此复选框，则使用与 Endpoint Detection and Response Expert (on-premises) 的集成。<br><br>只有在标准模式下使用应用程序时，该设置才适用<br><br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **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。默认情况下已清空该复选框。<br><br>仅当在 Light Agent 模式下使用应用程序时，才应用此设置。<br><br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **受保护的虚拟机被用作服务器** | 要安装应用程序的虚拟机的角色：服务器或工作站。此复选框默认处于选中状态（虚拟机在虚拟基础架构中用作服务器）。<br><br>仅当在 Light Agent 模式下使用应用程序时，才应用此设置。<br><br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **KSC 中事件的语言** | 发送到 Kaspersky Security Center 的应用程序事件使用的本地化语言：<br>• **系统**（默认）将使用操作系统区域设置。<br><br>如果应用程序无法检测操作系统的区域设置或不支持该区域设置，则使用英语作为事件本地化的语言。<br>• Kaspersky Endpoint Security 支持的语言之一：英语（美国）、西班牙语（墨西哥）、繁体中文、简体中文、德语、葡萄牙语（巴西）、俄语、法语、日语。<br><br>图形界面和应用程序命令行的区域设置取自 `LANG` 环境变量。如果应用程序不支持此本地化，则默认使用英语本地化。 |
| **激活应用程序** | 如果您想在安装过程中激活应用程序，请选中此复选框。在显示的字段中输入激活码。默认情况下已清空该复选框。<br><br>只有在标准模式下使用应用程序时，该设置才适用。 |

| 设置 | 描述 |
| --- | --- |
| **更新源** | 数据库和应用程序模块的更新源。<br>• **卡巴斯基更新服务器**（默认）。<br>• Kaspersky Security Center。<br>• **本地或全球网络上的其他源**。如果选择此选项，请在打开的字段中输入更新源的地址。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **安装后运行数据库更新任务** | 如果选中此复选框，则应用程序安装后，数据库和应用程序模块更新任务将会启动。默认情况下已选定该选框。<br>如果您已将预先下载的应用程序数据库添加到安装包中，请清除此复选框。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **指定代理服务器设置** | 如果您使用代理服务器访问互联网，请选中此复选框。在显示的字段中，采用以下格式之一输入代理服务器地址：<br>• `[<connection protocol>://]<address of the proxy server>:<port>`，如果连接到代理服务器不需要身份验证；<br>• `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。指定 IPv6 地址时，请将其输入方括号中。<br>不支持通过 HTTPS 连接到代理服务器。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **安装内核源代码** | 如果选中此复选框，启动文件威胁防护，将自动在不支持 fanotify 的操作系统上启动内核模块的编译。默认情况下已选定该选框。<br>此设置仅适用于不支持 fanotify 的操作系统。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **使用图形用户接口** | 如果您计划安装并使用应用程序图形界面，请选中此复选框。用于安装图形界面的文件必须添加到安装包中。默认情况下已清空该复选框。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **指定具有管理员角色的用户** | 选中此复选框可以指定要为其分配管理员角色的用户。管理员角色允许在应用程序的图形界面和命令行中管理应用程序设置和任务设置，而无需使用 `sudo` 命令。<br>在显示的字段中输入用户名。 |
| **自动配置 SELinux** | 如果选中此复选框，则在应用程序初始配置期间，SELinux 会自动配置为与 Kaspersky Endpoint Security 协同工作。默认情况下已选定该选框。 |
| **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将用户从“kesladmin”和“keslaudit”特权组中自动移除。默认情况下已清空该复选框。<br>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** | 如果在完成安装过程后，您想要在禁用保护组件和扫描任务的情况下运行应用程序，请选中此复选框。<br>禁用保护组件的安装很方便，例如，为了重现应用程序操作中的问题并创建跟踪文件。<br>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。 |
| **安装后首次启动应用程序时启用跟踪** | 如果您希望在安装后首次启动应用程序时创建跟踪文件，请选中此复选框。<br>为了创建跟踪文件，系统会在 /var/log/kaspersky/kesl 目录下自动创建一个名为 kesl_startup.log 的文件。常规应用程序跟踪文件的大小限制不适用于此文件。跟踪在五分钟后或文件威胁防护任务启动后停止。 |

| 设置 | 描述 |
| --- | --- |
| **拦截机制** | 应用程序使用的系统事件拦截机制：<br>• **fanotify 技术**（默认）。如果选择此选项，应用程序使用 fanotify 技术进行系统事件拦截。<br>• **可更新内核模块**。如果选择此选项，则会在应用程序安装期间安装可更新内核模块。应用程序使用该模块来拦截系统事件。<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **如果可更新内核模块启动失败** | 可更新内核模块启动失败时应用程序执行的操作：<br>• **使用 fanotify**（默认）。如果选择此选项，应用程序切换到 fanotify 技术进行系统事件拦截。<br>• **禁用系统事件拦截**如果应用程序不使用系统事件拦截，则不会执行实时文件扫描，并且设备的保护级别会降低。<br>如果选择了"**可更新内核模块**"拦截机制，则此选项可用。<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **启用包管理器错误忽略模式** | 选中此复选框，以在安装应用程序时忽略软件包管理器错误。默认情况下已清空该复选框。<br>如果无法正常安装应用程序，可以使用此设置。<br>我们建议您仅在技术支持的监督下启用此设置。 |

## 在管理控制台中进行初始配置设置

初始配置设置

| 设置 | 描述 |
| --- | --- |
| **KSC 中事件的语言** | 发送到 Kaspersky Security Center 的应用程序事件使用的本地化语言：<br>• **系统**（默认）将使用操作系统区域设置。<br>如果应用程序无法检测操作系统的区域设置或不支持该区域设置，则使用英语作为事件本地化的语言。<br>• Kaspersky Endpoint Security 支持的语言之一：英语（美国）、西班牙语（墨西哥）、繁体中文、简体中文、德语、葡萄牙语（巴西）、俄语、法语、日语。<br>图形界面和应用程序命令行的区域设置取自 `LANG` 环境变量。如果应用程序不支持此本地化，则默认使用英语本地化。 |
| **激活码** | 如果您想在安装过程中激活应用程序，请输入激活码。<br>只有在标准模式下使用应用程序时，该设置才适用。 |

| 设置 | 描述 |
| --- | --- |
| **选择更新源** | 点击“**配置**”按钮将打开一个窗口，您可以在其中选择数据库和应用程序模块更新源：<br>• **卡巴斯基更新服务器**（默认值）。<br>• “Kaspersky Security Center”。<br>• “**本地或全球网络上的其他源**”。如果选择此选项，请在“**地址**”字段中输入更新源的地址。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **安装后运行数据库更新任务** | 如果选中此复选框，则应用程序安装后，数据库和应用程序模块更新任务将会启动。默认情况下已选定该选框。<br>如果您已将预先下载的应用程序数据库添加到安装包中，请清除此复选框。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **代理服务器地址** | 如果使用代理服务器来访问互联网，请使用以下格式之一指定代理服务器的地址：<br>• `[<connection protocol>://]<address of the proxy server>:<port>`，如果连接到代理服务器不需要身份验证；<br>• `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。指定 IPv6 地址时，请将其输入方括号中。<br>不支持通过 HTTPS 连接到代理服务器。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **安装内核源代码** | 如果选中此复选框，启动文件威胁防护，将自动在不支持 fanotify 的操作系统上启动内核模块的编译。默认情况下已选定该选框。<br>此设置仅适用于不支持 fanotify 的操作系统。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **使用图形用户接口** | 如果您计划安装并使用应用程序图形界面，请选中此复选框。用于安装图形界面的文件必须添加到安装包中。默认情况下已清空该复选框。<br>仅当应用程序在标准模式或 EDR Agent 模式下使用时，此参数才适用。 |
| **具有管理员角色的用户** | 要向其分配管理员角色的用户的名称。管理员角色允许在应用程序的图形界面和命令行中管理应用程序设置和任务设置，而无需使用 `sudo` 命令。 |
| **自动配置 SELinux** | 如果选中此复选框，则在应用程序初始配置期间，SELinux 会自动配置为与 Kaspersky Endpoint Security 协同工作。默认情况下已选定该选框。 |
| **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将用户从“kesladmin”和“keslaudit”特权组中自动移除。默认情况下已清空该复选框。<br>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** | 如果在完成安装过程后，您想要在禁用保护组件和扫描任务的情况下运行应用程序，请选中此复选框。<br>禁用保护组件的安装很方便，例如，为了重现应用程序操作中的问题并创建跟踪文件。<br>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。 |
| **安装后首次启动应用程序时启用跟踪** | 如果您希望在安装后首次启动应用程序时创建跟踪文件，请选中此复选框。<br>为了创建跟踪文件，系统会在 /var/log/kaspersky/kesl 目录下自动创建一个名为 kesl_startup.log 的文件。常规应用程序跟踪文件的大小限制不适用于此文件。跟踪在五分钟后或文件威胁防护任务启动后停止。 |

| 设置 | 描述 |
| --- | --- |
| **应用程序模式** | 这组设置包含**配置**按钮。单击此按钮将打开**应用程序模式**窗口。在此窗口中，您可以选择应用程序的模式。<br>• **用于保护工作站和服务器的标准模式**（默认值）。如果选中此选项，则应用程序将作为独立应用程序用于保护 Linux 工作站和服务器。<br>• "**Endpoint Detection and Response Agent**"。如果选择此选项，则应用程序将用于支持 Kaspersky Detection and Response 解决方案与受保护设备上的第三方反病毒解决方案协同工作。<br>• "**用于保护虚拟环境的 Light Agent**"。如果选择此选项，则应用程序将在 Light Agent 模式下使用（作为 Kaspersky Security for Virtualization Light Agent 的一部分）。<br>EDR Agent 模式和 Light Agent 模式不适用于配备 Elbrus CPU 的设备。 |
| **启用 Endpoint Detection and Response Expert (cloud)** | 选中此复选框以使用 Endpoint Detection and Response Expert (cloud) 集成。<br>在标准模式下，应用程序支持与 Endpoint Detection and Response Expert (cloud) 和 Endpoint Detection and Response Expert (on-premises) 集成。如果清除此复选框，则使用与 Endpoint Detection and Response Expert (on-premises) 的集成。<br>只有在标准模式下使用应用程序时，该设置才适用。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **受保护的虚拟机被用作服务器** | 要安装应用程序的虚拟机的角色：服务器或工作站。此复选框默认处于选中状态（虚拟机在虚拟基础架构中用作服务器）。<br>仅当在 Light Agent 模式下使用应用程序时，才应用此设置。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **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。默认情况下已清空该复选框。<br>仅当在 Light Agent 模式下使用应用程序时，才应用此设置。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **系统事件拦截** | 这组设置包含**配置**按钮。单击此按钮将打开**系统事件拦截设置**窗口。在此窗口中，您可以选择应用程序要使用的系统事件拦截模式：<br>• **Fanotify 技术**（默认值）。如果选择此选项，应用程序使用 fanotify 技术进行系统事件拦截。<br>• "**可更新内核模块**"。如果选择此选项，则会在应用程序安装期间安装可更新内核模块。应用程序使用该模块来拦截系统事件。<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br>此设置不适用于配备 Elbrus CPU 的设备。 |

| 设置 | 描述 |
| --- | --- |
| **如果可更新内核模块启动失败**<br>（**系统事件拦截设置**窗口）。 | 可更新内核模块启动失败时应用程序执行的操作：<br>• **使用 fanotify**（默认）。如果选择此选项，应用程序切换到 fanotify 技术进行系统事件拦截。<br>• **禁用系统事件拦截**如果应用程序不使用系统事件拦截，则不会执行实时文件扫描，并且设备的保护级别会降低。<br>如果选择了"**可更新内核模块**"拦截机制，则此选项可用。<br>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br>此设置不适用于配备 Elbrus CPU 的设备。 |
| **启用包管理器错误忽略模式** | 选中此复选框，以在安装应用程序时忽略软件包管理器错误。默认情况下已清空该复选框。<br>如果无法正常安装应用程序，可以使用此设置。<br>我们建议您仅在技术支持的监督下启用此设置。 |

# 预设配置文件

初始配置后，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，您可以在 kesl.ini 文件中编辑设置值。

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。

要应用对配置文件所做的更改，请重新启动 Kaspersky Endpoint Security 应用程序。

如果文件中缺少参数或指定了错误的参数值，应用程序将使用默认值。

| 设置 | 描述 | 值 |
| --- | --- | --- |
| **[General]** 部分包含以下设置： | | |
| `Locale` | Kaspersky Endpoint Security 发送到 Kaspersky Security Center 的应用程序事件所使用的区域设置。<br>图形界面和应用程序命令行的区域设置取自 `LANG` 环境变量。如果应用程序不支持此本地化，则默认使用英语本地化。 | 区域设置采用 RFC 3066 指定的格式。<br>如果未指定 `Locale` 设置，则使用操作系统区域设置。<br>如果应用程序无法检测操作系统的区域设置或不支持该区域设置，则使用英语（RFC 3066 格式的 en_US.UTF-8）对事件进行本地化。 |
| `PackageType` | 已安装的应用程序软件包的格式。<br>我们不建议手动更改此设置的值。该值在初始应用程序配置期间自动填充。 | `rpm` – 安装了 RPM 软件包。<br>`deb` – 安装了 DEB 软件包。 |
| `UseFanotify` | 使用 fanotify 技术拦截文件操作。<br>我们不建议手动更改此设置的值。此设置在应用程序的初始配置期间指定。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `true/yes` – 应用程序使用 fanotify 技术来拦截文件操作。<br>`false/no` – 不使用 fanotify 技术。 |
| `KsvlaMode` | 在 Light Agent 模式下使用 Kaspersky Endpoint Security。<br>我们不建议手动更改此设置的值。此设置在应用程序的初始配置期间指定。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `true/yes` 表示应用程序正以 Light Agent 模式使用。<br>`false/no` – 在标准模式下使用应用程序。 |
| `EndpointAgentMode` | 在 EDR Agent 模式下使用 Kaspersky Endpoint Security。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `true/yes` 表示应用程序处于 EDR Agent 模式。<br>`false/no` – 在标准模式下使用应用程序。 |
| `KcsMode` | 将 Kaspersky Endpoint Security 用作卡巴斯基容器安全解决方案中的文件威胁防护组件。<br>我们不建议手动更改此设置的值。此设置仅由卡巴斯基容器安全解决方案使用。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `true/yes` 表示该应用程序用作卡巴斯基容器安全解决方案中的文件威胁防护组件。<br>`false/no`（默认）表示应用程序使用 Kaspersky Endpoint Security 的其中一种模式（标准模式、EDR Agent 模式或 Light Agent 模式）。 |
| `StartupTraces` | 启用在应用程序启动时生成跟踪文件。 | `true/yes` – 在应用程序启动时创建跟踪文件。<br>`false/no`（默认值）– 在应用程序启动时不创建跟踪文件。 |
| `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）– 显示应用程序跟踪文件中可能包含个人数据的信息。<br>`false/no`（默认值）– 不显示跟踪文件中可能包含个人数据的信息。 |
| `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。<br>`false/no`（默认值）– 不启用异步跟踪。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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 RAM 使用限制（MB）。 | 默认值：8192。<br>我们建议将`ScanMemoryLimit`设置为低于`MaxMemory`设置，以避免扫描任务耗尽所有可用内存并导致应用程序重启。 |
| `MachineId` | 用户的唯一设备 ID。 | 在应用程序安装期间会自动填充该设置的值。 |
| `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/bl4control。 |
| `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）。<br>如果操作系统中的设置小于`MaxInotifyWatches`设置，则应用程序会将操作系统设置更改为`MaxInotifyWatches`值。 | 默认值：299987。 |
| `MaxInotifyInstances` | 对 /proc/sys/fs/inotify/max_user_instances 中设置的一个用户的文件和目录变化的订阅数限制。<br>如果操作系统中的设置小于`MaxInotifyInstances`设置，则应用程序会将操作系统设置更改为`MaxInotifyInstances`值。 | 默认值：4047。 |
| `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：20。 |
| `AdditionalDNSLookup` | 指示公共 DNS 的使用。<br>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：<br>1. Google Public DNS™ (8.8.8.8)。<br>2. Cloudflare® DNS (1.1.1.1)。<br>3. Alibaba Cloud® DNS (223.6.6.6)。<br>4. Quad9® DNS (9.9.9.9)。<br>5. CleanBrowsing (185.228.168.168)。 | `true/yes` – 使用公共 DNS 访问卡巴斯基服务器。<br>`false/no`（默认值）– 不使用公共 DNS 访问卡巴斯基服务器。<br>应用程序的请求可能包含域地址和用户的外部 IP 地址，因为应用程序与 DNS 服务器建立 TCP/UDP 连接。例如，在通过 HTTPS 交互时检查 Web 资源的证书需要此信息。如果应用程序使用公共 DNS 服务器，则数据处理规则受相应服务的隐私政策约束。 |
| `PanicThreshold` | 使用可更新内核模块时的最大异常停止次数。当达到指定值时，应用程序进入“安全”模式，在该模式中不会启动可更新内核模块。<br>此设置不适用于配备 Elbrus CPU 的设备。 | 默认值：3。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| SafeMode | 使用可更新内核模块时启用“安全”模式。在此模式下，应用程序不会启动可更新内核模块。<br>如果应用程序达到 PanicThreshold 设置中指定的最大异常停止次数，则会自动激活“安全”模式。<br>此设置不适用于配备 Elbrus CPU 的设备。 | true/yes 表示应用程序的“安全”模式已启用。<br>false/no （默认）表示应用程序的“安全”模式被禁用，应用程序正常运行。 |
| GetContainerName | 与 Kaspersky Managed Detection and Response 集成时，遥测中包含以下容器信息：<br>• 容器中发生的事件指示<br>• 容器命名空间 ID<br>• 容器名称<br>仅当您拥有容器扫描任务的授权许可且容器具有足够的生命周期时，才会传输容器名称。<br>此设置不适用于配备 Elbrus CPU 的设备。 | true/yes 表示在与 Kaspersky Managed Detection and Response 集成时，遥测中包含有关容器的扩展信息。<br>false/no 表示在与 Kaspersky Managed Detection and Response 集成时，遥测中不包含有关容器的扩展信息。 |
| UseIncreasedXdrEventsCache | 与 Detection and Response 解决方案集成时管理事件缓存。高性能与 RAM 占用之间需要权衡。 | true/yes （默认值）可最大限度减少磁盘 I/O，但会占用更多 RAM（100 MB）。<br>false/no 使用较少内存（约 5 MB），但代价是需要执行更多磁盘读写操作。 |
| FastShutdown | 应用程序停止或重新启动时快速关闭 kesl 进程。 | true/yes 可在应用程序停止时快速关闭 kesl 进程。<br>false/no （默认值）会在应用程序停止时禁用 kesl 进程的快速关闭。 |
| [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。<br>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 前缀的十六进制数。<br>默认值：0x100。<br>当应用程序在用作 Kubernetes 等分布式系统一部分的节点上运行时，为避免循环流量扫描，您需要使用高位更改网络数据包标记的值。例如：0x1000 或 0x10000（该标记限制为 32 位整数）。 |
| 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。<br>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 前缀的十六进制数。<br>默认值：0x200。<br>当应用程序在用作 Kubernetes 等分布式系统一部分的节点上运行时，为避免循环流量扫描，您需要使用高位更改网络数据包标记的值。例如：0x2000 或 0x20000（该标记限制为 32 位整数）。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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 前缀的十六进制数。<br>默认值：0x400。<br>当应用程序在用作 Kubernetes 等分布式系统一部分的节点上运行时，为避免循环流量扫描，您需要使用高位更改网络数据包标记的值。例如：0x4000 或 0x40000（该标记限制为 32 位整数）。 |
| `BypassNFlogMark` | 应用程序在扫描时将忽略的数据包的标记。 | 十进制值或带有 0x 前缀的十六进制数。<br>默认值：0x800。<br>**例如：**<br>忽略与指定设备相关的所有 TCP 流量：<br>`iptables -t mangle -A PREROUTING -s <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`<br>`iptables -t mangle -A OUTPUT -d <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`<br>忽略 HTTPS 服务器流量：<br>`iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j MARK --set-xmark 0x800/0x800`<br>`iptables -t mangle -A OUTPUT -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x800/0x800`<br>当应用程序在用作 Kubernetes 等分布式系统一部分的节点上运行时，为避免循环流量扫描，您需要使用高位更改网络数据包标记的值。例如：0x8000 或 0x80000（该标记限制为 32 位整数）。 |
| `ProxyRouteTable` | 路由表编号。 | 默认值：101。 |
| **[ScannerImpactStats]** 部分包含以下设置： | | |
| `CollectFileScanStatistics` | 启用对应用程序的文件和进程扫描统计数据进行计数。 | `true/yes`（默认值）启用对文件和进程扫描统计数字进行计数。<br>`false/no` 禁用对文件和进程扫描统计数字进行计数。 |
| `StatCollectionPeriod` | 事件段，在此期间应用程序会收集已扫描文件和检测的进程的统计信息，并将统计信息保存到跟踪文件和报告中。 | 默认值：10 分钟。 |
| `StatCollectionCount` | 应用程序在 `StatCollectionPeriod` 参数指定的时间间隔内计数的被扫描文件和检测进程的数量，这些数量包含在报告和跟踪文件中。 | 默认值：10。 |
| `ReportStatAmount` | 当天被扫描最多的文件和进程的报告中要写入的记录数。 | 默认值：20。 |
| **[Virtualization]** 部分包含以下设置： | | |
| `ServerMode` | 运行以 Light Agent 模式使用的 Kaspersky Endpoint Security 的受保护的虚拟机的角色：服务器或工作站。<br>我们不建议手动更改此设置的值。此设置在应用程序的初始配置期间指定。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `true/yes` – 受保护的虚拟机被用作服务器。<br>`false/no` – 受保护的虚拟机被用作工作站。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| VdiMode | 在以 Light Agent 模式使用应用程序时启用 VDI 保护模式。<br>我们不建议手动更改此设置的值。此设置在应用程序的初始配置期间指定。<br>此设置不适用于配备 Elbrus CPU 的设备。 | true/yes – 启用 VDI 保护模式。<br>false/no – 禁用 VDI 保护模式。 |
| **[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 HEADSHOT 信号的一刻开始计算。 | 默认值：2 分钟。 |
| StartupTimeout | 等待应用程序启动的最长时间（以分钟为单位），此后 Watchdog 服务器将启动重新启动 kesl 进程的程序。 | 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。<br>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 Watchdog 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 毫秒。 |
| 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。<br>如果在此时间间隔内没有从应用程序收到消息，Watchdog 服务器将开始重启 kesl 进程的程序。 | 默认值：2 分钟。 |
| ConnectTimeout | 从 kesl 进程启动那一刻起，应用程序与 Watchdog 服务器的连接的最大超时时间。<br>如果应用程序在此时间间隔内没有建立连接，Watchdog 服务器将开始重启 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 毫秒。 |
| 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。<br>如果 kesl 进程使用的驻留内存超过此限制，Watchdog 服务器将开始重启 kesl 进程的程序。 | off – 驻留集大小不受限制。<br><value>% – RAM 的 1% 到 100% 之间的值。<br><value>MB – 以兆字节为单位的值。<br>lowest/<value>%/<value>MB – 百分比值和以兆字节为单位的绝对值中的较小值。<br>highest/<value>%/<value>MB – 百分比值和以兆字节为单位的绝对值中的较大值。<br>auto – 最多 50% 的可用内存，但不少于 2 GB 且不超过 16 GB。<br>默认值：auto。 |
| MaxVirtualMemory | kesl 进程的虚拟内存的使用限制。<br>如果 kesl 进程使用的虚拟内存超过此限制，Watchdog 服务器将开始重启 kesl 进程的程序。 | off（默认值）– 虚拟内存大小不受限制。<br><value>MB – 以兆字节为单位的值。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `MaxSwapMemory` | kesl 进程的交换文件的大小限制。<br>如果 kesl 进程的交换文件超过此限制，Watchdog 服务器将开始重启 kesl 进程的程序。 | `off`（默认值）– 交换文件大小不受限制。<br>`<value>%` – RAM 的 0% 到 100% 之间的值。<br>`<value>MB` – 以兆字节为单位的值。<br>`lowest/<value>%/<value>MB` – 百分比值和以兆字节为单位的绝对值中的较小值。<br>`highest/<value>%/<value>MB` – 百分比值和以兆字节为单位的绝对值中的较大值。 |
| `TrackProductCrashes` | 当应用程序不稳定时，启用将设备状态从 Kaspersky Endpoint Security 发送到 Kaspersky Security Center 的功能。 | `true/yes` 可启用将设备状态信息从 Kaspersky Endpoint Security 发送到 Kaspersky Security Center。<br>`false/no`（默认）表示禁用将设备状态从 Kaspersky Endpoint Security 发送到 Kaspersky Security Center 的功能。 |
| `ProductHealthLogFile` | 用于应用程序稳定性监控的文件路径。 | 默认值：/var/opt/kaspersky/kesl/private/kesl_health.log. |
| `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` | 应用程序异常停止的最大次数，超过该次数后会显示关于应用程序运行不稳定的通知。 | 默认值：10。<br>如果值为 0，则不显示不稳定的应用程序通知。 |
| `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。 |
| `SyscallHangProbePeriod` | Watchdog 服务器调用 open 和 execve 系统函数并增加这些函数的成功计数器的周期。 | 默认值：3 秒。 |
| `SyscallHangCheckPeriod` | Watchdog 服务器检查 open 和 execve 函数的成功计数器的周期。<br>如果此时间之后计数器的值没有变化，Watchdog 服务器将启动重新启动 kesl 进程的程序。 | 默认值：32 秒。 |
| `DumpSuspendPeriod` | 等待创建应用程序转储文件的最长时间，在此期间 Watchdog 服务器会暂停检查应用程序活动。<br>如果此时间之后转储创建仍未完成，Watchdog 服务器将启动重新启动 kesl 进程的程序。 | 可能的值：1-30 分钟。<br>默认值：2 分钟。 |
| `TimeoutAfterCoredump` | Watchdog 服务器在发送 SIGTRAP 信号作为异常进程终止程序的一部分后，暂停向 kesl 进程发送其他信号的最大持续时间。 | 默认值：2 分钟。<br>我们建议将 `TimeoutAfterCoredump` 设置为大于或等于 `DumpSuspendPeriod`。<br>您可以使用以下单位来指定此设置：<br>• `<n> day\|days\|d` 天<br>• `<n> hour\|hours\|hr\|h` 小时<br>• `<n> minute\|minutes\|min\|m` 分钟<br>• `<n> second\|seconds\|sec\|s` 秒<br>• `<n> [msec\|ms]` 毫秒<br>如果没有指定单位，应用程序会将该值解释为毫秒。 |
| `TimeoutMaxCleanPeriod` | 清除操作系统的 Firewall 规则的进程所分配的最长时间。如果该进程未在此时间内发出完成信号，Watchdog 服务器会将该进程视为已冻结。 | 默认值：10 秒。 |
| `TimeoutAfterClean` | Watchdog 服务器向清理进程发送 SIGTERM 信号后，清除操作系统的 Firewall 规则的进程完成操作所分配的最长时间。 | 默认值：10 秒。 |
| 默认情况下，配置文件中没有**[Environment]**部分。 | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `ExperimentalContainerdSupport` | 在运行容器监控组件时启用对 containerd 环境的支持。<br>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。<br>此设置不适用于配备 Elbrus CPU 的设备。 | `true/yes` – 在容器监控组件的运行中启用对 containerd 环境的支持。<br>`false/no` – 在容器监控组件的运行中不启用对 containerd 环境的支持。 |
| `ReduceSWMemoryConsumption` | 限制行为检测组件处理事件队列时的内存消耗。<br>设置内存限制会对威胁检测产生负面影响，包括作为与 Detection and Response 解决方案集成的一部分而传输的遥测的质量。如果没有其他选项可解决内存消耗过高的问题，建议仅在高负载系统上，并且在联系技术支持获取具体说明后设置限制。 | 1 – 限制行为检测组件处理事件队列时的内存使用量。<br>0（默认值）– 不限制内存使用量。<br>更改此设置后，必须重新启动应用程序。 |

# 命令行任务的默认设置

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。

“`Rollback`”和“`License`”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

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible
```

```
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

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible
```

```
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=*
```

## Default settings for the Scan_File task (ID:3)

```
ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0
```

```
QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

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

QueueScanTasks=No

ActionOnThreat=DisinfectDeleteIfNotPossible

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=*
```

## 更新任务（ID：6）的默认设置

```
ConnectionTimeout=10

ApplicationUpdateMode=DownloadOnly

[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

## 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

AllowToRequestTemporaryAccess=No

[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
```

```
ActionOnThreat=DisinfectDeleteIfNotPossible

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

QueueScanTasks=No
```

> 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

UseAEP=No

AEPMode=Block

UseTelemetryMonopolyMode=Yes

TelemetrySource=Default
```

## 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

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

## KATAEDR 任务（ID：24）的默认设置

```
Mode=EDRKATA

UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30
```

```
UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

## Web_Control 任务（ID：26）的默认设置

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

## Standalone_Sandbox 任务（ID：29）的默认设置

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly

QuarantineFile=Yes

ScanCriticalAreas=Yes
```

```
CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

## KATANDR 任务（ID：31）的默认设置

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

## KUMA 任务（ID：33）的默认设置

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

## 邮件威胁防护任务（ID: 35）的默认设置

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible

ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No

TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt
```

```
[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi

[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr

[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

## BadUSB 攻击防护任务（ID: 37）的默认设置

```
MaxAuthAttempts=5

TimeoutAfterAttempts=5

ProhibitOnScreenKeyboard=No

ProhibitBarcodeScanner=Yes
```

## KATANDR 任务（ID：31）的默认设置

```
ConnectionTimeout=10

RequestTimeout=10

SynchronizationPeriod=5

UseTunnel=No

TunnelAddress=127.0.0.1

TunnelPort=443

[Endpoints.item_0000]

Address=127.0.0.1
Port=443
EnableTelemetry=Yes
[TelemetrySettings]

ConnectionTimeout=10
RequestTimeout=10
OnlyTaggedEvents=No
UseTunnel=No
TunnelAddress=127.0.0.1
TunnelPort=443
[TelemetrySettings.Endpoints.item_0000]

Address=127.0.0.1
Port=443
[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
```

```
EventLimitExceededPercentage=15
MaximumNumberOfEventsInPackage=1024
```

# 附录 2.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下列部分：

   `[ExcludedFromScanScope.item_<项目编号>]`

   `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_<项目编号>]`

   `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>`

# 附录 3.与外部服务交互的设置

Kaspersky Endpoint Security 使用以下网络设置和加密设置与外部服务进行交互。

与外部服务交互的设置

| 服务和协议的网络地址 | 描述 |
| --- | --- |
| activation-v2.kaspersky.com/activationservice/activationservice.svc<br>协议：HTTPS<br>端口：443 | 应用程序激活。 |

| 服务和协议的网络地址 | 描述 |
| --- | --- |
| s00.upd.kaspersky.com<br>s01.upd.kaspersky.com<br>s02.upd.kaspersky.com<br>s03.upd.kaspersky.com<br>s04.upd.kaspersky.com<br>s05.upd.kaspersky.com<br>s06.upd.kaspersky.com<br>s07.upd.kaspersky.com<br>s08.upd.kaspersky.com<br>s09.upd.kaspersky.com<br>s10.upd.kaspersky.com<br>s11.upd.kaspersky.com<br>s12.upd.kaspersky.com<br>s13.upd.kaspersky.com<br>s14.upd.kaspersky.com<br>s15.upd.kaspersky.com<br>s16.upd.kaspersky.com<br>s17.upd.kaspersky.com<br>s18.upd.kaspersky.com<br>s19.upd.kaspersky.com<br>协议：HTTPS<br>端口：443 | 更新应用程序数据库和模块。 |

| 服务和协议的网络地址 | 描述 |
| --- | --- |
| p00.upd.kaspersky.com<br>p01.upd.kaspersky.com<br>p02.upd.kaspersky.com<br>p03.upd.kaspersky.com<br>p04.upd.kaspersky.com<br>p05.upd.kaspersky.com<br>p06.upd.kaspersky.com<br>p07.upd.kaspersky.com<br>p08.upd.kaspersky.com<br>p09.upd.kaspersky.com<br>p10.upd.kaspersky.com<br>p11.upd.kaspersky.com<br>p12.upd.kaspersky.com<br>p13.upd.kaspersky.com<br>p14.upd.kaspersky.com<br>p15.upd.kaspersky.com<br>p16.upd.kaspersky.com<br>p17.upd.kaspersky.com<br>p18.upd.kaspersky.com<br>p19.upd.kaspersky.com<br>downloads.kaspersky-labs.com<br>协议：HTTP<br>端口：80 | 更新应用程序数据库和模块。 |
| downloads.upd.kaspersky.com<br>协议：HTTPS<br>端口：443 | • 更新应用程序数据库和模块。<br>• 正在检查对卡巴斯基服务器的访问权限。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：<br>1. Google Public DNS (8.8.8.8)。<br>2. Cloudflare DNS (1.1.1.1)。<br>3. Alibaba Cloud DNS (223.6.6.6)。<br>4. Quad9 DNS (9.9.9.9)。<br>5. CleanBrowsing (185.228.168.168)。<br>应用程序的请求可能包含域地址和用户的外部 IP 地址，因为应用程序与 DNS 服务器建立 TCP/UDP 连接。例如，在通过 HTTPS 交互时检查 Web 资源的证书需要此信息。如果应用程序使用公共 DNS 服务器，则数据处理规则受相应服务的隐私政策约束。 |
| ds.kaspersky.com<br>协议：HTTPS<br>端口：443 | 使用卡巴斯基安全网络。 |
| ksn-a-stat-geo.kaspersky-labs.com<br>ksn-file-geo.kaspersky-labs.com<br>ksn-verdict-geo.kaspersky-labs.com<br>ksn-url-geo.kaspersky-labs.com<br>ksn-a-p2p-geo.kaspersky-labs.com<br>ksn-cinfo-geo.kaspersky-labs.com<br>协议：KSN<br>端口：443，1443 | 使用卡巴斯基安全网络。 |

| 服务和协议的网络地址 | 描述 |
| --- | --- |
| `click.kaspersky.com`<br>协议：`HTTPS`<br>端口：`443` | 打开用户接口上的链接。 |
| `crl.kaspersky.com`<br>`ocsp.kaspersky.com`<br>协议：`HTTP`<br>端口：`80` | 公共密钥基础架构(PKI)。<br>这些服务器（crl.kaspersky.com）是公钥基础设施（PKI）的一部分，是验证卡巴斯基数字签名证书有效性所必需的。CRL 服务器提供已吊销证书的列表。OCSP 服务允许实时查询特定证书的状态。这些组件可维护与数字证书的交互的安全性，并提供针对可能攻击的保护。 |

# 附录 4.快速可移动驱动器扫描的文件扩展名

com – 大小不超过 64 KB 的应用程序的可执行文件

exe – 可执行文件或自解压存档

sys – Microsoft Windows 系统文件

prg – dBase™ 程序文字、Clipper 或 Microsoft Visual FoxPro®，或 WAVmaker 程序

bin – 二进制文件

bat – 批文件

cmd – Microsoft Windows NT 的命令文件（与 DOS 批处理文件类似）、OS/2

dpl – 压缩的 Borland Delphi 库

dll – 动态链接库

scr – Microsoft Windows 屏保

cpl – Microsoft Windows 控制面板模块

ocx – Microsoft OLE（对象链接和嵌入）对象

tsp – 以分时模式运行的程序

drv – 设备驱动程序

vxd – Microsoft Windows 虚拟设备驱动程序

pif – 程序信息文件

lnk – Microsoft Windows 链接文件

reg – Microsoft Windows 系统注册表键文件

ini – 包含 Microsoft Windows、Windows NT 和某些应用程序配置数据的配置文件

cla – Java 类

vbs – Visual Basic® 脚本

vbe – BIOS 视频扩展程序

js, jse – JavaScript source text

htm – 超文本文档

htt – Microsoft Windows 超文本标头

hta – Microsoft Internet Explorer® 超文本程序

asp – Active Server Pages 脚本

chm – 编撰的 HTML 文件

pht – 带有 PHP 脚本的 HTML 文件

php – 集成到 HTML 文件的脚本

wsh – Microsoft Windows Script Host 文件

wsf – Microsoft Windows 脚本

the – Microsoft Windows 95 桌面壁纸文件

hlp – Win 帮助文件

msg – Microsoft Mail 邮件

plg – 邮件

mbx – 已保存的 Microsoft Office Outlook 邮件

doc* – Microsoft Office Word 文档，例如：doc（Microsoft Office Word 文档）、docx（带 XML 支持的 Microsoft Office Word 2007 文档）、docm（带宏支持的 Microsoft Office Word 2007 文档）

dot* – Microsoft Office Word 文档模块，例如 dot（Microsoft Office Word 文档模板）、dotx（Microsoft Office Word 2007 文档模板）、dotm（带宏支持的 Microsoft Office Word 2007 文档模板）

fpm – 数据库程序，Microsoft Visual FoxPro 启动文件

rtf – 富文本格式文档

shs – Windows Shell Scrap Object Handler 片段

dwg – AutoCAD® 图纸数据库

msi – Microsoft Windows Installer 安装包

otm – 适用于 Microsoft Office Outlook 的 VBA 项目

pdf – Adobe Acrobat 文档

swf – Shockwave® Flash 数据包文档

jpg, jpeg – 压缩图像格式

emf – 增强元文件格式文件；

ico – 对象图标文件

ov? – Microsoft Office Word 可执行文件

xl* – Microsoft Office Excel 文档和文件，例如：xla 对应 Microsoft Office Excel、xlc 对应图表、xlt 对应文档模板、xlsx 对应 Microsoft Office Excel 2007 工作簿、xltm 对应支持宏的 Microsoft Office Excel 2007 工作簿、xlsb 对应二进制格式（非 XML）的 Microsoft Office Excel 2007 工作簿、xltx 对应于 Microsoft Office Excel 2007 模板、xlsm 对应于支持宏的 Microsoft Office Excel 2007 模板、xlam 对应于支持宏的 Microsoft Office Excel 2007 插件

pp* – Microsoft Office PowerPoint® 文档和文件，例如：pps 代表 Microsoft Office PowerPoint 幻灯片、ppt 代表幻灯片、pptx 代表 Microsoft Office PowerPoint 2007 幻灯片、pptm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、potx 代表 Microsoft Office PowerPoint 2007 幻灯片模板、potm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppsx 代表 Microsoft Office PowerPoint 2007 幻灯片、ppsm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppam 代表支持宏的 Microsoft Office PowerPoint 2007 插件

md* – Microsoft Office Access® 文档和文件，例如：mda 代表 Microsoft Office Access 工作组，mdb 代表数据库

sldx – Microsoft PowerPoint 2007 幻灯片

sldm – 支持宏的 Microsoft PowerPoint 2007 幻灯片

thmx – Microsoft Office 2007 主题

# 附录 5.消息模板中的变量

设备控制和 Web 控制组件允许您配置 Kaspersky Endpoint Security 向尝试访问被阻止的设备、应用程序或资源，或尝试执行潜在危险操作的用户显示的消息模板。

提供了特殊变量来管理消息模板（例如，`%USER_NAME%`）。变量允许将单个消息模板用于不同的计算机。生成消息时，Kaspersky Endpoint Security 从操作系统设置中检索变量的值，并将其插入到与特定计算机、用户和事件匹配的消息中。

**设备控制消息模板中的变量**

您可以在用户消息模板或管理员消息模板中使用以下变量：

- **用户** – `%USER_NAME%`。

  生成该消息的计算机上的当前用户账户名称，以“`<device name>\<user alias>`”格式（例如，`DESKTOP-123\John.Smith`）。

- **计算机名称** – %COMPUTER_NAME%。

  设备被锁定的计算机名称。

- **规则名称** – %RULE%。

  阻止设备的规则的名称。

- **规则触发日期** – %DATE%。

  设备被锁定的日期，格式为 DD.MM.YYYY。

- **规则触发时间** – %TIME%。

  设备被锁定的时间，格式为 HH:MM。

- **设备名称** – %DEVICE_NAME%。

  被阻止设备的名称。

- **设备类型** – %DEVICE_TYPE%。

  被阻止的设备类型（例如，打印机、可移动驱动器、CD/DVD 驱动器）。

- **设备型号** – %DEVICE_VIDPID%。

  被阻止设备的型号（例如，VID_1234&PID_5678）。

- **设备 ID** – %DEVICE_ID%。

  被阻止设备的 ID（例如，
  SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000）。

- **设备操作** – %OPERATION%。

  对该设备进行的禁止操作类型。

**Web 控制消息模板中的变量**

您可以在用户消息模板或管理员消息模板中使用以下变量：

- **用户** – %USER_NAME%。

  生成该消息的计算机上的当前用户账户名称，以“<device name>\<user alias>”格式（例如，DESKTOP-123\John.Smith）。

- **网络资源地址** – %CANONIC_REQUEST_URL%。

  被阻止的 Web 资源的地址。

- **规则名称** – %RULE%。

  阻止该 Web 资源的规则名称。

- **用于发送消息的电子邮件** – %COMPLAIN_EMAIL%。

  用于接收关于 Web 资源被阻止反馈的电子邮件地址。点击电子邮件地址会打开一个窗口，用户可以在该窗口中向管理员发送消息。

- **内容类别的名称** – %CONTENT_CATEGORY_LIST%。

  被阻止资源所属的网站类别（例如，*支付系统*）。

- **数据类型类别的名称** – %TYPE_CATEGORY_LIST%。

  被阻止的 Web 资源的数据类型类别（例如，*图形文件*）。

- **到所请求网络资源的链接** – %CONTINUE_PAGE%。

  指向所请求网页的链接（例如，`http://www.example.com/pagename.html`）。

- **网站链接** – %CONTINUE_SITE%。

  指向包含所请求网页的网站的链接（例如，`http://www.example.com/`）。

- **用于访问域的链接** – %CONTINUE_DOMAIN%。

  点击此链接即可访问该域名下的所有现有网页。例如，如果被阻止网页的地址是 `http://www.example.com`，%CONTINUE_DOMAIN% 变量被替换为 `http://*.example.com` 链接。点击此链接即可访问基本域名 `http://www.example.com/` 下的所有网址，包括子域名。例如 `http://start.example.com/*` 或者 `http://domain.domain.example.com/*`，其中 * 字符代表任意字符序列（包括空字符串）。

# 附录 6.应用程序事件

有关每个 Kaspersky Endpoint Security 组件的运行、数据加密事件、每个恶意软件扫描任务、更新任务和完整性检查任务的完成情况以及应用程序的整体运行的信息，都记录在 Kaspersky Security Center 事件日志和操作系统事件日志 (syslog) 中。

## 严重

### 系统完整性违规

| | |
|---|---|
| 状态 | ⊗ |
| 组件 | 系统完整性监控 |
| Linux 事件 ID | 0 |
| Kaspersky Security Center 事件 ID | GNRL_EV_FIM_ALARM |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

### 应用程序启动被拒绝

| | |
|---|---|
| 状态 | ⊗ |
| 组件 | 应用程序控制 |
| Linux 事件 ID | 122 |
| Kaspersky Security Center 事件 ID | GNRL_EV_APPLICATION_LAUNCH_DENIED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

### 检测到恶意对象（本地数据库）

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 文件威胁防护<br>邮件威胁防护<br>行为检测<br>漏洞利用防御<br>Sandbox |
| Linux 事件 ID | 6 |
| Kaspersky Security Center 事件 ID | GNRL_EV_VIRUS_FOUND |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 已超出系统完整性监控事件限制

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 系统完整性监控 |
| Linux 事件 ID | 70 |
| Kaspersky Security Center 事件 ID | GNRL_EV_FIM_ALARM_OVERFLOW |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 禁止对设备执行操作

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 设备控制 |
| Linux 事件 ID | 94 |
| Kaspersky Security Center 事件 ID | GNRL_EV_DEVCTRL_DEV_PLUG_DENIED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 检测到网络攻击

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 网络威胁防护 |
| Linux 事件 ID | 102 |
| Kaspersky Security Center 事件 ID | GNRL_EV_ATTACK_DETECTED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 访问被拒绝（本地数据库）

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | Web 控制 |
| Linux 事件 ID | 190 |
| Kaspersky Security Center 事件 ID | GNRL_EV_WEB_URL_BLOCKED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

# 警告

### 无法清除

| | |
|---|---|
| 状态 | ⚠ |
| 组件 | 文件威胁防护<br>邮件威胁防护 |
| Linux 事件 ID | 10 |
| Kaspersky Security Center 事件 ID | GNRL_EV_OBJECT_NOTCURED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

### 有关有害内容的警告（本地数据库）

| | |
|---|---|
| 状态 | ⚠ |
| 组件 | Web 控制 |
| Linux 事件 ID | 192 |
| Kaspersky Security Center 事件 ID | GNRL_EV_WEB_URL_WARNING |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

### 关于阻止访问网页的管理员消息

| | |
|---|---|
| 状态 | ⚠ |
| 组件 | Web 控制 |
| Linux 事件 ID | 196 |
| Kaspersky Security Center 事件 ID | GNRL_EV_WC_USER_REQUEST |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

# 信息性消息

### 对象已清除

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 文件威胁防护<br>邮件威胁防护 |
| Linux 事件 ID | 9 |
| Kaspersky Security Center 事件 ID | GNRL_EV_OBJECT_CURED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

### 对象已删除

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 文件威胁防护<br>邮件威胁防护 |
| Linux 事件 ID | 8 |
| Kaspersky Security Center 事件 ID | GNRL_EV_OBJECT_DELETED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 已允许应用程序启动

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 应用程序控制 |
| Linux 事件 ID | 120 |
| Kaspersky Security Center 事件 ID | GNRL_EV_APPLICATION_LAUNCHED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志 | 未配置 |

## 在测试模式下已允许应用程序启动

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 应用程序控制 |
| Linux 事件 ID | 121 |
| Kaspersky Security Center 事件 ID | GNRL_EV_APP_LAUNCH_TESTED_ALLOW |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 在测试模式下已拒绝应用程序启动

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 应用程序控制 |
| Linux 事件 ID | 123 |
| Kaspersky Security Center 事件 ID | GNRL_EV_APP_LAUNCH_TESTED_DENIED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 设备已连接

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 设备控制 |
| Linux 事件 ID | 90 |
| Kaspersky Security Center 事件 ID | GNRL_EV_DEVCTRL_DEV_PLUGGED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

## 设备已断开连接

| | |
|---|---|
| 状态 | ⓘ |
| 组件 | 设备控制 |
| Linux 事件 ID | 91 |
| Kaspersky Security Center 事件 ID | GNRL_EV_DEVCTRL_DEV_UNPLUGGED |
| 日志 (syslog)（默认） | – |
| Kaspersky Security Center 事件日志（默认） | ✓ |

# 附录 7.返回代码

初始配置向导的返回代码

0 – 已成功完成安装。

**严重错误**

1 – 未知错误（除下列严重错误外的所有其他严重错误，例如：系统错误、内存不足、文件打开错误等）。

2 – 初始配置文件包含无效参数。

3 – 安装或更新应用程序失败。

4 – 无法删除应用程序。

5 – 无法启动应用程序。可能的原因：访问权限配置错误。检查是否只有根账户有权写入以下目录：/、/opt、/opt/kaspersky、/var、/var/opt、/var/opt/kaspersky、/usr 和 /usr/lib64。

6 – 安装之前未执行必要的操作。

7 – 更新应用程序失败。不支持安装较早版本的应用程序。

8 – 从特权组中删除用户失败。

9 – 未能为应用程序安装创建唯一的 MachineID。

10 – 启动或重新启动应用程序失败。

11 – 尚未接受最终用户授权许可协议(EULA)和隐私策略的条款和条件。

12 – 该应用程序不能同时在 Light Agent 模式和 EDR Agent 模式下使用。

13 – 未找到 Astra Linux 中封闭软件环境模式所需的 astra-digsig-oldkeys 软件包。

14 – 初始配置已开始。

15 – 必须删除作为 Kaspersky Security for Virtualization 5.2 Light Agent 解决方案的一部分安装的 Light Agent for Linux 组件。

16 – 必须安装 Kaspersky Security Center 网络代理。

17 – 由于应用程序进程已在运行，无法启动初始配置向导。

18 – 不支持 fanotify。编译文件威胁防护的内核模块失败。

19 – 安装需要管理员权限。

20 – 应用程序服务尚未启动。

21 – 应用程序更新已回滚。

22 – 不支持将 EDR Agent 模式或 Light Agent 模式下的应用程序与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成。

**警告**

71 – 安装过程中出现多个警告。请参见安装日志以了解更多详细信息。

72 – 更新应用程序数据库失败。

75 – 需要重启操作系统。

76 – 应用 KSN 设置失败，或未接受 KSN 声明的条款和条件。

77 – 启动可更新内核模块失败。

79 – 安装或更新应用程序的图形界面包失败。

80 – 下载应用程序数据库失败。

81 – 由于网络问题，应用程序激活终止并显示错误。

82 – 该应用程序由策略管理。

83 – 应用程序 GUI 未启动。

84 – 分配管理员角色失败。未找到指定的用户。

85 – 应用程序包只能在包管理器的错误忽略模式下安装或更新。

86 – 删除应用程序的图形界面包失败。

87 – 应用程序包只能在包管理器的错误忽略模式下删除。

88 – 将管理员角色分配给用户失败。

89 – 授权许可密钥无效。

90 – 设置更新任务的计划失败。

kesl-control 命令行实用程序的返回码

0 – 命令/任务成功完成。

1 – 命令语法中存在一般错误。

2 – 所传递的应用程序设置中存在错误。

64 — Kaspersky Endpoint Security 未运行。

66 – 应用程序数据库未加载（仅由 `kesl-control --app-info` 命令使用）。

67 – 由于网络问题，应用程序激活终止并显示错误。

68 – 无法执行该命令，因为应用程序由策略管理。

69 – 应用程序位于 Amazon Paid Ami 基础设施中。

70 – 尝试启动已在运行的任务、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恢复正在运行的任务。

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 – 尝试设置会影响应用程序运行的应用程序控制任务设置，而未使用 `--accept` 选项确认这些设置。

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 权限的用户才应具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。

78 – 无法运行命令/任务，因为应用程序正以 Light Agent 模式使用。

79 – 无法运行该命令，因为应用程序正以标准模式使用。

80 – 由于网络问题，更新下载操作失败。

81 – 设备上安装的操作系统版本不支持该组件。

128 – 未知错误。

65–所有其他错误。

# 附录 8.准备包含应用程序数据库的存档文件

在手动创建 Kaspersky Endpoint Security 安装包时，您可以向其中添加之前下载的应用程序数据库。如果您使用的是带有集成数据库的安装包，则应用程序和数据库一起安装；在这种情况下，您不需要在安装后立即更新数据库。

向安装包添加应用程序数据库会增大安装包。

对于受保护设备上操作系统的每种架构和位数组合，您都需要一组单独的应用程序数据库。您可以在安装包中添加包含一组或多组应用程序数据库的归档文件。要准备每组应用程序数据库，您需要一个已安装在设备上的 Kaspersky Endpoint Security 应用程序实例，该设备运行的操作系统需具有相匹配的架构和位数。

*要准备包含数据库的归档文件：*

1. 在设备上使用 Kaspersky Security Center或使用命令行安装 Kaspersky Endpoint Security 并执行初始配置。
2. 更新设备上的应用程序数据库。您可以在应用程序初始配置期间更新数据库，或在安装后通过在命令行中运行 *Update* 任务或在 Kaspersky Security Center 中运行 *Update* 任务来更新数据库。
3. 根据受保护设备上操作系统的架构和位数，为数据库创建目录：
   - 如果应用程序安装在 64 位操作系统上，则为 x86_64
   - 如果应用程序安装在 32 位操作系统上，则为 i386
   - 如果应用程序安装在适用于 Arm 架构的 64 位操作系统上，则为 arm64
   - 如果应用程序安装在适用于 Elbrus 架构的 64 位操作系统上，则为 e2k
4. 将 /var/opt/kaspersky/kesl/private/updates 目录的内容复制到创建的数据库目录中。
5. 将创建的数据库目录添加到 kesl-bases.tgz 归档文件中。

   如果要创建用于在具有不同架构和位数的多个操作系统上进行安装的安装包，您需要准备多个包含数据库的目录，并将它们全部添加到 kesl-bases.tgz 归档文件中。

默认情况下，数据库更新任务会在安装 Kaspersky Endpoint Security 应用程序后启动。如果您要从集成了数据库的安装包安装应用程序，请在安装应用程序后禁用数据库更新任务。您可以在已创建的安装包的属性中或在 autoinstall.ini 配置文件中配置此设置（`UPDATE_EXECUTE=No`）。

# 附录 9.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 OpenIOC 格式版本 1.0 和 1.1 中带有 IOC 或 .XML 扩展名的 IOC 文件，OpenIOC 格式版本是描述入侵指标的开放标准。
- 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。如果存在具有相同标识符的 IOC 文件，则可能会影响任务执行结果。
- 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 文件**

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：<br>• `is`<br>• `isnot`（作为集合排除项）<br>• `contains`<br>• `containsnot`（作为集合排除项）<br><br>OpenIOC 1.1：<br>• `is`<br>• `contains`<br>• `starts-with`<br>• `ends-with`<br>• `matches`<br>• `greater-than`<br>• `less-than` |
| **支持的条件属性** | OpenIOC 1.1：<br>• `preserve-case`<br>• `negate` |
| **支持的运算符** | `AND`<br>`OR` |
| **支持的数据类型** | `"date"`：日期（适用条件：`is`、`greater-than`、`less-than`）<br>`"int"`：整数（适用条件：`is`，`greater-than`，`less-than`）<br>`"string"`: string（适用条件：`is`、`contains`、`matches`、`starts-with`、`ends-with`）<br>`"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。<br>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：<br>• OpenIOC 1.0：<br>在`Content`字段中使用`TO`运算符：<br>`<Content type="int">49600 TO 50700</Content>`<br>`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`<br>`<Content type="int">[154192 TO 154192]</Content>`<br>• OpenIOC 1.1：<br>  • 使用`greater-than`和`less-than`条件<br>  • 在 `Content` 字段使用 `TO` 运算符<br><br>如果指标以`ISO 8601, Zulu time zone, UTC`格式指定，则应用程序支持`date`和`duration`数据类型的解释。 |

# 法律通告

## 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。

有关在使用应用程序期间获得并传输给卡巴斯基的信息的处理、存储和销毁的详细信息，请阅读最终用户授权许可协议、卡巴斯基安全网络声明以及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 在标准模式或 EDR Agent 模式下使用，并使用激活码激活，则为了验证应用程序的使用是否合法，以及获取有关应用程序分发和使用情况的统计信息，您同意自动向卡巴斯基提供以下信息：

- 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 在标准模式或 EDR Agent 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提供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 Kaspersky Endpoint Security 在 Light Agent 模式下用作 Kaspersky Security for Virtualization Light Agent 的一部分，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），并在应用程序运行期间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、受保护的虚拟机的 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的虚拟机的安全标签的信息。受保护的虚拟机的 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 会将受保护的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：受保护的虚拟机的标识符；受保护的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：有关受保护的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；受保护的虚拟机的标识符 (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
    - 应用程序策略与管理插件版本
    - 应用程序管理插件下载网址
    - 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
- 群组任务和本地任务的当前状态、执行结果以及任务设置。
- 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）及规则应用结果的信息
- 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
- 扫描任务统计数据：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；扫描的容器和镜像数量

    - 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

卡巴斯基安全网络向卡巴斯基提供的数据集取决于卡巴斯基安全网络的模式。

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。

基本 KSN 模式下的数据提供

如果您在基本 KSN 模式下使用卡巴斯基安全网络（在 Web Console 中启用**使用卡巴斯基安全网络 (KSN)**拨动开关，并取消选中**使用扩展 KSN 模式**复选框，且在管理控制台中选择**基本 KSN 模式**选项），则接受卡巴斯基安全网络声明的条款和条件，即表示您同意自动向卡巴斯基提供以下信息。

### 扩展 KSN 模式下的数据提供

如果您在扩展 KSN 模式下使用卡巴斯基安全网络（在 Web Console 中启用**使用卡巴斯基安全网络 (KSN)**拨动开关，并选中**使用扩展 KSN 模式**复选框，且在管理控制台中选择**扩展 KSN 模式**选项），则接受卡巴斯基安全网络声明的条款和条件，即表示您同意除上述信息外，自动向卡巴斯基提供以下信息。

### 在扩展 KSN 模式下与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成时的数据提供

如果您将 Kaspersky Endpoint Security 作为 Kaspersky Endpoint Detection and Response Expert (on-premises) 的一部分使用，并且在扩展模式下使用卡巴斯基安全网络，则接受卡巴斯基安全网络声明的条款，即表示您同意除上述所列信息外，自动向卡巴斯基提供以下信息。

### 在基本模式下或 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security 时的数据提供

如果您在标准模式或 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，并且在扩展模式下使用卡巴斯基安全网络，则接受卡巴斯基安全网络声明的条款即表示您同意除上述信息外，自动向卡巴斯基提供以下信息：

## 与 Kaspersky Endpoint Detection and Response Optimum 集成时提供的数据

### 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
    - 处理参数
    - 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
    - 进程开始的日期和时间
- 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
    - 卷字母
    - 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
- 已处理对象的相关信息：
  - 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
- 所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
- 已处理对象的全名
- 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
- 所处理对象的大小；
- 正在处理的对象的文件属性；
- 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
- 最后修改文件的应用程序的名称
- 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 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

# 与 Kaspersky Endpoint Detection and Response (KATA) 组件集成时提供的数据

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 存储以下信息，其中可能包含个人和机密数据：

- 提供与 Kaspersky Endpoint Detection and Response (KATA) 交互的中央节点服务器的地址（以下简称*KATA 服务器*）。
- 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) 集成的客户端证书
- 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 Expert (on-premise) 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
  - 授权许可密钥状态
- 任务执行报告中对 EDR Expert (on-premise) 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。
- 对于隔离的对象：
  - 文件路径
  - 文件大小
  - 隔离时分配的文件 ID
  - 原始文件删除标志
- 对于从隔离区获取的文件：
  - 隔离时分配的文件 ID
- 对于被阻止的可执行文件或脚本执行：
  - 进程 ID
  - 父进程 ID
  - 系统 ID
  - 登录会话 ID
  - 进程状态
  - 执行拦截的日期和时间
- 对于办公应用程序禁止打开的文档：
  - 进程 ID
  - 文件 ID
  - 执行拦截的日期和时间

- 有关文件的信息：
  - 文件的唯一 ID
  - 对象的 MD5 哈希值
  - 文件内容
- 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 ID
    - 进程 ID
    - 启动该进程的命令行选项
    - 会话 ID
    - 进程开始的日期和时间
    - 启动进程的用户和组的信息（名称和 ID）
  - 关于获取另一进程内存访问权限的进程的信息：
    - 进程 ID
    - 注入方法和地址。
    - 用于修改进程的命令行（包括参数）。
    - 进程的系统调用参数

- 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
- 有关将库加载到进程地址空间的信息：已加载库的 ID
- 有关已建立网络连接的信息：
  - 本地 IP 地址
  - 远程 IP 地址
  - 连接方向
  - 协议
- 在某个端口上监听外部网络连接的进程信息：
  - 本地地址（端口和 IP 地址）
  - 协议

- DNS 服务器查询信息：
  - 所查询资源的域名
  - 所查询资源的 IP 地址
  - DNS 服务器 IP 地址
  - 查询类型

此处列出的信息也可以保存在跟踪文件和转储文件中。

# 与 Kaspersky Endpoint Detection and Response Expert (on-premises) 组件集成时提供的数据

将 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成时，Kaspersky Endpoint Security 会存储以下信息，其中可能包含个人数据和机密数据：

- 用于与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的服务器列表。
- 提供与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的服务器的证书公钥。
- 用于与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的客户端证书。
- 用于在代理服务器上进行身份验证的凭据。
- 负责与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的服务器的同步频率设置，以及该服务器的数据传输设置。
- 处理与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的服务器的连接状态，以及客户端和服务器证书错误的相关信息。
- 来自用于与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的服务器的任务的参数：
  - 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

当 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成时，该应用程序会保存并可将以下数据传输到 Integration Server：

- 对 EDR Expert (on-premises) 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
  - 授权许可密钥状态
- 任务执行报告中对 EDR Expert (on-premises) 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 YARA 规则，将返回搜索结果（规则是否被触发、找到的对象以及关于触发了哪项规则的信息）。
- 对于在其中检测到 IOC 的对象和 YARA 规则，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。
- 对于隔离的对象：
  - 文件路径
  - 文件大小
  - 隔离时分配的文件 ID
  - 原始文件删除标志
- 对于从隔离区接收、恢复或删除的文件：
  - 隔离时分配的文件 ID
- 对于被阻止的可执行文件或脚本执行：
  - 进程 ID
  - 父进程 ID
  - 系统 ID
  - 登录会话 ID
  - 进程状态
  - 执行拦截的日期和时间

- 对于办公应用程序禁止打开的文档：
  - 进程 ID
  - 文件 ID
  - 执行拦截的日期和时间
- 指定目录中的文件列表：
  - 文件名
  - 文件的绝对路径
  - 文件大小
  - 文件类型
  - 所有者用户和所有者组的名称和 ID
  - 文件访问权限
  - 应用于每个文件的特殊文件系统标志
  - 文件元数据
  - 指向文件的硬链接数量
  - 文件创建、修改和上次访问时间
- 设备上正在运行的进程列表：
  - 进程名称
  - 进程开始时间
  - 进程状态
  - 进程 ID (PID) 和父进程 ID
  - 进程的当前工作目录
  - 启动该进程的命令行选项
  - 环境变量
  - 进程的可执行文件路径
  - 启动进程的用户的会话 ID
  - 启动进程的用户和组的 ID
  - 进程拥有系统文件和资源访问权限的用户和组的 ID

- 自动运行点列表：
  - 自动运行点类型
  - 文件名
  - 文件的绝对路径
  - 文件访问权限
  - 应用于每个文件的特殊文件系统标志
  - 所有者用户和所有者组的名称和 ID
  - 文件创建、修改和上次访问时间
- 进程内存镜像：
  - 进程名称
  - 进程文件的完整路径
  - 进程转储文件
  - 进程转储文件的大小
- 设备内存映像：设备 RAM 的转储文件
- 设备磁盘镜像

- 有关文件的信息：
  - 文件的唯一 ID
  - 对象的 MD5 哈希值
  - 文件内容
- 遥测数据包中的数据：
  - 遥测事件数据：
    - 事件 ID。
    - 事件在已发送的遥测数据包序列中的编号。
    - 事件类型。
    - 事件时间。
  - 关于受保护设备的信息：
    - 受保护设备的的名称。
    - Kaspersky Security Center 中受保护设备的 ID。

- Kaspersky Endpoint Detection and Response Expert (on-premises) 中受保护设备的 ID。
- 受保护设备上安装的操作系统的名称、版本和系列。
- 受保护设备上安装的操作系统的启动和关闭时间。

- 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 ID
  - 进程 ID
  - 启动该进程的命令行选项
  - 会话 ID
  - 进程开始的日期和时间
  - 启动进程的用户和组的信息（名称和 ID）
- 关于获取另一进程内存访问权限的进程的信息：
  - 进程 ID
  - 注入方法和地址。
  - 用于修改进程的命令行（包括参数）。
  - 进程的系统调用参数
- 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
  - 应用程序数据库的发布日期和版本

    - 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
- 有关将库加载到进程地址空间的信息：已加载库的 ID
- 有关建立和终止网络连接的信息：
    - 本地 IP 地址
    - 远程 IP 地址
    - 连接方向
    - 协议
    - 连接建立时间
    - 连接终止时间
    - 连接持续时间
    - 连接期间发送的字节数
    - 连接期间接收的字节数

- 在某个端口上监听外部网络连接的进程信息：
  - 本地地址（端口和 IP 地址）
  - 协议
- DNS 服务器查询信息：
  - 所查询资源的域名
  - 所查询资源的 IP 地址
  - DNS 服务器 IP 地址
  - 查询类型
- 已连接外部设备的信息：
  - 操作类型（设备连接）
  - 设备类型
  - 唯一设备 ID
  - 设备名称
  - 设备路径
- 应用程序及其模块的信息：
  - 应用程序版本。
  - 应用程序的安装、启动、停止或卸载时间、
  - 应用程序操作的发起者、
  - 异常停止时应用程序停止的原因、
  - 异常停止时的返回码。
- 有关与任务调度程序交互（任务创建和删除）的信息：
  - 任务名称。
  - 计划命令的路径。
  - 任务启动计划。
  - 创建任务的用户的名称。
  - 启动任务的用户的名称。
  - 删除任务的用户的名称。

- 关于服务创建、删除和修改的信息：
  - 服务名称（如果已更改，包括之前的名称）
  - 服务类型（如果已更改，包括之前的类型）
  - 可执行文件路径（如果已更改，包括之前的路径）
  - 服务依赖项（如果已更改，包括之前的依赖项）
  - 启动服务的用户名（如果已更改，包括之前的用户名）
  - 服务的显示名称（如果已更改，包括之前的显示名称）
  - 创建、删除或修改服务的用户名
  - 延迟删除标志
- 关于控制台输入的信息：
  - 发起控制台输入的进程的 ID 和类型
  - 控制台输入的内容
- 关于已挂载设备的信息：
  - 卷的系统名称
  - 挂载点
- 关于进程内存更改的信息：
  - 进程的系统调用参数
  - 关于执行代码注入的进程及其父进程的信息
    - 进程及其父进程的进程 ID 和唯一 ID
    - 用于启动进程及其父进程的命令行
    - 进程的环境变量
    - 用来启动进程及其父进程的用户账户类型
    - 用于生成进程的系统调用
    - 启动进程的用户和组的 ID
    - 进程及父进程的名称和全名
    - 进程及父进程的完整路径
    - 进程及父进程的 MD5 和 SHA256 哈希值

- 会话 ID
- 启动进程及父进程的用户的名称、域名和 ID

- 关于加载执行代码注入的进程的信息
  - 通过其加载进程的进程的唯一 ID
  - 通过其加载进程的文件的名称和全名
  - 通过其加载进程的进程的完整路径
  - 通过其加载进程的进程的 MD5 哈希值
- 关于作为进程发起者的进程的信息
  - 作为进程发起者的进程的进程 ID 和唯一 ID
  - 作为进程发起者的进程的命令行
  - 启动作为进程发起者之进程的用户的名称和域名
  - 作为进程发起者的进程的名称和全称
  - 作为进程发起者的进程的完整路径
  - 作为进程发起者的进程的 MD5 和 SHA256 哈希

此处列出的信息也可以保存在跟踪文件和转储文件中。

# 与 Kaspersky Endpoint Detection and Response Expert (cloud) 组件集成时提供的数据

将 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成时，Kaspersky Endpoint Security 会存储以下信息，其中可能包含个人数据和机密数据：

- 用于与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成的服务器列表。
- Kaspersky Endpoint Detection and Response Expert (cloud) 的遥测和响应服务器隧道的地址。
- 用于与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成的服务器证书。
- 用于与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成的客户端证书。
- 负责与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成的服务器的同步频率设置，以及该服务器的数据传输设置。
- 处理与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成的服务器的连接状态，以及有关客户端和服务器证书错误的信息。

- 用于与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成的服务器所下发任务的参数：
  - 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

当 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成时，该应用程序会保存以下数据，并可将其传输到 Integration Server：

- 发送到 EDR Expert (cloud) 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
  - 授权许可密钥状态
- 任务执行报告中发送到 EDR Expert (cloud) 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码
- 任务完成状态
- 任务完成时间
- 使用的任务设置版本
- 有关根据服务器请求在设备上启动的进程的信息：
  - 进程终止代码
  - 进程标准输出文件的唯一 ID。
  - 进程标准错误文件的唯一 ID。
- 有关根据服务器请求在设备上启动或停止的进程的信息：
  - PID（系统进程 ID）。
  - UniquePID（进程的唯一标识符）
  - 错误代码
- 服务器请求的文件副本，以及该文件的路径和 ID。
- 操作系统重启后删除文件的标志。
- 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）。
- 对于检测到 IoC 的对象，将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。
- 对于隔离的对象：
  - 文件路径
  - 文件大小

    - 隔离时分配的文件 ID
    - 原始文件删除标志
- 对于从隔离区接收、恢复或删除的文件：
    - 隔离时分配的文件 ID
- 对于被阻止的可执行文件或脚本执行：
    - 进程 ID
    - 父进程 ID
    - 系统 ID
    - 登录会话 ID
    - 进程状态
    - 执行拦截的日期和时间
- 对于办公应用程序禁止打开的文档：
    - 进程 ID
    - 文件 ID
    - 执行拦截的日期和时间
- 指定目录中的文件列表：
    - 文件名
    - 文件的绝对路径
    - 文件大小
    - 文件类型
    - 所有者用户和所有者组的名称和 ID
    - 文件访问权限
    - 应用于每个文件的特殊文件系统标志
    - 文件元数据
    - 指向文件的硬链接数量
    - 文件创建、修改和上次访问时间

- 设备上正在运行的进程列表：
  - 进程名称
  - 进程开始时间
  - 进程状态
  - 进程 ID (PID) 和父进程 ID
  - 进程的当前工作目录
  - 启动该进程的命令行选项
  - 环境变量
  - 进程的可执行文件路径
  - 启动进程的用户的会话 ID
  - 启动进程的用户和组的 ID
  - 进程拥有系统文件和资源访问权限的用户和组的 ID
- 自动运行点列表：
  - 自动运行点类型
  - 文件名
  - 文件的绝对路径
  - 文件访问权限
  - 应用于每个文件的特殊文件系统标志
  - 所有者用户和所有者组的名称和 ID
  - 文件创建、修改和上次访问时间
  - 可执行文件或可加载模块的 MD5 哈希值和 SHA-256 哈希值。
- 进程内存镜像：
  - 进程内存镜像文件的名称。
  - 进程文件的完整路径
  - 进程内存镜像文件的唯一 ID。
  - 进程内存镜像文件的大小。

- 设备内存镜像：
  - 开始转储的日期和时间。
  - 转储文件的完整路径
  - 设备内存镜像文件的大小。
- 设备磁盘镜像：
  - 开始转储的日期和时间。
  - 转储文件完整路径的数组
  - 设备磁盘镜像文件的大小。
  - 逻辑磁盘。
  - 物理磁盘。
- 遥测数据包中的数据：
  - 遥测事件数据：
    - 事件 ID。
    - 事件在已发送的遥测数据包序列中的编号。
    - 事件类型。
    - 事件时间。
  - 关于受保护设备的信息：
    - 受保护设备的的名称。
    - Kaspersky Security Center 中受保护设备的 ID。
    - Kaspersky Endpoint Detection and Response Expert (on-premises) 中受保护设备的 ID。
    - 受保护设备上安装的操作系统的名称、版本和系列。
    - 受保护设备上安装的操作系统的启动和关闭时间。
  - 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 ID
    - 进程 ID
    - 启动该进程的命令行选项
    - 会话 ID
    - 进程开始的日期和时间
    - 启动进程的用户和组的信息（名称和 ID）
- 关于获取另一进程内存访问权限的进程的信息：
    - 进程 ID
    - 注入方法和地址。
    - 用于修改进程的命令行（包括参数）。
    - 进程的系统调用参数
- 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
    - 应用程序数据库的发布日期和版本
    - 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
- 有关将库加载到进程地址空间的信息：已加载库的 ID
- 有关建立和终止网络连接的信息：
  - 本地 IP 地址
  - 远程 IP 地址
  - 连接方向
  - 协议
  - 连接建立时间
  - 连接终止时间
  - 连接持续时间
  - 连接期间发送的字节数
  - 连接期间接收的字节数
- 在某个端口上监听外部网络连接的进程信息：
  - 本地地址（端口和 IP 地址）
  - 协议
- DNS 服务器查询信息：
  - 所查询资源的域名
  - 所查询资源的 IP 地址
  - DNS 服务器 IP 地址
  - 查询类型

- 已连接外部设备的信息：
  - 操作类型（设备连接）
  - 设备类型
  - 唯一设备 ID
  - 设备名称
  - 设备路径
- 应用程序及其模块的信息：
  - 应用程序版本。
  - 应用程序的安装、启动、停止或卸载时间、
  - 应用程序操作的发起者、
  - 异常停止时应用程序停止的原因、
  - 异常停止时的返回码。
- 有关与任务调度程序交互（任务创建和删除）的信息：
  - 任务名称。
  - 计划命令的路径。
  - 任务启动计划。
  - 创建任务的用户的名称。
  - 启动任务的用户的名称。
  - 删除任务的用户的名称。
- 关于服务创建、删除和修改的信息：
  - 服务名称（如果已更改，包括之前的名称）
  - 服务类型（如果已更改，包括之前的类型）
  - 可执行文件路径（如果已更改，包括之前的路径）
  - 服务依赖项（如果已更改，包括之前的依赖项）
  - 启动服务的用户名（如果已更改，包括之前的用户名）
  - 服务的显示名称（如果已更改，包括之前的显示名称）
  - 创建、删除或修改服务的用户名
  - 延迟删除标志

- 关于控制台输入的信息：
  - 发起控制台输入的进程的 ID 和类型
  - 控制台输入的内容
- 关于已挂载设备的信息：
  - 卷的系统名称
  - 挂载点
- 关于进程内存更改的信息：
  - 进程的系统调用参数
  - 关于执行代码注入的进程及其父进程的信息
    - 进程及其父进程的进程 ID 和唯一 ID
    - 用于启动进程及其父进程的命令行
    - 进程的环境变量
    - 用来启动进程及其父进程的用户账户类型
    - 用于生成进程的系统调用
    - 启动进程的用户和组的 ID
    - 进程及父进程的名称和全名
    - 进程及父进程的完整路径
    - 进程及父进程的 MD5 和 SHA256 哈希值
    - 会话 ID
    - 启动进程及父进程的用户的名称、域名和 ID
  - 关于加载执行代码注入的进程的信息
    - 通过其加载进程的进程的唯一 ID
    - 通过其加载进程的文件的名称和全名
    - 通过其加载进程的进程的完整路径
    - 通过其加载进程的进程的 MD5 哈希值
  - 关于作为进程发起者的进程的信息
    - 作为进程发起者的进程的进程 ID 和唯一 ID
    - 作为进程发起者的进程的命令行

- 启动作为进程发起者之进程的用户的名称和域名
- 作为进程发起者的进程的名称和全称
- 作为进程发起者的进程的完整路径
- 作为进程发起者的进程的 MD5 和 SHA256 哈希

此处列出的信息也可以保存在跟踪文件和转储文件中。

# 与 Kaspersky Network Detection and Response (KATA) 组件集成时提供的数据

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

- NDR 服务器地址
- 用于与 Kaspersky Networks Detection and Response (KATA) 整合的服务器证书的公钥
- 用于与 Kaspersky Network Detection and Response (KATA) 整合的客户端证书
- 用于在代理服务器上进行身份验证的凭据。
- 与 NDR 服务器同步的频率设置以及向 NDR 服务器发送数据的设置
- NDR 服务器连接状态以及与客户端证书和服务器证书相关的错误信息

当 Kaspersky Endpoint Security 与 Kaspersky Networks Detection and Response (KATA) 组件集成时，Kaspersky Endpoint Security 应用程序会存储以下数据并将其发送到 NDR 服务器：

- 来自同步请求到 NDR 服务器的数据：
  - 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，系列和版本
  - Kaspersky Endpoint Security 的版本
  - 正在使用的应用程序数据库的发布日期

- 授权许可密钥状态
- 用户设备的型号和制造商

- 遥测数据包中的数据：
  - 有关设备和用户的信息
    - 设备名称和设备上的时间
    - 操作系统的系列、名称和版本
    - 有关网络接口的信息（描述、带子网掩码的 IP 地址列表、MAC 地址、度量数字、DNS 域名、路由信息、监听端口号）
    - 设备内部唯一 ID
    - 用户名和 ID
    - 用户组名称和 ID
  - 有关 Kaspersky Endpoint Security 应用程序的信息：
    - 应用程序的名称和版本
    - 上次应用程序更新的日期
    - 有关授权许可密钥的信息（序列号、类型、授权许可有效期、密钥状态）
    - 应用程序数据库版本
    - 支持的 API 版本列表
  - 有关已建立连接的信息：
    - 本地 IP 地址、端口和 MAC 地址
    - 远程 IP 地址、端口和 MAC 地址
    - 网关 IP 地址。
    - 协议类型（根据 IANA）、协议编号和 EtherType
    - 接收和发送的包数量
  - 有关已处理文件的信息：
    - 文件名和唯一 ID
    - 文件类型和大小
    - 文件镜像的完整路径
    - 文件系统属性掩码

- 文件创建和修改的时间
- 校验和（MD5 和 SHA256）
- 文件权限，包括继承和有效的权限

- 有关运行和终止进程的信息：
  - 进程 UID 和 PID
  - 进程类型。
  - 会话 ID
  - 已执行的命令
  - 环境变量
- 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

此处列出的信息也可以保存在跟踪文件和转储文件中。

# 与 Kaspersky Unified Monitoring and Analysis Platform 集成时提供的数据

将 Kaspersky Endpoint Security 与 Kaspersky Unified Monitoring and Analysis Platform 集成时，Kaspersky Endpoint Security 会存储以下信息，其中可能包含个人和机密数据：

- KUMA 服务器地址
- 用于与 Kaspersky Unified Monitoring and Analysis Platform 整合的服务器证书的公钥（使用 UDP 协议连接 KUMA 服务器时除外）
- 用于与 Kaspersky Unified Monitoring and Analysis Platform 整合的客户端证书
- 用于在代理服务器上进行身份验证的凭据。
- 与 KUMA 服务器同步的频率设置以及向 KUMA 服务器发送数据的设置
- KUMA 服务器连接状态以及与客户端证书和服务器证书相关的错误信息

将 Kaspersky Endpoint Security 与 Kaspersky Unified Monitoring and Analysis Platform 集成时，Kaspersky Endpoint Security 应用程序会将以下数据保存并通过遥测数据包传输到 KUMA 服务器：

- 有关文件修改的信息：
  - 修改前文件的唯一 ID
  - 被修改文件的唯一 ID
  - 做出更改的进程的唯一 ID
  - 文件操作类型及标志
  - 修改文件的日期和时间
- 有关运行和终止进程的信息：
  - 进程文件 ID
  - 进程 UID 和 PID
  - 启动该进程的命令行选项
  - 会话 ID
  - 进程开始的日期和时间
  - 启动进程的用户和组的信息（名称和 ID）
- 事件日志中有关事件的信息：
  - 事件的日期和时间
  - 与事件关联的进程的 UID
  - 事件的类型和描述
  - 执行操作的结果

# 有关第三方代码的信息

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。

# 商标通知

注册商标和服务标志均为其各自拥有者的财产。

Adobe、Acrobat、Flash 和 Shockwave 是 Adobe 在美国和/或其他国家/地区的注册商标或商标。

AMD64 是 Advanced Micro Devices, Inc. 的商标或注册商标。

Amazon 是 Amazon.com, Inc. 或其子公司的商标。

Arm 是 Arm Limited（或其子公司）在美国和/或其他地区的注册商标。

AutoCAD 是 Autodesk, Inc. 和/或其子公司和/或附属公司在美国和/或其他国家/地区的商标或注册商标。

Borland 是 Borland Software Corporation 的商标或注册商标。

dBase 是 dataBased Intelligence, Inc. 的商标

FireWire 是 Apple Inc. 的商标。

Bluetooth 文字、标志和徽标归 Bluetooth SIG, Inc. 所有。

Ubuntu 和 LTS 是 Canonical Ltd. 的注册商标。

XenServer 是 Cloud Software Group, Inc. 和/或其子公司在美国和/或其他国家/地区的注册商标或商标。

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。

Grafana 文字标记和 Grafana 徽标是 Coding Instinct AB 在美国和其他国家的注册商标/服务标志或商标/服务标志，并经 Coding Instinct 许可使用。我们与 Coding Instinct 或 Grafana 社区没有任何关联，也未得到其认可或赞助。

Docker 和 Docker 徽标是 Docker，Inc. 在美国和/或其他国家的商标或注册商标。Docker, Inc. 和其他各方也可能拥有此处使用的其他条款的商标权。

Chrome、Chromium、Google 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。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft、Microsoft Edge、Active Directory、Hyper-V、Outlook、Visual Basic、Visual FoxPro、Visual C++、PowerPoint、Excel、Internet Explorer、Windows 和 Windows Server 是 Microsoft 集团公司的商标。

OpenStack 是 OpenStack Foundation 在美国和其他国家/地区的注册商标。

Oracle、Java 和 JavaScript 是 Oracle 和/或其附属公司的注册商标。

Python 是 Python Software Foundation 的商标或注册商标。

Red Hat Enterprise Linux、CentOS 和 Fedora 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

Kubernetes 是 Linux Foundation 在美国和其他国家/地区的注册商标。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商标。

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。

Zabbix 是 Zabbix SIA 的注册商标。