kaspersky

# Kaspersky Endpoint Security for Linux

© 2026 AO Kaspersky Lab

# 目录


Kaspersky Endpoint Security 12.4 for Linux 帮助

Kaspersky Endpoint Security 12.4 for Linux

- 关于 Kaspersky Endpoint Security 使用模式
  - 在 Light Agent 模式下使用应用程序
  - 在 Endpoint Detection and Response Agent 模式下使用应用程序
- 分发包
- 硬件和软件要求
  - 硬件要求
  - 软件要求
  - Light Agent 模式的其他软件要求
  - 支持的 Kaspersky Security Center 版本
  - KATA 和 OSMP 平台上支持的解决方案版本

新功能

已修复问题

准备安装 Kaspersky Endpoint Security

Kaspersky Endpoint Security 的安装和初始配置

- Kaspersky Security Center 网络代理的安装和初始配置
- 安装 Kaspersky Endpoint Security 管理插件
  - 安装 Kaspersky Endpoint Security Web 插件
  - 安装 Kaspersky Endpoint Security MMC 插件
- 使用 Kaspersky Security Center 安装和初始配置应用程序
  - 在 Web Console 中创建安装包
  - 在 Web Console 中进行初始配置设置
  - 在管理控制台中创建安装包
  - 在管理控制台中进行初始配置设置
  - 准备包含应用程序数据库的压缩文件，以创建包含集成数据库的安装包
  - Autoinstall.ini 配置文件设置
  - 使用 Kaspersky Security Center 开始
- 使用命令行安装和初始配置应用程序
  - 使用命令行安装应用程序
  - 以交互模式对应用程序进行安装后配置
    - 选择标准模式或 Light Agent 模式
    - 定义虚拟机的角色
    - 启用 VDI 保护模式
    - 选择模式：标准模式或 Endpoint Detection and Response Agent
    - 选择区域设置
    - 查看最终用户授权许可协议和隐私策略
    - 接受最终用户授权许可协议
    - 接受隐私策略
    - 使用卡巴斯基安全网络
    - 从特权组中删除用户
    - 将管理员角色分配给一位用户
    - 配置系统事件拦截机制

启用 SELinux 的自动配置
配置更新源
配置代理服务器设置
启动应用程序数据库更新
启用应用程序数据库自动更新
激活应用程序
以自动模式对应用程序进行安装后配置
安装后配置的配置文件中的设置
在 SELinux 系统中配置允许规则
在封闭软件环境模式下针对 Astra Linux OS 运行应用程序
在封闭软件环境模式下的 ALT SP 上运行应用程序
配置 OSnova 操作系统以使应用程序正常运行
优化应用程序的资源消耗
针对典型服务器角色的建议
设备端应用程序性能分析
分析文件威胁防护任务的资源消耗情况
识别最常扫描的对象
针对文件威胁防护任务和扫描任务的建议
配置扫描排除项
配置文件操作拦截排除项
设置应用程序内存使用限制
针对 Web 威胁防护任务和网络威胁防护任务的建议。
从先前的版本更新应用程序
更新 Kaspersky Endpoint Security 管理插件
使用 Kaspersky Security Center 更新应用程序
使用命令行更新应用程序
更新应用程序时设置参数值的特殊注意事项
卸载应用程序
使用 Kaspersky Security Center 卸载应用程序和网络代理
使用命令行卸载应用程序
使用命令行移除网络代理
卸载 Kaspersky Endpoint Security 管理插件
应用程序授权许可
关于最终用户授权许可协议
关于授权许可
关于授权许可证书
关于授权许可密钥
关于激活码
关于密钥文件
关于订阅
不同授权许可下的应用程序功能比较
应用程序激活和授权许可密钥管理
使用 Kaspersky Security Center 激活应用程序
命令行中的授权许可密钥管理

查看有关使用的授权许可密钥的信息
使用 Web Console 查看设备上的授权许可密钥信息
使用管理控制台查看设备上的授权许可密钥信息
在命令行中查看有关授权许可和密钥的信息
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-premise) 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
应用程序管理理念
使用 Kaspersky Security Center 管理应用程序
Kaspersky Endpoint Security 管理插件
Kaspersky Security Center 策略
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
在 Web Console 中管理策略
在 Web Console 中创建策略
在 Web Console 中更改策略设置
Web Console 中的策略设置
在管理控制台中管理策略
使用管理控制台创建策略
在 Kaspersky Security Center 管理控制台中更改策略设置
管理控制台中的策略设置
在 Web Console 中管理任务
在 Web Console 中创建任务
在 Web Console 中更改任务设置
在 Web Console 中启动、停止、暂停和恢复任务
在管理控制台中管理任务
在管理控制台中创建任务
在管理控制台中更改任务设置
在管理控制台中启动、停止、暂停和恢复任务
使用命令行管理应用程序
启用自动添加 kesl-control 命令（bash 完成）
在命令行上管理任务
在命令行中查看任务列表
在命令行中查看任务的状态
在命令行中创建任务
在命令行中启动、停止、暂停和恢复任务
在命令行中删除任务
在命令行中显示任务设置

在命令行中编辑任务设置
使用配置文件编辑任务设置
使用命令行选项编辑任务设置
在命令行中恢复默认任务设置
在命令行中配置任务计划
通过命令行管理常规应用程序设置
显示常规应用程序设置
编辑常规应用程序设置
使用筛选器来限制查询结果
导出和导入应用程序设置
使用命令行管理用户角色
查看用户和角色列表
为用户分配角色
撤销用户角色
启动和停止应用程序
使用 Web Console 启动和停止应用程序
使用管理控制台启动和停止应用程序
使用命令行启动和停止应用程序
查看设备保护状态和应用程序性能信息
在 Web Console 中查看设备的保护状态
在管理控制台中查看设备的保护状态
在 Web Console 中查看有关应用程序运行的信息
在管理控制台中查看有关应用程序操作的信息
在命令行中查看有关应用程序操作的信息
查看应用程序统计数据
在 Web Console 中查看应用程序统计数据
在管理控制台中查看应用程序统计数据
在 Web Console 中查看挂载点列表
在管理控制台中查看挂载点列表
在命令行中查看应用程序统计数据和挂载点列表
获取系统性能指标
更新应用程序数据库和模块
更新数据库和模块
更新源和更新场景
在 Web Console 中更新应用程序数据库和模块
在管理控制台中更新应用程序数据库和模块
在命令行中更新应用程序数据库和模块
使用 Kaspersky 更新实用程序更新
回滚应用程序数据库和模块更新
文件威胁防护
在 Web Console 中配置文件威胁防护
在管理控制台中配置文件威胁防护
“扫描范围”窗口
<新扫描范围>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
<新建扫描范围>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
在命令行中配置文件威胁防护
“文件威胁防护任务”设置
优化网络目录扫描
扫描符号链接和硬链接的特殊注意事项
恶意软件扫描
Web Console 中的恶意软件扫描
“添加扫描范围”窗口
“扫描范围”部分
“扫描范围”窗口
“排除范围”部分
“排除范围”窗口
“添加排除范围”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
管理控制台中的恶意软件扫描
“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
命令行中的恶意软件扫描
恶意软件扫描预定义任务的设置
在命令行上自定义扫描文件和目录
关键区域扫描
Web Console 中的关键区域扫描
“添加扫描范围”窗口
“扫描范围”部分
“扫描范围”窗口
“排除范围”部分
“排除范围”窗口
“添加排除范围”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

管理控制台中的关键区域扫描
“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
命令行中的关键区域扫描
可移动驱动器扫描
在 Web Console 中配置可移动驱动器扫描
在管理控制台中配置可移动驱动器扫描
在命令行中配置可移动驱动器扫描
容器扫描
容器监控
在 Web Console 中配置容器监控
在管理控制台中配置容器监控
“容器扫描设置”窗口
在命令行中配置容器监控
按需扫描容器和镜像
Web Console 中的容器扫描
“排除范围”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
管理控制台中的容器扫描
“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
命令行中的容器扫描
容器扫描任务设置
自定义扫描容器和镜像
与 Jenkins 整合
防火墙管理
关于网络数据包规则
关于动态规则
关于预定义的可用网络
Web Console 中的防火墙管理
管理控制台中的防火墙管理
“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
命令行中的防火墙管理
在命令行中配置网络包规则列表
在命令行中配置网络区域
Web 威胁防护
在 Web Console 中配置 Web 威胁防护
在管理控制台中配置“Web 威胁防护”
“受信任网址”窗口
“扫描设置”窗口
在命令行上配置 Web 威胁防护
扫描网络流量
关于网络流量拦截模式
在 Web Console 中配置网络流量扫描
在管理控制台中配置网络流量扫描
“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
在命令行上配置网络流量扫描
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
使用操作系统工具排除流量拦截
网络威胁防护
在 Web Console 中配置网络威胁防护
在管理控制台中配置网络威胁防护
“排除项”窗口
在命令行中配置网络威胁防护
邮件威胁防护
在 Web Console 中配置邮件威胁防护
在管理控制台中配置邮件威胁防护
邮件威胁防护设置窗口
附件筛选窗口
在命令行中配置邮件威胁防护
BadUSB 攻击防护
在 Web Console 中配置 BadUSB 攻击防护
在管理控制台中配置 BadUSB 攻击防护
在命令行中配置 BadUSB 攻击防护
针对远程恶意加密的防护
在 Web Console 中配置反加密勒索
在管理控制台中配置反加密勒索
“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
在命令行上配置反加密勒索
管理被阻止的设备
应用程序控制
关于应用程序控制规则
应用程序控制规则测试模式
在 Web Console 中配置"应用程序控制"
在管理控制台中配置应用程序控制
"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
在命令行上配置应用程序控制
"应用程序控制"任务设置
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
导出和导入应用程序控制设置
清查
在 Web Console 中配置清查
"添加扫描范围"窗口
"排除范围"部分
"排除范围"窗口
"添加排除范围"窗口
在管理控制台中配置清查
"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
在命令行中配置清查
清查任务设置
查看检测到的应用程序列表
设备控制
在 Web Console 中配置设备控制
在管理控制台中配置设备控制
"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
- 配置设备控制消息模板
- 在命令行上配置设备控制
  - 设备控制任务设置
  - 在命令行中查看和导出连接设备列表
  - 在命令行中管理受信任设备列表
- 授予设备临时访问权限
  - 在 Web Console 中授予对被阻止设备的访问权限
  - 通过命令行获得对设备的临时访问权限

Web 控制

- 关于 Web 资源访问规则
- 在 Web Console 中配置 Web 控制
- 在管理控制台中配置 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
- 配置 Web 控制消息模板
- 在命令行中配置 Web 控制
  - Web 控制任务设置
  - 查看和编辑 Web 控制设置
- 创建 Web 资源地址掩码的规则

系统完整性监控

- 实时系统完整性监控
  - 在 Web Console 中配置系统完整性监控
  - 在管理控制台中配置系统完整性监控
    - “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
  - 在命令行中配置系统完整性监控
- 系统完整性检查
  - 在 Web Console 中配置系统完整性检查
    - “添加扫描范围”窗口
    - “排除范围”部分
    - “排除范围”窗口
    - “添加排除范围”窗口
    - “按掩码筛选的排除项”窗口

在管理控制台中配置系统完整性检查
"扫描范围"窗口
"新建扫描范围"窗口
"排除范围"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
在命令行中配置系统完整性检查
行为检测
在 Web Console 中配置行为检测
在管理控制台中配置行为检测
"按进程筛选的排除项"窗口
"受信任进程"窗口
在命令行中配置行为检测
漏洞利用防御
在 Web Console 中配置漏洞利用防御
在管理控制台中配置漏洞利用防御
漏洞利用防御排除窗口
漏洞利用防御排除窗口
在命令行中配置漏洞利用防御
使用卡巴斯基安全网络
在 Web Console 中配置使用卡巴斯基安全网络。
在管理控制台中配置使用卡巴斯基安全网络。
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
在命令行中配置使用卡巴斯基安全网络
使用命令行检查与卡巴斯基安全网络的连接
从命令行启用和禁用云模式
高级应用程序设置
配置代理服务器
在 Web Console 中配置代理服务器设置
在管理控制台中配置代理服务器设置
代理服务器排除项窗口
在命令行中配置代理服务器设置
配置全局排除项
在 Web Console 中配置全局排除项
在管理控制台中配置全局排除项
"挂载点路径"窗口
在命令行上配置全局排除
从扫描中排除进程内存
选择文件操作拦截模式
配置检测黑客可能用来危害的应用程序
启用应用程序稳定性监控
配置应用程序启动设置
限制应用程序对驻留内存的使用
限制内存和处理器资源的使用

限制"自定义扫描"任务的数量
配置数据传输到 Kaspersky Security Center 存储
配置任务管理的权限
使用电池供电时取消任务
配置系统事件拦截
检查是否可以安装可更新内核模块
当使用可更新内核模块时的"安全"模式
在 Web Console 中管理拦截设置
在管理控制台中管理拦截设置
使用命令行来管理拦截设置
管理附加遥测设置
备份
在 Web Console 中配置备份设置
在管理控制台中配置备份设置
使用命令行配置备份区设置
在命令行上操作备份区对象
与 Detection and Response 解决方案整合
关于基于 Detection and Response 解决方案命令的威胁响应操作
Kaspersky Endpoint Detection and Response Expert (on-premise) 集成
如何准备用于与 EDR Expert (on-premise) 正确集成的参考镜像
在 Web Console 中配置 Kaspersky Endpoint Detection and Response Expert（本地部署）集成
透过命令行配置 Kaspersky Endpoint Detection and Response Expert（本地部署）集成
Kaspersky Endpoint Detection and Response Expert（本地部署）集成设置
管理用于连接到 OSMP 服务器的证书
与 Kaspersky Anti Targeted Attack Platform 整合
在 Web Console 中配置 Kaspersky Endpoint Detection and Response (KATA) 集成
在管理控制台中配置 Kaspersky Endpoint Detection and Response (KATA) 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
在命令行上配置 Kaspersky Endpoint Detection and Response (KATA) 集成
Kaspersky Endpoint Detection and Response (KATA) 集成设置
管理用于连接到 Expert 服务器的证书
在 Web Console 中配置 Kaspersky Network Detection and Response (KATA) 集成
在管理控制台中配置 Kaspersky Network Detection and Response (KATA) 集成
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
在命令行上配置 Kaspersky Network Detection and Response (KATA) 集成
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
在 Web Console 中配置 Sandbox 集成
在命令行上配置 Sandbox 集成
Sandbox 集成设置
管理用于连接到 Sandbox 服务器的证书

Kaspersky Endpoint Detection and Response Optimum 整合
启用或禁用 Kaspersky Endpoint Detection and Response Optimum 整合
在 Web Console 中启用或禁用 Kaspersky Endpoint Detection and Response Optimum 整合
在命令行上启用或禁用 Kaspersky Endpoint Detection and Response Optimum 整合
查看 Kaspersky Endpoint Detection and Response Optimum 整合状态
查看有关检测到的威胁和响应操作的信息
与 Kaspersky Managed Detection and Response 整合
有关创建用于与 MDR 正确集成的参考镜像的建议
上传用于与 Kaspersky Managed Detection and Response 整合的 KPSN 配置文件
在 Web Console 中配置 Kaspersky Managed Detection and Response 整合
在管理控制台中配置 Kaspersky Managed Detection and Response 整合
在命令行上配置 Kaspersky Managed Detection and Response 整合
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
配置自动网络隔离的排除项
用于添加网络隔离排除的窗口
网络配置文件字典窗口
在命令行中管理设备的网络隔离
管理隔离区
使用 Web Console 隔离文件
编辑 Web Console 中的隔离区设置
编辑管理控制台中的隔离区设置
使用命令行编辑隔离区设置
通过命令行管理隔离文件
启动进程
终止进程
从设备接收文件
从设备删除文件
搜索入侵指标
在 Web Console 中搜索入侵指标
在命令行中搜索入侵指标
IOC 文件的要求
对象的执行防护
为 Web Console 中的对象配置执行防护
在管理控制台中配置对象的执行防护
通过命令行管理对象的执行防护
Cloud Sandbox
与 Kaspersky Unified Monitoring and Analysis Platform 整合
在 Web Console 中配置 KUMA 整合
在管理控制台中配置 KUMA 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
在命令行上配置 MDR 整合
Kaspersky Unified Monitoring and Analysis Platform 整合任务设置
管理用于连接到 KUMA 服务器的证书
配置在 Light Agent 模式下使用应用程序的设置
在 Web Console 中配置 Light Agent 设置
在管理控制台中配置 Light Agent 设置
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
在命令行中查看有关在 Light Agent 模式下的应用程序使用情况的信息
查看事件和报告
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
在 Kaspersky Security Center 中查看事件
在命令行中查看事件
配置图形界面中的弹出通知
通过图形界面管理应用程序
图形界面
启用和禁用应用程序组件
启动和停止扫描任务
启动自定义扫描和 Sandbox 扫描
启动和停止更新任务
配置卡巴斯基安全网络
查看报告
查看备份对象
管理授权许可密钥
添加授权许可密钥
移除授权许可密钥
查看授权许可信息
获取设备的临时访问权限
查看有关应用程序的信息
创建跟踪文件
应用程序组件完整性检查
联系技术支持
通过 Kaspersky CompanyAccount 获取技术支持
获取技术支持信息
关于应用程序跟踪文件
配置应用程序跟踪设置
应用程序管理插件跟踪文件

关于转储文件
管理转储文件设置
使用 Kaspersky Security Center 进行远程设备诊断
附录
附录 1.用于管理 Kaspersky Endpoint Security 的命令
用于管理应用程序任务和设置的命令
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
用于管理对象的执行防护的命令
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
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
用于管理授权许可密钥的命令
用于防火墙管理的命令
用于管理被阻止设备的命令
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
用于管理备份的命令
用于管理隔离区的命令
用于管理用户和角色的命令
用于管理 EDR Expert（本地部署）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
在用于保护虚拟环境的 Light Agent 模式中的应用程序命令
用于管理系统性能指标的命令
附录 2.配置文件和默认应用程序设置
编辑任务配置文件的规则
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
常规应用程序设置
常规容器扫描设置
网络流量扫描设置
任务计划设置
附录 3.命令行返回代码
附录 4.配置与 Kaspersky Anti-Virus for Linux Mail Server 的交互
附录 5.Web Console 中的策略设置
主机威胁防护
文件威胁防护
BadUSB 攻击防护
可移动驱动器扫描
行为检测
反加密
漏洞利用防御
通信和 Web 保护
邮件威胁防护
Web 威胁防护
网络威胁防护
防火墙
安全控制
设备控制
Web 控制
应用程序控制
系统完整性监控
信任区域
常规设置
检测设置
卡巴斯基安全网络
用户交互
性能
网络设置
容器扫描
技术支持
报告和存储
与 KSC 的整合

操作系统交互设置
事件设置
遥测设置
内置代理
Managed Detection and Response
Endpoint Detection and Response Optimum
Endpoint Detection and Response Expert (on-premise)
Network Detection and Response (KATA)
Sandbox
与 KUMA 的整合
Light Agent 模式
SVM 检测设置
Integration Server 连接设置
SVM 连接标签
SVM 选择算法
保护连接
附录 6.与外部服务交互的设置
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
有关 Kaspersky Endpoint Security 的信息来源
术语表
Integration Server
Light Agent
SIEM 系统
SVM
代理服务器
卡巴斯基更新服务器
反加密
受信任设备
受感染的对象
可疑网址的数据库
启动对象
备用密钥
应用程序数据库
应用程序设置
授权许可
授权许可证书
排除
文件掩码
活动密钥
活动策略
清除
激活应用程序
策略
管理服务器

- 管理组
- 组任务
- 组策略
- 订阅
- 误报
- 钓鱼网页地址数据库

有关第三方代码的信息

商标通知

# Kaspersky Endpoint Security 12.4 for Linux 帮助

## 新增功能

Kaspersky Endpoint Security 12.4 for Linux 中的新增功能

## 硬件和软件要求

应用程序的硬件和软件要求

## 功能比较

- 不同授权许可下的应用程序功能比较
- 在 Light Agent 模式下使用应用程序的特殊考虑事项
- 在 Endpoint Detection and Response Agent 模式下使用应用程序涉及的特殊考虑事项

## 入门

- Kaspersky Endpoint Security for Linux 安装和初始配置快速指南（应用程序在标准模式下使用）
- 从以前版本的应用程序升级
- 准备安装应用程序
- 应用程序的安装和初始配置
- 在初始配置期间通过命令行更新应用程序数据库和模块
- 使用预定义更新任务在命令行上更新应用程序数据库（初始配置后）
- 开始使用 Kaspersky Security Center

## 授权许可

- 应用程序授权许可
- 应用程序激活和授权许可密钥管理
- 在初始配置期间通过命令行激活应用程序
- 在命令行上激活应用程序并管理授权许可密钥（初始配置后）
- 使用 Kaspersky Security Center 激活应用程序

## 监控与报告

- 查看设备的保护状态和有关应用程序性能的信息
- 在命令行中查看有关应用程序运行的信息
- 查看事件和报告

## 数据提供与个人信息保护

- 数据提供

## 其他功能

- 配置在 Light Agent 模式下使用应用程序的设置
- 应用程序的高级配置
- 使用卡巴斯基安全网络
- 备份
- 与 Detection and Response 解决方案整合

## 优化操作系统资源消耗

- 资源消耗优化

## 联系技术支持

- 故障排除
- 联系技术支持

# Kaspersky Endpoint Security 12.4 for Linux

Kaspersky Endpoint Security 12.4 for Linux（“Kaspersky Endpoint Security”，“应用程序”）旨在保护运行 Linux® 操作系统的设备免受各种类型的威胁，包括网络攻击和诈骗攻击。

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

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

该应用程序的以下功能组件和任务提供用于保护和控制设备的主要功能：

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

  您还可以使用以下扫描任务按需扫描受保护的设备：

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

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

- **容器扫描**。*容器监控*（*容器扫描*，*容器监控*）组件支持实时扫描命名空间和正在运行的容器以查找恶意软件。支持与 Docker 容器管理系统、CRI-O 框架以及 Podman 和 runc 实用程序整合。您可以使用“*容器扫描*”任务按需扫描容器和镜像。

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

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

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

- **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。

- **BadUSB 攻击防护**。*BadUSB 攻击防护*保护组件可以阻止将受感染的、模拟键盘的 USB 设备连接到计算机。

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

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

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

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

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

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

- **系统完整性监控**允许您跟踪操作系统的文件和目录更改。*系统完整性监控*组件实时监控组件设置中指定的监控范围内的对象所执行的操作。您可以使用“*系统完整性检查*”任务来按需检查系统的完整性。执行检查时，将监控范围内对象的当前状态与其初始状态进行比较，该初始状态先前已被确定为基线。

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

- 应用程序数据库来检测和清除受感染的文件。在扫描过程中，应用程序会分析每个文件是否存在威胁：它将文件代码与特定威胁的代码进行比较，并查找可能的匹配项。

- 卡巴斯基安全网络。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对各种威胁作出响应，提高一些保护组件的性能，并减少误报风险。

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

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

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

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

- 与 Kaspersky Managed Detection and Response 的整合可实现持续搜索、检测和消除针对您组织的威胁。

- 与 Kaspersky Anti Targeted Attack Platform 整合可确保为组织的 IT 基础设施提供有效保护，并快速检测零日攻击、针对性攻击和高级持续性威胁等威胁。

- 与 Kaspersky Endpoint Detection and Response Optimum 的集成可保护组织的 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。

- 与 Integration with Kaspersky Unified Monitoring and Analysis Platform 整合可以接收、处理和存储信息安全事件，进行数据分析和关联，按事件搜索，以及创建有关检测到信息安全威胁迹象的通知。

- 与 Kaspersky Endpoint Detection and Response Expert（本地部署）集成可以防御大多数网络安全风险，并涵盖威胁传播的主要场景。

此外，还提供了其他应用程序功能来确保应用程序保持最新：

- 使用密钥文件或激活码来激活应用程序。

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

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

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

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

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

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

  如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟化环境，则必须使用 Kaspersky Security Center 来管理该应用程序。无法使用 Kaspersky Security Center 云控制台或图形用户界面来管理该应用程序。

应用程序的更新功能（包括反病毒签名更新和代码库更新）以及 KSN 功能可能无法在美国境内使用。

# 关于 Kaspersky Endpoint Security 使用模式

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

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

应用程序一次只能在一个模式下使用。

默认在标准模式下使用应用程序。

# 在 Light Agent 模式下使用应用程序

如果要在 Light Agent 模式下使用应用程序，则需要执行以下操作：

1. 在每个需要使用 Kaspersky Security for Virtualization Light Agent 进行保护的虚拟机上，以 Light Agent 模式安装 Kaspersky Endpoint Security。还可以在虚拟机模板上安装应用程序。

   在开始安装应用程序之前，您需要在虚拟机和虚拟机模板上安装 Kaspersky Security Center 网络代理。

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

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

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

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

   - 想要保护的虚拟机在虚拟基础架构中的角色：服务器或工作站。虚拟机的角色决定了在此虚拟机上使用应用程序时所用的授权许可以及可用的功能。
   - VDI 保护模式。如果要在用于创建临时虚拟机的虚拟机模板上安装应用程序，建议启用此模式。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的操作。

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

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

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

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

您可以在 Light Agent 模式下使用以下应用程序命令获取有关应用程序操作的信息以及与 Integration Server 和 SVM 的连接有关的信息：

- `kesl-control --ksvla-info`
- `kesl-control --viis-info`
- `kesl-control --svm-info`

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

- 状态“*运行中*”表示正在 Light Agent 模式下使用应用程序。
- *未安装*状态表示应用程序正在独立模式或者 Endpoint Detection and Response Agent 模式下运行。

## 关于在 Light Agent 模式下激活应用程序

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，则无需单独激活应用程序。您可以同时激活 Kaspersky Security for Virtualization Light Agent 解决方案的所有组件。激活是在 Protection Server 端（Kaspersky Security for Virtualization Light Agent 的一个组件）通过在 SVM 上添加授权许可密钥来执行的。有关更多详细信息，请参阅Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助。

Kaspersky Security for Virtualization Light Agent 的主授权许可可能不包括 Kaspersky Endpoint Security 应用程序的附加功能（例如，与 Kaspersky Detection and Response 解决方案的整合）。在这种情况下，您还需要向 SVM 添加授权许可密钥以激活附加功能。

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

您可以在 Kaspersky Security Center 的帮助下远程查看有关使用 Light Agent for Linux 的授权许可的信息，或者使用命令行在装有 Light Agent 的受保护的虚拟机上查看这些信息。

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

### 关于在 Light Agent 模式下更新应用程序数据库和模块

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

受保护的虚拟机上的数据库和软件模块使用 Kaspersky Endpoint Security 的特殊本地任务“*更新*”任务进行更新，此时需将 SVM 上的文件夹指定为更新源。该更新任务自动启动。您不能删除此任务，也不能更改其设置。

不支持除 SVM 上的文件夹以外的更新源。不支持使用组更新任务。

上一次的反恶意软件数据库更新也在 Protection Server 端回滚。在 SVM 上回滚数据库和应用程序模块更新后，将在受保护的虚拟机上启动一个特殊的本地 *Update* 任务。该任务使得 Light Agent 恢复为使用先前的一组恶意软件数据库。

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

### 在 Light Agent 模式下使用应用程序涉及的其他特殊考虑

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。

## 在 Endpoint Detection and Response Agent 模式下使用应用程序

Kaspersky Endpoint Security 在 Endpoint Detection and Response Agent 模式下可让您使用 Kaspersky Detection and Response 解决方案的功能来保护安装了第三方反病毒应用程序的设备。

在 Endpoint Detection and Response Agent 模式下，Kaspersky Endpoint Security 的标准保护和控制组件不会用于保护设备。第三方反病毒应用程序可提供标准的设备保护。Kaspersky Endpoint Security 在 Endpoint Detection and Response Agent 模式下会持续监控设备上运行的进程、打开的网络连接以及正在被修改的文件，并提供与 Detection and Response 解决方案的集成。

- Kaspersky Endpoint Detection and Response Expert (on-premise) 在 Open Single Management Platform (OSMP) 上（以下也称为“OSMP”）。
- Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 组件位于 Kaspersky Anti Targeted Attack Platform（以下也称为"KATA"）上。

Kaspersky Endpoint Security 12.4 for Linux 可以与 Dr. Web 反病毒应用程序协同工作。您可以在 Endpoint Security Detection and Response Agent 模式下在具有 Dr. Web 反病毒应用程序的设备上安装 Kaspersky Endpoint Security。

应用程序必须按以下顺序安装：首先是第三方反病毒应用程序，然后是 Kaspersky Security Center 网络代理，最后是 Kaspersky Endpoint Security 应用程序（在 Endpoint Detection and Response Agent 模式下）。这一点很重要，因为第三方应用程序的安装程序可能会将卡巴斯基应用程序识别为不兼容软件并将其删除。在设备上更新第三方应用程序后，我们建议确认 Kaspersky Endpoint Security 和网络代理正常运行，因为第三方应用程序的安装程序会重新检查设备是否存在不兼容软件，并可能删除卡巴斯基应用程序。

## 在 Endpoint Detection and Response Agent 模式下配置应用程序

如果要在 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，则需要执行以下操作：

1. 在要保护的每台虚拟机上以 Endpoint Detection and Response Agent 模式安装 Kaspersky Endpoint Security。

   您可以通过在命令行运行 `kesl-control --app-info` 命令来查询有关应用程序模式的信息。

2. 激活应用程序。您需要向应用程序添加单独的授权许可密钥“Kaspersky Endpoint Detection and Response Expert (on-premise) Add-on”（以下简称“EDR Expert (on-premise) 密钥”）。

   要在 Endpoint Detection and Response Agent 模式下激活应用程序，您只需要用于附加功能的密钥。您无需将主授权许可密钥添加到应用程序中。

3. 启用与您希望用于保护设备的 Detection and Response 解决方案的集成：

   - 要在 OSMP 平台上与 Kaspersky Endpoint Detection and Response Expert (on-premise) 集成，您需要启用 EDR Expert (on-premise) 组件，并在 Kaspersky Security Center Web Console 或命令行中管理集成设置。
   - 要在 Kaspersky Anti Targeted Attack Platform 平台上与 Kaspersky Endpoint Detection and Response 集成，您需要启用 EDR Expert (on-premise) 组件，并在 Kaspersky Security Center Web Console、管理控制台或命令行中管理集成设置。
   - 要在 Kaspersky Anti Targeted Attack Platform平台上与 Kaspersky Detection and Response集成，您需要启用 NDR (KATA)组件，并在 Kaspersky Security Center Web Console、管理控制台或命令行中管理集成设置。

   您可以检查 EDR Expert（本地部署）和 NDR (KATA) 组件的状态：

   - 在 Web Console 的设备属性中（**资产（设备）** → **受管理设备** →<设备名称>链接→ **应用程序** →<Kaspersky Endpoint Security 应用程序名称>链接→ **常规** → **组件**）。
   - 在命令行中运行 以下命令： `kesl-control --app-info`。

在 Endpoint Detection and Response Agent 模式下使用应用程序涉及的特殊考虑事项

如果 Kaspersky Endpoint Security 以Endpoint Detection and Response Agent 模式运行，则只有有限的应用程序组件子集和任务可用。安装后，应用程序设置如下：

- 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-premise)
  - 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 Endpoint Detection and Response 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`）。此设置无法修改。
- 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。以下参数无法修改：
  - 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-premise) 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。

# 分发包

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

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

- kesl-12.4.0-<版本号>.i386.rpm, kesl_12.4.0-<版本号>_i386.deb

  其中包含主要的应用程序文件。可以根据程序包管理器的类型将程序包安装到 32 位操作系统。

- kesl-12.4.0-<版本号>.x86_64.rpm, kesl_12.4.0-<版本号>_amd64.deb

  其中包含主要的应用程序文件。可以根据程序包管理器的类型将程序包安装到 64 位操作系统。

- kesl-12.4.0-<版本号>.aarch64.rpm, kesl_12.4.0-<版本号>_arm64.deb

  其中包含主要的应用程序文件。相关软件包管理器的软件包可以安装在 Arm® 架构的 64 位操作系统上。

- kesl-gui-12.4.0-<版本号>.i386.rpm, kesl-gui_12.4.0-<版本号>_i386.deb

  其中包含应用程序图形用户界面的文件。可以根据程序包管理器的类型将程序包安装到 32 位操作系统。

- kesl-gui-12.4.0-<版本号>.x86_64.rpm, kesl-gui_12.4.0-<版本号>_amd64.deb

  其中包含应用程序图形用户界面的文件。可以根据程序包管理器的类型将程序包安装到 64 位操作系统。

- kesl-gui-12.4.0-<版本号>.aarch64.rpm, kesl-gui_12.4.0-<版本号>_arm64.deb

  其中包含应用程序图形用户界面的文件。相关软件包管理器的软件包可以安装在 Arm 架构的 64 位操作系统上。

- kesl-12.4.0.<版本号>.zip

  包含用于使用 Kaspersky Security Center 远程安装应用程序的文件，包括 license.<语言 ID> 和 ksn_license.<语言 ID> 文件。

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

- ksn_license.<语言 ID>

  该文件包含卡巴斯基安全网络声明文本。

- license.<语言 ID>

  该文件包含最终用户授权许可协议文本。最终用户授权许可协议规定了使用该应用程序的条款。

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。

# 硬件和软件要求

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

## 硬件要求

Kaspersky Endpoint Security 具有以下硬件要求：

最低硬件要求

- 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 的交换分区
- 对于64 位操作系统，应用程序有 2GB RAM 可用（对于 32 位操作系统，应用程序有 1GB RAM 可用）。
- 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）。
- 使用图形接口时，显示器必须能够显示 1000 像素宽、600 像素高的窗口（如果应用屏幕缩放，这些尺寸也会被缩放）。
- 如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则需要带宽为 100 Mbps 的虚拟网络接口。

Arm 架构的最低硬件要求

- Armv8.2-A Kunpeng 920 或 Armv8-A Baikal-M (BE-M1000) 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）。
- 使用图形接口时，显示器必须能够显示 1000 像素宽、600 像素高的窗口（如果应用屏幕缩放，这些尺寸也会被缩放）。

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

# 软件要求

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

- 支持的 32 位操作系统：
  - Debian GNU/Linux 12.7、12.8、12.9、12.10、12.11、12.12。
- 支持的 64 位操作系统：
  - AlmaLinux OS 8.6、8.7、8.8、8.9。
  - AlmaLinux OS 9.4、9.5、9.6。
  - AlterOS® 2025。
  - Amazon™ Linux 2023。
  - Astra Linux Common Edition 2.12。
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)。
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)。
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)。
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.8)。
  - Astra Linux Special Edition RUSB.10015-03 (operational update 7.6)。
  - Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)。
  - Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3)。
  - Astra Linux Special Edition RUSB.10015-37 (operational update 7.7)。

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

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

  - CentOS 7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9。
  - CentOS Stream 8。
  - CentOS Stream 9。
  - CentOS Stream 10。

- Debian GNU/Linux 12.7、12.8、12.9、12.10、12.11、12.12。
- Debian GNU/Linux 13.0、13.1、13.2。
- EMIAS 1.0。
- EulerOS 2.0 SP10。
- Fedora Linux 41。
- Kylin Desktop OS V10 SP1。
- Linux Mint 21.3。
- Linux Mint 22.2。
- Mostech 12 版本 2021.1。
- openSUSE Leap 15.6。
- Oracle Linux 7.3、7.4、7.5、7.6、7.7、7.8、7.9。
- Oracle Linux 8.5、8.6、8.7、8.8、8.9。
- Oracle Linux 9.4、9.5、9.6。
- Red Hat Enterprise Linux 7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9。
- Red Hat Enterprise Linux 8.5、8.6、8.7、8.8、8.9。
- Red Hat Enterprise Linux 9.4、9.5、9.6。
- Red Hat Enterprise Linux 10.0, 10.1。
- Rocky Linux 8.6、8.7、8.8、8.9。
- Rocky Linux 9.4、9.5、9.6。
- Linux 8.10、9.1 9.5、9.6。
- SberOS 3.4.0、3.5.0。
- SUSE Linux Enterprise Server 12.5、12.6、12.7。
- SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7。
- Ubuntu® 22.04 LTS。
- Ubuntu 24.04 LTS。
- ALT Education 10。
- ALT Education 11。
- ALT Workstation 11。

- ALT Server 11。
- ALT SP Workstation 版本 10。
- ALT SP Server 版本 10。
- Atlant， Alcyone build，版本 2022.02。
- GosLinux 7.2。
- M OS 12 Server 版本 2021.1。
- Mos OS 15.5 Arbat。
- MSVSphere 9.4 Workstation。
- MSVSphere 9.4 Server。
- MES OS 12 V 版本 2021.1。
- MES OS 12 Panel 版本 2021.1。
- MES OS 12 Desktop 版本 2021.1。
- OSnova 2.14。
- OSnova 3.0.5。
- 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。
- SintezM-Client 8.6。
- SintezM-Server 8.6。

- Arm 架构的 64 位操作系统：
  - Astra Linux Special Edition RUSB.10152-02 (operational update 4.7)。
  - CentOS Stream 9。
  - EulerOS 2.0 SP10。
  - SUSE Linux Enterprise Server 15.4、15.5、15.6、15.7。
  - Ubuntu 22.04 LTS。

- ALT SP Workstation 版本 10。
- ALT SP Server 版本 10。
- RED OS 8.0。

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

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

# Light Agent 模式的其他软件要求

Kaspersky Endpoint Security 可以作为Kaspersky Security for Virtualization Light Agent 6.4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。

Kaspersky Endpoint Security 的软件和硬件要求在特定限制下适用于以 Light Agent 模式运行 Kaspersky Endpoint Security 的虚拟机。

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

必须在想要保护的虚拟机上安装以下软件包，具体取决于部署了 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的虚拟基础架构：

- 在 Microsoft Hyper-V 基础结构中，必须在虚拟机上安装 Integration Services 软件包。
- 在 VMware vSphere 基础架构中，必须在虚拟机上安装 VMware Tools 软件包。
- 在 XenServer 基础架构中，必须在虚拟机上安装 XenTools。
- 在 HUAWEI FusionSphere 基础架构中，必须在虚拟机上安装 HUAWEI Tools 软件包。
- 在基于 KVM、OpenStack、VK 私有云、TIONIX 云平台、Astra Linux、ALT Server Virtualization、Basis.Dynamix 或 Basis Dynamix Standard 的基础架构中，必须在虚拟机上安装 QEMU Guest Agent。

# 支持的 Kaspersky Security Center 版本

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

- Kaspersky Security Center Windows 14、14.2、15.1：可以使用 MMC 管理插件通过管理控制台管理 Kaspersky Endpoint Security，也可以使用 Web 管理插件通过 Kaspersky Security Center Web Console 进行管理。
- Kaspersky Security Center Linux 15.1、15.2、15.3、15.4、16.0、16.1、16.2：可以使用 Web 管理插件通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security。

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

- Kaspersky Security Center Windows 14.2、15.1。
- Kaspersky Security Center 15.4、16.0、16.1、16.2。

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

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

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

- Kaspersky Security Center Windows 14.2、15.1。
- Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2。

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

- Kaspersky Security Center Windows 15.1。
- Kaspersky Security Center Linux 15.3、15.4、16.0、16.1、16.2。

# KATA 和 OSMP 平台上支持的解决方案版本

Kaspersky Endpoint Security 与基于 Kaspersky Anti Targeted Attack Platform 的以下解决方案兼容：

- Kaspersky Anti Targeted Attack Platform 6.0（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA) 和 Sandbox）。
- Kaspersky Anti Targeted Attack Platform 6.1（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA) 和 Sandbox）。
- Kaspersky Anti Targeted Attack Platform 7.0（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA) 和 Sandbox）。
- Kaspersky Anti Targeted Attack Platform 7.1（Kaspersky Endpoint Detection and Response (KATA)、Kaspersky Network Detection and Response (KATA) 和 Sandbox）。
- Kaspersky Anti Targeted Attack Platform 8.0（Kaspersky Network Detection and Response (KATA) 和 Sandbox）。

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。

Kaspersky Endpoint Security 与 Open Single Management Platform（以下简称 OSMP）上的 Endpoint Detection and Response Expert（本地部署）8.0 兼容。

关于 Kaspersky Endpoint Detection and Response Expert（本地部署）8.0 的更多信息，请参阅Kaspersky Endpoint Detection and Response Expert（本地部署）帮助。

# 新功能

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

- 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。
- EDR (KATA) 组件提供与 Kaspersky Endpoint Detection and Response (KATA) 的集成，已被重命名为 EDR Expert (OSMP)。该组件还提供 Kaspersky Endpoint Detection and Response Expert (on-premise) 集成。集成任务已被重命名为 *Kaspersky Endpoint Detection and Response Expert (on-premise) 集成* (KATAEDR, ID: 24)。
- 现在，您可以设置与 Kaspersky Endpoint Detection and Response Expert (on-premise) 的集成，这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-premise) 的组件部署在 Open Single Management Platform (OSMP) 上。与 Kaspersky Endpoint Detection and Response Expert（本地部署）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 (OSMP) 组件，该组件提供与 Kaspersky Endpoint Detection and Response Expert（本地部署）和Kaspersky Endpoint Detection and Response (KATA) 的集成。
  - 通过命令行或在 Web Console 的策略属性中在 *Kaspersky Endpoint Detection and Response Expert (on-premise) 集成*任务的设置中选择一种集成模式。
- 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。策略中的部分结构进行了重新设计，以便更快地找到所需功能。

- 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，或者在 命令行 中查看此列表时，现在还会显示有关挂载点位于命名空间中的信息。
- 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
- 支持的操作系统列表已更新。

# 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。

## Web 插件 12.4.0.8289 中修复的问题列表

| 标识符 | 描述 |
| --- | --- |
| 10724878 | 将策略应用于设备时，`InterceptorApplyStrategy` 配置使用的是 `RestartServiceManually` 值，而不是默认值 `RestartServiceAutomatically`。 |

# 准备安装 Kaspersky Endpoint Security

## 常规操作

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

- 检查您的设备是否满足应用程序的硬件和软件要求。
- 确保您的设备上未安装第三方反病毒软件。
- 确保您的设备上未安装 Kaspersky Endpoint Agent for Linux。如果已安装 Kaspersky Endpoint Agent for Linux，您将在安装过程中看到一条关于需要手动将其删除的消息。
- 如果您计划使用 Kaspersky Security Center 管理 Kaspersky Endpoint Security，请准备在设备上安装 Kaspersky Security Center 网络代理（有关详细信息，请参阅 Kaspersky Security Center 帮助）。

  如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟化环境，则必须使用 Kaspersky Security Center 来管理该应用程序。

- 如果要使用 SELinux 访问控制系统，则需要确保操作系统上已安装 semanage 实用程序。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。
- 如果希望使用图形用户接口，需要确保您的设备满足 GUI 软件包的依赖项。如果设备位于隔离的网络段中，且无法访问软件包管理器的存储库，我们建议您在参考设备上检查依赖项列表（libice6、libsm6、libx11-6、libx11-xcb1、libxcb-icccm4、libxcb-image0、libxcb-keysyms1、libxcb-randr0、libxcb-render-util0、libxcb-render0、libxcb-shape0、libxcb-shm0、libxcb-sync1、libxcb-xfixes0、libxcb-xinerama0、libxcb-xkb1、libxcb1、libxi6、libxml2、zlib1g），然后在安装 GUI 之前将这些软件包下载并分发到所有设备。
- 如果要使用图形用户界面，则需要确保操作系统上已安装 Zenity 实用程序。
- 在操作系统不支持 fanotify 技术的设备上，请确保安装以下软件：
  - 用于编译应用程序和运行任务的软件包（gcc、binutils、glibc、glibc-devel、make）
  - 包含操作系统内核头文件的软件包，用于编译 Kaspersky Endpoint Security 模块
- 在运行 SUSE Linux Enterprise Server 15 操作系统的设备上，必须安装 insserv-compat 软件包。
- 默认情况下，Astra Linux 操作系统会阻止 ptrace（禁用 ptrace 功能），这可能会影响 Kaspersky Endpoint Security 的操作。为使 Kaspersky Endpoint Security 正常工作，请在安装 Astra Linux 时解除阻止 ptrace。如果已经安装 Astra Linux，请参阅“Astra Linux 帮助中心”网站，获取有关如何启用/禁用此模式的说明（“**阻止 ptrace**”部分中的“**配置保护和阻止机制**”）。

  您可以通过指定内核参数值对 `kernel.yama.ptrace_scope=3` 来禁用 ptrace 跟踪。在这种情况下，应用程序中将会发生以下情况：
  - 当应用程序崩溃时，无法创建 kesl 进程的转储文件。
  - 行为检测组件将无法接收进程的环境设置。

- 在内核版本高于 5.7 的操作系统上，应用程序控制组件将无法读取命令行参数和进程环境变量，因为读取 /proc/pid/syscall 和 /proc/pid/mem 被禁止。在内核版本为 5.0 的操作系统上，应用程序控制组件将无法正常运行。

- 进程内存和内核内存扫描将不会在扫描任务中起作用，因为读取 /proc/pid/mem 被禁止。

- 由于不允许读取 /proc/pid/mem，因此无法保证在强制访问控制模式下 YARA 对进程内存进行扫描。

- 为使防火墙管理、Web 威胁防护和网络威胁防护组件正常运行，您的设备上需要安装 iptables 实用程序。

- 为使 Kaspersky Endpoint Security MMC 管理插件正常工作，必须在安装了 Kaspersky Security Center 管理服务器的设备上安装 Microsoft® Visual C++® 2015 Redistributable Update 3 RC（请参阅 https://www.microsoft.com/en-us/download/details.aspx?id=52685）。

- 要正确运行应用程序，请确保 root 账户是以下目录的所有者，并且只有所有者拥有对这些目录的写入权限：/var、/var/opt、/var/opt/kaspersky、/var/log/kaspersky、/opt、/opt/kaspersky、/usr/bin、/usr/lib、/

- 确保在操作系统中配置了操作系统供应商推荐的文件描述符限制。要检查限制，请运行命令 `cat /proc/sys/fs/file-max`。当应用程序运行时，操作系统使用的描述符数量可能会显著增加。通常，我们建议通过在 /etc/sysctl.conf 文件中指定 `fs.file-max=9223372036854775807` 来禁用文件限制。更改此设置的值后，必须重新启动操作系统。

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

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

- 确保要保护的虚拟机满足Light Agent 模式的常规要求。

- 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 的安装和初始配置

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

以下情景描述了如何安装和执行 Kaspersky Endpoint Security 的初始配置、如何安装 Kaspersky Security Center 网络代理以及 Kaspersky Endpoint Security 管理插件。此安装方案依赖于您在使用 Kaspersky Endpoint 时所用的模式。

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

## 标准模式

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

1. **网络代理的安装和初始配置**

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

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

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

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

3. **安装应用程序包和图形用户界面**

   Kaspersky Endpoint Security 以 DEB 和 RPM 软件包进行分发。应用程序和应用程序的图形用户界面作为不同的软件包提供。安装 Kaspersky Endpoint Security，并在必要时从相应格式的软件包中安装图形界面。

   可以通过以下方法之一进行安装：

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

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

   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。

   如果您使用 Kaspersky Security Center 安装了 Kaspersky Endpoint Security，则安装过程中会根据安装包中指定的参数自动执行初始配置。完成安装后，请完成开始过程。

   如果您使用命令行安装了 Kaspersky Endpoint Security，请运行初始设置向导，并通过交互方式或自动模式来执行初始配置。

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。

## Light Agent 模式

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

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

1. **网络代理的安装和初始配置**

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

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

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

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

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

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

   Kaspersky Endpoint Security 以 DEB 和 RPM 软件包进行分发。从所需格式的软件包安装 Kaspersky Endpoint Security。应用程序和应用程序的图形用户界面作为不同的软件包提供。

   如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则不支持使用该应用程序的图形用户界面。

   可以通过以下方法之一安装应用程序：

   - 使用 Kaspersky Security Center。

     在开始安装之前，您需要在安装包参数中或者在安装包中包含的配置文件中指定初始配置设置。

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

     设置值区分大小写。

   - 使用命令行。如果使用命令行执行安装，则在初始配置期间选择应用程序使用模式为交互或者自动模式。

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

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。

如果您使用 Kaspersky Security Center 安装了 Kaspersky Endpoint Security，则安装过程中会根据安装包中指定的参数自动执行初始配置。完成安装后，请完成开始过程。

如果您使用命令行安装了 Kaspersky Endpoint Security，请运行初始设置向导，并通过交互方式或自动模式来执行初始配置。在初始配置期间通过以下方式之一选择 Light Agent 模式：

- 在初始配置向导的"在 Light Agent 模式下使用应用程序"步骤中输入 `yes`。
- 在初始配置文件中指定 `KSVLA_MODE=Yes` 设置。

  该设置值区分大小写。

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

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。

## Endpoint Detection and Response Agent 模式

我们建议在设备上安装第三方反病毒应用程序后再进行安装。

如果您计划在 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，安装过程包括以下步骤：

1. **网络代理的安装和初始配置**

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

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

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

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

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

   Kaspersky Endpoint Security 以 DEB 和 RPM 软件包进行分发。从所需格式的软件包安装 Kaspersky Endpoint Security。应用程序和应用程序的图形用户界面作为不同的软件包提供。

   可以通过以下方法之一安装应用程序：

   - 使用 Kaspersky Security Center。

在开始安装之前，您需要在安装包参数中或者在安装包中包含的配置文件中指定初始配置设置。

您需要选择 Endpoint Detection and Response Agent 模式（在配置文件中，设置 `ENDPOINT_AGENT_MODE=Yes`）。

该设置值区分大小写。

- 使用命令行。如果使用命令行执行安装，则在初始配置期间选择应用程序使用模式为交互或者自动模式。

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

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。

如果您使用 Kaspersky Security Center 安装了 Kaspersky Endpoint Security，则安装过程中会根据安装包中指定的参数自动执行初始配置。完成安装后，请完成开始过程。

如果您使用命令行安装了 Kaspersky Endpoint Security，请运行初始设置向导，并通过交互方式或自动模式来执行初始配置。在初始配置期间，通过以下方式之一选择 Endpoint Detection and Response Agent 模式：

- 在初始配置向导的“在 Endpoint Detection and Response Agent 模式下使用应用程序”步骤中输入 `yes`。
- 在初始配置文件中指定 `ENDPOINT_AGENT_MODE=Yes` 设置。

该设置值区分大小写。

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。

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

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

开始在 Linux 设备上安装网络代理之前，您必须执行一些准备步骤。有关如何准备设备以安装网络代理的说明，请参阅“Kaspersky Security Center 帮助”。该过程取决于操作系统。

您可以执行网络代理的安装和初始配置：

- 使用 Kaspersky Security Center Web Console 或管理控制台从管理员工作站远程操作。网络代理安装包用于远程安装。
- 使用命令行：
  - 在静默模式下并使用应答文件。应答文件是一个文本文件，其中包含一组自定义设置，用于网络代理的安装和初始配置。有关网络代理的安装选项和初始配置的说明，请参阅“Kaspersky Security Center 帮助”（“在静默模式（使用应答文件）下安装 Linux 网络代理”部分）。
  - 根据您的包管理器，通过 RPM 或 DEB 包以交互式方式进行操作。在这种情况下，安装完成后，您需要使用脚本执行网络代理的初始配置。

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

# 安装 Kaspersky Endpoint Security 管理插件

以下 Kaspersky Endpoint Security 管理插件用于通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security：

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

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

如果您使用 Kaspersky Security Center 管理控制台来管理应用程序，您还可以将使用早期版本的管理插件创建的策略和任务转换为较新版本。

# 安装 Kaspersky Endpoint Security Web 插件

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

您可以按如下方式安装该 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 的初始设置向导的更多信息，请参阅“Kaspersky Security Center 帮助”部分。

- 使用卡巴斯基 Web 插件列表或外部源的分发包手动安装。

*如要手动安装 Kaspersky Endpoint Security Web 插件：*

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

   已安装的 Web 插件列表将打开。

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

   - 从卡巴斯基 Web 插件列表中安装：

     a. 单击“**添加**”按钮。

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

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

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

d. 等待安装完成，然后在信息窗口中单击“**确定**”。

e. 这将打开**Web 插件设置**窗口。

> 在 Kaspersky Security Center Web Console 14.2 中，您需要刷新浏览器页面才能打开**Web插件设置**窗口。

f. 等待安装完成，然后在信息窗口中单击“**确定**”。

- 从第三方来源安装 Web 插件（安装 Web 插件所需的压缩文件包含在分发包中，也可以从卡巴斯基网站下载）：

  a. 单击“**从文件添加**”按钮。

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

  c. 单击“**添加**”按钮。

  d. 等待安装完成，然后在信息窗口中单击“**确定**”。

  e. 这将打开**Web 插件设置**窗口。

  > 在 Kaspersky Security Center Web Console 14.2 中，您需要刷新浏览器页面才能打开**Web插件设置**窗口。

  f. 等待安装完成，然后在信息窗口中单击“**确定**”。

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

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

# 安装 Kaspersky Endpoint Security MMC 插件

Kaspersky Endpoint Security管理 MMC 插件必须安装在已安装 Kaspersky Security Center 管理控制台的同一设备上。

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

*如要安装 MMC 插件：*

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

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

安装后，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：

   - 使用**管理服务器 <服务器名称>**节点上下文菜单中的“**属性**”项；
   - 在“**管理服务器**”部分中，单击位于**管理服务器 <服务器名称>**节点工作区中的“**管理服务器属性**”链接。

2. 在左侧列表的“**高级**”部分中，选择“**有关已安装的应用程序管理插件的信息**”部分。

   在窗口右侧，已安装的管理插件列表显示 Kaspersky Endpoint Security 的管理 MMC 插件：**Kaspersky Endpoint Security <版本号> for Linux**。

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

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

使用 Kaspersky Security Center 进行安装涉及以下步骤：

1. 创建安装包。

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

   您可以在安装包的属性中或安装包中包含的 autoinstall.ini 配置文件中指定应用程序的初始配置设置。

   > 如果您计划使用 Kaspersky Endpoint Security在 Light Agent 模式或者 Endpoint Detection and Response Agent 模式下保护虚拟环境（作为Kaspersky Security for Virtualization Light Agent 解决方案的一部分），则必须管理应用程序的初始配置设置。默认在标准模式下使用应用程序。

   如果您计划在基本模式或者 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security 应用程序，您可以在创建安装包时将以下内容添加到安装包中：

   - 安装期间自动激活应用程序的授权许可密钥
   - 预先下载的应用程序数据库，避免安装后更新数据库

   您也可以稍后在入门流程中激活该应用程序并更新数据库。

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

2. 在公司网络的设备上部署 Kaspersky Endpoint Security 应用程序。

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

- 使用“保护部署向导”安装应用程序。
- 使用远程安装任务安装应用程序。

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

- 使用远程安装向导安装应用程序。
- 使用远程安装任务安装应用程序。

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

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

3. 启动。

   在使用应用程序之前，您需要完成应用程序的初始配置并准备应用程序运行。

   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。

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

# 在 Web Console 中创建安装包

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

- 使用先前准备的压缩文件。
- 使用卡巴斯基服务器上托管的分发包。

如果您计划在用来保护虚拟环境的 Light Agent 模式或者 Endpoint Detection and Response Agent 下使用 Kaspersky Endpoint Security，则需要在初始配置设置中指定应用程序模式。您可以在已创建安装包的属性中的“**设置**”选项卡中或者在安装包中所含的配置文件中指定应用程序的初始配置设置。

*要准备用于创建安装包的压缩文件：*

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

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

   - 要安装 Kaspersky Endpoint Security：
     - kesl-12.4.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl_12.4.0-<版本号>_i386.deb （适用于使用 dpkg 的 32 位操作系统）
     - kesl-12.4.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）
     - kesl-gui-12.4.0-<内部版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
     - kesl-12.4.0-<版本号>.aarch64.rpm（适用于基于 Arm 架构且使用 rpm 的 64 位操作系统）
     - kesl-gui_12.4.0-<内部版本号>_arm64.deb（适用于基于 Arm 架构且使用 dpkg 的 64 位操作系统）
   - 要安装应用程序的图形用户界面：
     - kesl-gui-12.4.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl-gui-12.4.0-<内部版本号>_i386.deb（适用于使用 dpkg 的 32 位操作系统）
     - kesl-gui-12.4.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）
     - kesl-gui-12.4.0-<内部版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
     - kesl-gui-12.4.0-<版本号>.aarch64.rpm（适用于基于 Arm 架构且使用 rpm 的 64 位操作系统）
     - kesl-gui_12.4.0-<内部版本号>_arm64.deb（适用于基于 Arm 架构且使用 dpkg 的 64 位操作系统）

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

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

如果您不打算安装图形界面，请在已创建安装包的属性中或在 autoinstall.ini 配置文件中编辑相应的设置（`USE_GUI=No`），以禁用该界面。否则，安装将失败。

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，请将您需要的所有类型的操作系统和包管理器的文件放在目录中。

3. 如果您打算在标准模式下使用 Kaspersky Endpoint Security 应用程序并且想要使用预先下载的应用程序数据库：

   a. 将准备好的适用于所有操作系统类型的数据库的压缩文件放入该文件夹中。

   b. 在初始配置设置中，在安装应用程序后禁用数据库更新任务。您可以在已创建安装包的属性中，或者在 autoinstall.ini 配置文件中配置相关的设置（`UPDATE_EXECUTE=No`）。autoinstall.ini 文件位于 kesl.zip 压缩文件所解压到的文件夹中。

4. 如果想要使用配置文件执行应用程序的初始配置，请打开 autoinstall.ini 配置文件并根据需要进行编辑。

   如果您计划使用 Kaspersky Endpoint Security 以 Light Agent 模式保护虚拟环境，则需要在 autoinstall.ini 配置文件中设置 `KSVLA_MODE=Yes`。

   如果您计划使用 Kaspersky Endpoint Security 以 Endpoint Detection and Response Agent 模式，则需要在 autoinstall.ini 配置文件中设置 `ENDPOINT_AGENT_MODE=Yes`。

   autoinstall.ini 文件中的设置值区分大小写。

   您也可以稍后在已创建安装包的属性中的“**设置**”选项卡中管理初始配置设置。

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。

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

1. 在 Web Console 主窗口中，选择以下任一部分：

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

   将打开管理服务器上可用的安装包列表。

2. 单击“**添加**”按钮。
   创建安装包的向导将启动。

3. 选择要用于创建安装包的方法：

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

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

4. 根据所选的软件包创建方法：

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

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。使用安装包，您可以在公司网络中的设备上安装应用程序或更新应用程序版本。

7. 如有必要，管理初始配置设置。为此，打开安装包的属性并转到"**设置**"选项卡。

   早于 14.2 版的 Kaspersky Security Center Web Console 不支持在Kaspersky Endpoint Security 安装包的属性中提供初始配置设置。使用 autoinstall.ini 配置文件来配置设置。

# 在 Web Console 中进行初始配置设置

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**。

您还可以使用安装包中所含的配置文件指定应用程序的初始配置设置。

初始配置设置

| 设置 | 描述 |
| --- | --- |
| **KSC 中事件的语言** | 选择发送到 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。<br>应用程序使用 UTF-8 编码。<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>您还可以在安装后激活应用程序。<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** | 选择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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |
| **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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |
| **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>://]<IP 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>]@]<IP address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。<br>不支持通过 HTTPS 连接到代理服务器。<br>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |
| **安装内核源** | 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。 |
| **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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |
| **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，SELinux 将自动配置为与 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。 |
| **在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** | 选择应用程序的模式。<br>• **保护工作站和服务器的标准模式**（默认）。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>• **Light Agent 用于保护虚拟环境**。如果选择此选项，则应用程序将以用于保护虚拟环境的 Light Agent 模式使用（作为 Kaspersky Security for Virtualization Light Agent 的一部分）。 |
| **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。 |
| **受保护的虚拟机用作服务器** | 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。 |
| **拦截机制** | 选择应用程序要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。 |
| **如果可更新内核模块启动失败** | 选择当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。 |

# 在管理控制台中创建安装包

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

如果您计划在用来保护虚拟环境的 Light Agent 模式或者 Endpoint Detection and Response Agent 下使用 Kaspersky Endpoint Security，则需要在初始配置设置中指定应用程序模式。您可以通过以下方式指定初始配置设置：在创建安装包时；在已创建的安装包属性中的“**设置**”部分；或者在安装包中所含的配置文件中指定。

*要准备用于创建安装包的文件：*

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

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

   - 要安装 Kaspersky Endpoint Security：
     - kesl-12.4.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl_12.4.0-<版本号>_i386.deb （适用于使用 dpkg 的 32 位操作系统）
     - kesl-12.4.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）
     - kesl-gui-12.4.0-<内部版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
     - kesl-12.4.0-<版本号>.aarch64.rpm（适用于基于 Arm 架构且使用 rpm 的 64 位操作系统）
     - kesl-gui_12.4.0-<内部版本号>_arm64.deb（适用于基于 Arm 架构且使用 dpkg 的 64 位操作系统）
   - 要安装应用程序的图形用户界面：
     - kesl-gui-12.4.0-<版本号>.i386.rpm（适用于使用 rpm 的 32 位操作系统）
     - kesl-gui-12.4.0-<内部版本号>_i386.deb（适用于使用 dpkg 的 32 位操作系统）
     - kesl-gui-12.4.0-<版本号>.x86_64.rpm（适用于使用 rpm 的 64 位操作系统）
     - kesl-gui-12.4.0-<内部版本号>_amd64.deb（适用于使用 dpkg 的 64 位操作系统）
     - kesl-gui-12.4.0-<版本号>.aarch64.rpm（适用于基于 Arm 架构且使用 rpm 的 64 位操作系统）
     - kesl-gui_12.4.0-<内部版本号>_arm64.deb（适用于基于 Arm 架构且使用 dpkg 的 64 位操作系统）

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

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

如果您不打算安装图形界面，请在创建安装包时、在已创建安装包的属性中或在 autoinstall.ini 配置文件中编辑相应的设置（`USE_GUI=No`），以禁用该界面。否则，安装将失败。

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，请将您需要的所有类型的操作系统和包管理器的文件放在目录中。

3. 如果您打算在标准模式下使用 Kaspersky Endpoint Security 应用程序并且想要使用预先下载的应用程序数据库：

   a. 将准备好的适用于所有操作系统类型的数据库的压缩文件放入该文件夹中。

   b. 在初始配置设置中，在安装应用程序后禁用数据库更新任务。您可以在创建安装包时、在已创建安装包的属性中或在 autoinstall.ini 配置文件中编辑相关的设置（`UPDATE_EXECUTE=No`）。autoinstall.ini 文件位于 kesl.zip 压缩文件所解压到的目录中。

4. 如果想要使用配置文件执行应用程序的初始配置，请打开 autoinstall.ini 配置文件并根据需要进行编辑。

   如果您计划使用 Kaspersky Endpoint Security 以 Light Agent 模式保护虚拟环境，则需要在 autoinstall.ini 配置文件中设置 `KSVLA_MODE=Yes`。

   如果您计划使用 Kaspersky Endpoint Security 以 Endpoint Detection and Response Agent 模式，则需要在 autoinstall.ini 配置文件中设置 `ENDPOINT_AGENT_MODE=Yes`。

   autoinstall.ini 文件中的设置值区分大小写。

   您也可以稍后在创建安装包时，或者在已创建安装包的属性中的“**设置**”部分，管理初始配置设置。

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

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

   创建安装包的向导将启动。
3. 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. 选择 Kaspersky Endpoint Security 分发包。为此，请使用**“浏览”**按钮打开标准浏览窗口，然后指定 kesl.kud 文件的路径。该文件位于 kesl.zip 压缩文件所解压到的文件夹中。

   应用程序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。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. 如有必要，管理初始配置设置。

   您也可以稍后在已创建安装包的属性中的“**设置**”部分，执行应用程序的初始配置。
8. 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。
9. 结束向导。

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

# 在管理控制台中进行初始配置设置

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。

您还可以使用安装包中所含的配置文件指定应用程序的初始配置设置。

初始配置设置

| 设置 | 描述 |
| --- | --- |
| **KSC 中事件的语言** | 选择发送到 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，则默认使用英语。<br>• 明确指定的语言。<br>应用程序使用 UTF-8 编码。<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>您还可以在安装后激活应用程序。<br>只有在标准模式下使用应用程序时，该设置才适用。 |
| **选择更新源** | 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）。<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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |
| **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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |

| 设置 | 描述 |
| --- | --- |
| **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>://]<IP 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>]@]<IP address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。<br>不支持通过 HTTPS 连接到代理服务器。<br>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |
| **安装内核源** | 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。 |
| **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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 |
| **具有管理员角色的用户** | 输入您想要向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。 |
| **自动配置 SELinux** | 如果选中此复选框，SELinux 将自动配置为与 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。 |
| **在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。 |
| **应用程序模式** | 这组设置包含**配置**按钮，您可以单击该按钮打开**应用程序模式**窗口。在此窗口中，您可以选择应用程序模式。<br>• **保护工作站和服务器的标准模式**（默认）。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>• **Light Agent 用于保护虚拟环境**。如果选择此选项，则应用程序将以用于保护虚拟环境的 Light Agent 模式使用（作为 Kaspersky Security for Virtualization Light Agent 的一部分）。 |
| **受保护的虚拟机用作服务器**（**应用程序模式**窗口） | 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。 |
| **启用 VDI 保护模式**（**应用程序模式**窗口） | 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。 |

| 设置 | 描述 |
| --- | --- |
| **系统事件拦截** | 这组设置包含**配置**按钮。点击此按钮将打开**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）。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。 |
| **如果可更新内核模块启动失败**<br>（**系统事件拦截设置**窗口）。 | 选择当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。 |

# 准备包含应用程序数据库的压缩文件，以创建包含集成数据库的安装包

您可以创建一个用于远程安装的安装包，并在其中包含预先下载的应用程序数据库。例如，如果您在具有 Astra Linux 特别版操作系统的设备上安装应用程序，这可能会很有用。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。

*要创建带有应用程序安装数据库的压缩文件：*

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

在 Kaspersky Security Center 管理控制台或 Kaspersky Security Center Web Console 中创建安装包时，可以使用所创建的包含应用程序数据库的压缩文件。

# Autoinstall.ini 配置文件设置

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

设置值区分大小写。

| 设置 | 描述 | 值 |
| --- | --- | --- |
| KSVLA_MODE | 在 Light Agent 模式下使用 Kaspersky Endpoint Security。 | Yes – 在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境（用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。<br>No（默认值）– Kaspersky Endpoint Security 以标准模式或 Endpoint Detection and Response Agent 模式运行（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。 | Yes（默认值）– 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。 | 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（默认值）– 不启用 VDI 保护模式。 |
| ENDPOINT_AGENT_MODE | 在 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security | Yes — Kaspersky Endpoint Security 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。<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）。 |
| 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>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。 |
| 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 – 不从特权组中删除用户。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| LOCALE | 可选设置。<br>发送到 Kaspersky Security Center 的应用程序事件使用的区域设置。<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。 | 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<br>• `fr_FR.UTF-8` — 法语<br>• `ja_JP.UTF-8` — 日语<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>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 | 用于向应用程序添加授权许可密钥的激活码。<br>只有在标准模式下使用应用程序时，该设置才适用。 | <激活码>，如果您想在安装过程中激活应用程序。<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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 | `SCServer` —使用 Kaspersky Security Center 管理服务器作为更新源。<br>`KLServers` — 使用卡巴斯基服务器作为更新源。默认情况下使用此值。<br>< 更新源地址 >。 |
| PROXY_SERVER | 用于连接到互联网的代理服务器的地址。<br>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 | 代理服务器的地址采用以下格式之一：<br>• `[<connection protocol>://]<IP 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>]@]<IP address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。<br>不支持通过 HTTPS 连接到代理服务器。 |
| UPDATE_EXECUTE | 在初始配置期间启动应用程序数据库更新任务。<br>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 | `Yes`（默认值）– 启动更新任务。<br>`No` — 不启动更新任务。 |
| KERNEL_SRCS_INSTALL | 在启动文件威胁防护任务时自动开始编译内核模块（适用于不支持 fanotify 技术的操作系统）。 | `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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 | `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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |
| 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。 | `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。 |
| 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>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 进行系统事件拦截。<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>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。 | `RestartServiceAutomatically`（默认值）自动重启应用程序以启动可更新内核模块。<br>`RestartServiceManually` 会在用户手动重启应用程序后，启动可更新内核模块。<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>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>`No` — 不在首次启动应用程序时创建跟踪文件。 |

如果要更改 autoinstall.ini 配置文件中的设置，请按以下格式指定设置的值：<设置名称>=<设置值>（设置名称与其值之间没有空格）。

# 使用 Kaspersky Security Center 开始

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

### 标准模式

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

1. 如果未使用添加到应用程序安装包中的密钥进行激活，请激活该应用程序。

   您可以使用管理控制台或 Kaspersky Security Center Web Console 创建和执行激活任务，还可以将授权许可密钥从 Kaspersky Security Center 密钥存储分发到设备。

2. 如果您没有将预先下载的应用程序数据库添加到应用程序的安装包中，请更新数据库和应用程序模块。您可以使用*更新*任务，该任务是在安装MMC 管理插件或 Kaspersky Endpoint Security 管理 Web 插件后由 Kaspersky Security Center 的初始配置向导自动创建的。

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

3. 配置一个策略，以便使用 Kaspersky Security Center 管理控制台（在管理控制台中管理策略、使用管理控制台创建策略）或 Web Console 对应用程序进行集中管理。您可以使用在安装管理 MMC 插件或 Kaspersky Endpoint Security 管理 Web 插件后由 Kaspersky Security Center 的初始配置向导自动创建的策略。

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

### Light Agent 模式

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

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

   需要在策略属性中配置以下设置：

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

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

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

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

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

   在 SVM 上激活解决方案并将 Light Agent 连接到 SVM 后，Protection Server 组件会将授权许可信息发送到 Light Agent 。您可以使用 Kaspersky Security Center 或在受保护的虚拟机的命令行上远程查看有关 Kaspersky Endpoint Security 应用程序作为解决方案的一部分使用的授权许可的信息。

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

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

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

您还可以使用管理控制台或Web Console中的策略和应用程序管理任务来配置应用程序。

# 使用命令行安装和初始配置应用程序

您可以使用命令行在客户端设备上安装 Kaspersky Endpoint Security 应用程序。

使用命令行安装涉及以下步骤：

1. 安装应用程序及其图形界面根据您想要使用 Kaspersky Endpoint Security 的模式，您可以选择以下安装选项：
   - 如果要在基本模式下使用 Kaspersky Endpoint Security，您可以：
     - 安装应用程序和图形界面。
     - 安装应用程序，不安装图形界面。
     - 在安装应用程序的设备上安装图形界面。

       无法在未安装应用程序的设备上安装图形界面。
   - 如果您想在 Light Agent 模式下使用 Kaspersky Endpoint Security，则必须安装不带图形界面的应用程序。不支持图形界面。

   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。
2. 应用程序的初始配置

   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通过运行 Kaspersky Endpoint Security 分发包中的初始设置向导来执行。您可以在交互模式或自动模式下执行应用程序的初始配置。

# 使用命令行安装应用程序

安装应用程序，不安装图形界面。

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

```
# rpm -i kesl-12.4.0-<内部版本号>.i386.rpm
```

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

```
# rpm -i kesl-12.4.0-<内部版本号>.x86_64.rpm
```

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

```
# apt-get install kesl-12.4.0-<内部版本号>.x86_64.rpm
```

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

```
# rpm -i kesl-12.4.0-<内部版本号>.aarch64.rpm
```

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

```
# apt-get install kesl-12.4.0-<内部版本号>.aarch64.rpm
```

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

```
# apt-get install ./kesl_12.4.0-<内部版本号>_i386.deb
```

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

```
# apt-get install ./kesl_12.4.0-<内部版本号>_amd64.deb
```

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

```
# apt-get install ./kesl_12.4.0-<内部版本号>_arm64.deb
```

安装应用程序的图形界面

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

```
# rpm -i kesl-gui-12.4.0-<内部版本号>.i386.rpm
```

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

```
# rpm -i kesl-gui-12.4.0-<内部版本号>.x86_64.rpm
```

*要从 RPM 软件包将图形界面安装到 64 位 ALT 操作系统，请执行以下命令：*

```
# apt-get install kesl-gui-12.4.0-<内部版本号>.x86_64.rpm
```

*若要通过 RPM 软件包将图形界面安装到 Arm 架构的 64 位操作系统，请执行以下命令：*

```
# rpm -i kesl-gui-12.4.0-<内部版本号>.aarch64.rpm
```

*要从 RPM 软件包将图形界面安装到 Arm 架构的 64 位 ALT 操作系统，请执行以下命令：*

```
# apt-get install kesl-gui-12.4.0-<内部版本号>.aarch64.rpm
```

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

```
# apt-get install ./kesl-gui_12.4.0-<内部版本号>_i386.deb
```

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

```
# apt-get install ./kesl-gui_12.4.0-<内部版本号>_amd64.deb
```

*若要通过 DEB 软件包将图形界面安装到 Arm 架构的 64 位操作系统，请执行以下命令：*

```
# apt-get install ./kesl-gui_12.4.0-<内部版本号>_arm64.deb
```

# 以交互模式对应用程序进行安装后配置

要以交互模式执行应用程序的初始配置，您需要运行 Kaspersky Endpoint Security 应用程序的初始设置向导。

> 您必须以 root 用户身份运行初始设置向导。

*要运行初始设置向导，请执行以下命令：*

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

此向导会逐步提示您输入 Kaspersky Endpoint Security 设置的值。当完成向导且释放控制台时，即表示安装后配置已完成。

*要检查返回码，执行以下命令：*

```
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。

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

## 选择标准模式或 Light Agent 模式

在此步骤中，指定是否打算在 Light Agent 模式下使用应用程序来保护虚拟环境（作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分）：

- 如果要在Light Agent 模式下使用 Kaspersky Endpoint Security，请输入`yes`。
- 如果您希望将 Kaspersky Endpoint Security 作为独立应用程序在标准模式下用于保护工作站和服务器，请输入`no`。

  如果打算在 Endpoint Detection and Response Agent 模式下使用该应用程序，还需要在此步骤中输入`no`。您可以在下一步中选择 Endpoint Detection and Response Agent 模式。

初始配置完成后，即无法更改应用程序使用模式。

## 定义虚拟机的角色

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

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

- 如果要将虚拟机作为服务器，请输入`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。

## 启用 VDI 保护模式

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

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

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。

## 选择模式：标准模式或 Endpoint Detection and Response Agent

只有在第一步中选择在标准模式下使用 Kaspersky Endpoint Security 时，才会显示此步骤。该应用程序不能同时在Light Agent 模式和 Endpoint Detection and Response Agent 模式下使用。

在此步骤中，指定您是否打算在 Endpoint Detection and Response Agent模式下使用 Kaspersky Endpoint Security：

- 如果您希望将 Kaspersky Endpoint Security 以 Endpoint Detection and Response Agent 模式用作支持卡巴斯基 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的应用程序，请输入 yes。
- 如果您希望将 Kaspersky Endpoint Security 作为独立应用程序在标准模式下用于保护工作站和服务器，请输入 no。

初始配置完成后，即无法更改应用程序使用模式。

## 选择区域设置

在此步骤中，应用程序以 RFC 3066 格式显示支持的区域设置列表。

请按照此处所列来指定区域设置。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。

## 查看最终用户授权许可协议和隐私策略

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

## 接受最终用户授权许可协议

在此步骤中，您必须接受或拒绝最终用户授权许可协议的条款。

退出查看模式后，请输入以下值之一：

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

如果您不接受最终用户授权许可协议的条款和条件，Kaspersky Endpoint Security 安装过程将中止。

## 接受隐私策略

在此步骤中，您必须接受或拒绝隐私策略的条款。

退出查看模式后，请输入以下值之一：

- 如果您接受隐私策略的条款，请输入 `yes`（或 `y`）。
- 如果您不接受隐私策略的条款，则输入 `no`（或 `n`）。

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

## 使用卡巴斯基安全网络

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

输入以下值之一：

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

拒绝参与卡巴斯基安全网络不会中断 Kaspersky Endpoint Security 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。

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

## 从特权组中删除用户

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

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

要从 kesladmin 和/或 keslaudit 组中删除所有检测到的用户，请输入 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。

## 将管理员角色分配给一位用户

在此步骤中，您可以向用户授予管理员 (admin) 角色。

输入要向其授予管理员角色的用户的名称。您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。

## 配置系统事件拦截机制

在此步骤中，确定使用各种系统事件拦截机制的可能性。如果设备的操作系统支持 fanotify 技术，您可以选择应用程序要使用的系统事件拦截方法：

- 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。如果设备的操作系统支持 fanotify，但不满足安装可更新内核模块的要求，则应用程序使用 fanotify 来拦截系统事件。

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”。

如果设备的操作系统不支持 fanotify，则应用程序将使用内核模块进行文件威胁防护。如果所有依赖项均可用，文件威胁防护启动时会自动启动内核模块编译。

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。

## 启用 SELinux 的自动配置

仅当您的操作系统上安装了 SELinux 时，才会显示此步骤。

在此步骤中，您可以启用 SELinux 访问控制系统的自动配置，以使用 Kaspersky Endpoint Security。

输入 yes 可启用 SELinux 的自动配置。如果 SELinux 无法自动配置（例如，缺少 semanage 实用程序），则应用程序会显示错误消息并提示用户手动配置 SELinux。

如果您不希望应用程序自动配置 SELinux，请输入 no。

默认情况下，应用程序建议为 yes。

如有必要，在应用程序的初始配置完成后，您可以在之后手动配置 SELinux 以使用该应用程序。

## 配置更新源

仅当您在向导的初始步骤中选择在标准模式或者 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，此步骤才会显示。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收 Light Agent 的数据库和应用模块更新。

在此步骤中，您必须为数据库和应用程序模块指定更新源。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。您可以在局域网或互联网上指定自定义更新源的地址。

# 配置代理服务器设置

仅当您在向导的初始步骤中选择在标准模式或者 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，此步骤才会显示。

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

*要配置代理服务器设置，请执行以下操作之一：*

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

    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。
- 如果不使用代理服务器连接到互联网，请输入no作为答案。

默认情况下，应用程序建议为 no。

完成初始配置后，您可以稍后管理代理服务器设置。

# 启动应用程序数据库更新

仅当您在向导的初始步骤中选择在标准模式或者 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，此步骤才会显示。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收 Light Agent 的数据库和应用模块更新。

在此步骤中，您可以在客户端设备上运行应用程序数据库更新任务。

如果您不想开始下载应用程序数据库，请输入 no。

如果想要在设备上启动数据库更新任务，请输入 yes 。

默认情况下，应用程序建议为 yes。

如果选择 yes，则数据库更新后应用程序将自动重新启动。

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

完成初始配置后，您可以稍后运行更新任务。

## 启用应用程序数据库自动更新

仅当您在向导的初始步骤中选择在标准模式或者 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，此步骤才会显示。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收 Light Agent 的数据库和应用模块更新。

在此步骤中，您可以启用应用程序数据库的自动更新。

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

如果不希望应用程序自动更新数据库，请输入 no。

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。

## 激活应用程序

只有在向导的第一步中选择在独立模式下使用 Kaspersky Endpoint Security 时，才会显示此步骤。如果 Kaspersky Endpoint Security 以 Endpoint Detection and Response Agent 模式运行，则在完成应用程序的初始配置后，您需要添加一个授权许可密钥来激活 Kaspersky Endpoint Detection and Response Expert（本地部署）功能。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，Kaspersky Endpoint Security 将从 Protection Server 接收有关授权许可的信息；不需要单独激活 Kaspersky Endpoint Security。

在此步骤中，您可以使用激活码或密钥文件来激活应用程序。

要使用激活码激活应用程序，请输入激活码。

要使用密钥文件激活应用程序，请指定密钥文件的完整路径。

如果未指定激活码或密钥文件，则将使用试用密钥激活该应用程序一个月。

完成初始配置后，您可以稍后激活应用程序。

# 以自动模式对应用程序进行安装后配置

要在自动模式下执行应用程序的初始配置：

1. 准备一个包含初始配置设置的配置文件。您可以创建该文件，或从 autoinstall.ini 配置文件（用于使用 Kaspersky Security Center 远程安装应用程序）复制必要的结构。
2. 将配置文件的路径传递到 Kaspersky Endpoint Security 应用程序的初始设置向导。

> 您必须以 root 用户身份运行初始设置向导。

*要启动应用程序的自动初始设置，执行以下命令：*

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

其中，< 初始配置文件 > 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。

*要检查返回码，执行以下命令：*

```
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。

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

为了在完成向导后正确更新应用程序模块，可能需要重启应用程序。使用 `kesl-control --app-info` 命令检查应用程序的更新状态。

# 安装后配置的配置文件中的设置

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

设置值区分大小写。

| 设置 | 描述 | 值 |
| --- | --- | --- |
| KSVLA_MODE | 在 Light Agent 模式下使用 Kaspersky Endpoint Security。 | Yes – 在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境（用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。<br>No – Kaspersky Endpoint Security 以标准模式或 Endpoint Detection and Response Agent 模式运行（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。 | 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。 | 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。 |
| ENDPOINT_AGENT_MODE | 在 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security | Yes — Kaspersky Endpoint Security 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。<br>No – Kaspersky Endpoint Security 以标准模式或 Light Agent 模式运行（请参阅 KSVLA_MODE 设置）。 |
| EULA_AGREED | 必要设置。<br>接受最终用户授权许可协议的条款。 | Yes – 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。应用程序的初始配置已中止。 |
| PRIVACY_POLICY_AGREED | 必要设置。<br>接受隐私策略条款。 | Yes：接受隐私策略以继续安装应用程序。<br>No – 不接受隐私策略的条款和条件。应用程序的初始配置已中止。 |
| 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>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 – 不接受卡巴斯基安全网络声明。退出 KSN 不会中止初始配置过程。 |
| GROUP_CLEAN | 必要设置。<br>先从 kesladmin 和 keslaudit 特权组中移除用户，再安装应用程序。 | 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 – 不从特权组中删除用户。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| LOCALE | 可选设置。<br>发送到 Kaspersky Security Center 的应用程序事件使用的区域设置。<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。 | 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<br>• `fr_FR.UTF-8` — 法语<br>• `ja_JP.UTF-8` — 日语<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>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 | 用于向应用程序添加授权许可密钥的激活码或密钥文件路径。<br>只有在标准模式下使用应用程序时，该设置才适用。 | <激活码> 如果您想在安装期间使用激活码激活应用程序。<br><密钥文件的完整路径> 如果您想在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>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 | `SCServer` —使用 Kaspersky Security Center 管理服务器作为更新源。<br>`KLServers` — 使用卡巴斯基服务器作为更新源。<br>< 更新源地址 >。 |
| PROXY_SERVER | 用于连接到互联网的代理服务器的地址。<br>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 | 代理服务器的地址采用以下格式之一：<br>• `[<connection protocol>://]<IP 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>]@]<IP address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。<br>不支持通过 HTTPS 连接到代理服务器。 |
| UPDATE_EXECUTE | 在初始配置期间启动应用程序数据库更新任务。<br>仅当应用程序在独立模式或 Endpoint Detection and Response Agent 模式下使用时才适用。 | `Yes` — 启动更新任务。<br>`No` — 不启动更新任务。 |
| KERNEL_SRCS_INSTALL | 在启动文件威胁防护任务时自动开始编译内核模块（适用于不支持 fanotify 技术的操作系统）。 | `Yes` — 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。 |
| ADMIN_USER | 被分配了管理员角色 (admin) 的用户。 | |
| CONFIGURE_SELINUX | 自动配置 SELinux 以使用 Kaspersky Endpoint Security。 | `Yes` – 自动配置 SELinux 以使用 Kaspersky Endpoint Security。<br>`No` – 不执行 SELinux 自动配置。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| DISABLE_PROTECTION | 安装应用程序后禁用保护组件和扫描任务。<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>如果在使用 `DISABLE_PROTECTION=Yes` 参数安装应用程序后启用了必要的组件和任务，则启用的组件和任务将在应用程序重启后继续工作。 | `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。 |
| 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。 | `UseFanotify` 用于使用 fanotify 技术拦截系统事件。<br>`UseUpdatableKernelModule` — 用于通过可更新内核模块来拦截系统事件。 |
| 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>此设置仅适用于运行支持 fanotify 技术的操作系统的设备。 | `FallbackToFanotify` — 切换到 fanotify 进行系统事件拦截。<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。 |
| 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>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>`No` — 不在首次启动应用程序时创建跟踪文件。 |

以 <设置名称>=<设置值> 的格式指定各设置的值（设置名称与其值之间的空格不会被处理）。

# 在 SELinux 系统中配置允许规则

## 手动配置 SELinux 以与应用程序配合使用

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

*要手动配置 SELinux 以使用应用程序：*

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

     ```
     # setenforce Permissive
     ```

   - 如果禁用了 SELinux，请在配置文件 / etc / selinux / config 中设置 `SELINUX=permissive`，然后重新启动操作系统。
2. 确保 semanage 实用程序已安装在系统。如果未安装该实用程序，请安装 policycoreutils-python 或 policycoreutils-python-utils 包，具体取决于包管理器。

3. 如果您使用自定义 SELinux 策略而不是默认的目标策略，请根据所使用的 SELinux 策略为 Kaspersky Endpoint Security 的每个源可执行文件分配一个标签。为此，请运行以下命令：

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

   其中 <可执行文件> 为：

   - /var/opt/kaspersky/kesl/12.4.0.<内部版本号>_<安装时间戳>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.4.0.<内部版本号>_<安装时间戳>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.4.0.<内部版本号>_<安装时间戳>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.4.0.<内部版本号>_<安装时间戳>/opt/kaspersky/kesl/shared/kesl

4. 运行以下任务：

   - 文件威胁防护任务：

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

   - 关键区域扫描任务：

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

   > 推荐使用 Kaspersky Endpoint Security 运行您计划运行的所有任务。

5. 启动图形用户界面（如果您计划使用它）。

6. 确保 audit.log 文件中没有错误：

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

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

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

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

8. 将 SELinux 切换为阻止模式：

   ```
   # setenforce Enforcing
   ```

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

您可以在操作系统的文档中找到更多信息。

### 配置 SELinux 以运行“启动进程”任务

如果 SELinux 在您的操作系统中以 `Enforcing` 模式安装，则运行 启动进程 任务需要对 SELinux 进行额外配置。

*要配置 SELinux 以运行“启动进程”任务：*

1. 将 SELinux 切换为宽容模式：
   - 如果已激活 SELinux，请执行以下命令：
     ```
     # setenforce Permissive
     ```
   - 如果禁用了 SELinux，请在配置文件 / etc / selinux / config 中设置 `SELINUX=permissive`，然后重新启动操作系统。
2. 确保 semanage 实用程序已安装在系统。如果未安装该实用程序，请安装 policycoreutils-python 或 policycoreutils-python-utils 包，具体取决于包管理器。
3. 启动“启动进程”任务。
4. 确保 audit.log 文件中没有错误：
   ```
   # grep kesl /var/log/audit/audit.log
   ```
5. 如果 audit.log 文件中存在错误，则根据阻止规则创建并加载新的规则模块来修复错误，然后再次运行“启动进程”任务。
   ```
   # grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   # semodule -i kesl.pp
   ```
6. 将 SELinux 切换为阻止模式：
   ```
   # setenforce Enforcing
   ```

# 在封闭软件环境模式下针对 Astra Linux OS 运行应用程序

本节介绍如何在 Astra Linux Special Edition 操作系统中在封闭软件环境模式下启动应用程序。

### 适用于 Astra Linux Special Edition（更新 1.6、1.7 和 1.8）

*要在 Astra Linux Special Edition 操作系统（更新 1.6、1.7 或 1.8）中运行该应用程序：*

1. 在 /etc/digsig/digsig_initramfs.conf 文件中指定以下设置：
   ```
   DIGSIG_ELF_MODE=1
   ```
2. 安装兼容包：
   ```
   apt install astra-digsig-oldkeys
   ```

3. 为应用程序密钥创建一个目录：
   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```
4. 将应用程序密钥 (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) 置于上一步中创建的目录中：
   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```
5. 更新 initramfs 映像：
   ```
   update-initramfs -u -k all
   ```
6. 重新启动操作系统。

对于 Astra Linux Special Edition（operational update 1.5）

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

1. 在 /etc/digsig/digsig_initramfs.conf 文件中指定以下设置：
   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```
2. 为应用程序密钥创建一个目录：
   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```
3. 将应用程序密钥 (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) 置于上一步中创建的目录中：
   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```
4. 更新 initramfs 映像：
   ```
   sudo update-initramfs -u -k all
   ```
5. 重新启动操作系统。

在强制访问控制会话期间，可以使用应用程序图形用户界面。

# 在封闭软件环境模式下的 ALT SP 上运行应用程序

本节介绍在命令行中执行的步骤，以便在 ALT SP 操作系统中以封闭软件环境模式启动应用程序。

*要在 ALT SP 操作系统中运行该应用程序：*

1. 如果已启用封闭软件环境模式，请运行以下命令将其禁用：
   ```
   integrity-remover
   ```
2. 运行以下命令创建 kesl 组，以便对 IMA 策略进行进一步更改：
   ```
   groupadd kesl
   ```
3. 运行以下命令，查找已创建组的唯一标识符（GUID）：
   ```
   cat /etc/group | grep kesl
   ```

4. 编辑 IMA 策略，将 kesl 组排除在外。为此，请执行下列操作：

   a. 运行以下命令复制 /usr/share/integrity/policy 文件：

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

   b. 通过运行以下命令使用文本编辑器（例如，vim）编辑 /etc/integrity/policy 文件：

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

   c. 在 `dont_measure fsmagic=0xf97cff8c` 行（这通常是 `dont_measure` 部分中的最后一行）之后，添加 `dont_measure fgroup=<GUID>` 行，其中 `<GUID>` 是按照本说明第 2 步创建的组的唯一 ID）。

   d. 在 `dont_appraise fsmagic=0x27e0eb` 行（这通常是 `dont_appraise` 部分中的最后一行）之后，添加 `dont_appraise fgroup=<GUID>` 行，其中 `<GUID>` 是按照本说明第 2 步创建的组的唯一 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. 通过运行以下命令使用文本编辑器（例如，vim）编辑 /usr/sbin/integrity-sign 文件：

      ```
      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。

6. 安装 Kaspersky Endpoint Security 应用程序。为确保应用程序数据库更新在安装后正常工作，在初始配置阶段，拒绝启动应用程序数据库更新（为此，请在应用程序数据库更新步骤中输入“no”）。

7. 运行以下命令，为 Kaspersky Endpoint Security 应用程序的可更新组件分配 kesl 组和目录权限的继承：

   ```
   cd /var/opt/kaspersky/kesl/< 内部版本号 _*>/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 {} \;
   ```

8. 运行以下命令，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 {} \;
   ```

9. 使用以下命令启动系统签名，启用封闭软件环境模式：

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

10. 运行以下命令，确保 IMA 子系统已激活：

    ```
    cat /proc/cmdline
    ```

    命令输出应包含以下行 `lsm=integrity ima_hash=sha512 ima_appraise=enforce.`

11. 运行以下命令启动数据库更新任务：

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

    如果输出包含*EventType=BasesApplied*事件，则表示数据库更新已正确执行。

12. 运行以下命令重启应用程序：

    ```
    systemctl restart kesl
    ```

# 配置 OSnova 操作系统以使应用程序正常运行

对于 OSnova 2.4

*准备具有 OSnova 2.4 操作系统的设备以便远程安装网络代理：*

1. 打开 /etc/systemd/logind.conf 文件，并在 `[Login]` 部分中注释掉 `#KillUserProcesses=yes` 行。
2. 打开文件 /usr/lib/NESS/pam-user-session，并注释掉 `#loginctl terminate-session "$XDG_SESSION_ID"` 行。

*要在 OSnova 2.4 操作系统上运行该应用程序：*

1. 打开 /etc/NESS/systemd/kesl.service.config 文件并设置 `NESSCTX_MODIFY=t+ADDEQUSOCK,OMIT,70,SSUID_SAVE_CTX_PERMANENT"`。
2. 通过运行 `systemctl daemon-reload` 命令刷新服务设置。
3. 如果要运行进程内存和内核内存扫描，您需要禁用内核中的 mprotect（或 PaX）内存保护，即向内核命令行参数添加 `mprotect=off`。更多详情，请参考OSnova 文档。
4. 重新启动操作系统。

安装图形接口（kesl-gui 软件包）后，以 root 用户身份在命令行运行以下命令：

```
rm /etc/xdg/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /etc/xdg/autostart/kaspersky-
kesl.desktop

rm /usr/share/applications/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/app.desktop /usr/share/applications/kaspersky-
kesl.desktop
```

```
rm /usr/share/autostart/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/autostart.desktop /usr/share/autostart/kaspersky-kesl.desktop

rm /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kde4/services/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/kde.desktop /usr/share/kservices5/ServiceMenus/kaspersky-kesl.desktop

rm /usr/share/Thunar/sendto/kaspersky-kesl.desktop

cp /opt/kaspersky/kesl/resource/sendto.desktop /usr/share/Thunar/sendto/kaspersky-kesl.desktop
```

对于 OSnova 2.5.1 及更高版本

*准备具有 OSnova 操作系统 2.5.1 和更高版本的设备以便远程安装网络代理：*

1. 打开文件 /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf，并在 `[Login]` 部分中注释掉 `#KillUserProcesses=yes` 行。
2. 打开文件 /usr/lib/NESS/pam-user-session，并注释掉 `#loginctl terminate-session "$XDG_SESSION_ID"` 行。

*要在 OSnova 操作系统 2.5.1 和更高版本上运行该应用程序：*

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. 通过运行 `systemctl daemon-reload` 命令刷新服务设置。
3. 打开文件 /etc/sysctl.d/30-disable-ptrace.conf 并设置 `kernel.yama.ptrace_scope=0.`。
4. 如果要运行进程内存和内核内存扫描，您需要禁用内核中的 mprotect（或 PaX）内存保护，即向内核命令行参数添加 `mprotect=off`。更多详情，请参考OSnova 文档。
5. 重新启动操作系统。

在运行 OSnova 2.14 或更高版本的设备上安装 Kaspersky Endpoint Security 时，由于 /etc/os-release 文件中存在两行 `SUPPORT_URL`，您可能会遇到错误 `"dpkg: error processing package kesl (--install): installed kesl package post-installation script subprocess returned error exit status 1"`。要使应用程序正确安装，您需要删除 /etc/os-release 文件中的其中一行 `SUPPORT_URL`。

# 优化应用程序的资源消耗

本节包含卡巴斯基专家关于配置 Kaspersky Endpoint Security 以优化系统资源消耗的建议。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。为避免性能下降，建议在安装应用程序并完成初始配置后按照本部分中的步骤操作。

建议采取以下步骤来优化应用程序的系统资源消耗：

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应用程序。

3. **分析试点设备的性能。**

   在每个管理组中挑选 1 或 2 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。

   您还可以优化 Web 威胁防护和网络威胁防护组件。

5. **更新所有设备上应用程序的配置。**

   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。

# 针对典型服务器角色的建议

## Web 服务器

使用 HTTPS 时，如果服务器上的客户端负载较高，Web 威胁防护和网络威胁防护组件可能会显著增加系统资源的消耗。这是由于应用程序解密和 HTTPS 流量扫描造成的。

分析这些组件运行时服务器负载如何变化。如需帮助选择最佳参数并解决兼容性问题，请联系卡巴斯基技术支持。

## 代理服务器

建议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

建议在用于提供容器化服务的服务器上禁用 Web 威胁防护和网络威胁防护组件。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。

# 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。

*要查看应用程序的资源消耗情况，请执行以下命令：*

```
top -bn1|grep kesl
```

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 列显示驻留内存量 – `2.302g`。

第 9 列显示处理器核心使用率的百分比 – 120.0，其中每个核心通过 100% 表示。因此，120% 表示一个核心已完全使用，另一个核心的使用率为 20%。

如果 Kaspersky Endpoint Security 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，请使用命令行在设备上检查以下内容：

1. 分析文件威胁防护任务（OAS 类型任务）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 类型任务）有关，并遵循针对相关任务的建议。
2. 识别最常扫描的对象。您可以从扫描中排除安全对象和文件，从而优化性能。

您可以在命令行上分析任务的性能。如果设备受 Kaspersky Security Center 策略管理，则您需要在进行调查时允许本地任务管理。

# 分析文件威胁防护任务的资源消耗情况

*要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. 通过执行以下命令获取包含所有应用程序任务的列表：
      `kesl-control --get-task-list`
   b. 通过运行以下命令获取所有 ODS 和 ContainerScan 类型的任务的计划设置：
      `kesl-control --get-schedule <任务 ID/名称>`
      如果命令输出为 `RuleType=Manual`，则任务只能手动启动。
   c. 对于所有“`RuleType`”不是“`Manual`”的任务，通过运行以下命令更改计划：
      `kesl-control --set-schedule <任务 ID/名称> RuleType=Manual`
3. 通过执行以下命令，启用生成具有概要详细信息的应用程序跟踪文件：
   `kesl-control --set-app-settings TraceLevel=Detailed`
4. 如果文件威胁防护任务未运行，请使用以下命令启动该任务：
   `kesl-control --start-task 1`
5. 以导致性能问题的模式加载系统；几个小时的时间就够了。
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，则这些问题很有可能是按需扫描任务（ODS 和 ContainerScan 类型的任务）引起的，这意味着您需要优化这些任务。
7. 通过执行以下命令禁用创建应用程序跟踪文件：
   `kesl-control --set-app-settings TraceLevel=None`

# 识别最常扫描的对象

您可以通过运行以下命令来获取被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，聚合特定深度的子目录中的对象扫描统计信息，您可以在命令中添加“`cut -d/ -f 1-X`”，其中 X 是嵌套深度，示例如下：

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c | sort -k1 -n -r|less
```

如果各种服务频繁向系统中的文件写入数据，则此类文件会在待处理队列中再次受到扫描。运行以下命令，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，聚合特定深度的子目录中的对象扫描统计信息，您可以在命令中添加“`cut -d/ -f 1-X`”，其中 X 是嵌套深度，示例如下：

```
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
```

建议判断被扫描次数最多的对象是否具有危险性。您可以将确认安全的对象和文件添加到排除项，以优化文件威胁防护和扫描任务。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。

# 针对文件威胁防护任务和扫描任务的建议

## 优化文件威胁防护

要优化文件威胁防护组件，您可以：

- 为最常被扫描且安全的对象配置扫描排除项。
- 配置文件操作拦截排除项。
- 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**”。
  - 在设备本地使用以下命令：

    ```
    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。

- 确保压缩文件扫描已禁用（默认值）。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。

- 限制应用程序可以使用的 RAM 大小。

### 优化扫描任务

要优化扫描任务（ODS 和 ContainerScan 类型的任务），您可以：

- 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。
- 在服务器负载最小时运行扫描。
- 确保扫描任务的范围不包括通过 SMB 和 NFS 挂载在设备上的远程目录。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）。
- 为最常被扫描且安全的对象配置扫描排除项。
- 配置文件操作拦截排除项。
- 限制应用程序可以使用的 RAM 大小。

# 配置扫描排除项

扫描排除有助于平衡系统安全性和性能。例如，根据卡巴斯基病毒专家的建议，您可以将数据库的数据文件和索引文件安全添加到排除项中。一般情况下，此类文件不存在成为病毒载体的危险。

您可以从最常扫描的对象列表中排除安全对象。

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。如果您需要完全避免延迟，建议配置文件操作拦截排除项。

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。

您还可以为 ODS 和 ContainerScan 类型的扫描任务配置排除项。排除项可以在 Kaspersky Security Center 的任务设置中配置，或者在设备本地使用命令行进行配置。

> 一个扫描任务的扫描排除项设置不会影响其他扫描任务。必须为每个扫描任务单独配置排除项。

以下是在命令行上配置文件威胁防护排除项的示例。

*要递归排除 /tmp/logs 目录及其所有子目录和文件，请执行以下命令：*

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

*要在 /tmp/logs 目录中按掩码排除一个或多个特定文件，请执行以下命令：*

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

*要使用递归掩码排除 /tmp/ 目录和子目录中具有 .log 扩展名的所有文件，请执行以下命令：*

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

# 配置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。

您可以使用以下命令获取文件拦截统计信息：

```
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。

如有必要，您可以使用应用程序跟踪文件进行更详细的分析。默认情况下，应用程序不会生成跟踪文件。您可以使用以下命令启用跟踪：

```
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。

您可以使用以下命令禁用跟踪：

```
kesl-control --set-app-settings TraceLevel=None
```

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。您可以通过运行以下命令获取拦截文件列表：

```
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，聚合特定深度的子目录中的文件操作拦截统计信息，您可以在命令中添加“`cut -d/ -f 1-X`”，其中 X 是嵌套深度，示例如下：

```
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
```

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。通过排除挂载点（全局排除），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。

全局排除对非挂载点的路径没有影响。

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。

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。

您可以使用 Web Console 或管理控制台在策略中配置全局排除，或者使用命令行在设备本地配置全局排除。

下面是使用命令行配置文件操作拦截排除项的示例。

*要将 /tmp 目录中的所有文件排除在拦截范围之外：*

1. 如果目录不是挂载点，请通过该目录创建一个挂载点。例如，要从 /tmp 目录创建挂载点，请运行以下命令：
   ```
   mount --bind /tmp/ /tmp
   ```
2. 要在服务器重新启动后保留挂载点，请将以下行添加到 /etc/fstab 文件中：
   ```
   /tmp /tmp none defaults,bind 0 0
   ```
3. 通过执行以下命令将 /tmp 目录添加到全局例外中：
   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```
4. 如果要添加多个目录，请将 item_0000 计数器按 1 递增（例如 item_0001、item_0002 等）。

# 设置应用程序内存使用限制

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=<` 以兆字节为单位的内存量 `>` 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。

# 针对 Web 威胁防护任务和网络威胁防护任务的建议。

为了减少 Web 威胁防护和网络威胁防护组件对应用程序性能的影响，建议采取以下步骤。

- 配置操作系统的防火墙。如果系统已配置了自己的网络规则（或防火墙规则）且包含 Drop 策略，为确保应用程序正常工作，您需要添加一条接受规则以允许来自本地设备（环回接口）的传入连接：

  iptables 的命令示例：

  ```
  iptables -A INPUT -i lo -j ACCEPT
  ```

- 要确保 REDIRECT 规则（例如，从端口 443 重定向到 8443）与网络威胁防护组件拦截规则兼容，请执行以下操作：

  a. 删除如下规则：

  ```
  iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
  ```

  b. 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
  ```

- 配置证书验证策略。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，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。

  您可以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**”。
  - 在设备本地使用以下命令：

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  应用程序不使用互联网来验证证书。

  您可以使用 Web Console、管理控制台或在设备本地使用命令行来在策略中配置代理服务器。

- 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`”。

当将应用程序与 HAProxy 负载均衡器一起使用时，建议采取以下步骤：

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 Web 威胁防护和网络威胁保护组件与 Kubernetes 容器化技术结合使用时，需要对操作系统防火墙进行额外的细致微调。如果也使用 Cillium CNI，则这些组件不能与 Kubernetes 一起使用。

# 从先前的版本更新应用程序

您只能从 Kaspersky Endpoint Security 12.3 for Linux 升级到 Kaspersky Endpoint Security 12.4 for Linux。

不支持将更早的 Kaspersky Endpoint Security 版本升级到版本 12.4。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 12.4 for Linux。

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

应用程序更新过程包括以下步骤：

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

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

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

   在网络代理更新期间，应用程序将继续正常工作。

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

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

3. **更新受保护设备上的应用程序和图形界面**

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

   如果您在基本模式或 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security，并且您使用应用程序的图形界面，则您还需要更新图形界面。

   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。
   - 通过命令行在本地操作。

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

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

在将应用程序更新到较新的版本时，先前版本的转储文件将被删除。

当您更新应用程序时，先前版本的事件数据库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 Endpoint Detection and Response 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 管理 MMC 插件

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有名称“<Original policy/task name> （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。

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

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

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

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。

# 使用 Kaspersky Security Center 更新应用程序

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

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

使用 Kaspersky Security Center 进行更新涉及以下步骤：

1. 创建安装包。

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

2. 在公司网络的设备上部署 Kaspersky Endpoint Security 应用程序。

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

   - 使用“保护部署向导”安装应用程序。
   - 使用远程安装任务安装应用程序。

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

   - 使用远程安装向导安装应用程序。
   - 使用远程安装任务安装应用程序。

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

# 使用命令行更新应用程序

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

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

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

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

如果您不接受最终用户授权许可协议和/或隐私策略的条件，应用程序将不会更新。

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

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

如要在升级期间接受新协议的条款，请使用变量 `KESL_EULA_AGREED=yes`、`KESL_PRIVACY_POLICY_AGREED=yes` 和 `KESL_USE_KSN=yes/no`。

*要更新应用程序：*

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

   - 对于 RPM 软件包：

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.4.0-<内部版本号>.<arch>.rpm [kesl-gui-12.4.0-<内部版本号>.<arch>.rpm]`

     其中 `<arch>` 是架构类型：

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

     在具有 RPM 类型的包管理器的操作系统上，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。

   - 对于 DEB 软件包：

     `# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.4.0-<内部版本号>_<arch>.deb [./kesl-gui_12.4.0-<内部版本号>_<arch>.deb]`

     其中 `<arch>` 是架构类型：

     - i386 – 用于 32 位操作系统
     - amd64 – 用于 64 位操作系统
     - arm64 – 用于 Arm 架构 64 位操作系统

     在具有 dpkg 类型的包管理器的操作系统上，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。

2. Kaspersky Endpoint Security 将自动重启。

例如：
*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-12.4.0-<内部版本号>.x86_64.rpm kesl-gui-12.4.0-<内部版本号>.x86_64.rpm`

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

更新完成后且应用程序重新启动前对应用程序设置进行的更改不会保存。

# 更新应用程序时设置参数值的特殊注意事项

如果使用 Kaspersky Security Center 管理控制台来管理应用程序，您可以转换策略和任务以使用为应用程序的先前版本配置的策略和任务设置的值（有关更多信息，请参阅Kaspersky Security Center 帮助）。Kaspersky Security Center Web Console 中不提供转换策略和任务的程序。

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。

## 数据库更新源

在新版本的应用程序中，对数据库更新任务进行了以下更改：

- **如果其他更新源不可用，则使用卡巴斯基更新服务器**（`UseKLServersWhenUnavailable`）设置已被移除。您可以使用其他任务设置来配置此功能。
- 您可以同时指定多个数据库更新源。应用程序按照这些更新源在源列表中出现的顺序使用它们。

在MMC 插件中转换任务后，更新源配置如下：

- 如果在之前的版本中选择了**卡巴斯基更新服务器**选项，则在源列表中会选中**卡巴斯基更新服务器**复选框。
- 如果在之前的版本中选择了**Kaspersky Security Center**选项，则在源列表中会选中**Kaspersky Security Center**复选框。

  但是，如果在之前的版本中选中了**如果其他更新源不可用，则使用卡巴斯基更新服务器**复选框，则在源列表中也会选中**卡巴斯基更新服务器**复选框，并且**"Kaspersky Security Center"**源会被移至列表顶部。
- 如果在之前的版本中配置了自定义源（**本地或全局网络上的其他源**），则会将具有指定参数（源的路径或网址）的自定义源添加到源列表中，并且选中该复选框。

  但是，如果在之前的版本中选中了**如果其他更新源不可用，则使用卡巴斯基更新服务器**复选框，则在源列表中也会选中**卡巴斯基更新服务器**复选框，并且自定义源会被移至列表顶部。

Web 插件不支持策略转换。

通过命令行更新应用程序后，更新源的配置如下：

- 如果在之前的版本中 `SourceType` 设置为 `KLServers`，则会在 **[Sources]** 部分创建以下更新源：`SourceType=KLServers`，`Enabled=Yes`。
- 如果在之前的版本中 `SourceType` 设置为 `SCServer`，则会在 **[Sources]** 部分创建以下更新源：`SourceType=SCServer`，`Enabled=Yes`。

  不过，如果在之前的版本中参数设置为 `UseKLServersWhenUnavailable=Yes`，则会在 **[Sources]** 部分创建第二个更新源：`SourceType=KLServers`，`Enabled=Yes`。

- 如果在之前的版本中 SourceType 设置为 Custom，并且已在 **[CustomSources.item_#]** 部分配置自定义源，则会在 **[Sources]** 部分创建自定义更新源：SourceType=Custom，URL=< 源的路径或网址 >，Enabled=Yes。

  不过，如果在之前的版本中参数设置为 UseKLServersWhenUnavailable=Yes，则会在 **[Sources]** 部分创建第二个更新源：SourceType=KLServers，Enabled=Yes。

## 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。

Web 插件不支持策略转换。

在通过命令行升级应用程序后，如果您在更新时设置了 KESL_USE_KSN=No，则 UseKSN 设置会设置为 No；如果您设置了 KESL_USE_KSN=Yes，则会应用 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。

Web 插件不支持策略转换。

在命令行上更新应用程序后，CloudMode 将被设置为：

- 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：

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

Web 插件不支持策略转换。

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。

# 卸载应用程序

卸载 Kaspersky Endpoint Security 包括以下步骤：

1. **卸载应用程序及其图形界面**

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

   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。
   - 通过命令行在本地操作。

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

2. **移除网络代理**

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

   您可以通过以下方式卸载网络代理：

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

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

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

> 移除应用程序后，该应用程序保存的所有信息都将被删除，授权许可数据库除外。已安装的应用程序证书也会被删除。授权许可数据库已保存，您可以使用它来重新安装应用程序。还会保存应用程序安装的唯一 ID（SensorID）。

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

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

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

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

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

卸载在后台进行。应用程序卸载完成后，系统将提示您重新启动客户端设备。

# 使用命令行卸载应用程序

### 移除应用程序包和图形用户界面软件包

*要卸载从 RPM 软件包安装的应用程序和图形界面，请执行以下命令：*

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

*要移除从 DEB 软件包安装的应用程序和图形用户界面，请运行以下命令：*

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

### 卸载应用程序包，不卸载图形用户界面软件包

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

```
# rpm -e kesl
```

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

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

### 移除图形用户界面软件包

*要移除从 RPM 软件包安装的图形界面，请执行以下命令：*

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

*要移除从 DEB 软件包安装的图形界面，请执行以下命令：*

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

卸载过程完成后，会显示有关卸载结果的消息。

# 使用命令行移除网络代理

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

```
# rpm -e klnagent
```

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

```
# rpm -e klnagent64
```

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

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

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

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

卸载过程完成后，会显示有关卸载结果的消息。

# 卸载 Kaspersky Endpoint Security 管理插件

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

*要移除 Kaspersky Endpoint Security 管理 MMC 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**。

# 应用程序授权许可

本节包含与许可卡巴斯基应用程序相关的基本概念的信息，以及有关激活 Kaspersky Endpoint Security 应用程序的具体信息。

激活应用程序后，我们建议监控授权许可有效期，以便在必要时及时更新授权许可。您可以使用 Kaspersky Security Center 或受保护设备上的命令行查看有关 Kaspersky Endpoint Security 使用的授权许可密钥的信息。

# 关于最终用户授权许可协议

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

开始使用该应用程序之前，请仔细通篇阅读“最终用户授权许可协议”的条款。

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

- 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。

# 关于授权许可

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

可用功能列表和应用程序的有效期取决于使用该应用程序时所用的授权许可。

提供以下授权许可类型：

- *试用*

  用于试用应用程序的免费授权许可。试用授权许可的有效期很短。

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

  只能在一个试用期内根据试用授权许可使用应用程序。

- *商业*

付费授权许可。

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

建议在授权许可到期前进行续订，以确保继续保护设备免受安全威胁。

要激活 Kaspersky Endpoint Security 应用程序，您需要一个涵盖该应用程序基本功能的授权许可。主授权许可还可以包括应用程序的附加功能（例如，与 Kaspersky Detection and Response 解决方案的整合功能）。如果您用于应用程序的主授权许可不涵盖您所需的附加功能，则必须购买单独的授权许可才能激活附加功能。

为了明确主授权许可和附加功能授权许可中包含的功能范围，请联系您从其购买授权许可的卡巴斯基合作伙伴。

# 关于授权许可证书

*授权许可证书*是与密钥文件或激活码一起交付给用户的文档。

授权许可证书包含以下授权许可信息：

- 授权许可 ID 或订单号。
- 获得授权许可的用户的详细信息。
- 可使用该授权许可激活的应用程序的详细信息。
- 授权许可单元数量限制（例如，可根据该授权许可使用应用程序的设备数量）。
- 授权许可期限开始日期。
- 授权许可到期日期或授权许可期限。
- 授权许可类型。

# 关于授权许可密钥

*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。

要激活该应用程序，您需要主授权许可密钥。如果您用于应用程序的主授权许可不包含您需要的附加功能（例如，Kaspersky Endpoint Detection and Response Optimum 功能），您还需要授权许可密钥来激活附加功能。

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

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

授权许可密钥可以添加为活动密钥或备用密钥。

- *活动授权许可密钥*当前用于运行应用程序。可以将试用授权许可密钥、商业授权许可密钥（商业版密钥）或订阅密钥添加为活动密钥。您只能添加一个主授权许可密钥作为活动密钥。您可以拥有多个活动授权许可密钥来获得附加功能。

- *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。

  要延长应用程序主授权许可的期限，您可以为基本功能添加备用密钥。如果在单独的授权许可下激活了附加功能，您还可以添加用于附加功能的备用密钥。

  只有在添加了同样类型的活动授权许可密钥之后，才可以添加备用授权许可密钥。

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

# 关于激活码

*激活码*是由 20 个字母数字字符组成的唯一序列。您输入激活码以添加用于激活 Kaspersky Endpoint Security 的授权许可密钥。在购买 Kaspersky Endpoint Security 或请求 Kaspersky Endpoint Security 试用版本后，您会在您提供的电子邮件地址收到激活码。

要使用激活码激活本应用程序，需要因特网访问以连接到卡巴斯基的激活服务器。

如果您激活应用程序后丢失了激活码，请联系您购买授权许可的卡巴斯基合作伙伴。

# 关于密钥文件

*密钥文件*是您从 Kaspersky 接收到的 .key 扩展名的文件。密钥文件用于添加激活应用程序的授权许可密钥。

密钥文件会发送到您在购买 Kaspersky Endpoint Security 或订购 Kaspersky Endpoint Security 试用版本时提供的电子邮件地址。

使用密钥文件无需连接至卡巴斯基激活服务器以激活应用程序。

如果意外删除了密钥文件，您可以将其恢复。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。

- 根据您现有的激活码，在卡巴斯基网站上获取密钥文件。

# 关于订阅

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

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

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

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

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

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

# 不同授权许可下的应用程序功能比较

Kaspersky Endpoint Security 应用程序的可用功能取决于主授权许可的类型。

应用程序的主授权许可可能涵盖该应用程序的基本功能以及附加功能。例如，“Kaspersky Optimum Security”授权许可允许您激活主要保护和控制组件，以及 Kaspersky Endpoint Detection and Response Optimum 整合功能。

您可以使用单独的授权许可来获得应用程序的附加功能，例如，使用授权许可来激活 Kaspersky Unified Monitoring and Analysis Platform 功能。

为了明确主授权许可和附加功能授权许可中包含的功能范围，请联系您从其购买授权许可的卡巴斯基合作伙伴。

打开应用程序主授权许可涵盖的解决方案功能列表

# 应用程序激活和授权许可密钥管理

*激活*是授权许可生效的过程，允许您使用应用程序的完整功能版本，直到授权许可到期。

要在受保护的设备上激活 Kaspersky Endpoint Security 应用程序，您需要向该应用程序添加主授权许可密钥。如果您用于应用程序的主授权许可不涵盖您所需的附加 Kaspersky Endpoint Security 功能，您还需要添加授权许可密钥来激活附加功能：

- 单独的授权许可密钥“Kaspersky Endpoint Detection and Response Optimum 附加模块”（下文亦称“EDR Optimum 密钥”），用于激活 Kaspersky EDR Optimum 组件。
- 单独的授权许可密钥“卡Kaspersky Unified Monitoring and Analysis Platform Add-on”（以下也称为“KUMA 密钥”），用于激活Kaspersky Unified Monitoring and Analysis Platform功能。
- 单独的授权许可密钥“Kaspersky Managed Detection and Response Optimum/Expert 附加模块”（下文亦称“MDR 密钥”），用于激活 Kaspersky MDR 组件。
- 单独的授权许可密钥，"Kaspersky Endpoint Detection and Response Expert（本地部署）Add-on”（以下简称“EDR Expert（本地部署）密钥”），用于激活EDR Expert（本地部署）组件。

EDR Expert（本地部署）密钥也用于在 Endpoint Detection and Response Agent 模式下激活 Kaspersky Endpoint Security 应用程序。在此模式下，您无需向应用程序添加主授权许可密钥。

您可以通过以下方法之一向应用程序添加授权许可密钥：

- 使用密钥文件
- 使用激活码

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则无需激活应用程序。您仅激活 Kaspersky Security for Virtualization Light Agent。激活是在 Protection Server 端（Kaspersky Security for Virtualization Light Agent 的一个组件）通过在 SVM 上添加授权许可密钥来执行的。如果需要，还可以将用于激活附加功能的授权许可密钥添加到 SVM。

如果您在安装过程中未激活 Kaspersky Endpoint Security 应用程序（通过在安装包中添加密钥或完成初始配置），则需要通过以下一种方式激活已安装的应用程序：

- 使用 Kaspersky Security Center 远程执行：
  - 使用“添加密钥”任务。
  - 通过将管理服务器上存储的授权许可密钥分发到客户端设备。
- 在命令行上使用管理命令。

要向应用程序添加附加功能授权许可密钥，您还可以使用添加密钥任务、将密钥分发给客户端设备的程序或授权许可密钥管理命令。添加提供附加功能的密钥与添加应用程序的主授权许可密钥没有什么不同。

如果 Kaspersky Endpoint Security 以标准模式运行，则只有在添加应用程序的主授权许可密钥后，才能添加用于附加功能的密钥。

您还可以为应用程序的基本功能添加一个备用密钥，为附加功能添加一个备用密钥。当与活动密钥关联的授权许可到期或活动密钥被删除时，备用密钥成为活动密钥。备用密钥可避免当授权许可到期时应用程序功能受限。

只有在添加了活动授权许可密钥之后，才可以添加备用授权许可密钥。

您可以使用 Kaspersky Security Center 或受保护设备上的命令行查看有关远程添加到应用程序的授权许可密钥的信息。

您还可以使用图形用户接口来激活应用程序并管理授权许可密钥。

# 使用 Kaspersky Security Center 激活应用程序

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

- 使用“添加密钥”任务。

  使用此方法可以将授权许可密钥添加到特定设备或属于管理组的设备。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激活任务时将授权许可密钥添加到密钥存储中。

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

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

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

使用 Kaspersky Security Center Web Console 添加密钥。

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

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

*要使用“添加密钥”任务通过 Web Console 向应用程序添加密钥：*

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

5. 如果您之前已将密钥添加到 Kaspersky Security Center 密钥存储，请从列表中选择该密钥，然后单击“**下一步**”。

6. 如果在密钥存储中找不到所需密钥，请单击“**添加密钥**”按钮。

   a. 在打开的窗口中，选择如何将密钥添加到存储库：

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

   b. 根据您在上一步选择的密钥添加方法，执行以下操作之一：

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

   c. 阅读有关密钥的信息，然后单击“**关闭**”。

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

7. 阅读有关授权许可的信息，然后单击“**下一步**”。

8. 结束向导。
   在任务列表中将显示一个新任务。

9. 选中该任务旁边的复选框。单击**启动**按钮。

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

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

*要使用 Web Console 通过分发管理服务器上存储的密钥来将密钥添加到设备：*

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。

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

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

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

# 命令行中的授权许可密钥管理

如要管理设备上的授权许可密钥，可以使用授权许可密钥管理命令。

只有当应用程序以标准模式或 Endpoint Detection and Response Agent 模式运行时，才能使用授权许可密钥管理命令。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则管理授权许可密钥的命令将终止并显示错误。您可以将应用程序作为 Kaspersky Security for Virtualization Light Agent 的一部分进行激活，因此无需单独激活该应用程序。

*如要将活动密钥添加到应用程序，请运行以下命令：*

```
kesl-control [-L] --add-active-key <密钥文件路径/激活码>
```

其中：

- <密钥文件的路径> – 密钥文件的路径。如果密钥文件位于当前目录中，则仅指定文件名就足够了。
- <activation code> – 激活码。

*如要将备用授权许可密钥添加到应用程序，请运行以下命令：*

```
kesl-control [-L] --add-reserve-key <密钥文件路径/激活码>
```

如果活动密钥尚未被添加到设备上的应用程序，则命令失败。

您可以使用添加密钥命令添加应用程序的主授权许可密钥以及附加功能的授权许可密钥。您不需要在命令中指定密钥的类型。

不同命令已提供用来删除主授权许可密钥和附加功能密钥。

*若要删除活动的主密钥，请运行以下命令：*

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

*若要删除备用主密钥，请运行以下命令：*

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

*若要删除活动 EDR Optimum 密钥，请运行以下命令：*

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

*若要删除备用 EDR Optimum 密钥，请运行以下命令：*

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

*若要删除 KUMA 活动密钥，请运行以下命令：*

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

*若要删除 KUMA 备用密钥，请运行以下命令：*

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

*若要删除 MDR 活动密钥，请运行以下命令：*

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

*若要删除 MDR 备用密钥，请运行以下命令：*

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

*若要删除活动的 EDR Expert（本地部署）密钥，请运行以下命令：*

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

*若要删除备用 EDR Expert（本地部署）密钥，请运行以下命令：*

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

# 查看有关使用的授权许可密钥的信息

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Kaspersky Security Center 中，在添加密钥任务的属性中。

  在*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 Kaspersky Security Center 中，在客户端设备上安装的相关卡巴斯基应用程序的属性中。

  在受保护设备上的 Kaspersky Endpoint Security 应用程序的属性中，您可以找到有关在此设备上添加到应用程序的活动密钥和备用密钥的信息。您可以使用Web Console以及管理控制台查看应用程序的属性。

- 在 Kaspersky Security Center 的授权许可密钥使用情况报告中。

  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情况报告。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。

- 在 Kaspersky Security Center 的 Kaspersky Security Center 授权许可密钥存储区中。

  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。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。

- 在安装了 Kaspersky Endpoint Security 的设备上。您可以在命令行上查看有关 Kaspersky Endpoint Security 应用程序使用的授权许可的信息。

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。

如果您在标准模式或者 Endpoint Detection and Response Agent 下使用 Kaspersky Endpoint Security 应用程序，并且使用 Kaspersky Security Center 来管理该应用程序，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。

# 使用 Web Console 查看设备上的授权许可密钥信息

*要在 Web Console 中查看添加到设备的授权许可密钥的信息，请执行以下操作：*

1. 在 Web Console 的主窗口中，选择"**资产（设备）**"→"**受管理设备**"。

   将打开受管理设备列表。

2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

3. 在列表中，找到要查看信息的设备，然后单击设备名称。

4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。

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

6. 这将打开应用程序属性窗口；在该窗口中，选择**常规**选项卡并转到**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**是密钥的状态：活动或者备用。
   - **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。

# 使用管理控制台查看设备上的授权许可密钥信息

*要在 Kaspersky Security Center 管理控制台中查看添加到设备的授权许可密钥的信息，请执行以下操作：*

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。
   - **Status** – 授权许可密钥的状态，例如活动或备用。
   - **类型**：授权许可类型（商业或试用）。
   - **授权许可有效期** – 您可以使用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。

# 在命令行中查看有关授权许可和密钥的信息

在命令行中，使用 `-L --query` 命令，您可以查看有关添加到应用程序的活动授权许可密钥和备用授权许可密钥的信息，以及有关应用程序已激活的授权许可的信息。如果已向应用程序添加单独的密钥来激活附加功能，则还会显示有关为附加功能添加的活动和备用授权许可密钥的信息。

*要查看有关设备上的授权许可密钥和授权许可的信息，请运行以下命令：*

```
kesl-control -L --query [--json]
```

其中 `--json`：以 JSON 格式输出数据。如果未指定 `--json`选项，则设置以 INI 格式输出。

命令执行的结果会在控制台中显示如下信息：

- 有关活动授权许可主密钥的信息（如果已添加密钥）：
  - 使用应用程序的授权许可到期的日期和时间。
  - 距授权许可期限结束的剩余天数。
  - 有关保护功能限制的信息。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。
  - 与密钥关联的授权许可类型。
  - 密钥的授权许可限制（授权许可单元的数量）。
  - 该密钥要激活的应用程序的名称。
  - 活动授权许可密钥（唯一的字母数字序列）。
  - 激活日期。
- 有关备用主授权许可密钥的信息。如果应用程序在标准模式下使用且已添加备用密钥则显示。如果应用程序在用于保护虚拟环境的 Light Agent 模式下使用，则不会显示有关备用密钥的信息；备用密钥将添加到 SVM。
  - 使用应用程序的授权许可到期的日期和时间。
  - 有关保护功能限制的信息。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。

- 与密钥关联的授权许可类型。
- 密钥的授权许可限制（授权许可单元的数量）。
- 该密钥要激活的应用程序的名称。
- 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）。

- 如果添加了单独的密钥，有关附加功能的活动密钥的信息：
  - 激活附加功能的授权许可的到期日期和时间。
  - 距授权许可期限结束的剩余天数。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。
  - 与密钥关联的授权许可类型。
  - 密钥的授权许可限制（授权许可单元的数量）。
  - 该密钥要激活的应用程序的名称。
  - 活动授权许可密钥（唯一的字母数字序列）。
  - 激活日期。
- 有关附加功能的备用密钥的信息。如果应用程序在基本模式或 Endpoint Detection and Response Agent 模式下使用，并且已添加用于附加功能的备用密钥，则会显示此信息。如果应用程序在用于保护虚拟环境的 Light Agent 模式下使用，则不会显示有关备用密钥的信息；备用密钥将添加到 SVM。
  - 激活附加功能的授权许可的到期日期和时间。
  - 有关应用程序数据库更新功能限制的信息。
  - 有关授权许可密钥状态的信息。
  - 与密钥关联的授权许可类型。
  - 密钥的授权许可限制（授权许可单元的数量）。
  - 该密钥要激活的应用程序的名称。
  - 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）。

您还可以在使用 `kesl-control --app-info` 命令查看应用程序运行信息时，获取有关该应用程序所使用的授权许可的信息。

# 数据提供

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

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

有关处理、存储和销毁在使用应用程序期间获得和传输到卡巴斯基的各类信息的更多详情，请阅读最终用户授权许可协议、KSN 声明，并请参阅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 在标准模式或者 Endpoint Detection and Response Agent 模式下使用，且是使用激活码激活的，为了验证使用应用程序是否在被合法使用并获取有关应用程序分发和使用的统计信息，您同意向卡巴斯基自动提供以下信息：

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

# 从卡巴斯基更新服务器下载更新时提供的数据

如果 Kaspersky Endpoint Security 在标准模式或者 Endpoint Detection and Response 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

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

- 为了激活，Kaspersky Endpoint Security 会向 Protection Server 发送以下数据：授权许可密钥状态确认的有效期、受保护的虚拟机的 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-premise) 集成时的数据提供

如果您将 Kaspersky Endpoint Security 作为 Kaspersky Endpoint Detection and Response Expert (on-premise) 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

如果您在基本模式或 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所列信息外，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-premise) 组件集成时提供的数据

将 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Expert (on-premise) 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：

- 用于与 Kaspersky Endpoint Detection and Response Expert (on-premise) 进行集成的 Integration Server 列表。
- 提供与 Kaspersky Endpoint Detection and Response Expert (on-premise) 进行集成的服务器证书的公钥。
- 用于与 Kaspersky Endpoint Detection and Response Expert (on-premise) 进行集成的客户端证书。
- 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-premise) 进行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-premise) 进行集成的服务器的连接状态，以及客户端和服务器证书错误信息。
- 来自用于与 Kaspersky Endpoint Detection and Response Expert (on-premise) 进行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-premise) 集成时，该应用程序会保存以下数据并将其传输到 Integration Server：

- 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 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-premise) 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
- 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

# 应用程序管理理念

要管理 Kaspersky Endpoint Security，您可以使用：

- Kaspersky Security Center
- 命令行
- 应用程序的图形界面

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

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

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

# 使用 Kaspersky Security Center 管理应用程序

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

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

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

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

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

  通过卡巴斯基安全中心 Web 控制台管理卡巴斯基端点安全的界面由管理 Web 插件（以下也简称为 Web 插件）提供。

- 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。

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

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。

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）。

如果应用程序以 EDR Agent 模式使用，则只有部分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。

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

# Kaspersky Endpoint Security 管理插件

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

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

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

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

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

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

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

如果 Kaspersky Endpoint Security for Windows（内部版本 12.11.0.2004）和 Kaspersky Endpoint Security for Linux（内部版本 12.4.0.1354）的 Web 插件安装在 Kaspersky Security Center Web Console 16.0 或 Kaspersky Security Center Web Console 16.1 中，则将 Kaspersky Endpoint Security for Windows Web 插件更新到 12.11.0.6004 版本可能会导致 Kaspersky Endpoint Security for Linux 策略出现故障。在此情况下，请转到**设置** → **Web 插件**窗口，从列表中删除 Kaspersky Endpoint Security for Windows Web 插件、Kaspersky Endpoint Security for Linux Web 插件和 Unified Protection and Management 管理插件。然后，首先安装 Kaspersky Endpoint Security for Linux Web 插件，然后安装 Kaspersky Endpoint Security for Windows Web 插件。

# Kaspersky Security Center 策略

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

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

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

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

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

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

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

对于某些列表，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：

- 在子策略的属性中，在**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。

*策略配置文件*可能包含与“基本”策略设置不同的设置，并在满足配置的条件（激活规则）时应用于客户端设备。使用策略配置文件可让您灵活配置用于不同设备的应用程序设置。您可以在策略属性的**策略配置文件**部分中创建和配置配置文件。

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。

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。

如果应用程序在策略被删除后未运行，则应用程序启动后，此策略将继续应用于设备，并且应用程序将继续使用此策略指定的设置运行。

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。

# 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；
- 设备集任务，用于在多台设备上运行，而不论这些设备是否属于管理组

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

您可以创建任意数量的组任务、设备集任务或本地任务。

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

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。

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

- *恶意软件扫描*。在此任务执行期间，应用程序会扫描在任务设置中指定的设备区域以查找病毒和其他威胁。
- *关键区域扫描*。在此任务执行期间，应用程序会扫描引导扇区、启动对象、进程内存和内核内存。
- *容器扫描*。在此任务执行期间，应用程序会扫描容器和映像中是否有病毒和其他恶意软件。
- *清查*。在此任务执行期间，应用程序会接收有关设备上存储的所有可执行文件的信息。
- *系统完整性检查*。在此任务执行期间，应用程序通过将受监控对象的当前状态与之前作为基线建立的原始状态进行比较，以确定每个对象的更改。
- *添加密钥*。在此任务执行期间，应用程序会添加一个密钥（包括一个保留密钥）来激活应用程序。
- *更新*。在此任务执行期间，应用程序会根据配置的更新设置更新数据库。
- *回滚*。在此任务执行期间，应用程序会回滚上一次数据库更新。

策略设置的集合和任务设置的默认值取决于授权许可类型。如果应用程序在 Light Agent 模式下使用，则 *添加密钥*、*更新*和 *回滚* 任务不适用。

# 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。

# 在 Web Console 中管理策略

您可以使用 Web Console 中的策略执行以下操作：

- 创建策略。
- 编辑策略设置。您可以在“策略属性”窗口的**应用程序设置**选项卡上配置策略设置。Web Console 中的策略设置详见附录 5。

  如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。

- 导出和导入策略设置。

  不支持将策略设置从 Kaspersky Endpoint Security 12.3 for Linux 导出或导入到 Kaspersky Endpoint Security 12.4 for Linux。

- 复制和移动策略。
- 删除策略。
- 更改策略状态。
- 创建策略配置文件。

有关使用策略的一般信息，请参阅 Kaspersky Security Center 帮助系统。

# 在 Web Console 中创建策略

*要在 Web Console 中创建策略：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**策略和策略配置文件**”。

   将打开策略和策略配置文件的列表。

2. 选择包含必须应用该策略的设备的管理组。为此，请单击策略和策略配置文件列表上方的“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

3. 单击“**添加**”按钮。

   “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**，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。

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

a. 选择 Light Agent 用来发现可连接的 SVM 的方法。

- **使用 Integration Server**

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

- **使用 SVM 地址的自定义列表**

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

如果选择“**使用 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。

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**”按钮。

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

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

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

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

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

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

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

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

继续执行向导的下一步。

8. 将打开新建策略设置窗口的“**常规**”选项卡。指定新策略的名称。

您还可以配置以下策略设置：

- 策略状态：
  - **活动**。当前应用于设备的策略。如果选择此选项，则下次设备与管理服务器同步时，此策略将在设备上变为活动状态。默认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：
  - **从父策略继承设置**.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。
  - **强制继承子策略中的设置**。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，**从父策略继承设置**切换按钮将自动开启，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。

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

9. 如果您想配置其他策略设置，请转到“**应用程序设置**”选项卡并进行必要的更改。
   您也可以稍后更改策略设置。

10. 单击“**保存**”按钮。

创建的策略将显示在策略列表中。

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

## 在 Web Console 中更改策略设置

*要在 Web Console 中编辑策略设置：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**策略和策略配置文件**”。
   将打开策略列表。

2. 选择包含应用了策略的设备的管理组。为此，请单击窗口上部的“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。
   该列表仅显示为所选管理组配置的策略。

3. 单击列表中所需策略的名称。
   策略属性窗口将打开。

4. 在“应用程序设置”选项卡上修改**策略设置**。

5. 单击“**保存**”按钮以保存更改。

该策略将与更新的设置一起保存。

## Web Console 中的策略设置

策略设置的默认设置和值取决于用于激活应用程序的授权许可。是否对应用程序应用某些策略设置取决于应用程序模式。

您可以在“策略属性”窗口的“**应用程序设置**”选项卡上配置策略设置。

Web Console 中的策略设置详见附录 5。

| 部分 | 子部分 |
| --- | --- |
| **主机威胁防护** | “**文件威胁防护**”。在本小节中，您可以管理文件威胁防护。<br>“**BadUSB 攻击防护**”。在本小节中，您可以管理BadUSB 攻击防护设置。<br>“**可移动驱动器扫描**”。在本小节中，您可以配置当可移动驱动器连接到受保护设备时对其进行扫描的设置。<br>“**行为检测**”。在此小节中，您可以管理应用程序行为检测的设置。<br>“**反加密**”。在本小节中，您可以配置远程恶意加密防护设置。<br>“**漏洞利用防御**”。在本小节中，您可以管理漏洞利用防御设置。 |
| **通信和 Web 保护** | “**邮件威胁防护**”。在本小节中，您可以管理邮件威胁防护设置。<br>“**Web 威胁防护**”。在本小节中，您可以配置Web 威胁防护设置。<br>“**网络威胁防护**”。在本小节中，您可以配置网络威胁防护设置。<br>“**防火墙**”。在本小节中，您可以配置防火墙管理设置。 |
| **安全控制** | “**设备控制**”。在本小节中，您可以配置设备控制设置。<br>“**Web 控制**”。在本小节中，您可以配置Web 控制设置。<br>“**应用程序控制**”。在本小节中，您可以配置应用程序控制设置。<br>“**系统完整性监控**”。在本小节中，您可以配置系统完整性监控设置。 |
| **受信任区域** | 在本节中，您可以管理以下设置：<br>• 文件威胁防护组件应用的排除项。<br>• Web 威胁防护组件应用的排除项。<br>• 网络威胁防护组件应用的排除项。<br>• 网络流量扫描的排除项。<br>• 从文件操作拦截中排除挂载点。<br>• 设备控制组件的受信任设备。 |
| **常规设置** | “**检测设置**”。在本小节中，您可以管理以下设置：<br>• 检测威胁入侵者可以用来破坏设备或数据的合法应用程序。<br>• 文件操作拦截模式。<br>“**卡巴斯基安全网络**”。在本小节中，您可以配置 Kaspersky Endpoint Security 对卡巴斯基安全网络的使用。<br>“**用户交互**”。在本小节中，您可以管理以下设置：<br>• 应用程序启动设置。<br>• 用户的任务管理权限。<br>“**Performance**”。在本小节中，您可以管理以下设置：<br>• 设备使用电池供电时取消计划任务。<br>• 从扫描中排除进程内存。<br>• 扫描任务的内存和处理器资源使用限制。<br>• 应用程序对驻留内存的使用限制。<br>• 应用程序稳定性监控。<br>“**网络设置**”。在本小节中，您可以配置以下内容：<br>• 代理服务器设置，如果客户端设备的用户使用代理服务器连接到互联网。<br>• 网络流量扫描设置。<br>**容器扫描**。在本小节中，您可以管理容器监控组件。<br>“**技术支持**”。在此小节中，您可以管理跟踪和转储设置。<br>“**Reports and Storage**”。在此小节中，您可以管理备份区和隔离区设置。<br>“**KSC 整合**”。在此小节中，您可以管理向 Kaspersky Security Center 存储库发送信息的设置。<br>**操作系统交互设置**。在本小节中，您可以配置以下内容：<br>• 选择想要应用程序使用的**系统事件拦截**机制。<br>在 Web Console 中，您可以在策略属性中配置系统事件拦截（**应用程序设置 → 常规设置 → 操作系统交互设置**）。<br>这些设置仅适用于运行支持 fanotify 技术的操作系统的设备。<br>• 管理高级遥测参数设置。<br>**通知设置**。在此小节中，您可以管理事件通知设置。 |

| 部分 | 子部分 |
| --- | --- |
| **内置代理配置** | “**Managed Detection and Response**”。在本小节中，您可以启用和禁用与 Kaspersky Managed Detection and Response 集成，并上传集成所需的 MDR BLOB 文件。<br>“**Network Detection and Response (KATA)**”。在本小节中，您可以启用或禁用与Kaspersky Network Detection and Response (KATA) 集成。<br>“**Endpoint Detection and Response**”。在本小节中，您可以启用或禁用与卡巴斯基 Detection and Response Optimum 的集成并管理集成设置。<br>“**Endpoint Detection and Response Expert (on-premise)**”。在本小节中，您可以启用或禁用与Kaspersky Endpoint Detection and Response Expert （本地部署）或Kaspersky Endpoint Detection and Response (KATA)的集成并管理集成设置。<br>“**Sandbox**”。在本小节中，您可以启用或禁用与Sandbox 的集成并管理集成设置。<br>“**KUMA 整合**”。在本小节中，您可以启用或禁用与Kaspersky Unified Monitoring and Analysis Platform 集成，并管理集成设置。 |
| **Light Agent 模式**<br>仅当在用于保护虚拟环境的 Light Agent 模式下使用 Kaspersky Endpoint Security 时，本节中描述的设置才适用。 | “**SVM discovery settings**”。在本小节中，您可以选择 Light Agent 用来发现可连接的 SVM 的方法。<br>**Integration Server 连接设置**。在本小节中，您可以配置 Light Agent 与Integration Server 的连接，后者是 Kaspersky Security for Virtualization Light Agent 的一个组件。<br>“**SVM connection tag**”。在本小节中，您可以启用 Light Agent 以使用标签并分配 Light Agent 将用于连接的标签。<br>“**SVM selection algorithm**”。在本小节中，您可以指定希望 Light Agent 使用的 SVM 选择算法。<br>“**Connection protection**”。在此窗口中，可以启用 Light Agent 和 Protection Server 之间的数据链接的加密。 |

# 在管理控制台中管理策略

您可以使用 Kaspersky Security Center 管理控制台中的策略执行以下操作：

- 创建策略。
- 编辑策略设置。您可以在策略属性窗口中管理策略设置。

  如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。

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

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

## 使用管理控制台创建策略

*要在管理控制台中创建策略：*

1. 在管理控制台树中的“**受管理设备**”文件夹中，选择包含应当应用该策略的设备的管理组。

   您可以在采用该管理组名称的文件夹的“**设备**”选项卡上查看属于该管理组的设备列表。

2. 在工作区中选择“**策略**”选项卡。

3. 单击“**新建策略**”按钮以启动“新建策略”向导。

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

4. 在向导的第一步中，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 的模式：

   - 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保护虚拟环境，请配置 SVM 检测设置：

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

      - **使用 Integration Server**

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

      - **使用 SVM 地址的自定义列表**

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

如果选择“**使用 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。

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)。

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

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

  如果将地址指定为 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，该窗口将显示由此策略管理的 Light Agent 可以连接到的 SVM 列表。要向列表中添加 SVM，请单击“**添加**”按钮，然后在打开的窗口中指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。您可以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。

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

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

*要在管理控制台中编辑策略设置：*

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

4. 编辑策略设置。

5. 在**属性：<策略名称>**窗口中，单击“**确定**”以保存更改。

# 管理控制台中的策略设置

策略设置的默认设置和值取决于用于激活应用程序的授权许可。是否对应用程序应用某些策略设置取决于应用程序模式。

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

策略设置

| 部分 | 子部分 |
| --- | --- |
| **关键威胁防护** | **文件威胁防护**。在本小节中，您可以管理文件威胁防护。<br>**文件威胁防护排除项**。在本小节中，您可以配置应用于文件威胁防护保护组件的排除项。<br>**防火墙管理**。在本小节中，您可以配置防火墙管理设置。<br>**Web 威胁防护**。在本小节中，您可以配置Web 威胁防护设置。<br>**邮件威胁防护**。在本小节中，您可以管理邮件威胁防护设置。<br>**网络威胁防护**。在本小节中，您可以配置网络威胁防护设置。<br>**BadUSB 攻击防护**。在本小节中，您可以管理BadUSB 攻击防护设置。 |
| **高级威胁防护** | **卡巴斯基安全网络**。在本小节中，您可以配置 Kaspersky Endpoint Security 对卡巴斯基安全网络的使用。<br>**反加密勒索**。在本小节中，您可以配置远程恶意加密防护设置。<br>**行为检测**。在此小节中，您可以管理应用程序行为检测的设置。 |
| **Detection and Response** | **Managed Detection and Response**。在本小节中，您可以启用和禁用与 Kaspersky Managed Detection and Response 集成，并上传集成所需的 MDR BLOB 文件。<br>**EDR Expert (on-premise)**。在本小节中，您可以启用或禁用与Kaspersky Endpoint Detection and Response (KATA) 集成，并管理集成设置。<br>**Network Detection and Response (KATA)**。在本小节中，您可以启用或禁用与 Kaspersky Network Detection and Response (KATA) 集成。 |
| **安全控制** | **应用程序控制**。在本小节中，您可以配置应用程序控制设置。<br>**系统完整性监控**。在本小节中，您可以配置系统完整性监控设置。<br>**设备控制**。在本小节中，您可以配置设备控制设置。<br>**Web 控制**。在本小节中，您可以配置Web 控制设置。 |
| **本地任务** | **任务管理**。在本小节中，您可以配置用户管理任务的权限。<br>**可移动驱动器扫描**。在本小节中，您可以配置当可移动驱动器连接到受保护设备时对其进行扫描的设置。 |

| 部分 | 子部分 |
| --- | --- |
| **常规设置** | **代理服务器设置**。在本小节中，如果用户通过代理服务器从客户端设备访问互联网，您可以配置代理服务器设置。<br>**应用程序设置**。在本小节中，您可以管理以下设置：<br>• 检测威胁入侵者可以用来破坏设备或数据的合法应用程序。<br>• 通知设置。<br>• 扫描任务的内存和处理器资源使用限制。<br>• 非特权用户可以在同一设备上同时启动的自定义扫描任务的数量限制。<br>• 应用程序启动设置。<br>• 跟踪和转储设置。<br>• 应用程序稳定性监控。<br>• 应用程序对驻留内存的使用限制。<br>• 文件操作拦截模式。<br>**容器扫描设置**。在本小节中，您可以管理容器监控组件。<br>**网络设置** 在本小节中，您可以配置网络流量扫描设置。<br>**全局排除项**。在本小节中，您可以配置以下内容：<br>• 从文件操作拦截中排除挂载点。<br>• 工业软件排除项，用来排除与特定类型软件关联的进程、文件和目录。<br>**排除进程内存**。在本小节中，您可以配置从扫描中排除进程内存。<br>**存储设置**。在本小节中，您可以配置以下内容：<br>• 备份区和隔离区。<br>• 将数据传输至 Kaspersky Security Center 存储的设置。<br>**操作系统交互设置** 在此小节中，您可以配置以下内容：<br>• 选择想要应用程序使用的系统事件拦截机制。<br>• 管理高级遥测参数设置。 |
| **KUMA 整合** | **KUMA 整合**。在本小节中，您可以启用或禁用与Kaspersky Unified Monitoring and Analysis Platform 集成，并管理集成设置。 |
| **Light Agent 模式**<br>仅当在用于保护虚拟环境的 Light Agent 模式下使用 Kaspersky Endpoint Security 时，本节中描述的设置才适用。 | **与 Integration Server 的连接**。在本小节中，您可以配置 Light Agent 与 Integration Server 的连接，后者是 Kaspersky Security for Virtualization Light Agent 的一个组件。<br>**SVM 发现设置**。在本小节中，您可以选择 Light Agent 用来发现可连接的 SVM 的方法。<br>**SVM 连接标签**。在本小节中，您可以启用 Light Agent 以使用标签并分配 Light Agent 将用于连接的标签。<br>**SVM 选择算法**。在本小节中，您可以指定希望 Light Agent 使用的SVM 选择算法。<br>**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 |

# 在 Web Console 中管理任务

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

- 创建新的任务。
- 编辑任务设置。

  如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。

- 启动、停止、暂停和继续任务。

  “*更新*”任务无法暂停或继续，只能启动或停止。

- 导出和导入任务。
- 删除任务。

在任务列表中，您可以监控任务执行结果：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执行情况（“**监控和报告**”→“**事件选择**”）。有关事件选择的详细信息，请参阅 Kaspersky Security Center 文档。

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

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

如果设备受策略管理，则可能无法使用命令行或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。

## 在 Web Console 中创建任务

*要在 Web Console 中为设备组或设备集合创建任务：*

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

6. 结束向导。

在任务列表中将显示一个新任务。

*要在 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“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

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

8. 结束向导。

在任务列表中将显示一个新任务。

# 在 Web Console 中更改任务设置

*要在 Web Console 中编辑任务设置：*

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

   任务列表打开。

2. 执行下列操作之一：

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

     该列表仅显示为所选管理组配置的任务。

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

     该列表显示在管理服务器上创建的所有任务。

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

4. 配置任务设置：

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

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

5. 单击“**保存**”按钮以保存更改。

# 在 Web Console 中启动、停止、暂停和恢复任务

*要在 Web Console 中启动、停止、暂停或恢复任务：*

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

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

     该列表仅显示为所选管理组创建的任务。

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

  该列表显示在管理服务器上创建的所有任务。

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

# 在管理控制台中管理任务

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

- 创建新的任务。
- 编辑任务设置。

  如果用于访问管理服务器的用户帐户没有权限编辑某些功能范围的设置，则无法编辑这些功能范围的设置。

- 启动、停止、暂停和继续任务。

  “*更新*”任务无法暂停或继续，只能启动或停止。

- 导出和导入任务。
- 删除任务。

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

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

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

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

如果设备受策略管理，则可能无法使用命令行或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。

# 在管理控制台中创建任务

*要在管理控制台中为设备组或设备集合创建任务：*

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”系统）。

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

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

   继续执行向导的下一步。

4. 按照向导中的说明配置可用的任务设置。

5. 输入新任务的名称并继续执行向导的下一步。

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

7. 结束向导。

   在任务列表中将显示一个新任务。

*要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。

## 在管理控制台中更改任务设置

*要在管理控制台中编辑任务设置：*

1. 在管理控制台中，执行以下操作之一：

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

2. 在任务列表中，选择所需的任务并双击它以打开“**属性：<任务名称>**”窗口。
   您还可以使用任务上下文菜单中的“**属性**”项打开任务属性窗口。

3. 编辑任务设置。可配置设置的可用性取决于任务的类型。
   任务属性窗口的“**常规**”、“**通知**”、“**计划**”和“**修订历史记录**”选项卡是 Kaspersky Security Center 的标准配置；有关更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

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

## 在管理控制台中启动、停止、暂停和恢复任务

*要在管理控制台中启动、停止、暂停或恢复任务：*

1. 在管理控制台中，执行以下操作之一：

   - 要启动或停止在指定管理组中包含的设备上运行的任务，请在控制台树中选择此管理组，然后在工作区中选择“**任务**”选项卡。
     将打开为所选管理组创建的任务列表。
   - 要启动或停止在一台或多台设备上运行的任务（一组设备的任务），请选择控制台树中的“**任务**”文件夹。
     将打开管理服务器上创建的所有任务的列表。

2. 在任务列表中，选择所需的任务，打开该任务的上下文菜单，然后选择要执行的操作。

# 使用命令行管理应用程序

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

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

除了任务设置之外，还提供了以下设置以用于配置应用程序：

- 常规容器扫描设置。
- 网络流量扫描设置。
- 常规应用程序设置，定义应用程序整体的运行以及各个功能的操作。

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

如果应用程序以 EDR Agent 模式使用，则只有部分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。

# 启用自动添加 kesl-control 命令（bash 完成）

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

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

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

*要为所有新的 bash shell 会话启用自动添加，请运行以下命令：*

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

# 在命令行上管理任务

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

- *文件威胁防护*。此任务允许您启用或禁用实时文件威胁防护并定义文件威胁防护组件的设置。应用程序启动时会自动启动此任务。
- *恶意软件扫描*。此任务允许您根据需要扫描文件系统对象中的恶意软件并定义扫描的设置。您可以使用此任务对设备执行全盘扫描或自定义扫描。
- *关键区域扫描*。此任务允许您根据需要运行操作系统的关键区域扫描并定义扫描的设置。

- *自定义文件扫描*。此任务用于配置和存储使用 `kesl-control --scan-file` 命令扫描指定文件和目录时所用的设置。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。
- *容器扫描*。此任务允许您根据需要扫描容器和镜像并定义扫描的设置。
- *自定义容器扫描*。此任务用于配置和存储使用 `kesl-control [-T] --scan-container` 命令扫描指定容器和镜像时所用的设置。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。
- *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。
- *Web 威胁防护*。此任务允许您启用或禁用 Web 威胁防护并定义 Web 威胁防护组件的设置。
- *网络威胁防护*。此任务允许您启用或禁用网络威胁防护并定义网络威胁防护组件的设置。
- *反加密勒索*。此任务允许您启用或禁用对文件进行远程恶意加密的保护，并定义反加密勒索组件的设置。
- *防火墙管理*。此任务允许您启用或禁用防火墙管理并定义设备上的网络连接控制设置。
- *应用程序控制*。此任务允许您启用或禁用应用程序控制并定义应用程序控制组件的设置。
- *清查*。此任务允许您获取有关设备上存储的所有应用程序可执行文件的信息。
- *设备控制*。此任务允许您启用或禁用设备控制并定义设备控制组件的设置。当 Kaspersky Endpoint Security 启动时，此任务会自动启动。
- *Web 控制*。此任务允许您启用或禁用Web 控制并定义Web 控制组件的设置。
- *行为检测*。此任务允许您监控应用程序在操作系统中的恶意活动。当 Kaspersky Endpoint Security 启动时，此任务会自动启动。
- *系统完整性监控*。该任务允许您对系统完整性监控组件设置中指定监控范围内的对象执行的操作进行实时监控。
- *系统完整性检查*。此任务允许您通过将监控对象的当前状态与之前记录的状态进行比较来检查已包含在监控范围内的文件和目录的变化。
- *授权许可*。使用此任务可以激活安装在设备上的应用程序。该任务在应用程序启动时自动启动，并驻留在设备操作内存中。该任务没有设置；授权许可密钥使用特殊管理命令进行管理。该任务无法启动、停止或删除。
- *更新*。您可以使用此任务执行计划和按需的应用程序数据库和模块更新并编辑更新设置。
- *回滚*。您可以使用该任务回滚应用程序数据库和模块的上一次更新。
- *Kaspersky Endpoint Detection and Response Expert（本地部署）集成*。此任务可启用或禁用与Kaspersky Endpoint Detection and Response Expert（本地部署）或Kaspersky Endpoint Detection and Response (KATA) 的集成并管理集成设置。
- *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) 的整合并指定整合设置。
- *与 Sandbox 集成*。此任务可启用和禁用与 Sandbox 的集成并指定集成设置。
- *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。

- *对象的执行防护 (EDR Expert (on-premise))*。此任务允许您启用或禁用 Endpoint Detection and Response Expert (on-premise) 执行防护规则的使用，并查看这些规则的列表。

- *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。

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

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

任务名称不区分大小写。

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

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

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

应用程序任务

| 任务 | 命令行中的任务名称 | 任务 ID | 任务类型 |
|---|---|---|---|
| 文件威胁防护 | File_Threat_Protection | 1 | OAS |
| 恶意软件扫描 | Scan_My_Computer | 2 | ODS |
| 恶意软件扫描（用户任务） | 用户自定义 | 从 100 开始 | ODS |
| 自定义文件扫描 | Scan_File | 3 | ODS |
| 关键区域扫描 | Critical_Areas_Scan | 4 | ODS |
| 更新 | 更新 | 6 | 更新 |
| 更新（用户任务） | 用户自定义 | 从 100 开始 | 更新 |
| 回滚 | 回滚 | 7 | 回滚 |
| 回滚（用户任务） | 用户自定义 | 从 100 开始 | 回滚 |
| 授权许可 | 授权许可 | 9 | 授权许可 |
| 系统完整性监控 | System_Integrity_Monitoring | 11 | OAFIM |
| 系统完整性监控（用户任务） | 用户自定义 | 从 100 开始 | 光子晶体振荡器 |
| 防火墙管理 | Firewall_Management | 12 | 防火墙 |
| 反加密 | Anti_Cryptor | 13 | AntiCryptor |
| Web 威胁防护 | Web_Threat_Protection | 14 | WTP |
| 设备控制 | Device_Control | 15 | DeviceControl |
| 可移动驱动器扫描 | Removable_Drives_Scan | 16 | RDS |
| 网络威胁防护 | Network_Threat_Protection | 17 | NTP |
| 容器扫描 | Container_Scan | 18 | ContainerScan |
| 容器扫描（用户任务） | 用户自定义 | 从 100 开始 | ContainerScan |
| 自定义容器扫描 | Custom_Container_Scan | 19 | ContainerScan |
| 行为检测 | Behavior_Detection | 20 | BehaviorDetection |
| 应用程序控制 | Application_Control | 21 | AppControl |
| 清查 | Inventory_Scan | 22 | InventoryScan |
| 清查（用户任务） | 用户自定义 | 从 100 开始 | InventoryScan |

| 任务 | 命令行中的任务名称 | 任务 ID | 任务类型 |
| --- | --- | --- | --- |
| Kaspersky Endpoint Detection and Response Expert (on-premise) 集成 | KATAEDR | 24 | KATAEDR |
| Web 控制 | Web_Control | 26 | WebControl |
| Sandbox 集成 | Standalone_Sandbox | 29 | StandaloneSandbox |
| 对象的执行防护 (EDR Expert (on-premise)) | KATAEDR_Prevention | 30 | KATAEDRPrevention |
| Kaspersky Network Detection and Response (KATA) 整合 | KATANDR | 31 | KATANDR |
| 对象的执行防护 (EDR Optimum) | EDRO_Prevention | 32 | 预防 |
| KUMA 整合 | KUMA | 33 | KUMA |
| 邮件威胁防护 | Mail_Monitoring | 35 | MailMonitoring |
| BadUSB 攻击防护 | Bad_USB | 37 | BadUSB |

您可以对任务执行以下操作：

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

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

- 配置任务启动计划。

## 在命令行中查看任务列表

*要查看应用程序任务列表，请执行以下命令：*

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

其中：

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

将显示 Kaspersky Endpoint Security 任务列表。

将为每个任务显示以下信息：

- `Name`：任务名称
- `ID`：任务 ID

- `Type`：任务类型
- `State`：任务的当前状态

如果 Kaspersky Security Center 策略禁止用户查看和编辑本地任务，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。

## 在命令行中查看任务的状态

*若要查看任务状态，请执行以下命令：*

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

其中：

- `<任务 ID/名称>` 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- 指定 `--json`，则以 JSON 格式输出设置。

应用程序任务可以采取以下主要状态：

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

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

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

## 在命令行中创建任务

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

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

您可以使用默认设置或配置文件中指定的设置来创建任务。

*要使用默认设置创建任务，请执行以下命令：*

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

其中：

- <任务名称>是您为新任务指定的名称。
- <任务类型>是您正在创建的任务类型的标识。

*要使用配置文件中指定的设置创建任务，请运行以下命令：*

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

其中：

- <任务名称>是您为新任务指定的名称。
- <任务类型>是您正在创建的任务类型的标识符。
- <文件路径>是包含用于创建任务的设置的配置文件的完整路径。
- 指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json` 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。

## 在命令行中启动、停止、暂停和恢复任务

您可以启动和停止预定义任务和用户任务，但 License 类型的任务除外。

您可以暂停和恢复 ODS、ODFIM 和 InventoryScan 任务。

启动任务

```
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。

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。

停止任务

```
kesl-control --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]` 启用与此任务相关的当前事件的输出。

暂停任务

```
kesl-control --suspend-task <task ID|name>
```

恢复任务

```
kesl-control --resume-task <task ID|name>
```

# 在命令行中删除任务

您只能删除用户任务。无法删除预定义任务。

*要删除任务，请执行以下命令：*

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

其中 <任务 ID/名称> 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

# 在命令行中显示任务设置

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

您可以将任务设置的当前值输出到控制台或可用于更改任务设置的配置文件。

*要将任务设置的当前值输出到控制台，请执行以下命令：*

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

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- 指定 --json ，则以 JSON 格式输出设置。如果未指定 --json选项，则设置以 INI 格式输出。

*要将任务设置的当前值输出到配置文件，请执行以下命令：*

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

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- --file < 配置文件路径 > 是将写入任务设置的配置文件的路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定目录不存在，则不会创建配置文件。
- 指定 --json ，则以 JSON 格式输出设置。如果未指定 --json选项，则设置以 INI 格式输出。

# 在命令行中编辑任务设置

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

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

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

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

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

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

对于某些任务，还提供了单独的管理命令，可让您编辑任务设置。

# 使用配置文件编辑任务设置

*如要使用配置文件编辑任务设置的值：*

1. 使用命令 `kesl-control --get-settings` 将任务设置输出到配置文件中。

2. 打开配置文件并编辑必要设置的值。

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

   如果要添加扫描范围，请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。

     例如：

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

   您可以指定多个 `[ScanScope.item_#]` 和 `[ExcludedFromScanScope.item_#]` 部分。应用程序将按索引升序处理范围。

3. 保存配置文件。

4. 请执行命令：

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

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- --file < 配置文件路径 > 是要从中导入任务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。

# 使用命令行选项编辑任务设置

使用 kesl-control --set-settings 命令选项，您可以编辑任务设置的单个值，还可以为以下 *OAS*、*ODS*、*OAFIM*、*ODFIM* 和 *AntiCryptor* 类型的任务添加或删除扫描范围和排除范围。

## 配置单个任务设置

*如要使用命令行选项编辑任务设置的单个值，请执行以下命令：*

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

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- < 设置名称 >=< 设置值 > 是一项任务设置的名称和值。您可以使用用于显示任务设置的命令来获取任务设置的当前值。

指定任务设置的值将发生更改。

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

## 添加和删除扫描范围

*如要使用命令行选项添加扫描范围，请执行以下命令：*

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

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- --add-path < 路径 > 添加包含要扫描的对象的目录路径。

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

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

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

例如：
为 ID=100 的任务添加扫描范围：

```
kesl-control --set-settings 100 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

以下扫描范围设置将添加到任务中：

```
[ScanScope.item_0001]

AreaDesc=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

*如要使用命令行选项删除扫描范围，请执行以下命令：*

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

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- --del-path < 路径 > 删除包含要扫描的对象的目录路径。

包含指定路径的 [ScanScope.item_#] 部分将从任务设置中删除。应用程序将不会扫描指定目录中的对象。

添加和删除排除范围

*如要使用命令行选项添加排除范围，请执行以下命令：*

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

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- --add-exclusion < 路径 > 添加要从扫描中排除的对象所在目录的路径。

  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。

*如要使用命令行选项删除排除范围，请执行以下命令：*

```
kesl-control --set-settings < 任务 ID/名称 > --del-exclusion < 路径 >
```

其中：

- < 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- --del-exclusion < 路径 > 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。

## 在命令行中恢复默认任务设置

您可以恢复所有用户任务和所有预定义任务的默认设置，但“*回滚*”和“*授权许可*”类型的任务除外（这些任务没有设置）。

*要将任务设置重置为默认值，请执行以下命令：*

```
kesl-control --set-settings < 任务 ID/名称 > --set-to-default
```

其中 < 任务 ID/名称 > 是任务创建时分配给任务的 ID，或者是命令行中的任务名称。

应用程序将设置值改为默认值。

# 在命令行中配置任务计划

如果在标准模式下使用应用程序，则可以配置以下类型任务的运行计划：*ODS*、*更新*、*回滚*、*ODFIM*，*ContainerScan* 和 *InventoryScan*。

如果在 Light Agent 模式下使用应用程序来保护虚拟环境，则可以配置以下类型任务的启运行计划：*ODS*、*ODFIM*，*ContainerScan* 和 *InventoryScan*。

您可以将任务运行计划设置的当前值输出到控制台或配置文件。

*要将任务运行计划的当前设置输出到控制台，请执行以下命令：*

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

其中：

- <任务 ID/名称> 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- 指定 `--json` ，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

*要将任务运行计划的当前设置输出到配置文件，请执行以下命令：*

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

其中：

- <任务 ID/名称> 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- `--file` <配置文件路径> 是将写入任务计划设置的配置文件的路径。如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定目录不存在，则不会创建配置文件。
- 指定 `--json` ，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

例如：

*将更新任务设置保存到名为 update_schedule.ini 的文件，并将创建的文件保存到当前目录：*

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

*在控制台中显示更新任务计划：*

```
kesl-control --get-schedule 6
```

您可以通过下列方式编辑任务运行计划的设置：

- 从包含所有计划设置的配置文件中导入设置。
- 使用命令行，以 <设置名称>=<设置值> 格式指定任务计划的各项设置。

*要使用配置文件编辑任务运行计划设置的值，请执行以下操作：*

1. 使用 `kesl-control --get-schedule` 命令将任务设置输出到配置文件。
2. 编辑文件中必要设置的值并保存更改。
3. 请执行命令：

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

其中：

- < 任务 ID/ 名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- --file < 配置文件路径 > 是将从中导入任务计划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。

文件中定义的任务运行计划的所有设置值都将导入应用程序。

例如：
*从名为 /home/test/on_demand_schedule.ini 的配置文件将计划设置导入到 ID=2 的任务中：*

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

*要使用命令行编辑任务运行计划设置的各个值，请执行以下命令：*

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

其中：

- < 任务 ID/ 名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。
- < 设置名称 >=< 设置值 > 是一项任务计划设置的名称和值。

任务运行计划的指定设置的值被更改。

例如：

*要将任务安排为每十小时启动一次，请指定以下设置：*

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

*要将任务安排为每十分钟启动一次，请指定以下设置：*

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

*要将任务安排为在每月的第 15 天启动，请指定以下设置：*

```
RuleType=Monthly

RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

*要将任务安排为每星期二启动一次，请指定以下设置：*

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

*要将任务安排为每 11 天启动一次，请指定以下设置：*

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

# 通过命令行管理常规应用程序设置

常规应用程序设置定义了应用程序整体的运行以及各个功能的操作。

您可以使用特殊的管理命令来管理常规应用程序设置：

- 将常规应用程序设置的当前值输出到控制台或配置文件。
- 使用包含所有常规设置的配置文件，或使用格式为 < 设置名称 >=< 设置值 > 的命令行选项来编辑常规应用程序设置。

使用常规设置，您可以：

- 在应用程序中配置卡巴斯基安全网络和反恶意软件数据库精简版的使用。
- 在应用程序中配置代理服务器的使用。
- 选择文件操作拦截模式（扫描期间阻止/不阻止文件）。
- 配置从挂载点扫描范围中排除（全局排除项）。
- 配置从进程内存扫描范围中排除。
- 启用或禁用实时容器扫描。
- 启用或禁用对入侵者可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 资源使用率限制。
- 限制非特权用户可以同时启动的用户扫描任务的数量。

## 显示常规应用程序设置

您可以将常规应用程序设置的当前值输出到控制台或可用于编辑应用程序设置的配置文件。

*要将常规应用程序设置的当前值输出到控制台，请执行以下命令：*

```
kesl-control --get-app-settings [--json]
```

其中指定 `--json` ，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。

*要将常规应用程序设置的当前值输出到配置文件，请执行以下命令：*

```
kesl-control --get-app-settings --file <配置文件路径> [--json]
```

其中：

- `--file` <配置文件路径> 是应用程序常规设置将写入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。

例如：
*将常规应用程序设置输出到名为 kesl_config.ini 的文件。将创建的文件保存在当前目录中：*

```
kesl-control --get-app-settings --file kesl_config.ini
```

# 编辑常规应用程序设置

在命令行中，您可以使用 `kesl-control --set-app-settings` 命令编辑常规应用程序设置：

- 您可以使用包含常规应用程序设置的配置文件编辑所有常规设置。您可以使用显示常规设置的命令获取配置文件。
- 您可以使用命令行选项，以 < 设置名称 >=< 设置值 > 格式编辑单个设置。您可以使用显示常规设置的命令获取常规应用程序设置的当前值。

*要使用配置文件编辑常规应用程序设置的值：*

1. 将常规应用程序设置输出到配置文件。
2. 编辑文件中必要参数的值并保存更改。
3. 请执行命令：

   `kesl-control --set-app-settings --file <配置文件路径> [--json]`

   其中：

   - `--file <配置文件路径>` 是包含常规应用程序设置的配置文件的完整路径。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。

*要使用命令行选项编辑常规应用程序设置的值，请执行以下命令：*

`kesl-control --set-app-settings <设置名称>=<设置值> [<设置名称>=<设置值>]`

其中 < 设置名称 >=< 设置值 > 是其中一项常规应用程序设置的名称和值。

指定的常规设置的值将会更改。

例如：
*从配置文件 /home/test/kesl_config.ini 将常规设置导入到应用程序：*

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

*将跟踪文件的详细级别设置为低：*

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

*添加想要从文件操作拦截中排除的挂载点：*

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

# 使用筛选器来限制查询结果

筛选器允许您在执行应用程序管理命令时限制查询结果。

筛选条件是通过一个或多个*逻辑表达式*来指定的，这些表达式使用逻辑运算符 `and` 进行组合。筛选条件必须用引号括起来：

`"< 字段 > < 比较运算符 > '< 值 >'"`

`"< 字段 > < 比较运算符 > '< 值 >' and < 字段 > < 比较运算符 > '< 值 >'"`

其中：

- < 字段 > 是数据库字段的名称。
- < 比较运算符 > 是以下比较运算符之一：
  - > 表示“大于”
  - < 表示“小于”
  - `like` 匹配指定值。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

    > `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”
- < 值 > 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。

您可以在以下应用程序管理命令中使用筛选器：

- 输出有关某些当前应用程序事件的信息（在命令行上查看事件、在 Kaspersky Security Center 中查看事件）：

  `kesl-control -W --query "< 过滤条件 >"`

- 在事件日志中输出有关某些应用程序事件的信息（在命令行上查看事件、在 Kaspersky Security Center 中查看事件）：

  `kesl-control -E --query "< 过滤条件 >"`

- 显示备份中某些对象的相关信息：

  `kesl-control -B --query "< 过滤条件 >"`

- 从备份中删除某些对象：

  `kesl-control -B --mass-remove --query "< 过滤条件 >"`

例如：

*获取在 FileName 字段包含文本“etc”的事件的信息：*

```
kesl-control -E --query "FileName like '%etc%'"
```

*显示有关“ThreatDetected”类型的事件的信息：*

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

*显示由 ODS 类型的任务创建的“ThreatDetected”类型的事件信息：*

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

*获取在 UNIX™ 时间戳系统（自 1970 年 1 月 1 日 00:00:00 (UTC) 起经过的秒数）中指定日期后生成的事件的相关信息：*

```
kesl-control -E --query "Date > '1583425000'"
```

*获取以 YYYY-MM-DD hh:mm:ss 格式指定的日期后生成的事件的相关信息：*

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

*获取备份存储中严重级别为“高”的文件的信息：*

```
kesl-control -B --query "DangerLevel == 'High'"
```

# 导出和导入应用程序设置

如果通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security，则无法导入设置。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则无法导出或导入“*更新*”类型的预定义任务的设置。

Kaspersky Endpoint Security 可让您导出和导入所有应用程序设置，以进行故障排除、验证设置或简化其他用户设备上的应用程序配置。导出设置时，所有应用程序设置（包括常规“容器扫描”设置、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将设置导入应用程序。

在导入或导出设置时，必须启动应用程序。设置导入后，必须重新启动应用程序。

从较早的应用程序版本导入或导出设置时，新设置将设置为默认值。无法将设置导入到较旧的应用程序版本。

*要导出应用程序设置，请执行以下命令：*

```
kesl-control --export-settings --file < 配置文件路径 > [--json]
```

其中：

- `--file <配置文件路径>` 是将保存应用程序设置的配置文件的完整路径。
- 指定 `--json` 后，以 JSON 格式将设置导出到配置文件。如果不指定 `--json` 选项，设置将导出到 INI 文件。

*要从文件导入应用程序设置，请执行以下命令：*

```
kesl-control --import-settings --file <配置文件路径> [--json]
```

其中：

- `--file <配置文件路径>` 是要从中将设置导入应用程序的配置文件的完整路径。
- 指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json`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。

从文件导入设置时，`UseKSN` 和 `CloudMode` 设置会被设为 `No`，并且与 MDR 的集成会被禁用。要开始或恢复使用卡巴斯基安全网络，请将 `UseKSN` 设置的值设为 `Basic` 或 `Extended`。要启用云模式，必须将 `CloudMode` 设置设为 `Yes`。如果启用了 KSN，则云模式可用。要启用MDR 集成，您必须先启用卡巴斯基安全网络的扩展模式，然后将 `UseMDR` 设为 `Yes`。

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。

以下策略设置无法从应用程序 Web 插件 12.3 版本导入到应用程序 12.4 版本中：

- 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）

# 使用命令行管理用户角色

根据用户角色向用户提供通过命令行访问 Kaspersky Endpoint Security 功能的权限。*角色*是用于管理应用程序的一组权限和特权。

在操作系统中创建了四组系统用户：*kesladmin*、*kesluser*、*keslaudit* 和 *nokesl*。在向系统用户分配应用程序角色时，该用户将被添加到相应的组中（请参阅下方*角色*表）。撤消用户的角色时，该用户将从相应的组中移除。

如果没有为系统用户分配应用程序角色，则该用户属于*没有权限的用户*这个单独的组。

因此，这些角色对应于四组操作系统用户：

- kesladmin — 管理员角色
- kesluser — 用户角色
- keslaudit — 审计员角色
- 如果没有分配其他角色，则会将 nokesl 分配给用户。在这种情况下，用户属于*没有特权的用户*这个单独的组

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。

用户角色

| 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>撤销用户角色（管理员无权撤销自己的管理员角色）。<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>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。 |

# 查看用户和角色列表

*要查看用户及其角色的列表，请执行以下命令：*

```
kesl-control [-U] --get-user-list
```

# 为用户分配角色

*要将角色分配给特定用户，请执行以下命令：*

```
kesl-control [-U] --grant-role <角色> <用户>
```

例如：
*要将审计角色分配给用户 test15：*

```
kesl-control --grant-role audit test15
```

## 撤销用户角色

*要撤销特定用户的角色，请执行以下命令：*

```
kesl-control [-U] --revoke-role <角色> <用户>
```

例如：
*要为用户 test15 撤销 audit 角色：*

```
kesl-control --revoke-role audit test15
```

# 启动和停止应用程序

将 Kaspersky Endpoint Security 安装到设备后，应用程序将自动启动。默认情况下，启动操作系统时，应用程序将自动启动（处于每个操作系统的默认执行级别）。

默认情况下，启动 Kaspersky Endpoint Security 时，应用程序的以下功能组件将自动启动：

- 文件威胁防护。
- 设备控制。
- 行为检测。
- Web 威胁防护 — 仅当操作系统中安装了某个受支持的浏览器且在设备上允许本地管理 Web 威胁防护设置（未应用策略或策略未在策略属性中设置“锁定”）。
- 网络威胁防护—仅当通过策略定义设备上的网络威胁防护设置时。策略属性中默认启用网络威胁防护。如果在设备上应用本地配置的设置，则默认禁用网络威胁防护。

当应用程序启动时，设备上将自动启动服务任务，以确保附加应用程序功能的运行：应用程序激活功能和备份功能。

默认情况下，应用程序还将启动在命令行中配置的用户任务，这些任务的运行模式已被配置为“应用程序启动后”（PS 运行模式）。

如果停止应用程序，设备上运行的所有任务都将中断。应用程序重新启动后，中断的用户任务不会自动恢复。

# 使用 Web Console 启动和停止应用程序

*要远程启动或停止应用程序：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。
   将打开受管理设备列表。
2. 在列表中，选择要在其上启动或停止应用程序的设备，然后单击带有设备名称的链接以打开设备属性窗口。
3. 选择“**应用程序**”选项卡。
4. 选中 Kaspersky Endpoint Security 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。

# 使用管理控制台启动和停止应用程序

*要在客户端设备上启动或停止应用程序：*

1. 在管理控制台树中，进入“**受管理设备**”文件夹，选择包含必要设备的管理组。
2. 在工作区中选择“**设备**”选项卡。
3. 在受管理设备列表中，选择要为其启动或停止应用程序的设备。在设备上下文菜单中，选择“**属性**”。
4. 在“**属性：<设备名称>**”窗口中，选择“**应用程序**”部分。
   窗口右侧将显示设备上安装的卡巴斯基应用程序列表。
5. 选择“Kaspersky Endpoint Security”。
6. 执行下列操作之一：
   - 要运行应用程序，请单击卡巴斯基应用程序列表右侧的  按钮或在应用程序上下文菜单中选择“**启动**”。
   - 要停止应用程序，请单击卡巴斯基应用程序列表右侧的  按钮或在应用程序上下文菜单中选择“**停止**”。

# 使用命令行启动和停止应用程序

要运行应用程序，根账户必须是以下目录的所有者，并且只有所有者必须具有对这些目录的写入权限：/var、/var/opt、/var/opt/kaspersky、/var/log/kaspersky、/opt、/opt/kaspersky、/usr/bin、/usr/lib、/u

## 启动、重启和停止 Kaspersky Endpoint Security

*要启动应用程序，请运行以下命令：*

```
systemctl start kesl
```

*要停止应用程序，请运行以下命令：*

```
systemctl stop kesl
```

*要重启应用程序，请运行以下命令：*

```
systemctl restart kesl
```

## 监控 Kaspersky Endpoint Security 的状态

Kaspersky Endpoint Security 状态由监视服务监控。监视服务在应用程序启动时自动启动。

如果应用程序崩溃，则会生成 dump 文件，并自动重启应用程序。

*要导出应用程序设置，请运行以下命令：*

```
systemctl status kesl
```

# 查看设备保护状态和应用程序性能信息

您可以查看有关设备保护状态的信息，以及设备上 Kaspersky Endpoint Security 及其组件的状态。

您可以通过以下方式获取有关设备保护状态的信息：

- 在 Web Console 或管理控制台中，使用客户端设备的状态（*正常*、*严重*、*警告*）。安装了 Kaspersky Security Center 网络代理的设备是 Kaspersky Security Center 的客户端设备。客户端设备的状态可能由于以下原因变为“*严重*”或“*警告*”：

  - 按照 Kaspersky Security Center 定义的规则。例如，如果设备上未安装安全应用程序、长时间未执行病毒扫描、应用程序数据库已过时、授权许可已过期或应用程序不稳定，则状态会发生变化。有关更改状态的原因以及配置分配状态的条件的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

  - Kaspersky Security Center 从托管应用程序（即 Kaspersky Endpoint Security）接收设备状态。

    > 必须在 Kaspersky Security Center 中分配“*严重*”和“*警告*”状态的条件列表中启用从托管应用程序接收设备状态。分配设备状态的条件在管理组的属性窗口中配置。

  有关客户端设备状态的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

- 在 Web Console 或管理控制台中，使用设备上 Kaspersky Endpoint Security 功能组件的状态。在设备上安装的 Kaspersky Endpoint Security 的属性中，显示了应用程序的功能组件列表。对于每个组件，都会显示其状态。

- 在命令行上使用以下管理命令：

  - `kesl-control --app-info` 命令，用于显示应用程序性能信息以及应用程序功能组件和任务的状态。

  - `kesl-control --supported-tech-info` 命令，用于显示应用程序功能列表、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 --get-statistic` 命令，用于输出应用程序性能统计数据和挂载点列表。

  - `kesl-control --export-metrics` 命令，用于输出操作系统状态指标。

# 在 Web Console 中查看设备的保护状态

*要在 Web Console 中查看设备的保护状态：*

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

   将打开受管理设备列表。

2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

3. 在列表中，找到要查看信息的设备，然后单击设备名称。

4. 在打开的受管理设备的属性窗口中，在“**常规**”选项卡上，选择“**保护**”部分。

“**保护**”部分显示有关设备的以下信息：

- **在网络中可见**是所选设备在网络中的可见性：“*是*”或“*否*”。
- **设备状态**是根据管理员针对所选设备设置的保护状态标准以及设备在网络中的活动情况，生成的客户端设备的状态：*正常*、*严重*或*警告*。
- **状态描述**表示设备状态更改为“*严重*”或“*警告*”的原因。
- **保护状态**代表所选设备上“文件威胁防护”的当前状态，例如“*运行中*”、“*已停止*”或“*已暂停*”。
- **上次完全检查**表示所选设备上次完成全盘扫描任务的日期和时间。
- **检测到的病毒数**表示自安装 Kaspersky Endpoint Security 以来在所选设备上检测到的恶意对象总数（检测到的威胁计数器）。
- **清除失败的对象**表示 Kaspersky Endpoint Security 无法清除的受感染对象数量。

# 在管理控制台中查看设备的保护状态

*要在管理控制台中查看设备的保护状态：*

1. 在管理控制台树中，进入“**受管理设备**”文件夹，选择包含必要设备的管理组。

2. 在工作区中选择“**设备**”选项卡。

3. 在受管理设备列表中，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。

# 在 Web Console 中查看有关应用程序运行的信息

*要在 Web Console 中查看有关应用程序操作的信息：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。
   将打开受管理设备列表。
2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。
   列表仅显示所选管理组的受管理设备。
3. 在列表中，找到要查看信息的设备，然后单击设备名称。
4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。
5. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。
   应用程序属性窗口将打开。

此窗口显示有关 Kaspersky Endpoint Security 的以下信息：

- **信息**部分中的**常规**选项卡显示有关已安装应用程序的常规信息：
  - **名称**是应用程序的名称。
  - **版本**是应用程序的版本号。
  - **已安装**是在设备上安装应用程序时的日期和时间。
  - **上次软件更新**：Kaspersky Endpoint Security 软件模块上次更新的日期和时间。
  - **上次同步**是设备上次连接到 Kaspersky Security Center 管理服务器的日期和时间。
  - **当前状态**：设备上的文件威胁防护状态，例如“*运行中*”或“*已暂停*”。
  - **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。
- 在**“常规”**选项卡上，**“授权许可”**部分包含有关添加到应用程序的授权许可密钥以及与这些密钥对应的授权许可的信息。
- 在**常规**选项卡上，**组件**部分包含应用程序的功能组件列表。将显示每个组件的状态（例如，*“已停止”*、*“已暂停”*、*“未安装”*）和版本。
  在**用于保护虚拟环境的 Light Agent 模式**行中，您可以看到有关应用程序使用模式的信息：
  - 状态“*运行中*”表示正在 Light Agent 模式下使用应用程序。
  - 状态“*未安装*”表示正在标准模式下使用应用程序。
- **事件**选项卡显示设备上的应用程序事件列表。

- “**事件设置**”选项卡显示应用程序在事件存储中存储的事件类型以及存储时长。
- 在“**应用程序设置**”选项卡上，您可以执行以下操作：
  - 在**Detection and Response**部分，您可以管理设备的网络隔离。
  - 在**应用程序控制**部分，您可以将配置的组件设置和应用程序类别导出到文件，也可以从文件导入它们。
  - 在**统计数据**部分，您可以查看应用程序统计数据和挂载点列表。

# 在管理控制台中查看有关应用程序操作的信息

*要在 Kaspersky Security Center 管理控制台中查看有关应用程序操作的信息：*

1. 在 Kaspersky Security Center 管理控制台树的“**受管理设备**”文件夹中，选择包含所需设备的管理组。
2. 在工作区中选择“**设备**”选项卡。
3. 在受管理设备列表中，选择所需的设备并双击以打开“**属性：<任务名称>**”窗口。
4. 在显示的受管理设备属性窗口中，选择“**应用程序**”部分。
   窗口右侧将显示设备上安装的卡巴斯基应用程序列表。
5. 选择 Kaspersky Endpoint Security 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。

此窗口显示有关 Kaspersky Endpoint Security 的以下信息：

- **常规**部分包含有关已安装应用程序的常规信息：
  - **版本号**：应用程序的版本号。
  - **已安装**是在设备上安装应用程序时的日期和时间。
  - **当前状态**是设备上的文件威胁防护状态，例如“*运行中*”或“*已暂停*”。
  - **上次软件更新**：Kaspersky Endpoint Security 软件模块上次更新的日期和时间。
  - **已安装的更新**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。
- 在**应用程序控制**部分，您可以将配置的组件设置和应用程序类别导出到文件，也可以从文件导入它们。
- **统计数据**部分显示应用程序统计数据和有关挂载点的信息。
- “**组件**”部分包含标准应用程序组件的列表。将显示每个组件的状态（例如，*“已停止”*、*“已暂停”*、“*未安装*”）和版本。

在**用于保护虚拟环境的 Light Agent 模式**行中，您可以看到有关应用程序使用模式的信息：

- 状态“*运行中*”表示正在 Light Agent 模式下使用应用程序。
- 状态“*未安装*”表示正在标准模式下使用应用程序。

- “**授权许可密钥**”部分包含有关活动和备用授权许可密钥的信息。
- “**事件设置**”部分显示应用程序在事件存储中存储的事件类型以及存储时长。
- **高级**部分包含有关应用程序管理插件的信息。

# 在命令行中查看有关应用程序操作的信息

*要查看有关应用程序的信息，请运行以下命令：*

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

其中 `--json`：以 JSON 格式输出数据。如果未指定 `--json`选项，则设置以 INI 格式输出。

命令执行的结果会在控制台中显示如下信息：

- **Name**。应用程序名称。
- **版本**。当前应用程序版本。
- **策略**。有关 Kaspersky Security Center 策略是否应用于设备的信息。
- 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主授权许可的信息：
  - **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)。

- 有关激活应用程序附加功能的授权许可的授权许可信息。如果向受保护的设备添加了任何附加功能密钥，则会显示以下字段：
  - **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（本地部署）授权许可信息**。有关激活 Endpoint Detection and Response Expert（本地部署）组件所用的授权许可信息，或 EDR Expert（本地部署）授权许可密钥状态。
  - EDR **Expert（本地部署）**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。
- **备份使用**。备份容量。
- Scan_My_Computer **任务的上次运行日期**。上次运行"恶意软件扫描"任务的时间。
- **数据库的上次发布日期**。应用程序数据库的上次发布日期和时间。
- **应用程序数据库**。有关应用程序数据库是否已下载的信息。
- **可更新内核模块状态**。关于可更新内核模块状态的信息。
- **使用卡巴斯基安全网络**。有关使用卡巴斯基安全网络的信息：扩展 KSN 模式、基本 KSN 模式或已禁用。
- **用于保护虚拟环境的 Light Agent 模式**。有关在用于保护虚拟环境的 Light Agent 模式下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**。指示应用程序在 Endpoint Detection and Response Agent 模式下使用。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。
- 与 Kaspersky Managed Detection and Response **整合**。与 Kaspersky Managed Detection and Response 整合的状态：已启用、已禁用。

- **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（容器扫描、容器监控）。
- **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（本地部署）集成**。与Kaspersky Endpoint Detection and Response Expert（本地部署）或Kaspersky Endpoint Detection and Response (KATA)的集成状态。
- **与 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。
- **不稳定的应用程序操作**。有关应用程序失败和转储文件创建的信息。如果在上次启动应用程序时发生了失败，则显示该字段。

# 查看应用程序统计数据

为了提高性能，您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进程路径以及设备上检测到的挂载点。

在支持 fanotify 的操作系统的设备上，提高性能的最有效方法是排除挂载点。

您可以通过以下方式查看有关最常扫描的文件和启动的进程的统计数据以及检测到的挂载点列表：

- 在 Web Console 中
- 在管理控制台中
- 在命令行中

您可以在 kesl.ini 配置文件的 `[ScannerImpactStats]` 部分中配置应用程序计算和显示统计信息的参数。

# 在 Web Console 中查看应用程序统计数据

*要在 Web Console 中查看应用程序统计数据：*

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

   将打开受管理设备列表。

2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。

   列表仅显示所选管理组的受管理设备。

3. 在列表中，找到要查看信息的设备，然后单击设备名称。

4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。

5. 在设备上安装的应用程序列表中，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**。

   这将会打开**扫描统计**窗口。

   **扫描统计**窗口显示以下应用程序统计数据：

   - **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。

   使用位于每个块顶部的**导出**按钮，您可以将该块中显示的统计数据导出到文本文件。

# 在管理控制台中查看应用程序统计数据

*要在管理控制台中查看应用程序统计数据：*

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. 在打开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**。
   右侧窗口将显示以下应用程序统计数据：
   - **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。

   使用每个块下的**导出**按钮，您可以将该块中显示的统计数据导出到文本文件。

# 在 Web Console 中查看挂载点列表

*要在 Web Console 中查看挂载点列表：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。
   将打开受管理设备列表。
2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。
   列表仅显示所选管理组的受管理设备。
3. 在列表中，找到要查看信息的设备，然后单击设备名称。
4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。
5. 在设备上安装的应用程序列表中，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。

**挂载点**窗口会显示一个表格，其中包含以下列：

- **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

通过单击位于列表上方窗口顶部的“**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。

# 在管理控制台中查看挂载点列表

*要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. 在打开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 → 挂载点**。
   **挂载点列表表**显示在窗口右侧，包含以下列：

   - **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。

# 在命令行中查看应用程序统计数据和挂载点列表

*要查看应用程序统计数据和挂载点列表，请运行以下命令：*

```
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。

  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

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。

# 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。

*要配置应用程序以获取应用程序使用的操作系统资源的指标，请运行以下命令：*

```
kesl-control [-J] --export-metrics [--period <两次导出之间的间隔（秒）>|--interactive]
```

其中：

- `--period`可启用定期输出结果。
- `--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>传感器 | kesl 进程当前打开的描述符的数量。<br>如果描述符的数量增长速度超过每小时 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>传感器 | 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>传感器 | 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>传感器 | kesl 进程当前使用的交换内存量。<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_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>传感器 | 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>传感器 | 当前拦截的入站网络连接数。 |
| lfs_tproxy_connection_count<br>'direction=outbound' 标签<br>传感器 | 当前拦截的出站网络连接数。 |
| 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_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>传感器 | 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>传感器 | 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>传感器 | 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。 |
| 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>传感器 | 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>传感器 | fanotify 拦截器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 |
| --- | --- |
| lfs_oas_cache_file_count<br>传感器 | 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>传感器 | 文件威胁防护装载点缓存的当前大小。 |
| lfs_processManager_cache_size<br>传感器 | 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>传感器 | 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_prevention_cache_file_count<br>传感器 | 不需要扫描的对象的"对象执行保护"任务的文件缓存的当前大小。 |
| lfs_prevention_cache_file_hit_count<br>计数器 | 不需要扫描的对象的"对象执行保护"任务的击中次数。 |
| lfs_prevention_cache_file_miss_count<br>计数器 | 不需要扫描的对象的"对象执行保护"任务的错过次数。 |
| lfs_prevention_cache_volume_count<br>传感器 | "对象执行保护"任务的挂载点缓存的当前大小。 |
| eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds<br>传感器 | 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>传感器 | 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>传感器 | 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。 |

# 更新应用程序数据库和模块

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 Kaspersky Endpoint Security 的数据库和应用程序模块可确保为您的设备提供最新保护。新病毒、恶意软件和其他类型的威胁每天都在全世界出现。应用程序数据库包含有关威胁和威胁消除方法的信息。要快速检测到威胁，建议您定期更新应用程序数据库和模块。

定期更新数据库需要当前的应用程序授权许可。如果没有最新的授权许可，您将只能执行一次更新。

在更新过程中，数据库和应用程序模块将被下载并安装到您的设备上。您可以从卡巴斯基更新服务器、管理服务器存储库、本地或网络目录以及其他更新源获取数据库和应用程序模块的更新。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则 SVM 上的目录将用作更新源。

更新时，您设备上的应用程序模块和数据库将与更新源处的最新版本进行对比。如果您当前数据库和程序模块与相应的最新版本不同，缺少的更新部分将安装在您的设备上。

如果数据库过时，更新包可能会很大，这可能会花费更多的互联网流量（最多达几十 MB）。磁盘空间量最多可达 3 GB。

通过标准网络协议从卡巴斯基更新服务器或者其他 FTP、HTTP 或 HTTPS 服务器下载更新。默认情况下，系统将自动确定互联网连接设置。如果您使用代理服务器，请在应用程序的常规设置中指定代理服务器设置。

无论更新源是什么，都会下载更新包并使用“*更新*”任务在设备上安装数据库和应用程序模块更新。应用程序中创建了预定义任务“*更新*”。使用此任务，您可以对数据库和应用程序模块进行计划和按需更新并配置更新设置。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则受保护的虚拟机上的数据库使用特殊的“*更新*”本地任务进行更新，其中 SVM 上的目录被指定为更新源。该更新任务自动启动。您不能删除此任务，也不能更改其设置。不支持使用在 Kaspersky Security Center 中创建的任务来更新数据库和应用程序模块。

如果 Kaspersky Endpoint Security 以标准模式或 Endpoint Detection and Response Agent 模式使用，则在 Kaspersky Security Center 中，您可以使用安装管理 MMC 插件或 Kaspersky Endpoint Security 管理 Web 插件后由初始配置向导创建的 *Update* 组任务。您还可以在命令行和 Kaspersky Security Center 中创建更新用户任务。

您可以配置以下设置来更新数据库和应用程序模块：

- 根据所使用的更新方案，选择应用程序接收更新的来源。
- 配置尝试连接所选更新源时的响应超时。如果更新源在指定时间内未响应，应用程序将联系列表中的下一个更新源。
- 配置更新任务的运行计划。默认情况下，应用程序每 60 分钟更新一次数据库。

您还可以接收自动安装的应用程序更新（自动补丁）。在更新任务设置中，您可以选择自动补丁的下载和安装方式：下载并安装、仅下载或不下载。

# 更新数据库和模块

更新期间，以下对象将下载并安装到您的设备中：

- 应用程序数据库。应用程序数据库包括恶意软件特征数据库、网络攻击描述、恶意和钓鱼网址数据库、条幅数据库、垃圾邮件数据库以及其他数据。

  如果设备上的数据库更新中断或终止并显示错误，应用程序将继续使用先前安装的数据库版本。如果之前没有安装应用程序数据库，应用程序将继续在"无数据库"模式下运行。数据库和应用程序模块更新仍然可用。

  如果数据库更新成功，但数据库本身已损坏且应用程序连续多次因错误而终止，则数据库将被自动删除。应用程序继续在"无数据库"模式下工作；数据库和应用程序模块更新功能仍然可用。

  如果数据库是在不到三天前下载的，则该数据库为最新。默认情况下，如果最近安装的数据库更新在卡巴斯基服务器上发布的时间已超过三天但少于七天，则应用程序将生成"*应用程序数据库已过期*"事件。如果数据库已七天未更新，应用程序会生成"*应用程序数据库已严重过期*) 事件。

- 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。

  可以安装应用程序模块，而无需考虑应用程序的状态（已启动或已停止，由 Kaspersky Security Center 策略管理）和更新计划。在应用程序模块更新过程中，Kaspersky Endpoint Security 会继续保护您的设备。在更新期间，应用程序设置和应用程序日志文件将迁移到新版本的应用程序。

  如果应用程序设置的传输由于任何原因失败，应用程序将设置为默认值。

  更新完成后且应用程序重新启动前对应用程序设置进行的更改不会保存。

  如果应用程序在更新后不能正常工作，它会自动回滚到以前的版本。建议联系卡巴斯基技术支持。

# 更新源和更新场景

*更新源*是包含 Kaspersky Endpoint Security 数据库和应用程序模块更新的资源。更新源可以是 FTP、HTTP 或 HTTPS 服务器（如卡巴斯基更新服务器），以及用户挂载的本地或网络目录。

如果 Kaspersky Endpoint Security 在 Light Agent 模式下保护虚拟环境，则受保护的虚拟机上的数据库将从 SVM 上的目录进行更新。

主要的应用程序更新源是卡巴斯基更新服务器。您可以在"*更新*"任务设置中指定其他更新源。如果无法从一个更新源执行更新，Kaspersky Endpoint Security 会切换到下一个更新源。

Kaspersky Endpoint Security 支持下列数据库和应用程序模块更新方案：

- 从卡巴斯基更新服务器进行更新。卡巴斯基更新服务器位于世界各地的不同国家/地区，这确保了更新的高可靠性。如果无法从其中一个服务器执行更新，应用程序会切换到下一个服务器。通过 HTTPS 协议下载更新。

- 集中更新可减少外部互联网流量，并提供方便的更新监控。

  集中更新包括以下步骤：

  1. 将更新包下载到组织网络内的存储库。

您可以使用 Kaspersky Security Center 管理服务器的存储库作为存储库。

更新包通过管理服务器的“*将更新下载到管理服务器存储库*”任务下载到管理服务器存储库。

如果您使用 Kaspersky Security Center 云控制台来管理应用程序，则可以使用分发点（已安装网络代理的设备）的存储库作为存储库。有关分发点的更多详细信息，请参阅“Kaspersky Security Center 帮助”。

2. 将更新包分发到客户端设备

   更新包由 Kaspersky Endpoint Security 的“*更新*”任务分发到客户端设备。在任务设置中，选择 Kaspersky Security Center 作为更新源。

- 从用户挂载的本地或网络目录 (SMB/NFS)，或从 FTP、HTTP 或 HTTPS 服务器进行更新。您可以在“*更新*”任务设置中指定自定义更新源。

# 在 Web Console 中更新应用程序数据库和模块

在 Web Console 中，您可以使用“*更新*”任务更新数据库和应用程序模块。您可以使用自动创建的“*更新*”组任务，也可以创建用户任务进行更新。

*要在 Web Console 中配置更新设置：*

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

   任务列表打开。

2. 执行下列操作之一：

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

     该列表仅显示为所选管理组配置的任务。

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

     该列表显示在管理服务器上创建的所有任务。

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

4. 在任务属性窗口中，选择“**应用程序设置**”选项卡。在左侧列表中选择**更新源**部分。

5. 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。

6. 选择“**设置**”部分并配置其他更新设置。

7. 选择“**计划**”选项卡并配置运行更新任务的计划。

   如果您已选择 **Kaspersky Security Center** 作为更新源，请从“**启动计划**”下拉列表中选择“**当下载更新到存储库时**”。有关计划任务的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

8. 单击“**保存**”按钮以保存更改。

任务将根据配置的计划启动。您也可以手动运行任务。

Update 任务部分的更新源

| 设置 | 描述 |
| --- | --- |
| 更新源表 | 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>• **更新源**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**指示是否在任务中使用源（“**已启用**”或“**已禁用**”）。您可以通过在**更新源**窗口中启用或禁用**使用此源**拨动开关来更改状态，您可以通过单击源名称的链接打开该窗口。<br>您可以在表中**添加**、**编辑**、删除、**上移**或**下移**更新源。<br>单击“**下移**”按钮可将所选项目在表中向下移动。<br>如果在表中只选择一个项目，则此按钮可用。<br>单击“**上移**”按钮可将所选项目在表中向上移动。<br>如果在表中只选择一个项目，则此按钮可用。<br>所选元素的设置在单独的窗口中更改。<br>单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。 |

Update 任务设置部分

| 设置 | 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。 |

# 在管理控制台中更新应用程序数据库和模块

在管理控制台中，您可以使用“*更新*”任务更新数据库和应用程序模块。您可以使用自动创建的“*更新*”组任务，也可以创建用户任务进行更新。

*要在管理控制台中配置更新设置：*

1. 在管理控制台中，执行以下操作之一：
   - 要编辑在指定管理组中包含的设备上运行的任务的设置，请在控制台树中选择此管理组，然后在工作区中选择“**任务**”选项卡。
   - 要编辑在一台或多台设备上运行的任务（一组设备的任务）的设置，请选择控制台树中的“**任务**”文件夹。
2. 在任务列表中，选择所需的“**更新**”任务，然后双击以打开任务属性窗口。
3. 在任务属性窗口中，选择左侧列表中的“**更新源**”部分。

4. 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**”部分并配置运行更新任务的计划。

   如果您已选择 **Kaspersky Security Center** 作为更新源，请从“**计划启动**”下拉列表中选择“**当下载更新到存储库时**”。有关计划任务的更多详细信息，请参阅“Kaspersky Security Center 帮助”系统。

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

任务将根据配置的计划启动。您也可以手动运行任务。

Update 任务部分的更新源

| 设置 | 描述 |
| --- | --- |
| **更新源** | 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。<br>单击“**下移**”按钮可将所选项目在表中向下移动。<br>如果在表中只选择一个项目，则此按钮可用。<br>单击“**上移**”按钮可将所选项目在表中向上移动。<br>如果在表中只选择一个项目，则此按钮可用。<br>所选元素的设置在单独的窗口中更改。<br>单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。 |

Update 任务设置部分

| 设置 | 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。 |

# 在命令行中更新应用程序数据库和模块

在命令行上，您可以通过以下方式更新数据库和应用程序模块：

- 使用"*更新*"预定义任务。您可以手动启动、停止、暂停或恢复此任务并配置任务运行计划。您可以通过编辑此任务的设置来管理更新设置。
- 使用用户任务进行更新（"*更新*"类型的任务）。您可以手动启动用户任务并配置任务计划。

更新任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |

# 使用 Kaspersky 更新实用程序更新

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。

# 回滚应用程序数据库和模块更新

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则该任务不能用于回滚数据库更新。

第一次更新应用程序数据库后，就可以将应用程序数据库回滚至先前版本了。

每次用户开始更新过程时，Kaspersky Endpoint Security 都会为当前应用程序数据库创建一个备份副本。这可让您在需要时将应用程序数据库回滚到以前的版本。

回滚上一次数据库更新可能很有用，例如，当新的应用程序数据库版本包含无效签名而导致 Kaspersky Endpoint Security 阻止安全的应用程序时。

在命令行中，要回滚更新，您可以运行“*回滚*”预定义任务或创建并运行用于回滚更新的用户任务（“*回滚*”类型的任务）。

在 Kaspersky Security Center 中，您可以使用 Web Console 或管理控制台为管理组或单个设备创建回滚任务。

“*回滚*”任务没有任何设置。

# 文件威胁防护

文件威胁防护组件可防止设备的文件系统受到感染。当 Kaspersky Endpoint Security 启动时，该组件会使用默认设置自动启用。它驻留在设备操作内存中，并实时扫描已经打开、保存和启动的所有文件。

检测到恶意软件后，Kaspersky Endpoint Security 可能会移除受感染的文件并终止从该文件启动的恶意软件进程。

组件的运行会受到文件操作拦截模式的影响，您可以在应用程序的常规设置中选择该模式。默认在扫描期间阻止对文件的访问。

如果 root 用户没有权限访问通过 NFS4 协议挂载到设备上的远程目录，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并启用了容器监控（容器扫描、容器监控），应用程序还会扫描所有受支持的操作系统上的所有命名空间和容器。

您可以启用或禁用“文件威胁防护”，还可以配置保护设置：

- 选择文件扫描模式（打开时扫描或打开并修改时扫描）。
- 启用或禁用对压缩文件、邮件数据库、文本格式的电子邮件消息的扫描。
- 暂时从重新扫描范围中排除文本格式的文件。
- 限制要扫描的对象的大小以及对象扫描的持续时间。
- 选择应用程序将对感染对象执行的操作。
- 配置*扫描范围*。该应用程序将扫描文件系统指定区域中的对象。
- 配置从扫描范围中排除的对象。*扫描排除项*是一组条件。当满足这些条件时，该应用程序不会扫描对象中是否存在病毒和其他恶意软件。您可以从扫描范围中排除以下对象：
  - 按名称或掩码排除的对象
  - 按对象中检测到的威胁的名称排除的对象
  - 文件系统指定区域中的文件和目录
  - 指定进程正在修改的进程和文件

  应用程序还会自动将一些内部进程从扫描中排除，例如 Watchdog 服务器进程。
- 配置扫描期间启发式分析器和 iChecker 技术的使用。
- 启用或禁用对有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息进行记录。

要优化“文件威胁防护”任务，您可以从扫描范围中排除正在从网络目录复制的任何文件。只有在复制到本地目录的过程完成后才会扫描文件。要从扫描范围中排除位于网络目录中的文件，请根据用于从网络目录复制的实用程序（例如 cp 实用程序）的进程配置排除。如果您使用 Kaspersky Security Center 管理应用程序，则可以在 Web Console 或管理控制台中根据进程配置排除。如果您使用命令行管理应用程序，则可以通过向 OAS 任务设置中添加 [ExcludedForProgram.item_#] 部分来按进程配置排除项。

# 在 Web Console 中配置文件威胁防护

在 Web Console 中，您可以在策略属性中管理文件威胁防护设置（**应用程序设置 → 主机威胁防护 → 文件威胁防护**）。

# 在管理控制台中配置文件威胁防护

在管理控制台中，您可以在策略属性中管理文件威胁防护设置（在管理控制台中管理策略，使用管理控制台创建策略）（**基本威胁防护 → 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 |
| --- | --- |
| **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** | 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>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>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。<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。 |

# “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。 |
| **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。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |
| **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（在管理控制台中管理策略，使用管理控制台创建策略）（**基本威胁防护** → **文件威胁防护排除项**）中管理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 |
| --- | --- |
| **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。

# <新建扫描范围>窗口

在此窗口中，您可以添加和配置扫描排除范围。

排除范围设置

| 设置 | 描述 |
| --- | --- |
| **排除范围名称** | 用于输入排除范围名称的字段。此名称将显示在**排除范围**窗口的表格中。<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>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。<br>掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。<br>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。<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。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |

## “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。 |
| **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。<br>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。<br>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。<br>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 |
| **文件系统名称** | 用于输入要添加到排除范围中的目录所在的文件系统名称的字段。<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。 |

# 在命令行中配置文件威胁防护

在命令行中，您可以使用“文件威胁防护”预定义任务 (*File_Threat_Protection*) 来管理“文件威胁防护”。

默认启动“文件威胁防护”任务。您可以手动启动和停止该任务。

要从命令行启动和停止“文件威胁防护”任务，需要管理员角色权限。

您可以通过编辑“文件威胁防护”预定义任务的设置来配置“文件威胁防护”设置。

# “文件威胁防护任务”设置

该表介绍了可为文件威胁防护任务指定的所有设置的全部可能值以及默认值。

“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>例如：<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>例如：<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。 | 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。 | 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>例如：<br>AreaDesc=" 扫描电子邮件数据库 " |
| 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>例如：<br>AreaMask_item_< 项目编号 >=*doc |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。您可以使用**掩码**和**标签**指定路径。<br><br>您可以使用特殊标签来指定容器或镜像：<br><br>• [container-id:<id>]/<path to local directory><br><br>• [container-name:<name>]/<path to local directory><br><br>• [image-id:<id>]/<path to local directory><br><br>• [image-name:<name>]/<path to local directory><br><br>其中：<br><br><id> 是容器 ID。<br><br><name> 是容器名称<br><br><path to local directory> 是本地目录的路径。<br><br>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>。<br><br>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。<br><br>例如：<br><br>• [container-name:<name>][image-name:<name>]/path to local directory><br><br>• [container-id:<id>][image-name:<name>]/<path to local directory><br><br>• [image-name:<name>][image-id:<id>]/<path to local directory><br><br>• [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory><br><br>• [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory><br><br>您可以在名称和标识符中使用掩码（? 和 * 字符）。<br><br>您可以用 *（星号）字符来创建文件或目录名称掩码。<br><br>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。<br><br>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**/。<br><br>** 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| | | 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。<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） |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| Path | 包含要排除的对象的目录的路径。 | < 本地目录路径 > – 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><br>您可以使用特殊标签来指定容器或镜像：<br><br>• [container-id:<id>]/<path to local directory><br><br>• [container-name:<name>]/<path to local directory><br><br>• [image-id:<id>]/<path to local directory><br><br>• [image-name:<name>]/<path to local directory><br><br>其中：<br><br><id> 是容器 ID。<br><br><name> 是容器名称<br><br><path to local directory> 是本地目录的路径。<br><br>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>。<br><br>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。<br><br>例如：<br><br>• [container-name:<name>][image-name:<name>]/path to local directory><br><br>• [container-id:<id>][image-name:<name>]/<path to local directory><br><br>• [image-name:<name>][image-id:<id>]/<path to local directory><br><br>• [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory><br><br>• [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory><br><br>您可以在名称和标识符中使用掩码（? 和 * 字符）。<br><br>您可以用 *（星号）字符来创建文件或目录名称掩码。<br><br>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。<br><br>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**/。<br><br>** 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| | | 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。<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><文件系统类型> — 从扫描中排除指定设备文件系统的所有资源。 |
| **[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。 | < 进程的完整路径 > – 不扫描指定本地目录中的进程。 |
| `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） |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| Path | 包含由进程修改的文件的目录的路径。 | < 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。<br>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。<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。 |

# 优化网络目录扫描

要优化“文件威胁防护”任务，您可以从扫描中排除从网络目录复制到本地目录中的任何文件。为此，请根据用于从网络目录复制的实用程序（例如 cp 实用程序）的进程配置排除项。

*要配置从扫描中排除网络目录：*

1. 使用以下命令将“文件威胁防护”任务设置（File Threat Protection，ID：1）*输出*到配置文件：

   `kesl-control --get-settings 1 --file <配置文件的完整路径> [--json]`

2. 打开配置文件并添加 [ExcludedForProgram.item_#] 部分，设置如下：

   - ProgramPath – 要排除的进程或包含要排除的进程的目录的路径。
   - ApplyToDescendants 参数指示扫描是否应该排除已排除进程的子进程（可能的值：Yes 或 No）。
   - AreaDesc – 进程排除范围的说明，其中包含有关扫描排除范围的其他信息。
   - UseExcludedForProgram 允许在任务运行期间排除指定范围（可能的值：Yes 或 No）。

- `Path` – 文件或包含进程修改的文件的目录的路径。
- `AreaMask.item_#` 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。

例如：

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/cp
ApplyToDescendants=No
AreaDesc=
UseExcludedForProgram=Yes
Path=AllRemoteMounted
AreaMask.item_0000=*
```

3. 请执行命令：

   `kesl-control --set-settings 1 --file <配置文件的完整路径> [--json]`

   如果要以 JSON 格式从配置文件导入设置，请指定 `--json` 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。

# 扫描符号链接和硬链接的特殊注意事项

Kaspersky Endpoint Security 可以扫描文件符号链接和硬链接。

## 扫描符号链接

仅当由符号链接引用的文件在文件威胁防护组件的扫描范围内时，应用程序才会扫描符号链接。

如果符号链接引用的文件不在文件威胁防护组件的扫描范围内，则应用程序不会扫描此文件。但是，如果文件包含恶意代码，则设备的安全性将受到威胁。

## 扫描硬链接

当处理具有多个硬链接的文件时，应用程序会对原始文件进行清除。如果清除失败，则应用程序将删除该硬链接并使用已删除硬链接的名称在其原位置创建原始文件的副本。删除时，应用程序会删除正在被处理的硬链接，但不会处理指向该文件的其他硬链接。

从备份存储中恢复带有硬链接的文件时，应用程序将使用已被移动到备份存储中的硬链接的名称创建源文件的副本。将不会恢复与源文件其他硬链接的连接。

# 恶意软件扫描

*恶意软件扫描*是根据需要对设备上的文件执行一次性全盘扫描或自定义扫描。Kaspersky Endpoint Security 可以同时执行多个“恶意软件扫描”任务。

在应用程序中创建“*恶意软件扫描 (Scan_My_Computer)*”预定义任务。您可以使用此任务对设备执行全盘扫描。在全盘扫描期间，应用程序会使用推荐的安全设置扫描位于设备本地驱动器上的所有对象，以及通过 Samba 或 NFS 协议访问的所有已挂载和共享的对象。

如果 root 用户没有权限访问通过 NFSv4 协议挂载到设备上的远程目录，应用程序将阻止所有用户访问此类文件。

在 Kaspersky Security Center 中，安装管理 MMC 插件或 Kaspersky Endpoint Security 管理 Web 插件后，Kaspersky Security Center 初始设置向导会自动创建“恶意软件扫描”组任务。

在全盘扫描期间，处理器处于忙碌状态。建议业务闲时运行全盘扫描任务。

您可以在 Kaspersky Security Center 和命令行上配置自动创建任务的设置，还可以创建“恶意软件扫描”用户任务。

检测到恶意软件后，Kaspersky Endpoint Security 可能会移除受感染的文件并终止从该文件启动的恶意软件进程。

如果在执行恶意软件扫描任务期间，应用程序被控制服务或用户手动重新启动，任务将被停止。应用程序会记录 *OnDemandTaskInterrupted* 事件。

您可以运行“恶意软件扫描”任务并配置扫描设置：

- 选择要扫描的操作系统对象：文件、压缩文件、引导扇区、进程内存和内核内存、启动对象。
- 限制要扫描的对象的大小以及对象扫描的持续时间。
- 选择应用程序将对感染对象执行的操作。
- 配置从扫描范围中排除的对象：
  - 按名称或掩码进行排除
  - 按对象中检测到的威胁名称进行排除

  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。
- 扫描时启用或禁用全局排除和文件威胁防护排除。
- 启用有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息记录。
- 配置扫描期间启发式分析器和 iChecker 技术的使用。

- 限制需要扫描其引导扇区的设备集。
- 配置扫描范围和扫描排除范围。

# Web Console 中的恶意软件扫描

在 Web Console 中，您可以使用“*恶意软件扫描*”任务来扫描恶意软件。

您可以运行自动创建的组任务进行扫描，也可以创建并运行用户任务以进行扫描。您可以通过编辑“恶意软件扫描”任务的设置来配置扫描设置。

恶意软件扫描任务设置

| 设置 | 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。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，您可以减少扫描压缩文件的时间。<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。 |
| **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。 |

| 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** | 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。 |
| **扫描范围** | 包含任务扫描的范围的表。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。<br>您可以在表中"添加"、"修改"、"删除"、"上移"或"下移"扫描范围。<br>您还可以点击"**导入**"从文件中导入扫描范围列表，或点击"**导出**"将扫描范围列表以 JSON 格式导出到文件。导入时，系统会提示您替换扫描范围列表或将扫描范围添加到现有列表中。 |

# "添加扫描范围"窗口

在此窗口中，您可以添加和配置扫描范围。

扫描范围设置

| 设置 | 描述 |
| --- | --- |
| **范围名称** | 用于输入扫描范围名称的字段。此名称将显示在"**扫描设置**"部分的**扫描范围**表格中。<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** | 您可以在该下拉列表中选择文件系统的类型：<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。 |
| **访问协议** | 您可以在该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。<br>如果在文件系统下拉列表中选择**共享**或**挂载**类型，则此下拉列表可用。 |

| 设置 | 描述 |
| --- | --- |
| **Path** | 这是用于指定要包括在扫描范围中的目录路径的输入字段。您可以使用**掩码**和**标签**指定路径。<br>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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，则此字段可用。<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。 |
| **共享资源的名称** | 用于输入要添加到扫描范围中的目录所在的文件系统共享资源名称的字段。<br>如果在文件系统下拉列表中选择了**挂载**类型，并且在"**访问协议**"下拉列表中选择了"**自定义**"项，则该字段可用。 |
| **掩码** | 该列表包含应用程序扫描的对象的名称掩码。<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。 |

# "扫描范围"部分

您可以为恶意软件扫描任务配置扫描范围设置。应用程序允许您扫描文件、引导扇区、客户端设备内存和启动对象。

恶意软件扫描范围任务设置

| 设置 | 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客户端设备内存扫描。<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** | 单击“**配置设备掩码**”链接将打开“**扫描范围**”窗口，您可以在其中指定必须扫描其引导扇区的设备。 |

# “扫描范围”窗口

该表包含应用程序必须扫描其引导扇区的设备的名称掩码。默认情况下，该表包含 **/**** 设备名称掩码（所有设备）。

您可以在表中添加、编辑和删除项目。

# “排除范围”部分

在恶意软件扫描任务的**排除范围**部分，您可以配置排除范围、按掩码和威胁名称排除，以及在任务运行时全局排除和文件威胁防护排除的使用。

扫描排除项设置

| 设置 | 描述 |
| --- | --- |
| **配置排除范围** | 单击“**配置排除范围**”链接将打开“**排除范围**”窗口。在此窗口中，您可以定义扫描排除项列表。 |
| **按掩码配置排除项** | 单击“**按掩码配置排除项**”链接将打开“**按掩码筛选的排除项**”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。 |
| **按威胁名称配置排除项** | 单击“**按威胁名称配置排除项**”链接将打开“**按威胁名称筛选的排除项**”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。 |
| **使用全局排除项** | 该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。<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。 |

# “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 |
| --- | --- |
| **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。

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。

# “添加排除范围”窗口

在此窗口中，您可以添加和配置排除范围。

排除范围设置

| 设置 | 描述 |
| --- | --- |
| **排除范围名称** | 用于输入排除范围名称的字段。此名称将显示在**排除范围**窗口的表格中。<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排除范围。<br>如果选中该复选框，则应用程序会在其运行期间将此范围排除在扫描或保护之外。<br>如果清除该复选框，则应用程序在其运行期间将此范围包括在扫描或保护中。您可以在以后选中此复选框来从扫描或保护中排除此范围。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 在此下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型：<br>• “**本地**”，表示本地目录。<br>• **挂载**，表示设备上挂载的远程目录。<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。 |
| **访问协议** | 您可以在该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。<br>如果在文件系统下拉列表中选择**挂载**类型，则此下拉列表可用。 |

| 设置 | 描述 |
| --- | --- |
| **Path** | 要添加到排除范围的目录路径的输入字段。您可以使用**掩码**和**标签**指定路径。<br>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。<br>掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。<br>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。<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>如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。 |
| **共享资源的名称** | 用于输入要添加到排除范围中的目录所在的文件系统共享资源名称的字段。<br>如果在文件系统下拉列表中选择了**挂载**类型，并且在"**访问协议**"下拉列表中选择了"**自定义**"项，则该字段可用。 |
| **掩码** | 该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在**路径**字段中指定的目录内的对象。<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。 |

# "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**”或“**编辑**”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。

## “按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**添加**”或“**编辑**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

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。

# 管理控制台中的恶意软件扫描

在管理控制台中，您可以使用“*恶意软件扫描*”任务扫描恶意软件。

您可以运行自动创建的组任务进行扫描，也可以创建并运行用户任务以进行扫描。您可以通过编辑“恶意软件扫描”任务的设置来配置扫描设置。

在恶意软件扫描任务属性的**设置**部分中，您可以配置下表列出的设置。

恶意软件扫描任务设置

| 设置 | 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“**排除项**”部分中，您可以在恶意软件扫描任务的属性中配置排除范围，以及按掩码和威胁名称筛选的排除项。

# “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 |
| --- | --- |
| **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** | 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>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>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。<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。 |

# “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。 |
| **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。

| 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。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，您可以减少扫描压缩文件的时间。<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。 |
| **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：

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 |
| --- | --- |
| **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>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。<br>掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。<br>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。<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。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |

# “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。

# 命令行中的恶意软件扫描

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运行计划。您可以通过编辑该任务的设置来配置扫描设置。
- 使用“恶意软件扫描”用户任务（*ODS* 类型的任务）。您可以手动启动、停止、暂停或恢复用户任务，并配置任务计划。

使用 `kesl-control --scan-file` 命令，您可以对指定的文件和目录执行*自定义扫描*。

# 恶意软件扫描预定义任务的设置

该表介绍了可为恶意软件扫描任务指定的所有设置的全部可能值以及默认值。

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。 |
| 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。 |
| 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>例如：<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>例如：<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。 |
| 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>< 设备名称掩码 > – 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>例如：<br>AreaDesc=" 邮件库扫描 " |
| 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>例如：<br>AreaMask.item_< 项目编号 >=*doc |
| 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>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）。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。<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。 |

# 在命令行上自定义扫描文件和目录

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。

使用 *Scan_File* 预定义任务（ID：3）中存储的设置执行自定义扫描。您可以通过编辑该任务的设置来配置文件自定义扫描的设置（见下表）。

*如要启动对指定文件和目录的自定义扫描，请执行以下命令：*

```
kesl-control --scan-file <路径> [--action <操作>]
```

其中：

- < 路径 > 是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` < 操作 > 是应用程序将对感染对象执行的操作。可能的值：`DisinfectDeleteIfNotPossible`, `DisinfectInformIfNotPossible`,`Inform`。如果未指定 `--action` 选项，应用程序将执行 `DisinfectDeleteIfNotPossible` 操作。

执行该命令后，会创建一个临时的文件扫描任务，完成后自动删除。在这种情况下，扫描结果将输出到控制台。

该表介绍了可为 *Scan_File* 任务指定的所有设置的全部可能值以及默认值。

> 执行自定义扫描时，不考虑在 *Scan_File* 任务中定义的 `[ScanScope.item_#]` 和 `[ExcludedFromScanScope.item_#]` 部分。

Scan_File 任务设置

| 设置 | 描述 | 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。 |

| 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。 | 默认值为未定义。<br>例如：<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>例如：<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>< 设备名称掩码 > – 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>例如：<br>AreaDesc=" 扫描电子邮件数据库 " |
| 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>例如：<br>AreaMask.item_< 项目编号 >=*doc |
| 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>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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。<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。 |

# 关键区域扫描

执行关键区域扫描时，Kaspersky Endpoint Security 可以扫描引导扇区、启动对象、进程内存和内核内存。

检测到恶意软件后，该应用程序可能会删除受感染的文件并终止从该文件启动的恶意软件进程。

如果 root 用户没有权限访问通过 NFSv4 协议挂载到设备上的远程目录，应用程序将阻止所有用户访问此类文件。

您可以启动关键区域扫描并配置扫描的设置：

- 选择要扫描的操作系统对象。默认启用对引导扇区、进程内存和内核内存、启动对象和压缩文件的扫描。默认情况下，关键区域扫描期间不会扫描文件。
- 限制要扫描的对象的大小以及对象扫描的持续时间。
- 选择应用程序将对感染对象执行的操作。
- 配置从扫描范围中排除的对象：
  - 按名称或掩码进行排除
  - 按对象中检测到的威胁名称进行排除

  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。
- 扫描时启用或禁用全局排除和文件威胁防护排除。
- 启用有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息记录。
- 配置扫描期间启发式分析器和 iChecker 技术的使用。
- 限制需要扫描其引导扇区的设备集。
- 配置扫描范围和扫描排除范围。

# Web Console 中的关键区域扫描

在 Web Console 中，您可以使用“*关键区域扫描*”任务对受保护设备的操作系统执行关键区域扫描。

您可以创建并运行关键区域扫描用户任务。您可以通过编辑任务的设置来配置扫描设置。

| 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。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，您可以减少扫描压缩文件的时间。<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。 |
| **通知未处理的文件** | 此复选框的功能是：在扫描期间无法处理文件时，启用或禁用 *ObjectNotProcessed* 类型事件的记录。<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。 |

| 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。 |
| **扫描范围** | 包含任务扫描的范围的表。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。<br>您可以在表中"添加"、"修改"、"删除"、"上移"或"下移"扫描范围。<br>您还可以点击"**导入**"从文件中导入扫描范围列表，或点击"**导出**"将扫描范围列表以 JSON 格式导出到文件。导入时，系统会提示您替换扫描范围列表或将扫描范围添加到现有列表中。 |

# "添加扫描范围"窗口

在此窗口中，您可以添加和配置扫描范围。

扫描范围设置

| 设置 | 描述 |
| --- | --- |
| **范围名称** | 用于输入扫描范围名称的字段。此名称将显示在"**扫描设置**"部分的**扫描范围**表格中。<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** | 您可以在该下拉列表中选择文件系统的类型：<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。 |
| **访问协议** | 您可以在该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。<br>如果在文件系统下拉列表中选择**共享**或**挂载**类型，则此下拉列表可用。 |

| 设置 | 描述 |
| --- | --- |
| **Path** | 这是用于指定要包括在扫描范围中的目录路径的输入字段。您可以使用**掩码**和**标签**指定路径。<br><br>您可以使用特殊标签来指定容器或镜像：<br><br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br><br>其中：<br><br>`<id>` 是容器 ID。<br><br>`<name>` 是容器名称<br><br>`<path to local directory>` 是本地目录的路径。<br><br>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>`。<br><br>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。<br><br>例如：<br><br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br><br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br><br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br><br>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`。<br><br>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**/`。<br><br>`**` 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。<br><br>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。<br><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，则此字段可用。<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。 |
| **共享资源的名称** | 用于输入要添加到扫描范围中的目录所在的文件系统共享资源名称的字段。<br>如果在文件系统下拉列表中选择了**挂载**类型，并且在"**访问协议**"下拉列表中选择了"**自定义**"项，则该字段可用。 |
| **掩码** | 该列表包含应用程序扫描的对象的名称掩码。<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。 |

# “扫描范围”部分

关键区域扫描任务的扫描范围设置

| 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客户端设备内存扫描。<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>默认情况下已选定该选框。 |
| **要扫描的设备** | 单击“**配置设备掩码**”链接将打开“**扫描范围**”窗口，您可以在其中指定必须扫描其引导扇区的设备。 |

# “扫描范围”窗口

该表包含应用程序必须扫描其引导扇区的设备的名称掩码。默认情况下，该表包含 **/**** 设备名称掩码（所有设备）。

您可以在表中添加、编辑和删除项目。

# “排除范围”部分

在关键区域扫描任务的**排除范围**部分，您可以配置排除范围、按掩码排除和按威胁名称排除，以及在任务运行时全局排除和文件威胁防护排除的使用。

扫描排除项设置

| 设置 | 描述 |
| --- | --- |
| **配置排除范围** | 单击“**配置排除范围**”链接将打开“**排除范围**”窗口。在此窗口中，您可以定义扫描排除项列表。 |
| **按掩码配置排除项** | 单击“**按掩码配置排除项**”链接将打开“**按掩码筛选的排除项**”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。 |
| **按威胁名称配置排除项** | 单击“**按威胁名称配置排除项**”链接将打开“**按威胁名称筛选的排除项**”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。 |
| **使用全局排除项** | 该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。<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。 |

# “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 |
| --- | --- |
| **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。

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。

# “添加排除范围”窗口

在此窗口中，您可以添加和配置排除范围。

排除范围设置

| 设置 | 描述 |
| --- | --- |
| **排除范围名称** | 用于输入排除范围名称的字段。此名称将显示在**排除范围**窗口的表格中。<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排除范围。<br>如果选中该复选框，则应用程序会在其运行期间将此范围排除在扫描或保护之外。<br>如果清除该复选框，则应用程序在其运行期间将此范围包括在扫描或保护中。您可以在以后选中此复选框来从扫描或保护中排除此范围。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 在此下拉列表中，您可以选择要添加到扫描排除项的目录所在的文件系统类型：<br>• “**本地**”，表示本地目录。<br>• **挂载**，表示设备上挂载的远程目录。<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。 |
| **访问协议** | 您可以在该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。<br>如果在文件系统下拉列表中选择**挂载**类型，则此下拉列表可用。 |

| 设置 | 描述 |
| --- | --- |
| **Path** | 要添加到排除范围的目录路径的输入字段。您可以使用**掩码**和**标签**指定路径。<br>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。<br>掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。<br>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。<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>如果在文件系统下拉列表中选择**本地**类型选项，则此字段可用。 |
| **共享资源的名称** | 用于输入要添加到排除范围中的目录所在的文件系统共享资源名称的字段。<br>如果在文件系统下拉列表中选择了**挂载**类型，并且在"**访问协议**"下拉列表中选择了"**自定义**"项，则该字段可用。 |
| **掩码** | 该列表包含应用程序从扫描中排除的对象的名称掩码。掩码仅应用于在**路径**字段中指定的目录内的对象。<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。 |

# "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**”或“**编辑**”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。

## “按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**添加**”或“**编辑**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

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。

# 管理控制台中的关键区域扫描

在管理控制台中，您可以使用“*关键区域扫描*”任务对受保护设备的操作系统执行关键区域扫描。

您可以创建并运行关键区域扫描用户任务。您可以通过编辑任务的设置来配置扫描设置。

在关键区域扫描任务属性的“**设置**”部分中，您可以配置下表列出的设置。

关键区域扫描任务设置

| 设置 | 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属性的**排除项**部分中，您还可以按掩码和威胁名称配置排除范围或排除项。

# “扫描范围”窗口

该表包含扫描范围：应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个扫描范围，其中包括本地文件系统的所有目录。

扫描范围设置

| 设置 | 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** | 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>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>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。<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。 |

# “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。

| 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。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，您可以减少扫描压缩文件的时间。<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。 |
| **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：

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 |
| --- | --- |
| **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>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。<br>掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。<br>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。<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。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |

# “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。

# 命令行中的关键区域扫描

在命令行中，您可以使用“关键区域扫描”预定义任务 (*Critical_Areas_Scan*) 对受保护设备的操作系统执行关键区域扫描。

您可以手动启动、停止、暂停或恢复此任务并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。

关键区域扫描任务设置

| 设置 | 描述 | 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |
| 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。 |
| 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>例如：<br>UseExcludeMasks=Yes<br>ExcludeMasks.item_0000=eicar1.*<br>ExcludeMasks.item_0001=eicar2.* |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>例如：<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。 |
| 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>< 设备名称掩码 > – 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>例如：<br>AreaDesc=" 邮件库扫描 " |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>例如：<br>AreaMask.item_< 项目编号 >=*doc |
| 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>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）。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。<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。 |

# 可移动驱动器扫描

Kaspersky Endpoint Security 会对以下连接到受保护设备的可移动驱动器进行扫描：CD、DVD、蓝光光盘、闪存驱动器（包括 USB 调制解调器），外部硬盘驱动器和软盘。

如果启用了可移动驱动器扫描，Kaspersky Endpoint Security 会监控可移动驱动器与受保护设备之间的连接，如果检测到已连接的可移动驱动器，它会扫描该驱动器及其引导扇区是否存在病毒和其他恶意软件。

默认情况下，应用程序不会监控可移动驱动器的连接或对其进行扫描。

# 在 Web Console 中配置可移动驱动器扫描

在 Web Console 中，您可以在策略属性（**应用程序设置 → 主机威胁防护 → 可移动驱动器扫描**）中管理可移动驱动器扫描设置。

# 在管理控制台中配置可移动驱动器扫描

在管理控制台中，您可以在策略属性（在管理控制台中管理策略、使用管理控制台创建策略）（**本地任务 → 可移动驱动器扫描**）中管理可移动驱动器扫描设置。

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（不包括 CD/DVD 驱动器和蓝光光盘）上的**特定类型**的文件，不解压复合对象。快速扫描使用"*关键区域扫描*"任务的默认设置执行。<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>• **详细扫描** — 扫描可移动驱动器（不包括 CD/DVD 驱动器和蓝光光盘）上的所有文件。详细扫描使用"*恶意软件扫描*"任务的默认设置执行。 |
| **连接 CD / DVD 驱动器时的操作** | 在下拉列表中，您可以选择应用程序将 CD/DVD 驱动器和蓝光驱动器连接到用户设备时要执行的操作：<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**的文件。快速扫描使用"*关键区域扫描*"任务的默认设置执行。<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>• **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。 |

# 在命令行中配置可移动驱动器扫描

在命令行上，您可以使用“*可移动驱动器扫描*”预定义任务 (*Removable_Drives_Scan*) 管理可移动媒介扫描。

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*默认*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。 |
| `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*默认*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

您可以实时、按需扫描容器和镜像中是否存在恶意软件：

- *容器监控组件（容器扫描、容器监控）*允许实时扫描正在启动的容器和命名空间。
- 您可以使用“*容器扫描*”任务按需扫描容器和镜像。

要使用“容器扫描”功能，需要包含此功能的授权许可。

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。

支持与 Docker 28.5.2 及更早版本集成。

# 容器监控

容器监控组件默认处于启用状态。该应用程序实时扫描正在运行的容器和命名空间。

为了使容器监控组件正常工作，必须启用文件威胁防护组件。扫描容器和命名空间时应用文件威胁防护设置。

除非操作系统中安装了用于使用容器和命名空间的组件，否则应用程序不会扫描命名空间和容器。在这种情况下，命令行中“容器监控”的组件状态显示为 任务可用但未运行，而在 Kaspersky Security Center 中则显示为“已停止”。

您可以启用或禁用容器监控组件，还可以配置实时扫描容器和命名空间的设置：

- 选择应用程序在检测到受感染对象时对容器执行的操作。

  在支持此功能的授权许可下使用应用程序时，此设置可用。

- 配置 Kaspersky Endpoint Security 与 Docker 容器管理系统、CRI-O 框架以及 Podman 和 runc 实用程序的整合。

  支持与 Docker 28.5.2 及更早版本集成。

# 在 Web Console 中配置容器监控

在 Web Console 中，您可以在策略属性中管理容器扫描设置组件（**应用程序设置 → 常规设置 → 容器扫描设置**）。

# 在管理控制台中配置容器监控

在管理控制台中，您可以在策略属性中管理应用程序跟踪设置（在管理控制台中管理策略、使用管理控制台创建策略）（**常规设置 → 容器扫描设置**）。

容器监控设置

| 设置 | 描述 |
| --- | --- |
| **启用命名空间和容器扫描** | 此复选框可启用或禁用命名空间和容器的实时扫描。<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。<br>支持 Docker 28.5.2 及更早版本。 |
| **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。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |

# 在命令行中配置容器监控

在命令行中，您可以使用常规应用程序设置中的 `NamespaceMonitoring=Yes/No` 设置启用或禁用对命名空间和容器的实时扫描。

您可以使用包含所有常规应用程序设置的配置文件或使用命令行选项来编辑设置 `NamespaceMonitoring` 的值。

实时扫描命名空间和容器时，使用常规容器扫描设置。您可以使用 Kaspersky Endpoint Security 的特殊管理命令来查看和编辑这些设置：

- 您可以将常规“容器扫描”设置的当前值输出到控制台或配置文件。您可以使用此文件来编辑设置。
- 您可以使用包含设置的配置文件来编辑所有常规“容器扫描”设置。您可以使用显示常规“容器扫描”设置的命令来获取配置文件。
- 您可以使用命令行选项，以 < 设置名称 >=< 设置值 > 格式编辑单个设置。您可以使用显示常规“容器扫描”设置的命令获取设置的当前值。

*要将常规“容器扫描”设置的当前值输出到控制台，请执行以下命令：*

```
kesl-control --get-container-settings [--json]
```

其中指定 `--json` ，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。

*要将常规“容器扫描”设置的当前值输出到文件，请执行以下命令：*

```
kesl-control --get-container-settings --file <配置文件路径> [--json]
```

其中：

- `--file` <配置文件路径> 是将保存常规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。

*要使用配置文件编辑常规"容器扫描"设置的值：*

1. 将常规"容器扫描"设置输出到配置文件，如上所述。
2. 编辑文件中必要参数的值并保存更改。
3. 请执行命令：

   `kesl-control --set-container-settings --file <配置文件路径> [--json]`

   其中：

   - `--file <配置文件路径>` 是包含常规容器扫描设置的配置文件的完整路径。
   - 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。

文件中定义的所有常规"容器扫描"设置的值都将导入应用程序。

*要使用命令行选项编辑常规"容器扫描"设置的值，请执行以下命令：*

`kesl-control --set-container-settings <设置名称>=<设置值> [<设置名称>=<设置值>]`

其中 `<设置名称>=<设置值>` 是常规容器扫描设置之一的名称和值。

指定的常规"容器扫描"设置的值将被更改。

# 按需扫描容器和镜像

运行"*容器扫描*"任务时，Kaspersky Endpoint Security 会扫描容器和镜像中是否存在病毒和其他恶意软件。应用程序可以同时运行多个"容器扫描"任务。

使用此功能需要涵盖容器扫描任务的授权许可。

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。

支持与 Docker 28.5.2 及更早版本集成。

您可以启动容器扫描并配置扫描的设置：

- 按名称或名称掩码指定要扫描的容器和镜像。
- 启用扫描所有镜像层和容器。
- 选择应用程序将对容器执行的操作以及当检测到受感染对象时应用程序将对镜像执行的操作。

- 配置扫描容器或镜像内对象的设置：
  - 启用或禁用对压缩文件、邮件数据库、文本格式的电子邮件消息的扫描。
  - 限制要扫描的对象的大小以及对象扫描的持续时间。
  - 选择应用程序将对感染对象执行的操作。
  - 配置从扫描范围中排除的对象：
    - 按名称或掩码进行排除
    - 按对象中检测到的威胁名称进行排除
  - 扫描时启用或禁用全局排除。
  - 配置扫描期间启发式分析器和 iChecker 技术的使用。
  - 启用或禁用对有关扫描的未感染对象、压缩文件中的扫描对象以及未处理的对象的信息进行记录。

# Web Console 中的容器扫描

在 Web Console 中，您可以使用*容器扫描*任务来扫描容器和镜像。

您可以创建并运行"容器扫描"用户任务。您可以通过编辑任务的设置来配置扫描设置。

容器扫描任务设置

| 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。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，您可以减少扫描压缩文件的时间。<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。 |

| 设置 | 描述 |
| --- | --- |
| **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** | 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。 |
| **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** | 您可以选择应用程序在检测到受感染对象时对容器执行的操作：<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><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）。 |

| 设置 | 描述 |
| --- | --- |
| **检测到威胁后的操作** | 您可以选择应用程序在检测到受感染对象时对容器执行的操作：<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。 |

## “排除范围”部分

在容器扫描任务的**排除范围**部分，您可以按掩码和按威胁名称配置排除项，以及在任务运行时使用全局排除。

扫描排除项设置

| 设置 | 描述 |
| --- | --- |
| **按掩码配置排除项** | 单击“**按掩码配置排除项**”链接将打开“**按掩码筛选的排除项**”窗口。在此窗口中，您可以配置按名称掩码在扫描中排除对象的设置。 |
| **按威胁名称配置排除项** | 单击“**按威胁名称配置排除项**”链接将打开“**按威胁名称筛选的排除项**”窗口。在此窗口中，您可以根据威胁名称配置在扫描中排除对象。 |
| **使用全局排除项** | 该复选框可启用或禁用在应用程序运行时排除全局例外中指定的挂载点。<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**”或“**编辑**”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。

## “按威胁名称筛选的排除项”窗口

您可以根据威胁名称配置从扫描中排除的对象。应用程序不会阻止指定的威胁。默认情况下，威胁名称列表为空。

您可以添加、编辑和删除威胁名称。

单击“**添加**”或“**编辑**”按钮将打开“**威胁名称**”窗口。在此窗口中，您可以定义要从扫描中排除的威胁的名称。

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。

# 管理控制台中的容器扫描

在管理控制台中，您可以使用“*容器扫描*”任务扫描容器和镜像。

您可以创建并运行“容器扫描”用户任务。您可以通过编辑任务的设置来配置扫描设置。

在容器扫描任务属性的**设置**部分中，您可以配置下表列出的设置。

容器扫描任务设置

| 设置 | 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**排除项**部分的任务属性中，您还可以按掩码和按威胁名称为容器扫描任务配置排除项。

## “容器扫描设置”窗口

在此窗口中，您可以配置容器和映像扫描设置。

容器和映像扫描设置

| 设置 | 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）。 |

| 设置 | 描述 |
| --- | --- |
| **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。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，您可以减少扫描压缩文件的时间。<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。 |
| **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。 |

| 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：

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）。

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。

# 命令行中的容器扫描

在命令行上，您可以通过以下方式扫描容器和镜像：

- 使用“容器扫描”预定义任务 (*Container_Scan*)。您可以手动启动或停止该任务，并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。
- 使用“容器扫描”用户任务（*ContainerScan* 类型的任务）。您可以手动启动和停止用户任务，并配置任务运行计划。
- 使用 `kesl-control --scan-container` 命令，您可以对指定的容器和镜像执行*自定义扫描*。

# 容器扫描任务设置

该表描述了所有容器和镜像扫描设置的全部可用值以及默认值。

容器扫描任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `ScanContainers` | 扫描按掩码指定的容器。您可以使用 `ContainerNameMask` 设置指定掩码。 | `Yes`（默认值）— 扫描由掩码定义的容器。<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>例如：<br>扫描具有 my_container 名称的容器：<br>`ContainerNameMask=my_container`<br>扫描名称以 my_container 开头的所有容器：<br>`ContainerNameMask=my_container*`<br>扫描所有符合这些条件的容器：名称以 my_ 开头，后接任意五个字符、再接 _container，最后以任意字符序列结尾：<br>`ContainerNameMask=my_?????_container*` |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>例如：<br>扫描带有"my_image"名称和"latest"标签的镜像：<br>ImageNameMask=my_image:latest<br>扫描名称以 my_image_ 开头且带有任何标签的所有镜像：<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。 |
| 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。 |

| 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。 |
| 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>例如：<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>例如：<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。 |

| 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。 |

# 自定义扫描容器和镜像

您可以使用 kesl-control --scan-container 命令对指定的容器和镜像执行自定义扫描。

使用预定义任务“*Custom_Container_Scan*”（ID：19）中存储的设置执行自定义扫描。您可以通过编辑此任务的设置来配置“自定义容器扫描”设置。默认情况下，*Custom_Container_Scan*任务的设置与*Container_Scan*任务（ID:18）相同。

*要启动“自定义容器扫描”任务，请执行以下命令：*

```
kesl-control --scan-container <ID/名称 [:标签 ]>
```

其中 <ID/名称 [:标签 ]> 是容器或镜像的名称或 ID。您可以使用**掩码**来扫描多个对象。

您可以用 *（星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如，/dir/*/file 或 /dir/*/*/file。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如，/dir/**/file*/ 或 /dir/file**/。

** 掩码在目录名称中只能使用一次。例如，/dir/**/**/file 是不正确的掩码。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

如果有多个具有相同名称的实体，应用程序将扫描所有实体。

执行该命令后，会创建一个临时的容器和镜像扫描任务，完成后会自动删除。在这种情况下，扫描结果将输出到控制台。

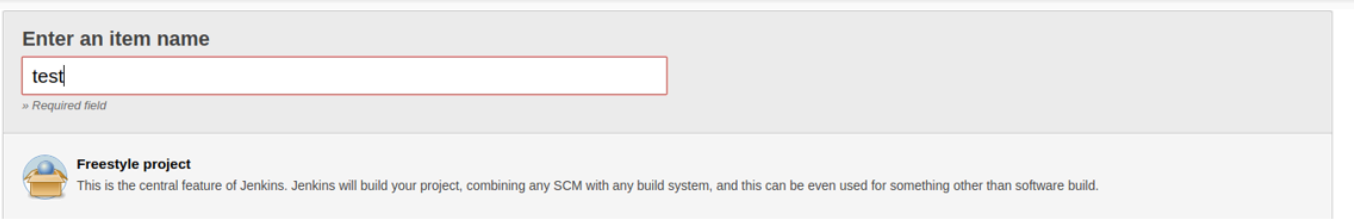
例如：
扫描名为 my_container 的容器：
```
kesl-control --scan-container my_container
```
扫描名为 my_image 的镜像（所有标签）：
```
kesl-control --scan-container my_image*
```

# 与 Jenkins 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。

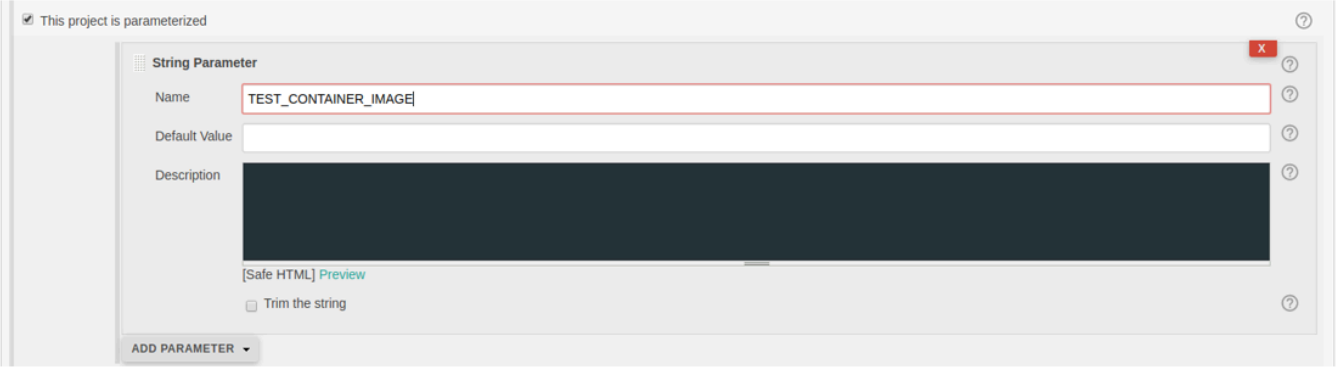
*要将 Kaspersky Endpoint Security 与 Jenkins 集成：*

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 <用户名 Jenkins>`
4. 将 Jenkins 用户添加到 docker 组：
   `sudo usermod -aG docker <用户名 Jenkins>`
   通常使用 jenkins 这一名称。
5. 在 Jenkins 中，创建一个名为 `test` 的新构建作业（**新建项目** → **输入项目名称**）。




6. 根据您的需求配置您的项目。假设结果是，您有一个映像或一个已启动的容器需要扫描。
7. 要启动 Docker 容器，请将以下脚本添加到 Jenkins 构建过程中。如果您使用 Jenkins 插件或其他方式来启动 Docker 容器，请将运行中的 Docker 容器的 ID 保存到 /tmp/kesl_cs_info 文件中，以便进一步扫描：

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE}
/storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```




8. 构建工件后，在步骤中添加以下脚本以构建 jenkins。

   对于扫描，此脚本支持一个容器。如有必要，请根据您的需求修改脚本。

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. 要从存储库中扫描 Docker 映像，请使用以下脚本：

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
```

```
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container
${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. 保存构建作业。

# 防火墙管理

在局域网 (LAN) 和互联网中使用的设备暴露于病毒、其他恶意软件、以及一系列针对操作系统和软件漏洞的攻击环境中。操作系统防火墙可保护用户设备上存储的数据，当设备连接到互联网或 LAN 时，防火墙可阻止大多数威胁。

操作系统防火墙可以检测用户设备上的所有网络连接，并提供这些网络连接的 IP 地址列表。防火墙管理组件允许您通过配置网络数据包规则来设置网络连接的状态。

您可以使用网络数据包规则指定想要的设备保护级别，例如从完全阻止所有应用程序的互联网访问到允许无限制访问。除非指定了防火墙管理组件的相应阻止规则，否则默认情况下将允许所有出站连接。

默认禁用防火墙管理组件。

> 在启用 Firewall 管理组件之前，禁用其他操作系统防火墙管理工具。

启用防火墙管理组件后，Kaspersky Endpoint Security 将使用操作系统提供的工具自动删除为防火墙配置的所有自定义规则。禁用组件后，这些规则不会恢复。如需要，请在启用防火墙管理组件之前保存自定义防火墙规则。

如果启用了防火墙管理，Kaspersky Endpoint Security 将扫描操作系统防火墙并阻止任何更改防火墙设置的尝试，例如当应用程序或实用程序试图添加或删除防火墙规则时。Kaspersky Endpoint Security 每 60 秒检查一次操作系统防火墙，并在必要时恢复使用应用程序创建的防火墙规则集。检查期间无法更改。

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。

您可以启用或禁用防火墙管理，还可以配置以下设置：

- 配置 Kaspersky Endpoint Security 在检测到建立网络连接的尝试时将应用的网络数据包规则列表。您可以添加或删除网络数据包规则，也可以更改网络数据包规则的执行优先级。

  > 在某些基于 Red Hat Enterprise Linux 代码库的操作系统中，只能使用管理命令 (`kesl-control -F --query`) 查看在 Kaspersky Endpoint Security 应用程序中创建的 Firewall 规则。

- 选择当没有任何其他网络数据包规则适用于此类连接时将对传入连接和数据包执行的默认操作。
- 将网络地址映射到预定义网络。您可以向可用网络添加 IP 地址或子网，也可以从可用网络中删除地址。
- 启用或禁用网络代理端口自动添加允许规则。

# 关于网络数据包规则

*网络数据包规则*是由 Kaspersky Endpoint Security 采取的操作，以允许或拒绝检测到的网络连接尝试。

网络数据包规则将对网络数据包进行限制，与应用程序无关。此类规则将限制通过特定端口的选定数据协议发送和接收的网络流量。

除非指定了防火墙管理的相应阻止规则，否则默认情况下允许所有出站连接（默认操作设置）。默认操作以最低优先级执行：如果未触发其他网络数据包规则，或者未指定任何网络数据包规则，则允许连接。

默认情况下，防火墙管理已指定了某些网络数据包规则。您可以创建自己的网络数据包规则，并为每个网络数据包规则指定执行优先级。

# 关于动态规则

Kaspersky Endpoint Security 允许向防火墙添加或删除*动态规则*，以确保应用程序正常运行。例如，网络代理会添加动态规则，允许由该应用程序或 Kaspersky Security Center 发起的与 Kaspersky Security Center 的连接。“反加密勒索”的规则也是动态的。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security，动态规则会被自动添加到防火墙，以允许连接到 SVM 和 Integration Server。

Kaspersky Endpoint Security 不会控制动态规则，也不会阻止应用程序组件访问网络资源。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。如果删除动态规则组中的任何规则，则应用程序会恢复动态规则组（例如，使用 iptables 实用程序）。

您可以查看动态规则集（使用 `kesl-control -F --query` 命令）；但是不能修改动态规则设置。

# 关于预定义的可用网络

*可用网络*是指一组已定义的 IP 地址或子网。可用网络允许您对多个 IP 地址或子网使用相同的规则，而无需为每个 IP 地址或子网创建单独的规则。创建网络数据包规则时，可用网络可以用作“远程地址”参数的值。Kaspersky Endpoint Security 提供三个预定义的网络：

- **Public**。未受反病毒应用程序、防火墙或过滤器保护的网络（例如网吧网络）。
- **Local**。用户有权访问设备上的文件和打印机的网络（例如企业局域网或家庭网络）。
- **受信任**。其中的设备不会暴露于攻击或未经授权数据访问尝试的安全网络。

您不能创建新的预定义网络或删除现有网络，但可以向网络中添加或删除 IP 地址和子网。

# Web Console 中的防火墙管理

在 Web Console 中，您可以在策略属性中管理Firewall 设置（**应用程序设置** → **通信和 Web 保护** → **防火墙**）。

# 管理控制台中的防火墙管理

在管理控制台中，您可以在策略属性中管理 Firewall 管理设置（在管理控制台中管理策略、使用管理控制台创建策略）（**基本威胁防护** → **Firewall 管理**）。

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 |

| 设置 | 描述 |
| --- | --- |
| 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** |

# 命令行中的防火墙管理

在命令行中，您可以使用“防火墙管理”预定义任务 (*Firewall_Management*) 来配置防火墙管理。

“防火墙管理”任务默认不运行。您可以手动启动和停止该任务。

您可以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。
- 使用命令 `kesl-control -F --query` 查看应用程序中创建的防火墙规则。

防火墙管理任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `DefaultIncomingAction` | 当没有任何网络规则适用于此类连接时，对入站连接执行的默认操作。 | `Allow`（默认值）– 允许入站连接。<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： | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |
| 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 ::。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 | | |
| 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） |

# 在命令行中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 --add-rule [--name <规则名称>] [--action <操作>] [--protocol <协议>] [--direction <方向>] [--remote <远程地址>[:<端口或端口范围>]] [--local <本地地址>[:<端口或端口范围>]] [--at <索引>]
```

其中：

- `--name <规则名称>` 是网络数据包规则的名称。
- `--action <操作>` 是要对网络数据包规则中指定的连接执行的操作。
- `--protocol <协议>` 是您要监控其网络活动的通信协议类型。
- `--direction <方向>` 是受监控网络活动的方向。
- `--remote <远程地址[:<端口或端口范围>]>` 是远程设备的网络地址。您可以将预定义网络区域的名称指定作为远程地址。
- `--local <本地地址[:<端口或端口范围>]>` 是已安装 Kaspersky Endpoint Security 的设备的网络地址。
- `--at <索引>` 是网络数据包规则列表中的规则索引。如果未指定 `--at` 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。

例如：
*要创建规则阻止到 TCP 端口 23 的所有传入和已建立的连接，请执行以下命令：*

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

*要为公共网络区域创建规则以阻止通过 TCP 端口 23 的传入和已建立的连接，请执行以下命令：*

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
Public
```

*要删除网络数据包规则，请执行以下命令之一：*

- `kesl-control --del-rule --name <规则名称>`
- `kesl-control --del-rule --index <索引>`

其中：

- `--name <规则名称>` 是网络数据包规则的名称。
- `--index <索引>` 是网络数据包规则列表中的当前规则索引。

如果网络数据包规则列表包含多个名称相同的规则或者不包含具有指定名称或索引的规则，则会发生错误。

*如要更改网络数据包规则的执行优先级，请执行以下命令之一：*

- `kesl-control --move-rule --name <规则名称> --at <索引>`
- `kesl-control --move-rule --index <索引> --at <索引>`

其中：

- `--name <规则名称>` 是网络数据包规则的名称。
- `--index <索引>`是网络数据包规则列表中的当前规则索引。
- `--at <索引>`是网络数据包规则列表中的新规则索引。

# 在命令行中配置网络区域

*要将网络地址添加到区域，请执行以下命令：*

```
kesl-control --add-zone <区域> --address <地址>
```

其中：

- `<区域>` 是网络区域的预定义名称。可能的值：`Public`、`Local`、`Trusted`。
- `<地址>` 是网络地址或子网。

*如要从区域中删除网络地址，请执行以下命令之一：*

- `kesl-control --del-zone <区域> --address <地址>`
- `kesl-control --del-zone <区域> --index <区域中的地址索引>`

如果一个区域包含多个具有相同网络地址的项目，则将不执行 `--del-zone` 命令。

如果指定的网络地址或索引不存在，则会生成错误消息。

# Web 威胁防护

Web 威胁防护组件允许您扫描通过 HTTP、HTTPS 和 FTP、网站和 IP 地址的入站流量，防止从互联网下载恶意文件，并阻止访问网络钓鱼、广告软件和其他恶意网站。Web 威胁防护使用端口 9879 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。

停止或启动应用程序或 Web 威胁防护保护组件会终止拦截端口（例如 HTTPS）上的连接。

默认情况下，“Web 威胁防护”任务被禁用。但是，如果允许在设备上对“Web 威胁防护”设置进行本地管理（策略未应用或未在策略属性中设置“锁定”），并且在系统中检测到以下可执行浏览器文件之一（包括 snap 格式），则会自动启用该任务：

- chrome
- chromium
- chromium-browser
- firefox
- firefox-esr
- google-chrome
- opera
- yandex-browser

您可以启用或禁用“Web 威胁防护”，还可以配置防护设置：

- 选择应用程序在检测到危险对象的 Web 资源上执行的操作。
- 配置受信任的网址列表。该应用程序不会扫描其网址包含在此列表中的网站的内容。
- 选择应用程序在扫描入站流量时将检测的对象。
- 配置加密连接扫描以扫描 HTTPS 流量。

  要扫描 FTP 流量，必须在网络流量扫描设置中配置对所有网络端口的控制。

打开网站时，应用程序会执行以下操作：

1. 使用下载的应用程序数据库检查网站的安全性。
2. 如果启用，使用**启发式分析**检查网站安全性。

   在启发式分析中，Kaspersky Endpoint Security 将分析应用程序在操作系统中的活动。启发式分析可以检测 Kaspersky Endpoint Security 数据库中当前没有记录的危险对象。

3. 如果启用了卡巴斯基安全网络，则使用卡巴斯基的信誉数据库检查网站的可信任性。

> 建议您启用卡巴斯基安全网络的使用，以帮助“Web 威胁防护”更有效地运行。

4. 阻止或允许打开网站。

当试图打开一个危险的网站时，应用程序会执行以下操作：

- 对于 HTTP 或 FTP 流量，应用程序会阻止访问并显示警告消息。
- 对于 HTTPS 流量，浏览器会显示一个错误页面。

> 删除应用程序证书可能会导致 Web 威胁防护组件无法正常运行。

> 如果您已为 Kaspersky Endpoint Security 配置了流量拦截排除，这些排除会影响 Web 威胁防护。

# 在 Web Console 中配置 Web 威胁防护

在 Web Console 中，您可以在策略属性中管理 Web 威胁防护设置（**应用程序设置** → **通信和 Web 保护** → **Web 威胁防护**）。

# 在管理控制台中配置“Web 威胁防护”

在管理控制台中，您可以在策略属性中管理 Web 威胁防护设置（在管理控制台中管理策略，使用管理控制台创建策略）（**基本威胁防护** → **Web 威胁防护**）。

Web 威胁防护组件设置

| 设置 | 描述 |
| --- | --- |
| **启用 Web 威胁防护** | 此复选框用于启用或禁用 Web 威胁防护。<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。

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。 |

# 在命令行上配置 Web 威胁防护

在命令行中，您可以使用“Web 威胁防护”预定义任务 (*Web_Threat_Protection*) 来管理 Web 威胁防护。

如果在系统中检测到某个受支持的浏览器且在设备上允许本地管理 Web 威胁防护设置（未应用策略或策略未在策略属性中设置“锁定”），则该任务会自动启动。您可以手动启动和停止任务。

您可以通过编辑“Web 威胁防护”预定义任务的设置来配置 Web 威胁防护设置。

Web 威胁防护任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `ActionOnDetect` | 指定在检测到 Web 流量中的受感染对象时要执行的操作。 | `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` | 启用或禁用根据恶意网址数据库检查链接的功能。 | `Yes`（默认值） – 检查链接是否列在恶意链接数据库中。<br>`No` – 不检查链接是否列在恶意链接数据库中。 |
| `CheckPhishing` | 启用或禁用根据网络钓鱼网址数据库检查链接的功能。 | `Yes`（默认值） – 检查链接是否列在网络钓鱼链接数据库中。<br>`No` – 不检查链接是否列在网络钓鱼链接数据库中。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseHeuristicForPhishing | 启用或禁用使用启发式分析来扫描网页中是否存在钓鱼链接。 | Yes（默认值）– 使用启发式分析来检测钓鱼链接。如果指定了此值，则启发式分析的级别是 Light（以最小的系统负载进行最低程度的扫描）。您无法更改 Web 威胁防护任务的启发式分析级别。<br>No – 不使用启发式分析来检测钓鱼链接。 |
| CheckAdware | 启用或禁用根据广告软件网址数据库检查链接的功能。 | Yes – 检查链接是否列在广告软件链接数据库中。<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 | 启用或禁用根据网址（包含入侵者可以用来破坏设备或数据的合法应用程序）数据库扫描链接的功能。 | Yes—检查这些链接是否列入网址（包含可能被入侵者用来破坏您的设备或数据的合法应用程序）数据库。<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。 |
| UseTrustedAddresses | 启用或禁用受信任网址列表。应用程序不会扫描受信任的网址中是否存在病毒或其他恶意对象。您可以使用 TrustedAddresses.item_# 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>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）。<br>不支持使用掩码指定 IP 地址。 |

# 扫描网络流量

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。Web 威胁防护、邮件威胁防护和 Web 控制组件可以解密和检查网络流量。默认启用加密连接扫描。

您可以管理以下网络流量扫描设置：

- 启用或禁用加密连接扫描。
- 选择应用程序在检测到不受信任的证书时要执行的操作。
- 选择网站上发生网络流量扫描错误时要执行的操作。
- 启用或禁用使用互联网进行证书验证。
- 查看和配置受信任域列表。应用程序将不会扫描访问指定域时建立的连接。
- 配置应用程序在执行加密连接扫描时将视为可信的根证书列表。
- 配置流量拦截排除 您可以指定要排除在流量拦截之外的连接。排除的连接由以下参数定义：
  - 流量方向，入站或出站。
  - 远程 IP 地址，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，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）。

  流量拦截排除仅适用于 TCP 连接，不会影响网络数据包规则。流量拦截排除会影响Web 威胁防护、网络威胁防护和Web 控制防护组件。

  您还可以使用操作系统工具为 Kaspersky Endpoint Security 配置流量拦截排除。
- 配置应用程序要监控的网络端口列表。您可以指定要监视的网络端口或网络端口范围。

  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。
- 选择应用程序使用的流量拦截模式。

更改网络流量扫描设置时，应用程序会在日志文件中记录 *NetworkSettingsChanged* 事件。

# 关于网络流量拦截模式

应用程序可以采用两种网络流量拦截模式之一：

- *使用 eBPF*。如果选择此模式，应用程序将使用 eBPF 技术来拦截流量。如果应用程序无法使用 eBPF 技术拦截网络流量，则会改用 iptables 实用程序。
- *使用 iptables*。如果选择此模式，应用程序将使用 iptables 技术来拦截流量。默认情况下已选择此模式。

在 **使用 eBPF** 模式下，应用程序会创建自己的独立网络命名空间（Linux 网络命名空间），并在其中使用与本地网络接口的 `tc`（Linux 流量控制）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。

如果您的设备容易受到网络端口枚举攻击（例如，如果本地设备上配置了带有端口过滤功能的操作系统防火墙），则我们不建议选择**使用 eBPF**模式。我们也不建议在组织网络边界的设备上使用此流量拦截模式。

如果设备位于隔离网段、本地网络或组织网络边界内，则可以选择**使用 eBPF**网络流量拦截模式。

您可以通过 Web Console、管理控制台或命令行来选择网络流量拦截模式。

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。

# 在 Web Console 中配置网络流量扫描

在 Web Console 中，您可以在策略属性中管理网络流量扫描设置（**应用程序设置** → **常规设置** → **网络设置** 以及 **应用程序设置** → **受信任区域**）。

# 在管理控制台中配置网络流量扫描

在管理控制台中，您可以在策略属性中管理网络流量扫描设置（在管理控制台中管理策略，使用管理控制台创建策略）（**安全控制** → **网络设置**）。

| 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。 |
| **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。

# 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。 |

# 在命令行上配置网络流量扫描

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` ，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 <配置文件路径> [--json]
```

其中：

- `--file <配置文件路径>` 是要将网络流量扫描设置保存到的配置文件的路径。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. 请执行命令：

   ```
   kesl-control --set-net-settings --file <配置文件路径> [--json]
   ```

   其中：

   - `--file <配置文件路径>` 是包含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 <设置名称>=<设置值> [<设置名称>=<设置值>]
```

其中 <设置名称>=<设置值> 是其中一项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 <证书路径>
```

其中：

<证书路径>是要添加的证书文件（PEM 或 DER 格式）的路径。

*要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 <证书主题>
```

*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 <远程 IP 地址> --dst-port <目标端口>
```

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。
- `<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>`，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 <远程 IP 地址> --dst-port <目标端口>
```

其中：

- `<in|out>` 是被排除连接中的流量方向。
- < 远程 `IP` 地址 > 是远程设备的 IPv4 或 IPv6 地址，该设备的流量将被排除在拦截范围之外（具体取决于流量方向）。
- < 目标端口 > 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）。

# 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。

如果应用程序使用 eBPF 技术拦截流量，则不会应用 kesl_bypass 规则。

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。

# 网络威胁防护

使用网络威胁防护组件，您可以扫描入站网络流量，查找典型的网络攻击活动。

Kaspersky Endpoint Security 从当前的应用程序数据库中接收 TCP 端口号，并扫描这些端口的传入流量。网络威胁防护使用端口 9789 拦截连接。

为了扫描网络流量，“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。在网络扫描过程中，它可能看起来像是设备上的一个开放端口，即使系统上没有任何应用程序正在侦听此端口。建议通过防火墙关闭未使用的端口。

启用“网络威胁防护”后，拦截的 TCP 端口的当前连接将被重置。

如果启用了网络威胁防护，在检测到受保护设备上的网络攻击尝试时，应用程序将阻止攻击设备的网络活动并创建“*检测到网络攻击*”事件。该事件包含有关攻击设备的信息。默认情况下，来自攻击设备的网络流量会被阻止一小时。一旦阻止时间到期，应用程序就会解除对设备的阻止。

默认情况下，网络威胁防护处于禁用状态。

您可以启用或禁用网络威胁防护，还可以配置防护设置：

- 选择应用程序在检测到属于典型网络攻击的网络活动时执行的操作。
- 此复选框会启用或禁用在检测到网络攻击企图时阻止网络活动。
- 设置阻止攻击设备的持续时间。
- 配置应用程序不会阻止其网络活动的 IP 地址列表。

您可以在命令行中使用管理受阻止设备的命令来查看受阻止的设备列表，并手动解除对这些设备的阻止。除“*检测到网络攻击*”事件外，Kaspersky Security Center 不提供用于监控和管理被阻止设备的工具。

如果您为 Kaspersky Endpoint Security 配置了流量拦截排除，这些排除会影响网络威胁防护。

# 在 Web Console 中配置网络威胁防护

在 Web Console 中，您可以在策略属性（**应用程序设置 → 通信和 Web 保护 → 网络威胁防护**）中管理 网络威胁防护设置。

# 在管理控制台中配置网络威胁防护

在管理控制台中，您可以在策略属性中管理网络威胁防护设置（在管理控制台中管理策略，使用管理控制台创建策略）（**基本威胁防护 → 网络威胁防护**）。

网络威胁防护组件设置

| 设置 | 描述 |
| --- | --- |
| **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。

# 在命令行中配置网络威胁防护

在命令行中，您可以使用“网络威胁防护”预定义任务 (*Network_Threat_Protection*) 来管理“网络威胁防护”。

默认情况下，“网络威胁防护”任务不运行。您可以手动启动和停止任务。

您可以通过编辑“网络威胁防护”预定义任务的设置来配置“网络威胁防护”设置。

“网络威胁防护”任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `ActionOnDetect` | 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。 |

# 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。

该应用程序支持所有邮件客户端中的 POP3、SMTP 和 IMAP 协议，以及 MyOffice Mail 和 R7-Office Organizer 邮件客户端中的扩展协议版本（POP3S、SMTPS 和 IMAPS）。邮件威胁防护不支持其他协议。

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、465、587、110、995、143 和 993。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。您可以使用 Web Console、管理控制台和命令行启用、禁用或配置邮件威胁防护。

# 在 Web Console 中配置邮件威胁防护

在 Web Console 中，您可以在策略属性中管理邮件威胁防护设置（**应用程序设置 → 通信和 Web 保护 → 邮件威胁防护**）。

# 在管理控制台中配置邮件威胁防护

在管理控制台中，您可以在策略属性中管理邮件威胁防护设置（在管理控制台中管理策略、使用管理控制台创建策略）（**基本威胁防护 → 邮件威胁防护**）。

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。 |

# 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**收发消息**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 1 MB 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。 |

# 在命令行中配置邮件威胁防护

在命令行中，您可以使用“邮件威胁防护”预定义任务 (*Mail_Monitoring*) 来管理邮件威胁防护。

默认启动“邮件威胁防护”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“邮件威胁防护”任务，需要管理员角色权限。

您可以通过编辑“邮件威胁防护”预定义任务的设置来管理邮件威胁防护设置。

下表描述了您可以为邮件威胁防护任务指定的设置的可用值和默认值。

邮件威胁防护任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| CheckIncomingMessagesOnly | *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。 | Yes 表示应用程序仅扫描传入邮件。<br>No （默认值）表示应用程序会扫描传入和传出邮件。 |
| ScanFileArchive | 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。 | Yes （默认值）表示应用程序会扫描附件中的压缩文件。<br>No 表示应用程序不会扫描附件中的压缩文件。 |
| ScanFileOffice | 启用或禁用扫描 Office 格式的附件。 | Yes （默认值）表示应用程序会扫描附件中的 Office 格式文件。<br>No 表示应用程序不会扫描 Office 格式附件。 |
| UseSizeLimit | 限制被扫描压缩文件的大小。 | Yes 表示应用程序会将大于 SizeLimit 的压缩文件附件排除在扫描范围之外。<br>No （默认值）表示应用程序会扫描附加到电子邮件的任何大小的压缩文件。 |
| SizeLimit | 设置可扫描文件的最大大小。 | 1 至 9999 (MB)。 |
| UseTimeLimit | 限制压缩文件附件的最大扫描持续时间。 | Yes 表示应用程序在达到 TimeLimit 后会停止扫描附件中的压缩文件。<br>No （默认值）表示附件中压缩文件的扫描时间不受限制。 |
| TimeLimit | 设置附加压缩文件的最大扫描持续时间。 | 1 到 9999（秒钟）。 |
| ExtensionFilter | 配置电子邮件附件过滤。 | Disable 表示应用程序不过滤电子邮件附件。<br>Rename （默认值）表示应用程序会将指定文件类型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 表示应用程序会从电子邮件中删除指定类型的附件。 |
| ExtensionMasks | 指定要重命名或从电子邮件中删除的附件类型的扩展名。 | 可以按如下方式指定多个扩展名列表：<br>[ExtensionMasks.item_0000]<br>UseExtensionMask=Yes<br>ExtensionMask=*.txt<br>[ExtensionMasks.item_0001]<br>UseExtensionMask=Yes<br>ExtensionMask=*.run<br>[ExtensionMasks.item_0002]<br>UseExtensionMask=Yes<br>ExtensionMask=*.exe<br>...<br>默认会处理扩展名为 TXT、RUN、EXE、JS、JSE、MSI、SCR、VBE、VBS 和 SH 的文件。<br>要更改扩展名列表，需要将任务设置导出到 INI 文件，然后编辑该文件中的列表并将 INI 文件导入到应用程序中。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `UseAnalyzer` | 启用或禁用启发式分析器。 | `Yes`（默认值）表示已启用启发式分析器。<br>`No` 表示已禁用启发式分析器。 |
| `AnalyzerLevel` | 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。 | `Light` — 详细程度最低的扫描，系统负载最小。<br>`Medium`（默认值）– 中等详细程度的扫描，系统负载均衡。<br>`Deep` — 最详细的扫描，系统负载最大。 |
| `ActionOnThreat` | 这是邮件威胁防护在传入电子邮件中检测到威胁时执行的操作。<br>`ActionOnThreat` 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。 | `DisinfectDeleteIfNotPossible`（默认值）– 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>*。默认情况下已选择此操作。<br>`DisinfectBlockIfNotPossible` – 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。<br>`Block` – 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。 |

# BadUSB 攻击防护

某些病毒会修改 USB 设备的固件以欺骗操作系统，将 USB 伪装为键盘。结果，病毒可以用您的用户账户执行命令，例如下载恶意软件。

BadUSB 攻击防护保护组件可以阻止将受感染的、模拟键盘的 USB 设备连接到设备。

当被操作系统识别为键盘的 USB 设备连接到设备时，应用程序会提示用户输入由应用程序从新连接的键盘或使用屏幕键盘（如果可用）生成的数字代码。这个步骤称为键盘授权。

如果代码输入正确，应用程序会将识别参数（即键盘的 VID/PID 及其连接的端口号）保存到已授权键盘列表中。重启操作系统后重新连接键盘时无需重复键盘授权。

> 但如果已授权的键盘连接到设备的不同 USB 端口，应用程序会要求重新授权。

如果输入的数字代码不正确，应用程序将生成一个新代码。您可以配置输入授权码的尝试次数。如果多次输入错误的数字代码或关闭键盘授权窗口，应用程序将阻止来自此键盘的输入。当达到 USB 设备阻止时间或者操作系统重启后，程序将再次提示用户重新执行键盘授权。

程序将允许使用经过授权的键盘并阻止未经授权的键盘。

默认情况下，BadUSB 攻击防护保护组件处于禁用状态。您可以使用 Web Console、管理控制台和命令行启用、禁用或配置 BadUSB 攻击防护。

# 在 Web Console 中配置 BadUSB 攻击防护

在 Web Console 中，您可以在策略属性中管理BadUSB 攻击防护设置（**应用程序设置** → **主机威胁防护** → **BadUSB 攻击防护**）。

# 在管理控制台中配置 BadUSB 攻击防护

在管理控制台中，您可以在策略属性中管理 Web 威胁防护设置（在管理控制台中管理策略、使用管理控制台创建策略）（**基本威胁防护** → **BadUSB 攻击防护**）。

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。 |
| **USB 设备授权尝试最多次数：** | 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。<br>默认值：5。 |
| **当授权尝试次数达到最大值时的阻止持续时间（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）<br>默认值：5。 |
| **授权 USB 设备时不允许使用屏幕键盘。** | 如果选中此复选框，应用程序将阻止使用屏幕键盘对无法从中输入授权码的 USB 设备进行授权。<br>默认情况下已清空该复选框。 |

# 在命令行中配置 BadUSB 攻击防护

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。 |
| `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。 |

# 针对远程恶意加密的防护

反加密勒索组件允许您保护通过 SMB/NFS 协议进行网络访问的本地目录中的文件，使其免受远程恶意加密侵扰。

要使用该组件，需要包含相应功能的授权许可。

如果启用了反加密勒索，Kaspersky Endpoint Security 将针对受保护设备的共享网络目录中的文件资源扫描远程设备的操作是否存在恶意加密。如果应用程序将远程设备访问共享网络资源的操作视为恶意加密，则应用程序将创建并启用操作系统的防火墙规则，阻止来自受感染设备的网络流量。受感染的设备将被添加到不受信任的设备列表中，并且所有不受信任的设备对共享网络目录的访问都会受到阻止。应用程序将创建一个*加密检测*事件，其中包含有关受感染设备的信息。

默认情况下，应用程序阻止非可信设备对网络文件资源访问的时间长度为 30 分钟。当阻止时间到期时，应用程序会将受感染的设备从不受信任的设备列表中删除，并自动恢复该设备对网络文件资源的访问权限。

无法使用 iptables 实用程序删除由反加密勒索组件创建的防火墙规则，因为应用程序每分钟都会恢复一组规则。

默认禁用针对远程恶意加密的防护。

您可以启用或禁用针对恶意加密的防护（反加密勒索），也可以配置防护设置：

- 选择检测到加密时应用程序将执行的操作：通知用户或阻止执行恶意加密的设备。

  如果选择了*"通知"*操作，则在启用反加密勒索时，应用程序仍会扫描远程设备在网络文件共享上的操作，以检查是否存在恶意加密。如果检测到恶意活动，则会创建*加密检测*事件，但不会阻止受感染的设备。

- 设置阻止不受信任的设备的持续时间。
- 指定应用程序要防护恶意加密的文件和目录。
- 指定从恶意加密防护中排除的文件和目录。

  如果在加密防护范围之外的目录中检测到加密活动（反加密勒索），应用程序不会将操作视为加密。

您可以在命令行中使用管理受阻止设备的命令来查看受阻止的设备列表，并手动解除对这些设备的阻止。除了*加密检测*事件之外，Kaspersky Security Center 不提供其他工具来监控和管理受阻止的设备。

为了保证反加密勒索组件正常工作，必须在操作系统上安装至少一项服务（Samba 或 NFS）。NFS 服务要求安装 rpcbind 软件包。

反加密勒索组件可以与 SMB1、SMB2、SMB3、NFS3、TCP/UDP 和 IP/IPv6 协议一起正常运行。不支持使用 NFS2 和 NFS4 协议。建议配置服务器设置，以保证不能使用 NFS2 和 NFS4 协议挂载资源。

在将设备活动识别为恶意活动之前，Kaspersky Endpoint Security 不会阻止对网络文件资源的访问。因此，在应用程序检测到恶意活动之前，至少有一个文件将被加密。

# 在 Web Console 中配置反加密勒索

在 Web Console 中，您可以在策略属性中（**应用程序设置** → **主机威胁防护** → **行为分析** → **反加密**）管理反加密勒索设置。

# 在管理控制台中配置反加密勒索

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**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 |
| --- | --- |
| **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** | 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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。<br>掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。<br>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。<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。 |

# “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 |
| --- | --- |
| **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>您可以使用特殊标签来指定容器或镜像：<br>• `[container-id:<id>]/<path to local directory>`<br>• `[container-name:<name>]/<path to local directory>`<br>• `[image-id:<id>]/<path to local directory>`<br>• `[image-name:<name>]/<path to local directory>`<br>其中：<br>`<id>` 是容器 ID。<br>`<name>` 是容器名称<br>`<path to local directory>` 是本地目录的路径。<br>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>`。<br>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。<br>例如：<br>• `[container-name:<name>][image-name:<name>]/path to local directory>`<br>• `[container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[image-name:<name>][image-id:<id>]/<path to local directory>`<br>• `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`<br>• `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`<br>您可以在名称和标识符中使用掩码（`?` 和 `*` 字符）。<br>您可以用 `*`（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>`**` 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。<br>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。<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。 |

# “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。

# 在命令行上配置反加密勒索

在命令行中，您可以使用“反加密勒索”任务 (*Anti_Cryptor*) 来管理反加密勒索。

默认情况下，“反加密勒索”任务不运行。您可以手动启动和停止该任务。

您可以通过编辑“反加密勒索”预定义任务的设置来配置“反加密勒索”设置。

“反加密勒索”任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| `ActionOnDetect` | 启用不受信任主机阻止。 | `Block`（默认值）— 启用不受信任主机阻止。<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`。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。 |
| `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>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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：<br> | | |
| `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>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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。 |

# 管理被阻止的设备

在保护设备免受网络威胁和远程恶意加密的同时，Kaspersky Endpoint Security 可以阻止其操作被视为恶意的远程设备：

- 如果检测到恶意加密，应用程序将阻止远程设备访问受保护设备的共享网络目录。
- 一旦检测到受保护设备上出现网络攻击尝试，应用程序就会阻止来自攻击设备的网络流量。

您可以在“网络威胁防护”和“针对远程恶意加密的防护”设置中更改阻止持续时间。指定时间一过，应用程序就会解除对设备的阻止。

如果您使用命令行来管理应用程序，则可以使用管理被阻止设备的命令查看由于该应用程序在设备上运行而被阻止的设备的列表，并在阻止时间到期之前手动解除对这些设备的阻止。除*检测到网络攻击*和*检测到加密*事件外，Kaspersky Security Center 不提供用于监控和管理被阻止设备的工具。

*要查看受阻止设备的列表，请执行以下命令：*

```
kesl-control --get-blocked-hosts
```

命令执行的结果是，应用程序将被阻止设备的列表输出到控制台。

*要解除阻止设备，请执行以下命令：*

```
kesl-control --allow-hosts < 地址 >
```

其中 < 地址 > 是设备或子网的一个或多个 IP 地址（IPv4/IPv6，包括缩写形式的地址）。您可以指定设备或子网的多个 IP 地址，用空格分隔。

命令执行的结果是，应用程序解除对指定设备的阻止。

例如：
IPv4 地址：
dec - 192.168.0.1
dec - 192.168.0.0/24
IPv6 地址：
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::

# 应用程序控制

应用程序控制组件允许您管理受保护设备上应用程序的启动。“应用程序控制”通过限制用户对应用程序的访问来降低设备感染的风险。您可以使用“清查”任务接收有关受保护设备上安装的应用程序的信息。

要使用该组件，需要包含相应功能的授权许可。

应用程序启动受*应用程序控制规则*的约束。

应用程序控制组件有两种运行模式可选：

- *拒绝列表*。在此模式下，Kaspersky Endpoint Security 允许所有用户启动应用程序控制规则中未指定的任何应用程序。默认情况下，应用程序控制组件在此模式下运行。
- *允许列表*。在此模式下，Kaspersky Endpoint Security 禁止所有用户启动应用程序控制规则中未指定的任何应用程序。

因此，如果创建了最大限度的“应用程序控制”规则，Kaspersky Endpoint Security 将禁止启动所有未经组织的本地网络管理员验证的新应用程序，但可以确保操作系统和用户履行工作职责所需的经过验证的应用程序的性能。

Kaspersky Security Center 管理员或在应用程序中分配了管理员角色的本地用户可以在 root 账户下使用“应用程序控制”允许或拒绝进程启动。

默认情况下，“应用程序控制”被禁用。您可以启用或禁用“应用程序控制”，还可以配置该组件的操作设置：

- 选择应用程序控制模式：*允许列表*或*拒绝列表*。
- 为各个模式创建应用程序控制规则。
- 选择 Kaspersky Endpoint Security 在检测到尝试运行符合规则的应用程序的行为时执行的操作：Kaspersky Endpoint Security 可以*应用规则*并执行规则中指定的操作，或者*测试规则*并仅通知尝试运行符合规则的应用程序。
- 导出和导入应用程序控制设置。

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。

如果应用程序控制规则允许解释器启动，Kaspersky Endpoint Security 不会阻止从该解释器启动的脚本。如果应用程序控制规则禁止启动解释器命令行中指定的至少一个脚本，Kaspersky Endpoint Security 会阻止解释器命令行中指定的所有脚本。排除：cat script.py | python。

# 关于应用程序控制规则

*应用程序控制规则*是一组设置，其中包含规则触发条件以及触发规则时应用程序控制组件的操作（允许或阻止用户启动应用程序）：

- 属于应用程序类别的应用程序。*应用程序类别*是一组具有共同特征的应用程序。例如，包含已安装应用程序的可执行文件的类别或操作所需的应用程序类别，其中包括组织使用的一组标准应用程序。每个类别只能在一条规则中使用。

  Kaspersky Endpoint Security 不支持使用 Kaspersky Security Center 的 KL 类别。

- 允许选定的用户和/或用户组运行应用程序，或阻止他们运行应用程序。您可以指定用户和/或用户组，以允许或不允许他们运行指定类别的应用程序。

- 规则触发条件。条件由以下对应关系表示："条件类型 – 条件标准 – 条件值"。根据规则的触发条件，Kaspersky Endpoint Security 可能为应用程序应用规则，也可能不会。这些规则使用包含条件和排除条件：

  - *包含条件*。如果应用程序符合至少一个包含条件，则 Kaspersky Endpoint Security 将规则应用于应用程序。

  - *排除条件*。如果应用程序符合至少一个排除条件或不符合任何包含条件，则 Kaspersky Endpoint Security 不将规则应用于应用程序。

  规则触发条件是使用以下条件创建的：

  - 应用程序的可执行文件的名称。

  - 包含应用程序可执行文件的目录的名称。

  - 应用程序可执行文件的哈希值。仅可使用 SHA256。

  对于条件中使用的每个标准，必须指定一个值。

  您可以使用**掩码**指定文件和目录的名称。

  可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。

  可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如，`/dir/*/file*/` 或 `/dir/file*/`。

  可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 /）。

  如果正在启动的应用程序的设置与包含条件中指定的条件匹配，则会触发规则。在这种情况下，Kaspersky Endpoint Security 将执行规则中指定的操作。如果应用程序设置与排除条件中指定的条件匹配，则 Kaspersky Endpoint Security 不会控制应用程序的启动。

应用程序控制规则可以具有以下*操作状态*之一：

- *已启用* – 规则已启用，Kaspersky Endpoint Security 对应用程序控制应用此规则。
- *已禁用*：该规则已禁用，并且不会应用于应用程序控制。
- *Test* – Kaspersky Endpoint Security 允许启动符合规则标准的应用程序，但在报告中记录有关这些应用程序启动的信息。

规则操作状态的优先级高于规则中指定的操作的优先级。

# 应用程序控制规则测试模式

要确保应用程序控制规则不会阻止工作所需的应用程序，建议启用*应用程序控制规则测试*。在此模式下，Kaspersky Endpoint Security 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。

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。

# 在 Web Console 中配置“应用程序控制”

在 Web Console 中，您可以在策略属性中（**应用程序设置** → **安全控制** → **应用程序控制**）管理应用程序控制设置。

# 在管理控制台中配置应用程序控制

在管理控制台中，您可以在策略属性中管理设备控制设置（在管理控制台中管理策略，使用管理控制台创建策略）（**安全控制** → **应用程序控制**）。

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。 |

# 在命令行上配置应用程序控制

在命令行中，您可以使用“应用程序控制”预定义任务 (*Application_Control*) 来管理应用程序控制。

默认情况下，“应用程序控制”任务不运行。您可以手动启动和停止任务。

您可以通过编辑“应用程序控制”预定义任务的设置来配置设备上的应用程序控制。

如果您更改允许的应用程序列表，或者禁止启动所有应用程序或影响 Kaspersky Endpoint Security 运行的应用程序，则在使用配置文件修改任务设置或使用命令行选项时，请运行带有 `--accept` 标志的 `kesl-control --set-settings` 命令。

您还可以使用应用程序控制命令来配置应用程序控制：

- 创建和编辑类别列表。
- 查看在应用程序中创建的类别列表。
- 配置应用程序控制规则列表。

# “应用程序控制”任务设置

该表介绍了可为应用程序控制任务指定的所有设置的所有可能值以及默认值。

“应用程序控制”任务设置

| 设置 | 描述 | 值 |
|---|---|---|
| `AppControlMode` | “应用程序控制”任务操作模式。 | `AllowList` – Kaspersky Endpoint Security 阻止用户启动应用程序控制规则中未指定的任何应用程序。<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。 |
| `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。<br>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。<br>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*/`。<br>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 `/`）。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `IncludeFolders.item_#` | 包含触发规则的应用程序可执行文件的目录的名称。 | 您可以使用**掩码**指定路径名称。<br>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。<br>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*/`。<br>可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 `/`）。 |
| `IncludeHashes.item_#` | 触发规则的可执行文件的 SHA256 哈希值。 | 仅可使用 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。<br>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。<br>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*/`。<br>可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 `/`）。 |
| `ExcludeFolders.item_#` | 包含触发规则的应用程序可执行文件的目录的名称。 | 您可以使用**掩码**指定路径名称。<br>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。<br>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*/`。<br>可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 `/`）。 |
| `ExcludeHashes.item_#` | 触发规则的可执行文件的 SHA256 哈希值。 | 仅可使用 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。 | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |

# 创建和编辑类别列表

您可以通过两种方式创建新类别：

- 使用“kesl --set-settings”命令和应用程序控制任务设置配置文件（Application_Control）；
- 使用 kesl --set-categories 命令和类别设置配置文件。

*要创建应用程序类别，请运行以下命令：*

```
kesl-control --set-categories --file < 配置文件路径 >
```

其中：

--file < 配置文件路径 > 是包含类别设置的配置文件路径。

包含类别设置的文件必须具有以下结构：

```
[
    {
        "Exclude" : [ "(FilePath like < 应用程序可执行文件的完整路径 >)", "(FileHash == < 可执行文件的哈希值 >)" ],
        "GUID" : "< 唯一类别 ID >",
        "Include" : [ "(FilePath like < 应用程序可执行文件的完整路径 >)", "(FileHash == < 可执行文件的哈希值 >)" ],
        "Name" : "< 类别 1 的名称 >"
    },
   {
        "Exclude" : [ "(FilePath like < 应用程序可执行文件的完整路径 >)", "(FileHash == < 可执行文件的哈希值 >)" ],
        "GUID" : "< 唯一类别 ID >",
        "Include" : [ "(FilePath like < 应用程序可执行文件的完整路径 >)", "(FileHash == < 可执行文件的哈希值 >)" ],
        "Name" : "< 类别 2 的名称 >"
    }
]
```

要在 Exclude 和 Include 字段中指定文件名，您可以使用**掩码**。

可以使用 * 字符（任意字符序列）或 ? 字符（任意一个字符）作为文件名或目录名掩码。

可以使用 * 字符表示包含 / 字符的文件名或目录名中的任意字符集（包括空字符集）。例如，/dir/*/file*/ 或 /dir/file*/。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符（包括 /）。

Name设置是必需的。如果不指定类别的名称，则不会创建或删除该类别。GUID设置也需要。如果不指定它，则会显示错误消息，不会创建类别。指定的GUID设置不得有连字符。

*要编辑已创建的应用程序类别的列表，请运行以下命令：*

```
kesl-control --set-categories [--names <类别 1 的名称> <类别 2 的名称> … <类别 N 的名称>] --file <配置文件路径>
```

其中：

- <类别 1 的名称> <类别 2 的名称> … <类别 N 的名称> 是您要更改其信息的类别名称。如果要更改有关多个类别的信息，请指定类别的名称，用空格分隔。如果不指定类别名称，则现有类别会被删除并从指定文件创建新类别。
- --file <配置文件路径> 是包含类别设置的配置文件路径。

# 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 <配置文件路径>] [--json]
```

其中：

- --file <配置文件路径> 是设置将写入到的 JSON 配置文件的完整路径。
- 指定 --json，则以 JSON 格式输出设置。如果 --json 选项被省略，则设置以 INI 格式输出。

Kaspersky Endpoint Security 显示以下有关每个应用程序类别的信息：

- 类别的唯一标识符 (GUID)
- 类别名称
- 用于触发规则的包含条件列表
- 用于触发规则的排除条件列表

*要查看单独应用程序类别的列表，请执行以下命令：*

```
kesl-control --get-categories [--names <类别 1 的名称> <类别 2 的名称> ... <类别 N 的名称>] [--file <配置文件路径>] [--json]
```

其中：

- `<类别 1 的名称> <类别 2 的名称> ... <类别 N 的名称>` 是要查看其信息的类别名称。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 <配置文件路径>` — 类别列表将导出到的 JSON 配置文件的完整路径。
- 指定 `--json`，则以 JSON 格式输出设置。如果 --json 选项被省略，则设置以 INI 格式输出。

如果在用于包含或排除规则触发条件的 `[Categories.item_#]` 部分的"应用程序控制"任务设置中指定指向应用程序文件或包含可执行文件的目录的符号链接，那么在查看这些条件的类别列表时，将显示符号链接所指向的源路径。

# 配置应用程序控制规则列表

*要查看应用程序控制规则的列表，请运行以下命令：*

```
kesl-control --get-settings 21 [--file <path to configuration file>] [--json]
```

其中：

- `--file <path to 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 configuration file>] [--json]
```

其中：

- `--file <path to 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
```

# 导出和导入应用程序控制设置

为了简化用户设备上应用程序控制组件的配置，您可以导出和导入应用程序控制设置和应用程序类别列表。

## 在 Web Console 中导出和导入应用程序控制设置

在 Web Console 中，您可以导出或导入受管理设备属性中的应用程序控制设置和应用程序类别列表（**资产（设备）** → **受管理设备** → <设备名称> 链接 → **应用程序**选项卡 → <Kaspersky Endpoint Security 应用程序名称> 链接 → **应用程序设置**选项卡 → **应用程序控制**部分）。

单击**应用程序控制设置**下的**导出**按钮将打开一个窗口，您可以在其中指定要保存设置的文件。单击**应用程序控制设置**下的**导入**按钮将打开一个窗口，您可以在其中指定要从中导入设置的文件。

单击**应用程序类别**下的**导出**按钮将打开一个窗口，您可以在其中指定要保存添加的应用程序类别的文件。单击**应用程序类别**下的**导入**按钮将打开一个窗口，您可以在其中指定要从中导入应用程序类别的文件。

## 在管理控制台中导出和导入应用程序控制设置

在管理控制台中，您可以导出和导入受管理设备属性中的应用程序控制设置和应用程序类别列表（ **受管理设备**→ **设备**选项卡→设备属性窗口 →**应用程序**部分 → <应用程序名称> →**属性**按钮 → **<应用程序名称> 设置**窗口 →**应用程序控制**部分）。

单击**应用程序控制设置**下的**导出**按钮将打开一个窗口，您可以在其中指定要保存设置的文件。单击**应用程序控制设置**下的**导入**按钮将打开一个窗口，您可以在其中指定要从中导入设置的文件。

单击**应用程序类别**下的**导出**按钮将打开一个窗口，您可以在其中指定要保存添加的应用程序类别的文件。单击**应用程序类别**下的**导入**按钮将打开一个窗口，您可以在其中指定要从中导入应用程序类别的文件。

## 在命令行中导出和导入应用程序控制设置

在命令行中，您可以使用应用程序控制管理命令导出或导入应用程序控制设置和应用程序类别列表。

# 清查

“清查”任务提供有关客户端设备上存储的所有应用程序可执行文件的信息。例如，获取设备上安装的应用程序的相关信息对于创建应用程序控制规则非常有用。

要使用该任务，需要包含相应功能的授权许可。

您还可以配置以下清查设置：

- 选择应用程序在清查时将在设备上检测的对象类型（文件、脚本）。
- 配置清查范围（搜索可执行应用程序文件的目录路径）。
- 配置清查排除项。
- 选择 Kaspersky Endpoint Security 在完成清查任务后必须对“黄金镜像”应用程序类别执行的操作。您可以将任务在设备上发现的应用程序添加到类别中、保持类别不变或将其删除。
- 启用或禁用将清查任务在设备上发现的应用程序的相关信息传输到 Kaspersky Security Center 管理服务器。如果设备上的应用程序的相关信息被传输到管理服务器，则可以使用该信息通过 Kaspersky Security Center 为应用程序控制规则配置应用程序类别。

# 在 Web Console 中配置清查

在 Web Console 中，您可以使用“*清查*”任务对受保护设备的应用程序执行清查。

您可以创建并运行“清查”用户任务。您可以通过编辑这些任务的设置来配置“清查”设置。

Kaspersky Security Center 数据库最多可以存储有关 150,000 个已处理文件的信息。达到此记录数时，将不会再处理新文件。要恢复“清查”任务，请从安装了 Kaspersky Endpoint Security 的设备中删除由于之前的清查而在 Kaspersky Security Center 数据库中注册的文件。

清查任务设置

| 设置 | 描述 |
| --- | --- |
| **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 在完成清查任务后必须对“黄金镜像”应用程序类别执行的操作：<br>• **没有变化** – 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** – 完成清查后删除“黄金镜像”类别。<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。 |

| 设置 | 描述 |
| --- | --- |
| **清查范围** | 该表包含应用程序扫描的清查范围。应用程序将扫描位于表中指定路径的文件和目录。默认情况下，该表包含一个清查范围 – /usr/bin。<br>您可以在表中添加、编辑、删除、上移或下移清查范围。<br>您还可以点击“**导入**”从文件中导入清查范围列表，或点击“**导出**”将清查范围列表以 JSON 格式导出到文件。导入时，系统会提示您替换清查范围列表或将清查范围添加到现有列表中。 |

# “添加扫描范围”窗口

在此窗口中，您可以为清查任务添加和配置扫描范围。

清查范围设置

| 设置 | 描述 |
| --- | --- |
| **范围名称** | 用于输入清查范围名称的字段。此名称将显示在“**扫描设置**”部分的表格中。<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清查范围。<br>如果清除此复选框，则应用程序在运行任务时不处理此清查范围。您可以在以后选中此复选框来在任务设置中包括此范围。<br>默认情况下已选定该选框。 |
| **文件系统，访问协议和路径** | 用于指定要包含在清查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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<br>该字段不能为空。默认情况下指定 **/** 路径 – 应用程序扫描本地文件系统的所有目录。 |
| **掩码** | 此列表包含应用程序在运行任务时扫描的对象的名称掩码。<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”部分

在“清查”任务的“**排除范围**”部分中，您可以配置要从扫描中排除的范围。

# “排除范围”窗口

此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 |
| --- | --- |
| **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。

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。

# “添加排除范围”窗口

在此窗口中，您可以为清查任务添加和配置扫描排除范围。

排除范围设置

| 设置 | 描述 |
| --- | --- |
| **排除范围名称** | 用于输入排除范围名称的字段。此名称将显示在**排除范围**窗口的表格中。<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。<br>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<br>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。 |

# 在管理控制台中配置清查

在 Kaspersky Security Center 管理控制台中，您可以使用“*清查*”任务对受保护设备的应用程序执行清查。

您可以创建并运行“清查”用户任务。您可以通过编辑任务的设置来配置扫描设置。

Kaspersky Security Center 数据库最多可以存储有关 150,000 个已处理文件的信息。达到此记录数时，将不会再处理新文件。要恢复“清查”任务，请从安装了 Kaspersky Endpoint Security 的设备中删除由于之前的清查而在 Kaspersky Security Center 数据库中注册的文件。

清查任务设置

| 设置 | 描述 |
| --- | --- |
| **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 在完成清查任务后必须对“黄金镜像”应用程序类别执行的操作：<br>• **没有变化** – 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** – 完成清查后删除“黄金镜像”类别。<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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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。 |

# “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 |
| --- | --- |
| **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。<br>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 |
| **掩码** | 该列表包含应用程序从扫描中排除的对象的名称掩码。<br>您可以添加、编辑或删除掩码。 |

# 在命令行中配置清查

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“Inventory_Scan”*预定义任务*。您可以手动启动或停止该任务，并配置任务运行计划。您可以通过编辑该任务的设置来配置扫描设置。
- 借助用户清查任务（*InventoryScan* 类型的任务）。您可以手动启动、停止、暂停或恢复用户任务，并配置任务计划。

您可以使用“应用程序控制”管理命令来查看“清查”任务完成后在设备上检测到的应用程序列表。

# 清查任务设置

该表介绍了可为清查任务指定的所有设置的全部可能值和默认值。

| 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 – 完成清查后删除"黄金镜像"类别。 |
| **[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。 |
| 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。<br>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 |

# 查看检测到的应用程序列表

*要查看在设备上检测到的应用程序列表，请执行以下命令：*

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

其中 `--json` 表示以 JSON 格式输出数据。

Kaspersky Endpoint Security 显示以下有关检测到的应用程序的信息：

- **清查的日期和时间**。执行清查任务的日期和时间
- **应用程序数量**。在设备上检测到的应用程序数量
- 包含以下信息的应用程序列表：
  - **路径**。应用程序的路径。
  - **哈希**。应用程序哈希和。
  - **Type**。应用程序类型。例如，`Script`、`Executable`。
  - **类别**。应用程序所属的类别（如果之前已创建）。您可以使用命令 `kesl-control --get-categories` 查看已创建的应用程序类别列表。

添加新类别时，其信息不会在应用程序列表中自动更新。要更新应用程序列表，您需要重新启动清查任务。

# 设备控制

*设备控制*组件允许您管理用户对已安装到或已连接到客户端设备的设备（例如，硬盘驱动器、摄像头或 Wi-Fi 模块）的访问。访问管理可保护客户端设备在连接外部设备时免受感染，并防止数据丢失或泄露。

当 Kaspersky Endpoint Security 启动时，“设备控制”组件会使用默认设置自动启用。

“设备控制”从以下几个方面来控制用户访问：

- 由“设备控制”分类的**设备类型**，例如打印机、可移动驱动器或 CD/DVD 驱动器。下列其中一种访问模式可应用于每种设备类型：
  - *允许*，允许访问此类型的设备。
  - *阻止*：阻止对此类型设备的访问。
  - *基于总线*：根据用于连接设备的总线的访问模式，允许或阻止对设备的访问。
  - *按规则*：根据访问规则，允许或阻止对设备的访问。*设备访问规则*是用于确定哪些用户可以访问已安装在客户端设备上或与其连接的设备，以及在什么时间访问的一组选项。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。
  - *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。
- **连接总线**。*连接总线*是用于将设备连接到客户端设备的接口（例如 USB 或 FireWire）。下列其中一种访问模式可应用于连接总线：
  - *允许*：允许访问通过此连接总线连接的设备。
  - *阻止*：拒绝访问使用此连接总线连接的设备。

  例如，可能拒绝访问所有通过 USB 连接的设备。

默认情况下，所有设备类型均选择*取决于连接总线*访问模式。连接总线选择*允许*访问模式。“设备控制”相应地授予用户对所有设备的完全访问权限。

首次启用“设备控制”时，它会为所有检测到的具有已知设备或总线类型的设备生成一个“*DeviceAllowed*”事件。除非这些设备的控制设置发生变化，否则后续组件运行时不会生成重复事件。

当“设备控制”被禁用时，应用程序将解除对被阻止设备的访问的阻止。

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。

您可以启用、禁用和配置“设备控制”：

- 选择当尝试访问设备控制设置禁止访问的设备时应用程序的操作模式：阻止或仅通知有关访问设备的尝试。
- 根据类型选择设备访问模式。
- 根据设备所连接的总线选择设备访问模式。
- 通过将单个设备添加到受信任设备的列表中，将其从“设备控制”范围中移除。*受信任设备*是用户拥有完全访问权限的设备。您还可以限制对特定 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。此外，您还可以指定受信任设备的用户或用户组。

  您可以用命令行或 Kaspersky Security Center 管理受信任设备列表。

  您可以通过标识符或标识符掩码将设备添加到受信任设备的列表中。您可以使用客户端设备上的命令行或使用 Kaspersky Security Center 获取关于安装在客户端设备上或连接到客户端设备的设备的信息。默认启用与 Kaspersky Security Center 管理服务器的信息共享。

  > 如果客户端设备受活动策略的控制并与网络代理同步（按照网络代理策略属性中指定的频率执行，默认情况下每 15 分钟一次），则会传输有关设备的信息。

  如果您使用 Kaspersky Security Center 管理应用程序，还可以使用以下方法将设备添加到受信任列表中：

  - 在受管理客户端设备上发现的设备列表。该列表显示在 Web Console 或管理控制台的策略属性中。
  - 基于 Kaspersky Security Center 中的设备控制事件生成的设备列表。您可以在管理控制台的策略属性中创建此列表。

  在管理控制台中，您还可以将配置的受信任设备列表导出到文件或从文件导入受信任设备列表。
- 配置存储设备（硬盘驱动器、可移动驱动器、软盘驱动器、CD/DVD 驱动器）的访问计划。

  > 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。
- 您可以根据设备的类型定义设备访问规则。在指定时间允许或阻止指定用户的访问。
- 允许用户请求对被阻止设备的临时访问权限和授予用户对该设备的访问权限。

  > 只有当组织中部署了 Kaspersky Security Center 16.2 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。

# 在 Web Console 中配置设备控制

在 Web Console 中，您可以在策略属性中管理设备控制设置（**应用程序设置→ 安全控制 → 设备控制**）。

# 在管理控制台中配置设备控制

在管理控制台中，您可以在策略属性中管理设备控制设置（在管理控制台中管理策略，使用管理控制台创建策略）（**安全控制** → **设备控制。**）。

设备控制设置

| 设置 | 描述 |
| --- | --- |
| **启用设备控制** | 此复选框用于启用或禁用设备控制。<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接口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。 |
| **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。 |

| 设置 | 描述 |
| --- | --- |
| 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。 |

| 设置 | 描述 |
| --- | --- |
| **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** | 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，或者是该规则所适用的用户组的名称。 |

# 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。 |

# 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。

*要在 Web Console 中编辑消息模板：*

1. 在策略属性窗口中，选择“**应用程序设置**” → “**安全控制**” → “**设备控制**”。
2. 在**消息模板**部分，单击**阻止消息**链接。
3. 这将打开**消息模板**窗口；在该窗口中，在**致用户的消息**选项卡上配置设备控制消息模板。

   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。

   您也可以通过单击**重置为默认**按钮恢复消息模板的文本。
4. 单击“**确定**”。
5. 单击“**保存**”按钮以保存更改。

*要在管理控制台中更改消息模板：*

1. 在管理控制台树的“**受管理设备**”文件夹中，打开具有所需设备所属的管理组名称的文件夹。
2. 在工作区中选择“**策略**”选项卡。
3. 在策略列表中，选择所需的策略并双击它以打开“**属性：<策略名称>**”窗口。

   您还可以通过使用策略上下文菜单中的“**属性**”项或单击位于策略设置部分中策略列表右侧的“**配置策略设置**”链接来打开策略属性窗口。
4. 在策略窗口中，选择**安全控制→ 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**。

# 在命令行上配置设备控制

您可以借助“设备控制”预定义任务 (*Device_Control*) 在命令行中管理设备控制。

“设备控制”任务默认不启动。您可以手动启动和停止任务。

您可以通过编辑“设备控制”预定义任务的设置来配置设备控制。

您还可以使用设备控制管理命令来：

- 查看已连接设备列表并将其导出到文件
- 查看和更改受信任设备列表

# 设备控制任务设置

该表介绍了可为设备控制任务指定的所有设置的全部可能值以及默认值。

设备控制任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `OperationMode` | 对尝试访问根据设备控制规则受到限制的设备的响应。 | `Block` （默认值）— 应用程序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接口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。 |
| `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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。 |
| `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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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=< 设备 ID >*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。 | | |
| 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>< 用户名 > 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 >\< 用户名 > 或 < 用户名 >@< 域名 > 格式）。<br>@< 组名 > 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>< 星期几 > 是一周中的某一天。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>< 小时 > 是小时数 [0:24]。对于小时，您仅能指定间隔时间。<br>例如：<br>*Schedule_1 的有效期为星期日至星期六，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：*<br>[Schedules.item_0001]<br>ScheduleName=schedule_1<br>DaysHours=Su-Sa:0..11,12..15,16..24<br>*Schedule_2 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>*Schedule_3 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>< 用户名 > 是访问规则适用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 >\< 用户名 > 或 < 用户名 >@< 域名 > 格式）。<br>@< 组名 > 是访问规则适用的（本地或域）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>< 用户名 > 是访问规则适用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 >\< 用户名 > 或 < 用户名 >@< 域名 > 格式）。<br>@< 组名 > 是访问规则适用的（本地或域）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。 |
| 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。 | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>< 用户名 > 是访问规则适用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 >\< 用户名 > 或 < 用户名 >@< 域名 > 格式）。<br>@< 组名 > 是访问规则适用的（本地或域）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>< 用户名 > 是访问规则适用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 >\< 用户名 > 或 < 用户名 >@< 域名 > 格式）。<br>@< 组名 > 是访问规则适用的（本地或域）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。 |

# 在命令行中查看和导出连接设备列表

*要查看所连接设备的列表，请执行以下命令：*

```
kesl-control --get-device-list [--all] [--json]
```

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。

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。

*要导出所连接设备的列表，请运行以下命令：*

```
kesl-control --get-device-list --export <文件>
```

其中，<文件>是要保存已连接设备列表的 JSON 文件的完整路径。

受信任设备列表被导出。

# 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的信息（针对特定用户或用户组）。

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。

*要查看受信任设备列表，请运行以下命令：*

```
kesl-control --trusted-devices --list
```

*要将设备添加到受信任设备列表，请运行以下命令：*

```
kesl-control --trusted-devices --add <ID>
```

其中，<标识符>是设备 ID 或设备 ID 掩码。

*要将设备从受信任设备列表中移除，请运行以下命令：*

```
kesl-control --trusted-devices --delete <ID>
```

其中，<标识符>是设备 ID 或设备 ID 掩码。

*要从文件导入受信任设备列表，请运行以下命令：*

```
kesl-control --trusted-devices --merge|--add|--replace --file <文件>
```

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 <文件>`是将从中导入受信任设备列表的 JSON 文件的完整路径。

# 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、管理控制台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接口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。用户可以通过应用程序的图形用户接口或命令行上传访问密钥。

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。

# 在 Web Console 中授予对被阻止设备的访问权限

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。

当管理员收到用户的临时访问请求时，管理员可以在 Web Console 中根据访问请求文件创建访问密钥。

要提供对设备的临时访问权限，管理员必须拥有**数据加密**功能的读取、写入和执行权限（**用户和角色**→**角色**→ <用户角色> → 用户角色属性窗口 →**访问权限**选项卡→ <应用程序名称> →**数据加密**→**读取/写入/执行**）。

*要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。

# 通过命令行获得对设备的临时访问权限

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，则用户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：`kesl-control --request-temporary-device-access`。

*要请求对被阻止设备的临时访问权限，请运行以下命令：*

```
kesl-control --request-temporary-device-access --device-id <设备 ID> --access-duration <访问持续时间> --path <访问请求文件的路径>
```

其中：

`--device-id <设备 ID>` 指定您要访问的被阻止设备的 ID。

`--access-duration <访问持续时间>` 指定您希望能够访问设备的时间段（以小时为单位）。可能的值：1 到 100

`--path <访问请求文件的路径>` 指定要将扩展名为 .akey 的访问请求文件保存到其中的目录路径。

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）。

从管理员处获得访问密钥后，您需要使用 `kesl-control --upload-temporary-device-access-key` 命令上传该访问密钥，以获得对设备的临时访问权限。

*要获得对被阻止设备的临时访问权限，请运行以下命令：*

```
kesl-control --upload-temporary-device-access-key --path <包含访问密钥的文件的路径>
```

其中：

`--path <包含访问密钥的文件的路径>` 是包含设备访问密钥的文件（扩展名为 .acode 的文件）的路径。

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。

# Web 控制

Web 控制控制用户对 Web 资源的访问。这样可以减少流量消耗和对工作时间的不当使用。当用户尝试打开受 Web 控制限制其访问的网站时，Kaspersky Endpoint Security 会阻止访问或显示一条警告消息，告知用户该网站不受欢迎。

Kaspersky Endpoint Security 仅监控 HTTP 和 HTTPS 流量。

Web 控制可让您通过以下方式配置对网站的访问：

- 按内容类别。网站内容基于卡巴斯基安全网络、启发式分析和已知网站数据库（包含在应用程序数据库中）进行分类。例如，您可以限制用户对“社交网络”内容类别或其他类别网站的访问。
- 按数据类型类别。例如，您可以限制用户对网站上数据的访问并隐藏图形。应用程序根据文件格式而不是扩展名来确定数据类型。

  应用程序不会扫描压缩文件内的文件。例如，如果图像文件被压缩，应用程序会将数据类型检测为压缩文件而不是图像文件。

- 按网址。您可以指定网址或网址掩码。

您可以同时使用多种方法来规范对网站的访问。例如，您可以仅限制对 “Webmail” 类别网站上的 “Office 应用程序文件”数据类型的访问。

默认情况下，为所有 Web 资源选择的*默认规则*是“**允许**”。根据此规则，如果没有定义其他*Web 资源访问规则*，则 Web 控制允许用户访问 Web 资源。

您可以更改 Web 控制的默认规则，该规则可控制应用程序如何控制对其他规则未涵盖的 Web 资源的访问，并将*默认规则*设置为**阻止**。根据此规则，如果没有定义其他*Web 资源访问规则*，则 Web 控制会阻止用户访问 Web 资源。

如果您已为 Kaspersky Endpoint Security 配置了流量拦截排除，这些将影响 Web 控制。

# 关于 Web 资源访问规则

*Web 资源访问规则*是一组筛选器和当用户在规则计划中指定的时间访问规则中描述的 Web 资源时应用程序执行的操作。筛选器可让您指定受 Web 控制组件监控访问的 Web 资源。

系统提供以下过滤：

- **按内容类别筛选**。Web 控制可以根据内容对 Web 资源进行分类。您可以控制用户对具有由这些类别定义的内容的 Web 资源的访问。当用户访问属于所选内容类别的 Web 资源时，应用程序将执行规则中指定的操作。
- **按数据类型类别筛选**。Web 控制可以根据数据类型对 Web 资源进行分类。您可以控制用户对位于与某些类型数据相关的 Web 资源上的数据的访问。当用户访问与所选数据类型类别相关的 Web 资源时，应用程序将执行规则中指定的操作。

- **按 Web 资源地址筛选**。您可以控制用户对 Web 资源的所有地址、Web 资源的个别地址和/或 Web 资源的地址组的访问。

  如果您同时定义了按内容类别和/或数据类型类别进行筛选以及按 Web 资源地址进行筛选，并且指定的 Web 资源地址和/或 Web 资源地址组属于选定的内容类别或数据类型类别，则应用程序不会控制对选定内容类别和/或数据类型类别的所有 Web 资源的访问，而只是控制对选定的 Web 资源地址和/或 Web 资源地址组的访问。

- **按用户和用户组名称进行筛选**。您可以定义用户和/或用户组，根据规则控制其对 Web 资源的访问。例如，您可以限制公司内除 IT 部门以外的所有用户通过浏览器访问 Internet。

- **规则计划**。您可以设置规则计划。规则计划可决定应用程序控制对规则中指定的 Web 资源的访问的时间。例如，您可以限制只能在工作时间通过浏览器访问 Internet。

对于每条规则，您可以指定当用户访问与规则设置匹配的 Web 资源时 Web 控制执行的操作：

- *允许*。Web 控制允许用户访问 Web 资源。

- *阻止*。Web 控制阻止用户对 Web 资源的访问并显示访问被阻止的消息。通过单击阻止消息中的链接，用户可以向企业局域网管理员发送关于误阻止的投诉消息，并请求访问被阻止的 Web 资源。

- *通知*。Web 控制显示一条警告，提示该 Web 资源不受欢迎。通过单击警告消息中的链接，用户可以向企业局域网管理员发送关于误警告的投诉消息。同时，不会阻止用户访问该 Web 资源。

每条规则都有优先级。规则在列表中的位置越靠前，其优先级就越高。如果将某个网站添加到多条规则中，Web 控制将按照优先级最高的规则来控制对该网站的访问。例如，应用程序可能将公司门户网站识别为社交网络。要限制对社交网络的访问，同时允许访问公司门户网站，请创建两条规则：一条针对“社交网络”类别的阻止规则和一条针对公司门户网站的允许规则。公司门户网站访问规则的优先级必须高于社交网络访问规则。

如果没有创建阻止规则，则不会解密 HTTPS 流量。

# 在 Web Console 中配置 Web 控制

在 Web Console 中，您可以在策略属性中配置Web 控制设置（**应用程序设置** → **安全控制** → **Web 控制**）。

# 在管理控制台中配置 Web 控制

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**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>单击"**下移**"按钮可将所选项目在表中向下移动。<br>如果在表中只选择一个项目，则此按钮可用。<br>单击"**上移**"按钮可将所选项目在表中向上移动。<br>如果在表中只选择一个项目，则此按钮可用。<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。

添加 Web 控制规则

| 设置 | 描述 |
| --- | --- |
| **规则名称** | 用于输入 Web 资源访问规则名称的字段。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。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |

# 配置 Web 控制消息模板

根据 Web 控制规则属性中指定的操作，当用户尝试访问 Web 资源时，应用程序将显示以下类型的消息之一（通过将 HTTP 服务器响应替换为包含消息的 HTML 页面）：

- 警告。此类消息警告用户，访问该 Web 资源是不良行为和/或违反公司安全政策。如果在与此 Web 资源匹配的规则设置中选择了“**通知**”操作，则应用程序会显示一条警告消息。

  如果用户认为警告是错误，警告中的链接可以让用户向公司的 LAN 管理员发送自动生成的投诉消息。

- 阻止的 Web 资源消息 如果在与此 Web 资源匹配的规则设置中选择了**阻止**操作，则应用程序会显示一条消息，表明此 Web 资源已被阻止。

  如果用户认为不应阻止该 Web 资源，则被阻止的 Web 资源消息中的链接可让用户向公司的 LAN 管理员发送自动生成的投诉。

提供了警告消息、阻止的 Web 资源消息以及发送给公司 LAN 管理员的投诉消息的模板。您可以编辑其内容。

*要在 Web Console 中编辑消息模板：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**策略和策略配置文件**”。

   将打开策略列表。

2. 选择包含应用了策略的设备的管理组。为此，请单击窗口上部的“当前路径”字段中的链接，然后在打开的窗口中选择管理组。

   该列表仅显示为所选管理组配置的策略。

3. 单击列表中所需策略的名称。

   策略属性窗口将打开。

4. 在策略属性窗口中，选择**应用程序设置** → **Security Controls** → **Web Control**。

5. 在 **消息模板** 部分，在以下选项卡上配置 Web 控制消息模板：

   - “**警告**”。输入字段包含触发规则时出现的消息模板，该消息警告尝试访问不良 Web 资源。
   - “**阻止消息**”。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。
   - “**给管理员的消息**”。输入字段包含当用户认为不应阻止被阻止的 Web 资源时向企业局域网管理员发送投诉的模板。在用户请求访问后，Kaspersky Endpoint Security 会向管理员发送一条关于拒绝访问Kaspersky Security Center*网页*事件的消息。事件描述包含向管理员发送的消息，其中变量被其值替换。如果您的组织中未部署 Kaspersky Security Center 解决方案或没有与管理服务器连接，则应用程序将向管理员指定的电子邮件地址发送一条消息。

   在 **警告 和 阻止消息** 选项卡上，您可以通过单击“**添加变量**”和“**添加链接**”按钮向用户消息添加变量和链接。

   您可以通过单击“**恢复默认**”按钮恢复消息模板的文本。

6. 单击“**确定**”。

7. 单击“**保存**”按钮以保存更改。

*要在管理控制台中更改消息模板：*

1. 在管理控制台树的“**受管理设备**”文件夹中，打开具有所需设备所属的管理组名称的文件夹。
2. 在工作区中选择“**策略**”选项卡。
3. 在策略列表中，选择所需的策略并双击它以打开“**属性：<策略名称>**”窗口。

   您还可以通过使用策略上下文菜单中的“**属性**”项或单击位于策略设置部分中策略列表右侧的“**配置策略设置**”链接来打开策略属性窗口。
4. 在策略窗口中，选择**安全控制→ Web 控制**。
5. 在**消息模板**部分，单击**配置**按钮。
6. 这将打开**消息模板**窗口；在该窗口中，在以下选项卡上配置 Web 控制消息模板：

   - **警告**。输入字段包含触发规则时出现的消息模板，该消息警告尝试访问不良 Web 资源。
   - **阻止消息**。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**。

# 在命令行中配置 Web 控制

在命令行上，您可以使用 Web 控制预定义任务 ( *Web_Control* ) 来管理 Web 控制。

默认情况下，Web 控制任务处于停止状态。您可以手动启动和停止任务。

您可以通过更改Web 控制预定义任务的设置来编辑 Web 控制设置。

您还可以使用 Web 控制管理命令查看和编辑 Web 控制设置。

# Web 控制任务设置

下表介绍了可为 Web 控制任务指定的所有设置的全部可用值以及默认值。

| 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, GenerativeAITools |
| [Rules.item_#.FormatCategories.item_#] | 用于指定数据类型类别的部分。 | – |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| FormatCategories.item_#.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。 | < 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。<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。 | < 星期几 > 是一周中的某一天。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>< 小时 > 是小时数 [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 <配置文件路径>] [--json]
```

其中：

--file < 配置文件路径 > 是要向其中写入设置的配置文件的完整路径。

--json：以 JSON 格式输出数据。

*要编辑 Web 控制设置，请运行以下命令：*

```
kesl-control --set-settings 26 [--file <配置文件路径>] [--json]
```

其中：

`--file <配置文件路径>` 是将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
```

# 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。 |

# 系统完整性监控

Kaspersky Endpoint Security 实时或按需求监控受保护设备上操作系统的完整性。

- "*系统完整性监控*"会实时跟踪您在组件设置中添加到监控范围的文件和目录的更改。您可以跟踪文件中的更改，这些更改可能表明受保护的设备存在安全漏洞。
- 您可以使用"*系统完整性检查*"任务，通过将受监控对象的当前状态与先前记录的状态进行比较，来检查已添加到监控范围的文件和目录中是否有更改。

使用"系统完整性监控"需要包含此功能的授权许可。

当检测到监控范围内的文件或目录出现更改时，Kaspersky Endpoint Security 会生成有关对象访问控制列表更改的事件。"系统完整性监控"不会共享有关所做更改的具体数据。"*系统完整性检查*"任务发送有关修改的属性以及移动的文件和目录的数据。

# 实时系统完整性监控

系统完整性监控通过实时拦截文件操作来检测监控范围内对象的每次更改。

系统完整性监控运行时，应用程序将监控以下文件设置的更改情况：

- 内容（write, truncate 等）
- 元数据（拥有权 (chmod/chown)）
- 时间戳 (utimensat)
- 扩展属性（(setxattr) 等）

不计算文件校验和。

由于 Linux 操作系统的技术限制，应用程序无法识别对文件进行更改的用户或进程。

默认情况下禁用系统完整性监控。您可以启用、禁用和配置系统完整性监控：

- 定义系统完整性监控的监控范围。应用程序监控系统完整性监控设置中定义的监控范围内的文件操作。您必须指定至少一个监控范围才能使组件正常工作。默认情况下定义*卡巴斯基内部对象* (/opt/kaspersky/kesl/) 监控范围。

  您可以指定多个监控范围。您可以实时更改监控范围。

  应用程序任务不监控未位于监控范围内的具有硬链接的文件（属性和内容）的更改。

- 您可以按名称掩码配置从监控中排除的对象。

- 设置系统完整性监控的排除范围。为每个监控范围定义排除项，并且仅对指定的范围有效。您可以指定多个监控排除。

  排除项的优先级高于监控范围；即使排除的对象在监控范围内，也会跳过该对象。如果监控范围定义的级别低于排除目录，则应用程序在系统完整性监控期间将跳过该监控范围。

当目录被添加到监控范围或排除范围时，应用程序不会检查该目录是否存在。

# 在 Web Console 中配置系统完整性监控

在 Web Console 中，您可以在策略属性中管理系统完整性监控设置（**应用程序设置→安全控制 → 系统完整性监控**）。

# 在管理控制台中配置系统完整性监控

在管理控制台中，您可以在策略属性中管理系统完整性监控设置（在管理控制台中管理策略、使用管理控制台创建策略）（**安全控制 → 系统完整性监控**）。

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。

# 在命令行中配置系统完整性监控

您可以使用“系统完整性监控”预定义任务 (*System_Integrity_Monitoring*) 在命令行中实时管理系统完整性监控。任务类型：*OAFIM*。

默认情况下，“系统完整性监控”任务不运行。您可以手动启动和停止任务。

您可以通过编辑“系统完整性监控”预定义任务的设置，在设备上配置系统完整性监控。

| 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：<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>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。<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：<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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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） |

# 系统完整性检查

当“*系统完整性检查*”任务运行时，通过比较受监控对象的当前状态和原始状态来发现每个对象的更改情况。可以使用以下比较标准：

- 文件哈希
- 文件更改时间
- 文件大小

受监控对象的初始状态被记录为*基线*。基线包含受监控对象及其元数据的路径。

基线可能也包含个人数据。

设备上首次运行“系统完整性检查”任务时会创建系统基线。如果您创建了多个“系统完整性检查”任务，则会为每个任务创建一个单独的基线。仅当基线包含有关在该任务定义的监控范围内的对象的信息时，才会执行任务。如果基线与监控范围不匹配，则 Kaspersky Endpoint Security 会生成系统完整性违规事件。

每当任务设置被修改（例如，当添加新的监控范围时）以及当任务以 `RebuildBaseline=Yes` 设置 启动（或者如果在 Kaspersky Security Center 的任务属性中选中了**每次任务启动时重建基线**复选框）时，基线都会更新。

应用程序在受保护设备上创建基线存储。默认情况下，基线的存储位于 /var/opt/kaspersky/kesl/private/fim.db。需要 root 特权才能访问包含基线的数据库。

您可以通过删除相应的“系统完整性检查”任务来删除基线。

您可以根据需要运行系统完整性检查并配置扫描设置：

- 启用或禁用每次系统完整性检查任务完成后重建基线。
- 选择用于比较受监控文件的当前状态与原始状态的标准：使用文件哈希和更改时间，或者仅使用文件大小。

- 配置系统完整性检查的监控范围。
- 配置系统完整性检查的排除范围。您可以指定排除文件和目录的路径，并按名称掩码排除单个对象。

# 在 Web Console 中配置系统完整性检查

您可以借助“*系统完整性检查*”任务在 Web Console 中运行系统完整性检查。

您可以创建并运行用户系统完整性检查任务。您可以通过编辑任务的设置来配置扫描设置。

“系统完整性检查”任务设置

| 设置 | 描述 |
| --- | --- |
| **每次任务启动时重建基线** | 此复选框用于启用或禁用在每次启动“*系统完整性检查*”任务时重新建立系统基线。<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运行时监控目录。<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** | 包含任务扫描的监控范围的表。<br>默认情况下，该表包含**卡巴斯基内部对象** (/opt/kaspersky/kesl/) 监控范围。<br>您可以在表中添加、编辑、删除、上移或下移监控范围。<br>您还可以点击“**导入**”从文件中导入监控范围列表，或点击“**导出**”将监控范围列表以 JSON 格式导出到文件中。导入过程中，系统会提示您替换监控范围列表或者在现有列表中添加监控范围。 |

# “添加扫描范围”窗口

在此窗口中，您可以为“系统完整性检查”任务添加或配置监控范围。

监控范围设置

| 设置 | 描述 |
| --- | --- |
| **范围名称** | 用于输入监控范围名称的字段。此名称将显示在“**扫描设置**”部分的表格中。<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。 |

| 设置 | 描述 |
| --- | --- |
| **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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<br>该字段不能为空。<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。 |
| **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”部分

在“系统完整性检查”任务的**排除范围**部分，您还可以配置扫描的排除项范围和按掩码排除。

## “排除范围”窗口

该表包含系统完整性检查组件的监控排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。

监控排除范围设置

| 设置 | 描述 |
| --- | --- |
| **排除范围名称** | 排除范围名称。 |
| **Path** | 从监控中排除的目录的路径。 |
| **状态** | 指示应用程序是否在任务运行期间将此范围排除在监控之外。 |

您可以在表中添加、编辑或删除项目。

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。

## “添加排除范围”窗口

在此窗口中，您可以为“系统完整性检查”任务添加和配置监控排除项。

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。 |

| 设置 | 描述 |
| --- | --- |
| **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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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。 |
| **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。 |

## “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）。

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。

# 在管理控制台中配置系统完整性检查

您可以在管理控制台中借助“*系统完整性检查*”任务来执行系统完整性检查。

您可以创建并运行用户系统完整性检查任务。您可以通过编辑任务的设置来配置扫描设置。

在系统完整性检查任务属性的**设置**部分中，您可以编辑下表列出的设置。

"系统完整性检查"任务设置

| 设置 | 描述 |
| --- | --- |
| **每次任务启动时重建基线** | 此复选框用于启用或禁用在每次启动系统完整性检查任务时重建系统基线。<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**"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。 |

| 设置 | 描述 |
| --- | --- |
| **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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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。 |

# “排除范围”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。

| 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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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。 |
| **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）。 |

# “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）。

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。

# 在命令行中配置系统完整性检查

您可以通过使用用户*系统完整性检查*任务（*ODFIM*任务），在命令行中对设备运行系统完整性检查。

您可以手动启动、停止、暂停或恢复用户任务，并配置任务计划。您可以通过编辑这些任务的设置来配置系统完整性检查。

"系统完整性检查"任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| RebuildBaseline | 启用在*系统完整性检查*任务完成后重建基线。 | Yes：每次*系统完整性检查*任务完成后重建基线。<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。 |
| 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： | | |
| 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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。<br>默认值：/opt/kaspersky/kesl/ |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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： | | |
| 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>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。<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） |

# 行为检测

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

当 Kaspersky Endpoint Security 启动时，行为检测组件会使用默认设置自动启用。

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。

您可以启用、禁用和配置“行为检测”：

- 选择 Kaspersky Endpoint Security 在检测到操作系统中的恶意活动时要执行的操作：告知用户或阻止执行恶意活动的应用程序。
- 将进程活动从行为检测组件以及 MDR 和 EDR Expert（本地部署）组件的扫描范围中排除。

  应用程序会自动将 Watchdog 服务器进程的活动从扫描中排除。此排除项无法移除。

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，为了确保行为检测组件正常运行，请将配置文件中的 auditd 模式更改为 `enabled 1`（无配置阻止），然后重新启动操作系统。

如果 root 用户没有权限访问通过 NFSv4 协议挂载到设备上的远程目录，应用程序将阻止所有用户访问此类文件。

# 在 Web Console 中配置行为检测

在 Web Console 中，您可以在 策略属性 中管理 行为检测设置（**应用程序设置** → **主机威胁防护** → **行为分析** → **行为检测**）。

# 在管理控制台中配置行为检测

在管理控制台中，您可以在策略属性中管理行为检测设置（在管理控制台中管理策略，使用管理控制台创建策略）（**高级威胁防护** → **行为检测**）。

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。 |

| 设置 | 描述 |
| --- | --- |
| **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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>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。<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。 |

| 设置 | 描述 |
| --- | --- |
| **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-premise) 遥测中排除** | 此复选框可启用或禁用将进程从 MDR 和 EDR Expert (on-premise) 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。 |

# 在命令行中配置行为检测

您可以使用 *Behavior_Detection* 预定义任务，通过命令行管理操作系统中的应用程序行为检测。

行为检测任务默认运行。您可以手动启动和停止任务。

您可以通过编辑行为检测预定义任务的设置来配置行为检测。

行为检测任务设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。 |
| **[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。<br>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。 |
| `ApplyToDescendants` | 从扫描中排除 `ProgramPath` 设置指定的排除进程的子进程。 | `Yes` – 从扫描中排除指定的进程及其所有子进程。<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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| UseTrustedProgramForMDRAndEDR | 将进程从 MDR 和 EDR Expert (on-premise) 组件收集的遥测数据中排除。 | Yes — 将此进程的活动从 MDR 和 EDR Expert (on-premise) 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。 |
| 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 | | 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。 |

# 漏洞利用防御

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。例如，漏洞利用程序可以利用缓冲区溢出攻击。为此，漏洞利用程序会向易受攻击的应用程序发送大量数据。处理此数据时，易受攻击的应用程序会执行恶意代码。此攻击的结果是，漏洞利用程序可启动未经授权的恶意软件安装。如果用户没有尝试从存在漏洞的应用程序运行可执行文件，Kaspersky Endpoint Security 会阻止该文件的执行或通知用户。默认禁用漏洞利用防御。

漏洞利用防御需要启用行为检测和可更新内核模块。为了使漏洞利用防御组件达到最佳性能，建议同时启用 Web 威胁防护组件。

您可以启用或禁用漏洞利用防御并管理组件设置：

- 选择应用程序在检测到漏洞利用时将执行的操作：
- 配置从扫描范围中排除的对象。扫描排除项是一组条件。当满足这些条件时，该应用程序不会扫描对象中是否存在病毒和其他恶意软件。您可以从扫描范围中排除以下对象：
  - 按对象中检测到的威胁的名称排除的对象
  - 所指定路径中的文件和目录
  - 具有指定哈希值的文件

# 在 Web Console 中配置漏洞利用防御

在 Web Console 中，您可以在策略属性中管理漏洞利用防御设置（**应用程序设置** → **主机威胁防护** → **行为分析** → **漏洞利用防御**）。

# 在管理控制台中配置漏洞利用防御

在管理控制台中，您可以在策略属性中管理漏洞利用防御设置（在管理控制台中管理策略、使用管理控制台创建策略）（**高级威胁防护** → **行为检测**）。

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**部分 | 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。 |
| **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。 |
| 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。 |

# 在命令行中配置漏洞利用防御

在命令行上，您可以使用行为检测 (*Behavior_Detection*) 预定义任务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

应用程序可能无法在美国境内使用 KSN 功能。

为了加强对设备和用户数据的保护，Kaspersky Endpoint Security 可以使用卡巴斯基基于云的知识库 – 卡巴斯基安全网络 (KSN) 来检查文件、互联网资源和软件的信誉。使用卡巴斯基安全网络数据可确保更快地响应各种威胁、高保护组件性能和更少的误报。

卡巴斯基安全网络的使用是自愿的。您可以随时开始或停止使用 KSN。

## 卡巴斯基安全网络基础设施解决方案

Kaspersky Endpoint Security 支持以下基础设施解决方案与卡巴斯基的信誉数据库一起使用：

- *卡巴斯基安全网络 (KSN)* – 一种解决方案，从卡巴斯基接收信息并将有关在用户设备上检测到的对象的数据发送到卡巴斯基以供卡巴斯基分析人员进行额外验证并添加到信誉和统计数据库中。
- *卡巴斯基私有安全网络 (KPSN)* – 一种解决方案，允许安装了 Kaspersky Endpoint Security 的设备的用户访问卡巴斯基的信誉数据库以及其他统计数据，而无需从他们的设备向卡巴斯基发送数据。KPSN 专为因例如以下原因而无法使用卡巴斯基安全网络的企业客户所设计：
  - 本地工作场所没有连接到互联网
  - 法律禁止或公司安全限制将任何数据发送到国家或组织的本地网络之外

要在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。

## 卡巴斯基安全网络使用选项：

使用 KSN 有两个选项：

- **扩展 KSN 模式** – 您可以从卡巴斯基知识库接收信息，同时 Kaspersky Endpoint Security 会自动向卡巴斯基安全网络发送操作期间获得的统计信息。该应用程序还可以发送给卡巴斯基，针对入侵者可用于损害设备或数据的其他某种文件（或部分文件）进行扫描。
- **基本 KSN 模式** – 您可以从卡巴斯基知识库接收信息，但 Kaspersky Endpoint Security 不会发送有关威胁类型和来源的匿名统计信息和数据。

您可以选择通过 Web Console、管理控制台或命令行来使用卡巴斯基安全网络。

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。

## Kaspersky Endpoint Security 的云模式

*云模式*是 Kaspersky Endpoint Security 的一种运行模式，使用轻量级版本的恶意软件数据库。这样有助于减少设备内存的负荷。

卡巴斯基安全网络有助于应用程序使用轻量级反恶意软件数据库。

如果 Kaspersky Endpoint Security 在标准模式下运行并使用 KSN，则可以启用云模式。

如果 Kaspersky Endpoint Security 在用于保护虚拟环境的 Light Agent 模式下运行，则不支持轻量级反恶意软件数据库。该应用程序从 Protection Server 接收 Light Agent 操作所需的特殊数据库。

启用云模式并执行应用程序数据库和模块的最新更新后，Kaspersky Endpoint Security 将切换为使用轻量级版本的恶意软件数据库。如果禁用云模式，Kaspersky Endpoint Security 会在下次更新应用程序数据库和模块时从卡巴斯基服务器下载完整版本的应用程序数据库。

如果不使用 KSN 或禁用云模式，Kaspersky Endpoint Security 将使用完整版本的应用程序数据库。

如果禁用 KSN，将自动禁用云模式。

## 使用 KSN 代理服务

由管理服务器管理的用户设备可以直接或通过管理服务器上的 KSN 代理服务与 KSN 通信。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，KSN 代理服务将支持与 KSN 基础架构的通信。不支持与 KSN 直接通信。如果 KSN 代理不可用，则应用程序不会使用 KSN。

KSN 代理服务器提供以下功能：

- 用户设备可查询 KSN 并将信息提交给 KSN，甚至无需访问互联网即可实现。
- KSN 代理服务器会缓存已处理的数据，从而降低外部网络连接的负载，并提高用户设备所请求信息的接收速度。

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”。

如果您在标准模式下使用 Kaspersky Endpoint Security，则可以使用 Kaspersky Security Center Web Console 或管理控制台配置以下 KSN 代理服务器设置：

无法通过命令行管理 KSN 代理设置。

在 Kaspersky Security Center 中，您可以配置以下设置以供 Kaspersky Endpoint Security 使用 KSN 代理服务器：

- 启用或禁用管理服务器作为 KSN 代理服务器。
- 如果 KSN 代理服务不可用，则允许或拒绝与 KSN 服务器的直接交互。

# 在 Web Console 中配置使用卡巴斯基安全网络。

在 Web Console 中，您可以在策略属性中配置应用程序使用卡巴斯基安全网络（**应用程序设置** → **常规设置** → **卡巴斯基安全网络**）。

Kaspersky Security Center 通过“*资产（设备）*”选项卡上的受管理设备列表中的客户端设备状态（**正常、严重、警告**）显示有关 KSN 可用性的信息。

# 在管理控制台中配置使用卡巴斯基安全网络。

在管理控制台中，您可以在策略属性中配置 Kaspersky Endpoint Security 对卡巴斯基安全网络的使用（在管理控制台中管理策略，使用管理控制台创建策略）（**高级威胁防护** → **卡巴斯基安全网络**）。

您可以在“卡巴斯基安全网络声明”窗口中阅读**卡巴斯基安全网络声明**的文本，单击**卡巴斯基安全网络声明**链接即可打开该窗口。

Kaspersky Security Center 通过“**设备**”选项卡上的受管理设备列表中的客户端设备状态（*正常*、*严重*、*警告*）显示有关 KSN 可用性的信息。

卡巴斯基安全网络设置

| 设置 | 描述 |
| --- | --- |
| **卡巴斯基安全网络声明** | 单击此链接将打开“**卡巴斯基安全网络声明**”窗口。在此窗口中，可以阅读卡巴斯基安全网络声明的文本。 |
| **卡巴斯基安全网络 (KSN)** | 该块显示有关 KSN 模式的信息或指示 Kaspersky Endpoint Security 未使用 KSN。<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** | 该复选框用于启用或禁用 Kaspersky Endpoint Security 使用轻量级版本恶意软件数据库的运行模式。<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。 |

| 设置 | 描述 |
| --- | --- |
| **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。在用于保护虚拟环境的 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。 |

# 在命令行中配置使用卡巴斯基安全网络

您可以使用常规应用程序设置中的 UseKSN 选项，在命令行中启用或禁用对卡巴斯基安全网络的使用。

您可以借助命令行开关或包含所有常规应用程序设置的配置文件来更改 UseKSN 的值。

*要借助命令行开关启用对卡巴斯基安全网络的使用，请运行：*

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

其中：

- <Extended/Basic>：卡巴斯基安全网络模式。
- --accept-ksn：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 <配置文件路径> [--json] [--accept-ksn]
```

其中：

- --file <配置文件路径> 是包含常规应用程序设置的配置文件的完整路径，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`。

# 使用命令行检查与卡巴斯基安全网络的连接

*要检查与卡巴斯基安全网络的连接，请运行以下命令：*

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

“**使用卡巴斯基安全网络**”行显示了与卡巴斯基安全网络的连接状态：

- 如果显示扩展 `KSN` 模式，Kaspersky Endpoint Security 将使用卡巴斯基安全网络，可以从知识库获取信息，并发送有关威胁类型和来源的匿名统计数据和信息。
- 如果显示基本 `KSN` 模式，Kaspersky Endpoint Security 将使用卡巴斯基安全网络，可以从知识库获取信息，但是不会发送有关威胁类型和来源的匿名统计数据和信息。
- 如果状态为“已禁用”，则表明 Kaspersky Endpoint Security 未使用卡巴斯基安全网络。

“**卡巴斯基安全网络基础架构**”行显示有关用于与卡巴斯基信誉数据库配合使用的基础架构解决方案的信息：卡巴斯基安全网络或卡巴斯基私人安全网络。

下列原因可导致无法连接到卡巴斯基安全网络：

- 用户设备未连接互联网。
- 卡巴斯基安全网络被禁用。
- 程序尚未激活或授权许可已过期。
- 检测到与授权许可密钥有关的问题。例如，密钥在拒绝列表中。

# 从命令行启用和禁用云模式

*云模式*是 Kaspersky Endpoint Security 的一种运行模式，使用轻量级版本的恶意软件数据库。

> 如果 Kaspersky Endpoint Security 在用于保护虚拟环境的 Light Agent 模式下运行，则不支持轻量级反恶意软件数据库。该应用程序从 Protection Server 接收 Light Agent 操作所需的特殊数据库。

您可以在常规应用程序设置中借助“`CloudMode=Yes/No`”选项在命令行中启用或禁用云模式。

您可以使用包含所有常规应用程序设置的配置文件或使用命令行选项来编辑设置 `CloudMode` 的值。

> 如果启用对卡巴斯基安全网络的使用，则云模式可用。

# 高级应用程序设置

您可以配置以下附加应用程序设置：

- 应用程序的代理服务器。
- 全局排除– 将挂载点从文件威胁防护、反加密勒索软件和容器监控组件以及关键区域扫描、容器扫描和可移动驱动器扫描任务的文件操作拦截中排除。
- 从扫描中排除进程内存。
- 文件操作拦截模式。
- 检测威胁入侵者可以用来破坏设备或数据的合法应用程序。
- 应用程序稳定性监控。
- 应用程序启动设置。
- 扫描任务的内存和处理器资源使用限制。
- 应用程序对驻留内存的使用限制。
- 非特权用户可以同时启动的“自定义扫描”任务数量限制。
- 将数据传输至 Kaspersky Security Center 存储的设置。
- 任务管理权限。
- 设备使用电池供电时取消计划任务。
- 系统事件拦截设置。
- 遥测附加设置。

# 配置代理服务器

如果客户端设备的用户使用代理服务器连接到互联网，您可以配置代理服务器设置。Kaspersky Endpoint Security 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。您可以启用管理服务器作为代理服务器，以便在 Web Console 或管理控制台中访问激活服务器。

您可以在 Web Console、管理控制台或命令行中为代理服务器配置以下排除项：

- 对于提供与 Detection and Response 解决方案集成的 EDR Expert（本地部署）、NDR (KATA) 和 Sandbox 组件。您可以指定必须绕过代理服务器的组件。
- 对于网址。您可以指定要绕过代理服务器进行连接的地址列表。

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。也不支持将 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。

# 在 Web Console 中配置代理服务器设置

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **网络设置**）中配置代理服务器设置。

# 在管理控制台中配置代理服务器设置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置** → **代理服务器设置**）中管理代理设置。

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。 |

| 设置 | 描述 |
| --- | --- |
| **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保护虚拟环境，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-premise)** 当连接到提供与 Kaspersky Endpoint Detection and Response Expert (on-premise) 或 Kaspersky Endpoint Detection and Response (KATA) 进行集成的服务器时，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**和**删除**地址。<br>单击**删除**按钮会将所选范围排除在扫描范围之外。<br>如果在表中选择至少一个扫描范围，则此按钮可用。<br>所选元素的设置在单独的窗口中更改。<br>单击**添加**按钮将打开一个窗口，您可以在其中指定新项目设置。 |

# 在命令行中配置代理服务器设置

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 设置允许您按以下格式指定代理服务器设置：< 连接协议 >://[< 用户 >[:< 密码 >]@]< 代理服务器地址<code class="programcharacter">a>:<</code>端口号 >，其中：

- < 用户 >是用于在代理服务器上进行身份验证的用户名。
- < 密码 >是用于在代理服务器上进行身份验证的用户密码。
- < 代理服务器地址 >是代理服务器的 IP 地址或域名。
- < 端口号 >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 < 地址 >[:< 端口号 >] 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）。

以下设置可让您配置 EDR Expert (on-premise)、NDR（KATA）和 Sandbox 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：

- ProxyBypassEdr 设置可启用或禁用当连接到提供与 Kaspersky Endpoint Detection and Response Expert (on-premise) 或 Kaspersky Endpoint Detection and Response (KATA) 进行集成的服务器时使用代理服务器。
- 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。

# 配置全局排除项

您可以配置文件威胁防护和反加密勒索组件的从文件操作拦截中排除挂载点，以及将这些挂载点按恶意软件扫描、关键区域扫描和容器扫描任务从扫描中排除。通过排除挂载点，您可以将挂载在设备上的本地或远程目录排除在文件操作拦截范围之外。此外，全局排除会影响容器监控组件（容器扫描、容器监控）和可移动驱动器扫描任务的运行。

## 在 Web Console 中配置全局排除项

在 Web Console 中，您可以在策略属性（**应用程序设置 → 受信任区域 → 受信任的挂载点**）中配置全局排除。

# 在管理控制台中配置全局排除项

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置 → 全局排除**）中管理全局排除。

**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>您可以用 * （星号）字符来创建文件或目录名称掩码。<br>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`。<br>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**/`。<br>** 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。<br>要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。<br>掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。<br>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。<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。 |

# 在命令行上配置全局排除

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。

`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:<` 文件系统类型 `>` – 从文件操作拦截中排除具有指定文件系统类型的所有已挂载目录。
- `/mnt` – 从文件操作拦截中排除 /mnt 挂载点（包括子目录）中的对象。此目录用作可移动驱动器的临时挂载点。
- `<` 包含 `/mnt/user*` 或 `/mnt/**/user_share>` 掩码的路径 – 从文件操作拦截中排除名称包含指定 **掩码** 的挂载点中的对象。

  您可以用 `*`（星号）字符来创建文件或目录名称掩码。

  您可以指定单个 `*` 字符来表示文件或目录名称中 `/` 字符前面的任意一组字符（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

  您可以指定两个连续的 `*` 字符来表示文件或目录名称中的任意一组字符（包括空集和 `/` 字符）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

  `**` 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

  要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。

  掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。

  可以使用单个 `?` 字符表示文件名或目录名中的任意一个字符。

> 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。

# 从扫描中排除进程内存

您可以配置进程内存的扫描排除项。应用程序不扫描指定进程的内存。

## 在 Web Console 中配置排除项

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **性能**）中配置从扫描中排除进程内存。

## 在管理控制台中配置排除项

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置 → 排除进程内存**）中管理进程内存排除项。

单击“**从扫描中排除进程内存**”下的“**配置**”将打开一个窗口，您可以在其中创建排除项列表。

“**从扫描中排除进程内存**”窗口中的列表包含应用程序从进程内存扫描中排除的进程的路径。您可以使用**掩码**指定路径。默认情况下，该列表为空。

您可以用 * （星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

要排除挂载点 `/dir`，您需要明确指定 `/dir`（无星号）。

掩码 `/dir/*` 会排除 `/dir` 下面级别的所有挂载点，但不会排除 `/dir` 本身。掩码 `/dir/**` 会排除 `/dir` 级别下面的所有挂载点，但不会排除 `/dir` 本身。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

您可以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。

## 在命令行中配置排除项

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。

`MemScanExcludedProgramPath.item_#` 包含本地目录中进程的完整路径。您可以使用**掩码**指定路径。

您可以用 * （星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

您可以指定多个要从扫描范围中排除的进程。

# 选择文件操作拦截模式

文件操作拦截模式会影响文件威胁防护和设备控制组件。

- 在扫描期间，应用程序可以阻止对文件威胁防护组件正在扫描的文件的访问。默认阻止对文件的访问：对所扫描文件的任何访问都必须等到扫描结果出来。如果扫描未检测到文件中存在威胁，应用程序将允许访问该文件。检测到感染对象时，应用程序执行文件威胁防护组件的 **检测到威胁后的操作**（`ActionOnThreat`）设置中指定的操作。

  您可以选择不阻止对文件威胁防护组件正在扫描的文件的访问。在这种情况下，则执行异步扫描。

- 当设备控制组件决定是否可以授予对设备的访问权限时，应用程序可以阻止对设备上的文件的访问。默认阻止对文件的访问：对受管理设备上的任何文件的访问都必须等到扫描结果出来。如果扫描后设备控制允许访问包含文件的设备，应用程序将允许访问该文件。

  您可以禁用设备控制组件所监控的设备上的文件访问阻止功能。在这种情况下，设备控制将确定是否允许以异步模式访问设备。

如果未启用文件操作拦截的阻止模式，则无论配置何种模式，文件威胁防护、设备控制和执行防护保护组件均以通知模式运行。

## 在 Web Console 中配置

在 Web Console 中，您可以在策略属性中配置文件操作拦截模式（**应用程序设置** → **常规设置** → **检测设置**）。

## 在管理控制台中配置

在管理控制台中，您可以在策略属性中管理应用程序跟踪设置（在管理控制台中管理策略、使用管理控制台创建策略）（**常规设置** → **应用程序设置** → **文件操作拦截模式**部分）。

“**扫描期间阻止对文件的访问**”复选框用于启用或禁用在文件威胁防护和设备控制组件扫描文件时阻止对文件的访问。

默认情况下已选定该选框。

如果清除该复选框，则允许在扫描期间访问任何文件，并且扫描以异步模式运行。

## 在命令行中配置

您可以使用常规应用程序设置中的 `FileBlockDuringScan`设置，在命令行中配置文件操作拦截模式。

您可以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。

`FileBlockDuringScan` 参数可以采用以下值：

- `Yes`（默认值）– 在文件威胁防护和设备控制组件扫描文件期间阻止对文件的访问。
- `No` – 在扫描期间允许访问文件。允许请求任何文件，扫描异步完成。

> 这种文件操作拦截模式对系统性能影响较小，但是如果文件在应用程序对文件状态做出决定之前（例如）在扫描过程中更改其名称，则存在文件中的威胁不会被消除或删除的风险。

# 配置检测黑客可能用来危害的应用程序

您可以启用或禁用对入侵者可以用来破坏设备或数据的合法应用程序的检测。此类应用程序不一定具有恶意的目的，但可能会被黑客利用。关于入侵者可以用来破坏设备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。

## 在 Web Console 中配置

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **检测设置**）中管理入侵者可以用来破坏设备或数据的合法应用程序的检测设置。

## 在管理控制台中配置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置** → **应用程序设置**，**扫描设置**部分）中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。

“**检测入侵者可以用来破坏设备或数据的合法应用程序**”复选框用于启用或禁用对入侵者可以用来破坏用户设备或数据的合法应用程序的检测。

默认情况下已清空该复选框。

## 在命令行中配置

在命令行中，您可以通过在常规应用程序设置中使用 `DetectOtherObjects` 设置，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。

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。

`DetectOtherObjects` 参数可以采用以下值：

- `Yes`：启用对入侵者可以用来破坏设备或数据的合法应用程序的检测。
- `No`：不启用对入侵者可以用来破坏设备或数据的合法应用程序的检测。

# 启用应用程序稳定性监控

您可以启用或禁用 Kaspersky Endpoint Security 稳定性监控，此功能可让您跟踪应用程序异常终止的次数，并将应用程序不稳定运行的情况通知给管理员，此外还可用于管理监控设置。

## 在 Web Console 中配置

在 Web Console 中，您可以在策略属性（**应用程序设置** → 常规设置 → **性能**）中启用或禁用应用程序稳定性监控。

## 在管理控制台中配置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置** → **应用程序设置**，**高级应用程序设置**）中启用或禁用应用程序稳定性监控。

**启用应用程序稳定性监控**复选框可启用或禁用对 Kaspersky Endpoint Security 应用程序状态的监控。

默认情况下已清空该复选框。

> 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>*。

## 在命令行中配置

在命令行中，您可以使用 kesl.ini 配置文件中的 `TrackProductCrashes`、`ProductHealthLogFile`、`WarnThreshold`、`WarnAfter_#_crash` 和 `WarnRemovingThreshold` 设置来配置 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。

# 配置应用程序启动设置

您可以配置应用程序启动设置。

## 在 Web Console 中设置限制

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **用户交互**）中管理应用程序启动设置。

## 在管理控制台中设置限制

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置** → **应用程序设置**，**应用程序启动设置**）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。 |

## 在命令行中设置限制

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。

# 限制应用程序对驻留内存的使用

您可以配置应用程序的驻留内存使用限制。默认情况下，会自动设置限制。

## 在 Web Console 中设置限制

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **性能**）中管理常驻内存使用限制。

## 在管理控制台中设置限制

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置** → **应用程序设置**）中设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。

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。 |

## 在命令行中设置限制

在命令行中，您可以使用 kesl.ini 配置文件中的 `MaxMemory` 设置来配置常驻内存使用限制。

MaxMemory 参数可以采用以下值：

- off – 驻留集大小不受限制。
- < 值 >% – 介于 RAM 的 1% 到 100% 之间的值。
- < 值 >MB – 以 MB 为单位的值。
- lowest/< <值> >%/< <值> >MB – 百分比值和以 MB 为单位的绝对值中的较小值。
- highest/< 值 >%/< 值 >MB – 百分比值和以 MB 为单位的绝对值中的较大值。
- auto – 最多 50% 的可用内存，但不少于 2 GB 且不超过 16 GB。

默认值： auto。

# 限制内存和处理器资源的使用

您可以配置扫描任务的内存使用限制。默认限制为 8192 兆字节。

> 我们建议为扫描任务指定低于驻留内存使用限制的内存使用限制，以避免扫描任务耗尽所有可用内存，导致应用程序重启。

您可以设置扫描任务的 CPU 使用率限制。默认不设置限制。配置限制时，我们建议牢记所有 CPU 核心的资源总和为 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%。如果希望在同一个 10 核 CPU 上， top实用程序报告的值保持在 150% 以下，则需要指定15作为 CPU 使用率限制。CPU 使用率限制必须是 10 到 100 之间的整数。此外，CPU 使用率限制并不适用于所有应用程序任务，而仅适用于*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。

## 在 Web Console 中设置限制

在 Web Console 中，您可以在策略属性中管理扫描任务的限制 CPU 和内存使用量的设置（**应用程序设置** → **常规设置** → **性能**）。

## 在管理控制台中设置限制

在管理控制台中，您可以在策略属性中启用或禁用 CPU 使用率限制，并为扫描任务配置 RAM 限制（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置** → **应用程序设置**，**性能**部分）。

单击“**性能**”下的“**配置**”将打开“**扫描任务的性能设置**”窗口，您可以在其中配置 **CPU 和内存使用**部分的限制（见下表）。

| 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，则这些任务在所有 CPU 核心上的最大负载将保持在右侧字段中指定的百分比值以下（所有 CPU 核心的最大总负载视为 100%）。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。 |

### 在命令行中设置限制

在命令行中，您可以使用常规应用程序设置中的 `UseOnDemandCPULimit` 和 `OnDemandCPULimit` 设置，为 *ODS*、*ContainerScan* 和 *InventoryScan* 任务配置 CPU 使用率限制。

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。

`UseOnDemandCPULimit` 参数可以采用以下值：

- `Yes`：启用*ODS*、*ContainerScan*和*InventoryScan* 类型任务的 CPU 使用率限制。
- `No`：禁用任务的 CPU 使用率限制。

`OnDemandCPULimit` 选项设置运行 *ODS*、*ContainerScan* 和 *InventoryScan* 任务时所有处理器核心的最大利用率级别（以百分比表示）。设置的值必须是 10 到 100 之间的整数。默认值：100。

在命令行中，您可以使用kesl.ini 配置文件中的 `ScanMemoryLimit` 设置，为 *ODS*、*ContainerScan* 和 *InventoryScan* 任务配置内存使用限制。默认值：8192。

# 限制“自定义扫描”任务的数量

您可以对非特权用户能够在设备上同时运行的自定义扫描任务的数量设置限制。具有 root 权限的用户可以运行的任务数量没有限制。

### 在管理控制台中设置限制

在管理控制台中，您可以在策略属性中配置非特权用户可在设备上同时运行的自定义扫描任务数量限制（在管理控制台中管理策略、使用管理控制台创建策略）（**常规设置** → **应用程序设置**，**性能**部分）。

单击**性能**部分中的**配置**按钮将打开**扫描任务的性能设置**窗口，您可以在其中**自定义扫描任务数量**部分的**自定义扫描任务的最大数量**字段中指定一个从 0 到 100,000 的值。默认值：0。如果指定为 0，则非特权用户将无法启动自定义扫描任务。

### 在命令行中设置限制

您可以使用应用程序常规设置中的 `LimitNumberOfScanFileTasks` 设置在命令行上配置并发自定义扫描任务的数量限制。

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。

`LimitNumberOfScanFileTasks` 接受 0 到 100000 之间的值。如果指定为 0，则非特权用户将无法启动自定义扫描任务。默认值：5。

# 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。

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 Web Console（**操作 →存储库→隔离区**）和管理控制台（**高级 →存储库→隔离区**）中获取。

客户端设备上由卡巴斯基应用程序放置在备份中的文件的常规列表保存在 Kaspersky Security Center 中，可在 Web Console（**高级→存储库→备份**）和 Web Console（**操作→存储库→备份**）中获取。

有关未处理文件的信息显示在 Web Console（**操作 → 存储库 → 活动威胁**）和管理控制台（**高级 → 存储库 → 活动威胁**）中的活动威胁列表中。

有关安装在客户端设备上或连接到客户端设备的设备的信息显示在 Web Console（**操作 → 存储库 → 硬件**）和管理控制台（**高级 → 存储库 → 硬件**）的硬件列表中。如果启用了设备控制，则会传输数据。

关于在客户端设备上发现的应用程序的信息显示在 Web Console 中的应用程序列表中（**操作 → 第三方应用程序 → 应用程序注册表**）和管理控制台（**高级 → 应用程序管理 → 应用程序注册表**）中。如果启用了应用程序控制，则会传输数据。

### 在 Web Console 中启用或禁用数据传输

在 Web Console 中，您可以在策略属性中管理管理服务器集成设置（**应用程序设置 → 常规设置 → KSC 整合**，**到管理服务器的数据传输**部分，**高级设置**链接），以及在受管理设备的属性中进行管理（**资产（设备） → 受管理设备** → <device name> 链接 → **应用程序**选项卡 → <Kaspersky Endpoint Security application name> 链接 → **应用程序设置**选项卡 → **存储设置**部分，**向管理服务器传输数据的设置**部分）。

Web Console 策略属性中向管理服务器传输数据的设置如附录 5 所述。

下表描述了受管理设备属性中数据传输到管理服务器的设置。

设备属性中的数据传输到管理服务器的设置

| 设置 | 描述 |
| --- | --- |
| **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。<br>默认情况下已清空该复选框。 |
| **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。<br>默认情况下已清空该复选框。 |
| **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。<br>默认情况下已清空该复选框。 |
| **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。<br>默认情况下已清空该复选框。 |
| **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。<br>默认情况下已清空该复选框。 |

### 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（在管理控制台中管理策略，使用管理控制台创建策略）（**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。 |

# 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（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。

### 在 Web Console 中配置

在 Web Console 中，您可以在策略属性中管理查看和管理任务的权限设置（**应用程序设置 → 常规设置 → 用户交互**）。

### 在管理控制台中配置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**本地任务 → 任务管理**）中管理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。 |

# 使用电池供电时取消任务

您可以启用或禁用使用电池供电时取消计划任务的功能。取消计划任务可以减少资源消耗，延长电池寿命。

如果启用了取消计划任务并且设备使用电池供电，Kaspersky Endpoint Security 将取消以下计划任务：

- 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）
- 清查
- 数据库和应用程序模块更新
- IOC 扫描
- 系统完整性检查

您可以根据需要手动运行任务。

### 在 Web Console 中配置

在 Web Console 中，您可以在策略属性中配置计划任务的取消（**应用程序设置** → **常规设置** → **Performance**）。

### 在管理控制台中配置

在管理控制台中，您可以在策略属性中管理计划任务的取消（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置** → **应用程序设置**，**性能**）。

“**使用电池供电时跳过计划任务**”复选框用于启用或禁用取消计划任务。

默认情况下已选定该选框。

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。

### 在命令行中配置

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。

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。

`PowerSaveMode` 参数可以采用以下值：

- `Yes`（默认值）：当设备使用电池供电时会跳过计划任务。
- `No`：无论设备是否使用电池供电，都会运行计划任务。

# 配置系统事件拦截

为确保正常运行，应用程序必须拦截系统事件，即文件操作和进程启动。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。

如果设备的操作系统支持 fanotify，您可以选择应用程序用来拦截系统事件的机制：

- 基于 fanotify 的系统拦截机制。默认使用此机制。
- 基于*可更新内核模块*的拦截机制。使用可更新内核模块能够优化 Kaspersky Endpoint Security 对文件操作的拦截和启动进程的拦截。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。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。

  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。

  可更新内核模块包含在应用程序的分发包中。

对于不支持 fanotify 的操作系统，无法选择拦截机制。该应用程序使用特殊的内核模块来拦截系统事件以提供文件威胁防护功能。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)。
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)。
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8)。

  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 Stream 8。
- Debian GNU/Linux 12.0。
- Red Hat Enterprise Linux 7.4。
- Red Hat Enterprise Linux 8.10。
- SberLinux 8.10。
- SberLinux 9.1。
- SberLinux 9.6。
- SberLinux 9.7。
- SberOS 3.4。
- SberOS 3.5。
- 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 版本 11。
- ALT SP Server 版本 11。

- ALT Education 11。
- RED OS 7.3。
- RED OS 8。
- ROSA "Cobalt" 7.9 Workstation。
- ROSA "Cobalt" 7.9 Server。
- ROSA "Chrome" 12 Workstation。
- ROSA "Chrome" 12 Server。

不支持 32 位操作系统和 Arm 架构的操作系统。

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。

您可以使用卡巴斯基 ULKM 工具来检查设备是否满足安装可更新内核模块的要求。

如果您的操作系统满足要求，您可以在安装应用程序时根据可更新内核模块选择拦截方法。这将安装可更新内核模块。如果您的操作系统获得支持，您也可以稍后安装可更新内核模块。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。您可以在 **Web Console**、管理控制台或**命令行**中选择系统事件拦截机制。

   在命令行中，可以使用 `InterceptorMode`、`InterceptorFallbackStrategy` 和 `InterceptorApplyStrategy` 常规应用程序设置来配置系统事件拦截。

   只有在操作系统支持 fanotify 技术的设备上才会显示和可以编辑这些设置。

   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。

   `InterceptorMode` 用于选择应用程序使用的系统事件拦截机制。设置可以使用以下值：

   - `UseFanotify` 用于使用 fanotify 技术拦截系统事件。
   - `UseUpdatableKernelModule` — 用于通过可更新内核模块来拦截系统事件。

   如果选择了可更新内核模块，则应用 `InterceptorFallbackStrategy` 设置。此设置用于指定当可更新内核模块启动失败时应用程序执行的操作。设置可以使用以下值：

   - 如果可更新内核模块启动失败，`FallbackToFanotify` 会将系统事件拦截机制切换成 fanotify。
   - 如果可更新内核模块启动失败，`FallbackToLimitedMode` 会关闭系统事件拦截。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。

如果选择了可更新内核模块，则应用 `InterceptorApplyStrategy` 设置。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：

- `RestartServiceAutomatically` 自动重启应用程序以启动可更新内核模块。
- `RestartServiceManually` 会在用户手动重启应用程序后，启动可更新内核模块。

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。

在 Web Console 中，您可以在策略属性中配置系统事件拦截（**应用程序设置 → 常规设置 → 操作系统交互设置**）。

这些设置仅适用于运行支持 fanotify 技术的操作系统的设备。

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。

为了使应用程序正常工作，必须在应用程序自动重启后切换到使用可更新内核模块。

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。

您可以通过以下方式查看设备上的可更新内核模块的状态和可用性信息：

- 在 Web Console 或管理控制台中，查看**可更新内核模块**功能组件的状态。
- 在命令行中，在 `kesl-control --app-info` 命令的输出中。

关于可更新内核模块状态的信息以状态的形式显示：

- “**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，模块没有运行。

# 检查是否可以安装可更新内核模块

您可以使用卡巴斯基 ULKM 工具来检查设备是否满足安装可更新内核模块的要求。

*要使用 Kaspersky Security Center Web Console 或管理控制台运行此工具：*

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。

**如何安装网络代理**

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。

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的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。

   有关远程安装过程的说明，请参阅 Kaspersky Security Center 帮助。

   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。
- *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。

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。

# 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。

*若要禁用应用程序的“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
   ```

# 在 Web Console 中管理拦截设置

在 Web Console 中，您可以在策略属性中配置系统事件拦截（**应用程序设置 → 常规设置 → 操作系统交互设置**）。

这些设置仅适用于运行支持 fanotify 技术的操作系统的设备。

# 在管理控制台中管理拦截设置

在管理控制台中，您可以在策略属性中管理系统事件拦截设置（在管理控制台中管理策略、使用管理控制台创建策略）（**常规设置 → 操作系统交互设置**、**系统事件拦截设置**）。

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。 |

# 使用命令行来管理拦截设置

在命令行中，可以使用 `InterceptorMode`、`InterceptorFallbackStrategy` 和 `InterceptorApplyStrategy` 常规应用程序设置来配置系统事件拦截。

只有在操作系统支持 fanotify 技术的设备上才会显示和可以编辑这些设置。

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。

`InterceptorMode` 用于选择应用程序使用的系统事件拦截机制。设置可以使用以下值：

- `UseFanotify` 用于使用 fanotify 技术拦截系统事件。
- `UseUpdatableKernelModule` — 用于通过可更新内核模块来拦截系统事件。

如果选择了可更新内核模块，则应用 `InterceptorFallbackStrategy` 设置。此设置用于指定当可更新内核模块启动失败时应用程序执行的操作。设置可以使用以下值：

- 如果可更新内核模块启动失败，`FallbackToFanotify` 会将系统事件拦截机制切换成 fanotify。
- 如果可更新内核模块启动失败，`FallbackToLimitedMode` 会关闭系统事件拦截。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。

如果选择了可更新内核模块，则应用 `InterceptorApplyStrategy` 设置。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：

- `RestartServiceAutomatically` 自动重启应用程序以启动可更新内核模块。
- `RestartServiceManually` 会在用户手动重启应用程序后，启动可更新内核模块。

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。

# 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。

## 在 Web Console 中配置

在 Web Console 中，您可以在策略属性中管理高级遥测设置（**应用程序设置 → 常规设置 → 操作系统交互设置**）。

## 在管理控制台中配置

在管理控制台中，您可以在策略属性中管理其他遥测设置（在管理控制台中管理策略、使用管理控制台创建策略）（**常规设置 → 操作系统交互设置**，**遥测附加设置**）。

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。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |

## 在命令行中配置

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。

您可以通过以下方式更改设置：使用 `kesl-control --set-settings 20` 命令，编辑包含任务所有设置的配置文件，或者使用 < 设置名称 >=< 设置值 > 格式的命令行选项。

`TelemetrySource` 设置可让您指定遥测源。设置可以使用以下值：

- `Default`（默认）表示使用 eBPF 技术和 auditd 服务来获取遥测数据。
- `OnlyEBPF` 表示仅使用 eBPF 技术获取遥测数据。

`UseTelemetryMonopolyMode` 设置可让您指定 auditd 服务（如果用于获取遥测数据）的使用模式。设置可以使用以下值：

- `True`（默认值）表示 Kaspersky Endpoint Security 以独占模式使用 auditd 服务。
- `False`表示 auditd 服务以非独占模式使用。

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。

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。该目录还存储被隔离的文件。您可以使用命令行更改存储备份和隔离对象的目录。

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。

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管理备份设置。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。
- 最大备份容量。默认情况下，备份的大小不受限制。

存储备份和隔离对象的目录路径（只能在命令行上配置）。

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。

Kaspersky Security Center 会生成客户端设备上由卡巴斯基应用程序放置在备份中的文件的一般列表，该列表可在管理控制台（**高级→存储库→备份**）和 Web Console（**操作→存储库→备份**）中查看。您可以查看受保护设备上备份存储中的文件的属性，并从中删除文件。Kaspersky Security Center 不会将文件从备份复制到管理服务器；所有文件都存储在受保护设备上的备份中。文件恢复在受保护的设备中进行。

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。

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。

# 在 Web Console 中配置备份设置

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **报告和存储**）和受管理设备属性（**资产（设备）** → **受管理设备** → <device name> 链接 → **应用程序**选项卡 → <Kaspersky Endpoint Security application name> 链接 → **应用程序设置**选项卡 → **存储设置**部分）中管理备份区设置。

Web Console 策略属性中的备份区设置详见附录 5。

下表描述了受管理设备属性中的备份区设置。

设备属性中的备份区设置

| 设置 | 描述 |
| --- | --- |
| **存储对象不超过 (天)** | 用于指定对象在备份存储内的存储期限的输入字段。<br>可用值：1-10000。如果清除该复选框，则在备份中存储对象的期限将不受限制。<br>默认值：30。 |
| **备份大小限制为 (MB)** | 用于指定备份存储的最大容量 (MB) 的输入字段。<br>如果清除该复选框，则备份的大小将不受限制。<br>默认值：1024。 |

# 在管理控制台中配置备份设置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略、使用管理控制台创建策略）（**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。

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：1-999999。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。 |

# 使用命令行配置备份区设置

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。

| 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 999999<br>0 — 无限制容量。<br>默认值：0。 |
| `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。 |

# 在命令行上操作备份区对象

您可以在命令行中使用备份管理命令对备份对象执行以下操作：

- 查看备份对象详细信息。
- 从备份中删除部分或全部对象。
- 从备份中恢复对象。

恢复受感染的对象可能会导致设备感染。

## 查看备份对象详细信息

*要查看备份中对象的详细信息，请运行：*

```
kesl-control -B --query ["< 过滤条件 >"] [-n < 数量 >] [--json]
```

其中：

- < 过滤条件 > 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，应用程序将显示备份中的所有对象的详细信息。
- < 数量 > 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。

## 从备份中恢复对象

*要将对象以其原始名称还原到其原始位置，请执行以下命令：*

```
kesl-control -B --restore <对象 ID>
```

其中 <对象 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 <对象 ID> --file <文件路径>
```

其中 --file <文件路径> 是文件的新名称以及要将其保存到的目录路径。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。

## 从备份中删除对象

*要从备份中移除所选对象，请运行：*

```
kesl-control -B --mass-remove --query "<过滤条件>"
```

其中 <过滤条件> 是一个或多个逻辑表达式，格式为 <字段> <比较运算符> '<值>'，并借助逻辑运算符 and 组合以限制结果。

例如：
*要移除 ID=15 的对象，请执行以下操作：*

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

*要移除名称或路径中包含“test”的对象：*

```
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

*要从备份中移除所有对象，请运行：*

```
kesl-control -B --mass-remove
```

# 与 Detection and Response 解决方案整合

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，可让您管理对检测的响应。

Kaspersky Endpoint Security 可与以下 Kaspersky Detection and Response 解决方案进行互操作：

- Kaspersky Endpoint Detection and Response Expert（本地部署）在 Open Single Management Platform (OSMP) 上。集成由 Kaspersky Endpoint Security 应用程序组件 Endpoint Detection and Response Expert (本地部署）（以下简称*EDR Expert (本地部署)*）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 (本地部署)（以下简称*EDR Expert (本地部署)*）。
  - 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。

如果您在Kaspersky Endpoint Detection and Response 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（本地部署）以及 Kaspersky Anti Targeted Attack Platform 上的 Kaspersky Endpoint Detection and Response 和 Kaspersky Network Detection and Response 组件集成。

如果 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 集成，可以将大量事件写入 systemd 日志。如果要禁用将审计事件记录到 systemd 日志，请禁用 systemd-journald-audit 套接字并重新启动操作系统。

*要禁用 systemd-journald-audit 套接字，请运行以下命令：*

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket

systemctl mask systemd-journald-audit.socket
```

默认情况下，在 SintezM-Client 操作系统中，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-premise) 正确集成的参考镜像

# 关于基于 Detection and Response 解决方案命令的威胁响应操作

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（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，网络隔离在 Detection and Response 解决方案端被启用或禁用。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（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务在 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（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，威胁响应操作在 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 Kaspersky Endpoint Detection and Response（本地部署）或者 Kaspersky Endpoint Detection and Response (KATA) 集成时，威胁响应操作在相关的 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（本地部署）或者 Kaspersky Endpoint Detection and Response (KATA) 集成时，威胁响应操作在相关的 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（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务在 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（本地部署）或者 Kaspersky Endpoint Detection and Response (KATA) 集成时，任务在 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（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务在 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（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务在 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。

  当与 Kaspersky Endpoint Detection and Response（本地部署）或者 Kaspersky Endpoint Detection and Response (KATA) 集成时，Kaspersky Endpoint Security 设备上的 IOC 扫描任务在相关的 Detection and Response 解决方案端创建并运行。

  与 Kaspersky Endpoint Detection and Response Optimum 集成时，使用 *IOC 扫描*任务执行 IOC 扫描。您可以手动创建 IOC 扫描任务。

- 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 扫描的命令在 Kaspersky Endpoint Detection and Response Expert（本地部署）解决方案端创建和运行。

- 执行防护

  当与 Endpoint Detection and Response Expert（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以启用执行防护规则。Kaspersky Endpoint Security 会阻止符合防护规则标准的对象执行操作或文档打开操作。

  当与 Kaspersky Endpoint Detection and Response Expert（本地）或 Kaspersky Endpoint Detection and Response (KATA) 集成时，应用程序会从 Kaspersky Endpoint Detection and Response Expert（本地部署）或 Kaspersky Endpoint Detection and Response (KATA) 接收执行防护规则。

  与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以在 Web Console 中配置执行防护规则。

- 获取取证信息。

  当与 Kaspersky Endpoint Detection and Response Expert（本地部署）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

  这些任务在 Kaspersky Endpoint Detection and Response Expert（本地部署）解决方案端创建和运行。

# Kaspersky Endpoint Detection and Response Expert (on-premise) 集成

Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise) 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-premise) 帮助。

与 Kaspersky Endpoint Detection and Response Expert (on-premise) 集成时，Kaspersky Endpoint Security 可以：

- 将关于设备上的事件的数据（遥测数据）发送到 OSMP 平台上的遥测服务器（以下简称*OSMP 遥测服务器*）。Kaspersky Endpoint Security 向遥测服务器发送有关进程、打开的网络连接和修改文件的监控数据，以及有关应用程序检测到的威胁的数据和处理这些威胁的结果数据。
- 根据从 OSMP 威胁响应服务器（以下简称OSMP 威胁响应服务器）收到的命令，执行旨在维护安全功能的*威胁响应操作*。

与 Kaspersky Endpoint Detection and Response Expert (on-premise) 解决方案的集成由 Kaspersky Endpoint Security 应用程序组件 Endpoint Detection and Response Expert (on-premise)（以下简称 *EDR Expert (on-premise)*）提供。

与 Kaspersky Endpoint Detection and Response Expert (on-premise) 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。为确保安全连接，使用 OSMP 服务器颁发的以下证书：

- 服务器证书。使用服务器的 TLS 证书对连接进行加密。您可以通过在 Kaspersky Endpoint Security 端验证服务器证书来提高连接的安全性。为此，请在启用与 Kaspersky Endpoint Detection and Response Expert (on-premise) 解决方案的集成之前添加服务器证书。
- 客户端证书。此证书用于通过双向身份验证（即 OSMP 服务器使用 Kaspersky Endpoint Security 应用程序来验证设备）提供额外的连接保护。多个设备可以使用同一客户端证书。默认情况下，服务器不验证客户端证书，但可以在 Kaspersky Endpoint Detection and Response Expert (on-premise) 端启用双向身份验证。在这种情况下，您需要在 EDR Expert (on-premise) 组件的设置中启用双向身份验证，并添加客户端证书（包含证书和私钥的加密容器）。

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。

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。

若要使用 Endpoint Detection and Response Expert (on-premise) 功能，您需要激活 EDR Expert (on-premise) 组件。如果您使用 Kaspersky Endpoint Security 所依据的主授权许可不包含 Kaspersky Endpoint Detection and Response Expert（本地部署）功能，则需要为此功能购买单独的授权许可，并将 EDR Expert（本地部署）授权许可密钥添加到该应用程序中。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，激活将通过向 SVM 添加授权许可密钥在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）上执行。

与 Kaspersky Endpoint Detection and Response Expert (on-premise) 集成包括以下步骤：

1. **启用所需的 Kaspersky Endpoint Security 组件**

   EDR Expert (on-premise) 组件可以使用来自以下组件的数据：

   - 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。

   要将 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (on-premise) 完全集成，您需要启用行为检测组件。如果禁用了行为检测，则不会传输必要的遥测数据（来自其他保护组件的同步请求和威胁检测数据除外）。

   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。

2. **激活 EDR Expert（本地部署）组件**

   确保满足以下条件之一：

   - 您正在使用包含 Kaspersky Endpoint Detection and Response Expert（本地部署）功能的授权许可来使用 Kaspersky Endpoint Security。
   - 您已购买使用 Kaspersky Endpoint Detection and Response Expert（本地部署）功能所需的单独授权许可，并将 EDR Expert（本地部署）授权许可密钥添加到应用程序中。

     如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟化环境，则需要向 SVM 添加用于激活附加功能的授权许可密钥。

3. **启用 EDR Expert（本地部署）组件**

   Kaspersky Endpoint Detection and Response Expert (on-premise) 集成默认处于禁用状态。要启用集成，您需要启用并配置 EDR Expert（本地部署）组件：

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

   不支持在 Kaspersky Security Center 的管理控制台中配置与 Kaspersky Endpoint Detection and Response Expert (on-premise) 的集成。

要与 Kaspersky Endpoint Detection and Response Expert (on-premise) 集成，您需要在 EDR Expert (on-premise) 组件的设置中选择 *EDR Expert (OSMP)* 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）** 。如果您使用命令行，请在任务设置中设置`Mode=EDRExpertOnPrem`。要在设备上配置与 Kaspersky Endpoint Detection and Response Expert (on-premise) 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"。

如果您希望对对象使用执行防护，可以启用 EDR Expert（本地部署）组件的对象执行保护规则。
您可以检查 EDR Expert (on-premise) 组件的状态：

- 使用 Web Console 中的*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 Web Console 的设备属性中（**资产（设备）** → **受管理设备** →<设备名称>链接→ **应用程序** →<Kaspersky Endpoint Security 应用程序名称>链接→ **常规** → **组件**）。

- 在命令行中运行 以下命令： `kesl-control --app-info`。

# 如何准备用于与 EDR Expert (on-premise) 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-premise) 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。

# 在 Web Console 中配置 Kaspersky Endpoint Detection and Response Expert（本地部署）集成

在 Web Console 中，您可以启用或禁用 EDR Expert（本地部署）组件，并在策略属性中管理Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert（本地部署）集成的设置（**应用程序设置 → 内置代理配置 → Endpoint Detection and Response Expert (on-premise)**）。

要与 Kaspersky Endpoint Detection and Response Expert（本地部署）集成，您需要启用 EDR Expert（本地部署）组件，并选择**Endpoint Detection and Response Expert（版本 8.0 或更高版本）**选项，即*EDR Expert (OSMP)* 集成模式。

对于 Kaspersky Endpoint Detection and Response Expert（本地部署）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（本地部署）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（本地部署）集成设置了。

# 透过命令行配置 Kaspersky Endpoint Detection and Response Expert（本地部署）集成

您可以在命令行中通过 *Kaspersky Endpoint Detection and Response（本地部署）(KATAEDR)* 预定义任务来管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Expert（本地部署）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（本地部署）集成，您需要选择 *EDR Expert (OSMP)* 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（本地部署）集成设置。

*Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise) 组件管理命令来管理用于连接到 OSMP 服务器的证书。

# Kaspersky Endpoint Detection and Response Expert（本地部署）集成设置

下表描述了*Kaspersky Endpoint Detection and Response Expert（本地部署）(KATAEDR) Integration*预定义任务的设置，您可以在与 Kaspersky Endpoint Detection and Response Expert（本地部署）集成时对其进行管理。

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（本地部署）集成，您需要在任务设置中选择*EDR Expert (OSMP)* 集成模式（`Mode=EDRExpertOnPrem`）。

Kaspersky Endpoint Detection and Response Expert（本地部署）集成设置

| 设置 | 描述 | 值 |
|---|---|---|
| `Mode` | 集成模式。<br>对于 Kaspersky Endpoint Detection and Response Expert (on-premise) 集成，Kaspersky Endpoint Security 应用程序与 OSMP 平台上的服务器进行交互。<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 (OSMP) 集成模式。启用 Kaspersky Endpoint Detection and Response Expert (on-premise) 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（本地部署）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` | 启用和禁用向 OSMP 遥测服务器发送事件数据（遥测数据）。 | `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（本地部署）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`。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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` | 启用或禁用仅发送包含攻击指标 (IOA) 的遥测数据。*攻击指标*是对组织 IT 基础架构中对象可疑行为的描述，可能是组织遭受定向攻击者攻击的迹象。 | `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` | 启用或禁用调节发送到 OSMP 遥测服务器的事件数量。 | `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 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 < 文件 > --server-type response
```

其中 < 文件 > 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 < 文件 > --server-type response
   ```

   其中 < 文件 > 是包含客户端证书和私钥的加密容器（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（本地部署）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 <文件> --server-type telemetry
```

其中 <文件> 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 <文件> --server-type telemetry
   ```

   其中 <文件> 是包含客户端证书和私钥的加密容器（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（本地部署）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
```

# 与 Kaspersky Anti Targeted Attack Platform 整合

Kaspersky Endpoint Security 与 Kaspersky Anti Targeted Attack Platform 解决方案兼容，旨在保护组织的 IT 基础设施并迅速检测威胁，例如零日攻击、针对性攻击和高级持续性威胁 (APT)。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 可以：
  - 将关于设备事件的信息（遥测数据）发送到提供 Kaspersky Endpoint Detection and Response (KATA) 交互功能的中央节点服务器（下文亦称“*KATA 服务器*”）。Kaspersky Endpoint Security 可向 Kaspersky Anti Targeted Attack Platform 上的 Central Node 服务器发送有关进程、打开的网络连接和修改文件的监控数据，以及有关应用程序检测到的威胁的数据和处理这些威胁的结果数据。
  - 在接收到 Kaspersky Anti Targeted Attack Platform 的命令时执行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。

- Kaspersky 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。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。当将 Kaspersky Endpoint Security 应用程序与 Kaspersky Anti Targeted Attack Platform 上的 Sandbox 集成时，该应用程序会将要扫描的文件发送到 Central Node 服务器，该服务器负责处理与 Sandbox 的交互。

与 Kaspersky Anti Targeted Attack Platform 上的组件的集成由 Kaspersky Endpoint Security 应用程序的以下组件提供：

- Endpoint Detection and Response Expert（本地部署）组件（以下简称*EDR Expert（本地部署）*）。

  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（本地部署）。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）集成，还提供与 Kaspersky Endpoint Detection and Response Expert（本地部署）解决方案集成。

- Network Detection and Response (KATA) 组件（下文亦称“*NDR (KATA)*”）。
- *Sandbox* 组件。

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。

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。为确保安全连接，使用 Central Node 服务器颁发的以下证书：

- 服务器证书。使用服务器的 TLS 证书对连接进行加密。您可以通过在 Kaspersky Endpoint Security 端验证服务器证书来提高连接的安全性。为此，在启用与 Kaspersky Anti Targeted Attack Platform 解决方案的集成之前，您需要添加服务器证书。
- 客户端证书。此证书用于通过双向身份验证（即 Central Node 服务器使用 Kaspersky Endpoint Security 应用程序验证设备）提供额外的连接保护。多个设备可以使用同一客户端证书。默认情况下，服务器不检查客户端证书，但可以在 Kaspersky Anti Targeted Attack Platform 端启用双向身份验证。在这种情况下，您需要在 EDR Expert (on-premise)、NDR (KATA) 或 Sandbox 组件的设置中启用双向身份验证，并添加客户端证书（包含证书和私钥的加密容器）。

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。

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。

要使用 Kaspersky Endpoint Detection and Response (KATA) 功能，您需要激活 EDR Expert（本地部署）组件。如果您使用 Kaspersky Endpoint Security 所依据的主授权许可不包含 Kaspersky Endpoint Detection and Response Expert（本地部署）功能，则需要为此功能购买单独的授权许可，并将 EDR Expert（本地部署）授权许可密钥添加到该应用程序中。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，激活将通过向 SVM 添加授权许可密钥在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）上执行。

设置与 Kaspersky Endpoint Detection and Response (KATA) 和 Kaspersky Network Detection and Response (KATA) 组件的集成涉及以下步骤：

1. **启用所需的 Kaspersky Endpoint Security 组件**

   EDR Expert（本地部署）和 NDR (KATA) 组件可以使用来自以下组件的数据：

   - 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。

为了将 Kaspersky Endpoint Security 应用程序与 Kaspersky Anti Targeted Attack Platform 正确整合，必须启用行为检测组件。如果禁用了行为检测，则不会传输必要的遥测数据（来自其他保护组件的同步请求和威胁检测数据除外）。

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。

### 2 激活 EDR Expert（本地部署）组件

要与 Kaspersky Endpoint Detection and Response (KATA) 集成，您需要激活 EDR Expert（本地部署）组件。确保满足以下条件之一：

- 您正在使用包含 Kaspersky Endpoint Detection and Response Expert（本地部署）功能的授权许可来使用 Kaspersky Endpoint Security。
- 您已购买使用 Kaspersky Endpoint Detection and Response Expert（本地部署）功能所需的单独授权许可，并将 EDR Expert（本地部署）授权许可密钥添加到应用程序中。

  如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟化环境，则需要向 SVM 添加用于激活附加功能的授权许可密钥。

您无需激活 NDR (KATA) 组件，因为Kaspersky Endpoint Security 的主授权许可已涵盖 Kaspersky Network Detection and Response (KATA) 集成功能。

### 3 启用 EDR Expert（本地部署）组件

默认情况下，Kaspersky Endpoint Detection and Response (KATA) 集成被禁用。要启用集成，您需要启用并配置 EDR Expert（本地部署）组件：

- 使用 Kaspersky Security Center Web Console。
- 使用 Kaspersky Security Center 管理控制台。
- 使用命令行。

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-premise) 组件的设置中选择 *EDR (KATA)* 集成模式。如果使用 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）** 。如果您使用命令行，请在任务设置中设置`Mode=EDRKATA`。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”。

如果您希望对对象使用执行防护，可以启用 EDR Expert（本地部署）组件的对象执行保护规则。

### 4 启用 NDR (KATA) 组件

默认情况下，Kaspersky Network Detection and Response (KATA) 集成被禁用。要启用集成，您需要启用并配置 NDR (KATA) 组件：

- 使用 Kaspersky Security Center Web Console。
- 使用 Kaspersky Security Center 管理控制台。
- 使用命令行。

您可以检查 EDR Expert（本地部署）和 NDR (KATA) 组件的状态：

- 使用 Web Console 中的*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 Web Console 的设备属性中（**资产（设备）** → **受管理设备** →<设备名称>链接→ **应用程序** →<Kaspersky Endpoint Security 应用程序名称>链接→ **常规** → **组件**）。
- 在命令行中运行 以下命令： `kesl-control --app-info`。

# 在 Web Console 中配置 Kaspersky Endpoint Detection and Response (KATA) 集成

在 Web Console 中，您可以在策略属性中管理Kaspersky Endpoint Detection and Response (KATA) 的集成设置（**应用程序设置** → **内置代理配置** → **Endpoint Detection and Response Expert (on-premise)**）。

要与 Kaspersky Endpoint Detection and Response (KATA) 集成，您需要启用 EDR Expert（本地部署）组件，并选择**Kaspersky Endpoint Detection and Response Expert（版本 7.1 或更早版本）**选项，即*EDR (KATA)*集成模式。

要应用在 Web Console 策略中为 Endpoint Detection and Response Expert (KATA) 组件的 **数据传输设置** 下指定的 **发送事件时的最大延迟时间（秒）** 设置值，您需要在策略属性中关闭 **数据传输设置** 和 **请求限流** 设置组的“锁”图标。要允许在设备本地修改 `MaximumDataTransferTime` 设置，在 EDR (KATA) 模式下 KATAEDR 任务的 `[EventTransferSettings]` 部分中，您需要在策略属性中解锁 **数据传输设置** 和 **请求限流** 设置组的“锁”图标。

# 在管理控制台中配置 Kaspersky Endpoint Detection and Response (KATA) 集成

在管理控制台中，您可以在策略属性中启用或禁用 EDR Expert (on-premise) 组件，并管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 组件的集成设置（在管理控制台中管理策略、使用管理控制台创建策略）（**Detection and Response** → **EDR Expert (on-premise)**）。

如果在 Web Console中为 EDR Expert（本地部署）组件选择了**Kaspersky Endpoint Detection and Response Expert（版本 8.0 及更高版本）**，即选择了 EDR Expert (OSMP) 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。

Kaspersky Endpoint Detection and Response (KATA) 集成设置

| 设置 | 描述 |
| --- | --- |
| **启用 Endpoint Detection and Response Expert (on-premise)** | 此复选框可启用或禁用 EDR Expert（本地部署）组件，该组件提供与 Kaspersky Endpoint Detection and Response (KATA) 进行集成。<br>默认禁用此组件。 |
| **启用对象执行防护** | 此复选框用于启用或禁用对象执行防护的 EDR Expert（本地部署）规则。 |

| 设置 | 描述 |
| --- | --- |
| **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。 |

| 设置 | 描述 |
| --- | --- |
| **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。如果存档受密码保护，请在"**加密容器密码**"字段中输入密码。<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`。 |

# 在命令行上配置 Kaspersky Endpoint Detection and Response (KATA) 集成

您可以在命令行中通过 *Kaspersky Endpoint Detection and Response (KATA) 集成(KATAEDR)* 预定义任务来管理 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response (KATA) 组件之间的集成。

此任务还可让您管理 Kaspersky Endpoint Detection and Response Expert (on-premise) 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，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配置Kaspersky Endpoint Detection and Response (KATA) 集成设置。

*Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise) 组件管理命令来管理用于连接到 KATA 服务器的证书。

# Kaspersky Endpoint Detection and Response (KATA) 集成设置

下表描述了Kaspersky Endpoint Detection and Response Expert（本地部署）(KATAEDR) Integration*预定义任务*的设置，您可以在与 Kaspersky Endpoint Detection and Response (KATA) 集成时对其进行管理。

此任务还可让您管理 Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise) 集成，Kaspersky Endpoint Security 应用程序与 OSMP 平台上的服务器进行交互。<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 (OSMP) 集成模式。启用 Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise) 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` | 启用和禁用向 KATA 发送事件数据（遥测数据）。 | `Yes`（默认值）– 向 KATA 服务器发送遥测数据。<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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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 < 文件 >
```

其中 < 文件 > 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 < 文件 >
   ```

   其中 < 文件 > 是包含客户端证书和私钥的加密容器（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 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-premise) 集成* 任务设置中，UseClientPinnedCertificate 被设为 yes，则客户端证书用于对与 KATA 服务器的连接进行额外保护。

*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
```

# 在 Web Console 中配置 Kaspersky Network Detection and Response (KATA) 集成

在 Web Console 中，您可以在策略属性中管理Kaspersky Network Detection and Response (KATA) 集成设置（**应用程序设置** → **内置代理配置** → **Network Detection and Response (KATA)**）。

要应用在 Web Console 的策略中为 Network Detection and Response (KATA) 组件的 **数据传输设置** 下指定的 **发送事件时的最大延迟时间（秒）** 设置值，您需要在策略属性中关闭 **数据传输设置** 和 **请求限流** 设置组的“锁”。要允许在设备本地修改 `MaximumDataTransferTime` 设置，您需要在 KATANDR 任务的 `[EventTransferSettings]` 部分中解锁策略属性中 **数据传输设置** 和 **请求限流** 设置组的“锁”。

# 在管理控制台中配置 Kaspersky Network Detection and Response (KATA) 集成

在管理控制台中，您可以在策略属性中启用或禁用 NDR (KATA) 组件，并管理 Kaspersky Endpoint Security 应用程序与 Kaspersky Network Detection and Response (KATA) 组件集成的设置（在管理控制台中管理策略，使用管理控制台创建策略）（**Detection and Response** → **Network Detection and Response (KATA)**）。

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`。 |
| **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`。 |

| 设置 | 描述 |
| --- | --- |
| **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。如果存档受密码保护，请在"**加密容器密码**"字段中输入密码。<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`。 |

# 在命令行上配置 Kaspersky Network Detection and Response (KATA) 集成

您可以在命令行中通过 *Kaspersky Network Detection and Response (KATA) 集成(KATAEDR)* 预定义任务来管理 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

该表描述了所有可用设置以及您可以为 *Kaspersky Network Detection and Response (KATA) 整合*任务指定的所有设置的默认值。

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 <文件>
```

其中 <文件> 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 <文件>
   ```

   其中 <文件> 是包含客户端证书和私钥的加密容器（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 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

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 应用程序可以与 Sandbox 在 Open Single Management Platform (OSMP) 或 Kaspersky Anti Targeted Attack Platform 上进行交互。根据平台的不同，Kaspersky Endpoint Security 应用程序与 Sandbox 的交互由 *Sandbox 服务器*处理：可以是 OSMP 服务器，也可以是 Central Node 服务器。

与 Sandbox 的集成由 Kaspersky Endpoint Security 的 *Sandbox* 组件提供。

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。为确保安全连接，使用 OSMP 服务器或者 Central Node 服务器颁发的以下证书：

- 服务器证书。使用服务器的 TLS 证书对连接进行加密。您可以通过在 Kaspersky Endpoint Security 端验证服务器证书来提高连接的安全性。为此，您需要在启用与 Sandbox 的集成之前添加服务器证书。
- 客户端证书。此证书用于使用双向身份验证进行额外的连接保护（OSMP 服务器或 Central Node 服务器使用 Kaspersky Endpoint Security 应用程序对设备进行身份验证）。多个设备可以使用同一客户端证书。默认情况下，服务器不检查客户端证书，但可以在 OSMP 或者 Kaspersky Anti Targeted Attack Platform 端启用双向身份验证。在这种情况下，您需要在 Sandbox 组件的设置中启用双向身份验证，并添加客户端证书（包含证书和私钥的加密容器）。

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。

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。

文件和目录可以通过以下几种模式之一发送到 Sandbox 进行扫描：

- *手动*。在此模式下，您可以使用命令或图形接口手动将文件发送到 Sandbox 进行扫描。
- *仅自动*。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。
- *自动和手动*。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 。

默认禁用 Sandbox 集成。您可以使用 Web Console或命令行启用或禁用 Sandbox 组件，以及管理以下集成设置。

- 选择发送对象进行扫描的模式（手动、仅自动、自动和手动）。
- 选择检测到威胁时应用程序执行的操作（如果已启用发送对象到 Sandbox 的异步模式）：
  - 删除包含检测到的对象的文件并隔离文件的副本。
  - 启动关键区域扫描任务。默认情况下，应用程序会扫描进程内存、内核内存、引导扇区、启动对象以及检测到的对象路径。
  - 创建IOC 扫描任务。应用程序会自动创建 IOC 扫描任务；您可以配置任务启动模式、扫描范围以及检测到 IOC 时要执行的操作（删除检测到的对象、启动关键区域扫描任务）。

- 配置常规 Sandbox 服务器连接设置。
- 添加或删除 Sandbox 服务器证书。
- 配置连接 Sandbox 服务器时执行双向认证并添加客户端证书。

# 在 Web Console 中配置 Sandbox 集成

在 Web Console 中，您可以在策略属性中管理 Sandbox 整合设置（**应用程序设置** → **内置代理配置** → **Sandbox**）。

# 在命令行上配置 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。

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*任务正在运行，您可以使用命令行将文件发送到 Sandbox 进行扫描。

*要将文件发送到 Sandbox 进行扫描，请运行以下命令：*

```
kesl-control [-X] --sandbox <路径>
```

其中 <路径> 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。

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 集成*任务指定的所有可用设置以及所有设置的默认值。

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`。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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 < 文件 >
```

其中 < 文件 > 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. 请执行命令：

   ```
   kesl-control [-X] --add-sandbox-client-certificate < 文件 >
   ```

   其中 < 文件 > 是包含客户端证书和私钥的加密容器（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
```

# Kaspersky Endpoint Detection and Response Optimum 整合

Kaspersky Endpoint Detection and Response Optimum 解决方案用于保护组织的 IT 基础设施免受漏洞、勒索软件、无文件攻击以及攻击者用来破坏设备或数据的合法系统工具等威胁。

Kaspersky Endpoint Detection and Response Optimum 监控和分析威胁的演变，并向安全官或管理员提供有关潜在攻击的信息，帮助他们及时采取威胁响应措施。

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。

Kaspersky Endpoint Security 12.4 for Linux 与 Kaspersky Endpoint Detection and Response Optimum 版本 3.1 兼容。

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。

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 Kaspersky Endpoint Detection and Response Optimum 功能，您需要激活 EDR Optimum 组件。如果您使用 Kaspersky Endpoint Security 所依据的主授权许可不包含 Kaspersky Endpoint Detection and Response Optimum 功能，则需要为此功能购买单独的授权许可，并将 EDR Optimum 授权许可密钥添加到该应用程序中。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，激活将通过向 SVM 添加授权许可密钥在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）上执行。

与 Kaspersky Endpoint Detection and Response Optimum 整合涉及以下步骤：

1. **启用所需的 Kaspersky Endpoint Security 组件**

   确保 Kaspersky Endpoint Security 的以下组件已启用并正在工作：

   - 文件威胁防护。
   - Web 威胁防护。
   - 行为检测。

您还可以启用对象的执行防护。

2. **启用威胁分析工具**

   确保卡巴斯基安全网络在标准或扩展模式下启用。

   为了使 Kaspersky Endpoint Detection and Response Optimum 最有效运行，我们建议使用扩展的卡巴斯基安全网络模式。

3. **激活 EDR Optimum 组件**

   确保满足以下条件之一：

   - 您正在使用包含 Kaspersky Endpoint Detection and Response Optimum 功能的授权许可来使用 Kaspersky Endpoint Security。
   - 您已购买使用 Kaspersky Endpoint Detection and Response Optimum 功能所需的单独授权许可，并将 EDR Optimum 授权许可密钥添加到应用程序中。

     如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟化环境，则需要向 SVM 添加用于激活附加功能的授权许可密钥。

4. **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。

5. **启用 EDR Optimum 组件**

   默认禁用 EDR Optimum。您可以启用或禁用该组件并管理整合设置：

   - 使用 Web Console。
   - 使用命令行。

     不支持使用 Kaspersky Security Center 管理控制台管理 EDR Optimum 组件。

   您可以检查 EDR Optimum 组件的状态：

   - 使用 Web Console 中的*应用程序组件状态报告*。

     **Endpoint Detection and Response Optimum**组件已被添加到 Kaspersky Endpoint Security 组件列表中。有关报告的详细信息，请参阅“Kaspersky Security Center 帮助”。
   - 在 Web Console 的设备属性中。
   - 使用命令行。

6. **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。

# 启用或禁用 Kaspersky Endpoint Detection and Response Optimum 整合

您可以启用或禁用 EDR Optimum 组件。

- 使用 Web Console。
- 使用命令行。

管理控制台不支持管理集成 Kaspersky Endpoint Detection and Response Optimum 的设置。

## 在 Web Console 中启用或禁用 Kaspersky Endpoint Detection and Response Optimum 整合

在 Web Console 中，您可以启用或禁用 EDR Optimum 组件并配置与 Kaspersky Endpoint Detection and Response Optimum 整合：

- 在策略属性中（**应用程序设置** → **内置代理配置** → **Endpoint Detection and Response**）
- 在受管理设备属性中（**资产（设备）** → **受管理设备** → <设备名称>链接 → **应用程序**选项卡 → <Kaspersky Endpoint Security 应用程序名称>链接 → **应用程序设置**选项卡 → **Detection and Response**部分 → **Endpoint Detection and Response Optimum**）。

如果将策略应用于设备，则无法在设备属性中启用或禁用 EDR Optimum 组件。

设备属性中的 Kaspersky Endpoint Detection and Response Optimum 集成设置

| 设置 | 描述 |
| --- | --- |
| **Endpoint Detection and Response Optimum 已启用/已禁用** | 启用或禁用 EDR Optimum 组件，这是将 Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 解决方案集成所必需的组件。<br>默认情况下，切换按钮处于关闭状态。 |
| **网络隔离** | **配置设备解除阻止**链接可打开**配置设备解除阻止**窗口，您可以在其中配置设备阻止的持续时间。 |
| **排除项** | **配置排除项**链接可打开**排除项**窗口，您可以在其中配置网络隔离例外。 |

# 在命令行上启用或禁用 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。

*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
```

# 查看 Kaspersky Endpoint Detection and Response Optimum 整合状态

## 在 Web Console 中查看整合状态

您可以通过选择资产（**设备**）**部分** →**受管理设备**→ <设备名称> 链接 →**应用程序**选项卡→ <Kaspersky Endpoint Security 应用程序名称> 链接 →**常规**选项卡→**组件**，在 Web Console 中查看 Kaspersky Endpoint Detection and Response Optimum and Response Optimum 整合的状态。

## 在命令行上查看整合状态

您可以通过运行命令 `kesl-control --app-info`，使用命令行查看与 Kaspersky Endpoint Detection and Response Optimum 的集成状态。

## 整合状态

EDR Optimum 组件将显示以下状态之一：

- *正在运行*。
  当同时满足以下条件时，会显示此状态：
  - 添加了 EDR Optimum 所需的授权许可密钥。
  - 当前日期早于授权许可到期日期。

- EDR Optimum 所需的一个或多个 Kaspersky Endpoint Security 组件已启用。
- 设备上已启用 Kaspersky Endpoint Detection and Response Optimum 整合。

- *已停止*。
  在以下情况下显示此状态：
  - Kaspersky Endpoint Detection and Response Optimum 整合已被禁用。
  - Kaspersky Endpoint Security 应用程序未停止。
- *不受授权许可支持*。
  在以下情况下显示此状态：
  - 当前日期晚于授权许可到期日期。
  - 当前授权许可不包括 EDR Optimum 功能。
- *故障*。
  当同时满足以下条件时，会显示此状态：
  - 当前日期早于授权许可到期日期。
  - EDR Optimum 所需的一个或多个 Kaspersky Endpoint Security 组件遇到错误。

# 查看有关检测到的威胁和响应操作的信息

要查看有关检测到的威胁的所有信息并执行适当的威胁响应措施，您可以使用警报详情窗口，其中包含：

- 威胁发展链图
- 使用 UI 执行所选操作来应对威胁的建议
- 有关威胁检测的常规信息（例如，检测模式）
- 关于受保护设备的信息
- 有关所检测到的对象的信息
- 设备上出现的文件历史记录
- 有关应用程序执行的威胁响应操作的信息

在警报详情窗口中，您可以执行以下威胁响应操作：

- 隔离在上面检测到威胁的设备
- 隔离文件
- 创建*IOC 扫描*任务

警报详情的存储期限为 30 天。此时间过后，旧条目将被被自动删除。

有关管理警报详情的更多详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

# 与 Kaspersky Managed Detection and Response 整合

Kaspersky Managed Detection and Response 是一款使用遥测技术和先进的机器学习技术来自动检测和分析基础设施中的安全事故的解决方案。关于该事故的信息将发送给卡巴斯基专家，他们可以自行处理该事故或提供处理建议。

与 Kaspersky Managed Detection and Response 交互时，Kaspersky Endpoint Security 可以执行以下功能：

- 将遥测数据发送到 Kaspersky Managed Detection and Response 以进行威胁检测。
- 在接收来自 Kaspersky Managed Detection and Response 的命令时，执行威胁响应操作以维护安全。

Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 解决方案的整合是通过该应用程序的 Managed Detection and Response (MDR) 组件来实现的。

要使用 Kaspersky Managed Detection and Response 功能，您需要通过以下其中一种方式来激活 MDR 组件：

- 通过使用密钥文件或激活码添加授权许可密钥。您可以使用包含 Kaspersky Managed Detection and Response 功能的授权许可来激活 Kaspersky Endpoint Security 应用程序（有关详细信息，请参阅 Kaspersky Managed Detection and Response 帮助）。如果您使用该应用程序所依据的主授权许可不包含 Kaspersky Managed Detection and Response 功能，则需要为此功能购买单独的授权许可，并将 MDR 授权许可密钥添加到该应用程序中。

  如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，激活将通过向 SVM 添加授权许可密钥在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）上执行。

  可用于激活 Kaspersky Managed Detection and Response 功能的授权许可必须首先在 MDR 门户上注册。

- 通过将包含 Kaspersky Managed Detection and Response 授权许可信息的 *MDR 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。您可以通过 Web Console、管理控制台或命令行来上传 BLOB 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。

要与 Kaspersky Managed Detection and Response 整合，需要执行以下步骤：

1. **启用所需的 Kaspersky Endpoint Security 组件**

   确保 Kaspersky Endpoint Security 的以下组件已启用并正在工作：

   - 文件威胁防护。
   - 行为检测。

   如果禁用这些组件，设备在 Kaspersky Managed Detection and Response 中将显示红色状态。

   我们还建议启动 Web 威胁防护和网络威胁防护组件。如果禁用这些组件，设备在 Kaspersky Managed Detection and Response 中将呈现黄色状态。

   请参阅“Kaspersky Managed Detection and Response 帮助”部分，了解有关设备状态的更多信息。

2. **启用在扩展模式下使用卡巴斯基安全网络。**

   如果卡巴斯基安全网络被禁用或在标准模式下运行，则 Kaspersky Managed Detection and Response 功能不可用。您可以在 Web Console、管理控制台或命令行中配置使用卡巴斯基安全网络。

3. **激活 MDR 组件**

   如果要在授权许可下使用 MDR 组件，请确保满足以下其中一项条件：

   - 您正在依据包含 Kaspersky Managed Detection and Response 功能的授权许可来使用 Kaspersky Endpoint Security。
   - 您已购买使用 Kaspersky Managed Detection and Response 功能所需的单独授权许可，并将 MDR 授权许可密钥添加到应用程序中。

     > 如果您在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟化环境，则需要向 SVM 添加用于激活附加功能的授权许可密钥。

   如果使用 MDR BLOB 文件来激活 MDR 组件，则需要在 Web Console、管理控制台或命令行中上传 BLOB 文件。

4. **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，则您需要将 KPSN 配置文件上传到 Kaspersky Security Center 管理服务器。

5. **启用 MDR 组件**

   默认禁用 MDR 组件。您可以通过以下方式启用或禁用该组件：

   - 使用 Web Console。
   - 通过管理控制台。
   - 使用命令行。

   您可以检查 MDR 组件的状态：

   - 在 Web Console 或管理控制台的设备属性中。
   - 使用命令行。

# 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。

# 上传用于与 Kaspersky Managed Detection and Response 整合的 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。

*要使用 Web Console 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。

*要使用管理控制台上传 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。

# 在 Web Console 中配置 Kaspersky Managed Detection and Response 整合

在 Web Console 中，您可以在策略属性（**应用程序设置** → **Built-in Agents Configuration** → **Managed Detection and Response**）中管理Kaspersky Managed Detection and Response 集成设置。

# 在管理控制台中配置 Kaspersky Managed Detection and Response 整合

在管理控制台中，您可以在策略属性中启用或禁用 MDR 组件并加载 MDR BLOB 文件（在管理控制台中管理策略，使用管理控制台创建策略）（**Detection and Response** → **Managed Detection and Response**）。

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。

| 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。 |

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。

# 在命令行上配置 Kaspersky Managed Detection and Response 整合

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。

- 编辑 Kaspersky Endpoint Security 成功与 Managed Detection and Response 集成后自动创建的“*Mdr_Autostart_Scan*”服务任务的启动时间。

建议在管理控制台或 Web Console 中配置 Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 之间的整合。

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。

`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 <文件路径 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。如果需要，您可以设置开始时间。无法编辑其他任务设置或计划选项。

# 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 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（本地部署）或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，并且已激活 EDR Expert（本地部署）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（本地部署）和 Kaspersky Endpoint Detection and Response (KATA) 集成时，启用或禁用设备的网络隔离，并且在 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（本地部署）帮助、Kaspersky Anti Targeted Attack Platform 帮助或者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（本地部署）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 中的设备属性中手动启用设备的网络隔离。

  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 Endpoint Detection and Response Agent 模式下运行，当使用网络隔离时，我们建议：

- 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. 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. 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。

     单击此按钮时， 应用程序会在 *启用网络隔离 (NetworkIsolationStart)* 任务的属性中指定的时间段内隔离设备。

   - 单击“**解除阻止隔离的设备**”按钮可禁用该设备的网络隔离。

8. 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（本地部署）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（本地部署））**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**按钮并从字典中选择一个网络配置文件。
   - 如果您想要删除某个被排除的网络连接的信息，请选中要删除的网络连接旁边的复选框，然后单击**删除**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（本地部署）、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 解决方案端进行配置。详情请参阅Kaspersky Endpoint Detection and Response Expert（本地部署）帮助、Kaspersky Anti Targeted Attack Platform 帮助或者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：

- 通过 Web Console 在策略属性中配置。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。

# 配置自动网络隔离的排除项

您可以在策略属性或设备属性中为自动隔离的设备配置网络隔离排除项。Web Console 策略属性中的网络隔离设置详见附录 5。

仅在与 Kaspersky Endpoint Detection and Response Optimum 集成的情况下，您才可以配置网络隔离排除项：

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。

*要在设备属性中添加或删除网络隔离排除：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。
   将打开受管理设备列表。
2. 选择包含必要设备的管理组。为此，请单击受管理设备列表上方“**当前路径**”字段中的链接，然后在打开的窗口中选择管理组。
   列表仅显示所选管理组的受管理设备。
3. 在列表中找到您的设备并单击其名称。
4. 这将打开一个受管理设备属性窗口；在该窗口中，转到“**应用程序**”选项卡。
5. 在设备上安装的应用程序列表中，单击 Kaspersky Endpoint Security。
   应用程序属性窗口将打开。
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. 这将打开一个窗口；在该窗口中，在**排除项**下，单击**配置排除项**链接以打开**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**按钮并从字典中选择一个网络配置文件。
   - 如果您想要删除某个被排除的网络连接的信息，请选中要删除的网络连接旁边的复选框，然后单击**删除**。
9. 单击“**确定**”按钮以保存所做的更改。

# 用于添加网络隔离排除的窗口

在此窗口中，您可以输入有关在启用网络隔离时不想被阻止的网络连接的信息。

网络连接设置

| 设置 | 描述 |
| --- | --- |
| Name | 用于输入网络连接名称的字段。 |
| Direction | 在下拉列表中，您可以选择网络连接的方向：<br>• **传出**。<br>• **传入**。<br>• **传入/传出**。 |
| **协议** | 在下拉列表中，您可以选择网络连接使用的协议：<br>• **任何**。<br>• **自定义**。<br>• ICMP。<br>• IPv6_ICMP<br>• TCP。<br>• UDP。<br>• IGMP。<br>• GRE。<br>• IPv4<br>• IPv6 |
| **编号** | 用于输入网络连接号码的字段。<br>如果在**协议**下拉列表中选择了**自定义**，则此字段可用。 |
| **本地端口/范围** | 此复选框可将下面字段中列出的本地端口号或本地端口范围添加到网络隔离排除项列表中。 |
| **远程端口/范围** | 此复选框可将下面字段中列出的远程端口号或远程端口范围添加到网络隔离排除项列表中。 |
| **远程地址** | 此复选框可将下面字段中指定的远程设备的 IP 地址添加到网络隔离排除项列表中。 |
| **附录** | 此复选框可将复选框下方表格中列出的应用程序添加到网络隔离排除项列表中。<br>您可以通过单击**添加**按钮来添加您不想阻止其网络连接的应用程序的路径。在打开的窗口中，在**应用程序路径**字段中输入应用程序的路径并保存更改。<br>您可以从表中删除该应用程序，方法是选中要删除的应用程序旁边的复选框，然后单击“**删除**”按钮。<br>这些设置适用于内核版本为 4.18 或更高版本，支持 eBPF 和 BTF，并且启用了内核跟踪的跟踪点和 kprobes 功能的设备。 |

# 网络配置文件字典窗口

在此窗口中，您可以选择一个或多个排除的网络连接配置文件。

网络连接配置文件

| 网络连接配置文件 | 描述 |
| --- | --- |
| **DNS 服务器** | 通过响应获取 IP 地址的请求和更新 DNS 记录的请求来提供 DNS 名称解析的服务。 |
| **DNS 客户端** | 通过执行 DNS 名称查询来提供 DNS 名称解析的服务。 |
| **Active Directory 证书服务** | 用于创建、验证和撤销供组织内部使用的公钥证书的服务。 |
| **Active Directory 联合服务** | 用于通过集中存储的统一凭证集授予用户对多个 Web 服务或网络资源的访问权限的服务。 |
| **Active Directory 轻型目录服务** | 提供与 Active Directory 域服务相同功能但不需要创建域或域控制器的服务。 |
| **Active Directory 权限管理服务** | 用于控制用户访问文档的服务。 |
| **DHCP** | 该服务使用动态主机配置协议 (DHCP) 自动分配 IP 地址。 |
| **文件传输协议 (FTP)** | 用于通过网络在客户端和服务器之间传输文件的标准网络协议。 |
| **Kerberos 密钥分发中心** | 用于向 Active Directory 域中的用户和设备提供票证 (TGS) 和临时会话密钥的网络服务。 |
| **Secure Shell (SSH)** | 允许远程控制操作系统和 TCP 连接隧道的协议。 |
| **Linux 系统组件** | Linux 网络系统服务，例如 NetworkManager。 |

# 在命令行中管理设备的网络隔离

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

*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。

您可以使用Web Console或管理控制台中的策略或使用命令行在设备上配置隔离设置。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）。

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。

您不能隔离系统关键对象 (SCO)。SCO 包含操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。

仅当满足以下条件之一时，才可以将文件置于隔离区：

- Kaspersky Endpoint Security 与 Kaspersky Endpoint Detection and Response Optimum 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（本地部署）或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，并且已激活 EDR Expert（本地部署）组件。
- Kaspersky Endpoint Security 与 Kaspersky Managed Detection and Response 的整合已启用，且 MDR 组件已激活。

存储隔离对象的目录必须可写。

当与 Kaspersky Endpoint Detection and Response（本地）或 Kaspersky Endpoint Detection and Response (KATA) 集成时，可以通过以下方式之一隔离文件：

- 通过在 Detection and Response 解决方案侧配置的任务。详情请参阅Kaspersky Endpoint Detection and Response Expert（本地部署）帮助 或 Kaspersky Anti Targeted Attack Platform 帮助。
- 通过扫描进程内存的YARA 扫描任务。

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。
- 由于遵循了警报详情中的建议。

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。

# 使用 Web Console 隔离文件

与 Kaspersky Endpoint Detection and Response Optimum 集成时，您可以在 Web Console 中使用“*隔离文件*”任务来隔离文件。

您可以为所有受管理设备或特定设备创建并运行“隔离文件”任务。

该任务针对“**隔离文件**”表中“**应用程序设置**”选项卡的任务属性中列出的文件执行。该表包含有关需要隔离的文件的以下信息：

- **路径**– 设备上文件所在目录的路径。
- **校验和类型**– 文件校验和验证类型。

使用表格上方的按钮，您可以添加或删除有关要隔离的文件的信息。

要添加有关要隔离的文件的信息，您需要单击**添加**按钮并在打开的窗口中指定任务设置。

隔离文件任务设置

| 设置 | 描述 |
| --- | --- |
| **指定要隔离的文件** | 在下拉列表中，您可以选择如何指定被隔离的文件的路径：<br>• **按完整路径指定文件**<br>• **按目录路径和校验和指定文件** |
| **文件的完整路径** | 用于输入要隔离的文件的完整路径的字段。<br>如果您在“**指定要隔离的文件**”下拉列表中选择了“**按完整路径指定文件**”时，此字段会显示。<br>如果文件位于网络驱动器上，请输入以 `//` 字符开头的文件路径。例如，您可以输入 `//server_ip/shared_folder`。 |
| **校验和类型** | 在下拉列表中，您可以选择要隔离的文件的校验和类型：<br>• MD5<br>• SHA256<br>如果您在“**指定要隔离的文件**”下拉列表中选择了“**按目录路径和校验和指定文件**”时，此下拉列表会显示。 |
| **文件校验和** | 用于输入要隔离的文件的校验和的字段。<br>如果您在“**指定要隔离的文件**”下拉列表中选择了“**按目录路径和校验和指定文件**”时，此字段会显示。 |
| **文件路径** | 用于输入要隔离的文件目录路径的字段。<br>如果您在“**指定要隔离的文件**”下拉列表中选择了“**按目录路径和校验和指定文件**”时，此字段会显示。<br>如果文件位于网络驱动器上，请输入以 `//` 字符开头的文件路径。例如，您可以输入 `//server_ip/shared_folder`。 |

如果您尝试隔离一个过大的文件，*隔离文件*任务可能会以*隔离区空间不足*的错误结束。在这种情况下，您可以清除隔离区或者增加隔离区大小，然后重试。

您可以在Web Console 中**结果**下的任务属性中查看启动进程任务的结果。

# 编辑 Web Console 中的隔离区设置

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **报告和存储**）和受管理设备属性（**资产（设备）** → **受管理设备** → <device name> 链接 → **应用程序**选项卡 → <Kaspersky Endpoint Security 应用程序名称> 链接 → **应用程序设置**选项卡 → **存储设置**部分）中管理隔离区设置。

下表描述了受管理设备属性中的隔离区设置。

设备属性中的隔离区设置

| 设置 | 描述 |
| --- | --- |
| **隔离区大小限制为 (MB):** | 用于输入隔离区最大容量 (MB) 的文本框。如果清除该复选框，则隔离区的大小不受限制。<br>默认值：200。 |
| **隔离区已满 (%) 时通知:** | 用于输入隔离区百分比的字段，该百分比必须达到 100% 才会生成隔离区已满的事件。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。 |

# 编辑管理控制台中的隔离区设置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略、使用管理控制台创建策略）（**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>默认值：如果应用程序在标准模式或者 Endpoint Detection and Response Agent 模式下使用，则为 200；如果应用应用程序在 Light Agent 模式下使用，则为 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。 |

# 使用命令行编辑隔离区设置

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。

| 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 999999<br>0 表示隔离区大小不受限制。<br>默认值：如果应用程序在标准模式或者 Endpoint Detection and Response Agent 模式下使用，则为 200；如果应用应用程序在 Light Agent 模式下使用，则为 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 <文件路径> [--md5] [--sha256] [--save-original-file]
```

其中：

- <文件路径>是要隔离的文件路径。
- `--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 ["< 过滤条件 >"] [-n < 数量 >] [--json]
```

其中：

- < 过滤条件 > 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。
- < 数量 > 是要显示的最新被隔离文件的数量。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 < 对象 ID >
```

其中 < 对象 ID > 是应用程序在隔离文件时分配给该文件的数字 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 < 对象 ID > --file < 文件路径 >
```

其中 `--file` < 文件路径 > 是文件的新名称以及要保存该文件的目录的路径。

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。

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 "< 过滤条件 >"
```

其中 < 过滤条件 > 是一个或多个逻辑表达式，格式为 < 字段 > < 比较运算符 > '< 值 >'，并借助逻辑运算符 and 组合以限制结果。

例如：
*要删除名称或路径中包含"test"的文件：*

```
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
```

# 启动进程

当 Kaspersky Endpoint Security 与 Detection and Response 解决方案集成时，您可以使用"*运行进程*"任务在受保护的设备上远程运行进程和可执行文件。

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以在 Web Console 中创建和执行运行进程的任务。当与 Endpoint Detection and Response Expert（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务在 Detection and Response 解决方案端创建并运行。

使用"*启动进程*"任务，您可以启动：

- 由于设备上的恶意活动而被停止的进程。
- 被您停止的进程。例如，您可以远程启动通过"终止进程 *任务*"停止的进程。
- 脚本。例如，您可以运行脚本从设备收集数据来调查威胁。
- 实用程序。例如，您可以运行实用程序将设备配置信息保存到文件中。
- 应用程序。

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

您可以在 Web Console 中创建和运行"*启动进程*"任务，并编辑其设置：无法在命令行上管理"*启动进程*"任务。

启动进程任务设置

| 设置 | 描述 |
| --- | --- |
| **可执行命令** | 用于输入启动进程的命令的字段。<br>例如，如果您要运行用于检查与管理服务器连接的 klnagchk 工具，请输入 /< 包含该工具的目录的绝对路径 >/klnagchk，然后根据需要填写下表中所述的其他字段。 |
| **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。<br>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。<br>如果需要传递多个参数，请用空格分隔它们。<br>例如，您可以输入 -logfile /tmp/klnagchk.log -savecert /home/user/certificate.cer 参数。这些参数指示该工具将结果保存到 tmp 目录中名为 klnagchk.log 的文件，并将用于检查对管理服务器访问权限的证书保存到 /home/user/ 目录中的 certificate.cer 文件。 |
| **工作目录路径（可选）** | 用于填写工作目录路径的字段，**可执行命令**字段中的命令将在该工作目录中执行。<br>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。 |

您可以在 Web Console 的*应用程序设置*→**执行结果**下的任务属性中查看**启动进程**任务的结果。

该表显示已运行*启动进程*任务的设备的列表，以及该任务的结果。在**设备**下拉列表中，您可以选择显示已运行该任务的所有受管理设备或特定设备的任务结果。

该表包含以下信息：

- **状态** – 任务完成状态
- **设备** – 在其上启动任务的设备的名称
- **时间** – 执行任务的日期和时间
- **结果**– 以返回代码形式显示的任务执行结果 带有返回代码的链接将打开**任务结果**窗口，其中显示以下信息：
  - 任务完成状态
  - 进程开始时间
  - 进程完成时间
  - 在其上启动进程的设备的名称
  - 已执行的命令
  - 命令行参数
  - 工作目录路径
  - 返回代码

通过单击**任务结果**窗口中的**下载 STDOUT 流**链接，您可以下载有关任务成功执行的 TXT 格式的报告。如果*启动进程*任务失败，您在尝试下载此报告时将看到一条错误消息。

通过单击**任务结果**窗口中的**下载 STDERR 流**链接，您可以下载有关任务执行期间所发生错误的 TXT 格式的报告。如果*启动进程*任务成功完成，您在尝试下载此报告时将看到一条错误消息。

# 终止进程

当 Kaspersky Endpoint Security 与 Detection and Response 解决方案集成时，您可以使用“*终止进程*”任务来远程终止受保护设备上的进程。

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以在 Web Console 中创建和运行终止进程的任务。当与 Endpoint Detection and Response Expert（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务在 Detection and Response 解决方案端创建并运行。

使用“*终止进程*”任务，您可以终止：

- 由于恶意活动而在设备上启动的进程。
- 由您启动的进程。例如，您可以远程终止通过“*启动进程*”任务启动的进程。
- 脚本。例如，您可以远程终止通过“*启动进程*”任务启动的脚本。
- 实用程序。例如，您可以远程终止使用“*启动进程*”任务启动的互联网速度测试实用程序。
- 应用程序。

系统关键对象 (SCO) 的进程无法终止。SCO 包含操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。

您可以在 Web Console 中创建和运行“*终止进程*”任务，并编辑其设置：无法在命令行上管理“*终止进程*”任务。

终止进程任务设置

| 设置 | 描述 |
| --- | --- |
| **指定想要终止其进程的文件** | 在下拉列表中，您可以选择如何指定文件路径：<br>• **按目录路径和校验和**<br>• **按完整路径**<br>• **按 PID**<br>仅对于在设备属性中创建的任务，下拉列表中才会出现“**按 PID**”值。 |
| **文件的完整路径** | 用于输入文件完整路径的字段。<br>仅当您在“**指定想要终止其进程的文件**”下拉列表中选择了“**按完整路径**”时，此字段才会显示。 |
| **校验和类型** | 在此下拉列表中，您可以选择文件校验和类型：<br>• **MD5**<br>• **SHA256**<br>如果您在**指定想要终止其进程的文件**下拉列表中选择**按目录路径和 校验和**，则会显示此下拉列表。 |
| **文件校验和** | 用于输入文件校验和的字段。<br>如果您在**指定想要终止其进程的文件**下拉列表中选择了**按目录路径和校验和**，并且在**校验和类型**下拉列表中选择了 **MD5**，则会显示此字段。 |

| 设置 | 描述 |
| --- | --- |
| **目录路径** | 用于输入文件目录路径的字段。<br>如果您在“**指定想要终止其进程的文件**”下拉列表中选择了“**按目录路径和校验和**”，此字段会显示。 |
| **进程 ID** | 进程 ID (PID) 输入字段。<br>如果您在“**指定想要终止其进程的文件**”下拉列表中选择了“**按 PID**”，此字段会显示。 |

您可以在 Web Console 中的*结果*下的任务属性中查看**终止进程**任务的结果。

# 从设备接收文件

当 Kaspersky Endpoint Security 与 Detection and Response 解决方案集成时，您可以使用“*获取文件*”任务从受保护的设备获取文件。

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以在 Web Console 中创建和运行从设备获取文件的任务。当与 Endpoint Detection and Response Expert（本地部署）、Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Managed Detection and Response 集成时，任务在 Detection and Response 解决方案端创建并运行。

例如，您可以接收由第三方应用程序生成的事件日志文件。

您可以创建和运行“*从设备接收文件*”任务，以及在 Web Console 中编辑其设置：无法在命令行上管理“*从设备接收文件*”任务。

“*从设备接收文件*”任务针对在“**接收文件**”表中“**应用程序设置**”选项卡上的任务属性中指定的文件执行。

该表包含有关任务应获取的文件的以下信息：

- **目录路径**– 设备上文件所在目录的路径。
- **校验和验证类型**– 文件校验和验证类型。

使用表格上方的按钮，您可以添加、更改或删除有关要从设备获取的文件的信息。

要添加有关您想要获取的文件的信息，您需要单击**添加**按钮并在打开的**接收文件**窗口中指定任务设置。

从设备接收文件任务的设置

| 设置 | 描述 |
| --- | --- |
| **指定要接收的文件** | 在下拉列表中，您可以选择如何指定文件路径：<br>• **按目录路径和校验和**<br>• **按完整路径** |
| **文件的完整路径** | 用于输入文件完整路径的字段。<br>如果您在“**指定要接收的文件**”下拉列表中选择了“**按完整路径**”时，此字段会显示。 |
| **校验和类型** | 在此下拉列表中，您可以选择文件校验和类型：<br>• MD5<br>• SHA256<br>如果您在“**指定要接收的文件**”下拉列表中选择“**按目录路径和 校验和**”，则会显示此下拉列表。 |
| **文件校验和** | 用于输入文件校验和的字段。<br>如果您在“**指定要接收的文件**”下拉列表中选择了**按目录路径和校验和**，此字段会显示。 |
| **文件目录路径** | 用于输入文件目录路径的字段。<br>如果您在“**指定要接收的文件**”下拉列表中选择了“**按目录路径和 校验和**”，则会显示此字段。 |

作为*从设备接收文件*任务的结果，文件的副本将在设备上被隔离。您可以使用 Web Console 将此副本从隔离区下载到您启动下载的设备。

文件大小不得超过 100 MB。

用户设备上的原始文件仍保留在其原始目录中。

在 Kaspersky Security Center 的隔离文件列表中，无论文件扫描结果如何，通过*从设备接收文件*任务接收的所有文件都将具有*"已感染"*状态。

如果出现以下情况，则*从设备接收文件*任务会以错误结束：

- 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）。

您可以在Web Console 中**结果**下的任务属性中查看启动进程任务的结果。

# 从设备删除文件

当 Kaspersky Endpoint Security 与 Detection and Response 解决方案集成时，您可以使用*"删除文件"*任务从受保护的设备中删除文件。

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以在 Web Console 中创建和运行删除文件的任务。与 Kaspersky Endpoint Detection and Response (KATA) 组件集成时，将在 Kaspersky Endpoint Detection and Response (KATA) 端生成并运行任务。

无法删除系统关键对象 (SCO)。SCO 包含操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。

您可以创建和运行*"从设备中删除文件"*任务，以及在 Web Console 中编辑其设置：无法在命令行上管理*"从设备中删除文件"*任务。

从设备删除文件任务的设置

| 设置 | 描述 |
| --- | --- |
| **指定要删除的文件** | 在下拉列表中，您可以选择如何指定被删除的文件的路径：<br>• **按路径和校验和**<br>• **按完整路径** |

| 设置 | 描述 |
| --- | --- |
| **文件的完整路径** | 用于输入要删除的文件的完整路径的字段。<br>如果您在“**指定要删除的文件**”下拉列表中选择了“**按完整路径**”，此字段会显示。 |
| **校验和类型** | 在下拉列表中，您可以选择要删除的文件的校验和类型：<br>• **MD5**<br>• **SHA256**<br>如果您在“**指定要删除的文件**”下拉列表中选择了“**按目录路径和校验和**”，则会显示此下拉列表。 |
| **文件校验和** | 用于输入要删除的文件的校验和的字段。<br>如果您在“**指定要删除的文件**”下拉列表中选择了“**按路径和校验和**”，此字段会显示。 |
| **目录路径** | 用于输入要删除的文件目录路径的字段。<br>如果您在“**指定要删除的文件**”下拉列表中选择了“**按路径和校验和**”，此字段会显示。 |
| **包括子目录** | 此复选框可启用或禁用子目录。 |

如果文件被另一个进程阻止，则任务将显示“*已完成*”状态，但文件本身只有在设备重新启动后才会被删除。重新启动设备后，确保该文件已被删除。

如果您尝试删除正在运行的可执行文件，则*从设备中删除文件*任务可能会以“*访问被拒绝*”错误结束。在这种情况下，您需要为该文件创建并运行“*终止进程*”*任务*，然后重试。

您可以在Web Console 中**结果**下的任务属性中查看启动进程任务的结果。

# 搜索入侵指标

*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。当 Kaspersky Endpoint Security 与 Detection and Response 解决方案集成时，您可以检测受保护设备上的入侵指标并执行威胁响应操作。

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。
- 已启用 Kaspersky Endpoint Security 应用程序与Kaspersky Endpoint Detection and Response Expert（本地部署）或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，并且已激活 EDR Expert（本地部署）组件。

当与 Kaspersky Endpoint Detection and Response（本地部署）或者 Kaspersky Endpoint Detection and Response (KATA) 集成时，IoC 扫描在相关解决方案端执行。

与 Kaspersky Endpoint Detection and Response Optimum 集成时，使用 *IOC 扫描*任务执行 IOC 扫描。您可以创建 IOC 扫描任务：

- 在 Web Console 中
- 从警报详情窗口
- 在命令行上

*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。

# 在 Web Console 中搜索入侵指标

仅当与 Kaspersky Endpoint Detection and Response Optimum 集成时，您才可以在 Web Console 中使用 IOC 扫描任务来扫描入侵指标。当与 Kaspersky Endpoint Detection and Response (on-premise) 或者 Kaspersky Endpoint Detection and Response (KATA) 集成时，IoC 扫描在相关的 Detection and Response 解决方案端执行。

您可以创建和运行*IoC 扫描*任务，以及在 Web Console 中编辑其设置。

对于*IOC 扫描*任务，计划设置中不提供 LAN 唤醒功能。为了运行任务，请确保设备已打开电源。

您可以在任务属性 中的**应用程序设置**选项卡 → **IOC 扫描设置**中更改*IOC 扫描*任务的主要设置。

*IOC 扫描*任务设置

| 设置 | 描述 |
| --- | --- |
| **重新定义 IOC 文件** | 此按钮可打开**重新定义 IOC 文件**窗格。<br>单击"**重新定义 IOC 文件**"面板中的"**添加 IOC 文件**"按钮将打开一个窗口，您可以在其中选择并下载设备上搜索入侵指标所需的 IOC 文件。上传 IOC 文件后，您可以查看 IOC 文件中的指标列表。 |
| **导出 IOC 集合** | 单击此按钮可将 IOC 文件下载到设备。 |

| 设置 | 描述 |
| --- | --- |
| **检测到 IOC 时应用响应操作** | 此复选框可启用或禁用在检测到入侵指标时应用响应操作。<br>如果选中该复选框，则当检测到入侵指标时，应用程序将执行您选择的操作：<br>• **开始关键区域扫描**。<br>如果选中此复选框，则当检测到入侵指标时，应用程序将启动*关键区域扫描*任务。<br>默认情况下，Kaspersky Endpoint Security 会扫描内核内存、正在运行的进程、引导扇区和其他**关键区域**。<br>◦ /lib/systemd<br>◦ /lib/udev<br>◦ /lib/dbus-1.0<br>◦ /usr/local/lib/systemd/user<br>◦ /usr/share/dbus-1<br>◦ /usr/share/gdm/autostart<br>◦ /usr/share/gnome/autostart<br>◦ /var/spool/at<br>◦ /var/spool/at/spool<br>◦ /var/spool/anacron<br>◦ /var/spool/cron<br>◦ /boot<br>◦ /bin<br>◦ /sbin<br>◦ /lib<br>◦ /lib32<br>◦ /lib64<br>◦ /libx32<br>◦ /usr/lib<br>◦ /usr/lib32<br>◦ /usr/lib64<br>◦ /usr/libx32<br>◦ ~/.config/autostart<br>◦ ~/.config/autostart-scripts<br>◦ ~/.config/plasma-workspace/env<br>◦ ~/.config/plasma-workspace/shutdown<br>◦ ~/.config/lxsession<br>◦ ~/.fluxbox/startup<br>◦ ~/.kde/Autostart<br>◦ /etc<br>• **隔离副本，删除对象**。<br>如果选中该复选框，当检测到入侵指标时，应用程序将隔离对象的副本并删除原始对象。<br>• **将设备从网络中隔离**。<br>如果选中此复选框，则当检测到入侵指标时，应用程序会将设备与网络隔离，以防止威胁蔓延。您可以配置隔离时长。<br>如果该策略适用于隔离设备，则会应用策略属性中指定的在指定时间段后自动禁用隔离和网络隔离排除项设置。<br>如果该策略不适用于隔离设备，则应用设备属性中指定的设置。 |

| 设置 | 描述 |
| --- | --- |
| | 如果清除该复选框，则应用程序在检测到入侵指标时不会执行任何威胁响应操作。有关检测到的入侵指标的信息显示在警报详情窗口和任务属性中。 |

您可以在*应用程序设置*选项卡→ **其他**的任务属性中更改**IOC 扫描**任务的其他设置。

如果您已在**重新定义 IOC 文件**面板中加载了 IOC 文件，则可以编辑**其他**部分。

*IOC 扫描*任务的其他设置

| 设置 | 描述 |
| --- | --- |
| **IOC 扫描期间要分析的数据类型（IOC 文档）** | **其他**部分中的复选框包括 IOC 扫描期间分析的以下数据类型（IOC 文档）：<br>• **进程** - ProcessItem。<br>• **文件** – FileItem。<br>  • **IOC 文档**。<br>  如果您已在**重新定义 IOC 文件**面板中加载了 IOC 文件，则可以使用**IOC 文档**链接。此链接将带您进入**文件扫描设置** - **FileItem** 窗口，您可以在其中添加扫描范围。<br>• ARP **表格** – ArpEntryItem。<br>• **网络端口** - PortItem。<br>• **用户账户** – UserItem。<br>• **系统对象** – SystemItem。 |
| **在以下区域内搜索 IOC** | 该复选框可启用或禁用扫描以下范围。<br>• **设备所有驱动器上的文件**。<br>• **设备的系统驱动器上的文件**。<br>• **设备上的关键区域**。默认情况下已选定该选项。<br>• **不扫描预定义区域**。 |
| **扫描自定义区域** | 该复选框可将复选框下方表格中列出的范围添加到扫描范围列表中。<br>您可以通过单击**添加**按钮来添加您想要扫描的范围的路径。在打开的窗口中，在**范围**字段中输入范围的路径并保存更改。<br>您可以从表中删除范围，方法是选中要删除的范围旁边的复选框，然后单击"**删除**"按钮。<br>如果在**在以下区域内搜索 IOC**列表中选择了**不扫描预定义区域**选项，则您无法清除此复选框。 |

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。我们建议创建一个新任务来基于新的 IOC 文件运行 IOC 扫描。

您可以在 Web Console 中*应用程序设置*→ **IOC 扫描结果**下的任务属性中查看**IOC 扫描**任务的结果。该表显示已运行*IOC 扫描*任务的设备的列表，以及该任务的结果。在**设备**下拉列表中，您可以选择显示已运行该任务的所有受管理设备或特定设备的任务结果。

该表包含以下信息：

- **状态** – 入侵指标检测状态，以图标形式显示。
- **设备** – 在其上启动任务的设备的名称
- **时间** – 执行任务的日期和时间

- **结果** – 有关*IOC 扫描*任务结果的信息。可能会显示下列状态之一：
  - *检测到 IOC* – 此状态显示为一个链接；单击链接将打开一个包含警报详情的窗口。
  - *未检测到 IOC*。

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。

# 在命令行中搜索入侵指标

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-premise) 或者 Kaspersky Endpoint Detection and Response (KATA) 集成时，IoC 扫描在相关的 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 <目录或文件路径> [--process on|off] [--hint <正则表达式>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <排除项列表>] [--scope <目录列表>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

其中：

- `--path <目录或文件路径>` 是 IOC 文件的路径，或包含扩展名为 .IOC 或 .XML 的 IOC 文件的目录路径，用于执行扫描。

  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 <正则表达式>` 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 <排除项列表>` 是从扫描中排除的路径列表。

  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 <目录列表>` 是要扫描的附加目录列表。

  > 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` — 应用程序将执行扫描**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。

# 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>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。 |

# 对象的执行防护

与 Detection and Response 解决方案集成时，Kaspersky Endpoint Security 可以控制可执行文件和脚本的执行以及设备上办公应用程序文件的打开操作，作为威胁响应操作。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。

对象的执行防护基于执行预防规则。*执行防护规则*是 Kaspersky Endpoint Security 应用程序在响应对象执行时考虑的一组标准。仅当对象满足执行防护规则的所有条件时，应用程序才会阻止该对象的执行。应用程序通过使用 MD5 和 SHA256 哈希算法计算的路径或校验和来识别文件。

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：

- 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（本地部署）或 Kaspersky Endpoint Detection and Response (KATA) 组件的集成，并且已激活 EDR Expert（本地部署）组件。

如果未启用文件操作拦截的阻止模式，则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。

## 与 Kaspersky Endpoint Detection and Response Expert（本地部署）或 Kaspersky Endpoint Detection and Response (KATA) 集成时，对象执行防护涉及一些特殊注意事项。

当 Kaspersky Endpoint Security 应用程序与 Kaspersky Endpoint Detection and Response Expert (on-premise) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，应用程序将使用*EDR Expert (on-premise) 组件的执行防护规则*。应用程序会从 Kaspersky Endpoint Detection and Response Expert (on-premise) 或 Kaspersky Endpoint Detection and Response (KATA) 获取这些规则。

当与 Kaspersky Endpoint Detection and Response Expert (on-premise) 或 Kaspersky Endpoint Detection and Response (KATA) 集成时，您可以：

- 在Web Console、管理控制台或命令行中启用或禁用应用 EDR Expert (on-premise) 组件的对象执行防护规则。

  当执行防护规则被触发时，Kaspersky Endpoint Security 会将报告发送至 Endpoint Detection and Response Expert (on-premise) 或 Kaspersky Anti Targeted Attack Platform。有关详细信息，请参阅相关解决方案的帮助文档。

- 在命令行上查看 EDR Expert (on-premise) 组件的对象执行防护规则列表。

## 与 Kaspersky Endpoint Detection and Response Optimum 集成时使用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或命令行中启用或禁用应用 EDR Optimum 组件的对象的执行防护规则。
- 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。

### 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。

## 为 Web Console 中的对象配置执行防护

### 配置对象执行防护（EDR Expert（本地部署））

如果已启用与 Kaspersky Endpoint Detection and Response Expert (on-premise) 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-premise)**）中为对象启用或禁用执行防护。

**对象执行防护**拨动开关可启用或者禁用对象执行防护的 EDR Expert（本地部署）规则。

### 配置对象的 EDR Optimum 执行防护。

如果已启用与 Kaspersky Endpoint Detection and Response Optimum集成，则可以启用或禁用对象执行防护并配置 EDR Optimum 组件的对象执行防护规则：

- 在策略属性中（**应用程序设置** → **内置代理配置** → **Endpoint Detection and Response**）。
- 在受管理设备属性中（**资产（设备）** → **受管理设备** → <设备名称>链接 → **应用程序**选项卡 → <Kaspersky Endpoint Security 应用程序名称>链接 → **应用程序设置**选项卡 → **Detection and Response**部分 → **Endpoint Detection and Response Optimum**）。

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。

设备属性中的 EDR Optimum 对象执行防护设置

| 设置 | 描述 |
| --- | --- |
| **已启用/禁用对象执行防护** | 启用或禁用用于对象执行防护的 EDR Optimum 规则。<br>默认不应用规则。 |
| **启动或打开对象时的操作** | 您可以选择对象执行防护的模式：<br>• **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。<br>• **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。 |
| 对象执行防护规则列表。 | **添加**链接将打开一个窗口，您可以在其中配置 EDR Optimum 组件的对象执行防护规则。<br>如果需要，您可以使用**删除**按钮以从列表中删除规则。 |

*要在设备属性中将规则添加到 EDR Optimum 组件的对象执行防护规则列表中：*

1. 点击执行防护规则列表上方的“**添加**”按钮。
2. 这将打开一个窗口；在该窗口中，输入执行防护规则的名称。
3. 通过将开关设置到适当的位置来指定执行防护规则的状态：
   - **已启用** 表示规则已启用，应用程序应用此规则。
   - **已禁用** 表示规则已禁用，不被应用程序使用。

   您可以随时启用或禁用创建的规则。
4. 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。
5. 要添加对象，请指定对象路径和/或对象的校验和。
   要指定对象路径，请选择**使用路径**并输入该对象的路径。
   要指定对象校验和，请选择 **SHA256** 或 **MD5** 选项并输入对象校验和。
6. 单击“**确定**”。
   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。

# 在管理控制台中配置对象的执行防护

只有在启用了与 Kaspersky Endpoint Detection and Response Expert (on-premise) 或 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。

您可以在策略属性中启用或禁用对象的执行防护（在管理控制台中管理策略，使用管理控制台创建策略）（**应用程序设置** → **Detection and Response** → **EDR Expert（本地部署）**）。

在"**执行防护**"下方，"**启用对象的执行防护**"复选框可用于启用或禁用 EDR Expert (on-premise) 组件的执行防护规则。

## 通过命令行管理对象的执行防护

在命令行上，您可以使用以下预定义任务启动或停止应用对象的执行防护规则：

- *对象执行防护（EDR Expert（本地部署））*（*KATAEDR_Prevention*）。
- *对象的执行防护（EDR Optimum）*（*EDRO_Prevention*）。

默认情况下，*对象执行防护（EDR Expert（本地部署））*和*对象执行防护（EDR Optimum）*任务未启动。您可以手动启动和停止这些任务。

仅当启用了*与 Kaspersky Endpoint Detection and Response Expert（本地部署）*或 Kaspersky Endpoint Detection and Response (KATA)的集成，才能运行对象执行防护（EDR Expert（本地部署））任务。

仅当*启用与 Kaspersky Endpoint Detection and Response Optimum 的整合*时，您才可以运行对象的执行防护 (EDR Optimum)任务。

您可以使用对象执行防护规则管理命令来查看 EDR Expert（本地部署）和 EDR Optimum 组件的对象执行防护规则列表。

*要查看 EDR Expert（本地部署）对象执行防护规则列表，请运行以下命令：*

```
kesl-control [-T] --get-prevention-state --kata
```

*要查看 EDR Optimum 对象执行防护规则列表，请运行以下命令：*

```
kesl-control [-T] --get-prevention-state --edro
```

# Cloud Sandbox

Cloud Sandbox 技术可以检测设备上的高级威胁。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。然后，有关这些文件的信息会被发送至卡巴斯基安全网络。因此，如果 Cloud Sandbox 检测到恶意文件，Kaspersky Endpoint Security 就会采取行动，消除所有检测到该文件的设备上的威胁。

为了使 Cloud Sandbox 正常工作，您需要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，无论您用来使用应用程序的授权许可类型如何。

如果您部署了Kaspersky Endpoint Detection and Response Optimum解决方案，则可以在 Web Console 中为使用 Cloud Sandbox 检测到的威胁启用单独的计数器：

- 在策略属性中（**应用程序设置** → **内置代理配置** → **Endpoint Detection and Response**）
- 在受管理设备属性中（**资产（设备）** → **受管理设备** → <设备名称>链接 → **应用程序**选项卡 → <Kaspersky Endpoint Security 应用程序名称>链接 → **应用程序设置**选项卡 → **Detection and Response**部分 → **Endpoint Detection and Response Optimum**）。

Cloud Sandbox 检测到的威胁计数器也显示在 GUI 报告中。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。

*要在 Web Console 的设备属性中启用 Cloud Sandbox 计数器，请执行以下操作：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**策略和策略配置文件**”。

   将打开策略列表。

2. 选择包含必要设备的管理组。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. 在打开的窗口中，在**Cloud Sandbox**下，启用**Cloud Sandbox**拨动开关。

8. 单击“**确定**”。

# 与 Kaspersky Unified Monitoring and Analysis Platform 整合

Kaspersky Endpoint Security 与 Kaspersky Unified Monitoring and Analysis Platform 解决方案（以下也称为 KUMA）兼容。

Kaspersky Unified Monitoring and Analysis Platform 是一个全面的软件解决方案，提供以下功能：

- 接收、处理和存储信息安全事件（遥测）。
- 对传入数据进行分析和关联。
- 在获取的事件中搜索。
- 在检测到信息安全威胁症状时创建通知。

有关该解决方案的更多信息，请参阅Kaspersky Unified Monitoring and Analysis Platform 帮助。

与 Kaspersky Unified Monitoring and Analysis Platform 集成时，运行 Kaspersky Endpoint Security 的设备会与 KUMA 服务器建立加密连接。为确保安全连接，使用 KUMA 服务器颁发的以下证书：

- KUMA 服务器证书。使用服务器的 TLS 证书对连接进行加密。您可以通过在 Kaspersky Endpoint Security 端验证服务器证书来提高连接的安全性。为此，请在启用 Kaspersky Unified Monitoring and Analysis Platform 整合之前添加 KUMA 服务器证书。

- 客户端证书。此证书用于使用双向身份验证对连接进行额外保护（使用 Kaspersky Endpoint Security KUMA 服务器扫描设备）。多个设备可以使用同一客户端证书。默认情况下，KUMA 服务器不检查客户端证书，但可以在 Kaspersky Unified Monitoring and Analysis Platform 端启用双向身份验证。在这种情况下，您需要在 Kaspersky Unified Monitoring and Analysis Platform 整合设置中启用双向身份验证并添加客户端证书（带证书和私钥的加密容器）。

用于保护与 KUMA 服务器连接安全的证书由 Kaspersky Unified Monitoring and Analysis Platform 的管理员提供。

如果在 Kaspersky Endpoint Security 的常规应用程序设置中配置了使用代理服务器，则使用代理服务器连接到 KUMA 服务器。

默认情况下，禁用 Kaspersky Unified Monitoring and Analysis Platform 整合。您可以通过命令行、 Web Console 和管理控制台启用或禁用整合，并配置以下整合设置：

- 配置常规 KUMA 服务器连接设置。

- 添加或删除 KUMA 服务器证书。

- 配置连接 KUMA 服务器时执行双向身份验证并添加客户端证书。

- 管理事件传输设置。

在启用与 Kaspersky Unified Monitoring and Analysis Platform 的整合之前，请确保满足以下条件之一：

- 您正在使用涵盖 Kaspersky Unified Monitoring and Analysis Platform 功能的授权许可来使用 Kaspersky Endpoint Security。

- 您已购买了 Kaspersky Unified Monitoring and Analysis Platform 功能的单独授权许可，并将附加功能的授权许可密钥（KUMA 密钥）添加到了应用程序。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，激活将通过向 SVM 添加授权许可密钥在 Protection Server（Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的组件）上执行。

# 在 Web Console 中配置 KUMA 整合

在 Web Console 中，您可以在策略属性中管理Kaspersky Unified Monitoring and Analysis Platform 整合设置（**应用程序设置** → **内置代理配置** → **KUMA 整合**）。

# 在管理控制台中配置 KUMA 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 的整合，并在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**KUMA 整合** → **KUMA 整合**）中管理整合设置。

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 或 UDP。<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。 |
| **使用双向身份验证** | 启用或禁用双向身份验证以进一步保护与 KUMA 服务器的连接。<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。如果存档受密码保护，请在“**加密容器密码**”字段中输入密码。

# 在命令行上配置 MDR 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 整合任务设置

该表描述了所有可用设置以及您可以为 *Kaspersky Unified Monitoring and Analysis Platform 整合*任务指定的所有设置的默认值。

| 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>`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。 |
| **[SiemTransferSettings]** 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 < 文件路径 >
```

其中 < 文件路径 > 是包含服务器证书的 DER 或 PEM 文件的路径。

*要添加或更改客户端证书：*

1. 请执行命令：

   ```
   kesl-control [-M] --add-kuma-client-certificate < 文件路径 >
   ```

   其中 < 文件路径 > 是包含客户端证书和私钥的加密容器（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 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
```

# 配置在 Light Agent 模式下使用应用程序的设置

仅当在用于保护虚拟环境的 Light Agent 模式下使用 Kaspersky Endpoint Security 时，本节中描述的设置才适用。

在 Light Agent 模式下运行 Kaspersky Endpoint Security 需要 Light Agent 与 SVM 上安装的 Protection Server 持续进行交互。如果没有连接到 Protection Server，Light Agent 无法将文件碎片传输到 Protection Server 进行扫描，因此不会执行扫描。

为了与 Protection Server 进行交互，Light Agent 会与安装了该 Protection Server 的 SVM 建立并保持连接。

您可以在 Web Console 或管理控制台中配置将 Light Agent 连接到 SVM 的设置。您无法在命令行中配置设置；您只能查看有关在 Light Agent 模式下的应用程序使用情况的信息。

您可以配置以下用于将 Light Agent 连接到 SVM 的设置：

- SVM 检测方法。您可以选择 Light Agent 将用来发现可连接的 SVM 的方法。Light Agent 可以通过以下方式之一发现网络上运行的 SVM：
  - 使用 Integration Server。SVM 将自身信息传输到 Integration Server。Integration Server 生成可连接的 SVM 列表并将其提供给 Light Agent。

    要使用此方法检测 SVM，您需要将 SVM 和 Light Agent 连接到 Integration Server。

    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。
  - 使用 SVM 地址列表。您可以指定 Light Agent 可以连接的 SVM 地址列表。
- 用于选择要连接的 SVM 的算法。Light Agent 在收到可用 SVM 的信息后，根据 SVM 选择算法选择最佳的 SVM 进行连接。您可以指定 Light Agent 在选择要连接的 SVM 时应使用的算法。
- 连接标签。您可以使用连接标签来控制 Light Agent 与 SVM 的连接。如果使用连接标签，Light Agent 只能连接到配置为使用该连接标签的 SVM。
- Light Agent 与 Protection Server 之间连接的安全。您可以使用加密来保护 Light Agent 与 Protection Server 之间的连接。

有关将 Light Agent 连接到 SVM 的设置的更多信息，请参阅 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的帮助。

# 在 Web Console 中配置 Light Agent 设置

在 Web Console 中，您可以在策略属性（**应用程序设置** → **Light Agent 模式**）中管理用于将 Light Agent 连接到 SVM 的设置。

# 在管理控制台中配置 Light Agent 设置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**Light Agent 模式**）中管理 Light Agent 的 SVM 连接设置。

## 与 Integration Server 的连接

仅当在用于保护虚拟环境的 Light Agent 模式下使用 Kaspersky Endpoint Security 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 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、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（在运行于 OpenStack 平台、VK Cloud (VK Private Cloud) 或 TIONIX Cloud Platform 上的虚拟基础架构中）。<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 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、Scala-R、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、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 OpenStack 项目中（在运行于 OpenStack 平台、VK Cloud (VK Private Cloud) 或 TIONIX Cloud Platform 上的虚拟基础架构中）。<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 与安装了 Light Agent 的虚拟机部署在同一数据中心中（在 Microsoft Hyper-V 平台、XenServer、VMware vSphere、KVM、Proxmox VE、Basis (Scala-R)、HUAWEI FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、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（在运行于 OpenStack 平台、VK Cloud (VK Private Cloud) 或 TIONIX Cloud Platform 上的虚拟基础架构中）。<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。 |

# 在命令行中查看有关在 Light Agent 模式下的应用程序使用情况的信息

在命令行中，您可以查看有关在用于保护虚拟环境的 Light Agent 模式下使用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

*如要查看有关在 Light Agent 模式下使用应用程序的设置信息，请运行以下命令：*

```
kesl-control [-V] --ksvla-info
```

该命令向控制台输出以下信息：

- 用于保护虚拟环境的 Light Agent 模式：已启用/已禁用。

  如果启用了 Light Agent 模式，应用程序将被用作 Light Agent （用作 Kaspersky Hybrid Cloud Security for Virtualization Light Agent 的一部分）。

- VDI 保护模式：已启用/已禁用。

  VDI 保护模式能够优化 Kaspersky Endpoint Security 以在临时虚拟机上运行。如果启用了 VDI 保护模式，则临时虚拟机上不会安装需要重启受保护的虚拟机的更新。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。

- 受保护的虚拟机的类型：临时或持久。
- 受保护的虚拟机在虚拟基础架构中的角色：服务器或工作站。
- 受保护的虚拟机的标识符 (UUID)。

*如要查看有关 Light Agent 连接 Integration Server 的信息，请运行以下命令：*

```
kesl-control [-V] --viis-info
```

该命令向控制台输出以下信息：

- Light Agent 连接到的 Integration Server 的地址和端口。

  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Kaspersky Hybrid Cloud Security for Virtualization Light Agent 帮助。

- 与 Integration Server 的连接状态。
- Light Agent 与 Integration Server 之间最后一次连接的日期和时间。

*如要查看有关 Light Agent 连接 SVM 的信息，请运行以下命令：*

```
kesl-control [-V] --svm-info
```

该命令向控制台输出以下信息：

- Light Agent 连接到的 SVM 的地址，以及虚拟基础架构中 SVM 相对于 Light Agent 的位置：本地或非本地。
- Light Agent 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。

# 查看事件和报告

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，应用程序将有关事件的信息保存到数据库 /var/opt/kaspersky/kesl/private/storage/events.db。您可以在命令行中配置应用程序事件日志。
- 操作系统日志 (syslog)。默认情况下，不使用操作系统日志。您可以启用将事件保存到此日志的功能。

访问应用程序事件日志和操作系统日志需要 root 权限。

如果 Kaspersky Endpoint Security 由 Kaspersky Security Center 管理，则有关事件的信息可能会传输到 Kaspersky Security Center 管理服务器。聚合规则适用于某些事件。如果在应用程序运行期间，短时间内生成大量相同类型的事件，则应用程序将切换到事件聚合模式，同时向 Kaspersky Security Center 发送一个聚合事件，并提供事件设置说明。不同的事件可以使用不同的聚合规则。有关事件的更多详细信息，请参阅“Kaspersky Security Center 帮助”。

您可以通过以下方式接收有关应用程序事件的信息：

- 在管理控制台和 Web Console 中
- 在命令行中（在命令行中查看事件，在 Kaspersky Security Center 中查看事件）
- 当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，则会弹出通知

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不会记录在操作系统日志中。您可以使用 Web Console、管理控制台或命令行启用或禁用将事件记录到此日志中。

如果您使用命令行来进行应用程序管理，则默认禁用在操作系统日志中进行事件记录。

如果您在标准模式或者 Endpoint Detection and Response Agent 下使用 Kaspersky Endpoint Security 应用程序，并使用 Kaspersky Security Center 管理该应用程序，则关于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默认操作系统日志中。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。

## 在 Web Console 中配置

在 Web Console 中，您可以在策略属性中启用或禁用将事件记录到操作系统日志（**应用程序设置** → **常规设置** → **事件设置**）。

单击事件严重级别（严重事件、功能失败、警告、信息消息）下的**设置**按钮将打开一个窗口，其中包含相应严重级别的事件列表。您可以为每个事件配置操作系统日志记录。

### 在管理控制台中配置

在管理控制台中，您可以在策略属性中配置将事件记录到操作系统日志（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置 → 应用程序设置**）。

单击“**通知**”中的“**配置**”将打开“**通知设置**”窗口。在此窗口中，您可以使用复选框选择应用程序在操作系统日志中记录的事件。

您可以选择单个事件类型或某个严重级别的所有事件类型（严重事件、功能失败、警告、信息消息）。

### 在命令行中配置

您可以通过常规应用程序设置中的 `UseSyslog` 选项，在命令行中启用或禁用将事件保存到操作系统日志。

您可以通过命令行开关或包含所有常规应用程序设置的配置文件来编辑该选项。

`UseSyslog` 参数可以采用以下值：

- `Yes`：启用将事件保存到 syslog。
- `No`（默认）：禁用将事件保存到 syslog。

# 配置应用程序事件日志设置

默认情况下，有关事件的信息会保存到设备上的应用程序事件日志中。

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。

您可以借助命令行开关或包含所有常规应用程序设置的配置文件来更改设置的值。

# 在 Kaspersky Security Center 中查看事件

所有 Kaspersky Endpoint Security 事件的列表显示在 Web Console 和管理控制台中。

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。

您可以配置事件通知。*通知*是一种消息，包含有关受保护设备上所发生事件的信息。通知会及时为您提供有关应用程序事件的信息。您可以配置当收到来自应用程序的事件或通过电子邮件收到有关事件的通知时执行脚本。

有关使用 Kaspersky Security Center 通知的详细信息，请参阅 Kaspersky Security Center 帮助。

# 在命令行中查看事件

在命令行中，您可以查看：

- 当前应用程序事件
- 应用程序事件日志中的事件

## 显示当前事件

您可以输出有关所有当前应用程序事件的信息，或与启动或停止指定任务相关的当前事件的信息。您可以使用筛选器输出某些当前事件，例如指定类型的事件。

*要输出有关所有当前应用程序事件的信息，请运行：*

```
kesl-control -W
```

该命令将返回事件的名称以及有关事件的其他信息。

*要仅输出与运行中任务相关的当前事件的信息，请运行：*

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

例如：
*启用 ID=1 的运行中任务的当前事件的显示：*

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

*要输出符合筛选条件的当前事件信息，请运行：*

```
kesl-control -W --query "< 过滤条件 >"
```

过滤条件通过一个或多个逻辑表达式进行设置，格式为 < 字段 > < 比较运算符 > '< 值 >'，并使用逻辑运算符 and 组合。

例如：
*显示 TaskStateChanged 事件：*

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

*显示由"User"用户发起的 TaskSettingsChanged 事件：*

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

## 显示事件日志中的事件

您可以将有关事件的信息从应用程序事件日志输出到控制台或文件。您可以使用筛选器仅显示某些事件。

*要输出有关应用程序事件日志中的所有事件的信息，请运行：*

```
kesl-control -E --query [--db < 数据库文件 >]
```

其中 < 数据库文件 > 是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。

如果事件日志位于默认数据库中，则可以使用kesl-control -E命令输出有关所有事件的信息：

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。

*要输出应用程序事件日志中符合特定条件的事件的信息，请运行：*

```
kesl-control -E --query "< 过滤条件 >" [--db < 数据库文件 >] [-n < 数量 >] [--json] [--
reverse]
```

其中：

- < 过滤条件 > 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。
- < 数量 > 是要显示的所选内容中最新事件的数量（从所选内容的末尾开始计算的记录数量）。

- `--json`：以 JSON 格式输出事件。
- `--reverse`：倒序显示事件（最新事件显示在顶部，最早事件显示在底部）。

*要将有关应用程序事件日志中符合特定条件的事件的信息输出到文件，请运行：*

```
kesl-control -E --query "<过滤条件>" [--db <数据库文件>] [-n <数量>] --file <文件路径>
[--json]
```

其中 `--file <文件路径>` 是要将事件输出到的文件的完整路径。

# 配置图形界面中的弹出通知

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。您可以使用管理控制台或命令行启用或禁用弹出通知。

## 在管理控制台中配置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**常规设置 → 应用程序设置**）中启用或禁用图形界面中弹出通知的显示。

“**在图形用户界面中显示弹出通知**”复选框可启用图形用户界面中的弹出通知。

默认情况下已选定该选框。

## 在命令行中配置

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。

`ShowPopUpNotifications` 参数可以采用以下值：

- `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。

# 通过图形界面管理应用程序

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

您可以使用 Kaspersky Endpoint Security 图形界面来执行以下操作：

- 查看有关设备保护状态的信息。
- 启用和禁用应用程序组件：
  - 文件威胁防护。
  - 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。
- 启动和停止扫描任务：
  - 恶意软件扫描。
  - 关键区域扫描。
  - 容器扫描。
- 执行文件和目录的自定义扫描。
- 启动和停止数据库更新和回滚任务。
- 发送文件或目录以供在 Sandbox 中扫描。

- 启用和禁用卡巴斯基安全网络。
- 管理应用程序授权许可密钥和查看有关应用程序在其下使用的授权许可以及与授权许可关联的密钥的信息。
- 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。
- 查看应用程序统计数据和报告。
- 查看有关放置在备份中的对象的信息。
- 创建应用程序跟踪文件。

如果应用程序以 EDR Agent 模式使用，则只有部分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。

如果应用程序组件或任务以"仅通知"模式运行，则应用程序界面会显示该组件或任务*已选择"仅通知"模式*警告。

# 图形界面

## 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 12.4 for Linux**。打开应用程序图形界面的主窗口，其中显示设备的保护状态，并包含用于访问应用程序功能的界面元素。
- **退出**。退出图形界面。

## 应用程序图形界面的主窗口

要打开应用程序的主窗口，请执行以下操作之一：

- 在操作系统窗口管理器的应用程序菜单中选择应用程序名称。
- 右键单击或双击任务栏通知区域中的应用程序图标。

应用程序图形界面的主窗口分为几个部分：

- 主窗口的上部显示设备的保护状态。点击“**查看**”按钮将打开“**保护中心**”窗口。此窗口显示有关设备保护状态的信息，以及为修复保护问题（如果有）所要执行的操作的相关建议。
- 在“**扫描**”下方，显示恶意软件扫描任务状态和检测到的威胁数量。点击此处将打开“**扫描**”窗口。在此窗口中，您可以启动和停止“*恶意软件扫描*”、“*关键区域扫描*”和“*容器扫描*”任务。您还可以查看这些任务的报告。
- 在“**更新**”下方，显示*更新*任务的状态。点击此处将打开“**更新**”窗口。在此窗口中，您可以启动“*更新*”和“*回滚*”任务。您还可以查看这些任务的报告。
- 主窗口的下部包含以下元素：
  - “**报告**”按钮。单击此按钮将打开“**报告**”窗口，您可以在其中查看组件、任务统计数据和各种报告。
  - **备份**按钮。单击此按钮将打开“**备份**”窗口，其中包含有关备份中对象的信息。
  - “**设置**”按钮。单击此按钮将打开“**设置**”窗口，您可以在其中启用或禁用应用程序组件，以及配置卡巴斯基安全网络的使用。
  - **临时访问权限**按钮。单击此按钮会打开**临时访问权限**窗口，您可以在该窗口中请求并获得对被阻止设备的临时访问权限。
  - “**支持**”按钮。点击此按钮将打开“**支持**”窗口，您可以在其中查看关于应用程序的信息并创建应用程序跟踪文件。
- 应用程序主窗口的最下面显示有关授权许可和密钥的信息，以及有关授权许可问题（如果有的话）的信息。单击窗口的此区域将打开**授权许可**窗口，其中显示详细的授权许可信息。单击此窗口中的**“购买授权许可”**按钮将打开卡巴斯基在线商店，您可以在那里购买授权许可。购买授权许可后，您将收到用于激活应用程序的激活码或密钥文件。

管理图形界面需要“管理员”(admin) 角色权限。其他角色的用户可能无法使用图形界面的某些部分。

# 启用和禁用应用程序组件

您可以使用图形界面中的拨动开关启用或禁用应用程序组件。

默认情况下，将启用以下组件：文件威胁防护、设备控制和行为检测。如果允许在设备上本地管理 Web 威胁防护设置（未应用策略或未为策略设置“锁定”）并且在系统上检测到一个受支持的浏览器，则可以自动启用 Web 威胁防护组件。

*如要启用或禁用应用程序组件：*

1. 打开应用程序图形界面的主窗口。
2. 在主窗口下部，点击“**设置**”按钮。

   将打开“**设置**”窗口。
3. 启用或禁用相关组件的拨动开关。

# 启动和停止扫描任务

*要启动或停止扫描任务：*

1. 打开应用程序图形界面的主窗口。
2. 在主窗口中，点击“**扫描**”。
   这将会打开**扫描**窗口。
3. 执行下列操作之一：
   - 如果要启动一项扫描任务，请单击要启动的扫描任务下的**启动**按钮。
     此时将显示正在运行的扫描任务的进度。
   - 如果要停止一项扫描任务，请单击要停止的扫描任务下的**停止**按钮。
     扫描任务将停止，并显示有关已扫描对象和已检测到的威胁的信息。
4. 要查看有关扫描任务的报告，请单击**显示报告**按钮。

当检测到受感染的对象或扫描任务已完成时，在任务栏右侧应用程序图标附近的通知区域中将出现一个弹出窗口。

“**扫描**”窗口还显示临时引导扇区扫描任务 (*Scan_Boot_Sectors_{ID}*) 和临时自定义文件扫描任务 (*Scan_File_{ID}*) 的进度和结果。通过单击十字或关闭“**扫描**”窗口（切换到主窗口或退出应用程序时），可以隐藏有关已完成的临时任务的信息。

# 启动自定义扫描和 Sandbox 扫描

您可以使用图形界面来运行文件和目录的自定义扫描。

*要运行文件或目录的自定义扫描：*

1. 右键单击要扫描的文件或目录以打开上下文菜单。
2. **选择 Kaspersky Endpoint Security 12.4 for Linux** 作为扫描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。

自定义扫描任务及其进度显示在图形界面中。

如果启用了 Kaspersky Endpoint Security 应用程序与 Sandbox 的集成，您可以使用图形界面将文件或目录发送到 Sandbox 进行扫描。

*要将文件或目录提交到 Sandbox 进行扫描：*

1. 右键单击要发送扫描的文件或目录以打开上下文菜单。
2. **选择 Kaspersky Endpoint Security 12.4 for Linux** 作为扫描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. 在打开的窗口中，选择**发送到 Sandbox 进行扫描**。

# 启动和停止更新任务

*要启动或停止更新任务，请执行以下操作：*

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。
     如果更新任务成功完成，则**回滚更新**链接将变为可用，并且您可以回滚上次成功的数据库更新。
   - 如果要停止一项任务，请单击要停止的任务下的**停止**按钮。
     更新任务将会停止。
4. 要查看有关任务的报告，请单击**显示报告**按钮。

*要启动回滚任务：*

1. 打开应用程序图形界面的主窗口。
2. 在主应用程序窗口中，选择**更新**部分。
   **更新**窗口将打开。
3. 单击**回滚更新**链接以运行回滚任务。

# 配置卡巴斯基安全网络

您可以使用图形界面来启用或禁用卡巴斯基安全网络。

*要启用卡巴斯基安全网络：*

1. 打开应用程序图形界面的主窗口。
2. 在主窗口下部，点击“**设置**”按钮。
   将打开“**设置**”窗口。
3. 在“**设置**”窗口中，选择以下选项之一：
   - **扩展 KSN 模式** — 如果要使用卡巴斯基安全网络，从知识库中获取信息，并发送有关威胁类型和来源的匿名统计数据和信息。
   - **基本 KSN 模式**，如果要使用卡巴斯基安全网络，从知识库中获取信息，但不发送有关威胁类型和来源的匿名统计数据和信息。
4. 单击“**启用**”按钮。
   “**使用卡巴斯基安全网络**”窗口打开。
5. 在“**使用卡巴斯基安全网络**”窗口中，仔细阅读卡巴斯基安全网络声明并选择“**我确认已完全阅读、理解并接受卡巴斯基安全网络声明的条款和条件**”选项。
6. 单击“**确定**”。
   如果在“**卡巴斯基安全网络使用**”窗口中未选择任何选项，则“**确定**”按钮不可用。

*要禁用卡巴斯基安全网络：*

1. 打开应用程序图形界面的主窗口。
2. 在主应用程序窗口下部，单击“**设置**”按钮。
   将打开“**设置**”窗口。
3. 单击**启用**。
4. 在打开的窗口中，单击“**是**”按钮拒绝使用卡巴斯基安全网络。

# 查看报告

您可以使用图形界面来查看应用程序组件和任务的报告。点击应用程序图形界面主窗口下部的“**报告**”后，报告将显示在打开的窗口中。

报告数据将以表格的形式呈现，该表格中包含一个事件列表。表中的每一行都包含有关单独事件的信息。事件属性将在表格列中显示。各种组件和任务运行时记录的事件具有不同的属性集。

报告中使用以下事件重要级别：

- *严重* — 重要性级别为“严重”的事件，需要予以注意，因为它们表明应用程序操作中存在问题或设备保护中存在漏洞
- *高*
- *中度*

- *低*
- *信息*
- *Error*

应用程序中提供以下报告：

- **统计**。此报告包含“文件威胁防护”和扫描任务统计信息。您可以通过单击“**重新加载**”按钮来更新显示的报告。
- **系统审计**。此报告包含有关在应用程序操作期间以及用户与应用程序交互期间发生的事件的信息。
- **威胁防护**。此报告包含有关在运行以下应用程序组件时记录的事件的信息：
  - 文件威胁防护
  - 可移动驱动器扫描
  - 反加密
  - 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-premise) 和 EDR Optimum 组件执行对象执行防护期间记录的事件的信息。

*要查看报告：*

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。

包含事件列表的报告将显示在窗口的右侧。
默认情况下，事件已根据**日期**列的值按照升序进行排序。

4. 要查看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。

为便于处理报告，您可以通过以下几种方法修改数据的显示方式：

- 按发生时间筛选事件列表。
- 使用搜索功能查找特定的事件。
- 在单独的区域中查看所选事件。

# 查看备份对象

您可以使用图形用户接口对备份区中的对象执行以下操作：

- 查看有关放入设备备份中的对象的信息。
- 将对象从备份恢复到其原始目录。
- 从备份中删除对象。删除的对象以后将无法恢复。

有关恢复和删除对象的信息保存到事件日志中。

*如要查看备份中的对象：*

1. 打开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。

# 管理授权许可密钥

使用图形界面，您可以添加和删除应用程序授权许可密钥，并查看授权许可相关信息（使用应用程序所依据的授权许可）以及与该授权许可关联的授权许可密钥。

要在受保护的设备上激活 Kaspersky Endpoint Security 应用程序，您需要向该应用程序添加主授权许可密钥。

*激活*是授权许可生效的过程，允许您使用应用程序的完整功能版本，直到授权许可到期。

如果您用于应用程序的主授权许可不涵盖您所需的附加 Kaspersky Endpoint Security 功能，您还需要添加授权许可密钥来激活附加功能：

- 单独的授权许可密钥“Kaspersky Endpoint Detection and Response Optimum 附加模块”（下文亦称“EDR Optimum 密钥”），用于激活 Kaspersky EDR Optimum 组件。
- 单独的授权许可密钥“卡Kaspersky Unified Monitoring and Analysis Platform Add-on”（以下也称为“KUMA 密钥”），用于激活Kaspersky Unified Monitoring and Analysis Platform功能。
- 单独的授权许可密钥，即“Kaspersky Managed Detection and Response Optimum/Expert 附加模块”（下文亦称“MDR 密钥”），用于激活 MDR 组件功能。

您还可以为基本功能添加一个备用密钥，为附加功能添加一个备用密钥。当与活动密钥关联的授权许可到期或活动密钥被删除时，备用密钥成为活动密钥。备用密钥可避免当授权许可到期时应用程序功能受限。

只有在添加了活动授权许可密钥之后，才可以添加备用授权许可密钥。

# 添加授权许可密钥

如果应用程序尚未激活（尚未添加活动的主授权许可密钥），您可以根据商业授权许可或试用授权许可激活该应用程序。

*要激活应用程序：*

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。

      该窗口显示有关密钥及其相关授权许可的信息。
   b. 单击**激活**按钮。

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。该窗口显示有关试用授权许可和相关密钥的信息。

   只能在一个试用期内根据试用授权许可使用应用程序。

激活应用程序后，您可以添加备用主授权许可密钥，并根据需要添加活动密钥和备用密钥以获得附加功能。添加备用主密钥和附加功能密钥的程序相同。

*要向应用程序添加备用主密钥或附加功能密钥：*

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。

   该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。

如果您添加主授权许可密钥并且应用程序已激活，则新密钥将作为备用主密钥添加。

如果您为附加功能添加单独密钥，则会将其添加为活动密钥，除非先前已将此附加功能的密钥添加到应用程序中。如果已将用于附加功能的密钥添加到应用程序，则会将用于该附加功能的新密钥添加为备用密钥。

如果先前已将活动密钥和备用密钥添加到应用程序中，则新密钥将替换先前添加的备用密钥。

试用授权许可密钥和订阅密钥不能作为备用密钥添加。

# 移除授权许可密钥

*要删除已添加到应用程序的授权许可密钥：*

1. 打开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。
3. 单击要删除的密钥信息右侧的**“删除”**按钮。
4. 在打开的窗口中确认删除。

# 查看授权许可信息

*要查看授权许可信息：*

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**部分显示有关添加的活动密钥（活动主密钥和活动附加功能密钥）以及与这些密钥关联的授权许可的信息：

- 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**部分显示有关添加的备用密钥（备用主密钥和备用附加功能密钥）以及与这些密钥关联的授权许可的信息：

- 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。

# 获取设备的临时访问权限

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**”。

# 查看有关应用程序的信息

您可以在“**支持**”窗口中查看关于已安装应用程序及其设备的信息，您可以通过点击应用程序图形界面主窗口下部的“**支持**”按钮来打开该窗口。

“**支持**”窗口显示以下信息：

- 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。此字段中的链接可打开**“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）。

**支持**窗口底部显示以下链接：

- **授权许可**，其可打开**授权许可**窗口，显示详细的授权许可信息。
- **知识库**，其可打开知识库页面。
- “**支持**”用于打开 Kaspersky CompanyAccount 页面。

- **跟踪**，其可打开**跟踪**窗口。在此窗口中，您可以创建应用程序跟踪文件并配置跟踪文件的详细程度。

  要访问“**跟踪**”链接，您需要具有管理员角色的权限。

# 创建跟踪文件

您可以使用图形界面创建应用程序跟踪文件并配置跟踪文件的详细程度。

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。

*要创建跟踪文件：*

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。
   我们建议您通过卡巴斯基技术支持专家了解所需的细节级别。默认值为**诊断 (300)**。
5. 单击**启用**按钮开始跟踪。
6. 重现导致问题的情况。
7. 单击**禁用**按钮停止跟踪。

创建的跟踪文件存储在 /var/log/kaspersky/kesl/ 目录中。

# 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。每个组件的清单文件名相同，但清单文件的内容不同。清单文件经过数字签名，其完整性也得到检查。

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。在 Windows 设备上运行完整性检查实用程序需要管理员账户。

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
- 检查 Kaspersky Endpoint Security 管理 Web 插件目录：
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console\server\plugins\kesl_<版本编号>\integrity_check.xml – 在装有 Windows 操作系统的设备上
  - /var/opt/kaspersky/ksc-web-console/server/plugins/kesl_<版本编号>/integrity_check.xml – 在装有 Linux 操作系统的设备上

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。

*要运行完整性检查实用程序，请运行以下命令之一：*

- 对软件包执行应用程序完整性检查：

  ```
  integrity_checker [<清单文件的路径>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- 要检查图形用户界面软件包的完整性：

  ```
  integrity_checker <清单文件的路径> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-with-filename
  ```

- 要检查 Kaspersky Endpoint Security MMC 管理插件的完整性：

  ```
  integrity_checker.exe [<清单文件的路径>]
  ```

- 检查网络代理的完整性：

  ```
  integrity_checker <清单文件的路径>
  ```

- 要检查 Kaspersky Endpoint Security 管理 Web 插件目录的完整性：

  ```
  integrity_checker <清单文件的路径> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds
  ```

  默认路径表示清单文件与完整性检查实用程序位于同一目录。

您可以使用以下可选设置运行该实用程序：

- `--crl <目录>` 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 <文件名>`，其中 `<文件名>` 是将以 DEBUG 详细级别记录扫描期间发生的事件的文件名称。
- `--signature-type kds` 是要检查的签名类型（扫描 Kaspersky Endpoint Security 管理 Web 插件目录时需要此选项）。
- `--signature-type kds-with-filename` 是要检查的签名类型（检查应用程序软件包和图形用户界面软件包时需要此选项）。

- `--single-file <文件>` 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。

您可以通过运行 `integrity_checker --help` 命令，在实用程序选项帮助中查看所有可用完整性检查实用程序设置的说明。

检查清单文件的结果如下所示：

- `SUCCEEDED` — 已确认文件的完整性（返回码 0）。
- `FAILED`— 未确认文件的完整性（返回码不是 0）。

如果在应用程序启动时检测到应用程序或网络代理的完整性被破坏，Kaspersky Endpoint Security 会在事件日志和 Kaspersky Security Center 中生成相应的事件。

# 联系技术支持

如果您在应用程序文档或其他应用程序信息来源中找不到问题的解决方案，建议联系技术支持团队。技术支持专家将回答您关于安装和使用 Kaspersky Endpoint Security 的任何问题。

卡巴斯基为 Kaspersky Endpoint Security 的整个生命周期提供支持（请参阅应用程序生命周期）。与技术支持部门联系之前，请阅读支持规则。

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 门户设计用于方便用户与卡巴斯基专家之间通过在线请求进行交互。通过使用 Kaspersky CompanyAccount 门户，您可以跟踪卡巴斯基专家处理电子请求的进度，并存储电子请求的历史记录。

您可以在一个 Kaspersky CompanyAccount 帐户下注册您所有的公司员工。单个帐户使您能够集中管理注册员工向卡巴斯基发送的电子请求，同时通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户支持以下语言：

- 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。

# 关于应用程序跟踪文件

*跟踪文件*可跟踪应用程序命令的逐步执行情况，并检测错误发生在应用程序操作的哪个阶段。

默认情况下，不会生成应用程序跟踪文件。您可以通过常规应用程序设置和图形用户界面在命令行中启用或禁用应用程序跟踪文件的生成并定义跟踪文件中的详细程度。

如果您启用了应用程序跟踪文件，这些文件将存储在 /var/log/kaspersky/kesl/ 目录中。访问此目录需要 root 权限。

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，还需要其他磁盘空间。

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。

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。

# 配置应用程序跟踪设置

如果您在通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security 应用程序，则可以使用 Web Console 或管理控制台在 Kaspersky Endpoint Security 策略设置中管理该应用程序的跟踪设置。

如果您在命令行上管理应用程序，则可以在常规应用程序设置中配置应用程序的跟踪设置。

### 编辑 Web Console 中的跟踪设置

在 Web Console 中，您可以在策略属性（**应用程序设置 → 常规设置 → 技术支持**）中管理应用程序跟踪设置。

要应用跟踪设置，必须重新启动应用程序。

### 编辑管理控制台中的跟踪设置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略、使用管理控制台创建策略）（**安全控制 → 应用程序设置**）中管理应用程序跟踪设置。

在“**跟踪和转储设置**”下，单击“**配置**”以打开一个窗口，您可以在其中编辑跟踪设置（请见下表）。

应用程序跟踪设置

| 设置 | 描述 |
| --- | --- |
| **跟踪文件目录的路径** | 用于输入跟踪文件的目录路径的字段。<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。 |

要应用跟踪设置，必须重新启动应用程序。

### 在命令行中编辑跟踪设置

在命令行中，您可以使用 常规应用程序设置中的 `TraceLevel`、 `TraceFolder`、 `TraceMaxFileCount` 和 `TraceMaxFileSize` 设置来配置应用程序跟踪设置。

`TraceLevel` 设置可让您启用或禁用应用程序跟踪文件的创建，并指定跟踪文件的详细程度。设置可以使用以下值：

- `Detailed` – 生成详细的跟踪文件。
- `MediumDetailed` – 生成包含信息消息和错误消息的跟踪文件。
- `NotDetailed` – 生成一个包含错误消息的跟踪文件。
- `None`（默认值）– 不生成跟踪文件。

`TraceFolder` 设置可让您指定存储应用程序跟踪文件的目录。默认值：/var/log/kaspersky/kesl。如果指定其他目录，请确保运行 Kaspersky Endpoint Security 的帐户对该目录仅具有读/写权限（rwx-------- 700 权限）。需要 root 特权才能访问默认跟踪文件目录。

`TraceMaxFileCount` 设置可让您指定应用程序跟踪文件的最大数量。该设置可采用 1 至 10000 之间的值。默认值：10。

`TraceMaxFileSize` 设置可让您指定应用程序跟踪文件的最大大小（以兆字节为单位）。该设置可采用 1 至 1000 之间的值。默认值：500。

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。

更改`TraceFolder`、`TraceMaxFileCount`或`TraceMaxFileSize`设置的值后，需要重新启动应用程序。

# 应用程序管理插件跟踪文件

管理插件跟踪文件不会自动发送到卡巴斯基。

跟踪文件以人类可读的格式保存。建议在将信息发送到卡巴斯基之前保护信息，以避免未经授权的访问。

## MMC 管理插件跟踪文件

如果您使用管理控制台来管理 Kaspersky Endpoint Security，则有关管理 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。

管理插件跟踪文件的内容

跟踪文件包含以下常规数据：

- 事件时间。
- 执行线程编号。
- 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，跟踪文件还可能包含以下信息：

- 个人数据，包括姓氏、名字和中间名（如果此类数据是文件路径的一部分）。
- 用于登录操作系统的账户名（如果用户账户名是文件名的一部分）。

# 关于转储文件

*转储文件*包含有关在创建转储文件时 Kaspersky Endpoint Security 进程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。您可以启用或禁用应用程序发生故障时的转储。

如果您已启用转储功能，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。

# 管理转储文件设置

如果您在通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security 应用程序，则可以使用 Web Console 或管理控制台在 Kaspersky Endpoint Security 策略设置中管理该应用程序的转储文件设置。

如果您使用命令行来管理应用程序，则可以通过 kesl.ini 配置文件启用或禁用转储。

转储文件的最大数量有限。

根据操作系统设置，可能无法创建用户转储文件。确保使用 `sysctl kernel.yama.ptrace_scope=0` 配置系统内核。

### 在 Web Console 中管理转储文件设置

在 Web Console 中，您可以在策略属性（**应用程序设置** → **常规设置** → **技术支持**）中管理应用程序转储文件设置。

Web Console 策略属性中的应用程序转储文件设置详见附录 5。

您必须重新启动应用程序才能应用转储文件设置。

### 在管理控制台中管理转储文件设置

在管理控制台中，您可以在策略属性（在管理控制台中管理策略，使用管理控制台创建策略）（**安全控制** → **应用程序设置**）中管理应用程序的转储设置。

在 **跟踪和转储设置**下，单击 **配置**可打开一个窗口，您可以在其中编辑转储设置（请参见下表）。

转储文件设置

| 设置 | 描述 |
| --- | --- |
| **如果应用程序崩溃，创建转储文件** | 该复选框用于启用或禁用在应用程序崩溃时创建转储文件。<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。 |

您必须重新启动应用程序才能应用转储文件设置。

### 使用命令行来管理转储文件设置

*要通过 kesl.ini 配置文件启用或禁用转储，请执行以下操作：*

1. 停止 Kaspersky Endpoint Security。
2. 打开 /var/opt/kaspersky/kesl/common/kesl.ini 文件进行编辑。

3. 在**[General]**下，设置参数值：

   - `CoreDumps=yes`：启用在发生故障时转储。
   - `CoreDumps=no`：禁用转储。

4. 如果要更改保存转储文件的默认目录，请在 `CoreDumpsPath` 选项中指定该目录的路径。

5. 启动 Kaspersky Endpoint Security。

# 使用 Kaspersky Security Center 进行远程设备诊断

在 Kaspersky Security Center 中，您可以对客户端设备执行远程诊断。远程诊断程序可让您远程执行以下操作：

- 启用和禁用跟踪。
- 更改跟踪级别。
- 下载跟踪文件。
- 下载远程应用程序安装日志。
- 下载系统事件 (syslog) 日志。
- 启动、停止和重启应用程序。

## Web Console 中的远程诊断

如果您使用 Web Console 管理 Kaspersky Endpoint Security，则客户端设备的远程诊断将在远程诊断窗口中完成。

*要打开设备的远程设备诊断窗口：*

1. 在 Web Console 的主窗口中，选择“**资产（设备）**”→“**受管理设备**”。
   将打开受管理设备列表。

2. 选择您想要远程诊断的设备并单击<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.用于管理 Kaspersky Endpoint Security 的命令

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

您可以通过运行以下命令查看管理命令的帮助：

```
kesl-control --help < 命令组前缀 >
```

其中 < 命令组前缀 > 可接受以下值：

- -A：用于管理应用程序控制的命令
- -B：用于管理备份的命令
- -C：用于管理常规容器扫描设置的命令（容器扫描、容器监控）
- -D：用于管理设备控制的命令
- -E：用于管理应用程序事件的命令（在命令行中查看事件、在 Kaspersky Security Center 中查看事件）
- -F：用于管理防火墙的命令
- -H：用于管理受阻止设备的命令
- -J：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 的整合设置的命令
- -N: 用于管理网络流量扫描设置的命令
- -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（本地部署）和 Kaspersky Endpoint Detection and Response Optimum集成设置的命令
- -S：统计命令
- -T：用于管理应用程序任务和设置的命令
- -U：用于管理用户和角色的命令
- -V：在用于保护虚拟环境的 Light Agent 模式中的应用程序命令

- -W：事件输出命令（在命令行中查看事件、在 Kaspersky Security Center 中查看事件）
- -X：用于管理 Kaspersky Endpoint Security 应用程序与 Sandbox 的集成设置的命令

# 用于管理应用程序任务和设置的命令

-T 前缀表示该命令属于用于管理应用程序设置和任务的命令组。

-C 前缀表示该命令属于用于管理容器扫描设置（容器扫描、容器监控）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。

**命令语法**

```
kesl-control [-T] --export-settings [--file <配置文件路径>] [--json]
```

**参数和键**

`--file <配置文件路径>` 是将保存应用程序设置的配置文件的完整路径。

指定 `--json` ，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

## kesl-control --import-settings

此命令从配置文件导入所有应用程序设置，包括常规容器扫描设置、加密连接扫描设置、常规应用程序设置和任务设置。

**命令语法**

```
kesl-control [-T] --import-settings --file <配置文件路径> [--json]
```

**参数和键**

`--file <配置文件路径>` 是要从中将设置导入应用程序的配置文件的完整路径。

指定 `--json` 后，以 JSON 格式从配置文件中导入设置。如果不指定 `--json`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。

**命令语法**

```
kesl-control [-T] --update-application
```

## 管理常规应用程序设置的命令

### kesl-control --get-app-settings 命令

该命令将常规应用程序设置的当前值输出到控制台或配置文件。

**命令语法**

```
kesl-control [-T] --get-app-settings [--file <配置文件路径>] [--json]
```

**参数和键**

`--file <配置文件路径>` 是应用程序常规设置将写入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。如果未指定 `--json`选项，则设置以 INI 格式输出。

### kesl-control --set-app-settings 命令

该命令使用命令选项或从配置文件导入设置来配置常规应用程序设置。

**命令语法**

通过命令选项定义设置：

```
kesl-control [-T] --set-app-settings <设置名称>=<设置值> [<设置名称>=<设置值>]
```

通过配置文件定义设置：

```
kesl-control [-T] --set-app-settings --file <配置文件路径> [--json]
```

**参数和键**

< 设置名称 >=< 设置值 > 是其中一项常规应用程序设置的名称和值。

`--file` < 配置文件路径 > 是要从中将设置导入应用程序的配置文件的完整路径。

指定 `--json` ，则以 JSON 格式将配置文件中的设置导入应用程序。如果不指定 `--json`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。

**命令语法**

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

**参数和键**

< 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。

`--file` < 配置文件路径 > 是将写入任务设置的配置文件的路径。如果不指定 `--file` 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 `--json` ，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

kesl-control --set-settings

此命令通过命令选项或从配置文件导入设置来定义指定任务的设置。

**命令语法**

通过命令选项定义设置：

```
kesl-control [-T] --set-settings < 任务 ID/名称 > < 设置名称 >=< 设置值 > [< 设置名称 >=< 设置值 >] [--add-path < 路径 >] [--del-path < 路径 >] [--add-exclusion < 路径 >] [--del-exclusion < 路径 >]
```

通过配置文件定义设置：

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

**参数和键**

< 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。

< 设置名称 >=< 设置值 > 是一项任务设置的名称和值。

--add-path < 路径 > 添加包含要扫描的对象的目录路径。

--del-path < 路径 > 删除包含要扫描的对象的目录路径。

--add-exclusion < 路径 > 添加包含要从扫描中排除的对象的目录路径。

--del-exclusion < 路径 > 删除包含要从扫描中排除的对象的目录路径。

--file < 配置文件路径 > 是要从中导入任务设置的配置文件的完整路径。

指定 --json 后，以 JSON 格式从配置文件中导入设置。如果不指定 --json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。

**命令语法**

```
kesl-control [-T] --set-settings < 任务 ID/名称 > --set-to-default
```

**参数和键**

< 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。

kesl-control --get-schedule 命令

该命令将指定任务的当前计划输出到控制台或配置文件。

**命令语法**

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

**参数和键**

< 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。

--file < 配置文件路径 > 是将写入任务计划设置的配置文件的路径。如果不指定 --file 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 --json ，则以 JSON 格式输出设置。如果未指定 --json选项，则设置以 INI 格式输出。

kesl-control --set-schedule 命令

该命令通过命令选项或从配置文件导入设置来定义指定任务的计划。

**命令语法**

通过命令选项定义设置：

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

通过配置文件定义设置：

```
kesl-control [-T] --set-schedule <任务 ID/名称> --file <配置文件路径> [--json]
```

**参数和键**

<任务 ID/名称> 是创建任务时分配给任务的 ID，或命令行中的任务名称。

<设置名称>=<设置值> 是一项任务计划设置的名称和值。

--file <配置文件路径> 是将从中导入任务计划设置的配置文件的完整路径。

指定 --json 后，以 JSON 格式从配置文件中导入设置。如果不指定 --json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。

**命令语法**

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

**参数和键**

指定 --json，则以 JSON 格式输出设置。

kesl-control --get-task-state

此命令输出指定任务的状态。

**命令语法**

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

**参数和键**

< 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。

指定 --json，则以 JSON 格式输出设置。

kesl-control --create-task

此命令使用默认设置或配置文件中指定的设置来创建指定类型的任务。

**命令语法**

使用默认设置创建任务：

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

使用配置文件中的设置创建任务：

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

**参数和键**

< 任务名称 > 是您为新任务指定的名称。

< 任务类型 > 是您正在创建的任务类型的标识。

--file < 配置文件路径 > 是配置文件的完整路径，该配置文件包含将用于创建任务的设置。

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。

kesl-control --delete-task

此命令删除一项任务。

**命令语法**

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

**参数和键**

< 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。

kesl-control --start-task

该命令启动一项任务。

**命令语法**

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

**参数和键**

<任务 ID/名称> 是创建任务时分配给任务的 ID，或命令行中的任务名称。

[-W]：启用当前事件输出。

[--progress]：显示任务进度。

kesl-control --stop-task

该命令停止一项任务。

**命令语法**

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

**参数和键**

<任务 ID/名称> 是创建任务时分配给任务的 ID，或命令行中的任务名称。

[-W]：启用当前事件输出。

kesl-control --suspend-task

此命令暂停一项任务。

**命令语法**

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

**参数和键**

<任务 ID/名称> 是创建任务时分配给任务的 ID，或命令行中的任务名称。

kesl-control --resume-task

此命令恢复一项任务。

**命令语法**

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

**参数和键**

< 任务 ID/名称 > 是创建任务时分配给任务的 ID，或命令行中的任务名称。

kesl-control --scan-file

此命令创建并运行一项自定义扫描任务。

**命令语法**

```
kesl-control [-T] --scan-file < 路径 > [--action < 操作 >]
```

**参数和键**

< 路径 > 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` < 操作 > 是应用程序将对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。

**命令语法**

```
kesl-control [-T] --scan-container < ID/名称 [: 标签 ]>
```

**参数和键**

< ID/名称 [: 标签 ]> 是容器或镜像的名称或 ID。您可以使用**掩码**来扫描多个对象。

您可以用 * （星号）字符来创建文件或目录名称掩码。

您可以指定单个 * 字符来表示文件或目录名称中 / 字符前面的任意一组字符（包括空集）。例如，`/dir/*/file` 或 `/dir/*/*/file`。

您可以指定两个连续的 * 字符来表示文件或目录名称中的任意一组字符（包括空集和 / 字符）。例如，`/dir/**/file*/` 或 `/dir/file**/`。

** 掩码在目录名称中只能使用一次。例如，`/dir/**/**/file` 是不正确的掩码。

可以使用单个 ? 字符表示文件名或目录名中的任意一个字符。

# 用于管理对象的执行防护的命令

kesl-control --get-prevention-state

此命令将输出指定组件的对象执行防护规则。

**命令语法**

```
kesl-control [-T] --get-prevention-state [--kata|--edro]
```

**参数和键**

`--kata`：EDR Expert (on-premise) 组件的执行防护规则

`--edro`：EDR Optimum 组件的执行防护规则

# 管理常规容器扫描设置的命令

The kesl-control --get-container-settings 命令

该命令将当前的常规容器扫描设置输出到控制台或配置文件。

**命令语法**

```
kesl-control [-C] --get-container-settings [--file <配置文件路径>] [--json]
```

**参数和键**

`--file <配置文件路径>` 是将写入常规容器扫描设置的配置文件路径。如果不指定 `--file` 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 `--json` ，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

The kesl-control --set-container-settings 命令

该命令使用命令选项或从配置文件导入设置来配置常规容器扫描设置。

**命令语法**

通过命令选项定义设置：

```
kesl-control [-C] --set-container-settings <设置名称>=<设置值> [<设置名称>=<设置值>]
```

通过配置文件定义设置：

```
kesl-control [-C] --set-container-settings --file <配置文件路径> [--json]
```

**参数和键**

<设置名称>=<设置值>是其中一项常规容器扫描设置的名称和值。

`--file` <配置文件路径>是配置文件的完整路径；此文件中的常规容器扫描设置将被导入应用程序。

指定 `--json` ，则以 JSON 格式将配置文件中的设置导入应用程序。如果不指定 `--json`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。

**命令语法**

```
kesl-control -N --query user

kesl-control -N --query auto

kesl-control -N --query kl
```

kesl-control --clear-web-auto-excluded

此命令清除应用程序自动排除在扫描范围之外的域列表。

**命令语法**

```
kesl-control -N --clear-web-auto-excluded
```

kesl-control --get-net-settings

该命令将当前的网咯流量扫描设置输出到控制台或配置文件。

**命令语法**

```
kesl-control [-N] --get-net-settings [--file <配置文件路径>] [--json]
```

**参数和键**

`--file <配置文件路径>` 是将写入网络流量扫描设置的配置文件路径。如果不指定 `--file` 选项，设置将输出到控制台。

如果指定文件名但未指定其路径，则将在当前目录中创建该文件。如果指定路径中已存在文件，该文件将被覆盖。如果指定的目录不存在，则不会生成配置文件。

指定 `--json` ，则以 JSON 格式输出设置。如果未指定 `--json`选项，则设置以 INI 格式输出。

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。

**命令语法**

通过命令选项定义设置：

```
kesl-control [-N] --set-net-settings <设置名称>=<设置值> [<设置名称>=<设置值>]
```

通过配置文件定义设置：

```
kesl-control [-N] --set-net-settings --file <配置文件路径> [--json]
```

**参数和键**

`<设置名称>=<设置值>` 是其中一项网络流量扫描设置的名称和值。

`--file <配置文件路径>` 是将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。

**命令语法**

```
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。

**命令语法**

```
kesl-control [-N] --add-certificate <证书路径>
```

**参数和键**

<证书路径>是要添加的证书文件（PEM 或 DER 格式）的路径。

### kesl-control --remove-certificate

此命令将证书从受信任根证书列表中移除。

**命令语法**

```
kesl-control [-N] --remove-certificate <证书主题>
```

### kesl-control --add-bypass-endpoints

此命令可让您添加流量拦截排除。

**命令语法**

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <远程 IP 地址>
--dst-port <目标端口>
```

**参数和键**

<in|out>是被排除连接中的流量方向：出站或入站。

<远程 IP 地址>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。

<目标端口>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。

**命令语法**

```
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。

**命令语法**

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <远程 IP 地址> --dst-port <目标端口>
```

**参数和键**

<in|out> 是被排除连接中的流量方向：出站或入站。

<远程 IP 地址> 是远程设备的 IPv4 或 IPv6 地址，该设备的流量将被排除在拦截范围之外（具体取决于流量方向）。

<目标端口> 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）。

# 统计命令

-S 前缀表示该命令属于统计命令组。

kesl-control --app-info

此命令输出有关应用程序的信息。

**命令语法**

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

**参数和键**

指定 --json，则以 JSON 格式输出设置。

kesl-control --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。

**命令语法**

```
kesl-control [-S] --supported-tech-info [--json]
```

**参数和键**

`--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。

**命令语法**

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

**参数和键**

`[--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。

**命令语法**

```
kesl-control [-S] --omsinfo --file <文件路径>
```

# 用于显示事件的命令

### kesl-control -W

该命令将启用当前应用程序事件的显示。该命令将返回事件的名称以及有关事件的其他信息。您可以使用该命令显示所有当前应用程序事件或仅显示与当前运行中任务相关的事件。

**命令语法**

```
kesl-control -W [--query "<过滤条件>"]
```

**参数和键**

<过滤条件>指定一个或多个逻辑表达式，采用 <字段> <比较操作> '<值>' 格式，并使用 and 逻辑运算符组合，用于输出特定当前事件。

# 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（在命令行中查看事件、在 Kaspersky Security Center 中查看事件）。

### kesl-control -E

此命令输出有关应用程序事件日志中所有事件的信息。您可以使用 `less` 命令在显示的事件列表中导航。

**命令语法**

```
kesl-control -E
```

### kesl-control -E --query

此命令输出有关应用程序事件日志中的事件的信息。您可以使用 `less` 命令在显示的事件列表中导航。您可以使用筛选器来输出特定事件或将事件列表输出到文件。

**命令语法**

```
kesl-control -E --query "<过滤条件>" [--db <数据库文件>] [-n <数量>] [--file <文件路径>] [--json] [--reverse]
```

**参数和键**

< 数据库文件 > 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。

< 过滤条件 > 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。

< 数量 > 是要显示的所选内容中最新事件的数量（从所选内容的末尾开始计算的记录数量）。

`--file` < 文件路径 > 是要将事件输出到的文件的完整路径。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。

> 只有当应用程序在基本模式或 Endpoint Detection and Response Agent 模式下运行时，才能使用添加或移除授权许可密钥命令。如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则管理授权许可密钥的命令将终止并显示错误。您可以将应用程序作为 Kaspersky Security for Virtualization Light Agent 的一部分进行激活，因此无需单独激活该应用程序。

kesl-control --add-active-key

该命令可让您使用密钥文件或激活码向应用程序添加活动授权许可密钥。

您可以使用此命令添加应用程序的主授权许可密钥以及附加功能的授权许可密钥。您不需要在命令中指定密钥的类型。

**命令语法**

`kesl-control [-L] --add-active-key` < 密钥文件路径 >

`kesl-control [-L] --add-active-key` < 激活码 >

**参数和键**

< 密钥文件路径 > 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。

< 激活码 > 是 激活码。

例如：
*从 /home/test/00000001.key 文件中添加一个密钥作为活动密钥：*

```
kesl-control --add-active-key /home/test/00000001.key
```

### kesl-control --add-reserve-key

该命令可让您使用密钥文件或激活码向应用程序添加备用授权许可密钥。

您可以使用此命令添加应用程序的主授权许可密钥以及附加功能的授权许可密钥。您不需要在命令中指定密钥的类型。

如果活动密钥尚未被添加到设备上的应用程序，则命令失败。

**命令语法**

```
kesl-control [-L] --add-reserve-key <密钥文件路径>

kesl-control [-L] --add-reserve-key <激活码>
```

**参数和键**

<密钥文件路径> 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。

<激活码> 是 激活码。

例如：
*使用 /home/test/00000002.key 文件添加备用密钥：*

```
kesl-control --add-reserve-key /home/test/00000002.key
```

### kesl-control --remove-active-key

此命令可让您删除活动的授权许可密钥。

**命令语法**

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

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

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

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

**参数和键**

`--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-premise) 授权许可密钥。

如果未在命令行中指定 --edr-optimum、 --kuma、 --mdr 或 --edr-kata 选项，该命令将从应用程序中删除主要活动密钥。

kesl-control --remove-reserve-key

此命令可让您删除备用授权许可密钥。

**命令语法**

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

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

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

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

**参数和键**

--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 EDR Expert (on-premise) 授权许可备用密钥。

如果未在命令行中指定 --edr-optimum、 --kuma、 --mdr 或 --edr-kata 选项，该命令将从应用程序中删除主要备用密钥。

kesl-control -L --query

-L --query 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。

**命令语法**

```
kesl-control -L --query [--json]
```

**参数和键**

--json：以 JSON 格式输出数据。

kesl-control --load-mdr-blob

`--load-mdr-blob` 命令允许您将可用于与 Kaspersky Managed Detection and Response 整合的 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。

**命令语法**

```
kesl-control [-L] --load-mdr-blob <文件路径 MDR BLOB>
```

kesl-control --remove-mdr-blob

`--remove-mdr-blob` 命令允许您从设备中删除用于与 Kaspersky Managed Detection and Response 整合的 BLOB 文件。

**命令语法**

```
kesl-control [-L] --remove-mdr-blob
```

# 用于防火墙管理的命令

-F 前缀表示该命令属于防火墙管理命令。

kesl-control --add-rule

此命令用于添加一个新的网络数据包规则。

**命令语法**

```
kesl-control [-F] --add-rule [--name <规则名称>] [--action <操作>] [--protocol <协议>] [--direction <方向>] [--remote <远程地址>[:<端口范围>]] [--local <本地地址>[:<端口范围>]] [--at <索引>]
```

**参数和键**

`--name <规则名称>` 是网络数据包规则的名称。

`--action <操作>` 是要对网络数据包规则中指定的连接执行的操作。

`--protocol <协议>` 是您要监控其网络活动的通信协议类型。

`--direction <方向>` 是受监控网络活动的方向。

`--remote <远程地址>[:<端口范围>]` 是远程设备的网络地址。

`--local <本地地址>[:<端口范围>]` 是 Kaspersky Endpoint Security 设备的网络地址。

`--at <索引>` 是该规则在网络数据包规则列表中的编号。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。

**命令语法**

```
kesl-control [-F] --del-rule --name <规则名称>

kesl-control [-F] --del-rule --index <索引>
```

**参数和键**

`--name <规则名称>` 是网络数据包规则的名称。

`--index <索引>` 是该规则在网络数据包规则列表中的编号。

### kesl-control --move-rule

该命令用于更改网络数据包规则的执行优先级。

**命令语法**

```
kesl-control [-F] --move-rule --name <规则名称> --at <索引>

kesl-control [-F] --move-rule --index <索引> --at <索引>
```

**参数和键**

`--name <规则名称>` 是网络数据包规则的名称。

`--index <索引>` 是网络数据包规则列表中规则的当前编号。

`--at <索引>` 是该规则在网络数据包规则列表中的新编号。

### kesl-control --add-zone

此命令用于将地址添加到网络区域。

**命令语法**

```
kesl-control [-F] --add-zone --zone <区域> --address <地址>
```

**参数和键**

`--zone <区域>` 是网络区域的预定义名称。

`--address <地址>` 是网络地址或子网。

### kesl-control --del-zone

此命令用于从网络区域中移除一个地址。

**命令语法**

```
kesl-control [-F] --del-zone --zone <区域> --address <地址>
kesl-control [-F] --del-zone --zone <区域> --index <地址索引>
```

**参数和键**

`--zone <区域>` 是网络区域的预定义名称。

`--address <地址>` 是网络地址或子网。

`--index <地址索引>` 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。

**命令语法**

```
kesl-control -F --query
```

## 用于管理被阻止设备的命令

-H 前缀表示该命令属于用于管理被 反加密勒索 和 网络威胁防护 阻止的设备的命令组。

### The kesl-control --get-blocked-hosts 命令

该命令可让您将被阻止设备的列表输出到控制台。

**命令语法**

```
kesl-control [-H] --get-blocked-hosts
```

### The kesl-control --allow-hosts 命令

该命令可让您解除对被阻止设备的阻止。

**命令语法**

```
kesl-control [-H] --allow-hosts <地址>
```

**参数和键**

<地址>是设备或子网的 IP 地址（IPv4/IPv6，包括缩写形式的地址）。您可以指定设备或子网的多个 IP 地址，用空格分隔。

## 用于管理设备控制的命令

D 前缀表示该命令属于用于管理设备控制的命令组。

### kesl-control --get-device-list

此命令可输出主机上已安装或连接到主机的设备列表，或将已连接设备列表导出到 JSON 文件。

**命令语法**

```
kesl-control [-D] --get-device-list [--all] [--json] [--export <文件>]
```

**参数和键**

`--all`列出所有已连接的设备。

`--json`列出已连接的 JSON 格式设备。

`--export <文件>`将已连接设备列表导出到文件，格式为受信任设备列表。您需要指定 JSON 文件的完整路径。

### kesl-control --trusted-devices

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。

**命令语法**

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <文件>]
```

**参数和键**

--list – 显示受信任设备列表。

--add <ID> 按设备 ID 或设备 ID 掩码将设备添加到受信任设备列表。

--delete <ID> 按设备 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 <文件> 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。

## kesl-control --request-temporary-device-access

此命令可让您创建访问请求文件，以请求对被阻止设备进行临时访问。

**命令语法**

```
kesl-control [-D] --request-temporary-device-access --device-id <设备 ID> --access-duration <访问持续时间> --path <访问请求文件的路径>
```

**参数和键**

--device-id <设备 ID> 指定您要访问的被阻止设备的 ID。

--access-duration <访问持续时间> 指定您希望能够访问设备的时间段（以小时为单位）。可能的值：1到100

--path <访问请求文件的路径> 指定要将扩展名为 .akey 的访问请求文件保存到其中的目录路径。

## kesl-control --upload-temporary-device-access-key

此命令可让您上传访问密钥，以获取对被阻止设备的临时访问权限。

**命令语法**

```
kesl-control [-D] --upload-temporary-device-access-key --path <包含访问密钥的文件的路径>
```

**参数和键**

--path <包含访问密钥的文件的路径> 是包含设备访问密钥的文件（扩展名为 .acode 的文件）的路径。

# 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。

## kesl-control --get-app-list

该命令输出由"清查"任务在客户端设备上找到的应用程序列表。

**命令语法**

```
kesl-control [-A] --get-app-list [--json]
```

**参数和键**

`--json`：以 JSON 格式输出数据。

## kesl-control --get-categories

该命令输出已创建的应用程序控制类别列表。

**命令语法**

```
kesl-control [-A] --get-categories [--names <类别 1 的名称> <类别 2 的名称> ... <类别 N 的名称>] [--file <配置文件路径>] [--json]
```

**参数和键**

`<类别 1 的名称> <类别 2 的名称> ... <类别 N 的名称>` 是要查看其信息的类别名称。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 <配置文件路径>` 是设置将写入到的 JSON 配置文件的完整路径。

`--json`：以 JSON 格式输出数据。

## kesl-control --set-categories

此命令可让您创建或编辑已创建的应用程序控制类别列表。

**命令语法**

```
kesl-control [-A] --set-categories [--names <类别 1 的名称> <类别 2 的名称> ... <类别 N 的名称>] --file <配置文件路径>
```

**参数和键**

<类别 1 的名称> <类别 2 的名称> ... <类别 N 的名称> 是您要更改其信息的类别名称。如果要更改有关多个类别的信息，请指定类别的名称，用空格分隔。如果您不指定类别名称，该类别将被从列表中删除。

--file <配置文件路径> 是包含类别设置的配置文件路径。

### kesl-control --get-settings 21

该命令输出已创建的应用程序控制规则列表。

**命令语法**

```
kesl-control --get-settings 21 [--file <配置文件路径>] [--json]
```

**参数和键**

--file <配置文件路径> 是要向其中写入设置的配置文件的完整路径。

--json：以 JSON 格式输出数据。

### kesl-control --set-settings 21

此命令可让您编辑已创建的应用程序类别和应用程序控制规则的列表。

**命令语法**

```
kesl-control --set-settings 21 [--file <配置文件路径>] [--json]
```

**参数和键**

--file <配置文件路径> 是将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。

### kesl-control --set-to-default 21

此命令可让您删除应用程序类别和应用程序控制规则的列表。

**命令语法**

```
kesl-control --set-settings 21 --set-to-default
```

# Web 控制管理命令

kesl-control --get-settings 26

此命令可让您显示指定的 Web 控制设置的列表。

**命令语法**

```
kesl-control --get-settings 26 [--file <配置文件路径>] [--json]
```

**参数和键**

`--file <配置文件路径>` 是要向其中写入设置的配置文件的完整路径。

`--json`：以 JSON 格式输出数据。

kesl-control --set-settings 26

此命令可让您编辑指定的 Web 控制设置的列表。

**命令语法**

```
kesl-control --set-settings 26 [--file <配置文件路径>] [--json]
```

**参数和键**

`--file <配置文件路径>` 是将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。

kesl-control --set-to-default 26

此命令可让您删除指定的设置并将 Web 控制设置重置为默认规则。

**命令语法**

```
kesl-control --set-settings 26 --set-to-default
```

# 用于管理备份的命令

-B 前缀表示该命令属于用于管理备份存储的命令组。

kesl-control -B --mass-remove

该命令从备份中删除部分或全部对象。

**命令语法**

删除全部对象：

```
kesl-control -B --mass-remove
```

删除符合筛选条件的对象：

```
kesl-control -B --mass-remove --query "< 过滤条件 >"
```

**参数和键**

< 过滤条件 > 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。

kesl-control -B --query

此命令输出有关备份对象的信息。

**命令语法**

输出有关备份中所有对象的信息：

```
kesl-control -B --query [-n < 数量 >] [--json] [--reverse]
```

输出有关符合筛选条件的备份对象的信息：

```
kesl-control -B --query ["< 过滤条件 >"] [-n < 数量 >] [--json] [--reverse]
```

**参数和键**

< 过滤条件 > 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，应用程序将显示备份中的所有对象的详细信息。

< 数量 > 是要显示的最近对象的数量。如果您不指定 -n 开关，则会显示最后 30 个对象。要显示所有对象，请指定 0。

--json：以 JSON 格式输出数据。

--reverse — 倒序输出对象（最新对象在顶部，最早对象在底部）。

kesl-control -B --restore

此命令从备份中恢复对象。

**命令语法**

```
kesl-control -B --restore <对象 ID> [--file <文件路径>]
```

**参数和键**

<对象 ID> 是备份区对象的 ID。

--file <文件路径> 是文件的新名称以及用于保存该文件的目录路径。如果不指定 --file 选项，则对象将以其原始名称和原始位置恢复。

# 用于管理隔离区的命令

-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。

**命令语法**

删除全部文件：

```
kesl-control -Q --mass-remove
```

删除符合筛选条件的文件：

```
kesl-control -Q --mass-remove --query "<过滤条件>"
```

**参数和键**

<过滤条件> 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。

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。

**命令语法**

```
kesl-control [-Q] --put <文件路径> [--md5] [--sha256] [--save-original-file]
```

**参数和键**

<文件路径>是要隔离的文件路径。

`--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。

**命令语法**

输出所有被隔离文件的信息：

```
kesl-control -Q --query [-n <数量>] [--json]
```

显示符合过滤条件的隔离文件信息：

```
kesl-control -Q --query ["<过滤条件>"] [-n <数量>]
```

**参数和键**

<过滤条件>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。

<数量>是要显示的最新被隔离文件的数量。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。

**命令语法**

```
kesl-control -Q --restore <文件 ID> [--file <文件路径>]
```

**参数和键**

<文件 ID>：被隔离文件的 ID。

`--file <文件路径>` 是文件的新名称以及用于保存该文件的目录路径。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。

# 用于管理用户和角色的命令

-U 前缀表示该命令属于用于管理用户和角色的命令组。

kesl-control --get-user-list

此命令输出用户和角色的列表。

**命令语法**

```
kesl-control [-U] --get-user-list
```

kesl-control --grant-role

此命令将角色分配给特定用户。

**命令语法**

```
kesl-control [-U] --grant-role <角色> <用户>
```

kesl-control --revoke-role

此命令撤销特定用户的角色。

**命令语法**

```
kesl-control [-U] --revoke-role <角色> <用户>
```

# 用于管理 EDR Expert（本地部署）组件的命令

-R 前缀表示该命令属于用于管理与Kaspersky Endpoint Detection and Response (KATA) Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert（本地部署） 和 Kaspersky Endpoint Detection and Response Optimum进行集成的设置的命令组。

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）。

**命令语法**

```
kesl-control [-R] --add-kataedr-server-certificate < 文件 > [--server-type
<response|telemetry>]
```

**参数和键**

< 文件 > 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 (OSMP) 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）。

**命令语法**

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type
<response|telemetry>]
```

**参数和键**

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (OSMP) 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。

**命令语法**

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

**参数和键**

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (OSMP) 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）。

**命令语法**

```
kesl-control [-R] --add-kataedr-client-certificate < 文件 > [--server-type
<response|telemetry>]
```

**参数和键**

< 文件 > 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (OSMP) 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）。

**命令语法**

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type
<response|telemetry>]
```

**参数和键**

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (OSMP) 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）。

**命令语法**

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

**参数和键**

`--server-type <response|telemetry>` 可让您选择要在 EDR Expert (OSMP) 集成模式下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

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 NDR (KATA) 组件的命令

-R 前缀表示该命令属于用于管理与Kaspersky Endpoint Detection and Response (KATA) Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert（本地部署） 和 Kaspersky Endpoint Detection and Response Optimum进行集成的设置的命令组。

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。

**命令语法**

```
kesl-control [-R] --add-katandr-server-certificate <文件>
```

**参数和键**

<文件> 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。

**命令语法**

```
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。

**命令语法**

```
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。

**命令语法**

```
kesl-control [-R] --add-katandr-client-certificate <文件>
```

**参数和键**

<文件> 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

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。

**命令语法**

```
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。

**命令语法**

```
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Kaspersky Endpoint Detection and Response (KATA) Kaspersky Network Detection and Response (KATA)、Kaspersky Endpoint Detection and Response Expert（本地部署） 和 Kaspersky Endpoint Detection and Response Optimum进行集成的设置的命令组。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。

**命令语法**

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

此命令可让您禁用设备的网络隔离。

**命令语法**

```
kesl-control [-R] --isolation-off
```

# 用于管理 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。

**命令语法**

```
kesl-control [-M] --add-kuma-server-certificate < 文件路径>
```

**参数和键**

< 文件路径 > 是包含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。

**命令语法**

```
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。

**命令语法**

```
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。

**命令语法**

```
kesl-control [-M] --add-kuma-client-certificate < 文件路径 >
```

**参数和键**

< 文件路径 > 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

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。

**命令语法**

```
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。

**命令语法**

```
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。

**命令语法**

```
kesl-control [-X] --add-sandbox-server-certificate < 文件>
```

**参数和键**

< 文件 > 是包含服务器证书的文件的路径。

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。

**命令语法**

```
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。

**命令语法**

```
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。

**命令语法**

```
kesl-control [-X] --add-sandbox-client-certificate <文件>
```

**参数和键**

<文件> 是包含客户端证书和私钥的加密容器（PFX 存档）的路径。

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。

**命令语法**

```
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。

**命令语法**

```
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。

**命令语法**

```
kesl-control [-X] --sandbox <路径 1> <路径 2>
```

**参数和键**

<路径> 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)。

**命令语法**

`kesl-control [-T] --scan-ioc --path <目录或文件路径> [--process on|off] [--hint <正则表达式>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--excludes <排除项列表>] [--scope <目录列表>] [--action Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]`

**参数和键**

`--path <目录或文件路径>` 是 IOC 文件的路径，或包含扩展名为 .IOC 或 .XML 的 IOC 文件的目录路径，用于执行扫描。

> 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 <正则表达式>` 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 <排除项列表>` 是从扫描中排除的路径列表。

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 <目录列表>` 是要扫描的附加目录列表。

> 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`— 应用程序将执行扫描**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。

# 在用于保护虚拟环境的 Light Agent 模式中的应用程序命令

-V 前缀表示该命令属于 Kaspersky Endpoint Security 命令组，这些命令在用于保护虚拟环境的 Light Agent 模式下使用（作为 Kaspersky Security for Virtualization Light Agent 的一部分）。

仅当在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境时，才能执行以下命令。

kesl-control --ksvla-info

该命令针对在用于保护虚拟环境的 Light Agent 模式下使用应用程序输出有关信息：

**命令语法**

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

kesl-control --viis-info

该命令针对 Light Agent（Kaspersky Endpoint Security 用作 Light Agent，作为 Kaspersky Security for Virtualization Light Agent 的一部分）连接到 Integration Server 输出有关信息：

**命令语法**

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

kesl-control --svm-info

该命令针对 Light Agent（Kaspersky Endpoint Security 用作 Light Agent，作为 Kaspersky Security for Virtualization Light Agent 的一部分）连接到 SVM 输出有关信息：

**命令语法**

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

# 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。

**命令语法**

```
kesl-control [-J] --export-metrics [--period <两次导出之间的间隔（秒）>|--interactive]
```

**参数和键**

`--period`可启用定期输出结果。

<两次导出之间的间隔（秒）>（以秒为单位）设置输出周期。

`--interactive`可启用交互式输出（按下**Enter**键时）。

# 附录 2.配置文件和默认应用程序设置

以下配置文件用于管理 Kaspersky Endpoint Security：

- 包含应用程序初始配置设置的配置文件：
  - autoinstall.ini 配置文件，通过 Kaspersky Security Center 安装应用程序时使用。
  - 通过命令行安装应用程序时使用的配置文件。
- 应用程序初始配置期间自动生成的预设配置文件，包含初始配置时设置的选项。这些设置在运行时应用。
- 您可以使用 Kaspersky Endpoint Security 管理命令创建的配置文件。这些配置文件可能包含任务设置和其他应用程序设置。您可以修改这些文件并导入到应用程序来修改相应选项。

# 编辑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。

# 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，您可以编辑这些文件中的设置值。

只有在技术支持专家的监督下并按照他们的说明，才能更改这些文件中的默认值。

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。

kesl.ini 配置文件的设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| **[General]** 部分包含以下设置： | | |
| `Locale` | Kaspersky Endpoint Security 发送到 Kaspersky Security Center 的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 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。 | `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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 | true/yes – 在 Light Agent 模式下使用应用程序保护虚拟环境。<br>false/no – 在标准模式下使用应用程序。 |
| EndpointAgentMode | 在 Endpoint Detection and Response Agent 模式下使用 Kaspersky Endpoint Security | true/yes – 应用程序在 Endpoint Detection and Response Agent 模式下使用。<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。 | 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）表示该应用程序以 Kaspersky Endpoint Security 的某种模式（标准模式、Endpoint Detection and Response Agent 模式或用于虚拟化的 Light Agent 模式）运行。 |
| 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。 |
| CoreDumps | 当应用程序发生故障时，启用创建转储文件。 | true/yes 表示应用程序崩溃时创建转储文件。<br>false/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：/var/opt/kaspersky/kesl/common/dumps。<br>需要 root 特权才能访问默认转储文件目录。 |
| MinFreeDiskSpace | 写入转储文件后剩余的最小磁盘存储空间（以 MB 为单位）。 | 默认值：300。 |
| ScanMemoryLimit | 应用程序的内存使用限制 (MB)。 | 默认值：8192。<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：2047。 |
| 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。 | 默认值：3。 |
| `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。 | `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。 | `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。 |
| **[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 | 对由应用程序创建或扫描的软件包进行标记，以防止其被 iptable 实用程序记录。 | 十进制值或带有 0x 前缀的十六进制数。<br>默认值：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 | 在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境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。 | 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。 |
| VdiMode | 在 Light Agent 模式下使用应用程序保护虚拟环境时启用 VDI 保护模式。<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。 | 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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>< 值 >% – 介于 RAM 的 1% 到 100% 之间的值。<br>< 值 >MB – 以 MB 为单位的值。<br>lowest/< <值> >%/< <值> >MB – 百分比值和以 MB 为单位的绝对值中的较小值。<br>highest/< 值 >%/< 值 >MB – 百分比值和以 MB 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>< 值 >MB – 以 MB 为单位的值。 |
| 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>< 值 >% – 介于 RAM 的 0% 到 100% 之间的值。<br>< 值 >MB – 以 MB 为单位的值。<br>lowest/< <值> >%/< <值> >MB – 百分比值和以 MB 为单位的绝对值中的较小值。<br>highest/< 值 >%/< 值 >MB – 百分比值和以 MB 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |
| 默认情况下，配置文件中没有**[Environment]**部分。 | | |
| ExperimentalContainerdSupport | 在容器监控组件（ContainerScan、容器监控）运行时启用对 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。 | 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

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

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

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
```

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`

# 常规应用程序设置

常规应用程序设置定义了应用程序整体的运行以及各个功能的操作。

常规应用程序设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `SambaConfigPath` | 存储 Samba 配置文件的目录。需要 Samba 配置文件以确保可将 `AllShared` 或 `Shared:SMB` 值用于 `Path` 设置。<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 配置文件的标准目录。<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 配置文件的标准目录。<br>默认值：/etc/exports。 |
| `TraceLevel` | 启用应用程序跟踪和跟踪文件的细节级别。 | `Detailed` – 生成详细的跟踪文件。<br>`MediumDetailed` – 生成包含信息消息和错误消息的跟踪文件。<br>`NotDetailed` – 生成一个包含错误消息的跟踪文件。<br>`None`（默认值）– 不生成跟踪文件。 |
| `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）。 |
| `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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |
| 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法应用程序的检测。<br>No（默认）：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。 |
| NamespaceMonitoring | 启用命名空间和容器扫描（容器扫描、容器监控）。<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。 | 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，扫描异步完成。这种文件操作拦截模式对系统性能影响较小，但是如果文件在应用程序对文件状态做出决定之前（例如）在扫描过程中更改其名称，则存在文件中的威胁不会被消除或删除的风险。不过，无论配置何种模式，文件威胁防护、设备控制和"执行防护"组件均以通知模式运行。 |
| 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络。<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 — 启用一种运行模式，在该模式下 Kaspersky Endpoint Security 使用轻量级版本的恶意软件数据库。<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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `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。 | `Yes` – 启用 Managed Detection and Response 组件。<br>`No`（默认值）– 禁用 Managed Detection and Response 组件。 |
| `UseEdrOptimum` | 启用 EDR Optimum 组件以便与 Kaspersky Endpoint Detection and Response Optimum整合。 | `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>://]<IP 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>]@]<IP address of the proxy server>:<port>`，如果连接到代理服务器时需要身份验证。<br>不支持通过 HTTPS 连接到代理服务器。 |
| `ProxyBypass` | 需绕过代理服务器的地址列表。 | 地址以 `<地址>[:<端口号>` 格式指定。<br>要指定地址，您可以使用掩码（`*`符号）和注释（在 `\` 符号之后）。 |
| `ProxyBypassEdr` | 连接到 Kaspersky Endpoint Detection and Response Expert (on-premise) Integration Server 时是否使用代理服务器。 | `Yes` — 连接到 Kaspersky Endpoint Detection and Response Expert (on-premise) Integration Server 时不使用代理服务器。<br>`No`（默认值）– 连接到 Kaspersky Endpoint Detection and Response Expert (on-premise) Integration Server 时使用代理服务器。 |
| `ProxyBypassNdr` | 连接到 Kaspersky Network Detection and Response (KATA) Integration Server 时是否使用代理服务器。 | `Yes` — 连接到 Kaspersky Network Detection and Response（KATA）Integration Server 时不使用代理服务器。<br>`No`（默认值）– 连接到 Kaspersk Network Detection and Response (KATA) Integration Server 时使用代理服务器。 |
| `ProxyBypassSandbox` | 连接到提供与 Sandbox 交互的服务器时是否使用代理服务器。 | `Yes`，在连接到提供与 Sandbox 交互的服务器时绕过代理服务器。<br>`No`（默认值），在连接到提供与 Sandbox 交互的服务器时使用代理服务器。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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：5。 |
| 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：/var/opt/kaspersky/kesl/private/storage/events.db。 |
| ExcludedMountPoint.item_# | 要从扫描范围中排除的挂载点。该排除适用于文件威胁防护、反加密勒索、容器监控（容器扫描、容器监控）组件以及可移动驱动器扫描任务的运行，并且也可在 ODS 和 ContainerScan 扫描任务的运行中配置。<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 SMB 和 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 协议挂载在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 协议挂载在计算机上的所有远程目录。<br>Mounted:< 文件系统类型 > – 从文件操作拦截中排除具有指定文件系统类型的所有已挂载目录。<br>/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。<br>< 包含 /mnt/user* 或 /mnt/**/user_share> 掩码的路径 – 从文件操作拦截中排除名称包含指定 **掩码** 的挂载点中的对象。<br>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>要排除挂载点 /dir，您需要明确指定 /dir（无星号）。<br>掩码 /dir/* 会排除 /dir 下面级别的所有挂载点，但不会排除 /dir 本身。掩码 /dir/** 会排除 /dir 级别下面的所有挂载点，但不会排除 /dir 本身。<br>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。 |
| 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。 | < 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。<br>您可以用 *（星号）字符来创建文件或目录名称掩码。<br>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。<br>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**/。<br>** 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。<br>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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| `UseOnDemandCPULimit` | 对以下类型的任务启用 CPU 使用率限制：*ODS*、*ContainerScan* 和 *InventoryScan*。 | `Yes`：启用 *ODS*、*ContainerScan* 和 *InventoryScan* 任务的 CPU 使用率限制。<br>`No`（默认）：禁用任务的 CPU 使用率限制。 |
| `OnDemandCPULimit` | 以下类型任务的所有处理器核心的最大利用率（百分比）：*ODS*、*ContainerScan* 和 *InventoryScan*。 | 10 到 100 之间的整数值。<br>默认值：100。 |
| `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 999999<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。 | 默认值：/var/opt/kaspersky/kesl/common/objects-backup/<br>访问默认目录需要 root 特权。 |
| `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 999999<br>0 表示隔离区大小不受限制。<br>如果应用程序在基本模式下使用，则默认值为 200；如果应用应用程序在 Light Agent 模式下使用，则默认值为 100。 |
| `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。 |
| `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划任务。<br>`No`：无论设备是否使用电池供电，都会运行计划任务。 |
| `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。 | `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` | 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 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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 自动重启应用程序以启动可更新内核模块。<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>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。 |
| SystemEventsTransmission | 启用将有关第三方应用程序事件的信息记录到 syslog<br>访问 syslog 需要 root 特权。 | Yes — 启用将有关第三方应用程序事件的信息记录到 syslog。<br>No （默认值）— 禁用将有关第三方应用程序事件的信息记录到 syslog。 |

# 常规容器扫描设置

常规容器扫描设置用于实时扫描命名空间和容器（容器扫描、容器监控）。

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。<br>支持与 Docker 28.5.2 及更早版本集成。 | Yes （默认）启用 Docker 容器管理系统。<br>No 禁用 Docker 容器管理系统。 |
| 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。 |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |

# 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。 |
| 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。 | 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。 | | |

| 设置 | 描述 | 值 |
| --- | --- | --- |
| 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。 |

# 任务计划设置

下表介绍了可为所有应用程序任务管理的任务计划设置。

任务计划设置

| 设置 | 描述 | 值 |
| --- | --- | --- |
| RuleType | 任务启动计划。 | 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。<br>如果 StartTime 选项设置为 Once、Monthly、Weekly、Daily、Hourly 或 Minutely 中的一项，则 RuleType 是必需选项。 | [< 年 >/< 月 >/< 每月的某一天 >] [ hh ]:[ mm ]:[ ss ]; [< 每月的某一天 >\|< 星期几 >]; [< 开始周期 >] |
| RandomInterval | 从 0 到指定值（以分钟为单位）的时间间隔，将添加到任务开始时间以避免同时启动任务。 | 默认值：99 分钟。 |
| RunMissedStartRules | 在应用程序启动后运行漏掉的任务。 | Yes（默认值）– 应用程序启动后启用运行漏掉的任务。<br>No：禁用在应用程序启动后运行漏掉的任务。 |
| 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。 | 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）。 | 默认值：120 分钟。 |

# 附录 3.命令行返回代码

Kaspersky Endpoint Security 具有以下命令行返回码：

0 意思是命令/任务成功完成。

1 意思是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 意思是 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，激活 2.0 终止并显示错误。

68 意思是命令无法执行，因为应用程序正被某项策略管理。

69 – 应用程序位于 Amazon Paid Ami 基础设施中。

70 – 尝试启动正在运行的任务、删除正在运行的任务、更改正在运行的任务的设置、停止已停止的任务、暂停已暂停的任务或继续正在运行的任务。

71 – 尚未接受卡巴斯基安全网络声明。

72 意思是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 意思是更新后必须重新启动 Kaspersky Endpoint Security。

75 意思是必须重启设备。

76 – 禁止连接，因为只有具有 root 权限的用户才拥有指定路径的写访问权限。

77 – 指定的授权许可密钥已在设备上使用。

78 表示无法运行命令/任务，因为应用程序正在以 Light Agent 模式使用。

79 表示无法运行该命令，因为应用程序正在标准模式下使用。

80 – 由于网络问题，更新下载操作失败。

128 表示未知错误。

65–所有其他错误。

# 附录 4.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 5.Web Console 中的策略设置

本节介绍Web Console**“应用程序设置”**选项卡中的策略设置。

# 主机威胁防护

## 文件威胁防护

适用于 Windows、 macOS 和 Linux

文件威胁防护组件可防止计算机文件系统受到感染。默认情况下，文件威胁防护组件永久驻留在计算机的 RAM 中，并实时扫描所有打开、保存和启动的文件。该组件扫描所有计算机驱动器（包括连接的驱动器）上的文件。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。

该组件将扫描用户或应用程序访问的文件。如果检测到恶意文件，Kaspersky Endpoint Security 将阻止文件操作。应用程序随后将根据“文件威胁防护”组件的设置来清除或删除恶意文件。

当尝试访问其内容驻留在 OneDrive 云存储中的文件时，Kaspersky Endpoint Security 会下载并扫描文件内容。

`Linux` 对于 Linux 设备，该组件受扫描期间阻止访问文件的模式的影响，您可以在常规应用程序设置中选择该模式。默认在扫描期间阻止对文件的访问。

文件反病毒设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **扫描排除项** | `Windows` `macOS` `Linux` | “*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。<br>当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。 |
| **检测到威胁后的操作** | `Windows` `macOS` `Linux` | “**清除；如果清除失败则删除**”。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>“**清除；如果清除失败则阻止(取决于操作系统)**”。<br>`Windows` `Linux` 如果选择该选项，应用程序将自动尝试对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>“**阻止或提示操作(取决于操作系统)**”。<br>`Windows` `Linux` 如果选择该选项，应用程序将自动阻止受感染的文件，而不尝试对其进行清除或删除。<br>`macOS` Kaspersky Endpoint Security 将显示一个通知窗口，其中包含文件已感染的恶意对象的相关信息，并提示用户选择 Kaspersky Endpoint Security 要执行的操作。可用的操作可能因对象状态不同而有所差异。<br>在清除或删除受感染文件之前，应用程序会创建该文件的备份副本，以便日后需要恢复该文件或可以进行清除。 |
| **保护范围** | `Windows` `macOS` `Linux` | 包含“文件威胁防护”组件扫描的对象。扫描对象可能是硬盘驱动器、可移动驱动器、网络驱动器、文件夹、文件或由掩码定义的多个文件。<br>默认情况下，“文件威胁防护”组件将扫描任何硬盘驱动器、网络驱动器或可移动驱动器中启动的文件。无法更改或删除这些对象的保护范围。您仅可以从扫描中排除对象（例如可移动驱动器）。<br>`Linux` 对于 Linux 设备，您可以使用文件威胁防护组件修改或删除扫描范围。指定至少一个保护范围才能使组件正常工作。 |
| **File types** | `macOS` | “**Scan all files**”。如果启用该设置，Kaspersky Endpoint Security 将毫无例外地扫描所有文件（所有格式和扩展名）。<br>“**Scan applications and documents by content**”。如果启用该设置，则应用程序仅扫描被感染的文件。在扫描文件以查找恶意代码之前，系统将分析文件的内部头以确定文件的格式（例如，.txt、.doc 或 .exe）。该扫描也查找具有特殊文件扩展名的文件。<br>“**Scan applications and documents by extension**”。如果启用该设置，则应用程序仅扫描被感染的文件。此时，系统将根据文件的扩展名确定文件格式。 |
| **扫描优化** | `Windows` `macOS` | 在“**扫描优化**”下，您可以配置 Kaspersky Endpoint Security，以便在扫描文件时获得更高的性能。<br>• `Windows` `macOS` **仅扫描新建和已修改的文件**。仅扫描新文件以及自从上次扫描以来被修改的文件。这有助于缩短扫描的持续时间。此模式适用于简单文件和复合文件。<br>• `Windows` **如果清除失败则停止容器**。应用程序可能没有足够的读写权限来访问检测到的对象。在这种情况下，无法对检测到的对象进行清除或删除。如果选中此复选框，应用程序将阻止检测到的对象并停止容器。如果取消选中此复选框，应用程序仅阻止检测到的对象。<br>• `macOS` **跳过扫描只读系统卷**。如果选中此复选框，应用程序将不会扫描只读系统卷。这将显著缩短扫描时间。<br>• `Windows` **不扫描在 Windows 容器中执行的文件操作**。如果选中此复选框，应用程序仅在容器启动时扫描容器。如果取消选中此复选框，应用程序将实时持续扫描容器。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **扫描复合文件** | `Windows` `macOS` `Linux` | 隐藏病毒和其他恶意软件的一种常用方法就是将其植入复合文件中，例如存档或数据库中。为了检测以这种方式隐藏的病毒和其他威胁，必须解包复合文件，这可能会降低扫描速度。您可以限制要扫描的复合文件类型，从而加快扫描速度。<br>• **压缩文件**。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>• **分发包和自解压存档**。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。要扫描自解压存档，您需要选择"**扫描压缩包**"复选框。<br>• `Windows` `macOS` **Office 格式文件和嵌入式 OLE 对象**。扫描 Microsoft Office 文件（例如 DOC、DOCX、XLS、PPT）和嵌入文件中的 OLE 对象（例如 Excel 表格、宏、电子邮件附件）。<br>• `Windows` `Linux` **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。<br>• `Linux` **扫描电子邮件格式文件**。扫描纯文本格式的电子邮件文件。 |
| **允许在后台解压大于此值的存档文件 (MB)** | `Windows` `macOS` | 如果选中该复选框，应用程序会提供对大于指定值的复合文件的访问权限，然后再扫描这些文件。在这种情况下，Kaspersky Endpoint Security 在后台解压并扫描复合文件。<br>对于小于该值的复合文件，只有在解压和扫描这些文件后，应用程序才会提供对这些文件的访问权限。<br>如果未选中该复选框，则只有在解压和扫描任何大小的复合文件后，应用程序才会提供对这些文件的访问权限。 |
| **不扫描大小大于该值(MB)的压缩包** | `Windows` `macOS` `Linux` | 如果选中该复选框，应用程序不会扫描其大小超过指定值的复合文件。<br>如果清除该复选框，应用程序将扫描所有大小的复合文件。<br>应用程序扫描从存档中提取的大文件，无论是否选择该复选框。 |
| **跳过扫描时间超过以下值的文件 (秒)** | `Linux` | 如果选中该复选框，应用程序将在指定时间过后停止扫描复合文件。<br>如果该值设置为 `0`，则扫描时间不受限制。 |
| **后台扫描** | `Windows` | "*后台扫描*"是 Kaspersky Endpoint Security 的一种扫描模式，不会向用户显示通知。后台扫描比其他类型的扫描（如全盘扫描）需要更少的计算机资源。在此模式下，Kaspersky Endpoint Security 扫描启动对象、引导扇区、内核内存和系统分区。 |
| **从上下文菜单扫描** | `Windows` | Kaspersky Endpoint Security 允许您从上下文菜单运行单个文件扫描来查找病毒和其他恶意软件。<br>从上下文菜单执行扫描时，Kaspersky Endpoint Security 不扫描其内容位于 OneDrive 云存储中的文件。 |

# BadUSB 攻击防护

适用于 Windows 和 Linux

某些病毒会修改 USB 设备的固件以欺骗操作系统，将 USB 伪装为键盘。结果，病毒可能在您的用户账户下执行命令以下载恶意软件。

BadUSB 攻击防护组件可以防止受感染的模拟键盘 USB 设备连接至计算机。

当 USB 设备连接至计算机并被操作系统识别为键盘时，应用程序将提示用户从该键盘输入其生成的数字代码或使用屏幕键盘（如果可用）（参见下图）。这个步骤称为键盘授权。

如果代码输入正确，应用程序会将识别参数（键盘的 VID/PID 及其连接的端口号）保存在已授权键盘列表中。重启操作系统后重新连接键盘时无需重复键盘授权。

经授权的键盘连接至该计算机不同的 USB 端口时，应用程序将提示为该键盘再次授权。

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尝试次数。如果数字代码多次输入错误或键盘授权窗口关闭（参见下图），应用程序将阻止从该键盘输入。当达到 USB 设备阻止时间或者操作系统重启后，程序将再次提示用户重新执行键盘授权。

程序将允许使用经过授权的键盘并阻止未经授权的键盘。

默认情况下，未安装“BadUSB 攻击防护”组件。如果需要“BadUSB 攻击防护”组件，可以在安装应用程序前在安装包的属性中添加该组件，或者在安装应用程序后更改可用应用程序组件。




*键盘授权*

BadUSB 攻击防护设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **USB 设备授权尝试的最大次数** | `Windows` `Linux` | 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)** | `Windows` `Linux` | 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） |
| **禁止使用屏幕键盘授权 USB 设备** | `Windows` `Linux` | 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** | `Windows` `Linux` | 如果此切换开关被启用，Kaspersky Endpoint Security 不会在条形码扫描器身份验证的通知中显示条形码。 |

# 可移动驱动器扫描

适用于 Windows、macOS 和 Linux

Kaspersky Endpoint Security 扫描您运行或复制的所有文件，即使该文件位于可移动驱动器（文件威胁保护组件）上。为了防止病毒和其他恶意软件的传播，您可以配置可移动驱动器连接到计算机时的自动扫描。Kaspersky Endpoint Security 将自动尝试对已经检测到的所有受感染的文件执行清除操作。如果清除失败，Kaspersky Endpoint Security 将删除文件。该组件通过运行实现了机器学习、启发式分析（高级别）和特征码分析的扫描来保证计算机的安全。Kaspersky Endpoint Security 还使用 iSwift 和 iChecker 扫描优化技术。该技术总是启用且无法被禁用。

“可移动驱动器扫描”设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **扫描类型** | `Windows` `Linux` | “**快速扫描**”。如果选择此选项，Kaspersky Endpoint Security 将在连接可移动驱动器后只扫描最容易被感染的特定格式的文件，并且不会解压缩复合对象。<br>“**详细扫描**”。如果选择此选项，Kaspersky Endpoint Security 将在连接可移动驱动器时扫描所有文件，包括嵌套在复合对象、存档、分发包和 Office 格式文件中的文件。Kaspersky Endpoint Security 不扫描邮件格式的文件或受密码保护的存档文件。 |
| **阻止用户停止扫描** | `Windows` | 如果选中了该复选框，则对于 Kaspersky Endpoint Security 本地界面中的可移动驱动器扫描任务，“**任务**”区域的“**停止**”按钮和“可移动驱动器扫描”窗口中的“**停止**”按钮不可用。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **扫描期间阻止对可移动驱动器的访问** | `Linux` | 如果选中该复选框，Kaspersky Endpoint Security 将在执行扫描时阻止对已连接驱动器上的文件的访问。 |
| **隐藏扫描进度条** | `Windows` | 如果选中此复选框，Kaspersky Endpoint Security 将隐藏可移动驱动器扫描进度条。应用程序在后台执行扫描。<br>如果清空该复选框，Kaspersky Endpoint Security 将在单独的窗口和"**任务**"区域中显示可移动驱动器扫描进度。 |
| **不扫描大于此值的可移动驱动器** | `Windows` | 如果选中该复选框，Kaspersky Endpoint Security 对于大小不超过指定最大驱动器大小的可移动驱动器，执行所选操作。如果可移动驱动器的大小超出配置的值，Kaspersky Endpoint Security 将跳过扫描。<br>如果清除该复选框，Kaspersky Endpoint Security 将对任意大小的可移动驱动器执行选定的操作。 |

# 行为检测

适用于 Windows、macOS 和 Linux

"行为检测"组件接收您计算机上的应用程序操作的信息，并将此信息提供给其他保护组件以提高性能。"行为检测"组件将行为流签名 (BSS) 用于应用程序。如果应用程序操作匹配行为流签名，Kaspersky Endpoint Security 将执行选定的响应操作。Kaspersky Endpoint Security 功能基于行为流签名，并为计算机提供主动防御。

行为检测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。

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。

行为检测设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **受信任应用程序** | `Windows` `macOS` `Linux` | *受信任应用程序列表*是一个应用程序列表，其中所包含应用程序的文件和网络活动（包含恶意活动）以及对系统注册表的访问不受 Kaspersky Endpoint Security 的监控。默认情况下，Kaspersky Endpoint Security 将监控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及其产生的网络流量。将应用程序添加到受信任应用程序列表后，Kaspersky Endpoint Security 将停止监控该应用程序的活动。<br>当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。 |
| **扫描排除项** | `Windows` `macOS` `Linux` | "*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。<br>当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。 |
| **检测到威胁后的操作** | `Windows` `macOS` `Linux` | "**删除文件或块(取决于 OS)**"。<br>`Windows` `macOS` 如果选择此选项，当检测到恶意活动时，Kaspersky Endpoint Security 会删除恶意应用程序的可执行文件并在备份中创建该文件的备份副本。<br>`Linux` 如果检测到恶意活动，Kaspersky Endpoint Security 会阻止执行恶意活动的应用程序，并记录有关检测到的恶意活动的信息。<br>**通知**。`WindowsLinux` 如果选择此选项，当检测到应用程序的恶意活动时，Kaspersky Endpoint Security 不会终止该应用程序，但会将该应用程序的恶意活动的相关信息添加至活动威胁列表。<br>`macOS` 如果检测到恶意的活动，Kaspersky Endpoint Security 会提示用户选择检测到恶意活动时要执行的操作。可用的操作可能因对象状态不同而有所差异。<br>"**阻止**"。如果选择此选项，在检测到恶意活动时，Kaspersky Endpoint Security 会终止该应用程序。 |

# 反加密

适用于 Windows、 macOS 和 Linux

`Windows` 对于 Windows 设备，该组件仅监视 NTFS 文件系统级别且未被 EFS 系统加密的文件的操作。

`Linux` 对于 Linux 设备，该组件分析通过 SMB/NFS 进行网络访问的本地目录中的文件。

`macOS` 对于 macOS 设备，该组件会监控 SMB 共享。

反加密组件通过分析网络共享中的活动来防止远程加密。如果该活动与外部加密的典型行为流签名匹配，Kaspersky Endpoint Security 将执行选定操作。

`Linux` 在 Linux 设备上启用该组件之前，请务必阅读并理解关于反加密的信息。

反加密设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **扫描排除项** | `Windows` `Linux` | "*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。<br>当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。 |
| **按名称或 IP 地址的排除项** | `Windows` | "**受信任的计算机名称/IP 地址**"。尝试加密共享文件夹的计算机的列表不会受到监控。<br>"**按掩码的排除项**"。保护范围排除项。如果您的组织在使用共享文件夹交换文件时使用数据加密，则从保护范围排除文件夹可以减少误报量。使用**掩码**。<br>• `*`（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文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。<br>• 两个连续 `*` 字符在文件或文件夹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文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。<br>• `?`（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文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。 |
| **检测到威胁后的操作** | `Windows` `macOS` `Linux` | "**通知**"。如果选择此选项，在检测到修改共享文件夹中的文件的尝试时，Kaspersky Endpoint Security 会将有关此尝试的信息添加到活动威胁列表中，并将条目添加到报告中。<br>"**阻止连接(分钟)**"。<br>`Windows` 如果选择此选项，当 Kaspersky Endpoint Security 检测到有人试图修改共享文件夹中的文件时，它将阻止启动恶意活动的会话对文件进行修改的权限，并创建已修改文件的备份副本。<br>`macOS` `Linux` 当 Kaspersky Endpoint Security 检测到有人试图修改共享文件夹中的文件时，它会阻止来自从事恶意的活动的设备的网络流量。应用程序将创建一个*检测到加密*事件，其中包含有关受感染设备的信息。 |
| **保护范围** | `Windows` `macOS` `Linux` | *保护范围*是 Kaspersky Endpoint Security 监控文件活动的共享文件夹路径列表。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。默认情况下，应用程序会自动识别共享文件夹并监控所有文件夹中的文件活动。<br>`macOS` Kaspersky Endpoint Security 会保护 macOS 设备上的所有共享文件夹。保护范围无法更改。<br>`Windows` `Linux` 您可以选择保护范围：<br>"**受保护设备上的所有共享网络文件夹**"。应用程序将监控所有共享文件夹中的文件活动。<br>"**仅指定的共享文件夹**"。应用程序只会监控指定共享文件夹中的加密尝试。 |

## 漏洞利用防御

适用于 Windows、macOS 和 Linux

"漏洞利用防御"组件可检测利用计算机漏洞来利用管理员权限或执行恶意活动的程序代码。例如，漏洞利用程序可以利用缓冲区溢出攻击。为此，漏洞利用程序会向易受攻击的应用程序发送大量数据。处理此数据时，易受攻击的应用程序会执行恶意代码。此攻击的结果是，漏洞利用程序可启动未经授权的恶意软件安装。当存在从易于感染的应用程序运行可执行文件的尝试，并且该尝试并非由用户执行时，Kaspersky Endpoint Security 将阻止该文件运行或通知用户。

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。

为了使漏洞利用防御组件正常工作，必须启用行为检测组件。为了使漏洞利用防御组件达到最佳性能，建议同时启用 Web 威胁防护组件。

`Linux` 对于 Linux 设备，用于系统事件拦截的可更新内核模块也必须被启用。

漏洞利用防御设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **检测到威胁后的操作** | `Windows` `macOS` `Linux` | "**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。<br>"**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。 |
| **系统进程内存保护** | `Windows` | 如果打开此切换按钮，Kaspersky Endpoint Security 将阻止尝试访问系统进程内存的外部进程。 |

# 通信和 Web 保护

## 邮件威胁防护

适用于 Windows、macOS 和 Linux

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。

邮件威胁防护可以扫描收件和发件。该应用程序支持 POP3、SMTP、IMAP、NNTP 协议。

`Linux` Linux 设备应用程序不支持 NNTP 协议。

**支持的邮件客户端**

- `Windows`、`macOS` Microsoft Office Outlook
- `Windows`、`macOS` Mozilla Thunderbird

- `Windows` Windows Mail
- `Windows`、`Linux` MyOffice Mail
- `Windows`、`Linux` R7-Office Organizer
- `macOS` Apple Mail
- `macOS` Canary Mail
- `macOS` Spark
- `macOS` Mimestream
- `macOS` Airmail
- `macOS` Post Box
- `macOS` Boxy Suite 2
- `macOS` Twobird
- `macOS` Shift
- `macOS` Clean Email
- `macOS` eM Client
- `macOS` Superhuman
- `macOS` Polymail
- `macOS` HEY
- `macOS` Mail+ for Gmail
- `macOS` Spike mail

`Windows` 邮件威胁防护可能并不总是能够获得邮件的协议级访问权限（例如，使用 Microsoft Exchange 解决方案时）。为此，邮件反病毒包括适用于 Microsoft Office Outlook 的 Kaspersky ASAP Outlook 插件扩展程序。该扩展程序允许在邮件客户端级别扫描邮件。Kaspersky ASAP Outlook 插件支持 Outlook 2010、2013、2016、2019 和 2021 的操作。

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。

当在附件中检测到恶意文件时，Kaspersky Endpoint Security 会将有关已执行操作的信息添加到邮件主题，例如，*[邮件已被处理] <邮件主题>*。

| 设置 | OS | 描述 |
| --- | --- | --- |
| **扫描排除项** | `Windows` `macOS` `Linux` | "*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。<br>当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。 |
| **检测到威胁后的操作** | `Windows` `macOS` `Linux` | "**清除；如果清除失败则删除**"。在入站或出站邮件中检测到受感染的对象时，应用程序会尝试对检测到的对象进行清除。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>*。<br>`Windows` `Linux` **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。在出站邮件中检测到受感染的对象时，应用程序会尝试对检测到的对象进行清除。如果无法清除对象，应用程序会阻止邮件的传输，邮件客户端会显示错误。<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。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>`Linux` 对于 Linux 设备，邮件威胁防护组件不会尝试清除传出邮件中的受感染对象，而是立即阻止邮件的传输。 |
| **扫描 POP3、SMTP、NNTP 和 IMAP 流量** | `Windows` | "邮件威胁防护"组件对通过 POP3、SMTP、NNTP 和 IMAP 协议传送的流量进行扫描。 |
| **连接 Microsoft Outlook 扩展程序** | `Windows` | 如果选中该复选框，则在 Microsoft Outlook 中集成的扩展程序一侧启用对通过 POP3、SMTP、NNTP、IMAP 协议传输的电子邮件的扫描。该应用程序可以扫描 Microsoft Outlook 中不同阶段的收发邮件：<br>• "**接收时扫描**"。如果选中此复选框，则应用程序在通过 Microsoft Outlook 接收邮件时会使用邮件威胁防护。<br>• "**读取时扫描**"。<br>• "**发送时扫描**"。<br>如果使用 Microsoft Outlook 的扩展程序扫描邮件，建议使用Cached Exchange Mode。有关缓存 Exchange 模式的详细信息和对其用途的建议，请参阅 Microsoft 知识库。 |
| **扫描附加存档** | `Windows` `Linux` | 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** | `Windows` `Linux` | 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** | `Windows` `macOS` `Linux` | 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)** | `Windows` `macOS` `Linux` | 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。 |
| **附件过滤器** | `Windows` `Linux` | 附件过滤器决定邮件威胁防护对电子邮件附件执行的操作。<br>附件过滤器不适用于传出电子邮件。<br>• "**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。<br>• "**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。<br>• "**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。<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。 |

# Web 威胁防护

适用于 Windows、macOS 和 Linux

"Web 威胁防护"组件可防止从 Internet 下载恶意文件，同时阻止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 威胁防护组件会扫描入站 HTTP、HTTPS 和 FTP 流量、网站和 IP 地址。

`Linux` Web 威胁防护默认处于禁用状态。启用 Web 反病毒可能会降低已安装的第三方应用程序和操作系统的性能。有关配置应用程序以在 Linux 设备上启用 Web 反病毒的详细信息，请参阅技术支持知识库。

Web 反病毒设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **受信任网址** | `Windows` `macOS` `Linux` | Web 威胁防护认为可信的网址列表。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。在一些情况下可以使用受信任地址列表，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。<br><br>您可以将网页/网站的特定地址和地址掩码添加至受信任网址列表。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |
| **扫描排除项** | `Windows` | "*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。<br><br>输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |
| **检测到威胁后的操作** | `Windows` `macOS` `Linux` | "**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。<br><br>"**允许、通知或提示操作(取决于操作系统)**"。<br><br>`Windows` 如果选择此选项并且在 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。<br><br>`macOS` Kaspersky Endpoint Security 会显示一个通知，其中包含有关已感染 Web 流量对象的恶意软件类型的信息，并提示用户选择 Kaspersky Endpoint Security 对此对象执行的操作。可用的操作可能因对象状态不同而有所差异。<br><br>`Linux` 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。 |

# 网络威胁防护

适用于 Windows、macOS 和 Linux

*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。

`Linux` 网络威胁防护默认处于禁用状态。启用网络威胁防护可能会降低已安装的第三方应用程序和操作系统的性能。有关配置应用程序以在 Linux 设备上启用网络威胁防护的详细信息，请参阅技术支持知识库。

网络威胁防护设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **受信任 IP 地址** | `Windows` `Linux` | 受信任设备的 IP 地址列表。网络威胁防护组件不会阻止来自这些地址的网络活动。<br><br>`Windows` 您可以添加指定端口或端口范围和协议的 IP 地址。<br><br>`Linux` 您只能将 IP 地址添加到排除列表中。<br><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。 |
| **检测到威胁后的操作** | `Windows` `macOS` `Linux` | "**阻止**"。当检测到威胁时，网络威胁防护会阻止该攻击。<br><br>"**阻止攻击和攻击设备(分钟)**"。如果启用此选项，"网络威胁防护"组件将把攻击计算机添加至阻止列表。这意味着，"网络威胁防护"组件将会在攻击计算机的首次网络攻击尝试后的指定时间段内，阻止与该计算机的网络连接。此阻止动作将会自动保护计算机免受以后来自同一地址的更多攻击。攻击计算机必须保持在阻止列表中的最短时间为一分钟。最长时间为 999 分钟。<br><br>当应用程序重启和网络威胁防护设置被更改时，Kaspersky Endpoint Security 清空阻止列表。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **将端口扫描和网络 Flooding 视为攻击** | `Windows` | *端口扫描*攻击包括扫描计算机上的 UDP 端口、TCP 端口和网络服务。该攻击允许攻击者识别计算机的漏洞程度，然后再发起更危险的网络攻击。端口扫描也允许攻击者识别计算机上的操作系统并选择针对性的网络攻击。<br>*网络 Flooding* 是对网络资源或组织（例如 Web 服务器）的攻击。该攻击包括发送大量的请求以让网络资源过载。当发生此类事情时，用户无法访问组织的网络资源。<br>若选中此复选框，则 Kaspersky Endpoint Security 将监控网络流量以检测这些攻击。如果检测到攻击，应用程序会通知用户并将相应事件发送到 Kaspersky Security Center。该应用程序提供有关攻击计算机的信息，这是及时威胁响应操作所必需的。<br>如果一些您允许的应用程序执行了类似某些类型攻击的操作，您可以禁用对这些类型攻击的检测。这将帮助避免误报。 |
| **MAC 欺骗防护** | `Windows` | *MAC 欺骗攻击*包括更改网络设备（网卡）的 MAC 地址。结果，攻击者可以将发送到某台设备的数据重定向到另一台设备，并获得对该数据的访问权限。Kaspersky Endpoint Security 允许您阻止 MAC 欺骗攻击并接收关于攻击的通知。 |

# 防火墙

适用于 Windows、macOS 和 Linux

在互联网或局域网上工作时，防火墙组件会阻止未经授权的计算机连接。防火墙还控制计算机上应用程序的网络活动。这允许您保护公司局域网免受身份盗窃和其他攻击。该组件借助反病毒数据库、卡巴斯基安全网络云服务和预定义*网络规则*来提供计算机保护。

`Linux` 对于 Linux 设备，应用程序使用防火墙管理组件。该组件管理操作系统防火墙的设置和规则。

防火墙设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **网络数据包规则** | `Windows` `macOS` `Linux` | 包含网络数据包规则清单的表。网络数据包规则将对网络数据包进行限制，与应用程序无关。此类规则将限制通过特定端口的选定数据协议发送和接收的网络流量。<br>该表格列出了由卡巴斯基推荐的预配置网络数据包规则，它们能最好地为 Microsoft Windows 和 Linux 操作系统的计算机提供网络流量保护。<br>防火墙将为每条网络数据包规则设置执行优先级。防火墙将按照包规则列表上的顺序从上到下处理网络数据包规则。防火墙将找到最适合网络连接的网络数据包规则，并应用该规则来允许或阻止网络活动。然后，防火墙会对特定网络连接忽略所有后续网络数据包规则。<br>网络数据包规则的优先级比应用程序网络规则高。 |
| **可用网络** | `Windows` `macOS` `Linux` | 该表格包含防火墙在计算机上检测到的网络连接的信息。<br>默认情况下已将“**公用网络**”类型分配给互联网。您无法更改互联网的类型。<br>有以下网络连接类型可用：<br>• “**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。防火墙根据为每一个应用程序设置的网络规则，过滤应用程序的网络活动。<br>• “**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）。<br>• “**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。 |
| **始终为网络代理端口添加允许规则** | `macOS` `Linux` | 此复选框启用或禁用网络代理端口的自动添加允许规则。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **应用程序权限和受保护资源** | `Windows` | “**应用程序**”。“防火墙”组件控制的应用程序表。应用程序分配到信任组中。信任组定义 Kaspersky Endpoint Security 控制应用程序的网络活动时使用的权限。<br>您可以从受策略影响的计算机上安装的所有应用程序的单一列表中选择应用程序，并将该应用程序添加到信任组。<br>“**网络规则**”。属于信任组的应用程序的网络规则表。防火墙按照这些规则管理应用程序的网络活动。<br>该表显示了 Kaspersky 专家推荐的预定义网络规则。这些网络规则已添加，以最佳方式保护运行 Windows 操作系统的计算机的网络流量。无法删除预定义网络规则。 |

# 安全控制

## 设备控制

适用于 Windows、macOS 和 Linux

“设备控制”管理用户对安装在计算机上或连接到计算机的设备（例如，硬盘驱动器、相机或 Wi-Fi 模块）的访问。这样可以在连接此类设备时保护计算机免受感染，并防止数据丢失或数据泄漏。

设备控制允许或阻止对以下级别的设备的访问：

- **设备类型**。例如，打印机、可移动驱动器和 CD/DVD 驱动器。
- **连接总线**。“*连接总线*”是用于将设备连接到设备的接口（例如 USB 或 FireWire）。如果为设备类型选择了“**取决于总线**”模式，应用程序根据设备连接的总线（例如 USB）的模式控制对设备的访问。
- **受信任设备**。*受信任设备*是指指定用户或用户组始终拥有完全访问权限的设备。

  您可以根据以下数据添加受信任设备：

  - `Windows` `macOS` **型号**。每个设备都有一个供应商 ID (VID) 和一个产品 ID (PID)。您可以使用操作系统工具在设备属性中查看 ID。用于输入 VID 和 PID 的模板：`VID_1234&PID_5678`。如果在组织中使用特定型号的设备，则按型号添加设备很方便。这样，您可以添加该型号的所有设备。
  - “**ID**”。每个设备都有一个唯一的标识符（硬件 ID 或 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。
  - `Windows` `macOS` **设备型号掩码**。如果您使用具有相似 VID 或 PID 的多个设备（例如，来自同一制造商的设备），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，`VID_05AC&PID_*`。
  - **设备 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*`。

`Linux` 对于 Linux 设备，组件执行的操作取决于在“常规设置”部分的“检测设置”子部分中选择的文件操作拦截模式。

| 设置 | OS | 描述 |
| --- | --- | --- |
| **受信任设备** | `Windows` `macOS` `Linux` | 被授权访问这些设备的受信任设备和用户的列表。<br>输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 |
| **消息模板** | `Windows` `Linux` | "**发送给用户的邮件**"。当用户尝试访问阻止的设备时所显示的消息的模板。当用户尝试对被阻止使用的设备内容执行操作时，也会显示此消息。<br>"**给管理员的消息**"。当用户确信设备的访问权限或设备内容操作被错误地禁止时，发送给 LAN 管理员的消息的模板。 |
| **允许临时访问请求** | `Windows` `Linux` | 如果选中此选框，"**请求访问**"按钮将在 Kaspersky Endpoint Security 的本地界面中可用。使用此按钮，用户可以请求临时访问被阻止的设备。 |
| **操作模式** | `Linux` | 当尝试对根据设备控制设置被阻止访问的设备进行访问时，Kaspersky Endpoint Security 执行所选的操作。<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**"。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。 |
| **设备和 Wi-Fi 网络** | `Windows` `macOS` `Linux` | 符合"设备控制"组件分类的所有可用设备类型的列表，包括其各自的访问状态。 |
| **连接总线** | `Windows` `Linux` | 符合"设备控制"组件分类的所有可用连接总线的列表，包括这些连接总线各自的访问状态。如果选择了"**取决于连接总线**"模式，Kaspersky Endpoint Security 根据连接总线的类型允许或拒绝访问设备。 |
| **反桥接** | `Windows` | 反桥接通过阻止为一台计算机同时建立多个网络连接来禁止创建网桥。这样可以保护公司网络避免未受保护和未经授权的网络上的攻击。<br>反桥接根据设备的优先级阻止建立多个连接。设备在列表中的位置越高，优先级越高。<br>如果活动连接和新连接属于同一类型（例如 Wi-Fi），则 Kaspersky Endpoint Security 会阻止活动连接并允许建立新连接。<br>如果活动连接和新连接属于不同类型（例如，网络适配器和 Wi-Fi），则 Kaspersky Endpoint Security 会阻止具有较低优先级的连接，允许具有较高优先级的连接。<br>反桥接支持以下类型的设备的操作：网络适配器、Wi-Fi 和调制解调器。 |

# Web 控制

适用于 Windows、macOS 和 Linux

"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。

## 网站访问规则

"Web 控制"通过使用*访问规则*管理用户对网站的访问。您可以配置对以下扫描区域的网站访问权限：

- **网站类别**。网站按照卡巴斯基安全网络云服务、启发式分析和已知网站数据库（包含在应用程序数据库中）进行分类。您可以限制用户对某些类别的访问，例如：*社交网络*类别或其他类别。
- `Windows` **数据类型**。例如，您可以限制用户访问网站上的数据，并隐藏图像。Kaspersky Endpoint Security 根据文件格式确定数据类型，而不是基于其扩展名。

  Kaspersky Endpoint Security 不扫描压缩文件内的文件。例如，如果图像文件放在压缩文件中，Kaspersky Endpoint Security 会识别"*存档*"数据类型而不是"*图形文件*"。

- **单个地址**。您可以输入网址或使用掩码。

可以同时使用多种方法来管理对网站的访问。例如，您可以仅针对“*基于 Web 的邮件*”网站类别限制对“*Office 文件*”数据类型的访问。

Web Control 还允许您配置以下网站访问规则的高级设置：

- **要应用应用程序控制规则的用户或组。**
  例如，您可以限制公司内除 IT 部门以外的所有用户通过浏览器访问 Internet。
- **设备访问计划。**
  例如，您可以限制只能在工作时间通过浏览器访问 Internet。

Web 控制设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **消息模板** | `Windows` `Linux` | “**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。<br>“**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。<br>“**给管理员的消息**”。发送给公司本地网络管理员的消息模板。如果用户认为对 Web 资源的访问被错误地阻止，则使用。<br>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。 |
| **规则列表** | `Windows` `macOS` `Linux` | 包含 Web 资源访问规则的列表。每条规则都有优先级。规则在列表中的位置越靠前，其优先级就越高。如果某个网站已添加到多条规则，“Web 控制”会基于优先级最高的规则来管理对该网站的访问。 |
| **默认操作** | `Windows` `macOS` `Linux` | 对不被任何其他规则覆盖的 Web 资源的访问规则。下列选项可用：<br>• “**允许除规则列表外的所有内容**”。<br>• “**阻止除规则列表外的所有内容**”。 |
| **应用规则后终止活动用户浏览器会话** | `Windows` | 如果选中该复选框，Web 控制将在应用策略之后立即终止与被阻止的 Web 资源的连接。浏览器立即停止从网页下载数据。当您刷新网页或转到另一个禁止的网页时，应用程序会显示警告。<br>Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。<br>如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。 |
| **Web 会话监控** | `Windows` | Kaspersky Endpoint Security 会记录对所有网站（包括允许的网站）的访问数据。Kaspersky Endpoint Security 会将事件发送到 Kaspersky Security Center、Windows 事件日志和一份报告。要监控用户 Internet 活动，您需要配置用于保存事件的设置。<br>支持监控功能的浏览器：Microsoft Edge、Microsoft Internet Explorer、Google Chrome、Yandex Browser、Mozilla Firefox。用户活动监控在其他浏览器中不起作用。<br>在解密 HTTPS 流量时，监控用户 Internet 活动可能需要更多计算机资源。 |

# 应用程序控制

适用于 Windows 和 Linux

“应用程序控制”管理用户计算机上的应用程序启动。这允许您在使用应用程序时实施公司安全策略。“应用程序控制”还通过限制对应用程序的访问来降低计算机感染的风险。

应用程序控制组件使用规则管理受保护设备上应用程序的启动。规则包含条件以及应用程序控制组件在规则触发时执行的操作。例如，应用程序所属的类别。*应用程序类别*是一组具有共同特征的应用程序。例如，包含已安装应用程序的可执行文件的类别，或包含组织中使用的标准应用程序集的类别。每个类别只能在一条规则中使用。

管理员可以创建许多规则。一个应用程序可能符合多个规则的条件。阻止规则的优先级高于允许规则的优先级。Kaspersky Endpoint Security 每次启动时都会检查应用程序是否符合规则。Kaspersky Endpoint Security 按顺序将应用程序与所有应用程序控制规则进行匹配。

应用程序控制设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **消息模板** | Windows | **给用户的消息**。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。<br>**致管理员消息**。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。 |
| **操作模式** | Windows<br>Linux | 您可以选择以下选项之一：<br>• "**允许除规则列表外的所有内容**"。如果选择该选项，应用程序控制允许所有用户启动任何应用程序，但应用程序控制阻止规则禁止的应用程序除外。<br>• "**阻止除规则列表外的所有内容**"。如果选择该选项，应用程序控制阻止所有用户启动任何应用程序，但应用程序控制允许规则允许的应用程序除外。 |
| **启动应用程序时的操作** | Windows<br>Linux | • "**应用规则**"。Kaspersky Endpoint Security 根据所选模式管理应用程序的启动。<br>• "**通知**"。Kaspersky Endpoint Security 会通知您尝试运行应用程序的情况。 |
| **将策略规则添加到本地规则** | Linux | 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。 |
| **使用严格的数字签名验证** | Windows | 您可以选择证书作为应用程序控制规则的触发条件。<br>如果选中此复选框，Kaspersky Endpoint Security 将规则应用于仅使用以下证书签名的应用程序：受信任的系统证书存储。使用此类证书签名的应用程序也被视为受到保护组件（例如"*恶意软件扫描*"任务）的信任。但是，如果您在应用程序控制规则中指定来自不同存储的证书，Kaspersky Endpoint Security 将不会应用此类规则。<br>如果清除该复选框， Kaspersky Endpoint Security 会将规则应用于由 Windows 受信任根证书存储区的证书签名的应用程序。此类应用程序不属于受信任区域的一部分。保护组件监控此类应用程序的活动。 |
| **监控 DLL 模块的加载** | Windows | 如果选定该复选框，Kaspersky Endpoint Security 将在用户启动应用程序时控制 DLL 模块的加载。有关 DLL 模块和加载该 DLL 模块的应用程序的信息将记录在该报告中。<br>当启用对加载 DLL 模块和驱动程序的控制时，请确保在"应用程序控制"设置中已启用以下规则之一：默认"**黄金镜像**"规则或其他包含"**黄金镜像\受信任证书**"KL 类别的规则，并确保在启动 Kaspersky Endpoint Security 之前加载受信任的 DLL 模块和驱动程序。如果在禁用"**黄金镜像**"规则时启用对加载 DLL 模块和驱动程序的控制，可能导致操作系统不稳定。<br>Kaspersky Endpoint Security 仅监控自选中该复选框后加载的 DLL 模块和驱动程序。选择复选框后，建议重启计算机以确保应用程序监控所有 DLL 模块和驱动程序，包括那些在 Kaspersky Endpoint Security 启动之前加载的。 |
| **规则** | Windows<br>Linux | Kaspersky Endpoint Security 使用的应用程序控制规则，用于控制受保护设备上的应用程序启动。<br>对于每种应用程序控制模式，您最多可以添加 5 项规则。 |
| **受信任更新程序** | Windows | 如果选中此复选框，Kaspersky Endpoint Security 会将规则中包含的应用程序视为受信任更新程序。Kaspersky Endpoint Security 允许创建和运行此类应用程序的新可执行文件。 |

# 系统完整性监控

适用于 Windows 和 Linux

如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件不可用。

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。系统完整性监控可以实时运行，也可以根据需要执行系统完整性检查。

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。

`Linux` 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。

系统完整性监控设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **实时系统完整性监控** | `Windows` | 在实时模式下，系统完整性监控跟踪组件范围（*监控范围*）中包含的对象中的更改。系统完整性监控还允许实时阻止对此类对象的未经授权的访问。 |
| **检测到系统更改时的操作** | `Windows` | "**应用规则**"。在此模式下，系统完整性监控会阻止对监控范围内的文件和注册表项的操作，并生成相应的事件。<br>"**测试规则(通知)**"。在此模式下，系统完整性监控会允许对监控范围内的文件和注册表项的操作，并生成相应的事件。 |
| **监控文件和注册表** | `Windows` | 系统完整性监控监控文件、文件夹和注册表的更改。 |
| **监控设备** | `Windows` | 系统完整性监控监控外部设备的连接和断开连接。 |
| **系统完整性检查** | `Windows` | 按需系统完整性检查是一项您可以手动或按计划运行的任务。要运行"*系统完整性检查*"任务，您必须配置组件的范围（*监控范围*）并创建基线。*基线*是系统中对象的记录状态，应用程序在与当前状态进行比较时以其作为参考。 |
| **监控范围** | `Linux` | 该表包含系统完整性监控组件的监控范围。应用程序会监控位于表中指定路径的文件和目录。默认情况下，该表包含**卡巴斯基内部对象**监控范围。 |
| **排除范围** | `Linux` | 此表包含扫描排除范围。应用程序不会扫描位于表中指定路径的文件和目录。默认情况下，该表为空。 |
| **按掩码的排除项** | `Linux` | 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。 |

# 信任区域

适用于 Windows、macOS 和 Linux

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。

Kaspersky Endpoint Security 支持使用掩码指定文件或文件夹名称。您可以在掩码中使用以下通配符：

- `*`（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文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。
- `?`（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文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

受信任区域设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **网址** | `Windows` `macOS` `Linux` | Web 威胁防护认为可信的网址列表。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。在一些情况下可以使用受信任地址列表，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。<br><br>您可以将网页/网站的特定地址和地址掩码添加至受信任网址列表。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **IP 地址** | `Windows` `Linux` | 受信任设备的 IP 地址列表。网络威胁防护组件不会阻止来自这些地址的网络活动。<br>`Windows` 您可以添加指定端口或端口范围和协议的 IP 地址。<br>`Linux` 您只能将 IP 地址添加到排除列表中。<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。 |
| **网络端口** | `Windows` `macOS` `Linux` | Web 控制、文件威胁防护、 Web 威胁防护、邮件威胁防护、漏洞利用防御和行为检测组件监控数据流的已知和已注册端口列表。如果启用此切换开关，则该端口被视为受信任端口，并且不会监控用户设备上通过此类端口传输的数据。 |
| **受信任证书** | `Windows` `macOS` `Linux` | Kaspersky Endpoint Security 认为受信任的根证书列表。扫描加密连接时，将使用受信任的根证书列表。 |
| **受信任的计算机名称/IP 地址** | `Windows` | 行为检测组件认为可信的主机名和 IP 地址列表。Kaspersky Endpoint Security 不会扫描指定设备上的病毒和其他威胁性应用程序。 |
| **域** | `Windows` `Linux` | 受信任域列表。Web 威胁防护、Web 控制和云发现组件（仅适用于 Windows 设备）不会监控与这些域的加密连接。<br>如果通过 SSL/TLS 访问并且启用了"阻止 SSL/TLS 连接"选项，则将阻止 Windows 设备上与此列表中的域的连接。 |
| **受信任的挂载点** | `Linux` | 受信任挂载点列表。这些内容会被文件威胁防护、反加密、应用程序控制和行为检测组件排除在扫描范围之外。<br>必须以与 `mount` 命令输出中所显示的相同方式指定挂载点。 |
| **流量拦截排除项** | `Linux` | Kaspersky Endpoint Security 从流量拦截中排除的网络连接列表。流量拦截排除项会影响 Web 威胁防护、网络威胁防护和 Web 控制组件。排除的连接由以下参数定义：<br>• 流量方向，入站或出站。<br>• 远程设备的 IP 地址，即入站和出站流量被排除在拦截范围之外的 IP 地址（取决于流量方向）。<br>• 目标端口，即受保护设备上的端口（在入站流量拦截排除项中）或远程设备上的端口（在出站流量拦截排除项中）。<br>流量拦截排除仅适用于 TCP 连接，不会影响网络数据包规则。 |
| **Wi-Fi 网络** | `macOS` | 受信任 Wi-Fi 网络列表。您可以指定以下设置：<br>• Wi-Fi 网络名称。<br>• 加密类型。<br>• 身份验证类型。 |
| **应用程序** | `Windows` `macOS` `Linux` | *受信任应用程序列表*是一个应用程序列表，其中所包含应用程序的文件和网络活动（包含恶意活动）以及对系统注册表的访问不受 Kaspersky Endpoint Security 的监控。默认情况下，Kaspersky Endpoint Security 将监控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及其产生的网络流量。将应用程序添加到受信任应用程序列表后，Kaspersky Endpoint Security 将停止监控该应用程序的活动。 |
| **恶意软件扫描排除项** | `Windows` `macOS` `Linux` | "*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。 |
| **设备** | `Windows` `Linux` | *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。<br>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。 |

# 常规设置

# 检测设置

适用于 Windows、 macOS 和 Linux

本节介绍如何根据您的需要配置检测设置。威胁检测和预防的有效性取决于正确的配置设置。

检测设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **检测其他类型的对象** | `Windows` `macOS` `Linux` | 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、木马和恶意工具。它们可能会给计算机带来巨大的损害。<br>您还可以启用对以下类型对象的检测：<br>• "**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**"。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。<br>• `Windows` **广告软件**。广告软件程序会在其他程序的界面中显示条幅广告，并将搜索查询重定向至广告网页。<br>• `Windows` **自动拨号程序**。自动拨号程序可以利用调制解调器秘密建立电话连接。这类应用程序本身也是合法软件，但黑客可以利用它们来入侵设备或窃取用户数据。<br>• `Windows` **打包程序**。为了躲避反病毒软件的检测，黑客会使用特殊的加壳工具对恶意软件进行加壳。卡巴斯基专家已经识别出黑客中最常用的几种加壳工具。 |
| **高级清除技术** | `Windows` | 通常情况下，Kaspersky Endpoint Security 会在计算机被感染之前终止检测到的恶意软件。高级清除技术可保护计算机免受已活动的恶意软件（活动感染）的侵害，从而最大限度地降低数据丢失和威胁扩散的风险。<br>如果启用此技术，当检测到恶意活动时，Kaspersky Endpoint Security 会显示弹出通知。在该通知中，Kaspersky Endpoint Security 将提供用户执行计算机高级清除的选项。用户批准此操作后，Kaspersky Endpoint Security 将消除威胁，然后重新启动计算机。高级清除技术会占用相当多的计算资源，这可能会降低其他应用程序的运行速度。<br>当应用程序正在检测活动感染时，某些操作系统功能可能不可用。高级清除完成并重新启动计算机后，操作系统的可用性将恢复。<br>如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，Kaspersky Endpoint Security 不显示通知。因此，您无法选择操作以清除活动威胁。要清除威胁，您需要在应用程序设置中启用高级清除技术以及在"*恶意软件扫描*"任务设置中立即启动高级清除。然后您需要启动"*恶意软件扫描*"任务。 |
| **扫描期间阻止访问文件** | `Linux` | 如果选中此复选框，应用程序将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，阻止访问文件。<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。 |
| **对象日志记录设置** | `Linux` | "**记录清洁对象**"。如果选中此复选框，应用程序将为所有扫描的对象记录 *ObjectProcessed* 事件。<br>"**记录未处理的对象**"。如果选中此复选框，则应用程序将记录 *ObjectNotProcessed* 事件。<br>"**记录打包对象**"。如果选中此复选框，则应用程序将记录 *PackedObjectDetected* 事件。 |

# 卡巴斯基安全网络

适用于 Windows、 macOS 和 Linux

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

## 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

卡巴斯基安全网络设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **使用扩展 KSN 模式** | `Windows` `macOS` `Linux` | *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。Kaspersky Endpoint Security 使用 KSN 检测威胁，无论切换位置如何。<br>`Linux` 对于 Linux 设备，使用*卡巴斯基私人安全网络(KPSN)*解决方案时此选项将被隐藏。 |
| **使用云模式** | `Windows` `macOS` `Linux` | *云模式* 是指 Kaspersky Endpoint Security 使用轻量级版本的反病毒数据库的应用程序运行模式。当使用轻量级反病毒数据库时，卡巴斯基安全网络支持应用程序运行。与通常的数据库相比，轻量级版本的反病毒数据库仅需要大约一半的计算机 RAM。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。<br>如果选中此复选框，Kaspersky Endpoint Security 将使用反病毒数据库的轻量级版本，这可以减少操作系统资源上的负载。<br>选中该复选框后，Kaspersky Endpoint Security 在下次更新期间下载反病毒数据库的轻量级版本。<br>如果清空此复选框，Kaspersky Endpoint Security 将使用反病毒数据库的完全版本。<br>清除该复选框后，Kaspersky Endpoint Security 在下次更新期间下载反病毒数据库的完全版本。 |
| **KSN 服务器不可用时计算机状态** | `Windows` | 此下拉列表中的项可确定当 KSN 服务器不可用时计算机在 Kaspersky Security Center 中的状态。 |
| **使用管理服务器作为 KSN 代理服务器** | `Windows` `macOS` `Linux` | 如果选中该复选框，Kaspersky Endpoint Security 将使用 KSN 代理服务。您可以在管理服务器属性中配置 KSN 代理服务设置。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **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** | `Windows` `macOS` `Linux` | 如果选中该复选框，当 KSN Proxy服务不可用时，Kaspersky Endpoint Security 将使用 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）。 |

# 用户交互

适用于 Windows、macOS 和 Linux

本节介绍如何配置应用程序界面设置以及用户交互设置。

应用程序界面设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **在计算机启动时启动 Kaspersky Endpoint Security (建议)** | `Windows` `macOS` | 如果启用此功能，Kaspersky Endpoint Security 将在操作系统加载后启动，从而在整个会话期间保护计算机。<br>如果禁用此功能，Kaspersky Endpoint Security 不会在操作系统加载后启动，直到用户手动启动它。计算机保护已禁用，用户数据可能受到威胁。 |
| **显示应用程序图标** | `Windows` `macOS` | 客户端计算机的通知区域中有一个应用程序图标。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行操作。Kaspersky Endpoint Security 还会在应用程序图标上方显示通知。 |
| **不向用户显示应用程序界面** | `Windows` `macOS` | 如果选中此复选框，Kaspersky Endpoint Security 不允许用户打开主应用程序窗口并隐藏远程计算机上的应用程序界面。<br>如果清除此复选框，则用户可以打开 Kaspersky Endpoint Security 主窗口并使用远程计算机上的应用程序界面。 |
| **隐藏应用程序活动监控区域** | `Windows` | 如果选中此复选框，则客户端计算机上的 Kaspersky Endpoint Security 主窗口中没有“**应用程序活动监控**”按钮。*应用程序活动监控器*是一个用于实时查看用户计算机应用程序活动信息的工具。 |
| **在本地管理更新** | `macOS` | 如果选中此复选框，用户可以在远程计算机上本地管理 Kaspersky Endpoint Security 更新。<br>如果清除此复选框，则只能使用 Kaspersky Security Center 中的 Kaspersky Endpoint Security 插件在远程计算机上管理 Kaspersky Endpoint Security 更新。 |
| **在本地管理密钥** | `macOS` | 如果选中此复选框，用户可以在远程计算机上本地管理 Kaspersky Endpoint Security 密钥。<br>如果清除此复选框，则只能使用 Kaspersky Security Center 中的 Kaspersky Endpoint Security 插件在远程计算机上管理 Kaspersky Endpoint Security 密钥。 |
| **退出应用程序** | `macOS` | 如果选中此复选框，则“**退出**”命令在应用程序图标的上下文菜单中可用。远程计算机的用户可以停止远程计算机上的 Kaspersky Endpoint Security。<br>如果清除此复选框，则“**退出**”命令在应用程序图标的上下文菜单中不可用。远程计算机的用户无法停止远程计算机上的 Kaspersky Endpoint Security。 |
| **访问本地任务** | `Windows` `Linux` | 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。当没有其他策略限制时，用户可以配置并运行任务。然而，配置任务运行计划对该用户保持不可用。用户仅可以手动运行任务。<br>如果该复选框被清空，则停止使用本地任务。在该模式中，本地任务不根据计划运行。任务无法在 Kaspersky Endpoint Security 本地界面中启动或编辑，使用命令行工作时也无法进行。<br>用户仍可以通过在文件或文件夹的上下文菜单中选择“**扫描病毒**”选项开始文件或文件夹扫描。扫描任务将使用自定义扫描任务的默认设置值启动。 |
| **查看组任务** | `Windows` | 如果选择此复选框，组任务将显示在 Kaspersky Endpoint Security 的本地界面上。用户可以在应用程序界面中查看所有任务的列表。<br>如果清除该复选框，则 Kaspersky Endpoint Security 将显示空任务列表。 |
| **管理组任务** | `Windows` `Linux` | 如果选中该复选框，则用户可以启动和停止在 Kaspersky Endpoint Security 控制台中指定的组任务。用户可以在应用程序界面或简化应用程序界面中启动和停止任务。<br>如果清除该复选框，则 Kaspersky Endpoint Security 将自动启动计划任务，或者由管理员在 Kaspersky Endpoint Security 控制台中手动启动任务。 |
| **计算机状态** | `Windows` | 应用策略或执行任务出错时，安装了 Kaspersky Endpoint Security 的客户端计算机的状态在 Web 控制台中的显示设置。有以下状态可用：*正常*、*警告*和*严重*。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **应用程序状态通知** | `Windows` | 系统托盘中的应用程序事件通知设置。选择您要在通知区域中看到通知的事件类别旁的复选框。<br>• "**活动威胁**"。<br>• "**需要重启计算机**"。<br>• "**反恶意软件数据库问题**"。<br>• "**保护级别问题**"。<br>• "**授权许可问题**"。<br>• "**有更新可用**"。<br>发生与选定类别关联的事件时，通知区域的应用程序图标将根据警告的严重性更改为 或 。 |
| **本地反恶意软件数据库状态通知** | `Windows` | 应用程序使用的反病毒数据库过期的通知设置。您可以指定 Kaspersky Endpoint Security 在多少天后向用户发送"数据库已过期"和"数据库已严重过期"的消息。 |
| **应用程序启动设置** | `Linux` | 应用程序启动设置：<br>• "**启动应用程序的最大连续不成功尝试次数**"。<br>• "**等待应用程序启动的最长时间(分钟)**"。指定的等待时间到期后，kesl 进程将重新启动。 |
| **安装应用程序更新而不重启计算机** | `Windows` | 在应用程序版本更新时，无需重新启动即可升级应用程序可提供不间断的服务器操作。<br><br>在不重新启动的情况下升级应用程序有以下限制：<br>• 从 11.10.0 版开始，无需重新启动即可升级应用程序。要升级应用程序的早期版本，必须重新启动计算机。<br>• 从 11.11.0 版开始，您可以无需重新启动即可安装补丁。要安装应用程序早期版本的补丁，可能需要重新启动计算机。<br>• 在启用了数据加密（卡巴斯基加密（FDE）、BitLocker、文件级加密（FLE））的计算机上，无法在不重新启动的情况下升级应用程序。要在启用了数据加密的计算机上升级应用程序，必须重新启动计算机。<br>• 如果不重新启动，则无法在虚拟机上升级该应用程序。要升级虚拟机上的应用程序，必须重新启动虚拟机。<br><br>不重启而将 Kaspersky Endpoint Security 升级到 11.10.0 或更高版本后，计算机将安装两个 Kaspersky Endpoint Security 应用程序。不要手动卸载应用程序的早期版本。重新启动计算机时，将自动卸载以前的版本。<br><br>参数的默认值因操作系统类型而异。如果应用程序安装在工作站上，则禁用在不重新启动的情况下升级应用程序选项。如果应用程序安装在服务器上，则启用在不重新启动的情况下升级应用程序选项。 |
| **与远程管理软件的兼容性** | `Windows` | 如果将 Kaspersky Endpoint Security 与远程管理工具（RAT）一起使用会导致问题，您可以启用兼容模式。这些问题可能与 RAT 与应用程序"Secure Desktop"功能不兼容有关。此功能的目的是确认可能降低计算机安全级别的操作。此功能允许应用程序显示与其他进程隔离的确认对话框。此功能使用提升的权限来保护请求。这样，只有用户才能确认操作，而恶意软件无法确认。<br>RAT 兼容模式可能降低计算机的安全级别。如果 Kaspersky Endpoint Security 不会导致您的 RAT 出现问题，我们不建议启用兼容模式。默认情况下，该功能处于禁用状态。<br>示例：在 RemoteApp 模式下使用浏览器时，Kaspersky Endpoint Security 在访问具有不受信任证书的网站时可能不会显示确认窗口，因为 RemoteApp 不支持应用程序的安全桌面功能。这可能会导致浏览器无响应。为了使浏览器在 RemoteApp 模式下正常工作，您必须启用兼容模式。如果您在使用其他第三方软件时遇到安全桌面功能问题，也可以尝试启用兼容模式。 |

# 性能

适用于 Windows、 macOS 和 Linux

Kaspersky Endpoint Security 性能是指能源消耗和计算机资源的使用。

应用程序性能设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **为其他应用程序让出资源** | `Windows` | Kaspersky Endpoint Security 在扫描计算机时消耗计算机资源可能会增加 CPU 和硬盘驱动器子系统的负载。这可能会减慢其他应用程序的速度。为了优化性能，Kaspersky Endpoint Security 提供了*一种将资源传输到其他应用程序的模式*。在这种模式下，当 CPU 负载高时，操作系统可以降低 Kaspersky Endpoint Security 扫描任务线程的优先级。这允许将操作系统资源重新分配给其他应用程序。因此，扫描任务将获得更少的 CPU 时间。因此，Kaspersky Endpoint Security 将需要更长的时间来扫描计算机。默认情况下，程序已配置为允许其他应用程序使用资源。 |
| **使用电池供电时推迟或跳过计划任务** | `Windows` `macOS` `Linux` | 如果启用此功能，Kaspersky Endpoint Security 将切换到节能模式。<br>`Windows` Kaspersky Endpoint Security *推迟*计划任务。如果需要，您可以手动启动扫描和更新任务。<br>`macOS` `Linux` Kaspersky Endpoint Security *取消*计划任务。如果需要，您可以手动启动扫描和更新任务。<br>启用节能模式且计算机使用电池运行时，即使计划了以下任务，以下任务也不会运行：<br>• *恶意软件扫描*<br>• *反恶意软件数据库更新*<br>• *应用程序完整性检查*<br>• "*IOC 扫描*"。 |
| **限制扫描任务的 CPU 使用率** | `Windows` `macOS` `Linux` | 为了优化 Kaspersky Endpoint Security 的性能，您可以限制扫描任务的 CPU 使用率。根据所使用的操作系统，CPU 使用率受限的任务可能会有所不同：<br>• `Windows` `Linux` 恶意软件扫描<br>• `macOS` `Linux` Critical Areas Scan<br>• `Linux` Inventory<br>• `Linux` 容器扫描<br>如果启用此功能，扫描任务在所有 CPU 核心上的平均负载会接近指定值。 |
| **扫描任务的内存使用限制 (MB)** | `Linux` | 您可以配置扫描任务的内存使用限制（*恶意软件扫描*、*关键区域扫描*、*清查*和 *容器扫描*）。 |
| **配置从扫描中排除进程内存** | `Linux` | 您可以配置进程内存的扫描排除项。应用程序不扫描指定进程的内存。<br>指定应用程序将从进程内存扫描中排除的进程路径。您可以使用掩码指定路径。默认情况下，该列表为空。 |
| **限制应用程序内存使用** | `Linux` | 您可以配置应用程序的驻留内存使用限制。默认情况下，会自动设置限制。<br>**限制计算方法**：<br>• "**无限制**"。如果选择此选项，驻留内存的使用不受限制。<br>• "**设置一个精确值 (%)**"。<br>• "**设置一个精确值 (MB)**"。<br>• "**使用两个值中的最低值 (% 或 MB)**"。<br>• "**使用两个值中的最高值 (% 或 MB)**"。<br>• "**自动限制（建议）**"。如果选择此选项，驻留内存的使用被自动限制。 |
| **启用应用程序稳定性监控** | `Linux` | 您可以启用或禁用 Kaspersky Endpoint Security 应用程序稳定性监控，该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。<br>如果选中该复选框，应用程序监控 Kaspersky Endpoint Security 的操作。<br>要应用设置，请重新启动应用程序。<br>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>*。 |

# 网络设置

## 适用于 Windows、macOS 和 Linux

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。

网络设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **受信任根证书** | `Windows` `macOS` `Linux` | 受信任的根证书列表。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。要添加到系统证书存储，您可以使用 Active Directory 组策略。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **代理服务器** | Windows<br>macOS<br>Linux | 用于客户端计算机用户访问 Internet 的代理服务器的设置。Kaspersky Endpoint Security 使用这些设置来配置某些保护组件，包括进行与更新数据库和程序模块有关的配置。 |
| **使用代理服务器身份验证** | Windows<br>macOS<br>Linux | 如果选中此复选框，则应用程序在连接到代理服务器时将使用用户名和密码进行身份验证。<br>Windows 对于 Windows 设备，您需要选择一种身份验证类型：<br>• "**NTLM 身份验证**"。使用当前用户账户进行的 NTLM 身份验证（默认）。<br>• "**使用用户名和密码的 NTLM 身份验证**"。使用手动指定凭证的 NTLM 身份验证。<br>• "**用户名和密码**"。使用手动指定的凭证进行身份验证。<br>• "**自动身份验证**"。<br>• "**Kerberos 身份验证**"。使用当前用户账户进行的 Kerberos 身份验证。<br>• "**使用用户名和密码的 Kerberos 身份验证**"。使用手动指定凭证的 Kerberos 身份验证。 |
| **对本地地址不使用代理服务器** | Windows<br>macOS | 如果选择该选框，则 Kaspersky Endpoint Security 从共享文件夹执行更新时不使用代理服务器。 |
| **对以下组件不使用代理服务器** | Linux | 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-premise)** – 连接到 KATA 服务器时，不使用代理服务器。<br>• **KATA Sandbox** – 连接到负责与 KATA Sandbox 交互的 Central Node 服务器时，不使用代理服务器。<br>• **Network Detection and Response (KATA)** – 连接到 Network Detection and Response 服务器时，不使用代理服务器。 |
| **不对指定的 IP 地址和 DNS 名称使用代理服务器** | Linux | 该表包含不得使用代理服务器的 IP 地址和 DNS 名称的列表。您可以使用掩码（"*"和"?"字符）来指定地址。<br>您可以在表中添加、编辑或删除地址。 |
| **加密连接扫描** | Windows<br>macOS<br>Linux | 此功能允许 Web 威胁防护、邮件威胁防护、Web 控制和 Cloud Discovery 组件监控和处理加密 (HTTPS) 连接。<br>Linux 对于Linux设备而言，**证书验证策略**可用，它决定应用程序如何验证证书：<br>• **本地检查**表示应用程序不通过互联网来验证证书。<br>• **完整检查**（默认）表示应用程序使用互联网来验证和下载验证证书所需的缺失链。 |
| **受信任域** | Windows<br>Linux | 这将使用 Kaspersky Endpoint Security 不对其扫描网络连接的网址列表。此种情况下，在 Web 威胁防护、邮件威胁防护和 Web 控制组件正常运行的情况下，Kaspersky Endpoint Security 不扫描受信任网址的 HTTPS 流量。<br>您可以输入域名或 IP 地址。Kaspersky Endpoint Security 支持使用 * 字符在域名中输入掩码。 |
| **限制计量连接的流量** | Windows | 如果选定该复选框，应用程序将在互联网连接受限时限制其网络流量。Kaspersky Endpoint Security 会将高速移动互联网连接识别为受限制连接，将 Wi-Fi 连接识别为无限制连接。<br>计量网络运行在 Windows 8 或更新版本的计算机上。 |
| **注入脚本到 Web 流量从而与网页交互** | Windows | 如果选定该复选框，Kaspersky Endpoint Security 会将网页监听脚本注入网页流量。该脚本确保 Web 控制组件的正常工作。该脚本确保 Web 控制事件的注册。<br>Kaspersky 专家建议注入该网页交互脚本到流量以确保 Web 控制的正确操作。 |
| **检查与使用 EV 证书的网站的加密连接** | Windows | EV 证书（Extended Validation Certificate）确认网站的真实性并增强连接的安全性。浏览器在地址栏中使用锁定图标来指示网站具有 EV 证书。浏览器还可能将地址栏的全部或部分填充绿色。<br>如果启用此切换开关，应用程序将解密并监控与使用 EV 证书的网站的加密连接。<br>如果关闭此切换开关，应用程序无权访问 HTTPS 流量的内容。为此，应用程序仅基于网址（例如 https://bing.com）监控 HTTPS 流量。<br>如果您第一次打开具有 EV 证书的网站，则无论是否选中该复选框，加密连接都将被解密。 |
| **阻止 SSL 2.0 连接** | Windows | 如果选中该复选框，应用程序将监控并阻止通过 SSL 2.0 协议建立的网络连接。<br>如果清除该复选框，应用程序将不会阻止通过 SSL 2.0 协议建立的网络连接。但是，应用程序不会监控通过该协议的网络流量。 |
| **阻止 TLS 1.0 连接** | Windows | 如果选中该复选框，应用程序将阻止通过 TLS 1.0 协议建立的网络连接。<br>如果清除该复选框，应用程序将不会阻止通过 TLS 1.0 协议建立的网络连接。应用程序监控通过该协议的网络流量。应用程序的所有组件均不受限制地运行。 |
| **阻止 SSL 3.0 连接** | Windows | 如果选中该复选框，应用程序将阻止通过 SSL 3.0 协议建立的网络连接。<br>如果清除该复选框，应用程序将不会阻止通过 SSL 3.0 协议建立的网络连接。应用程序监控通过该协议的网络流量。应用程序的所有组件均不受限制地运行。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **受监控端口** | `Windows` `macOS` `Linux` | "**监控所有网络端口**"。在此网络端口监控模式下，保护组件（文件威胁防护、Web 威胁防护和邮件威胁防护）会监控通过任何开放的计算机网络端口传输的数据流。<br>"**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。通常用于传输电子邮件和网络流量的网络端口的列表按照 Kaspersky 专家的建议进行配置。<br>对于 Mac 设备，只能监控选定的端口。 |
| **监控的应用程序** | `Windows` | 应用程序列表，对于这些应用程序，无论端口扫描设置如何，都会监控所有端口上的所有流量。 |
| **选择 Firefox 要使用的证书存储** | `macOS` | "**系统根钥匙串(推荐)**"。如果选择此选项，Kaspersky Endpoint Security 将使用来自 System Roots 钥匙串的根证书来扫描 Mozilla Firefox 浏览器中的加密 HTTPS 流量。<br>默认情况下已选定该选项。<br>"**Mozilla Firefox 浏览器设置中的证书存储**"。如果选择此选项，Kaspersky Endpoint Security 将使用来自浏览器证书存储的证书。<br>此种情况下，您需要手动将 Kaspersky Endpoint Security 证书添加到 Mozilla Firefox 浏览器的证书存储中。有关更多信息，请参阅"如何将卡巴斯基证书添加到 Mozilla Firefox 证书存储"。 |
| **流量拦截模式** | `Linux` | "**iptables**"。Kaspersky Endpoint Security 使用 iptables 工具进行流量拦截。<br>"**eBPF**"。应用程序使用 eBPF 技术拦截流量。 |

# 容器扫描

对于 Linux

该应用程序实时扫描正在运行的容器和命名空间。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。

容器扫描需要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。

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。

容器扫描设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **检测到威胁后的操作** | `Linux` | "**跳过容器**"。当检测到感染对象时，应用程序不会对容器执行任何操作。<br>"**停止容器**"。当检测到感染对象时，应用程序将停止容器。<br>"**如果清除失败则停止容器**"。如果无法清除感染对象，应用程序将停止容器。 |
| **使用 Docker** | `Linux` | 使用 Docker 环境。要使用该环境，请输入 Docker 套接字的路径或 URI（通用资源 ID）。 |
| **使用 CRI-O** | `Linux` | 使用 CRI-O 环境。要使用该环境，请输入 CRI-O 配置文件的路径。 |
| **使用 Podman** | `Linux` | 使用 Podman 实用程序。要使用此实用程序，请输入实用程序可执行文件的路径和容器存储的根目录的路径。 |
| **使用 runc** | `Linux` | 使用 runc 实用程序。要使用此实用程序，请输入实用程序可执行文件的路径和容器状态存储的根目录的路径。 |

# 技术支持

适用于 Windows 和 Linux

为了排查 Kaspersky Endpoint Security 在计算机上可能出现的故障，技术支持人员可能需要有关系统以及应用程序运行期间发生的事件的信息。此信息存储在转储文件和跟踪文件中。

*转储文件*包含该文件创建时 Kaspersky Endpoint Security 进程的工作内存的所有相关信息。

使用*跟踪文件*可以跟踪逐步执行应用程序命令的过程，并确定应用程序操作中发生错误的阶段。

转储文件和跟踪文件可能包含敏感数据。要控制对数据的访问，必须单独确保这些文件的安全性。

只要应用程序在使用中，就会在计算机中存储转储文件和跟踪文件，当应用程序被卸载后，这些文件将被永久删除。

在计算机上应用安全配置文件后，应用程序开始写入转储文件。出现故障后，下次启动应用程序时，将打开一个窗口以加载技术支持信息。在此窗口中，您可以查看关于创建的转储文件的信息并批准将其发送给卡巴斯基。

技术支持设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **转储写入已启用** | `Windows` `Linux` | 如果启用了转储写入功能，Kaspersky Endpoint Security 会在应用程序崩溃时创建转储文件。<br>`Linux` 转储文件使用相当多的可用磁盘空间。如果硬盘上的可用空间不足 4 GB，则启用转储可能会导致磁盘空间不足。 |
| **转储和跟踪文件保护已启用** | `Windows` | 如果启用了转储文件和跟踪文件保护，则以下用户可以访问这些文件：<br>• 系统管理员和本地管理员以及启用写入转储文件和跟踪文件的用户可以访问转储文件。<br>• 只有系统管理员和本地管理员可以访问跟踪文件。 |
| **代码转储路径** | `Windows` `Linux` | 转储文件存储在以下文件夹中：<br>• `Windows`：`%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces`<br>您无法为转储文件设置不同的文件夹。<br>• `Linux`：`var/opt/kaspersky/kesl/common/dumps` 和 `var/opt/kaspersky/kesl/common/dumps-user`<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。访问转储文件目录需要 root 权限。 |
| **跟踪文件夹路径** | `Windows` `Linux` | 跟踪文件存储在以下文件夹中：<br>• `Windows`：`%ProgramData%\Kaspersky Lab\KES.[AppVersion]\Traces`<br>您无法为跟踪文件设置不同的文件夹。<br>• `Linux`：`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。访问跟踪文件目录需要 root 权限。 |
| **跟踪文件最大大小 (MB)** | `Linux` | 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）。 |
| **跟踪文件的最大数量** | `Linux` | 在此字段中，您可以输入应用程序跟踪文件的最大数量。 |
| **自定义技术支持 Web 资源** | `Windows` | 此表包含用户在 Kaspersky Endpoint Security 出现故障时可用来联系技术支持的联系信息。您还可以为用户配置消息模板，其中包含如何获得帮助的说明。<br>默认情况下，应用程序会显示指向卡巴斯基网站的链接。 |

# 报告和存储

适用于 Windows、macOS 和 Linux

本部分允许您管理有关 Kaspersky Endpoint Security 遇到的事件的报告的创建和保留设置，以及配置备份和隔离区中对象的存储。

## 报告

有关每个 Kaspersky Endpoint Security 组件的操作、数据加密事件、每个扫描任务的性能、更新任务和完整性检查任务以及应用程序的整体操作的信息都记录在*报告*中。

`Windows` 报告存储在 `C:\ProgramData\Kaspersky Lab\KES.12.4.0\Report` 文件夹中。

## 备份

*备份*存储保存在清除过程中删除或修改的文件的副本。*备份副本*是指对文件进行病毒清除或删除前创建的文件副本。文件的备份副本以特定格式保存并且不会带来威胁。

文件的备份副本存储在文件夹中：

- `Windows`：`C:\ProgramData\Kaspersky Lab\KES.12.4.0\QB`
- `Linux`：`/var/opt/kaspersky/kesl/common/objects-backup/`

管理员组中的用户被授予访问该文件夹的完整权限。其账户用于安装 Kaspersky Endpoint Security 的用户被授予该文件夹的有限访问权限。

## 隔离

*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。

"报告和存储"设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **在此时间段后删除报告(天)** | `Windows` `macOS` | 如果选中该复选框，则最大报告存储期限制为定义的时间间隔。在此时间之后，Kaspersky Endpoint Security 将自动删除报告文件中的最早条目。 |
| **限制报告文件大小为(MB)** | `Windows` | 如果选中该复选框，则最大报告文件大小限制为定义值。要避免超过最大报告文件大小，当达到最大报告文件大小时，Kaspersky Endpoint Security 将自动删除报告文件中的最早条目。 |
| **仅保留最近事件** | `macOS` | 如果选中此复选框，则每次启动任务时，Kaspersky Endpoint Security 都会删除自上次启动任务以来发生的非关键事件的信息，但会保留报告中的重要注释（例如，有关检测到的恶意对象的信息）。 |
| **记录非关键事件** | `macOS` | 如果选中此复选框，则 Kaspersky Endpoint Security 会在报告中记录非关键事件（例如，信息性事件）。非关键事件不会影响保护。 |
| **在此时间段后删除对象(天)** | `Windows` `macOS` `Linux` | 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。最长存储期限到期后，Kaspersky Endpoint Security 将删除备份区中最旧的文件。 |
| **限制备份区大小为(MB)** | `Windows` `Linux` | 如果选中该复选框，则最大存储大小限制为定义值。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。 |
| **限制隔离区大小** | `Windows` `Linux` | "**隔离区最大大小(MB)**"。如果选中该复选框，则最大隔离区大小限制为定义值。当隔离区达到最大大小时，Kaspersky Endpoint Security 将"*隔离区存储空间不足*"事件发送到 Kaspersky Security Center，并在操作系统事件日志中创建事件。同时，应用程序停止隔离新对象。您必须手动清空隔离区。<br>"**当隔离区存储达到此值时通知(%)**"。隔离的阈值。例如，您可以将隔离阈值设置为 50%。当隔离区达到阈值时，应用程序会将相应事件发送到 Kaspersky Security Center 并记录该事件。同时，应用程序继续隔离新对象。 |

# 与 KSC 的整合

本节介绍如何配置 Kaspersky Endpoint Security 与 Kaspersky Security Center 的集成。

Kaspersky Security Center 集成设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **将 Kaspersky Security Center 用作代理服务器以进行激活** | `Windows` `macOS` `Linux` | 如果选中此复选框，应用程序将使用 Kaspersky Security Center 管理服务器作为连接到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。如果您正使用密钥文件激活应用程序，不需要互联网访问。<br>如果应用程序以 Light Agent 模式使用，则不适用。 |
| **到管理服务器的数据传输** | `Windows` `macOS` `Linux` | 其信息必须发送到管理服务器的客户端计算机上的事件类别。您可以禁用某些数据的传输以优化管理服务器上的磁盘空间。<br>应用程序发送以下类别的事件：<br>• `Windows` **关于威胁发展链**。<br>• `Windows` `macOS` `Linux` **关于隔离区文件**。<br>• `Windows` `Linux` **关于备份区中的文件**。<br>• `Windows` `Linux` **关于未处理的文件**。<br>• `Windows` `macOS` `Linux` **关于已安装的设备**。<br>• `Windows` `Linux` **关于已启动的应用程序**。<br>• `Windows` **关于文件加密错误**。<br>• `Windows` **有关自适应异常控制规则状态的报告**。<br>• `Windows` **有关触发的自适应异常控制规则的报告**。 |

# 操作系统交互设置

## 对于 Linux

为确保正常运行，应用程序必须拦截系统事件，即文件操作和进程启动。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。

操作系统交互设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **拦截机制** | `Linux` | 应用程序使用的系统事件拦截机制：<br>• "**Fanotify 技术**"。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** | `Linux` | 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**"。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(较低的保护级别)**"。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。<br>此设置在选择"**可更新内核模块**"拦截机制时可用。 |
| **遥测源** | `Linux` | Kaspersky Endpoint Security 用于遥测数据采集的来源：<br>• "**仅使用 eBPF**"。仅使用 eBPF 技术。<br>• "**默认**"。同时使用了 eBPF 技术和 auditd 服务。 |
| **auditd 操作模式** | `Linux` | 在此模式下，auditd 服务会记录审计事件，以便后续传输至 Detection and Response 解决方案：<br>• "**独占的**"。如果选择此选项，Kaspersky Endpoint Security 仅使用 auditd 服务。第三方应用程序无法连接到审计流。<br>• "**非独占的**"。如果选择此选项，auditd 服务可以接受来自使用系统审计的不同进程的多个连接。 |

# 事件设置

适用于 Windows、macOS 和 Linux
本部分允许您配置有关受管理设备事件和一般事件的通知。通知可以发送到此工作区中用户的电子邮件地址。

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数据库更新成功，或者指出需要修复的组件错误。

Kaspersky Endpoint Security 事件可分为以下几个严重级别：

- *关键事件* 对计算机安全构成严重威胁（检测到恶意对象、漏洞、Kaspersky Endpoint Security 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。
- *功能性故障* 是 Kaspersky Endpoint Security 发生故障时发生的事件（处理错误、任务设置错误）。此类事件不会直接威胁计算机的安全，但需要您进行干预，以确保 Kaspersky Endpoint Security 正常工作并保护您的设备。
- *警告* 虽然不需要您立即采取行动，但可能表明计算机安全存在未来威胁。
- "*信息性消息*"。

无论是否启用通知，Kaspersky Endpoint Security 都会将所有应用程序事件的信息记录在应用程序报告中。

您可以为每个 Kaspersky Endpoint Security 事件配置接收通知的方式：

- `Windows` **通过电子邮件通知**。
- `Windows` **保存在本地报告中**。
- `Windows` `macOS` **在屏幕上通知**。
- `Windows` `Linux` **保存到系统事件日志**。

# 遥测设置

适用于 Windows、macOS 和 Linux
本部分允许您配置从受管理设备到遥测采集服务器的遥测发送。*遥测*是受保护计算机上发生的事件的列表。Kaspersky Endpoint Security 分析遥测数据并在同步期间将其发送到 Kaspersky Anti Targeted Attack Platform 或遥测采集服务器。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。

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。

您可以在"内置代理"部分管理每个内置代理的同步设置，并根据您的网络负载选择最佳值。

在本部分，您可以配置：

- 遥测的包含和排除规则。
- 要发送到 KATA 服务器、遥测采集服务器或响应服务器的遥测数据采集。

### EDR Expert (on-premise) 遥测

适用于 Windows、macOS 和 Linux

EDR Expert (on-premise) 遥测设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **EDR Expert (on-premise) 遥测** | `Windows` `macOS` `Linux` | **导入** 和 **导出**。您可以将 EDR Expert (on-premise) 遥测设置导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。您还可以使用导出/导入功能备份已发送事件的设置，或将列表迁移到另一个策略。 |
| **常规排除项** | `Windows` `macOS` `Linux` | 为了优化传输的数据，您可以为某些事件类型配置排除规则。Kaspersky Endpoint Security 不会采集属于此类规则范围内的遥测数据。这样可以减少流量，并避免处理来自受信任对象和进程的事件。<br><br>“**规则名称**”。<br><br>**操作**：<br><br>• “**不采集**”。如果您选择此选项，Kaspersky Endpoint Security 将不会采集满足该规则条件的遥测数据。<br>• “**排除 IOA**”。如果您选择此选项，Kaspersky Endpoint Security 将不会根据 IOA 规则触发采集遥测数据。*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。<br>“**条件**”。规则触发条件。指定遥测参数、条件运算符以及参数的值。默认情况下，Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。您可以使用 AND 和 OR 逻辑运算符添加多个条件或条件组。 |
| **所有事件类型** | `Windows` `macOS` `Linux` | 卡巴斯基默认定义遥测采集的事件类型列表。<br><br>您可以手动启用或禁用每种事件类型的遥测，并配置遥测排除项和包含规则。 |

### EDR (KATA) / NDR (KATA) 遥测

适用于 Windows 和 Linux

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。

| 设置 | OS | 描述 |
| --- | --- | --- |
| **排除的进程** | `Windows` `Linux` | Kaspersky Endpoint Security 不会处理与列表中进程相关的数据。<br>“**优化要发送的遥测大小**”。Kaspersky Endpoint Security 允许优化传输的数据量并从遥测中排除具有某些代码的事件：Microsoft SMB 协议、WinRM 服务和网络代理 klnagent.exe 进程的代码 102（基本通信）和 8（进程的网络活动），以及有关所有类型网络协议的网络数据包类型的扩展信息。<br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br>**用于以下事件类型**：<br>• “**文件修改**”。<br>• “**网络事件**”。<br>• “**进程: 控制台交互式输入**”。<br>• “**模块已加载**”。<br>• “**注册表已修改**”。<br>• “DNS **日志**”。<br>• “**进程访问**”。<br>• “**代码注入**”。<br>• `Windows` **WMI 查询**。<br>• “**管道**”。<br>• “LDAP”。<br>• `Windows` **AMSI**。 |
| **排除的网络通信** | `Windows` `Linux` | Kaspersky Endpoint Security 不会处理与列表中网络通信相关的数据。在排除规则中，您可以指定：<br>“**规则名称**”。<br>“**方向**”。<br>“**协议**”。<br>“**原始套接字**”。<br>“**协议号**”。<br>“**本地地址**”。Kaspersky Endpoint Security 从网络流量中排除遥测的计算机的网络地址。<br>“**本地端口或范围**”。<br>“**远程地址**”。Kaspersky Endpoint Security 从网络流量中排除遥测的计算机的网络地址。<br>“**远程端口或范围**”。<br>IP 地址仅支持 IPv4 格式。<br>“**将规则应用于所选应用程序**”。如果选中此复选框，Kaspersky Endpoint Security 会将 EDR 遥测数据从列表中应用程序的可执行文件的网络流量中排除。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **排除的文件操作** | `Windows` `Linux` | Kaspersky Endpoint Security 不会处理列表中的文件操作。在排除规则中，您可以指定：<br>“**规则名称**”。<br>“**文件名或掩码**”。当访问文件时，Kaspersky Endpoint Security 将应用排除规则的文件名或掩码。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。<br>“**选择文件操作**”。将应用该规则的文件操作类型。<br>“**先前路径**”。<br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。 |
| **排除的 DNS 操作** | `Windows` `Linux` | Kaspersky Endpoint Security 不会处理列表中的 DNS 操作。在排除规则中，您可以指定：<br>“**规则名称**”。<br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br>**DNS 操作**：<br>• “**DNS 服务器 IP 地址**”。<br>• “**查询选项**”。<br>• “**状态**”。<br>• “**域名**”。<br>• “**设置类型 ID**”。<br>• “**相应数据**”。DNS 查询响应的内容。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **排除的 LDAP 操作** | `Windows` | Kaspersky Endpoint Security 不会处理列表中的 LDAP 操作。在排除规则中，您可以指定：<br>“**规则名称**”。<br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br>**LDAP 操作**：<br>• “**LDAP 搜索范围**”。LDAP 搜索范围。可以取以下值之一：ADS_SCOPE_BASE、ADS_SCOPE_ONELEVEL、ADS_SCOPE_SUBTREE。<br>• “**过滤器**”。<br>• “**LDAP 对象搜索的可分辨名称**”。LDAP 目录中记录的名称。<br>• “**用于 LDAP 操作搜索的对象属性**”。查询中设置的属性作为返回值。 |
| **排除的进程访问查询** | `Windows` | Kaspersky Endpoint Security 不会处理对列表中进程的访问请求。在排除规则中，您可以指定：<br>“**规则名称**”。<br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br>**进程**、**父进程**、**目标进程文件**、**源进程句柄** 和 **目标进程的句柄**。<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br>**进程访问查询**：<br>• “**操作类型**”。<br>• “**进程访问请求**”。<br>• “**调用堆栈跟踪**”。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **排除的代码注入** | `Windows` | Kaspersky Endpoint Security 不会处理列表中的代码注入。在排除规则中，您可以指定：<br>“**规则名称**”。<br><br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br><br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br><br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br><br>**代码注入**：<br><br>• “**访问方法**”。<br>• “**调用堆栈**”。拦截与代码注入相关的函数时的 API 调用堆栈<br>• “**修改的命令行**”。<br>• “**注入地址**”。远程运行代码在目标进程地址空间中的地址。<br>如果使用 SET_WINDOWS_HOOK 和 ARG_SPOOFING 方法实现代码注入，则此字段留空。<br>• “**修改的命令行**”。<br>• “**注入的 DLL 名称**”。包含拦截器例程的 DLL 的名称以及注入后控制权传递到的函数的名称。<br>如果使用 SET_WINDOWS_HOOK 方法实现了代码注入，则此字段将被填充。<br>• “**注入的 DLL 路径**”。包含拦截器例程的 DLL 的路径。<br>如果使用 SET_WINDOWS_HOOK 方法实现了代码注入，则此字段将被填充。 |
| **排除的 WMI 查询** | `Windows` | Kaspersky Endpoint Security 不会处理列表中的 WMI 请求。在排除规则中，您可以指定：<br>“**规则名称**”。<br><br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br><br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br><br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br><br>**WMI 查询**：<br>• “**WMI 操作类型**”。<br>• “**远程查询**”。<br>• “**执行 WMI 命令的计算机的名称**”。<br>• “**WMI 用户账户**”。<br>• “**执行的 WMI 命令**”。<br>• “**WMI 名字空间**”。<br>• “**WMI 事件使用者过滤器**”。<br>• “**创建的 WMI 事件使用者的名称**”。<br>• “**WMI 事件使用者源代码**”。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **排除的管道操作** | `Windows` | Kaspersky Endpoint Security 不会处理列表中的管道操作。在排除规则中，您可以指定：<br>“**规则名称**”。<br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br>**管道操作**：<br>• “**管道名称**”。<br>• “**操作类型**”。 |
| **被排除的注册表更改** | `Windows` | Kaspersky Endpoint Security 不会处理列表中的注册表修改。在排除规则中，您可以指定：<br>“**规则名称**”。<br>Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。<br>**进程** 和 **父进程**：<br>• “**完整路径**”。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。<br>• “**命令行文本**”。用于运行文件的命令。<br>• “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。<br>• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。<br>• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。<br>• “**文件校验和**”。MD5 和 SHA256。<br>您也可以手动选择文件，应用程序将自动填写所选文件中的字段。<br>在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。<br>**注册表更改**：<br>• “**操作类型**”。<br>• “**路径**”。进行修改的注册表键的路径。<br>• “**值名称**”。修改后的值的名称，例如 RegistrySizeLimit。<br>• “**值**”。<br>• “**注册表文件全称**”。 |
| **排除的设备操作** | `Windows` | Kaspersky Endpoint Security 不会处理与列表中的 USB 设备相关的操作。在排除规则中，您可以指定：<br>“**规则名称**”。<br>“**设备类型**”。<br>“**设备 ID**”。<br>“**设备名称**”。 |

## KUMA 遥测

对于 Windows

默认情况下，向 KUMA 服务器发送事件是禁用的。为确保 KUMA 正常工作，您必须启用遥测发送功能。您可以从标准日志中选择事件源：*Application*、*Security*或*System*。您还可以指定第三方应用程序的日志。为了提高性能并优化向 KUMA 服务器的数据传输，您可以手动添加单个事件日志。

KUMA 遥测设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **Windows 事件日志** | `Windows` | 应用程序发送给 KUMA 的 Windows 日志事件。您可以手动逐个添加日志，也可以导入包含设置的 JSON 文件。<br><br>您可以为每个事件日志选择发送方式：<br><br>• "**发送所有事件**"。在此模式下，应用程序会发送 Windows 日志中的所有事件（添加到排除规则的事件除外）。<br>• "**仅发送选定的事件**"。在此模式下，应用程序仅发送包含规则中添加的事件。<br>您还可以为相关事件发送模式配置排除或包含规则。要添加规则，您需要指定 Windows 事件日志中事件的 ID。您可以在一个规则中列出多个事件 ID。指定多个事件 ID 时，请使用逗号作为分隔符。 |

# 内置代理

## Managed Detection and Response

适用于 Windows、macOS 和 Linux

Kaspersky Endpoint Security 支持与 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。

您必须启用以下组件以便 Managed Detection and Response 正常工作：

- 卡巴斯基安全网络（扩展模式）
- 行为检测

启用这些组件不是可选的。否则 Kaspersky Managed Detection and Response 无法工作，因为它不接收所需的遥测数据。

Managed Detection and Response 组件设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **MDR 配置文件** | `Windows`<br>`macOS`<br>`Linux` | BLOB 文件包含客户端 ID 和 Kaspersky Managed Detection and Response 授权许可信息。BLOB 文件存在于 MDR 配置文件的 ZIP 存档中。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 存档。对于 BLOB 文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。 |

## Endpoint Detection and Response Optimum

适用于 Windows、macOS 和 Linux

Kaspersky Endpoint Security 包含 Kaspersky Endpoint Detection and Response Optimum 解决方案（也叫"EDR Optimum"）的内置代理。*Kaspersky Endpoint Detection and Response* 是一种保护企业 IT 基础架构免受高级网络威胁的一系列解决方案。该解决方案的功能将自动检测威胁与应对这些威胁的能力结合起来，以抵御高级攻击，包括新的漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法。

Kaspersky Endpoint Detection and Response 分析用户设备上潜在的危险活动并提供给*安全人员*或者*管理员*有关可能发生的攻击的信息，以便及时采取响应措施或自动应用已配置的响应措施。

您必须启用以下组件以便 Endpoint Detection and Response 正常工作：

- 文件威胁防护
- Web 威胁防护
- 邮件威胁防护
- 漏洞利用防御
- 行为检测
- 主机入侵防御
- 修复引擎
- 自适应异常控制

不同平台的组件列表可能不同。

Endpoint Detection and Response 组件设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **启用高级系统活动日志记录** | Windows<br>macOS<br>Linux | 此设置有助于确保"**IOC 追溯扫描**"任务的正确性。它需要消耗大量的计算机资源。 |
| **网络隔离** | Windows<br>macOS<br>Linux | 为响应检测到的威胁，自动将计算机与网络隔离。<br>打开网络隔离后，应用程序将断开所有活动连接并阻止计算机上的所有新 TCP/IP 连接。应用程序仅保留以下连接处于活动状态：<br>• 网络隔离排除中列出的连接。<br>• 由 Kaspersky Endpoint Security 服务启动的连接。<br>• 由 Kaspersky Security Center 网络代理发起的连接。 |
| **自动解锁被隔离设备的时间(小时)** | Windows<br>macOS<br>Linux | 网络隔离可以在指定时间后自动关闭，也可以手动关闭。 |
| **网络隔离排除项** | Windows<br>macOS<br>Linux | 网络隔离排除规则列表。当网络隔离打开时，符合规则的网络连接不会在计算机上被阻止。<br>要配置网络隔离排除项，您可以使用*标准网络配置文件*列表。默认情况下，排除项包括网络配置文件，其中包含确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备不间断运行的规则。您还可以修改标准网络配置文件的设置或手动定义排除项。<br>只有在网络隔离自动打开以响应检测到的威胁时，才会应用策略属性中指定的排除项。仅当在 Kaspersky Security Center 控制台的"计算机属性"中或警报详情中手动打开网络隔离时，才会应用"计算机属性"中指定的排除项。 |
| **执行防护** | Windows<br>macOS<br>Linux | 控制可执行文件和脚本的执行以及 Office 格式文件的打开。例如，您可以防止在所选计算机上执行被认为不安全的应用程序。执行防护支持一组 Office 文件扩展名和一组脚本解释器。<br>要使用执行防护组件，您需要添加执行防护规则。 |
| **执行或打开禁止的对象时的操作** | Windows<br>macOS<br>Linux | "**阻止并添加到事件日志**"。在此模式下，应用程序将阻止执行符合防护规则标准的对象或打开这样的文档。应用程序还将尝试执行对象或打开文档的事件发布到系统事件日志和 Kaspersky Security Center。<br>"**添加到事件日志**"。在此模式下，Kaspersky Endpoint Security 将发布关于尝试执行符合防护规则标准的可执行对象或打开这样的文档的事件到系统事件日志和 Kaspersky Security Center，但不会阻止尝试运行对象或打开文档。默认情况下已选择此模式。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **执行防护规则** | `Windows` `macOS` `Linux` | *执行防护规则*是应用程序在对对象执行做出反应时（例如，在阻止对象执行时）考虑的一组条件。应用程序通过使用 MD5 和 SHA256 哈希算法计算的路径或校验和来识别文件。 |
| **使用区分大小写的路径** | `Linux` | 如果选中此复选框，则应用程序在创建执行阻止规则时将区分大小写。 |
| **Cloud Sandbox** | `Windows` `macOS` `Linux` | *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。<br><br>要获取有关被分析对象的信息，需要建立 KSN 连接。 |

# Endpoint Detection and Response Expert (on-premise)

适用于 Windows、 macOS 和 Linux

Endpoint Detection and Response Expert 版本 7.1 或更早版本

Kaspersky Endpoint Security 支持 Kaspersky Endpoint Detection and Response Expert 组件（版本 7.1 及更早版本，以下简称“EDR (KATA)”），该组件是 Kaspersky Anti Targeted Attack Platform 解决方案的一部分。*Kaspersky Anti Targeted Attack Platform* 是旨在及时检测复杂威胁（如针对性攻击、高级持久性威胁 (APT)、零日攻击等）的解决方案。Kaspersky Anti Targeted Attack Platform 包括三个功能单元：

- Kaspersky Anti Targeted Attack Platform（*KATA*）
- Kaspersky Endpoint Detection and Response（*EDR（KATA）*）
- Network Detection and Response（*NDR（KATA）*）

您可以购买所有功能单元，也可以单独购买单个功能单元。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack 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 Anti Targeted Attack Platform 服务器。此种情况下，Kaspersky Endpoint Security 也将应用程序发现的威胁信息和威胁处理结果信息发送到 Kaspersky Anti Targeted Attack Platform 服务器。

EDR (KATA) 和 NDR (KATA) 集成在 Kaspersky Security Center 控制台上配置。然后使用 Kaspersky Anti Targeted Attack Platform 控制台管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

Endpoint Detection and Response Expert 版本 8.0 或更高版本

Kaspersky Endpoint Security 支持卡巴斯基的 Endpoint Detection and Response Expert 类解决方案（版本 8.0 及更高版本，以下简称“EDR Expert (on-premise)”）。例如，Kaspersky Symphony XDR 就是此类解决方案之一。*Endpoint Detection and Response Expert (on-premise)* 是一款企业网络安全解决方案，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 (on-premise) 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，并允许使用统一调查图调查事件。该调查图整合了 EDR Expert (on-premise) 中收集的所有事件，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。

## Endpoint Detection and Response Expert 所需的组件

您必须启用以下组件以便 Endpoint Detection and Response Expert 正常工作：

- 文件威胁防护
- Web 威胁防护
- 邮件威胁防护
- 漏洞利用防御
- 行为检测
- 主机入侵防御
- AMSI 保护
- 后台扫描
- 卡巴斯基安全网络

不同平台的组件列表可能不同。

Endpoint Detection and Response Expert (on-premise) 组件设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **Endpoint Detection and Response Expert 解决方案** | `Windows` `macOS` `Linux` | Kaspersky Endpoint Security 可与之集成的 Endpoint Detection and Response Expert 解决方案。<br>• "**Endpoint Detection and Response Expert (版本 7.1 或更早版本)**"。<br>• "**Endpoint Detection and Response Expert (版本 8.0 或更高版本)**"。 |
| **连接设置** | `Windows` `macOS` `Linux` | 管理以下 KATA 或遥测采集服务器连接设置：<br>• "**服务器连接超时**"。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。<br>• "**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）。<br>• "**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。<br>加密容器必须受密码保护。无法添加密码为空的加密容器。 |

| 设置 | OS | 描述 |
| --- | --- | --- |
| **发送同步请求到服务器的间隔(分钟)**<br>*（仅适用于 Endpoint Detection and Response Expert 7.1 或更早版本）* | `Windows` `macOS` `Linux` | 发送到服务器的同步请求的频率。在同步期间，Kaspersky Endpoint Security 发送有关修改的应用程序设置和任务的信息。 |
| **连接到 KATA 服务器 / 连接到遥测采集服务器** | `Windows` `macOS` `Linux` | 输入 IP 地址 (IPv4 或 Ipv6) 和端口以连接到 Kaspersky Anti Targeted Attack Platform 服务器或遥测采集服务器。<br>您可以为 Central Node 服务器 (KATA) 或遥测采集服务器添加多个地址。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。<br>EDR (KATA) 和 EDR Expert (on-premise) 解决方案具有不同的架构。为了处理遥测数据，EDR Expert (on-premise) 使用遥测收集服务器，而 EDR (KATA) 使用 Central Node 服务器。因此，如果您要将应用程序与 EDR Expert (on-premise) 集成，则需要添加遥测收集服务器。 |
| **发送遥测到 KATA / 将遥测发送到遥测采集服务器** | `Windows` `macOS` `Linux` | 此功能允许完全阻止遥测数据发送到 KATA 服务器或遥测采集服务器，具体取决于所选解决方案。例如，如果您将 Kaspersky Anti Targeted Attack Platform 与另一个也使用遥测的解决方案一起使用，您可以关闭 KATA (EDR) 的遥测发送。这使您可以优化这些解决方案的服务器负载。<br>如果您部署了 Managed Detection and Response 解决方案和 KATA (EDR)，则可以使用 MDR 遥测并在 KATA (EDR) 中创建威胁响应任务。 |
| **仅发送带有 IOA 的遥测**<br>*（仅适用于 Endpoint Detection and Response Expert 8.0 或更高版本）* | `Windows` `Linux` | 这允许优化遥测并仅发送带有 IOA 的遥测。<br>*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。 |
| **最大事件传输延迟(秒)** | `Windows` `macOS` `Linux` | 应用程序在同步间隔到期后与服务器同步以发送事件。 |
| **事件包的最大数量** | `Windows` | 当缓冲区充满事件时，应用程序会与服务器同步。 |
| **启用请求限制** | `Windows` `macOS` `Linux` | 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>“**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。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。<br>“**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。 |
| **连接到响应服务器**<br>*（仅适用于 Endpoint Detection and Response Expert 8.0 或更高版本）* | `Windows` `macOS` `Linux` | 到响应服务器的连接设置。请输入响应服务器 IP 地址（IPv4 或 IPv6）和连接到服务器的端口。<br>您可以添加多个响应服务器地址。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。 |
| **连接设置**<br>*（仅适用于 Endpoint Detection and Response Expert 8.0 或更高版本）* | `Windows` `macOS` `Linux` | 为响应服务器连接配置以下内容：<br>• “**服务器连接超时**”。最大响应服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的响应服务器。<br>• “**服务器证书**”。用于与响应服务器建立受信任连接的 TLS 证书。<br>• “**使用双向身份验证**”。在 Kaspersky Endpoint Security 和响应服务器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，您需要在响应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）。配置响应服务器设置后，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。<br>加密容器必须受密码保护。无法添加密码为空的加密容器。 |

# Network Detection and Response (KATA)

适用于 Windows 和 Linux

Kaspersky Endpoint Security 支持作为 Kaspersky Anti Targeted Attack Platform (EDR (KATA)) 解决方案的一部分与 Kaspersky Network Detection and Response 组件协同工作。*Kaspersky Anti Targeted Attack Platform* 是旨在及时检测复杂威胁（如针对性攻击、高级持久性威胁 (APT)、零日攻击等）的解决方案。Kaspersky Anti Targeted Attack Platform 包括三个功能单元：

- Kaspersky Anti Targeted Attack Platform（*KATA*）
- Kaspersky Endpoint Detection and Response（*EDR（KATA）*）
- Network Detection and Response（*NDR（KATA）*）

您可以购买所有功能单元，也可以单独购买单个功能单元。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack 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 Anti Targeted Attack Platform 服务器。此种情况下，Kaspersky Endpoint Security 也将应用程序发现的威胁信息和威胁处理结果信息发送到 Kaspersky Anti Targeted Attack Platform 服务器。

EDR (KATA) 和 NDR (KATA) 集成在 Kaspersky Security Center 控制台上配置。然后使用 Kaspersky Anti Targeted Attack Platform 控制台管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

必须启用以下组件才能使 Network Detection and Response (KATA) 工作：

- 文件威胁防护
- Web 威胁防护
- 邮件威胁防护
- 漏洞利用防御
- 行为检测
- 主机入侵防御
- AMSI 保护
- 后台扫描
- 卡巴斯基安全网络

不同平台的组件列表可能不同。

| 设置 | OS | 描述 |
| --- | --- | --- |
| **连接设置 到 KATA 服务器** | Windows Linux | "**服务器连接超时**"。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。<br>"**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）。<br>"**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。<br>加密容器必须受密码保护。无法添加密码为空的加密容器。 |
| **连接到 KATA 服务器** | Windows Linux | 连接到 Kaspersky Anti Targeted Attack Platform 服务器的设置。输入要连接的 Central Node 服务器的 IP 地址（IPv4 或 IPv6）和端口。<br>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。 |
| **发送同步请求到 KATA 服务器的间隔(分钟)** | Windows Linux | 发送到服务器的同步请求的频率。在同步期间，Kaspersky Endpoint Security 发送有关修改的应用程序设置和任务的信息。 |
| **最大事件传输延迟(秒)** | Windows Linux | 应用程序在同步间隔到期后与服务器同步以发送事件。 |
| **启用请求限制** | Windows Linux | 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>"**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。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。<br>"**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。 |

# Sandbox

适用于 Windows 和 Linux

Kaspersky Endpoint Security 支持与 Kaspersky Sandbox 解决方案和 Sandbox 组件的集成，后者是 Kaspersky Anti Targeted Attack Platform 解决方案的一部分。*Sandbox* 组件检测并自动阻止计算机上的高级威胁。Sandbox 分析对象行为，以检测恶意活动和针对组织 IT 基础设施的攻击的活动特征。Sandbox 使用部署的 Microsoft Windows 操作系统虚拟映像（Sandbox 服务器）分析和扫描特殊服务器上的对象。有关解决方案的详细信息，请参阅 Kaspersky Sandbox 帮助 和 Kaspersky Anti Targeted Attack Platform 帮助 。

KATA Sandbox 组件允许不仅自动扫描文件，还可以从文件上下文菜单手动扫描文件。

KATA Sandbox 需要部署 Kaspersky Anti Targeted Attack Platform 7.0 或更高版本。

Sandbox 组件设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **整合模式** | `Windows` `Linux` | "**Kaspersky Sandbox**"。与 Kaspersky Sandbox 解决方案集成。应用程序仅在自动模式下发送文件以在 Kaspersky Sandbox 中进行扫描。<br>"**KATA Sandbox**"。与 Kaspersky Anti Targeted Attack Platform 解决方案的 Sandbox 组件集成。您可以选择扫描的文件提交模式：<br>• "**手动**"。用户从上下文菜单手动提交文件进行扫描（**发送到 Sandbox**）。<br>• "**自动**"。应用程序自动检测对象并将其提交到 Sandbox 进行扫描。<br>• "**组合的**"。应用程序会自动将要扫描的对象发送到 Sandbox。如有需要，用户还可以通过上下文菜单提交单个文件进行扫描。 |
| **连接到 Sandbox 服务器** | `Windows` `Linux` | **Kaspersky Sandbox**。Sandbox 服务器连接设置。服务器使用部署的 Microsoft Windows 操作系统虚拟映像来运行需要扫描的对象。请输入 Sandbox 服务器 IP 地址（IPv4、IPv6 或 DNS）和连接到服务器的端口。<br>**KATA Sandbox**。Central Node 服务器连接设置。Central Node 选择最佳扫描设置并平衡 Sandbox 服务器之间的负载。请输入 Central Node 服务器 IP 地址（IPv4、IPv6 或 DNS）和连接到服务器的端口。 |
| **服务器连接设置** | `Windows` `Linux` | "**服务器连接超时**"。Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）的连接超时。配置的超时时间过后，Kaspersky Endpoint Security 将向下一台服务器发送请求。如果连接速度低或连接不稳定，您可以增加服务器的连接超时。建议的请求超时是 0.5 秒或更少。<br>"**请求队列**"。请求队列文件夹的大小。在发送多个对象以在 Sandbox 中进行扫描时，Kaspersky Endpoint Security 会创建一个请求队列。默认情况下，请求队列文件夹的大小限制为 100 MB。达到最大大小后，Sandbox 停止向队列添加新请求，并将相应的事件发送到 Kaspersky Security Center。您可以根据您的服务器配置来配置请求队列文件夹的大小。<br>"**服务器 TLS 证书**"。要配置与 Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）的受信任连接，您必须准备 TLS 证书。您必须使用策略将证书添加到计算机。您还需要将证书添加到 Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）。<br>**使用双向身份验证**（仅适用于 KATA Sandbox）。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。 |
| **检测到威胁后的操作** | `Windows` `Linux` | "**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。<br>"**运行关键区域扫描**"。如果选择此选项，Kaspersky Endpoint Security 运行*Critical Areas Scan*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。<br>"**创建 IOC 扫描任务**"。如果选择此选项，Kaspersky Endpoint Security 将自动创建 *IOC Scan(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 Scan*任务的其他设置，请转到任务设置。 |
| **IOC 扫描范围** | `Windows` `Linux` | "**关键文件区域**"。如果选择此选项，Kaspersky Endpoint Security 将仅在计算机的重要文件区域（例如选定的用户配置文件目录和关键系统对象）中扫描 IOC。<br>"**计算机系统驱动器上的文件区域**"。如果选择此选项，Kaspersky Endpoint Security 在计算机的系统驱动器上执行 IOC 扫描。<br>无论选择的扫描范围如何，应用程序还会扫描检测到威胁的文件路径中的 IOC。 |
| **运行 IOC 扫描任务** | `Windows` `Linux` | "**手动**"。您可以在方便时手动启动"*IOC Scan*"任务的运行模式。<br>"**自动**"。Kaspersky Endpoint Security 在检测到威胁时自动运行 *IOC 扫描*任务。<br>`Windows` **仅在计算机空闲时运行**。Kaspersky Endpoint Security 在屏幕保护程序处于活动状态或屏幕被锁定时运行 *IOC 扫描*任务。如果用户解锁计算机，Kaspersky Endpoint Security 将暂停任务。这意味着任务可能需要几天才能完成。 |

# 与 KUMA 的整合

适用于 Windows 和 Linux

Kaspersky Endpoint Security 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。

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。

默认情况下，向 KUMA 服务器发送事件是禁用的。为确保 KUMA 正常运行，首先需要在“常规设置 → 遥测设置”部分启用向 KUMA 发送遥测数据的功能。

Kaspersky Endpoint Security 不提供 KUMA 代理的所有功能。应用程序仅向 KUMA 发送不带标记的事件。要访问所有 KUMA 功能，您需要购买授权许可并按照以下说明部署解决方案：KUMA 管理员指南。

KUMA 组件设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **服务器连接设置** | Windows Linux | “**服务器连接超时**”。最大 KUMA 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 KUMA 服务器。<br>“**服务器证书**”。用于与 KUMA 服务器建立受信任连接的 TLS 证书。您可以在 Kaspersky Unified Monitoring and Analysis Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Unified Monitoring and Analysis Platform 中的说明）。<br>“**使用双向身份验证**”。在 Kaspersky Endpoint Security 和 KUMA 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，在 KUMA 控制台的 TCP 连接器设置中，必须选择“**自定义 PFX**”TLS 模式（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助 中的 tcp 类型连接器设置）。然后您必须获取一个加密容器并设置一个密码来保护该加密容器。*加密容器*是带有证书和私钥的 PFX 存档。配置 KUMA 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。<br>加密容器必须受密码保护。无法添加密码为空的加密容器。 |
| **发送事件时的最大延时（秒）** | Windows Linux | 应用程序在同步间隔到期后与服务器同步以发送事件。 |
| **使用 TLS 加密** | Windows Linux | 如果启用此功能，Kaspersky Endpoint Security 将使用 TLS 证书与 KUMA 服务器建立受信任连接。 |
| **连接到 KUMA 服务器** | Windows Linux | KUMA 服务器连接设置。指定连接到服务器的 IP 地址（IPv4 或 IPv6）、连接协议和端口。<br>您可以添加多个 KUMA 服务器地址。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。 |

# Light Agent 模式

## SVM 检测设置

适用于 Windows 和 Linux

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）。因此，SharedCache 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。Integration Server 组件用于解决方案组件和虚拟基础架构之间的交互。*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。

SVM 检测设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **使用 Integration Server** | `Windows` `Linux` | Integration Server 在大规模虚拟基础架构中很有用，因为 Integration Server 可以自动平衡 SVM 之间的负载。<br>输入 Integration Server 连接设置：<br>• 安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。<br>• 用于连接到 Integration Server 的端口号。默认情况下，指定端口为 7271。<br>• Integration Server 管理员的密码（admin 账户密码）。 |
| **使用 SVM 地址的自定义列表** | `Windows` `Linux` | 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)。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>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。 |

# Integration Server 连接设置

适用于 Windows 和 Linux

*Integration Server* 是实现 Kaspersky Security for Virtualization Light Agent 与虚拟基础架构交互的解决方案组件。Integration Server 维护可连接的 SVM 列表。Light Agent 与Integration Server 建立连接并获取 SVM 地址列表。

Integration Server 在大规模虚拟基础架构中很有用，因为 Integration Server 可以自动平衡 SVM 之间的负载。Integration Server 获取有关可用 SVM 的信息，对其进行分析并向 Light Agent 提供最适合连接的 Protection Server (SVM) 列表。

Integration Server 连接设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **地址** | `Windows` `Linux` | Integration Server 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。<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** | `Windows` `Linux` | 用于连接到 Integration Server 的端口号。<br>默认情况下，指定端口为 7271。 |
| **Integration Server 上的身份验证** | `Windows` `Linux` | Integration Server 管理员的密码（`admin` 账户密码）。<br>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 连接标签

适用于 Windows 和 Linux

多个 Light Agent 可以连接到一个 SVM。要平衡 Light Agent 连接，您可以在 SVM 发现设置区域中指定单独的 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。

选择“**使用连接标签**”复选框，即可使用标签将 Light Agent 连接到 SVM。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。

## SVM 选择算法

适用于 Windows 和 Linux

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 选择算法设置

| 设置 | OS | 描述 |
| --- | --- | --- |
| **使用标准 SVM 选择算法** | `Windows` `Linux` | 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。为了将 SVM 标识为本地，Light Agent 主要使用 SVM 在虚拟基础架构中的位置。如果 SVM 与 Light Agent 位于同一个 Hypervisor 中，则 Light Agent 会将此类 SVM 视为本地 SVM。在某些虚拟基础架构中，您必须使用配置文件手动指定本地 SVM。<br><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。 |
| **使用扩展 SVM 选择算法** | `Windows` `Linux` | 扩展算法允许您手动指定本地 SVM 选择标准或禁用本地 SVM 发现。为此，您需要选择虚拟基础架构中的 SVM 路径：Hypervisor、集群或数据中心。也就是说，您必须选择要发现本地 SVM 的范围。如果 Light Agent 无法连接到配置的发现范围内的本地 SVM，它将停止尝试连接。<br>扩展算法还允许禁用 Light Agent 的本地 SVM 发现。这种情况下，Light Agent 会选择整个虚拟基础架构中连接的 Light Agent 数量最少的 SVM。 |

## 保护连接

适用于 Windows 和 Linux

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影响 Kaspersky Security for Virtualization Light Agent 的性能。

# 附录 6.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。

| 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。 |
| 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><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。 |

# 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。

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/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 | – |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 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。 |
| 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 | – |
| 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。 |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 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`<br>• `/tmp/*`<br>对 /tmp 和 /tmp/* 挂载点的排除适用于 10.0 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 | – |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 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 | – |
| 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。 |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 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<br>• /tmp/*<br>对 /tmp 和 /tmp/* 挂载点的排除适用于 10.0 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 |
| 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 | – |

| 应用程序组件 | 建议的组件状态 | 建议 |
| --- | --- | --- |
| 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 | – |

# 有关 Kaspersky Endpoint Security 的信息来源

## 知识库中的 Kaspersky Endpoint Security 页面

*知识库*是技术支持网站的一部分。

在知识库中的 Kaspersky Endpoint Security 页面，您可以阅读提供有关如何购买、安装和使用该应用程序的有用信息、建议和常见问题解答的文章。

知识库中的文章可能提供关于 Kaspersky Endpoint Security 和其他卡巴斯基应用程序的问题的答案。知识库中的文章也可能包含技术支持新闻。

## 在论坛上讨论卡巴斯基应用程序

如果您的问题不需要紧急回答，您可以在我们的论坛中与卡巴斯基专家和其他用户一起进行讨论。

在论坛上，您可以查看现有主题、发表自己的评论以及创建新的讨论主题。

# 术语表

## Integration Server

Kaspersky Endpoint Security for Virtualization Light Agent 组件。在 Kaspersky Endpoint Security 组件和虚拟基础架构之间交互。

## Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent 组件。它安装在需要保护的每个虚拟机上。

## SIEM 系统

安全信息和事件管理系统。用于管理组织安全系统中的信息和事件的解决方案。

## SVM

安全虚拟机 – 安装了扫描服务器服务（保护虚拟机，即 Kaspersky Endpoint Security for Virtualization Light Agent 的组件）的特殊虚拟机。

## 代理服务器

允许用户对其他网络服务发起间接请求的一种计算机网络服务。首先，用户连接到代理服务器并请求获取位于另一台服务器上的资源（例如文件）。然后，代理服务器要么连接到指定的服务器并从中获取该资源，要么从其自己的缓存中（如果代理具有自己的缓存）返回该资源。在某些情况下，出于某种目的，代理服务器可能会修改用户的请求或服务器的响应。

## 卡巴斯基更新服务器

卡巴斯基 HTTP 和 FTP 服务器，卡巴斯基应用程序从中下载数据库和应用程序模块更新。

## 反加密

勒索软件的恶意活动旨在加密包含用户数据的文件。这样加密的文件无法被读取或使用。

## 受信任设备

在受信任设备设置下列出，可供用户随时完整访问的设备。

## 受感染的对象

包含与某个已知恶意软件代码部分完全匹配的部分代码的对象。卡巴斯基专家不推荐访问此类对象。

## 可疑网址的数据库

其内容被视为存在危险的网址列表。这是一个由 Kaspersky 专家创建的列表。它会定期更新，并且会包含在 Kaspersky 应用程序分发包中。

## 启动对象

计算机上安装的操作系统和软件正常启动和运行所需的一组应用程序。每次启动操作系统时，都会执行这些对象。有些病毒专门感染此类对象，例如，可能会导致操作系统无法启动。

## 备用密钥

允许用户使用该程序但当前未使用的密钥。

## 应用程序数据库

包含在数据库发布之时，卡巴斯基已知的计算机安全威胁信息的数据库。应用程序数据库由卡巴斯基专家创建并且每小时都会更新。

## 应用程序设置

对所有任务类型通用并且管辖应用程序总体操作情况的应用程序设置，例如应用程序性能设置、报告设置和备份设置。

## 授权许可

根据最终用户授权许可协议授予的在有限时间内使用本应用程序的权限。

## 授权许可证书

与密钥文件或激活码一起由 Kaspersky 传输给用户的文档。该文档包含授予用户的授权许可信息。

## 排除

*排除项*是从卡巴斯基应用程序扫描中排除的对象。您可以根据病毒百科全书的分类，按名称从扫描文件中排除某些格式、文件掩码、特定区域（例如文件夹或应用程序）、应用程序进程或对象。可以为每个任务分配一组排除项。

## 文件掩码

使用通配符表示文件名。文件掩码中使用的标准通配符为 * 和 ?，其中 * 代表任意数量的任意字符，? 代表单个任意字符。

## 活动密钥

程序当前正在使用的密钥。

## 活动策略

应用程序当前用于控制数据泄漏的策略。应用程序可以同时使用多个策略。

## 清除

能够完全或部分恢复对象数据的一种处理已感染对象的处理方法。并非所有受感染的对象都能被杀毒。

## 激活应用程序

将应用程序切换到全功能模式。应用程序激活在应用程序安装期间或之后执行。您需要提供激活码或密钥文件才能激活应用程序。

## 策略

在管理组内，策略决定应用程序的设置并管理对设备上安装的应用程序的配置的访问。必须为每个应用程序创建单独策略。您可以在每个管理组内为设备上安装的应用程序创建无限数量的不同策略，但在一个管理组内一次只能对每个应用程序应用一个策略。

## 管理服务器

Kaspersky Security Center 的一个组件，可集中存储公司网络内安装的所有卡巴斯基应用程序的信息。它也可用于管理这些应用程序。

## 管理组

根据设备执行的功能和安装在其上的卡巴斯基应用程序集合，在 Kaspersky Security Center 内分组在一起的一组设备。由于设备组可以作为单个实体进行管理，因此我们对设备进行分组以便简化管理。一个管理组可以包含其他组。对于管理组中已安装的每个应用程序，都可以创建组策略和组任务。

## 组任务

分配给管理组并在此管理组中包括的所有受管理设备上执行的任务。

## 组策略

请参阅策略。

## 订阅

以选定设置（到期日期和设备数量）启用应用程序。您可以暂停或继续订阅、自动续订或取消订阅。

## 误报

卡巴斯基应用程序将非感染对象认为是受感染的情况，因为该对象的代码类似于病毒的代码。

## 钓鱼网页地址数据库

Kaspersky 专家确定的与钓鱼有关的网址列表。该数据库会定期更新，并且会包含在 Kaspersky 应用程序分发包中。

# 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。

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。

Mac 和 FireWire 是 Apple Inc. 的商标。

Arm 是 Arm Limited（或其子公司）在美国和/或其他地区的注册商标。

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、Google Public DNS 是 Google LLC 的商标。

HUAWEI、EulerOS 和 FusionSphere 是华为技术有限公司的商标。

Intel、Core 是 Intel Corporation 或其子公司的商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft、Active Directory、Hyper-V、Outlook、Visual C++ 和 Windows 是 Microsoft 公司集团的商标。

OpenStack 是 OpenStack Foundation 在美国和其他国家/地区的注册商标。

Oracle 和 JavaScript 是 Oracle 和/或其附属公司的注册商标。

Python 是 Python Software Foundation 的商标或注册商标。

Red Hat、Red Hat Enterprise Linux、CentOS、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

SUSE 是 SUSE LLC 在美国和其他国家/地区的注册商标。

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。