kaspersky

Kaspersky Industrial CyberSecurity for Nodes 4.5

© 2026 AO Kaspersky Lab

目录

Kaspersky Industrial CyberSecurity for Nodes
- 新功能
- 分发包
- 软件和硬件要求
- 支持的 Kaspersky Security Center 版本
- 卡巴斯基病毒清除工具
- 功能要求和限制
  - 安装和删除程序
  - 系统完整性监控
  - 防火墙
  - 对过时 Windows 版本的限制
  - 与 Kaspersky Security Center 集成
  - 其他限制
- 典型部署
- 与其他应用程序的兼容性

安装和删除程序
- 安装计划
  - 选择管理工具
  - 选择安装类型
- 使用向导安装和卸载应用程序
  - 使用安装向导安装
    - Kaspersky Industrial CyberSecurity for Nodes 安装
    - Kaspersky Industrial CyberSecurity for Nodes 控制台安装
    - 在其他设备上安装应用程序控制台以后的高级设置
    - 在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作
      - 启动并配置“数据库和应用程序模块更新”任务
      - 关键区域扫描
  - 修改组件集和修复 Kaspersky Industrial CyberSecurity for Nodes
  - 使用安装向导卸载
    - Kaspersky Industrial CyberSecurity for Nodes 卸载
    - Kaspersky Industrial CyberSecurity for Nodes 控制台卸载
- 从命令行安装和卸载应用程序
  - 关于从命令行安装和卸载 Kaspersky Industrial CyberSecurity for Nodes
  - 适用于 Windows Installer 服务的 Kaspersky Industrial CyberSecurity for Nodes 软件组件代码
    - Kaspersky Industrial CyberSecurity for Nodes 软件组件
    - “管理工具”软件组件
  - 安装和恢复设置，以及 Windows 安装程序命令行选项
  - 安装 Kaspersky Industrial CyberSecurity for Nodes 的命令示例
  - 在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作
  - 添加/删除组件。命令示例
  - Kaspersky Industrial CyberSecurity for Nodes 卸载。命令示例
  - 返回代码

使用 Kaspersky Security Center 安装和卸载应用程序
有关通过 Kaspersky Security Center 安装的常规信息
安装或卸载 Kaspersky Industrial CyberSecurity for Nodes 的权限
通过 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Nodes
在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作
通过 Kaspersky Security Center 安装应用程序控制台
通过 Kaspersky Security Center 卸载 Kaspersky Industrial CyberSecurity for Nodes
使用 Kaspersky Security Center 更改应用程序组件集
通过 Active Directory 组策略安装和卸载应用程序
通过 Active Directory 组策略安装 Kaspersky Industrial CyberSecurity for Nodes
在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作
通过 Active Directory 组策略卸载 Kaspersky Industrial CyberSecurity for Nodes
Kaspersky Industrial CyberSecurity for Nodes 安装和卸载日志
Kaspersky Industrial CyberSecurity for Nodes 安装后的系统更改
Kaspersky Industrial CyberSecurity for Nodes 进程
检查 Kaspersky Industrial CyberSecurity for Nodes 功能。使用 EICAR 测试病毒
关于 EICAR 测试病毒
检查实时文件保护和按需扫描功能
将旧版本的 Kaspersky Industrial CyberSecurity for Nodes 升级至 4.5 版
更新 Kaspersky Industrial CyberSecurity for Nodes
更新 Kaspersky Industrial CyberSecurity for Nodes 管理工具
迁移策略和任务
正在更新的应用程序版本的设置迁移
Kaspersky Industrial CyberSecurity for Nodes 版本 4.0 和 4.5 中的组件和任务对应关系
安装和删除 Kaspersky Security Gateway
更新 Kaspersky Security Gateway
使用安装向导安装 Kaspersky Security Gateway
步骤 1. 验证安装要求
步骤 2. 安装程序的欢迎页面
步骤 3. 查看最终用户授权许可协议和隐私策略
步骤 4. 选择目标文件夹
步骤 5. 选择组件
步骤 6. 配置与 SCADA 系统的连接
步骤 7. 安装 Kaspersky Security Gateway
从命令行安装 Kaspersky Security Gateway
删除 Kaspersky Security Gateway
步骤 1. 保存 Kaspersky Security Gateway 数据以供将来使用
步骤 2. 删除 Kaspersky Security Gateway
程序界面
使用管理插件
从 Kaspersky Security Center 管理 Kaspersky Industrial CyberSecurity for Nodes
管理应用程序设置
导航
在应用程序属性窗口中打开常规设置
通过策略打开常规设置

在 Kaspersky Security Center 中配置常规应用程序设置
在 Kaspersky Security Center 中配置界面和扫描设置
在 Kaspersky Security Center 中配置安全性设置
使用 Kaspersky Security Center 配置连接设置
配置本地任务的计划启动
在 Kaspersky Security Center 中配置隔离和备份设置
创建和配置策略
创建策略
配置策略
使用 Kaspersky Security Center 创建和配置任务
关于 Kaspersky Security Center 中的任务创建
使用 Kaspersky Security Center 创建任务
转至单台计算机的本地任务设置和常规应用程序设置
在 Kaspersky Security Center 中配置组任务
应用程序激活任务
更新任务
应用程序完整性控制
管理任务计划
计划任务
启用和禁用计划任务
Kaspersky Security Center 中的报告
使用 Kaspersky Industrial CyberSecurity for Nodes 控制台
启动应用程序控制台
Kaspersky Industrial CyberSecurity for Nodes 控制台界面
Kaspersky Industrial CyberSecurity for Nodes 控制台窗口
通知区域中的系统托盘图标
通过应用程序控制台配置常规设置
管理 Kaspersky Industrial CyberSecurity for Nodes 任务
Kaspersky Industrial CyberSecurity for Nodes 任务类别
手动启动、暂停、恢复和停止任务
管理任务计划
配置任务计划设置
启用和禁用计划任务
使用用户账户启动任务
关于使用账户启动任务
指定用户账户以启动任务
导入和导出设置
关于导入和导出设置
导出设置
导入设置
查看保护状态和 Kaspersky Industrial CyberSecurity for Nodes 信息
从 Web Console 使用 Web 插件
从 Web Console 管理 Kaspersky Industrial CyberSecurity for Nodes
Web 插件限制

管理应用程序设置
在 Web 插件中配置常规应用程序设置
在 Web 插件中配置界面和扫描设置
在 Web 插件中配置安全和可靠性设置
在 Web 插件中配置连接设置
在 Web 插件中配置本地任务的计划启动
在 Web 插件中配置隔离和备份设置
创建和配置策略
使用 Kaspersky Security Center 创建和配置任务
关于 Web 插件中的任务创建
在 Web 插件中创建任务
在 Web 插件中配置组任务
在 Web 插件中配置应用程序激活任务
在 Web 插件中配置更新任务
管理任务计划
计划任务
启用和禁用计划任务
Kaspersky Security Center 中的报告
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
关于密钥
关于密钥文件
关于激活码
使用密钥文件激活应用程序
使用激活码激活应用程序
查看有关当前授权许可的信息
续订授权许可
删除密钥
关于数据提供
与欧盟立法兼容(GDPR)
启动和停止 Kaspersky Industrial CyberSecurity for Nodes
启动和停止应用程序
暂停和恢复计算机保护和控制
小型诊断窗口
关于小型诊断窗口
通过小型诊断窗口查看 Kaspersky Industrial CyberSecurity for Nodes 状态
查看安全事件统计
查看当前应用程序活动
配置应用程序跟踪和内存转储记录
Kaspersky Industrial CyberSecurity for Nodes 自我保护
启用和禁用自我防御
对 AM-PPL 技术的支持
保护操作系统服务
配置用户权限以管理 Kaspersky Industrial CyberSecurity for Nodes
配置管理 Kaspersky Security 服务的用户权限

对 Kaspersky Industrial CyberSecurity for Nodes 功能进行受密码保护的访问
安全桌面通知
信任区域
创建扫描排除项
选择可检测对象的类型
编辑受信任应用程序列表
创建本地受信任区域
导出和导入受信任域
使用受信任的系统证书存储
关于工业软件排除项配置文件
实时文件保护
关于任务保护范围和安全设置
预定义的保护范围
关于预定义安全级别
“实时文件保护”组件默认扫描的文件扩展名
配置“实时文件保护”组件
配置“实时文件保护”组件的保护范围
手动配置安全性设置
容器扫描
KSN 使用
启用卡巴斯基安全网络的使用
卡巴斯基安全网络使用统计信息
卡巴斯基私有安全网络的限制
KSN 代理设置
漏洞利用防御
漏洞利用防御模式
启用和禁用漏洞利用防御
启用和禁用内存保护
创建受保护进程列表
修复引擎
反加密
启用和禁用本地文件夹的加密保护
防止共享文件夹被外部加密
启用和禁用共享文件夹对外部加密的防护
创建保护范围
添加受信任的计算机以进行外部数据加密
配置不受信任的计算机的阻止期限
从共享文件夹对外部加密的防护中导出和导入排除项列表
网络威胁防护
AMSI 扫描程序
启用和禁用 AMSI 扫描程序
AMSI 扫描程序设置
应用程序启动控制
关于应用程序启动控制规则
关于软件分发控制
关于应用程序启动控制规则生成器
启用并配置应用程序启动控制

- 配置软件分发控制
- 使用应用程序启动控制规则
  - 添加应用程序启动控制规则
  - 为应用程序启动控制规则添加触发条件
  - 从应用程序启动控制规则范围添加排除项
  - 启用默认允许模式
  - 生成包含 Kaspersky Security Center 阻止的应用程序事件的 TXT 文件
- 配置“应用程序启动控制规则生成器”组任务
- 使用“应用程序启动控制规则生成器”组任务创建规则。
- 设备控制
  - 设备访问规则
  - 按类型进行设备访问控制
  - Wi-Fi 连接控制
  - 打印控制
  - 输入设备控制 (HID)
  - 监控可移动驱动器的使用
  - 管理对蓝牙设备的访问
  - 区分用户对设备的访问权限
  - 外部设备审计
  - 添加受信任设备
  - 导出和导入受信任设备的列表
- 防火墙
  - 关于防火墙规则
  - 配置防火墙
    - 配置常规防火墙设置
    - 创建和配置防火墙规则
    - 启用和禁用防火墙规则
- BadUSB 攻击防护
- 系统完整性监控
  - 关于系统完整性监控规则
  - 实时系统完整性监控
  - 按需系统完整性检查
  - 导出和导入系统完整性监控规则
  - 查看系统完整性监控报告
- 日志审查
  - 添加自定义规则
  - 配置预定义规则
- 性能分析器
- 按需扫描
  - 关于按需扫描任务
  - 关于任务扫描范围和安全设置
  - 预定义的扫描范围
  - 在线存储文件扫描
  - 关于预定义安全级别
  - 可移动驱动器扫描
  - 默认按需扫描任务设置

管理按需扫描任务
导航
打开按需扫描任务向导
打开按需扫描任务设置
创建按需扫描任务
在后台运行按需扫描任务
记录关键区域扫描执行
在按需扫描任务中配置扫描范围
配置按需扫描任务设置
配置可移动驱动器扫描
为按需扫描任务选择预定义的安全级别
手动配置安全性设置
按需扫描任务统计
工业网络保护
关于PLC 项目完整性检查
配置 PLC 项目完整性检查任务
配置 PLC 项目调查
配置 PLC 项目完整性检查
启用和禁用 PLC 项目完整性检查
关于 PLC 配置注册表
配置 PLC 注册表
便携式扫描程序
创建便携式扫描程序的要求
创建便携式扫描程序
启动便携式扫描程序
更新便携式扫描程序数据库
查看便携式扫描程序结果
从 Rutoken 可移动驱动器导出便携式扫描程序结果
查看常规扫描报告
安全审计
安全审计任务设置的限制
支持的 OVAL 扫描类型
管理安全审计任务
使用默认设置创建和配置安全审计任务
使用用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库配置安全审计任务设置
使用安全和标准合规性配置来配置安全审计任务设置
使用来自 Kaspersky Security Center 存储库的自定义规则数据库配置安全审计任务设置
使用文件中的自定义数据库配置安全审计任务设置
查看安全审计任务执行结果
将安全审计任务执行结果导出到单独的文件
创建用于使用 OVAL 或 XCCDF 规则签名文件的证书指纹
使用自定义 OVAL 或 XCCDF 规则创建 Kaspersky Security Center 安装包
使用命令行配置和启动安全审计任务
使用 Kaspersky Security Gateway
诊断信息
Kaspersky Security Gateway 的限制和已知问题
Kaspersky Security Gateway 控制台界面

- 配置与 Kaspersky Security Center 的连接
- 配置与 Kaspersky Industrial CyberSecurity for Networks 的连接
- 配置 DCOM 协议
- 使用通信协议配置数据传输设置
  - 使用 IEC 60870-5-104 协议配置数据传输
  - 使用 OPC DA 协议配置数据传输
  - 使用 OPC UA 协议配置数据传输
  - 使用配置文件配置数据传输
- 配置 Kaspersky Security Gateway 附加设置
- 查看 Kaspersky Security Gateway 事件

BitLocker 完整磁盘加密管理
- 启动 BitLocker 驱动器加密
- 解密受 BitLocker 保护的硬盘驱动器
- 恢复对 BitLocker 保护的驱动器的访问权限
- 暂停 BitLocker 保护以更新软件

Kaspersky Industrial CyberSecurity for Nodes 数据库和软件模块更新
- 更新数据库和应用程序模块
- 关于更新任务
- Kaspersky Industrial CyberSecurity for Nodes 数据库和模块更新方案
- 配置更新任务
- 应用程序的 SMU 更新
- 回滚 Kaspersky Industrial CyberSecurity for Nodes 数据库更新
- 更新任务统计

Detection and Response 解决方案
- Kaspersky Endpoint Agent
  - 迁移 [KICS+KEA] 配置到 [KICS+内置代理] 配置
  - 将 [KICS+KEA] 配置的策略和任务迁移到 [KICS+内置代理] 配置
  - 端点代理配置
    - 安装端点代理配置
    - 与第三方 EPP 应用程序的兼容性
- Managed Detection and Response
  - 配置 MDR 集成
- Kaspersky Endpoint Detection and Response Optimum
  - 内置代理与 EDR Optimum 的集成
  - 扫描入侵指标 (IOC)
    - IOC 文件需求
    - IOC 扫描的扩展遥测
    - 注册表中的 IOC 扫描范围 (RegistryItem)
  - 移动文件到隔离区
  - 获取文件
  - 删除文件
  - 进程启动
  - 终止进程
  - 执行防护
  - 计算机网络隔离
  - Cloud Sandbox
  - 授权 EDR Optimum

- Endpoint Detection and Response Expert (on-premise)
  - 配置 EDR Expert (on-premise) 集成
  - 配置 EDR Expert (on-premise) 遥测设置
  - EDR Expert (on-premise) 遥测排除项
  - 导出和导入 EDR Expert (on-premise) 事件过滤器
  - YARA 扫描
- Kaspersky Anti Targeted Attack Platform
  - 配置 KATA 集成
  - 配置遥测
- EDR 遥测排除项
- 与 Kaspersky Industrial CyberSecurity for Networks 集成
- 监控 EDR 操作

与 SIEM 集成
- 过滤要发送到 SIEM 的事件
- 导出和导入遥测事件过滤规则

使用 Sigma 规则进行异常检测
- 使用 Sigma 规则进行异常检测的特殊考虑和限制
- 使用 Sigma 规则启用异常检测
- 添加 Sigma 规则集合
- 更改 Sigma 规则集合的状态
- 将 Sigma 规则添加到自定义集合
- 用户账户控制
- 导出和导入自定义集合的 Sigma 规则
- 更改 Sigma 规则
- Sigma 规则中的排除项
- 在规则集合内过滤 Sigma 规则
- 在命令行中使用 Sigma 规则配置异常检测

对象隔离和备份
- 隔离可能已感染对象。隔离
  - 查看隔离对象
    - 排序隔离的对象
    - 筛选隔离的对象
  - 还原已隔离的对象
  - 从隔离删除对象
  - 发送疑似感染对象到 Kaspersky 以供分析
  - 配置隔离设置
- 制作对象的备份副本。备份
  - 查看备份中的对象
    - 排序备份中的文件
    - 筛选备份中的文件
  - 从备份还原文件
  - 从备份删除文件
  - 配置备份设置
  - 备份统计
- 阻止访问网络资源。被阻止的网络会话
  - 被阻止的网络会话列表
  - 管理被阻止的网络会话列表

事件注册。Kaspersky Industrial CyberSecurity for Nodes 日志
注册 Kaspersky Industrial CyberSecurity for Nodes 事件的方式
配置日志设置
对日志中的事件进行排序
过滤日志中的事件
从日志中删除事件
导出日志中的信息
系统审核日志
任务日志
在任务日志中查看有关 Kaspersky Industrial CyberSecurity for Nodes 任务的统计和信息
在事件查看器中查看 Kaspersky Industrial CyberSecurity for Nodes 事件日志
管理员和用户通知方式
配置管理员和用户通知
配置电子邮件通知
配置与管理服务器的交互
配置事故生成
联系技术支持
如何获取技术支持
通过 Kaspersky CompanyAccount 获取技术支持
向技术支持专家提供扩展诊断信息
应用程序操作跟踪
记录内存转储
有关 Kaspersky Industrial CyberSecurity for Nodes 的信息来源
术语表
事件重要性
任务
任务设置
保护状态
卡巴斯基安全网络 (KSN)
反病毒数据库
受感染的对象
可感染的文件
启动对象
启发式分析
备份
存档
安全信息与事件管理（SIEM）
安全级别
实时保护
对象链接与嵌入（OLE）对象
授权许可期限
文件掩码
更新
本地任务
活动密钥
清除
漏洞

- 策略
- 管理服务器
- 误报
- 隔离

有关第三方代码的信息

商标通知

附录

- 用于快速扫描的文件扩展名
- 应用程序组件规则中的用户账户

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Nodes 是一款针对工业控制系统中 IT 威胁的全面的服务器和工作站安全解决方案。

该应用程序控制工业企业网络计算机的运行，并使用以下组件、功能和技术：

- “**应用程序启动控制**”。该组件监控用户应用程序的启动并规范应用程序的启动。
- “**设备控制**”。该组件可控制外部设备的注册和使用，以便保护计算机在与通过 USB 连接的闪存驱动器或其他类型的外部设备交换文件时，免受可能产生的计算机安全威胁。
- “**PLC 项目完整性检查**”。此功能用于检查工业系统中使用的可编程逻辑控制器 (PLC) 项目的完整性。

控制组件的运行基于规则，例如：

- 应用程序启动控制使用应用程序启动控制规则。
- 设备控制使用设备访问规则和连接器总线访问规则。
- PLC 项目完整性检查功能使用 PLC 项目完整性检查规则。

每种类型的威胁均由单独的组件应对。可以独立启动和停止组件以及调整其设置。

应用程序使用以下组件检查和保护工业网络组件：

- **实时文件保护**。该组件可防止计算机的文件系统受到感染。该组件在 Kaspersky Industrial CyberSecurity for Nodes 启动时启动，并在计算机的 RAM 中持续运行，并检查计算机和所有已挂载驱动器上所有打开、保存和启动的文件。实时文件保护观察每个文件事件并检查该文件是否存在病毒和其他构成威胁的程序。
- “**Wi-Fi 控制**”。该组件跟踪受保护设备连接 Wi-Fi 网络的尝试，并阻止或允许连接到检测到的网络。
- “**防火墙**”。根据其模式，该组件：监控 Windows 防火墙的流量过滤；仅在组件的日志中记录有关受保护计算机的网络活动事件；或根据防火墙设置过滤网络流量。
- **反加密**。该组件可以检测从公司网络上的远程计算机对受保护设备的网络文件资源进行的恶意加密。
- **便携式扫描程序**。该组件检查隔离的设备并执行安全检查。
- “**BadUSB 攻击防护**”。该组件可以防止受感染的模拟键盘的 USB 设备连接至计算机。
- “**文件完整性监控**”。Kaspersky Industrial CyberSecurity for Nodes 可以检测任务设置中指定的监控范围内的文件更改。这些更改可能表示受保护设备遭到安全入侵。
- **注册表访问监控**。此组件可以监控使用任务设置中定义的监控范围内的特定注册表分支和注册表项执行的操作。
- “**日志审查**”。此组件根据 Windows 事件日志的审查结果，对受保护环境的完整性进行监控。

除了组件提供的实时保护之外，我们还建议定期扫描计算机以检查病毒和其他可能构成威胁的应用程序。这样做是为了防止任何未被组件检测到的恶意软件的传播，例如由于设置中的保护级别较低或其他原因。

为了使 Kaspersky Industrial CyberSecurity for Nodes 正常运行，应更新程序运行期间使用的数据库和软件模块。默认情况下，应用程序会自动更新，但如果需要，您可以手动更新应用程序数据库和模块。

以下任务用于保护计算机：

- "**全盘扫描**"。Kaspersky Industrial CyberSecurity for Nodes 仔细检查操作系统，包括系统内存、操作系统启动时启动的任何对象、操作系统的备份以及所有硬盘和可移动驱动器。
- **自定义扫描**。Kaspersky Industrial CyberSecurity for Nodes 扫描用户选择的对象。
- "**关键区域扫描**"。Kaspersky Industrial CyberSecurity for Nodes 扫描操作系统启动时加载的对象、位于系统内存中的对象或可能包含 rootkit 的对象。
- **更新**。Kaspersky Industrial CyberSecurity for Nodes 下载应用程序数据库和模块更新。更新可以帮助计算机保持最新的防护，抵御病毒和其他构成威胁的程序。

通过 Kaspersky Security Center 进行远程访问

Kaspersky Security Center 允许在客户端计算机上远程启动和停止 Kaspersky Industrial CyberSecurity for Nodes、管理任务以及调整程序设置。

应用程序实用工具

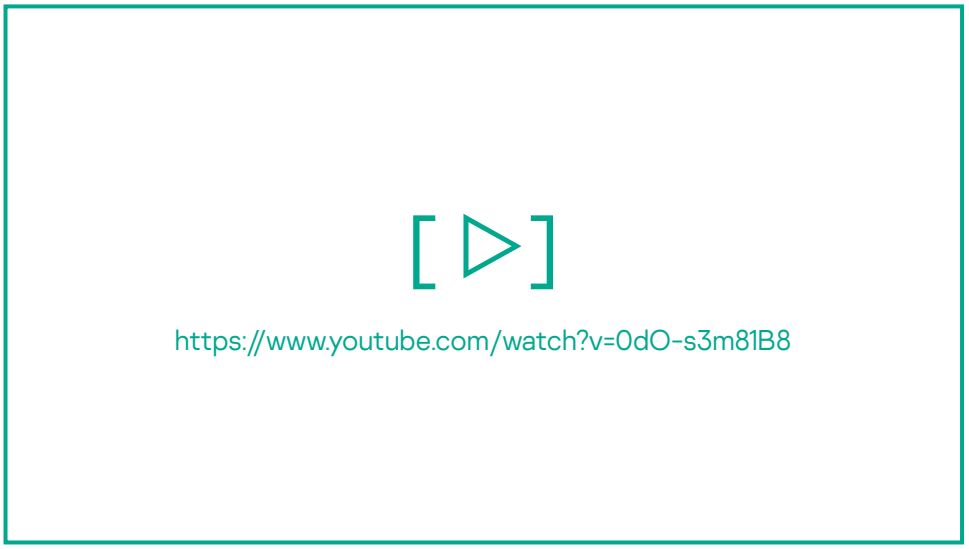
Kaspersky Industrial CyberSecurity for Nodes 包含一系列实用程序。实用工具旨在使应用程序保持最新状态并扩展应用程序提供帮助的能力。

- **日志**。应用程序运行期间，每个组件和任务的活动都记录在日志中。日志是 Kaspersky Industrial CyberSecurity for Nodes 运行期间发生的事件以及应用程序执行的所有操作的列表。如果出现问题，日志可能会被发送到卡巴斯基供技术支持专家进行分析。
- **存储**。如果在扫描病毒和其他构成威胁的程序期间，应用程序检测到计算机上有受感染或可能被感染的文件，它会阻止该文件。可能被感染的文件将被 Kaspersky Industrial CyberSecurity for Nodes 转移到隔离区，一个专门的存储。Kaspersky Industrial CyberSecurity for Nodes 将已消毒和删除的文件的副本保存到备份中。Kaspersky Industrial CyberSecurity for Nodes 将因任何原因未被处理的文件放置在未处理文件列表中。您可以扫描文件、将文件恢复到原始文件夹、手动隔离文件以及清除数据存储。
- **通知**。通知服务允许用户了解事件、计算机的当前状态以及 Kaspersky Industrial CyberSecurity for Nodes 的运行情况。通知可能会显示在屏幕上或通过电子邮件发送。
- **卡巴斯基安全网络**。用户参与卡巴斯基安全网络(KSN)可以允许系统实时接收来自世界各地用户的文件信誉、网络资源和软件信息，从而提高计算机保护能力。
- **漏洞利用防御**。您可以使用注入进程的保护代理来保护进程内存免受漏洞利用。
- **被阻止的网络会话列表**。如果检测到任何恶意的活动，您可以阻止尝试访问计算机共享网络文件夹的网络会话。
- **受信任区域**。您可以从保护或扫描范围中创建一个排除项列表，Kaspersky Industrial CyberSecurity for Nodes 将在按需扫描和实时文件保护任务以及其他任务中默认使用该排除项列表（如果您在排除项设置中指定了这些排除项）。
- **支持**。所有注册的 Kaspersky Industrial CyberSecurity for Nodes 用户都可以访问应用程序数据库和模块更新，并可以通过电子邮件与卡巴斯基技术支持专家就与应用程序的安装、配置和使用相关的任何问题进行咨询。

新功能

观看视频以了解 Kaspersky Industrial CyberSecurity for Nodes 4.5 的新功能。

目前，该视频仅提供英语版本。



以下新功能和改进已在 Kaspersky Industrial CyberSecurity for Nodes 4.5 中实现：

- 显著更新了应用程序控制台的用户界面以及使用 Kaspersky Security Center 管理应用程序的插件。
- 支持 Windows 11 24H2。
- 现在，您可以更改应用程序控制台用于连接安装了该应用程序的计算机的端口。
- 在“*受信任区域*”，您可以：
  - 在安装应用程序和使用 Kaspersky Security Center 创建应用程序管理策略时，编辑工业应用程序的排除项配置文件。
  - 以更精细的方式配置受信任进程。
  - 使用受信任证书存储。
- 用于管理应用程序的用户和组权限的新设置。
- 新的 *Anti-Rootkit* 组件。默认情况下，如果“实时文件保护”已启用，则组件被启用。您可以在安装应用程序时禁用该组件，使用“更改 Kaspersky Industrial CyberSecurity for Nodes 的应用程序组件”任务，或者在应用程序安装包的属性中。
- 在“*漏洞利用防御*”设置中，应用程序现在可以自动识别受保护的进程。
- 新的“*修复引擎*”组件。
- “*反加密*”组件监控共享文件夹以及本地文件夹。

- 重新设计的“*应用程序启动控制*”组件：
  - 组件设置结构中的重大变化。
  - 要指定应用程序启动控制规则触发条件和排除项，您现在可以使用驱动器类型、KL 类别、KSN 组。
- 重新设计的“*设备控制*”组件：
  - 默认情况下，“*设备控制*”组件配置为允许所有设备的连接。
  - “*Wi-Fi 控制*”不再是一个单独的组件，而是“设备控制”的一部分。
  - 增加了根据连接总线控制连接设备的可能性。
  - 添加了从应用程序的先前版本升级到 4.3 版本时对可移动驱动器的访问设置的迁移。
- “*防火墙管理*”组件已重新设计为“*防火墙*”组件，除了与 Windows 防火墙交互之外，现在还可以充当防火墙。
- “*文件完整性监控*”和”*注册表访问监控*”组件的功能已合并到新的”*系统完整性监控*“组件。这一改进使您能够有效地跟踪文件系统和 Windows 注册表中的更改，从而增强对未经授权的数据修改的保护。
- Kaspersky Endpoint Agent 功能现已集成到应用程序中，作为内置端点代理（Detection and Response）。
- 发送到 SIEM 的事件配置已经扩展。现在，Kaspersky Industrial CyberSecurity for Nodes 支持发送 Windows 事件日志事件。
- 应用程序不支持计划单个组件。如果启用这些组件，它们会在应用程序运行时继续运行。
- 现在支持 Kaspersky Security Center 15.1。
- 新增组任务：
  - 要实现 Kaspersky Endpoint Agent 的功能：安全审计、运行进程、终止进程、 IOC 扫描、获取文件、将文件移动到隔离区、删除文件。
  - 其他任务：
    - 管理服务器连接保护
    - 更改 Kaspersky Industrial CyberSecurity for Nodes 组件
    - 基线系统完整性监控而不是基线文件完整性监控
    - 更新而不是复制更新、应用程序数据库更新和软件模块更新
    - 更新回滚而不是应用程序数据库更新回滚
    - 删除密钥
- 发送到 Kaspersky Industrial CyberSecurity for Networks 的 L2 级网络通信事件现在包括流量通过的网络接口的 IPv4 地址（adapter.address 字段）。

- 有助于与 Kaspersky Industrial CyberSecurity for Networks 解决方案的集成。从 4.5 版本的 Kaspersky Industrial CyberSecurity for Networks 开始，以下类型的配置受支持：
  - ARP 表
  - 路由表
  - 密码策略
  - 安全审计策略
  - 扩展审计策略
- Kaspersky Industrial CyberSecurity for Networks 集成设置现在允许为主机的应用程序和网络接口配置混杂模式，从而允许将扩展遥测数据发送到 Kaspersky Industrial CyberSecurity for Networks。
- 现在可以将共享文件夹和连接到本地主机的设备上的文件操作（读取、写入、删除）的信息发送到 Kaspersky Industrial CyberSecurity for Networks 服务器。要获取有关文件操作的信息，您需要一组相应的 Sigma 规则。Kaspersky Industrial CyberSecurity for Networks 可以使用收到的信息来检测在运行 Kaspersky Industrial CyberSecurity for Nodes 的计算机的网络共享之间复制的文件的实例，或从网络共享复制到连接到运行 Kaspersky Industrial CyberSecurity for Nodes 的计算机的设备的文件的实例。
- 在 Kaspersky Security Center Web Console 中，在安装应用程序的主机的属性中，在 Detection and Response 部分，您现在可以查看 Kaspersky Industrial CyberSecurity for Nodes 的威胁响应历史记录以及管理主机的其他解决方案的响应历史记录。
- 卡巴斯基的 Endpoint Detection and Response (EDR) 解决方案的用户可以使用以下功能和改进。
  - 使用新数据填写警报详细信息。现在警报详细信息包含有关威胁的更多信息，包括应用程序在响应 EDR 威胁时的行为方式。
  - 现在您可以在警报详细信息中管理网络隔离。此外，您可以在警报详细信息中指定计算机网络隔离时间段并添加排除项。
  - IOC 文件处理已得到改进。现在您可以在 Kaspersky Security Center Web Console 界面中查看和编辑 IOC 文件的内容。加载 IOC 文件后，应用程序将显示有关 IOC 术语应用程序的报告。
  - 改进了对检测到的 IOC 的响应。现在，您可以在任务属性中的 IOC 检测结果中直接隔离 *IOC 扫描*任务检测到的文件。您还可以在任务属性中将计算机与网络隔离。
  - 您可以根据包含文件哈希、IP 地址或 DNS 名称列表的 TXT 文件，直接在 *IOC 扫描*任务的属性中创建 IOC 文件。
  - 扩大 *IOC 扫描*任务的扫描范围。现在您可以在注册表中定义 IOC 扫描范围（**Windows 注册表 – RegistryItem**）。在应用程序的早期版本中，您只能使用注册表中预定义的 IOC 扫描范围。
- *网络威胁防护*组件可以监控网络流量，检测端口扫描和高强度的网络请求。
- 在应用程序控制台中，在“**遥测采集服务器**”部分，您现在可以配置以下集成：
  - 与 Kaspersky Endpoint Detection and Response Expert (on-premise) 的整合
  - 与 KICS for Networks 集成
  - SIEM 集成

- 作为与 KICS for Networks 集成的一部分，您可以将遥测数据发送到内置于软件数据二极管的 MQTT 代理服务器。

- *PLC 项目完整性检查*任务中添加了对 Allen-Bradley ControlLogix PLC 的支持。

- 介绍*性能分析器*。性能分析器是一项收集和分析有关访问设备上的文件和应用程序的信息的任务。此信息可以帮助您定义受信任区域，以最大限度地减少应用程序对工业软件性能的影响。

- 对于“使用 Sigma 规则进行异常检测”组件，现在可以使用以下新集合：

  - *使用 Windows 日志进行的用户活动监控规则集合*。此集合允许在添加新用户、提升用户权限、用户登录系统等时注册事件。

  - *使用 SIMATIC PCS7*、*Siemens STEP7*、*Siemens TIA Portal*、*Siemens WinCC 软件时的可疑活动检测规则集合*。

  - *使用 Yokogawa CENTUM VP*、*ProSafe-RS 系统时的可疑活动检测规则集合*。

- 应用程序在保存设置之前会检查控制组件的配置。增加了对应用程序启动控制、设备控制、系统完整性监控组件的检查。如果控制组件的当前设置可能会增加计算机负载或导致系统故障，应用程序会显示警告。例如，在应用程序启动控制的情况下，如果您选择了阻止除允许的应用程序之外的所有应用程序的模式，并且您没有添加任何允许规则，则应用程序会显示警告，因为这样的配置可能会导致系统故障。

- 添加的新组件：

  - *Managed Detection and Response for ICS*。该组件促进与 Kaspersky Managed Detection and Response for Industrial Control Systems 解决方案的交互。*Kaspersky Managed Detection and Response (MDR)* 解决方案可自动检测和分析工业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。

  - *BadUSB 攻击防护*。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。当操作系统标识为键盘的 USB 设备连接到计算机时，应用程序会提示用户在此键盘上键入代码以授权键盘。

  - *BitLocker 完整磁盘加密*。BitLocker 是 Windows 操作系统内置的加密技术。Kaspersky Industrial CyberSecurity for Nodes 允许您使用 Kaspersky Security Center 控制和管理 Bitlocker。

- 支持 *OPC UA* 协议，用于通过 Kaspersky Security Gateway 向 SCADA 系统发送数据。除了 IEC 60870-5-104 和 OPC DA 协议外，应用程序现在还支持 OPC UA 协议，提供跨平台兼容性。

- Windows XP 和 Windows XP SP1 支持便携式扫描程序。便携式扫描程序可以扫描隔离设备以查找病毒和其他威胁。

- *PLC 项目调查*任务现在支持在 Siemens SIMATIC S7-1200/1500 控制器上进行身份验证。现在，您可以在任务属性中输入与这些 PLC 模型的连接的密码。

分发包

分发包包括欢迎应用程序，您可以用它来执行以下操作：

- 启动 Kaspersky Industrial CyberSecurity for Nodes 应用程序安装向导。

- 启动 Kaspersky Industrial CyberSecurity for Nodes 控制台安装向导。

- 启动卡巴斯基病毒清除工具。

- 启动 Kaspersky Security Gateway 设置。
- 了解此版本的 Kaspersky Industrial CyberSecurity for Nodes。
- 打开 Kaspersky Industrial CyberSecurity for Nodes 4.5 帮助。
- 打开 Kaspersky Industrial CyberSecurity Endpoint Detection and Response 帮助。
- 转到卡巴斯基网站上的 Kaspersky Industrial CyberSecurity for Nodes 页面。
- 访问卡巴斯基网站。
- 访问技术支持网站。

分发包文件保存在不同的文件夹中，具体位置取决于它们的目标用途（请参见以下表格）。

Kaspersky Industrial CyberSecurity for Nodes 分发包文件

文件	用途
autorun.inf	从可移动驱动器安装应用程序时，Kaspersky Industrial CyberSecurity for Nodes 安装向导的自动运行文件。
setupui.exe	应用程序欢迎屏幕启动文件。
kics_win.kud	Kaspersky Unicode 定义格式的文件，带有用于通过 Kaspersky Security Center 远程安装应用程序的安装包的说明。
\client\kicstools.msi	Windows 安装程序安装包；在受保护的设备上安装 Kaspersky Industrial CyberSecurity for Nodes 控制台。
\client\setup_kicstool.exe	用于安装一组管理工具组件（包括 Kaspersky Industrial CyberSecurity for Nodes 控制台）的向导的启动文件。安装包文件 kicstools.msi 以向导中指定的安装设置启动。
\client\license.txt	Kaspersky Industrial CyberSecurity for Nodes 管理控制台最终用户授权许可协议和隐私策略文本文件。
\exec\bases.cab	程序发布时最新反病毒数据库的压缩文件。
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	用于删除不兼容软件的文件。
\exec\incompatible.txt	卡巴斯基不保证 Kaspersky Industrial CyberSecurity for Nodes 与文件中列出的应用程序的兼容性。
\exec\installer.ini	包含分发套装内部设置的文件。
\exec\kics.cab	应用程序图形界面的文件。
\exec\kics_win.kud	Kaspersky Unicode 定义格式的文件，带有用于通过 Kaspersky Security Center 远程安装应用程序的安装包的说明。
\exec\kics_win.msi	Windows 安装程序安装包；在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes。
\exec\klcfginst.msi	可通过 Kaspersky Security Center 获取 Kaspersky Industrial CyberSecurity for Nodes 管理插件的安装程序。如果您计划使用管理插件来管理 Kaspersky Industrial CyberSecurity for Nodes，请在安装了 Kaspersky Security Center 管理控制台的每个受保护设备上安装管理插件。
\exec\ksn_en.txt	包含 KSN 声明文本的文件。
\exec\license.txt	Kaspersky Industrial CyberSecurity for Nodes 最终用户授权许可协议和隐私策略文本文件。
\exec\package.kcat	带有分发包文件签名的文件。
\exec\setup_kics.exe	该文件启动在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes 的向导；它使用向导中指定的安装设置启动安装程序包文件 kics_win.msi。
\gateway\security_gateway.msi	Windows 安装程序安装包；安装 Kaspersky Security Gateway。
\gateway\license.txt	Kaspersky Security Gateway 最终用户授权许可协议和隐私策略文本文件。
\kvrt\KVRT.exe	卡巴斯基病毒清除工具的安装程序。
\setup\images	包含应用程序欢迎屏幕启动文件的文件夹。

文件	用途
\setup\setup.hta	应用程序欢迎屏幕启动文件。
\setup\SETUP_STRINGS.JS	包含应用程序文本资源的文件。

分发工具包文件可以从安装 CD 运行。如果您事先将分发包文件复制到本地驱动器，请确保分发套件文件的结构已保留。

软件和硬件要求

对受保护设备的软件要求

在运行 Microsoft Windows XP 的受保护设备上正确安装和运行应用程序需要 Windows Installer 3.1。

要在运行嵌入式操作系统的受保护设备上安装和使用 Kaspersky Industrial CyberSecurity for Nodes，“筛选管理器”组件是必需的。

为了让 Kaspersky Industrial CyberSecurity for Nodes 正常运行，Microsoft Windows 需要 SHA-2 支持。有关详细信息，请参阅技术支持网站上的知识库。

您可以在运行下列 32 位或 64 位 Microsoft Windows 操作系统的设备上安装 Kaspersky Industrial CyberSecurity for Nodes：

桌面操作系统：

- Windows 2000 Professional SP4 32 位

  只有在可选择反病毒扫描模式下的便携式扫描程序才能在具有此操作系统的设备上运行。无法进行网络流量写入或者设备安全审计。

- Windows XP Professional SP2 以及更高版本 32 位/64 位

  如果便携式扫描程序在具有此操作系统的设备上运行，则无法在此设备上执行网络流量的写入。

- Windows Vista SP2 32 位/64 位

  如果便携式扫描程序在具有此操作系统的设备上运行，则无法在此设备上执行网络流量的写入。

- Windows 7 SP1 和更高版本 Home / Pro / Enterprise / Ultimate 32 位/64 位

  在 Windows 7 SP1 之前的 Windows 版本的计算机上，在安全可移动驱动器上创建便携式扫描程序的任务和从安全可移动驱动器运行便携式扫描程序的任务不可用。

- Windows 8 Pro / Enterprise 32 位/64 位
- Windows 8.1 Pro / Enterprise 32 位/64 位
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 位/64 位
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 位

服务器操作系统：

- Windows Server 2003 SP1 Standard / Enterprise 32 位/64 位

  如果便携式扫描程序在具有此操作系统的设备上运行，则无法在此设备上执行网络流量的写入。

- Windows Server 2008 R2 SP1 和更高版本 Foundation / Standard / Enterprise 64 位

  在 Windows Server 2008 R2 SP1 之前的 Windows 版本的计算机上、安全复制和更新应用程序数据库的任务、在安全可移动驱动器上创建便携式扫描程序的任务以及从安全可移动驱动器运行便携式扫描程序的任务不可用。

- Windows Server 2008 SP2 Standard / Enterprise 64 位
- Windows Small Business Server 2011 Essentials / Standard 64 位
- Windows MultiPoint Server 2011 64 位
- Windows Server 2012 Foundation / Essentials / Standard 64 位
- Windows Server 2012 R2 Foundation / Essentials / Standard 64 位
- Windows Server 2016 Essentials / Standard 64 位
- Windows Server 2019 RS5 Essentials / Standard 64 位
- Windows Server 2022 21H2 64 位
- Windows Server 2022 版本 20348.350 64 位
- Windows Server 2025 版本 26100.1742 64 位

嵌入式系统：

- Windows XP Embedded Service Pack 3 32 位

  如果便携式扫描程序在具有此操作系统的设备上运行，则无法在此设备上执行网络流量的写入。

- Windows Embedded POSReady 7 32 位/64 位

  在配备 Windows Embedded POSReady 7 的计算机上，安全复制和更新应用程序数据库的任务、在安全可移动驱动器上创建便携式扫描程序的任务以及从安全可移动驱动器运行便携式扫描程序的任务不可用。

- Windows Embedded Standard 7 Service Pack 1 32 位/64 位
- Windows Embedded 8 Standard 32 位/64 位
- Windows Embedded 8.1 Industry Pro 32 位/64 位
- Windows 10 IoT Enterprise 版本 1507 32 位/64 位
- Windows 10 IoT Enterprise 版本 1607 32 位/64 位
- Windows 10 IoT Enterprise 版本 1803 32 位/64 位
- Windows 10 IoT Enterprise 版本 1809 32 位/64 位

- Windows 10 IoT Enterprise 版本 1903 32 位/64 位
- Windows 10 IoT Enterprise 版本 2004 32 位/64 位
- Windows 10 IoT Enterprise 版本 20H2 32 位/64 位
- Windows 10 IoT Enterprise 版本 21H1 32 位/64 位
- Windows 10 IoT Enterprise 版本 21H2 32 位/64 位
- Windows 10 IoT Enterprise 版本 22H2 32 位/64 位
- Windows 11 IoT Enterprise 版本 21H2 64 位
- Windows 11 IoT Enterprise 版本 22H2 64 位
- Windows 11 IoT Enterprise 版本 23H2 64 位

对受保护设备的硬件要求

对受保护设备的硬件要求

操作系统类型	操作系统名称	最低要求	推荐要求
工作站	Windows 7 / 8 x86 Windows XP x86 / x64	• 处理器：1.4 Ghz 单核处理器，英特尔奔腾 IV (x64) 或更高版本。 • 内存：512 MB。 • 可用磁碟空间：2GB	• 处理器：2.4 GHz 四核 • 内存：2 GB • 可用磁碟空间：4GB
	Windows 7 / 8 / 10 / 11 x64	• 处理器：1.4 Ghz 单核处理器，英特尔奔腾 IV (x64) 或更高版本。 • 内存：1 GB。 • 可用磁碟空间：2GB	• 处理器：2.4 GHz 四核 • 内存：2 GB • 可用磁碟空间：4GB
对于服务器	Windows Server 2003 x86/x64 Windows Server 2008 x86	• 处理器：1.4 Ghz 单核处理器，英特尔奔腾 IV (x64) 或更高版本。 • 内存：512 MB。 • 可用磁碟空间：4GB	• 处理器：2.4 GHz 四核 • 内存：2 GB • 可用磁碟空间：4GB
	Windows Server 2016 x64 Windows Server 2012 x64 Windows Server 2008 x64 Windows Server 2019 x64 Windows Server 2022 x64	• 处理器：1.4 GHz 单核。 • 内存：1 GB。 • 可用磁碟空间：4GB	• 处理器：2.4 GHz 四核 • 内存：2 GB • 可用磁碟空间：4GB
嵌入式系统	Windows Embedded XP	• 处理器：1.4 Ghz 单核处理器，英特尔奔腾 IV (x64) 或更高版本。 • 内存：512 MB。 • 可用磁碟空间：2GB	• 处理器：2.4 GHz 四核 • 内存：2 GB • 可用磁碟空间：4GB
	Windows 7 / 8 / 10 Embedded	• 处理器：1.4 Ghz 单核处理器，英特尔奔腾 IV (x64) 或更高版本。 • 内存：1 GB。 • 可用磁碟空间：2GB	• 处理器：2.4 GHz 四核 • 内存：2 GB • 可用磁碟空间：4GB

支持的工业系统

Kaspersky Industrial CyberSecurity for Nodes 4.5 可保护以下可编程逻辑控制器：

- Siemens™ SIMATIC™ S7-300
- Siemens SIMATIC S7-400

- Siemens SIMATIC S7-400H 冗余模式
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- Siemens SIPROTEC 4
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- 基于 CODESYS V3 的设备
- OWEN PLC210
- Fastwel CPM723-01
- PROSOFT Regul R500
- Emerson DeltaV
- Rockwell Automation Allen-Bradley ControlLogix

Kaspersky Security Gateway 的硬件和软件要求

一般硬件和软件要求：

- 1 GB 的可用磁盘空间。
- 如果选择 klakaut 服务作为数据提供商，则必须安装 Kaspersky Security Center 管理服务器。

桌面操作系统：

- Windows 7 SP1 以及更高版本 /专业版/企业版/旗舰版 SP1 32 位/64 位
- Windows 8 Pro / Enterprise 32 位/64 位
- Windows 8.1 Pro / Enterprise 32 位/64 位
- Windows 10 LTSC 2015 版本 1507 32 位/64 位
- Windows 10 LTSC 2016 版本 1607 32 位/64 位
- Windows 10 RS4 版本 1803 家庭版/专业版/教育版/企业版 32 位/64 位
- Windows 10 RS5 版本 1809 家庭版/专业版/教育版/企业版 32 位/64 位
- Windows 10 LTSC 2019 版本 1809 32 位/64 位
- Windows 10 19H1 版本 1903 家庭版/专业版/教育版/企业版 32 位/64 位
- Windows 10 20H1 版本 2004 家庭版/专业版/教育版/企业版 32 位/64 位

- Windows 10 20H2 版本 2009 家庭版/专业版/教育版/企业版 32 位/64 位
- Windows 10 21H1 家庭版/专业版/教育版/企业版 32 位/64 位
- Windows 10 LTSC 2021 版本 21H2 32 位/64 位
- Windows 10 22H2 家庭版/专业版/教育版/企业版 32 位/64 位
- Windows 11 23H2 家庭版/专业版/教育版/企业版 64 位
- Windows 11 22H2 家庭版/专业版/教育版/企业版 64 位
- Windows 11 21H2 家庭版/专业版/教育版/企业版 64 位

服务器操作系统：

- Windows Server 2008 R2 Standard / Enterprise 32 位/64 位
- Windows Server 2008 SP1 R2 Standard / Enterprise 32 位/64 位
- Windows Server 2012 Essentials / Standard / Foundation / Datacenter（64 位）
- Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter（64 位）
- Windows Server 2016 Essentials / Standard / Datacenter（64 位）
- Windows Server 2019 Essentials / Standard / Datacenter（64 位）
- Windows Server 2022 Standard / Datacenter（64 位）

支持的 Kaspersky Security Center 版本

Kaspersky Industrial CyberSecurity for Nodes 与以下版本的 Kaspersky Security Center 兼容：

- Kaspersky Security Center Windows 10.5。支持通过 Kaspersky Security Center 管理控制台和 Kaspersky Security Center Web Console 来管理运行 Microsoft Windows XP SP2 操作系统的计算机上安装的 Kaspersky Industrial CyberSecurity for Nodes。
- Kaspersky Security Center Windows 14.0。支持通过 Kaspersky Security Center 管理控制台和 Kaspersky Security Center Web Console 来管理运行 Microsoft Windows XP SP3 操作系统的计算机上安装的 Kaspersky Industrial CyberSecurity for Nodes。
- Kaspersky Security Center Windows 版本 14.2、15.1。支持通过 Kaspersky Security Center 管理控制台和 Kaspersky Security Center Web Console 对 Kaspersky Industrial CyberSecurity for Nodes 进行管理。
- Kaspersky Security Center Linux 版本 15.2、15.3、15.4、16.0。支持通过 Kaspersky Security Center Web Console 对 Kaspersky Industrial CyberSecurity for Nodes 进行管理。

要通过 Kaspersky Security Center 管理 Kaspersky Industrial CyberSecurity for Nodes，需要 Kaspersky Security Center 网络代理。

Kaspersky Industrial CyberSecurity for Nodes 分发包中不包含 Kaspersky Security Center 网络代理。您可以在应用程序下载页面的“**Kaspersky Security Center**”部分中下载该软件。

卡巴斯基病毒清除工具

卡巴斯基病毒清除工具是一款用于检查和清除运行 Microsoft Windows 操作系统的受感染计算机的实用程序。卡巴斯基病毒清除工具可检测威胁受保护设备的病毒、木马和其他程序，并让用户选择如何处理检测到的受感染对象。

卡巴斯基病毒清除工具不需要安装。可以通过以下方式启动该应用程序：

- 从 kvrt\ 文件夹中，启动 Kaspersky Industrial CyberSecurity for Nodes 4.5 分发包中包含的 kvrt.exe 可执行文件。
- 在欢迎窗口中单击“**运行卡巴斯基病毒清除工具。**”链接。

无法通过 Kaspersky Industrial CyberSecurity for Nodes 4.5 的本地控制台或管理插件启动该实用程序。

消除任何检测到的感染后，必须重新启动计算机。我们建议仅在工业网络运行的技术窗口期间运行卡巴斯基病毒清除工具。

卡巴斯基病毒清除工具不是 Kaspersky Industrial CyberSecurity for Nodes 解决方案的一部分，也不依赖于应用程序组件。

反病毒数据库更新独立于 Kaspersky Industrial CyberSecurity for Nodes 4.5 更新进行。启动卡巴斯基病毒清除工具时，应用程序将通知您是否需要更新。要更新实用程序，您必须连接到互联网。

卡巴斯基病毒清除工具的运行受单独的最终用户授权许可协议控制，您可以在技术支持站点阅读它。

技术支持站点还提供有关启动该实用程序的计算机的系统要求的信息，以及使用卡巴斯基病毒清除工具的详细说明。

功能要求和限制

本节介绍 Kaspersky Industrial CyberSecurity for Nodes 组件的附加功能要求和现有限制。

安装和删除程序

- 为了让 Kaspersky Industrial CyberSecurity for Nodes 正常运行，Microsoft Windows 需要 SHA-2 支持。
- 安装应用程序时，如果 Kaspersky Industrial CyberSecurity for Nodes 安装文件夹的指定路径长度超过 150 个字符，屏幕上可能会出现警告。该警告不影响安装过程：您可以正常安装并运行 Kaspersky Industrial CyberSecurity for Nodes。
- 如果需要安装 SNMP 协议支持组件，倘若 SNMP 服务正在运行，请确保重新启动 SNMP 服务。
- 如果需要在运行嵌入式操作系统的设备上安装和运行 Kaspersky Industrial CyberSecurity for Nodes，请确保安装“筛选管理器”组件。
- 无法通过 Microsoft Active Directory® 组策略安装 Kaspersky Industrial CyberSecurity for Nodes 管理工具。
- 如果从已安装应用程序组件列表中排除反病毒保护节点，则该节点会在安装完成后从可用组件列表中消失。要安装反病毒保护节点的组件，请从安装包启动“安装向导”，因为安装包中包含完整的组件列表。
- 如果安装了 Kaspersky Industrial CyberSecurity for Nodes 管理控制台，“安装向导”可能会提示重新启动计算机。在这种情况下，重启不是强制性的。结束安装管理控制台的用户的会话并再次登录系统即可。
- 在 Windows XP 或 Windows Vista 设备上安装应用程序时，您可能需要安装 DigiCert Assured ID Root CA 证书以启用驱动程序签名验证。如有必要，指定的证书将从应用程序的安装包自动安装到操作系统的受信任根证书存储中。
- 在 Windows XP 或 Windows Vista 设备上安装应用程序时，您需要检查 DigiCert High Assurance EV Root CA. 是否存在。

  如果未安装该根证书，应用程序可能无法正常运行。我们建议您尽快安装证书。
- 如果安装文件夹的路径与下列至少一个文件夹的路径相同，则应用程序安装完成并出现错误：应用程序数据库文件夹、备份文件夹、用于从隔离区恢复对象的文件夹、临时文件文件夹。
- 如果您使用 Kaspersky Security Center 云控制台管理 Kaspersky Industrial CyberSecurity for Nodes，则不允许在本地更新应用程序。在本地更新应用程序时，无法接受 Kaspersky Security Center 云控制台的数据处理协议。

系统完整性监控

默认情况下，“系统完整性监控”组件不监控系统文件夹或文件系统清理文件的更改，以免有关操作系统不断执行的例程文件更改的信息混杂在任务报告中。您无法在监控范围中包含此类文件夹。

监控范围中排除以下文件夹和文件：

- 文件 id 从 0 到 33 的 NTFS 清理文件
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\

- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

应用程序会排除顶层文件夹。

该组件不监控绕过 ReFS/NTFS 文件系统的文件更改（通过 BIOS、LiveCD 等进行的文件更改）。

防火墙

- 您应该指定多个地址，否则无法使用 IPv6。
- 预设的防火墙规则支持受保护设备与管理服务器之间的基本交互方案。要充分利用 Kaspersky Security Center 功能，您需要配置端口规则。您可以在 Kaspersky Security Center 知识库中找到有关端口号、协议及其功能的信息。
- 安装应用程序并配置防火墙规则后，应用程序将在防火墙组件运行时监控 Windows 防火墙规则和规则组的更改。要更新状态并添加必要的 Windows 防火墙规则，请重新启动防火墙组件。
- 当您启动防火墙组件时，拒绝规则和控制出站流量的规则会自动从 Windows 防火墙设置中删除。

- 应用程序路径和应用程序的防火墙规则名称中不能使用字符“*”和“?”。
- 在 Windows 操作系统中，在防火墙设置（**设置 → 更新和安全 → Windows 安全 → 防火墙和网络保护**）中，启用 Kaspersky Industrial CyberSecurity for Nodes 防火墙的按钮仅启用防火墙，而不会将其切换为“*阻止*”模式，除非在启用防火墙之前，你已经启用了“*观察 Windows 防火墙的状态*”防火墙模式。启用 Kaspersky Industrial CyberSecurity for Nodes 防火墙的按钮只有在防火墙模式更改为“*阻止*”后才会停止显示。

对过时 Windows 版本的限制

- Windows XP SP2 版本不允许阻止远程设备和配置阻止的网络会话列表设置。在此 Windows 版本中，“**阻止显示恶意活动的会话访问网络共享资源**”复选框处于非活动状态。
- Kaspersky Industrial CyberSecurity for Nodes 安装：
  - 在运行 Windows XP SP2 Professional（32 位或 64 位）、Windows Server 2003 或 Windows Server 2003 R2 的计算机上，当使用 Kaspersky Security Center 安装应用程序时，必须将 Network Agent 10.5.1781 安装包中的 setup.exe 文件放入应用程序安装包文件夹中，并安装 Kaspersky Security Center 的私有补丁。
  - 在运行 Windows XP SP3 Professional（32 位）或 Windows XP Embedded SP3（32 位）的计算机上，当使用 Kaspersky Security Center 安装应用程序时，必须将 Network Agent 14.0.0.20023 安装包中的 setup.exe 文件放入应用程序安装包文件夹中，并安装 Kaspersky Security Center 的私有补丁。

    如需所需文件和说明，请联系技术支持。
- 要通过 Kaspersky Security Center 管理 Kaspersky Industrial CyberSecurity for Nodes：
  - 在运行 Windows XP SP2 Professional（32 位/64 位）、Windows Server 2003 或 Windows Server 2003 R2 的计算机上，您必须使用 Kaspersky Security Center 网络代理版本 10.5.1781。
  - 在运行 Windows XP SP3 Professional（32 位）和 Windows XP Embedded SP3（32 位）的计算机上，您必须使用 Kaspersky Security Center 网络代理版本 14.0.0.20023。
- 在 Windows XP 计算机上，无法使用 MQTT 协议将遥测数据发送到数据二极管。
- 要让“*性能分析器*”任务正常工作，启动该任务的计算机必须运行 Windows Vista 或更高版本。

与 Kaspersky Security Center 集成

- 收到更新包后，管理服务器会先验证数据库更新，然后再将更新发送到网络上的受保护设备。Kaspersky Security Center 管理服务器不验证应用程序模块更新。
- 当使用借助网络列表（隔离、备份）将动态数据传输到 Kaspersky Security Center 的组件时，确保在“与 Kaspersky Security Center 管理服务器交互”设置中选中所需复选框。
- 网络代理 10.5 不会将有关已安装组件的信息发送到 Kaspersky Security Center 管理服务器。因此，在 Kaspersky Security Center 管理控制台和 Kaspersky Security Center Web Console 中，安装了网络代理 10.5 的设备的设置不会显示已安装的 Kaspersky Industrial CyberSecurity for Nodes 组件及其设置。

- 如果设备上安装了 Kaspersky Security Center 网络代理 10.5，则您无法使用 Kaspersky Security Center Web Console 下载备份中的文件。

- 如果安装了 Kaspersky Industrial CyberSecurity for Nodes ，并且启用了Kaspersky Security Center 网络代理的低资源消耗模式（默认，`SKIP_KLNAG_FLAG_TEST_VM_PERF=0`），然后安装网络代理，Kaspersky Industrial CyberSecurity for Nodes 不会在 Windows 防火墙中为网络代理创建排除项，因此 Windows 防火墙会阻止网络代理。

- 如果安装了 Kaspersky Industrial CyberSecurity for Nodes，并且启用了 Kaspersky Security Center 网络代理的低资源消耗模式（默认，`SKIP_KLNAG_FLAG_TEST_VM_PERF=0`），网络列表的修改反映在 Kaspersky Security Center 管理控制台中大约需要十分钟的延迟。

其他限制

按需扫描 和 实时文件保护

- 不能扫描已连接的 MTP 设备。

- 如果没有 SFX 压缩文件扫描，压缩文件扫描不可用：如果 Kaspersky Industrial CyberSecurity for Nodes 的保护设置中启用了压缩文件扫描，应用程序会自动扫描压缩文件和 SFX 压缩文件中的对象。如果没有压缩文件扫描，SFX 压缩文件扫描仍可用。

- 如果“**深度分析启动进程(在分析期间，进程启动被阻止)**”复选框和“**KSN 使用**”同时启用，任何接收 URL 网址作为参数的启动进程都将被阻止，即使选择了“通知”模式。为避免阻止此进程，请选择以下选项之一：

  - 禁用 **KSN 使用**。

  - 禁用“**深度分析启动进程(在分析期间，进程启动被阻止)**”复选框

  推荐选项：清除“**深度分析启动进程(在分析期间，进程启动被阻止)**”复选框。

授权许可

- 如果密钥使用 SUBST 命令创建，或者密钥文件的路径是网络路径，则无法通过安装向导使用密钥激活应用程序。

- 如果计划使用 Kaspersky Security Center 代理服务器在客户端设备上激活产品，请在安装 Kaspersky Security Center 网络代理时在此设备上禁用 VDI 优化。

更新

- 默认情况下，应用程序图标在安装 Kaspersky Industrial CyberSecurity for Nodes 关键模块更新后隐藏。

- 运行 Windows XP 或 Windows Server® 2003 操作系统的受保护设备不支持 KLRAMDISK。

- 如果 Kaspersky Industrial CyberSecurity for Nodes 补丁安装失败，则会回滚该补丁并提示您重新启动操作系统。

界面

- 在应用程序控制台中，隔离区、备份区、系统审核日志或任务日志中的过滤区分大小写。
- 在应用程序控制台中配置保护或扫描范围时，只能使用一个掩码，并且只能在路径末尾使用。下面是正确掩码的示例：`C:\Temp\Temp*`、`C:\Temp\Temp???.doc`、`C:\Temp\Temp*.doc`。此限制不影响信任区域的配置。
- 在应用程序控制台中，在"**遥测采集服务器**"部分中，不显示任务计划运行的时间。"**开始时间**"列为空。

安全性

- 如果操作系统的用户账户控制功能已启用，则用户账户必须属于 KICS 管理员组，才能通过双击任务栏通知区域中的应用程序图标来打开应用程序控制台。否则，需要以被允许打开小型诊断窗口或 Microsoft 管理控制台管理单元的用户身份登录。
- 如果启用了用户账户控制，则无法通过 Microsoft Windows 程序和功能窗口卸载应用程序。

漏洞利用防御

- 如果当前环境配置中未加载 apphelp.dll 库，则"漏洞利用防御"不可用。
- "漏洞利用防御"组件与运行 Microsoft Windows 10 操作系统的受保护设备上的 Microsoft EMET 实用程序不兼容。如果在安装了 EMET 实用程序的受保护设备上安装"漏洞利用防御"组件，Kaspersky Industrial CyberSecurity for Nodes 会阻止 EMET。
- "漏洞利用防御"组件与 SQL Server® 2012 数据库引擎不兼容。如果在装有 MS SQL Server 2012 的计算机上安装 Kaspersky Industrial CyberSecurity for Nodes，必须将数据库服务器的 sqlos.dll 库添加到"漏洞利用防御"任务的排除列表中。

Detection and Response

- 如果在威胁响应过程中发生共享文件夹访问错误，则此类错误不会反映在威胁响应历史记录中（Kaspersky Security Center Web Console → 已安装应用程序的主机的属性 → **Detection and Response** – **响应历史**）。
- 将 [KICS+KEA] 配置迁移到 [KICS+内置代理] 配置可能会导致 Kaspersky Endpoint Agent 应用程序卸载错误。最新版本的 Kaspersky Endpoint Agent 修复了应用程序卸载错误。要卸载 Kaspersky Endpoint Agent，请重新启动计算机并创建应用程序卸载任务。
- 不支持[KICS+KEA+内置代理]配置。此类配置会破坏应用程序与组织中部署的 Detection and Response 解决方案之间的交互。此外，在同一台计算机上使用 Kaspersky Endpoint Agent 和内置代理会导致重复遥测并增加计算机和网络的负载。迁移到[KICS+内置代理]配置后，请确保 Kaspersky Endpoint Agent 已从计算机中删除。如果 Kaspersky Endpoint Agent 在迁移后继续工作，请手动卸载应用程序（例如，使用*远程卸载应用程序*任务）。

  安装程序允许您在安装了 Kaspersky Industrial CyberSecurity for Nodes 和内置代理的计算机上部署 Kaspersky Endpoint Agent。Kaspersky Endpoint Agent 和内置代理也可以安装在一台计算机上，作为*更改应用程序组件*任务的结果。该行为取决于 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Endpoint Agent 的版本。

事件配置

Kaspersky Security Center 策略的"**事件配置**"部分中可以配置的"*受控区域中不受控制的文件操作*"事件设置也适用于以下事件：

- "*已允许受信任用户在受控制区域执行文件操作*"。
- "*在受控区域中禁止的文件操作*"。
- "*仅统计：受控制区域内禁止的文件操作*"。
- "*受控区域中不受控制的文件操作*"。

小型诊断窗口

在 Windows XP 计算机上，小型诊断窗口需要终端服务才能运行。

设备控制

卸载并重新安装应用程序而不重新启动时，设备控制可能会保持启用状态。要恢复设备控制的正确操作，请重新启动计算机。

典型部署

Kaspersky Industrial CyberSecurity for Nodes 是 Kaspersky Industrial CyberSecurity 解决方案的一部分。

Kaspersky Industrial CyberSecurity 解决方案包括以下实用程序和应用程序：

- Kaspersky Security Gateway。
- Kaspersky Industrial CyberSecurity for Nodes。
- Kaspersky Industrial CyberSecurity for Networks。
- Kaspersky Security Center。

Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky Industrial CyberSecurity for Nodes 在*专用网络*不同层面上工作。专用的 Kaspersky Industrial CyberSecurity 网络是工业网络的一部分，其中包括设计用于运行 Kaspersky Industrial CyberSecurity 应用程序的计算机，以保护工业系统和辅助硬件（例如交换机）。

Kaspersky Industrial CyberSecurity for Networks 监控并分析工业网络流量。安装在工业网络节点上的 Kaspersky Industrial CyberSecurity for Nodes 保护计算机免受已知的计算机安全威胁，并监控扫描范围内的 PLC 项目的完整性。

您可以使用单个 Kaspersky Security Center 管理控制台控制部署在同一专用网络上的 Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky Industrial CyberSecurity for Nodes。您还可以配置从 Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky Industrial CyberSecurity for Nodes 收到的诊断信息，以便从 Kaspersky Security Center 发送到 SCADA 系统，使用 Kaspersky Security 网关。

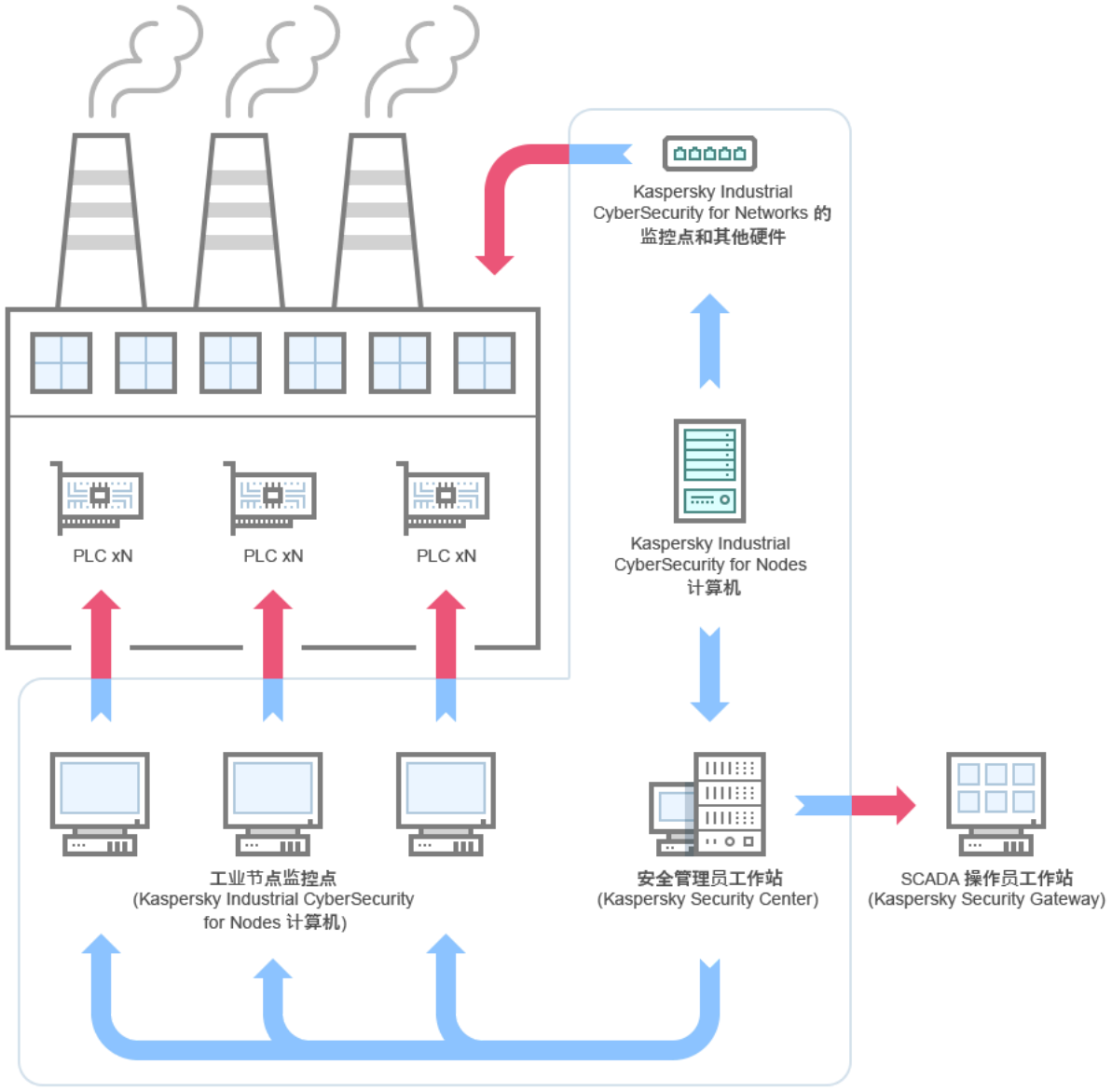
Kaspersky Industrial CyberSecurity for Nodes 包括：

- *功能模块* – 记录有关工业网络节点状态的信息并保护节点免受数据威胁。

- *控制台* – 是本地图形用户界面。您可以使用 Kaspersky Industrial CyberSecurity for Nodes 控制台来控制工业网络节点上的应用程序。控制台可以安装在安装了 Kaspersky Industrial CyberSecurity for Nodes 的计算机上，也可以安装在受保护网络上的任何其他计算机上。在这种情况下，控制台用于远程控制应用程序。您还可以使用一个控制台来控制受 Kaspersky Industrial CyberSecurity for Nodes 保护的多台计算机。

Kaspersky Industrial CyberSecurity for Nodes 记录受保护节点上的安全事件，并将事件发送到应用程序控制台和 Kaspersky Security Center 管理控制台。本地应用程序控制台和 Kaspersky Security Center 管理控制台可从企业工业流程监控专家的工作站以及信息安全专家的工作站访问。

在作为 Kaspersky Industrial CyberSecurity 解决方案一部分的 Kaspersky Industrial CyberSecurity for Nodes 的部署示例中（见下图），专用网络以蓝色显示，工业网络组件以红色显示。部署方案取决于计划安装 Kaspersky Industrial CyberSecurity 解决方案应用程序的工业网络的具体情况。



Kaspersky Industrial CyberSecurity for Nodes 部署方案

与其他应用程序的兼容性

*完整功能*配置下的 Kaspersky Industrial CyberSecurity for Nodes 与第三方端点保护系统 (Endpoint Protection Platform，EPP) 中的应用程序不兼容。Kaspersky Industrial CyberSecurity for Nodes 也可能与其他应用程序和某些卡巴斯基应用程序不兼容。为了确定兼容性，Kaspersky Industrial CyberSecurity for Nodes 参考了卡巴斯基准备的软件列表。此列表包含在 incompatible.txt 文件中。此文件包含在分发包中。

如果检测到 incompatible.txt 列表中的应用程序，安装程序将中止 Security for Nodes 的安装。您需要删除第三方反病毒应用程序。安装程序可能会自动从列表中删除一些应用程序。

如果计算机上安装了 Windows 防火墙，安装程序会将其关闭以继续安装 Kaspersky Industrial CyberSecurity for Nodes。

如果您不顾风险，仍需要安装 Kaspersky Industrial CyberSecurity for Nodes 以及 incompatible.txt 列表中的应用程序，则可以跳过对已安装的第三方反病毒应用程序的检查。为此，请将"`SKIPINCOMPATIBLESW= 1`"参数传递给安装程序。

例如：

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 /p SKIPINCOMPATIBLESW= 1
```

*端点代理*配置下的 Kaspersky Industrial CyberSecurity for Nodes 可以和第三方 EPP 应用程序安装在同一台计算机上。

安装和删除程序

本节提供安装和卸载 Kaspersky Industrial CyberSecurity for Nodes 的逐步说明。

安装计划

本节介绍 Kaspersky Industrial CyberSecurity for Nodes 管理工具集，以及使用向导、命令行、使用 Kaspersky Security Center 和通过 Active Directory 组策略安装和卸载 Kaspersky Industrial CyberSecurity for Nodes 的特殊方面。

如果您在删除 Kaspersky Embedded Systems Security for Windows 或 Kaspersky Endpoint Security for Windows 后安装 Kaspersky Industrial CyberSecurity for Nodes，则必须重新启动计算机。

在开始安装 Kaspersky Industrial CyberSecurity for Nodes 前，请计划安装的主要阶段。

1. 确定管理和配置 Kaspersky Industrial CyberSecurity for Nodes 所使用的管理工具。
2. 选择安装所需的应用程序组件。
3. 选择安装方法。

选择管理工具

确定将用于配置 Kaspersky Industrial CyberSecurity for Nodes 设置和管理该应用程序的管理工具。可以使用应用程序控制台、命令行实用工具和 Kaspersky Security Center 管理控制台管理 Kaspersky Industrial CyberSecurity for Nodes。

Kaspersky Industrial CyberSecurity for Nodes 控制台

Kaspersky Industrial CyberSecurity for Nodes 控制台是添加到 Microsoft 管理控制台的独立管理单元。您可以通过安装在受保护设备或公司网络中其他设备上的应用程序控制台来管理 Kaspersky Industrial CyberSecurity for Nodes。

您可以将多个 Kaspersky Industrial CyberSecurity for Nodes 管理单元添加到在作者模式下打开的 Microsoft 管理控制台的单个副本中，以便用它来管理多台已安装 Kaspersky Industrial CyberSecurity for Nodes 的设备的保护。

应用程序控制台包含在“管理工具”应用程序组件集内。

命令行实用工具

您可以从受保护设备的命令行管理 Kaspersky Industrial CyberSecurity for Nodes。

命令行实用工具包含在 Kaspersky Industrial CyberSecurity for Nodes 软件组件组中。

Kaspersky Security Center

如果 Kaspersky Security Center 用于公司设备反病毒保护的集中管理，您可以通过 Kaspersky Security Center 管理控制台管理 Kaspersky Industrial CyberSecurity for Nodes。

必须安装以下组件：

- **用来与 Kaspersky Security Center 网络代理进行集成的模块**。该组件包含在 Kaspersky Industrial CyberSecurity for Nodes 软件组件组中。它允许 Kaspersky Industrial CyberSecurity for Nodes 与网络代理通信。将用来与 Kaspersky Security Center 网络代理进行集成的模块安装到受保护设备上。

- **Kaspersky Security Center 网络代理**。在每台受保护设备上安装该组件。该组件支持受保护设备上安装的 Kaspersky Industrial CyberSecurity for Nodes 与 Kaspersky Security Center 管理控制台之间的交互。网络代理安装文件包含在 Kaspersky Security Center 分发包文件夹中。

- **Kaspersky Industrial CyberSecurity for Nodes 管理插件**。此外，在安装了 Kaspersky Security Center 管理服务器的受保护设备上通过管理控制台安装管理插件，以便管理 Kaspersky Industrial CyberSecurity for Nodes。此插件提供了通过 Kaspersky Security Center 进行应用程序管理的界面。管理插件安装文件 \exec\klcfginst.exe 包含在 Kaspersky Industrial CyberSecurity for Nodes 分发包中。

选择安装类型

指定 Kaspersky Industrial CyberSecurity for Nodes 安装的软件组件后，您需要选择应用程序安装方法。

根据网络体系结构和以下状况选择安装方法：

- 是需要特殊的 Kaspersky Industrial CyberSecurity for Nodes 安装设置，还是推荐的安装设置。

- 所有受保护设备的安装设置均相同，还是每台受保护设备使用特定的安装设置。

Kaspersky Industrial CyberSecurity for Nodes 可以使用安装向导以互动方式安装，也可以在静默模式下，通过从命令行运行带安装设置的安装包文件进行安装，后者无需用户参与。使用 Active Directory 组策略或使用 Kaspersky Security Center 远程安装任务可对 Kaspersky Industrial CyberSecurity for Nodes 执行集中远程安装。

Kaspersky Industrial CyberSecurity for Nodes 可以在单台受保护设备上安装和配置，其设置保存到一个配置文件中；该文件随后可用于在其他受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes。请注意，当使用 Active Directory 组策略安装应用程序时，此功能不存在。

启动安装向导

安装向导可以用于：

- 通过单击欢迎应用程序中的链接，在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes 组件，可以通过打开 setupui.exe 或直接使用分发包中的 \exec\setup_kics.exe 文件来启动欢迎应用程序。

- 通过单击欢迎应用程序中的链接，在受保护设备或 LAN 上的其他设备上安装 Kaspersky Industrial CyberSecurity for Nodes 控制台，可以通过打开 setupui.exe 或直接使用分发包中的 \client\setup_kicstools.exe 文件来启动欢迎应用程序。

从命令行以必要的安装设置运行安装包文件

如果不以任何命令行选项启动安装包文件，则 Kaspersky Industrial CyberSecurity for Nodes 将以默认设置安装。可以使用 Kaspersky Industrial CyberSecurity for Nodes 选项修改安装设置。

应用程序控制台可以安装在受保护设备和/或管理员工作站上。

您还可以使用示例命令安装 Kaspersky Industrial CyberSecurity for Nodes 和应用程序控制台。

通过 Kaspersky Security Center 集中安装

如果 Kaspersky Security Center 在您的网络中的用途是管理网络设备的反病毒保护，则可以使用远程安装任务在多台设备上安装 Kaspersky Industrial CyberSecurity for Nodes。

要使用 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备可以与 Kaspersky Security Center 在同一域中，也可以在不同的域中，或完全不在任何域中。

使用 Active Directory 组策略集中安装

可以使用 Active Directory 组策略在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes。应用程序控制台可以安装在受保护设备或管理员工作站上。

可以仅使用推荐的安装设置安装 Kaspersky Industrial CyberSecurity for Nodes。

要通过 Active Directory 组策略安装 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备必须位于同一域和同一组织单元中。在登录 Microsoft Windows 前，在受保护设备启动时执行安装。

使用向导安装和卸载应用程序

本节介绍通过安装向导安装和卸载 Kaspersky Industrial CyberSecurity for Nodes 和应用程序控制台，并包含有关 Kaspersky Industrial CyberSecurity for Nodes 的附加配置以及要在安装后执行的操作的信息。

使用安装向导安装

以下各节包含有关安装 Kaspersky Industrial CyberSecurity for Nodes 和应用程序控制台的信息。

要安装和继续使用 Kaspersky Industrial CyberSecurity for Nodes：

1. 在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes。
2. 在您打算用来管理 Kaspersky Industrial CyberSecurity for Nodes 的设备上安装应用程序控制台。
3. 如果应用程序控制台已经安装在网络中的其他设备上，而不是安装在受保护设备上，请执行附加配置以允许应用程序控制台用户远程管理 Kaspersky Industrial CyberSecurity for Nodes。
4. 安装 Kaspersky Industrial CyberSecurity for Nodes 后执行操作。

Kaspersky Industrial CyberSecurity for Nodes 安装

在安装 Kaspersky Industrial CyberSecurity for Nodes 之前，请执行以下操作：

1. 确保受保护设备上未安装其他反病毒程序。
2. 确保用来运行安装向导的账户属于受保护设备上的管理员组。

完成上述操作后，继续安装程序。按照安装向导说明，指定 Kaspersky Industrial CyberSecurity for Nodes 的安装设置。可以在安装向导的任何一个步骤停止 Kaspersky Industrial CyberSecurity for Nodes 安装过程。若要停止安装，请在安装向导窗口中单击“**取消**”按钮。

您可以阅读有关安装（卸载）设置的更多信息。

要通过安装向导安装 Kaspersky Industrial CyberSecurity for Nodes：

1. 在受保护设备上运行 setupui.exe 文件。
2. 在打开的窗口中，在“**安装**”下，点击“**安装 Kaspersky Industrial CyberSecurity for Nodes 4.5**”链接。
3. 在 Kaspersky Industrial CyberSecurity for Nodes 安装向导的欢迎页面，单击“**下一步 >**”按钮。
   “**最终用户授权许可协议**”窗口将打开。
4. 查看授权许可协议和隐私策略的条款。
5. 如果您同意最终用户授权许可协议和隐私策略的条款和条件，请选择“**我确认我已完全阅读、理解并接受这些最终用户授权许可协议的条款和条件**”和“**I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy**”复选框。

   如果您不接受最终用户授权许可协议和/或隐私策略，安装将中止。

6. 单击“**下一步 >**”。
7. “**自定义安装**”窗口将打开。选择要安装的组件。

   - **完整功能**

     默认情况下，除性能计数器和 端点代理 之外，所有 Kaspersky Industrial CyberSecurity for Nodes 组件都属于推荐安装的组件。

     仅在受保护设备上已安装 Microsoft Windows SNMP 服务时，Kaspersky Industrial CyberSecurity for Nodes 的“SNMP 协议支持”组件才会出现在推荐安装的组件列表中。

   - **端点代理**

     选择此选项后，Kaspersky Industrial CyberSecurity for Nodes 安装在 端点代理 配置下。有关此配置的详细信息，请参阅本节。

8. 单击“**下一步 >**”。

9. 在“**选择目标文件夹**”窗口中，执行以下操作之一：

   - 如果需要，指定 Kaspersky Industrial CyberSecurity for Nodes 文件将复制到的文件夹。
   - 如果需要，单击“**浏览**”按钮查看有关本地驱动器上可用空间的信息。

10. 单击“**下一步 >**”。

11. 在“**更改默认文件夹**”窗口中，您可以编辑应用程序使用的文件夹路径。

    如果安装文件夹的路径与下列至少一个文件夹的路径相同，则应用程序安装完成并出现错误：应用程序数据库文件夹、备份文件夹、用于从隔离区恢复对象的文件夹、临时文件文件夹。

12. 在“**高级设置**”窗口中，您可以从保护范围中排除对象和文件夹并配置实时文件保护。

    如果需要，选择一个工业应用程序排除项配置文件：一组 XML 配置规则，用于将工业应用程序进程和文件添加到受信任进程和排除项列表中，以及用于配置应用程序启动控制规则和设置。

    如果未选择“实时文件保护”运行模式，则无法继续执行安装向导的下一步。

13. 单击“**下一步 >**”。

14. 在“**从配置文件导入设置**”窗口中，如果您想从应用程序先前版本中创建的现有配置文件中导入 Kaspersky Industrial CyberSecurity for Nodes 设置，请指定配置文件的路径。

15. 单击“**下一步 >**”。

16. 在“**远程访问设置**”部分中，如果需要，您可以更改应用程序控制台用于远程连接到安装了应用程序的计算机的 TCP 端口号。

    使用 Windows 凭证进行连接的默认端口号为 13032，使用手动创建的用户的凭证进行连接的默认端口号为 13031。可能的端口号范围：1–65535。

    要防止与手动创建的用户账户的凭据进行连接，请清除“**使用手动创建的用户的凭证**”复选框。

17. 单击“**下一步 >**”。

18. 在“**应用程序激活**”窗口中，执行下列操作之一：

    - 如果您想要激活应用程序，请指定 Kaspersky Industrial CyberSecurity for Nodes 密钥文件以激活应用程序。
    - 如果您想要稍后激活应用程序，请单击“**下一步 >**”按钮。
    - 如果密钥文件先前已保存在分发包的 \exec 文件夹中，该文件的名称将显示在“**密钥**”字段中。

    添加密钥文件后，窗口中将显示授权许可信息。Kaspersky Industrial CyberSecurity for Nodes 会显示计算出的授权许可过期日期。授权许可期限从您添加密钥开始生效，在不迟于密钥文件过期日期前失效。

19. 点击“**下一步 >**”将密钥文件添加到应用程序。

20. 在“**准备安装**”窗口中，您可以在必要时禁用“**保护应用程序安装进程**”选项。安装保护包括防止分发包被替换为恶意应用程序、阻止对 Kaspersky Industrial CyberSecurity for Nodes 安装文件夹的访问，以及阻止对包含应用程序密钥的系统注册表部分的访问。但是，如果无法安装应用程序（例如，使用 Windows 远程桌面协助执行远程安装），我们建议您禁用安装过程的保护。

21. 如果必要，将 kavshell.exe 文件路径添加到 %PATH% 系统变量中，以方便使用命令行界面。

22. 单击“**安装**”。

    该向导将开始安装 Kaspersky Industrial CyberSecurity for Nodes。安装完成后将打开“**已完成应用程序安装向导。**”窗口。

23. 单击“**完成**”按钮。

    安装向导关闭。

Kaspersky Industrial CyberSecurity for Nodes 控制台安装

按照安装向导说明配置应用程序控制台的安装设置。可以在安装向导的任何一个步骤停止安装过程。若要停止安装，请在安装向导窗口中单击“**取消**”按钮。

要安装 Kaspersky Industrial CyberSecurity for Nodes 控制台，请运行：

1. 确保用来运行安装向导的账户属于设备上的管理员组。

2. 在受保护设备上运行 setupui.exe 文件。

   将打开欢迎窗口。

3. 单击“**安装 Kaspersky Industrial CyberSecurity for Nodes 控制台**”链接。

   将打开“安装向导”欢迎窗口。

4. 单击“**下一步 >**”。

5. 如果您同意最终用户授权许可协议和隐私策略的条款和条件，请选择“**我确认我已完全阅读、理解并接受这些最终用户授权许可协议的条款和条件**”和“**我了解并同意按照隐私策略所述来处理和传输我的数据(包括传输到第三方国家/地区)。我确认我已完全阅读并理解隐私策略。**”复选框。

6. 如果需要，在“**选择目标文件夹**”窗户中指定要安装的文件应保存到的文件夹。

7. 单击“**下一步 >**”。

8. 在“**准备安装**”窗口中单击“**安装**”按钮。

   该向导将开始安装 Kaspersky Industrial CyberSecurity for Nodes Console。

9. 单击“**完成**”。

应用程序控制台将被安装。

如果管理工具已安装在网络中除受保护设备以外的任何设备上，请配置高级设置。

在其他设备上安装应用程序控制台以后的高级设置

如果应用程序控制台已经安装在网络中的其他设备上，而不是安装在受保护设备上，请执行以下操作，以允许用户远程管理 Kaspersky Industrial CyberSecurity for Nodes：

- 在应用程序设置中使用具有远程连接权限的用户账户。默认情况下，管理员和 KICS 管理员组中的所有用户都拥有此权限。
- 在远程设备上，在 Windows 防火墙设置中，打开 TCP 13032 端口以供 Windows 系统用户账户连接，并打开 TCP 13031 端口以供在应用程序设置中手动创建的用户账户连接。还允许 Kaspersky Industrial CyberSecurity for Nodes 远程管理进程的可执行文件 avp.exe 进行网络连接。在命令行上安装应用程序时，您可以使用 `ADDWFEXCLUSION=1` 选项管理此设置。

如果您需要远程运行 Kaspersky Industrial CyberSecurity for Nodes，请另外执行以下操作：

远程启动应用程序的用户账户必须是管理员组的一部分。确保此账户具有必要的权限管理 Kaspersky Industrial CyberSecurity for Nodes 以及管理 Kaspersky Security 服务。

- 在远程设备上的 Windows 防火墙设置中，启用“**文件和打印机共享（SMB-In）**”规则（端口 TCP 445）。我们还建议打开 TCP 135 端口以方便与设备的连接。
- 对于运行 Windows Vista 或更高版本且不属于域或由本地用户账户管理的远程设备，**禁用用户账户的远程控制（UAC）。**

  1. 打开计算机上的注册表编辑器。
  2. 在注册表编辑器中，打开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 密钥。
  3. 打开 LocalAccountTokenFilterPolicy 值。

     如果此键下缺少 LocalAccountTokenFilterPolicy 值，请使用此名称创建一个 DWORD（32 位）值（有关详细信息，请参阅 Microsoft 技术支持网站）。
  4. 将其设置为 1 并点击 **确定**。

     禁用远程 UAC 不会影响本地 UAC。

- 如果安装了应用程序控制台的设备或受保护的设备运行的是 Windows 8.1 或更早版本的 Windows，**在运行 Windows 10 或更高版本的设备上启用对 SMB 1.0/CIFS 文件的共享访问支持。**

  - 在“Windows 功能”应用程序中：
    1. 选择“**开始** → **控制面板** → **程序和功能** → **打开或关闭 Windows 功能**”。
    2. 在“**Windows 功能**”窗口中，选择“**SMB 1.0/CIFS 文件共享支持**”复选框。
    3. 单击“**确定**”。
  - 在 Windows PowerShell 中：
    1. 以管理员身份运行 Windows PowerShell。
    2. 运行以下命令：

       ```
       Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
       ```

配置任何其他软件或硬件防火墙应该应用相同步骤。

如果在配置受保护设备与安装了应用程序控制台的设备之间的连接时，应用程序控制台处于打开状态：

1. 关闭应用程序控制台。
2. 等待至 Kaspersky Industrial CyberSecurity for Nodes 远程管理进程 avp.exe 结束。
3. 重新启动应用程序控制台。
   将应用新的连接设置。

在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作

如果您已激活 Kaspersky Industrial CyberSecurity for Nodes，该应用程序会在安装后立即启动保护和扫描任务。如果在安装 Kaspersky Industrial CyberSecurity for Nodes 期间选中“**安装应用程序后启用实时文件保护(推荐)**”（默认选项），当设备的文件系统对象被访问时，应用程序会扫描这些对象。如果脚本监控组件作为自定义安装的一部分进行安装， Kaspersky Industrial CyberSecurity for Nodes 会在启动所有脚本时扫描其源代码。Kaspersky Industrial CyberSecurity for Nodes 将在每个星期五的晚上 8 点运行“*关键区域扫描*”任务。

建议在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行下列步骤：

- 启动应用程序数据库更新任务。安装后 Kaspersky Industrial CyberSecurity for Nodes 将使用应用程序分发包中的数据库扫描对象。

  我们推荐立即更新 Kaspersky Industrial CyberSecurity for Nodes 数据库，因为它们可能已过期。

  然后，应用程序将根据任务中配置的默认计划每小时更新一次数据库。

- 如果安装 Kaspersky Industrial CyberSecurity for Nodes 之前受保护设备上未安装任何具有实时文件保护的反病毒软件，请对设备运行“关键区域扫描”。
- 配置有关 Kaspersky Industrial CyberSecurity for Nodes 事件的管理员通知。

启动并配置“数据库和应用程序模块更新”任务

要在安装后更新应用程序数据库：

1. 在“数据库和应用程序模块更新”任务中，配置与更新源的连接。
2. 启动“数据库和应用程序模块更新”任务。

您的网络中可能未配置 Web Proxy Auto-Discovery Protocol (WPAD) 以在 LAN 中自动检测代理服务器设置。而且，在访问代理服务器时，您的网络可能需要身份验证。

要为访问代理服务器指定可选的代理服务器设置和身份验证设置：

1. 打开“**Kaspersky Industrial CyberSecurity for Nodes**”节点的上下文菜单。
2. 选择“**应用程序属性**”。
3. 在打开的窗口中，选择“**网络设置**”选项卡。
4. 在“**代理服务器设置**”部分，点击“**设置**”并在显示的窗口中选择“**使用指定的代理服务器**”复选框。
5. 在“**地址**”字段中输入代理服务器地址，在“**端口**”字段中输入代理服务器的端口号。
6. 在“**代理服务器身份验证设置**”部分的下拉列表中选择必要的身份验证方法：
   - **NTLM 身份验证**，如果代理服务器支持内置的 Microsoft Windows NTLM 身份验证。Kaspersky Industrial CyberSecurity for Nodes 将使用任务设置中指定的账户来访问代理服务器。默认情况下，任务在系统用户账户(SYSTEM)下启动。
   - **使用用户名和密码的 NTLM 身份验证**，如果代理服务器支持内置的 Microsoft Windows NTLM 身份验证。Kaspersky Industrial CyberSecurity for Nodes 将使用指定的账户来访问代理服务器。输入用户名和密码，或从列表中选择用户。
   - **用户名和密码**，选择基本身份验证。输入用户名和密码，或从列表中选择用户。
7. 单击“**确定**”。

要运行“数据库和应用程序模块更新”任务：

1. 在应用程序控制台树中，展开“**更新**”节点。
2. 在“**数据库更新**”子节点的上下文菜单中，选择“**启动**”条目。

“数据库和应用程序模块更新”任务开始。

成功完成该任务后，您可以在 **Kaspersky Industrial CyberSecurity for Nodes** 节点的结果窗格中查看安装的最新数据库更新的发布日期。

关键区域扫描

更新 Kaspersky Industrial CyberSecurity for Nodes 数据库后，使用“*关键区域扫描*”任务扫描受保护设备是否存在恶意软件。

要运行“关键区域扫描”任务：

1. 在应用程序控制台树中，展开“**按需扫描**”节点。
2. 在“**关键区域扫描**”子节点的上下文菜单中，选择“**启动**”命令。

任务启动；结果窗格中显示任务状态“**正在运行**”。

要查看任务日志，请执行下列操作：

在“**关键区域扫描**”节点的结果窗格中，单击“**打开任务日志**”链接。

修改组件集和修复 Kaspersky Industrial CyberSecurity for Nodes

可以添加或删除 Kaspersky Industrial CyberSecurity for Nodes 组件。您需要先停止“实时文件保护”任务，才能删除“实时文件保护”组件。其他情况下，无需停止实时文件保护任务或 Kaspersky Security 服务。

如果应用程序管理受密码保护，Kaspersky Industrial CyberSecurity for Nodes 会在您在安装向导中尝试删除组件或修改组件集时请求密码。

要修改 Kaspersky Industrial CyberSecurity for Nodes 组件集：

1. 在 Windows **控制面板**中，选择“**应用和功能**”。将打开“**修改或删除**”窗口。
2. 右键单击 **Kaspersky Industrial CyberSecurity for Nodes** 并选择 **编辑**。
   这将打开安装向导 **修改、修复或卸载应用程序**。
3. 选择“**修改**”。
   “**自定义安装**”窗口将打开。选择 **完整功能** 并点击 **下一步(N) >**。
4. 在“**自定义安装**”窗口的可用组件列表中，选择要从 Kaspersky Industrial CyberSecurity for Nodes 添加或删除的组件。为此，请执行以下操作：
   - 要更改组件集，请单击所选组件名称旁边的按钮。然后在上下文菜单中选择：
     - **该功能将被安装到本地硬盘驱动器上。**，如果您想安装一个组件；
     - **安装所有功能及其子功能至本地硬盘驱动器。**，如果您想安装该组组件；
   - 要删除先前安装的组件，请单击所选组件名称旁边的按钮。在上下文菜单中，选择“**功能将不可用。**”。

   单击“**下一步(N) >**”。

5. 在 **准备安装** 窗口中，单击“**安装**”确认选择应用程序组件。

6. 在安装完成后打开的窗口中，单击“**完成**”按钮。

将根据指定设置修改 Kaspersky Industrial CyberSecurity for Nodes 组件集。

如果在 Kaspersky Industrial CyberSecurity for Nodes 运行期间出现问题（Kaspersky Industrial CyberSecurity for Nodes 崩溃；任务崩溃或无法启动），可以对 Kaspersky Industrial CyberSecurity for Nodes 执行修复。您可在保存 Kaspersky Industrial CyberSecurity for Nodes 的当前设置时执行修复，或选择一个选项以将所有 Kaspersky Industrial CyberSecurity for Nodes 设置重置为默认值。

要在应用程序或任务崩溃后修复 Kaspersky Industrial CyberSecurity for Nodes：

1. 在 Windows **控制面板**中，选择“**应用和功能**”。将打开“**修改或删除**”窗口。

2. 右键单击 **Kaspersky Industrial CyberSecurity for Nodes** 并选择 **编辑**。

3. 这将打开安装向导 **修改、修复或卸载应用程序**。

4. 请选择**修复**选项。

“**修复 Kaspersky Industrial CyberSecurity for Nodes**”窗口将打开。单击“**下一步(N) >**”。

5. 等待恢复操作完成，然后在打开的窗口中单击“**完成**”。

将使用指定设置修复 Kaspersky Industrial CyberSecurity for Nodes。

使用安装向导卸载

本节包含有关使用安装/卸载向导从受保护设备上删除 Kaspersky Industrial CyberSecurity for Nodes 和应用程序控制台的说明。

Kaspersky Industrial CyberSecurity for Nodes 卸载

卸载 Kaspersky Industrial CyberSecurity for Nodes 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

设置的名称可能有所不同，具体取决于安装的 Windows 操作系统。

可以使用安装/卸载向导从受保护设备卸载 Kaspersky Industrial CyberSecurity for Nodes。

从受保护设备卸载 Kaspersky Industrial CyberSecurity for Nodes 后，可能需要重新启动计算机。重启可以推迟。

应用程序无法通过 Windows 控制面板进行卸载、修复和安装。

当用户尝试在安装向导中删除或修改组件集时，Kaspersky Industrial CyberSecurity for Nodes 会提示用户输入账户凭证。您需要输入具有足够权限的用户的凭证。如果为执行删除操作的用户账户设置了空的 Windows 密码，则在开始删除前禁用“**请求密码以确认关键操作**”功能。

要卸载 Kaspersky Industrial CyberSecurity for Nodes：

1. 在 Windows **控制面板**中，选择“**应用和功能**”。将打开“**修改或删除**”窗口。
2. 右键单击 **Kaspersky Industrial CyberSecurity for Nodes** 并选择 **编辑**。
3. 这将打开安装向导 **修改、修复或卸载应用程序**。
4. 选择“**卸载**”。
   “**保存对象**”窗口将打开。
5. 如果需要，在“**保存对象**”窗口中，执行以下操作之一：
   在“**保存对象**”下，指定要保留的对象或设置。默认下，复选框被清除。
   - 选择**激活数据**复选框。
   - 选择**备份文件**复选框。
   - 选择**应用程序操作设置**复选框。

   在“**导出对象**”下，指定要导出的对象。默认下，复选框被清除。
   - 选中“**导出隔离对象**”复选框，以从 Kaspersky Industrial CyberSecurity for Nodes 隔离区导出对象。默认下，复选框被清除。
   - 选中“**导出备份对象**”复选框，以从 Kaspersky Industrial CyberSecurity for Nodes 备份区导出对象。默认下，复选框被清除。
   - 单击“**保存**”按钮并选择您希望将对象导出到的文件夹。默认情况下，对象将导出到 %ProgramData%\Kaspersky Lab\KICS.4.5\QB。
     单击“**下一步**”。
6. 在“**准备卸载**”窗口中，点击“**卸载**”确认删除。
7. 在卸载完成后打开的窗口中，单击“**完成**”按钮。

Kaspersky Industrial CyberSecurity for Nodes 将从受保护设备卸载。

Kaspersky Industrial CyberSecurity for Nodes 控制台卸载

设置的名称可能有所不同，具体取决于安装的 Windows 操作系统。

您可以使用安装/卸载向导，从受保护设备卸载应用程序控制台。

卸载应用程序控制台后，无需重新启动受保护设备。

要卸载应用程序控制台，请执行下列步骤：

1. 在 Windows **控制面板**中，选择“**应用和功能**”。将打开“**修改或删除**”窗口。
2. 右键单击“**Kaspersky Industrial CyberSecurity for Nodes 控制台**”并选择“**编辑**”。
   这将打开“**修改、修复或卸载应用程序**”向导窗口。
3. 选择“**卸载**”。
   “**准备卸载**”窗口将打开。单击“**卸载**”。
4. 在卸载完成后打开的窗口中，单击“**正常**”按钮。

此时，卸载完成，且安装向导关闭。

从命令行安装和卸载应用程序

本节介绍了从命令行安装和卸载 Kaspersky Industrial CyberSecurity for Nodes 的详细信息，包含从命令行安装和卸载 Kaspersky Industrial CyberSecurity for Nodes 的命令的示例，以及从命令行添加和移除 Kaspersky Industrial CyberSecurity for Nodes 组件的命令的示例。

关于从命令行安装和卸载 Kaspersky Industrial CyberSecurity for Nodes

卸载 Kaspersky Industrial CyberSecurity for Nodes 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

在使用命令行选项指定安装设置后，可以从命令行运行 \exec\kics_win.msi 安装包文件，来安装或卸载 Kaspersky Industrial CyberSecurity for Nodes，以及添加或删除其组件。

“管理工具”集可以安装在受保护设备或网络上的其他设备上，以便在本地或远程与应用程序控制台配合使用。若要执行该操作，请使用 \client\kicstools.msi 安装包。

在安装了该应用程序的受保护设备上，使用包含在管理员组中的账户执行安装。

如果在受保护设备上运行 \exec\kics_win.msi 文件且没有其他命令行选项，Kaspersky Industrial CyberSecurity for Nodes 将使用默认安装设置进行安装。

您可以使用 ADDLOCAL 命令行选项，并列出选定组件或组件集的代码，来分配要安装的组件集。

适用于 Windows Installer 服务的 Kaspersky Industrial CyberSecurity for Nodes 软件组件代码

\exec\kics_win.msi 文件用于安装 Kaspersky Industrial CyberSecurity for Nodes。

\client\kicstools.msi 文件安装管理工具中的所有软件组件。

以下各节列出了适用于 Windows Installer 服务的 Kaspersky Industrial CyberSecurity for Nodes 组件代码。这些代码可以用于定义从命令行安装 Kaspersky Industrial CyberSecurity for Nodes 时要安装的组件列表。

Kaspersky Industrial CyberSecurity for Nodes 软件组件

下表包含 Kaspersky Industrial CyberSecurity for Nodes 软件组件的代码和描述。

Kaspersky Industrial CyberSecurity for Nodes 软件组件的描述

组件	代码	组件功能
实时文件保护	`FileThreatProtection`	此组件在受保护设备上的文件被访问时对这些文件执行病毒扫描。
AMSI 扫描程序	`AMSI`	该组件旨在支持 Microsoft 的Antimalware Scan Interface。 Antimalware Scan Interface (AMSI) 允许具有 AMSI 支持的第三方应用程序将对象（例如，PowerShell 脚本）发送到 Kaspersky Industrial CyberSecurity for Nodes 进行附加扫描，然后接收这些对象的扫描结果。
反加密	`BehaviorDetection`	该组件用表现出恶意的活动的远程设备的名称填充被阻止主机的列表。
漏洞利用防御	`ExploitPrevention`	此组件可管理设置，以便保护设备内存中的进程所使用的内存。
修复引擎	`RemediationEngine`	该组件允许 Kaspersky Industrial CyberSecurity for Nodes 回滚恶意软件在操作系统中执行的操作。
防火墙	`Firewall`	该组件使通过 Kaspersky Industrial CyberSecurity for Nodes 图形用户界面管理 Windows 防火墙成为可能。
网络威胁防护	`NetworkThreatProtection`	此组件扫描入站网络流量中是否存在典型网络攻击活动。在检测到以您的计算机为目标的网络攻击企图时，Kaspersky Industrial CyberSecurity for Nodes 将阻止攻击计算机的网络活动。
应用程序启动控制	`ApplicationControl`	此组件监控用户尝试启动应用程序的情况，并根据指定的应用程序启动控制规则允许或拒绝应用程序启动。
设备控制	`DeviceControl`	此组件跟踪将外部设备连接到受保护设备的尝试，并根据指定的设备控制规则允许或拒绝使用这些设备。
用来与 Kaspersky Security Center 网络代理进行集成的模块	`AdminKitConnector`	在 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Security Center 网络代理之间提供连接。 如果要通过 Kaspersky Security Center 管理应用程序，可以在受保护设备上安装此组件。
日志审查	`LogInspector`	此组件根据 Windows 事件日志的审查结果，对受保护环境的完整性进行监控。
系统完整性监控	`SystemIntegrityMonitor`	该组件包括文件完整性监控的所有功能，另外还允许监控注册表更改和外部设备的连接。
Endpoint Detection and Response（KSC）	`EDR`	该组件促进与 Kaspersky Endpoint Detection and Response Optimum 解决方案的交互。
Endpoint Detection and Response Expert (on-premise)	`AntiAPT`	该组件有助于与作为 Kaspersky Anti Targeted Attack Platform 的一部分的 Endpoint Detection and Response 解决方案的集成。
BadUSB 攻击防护	`BadUSBAttackPrevention`	该组件可以防止受感染的模拟键盘的 USB 设备连接至计算机。
Managed Detection and Response	`MDR`	该组件促进与 Kaspersky Managed Detection and Response 解决方案的交互。
与 KICS for Networks 集成	`KicsForNetworks`	该组件有助于与 Kaspersky Industrial CyberSecurity for Networks 解决方案的集成。
便携式扫描程序	`PortableScanner`	该组件检查隔离的设备并执行安全检查。 您可以连续扫描多个设备。便携式扫描程序为每个扫描的设备生成单独的报告。扫描程序应用默认安全级别：清除。清除失败则删除。
PLC 项目调查	`KicsPlcFeature`	该组件允许接收有关工业网络中当前使用的 PLC 项目的信息。
PLC 项目完整性检查	`KicsPlcFeature`	该组件可以检查工业系统中使用的 PLC 项目的完整性

组件	代码	组件功能
按需扫描	`Ods`	此组件安装 Kaspersky Industrial CyberSecurity for Nodes 系统文件，并执行按需扫描任务（根据请求扫描受保护设备上的对象）。
使用卡巴斯基安全网络	`Ksn`	此组件基于 Kaspersky 云技术提供保护。 它执行"KSN 使用"任务（向卡巴斯基安全网络服务发送请求及从该服务接收结论）。
使用 Sigma 规则进行异常检测	`SigmaMonitoring`	该组件使用 Sigma 规则分析内部事件和事件日志的数据以查找异常。
与 SIEM 集成	`SiemTelemetry`	该组件允许您配置与 SIEM 服务器的集成。

"管理工具"软件组件

下表包含"管理工具"软件组件的代码和说明。

"管理工具"软件组件说明

组件	代码	组件功能
Kaspersky Industrial CyberSecurity for Nodes 管理单元	MmcSnapin	此组件通过 Kaspersky Industrial CyberSecurity for Nodes 控制台安装用于管理应用程序的 Microsoft 管理控制台管理单元。 MmcSnapin 是自动安装的；不需要在安装命令参数中指定。

安装和恢复设置，以及 Windows 安装程序命令行选项

本节介绍 Kaspersky Industrial CyberSecurity for Nodes 的安装和恢复设置。本节还包含用于更改安装设置的项和可能的项值。在从命令行安装 Kaspersky Industrial CyberSecurity for Nodes 时，这些键可以和 Windows Installer 服务的 `msiexec` 命令的标准键一起使用。

安装设置和 Windows 安装程序命令行选项

- 接受最终用户授权许可协议的条款。

  `EULA=<` 值 `>` 命令行选项的可能值如下：

  - `0` - 拒绝最终用户授权许可协议条款（默认值）。
  - `1` - 接受最终用户授权许可协议条款。

- 接受隐私策略的条款。

  `PRIVACYPOLICY=<` 值 `>` 命令行选项的可能值如下：

  - `0` – 拒绝隐私策略条款（默认值）。
  - `1` – 接受隐私策略条款。

- 选择应用程序的模式。

  `STANDALONEMODE=<` 值 `>` 命令行选项的可能值如下：

  - `0` – 完整功能（默认值）。
  - `1` – 端点代理。

- 安装过程中将保存 Kaspersky Industrial CyberSecurity for Nodes 文件的目标文件夹。可以指定其他文件夹。

  INSTALLDIR=< 文件夹的完整路径 > 命令行选项的默认值如下：

  - 对于 32 位版本的 Microsoft Windows：
    - Kaspersky Industrial CyberSecurity for Nodes：%ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0
    - Kaspersky Industrial CyberSecurity for Nodes Console：%ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Admins Tools.4.5.0
  - 对于 64 位版本的 Microsoft Windows：%ProgramFiles(x86)%，并且与 32 位版本的 Microsoft Windows 的路径类似。

- 实时文件保护任务在 Kaspersky Industrial CyberSecurity for Nodes 启动后立即启动。

  RUNRTP=< 值 > 命令行选项的可能值如下：

  - 1 – 启动（默认值）。
  - 0 – 不启动。

- 实时文件保护任务的运行模式。

  RTP_BLOCKING=< 值 > 命令行选项的可能值如下：

  - 1 – 推荐（默认值）。
  - 0 – 通知。

- 将工业软件的进程和文件添加到受信任进程和排除项列表中以及配置应用程序启动控制规则。使用以下命令行选项将进程和文件添加到排除项：ADDEXCLUSION=< 排除项配置文件名称 1 >;< 排除项配置文件名称 2 >;...;< 排除项配置文件名称 n >。受支持的排除项文件的名称列在这里。

- 密钥文件的路径 (LICENSEKEYPATH)。默认情况下，Windows Installer 会尝试在分发包的 \exec 文件夹中查找扩展名为 .key 的文件。如果 \exec 文件夹包含多个密钥文件，Windows Installer 将选择到期日期最远的密钥文件。密钥文件可以预先保存在 \exec 文件夹或者在 LICENSEKEYPATH 参数中指定的其他路径。

  LICENSEKEYPATH 可以采用以下值。

  - 密钥文件的完整路径，包括其名称。
  - 存储密钥文件的文件夹路径。

  您可以在安装 Kaspersky Industrial CyberSecurity for Nodes 后使用所选的管理工具（例如，应用程序控制台）添加密钥。如果您在应用程序安装期间未添加密钥，Kaspersky Industrial CyberSecurity for Nodes 将不会发挥功能。

- 配置文件的路径。Kaspersky Industrial CyberSecurity for Nodes 从在应用程序中创建的指定配置文件导入设置。Kaspersky Industrial CyberSecurity for Nodes 不会从配置文件导入密码，例如用于启动任务的账户密码或用于连接代理服务器的密码。一旦导入设置，将要手动输入所有密码。如果未指定配置文件，安装后应用程序将开始使用默认设置。

  CONFIGPATH=< 配置文件名称 > 的默认值未指定。

- "*在操作系统启动时扫描*"模式(SCANSTARTUP_BLOCKING)。如果安装 Kaspersky Industrial CyberSecurity for Nodes 没有使用 SCANSTARTUP_BLOCKING 参数，则"*在操作系统启动时扫描*"任务中的"**扫描范围**"参数设置如下：

  - 对受感染对象和其他对象执行的操作：**通知**。
  - 对疑似感染的对象执行操作：**通知**。

  如果安装 Kaspersky Industrial CyberSecurity for Nodes 使用了 SCANSTARTUP_BLOCKING 参数，则"*在操作系统启动时扫描*"任务中的"**扫描范围**"参数设置如下：

  - 对受感染对象和其他对象执行的操作：**执行建议的操作**。
  - 对疑似感染的对象执行操作：**执行建议的操作**。

  "*在操作系统启动时扫描*"任务是自动创建的。默认应用"**通知**"模式。在这种情况下，在设备上部署 Kaspersky Industrial CyberSecurity for Nodes 后，如果在扫描期间未发现系统服务问题，您可以启用"*在操作系统启动时扫描*"任务。如果应用程序将关键系统服务检测为受感染或可能受感染的对象，"**通知**"模式会让您有时间找出原因并解决问题。如果应用程序应用"**执行建议的操作**"模式，则执行"**清除。清除失败则删除**"操作。清除或删除系统文件可能会导致操作系统启动出现严重问题。

- 配置操作系统服务保护功能。

  如果启用此功能，则第三方应用程序无法对操作系统的进程进行操作。 PROTECTOSSERVICES=< 值 > 命令行选项的可能值如下：

  - 1 表示操作系统服务的保护已启用（默认值）。
  - 0 表示操作系统服务的保护已禁用。

- 配置应用程序控制台与安装该应用程序的计算机的远程连接所使用的端口：

  要配置用于连接 Windows 凭证的端口，您可以使用 UIPORT=< 端口号 > 参数。可能的端口号范围：1–65535。如果该数字超出指定的间隔，则使用默认端口号。默认值为 13032。

  如果需要，您可以使用"ENABLEUIKLPORT=< 值 >"参数关闭使用手动创建的用户的凭证进行连接的端口：

  - 1 打开端口（默认值）。
  - 0 关闭端口。

  此端口的默认值为 13031。您可以通过指定"UIKLPORT=< 值 >"参数更改端口号。可能的端口号范围：1–65535。

- 启用网络连接的设置，以便使用安装在不同计算机上的应用程序控制台对 Kaspersky Industrial CyberSecurity for Nodes 进行远程管理。

  ADDWFEXCLUSION=< 值 > 命令行选项的可能值如下：

  - 1。如果指定了此值，则为应用程序控制台与安装了应用程序的计算机的远程连接配置的 TCP 端口（"UIPORT=< 值 >"和"UIKLPORT=< 值 >"参数）在 Windows 防火墙中被打开，并允许 Kaspersky Industrial CyberSecurity for Nodes 远程管理进程的可执行文件 avp.exe 进行网络连接。

    另请阅读在另一台设备上安装应用程序时进行的额外配置。

  - 0。如果指定了该值，则不会发生任何事情。

- 禁用不兼容软件检查。使用此设置，可在受保护设备上后台安装应用程序期间启用或禁用不兼容软件检查。无论此设置的值如何，在安装 Kaspersky Industrial CyberSecurity for Nodes 期间，该应用程序始终警告受保护设备上安装的该应用程序的其他版本。

  SKIPINCOMPATIBLESW=< 值 > 命令行选项的可能值如下：

  - 0 - 执行不兼容软件检查（默认值）。
  - 1 - 不执行不兼容软件检查。

- 禁用对 KB5007186 操作系统更新的检查。

  安装 KB5007186 更新后，应用程序继续正常运行，系统安全性不会降低，但应用程序的小版本更新变得无法进行。在安装应用程序之前，安装程序会检查已安装的操作系统更新。如果发现更新 KB5007186，安装程序将中止安装。您可以使用命令行上的 SKIPKB5007186CHECK 键来启用或禁用对 KB5007186 操作系统更新的检查。

  SKIPKB5007186CHECK=< 值 > 命令行选项的可能值如下：

  - 0：安装程序检查是否安装了 KB5007186 操作系统更新。
  - 1：安装程序不检查 KB5007186 操作系统更新是否已安装。

  默认情况下不设置该键，对应于 0。

恢复设置和 Windows 安装程序命令行选项

- 还原已隔离的对象。

  RESTOREQTN=< 值 > 命令行选项的可能值如下：

  - 0 – 删除隔离内容（默认值）。
  - 1 – 将隔离内容还原到 RESTOREPATH 参数指定的文件夹的 \QB 子文件夹中。

- 还原备份内容。

  RESTOREBCK=< 值 > 命令行选项的可能值如下：

  - 0 – 删除备份内容（默认值）。
  - 1 – 将备份内容还原到 RESTOREPATH 参数指定的文件夹的 \QB 子文件夹中。

- 输入当前密码以确认恢复（如果已启用密码保护）。

  UNLOCK_PASSWORD=< 指定密码 > 的默认值未指定。

- 还原对象的文件夹。还原的对象将保存到指定的文件夹。

  RESTOREPATH=< 文件夹的完整路径 > 命令行选项的默认值如下：%ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KICS.4.5.0\QB\Restored。

安装 Kaspersky Industrial CyberSecurity for Nodes 的命令示例

本节提供安装 Kaspersky Industrial CyberSecurity for Nodes 所使用的命令示例。

在受保护的设备上运行分发工具包中的 kics_win.msi 文件。

有关使用 Windows Installer 标准命令和命令行选项的详细信息，提供在 Microsoft 提供的文档中。

从 setup_kics.exe 文件安装 Kaspersky Industrial CyberSecurity for Nodes 的示例

要在无需用户参与的情况下使用推荐的安装设置安装 Kaspersky Industrial CyberSecurity for Nodes：

```
\exec\setup_kics.exe EULA=1 PRIVACYPOLICY=1
```

要安装组件（如设备控制）：

```
\exec\setup_kics.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

在安装应用程序后网络设备和 SCSI 设备会导致系统崩溃的计算机上安装 Kaspersky Industrial CyberSecurity for Nodes 时，可以对此命令使用以下附加选项：

`/p SKIP_NETWORK_UPPERFILTERS=<1|0>`

启用 (1) 或禁用 (0) 拦截网络适配器的连接。

`/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>`

启用 (1) 或禁用 (0) 拦截 SCSI 适配器的连接。

若要安装并使用密钥文件激活 Kaspersky Industrial CyberSecurity for Nodes：

```
setup_kics.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

要更改应用程序控制台与使用 Windows 用户凭证安装应用程序的计算机的远程连接所使用的端口：

```
setup_kics.exe /pUIPORT=<端口号>
```

可能的端口号范围：1–65535。默认值为 13032。

用于安装的命令列表：运行 .msi 文件

要在无需用户参与的情况下使用推荐的安装设置安装 Kaspersky Industrial CyberSecurity for Nodes：

```
msiexec /i kics_win.msi /qn EULA=1 PRIVACYPOLICY=1
```

要使用推荐的安装设置安装 Kaspersky Industrial CyberSecurity for Nodes 并显示安装界面：

```
msiexec /i kics_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

要使用推荐的安装设置安装 Kaspersky Industrial CyberSecurity for Nodes 并在跟踪文件数量达到指定的最大数量时启用跟踪文件轮换：

```
msiexec /i kics_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1
PRIVACYPOLICY=1
```

TRACE_FOLDER 参数是必需的。

以下规则适用于 TRACE_MAX_ROLL_COUNT 参数：

- 如果指定此参数，当跟踪文件数量达到参数中指定的最大数量时，启用跟踪文件轮换。可用的参数值范围：1 到 999。
- 如果将跟踪文件的最大数量指定为 0，则禁用跟踪文件轮换。
- 如果指定了参数值，但该值无效或超出可用值范围（1到 999），则启用跟踪文件轮换，并将跟踪文件的默认最大数量设置为 5。
- 如果未指定参数：
  - 如果设备上已配置跟踪文件轮换，其设置不会更改。应用程序将忽略输入的参数。
  - 如果设备上未配置跟踪文件轮换，则将启用轮换选项，并将跟踪文件的默认最大数量设置为 5。

若要安装 Kaspersky Industrial CyberSecurity for Nodes 并使用密钥文件 C:\0000000A.key 激活：

```
msiexec /i kics_win.msi     LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

要安装 Kaspersky Industrial CyberSecurity for Nodes 并初步扫描活动进程和本地驱动器的引导扇区：

```
msiexec /i kics_win.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

要将 Kaspersky Industrial CyberSecurity for Nodes 安装在安装文件夹 C:\KICS 中：

```
msiexec /i kics_win.msi INSTALLDIR=C:\KICS /qn EULA=1 PRIVACYPOLICY=1
```

要安装 Kaspersky Industrial CyberSecurity for Nodes 并将名为 kics.log 的安装日志文件保存在存储 Kaspersky Industrial CyberSecurity for Nodes msi 文件的文件夹中：

```
msiexec /i kics_win.msi/l*v kics.log /qn EULA=1 PRIVACYPOLICY=1
```

要安装 Kaspersky Industrial CyberSecurity for Nodes 控制台：

```
msiexec /i kicstools.msi /qn EULA=1
```

要安装 Kaspersky Industrial CyberSecurity for Nodes 并使用密钥文件 C:\0000000A.key 激活，并且根据配置文件 C:\settings.xml 中的设置配置 Kaspersky Industrial CyberSecurity for Nodes：

```
msiexec /i kics_win.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn
EULA=1 PRIVACYPOLICY=1
```

要在 Kaspersky Industrial CyberSecurity for Nodes 受密码保护的情况下安装应用程序补丁：

```
msiexec /p "<msp 文件名及路径>" UNLOCK_PASSWORD=<密码>
```

在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作

如果您已激活 Kaspersky Industrial CyberSecurity for Nodes，该应用程序会在安装后立即启动保护和扫描任务。如果在安装 Kaspersky Industrial CyberSecurity for Nodes 期间选中“**安装应用程序后启用实时文件保护(推荐)**”复选框，当设备的文件系统对象被访问时，应用程序会扫描这些对象。如果脚本监控组件作为自定义安装的一部分进行安装， Kaspersky Industrial CyberSecurity for Nodes 会在启动所有脚本时扫描其源代码。Kaspersky Industrial CyberSecurity for Nodes 将在每个星期五的晚上 8 点运行“*关键区域扫描*”任务。

建议在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行下列步骤：

- 启动 Kaspersky Industrial CyberSecurity for Nodes 数据库更新任务。安装后 Kaspersky Industrial CyberSecurity for Nodes 将使用其分发包中的数据库扫描对象。建议立即更新 Kaspersky Industrial CyberSecurity for Nodes 数据库。为此，您必须运行“数据库更新”任务。然后将根据默认计划，每小时更新一次数据库。

  例如，您可以通过运行以下命令来启动“数据库更新”任务：

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
  /PROXYPWD:123456
  ```

  在此情况下，将从 卡巴斯基更新服务器下载 Kaspersky Industrial CyberSecurity for Nodes 数据库更新。与更新源的连接是通过代理服务器（代理服务器地址：proxy.company.com，端口：8080）使用内置的 Windows NTLM 身份验证以某个账户访问服务器来建立的（用户名：inetuser；密码：123456）。

- 如果安装 Kaspersky Industrial CyberSecurity for Nodes 之前受保护设备上未安装任何具有实时文件保护的反病毒软件，请对设备运行“关键区域扫描”。

要使用命令行启动“关键区域扫描”任务：

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

此命令可将任务日志保存在当前文件夹内名为 scancritical.log 的文件中。

- 配置有关 Kaspersky Industrial CyberSecurity for Nodes 事件的管理员通知。

添加/删除组件。命令示例

“按需扫描”组件自动安装。您不需要通过添加或删除 Kaspersky Industrial CyberSecurity for Nodes 组件在 ADDLOCAL 键值列表中指定它。

要将应用程序启动控制组件添加到已安装的组件中，请运行以下命令：

```
msiexec /i kics_win.msi ADDLOCAL=Oas,AppCtrl /qn
```

或

```
\exec\setup_kics.exe /s /p ADDLOCAL=Oas,AppCtrl
```

如果您将要安装的组件与已安装的组件一起列出， Kaspersky Industrial CyberSecurity for Nodes 将重新安装现有组件。

要删除已安装的组件，请运行以下命令：

```
msiexec /i kics_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,Bases,Core,CoreBLFiles,CoreFolde
ADD_ADV=IDS,RegMonitor REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Kaspersky Industrial CyberSecurity for Nodes 卸载。命令示例

要在静默模式下从受保护设备卸载 Kaspersky Industrial CyberSecurity for Nodes，请运行以下命令：

```
msiexec /x kics_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

或

```
msiexec /x {7145B040-E1C7-494D-969C-5F91F477ACDC} KLLOGIN=<user name> KLPASSWD=<password>
/qn
```

或

```
setup_kics.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

`<user name>`是具有足够卸载权限的用户的名称和登录名。

如果为执行删除操作的用户账户设置了空的 Windows 密码，则在开始删除前禁用**"请求密码以确认关键操作"**功能。

要在静默模式下卸载 Kaspersky Industrial CyberSecurity for Nodes 控制台，请运行以下命令：

```
msiexec /x kicstools.msi /qn
```

或

```
msiexec /x {83CEC7FC-0E7D-4F38-8D2B-12EAC40CBD23} /qn
```

返回代码

应用程序安装程序可以返回该文章内描述的返回代码。

下表包含了命令行返回代码的列表。

返回代码

代码	描述
27100	计算机已检测到在测试模式下安装了身份验证代理的驱动器。
27101	计算机已检测到在测试模式下安装了身份验证代理的驱动器。
27102	查找加密磁盘失败。
27200	从 RAM 卸载应用程序失败。
27201	启动 AVP.exe 进程时出错。您的计算机可能已被感染。
27204	缓存分发包失败。
27205	迁移授权许可信息失败。
27206	删除授权许可信息失败。
27207	删除不兼容的软件失败。

代码	描述
27208	检查不兼容的软件失败。
27209	从文件柜中提取文件失败。
27210	配置自我防御失败。
27211	启用自我防御失败。
27212	获取操作系统版本信息失败。
27213	获取启动目录失败。
27214	验证安装目录失败。
27215	配置服务失败。
27216	配置 klcp 升级失败。
27217	升级 klcp 失败。
27218	配置 kl1 驱动程序参数失败。
27219	配置 klelam 驱动程序参数失败。
27220	配置 klwfp 驱动程序参数失败。
27221	配置驱动程序兼容模式失败。
27222	删除注册表项失败。
27223	重新启动操作系统失败。
27224	安装驱动程序失败。
27225	迁移驱动程序设置失败。
27226	停止驱动程序失败。
27227	阻止驱动程序启动失败。
27228	验证文件的签名失败。
27230	准备 kldl 驱动程序设置失败。
27231	配置 kldl 驱动程序设置失败。
27300	安装驱动程序错误。
27301	删除驱动程序时出错。
27302	安装网络组件错误。
27303	驱动程序的注册信息不一致或不完整。请重新启动操作系统并重试。
27305	禁用驱动程序时出错。
27310	安装数字签名的目录文件失败。
27311	卸载数字签名的目录文件失败。
27312	安装证书失败。
27313	删除证书失败。
27320	配置服务失败。
27321	解除服务保护失败。
27350	补丁<补丁名称>不适用于<应用程序名称>应用程序本地化。
27352	完整磁盘加密补丁无法删除。
27353	补丁<补丁 1 名称>只能与补丁<补丁 2 名称>一起安装。
27354	在修改/恢复应用程序之前，必须重新启动计算机才能应用补丁。
27355	锁定完整磁盘加密管理失败。锁定完整磁盘加密管理失败。您必须完成加密才能安装完整磁盘加密更新。
27356	无法安装补丁。
27357	发现安装包中包含召回的补丁。安装将被中止。

代码	描述
27360	补丁无法注册。
27361	设置补丁安装参数失败。
27363	该补丁包含与已安装的加密库不兼容的加密库。
27370	初始化 .NET 8.0 解压时出错。
27371	解压 .NET 8.0 时出错。
27372	先前应用程序版本的注册信息已被删除。请重新启动安装。
27373	删除应用程序上一版本的注册信息失败。
27374	应用程序正在升级。请稍后重试。
27375	卸载密码或用户名未指定或者不正确。
27376	卸载 Kaspersky Endpoint Agent 失败。请自行卸载或在设置中禁用密码保护。然后重新启动应用程序的安装。
27377	卸载 Kaspersky Security for Windows Server 失败。请自行卸载或在设置中禁用密码保护。然后重新启动应用程序的安装。
27378	磁盘空间不足。
27379	由于选择了不兼容的组件，因此安装应用程序失败。请更改组件集并重新启动安装。
27380	选择了无效的配置文件。
27381	选择了无效的授权许可密钥。
27382	创建应用程序管理组失败。
27383	您选择了无效的文件夹。目标文件夹的名称不能超过 160 个字符。
27384	您选择了无效的文件夹或驱动器。该应用程序必须安装在本地硬盘上。
27385	您选择了无效的文件夹。该应用程序无法安装到根文件夹。
27386	您选择了无效的文件夹。该应用程序无法安装到 Windows 文件夹或其子文件夹。
27387	您选择了无效的文件夹。无法将应用程序安装到包含 Temp 子文件夹的文件夹中。
27388	您选择了无效的文件夹。该应用程序不能直接安装在 Program Files 文件夹中。
27389	您选择了无效的文件夹。该应用程序无法安装在虚拟磁盘上。
27390	您选择了无效的文件夹或驱动器。无法将应用程序安装到安装该应用程序先前版本的文件夹。
27391	选定的文件夹或驱动器已包含文件。该应用程序无法安装到包含其他数据的文件夹中，因为启用自我防御后这些数据可能变得不可用。
27392	该应用程序无法安装到包含重新解析点的文件夹。请选择其他安装文件夹。
27393	无法将该应用程序安装到名称中包含分号 (;) 的文件夹中。请选择其他安装文件夹。
27394	您选择了无效的文件夹。无法指定根文件夹。
27395	您选择了无效的文件夹。无法指定 Windows 文件夹或其子文件夹。
27396	您选择了无效的文件夹。无法直接指定 Program Files 文件夹。
27397	您选择了无效的文件夹。无法指定包含 Temp 子文件夹的文件夹。
27400	初始化文件更新时出错。
27450	无法安装 CAB 文件。
27451	删除错误。
27452	删除文件时出错。
27453	移动文件错误。
27454	创建注册表文件失败。
27455	获取操作系统版本信息失败。
27456	安排回滚注册表值失败。
27457	获取已知的安全标识符 (SID) 失败。

代码	描述
27460	创建安全描述符时出错。
27461	恢复安全描述符时出错。
27462	为 Microsoft Windows 防火墙创建规则失败。
27463	删除 Microsoft Windows 防火墙规则失败。

使用 Kaspersky Security Center 安装和卸载应用程序

本节包含有关使用 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Nodes 的信息、通过 Kaspersky Security Center 安装和卸载 Kaspersky Industrial CyberSecurity for Nodes 的过程的说明，以及安装 Kaspersky Industrial CyberSecurity for Nodes 后要采取的操作的说明。

有关通过 Kaspersky Security Center 安装的常规信息

您可以通过 Kaspersky Security Center，使用远程安装任务来安装 Kaspersky Industrial CyberSecurity for Nodes。

完成远程安装任务后，将在多台受保护设备上使用相同的设置安装 Kaspersky Industrial CyberSecurity for Nodes。

所有受保护设备可以组合到一个管理组中，并且可以创建组任务来在该组的受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes。

您可以创建一个任务，在不属于相同管理组的一组受保护设备上远程安装 Kaspersky Industrial CyberSecurity for Nodes。创建该任务时，您必须生成应安装 Kaspersky Industrial CyberSecurity for Nodes 的各个受保护设备的列表。

有关远程安装任务的详细信息，请参见 *Kaspersky Security Center 帮助*。

安装或卸载 Kaspersky Industrial CyberSecurity for Nodes 的权限

在除下述以外的所有情况下，在远程安装（删除）任务中指定的账户必须包含在每个受保护设备的管理员组中：

- 如果 Kaspersky Security Center 网络代理已安装在要安装 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备上（不论这些受保护设备位于哪个域，或它们是否属于任何域）。

  如果网络代理尚未安装在受保护设备上，可以使用远程安装任务安装它和 Kaspersky Industrial CyberSecurity for Nodes。在安装网络代理之前，请确保要在该任务中指定的账户包含在每台受保护设备的管理员组中。

- 要安装 Kaspersky Industrial CyberSecurity for Nodes 的所有受保护设备都和管理服务器在同一个域中，且管理服务器以“**域管理员**”账户身份注册（如果该账户在该域的受保护设备上具有本地管理员权限）。

默认情况下，在使用“**强制安装**”方法时，远程安装任务从运行管理服务器的账户运行。

在强制安装（卸载）模式下对多组受保护设备执行组任务或其他任务时，受保护设备上的账户必须具有以下权限：

- 远程执行应用程序的权限。
- **Admin$** 共享的权限。
- **作为服务登录**的权限。

通过 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Nodes

有关生成安装包和创建远程安装任务的详细信息，请参见《Kaspersky Security Center 实施指南》。

如果希望以后通过 Kaspersky Security Center 管理 Kaspersky Industrial CyberSecurity for Nodes，请确保符合以下条件：

- 安装了 Kaspersky Security Center 管理服务器的受保护设备上还安装了管理插件（Kaspersky Industrial CyberSecurity for Nodes 分发包中的 \exec\klcfginst.exe 文件）。
- Kaspersky Security Center 网络代理安装在受保护设备上。如果 Kaspersky Security Center 网络代理未安装在受保护设备上，可以使用远程安装任务同时安装它和 Kaspersky Industrial CyberSecurity for Nodes。

也可以将多台设备组合到一个管理组中，以便以后使用 Kaspersky Security Center 策略和组任务管理保护设置。

要通过 Kaspersky Security Center 使用远程安装任务安装 Kaspersky Industrial CyberSecurity for Nodes：

1. 打开 Kaspersky Security Center Administration Console。
2. 在 Kaspersky Security Center 管理控制台中，展开“**高级**”节点。
3. 展开“**远程安装**”子节点。
4. 在“**安装包**”子节点的结果窗格中，单击“**创建安装包**”按钮。
5. 请选择**为卡巴斯基应用程序创建安装包**选项。
6. 输入新安装包名称。
7. 指定 Kaspersky Industrial CyberSecurity for Nodes 分发包中的 kics_win.kud 文件为安装包文件。

   “**最终用户授权许可协议和隐私策略**”窗口将打开。
8. 如果您同意最终用户授权许可协议和隐私策略的条款和条件，请选择“**我确认我已完全阅读、理解并接受该最终用户授权许可协议的条款和条件**”和“**我了解并同意我的数据按照隐私策略中所描述被处理和传输(包括到第三方国家)。我确认我已完整阅读并理解隐私策略**”复选框。

   您必须接受授权许可协议和隐私策略才能继续。

9. 要更改要安装的 Kaspersky Industrial CyberSecurity for Nodes 组件集以及安装包中的默认安装设置：

   a. 在 Kaspersky Security Center 管理控制台中，展开“**远程安装**”节点。

   b. 在“**安装包**”子节点的结果窗格中，打开已创建的 Kaspersky Industrial CyberSecurity for Nodes 安装包的上下文菜单，然后选择“**属性**”。

   c. 在“**属性：<安装包名称>**”窗口中打开“**设置**”部分。

   d. 选择安装类型。

   e. 单击“**配置**”按钮指定工业系统的排除项列表。

   f. 在“**组件选择**”部分中，选中要安装的 Kaspersky Industrial CyberSecurity for Nodes 组件名称旁边的复选框。

   g. 在“**实时文件保护模式**”部分，选择“**安装应用程序后启用实时文件保护(推荐)**”复选框并指定安全级别。

   h. 如有必要，请更改应用程序控制台用于远程连接到安装了应用程序的计算机的 TCP 端口号。

      使用 Windows 凭证进行连接的默认端口号为 13032，使用手动创建的用户的凭证进行连接的默认端口号为 13031。可能的端口号范围：1–65535。

      要防止与手动创建的用户账户的凭据进行连接，请清除“**使用手动创建的用户的凭证**”复选框。

   i. 要指定默认文件夹以外的安装文件夹，请在“**配置应用程序安装路径**”部分通过单击“**设置**”按钮指定文件夹名称和路径。

   j. 如果适用，请指定配置文件。

   k. 保存更改。

10. 在“**安装包**”节点中，创建一个任务，在选定的受保护设备（管理组）上远程安装 Kaspersky Industrial CyberSecurity for Nodes。配置任务设置。

    要了解创建和配置远程安装任务的详细信息，请参见 *Kaspersky Security Center 帮助*。

11. 运行 Kaspersky Industrial CyberSecurity for Nodes 远程安装任务。

Kaspersky Industrial CyberSecurity for Nodes 将安装于在任务中指定的受保护设备上。

在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作

安装 Kaspersky Industrial CyberSecurity for Nodes 后，推荐更新设备上的 Kaspersky Industrial CyberSecurity for Nodes 数据库，如果在安装 Kaspersky Industrial CyberSecurity for Nodes 之前，设备上未安装启用实时保护功能的反病毒应用程序，则还推荐对设备执行关键区域扫描。

如果安装了 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备在 Kaspersky Security Center 中属于同一个管理组，您可以使用以下方法执行这些任务：

1. 为安装了 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备组创建“数据库更新”任务。将 Kaspersky Security Center 管理服务器设置为更新源。
2. 创建状态为“*关键区域扫描*”的按需扫描组任务。Kaspersky Security Center 根据此任务的结果（而不是根据“*关键区域扫描*”任务的结果）评估组中每台受保护设备的安全状态。
3. 为受保护设备组创建新的策略。在策略属性的“**应用程序设置**”部分中，停用本地系统按需扫描任务的计划启动，并在“**运行本地系统任务**”子部分的设置中停用对管理组受保护设备的数据库更新任务。

您还可以配置有关 Kaspersky Industrial CyberSecurity for Nodes 事件的管理员通知。

通过 Kaspersky Security Center 安装应用程序控制台

有关创建安装包和远程安装任务的详细信息，请参见《Kaspersky Security Center 实施指南》。

要使用远程安装任务安装应用程序控制台，请执行下列操作：

1. 在 Kaspersky Security Center 管理控制台中，展开“**高级**”节点。
2. 展开“**远程安装**”子节点。
3. 创建安装包：
   a. 在“**安装包**”子节点的结果窗格中，单击“**创建安装包**”按钮。
   b. 在“**新建安装包向导**”窗口中，选择“**创建指定可执行文件的安装包**”作为安装包类型。
   c. 输入新安装包名称。
   d. 选择 Kaspersky Industrial CyberSecurity for Nodes 分发包文件夹中的 \client\setup_kicstool.exe 文件，然后选中“**将整个文件夹复制到安装包**”复选框。
   e. 在“**可执行文件启动设置（可选）**”字段，指定参数值 EULA=1 和 PRIVACYPOLICY=1。否则无法安装组件。
   ```
   /s /p "EULA=1 PRIVACYPOLICY=1"
   ```
   f. 如有必要，在“**可执行文件启动参数（可选）**”字段中，可以指定 ADDLOCAL 命令行参数来更改要安装的组件集，并指定 INSTALLDIR 命令行参数来指定默认文件夹以外的目标文件夹。例如，要在 C:\KasperskyConsole 文件夹中执行应用程序控制台的独立安装，请使用以下命令行选项：
   ```
   /s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
   ```
4. 在“**安装包**”子节点中，创建一个任务，在选定的受保护设备（管理组）上远程安装应用程序控制台。

5. 配置任务设置。

要了解创建和配置远程安装任务的详细信息，请参见 Kaspersky Security Center 帮助。

6. 运行远程安装任务。

应用程序控制台安装到该任务指定的受保护设备上。

通过 Kaspersky Security Center 卸载 Kaspersky Industrial CyberSecurity for Nodes

卸载 Kaspersky Industrial CyberSecurity for Nodes 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

如果网络设备上的 Kaspersky Industrial CyberSecurity for Nodes 管理受密码保护，在创建用于卸载多个应用程序的任务时请输入密码。如果密码保护未通过 Kaspersky Security Center 策略集中管理，Kaspersky Industrial CyberSecurity for Nodes 将从设备成功卸载，在该设备上输入的密码与设置值匹配。不会从其他受保护设备卸载 Kaspersky Industrial CyberSecurity for Nodes。

要卸载 Kaspersky Industrial CyberSecurity for Nodes：

1. 在 Kaspersky Security Center 管理控制台中，创建并启动应用程序删除任务。
2. 在该任务中，选择卸载方法（与选择安装方法类似，请参见上一节）并指定管理服务器将用来访问受保护设备的账户。您可以仅使用默认卸载设置卸载 Kaspersky Industrial CyberSecurity for Nodes。

使用 Kaspersky Security Center 更改应用程序组件集

“*更改应用程序组件*”任务允许您在安装应用程序后更改 Kaspersky Industrial CyberSecurity for Nodes 组件集。

如何在 Kaspersky Security Center 管理控制台中更改应用程序组件集

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”文件夹。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Industrial CyberSecurity for Nodes → 更改应用程序组件**”。

步骤 2. 更改应用程序组件的任务设置

选择将在用户计算机上可用的应用程序组件。为任务（参加下表）配置高级设置。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 配置任务启动计划

配置启动任务的计划，例如，手动或在计算机空闲时。

步骤 5. 定义任务名称

输入任务的名称，例如“*添加应用程序控制组件*”。

步骤 6. 完成任务创建

完成向导操作。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 中更改应用程序组件集

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**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes 4.5.0**”。
2. 在“**任务类型**”下拉列表中，选择“**更改 Kaspersky Industrial CyberSecurity for Nodes 组件**”。

3. 在“**任务名称**”字段中，输入简要说明，例如，“*添加应用程序控制组件*”。

4. 在“**要对其分配任务的设备**”块，选择任务范围。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。例如，选择单独的管理组或构建一个选项。

步骤 3. 完成任务创建

1. 选择“**创建完成时打开任务详情**”复选框并完成向导。

2. 在任务属性中，选择“**应用程序设置**”选项卡。

3. 选择将在用户计算机上可用的应用程序组件。为任务（参加下表）配置高级设置。

结果，用户计算机上的 Kaspersky Industrial CyberSecurity for Nodes 组件集将在静默模式下更改。

高级任务设置

参数	描述
工业软件排除项配置文件	对于“*更改应用程序组件*”任务，您只能将扫描排除项和受信任的应用程序添加到受信任区域。
使用密码修改应用程序组件集	管理员通常启用密码保护以限制对 Kaspersky Industrial CyberSecurity for Nodes 的访问。也就是说，要修改应用程序组件的选择，您必须输入具有**卸载/修改/恢复应用程序**权限的用户的凭据。例如，您可以使用 KL Admin 账户。

通过 Active Directory 组策略安装和卸载应用程序

本节介绍如何通过 Active Directory 组策略安装和卸载 Kaspersky Industrial CyberSecurity for Nodes，以及有关通过组策略安装 Kaspersky Industrial CyberSecurity for Nodes 后必须执行的操作的信息。

通过 Active Directory 组策略安装 Kaspersky Industrial CyberSecurity for Nodes

您可以通过 Active Directory 组策略在多台受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes。您可以用相同的方式安装应用程序控制台。

要安装 Kaspersky Industrial CyberSecurity for Nodes 或应用程序控制台的受保护设备必须在同一个域中和一个组织单元中。

要使用策略安装 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备的操作系统必须为相同的位数（32 位或 64 位）。

您必须具有域管理员权限。

以使用 kics_win.msi 安装包安装 Kaspersky Industrial CyberSecurity for Nodes。以安装应用程序控制台，使用 kicstools.msi 安装包。

有关使用 Active Directory 组策略的详细信息，提供在 Microsoft 提供的文档中。

要安装 Kaspersky Industrial CyberSecurity for Nodes 或应用程序控制台：

1. 将 kics_win.msi 保存到域控制器上的共享文件夹。
2. 将密钥文件保存在域控制器上的同一公共文件夹中。
3. 在域控制器上的同一共享文件夹中，创建包含以下行的 install_props.json 文件。这表示您同意最终用户授权许可协议和隐私策略的条款。

```
{
"EULA": "1",
"PRIVACYPOLICY": "1"
}
```

4. 在域控制器上，为受保护设备所属的组创建新策略。
5. 使用“**组策略对象编辑器**”，在“**计算机配置**”节点中创建新的安装包。以 UNC 格式（通用命名约定）指定 Kaspersky Industrial CyberSecurity for Nodes（或应用程序控制台） msi 文件的路径。
6. 在选定组的“**计算机配置**”节点和“**用户配置**”节点中，选中 Windows Installer 的“**始终使用提升的权限安装**”复选框。
7. 使用 `gpupdate / force` 命令应用更改。

Kaspersky Industrial CyberSecurity for Nodes 将在该组的受保护设备重新启动后安装到这些设备上。

在安装 Kaspersky Industrial CyberSecurity for Nodes 后执行的操作

在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes 后，推荐您立即更新应用程序数据库并运行关键区域扫描。您可以从应用程序控制台执行这些操作。

您还可以配置有关 Kaspersky Industrial CyberSecurity for Nodes 事件的管理员通知。

通过 Active Directory 组策略卸载 Kaspersky Industrial CyberSecurity for Nodes

卸载 Kaspersky Industrial CyberSecurity for Nodes 时不会删除 dump 和跟踪文件。您可以手动删除在配置 dump 和跟踪文件写入期间指定的文件夹中的 dump 和跟踪文件。

如果在受保护设备组中使用了 Active Directory 组策略安装 Kaspersky Industrial CyberSecurity for Nodes（或应用程序控制台），则可以使用该策略卸载 Kaspersky Industrial CyberSecurity for Nodes（或应用程序控制台）。

您可以仅使用默认卸载参数卸载应用程序。

有关使用 Active Directory 组策略的详细信息，提供在 Microsoft 提供的文档中。

如果应用程序管理受密码保护，则无法使用 Active Directory 组策略卸载 Kaspersky Industrial CyberSecurity for Nodes。

要卸载 Kaspersky Industrial CyberSecurity for Nodes（或应用程序控制台）：

1. 在域控制器上，从要卸载 Kaspersky Industrial CyberSecurity for Nodes 或应用程序控制台的受保护设备中选择组织单元。
2. 在“**组策略编辑器**”中选择为安装 Kaspersky Industrial CyberSecurity for Nodes 所创建的策略，在“**软件安装**”节点（“**计算机配置** > **软件设置** > **软件安装**”）中打开 Kaspersky Industrial CyberSecurity for Nodes （或应用程序控制台）安装包的上下文菜单，然后选择“**所有任务** > **删除**”命令。
3. 选择卸载方法“**立即从用户处和计算机中卸载软件**”。
4. 使用 `gpupdate /force` 命令应用更改。

Kaspersky Industrial CyberSecurity for Nodes 将在受保护设备重启后和登录 Microsoft Windows 前从受保护设备中删除。

Kaspersky Industrial CyberSecurity for Nodes 安装和卸载日志

如果使用安装（卸载）向导安装（卸载）Kaspersky Industrial CyberSecurity for Nodes 或应用程序控制台，Windows Installer 服务会创建安装（卸载）日志。一个名为 kl-install-<uid>.log（其中 <uid> 是唯一的 8 字符日志标识符）的日志文件将保存在用于启动 setup_kics.exe 或 setup_kicstool.exe 文件的账户所属用户的 %temp% 文件夹中。

默认情况下，如果从命令行安装或卸载 Kaspersky Industrial CyberSecurity for Nodes，将不会创建安装日志文件。

要安装 Kaspersky Industrial CyberSecurity for Nodes 并在磁盘 C:\ 上创建日志文件，请执行以下命令：

```
msiexec /i kics_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

Kaspersky Industrial CyberSecurity for Nodes 安装后的系统更改

当 Kaspersky Industrial CyberSecurity for Nodes 和“管理工具”集（包括应用程序控制台）同时安装时，Windows Installer 服务将对受保护设备进行以下修改：

- 在受保护设备和安装了应用程序控制台的设备上创建 Kaspersky Industrial CyberSecurity for Nodes 文件夹。
- 注册 Kaspersky Industrial CyberSecurity for Nodes 服务。
- 创建 Kaspersky Industrial CyberSecurity for Nodes 用户组。
- 在系统注册表中注册 Kaspersky Industrial CyberSecurity for Nodes 项。
- 创建了 Windows 任务计划程序中显示的“Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect”系统任务。

下文介绍了这些更改。

受保护设备上的 Kaspersky Industrial CyberSecurity for Nodes 文件夹

安装 Kaspersky Industrial CyberSecurity for Nodes 后，受保护设备上会创建以下文件夹：

- Kaspersky Industrial CyberSecurity for Nodes 默认安装文件夹，其中包含 Kaspersky Industrial CyberSecurity for Nodes 可执行文件。默认使用以下安装文件夹：

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0

- Management Information Base (MIB) 文件，其中包含 Kaspersky Industrial CyberSecurity for Nodes 通过 SNMP 协议发布的计数器和挂钩的说明：

  %ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0\mibs

- Kaspersky Industrial CyberSecurity for Nodes 服务文件：
  - %ProgramData%\Kaspersky Lab\KICS.4.5\Data
  - %ProgramData%\Kaspersky Lab\KICS.4.5\Settings
  - %ProgramData%\Kaspersky Lab\KICS.4.5\Dskm
- 具有更新源设置的文件：

  %ProgramData%\Kaspersky Lab\KICS.4.5\Data

- 使用“*更新*”任务下载的数据库和软件模块更新（该文件夹将在第一次使用“*更新*”任务下载更新时创建）。

  %ProgramData%\Kaspersky Lab\KICS.4.5\Update distribution

- 任务日志和系统审核日志：

  %ProgramData%\Kaspersky Lab\KICS.4.5\Reports

- 当前使用的数据库集：
  %ProgramData%\Kaspersky Lab\KICS.4.5\Bases
- 数据库的备份副本；每次更新数据库时都将覆盖这些副本：
  %ProgramData%\Kaspersky Lab\KICS.4.5\QB
- 在执行更新任务过程中创建的临时文件：
  %ProgramData%\Kaspersky Lab\KICS.4.5\Data\temp\temporaryFolder
- 隔离的对象（默认文件夹）：
  %ProgramData%\Kaspersky Lab\KICS.4.5\QB
- 备份中的对象（默认文件夹）：
  %ProgramData%\Kaspersky Lab\KICS.4.5\QB
- 从备份和隔离还原的对象（用于还原对象的默认的文件夹）：
  %ProgramData%\Kaspersky Lab\KICS.4.5\QB\Restored

在应用程序控制台安装过程中创建的文件夹

应用程序控制台默认安装文件夹，其中包含“管理工具”文件，具体取决于操作系统位集。默认使用以下安装文件夹：

%ProgramFiles%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes Admins Tools.4.5.0

Kaspersky Industrial CyberSecurity for Nodes 组

“KICS 管理员”是受保护设备上的组，其中的用户对 Kaspersky Security Management 服务和所有 Kaspersky Industrial CyberSecurity for Nodes 功能拥有完全访问权限。

系统注册表键

安装 Kaspersky Industrial CyberSecurity for Nodes 后，将创建以下系统注册表项：

- Kaspersky Industrial CyberSecurity for Nodes 设置：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.KICS.4.5]
- Kaspersky Industrial CyberSecurity for Nodes 事件日志 (Kaspersky Event Log) 参数：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Industrial CyberSecurity for Nodes]
- 跟踪文件设置：
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.4.5\Trace]
- 应用程序任务和功能的设置：
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.4.5\environment]

Kaspersky Industrial CyberSecurity for Nodes 操作系统升级检测系统任务

Windows Installer 服务在应用程序安装期间创建 Kaspersky Industrial CyberSecurity for Nodes OS Upgrade Detect 任务。该任务在创建后立即启动，以后在每次操作系统启动时启动。该任务检查应用程序使用的驱动程序版本：如果操作系统版本已更新，应用程序会更新相应操作系统版本的驱动程序。

该任务不会影响应用程序，可以删除。我们建议牢记操作系统升级方案。

Kaspersky Industrial CyberSecurity for Nodes 进程

Kaspersky Industrial CyberSecurity for Nodes 将启动下表中描述的进程。

Kaspersky Industrial CyberSecurity for Nodes 进程

文件名	用途
avp.exe	Kaspersky Industrial CyberSecurity for Nodes 工作流
avpsus.exe	此过程允许安装和回滚关键且已批准的应用程序模块更新。

检查 Kaspersky Industrial CyberSecurity for Nodes 功能。使用 EICAR 测试病毒

本节介绍 EICAR 测试病毒以及如何使用 EICAR 测试病毒检查 Kaspersky Industrial CyberSecurity for Nodes 的实时文件保护和按需扫描功能。

关于 EICAR 测试病毒

测试病毒的用途是验证反病毒应用程序的运行情况。它由欧洲计算机反病毒研究协会 (EICAR) 开发。

> 测试病毒不是恶意对象，不包含针对设备的可执行代码，但大部分供应商的反病毒应用程序将它识别为威胁。

包含该测试病毒的文件被称为 eicar.com。您可以从 EICAR 网站下载该文件。

> 在将该文件保存在设备硬盘驱动器上的文件夹之前，确保已在该驱动器上禁用实时文件保护。

eicar.com 文件包含一个文本行。在扫描该文件时，Kaspersky Industrial CyberSecurity for Nodes 会检测该文本行中的测试威胁，向该文件分配“**被感染**”状态并删除它。有关在该文件中检测到的威胁的信息，将显示在应用程序控制台和任务日志中。

您可以使用 eicar.com 文件来检查 Kaspersky Industrial CyberSecurity for Nodes 如何清除感染对象以及如何检测可能已感染对象。要执行此操作，请使用文本编辑器打开该文件，将以下表格中列出的其中一个前缀添加到文件中文本行的开头，并将该文件保存为新的名称，例如 eicar_cure.com。

为确保 Kaspersky Industrial CyberSecurity for Nodes 处理带有前缀的 eicar.com 文件，在“**对象保护**”安全设置部分中，为 Kaspersky Industrial CyberSecurity for Nodes 的“实时计算机保护”任务和“默认按需扫描”任务设置“**所有对象**”值。

EICAR 文件中的前缀

前缀	扫描后的文件状态和 Kaspersky Industrial CyberSecurity for Nodes 操作
无前缀	**Kaspersky Industrial CyberSecurity for Nodes 向对象分配“被感染”状态并删除它。**
SUSP-	Kaspersky Industrial CyberSecurity for Nodes 向启发式分析检测到的对象分配“**疑似被感染**”状态并删除它，因为不会清除可能已感染对象。
WARN-	Kaspersky Industrial CyberSecurity for Nodes 向对象（对象的代码与已知威胁的代码部分匹配）分配“**疑似被感染**”状态并删除它，因为不会清除可能已感染对象。
CURE-	Kaspersky Industrial CyberSecurity for Nodes 向对象分配“**被感染**”状态并清除它。如果成功清除，则文件中的全部文本将用“CURE”一词代替。

检查实时文件保护和按需扫描功能

安装 Kaspersky Industrial CyberSecurity for Nodes 后，您可以确认 Kaspersky Industrial CyberSecurity for Nodes 检测包含恶意代码的对象。为此，请使用 EICAR 测试病毒。

要检查“实时文件保护”功能：

1. 从 EICAR 网站 下载 eicar.com 文件。将它保存到网络中任一设备的本地驱动器上的共享文件夹中。

   在将该文件保存到文件夹之前，请确保对该文件夹禁用实时文件保护。

2. 如果要检查网络用户通知是否正常工作，请确保受保护设备和保存 eicar.com 文件的设备均启用了 Microsoft Windows Messenger 服务。

3. 在受保护设备上打开应用程序控制台。

4. 使用以下其中一种方法，将保存的 eicar.com 文件复制到受保护设备的本地驱动器上：

   - 若要通过“终端服务”窗口进行通知测试，请在使用远程桌面连接实用程序连接到受保护设备后，将 eicar.com 文件复制到受保护设备。
   - 若要通过“Microsoft Windows Messenger 服务”进行通知测试，请使用设备的网络位置从您保存 eicar.com 文件的设备复制它。

如果满足以下条件，则“实时文件保护”正常工作：

- eicar.com 文件已从受保护设备删除。
- 在应用程序控制台中，任务日志的状态为“*严重*”。日志中新增一行有关 eicar.com 文件中的威胁的信息。

- 以下 Microsoft Windows Messenger 服务消息将出现在您从中复制文件的设备上：Kaspersky Industrial CyberSecurity for Nodes 在 <发生事件的时间> 阻止了对计算机 <设备的网络名称> 上的 <设备上的文件的路径>\eicar.com 的访问。Reason: Threat detected.病毒：EICAR-Test-File。User name: <user name>.Computer name: <network name of the device from which you copied the file>.

  确保 Microsoft Windows Messenger 服务在从中复制 eicar.com 文件的设备上运行。

要检查按需扫描功能：

1. 从 EICAR 网站 下载 eicar.com 文件。将它保存到网络中任一设备的本地驱动器上的共享文件夹中。

   在将该文件保存到文件夹之前，请确保对该文件夹禁用实时文件保护。

2. 打开应用程序控制台并展开应用程序控制台树中的“**按需扫描**”节点。
3. 选择“**关键区域扫描**”子节点。
4. 添加“**所有网络驱动器**”到“按需扫描”任务的范围。
5. 运行“关键区域扫描”任务。

如果满足以下条件，则按需扫描正常运行：

- eicar.com 文件已从设备的硬盘驱动器中删除。
- 在应用程序控制台中，任务日志的状态为“*严重*”。“按需扫描”任务日志中新增一行有关 eicar.com 文件中的威胁的信息。

将旧版本的 Kaspersky Industrial CyberSecurity for Nodes 升级至 4.5 版

将旧版本的 Kaspersky Industrial CyberSecurity for Nodes 升级到 4.5 版本时，请遵循以下建议：

- 提前计划并安排升级。选择服务器在最轻负载下运行的时间，例如周末。
- 升级完成后，逐个开启应用程序组件。即，例如，首先单独启用实时文件保护组件，然后启用其他防护组件，再启用控制组件，依此类推。我们建议在每个步骤中测试该应用程序。
- 逐步进行升级。首先升级单台计算机，然后升级多台计算机，最后升级组织的所有计算机。

升级过程的步骤

按照以下顺序将 Kaspersky Industrial CyberSecurity for Nodes 升级至版本 4.5：

1. **升级 Kaspersky Security Center**

   将所有 Kaspersky Security Center 组件升级到版本 14.2 或更高版本，包括用户计算机上的网络代理和 Kaspersky Security Center Web Console。

2. **升级 Kaspersky Industrial CyberSecurity for Nodes Web 插件**

   在 Kaspersky Security Center Web Console 中，将 Kaspersky Industrial CyberSecurity for Nodes Web 插件升级到版本 4.5。

3. **迁移 Kaspersky Industrial CyberSecurity for Nodes 任务和策略**

   迁移策略和任务后，您必须迁移向导无法迁移的配置，而这在旧版本的应用程序中并不存在。我们还建议检查迁移向导是否正确迁移了所有设置。

4. **安装 Kaspersky Industrial CyberSecurity for Nodes 4.5**

   Kaspersky Industrial CyberSecurity for Nodes 版本 4.5 使用 HTTPS 协议而不是 DCOM 协议。因此，在安装新版本的 Kaspersky Industrial CyberSecurity for Nodes 之前，需要配置将在其上更新应用程序的设备，以启用 KICS 服务的远程启动。如果不进行这样的配置，远程服务将无法启动。

   您可以在删除该应用程序的早期版本后或在其基础上安装 Kaspersky Industrial CyberSecurity for Nodes 4.5。

   在旧版本的应用程序上安装时，将安装同一组应用程序组件，同时考虑到部分组件的新名称和内容。

   当远程安装时，安装程序会安装您在安装包的属性中选择的组件。

5. **如果有必要，激活 Kaspersky Industrial CyberSecurity for Nodes 4.5**

   在旧版本的应用程序上安装 Kaspersky Industrial CyberSecurity for Nodes 4.5 时，当前授权许可将自动应用于该应用程序，并且新的应用程序组件和任务完全可用。授权许可期限保持不变。

6 确保应用程序正常运行

升级 Kaspersky Industrial CyberSecurity for Nodes 后，请确保应用程序正常运行。确保应用程序没有报告任何错误，还要检查最后一次连接到管理服务器的时间、最后一次更新的时间和计算机保护状态。

注意排除项列表、受信任的应用程序、设备控制规则和应用程序启动控制规则的迁移。

更新 Kaspersky Industrial CyberSecurity for Nodes

支持从版本 3.2 或更高版本升级到 Kaspersky Industrial CyberSecurity for Nodes 4.5。要从应用程序更早版本更新，您必须删除已安装的版本并安装版本 4.5。

更新是通过在已安装的应用程序版本上安装新版本的应用程序来执行的，不需要重新启动计算机。

默认情况下，应用程序会根据现有应用程序安装文件夹的路径以新应用程序版本的名称创建新的安装文件夹。您可以手动指定新的应用程序安装文件夹路径。

将 Kaspersky Industrial CyberSecurity for Nodes 升级到版本 4.5 时，先前安装的应用程序版本将被自动删除。

更新受密码保护的 Kaspersky Industrial CyberSecurity for Nodes 安装时，请通过以下方式之一将密码传递给安装程序：

- 如果通过安装向导界面或在交互式 CLI 模式下进行本地安装，请在系统要求输入密码时指定密码。
- 如果在非交互式 CLI 模式下进行本地安装，请在 `UNLOCK_PASSWORD` 项中指定密码。
- 如果使用 Active Directory 组策略安装，请在 install_props.json 配置文件中指定 `UNLOCK_PASSWORD` 键的值。

当您通过 Kaspersky Security Center 远程升级的应用程序受密码保护时，您必须首先使用 Kaspersky Security Center 策略禁用密码保护。

更新应用程序时，当前授权许可将自动应用于 Kaspersky Industrial CyberSecurity for Nodes 版本 4.5，并且新的应用程序组件和任务完全可用。授权许可期限保持不变。

如果使用过期的授权许可更新应用程序，则新版本的应用程序在安装后将以有限功能模式运行（例如，应用程序数据库更新不可用）。

更新 Kaspersky Industrial CyberSecurity for Nodes 管理工具

您只能将使用 Kaspersky Security Center 管理应用程序的管理插件从 3.2、4.0 或更高版本更新至 4.5 版本。要更新管理插件和应用程序控制台的早期版本，必须删除已安装的版本，然后安装 4.5 版。

更新期间，新版本的管理插件将安装在以前安装的版本旁边，并且不需要重新启动计算机。

有关迁移管理插件设置的信息，请参阅此文章。

迁移策略和任务

您可以通过以下方式将应用程序先前版本的策略和任务设置迁移到 4.5 版本：

- 使用策略和任务批量转换向导（仅在 Kaspersky Security Center 管理控制台中可用）。
- 使用 Kaspersky Industrial CyberSecurity for Nodes 4.5 策略和任务迁移向导（仅在 Kaspersky Security Center Web Console 中可用）。

建议首先在一台计算机上迁移 Kaspersky Industrial CyberSecurity for Nodes 策略和任务，然后在一组计算机上进行迁移，然后在组织的所有计算机上完成迁移。

如何使用策略和任务批量转换向导迁移策略和任务设置

1. 在 Kaspersky Security Center 管理控制台中，选择管理服务器并打开上下文菜单。
2. 选择“**所有任务**” → “**策略和任务批量转换向导**”。

   这将启动策略和任务批量转换向导。按照向导的说明进行操作。

步骤 1. 选择您要转换其策略和任务的应用程序

选择 Kaspersky Industrial CyberSecurity for Nodes 4.5。转到下一步。

步骤 2. 策略转换

选择您想要为 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建的要升级的应用程序版本的策略。

步骤 3. 使用 Kaspersky Endpoint Agent 进行迁移

如有必要，请针对您在向导上一步中选择的每个 Kaspersky Industrial CyberSecurity for Nodes 策略逐一选择要将其设置添加到新的 Kaspersky Industrial CyberSecurity for Nodes 4.5 策略中的 Kaspersky Endpoint Agent 策略。转到下一步。

步骤 4. 任务转换

选择您想要为 Kaspersky Industrial CyberSecurity for Nodes 4.5 转换的正在升级的应用程序版本的组任务。

非组任务（前两个选项在任务向导的“**选择要对其分配任务的设备**”窗口中选择）不会在当前步骤中显示。

要将非组任务从您的应用程序版本转换为 Kaspersky Industrial CyberSecurity for Nodes 4.5：

1. 单击“**下一步**”。
   “**附加迁移计划和任务**”窗口将打开。
2. 选择**迁移非组任务**复选框。
3. 指定 Kaspersky Security Center 管理服务器的连接设置。
4. 单击“**确定**”。

步骤 5. 向导完成

完成向导操作。因此，向导会执行以下操作：

- 针对 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建了新策略。
  新策略包含选定的 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Endpoint Agent 策略的设置以及 Kaspersky Industrial CyberSecurity for Nodes 4.5 中引入的新设置。新策略的名称与转换前的 Kaspersky Industrial CyberSecurity for Nodes 策略名称相同，但添加了“（已转换）”。新策略具有“*非活动策略*”状态。
- 为 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建新的任务。
  新任务包含所选 Kaspersky Industrial CyberSecurity for Nodes 任务的设置以及 Kaspersky Industrial CyberSecurity for Nodes 4.5 中引入的新设置。新任务的名称与转换前的 Kaspersky Industrial CyberSecurity for Nodes 任务名称相同，但添加了“（转换）”。
- 选择转换的策略和任务保持不变。

如何使用迁移向导迁移策略和任务设置

在 Web Console 或云控制台的主窗口中，选择“**操作 → 迁移到 Kaspersky Industrial CyberSecurity for Nodes 4.5.0**”。

这将运行策略和任务迁移向导。按照向导的说明进行操作。

步骤 1. 策略迁移

选择 Kaspersky Industrial CyberSecurity for Nodes，如果需要，还选择要合并其设置的 Kaspersky Endpoint Agent 策略。

确保选择了正确的策略，然后转到下一步。

步骤 2. 任务迁移

选择您想要为 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建的 Kaspersky Industrial CyberSecurity for Nodes 任务。

转到下一步。

步骤 3. 向导完成

完成向导操作。因此，向导会执行以下操作：

- 针对 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建了新策略。

  新策略包含迁移的 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Endpoint Agent 策略的设置，以及 Kaspersky Industrial CyberSecurity for Nodes 4.5 中引入的新设置。新策略的名称与合并前的 Kaspersky Industrial CyberSecurity for Nodes 策略的名称相同，并添加了“从 KICS 复制”短语。新策略具有“*非活动策略*”状态。

- 为 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建新的任务。

  新任务包含迁移的 Kaspersky Industrial CyberSecurity for Nodes 任务的设置以及 Kaspersky Industrial CyberSecurity for Nodes 4.5 中引入的新设置。新任务的名称与迁移前的 Kaspersky Industrial CyberSecurity for Nodes 任务名称相同，并添加了“从 KICS 复制”短语。

正在更新的应用程序版本的设置迁移

将应用程序及其管理插件升级到 4.5 版后，以下内容将无更改地迁移：

- 组件和任务的设置（重置为默认值的设置和在“设置和组件迁移的限制”下列出的设置除外）
- 任务日志和系统审计日志，以及 Windows 事件日志中的记录
- 任务通知设置
- 启动任务的用户账户
- 应用程序管理的用户访问权限
- 代理服务器连接密码
- Kaspersky Security Center 策略中 属性的状态。

升级应用程序和其插件到版本 4.5 后，以下设置将重置或设置为新版本应用程序的默认值：

- 所有计数器，包括反病毒数据库状态
- 有关已安装的应用程序模块更新和反病毒数据库的数据
- 任务状态
- Kaspersky Security 服务的管理权限
- 通过注册表配置的应用程序和任务设置
- 在安装关键修复期间更改的应用程序和任务设置
- 事件配置
- 向 Kaspersky Security Center 管理服务器传输数据的设置 - 默认情况下，所有数据的传输均已启用

- 跟踪和转储设置
- 应用程序本地任务的设置，位于“**通知**”选项卡。

您正在更新的应用程序版本中不存在的设置将获取默认值。

设置和组件迁移的限制

- 正在升级的版本的隔离区内容被移至 4.5 版本的备份中。升级后，备份的最大大小设置为正在升级的应用程序的备份和隔离区的最大大小之和；可用空间阈值会相应更新。同时，备份的默认最大大小增加至 400 Mb，可用空间阈值增加至 100 MB。
- Kaspersky Industrial CyberSecurity for Nodes 4.0 设置“**隔离区文件夹**”、“**备份文件夹**”和“**用于恢复对象的文件夹**”不存在于 Kaspersky Industrial CyberSecurity for Nodes 4.5 及更高版本中，因此它们不会被迁移。同样，旧版本中存在但新版本中不存在的其他设置也不会迁移。
- 当将 [KICS+KEA] 配置迁移到 [KICS+内置代理]时，Kaspersky Endpoint Agent 隔离区的内容将迁移至 Kaspersky Industrial CyberSecurity for Nodes 4.5 隔离区。
- 客户端计算机的被阻止的网络会话列表不被迁移。同时，在应用程序升级后，自动解除阻止访问被阻止的网络文件资源的设置保持不变。
- 密码保护设置未迁移。在 Kaspersky Industrial CyberSecurity for Nodes 4.5 中，密码保护发生了重大变化。如有需要，开启密码保护并设置密码。
- 信任区域：
  - 在 Kaspersky Industrial CyberSecurity for Nodes 4.5 版中，选择受信任区域对象的方法已经改变。可以迁移定义为单个文件或文件或文件夹路径的排除项。定义为预定义范围 (例如，硬盘驱动器) 或脚本 URL 的排除项不会被迁移。迁移后，您必须手动添加此类排除项。
  - 预定义的扫描排除项和受信任的应用程序已添加到受信任区域，有助于在服务器上设置应用程序及其与工业软件的交互。
- 应用程序控制和设备控制组件已经经过重大改造。升级版本的组件设置将根据 Kaspersky Industrial CyberSecurity for Nodes 4.5 中的新设置结构进行迁移。
- 正在升级的应用程序版本的文件完整性监控和注册表访问监控组件的设置将迁移到系统完整性监控组件的设置。
- “防火墙管理”组件已重新设计为“防火墙”组件，除了与 Windows 防火墙交互之外，现在还可以充当防火墙。完成迁移后，您必须从头开始配置组件模式。
- 要使用 KSN，您必须再次阅读并接受 KSN 声明。
- 应用程序的 4.5 及更高版本不支持调度单个组件。如果启用这些组件，它们会在应用程序运行时继续运行。
- 在迁移任务时，任务的计划开始时间会偏移与执行迁移的计算机的操作系统设置中配置的时区数相匹配的小时数。例如，假设旧版本应用程序中任务的开始时间是 7:00，而操作系统配置的时区是 UTC+3:00。然后，任务迁移后，开始时间更改为 10:00。
- 实时文件保护组件和按需扫描任务的设置中已删除设置对可能被感染的对象执行的操作的部分。这些设置不会迁移到较新的应用程序版本。

- 如果您正在使用该应用程序 4.5 或更高版本作为 EDR Optimum 解决方案的一部分，为了管理警报详细信息，您必须将 Endpoint Detection and Response 的 Web 插件升级到 15.1 或更高版本。否则，如果您安装了 Kaspersky Endpoint Agent Web 插件，使用此 Web 插件打开的事故卡中的威胁发展链可能包含有限的数据或错误。

- 如果隔离和备份对象是在应用程序 4.0 或更早版本升级到 4.5 或更高版本后迁移的，或者这些对象是由 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Industrial CyberSecurity for Networks 放置在存储中的，则 Kaspersky Security Center Web Console 或管理控制台不能用于将隔离和备份对象发送到卡巴斯基进行分析。

- 迁移按需扫描任务时，预定义扫描范围的默认安全级别将从“*通知*”更改到“*自定义*”。

- 发送给 SIEM 的事件现在使用新的日期和时间格式。在以前版本的 Kaspersky Industrial CyberSecurity for Nodes 中，事件是使用时间戳生成的。现在，应用程序使用 `<DATE-TIME>` 格式的日期和时间生成事件。如有必要，重新配置 SIEM 交互，以将日期和时间转换为时间戳格式。

Kaspersky Industrial CyberSecurity for Nodes 版本 4.0 和 4.5 中的组件和任务对应关系

将 Kaspersky Industrial CyberSecurity for Nodes 4.0 升级到 4.5 版本时，仅当应用程序在本地安装时才会迁移组件和任务集。

Kaspersky Industrial CyberSecurity for Nodes 版本 4.0 和 4.5 中的组件对应关系

Kaspersky Industrial CyberSecurity for Nodes 4.0 组件	**Kaspersky Industrial CyberSecurity for Nodes 4.5 组件**
信任区域	受信任区域
实时文件保护	实时文件保护
KSN 使用	KSN 使用
漏洞利用防御	漏洞利用防御
网络威胁防护	网络威胁防护
AMSI 扫描程序	AMSI 保护
应用程序启动控制	应用程序启动控制
设备控制	设备控制
Wi-Fi 控制	设备控制 “Wi-Fi 控制”组件的功能已合并到“设备控制”组件中。
防火墙管理	防火墙 Windows 防火墙充当 Kaspersky Industrial CyberSecurity for Nodes 4.0 的防火墙，而应用程序则管理 Windows 防火墙。在 Kaspersky Industrial CyberSecurity for Nodes 4.5 中，一个单独的组件负责防火墙功能。
反加密	反加密勒索
文件完整性监控	系统完整性监控 “文件完整性监控”和“注册表访问监控”组件的功能已合并到“系统完整性监控”组件。
日志审查	日志审查
注册表访问监控	系统完整性监控 “文件完整性监控”和“注册表访问监控”组件的功能已合并到“系统完整性监控”组件。
便携式扫描程序	便携式扫描程序
（没有任何）	修复引擎

Kaspersky Industrial CyberSecurity for Nodes 4.0 组件	Kaspersky Industrial CyberSecurity for Nodes 4.5 组件
(没有任何)	与 KICS for Networks 整合 充当 Kaspersky Endpoint Agent 的组件。
(没有任何)	SIEM 整合 充当 Kaspersky Endpoint Agent 的组件。
(没有任何)	Managed Detection and Response 充当 Kaspersky Endpoint Agent 的组件。
(没有任何)	KATA 整合 充当 Kaspersky Endpoint Agent 的组件。
(没有任何)	Endpoint Detection and Response (Industrial CyberSecurity)
(没有任何)	使用 Sigma 规则的异常检测 充当 Kaspersky Endpoint Agent 的组件。
Kaspersky Industrial CyberSecurity for Nodes 4.0 的任务	**Kaspersky Industrial CyberSecurity for Nodes 4.5 的任务**
应用程序激活	应用程序激活
复制更新	更新 复制更新任务的功能已合并到更新任务中。
基线文件完整性监控	基线系统完整性监控
数据库更新	更新 数据库更新任务的功能已合并到更新任务中。
软件模块更新	更新 软件模块更新任务的功能已合并到更新任务中。
回滚应用程序数据库更新	更新回滚
按需扫描	按需扫描
应用程序完整性控制	应用程序完整性控制
应用程序启动控制规则生成器	应用程序启动控制规则生成器
设备控制规则生成器	设备控制规则生成器
(没有任何)	管理服务器连接保护
(没有任何)	更改 Kaspersky Industrial CyberSecurity for Nodes 组件
(没有任何)	安全审计 实现 Kaspersky Endpoint Agent 功能的任务。
(没有任何)	终止进程 实现 Kaspersky Endpoint Agent 功能的任务。
(没有任何)	启动进程 实现 Kaspersky Endpoint Agent 功能的任务。
(没有任何)	IOC 扫描 实现 Kaspersky Endpoint Agent 功能的任务。
(没有任何)	获取文件 实现 Kaspersky Endpoint Agent 功能的任务。
(没有任何)	移动文件到隔离区 实现 Kaspersky Endpoint Agent 功能的任务。
(没有任何)	删除文件 实现 Kaspersky Endpoint Agent 功能的任务。

安装和删除 Kaspersky Security Gateway

本节提供安装和删除 Kaspersky Security Gateway 的说明。

更新 Kaspersky Security Gateway

更新是通过在应用程序现有版本之上安装新版本来执行的，不需要重新启动计算机。

将 Kaspersky Security Gateway 升级到版本 4.5 时，先前安装的应用程序版本将被自动删除。

先前安装的 Kaspersky Security Gateway 版本的设置值将原封不动地传输至 Kaspersky Security Gateway 4.5。

使用安装向导安装 Kaspersky Security Gateway

要安装 Kaspersky Security Gateway，

运行包含在分配套件中的 security_gateway.msi 文件。

相应的向导将指导您完成安装。按照向导的说明进行操作。

Kaspersky Security Gateway 安装向导的界面由一系列窗口（步骤）组成。要在安装向导的窗口之间移动，请使用“**< 上一步**”和“**下一步 >**”按钮。完成后要关闭安装向导，请点击“**完成**”按钮。要在安装过程的任何阶段退出安装向导，请单击“**取消**”按钮。

步骤 1. 验证安装要求

如果检测到的应用程序中存在旧版本的 Kaspersky Security Gateway，安装向导将自动删除旧版本并安装新版本的 Kaspersky Security Gateway。

如果安装了 Kaspersky Security Gateway 2.0 或更早版本，安装向导将不会删除旧版本并且会取消安装。在安装 Kaspersky Security Gateway 4.5 之前，请手动删除 Kaspersky Security Gateway 2.0 或任何早期版本。

在安装或升级 Kaspersky Security Gateway 之前，安装向导将验证是否满足以下要求：

- 计算机和安装的软件满足硬件和软件要求。
- 用户账户具有安装应用程序所需的权限。

如果不满足以上任何要求，系统将在计算机屏幕上显示相关通知，且安装进程将被终止。

步骤 2. 安装程序的欢迎页面

如果您安装 Kaspersky Security Gateway 的计算机完全满足硬件和软件要求，则会打开安装过程的欢迎页面。欢迎页面宣布开始在计算机上安装 Kaspersky Security Gateway。

继续执行向导的下一步。

步骤 3. 查看最终用户授权许可协议和隐私策略

在此步骤中，您必须阅读卡巴斯基最终用户授权许可协议和隐私策略。

如果您同意最终用户授权许可协议和隐私策略的条款和条件，请选择“**I accept the terms of the End User License Agreement**”和“**I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy**”复选框。

如果您不接受最终用户授权许可协议和/或隐私策略，安装将中止。

继续执行向导的下一步。

步骤 4. 选择目标文件夹

在此步骤中，您必须指定安装 Kaspersky Security Gateway 的目标文件夹的路径。要选择目标文件夹，请单击“**浏览**”按钮。

继续执行向导的下一步。

步骤 5. 选择组件

在此步骤中，您可以选择要安装的 Kaspersky Security Gateway 组件。默认选择安装所有组件。

要选择想要安装的组件，请单击组件名称旁边的图标以调出上下文菜单。然后选择“**Feature will be installed on the local hard drive**”或者“**Entire feature and its subfeatures will be installed on local hard drive**”。有关所选组件执行哪些任务以及安装该组件需要多少磁盘空间的详细信息，请参阅当前安装向导页面的下部。

要查看本地硬盘可用空间的详细信息，请单击“**Volume**”按钮。信息显示在打开的“**Disk Space Requirements**”窗口。

要取消组件安装，请在上下文菜单中选择“**Feature will be unavailable**”选项。

要返回默认安装的组件列表，请点击“**重置**”按钮。

继续执行向导的下一步。

步骤 6. 配置与 SCADA 系统的连接

在此步骤中，您需要指定 SCADA 连接设置：

- 对于 IEC 60870-5-104 连接：将安装 Kaspersky Security Gateway 的计算机的地址（1 到 65535 之间的数字）和 TCP 端口（1 到 65535 之间的数字）。
- 对于 OPC UA 连接：将安装 Kaspersky Security Gateway 的计算机的 TCP 端口（从 1 到 65535 的数字）。

要安装该程序，请单击“**安装**”按钮。

在计算机上安装 Kaspersky Security Gateway 时，当前网络连接可能会终止。大多数终止的连接会在短时间后恢复。

步骤 7. 安装 Kaspersky Security Gateway

安装向导将 Kaspersky Security Gateway 文件复制到计算机。等待安装完成。

完成向导操作。

从命令行安装 Kaspersky Security Gateway

要从命令行安装 Kaspersky Security Gateway，请运行以下命令：

```
msiexec /i security_gateway.msi EULA=1 PRIVACYPOLICY=1 /qn
```

`EULA=1 PRIVACYPOLICY=1` – 接受您与卡巴斯基之间的 Kaspersky Security Gateway 最终用户授权许可协议的条款以及描述数据处理和传输的隐私策略的条款。

通过将参数设置为 1，您确认以下内容：

- 您已完全阅读、理解并接受最终用户授权许可协议的条款和条件。
- 您已充分阅读并理解本隐私策略，您知悉并同意您的数据将按照本隐私策略中描述的方式处理和传输（包括向第三国传输）。

您必须接受最终用户授权许可协议和隐私策略的条款才能安装 Kaspersky Security Gateway。

最终用户授权许可协议和隐私策略的文本包含在分配套件中。

删除 Kaspersky Security Gateway

删除 Kaspersky Security Gateway 需要管理员账户权限。

要删除 Kaspersky Security Gateway：

1. 打开 Microsoft Windows 控制面板。
2. 在 Microsoft Windows 控制面板中，单击“**程序和功能**”图标。
   “**卸载或更改程序**”窗口将在 Microsoft Windows 中打开。
3. 在“**卸载或更改程序**”窗口中，选择 **Kaspersky Security Gateway** 并单击“**更改**”按钮。
   “安装向导”将启动。
4. 在安装向导的“**Modify, Repair, or Remove application**”窗口中，单击“**Remove**”按钮。

   安装向导提示您配置删除设置。按照向导的说明进行操作。

步骤 1. 保存 Kaspersky Security Gateway 数据以供将来使用

在此步骤中，安装向导会提示您保存 Kaspersky Security Gateway 配置文件，以便在后续安装 Kaspersky Security Gateway 时使用（例如，安装新版本时）。

要保存 Kaspersky Security Gateway 配置文件，

选择“**Save application configuration file**”复选框。

仅当通过单击控制面板的“**程序和功能**”部分中的“**更改**”按钮运行安装向导时，“**Save application configuration file**”选项才可用。

继续执行向导的下一步。

步骤 2. 删除 Kaspersky Security Gateway

在此步骤中，安装向导将从计算机中删除 Kaspersky Security Gateway。等到删除过程完成。

完成向导操作。

删除 Kaspersky Security Gateway 时，您的操作系统可能需要重新启动。如果您决定不立即重新启动，则 Kaspersky Security Gateway 的删除将不会完成，直到操作系统重新启动，或者直到计算机关闭并再次打开。

程序界面

您可以使用以下界面控制 Kaspersky Industrial CyberSecurity for Nodes：

- 应用程序控制台。
- Kaspersky Security Center 管理控制台。
- Kaspersky Security Center Web Console。

Kaspersky Security Center 管理控制台

Kaspersky Security Center 允许您远程安装和卸载、启动和停止 Kaspersky Industrial CyberSecurity for Nodes、配置应用程序设置、更改可用应用程序组件集、添加密钥以及启动和停止任务。

可以使用 Kaspersky Industrial CyberSecurity for Nodes 管理插件通过 Kaspersky Security Center 管理应用程序。有关 Kaspersky Security Center 界面的详细信息，请参见 *Kaspersky Security Center 帮助*。

Kaspersky Security Center Web 控制台

Kaspersky Security Center Web 控制台（以下简称“Web 控制台”）是一个 Web 应用程序，用于集中执行主要任务以管理和维护组织网络的安全系统。Kaspersky Security Center Web Console 是提供用户界面的 Kaspersky Security Center 组件。有关 Kaspersky Security Center Web Console 的详细信息，请参阅 *Kaspersky Security Center 帮助*。

Web Console 可执行以下操作：

- 监控组织安全系统的状态。
- 在网络内的设备上安装卡巴斯基应用程序。
- 管理已安装的应用程序。
- 查看有关安全系统状态的报告。

使用管理插件

本节提供有关 Kaspersky Industrial CyberSecurity for Nodes 管理插件的信息，并介绍如何管理一台或一组受保护设备上安装的应用程序。

从 Kaspersky Security Center 管理 Kaspersky Industrial CyberSecurity for Nodes

您可以通过 Kaspersky Industrial CyberSecurity for Nodes 管理插件集中管理多台安装了 Kaspersky Industrial CyberSecurity for Nodes 并加入同一管理组的受保护设备。通过 Kaspersky Security Center 还可以单独配置管理组中包含的每台受保护设备的设置。

*管理组*通过 Kaspersky Security Center 手动创建。该组包括您要为其配置相同的控制和保护设置并已安装了 Kaspersky Industrial CyberSecurity for Nodes 的多个设备。有关使用管理组的详细信息，请参见 *Kaspersky Security Center 帮助*。

如果 Kaspersky Industrial CyberSecurity for Nodes 在某台受保护设备上的运行受活动 Kaspersky Security Center 策略的控制，则该台受保护设备的应用程序设置不可用。

在 Kaspersky Security Center 中启动 Kaspersky Industrial CyberSecurity for Nodes 管理插件无需执行额外的操作。在管理员的受保护设备上安装管理插件后，它会与任何类型的 Kaspersky Security Center 管理控制台一起启动。

可通过以下方式通过 Kaspersky Security Center 管理 Kaspersky Industrial CyberSecurity for Nodes：

- **使用 Kaspersky Security Center 策略**。可使用 Kaspersky Security Center 策略为一组设备远程配置相同的保护设置。在活动策略中指定的任务设置的优先级高于在应用程序控制台中本地配置或在 Kaspersky Security Center 的“**属性：<受保护设备名称>**”窗口中远程配置的任务设置。

  策略可用于配置常规应用程序设置、实时计算机保护任务的设置、设备上的活动控制任务设置、网络存储保护任务设置以及按计划启动本地系统任务的设置。

- **使用 Kaspersky Security Center 组任务**。使用 Kaspersky Security Center 组任务可远程配置任务的通用设置，一组设备具有过期期限。

  您可使用组任务激活应用程序，配置“按需扫描”任务设置，更新任务设置，以及“应用程序启动控制规则生成器”任务设置。

- **使用一组设备的任务**。使用一组设备的任务允许远程配置通用任务设置，不属于任何管理组的受保护设备具有有限执行期限。

- **使用单个设备的属性窗口**。在“**属性：<受保护设备名称>**”窗口中，您可远程配置管理组中包含的单台受保护设备的任务设置。如果选中的受保护设备不受活动 Kaspersky Security Center 策略的控制，您可配置常规应用程序设置和所有 Kaspersky Industrial CyberSecurity for Nodes 任务的设置。

管理应用程序设置

本部分包含有关在 Kaspersky Security Center 管理控制台中配置 Kaspersky Industrial CyberSecurity for Nodes 常规设置的信息。

导航

了解如何通过所选界面导航到所需任务设置。

在应用程序属性窗口中打开常规设置

要打开单台受保护设备的 Kaspersky Industrial CyberSecurity for Nodes 属性窗口：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择**设备**选项卡。
4. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：
   - 双击受保护设备的名称。
   - 打开受保护设备名称的上下文菜单，然后选择“**属性**”项。

   将打开“**属性：<受保护设备名称>**”窗口。
5. 在“**应用程序**”部分中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
6. 单击“**属性**”。
   将打开 **Kaspersky Industrial CyberSecurity for Nodes** 的“**设置**”窗口。
7. 转到**应用程序设置**区域。
8. 在您要配置的设置的子部分中单击“**设置**”按钮。

通过策略打开常规设置

要通过策略打开 Kaspersky Industrial CyberSecurity for Nodes 的应用程序设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。

3. 选择**策略**选项卡。

4. 双击要配置的策略名称。

5. 在打开的“**属性：<策略名称>**”窗口中，转到“**应用程序设置**”。

6. 在您要配置的设置的子部分中单击“**设置**”按钮。

在 Kaspersky Security Center 中配置常规应用程序设置

您可以通过 Kaspersky Security Center 为一组受保护设备或一台受保护设备配置 Kaspersky Industrial CyberSecurity for Nodes 常规设置。

在 Kaspersky Security Center 中配置界面和扫描设置

要配置扩展性设置和应用程序界面：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择要为其配置应用程序设置的管理组。

3. 在选定的管理组的详细窗格中执行以下操作之一：

   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单个受保护设备配置任务或应用程序的设置，请选择“**设备**”选项卡并转至本地任务设置或应用程序设置。

4. 在“**应用程序设置**”部分中，单击“**界面设置** ”子部分中的“**设置**”按钮。

5. 在“**界面设置**”窗口中，在“**常规**”选项卡上，配置以下设置：

   - 在“**用户交互**”部分中，配置在每个应用程序启动后，系统托盘图标是否将显示在任务栏中。
     - “**显示用户界面**”。在客户端计算机上，Windows 托盘中有一个图标。在该图标的上下文菜单中，用户可以使用 Kaspersky Industrial CyberSecurity for Nodes 执行操作。Kaspersky Industrial CyberSecurity for Nodes 还会在应用程序图标上方显示通知。Windows 系统托盘中图标的上下文菜单可让您打开小型诊断窗口。单击小型诊断窗口中的链接即可打开应用程序控制台。
     - “**不显示用户界面**”。在客户端计算机上，不显示 Kaspersky Industrial CyberSecurity for Nodes 操作的迹象。Windows 通知区域中的图标和通知不可用。
   - 在“**状态**”部分中，您可以指定想要在 Kaspersky Industrial CyberSecurity for Nodes 系统托盘图标上看到的警告。

6. 单击“**确定**”。

将保存配置的应用程序设置。

在 Kaspersky Security Center 中配置安全性设置

要手动配置安全设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单个受保护设备配置任务或应用程序的设置，请选择“**设备**”选项卡并转至本地任务设置或应用程序设置。
4. 在“**应用程序设置**”部分中，单击“**安全性和可靠性** ”子部分中的“**设置**”按钮。
5. 在“**安全设置**”窗口中，在“**安全**”选项卡上，配置以下设置：
   - 在“**常规**”部分，我们建议启用“**在计算机开启时启动应用程序(建议)**”（默认）。
   - 在“**自我保护**”部分，启用或禁用“**保护应用程序进程免受外部威胁**”功能。
   - 在“**切换到 UPS 备用电源时的操作**”部分，指定在切换为 UPS 备份电源后 Kaspersky Industrial CyberSecurity for Nodes 对受保护设备产生的负荷的限制：
     - **不启动已计划的扫描任务**
     - **停止正在运行的扫描任务**
   - 在“**应用设置时的计算机状态**”部分中，配置在应用策略或运行任务时出现错误时显示安装了该应用程序的客户端计算机的状态。
   - 在“**兼容性设置**”部分中，配置“**与远程管理软件的兼容性**”设置。

     如果将 Kaspersky Industrial CyberSecurity for Nodes 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 与应用程序安全桌面功能不兼容有关。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。

     如果选中此复选框，则启用 RAT 兼容模式。应用程序会显示一个没有此功能的确认对话框。这可能降低计算机的安全级别。如果 Kaspersky Industrial CyberSecurity for Nodes 不会导致您的 RAT 出现问题，我们不建议启用兼容模式。

     如果清除该复选框，则禁用 RAT 兼容模式。默认下，复选框被清除。

     示例：在 RemoteApp 模式下使用浏览器时，Kaspersky Industrial CyberSecurity for Nodes 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。

6. 在“**扫描设置**”选项卡上，配置以下设置：

   - “**限制扫描任务的 CPU 使用率**”。Kaspersky Industrial CyberSecurity for Nodes 在按需扫描任务期间会将对受保护设备 CPU 的使用率限制为“**上限**”字段中指定的值。启用此选项可能会对 Kaspersky Industrial CyberSecurity for Nodes 的性能产生负面影响。

   - 为其他应用程序让出资源。Kaspersky Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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。

7. 单击“**确定**”。

   将保存扩展性和可靠性设置。

使用 Kaspersky Security Center 配置连接设置

配置的连接设置用于将 Kaspersky Industrial CyberSecurity for Nodes 连接到更新和激活服务器，以及在将应用程序与 KSN 服务集成期间使用。

若要配置连接设置，请执行以下步骤：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。

2. 选择要为其配置应用程序设置的管理组。

3. 在选定的管理组的详细窗格中执行以下操作之一：

   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。

   - 要为单个受保护设备配置任务或应用程序的设置，请选择“**设备**”选项卡并转至本地任务设置或应用程序设置。

4. 在“**应用程序设置**”部分中，单击“**连接设置** ”子部分中的“**设置**”按钮。

   “**连接设置**”窗口将打开。

5. 在“**连接设置**”窗口中，配置以下设置：

   - 在“**代理服务器**”部分，通过单击“**设置**”按钮指定代理服务器设置：

     - **不使用代理服务器**。

     - **自动检测代理服务器设置**

     - **使用指定的代理服务器**。

     - **代理服务器和端口号的 IP 地址或符号名称**

     - **对本地地址不使用代理服务器**。

- 在“**代理服务器身份验证设置**”部分中，指定身份验证设置。在下拉列表中选择身份验证设置:
  - **不使用身份验证** - 不执行身份验证。
  - **NTLM 身份验证** – 使用由 Microsoft 开发的 NTLM 网络身份验证协议执行身份验证。默认选择该模式。
- 需要时，输入用户名和密码。
- 在“**授权许可**”部分中，选中或清除“**激活应用程序时使用 Kaspersky Security Center 作为代理服务器**”复选框。

- 在“**受监控端口**”部分，指定监控的网络端口：
  - “**监控所有网络端口**”。在此网络端口监控模式下，保护组件会监控通过任何开放的计算机网络端口传输的数据流。
  - “**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。

  点击“**设置**”并指定以下设置**:**
  - “**监控卡巴斯基推荐的列表中的应用程序的所有端口**”。这将使用被 Kaspersky Industrial CyberSecurity for Nodes 监控其网络端口的预定义应用程序列表。例如，该列表包括 Google Chrome、 Adobe Reader、 Java 和其他应用程序。
  - “**监控指定应用程序的所有端口**”。被 Kaspersky Industrial CyberSecurity for Nodes 监控其网络端口的应用程序列表。

6. 单击“**确定**”。

将保存配置的连接设置。

配置本地任务的计划启动

您可以使用策略来允许或阻止本地系统“按需扫描”任务和“更新”任务的启动。此操作根据管理组中每个受保护设备上本地配置的计划来完成：

- 如果特定类型的本地系统任务的计划启动受到策略禁止，则这些任务将不会按照计划在受保护设备上执行。您可以手动启动该本地系统任务。
- 如果特定类型的本地系统任务的计划启动被策略允许，则这些任务将按照为此任务进行的本地配置的计划参数来执行。

默认情况下，策略会禁止本地系统任务的启动。

如果更新或按需扫描受 Kaspersky Security Center 组任务的管理，我们推荐不要允许本地系统任务启动。

如果不使用组更新或按需扫描任务，则允许在策略中启动本地系统任务： Kaspersky Industrial CyberSecurity for Nodes 将执行应用程序数据库和模块更新，并根据默认计划启动所有本地系统按需扫描任务。

您可使用策略允许或阻止以下本地系统任务的计划启动：

- 按需扫描任务：*关键区域扫描*、*在操作系统启动时扫描*、*应用程序完整性控制*、*基线系统完整性监控*。
- 更新任务：*数据库和应用程序模块的更新*，*应用程序更新*。

如果受保护设备被从管理组中排除，将自动启用本地系统任务计划。

要在策略中允许或阻止应用程序本地任务的启动计划管理：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，展开相关组，然后在结果窗格中选择“**策略**”选项卡。
2. 在“**策略**”选项卡上，在要为受保护设备组计划 Kaspersky Industrial CyberSecurity for Nodes 本地系统任务的策略的上下文菜单中，选择“**属性**”。
3. 在策略属性窗口中，选择“**应用程序设置**”区域。
4. 在“**运行本地系统任务**”字部分中单击“**设置**”。
5. 选择“**允许使用本地任务**”复选框。
6. 使用“**允许计划管理**”复选框以允许或阻止应用程序本地任务的启动计划管理。

在 Kaspersky Security Center 中配置隔离和备份设置

要在 Kaspersky Security Center 中配置常规隔离和备份设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置应用程序设置的管理组。
3. 在选定的管理组的详细窗格中执行以下操作之一：
   - 要为一组受保护设备配置应用程序设置，请选择“**策略**”选项卡，然后打开“**属性：<策略名称>**”窗口。
   - 要为单个受保护设备配置任务或应用程序的设置，请选择“**设备**”选项卡并转至本地任务设置或应用程序设置。
4. 转到**补充**区域。
5. 在“**存储**”子部分中单击“**设置**”按钮。
6. 按下表所述配置设置。

存储设置

参数	描述
在“**报告**”选项卡上，指定报告设置：	
存储报告时间不超过	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。报告的默认最大存储条件为 30 天。在此时间之后，Kaspersky Industrial CyberSecurity for Nodes 将自动删除报告文件中的最早条目。
限制报告文件大小为	如果选中该复选框，则最大报告文件大小限制为定义值。默认情况下，最大文件大小数据为 1024 MB。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 Industrial CyberSecurity for Nodes 将自动删除报告文件中的最早条目。

参数	描述
在“**备份**”选项卡上，指定备份设置：	
存储对象时间不超过	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。文件的默认最大存储条件为 30 天。最长存储期限到期后，Kaspersky Industrial CyberSecurity for Nodes 将删除备份区中最旧的文件。
限制备份区大小为	如果选中该复选框，则最大存储大小限制为定义值。默认情况下，最大大小为 400 MB。为避免超过最大存储大小，当达到最大存储大小时，Kaspersky Industrial CyberSecurity for Nodes 将自动删除存储中的最早文件。
可用空间阈值	该复选框用于启用或禁用监控备份中的最小可用空间大小（默认值为 100 MB）的功能。如果可用空间大小下降到低于指定阈值，Kaspersky Industrial CyberSecurity for Nodes 会记录“*已超过隔离区区可用空间阈值*”事件，并根据此事件类型的通知设置发布通知。 如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控备份中的可用空间的大小。 如果选中“**限制备份区大小为**”复选框被选中，则“**可用空间阈值**”复选框被激活。
在“**隔离区**”选项卡上，指定隔离设置：	
限制隔离区大小为	最大隔离区大小 (MB)。例如，您可以将最大隔离区大小设置为 200 MB。当隔离区达到最大大小时，Kaspersky Industrial CyberSecurity for Nodes 将相应的事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序停止隔离新对象。您必须手动清空隔离区。
可用空间阈值	该复选框用于启用或禁用监控隔离区中的最小可用空间大小（默认值为 50 MB）的功能。如果可用空间大小下降到低于指定阈值，Kaspersky Industrial CyberSecurity for Nodes 会记录“*已超过隔离区可用空间阈值*”事件，并根据此事件类型的通知设置发布通知。 如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控隔离区中的可用空间的大小。 默认选中该复选框。

创建和配置策略

本节提供有关使用 Kaspersky Security Center 策略在多个受保护设备上管理 Kaspersky Industrial CyberSecurity for Nodes 的信息。

可以创建全局性 Kaspersky Security Center 策略，以便管理多个安装了 Kaspersky Industrial CyberSecurity for Nodes 的设备上的保护。

策略在一个管理组的所有受保护设备上实施 Kaspersky Industrial CyberSecurity for Nodes 设置、功能和指定的任务。

可以为一个管理组依次创建和实施多个策略。该策略当前对管理控制台中具有“*活动*”状态的组有效。

Kaspersky Industrial CyberSecurity for Nodes 系统审核日志中记录了有关策略实施情况的信息。可在应用程序控制台的“**日志审查**”节点中查看该信息。

Kaspersky Security Center 提供一种在受保护设备上应用策略的方式：*禁止编辑设置*。应用某个策略后，Kaspersky Industrial CyberSecurity for Nodes 会使用您在策略属性中指定的设置“**已禁止编辑**”的值。在这种情况下，Kaspersky Industrial CyberSecurity for Nodes 不会使用应用该策略之前有效的设置值。Kaspersky Industrial CyberSecurity for Nodes 不会应用在策略属性中指定的活动策略设置“**已允许编辑**”的值。

如果策略为活动的，则策略中标记图标的设置的值在应用程序控制台中显示，但无法编辑。其他设置的值可以在应用程序控制台中编辑。

活动策略中配置的且标记图标的设置也会阻止在 Kaspersky Security Center 的“**属性：<受保护设备名称>**”窗口中针对单台受保护设备进行更改。

在禁用活动策略后，使用活动策略指定并发送到受保护设备的设置将保存在本地任务设置中。

如果某个策略定义了当前正在运行的实时计算机保护任务或网络附加存储保护任务的设置，则该策略定义的设置将在应用该策略后立即更改。如果任务未运行，则设置将在该任务启动时应用。

创建策略

在创建策略之前，您需要安装管理插件 klcfginst.exe。

要为安装并运行应用程序的一组受保护设备创建策略：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点，然后选择包含您希望为其创建策略的受保护设备的管理组。
2. 在选定管理组的结果窗格中，选择“**策略**”选项卡，然后单击“**创建策略**”链接以启动新策略向导。
   将打开“**新建策略向导**”窗口。
3. 在“**选择要为其创建组策略的应用程序**”窗口中，选择 Kaspersky Industrial CyberSecurity for Nodes。
4. 点击“**下一步**”。
5. 在“**名称**”字段中输入组策略名称。

   策略名称不能包含以下符号：`" * < : > ? \ |` 。
6. 要应用以前版本的应用程序中使用的策略配置：
   a. 选择**使用早期版本应用程序的策略设置**复选框。
   b. 单击“**浏览**”按钮。
   c. 选择要应用的策略。
   d. 点击“**下一步**”。
7. 在“**选择操作类型**”窗口中，“**实时文件保护设置**”下，选择“**启用实时文件保护**”复选框并指定安全级别。

   如果未选择任务运行模式，则无法继续执行新策略向导的下一步。
8. 配置实时计算机保护。
9. 配置扫描排除项和受信任的应用程序。
10. 在“**为应用程序创建组策略**”窗口中选择下列策略状态之一：
    - “**活动策略**”，如果您希望在创建策略后立即应用该策略。如果组中已经存在活动策略，则会将其停用并应用新策略。
    - “**非活动策略**”，如果您不希望立即应用所创建的策略。在此情况下，可在以后激活该策略。

- 当计算机离开组织网络周界时，“**漫游**”策略激活。
- 选中“**创建策略后立即打开策略属性**”复选框以在单击“**下一步**”按钮后自动关闭**新建策略向导**并配置新创建的策略。

11. 单击“**完成**”按钮。

所创建的策略将显示在选定管理组的“**策略**”选项卡上的策略列表中。在“**属性：<策略名称>**”窗口中，您可配置 Kaspersky Industrial CyberSecurity for Nodes 的其他设置、任务和功能。

创建新策略后，会创建一组允许规则，以防止应用程序被阻止，保证应用程序不间断运行。您可以在任务设置中查看默认规则。有关详细信息和限制，请参阅下文。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 在创建新策略时会创建一组入站网络流量规则：

- 使用 Kaspersky Security Center 网络代理共享 Windows 桌面的过程的两个允许规则，该代理位于 %Program Files% 和 %Program Files (x86)% 文件夹中。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。
- 本地端口 15000 的两个允许规则。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 在创建新策略时会创建一组传出网络流量规则：

- Kaspersky Industrial CyberSecurity for Nodes 服务的两个允许规则，该服务位于 %Program Files% 和 %Program Files (x86)% 文件夹中。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。
- Kaspersky Industrial CyberSecurity for Nodes 工作进程的两个允许规则，该应用程序位于 %Program Files% 和 %Program Files (x86)% 文件夹中。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。
- 本地端口 13000 的两个允许规则。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。

配置策略

要配置策略设置：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 展开您希望为其配置关联策略设置的管理组，然后打开详细信息窗格中的“**策略**”选项卡。
3. 单击要配置的策略名称。

采用以下方法之一打开“**属性：<策略名称>**”窗口：

- 在策略上下文菜单中，选择“**属性**”选项。
- 双击所选策略。

4. 在“**策略状态**”部分的“**常规**”选项卡上，启用或禁用策略。为此，请选择以下选项之一：

   - **活动策略**，如果您希望在选定管理组内的所有受保护设备上应用策略。
   - **漫游策略**，当计算机离开组织网络周界时，将激活该策略。
   - **非活动策略**，如果您不希望以后在选定管理组内的所有受保护设备上激活策略。

5. 在策略的其他部分配置应用程序设置。

   您可通过 Kaspersky Security Center 策略启用或禁用在管理组内的所有受保护设备上执行任何任务。

   您可为每个单个软件组件配置在所有网络受保护设备上应用策略设置。

6. 单击“**确定**”。

   将在策略中应用配置的设置。

使用 Kaspersky Security Center 创建和配置任务

本节包含有关 Kaspersky Industrial CyberSecurity for Nodes 任务、如何创建任务、配置任务设置，以及启动和停止任务的信息。

关于 Kaspersky Security Center 中的任务创建

您可为管理组和受保护设备集创建组任务。您可以通过 Kaspersky Security Center 创建以下任务类型：

- *应用程序激活*
- *安全审计*
- *终止进程*
- *运行进程*
- *管理服务器连接保护*
- *更改 Kaspersky Industrial CyberSecurity for Nodes 组件*
- *基线系统完整性监控*
- *更新*
- *更新回滚*
- *IOC 扫描*

- *获取文件*
- *移动文件到隔离区*
- *按需扫描*
- *应用程序完整性控制*
- *删除密钥*
- *删除文件*
- *应用程序启动控制规则生成器*
- "*设备控制规则生成器*"。

您可采用以下方式创建本地和组任务：

- 对于单个受保护的设备，在"**任务**"部分。
- 对于管理组：在选定受保护设备组的节点的详细信息窗格中的"**任务**"选项卡上。
- 对于一组受保护设备：在"**设备分类**"节点的详细信息窗格中。

> 您可以使用策略禁用同一管理组中所有受保护设备上的"*更新*"和"*按需扫描*"本地系统任务的计划。

有关 Kaspersky Security Center 中任务的常规信息，请参见 *Kaspersky Security Center 帮助*。

使用 Kaspersky Security Center 创建任务

要在 Kaspersky Security Center 管理控制台中创建新任务：

1. 采用以下方式之一启动任务向导：
   - 若要创建本地任务：
     a. 展开管理控制台树中的"**受管理设备**"节点，并选择受保护服务器所属的组。
     b. 在结果窗格的"**设备**"选项卡上，打开受保护设备的上下文菜单，然后选择"**属性**"。
     c. 在打开的窗口中，在"**任务**"部分，点击"**添加**"按钮。
   - 创建组任务：
     a. 展开 Kaspersky Security Center 管理控制台树中的"**受管理设备**"节点。
     b. 选择要为其创建任务的管理组。
     c. 在结果窗格中，打开"**任务**"选项卡，然后选择"**新任务**"。

   将打开任务向导窗口。

2. 在标题“**Kaspersky Industrial CyberSecurity for Nodes**”下的“**选择任务类型**”窗口中，选择要创建的任务的类型。

3. 根据任务类型，设置可能有所变化：

   - 创建按需扫描任务。
   - 要创建更新任务，请根据您的需要配置任务设置：

     a. 您可在“**更新源**”块中将 Kaspersky Security Center 管理服务器或卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。

     如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。

     b. 配置减少磁盘子系统负载的功能设置：

     c. 您可以指定 Kaspersky Industrial CyberSecurity for Nodes 在需要关键应用程序模块更新时以及关键更新安装完成后将执行的操作。此外，您还可以指定 Kaspersky Industrial CyberSecurity for Nodes 是否接收有关可用计划更新的信息。

     d. 指定要复制的更新集和 Kaspersky Industrial CyberSecurity for Nodes 将用于存储已复制更新的文件夹的路径。

   - 要创建“*应用程序激活*”任务：

     a. 在“**激活设置**”窗口中，指定您要使用的密钥文件或激活码来激活应用程序。

     b. 如果您想要创建用于续订授权许可的任务，请选中“**用作附加密钥**”复选框。

   - 创建“应用程序启动控制规则生成器”任务。
   - 创建“设备控制规则生成器”任务。

4. 配置任务计划。

5. 单击“**确定**”。

6. 如果是为一组受保护设备创建任务，请选择将执行该任务的受保护设备网络（或组）。

7. 在“**选择账户以运行任务**”窗口中，指定您要用于运行任务的账户。

8. 在“**定义任务名称**”窗口中，输入任务名称（长度不得超过 100 个字符，不得包含符号 `" * < > ? \ | :`）。建议将任务类型添加到任务名称中（例如，“按需扫描共享文件夹”）。

9. 在“**完成任务创建**”窗口中，执行以下操作之一：

   a. 如果您希望任务在创建后立即启动，请选中“**向导完成时运行任务**”复选框。

   b. 单击“**完成**”。

所创建的任务将显示在“**任务**”列表中。

转至单台计算机的本地任务设置和常规应用程序设置

如果应用程序当前受 Kaspersky Security Center 策略控制，且该策略禁止更改应用程序设置，则无法编辑单台计算机的这些设置。

要转到单台计算机的本地任务设置：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择受保护设备所属的组。
3. 在结果窗格中，选择“**设备**”选项卡。
4. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：
   - 双击受保护设备的名称。
   - 在受保护设备名称的上下文菜单中，选择“**属性**”。

   将打开“**属性：<受保护设备名称>**”窗口。
5. 转至“**任务**”部分。
6. 在任务列表中，选择要通过以下方式之一配置的本地任务：
   - 双击任务名称
   - 在列表中选择一个任务，然后单击“**属性**”按钮
   - 在任务名称的上下文菜单中，选择“**属性**”。

   将打开“**属性：<任务名称>**”窗口。

要转到单台计算机的常规应用程序设置：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点，并选择受保护设备所属的组。
2. 在结果窗格中，选择“**设备**”选项卡。
3. 采用以下方法之一打开“**属性：<受保护设备名称>**”窗口：
   - 双击受保护设备的名称。
   - 在受保护设备名称的上下文菜单中，选择“**属性**”。

   将打开“**属性：<受保护设备名称>**”窗口。
4. 转至“**应用程序**”部分。

5. 在已安装的应用程序列表中，通过以下方式之一选择 Kaspersky Industrial CyberSecurity for Nodes：

   - 双击 Kaspersky Industrial CyberSecurity for Nodes 的名称
   - 在列表中选择 Kaspersky Industrial CyberSecurity for Nodes，然后单击“**属性**”按钮。
   - 在 Kaspersky Industrial CyberSecurity for Nodes 名称的上下文菜单中，选择“**属性**”项。

   将打开 **Kaspersky Industrial CyberSecurity for Nodes** 的“**设置**”窗口。

在 Kaspersky Security Center 中配置组任务

要为多个受保护设备配置组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：

   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中选择任务名称，然后单击“**配置任务**”链接。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。
5. 在“**通知**”部分中，配置任务事件通知设置。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
6. 根据所配置的任务类型，执行下列操作之一：

   - 要配置“*按需扫描*”任务：
     - 在“**扫描范围**”部分中，配置扫描范围。
     - 在“**设置**”部分中，配置任务优先级水平及与其他软件组件的集成。
   - 要配置“*更新*”任务：
     - 转到“**设置**”部分并指定“**应用程序数据库和模块更新设置**”。
     - 选择要执行的操作：复制并安装软件模块的关键更新或仅检查它们。
   - 要配置“*应用程序激活*”任务：
     - 在“**设置**”部分中，指定您要使用的密钥文件或激活码来激活应用程序。
     - 如果您想要添加用于续订授权许可的激活码或密钥文件，请选中“**用作附加密钥**”复选框。
   - 要配置*设备控制规则生成器*任务，在“**设置**”部分中，指定要用于创建设备控制规则列表的设置。

7. 在“**计划**”部分中配置任务计划。

8. 在“**账户**”部分中，指定将使用其权限运行任务的账户。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

9. 如果需要，在“**任务范围排除项**”部分中，指定要从任务范围中排除的对象。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

10. 在“**属性：<任务名称>**”窗口中单击“**确定**”按钮。

将保存新配置的组任务设置。

组任务的可配置设置如下所列。

- 应用程序启动控制规则生成器

  在配置“*应用程序启动控制规则生成器*”任务设置时，您可以在“**规则**”选项卡上选择如何创建允许规则：

  - **基于运行的应用程序创建允许规则**
  - **为文件夹中的应用程序创建允许规则**

  您可以在“**设置**”选项卡上指定在创建应用程序启动控制允许规则时执行以下操作：

  - **使用数字证书**
  - **使用数字证书主题和指纹**
  - **如果证书丢失，请使用**
  - **使用 SHA256 哈希**
  - **为用户和/或用户组生成规则**

  您可以使用 Kaspersky Industrial CyberSecurity for Nodes 在任务完成时创建的允许规则列表为配置文件配置设置。

  您可以配置按计划启动任务的设置。

- 设备控制规则生成器

  - 选择运行模式：考虑曾经连接过的所有外部的系统数据，或仅考虑当前连接的外部设备。
  - 使用 Kaspersky Industrial CyberSecurity for Nodes 在任务完成时创建的允许规则列表为配置文件配置设置。
  - 您可以配置按计划启动任务的设置。

- 应用程序激活

  - 要激活应用程序或续订授权许可，您可以添加密钥文件或激活码。
  - 您可以配置按计划启动任务的设置。

- 数据库和应用程序模块的更新
  - 您可在“**更新源**”设置块中将 Kaspersky Security Center 管理服务器或卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。

    如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。
  - 您可以配置减少磁盘子系统负载的功能设置：
    - **降低磁盘 I/O 的负载**
    - **用于优化的 RAM (MB)**
  - 您可以指定 Kaspersky Industrial CyberSecurity for Nodes 在需要关键应用程序模块更新时以及关键更新安装完成后将执行的操作。此外，您还可以指定 Kaspersky Industrial CyberSecurity for Nodes 是否接收有关可用计划更新的信息。
  - 您可以指定要复制的更新集和 Kaspersky Industrial CyberSecurity for Nodes 将用于存储已复制更新的文件夹的路径。
  - 您可以配置按计划启动任务的设置。
- 按需扫描
  - 您可指定“按需扫描”任务的扫描范围，并配置安全级别设置。
  - 在“**启发式分析**”设置块中，您可以为按需扫描任务启用或禁用启发式分析，并使用滑块设置分析级别。
  - 在“**与其他组件整合**”块中，您可配置以下设置：
    - 在后台模式下启动扫描任务。
    - 将任务视为关键区域扫描。
    - 禁止同时启动多个扫描任务。
  - 您可以配置按计划启动任务的设置。
- 应用程序完整性控制
  - 您可以配置按计划启动任务的设置。
- 基线系统完整性监控
  - 您可以配置监控模式和指定对文件、注册表和设备采取的操作的规则。
  - 您可以配置按计划启动任务的设置。

应用程序激活任务

要配置“应用程序激活 ”任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

   > 在“**通知**”部分中，配置任务事件通知设置。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
5. 在“**激活设置**”部分中，指定您要使用的密钥文件来激活应用程序。如果要添加用于续订授权许可的密钥，请选中“**用作附加密钥**”复选框。
6. 在“**计划**”部分中，配置任务计划设置。
7. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。
   有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
8. 在“**属性：<任务名称>**”窗口中单击“**确定**”按钮。
   将保存新配置的组任务设置。

更新任务

要配置“更新 ”任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的任务。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：
   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

5. 在“**通知**”部分中，配置任务事件通知设置。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

6. 在“**设置**”部分中，执行以下操作：

   a. 使用“**应用程序数据库和模块更新设置**”部分的“**设置**”按钮选择更新源：

   - Kaspersky Security Center 管理服务器。
   - 卡巴斯基更新服务器。
   - 自定义 HTTP 或 FTP 服务器或网络文件夹。

   > 要将 SMB 共享文件夹用作更新源，您需要指定用户账户以启动任务。

   如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。

   b. 配置减少磁盘子系统负载的功能设置：

   - “**降低磁盘 I/O 的负载**”。使用此复选框可以启用或禁用通过将虚拟驱动器上的更新文件存储在内存中实现磁盘子系统优化的进程。默认下，复选框被清除。
   - **用于优化的 RAM (MB)**。

   c. 指定当应用程序模块的关键更新可用或有关于计划更新的信息时，Kaspersky Industrial CyberSecurity for Nodes 应执行的操作。

   d. 指定更新复制设置。

7. 在“**计划**”部分中配置任务计划（您可为除“更新回滚”外的所有任务类型配置计划）。

8. 在“**账户**”部分中，指定将使用其权限运行任务的账户。

   > 有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

9. 在“**属性：<任务名称>**”窗口中，单击“**确定**”。

对于“*更新回滚*”任务，您仅可以在“**通知**”和“**任务范围的排除项**”部分中配置由 Kaspersky Security Center 控制的标准任务设置。有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

应用程序完整性控制

要配置“应用程序完整性控制”组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择要为其配置应用程序完整性控制任务的管理组。
2. 在所选管理组的详细信息窗格中，打开“**任务**”选项卡。
3. 在先前创建的组任务列表中，选择您要配置的应用程序完整性控制任务。

4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：

   - 在创建的任务列表中双击任务名称。
   - 在创建的任务列表中打开任务名称的上下文菜单，然后选择“**属性**”项。

5. 在“**通知**”部分中，配置任务事件通知设置。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。
6. 在“**设备**”部分中，选择要为其配置“应用程序完整性控制”任务的设备。
7. 在“**计划**”部分中，配置任务计划设置。
8. 在“**账户**”部分中，指定将使用其权限运行任务的账户。
9. 如有需要，在“**任务范围的排除项**”部分中指定要从任务范围中排除的对象。

   有关配置此节中设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

10. 在“**属性：<任务名称>**”窗口中单击“**确定**”按钮。

管理任务计划

您可以为计划 Kaspersky Industrial CyberSecurity for Nodes 任务。

计划任务

要使用管理插件计划组任务：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择受保护设备所属的组。
3. 在结果窗格中，选择“**任务**”选项卡。
4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：

   - 双击任务的名称。
   - 打开任务名称的上下文菜单，然后选择“**属性**”项。

5. 选择“**计划**”部分。
6. 在“**计划开始**”下拉列表中，选择启动参数：

如果 Kaspersky Security Center 策略阻止按需扫描任务和更新任务的计划，则这些任务的计划设置字段将不可用。

- **每 N 小时**，如果您希望任务每隔几个小时定期运行一次，请在“**开始间隔 (小时)**”字段输入小时数。
- **每 N 天**，如果您希望任务每隔几天定期运行，请在“**开始间隔 (天)**”字段输入天数。
- **每 N 分钟**，如果您希望任务每隔几分钟定期运行一次，请在“**开始间隔 (分钟)**”字段输入分钟数。
- **每周**，如果您希望任务在一周的某一天运行；还请指定您希望它运行的时间。
- **每月**，如果您希望任务在每月的某一天运行；还请指定希望其运行的时间。
- **一次**，如果您想在指定的日期和时间运行一次任务。
- **手动**，如果您想手动运行该任务。
- **在程序启动时**，如果您希望在每次启动 Kaspersky Industrial CyberSecurity for Nodes 时运行该任务。
- **当新更新下载至存储库时**，如果您希望每次将更新下载到存储库时运行该任务。
- **在检测到病毒爆发时**，如果您希望在检测到病毒攻击时运行该任务。
- **在完成其他任务时**，如果您希望该任务在另一个任务完成后运行。

a. 在“**开始时间**”字段中指定首次启动任务的时间。

b. 在“**计划为**”字段中，指定计划启动的日期。

在计划了任务的开始时间、日期和频率之后，将显示下一次启动的预估时间。

转到“**计划**”选项卡，然后打开“**任务设置**”窗口。在窗口上部的**下一次启动**字段中，显示了预计启动时间。每次打开窗口时，此估计启动时间都会更新并显示。

如果 Kaspersky Security Center 活动策略设置禁止启动计划的本地系统任务，则“**下一次启动**”字段将显示“**被策略阻止**”值。

7. 选中“**运行错过的任务**”复选框以允许启动跳过的任务。
8. 如果选中“**使用任务启动自动随机延迟**”复选框，则任务不会严格按计划运行，而是在一定的时间间隔内随机运行，即任务的开始时间是分散的。
9. 根据需要单击“**高级**”来配置以下计划设置：

- “**使用 Wake-On-LAN 功能在任务启动之前开启设备**”。如果选中该复选框，则在运行任务之前，计算机的操作系统将有一个指定的提前期来完成启动。默认提前期为 5 分钟。
- “**任务完成后关闭设备**”。如果选中该复选框，则任务完成后设备将被关闭。
- “**如果任务运行超过该时间则停止**”。如果选中该复选框，则任务运行时间超过指定时间时将停止。

10. 单击“**确定**”。

11. 单击“**应用**”按钮保存任务启动设置。

如果要使用 Kaspersky Security Center 配置单个任务的应用程序设置，请参见“在 Kaspersky Security Center 的应用程序设置窗口中配置本地任务”部分。

启用和禁用计划任务

可在配置计划设置之前或之后启用和禁用计划任务。

要启用或禁用任务启动计划：

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

2. 选择受保护设备所属的组。

3. 在结果窗格中，选择“**任务**”选项卡。

4. 采用以下方法之一打开“**属性：<任务名称>**”窗口：

   - 双击任务的名称。
   - 打开任务名称的上下文菜单，然后选择“属性”项。

5. 选择“**计划**”部分。

6. 如果您要启用计划任务启动，请从“**计划开始**”下拉列表中选择运行计划任务的设置。

7. 如果要禁用计划任务启动，请在下拉列表中选择“**手动**”。

   已配置的任务启动计划设置不会被删除，并在下次启用计划任务启动时应用。

8. 单击“**确定**”。

将保存已配置的任务启动计划设置。

Kaspersky Security Center 中的报告

Kaspersky Security Center 中的报告包含有关受管理设备状态的信息。报告基于管理服务器上存储的信息。

从 Kaspersky Security Center 11 开始，对于 Kaspersky Industrial CyberSecurity for Nodes，以下类型的报告可用：

- 有关应用程序组件状态的报告
- 有关已禁止的应用程序的报告
- 有关在测试模式下禁止的应用程序的报告

有关所有 Kaspersky Security Center 报告以及如何配置它们的详细信息，请参阅 *Kaspersky Security Center 帮助*。

有关 Kaspersky Industrial CyberSecurity for Nodes 组件状态的报告

您可以监视所有网络设备的保护状态，并获得每个设备上的组件集的结构化概览。

报告显示每个组件的以下状态之一：*正在运行*、*已暂停*、*已停止*、*授权许可未涵盖*。

*未安装*状态指的是组件，而不是应用程序本身。如果未安装应用程序，Kaspersky Security Center 会分配 N/A（不可用）状态。

您可以创建组件选择并使用筛选来显示具有指定组件集和状态的网络设备。

有关创建和使用选择的详细信息，请参见 *Kaspersky Security Center 帮助*。

要在应用程序设置中查看组件状态：

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点，然后选择您希望为其配置应用程序设置的管理组。
2. 选择“**设备**”选项卡，然后打开“**应用程序设置**”窗口。
3. 选择“**组件**”部分。
4. 查看状态表。

要查看 Kaspersky Security Center 标准报告：

1. 在管理控制台树中选择“**管理服务器 <管理服务器名称>**”节点。
2. 选择“**报告**”选项卡。
3. 双击“**有关应用程序组件状态的报告**”列表项。
   将生成报告。

4. 查看以下报告详细信息：

   - 图形化图表。
   - 组件和安装了每个组件的网络设备总数以及设备所属的组的汇总表格。
   - 指定了组件状态、版本、设备和组的详细表格。

有关在活动模式和测试模式下禁止的应用程序的报告

根据“应用程序启动控制”任务的结果，可以生成两种类型的报告：有关已禁止的应用程序的报告（如果在活动模式下启动该任务）和有关在测试模式下禁止的应用程序的报告（如果在通知模式下启动该任务）。这两种报告显示了有关网络的受保护设备上阻止的应用程序的信息。每个报告都针对所有管理组生成，并累积来自受保护设备上安装的所有 Kaspersky 应用程序的数据。

要查看有关在通知模式下禁止的应用程序的报告：

1. 在“通知”模式下启动“应用程序启动控制”任务。
2. 在管理控制台树中选择“**管理服务器 <管理服务器名称>**”节点。
3. 选择“**报告**”选项卡。
4. 双击“**有关在测试模式下禁止的应用程序的报告**”项。
   将生成报告。
5. 查看以下报告详细信息：

   - 显示阻止启动次数最多的前 10 个应用程序的图形化图表。
   - 应用程序阻止行为的汇总表格，其中指定可执行文件名、原因、阻止时间和发生阻止的设备数量。
   - 指定了有关设备、文件路径和阻止条件的数据的详细表格。

要查看有关在活动模式下禁止的应用程序的报告：

1. 在“活动”模式下启动“应用程序启动控制”任务。
2. 在管理控制台树中选择“**管理服务器 <管理服务器名称>**”节点。
3. 选择“**报告**”选项卡。
4. 双击“**有关禁止的应用程序的报告**”项。
   将生成报告。

此报告包含的阻止数据与有关在测试模式下禁止的应用程序的报告相同。

使用 Kaspersky Industrial CyberSecurity for Nodes 控制台

本节提供有关 Kaspersky Industrial CyberSecurity for Nodes 控制台的信息，并介绍了如何使用安装在受保护设备或其他设备上的应用程序控制台来管理该应用程序。

启动应用程序控制台

要安装应用程序控制台：

1. 采用以下方式之一打开小型诊断窗口：

   - 运行受保护设备上的应用程序安装文件夹中的 avpui.exe 文件。默认情况下，该文件位于 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0。
   - 单击任务栏通知区域中的应用程序图标。

2. 在打开的小型诊断窗口中，单击“**Kaspersky Industrial CyberSecurity for Nodes 控制台**”链接。

   如果您已经配置了与受保护设备的连接，则会打开应用程序控制台。

   如果您是第一次启动应用程序控制台，您将被带到“**选择受保护设备**”窗口，您必须在那里**配置应用程序控制台与受保护计算机的连接**。

   a. 如果 Kaspersky Industrial CyberSecurity for Nodes 和应用程序控制台安装在同一台计算机上，请选择“**本地计算机(运行应用程序控制台的计算机)**”。

   b. 如果 Kaspersky Industrial CyberSecurity for Nodes 和应用程序控制台安装在不同的计算机上：

      1. 选择“**其他设备**”。
      2. 点击“**浏览**”并指定安装该应用程序的计算机的名称。
      3. 输入用于连接安装了应用程序的计算机的端口。

   c. 选择或清除“**以此用户身份连接**”复选框以在将应用程序控制台连接到安装了应用程序的计算机时启用或禁用用户账户权限的使用。

   d. 如果启用以用户身份连接，请输入该用户的用户名和密码。指定的用户必须是安装了应用程序的计算机上的 KICS 管理员组的成员。

      用户名区分大小写。

   e. 单击“**连接**”。

Kaspersky Industrial CyberSecurity for Nodes 控制台界面

本节介绍程序界面的主要元素。

Kaspersky Industrial CyberSecurity for Nodes 控制台窗口

与其他受保护设备上安装的 Kaspersky Industrial CyberSecurity for Nodes 建立连接后，将在节点名称后面附加已安装应用程序的受保护设备的名称和建立连接时所使用的用户账户名称：**Kaspersky Industrial CyberSecurity for Nodes <受保护设备名称> 作为 <账户名称>**。连接到与 Kaspersky Industrial CyberSecurity for Nodes 控制台安装在同一台受保护设备上的 Kaspersky Industrial CyberSecurity for Nodes 时，节点名称为 Kaspersky Industrial CyberSecurity for Nodes。

控制台树

应用程序控制台树显示 Kaspersky Industrial CyberSecurity for Nodes 节点和应用程序功能组件的子节点。

Kaspersky Industrial CyberSecurity for Nodes 节点包括以下子节点：

- “**实时计算机保护**”允许配置以下任务：
  - **实时文件保护**
  - **卡巴斯基安全网络**
  - **漏洞利用防御**
  - **网络威胁防护**
  - **反加密**
  - **修复引擎**
  - **AMSI 保护**
- **计算机控制**：控制受保护设备和连接的设备上运行的应用程序。
  - **应用程序启动控制**
  - **设备控制**
  - **防火墙**
- **自动规则生成**：配置“应用程序启动控制”任务和“设备控制”任务的组和系统规则的自动生成。
  - **应用程序启动控制规则生成器**
  - **设备控制规则生成器**

- 规则生成组任务 **<任务名称>**（如果有）

  使用 Kaspersky Security Center 创建组任务。您无法通过 Kaspersky Industrial CyberSecurity for Nodes 控制台管理组任务。

- **系统审查**：配置系统完整性监控和 Windows 事件日志分析的设置。
  - **日志审查**
  - **系统完整性监控**
- **工业网络保护**：接收有关受保护的 PLC 的信息并监控其完整性。
  - **PLC 项目完整性检查**
  - **PLC 项目调查**
- **按需扫描**：管理按需扫描任务。每个任务具有单独的节点：
  - **在操作系统启动时扫描**
  - **关键区域扫描**
  - **应用程序完整性控制**
  - **可移动驱动器扫描**
  - **全盘扫描**
  - 自定义任务 **<任务名称>**（如有）

  该节点显示安装应用程序时创建的系统任务、自定义任务，以及使用 Kaspersky Security Center 创建并发送到受保护设备的组按需扫描任务。

- **更新**：管理 Kaspersky Industrial CyberSecurity for Nodes 数据库和应用程序模块的更新，并提供回滚上次更新的可能性：
  - **数据库和应用程序模块更新**
  - **上次更新回滚**
  - **应用程序更新**

  该节点显示使用 Kaspersky Security Center 创建并发送到受保护设备的所有自定义和组更新任务。

- **存储**：管理备份设置和被阻止的网络会话列表。
  - **备份区**
  - **阻止的网络会话**
- **日志和通知**：管理本地任务日志和 Kaspersky Industrial CyberSecurity for Nodes 系统审计日志。
  - **系统审计**
  - **工业网络保护**

- **应用程序启动控制**
- **设备控制**
- **应用程序完整性控制**
- **日志审查**
- **系统完整性监控**
- **网络威胁防护**
- **按需扫描**
- **防火墙**
- **漏洞利用防御**
- **反加密**
- **AMSI 扫描程序**
- **更新**
- **实时文件保护**
- **备份**
- **Endpoint Detection and Response (Industrial CyberSecurity)**

- **授权许可**：添加或删除 Kaspersky Industrial CyberSecurity for Nodes 密钥，查看授权许可详细信息。

详细信息窗格

详细信息窗格显示有关选定节点的信息。如果选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点，详细信息窗格将显示有关当前设备保护状态的信息，以及有关 Kaspersky Industrial CyberSecurity for Nodes、其功能组件的保护状态和密钥状态的信息。

Kaspersky Industrial CyberSecurity for Nodes 节点的上下文菜单

可使用 **Kaspersky Industrial CyberSecurity for Nodes** 节点的上下文菜单项执行以下操作：

- “**暂停保护**”。
- “**受信任区域**”。查看和配置受信任区域设置。
- “**KATA 整合/与 KICS for Networks 整合的遥测设置**”。
- “**可移动驱动器扫描**”。配置通过 USB 端口连接到受保护设备的可移动驱动器的扫描。
- “**应用程序管理的用户访问权限**”。查看和配置 Kaspersky Industrial CyberSecurity for Nodes 功能的访问权限。
- “**Kaspersky Security Service 管理的用户访问权限**”。查看和配置 Kaspersky Security 服务管理用户权限。

- “**存储**”。
- “**导出设置**”。将应用程序设置保存到 XML 格式的配置文件中。也可以在应用程序任务的上下文菜单中执行此操作。
- **导入设置**. 从 XML 格式的配置文件中导入应用程序设置。也可以在应用程序任务的上下文菜单中执行此操作。
- “**刷新**”。刷新 Kaspersky Industrial CyberSecurity for Nodes 控制台窗口的内容。也可以在应用程序任务的上下文菜单中执行此操作。
- “**应用程序属性**”。查看和配置 Kaspersky Industrial CyberSecurity for Nodes 或选定任务的设置。也可以在应用程序任务的上下文菜单中执行此操作。

  为此，您还可以使用 Kaspersky Industrial CyberSecurity for Nodes 节点详细信息窗格中的“**应用程序属性**”链接。

- “**帮助**”。查看 Kaspersky Industrial CyberSecurity for Nodes 帮助信息。也可以在应用程序任务的上下文菜单中执行此操作。

Kaspersky Industrial CyberSecurity for Nodes 任务的工具栏和上下文菜单

您可以使用 Kaspersky Industrial CyberSecurity for Nodes 控制台树中每个任务的上下文菜单项来管理应用程序任务。

可使用上下文菜单项执行以下操作：

- **恢复/暂停**。恢复或暂停任务执行。要执行这些操作，您还可以使用工具栏上的按钮。此操作适用于“实时保护”任务和“按需扫描”任务。
- “**创建任务**”。新建自定义任务。
- “**删除任务**”。删除自定义任务。
- **导出设置/导入设置**。导出或导入任务设置。
- “**属性**”。打开“任务设置”窗口。
- “**帮助**”。打开相应的在线帮助主题。

通知区域中的系统托盘图标

Kaspersky Industrial CyberSecurity for Nodes 安装完成后，应用程序图标将立即出现在 Microsoft Windows 任务栏通知区域。

如果任务栏通知区域的应用程序图标被隐藏，管理员禁止在策略中显示应用程序界面。

该图标有以下功能：

- 它指示程序活动。
- 是访问上下文菜单和应用程序主窗口的快捷方式。

提供以下应用程序图标状态以显示应用程序运行信息：

- 图标表示应用程序至关重要的保护组件已启用。如果需要用户执行操作（例如，在更新应用程序后重新启动计算机），则 Kaspersky Industrial CyberSecurity for Nodes 将显示警告 。
- 图标表示应用程序至关重要的保护组件已禁用或发生故障。例如，如果授权许可已过期或存在应用程序错误，则可能导致保护组件发生故障。Kaspersky Industrial CyberSecurity for Nodes 将显示警告 并描述计算机保护中的问题。

右键单击系统托盘图标可打开该图标的上下文菜单。

上下文菜单提供了多个可显示应用程序窗口的命令（请参见下表）。

系统托盘图标中的上下文菜单命令

命令	描述
打开应用程序控制台	打开 Kaspersky Industrial CyberSecurity for Nodes 控制台（如已安装）。
打开小型诊断窗口	打开小型诊断窗口。
关于	打开“**关于**”窗口，其中包含有关 Kaspersky Industrial CyberSecurity for Nodes 的信息。 对于注册的 Kaspersky Industrial CyberSecurity for Nodes 用户，“**关于**”窗口包含有关已安装的紧急更新的信息。
隐藏	隐藏任务栏通知区域中的系统托盘图标。

您可以随时重新显示隐藏的系统托盘图标。

要再次显示系统托盘图标，

在 Microsoft Windows 的“**Start**”菜单中，选择“**所有程序** > **Kaspersky Industrial CyberSecurity for Nodes**”。该图标将出现在 Microsoft Windows 任务栏的通知区域中。

设置的名称可能有所不同，具体取决于安装的操作系统。

通过应用程序控制台配置常规设置

Kaspersky Industrial CyberSecurity for Nodes 的常规设置和故障诊断设置设定了应用程序的常规运行条件。您可以通过这些设置来控制 Kaspersky Industrial CyberSecurity for Nodes 所使用的工作进程数，在异常终止后恢复 Kaspersky Industrial CyberSecurity for Nodes 任务，维护日志，在异常终止后创建 Kaspersky Industrial CyberSecurity for Nodes 进程的 Dump 文件，以及配置其他常规设置。

如果 Kaspersky Security Center 活动策略阻止对应用程序设置的更改，则无法在 Kaspersky Industrial CyberSecurity for Nodes 控制台中配置这些设置。

要配置 Kaspersky Industrial CyberSecurity for Nodes 的常规设置：

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并执行以下操作之一：

   - 在节点的结果窗格中，单击“**应用程序属性**”链接。
   - 在节点的上下文菜单中选择“**应用程序属性**”。

   “**应用程序属性**”窗口将打开。

2. 在“**界面**”选项卡上，指定想要在 Kaspersky Industrial CyberSecurity for Nodes 系统托盘图标上看到的警告。

3. 在“**安全设置**”选项卡上，配置以下设置：

   - 在“**常规**”部分中，配置“**在计算机开启时启动应用程序(建议)**”选项。
   - 在“**自我保护**”下，配置应用程序模块保护和操作系统服务。
   - 在“**切换到 UPS 备用电源时的操作**”部分，指定在切换为 UPS 备份电源后 Kaspersky Industrial CyberSecurity for Nodes 对受保护设备产生的负荷的限制：
     - **不启动已计划的扫描任务**
     - **停止正在运行的扫描任务**
   - 在“**兼容性设置**”部分中，配置“**与远程管理软件的兼容性**”设置。

     如果将 Kaspersky Industrial CyberSecurity for Nodes 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 与应用程序安全桌面功能不兼容有关。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。

     如果选中此复选框，则启用 RAT 兼容模式。应用程序会显示一个没有此功能的确认对话框。这可能降低计算机的安全级别。如果 Kaspersky Industrial CyberSecurity for Nodes 不会导致您的 RAT 出现问题，我们不建议启用兼容模式。

     如果清除该复选框，则禁用 RAT 兼容模式。默认下，复选框被清除。

     示例：在 RemoteApp 模式下使用浏览器时，Kaspersky Industrial CyberSecurity for Nodes 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。

   - 在“**扫描设置**”部分，配置“**限制扫描任务的 CPU 使用率**”并允许“将资源让给其他应用程序”。

     Kaspersky Industrial CyberSecurity for Nodes 在按需扫描任务期间会将对受保护设备 CPU 的使用率限制为“**上限**”字段中指定的值。

     > 但是，由于其他组件的存在，应用程序可能会使用更多的 CPU 时间。

     启用此功能可能会对 Kaspersky Industrial CyberSecurity for Nodes 的性能产生负面影响。

默认情况下，禁用此功能。

4. 在“**网络设置**”选项卡上，配置以下设置：

- 在“**代理服务器**”部分中，指定代理服务器设置：身份验证类型以及代理服务器上身份验证所需的详细信息。
- 在“**远程连接端口**”下，如果需要，您可以更改应用程序控制台用于连接安装了应用程序的计算机的端口。

  使用 Windows 凭证进行连接的默认端口号为 13032，使用手动创建的用户的凭证进行连接的默认端口号为 13031。可能的端口号范围：1–65535。

  之前保存的端口号将一直使用直到应用程序重新启动。

5. 在“**故障诊断**”选项卡上，点击“**设置**”并**配置应用程序的跟踪**和**内存转储**。

1. 选择**应用程序转储设置**选项卡。
2. 选择或清除“**创建转储文件**”复选框用于在发生故障时启用或禁用内存转储。

   默认情况下，内存转储文件存储在以下文件夹中：%ProgramData%\Kaspersky Lab\KICS.4.5\Trace。您可以指定另一个路径。

“**跟踪文件文件夹**”字段包含 Kaspersky Embedded Systems Security 默认保存跟踪文件的本地文件夹的完整路径。您可以指定另一个路径。

1. 在“**详细级别**”下拉列表中，选择调试信息的详细级别。
   - **关键**，意味着跟踪文件仅保存有关致命错误的消息。
   - **诊断**，意味着跟踪文件保存有关所有错误和警告的消息。
   - **重要**，意味着跟踪文件保存有关所有错误、警告和附加信息的消息。
   - **正常**，意味着跟踪文件保存有关所有错误、警告的消息，以及有关应用程序正常运行的信息（默认）。
   - **详细**，意味着跟踪文件保存有关应用程序运行的所有信息。

   技术支持代表确定解决任何潜在问题所需的详细级别。

   默认的详细级别设置为“**正常**”。
2. 指定**跟踪文件的最大大小 (MB)**。

   可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小为 100 MB。
3. 要在达到最大文件数时删除旧的跟踪文件，请选中“**删除旧的跟踪文件**”复选框。
4. 指定**一个跟踪日志的最大文件数**。

   可用值：1 到 999。默认情况下，最大文件数为 5。如果选中“**删除旧的跟踪文件**”复选框，则该字段可用。

Kaspersky Industrial CyberSecurity for Nodes 会以未加密的形式将信息写入到跟踪文件和 Dump 文件。保存文件的文件夹由操作系统配置和 Kaspersky Industrial CyberSecurity for Nodes 设置管理。您可以配置访问权限并只允许所需用户访问日志、跟踪文件和 dump 文件。

6. 单击“**确定**”。

Kaspersky Industrial CyberSecurity for Nodes 设置即被保存。

管理 Kaspersky Industrial CyberSecurity for Nodes 任务

本节包含有关如何创建、配置、启动和停止 Kaspersky Industrial CyberSecurity for Nodes 任务的信息。

Kaspersky Industrial CyberSecurity for Nodes 任务类别

Kaspersky Industrial CyberSecurity for Nodes 中的实时计算机保护、计算机控制、自动规则生成、系统审查、按需扫描、工业网络保护、存储管理和更新功能都是作为任务实现的。

您可以使用 Kaspersky Industrial CyberSecurity for Nodes 控制台树中的任务上下文菜单和结果窗格来管理这些任务。可在结果窗格中查看任务状态信息。任务管理操作记录在系统审核日志中。

Kaspersky Industrial CyberSecurity for Nodes 任务分为两种类型：*本地*和*组*。

本地任务

本地任务只能在为其创建的受保护设备上执行。根据启动方式，存在以下几种类型的本地任务：

- **本地系统任务**。这些任务在安装 Kaspersky Industrial CyberSecurity for Nodes 过程中自动创建。您可以更改除*更新回滚*任务之外的所有本地系统任务的设置。无法重命名或删除本地系统任务。您可以同时运行本地系统和自定义按需扫描任务。
- **本地自定义任务**。在应用程序控制台中，您可以创建按需扫描任务、更新任务和基线系统完整性监控任务。在 Kaspersky Security Center 中，您可以创建按需扫描任务、更新任务等。您可以重命名、配置或删除自定义任务。可同时运行多个自定义任务。

组任务

您可以从 Kaspersky Security Center 管理组任务和受保护设备集任务。所有组任务都是自定义任务。组任务也显示在应用程序控制台中。在应用程序控制台中，只能查看组任务的状态。您不能使用应用程序控制台来管理或配置组任务。

手动启动、暂停、恢复和停止任务

您可以手动启动、暂停、恢复或停止任务。这些选项并非适用于所有 Kaspersky Industrial CyberSecurity for Nodes 任务。

要启动、暂停、恢复或停止任务：

1. 在应用程序控制台中，打开任务的上下文菜单。
2. 选择以下命令之一：**启动** 或 **暂停**。

该操作将执行并记录到系统审核日志中。

管理任务计划

您可以为计划 Kaspersky Industrial CyberSecurity for Nodes 任务。

配置任务计划设置

在应用程序控制台中，您可以计划何时启动本地系统和自定义任务。但是，您无法计划何时启动组任务。

要计划任务：

1. 在控制台树中，选择要为其配置计划的任务。
2. 在结果窗格中，单击“**运行模式**”或“**属性**”。
3. 在“**运行模式**”区域中，选择“**根据计划**”。
4. 配置计划：
   a. 在“**频率**”下拉列表中，选择以下选项之一：
      - **分钟**，如果您希望任务每隔几分钟定期运行一次，请在“**运行间隔 <数量> 分钟**”字段输入分钟数。
      - **小时**，如果您希望任务每隔几个小时定期运行一次，请在“**运行间隔 <数量> 小时**”字段输入小时数。
      - **天**，如果您希望任务每隔几天定期运行，请在“**运行间隔 <数量> 天**”字段输入天数。
      - **在指定时间**，如果您希望任务在指定的日期和时间运行一次。
      - **每月**，如果您希望该任务每月运行一次。指定希望运行任务的月份日期和时间（默认情况下，任务在每月 1 日运行）。
      - **在应用程序启动后**，如果您希望在每次启动 Kaspersky Industrial CyberSecurity for Nodes 时运行该任务。
   b. 根据第一步选择的选项指定任务首次启动的时间段或日期和时间。
   c. 您还可以指定应用程序启动后延迟运行任务的时间。
   d. 指定运行任务的登录名和密码。
5. 单击“**确定**”。

将保存任务计划设置。

启用和禁用计划任务

可在配置计划设置之前或之后启用和禁用计划任务。

要启用或禁用已计划任务的启动：

1. 在应用程序控制台树中选择必要的任务。
2. 在结果窗格中，单击“**运行模式**”。
   “**计划和运行模式**”窗口将打开。
3. 在打开的窗口的“**运行模式**”选项卡上，选择以下操作之一：
   - 如果您希望启用任务的启动计划，请选中“**根据计划**”复选框。
   - 如果您希望禁用任务的启动计划，请清空“**根据计划**”复选框。
4. 单击“**确定**”。

   将保存任务计划设置。

使用用户账户启动任务

您可以在系统账户下启动任务，也可以指定其他账户。

关于使用账户启动任务

您可以指定运行以下 Kaspersky Industrial CyberSecurity for Nodes 任务的账户：

- 应用程序启动控制规则生成器
- 设备控制规则生成器
- 日志审查
- 应用程序完整性控制
- 数据库和应用程序模块的更新
- 更新

默认情况下，使用系统账户权限运行这些任务。

在以下情况下，推荐您使用具有正确访问权限的其他账户：

- **更新**任务：如果您已指定在网络上其他设备的共享文件夹作为更新源。
- **更新**任务：如果使用带有内置 Windows NTLM 身份验证的代理服务器来访问更新源。
- **应用程序启动控制规则生成器**任务：如果将生成的规则导出到系统账户无法访问的配置文件（例如，在受保护设备上的共享文件夹中）。

您可以使用系统账户权限启动列出的任务。如果此设备与受保护设备在同一个域中注册，则 Kaspersky Industrial CyberSecurity for Nodes 将执行这些任务并访问网络中的另一台设备上的共享文件夹。在这种情况下，系统账户必须具有对这些文件夹的访问权限。Kaspersky Industrial CyberSecurity for Nodes 将使用账户**<域名\设备名称>**的权限来访问该设备。

指定用户账户以启动任务

在应用程序控制台中指定账户的选项并非适用于所有任务。

要指定用于启动任务的账户：

1. 在应用程序控制台树中，选择要使用特定账户的权限启动的任务。
2. 在结果窗格中，单击“**属性**”链接。
   将打开“**属性：<任务名称>**”窗口。
3. 转到“**运行模式**”选项卡，然后做以下事情：
   a. 选择**任务运行身份**复选框。
   b. 输入您要使用的账户的用户名和密码。

   选定用户必须在受保护设备上经过注册，或者与该计算机在同一域中。
4. 单击“**确定**”。

将保存修改的设置。

导入和导出设置

本节说明如何导出 Kaspersky Industrial CyberSecurity for Nodes 设置。您还将学习如何将特定的应用程序组件设置导出到 XML 配置文件，以及如何将这些设置从配置文件导入回应用程序。

关于导入和导出设置

可以将 Kaspersky Industrial CyberSecurity for Nodes 设置导出到 XML 配置文件，也可以将配置文件中的设置导入到 Kaspersky Industrial CyberSecurity for Nodes 中。可以将所有应用程序设置或仅将单个组件的设置保存到配置文件。

在将 Kaspersky Industrial CyberSecurity for Nodes 的所有设置导出到文件时，将保存常规程序设置以及下列 Kaspersky Industrial CyberSecurity for Nodes 组件和功能的设置：

- 实时文件保护
- 漏洞利用防御
- 网络威胁防护
- 反加密
- 修复引擎
- AMSI 扫描程序
- 应用程序启动控制
- 设备控制
- 防火墙
- 应用程序启动控制规则生成器
- 设备控制规则生成器
- 日志审查
- 系统完整性监控
- PLC 项目完整性检查
- PLC 项目调查
- 在操作系统启动时扫描
- 关键区域扫描
- 应用程序完整性控制
- 可移动驱动器扫描
- 全盘扫描
- 更新数据库和程序软件模块

- 上次更新回滚
- 更新

此外，还可以在文件中保存 Kaspersky Industrial CyberSecurity for Nodes 的常规设置及用户账户的权限。

无法导出组任务设置。

Kaspersky Industrial CyberSecurity for Nodes 将导出程序所使用的所有密码，例如，用于运行任务或连接代理服务器的用户账户设置。导出的密码以加密的形式保存在配置文件中。只有该受保护设备上安装的 Kaspersky Industrial CyberSecurity for Nodes 未重新安装或更新，才能使用它导入密码。

您无法使用安装在其他受保护设备上的 Kaspersky Industrial CyberSecurity for Nodes 导入之前保存的密码。在受保护设备上导入设置后，必须手动输入所有密码。

如果在导出时 Kaspersky Security Center 策略有效，则应用程序将导出该策略所使用的指定值。

可以从包含单个 Kaspersky Industrial CyberSecurity for Nodes 组件设置的配置文件（例如，从未安装全部组件的 Kaspersky Industrial CyberSecurity for Nodes 中创建的文件）导入设置。导入设置后，只有该配置文件中包含的那些 Kaspersky Industrial CyberSecurity for Nodes 设置会发生变化。所有其他设置保持不变。

导入设置时，已被阻止的活动 Kaspersky Security Center 策略的设置不会发生更改。

导出设置

要将设置导出到配置文件：

1. 要导出所有 Kaspersky Industrial CyberSecurity for Nodes 设置，请在“**Kaspersky Industrial CyberSecurity for Nodes**”节点的上下文菜单中，选择“**导出设置**”命令。

   要导出单个组件的设置，请单击结果窗格中的“**导出设置**”。

   卡巴斯基安全网络设置无法导出。必须手动配置卡巴斯基安全网络。

2. 在打开的窗口中，指定您要将设置列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   指定路径时可以使用系统环境变量，但不能使用用户环境变量。

   如果在导出时 Kaspersky Security Center 策略有效，则应用程序将导出该策略使用的设置。

3. 保存文件。

4. 在“**设置导出已成功完成**”窗口中单击“**确定**”按钮。

   Kaspersky Industrial CyberSecurity for Nodes 会将设置列表导出到 XML 文件。

要导出受信任应用程序列表：

1. 在应用程序控制台树中，打开 **Kaspersky Industrial CyberSecurity for Nodes** 节点的上下文菜单。

2. 选择“**配置信任区域设置**”。

3. “**配置信任区域设置**”窗口将打开。

4. 转到“**受信任应用程序**”部分并单击“**设置**”。

   这将打开包含受信任应用程序列表的窗口。

5. 选择您要导出的受信任应用程序。

   如果您未选择任何受信任应用程序，Kaspersky Industrial CyberSecurity for Nodes 将导出所有受信任应用程序。

6. 单击箭头并在下拉列表中选择“**导出**”。

7. 在打开的窗口中，输入您要将受信任应用程序列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

8. 保存文件。

   Kaspersky Industrial CyberSecurity for Nodes 会将受信任应用程序列表导出到 XML 文件。

导入设置

要从保存的配置文件导入设置：

1. 要导入所有 Kaspersky Industrial CyberSecurity for Nodes 设置，请在“**Kaspersky Industrial CyberSecurity for Nodes**”节点的上下文菜单中，选择“**导入设置**”命令。

   要导入单个组件的设置，请单击结果窗格中的“**导入设置**”。

   将 Kaspersky Industrial CyberSecurity for Nodes 设置或其功能组件常规设置导入到在受保护设备之后，无法恢复到先前的设置。

   无法导入卡巴斯基安全网络设置。必须手动配置卡巴斯基安全网络。

2. 在显示的窗口中，选择要从中导入设置的 XML 配置文件，然后单击“**打开**”。

3. 在“**设置导入已成功完成**”窗口中单击“**确定**”按钮。

4. 在应用程序控制台工具栏中，单击“**更新**”按钮。

应用程序控制台窗口将显示已导入的设置。

如果受保护设备上的 Kaspersky Industrial CyberSecurity for Nodes 进行了重新安装或更新，Kaspersky Industrial CyberSecurity for Nodes 不会从在其他受保护设备上或同一受保护设备上创建的文件导入密码（用于启动任务或连接到代理服务器的账户凭据）。导入完成后，必须手动输入密码。

要导入受信任应用程序列表：

1. 在应用程序控制台树中，打开 **Kaspersky Industrial CyberSecurity for Nodes** 节点的上下文菜单。

2. 选择“**配置信任区域设置**”。

3. “**配置信任区域设置**”窗口将打开。

4. 转到“**受信任应用程序**”部分并单击“**设置**”。

5. 单击箭头并在下拉列表中选择“**导入**”。

6. 在打开的窗口中，选择要从中导入受信任应用程序列表的 XML 文件。

7. 打开文件。

   如果计算机已经具有受信任应用程序的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

8. 该列表显示在“**受信任应用程序**”选项卡。单击“**确定**”。

查看保护状态和 Kaspersky Industrial CyberSecurity for Nodes 信息

要查看有关 Kaspersky Industrial CyberSecurity for Nodes 的设备保护状态的信息，

在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点。

默认情况下，将自动刷新 Kaspersky Industrial CyberSecurity for Nodes 控制台的详细信息窗格中的信息：

- 对于本地连接，每 10 秒钟刷新一次。
- 对于远程连接，每 15 秒钟刷新一次。

您可以手动刷新信息。

*要在“**Kaspersky Industrial CyberSecurity for Nodes**”节点中手动刷新信息，*

请在“**Kaspersky Industrial CyberSecurity for Nodes**”节点的上下文菜单中选择“**刷新**”命令。

Kaspersky Industrial CyberSecurity for Nodes 控制台的详细信息窗格中会显示以下应用程序信息：

- “卡巴斯基安全网络使用”状态。
- 设备保护状态。
- 有关数据库和应用程序模块更新的信息。
- 实际诊断数据。
- 受保护设备控制任务的数据。
- 授权许可信息。

- 工业网络保护状态。
- 与 Kaspersky Security Center 的集成状态：已安装与应用程序连接的 Kaspersky Security Center 的服务器的详细信息；有关活动策略控制的应用程序任务的信息。

使用颜色编码来显示保护状态：

- *绿色*。根据配置的设置运行任务。保护处于活动状态。
- *黄色*。任务未启动，已暂停或已停止。可能会发生安全威胁。推荐您配置并启动任务。
- *红色*。任务完成，但出现错误，或任务运行时检测到安全威胁。推荐您启动任务或采取措施消除检测到的安全威胁。

此块中的某些详细信息（例如，任务名称或检测到的威胁数量）为单击后将转至相关任务的节点或打开任务日志的链接。

"**KSN 使用**"部分显示当前任务状态，例如，*正在运行*、*已停止*或者*从未执行*。该指示器可以使用以下值：

- 面板为绿色 – "**KSN 使用**"任务正在运行，并且对状态的文件请求正在发送到 KSN。
- 面板为黄色 – 其中一项声明已被接受，但任务未运行；或任务正在运行，但文件请求未发送到 KSN。
- 面板为红色 – 任务失败。

计算机保护

"**计算机保护**"部分（请参见下表）显示有关设备当前保护状态的信息。

有关设备保护状态的信息

"保护"部分	信息
设备保护状态指示器	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下值： • 面板为绿色 – 默认显示此颜色，指示"实时文件保护"组件已安装且任务正在运行。 • 面板为黄色 – 指示"实时文件保护"组件未安装，且"*关键区域扫描*"任务已长时间未执行。 • 面板为红色 – 实时文件保护任务未运行。
实时文件保护	**状态** – 组件的当前状态，例如，"*正在运行*"或者"*已禁用*"。
关键区域扫描	**上次扫描日期** - 上次在关键区域扫描病毒和其他计算机安全威胁的日期和时间。 *从未执行* – 在过去 30 天或更长时间（默认值）内没有执行"*关键区域扫描*"任务时所发生的一个事件。您可以更改产生此事件的阈值。
网络威胁防护	**状态** – 组件的当前状态，例如，"*正在运行*"或者"*已禁用*"。
漏洞利用防御	**状态** – 组件的当前状态，例如，"*正在运行*"或者"*已禁用*"。 **操作模式** – 漏洞利用防御任务的两种可用模式之一：**阻止**或者**通知**。
反加密	**状态** – 组件的当前状态，例如，"*正在运行*"或者"*已禁用*"。 **操作模式** – 反加密任务的三种可用模式之一："**删除**"或者"**通知**"。

更新

"**更新**"部分（请参见下表）显示有关当前数据库和应用程序模块状况的信息。

有关 Kaspersky Industrial CyberSecurity for Nodes 数据库和模块状态的信息

“更新”部分	信息
数据库和应用程序模块的状态指示器	带有部分名称的面板的颜色反映了数据库和应用程序模块的状态。该指示器可以使用以下值： • 面板为绿色 – 默认显示此颜色，指示应用程序数据库处于最新状态，并且最近的数据库更新任务已成功完成。 • 面板为黄色 – 指示数据库已过期，或者上次数据库和模块更新任务失败。 • 面板为红色 – 事件“*数据库已严重过期*”或者“*数据库已为最新*”已经发生。
数据库更新	**数据库状态** – 数据库更新状态的评估。 该选项可以采用以下值： • **数据库已为最新** – 应用程序数据库在之前 7 天内进行过更新（默认）。 • **数据库已过期** – 应用程序数据库在 7 至 14 天前更新（默认）。 • **数据库已严重过期** – 应用程序数据库已更新超过 14 天（默认）。 您可以更改产生“*数据库已过期*”和“*数据库已严重过期*”事件的阈值。 **数据库发布日期** – 最新数据库更新的发布日期和时间。日期和事件指定为 UTC 格式。 **最新完成的“数据库更新”任务的状态** – 最新数据库更新的日期和时间。日期和时间根据受保护设备的当地时间指定。如果发生“*已失败*”事件，则字段的值为红色。

控制

“**控制**”部分（请参见下表）显示有关“应用程序启动控制”、“设备控制”和“防火墙”任务的信息。

有关受保护设备控制状态的信息

“控制”部分	信息
受保护设备控制状态指示器	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下值： • 面板颜色为绿色 – 默认显示，表示所有应用程序启动控制组件均已安装，且任务正在活动模式下运行；漏洞利用防御功能已安装并激活。 • 在以下一种或多种情况下，面板颜色为黄色：漏洞利用防御未运行；应用程序启动控制在通知模式下运行；漏洞利用防御在主动模式下运行，并且应用程序启动控制未运行或失败。 • 面板颜色为红色 – 应用程序启动控制任务未运行或失败，漏洞利用防御未运行或处于“**通知**”模式。
应用程序启动控制	**状态** – 组件的当前状态，例如，“*正在运行*”或者“*已禁用*”。 **操作模式** –应用程序启动控制任务的两种可用模式之一：**通知**或者**阻止**。
设备控制	**状态** – 组件的当前状态，例如，“*正在运行*”或者“*已禁用*”。 **操作模式** – 设备控制任务的两种可用模式之一：**根据规则**或者**通知**。
防火墙	**状态** – 组件的当前状态，例如，“*正在运行*”或者“*已禁用*”。

诊断

“**诊断**”部分（请参见下表）显示有关“文件完整性监控”和“日志审查”任务的信息。

有关系统审查状态的信息

“诊断”部分	信息
诊断状态指示器	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下值： • 绿色 – 默认显示此颜色，指示一个或两个系统审查组件已安装，且任务正在运行。 • 黄色 – 两个组件均已安装，但其中一个系统审查任务未运行；发生“*未在运行*”事件。 • 红色 – 其中一个任务失败。
系统完整性监控	**状态** – 组件的当前状态，例如，“*正在运行*”或者“*已禁用*”。
日志审查	**状态** – 组件的当前状态，例如，“*正在运行*”或者“*已禁用*”。

“**工业网络保护**”选项卡

“**PLC 项目调查**”部分显示有关包含在保护范围内的 PLC 列表的信息。

有关接收 PLC 数据的信息

“PLC 项目调查”部分	信息
PLC 在保护区状态指示灯	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下值： • 绿色 – 表示该任务至少已成功完成一次。 • 黄色 – 表示从未进行过调查。 • 红色 – 任务失败。
PLC 项目调查	**状态** – 组件的当前状态，例如，“*正在运行*”或者“*已禁用*”。

“**PLC 项目完整性检查**”部分显示有关受保护 PLC 的数量和完整性违规事件的信息。

有关 PLC 项目完整性检查任务的信息

“PLC 项目完整性检查”部分	信息
PLC 完整性状态指示器	带有此部分名称的面板的颜色反映了在该部分中正在执行的任务的状态。该指示器可以使用以下值： • 绿色 – 表示该任务至少已成功完成一次。 • 黄色 – 表示从未执行完整性检查。 • 红色 – 任务失败。
PLC 项目完整性检查	**状态** – 组件的当前状态，例如，“*正在运行*”或者“*已禁用*”。

Kaspersky Industrial CyberSecurity for Nodes 授权信息显示在 **Kaspersky Industrial CyberSecurity for Nodes** 节点的详细信息窗格左下角的行中。

您可以按照“应用程序属性”链接配置 Kaspersky Industrial CyberSecurity for Nodes 属性。

您可以点击“连接到远程计算机”链接连接到不同的受保护设备。

从 Web Console 使用 Web 插件

本节提供有关 Kaspersky Industrial CyberSecurity for Nodes 管理插件的信息，并介绍如何管理一台或一组受保护设备上安装的应用程序。

从 Web Console 管理 Kaspersky Industrial CyberSecurity for Nodes

您可以使用 Kaspersky Industrial CyberSecurity for Nodes Web 插件集中管理多台安装了 Kaspersky Industrial CyberSecurity for Nodes 并加入同一管理组的受保护设备。通过 Kaspersky Security Center Web Console 还可以单独配置管理组中包含的每台受保护设备的设置。

*管理组*是在 Kaspersky Security Center Web Console 上手动创建的。该组包括您要为其配置相同的控制和保护设置并已安装了 Kaspersky Industrial CyberSecurity for Nodes 的多个设备。有关使用管理组的详细信息，请参见 *Kaspersky Security Center 帮助*。

如果 Kaspersky Industrial CyberSecurity for Nodes 在某台受保护设备上的运行受活动 Kaspersky Security Center 策略的控制，则该台受保护设备的应用程序设置不可用。

可通过以下方式通过 Kaspersky Security Center Web 控制台管理 Kaspersky Industrial CyberSecurity for Nodes：

- **使用 Kaspersky Security Center 策略**。可使用 Kaspersky Security Center 策略为一组设备远程配置相同的保护设置。在活动策略中指定的任务设置的优先级高于在应用程序控制台中本地配置或在 Kaspersky Security Center Web Console 的“属性：<受保护设备名称>”窗口中远程配置的任务设置的优先级。策略可用于配置常规应用程序设置、实时计算机保护任务的设置、设备上的活动控制任务设置、网络存储保护任务设置以及按计划启动本地系统任务的设置。

- **使用 Kaspersky Security Center 组任务**。使用 Kaspersky Security Center 组任务可远程配置任务的通用设置，一组设备具有过期期限。您可使用组任务激活应用程序，配置“按需扫描”任务设置，更新任务设置，以及“应用程序启动控制规则生成器”任务设置。

- **使用一组设备的任务**。使用一组设备的任务允许远程配置通用任务设置，不属于任何管理组的受保护设备具有有限执行期限。

- **使用单个设备的属性窗口**。在设备属性窗口中，您可远程配置管理组中包含的单台受保护设备的任务设置。如果选中的受保护设备不受活动 Kaspersky Security Center 策略的控制，您可配置常规应用程序设置和所有 Kaspersky Industrial CyberSecurity for Nodes 任务的设置。

Kaspersky Security Center Web Console 可以配置应用程序设置和高级功能，还可以使用日志和通知。您可以为一组受保护设备和单台受保护设备配置这些设置。

Web 插件限制

与 Kaspersky Industrial CyberSecurity for Nodes 管理插件相比，Kaspersky Industrial CyberSecurity for Nodes Web 插件具有以下限制：

- 无法使用数字证书或 Kaspersky Security Center 事件创建“应用程序启动控制”任务规则。
- 无法根据连接的设备或系统数据生成“设备控制”任务规则。

管理应用程序设置

本部分包含有关在 Kaspersky Security Center Web Console 中配置 Kaspersky Industrial CyberSecurity for Nodes 常规设置的信息。

在 Web 插件中配置常规应用程序设置

您可以在 Web 插件中为一组受保护设备或一台受保护设备配置 Kaspersky Industrial CyberSecurity for Nodes 常规设置。

在 Web 插件中配置界面和扫描设置

要配置应用程序界面设置：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**应用程序设置**”部分。
5. 在“**界面设置**”字部分中单击“**配置**”。
6. 按下表所述配置设置。

用户交互设置和扫描设置

参数	描述
用户交互	"**不显示用户界面**"。在客户端计算机上，不显示 Kaspersky Industrial CyberSecurity for Nodes 操作的迹象。Windows 通知区域中的图标和通知不可用。 "**显示用户界面**"。在客户端计算机上，Windows 托盘中有一个图标。在该图标的上下文菜单中，用户可以使用 Kaspersky Industrial CyberSecurity for Nodes 执行操作。Kaspersky Industrial CyberSecurity for Nodes 还会在应用程序图标上方显示通知。Windows 系统托盘中图标的上下文菜单可让您打开小型诊断窗口。单击小型诊断窗口中的链接即可打开应用程序控制台。
在通知区域显示应用程序状态	选择您要在 Microsoft Windows 通知区域中看到通知的事件类型旁的复选框。

在 Web 插件中配置安全和可靠性设置

若要手动配置安全性设置，请执行以下步骤：

1. 在 Web Console 的主窗口中，选择"**资产(设备)**" → "**策略和配置文件**"。
2. 单击要配置的策略名称。
3. 在打开的"**<策略名称>**"窗口中，选择"**应用程序设置**"选项卡。
4. 选择"**应用程序设置**"部分。
5. 在"**安全性和可靠性**"字部分中单击"**配置**"。
6. 按下表所述配置设置。

安全性和可靠性设置

参数	描述
在计算机开启时启动应用程序(建议)	选中该复选框后，将在加载操作系统过后启动 Kaspersky Industrial CyberSecurity for Nodes，从而在整个会话期间保护计算机。 清除该复选框后，不会在加载操作系统后启动 Kaspersky Industrial CyberSecurity for Nodes，直到用户手动启动该软件。计算机保护已禁用，用户数据可能受到威胁。
保护应用程序进程免受外部威胁	当选中此选框时，Kaspersky Industrial CyberSecurity for Nodes 可避免修改或删除硬盘驱动器中的应用程序文件、内存进程和系统注册表中的条目。
保护操作系统服务	如果启用了操作系统服务保护，第三方应用程序就无法对操作系统的进程采取行动。 如果禁用了操作系统服务保护，第三方应用程序就可以对操作系统的进程采取行动。
使用电池供电时推迟计划任务	如果选中此复选框，则启用节能模式。Kaspersky Industrial CyberSecurity for Nodes 延迟计划任务。如果需要，您可以手动启动扫描和更新任务。 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： • *数据库和应用程序模块的更新* • *全盘扫描* • *关键区域扫描* • *自定义扫描* • *应用程序完整性控制* • "*IOC 扫描*"。

参数	描述
应用设置时的计算机状态	应用策略或执行任务出错时，安装了 Kaspersky Industrial CyberSecurity for Nodes 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*关键*。
与远程管理软件的兼容性	如果将 Kaspersky Industrial CyberSecurity for Nodes 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 与应用程序安全桌面功能不兼容有关。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。 如果选中此复选框，则启用 RAT 兼容模式。应用程序会显示一个没有此功能的确认对话框。这可能降低计算机的安全级别。如果 Kaspersky Industrial CyberSecurity for Nodes 不会导致您的 RAT 出现问题，我们不建议启用兼容模式。 如果清除该复选框，则禁用 RAT 兼容模式。默认下，复选框被清除。 示例：在 RemoteApp 模式下使用浏览器时，Kaspersky Industrial CyberSecurity for Nodes 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。
限制扫描任务的 CPU 使用率	Kaspersky Industrial CyberSecurity for Nodes 在按需扫描任务期间会将对受保护设备 CPU 的使用率限制为“**上限**”字段中指定的值。 但是，由于其他组件的存在，应用程序可能会使用更多的 CPU 时间。 启用此功能可能会对 Kaspersky Industrial CyberSecurity for Nodes 的性能产生负面影响。 默认情况下，禁用此功能。
为其他应用程序让出资源	Kaspersky Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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。

在 Web 插件中配置连接设置

配置的连接设置用于将 Kaspersky Industrial CyberSecurity for Nodes 连接到更新和激活服务器，以及在将应用程序与 KSN 服务集成期间使用。

若要配置连接设置，请执行以下步骤：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**应用程序设置**”部分。
5. 在“**连接设置**”字部分中单击“**配置**”。
6. 按下表所述配置设置。

连接设置

参数	描述
限制计量连接的流量	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 Industrial CyberSecurity for Nodes 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。 计量网络运行在 Windows 8 或更新版本的计算机上。
不使用代理服务器	如果选择此选项，Kaspersky Industrial CyberSecurity for Nodes 会直接连接到 KSN 服务，而不使用任何代理服务器。
自动检测代理服务器设置	如果选择此选项，Kaspersky Industrial CyberSecurity for Nodes 会自动定义代理服务器设置。
使用指定的代理服务器	如果选择此选项，Kaspersky Industrial CyberSecurity for Nodes 会使用手动指定的代理服务器设置连接到 KSN。
对本地地址不使用代理服务器	此复选框用于在访问与安装了 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备位于同一网络上的设备时启用或禁用代理服务器。 如果选中该复选框，则会直接通过托管已安装了 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备的网络访问设备。不使用代理服务器。 如果清除该复选框，将使用代理服务器连接到本地设备。 默认选中该复选框。
代理服务器身份验证设置	指定身份验证设置
不使用身份验证	不执行身份验证。
NTLM 身份验证	使用由 Microsoft 开发的 NTLM 网络身份验证协议执行身份验证。默认选择该模式。
使用用户名和密码的 NTLM 身份验证	使用由 Microsoft 开发的 NTLM 网络身份验证协议执行带用户名和密码的身份验证。
用户名和密码	使用用户名和密码执行身份验证。
监控所有网络端口	在此网络端口监控模式下，保护组件会监控通过任何开放的计算机网络端口传输的数据流。
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。
激活应用程序时使用 Kaspersky Security Center 作为代理服务器	指定是否将 Kaspersky Security Center 用作应用程序激活的代理服务器。

在 Web 插件中配置本地任务的计划启动

您可以使用策略来允许或阻止本地系统“按需扫描”任务和“更新”任务的启动。此操作根据管理组中每个受保护设备上本地配置的计划来完成：

- 如果特定类型的本地系统任务的计划启动受到策略禁止，则这些任务将不会按照计划在受保护设备上执行。您可以手动启动该本地系统任务。
- 如果特定类型的本地系统任务的计划启动被策略允许，则这些任务将按照为此任务进行的本地配置的计划参数来执行。

默认情况下，策略会禁止本地系统任务的启动。

如果更新或按需扫描受 Kaspersky Security Center 组任务的管理，我们推荐不要允许本地系统任务启动。

如果不使用组更新或按需扫描任务，则允许在策略中启动本地系统任务：Kaspersky Industrial CyberSecurity for Nodes 将执行应用程序数据库和模块更新，并根据默认计划启动所有本地系统按需扫描任务。

您可使用策略允许或阻止以下本地系统任务的计划启动：

- 按需扫描任务：*关键区域扫描、在操作系统启动时扫描、应用程序完整性控制、基线系统完整性监控。*
- 更新任务：数据库和应用程序模块的更新，应用程序更新。

如果受保护设备被从管理组中排除，将自动启用本地系统任务计划。

要在策略中允许或阻止 Kaspersky Industrial CyberSecurity for Nodes 本地系统任务的计划启动：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**应用程序设置**”部分。
5. 在“**运行本地系统任务**”字部分中单击“**配置**”。
6. 按下表所述配置设置。

启动本地任务的设置

参数	描述
允许使用本地任务	如果选择此复选框，本地任务将显示在 Kaspersky Industrial CyberSecurity for Nodes 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。 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 Industrial CyberSecurity for Nodes 本地界面中启动或编辑，使用命令行工作时也无法进行。
允许计划管理	如果选中“**允许使用本地任务**”复选框，则该复选框可用。 如果选中该复选框，则计划管理将在应用程序控制台的本地任务属性中变为可用。 默认下，复选框被清除。
允许显示组任务	如果选择此复选框，组任务将显示在 Kaspersky Industrial CyberSecurity for Nodes 的本地界面上。用户可以在应用程序控制台中查看所有任务的列表。 如果清除该复选框，则 Kaspersky Industrial CyberSecurity for Nodes 将显示空任务列表。
允许管理组任务	如果选中该复选框，则用户可以启动和停止在 Kaspersky Security Center 中指定的组任务。用户可以在应用程序控制台或简化应用程序界面中启动和停止任务。 如果清除该复选框，则 Kaspersky Industrial CyberSecurity for Nodes 将自动启动计划任务，或者由管理员在 Kaspersky Security Center 中手动启动任务。

在 Web 插件中配置隔离和备份设置

要在 Kaspersky Security Center 中配置常规隔离和备份设置：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 选择“**补充**”部分。
5. 在“**存储**”子部分中单击“**设置**”按钮。

6. 按下表所述配置设置。

存储设置

参数	描述
在“**报告**”选项卡上，指定报告设置：	
存储报告时间不超过	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。报告的默认最大存储条件为 30 天。在此时间之后，Kaspersky Industrial CyberSecurity for Nodes 将自动删除报告文件中的最早条目。
限制报告文件大小为	如果选中该复选框，则最大报告文件大小限制为定义值。默认情况下，最大文件大小数据为 1024 MB。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 Industrial CyberSecurity for Nodes 将自动删除报告文件中的最早条目。
在“**备份区**”选项卡上，指定备份设置：	
存储对象时间不超过	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。文件的默认最大存储条件为 30 天。最长存储期限到期后，Kaspersky Industrial CyberSecurity for Nodes 将删除备份区中最旧的文件。
限制备份区大小为	如果选中该复选框，则最大存储大小限制为定义值。默认情况下，最大大小为 400 MB。为避免超过最大存储大小，当达到最大存储大小时，Kaspersky Industrial CyberSecurity for Nodes 将自动删除存储中的最早文件。
可用空间阈值	该复选框用于启用或禁用监控备份中的最小可用空间大小（默认值为 100 MB）的功能。如果可用空间大小下降到低于指定阈值，Kaspersky Industrial CyberSecurity for Nodes 会记录“已超过备份区可用空间阈值”事件，并根据此事件类型的通知设置发布通知。 如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控备份中的可用空间的大小。 如果选中“**限制备份区大小为**”复选框被选中，则“**可用空间阈值**”复选框被激活。 默认选中该复选框。
在“**隔离区**”选项卡上，指定隔离设置：	
限制隔离区大小为	最大隔离区大小 (MB)。例如，您可以将最大隔离区大小设置为 200 MB。当隔离区达到最大大小时，Kaspersky Industrial CyberSecurity for Nodes 将相应的事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序停止隔离新对象。您必须手动清空隔离区。
可用空间阈值	该复选框用于启用或禁用监控隔离区中的最小可用空间大小（默认值为 50 MB）的功能。如果可用空间大小下降到低于指定阈值，Kaspersky Industrial CyberSecurity for Nodes 会记录“*已超过隔离区可用空间阈值*”事件，并根据此事件类型的通知设置发布通知。 如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控隔离区中的可用空间的大小。 默认选中该复选框。

创建和配置策略

本节提供有关使用 Kaspersky Security Center 策略在多个受保护设备上管理 Kaspersky Industrial CyberSecurity for Nodes 的信息。

可以创建全局性 Kaspersky Security Center 策略，以便管理多个安装了 Kaspersky Industrial CyberSecurity for Nodes 的设备上的保护。

策略在一个管理组的所有受保护设备上实施 Kaspersky Industrial CyberSecurity for Nodes 设置、功能和指定的任务。

可以为一个管理组依次创建和实施多个策略。该策略当前对 Web Console 中具有“*活动*”状态的组有效。

Kaspersky Industrial CyberSecurity for Nodes 系统审核日志中记录了有关策略实施情况的信息。可在应用程序控制台的“**日志和通知**”节点中查看该信息。

Kaspersky Security Center 提供一种在受保护设备上应用策略的方式：*禁止更改策略*。应用策略后，Kaspersky Industrial CyberSecurity for Nodes 将使用您在受保护设备上的策略属性中为其选择了图标的设置。在这种情况下，将使用所选设置，而不是应用策略之前生效的设置。Kaspersky Industrial CyberSecurity for Nodes 不会应用在策略属性中为其选择了 图标的活动策略设置。

如果策略为活动的，则策略中标记 图标的设置的值在应用程序控制台中显示，但无法编辑。其他设置的值（策略中标记 图标）可在应用程序控制台中编辑。

活动策略中配置的且标记图标的设置也会阻止在 Kaspersky Security Center 的“**属性：<受保护设备名称>**”窗口中针对单台受保护设备进行更改。

在禁用活动策略后，使用活动策略指定并发送到受保护设备的设置将保存在本地任务设置中。

如果某个策略定义了当前正在运行的任一实时计算机保护任务和网络存储保护任务的设置，则该策略定义的设置将在应用该策略后立即更改。如果任务未运行，则设置将在该任务启动时应用。

如何在 Kaspersky Security Center Web Console 中创建策略

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击“**添加**”。
3. “**新策略**”窗口将打开。
4. 在“**选择应用程序**”部分中，选择“Kaspersky Industrial CyberSecurity for Nodes”。
5. 指定受保护设备上的 Kaspersky Industrial CyberSecurity for Nodes 模式。
6. 如果有必要，请指定要从所有或部分应用程序组件的扫描中排除的文件或文件夹以及对象的名称（根据病毒百科全书）。
7. 在“**常规**”选项卡上，可以执行以下操作：
   - 更改策略名称。

     策略名称不能包含以下符号： `" * < : > ? \ |` 。
   - 选择策略状态：
     - “**活动**”。下次同步后，该策略将用作计算机上的活动策略。
     - “**不活动**”。备份策略。如有必要，不活动策略可切换为活动状态。
     - “**漫游**”。当计算机离开组织网络周界时，将激活该策略。
   - 配置设置继承：
     - “**从父策略继承设置**”。如果打开此切换按钮，策略设置值将继承自顶级策略。如果为父策略设置了，则无法编辑策略设置。
     - “**在子策略中强制继承设置**”。如果开启该切换按钮，策略设置的值将传播到子策略。在子策略设置中，“**从父策略继承设置**”复选框被自动选中。子策略设置继承自父策略，但标记了 的设置除外。如果为父策略设置了，则无法编辑子策略设置。
8. 在“**应用程序设置**”选项卡上，根据需要配置策略设置。
9. 单击“**保存**”。

所创建的策略将显示在选定管理组的“**策略和配置文件**”选项卡上的策略列表中。在“**<策略名称>**”窗口中，您可配置 Kaspersky Industrial CyberSecurity for Nodes 的其他设置、任务和功能。

创建新策略后，会创建一组允许规则，以防止应用程序被阻止，保证应用程序不间断运行。您可以在任务设置中查看默认规则。有关详细信息和限制，请参阅下文。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 在创建新策略时会创建一组入站网络流量规则：

- 使用 Kaspersky Security Center 网络代理共享 Windows 桌面的过程的两个允许规则，该代理位于 %Program Files% 和 %Program Files (x86)% 文件夹中。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。
- 本地端口 15000 的两个允许规则。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 在创建新策略时会创建一组传出网络流量规则：

- Kaspersky Industrial CyberSecurity for Nodes 服务的两个允许规则，该服务位于 %Program Files% 和 %Program Files (x86)% 文件夹中。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。
- Kaspersky Industrial CyberSecurity for Nodes 工作进程的两个允许规则，该应用程序位于 %Program Files% 和 %Program Files (x86)% 文件夹中。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。
- 本地端口 13000 的两个允许规则。状态：启用。允许的外部地址：全部。协议：TCP 和 UDP，每个协议一个规则。

使用 Kaspersky Security Center 创建和配置任务

本节包含有关 Kaspersky Industrial CyberSecurity for Nodes 任务、如何创建任务、配置任务设置，以及启动和停止任务的信息。

关于 Web 插件中的任务创建

您可采用以下方式创建本地和组任务：

- 对于一台受保护设备：在“**属性 <受保护设备名称>**”窗口的“**任务**”部分中。
- 对于管理组：在选定受保护设备组的节点的详细信息窗格中的“**任务**”选项卡上。
- 对于一组受保护设备：在“**设备分类**”节点的详细信息窗格中。

您可以使用策略禁用同一管理组中所有受保护设备上的“*更新*”和“*按需扫描*”本地系统任务的计划。

有关 Kaspersky Security Center 中任务的常规信息，请参见 *Kaspersky Security Center 帮助*。

在 Web 插件中创建任务

要在 Kaspersky Security Center Web Console 中创建新任务：

1. 采用以下方式之一启动任务向导：

   - 若要创建本地任务：

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

     b. 单击受保护设备名称。

     c. 在打开的“**<设备名称>**”窗口中，选择“**任务**”选项卡。

     d. 单击“**添加**”。

   - 创建组任务：

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

     b. 单击“**添加**”。

   将打开任务向导窗口。

2. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。

3. 在“**任务类型**”下拉列表中，选择要创建的任务的类型。

4. 根据所选的任务类型，执行下列操作之一：

   - 创建按需扫描任务。

   - 要创建更新任务，请根据您的需要配置任务设置：

     a. 您可在“**更新源**”块中将 Kaspersky Security Center 管理服务器或卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。

     如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。

     b. 配置减少磁盘子系统负载的功能设置：

     c. 您可以指定 Kaspersky Industrial CyberSecurity for Nodes 在需要关键应用程序模块更新时以及关键更新安装完成后将执行的操作。此外，您还可以指定 Kaspersky Industrial CyberSecurity for Nodes 是否接收有关可用计划更新的信息。

     d. 指定要复制的更新集和 Kaspersky Industrial CyberSecurity for Nodes 将用于存储已复制更新的文件夹的路径。

- 要创建“应用程序激活”任务：

  a. 在“**选择授权许可密钥**”窗口中，指定您要使用的密钥文件或激活码来激活应用程序。

  b. 如果您想要创建用于续订授权许可的任务，请选中“**用作备用密钥**”复选框。

- 创建并配置“应用程序启动控制规则生成器”任务。
- 创建并配置“设备控制规则生成器”任务。

5. 单击“**下一步**”。
6. 如果是为一组受保护设备创建任务，请选择将执行该任务的受保护设备网络（或组）。
7. 单击“**下一步**”。
8. 在“**完成任务创建**”窗口中，如果要配置任务设置，请选中“**创建完成时打开任务详情**”复选框。
9. 单击“**完成**”。

所创建的任务将显示在“**任务**”列表中。

在 Web 插件中配置组任务

要为多个受保护设备配置组任务：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**<任务名称>**”窗口。
3. 转到“**应用程序设置**”选项卡。
4. 根据所配置的任务类型，执行下列操作之一：

   - 要配置“*按需扫描*”任务：

     a. 在“**扫描范围**”部分中，配置扫描范围。

     b. 在“**选项**”部分中，配置启发式分析级别和与其他应用程序组件的集成。

   - 要配置*更新*任务，请根据您的需要调整任务设置：

     a. 在“**更新源**”部分中，配置更新源设置。

     b. 在“**更新设置**”部分，管理磁盘子系统优化设置，指定当应用程序模块的关键更新可用或有关计划更新的信息可用时，您希望 Kaspersky Industrial CyberSecurity for Nodes 执行的操作；指定更新复制设置。

   - 要配置“*应用程序激活*”任务，请应用您要用于激活应用程序的密钥文件或激活码。如果您想要添加用于续订授权许可的激活码或密钥文件，请选中“**用作附加密钥**”复选框。
   - 要配置设备控制允许规则的自动生成，请指定将用于创建允许规则列表的设置。

5. 在“**计划**”部分中配置任务计划（您可为除“*更新回滚*”外的所有任务类型配置计划）。

6. 在“**账户**”部分中的“**设置**”选项卡上，指定将使用其权限运行任务的账户。有关此节中配置设置的详细信息，请参见 *Kaspersky Security Center 帮助*。

7. 单击“**保存**”。

将保存新配置的组任务设置。

在 Web 插件中配置应用程序激活任务

要配置“应用程序激活 ”任务：

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

2. 单击 Kaspersky Security Center 任务列表中的任务名称。

   将打开“**<任务名称>**”窗口。

3. 在“**应用程序设置**”部分中，指定您要使用的密钥文件来激活应用程序。如果要添加用于续订授权许可的密钥，请选中“**用作备用密钥**”复选框。

4. 在“**计划**”部分中配置任务计划。

5. 在“**<任务名称>**”窗口中，单击“**保存**.”。

在 Web 插件中配置更新任务

要配置“更新 ”任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。

2. 单击 Kaspersky Security Center 任务列表中的任务名称。

   将打开“<任务名称>”窗口。

3. 选择**应用程序设置**选项卡。

4. 在“**更新源**”部分中，配置更新源设置：

   a. 将 Kaspersky Security Center 管理服务器或卡巴斯基更新服务器指定为应用程序更新源。您也可以创建自定义更新源列表：通过手动添加自定义 HTTP 和 FTP 服务器或网络文件夹，并将他们设置为更新源。

   如果手动自定义的服务器不可用，您可指定使用 卡巴斯基更新服务器。

   b. 配置减少磁盘子系统负载的功能设置：

   - **降低磁盘 I/O 的负载**
   - **用于优化的 RAM (MB)**

c. 指定当应用程序模块的关键更新可用或有关于计划更新的信息时，Kaspersky Industrial CyberSecurity for Nodes 应执行的操作。

d. 指定更新复制设置。

5. 在“**计划**”部分中配置任务计划（您可为除“*更新回滚*”外的所有任务类型配置计划）。

6. 在“**<任务名称>**”窗口中，单击“**确定**”。

管理任务计划

您可以为计划 Kaspersky Industrial CyberSecurity for Nodes 任务。

计划任务

您可以在 Web Console 中计划本地系统和自定义任务。

要使用 Web Console 计划组任务：

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

2. 单击 Kaspersky Security Center 任务列表中的任务名称。
将打开“**<任务名称>**”窗口。

3. 转到“**计划**”部分并根据需要配置计划。

如果 Kaspersky Security Center 策略阻止按需扫描任务和更新任务的计划，则这些任务的计划设置字段将不可用。

a. 在“**启动任务**”下拉列表中，选择以下选项之一：

- **每 N 小时**，如果您希望任务每隔几个小时定期运行一次，请在“**间隔**”字段输入小时数。
- **每 N 天**，如果您希望任务每隔几天定期运行，请在“**间隔**”字段输入天数。
- **每 N 分钟**，如果您希望任务每隔几分钟定期运行一次，请在“**间隔**”字段输入分钟数。
- **按星期中的天数**，如果您希望任务在一周的某一天运行；还请指定您希望它运行的时间。

在 Kaspersky Security Center 15.1 中，您可以每隔几周运行一次任务（“**周期**”参数）。Kaspersky Industrial CyberSecurity for Nodes 不支持以多周为间隔运行任务。如果您为 Kaspersky Industrial CyberSecurity for Nodes 计划了一项每隔几周运行一次的任务，则应用程序会在每周指定的天和时间运行该任务。

- **每月**，如果您希望任务在每月的某一天运行；还请指定希望其运行的时间。
- **一次**，如果您想在指定的日期和时间运行一次任务。

- **手动**，如果您想手动运行该任务。
- **在程序启动时**，如果您希望在每次启动 Kaspersky Industrial CyberSecurity for Nodes 时运行该任务。
- **当新更新下载至存储库时**，如果您希望每次将更新下载到存储库时运行该任务。
- **在检测到病毒爆发时**，如果您希望在检测到病毒攻击时运行该任务。
- **在完成其他任务时**，如果您希望该任务在另一个任务完成后运行。

b. 在“**开始时间**”和“**日期**”字段中，指定第一次任务开始的时间。

4. 在“**附加设置**”块中：
   - 选中“**运行错过的任务**”复选框以允许启动跳过的任务。
   - 如果选中“**使用任务启动自动随机延迟**”复选框，则任务不会严格按计划运行，而是在一定的时间间隔内随机运行，即任务的开始时间是分散的。
   - “**使用 Wake-On-LAN 功能在任务启动之前开启设备**”。如果选中该复选框，则在运行任务之前，计算机的操作系统将有一个指定的提前期来完成启动。默认提前期为 5 分钟。
   - “**任务完成后关闭设备**”。如果选中该复选框，则任务完成后设备将被关闭。
   - “**如果任务运行超过该时间则停止**”。如果选中该复选框，则任务运行时间超过指定时间时将停止。
5. 单击“**保存**”按钮保存任务启动设置。

启用和禁用计划任务

配置计划设置后，您可以禁用计划任务。

要禁用任务启动计划：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。
   将打开“**<任务名称>**”窗口。
3. 转到**应用程序设置**区域。
4. 选择“**计划**”部分。
5. 如果您要启用计划任务启动，请从“**计划开始**”下拉列表中选择运行计划任务的设置。
6. 如果要禁用计划任务启动，请在下拉列表中选择“**手动**”。
7. 单击“**保存**”按钮。

Kaspersky Security Center 中的报告

Kaspersky Security Center 中的报告包含有关受管理设备状态的信息。报告基于管理服务器上存储的信息。

从 Kaspersky Security Center 11 开始，对于 Kaspersky Industrial CyberSecurity for Nodes，以下类型的报告可用：

- 有关应用程序组件状态的报告
- 有关已禁止的应用程序的报告
- 有关在测试模式下禁止的应用程序的报告

有关所有 Kaspersky Security Center 报告以及如何配置它们的详细信息，请参阅 *Kaspersky Security Center 帮助*。

有关 Kaspersky Industrial CyberSecurity for Nodes 组件状态的报告

您可以监视所有网络设备的保护状态，并获得每个设备上的组件集的结构化概览。

报告显示每个组件的以下状态之一：*正在运行*、*已暂停*、*已停止*、*授权许可未涵盖*。

*未安装*状态指的是组件，而不是应用程序本身。如果未安装应用程序，Kaspersky Security Center Web 控制台会分配 N/A（不可用）状态。

您可以创建组件选择并使用筛选来显示具有指定组件集和状态的网络设备。

有关创建和使用选择的详细信息，请参见 *Kaspersky Security Center 帮助*。

要查看 Kaspersky Security Center Web Console 中组件的状态：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。
2. 单击设备名称并转到“**应用程序**”部分。
3. 单击 Kaspersky Industrial CyberSecurity for Nodes 应用程序的名称。
4. 在打开的窗口中，在“**常规**”选项卡上，转到“**组件**”部分。
5. 查看状态表。

要在 Kaspersky Security Center Web Console 中查看标准报告，请执行以下操作：

1. 选择“**监控和报告**”→“**报告**”。
2. 选择“**有关应用程序组件状态的报告**”列表项，然后单击它。
   将生成报告。
3. 查看以下报告详细信息：
   - 图形化图表。
   - 组件和安装了每个组件的网络设备总数以及设备所属的组的汇总表格。
   - 指定了组件状态、版本、设备和组的详细表格。

有关在活动模式和测试模式下禁止的应用程序的报告

根据“应用程序启动控制”任务的结果，可以生成两种类型的报告：有关已禁止的应用程序的报告（如果在活动模式下启动该任务）和有关在测试模式下禁止的应用程序的报告（如果在通知模式下启动该任务）。这两种报告显示了有关网络的受保护设备上阻止的应用程序的信息。每个报告都针对所有管理组生成，并累积来自受保护设备上安装的所有 Kaspersky 应用程序的数据。

要查看有关在通知模式下禁止的应用程序的报告：

1. 在“通知”模式下启动“应用程序启动控制”任务。
2. 选择“**监控和报告**”→“**报告**”。
3. 选择“**有关在测试模式下禁止的应用程序的报告**”列表项，然后单击它。
   将生成报告。
4. 查看以下报告详细信息：
   - 显示阻止启动次数最多的前 10 个应用程序的图形化图表。
   - 应用程序阻止行为的汇总表格，其中指定可执行文件名、原因、阻止时间和发生阻止的设备数量。
   - 指定了有关设备、文件路径和阻止条件的数据的详细表格。

要查看有关在活动模式下禁止的应用程序的报告：

1. 在“活动”模式下启动“应用程序启动控制”任务。
2. 选择“**监控和报告**”→“**报告**”。
3. 选择“**禁止的应用程序报告**”列表项并单击它。
   将生成报告。

此报告包含的阻止数据与有关在测试模式下禁止的应用程序的报告相同。

应用程序授权许可

本节提供了与应用程序授权有关的主要概念的信息。

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。

请仔细查看最终用户授权许可协议的条款，然后再开始使用程序。

您可以通过以下方式阅读描述数据处理和传输的最终用户授权许可协议和隐私策略的条款：

- 在安装 Kaspersky Industrial CyberSecurity for Nodes 期间。
- 在安装 Kaspersky Industrial CyberSecurity for Nodes 控制台期间。
- 在安装 Kaspersky Security Gateway 期间。
- 通过阅读分发包中包含的 license.txt 文件。
- 在卡巴斯基网站 (https://www.kaspersky.com/business/eula)。

安装程序时确认您同意最终用户授权许可协议即表示您同意最终用户授权许可协议中的条款。如果您不接受最终用户授权许可协议的条款，则必须中止程序安装，且不得使用程序。

关于授权许可

*授权许可*是指在有限时间内使用应用程序的权限，这是根据最终用户授权许可协议为您授予的。

有效的授权许可授权您根据最终用户授权许可协议的条款使用该应用程序，并在必要时获得技术支持。

服务范围和应用程序使用期限取决于用于激活应用程序的授权许可类型。

您可以通过两种方式激活应用程序：

- 使用密钥文件，授予您商业授权许可下的使用权
- 使用激活码购买商业授权许可

商业授权许可到期后，只有以下应用程序组件和任务无需数据库更新即可继续使用：

- 实时文件保护
- 系统完整性监控
- 按需扫描任务

要继续使用 Kaspersky Industrial CyberSecurity for Nodes 的所有功能，您必须续费您的商业授权许可。推荐在授权许可到期之前延长其有效期，以确保最大保护。

如果删除授权许可密钥，应用程序将继续运行。系统完整性监控组件仍然可用，其余组件、任务和 Kaspersky Industrial CyberSecurity for Nodes 数据库更新均不可用。如果卡巴斯基将您的授权许可添加到拒绝列表，也会发生同样的情况。

关于授权许可证书

*授权许可证书*是您与密钥文件或激活码一起收到的文档。

授权许可证书包含有关授权许可的以下信息：

- 授权许可标识符或订单号
- 有关被授予授权许可的用户的信息
- 有关可以使用所提供的授权许可激活的应用程序的信息
- 授权单元的数量限制（例如，可以在该授权许可下使用应用程序的设备数量）
- 授权许可有效开始日期
- 授权许可到期日期或授权许可期限
- 授权许可类型

关于密钥

*密钥*是一串位数据，您可以依照最终用户授权许可协议的条款通过该密钥来激活并在激活后使用应用程序。密钥是由 Kaspersky 生成的。

您可以通过密钥文件在应用程序中添加授权许可。在应用程序中添加密钥后，将在应用程序界面中以唯一的字母数字序列形式显示该密钥。

Kaspersky 可以针对违反授权许可协议的行为将密钥添加到拒绝列表中。如果阻止了您的密钥，则必须添加其他密钥以使应用程序正常工作。

有两种类型的密钥：活动密钥和备用密钥。

*活动密钥*是指当前正在使用的密钥文件以使应用程序正常工作。可以将商业授权许可的密钥添加为活动密钥。本应用程序不能拥有两个及以上活动密钥。

*备用密钥*是指确认有权使用应用程序但当前未使用的密钥。在与当前活动密钥关联的授权许可过期时，备用密钥将自动变为活动密钥。仅当活动密钥可用时才能添加备用密钥。

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。密钥文件的目的是添加能够激活应用程序的授权许可密钥。

购买 Kaspersky Industrial CyberSecurity for Nodes 后，您会在指定的电子邮件地址收到一个密钥文件。

您不需要连接到 Kaspersky 激活服务器，即可使用密钥文件激活应用程序。

如果密钥文件被意外删除，则您可以恢复它。您可能需要密钥文件注册诸如 Kaspersky CompanyAccount 之类的服务。

若要恢复密钥文件，请执行以下操作：

- 联系授权许可销售商。
- 基于您现有的激活码在Kaspersky 网站上获得密钥文件。

关于激活码

*激活码*是由 20 个字母和数字组成的唯一序列。您必须输入激活码才能添加用于激活 Kaspersky Industrial CyberSecurity for Nodes 的密钥。在您购买 Kaspersky Industrial CyberSecurity for Nodes 之后，您指定的电子邮件地址会收到激活码。

要用激活码激活应用程序，需要互联网接入连接到 Kaspersky 的激活服务器。

如果您在安装应用程序后丢失了激活码，可以将其恢复。例如，您可能需要激活码才能注册 Kaspersky CompanyAccount。要恢复您的激活码，请联系您购买授权许可的卡巴斯基实验室合作伙伴。

使用密钥文件激活应用程序

您可以应用密钥文件激活 Kaspersky Industrial CyberSecurity for Nodes。

要通过应用密钥文件激活 Kaspersky Industrial CyberSecurity for Nodes：

1. 在应用程序控制台树中，展开“**授权许可**”节点。
2. 在“**授权许可**”节点的结果窗格中，单击“**添加密钥**”链接。
3. 单击打开的窗口中的“**浏览**”按钮。

4. 选择具有 .key 扩展名的密钥文件。

> 还可以添加密钥作为备用密钥。若要添加密钥作为附加密钥，请选中“**用作附加密钥**”复选框。

5. 单击“**确定**”。

将会应用选定的密钥文件。在这种情况下：

- 如果已经为应用程序添加了活动密钥，并且您添加另一个密钥作为活动密钥，则新密钥会替换之前添加的密钥。之前添加的密钥将被删除。
- 如果已经为应用程序添加了备用密钥，并且您添加另一个密钥作为备用密钥，则新密钥会替换之前添加的密钥。之前添加的备用密钥将被删除。
- 如果已经为应用程序添加了活动密钥和备用密钥，并且您添加新密钥作为活动密钥，则新密钥会替换之前添加的活动密钥；备用密钥不会被删除。

“**授权许可**”节点将提供有关添加的密钥的信息。

使用激活码激活应用程序

> 要使用激活码激活应用程序，受保护设备必须连接到互联网。

您可以使用激活码激活 Kaspersky Industrial CyberSecurity for Nodes。

使用此方法激活应用程序时，Kaspersky Industrial CyberSecurity for Nodes 将数据发送到激活服务器来验证所输入的代码：

- 如果激活码验证成功，应用程序将激活。
- 如果激活码验证失败，将显示相应通知。在这种情况下，您必须联系向您销售 Kaspersky Industrial CyberSecurity for Nodes 授权许可的软件供应商。
- 如果已超过激活码的激活数量，将显示相应通知。应用程序激活过程中断，应用程序会提示您联系技术支持。

您可以通过应用程序控制台使用激活码激活 Kaspersky Industrial CyberSecurity for Nodes，或者通过管理插件或 Web 插件创建“*应用程序激活*”组任务来进行激活。

要通过应用程序控制台使用激活码激活 Kaspersky Industrial CyberSecurity for Nodes：

1. 在应用程序控制台树中，展开“**授权许可**”节点。
2. 在“**授权许可**”节点的结果窗格中，单击“**添加激活码**”链接。
3. 在打开的窗口的“**激活码**”字段中输入激活码。
   - 如果要将激活码用作备用密钥，请选择“**用作附加密钥**”复选框。
   - 要查看有关授权许可的信息，请单击“**显示授权许可信息**”按钮。该信息将显示在“**授权许可信息**”块中。

4. 单击“**确定**”。

Kaspersky Industrial CyberSecurity for Nodes 会将有关应用的激活码的信息发送到激活服务器。

查看有关当前授权许可的信息

查看授权许可状态

有关当前授权许可状态的信息显示在应用程序控制台的 **Kaspersky Industrial CyberSecurity for Nodes** 节点的详细信息窗格中。授权许可状态可以是以下值：

- **检查密钥状态。** – Kaspersky Industrial CyberSecurity for Nodes 正在检查已添加的密钥文件，等待有关当前状态的响应。
- **到期日期。** – Kaspersky Industrial CyberSecurity for Nodes 已激活，且在指定日期之前有效。在以下情况下，状态以黄色突出显示：
  - 授权许可将在 30 天后过期，并且未添加任何备用密钥。
  - 添加的密钥已被添加到拒绝列表且将被阻止。
- **应用程序未激活** – 由于未添加密钥，因此 Kaspersky Industrial CyberSecurity for Nodes 未激活。状态红色高亮显示。
- **授权许可已到期。** – 由于授权许可已过期，Kaspersky Industrial CyberSecurity for Nodes 未激活。状态红色高亮显示。
- **违反了最终用户授权许可协议。** – 由于违反了最终用户授权许可协议的条款，Kaspersky Industrial CyberSecurity for Nodes 未激活。状态红色高亮显示。
- **密钥在拒绝列表中。** – 添加的密钥文件已被卡巴斯基阻止并添加到拒绝列表，例如，密钥被第三方用来非法激活应用程序。状态红色高亮显示。

查看有关当前授权许可的信息

要查看有关当前授权许可的信息，

在应用程序控制台树中，展开“**授权许可**”节点。

有关当前授权许可的常规信息显示在“**授权许可**”节点的详细信息窗格中（请参见下表）。

“授权”节点中有关授权许可的常规信息

字段	描述
激活码状态或密钥状态	激活码状态或密钥状态：*活动密钥*或*备用*。
到期日期	与活动密钥相关联的授权许可的到期日期和时间。
授权许可类型	授权许可类型：*商业版授权许可*。

字段	描述
激活状态	激活状态信息可以采用以下值： • **已应用** – 如果您已使用密钥激活应用程序。 • **应用程序激活** – 如果您已应用激活码激活应用程序，但激活过程尚未最终完成。应用程序激活完成并且节点的详细信息窗格的内容刷新后，状态更改为“**已应用**”。 • **激活错误** – 如果应用程序激活失败。您可在任务日志中查看激活不成功的原因。
密钥	您用来激活应用程序的密钥号码。

要查看有关授权许可的详细信息，

在“**授权许可**”子节点的详细信息窗格中，打开您要查看的授权许可的上下文菜单并选择“**属性**”。

“属性<密钥号码>”窗口中的详细授权许可信息

字段	描述
密钥	您用来激活应用程序的密钥号码。
应用程序	使用添加的密钥激活的应用程序的名称。
授权许可类型	授权许可类型：商用或试用。
授权许可期限	从应用程序激活日期开始，授权许可有效的天数。
激活日期	密钥添加到应用程序的日期。
到期日期	与活动密钥相关联的授权许可的到期日期。如果在无期限订阅下激活应用程序，此字段的值为*无期限*。如果 Kaspersky Industrial CyberSecurity for Nodes 无法确定授权许可过期日期，则字段值设置为*未知*。
到期前的天数	与活动密钥相关联的授权许可在到期前所剩的天数。
符合技术支持条件	有关卡巴斯基或其合作伙伴是否会根据授权许可条款为客户提供技术支持的信息。
支持信息	Kaspersky 或其提供技术支持的合作伙伴的联系人详细信息。如果不提供技术支持，则此字段可为空。
所有者信息	有关授权许可客户的信息：客户名称和获取授权许可的组织的名称。
授权许可信息	当前授权许可的编号和类型。
功能	在授权许可下提供的应用程序功能。

续订授权许可

默认情况下，当授权许可距离到期还有 30 天时，Kaspersky Industrial CyberSecurity for Nodes 会通知您。

您可以在到期日期前使用备用密钥续订授权许可。这可确保在当前授权许可到期后和您使用新的授权许可激活应用程序之前继续保护您的设备。

要续订授权许可：

1. 获取新的激活码或密钥文件。
2. 在应用程序控制台树中，选择“**授权许可**”节点。
3. 在“**授权许可**”节点的结果窗格中执行以下操作之一：
   - 如果您想要使用密钥文件续订授权许可：
     a. 单击“**添加密钥**”链接。
     b. 单击打开的窗口中的“**浏览**”按钮。

c. 选择具有 .key 扩展名的新密钥文件。

d. 选择**用作附加密钥**复选框。

- 如果您想要使用激活码续订授权许可：

  a. 单击“**添加激活码**”链接。

  b. 在打开的窗口中输入购买的激活码。

  c. 选择**用作附加密钥**复选框。

  > 应用激活码需要 Internet 连接。

4. 单击“**确定**”。

当前 Kaspersky Industrial CyberSecurity for Nodes 授权许可到期后，会添加并自动应用备用密钥。

删除密钥

> 如果您删除所添加的密钥，则可以通过重新应用密钥文件来将其还原。

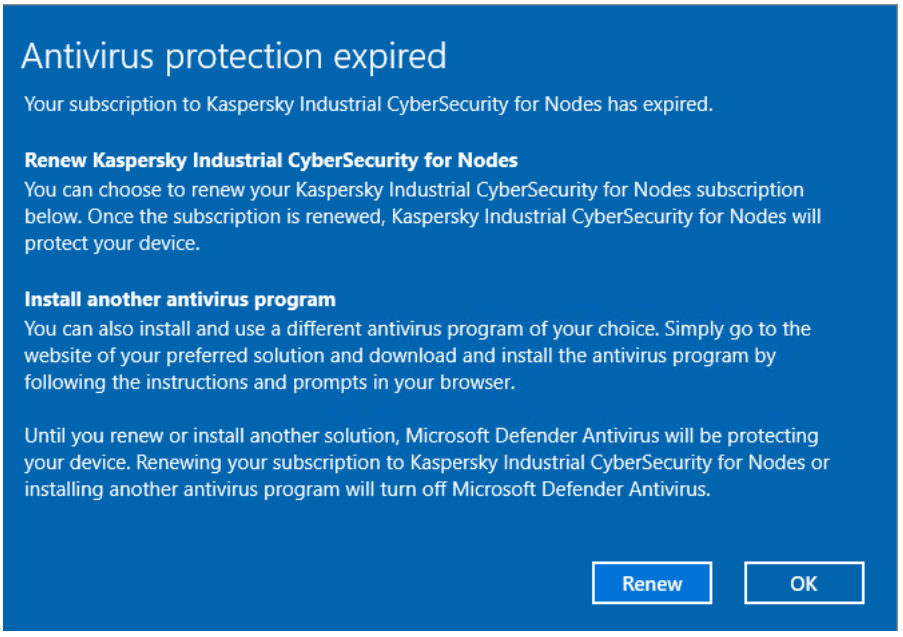
要删除先前添加的密钥：

1. 在应用程序控制台树中，选择“**授权许可**”节点。
2. 在包含有关已添加密钥的信息的表格中的“**授权许可**”节点的结果窗格中，选择您要删除的密钥。
3. 在包含有关所选密钥的信息的行的上下文菜单中，选择“**删除**”。
4. 在确认窗口中单击“**是**”按钮以确认您希望删除该密钥。

选定的密钥将被删除。

密钥被删除后，计算机将不再受到 Kaspersky Industrial CyberSecurity for Nodes 的保护。然后应用程序发送一个保护状态命令到 Windows Security Center （WSC）以启用内置保护工具。在此过程中，应用程序会显示一个建议续费授权许可的窗口（见下图）。如果弹出窗口妨碍了其他应用程序，而您想禁用此窗口，请在注册表中设置 `NeedShowUPAOWindows=0`。此键位于 `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KICS.4.5\environment\` 下。

如果您禁用授权许可续费窗口，Kaspersky Industrial CyberSecurity for Nodes 不会将保护状态命令发送到 Windows 安全中心。这意味着 Windows 安全中心没有启用内置的保护工具。禁用窗口时请记住这个风险。



建议授权许可续费的窗口

关于数据提供

接受最终用户授权许可协议的条款，即表示您同意自动将以下数据发送到 Kaspersky：

- 为支持接收更新的机制 - 有关已安装的应用程序及其授权证书的信息：已安装的应用程序及其完整版本的标识符，包括内部版本号、类型以及授权许可标识符、安装标识符、唯一更新任务标识符。
- 为管理数据处理的确认 - 有关授权许可协议和规定了数据传输条款的其他文档的接受状态的信息：授权许可协议或其他文档（接受或拒绝作为其一部分的数据处理条款）的标识符和版本；表示用户操作（确认或撤消接受条款）的属性；数据处理条款接受的状态更改的日期和时间。
- 为使用激活码激活应用程序 - 有关已安装应用程序的类型、版本和本地化的信息，已安装更新的版本，受保护设备的标识符和受保护设备上应用程序安装的标识符，激活码和当前授权许可的唯一标识符，操作系统的类型、版本和字长，在虚拟环境中安装应用程序时的虚拟环境名称，以及在提供信息时处于活动的应用程序组件的标识符。

卡巴斯基在您使用该应用程序时从您那里收到的数据将受到保护，并按照法律和现行卡巴斯基规则的要求进行处理。数据通过加密的通信通道传输。有关处理、存储和销毁在使用应用程序期间获得并传输给卡巴斯基的信息的更多详细信息，请参阅隐私策略 www.kaspersky.com/Products-and-Services-Privacy-Policy。

本地数据处理

在执行本指南所述的应用程序主要功能时，Kaspersky Industrial CyberSecurity for Nodes 会在受保护设备上本地处理和存储一系列数据。

下表包含有关 Kaspersky Industrial CyberSecurity for Nodes 对报告中包含的数据进行本地处理和存储的信息。

对报告中包含的数据进行处理和存储

功能区域	审计。
使用类型	Kaspersky Industrial CyberSecurity for Nodes 本地存储数据，并将数据发送到管理服务器。管理服务器数据库存储有关在受管理的受保护设备上发生的应用程序事件的信息。
存储	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<产品版本>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • 管理服务器的数据库
安全措施	访问控制列表。
存储期	Kaspersky Industrial CyberSecurity for Nodes 将一直存储数据，直到卸载 Kaspersky Industrial CyberSecurity for Nodes 为止。 卸载 Kaspersky Industrial CyberSecurity for Nodes 期间，Kaspersky Industrial CyberSecurity for Nodes 在受保护设备上存储的所有数据都将被删除。
用途	提供主要功能。

Kaspersky Industrial CyberSecurity for Nodes 不会删除 Windows 事件日志中的事件。

Kaspersky Industrial CyberSecurity for Nodes 在本地处理并存储报告中的以下数据：

- 所处理文件的名称和属性，以及它们在被扫描介质上的完整路径。
- Kaspersky Industrial CyberSecurity for Nodes 对扫描的文件所采取的操作。
- 用户对受保护设备上的被扫描文件执行的操作。
- 有关对受保护网络或受保护设备执行任何操作的用户账户的信息。
- 添加到设备控制规则中的设备的设备实例路径值。
- 有关系统上运行的进程和脚本的信息：可执行文件的校验和（MD5、SHA-256）以及完整路径，有关数字证书的信息。
- Windows 防火墙设置。
- Windows 事件日志条目。
- 对受保护设备上的被扫描文件采取操作的用户账户的名称。
- 正在启动的可执行文件实例，以及这些文件的类型、名称、校验和和属性。
- 有关网络活动的信息：被阻止的外部设备的 IP 地址、执行对受保护共享资源的访问的已泄露登录会话的标识符。
- 有关受保护设备连接到的 Wi-Fi 网络的信息：网络名称和网络标识符。

- 有关添加到保护范围的 PLC 项目的信息，包括 PLC 连接设置（IP、机架和插槽号、密码）和固件校验和。
- 有关 Windows USN 日志状态的信息。

下表包含有关 Kaspersky Industrial CyberSecurity for Nodes 对用户指定的参数的数据进行本地处理和存储的信息。

Kaspersky Industrial CyberSecurity for Nodes 仅处理和存储用户指定的参数数据。

对用户指定的参数的数据进行处理和存储

功能区域	自动修复、沙盒集成。
使用类型	Kaspersky Industrial CyberSecurity for Nodes 本地存储参数数据，并将数据发送到管理服务器。管理服务器数据库存储有关受管理的受保护设备的参数信息。
存储	%ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes\<产品版本>\
安全措施	访问控制列表。
存储期	Kaspersky Industrial CyberSecurity for Nodes 将一直存储数据，直到卸载 Kaspersky Industrial CyberSecurity for Nodes 为止。 卸载 Kaspersky Industrial CyberSecurity for Nodes 期间，Kaspersky Industrial CyberSecurity for Nodes 在受保护设备上存储的所有数据都将被删除。
用途	提供主要功能。

Kaspersky Industrial CyberSecurity for Nodes 不会删除导出到配置文件中的参数的数据。

如果在安装向导中选中“**导出隔离对象**”和“**导出备份对象**”复选框，则 Kaspersky Industrial CyberSecurity for Nodes 不会删除隔离对象和备份对象。

Kaspersky Industrial CyberSecurity for Nodes 对用户指定的以下参数数据进行本地处理和存储：

- 隔离区或备份区中放置的对象信息。
- 有关通过应用程序控制台或管理插件配置的设置的信息，例如：
  - Kaspersky Industrial CyberSecurity for Nodes 密码、运行 Kaspersky Industrial CyberSecurity for Nodes 任务的用户账户名称。
  - 用于代理服务器身份验证的用户账户名称。
  - 用作用户定义更新源的网络文件夹或 HTTP 或 FTP 服务器上的文件夹的地址。
  - 有关 Wi-Fi 网络的信息。
  - 有关添加到保护范围的 PLC 项目的信息，包括 PLC 连接设置和固件校验和。
  - 已阻止的登录会话的 IP 地址和标识符。
  - Windows 防火墙设置。
  - 添加到“应用程序启动控制”任务规则中的可执行文件的校验和（MD5、SHA-256）和路径。
  - 添加到设备控制规则中的设备的设备实例路径值。

- 有关包括在 Kaspersky Industrial CyberSecurity for Nodes 任务范围中的文件夹的信息。
- 有关 Windows 事件日志中的事件的信息。
- 有关使用 iSwift 或 iChecker 技术检测到的文件的信息。
- 添加到信任区域的文件的校验和（MD5、SHA-256）和路径。
- 有关已添加的授权许可密钥的信息。
- 有关数字证书的信息。
- 文件的校验和、数字证书数据、文件的完整路径（SDC 数据库、基线文件完整性监控任务的文件）。
- 应用程序扫描存档时创建的临时文件。
- %SystemRoot% 中的信息。

- 有关 Kaspersky Industrial CyberSecurity for Nodes 处理的文件的数据，例如文件的校验和（MD5、SHA-256）、有关数字证书的信息、文件的完整路径。

作为应用程序基本功能的一部分，Kaspersky Industrial CyberSecurity for Nodes 处理并存储数据，包括记录应用程序事件和接收诊断数据。本地处理的数据按照配置和应用的应用程序设置进行处理和保护。

Kaspersky Industrial CyberSecurity for Nodes 允许您配置本地处理数据的保护级别：您可以更改用户访问进程数据的权限、更改此类数据的数据保留期限、完全或部分禁用涉及数据记录的功能，以及更改记录数据的驱动器上的文件夹的路径和属性。

有关配置涉及数据处理的应用程序功能的详细信息，请参阅本指南的相应部分。

通过应用程序辅助组件处理本地数据

Kaspersky Industrial CyberSecurity for Nodes 安装包包含应用程序辅助组件，这些辅助组件可以安装在设备上，即使该设备未安装 Kaspersky Industrial CyberSecurity for Nodes。

当执行本指南所述的主要应用程序功能时，应用程序辅助组件本地处理一组数据并将数据存储在安装了这些组件的受保护设备上，即使它们与 Kaspersky Industrial CyberSecurity for Nodes 分开安装也是如此。

下表包含有关 Kaspersky Industrial CyberSecurity for Nodes 对写入 dump 和跟踪文件的数据进行本地处理和存储的信息。

默认情况下， Kaspersky Industrial CyberSecurity for Nodes 不会写入转储和跟踪文件。

处理和存储转储和跟踪文件中写入的数据

存储	默认情况下，未指定保存转储和跟踪文件的文件夹。 您可以指定文件夹
安全措施	Kaspersky Industrial CyberSecurity for Nodes 不限制对转储和跟踪文件的访问。
存储期	Kaspersky Industrial CyberSecurity for Nodes 不会删除转储和跟踪文件。
用途	提供技术支持。

Kaspersky Industrial CyberSecurity for Nodes 本地处理并存储以下写入 dump 和跟踪文件的数据：

- 有关 Kaspersky Industrial CyberSecurity for Nodes 对受保护设备执行的操作的信息。
- 有关 Kaspersky Industrial CyberSecurity for Nodes 处理的对象的信息。
- 有关 Kaspersky Industrial CyberSecurity for Nodes 运行期间发生的错误的信息。

辅助组件处理的数据不会自动发送到 Kaspersky 或其他第三方系统。

默认情况下，在卸载这些应用程序辅助组件后，这些组件在运行期间本地处理的数据都将被删除。

辅助应用程序组件的跟踪文件除外。我们建议您手动删除这些文件。

有关处理包含应用程序辅助组件诊断数据的文件的详细信息，请参阅本指南的相应章节。

与欧盟立法兼容(GDPR)

Kaspersky Industrial CyberSecurity for Nodes 可能在以下情景下传输数据到 Kaspersky：

- 使用卡巴斯基安全网络。
- 用激活码激活应用程序。
- 更新应用程序模块和反病毒数据库。
- 遵从应用程序控制台的链接。

无论数据分类和接收数据的地区如何，Kaspersky 都坚持高标准的数据安全，并采用各种法律、组织和技术措施来保护用户的数据，保证数据的安全性和保密性，并确保用户权利的实现适用法律。隐私策略的文本包含在应用程序分发工具并在 Kaspersky 网站 上可用。

在使用 Kaspersky Industrial CyberSecurity for Nodes 之前，请仔细阅读最终用户授权许可协议和卡巴斯基安全网络声明中关于数据传输的说明。如果根据当地法律或标准，Kaspersky Industrial CyberSecurity for Nodes 在上述任何情景下传输的特定数据被归类为个人数据，则您必须确保这些数据是合法处理的，并在收集和传输此类数据时获得最终用户的同意。

请阅读最终用户授权许可协议并访问 Kaspersky 网站 了解当您接受《最终用户授权许可协议》和同意《卡巴斯基安全网络声明》之后我们如何接收、保存和销毁有关程序使用的信息。license.txt 和 ksn_<语言 ID>.txt 文件包含最终用户授权许可协议的文本，卡巴斯基安全网络声明包含在应用程序分发包中。

如果您不想传输数据到 Kaspersky，您可以禁用数据提供。

使用卡巴斯基安全网络

通过使用卡巴斯基安全网络，您同意自动提供卡巴斯基安全网络声明中列出的数据。如果您不同意将此数据提供给卡巴斯基，请使用私有卡巴斯基私有安全网络（KPSN）或禁用 KSN 的使用。

使用激活码激活应用程序

通过使用激活码，您同意在最终用户授权许可协议下自动提供数据。如果您不同意提供这些数据给卡巴斯基，请使用密钥文件来激活 Kaspersky Industrial CyberSecurity for Nodes。

更新应用程序模块和反病毒数据库

通过使用卡巴斯基服务器，您同意在最终用户授权许可协议下自动提供数据。卡巴斯基需要这些信息来验证 Kaspersky Industrial CyberSecurity for Nodes 是否被合法使用。如果您不同意将此信息提供给卡巴斯基，请使用 Kaspersky Security Center 进行数据库更新。

遵从应用程序控制台的链接。

通过使用应用程序控制台中的链接，您同意在最终用户授权许可协议下自动提供数据。每个特定链接中传输的数据的精确列表取决于链接在应用程序控制台中的位置以及它要解决的问题。如果您不同意向卡巴斯基提供该信息，则禁止显示应用程序界面。

启动和停止 Kaspersky Industrial CyberSecurity for Nodes

本节包含有关启动和停止 Kaspersky Industrial CyberSecurity for Nodes 的信息，以及有关启动 Kaspersky Industrial CyberSecurity for Nodes 控制台和 Kaspersky Security Center 管理控制台的管理插件的信息。

启动和停止应用程序

将 Kaspersky Industrial CyberSecurity for Nodes 安装到用户的计算机后，该应用程序会自动启动。默认情况下，Kaspersky Industrial CyberSecurity for Nodes 在操作系统启动后启动。在操作系统设置中无法配置应用程序的自动启动。

在操作系统启动后下载 Kaspersky Industrial CyberSecurity for Nodes 反病毒数据库最多可能需要两分钟，具体取决于计算机的功能。在该期间计算机保护级别降低。在已启动的操作系统上启动 Kaspersky Industrial CyberSecurity for Nodes 时，下载反病毒数据库不会导致计算机保护等级降低。

如何在 Kaspersky Security Center 管理控制台中配置应用程序自动启动

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**应用程序设置 → 安全性和可靠性**”并点击“**设置**”。
4. 在“**安全**”选项卡上，选中或清空“**在计算机开启时启动应用程序(建议)**”复选框以启用或禁用应用程序自动运行。
5. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置应用程序自动启动

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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 **应用程序设置 → 安全性和可靠性**。
5. 单击“**配置**”。
   “**安全性和可靠性**”窗口将打开。

6. 使用“**在计算机开启时启动应用程序(建议)**”复选框启用或禁用应用程序自动启动。
7. 保存更改。

如何在应用程序控制台中配置应用程序自动启动

1. 在应用程序控制台树中选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点。
2. 在节点的上下文菜单中选择“**应用程序属性**”。
3. 这将打开一个窗口；在该窗口中，选择“**安全设置**”选项卡。
4. 使用“**在计算机开启时启动应用程序(建议)**”复选框启用或禁用应用程序自动启动。
5. 保存更改。

如果您是受保护设备上“管理员”组的成员，您可以启动和停止 Kaspersky Industrial CyberSecurity for Nodes。

如何在 Kaspersky Security Center 管理控制台中启动或停止应用程序

1. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
2. 在工作区中选择“**设备**”选项卡。
3. 双击以打开计算机属性窗口。
4. 在计算机属性窗口中，选择“**应用程序**”区域。
5. 在计算机上安装的卡巴斯基应用程序列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes (4.5.0)**”。
6. 执行下列操作之一：
   - 要启动应用程序，请单击 Kaspersky 应用程序列表右侧的 按钮。
   - 要停止应用程序，请单击 Kaspersky 应用程序列表右侧的 按钮。

如何在 Kaspersky Security Center Web Console 中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**”。
2. 单击您要在其上启动或停止 Kaspersky Industrial CyberSecurity for Nodes 的计算机的名称。
   计算机属性窗口将打开。
3. 选择**应用程序**选项卡。

4. 选中“**Kaspersky Industrial CyberSecurity for Nodes (4.5.0)**”对面的复选框。

5. 单击“**开始**”或“**停止**”按钮。

如何在应用程序控制台中启动或停止应用程序

1. 在“**Kaspersky Industrial CyberSecurity for Nodes**”节点工作区的应用程序控制台树中，点击“**连接到远程计算机**”。

2. 在应用程序重启消息中，单击“**是**”。

3. 在“**选择受保护设备**”窗口中，在“**管理服务**”旁边，执行下列操作之一：

   - 如果您想要停止应用程序，请单击“**停止**”按钮。
   - 如果您想要启动应用程序，请单击“**启动**”按钮。

   应用程序将被停止或启动。

如果与安装该应用程序的计算机的连接丢失或 KICS 服务失败，也会显示“**选择受保护设备**”窗口。您可以通过点击“**启动**”按钮恢复 KICS 服务。

如何从命令行启动或停止应用程序

1. 以管理员身份运行命令行解释器 (cmd.exe)。

2. 使用 `cd` 命令，导航到 klpsm.exe 和 kavshell.exe 文件所在的文件夹。

   例如：`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0`。

3. 要从命令行启动应用程序，请执行以下命令之一：

   - `klpsm.exe start_avp_service`
   - `KAVSHELL start [/login:<当前用户账户的名称>] [/PWD:</login 密码或 KLAdmin 密码（如果未指定 /login）>]`

4. 要从命令行停止应用程序，请执行以下命令之一：

   - `klpsm.exe stop_avp_service`
   - `KAVSHELL stop [/login:<当前用户账户的名称>] [/PWD:</login 密码或 KLAdmin 密码（如果未指定 /login）>]`

暂停和恢复计算机保护和控制

暂停计算机保护和控制意味着禁用 Kaspersky Industrial CyberSecurity for Nodes 的所有保护和控制组件一段时间。

应用程序状态使用任务栏通知区域中应用程序图标进行显示。

- 图标表示计算机保护和控制已暂停。
- 图标表示计算机保护和控制已启用。

暂停或恢复计算机保护和控制不影响扫描或更新任务。

如果在暂停或恢复计算机保护和控制时已建立任何网络连接，系统会显示有关终止这些网络连接的通知。

暂停计算机保护和控制：

1. 在应用程序控制台树中，打开 **Kaspersky Industrial CyberSecurity for Nodes** 节点的上下文菜单。
2. 选择“**暂停保护**”。
3. 选择以下选项之一：
   - **指定暂停时长 <时间段>** – 经过下面的下拉列表中所指定的时间后将恢复计算机保护和控制。
   - **暂停至重启为止** – 重启应用程序或重启操作系统后将恢复计算机保护和控制。必须启用应用程序的自动启动才能使用该选项。
   - **暂停** – 在您决定重新启用时将恢复计算机保护和控制。

Kaspersky Industrial CyberSecurity for Nodes 将暂停策略中不带锁标记 () 的所有保护和控制组件的运行。

恢复计算机保护和控制：

1. 打开位于任务栏通知区域的应用程序图标的上下文菜单。
2. 在上下文菜单中，选择“**恢复保护**”。

如果您决定恢复计算机保护和控制，可以随时进行该操作，这与您之前选择的保护和控制暂停选项无关。

小型诊断窗口

本节介绍小型诊断窗口的使用。

关于小型诊断窗口

“小型诊断窗口”组件（也称为“CDI”）连同“系统托盘图标”组件独立于应用程序控制台安装和卸载，可在受保护设备上未安装应用程序控制台时使用。小型诊断窗口通过系统托盘图标启动，或通过运行受保护设备上的应用程序文件夹中的 avpui.exe 启动。

在小型诊断窗口中，可以执行以下操作：

- 打开含有已安装更新和可用补丁列表的“**关于**”窗口。
- 查看有关常规应用程序状态的信息。
- 查看已发生的安全事件。
- 查看受保护设备上的当前活动。
- 启动或停止写入 dump 和跟踪文件。
- 创建便携式扫描程序。
- 打开应用程序控制台。

即使对 Kaspersky Industrial CyberSecurity for Nodes 功能的访问受密码保护，小型诊断窗口仍然可用。无需任何密码。

小型诊断窗口组件不能通过 Kaspersky Security Center 进行配置。

通过小型诊断窗口查看 Kaspersky Industrial CyberSecurity for Nodes 状态

要通过小型诊断窗口查看应用程序状态：

1. 采用以下方式之一打开小型诊断窗口：
   - 运行受保护设备上的应用程序安装文件夹中的 avpui.exe 文件。默认情况下，该文件位于 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0。
   - 单击任务栏通知区域中的应用程序图标。
2. 在“**保护状态**”部分中查看密钥、实时计算机保护任务和更新任务的当前状态。使用不同的颜色来向用户通知保护状态（参见下表）。

小型诊断窗口中的颜色指示

部分	状态

实时保护状态	在以下任一情况（满足任意条件）下，面板呈*绿色*：
	• 推荐配置：
	  • “实时文件保护”任务以默认设置启动。
	  • “应用程序启动控制”任务在“**阻止**”模式下以默认设置启动。
	• 可接受配置：
	  • “实时文件保护”任务由用户配置。
	  • “应用程序启动控制”任务设置被修改。

	如果满足以下一个或多个条件，面板呈*黄色*： • “实时文件保护”任务暂停（用户暂停或按计划暂停）。 • “应用程序启动控制”任务在“**通知**”模式下启动。 • “漏洞利用防御”和“应用程序启动控制”任务在“**通知**”模式下启动。
	如果同时满足以下两个条件，面板呈*红色*： • “实时文件保护”组件未安装或者任务停止或暂停。 • “应用程序启动控制”组件未安装或任务在“**通知**”模式下启动。
授权许可	如果当前授权许可有效，面板呈*绿色*。
	*黄色*面板表示发生以下事件之一： • *检查授权许可状态。* • *授权许可将在 30 天后过期，且未添加附加密钥或激活码。* • *添加的密钥已被添加到拒绝列表且将被阻止。*
	*红色*面板表示发生以下事件之一： • *应用程序未激活* • *授权许可已到期。* • *违反了最终用户授权许可协议。* • *密钥在拒绝列表中。*
更新	应用程序数据库为最新时，面板呈*绿色*。
	应用程序数据库已过期时，面板呈*黄色*。
	应用程序数据库已严重过期时，面板呈*红色*。

查看安全事件统计

“**统计信息**”部分显示所有安全事件。单独块中显示的每个保护任务统计说明了事件数量和上次发生事件的日期和时间。记录某个事件后，块颜色变为红色。

要查看统计信息：

1. 采用以下方式之一打开小型诊断窗口：
   - 运行受保护设备上的应用程序安装文件夹中的 avpui.exe 文件。默认情况下，该文件位于 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0。
   - 单击任务栏通知区域中的应用程序图标。
2. 转到**统计信息**区域。
3. 查看保护任务的安全事件。

查看当前应用程序活动

要查看受保护设备上的当前应用程序活动：

1. 采用以下方式之一打开小型诊断窗口：
   - 运行受保护设备上的应用程序安装文件夹中的 avpui.exe 文件。默认情况下，该文件位于 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0。
   - 单击任务栏通知区域中的应用程序图标。
2. 转到**当前应用程序活动**区域。

使用不同的颜色指示应用程序活动状态：

- 在“**任务**”部分中：
  - *绿色*。没有达到显示黄色或红色的条件。
  - *黄色*。很长时间未扫描关键区域。
  - *红色*。符合以下至少一个条件：
    - 未启动任何任务和没有为任何任务设置启动计划。
    - 应用程序启动错误将记录为严重事件。
- 在“**卡巴斯基安全网络**”部分中：
  - *绿色*。“**KSN 使用**”任务已启动。
  - *黄色*。KSN 声明被接受，但任务未启动。

配置应用程序跟踪和内存转储记录

要配置应用程序跟踪和内存转储记录：

1. 采用以下方式之一打开小型诊断窗口：
   - 运行受保护设备上的应用程序安装文件夹中的 avpui.exe 文件。默认情况下，该文件位于 C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0。
   - 单击任务栏通知区域中的应用程序图标。
2. 转到**故障诊断**区域。
3. 使用“**将调试信息写入跟踪文件**”复选框启用或禁用应用程序操作跟踪。

4. 如果必要，单击“**浏览**”按钮以指定 Kaspersky Industrial CyberSecurity for Nodes 将会保存跟踪文件的文件夹。

   该文件夹必须提前创建并且可由 SYSTEM 账户写入。您不能指定网络文件夹、驱动器或环境变量。

5. 在“**详细级别**”下拉列表中，选择调试信息的详细级别。

   - **关键**，意味着跟踪文件仅保存有关致命错误的消息。
   - **诊断**，意味着跟踪文件保存有关所有错误和警告的消息。
   - **重要**，意味着跟踪文件保存有关所有错误、警告和附加信息的消息。
   - **正常**，意味着跟踪文件保存有关所有错误、警告的消息，以及有关应用程序正常运行的信息（默认）。
   - **详细**，意味着跟踪文件保存有关应用程序运行的所有信息。

   技术支持代表确定解决任何潜在问题所需的详细级别。
   默认的详细级别设置为“**正常**”。

6. 指定**跟踪文件最大大小(MB)**。
   可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小为 100 MB。

7. 要在达到最大文件数时删除旧的跟踪文件，请选中“**删除最旧的跟踪文件**”复选框。

8. 指定**跟踪文件最大数量**。
   可用值：1 到 999。默认情况下，最大文件数为 5。如果选中“**删除最旧的跟踪文件**”复选框，则该字段可用。

9. 如果有必要，配置内存转储：

   a. 选择或清除“**在此文件夹中创建故障转储文件**”复选框用于在发生故障时启用或禁用内存转储。

   b. 如果必要，单击“**浏览**”按钮以指定 Kaspersky Industrial CyberSecurity for Nodes 将会保存内存转储文件的文件夹。默认情况下，内存转储文件存储在以下文件夹中：%ProgramData%\Kaspersky Lab\KICS.4.5\Trace。

      该文件夹必须提前创建并且可由 SYSTEM 账户写入。您不能指定网络文件夹、驱动器或环境变量。

10. 单击“**应用**”。

Kaspersky Industrial CyberSecurity for Nodes 自我保护

自我保护可阻止其他应用程序执行可能干扰 Kaspersky Industrial CyberSecurity for Nodes 运行的操作。应用程序具有自我保护机制，可防止该应用程序的文件夹、内存进程和系统注册表项被修改或删除。Kaspersky Industrial CyberSecurity for Nodes 支持由微软开发的“Antimalware Protected Process Light (AM-PPL)”技术，可保护应用程序进程免受恶意活动的侵害。此外，应用程序还允许分别管理用户对应用程序功能和应用程序服务的访问权限。

启用和禁用自我防御

Kaspersky Industrial CyberSecurity for Nodes 可防止修改或删除硬盘驱动器中的应用程序文件、内存进程和系统注册表中的条目。

该技术阻止对以下应用程序组件的访问：

- 位于 Kaspersky Industrial CyberSecurity for Nodes 安装文件夹中的文件和应用程序的其他文件；
- 属于应用程序的注册表键；
- 应用程序运行的进程。

默认情况下已启用 Kaspersky Industrial CyberSecurity for Nodes 的自我保护机制。

如何在 Kaspersky Security Center 管理控制台中启用或禁用自我保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，转到“**应用程序设置**”区域。
4. 在“**安全性和可靠性**”块中单击“**设置**”按钮。
5. 这将打开一个窗口；在该窗口中，选择“**安全**”选项卡。
6. 在“**自我保护**”块，使用“**保护应用程序进程免受外部威胁**”复选框启用或禁用自我保护。
7. 关闭挂锁以将策略应用于计算机。
8. 点击“**确定**”保存更改。

如何在应用程序控制台中启用或禁用自我保护

1. 在应用程序控制台树中，选择 **Kaspersky Industrial CyberSecurity for Nodes** 节点，并在结果窗格中，单击“**应用程序属性**”链接。
2. 这将打开一个窗口；在该窗口中，选择“**安全设置**”选项卡。
3. 在“**自我保护**”块，使用“**保护应用程序进程免受外部威胁**”复选框启用或禁用自我保护。
4. 点击“**确定**”保存更改。

如何在 Kaspersky Security Center Web Console 中启用或禁用自我保护

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**应用程序设置**”部分。
5. 在“**安全性和可靠性**”块中单击“**配置**”按钮。
   “**安全性和可靠性**”窗口将打开。
6. 在“**自我保护**”块，使用“**保护应用程序进程免受外部威胁**”复选框启用或禁用自我保护。
7. 关闭挂锁以将策略应用于计算机。
8. 点击“**确定**”保存更改。

对 AM-PPL 技术的支持

Kaspersky Industrial CyberSecurity for Nodes 支持 Microsoft 的 Antimalware Protected Process Light 技术（以下简称“AM-PPL”）。AM-PPL 保护 Kaspersky Industrial CyberSecurity for Nodes 进程免受恶意操作（例如，终止应用程序）。AM-PPL 仅允许运行受信任的进程。Kaspersky Industrial CyberSecurity for Nodes 进程根据 Windows 安全要求进行签名，因此它们是受信任的。有关 AM-PPL 技术的详细信息，请访问 Microsoft 网站。默认情况下启用 AM-PPL 技术。

Kaspersky Industrial CyberSecurity for Nodes 还具有用于保护应用程序进程的内置机制。AM-PPL 支持允许您将进程安全功能委派给操作系统。从而可以提高应用程序的速度并减少计算机资源的消耗。

应用程序注册了 Kaspersky Industrial CyberSecurity for Nodes (AVP) 服务和 Kaspersky Seamless Update Service (AVPSUS) 服务。AM-PPL 技术只保护 AVP 服务。

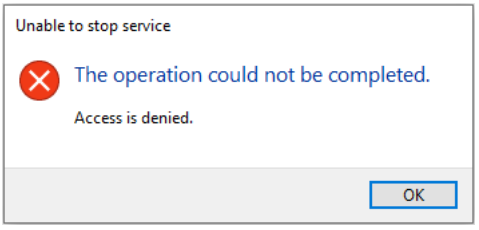
保持 AM-PPL 技术始终活动。AM-PPL 是操作系统防护的重要组件。仅允许在单独的测试环境中禁用 AM-PPL 以排除应用程序故障。

AM-PPL 技术适用于 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 操作系统。

要启用或禁用 AM-PPL 技术：

1. 关闭应用程序的自我保护机制。
   自我保护机制会阻止修改和删除计算机内存中的应用程序进程，包括更改 AM-PPL 状态。
2. 以管理员身份运行命令行解释器 (cmd)。
3. 转到 Kaspersky Industrial CyberSecurity for Nodes 可执行文件所在文件夹。
4. 在命令行中输入以下命令：
   - `klpsm.exe enable` – 启用对 AM-PPL 技术的支持。
   - `klpsm.exe disable` – 禁用对 AM-PPL 技术的支持。
5. 重新启动 Kaspersky Industrial CyberSecurity for Nodes。
6. 恢复应用程序的自我保护机制。

因此，当用户尝试停止 AVP 服务时，会出现一个带有错误消息的系统窗口。用户只能从 Kaspersky Industrial CyberSecurity for Nodes 界面管理应用程序服务。



应用程序服务访问错误

保护操作系统服务

您可以使用“*保护操作系统服务*”允许或禁止第三方应用程序对操作系统服务采取行动的功能。

如何在 Kaspersky Security Center 管理控制台中启用或禁用操作系统服务保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略属性窗口中，转到“**应用程序设置**”区域。
4. 在“**安全性和可靠性**”块中单击“**设置**”按钮。
5. 这将打开一个窗口；在该窗口中，选择“**安全**”选项卡。
6. 使用“**保护操作系统服务**”复选框启用或禁用操作系统服务保护。
   如果启用了操作系统服务保护，第三方应用程序就无法对操作系统的进程采取行动。
   如果禁用了操作系统服务保护，第三方应用程序就可以对操作系统的进程采取行动。
   启用或禁用该功能后，您必须重新启动计算机才能应用更改。
7. 关闭挂锁以将策略应用于计算机。
8. 点击“**确定**”保存更改。

如何在应用程序控制台中启用或禁用操作系统服务保护

1. 在应用程序控制台树中，选择 **Kaspersky Industrial CyberSecurity for Nodes** 节点，并在结果窗格中，单击“**应用程序属性**”链接。
2. 这将打开一个窗口；在该窗口中，选择“**安全设置**”选项卡。
3. 使用“**保护操作系统服务**”复选框启用或禁用操作系统服务保护。
   如果启用了操作系统服务保护，第三方应用程序就无法对操作系统的进程采取行动。
   如果禁用了操作系统服务保护，第三方应用程序就可以对操作系统的进程采取行动。
   启用或禁用该功能后，您必须重新启动计算机才能应用更改。
4. 点击“**确定**”保存更改。

如何在 Kaspersky Security Center Web Console 中启用或禁用操作系统服务保护

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**应用程序设置**”部分。
5. 在“**安全性和可靠性**”块中单击“**配置**”按钮。
   “**安全性和可靠性**”窗口将打开。
6. 使用“**保护操作系统服务**”复选框启用或禁用操作系统服务保护。
   如果启用了操作系统服务保护，第三方应用程序就无法对操作系统的进程采取行动。
   如果禁用了操作系统服务保护，第三方应用程序就可以对操作系统的进程采取行动。
   启用或禁用该功能后，您必须重新启动计算机才能应用更改。

7. 关闭挂锁以将策略应用于计算机。

8. 点击“**确定**”保存更改。

配置用户权限以管理 Kaspersky Industrial CyberSecurity for Nodes

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 的所有功能可供受保护设备上的管理员组成员、安装 Kaspersky Industrial CyberSecurity for Nodes 时在受保护设备中创建的 KICS 管理员组成员以及 SYSTEM 组访问。

未在 Kaspersky Industrial CyberSecurity for Nodes 用户列表中注册的用户无法打开应用程序控制台。

您可以允许或阻止个人用户或用户组访问 Kaspersky Industrial CyberSecurity for Nodes 的特定功能。

关于 Kaspersky Industrial CyberSecurity for Nodes 功能的访问权限

用户权限	描述
管理任务	可启动/停止/暂停/恢复 Kaspersky Industrial CyberSecurity for Nodes 任务。
创建和删除任务	可创建和删除按需扫描任务。
编辑设置	可执行以下操作： • 从配置文件导入 Kaspersky Industrial CyberSecurity for Nodes 设置。 • 编辑应用程序设置。
读取设置	可执行以下操作： • 查看 Kaspersky Industrial CyberSecurity for Nodes 常规设置和任务设置。 • 将 Kaspersky Industrial CyberSecurity for Nodes 设置导出到配置文件。 • 查看任务日志、系统审核日志和通知的设置。
管理存储	可执行以下操作： • 将对象移到隔离。 • 从隔离和备份中删除对象。 • 从隔离和备份中恢复对象。
管理日志	可删除任务日志和清除系统审核日志。
读入日志	可查看任务日志和系统审核日志中的反病毒事件。
获取统计信息	可查看每个 Kaspersky Industrial CyberSecurity for Nodes 任务的统计。
管理应用程序授权许可	能激活 Kaspersky Industrial CyberSecurity for Nodes。
卸载应用程序	可卸载 Kaspersky Industrial CyberSecurity for Nodes。
读取权限	可查看 Kaspersky Industrial CyberSecurity for Nodes 用户和用户访问权限的列表。
编辑权限	可执行以下操作： • 编辑具有应用程序管理访问权限的用户列表。 • 编辑 Kaspersky Industrial CyberSecurity for Nodes 功能的用户访问权限。
与应用程序的远程连接	能够使用应用程序控制台远程连接到应用程序。 对于远程访问，用户还必须具有“**读取设置**”功能的访问权限。
退出应用程序	能够使用应用程序控制台退出应用程序。
禁用 Kaspersky Security Center 策略	能够禁用 Kaspersky Security Center 策略。
导出设置	Kaspersky Industrial CyberSecurity for Nodes 设置的功能。

如何在 Kaspersky Security Center 管理控制台中配置用户权限以管理 Kaspersky Industrial CyberSecurity for Nodes

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**补充**”。
4. 在“**应用程序管理的用户访问权限**”区域中单击“**设置**”。
5. 这会打开一个窗口；在该窗口中，选择“**允许使用手动创建的用户的凭证确认应用程序的操作**”复选框并为 KLAdmin 用户账户设置密码。该用户账户会自动添加到用户账户列表中。
6. 如有必要，添加您想要授予应用程序管理访问权限的用户账户。为此，请在用户账户表中单击“**添加**”。
   这将打开配置用户访问权限的表单。
7. 选择要使用的添加用户的方法：
   - “**从 Active Directory 中选择用户/组**”。您可以向 Active Directory 域中的单个用户或组授予 Kaspersky Industrial CyberSecurity for Nodes 访问权限。例如，如果 Everyone 组被阻止退出应用程序，您可以将“**退出应用程序**”权限授予给单个用户。
   - “**手动添加用户/用户组**”。您可以创建 Active Directory 中不存在的用户账户，并为该用户账户分配单独权限。也就是说，您可以创建一个*服务用户账户*并使用它来代替 KLAdmin。这样，您就不需要与其他用户共享您的 KLAdmin 密码或创建新的 Active Directory 用户账户。您可以指定任何用户名和密码。例如，您可以将“**读入日志**”权限授予服务用户账户。因此，如果“全部”组禁止查看报告，您可以使用服务用户账户或 KLAdmin 用户账户打开报告。

     要手动添加用户或用户组，您必须启用密码保护。
8. 选择要授予其管理应用程序的权限的用户或用户组。
9. 在“**权限**”列表，配置用户对应用程序功能的访问权限。
10. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用控制台台中配置用户权限以管理 Kaspersky Industrial CyberSecurity for Nodes

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**应用程序管理的用户访问权限**”。
2. 这会打开一个窗口；在该窗口中，选择“**允许使用手动创建的用户的凭证确认应用程序的操作**”复选框并为 KLAdmin 用户账户设置密码。该用户账户会自动添加到用户账户列表中。
3. 如有必要，添加您想要授予应用程序管理访问权限的用户账户。为此，请在用户账户表中单击“**添加**”。
   这将打开配置用户访问权限的表单。

4. 选择要使用的添加用户的方法：

   - "**从 Active Directory 中选择用户/组**"。您可以向 Active Directory 域中的单个用户或组授予 Kaspersky Industrial CyberSecurity for Nodes 访问权限。例如，如果 Everyone 组被阻止退出应用程序，您可以将"**退出应用程序**"权限授予给单个用户。

   - "**手动添加用户/用户组**"。您可以创建 Active Directory 中不存在的用户账户，并为该用户账户分配单独权限。也就是说，您可以创建一个*服务用户账户*并使用它来代替 KLAdmin。这样，您就不需要与其他用户共享您的 KLAdmin 密码或创建新的 Active Directory 用户账户。您可以指定任何用户名和密码。例如，您可以将"**读入日志**"权限授予服务用户账户。因此，如果"全部"组禁止查看报告，您可以使用服务用户账户或 KLAdmin 用户账户打开报告。

     要手动添加用户或用户组，您必须启用密码保护。

5. 选择要授予其管理应用程序的权限的用户或用户组。

6. 在"**权限**"列表，配置用户对应用程序功能的访问权限。

7. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置用户权限以管理 Kaspersky Industrial CyberSecurity for Nodes

1. 在 Web Console 的主窗口中，选择"**资产(设备)**" → "**策略和配置文件**"。

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到"**补充 → 应用程序管理的用户访问权限**"并点击"**配置**"按钮。

5. 这会打开一个窗口；在该窗口中，选择"**允许使用手动创建的用户的凭证确认应用程序的操作**"复选框并为 KLAdmin 用户账户设置密码。该用户账户会自动添加到用户账户列表中。

6. 如有必要，添加您想要授予应用程序管理访问权限的用户账户。为此，请在用户账户表中单击"**添加**"。

   这将打开配置用户访问权限的表单。

7. 选择要使用的添加用户的方法：

   - "**从 Active Directory 中选择用户/组**"。您可以向 Active Directory 域中的单个用户或组授予 Kaspersky Industrial CyberSecurity for Nodes 访问权限。例如，如果 Everyone 组被阻止退出应用程序，您可以将"**退出应用程序**"权限授予给单个用户。

   - "**手动添加用户/用户组**"。您可以创建 Active Directory 中不存在的用户账户，并为该用户账户分配单独权限。也就是说，您可以创建一个*服务用户账户*并使用它来代替 KLAdmin。这样，您就不需要与其他用户共享您的 KLAdmin 密码或创建新的 Active Directory 用户账户。您可以指定任何用户名和密码。例如，您可以将"**读入日志**"权限授予服务用户账户。因此，如果"全部"组禁止查看报告，您可以使用服务用户账户或 KLAdmin 用户账户打开报告。

     要手动添加用户或用户组，您必须启用密码保护。

8. 选择要授予其管理应用程序的权限的用户或用户组。

9. 在"**权限**"列表，配置用户对应用程序功能的访问权限。

10. 保存更改。要在计算机上应用该策略，请关闭锁。

配置管理 Kaspersky Security 服务的用户权限

在安装过程中，Kaspersky Industrial CyberSecurity for Nodes 会在 Windows 中注册应用程序服务 - *Kaspersky Security 服务*。因此，应用程序包括在操作系统启动时启动的功能组件。为了降低第三方使用应用程序服务访问受保护设备的应用程序功能和安全设置的风险，您可以限制管理 Kaspersky Security 服务的权限。

默认情况下，用于管理 Kaspersky Security 服务的访问权限被授予受保护设备上管理员组中的用户。读取权限被授予 SERVICE 和 INTERACTIVE 组，读取和执行权限被授予 SYSTEM 组。

您无法删除 SYSTEM 用户账户或编辑此账户的权限。如果编辑 SYSTEM 账户的权限，则当保存更改时会恢复此账户的最大权限。

有权访问编辑权限级别功能的用户可以向在受保护设备上注册的其他用户或者该域中包含的其他用户授予对管理 Kaspersky Security 服务的权限。

您可以为 Kaspersky Industrial CyberSecurity for Nodes 用户或用户组选择以下预设的访问权限级别之一以管理 Kaspersky Security 服务：

- **完整控制**：可查看和编辑 Kaspersky Security 服务的常规设置和用户权限，以及启动和停止 Kaspersky Security 服务。
- **读取**：可查看 Kaspersky Security 服务常规设置和用户权限。
- **编辑**：可查看和编辑 Kaspersky Security 服务常规设置和用户权限。
- **执行**：可启动和停止 Kaspersky Security 服务。

您还可以配置高级访问权限：允许或拒绝访问指定的 Kaspersky Industrial CyberSecurity for Nodes 功能（请参见下表）。

Kaspersky Security 服务功能的访问权限

功能	描述
读取服务设置	可查看 Kaspersky Security 服务常规设置和用户权限。
从服务控制管理器请求服务状态	可从 Microsoft Windows 服务控制管理器请求 Kaspersky Security 服务的执行状态。
请求服务状态	可从 Kaspersky Security 服务请求服务执行状态。
读取依赖服务列表	可查看 Kaspersky Security 服务依存的以及依存于 Kaspersky Security 服务的服务列表。
修改服务设置	可查看和编辑 Kaspersky Security 服务常规设置和用户权限。
启动服务	可启动 Kaspersky Security 服务。
停止服务	可停止 Kaspersky Security 服务。
暂停/恢复服务	可暂停和恢复 Kaspersky Security 服务。
读取权限	可查看 Kaspersky Security 服务用户列表和每个用户的访问权限。
编辑权限	可执行以下操作： • 添加和删除 Kaspersky Security 服务用户。 • 编辑 Kaspersky Security 服务的用户访问权限。
删除服务	可在 Microsoft Windows 服务控制管理器中取消注册 Kaspersky Security 服务。
用户定义的服务请求	可创建和发送对 Kaspersky Security 服务的用户请求。

您可以编辑允许管理 Kaspersky Security 服务的用户和用户组列表，还可以编辑这些用户和用户组的访问权限。

如何在 Kaspersky Security Center 管理控制台中配置用户权限以管理 Kaspersky Security 服务

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**补充**”。
4. 在“**Kaspersky Security Service 管理的用户访问权限**”区域中单击“**设置**”。
   这将打开配置用户访问权限的表单。
5. 添加您想要配置 Kaspersky Security Service 用户权限的 Active Directory 用户或组。
6. 选择要授予其管理应用程序的权限的用户或用户组。
7. 在权限列表中，配置用户管理 Kaspersky Security Service 的权限。
8. 如果有必要，为用户配置特殊权限：
   a. 点击“**附加**”。
   b. 这打开了一个窗户；在该窗口中，选择一个用户账户。
   c. 双击打开用户账户属性。
   d. 这将打开一个窗口；在该窗口中，单击“**显示其他权限**”链接。
   e. 这将打开一个窗口；在该窗口中，为用户配置特殊权限。
9. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在应用程序控制台中配置用户权限以管理 Kaspersky Security 服务

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**Kaspersky Security Service 管理的用户访问权限**”。
2. 在打开的窗口中，在“**权限**”块，点击“**添加**”按钮。
   这将打开配置用户访问权限的表单。
3. 添加您想要配置 Kaspersky Security Service 用户权限的 Active Directory 用户或组。
4. 选择要授予其管理应用程序的权限的用户或用户组。
5. 在权限列表中，配置用户管理 Kaspersky Security Service 的权限。
6. 如果有必要，为用户配置特殊权限：
   a. 点击“**附加**”。
   b. 这打开了一个窗户；在该窗口中，选择一个用户账户。
   c. 双击打开用户账户属性。
   d. 这将打开一个窗口；在该窗口中，单击“**显示其他权限**”链接。
   e. 这将打开一个窗口；在该窗口中，为用户配置特殊权限。
7. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置用户权限以管理 Kaspersky Security 服务

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**补充** → **Kaspersky Security Service 管理的用户访问权限**”并点击“**配置**”按钮。
   “**Kaspersky Security Service 管理的用户访问权限**”窗口将打开。
5. 添加您想要配置 Kaspersky Security Service 用户权限的 Active Directory 用户或组。
6. 选择要授予其管理应用程序的权限的用户或用户组。

   > 您不能配置特殊权限以在 Web Console 中管理应用程序服务。

7. 保存更改。要在计算机上应用该策略，请关闭锁。

对 Kaspersky Industrial CyberSecurity for Nodes 功能进行受密码保护的访问

配置用户权限使您可以来限制对应用程序管理和已注册服务的访问。您也可在 Kaspersky Industrial CyberSecurity for Nodes 设置中设置密码保护，以提供关键操作的额外保护。

当用户尝试执行受密码保护的操作时，Kaspersky Industrial CyberSecurity for Nodes 会提示用户输入用户名和密码或者临时密码。密码保护支持以下账户：

- **KLAdmin**。具有 Kaspersky Industrial CyberSecurity for Nodes 无限制访问权限的管理员账户。KLAdmin 账户有权执行任何受密码保护的操作。KLAdmin 账户的权限无法撤销。当启用密码保护时，Kaspersky Industrial CyberSecurity for Nodes 会提示您设置 KLAdmin 账户的密码。
- **手动添加的账户**。Active Directory 域之外的账户。如果您不想共享管理员密码，可以使用此服务账户而不是 KLAdmin。您可以设置任何用户名和密码，并配置个人权限。
- **Everyone 组**。Windows 内置的组，包括公司网络内的所有用户。Everyone 组中的用户可以根据其被分配的权限访问应用程序。
- **单个用户或组**。可以为其配置单个权限的用户账户。例如，如果针对 Everyone 组阻止某个操作，您可以允许单个用户或组执行该操作。

Kaspersky Industrial CyberSecurity for Nodes 界面会在屏幕上隐藏指定密码。输入密码后，Kaspersky Industrial CyberSecurity for Nodes 将密码存储为计算得出的校验和。

多次尝试失败后，Kaspersky Industrial CyberSecurity for Nodes 不会检查密码强度，也不会阻止密码输入。

创建密码时，建议满足以下条件：

- 密码不包含账户名或计算机名。
- 密码长度至少为 8 个字符。
- 密码包含的字符与以下至少三个类别匹配：
  - 大写拉丁字母 (A-Z)
  - 小写拉丁字母 (a-z)
  - 数字（0-9）
  - 感叹号 (!)、美元符号 ($)、英镑符号 (#) 和百分号 (%)

如何在 Kaspersky Security Center 管理控制台中使用密码保护对 Kaspersky Industrial CyberSecurity for Nodes 功能的访问

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**补充**”。
4. 在“**应用程序管理的用户访问权限**”区域中单击“**设置**”。
5. 在打开的窗口中，选中“**允许使用手动创建的用户的凭证确认应用程序的操作**”复选框。
6. 如有必要，清空“**请求密码以确认关键操作**”复选框。
   如果启用了此功能，则应用程序在删除、修改或恢复应用程序时，以及在命令行上执行**可能降低设备保护级别的操作**时，会请求用户名和密码。

   应用程序在运行以下命令时请求凭证：

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`
   - `KAVSHELL QUARANTINE /DELETE`
   - `KAVSHELL REMOTEACCESS`
   - `KAVSHELL RESETMDRMACHINEID`
   - `KAVSHELL SERVERBINDINGDISABLE`
   - `KAVSHELL SIGMA /DISABLE`
   - `KAVSHELL SIGMA /ADD`

- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

如果此功能被禁用，并且当前用户拥有必要权利，Kaspersky Industrial CyberSecurity for Nodes 不要求凭证。默认启用该选项。

如果为当前用户设置了空的 Windows 密码，则需要输入拥有必要权限且密码非空的用户的凭证。

7. 指定 KLAdmin 用户账户的密码。
8. 如有必要，添加您想要授予应用程序管理访问权限的用户账户：
   a. 单击“**添加**”。
   这将打开配置用户访问权限的表单。
   b. 在打开的窗口中，选择添加用户的方法：**手动添加用户/用户组**。
   c. 指定用户名和密码。
   d. 在“**权限**”列表，配置用户对应用程序功能的访问权限。
9. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用控制台台中使用密码保护对 Kaspersky Industrial CyberSecurity for Nodes 功能的访问

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**应用程序管理的用户访问权限**”。
2. 在打开的窗口中，选中“**允许使用手动创建的用户的凭证确认应用程序的操作**”复选框。
3. 如有必要，清空“**请求密码以确认关键操作**”复选框。
   如果启用了此功能，则应用程序在删除、修改或恢复应用程序时，以及在命令行上执行**可能降低设备保护级别的操作**时，会请求用户名和密码。

   应用程序在运行以下命令时请求凭证：
   - KAVSHELL APPCONTROL
   - KAVSHELL APPCONTROL /CONFIG
   - KAVSHELL APPCONTROL /GENERATE /import
   - KAVSHELL DEVCONTROL
   - KAVSHELL EXITPOLICY

- KAVSHELL IMPORT
- KAVSHELL ISOLATION /DISABLE
- KAVSHELL LICENSE /DEL
- KAVSHELL PASSWORD
- KAVSHELL PREVENTION /DISABLE
- KAVSHELL QUARANTINE /ADD
- KAVSHELL QUARANTINE /DELETE
- KAVSHELL REMOTEACCESS
- KAVSHELL RESETMDRMACHINEID
- KAVSHELL SERVERBINDINGDISABLE
- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

如果此功能被禁用，并且当前用户拥有必要权利，Kaspersky Industrial CyberSecurity for Nodes 不要求凭证。默认启用该选项。

如果为当前用户设置了空的 Windows 密码，则需要输入拥有必要权限且密码非空的用户的凭证。

4. 指定 KLAdmin 用户账户的密码。
5. 如有必要，添加您想要授予应用程序管理访问权限的用户账户：
   a. 单击“**添加**”。
      这将打开配置用户访问权限的表单。
   b. 在打开的窗口中，选择添加用户的方法：**手动添加用户/用户组**。
   c. 指定用户名和密码。
   d. 在“**权限**”列表，配置用户对应用程序功能的访问权限。
6. 保存更改。

如何在 Kaspersky Security Center Web Console 中使用密码保护对 Kaspersky Industrial CyberSecurity for Nodes 功能的访问

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**补充 → 应用程序管理的用户访问权限**”并点击“**配置**”按钮。
5. 在打开的窗口中，选中“**允许使用手动创建的用户的凭证确认应用程序的操作**”复选框。
6. 如有必要，清空“**请求密码以确认关键操作**”复选框。
   如果启用了此功能，则应用程序在删除、修改或恢复应用程序时，以及在命令行上执行**可能降低设备保护级别的操作**时，会请求用户名和密码。

   应用程序在运行以下命令时请求凭证：

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`
   - `KAVSHELL QUARANTINE /DELETE`
   - `KAVSHELL REMOTEACCESS`
   - `KAVSHELL RESETMDRMACHINEID`
   - `KAVSHELL SERVERBINDINGDISABLE`
   - `KAVSHELL SIGMA /DISABLE`

- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

如果此功能被禁用，并且当前用户拥有必要权利，Kaspersky Industrial CyberSecurity for Nodes 不要求凭证。默认启用该选项。

如果为当前用户设置了空的 Windows 密码，则需要输入拥有必要权限且密码非空的用户的凭证。

7. 指定 KLAdmin 用户账户的密码。
8. 如有必要，添加您想要授予应用程序管理访问权限的用户账户：
   a. 单击“**添加**”。
      这将打开配置用户访问权限的表单。
   b. 在打开的窗口中，选择添加用户的方法：**手动添加用户/用户组**。
   c. 指定用户名和密码。
   d. 在“**权限**”列表，配置用户对应用程序功能的访问权限。
9. 保存更改。要在计算机上应用该策略，请关闭锁。

此密码无法恢复。丢失密码会导致完全失去对应用程序的控制。此外，您还将无法从受保护设备卸载应用程序。

您可以随时重置密码。为此，请清除“**允许使用手动创建的用户的凭证确认应用程序的操作**”复选框并保存更改。密码保护将被禁用，旧密码校验和将被删除。使用新密码重复密码创建过程。

安全桌面通知

Kaspersky Industrial CyberSecurity for Nodes 支持（Secure Desktop）功能。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。

Kaspersky Industrial CyberSecurity for Nodes 显示安全桌面通知以确认以下操作：

- 已启用或禁用跟踪
- 已导出或导入应用程序设置

- 保护已暂停
- 应用程序已退出
- 已删除活动密钥
- Kaspersky Industrial CyberSecurity for Nodes 已卸载
- 设备控制已禁用
- 实时文件保护已禁用
- Kaspersky Security Center 策略已禁用
- 已查看报告
- 文件已从备份区中恢复
- Kaspersky Industrial CyberSecurity for Nodes 设置已修改
- 应用程序任务已由启动以外的方式管理

如何在 Kaspersky Security Center 管理控制台中启用或禁用安全桌面通知

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，转到“**应用程序设置**”区域。
4. 在“**安全性和可靠性**”块中单击“**设置**”按钮。
5. 这将打开一个窗口；在该窗口中，选择“**安全**”选项卡。
6. 在“**自我保护**”块，选中或清空“**启用安全桌面通知**”复选框以启用或禁用安全桌面通知。

   如果自我保护被禁用，则“**启用安全桌面通知**”复选框不可用。

7. 关闭挂锁以将策略应用于计算机。
8. 点击“**确定**”保存更改。

如何在应用程序控制台中启用或禁用安全桌面通知

1. 在应用程序控制台树中，选择 **Kaspersky Industrial CyberSecurity for Nodes** 节点，并在结果窗格中，单击“**应用程序属性**”链接。
2. 这将打开一个窗口；在该窗口中，选择“**安全设置**”选项卡。

3. 在“**自我保护**”块，选中或清空“**启用安全桌面通知**”复选框以启用或禁用安全桌面通知。

   如果自我保护被禁用，则“**启用安全桌面通知**”复选框不可用。

4. 点击“**确定**”保存更改。

如何在 Kaspersky Security Center Web Console 中启用或禁用安全桌面通知

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**应用程序设置**”部分。
5. 在“**安全性和可靠性**”块中单击“**配置**”按钮。
   “**安全性和可靠性**”窗口将打开。
6. 在“**自我保护**”块，选中或清空“**启用安全桌面通知**”复选框以启用或禁用安全桌面通知。

   如果自我保护被禁用，则“**启用安全桌面通知**”复选框不可用。

7. 关闭挂锁以将策略应用于计算机。
8. 点击“**确定**”保存更改。

信任区域

受*信任区域*是由系统管理员配置的、Kaspersky Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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。管理员也可以允许用户为特定计算机创建他们自己的本地受信任域。这样，除了策略中的常规受信任域，用户可以创建他们自己的本地排除项和受信任应用程序列表。

您还可以将 EDR 遥测添加到受信任区域。这允许优化应用程序发送到卡巴斯基反针对性攻击平台 (EDR) 解决方案的遥测服务器的数据。

预定义的扫描排除项和受信任的应用程序被添加到受信任区域。预定义的扫描排除项和受信任的应用程序有助于快速配置 Kaspersky Industrial CyberSecurity for Nodes，而无需手动创建受信任区域。

创建扫描排除项

"*扫描排除项*"是一组条件，必须满足这些条件，Kaspersky Industrial CyberSecurity for Nodes 才不会扫描特定对象是否存在病毒和其他威胁。

扫描排除项可供以下应用程序组件和任务使用：

- **实时文件保护**
- **按需扫描**
- **反加密**
- **AMSI 保护**
- **网络威胁防护**

如果包含某个对象的驱动器或文件夹在扫描任务启动时包括在扫描范围中，则 Kaspersky Industrial CyberSecurity for Nodes 不会扫描该对象。但是，当启动了针对该特殊对象的自定义扫描任务时，扫描排除项将不应用。

Kaspersky Industrial CyberSecurity for Nodes 不支持包含超过 5000 个对象的排除列表。

如何在 Kaspersky Security Center 管理控制台中创建扫描排除项

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择"**补充 → 受信任区域**"并点击"**设置**"。

4. 选择**扫描排除项**选项卡。

5. 如果要为公司内的所有计算机创建排除项的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的排除项列表。如果启用继承时合并值，则将合并列表。父策略中的排除项以只读视图的形式显示在子策略中。无法更改或删除父策略的排除项。

6. 如果您要让用户创建排除项本地列表，选择“**允许使用本地排除项**”复选框。这样，除了策略中生成的排除项常规列表，用户可以创建他们自己的排除项本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的排除项常规列表。此外，如果清除此复选框，Kaspersky Industrial CyberSecurity for Nodes 会在应用程序控制台中隐藏扫描排除项的综合列表。

7. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。
   - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的扫描排除项添加到列表的根目录中。
   - “**将新排除项添加到所选类别**”。要将新的扫描排除项添加到特定类别，请选择一个类别。
   - “**从列表选择排除项**”。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义扫描排除项列表中添加排除项。

8. 要从扫描中排除某个文件或文件夹，请选择“**文件或文件夹**”复选框。点击“**选择文件或文件夹**”链接打开一个窗口，然后通过单击“**浏览**”选择一个文件或文件夹。

   您也可以手动输入路径。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

   - `*`（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。
   - 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。
   - `?`（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。

     您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

9. 要从扫描中排除预定义区域，请选择“**预定义范围**”复选框。点击“**选择预定义范围**”链接打开一个窗口，并在该窗口中选择受保护设备上的标准范围之一。

10. 要从扫描中排除特定对象，请选择“**检测对象类型**”复选框。点击“**输入对象名称**”链接，点击“**添加**”按钮，在显示的窗口中，根据卡巴斯基百科全书分类（例如， `Email-Worm`、 `Rootkit` 或者 `RemoteAdmin`）输入对象类型名称。

    您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Industrial CyberSecurity for Nodes 从扫描中排除 `Client-IRC`、 `Client-P2P` 和 `Client-SMTP` 对象。

11. 要从扫描中排除单个文件，请选择“**对象哈希**”复选框。点击“**输入对象哈希值**”链接打开一个窗口，并在该窗口中输入文件哈希。

    如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

12. 在**规则使用范围**块，选择您要应用扫描排除项的组件。

13. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

14. 保存更改以将排除项添加到列表中。您可以随时使用对象旁边的复选框禁用排除项。

如何在 Kaspersky Security Center Web Console 中创建扫描排除项

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**补充** → **受信任区域**”并点击“**配置**”按钮。

5. 选择**扫描排除项**选项卡。

6. 如果要为公司内的所有计算机创建排除项的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的排除项列表。如果启用继承时合并值，则将合并列表。父策略中的排除项以只读视图的形式显示在子策略中。无法更改或删除父策略的排除项。

7. 如果您要让用户创建排除项本地列表，选择“**允许使用本地排除项**”复选框。这样，除了策略中生成的排除项常规列表，用户可以创建他们自己的排除项本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的排除项常规列表。此外，如果清除此复选框，Kaspersky Industrial CyberSecurity for Nodes 会在应用程序控制台中隐藏扫描排除项的综合列表。

8. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。
   - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的扫描排除项添加到列表的根目录中。
   - “**从列表选择排除项**”。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义扫描排除项列表中添加排除项。

9. 如果要从扫描中排除文件或文件夹，请选择“**文件或文件夹**”并选中同名字段中的复选框。指定文件或文件夹的路径。

当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

- `*`（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。

- 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。

- `?`（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。

  您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

10. 要从扫描中排除预定义范围，请选择“**预定义范围**”。在下拉列表中，选择受保护设备上的标准范围之一。

11. 如果要从排除中排除某些对象，请选择“**检测对象类型**”复选框并根据卡巴斯基百科全书分类输入对象类型的名称（例如，`Email-Worm`、`Rootkit` 或者 `RemoteAdmin`）。

    您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Industrial CyberSecurity for Nodes 从扫描中排除 *Client-IRC*、*Client-P2P* 和 *Client-SMTP* 对象。

12. 要从扫描中排除单个文件，请选择“**对象哈希**”复选框并从文件或事件列表中添加哈希。

    如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

13. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

14. 在**保护组件**块，选择您要应用扫描排除项的组件。

15. 新的排除项将被添加到列表。您可以随时使用“**状态**”列中的复选框禁用排除项。

16. 保存更改。

如何在应用程序控制台中创建扫描排除项

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**受信任区域**”。

   “**配置信任区域设置**”窗口将打开。

2. 在“**排除项**”部分，点击“**扫描排除项**”块旁边的“**设置**”按钮。

3. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。

   - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的扫描排除项添加到列表的根目录中。

- "**将新排除项添加到所选类别**"。要将新的扫描排除项添加到特定类别，请选择一个类别。
- "**从列表选择排除项**"。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义扫描排除项列表中添加排除项。

4. 要从扫描中排除某个文件或文件夹，请选择"**文件或文件夹**"复选框。点击"**选择文件或文件夹。**"链接打开一个窗口，然后在该窗口中通过单击"**浏览**"选择一个文件或文件夹。

   您也可以手动输入路径。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

   - `*`（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。
   - 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。
   - `?`（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。

     您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

5. 要从扫描中排除预定义区域，请选择"**预定义范围**"复选框。点击"**选择预定义范围**"链接打开一个窗口，并在该窗口中选择受保护设备上的标准范围之一。

6. 要从扫描中排除特定对象，请选择"**检测对象类型**"复选框。点击"**输入对象名称**"链接，点击"**添加**"按钮，在显示的窗口中，根据卡巴斯基百科全书分类（例如， `Email-Worm`、`Rootkit` 或者 `RemoteAdmin`）输入对象类型名称。

   您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Industrial CyberSecurity for Nodes 从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

7. 要从扫描中排除单个文件，请选择"**对象哈希**"复选框。点击"**输入对象哈希值**"链接打开一个窗口，并在该窗口中输入文件哈希。

   如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

8. 在**规则使用范围**块，选择您要应用扫描排除项的组件。

9. 如有必要，在"**注释**"字段，输入您创建的扫描排除项的简短描述。

10. 保存更改以将排除项添加到列表中。您可以随时使用对象旁边的复选框禁用排除项。

路径掩码例子：
位于任意文件夹的文件的路径：

- 掩码 `*.exe` 将包括具有 exe 扩展名的文件的所有路径。
- 掩码 `example*` 将包括名为 EXAMPLE 的文件的所有路径。

位于指定文件夹的文件的路径：

- 掩码 `C:\dir\*.*` 将包括位于 C:\dir\ 文件夹中的所有文件的路径，但不包括 C:\dir\ 的子文件夹中的文件的路径。
- 掩码 `C:\dir\*` 将包括位于 C:\dir\ 文件夹中的所有文件的路径，包括子文件夹。
- 掩码 `C:\dir\` 将包括位于 C:\dir\ 文件夹中的所有文件的路径，包括子文件夹。
- 掩码 `C:\dir\*.exe` 将包括位于 C:\dir\ 文件夹中具有 EXE 扩展名的所有文件的路径，但不包括 C:\dir\ 的子文件夹中的此类文件的路径。
- 掩码 `C:\dir\test` 将包括位于 C:\dir\ 文件夹中名为“test”的所有文件的路径，但不包括 C:\dir\ 的子文件夹中的此类文件的路径。
- 掩码 `C:\dir\*\test` 将包括位于 C:\dir\ 文件夹及 C:\dir\ 的子文件夹中名为“test”的所有文件的路径。
- 掩码 `C:\dir1\*\dir3\` 将包含指向 C:\dir1\ 文件夹中一级 dir3 子文件夹中文件的所有路径。
- 掩码 `C:\dir1\**\dirN\` 将包括 C:\dir1\ 文件夹中 dirN 子文件夹中任何级别的所有文件路径。

位于所有文件夹中具有指定名称的文件的路径：

- 掩码 `dir\*.*` 将包括名为“dir”的文件夹中的所有文件的路径，但不包括这些文件夹的子文件夹中的文件的路径。
- 掩码 `dir\*` 将包括名为“dir”的文件夹中的所有文件的路径，但不包括这些文件夹的子文件夹中的文件的路径。
- 掩码 `dir\` 将包括名为“dir”的文件夹中的所有文件的路径，但不包括这些文件夹的子文件夹中的文件的路径。
- 掩码 `dir\*.exe` 将包括名为“dir”的文件夹中具有 EXE 扩展名的所有文件的路径，但不包括这些文件夹的子文件夹中的此类文件的路径。
- 掩码 `dir\test` 将包括名为“dir”的文件夹中名为“test”的所有文件的路径，但不包括这些文件夹的子文件夹中的此类文件的路径。

选择可检测对象的类型

要选择可检测对象的类型，请执行以下操作：

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并执行以下操作之一：
   - 在节点的结果窗格中，单击“**配置信任区域设置**”链接。
   - 在节点的上下文菜单中选择“**受信任区域**”。

   “**配置信任区域设置**”窗口将打开。
2. 在“**检测对象类型**”区域中单击“**设置**”。
3. 在打开的窗口中，请选择您想要 Kaspersky Industrial CyberSecurity for Nodes 检测的对象类型旁边的复选框：
   - **病毒和蠕虫**

     子分类：病毒和蠕虫 (Viruses_and_Worms)

     危险级别：高

典型的病毒和蠕虫会执行未经用户授权的操作。它们会创建可自我复制的副本。

典型病毒

典型病毒侵入计算机后，会感染文件，激活并执行恶意操作，以及将自身的副本添加到其他文件中。

典型病毒仅在计算机本地资源上复制副本，不会自行侵入其他计算机。仅当该病毒将其副本添加至存储在共享文件夹或放入计算机中的 CD 中的文件时，或者在用户发送附有受感染文件的电子邮件消息时，该病毒才会传染给其他计算机。

典型病毒代码可以入侵计算机、操作系统和应用程序的各种区域。根据具体的环境，病毒可分为*文件病毒*、*引导区病毒*、*脚本病毒*和*宏病毒*。

病毒可以使用多种不同的技术来感染文件。*覆盖*病毒会使用其代码覆盖受感染文件的代码，从而抹除文件的内容。感染的文件会停止发挥作用，且无法恢复。*寄生*病毒会修改文件，从而使自身发挥全部或部分功能。*伴随病毒*不会修改文件，而是创建副本。当您打开受感染的文件时会启动该文件的副本（实际上是病毒）。您也会遇到以下类型的病毒：*链接病毒*、*OBJ 病毒*、*LIB 病毒*、*源代码病毒*和许多其他病毒。

蠕虫

与典型病毒一样，蠕虫在侵入计算机后，其代码将激活并执行恶意操作。之所以称为蠕虫，是因为它们能够从一台计算机“爬”到另一台计算机，并不需用户权限即可通过许多数据通道来传播副本。

可用于区分各种类型蠕虫的主要特征是蠕虫的传播方式。下表提供了各种类型蠕虫的概览，这些蠕虫按其传播方式进行了分类。

蠕虫传播方式

类型	名称	描述
电子邮件蠕虫	电子邮件蠕虫	这些蠕虫通过电子邮件传播。 受感染的电子邮件消息包含带有蠕虫副本的附件，或指向上传到可能已被攻击或者专门创建用于传播蠕虫的网站上某文件的链接。打开该附件时，蠕虫将被激活。在您单击该链接，进行下载，然后打开文件时，蠕虫还会开始执行其恶意操作。之后，蠕虫会继续传播其副本，搜索其他电子邮件地址，并向它们发送受感染的邮件。
IM 蠕虫	IM 客户端蠕虫	它们通过 IM 传播。 通常，此类蠕虫会利用用户的联系人列表发送消息，其中包含指向某网站上带有蠕虫副本的文件的链接。用户下载并打开文件时，蠕虫将被激活。
IRC 蠕虫	互联网聊天蠕虫	这些蠕虫会通过互联网中继聊天（允许通过互联网与其他人实时通信的服务系统）传播。 这些蠕虫会在互联网聊天中年发布包含自身副本的文件或指向该文件的链接。用户下载并打开文件时，蠕虫将被激活。
网络蠕虫	网络蠕虫	这些蠕虫通过计算机网络传播。 与其他类型的蠕虫不同，典型的网络蠕虫不需用户参与即可传播。它会扫描本地网来寻找安装了有漏洞的程序的计算机。为此，它会发送特殊格式的网络数据包（漏洞），其中包含蠕虫代码或部分蠕虫代码。如果网络上存在“有漏洞”的计算机，该计算机会接收到此种网络数据包。蠕虫完全入侵计算机后，将被激活。
P2P 蠕虫	文件共享网络蠕虫	它们通过点对点文件共享网络传播。 为了渗透到 P2P 网络，蠕虫会将自身复制到通常位于用户计算机上的文件共享文件夹中。P2P 网络会显示有关该文件的信息，以便用户可以在网络中像任何其他文件一样“找到”受感染的文件，然后下载并打开该文件。 更加狡猾的蠕虫会模仿特定 P2P 网络的网络协议：它们会返回对搜索程序的积极响应，并提供自身的副本供下载。
蠕虫	其他类型的蠕虫	其他类型的蠕虫包括： • 通过网络资源传播自身副本的蠕虫。通过使用操作系统的功能，它们扫描可用的网络文件夹，连接到互联网上的计算机，并尝试获取对磁盘驱动器的完全访问。与之前描述的蠕虫类型不同，其他类型的蠕虫不会自行激活，而是在用户打开包含蠕虫副本的文件时激活。 • 不使用上表中所述的任何方法进行传播的蠕虫（例如，通过手机传播的蠕虫）。

- **木马**

子类别：木马

危险级别：高

与蠕虫和病毒不同，木马不能进行自我复制。例如，用户访问受感染的网页时，它们会通过电子邮件或浏览器侵入计算机。木马通过用户参与而启动。木马启动后即会开始执行恶意操作。

在受感染的计算机上，不同的木马会表现出不同的行为。木马的主要功能包括阻止、修改或破坏信息，以及禁用计算机或网络。木马还可以接收或发送文件，在屏幕上显示消息，请求网页，下载和安装程序，以及重启计算机。

黑客通常使用各种不同木马的“集合”。

下表中介绍了木马行为的类型。

受感染计算机上木马行为的类型

类型	名称	描述
木马炸弹	木马 –“压缩文件炸弹”	解压缩时，这些压缩文件的大小会急剧增加，从而影响计算机的操作。 用户尝试解压缩这种压缩文件时，计算机可能会运行缓慢或停止运行；硬盘可能会充满“空白”数据。“压缩文件炸弹”对于文件和邮件服务器尤为危险。如果服务器使用自动系统处理接收信息，则“压缩文件炸弹”可能会中断服务器运行。
后门	用于远程管理的木马	此种木马被视为最危险的木马类型。在功能方面，这些木马与安装在计算机上的远程管理应用程序相似。 这些程序会在不被用户发觉的情况下将自身安装到计算机上，以便入侵者远程管理计算机。
木马	木马	木马包括以下恶意应用程序： • **典型木马**。这些程序仅执行木马的主要功能：阻止、修改或破坏信息，以及禁用计算机或网络。它们没有任何高级功能，与表中描述的其他类型的木马不同。 • **万能木马**。这些程序具有多种典型木马类型的高级功能。
勒索木马	勒索木马	这些木马将用户信息作为“人质”，修改或阻止信息，或者影响计算机的操作，以使用户无法使用信息。入侵者向用户进行勒索，许诺发送应用程序来恢复计算机的性能以及计算机上存储的数据。
木马点击器	木马点击器	这些木马通过自行向浏览器发送命令或更改在操作系统文件中指定的网址的方式，从用户的计算机访问网页。 通过使用这些程序，入侵者进行网络攻击并提高网站访问量，从而增加条幅广告的显示次数。
木马下载器	木马下载器	这些木马会访问入侵者的网页，从中下载其他恶意应用程序，并将它们安装到用户的计算机。这些木马包含要下载的恶意应用程序的文件名，或从访问的网页中接收该文件名。
木马释放器	木马释放器	这些木马包含安装在硬盘驱动器上并随后进行安装的其他木马。 入侵者可能会使用木马释放器类型的程序来达到以下目的： • 未通知用户就安装恶意应用程序：木马释放器类型的程序不会显示消息，或者会显示虚假消息，例如通知压缩文件中存在错误或操作系统的版本不兼容。 • 保护另一个已知恶意应用程序不被检测：并非所有反病毒软件都可检测到木马释放器类型应用程序中的恶意应用程序。
通知型木马	通知型木马	这些木马会通知入侵者受感染的计算机可供访问，并向入侵者发送有关计算机的信息：IP 地址、已开放端口号或电子邮件地址。它们通过电子邮件、FTP、访问入侵者的网页或以其他方式与入侵者联系。 通知型木马类型的程序通常用于包含多种木马的集合中。这些木马会通知入侵者其他木马已成功安装到用户的计算机。
代理型木马	代理型木马	这些木马允许入侵者使用用户的计算机匿名访问网页，它们通常用于发送垃圾邮件。
PSW 木马	密码盗窃软件	密码盗劫软件是盗窃用户账户（如软件注册数据）的一种木马。这些木马会查找系统文件和注册表中的机密数据，并通过电子邮件、FTP、访问入侵者的网页或以其他方式将其发送给“攻击者”。 部分这些木马分类为此表中描述的单独类型。这些木马会盗窃银行账户（网银窃贼木马），窃取 IM 客户端用户的数据（IM 木马），以及盗窃在线游戏用户的信息（游戏窃贼木马）。

类型	名称	描述
间谍木马	间谍木马	这些木马暗中监视用户，收集有关用户使用计算机时所做的操作的信息。它们可能会拦截用户通过键盘输入的数据，截取屏幕，或收集活动应用程序的列表。收到信息后，这些木马会通过电子邮件、FTP、访问入侵者的网页或以其他方式将信息传输给入侵者。
分布式拒绝服务攻击木马	木马网络攻击者	这些木马会从用户计算机将大量请求发送至远程服务器。服务器缺少资源来处理所有请求，因此会停止运行（拒绝服务，或简称为 DoS）。黑客通常会使用这些程序感染许多计算机，以使用这些计算机来同时攻击一个服务器。 DoS 程序在用户知悉的情况下从一台计算机发起攻击。DDoS（分布式 DoS）程序在不被受感染计算机用户发觉的情况下从多台计算机发起分布式攻击。
IM 木马	从 IM 客户端用户那里窃取信息的木马	它们会窃取 IM 客户端用户的帐号和密码。这些木马会通过电子邮件、FTP、访问入侵者的网页或以其他方式将数据传输给入侵者。
Rootkit	Rootkit	这些木马会掩盖其他恶意应用程序及其活动，从而延长这些应用程序在操作系统中持续存在的时间。它们还会隐藏文件、受感染计算机内存中的进程或运行恶意应用程序的注册表键。Rootkit 会掩盖用户计算机上的应用程序与网络上其他计算机之间进行的数据交换。
SMS 木马	SMS格式的木马	这些木马会感染手机，向额外收费的手机号码发送 SMS。
游戏窃贼木马	从在线游戏用户那里窃取信息的木马	这些木马会窃取在线游戏用户的账户凭据，然后将这些凭据通过电子邮件、FTP、访问黑客的网页或以其他方式发送给黑客。
网银窃贼木马	窃取银行账户的木马	这些木马会窃取银行账户数据或电子货币系统数据；将这些数据通过电子邮件、FTP、访问黑客的网页或以其他方式发送给黑客。
邮件侦测木马	收集电子邮件地址的木马	这些木马会收集存储在计算机上的电子邮件地址，然后通过电子邮件、FTP、访问入侵者的网页或以其他方式将它们发送给入侵者。入侵者可能会向收集到的地址发送垃圾邮件。

- **恶意工具**

子类别：恶意工具

危险级别：中

与其他类型的恶意软件不同，恶意工具在启动过后不会执行其操作。恶意工具可以在用户的计算机上安全地存储和启动。入侵者通常使用这些程序的功能来创建病毒、蠕虫和木马，对远程服务器进行网络入侵，攻击计算机或执行其他恶意操作。

恶意工具的各种功能按下表中所述的类型进行分组。

恶意工具的功能

类型	名称	描述
构建器	构建器	通过它们可以创建新的病毒、蠕虫和木马。一些构建器扬言构建了基于窗口的标准界面，用户可在该界面中选择要创建的恶意应用程序的类型，对付调试程序的方式，以及其他功能。
拒绝服务攻击	网络攻击	这些木马会从用户计算机将大量请求发送至远程服务器。服务器缺少资源来处理所有请求，因此会停止运行（拒绝服务，或简称为 DoS）。
漏洞	漏洞	"*漏洞*"是一组数据或程序代码，利用处理它们的应用程序的缺陷对计算机执行恶意操作。例如，漏洞可以写入或读取文件，或请求"受感染"的网页。 不同的漏洞会利用不同应用程序或网络服务的缺陷。漏洞会伪装成网络数据包通过网络传输到许多计算机，然后搜索网络服务存在缺陷的计算机。DOC 文件中的漏洞会利用文本编辑器的缺陷。在用户打开受感染的文件时，它可能会开始执行黑客编程的操作。嵌入在电子邮件消息中的漏洞会搜索电子邮件客户端的缺陷。用户在电子邮件客户端中打开受感染的邮件时，漏洞会立即开始执行恶意操作。 网络蠕虫会使用漏洞通过网络进行传播。Nuker 漏洞是可禁用计算机的网络数据包。
文件加密器	加密器	加密器会加密其他恶意应用程序，以隐藏它们不被反病毒应用程序发现。
洪水攻击器	用于"污染"网络的程序	这些程序会通过网络通道发送大量邮件。例如，该类型的工具包括污染互联网中继聊天的程序。 洪水攻击器工具不包括"污染"电子邮件、IM 客户端以及移动通信系统所使用通道的程序。这些程序可分为表中介绍的各种类型（电子邮件洪水攻击器、IM 洪水攻击器和 SMS 洪水攻击器）。

类型	名称	描述
黑客工具	黑客工具	这些工具可以破坏其所在的计算机，或攻击其他计算机（例如，未经用户许可添加新系统账户，或清除系统日志以隐藏在操作系统中的存在路径）。这种类型的工具包括一些具有恶意功能的嗅探器，例如密码截取。嗅探器是允许查看网络流量的程序。
恶作剧程序	恶作剧程序	这些程序会警告用户类似病毒的消息：它们可能会在未受感染的文件中"检测到病毒"，或通知用户磁盘已被格式化，尽管这些情况实际并未发生。
地址欺骗程序	地址欺骗工具	这些工具使用伪造的发件人地址发送邮件和网络请求。例如，入侵者会使用地址欺骗程序类型的工具来掩盖他们作为邮件实际发件人的事实。
病毒修改工具	修改恶意应用程序的工具	通过这些工具可以修改其他恶意软件，隐藏它们不被反病毒程序发现。
电子邮件洪水攻击器	"污染"电子邮件地址的程序	这些程序会向各种电子邮件地址发送大量邮件，从而"污染"这些地址。大量的接收邮件会妨碍用户查看收件箱中的有用邮件。
IM 洪水攻击器	"污染"IM 流量的程序	它们向 IM 的用户发送大量消息。大量的信息会妨碍用户查看有用的接收信息。
SMS 洪水攻击器	使用 SMS"污染"流量的程序	这些程序向手机发送大量 SMS。

- **广告软件**

  子类别：广告软件；

  危险级别：中

  广告软件向用户显示广告信息。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。某些广告软件程序会收集有关用户的营销信息，并将其发送给开发者：该信息可能包括用户访问的网站的名称，或用户搜索查询的内容。与间谍木马类型的程序不同，广告软件程序会在用户许可的情况下将该信息发送给开发者。

- **自动拨号程序**

  子类别：自动拨号器（拨号器）。

  危险级别：中

  自动拨号器可以使用调制解调器秘密建立电话连接。

- **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**

  子类别：可能会被犯罪分子用来破坏计算机或个人数据的合法软件。

  危险级别：中

  大多数这些应用程序都很有用，因此有许多用户使用它们。这些应用程序包括 IRC 客户端、自动拨号程序、文件下载程序、计算机系统活动监控器、密码实用程序以及用于 FTP、HTTP 和 Telnet 的互联网服务器。

  但是，如果入侵者获得了这些程序的访问权限，或如果他们在用户的计算机上安置这些程序，应用程序的某些功能可能会被用来危害安全。

这些应用程序具有不同的功能，下表介绍了它们的类型。

类型	名称	描述
客户端 IRC	互联网聊天客户端	用户安装这些程序与他人进行互联网中继聊天。入侵者使用这些程序来传播恶意软件。
下载器	用于下载的程序	这些程序可以在隐藏模式下从网页下载文件。
监控器	用于监控的程序	这些程序可监控其安装到的计算机上的活动（查看哪些应用程序正在活动，以及它们如何与安装在其他计算机上的应用程序交换数据）。
密码工具	密码恢复器	通过它们可以查看和恢复已忘记的密码。入侵者出于相同的目的，秘密地将它们安置在用户的计算机上。
远程管理程序	远程管理程序	系统管理员广泛使用的一些程序。通过这些程序可以获取对远程计算机界面的访问权限，以监控和管理该计算机。入侵者出于同样的目的，秘密地将它们安置在用户的计算机上：用于监控和管理远程计算机。 合法的远程管理程序与实现远程管理的后门类型的木马不同。木马能够独自入侵操作系统并自行安装；合法的程序则无法做到这些。
FTP 服务程序	FTP 服务器	这些程序可起到 FTP 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 FTP 对该计算机的远程访问。
代理服务程序	代理服务器	这些程序可起到代理服务器的作用。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。
Telnet 服务程序	Telnet 服务器	这些程序可起到 Telnet 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 Telnet 对该计算机的远程访问。
Web 服务程序	Web 服务器	这些程序可起到 Web 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 HTTP 对该计算机的远程访问。
风险工具	在本地计算机上工作的工具	在用户自己的计算机上工作时，这些工具会为用户提供其他选项。通过这些工具，用户可以隐藏文件或活动应用程序的窗口，并终止活动的进程。
网络工具	网络工具	与网络上的其他计算机配合工作时，这些工具会为用户提供其他选项。通过这些工具可以进行重启，检测开放的端口，以及启动安装在计算机上的应用程序。
P2P 客户端	P2P 网络客户端	通过它们可以在对等网络中工作。入侵者可能会利用它们传播恶意软件。
客户端 SMTP	SMTP 客户端	它们未经用户的同意便发送电子邮件。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。
Web 工具栏	Web 工具栏	它们会向其他应用程序的界面中添加工具栏，以使用搜索引擎。
欺骗工具	欺骗程序	这些程序将自己伪装为其他程序。例如，一些欺骗反病毒程序会显示有关恶意软件检测的信息。但实际上，它们并未找到任何内容或进行清除。

- **可能被用来保护恶意代码的打包对象**

  子类别：可能造成危害的打包文件。

  危险级别：中。

  该文件使用专门用于打包恶意软件（病毒、蠕虫、特洛伊木马）的特殊打包程序进行打包。Kaspersky Industrial CyberSecurity for Nodes 会扫描 SFX（自解压）存档中的解包工具模块。

  为了隐藏恶意软件以避免被反病毒软件检测到，黑客使用特殊的打包程序对其进行打包。卡巴斯基专家已识别出黑客最常使用的解包工具。

- **多层打包对象**

  子类别：多重打包文件。

危险级别：中。

该文件被一个或多个打包程序打包三次或三次以上。

为了隐藏恶意软件以避免被反病毒软件检测到，黑客可能会多次打包文件。Kaspersky Industrial CyberSecurity for Nodes 将扫描打包文件。

4. 保存更改。

编辑受信任应用程序列表

*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 Industrial CyberSecurity for Nodes 的监控。默认情况下，Kaspersky Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 将停止监控该应用程序的活动。

扫描排除项和受信任的应用程序之间的区别在于，对于排除项，Kaspersky Industrial CyberSecurity for Nodes 不扫描文件，而对于受信任的应用程序，它不控制启动的进程。如果受信任的应用程序在未包含在扫描排除项中的文件夹中创建恶意文件，Kaspersky Industrial CyberSecurity for Nodes 将检测该文件并消除威胁。如果该文件夹被添加到排除项，Kaspersky Industrial CyberSecurity for Nodes 将跳过该文件。

例如，如果您认为被标准 Microsoft Windows 记事本使用的对象是安全的，也即您信任此应用程序，则可将 Microsoft Windows 记事本添加到受信任的应用程序列表中，从而不监控该应用程序所使用的对象。这将提高计算机性能，这在使用服务器应用程序时尤为重要。

此外，被 Kaspersky Industrial CyberSecurity for Nodes 分类为可疑操作的某些操作，在很多应用程序的功能环境中可能是安全的。例如，拦截键盘键入的文本，是自动键盘布局切换器中的一种例行程序（例如 Punto Switcher）。考虑到此类程序的特点并将其行为从监控中排除，我们建议您可将此类程序添加到受信任应用程序列表中。

受信任的应用程序有助于避免 Kaspersky Industrial CyberSecurity for Nodes 与其他应用程序之间的兼容性问题（例如，Kaspersky Industrial CyberSecurity for Nodes 和另一个反病毒应用程序对第三方计算机的网络流量进行双重扫描的问题）。

同时，受信任应用程序的可执行文件和进程仍然会扫描病毒和其他恶意软件。您可以通过扫描排除项将应用程序从 Kaspersky Industrial CyberSecurity for Nodes 扫描中完全排除。

Kaspersky Industrial CyberSecurity for Nodes 不支持包含超过 5000 个对象的受信任应用程序列表。

如何添加应用程序到 Kaspersky Security Center 管理控制台中的受信任列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**补充**”。
4. 在“**受信任区域**”块中单击“**设置**”按钮。

5. 在打开的窗口中，选择“**受信任应用程序**”选项卡。

   这将打开包含受信任应用程序列表的窗口。

6. 如果您想要跳过受保护设备上安装的备份工具对文件读取操作执行的扫描，请选择“**不检查文件备份操作**”复选框。

7. 如果要为公司内的所有计算机创建受信任应用程序的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的受信任应用程序列表。如果启用继承时合并值，则将合并列表。父策略中的受信任应用程序以只读视图的形式显示在子策略中。无法更改或删除父策略的受信任应用程序

8. 如果您要让用户创建受信任应用程序本地列表，选择**允许编辑本地受信任应用程序**复选框。这样，除了策略中生成的受信任应用程序常规列表，用户可以创建他们自己的受信任应用程序本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的受信任应用程序常规列表。此外，如果清除此复选框，Kaspersky Industrial CyberSecurity for Nodes 会在应用程序控制台中隐藏受信任应用程序的综合列表。

9. 选择“**不检查指定进程的文件活动**”复选框以跳过对受信任进程的文件操作的扫描。

10. 点击“**添加**”并选择一个操作：

    - “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
    - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的受信任应用程序添加到列表的根目录中。
    - “**将新排除项添加到所选类别**”。要将新的受信任的应用程序添加到特定类别，请选择一个类别。
    - “**从列表选择排除项**”。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义的受信任应用程序列表中添加应用程序。

11. 在打开的窗口中，选择“**使用磁盘上的完整进程路径将其视为受信任**”复选框并输入文件路径来确定该进程是否受信任。

    当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

    在 Kaspersky Security Center 控制台上生成受信任应用程序列表时，Kaspersky Industrial CyberSecurity for Nodes 不支持 `%userprofile%` 环境变量。要应用条目到所有用户账户，您可以使用 * 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。

12. 为受信任应用程序（参加下表）配置高级设置。

13. 单击“**确定**”。

    新的受信任的应用程序将被添加到列表。您可以随时使用对象旁边的复选框将应用程序从信任区域中排除。

14. 保存更改。

如何添加应用程序到 Kaspersky Security Center Web Console 中的受信任列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。
4. 选择**应用程序设置**选项卡。
5. 转到“**补充 → 受信任区域**”并点击“**配置**”按钮。
6. 在打开的窗口中，选择“**受信任应用程序**”选项卡。
7. 如果您想要跳过受保护设备上安装的备份工具对文件读取操作执行的扫描，请选择“**不检查文件备份操作**”复选框。
8. 如果要为公司内的所有计算机创建受信任应用程序的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的受信任应用程序列表。如果启用继承时合并值，则将合并列表。父策略中的受信任应用程序以只读视图的形式显示在子策略中。无法更改或删除父策略的受信任应用程序
9. 如果您要让用户创建受信任应用程序本地列表，选择**允许编辑本地受信任应用程序**复选框。这样，除了策略中生成的受信任应用程序常规列表，用户可以创建他们自己的受信任应用程序本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的受信任应用程序常规列表。此外，如果清除此复选框，Kaspersky Industrial CyberSecurity for Nodes 会在应用程序控制台中隐藏受信任应用程序的综合列表。
10. 选择“**不检查指定进程的文件活动**”复选框以跳过对受信任进程的文件操作的扫描。
11. 点击“**添加**”并选择一个操作：
    - “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
    - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的受信任应用程序添加到列表的根目录中。
    - “**将新排除项添加到所选类别**”。要将新的受信任的应用程序添加到特定类别，请选择一个类别。
    - “**从列表选择排除项**”。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义的受信任应用程序列表中添加应用程序。
12. 在打开的窗口中，选择“**使用磁盘上的完整进程路径将其视为受信任**”复选框并输入文件路径来确定该进程是否受信任。

    当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

    > 在 Kaspersky Security Center 控制台上生成受信任应用程序列表时，Kaspersky Industrial CyberSecurity for Nodes 不支持 `%userprofile%` 环境变量。要应用条目到所有用户账户，您可以使用 * 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。

13. 为受信任应用程序（参加下表）配置高级设置。

14. 单击“**OK**”。

    新的受信任的应用程序将被添加到列表。您可以随时使用“**操作**”列中的复选框将应用程序从信任区域中排除。

15. 保存更改。

如何添加应用程序到应用程序控制台中的受信任列表

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**受信任区域**”。

   “**配置信任区域设置**”窗口将打开。

2. 在“**排除项**”部分，点击“**受信任应用程序**”块旁边的“**设置**”按钮。

3. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
   - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的受信任应用程序添加到列表的根目录中。
   - “**将新排除项添加到所选类别**”。要将新的受信任的应用程序添加到特定类别，请选择一个类别。
   - “**从列表选择排除项**”。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义的受信任应用程序列表中添加应用程序。

4. 从列表中选择一个文件或输入受信任应用程序的可执行文件的路径。

   当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

   > Kaspersky Industrial CyberSecurity for Nodes 支持环境变量。同时，Kaspersky Industrial CyberSecurity for Nodes 在应用程序的本地界面中转换路径。换言之，如果您输入文件路径 `%userprofile%\Documents\File.exe`，`C:\Users\Fred123\Documents\File.exe` 记录被添加到用户 Fred123 的应用程序的本地界面中。相应地，Kaspersky Industrial CyberSecurity for Nodes 对其他用户忽略 `File.exe` 受信任程序。要应用条目到所有用户账户，您可以使用 `*` 字符（例如，`C:\Users\*\Documents\File.exe`）。

   > 无论何时添加新的环境变量，都需要重新启动应用程序。

5. 为受信任应用程序（参加下表）配置高级设置。

6. 单击“**确定**”。

   新的受信任的应用程序将被添加到列表。您可以随时使用对象名称旁边的复选框将应用程序从信任区域中排除。

7. 保存更改。

受信任应用程序设置

参数	描述
使用磁盘上的完整进程路径来将它视为受信任	Kaspersky Industrial CyberSecurity for Nodes 使用文件的完整路径来确定进程是否受信任。
使用进程文件哈希来将它视为受信任	Kaspersky Industrial CyberSecurity for Nodes 使用选定的文件哈希来确定进程信任状态。如果清除该复选框，则不使用文件哈希来确定进程信任状态。
允许与应用程序界面交互	Kaspersky Industrial CyberSecurity for Nodes 阻止所有从远程计算机管理应用程序服务的尝试。如果选择该复选框，则允许远程访问应用程序通过 Kaspersky Industrial CyberSecurity for Nodes 界面管理 Kaspersky Industrial CyberSecurity for Nodes 设置。
不监控子程序活动	Kaspersky Industrial CyberSecurity for Nodes 将不监控被该应用程序启动的应用程序的文件活动或网络活动。您可以递归地应用排除。这样应用程序就不会监控整个子应用程序链的活动。
不继承父进程(应用程序)的限制	为父进程配置的限制将不被 Kaspersky Industrial CyberSecurity for Nodes 应用到子进程。父进程由配置了应用程序权限和应用程序网络规则的应用程序启动。
不扫描进程内存	Kaspersky Industrial CyberSecurity for Nodes 不扫描进程内存。

创建本地受信任区域

用户现在可以为特定计算机创建自己的本地受信任区域。这样，除了策略中的常规受信任域，用户可以创建他们自己的本地排除项和受信任应用程序列表。管理员可以在策略设置中允许或阻止使用本地排除项或本地受信任应用程序。为此，请使用策略“**受信任区域**”区域中的“**扫描排除项**”和“**受信任应用程序**”选项卡上的“**允许使用本地排除项**”和“**允许编辑本地受信任应用程序**”复选框a。

如果管理员允许创建本地受信任区域，则用户可以在应用程序控制台中添加自己的扫描排除项和受信任应用程序。同时，用户无权修改或删除策略中配置的受信任区域中的对象。如果需要为单台计算机添加排除项，管理员还可以在 Kaspersky Security Center 控制台中查看、添加、修改或删除列表项。

如果管理员在控制台中阻止受信任域的配置（“关闭锁”符号）并且本地扫描排除项和受信任应用程序被禁止，则 Kaspersky Industrial CyberSecurity for Nodes 会在应用程序控制台中隐藏扫描排除项和受信任应用程序列表。

如何添加对象到 Kaspersky Security Center 管理控制台中的本地受信任域

1. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
2. 在工作区中选择“**设备**”选项卡。
3. 双击以打开计算机属性窗口。
4. 在计算机属性窗口中，选择“**应用程序**”区域。
5. 在计算机上安装的卡巴斯基应用程序列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”并双击以打开应用程序属性。
6. 在应用程序设置中，选择“**补充 → 受信任区域**”并点击“**设置**”。
7. 在“**扫描排除项**”选项卡上，制作本地扫描排除项列表。

   创建本地扫描排除项的规则与常规排除项相同。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

8. 在“**受信任应用程序**”选项卡上，制作本地受信任的应用程序列表。这将打开包含本地受信任应用程序列表的窗口。

   添加应用程序到本地受信任应用程序列表的规则与将它们添加到常规列表的规则相同。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

9. 保存更改。

如何添加对象到 Kaspersky Security Center Web Console 中的本地受信任域

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 单击要允许用户执行阻止操作的计算机的名称。
3. 选择**应用程序**选项卡。
4. 单击“**Kaspersky Industrial CyberSecurity for Nodes**”。

   这将打开本地应用程序设置。
5. 选择**应用程序设置**选项卡。
6. 在应用程序设置中，选择“**补充 → 受信任区域**”并点击“**配置**”。

   “**排除项和检测对象类型**”窗口将打开。
7. 在“**扫描排除项**”选项卡上，制作本地扫描排除项列表。

   创建本地排除项的规则与创建常规排除项的规则相同。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：
8. 在“**受信任应用程序**”选项卡上，制作本地受信任的应用程序列表。

   添加应用程序到本地受信任应用程序列表的规则与将它们添加到常规列表的规则相同。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：
9. 保存更改。

如何在应用程序控制台中创建本地扫描排除项

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**受信任区域**”。

   “**配置信任区域设置**”窗口将打开。
2. 在“**扫描排除项和受信任应用程序**”部分，点击“**本地扫描排除项**”块旁边的“**设置**”按钮。

   如果管理员在 Kaspersky Security Center 管理控制台中阻止扫描排除项的配置（“关闭锁”符号）并且本地扫描排除项被禁止（“**允许使用本地排除项**”复选框被清除），则 Kaspersky Industrial CyberSecurity for Nodes 会在应用程序控制台中隐藏扫描排除项的列表。

3. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。
   - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的扫描排除项添加到列表的根目录中。
   - “**将新排除项添加到所选类别**”。要将新的扫描排除项添加到特定类别，请选择一个类别。
   - “**从列表选择排除项**”。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义扫描排除项列表中添加排除项。

4. 选择“**新建排除项**”打开“**扫描排除项**”窗口。

5. 要从扫描中排除某个文件或文件夹，请选择“**文件或文件夹**”复选框。点击“**选择文件或文件夹。**”链接打开一个窗口，然后在该窗口中通过单击“**浏览**”选择一个文件或文件夹。

   您也可以手动输入路径。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

   - `*`（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。
   - 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。
   - `?`（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。

     您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

6. 要从扫描中排除预定义区域，请选择“**预定义范围**”复选框。点击“**选择预定义范围**”链接打开一个窗口，并在该窗口中选择受保护设备上的标准范围之一。

7. 要从扫描中排除特定对象，请选择“**检测对象类型**”复选框。点击“**输入对象名称**”链接，点击“**添加**”按钮，在显示的窗口中，根据卡巴斯基百科全书分类（例如，`Email-Worm`、`Rootkit` 或者 `RemoteAdmin`）输入对象类型名称。

   您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Industrial CyberSecurity for Nodes 从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

8. 要从扫描中排除单个文件，请选择“**对象哈希**”复选框。点击“**输入对象哈希值**”链接打开一个窗口，并在该窗口中输入文件哈希。

   如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

9. 在**规则使用范围**块，选择您要应用扫描排除项的组件。

10. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

11. 保存更改以将排除项添加到列表中。您可以随时使用对象旁边的复选框禁用排除项。

如何在应用程序控制台中添加应用程序到本地受信任应用程序列表

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**受信任区域**”。

   “**配置信任区域设置**”窗口将打开。

2. 在“**排除项**”部分，点击“**本地受信任应用程序**”块旁边的“**设置**”按钮。

   如果管理员在 Kaspersky Security Center 管理控制台中阻止受信任应用程序的配置（“关闭锁”符号）并且本地受信任应用程序被禁止（“**允许编辑本地受信任应用程序**”复选框被清除），则 Kaspersky Industrial CyberSecurity for Nodes 会在应用程序控制台中隐藏受信任应用程序的综合列表。

3. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
   - “**新建排除项**”。Kaspersky Industrial CyberSecurity for Nodes 会将新的受信任应用程序添加到列表的根目录中。
   - “**将新排除项添加到所选类别**”。要将新的受信任的应用程序添加到特定类别，请选择一个类别。
   - “**从列表选择排除项**”。要快速配置 Kaspersky Industrial CyberSecurity for Nodes，您可以从预定义的受信任应用程序列表中添加应用程序。

4. 选择“**新建排除项**”打开“**扫描排除项**”窗口。

5. 选择“**使用磁盘上的完整进程路径将其视为受信任**”复选框并输入受信任应用程序的可执行文件的路径。

   当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：

   Kaspersky Industrial CyberSecurity for Nodes 支持环境变量。同时，Kaspersky Industrial CyberSecurity for Nodes 在应用程序的本地界面中转换路径。换言之，如果您输入文件路径 `%userprofile%\Documents\File.exe`，`C:\Users\Fred123\Documents\File.exe` 记录被添加到用户 Fred123 的应用程序的本地界面中。相应地，Kaspersky Industrial CyberSecurity for Nodes 对其他用户忽略 `File.exe` 受信任程序。要应用条目到所有用户账户，您可以使用 `*` 字符（例如，`C:\Users\*\Documents\File.exe`）。

   无论何时添加新的环境变量，都需要重新启动应用程序。

6. 在受信任应用程序属性窗口，配置高级设置。

7. 保存更改以将排除项添加到列表中。

导出和导入受信任域

*受信任区域*是由系统管理员配置的、Kaspersky Industrial CyberSecurity for Nodes 在活动期间不予监控的对象和应用程序的列表。受信任区域由以下列表组成："*扫描排除项*"和"*受信任应用程序*"。然后可以修改文件，例如，添加大量相同类型的排除项。还可以使用导出/导入功能备份排除列表和受信任应用程序列表或将列表迁移到其他服务器。

应用程序使用 XML 格式导出和导入排除项和*受信任应用程序列表*：

Kaspersky Industrial CyberSecurity for Nodes 不支持包含超过 5000 个对象的排除列表和受信任应用程序列表。

如何在 Kaspersky Security Center 管理控制台中导出和导入受信任区域

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择"**补充 → 受信任区域**"并点击"**设置**"。
4. 要导出规则列表：
   a. 选择**扫描排除项**选项卡。
   b. 选择您要导出的排除项。
      如果您未选择任何排除项，Kaspersky Industrial CyberSecurity for Nodes 将导出所有排除项。
   c. 单击文件夹图标并从下拉列表中选择"**导出**"。
      在打开的窗口中，指定您要将排除项列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
5. 要导出受信任应用程序列表：
   a. 选择**受信任应用程序**选项卡。
      这将打开包含受信任应用程序列表的窗口。
   b. 选择您要导出的受信任应用程序。
      如果您未选择任何受信任应用程序，Kaspersky Industrial CyberSecurity for Nodes 将导出所有受信任应用程序。
   c. 单击文件夹图标并从下拉列表中选择"**导出**"。
   d. 在打开的窗口中，输入您要将受信任应用程序列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

e. 保存文件。

Kaspersky Industrial CyberSecurity for Nodes 会将列表导出到 XML 文件。

6. 要导入排除项列表：

a. 选择**扫描排除项**选项卡。

这将打开包含排除项列表的窗口。

b. 单击文件夹图标并从下拉列表中选择“**导入**”。

c. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。

d. 打开文件。

如果计算机已经具有排除项的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

7. 要导入受信任应用程序列表：

a. 选择**受信任应用程序**选项卡。

这将打开包含受信任应用程序列表的窗口。

b. 单击“**导入**”。

c. 在打开的窗口中，选择要从中导入受信任应用程序列表的 XML 文件。

d. 打开文件。

如果计算机已经具有受信任应用程序的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

8. 保存更改。

如何在 Kaspersky Security Center Web Console 中导出和导入受信任区域

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。
4. 转到“**补充 → 受信任区域**”并点击“**配置**”按钮。
5. 要导出规则列表：

a. 在“**扫描排除项和受信任应用程序**”选项卡上，选择您要导出的排除项。

b. 点击三个点并选择“**导出**”。

c. 确认您仅想导出所选排除项，或导出整个排除项列表。

Kaspersky Industrial CyberSecurity for Nodes 会将列表导出到 XML 文件。

6. 要导出受信任应用程序列表：

   a. 在“**扫描排除项和受信任应用程序**”选项卡上，选择您要导出的应用程序。

   b. 点击三个点并选择“**导出**”。

   c. 确认您仅想导出所选应用程序，或导出整个列表。

   Kaspersky Industrial CyberSecurity for Nodes 会将列表导出到 XML 文件。

7. 要导入排除项列表：

   a. 在“**扫描排除项和受信任应用程序**”选项卡上，如果您想从在应用程序版本 4.0 版本或更早版本中创建的 XML 文件导入排除列表，点击“**从以前版本导入**”。

   如果您要从在 4.5 版本或更高版本中创建的 XML 文件导入规则，请单击“**导入**”。

   b. 如果计算机已经具有排除项的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

   c. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。

   d. 单击“**导入**”。

8. 要导入受信任应用程序列表：

   a. 在“**扫描排除项和受信任应用程序**”选项卡上，如果您想从在应用程序版本 4.0 版本或更早版本中创建的 XML 文件导入受信任的应用程序列表，点击“**从以前版本导入**”。

   如果您要从在 4.5 版本或更高版本中创建的 XML 文件导入受信任的应用程序，请单击“**导入**”。

   b. 如果计算机已经具有受信任应用程序的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

   c. 在打开的窗口中，选择要从中导入受信任应用程序列表的 XML 文件。

   d. 单击“**导入**”。

9. 保存更改。

如何在应用程序控制台中导出和导入受信任区域

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**受信任区域**”。

   “**配置信任区域设置**”窗口将打开。

2. 要导出受信任应用程序排除项列表：

   a. 在“**排除项**”部分，点击“**扫描排除项**”或者“**受信任应用程序**”块旁边的“**设置**”按钮。

   b. 选择您要导出的排除项或受信任应用程序。

   c. 单击文件夹图标并选择“**导出**”。

d. 在打开的窗口中，输入您要将排除项或受信任应用程序列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

e. 保存文件。

Kaspersky Industrial CyberSecurity for Nodes 会将列表导出到 XML 文件。

3. 要导入排除项或受信任应用程序列表：

a. 在“**排除项**”部分，点击“**扫描排除项**”或者“**受信任应用程序**”块旁边的“**设置**”按钮。

b. 选择您要导入的排除项或受信任应用程序。

c. 单击文件夹图标并选择“**导出**”。

d. 在打开的窗口中，选择要从中导入排除项或受信任应用程序列表的 XML 文件。

e. 打开文件。

如果计算机已经具有排除项的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

4. 保存更改。

使用受信任的系统证书存储

使用系统证书存储允许您从病毒扫描中排除由受信任数字签名签发的应用程序。Kaspersky Industrial CyberSecurity for Nodes 自动分配此类应用程序到*受信任*组。

若要使用受信任的系统证书存储：

如何在 Kaspersky Security Center 管理控制台中配置受信任系统证书存储的使用

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**补充 → 受信任区域**”并点击“**设置**”。
4. 选择**受信任的系统证书存储**选项卡。
5. 选择“**使用受信任的系统证书存储**”复选框，然后在下拉列表中选择您希望 Kaspersky Industrial CyberSecurity for Nodes 视为受信任的系统存储。
6. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置受信任系统证书存储的使用

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**补充** → **受信任区域**”并点击“**配置**”按钮。
5. 选择**受信任的系统证书存储**选项卡。
6. 选择“**使用受信任的系统证书存储**”复选框，然后在下拉列表中选择您希望 Kaspersky Industrial CyberSecurity for Nodes 视为受信任的系统存储。
7. 保存更改。

如何在应用程序控制台中配置受信任系统证书存储的使用

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并从节点的上下文菜单中选择“**受信任区域**”。
   “**配置信任区域设置**”窗口将打开。
2. 在“**受信任的系统证书存储**”下，选择“**使用受信任的系统证书存储**”复选框，然后在下拉列表中选择您希望 Kaspersky Industrial CyberSecurity for Nodes 视为受信任的系统存储。
3. 保存更改。

关于工业软件排除项配置文件

排除项配置文件是一组 XML 格式的排除规则，旨在将特定工业应用程序的进程和文件添加到受信任进程和排除项列表中，以及配置应用程序启动控制规则。

下表列出了所有可用的工业应用程序排除项配置文件。

每个排除项配置文件的规则都假定工业应用程序安装在默认文件夹中。如果工业应用程序安装在默认文件夹以外的文件夹中，则在安装 Kaspersky Industrial CyberSecurity for Nodes 后必须手动调整相应排除项配置文件的规则。

工业软件排除项配置文件

排除项配置文件	受信任区域配置规则	应用程序启动控制配置规则
ABB MicroSCADA	是	否
ABB 800xA DCS	是	否
Bently Nevada System 1	是	是

排除项配置文件	受信任区域配置规则	应用程序启动控制配置规则
Bosch Building Integration System	是	否
Bosch Rexroth MMS 4.0	是	否
BRIC	是	否
Consen SC9000	是	否
Emerson DeltaV	是	是
Emerson OpenEnterprise	是	是
Emerson Ovation	是	否
Emerson PipelineManager	是	否
GE Cimplicity	是	否
Honeywell Experion PKS	是	否
MasterSCADA4D	是	否
Mitsubishi MAPS	是	否
OMRON CX-Supervisor	是	否
PcVue Solutions 15	是	是
Rockwell Automation FactoryTalk View	是	否
Schneider Electric Citect SCADA	是	否
Schneider Electric Clear SCADA	是	是
Schneider Electric EcoStruxure Foxboro DCS	是	否
Schneider Electric Unity Pro	是	否
Siemens SIMATIC PCS 7 v8.2	是	否
Siemens SIMATIC PCS 7 v9.0	是	否
Siemens SIMATIC PCS 7 v9.1	是	是
Siemens SIMATIC WinCC OA	是	是
Siemens SIMATIC WinCC	是	否
Siemens SIMATIC STEP7	是	否
Siemens TIA Portal	是	否
Siemens DIGSI	是	否
Siemens SICAM PAS	是	否
Valmet DNA	是	是
Wonderware InTouch	是	否
Wonderware System Platform 2017	是	否
Yokogawa CENTUM VP	是	否
Yokogawa ProSafe-RS	是	否
Yokogawa FAST/TOOLS	是	否
Alpha.Platform	是	是
BAKC	是	是
GAUS	是	否
ISUB ARBITER	是	否
PK AstraRegul	是	否
NaftaProcess DCS	是	是
TEKON	是	否

排除项配置文件	受信任区域配置规则	应用程序启动控制配置规则
Tornado-N	是	是
CASCADE 3.18 Digital Platform	是	否
EKRA (EKRASMS, EKRASMS-SP)	是	是

要在安装 Kaspersky Industrial CyberSecurity for Nodes 期间应用工业软件排除项配置文件：

- 在安装向导的相应步骤中选择所需的排除项配置文件
- 输入命令行安装选项：`ADDEXCLUSION=<` 排除项配置文件名称 `1>;<` 排除项配置文件名称 `2>;...;<` 排除项配置文件名称 `n>`。

实时文件保护

在访问以下受保护设备对象时，Kaspersky Industrial CyberSecurity for Nodes 的“实时文件保护”组件会对这些对象进行扫描：

- 文件
- NTFS 交换数据流。
- 本地硬盘驱动器和外部设备上的主引导记录和引导扇区。
- Windows Server 2016 和 Windows Server 2019 容器文件。

当任何应用程序在受保护设备上写入或读取文件时，Kaspersky Industrial CyberSecurity for Nodes 会拦截此文件进行扫描以检测其是否存在威胁；如果检测到威胁，则执行默认操作或您指定的操作：尝试清除文件、移至隔离区或将其删除。在清除或删除前，Kaspersky Industrial CyberSecurity for Nodes 会将源文件的加密副本保存到备份文件夹。

Kaspersky Industrial CyberSecurity for Nodes 拦截在 Windows Server 2016 和 Windows Server 2019 容器中执行的文件操作。

*容器*是一个隔离的环境，应用程序可以在其中运行而无需与操作系统直接交互。如果容器位于组件保护范围内，Kaspersky Industrial CyberSecurity for Nodes 会扫描用户正在访问的容器文件以查找计算机威胁。当检测到威胁时，应用程序尝试对容器进行清除。如果清除成功，容器将继续工作。如果清除失败，则容器被关闭。

Kaspersky Industrial CyberSecurity for Nodes 还会检测在 Windows Subsystem for Linux® 下运行的进程是否存在恶意软件。对于此类进程，“实时文件保护”组件将应用当前配置定义的操作。

关于任务保护范围和安全设置

默认情况下，“实时文件保护”组件将保护设备文件系统中的所有对象。如果不需要对文件系统中的所有对象进行安全保护，或者您想从任务范围中排除任何对象，则可以限制保护范围。

在应用程序控制台中，保护范围以 Kaspersky Industrial CyberSecurity for Nodes 可以监控的设备文件资源列表的形式显示。

安全性设置

任务安全设置可以配置为保护范围中包括的所有节点或项的通用设置，或配置为设备文件资源列表中各个节点或项的不同设置。

为所选父节点配置的安全设置将自动应用到其所有子节点。父节点的安全设置不会应用到单独配置的子节点。

可以使用以下方法之一配置选定保护范围的设置：

- 选择三个预定义安全级别中的一个。
- 手动为文件资源列表中的选定节点或项配置安全性设置（安全级别更改为“**自定义**”）。

预定义的保护范围

文件资源列表显示基于配置的 Microsoft Windows 安全设置拥有读取访问权限的节点。

Kaspersky Industrial CyberSecurity for Nodes 覆盖以下预定义保护范围：

- “**本地硬盘驱动器**”。Kaspersky Industrial CyberSecurity for Nodes 将保护设备硬盘驱动器上的文件。
- “**可移动驱动器**”。Kaspersky Industrial CyberSecurity for Nodes 将保护外部设备上的文件，如 CD 或可移动驱动器。您可以在保护范围中包含或排除所有可移动驱动器、单个磁盘、文件夹或文件。
- “**网络**”。Kaspersky Industrial CyberSecurity for Nodes 将保护设备上运行的应用程序写入到网络文件夹或从网络文件夹读取的文件。当其他受保护设备上的应用程序访问此类文件时，Kaspersky Industrial CyberSecurity for Nodes 不会保护此类文件。

默认情况下，您可以在范围列表中查看和配置预定义保护范围；还可以在列表形成期间在保护范围设置中向该列表添加预定义范围。

已连接的网络驱动器也不会显示在受保护设备的文件资源列表中。若要将网络驱动器上的对象包含在保护范围内，请按 UNC (Universal Naming Convention) 格式指定与该网络驱动器对应的文件夹的路径。

关于预定义安全级别

可以为受保护设备文件资源树或文件资源列表中的选定节点应用以下预定义安全级别之一：**最高性能**、**建议**、**最大保护**和**通知**。每个级别都包含其自有的预定义安全设置集合（请参见下表）。

最高性能

如果您的网络除了在受保护设备和工作站上使用 Kaspersky Industrial CyberSecurity for Nodes 外，还有其他受保护设备安全措施，例如防火墙和现有安全策略，则建议使用“**最高性能**”安全级别。

建议

“**建议**”安全级别确保保护与对设备的性能影响的最佳组合。Kaspersky 专家推荐此级别，因为其足以保护大多数公司网络上的设备。默认情况下，将设置“**建议**”安全级别。

最大保护

如果组织的网络有更高的设备安全要求，则推荐使用“**最大保护**”安全级别。

通知

如果企业网络中可能存在多台受感染的计算机，而阻止这些计算机可能会严重扰乱组织的运营，则推荐“**通知**”安全级别。

预设安全级别和对应的设置值

选项	安全级别			
最高性能	**建议**	**最大保护**	**通知**	
对象保护	按反病毒数据库中指定的扩展名列表扫描对象	按格式扫描对象	按格式扫描对象	按格式扫描对象
仅扫描新建和已修改的文件	已启用	已启用	已禁用	已启用
扫描复合文件	已禁用	扫描 Microsoft Office 格式的文件	扫描 Microsoft Office 格式的文件	扫描 Microsoft Office 格式的文件
对受感染对象和其他对象执行的操作	阻止访问并清除。清除失败则删除	阻止访问并执行卡巴斯基专家建议的操作	阻止访问并清除。清除失败则删除	通知
将操作应用于选定的对象类型	已禁用	已禁用	已禁用	已禁用
在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件	已禁用	已禁用	已启用	已禁用
系统关键对象是操作系统和 Kaspersky Industrial CyberSecurity for Nodes 运行所需的文件。这些文件无法删除。与此类对象关联的进程无法终止。				
在后台解压缩大于此值的复合文件(MB)				
如果扫描时间超过此值则停止(秒)	60 秒	60 秒	60 秒	60 秒
不扫描大于此值的复合对象(MB)	8 MB	8 MB	未设置	8 MB
使用 iSwift 技术	已启用	已启用	已启用	已启用
使用 iChecker 技术	已启用	已启用	已启用	已启用

“实时文件保护”组件默认扫描的文件扩展名

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 将扫描具有以下扩展名的文件：

- *386;*
- *acm;*
- *ade、adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*

- *bin;*
- *chm;*
- *cla、clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *.exe*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm、html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg、jpe;*

- *js、jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*

- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?。*

配置“实时文件保护”组件

默认情况下，“实时文件保护”组件使用下表描述的设置。您可以更改这些设置的值。

“实时文件保护”组件的默认设置

参数	默认值	描述
保护范围	整个受保护设备，虚拟驱动器除外。	使用此选项更改保护范围。
安全性设置	整个保护范围的常规设置；对应“**建议**”安全级别。	您可以对受保护设备文件资源列表或树中选定的节点执行以下操作： • 选择不同的预定义安全级别 • 手动更改安全性设置 您可以将选定节点的一组安全性设置保存为模板，以便在以后将其应用至其他节点。
对象保护模式	**智能模式**	使用此选项可以选择保护模式，即定义 Kaspersky Industrial CyberSecurity for Nodes 扫描对象所采用的访问尝试类型。
启发式分析	应用“**中度**”安全级别。	可以启用或禁用“启发式分析”并配置分析级别。
阻止显示恶意活动的会话访问网络共享资源	未应用。	使用此选项可以阻止当前会话并添加在被阻止主机存储部分中检测到恶意活动的主机 IP 或主机 LUID。
检测到活动感染时启动关键区域扫描	已应用。	在检测到活动感染时，Kaspersky Industrial CyberSecurity for Nodes 创建并启动“关键区域扫描”任务。
如果清除失败，则停止容器	已应用。	应用程序可能没有对检测到的对象进行读写的权限。在这种情况下，无法对检测到的对象清除或删除。如果选中该复选框，应用程序阻止检测到的对象并停止容器。如果清除该复选框，应用程序仅阻止检测到的对象。
不扫描在 Windows 容器中执行的文件操作	已应用。	如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。

如何在 Kaspersky Security Center 管理控制台中启用文件病毒扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 在“**实时文件保护设置**”区域中单击“**设置**”。
5. 选择**实时文件保护**复选框。
6. 在“**对象保护模式**”块，在“**常规**”选项卡上，选择“实时文件保护”操作模式：
   - “**智能模式**”。Kaspersky Industrial CyberSecurity for Nodes 自行选择扫描对象。对象在打开时被扫描，如果对象进行了修改，则在保存对象后重新扫描该对象。如果进程多次访问并修改对象，只有进程最后一次保存对象后，Kaspersky Industrial CyberSecurity for Nodes 才会重新扫描对象。
   - “**在访问和修改时**”。Kaspersky Industrial CyberSecurity for Nodes 在对象打开时扫描该对象，如果对象进行了修改，则在对象保存后重新扫描该对象。默认选中该选项。

- “**在访问时**”。Kaspersky Industrial CyberSecurity for Nodes 在对象打开以进行读取、执行或修改时扫描所有对象。
- “**运行时**”。仅在访问文件以执行该文件时，Kaspersky Industrial CyberSecurity for Nodes 才扫描该文件。

7. 清除或选中“**使用启发式分析**”复选框。
8. 选中或清除“**阻止显示恶意活动的会话访问网络共享资源**”复选框。
9. 清除或选中“**检测到活动感染时启动关键区域扫描**”复选框。

   如果选中此复选框，在检测到活动感染时，Kaspersky Industrial CyberSecurity for Nodes 将运行预定义的“*关键区域扫描*”任务。默认选中该复选框。
10. 指定扫描在 Windows 容器中执行的文件操作的设置。
11. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用文件病毒扫描

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 实时文件保护**”并点击“**配置**”按钮。
5. 选择**启用实时文件保护**复选框。
6. 在“**对象保护模式**”块，在“**常规**”选项卡上，选择“实时文件保护”操作模式：
   - “**智能模式**”。Kaspersky Industrial CyberSecurity for Nodes 自行选择扫描对象。对象在打开时被扫描，如果对象进行了修改，则在保存对象后重新扫描该对象。如果进程多次访问并修改对象，只有进程最后一次保存对象后，Kaspersky Industrial CyberSecurity for Nodes 才会重新扫描对象。
   - “**在访问和修改时**”。Kaspersky Industrial CyberSecurity for Nodes 在对象打开时扫描该对象，如果对象进行了修改，则在对象保存后重新扫描该对象。默认选中该选项。
   - “**在访问时**”。Kaspersky Industrial CyberSecurity for Nodes 在对象打开以进行读取、执行或修改时扫描所有对象。
   - “**运行时**”。仅在访问文件以执行该文件时，Kaspersky Industrial CyberSecurity for Nodes 才扫描该文件。
7. 清除或选中“**使用启发式分析**”复选框。
8. 选中或清除“**阻止显示恶意活动的网络会话访问网络共享资源**”复选框。

9. 清除或选中“**检测到活动感染时启动关键区域扫描**”复选框。

   如果选中此复选框，在检测到活动感染时，Kaspersky Industrial CyberSecurity for Nodes 将运行预定义的“*关键区域扫描*”任务。默认选中该复选框。

10. 指定扫描在 Windows 容器中执行的文件操作的设置。

11. 保存更改。

如何在应用程序控制台中启用文件病毒扫描

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**实时计算机保护**” → “**实时文件保护**”。

2. 在“**实时文件保护**”节点的结果窗格中，单击“**属性**”。

   “**属性: 实时文件保护**”窗口将打开。

3. 选择**实时文件保护**复选框。

4. 在“**对象保护模式**”块，在“**常规**”选项卡上，选择“实时文件保护”操作模式：

   - “**智能模式**”。Kaspersky Industrial CyberSecurity for Nodes 自行选择扫描对象。对象在打开时被扫描，如果对象进行了修改，则在保存对象后重新扫描该对象。如果进程多次访问并修改对象，只有进程最后一次保存对象后，Kaspersky Industrial CyberSecurity for Nodes 才会重新扫描对象。

   - “**在访问和修改时**”。Kaspersky Industrial CyberSecurity for Nodes 在对象打开时扫描该对象，如果对象进行了修改，则在对象保存后重新扫描该对象。默认选中该选项。

   - “**在访问时**”。Kaspersky Industrial CyberSecurity for Nodes 在对象打开以进行读取、执行或修改时扫描所有对象。

   - “**运行时**”。仅在访问文件以执行该文件时，Kaspersky Industrial CyberSecurity for Nodes 才扫描该文件。

5. 清除或选中“**使用启发式分析**”复选框。

6. 选中或清除“**阻止显示恶意活动的会话访问网络共享资源**”复选框。

7. 清除或选中“**检测到活动感染时启动关键区域扫描**”复选框。

   如果选中此复选框，在检测到活动感染时，Kaspersky Industrial CyberSecurity for Nodes 将运行预定义的“*关键区域扫描*”任务。默认选中该复选框。

8. 指定扫描在 Windows 容器中执行的文件操作的设置。

9. 保存更改。

配置“实时文件保护”组件的保护范围

默认情况下，“实时文件保护”组件对整个保护范围使用通用安全设置。这些设置对应于“**建议**”预定义安全级别。

可以通过将安全性设置配置为用于整个保护范围的通用设置，或配置为设备文件资源列表的单个项目的不同设置，来修改安全性设置的默认值。

如果同一对象包含在多个保护范围条目中，并且这些条目具有不同的安全级别，则列表中的最后一条规则具有优先级。例如，考虑包含两个条目的保护范围：“**所有硬盘驱动器**”（安全级别“**通知**”）和“`*\Users\*\Downloads\*`”（安全级别“**自定义**”）。应用程序根据“通知”级别扫描硬盘驱动器，但“`Downloads`”文件夹除外。应用程序根据手动指定的设置扫描“`Downloads`”文件夹，因为该条目是保护范围列表中的最后一个条目。

要手动配置选定节点的安全设置：

如何在 Kaspersky Security Center 管理控制台中配置“实时文件保护”的保护范围

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 在“**实时文件保护**”区域中单击“**设置**”。
5. 选择**保护范围**选项卡。
6. 在受保护设备的文件资源列表中，选择要设置预定义安全级别的项目。
7. 如果文件共享不在列表中，请手动添加：
   a. 单击“**添加**”。
   b. 使用文件夹树指定所需对象的路径，或在“**对象**”字段中输入路径。
      如果必要的话，使用特殊字符输入对象路径掩码：
      - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和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。
      - 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。
      - `?`（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。

      计算机的文件资源列表中的“**此 PC**”对象包括以下对象：**所有硬盘驱动器**、**所有网络驱动器** 和 **所有可移动驱动器**。
   c. 单击“**确定**”。
8. 确保选定的文件资源包含在保护范围中。

9. 通过点击“**配置**”为所选保护范围指定预定义安全级别。默认情况下，相同的安全设置应用于整个保护范围。这些设置对应于“**建议**”预定义安全级别。您还可以编辑默认安全设置。

10. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置“实时文件保护”的保护范围

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**实时计算机保护 → 实时文件保护**”并点击“**配置**”按钮。

5. 选择**保护范围**选项卡。

6. 在受保护设备的文件资源列表中，选择要设置预定义安全级别的项目。

7. 如果文件共享不在列表中，请手动添加：

   a. 单击“**添加**”。

   b. 在“**对象类型**”列表中，选择一个选项：
   对于“**掩码**”选项，使用特殊字符输入对象路径掩码：

   - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和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。

   - 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。

   - `?`（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。

   计算机的文件资源列表中的“**此 PC**”对象包括以下对象：**所有硬盘驱动器**、**所有网络驱动器** 和 **所有可移动驱动器**。

   c. 单击“**确定**”。

8. 使用列表项旁边的切换开关确保所选的文件资源包含在保护范围内。

9. 通过点击“**编辑**”为所选保护范围指定预定义安全级别。默认情况下，相同的安全设置应用于整个保护范围。这些设置对应于“**建议**”预定义安全级别。您还可以编辑默认安全设置。

10. 保存更改。

如何在应用程序控制台中配置"实时文件保护"的保护范围

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择"**实时计算机保护**" → "**实时文件保护**"。
2. 在"**实时文件保护**"节点的结果窗格中，单击"**配置保护范围**"。
   "**属性: 实时文件保护**"窗口将打开。
3. 在受保护设备的文件资源列表中，选择要设置预定义安全级别的项目。
4. 如果文件共享不在列表中，请手动添加：
   a. 单击"**添加**"。
   b. 使用文件夹树指定所需对象的路径，或在"**对象**"字段中输入路径。
      如果必要的话，使用特殊字符输入对象路径掩码：
      - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和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。
      - 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。
      - `?`（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。

      计算机的文件资源列表中的"**此 PC**"对象包括以下对象：**所有硬盘驱动器**、**所有网络驱动器** 和 **所有可移动驱动器**。
   c. 单击"**确定**"。
5. 确保选定的文件资源包含在保护范围中。
6. 通过点击"**配置**"为所选保护范围指定预定义安全级别。默认情况下，相同的安全设置应用于整个保护范围。这些设置对应于"**建议**"预定义安全级别。您还可以编辑默认安全设置。
7. 保存更改。

手动配置安全性设置

默认情况下，实时计算机保护任务对整个保护范围使用通用安全设置。这些设置对应于"**建议**"预定义安全级别。

可以通过将安全性设置配置为用于整个保护范围的常规设置，或配置为设备文件资源列表或树中节点的单个项目的不同设置，来修改安全性设置的默认值。

在使用受保护设备文件资源树时，为所选父节点配置的安全性设置将自动应用于所有子节点。父节点的安全设置不会应用到单独配置的子节点。

如何在 Kaspersky Security Center 管理控制台中手动配置安全设置

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 在“**实时文件保护**”区域中单击“**设置**”。
5. 在“**实时文件保护**”窗口，转到“**保护范围**”选项卡。
6. 选择要配置其安全设置的资源。
7. 单击“**配置**”。
8. 在打开的窗口中，选择所需安全级别并单击“**设置**”。
9. 在“**常规**”选项卡上，指定以下设置：
   - 应纳入保护范围的对象：
     - **所有对象**
     - **按格式扫描对象**
     - **按反病毒数据库中指定的扩展名列表扫描的对象**
   - 在“**优化**”块中，选中或清除“**仅扫描新建和已修改的文件**”复选框。
   - 在“**扫描复合文件**”部分中，指定要包含在扫描范围内的复合对象：
     - **扫描压缩包**
     - **扫描分发包**
     - **扫描 Microsoft Office 格式文件**
     - **扫描电子邮件格式文件**
10. 在“**操作**”选项卡上，指定以下设置：
    - 选择要对受感染的对象和其他检测到的对象执行的操作：
      - **通知**
      - **阻止**
      - **运行其他操作**

从下拉列表中选择操作：

- **清除**
- **清除。清除失败则删除**
- **删除**
- **建议**

- 根据检测的对象类型配置要对对象执行的操作：

  a. 清除或选中“**将操作应用于选定的对象类型**”复选框。

  b. 点击“**设置**”并选择要检测的对象类型。

- 配置对不可修改的复合文件的操作：清除或选择“**在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件**”复选框。

11. 在“**性能**”选项卡上，指定以下设置：

- **在后台解压缩大于此值的复合文件 (MB)**
- **如果扫描时间超过此值则停止(秒)**
- **不扫描大于此值的复合对象(MB)**
- **使用 iSwift 技术**
- **使用 iChecker 技术**

12. 保存新的安全设置。

如何在 Kaspersky Security Center Web Console 中手动配置安全设置

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 实时文件保护**”并点击“**配置**”按钮。
5. 选择**保护范围**选项卡。
6. 执行下列操作之一：

- 点击“**添加**”按钮添加新规则并为其指定安全设置。
- 选择一个现有规则，然后单击“**编辑**”按钮。

“**编辑范围**”窗口将打开。

7. 将切换开关设置为“**活动**”。
8. 选择一个安全级别并根据需要指定安全设置。
9. 在“**对象保护模式**”部分中，指定要包含在保护范围内的对象类型：
   - **所有对象**
   - **按格式扫描对象**
   - **按反病毒数据库中指定的扩展名列表扫描的对象**
10. 在“**优化**”部分中，选中或清除“**仅保护新建和已修改的文件**”复选框。
11. 在“**复合对象保护**”部分中，指定要包含在扫描范围内的复合对象：
    - **扫描压缩文件**
    - **扫描分发包**
    - **扫描 Microsoft Office 格式文件**
    - **扫描电子邮件格式文件**
12. 选择要对受感染的对象和其他检测到的对象执行的操作：
    - **通知**
    - **阻止**
    - **运行其他操作**
      从下拉列表中选择操作：
      - **清除**
      - **清除；如果清除失败则删除**
      - **删除**
      - **建议**
13. 根据检测的对象类型配置要对对象执行的操作：
    a. 清除或选中“**将操作应用于选定的对象类型**”复选框。
    b. 如果已选中复选框，请单击“**设置**”并选择要检测的对象类型。
14. 配置对不可修改的复合文件的操作：清除或选择“**在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件**”复选框。
15. 在“**优化**”部分中，配置以下设置：
    - **在后台解压复合文件**
    - **如果扫描时间超过此值则停止(秒)**

- **不扫描大于此值的复合对象(MB)**
- **使用 iSwift 技术**
- **使用 iChecker 技术**

16. 保存新的安全设置。

如何在应用程序控制台中手动配置安全设置

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**实时计算机保护**” → “**实时文件保护**”。
2. 在“**实时文件保护**”节点的结果窗格中，单击“**配置保护范围**”。
   “**属性: 实时文件保护**”窗口将打开。
3. 选择要配置其安全设置的资源。
4. 单击“**配置**”。
5. 在打开的窗口中，选择所需安全级别并单击“**设置**”。
6. 在“**常规**”选项卡上，指定以下设置：
   - 应纳入保护范围的对象：
     - “**所有对象**”。Kaspersky Industrial CyberSecurity for Nodes 扫描所有对象。
     - “**按格式扫描对象**”。Kaspersky Industrial CyberSecurity for Nodes 仅根据文件格式扫描可感染的对象。Kaspersky 编制了该格式列表。它包含在 Kaspersky Industrial CyberSecurity for Nodes 数据库中。
     - “**按反病毒数据库中指定的扩展名列表扫描的对象**”。Kaspersky Industrial CyberSecurity for Nodes 仅根据文件扩展名扫描可感染的对象。Kaspersky 编制了该扩展名列表。它包含在 Kaspersky Industrial CyberSecurity for Nodes 数据库中。
   - 在“**优化**”块中，选中或清除“**仅保护新建和已修改的文件**”复选框。
   - 在“**扫描复合文件**”部分中，指定要包含在扫描范围内的复合对象：
     - “**扫描压缩包**”。扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他压缩包。应用程序不仅按扩展名扫描压缩包，还按格式扫描压缩包。当检查存档时，应用程序执行递归解包。这允许检测多级存档（存档中的存档）中的威胁。
     - “**扫描分发包**”。该复选框用于启用/禁用对第三方分发包的扫描。
     - “**扫描 Microsoft Office 格式文件**”。扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。Kaspersky Industrial CyberSecurity for Nodes 扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。
     - “**扫描电子邮件格式文件**”。

7. 在“**操作**”选项卡上，指定以下设置：

- 选择要对受感染的对象和其他检测到的对象执行的操作：
  - **通知**。
  - **阻止**。
  - “**运行其他操作**”。
    从下拉列表中选择操作：
    - **清除**
    - **清除。清除失败则删除**
    - **删除**
    - **建议**
- 根据检测的对象类型配置要对对象执行的操作：
  a. 清除或选中“**将操作应用于选定的对象类型**”复选框。
  b. 点击“**设置**”并选择要检测的对象类型。
- 配置对不可修改的复合文件的操作：清除或选择“**在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件**”复选框。

8. 在“**性能**”选项卡上，指定以下设置：

- **在后台解压缩大于此值的复合文件 (MB)**
- **如果扫描时间超过此值则停止(秒)**
- **不扫描大于此值的复合对象(MB)**
- **使用 iSwift 技术**
- **使用 iChecker 技术**

9. 保存新的安全设置。

容器扫描

*容器*是一个隔离的环境，应用程序可以在其中运行而无需与操作系统直接交互。使用容器存在以下风险：

- 黑客可能能够利用容器化漏洞来破坏容器内的应用程序。
- 黑客可能会利用容器环境的不安全配置来获取对计算机上的数据的未经授权的访问或破坏系统的完整性。

- 成功攻击容器可以让黑客获得计算机上的数据。
- 黑客可能利用网络漏洞来拦截网络流量。

Kaspersky Industrial CyberSecurity for Nodes 是一个用于检测容器内部恶意活动的外部工具。这可以维持容器的性能并防止与容器内的其他应用程序发生冲突。不支持在容器内安装 Kaspersky Industrial CyberSecurity for Nodes。

除了提供容器安全之外，Kaspersky Industrial CyberSecurity for Nodes 还允许使用应用程序启动控制管理容器内的应用程序。容器的应用程序启动控制配置方式与计算机上安装的应用程序的配置方式相同。系统完整性监控还支持容器。

容器要求

- 该容器必须是 Docker 容器。不支持其他容器化工具。
- 容器必须以进程隔离模式运行。不支持 Hyper-V 隔离模式。
- 容器必须放置在 Windows Server 2016、2019 或 2022 服务器上（Docker Host）。
- 容器必须包含 Windows 映像 (Docker Image）。不支持 Windows 10 和 11。不支持 Linux 镜像。
- 扫描在 WSL2 中运行的容器 – Windows Subsystem for Linux v2（Docker Wine) 模式不受支持。

检测到威胁后的操作

如果在容器内检测到威胁，该应用程序将应用为“实时文件保护”组件选择的操作。容器扫描有附加设置（请参阅下面的说明）。如果检测到威胁，应用程序会阻止恶意的活动并执行选定的操作（例如，尝试对对象清除）。如果 Kaspersky Industrial CyberSecurity for Nodes 无法对检测到的对象清除，则可以停止该容器。默认情况下，启用容器停止。

如何在 Kaspersky Security Center 管理控制台中配置容器扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 在“**实时文件保护**”区域中单击“**设置**”。
5. 在“**扫描在 Windows 容器中执行的文件操作**”块，配置容器扫描设置：
   - “**如果清除失败，则停止容器**”。应用程序可能没有对检测到的对象进行读写的权限。在这种情况下，无法对检测到的对象清除或删除。如果选中该复选框，应用程序阻止检测到的对象并停止容器。如果清除该复选框，应用程序仅阻止检测到的对象。
   - “**不扫描在 Windows 容器中执行的文件操作**”。如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。
6. 保存新的安全设置。

如何在 Kaspersky Security Center Web Console 中配置容器扫描

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 实时文件保护**”并点击“**配置**”按钮。
5. 在“**扫描在 Windows 容器中执行的文件操作**”块，配置容器扫描设置：
   - “**如果清除失败，则停止容器**”。应用程序可能没有对检测到的对象进行读写的权限。在这种情况下，无法对检测到的对象清除或删除。如果选中该复选框，应用程序阻止检测到的对象并停止容器。如果清除该复选框，应用程序仅阻止检测到的对象。
   - “**不扫描在 Windows 容器中执行的文件操作**”。如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。
6. 保存新的安全设置。

如何在应用程序控制台中配置容器扫描

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**实时计算机保护**” → “**实时文件保护**”。
2. 在“**实时文件保护**”节点的结果窗格中，单击“**属性**”。
   “**属性: 实时文件保护**”窗口将打开。
3. 在“**扫描在 Windows 容器中执行的文件操作**”块，配置容器扫描设置：
   - “**如果清除失败，则停止容器**”。应用程序可能没有对检测到的对象进行读写的权限。在这种情况下，无法对检测到的对象清除或删除。如果选中该复选框，应用程序阻止检测到的对象并停止容器。如果清除该复选框，应用程序仅阻止检测到的对象。
   - “**不扫描在 Windows 容器中执行的文件操作**”。如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。
4. 保存更改。

KSN 使用

为了更有效地保护您的计算机，Kaspersky Industrial CyberSecurity for Nodes 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。

KSN 功能可能无法在美国的应用程序中使用。

卡巴斯基安全网络 (KSN) 是一个云服务的基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件信誉、网页资源和软件的相关信息。使用卡巴斯基安全网络的数据可确保 Kaspersky Industrial CyberSecurity for Nodes 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 服务将为 Kaspersky Industrial CyberSecurity for Nodes 提供有关所扫描文件的类别和信誉的信息，以及有关所扫描网址的信誉的信息。

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 期间生成的卡巴斯基统计信息的发送详情，以及有关此类信息的存储和销毁，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 Industrial CyberSecurity for Nodes 支持以下用于使用卡巴斯基信誉数据库的基础设施解决方案：

- *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 Industrial CyberSecurity for Nodes 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策略限制将任何数据传输到国家/地区外部或公司 LAN 外部。

启用卡巴斯基安全网络的使用

如何在 Kaspersky Security Center 管理控制台中启用卡巴斯基安全网络的使用

1. 在卡巴斯基安全网络管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的 Kaspersky Industrial CyberSecurity for Nodes 策略并双击以打开策略属性。
3. 这将打开一个窗口；在该窗口中，在部分列表中，选择“**实时计算机保护 → KSN 使用**”。

4. 单击“**设置**”。

5. 选择“**卡巴斯基安全网络**”复选框启用组件。

   如果您启用了 KSN，Kaspersky Industrial CyberSecurity for Nodes 将显示卡巴斯基安全网络声明。如果您同意，请阅读并接受卡巴斯基安全网络 (KSN) 声明使用条款。

   默认情况下， Kaspersky Industrial CyberSecurity for Nodes 使用卡巴斯基安全网络的扩展模式。扩展卡巴斯基安全网络模式是 Kaspersky Industrial CyberSecurity for Nodes 向卡巴斯基发送附加数据的一种模式。

6. 如有必要，清空“**启用扩展 KSN 模式**”复选框。

7. 保存更改。

如果启用卡巴斯基安全网络，Kaspersky Industrial CyberSecurity for Nodes 使用从卡巴斯基安全网络接收的文件、Web 资源和应用程序的信誉信息。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中启用卡巴斯基安全网络的使用

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。

2. 选择“**卡巴斯基安全网络**”子节点。

3. 在主应用程序窗口中，单击“**属性**”。

4. 选择“**卡巴斯基安全网络**”复选框启用组件。

   如果您启用了 KSN，Kaspersky Industrial CyberSecurity for Nodes 将显示卡巴斯基安全网络声明。如果您同意，请阅读并接受卡巴斯基安全网络 (KSN) 声明使用条款。

   默认情况下， Kaspersky Industrial CyberSecurity for Nodes 使用卡巴斯基安全网络的扩展模式。扩展卡巴斯基安全网络模式是 Kaspersky Industrial CyberSecurity for Nodes 向卡巴斯基发送附加数据的一种模式。

5. 如有必要，清空“**启用扩展 KSN 模式**”复选框。

6. 保存更改。

   如果启用卡巴斯基安全网络，Kaspersky Industrial CyberSecurity for Nodes 使用从卡巴斯基安全网络接收的文件、Web 资源和应用程序的信誉信息。

如何在 Kaspersky Security Center Web Console 中启用卡巴斯基安全网络的使用

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**实时计算机保护 → KSN 使用**”部分，然后单击“**配置**”按钮。

5. 在显示的窗口中，选择“**启用卡巴斯基安全网络**”复选框来启用该组件。

   如果您启用了 KSN，Kaspersky Industrial CyberSecurity for Nodes 将显示卡巴斯基安全网络声明。如果您同意，请接受卡巴斯基安全网络使用条款。

   默认情况下， Kaspersky Industrial CyberSecurity for Nodes 使用卡巴斯基安全网络的扩展模式。扩展卡巴斯基安全网络模式是 Kaspersky Industrial CyberSecurity for Nodes 向卡巴斯基发送附加数据的一种模式。

6. 如有必要，清空“**启用扩展 KSN 模式**”复选框。

7. 保存更改。

结果，如果启用卡巴斯基安全网络，Kaspersky Industrial CyberSecurity for Nodes 使用从卡巴斯基安全网络接收的文件、Web 资源和应用程序的信誉信息。

卡巴斯基安全网络使用统计信息

当“*KSN 使用*”任务运行时，您可以查看有关 Kaspersky Industrial CyberSecurity for Nodes 从任务开始到现在处理的对象数量的实时信息。

要查看 KSN 使用统计信息：

1. 在应用程序控制台树中，选择“**实时计算机保护**”部分。

2. 选择“**卡巴斯基安全网络**”子节点。

   在结果窗格中，在“**统计信息**”部分中，显示任务统计信息（见下表）。

KSN 统计信息

字段	描述
发送的文件请求	Kaspersky Industrial CyberSecurity for Nodes 向 KSN 发送的对象信誉查询数量。
KSN 中不信任的文件	KSN 分配的信誉不受信任的对象数量。
请求发送错误	处理时出现错误的 KSN 请求数。
形成的统计信息	发送到 KSN 的生成的统计包数量。
对象已删除	Kaspersky Industrial CyberSecurity for Nodes 成功删除的对象数量。
对象未删除	Kaspersky Industrial CyberSecurity for Nodes 尝试删除但无法删除（例如，由于其他应用程序阻止访问对象）的对象数。
已移至备份区	Kaspersky Industrial CyberSecurity for Nodes 成功复制到备份的对象数量。
对象未移至备份区	Kaspersky Industrial CyberSecurity for Nodes 无法复制到备份（例如，由于磁盘空间不足）的对象数。程序不会清除或删除无法移动到备份中的文件。
受限模式	该状态表示应用程序是否在受限制模式下发送文件信誉请求。根据卡巴斯基专家的建议，在受限制模式下，Kaspersky Industrial CyberSecurity for Nodes 仅发送文件信誉请求的一部分。

“**对象已删除**”、“**对象未删除**”、“**已移至备份区**”、“**对象未移至备份区**”字段的值是根据“实时文件保护”组件的统计信息生成的。

卡巴斯基私有安全网络的限制

*卡巴斯基私有安全网络*是让运行 Kaspersky Industrial CyberSecurity for Nodes 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。卡巴斯基私有安全网络允许您使用自己的本地信誉数据库来检查对象（文件或网址）的信誉。添加到本地信誉数据库的对象的信誉比添加到 KSN/KPSN 的对象的信誉具有更高的优先级。例如，假设 Kaspersky Industrial CyberSecurity for Nodes 正在扫描计算机并请求 KSN/KPSN 中文件的信誉。如果文件在本地信誉数据库中具有"*不信任组*"的信誉，但在 KSN/KPSN 中具有"*受信任组*"信誉，Kaspersky Industrial CyberSecurity for Nodes 将检测到该文件为"*不信任组*"，并将采取为检测到的威胁定义的操作。

但是，在某些情况下，Kaspersky Industrial CyberSecurity for Nodes 可能不会请求 KSN/KPSN 中对象的信誉。如果是这种情况，Kaspersky Industrial CyberSecurity for Nodes 将不会从 KPSN 的本地信誉数据库接收数据。Kaspersky Industrial CyberSecurity for Nodes 可能不会请求 KSN/KPSN 中对象的信誉，原因如下：

- Kaspersky 应用程序正在使用离线信誉数据库。离线信誉数据库旨在优化 Kaspersky 应用程序运行期间的资源，并保护计算机上至关重要的对象。离线信誉数据库由 Kaspersky 专家根据卡巴斯基安全网络的数据创建。Kaspersky 应用程序使用特定应用程序的防病毒数据库更新脱机信誉数据库。如果脱机信誉数据库包含有关正在扫描的对象的信息，则应用程序不会从 KSN/KPSN 请求此对象的信誉。
- 扫描排除（受信任区域）在应用程序设置中配置。如果是这种情况，则应用程序不会考虑对象在本地信誉数据库中的信誉。
- 应用程序使用扫描优化技术，如 iSwift 或 iChecker，或正在缓存信誉请求到 KSN / KPSN。如果是这种情况，应用程序可能不会请求以前扫描的对象的信誉。
- 为了优化其工作负载，应用程序扫描特定格式和大小的文件。相关格式和尺寸限制列表由 Kaspersky 专家确定。该列表与应用程序的反病毒数据库一起更新。

KSN 代理设置

受 Kaspersky Security Center 管理服务器管理的用户计算机可以通过 KSN 代理服务与 KSN 互动。

KSN 代理服务提供以下功能：

- 用户计算机可查询 KSN 并将信息提交给 KSN，甚至无需访问互联网即可实现。
- KSN 代理服务会缓存已处理的数据，从而降低外部网络通信信道的负载，并提高用户计算机所请求信息的接收速度。

默认情况下，在启用 KSN 并接受 KSN 声明后，应用程序使用代理服务器连接到卡巴斯基安全网络。应用程序使用的代理服务器是通过 TCP 端口 13111 的 Kaspersky Security Center 管理服务器。因此，如果 KSN 代理不可用，您必须检查设备作为 KSN 代理服务器的运行情况。您必须检查以下内容：

- *Ksnproxy* 服务正在管理服务器上运行。
- 计算机上的防火墙未阻止端口 13111。

您可以按如下方式配置 KSN 代理的使用：启用或禁用 KSN 代理，并配置连接的端口。为此，您需要打开管理服务器属性。有关 KSN 代理配置的详细信息，请参阅 Kaspersky Security Center 帮助。您还可以在 Kaspersky Industrial CyberSecurity for Nodes 策略中为单个计算机启用或禁用 KSN 代理。

如何在 Kaspersky Security Center 管理控制台中启用 KSN 代理

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的 Kaspersky Industrial CyberSecurity for Nodes 策略并双击以打开策略属性。
3. 这将打开一个窗口；在该窗口中，在部分列表中，选择“**实时计算机保护 → KSN 使用**”。
4. 单击“**设置**”。
5. 在“**KSN 代理设置**”块，使用“**使用管理服务器作为 KSN 代理服务器**”复选框启用或禁用 KSN 代理。
6. 如有必要，选中“**如果 KSN 代理服务器不可用则使用卡巴斯基安全网络服务器**”复选框。
   如果选中该复选框，当 KSN 代理服务不可用时，Kaspersky Industrial CyberSecurity for Nodes 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）。
7. 保存更改。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中启用 KSN 代理

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**卡巴斯基安全网络**”子节点。
3. 在主应用程序窗口中，单击“**属性**”。
4. 在“**KSN 代理设置**”块，使用“**使用管理服务器作为 KSN 代理服务器**”复选框启用或禁用 KSN 代理。
5. 如有必要，选中“**如果 KSN 代理服务器不可用则使用卡巴斯基安全网络服务器**”复选框。
   如果选中该复选框，当 KSN 代理服务不可用时，Kaspersky Industrial CyberSecurity for Nodes 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）。
6. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用 KSN 代理

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → KSN 使用**”并点击“**配置**”按钮。
5. 选择或清除“**使用管理服务器作为 KSN 代理服务器**”复选框启用或禁用 KSN 代理。

6. 如有必要，选中“**如果 KSN 代理服务器不可用则使用卡巴斯基安全网络服务器**”复选框。

   如果选中该复选框，当 KSN 代理服务不可用时，Kaspersky Industrial CyberSecurity for Nodes 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）。

7. 保存更改。

KSN 代理地址与管理服务器地址匹配。更改管理服务器域名时，需要手动更新 KSN 代理地址。

漏洞利用防御

Kaspersky Industrial CyberSecurity for Nodes 提供保护进程内存免受漏洞利用的能力。此功能由漏洞利用防御组件实现，您可以使用它来更改组件的活动状态并配置对进程的保护以免受漏洞攻击。

“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 Industrial CyberSecurity for Nodes 将阻止该文件运行或通知用户。该组件通过在受保护的进程中插入外部“进程保护代理”（“保护代理”）保护进程内存免受漏洞利用。

“*进程保护代理*”是一个动态加载的 Kaspersky Industrial CyberSecurity for Nodes 模块，该模块可以插入到受保护的进程中，以便监控进程的完整性并降低被漏洞利用的风险。

该代理在受保护的进程内的运行需要启动和停止进程：只有进程已重启，才能实现首次加载代理到已添加到受保护的进程列表中。此外，从受保护的进程列表中删除进程后，只有该进程已重启才能卸载代理。

必须停止代理才能从受保护的进程中卸载它：如果已卸载“漏洞利用防御”组件，则应用程序将冻结环境并强制从受保护的进程中卸载代理。如果在组件卸载过程中在任一受保护进程中插入代理，则必须终止受影响的进程。可能需要重新启动受保护设备（例如，如果系统进程正在受到保护）。

如果检测到受保护的进程中存在漏洞利用攻击的迹象，则 Kaspersky Industrial CyberSecurity for Nodes 执行以下操作之一：

- 如果进行漏洞利用尝试，则终止该进程。
- 报告进程已遭到入侵的事实。

您可采用以下方法之一停止进程保护：

- 卸载该组件。
- 从受保护的进程列表中删除该进程并重启该进程。

漏洞利用防御模式

可以选择以下一种模式来配置所执行的操作，以降低漏洞在受保护进程中被利用的风险：

- “**阻止**”。如果选择此模式，则 Kaspersky Industrial CyberSecurity for Nodes 在检测到漏洞利用尝试时（如果已对该进程应用积极的攻击缓解技术），将终止受保护的进程。

  当检测到尝试在受保护的关键操作系统进程中利用漏洞时，无论“漏洞利用防御”组件设置中所指定的模式如何，Kaspersky Industrial CyberSecurity for Nodes 都不会终止进程。

- **通知**（在 Kaspersky Security Center Web Console 中工作时 – **通知**）。应用此模式可以使用安全日志中的事件来接收受保护进程中的漏洞实例的有关信息。被利用的进程将继续运行。

  如果选择此模式，Kaspersky Industrial CyberSecurity for Nodes 将创建事件来记录所有漏洞利用尝试。默认情况下选中。

启用和禁用漏洞利用防御

Kaspersky Industrial CyberSecurity for Nodes 允许监控易受攻击的应用程序运行的可执行文件。如果 Kaspersky Industrial CyberSecurity for Nodes 检测到某个易于感染的应用程序的可执行文件被除用户以外的事物运行，Kaspersky Industrial CyberSecurity for Nodes 将执行所选操作（例如，阻止操作）。

如何在 Kaspersky Security Center 管理控制台中启用或禁用漏洞利用防御

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的 Kaspersky Industrial CyberSecurity for Nodes 策略并双击以打开策略属性。
3. 这将打开一个窗口；在该窗口中，在部分列表中，选择“**实时计算机保护 → 漏洞利用防御**”。
4. 单击“**设置**”。
5. 选择“**漏洞利用防御**”复选框启用组件。
6. 在“**常规**”选项卡上，选择一个漏洞预防模式：**阻止**或者**通知**。
7. 如果有必要，清除“**漏洞利用防御**”复选框来禁用该组件。
8. 保存更改。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中启用或禁用漏洞利用防御

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**漏洞利用防御**”子节点。
3. 在主应用程序窗口中，单击“**属性**”。
4. 选择“**漏洞利用防御**”复选框启用组件。
5. 在“**常规**”选项卡上，选择一个漏洞预防模式：**阻止**或者**通知**。
6. 如果有必要，清除“**漏洞利用防御**”复选框来禁用该组件。
7. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用或禁用漏洞利用防御

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 漏洞利用防御**”并点击“**配置**”按钮。
5. 这将打开一个窗口；在该窗口中，在“**漏洞利用防御模式**”下，选择“**防止易受感染的进程被利用漏洞**”复选框来启用该组件。
6. 选择漏洞预防模式：**阻止**或者**通知**。
7. 如果有必要，清除“**防止易受感染的进程被利用漏洞**”复选框来禁用该组件。
8. 保存更改。

启用和禁用内存保护

Kaspersky Industrial CyberSecurity for Nodes 会阻止尝试访问系统进程的外部进程。默认情况下，启用系统进程内存保护。

如何在 Kaspersky Security Center 管理控制台中启用或禁用内存保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的 Kaspersky Industrial CyberSecurity for Nodes 策略并双击以打开策略属性。
3. 这将打开一个窗口；在该窗口中，在部分列表中，选择“**实时计算机保护 → 漏洞利用防御**”。
4. 单击“**设置**”。
5. 在“**常规**”选项卡上，选中“**启用系统进程内存保护**”复选框。
6. 如有必要，清空“**启用系统进程内存保护**”复选框。
7. 保存更改。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中启用或禁用内存保护

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**漏洞利用防御**”子节点。

3. 在主应用程序窗口中，单击“**属性**”。
4. 在“**常规**”选项卡上，选中“**启用系统进程内存保护**”复选框。
5. 如有必要，清空“**启用系统进程内存保护**”复选框。
6. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用或禁用内存保护

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 漏洞利用防御**”并点击“**配置**”按钮。
5. 在打开的窗口中的“**系统进程内存保护**”块中，选中“**系统进程内存保护**”复选框。
6. 如果有必要，清除“**系统进程内存保护**”复选框来禁用系统进程内存保护。
7. 保存更改。

创建受保护进程列表

默认情况下，漏洞利用防御组件保护多个进程。应用程序可以自动生成受保护进程列表。您还可以手动添加或删除进程。

如何在 Kaspersky Security Center 管理控制台中管理受保护进程列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的 Kaspersky Industrial CyberSecurity for Nodes 策略并双击以打开策略属性。
3. 这将打开一个窗口；在该窗口中，在部分列表中，选择“**实时计算机保护 → 漏洞利用防御**”。
4. 单击“**设置**”。
5. 在“**受保护进程**”选项卡上，选择以下选项之一来保护进程免遭恶意代码注入：
   - “**自动检测受保护的进程**”。如果选择此选项，应用程序将自动创建受保护进程的列表。
   - “**仅保护以下列表中的进程**”。如果选择此选项，您可以选择想要保护的进程。

6. 如果您选择了“**仅保护以下列表中的进程**”，您可以通过执行以下操作之一来编辑受保护进程列表：

   - 如果需要，单击“**添加**”并选择要添加到受保护进程列表中的进程。
   - 如果要从已创建的受保护进程列表中删除某个进程，请在列表中选中该进程，然后单击“**删除**”。
     在列表中选择一个或多个进程后，“**删除**”按钮变为可用。

7. 保存更改。

如何使用 Kaspersky Industrial CyberSecurity for Nodes 控制台管理受保护进程列表

1. 在应用程序控制台树中，展开“**实时计算机保护**”节点。
2. 选择“**漏洞利用防御**”子节点。
3. 在主应用程序窗口中，单击“**属性**”。
4. 在“**受保护进程**”选项卡上，选择以下选项之一来保护进程免遭恶意代码注入：

   - “**自动检测受保护的进程**”。如果选择此选项，应用程序将自动创建受保护进程的列表。
   - “**仅保护以下列表中的进程**”。如果选择此选项，您可以选择想要保护的进程。

5. 如果您选择了“**仅保护以下列表中的进程**”，您可以通过执行以下操作之一来编辑受保护进程列表：

   - 如果需要，单击“**添加**”并选择要添加到受保护进程列表中的进程。
   - 如果要从已创建的受保护进程列表中删除某个进程，请在列表中选中该进程，然后单击“**删除**”。
     在列表中选择一个或多个进程后，“**删除**”按钮变为可用。

6. 保存更改。

如何在 Kaspersky Security Center Web Console 中管理受保护进程列表

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 漏洞利用防御**”部分，然后单击“**配置**”按钮。
5. 在“**受保护进程列表**”下，选择以下选项之一来保护进程免遭恶意代码注入：

   - “**自动检测受保护的进程**”。如果选择此选项，应用程序将自动创建受保护进程的列表。
   - “**仅保护以下列表中的进程**”。如果选择此选项，您可以添加、编辑和删除想要保护的进程。

6. 如果您选择了“**仅保护以下列表中的进程**”，执行以下操作之一：

- 点击“**添加**”打开“**受保护进程**”窗口，在该窗口中：

  a. 选择**受保护进程**复选框。

  b. 在“**进程名称**”字段中输入进程的名称。

  c. 保存更改。

- 如有必要，请在受保护进程列表中编辑进程设置。为此，请执行以下操作：

  a. 在受保护的进程列表中选择进程。

  b. 单击“**编辑**”。在列表中选择一个或多个进程后，“**编辑**”按钮变为可用。

  c. 在“**受保护进程**”窗口中，选中或清除“**受保护进程**”复选框。

  d. 如有必要，可在“**进程名称**”字段编辑进程名称。

  e. 保存更改。

- 如有必要，您可以从受保护进程列表中删除一个进程。为此，请执行以下操作：

  a. 在受保护进程列表中选择一个或多个进程。

  b. 单击“**删除**”。在列表中选择一个或多个进程后，“**删除**”按钮变为可用。

7. 保存更改。

修复引擎

修复引擎允许 Kaspersky Industrial CyberSecurity for Nodes 回滚恶意软件在操作系统中执行的操作。

回滚操作系统中的恶意软件活动时，Kaspersky Industrial CyberSecurity for Nodes 执行以下操作：

- **文件活动**
  - 删除恶意软件在除网络驱动器外的所有介质上创建的可执行文件。
  - 删除已被恶意软件入侵的程序所创建的可执行文件。
  - 恢复被恶意软件修改或删除的文件。

  文件恢复功能有**一些限制**。

  - 应用程序只能还原文件系统为 NTFS 或 FAT32 的设备上的文件。
  - 应用程序可还原具有以下扩展名的文件：odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd。
  - 无法还原位于网络驱动器或可擦写 CD/DVD 上的文件。
  - 无法还原使用加密文件系统 (EFS) 加密的文件。有关 EFS 操作的详细信息，请访问 Microsoft 网站。
  - 应用程序不会监控由操作系统内核级别的进程对文件执行的修改。
  - 应用程序不会监控通过网络接口对文件执行的修改（例如，如果某个文件存储在共享文件夹中，并且进程从其他计算机上远程启动）。
- **注册表活动**
  - 删除由恶意软件创建的注册表项。

  Kaspersky Industrial CyberSecurity for Nodes 不会恢复被恶意软件修改或删除的注册表项。
- **系统活动**
  - 终止由恶意软件启动的进程。
  - 终止被恶意应用程序渗透的进程。

  Kaspersky Industrial CyberSecurity for Nodes 不恢复被恶意软件挂起的进程。

- **网络活动**
  - 阻止恶意软件的网络活动。
  - 阻止被恶意软件入侵的进程的网络活动。

“实时文件保护”组件或在按需扫描期间可以启动恶意应用程序操作的回滚。

回滚恶意软件操作会影响一组严格定义的数据。回滚对操作系统或计算机数据完整性无不良影响。

如何在 Kaspersky Security Center 管理控制台中启用或禁用修复引擎组件

1. **打开要配置的策略中的修复引擎组件的设置**。
   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
   b. 选择要为其配置任务的管理组。
   c. 选择**策略**选项卡。
   d. 双击策略名称打开策略属性窗口。
   e. 在策略属性窗口中，转到“**实时计算机保护**”区域。
   f. 在“**修复引擎**”块中单击“**设置**”按钮。
   将打开“**修复引擎**”窗口的“**常规**”选项卡。
2. 执行下列操作之一：
   - 如果要启用修复引擎组件，请选中“**修复引擎**”复选框。
   - 如果要禁用修复引擎组件，请清除“**修复引擎**”复选框。
3. 在“**修复引擎**”窗口中单击“**确定**”按钮。
4. 在“**属性：<策略名称>**”窗口中，单击“**确定**”按钮。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中启用或禁用修复引擎组件

1. 在应用程序控制台树中，选择“**实时计算机保护 → 修复引擎**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“**修复引擎**”窗口的“**常规**”选项卡。

3. 执行下列操作之一：

   - 如果要启用修复引擎组件，请选中“**修复引擎**”复选框。
   - 如果要禁用修复引擎组件，请清除“**修复引擎**”复选框。

4. 在“**修复引擎**”窗口中单击“**确定**”按钮。

如何在 Kaspersky Security Center Web Console 中启用或禁用修复引擎组件

1. **打开要配置的策略中的修复引擎组件的设置**。

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

   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

   c. 选择**应用程序设置**选项卡。

   d. 选择“**实时计算机保护**”部分。

   e. 在“**修复引擎**”块中单击“**配置**”按钮。
   “**修复引擎**”窗口将打开。

2. 执行下列操作之一：

   - 如果要启用修复引擎组件，请选中“**修复引擎**”复选框。
   - 如果要禁用修复引擎组件，请清除“**修复引擎**”复选框。

3. 在“**修复引擎**”窗口中单击“**确定**”按钮。

4. 在“**<策略名称>**”窗口中，单击“**保存**”。

反加密

“反加密”组件接收您计算机上的应用程序操作的数据，并将此信息提供给其他保护组件以提高性能。“反加密”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 Industrial CyberSecurity for Nodes 将执行选定的响应操作。基于行为流签名的 Kaspersky Industrial CyberSecurity for Nodes 功能为计算机提供了主动防御。

启用和禁用本地文件夹的加密保护

如何在 Kaspersky Security Center 管理控制台中启用或禁用反加密

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 点击“**反加密**”部分中的“**设置**”。
5. 使用“**反加密**”复选框启用或禁用组件。
6. 转到“**常规**”选项卡。
7. 使用“**启用本地文件夹对外部加密的防护**”复选框启用或禁用选项。如果选择该复选框，Kaspersky Industrial CyberSecurity for Nodes 会使用下面指定的操作响应恶意活动。
8. 在“**检测到恶意软件活动时的操作**”块中选择相关操作：
   - “**删除**”。如果选择此项目，在检测到恶意活动时，Kaspersky Industrial CyberSecurity for Nodes 会删除恶意应用程序的可执行文件，同时在备份区创建该文件的备份副本。
   - “**阻止**”。如果选择此项目，在检测到恶意活动时，Kaspersky Industrial CyberSecurity for Nodes 会终止该应用程序。
   - “**通知**”。如果选择此项目并且检测到应用程序的恶意软件活动，Kaspersky Industrial CyberSecurity for Nodes 将应用程序恶意软件活动的相关信息添加至活动威胁列表。
9. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Security Center Web Console 中启用或禁用反加密

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 转到“**实时计算机保护 → 反加密勒索**”并点击“**配置**”按钮。
   “**反加密勒索**”窗口将打开。

5. 使用“**启用反加密勒索**”复选框启用或禁用组件。

6. 转到“**常规**”选项卡。

7. 使用“**启用本地文件夹对外部加密的防护**”复选框启用或禁用选项。如果选择该复选框，Kaspersky Industrial CyberSecurity for Nodes 会使用下面指定的操作响应恶意活动。

8. 在“**检测到共享文件夹的外部加密时**”块中选择相关操作：

   - “**删除**”。如果选择此项目，在检测到恶意活动时，Kaspersky Industrial CyberSecurity for Nodes 会删除恶意应用程序的可执行文件，同时在备份区创建该文件的备份副本。
   - “**阻止**”。如果选择此项目，在检测到恶意活动时，Kaspersky Industrial CyberSecurity for Nodes 会终止该应用程序。
   - “**通知**”。如果选择此项目并且检测到应用程序的恶意软件活动，Kaspersky Industrial CyberSecurity for Nodes 将应用程序恶意软件活动的相关信息添加至活动威胁列表。

9. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中启用或禁用反加密

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中选择“**实时计算机保护 → 反加密**”。

2. 点击“**反加密**”节点的结果窗格中的“**属性**”。
   “**属性: 反加密**”窗口打开。

3. 选择“**反加密**”复选框。

4. 转到“**常规**”选项卡。

5. 使用“**启用本地文件夹对外部加密的防护**”复选框启用或禁用选项。如果选择该复选框，Kaspersky Industrial CyberSecurity for Nodes 会使用下面指定的操作响应恶意活动。

6. 在“**检测到共享文件夹的外部加密时**”块中选择相关操作：

   - “**删除**”。如果选择此项目，在检测到恶意活动时，Kaspersky Industrial CyberSecurity for Nodes 会删除恶意应用程序的可执行文件，同时在备份区创建该文件的备份副本。
   - “**阻止**”。如果选择此项目，在检测到恶意活动时，Kaspersky Industrial CyberSecurity for Nodes 会终止该应用程序。
   - “**通知**”。如果选择此项目并且检测到应用程序的恶意软件活动，Kaspersky Industrial CyberSecurity for Nodes 将应用程序恶意软件活动的相关信息添加至活动威胁列表。

7. 保存更改。

防止共享文件夹被外部加密

该组件只能监控针对存储在文件系统为 NTFS 的大容量存储设备上并且未使用 EFS 加密的文件所进行的操作。

共享文件夹对外部加密的防护提供对共享文件夹中活动的分析。如果该活动与外部加密的典型行为流签名匹配，Kaspersky Industrial CyberSecurity for Nodes 将执行选定操作。

如果检测到尝试修改共享文件夹中的文件，Kaspersky Industrial CyberSecurity for Nodes 将执行以下操作：

- 阻止对启动恶意活动的会话的文件修改（该文件将是只读的）。
- 创建被修改的文件的备份副本。
- 向本地应用程序接口报告添加条目，并将有关检测到的恶意活动的信息发送到 Kaspersky Security Center。
- 此外，如果启用了“修复引擎”组件，将从备份副本还原被修改的文件。

启用和禁用共享文件夹对外部加密的防护

默认情况下，共享文件夹防外部加密保护功能已启用，并以卡巴斯基专家推荐的模式工作。要配置此功能，您可以创建保护范围，并在必要时配置排除项。默认情况下，应用程序会自动识别共享文件夹并跟踪所有文件夹中的文件活动。如果检测到尝试对共享文件夹中的文件进行外部加密，Kaspersky Industrial CyberSecurity for Nodes 会阻止远程用户的会话一小时（默认）。

安装 Kaspersky Industrial CyberSecurity for Nodes 后，共享文件夹对外部加密的防护将受到限制，直到计算机重启为止。

如何在 Kaspersky Security Center 管理控制台中启用或禁用共享文件夹对外部加密的保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 点击“**反加密**”部分中的“**设置**”。
5. 使用“**反加密**”复选框启用或禁用组件。
6. 转到“**共享文件夹的保护**”选项卡。
7. 使用“**保护共享文件夹**”复选框启用或禁用选项。

8. 在“**共享文件夹对外部加密的防护**”块中选择相关操作：

   - **阻止连接时间 N 分钟**。如果选择此选项，当 Kaspersky Industrial CyberSecurity for Nodes 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修改（只读）的访问，并创建已修改文件的备份副本。

     如果启用了“修复引擎”组件，并且选择“**阻止连接时间 N 分钟**”选项，被修改的文件将被从备份副本恢复。

   - “**通知**”。如果选择此选项，则当检测到尝试修改共享文件夹中的文件时， Kaspersky Industrial CyberSecurity for Nodes 会将有关共享文件夹中此文件修改尝试的信息添加到活动威胁列表中，将记录添加到应用程序本地接口的报告，并将有关恶意活动检测的信息发送到 Kaspersky Security Center。

9. 如有必要，创建保护范围并配置排除项。

10. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Security Center Web Console 中启用或禁用共享文件夹对外部加密的保护

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**实时计算机保护 → 反加密勒索**”并点击“**配置**”按钮。

   “**反加密勒索**”窗口将打开。

5. 使用“**启用反加密勒索**”复选框启用或禁用组件。

6. 转到“**共享文件夹的保护**”选项卡。

7. 使用“**启用共享文件夹对外部加密的防护**”复选框启用或禁用选项。

8. 在“**检测外部加密**”块中选择相关操作：

   - “**阻止连接**”。如果选择此选项，当 Kaspersky Industrial CyberSecurity for Nodes 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修改（只读）的访问，并创建已修改文件的备份副本。

     如果启用了“修复引擎”组件，并且选择了“**阻止连接**”选项，被修改的文件将被从备份副本恢复。

   - “**通知**”。如果选择此选项，则当检测到尝试修改共享文件夹中的文件时， Kaspersky Industrial CyberSecurity for Nodes 会将有关共享文件夹中此文件修改尝试的信息添加到活动威胁列表中，将记录添加到应用程序本地接口的报告，并将有关恶意活动检测的信息发送到 Kaspersky Security Center。

9. 如有必要，创建保护范围并配置排除项。
10. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中启用或禁用共享文件夹对外部加密的保护

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中选择“**实时计算机保护 → 反加密**”。
2. 点击“**反加密**”节点的结果窗格中的“**属性**”。
   “**属性: 反加密**”窗口打开。
3. 选择“**反加密**”复选框。
4. 转到“**共享文件夹的保护**”选项卡。
5. 使用“**保护共享文件夹**”复选框启用或禁用选项。
6. 在“**共享文件夹对外部加密的防护**”块中选择相关操作：
   - **阻止连接时间 N 分钟**。如果选择此选项，当 Kaspersky Industrial CyberSecurity for Nodes 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修改（只读）的访问，并创建已修改文件的备份副本。

     如果启用了“修复引擎”组件，并且选择“**阻止连接时间 N 分钟**”选项，被修改的文件将被从备份副本恢复。

   - “**通知**”。如果选择此选项，则当检测到尝试修改共享文件夹中的文件时， Kaspersky Industrial CyberSecurity for Nodes 会将有关共享文件夹中此文件修改尝试的信息添加到活动威胁列表中，将记录添加到应用程序本地接口的报告，并将有关恶意活动检测的信息发送到 Kaspersky Security Center。
7. 如有必要，创建保护范围并配置排除项。
8. 保存更改。

创建保护范围

*保护范围*是 Kaspersky Industrial CyberSecurity for Nodes 监控其内部文件活动的共享文件夹路径列表。Kaspersky Industrial CyberSecurity for Nodes 在输入掩码时支持环境变量和 `*` 和 `?` 字符：默认情况下，应用程序会自动识别共享文件夹并跟踪所有文件夹中的文件活动。

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。例如，当用户处理共享文件夹中具有 ENC 扩展名的文件时，反加密组件可能会引发误报。这种活动与外部加密的典型行为模式相匹配。如果您在共享文件夹中有加密文件以保护数据，请将该文件夹添加到排除项。

如果您希望忽略来自某些计算机的外部加密尝试，您也可以排除这些计算机。

如何在 Kaspersky Security Center 管理控制台中配置保护范围

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 点击“**反加密**”部分中的“**设置**”。
5. 使用“**反加密**”复选框启用或禁用组件。
6. 转到“**共享文件夹的保护**”选项卡。
7. 在“**保护范围**”块中单击“**配置**”按钮。
8. 在打开的窗口中，选择“**仅指定的共享文件夹**”模式。
9. 单击“**添加**”。
10. 这将打开一个窗口；在该窗口中，输入要包含在保护范围内的共享文件夹的路径（例如，`C:\Share`）。

    > 要将共享文件夹添加到保护范围，请使用本地路径。

11. 单击“**确定**”。
12. 如果有必要，配置保护范围的排除项：

    a. 在“**排除项**”块中单击“**配置**”按钮。

    b. 单击打开的窗口中的“**添加**”按钮。

    c. 在显示的窗口中，输入文件夹或文件的路径。

    使用掩码：

    - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和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。
    - 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。
    - `?`（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。

    您可以从扫描排除对象，而不用将其从保护范围对象列表中删除。为此，清空对象旁边的复选框。

13. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中配置保护范围

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 反加密勒索**”并点击“**配置**”按钮。
   “**反加密勒索**”窗口将打开。
5. 使用“**启用反加密勒索**”复选框启用或禁用组件。
6. 转到“**共享文件夹的保护**”选项卡。
7. 在“**保护范围**”下，选择“**仅指定的共享文件夹**”模式。
8. 单击“**添加**”。
9. 这将打开一个窗口；在该窗口中，输入要包含在保护范围内的共享文件夹的路径（例如，`C:\Share`）。

   > 要将共享文件夹添加到保护范围，请使用本地路径。

10. 单击“**确定**”。
11. 如果有必要，配置保护范围的排除项：
    a. 在“**要排除的对象**”块中单击“**添加**”按钮。
    b. 在显示的窗口中，输入文件夹或文件的路径。
       使用掩码：
       - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和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。
       - 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。
       - `?`（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。

    您可以从扫描排除对象，而不用将其从保护范围对象列表中删除。为此，清空对象旁边的复选框。
12. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中配置保护范围

1. 在策略属性窗口中，选择“**实时计算机保护**”。
2. 点击“**反加密**”部分中的“**设置**”。
3. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中选择“**实时计算机保护 → 反加密**”。
4. 点击“**反加密**”节点的结果窗格中的“**属性**”。
   “**属性: 反加密**”窗口打开。
5. 使用“**反加密**”复选框启用或禁用组件。
6. 转到“**共享文件夹的保护**”选项卡。
7. 在“**保护范围**”块中单击“**配置**”按钮。
8. 在打开的窗口中，选择“**仅指定的共享文件夹**”模式。
9. 在“**保护范围**”块中单击“**添加**”按钮。
10. 这将打开一个窗口；在该窗口中，输入要包含在保护范围内的共享文件夹的路径（例如，`C:\Share`）。

    > 要将共享文件夹添加到保护范围，请使用本地路径。

11. 单击“**确定**”。
12. 如果有必要，配置保护范围的排除项：
    a. 在“**排除项**”块中单击“**设置**”按钮。
    b. 在显示的“**按掩码的排除项**”窗口中单击“**添加**”按钮。
    c. 在显示的窗口中，输入文件夹或文件的路径。
       使用掩码：
       - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和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。
       - 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。
       - `?`（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。

您可以从扫描排除对象，而不用将其从保护范围对象列表中删除。为此，清空对象旁边的复选框。

13. 保存更改。

添加受信任的计算机以进行外部数据加密

如果您的组织使用外部数据加密进行文件交换，则必须制作受信任的计算机列表。Kaspersky Industrial CyberSecurity for Nodes 不监控来自受信任计算机的数据加密。

必须启用审计登录服务，才能从共享文件夹对外部加密的防护中排除地址。默认情况下，审计登录服务已禁用（有关启用审计登录服务的详细信息，请访问 Microsoft 网站）。

如果远程计算机在 Kaspersky Industrial CyberSecurity for Nodes 启动前启动，从共享文件夹保护中排除地址的功能将不适用于该远程计算机。您可以在 Kaspersky Industrial CyberSecurity for Nodes 启动后重启该远程计算机，确保从共享文件夹保护中排除地址的功能在该远程计算机上有效。

如何在 Kaspersky Security Center 管理控制台中添加受信任计算机以对数据进行外部加密

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 点击“**反加密**”部分中的“**设置**”。
5. 转到“**共享文件夹的保护**”选项卡。
6. 在“**IP 地址排除项**”块中单击“**配置**”按钮。
7. 单击打开的窗口中的“**添加**”按钮。
8. 输入不应处理其外部加密尝试的计算机的 IP 地址或名称。
9. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Security Center Web Console 中添加受信任计算机以对数据进行外部加密

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 转到“**实时计算机保护 → 反加密勒索**”并点击“**配置**”按钮。
   “**反加密勒索**”窗口将打开。
5. 转到“**共享文件夹的保护**”选项卡。
6. 在“**排除项**”块中单击“**添加**”按钮。
7. 输入不应处理其外部加密尝试的计算机的 IP 地址或名称。
8. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中添加受信任计算机以对数据进行外部加密

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中选择“**实时计算机保护 → 反加密**”。
2. 点击“**反加密**”节点的结果窗格中的“**属性**”。
   “**属性: 反加密**”窗口打开。
3. 转到“**共享文件夹的保护**”选项卡。
4. 在“**IP 地址排除项**”块中单击“**配置**”按钮。
5. 单击打开的窗口中的“**添加**”按钮。
6. 输入不应处理其外部加密尝试的计算机的 IP 地址或名称。
7. 保存更改。

配置不受信任的计算机的阻止期限

*不受信任的计算机*是正在从事恶意活动或数据加密的远程计算机。默认情况下，Kaspersky Industrial CyberSecurity for Nodes 会阻止远程用户会话一小时。当阻止期限到期时，Kaspersky Industrial CyberSecurity for Nodes 会将计算机从阻止列表中删除，并恢复对共享文件夹的访问权限。

如何在 Kaspersky Security Center 管理控制台中配置不受信任计算机的阻止期限

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 点击“**反加密**”部分中的“**设置**”。
5. 使用“**反加密**”复选框启用或禁用组件。
6. 转到“**共享文件夹的保护**”选项卡。

7. 在“**检测到共享文件夹的外部加密时**”下，配置正在从事恶意活动或数据加密的不受信任的计算机的阻止期限。
8. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中配置不受信任计算机的阻止期限

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 反加密勒索**”并点击“**配置**”按钮。
   “**反加密勒索**”窗口将打开。
5. 使用“**启用反加密勒索**”复选框启用或禁用组件。
6. 转到“**共享文件夹的保护**”选项卡。
7. 在“**检测外部加密**”下，配置正在从事恶意活动或数据加密的不受信任的计算机的阻止期限。
8. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中配置不受信任计算机的阻止期限

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中选择“**实时计算机保护 → 反加密**”。
2. 点击“**反加密**”节点的结果窗格中的“**属性**”。
   “**属性: 反加密**”窗口打开。
3. 选择“**反加密**”复选框。
4. 转到“**共享文件夹的保护**”选项卡。
5. 在“**共享文件夹对外部加密的防护**”下，配置正在从事恶意活动或数据加密的不受信任的计算机的阻止期限。
6. 保存更改。

从共享文件夹对外部加密的防护中导出和导入排除项列表

可以将排除列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的地址。还可以使用导出/导入功能备份排除列表或将列表迁移到其他服务器。

如何在 Kaspersky Security Center 管理控制台中导出和导入排除列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**实时计算机保护**”。
4. 点击“**反加密**”部分中的“**设置**”。
5. 转到“**共享文件夹的保护**”选项卡。
6. 在“**IP 地址排除项**”块中单击“**配置**”按钮。
7. 要导出规则列表：
   a. 如果需要，选择您要导出的排除项。
   b. 点击 按钮并选择导出模式：导出整个排除列表或仅导出选定的排除项。
   c. 在打开的窗口中，指定您要将排除项列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
      Kaspersky Industrial CyberSecurity for Nodes 会将排除项列表导出到 XML 文件。
8. 要导入排除项列表：
   a. 单击“ → **导入**”按钮。
      在打开的窗口中，选择要从中导入排除项列表的 XML 文件。
   b. 打开文件。
      Kaspersky Industrial CyberSecurity for Nodes 导入排除项。
9. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Security Center Web Console 中导出和导入排除列表

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护 → 反加密勒索**”并点击“**配置**”按钮。
   “**反加密勒索**”窗口将打开。
5. 使用“**启用反加密勒索**”复选框启用或禁用组件。

6. 转到“**共享文件夹的保护**”选项卡。

7. 要在**排除项**块导出排除项列表：

   a. 如果需要，选择您要导出的排除项。

   b. 点击“**导出**”按钮并选择导出模式：导出整个排除项列表或仅导出选定的排除项。

   c. 保存文件。
   Kaspersky Industrial CyberSecurity for Nodes 会将排除项列表导出到 XML 文件。

8. 要在**排除项**块导入排除项列表：

   a. 点击“**导入**”按钮并选择导入模式：添加或替换。

   b. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。

   c. 打开文件。
   Kaspersky Industrial CyberSecurity for Nodes 根据所选模式导入排除项。

9. 保存更改。要在计算机上应用该策略，请关闭锁 。

网络威胁防护

“网络威胁防护”组件扫描入站网络流量中是否存在典型网络攻击活动。在检测到以您的计算机为目标的网络攻击企图时，Kaspersky Industrial CyberSecurity for Nodes 将阻止攻击计算机的网络活动。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。

默认情况下，“网络威胁防护”任务在“**通知**”模式下运行。在此模式下，Kaspersky Industrial CyberSecurity for Nodes 会扫描入站网络流量以查找典型的网络攻击活动，并记录与检测到的活动对应的事件，但不会阻止与参与此类活动的计算机的连接，也不会将计算机的 IP 地址添加到阻止的网络会话列表中。

在此模式下“**阻止**”，Kaspersky Industrial CyberSecurity for Nodes 会阻止连接到表现出典型网络攻击活动的计算机，并且在某些情况下将此类计算机的 IP 地址添加到阻止的网络会话列表中。

您可以在阻止的主机存储中查看阻止的主机列表。

当应用程序重启和网络威胁防护设置被更改时，Kaspersky Industrial CyberSecurity for Nodes 清空阻止列表。

您可以通过配置阻止的主机存储设置来恢复对阻止的主机的访问，并指定主机在被阻止多少天、小时和分钟后可重新获得对网络文件资源的访问权限。

在以下情况下，将从阻止的主机列表中删除出现典型网络攻击活动的主机的 IP 地址：

- Kaspersky Industrial CyberSecurity for Nodes 已卸载。
- 手动从阻止的主机列表中删除了 IP 地址。
- 主机阻止期限已到期。
- “**阻止**”模式已关闭。

为了使 Kaspersky Industrial CyberSecurity for Nodes 在 Microsoft Hyper-V 基础架构中的虚拟机上正常运行，您需要在配置 Hyper-V 虚拟交换机之前安装 Kaspersky Industrial CyberSecurity for Nodes 。

如何在 Kaspersky Security Center 管理控制台中启用和配置网络威胁防护

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在策略属性窗口中，转到“**网络活动控制**”区域。
6. 在“**网络威胁防护**”块中单击“**设置**”按钮。
   将打开“**网络威胁防护**”窗口的“**常规**”选项卡。

7. 选择“**网络威胁防护**”复选框启用“网络威胁防护”组件。

8. 在“**操作模式**”部分中选择任务模式：

   - “**阻止**”。如果选择此模式，Kaspersky Industrial CyberSecurity for Nodes 会扫描入站网络流量，查找典型的网络攻击活动，阻止与显示此类活动的计算机的连接，并且在某些情况下将计算机的 IP 地址添加到阻止的网络会话列表中。应用程序还在组件日志中记录有关检测到的典型网络攻击活动的事件。

   - “**通知**”。如果选择此模式， Kaspersky Industrial CyberSecurity for Nodes 会扫描入站网络流量以查找典型的网络攻击活动，但不会阻止与显示此类活动的计算机的连接，也不会将计算机的 IP 地址添加到阻止的网络会话列表中。应用程序在组件日志中记录有关检测到的典型网络攻击活动的事件。

9. 使用“**将端口扫描和网络 Flooding 视为攻击**”复选框启用或禁用对相应攻击的检测。

10. 如有必要，选中“**阻止攻击设备 N 分钟**”复选框。

11. 在“**MAC 欺骗防护**”块中，选中或清除“**启用针对 MAC 欺骗攻击的保护**”复选框。

12. 如果需要的话，你可以**添加阻止排除项**。

    Kaspersky Industrial CyberSecurity for Nodes 可以识别网络攻击并阻止不安全的传输大量数据包的网络连接（例如，从摄像头）。要使用收信人设备，您可以添加这些设备的 IP 地址到排除项列表。您还可以选择用于通信并允许特定网络活动的协议和端口。

    Kaspersky Industrial CyberSecurity for Nodes 4.5 中添加了选择排除项的协议和端口的功能。确保应用程序和管理插件已更新至版本 4.5 或更高版本。如果您使用的是早期版本的应用程序或管理插件，Kaspersky Industrial CyberSecurity for Nodes 只能通过 IP 地址允许网络活动。

    a. 选择**排除项**选项卡。

    b. 选中“**不控制排除的地址**”复选框，以阻止 Kaspersky Industrial CyberSecurity for Nodes 扫描排除的 IP 地址的入站网络流量。

    c. 单击“**添加**”。

    d. 在“**排除项**”窗口中，输入不阻止其网络攻击的计算机的 IP 地址。

    e. 如果需要，选择用于传输数据的协议和端口。

    f. 单击“**确定**”。

    g. 对每个添加的排除项执行步骤 c-f。

13. 保存更改。

如何在应用程序控制台中启用或禁用网络威胁防护

1. 在应用程序控制台树中，选择“**实时计算机保护 → 网络威胁防护**”节点。

2. 在结果窗格中单击“**属性**”链接。
   “**属性：网络威胁防护**”窗口将打开。

3. 选择“**网络威胁防护**”复选框以启用网络威胁防护组件。

4. 在“**操作模式**”部分中选择任务模式：

   - “**阻止**”。如果选择此模式，Kaspersky Industrial CyberSecurity for Nodes 会扫描入站网络流量，查找典型的网络攻击活动，阻止与显示此类活动的计算机的连接，并且在某些情况下将计算机的 IP 地址添加到阻止的网络会话列表中。应用程序还在组件日志中记录有关检测到的典型网络攻击活动的事件。

   - “**通知**”。如果选择此模式， Kaspersky Industrial CyberSecurity for Nodes 会扫描入站网络流量以查找典型的网络攻击活动，但不会阻止与显示此类活动的计算机的连接，也不会将计算机的 IP 地址添加到阻止的网络会话列表中。应用程序在组件日志中记录有关检测到的典型网络攻击活动的事件。

5. 使用“**将端口扫描和网络 Flooding 视为攻击**”复选框启用或禁用对相应攻击的检测。

6. 如有必要，选中“**阻止攻击设备 N 分钟**”复选框。

7. 在“**MAC 欺骗防护**”块中，选中或清除“**启用针对 MAC 欺骗攻击的保护**”复选框。

8. 如果需要的话，你可以**添加阻止排除项**。

   Kaspersky Industrial CyberSecurity for Nodes 可以识别网络攻击并阻止不安全的传输大量数据包的网络连接（例如，从摄像头）。要使用收信人设备，您可以添加这些设备的 IP 地址到排除项列表。您还可以选择用于通信并允许特定网络活动的协议和端口。

   > Kaspersky Industrial CyberSecurity for Nodes 4.5 中添加了选择排除项的协议和端口的功能。确保应用程序和管理插件已更新至版本 4.5 或更高版本。如果您使用的是早期版本的应用程序或管理插件，Kaspersky Industrial CyberSecurity for Nodes 只能通过 IP 地址允许网络活动。

   a. 选择**排除项**选项卡。

   b. 选中“**不控制排除的地址**”复选框，以阻止 Kaspersky Industrial CyberSecurity for Nodes 扫描排除的 IP 地址的入站网络流量。

   c. 单击“**添加**”。

   d. 在“**排除项**”窗口中，输入不阻止其网络攻击的计算机的 IP 地址。

   e. 如果需要，选择用于传输数据的协议和端口。

   f. 单击“**确定**”。

   g. 对每个添加的排除项执行步骤 c-f。

9. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用和配置网络威胁防护

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**网络活动控制**” → “**网络威胁防护**”。

5. 在“**常规**”选项卡上，选择“**启用网络威胁防护**”复选框以启用“网络威胁防护”组件。

6. 选择任务运行模式:

   - “**阻止**”。如果选择此模式，Kaspersky Industrial CyberSecurity for Nodes 会扫描入站网络流量，查找典型的网络攻击活动，阻止与显示此类活动的计算机的连接，并且在某些情况下将计算机的 IP 地址添加到阻止的网络会话列表中。应用程序还在组件日志中记录有关检测到的典型网络攻击活动的事件。

   - “**通知**”。如果选择此模式， Kaspersky Industrial CyberSecurity for Nodes 会扫描入站网络流量以查找典型的网络攻击活动，但不会阻止与显示此类活动的计算机的连接，也不会将计算机的 IP 地址添加到阻止的网络会话列表中。应用程序在组件日志中记录有关检测到的典型网络攻击活动的事件。

7. 使用“**将端口扫描和网络 Flooding 视为攻击**”复选框启用或禁用对相应攻击的检测。

8. 如有必要，选中“**阻止攻击设备 N 分钟**”复选框。

9. 选中或清除“**启用针对 MAC 欺骗攻击的保护**”复选框。

10. 如果需要的话，你可以**添加阻止排除项**。

    Kaspersky Industrial CyberSecurity for Nodes 可以识别网络攻击并阻止不安全的传输大量数据包的网络连接（例如，从摄像头）。要使用收信人设备，您可以添加这些设备的 IP 地址到排除项列表。您还可以选择用于通信并允许特定网络活动的协议和端口。

    > Kaspersky Industrial CyberSecurity for Nodes 4.5 中添加了选择排除项的协议和端口的功能。确保应用程序和管理插件已更新至版本 4.5 或更高版本。如果您使用的是早期版本的应用程序或管理插件，Kaspersky Industrial CyberSecurity for Nodes 只能通过 IP 地址允许网络活动。

    a. 选择**排除项**选项卡。

    b. 选中“**不控制排除的地址**”复选框，以阻止 Kaspersky Industrial CyberSecurity for Nodes 扫描排除的 IP 地址的入站网络流量。

    c. 单击“**添加**”。

    d. 在“**排除项**”窗口中，输入不阻止其网络攻击的计算机的 IP 地址。

    e. 如果需要，选择用于传输数据的协议和端口。

    f. 单击“**确定**”。

    g. 对每个添加的排除项执行步骤 c-f。

11. 保存更改。

AMSI 扫描程序

当“AMSI 扫描程序”任务运行时，Kaspersky Industrial CyberSecurity for Nodes 控制使用 Microsoft Windows 脚本技术 (Active Scripting)（例如 VBScript 或 JScript）创建的脚本的执行。应用程序还可以处理 PowerShell 脚本和在安装了Antimalware Scan Interface (AMSI) 的操作系统上的 Microsoft Office 应用程序中运行的脚本。

AMSI 允许应用程序和服务与安装在设备上的任何反恶意软件应用程序集成，以便反恶意软件拦截和扫描所有执行的脚本。您可以在 Microsoft 网站 上找到有关 AMSI 功能的更多信息。

在组件设置中，您可以允许或者拒绝危险脚本的运行。如果 Kaspersky Industrial CyberSecurity for Nodes 将脚本识别为危险，它会根据您选择的操作阻止或允许执行该脚本。如果您选择“**阻止**”操作，应用程序阻止危险脚本并允许其他脚本。

Kaspersky Industrial CyberSecurity for Nodes 支持 Microsoft Windows 10 和 Microsoft Windows Server 2016 及更高版本中的 AMSI 技术。

启用和禁用 AMSI 扫描程序

如何在 Kaspersky Security Center 管理控制台中启用或禁用 AMSI 扫描程序

1. **转到您要配置的策略中的 AMSI 扫描程序设置**。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择“**策略**”选项卡。

   d. 双击策略名称打开策略属性窗口。

   e. 在策略属性窗口中，转到“**实时计算机保护**”区域。

   f. 在“**AMSI 扫描程序**”块中单击“**设置**”按钮。
   将打开“**AMSI 扫描程序**”窗口的“**常规**”选项卡。

2. 执行下列操作之一：

   - 如果要启用 AMSI 扫描程序，请选择“**AMSI 扫描程序**”复选框。
   - 如果要禁用 AMSI 扫描程序，请清除“**AMSI 扫描程序**”复选框。

3. 在“**AMSI 扫描程序**”窗口中单击“**确定**”按钮。

4. 在“**属性：<策略名称>**”窗口中，单击“**确定**”按钮。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中启用 AMSI 扫描程序

1. 在应用程序控制台树中，选择“**实时计算机保护** → **AMSI 扫描程序**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“**AMSI 扫描程序**”窗口的“**常规**”选项卡。
3. 执行下列操作之一：
   - 如果要启用 AMSI 扫描程序，请选择“**AMSI 扫描程序**”复选框。
   - 如果要禁用 AMSI 扫描程序，请清除“**AMSI 扫描程序**”复选框。
4. 在“**AMSI 扫描程序**”窗口中单击“**确定**”按钮。

如何在 Kaspersky Security Center Web Console 中启用 AMSI 扫描程序

1. **转到您要配置的策略中的 AMSI 扫描程序设置**。
   a. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
   c. 选择**应用程序设置**选项卡。
   d. 选择“**实时计算机保护**”部分。
   e. 在“**AMSI 扫描程序**”块中单击“**配置**”按钮。
   “**AMSI 扫描程序**”窗口将打开。
2. 执行下列操作之一：
   - 如果要启用 AMSI 扫描程序，请选择“**AMSI 扫描程序**”复选框。
   - 如果要禁用 AMSI 扫描程序，请清除“**AMSI 扫描程序**”复选框。
3. 在“**AMSI 扫描程序**”窗口中单击“**确定**”按钮。
4. 在“**<策略名称>**”窗口中，单击“**保存**”。

AMSI 扫描程序设置

如何在 Kaspersky Security Center 管理控制台中配置 AMSI 扫描程序设置

1. **转到您要配置的策略中的 AMSI 扫描程序设置**。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择“**策略**”选项卡。

   d. 双击策略名称打开策略属性窗口。

   e. 在策略属性窗口中，转到“**实时计算机保护**”区域。

   f. 在“**AMSI 扫描程序**”块中单击“**设置**”按钮。
   将打开“**AMSI 扫描程序**”窗口的“**常规**”选项卡。

2. 选择当运行危险脚本时 Kaspersky Industrial CyberSecurity for Nodes 要执行的操作：

   - “**通知**”。应用程序允许运行可能危险的脚本。相应事件记录在任务日志中。
   - “**阻止**”。应用程序阻止可能的危险脚本。

3. 在“**扫描复合文件**”块中，指定您希望扫描的复合文件类型：存档、分发包或 Office 格式文件。

4. 在“**大小限制**”块中执行以下操作之一：

   - 要阻止“AMSI 扫描程序”组件解压缩大型复合文件，请选中“**复合文件大于指定值时不解压**”复选框，并在“**最大文件大小(MB)**”字段中指定所需值。“AMSI 扫描程序”组件不会解压缩大于指定大小的复合文件。
   - 要允许“AMSI 扫描程序”组件解压缩大型复合文件，请取消选中“**复合文件大于指定值时不解压**”复选框。

   无论是否选中“**复合文件大于指定值时不解压**”复选框，“AMSI 扫描程序”组件均会扫描从存档中提取的大型文件。

5. 在“**AMSI 扫描程序**”窗口中单击“**确定**”按钮。

6. 在“**属性：<策略名称>**”窗口中，单击“**确定**”按钮。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中配置 AMSI 扫描程序设置

1. 在应用程序控制台树中，选择“**实时计算机保护** → AMSI **扫描程序**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“AMSI **扫描程序**”窗口的“**常规**”选项卡。
3. 选择当运行危险脚本时 Kaspersky Industrial CyberSecurity for Nodes 要执行的操作：
   - “**通知**”。应用程序允许运行可能危险的脚本。相应事件记录在任务日志中。
   - “**阻止**”。应用程序阻止可能的危险脚本。
4. 在“**扫描复合文件**”块中，指定您希望扫描的复合文件类型：存档、分发包或 Office 格式文件。
5. 在“**大小限制**”块中执行以下操作之一：
   - 要阻止“AMSI 扫描程序”组件解压缩大型复合文件，请选中“**复合文件大于指定值时不解压**”复选框，并在“**最大文件大小(MB)**”字段中指定所需值。“AMSI 扫描程序”组件不会解压缩大于指定大小的复合文件。
   - 要允许“AMSI 扫描程序”组件解压缩大型复合文件，请取消选中“**复合文件大于指定值时不解压**”复选框。

   无论是否选中“**复合文件大于指定值时不解压**”复选框，“AMSI 扫描程序”组件均会扫描从存档中提取的大型文件。
6. 在“AMSI **扫描程序**”窗口中单击“**确定**”按钮。

如何在 Kaspersky Security Center Web Console 中配置 AMSI 扫描程序设置

1. **转到您要配置的策略中的 AMSI 扫描程序设置**。
   a. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
      策略属性窗口将打开。
   c. 选择**应用程序设置**选项卡。
   d. 选择“**实时计算机保护**”部分。
   e. 在“AMSI **扫描程序**”块中单击“**配置**”按钮。
      “AMSI **扫描程序**”窗口将打开。

2. 选择当运行危险脚本时 Kaspersky Industrial CyberSecurity for Nodes 要执行的操作：

- “**通知**”。应用程序允许运行可能危险的脚本。相应事件记录在任务日志中。
- “**阻止**”。应用程序阻止可能的危险脚本。

3. 在“**扫描复合文件**”块中，指定您希望扫描的复合文件类型：存档、分发包或 Office 格式文件。

4. 在“**大小限制**”块中执行以下操作之一：

- 要阻止“AMSI 扫描程序”组件解压缩大型复合文件，请选中“**复合文件大于指定值时不解压**”复选框，并在“**最大文件大小(MB)**”字段中指定所需值。“AMSI 扫描程序”组件不会解压缩大于指定大小的复合文件。
- 要允许“AMSI 扫描程序”组件解压缩大型复合文件，请取消选中“**复合文件大于指定值时不解压**”复选框。

无论是否选中“**复合文件大于指定值时不解压**”复选框，“AMSI 扫描程序”组件均会扫描从存档中提取的大型文件。

5. 在“**AMSI 扫描程序**”窗口中单击“**确定**”按钮。

6. 在“**<策略名称>**”窗口中，单击“**保存**”。

应用程序启动控制

在运行“应用程序启动控制”任务时，Kaspersky Industrial CyberSecurity for Nodes 会监控用户启动应用程序的尝试，并允许或拒绝这些应用程序启动。“应用程序启动控制”任务依赖于“默认拒绝”原则，这意味着任务设置中不允许的任何应用程序都会被自动阻止。

您可以通过为应用程序创建应用程序启动控制允许规则来允许启动应用程序。

所有启动应用程序的尝试都将记录在任务日志中。

“应用程序启动控制”任务可以运行在以下两种模式之一：

- “**阻止**”。Kaspersky Industrial CyberSecurity for Nodes 使用应用程序启动控制规则来控制应用程序的启动。应用程序启动控制规则的范围在应用程序启动控制规则的常规设置中指定。如果应用程序满足应用程序启动控制规则，但没有任何规则与应用程序启动控制规则的范围匹配，则会阻止此类应用程序运行。

  禁止运行不受应用程序启动控制规则覆盖的应用程序。

  如果未创建任何应用程序启动控制规则或为一台受保护设备创建了超过 65,535 条应用程序启动控制规则，则“**应用程序启动控制**”任务无法在活动模式下启动。

- “**通知**”。Kaspersky Industrial CyberSecurity for Nodes 允许启动所有应用程序。仅记录有关所有应用程序启动的信息、涵盖已启动应用程序的规则以及任务运行在“**阻止**”模式时将执行的操作。默认设置此模式。

创建应用程序启动控制规则时，我们建议确保它们不会阻止操作系统的应用程序运行。

Kaspersky Industrial CyberSecurity for Nodes 还会拦截在 Linux 的 Windows 子系统下启动的进程（从 UNIX™ shell 或命令行解释器运行的脚本除外）。对于此类进程，“应用程序启动控制”任务将应用当前配置定义的操作。“应用程序启动控制规则生成器”任务会检测应用程序启动，并为在 Linux 的 Windows 子系统下运行的应用程序生成相应规则。

关于应用程序启动控制规则

应用程序启动控制规则的工作原理

应用程序启动控制规则的操作基于以下组件：

- 规则类型。

  应用程序启动控制规则可以允许或拒绝应用程序启动。相应地，它们被称为*允许*或*拒绝*规则。

- 规则使用范围。

  应用程序启动控制规则可应用于*可执行文件*、*脚本*和 *MSI 安装包*。

- 规则触发条件。

  应用程序启动控制规则规范满足规则设置中指定的至少一个触发条件的文件的启动。例如，可执行文件使用指定的“*数字证书*”签名，具有指定的 *SHA256 哈希*，位于指定*路径*，匹配指定的*命令行*参数。您必须添加至少一个规则触发条件。否则不会添加应用程序启动控制规则。

- 规则的排除项。

  您可以为应用程序启动控制规则配置排除项，该排除项可能基于与规则触发条件相同的标准。对于某些允许规则时，可能需要指定应用程序启动控制规则的排除：例如，如果您希望允许用户从 C:\Windows 路径启动应用程序，同时阻止启动文件 Regedit.exe。

- 用户或用户组。

  应用程序启动控制规则可以按特定用户或用户组控制特定应用程序的启动。

创建应用程序启动控制规则时，我们建议确保新规则不会阻止操作系统的应用程序运行。

管理应用程序启动控制规则

您可以对应用程序启动控制规则执行以下操作：

- 手动添加。
- 自动生成和添加规则。
- 删除。
- 导入和导出。
- 过滤规则列表。

关于软件分发控制

如果您想控制软件的分发，生成应用程序启动控制可能会变得更加复杂。例如，您可能希望在受保护的设备上执行此操作，其中安装的软件会定期自动更新。在这种情况下，必须在每次软件更新后更新允许规则的列表，以便在“应用程序启动控制”任务设置中考虑新创建的文件。为了简化软件分发方案中的启动控制，可以使用“软件分发控制”。

安装包（下文称为“软件包”）表示要在受保护设备上安装的一个或几个应用程序。安装包可能还包含更新和单独的命令。

“软件分发控制”子系统作为附加排除列表实施。安装包添加到列表后，会变为受信任。允许对受信任的软件包进行解压缩，并且允许从受信任的软件包安装或更新的应用程序自动启动。提取的文件可以继承主分发包的受信任属性。*主分发包*是由用户添加到软件分发控制排除列表并成为受信任包的软件包。

如果第一次启动软件包时软件分发控制关闭，或者“应用程序启动控制”组件未安装，Kaspersky Industrial CyberSecurity for Nodes 仅控制应用程序分发的完整周期，无法正确处理由受信任包修改的文件的启动。

要使用软件分发控制，您必须启用常规应用程序启动控制设置中的“**将规则应用于可执行文件**”功能。

软件分发缓存

Kaspersky Industrial CyberSecurity for Nodes 使用动态生成的软件分发缓存（“分发缓存”）在受信任包与软件分发期间创建的文件之间建立关系。第一次启动软件包时，Kaspersky Industrial CyberSecurity for Nodes 将检测该软件包在软件分发过程中创建的所有文件，并将文件校验和及路径存储在分发缓存中。然后，默认情况下，所有在分发缓存中保存了信息的文件都被允许启动。

您不能通过用户界面查看、删除或手动修改分发缓存。缓存由 Kaspersky Industrial CyberSecurity for Nodes 填充和控制。

您可以将分发缓存导出到配置文件（XML 格式），或使用命令行删除分发缓存。

要将分发缓存导出到配置文件，请执行以下命令：

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

要删除分发缓存，请执行以下命令：

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Industrial CyberSecurity for Nodes 每 24 小时更新一次分发缓存。如果先前允许的文件的校验和发生变化，应用程序将从分发缓存中删除此文件的记录。如果“应用程序启动控制”任务在活动模式下启动，后续启动该文件的尝试将被阻止。如果先前允许的文件的完整路径发生变化，后续启动该文件的尝试不会被阻止，因为校验和存储在分发缓存内。

处理提取的文件

在第一次打开排除列表中的软件分发包时，受信任的主分发包（在嵌套的第一级）所创建的提取文件和包会在它们的校验和被添加到分发缓存时继承受信任属性。因此，分发包本身和从该分发包提取的所有文件也将被信任。

例如，如果将包含多个软件包和应用程序的软件包 test.msi 添加到排除列表并启用“**允许将所有子文件作为受信任的分发包启动**”功能，则可以解压并运行 test.msi 软件包中包含的所有软件包和应用程序，即使它们包含其他嵌套文件。此方案适用于所有嵌套级别上的提取文件。

如果将 test.msi 包添加到排除列表中，并且“**允许将所有子文件作为受信任的分发包启动**”功能被禁用，应用程序仅将受信任属性分配给直接从受信任数据包中提取的软件包和可执行文件（在第一级嵌套）。此类文件的校验和存储在分发缓存中。在第二个和更后面的嵌套级别上的所有文件都将被“默认拒绝”原则阻止。

操作系统重新启动后，提取的文件将保留受信任属性。

要从所有提取的文件中删除继承属性，您必须删除分发缓存并禁用“**允许将所有子文件作为受信任的分发包启动**”功能，然后再次运行受信任的安装包。

使用应用程序启动控制规则列表

软件分发控制的受信任包列表是一个排除项列表，该列表扩大了但未替换应用程序启动控制规则常规列表。

拒绝应用程序启动控制规则具有最高优先级：受信任包的解压缩和新文件或已修改文件的启动将被阻止（如果这些包和文件受应用程序启动控制拒绝规则影响）。

软件分发控制排除项适用于受信任包和这些包创建或修改的文件（如果应用程序启动控制列表中没有拒绝规则适用于这些包和文件）。

关于应用程序启动控制规则生成器

您可使用 Kaspersky Security Center 任务和策略同时为公司网络上的所有受保护设备和受保护设备组创建应用程序启动控制规则列表。如果公司网络没有参考计算机，并且您无法基于模板机上安装的应用程序创建允许规则列表，则建议使用下面列出的方案。

您可以通过应用程序控制台在本地运行“应用程序启动控制规则生成器”任务，以基于单台受保护设备上运行的应用程序创建规则列表。

您可以使用以下方式之一在 Kaspersky Security Center 一侧创建应用程序启动控制规则列表：

- 使用“应用程序启动控制规则生成器”组任务。

  在此方案下，一个组任务会为网络上的每台受保护设备生成其自己的应用程序启动控制规则列表，并将这些列表保存到指定共享文件夹中的 XML 文件。“应用程序启动控制规则生成器”任务生成的 XML 文件包含该任务启动前在应用程序启动控制任务设置中指定的允许规则。对于在任务设置中不允许启动的应用程序，不会创建任何规则。默认情况下将拒绝此类应用程序启动。然后，您可将创建的规则列表手动导入 Kaspersky Security Center 策略中的“应用程序启动控制”任务设置。

  您可将生成的规则配置为自动导入“应用程序启动控制”任务的规则列表中。

  当您需要快速创建应用程序启动控制规则列表时，推荐使用此方案。建议仅当允许规则使用范围包含已知安全的文件夹和文件时，才配置“应用程序启动控制规则生成器”任务的计划启动。

  在网络中使用“应用程序启动控制”任务之前，请确保所有受保护设备都能够访问共享文件夹。如果组织的策略未规定使用网络中的共享文件夹，建议在测试受保护设备组中的受保护设备或参考计算机上启动“应用程序启动控制规则生成器”任务。

- 根据 Kaspersky Security Center 中针对应用程序启动控制任务生成的事件报告，运行在“*通知*”模式。

  在此方案下，Kaspersky Industrial CyberSecurity for Nodes 不拒绝应用程序启动。相反，当“应用程序启动控制”在“*通知*”模式下运行时，它会在 Kaspersky Security Center 中的管理服务器节点的工作区的“**事件**”选项卡中报告所有网络受保护设备中所有已允许和已拒绝的应用程序启动。Kaspersky Security Center 使用报告来生成一个拒绝了应用程序启动的事件列表。

  您需要配置任务执行期限，以便在指定时间期限内执行所有可能的涉及受保护设备和受保护设备组的方案以及至少一次受保护设备重新启动。任务执行期限结束后，您可从保存的 Kaspersky Security Center 事件报告（TXT 格式）导入应用程序启动数据，并基于该数据为此类应用程序生成应用程序启动控制允许规则。

  如果公司网络包含大量不同类型的受保护设备（安装了不同的软件），则推荐使用此方案。

- 根据通过 Kaspersky Security Center 接收到的拒绝应用程序启动事件，无需创建和导入配置文件。

  要使用此功能，必须在有效的 Kaspersky Security Center 策略下运行受保护设备上的应用程序启动控制任务。在本例中，受保护设备上的所有事件均被发送到管理服务器。

推荐当网络受保护设备上安装的应用程序集合更改时（例如，安装更新或重新安装操作系统时）更新规则列表。建议通过在测试管理组中的受保护设备上以“*通知*”模式运行“应用程序启动控制规则生成器”任务或“应用程序启动控制”任务来生成更新的规则列表。测试管理组包含在网络受保护设备上安装新的应用程序之前对这些应用程序的启动进行测试所需的受保护设备。

包含允许规则列表的 XML 文件基于在受保护设备上启动的任务分析创建。为了在生成规则列表时将网络上使用的所有应用程序考虑在内，建议在模板机上以“*通知*”模式启动“应用程序启动控制规则生成器”任务和“应用程序启动控制”任务。

在基于参考计算机上启动的应用程序生成允许规则之前，确保模板机是安全的，并且不包含任何恶意软件。

添加允许规则之前，请选择其中一个可用的规则应用模式。Kaspersky Security Center 策略规则列表将仅显示由策略指定的那些规则，与规则应用模式无关。本地规则列表包括所有已应用的规则 — 本地规则和通过策略添加的规则。

启用并配置应用程序启动控制

如何在 Kaspersky Security Center 管理控制台中启用和配置应用程序启动控制的常规设置

1. **转到您要配置的策略中的应用程序启动控制设置**。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择**策略**选项卡。

   d. 双击要配置的策略名称。

   e. 在策略属性窗口中，转到“**本地活动控制**”区域。

   f. 在“**应用程序启动控制**”块中单击“**设置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 使用同名的复选框启用“**应用程序启动控制**”。

3. 在“**阻止规则的操作模式**”块中，配置以下设置：

   - 任务运行模式：

     - “**阻止**”。Kaspersky Industrial CyberSecurity for Nodes 应用所有创建的应用程序启动控制规则。

     - “**通知**”。Kaspersky Industrial CyberSecurity for Nodes 不使用应用程序启动控制规则。它仅在任务日志中记录有关应用程序启动的信息。所有应用程序均允许启动。您可以使用此模式根据任务日志中记录的有关拒绝的应用程序启动的信息应用程序启动控制规则生成器列表。

- **在该文件的所有后续启动中重复对第一次文件启动所采取的操作**。
- **拒绝在没有要执行的命令的情况下启动命令解释器**。

4. 在“**规则使用范围**”块中，配置以下设置：
   - **将规则应用于可执行文件**。
   - **监控 DLL 模块的加载**。

     控制 DLL 模块的加载可能影响操作系统的性能。

   - **将规则应用于脚本和 MSI 包**。
5. 在“**证书监控**”下，启用或禁用“**验证证书时忽略缺少的签名时间戳**”功能。
6. 在“**应用程序启动控制**”窗口中，单击“**确定**”保存更改。

Kaspersky Industrial CyberSecurity for Nodes 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中启用和配置应用程序启动控制的常规设置

1. 在应用程序控制台树中，选择“**计算机控制 → 应用程序启动控制**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。
3. 使用同名的复选框启用“**应用程序启动控制**”。
4. 在“**阻止规则的操作模式**”块中，配置以下设置：
   - 任务运行模式：
     - “**阻止**”。Kaspersky Industrial CyberSecurity for Nodes 应用所有创建的应用程序启动控制规则。
     - “**通知**”。Kaspersky Industrial CyberSecurity for Nodes 不使用应用程序启动控制规则。它仅在任务日志中记录有关应用程序启动的信息。所有应用程序均允许启动。您可以使用此模式根据任务日志中记录的有关拒绝的应用程序启动的信息应用程序启动控制规则生成器列表。
   - **在该文件的所有后续启动中重复对第一次文件启动所采取的操作**。
   - **拒绝在没有要执行的命令的情况下启动命令解释器**。

5. 在“**规则使用范围**”块中，配置以下设置：

- **将规则应用于可执行文件**。
- **监控 DLL 模块的加载**。

  控制 DLL 模块的加载可能影响操作系统的性能。

- **将规则应用于脚本和 MSI 包**。

6. 在“**证书监控**”下，启用或禁用“**验证证书时忽略缺少的签名时间戳**”功能。

7. 在“**应用程序启动控制**”窗口中，单击“**确定**”保存更改。

Kaspersky Industrial CyberSecurity for Nodes 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

如何在 Kaspersky Security Center Web Console 中启用和配置应用程序启动控制的常规设置

1. **转到您要配置的策略中的应用程序启动控制设置**。

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

   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

   c. 选择**应用程序设置**选项卡。

   d. 选择“**本地活动控制**”部分。

   e. 在“**应用程序启动控制**”块中单击“**配置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 使用同名的复选框启用“**应用程序启动控制**”。

3. 在“**阻止规则的操作模式**”块中，配置以下设置：

- 任务运行模式：
  - “**阻止**”。Kaspersky Industrial CyberSecurity for Nodes 应用所有创建的应用程序启动控制规则。
  - “**通知**”。Kaspersky Industrial CyberSecurity for Nodes 不使用应用程序启动控制规则。它仅在任务日志中记录有关应用程序启动的信息。所有应用程序均允许启动。您可以使用此模式根据任务日志中记录的有关拒绝的应用程序启动的信息应用程序启动控制规则生成器列表。
- **在该文件的所有后续启动中重复对第一次文件启动所采取的操作**。
- **拒绝在没有要执行的命令的情况下启动命令解释器**。

4. 在“**规则使用范围**”块中，配置以下设置：

   - **将规则应用于可执行文件**。
   - **监控 DLL 模块的加载**。

     控制 DLL 模块的加载可能影响操作系统的性能。

   - **将规则应用于脚本和 MSI 包**。

5. 在“**证书监控**”下，启用或禁用“**验证证书时忽略缺少的签名时间戳**”功能。

6. 在“**应用程序启动控制**”窗口中，单击“**确定**”保存更改。

7. 保存修改的策略。

Kaspersky Industrial CyberSecurity for Nodes 将对正在运行的任务立即应用新设置。有关设置修改日期和时间以及修改前后任务设置值的信息保存在系统审核日志中。

配置软件分发控制

如何在 Kaspersky Security Center 管理控制台中配置软件分发控制

1. **转到您要配置的策略中的应用程序启动控制设置**。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择**策略**选项卡。

   d. 双击要配置的策略名称。

   e. 在策略属性窗口中，转到“**本地活动控制**”区域。

   f. 在“**应用程序启动控制**”块中单击“**设置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**软件分发控制**选项卡。

3. 启用“**自动允许通过列出的应用程序和软件包进行软件分发**”功能。

   您可以启用“**自动允许通过列出的应用程序和软件包进行软件分发**”功能，如果在“**常规**”选项卡上，“**将规则应用于可执行文件**”功能已启用。

4. 如果有必要，请禁用“**始终允许通过 Windows Installer 进行软件分发**”功能。

关闭此功能可能导致更新操作系统文件出问题，还可能阻止从分发包中提取的文件启动。

5. 如果需要，启用“**始终允许使用后台智能传输服务通过 SCCM 进行软件分发**”功能。

应用程序控制受保护设备上从软件包传送到安装或更新的软件分发周期。如果在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes 之前已执行分发的任何阶段，则应用程序不会控制过程。

6. 添加您想要允许启动的可执行文件和安装包：

- **手动添加一个**

  a. 在“**Add** ”按钮的上下文菜单中，选择“**添加一个分发包**”。

  b. 单击打开的窗口中的“**浏览**”按钮。

  c. 选择可执行文件或分发包。
  “**信任标准**”下的字段会自动填充有关所选文件的信息。

  d. 如果需要，启用“**允许将所有子文件作为受信任的分发包启动**”功能。

  e. 选择决定可执行文件或安装包是否受信任的标准：**证书详情**或者**SHA256 哈希**。

  f. 单击“**确定**”。

  可执行文件或安装包已添加到列表中。

- **按哈希添加多项**

  a. 在“**Add** ”按钮的上下文菜单中，选择“**按哈希添加多个包**”。

  b. 这将打开一个窗口；在该窗口中，选择任意数量的文件或安装包。

  c. 点击“**打开**”。

  可执行文件或安装包被添加到列表中。SHA256 哈希在其属性中指定。

- **从文件导入**

  a. 单击“**导入**”。

  b. 在打开的窗口中，选择包含有关可执行文件和安装包信息的 .TXT 文件。

  c. 点击“**打开**”。

可执行文件或安装包被添加到列表中。SHA256 哈希在其属性中指定。

如果基于可执行文件创建受信任分发包，并且在受信任区域设置中基于同一可执行文件添加了一个进程，并使其受“应用程序启动控制”任务信任，则受信任区域设置具有更高的优先级。Kaspersky Industrial CyberSecurity for Nodes 会阻止此可执行文件启动，但认为该可执行文件的进程是受信任的。

7. 如有必要，可通过单击“**编辑**”按钮编辑添加的可执行文件和安装包列表。
8. 如果需要，可通过单击“**删除** ”按钮删除添加的可执行文件和安装包。在这种情况下，解包后的可执行文件可以运行。

为了防止执行解压后的可执行文件，您必须从受保护的设备中删除 Kaspersky Industrial CyberSecurity for Nodes ，或者为解压后的文件创建应用程序启动控制拒绝规则。

9. 单击“**确定**”。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中配置软件分发控制

1. 在应用程序控制台树中，选择“**计算机控制** → **应用程序启动控制**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。
3. 选择**软件分发控制**选项卡。
4. 启用“**自动允许通过列出的应用程序和软件包进行软件分发**”功能。

您可以启用“**自动允许通过列出的应用程序和软件包进行软件分发**”功能，如果在“**常规**”选项卡上，“**将规则应用于可执行文件**”功能已启用。

5. 如果有必要，请禁用“**始终允许通过 Windows Installer 进行软件分发**”功能。

关闭此功能可能导致更新操作系统文件出问题，还可能阻止从分发包中提取的文件启动。

6. 如果需要，启用“**始终允许使用后台智能传输服务通过 SCCM 进行软件分发**”功能。

应用程序控制受保护设备上从软件包传送到安装或更新的软件分发周期。如果在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes 之前已执行分发的任何阶段，则应用程序不会控制过程。

7. 添加您想要允许启动的可执行文件和安装包：

- **手动添加一个**

  a. 在“Add ”按钮的上下文菜单中，选择“**添加一个分发包**”。

  b. 单击打开的窗口中的“**浏览**”按钮。

  c. 选择可执行文件或分发包。
  “**信任标准**”下的字段会自动填充有关所选文件的信息。

  d. 如果需要，启用“**允许将所有子文件作为受信任的分发包启动**”功能。

  e. 选择决定可执行文件或安装包是否受信任的标准：**证书详情**或者**SHA256 哈希**。

  f. 单击“**确定**”。

  可执行文件或安装包已添加到列表中。

- **按哈希添加多项**

  a. 在“Add ”按钮的上下文菜单中，选择“**按哈希添加多个包**”。

  b. 这将打开一个窗口；在该窗口中，选择任意数量的文件或安装包。

  c. 点击“**打开**”。

  可执行文件或安装包被添加到列表中。SHA256 哈希在其属性中指定。

- **从文件导入**

  a. 单击“**导入**”。

  b. 在打开的窗口中，选择包含有关可执行文件和安装包信息的 .TXT 文件。

  c. 点击“**打开**”。

  可执行文件或安装包被添加到列表中。SHA256 哈希在其属性中指定。

如果基于可执行文件创建受信任分发包，并且在受信任区域设置中基于同一可执行文件添加了一个进程，并使其受“应用程序启动控制”任务信任，则受信任区域设置具有更高的优先级。Kaspersky Industrial CyberSecurity for Nodes 会阻止此可执行文件启动，但认为该可执行文件的进程是受信任的。

8. 如有必要，可通过单击“**编辑**”按钮编辑添加的可执行文件和安装包列表。

9. 如果需要，可通过单击“**删除**”按钮删除添加的可执行文件和安装包。在这种情况下，解包后的可执行文件可以运行。

   为了防止执行解压后的可执行文件，您必须从受保护的设备中删除 Kaspersky Industrial CyberSecurity for Nodes，或者为解压后的文件创建应用程序启动控制拒绝规则。

10. 单击“**确定**”。

如何在 Kaspersky Security Center Web Console 中配置软件分发控制

1. **转到您要配置的策略中的应用程序启动控制设置**。

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

   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

   c. 选择**应用程序设置**选项卡。

   d. 选择“**本地活动控制**”部分。

   e. 在“**应用程序启动控制**”块中单击“**配置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**软件分发控制**选项卡。

3. 启用“**自动允许通过所列应用程序和软件包分发软件**”功能。

   您可以启用“**自动允许通过所列应用程序和软件包分发软件**”功能，如果在“**常规**”选项卡上，“**将规则应用于可执行文件**”功能已启用。

4. 如果有必要，请禁用“**始终允许通过 Windows Installer 进行软件分发**”功能。

   关闭此功能可能导致更新操作系统文件出问题，还可能阻止从分发包中提取的文件启动。

5. 如果需要，启用“**始终允许使用后台智能传输服务通过 SCCM 进行软件分发**”功能。

   应用程序控制受保护设备上从软件包传送到安装或更新的软件分发周期。如果在受保护设备上安装 Kaspersky Industrial CyberSecurity for Nodes 之前已执行分发的任何阶段，则应用程序不会控制过程。

6. 添加您想要允许启动的可执行文件和安装包：

- **手动**

  a. 单击“**添加**”按钮。

  b. 在“**信任条件**”下，选择决定可执行文件或安装包是否受信任的标准：**使用数字证书**或者**使用 SHA256 哈希**。

  c. 如果您选择了“**使用数字证书**”，输入对可执行文件或安装包签名的证书的标头和指纹，以及可执行文件或安装包的名称。

  d. 如果您选择了“**使用 SHA256 哈希**”，点击“**浏览**”选择可执行文件或安装包。

  e. 如果需要，启用“**允许启动所有受信任分发包形式的子文件**”功能。

  f. 单击“**确定**”。

  可执行文件或安装包已添加到列表中。

- **从文件导入**

  a. 单击“**导入**”。

  b. 在打开的窗口中，选择包含有关可执行文件和安装包信息的 .TXT 文件。

  c. 单击**打开**按钮。

  可执行文件或安装包被添加到列表中。SHA256 哈希在其属性中指定。

如果基于可执行文件创建受信任分发包，并且在受信任区域设置中基于同一可执行文件添加了一个进程，并使其受“应用程序启动控制”任务信任，则受信任区域设置具有更高的优先级。Kaspersky Industrial CyberSecurity for Nodes 会阻止此可执行文件启动，但认为该可执行文件的进程是受信任的。

7. 如有必要，可通过单击“**编辑**”按钮编辑添加的可执行文件和安装包列表。

8. 如果需要，可通过单击“**删除** ”按钮删除添加的可执行文件和安装包。在这种情况下，解包后的可执行文件可以运行。

为了防止执行解压后的可执行文件，您必须从受保护的设备中删除 Kaspersky Industrial CyberSecurity for Nodes ，或者为解压后的文件创建应用程序启动控制拒绝规则。

9. 单击“**确定**”。

10. 在“**应用程序启动控制**”窗口中单击“**确定**”按钮。

使用应用程序启动控制规则

本节提供创建应用程序启动控制规则列表的说明。

添加应用程序启动控制规则

如何在 Kaspersky Security Center 管理控制台中添加应用程序启动控制规则

1. **转到您要配置的策略中的应用程序启动控制设置**。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择**策略**选项卡。

   d. 双击要配置的策略名称。

   e. 在策略属性窗口中，转到“**本地活动控制**”区域。

   f. 在“**应用程序启动控制**”块中单击“**设置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**规则**选项卡。

3. 在“**规则使用**”下拉列表中，选择应用程序模式：

   - “**将策略规则添加到本地规则**”。应用程序将与本地规则列表一起应用策略中指定的规则列表。
   - “**使用策略规则替换本地规则**”。应用程序将针对受保护设备组上的应用程序启动控制应用策略中指定的规则列表。不能创建、编辑或应用本地规则列表。

4. 如果需要，启用“**拒绝用户修改本地规则**”功能。
   如果启用此功能，应用程序将不允许在应用程序控制台中本地编辑应用程序启动控制规则。默认禁用此选项。

5. 通过以下方式之一添加应用程序启动控制规则：

   - **手动**。

     a. 单击“**添加**”。
     “**应用程序启动控制**”窗口将打开。

     b. 在“**名称**”字段中输入规则的名称。

c. 如有必要，在“**描述**”字段中输入规则的描述。

d. 在“**类型**”下拉列表中，选择规则类型：

- **允许**，如果您希望该规则允许运行规则描述的应用程序。
- **拒绝**，如果您希望该规则阻止启动该规则描述的应用程序。

e. 在“**范围**”下拉列表中，选择将由规则控制执行的文件类型：

- **可执行文件**，如果您希望规则控制可执行文件的启动。
- **脚本和 MSI 包**，如果希望规则控制脚本和 MSI 数据包的启动。支持以下扩展名的文件：.js、.vbs、.cmd、.bat、.py、.ps1、.pl、.msi、.msp、.mst、.com、.vbe、.jse、.psd1、.psm1、

f. 如果您想让 Kaspersky Industrial CyberSecurity for Nodes 将匹配规则触发条件的应用程序视为受信任更新程序，请选择“**受信任更新程序**”复选框。受信任更新程序是允许创建其他可执行文件的应用程序，这些文件随后将被允许运行。

如果一个应用程序触发多个规则，如果满足以下条件，Kaspersky Industrial CyberSecurity for Nodes 设置“*受信任的更新程序*”标志：

- 所有规则都允许应用程序运行。
- 至少有一条规则选中了“**受信任更新程序**”复选框。

g. 为应用程序启动控制规则添加触发条件。

h. 为应用程序启动控制规则添加触发条件排除项。

i. **添加允许或禁止启动满足规则的应用程序的用户和/或用户组**。

a. 选择**用户或组**选项卡。

b. 在“**添加**”按钮的上下文菜单中，选择添加用户或组的方法。

c. 这将打开一个窗口；在该窗口中，输入或选择用户或用户组的名称。

d. 单击“**确定**”。

e. 为每个用户或用户组完成步骤 b 到 d。

j. 单击“**确定**”。

- **通过导入包含应用程序启动控制规则的 XML 文件**。

  a. 在 按钮的上下文菜单中，选择“**导入 → 从 XML 文件**”条目。

  b. 选择如何将 XML 文件中的设备控制规则添加到策略中可用的规则中：

  - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
  - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
  - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不会复制具有相同设置的规则。如果至少一项规则设置是唯一的，则添加该规则。

  c. 在打开的窗口中，指定“应用程序启动控制规则生成器”本地任务或组任务完成后创建的 XML 文件的路径。

  d. 单击“**打开**”。

- **根据 Kaspersky Security Center 事件使用请求**。

  a. 在 按钮的上下文菜单中，选择“**导入 → 基于 Kaspersky Security Center 事件(请求)创建允许规则**”条目。

  b. 选择将规则添加到先前创建的应用程序启动控制规则列表中的原则：

  - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
  - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
  - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不添加具有相同设置的规则；如果至少一个规则参数是唯一的，则会添加规则。

  “**应用程序启动控制规则生成**”窗口将打开。

  c. 选择应用程序创建应用程序启动控制规则所依据的事件类型：

  - “**应用程序启动被拒绝**”。
  - “**仅统计模式: 应用程序启动被拒绝**”。

  d. 从“**在此期间内生成的请求事件**”下拉列表中选择期间。

  e. 清除或选中“**生成规则时优先考虑哈希的使用**”复选框。

  如果选中此复选框，则当文件的校验和与证书均可用时，Kaspersky Industrial CyberSecurity for Nodes 将使用文件的校验和来生成规则。

  如果清除此复选框，则当文件的校验和与证书均可用时，Kaspersky Industrial CyberSecurity for Nodes 将使用文件的数字证书来生成规则。

f. 单击“**生成规则**”。

g. 单击“**确定**”。

- **通过导入 TXT 文件，其中包含 Kaspersky Security Center 阻止的应用程序事件**

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择**策略**选项卡。
4. 双击要配置的策略名称。
5. 在策略属性窗口中，转到“**日志和通知**”区域。
6. 在“**任务日志**”块中单击“**设置**”按钮。
   “**通知**”窗口将打开。
7. 展开“**本地活动控制**”节点。
8. 选择“**应用程序启动控制**”部分。
9. 在应用程序启动控制事件列表中，在“**发送事件到 Kaspersky Security Center**”列，选中“*已禁止应用程序启动*”和“*禁止应用程序在测试模式下启动*”旁边的复选框。
10. 保存更改。
11. 在策略的“**事件配置**”部分，确保“**存储在管理服务器数据库上(天)**”字段中指定的事件存储期限大于您计划收集有关阻止应用程序启动的信息的时间段（默认为 30 天）。

    一旦应用程序启动控制任务日志保留期到期，记录的事件就会被删除，并且不会出现在报告中。

12. 激活配置的策略以收集有关被拒绝的应用程序启动的数据。
13. 如果需要，修改应用程序启动控制模式。
14. 当收集有关阻止应用程序启动的信息的期限到期时，请从“*已禁止应用程序启动*”和“*禁止应用程序在测试模式下启动*”事件中进行选择并将其导出到 TXT 文件。有关详细信息，请参阅“*Kaspersky Security Center 帮助*”中的“事件分类”部分。
15. 打开导出的 TXT 文件。
16. 如果有必要，编辑事件列表。

在导入被阻止的应用程序数据之前，请确保您导入的列表仅包含您要允许的应用程序，而不包含其他任何内容。

a. 在 按钮的上下文菜单中，选择“**导入 → 基于带有选定 Kaspersky Security Center 事件的 TXT 文件创建允许规则**”条目。

b. 选择如何将报告中的应用程序启动控制规则添加到策略中已经可用的规则列表中：

- **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不会复制具有相同设置的规则。如果至少一项规则设置是唯一的，则添加该规则。
- **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
- **替换现有规则**，如果您希望将现有规则替换为导入的规则。

c. 在打开的 Windows 系统窗口中，指定 Kaspersky Security Center 阻止设备报告中的事件导出到的 TXT 文件的路径。

d. 单击“**打开**”。

添加的应用程序启动控制规则显示在列表中。

6. 如果需要，请执行步骤 5 添加更多应用程序启动控制规则。
7. 如有必要，通过单击“**编辑**”按钮编辑添加的应用程序启动控制规则。
8. 如有必要，通过单击“**删除**”按钮删除添加的应用程序启动控制规则。
9. 单击“**确定**”。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中添加应用程序启动控制规则

1. 在应用程序控制台树中，选择“**计算机控制 → 应用程序启动控制**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。
3. 选择**规则**选项卡。
4. 通过以下方式之一添加应用程序启动控制规则：

- **手动**

a. 单击“**添加**”。
   “**应用程序启动控制**”窗口将打开。

b. 在“**名称**”字段中输入规则的名称。

c. 如有必要，在“**描述**”字段中输入规则的描述。

d. 在“**类型**”下拉列表中，选择规则类型：

- **允许**，如果您希望该规则允许运行规则描述的应用程序。
- **拒绝**，如果您希望该规则阻止启动该规则描述的应用程序。

e. 在“**范围**”下拉列表中，选择将由规则控制执行的文件类型：

- **可执行文件**，如果您希望规则控制可执行文件的启动。
- **脚本和 MSI 包**，如果希望规则控制脚本和 MSI 数据包的启动。支持以下扩展名的文件：.js、.vbs、.cmd、.bat、.py、.ps1、.pl、.msi、.msp、.mst、.com、.vbe、.jse、.psd1、.psm1、

f. 如果您想让 Kaspersky Industrial CyberSecurity for Nodes 将匹配规则触发条件的应用程序视为受信任更新程序，请选择“**受信任更新程序**”复选框。受信任更新程序是允许创建其他可执行文件的应用程序，这些文件随后将被允许运行。

如果一个应用程序触发多个规则，如果满足以下条件，Kaspersky Industrial CyberSecurity for Nodes 设置“*受信任的更新程序*”标志：

- 所有规则都允许应用程序运行。
- 至少有一条规则选中了“**受信任更新程序**”复选框。

g. 为应用程序启动控制规则添加触发条件。

h. 为应用程序启动控制规则添加触发条件排除项。

i. **添加允许或禁止启动满足规则的应用程序的用户和/或用户组**。

a. 选择**用户或组**选项卡。

b. 在“**添加**”按钮的上下文菜单中，选择添加用户或组的方法。

c. 这将打开一个窗口；在该窗口中，输入或选择用户或用户组的名称。

d. 单击“**确定**”。

e. 为每个用户或用户组完成步骤 b 到 d。

j. 单击“**确定**”。

- **通过导入包含应用程序启动控制规则的 XML 文件。**

  a. 在 按钮的上下文菜单中，选择“**导入 → 从 XML 文件**”条目。

  b. 选择如何将 XML 文件中的设备控制规则添加到策略中可用的规则中：

  - **替换现有规则**，如果您希望将现有规则替换为导入的规则。
  - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
  - **与现有规则合并**，如果您希望将导入的规则添加到现有规则列表。不会复制具有相同设置的规则。如果至少一项规则设置是唯一的，则添加该规则。

  c. 在打开的窗口中，指定“应用程序启动控制规则生成器”本地任务或组任务完成后创建的 XML 文件的路径。

  d. 单击“**打开**”。

添加的应用程序启动控制规则显示在列表中。

5. 如果需要，请执行步骤 5 添加更多应用程序启动控制规则。
6. 如有必要，通过单击“**编辑**”按钮编辑添加的应用程序启动控制规则。
7. 如有必要，通过单击“**删除**”按钮删除添加的应用程序启动控制规则。
8. 单击“**确定**”。

如何在 Kaspersky Security Center Web Console 中添加应用程序启动控制规则

1. **转到您要配置的策略中的应用程序启动控制设置**。

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

   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

   c. 选择**应用程序设置**选项卡。

   d. 选择“**本地活动控制**”部分。

   e. 在“**应用程序启动控制**”块中单击“**配置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**规则**选项卡。

3. 在“**规则应用**”下拉列表中，选择应用程序模式：

- “**将策略规则添加到本地规则**”。应用程序将与本地规则列表一起应用策略中指定的规则列表。
- “**将本地规则替换为策略规则**”。应用程序将针对受保护设备组上的应用程序启动控制应用策略中指定的规则列表。不能创建、编辑或应用本地规则列表。

4. 如果需要，启用“**拒绝用户修改本地规则**”功能。

5. 通过以下方式之一添加应用程序启动控制规则：

- **手动**

  a. 单击“**添加**”。

  “**规则设置**”窗口将打开。

  b. 在“**名称**”字段中输入规则的名称。

  c. 在“**类型**”下拉列表中，选择规则类型：

  - **允许**，如果您希望该规则允许运行规则描述的应用程序。
  - **拒绝**，如果您希望该规则阻止启动该规则描述的应用程序。

  d. 在“**范围**”下拉列表中，选择将由规则控制执行的文件类型：

  - **可执行文件**，如果您希望规则控制可执行文件的启动。
  - **脚本和 MSI 数据包**，如果希望规则控制脚本和 MSI 数据包的启动。

  e. 如果您希望应用程序阻止所有未在“**用户或组**”选项卡中列出的用户的规则描述的应用程序的启动，请选择“**拒绝其他用户**”复选框。

  f. 如果您想让 Kaspersky Industrial CyberSecurity for Nodes 将匹配规则触发条件的应用程序视为受信任更新程序，请选择“**受信任更新程序**”复选框。受信任更新程序是允许创建其他可执行文件的应用程序，这些文件随后将被允许运行。

  如果一个应用程序触发多个规则，如果满足以下条件，Kaspersky Industrial CyberSecurity for Nodes 设置“*受信任的更新程序*”标志：

  - 所有规则都允许应用程序运行。
  - 至少有一条规则选中了“**受信任更新程序**”复选框。

  g. 为应用程序启动控制规则添加触发条件。

  h. 为应用程序启动控制规则添加触发条件排除项。

  i. **添加允许或禁止启动满足规则的应用程序的用户和/或用户组**。

  a. 选择**用户或组**选项卡。

  b. 单击“**添加**”。

c. 这将打开一个窗口；在该窗口中，输入或选择用户或用户组的名称。

d. 单击“**选择**”。

e. 为每个用户或用户组完成步骤 b 到 d。

j. 单击“**确定**”。

添加的应用程序启动控制规则显示在列表中。

- **通过导入包含应用程序启动控制规则的 XML 文件。**

a. 单击“**导入**”。

b. 在显示的“**从文件导入**”窗口中单击“**选择**”按钮。

c. 指定“应用程序启动控制规则生成器”本地任务或组任务完成后创建的 XML 文件的路径。

d. 单击“**打开**”。

e. 单击“**导入**”。

导入的应用程序启动控制规则被添加到现有规则列表。不会复制具有相同设置的规则。如果至少一项规则设置是唯一的，则添加该规则。

- **通过导入包含 Kaspersky Industrial CyberSecurity for Nodes 4.0 应用程序启动控制规则的 XML 文件。**

a. 单击“**从以前版本导入**”。

b. 在显示的“**从文件导入**”窗口中单击“**选择**”按钮。

c. 指定从 Kaspersky Industrial CyberSecurity for Nodes 4.0 导出的包含应用程序启动控制规则的 XML 文件的路径。

d. 点击“**打开**”。

e. 单击“**导入**”。

导入的应用程序启动控制规则被添加到现有规则列表。不会复制具有相同设置的规则。如果至少一项规则设置是唯一的，则添加该规则。

- **通过从 Kaspersky Security Center 报告文件导入规则。**

a. 单击“**从 KSC 报告导入**”。

b. 在打开的窗口中，选择导出报告中事件的 TXT 文件。

c. 点击“**打开**”。

基于 Kaspersky Security Center 报告的规则被添加到策略中的规则列表中。

- **根据 Kaspersky Security Center 事件使用请求**

  a. 单击“**来自 KSC 事件的允许规则**”。

  “**应用程序启动控制规则生成器**”窗口将打开。

  b. 选择应用程序创建应用程序启动控制规则所依据的事件类型：

  - “**所有事件**”。
  - “**应用程序启动被拒绝**”。
  - “**仅统计模式: 应用程序启动被拒绝**”。

  c. 从“**使用在此期间内生成的事件**”下拉列表中选择期间。

  d. 清除或选中“**生成规则时优先考虑使用哈希**”复选框。

  如果选中此复选框，则当文件的校验和与证书均可用时，Kaspersky Industrial CyberSecurity for Nodes 将使用文件的校验和来生成规则。

  如果清除此复选框，则当文件的校验和与证书均可用时，Kaspersky Industrial CyberSecurity for Nodes 将使用文件的数字证书来生成规则。

  e. 如有必要，可在“**使用为一组受管理设备生成的事件**”字段指定受管理设备组的名称。

  f. 单击“**生成规则**”。

  g. 从“**添加到主列表的规则**”下拉列表中，选择将规则添加到先前创建的应用程序启动控制规则列表中的原则：

  - **添加到现有规则**，如果您希望将导入的规则添加到现有规则列表。将复制具有相同设置的规则。
  - **替换现有规则**，如果您希望将现有规则替换为导入的规则。

  h. 选择要导出到策略的应用程序启动控制规则中的规则，然后单击“**导出**”按钮。

  i. 保存更改。

6. 如果需要，请执行步骤 5 添加更多应用程序启动控制规则。
7. 如有必要，通过单击“**编辑**”按钮编辑添加的应用程序启动控制规则。
8. 如有必要，通过单击“**删除**”按钮删除添加的应用程序启动控制规则。
9. 单击“**确定**”。

为应用程序启动控制规则添加触发条件

如何在 Kaspersky Security Center 管理控制台中添加应用程序启动控制规则的触发条件

1. 转到您要配置的策略中的应用程序启动控制设置。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择**策略**选项卡。

   d. 双击要配置的策略名称。

   e. 在策略属性窗口中，转到“**本地活动控制**”区域。

   f. 在“**应用程序启动控制**”块中单击“**设置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**规则**选项卡。

3. 执行下列操作之一：

   a. 点击“**添加**”，如果您要添加新的应用程序启动控制规则。

   b. 在应用程序启动控制规则列表中，选择要添加触发条件的规则，然后单击“**编辑**”按钮。

   “**应用程序启动控制**”窗口将打开。

4. 在“**条件**”选项卡上，在“**添加**”按钮的上下文菜单中，选择应用程序启动控制规则的触发条件：

   - **文件中的信息**。选定文件的信息被用作规则触发条件。

     a. 在“**文件中的信息**”窗口中单击“**浏览**”按钮。
     将打开标准 Microsoft Windows“**打开文件** ”窗口。

     b. 选择文件。

     c. 点击“**打开**”。
     所选文件的信息显示在“**文件中的信息**”窗口。

     d. 请选择至少一个选项：

     - “**证书详情**”。如果选中此复选框，规则将不会控制使用具有指定数据的数字证书签名的应用程序的启动。
     - “**元数据**”。如果选中此复选框，规则将不会控制具有指定元数据的应用程序的启动。

- “**文件哈希**”。如果选中此复选框，规则将不会控制具有指定 SHA256 哈希的应用程序的启动。
- “**文件路径**”。如果选中此复选框，规则将不会控制在指定路径上启动应用程序。

e. 如果有必要，在“**命令行**”字段，在命令行中输入启动应用程序的命令。该规则控制此应用程序的启动。您可以使用 ? 和 * 字符来输入掩码。

> Kaspersky Industrial CyberSecurity for Nodes 无法识别包含斜线“/”的路径。在路径中使用反斜杠字符（“\”）。

f. 单击“**确定**”。

- “**驱动器类型**”。该规则控制从连接到受保护计算机的所有可移动驱动器启动的应用程序。
- “**KL 类别**”。该规则控制属于所选 KL 类别的应用程序的启动。
- “**受 KSN 信任**”。该规则控制 KSN 中受信任的应用程序的启动。
- “**不受 KSN 信任**”。该规则控制 KSN 中不受信任的应用程序的启动。
- “**受操作系统信任**”。该规则控制操作系统中受信任的应用程序的启动。

添加的条件将显示在列表中。

5. 如果有必要，请针对后续每个规则触发条件执行上一步的说明。
6. 如果需要，可以通过点击“**编辑**”按钮编辑规则触发条件。
7. 保存更改。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中添加应用程序启动控制规则的触发条件

1. 在应用程序控制台树中，选择“**计算机控制 → 应用程序启动控制**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。
3. 选择**规则**选项卡。
4. 执行下列操作之一：

   a. 点击“**添加**”，如果您要添加新的应用程序启动控制规则。

   b. 在应用程序启动控制规则列表中，选择要添加触发条件的规则，然后单击“**编辑**”按钮。

   “**应用程序启动控制**”窗口将打开。

5. 在“**条件**”选项卡上，在“**添加**”按钮的上下文菜单中，选择应用程序启动控制规则的触发条件：

- **文件中的信息**。**选定文件的信息**被用作规则触发条件。

  a. 在“**文件中的信息**”窗口中单击“**浏览**”按钮。
  将打开标准 Microsoft Windows“**打开文件** ”窗口。

  b. 选择文件。

  c. 点击“**打开**”。
  所选文件的信息显示在“**文件中的信息**”窗口。

  d. 请选择至少一个选项：

  - “**证书详情**”。如果选中此复选框，规则将不会控制使用具有指定数据的数字证书签名的应用程序的启动。
  - “**元数据**”。如果选中此复选框，规则将不会控制具有指定元数据的应用程序的启动。
  - “**文件哈希**”。如果选中此复选框，规则将不会控制具有指定 SHA256 哈希的应用程序的启动。
  - “**文件路径**”。如果选中此复选框，规则将不会控制在指定路径上启动应用程序。

  e. 如果有必要，在“**命令行**”字段，在命令行中输入启动应用程序的命令。该规则控制此应用程序的启动。您可以使用 ? 和 * 字符来输入掩码。

  > Kaspersky Industrial CyberSecurity for Nodes 无法识别包含斜线“/”的路径。在路径中使用反斜杠字符（“\”）。

  f. 单击“**确定**”。

- “**驱动器类型**”。该规则控制从连接到受保护计算机的所有可移动驱动器启动的应用程序。
- “**KL 类别**”。该规则控制属于所选 KL 类别的应用程序的启动。
- “**受 KSN 信任**”。该规则控制 KSN 中受信任的应用程序的启动。
- “**不受 KSN 信任**”。该规则控制 KSN 中不受信任的应用程序的启动。
- “**受操作系统信任**”。该规则控制操作系统中受信任的应用程序的启动。

添加的条件将显示在列表中。

6. 如果有必要，请针对后续每个规则触发条件执行上一步的说明。

7. 如果需要，可以通过点击“**编辑**”按钮编辑规则触发条件。

8. 保存更改。

如何在 Kaspersky Security Center Web Console 中添加应用程序启动控制规则的触发条件

1. 转到您要配置的策略中的应用程序启动控制设置。

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

   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

   c. 选择**应用程序设置**选项卡。

   d. 选择“**本地活动控制**”部分。

   e. 在“**应用程序启动控制**”块中单击“**配置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**规则**选项卡。

3. 单击“**添加**”。
   “**规则设置**”窗口将打开。

4. 在“**条件**”选项卡上单击“**添加**”按钮。
   “**规则设置**”窗口将打开。

5. 为应用程序启动控制规则选择触发条件：

   - **文件中的信息**。来自文件的信息被用作规则触发条件。

     a. 在“**规则触发标准**”下，请为至少一个条件指定值：

     - “**数字证书**”。如果选中此复选框，规则将不会控制使用具有指定数据的数字证书签名的应用程序的启动。
     - “**元数据**”。如果选中此复选框，规则将不会控制具有指定元数据的应用程序的启动。
     - “**SHA256 哈希**”。如果选中此复选框，规则将不会控制具有指定 SHA256 哈希的应用程序的启动。
     - “**文件路径**”。如果选中此复选框，规则将不会控制在指定路径上启动应用程序。

     b. 单击“**确定**”。

   - “**来自 KL 类别**”。该规则控制属于所选 KL 类别的应用程序的启动。
   - “**可移动驱动器**”。该规则控制从连接到受保护计算机的所有可移动驱动器启动的应用程序。
   - “**受操作系统信任**”。该规则控制操作系统中受信任的应用程序的启动。

   添加的条件将显示在列表中。

6. 如有必要，请针对后续每个规则触发条件执行说明中的第 4 步至第 5 步。

7. 如果需要，可以通过点击“**编辑**”按钮编辑规则触发条件。

8. 保存更改。

从应用程序启动控制规则范围添加排除项

如何在 Kaspersky Security Center 管理控制台中添加应用程序启动控制规则范围的排除项

1. **转到您要配置的策略中的应用程序启动控制设置**。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择**策略**选项卡。

   d. 双击要配置的策略名称。

   e. 在策略属性窗口中，转到“**本地活动控制**”区域。

   f. 在“**应用程序启动控制**”块中单击“**设置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**规则**选项卡。

3. 执行下列操作之一：

   a. 点击“**添加**”，如果您要添加新的应用程序启动控制规则。

   b. 在应用程序启动控制规则列表中，选择要添加排除项的规则，然后单击“**编辑**”按钮。

   “**应用程序启动控制**”窗口将打开。

4. 在“**排除项**”选项卡上，在“**添加**”按钮的上下文菜单中，选择创建应用程序启动控制规则范围排除项的标准：

   - **文件中的信息**。**选定文件的信息**被用做标准。

     a. 在“**文件中的信息**”窗口中单击“**浏览**”按钮。
     将打开标准 Microsoft Windows“**打开文件** ”窗口。

     b. 选择文件。

     c. 点击“**打开**”。
     所选文件的信息显示在“**文件中的信息**”窗口。

d. 请选择至少一个选项：

- “**证书详情**”。如果选中此复选框，规则将不会控制使用具有指定数据的数字证书签名的应用程序的启动。
- “**元数据**”。如果选中此复选框，规则将不会控制具有指定元数据的应用程序的启动。
- “**文件哈希**”。如果选中此复选框，规则将不会控制具有指定 SHA256 哈希的应用程序的启动。
- “**文件路径**”。如果选中此复选框，规则将不会控制在指定路径上启动应用程序。

e. 如果有必要，在“**命令行**”字段，在命令行中输入启动应用程序的命令。该规则不控制此应用程序的启动。您可以使用 ? 和 * 字符来输入掩码。

Kaspersky Industrial CyberSecurity for Nodes 无法识别包含斜线“/”的路径。在路径中使用反斜杠字符（“\”）。

f. 单击“**确定**”。

- “**驱动器类型**”。该规则不控制连接到受保护计算机的所有可移动驱动器上的应用程序的启动。
- “**KL 类别**”。该规则不控制属于所选 KL 类别的应用程序的启动。
- “**受 KSN 信任**”。该规则不控制 KSN 中受信任的应用程序的启动。
- “**不受 KSN 信任**”。该规则不控制 KSN 中不受信任的应用程序的启动。
- “**受操作系统信任**”。该规则不控制操作系统中受信任的应用程序的启动。

添加的排除项将显示在列表中。

5. 如果有必要，请按照说明的上一步从应用程序启动控制规则范围中添加每个后续排除项。
6. 如果需要，请点击“**编辑**”按钮编辑排除项。
7. 保存更改。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中添加应用程序启动控制规则范围的排除项

1. 在应用程序控制台树中，选择“**计算机控制 → 应用程序启动控制**”部分。
2. 在结果窗格中单击“**属性**”链接。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。
3. 选择**规则**选项卡。

4. 执行下列操作之一：

   a. 点击“**添加**”，如果您要添加新的应用程序启动控制规则。

   b. 在应用程序启动控制规则列表中，选择要添加排除项的规则，然后单击“**编辑**”按钮。

   “**应用程序启动控制**”窗口将打开。

5. 在“**排除项**”选项卡上，在“**添加**”按钮的上下文菜单中，选择创建应用程序启动控制规则范围排除项的标准：

   - **文件中的信息**。**选定文件的信息**被用做标准。

     a. 在“**文件中的信息**”窗口中单击“**浏览**”按钮。
     将打开标准 Microsoft Windows“**打开文件** ”窗口。

     b. 选择文件。

     c. 点击“**打开**”。
     所选文件的信息显示在“**文件中的信息**”窗口。

     d. 请选择至少一个选项：

     - “**证书详情**”。如果选中此复选框，规则将不会控制使用具有指定数据的数字证书签名的应用程序的启动。
     - “**元数据**”。如果选中此复选框，规则将不会控制具有指定元数据的应用程序的启动。
     - “**文件哈希**”。如果选中此复选框，规则将不会控制具有指定 SHA256 哈希的应用程序的启动。
     - “**文件路径**”。如果选中此复选框，规则将不会控制在指定路径上启动应用程序。

     e. 如果有必要，在“**命令行**”字段，在命令行中输入启动应用程序的命令。该规则不控制此应用程序的启动。您可以使用 ? 和 * 字符来输入掩码。

     > Kaspersky Industrial CyberSecurity for Nodes 无法识别包含斜线“/”的路径。在路径中使用反斜杠字符（“\”）。

     f. 单击“**确定**”。

   - “**驱动器类型**”。该规则不控制连接到受保护计算机的所有可移动驱动器上的应用程序的启动。
   - “**KL 类别**”。该规则不控制属于所选 KL 类别的应用程序的启动。
   - “**受 KSN 信任**”。该规则不控制 KSN 中受信任的应用程序的启动。
   - “**不受 KSN 信任**”。该规则不控制 KSN 中不受信任的应用程序的启动。
   - “**受操作系统信任**”。该规则不控制操作系统中受信任的应用程序的启动。

   添加的排除项将显示在列表中。

6. 如果有必要，请按照说明的上一步从应用程序启动控制规则范围中添加每个后续排除项。

7. 如果需要，请点击“**编辑**”按钮编辑排除项。

8. 保存更改。

如何在 Kaspersky Security Center Web Console 中添加应用程序启动控制规则范围的排除项

1. **转到您要配置的策略中的应用程序启动控制设置**。

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

   b. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

   c. 选择**应用程序设置**选项卡。

   d. 选择“**本地活动控制**”部分。

   e. 在“**应用程序启动控制**”块中单击“**配置**”按钮。
   将打开“**应用程序启动控制**”窗口的“**常规**”选项卡。

2. 选择**规则**选项卡。

3. 单击“**添加**”。
   “**规则设置**”窗口将打开。

4. 在“**排除项**”选项卡上单击“**添加**”按钮。
   “**规则设置**”窗口将打开。

5. 从应用程序启动控制规则的范围中选择创建排除项的标准：

   - “**文件中的信息**”。该规则不控制其数据与**文件中的数据**匹配的应用程序的启动。

     a. 在“**规则触发标准**”下，请为至少一个条件指定值：

     - “**数字证书**”。如果选中此复选框，规则将不会控制使用具有指定数据的数字证书签名的应用程序的启动。
     - “**元数据**”。如果选中此复选框，规则将不会控制具有指定元数据的应用程序的启动。
     - “**SHA256 哈希**”。如果选中此复选框，规则将不会控制具有指定 SHA256 哈希的应用程序的启动。
     - “**文件路径**”。如果选中此复选框，规则将不会控制在指定路径上启动应用程序。

     b. 单击“**确定**”。

- “**KL 类别**”。该规则不控制属于所选 KL 类别的应用程序的启动。
- “**驱动器类型**”。该规则不控制连接到受保护计算机的所有可移动驱动器上的应用程序的启动。
- “**受操作系统信任**”。该规则不控制操作系统中受信任的应用程序的启动。

添加的条件将显示在列表中。

6. 如果有必要，请按照说明的步骤 4 到步骤 5 从应用程序启动控制规则范围中添加每个后续排除项。
7. 如果需要，请点击“**编辑**”按钮编辑排除项。
8. 保存更改。

启用默认允许模式

您可以使用专门配置的应用程序启动控制允许规则来允许启动所有应用程序。

要允许启动所有应用程序：

1. 手动添加两个具有以下参数的应用程序启动控制允许规则：
   - 规则类型：*允许*，范围：*可执行文件*，文件路径：`?:\`。
   - 规则类型：*允许*，范围：*脚本和 MSI 包*，文件路径：`?:\`。
2. 如果已添加应用程序启动控制拒绝规则，请删除这些拒绝规则。
3. 对于所有先前创建的应用程序启动控制允许规则，删除排除项。
4. 保存更改。

生成包含 Kaspersky Security Center 阻止的应用程序事件的 TXT 文件

您可以将选定的 Kaspersky Security Center 阻止的应用程序事件导出到 TXT 文件，然后导入此数据以生成您正在配置的策略中的应用程序启动控制允许规则列表。

如何使用 Kaspersky Security Center 管理控制台生成包含 Kaspersky Security Center 阻止的应用程序事件的 TXT 文件

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择**策略**选项卡。

4. 双击要配置的策略名称。
5. 在策略属性窗口中，转到“**日志和通知**”区域。
6. 在“**任务日志**”块中单击“**设置**”按钮。
   “**通知**”窗口将打开。
7. 展开“**本地活动控制**”节点。
8. 选择“**应用程序启动控制**”部分。
9. 在应用程序启动控制事件列表中，在“**发送事件到 Kaspersky Security Center**”列，选中“*已禁止应用程序启动*”和“*禁止应用程序在测试模式下启动*”旁边的复选框。
10. 保存更改。
11. 在策略的“**事件配置**”部分，确保“**存储在管理服务器数据库上(天)**”字段中指定的事件存储期限大于您计划收集有关阻止应用程序启动的信息的时间段（默认为 30 天）。

    一旦应用程序启动控制任务日志保留期到期，记录的事件就会被删除，并且不会出现在报告中。

12. 激活配置的策略以收集有关被拒绝的应用程序启动的数据。
13. 如果需要，修改应用程序启动控制模式。
14. 当收集有关阻止应用程序启动的信息的期限到期时，请从“*已禁止应用程序启动*”和“*禁止应用程序在测试模式下启动*”事件中进行选择并将其导出到 TXT 文件。有关详细信息，请参阅“*Kaspersky Security Center 帮助*”中的“事件分类”部分。
15. 打开导出的 TXT 文件。
16. 如果有必要，编辑事件列表。

如何使用 Kaspersky Security Center Web Console 生成包含 Kaspersky Security Center 阻止的应用程序事件的 TXT 文件

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**日志和通知**”部分。
5. 在“**任务日志**”块中单击“**配置**”按钮。
   “**任务日志**”窗口将打开。
6. 选择“**应用程序启动控制**”部分。

7. 在应用程序启动控制事件列表中，在“**发送事件到 Kaspersky Security Center**”列，选中“*已禁止应用程序启动*”和“*禁止应用程序在测试模式下启动*”旁边的复选框。

8. 保存更改。

9. 在您正在配置的策略的“**事件配置**”选项卡上，请确保在“**存储在管理服务器数据库上(天)**”字段中指定的事件存储时长大于您计划收集有关阻止的应用程序启动的信息的时间段（默认为 30 天）。

   一旦应用程序启动控制任务日志保留期到期，记录的事件就会被删除，并且不会出现在报告中。

10. 激活配置的策略以收集有关被拒绝的应用程序启动的数据。

11. 如果需要，修改应用程序启动控制模式。

12. 当收集有关阻止应用程序启动的信息的期限到期时，请从“*已禁止应用程序启动*”和“*禁止应用程序在测试模式下启动*”事件中进行选择并将其导出到 TXT 文件。有关详细信息，请参阅“*Kaspersky Security Center 帮助*”中的“事件分类”部分。

13. 打开导出的 TXT 文件。

14. 如果有必要，编辑事件列表。

配置“应用程序启动控制规则生成器”组任务

如何在 Kaspersky Security Center 管理控制台中配置“应用程序启动控制规则生成器”组任务

1. **打开“应用程序启动控制规则生成器”组任务的属性**。

   a. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。

   b. 选择要为其配置任务的管理组。

   c. 选择**任务**选项卡。

   d. 在组任务列表中，双击任务名称打开“应用程序启动控制规则生成器”任务。
   “**属性: 应用程序启动控制规则生成器**”窗口将打开。

2. 转到**选项**区域。

3. 如果需要，在“**规则**”选项卡上，输入规则名称的前缀。

4. 在“**允许规则使用范围**”下，指定要用于创建允许规则的方法：

   - **基于运行的应用程序创建允许规则**
   - **为文件夹中的应用程序创建允许规则**

5. 在“**设置**”选项卡上，选择创建应用程序启动控制允许规则时任务将应用的标准：

   - **使用数字证书**。
   - **使用数字证书主题和指纹**。
   - **如果证书丢失，请使用**。
   - **使用 SHA256 哈希**。

6. 配置“**为基于哈希和生成的规则添加文件路径**”设置。

   如果选中此复选框，则在导出规则时，Kaspersky Industrial CyberSecurity for Nodes 会将可执行文件的完整路径添加到 XML 文件中。完整路径可以帮助您确定可执行文件属于哪个软件。

   如果清除该复选框，则 XML 文件仅包含可执行文件的名称和 SHA256 哈希。默认下，复选框被清除。

7. **添加您希望能够启动满足使用任务创建的规则的应用程序的用户和/或用户组**。

   a. 在“**添加**”按钮的上下文菜单中，选择添加用户或组的方法。

   b. 这将打开一个窗口；在该窗口中，输入或选择用户或用户组的名称。

   c. 单击“**确定**”。

   d. 为每个用户或用户组完成步骤 a 到 c。

8. 在“**任务完成后**”块中，配置以下设置：

   - **将允许规则添加到应用程序启动控制规则列表**。
   - **添加原则**。
   - “**将允许规则导出到文件**”。您可以点击“**浏览**”按钮指定当“应用程序启动控制规则生成器”任务完成时，Kaspersky Industrial CyberSecurity for Nodes 将允许规则导出到 XML 文件的路径。
   - **将受保护设备的详细信息添加到文件名**。

9. 如果需要，在“**排除项**”选项卡上，指定要从任务范围中排除的对象。

10. 在“**属性: 应用程序启动控制规则生成器**”窗口中单击“**确定**”按钮。

如何在 Kaspersky Security Center Web Console 中配置“应用程序启动控制规则生成器”组任务

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

2. 在组任务列表中，打开“应用程序启动控制规则生成器”任务。

   “**应用程序启动控制规则生成器**”窗口将打开。

3. 打开“**应用程序设置**”选项卡。

4. 如果有必要，在“**允许规则的使用范围**”部分中，输入规则名称的前缀。

5. 在“**允许规则的使用范围**”下，指定要用于创建允许规则的方法：

   - **基于正在运行的应用程序创建允许规则**
   - **为文件夹中的应用程序创建允许规则**

6. 在“**参数**”选项卡上，选择创建应用程序启动控制允许规则时任务将应用的标准：

   - **使用数字证书**。
   - **使用数字证书主题和指纹**。
   - **证书丢失则使用**。
   - **使用 SHA256 哈希**。

7. 配置“**为基于哈希和生成的规则添加文件路径**”设置。

   如果选中此复选框，则在导出规则时，Kaspersky Industrial CyberSecurity for Nodes 会将可执行文件的完整路径添加到 XML 文件中。完整路径可以帮助您确定可执行文件属于哪个软件。

   如果清除该复选框，则 XML 文件仅包含可执行文件的名称和 SHA256 哈希。默认下，复选框被清除。

8. **添加您希望能够启动满足使用任务创建的规则的应用程序的用户和/或用户组**。

   a. 单击“**选择用户或组**”。

   b. 这将打开一个窗口；在该窗口中，输入或选择用户或用户组的名称。

   c. 单击“**选择**”。

   d. 为每个用户或用户组完成步骤 a 到 c。

9. 在“**任务完成后**”块中，配置以下设置：

   - **将允许规则添加到应用程序启动控制规则列表**。
   - **添加原则**。
   - “**允许规则将被导出到文件。**”。在“**指定带 .xml 扩展名的文件的完整路径**”字段中，您可以指定当“应用程序启动控制规则生成器”任务完成时，Kaspersky Industrial CyberSecurity for Nodes 将允许规则导出到 XML 文件的路径。
   - **将受保护设备详细信息添加到文件名**。

10. 如果需要，在“**排除项**”选项卡上，指定要从任务范围中排除的对象。

11. 在“**应用程序启动控制规则生成器**”窗口中单击“**确定**”按钮。

使用“应用程序启动控制规则生成器”组任务创建规则。

要使用“应用程序启动控制规则生成器”组任务创建规则：

1. 创建一个“*应用程序启动控制规则生成器*”组任务或选择现有任务。
2. 配置应用程序启动控制规则生成器任务。
3. 运行“应用程序启动控制规则生成器”任务。

任务完成后，根据任务设置：

- 如果您指定了任务完成时执行的“**将允许规则添加到应用程序启动控制规则列表**”操作，生成的应用程序启动控制规则将添加到应用程序控制台中的应用程序启动控制设置列表中。
- 如果您指定了任务完成时执行的“**允许规则将被导出到文件中。**”操作，生成的应用程序启动控制规则将保存到任务设置中指定路径的 XML 文件中。

这些列表包含其类型与“应用程序启动控制规则生成器”组任务的设置匹配的应用程序启动的允许规则。

设备控制

“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，并防止丢失或泄漏数据。

设备控制提供了以下功能：

- 管理用户对存储设备（例如可移动驱动器、移动电话、CD/DVD 驱动器等）的访问权限。
- 控制没有文件系统的设备的连接（例如，外部调制解调器、蓝牙适配器、USB 键盘等）。
- 管理 Wi-Fi 连接。

默认情况下，设备控制被禁用。启用设备控制时，默认情况下，Kaspersky Industrial CyberSecurity for Nodes 拒绝访问以下设备类型：

- 可移动驱动器（包括 USB 闪存驱动器）
- 软盘
- CD/DVD 驱动器
- 便携式设备 (MTP)
- 调制解调器。
- 智能卡读卡器
- 外部网络适配器
- 蓝牙（输入设备除外）

设备控制级别

Kaspersky Industrial CyberSecurity for Nodes 在以下级别控制设备访问：

1. **设备类型**。

   将设备连接到计算机时，操作系统会确定设备的类型：打印机、可移动驱动器、CD/DVD 驱动器等。在此级别上，您可以按类型允许或拒绝设备连接。

2. **连接总线**。

   *连接总线*是用于将设备连接到计算机的接口。有些设备类型有多个连接接口。例如，您可以将打印机连接到 USB 或串行 (COM) 端口。

   在此级别，您可以根据连接总线允许或拒绝对设备的访问。

   例如，假设您拒绝通过 USB 访问。当通过 USB 连接时，Kaspersky Industrial CyberSecurity for Nodes 拒绝以“**取决于连接总线**”模式访问所有设备类型。

   > 如果为设备选择了“**允许**”或“**阻止**”访问模式，则访问控制将忽略设备的连接总线。

3. **受信任设备**。

   *受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

“设备控制”运行模式

设备控制可以工作在以下模式下：

- **主动模式**。

  Kaspersky Industrial CyberSecurity for Nodes 根据配置的设备访问规则拒绝或允许设备。应用程序还允许访问受信任设备。应用程序注册设备连接和断开连接事件。

- **通知**。

  Kaspersky Industrial CyberSecurity for Nodes 允许所有设备并记录相应事件。允许所有设备。默认设置此模式。您可以启用此模式来对组织内的设备进行审核并利用这些信息来起草一份受信任设备列表。

设备访问规则

*设备访问规则*包含一组设置，用于确定用户如何访问安装到或连接到计算机的设备。这些设置包含到特定设备的访问权限，访问计划和读写权限等。访问规则的设置组根据设备类型的不同而不同。

访问规则设置

设备	用户和/或用户组的分配	设备访问计划	读/写权限	连接总线监控
硬盘	✓	✓	✓	✓
可移动驱动器（包括 USB 闪存驱动器）	✓	✓	✓	✓
软盘	✓	✓	✓	✓
CD/DVD 驱动器	✓	✓	✓	✓
便携式设备 (MTP)	✓	✓	✓	✓
本地打印机	✓	–	–	✓
网络打印机	✓	–	–	–
调制解调器	–	–	–	✓
Streamer	–	–	–	✓
多功能设备	–	–	–	✓
智能卡读卡器	–	–	–	✓
Windows CE USB ActiveSync 设备	–	–	–	✓
外部网络适配器	–	–	–	✓
蓝牙	–	–	–	–
照相机和扫描仪	–	–	–	✓
Wi-Fi	–	–	–	–
USB 键盘	–	–	–	✓
USB 鼠标	–	–	–	✓

按类型进行设备访问控制

设备控制允许按设备类型控制对设备的访问。设备的类型由设备连接时操作系统确定。您可以使用操作系统内置的设备管理器工具找出设备类型。要管理设备访问，您需要配置规则。*设备访问规则*包含一组设置，用于确定用户如何访问安装到或连接到计算机的设备。这些设置包含到特定设备的访问权限，访问计划和读写权限等。访问规则的设置组根据设备类型的不同而不同。

您可以按如下方式配置设备访问权限：

- **允许**。

  Kaspersky Industrial CyberSecurity for Nodes 授予所有用户对设备的完全访问权限。

- **阻止**。

  Kaspersky Industrial CyberSecurity for Nodes 软件阻止设备连接。应用程序允许仅连接受信任设备。

- **取决于连接总线**。

  Kaspersky Industrial CyberSecurity for Nodes 识别设备的连接总线，并根据连接总线的访问模式执行访问控制。应用程序还允许连接受信任设备。

- **按规则**。

  对于某些设备类型，您可以选择用户或一组用户，这用户将被允许使用设备、配置设备访问计划以及读写权限。应用程序还允许连接受信任设备。

配置对“**硬盘**”类型的设备的访问时要小心。如果禁止访问系统驱动器，应用程序可能会使启动操作系统崩溃（BSOD）。

如果设备超出了设备控制分类方案，则无法限制对此类设备的访问。

如何在 Kaspersky Security Center 管理控制台中按类型控制对设备的访问

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。
5. 选择**设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。

   “**设备类型**”选项卡显示包含在设备控制组件分类的所有设备的访问规则。

8. 配置设备访问规则：

   a. 选择访问模式：**允许**、**阻止**、**取决于连接总线**、**按规则**。

      要选择“**按规则**”访问模式，必须双击以打开访问规则属性。

   b. 如果您选择“**取决于连接总线**”访问模式，必须在“**连接总线**”选项卡上配置连接接口的访问规则。

   c. 对于存储设备（例如可移动驱动器），您可以配置个人用户的访问权限。您还可以配置设备访问计划并配置读写权限。

   d. 如果有必要，配置打印规则。

   e. 如果有必要，配置 Wi-Fi 连接规则。

9. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中按类型控制对设备的访问

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。

   “**设备控制**”窗口将打开。
5. 选择**启用设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在**设备控制设置**块，单击**设备和 wi-fi 网络的访问规则**。

   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。
8. 配置设备访问规则：

   a. 选择访问模式：**允许**、**阻止**、**取决于连接总线**、**按规则**。

      如果下拉菜单中没有访问模式，请双击设备类型打开访问规则的属性。

   b. 如果您选择“**取决于连接总线**”访问模式，您必须返回到常规设备控制设置的窗口，单击“**连接总线**”，并配置连接接口的访问规则。

   c. 对于存储设备（例如可移动驱动器），您可以配置个人用户的访问权限。您还可以配置设备访问计划并配置读写权限。

   d. 如果有必要，配置打印规则。

   e. 如果有必要，配置 Wi-Fi 连接规则。

9. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中按类型控制设备访问

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制**”窗口将打开。
3. 选择**设备控制**复选框。
4. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。
6. 配置设备访问规则：
   a. 选择访问模式：**允许**、**阻止**、**取决于连接总线**、**根据规则**。
      要选择“**根据规则**”访问模式，必须双击以打开访问规则属性。
   b. 如果您选择“**取决于连接总线**”访问模式，必须在“**连接总线**”选项卡上配置连接接口的访问规则。
   c. 对于存储设备（例如可移动驱动器），您可以配置个人用户的访问权限。您还可以配置设备访问计划并配置读写权限。
   d. 如果有必要，配置打印规则。
   e. 如果有必要，配置 Wi-Fi 连接规则。
7. 保存更改。

因此，当用户试图访问设备时，应用程序会根据规则阻止访问。Kaspersky Industrial CyberSecurity for Nodes 也记录相应事件。如果您想授予单个设备访问权限，您可以将这些设备添加到受信任设备列表中。

Wi-Fi 连接控制

设备控制允许管理计算机（终端）的 Wi-Fi 连接。公共 Wi-Fi 网络可能不安全，使用此类网络可能会导致数据丢失。设备控制允许您阻止用户连接到 Wi-Fi 或仅允许连接到受信任的网络。例如，您可以只允许连接到足够安全的公司 Wi-Fi 网络。设备控制将阻止访问除受信任列表中指定的 Wi-Fi 网络之外的所有网络。

在运行 Windows 11 的计算机上，您需要启用定位服务才能控制 Wi-Fi 连接。为此，您需要启用操作系统设置中的“**定位服务**”开关（**设置** → **隐私&安全** → **位置**）。如果禁用定位服务，Kaspersky Industrial CyberSecurity for Nodes 将不会控制与 Wi-Fi 网络的连接。

如何在 Kaspersky Security Center 管理控制台中限制 Wi-Fi 连接

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。
5. 选择**设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   “**设备类型**”选项卡显示包含在设备控制组件分类的所有设备的访问规则。
8. 对 **Wi-Fi** 设备，配置访问规则：
   a. 选择访问模式：**允许**、**阻止**、**阻止但带有例外**。
   b. 如果您选择了“**阻止但带有例外**”模式，您必须创建一个受信任的 Wi-Fi 网络列表：
      1. 双击“**Wi-Fi**”设备类型打开受信任的 Wi-Fi 网络列表。
      2. 单击打开的窗口中的“**添加**”按钮。
      3. 这将打开一个窗口；在该窗口中，配置受信任的 Wi-Fi 网络：
         - “**网络名称**”。Wi-Fi 网络的名称或 SSID（Service Set Identifier）。
         - “**身份验证类型**”。连接到 Wi-Fi 网络时使用的身份验证类型。
         - “**加密类型**”。用于保护 Wi-Fi 流量的加密类型。
         - “**注释**”。有关添加的 Wi-Fi 网络的更多信息。

      您可以在路由器设置中查看受信任的 Wi-Fi 网络的设置。

      > 如果某个 Wi-Fi 网络的设置匹配规则中指定的所有设置则其被认定为受信任。

9. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中限制 Wi-Fi 连接

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。
4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。
   “**设备控制**”窗口将打开。
5. 选择**启用设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在**设备控制设置**块，单击**设备和 wi-fi 网络的访问规则**。
   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。
8. 双击“**Wi-Fi**”设备类型来打开访问规则属性。
9. 选择访问模式：**允许**、**阻止**、**阻止但带有例外**。
10. 如果您选择了“**阻止但带有例外**”模式，您必须创建一个受信任的 Wi-Fi 网络列表：
    1. 在“**受信任的 Wi-Fi 网络**”块中单击“**添加**”按钮。
    2. 这将打开一个窗口；在该窗口中，配置受信任的 Wi-Fi 网络：
       - “**网络名称**”。Wi-Fi 网络的名称或 SSID（Service Set Identifier）。
       - “**身份验证类型**”。连接到 Wi-Fi 网络时使用的身份验证类型。
       - “**加密类型**”。用于保护 Wi-Fi 流量的加密类型。
       - “**注释**”。有关添加的 Wi-Fi 网络的更多信息。

    您可以在路由器设置中查看受信任的 Wi-Fi 网络的设置。

    > 如果某个 Wi-Fi 网络的设置匹配规则中指定的所有设置则其被认定为受信任。

11. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中限制 Wi-Fi 连接

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制**”窗口将打开。
3. 选择**设备控制**复选框。
4. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。

6. 对“**Wi-Fi**”设备，配置访问规则：

   a. 选择访问模式：**允许**、**阻止**、**阻止但带有例外**。

   b. 如果您选择了“**阻止但带有例外**”模式，您必须创建一个受信任的 Wi-Fi 网络列表：

      1. 双击“**Wi-Fi**”设备类型打开受信任的 Wi-Fi 网络列表。

      2. 单击打开的窗口中的“**添加**”按钮。

      3. 这将打开一个窗口；在该窗口中，配置受信任的 Wi-Fi 网络：

         - “**网络名称**”。Wi-Fi 网络的名称或 SSID（Service Set Identifier）。
         - “**身份验证类型**”。连接到 Wi-Fi 网络时使用的身份验证类型。
         - “**加密类型**”。用于保护 Wi-Fi 流量的加密类型。
         - “**注释**”。有关添加的 Wi-Fi 网络的更多信息。

      您可以在路由器设置中查看受信任的 Wi-Fi 网络的设置。

      如果某个 Wi-Fi 网络的设置匹配规则中指定的所有设置则其被认定为受信任。

7. 保存更改。

因此，当用户尝试连接到未列为受信任的 Wi-Fi 网络时，应用程序会阻止连接。

打印控制

设备控制允许配置用户对本地和网络打印机的访问。

本地打印机控制

Kaspersky Industrial CyberSecurity for Nodes 通过以下总线控制本地打印机连接：USB、串行端口（COM）、并行端口（LPT）。

Kaspersky Industrial CyberSecurity for Nodes 仅在总线级别控制本地打印机与 COM 和 LPT 端口的连接。即，要防止打印机连接到 COM 和 LPT 端口，对于“**本地打印机**”设备类型，选择“**取决于连接总线**”模式并禁止将设备连接到 COM 和 LPT 总线。

对于连接到 USB 的打印机，应用程序在两个级别上进行控制：设备类型（本地打印机）和连接总线（USB）。

你可以选择以下模式之一通过 USB 访问本地打印机：

- “**允许**”。Kaspersky Industrial CyberSecurity for Nodes 授予所有用户对本地打印机的完全访问权限。用户可以连接打印机并使用操作系统提供的方式打印文档。
- “**阻止**”。Kaspersky Industrial CyberSecurity for Nodes 阻止本地打印机的连接。应用程序仅允许连接受信任的打印机。
- “**取决于连接总线**”。Kaspersky Industrial CyberSecurity for Nodes 允许根据 USB 总线连接状态（**允许** 或**阻止** ）连接到本地打印机。
- “**根据规则**”。要控制打印，您必须添加*打印规则*。在规则中，您可以选择要允许或阻止在本地打印机上打印文档的用户或用户组。

网络打印机控制

Kaspersky Industrial CyberSecurity for Nodes 允许配置对网络打印机上打印的访问。您可以选择以下网络打印机访问模式之一：

- **允许且不记录** 。 Kaspersky Industrial CyberSecurity for Nodes 不控制网络打印机上的打印。该应用程序向所有用户授予打印访问权限，并且不会将有关打印的信息保存到事件日志中。
- **允许** 。Kaspersky Industrial CyberSecurity for Nodes 向所有用户授予在网络打印机上打印的权限。
- **阻止** 。Kaspersky Industrial CyberSecurity for Nodes 限制所有用户访问网络打印机。该应用程序仅允许访问受信任的打印机。
- “**根据规则**”。要控制打印，您必须添加*打印规则*。在规则中，您可以选择要允许或阻止在网络打印机上打印文档的用户或用户组。

为打印机添加打印规则

如何在 Kaspersky Security Center 管理控制台中添加打印规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。
5. 选择**设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   “**设备类型**”选项卡显示包含在设备控制组件分类的所有设备的访问规则。

8. 配置打印机访问规则：

   a. 对于“**本地打印机**”和“**网络打印机**”设备类型，配置访问规则：**允许**、**阻止**、**允许且不记录**（仅适用于网络打印机）、**取决于连接总线**（仅适用于本地打印机）、**根据规则**。

   b. 如果您选择“**取决于连接总线**”访问模式，必须在“**连接总线**”选项卡上配置连接接口的访问规则。

   c. 如果您选择“**根据规则**”访问模式，必须配置打印规则：

      1. 双击“**本地打印机**”和“**网络打印机**”设备类型来打开访问规则属性。

      2. 选择您要应用打印规则的用户或用户组。要执行此操作，请单击“**添加**”按钮。

         这将打开添加新打印规则的窗口。

      3. 将优先级分配到*规则条目*。规则条目包括以下属性：用户账户、操作（允许/阻止）和优先级。

         规则具有特定优先级。如果用户被添加到若干组，Kaspersky Industrial CyberSecurity for Nodes 基于具有最高优先级的规则规范设备访问。Kaspersky Industrial CyberSecurity for Nodes 允许分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

         例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

         阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Industrial CyberSecurity for Nodes 基于任何现有的阻止规则规范设备访问。

      4. 在“**操作**”下，配置用户对打印机打印的访问权限。

      5. 单击“**用户和组**”，选择要访问打印的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

      6. 单击“**确定**”。

9. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Security Center Web Console 中添加打印规则

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。

   “**设备控制**”窗口将打开。

5. 选择**启用设备控制**复选框。

6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。

7. 在**设备控制设置**块，单击**设备和 wi-fi 网络的访问规则**。

   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。

8. 配置打印机访问规则：

   a. 对于“**本地打印机**”和“**网络打印机**”设备类型，选择访问模式：**允许**、**阻止**、**允许且不记录**（仅适用于网络打印机）、**取决于连接总线**（仅适用于本地打印机）、**根据规则**。

      如果下拉菜单中没有访问模式，请双击设备类型打开访问规则的属性。

   b. 如果您选择“**取决于连接总线**”访问模式，您必须返回到常规设备控制设置的窗口，单击“**连接总线**”，并配置连接接口的访问规则。

   c. 如果需要配置打印：

      1. 双击“**本地打印机**”或“**网络打印机**”设备类型来打开访问规则属性。

      2. 选择“**根据规则**”访问模式。

      3. 选择您要应用打印规则的用户或用户组。要执行此操作，请单击“**添加**”按钮。

         这将打开添加新打印规则的窗口。

      4. 将优先级分配到*规则条目*。规则条目包括以下属性：用户账户、操作（允许/阻止）和优先级。

         规则具有特定优先级。如果用户被添加到若干组，Kaspersky Industrial CyberSecurity for Nodes 基于具有最高优先级的规则规范设备访问。Kaspersky Industrial CyberSecurity for Nodes 允许分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

         例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

         阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Industrial CyberSecurity for Nodes 基于任何现有的阻止规则规范设备访问。

      5. 在“**操作**”下，配置用户对打印机打印的访问权限。

      6. 单击“**用户和组**”，单击“**添加**”并选择要访问打印的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

      7. 单击“**确定**”。

9. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中添加打印规则

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。

2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。

   “**属性: 设备控制**”窗口将打开。

3. 选择**设备控制**复选框。

4. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。

5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。

   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。

6. 配置打印机访问规则：

   a. 对于“**本地打印机**”和“**网络打印机**”设备类型，配置访问规则：**允许**、**阻止**、**允许且不记录**（仅适用于网络打印机）、**取决于连接总线**（仅适用于本地打印机）、**根据规则**。

   b. 如果您选择“**取决于连接总线**”访问模式，必须在“**连接总线**”选项卡上配置连接接口的访问规则。

   c. 如果您选择“**根据规则**”访问模式，必须配置打印规则：

      1. 双击“**本地打印机**”和“**网络打印机**”设备类型来打开访问规则属性。

      2. 选择您要应用打印规则的用户或用户组。要执行此操作，请单击“**添加**”按钮。

         这将打开添加新打印规则的窗口。

      3. 将优先级分配到*规则条目*。规则条目包括以下属性：用户账户、操作（允许/阻止）和优先级。

         规则具有特定优先级。如果用户被添加到若干组，Kaspersky Industrial CyberSecurity for Nodes 基于具有最高优先级的规则规范设备访问。Kaspersky Industrial CyberSecurity for Nodes 允许分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

         例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

         阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Industrial CyberSecurity for Nodes 基于任何现有的阻止规则规范设备访问。

      4. 在“**操作**”下，配置用户对打印机打印的访问权限。

      5. 单击“**用户和组**”，选择要访问打印的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

      6. 单击“**确定**”。

7. 保存更改。

输入设备控制 (HID)

输入设备包括键盘、鼠标、轨迹球、触摸板和其他此类设备。您可以使用以下接口连接输入设备：USB、蓝牙、PS/2 端口、RS-232（COM）端口、IR 端口等。

Kaspersky Industrial CyberSecurity for Nodes 允许控制 USB 和蓝牙鼠标和键盘。设备控制记录输入设备的连接和断开设备。

当蓝牙设备连接或断开连接时，应用程序可能会创建有关该设备的多个事件。原因是操作系统可能会将一个蓝牙设备检测为多个不同类型的设备。Kaspersky Industrial CyberSecurity for Nodes 还管理蓝牙适配器，通过该适配器将设备作为单独的设备进行连接。这就是应用程序为每个检测到的设备创建事件的原因。

Kaspersky Industrial CyberSecurity for Nodes 允许您允许或禁止使用输入设备，以及制作受信任设备列表。

如何在 Kaspersky Security Center 管理控制台中启用设备控制

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。
5. 选择**设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   “**设备类型**”选项卡显示包含在设备控制组件分类的所有设备的访问规则。
8. 对于“**蓝牙**”设备类型，选择访问模式：**允许**、**阻止**、**允许且不记录**。
   您可以阻止或允许所有蓝牙设备，或者可以仅允许连接蓝牙输入设备（HID（人机接口设备）类）。

   > 您仅可以在 Kaspersky Security Center Web Console 中允许连接输入设备。您不能允许在管理控制台（MMC）或 Kaspersky Industrial CyberSecurity for Nodes 控制台中连接输入设备。

9. 对于“**USB 键盘**”和“**USB 鼠标**”设备类型，选择访问模式：**允许**、**阻止**、**取决于连接总线**。
10. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中启用设备控制

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。
   “**设备控制**”窗口将打开。
5. 选择**启用设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在**设备控制设置**块，单击**设备和 wi-fi 网络的访问规则**。
   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。
8. 点击“**蓝牙**”设备类型来打开访问规则属性。

9. 选择访问模式：**允许**、**阻止**、**允许且不记录**。
   您可以阻止或允许所有蓝牙设备，或者可以仅允许连接蓝牙输入设备（HID（人机接口设备）类）。
10. 对于“**USB 键盘**”和“**USB 鼠标**”设备类型，选择访问模式：**允许**、**阻止**、**取决于连接总线**。
11. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中配置设备控制

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制**”窗口将打开。
3. 选择**设备控制**复选框。
4. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。
6. 对于“**蓝牙**”设备类型，选择访问模式：**允许**、**阻止**、**允许且不记录**。
   您可以阻止或允许所有蓝牙设备，或者可以仅允许连接蓝牙输入设备（HID（人机接口设备）类）。

   > 您仅可以在 Kaspersky Security Center Web Console 中允许连接输入设备。您不能允许在管理控制台（MMC）或 Kaspersky Industrial CyberSecurity for Nodes 控制台中连接输入设备。

7. 对于“**USB 键盘**”和“**USB 鼠标**”设备类型，选择访问模式：**允许**、**阻止**、**取决于连接总线**。
8. 保存更改。

监控可移动驱动器的使用

监控可移动驱动器的使用包括：

- 监控可移动驱动器上文件的操作。
- 监控受信任的可移动驱动器的连接和断开。
  Kaspersky Industrial CyberSecurity for Nodes 允许监控所有受信任设备的连接和断开，而不仅仅是可移动驱动器。您可以在设备控制组件的通知设置中打开事件日志记录。事件具有“*信息*”严重级别。

如何在 Kaspersky Security Center 管理控制台中启用对可移动驱动器上的文件操作的监控

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。
5. 选择**设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   “**设备类型**”选项卡显示包含在设备控制组件分类的所有设备的访问规则。
8. 选择“**可移动驱动器**”设备类型，然后单击“**记录**”按钮。
   这将打事件记录窗口。
9. 选择**启用日志记录**复选框。
10. 在**文件操作**块下，选择您要监控的操作：**写入**、**删除**。
11. 在**按文件格式筛选**块，选择其操作要被设备控制所记录的文件格式。
12. 选择您要监控其使用可移动驱动器的用户或用户组。
13. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中启用对可移动驱动器上的文件操作的监控

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。
   “**设备控制**”窗口将打开。
5. 选择**启用设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在**设备控制设置**块，单击**设备和 wi-fi 网络的访问规则**。
   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。
8. 双击“**可移动驱动器**”设备类型来打开访问规则属性。

9. 在打开的窗口中，选择“**记录**”选项卡。
10. 将切换开关设置为“**记录已启用**”。
11. 在**文件操作**块下，选择您要监控的操作：**写入**、**删除**。
12. 在**按文件格式筛选**块，选择其操作要被设备控制所记录的文件格式。
13. 选择您要监控其使用可移动驱动器的用户或用户组。
14. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中启用对可移动驱动器上的文件操作的监控

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制**”窗口将打开。
3. 选择**设备控制**复选框。
4. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。
6. 选择“**可移动驱动器**”设备类型，然后单击“**记录**”按钮。
   这将打事件记录窗口。
7. 选择**启用日志记录**复选框。
8. 在**文件操作**块下，选择您要监控的操作：**写入**、**删除**。
9. 在**按文件格式筛选**块，选择其操作要被设备控制所记录的文件格式。
10. 选择您要监控其使用可移动驱动器的用户或用户组。
11. 保存更改。

结果，当用户在可移动驱动器上写入文件或删除文件时，Kaspersky Industrial CyberSecurity for Nodes 会将此类操作的信息写入事件日志并将事件发送至 Kaspersky Security Center。您可以在 Kaspersky Security Center 控制台中查看与可移动驱动器上文件关联的事件，其位于“**事件**”选项卡上“**管理服务器**”节点的工作区中。要使事件显示在本地 Kaspersky Industrial CyberSecurity for Nodes 事件日志中，您必须选择“设备控制”组件的“通知设置”中的“**文件操作已执行**”复选框。

管理对蓝牙设备的访问

Kaspersky Industrial CyberSecurity for Nodes 允许管理对蓝牙设备的访问。蓝牙设备包括无线键盘、鼠标、耳机、打印机等。您还可以使用蓝牙进行通信，例如使用移动设备。

当蓝牙设备连接或断开连接时，应用程序可能会创建有关该设备的多个事件。原因是操作系统可能会将一个蓝牙设备检测为多个不同类型的设备。Kaspersky Industrial CyberSecurity for Nodes 还管理蓝牙适配器，通过该适配器将设备作为单独的设备进行连接。这就是应用程序为每个检测到的设备创建事件的原因。

您可以选择以下访问移动设备的模式之一：

- **允许且不记录**。Kaspersky Industrial CyberSecurity for Nodes 允许连接任何蓝牙设备，并且不会在事件日志中保存有关连接的信息。您可以连接蓝牙输入设备（键盘、鼠标等）、通过蓝牙发送数据、管理其他蓝牙设备（耳机等）。
- **允许**。Kaspersky Industrial CyberSecurity for Nodes 允许连接任何蓝牙设备。您可以连接蓝牙输入设备（键盘、鼠标等）、通过蓝牙发送数据、管理其他蓝牙设备（耳机等）。
- **阻止**。Kaspersky Industrial CyberSecurity for Nodes 限制对蓝牙设备的访问。您可以仅允许连接蓝牙输入设备（人机接口设备类）。这些设备包括键盘、鼠标、操纵杆等。

无法创建受信任的蓝牙设备列表。如果您对蓝牙设备的访问受到限制，则只能连接蓝牙输入设备。

您仅可以在应用程序控制台或 Kaspersky Security Center Web Console 中允许连接输入设备。您无法在 Kaspersky Security Center 管理控制台中允许连接输入设备。

如何在 Kaspersky Security Center 管理控制台中配置蓝牙设备访问规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**本地活动控制 → 设备控制**”并点击“**设置**”。
4. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。
5. 在“**蓝牙**”设备类型的上下文菜单中，配置蓝牙设备访问模式：**允许**、**阻止**或者**允许且不记录**。

   如果您阻止了对蓝牙设备的访问，则仅可以在应用程序控制台或 Kaspersky Security Center Web Console 中允许连接输入设备（键盘、鼠标等）。您无法在 Kaspersky Security Center 管理控制台中允许连接输入设备。
6. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置蓝牙设备访问规则

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在策略窗口中，选择“**本地活动控制 → 设备控制**”并点击“**设置**”。
5. 在“**设备控制设置**”区域，单击“**设备和 wi-fi 网络的访问规则**”链接。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。
6. 选择“**蓝牙**”设备类型。
   这将打开蓝牙设备访问设置。
7. 配置蓝牙设备访问模式：**允许**, **阻止**, **允许且不记录**。
8. 如果您选择**阻止**模式，您可以只允许连接蓝牙输入设备（键盘、鼠标等）。为此，在“**排除项**”下，选择“**输入设备(鼠标和键盘)**”复选框。
9. 保存更改。

如何在应用程序控制台中配置蓝牙设备访问规则

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制**”窗口将打开。
3. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。
4. 在“**访问**”下，配置蓝牙设备访问模式：**允许**、**阻止**或者**允许且不记录**。
5. 如果您选择**阻止**模式，您可以只允许连接蓝牙输入设备（键盘、鼠标等）。为此，在“**排除项**”下，选择“**输入设备(鼠标和键盘)**”复选框。
6. 保存更改。

区分用户对设备的访问权限

您可以按设备类型或受信任设备访问权限来配置用户访问权限。

根据设备类型区分用户访问权限

设备控制允许配置用户对*存储设备*数据的访问权限。对于这样的设备，您可以配置读写权限。设备控制支持以下类型的存储设备：

- 硬盘
- 可移动驱动器
- 软盘
- CD/DVD 驱动器
- 便携式设备 (MTP)，包括例如移动设备、照相机、媒体播放器等。

例如，这意味着您可以仅允许管理员组使用可移动驱动器。对于其他设备类型，您可以拒绝或允许所有用户的访问。您还可以配置用户对打印机的访问权限。

如何在 Kaspersky Security Center 管理控制台中配置用户对可移动驱动器上数据的访问权限

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。
5. 选择**设备控制**复选框。
6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
7. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   “**设备类型**”选项卡显示包含在设备控制组件分类的所有设备的访问规则。
8. 要配置存储设备访问规则，请双击打开规则列表。
9. 配置存储设备访问规则：
   a. 在“**访问规则**”块中单击“**添加**”按钮。
      这将打开添加新存储设备访问规则的窗口。
   b. 在“**优先级**”字段，设置*规则条目*优先级。规则包含以下属性：用户账户、计划、权限（读/写）和优先级。
      规则具有特定优先级。如果用户被添加到若干组，Kaspersky Industrial CyberSecurity for Nodes 基于具有最高优先级的规则规范设备访问。Kaspersky Industrial CyberSecurity for Nodes 允许分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。
      例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。
      阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Industrial CyberSecurity for Nodes 基于任何现有的阻止规则规范设备访问。

c. 在“**用户和组规则**”下，选择用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

d. 单击“**确定**”。

10. 在“**所选访问规则的计划**”下，为用户配置存储设备访问计划。

例如，您可以仅允许用户在工作时间访问存储设备。

11. 在文件管理器中配置用户对存储设备的访问权限（**读取 / 写入**）。

12. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中配置用户对存储设备上的数据的访问权限

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。

“**设备控制**”窗口将打开。

5. 选择**启用设备控制**复选框。

6. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。

7. 在**设备控制设置**块，单击**设备和 wi-fi 网络的访问规则**。

一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。

8. 在“**对存储设备的访问权限**”块，打开存储设备访问规则的属性。

9. 配置存储设备访问规则：

a. 在“**用户**”块中单击“**添加**”按钮。

这将打开添加新存储设备访问规则的窗口。

b. 在“**优先级**”字段，设置*规则条目*优先级。规则包含以下属性：用户账户、计划、权限（读/写）和优先级。

规则具有特定优先级。如果用户被添加到若干组，Kaspersky Industrial CyberSecurity for Nodes 基于具有最高优先级的规则规范设备访问。Kaspersky Industrial CyberSecurity for Nodes 允许分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Industrial CyberSecurity for Nodes 基于任何现有的阻止规则规范设备访问。

c. 在“**用户**”下，选择用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

d. 在“**设备访问计划**”下，为用户配置存储设备访问计划。

例如，您可以仅允许用户在工作时间访问存储设备。

e. 在文件管理器中配置用户对存储设备的访问权限（**读取 / 写入**）。

f. 单击“**确定**”。

10. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中配置用户对存储设备上的数据的访问权限

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。

“**属性: 设备控制**”窗口将打开。

3. 选择**设备控制**复选框。
4. 在“**阻止规则的操作模式**”块，选择“**阻止**”或者“**通知**”。
5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。

一个窗口打开，其中显示包含在设备控制组件分类的所有设备的访问规则。

6. 要配置存储设备访问规则，请双击打开规则列表。
7. 配置存储设备访问规则：

a. 在“**访问规则**”块中单击“**添加**”按钮。

这将打开添加新存储设备访问规则的窗口。

b. 在“**规则优先级**”字段，设置*规则条目*优先级。规则包含以下属性：用户账户、计划、权限（读/写）和优先级。

规则具有特定优先级。如果用户被添加到若干组，Kaspersky Industrial CyberSecurity for Nodes 基于具有最高优先级的规则规范设备访问。Kaspersky Industrial CyberSecurity for Nodes 允许分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Industrial CyberSecurity for Nodes 基于任何现有的阻止规则规范设备访问。

c. 在“**用户和组规则**”下，选择用户或用户组。您可以在 Active Directory 中选择用户，也可以手动输入本地用户名。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

d. 单击“**确定**”。

8. 在“**所选访问规则的计划**”下，为用户配置存储设备访问计划。

例如，您可以仅允许用户在工作时间访问存储设备。

9. 在文件管理器中配置用户对存储设备的访问权限（**读取 / 写入**）。
10. 保存更改。

区分用户对受信任设备的访问权限

*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。要使用受信任设备，您可以为单个用户、一组用户或组织的所有用户授予访问权限。你可以在受信任设备的属性中配置用户访问权限。

外部设备审计

要创建受信任设备列表，您必须对组织中的外部设备进行审核。要添加受信任的设备，您必须选择一个已连接的设备并为该设备分配受信任状态。您可以通过以下方式获取设备列表：

- 以“通知”模式启用设备控制。

  如何在 Kaspersky Security Center 管理控制台中以“通知”模式启用设备控制

  1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
  2. 选择必要的策略并双击以打开策略属性。
  3. 在策略属性窗口中，选择“**本地活动控制**”。
  4. 在“**设备控制**”区域中单击“**设置**”。
  5. 选择**设备控制**复选框。
  6. 在“**阻止规则的操作模式**”下，选择“**通知**”。
  7. 保存更改。要在计算机上应用该策略，请关闭锁。

  如何在 Kaspersky Security Center Web Console 中以“通知”模式启用设备控制

  1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
  2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
     策略属性窗口将打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。
     “**设备控制**”窗口将打开。
  5. 选择**启用设备控制**复选框。

6. 在“**阻止规则的操作模式**”下，选择“**通知**”。
7. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中以“通知”模式启用设备控制

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制**”窗口将打开。
3. 选择**设备控制**复选框。
4. 在“**阻止规则的操作模式**”下，选择“**通知**”。
5. 保存更改。

结果，Kaspersky Industrial CyberSecurity for Nodes 将记录外部设备的连接和断开连接事件。然后，您可以生成设备报告，并在分析报告后，添加受信任设备。

- 运行“*设备控制规则生成器*”任务。

  如何在 Kaspersky Security Center 管理控制台中运行“设备控制规则生成器”任务

  1. 打开 Kaspersky Security Center Administration Console。
  2. 在控制台树中，选择“**任务**”。
  3. 选择“*设备控制规则生成器*”任务并双击以打开任务属性。
     如果需要，创建新任务。
  4. 在“**模式**”部分，选择任务的模式：
     - “**考虑所有已连接的外部设备的系统数据**”。
       应用程序从操作系统内存中获取有关已连接到计算机的所有设备的信息。
     - “**仅考虑当前连接的外部设备**”。
       应用程序获取有关任务启动时所连接的设备的信息。
  5. 输入您想要保存包含数据的文件的路径。
  6. 如果您在多台计算机上运行该任务，我们建议选择“**将受保护设备详细信息添加到文件名**”复选框。
  7. 保存更改。
  8. 运行任务。

如何在 Kaspersky Security Center Web Console 中运行“设备控制规则生成器”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. 选择“*设备控制规则生成器*”任务并双击以打开任务属性。
   如果需要，创建新任务。
3. 在“**模式**”部分，选择任务的模式：
   - “**考虑曾经连接过的所有外部设备的系统数据**”。
     应用程序从操作系统内存中获取有关已连接到计算机的所有设备的信息。
   - “**仅考虑当前连接的外部设备**”。
     应用程序获取有关任务启动时所连接的设备的信息。
4. 输入您想要保存包含数据的文件的路径。
5. 如果您在多台计算机上运行该任务，我们建议选择“**将受保护设备详细信息添加到文件名**”复选框。
6. 保存更改。
7. 运行任务。

如何在应用程序控制台中启动“设备控制规则生成器”任务

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**自动规则生成**” → “**设备控制规则生成器**”。
2. 在“**设备控制规则生成器**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制规则生成器**”窗口将打开。
3. 在“**模式**”部分，选择任务的模式：
   - “**考虑所有已连接的外部设备的系统数据**”。
     应用程序从操作系统内存中获取有关已连接到计算机的所有设备的信息。
   - “**仅考虑当前连接的外部设备**”。
     应用程序获取有关任务启动时所连接的设备的信息。
4. 在“**任务完成后**”部分，选择任务完成后的应用程序操作：
   - “**将允许规则添加到设备控制规则列表**”。设备控制规则列表可在“设备控制”设置中找到。
     如果选中此复选框，则应用程序将根据所选的规则添加原则，将任务生成的规则添加到设备控制规则列表中。
     如果清除此复选框，则应用程序不会将新生成的允许规则添加到设备控制规则列表中。应用程序仅将规则导出到文件。

- “**添加原则**”。将新生成的允许规则添加到设备控制规则列表的方法：
  - “**添加到现有规则**”。应用程序添加规则到现有规则列表。在这种情况下，应用程序重复了相同的规则。
  - “**替换现有规则**”。应用程序添加新规则来代替现有规则。
  - “**与现有规则合并**”。应用程序添加规则到现有规则列表。在这种情况下，应用程序会合并相同的规则。
- “**将允许规则导出到文件**”。应用程序将允许规则导出到下面字段中指定的文件。然后，您可以在其他计算机上的应用程序设置中导入该文件以分发允许规则。该文件还可以用于备份允许规则。
- “**将受保护设备的详细信息添加到文件名**”。除了日期和时间之外，应用程序还会将计算机名称添加到导出的文件名中。如果您收集多台计算机的允许规则，则会很方便。

5. 保存更改。

因此，Kaspersky Industrial CyberSecurity for Nodes 会对外部设备进行审核，并将信息保存在 Kaspersky Security Center 的注册表中。外部设备列表在以下情况下可用：添加受信任设备。

添加受信任设备

*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

要使用受信任设备，您可以为单个用户、一组用户或组织的所有用户授予访问权限。

例如，如果您的组织不允许使用可移动驱动器，但是管理员在工作中使用可移动驱动器，您可以仅允许一组管理员使用可移动驱动器。为此，请将可移动驱动器添加到受信任列表，并配置用户访问权限。

不建议添加超过 1000 个受信任设备，因为这可能会导致系统不稳定。

如何在 Kaspersky Security Center 管理控制台中添加受信任设备

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。
5. 在“**设备监控设置**”下，选择“**受信任设备**”选项卡。
   这将打开受信任设备列表。
6. 如果要为公司内的所有计算机创建受信任设备的综合列表，请选中“**继承时合并值**”复选框。
   将合并父策略和子策略中的受信任设备列表。如果启用继承时合并值，则将合并列表。父策略中的受信任设备以只读视图的形式显示在子策略中。无法更改或删除父策略的受信任设备。

7. 单击“**添加**”按钮，然后选择将设备添加到受信任列表的方法：

   - “**基于连接的设备生成规则**”。
   - “**基于系统数据生成规则**”。
   - “**根据 Kaspersky Security Center 注册表生成规则**”。

   如果设备列表为空，您必须对外部设备进行审计。为此，请运行“*设备控制规则生成器*”任务。

   > Kaspersky Industrial CyberSecurity for Nodes 不支持添加“**软盘**”类型的设备到受信任列表。

8. 单击“**为所选设备添加规则**”。
9. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在 Kaspersky Security Center Web Console 中添加受信任的设备

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。
   “**设备控制**”窗口将打开。
5. 在**设备控制设置**块，单击**受信任设备**。
   这将打开受信任设备列表。
6. 如果要为公司内的所有计算机创建受信任设备的综合列表，请选中“**继承时合并值**”复选框。
   将合并父策略和子策略中的受信任设备列表。如果启用继承时合并值，则将合并列表。父策略中的受信任设备以只读视图的形式显示在子策略中。无法更改或删除父策略的受信任设备。
7. 单击“**从 KSC 注册表**”。
   如果设备列表为空，您必须对外部设备进行审计。为此，请运行“*设备控制规则生成器*”任务。

   > Kaspersky Industrial CyberSecurity for Nodes 不支持添加“**软盘**”类型的设备到受信任列表。

8. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中添加受信任设备

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。
2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。
   “**属性: 设备控制**”窗口将打开。
3. 在“**设备控制设置**”下，选择“**受信任设备**”选项卡。
   这将打开受信任设备列表。
4. 单击“**添加**”按钮，然后选择将设备添加到受信任列表的方法：
   - “**基于连接的设备生成规则**”。
   - “**基于系统数据生成规则**”。
   - “**根据 Kaspersky Security Center 注册表生成规则**”。

   如果设备列表为空，您必须对外部设备进行审计。为此，请运行“*设备控制规则生成器*”任务。

   > Kaspersky Industrial CyberSecurity for Nodes 不支持添加“**软盘**”类型的设备到受信任列表。

5. 单击“**为所选设备添加规则**”。
6. 保存更改。

导出和导入受信任设备的列表

要将受信任设备的列表分发到组织中的其他计算机，可以使用导出/导入过程。可以将受信任设备列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的设备。还可以使用导出/导入功能备份受信任设备列表或将列表迁移到其他服务器。

> Kaspersky Industrial CyberSecurity for Nodes 允许从 Kaspersky Endpoint Security for Windows 导入受信任设备的列表。这些应用程序的 XML 文件格式相同。

如何在 Kaspersky Security Center 管理控制台中导出和导入受信任设备列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**本地活动控制**”。
4. 在“**设备控制**”区域中单击“**设置**”。

5. 在“**设备控制设置**”下，选择“**受信任设备**”选项卡。
   这将打开受信任设备列表。

6. 要导出受信任设备的列表：

   a. 选择您要导出的受信任设备。

   b. 点击 按钮并选择导出模式：导出整个受信任设备列表或仅导出选定的受信任设备。

   c. 在打开的窗口中，指定您要将受信任设备列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。
      Kaspersky Industrial CyberSecurity for Nodes 导出 Web 资源地址列表到 XML 文件。

7. 要导入受信任设备的列表：

   a. 点击“**添加 → 从 XML 文件导入规则**”并选择导入模式：添加或替换。
      在打开的窗口中，选择要从中导入 Web 资源列表的 XML 文件。
      在合并模式下，应用程序会检查受信任设备的列表并删除重复的条目。在添加模式下，应用程序将条目添加到受信任应用程序列表中，而不检查是否有重复。

   b. 打开文件。
      Kaspersky Industrial CyberSecurity for Nodes 根据所选模式导入受信任设备。

8. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Security Center Web Console 中导出和导入受信任设备列表

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**本地活动控制 → 设备控制**”并点击“**配置**”按钮。
   “**设备控制**”窗口将打开。

5. 在**设备控制设置**块，单击**受信任设备**。
   这将打开受信任设备列表。

6. 要导出受信任设备的列表：

   a. 选择您要导出的受信任设备。

   b. 点击“**导出**”按钮并选择导出模式：导出整个受信任设备列表或仅导出选定的受信任设备。

   c. 保存文件。
      Kaspersky Industrial CyberSecurity for Nodes 导出 Web 资源地址列表到 XML 文件。

7. 要导入受信任设备的列表：

   a. 点击“**导入**”按钮并选择导入模式：添加或替换。

   b. 在打开的窗口中，选择要从中导入 Web 资源列表的 XML 文件。

   c. 打开文件。

      Kaspersky Industrial CyberSecurity for Nodes 根据所选模式导入受信任设备。

8. 保存更改。要在计算机上应用该策略，请关闭锁。

如何在应用程序控制台中导出和导入受信任设备列表

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**设备控制**”。

2. 在“**设备控制**”节点的结果窗格中，单击“**属性**”。

   “**属性: 设备控制**”窗口将打开。

3. 在“**设备控制设置**”下，选择“**受信任设备**”选项卡。

   这将打开受信任设备列表。

4. 要导出受信任设备的列表：

   a. 选择您要导出的受信任设备。

   b. 点击 按钮并选择导出模式：导出整个受信任设备列表或仅导出选定的受信任设备。

   c. 在打开的窗口中，指定您要将受信任设备列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

      Kaspersky Industrial CyberSecurity for Nodes 导出 Web 资源地址列表到 XML 文件。

5. 要导入受信任设备的列表：

   a. 点击“**添加 → 从 XML 文件导入规则**”并选择导入模式：添加或替换。

      在打开的窗口中，选择要从中导入 Web 资源列表的 XML 文件。

      在合并模式下，应用程序会检查受信任设备的列表并删除重复的条目。在添加模式下，应用程序将条目添加到受信任应用程序列表中，而不检查是否有重复。

   b. 打开文件。

      Kaspersky Industrial CyberSecurity for Nodes 根据所选模式导入受信任设备。

6. 保存更改。

防火墙

防火墙组件可以在以下模式下运行：

- “**观察 Windows 防火墙的状态**”。该模式旨在从应用程序版本 4.0 及以下版本中的防火墙管理任务逻辑平稳过渡到应用程序版本 4.5 及更高版本中的全功能防火墙。当您升级应用程序版本 4.0 及以下时，集成到 Windows 防火墙中的防火墙管理任务的规则将被保留。但防火墙组件不再与 Windows 防火墙进行交互，而只是监控 Windows 防火墙的流量过滤，并在组件的运行日志中记录相应的事件。然后，您可以创建防火墙规则和/或导入 Windows 防火墙规则并将防火墙操作模式更改为“**通知**”。

- “**通知**”。应用程序仅监控防火墙规则的运行，并在组件的运行日志中记录相应事件。该模式用于测试防火墙规则。您可以使用防火墙操作日志评估它们的适用性。然后，如有必要，您可以调整防火墙规则并将防火墙运行模式更改为“**阻止**”。

- “**阻止**”。应用程序根据组件设置过滤网络流量，并在组件的操作日志中记录相应事件。

关于防火墙规则

如果选择“**阻止**”模式，防火墙组件将使用防火墙规则过滤网络流量。

应用程序的防火墙规则控制指定应用程序的网络连接。这些规则的触发条件基于应用程序可执行文件的路径。

防火墙端口规则控制指定端口和协议 (TCP/UDP) 的网络连接。此类规则的触发条件是协议类型和端口或端口范围。

端口规则涉及的范围比应用程序规则的范围要广。通过基于端口规则允许网络连接，您可以降低受保护计算机的安全级别。

配置防火墙

本节提供有关配置防火墙组件的常规设置以及创建和配置防火墙规则的说明。

配置常规防火墙设置

在 Kaspersky Security Center 管理控制台中配置防火墙组件的常规设置

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。

2. 选择必要的策略并双击以打开策略属性。

3. 在“**网络活动控制**”部分中，单击“**防火墙** ”子部分中的“**设置**”按钮。

   “**防火墙**”窗口将打开。

4. 在“**常规**”选项卡上，“**阻止规则的操作模式**”块中，选择组件操作模式：

   - “**观察 Windows 防火墙的状态**”。该模式旨在从应用程序版本 4.0 及以下版本中的防火墙管理任务逻辑平稳过渡到应用程序版本 4.5 及更高版本中的全功能防火墙。当您升级应用程序版本 4.0 及以下时，集成到 Windows 防火墙中的防火墙管理任务的规则将被保留。但防火墙组件不再与 Windows 防火墙进行交互，而只是监控 Windows 防火墙的流量过滤，并在组件的运行日志中记录相应的事件。然后，您可以创建防火墙规则和/或导入 Windows 防火墙规则并将防火墙操作模式更改为“**通知**”。

   - “**通知**”。应用程序仅监控防火墙规则的运行，并在组件的运行日志中记录相应事件。该模式用于测试防火墙规则。您可以使用防火墙操作日志评估它们的适用性。然后，如有必要，您可以调整防火墙规则并将防火墙运行模式更改为“**阻止**”。

   - “**阻止**”。应用程序根据组件设置过滤网络流量，并在组件的操作日志中记录相应事件。

5. 在“**入站连接**”块中，配置针对传入网络连接的设置：

   - 使用“**入站连接操作**”下拉列表指定应用程序对所有传入网络连接执行的操作，除非在针对传入连接的防火墙规则中另有定义。

   - 如有必要，添加针对传入连接的防火墙规则。

     针对传入连接的防火墙规则起到排除的作用。例如，如果针对传入网络连接配置允许规则，并在“**入站连接操作**”下拉列表中选择“**阻止**”，则应用程序将允许符合规则条件的传入网络连接。

6. 在“**出站连接**”块中，配置针对传出网络连接的设置：

   - 使用“**出站连接操作**”下拉列表指定应用程序对所有传出网络连接执行的操作，除非在针对传出连接的防火墙规则中另有定义。

   - 如有必要，添加针对传出连接的防火墙规则。

     针对传出连接的防火墙规则起到排除的作用。例如，如果针对传出网络连接配置阻止规则，并在“**出站连接操作**”下拉列表中选择“**允许**”，则应用程序将阻止符合规则条件的传出网络连接。

7. 保存更改。

Kaspersky Industrial CyberSecurity for Nodes 应用新设置。更改设置的日期和时间保存在系统审核日志中。

在 Kaspersky Security Center Web Console 中配置防火墙组件的常规设置

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在“**网络活动控制**”部分中，单击“**防火墙** ”子部分中的“**配置**”按钮。

   “**防火墙**”窗口将打开。

5. 将切换开关设置为“**防火墙已启用**”。

6. 在**阻止规则的操作模式**块，选择组件操作模式：

   - "**观察 Windows 防火墙的状态**"。该模式旨在从应用程序版本 4.0 及以下版本中的防火墙管理任务逻辑平稳过渡到应用程序版本 4.5 及更高版本中的全功能防火墙。当您升级应用程序版本 4.0 及以下时，集成到 Windows 防火墙中的防火墙管理任务的规则将被保留。但防火墙组件不再与 Windows 防火墙进行交互，而只是监控 Windows 防火墙的流量过滤，并在组件的运行日志中记录相应的事件。然后，您可以创建防火墙规则和/或导入 Windows 防火墙规则并将防火墙操作模式更改为"**通知**"。

   - "**通知**"。应用程序仅监控防火墙规则的运行，并在组件的运行日志中记录相应事件。该模式用于测试防火墙规则。您可以使用防火墙操作日志评估它们的适用性。然后，如有必要，您可以调整防火墙规则并将防火墙运行模式更改为"**阻止**"。

   - "**阻止**"。应用程序根据组件设置过滤网络流量，并在组件的操作日志中记录相应事件。

7. 在"**入站连接**"块中，配置针对传入网络连接的设置：

   - 使用"**入站连接操作**"下拉列表指定应用程序对所有传入网络连接执行的操作，除非在针对传入连接的防火墙规则中另有定义。

   - 如有必要，添加针对传入连接的防火墙规则。

     针对传入连接的防火墙规则起到排除的作用。例如，如果针对传入网络连接配置允许规则，并在"**入站连接操作**"下拉列表中选择"**阻止**"，则应用程序将允许符合规则条件的传入网络连接。

8. 在"**出站连接**"块中，配置针对传出网络连接的设置：

   - 使用"**出站连接操作**"下拉列表指定应用程序对所有传出网络连接执行的操作，除非在针对传出连接的防火墙规则中另有定义。

   - 如有必要，添加针对传出连接的防火墙规则。

     针对传出连接的防火墙规则起到排除的作用。例如，如果针对传出网络连接配置阻止规则，并在"**出站连接操作**"下拉列表中选择"**允许**"，则应用程序将阻止符合规则条件的传出网络连接。

9. 保存更改。

Kaspersky Industrial CyberSecurity for Nodes 应用新设置。更改设置的日期和时间保存在系统审核日志中。

在应用程序控制台中配置防火墙组件的常规设置

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择"**计算机控制**" → "**防火墙**"。

2. 在"**防火墙**"节点的结果窗格中，单击"**属性**"。

   "**属性: 防火墙**"窗口将打开。

3. 选择**防火墙**复选框。

4. 在**阻止规则的操作模式**块，选择组件操作模式：

   - “**观察 Windows 防火墙的状态**”。该模式旨在从应用程序版本 4.0 及以下版本中的防火墙管理任务逻辑平稳过渡到应用程序版本 4.5 及更高版本中的全功能防火墙。当您升级应用程序版本 4.0 及以下时，集成到 Windows 防火墙中的防火墙管理任务的规则将被保留。但防火墙组件不再与 Windows 防火墙进行交互，而只是监控 Windows 防火墙的流量过滤，并在组件的运行日志中记录相应的事件。然后，您可以创建防火墙规则和/或导入 Windows 防火墙规则并将防火墙操作模式更改为“**通知**”。

   - “**通知**”。应用程序仅监控防火墙规则的运行，并在组件的运行日志中记录相应事件。该模式用于测试防火墙规则。您可以使用防火墙操作日志评估它们的适用性。然后，如有必要，您可以调整防火墙规则并将防火墙运行模式更改为“**阻止**”。

   - “**阻止**”。应用程序根据组件设置过滤网络流量，并在组件的操作日志中记录相应事件。

5. 在“**入站连接**”块中，配置针对传入网络连接的设置：

   - 使用“**入站连接操作**”下拉列表指定应用程序对所有传入网络连接执行的操作，除非在针对传入连接的防火墙规则中另有定义。

   - 如有必要，添加针对传入连接的防火墙规则。

     针对传入连接的防火墙规则起到排除的作用。例如，如果针对传入网络连接配置允许规则，并在“**入站连接操作**”下拉列表中选择“**阻止**”，则应用程序将允许符合规则条件的传入网络连接。

6. 在“**出站连接**”块中，配置针对传出网络连接的设置：

   - 使用“**出站连接操作**”下拉列表指定应用程序对所有传出网络连接执行的操作，除非在针对传出连接的防火墙规则中另有定义。

   - 如有必要，添加针对传出连接的防火墙规则。

     针对传出连接的防火墙规则起到排除的作用。例如，如果针对传出网络连接配置阻止规则，并在“**出站连接操作**”下拉列表中选择“**允许**”，则应用程序将阻止符合规则条件的传出网络连接。

7. 保存更改。

Kaspersky Industrial CyberSecurity for Nodes 应用新设置。更改设置的日期和时间保存在系统审核日志中。

创建和配置防火墙规则

在 Kaspersky Security Center 管理控制台中创建和配置防火墙规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。

2. 选择必要的策略并双击以打开策略属性。

3. 在“**网络活动控制**”部分中，单击“**防火墙** ”子部分中的“**设置**”按钮。

   “**防火墙**”窗口将打开。

4. 在“**入站连接**”块中单击“**规则列表**”按钮。

   “**入站连接规则**”窗口将打开。

5. **创建并配置传入连接的防火墙规则**。

   1. 在“**应用程序**”选项卡上单击“**添加**”按钮。
      “**应用程序规则**”窗口将打开。

   2. 配置规则设置：

      a. 在“**规则名称**”字段中输入规则的名称。

      > 规则名称，无论字符大小写，都不得与保留名称 All、ICMPv4 和 ICMPv6 相匹配；它在针对入站网络连接的所有规则列表中必须是唯一的。

      b. 在“**操作**”列表中，选择以下选项之一：

      - “**允许**”。如果选择此选项，应用程序将允许该应用程序的传入网络连接。
      - “**阻止**”。如果选择此选项，应用程序将阻止该应用程序的传入网络连接。

      c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

      d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

      e. 在“**应用程序路径**”字段中，手动或使用“**浏览**”按钮指定要为其配置规则的应用程序的可执行文件路径。

      f. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控来自指定网络地址的传入连接。

      > IP 地址仅支持 IPv4 格式。

      g. 在“**网络适配器**”块，指定网络适配器列表。

      h. 单击“**确定**”按钮保存规则。

   3. 在“**本地端口**”选项卡上单击“**添加**”按钮。
      “**端口规则**”窗口将打开。

   4. 配置规则设置：

      a. 在“**规则名称**”字段中输入规则的名称。

      b. 在“**操作**”列表中，选择以下选项之一：

      - “**允许**”。如果选择此选项，应用程序将允许端口的传入网络连接。
      - “**阻止**”。如果选择此选项，应用程序将阻止端口的传入网络连接。

      c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

      d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控来自指定网络地址的传入连接。

> IP 地址仅支持 IPv4 格式。

f. 在“**网络适配器**”块，指定网络适配器列表。

g. 单击“**确定**”按钮保存规则。

5. 在“**入站连接规则**”窗口中单击“**确定**”按钮。

6. 在“**出站连接**”块中单击“**规则列表**”按钮。

“**出站连接规则**”窗口将打开。

7. **创建并配置传出连接的防火墙规则**。

1. 在“**应用程序**”选项卡上单击“**添加**”按钮。

“**应用程序规则**”窗口将打开。

2. 配置规则设置：

a. 在“**规则名称**”字段中输入规则的名称。

> 规则名称，无论字符大小写，都不得与保留名称 All、ICMPv4 和 ICMPv6 相匹配；它在针对出站网络连接的所有规则列表中必须是唯一的。

b. 在“**操作**”列表中，选择以下选项之一：

- “**允许**”。如果选择此选项，应用程序将允许该应用程序的传出网络连接。
- “**阻止**”。如果选择此选项，应用程序将阻止该应用程序的传出网络连接。

c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**应用程序路径**”字段中，手动或使用“**浏览**”按钮指定要为其配置规则的应用程序的可执行文件路径。

f. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

> IP 地址仅支持 IPv4 格式。

g. 在“**网络适配器**”块，指定网络适配器列表。

h. 单击“**确定**”按钮保存规则。

3. 在“**端口**”选项卡上单击“**添加**”按钮。
“**端口规则**”窗口将打开。

4. 配置规则设置：

a. 在“**规则名称**”字段中输入规则的名称。

b. 在“**操作**”列表中，选择以下选项之一：

- “**允许**”。如果选择此选项，应用程序将允许端口的传出网络连接。
- “**阻止**”。如果选择此选项，应用程序将阻止端口的传出网络连接。

c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

IP 地址仅支持 IPv4 格式。

f. 在“**网络适配器**”块，指定网络适配器列表。

g. 单击“**确定**”按钮保存规则。

5. 在“**出站连接规则**”窗口中单击“**确定**”按钮。

8. 如果要从 XML 文件导入或导出自定义规则，请使用“**规则的导入和导出**”块中的“**导入**”或者“**导出**”按钮。

9. 保存更改。

Kaspersky Industrial CyberSecurity for Nodes 应用新设置。更改设置的日期和时间保存在系统审核日志中。

在 Kaspersky Security Center Web Console 中创建和配置防火墙规则

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在“**网络活动控制**”部分中，单击“**防火墙** ”子部分中的“**配置**”按钮。
“**防火墙**”窗口将打开。

5. 将切换开关设置为“**防火墙已启用**”。

6. 在“**入站连接**”块中单击“**配置**”按钮。
   “**入站连接规则**”窗口将打开。

7. **创建并配置传入连接的防火墙规则**。

   1. 在“**本地端口**”选项卡上单击“**添加**”按钮。
      “**端口规则**”窗口将打开。

   2. 配置规则设置：

      a. 在“**规则名称**”字段中输入规则的名称。

      b. 在“**操作**”列表中，选择以下选项之一：

      - “**允许**”。如果选择此选项，应用程序将允许端口的传出网络连接。
      - “**拒绝**”。如果选择此选项，应用程序将阻止端口的传出网络连接。

      c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

      d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

      e. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

      > IP 地址仅支持 IPv4 格式。

      f. 在“**网络适配器**”块，指定网络适配器列表。

      g. 单击“**确定**”按钮保存规则。

   3. 在“**应用程序**”选项卡上单击“**添加**”按钮。
      “**应用程序规则**”窗口将打开。

   4. 配置规则设置：

      a. 在“**规则名称**”字段中输入规则的名称。

      > 规则名称，无论字符大小写，都不得与保留名称 All、ICMPv4 和 ICMPv6 相匹配；它在针对出站网络连接的所有规则列表中必须是唯一的。

      b. 在“**操作**”列表中，选择以下选项之一：

      - “**允许**”。如果选择此选项，应用程序将允许该应用程序的传出网络连接。
      - “**拒绝**”。如果选择此选项，应用程序将阻止该应用程序的传出网络连接。

      c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

      d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**应用程序路径**”字段中，手动指定要为其配置规则的应用程序的可执行文件路径。

f. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

> IP 地址仅支持 IPv4 格式。

g. 在“**网络适配器**”块，指定网络适配器列表。

h. 单击“**确定**”按钮保存规则。

5. 在“**入站连接规则**”窗口中单击“**确定**”按钮。

8. 在“**出站连接**”块中单击“**配置**”按钮。
“**出站连接规则**”窗口将打开。

9. **创建并配置传出连接的防火墙规则**。

1. 在“**本地端口**”选项卡上单击“**添加**”按钮。
“**端口规则**”窗口将打开。

2. 配置规则设置：

a. 在“**规则名称**”字段中输入规则的名称。

b. 在“**操作**”列表中，选择以下选项之一：

- “**允许**”。如果选择此选项，应用程序将允许端口的传出网络连接。
- “**拒绝**”。如果选择此选项，应用程序将阻止端口的传出网络连接。

c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

> IP 地址仅支持 IPv4 格式。

f. 在“**网络适配器**”块，指定网络适配器列表。

g. 单击“**确定**”按钮保存规则。

3. 在“**应用程序**”选项卡上单击“**添加**”按钮。
“**应用程序规则**”窗口将打开。

4. 配置规则设置：

   a. 在“**规则名称**”字段中输入规则的名称。

   > 规则名称，无论字符大小写，都不得与保留名称 All、ICMPv4 和 ICMPv6 相匹配；它在针对出站网络连接的所有规则列表中必须是唯一的。

   b. 在“**操作**”列表中，选择以下选项之一：

   - “**允许**”。如果选择此选项，应用程序将允许该应用程序的传出网络连接。
   - “**拒绝**”。如果选择此选项，应用程序将阻止该应用程序的传出网络连接。

   c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

   d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

   e. 在“**应用程序路径** ”字段中，手动指定要为其配置规则的应用程序的可执行文件路径。

   f. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

   > IP 地址仅支持 IPv4 格式。

   g. 在“**网络适配器**”块，指定网络适配器列表。

   h. 单击“**确定**”按钮保存规则。

5. 在“**出站连接规则**”窗口中单击“**确定**”按钮。

10. 如果要从 XML 文件导入或导出自定义规则，请使用“**规则导入和导出**”块中的“**规则导入**”或者“**规则导出**”按钮。

11. 保存更改。

Kaspersky Industrial CyberSecurity for Nodes 应用新设置。更改设置的日期和时间保存在系统审核日志中。

在应用程序控制台中创建和配置防火墙规则

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**防火墙**”。

2. 在“**防火墙**”节点的结果窗格中，单击“**属性**”。
   “**属性: 防火墙**”窗口将打开。

3. 在“**入站连接**”块中单击“**规则列表**”按钮。
   “**入站连接规则**”窗口将打开。

4. **创建并配置传入连接的防火墙规则**。

   1. 在“**应用程序**”选项卡上单击“**添加**”按钮。
      “**应用程序规则**”窗口将打开。

   2. 配置规则设置：

      a. 在“**规则名称**”字段中输入规则的名称。

      > 规则名称，无论字符大小写，都不得与保留名称 All、ICMPv4 和 ICMPv6 相匹配；它在针对入站网络连接的所有规则列表中必须是唯一的。

      b. 在“**操作**”列表中，选择以下选项之一：

      - “**允许**”。如果选择此选项，应用程序将允许该应用程序的传入网络连接。
      - “**阻止**”。如果选择此选项，应用程序将阻止该应用程序的传入网络连接。

      c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

      d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

      e. 在“**应用程序路径**”字段中，手动或使用“**浏览**”按钮指定要为其配置规则的应用程序的可执行文件路径。

      f. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控来自指定网络地址的传入连接。

      > IP 地址仅支持 IPv4 格式。

      g. 在“**网络适配器**”块，指定网络适配器列表。

      h. 单击“**确定**”按钮保存规则。

   3. 在“**本地端口**”选项卡上单击“**添加**”按钮。
      “**端口规则**”窗口将打开。

   4. 配置规则设置：

      a. 在“**规则名称**”字段中输入规则的名称。

      b. 在“**操作**”列表中，选择以下选项之一：

      - “**允许**”。如果选择此选项，应用程序将允许端口的传入网络连接。
      - “**阻止**”。如果选择此选项，应用程序将阻止端口的传入网络连接。

      c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

      d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控来自指定网络地址的传入连接。

> IP 地址仅支持 IPv4 格式。

f. 在“**网络适配器**”块，指定网络适配器列表。

g. 单击“**确定**”按钮保存规则。

5. 在“**入站连接规则**”窗口中单击“**确定**”按钮。

5. 在“**出站连接**”块中单击“**规则列表**”按钮。

“**出站连接规则**”窗口将打开。

6. **创建并配置传出连接的防火墙规则**。

1. 在“**应用程序**”选项卡上单击“**添加**”按钮。

“**应用程序规则**”窗口将打开。

2. 配置规则设置：

a. 在“**规则名称**”字段中输入规则的名称。

> 规则名称，无论字符大小写，都不得与保留名称 All、ICMPv4 和 ICMPv6 相匹配；它在针对出站网络连接的所有规则列表中必须是唯一的。

b. 在“**操作**”列表中，选择以下选项之一：

- “**允许**”。如果选择此选项，应用程序将允许该应用程序的传出网络连接。
- “**阻止**”。如果选择此选项，应用程序将阻止该应用程序的传出网络连接。

c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**应用程序路径**”字段中，手动或使用“**浏览**”按钮指定要为其配置规则的应用程序的可执行文件路径。

f. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

> IP 地址仅支持 IPv4 格式。

g. 在“**网络适配器**”块，指定网络适配器列表。

h. 单击“**确定**”按钮保存规则。

3. 在“**端口**”选项卡上单击“**添加**”按钮。
“**端口规则**”窗口将打开。

4. 配置规则设置：

a. 在“**规则名称**”字段中输入规则的名称。

b. 在“**操作**”列表中，选择以下选项之一：

- “**允许**”。如果选择此选项，应用程序将允许端口的传出网络连接。
- “**阻止**”。如果选择此选项，应用程序将阻止端口的传出网络连接。

c. 选择“**协议**”复选框，以选择应用程序控制传入网络连接的协议类型。

d. 在“**本地端口**”和“**远程端口**”块中，指定端口或端口范围。

e. 在“**规则使用范围**”字段中，指定网络地址。应用程序将根据规则设置监控到指定网络地址的传出连接。

IP 地址仅支持 IPv4 格式。

f. 在“**网络适配器**”块，指定网络适配器列表。

g. 单击“**确定**”按钮保存规则。

5. 在“**出站连接规则**”窗口中单击“**确定**”按钮。

7. 如果要从 XML 文件导入或导出自定义规则，请使用“**规则的导入和导出**”块中的“**导入**”或者“**导出**”按钮。

8. 要导入 Windows 防火墙规则，请单击“**导入 Windows 防火墙规则**”。

在 Windows 11 24H2 计算机上，应用程序可能会跳过某些 Windows 防火墙规则。由于此版本操作系统的特殊功能，Kaspersky Industrial CyberSecurity for Nodes 可能无法识别应用程序数据包的某些规则的参数。

9. 保存更改。

Kaspersky Industrial CyberSecurity for Nodes 应用新设置。更改设置的日期和时间保存在系统审核日志中。

启用和禁用防火墙规则

在 Kaspersky Security Center 管理控制台中创建和配置防火墙规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在“**网络活动控制**”部分中，单击“**防火墙** ”子部分中的“**设置**”按钮。
   “**防火墙**”窗口将打开。
4. 在打开的窗口中，点击“**入站连接**”或者“**出站连接**”部分中的“**规则列表**”按钮，具体取决于您要更改其状态的规则的类型。
5. 在打开的窗口中，选择“**应用程序**”或“**本地端口**”选项卡。
   在规则列表中，选择要修改其状态的规则，然后执行以下操作之一：
   - 如果您想要启用已禁用的规则，选中规则名称左侧的复选框。
     将启用所选规则。
   - 如果您想要禁用已启用的规则，清除规则名称左侧的复选框。
     将禁用所选规则。
6. 要从列表中删除规则，请选择规则并单击“**删除**”。
7. 保存更改。

在 Kaspersky Security Center Web Console 中创建和配置防火墙规则

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**网络活动控制**”部分中，单击“**防火墙** ”子部分中的“**配置**”按钮。
   “**防火墙**”窗口将打开。
5. 在打开的窗口中，点击“**入站连接**”或者“**出站连接**”部分中的“**配置**”按钮，具体取决于您要更改其状态的规则的类型。
6. 在打开的窗口中，选择“**本地端口**”或“**应用程序**”选项卡。

在规则列表中，选择要修改其状态的规则，然后执行以下操作之一：

- 如果您想要启用已禁用的规则，选中规则名称左侧的复选框。
  将启用所选规则。
- 如果您想要禁用已启用的规则，清除规则名称左侧的复选框。
  将禁用所选规则。

7. 要从列表中删除规则，请选择规则并单击“**删除**”。
8. 保存更改。

在应用程序控制台中创建和配置防火墙规则

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**计算机控制**” → “**防火墙**”。
2. 在“**防火墙**”节点的结果窗格中，单击“**属性**”。
   “**属性: 防火墙**”窗口将打开。
3. 在打开的窗口中，点击“**入站连接**”或者“**出站连接**”部分中的“**规则列表**”按钮，具体取决于您要更改其状态的规则的类型。
4. 在打开的窗口中，选择“**应用程序**”或“**本地端口**”选项卡。
   在规则列表中，选择要修改其状态的规则，然后执行以下操作之一：
   - 如果您想要启用已禁用的规则，选中规则名称左侧的复选框。
     将启用所选规则。
   - 如果您想要禁用已启用的规则，清除规则名称左侧的复选框。
     将禁用所选规则。
5. 要从列表中删除规则，请选择规则并单击“**删除**”。
6. 保存更改。

BadUSB 攻击防护

默认情况下，未安装“BadUSB 攻击防护”组件。您可以在应用程序安装期间添加组件，也可以在应用程序安装后更改应用程序组件集。

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）。这个步骤称为键盘授权。

如果正确输入代码，程序将在授权键盘列表中保存识别参数 - 键盘的 VID/PID 和其所连接的端口号。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，程序将再次提示为该键盘授权。

如果错误输入数字代码，则程序将生成新的代码。您可以配置尝试输入数字代码的次数。如果数字代码多次输入错误或键盘授权窗口关闭，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。

在 BadUSB 攻击防护组件安装前被计算机识别为键盘的 USB 设备在该组件安装后仍将被认定为经过授权。

如何在 Kaspersky Security Center 管理控制台中启用和配置 BadUSB 攻击防护组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，转到“**本地活动控制**”区域。
4. 在“**BadUSB 攻击防护**”块中单击“**设置**”按钮。
   “**BadUSB 攻击防护**”窗口将打开。
5. 使用“**BadUSB 攻击防护**”复选框启用或禁用组件。

6. 在“**USB 设备授权**”部分中，配置以下设置：

   - “**USB 设备授权尝试的最大数量**”。如果授权码输入不正确达到指定次数，则自动阻止 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，USB 设备将被阻止。Kaspersky Industrial CyberSecurity for Nodes 显示 USB 设备的阻塞持续时间。此时间过后，您可以尝试 5 次输入授权代码。

   - “**达到最大尝试数量的超时时间(分钟)**”。在输入授权代码失败指定次数后，阻止 USB 设备的持续时间。有效值为 1 到 180（分钟）。

7. 在“**连接时的 USB 设备授权**”部分中，配置以下设置：

   - “**禁止使用屏幕键盘授权 USB 设备**”。如果选定该复选框，应用程序将阻止使用屏幕键盘授权无法输入授权码的 USB 设备（例如，条形码扫描器）。

   - “**禁止使用条形码授权 USB 设备**”。如果选中该复选框，应用程序将不会在条形码扫描器授权通知中显示条形码。

8. 关闭挂锁以将策略应用于计算机。

9. 点击“**确定**”保存更改。

如何在 Kaspersky Security Center Web Console 中启用和配置 BadUSB 攻击防护组件

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**本地活动控制**”部分。

5. 在“**BadUSB 攻击防护**”块中单击“**配置**”按钮。
   “**BadUSB 攻击防护**”窗口将打开。

6. 使用**BadUSB 攻击防护**开关启用或禁用组件。

7. 启用或禁用“**禁止使用屏幕键盘授权 USB 设备已启用**”切换开关以允许或阻止使用屏幕键盘授权无法输入授权码的 USB 设备（例如，条形码扫描器）。

8. 启用或禁用“**禁止使用条形码授权 USB 设备已启用**”切换开关以允许或阻止在条形码扫描器授权通知中显示条形码。

9. 在“**USB 设备授权**”部分中，配置以下设置：

   - “**USB 设备授权尝试的最大数量(1-10)**”。如果授权码输入不正确达到指定次数，则自动阻止 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，USB 设备将被阻止。Kaspersky Industrial CyberSecurity for Nodes 显示 USB 设备的阻塞持续时间。此时间过后，您可以尝试 5 次输入授权代码。

   - “**达到最大尝试数量的超时分钟数(1-180)**”。在输入授权代码失败指定次数后，阻止 USB 设备的持续时间。有效值为 1 到 180（分钟）。

10. 关闭挂锁以将策略应用于计算机。

11. 点击“**确定**”保存更改。

如何在应用程序控制台中启用和配置 BadUSB 攻击防护组件

1. 在应用程序控制台树中，选择“**计算机控制** → **BadUSB 攻击防护**”部分。

2. 在结果窗格中单击“**属性**”链接。

   “**BadUSB 攻击防护**”窗口将打开。

3. 使用“**BadUSB 攻击防护**”复选框启用或禁用组件。

4. 在“**USB 设备授权**”部分中，配置以下设置：

   - “**USB 设备授权尝试的最大数量**”。如果授权码输入不正确达到指定次数，则自动阻止 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，USB 设备将被阻止。Kaspersky Industrial CyberSecurity for Nodes 显示 USB 设备的阻塞持续时间。此时间过后，您可以尝试 5 次输入授权代码。

   - “**达到最大尝试数量的超时时间(分钟)**”。在输入授权代码失败指定次数后，阻止 USB 设备的持续时间。有效值为 1 到 180（分钟）。

5. 在“**连接时的 USB 设备授权**”部分中，配置以下设置：

   - “**禁止使用屏幕键盘授权 USB 设备**”。如果选定该复选框，应用程序将阻止使用屏幕键盘授权无法输入授权码的 USB 设备（例如，条形码扫描器）。

   - “**禁止使用条形码授权 USB 设备**”。如果选中该复选框，应用程序将不会在条形码扫描器授权通知中显示条形码。

6. 点击“**确定**”保存更改。

系统完整性监控

Kaspersky Industrial CyberSecurity for Nodes 4.5 现在包含系统完整性监控组件，而不是文件完整性监控和注册表访问监控组件。系统完整性监控组件包括文件完整性监控的所有功能，另外还允许监控注册表更改和外部设备的连接。

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 Industrial CyberSecurity for Nodes 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。

实时系统完整性监控

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。

按需系统完整性检查

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"**基线系统完整性监控**"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。任务首次启动时会创建基线。

迁移文件完整性监控设置

当您将 Kaspersky Industrial CyberSecurity for Nodes 版本 4.0 或更早版本更新至 4.5 版本时，文件完整性监控和注册表访问监控设置会自动迁移。作为迁移的一部分，应用程序将监控规则移动到系统完整性监控。

关于系统完整性监控规则

要使系统完整性监控正常工作，您必须添加至少一个规则。*系统完整性监控规则*是一组定义用户对文件或注册表的访问权限的标准。系统完整性监控检测指定*监测范围*内文件或注册表的更改。监控范围是系统完整性监控规则的标准之一。

系统完整性监控允许监控以下对象：

- 文件
- 注册表
- 外部设备

文件监控中涉及的特殊注意事项

系统完整性监控监控文件和文件夹的变化以及添加到监控范围或从监控范围中删除的文件。这些更改可能表明存在计算机安全漏洞。我们建议添加很少修改的对象或只有管理员才能访问的对象。这将帮助减少系统完整性监控事件的数量。

Kaspersky Industrial CyberSecurity for Nodes 仅监控实时系统完整性监控开始运行时连接的磁盘上的文件和文件夹的变化。如果实时系统完整性监控开始运行时未连接磁盘，则即使将文件和文件夹添加到监控范围，应用程序也不会监控该磁盘上文件和文件夹的变化。

注册表监控中涉及的特殊注意事项

系统完整性监控负责监控注册表。这些更改可能表明存在计算机安全漏洞。

系统完整性监控监控注册表的以下根键：

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

系统完整性监控不支持 HKEY_CURRENT_USER 键。您可以指定 HKEY_USERS 下的一个键，作为 HKEY_USERS\<user profile ID>\<key>。

外部设备监控涉及的特殊注意事项

系统完整性监控监控外部设备的连接和断开连接。这对于保护计算机免受与此类设备进行文件交换所导致的安全威胁是必要的。系统完整性监控不会监控对外部设备的访问，也不会阻止文件交换。您可以使用不同的应用程序组件配置对设备的访问，例如设备控制。

当运行“*基线系统完整性监控*”任务时，如果外部设备在操作系统中具有相同的驱动器号，则应用程序将忽略该设备的重新连接。为了记录，重新连接的设备必须具有不同的驱动器号。

系统完整性监控监视以下类型的外部设备的连接：

- 可移动驱动器 （包括 USB 闪存驱动器）
- 硬盘驱动器
- 外部网络适配器
- CD/DVD/Blu-ray 驱动器
- 扫描仪/摄像头

实时系统完整性监控

系统完整性监控允许实时跟踪操作系统的变化。您可以跟踪可能表明计算机存在安全漏洞的变化。该组件允许阻止这些更改或仅记录更改事件。

要使系统完整性监控正常工作，您必须添加至少一个规则。系统完整性监控规则是一组定义用户对文件和注册表的访问权限的标准。系统完整性监控检测指定监测范围内文件和注册表的更改。监控范围是系统完整性监控规则的标准之一。

如何在 Kaspersky Security Center 管理控制台中启用和配置实时系统完整性监控

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**系统审查**”。
4. 在“**系统完整性监控**”区域中单击“**设置**”。
5. 选择**系统完整性监控**复选框。
6. 配置“文件完整性监控”：
   a. 选择“**文件**”选项卡上的“**监控文件**”复选框。
   b. 在“**阻止规则的操作模式**”下，选择文件完整性监控模式：
      - “**阻止**”。在此模式下，应用程序根据文件完整性监控规则对文件执行操作，并在系统完整性监控日志中生成相应的事件。
      - “**通知**”。在此模式下，应用程序仅在系统完整性监控日志中生成有关触发的文件完整性监控规则的事件。
   c. 使用 **添加** 按钮或通过从 XML 文件导入来手动添加文件完整性监控规则。文件完整性监控规则设置如下表所述。
   d. 在文件完整性监控规则列表中，管理复选框以启用您需要的规则。
7. 配置注册表访问监控：
   a. 选择“**注册表**”选项卡上的“**监控注册表**”复选框。
   b. 在“**阻止规则的操作模式**”下，选择一个注册表访问监控模式：
      - “**阻止**”。在此模式下，应用程序根据注册表访问监控规则阻止注册表操作，并在系统完整性监控日志中生成相应的事件。
      - “**通知**”。在此模式下，应用程序仅在系统完整性监控日志中生成有关触发的注册表访问监控规则的事件。

c. 使用 **添加** 按钮或通过从 XML 文件导入来手动添加注册表访问监控规则。注册表访问监控规则设置如下表所述。

d. 在注册表访问监控规则列表中，管理复选框以启用您需要的规则。

8. 配置外部设备监控：

a. 选择“**设备**”选项卡上的“**监控设备**”复选框。

b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

应用外部设备监控设置后，应用程序会记住当前的外部设备连接。随后，当外部设备连接或者断开时，应用程序会在系统完整性监控日志中生成相应的事件。

9. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用和配置实时系统完整性监控

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**系统审查 → 系统完整性监控**”并点击“**配置**”按钮。

5. 选择**系统完整性监控**复选框。

6. 配置“文件完整性监控”：

a. 选择“**文件**”选项卡上的“**监控文件**”复选框。

b. 在“**阻止规则的操作模式**”下，选择文件完整性监控模式：

- “**阻止**”。在此模式下，应用程序根据文件完整性监控规则对文件执行操作，并在系统完整性监控日志中生成相应的事件。
- “**通知**”。在此模式下，应用程序仅在系统完整性监控日志中生成有关触发的文件完整性监控规则的事件。

c. 使用 **添加** 按钮或通过从 XML 文件导入来手动添加文件完整性监控规则。文件完整性监控规则设置如下表所述。

d. 在文件完整性监控规则列表中，管理“**状态**”列中的复选框以启用您需要的规则。

7. 配置注册表访问监控：

   a. 选择“**注册表**”选项卡上的“**监控注册表**”复选框。

   b. 在“**阻止规则的操作模式**”下，选择一个注册表访问监控模式：

   - “**阻止**”。在此模式下，应用程序根据注册表访问监控规则阻止注册表操作，并在系统完整性监控日志中生成相应的事件。
   - “**通知**”。在此模式下，应用程序仅在系统完整性监控日志中生成有关触发的注册表访问监控规则的事件。

   c. 使用 **添加** 按钮或通过从 XML 文件导入来手动添加注册表访问监控规则。注册表访问监控规则设置如下表所述。

   d. 在注册表访问监控规则列表中，管理“**状态**”列中的复选框以启用您需要的规则。

8. 配置外部设备监控：

   a. 选择“**设备**”选项卡上的“**监控设备**”复选框。

   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   系统完整性监控记录外部设备的当前连接。在应用程序设置中启用该组件后，应用程序开始监控外部设备的连接和断开连接。随后，当外部设备连接或者断开时，应用程序就会产生相应的事件。

9. 保存更改。

如何在应用程序控制台中启用和配置实时系统完整性监控

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**系统审查**” → “**系统完整性监控**”。
2. 在“**系统完整性监控**”节点的结果窗格中，单击“**属性**”。

   “**属性: 系统完整性监控**”窗口将打开。
3. 选择**系统完整性监控**复选框。
4. 配置“文件完整性监控”：

   a. 选择“**文件**”选项卡上的“**监控文件**”复选框。

   b. 在“**阻止规则的操作模式**”下，选择文件完整性监控模式：

   - “**阻止**”。在此模式下，应用程序根据文件完整性监控规则对文件执行操作，并在系统完整性监控日志中生成相应的事件。
   - “**通知**”。在此模式下，应用程序仅在系统完整性监控日志中生成有关触发的文件完整性监控规则的事件。

   c. 使用 **添加** 按钮或通过从 XML 文件导入来手动添加文件完整性监控规则。文件完整性监控规则设置如下表所述。

   d. 在文件完整性监控规则列表中，管理复选框以启用您需要的规则。

5. 配置注册表访问监控：

   a. 选择“**注册表**”选项卡上的“**监控注册表**”复选框。

   b. 在“**阻止规则的操作模式**”下，选择一个注册表访问监控模式：

   - “**阻止**”。在此模式下，应用程序根据注册表访问监控规则阻止注册表操作，并在系统完整性监控日志中生成相应的事件。
   - “**通知**”。在此模式下，应用程序仅在系统完整性监控日志中生成有关触发的注册表访问监控规则的事件。

   c. 使用 **添加** 按钮或通过从 XML 文件导入来手动添加注册表访问监控规则。注册表访问监控规则设置如下表所述。

   d. 在注册表访问监控规则列表中，管理复选框以启用您需要的规则。

6. 配置外部设备监控：

   a. 选择“**设备**”选项卡上的“**监控设备**”复选框。

   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   应用外部设备监控设置后，应用程序会记住当前的外部设备连接。随后，当外部设备连接或者断开时，应用程序会在系统完整性监控日志中生成相应的事件。

7. 保存更改。

系统完整性监控规则设置

参数	描述
监控该范围的文件操作	您想要应用文件完整性监控的范围。此字段为必填项。 使用掩码： 当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： `*`（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。 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。 `?`（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。
被监控对象	您可以在此处指定注册表项的名称或值。 使用掩码： 输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持 `*` 字符和 `?` 字符：
文件操作	• “**检测**”。应用程序允许对监控范围内的文件进行操作。 • “**检测并阻止**”。应用程序的功能取决于所选的文件完整性监控模式。如果您选择了“*阻止*”模式，系统完整性监控阻止对监控范围内的文件执行操作。如果您选择了“*通知*”模式，系统完整性监控允许对监控范围内的文件执行操作。
受信任的用户和/或用户组	受信任的用户是被允许对监控范围内的文件和注册表项执行操作的用户。 如果 Kaspersky Industrial CyberSecurity for Nodes 检测到受信任用户执行的操作，系统完整性监控会生成“信息” 事件。 您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。
文件操作标记 / 操作	使用应用程序将监控的文件或注册表项来描述操作的标记。
基于所有识别的标记检测文件操作 / 基于所有识别的标记检测注册表操作	默认情况下，Kaspersky Industrial CyberSecurity for Nodes 检测所有文件/注册表操作标记。

参数	描述
基于以下标记检测文件操作 / 基于以下标记检测注册表操作	在可用文件/注册表操作列表中，选中要监控的操作旁边的复选框。
如果可能的话，在文件操作后计算校验和。校验和将显示在任务日志中	如果选中该复选框，当检测到至少带有一个选定标记的文件操作时，Kaspersky Industrial CyberSecurity for Nodes 将计算修改后的文件的校验和。 如果通过多个标记检测到文件操作，只计算所有修改后最终文件的校验和。 如果清除该复选框，Kaspersky Industrial CyberSecurity for Nodes 不计算修改的文件的校验和。 以下情况不会执行任何校验和计算： • 如果文件变为不可用（例如，由于访问权限更改）。 • 如果检测到文件操作的文件后来被删除。 默认下，复选框被清除。
校验和计算算法	从下拉列表中选择其中一个校验和计算算法： • MD5 哈希 • SHA256 哈希
排除项	在“**排除项**”选项卡上，您可以添加想要排除在监控范围之外的对象： • 对于文件完整性监控规则，您可以指定文件夹列表。 • 对于注册表访问监控规则，您可以指定注册表项或值。 使用掩码： **文件** 组件监控的文件和文件夹列表。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： `*`（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。 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。 `?`（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。 **注册表** Kaspersky Industrial CyberSecurity for Nodes 在输入掩码时支持 `*` 和 `?` 字符：排除项条目比监控范围条目具有更高的优先级。
事件严重级别	Kaspersky Industrial CyberSecurity for Nodes 在监控范围内的文件或注册表项被修改时记录文件修改事件。以下事件严重性级别可用：**信息**、**警告**、**关键**。

按需系统完整性检查

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。运行“*基线系统完整性监控*”任务时，应用程序将监控范围内的对象的当前状态与其*基线*状态进行比较。任务首次启动时会创建基线。

要使系统完整性监控正常工作，您必须添加至少一个规则。系统完整性监控规则是一组定义用户对文件和注册表的访问权限的标准。系统完整性监控检测指定监测范围内文件和注册表的更改。监控范围是系统完整性监控规则的标准之一。

配置“基线系统完整性监控”任务的监控范围

默认情况下，“*基线系统完整性监控*”任务的监控范围与系统完整性监控的监控范围相同。您可以为任务配置不同的监控范围。

系统完整性监控不支持为“*系统完整性检查*”任务导入键 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG`。如果任务的监控范围包含这些键，应用程序将生成“*监控范围包括错误对象*”事件。

如何在 Kaspersky Security Center 管理控制台中为“基线系统完整性监控”任务配置不同的监控范围

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”文件夹。
2. 选择必要的“*基线系统完整性监控*”任务并双击以打开任务属性。
3. 在打开的窗口中，选择“**设置**”。
4. 配置文件监控：
   a. 选择“**文件**”选项卡上的“**监控文件**”复选框。
   b. 通过选中复选框来选择列表中的规则。
   c. 如果需要，点击“**添加**”按钮添加新规则。下表描述了基线系统完整性监控规则设置。
   d. 您也可以从其他来源导入规则。
5. 配置注册表监控：
   a. 选择“**注册表**”选项卡上的“**监控注册表**”复选框。
   b. 通过选中复选框来选择列表中的规则。
   c. 如果需要，点击“**添加**”按钮添加新规则。下表描述了基线系统完整性监控规则设置。
   d. 您也可以从其他来源导入规则。
6. 配置外部设备监控：
   a. 选择“**设备**”选项卡上的“**监控设备**”复选框。
   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。
      基线系统完整性监控任务记录基线创建时所连接的外部设备的信息。随后，当外部设备连接时，应用程序就会产生相应的事件。运行任务时，应用程序不会监控外部设备的断开连接。
7. 保存更改。

如何在 Kaspersky Security Center Web Console 中为“基线系统完整性监控”任务配置不同的监控范围

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 选择必要的“*基线系统完整性监控*”任务并双击以打开任务属性。
3. 在打开的窗口中，选择“**应用程序设置**”。
4. 配置文件监控：
   a. 选择**监控文件**复选框。
   b. 通过选中复选框来选择列表中的规则。

c. 如果需要，点击“**添加**”按钮添加新规则。下表描述了基线系统完整性监控规则设置。

d. 您也可以从其他来源导入规则。

5. 配置注册表监控：

a. 选择**监控注册表**复选框。

b. 通过选中复选框来选择列表中的规则。

c. 如果需要，点击“**添加**”按钮添加新规则。下表描述了基线系统完整性监控规则设置。

d. 您也可以从其他来源导入规则。

6. 配置外部设备监控：

a. 选择**监控设备**复选框。

b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

“*基线系统完整性监控*”任务记录基线创建时所连接的外部设备的信息。随后，当外部设备连接时，应用程序就会产生相应的事件。运行任务时，应用程序不会监控外部设备的断开连接。

7. 保存更改。

如何在应用程序控制台中为“基线系统完整性监控”任务配置不同的监控范围

如果任务是在本地创建的，或者如果在策略属性的“**应用程序设置** → **运行本地系统任务**”部分中选择了“**允许使用本地任务**”复选框，则可以在 Kaspersky Industrial CyberSecurity for Nodes 控制台中编辑“**基线系统完整性监控**”任务的属性。

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**系统审查**” → “**基线系统完整性监控**”。

2. 在“**基线系统完整性监控**”节点的结果窗格中，单击“**属性**”。

“**属性: 基线系统完整性监控**”窗口将打开。

3. 配置文件监控：

a. 选择“**文件**”选项卡上的“**监控文件**”复选框。

b. 通过选中复选框来选择列表中的规则。

c. 如果需要，点击“**添加**”按钮添加新规则。下表描述了基线系统完整性监控规则设置。

d. 您也可以从其他来源导入规则。

4. 配置注册表监控：

a. 选择“**注册表**”选项卡上的“**监控注册表**”复选框。

b. 通过选中复选框来选择列表中的规则。

c. 如果需要，点击“**添加**”按钮添加新规则。下表描述了基线系统完整性监控规则设置。

d. 您也可以从其他来源导入规则。

5. 配置外部设备监控：

a. 选择“**设备**”选项卡上的“**监控设备**”复选框。

b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

基线系统完整性监控任务记录基线创建时所连接的外部设备的信息。随后，当外部设备连接时，应用程序就会产生相应的事件。运行任务时，应用程序不会监控外部设备的断开连接。

6. 保存更改。

“基线系统完整性监控”任务规则设置

参数	描述
监控该范围的文件操作	您想要应用文件完整性监控的范围。此字段为必填项。 使用掩码： 当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： `*`（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。 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。 `?`（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。
被监控对象	您可以在此处指定注册表项的名称或值。 使用掩码： 输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持 `*` 字符和 `?` 字符：
排除项	在“**排除项**”选项卡上，您可以添加想要排除在监控范围之外的对象： • 对于文件完整性监控规则，您可以指定文件夹列表。 • 对于注册表访问监控规则，您可以指定注册表项或值。 使用掩码： **文件** 组件监控的文件和文件夹列表。当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： `*`（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。 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。 `?`（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。 **注册表** Kaspersky Industrial CyberSecurity for Nodes 在输入掩码时支持 `*` 和 `?` 字符：排除项条目比监控范围条目具有更高的优先级。
事件严重级别	Kaspersky Industrial CyberSecurity for Nodes 在监控范围内的文件或注册表项被修改时记录文件修改事件。以下事件严重性级别可用：**信息**、**警告**、**关键**。

运行“基线系统完整性监控”任务

“**基线系统完整性监控**”任务允许检查文件或注册表项是否发生变化，还可以检查外部设备的连接。要检查文件是否有更改，您可以在下列模式中运行“**基线系统完整性监控**”任务：

- “**全盘扫描**”。在这种模式下，应用程序会检查文件的所有属性和哈希值。
- “**快速扫描**”。在这种模式下，应用程序仅检查文件的属性。

任务运行的模式不会影响注册表或外部设备的检查。

如何在 Kaspersky Security Center 管理控制台中运行“基线系统完整性监控”任务

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”文件夹。

   任务列表打开。

2. 单击“**新任务**”。

   “任务向导”将启动。按照向导的说明进行操作。

3. 选择“**Kaspersky Industrial CyberSecurity for Nodes → 基线系统完整性监控**”。选择系统完整性监控模式：

   - “**全盘扫描**”。在这种模式下，应用程序会检查文件的所有属性和哈希值。
   - “**快速扫描**”。在这种模式下，应用程序仅检查文件的属性。

4. 选择将要执行任务的计算机。下列选项可用：

   - 选择管理服务器在网络中检测到的计算机：未分配设备。特定设备可包括管理组中的设备以及未分配设备。
   - 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。
   - 指定要运行任务的设备分类。
   - 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。

5. 选择要运行任务的账户。默认情况下，Kaspersky Industrial CyberSecurity for Nodes 将使用本地用户账户的权限启动任务。

6. 为任务配置计划，例如手动或在一周中的某一天。

7. 输入任务名称。

8. 完成向导操作。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Kaspersky Security Center Web Console 中运行“基线系统完整性监控”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**”。

   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“Kaspersky Industrial CyberSecurity for Nodes”。

   b. 在“**任务类型**”下拉列表中，选择“**基线系统完整性监控**”。

   c. 在“**任务名称**”字段中，输入简要说明，例如“*每周系统完整性检查*”。

4. 在“**要对其分配任务的设备**”块，选择任务范围。

5. 按照所选任务范围选项选择设备。转到下一步。

6. 选择校验和计算算法。

7. 选择要运行任务的账户。默认情况下，Kaspersky Industrial CyberSecurity for Nodes 将使用本地用户账户的权限启动任务。

8. 完成向导操作。
   在任务列表中将显示一个新任务。

9. 单击新任务。
   任务属性窗口将打开。

10. 选择**应用程序设置**选项卡。

11. 选择系统完整性检查模式：

    - “**全盘扫描**”。在这种模式下，应用程序会检查文件的所有属性和哈希值。
    - “**快速扫描**”。在这种模式下，应用程序仅检查文件的属性。

12. 保存更改。

13. 选中该任务旁边的复选框。

14. 单击“**开始**”。

导出和导入系统完整性监控规则

您可以将系统完整性监控规则列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的记录。您还可以使用导出/导入功能备份系统完整性监控规则列表或将列表迁移到其他服务器。

系统完整性监控不支持为“*系统完整性检查*”任务导入键 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG`。如果任务的监控范围包含这些键，应用程序将生成“*监控范围包括错误对象*”事件。

如何在 Kaspersky Security Center 管理控制台中导出和导入系统完整性监控规则列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**系统审查**”。
4. 在“**系统完整性监控**”区域中单击“**设置**”。
5. 要导出文件/注册表规则：
   a. 在“**文件**”或“**注册表**”选项卡上，选择您要导出的规则。
   b. 点击“**导出**”按钮并选择“**导出所选**”。
   c. 如果您未选择任何规则，单击“**导出 → 导出**”使 Kaspersky Industrial CyberSecurity for Nodes 导出所有规则。
   d. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   e. 保存文件。
      Kaspersky Industrial CyberSecurity for Nodes 会将整个规则列表导出到 XML 文件。
6. 要导入文件/注册表规则：
   a. 在“**文件**”或“**注册表**”选项卡上单击“**导入**”按钮。
      在打开的窗口中，选择要从中导入规则列表的 XML 文件。
   b. 打开文件。
      如果计算机已经具有规则的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。
7. 保存更改。

如何在 Kaspersky Security Center Web Console 中导出和导入系统完整性监控规则列表

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**系统审查 → 系统完整性监控**”并点击“**配置**”按钮。
   “**系统完整性监控设置**”窗口将打开。

5. 要导出文件/注册表规则：

   a. 在“**文件**”或“**注册表**”选项卡上，选择您要导出的规则。

   b. 点击“**导出**”按钮。这将打开一个窗口；在该窗口中，指定是否要导出选定规则或所有规则，然后单击“**导出**”。

   如果您未选择任何规则，Kaspersky Industrial CyberSecurity for Nodes 将导出所有规则。

   Kaspersky Industrial CyberSecurity for Nodes 会将整个规则列表导出到 XML 文件。

6. 要导入文件/注册表规则：

   a. 在“**文件**”或者“**注册表**”选项卡上，如果您想要从在应用程序 4.0 版本或更早版本中创建的 XML 文件导入规则，点击“**从以前版本导入**”按钮。

   如果您要从在 4.5 版本或更高版本中创建的 XML 文件导入规则，请单击“**导入**”。

   b. 如果计算机已经具有规则的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

   c. 在打开的窗口中，选择要从中导入规则列表的 XML 文件。

   d. 单击“**导入**”。

7. 保存更改。

如何在应用程序控制台中导出和导入系统完整性监控规则列表

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**系统审查**” → “**系统完整性监控**”。

2. 在“**系统完整性监控**”节点的结果窗格中，单击“**属性**”。

   “**属性: 系统完整性监控**”窗口将打开。

3. 要导出文件/注册表规则：

   a. 在“**文件**”或“**注册表**”选项卡上，选择您要导出的规则。

   b. 点击“**导出**”按钮并选择“**导出所选**”。

   c. 如果您未选择任何规则，单击“**导出 → 导出**”使 Kaspersky Industrial CyberSecurity for Nodes 导出所有规则。

   d. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   e. 保存文件。

   Kaspersky Industrial CyberSecurity for Nodes 会将整个规则列表导出到 XML 文件。

4. 要导入文件/注册表规则：

   a. 在“**文件**”或“**注册表**”选项卡上单击“**导入**”按钮。

   在打开的窗口中，选择要从中导入规则列表的 XML 文件。

b. 打开文件。

如果计算机已经具有规则的列表，则 Kaspersky Industrial CyberSecurity for Nodes 将提示您删除现有列表或从 XML 文件向其中添加新条目。

5. 保存更改。

查看系统完整性监控报告

要分析系统完整性监控规则的性能，您可以查看应用程序生成的报告和事件。Kaspersky Industrial CyberSecurity for Nodes 生成有关该组件的以下报告：

- 在应用程序界面中：
  - 基线更新报告。

  报告包含系统完整性监控事件。
- 在 Kaspersky Security Center 控制台中
  - 监控规则触发次数最多的计算机报告
  - 最常触发的监控规则报告

    为了生成有关最常触发的监控规则的报告，应用程序会记录以下事件：
    - *检测到文件或文件夹更改*
    - *仅统计: 受控制区域内禁止的文件操作*
    - *已允许受信任用户在受控制区域执行文件操作*
    - "*受控区域中不受控制的文件操作*"。

      要配置这些事件的存储期限，请在策略的"**事件配置**"部分，指定一般系统完整性监控事件："*检测到文件或文件夹更改*"的持续时间。

默认情况下，将创建前 30 天的报告，包括创建报告的日期。

如何在 Kaspersky Security Center 管理控制台中查看系统完整性监控报告

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的"**管理服务器**"中选择"**报告**"选项卡。
3. 单击"**新建报告模板**"。

   "新报告模板向导"将启动。

4. 按照“报告模板向导”的说明进行操作。在“**选择报告模板类型**”步骤，选择系统完整性监控报告（“**其他**”部分）：

   - “**文件完整性监控/系统完整性监控规则触发最频繁的 10 台设备**”。
   - “**在设备上触发次数最频繁的 10 条文件完整性监控/系统完整性监控规则**”。

   完成新报告模板向导之后，新报告模板将出现在“**报告**”选项卡上。

5. 双击报告将其打开。

报告生成过程将开始。该报告将显示在新窗口中。

如何在 Kaspersky Security Center Web Console 中查看系统完整性监控报告

1. 在 Web Console 的主窗口中，选择“**监控和报告**” → “**报告**”。
2. 单击“**添加**”。
   “新报告模板向导”将启动。
3. 在“**模板**”下，在“**其他**”部分中，选择系统完整性监控报告：

   - “**文件完整性监控/系统完整性监控规则触发最频繁的 10 台设备**”。
   - “**在设备上触发次数最频繁的 10 条文件完整性监控/系统完整性监控规则**”。

   完成新报告模板向导之后，新报告模板将出现在表格中。

4. 选择并运行报告。

报告生成过程将开始。该报告将显示在新窗口中。

要查看应用程序生成的事件，您还可以使用 Kaspersky Security Center 控制台中的事件分类。

日志审查

日志检查根据 Windows 事件日志分析监控受保护环境的完整性。当应用程序在系统中检测到非典型行为的迹象时，它会通知管理员，因为该行为可能表示试图进行网络攻击。

Kaspersky Industrial CyberSecurity for Nodes 分析 Windows 事件日志，并根据规则检测违规行为。该组件包括预定义规则。预定义规则由启发式分析提供支持。您还可以添加自己的规则（自定义规则）。当规则触发时，应用程序将创建具有“*严重*”状态的事件。

如果您要使用日志审查，请确保已配置安全审计策略，并且系统正在记录相关事件（有关详细信息，请参阅 Microsoft 技术支持网站）。

参数	描述
预定义规则	日志审查规则列表。预定义规则包括受保护计算机上异常活动的模板。异常活动可能表示攻击未遂。
自定义规则	用户添加的日志审查规则列表。您可以设置自己的日志审查规则和触发条件。为此，您必须输入事件 ID 并选择事件源。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。

添加自定义规则

您可以设置自己的日志审查规则和触发条件。为此，您必须输入事件 ID 并选择事件源。您可以在 Microsoft 技术支持网站上查找事件 ID。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。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如，*Windows PowerShell* 日志）。

应用程序不检查指定的日志是否实际存在于 Windows 事件日志中。如果日志名称有错误，则应用程序不会监控该日志中的事件。

自定义规则列表已经包括卡巴斯基专家创建的几个规则。

如何在 Kaspersky Security Center 管理控制台中添加自定义规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**系统审查**”。
4. 在“**日志审查**”区域中单击“**设置**”。
5. 选择**日志审查**复选框。
6. 在“**自定义规则**”选项卡上，选中“**应用日志审查的自定义规则**”复选框。
7. 选中要启用的自定义规则旁边的复选框。

8. 如有必要，单击“**添加**”创建您自己的自定义规则。
9. 这打开了一个窗口；在该窗口中，配置自定义规则：
   - “**规则名称**”。
   - “**日志名称**”。Windows 事件日志。有以下日志可用： *Application*、*Security*、*System*。
   - “**源**”。第三方应用程序日志。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如，Windows PowerShell 日志）。
   - “**事件标识符**”。Windows 事件日志中的事件 ID。您可以在 Microsoft 技术文档中查找事件 ID。
10. 保存更改。

如何在 Kaspersky Security Center Web Console 中添加自定义规则

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**系统审查 → 日志审查**”并点击“**配置**”按钮。
5. 选择**启用日志审查**复选框。
6. 在“**自定义规则**”选项卡上，选中“**应用日志审查的自定义规则**”复选框。
7. 使用切换按钮配置自定义规则：
8. 如有必要，单击“**添加**”创建您自己的自定义规则。
9. 这打开了一个窗口；在该窗口中，配置自定义规则：
   - “**规则名称**”。
   - “**Windows 事件日志名称**”。Windows 事件日志。有以下日志可用： *Application*、*Security*、*System*。
   - “**源**”。第三方应用程序日志。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如，Windows PowerShell 日志）。
   - “**事件 ID**”。Windows 事件日志中的事件 ID。您可以在 Microsoft 技术文档中查找事件 ID。
10. 保存更改。

如何在应用程序控制台中添加自定义规则

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**系统审查**” → “**日志审查**”。
2. 在“**日志审查**”节点的结果窗格中，单击“**属性**”。
   这将打开“**属性：日志审查**”窗口。
3. 选择**日志审查**复选框。
4. 在“**自定义规则**”选项卡上，选中“**应用日志审查的自定义规则**”复选框。
5. 选中要启用的自定义规则旁边的复选框。
6. 如有必要，单击“**添加**”创建您自己的自定义规则。
7. 这打开了一个窗口；在该窗口中，配置自定义规则：
   - “**规则名称**”。
   - “**日志名称**”。Windows 事件日志。有以下日志可用： *Application*、*Security*、*System*。
   - “**源**”。第三方应用程序日志。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如，Windows PowerShell 日志）。
   - “**事件标识符**”。Windows 事件日志中的事件 ID。您可以在 Microsoft 技术文档中查找事件 ID。
8. 保存更改。

因此，当触发规则时，Kaspersky Industrial CyberSecurity for Nodes 创建“*严重*”事件。

配置预定义规则

预定义规则包括受保护计算机上异常活动的模板。异常活动可能表示攻击未遂。预定义规则由启发式分析提供支持。有七条预定义规则可用于日志审查。您可以启用或禁用任意这些规则。无法删除预定义规则。

您可以为监视以下操作事件的规则配置触发条件：

- 密码强力检测
- 网络登录检测

如何在 Kaspersky Security Center 管理控制台中配置预定义规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**系统审查**”。

4. 在“**日志审查**”区域中单击“**设置**”。

5. 选择**日志审查**复选框。

6. 在“**预定义规则**”选项卡上，选中“**应用日志审查的预定义规则**”复选框。

7. 选择或清空复选框以配置预定义规则：

   - “**系统中存在可能的暴力攻击模式**”。
   - “**在网络登录会话期间检测到非典型活动**”。
   - “**存在可能的 Windows 事件日志滥用模式**”。
   - “**检测到代表安装了新服务的非典型操作**”。
   - “**检测到使用显式凭证的非典型登录**”。
   - “**系统中存在可能的 Kerberos 伪造的 PAC (MS14-068) 攻击模式**”。
   - “**在特权内置管理员组中检测到可疑更改**”。

8. 如果必要，配置“**系统中存在可能的暴力攻击模式**”规则：

   a. 单击规则旁边的“**设置**”按钮。

   b. 在打开的窗口中，指定要触发规则必须尝试输入密码的次数和时间段。

   c. 单击“**确定**”。

9. 如果您选择了“**在网络登录会话期间检测到非典型活动**”规则，您需要配置其设置：

   a. 单击规则旁边的“**设置**”按钮。

   b. 在打开的窗口中，在“**网络登录检测**”块中，指定时间间隔的开始和结束。

   Kaspersky Industrial CyberSecurity for Nodes 将在所定义期间执行的登录尝试视为异常活动。

   默认情况下，不设置间隔，并且应用程序不监控登录尝试。要让应用程序连续监控登录尝试，请将间隔设置为 12:00 AM - 11:59 PM。间隔的开始和结束不能重合。如果它们相同，则应用程序不会监控登录尝试。

   c. 创建受信任用户和受信任 IP 地址（IPv4 和 IPv6）列表。

   您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。Kaspersky Industrial CyberSecurity for Nodes 不监控这些用户和计算机的登录尝试。

   > 在 Windows XP 上运行的应用程序中，通过 IP 地址排除受信任的计算机不起作用。

   d. 单击“**确定**”。

10. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置预定义规则

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**系统审查 → 日志审查**”并点击“**配置**”按钮。
5. 选择**启用日志审查**复选框。
6. 在“**预定义规则**”选项卡上，选中“**应用日志审查的预定义规则**”复选框。
7. 使用切换按钮配置预定义规则：
   - “**系统中存在可能的暴力攻击模式**”。
   - “**在网络登录会话期间检测到非典型活动**”。
   - “**存在可能的 Windows 事件日志滥用模式**”。
   - “**检测到代表安装了新服务的非典型操作**”。
   - “**检测到使用显式凭证的非典型登录**”。
   - “**系统中存在可能的 Kerberos 伪造的 PAC (MS14-068) 攻击模式**”。
   - “**在特权内置管理员组中检测到可疑更改**”。
8. 在“**扩展**”选项卡上，配置以下设置：
   - 为触发规则“**系统中存在可能的暴力攻击模式**”，必须尝试输入密码的次数和时间段。
   - 为触发“**在网络登录会话期间检测到非典型活动**”规则，指定应用程序将所有登录尝试视为异常活动的时间间隔的开始和结束。
     默认情况下，不设置间隔，并且应用程序不监控登录尝试。要让应用程序连续监控登录尝试，请将间隔设置为 12:00 AM - 11:59 PM。间隔的开始和结束不能重合。如果它们相同，则应用程序不会监控登录尝试。
9. 在相应的选项卡上创建受信任用户和受信任 IP 地址（IPv4 和 IPv6）列表。
   您可以从账户列表中选择用户，或者手动输入本地用户名。

   > 在 Windows XP 上运行的应用程序中，通过 IP 地址排除受信任的计算机不起作用。

10. 保存更改。

如何在应用程序控制台中配置预定义规则

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**系统审查**” → “**日志审查**”。
2. 在“**日志审查**”节点的结果窗格中，单击“**属性**”。
   这将打开“**属性：日志审查**”窗口。
3. 选择**日志审查**复选框。
4. 在“**预定义规则**”选项卡上，选中“**应用日志审查的预定义规则**”复选框。
5. 选择或清空复选框以配置预定义规则：
   - “**系统中存在可能的暴力攻击模式**”。
   - “**在网络登录会话期间检测到非典型活动**”。
   - “**存在可能的 Windows 事件日志滥用模式**”。
   - “**检测到代表安装了新服务的非典型操作**”。
   - “**检测到使用显式凭证的非典型登录**”。
   - “**系统中存在可能的 Kerberos 伪造的 PAC (MS14-068) 攻击模式**”。
   - “**在特权内置管理员组中检测到可疑更改**”。
6. 如果必要，配置“**系统中存在可能的暴力攻击模式**”规则：
   a. 单击规则旁边的“**设置**”按钮。
   b. 在打开的窗口中，指定要触发规则必须尝试输入密码的次数和时间段。
   c. 单击“**确定**”。
7. 如果您选择了“**在网络登录会话期间检测到非典型活动**”规则，您需要配置其设置：
   a. 单击规则旁边的“**设置**”按钮。
   b. 在打开的窗口中，在“**网络登录检测**”块中，指定时间间隔的开始和结束。
      Kaspersky Industrial CyberSecurity for Nodes 将在所定义期间执行的登录尝试视为异常活动。
      默认情况下，不设置间隔，并且应用程序不监控登录尝试。要让应用程序连续监控登录尝试，请将间隔设置为 12:00 AM - 11:59 PM。间隔的开始和结束不能重合。如果它们相同，则应用程序不会监控登录尝试。
   c. 创建受信任用户和受信任 IP 地址（IPv4 和 IPv6）列表。
      您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。从活动目录创建用户列表。Kaspersky Industrial CyberSecurity for Nodes 不监控这些用户和计算机的登录尝试。

在 Windows XP 上运行的应用程序中，通过 IP 地址排除受信任的计算机不起作用。

d. 单击“**确定**”。

8. 保存更改。

因此，当触发规则时，Kaspersky Industrial CyberSecurity for Nodes 创建“*严重*”事件。

性能分析器

*性能分析器*任务创建具有最多访问尝试的最活跃的应用程序和文件的列表。此信息可以帮助您定义受信任区域，以最大限度地减少应用程序对工业软件性能的影响。

要让“*性能分析器*”任务正常工作，启动该任务的计算机必须运行 Windows Vista 或更高版本。

您仅可以在 Kaspersky Security Center Web Console 和应用程序控制台中管理此任务。

任务设置和在 Kaspersky Security Center Web Console 中运行“性能分析器”任务

1. 启动新任务向导。
2. 在“**任务类型**”下拉列表中，选择“**性能分析器**”。
3. 输入任务名称或保留默认名称。
4. 选择要分配任务的设备并单击“**下一步**”按钮。
5. 在“**任务范围**”窗口中，指定任务范围并单击“**下一步**”。
6. 在“**选择账户以运行任务**”窗口中，指定一个账户并单击“**下一步**”按钮。
7. 在“**完成任务创建**”窗口中，选择“**创建完成时打开任务详情**”复选框并单击“**完成**”。
8. 这将打开一个窗口；在该窗口中，选择“**应用程序设置**”选项卡。
9. 转到**性能分析器设置**区域。
10. 在“**在此时间后自动停止任务**”字段中，以小时（1–168 小时）或天（1–7 天）为单位设置时间间隔，在此间隔之后，Kaspersky Industrial CyberSecurity for Nodes 必须停止分析。
11. 如果必要，在“**规则生成范围限制**”下，创建一个您希望 Kaspersky Industrial CyberSecurity for Nodes 在其中执行分析以生成排除规则的文件夹列表：

    当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：您还可以通过以 UNC（通用命名约定）格式指定网络文件夹或文件的路径，将其添加到扫描范围。

    默认情况下，Kaspersky Industrial CyberSecurity for Nodes 在没有限制范围的情况下运行任务。
12. 选择“**计划**”选项卡并配置任务计划。
13. 保存更改。
14. 选中已创建任务名称旁边的复选框，然后单击“**开始**”按钮。

管理设置和在应用程序控制台中运行“性能分析器”任务

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**系统审查**” → “**性能分析器**”。
2. 在结果窗格中，单击“**属性**”链接。
3. 这将打开一个窗口；在该窗口中，在“**任务设置**”选项卡上，在“**在此时间后停止任务**”字段中，以小时（1–168 小时）或天（1–7 天）为单位设置时间间隔，在此间隔之后，Kaspersky Industrial CyberSecurity for Nodes 必须停止分析。
4. 如果必要，在“**规则生成范围**”下，创建一个您希望 Kaspersky Industrial CyberSecurity for Nodes 在其中执行分析以生成排除规则的文件夹列表：

   当输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符：您还可以通过以 UNC（通用命名约定）格式指定网络文件夹或文件的路径，将其添加到扫描范围。

   默认情况下，Kaspersky Industrial CyberSecurity for Nodes 在没有限制范围的情况下运行任务。
5. 转到“**运行模式**”选项卡。
6. 选择“**手动**”或配置任务运行模式。
7. 如果必要，在“**用户**”下，指定运行任务的用户账户。
8. 点击“**确定**”保存更改。
9. 在“**管理**”区域，单击“**启动**”链接。

您可以将“*性能分析器*”任务结果直接导出到 Kaspersky Industrial CyberSecurity for Nodes 策略的受信任区域设置或应用程序的本地受信任区域设置，也可以将报告中的对象信息保存到 XML 文件中，然后将其导入设置。

Kaspersky Industrial CyberSecurity for Nodes 将报告中的文件添加到扫描排除列表中，并将应用程序添加到受信任区域的受信任应用程序列表中。

在 Kaspersky Security Center Web Console 中导出“性能分析器”任务的结果

1. 要导出本地任务结果，请执行以下操作：
   a. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
   b. 单击您要对其配置任务设置的设备的名称。
   c. 在打开的“**<设备名称>**”窗口中，选择“**任务**”选项卡。
   d. 单击相关的“性能分析器”任务。
2. 要导出组任务结果，请执行以下操作：
   a. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
   b. 单击相关的“性能分析器”任务。

3. 这将打开一个窗口；在该窗口中，选择“**应用程序设置**”选项卡。
   任务属性窗口将打开。
4. 转到**性能分析器结果**区域。
5. 选择“**考虑文件哈希**”复选框以在报告中包含哈希。默认下，复选框被清除。
6. 如果必要，清除“**考虑文件路径**”复选框以从报告中排除文件路径。默认选中该复选框。

   必须至少选中“**考虑文件哈希**”和“**考虑文件路径**”复选框中的一个。

7. 在“**文件**”和“**应用程序**”选项卡上选择要导出的对象。
   您可以导出整个报告，也可以展开报告并选择要导出的单个对象。
8. 要将任务结果导出到策略的受信任区域设置，请执行以下操作：
   a. 单击“**导出到设置**”。
   b. 这将打开一个窗口；在该窗口中，选中要将设置导出到的策略名称旁边的复选框，然后单击“**导出**”按钮。
      如果已在策略中配置排除列表，则 Kaspersky Industrial CyberSecurity for Nodes 会将新条目添加到此列表中。
9. 要将任务结果导出到 XML 文件，请执行以下操作：
   a. 单击“**导出至文件**”。
   b. 单击“**导出**”。这将打开一个窗口；在该窗口中，指定是要导出选定对象还是所有对象，然后单击“**导出**”。

在应用程序控制台中导出“性能分析器”任务结果

如果在策略的“**补充 → 受信任区域**”部分中的“**扫描排除项**”和“**受信任应用程序**”选项卡上选择了“**允许使用本地排除项**”和“**允许编辑本地受信任应用程序**”，则可以在 Kaspersky Industrial CyberSecurity for Nodes 控制台中将“性能分析器”任务的结果导出到 Kaspersky Industrial CyberSecurity for Nodes 的本地受信任区域设置中。

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**系统审查**” → “**性能分析器**”。
2. 在结果窗格中，单击“**结果**”链接。
   “**性能分析器结果**”窗口将打开。
3. 选择“**考虑文件哈希**”复选框以在报告中包含哈希。默认下，复选框被清除。
4. 如果必要，清除“**考虑文件路径**”复选框以从报告中排除文件路径。默认选中该复选框。

   必须至少选中“**考虑文件哈希**”和“**考虑文件路径**”复选框中的一个。

5. 在“**文件**”和“**应用程序**”选项卡上选择要导出的对象。

   您可以导出整个报告，也可以展开报告并选择要导出的单个对象。

6. 要将任务结果导出到应用程序的受信任区域设置，请执行以下操作：

   a. 单击“**导出到设置**”。

   b. 确认您要将所选对象导出到受信任区域设置。

      如果已在设置中配置排除列表，则 Kaspersky Industrial CyberSecurity for Nodes 会将新条目添加到此列表中。

7. 要将任务结果导出到 XML 文件，请执行以下操作：

   a. 单击“**导出至文件**”。

   b. 在打开的窗口中，指定您要将对象列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

按需扫描

本节提供有关按需扫描任务的信息，并说明如何配置按需扫描任务设置和受保护设备上的安全性设置。

关于按需扫描任务

Kaspersky Industrial CyberSecurity for Nodes 会扫描指定区域，以检测病毒和其他计算机安全威胁。Kaspersky Industrial CyberSecurity for Nodes 将扫描受保护设备文件、RAM 以及自动运行对象。

Kaspersky Industrial CyberSecurity for Nodes 提供以下按需扫描任务：

- "*在操作系统启动时扫描*"任务在每次 Kaspersky Industrial CyberSecurity for Nodes 启动时都会执行。应用程序将扫描硬盘驱动器和可移动驱动器的引导扇区和主引导记录、系统内存以及进程内存。Kaspersky Industrial CyberSecurity for Nodes 每次运行该任务时，都会创建未感染的引导扇区的副本。如果在这些扇区中检测到威胁，则下次任务启动时，会将这些扇区替换为备份副本。

  "*在操作系统启动时扫描*"任务在安装后会自动创建。默认应用"**通知**"模式。在这种情况下，在设备上部署 Kaspersky Industrial CyberSecurity for Nodes 后，如果在扫描期间未发现系统服务问题，您可以启用"*在操作系统启动时扫描*"任务。如果应用程序将关键系统服务检测为受感染或可能受感染的对象，"**通知**"模式会让您有时间找出原因并解决问题。清除或删除系统文件可能会导致操作系统启动出现严重问题。如果应用程序应用"**建议**"模式，则执行以下操作：**执行建议的操作**。

  > 如果受保护设备在睡眠或休眠模式后唤醒，则可能不会执行"*在操作系统启动时扫描*"任务。仅当受保护设备重新启动或在完全关闭后启动时才执行该任务。

- 默认情况下，根据计划每周执行一次"*关键区域扫描*"任务。Kaspersky Industrial CyberSecurity for Nodes 将扫描操作系统关键区域中的对象：自动运行对象、硬盘驱动器和可移动驱动器的引导扇区和主引导记录、系统内存以及进程内存。Kaspersky Industrial CyberSecurity for Nodes 将应用与"**通知**"对应的安全性设置。您可以修改"*关键区域扫描*"任务的设置。

- "*应用程序完整性控制*"任务每天执行。它提供了检查 Kaspersky Industrial CyberSecurity for Nodes 模块是否损坏或修改的选项。检查程序安装文件夹。任务执行统计指示检查的模块数和发现损坏的模块数。默认情况下，任务设置值已定义，无法编辑。可以编辑任务启动计划设置。

- *可移动驱动器扫描*任务将扫描您运行或复制的所有文件，即使文件位于可移动驱动器上。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。

- "*全盘扫描*"任务每周执行一次。该任务确保对受保护的设备进行彻底扫描，包括系统备份存储、引导扇区和邮件数据库。

此外，您还可以创建自定义按需扫描任务，例如，扫描受保护设备上的共享文件夹的任务。

Kaspersky Industrial CyberSecurity for Nodes 可以一次运行多个按需扫描任务。

关于任务扫描范围和安全设置

在应用程序控制台中，选定按需扫描任务的扫描范围以 Kaspersky Industrial CyberSecurity for Nodes 可以控制的受保护设备文件资源列表的形式显示。

项或节点将显示在受保护设备文件资源的列表视图模式中，如下所示：

☑ 该节点包括在扫描范围内。

☐ 该节点已从扫描范围中排除。

安全性设置

在所选的按需扫描任务中，若要修改默认安全性设置，可通过将它们配置为用于整个保护或扫描范围的常规设置，或为设备文件资源列表中的不同节点或项配置不同设置。

如果同一对象包含在多个保护范围条目中，并且这些条目具有不同的安全级别，则列表中的最后一条规则具有优先级。例如，考虑包含两个条目的保护范围：“**所有硬盘驱动器**”（安全级别“**通知**”）和“`*\Users\*\Downloads\*`”（安全级别“**自定义**”）。应用程序根据“通知”级别扫描硬盘驱动器，但“`Downloads`”文件夹除外。应用程序根据手动指定的设置扫描“`Downloads`”文件夹，因为该条目是保护范围列表中的最后一个条目。

为所选父节点配置的安全设置将自动应用到所有子节点。父节点的安全设置不会应用到单独配置的子节点。

您可以使用以下方式之一配置选定扫描范围或保护范围的设置：

- 从三个预定义的安全级别中选择一个级别（**最高性能**、**建议**或**最大保护**）。
- 在受保护设备文件资源列表中手动更改选定节点或项的安全性设置（安全级别更改为“**自定义**”）。

预定义的扫描范围

所选按需扫描任务的受保护设备文件资源列表显示在“**扫描范围**”窗口中。

文件资源列表显示基于配置的 Microsoft Windows 安全设置拥有读取访问权限的节点。

Kaspersky Industrial CyberSecurity for Nodes 包含以下预定义扫描范围：

- “**所有硬盘驱动器**”。Kaspersky Industrial CyberSecurity for Nodes 扫描受保护设备硬盘驱动器上的对象。您可以在扫描范围中包含或排除所有硬盘驱动器、单个磁盘、文件夹或文件。
- “**所有可移动驱动器**”。Kaspersky Industrial CyberSecurity for Nodes 扫描外部设备（如 CD 或可移动驱动器）上的文件。您可以在扫描范围中包含或排除所有可移动驱动器、单个磁盘、文件夹或文件。
- “**所有网络驱动器**”。您可以按照 UNC（通用命名惯例）格式指定网络文件夹或文件的路径以将它们添加至扫描范围。用于启动任务的账户必须拥有对所添加网络文件夹和文件的访问权限。默认情况下，按需扫描任务在系统账户下运行。

  已连接的网络驱动器也不会显示在受保护设备文件资源树中。若要在扫描范围中包含网络驱动器上的对象，请以 UNC 格式指定对应于该网络驱动器的文件夹。

- “**内核内存**”。在启动扫描之后，Kaspersky Industrial CyberSecurity for Nodes 将扫描操作系统中正在运行的进程的可执行文件和模块。

- “**正在运行的进程和启动对象**”。Kaspersky Industrial CyberSecurity for Nodes 扫描注册表项和配置文件所引用的对象，例如 WIN.INI 或 SYSTEM.INI，以及在受保护设备启动时自动启动的应用程序模块。
- “**磁盘引导扇区**”。Kaspersky Industrial CyberSecurity for Nodes 扫描硬盘和可移动媒体的引导扇区。
- “**我的电子邮件**”。Kaspersky Industrial CyberSecurity for Nodes 扫描与 Outlook 邮件客户端相关的文件：数据文件 (PST)、脱机数据文件 (OST)。
- “**系统备份**”。Kaspersky Industrial CyberSecurity for Nodes 扫描 System Volume Information 文件夹的内容。

默认情况下，标准扫描范围显示在网络文件资源树中。在扫描范围设置中创建网络文件资源列表时，可以将它们添加到网络文件资源列表中。

默认情况下，“按需扫描”任务在以下范围下运行：

- “*在操作系统启动时扫描*”任务：
  - “**内核内存**”。
  - “**磁盘引导扇区**”。
- “*关键区域扫描*”任务：
  - **所有硬盘驱动器** （不包括 Windows 文件夹）。
  - “**所有可移动驱动器**”。
  - “**内核内存**”。
  - “**正在运行的进程和启动对象**”。
- “*按需扫描*”任务：
  - **所有硬盘驱动器** （不包括 Windows 文件夹）。
  - “**所有可移动驱动器**”。
  - “**内核内存**”。
  - “**正在运行的进程和启动对象**”。
- “*全盘扫描*”任务：
  - **所有硬盘驱动器** （不包括 Windows 文件夹）。
  - “**所有可移动驱动器**”。
  - “**内核内存**”。
  - “**正在运行的进程和启动对象**”。
  - “**系统备份**”。
  - “**磁盘引导扇区**”。
  - “**我的电子邮件**”。

在线存储文件扫描

关于云文件

Kaspersky Industrial CyberSecurity for Nodes 可以与 Microsoft OneDrive 云文件进行交互。该应用程序支持新的“OneDrive 文件按需”功能。

Kaspersky Industrial CyberSecurity for Nodes 不支持其他在线存储。

“OneDrive 文件随选”帮助您访问所有 OneDrive 文件，而无需下载所有文件和使用设备上的存储空间。您可以在需要时将文件下载到硬盘驱动器。

当“OneDrive 按需文件”功能开启时，可以在文件资源管理器的“**状态**”列中看到每个文件旁边的状态图标。每个文件都具有以下状态之一：

此状态图标指示文件*仅在线可用*。仅在线文件不会物理存储在您的硬盘驱动器中。当设备未连接到 Internet 时，无法打开仅在线文件。

此状态图标指示文件*本地可用*。当打开仅在线文件时会显示此图标，该文件会下载到您的设备中。您可以随时打开本地可用的文件，即使没有 Internet 访问权限。要清理空间，可以将文件更改回 仅在线。

此状态图标指示文件*存储在硬盘驱动器中并且始终可用*。

云文件扫描

Kaspersky Industrial CyberSecurity for Nodes 只能扫描受保护设备上本地存储的云文件。此类 OneDrive 文件的状态为 和 。在扫描期间会跳过 文件，因为这些文件没有物理存储在受保护设备上。

Kaspersky Industrial CyberSecurity for Nodes 在扫描时不会自动从云端下载 文件，即使这些文件已包括在扫描范围中。

在各种方案中，云文件由多种 Kaspersky Industrial CyberSecurity for Nodes 任务处理，具体取决于任务类型：

- 实时云文件扫描：您可以将包含云文件的文件夹添加到“实时文件保护”任务的保护范围中。当用户访问该文件时会对其进行扫描。如果用户访问 文件，系统会下载该文件，该文件将变为本地可用，并且其状态将更改为 。这样该文件可以被“实时文件保护”任务处理。
- 按需云文件扫描：您可以将包含云文件的文件夹添加到“按需扫描”任务的扫描范围中。该任务会扫描状态为 和 的文件。如果在范围中找到任何 文件，在扫描期间将跳过这些文件，并在任务日志中记录信息事件，指示所扫描的文件只是云文件的占位符，并不存在于本地驱动器中。

- 生成和使用应用程序启动控制规则：您可以使用“应用程序启动控制规则生成器”任务为 和 文件创建允许和拒绝规则。“应用程序启动控制”任务应用“默认拒绝”原则和所创建的规则来处理和阻止云文件。

  “应用程序启动控制”任务会阻止所有云文件启动，不管它们的状态如何。应用程序不会将 文件包括在规则生成范围中，因为它们没有物理存储在硬盘驱动器上。由于不能为此类文件创建允许规则，因此对它们实施“默认拒绝”原则。

在 OneDrive 云文件中检测到威胁时，应用程序会应用执行扫描的任务的设置中指定的操作。因此，可以将文件删除、清除、移至隔离区或备份。

按照相关 Microsoft OneDrive 文档中概述的原则，对本地文件的更改将与 OneDrive 中存储的副本进行同步。

关于预定义安全级别

“**使用启发式分析**”安全设置不包含在预设安全级别的设置中。更改此设置不会改变您选择的默认安全级别。

您可以将四个预定义安全级别之一应用于设备文件资源树中选择的节点：**最高性能**、**建议**、**最大保护**或**通知**。每个级别都包含其自有的预定义安全设置（请参见下表）。

最高性能

如果您的网络除了在受保护设备和工作站上使用 Kaspersky Industrial CyberSecurity for Nodes 外，还有其他受保护设备安全措施，例如防火墙和现有安全策略，则建议使用“**最高性能**”安全级别。

建议

“**建议**”安全级别确保保护与对设备的性能影响的最佳组合。Kaspersky 专家推荐此级别，因为其足以保护大多数公司网络上的设备。默认情况下，将设置“**建议**”安全级别。

最大保护

如果组织的网络有更高的设备安全要求，则推荐使用“**最大保护**”安全级别。

通知

如果企业网络中可能存在多台受感染的计算机，而阻止这些计算机可能会严重扰乱组织的运营，则推荐“**通知**”安全级别。

预定义的安全级别和对应的安全性设置值

选项	安全级别			
最高性能	**建议**	**最大保护**	**通知**	
对象类型	按格式扫描对象	所有对象	所有对象	所有对象
仅扫描新建和已修改的文件	已启用	已禁用	已禁用	已禁用
对受感染对象和其他对象执行的操作	清除。清除失败则删除	执行卡巴斯基专家建议的操作	清除。清除失败则删除	通知

选项	安全级别			
扫描复合文件	扫描 Microsoft Office 格式的分发包和文件	扫描所有 Microsoft Office 格式的档案、分发包和文件	扫描所有 Microsoft Office 格式的档案、分发包和文件	扫描所有 Microsoft Office 格式的档案、分发包和文件
系统关键对象是操作系统和 Kaspersky Industrial CyberSecurity for Nodes 运行所需的文件。这些文件无法删除。与此类对象关联的进程无法终止。				
将操作应用于选定的对象类型	默认情况下，扫描所有对象类型	默认情况下，扫描所有对象类型	默认情况下，扫描所有对象类型	默认情况下，扫描所有对象类型
在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件	否	否	否	否
排除文件	否	否	否	否
不按类型检测对象	否	否	否	否
如果扫描时间超过此值则停止(秒)	60 秒	否	否	否
不扫描大于此值的复合对象(MB)	8 MB	否	否	否
使用 iSwift 技术	是	是	是	是
使用 iChecker 技术	是	是	是	是

可移动驱动器扫描

可以配置通过 USB 端口连接到受保护设备的可移动驱动器的扫描。

当连接的可移动驱动器在操作系统中注册为 USB 外部设备时，Kaspersky Industrial CyberSecurity for Nodes 将扫描这些可移动驱动器。如果连接被设备控制任务阻止，则应用程序不会扫描可移动驱动器。

Kaspersky Industrial CyberSecurity for Nodes 允许在扫描期间访问可移动驱动器。

每个可移动驱动器的扫描结果提供在连接可移动驱动器时创建的按需扫描任务的任务日志中。

可以更改“可移动驱动器扫描”组件的设置（请参见以下表格）。

可移动驱动器扫描设置

参数	默认值	描述
扫描通过 USB 连接的可移动驱动器	已清除	您可以打开或关闭通过 USB 连接到受保护设备的可移动驱动器的扫描。
扫描大小未超过此值的可移动驱动器(MB)	4096 MB	您可通过在可移动驱动器上设置最大数据量，来缩小组件的范围。 如果存储的数据量超出指定值，Kaspersky Industrial CyberSecurity for Nodes 不会扫描可移动驱动器。

使用此安全级别扫描	最佳保护	您可通过选择以下三个安全级别之一来配置创建的按需扫描任务： • **最大保护** • **建议** • **最高性能** • **通知** 当检测到已感染、可能已感染和其他对象时使用的算法，以及每个安全级别的其他扫描设置，对应于按需扫描任务中的预设安全级别。

默认按需扫描任务设置

默认情况下，按需扫描任务将使用下表所述的设置。您可以配置本地系统和自定义按需扫描任务。

默认按需扫描任务设置

参数	默认值	描述
扫描范围	应用于本地系统和自定义任务： • **在操作系统启动时扫描**：整个受保护设备，排除共享文件夹和自动运行对象。 • **关键区域扫描**：整个受保护设备，排除共享文件夹和某些操作系统文件。 • **按需扫描**（自定义任务）：整个受保护设备。 • **全盘扫描**：彻底扫描受保护设备。	您可以更改扫描范围。无法为“**可移动驱动器扫描**”和“**应用程序完整性控制**”本地系统任务配置扫描范围。
安全性设置	整个扫描范围的常规设置；对应“**建议**”安全级别。	您可以对受保护设备文件资源列表中选定的节点执行以下操作： • 选择不同的预定义安全级别 • 手动更改安全性设置
使用启发式分析	适用于“*关键区域扫描*”、“*在操作系统启动时扫描*”、“*按需扫描*”和“*全盘扫描*”任务的“**中度**”分析级别。	可以启用或禁用“启发式分析”并配置分析级别。
以特定权限启动任务的设置	在系统账户下启动任务。	您可以为所有系统和自定义按需扫描任务编辑以特定账户权限启动任务的设置，但“*应用程序完整性控制*”任务除外。
在后台模式下执行任务	未应用	您可以配置按需扫描任务的优先级。
将任务视为关键区域扫描	适用于“*按需扫描*”、“*在操作系统启动时扫描*”、“*关键区域扫描*”和“*全盘扫描*”任务。	您可以配置按需扫描任务的优先级。
不同时运行多个扫描任务	未应用	您可以配置按需扫描任务的优先级。
任务启动计划	应用于本地系统任务： • *在操作系统启动时扫描* – **在应用程序启动后**。 • *关键区域扫描*、*应用程序完整性控制* 和 *全盘扫描* – **每周**。	您可以配置计划任务启动的设置。

管理按需扫描任务

本节介绍界面导航以及在受保护设备上配置“按需扫描”任务。

导航

了解如何通过所选界面导航到所需任务设置。

打开按需扫描任务向导

要创建新的按需扫描任务：

转到新任务向导，在 Kaspersky Security Center 管理控制台中创建按需扫描任务

1. 若要创建本地任务：
   a. 展开 Kaspersky Security Center 管理控制台中的“**受管理设备**”节点。
   b. 选择受保护设备所属的管理组。
   c. 在结果窗格的“**设备**”选项卡上，打开受保护设备的上下文菜单。
   d. 选择“**属性**”菜单选项。
   e. 在打开的窗口中，单击“**任务**”部分中的“**添加**”按钮。

   将打开“**新建任务向导**”窗口。
2. 创建组任务：
   a. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
   b. 选择要为其创建任务的管理组。
   c. 选择“**任务**”选项卡。
   d. 单击“**新任务**”。

   将打开“**新建任务向导**”窗口。
3. 要为自定义的一组受保护设备创建任务：
   a. 在 Kaspersky Security Center 管理控制台树的“**设备选择**”节点中，单击“**运行选择**”按钮以执行设备选择。
   b. 选择“**选择结果'分类名称'**”选项卡。
   c. 从“**执行操作**”下拉列表中，选择“**新任务**”。

   将打开“**新建任务向导**”窗口。
4. 在 Kaspersky Industrial CyberSecurity for Nodes 的可用任务列表中选择“**按需扫描**”任务。
5. 点击“**下一步**”并根据需要配置任务。

要配置现有按需扫描任务，

双击 Kaspersky Security Center 任务列表中的任务名称。

将打开“**属性：按需扫描**”窗口。

转到新任务向导，在 Kaspersky Security Center Web Console 中创建按需扫描任务

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。
2. 单击受保护设备名称。
3. 在打开的“**<设备名称>**”窗口中，选择“**任务**”选项卡。
4. 单击“**添加**”按钮。
   将打开“**新建任务向导**”窗口。
5. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
6. 在“**任务类型**”下拉列表中，选择“**按需扫描**”任务。
7. 点击“**下一步**”。

   根据需要配置任务设置。

要开始创建新的组按需扫描任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击“**组**”选项卡以选择要为其创建任务的管理组。
3. 单击“**添加**”按钮。
   将打开“**新建任务向导**”窗口。
4. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
5. 在“**任务类型**”下拉列表中，选择“**按需扫描**”任务。
6. 点击“**下一步**”。

   根据需要配置任务设置。

要开始为自定义组创建新的按需扫描任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**设备选择**”。
2. 选择要为其创建任务的选择项。
3. 单击“**启动**”按钮。
4. 在“**选择结果**”窗口中，选择要为其创建任务的设备。
5. 单击“**新建任务**”按钮。

6. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
7. 在“**任务类型**”下拉列表中，选择“**按需扫描**”任务。
8. 点击“**下一步**”。

根据需要配置任务设置。

要配置现有按需扫描任务：

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**任务**”。
2. 单击 Kaspersky Security Center 任务列表中的任务名称。

将打开“**<任务名称>**”窗口。

打开按需扫描任务设置

要打开单台受保护设备的按需扫描任务的应用程序设置：

在 Kaspersky Security Center 管理控制台中打开按需扫描任务的常规设置

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择受保护设备所属的管理组。
3. 选择“**设备**”选项卡。
4. 双击要为其配置扫描范围的受保护设备的名称。
   将打开“**属性：<受保护设备名称>**”窗口。
5. 选择“**任务**”部分。
6. 在为设备创建的任务列表中，选择您创建的按需扫描任务。
7. 单击“**属性**”按钮。
   将打开“**属性：按需扫描**”窗口。

根据需要配置任务设置。

在 Kaspersky Security Center Web Console 中打开按需扫描任务的常规设置

1. 在 Web 控制台的主窗口中，选择“**设备**”→“**受管理设备**”。
2. 选择受保护设备所属的管理组。
3. 单击受保护设备名称。

4. 在打开的“**<设备名称>**”窗口中，选择“**任务**”选项卡。

5. 在为设备创建的任务列表中，选择您创建的按需扫描任务。

6. 打开“**应用程序设置**”选项卡。

在应用程序控制台中打开按需扫描任务的常规设置

1. 在应用程序控制台树中，展开“**按需扫描**”节点。

2. 选择与要配置的任务相应的子节点。

3. 在子节点结果窗格中，单击“**属性**”链接。
   将打开“**属性：<任务名称>**”窗口。

创建按需扫描任务

在 Kaspersky Security Center 管理控制台中创建按需扫描任务

1. 启动新任务向导。

2. 在“**选择任务类型**”窗口，选择“**按需扫描**”并点击“**下一步**”。

3. 在“**扫描范围**”窗口中创建扫描范围：

   默认情况下，扫描范围包括受保护设备的关键区域。扫描范围在表中用图标 ☑ 标记。排除的扫描范围在表中用图标 ☐ 标记。可以按如下方式更改扫描范围：添加特定的预设扫描范围、磁盘、文件夹、网络对象和文件，然后为添加的每个范围分配特定的安全性设置。

   - 要从扫描中排除某些范围，请选择相应的列表项并单击“**删除**”。
   - 要在扫描范围中包括预定义的扫描范围、磁盘、文件夹、网络对象或文件：
     a. 单击“**添加**”。
     b. 在“**选择扫描范围**”窗口中，从列表中选择预定义的扫描范围，然后单击“**确定**”。
   - 要从扫描范围中排除子文件夹或文件：
     a. 在“**扫描范围**”窗户中选择添加的文件夹（或磁盘）。
     b. 单击“**编辑**”。
     c. 禁用“**包括子文件夹**”复选框

- 要更改扫描范围安全性设置：

  a. 选择要编辑设置的扫描范围，然后单击“**配置**”。

  b. 这将打开一个窗口；在该窗口中，选择预定义的安全级别之一，或单击“**设置**”按钮手动配置安全设置。

  安全性设置的配置方式与实时文件保护任务的配置方式相同。

4. 配置启发式分析以及与其他组件的集成：

   - 配置启发式分析的使用。
   - 如果你想分配一个*低*任务运行的工作进程的优先级，选择“**在后台模式下执行任务**”复选框。

     默认情况下，执行 Kaspersky Industrial CyberSecurity for Nodes 任务的工作进程的优先级为“*中*”（正常）。

   - 如果要将该任务用作“*关键区域扫描*”任务，请选中“**将任务视为关键区域扫描**”复选框。
   - 选择“**不同时运行多个扫描任务**”复选框来优化计算机的负载。

5. 在“**选择要对其分配任务的设备**”窗口中，指定设备列表并单击“**下一步**”。
6. 在“**选择账户以运行任务**”窗口中，指定一个账户并点击“**下一步**”。
7. 在“**配置任务计划**”窗口中，配置任务计划并点击“**下一步**”。
8. 输入任务名称。

   任务名称不应超过 100 个字符，并且不能包含以下符号：" * < > & \ : |

9. “**完成任务创建**”窗口将打开。单击“**完成**”按钮完成创建任务。

将为所选受保护设备或受保护设备组创建新的按需扫描任务。

在 Kaspersky Security Center Web Console 中创建按需扫描任务

1. 启动新任务向导。
2. 在“**新任务**”窗口中，在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
3. 在**任务类型**下拉列表中，选择**按需扫描**并单击**下一步**。
4. 选择任务范围并单击“**下一步**”。
5. 在“**选择账户以运行任务**”窗口中，指定一个账户并点击“**下一步**”。

6. 输入任务名称。

   任务名称不应超过 100 个字符，并且不能包含以下符号：" * < > & \ : |

7. “**完成任务创建**”窗口将打开。单击“**完成**”按钮完成创建任务。

将为所选受保护设备或受保护设备组创建新的按需扫描任务。

在应用程序控制台中创建按需扫描任务

单台受保护设备的自定义任务可以在“**按需扫描**”节点中创建。

要创建和配置新的按需扫描任务：

1. 在应用程序控制台树中，打开“**按需扫描**”节点的上下文菜单。
2. 请选择**创建任务**选项。
   “**创建任务**”窗口将打开。
3. 输入任务的名称并单击“**确定**”。

已创建针对单个受保护设备的按需扫描任务。

在后台运行按需扫描任务

默认情况下，将为执行 Kaspersky Industrial CyberSecurity for Nodes 任务的进程分配“*中度（正常）*”优先级。

可以为将运行按需扫描任务的进程分配“*低*”优先级。将进程的优先级降级会增加执行任务所需的时间，但可能对其他正在运行的程序的进程性能产生有利影响。

多个后台任务可以在单个具有低优先级的工作进程中运行。

要更改现有按需扫描任务的优先级，请选择或清除任务设置中的“**在后台模式下执行任务**”复选框。

将保存已配置的任务设置，这些设置会立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

记录关键区域扫描执行

默认情况下，设备保护状态显示在 **Kaspersky Industrial CyberSecurity for Nodes** 节点的结果窗格中，并在执行*关键区域扫描*任务后每周更新一次。

设备保护状态的更新时间与设置中已选中“**将任务视为关键区域扫描**”复选框的按需扫描任务的计划相关联。

在按需扫描任务中配置扫描范围

如果在“*在操作系统启动时扫描*”和“*关键区域扫描*”任务中修改扫描范围，可以通过使用安装向导修复 Kaspersky Industrial CyberSecurity for Nodes 来恢复这些任务的默认扫描范围。

在 Kaspersky Security Center 管理控制台中配置按需扫描任务的扫描范围

1. 打开“**属性: 按需扫描**”窗口。
2. 选择“**扫描范围**”部分。
3. 要将范围添加到扫描范围，请选中其旁边的复选框。
4. 如果要添加不在列表中的扫描范围：
   a. 单击“**添加**”。
   b. 在显示的窗口中，选择范围、单个磁盘、文件夹或网络位置。
   c. 如果要在扫描范围内包含子文件夹，请选择“**包括子文件夹**”复选框。
5. 要从扫描范围中排除单个节点，请清除这些节点名称旁边的复选框。
6. 要编辑扫描范围，请在列表中选择扫描范围，然后单击“**编辑**”。
7. 要从网络文件资源列表中隐藏先前添加的扫描范围，请选择扫描范围并单击“**Delete**”。

   将扫描范围从网络文件资源列表中删除时，该扫描范围也从“按需扫描”任务范围中排除。

8. 单击“**确定**”。

扫描范围设置窗口关闭。将保存新配置的设置。

在 Kaspersky Security Center Web Console 中配置按需扫描任务的扫描范围

1. 打开“**按需扫描**”窗口。
2. 选择**应用程序设置**选项卡。
3. 要将范围添加到扫描范围，请选中旁边的复选框并将切换开关设置为开。

4. 如果要添加不在列表中的扫描范围：

   a. 单击“**添加**”。

   b. 在显示的窗口中，选择范围、单个磁盘、文件夹或网络位置。

   c. 如果要在扫描范围内包含子文件夹，请选择“**子文件夹**”复选框。

5. 要从扫描范围中排除单个节点，请清除这些节点名称旁边的复选框。

6. 要编辑扫描范围，请在列表中选择扫描范围，然后单击“**编辑范围**”。

7. 要从网络文件资源列表中隐藏先前添加的扫描范围，请选择扫描范围并单击“Delete”。

   将扫描范围从网络文件资源列表中删除时，该扫描范围也从“按需扫描”任务范围中排除。

8. 单击“**保存**”。

扫描范围设置窗口关闭。将保存新配置的设置。

在应用程序控制台中配置按需扫描任务的扫描范围

1. 在应用程序控制台树中，展开“**按需扫描**”节点。

2. 选择与要配置的按需扫描任务相应的子节点。

3. 在选定节点的结果窗格中，单击“**配置保护范围**”链接。

4. 在显示的窗口中，要将范围添加到扫描范围，请选中其旁边的复选框。

5. 如果要添加不在列表中的扫描范围：

   a. 单击“**添加**”。

   b. 在显示的窗口中，选择范围、单个磁盘、文件夹或网络位置。

   c. 如果要在扫描范围内包含子文件夹，请选择“**包括子文件夹**”复选框。

6. 要从扫描范围中排除单个节点，请清除这些节点名称旁边的复选框。

7. 要编辑扫描范围，请在列表中选择扫描范围，然后单击“**编辑范围**”。

8. 要从网络文件资源列表中隐藏先前添加的扫描范围，请选择扫描范围并单击“Delete”。

   将扫描范围从网络文件资源列表中删除时，该扫描范围也从“按需扫描”任务范围中排除。

9. 单击“**确定**”。

扫描范围设置窗口关闭。将保存新配置的设置。

配置按需扫描任务设置

如何在 Kaspersky Security Center 管理控制台中配置“按需扫描”任务

1. 打开按需扫描任务属性。
2. 选择“**选项**”部分。
3. 清除或选中“**使用启发式分析**”复选框。
4. 如果有必要，更改分析级别。
5. 如果你想分配一个*低*任务运行的工作进程的优先级，选择“**在后台模式下执行任务**”复选框。

   默认情况下，执行 Kaspersky Industrial CyberSecurity for Nodes 任务的工作进程的优先级为“*中*”（正常）。
6. 如果要将该任务用作“*关键区域扫描*”任务，请选中“**将任务视为关键区域扫描**”复选框。
7. 选择“**不同时运行多个扫描任务**”复选框来优化计算机的负载。
8. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置“按需扫描”任务

1. 打开按需扫描任务属性。
2. 选择“**应用程序设置**”部分。
3. 转到**设置**区域。
4. 清除或选中“**使用启发式分析**”复选框。
5. 如有必要，使用“**启发式分析级别**”下拉列表中选择分析级别。
6. 如果你想分配一个*低*任务运行的工作进程的优先级，选择“**在后台模式下执行任务**”复选框。

   默认情况下，执行 Kaspersky Industrial CyberSecurity for Nodes 任务的工作进程的优先级为“*中*”（正常）。
7. 如果要将该任务用作“*关键区域扫描*”任务，请选中“**将任务视为关键区域扫描**”复选框。

8. 选择“**不同时运行多个扫描任务**”复选框来优化计算机的负载。
9. 保存更改。

如何在应用程序控制台中配置按需扫描任务

1. 在应用程序控制台树中，展开“**按需扫描**”节点。
2. 选择与要配置的按需扫描任务相应的子节点。
3. 在选定节点的结果窗格中，单击“**属性**”。
4. 选择**任务设置**选项卡。
5. 清除或选中“**使用启发式分析**”复选框。
6. 如果有必要，更改分析级别。
7. 如果你想分配一个*低*任务运行的工作进程的优先级，选择“**在后台模式下执行任务**”复选框。

   默认情况下，执行 Kaspersky Industrial CyberSecurity for Nodes 任务的工作进程的优先级为“*中*”（正常）。
8. 如果要将该任务用作“*关键区域扫描*”任务，请选中“**将任务视为关键区域扫描**”复选框。
9. 选择“**不同时运行多个扫描任务**”复选框来优化计算机的负载。
10. 保存更改。

配置可移动驱动器扫描

在 Kaspersky Security Center 管理控制台中配置可移动驱动器扫描

1. 展开 Kaspersky Security Center 管理控制台树中的“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
   在策略属性窗口中，转到“**补充**”区域。
5. 在“**可移动驱动器扫描**”字部分中单击“**设置**”。
   “**可移动驱动器扫描**”窗口将打开。

6. 执行以下操作：

   - 如果想让 Kaspersky Industrial CyberSecurity for Nodes 在可移动驱动器连接时自动扫描，请选择“**扫描通过 USB 连接的可移动驱动器**”复选框。
   - 如果需要，选中“**扫描大小未超过此值的可移动驱动器(MB)**”，然后在右侧的字段中指定最大值。
   - 在“**使用此安全级别扫描**”下拉列表中，指定“可移动驱动器扫描”任务所需设置的安全级别。

7. 单击“**确定**”。

即会保存并应用指定设置。

在 Kaspersky Security Center Web Console 中配置可移动驱动器扫描

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**补充**区域。
5. 在“**可移动驱动器扫描**”下点击“**配置**”。
   “**可移动驱动器扫描**”窗口将打开。
6. 执行以下操作：

   - 如果想让 Kaspersky Industrial CyberSecurity for Nodes 在可移动驱动器连接时自动扫描，请选择“**扫描通过 USB 连接的可移动驱动器**”复选框。
   - 如果需要，选中“**扫描大小未超过此值的可移动驱动器(MB)**”，然后在右侧的字段中指定最大值。
   - 在“**使用此安全级别扫描**”下拉列表中，指定“可移动驱动器扫描”任务所需设置的安全级别。

7. 单击“**确定**”。

即会保存并应用指定设置。

在应用程序控制台中配置可移动驱动器扫描

1. 在应用程序控制台树中，打开“**Kaspersky Industrial CyberSecurity for Nodes**”节点的上下文菜单，并选择“**可移动驱动器扫描**”。
   “**可移动驱动器扫描**”窗口将打开。

2. 执行以下操作：

   - 如果想让 Kaspersky Industrial CyberSecurity for Nodes 在可移动驱动器连接时自动扫描，请选择“**扫描通过 USB 连接的可移动驱动器**”复选框。
   - 如果需要，选中“**扫描大小未超过此值的可移动驱动器(MB)**”，然后在右侧的字段中指定最大值。
   - 在“**使用此安全级别扫描**”下拉列表中，指定“可移动驱动器扫描”任务所需设置的安全级别。

3. 单击“**确定**”。

为按需扫描任务选择预定义的安全级别

可以为受保护设备文件资源列表中的选定节点应用以下三个预定义安全级别之一：**最高性能**、**建议**和**最大保护**。

在 Kaspersky Security Center 管理控制台中选择一个预定义的安全级别

1. 打开按需扫描任务属性。
2. 选择“**扫描范围**”部分。
3. 在受保护设备列表中，选择一个包含在扫描范围中的项目以设置预定义安全级别。
4. 单击“**配置**”。
5. 这将打开一个窗口；在该窗口中，在“**安全级别**”选项卡上，选择要应用的安全级别。
6. 单击“**确定**”。
7. 在“**属性：按需扫描**”窗口中，单击“**确定**”按钮。

将保存已配置的任务设置，这些设置会立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

在应用程序控制台中选择一个预定义的安全级别

1. 在应用程序控制台树中，展开“**按需扫描**”节点。
2. 选择与要配置的按需扫描任务相应的子节点。
3. 在选定节点的结果窗格中，单击“**配置保护范围**”。
4. 在受保护设备的网络文件资源列表中，选择需要设置预定义安全级别的节点或项目。
5. 确保选定的节点或项包含在扫描范围中。
6. 单击“**配置**”。

7. 这将打开一个窗口；在该窗口中，选择您想要的安全级别。
   该窗口将显示与选定安全级别相对应的安全性设置列表。
8. 单击“**正常**”。

将保存任务设置，并将这些设置立即应用到正在运行的任务。如果任务未运行，则将在下次启动时应用修改后的设置。

手动配置安全性设置

默认情况下，按需扫描任务对整个扫描范围使用通用安全性设置。

这些设置对应于“**建议**”预定义安全级别。

可以通过将安全性设置配置为用于整个扫描范围的常规设置，或配置为受保护设备文件资源列表或树中节点的不同项目的不同设置，来修改安全性设置的默认值。

在 Kaspersky Security Center 管理控制台中手动管理安全设置

1. 打开按需扫描任务属性。
2. 选择“**扫描范围**”部分。
3. 在受保护设备列表中，选择一个包含在扫描范围中的项目以管理安全设置。
4. 单击“**配置**”。
5. 这将打开一个窗口；在该窗口中，在“**安全级别**”选项卡上，选择要应用的安全级别。
6. 选择要配置其安全设置的资源。
7. 单击“**配置**”。
8. 在打开的窗口中，选择所需安全级别并单击“**设置**”。
9. 在“**常规**”选项卡上，指定以下设置：
   - 应纳入保护范围的对象：
     - **所有对象**
     - **按格式扫描对象**
     - **按反病毒数据库中指定的扩展名列表扫描的对象**
   - 在“**优化**”块中，选中或清除“**仅保护新建和已修改的文件**”复选框。
   - 在“**扫描复合文件**”部分中，指定要包含在扫描范围内的复合对象：
     - **扫描压缩包**

- **扫描分发包**
- **扫描 Microsoft Office 格式文件**
- **扫描电子邮件格式文件**

10. 在“**操作**”选项卡上，指定以下设置：

- 选择要对受感染的对象和其他检测到的对象执行的操作：
  - **清除**
  - **清除。清除失败则删除**
  - **删除**
  - **建议**
  - **通知**
- 根据检测的对象类型配置要对对象执行的操作：
  a. 清除或选中“**将操作应用于选定的对象类型**”复选框。
  b. 点击“**设置**”并选择要检测的对象类型。
- 配置对不可修改的复合文件的操作：清除或选择“**在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件**”复选框。

11. 在“**性能**”选项卡上，指定以下设置：

- 在“**排除项**”块中：
  - 清除或选中“**排除文件**”复选框。
  - 清除或选中“**不按类型检测对象**”复选框。
    针对每个设置单击“**编辑**”按钮以添加排除项。
- 在“**高级设置**”块中：
  - **如果扫描时间超过此值则停止(秒)**
  - **不扫描大于此值的复合对象(MB)**
  - **使用 iSwift 技术**
  - **使用 iChecker 技术**

12. 保存新的安全设置。

在 Kaspersky Security Center Web Console 中手动管理安全设置

1. 打开按需扫描任务属性。
2. 选择“**应用程序设置**”部分。
3. 转到**扫描范围**区域。
4. 在受保护设备的网络文件资源列表中，选择需要管理安全设置的项目。确保选定的项包含在扫描范围中。
5. 单击“**编辑**”。
6. 在下拉列表中选择对象保护模式：
   - **所有对象**
   - **按格式扫描对象**
   - **按反病毒数据库中指定的扩展名列表扫描的对象**
7. 选择或清除“**仅保护新建和已修改的文件**”复选框并指定是否要包含“子文件夹”在扫描中。
8. 管理复合对象保护设置：
   - **扫描压缩包**
   - **扫描分发包**
   - **扫描 Microsoft Office 格式文件**
   - **扫描电子邮件格式文件**
9. 选择要对受感染的对象和其他检测到的对象执行的操作：
   - **清除**
   - **清除。清除失败则删除**
   - **删除**
   - **建议**
   - **通知**
10. 根据检测的对象类型配置要对对象执行的操作：
    a. 清除或选中“**将操作应用于选定的对象类型**”复选框。
    b. 点击“**设置**”并选择要检测的对象类型。
11. 配置对不可修改的复合文件的操作：清除或选择“**在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件**”复选框。

12. 在“**排除项**”块中：

    - 清除或选中“**排除文件**”复选框。
    - 清除或选中“**不按类型检测对象**”复选框。

13. 在“**添加密钥**”块中：

    - **如果扫描时间超过此值则停止(秒)**
    - **不扫描大于此值的复合对象(MB)**
    - **使用 iSwift 技术**
    - **使用 iChecker 技术**

14. 保存新的安全设置。

在应用程序控制台中手动管理安全设置

1. 在应用程序控制台树中，展开“**按需扫描**”节点。
2. 选择与要配置的按需扫描任务相应的子节点。
3. 在选定节点的结果窗格中，单击“**配置保护范围**”。
4. 在受保护设备的网络文件资源列表中，选择需要管理安全设置的项目。
5. 确保选定的项包含在扫描范围中。
6. 单击“**配置**”。
7. 在打开的窗口中，选择所需安全级别并单击“**设置**”。
8. 在“**常规**”选项卡上，指定以下设置：
    - 应纳入保护范围的对象：
        - **所有对象**
        - **按格式扫描对象**
        - **按反病毒数据库中指定的扩展名列表扫描的对象**
    - 在“**优化**”块中，选中或清除“**仅保护新建和已修改的文件**”复选框。
    - 在“**扫描复合文件**”部分中，指定要包含在扫描范围内的复合对象：
        - **扫描压缩包**
        - **扫描分发包**

- **扫描 Microsoft Office 格式文件**
- **扫描电子邮件格式文件**

9. 在“**操作**”选项卡上，指定以下设置：

- 选择要对受感染的对象和其他检测到的对象执行的操作：
  - **清除**
  - **清除。清除失败则删除**
  - **删除**。
  - **建议**。
  - **通知**。
- 根据检测的对象类型配置要对对象执行的操作：
  a. 清除或选中“**将操作应用于选定的对象类型**”复选框。
  b. 点击“**设置**”并选择要检测的对象类型。
- 配置对不可修改的复合文件的操作：清除或选择“**在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件**”复选框。

10. 在“**性能**”选项卡上，指定以下设置：

- 在“**排除项**”块中：
  - 清除或选中“**排除文件**”复选框。
  - 清除或选中“**不按类型检测对象**”复选框。

  针对每个设置单击“**编辑**”按钮以添加排除项。
- 在“**高级设置**”块中：
  - **如果扫描时间超过此值则停止(秒)**。
  - **不扫描大于此值的复合对象(MB)**。
  - **使用 iSwift 技术**。
  - **使用 iChecker 技术**。

11. 保存新的安全设置。

按需扫描任务统计

执行按需扫描任务时，您可以查看有关 Kaspersky Industrial CyberSecurity for Nodes 自启动以来已处理的对象数量的信息。

即使任务暂停，也仍可查看该信息。您可以在任务日志中查看任务统计。

要查看按需扫描任务的统计：

1. 在应用程序控制台树中，展开“**按需扫描**”节点。
2. 选择您要查看其统计的按需扫描任务。

任务统计信息显示在选定节点的结果窗格的“**统计信息**”部分中。

下表给出了 Kaspersky Industrial CyberSecurity for Nodes 自启动以来已处理的对象的信息。

按需扫描任务统计

字段	描述
检测到	Kaspersky Industrial CyberSecurity for Nodes 检测到的对象数量。例如，如果 Kaspersky Industrial CyberSecurity for Nodes 在五个文件中检测到一个恶意对象，该字段中的值将增加 1。
受感染对象和其他对象	Kaspersky Industrial CyberSecurity for Nodes 发现并归类为“已感染”的对象数量，或者发现的未从扫描范围中排除且归类为可被入侵者用来破坏设备或个人数据的合法软件文件数量。
对象未清除	Kaspersky Industrial CyberSecurity for Nodes 因以下原因未清除的对象数： • 检测到的对象是无法清除的类型。 • 清除期间出现错误。
对象已清除	Kaspersky Industrial CyberSecurity for Nodes 已清除的对象的数量。
对象已删除	Kaspersky Industrial CyberSecurity for Nodes 成功删除的对象数量。
对象未扫描	Kaspersky Industrial CyberSecurity for Nodes 在保护范围中无法扫描（例如，其他应用程序阻止访问对象）的对象数。
存档	被 Kaspersky Industrial CyberSecurity for Nodes 扫描的存档数量。
打包对象	被 Kaspersky Industrial CyberSecurity for Nodes 扫描的打包对象数量。
密码保护对象	因受到密码保护而被 Kaspersky Industrial CyberSecurity for Nodes 跳过的对象（例如压缩文件）数量。
已损坏的对象	Kaspersky Industrial CyberSecurity for Nodes 由于对象格式损坏而跳过的对象数。
处理错误	对其处理产生错误的对象数。
对象未删除	Kaspersky Industrial CyberSecurity for Nodes 尝试删除但无法删除（例如，由于其他应用程序阻止访问对象）的对象数。
对象未处理	未被 Kaspersky Industrial CyberSecurity for Nodes 处理的对象的总数。

通过单击结果窗格中“**管理**”部分的“**打开任务日志**”链接，还可以在选定任务日志中查看按需扫描任务统计。

建议您在任务完成后手动处理任务日志中“**事件**”选项卡上记录的事件。

工业网络保护

本节介绍可编程逻辑控制器项目（也称为“PLC 项目”）调查和完整性检查任务，并提供有关如何配置它的说明。

关于PLC 项目完整性检查

此功能用于检查工业系统中使用的 PLC 项目的完整性。

PLC 项目是为 PLC 编写的微程序。PLC 项目存储在 PLC 的内存中，并作为使用 PLC 的生产过程的一部分运行。

PLC 项目完整性检查要求安装了 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备的网络能够访问 PLC。

在开始使用此功能之前，请执行以下操作：

1. 使用应用程序控制台“**PLC 项目调查**”本地任务获取有关 PLC 项目的信息 。
2. 在应用程序控制台“**PLC 项目完整性检查**”本地任务设置中，从上一步获取的项目列表中指明 PLC 参考项目。

要查看有关“PLC 项目完整性检查”任务中 PLC 项目的信息：

在策略属性中打开“**与管理服务器交互**”窗口，选择“**PLC 项目版本**”复选框来配置向管理服务器的数据传输。

在“*PLC 项目完整性检查*”本地任务启动后，如果 PLC 项目相对于 PLC 参考项目发生了更改，应用程序将发出警告。

PLC 项目完整性检查默认是禁用的。

报告

报告是 Kaspersky Security Center 管理服务器的基本功能之一。此功能只能通过 Kaspersky Security Center 的管理控制台使用。

PLC 项目完整性检查任务成功完成后，您可以生成并查看包含以下信息的报告：

- 完成“*PLC 项目完整性检查*”的计算机的名称。
- 正在监控其完整性的 PLC。
- 最后检查日期。
- 完整性检查的结果。

要在 Kaspersky Security Center 管理服务器中生成报告，

打开“**报告**”选项卡并选择“**可编程逻辑控制器(PLC)完整性检查报告**”。

有关生成报告的详细信息，请参见 *Kaspersky Security Center 帮助*。

配置 PLC 项目完整性检查任务

本节提供有关配置 PLC 项目控制任务的常规设置的说明。

配置 PLC 项目调查

在运行 PLC 项目完整性检查之前，您必须收到有关工业网络中当前使用的 PLC 项目的信息。关于 PLC 项目的信息可以使用“*PLC 项目调查*”本地任务获取。

在 Kaspersky Security Center 管理控制台中配置 PLC 项目调查

1. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
2. 在工作区中选择“**设备**”选项卡。
3. 双击以打开计算机属性窗口。
4. 转到**任务**区域。
5. 在打开的窗口中，选中“**PLC 项目调查**”任务并单击“**属性**”。
   “**属性: PLC 项目调查**”窗口将打开。
6. 转至“**设置**”部分，然后单击“**任务设置**”选项卡上的“**从 PLC 注册表中添加**”按钮。
   “**PLC 注册表管理 4.5.0**”窗口将打开。
7. 单击“**添加**”。
8. 在“**常规设置**”下，输入 PLC 配置的名称并 在“**PLC 类型**”下拉列表中，选择 PLC 类型。
   PLC 类型代表 PLC 制造商提供的型号和系列。
9. 在“**描述**”字段中，输入 PLC 描述。
   应用程序将指定的描述链接到运行“*PLC 项目调查*”任务时获得的 PLC 项目每个新版本。
10. 在“**等待连接**”字段指定等待时间值（以秒为单位）。
11. 在“**连接设置**”下，根据所选的 PLC 类型，填写以下字段：**IP 地址**、**端口**、**机架**、**Telnet 端口**、**控制器虚拟地址**和**插槽**。
12. 如果要保护与 PLC 的连接，则根据所选的 PLC 类型，选择身份验证方法：
    - “**密码**”。
      如果选中该复选框，应用程序将使用您在连接 PLC 时指定的密码进行查询。
      如果清除该复选框，应用程序将无需使用密码即可连接到 PLC。
      默认下，复选框被清除。

该复选框不会分配新密码来连接到 PLC。必须在 PLC 端设置密码。

- "**应用密码**"。

13. 选中或清除"**读取数据块**"复选框。

    如果选中该复选框，应用程序将在计算 PLC 项目校验和时考虑数据块。如果数据块仅包含统计值，推荐选中该复选框，以提高扫描的安全级别。

    如果清除该复选框，应用程序将不会考虑数据块。如果数据块包含动态值，推荐不要选中该复选框，以防止在将选定的 PLC 项目与参考项目进行比较时在"*PLC 项目完整性检查*"任务中出现误报。

    默认下，复选框被清除。

14. 单击"**确定**"。

    不支持冗余控制器。

    添加的 PLC 配置显示在"**任务设置**"选项卡。

15. 如果您想从任务列表中删除选定的 PLC 配置，点击"**删除**"。

    PLC 配置不会从 PLC 注册表中删除，并且可以随时再次添加。

16. 保存更改。

运行"*PLC 项目调查*"任务后获得的 PLC 项目信息用于选择 PLC 参考项目和配置"*PLC 项目完整性检查*"任务。

在 Kaspersky Security Center Web Console 中配置 PLC 项目调查

1. 在 Web Console 的主窗口中，选择"**资产(设备)**" → "**受管理设备**"。
2. 单击您要在其上配置"*PLC 项目调查*"任务的计算机的名称。
3. 选择**任务**选项卡。
4. 这将打开一个窗口；在该窗口中，双击打开"**PLC 项目调查**"任务的属性。
5. 选择"**应用程序设置**"选项卡并单击"**从 PLC 注册表中添加**"。

   "**PLC 配置**"窗口将打开。
6. 在"**PLC 设置**"部分，在"**PLC 类型**"下拉列表中，选择 PLC 类型。

   PLC 类型代表 PLC 制造商提供的型号和系列。
7. 在"**描述**"字段中，输入 PLC 描述。

   应用程序将指定的描述链接到运行"*PLC 项目调查*"任务时获得的 PLC 项目每个新版本。
8. 在"**连接超时，秒。**"字段指定等待时间值（以秒为单位）。

9. 在"**连接设置**"部分，根据所选的 PLC 类型，填写以下字段：**控制器地址**、**端口**、**机架**、**Telnet 端口**、**控制器虚拟地址**和**插槽**。

10. 如果要保护与 PLC 的连接，则根据所选的 PLC 类型，选择身份验证方法：

    - "**密码**"。

      如果选中该复选框，应用程序将使用您在连接 PLC 时指定的密码进行查询。

      如果清除该复选框，应用程序将无需使用密码即可连接到 PLC。

      默认下，复选框被清除。

      该复选框不会分配新密码来连接到 PLC。必须在 PLC 端设置密码。

    - "**应用密码**"。

11. 选中或清除"**读取数据块**"复选框。

    如果选中该复选框，应用程序将在计算 PLC 项目校验和时考虑数据块。如果数据块仅包含统计值，推荐选中该复选框，以提高扫描的安全级别。

    如果清除该复选框，应用程序将不会考虑数据块。如果数据块包含动态值，推荐不要选中该复选框，以防止在将选定的 PLC 项目与参考项目进行比较时在"*PLC 项目完整性检查*"任务中出现误报。

    默认下，复选框被清除。

12. 单击"**确定**"。

    > 不支持冗余控制器。

    添加的 PLC 配置显示在"**应用程序设置**"选项卡。

13. 如果您想从任务列表中删除选定的 PLC 配置，点击"**删除**"。

    > PLC 配置不会从 PLC 注册表中删除，并且可以随时再次添加。

14. 保存更改。

在应用控制台台中配置 PLC 项目调查

1. 在应用程序控制台树中，展开"**工业网络保护**"节点。
2. 选择"**PLC 项目调查**"子节点。
3. 在"**PLC 项目调查**"节点的详细信息窗格中，单击"**属性**"链接。

   "**属性: PLC 项目调查**"窗口将打开。
4. 在"**任务设置**"选项卡上单击"**添加**"按钮。

   "**PLC 配置**"窗口将打开。
5. 在"**常规设置** "下，在"**PLC 类型**"下拉列表中，选择 PLC 类型。

   PLC 类型代表 PLC 制造商提供的型号和系列。

6. 在“**描述**”字段中，输入 PLC 描述。

   应用程序将指定的描述链接到运行“*PLC 项目调查*”任务时获得的 PLC 项目每个新版本。

7. 在“**等待连接**”字段指定等待时间值（以秒为单位）。

8. 在“**连接设置**”下，根据所选的 PLC 类型，填写以下字段：**IP 地址**、**端口**、**机架**、**Telnet 端口**、**控制器虚拟地址**和**插槽**。

9. 如果要保护与 PLC 的连接，则根据所选的 PLC 类型，选择身份验证方法：

   - “**密码**”。

     如果选中该复选框，应用程序将使用您在连接 PLC 时指定的密码进行查询。

     如果清除该复选框，应用程序将无需使用密码即可连接到 PLC。

     默认下，复选框被清除。

     该复选框不会分配新密码来连接到 PLC。必须在 PLC 端设置密码。

   - “**应用密码**”。

10. 选中或清除“**读取数据块**”复选框。

    如果选中该复选框，应用程序将在计算 PLC 项目校验和时考虑数据块。如果数据块仅包含统计值，推荐选中该复选框，以提高扫描的安全级别。

    如果清除该复选框，应用程序将不会考虑数据块。如果数据块包含动态值，推荐不要选中该复选框，以防止在将选定的 PLC 项目与参考项目进行比较时在“*PLC 项目完整性检查*”任务中出现误报。

    默认下，复选框被清除。

11. 单击“**确定**”。

    > 不支持冗余控制器。

    添加的 PLC 配置显示在“**任务设置**”选项卡。

12. 如果您想从任务列表中删除选定的 PLC 配置，点击“**删除**”。

    > PLC 配置不会从 PLC 注册表中删除，并且可以随时再次添加。

13. 保存更改。

运行“*PLC 项目调查*”任务后获得的 PLC 项目信息用于选择 PLC 参考项目和配置“*PLC 项目完整性检查*”任务。

配置 PLC 项目完整性检查

在 Kaspersky Security Center 管理控制台中配置 PLC 项目完整性检查

1. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
2. 在工作区中选择“**设备**”选项卡。
3. 双击以打开计算机属性窗口。
4. 转到**任务**区域。
5. 在打开的窗口中，选中“**PLC 项目完整性检查**”任务并单击“**属性**”。
   “**属性: PLC 项目完整性检查**”窗口将打开。
6. 转到**设置**区域。
7. 在打开的窗口中，点击“**添加**”按钮将运行“*PLC Project Integrity Check*”任务的配置添加到列表中。
   “**PLC 项目完整性检查数据**”窗口将打开。
   此窗口中的所有信息均通过运行 Kaspersky Security Center 的“*PLC 项目调查*”任务获取。
8. 在“**PLC 类型**”下拉列表中，选择要检查其项目完整性的 PLC 类型。

   可用 PLC 类型的下拉列表，可接收与项目相关的数据。PLC 类型代表 PLC 制造商提供的型号和系列。
9. 从列表中，为所选 PLC 类型选择配置，并为 PLC 项目指定参考版本。根据与 PLC 参考项目设置的比较结果，应用程序对 PLC 项目的完整性做出结论。
10. 在“**PLC 项目完整性检查数据**”窗口中，单击“**确定**”保存更改。PLC 项目信息已添加到任务中。
11. 在“**属性: PLC 项目完整性检查**”窗口的列表中选择添加的 PLC 配置。
    - “**PLC 配置**”选项卡显示有关 PLC 项目的哈希值及其接收日期的信息。
    - “**PLC 项目完整性检查设置**”选项卡包含有关 PLC 配置的详细信息。
12. 保存更改。

在 Kaspersky Security Center Web Console 中配置 PLC 项目完整性检查

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 单击要配置“*PLC 项目完整性检查*”任务的计算机的名称。
3. 选择“**任务**”部分。
4. 这将打开一个窗口；在该窗口中，双击打开“**PLC 项目完整性检查**”任务的属性。
5. 选择“**应用程序设置**”选项卡并单击“**添加**”。

"**PLC 项目完整性检查数据**"窗口将打开。

此窗口中的所有信息均通过运行 Kaspersky Security Center 的"*PLC 项目调查*"任务获取。

6. 点击"**选择控制器**"选择 PLC 配置。
7. 选择应用程序在请求有关 PLC 项目的信息时必须遵守的时间间隔。
8. 点击"**选择校验和**"并指定 PLC 项目的参考版本。根据与 PLC 参考项目设置的比较结果，应用程序对 PLC 项目的完整性做出结论。
9. 点击"**确定**"保存更改。
10. 在列表中选择添加的 PLC 配置。
11. 保存更改。

在应用控制台台中配置 PLC 项目完整性检查

1. 在应用程序控制台树中，展开"**工业网络保护**"节点。
2. 选择"**PLC 项目完整性检查**"子节点。
3. 在"**PLC 项目完整性检查**"节点的详细信息窗格中，单击"**属性**"链接。

   "**计划和运行模式**"窗口将打开。
4. 在打开的窗口中，配置以下设置：
   - 管理任务计划设置。
   - 在"**用户**"部分，选择"**任务运行身份**"并指定要使用的用户账户的用户名和密码。
5. 在"**PLC 项目完整性检查**"节点的结果窗格中，单击"**配置保护范围**"链接。
6. 在打开的窗口中，点击"**添加**"按钮将运行"*PLC 项目完整性检查*"任务的配置添加到列表中。

   "**PLC 项目完整性检查数据**"窗口将打开。此窗口中的所有信息均通过运行 Kaspersky Security Center 的"*PLC 项目调查*"任务获取。
7. 在"**PLC 类型**"下拉列表中，选择要检查其项目完整性的 PLC 类型。

   可用 PLC 类型的下拉列表，可接收与项目相关的数据。PLC 类型代表 PLC 制造商提供的型号和系列。
8. 从列表中，为所选 PLC 类型选择配置，并为 PLC 项目指定参考版本。根据与 PLC 参考项目设置的比较结果，应用程序对 PLC 项目的完整性做出结论。
9. 在"**PLC 项目完整性检查数据**"窗口中，单击"**确定**"保存更改。PLC 项目信息已添加到任务中。

10. 在“**属性: PLC 项目完整性检查**”窗口的列表中选择添加的 PLC 配置。
    - “**PLC 配置**”选项卡显示有关 PLC 项目的哈希值及其接收日期的信息。
    - “**PLC 项目完整性检查设置**”选项卡包含有关 PLC 配置的详细信息。
11. 保存更改。

启用和禁用 PLC 项目完整性检查

“*PLC 项目完整性检查*”任务仅在 Kaspersky Industrial CyberSecurity for Nodes 使用“*PLC 项目调查*”任务接收固件信息后才会运行。

在 Kaspersky Security Center 管理控制台中启用或禁用 PLC 项目完整性检查

1. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
2. 在工作区中选择“**设备**”选项卡。
3. 双击以打开计算机属性窗口。
4. 转到**任务**区域。
5. 在打开的窗口中，选择“**PLC 项目调查**”任务，并执行以下操作之一：
    - 要启用 PLC 项目完整性检查，请在任务的上下文菜单中选择“**启动**”。
      “*PLC 项目完整性检查*”任务已启动。
    - 要禁用“*PLC 项目完整性检查*”，在任务的上下文菜单中，选择“**停止**”。
      PLC 项目完整性检查任务被停止。

在 Kaspersky Security Center Web Console 中启用或禁用 PLC 项目完整性检查

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 单击您要在其上配置“*PLC 项目调查*”任务的计算机的名称。
3. 选择**任务**选项卡。
4. 选中“**PLC 项目调查**”任务旁边的复选框并执行以下操作之一：
    - 要启用 PLC 项目完整性检查，请单击“**启动**”按钮。
      “*PLC 项目完整性检查*”任务已启动。

- 要禁用 PLC 项目完整性检查，请单击“**停止**”按钮。
  “*PLC 项目完整性检查*”任务被停止。

在应用控制台台中启用或禁用 PLC 项目完整性检查

1. 在应用程序控制台树中，展开“**工业网络保护**”节点。
2. 选择“**PLC 项目调查**”子节点。
3. 在“**PLC 项目调查**”节点的详细信息窗格的“**管理**”部分中，单击“**启动**”链接。
4. 选择“**PLC 项目完整性检查**”子节点。
5. 在“**PLC 项目完整性检查**”节点的详细信息窗格的“**管理**”部分中，执行以下步骤之一：
   - 要启用 PLC 项目完整性检查，单击“**启动**”链接。
     “*PLC 项目完整性检查*”任务已启动。
   - 要禁用 PLC 项目完整性检查，单击“**停止**”链接。
     “*PLC 项目完整性检查*”任务被停止。

关于 PLC 配置注册表

PLC 配置注册表（也称为“注册表”）是所有 PLC 配置的共享列表，由 Kaspersky Industrial CyberSecurity for Nodes 使用。*PLC 配置*是 PLC 的单独属性的集合，可以在设置中指定（IP 地址、机架号、型号等）。您可以在使用注册表时添加、修改和删除 PLC 配置。

在 Kaspersky Industrial CyberSecurity for Nodes 4.5 中，计算 Siemens SIMATIC S7-300 / 400 / 400H 型 PLC 配置哈希值的程序已经改变。因此，升级应用程序后，您必须重新启动“*PLC 项目调查*”任务，为这些 PLC 项目创建新基线。

PLC 配置注册表可以手动填充，也可以通过导入包含 PLC 配置数据的配置文件来填充。

注册表中的 PLC 配置列表用于创建“*PLC 项目完整性检查*”任务的保护范围，通过 Kaspersky Security Center 管理控制台进行配置。创建“*PLC 项目调查*”任务列表时，您可以添加和删除已添加到注册表的 PLC 配置。如果从任务列表中删除 PLC 配置，则该配置不会从注册表中删除。

添加到注册表的每个 PLC 配置都会获得一个唯一的识别号。如果 PLC 配置发生改变，识别号也会改变。Kaspersky Industrial CyberSecurity for Nodes 控制台中的“*PLC 项目调查*”任务列表中添加的 PLC 配置没有任何识别号。在 Kaspersky Security Center 中创建“*PLC 项目调查*”任务保护范围时，可以手动将此类 PLC 配置添加到注册表中。

Kaspersky Security Center 中的“*PLC 项目调查*”任务的 PLC 配置列表来自两个来源：

- 没有 ID 的 PLC 配置，通过应用程序控制台添加到本地任务列表中（列表自动同步）；
- 带有 ID 的 PLC 配置，由管理员从注册表中添加。

如果从注册表中删除添加到“*PLC 项目调查*”任务列表中的 PLC 配置，Kaspersky Industrial CyberSecurity for Nodes 会通知您完整性检查结果可能会失真。确保“*PLC 项目调查*”任务列表中的所有 PLC 配置都存在于注册表中，然后重新启动 PLC 项目调查任务。

配置 PLC 注册表

要配置 PLC 注册表：

1. 采用以下方法之一打开“**PLC 注册表管理**”窗口：

   - **从本地“PLC 项目调查”任务的设置**

     1. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
     2. 在工作区中选择“**设备**”选项卡。
     3. 双击以打开计算机属性窗口。
     4. 转到**任务**区域。
     5. 在打开的窗口中，选中“**PLC 项目调查**”任务并单击“**属性**”。
        “**属性: PLC 项目调查**”窗口将打开。
     6. 转至“**设置**”部分，然后单击“**任务设置**”选项卡上的“**从 PLC 注册表中添加**”按钮。
        “**PLC 注册表管理 4.5.0**”窗口将打开。

   - **从 Kaspersky Security Center 管理控制台硬件文件夹**

     a. 在 Kaspersky Security Center 管理控制台树中，展开“**管理服务器<服务器名称>**”节点。

     b. 展开“**高级**”节点。

     c. 在“**存储库**”文件夹中，选择“**硬件**”嵌套文件夹。

     > 如果你看不到“**硬件**”文件夹，在管理服务器界面设置中选择“**显示漏洞和补丁管理**”复选框。

     d. 在“**硬件**”文件夹的工作区中，在“**附加操作**”按钮的上下文菜单中，选择“**PLC 注册表管理 4.5.0**”。
        “**PLC 注册表管理 4.5.0**”窗口将打开。

2. 手动添加所需的 PLC 配置。

3. 如果需要，**从 XML 文件导入 PLC 项目配置数据**。

   a. 单击“**导入**”。
      将打开标准 Microsoft Windows“**打开文件** ”窗口。

b. 指定 PLC 设置 XML 文件的路径。

c. 点击“**打开**”。
新的 PLC 配置数据条目出现在“**PLC 注册表管理**”窗户中的列表中。

4. 如果需要，**将 PLC 项目配置数据导出到 XML 文件**。

a. 单击“**导出**”。

b. 在弹出窗口中，提供您希望保存 PLC 项目配置数据的 XML 文件的位置和文件名。

c. 单击“**保存**”按钮。

5. 要更改 PLC 配置设置，请单击“**编辑**”。

在 PLC 注册表中修改 PLC 配置时，“*PLC 项目完整性检查*”任务结果受到影响。您需要运行“*PLC 项目调查*”任务获取更新的数据，然后再次运行“*PLC 项目完整性检查*”获得实际结果。

1. 点击“**删除**”按钮，如果您不再使用 PLC 项目配置。

当 PLC 项目从 PLC 注册表中删除时，它将无法进行进一步调查和完整性检查。

2. 使用“**过滤器**”字段来检查 PLC 配置是否具有所需的值。

3. 如有需要，选中“**仅显示可以被 Kaspersky Industrial CyberSecurity for Nodes 保护的 PLC 配置**”复选框。

4. 单击“**关闭**”。

将保存 PLC 注册表。

便携式扫描程序

便携式扫描程序可以扫描隔离设备中的病毒和其他恶意软件，记录被扫描设备在指定时间内的入站和出站流量，并对设备运行安全审核。

使用便携式扫描程序，您可以连续扫描多个设备，并为每个要扫描的设备生成单独的报告。

便携式扫描程序可以在以下操作系统的设备上运行：软件和硬件要求。

创建便携式扫描程序的要求

创建便携式扫描程序的先决条件如下。

- 可移动 USB 驱动器，具有 2 GB 的可用空间。
- 已安装带有便携式扫描程序组件的 Kaspersky Industrial CyberSecurity for Nodes 的安装实例。
- 当前的 Kaspersky Industrial CyberSecurity for Nodes 授权许可。
- Kaspersky Industrial CyberSecurity for Nodes 便携式扫描程序的当前授权许可。

创建便携式扫描程序

在创建便携式扫描程序之前，请确保没有正在运行的便携式扫描程序数据库更新进程。

如何使用便携式扫描程序安装向导创建便携式扫描程序

1. 在通知区域中，在应用程序图标的上下文菜单中，选择“**小型诊断窗口**”。
2. 在打开的小型诊断窗口中，单击“**创建便携式扫描程序**”链接。
   在欢迎步骤中将打开一个新的便携式扫描程序向导窗口。

   要继续向导的下一步，请单击“**下一步**”。

3. 如果必要，从先前创建的 XML 文件导入便携式扫描程序设置。

   a. 单击“**导入**”。

   b. 在打开的窗口中，选择包含便携式扫描程序设置的 XML 文件。

c. 点击“**打开**”。

d. XML 文件中的设置将显示在后续的向导步骤中。

4. 添加创建便携式扫描程序所需的密钥文件。

a. 单击“**选择授权许可文件**”。

b. 在打开的窗口中，选择便携式扫描程序的密钥文件。

c. 点击“**打开**”。

d. 授权许可信息将显示在向导窗口中。

5. 启用便携式扫描程序在设备上启动时执行的操作：

- “**使用反病毒数据库扫描所选区域**”。便携式扫描程序可扫描选定区域以查找病毒和其他威胁。便携式扫描程序采用默认安全级别：消毒。清除失败则删除。
- “**记录来自所有网络接口的流量**”。便携式扫描程序会在指定的时间内记录被扫描设备的入站和出站流量。
- “**使用 OVAL 规则扫描系统**”。根据设置，便携式扫描程序可以扫描设备中的漏洞、评估设备安全性和操作系统合规性，或使用 OVAL 和 XCCDF 编写的规则收集设备配置数据。

6. **设置扫描范围**。

a. 单击“**添加**”。

b. 在打开的“**扫描范围**”窗口中，选择要添加的对象类型：

- **预定义范围**，如果您希望扫描范围包括受保护设备上的预定义范围之一。然后在下拉列表中，选择所需扫描范围。
- **磁盘、文件夹或网络位置**，将单个驱动器或文件夹纳入扫描范围。然后在通过“**浏览**”按钮打开的窗口中选择所需的范围。
- **文件**，将单个文件纳入扫描范围。然后，在打开的“**浏览**”窗口中，选择文件。

c. 在“**扫描范围**”窗口中单击“**确定**”按钮。

d. 通过选中或清除扫描范围名称左侧的复选框来启用或禁用扫描范围项。

7. **配置扫描**。

a. 单击“**扫描设置**”。
“**扫描设置**”窗口将打开。

b. 在“**常规**”选项卡上，选择适当的选项：

- **扫描对象.**

  下列选项可用：

  - 所有对象
  - 按格式扫描对象
  - 按反病毒数据库中指定的扩展名列表扫描的对象
  - 按指定的扩展名列表扫描的对象
  - 扫描磁盘引导扇区
  - 扫描 NTFS 交换数据流。

- **扫描复合文件.**

  下列选项可用：

  - 存档
  - SFX 压缩包
  - 电子邮件数据库
  - 打包对象
  - 纯文本电子邮件
  - 嵌入的 OLE 对象。

c. 在“**附加**”选项卡上，选择适当的选项：

- **常规设置.**

  - **扫描后恢复文件属性**
    如果在扫描期间打开了文件，则会更新该文件的最后访问时间。因此，存档程序和云存储会重新计算文件数据以将其传输到云端或备份。为了避免重新计算过程，您可以在扫描完成后恢复上次访问的时间。默认情况下，禁用此选项。
  - **限制扫描任务的 CPU 使用率**
    此设置用于避免计算机在扫描过程中挂起。对于工业系统来说，这个选项可能至关重要，因为工业系统的主要软件不应该冻结。默认情况下，禁用此选项。

- **扫描期间创建的临时文件文件夹.**

  点击“**浏览**”按钮来指定将在扫描过程中创建的**临时文件的文件夹**。默认情况下，临时文件会在 USB 驱动器上创建。

- **要对检测到的对象执行的操作**.

  - **清除；如果清除失败则删除**
    隔离区不适用于**便携式扫描程序**，因此留下疑似感染对象可能是不安全的。如果清除失败，请使用此选项删除检测到的文件。默认情况下，启用此选项。

  - **通知**
    使用此选项进行快速扫描。安全人员在收到有关检测到对象的通知时采取安全措施。对于工作流程不应该因删除工业软件模块而中断的系统，请使用此选项。默认情况下，禁用此选项。

- **对不可修改的复合文件的操作**.

  如果适用，请选择以下选项。

  "**在检测嵌入对象的情况下，完全删除应用程序无法修改的复合文件**"。

d. 在"**性能**"选项卡上，选择适当的选项：

- **排除项**.

  - **排除文件**
    使用此选项可以将文件排除在扫描范围之外，并且如果检测到则不删除它们。您既可以指定完整路径，也可以使用掩码。默认情况下，禁用此选项。

  - **不按类型检测对象**
    使用此选项可以避免检测并随后删除对象。您既可以指定完整路径，也可以使用掩码。默认情况下，禁用此选项。

- **高级设置**.

  - **如果扫描时间超过此值则停止(秒)**
    当扫描需要很长时间才能完成时，请使用此选项来扫描大文件和网络。如果扫描对象花费的时间过长，超时将终止冻结的进程，并且扫描程序将继续扫描范围检查。默认情况下，禁用此选项。

  - **不扫描大于此值的复合对象(MB)**
    使用此选项可以加速扫描。例如，您可能希望跳过 100 GB 的数据库存档并将其排除在扫描范围之外。默认情况下，禁用此选项。

  - **使用 iChecker 技术**
    有关 iChecker 技术的更多信息，请参阅文章。默认情况下，启用此选项。

8. 如果需要，在"**网络流量记录**"下，更改便携式扫描程序记录被扫描设备的入站和出站流量的时间段。默认值为 300 秒。

9. 在“**扫描规则源**”下，**选择便携式扫描程序用于审核设备安全的规则源。**

   - “**用于 SCADA 的 Kaspersky ICS CERT 漏洞数据库**”。如果选择此源，便携式扫描程序将扫描设备以查找卡巴斯基 ICS CERT 的 ICS 漏洞数据库中 OVAL 规则中描述的所有漏洞。
   - “**收集主机配置数据的规则**”。选择此来源后，便携式扫描程序会收集**来自主机的配置数据**。

     规则收集以下主机数据：

     - 运行服务
     - 已安装的驱动程序
     - 计划任务
     - 已安装的应用程序和补丁
     - 共享网络资源的名称
     - 启动项
     - 主机信息（IP 地址、DNS 名称）
     - 本地用户和组
     - 主机硬件。
   - “**操作系统的合规和安全配置**”。如果选择此源，便携式扫描程序将检查设备操作系统设置是否符合 OVAL 和 XCCDF 规则中描述的安全标准。

   用于 SCADA 的 Kaspersky ICS CERT 漏洞数据库， 收集主机配置数据的规则 和 操作系统的合规和安全配置 随便携式扫描程序数据库一起提供。因此，在启动便携式扫描程序并选择至少一个列出的规则源之前，请确保便携式扫描程序数据库是最新的。

   - “**自定义规则数据库**”。如果选择此源，便携式扫描程序将检查设备是否存在自定义 OVAL 和 XCCDF 规则中描述的漏洞。

10. 选择将创建便携式扫描程序的可移动驱动器：

    - “**已连接可移动驱动器**”。可移动 USB 驱动器。从下拉列表中选择可移动驱动器。
    - “**安全可移动驱动器**”。Rutoken 可移动 USB 驱动器受管理员密码保护，不可读取、复制和写入。如果您选择了此选项，请在下一个向导步骤中选择一个安全的可移动驱动器。

11. 如果需要，启用“**写入磁盘后验证扫描程序数据。** ”。

    此功能可验证便携式扫描程序数据。例如，如果您计划连续创建具有相同设置的多个便携式扫描仪，则验证第一个便携式扫描程序的数据并尽早发现差异可以节省时间。

12. 如果您选择了**安全可移动驱动器**，请从下拉列表中选择要设置便携式扫描程序的所连接的 Rutoken 可移动驱动器。

    要使 Rutoken 可移动驱动器显示在运行 Windows Server 2022 的计算机上的已连接可移动媒体列表中，必须将 USB 读卡器的 UMDF2 驱动程序替换为 WUDF 驱动程序。

13. 在“**安全设置**”下，在“**输入当前管理员密码**”字段中，输入在 Rutoken 可移动驱动器上设置的管理员密码，以保护其内容不被潜在入侵者读取、复制或写入。

14. 如果需要的话，**更改当前管理员密码**。

    a. 选择**更改管理员的当前密码(只允许使用数字和拉丁符号)**复选框。

    b. 在相应的字段中输入新密码。

    c. 在相应的字段中重新输入密码。

15. 单击“**下一步**”。

    将打开一个向导窗口，其中包含便携式扫描程序配置的描述。

16. 如果需要，**将当前便携式扫描程序设置导出到 XML 文件**。

    a. 单击“**导出**”。

    b. 在打开的窗口中，选择要保存包含便携式扫描程序设置的 XML 文件的路径。

    c. 输入 XML 文件的名称。

    d. 单击“**保存**”按钮。

17. 点击“**创建**”使用指定的设置创建便携式扫描程序。

    便携式扫描程序将被写入选定的可移动驱动器。可移动驱动器上将出现一个 Kavscan 文件夹，其中包含便携式扫描程序工作所需的文件和文件夹。

    如果可移动驱动器上已有便携式扫描程序，则向导将覆盖其文件（报告除外）。

    如果您决定中止写入，安装向导将终止写入操作而不回滚所做的更改。

    完成设置后，向导将提示您创建另一个便携式扫描程序。

如何在命令行上创建便携式扫描程序

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，命令提示符 cmd.exe）。

2. 使用 `cd` 命令，导航到 kavshell.exe 文件所在的文件夹。

例如：`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes 4.5.0`。

您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

3. 运行以下命令：

```
KAVSHELL PORTABLESCANNER /drive=<可移动驱动器的名称或 Rutoken 可移动驱动器的序列号> /license=<授权许可密钥文件的路径> [/tokenpin=<密码> [/newtokenpin=<密码>]] [/verify] [/av <病毒和其他威胁程序扫描设置>] [/traffic <扫描设备上传入和传出流量的记录设置>] [/oval <安全审计任务设置>]
```

创建便携式扫描程序的命令参数

参数	描述
PORTABLESCANNER	必需参数。 发起便携式扫描程序的创建。
/drive=<可移动驱动器的名称或 Rutoken 可移动驱动器的序列号>	必需参数。 选择要生成便携式扫描程序的可移动驱动器： 如果要将便携式扫描程序写入 Rutoken 可移动驱动器，则必须输入 Rutoken 驱动器的十位数序列号。
/license=<授权许可密钥文件的路径>	必需参数。 指定创建便携式扫描程序所需的密钥文件的路径。
/tokenpin=<密码>	可选参数。 设置用于访问 Rutoken 驱动器的管理员密码。
/newtokenpin=<密码>	可选参数。 设置用于访问 Rutoken 驱动器的新管理员密码。
/verify	可选参数。 将便携式扫描程序写入可移动驱动器后对其进行验证。
/av <病毒和其他威胁程序扫描设置>	可选参数。 扫描病毒和其他威胁程序。
/traffic <扫描设备上传入和传出流量的记录设置>	可选参数。 记录扫描设备上的传入和传出流量。
/oval <安全审计任务设置>	可选参数。 启用安全审计任务。

/av、/oval 或 /traffic 参数中的至少一个必须被指定。

病毒和其他威胁程序扫描设置	
<文件列表>	以空格分隔的文件、文件夹、网络路径或预定义扫描范围的列表。
/l=<包含扫描范围列表的文件的路径>	包含扫描范围列表的文件的路径。必须手动创建该文件并以 TXT 格式保存。 文件必须以不带 BOM 的 UTF-8 编码保存。
/memory	开始扫描所有内存进程。
/shared	开始扫描共享文件夹。
/startup	开始扫描启动对象。
/remdrives	开始扫描所有可移动驱动器。
/fixdrives	开始扫描所有固定驱动器。
/mycomp	开始扫描整个计算机。

/fa	扫描所有文件 如果启用该设置，应用程序将毫无例外地检查所有文件（所有格式和扩展名）。
/fc	按格式扫描对象。应用程序只扫描其格式包含在受感染对象格式列表中的对象。
/fe	按扩展名扫描对象。应用程序只扫描其扩展名包含在受感染对象扩展名列表中的对象。
/ai=< 操作 >	对检测到的受感染对象采取的操作。 可能的值： • disinfdel 表示清除，清除失败则删除。 • report 表示发送报告。
/e=< 对象类型 >	排除指定的对象类型。 可能的值： • a 从扫描中排除 RAR、ARJ、ZIP、CAB、LHA、JAR 和 ICE 压缩文件。 • b 排除邮件数据库、传入和传出的电子邮件消息。
/em=< 文件掩码 >	与文件掩码匹配的文件将从扫描范围中排除。例如： • 掩码 *.exe 将包括具有 exe 扩展名的文件的所有路径。 • 掩码 example* 将包括名为 EXAMPLE 的文件的所有路径。
/et=< 扫描持续时间（秒） >	扫描时间长于指定时间限制（以秒为单位）的文件将从扫描范围中排除。
/es=< 大小（兆字节） >	大于指定大小限制（以兆字节为单位）的文件将从扫描范围中排除。
/norecall	扫描文件而不复制到磁盘（如果可能）。
/noichecker	禁用 iChecker。
/w=< 文件路径 >	扫描日志文件的路径和名称。

扫描设备上传入和传出流量的记录设置	
/limit=< 持续时间（秒） >	指定您希望记录流量的时间长度。 可用值：1到1800。

安全审计任务设置	
/source=<kl|kl-compl|file>	指定安全审计所需规则的来源。 可能的参数值： • kl – 分发套件中包含的卡巴斯基 ICS CERT 漏洞数据库 • kl-compl – 操作系统的安全配置和标准合规性，包含 • file – 来自文件的自定义规则数据库。
/path=< 带有安全审计规则的 ZIP 压缩文件的完整路径 >	此参数将路径传递给具有以下规则的文件：**来自文件的自定**（/source=file）。 根据指定 ZIP 存档内的规则启动安全审计任务。 ZIP 压缩文件必须包含一个 OVAL 语言规则的 XML 文件。 您需要提供 ZIP 文件的完整路径，包括其名称。 OVAL 规则必须以不带 BOM 的 UTF-8 编码保存。
/mode=<all|exclude|include>	该参数定义漏洞扫描模式。 可能的参数值： • all – 扫描源中列出的所有漏洞。 • exclude – 扫描源中列出的漏洞，但不包括 /definit • include – 扫描 /definitions 参数所指定的漏洞。 与 /source=kl 参数一起使用。
/definitions=<vulnerability_type_01;vulnerability_type_02;...;vulnerability_type_N>	必须扫描或必须排除在扫描范围之外的漏洞类型的分号分隔 例如： oval:org.mitre.oval.test:def:998;oval:org.mitre 与 /mode=include 或 /mode=exclude 参数一起使用。

例如：

```
KAVSHELL PORTABLESCANNER /drive=E: /license=C:\0000000A.key /verify /av /l="C:\Documents and Settings\file.txt" /ai=disinfdel
```

启动便携式扫描程序

要运行便携式扫描程序：

1. 将包含便携式扫描程序的可移动驱动器连接到您想要扫描的设备。
2. 在设备上使用本地管理员权限启动命令行解释器。
3. 运行 `cd /D` 命令（例如，`cd /D "E:\kavscan"`，其中 `E` 是可移动驱动器的盘符）以更改为包含 kavscan.exe 文件的文件夹。
4. 执行下列操作之一：

   - 如果要使用在录制便携式扫描程序之前指定的设置来启动便携式扫描程序，

     运行 `kavscan.exe scan`

   - 如果您想使用与写入便携式扫描程序之前指定的设置不同的设置来启动便携式扫描程序，

     运行 `kavscan.exe scan [/av] [/traffic=<` 持续时间（秒） `>] [/oval=<` 包含安全审计规则的 `ZIP` 存档的完整路径 `>] [/mycomputer] [/fixed] [/removable] [/remote] [/shared] [/memory] [/startup] [/drive=<` 磁盘 `>] [/folder=<` 要扫描的文件夹的完整路径 `>] [/file=<` 包括名称在内的文件完整路径 `>] [/cure={yes|no}] [/trace] [/dump] [/report=<` 类型 `>] [/settings=<` 具有自定义设置的文件的完整路径 `>]`

     > 如果 ? 字符显示在命令行而不是对话框中，这意味着操作系统和 Kaspersky Industrial CyberSecurity for Nodes 的编码不匹配。为了正确显示对话框，您必须管理操作系统设置以选择不支持 Unicode 的应用程序的语言。您需要选择 Kaspersky Industrial CyberSecurity for Nodes 所使用的语言。

   > 要查看便携式扫描程序运行命令的帮助文档，请运行 `kavscan.exe help`。

   > 全部 `kavscan.exe scan` 开关，除了 `/cure`、`/trace`、`/dump` 和 `/report`，覆盖任何原始便携式扫描程序设置。例如，如果 `kavscan.exe scan` 开关 `/av`、`/traffic` 和 `/oval` 以任意组合或单独指定，便携式扫描程序仅执行由指定键定义的操作，即使原始便携式扫描程序设置包括所有操作。

5. 如果您从安全的可移动驱动器启动便携式扫描程序，请输入您首次配置扫描程序时设置的管理员密码。

启动便携式扫描程序的命令参数

参数	描述
`/av`	开始扫描病毒和其他威胁。
`/traffic=<` 持续时间（秒） `>`	记录指定时间内正在扫描的设备的入站和出站流量。 可用值：1 到 1800。 如果命令中未设置记录持续时间，便携式扫描程序将使用其默认持续时间。如果便携式扫描程序设置中未指定任何值，则使用默认值 300 秒。

/oval=< 包含安全审计规则的 ZIP 存档的完整路径 >	根据指定 ZIP 存档内的规则启动安全审计任务。 ZIP 存档必须包含一个以 OVAL 编写规则的 XML 文件或一组以 XCCDF 编写规则的 XML 文件。 您需要提供 ZIP 文件的完整路径，包括其名称。 如果未指定包含规则的 ZIP 存档的完整路径，便携式扫描程序将根据其原始设置运行安全审计。
/mycomputer	开始扫描整个计算机。
/fixed	开始扫描所有固定驱动器。
/removable	开始扫描所有可移动驱动器。
/remote	开始扫描所有远程驱动器。
/shared	开始扫描共享文件夹。
/memory	开始扫描所有内存进程。
/startup	开始扫描启动对象。
/drive=< 驱动器 >	开始扫描指定驱动器上的所有引导扇区和文件。
/folder=< 要扫描的文件夹的完整路径 >	开始扫描指定文件夹。 您不能使用文件夹标签模板作为参数的值。
/file=< 文件的完整路径，包括其名称 >	开始扫描指定文件。 您需要指定文件的完整路径，包括其名称。
/cure={yes|no}	定义扫描模式。有以下值可用： • yes：扫描并清除。若未设置该参数，则采用设置中配置的模式。 • no：以检测模式扫描。若未设置该参数，则采用设置中配置的模式。
/trace	启用跟踪。
/dump	启用转储记录。
/report=< 类型 >	定义扫描完成后在 Kavscan\Report\report.txt 中创建的报告类型。有以下值可用： • full：包含所有事件类型的完整扫描报告 • critical：仅包含关键事件的扫描报告 • short：仅包含一般统计数据但不包含事件的扫描报告。 默认采用 short 类型。
/settings=< 包含自定义设置的文件的完整路径 >	从包含文件名的完整路径中的文件应用自定义设置。 如果未指定值，便携式扫描程序将应用其原始设置。这些设置位于 Kavscan\settings.dat。

kavscan.exe scan 命令的返回代码：

- 0：命令成功执行。
- 1 – 一般错误。

更新便携式扫描程序数据库

要更新便携式扫描程序反病毒数据库：

1. 通过以下方式之一下载更新的应用程序数据库：
   - 使用分发点的存储库更新数据库。

     在安装了 Kaspersky Industrial CyberSecurity for Nodes 的设备上，为设备或一组设备创建或配置现有的数据库更新任务。开始任务。

设备上安装的 Kaspersky Industrial CyberSecurity for Nodes 版本必须与用于创建便携式扫描程序的 Kaspersky Industrial CyberSecurity for Nodes 版本匹配或更高。否则，更新的应用程序数据库可能不包含便携式扫描程序正常运行所需的某些文件。

- 通过卡巴斯基更新实用程序 (KUU) 更新数据库。

  使用卡巴斯基更新实用程序将最新的数据库下载到设备上的文件夹中。

2. 加载数据库后，将包含便携式扫描程序的可移动驱动器连接到具有最新数据库的设备。

3. 运行 `kavscan.exe update /source=<` 包含最新数据库的文件夹的完整路径 `>`，其中 `<` 包含最新数据库的文件夹的完整路径 `>` 是包含下载的应用程序数据库的分发点存储库或本地文件夹，具体取决于步骤 1 中选择的选项。

   便携式扫描程序将更新位于 Bases 文件夹中的应用程序数据库，然后运行数据库完整性检查。此检查的结果将作为消息显示在命令行界面中。

查看便携式扫描程序结果

写入 Rutoken 可移动驱动器的便携式扫描程序结果被隐藏。要访问便携式扫描程序的结果，您需要将它们导出到任何其他可用的存储设备。

扫描完成后，会在 Kavscan 文件夹中创建一个 Results 文件夹。它具有以下结构：

- <scanned device name>：以正在扫描的设备命名的文件夹，包含以下子文件夹：
  - <Date_time>：一个文件夹，其名称包含设备扫描的日期和时间，格式为 YYYY-MM-DD_HH-MM-SS。根据扫描设置，它可能包含以下子文件夹：
    - Backup：包含系统尝试清除的原始文件的备份副本的文件夹。每个文件的名称都包含文件在被扫描设备上的路径。每个文件都打包到受密码保护的 .ZIP 存档中。使用 `infected` 作为密码来访问文件。
    - Detects：包含有关检测的服务信息的文件夹。该文件夹的内容对于在 Kaspersky Industrial CyberSecurity for Networks 中显示警报详细信息是必要的。
    - Dump：包含内存转储的文件夹。如果扫描以内存转储模式启动并且在扫描期间发生严重错误，则会创建此文件夹。
    - Network：包含设备入站和出站流量转储的文件夹。如果扫描以流量记录模式启动，则会创建此文件夹。
    - Oval：包含 ZIP 存档的文件夹，该存档包含针对每个审计安全规则源的 XML 和 HTML 报告。如果扫描包含安全审计，则会创建此文件夹。
    - Report：包含带有扫描报告的 report.txt 文件的文件夹。
    - Results：包含 results_<scanned device name>_<scan date_time>.zip 存档的文件夹，其中包含已完成扫描的结果。此存档对于将扫描结果导入 Kaspersky Industrial CyberSecurity for Networks 是必需的。
    - Temp：包含扫描期间创建的临时数据的文件夹。
    - Trace：包含跟踪日志文件的文件夹。如果扫描程序以跟踪模式启动，则会创建此文件夹。

从 Rutoken 可移动驱动器导出便携式扫描程序结果

如果将便携式扫描程序写入 Rutoken 可移动驱动器，则 Kavscan\Results 文件夹中显示的便携式扫描程序结果将写入隐藏的 Rutoken 驱动器分区。因此，您无法直接查看、复制或将便携式扫描程序的结果传输到其他介质。

要从 Rutoken 可移动驱动器导出便携式扫描程序结果：

1. 将 Rutoken 可移动驱动器连接到您想要将便携式扫描程序结果导出到的设备。
2. 在设备上启动命令行解释器。
3. 运行 `cd /D` 命令（例如，`cd /D "E:\kavscan"`，其中 `E` 是可移动驱动器的盘符）以更改为包含 kavscan.exe 文件的文件夹。
4. 运行 `kavscan export /folder=<` 文件夹的完整路径 `> [/clean]`

   其中：

   `/folder=<` 文件夹完整路径 `>` 指定要将便携式扫描程序结果复制到的文件夹的完整路径。这可以是设备上的文件夹、连接到设备的可移动驱动器或网络共享。

   `/clean` 表示必须从 Rutoken 可移动驱动器中删除便携式扫描程序的结果。如果应用程序无法访问导出文件夹或文件尚未复制到该文件夹，则应用程序不会从 Rutoken 可移动驱动器中删除便携式扫描程序的结果。
5. 出现提示时，输入您在创建便携式扫描程序时设置的管理员密码。

Kavscan\Results 中显示的便携式扫描程序结果将被复制到指定路径的文件夹中，并且文件夹结构将被保存。添加 `/clean` 参数从 Rutoken 可移动驱动器中删除便携式扫描程序的结果。

查看常规扫描报告

扫描完成后，会在 Kavscan\Results\<扫描的设备名称>\<扫描日期时间>\Reports 中创建一个 report.txt 文件。

该报告包含以下部分：

- **标题**

  - 便携式扫描程序版本
  - 扫描日期和时间
  - 用于启动扫描的命令
  - 启动扫描的设备的名称
  - 被扫描设备的操作系统
  - 网络接口：名称、MAC 地址、IP 地址
  - 启动扫描的用户

- 应用程序数据库创建日期
- 扫描范围

- **事件列表**

事件列表包含以下扫描详细信息： `/type=full` 和 `/type=critical` 模式。它包含被扫描设备的名称和针对检测到的对象执行的操作。
对于 `/type=short` 模式，不会生成事件列表。

- **统计信息**

报告的此部分包含扫描完成的日期和时间以及以下类别的对象数量：

- 检测到
- 检测到的受感染对象和其他对象
- 可能被感染的对象
- 对象未清除
- 未删除的对象
- 对象未扫描
- 对象未备份
- 处理错误
- 对象已清除
- 已移至备份区
- 已删除对象
- 已处理对象。
- 受密码保护的对象
- 加密对象
- 已处理对象。

安全审计

仅当您拥有具有 ICS 审计许可对象的活动 Kaspersky Industrial CyberSecurity for Node 授权许可密钥时，才可运行该任务。

安全审计任务是旨在搜索设备上的漏洞并评估设备是否符合操作系统标准的组或本地任务。为了执行安全审计任务，Kaspersky Industrial CyberSecurity for Nodes 使用产品提供的 XML 格式或自定义格式的数据库。

- 为了搜索设备上的漏洞，应用程序使用 OVAL 语言编写的规则。
- 为了评估设备安全性和操作系统的标准合规性，应用程序使用 OVAL 和 XCCDF 语言编写的规则配置。

安全审计规则分为以下几类：

- 合规性 – 这些规则检查系统配置设置是否符合安全策略。
- 清查 – 这些规则检查系统中是否存在规则中指定的软件或硬件。
- 杂项 – 这些规则包含自定义检查。
- 补丁 – 这些规则检查规则中指定的补丁是否安装在系统上。
- 漏洞 – 这些规则检查系统中是否存在规则中指定的漏洞。

安全审计任务设置的限制

创建和配置安全审计任务时，请考虑以下限制：

- 选择“**来自文件的自定义规则库**”来源时，使用的文件累计大小总计限制为 2 MB 。
- 任务执行结果报告的大小限制为 7.5 MB。

支持的 OVAL 扫描类型

安全审计任务支持以下类型的 OVAL 扫描：

- accesstoken；
- auditeventpolicy；
- auditeventpolicysubcategories；
- cmdlet - 适用于 Windows Vista / Server 2008 及更高版本；
- environmentvariable58；

- environmentvariable；
- family；
- file；
- fileauditedpermissions53；
- filehash58；
- filehash；
- group_sid；
- interface；
- lockoutpolicy；
- passwordpolicy；
- port；
- process58；
- process；
- registry；
- rpmverifyfile；
- service；
- sid；
- textfilecontent54；
- user；
- user_sid；
- variable；
- wmi57；
- wmi；
- xmlfilecontent；

对于不受支持的 OVAL 扫描类型，安全审计任务的结果是“*未知*”。

管理安全审计任务

仅当您拥有具有 ICS 审计许可对象的活动 Kaspersky Industrial CyberSecurity for Node 授权许可密钥时，才可运行该任务。

安全审计任务是使用 Kaspersky Security Center Web Console 或命令行界面创建和配置的本地任务或组任务。这些任务用于搜索漏洞并评估企业系统是否符合安全标准。

本节提供有关如何管理安全审计任务的说明。

使用默认设置创建和配置安全审计任务

要使用默认设置创建和配置安全审计任务：

1. 在 Kaspersky Security Center Web Console 主窗口中选择“**资产(设备)** → **任务**”。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 在“**应用程序**”下拉列表中，选择“Kaspersky Industrial CyberSecurity for Nodes”。
4. 在“**任务类型**”下拉列表中，选择“**安全审计**”。
5. 输入任务名称或保留默认名称。
6. 选择任务将分配到的设备。
7. 单击“**下一步**”。
8. 在“**选择账户以运行任务**”窗口中，执行下列操作之一：
   - 选择默认账户。
   - 输入将使用其账户权限来启动任务的用户的名称和密码。
9. 单击“**下一步**”。
10. 在“**完成任务创建**”窗口中，选择“**创建完成时打开任务详情**”复选框。
11. 单击“**完成**”。
    任务属性窗口将打开，其中包含默认设置。
12. 打开“**应用程序设置**”选项卡。
    在“**规则源**”部分，“**来自文件的自定义规则库**”默认处于选中状态。
13. 单击“**从文件导入规则库**”按钮。

14. 在打开的窗口中，指定包含规则数据库的文件。

    您只能加载一个包含具有 OVAL 规则和 XCCDF 规则的 XML 文件的存档。

    存档总大小不得超过 2 MB。

15. 单击“**打开**”。

    “**规则源**”部分显示有关已加载规则的信息。单击“**平台**”字段中的“**了解更多**”链接打开窗口，其中显示所选源的规则中提到的操作系统和产品的列表。

16. 如果需要，可以加载带有外部变量的文件：

    如果选定的规则源包含 XCCDF 规则，则不能使用外部变量。

    a. 选择**将外部变量数据与自定义数据库一起使用**复选框。

    b. 单击“**从文件导入外部变量**”链接。

    c. 在打开的窗口中，指定带有外部变量的文件的路径。

    d. 单击“**打开**”。

17. 在“**范围**”部分，如果需要，更改漏洞扫描模式：

    如果选定的规则源包含 XCCDF 规则，则“**范围**”部分不可用。

    a. 选择以下模式之一：

    - “**扫描所有漏洞**”。

      Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测漏洞数据库规则中描述的所有漏洞。

    - “**扫描除添加到列表之外的所有漏洞**”。

      Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测漏洞数据库规则中描述的所有漏洞（以下列表中添加的漏洞除外）。

    - “**扫描添加到列表中的漏洞**”。

      Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测添加到以下列表中的漏洞。

    b. 如果您选择了“**扫描除添加到列表之外的所有漏洞**”或者“**扫描添加到列表中的漏洞**”，使用“**添加**”或者“**按条件添加**”按钮创建漏洞列表。

18. 在“**高级设置**”部分，如有必要，确定将包含在安全审计任务报告中的基于指令的扫描的状态：

    如果选定的规则源包含 XCCDF 规则，则无法应用指令。

    a. 选择“**使用指令**”复选框。

b. 使用每个指令旁边的开关，确定将显示在安全审计任务报告中的基于指令的扫描的状态。

如果指令状态旁边的开关打开，则基于该指令规则的具有此状态的扫描结果将显示在安全审计任务报告中。

默认情况下，为所有指令选择了“**True**”和“**False**”扫描结果的复选框。

19. 在“**高级设置**”部分，如果需要，配置记录任务完成事件的设置：

a. 选择**启用日志记录**复选框。

b. 从列表中选择所需的**日志记录级别**。

默认情况下，日志存储在 C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs 文件夹中。

以下日志级别可用：

- **关键级别** – 仅限关键事件
- **警告级别** – 仅限关键和警告事件
- **信息级别** – 所有关键、警告和信息事件
- **调试级别** – 所有关键、警告、信息和调试事件

20. 点击“**保存**”保存更改。

您可以手动启动创建的任务或配置计划任务启动。有关详细信息，请参见 *Kaspersky Security Center 帮助*。

使用用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库配置安全审计任务设置

用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库与 Kaspersky Industrial CyberSecurity for Nodes 数据库和模块的更新一起提供和更新。因此，在配置安全审计任务设置之前，使用用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库作为规则源，更新应用程序数据库和模块。

要使用用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库作为规则源来配置安全审计任务设置：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 单击安全审计任务的名称打开任务设置窗口。
3. 选择**应用程序设置**选项卡。
4. 在“**规则源**”部分，选择“ **用于 SCADA 的 Kaspersky ICS CERT 漏洞数据库**”。

将显示有关漏洞数据库的信息。单击“**平台**”字段中的“**详细信息**”链接打开窗口，其中显示所选源的规则中提到的操作系统和产品的列表。

5. 在“**范围**”部分，如果需要，更改漏洞扫描模式：

   a. 选择以下模式之一：

   - “**扫描所有漏洞**”。

     Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库规则中描述的所有漏洞。

   - “**扫描除添加到列表之外的所有漏洞**”。

     Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库规则中描述的所有漏洞（以下列表中添加的漏洞除外）。

   - “**扫描添加到列表中的漏洞**”。

     Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测添加到以下列表中的漏洞。

   b. 如果您选择了“**扫描除添加到列表之外的所有漏洞**”或者“**扫描添加到列表中的漏洞**”，使用“**添加**”或者“**按条件添加**”按钮创建漏洞列表。

6. 在“**高级设置**”部分，如有必要，确定将包含在安全审计任务报告中的基于指令的扫描的状态：

   a. 选择“**使用指令**”复选框。

   b. 使用每个指令旁边的开关，确定将显示在安全审计任务报告中的基于指令的扫描的状态。

   如果指令状态旁边的开关打开，则基于该指令规则的具有此状态的扫描结果将显示在安全审计任务报告中。

   默认情况下，为所有指令选择了“**True**”和“**False**”扫描结果的复选框。

7. 在“**高级设置**”部分，如果需要，配置记录任务完成事件的设置：

   a. 选择**启用日志记录**复选框。

   b. 从列表中选择所需的**日志记录级别**。

   默认情况下，日志存储在 C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs 文件夹中。

   以下日志级别可用：

   - **关键级别** – 仅限关键事件
   - **警告级别** – 仅限关键和警告事件
   - **信息级别** – 所有关键、警告和信息事件
   - **调试级别** – 所有关键、警告、信息和调试事件

8. 单击“**保存**”按钮保存任务设置。

使用安全和标准合规性配置来配置安全审计任务设置

安全和标准合规性配置与 Kaspersky Industrial CyberSecurity for Nodes 数据库和模块更新一起设置和更新。因此，在配置安全审计任务设置之前，使用安全和标准合规性配置，更新应用程序数据库和模块。

要使用安全和标准合规性配置作为规则源来配置安全审计任务设置：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 单击安全审计任务的名称打开任务设置窗口。
3. 选择**应用程序设置**选项卡。
4. 在“**规则源**”部分，选择“ **操作系统的合规和安全配置**”。
5. 单击“**选择规则配置**”。
6. 在打开的窗口中，选择其中一项安全和标准合规性配置。
7. 单击“**确定**”。

   “**规则源**”部分显示有关所选安全和标准合规性配置的信息。“**规则**”部分显示作为源选择的安全和标准合规性配置中包含的规则列表。
8. 在“**高级设置**”部分，如果需要，配置记录任务完成事件的设置：
   a. 选择**启用日志记录**复选框。
   b. 从列表中选择所需的**日志记录级别**。

   默认情况下，日志存储在 C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs 文件夹中。

   以下日志级别可用：

   - **关键级别** – 仅限关键事件
   - **警告级别** – 仅限关键和警告事件
   - **信息级别** – 所有关键、警告和信息事件
   - **调试级别** – 所有关键、警告、信息和调试事件
9. 在“**规则**”部分中，查看所选安全和标准合规性配置中包含的规则列表：
   - 单击规则名称以打开规则描述。
   - 点击“**过滤器**”按钮打开过滤规则的窗口。
10. 单击“**保存**”按钮保存任务设置。

使用来自 Kaspersky Security Center 存储库的自定义规则数据库配置安全审计任务设置

配置安全审计任务设置之前，使用 Kaspersky Security Center 存储库的自定义数据库：

1. 从命令行界面创建用于签署自定义数据库的证书指纹。

   您可以使用现有指纹作为证书来签署自定义数据库。

2. 使用命令行界面创建名为 package.zip 的 Kaspersky Security Center 安装包。

3. 将上一步创建的包含 OVAL 和 XCCDF 规则的 package.zip 存档添加到 Kaspersky Security Center 存储库。为此，请创建并运行安装包安装任务，并使用以下设置：

   - 必须根据上一步创建的 package.zip 存档中的文件来创建安装包。
   - 在选择要分配安装包安装任务的设备的窗口中，手动指定安装了 Kaspersky Security Center 管理服务器的计算机的地址。

在 Kaspersky Industrial CyberSecurity for Nodes 中，您只能使用自定义规则数据库更新已安装和部署的包。无法删除该规则包。

要使用 Kaspersky Security Center 存储库中的自定义规则数据库配置安全审计任务设置：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 点击任务名称打开任务设置窗口。
3. 选择**应用程序设置**选项卡。
4. 在“**规则源**”区域中，选择“**Kaspersky Security Center 存储库中的自定义规则库**”。
5. 单击“**从自定义集合中选择文件**”按钮。
6. 在打开的窗口中，指定具有规则数据库的存档。

   您只能加载一个包含具有 OVAL 规则和/或 XCCDF 规则的 XML 文件的存档。

   存档总大小不得超过 2 MB。

7. 单击“**打开**”。

   “**规则源**”部分显示有关已加载规则的信息。单击“**平台**”字段中的“**详细信息**”链接打开窗口，其中显示所选源的规则中提到的操作系统和产品的列表。

8. 如有必要，请指定用于签署自定义规则数据库的证书的指纹：

   a. 选择“**使用指纹**”复选框。

   b. 在“**指纹**”字段中，输入使用命令行界面获取的指纹。

9. 如果需要，可以加载带有外部变量的文件：

   如果选定的规则源包含 XCCDF 规则，则不能使用外部变量。

   a. 选择**将外部变量数据与自定义数据库一起使用**复选框。

   b. 单击“**从文件导入外部变量**”。

   c. 在打开的窗口中，指定带有外部变量的文件的路径。

   d. 单击“**确定**”。

10. 在“**范围**”部分，如果需要，更改漏洞扫描模式：

    如果选定的规则源包含 XCCDF 规则，则“**范围**”部分不可用。

    a. 选择以下模式之一：

    - “**扫描所有漏洞**”。

      Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库规则中描述的所有漏洞。

    - “**扫描除添加到列表之外的所有漏洞**”。

      Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库规则中描述的所有漏洞（以下列表中添加的漏洞除外）。

    - “**扫描添加到列表中的漏洞**”。

      Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测添加到以下列表中的漏洞。

    b. 如果您选择了“**扫描除添加到列表之外的所有漏洞**”或者“**扫描添加到列表中的漏洞**”，使用“**添加**”或者“**按条件添加**”按钮创建漏洞列表。

11. 在“**高级设置**”部分，如有必要，确定将包含在安全审计任务报告中的基于指令的扫描的状态：

    如果选定的规则源包含 XCCDF 规则，则无法应用指令。

    a. 选择“**使用指令**”复选框。

    b. 使用每个指令旁边的开关，确定将显示在安全审计任务报告中的基于指令的扫描的状态。

       如果指令状态旁边的开关打开，则基于该指令规则的具有此状态的扫描结果将显示在安全审计任务报告中。

       默认情况下，为所有指令选择了“**True**”和“**False**”扫描结果的复选框。

12. 在“**高级设置**”部分，如果需要，配置记录任务完成事件的设置：

    a. 选择**启用日志记录**复选框。

    b. 从列表中选择所需的**日志记录级别**。

    默认情况下，日志存储在 C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs 文件夹中。

    以下日志级别可用：

    - **关键级别** – 仅限关键事件
    - **警告级别** – 仅限关键和警告事件
    - **信息级别** – 所有关键、警告和信息事件
    - **调试级别** – 所有关键、警告、信息和调试事件

13. 单击“**保存**”按钮保存任务设置。

使用文件中的自定义数据库配置安全审计任务设置

要使用文件中的自定义数据库配置安全审计任务设置：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 点击任务名称打开任务设置窗口。
3. 打开“**应用程序设置**”选项卡。
4. 在“**规则源**”部分，选择“ **来自文件的自定义规则库**”。
5. 单击“**从文件导入规则库**”按钮。
6. 在打开的窗口中，指定包含规则数据库的文件。
   您只能加载一个包含具有 OVAL 规则和 XCCDF 规则的 XML 文件的存档。

   存档总大小不得超过 2 MB。

7. 单击“**打开**”。
   “**规则源**”部分显示有关已加载规则的信息。单击“**平台**”字段中的“**了解更多**”链接打开窗口，其中显示所选源的规则中提到的操作系统和产品的列表。
8. 如果需要，可以加载带有外部变量的文件：

如果选定的规则源包含 XCCDF 规则，则不能使用外部变量。

a. 选择**将外部变量数据与自定义数据库一起使用**复选框。

b. 单击“**从文件导入外部变量**”链接。

c. 在打开的窗口中，指定带有外部变量的文件的路径。

d. 单击“**打开**”。

9. 在“**范围**”部分，如果需要，更改漏洞扫描模式：

如果选定的规则源包含 XCCDF 规则，则“**范围**”部分不可用。

a. 选择以下模式之一：

- “**扫描所有漏洞**”。

  Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测漏洞数据库规则中描述的所有漏洞。

- “**扫描除添加到列表之外的所有漏洞**”。

  Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测漏洞数据库规则中描述的所有漏洞（以下列表中添加的漏洞除外）。

- “**扫描添加到列表中的漏洞**”。

  Kaspersky Industrial CyberSecurity for Nodes 扫描分配了任务的设备，以检测添加到以下列表中的漏洞。

b. 如果您选择了“**扫描除添加到列表之外的所有漏洞**”或者“**扫描添加到列表中的漏洞**”，使用“**添加**”或者“**按条件添加**”按钮创建漏洞列表。

10. 在“**高级设置**”部分，如有必要，确定将包含在安全审计任务报告中的基于指令的扫描的状态：

如果选定的规则源包含 XCCDF 规则，则无法应用指令。

a. 选择“**使用指令**”复选框。

b. 使用每个指令旁边的开关，确定将显示在安全审计任务报告中的基于指令的扫描的状态。

如果指令状态旁边的开关打开，则基于该指令规则的具有此状态的扫描结果将显示在安全审计任务报告中。

默认情况下，为所有指令选择了“**True**”和“**False**”扫描结果的复选框。

11. 在“**高级设置**”部分，如果需要，配置记录任务完成事件的设置：

a. 选择**启用日志记录**复选框。

b. 从列表中选择所需的**日志记录级别**。

默认情况下，日志存储在 C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs 文件夹中。

以下日志级别可用：

- **关键级别** – 仅限关键事件
- **警告级别** – 仅限关键和警告事件
- **信息级别** – 所有关键、警告和信息事件
- **调试级别** – 所有关键、警告、信息和调试事件

12. 单击“**保存**”按钮保存任务设置。

查看安全审计任务执行结果

要查看安全审计任务执行结果：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 点击任务名称打开任务设置窗口。
3. 选择**应用程序设置**选项卡。
4. 选择“**报告**”部分。

报告列表包含按日期排序的任务执行结果。列表的每一行包含在任务设置中指定的节点上的**任务执行状态**以及任务执行完成的日期和时间。

Kaspersky Industrial CyberSecurity for Nodes 返回安全审计任务执行结果：

- *已通过*。
  如果**漏洞**指令的扫描结果是*假*，且其余指令的扫描结果是*真*，则安全审计任务具有此状态。
- *未通过*。
  如果**漏洞**指令的扫描结果是*真*，且其余指令的扫描结果是*假*，则安全审计任务具有此状态。
- *警告*。
  如果所有指令的扫描结果为*假*，则安全审计任务具有此状态。
- *其他*。
  如果所有指令的扫描结果为*未知*、*未评估*或*不适用*，则安全审计任务具有此状态。

您可以使用过滤器过滤报告中的数据。

安全审计任务执行结果报告可在任务完成后 7 天内在 Kaspersky Security Center 中查看，或直到任务被删除。

将安全审计任务执行结果导出到单独的文件

要将安全审计任务执行结果导出到单独的文件：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**任务**”。
2. 点击任务名称打开任务设置窗口。
3. 选择**应用程序设置**选项卡。
4. 在“**报告**”选项卡上，选择所需的报告并点击“**详细信息**”按钮。
5. 在打开的“**安全审计结果**”窗口中，执行以下操作之一：
   - 要接收包含 XML 格式的所有任务执行结果报告的存档，请单击“**导出**”。

     包含 XML 格式报告的 ZIP 存档将保存到下载文件的标准操作系统文件夹中。如果任务设置启用了记录安全审计事件，还会添加一个包含 TXT 格式日志的 ZIP 存档。
   - 要接收 HTML 格式的任务执行结果报告存档：
     a. 如果需要，可以使用“**过滤器**”按钮过滤报告数据。
     b. 单击“**创建报告**”。

     包含 HTML 格式报告的 ZIP 存档将保存到下载文件的标准操作系统文件夹中。报告将仅包含匹配过滤器的行。

带有报告的存档名称包含执行任务的节点的名称以及执行任务的日期和时间。

创建用于使用 OVAL 或 XCCDF 规则签名文件的证书指纹

要为使用 OVAL 或 XCCDF 规则签名文件的证书创建指纹：

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，命令提示符 `cmd.exe`）。
2. 使用 `cd` 命令，导航到 ovaldbmgr.exe 文件所在的文件夹。

   默认情况下，该文件位于分发套件的 \tools\ovaldbmgr 文件夹中。
3. 根据证书的位置，运行以下命令之一并按 Enter：
   - 要创建证书然后将其放入 System Storage Local Machine 中：

     `ovaldbmgr.exe --signer=make-cert --subject=<证书名称>`
   - 要创建证书然后将其放入 PFX 容器中：

     `ovaldbmgr.exe --signer=make-cert --subject=<证书名称> --export --pwd=<用于访问 PFX 容器的密码> --pfx=<PFX 容器的完整路径和文件名>`

如果证书创建成功，则证书的指纹将在命令行中返回。

使用自定义 OVAL 或 XCCDF 规则创建 Kaspersky Security Center 安装包

要创建包含 OVAL 或 XCCDF 规则的 Kaspersky Security Center 安装包作为签名存档：

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，命令提示符 `cmd.exe`）。
2. 使用 `cd` 命令，导航到 ovaldbmgr.exe 文件所在的文件夹。

   默认情况下，该文件位于分发套件的 \tools\ovaldbmgr 文件夹中。
3. 根据 OVAL 或 XCCDF 规则文件的签名证书的位置，运行以下命令之一：

   - 如果签名证书位于系统存储本地机器中：

     `ovaldbmgr.exe --make-package --command={replace|merge} --subject=<证书名称> --output=<完整路径> --source=<完整路径> <具有 OVAL 或 XCCDF 规则的文件的完整路径>`

   - 如果签名证书位于 PFX 容器中：

     `ovaldbmgr.exe --make-package --command={replace|merge} --pfx=<PFX 容器的完整路径> --pwd=<访问 PFX 容器的密码> --output=<完整路径> --source=<完整路径> <具有 OVAL 或 XCCDF 规则的文件的完整路径>`

创建 Kaspersky Security Center 安装包的命令参数

选项	描述
`--make-package`	必需参数。 创建一个包含文件的存档。
`--command={replace|merge}`	必需参数。 此参数定义 Kaspersky Security Center 中的包部署模式。 可用值： • `replace` – 使用正在创建的安装包替换 Kaspersky Security Center 存储库中的安装包。 • `merge` – 将正在创建的安装包与 Kaspersky Security Center 存储库中已存在的安装包合并。 如果未指定参数值，则任务以错误结束。
`--pfx=<PFX 容器的完整路径>`	必需参数。 参数指定带有 OVAL 或 XCCDF 规则文件的签名证书足迹的 PFX 容器的完整路径。
`--pwd=<访问 PFX 容器的密码>`	必需参数。 此参数定义访问 PFX 容器的密码。
`--subject=<证书名称>`	必需参数。 此参数传递要签名的证书的名称。如果指定了不存在的签名证书的名称，则命令将以错误结束。
`--output=<完整路径>`	必需参数。 此参数指定运行该命令后将创建安装包的文件夹的完整路径。
`--source=<完整路径>`	此参数指定包含要包含在 Kaspersky Security Center 包中的 OVAL 和 XCCDF 规则的文件夹的完整路径。

选项	描述
< 具有 OVAL 或 XCCDF 规则的文件的完整路径 >	此参数定义您想要包含在 Kaspersky Security Center 包中的 XML 格式的 OVAL 或 XCCDF 规则文件的完整路径。 OVAL 和 XCCDF 规则必须以无 BOM 的 UTF-8 格式保存。 具有 OVAL 或 XCCDF 规则的文件必须位于另一个文件夹内的文件夹中。例如：C:\Users\UserName\Desktop\folder\subfolder\OvalRules.xml 您可以指定由空格分隔的多个参数值。 要指定具有 OVAL 或 XCCDF 规则的文件，请选择以下选项之一： • 仅指定 --source=< 完整路径 > 参数的值。 • 指定一个或多个用空格分隔的 < OVAL 或 XCCDF 规则的完整路径 > 值。 • 同时指定 --source=< 完整路径 > 参数的值和一个或多个 < 具有 OVAL 或 XCCDF 规则的文件的完整路径 > 值，以空格分隔。 如果没有指定 < 具有 OVAL 或 XCCDF 规则的文件的完整路径 > 值，并且省略了 --source=< 完整路径 > 参数，任务将以错误结束。

运行该命令后，Kaspersky Industrial CyberSecurity for Nodes 将创建：

- 由 --output=< full path > 参数的值指定的文件夹中的名为 package.zip 的存档。该存档包含以下文件：
  - 每个带有 OVAL 或 XCCDF 规则的自定义文件有一个或多个 ZIP 文件。每个存档包含一个带有规则的 XML 文件以及该 XML 文件的签名文件。
  - 用于部署 Kaspersky Security Center 包的 ovaldbmgr.kud 文件。
  - Ovaldbmgr.exe 部署实用程序。
- 用于对 package.zip 存档进行签名的签名指纹。

  您可以在"使用来自 Kaspersky Security Center 存储库的自定义规则数据库进行安全审计任务设置"中指定指纹作为规则源。

使用命令行配置和启动安全审计任务

对于以下规则源，您可以使用命令行界面配置和启动安全审计任务：

- **用于 SCADA 的 Kaspersky ICS CERT 漏洞数据库**
- **操作系统的合规和安全配置**
- "**来自文件的自定义规则库**"。

要使用命令行界面配置和启动安全审计任务：

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，cmd.exe）。
2. 使用 cd 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如，`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0` 并按 **ENTER**。

   您还可以在应用程序安装阶段将可执行文件路径添加到 %PATH% 系统变量，并在不导航到应用程序文件夹的情况下运行命令。

3. 运行以下命令：

   `KAVSHELL SCAN-OVAL [/SOURCE:<kl|kl-compl|file>] [/REPOSITORY:show] [/PATH:<具有 OVAL 规则的存档的完整路径和名称，或具有 OVAL 和 XCCDF 规则的存档>] [/EXTERNAL-VARS:<带有外部变量的 ZIP 存档的完整路径和名称>] [/MODE:<all|exclude|include>] [/DEFINITIONS:<vulnerability_type_01;vulnerability_type_02;...;vulnerability_type_N>] /RESULT-PATH:包含报告的文件夹路径>`

4. 按 **Enter**。

配置和启动安全审计任务的命令参数

参数	描述
`SCAN-OVAL`	必需参数。 在设备上启动安全审计任务。
`/SOURCE`	指定安全审计所需规则的来源。 可用值： • `kl` – 分发套件中包含的卡巴斯基 ICS CERT 漏洞数据库。成功更新 Kaspersky Industrial CyberSecurity for Nodes 数据库和模块后，可从命令行使用。 • `kl-compl` – 操作系统的安全配置和标准合规性，包含在分发套件中。成功更新 Kaspersky Industrial CyberSecurity for Nodes 数据库和模块后，可从命令行使用。 • `file` – 来自文件的自定义规则数据库。 若未指定参数值，则默认使用以下源：**用于 SCADA 的 Kaspersky ICS CERT 漏洞数据库**（`/SOURCE=kl`）。
`/REPOSITORY`	如果所选规则源是操作系统的安全配置和标准合规性（`/SOURCE=kl-compl`），该参数可用。 如果指定了该参数，则 Kaspersky Industrial CyberSecurity for Nodes 不会执行安全审计任务，而是将列出现有安全配置名称的 XML 文件保存到由 `/RESULT-PATH` 参数指定的文件夹。
`/PATH`	此参数指定包含具有 OVAL 规则的 XML 文件的存档的完整路径，或者指定包含具有“**操作系统的合规和安全配置**”（`/SOURCE=kl-compl`）和“**来自文件的自定义规则库**”（`/SOURCE=file`）源的 OVAL 和 XCCDF 规则的 XML 存档的完整路径。 OVAL 和 XCCDF 规则必须以无 BOM 的 UTF-8 格式保存。
`/EXTERNAL-VARS`	此参数指定 ZIP 存档的完整路径和名称，该存档包含带有 OVAL 规则的外部变量的 XML 文件。 如果源仅包含 OVAL 规则，则该参数可用。
`/MODE`	该参数定义漏洞扫描模式。 如果源仅包含 OVAL 规则，则该参数可用。 可能的参数值： • `all` – 扫描源中列出的所有漏洞。 • `exclude` – 扫描源中列出的漏洞，但不包括 `/definitions` 参数指定的漏洞。 • `include` – 扫描 `/definitions` 参数所指定的漏洞。 如果未指定参数值，则默认使用 `all` 模式。
`/DEFINITIONS`	必须扫描或必须排除在扫描范围之外的漏洞类型的分号分隔列表。 如果源仅包含 OVAL 规则，则该参数可用。 例如：`oval:org.mitre.oval.test:def:998;oval:org.mitre.oval.test:def:999`。 与 `/MODE=include` 或 `/MODE=exclude` 参数一起使用。
`/RESULT-PATH`	必需参数。 指定存储 XML 格式的扫描报告的文件夹路径。文件名包含节点名称以及运行任务的日期和时间。 如果不指定该参数，任务执行将失败。

SCAN-OVAL 命令的返回代码：

- 0 – 命令成功执行；
- 1 – 一般错误。

如果命令成功完成（代码 0），XML 格式的报告将保存在 /RESULT-PATH 参数指定的文件夹中。

使用 Kaspersky Security Gateway

该应用程序与 Kaspersky Security Gateway 4.0 或更高版本兼容。

Kaspersky Security Gateway 旨在将从 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 接收的诊断信息，或直接从 Kaspersky Industrial CyberSecurity for Networks 接收的诊断信息，从 Kaspersky Security Center 传输到 SCADA 系统。将工业网络及网络中各个计算机的保护状态信息显示在 SCADA 系统的屏幕上，使得 SCADA 系统操作员能够对工业网络保护问题做出及时响应。

Kaspersky Security Gateway 使用以下通信协议与 SCADA 系统交互：

- **IEC 60870-5-104**。自动化系统的统一开放协议。
- **OPC DA**。基于 Microsoft COM 技术的工业网络设备交互规范。
- **OPC UA**。提供跨平台兼容性的工业网络设备交互规范。

您可以使用 Kaspersky Security Gateway 图形用户界面或标准 Microsoft Windows 工具配置数据传输设置。

诊断信息

Kaspersky Security Gateway 向 SCADA 系统传输以下信息：

- “**SecurityServerAvailable**”。Kaspersky Security Center 管理服务器的可用性。可能的值：
  - `1`。Kaspersky Security Gateway 已成功连接到 Kaspersky Security Center 管理服务器。
  - `0`。Kaspersky Security Gateway 无法连接到 Kaspersky Security Center 管理服务器。
- “**AllSecuredHostAvailable**”。网络上所有受保护计算机的可用性。如果计算机上运行有保护应用程序和网络代理，则该计算机可用。可能的值：
  - `0`。当确定状态时，至少有一台由 Kaspersky Security Center 管理服务器管理并在 Kaspersky Security Gateway 设置中选择用于监控的计算机不可用。
  - `1`。当状态确定时，所有由 Kaspersky Security Center 管理服务器管理并在 Kaspersky Security Gateway 设置中选择用于监控的计算机均可用。

  如果至少有一台计算机与 Kaspersky Security Center 管理服务器之间没有连接，则发送 *0（不可用）*。
- “**GeneralizedThreatOccured**”。网络保护状态。可能的值：
  - `0`。网络上的所有计算机上均未检测到威胁。
  - `1`。网络上至少有一台计算机检测到威胁。
  - `2`。网络上至少有一台计算机出现警告。

在确定网络保护状态时，Kaspersky Security Gateway 仅使用已在 Kaspersky Security Gateway 设置中选择的要在 SCADA 系统中显示的计算机的状态信息。

- **<计算机名称>**。计算机的可用性和保护状态。计算机上装有保护应用程序并且网络代理正在运行。可能的值：
  - `0`。计算机可以使用。
  - `1`。在计算机上检测到了威胁。
  - `2`。已向计算机发出警告。
  - `3`。计算机不可用。

  Kaspersky Security Gateway 仅发送已在 Kaspersky Security Gateway 设置中选择的要在 SCADA 系统中显示的计算机的状态信息。

  如果计算机或 Kaspersky Security Gateway 与 Kaspersky Security Center 管理服务器之间没有连接，则发送 *3 (不可用)*。

- **<PLC 的 IP 地址>**。连接到 Kaspersky Security Center 的 PLC 的状态：
  - `0`。没有错误消息或未检查 PLC。
  - `1`。严重错误（例如，PLC 项目与参考项目不匹配）。
  - `2`。警告。
  - `3`。PLC 不可用。

Kaspersky Security Gateway 的限制和已知问题

- 要将安装在运行 Windows 7、Windows Server 2008 或 Windows Server 2012 的设备上的 Kaspersky Security Gateway 连接到 Kaspersky Security Center 14 及更高版本，必须在操作系统中启用 TLS 1.1 和 1.2 作为默认安全协议。有关详细信息，请参阅 Microsoft 文档。
- `gateway_service.exe` 紧急终止可能是由于第三方 grpc 库错误导致的。当使用Application Verifier执行动态代码分析的同时建立与 Kaspersky Industrial CyberSecurity for Networks 的连接时，会发生服务紧急终止。
- Kaspersky Security Gateway 与 Kaspersky Industrial CyberSecurity for Networks 版本 4.2 及更高版本兼容。
- 当将 KSG OPC UA 服务器与 PcVue 16.2 一起使用时，打开 SessionsDiagnosticsSummary 节点时 PcVue 16.2 可能会崩溃。
- 在装有 SCADA 系统的设备上安装 Kaspersky Security Gateway 可能会降低 OPC Core Components Redistributable 的版本。这可能会导致 SCADA 系统运行出错。

如果出现此问题，请执行以下操作：

1. 使用标准 Microsoft Windows 工具移除 OPC Core Components Redistributable。
2. 安装最新版本的 Kaspersky Security Gateway。要获取 Kaspersky Security Gateway 的安装包，请联系技术支持。
3. 重启设备。

Kaspersky Security Gateway 控制台界面

Kaspersky Security Gateway 控制台在 Microsoft Management Console 树中以节点形式显示，名称为“**Kaspersky Security Gateway**”。

控制台树显示 **Kaspersky Security Gateway** 节点和子节点，用于配置 SCADA 系统中使用的数据传输协议：

- “**IEC 60870-5-104**”。
- “**OPC DA**”。
- “**OPC UA**”。

“**Kaspersky Security Gateway**”节点的结果窗格显示以下内容：

- 关于 Kaspersky Security Gateway 的一般信息。
- 有关连接 Kaspersky Security Center 以及 Kaspersky Industrial CyberSecurity for Networks 的设置的详细信息，以及设置窗口的链接。
- 当前 Kaspersky Security Gateway 附加设置的详细信息以及设置窗口的链接。

配置与 Kaspersky Security Center 的连接

要配置到 Kaspersky Security Center 的连接：

1. 打开 Kaspersky Security Gateway 控制台
2. 选择“**Kaspersky Security Gateway**”节点。
3. 在结果窗格的“**Connection Settings**”部分中，单击“**Configure connection**”链接。
   “**Connection Settings**”窗口将打开。

4. 在“**Kaspersky Security Center**”下，指定以下设置以连接到 Kaspersky Security Center 管理服务器：

- “**Server**”。Kaspersky Security Center 管理服务器的 IP 地址或域名以及用于连接该服务器的端口号。端口号的值范围是 1–65535。

  - 对于 klakaut 数据提供商，默认端口号是 13291。*klakaut* 是 Kaspersky Security Center 自动化实用程序，它允许您使用 COM (Component Object Model) 对象通过外部 API 管理 Kaspersky Security Center 管理服务器。如果选择 klakaut 实用程序作为数据提供程序，则必须在同一台计算机上安装 Kaspersky Security Center 管理控制台，然后才可安装 Kaspersky Security Gateway。

  如果您在 Kaspersky Security Gateway 之后安装 Kaspersky Security Center 管理控制台，则无法建立 Kaspersky Security Gateway 和 Kaspersky Security Center 管理服务器之间的连接。

  - 对于 Open API 数据提供商，默认端口号是 13299。如果选择 Open API 接口作为数据提供程序，则必须**导出 Kaspersky Security Center 根证书**并将其安装到受信任的根证书颁发机构 (CA) 的证书存储区中。

    1. 在浏览器中输入 `https://<Web Console 地址>:13299`。
    2. 在您的浏览器中，打开与 Kaspersky Security Center Web Console 建立的连接的证书信息。
    3. 在“**证书**”窗口中，选择“**证书路径**”选项卡。
    4. 选择根证书。
    5. 转到“**详细信息**”选项卡。
    6. 通过单击“**复制到文件**”按钮导出所选的证书。

  有关 Kaspersky Security Center 配置的详细信息，请参阅 *Kaspersky Security Center 帮助*。

- “**User name**”。Kaspersky Security Center 管理服务器管理员的账户名。
- “**Password**”。Kaspersky Security Center 管理服务器管理员的账户密码。

5. 单击**Test connection**按钮。

   状态“*Connected*”将在连接建立后出现。

6. 单击“**OK**”。

7. 点击“**OK**”按钮关闭 **Kaspersky Security Gateway** 窗户。

您还可以使用位于 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 文件夹中的 `ConnectionSettings.xml` 配置文件配置连接设置。请注意，您不能在配置文件中设置密码。使用 Kaspersky Security Gateway 控制台设置密码。

配置与 Kaspersky Industrial CyberSecurity for Networks 的连接

要配置与 Kaspersky Industrial CyberSecurity for Networks 的连接

1. 打开 Kaspersky Security Gateway 控制台
2. 选择“**Kaspersky Security Gateway**”节点。
3. 在结果窗格的“**Connection Settings**”部分中，单击“**Configure connection**”链接。

   “**Connection Settings**”窗口将打开。
4. 在“**Kaspersky Industrial CyberSecurity for Networks**”下，添加一个或多个 Kaspersky Industrial CyberSecurity for Networks 服务器的连接设置：

   a. 单击**Add**按钮。

   “**Kaspersky Industrial CyberSecurity for Networks connection settings**”窗口将打开。

   b. 输入之前添加到 Kaspersky Industrial CyberSecurity for Networks 的通用类型连接器的 IP 地址，以及用于连接到该连接器的端口号。端口号的值范围是 1–65535。

   > 连接器连接设置与 Kaspersky Industrial CyberSecurity for Networks 集成服务器的连接设置不同。有关连接器的详细信息，请参阅 Kaspersky Industrial CyberSecurity for Networks 帮助。

   c. 如果您想配置与 Kaspersky Industrial CyberSecurity for Networks 的受信任连接：

      1. 选择**Use pinned certificate to secure connection**复选框。
      2. 单击“**Load**”。
      3. 这将打开一个窗口；在该窗口中，选择带有 TLS 证书的文件。
      4. 点击“**打开**”。

   有关添加的 TLS 证书的信息显示在“**TLS certificate data**”下。

   > 如果您指定了固定证书来保护连接，则还必须指定客户端证书。否则，无法建立与 Kaspersky Industrial CyberSecurity for Networks 的连接。

   d. 如果要使用客户端证书配置额外的连接保护：

      1. 选择**Secure connection with client certificate**复选框。
      2. 单击“**Load**”。
      3. 这打开了一个窗户；在该窗口中，选择一个带有客户端证书的 PFX 文件。

4. 点击“**打开**”。

5. 在同名字段中，输入客户端证书的密码。

e. 单击“**Test connection**”。
状态“*Connected*”将在连接建立后出现。

f. 单击“**OK**”。

g. 如有必要，重复步骤 a–f 以添加其他 Kaspersky Industrial CyberSecurity for Networks 服务器的连接设置。

Kaspersky Industrial CyberSecurity for Networks 连接信息显示在“**Connection settings**”窗口中的列表中。

5. 单击“**确定**”。

您还可以使用位于 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 文件夹中的 `ConnectionSettings.xml` 配置文件配置连接设置。请注意，您不能在配置文件中设置密码。使用 Kaspersky Security Gateway 控制台设置密码。

配置 DCOM 协议

如果通过 OPC DA 协议发送和接收数据的计算机未加入 Active Directory 域，请为每台计算机创建具有相同名称和密码的用户账户。

要建立 OPC DA 连接，请配置分布式组件对象模型 (DCOM) 协议的访问权限。

如何配置 DCOM 协议以实现 Kaspersky Security Gateway 与安装在一台计算机上的 SCADA 系统之间的交互

1. 在安装了 Kaspersky Security Gateway 和 SCADA 系统的计算机上，如果要配置它们之间的交互，请按 **Win+R** 组合键。
将打开标准 Microsoft Windows“**运行**”窗口。

2. 在“**打开**”字段输入“*dcomcnfg*”并按“**确定**”。
“**组件服务**”窗口打开。

3. 在窗口左侧的文件夹树中，选择“**组件服务** → **计算机** → **我的电脑**”。

4. 打开“**我的电脑**”文件夹的上下文菜单并选择“**属性**”。

5. 选择“**我的电脑属性**”窗户中的“**COM 安全性**”选项卡。

6. 在“**访问权限**”下， 点击“**编辑默认**”。
这将打开“**访问权限**”窗口。

7. 在“**组或用户名**”，选择“**网络服务**”组。

8. 在“**网络服务**”组的权限表中，在“**允许**”列中，选择“**本地访问**”和“**远程访问**”复选框。

9. 选择“**默认属性**”选项卡并确保配置了以下值：**默认身份验证级别** – *连接*，**默认模拟级别** – *识别*。
10. 单击“**确定**”。
11. 在“**属性：我的电脑**”窗口中，单击“**确定**”按钮。
12. 重新启动计算机。

如何配置 DCOM 协议以实现 Kaspersky Security Gateway 与安装在不同计算机上的 SCADA 系统之间的交互

在两台计算机上：

1. 按 **Win+R** 组合键。
   将打开标准 Microsoft Windows“**运行**”窗口。
2. 在“**打开**”字段输入“*dcomcnfg*”并按“**确定**”。
   “**组件服务**”窗口打开。
3. 在窗口左侧的文件夹树中，选择“**组件服务 → 计算机 → 我的电脑**”。
4. 打开“**我的电脑**”文件夹的上下文菜单并选择“**属性**”。
5. 选择“**我的电脑属性**”窗户中的“**COM 安全性**”选项卡。
6. 在“**访问权限**”部分，点击“**编辑限制**”按钮。
   这将打开“**访问权限**”窗口。
7. 在“**组名或用户名**”部分，选择“**匿名登录**”组。
8. 在“**匿名登录**”组的权限表中，在“**允许**”列中，选择“**本地访问**”和“**远程访问**”复选框。

   > 允许对“匿名登录”组进行远程访问会影响系统的安全级别。我们建议在没有此权限的情况下测试 OPC DA 协议的运行，并且仅在没有此权限就无法工作时才授予此权限。

9. 在“**访问权限**”下，点击“**编辑默认**”并重新执行说明中的第 7 步至第 8 步。
10. 在“**启动和激活权限**”下，点击“**编辑限制**”并重新执行说明中的第 7 步至第 8 步。
11. 在“**启动和激活权限**”下，点击“**编辑默认**”并重新执行说明中的第 7 步至第 8 步。
12. 在“**默认属性**”选项卡上，确保配置了以下值：**默认身份验证级别** – *连接*，**默认模拟级别** – *识别*。
13. 单击“**确定**”。
14. 在“**属性：我的电脑**”窗口中，单击“**确定**”按钮。

15. 配置 OPCEnum 应用程序。

    a. 在窗口左侧的文件夹树中，选择“**组件服务** → **计算机** → **我的电脑** → DCOM Config → OPCEnum”。

    b. 右键单击以显示“**OPCEnum**”的上下文菜单并选择“**属性**”。
    这将打开“**属性：OPCEnum**”窗口。

    c. 在“**常规**”选项卡上，确保“**默认身份验证级别**”设置为“*连接*”。

    d. 在“**安全**”选项卡上，在“**启动和激活权限**”下， 点击“**编辑**”。

    e. 在“**组名或用户名**”下，选择“**全部**”组。

    f. 在“**全部**”组的权限表中，在“**允许**”列中，选择“**本地访问**”、“**远程访问**”、“**本地激活**”、“**远程激活**”复选框。

    g. 在“**访问权限**”部分，点击“**编辑**”按钮。

    h. 在“**组名或用户名**”下，选择“**全部**”组。

    i. 在“**全部**”组的权限表中，在“**允许**”列中，选择“**本地访问**”和“**远程访问**”复选框。

    j. 在“**身份**”选项卡上，选择“**系统帐户**”。

    k. 单击“**确定**”。

16. 重新启动计算机。

在安装了 Kaspersky Security Gateway 实用程序的计算机上：

1. 按 **Win+R** 组合键。
   将打开标准 Microsoft Windows“**运行**”窗口。

2. 在“**打开**”字段输入“*dcomcnfg*”并按“**确定**”。
   “**组件服务**”窗口打开。

3. 在窗口左侧的文件夹树中，选择“**组件服务** → **计算机** → **我的电脑** → DCOM Config → Kaspersky Gateway OPC Service”。

4. 打开“Kaspersky Gateway OPC Service”的上下文菜单并选择“**属性**”。
   这将打开“**属性：Kaspersky Gateway OPC Service**”窗口。

5. 在“**常规**”选项卡上，确保“**默认身份验证级别**”设置为“*连接*”。

6. 单击“**确定**”。

7. 如果 Kaspersky Security Gateway 和 SCADA 系统安装在属于不同域的计算机上：

   a. 在操作系统中，打开“**控制面板** – **管理工具** – **本地安全策略**”。

   b. 在本地安全策略控制台树中，选择“**本地策略** – **安全选项**”部分。

   c. 在“**安全选项**”部分的工作区中，在“**网络访问：让 Everyone 权限应用于匿名用户**”本地策略的上下文菜单中，选择“**已启用**”。

8. 重新启动计算机。

使用通信协议配置数据传输设置

本节提供有关使用可用通信协议配置数据传输的说明。

使用 IEC 60870-5-104 协议配置数据传输

要使用 Kaspersky Security Gateway 控制台配置通过 IEC 60870-5-104 协议的数据传输：

1. 打开 Kaspersky Security Gateway 控制台
2. 在“**Kaspersky Security Gateway**”节点选择“**IEC 60870-5-104**”。
3. 在结果窗格的“**Data transmission settings**”部分中，单击“**Change**”链接。
   “**Settings**”窗口将打开。
4. 在“**Transmission settings**”部分，禁用或启用“**Enable data transmission**”选项。
   如果启用此功能，Kaspersky Security Gateway 会将工业网络节点的保护状态发送到 SCADA 系统。默认禁用此选项。
5. 在“**Connection settings**”组框中，配置以下设置：
   - “**Device address**”。分配给 SCADA 系统中的计算机的辅助地址。可能的值范围：1–65535。
   - “**Device port**”。用于建立与 SCADA 系统的连接的端口号。可能的值范围：1–65535。
   - “**TCP connection timeout**”。该值以秒为单位指定。可能的值范围：1–255。
   - “**Message send timeout**”。该值以秒为单位指定。可能的值范围：1–255。
   - “**Message confirmation timeout**”。该值以秒为单位指定。可能的值范围：1–255。
   - “**Test connection timeout**”。该值以秒为单位指定。可能的值范围：1–255。
   - “**Maximum unconfirmed received messages allowed**”。可能的值范围：1–32767。
   - “**Maximum unconfirmed sent messages allowed**”。可能的值范围：1–32767。
6. 单击“**OK**”。

7. 在结果窗格的“**Tracked data**”部分中，单击“**Change**”链接。

   “**Selecting tracked data**”窗口将打开。该列表显示连接到数据源（例如 Kaspersky Security Center 和/或 Kaspersky Industrial CyberSecurity for Networks）后自动添加的跟踪数据。

8. 选中或清除计算机名称旁边的复选框以启用或禁用对其可用性和保护状态的跟踪。计算机上装有保护应用程序并且网络代理正在运行。

   如果启用跟踪，数据将被传输到 SCADA 系统。

   如果禁用跟踪，数据将不会传输到 SCADA 系统。

   如果计算机或 Kaspersky Security Gateway 与 Kaspersky Security Center 管理服务器之间没有连接，则发送 *3 (不可用)*。

9. 如果需要，可以在“**Service tag**”列编辑或添加服务标签。您可以使用服务标签来过滤 SCADA 系统中接收的数据。标签可能仅由数字组成。

10. 单击“**OK**”。

您可以使用 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 文件夹中的 `ProtocolEICSettings.xml` 配置文件配置通过 IEC 60870-5-104 协议的数据传输。

使用 OPC DA 协议配置数据传输

要通过 OPC DA 协议成功传输数据，必须满足以下先决条件：

- 所需的 DCOM 权限在 SCADA 系统和 Kaspersky Security Gateway 中均分配给 OPCEnum。
- 对安装 Kaspersky Security Gateway 的计算机和 SCADA 系统设置了统一身份验证：采用域身份验证，或者工作组所有计算机使用相同的用户名/密码。

要使用 Kaspersky Security Gateway 控制台配置通过 OPC DA 协议的数据传输：

1. 打开 Kaspersky Security Gateway 控制台
2. 在“**Kaspersky Security Gateway**”节点选择“**OPC DA**”。
3. 在结果窗格的“**Data transmission settings**”部分中，单击“**Change**”链接。

   “**Settings**”窗口将打开。

4. 禁用或启用“**Enable data transmission**”选项。

   如果启用此功能，Kaspersky Security Gateway 会将工业网络节点的保护状态发送到 SCADA 系统。默认禁用此选项。

5. 单击“**OK**”。
6. 在结果窗格的“**Tracked data**”部分中，单击“**Change**”链接。

   “**Selecting tracked data**”窗口将打开。该列表显示连接到数据源（例如 Kaspersky Security Center 和/或 Kaspersky Industrial CyberSecurity for Networks）后自动添加的跟踪数据。

7. 选中或清除计算机名称旁边的复选框以启用或禁用对其可用性和保护状态的跟踪。计算机上装有保护应用程序并且网络代理正在运行。

   如果启用跟踪，数据将被传输到 SCADA 系统。

   如果禁用跟踪，数据将不会传输到 SCADA 系统。

   如果计算机或 Kaspersky Security Gateway 与 Kaspersky Security Center 管理服务器之间没有连接，则发送 *3 (不可用)*。

8. 如果需要，可以在“**Service tag**”列编辑或添加服务标签。您可以使用服务标签来过滤 SCADA 系统中接收的数据。标签可能包含数字或字母。

9. 单击“**OK**”。

您可以使用 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 文件夹中的 `ProtocolOPCSettings.xml` 配置文件配置通过 OPC DA 协议的数据传输。

使用 OPC UA 协议配置数据传输

要使用 Kaspersky Security Gateway 控制台配置通过 OPC UA 协议的数据传输：

1. 打开 Kaspersky Security Gateway 控制台

2. 在“**Kaspersky Security Gateway**”节点选择“**OPC UA**”。

3. 在结果窗格的“**Data transmission settings**”部分中，单击“**Change**”链接。

   “**Settings**”窗口将打开。

4. 禁用或启用“**Enable data transmission**”选项。

   如果启用此功能，Kaspersky Security Gateway 会将工业网络节点的保护状态发送到 SCADA 系统。默认禁用此选项。

5. 在“**Connection settings**”下，输入建立与 SCADA 系统的连接的端口号。端口号的值范围是 1–65535。

6. 单击“**OK**”。

7. 在结果窗格的“**Tracked data**”部分中，单击“**Change**”链接。

   “**Selecting tracked data**”窗口将打开。该列表显示连接到数据源（例如 Kaspersky Security Center 和/或 Kaspersky Industrial CyberSecurity for Networks）后自动添加的跟踪数据。

8. 选中或清除计算机名称旁边的复选框以启用或禁用对其可用性和保护状态的跟踪。计算机上装有保护应用程序并且网络代理正在运行。

   如果启用跟踪，数据将被传输到 SCADA 系统。

   如果禁用跟踪，数据将不会传输到 SCADA 系统。

   如果计算机或 Kaspersky Security Gateway 与 Kaspersky Security Center 管理服务器之间没有连接，则发送 *3 (不可用)*。

9. 如果需要，可以在“**Service tag**”列编辑或添加服务标签。您可以使用服务标签来过滤 SCADA 系统中接收的数据。标签可能包含数字或字母。

10. 单击“**OK**”。

您可以使用 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 文件夹中的 `ProtocolOPCUASettings.xml` 配置文件配置通过 OPC UA 协议的数据传输。

使用配置文件配置数据传输

编辑配置文件需要专业知识。错误地编辑配置文件可能会导致 Kaspersky Security Gateway 错误。

要使用配置文件配置数据传输：

1. 在任何文本编辑器中，打开 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 文件夹中带有 Kaspersky Security Gateway 设置的配置文件：

   - `ProtocolIECSettings.xml` 是 IEC 60870-5-104 协议的配置文件。
   - `ProtocolOPCSettings.xml` 是 OPC DA 协议的配置文件。
   - `ProtocolOPCUASettings.xml` 是 OPC UA 协议的配置文件。

2. 配置数据传输设置。

3. 保存配置文件。

4. 重新启动 Kaspersky Security Gateway 服务以应用新设置。

配置 Kaspersky Security Gateway 附加设置

要配置 Kaspersky Security Gateway 的其他设置：

1. 打开 Kaspersky Security Gateway 控制台

2. 选择“**Kaspersky Security Gateway**”节点。

3. 在结果窗格的“**Application Settings**”部分中，单击“**Configure application settings**”链接。
   “**Application settings**”窗口将打开。

4. 在“**Interrogation**”部分中，设置“**Interrogation period (sec)**”。

5. 在“**System tracing**”部分中：

   - 清除或选中“**Enable tracing**”复选框。
   - 在下拉列表中，选择“**Level**”信息以记录。

6. 在“**Application settings**”窗口中，单击“**OK**”。

您可以使用 `C:\ProgramData\Kaspersky Lab\Security Gateway\Settings` 文件夹中的 `AppSettings.xml` 配置文件配置 Kaspersky Security Gateway 的高级设置。

查看 Kaspersky Security Gateway 事件

Kaspersky Security Gateway 运行期间可能会发生以下事件：

- 启用和禁用 Kaspersky Security Gateway 服务。
- Kaspersky Security Gateway 和 SCADA 系统之间的通信问题。
- 连接到 Kaspersky Security Center 管理服务器并从管理服务器接收数据时出现问题。
- 访问 Kaspersky Security Gateway 配置文件时出现问题。

有关此类事件的信息记录在存储在 `%ProgramData%\Kaspersky Lab\Security Gateway\Traces` 文件夹中的跟踪文件中。

BitLocker 完整磁盘加密管理

BitLocker 是 Windows 操作系统内置的加密技术。Kaspersky Industrial CyberSecurity for Nodes 允许您使用 Kaspersky Security Center 控制和管理 Bitlocker。BitLocker 可对逻辑卷进行加密。有关 BitLocker 的详细信息，请参阅 Microsoft 文档。

Kaspersky Industrial CyberSecurity for Nodes 不支持在 Windows Vista 和 Windows Server 2008 计算机上管理 BitLocker。

加密磁盘时，BitLocker 将引导加载程序和其他辅助文件放入 system partition。此分区未加密。操作系统在安装 Windows 时会自动创建系统分区。如果在安装 Windows 之前磁盘已完全分区，则操作系统无法创建系统分区。在这种情况下，当启动 BitLocker 磁盘加密时，操作系统会提示用户对磁盘重新分区，并创建系统分区。创建系统分区后，操作系统启动 BitLocker 加密。

Kaspersky Industrial CyberSecurity for Nodes 不支持可移动驱动器的 BitLocker 加密。

BitLocker 使用受信任平台模块提供对访问密钥的安全存储。*受信任平台模块 (TPM)* 是一个与安全相关的提供基本功能的微芯片（例如用于存储加密密钥）。受信任平台模块通常安装在计算机主板上，并通过硬件总线与其他所有系统组件进行交互。使用 TPM 是存储 BitLocker 访问密钥的最安全方式，因为 TPM 提供了启动前系统完整性验证。您仍然可以在没有 TPM 的计算机上对驱动器进行加密。在这种情况下，将使用密码对访问密钥进行加密。BitLocker 使用以下身份验证方式：

- TPM。
- TPM 和 PIN。
- 密码。

在对驱动器进行加密前，BitLocker 会创建一个恢复密码。Kaspersky Industrial CyberSecurity for Nodes 会读取主密钥并将其发送到 Kaspersky Security Center，以便您可以恢复对磁盘的访问，例如，如果用户忘记了密码。

对系统硬盘驱动器进行加密后，用户需要通过 BitLocker 身份验证才能启动操作系统。经过身份验证程序后，BitLocker 将允许用户登录。BitLocker 不支持单点登录技术 (SSO)。

如果用户使用 BitLocker 对磁盘进行加密，Kaspersky Industrial CyberSecurity for Nodes 会将有关磁盘加密的信息发送到 Kaspersky Security Center。但是，Kaspersky Industrial CyberSecurity for Nodes 不会将恢复密码发送到 Kaspersky Security Center，因此将无法使用 Kaspersky Security Center 恢复对磁盘的访问。为使 BitLocker 与 Kaspersky Security Center 正常协同工作，请解密驱动器，然后使用策略重新对该驱动器进行加密。您可以在本地解密驱动器，也可以使用策略解密驱动器。

如果正在使用 Windows 组策略，请在策略设置中关闭 BitLocker 管理。Windows 策略设置可能与 Kaspersky Industrial CyberSecurity for Nodes 策略设置冲突。在对驱动器进行加密时，可能会发生错误。

启动 BitLocker 驱动器加密

在开始完整磁盘加密之前，建议您确保计算机未受到感染。若要执行操作，应启动全盘扫描或关键区域扫描任务。在已被 rootkit 感染的计算机上执行完整磁盘加密可能导致计算机无法运行。

若要在运行适用于服务器的 Windows 操作系统的计算机上使用 BitLocker 驱动器加密，可能需要安装“BitLocker 驱动器加密”组件。可使用操作系统工具（添加角色和组件向导）安装该组件。有关安装“BitLocker 驱动器加密”的更多信息，请参阅 Microsoft 文档。

如何在 Kaspersky Security Center 管理控制台中运行 BitLocker 驱动器加密

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 选择“**数据加密**”部分。
4. 在“**加密模式**”下拉列表中，选择“**加密所有硬盘驱动器**”。

   如果计算机安装了多个操作系统，在加密后，您将能够只加载执行了加密的操作系统。
5. 配置高级 BitLocker 驱动器加密选项（参见下表）。
6. 点击“**确定**”保存更改。

如何在 Kaspersky Security Center Web Console 中运行 BitLocker 驱动器加密

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**数据加密**区域。
5. 在“**完整磁盘加密**”子部分中单击“**配置**”按钮。
6. 在“**加密模式**”下拉列表中，选择“**加密所有硬盘驱动器**”。

   如果计算机安装了多个操作系统，在加密后，您将能够只加载执行了加密的操作系统。

7. 配置高级 BitLocker 驱动器加密选项（参见下表）。

8. 点击“**确定**”保存更改。

BitLocker 驱动器加密组件设置

参数	描述
启用需要在平板电脑上预启动键盘输入的 BitLocker 身份验证	使用在预启动环境中需要数据输入的身份验证，即使该平台没有能力进行预启动输入（例如使用平板电脑上的触摸屏键盘）。 平板电脑的触摸屏在预启动环境中不可用。例如，要在平板电脑上完成 BitLocker 身份验证，用户必须连接 USB 键盘。 如果选定该复选框，则允许使用需要预启动输入的身份验证。推荐在预启动环境中仅对拥有备用数据输入的设备（例如除了触摸屏键盘之外的 USB 键盘）使用该设置。 如果清除此复选框，则无法在平板电脑上使用 BitLocker 驱动器加密。
使用硬件加密(OS Windows 8 和后续版本)	如果选定该复选框，则应用程序将应用硬件加密。这可以提高加密速度并使用较少的计算机资源。
仅加密使用的磁盘空间(Windows 8 和后续版本)	该复选框可启用/禁用将加密区域仅限为已用硬盘驱动器扇区的选项。该限制可减少加密时间。 加密开始后启用或禁用**仅加密使用的磁盘空间(Windows 8 和后续版本)**功能在硬盘驱动器被加密之前并不修改该设置。开始加密之前您必须选择或清除该复选框。 如果选定该复选框，则仅加密使用的硬盘驱动器部分。Kaspersky Industrial CyberSecurity for Nodes 在添加新数据时自动加密这些数据。 如果清空该复选框，整个硬盘驱动器将被加密，包括先前删除和修改文件残留的碎片。 推荐对尚未修改或删除数据的新硬盘驱动器使用该选项。如果对已在使用中的硬盘驱动器应用加密，则推荐加密整个硬盘驱动器。这样可确保保护所有数据，甚至已删除的数据也能够部分恢复。 默认下，复选框被清除。
身份验证方法	**受信任平台模块 (TPM)** 如果选定该复选框，则 BitLocker 使用受信任平台模块 (TPM)。 受信任平台模块 (TPM) 是一个与安全相关的提供基本功能的微芯片（例如用于存储加密密钥）。受信任平台模块通常安装在计算机主板上并且通过硬件总线与其他所有系统组件进行互动。 对于运行 Windows 7 或 Windows Server 2008 R2 的计算机，只能使用 TPM 模块进行加密。如果未安装 TPM 模块，则无法进行 BitLocker 加密。不支持在这些计算机上使用密码。 配有受信任平台模块的设备可以创建只能使用该设备解密的加密密钥。受信任平台模块将使用其自有的根存储密钥加密加密密钥。根存储密钥存储在受信任平台模块中。这提供了防御黑客攻击加密密钥的附加保护。 默认情况下已选择此操作。 您可以为访问加密密钥设置额外的保护层，并使用密码或 PIN 加密密钥： “**为 TPM 使用 PIN**”。如果选中该复选框，用户可以使用 PIN 码获得对存储在受信任平台模块 (TPM) 中的加密密钥的访问权限。如果清除此复选框，则禁止用户使用 PIN 码。要访问加密密钥，用户必须输入密码。 **受信任平台模块 (TPM)，或密码(如果 TMP 不可用)** 如果选定该选项，当受信任平台模块 (TPM) 不可用时，用户可使用密码访问加密密钥。如果清除该复选框且 TPM 不可用，则将不会启动完整磁盘加密。 **仅密码(Windows 8 和后续版本)** 如果选定该选项，Kaspersky Endpoint Security 将在用户尝试访问加密磁盘时提示用户输入密码。 没有使用受信任平台模块 (TPM) 时可以选择该选项。 必须通过指定密码或 PIN 来配置所选的身份验证方法： • “**最小 PIN 码长度(字符数)**”。 • “**使用增强 PIN (字母和数字)**”。增强 PIN 允许使用数字字符以外的其他字符：大写和小写拉丁字母、特殊字符和空格。 • “**最小密码长度(字符数)**”。 • “**为 TPM 限制密码/PIN 有效期(天)**”。
自动重新创建恢复密钥(天)	自动更新密码以恢复对受 BitLocker 保护的驱动器的访问权限。如果选中该复选框，请指定恢复密钥密码的有效期。

您可以使用应用程序控制台控制用户计算机上的磁盘加密或解密过程。

应用策略后，根据身份验证设置，应用程序在小型诊断窗口或应用程序控制台中显示以下请求：

- 仅 TPM。不需要用户输入。磁盘将在计算机重启时被加密。
- TPM + PIN / 密码。如果 TPM 模块可用，将显示 PIN 码提示窗口。如果 TPM 模块不可用，您将看到一个用于预启动身份验证的密码提示窗口。
- 仅密码。您将看到预启动身份验证的密码提示窗口。

设置密码或 PIN 码后，BitLocker 会提示重新启动用户的计算机，以检查计算机与 BitLocker 的兼容性。Kaspersky Industrial CyberSecurity for Nodes 在小型诊断窗口或应用程序控制台中显示相应的通知。接下来，用户需要完成 BitLocker 身份验证过程。完成身份验证过程后，用户必须登录到系统。加载操作系统后，BitLocker 开始加密。

如果无法访问加密密钥, 用户可以请求局域网管理员提供恢复密钥（如果恢复密钥在较早前未保存在存储设备上或已丢失）。

解密受 BitLocker 保护的硬盘驱动器

用户可以使用操作系统解密磁盘（“*关闭 BitLocker*”功能）。此后，Kaspersky Industrial CyberSecurity for Nodes 提示重新加密磁盘。除非在策略中启用磁盘解密，否则 Kaspersky Industrial CyberSecurity for Nodes 将提示您加密磁盘。

如何使用 Kaspersky Security Center 管理控制台解密受 BitLocker 保护的硬盘驱动器

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 选择“**数据加密**”部分。
4. 在“**加密模式**”下拉列表中，选择“**解密所有硬盘驱动器**”。
5. 点击“**确定**”保存更改。

如何使用 Kaspersky Security Center Web Console 解密受 BitLocker 保护的硬盘驱动器

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**数据加密**区域。
5. 在“**完整磁盘加密**”子部分中单击“**配置**”按钮。

6. 在“**加密模式**”下拉列表中，选择“**解密所有硬盘驱动器**”。

7. 点击“**确定**”保存更改。

您可以使用应用程序控制台控制磁盘加密或解密过程。

恢复对 BitLocker 保护的驱动器的访问权限

如果用户忘记了由 BitLocker 加密的硬盘驱动器的访问密码，则需要启动恢复过程（请求-响应）。

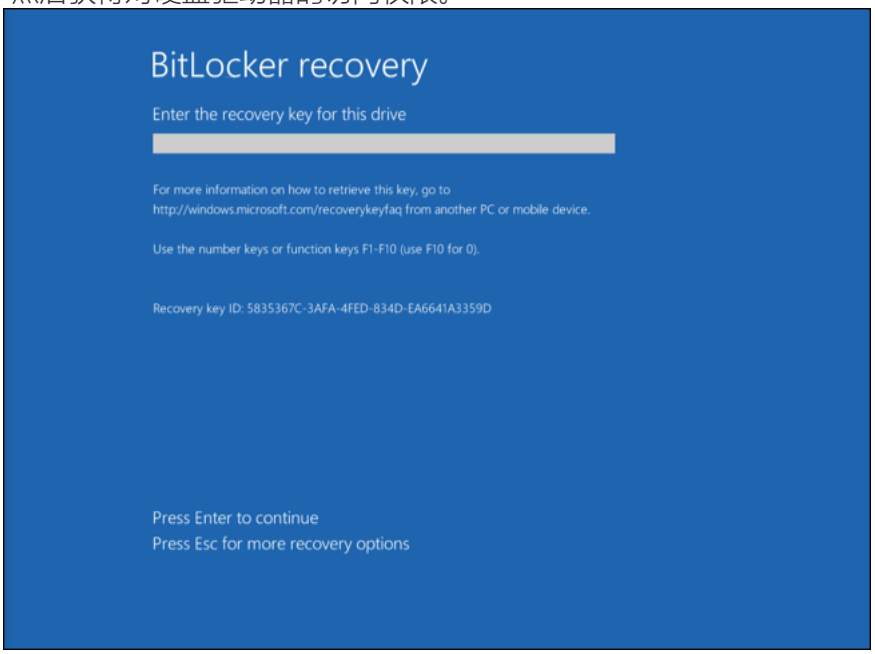
恢复对 BitLocker 加密的硬盘驱动器的访问权限包括以下步骤：

1. 用户告知管理员恢复密钥 ID（请参见下图）。

2. 管理员在 Kaspersky Security Center 中验证计算机属性中的恢复密钥 ID。用户提供的 ID 必须与计算机属性中显示的 ID 匹配。

   如果恢复密钥 ID 匹配，则管理员将恢复密钥移交给用户。

3. 用户输入恢复密钥，然后获得对硬盘驱动器的访问权限。



恢复对 BitLocker 加密的硬盘驱动器的访问权限

恢复对系统驱动器的访问权限

要启动恢复过程，用户需要在预引导身份验证阶段按 **Esc** 键。

如何在 Kaspersky Security Center 管理控制台中查看由 BitLocker 加密的系统驱动器的恢复密钥

1. 在 Kaspersky Security Center 管理控制台树中，选择“**受管理设备**”文件夹。

2. 转到“**设备**”选项卡。

3. 打开请求加密数据访问恢复的用户计算机的上下文菜单。

4. 在上下文菜单中，选择“**授予离线模式下的访问权限**”。

5. 向用户询问 BitLocker 密码输入窗口中指示的恢复密钥 ID，并将其与“**访问受 BitLocker 保护的系统驱动器**”选项卡上的“**恢复密钥 ID**”字段中的 ID 进行比较。

   如果 ID 不匹配，该密钥无法用于恢复指定系统驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

6. 向用户发送“**恢复密钥**”字段中指定的密钥。

如何在 Kaspersky Security Center Web Console 中查看由 BitLocker 加密的系统驱动器的恢复密钥

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

2. 选中要恢复其驱动器访问权限的计算机名称旁边的复选框。

3. 单击“**授予移动模式设备访问权限**”。

4. 验证恢复密钥 ID。用户提供的 ID 必须与计算机设置中显示的 ID 匹配。

   如果 ID 不匹配，该密钥无法用于恢复指定系统驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

5. 单击“**接收密钥**”。

6. 向用户发送“**恢复密钥**”字段中指定的密钥。

在操作系统锁定后，Kaspersky Industrial CyberSecurity for Nodes 提示用户更改密码或 PIN 码。在您设置了新密码或 PIN 码后，BitLocker 创建新的恢复密码，应用程序将其发送到 Kaspersky Security Center。

恢复对非系统驱动器的访问权限

要启动恢复过程，用户需要在提供驱动器访问的窗口中单击“**Forgot your password**”链接。获得对加密驱动器的访问权限后，用户可以在 BitLocker 设置中启用在 Windows 身份验证期间自动解锁驱动器。

如何在 Kaspersky Security Center 管理控制台中查看由 BitLocker 加密的非系统驱动器的恢复密钥

1. 在 Kaspersky Security Center 管理控制台树中，选择“**高级**” → “**数据加密和保护**” → “**加密驱动器**”文件夹。

2. 在工作区中，选择要为其创建访问密钥文件的加密设备，然后在该设备的上下文菜单中，单击“**获取 Kaspersky Industrial CyberSecurity for Nodes中的设备访问权限**”。

3. 提示用户在 BitLocker 密码输入窗口中输入恢复密钥 ID，然后在“**恢复密钥 ID**”字段中对比该 ID。

   如果 ID 不匹配，该密钥无法用于恢复指定驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

4. 向用户发送“**恢复密钥**”字段中指定的密钥。

如何在 Kaspersky Security Center Web Console 中查看由 BitLocker 加密的非系统驱动器的恢复密钥

1. 在 Web Console 的主窗口中，选择“**操作**” → “**数据加密和保护**” → “**加密驱动器**”。
2. 选中要恢复其驱动器访问权限的计算机名称旁边的复选框。
3. 单击“**授予移动模式设备访问权限**”。
   这将启动用于授予设备访问权限的向导。
4. 按照向导的说明授予对设备的访问权限：
   a. 选择 Kaspersky Industrial CyberSecurity for Nodes 插件。
   b. 验证恢复密钥 ID。用户提供的 ID 必须与计算机设置中显示的 ID 匹配。

      如果 ID 不匹配，该密钥无法用于恢复指定系统驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

   c. 单击“**接收密钥**”。
5. 向用户发送“**恢复密钥**”字段中指定的密钥。

暂停 BitLocker 保护以更新软件

在更新操作系统、安装操作系统更新包或在启用 BitLocker 保护的情况下更新其他软件时，有许多特殊注意事项。安装更新可能需要多次重新启动计算机。每次重新启动后，用户必须完成 BitLocker 身份验证。要确保更新安装正确，可以暂时关闭 BitLocker 身份验证。在这种情况下，磁盘保持加密状态，用户在登录系统后可以访问数据。要管理 BitLocker 身份验证，您可以使用 *BitLocker 保护管理*任务。您可以使用此任务指定不需要 BitLocker 身份验证的计算机重启次数。这样，在安装更新并完成“*BitLocker 保护管理*”任务后，BitLocker 身份验证将自动启用。您可以随时启用 BitLocker 身份验证。

如何在 Kaspersky Security Center 管理控制台中暂停 BitLocker 保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”文件夹。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Industrial CyberSecurity for Nodes → BitLocker 保护管理**”。

步骤2. BitLocker 保护管理

配置 BitLocker 身份验证。要暂停 BitLocker 保护，请选择“**临时允许跳过 BitLocker 身份验证**”，然后输入未经 BitLocker 身份验证的重新启动次数（1 到 15 次）。如有必要，请输入任务的到期日期和时间。在指定的时间，任务将自动关闭，并且用户必须在计算机重新启动时完成 BitLocker 身份验证。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 定义任务名称

输入任务的名称，例如*更新到 Windows 10*。

步骤 5. 完成任务创建

完成向导操作。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Kaspersky Security Center Web Console 中暂停 BitLocker 保护

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**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
2. 在“**任务类型**”下拉列表中，选择“**BitLocker 保护管理**”。
3. 在“**任务名称**”字段中，输入简要说明，例如，“*更新到 Windows 10*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。

步骤2. BitLocker 保护管理

配置 BitLocker 身份验证。要暂停 BitLocker 保护，请选择“**临时允许跳过 BitLocker 身份验证**”，然后输入未经 BitLocker 身份验证的重新启动次数（1 到 15 次）。如有必要，请输入任务的到期日期和时间。在指定的时间，任务将自动关闭，并且用户必须在计算机重新启动时完成 BitLocker 身份验证。

步骤 3. 完成任务创建

完成向导操作。在任务列表中将显示一个新任务。

要运行任务，请选中与任务对应的复选框，然后单击“**开始**”按钮。

因此，当任务运行时，在下次重新启动计算机后，BitLocker 不会提示用户进行身份验证。每次在没有 BitLocker 身份验证的情况下重新启动计算机后，Kaspersky Industrial CyberSecurity for Nodes 都会生成相应的事件并记录剩余的重新启动次数。

当达到指定的重新启动次数或任务到期时间时，BitLocker 身份验证将自动打开。要访问数据，用户必须完成 BitLocker 身份验证。

在运行 Windows 7 的计算机上，BitLocker 无法计算计算机重新启动的次数。Windows 7 计算机上的重新启动计数由 Kaspersky Industrial CyberSecurity for Nodes 处理。因此，要在每次重新启动后自动启用 BitLocker 身份验证，必须启动 Kaspersky Industrial CyberSecurity for Nodes。

要提前打开 BitLocker 身份验证，请打开“*BitLocker 保护管理*”任务属性，然后选择“**每次预启动时都请求身份验证**”。

Kaspersky Industrial CyberSecurity for Nodes 数据库和软件模块更新

本节包含有关 Kaspersky Industrial CyberSecurity for Nodes 更新的更新任务和回滚的信息，以及任务配置说明。

在美国境内，本软件中将不再提供更新功能（包括提供反病毒签名更新和代码库更新）。

更新数据库和应用程序模块

更新 Kaspersky Industrial CyberSecurity for Nodes 的数据库和程序模块可为您的计算机提供最新保护。新病毒和其他类型的恶意软件每天都在全世界出现。Kaspersky Industrial CyberSecurity for Nodes 数据库包含有关威胁的信息和使其失效的方法。要快速检测到威胁，建议您定期更新数据库和应用程序模块。

常规更新要求具有已生效的授权许可。如果当前没有授权许可，您将只能执行一次更新。

Kaspersky Industrial CyberSecurity for Nodes 会从 Kaspersky 的 HTTP 或 FTP 更新服务器、Kaspersky Security Center 管理服务器或其他更新源下载应用程序数据库和模块更新。

您可以将更新下载到每个受保护的设备，或使用一个受保护的设备作为中介。更新将被复制到其上，然后分发到受保护设备。如果使用 Kaspersky Security Center 集中管理组织的设备安全，可以利用管理服务器作为下载更新的代理。

如果更新下载过程中断或者产生错误，Kaspersky Industrial CyberSecurity for Nodes 将自动切换至使用上次更新的数据库。如果 Kaspersky Industrial CyberSecurity for Nodes 数据库损坏，可以手动回滚至先前安装的更新。

当执行更新时，以下对象将下载并安装到您的计算机中：

- Kaspersky Industrial CyberSecurity for Nodes 数据库。该程序使用包含病毒签名和其他威胁签名以及清除方法的数据库实现计算机保护。当搜索并为受感染文件清除时，保护组件将使用此信息。数据库将不断更新应对它们的方法和新威胁记录。因此，我们建议您定期更新数据库。

  除了 Kaspersky Industrial CyberSecurity for Nodes 数据库之外，系统也会更新已启用程序组件以拦截网络流量的网络驱动程序。

- 程序模块。除了 Kaspersky Industrial CyberSecurity for Nodes 数据库，您也可以更新程序模块。更新程序模块可以修补 Kaspersky Industrial CyberSecurity for Nodes 中的漏洞、添加新功能或增强现有功能。

更新时，您的计算机上的程序模块和数据库将与最新版本更新源进行对比。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计算机上。

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）。

有关 Kaspersky Industrial CyberSecurity for Nodes 数据库的当前状态的信息显示在主应用程序窗口中，或将光标悬停在通知区域中的应用程序图标上时看到的工具提示中。

有关更新任务运行期间更新结果和所有发生事件的信息将记录在更新任务日志中。

关于更新任务

Kaspersky Industrial CyberSecurity for Nodes 有两个更新任务：更新和更新回滚。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 每小时连接一次更新源。您可配置所有更新任务，除“更新回滚”任务外。修改了任务设置后，Kaspersky Industrial CyberSecurity for Nodes 会在下次启动任务时应用新值。

不允许暂停和恢复更新任务。

更新

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 会将数据库（以及应用程序模块）从更新源复制到设备，并在正在运行的“实时计算机保护”任务中立即开始使用它们。“按需扫描”任务在下次启动时开始使用更新的数据库。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 每小时运行一次“数据库更新”任务。

更新回滚

该任务使 Kaspersky Industrial CyberSecurity for Nodes 返回到以前的数据库和应用程序模块。

默认情况下，禁用“更新回滚”任务。

Kaspersky Industrial CyberSecurity for Nodes 数据库和模块更新方案

更新任务中更新源的选择取决于组织中使用的数据库和软件模块的更新方案。

您可以使用以下方案在受保护设备上更新 Kaspersky Industrial CyberSecurity for Nodes 数据库和模块：

- 直接通过互联网将更新下载到每个受保护设备（方案 1）。
- 通过互联网将更新下载到中间设备，然后再将更新从该设备分发到受保护设备。
  任何安装了以下应用程序的设备都可以充当中介：
  - Kaspersky Industrial CyberSecurity for Nodes（方案 2）。
  - Kaspersky Security Center 管理服务器（方案 3）。

  使用中间设备进行更新不仅可减少 Internet 流量，还提供了额外的网络受保护设备安全性。
- 通过安全可移动驱动器将数据库更新下载到每个受保护设备（方案 4）。

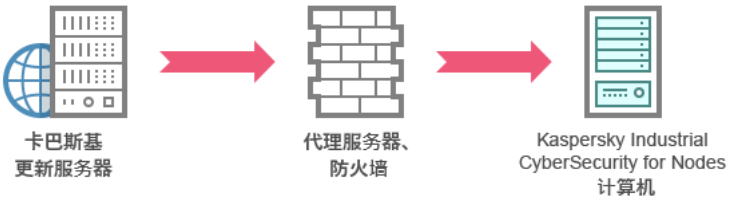
下面说明了列出的更新方案。

方案 1。直接从 Internet 更新数据库和模块

要配置直接通过互联网进行 Kaspersky Industrial CyberSecurity for Nodes 更新：

在每台受保护设备上，在“数据库更新”任务的设置中，将卡巴斯基更新服务器指定为更新源。

您可以将拥有更新文件夹的其他 HTTPS 或 HTTP 服务器配置为更新源。



方案 1：直接从 Internet 更新数据库和模块

方案 2。通过一个受保护设备更新数据库和模块

要配置通过一台受保护设备接收 Kaspersky Industrial CyberSecurity for Nodes 更新：

1. 将更新复制到选定的受保护设备。

   - 在选定受保护设备上配置“更新”任务设置：

     a. 指定 Kaspersky 的更新服务器作为更新源。

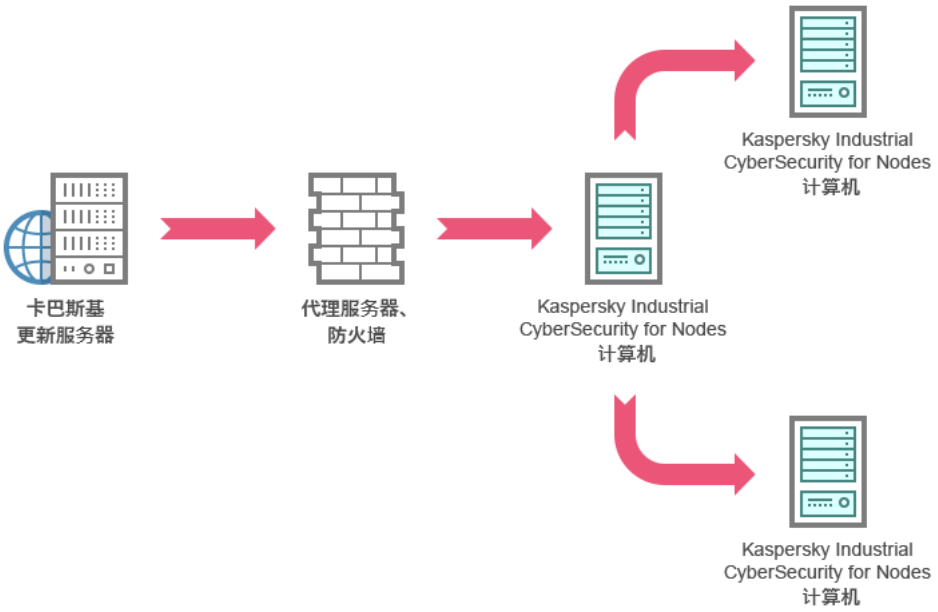
     b. 指定用作保存更新的文件夹的共享文件夹。

2. 将更新分发到其他受保护设备：

- 在每台受保护设备上配置更新任务：

  a. 对于更新源，在中间设备驱动器上指定一个用于保存下载的更新的文件夹。

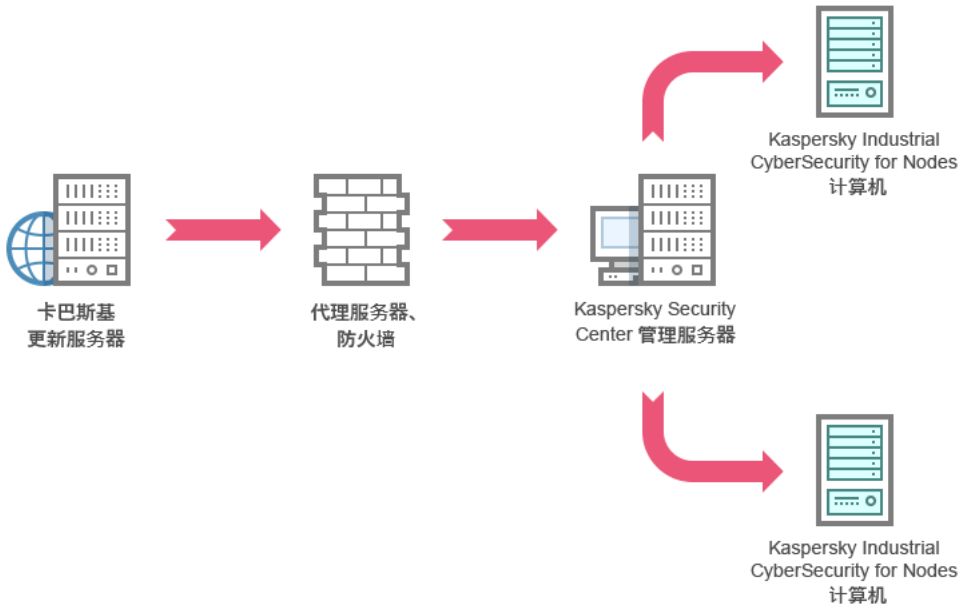
Kaspersky Industrial CyberSecurity for Nodes 将通过一个受保护设备获取更新。



方案 2：通过一个受保护设备更新数据库和模块

方案 3。通过 Kaspersky Security Center 管理服务器更新数据库和模块

如果使用 Kaspersky Security Center 集中管理设备的反病毒保护，则可以通过安装在局域网上的 Kaspersky Security Center 管理服务器下载更新。



方案 3：通过 Kaspersky Security Center 管理服务器更新数据库和模块

要配置通过 Kaspersky Security Center 管理服务器接收 Kaspersky Industrial CyberSecurity for Nodes 更新：

1. 在每个受保护设备上安装网络代理。网络代理是 Kaspersky Security Center 分发包中包含的软件组件。这可确保受保护设备上的管理服务器与 Kaspersky Industrial CyberSecurity for Nodes 进行互动。有关网络代理以及使用 Kaspersky Security Center 对其进行配置的详细信息，请参见 *Kaspersky Security Center 帮助*。
2. 将更新从 Kaspersky 更新服务器下载到 Kaspersky Security Center 管理服务器。
   - 为指定的一组受保护设备配置“按管理服务器检索更新”任务：
     a. 指定 Kaspersky 的更新服务器作为更新源。
3. 将更新分发到受保护设备。为此，请执行以下操作之一：
   - 在 Kaspersky Security Center 上，配置反病毒数据库（应用程序模块）更新组任务以将更新发布到受保护设备：
   - 在每台受保护设备上配置更新任务：
     a. 指定 Kaspersky Security Center 管理服务器作为更新源。
     b. 如有必要，配置任务计划。

Kaspersky Industrial CyberSecurity for Nodes 将通过 Kaspersky Security Center 管理服务器获取更新。

配置更新任务

如何在 Kaspersky Security Center 管理控制台中配置更新任务

1. 在 Kaspersky Security Center 管理控制台中，转到本地或要配置的组更新任务。
2. 打开“**设置**”部分。
3. 对于连接到 Kaspersky Security Center 管理服务器的 Kaspersky Industrial CyberSecurity for Nodes，在“**本地模式更新设置**”下，配置更新源：
   a. 单击“**设置**”。
   “**数据库和应用程序模块更新**”窗口将打开。
   b. 选中要使用的更新源旁边的复选框：
   - Kaspersky Security Center 管理服务器
   - 卡巴斯基更新服务器

   如有必要，请单击“**添加**”按钮添加自定义更新源。

c. 如果选择多个更新源，请使用“**向上**”和“**向下**”按钮按优先级对更新源进行排序。Kaspersky Industrial CyberSecurity for Nodes 严格按照配置的顺序访问更新源，并使用来自第一个可用更新源的更新包执行更新任务。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 使用 Kaspersky Security Center 服务器作为第一个更新源。这有助于在更新时节省流量。如果策略未应用到计算机，卡巴斯基服务器将被选为本地更新任务设置中的第一个更新源，因为应用程序可能无法访问 Kaspersky Security Center。

d. 如果您选择了“**卡巴斯基更新服务器**”作为更新源，选择 Kaspersky Industrial CyberSecurity for Nodes 在选择卡巴斯基更新服务器时必须遵循的原则：

- “**自动检测**”。应用程序使用最近可用的卡巴斯基更新服务器。
- “**从列表中选择**”。应用程序使用列表中所选国家/地区的卡巴斯基更新服务器。

e. 在“**数据库和应用程序模块更新**”窗口中单击“**确定**”按钮。

4. 配置应用程序数据库更新：

a. 选中或清除“**下载应用程序数据库更新**”复选框。

b. 选中或清除“**降低磁盘 I/O 的负载**”复选框。

c. 如果您选择了“**降低磁盘 I/O 的负载**”复选框，在“**用于优化的 RAM (MB)**”字段中，以兆字节为单位指定 RAM 数量。操作系统临时分配指定的 RAM 容量，用于在运行任务时存储更新文件。默认 RAM 大小为 640 MB。最小 RAM 大小为 400 MB。

在启用磁盘子系统优化功能的情况下运行更新任务时，可能会发生以下情况之一：

- 如果该值太小，则分配的 RAM 大小可能不足以完成数据库更新任务（例如，在第一次更新过程中），这将导致任务完成并出现错误。

  在这种情况下，建议为磁盘子系统优化功能分配更多 RAM。

- 如果该值太大，在启动数据库更新任务时，可能无法在 RAM 中创建选定大小的虚拟驱动器。结果，磁盘子系统优化功能将自动禁用，并且数据库更新任务将在没有优化功能的情况下运行。

  在这种情况下，建议为磁盘子系统优化功能分配更少 RAM。

5. 配置应用程序软件模块更新：

a. 选中或清除“**下载应用程序模块更新**”复选框。

b. 选择您要应用的应用程序模块更新类型。

- “**安装关键和批准的更新**”。如果选择此选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Industrial CyberSecurity for Nodes 才会自动安装关键更新和所有其他应用程序模块更新。
- “**仅安装批准的更新**”。如果选择该选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Industrial CyberSecurity for Nodes 才会安装它们。默认选中该选项。

如果应用程序模块更新需要查看和接受最终用户授权许可协议，应用程序将在最终用户授权许可协议被接受后，安装更新。

6. 配置将更新复制到本地存储的文件夹：

   a. 选中或清除“**将更新复制到本地存储文件夹**”复选框。

   b. 选择您希望应用程序复制到本地存储文件夹的更新内容：

      - “**复制数据库更新**”。应用程序仅下载数据库更新。
      - “**复制关键应用程序模块更新**”。应用程序仅下载关键的应用程序模块更新。
      - “**复制数据库更新和应用程序模块的关键更新**”。应用程序下载数据库更新和关键应用程序模块更新。

   c. 指定 Kaspersky Industrial CyberSecurity for Nodes 用来分发下载的更新的本地或网络文件夹。

7. 保存更改。

如何在应用程序控制台中配置更新任务

1. 在应用程序控制台树中，打开“**更新**” → “**数据库和应用程序模块更新**”节点。

2. 在结果窗格中单击“**属性**”链接。
   “**属性: 数据库和应用程序模块更新**”窗口将打开。

3. 对于连接到 Kaspersky Security Center 管理服务器的 Kaspersky Industrial CyberSecurity for Nodes，在“**本地模式更新设置**”下，配置更新源：

   a. 单击“**设置**”。
   “**数据库和应用程序模块更新**”窗口将打开。

   b. 选中要使用的更新源旁边的复选框：

      - Kaspersky Security Center 管理服务器
      - 卡巴斯基更新服务器

      如有必要，请单击“**添加**”按钮添加自定义更新源。

   c. 如果选择多个更新源，请使用“**向上**”和“**向下**”按钮按优先级对更新源进行排序。Kaspersky Industrial CyberSecurity for Nodes 严格按照配置的顺序访问更新源，并使用来自第一个可用更新源的更新包执行更新任务。
   默认情况下，Kaspersky Industrial CyberSecurity for Nodes 使用 Kaspersky Security Center 服务器作为第一个更新源。这有助于在更新时节省流量。如果策略未应用到计算机，卡巴斯基服务器将被选为本地更新任务设置中的第一个更新源，因为应用程序可能无法访问 Kaspersky Security Center。

d. 如果您选择了“**卡巴斯基更新服务器**”作为更新源，选择 Kaspersky Industrial CyberSecurity for Nodes 在选择卡巴斯基更新服务器时必须遵循的原则：

- “**自动检测**”。应用程序使用最近可用的卡巴斯基更新服务器。
- “**从列表中选择**”。应用程序使用列表中所选国家/地区的卡巴斯基更新服务器。

e. 在“**数据库和应用程序模块更新**”窗口中单击“**确定**”按钮。

4. 配置应用程序数据库更新：

a. 选中或清除“**下载应用程序数据库更新**”复选框。

b. 选中或清除“**降低磁盘 I/O 的负载**”复选框。

c. 如果您选择了“**降低磁盘 I/O 的负载**”复选框，在“**用于优化的 RAM (MB)**”字段中，以兆字节为单位指定 RAM 数量。操作系统临时分配指定的 RAM 容量，用于在运行任务时存储更新文件。默认 RAM 大小为 640 MB。最小 RAM 大小为 400 MB。

在启用磁盘子系统优化功能的情况下运行更新任务时，可能会发生以下情况之一：

- 如果该值太小，则分配的 RAM 大小可能不足以完成数据库更新任务（例如，在第一次更新过程中），这将导致任务完成并出现错误。

  在这种情况下，建议为磁盘子系统优化功能分配更多 RAM。

- 如果该值太大，在启动数据库更新任务时，可能无法在 RAM 中创建选定大小的虚拟驱动器。结果，磁盘子系统优化功能将自动禁用，并且数据库更新任务将在没有优化功能的情况下运行。

  在这种情况下，建议为磁盘子系统优化功能分配更少 RAM。

5. 配置应用程序软件模块更新：

a. 选中或清除“**下载应用程序模块更新**”复选框。

b. 选择您要应用的应用程序模块更新类型。

- “**安装关键和批准的更新**”。如果选择此选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Industrial CyberSecurity for Nodes 才会自动安装关键更新和所有其他应用程序模块更新。
- “**仅安装批准的更新**”。如果选择该选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Industrial CyberSecurity for Nodes 才会安装它们。默认选中该选项。

如果应用程序模块更新需要查看和接受最终用户授权许可协议，应用程序将在最终用户授权许可协议被接受后，安装更新。

6. 配置将更新复制到本地存储的文件夹：

   a. 选中或清除“**将更新复制到本地存储文件夹**”复选框。

   b. 选择您希望应用程序复制到本地存储文件夹的更新内容：

      - “**复制数据库更新**”。应用程序仅下载数据库更新。
      - “**复制关键应用程序模块更新**”。应用程序仅下载关键的应用程序模块更新。
      - “**复制数据库更新和应用程序模块的关键更新**”。应用程序下载数据库更新和关键应用程序模块更新。

   c. 指定 Kaspersky Industrial CyberSecurity for Nodes 用来分发下载的更新的本地或网络文件夹。

7. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置更新任务

1. 在 Web Console 中，转到您想要配置的本地或组更新任务。
2. 打开“**设置**”部分。
3. 选择“**本地模式**”选项卡用于配置连接到 Kaspersky Security Center 管理服务器的 Kaspersky Industrial CyberSecurity for Nodes 的更新任务。
4. 配置更新源：

   a. 在“**更新源**”，选中要使用的更新源旁边的复选框：

      - **Kaspersky Security Center 管理服务器**
      - **卡巴斯基更新服务器**

      如有必要，请单击“**添加**”按钮添加自定义更新源。

   b. 如果选择多个更新源，请使用“**向上**”和“**向下**”按钮按优先级对更新源进行排序。Kaspersky Industrial CyberSecurity for Nodes 严格按照配置的顺序访问更新源，并使用来自第一个可用更新源的更新包执行更新任务。

      默认情况下，Kaspersky Industrial CyberSecurity for Nodes 使用 Kaspersky Security Center 服务器作为第一个更新源。这有助于在更新时节省流量。如果策略未应用到计算机，卡巴斯基服务器将被选为本地更新任务设置中的第一个更新源，因为应用程序可能无法访问 Kaspersky Security Center。

5. 配置应用程序数据库更新：

   a. 选中或清除“**下载应用程序数据库更新**”复选框。

   b. 选中或清除“**降低磁盘 I/O 的负载**”复选框。

   c. 如果您选择了“**降低磁盘 I/O 的负载**”复选框，在“**用于优化的 RAM (MB)**”字段中，以兆字节为单位指定 RAM 数量。操作系统临时分配指定的 RAM 容量，用于在运行任务时存储更新文件。默认 RAM 大小为 640 MB。最小 RAM 大小为 400 MB。

在启用磁盘子系统优化功能的情况下运行更新任务时，可能会发生以下情况之一：

- 如果该值太小，则分配的 RAM 大小可能不足以完成数据库更新任务（例如，在第一次更新过程中），这将导致任务完成并出现错误。

  在这种情况下，建议为磁盘子系统优化功能分配更多 RAM。

- 如果该值太大，在启动数据库更新任务时，可能无法在 RAM 中创建选定大小的虚拟驱动器。结果，磁盘子系统优化功能将自动禁用，并且数据库更新任务将在没有优化功能的情况下运行。

  在这种情况下，建议为磁盘子系统优化功能分配更少 RAM。

6. 配置应用程序软件模块更新：

   a. 选中或清除“**下载应用程序模块更新**”复选框。

   b. 选择您要应用的应用程序模块更新类型。

   - “**安装关键和批准的更新**”。如果选择此选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Industrial CyberSecurity for Nodes 才会自动安装关键更新和所有其他应用程序模块更新。

   - “**仅安装批准的更新**”。如果选择该选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Industrial CyberSecurity for Nodes 才会安装它们。默认选中该选项。

   如果应用程序模块更新需要查看和接受最终用户授权许可协议，应用程序将在最终用户授权许可协议被接受后，安装更新。

7. 配置将更新复制到本地存储的文件夹：

   a. 选中或清除“**将更新复制到文件夹**”复选框。

   b. 选择您希望应用程序复制到本地存储文件夹的更新内容：

   - “**复制数据库更新**”。应用程序仅下载数据库更新。

   - “**复制关键应用程序模块更新**”。应用程序仅下载关键的应用程序模块更新。

   - “**复制数据库更新和应用程序模块的关键更新**”。应用程序下载数据库更新和关键应用程序模块更新。

   c. 指定 Kaspersky Industrial CyberSecurity for Nodes 用来分发下载的更新的本地或网络文件夹。

8. 保存更改。

应用程序的 SMU 更新

要使用卡巴斯基更新服务更新应用程序（Seamless Update；SMU），与其他更新方法不同，您无需运行安装程序。Kaspersky Industrial CyberSecurity for Nodes 获得了新版本的应用程序以及来自同一源的反病毒数据库。

SMU 更新允许将您组织的所有计算机上的应用程序更新到最新版本。在应用 SMU 更新之前，我们建议在几台计算机上测试应用程序的新版本。为此，您必须手动更新这些计算机上的应用程序（例如，在本地使用安装向导）。执行 SMU 更新时，您无法选择单个计算机。

应用程序的更新计划由卡巴斯基工作人员决定。为了确保新版本的应用程序顺利运行，卡巴斯基会逐步提供更新。这意味着您可能会在新版本发布后最多两个月内获得 SMU 更新。

您可以使用“*数据库和应用程序模块更新*”任务管理应用程序的 SMU 更新。要将应用程序的新版本包含在与反病毒数据库相同的软件包中，您必须在“*数据库和应用程序模块更新*”任务设置中允许更新*应用程序模块*。

应用程序 SMU 更新的步骤

1. **在应用程序的新版本被发布或模块被更新后，卡巴斯基会分发更新。**
2. **用户批准应用程序的更新。**

   如果计算机已连接到 Kaspersky Security Center，则可以在 Kaspersky Security Center 的“**卡巴斯基数据库和软件模块更新**”部分获取更新。有关批准更新的详细信息，请参阅 Kaspersky Security Center 帮助。

   如果计算机未连接到 Kaspersky Security Center，则可以在应用控制台获取更新。要批准更新，请转到“**更新** → **应用程序更新**”部分，选择应用程序版本，如有必要，接受协议的条款和条件。
3. **Kaspersky Industrial CyberSecurity for Nodes 按计划运行“数据库和应用程序模块更新”任务。**

结果，Kaspersky Industrial CyberSecurity for Nodes 将在“静默”模式下更新应用程序。

回滚 Kaspersky Industrial CyberSecurity for Nodes 数据库更新

在执行数据库更新之前，Kaspersky Industrial CyberSecurity for Nodes 会创建先前使用的数据库的备份副本。如果更新中断或产生错误，Kaspersky Industrial CyberSecurity for Nodes 将自动恢复为使用之前安装的数据库。

如果在您已更新数据库后出现任何问题，则可通过“*上次更新回滚*”任务将数据库回滚到之前安装的更新。

要运行“上次更新回滚”任务：

1. 在应用程序控制台树中，打开“**更新**” → “**上次更新回滚**”部分。
2. 在结果窗格中，单击“**启动**”链接。

更新任务统计

更新任务运行时，将显示自任务启动以来下载的数据量的实时信息，以及其他任务执行统计信息。

任务完成或停止后，该信息可以在任务日志中查看。

要查看“更新”任务统计信息：

在应用程序控制台树中，打开“**更新**” → “**数据库和应用程序模块更新**”部分。

结果面板，在“**统计信息**”下，您可以查找到所获取数据总量的信息。

Detection and Response 解决方案

Kaspersky Detection and Response 解决方案是用于检测组织基础设施不同级别的高级威胁和攻击指标的安全系统。Detection and Response 解决方案提供有关检测到的威胁的信息，并允许管理威胁响应操作。

因此，Detection and Response 解决方案执行以下操作：

- 接收有关计算机、服务器或其他设备（遥测）操作的信息。
- 自动分析信息以检测威胁。
- 生成警报详细信息作为威胁发展链的列，以供分析和选择威胁响应操作。
- 执行威胁响应操作（例如，计算机的网络隔离）。

Kaspersky Industrial CyberSecurity for Nodes 使用内置代理支持 Detection and Response 解决方案。内置代理将遥测数据发送到解决方案的服务器并执行威胁响应操作。内置代理支持：

- Kaspersky Endpoint Detection and Response Optimum 2.0 版及更高版本（EDR Optimum）
- Kaspersky Anti Targeted Attack Platform (仅遥测)

您可以在各种配置中使用 Kaspersky Industrial CyberSecurity for Nodes 和 Detection and Response 解决方案，例如，[EDR Optimum+MDR]。

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent 支持在应用程序与其他卡巴斯基解决方案之间进行交互以检测高级威胁（例如，Kaspersky Sandbox）。卡巴斯基解决方案与特定版本的 Kaspersky Endpoint Agent 兼容。

> 要使用 Kaspersky Endpoint Agent 作为卡巴斯基解决方案的一部分，您必须使用对应的授权许可密钥激活这些解决方案。

Kaspersky Endpoint Agent 支持与以下卡巴斯基解决方案交互，以检测复杂威胁（例如针对性攻击）：

- Kaspersky Endpoint Detection and Response Optimum（支持 Kaspersky Endpoint Agent 3.9 及更高版本）
- Kaspersky Anti Targeted Attack Platform（支持 Kaspersky Endpoint Agent 3.8 及更高版本）
- Kaspersky Sandbox（支持 Kaspersky Endpoint Agent 3.7 及更高版本。）
- Kaspersky Managed Detection and Response。

Kaspersky Industrial CyberSecurity for Nodes 4.0 分发套件包括 Kaspersky Endpoint Agent 应用程序；对于早期版本，您可以向技术客户经理 (TAM) 请求 Kaspersky Endpoint Agent 分发套件。从 4.5 版本开始，Kaspersky Industrial CyberSecurity for Nodes 分发套件不包含 Kaspersky Endpoint Agent 分发套件。Kaspersky Industrial CyberSecurity for Nodes 4.5 包含内置代理，应用程序使用该代理支持与 Detection and Response 解决方案的集成。您不能在同一台计算机上安装这两个应用程序。

迁移 [KICS+KEA] 配置到 [KICS+内置代理] 配置

从 4.5 版开始，Kaspersky Industrial CyberSecurity for Nodes 包含内置 *端点代理* 代理（以下也称为“内置代理”）来支持 Detection and Response 解决方案。使用这些解决方案您不再需要单独的 Kaspersky Endpoint Agent 应用程序。当您在安装了 Kaspersky Endpoint Agent 的计算机上部署 Kaspersky Industrial CyberSecurity for Nodes 时，Detection and Response 解决方案将继续与 Kaspersky Industrial CyberSecurity for Nodes 协同工作，并且 Kaspersky Endpoint Agent 应用程序将从计算机中删除。

迁移 [KICS+KEA] 配置到 [KICS+内置代理] 需要以下步骤：

1. **升级 Kaspersky Security Center**

   将所有 Kaspersky Security Center 组件升级到版本 14.2 或更高版本，包括用户计算机上的网络代理。

2. **安装/升级 Kaspersky Industrial CyberSecurity for Nodes 至版本 4.5**

   如果您正在安装该应用程序，则在安装包设置或在安装向导的其他必需组件中，选择“**完整功能 → 端点代理**”。

   如果您更新应用程序，Kaspersky Industrial CyberSecurity for Nodes 支持在安装了 Kaspersky Endpoint Agent 的计算机上自动选择组件。组件的自动选择取决于升级应用程序的用户账户的权限。

   如果您在系统账户（SYSTEM）下使用 EXE 或 MSI 文件升级 Kaspersky Industrial CyberSecurity for Nodes，Kaspersky Industrial CyberSecurity for Nodes 获得对卡巴斯基解决方案的当前授权许可的访问权。因此，如果计算机安装了 Kaspersky Endpoint Agent，并且激活了 EDR Optimum 解决方案，则 Kaspersky Industrial CyberSecurity for Nodes 安装程序将自动配置组件集并选择 EDR Optimum 组件。这将使 Kaspersky Industrial CyberSecurity for Nodes 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。在系统账户(SYSTEM)下运行 MSI 安装程序通常在通过 Kaspersky 更新服务(SMU)升级时执行，或者当通过 Kaspersky Security Center 部署安装包时。

   如果您在非特权用户账户下使用 MSI 文件升级 Kaspersky Industrial CyberSecurity for Nodes，Kaspersky Industrial CyberSecurity for Nodes 缺少对卡巴斯基解决方案的当前授权许可的访问权。这种情况下，Kaspersky Industrial CyberSecurity for Nodes 基于 Kaspersky Endpoint Agent 配置自动选择组件。此后，Kaspersky Industrial CyberSecurity for Nodes 将切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

3. **授权许可功能**

   如果您使用通用 Kaspersky Endpoint Detection and Response Optimum 授权许可激活 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Endpoint Agent，EDR Optimum 功能将在升级应用程序到版本 4.5 后被自动激活。您不需要做任务其他事情。

   如果您使用独立 Kaspersky EDR Optimum 加载项授权许可激活 EDR Optimum 功能，您必须确保 EDR Optimum 加载项密钥已添加到 Kaspersky Security Center 存储库且授权许可密钥自动分发功能已启用。在您升级应用程序到版本 4.5 后，EDR Optimum 功能被自动激活。

   如果您使用 Kaspersky Endpoint Detection and Response Optimum 授权许可激活 Kaspersky Endpoint Agent，并使用其他授权许可激活 Kaspersky Industrial CyberSecurity for Nodes，您必须使用通用 Kaspersky Endpoint Detection and Response Optimum 密钥替换 Kaspersky Industrial CyberSecurity for Nodes 密钥。您可以使用“*添加密钥*”任务替换密钥。

4. **升级 Kaspersky Industrial CyberSecurity for Nodes Web 插件**

   在 Kaspersky Security Center Web Console 中，将 Kaspersky Industrial CyberSecurity for Nodes Web 插件升级到版本 4.5。

5. **迁移策略和任务**

   使用策略和任务迁移向导将 Kaspersky Endpoint Agent 设置迁移到 Kaspersky Industrial CyberSecurity for Nodes。

将 [KICS+KEA] 配置的策略和任务迁移到 [KICS+内置代理] 配置

您可以使用 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Endpoint Agent 4.0 或更早版本至带有内置代理的 Kaspersky Industrial CyberSecurity for Nodes 4.5 的策略和任务迁移向导来迁移以下解决方案的策略和任务设置：

- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform (EDR)。

策略和任务迁移向导仅在 Web Console 和云控制台中可用。

我们建议首先在一台计算机上将 [KICS+KEA] 配置的策略和任务迁移到 [KICS+内置代理]，然后在一组计算机上进行，然后在组织的所有计算机上完成迁移。

要将 [KICS+KEA] 配置的策略和任务迁移到 [KICS+内置代理] 配置：

在 Web Console 或云控制台的主窗口中，选择“**操作 → 迁移到 Kaspersky Industrial CyberSecurity for Nodes 4.5.0**”。

这将运行策略和任务迁移向导。按照向导的说明进行操作。

步骤 1. 策略迁移

选择要合并其设置的 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Endpoint Agent 策略。

确保选择了正确的策略，然后转到下一步。

步骤 2. 任务迁移

在任务列表中，选择要为 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建的 Kaspersky Industrial CyberSecurity for Nodes 任务。

转到下一步。

步骤 3. 向导完成

完成向导操作。因此，向导会执行以下操作：

- 针对 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建了新策略。

  这些策略结合了 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Endpoint Agent 的先前版本的设置。新策略的名称与合并前的 Kaspersky Industrial CyberSecurity for Nodes 策略的名称相同，并添加了“从 KICS 复制”短语。新策略具有“*不活动*”状态。要应用新的合并策略，请使其活动。

当从 Kaspersky Endpoint Agent 迁移到 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案的 Kaspersky Industrial CyberSecurity for Nodes 时，您将计算机连接到 KATA 服务器时可能会遇到错误。原因是迁移向导跳过了以下策略设置并且不迁移它们：

- 禁止修改设置“**KATA 服务器连接设置**”（“挂锁”）。

  默认情况下，允许修改设置（“挂锁”打开）。因此，这些设置不会应用到计算机上。您必须禁止设置修改并关闭“挂锁”。

- 加密容器。

  如果您使用双向身份验证连接到 KATA 服务器，则必须重新添加加密容器。迁移向导正确迁移了服务器的 TLS 证书。

- 为 Kaspersky Industrial CyberSecurity for Nodes 4.5 创建新的任务。

  新任务包含迁移的 Kaspersky Industrial CyberSecurity for Nodes 任务的设置以及 Kaspersky Industrial CyberSecurity for Nodes 4.5 中引入的新设置。新任务的名称与迁移前的 Kaspersky Industrial CyberSecurity for Nodes 任务名称相同，并添加了“从 KICS 复制”短语。

端点代理配置

Kaspersky Industrial CyberSecurity for Nodes 可以安装在 端点代理 配置下（以下也称为“端点代理配置”）。Endpoint Agent 配置持续监控计算机上运行的进程、打开的网络连接以及正在修改的文件。Kaspersky Industrial CyberSecurity for Nodes 保护组件不可用。Endpoint Agent 配置与第三方 EPP 应用程序兼容。您可以将第三方基础设施安全工具与 Kaspersky Detection and Response 解决方案一起使用。

Endpoint Agent 配置安装在企业 IT 基础设施的各个工作站和服务器上，以支持以下卡巴斯基解决方案：

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform

此外，Endpoint Agent 配置包括与 Kaspersky Industrial CyberSecurity for Networks 应用程序集成和使用 Sigma 规则进行异常检测功能。

安装端点代理配置

Endpoint Agent 配置的安装过程与安装 Kaspersky Industrial CyberSecurity for Nodes 相同；在安装包设置或安装向导中，在应用程序组件选择步骤中选择 端点代理。

在 Endpoint Agent 配置中安装 Kaspersky Industrial CyberSecurity for Nodes 后，应用程序控制台将可用，并且系统托盘中将显示应用程序图标 。

在 Kaspersky Security Center 管理控制台中，在 Endpoint Agent 配置中安装了应用程序的计算机具有“*严重*”状态：。计算机出现此状态是因为缺少实时文件保护组件。您无需执行任何操作。

如果由于安装程序在计算机上发现不兼容的软件而无法在具有第三方 EPP 应用程序的计算机上安装 Endpoint Agent 配置，您可以使用 SKIPINCOMPATIBLESW 选项跳过不兼容软件检查。

与第三方 EPP 应用程序的兼容性

端点代理配置用于 Kaspersky Detection and Response 解决方案。保护和控制组件不可用于 Endpoint Agent 配置。此配置允许安装第三方 EPP 应用程序并在组织的基础设施中部署 Kaspersky Detection and Response 解决方案。Endpoint Agent 支持 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform。

Endpoint Agent 配置与以下供应商的 EPP 应用程序兼容：

- **Bitdefender**

  Bitdefender Endpoint Security Tools 版本 7.9.21.523 或更高版本。

- **Dallas Lock**

  Dallas Lock 8.0-C 版本 11.4.2.843 或更高版本。

- **ESET**

  ESET Endpoint Security 版本 12.0.2049.0 或更高版本以及 ESET Management Agent 版本 12.0 或更高版本。

- **Secret Net Studio**

  Secret Net Studio 版本 8.11 或更高版本。

  > 应用程序无法安装在部署了带有反病毒组件的 Secret Net Studio 的计算机上。要实现互操作性，您必须从 Secret Net Studio 中删除反病毒组件。

- **Sophos**

  Sophos Intercept X 版本 2024.1.2 或更高版本（包括 Endpoint Agent）以及 Sophos Core Agent 版本 2024.3.2.3。

- **Trend Micro**

  Trend Micro Apex One 版本 14.0.12994 或更高版本（包括 Security Agent）。

  Trend Micro Deep Security 版本 20.0.2-4960 或更高版本。

- **Windows 防火墙**

必须按以下顺序安装应用程序：首先安装 EPP 应用程序，然后安装 Kaspersky Security Center 网络代理，最后安装 Endpoint Agent 配置。这是必要的，因为 EPP 应用程序的安装程序可能会将 Endpoint Agent 配置和网络代理检测为不兼容的软件并将其删除。更新第三方 EPP 应用程序后，还应检查 Endpoint Agent 配置和网络代理的运行情况，因为其安装程序可能会重新扫描计算机中是否有不兼容的软件并删除这些应用程序。

Managed Detection and Response

Kaspersky Industrial CyberSecurity for Nodes 支持与 Managed Detection and Response 解决方案集成。

Kaspersky Managed Detection and Response（也称为 MDR）为那些难以找到专业知识和员工或内部资源有限的组织提供全天候保护，抵御日益增多的绕过自动安全屏障的威胁。与市场上的同类产品不同，该服务利用有效的针对性攻击研究经验，确保持续防御最复杂的威胁。该服务有助于提高您的企业应对网络威胁的能力，同时释放您现有的资源以将注意力集中在其他任务上。

MDR 使用从端点和机器学习接收的遥测数据。MDR 发送事故数据到 Kaspersky 专家。然后专家便可以处理事故，例如，添加新条目到反病毒数据库。或者，专家可以发布处理事件的建议，例如，建议将计算机从网络隔离。对于该解决方案如何工作的详情，请参考 Kaspersky Managed Detection and Response 帮助。

Kaspersky Industrial CyberSecurity for Nodes 与 MDR 集成的配置

以下配置可用于与 MDR 配合使用：

- **[KICS+内置代理]**。在此配置中，Kaspersky Industrial CyberSecurity for Nodes 既充当确保计算机安全的应用程序，又充当使用 MDR 的应用程序。从 4.5 版开始，Kaspersky Industrial CyberSecurity for Nodes 中就有内置代理。
- **[第三方 EPP+端点代理配置]**。在此配置中，IT 基础设施的安全性由第三方端点保护平台（EPP）提供。Kaspersky Industrial CyberSecurity for Nodes 在端点代理配置中提供了与 MDR 的集成。从 4.5 版开始，Kaspersky Industrial CyberSecurity for Nodes 中提供了端点代理配置。

配置 MDR 集成

Kaspersky Managed Detection and Response 需要启用卡巴斯基安全网络组件的扩展模式。否则，Kaspersky Managed Detection and Response 将无法收到正常运行所需的遥测数据。

为了 Kaspersky Managed Detection and Response 通过 Kaspersky Security Center Web Console 与管理服务器协作，您还必须建立新的安全连接，一个*后台连接*。Kaspersky Managed Detection and Response 在您部署解决方案时提示您建立后台连接。确保后台连接已建立。

如何在 Kaspersky Security Center Web Console 中建立后台连接

1. 在 Web Console 的主窗口中，选择“**设置**” → “**整合**”。
2. 转到**整合**区域。
3. 开启 **用于整合的后台连接 已启用** 切换开关。
4. 保存更改。

与 Kaspersky Managed Detection and Response 的整合包括以下步骤：

1. **安装“Managed Detection and Response (Industrial CyberSecurity)”组件**

为了将 Kaspersky Industrial CyberSecurity for Nodes 与 Managed Detection and Response 解决方案集成，将使用 Managed Detection and Response (Industrial CyberSecurity) 组件。要安装此组件，在安装包设置或安装向导中，或通过在 Windows 控制面板中更改应用程序组件集，在必须选择要安装的应用程序组件的步骤中，选择以下内容：

- **完整功能 → 端点代理 → Managed Detection and Response (Industrial CyberSecurity)**，对于内置代理
- **端点代理 → Managed Detection and Response (Industrial CyberSecurity)**，对于端点代理配置

2 配置卡巴斯基私有安全网络

从 2025 年 7 月的更新开始，Managed Detection and Response 解决方案支持在没有 KPSN 配置文件的情况下运行。对于 MDR 解决方案如何使用卡巴斯基安全网络的详情，请参考 Kaspersky Managed Detection and Response 帮助。

如果您的配置不符合在没有 KPSN 配置文件的情况下运行的要求，请在管理服务器属性中上传 KPSN 配置文件。KPSN 配置文件存在于 MDR 配置文件的 ZIP 存档中。您也可以**使用命令行上传 KPSN 配置文件**。

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，cmd.exe）。
2. 使用 `cd` 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如，`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0` 并按 **ENTER**。

   您还可以在应用程序安装阶段将可执行文件路径添加到 %PATH% 系统变量，并在不导航到应用程序文件夹的情况下运行命令。
3. 运行以下命令：

   `KAVSHELL KSN [/global] [/private <私有 KSN 配置文件的完整路径>] [/login=<当前用户账户的名称>] [/pwd=</login 密码或 KLAdmin 密码（如果未指定 /login）>]`

   例如：

   `KAVSHELL KSN /private C:\kpsn_config.pkcs7`

对于配置卡巴斯基私有安全网络的详情，请参考 Kaspersky Security Center 帮助。

3 激活 Kaspersky Managed Detection and Response

将早期版本的 Kaspersky Industrial CyberSecurity for Nodes 更新到 4.5 或更高版本时，之前使用 MDR 配置文件（BLOB 文件）激活的 Managed Detection and Response 解决方案将不会自动激活。您需要使用密钥文件或激活码重新激活 Managed Detection and Response 解决方案。

要激活 Kaspersky Industrial CyberSecurity for Nodes 中的 Managed Detection and Response 解决方案，您需要单独的 Kaspersky Managed Detection and Response for Industrial CyberSecurity 插件的授权许可。

从 4.5 版本开始， Kaspersky Industrial CyberSecurity for Nodes 不再支持仅使用 MDR 配置文件（BLOB 文件）激活 Managed Detection and Response 解决方案。

如果您使用的是 MDR 租户，则即使 BLOB 文件已过期，您也需要在应用激活码之前上传租户的 BLOB 文件。

如果您未使用且从未创建过 MDR 租户，则无需上传 BLOB 文件。

对于激活解决方案的详情，请参考 Kaspersky Managed Detection and Response 帮助。

4 启用 Managed Detection and Response (Industrial CyberSecurity) 组件

如何在 Kaspersky Security Center 管理控制台中启用 Managed Detection and Response 组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 选择“**遥测采集服务器**”部分。
4. 在“**Managed Detection and Response (Industrial CyberSecurity)**”块中单击“**设置**”按钮。
   “**Managed Detection and Response (Industrial CyberSecurity)**”窗口将打开。
5. 选择**Managed Detection and Response**复选框。
6. 如有必要，请点击“**上传**”按钮上传 MDR 配置文件。对于 MDR 配置文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

   通过上传 Managed Detection and Response 配置文件，您同意自动将指定数据从预装 Kaspersky Industrial CyberSecurity for Nodes 的设备传输到卡巴斯基进行处理。如果您不想处理指定的信息，请不要上传配置文件。

7. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用 Managed Detection and Response 组件

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**遥测采集服务器**”部分。
5. 在“**Managed Detection and Response (Industrial CyberSecurity)**”块中单击“**设置**”按钮。
   “**Managed Detection and Response (Industrial CyberSecurity)**”窗口将打开。
6. 选择**Managed Detection and Response (Industrial CyberSecurity) 已禁用**复选框。
7. 如有必要，请点击“**上传**”按钮上传 MDR 配置文件。对于 MDR 配置文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

   通过上传 Managed Detection and Response 配置文件，您同意自动将指定数据从预装 Kaspersky Industrial CyberSecurity for Nodes 的设备传输到卡巴斯基进行处理。如果您不想处理指定的信息，请不要上传配置文件。

8. 保存更改。

如何在应用程序控制台中启用 Managed Detection and Response 组件

1. 在应用程序控制台树中，选择“**遥测采集服务器** → **Managed Detection and Response (Industrial CyberSecurity)**”部分。
2. 在结果窗格中单击“**属性**”链接。

   将打开“**Managed Detection and Response (Industrial CyberSecurity)**”窗口的“**常规**”选项卡。
3. 选择**Managed Detection and Response**复选框。
4. 如有必要，请点击“**上传**”按钮上传 MDR 配置文件。对于 MDR 配置文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

   通过上传 Managed Detection and Response 配置文件，您同意自动将指定数据从预装 Kaspersky Industrial CyberSecurity for Nodes 的设备传输到卡巴斯基进行处理。如果您不想处理指定的信息，请不要上传配置文件。
5. 保存更改。

如何从命令行启用 Managed Detection and Response 组件

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，cmd.exe）。
2. 使用 `cd` 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如，`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.5.0.0` 并按 **ENTER**。

   您还可以在应用程序安装阶段将可执行文件路径添加到 %PATH% 系统变量，并在不导航到应用程序文件夹的情况下运行命令。
3. 运行以下命令：

   `KAVSHELL MDR /<enable|disable|show> /BLOB:<MDR 配置文件的完整路径> [/login:<当前用户账户的名称>] [/pwd:</login 密码或 KLAdmin 密码（如果未指定 /login）>]`

启用 Managed Detection and Response 的命令参数

参数	描述
`MDR /<enable|disable|show>`	必需参数。 允许启用、禁用和查看 Managed Detection and Response 的状态
`/BLOB:<MDR 配置文件的完整路径>`	必需参数。 允许您指定 MDR 配置文件的路径。
`/LOGIN=<用户账户名称>`	可选参数。 允许您指定具有足够权限的用户账户名。 如果未指定此选项，应用程序将在下一行提示您输入用户名。 如果您输入了 KLAdmin 密码，则无需输入此值。
`/PWD=</login 密码或 KLAdmin 密码（如果未指定 /login）>`	允许您指定 KLAdmin 用户账户或具有足够权限的用户账户的密码。 如果未指定此选项，应用程序将在下一行提示您输入密码。

Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum（以下也称为 EDR Optimum）是一种旨在保护组织的 IT 基础设施免受复杂网络威胁的解决方案。该解决方案的功能将自动威胁检测与应对这些威胁的能力相结合，以抵御复杂的攻击，包括新的漏洞、勒索软件、无文件攻击以及使用合法系统工具的方法。有关该解决方案的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

Kaspersky Industrial CyberSecurity for Nodes 4.5 引入内置代理，作为 EDR Optimum 解决方案 2.0 及更高版本的一部分工作。

解决方案架构

该解决方案由以下组件组成：

- Kaspersky Industrial CyberSecurity for Nodes 安装在运行 Microsoft Windows 操作系统的企业 IT 基础设施中的各个设备上。应用程序不断监控这些设备上运行的进程，以及开放的网络连接和文件修改。
- Kaspersky Security Center 与 Kaspersky Security Center Web Console 允许集中管理解决方案及其设置。

解决方案的工作原理

EDR Optimum 查看和分析威胁发展，并向*安全官*或*管理员*提供及时响应所需的潜在攻击信息。EDR Optimum 在单独的窗口中显示警报详细信息。*警报*是企业 IT 基础设施中发生的事件，应用程序将其识别为异常或可疑，并可能对企业 IT 基础设施构成安全威胁。

*警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。

该解决方案使用以下威胁情报工具来分析威胁：

- 卡巴斯基安全网络 (KSN) 云服务基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件、网页资源和软件的信誉信息。使用卡巴斯基安全网络的数据可确保卡巴斯基应用程序对威胁做出更快响应，提高一些保护组件的性能，并降低误报可能性。
- 与卡巴斯基私人安全网络（以下也称为 KPSN）集成，允许用户访问 KSN 信誉数据库以及其他统计数据，而无需从他们的计算机向 KSN 提交数据。
- 与卡巴斯基威胁情报门户信息系统集成，该系统包含并显示有关文件和网址信誉的信息。
- 卡巴斯基威胁数据库。

威胁响应

威胁响应功能提供了应用程序在检测到威胁时执行的以下自动操作：

- 隔离对象。
- 删除文件。

- 将设备与网络隔离。
- 在设备上运行关键区域扫描。
- 开始搜索一组设备的入侵指标（IOC 扫描）。

此外，安全官或管理员可以执行以下操作：

- 将对象放入执行防护列表中。
- 在设备上启动进程。
- 在设备上终止进程。

如果您正在使用该应用程序 4.5 或更高版本作为 EDR Optimum 解决方案的一部分，为了管理警报详细信息，您必须将 Endpoint Detection and Response 的 Web 插件升级到 15.1 或更高版本。否则，如果您安装了 Kaspersky Endpoint Agent Web 插件，使用此 Web 插件打开的事故卡中的威胁发展链可能包含有限的数据或错误。

Kaspersky Industrial CyberSecurity for Nodes 4.5 版的功能

作为 EDR Optimum 解决方案的一部分，Kaspersky Industrial CyberSecurity 执行以下操作：

- 收集有关警报的信息。
- 利用检测数据补充判决信息。
- 将数据发送到 Kaspersky Security Center 以生成警报详细信息。
- 在受保护设备组上启动 IOC 扫描任务（搜索入侵指标）。
- 处理检测到的入侵指标，例如：
  - 实现设备的网络隔离；
  - 启动设备上的关键区域扫描。

对以前版本的 Kaspersky Industrial CyberSecurity for Nodes 的支持

如果您使用 Kaspersky Industrial CyberSecurity for Nodes 4.5 之前的版本与 EDR Optimum 进行交互，则必须安装 Kaspersky Endpoint Agent。Kaspersky Industrial CyberSecurity for Nodes 4.5 使用内置代理与 EDR Optimum 进行交互。

内置代理与 EDR Optimum 的集成

“Endpoint Detection and Response (KSC)”和“Endpoint Detection and Response Expert (on-premise)”组件彼此不兼容。

要使 Kaspersky Industrial CyberSecurity for Nodes 作为 EDR Optimum 解决方案的一部分发挥作用，必须满足以下条件：

- 安装了带 Web Console 的 Kaspersky Security Center 14.2 或更高版本。
- 要通过 Kaspersky Security Center Web Console 启用 EDR Optimum 解决方案和管理服务器之间的交互，您必须建立新的安全连接，一个“*后台连接*”。

  在 Web Console 中建立后台连接

  1. 在 Web Console 的主窗口中，选择“**设置**” → “**整合**”。
  2. 转到**整合**区域。
  3. 开启 **用于整合的后台连接 已启用** 切换开关。
  4. 保存更改。

- 已安装 Kaspersky Endpoint Detection and Response 管理插件。
- 确保“Endpoint Detection and Response (KSC)”操作的以下 Kaspersky Industrial CyberSecurity for Nodes 组件已启用并可运行：
  - 实时文件保护。
  - 漏洞利用防御。
  - 反加密。
  - 修复引擎。

设置 EDR Optimum 集成涉及以下步骤：

1. **安装“Endpoint Detection and Response (KSC)”组件**

   在安装包设置或安装向导中，或通过更改 Windows 控制面板中的应用程序组件集，在必须选择要安装的应用程序组件的步骤中，选择以下内容：**完整功能 → 端点代理 → Endpoint Detection and Response (KSC)**。

   要完成更改应用程序组件集，您必须重新启动计算机。

2. **Kaspersky Endpoint Detection and Response Optimum 激活**

   有关 Endpoint Detection and Response (KSC) 组件授权许可的信息，请参阅此文章。

   确保授权许可中包含“Endpoint Detection and Response (KSC)”功能。

3. **启用和配置“Endpoint Detection and Response (KSC)”组件**

如何在 Kaspersky Security Center Web Console 中启用和配置“Endpoint Detection and Response (KSC)”组件

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**遥测采集服务器**”部分。
5. 在“**Endpoint Detection and Response (Industrial CyberSecurity)**”块中单击“**设置**”按钮。
   “**Endpoint Detection and Response (Industrial CyberSecurity)**”窗口将打开。
6. 选择**启用 Endpoint Detection and Response (Industrial CyberSecurity)**复选框。
7. 配置网络隔离设置。
8. 配置执行防护设置。
9. 如有必要，使用同名开关为 Cloud Sandbox 检测到的威胁启用计数器。
10. 保存更改。

这样，“Endpoint Detection and Response (KSC)”组件被启用。通过查看“*应用程序组件状态报告*”检查组件的运行状态。您还可以在“**Kaspersky Industrial CyberSecurity for Nodes**”节点工作区的应用程序控制台树中查看组件的运行状态。

4 **启用到 Kaspersky Security Center 管理服务器的数据传输**

为了正确运行 EDR Optimum 的所有功能，必须启用以下类型数据的数据传输：

- 隔离文件数据。
  在 Kaspersky Security Center Web Console 中，您可以从隔离区下载文件进行分析。
- 威胁发展链数据。
  您可以在 Web Console 中查看警报详细信息并采取响应操作。

如何在 Web 控制台中启用到管理服务器的数据传输

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击要配置的策略名称。
3. 在打开的“**<策略名称>**”窗口中，选择“**应用程序设置**”选项卡。
4. 转到**日志和通知**区域。
5. 在“**与管理服务器交互**”块中单击“**设置**”按钮。

6. 在打开的窗口中，选中以下复选框：

   - “**关于隔离区文件**”。
   - “**关于威胁发展链**”。

7. 保存更改。

扫描入侵指标 (IOC)

妥协的指标 (IOC) 是一组关于对象或活动的数据，表示未经授权访问计算机（数据泄露）。例如，许多登录系统的尝试都不成功，这可能构成妥协的指标。

*IOC 扫描任务*是一个使用包含一组入侵指标的 IOC 文件的组或本地任务。如果匹配入侵指标，应用程序将执行“*IOC 扫描*”任务属性中指定的操作。

如果您要手动添加入侵指标，请阅读“IOC 文件需求”。

您可以用以下方式创建*IOC 扫描*任务：

- 在警报详细信息中。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详细信息的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

- 在 Web Console 中。
- 在命令行上。

如何在 Kaspersky Security Center Web Console 中创建、配置和启动 IOC 扫描任务

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**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
   b. 在“**任务类型**”下拉列表中，选择“**IOC 扫描**”。
   c. 如有必要，可在“**任务名称**”字段编辑任务名称。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。
5. 输入要使用其权限运行任务的用户的账户凭证。

默认下，Kaspersky Industrial CyberSecurity for Nodes 以系统用户账户 (SYSTEM) 启动任务。

系统账户（SYSTEM）没有权限在网络驱动器上执行 *IOC 扫描*任务。如果您要为网络驱动器运行任务，选择对该驱动器具有访问权限的用户账户。

6. 完成向导操作。

   已创建的任务显示在任务列表中。

7. 单击已创建任务的名称。

   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 转到**IOC 扫描设置**区域。

10. 加载 IOC 文件以搜索妥协的指标。

    我们不建议在启动任务后添加或删除 IOC 文件。这可能会导致 IOC 扫描结果在任务之前的运行中显示不正确。要通过新的 IOC 文件搜索入侵指标，建议添加新任务。

11. 如果有必要，配置回顾性 IOC 扫描。在"*IOC 扫描*"任务的这种模式中，Kaspersky Industrial CyberSecurity for Nodes 在指定时间段内收到的受保护设备数据中搜索入侵指标。应用程序分析受保护计算机上安装的操作系统日志和浏览器日志中的数据。

    要在"*IOC 追溯扫描*"模式中启动任务，上传的 IOC 文件必须包含此列表中的一个或多个术语：*FileItem/**、*Network/**、*PortItem/**、*ProcessItem/**、*RegistryItem/**、*UrlHistoryItem/**。

    执行以下操作：

    a. 选择**启用 IOC 追溯扫描**复选框。

    b. 指定搜索的时间段（以天为单位）。最大值为 14 天。

       在运行任务时，应用程序会分析从任务启动时起指定时间段内收集的信息。

       默认设置是 1 天。

    c. 在任务属性的"**高级**"部分，确保选中上传的 IOC 文件中提到的所有数据类型的复选框。

    d. 如果上传的 IOC 文件包含带有 *Network/** 术语的入侵指标，选中"*网络数据 - NetworkItem*"数据类型旁边的复选框，默认为清除。

    "*IOC 扫描*"任务以回顾扫描模式启动。在此模式下，对于每个文件，应用程序都会发布正常任务结果和回顾性 IOC 扫描结果。

    Kaspersky Industrial CyberSecurity for Nodes 仅为回顾性扫描结果显示 PID 和 UPID 字段。此外，如果扩展遥测被禁用，回顾性 IOC 扫描有以下限制：

    - 应用程序不会填充 FileItem 记录的 Created、Modified、Changed、Accessed、FileAttributes 字段。
    - 对于尚未执行的现有文件，回顾性扫描结果中的 Md5sum、Sha256sum、SizeInBytes 字段设置为 0。
    - 对于检测到的已删除的文件，应用程序不会计算哈希。

12. 如果有必要，**配置 Kaspersky Industrial CyberSecurity for Nodes 在检测到入侵指标时要执行的操作**。

    a. 选择**在发现 IOC 后采取响应操作**复选框。

    b. 选中 Kaspersky Industrial CyberSecurity for Nodes 在检测到入侵指标时要执行的操作旁边的复选框：

    - "**从网络隔离计算机**"。如果选择此选项，Kaspersky Industrial CyberSecurity for Nodes 将计算机与网络隔离，以防止威胁扩散。您可以在 Endpoint Detection and Response (KSC) 组件设置中配置隔离的持续时间。
    - "**将副本移动到隔离区，删除对象**"。如果选择此选项，Kaspersky Industrial CyberSecurity for Nodes 删除在计算机上发现的恶意对象。在删除对象之前，Kaspersky Industrial CyberSecurity for Nodes 会创建一份备份副本并将其置于隔离区。
    - "**运行关键区域扫描**"。如果选择此选项，Kaspersky Industrial CyberSecurity for Nodes 运行预定义任务：*关键区域扫描*。

13. 转到**高级**区域。

14. 选择作为任务的一部分必须被分析的数据类型 (IOC 文档)。

    Kaspersky Industrial CyberSecurity for Nodes 根据加载的 IOC 文件的内容自动选择"*IOC 扫描*"任务的数据类型（IOC 文档）。我们不建议您自行清除数据类型的选择。

    对于数据类型"*Windows 注册表 – RegistryItem*"，Kaspersky Industrial CyberSecurity for Nodes 分析一组预定义的注册表键集合。

15. 如果有必要，**指定"文件 – FileItem"数据类型的其他设置**。

    a. 单击"**IOC 文件**"。

    "**文件扫描设置 – FileItem**"窗口将打开。

    b. 在"**在以下区域内搜索 IOC**"下，选择您想要该任务分析的数据。

    c. 在"**扫描自定义区域**"下，选择受保护设备磁盘上想要查找入侵指标的区域。

    默认下，Kaspersky Industrial CyberSecurity for Nodes 仅在计算机的重要区域扫描 IOC，例如"下载"文件夹、桌面、临时操作系统文件文件夹等等。您可以指定自己的所需区域的路径。

    d. 单击"**确定**"。

16. 如果有必要，**指定"Windows 事件日志 – EventLogItem"数据类型的其他设置**。

    a. 单击"**日志和日期**"。

    "**Windows 事件日志扫描设置 – EventLogItem**"窗口将打开。

    b. 要让任务忽略在特定时刻之前注册的事件，请选择"**仅扫描指定时间段内记录的事件**"复选框并指定日期和时间。

c. 在“**扫描属于以下信道的事件**”下，选择您想要该任务分析的 Windows 事件日志。

d. 单击“**确定**”。

17. 在任务属性窗口中，选择“**计划**”选项卡。
18. 配置任务计划。
19. 保存更改。
20. 选中该任务旁边的复选框。
21. 单击“**开始**”。

如何在命令行上配置和启动 IOC 扫描任务

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，Command Prompt cmd.exe）。
2. 使用 cd 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如：`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0`。
3. 输入命令：

   ```
   KAVSHELL SCAN-IOC <IOC 文件的完整路径> [/PATH:<IOC 文件的文件夹路径>] [/PROCESS=no] [/HINT=<进程可执行文件的完整路径|文件的完整路径>] [/REGISTRY=no] [/DNSENTRY=no] [/ARPENTRY=no] [/PORTS=no] [/SERVICES=no] [/SYSTEM=no] [/USERS=no] [/VOLUMES=no] [/EVENTLOG=no] [/DATETIME=<事件发布日期>] [/CHANNELS=<通道列表>] [/FILES=no] [/DRIVES=<all|system|critical|custom>] [/NETWORK=no] [/URL=no] [/EMAIL=no] [/ROUTE=no] [/RETRO] [/EXCLUDES=<排除项列表>] [/SCOPE=<可配置的文件夹列表>]
   ```
4. 按 Enter。

用于配置和启动 IOC 扫描任务的命令行选项

选项	描述
SCAN-IOC	必需参数。 启动设备上的标准 IOC 扫描任务。
<IOC 文件的完整路径>	您想要用于搜索的具有 ioc 或 xml 扩展名的 IOC 文件的完整路径。 必需参数，如果未指定 /PATH:<包含 IOC 文件的文件夹的路径> 参数。
/PATH:<IOC 文件的文件夹路径>	您要用于扫描的 IOC 文件的文件夹路径。 必需参数，如果未指定“<IOC 文件的完整路径>”。
/PROCESS=no	可选参数。 扫描期间禁用进程信息分析。 如果参数的值为“<no>”，则在执行扫描时，Kaspersky Industrial CyberSecurity for Nodes 不会分析计算机上运行的进程。如果 IOC 文件包含 ProcessItem IOC 文档的 IOC 术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 ProcessItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析进程数据。

/HINT=<进程可执行文件的完整路径|文件的完整路径>	可选参数。 此参数允许通过指定单个文件来缩小使用 ProcessItem 和 FileItem IOC 文档进行扫描的分析数据的范围。 您可以将以下内容作为此参数的值传递： • <进程可执行文件的完整路径 (ProcessItem)> – ProcessItem • <文件的完整路径> – FileItem 此参数只能与 /PROCESS=yes 和 /FILES=yes 参数一起传递。
/REGISTRY=no	可选参数。 此参数禁用在 IOC 扫描期间分析有关注册表键（IOC 文档 FileItem）的信息。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会分析注册表键信息。如果 IOC 文件包含 RegistryItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 RegistryItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析注册表。
/DNSENTRY=no	可选参数。 此参数禁用 IOC 扫描期间对本地 DNS 缓存记录（ IOC 文档 DnsEntryItem）的分析。 如果参数的值为<no>，Kaspersky Industrial CyberSecurity for Nodes 不会扫描本地 DNS 缓存。如果 IOC 文件包含 DnsEntryItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 DnsEntryItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会扫描本地 DNS 缓存。
/ARPENTRY=no	可选参数。 此参数禁用 IOC 扫描期间对本地 ARP 表记录（IOC 文档 ArpEntryItem）的分析。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会扫描本地 ARP 表。如果 IOC 文件包含 ArpEntryItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 ArpEntryItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会扫描本地 ARP 表。
/PORTS=no	可选参数。 此参数禁用在 IOC 扫描期间对正在监听的端口（IOC 文档 PortItem）的信息的分析。 如果参数的值为<no>，Kaspersky Industrial CyberSecurity for Nodes 不会扫描设备上的活动连接表。如果 IOC 文件包含 PortItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 PortItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会扫描设备上的活动连接表。
/SERVICES=no	可选参数。 此参数禁用在 IOC 扫描期间分析有关设备上安装的服务（IOC 文档 ServiceItem）的信息。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会扫描设备上安装的服务的信息。如果 IOC 文件包含 ServiceItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 ServiceItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析服务信息。
/SYSTEM=no	可选参数。 此参数禁用 IOC 扫描期间分析有关环境（IOC 文档 SystemInfoItem）的信息。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会分析环境信息。如果 IOC 文件包含 SystemInfoItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 SystemInfoItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析环境信息。
/USERS=no	可选参数。 此参数禁用 IOC 扫描期间分析有关用户（IOC 文档 UserItem）的信息。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会分析系统中创建的用户的信息。如果 IOC 文件包含 UserItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 UserItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析系统中创建的用户的信息。

/VOLUMES=no	可选参数。 此参数禁用在 IOC 扫描期间分析有关卷（IOC 文档 VolumeItem）的信息。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会扫描设备上的卷的信息。如果 IOC 文件包含 VolumeItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 VolumeItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析卷信息。
/EVENTLOG=no	可选参数。 此参数禁用 IOC 扫描期间对 Windows 事件日志记录（IOC 文档 EventLogItem）的分析。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会扫描 Windows 事件日志记录。如果 IOC 文件包含 EventLogItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 EventLogItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析 Windows 事件日志记录。
/DATETIME=< 事件发布日期 >	可选参数。 该参数允许在确定相应 IOC 文档的 IOC 扫描范围时启用或禁用考虑事件在 Windows 事件日志中发布的日期。 在执行 IOC 扫描时，Kaspersky Industrial CyberSecurity for Nodes 仅扫描从指定时间和日期到任务运行时刻期间发布的事件。 Kaspersky Industrial CyberSecurity for Nodes 允许将事件发布日期指定为参数值。仅对在指定日期之后和运行扫描之前在 Windows 事件日志中发布的事件执行扫描。 如果未指定参数，Kaspersky Industrial CyberSecurity for Nodes 将扫描具有任何发布日期的事件。 仅当为扫描提供的 IOC 文件中描述了 EventLogItem IOC 文档时，才使用该设置。
/CHANNELS=< 通道列表 >	可选参数。 此参数允许您传递要对其执行 IOC 扫描的通道（日志）名称列表。 如果传递此参数，则在运行 IOC 扫描任务时，Kaspersky Industrial CyberSecurity for Nodes 只会考虑已在指定日志中发布的事件。 根据日志属性（“Full Name”参数）或事件属性（事件 xml 架构中的“<Channel></Channel>”参数）中指定的日志（通道）名称，将日志名称指定为字符串。 默认情况下（包括不传递该参数的情况），对“Application”、“System”和“Security”通道执行 IOC 扫描。 您可以在此参数中传递多个值（以空格分隔）。 仅当为扫描提供的 IOC 文件中描述了 EventLogItem IOC 文档时，才使用该设置。
/FILES=no	可选参数。 此参数禁用在 IOC 扫描期间分析有关文件（IOC 文档 FileItem）的信息。 如果参数的值为“<no>”，Kaspersky Industrial CyberSecurity for Nodes 不会分析文件信息。如果 IOC 文件包含 FileItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 FileItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析文件信息。
/DRIVES=<all|system|critical|custom>	可选参数。 此参数允许您在分析 FileItem IOC 文档的数据时指定 IOC 扫描范围。 您可以使用以下值之一： • <all> 使应用程序扫描所有可用的文件区域。 • <system> 使应用程序仅扫描安装操作系统的文件夹中的文件。 • <critical> 使应用程序仅扫描用户和系统文件夹中的临时文件。 • <custom> 使应用程序仅扫描用户指定范围内的文件。 如果没有指定参数，则扫描关键区域。
/NETWORK=no	可选参数。 此参数禁用在 IOC 扫描期间基于 Network IOC 文档的威胁扫描。 如果参数的值是 <no>，Kaspersky Industrial CyberSecurity for Nodes 不会基于 Network IOC 文档扫描威胁。如果 IOC 文件包含 Network IOC 文档的术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 Network IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会基于 Network IOC 文档扫描威胁。

/URL=no	可选参数。 此参数禁用在 IOC 扫描期间基于 UrlHistoryItem IOC 文档的威胁扫描。 如果参数的值是 <no>， Kaspersky Industrial CyberSecurity for Nodes 不会根据 UrlHistoryItem IOC 文档扫描威胁。如果 IOC 文件包含 UrlHistoryItem IOC 文档的术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 UrlHistoryItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会基于 UrlHistoryItem IOC 文档扫描威胁。
/EMAIL=no	可选参数。 此参数禁用在 IOC 扫描期间分析有关邮件对象（IOC 文档 Email）的信息。 如果参数的值为“ <no> ”，Kaspersky Industrial CyberSecurity for Nodes 不会分析邮件对象。如果 IOC 文件包含 Email IOC 文档的术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 Email IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会分析邮件对象。
/ROUTE=no	可选参数。 此参数启用在 IOC 扫描期间基于 RouteEntryItem IOC 文档的威胁扫描。 如果参数的值是 <no>， Kaspersky Industrial CyberSecurity for Nodes 不会根据 RouteEntryItem IOC 文档扫描威胁。如果 IOC 文件包含 UrlHistoryItem IOC 文档的术语，则忽略这些术语（检测为不匹配）。 如果未指定此参数，则仅当为扫描提供的 IOC 文件中描述了 RouteEntryItem IOC 文档时，Kaspersky Industrial CyberSecurity for Nodes 才会基于 RouteEntryItem IOC 文档扫描威胁。
/RETRO	可选参数。 此参数在 *IOC 追溯扫描* 模式中运行任务。 通过此参数，您还可以通过使用 DEPTH=< 间隔天数 > 参数传递希望应用程序执行回顾性 IOC 扫描的时间段。最大值为 14 天。时间从任务开始的时刻开始计算。 例如： KAVSHELL SCAN-IOC /PATH=< IOC 文件的文件夹路径 > /RETRO /DEPTH=2 如果时间间隔未传递，则默认为 1 天。
/EXCLUDES= <排除项列表>	可选参数。 此参数允许您在分析 FileItem IOC 文档的数据时指定排除项范围。您可以在此参数中传递多个以空格分隔的路径。 如果未指定此参数，扫描将在没有排除项的情况下进行。
/SCOPE= <可配置的文件夹列表>	可选参数。 如果指定了 /DRIVES=custom 参数，则需要该参数。 此参数允许您指定扫描范围的列表。您可以在此参数中传递多个以空格分隔的路径。

SCAN-IOC 命令的返回代码：

- -1：设备上安装的 Kaspersky Industrial CyberSecurity for Nodes 版本不支持该命令。
- 0 – 命令成功完成。
- 1 – 表示未将强制参数传递给命令。
- 2 – 一般错误。
- 4 – 语法错误。

如果命令成功完成（返回值 0），并且检测到入侵指标，Kaspersky Industrial CyberSecurity for Nodes 将向命令行输出以下任务结果信息：

应用程序检测到入侵指标时输出到命令行的信息

Uuid	IOC 文件结构头中的 IOC 文件 ID（<ioc id=""> 标记）
Name	IOC 文件结构头中的 IOC 文件描述（<description></description> 标记）

Matched Indicator Items	所有匹配的指示器 ID 列表。
Matched objects	与之匹配的每个 IOC 文件的数据。
Date	发现入侵指标的文件的创建日期。
Created	仅适用于 FileItem。发现入侵指标的对象的创建日期。
Pid	发现入侵指标的进程的 ID。
Upid	发现入侵指标的进程的唯一 ID。
ParentPid	包含发现入侵指标的进程的父对象的 ID。
Username	修改扫描对象的用户的名称。
StartTime	发现入侵指标的进程的开始时间。

您可以在“**结果**”部分的“任务属性”中查看任务结果。您可以在任务属性中查看有关检测到的入侵指标的信息：**应用程序设置 → IOC 扫描结果**。

Kaspersky Industrial CyberSecurity for Nodes 会在为同一 IOC 文件创建的记录中查找重复项，并仅在任务结果中保留唯一记录。重复项是同一类型的记录，所有比较字段的值都相同。如果应用程序在一个或多个字段中缺少值，也可能不会创建记录（见下表）。

类型	比较字段	不创建记录的条件
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• FullPath、Md5sum、Sha256sum 字段的值缺失。 • FullPath 字段的值缺失，而 Md5sum、Sha256sum 字段的值相同。
RegistryItem	• Hive • KeyPath • ValueName • Text • 类型	以下字段中至少一个缺少值：Hive、KeyPath、ValueName。
ProcessItem	• startTime • PID	startTime 或 PID 字段的值缺失。

“**警报详情**”窗口可能会显示具有相同字段值的 RegistryItem 记录。此类记录不属于重复，因为它们的文本字段值不同，不会显示在界面中。

IOC 扫描结果被保存 30 天。在此时间之后，Kaspersky Industrial CyberSecurity for Nodes 将自动删除最早条目。

在找到 128 个与 IOC 文件中描述的入侵指标相匹配的内容后，IOC 扫描结束。有必要限制 *IOC 扫描*任务报告中的条目数量，以便于分析，并防止由于不精确制定的入侵指标而产生大量匹配而导致报告变得太大。

IOC 文件需求

当创建 IOC 扫描任务时，考虑以下 IOC 文件需求和限制：

- 该应用程序支持开放标准 OpenIOC 版本 1.0 和 1.1 中具有 IOC 和 XML 扩展名的 IOC 文件，用于描述妥协的指标。
- 下载 IOC 文件后，在任务属性中，您可以直接在内置编辑器中手动修改文件内容。Kaspersky Industrial CyberSecurity for Nodes 支持更改符合 OpenIOC 版本 1.1 的 IOC 文件的内容。无法修改符合 OpenIOC 1.0 版本的 IOC 文件的内容。
- 如果在命令行创建一个“*IOC 扫描*”任务，您上传 IOC 文件（其中一些文件不受支持），则当任务运行时，应用程序仅使用受支持的 IOC 文件。如果在命令行创建一个“*IOC 扫描*”任务，你上传的所有 IOC 文件都不受支持，任务仍然可以运行，但它不会检测到任何入侵指标。无法使用 Web 控制台或云控制台上传不受支持的 IOC 文件。
- 语义错误和 IOC 文件中不支持的 IOC 术语和标记不会导致任务执行失败。在 IOC 文件的这些部分中，应用程序检测不到匹配。
- 单个 IOC 扫描任务中使用的所有 IOC 文件的标识符必须是唯一的。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。
- 单个 IOC 文件的大小不得超过 2 MB。使用较大的文件将导致 IOC 扫描任务因错误而终止。添加到 IOC 集合的所有文件的总大小不能超过 10 MB。如果所有文件的总大小超过 10 MB，您需要拆分 IOC 集合并创建多个“IOC 扫描”任务。
- 建议为每个威胁创建一个 IOC 文件。这使得分析“*IOC 扫描*”任务的结果更加容易。

您可以通过单击下面的链接下载该文件，该文件包含一个表，其中包含 OpenIOC 标准的 IOC 术语的完整列表。

下载 IOC TERMS.XLSX 文件

下表显示了应用程序支持 OpenIOC 标准的特性和限制。

OpenIOC 版本 1.0 和 1.1 的功能和支持限制。

支持条件	OpenIOC 1.0： is isnot（作为集合中的排除项） contains containsnot（作为集合中的排除项） OpenIOC 1.1： is contains starts-with ends-with matches greater-than less-than
支持的条件属性	OpenIOC 1.1： preserve-case negate

支持的运算符	AND OR
支持的数据类型	"date"：日期（适用条件：is、greater-than、less-than） "int"：整数（适用条件：is、greater-than、less-than） "string"：字符串（适用条件：is、contains、matches、starts-with、ends-with） "duration"：持续秒数（适用条件：is、greater-than、less-than）
数据类型解释的特点	"boolean string"、"restricted string"、"md5"、"IP"、"sha256"和"base64Binary"数据类型被解释为字符串。 对于 int 和 date 类型指定为间隔的情况，应用程序支持解释 Content 参数： OpenIOC 1.0： 在 Content 字段使用 TO 运算符： <Content type="int">49600 TO 50700</Content> <Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content> <Content type="int">[154192 TO 154192]</Content> OpenIOC 1.1： 使用 greater-than 和 less-than 条件 在 Content 字段使用 TO 运算符 如果指示器设置为“ISO 8601, Zulu time zone, UTC”格式，则应用程序支持对 date 和 duration 数据类型的解释。

IOC 扫描的扩展遥测

我们建议在计算机上启用扩展遥测以进行回顾性 IOC 扫描。扩展遥测提高了 IOC 检测的准确性，但会占用更多的计算机资源。

扩展遥测包括对以下附加术语的支持：

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

如果禁用扩展遥测，Kaspersky Industrial CyberSecurity for Nodes 可能会轮换有关检测到的入侵指标的信息。

要启用扩展遥测：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**遥测采集服务器** → **Endpoint Detection and Response (Industrial CyberSecurity)**”并点击“**配置**”。
5. 选择**启用高级系统活动日志记录**复选框。
6. 保存更改。

注册表中的 IOC 扫描范围 (RegistryItem)

当您添加 RegistryItem 数据类型到 IOC 扫描范围时，Kaspersky Industrial CyberSecurity for Nodes 扫描以下注册表键：

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile
```

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

移动文件到隔离区

在响应威胁时，Kaspersky Endpoint Detection and Response 可能创建“*移动文件到隔离区*”任务。这对于将威胁的后果降至最低是必要的。隔离区是计算机上的一个特别的本地存储区。用户可以隔离其认为对计算机有危险的文件。隔离的文件以加密形式存储，因此不会危害您设备的安全。Kaspersky Industrial CyberSecurity for Nodes 仅在使用以下 Detection and Response 解决方案时使用隔离：EDR Optimum、KATA (EDR)。在其他情况下，Kaspersky Industrial CyberSecurity for Nodes 将相关文件置于备份中。有关将隔离管理作为解决方案的一部分的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Anti Targeted Attack Platform 帮助。

您可以用以下方式创建*移动文件到隔离区*任务：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。

- 使用任务向导。

  必须输入文件路径或哈希（SHA256 或 MD5），或者同时输入文件路径和文件哈希。

“*将文件移至隔离区*”任务具有以下限制：

1. 文件大小不得超过 100 MB。
2. 系统关键对象(SCO)无法被隔离。SCO 是操作系统和 Kaspersky Industrial CyberSecurity for Nodes 应用程序运行所需的文件。

要创建“移动文件到隔离区”任务：

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

   任务列表打开。

2. 单击“**添加**”。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。

   b. 在“**任务类型**”下拉列表中，选择“**移动文件到隔离区**”。

   c. 在“**任务名称**”字段中，输入任务的简要说明并单击“**下一步**”。

4. 在“**任务范围**”部分，选择受管理设备并单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。
   默认下，Kaspersky Industrial CyberSecurity for Nodes 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。

7. 单击新任务。任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 在文件列表中，单击“**添加**”。文件添加向导将启动。

0. 要添加文件，您必须输入文件的完整路径或文件夹路径的校验和。

   > 如果文件位于网络驱动器上，请输入以“\\”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现未找到文件错误。

1. 在任务属性窗口中，选择“**计划**”选项卡。配置任务计划。

   > LAN 唤醒不可用于此任务。确保计算机已打开以运行任务。

2. 单击“**保存**”。

3. 选中任务旁边的复选框，然后单击“**启动**”按钮。

结果，Kaspersky Industrial CyberSecurity for Nodes 将文件移动到隔离区。

如果文件被其他进程锁定，则任务显示为“**已通过**”，但文件本身只有在计算机重新启动后才会被隔离。重新启动计算机后，确认文件已删除。

如果试图隔离太大的文件，则“*移动文件到隔离区*”任务可能会以“*隔离区存储空间不足*”错误结束。清空隔离区或增加其大小。然后再次尝试。

您可以使用 Kaspersky Security Center Web Console 从隔离区恢复文件或清空隔离区。您可以使用**命令行**在计算机上本地恢复对象。

将文件从隔离区或备份区恢复到原始文件夹。Kaspersky Industrial CyberSecurity for Nodes 仅在与 EDR Optimum 和 KATA (EDR) 解决方案配合使用时使用隔离区。在其他情况下，Kaspersky Industrial CyberSecurity for Nodes 将相关文件置于备份中。有关将隔离管理作为解决方案的一部分的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Anti Targeted Attack Platform 帮助。

对象在系统账户 (SYSTEM) 下隔离。

从隔离恢复文件涉及以下特殊注意事项：

- 如果目标文件夹已被删除或用户没有该文件夹的访问权限，则应用程序会将该文件放在 `%DataRoot%\QB\Restored` 文件夹中。然后必须手动将文件移动到目标文件夹。
- 应用程序对要还原的文件的名称区分大小写。如果您在输入文件名时没有观察到这种情况，则应用程序不会恢复文件。
- 如果目标文件夹中已有同名文件，如果命令中未指定 `/replace` 参数，则应用程序将取消恢复该文件。
- 如果您使用的是 KATA（EDR）解决方案，应用程序会在恢复文件后将文件副本保存在隔离区中。您可以手动清空隔离区。对于 EDR Optimum 解决方案，应用程序在恢复后删除文件。

要运行命令，请转到 kavshell.exe 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
KAVSHELL restore <要恢复的文件的名称> [/replace] [/quarantine] [/backup] [/login=<当前用户账户的名称>] [/PWD=
</login 密码或 KLAdmin 密码（如果未指定 /login）>]
```

示例

```
KAVSHELL restore /replace_file.txt /password=samplePassword
```

命令返回值：

- -1：计算机上安装的应用程序版本不支持该命令。
- 0：命令成功完成。
- 1：表示未将强制参数传递给命令。
- 2：一般错误。
- 4：语法错误。
- 9 - 错误操作（例如，在组件已禁用时尝试禁用该组件）。

获取文件

您可以从用户计算机获取文件。例如，您可以配置获取由第三方应用程序创建的事件日志文件。要获取文件，您必须创建专用任务。执行任务后，文件将保存在隔离区中。您可以使用 Kaspersky Security Center Web Console 将此文件从隔离区下载到您的计算机。在用户的计算机上，文件保留在其原始文件夹中。

文件大小不得超过 100 MB。

要创建“获取文件”任务：

1. 在 Web Console 的主窗口中，选择“**设备**” → “**任务**”。
   任务列表打开。
2. 单击“**添加**”。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“Kaspersky Industrial CyberSecurity for Nodes”。
   b. 在“**任务类型**”下拉列表中，选择“**获取文件**”。
   c. 在“**任务名称**”字段中，输入任务的简要说明并单击“**下一步**”。
4. 在“**任务范围**”部分，选择受管理设备并单击“**下一步**”。
5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。
   默认下，Kaspersky Industrial CyberSecurity for Nodes 以系统用户账户 (SYSTEM) 启动任务。
6. 单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。
7. 单击新任务。任务属性窗口将打开。
8. 选择**应用程序设置**选项卡。
9. 在文件列表中，单击“**添加**”。文件添加向导将启动。
0. 要添加文件，您必须输入文件的完整路径或文件夹路径的校验和。

   如果文件位于网络驱动器上，请输入以“\\”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现*未找到文件*错误。

1. 在任务属性窗口中，选择“**计划**”选项卡。配置任务计划。

   LAN 唤醒不可用于此任务。确保计算机已打开以运行任务。

2. 单击“**保存**”。

3. 选中任务旁边的复选框，然后单击“**启动**”按钮。

结果，Kaspersky Industrial CyberSecurity for Nodes 创建文件的副本并将其移动到隔离区。您可以使用 Kaspersky Security Center Web Console 从隔离区下载此文件。

删除文件

您可以使用“*删除文件*”任务远程删除文件。例如，您可以在响应威胁时远程删除文件。

> 系统关键对象(SCO)无法被删除。SCO 是操作系统和 Kaspersky Industrial CyberSecurity for Nodes 应用程序运行所需的文件。

要创建“删除文件”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**”。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。

   b. 在“**任务类型**”下拉列表中，选择“**删除文件**”。

   c. 在“**任务名称**”字段中，输入任务的简要说明并单击“**下一步**”。

4. 在“**任务范围**”部分，选择受管理设备并单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。
   默认下，Kaspersky Industrial CyberSecurity for Nodes 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。

7. 单击新任务。任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 要删除文件，您必须输入文件的完整路径或文件夹路径的校验和。

   > 如果文件位于网络驱动器上，请输入以“\\”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现*未找到文件*错误。

0. 在任务属性窗口中，选择“**计划**”选项卡。配置任务计划。

   > LAN 唤醒不可用于此任务。确保计算机已打开以运行任务。

1. 单击“**保存**”。

2. 选中任务旁边的复选框，然后单击“**启动**”按钮。

   结果，Kaspersky Industrial CyberSecurity for Nodes 将从计算机删除文件。如果文件被其他进程锁定，则任务显示为*已完成*，但文件本身只有在计算机重新启动后才会被删除。重新启动计算机后，确认文件已删除。

如果试图删除当前正在运行的可执行文件，则“*删除文件*”任务可能会以“*访问被拒绝*”错误结束。为文件创建终止进程任务，然后重试。

进程启动

您可以使用“*启动进程*”任务远程运行文件。例如，您可以远程运行创建计算机配置文件的实用程序。下一步，您可以使用*获取文件*任务接收在 Kaspersky Security Center Web Console 中创建的文件。

要创建“启动进程”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**”。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。

   b. 在“**任务类型**”下拉列表中，选择“**启动进程**”。

   c. 在“**任务名称**”字段中，输入任务的简要说明并单击“**下一步**”。

4. 在“**任务范围**”部分，选择受管理设备并单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。
   默认下，Kaspersky Industrial CyberSecurity for Nodes 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。

7. 单击新任务。任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 选择“**启动设置**”部分并输入进程启动命令：
   假设您想运行一个实用程序(`utility.exe`)，该实用程序将有关计算机配置的信息保存到当前文件夹中名为 `conf.txt` 的文件中（默认情况下）。该实用程序位于 `C:\Users\admin\Diagnostic\` 文件夹。您必须将配置文件保存在 `C:\Users\admin\Documents\Configuration` 文件夹。输入以下值：

   - **可执行命令** – `C:\Users\admin\Diagnostic\utility.exe`
   - **命令行参数(可选)** – `/R conf.txt`
   - **工作文件夹路径(可选)** – `C:\Users\admin\Documents\Configuration`

0. 在任务属性窗口中，选择“**计划**”选项卡。

1. 配置任务计划。

> LAN 唤醒不可用于此任务。确保计算机已打开以运行任务。

2. 单击“**保存**”。

3. 选中任务旁边的复选框，然后单击“**开始**”按钮。

结果，Kaspersky Industrial CyberSecurity for Nodes 在静默模式下运行命令并启动进程。您可以在“**执行结果**”部分的“任务属性”中查看任务结果。

终止进程

您可以使用“*终止进程*”任务远程终止进程。例如，您可以远程终止使用“*运行进程*”任务启动的互联网速度测试实用程序。

如果您要禁止运行一个文件，您可以配置执行防护组件。您可以禁止执行可执行文件、脚本、Office 格式文件。

> 系统关键对象(SCO)的进程无法被终止。SCO 是操作系统和 Kaspersky Industrial CyberSecurity for Nodes 应用程序运行所需的文件。

要创建“终止进程”任务：

1. 在 Web Console 的主窗口中，选择“**设备**” → “**任务**”。
   任务列表打开。

2. 单击“**添加**”。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。

   b. 在“**任务类型**”下拉列表中，选择“**终止进程**”。

   c. 在“**任务名称**”字段中，输入任务的简要说明并单击“**下一步**”。

4. 在“**任务范围**”部分，选择受管理设备并单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。
   默认下，Kaspersky Industrial CyberSecurity for Nodes 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。

7. 单击新任务。任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 要完成此过程，必须选择要终止的文件。您可以采用以下方式之一选择文件：

   - 输入文件的全名。
   - 输入文件的哈希值和文件的路径。
   - 输入进程的 PID（仅适用于本地任务）。

   如果文件位于网络驱动器上，请输入以“\\”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现*未找到文件*错误。

0. 在任务属性窗口中，选择“**计划**”选项卡。

1. 配置任务计划。

   LAN 唤醒不可用于此任务。确保计算机已打开以运行任务。

2. 单击“**保存**”。

3. 选中任务旁边的复选框，然后单击“**启动**”按钮。

结果，Kaspersky Industrial CyberSecurity for Nodes 将在计算机上终止该进程。例如，如果某个“游戏”应用程序正在运行，而您终止了 game.exe 进程，则该应用程序将在不保存数据的情况下关闭。您可以在“**结果**”部分的“任务属性”中查看任务结果。

执行防护

执行防护允许管理可执行文件和脚本的运行，以及打开 Office 格式文件。这样，例如，您可以防止执行您认为不安全的应用程序。结果，威胁传播可以被停止。执行防护支持**一组 Office 文件扩展名**和**一组脚本解释器**。

执行防护支持以下脚本解释器：

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe

- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

执行防护支持在 Java 运行时环境（Java.exe 和 javaw.exe 进程）中使用 Java 应用程序。

Kaspersky Industrial CyberSecurity for Nodes 支持防止在某些应用程序中打开 Office 格式文件。下表列出了有关支持的文件扩展名和应用程序的信息。

执行防护支持的文件扩展名

应用程序名称	可执行文件	文件扩展名
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

执行防护规则

执行防护使用执行防护规则管理用户对文件的访问。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。

您可以创建执行防护规则：

- 在警报详细信息中（仅适用于 EDR Optimum）。
- *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详细信息的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。
- 使用组策略或本地应用程序设置。

  必须输入文件路径或哈希（SHA256 或 MD5），或者同时输入文件路径和文件哈希。

您还可以使用**命令行**在本地管理执行防护。

禁用执行防护组件或显示组件的当前设置，包括执行防护规则列表。

要运行命令，请转到 kavshell.exe 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
KAVSHELL prevention [/disable] [/show] [/login:<当前用户账户的名称>] [/pwd:</login 密码或 KLAdmin 密码（如果未指定 /login）>]
```

在执行 `KAVSHELL prevention /show` 命令时，您将得到以下响应：

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

命令返回值：

- -1：计算机上安装的应用程序版本不支持该命令。
- 0：命令成功完成。
- 1：表示未将强制参数传递给命令。
- 2：一般错误。
- 4：语法错误。
- 9 - 错误操作（例如，在组件已禁用时尝试禁用该组件）。

执行防护具有以下限制：

1. 预防规则不包括 CD 或 ISO 映像中的文件。应用程序不会阻止这些文件的执行或打开。
2. 无法阻止系统关键对象（SCO）的启动。SCO 是操作系统和 Kaspersky Industrial CyberSecurity for Nodes 应用程序运行所需的文件。
3. 不建议创建超过 5000 个运行防护规则，因为这可能会导致系统不稳定。

执行防护规则模式

执行防护组件可以在两种模式下工作：

- **仅记录**

  在此模式下，Kaspersky Industrial CyberSecurity for Nodes 将发布关于尝试执行符合防护规则标准的对象或打开这样的文档的事件到 Windows 事件日志和 Kaspersky Security Center，但不会阻止尝试运行对象或打开文档。默认选择该模式。

- **阻止并写入报告**

  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 Windows 事件日志和 Kaspersky Security Center 事件日志。

管理执行防护

您仅可以在 Kaspersky Security Center Web Console 配置组件设置。

如何在 Kaspersky Security Center Web Console 中阻止对象执行

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**遥测采集服务器 → Endpoint Detection and Response (Industrial CyberSecurity)**”并点击“**配置**”。
5. 选择**启用执行防护**复选框。
6. 在**执行或打开禁止的对象时的操作**块，选择组件操作模式：
   - “**阻止**”。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 Windows 事件日志和 Kaspersky Security Center 事件日志。
   - “**通知**”。在此模式下，Kaspersky Industrial CyberSecurity for Nodes 将发布关于尝试执行符合防护规则标准的对象或打开这样的文档的事件到 Windows 事件日志和 Kaspersky Security Center，但不会阻止尝试运行对象或打开文档。默认选择该模式。

7. 创建执行防护规则列表：

   a. 单击“**添加**”。

   b. 这将打开一个窗口，在此窗口中，输入执行防护规则名称。

   c. 在**类型**下拉列表，选择您要阻止的对象：**可执行文件**、**脚本**、**Microsoft Office 文档**。

   如果您选择了错误的对象类型，Kaspersky Industrial CyberSecurity for Nodes 不阻止文件或脚本。

   d. 要添加文件，您必须输入文件的哈希值（SHA256 或 MD5）、文件的完整路径或哈希值和路径两者。

   如果文件位于网络驱动器上，请输入以“\\”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，Kaspersky Industrial CyberSecurity for Nodes 不阻止文件或脚本。

   e. 执行防护支持**一组 Office 文件扩展名**和**一组脚本解释器**。

   执行防护支持以下脚本解释器：

   - AutoHotkey.exe
   - AutoHotkeyA32.exe
   - AutoHotkeyA64.exe
   - AutoHotkeyU32.exe
   - AutoHotkeyU64.exe
   - InstallUtil.exe
   - RegAsm.exe
   - RegSvcs.exe
   - autoit.exe
   - cmd.exe
   - control.exe
   - cscript.exe
   - hh.exe
   - mmc.exe
   - msbuild.exe
   - mshta.exe
   - msiexec.exe

- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

执行防护支持在 Java 运行时环境（Java.exe 和 javaw.exe 进程）中使用 Java 应用程序。

Kaspersky Industrial CyberSecurity for Nodes 支持防止在某些应用程序中打开 Office 格式文件。下表列出了有关支持的文件扩展名和应用程序的信息。

执行防护支持的文件扩展名

应用程序名称	可执行文件	文件扩展名
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf

应用程序名称	可执行文件	文件扩展名
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

f. 单击“**确定**”。

8. 保存更改。

因此，Kaspersky Industrial CyberSecurity for Nodes 会阻止对象的执行：运行可执行文件和脚本，打开 Office 格式文件。您也可以在文本编辑器中打开脚本文件，即便执行脚本被阻止。当阻止对象的执行时，如果在应用程序设置中启用了通知，Kaspersky Industrial CyberSecurity for Nodes 将显示标准通知。

计算机网络隔离

计算机网络隔离是指计算机操作系统的所有进程和服务，除特别排除的进程和服务外，都与网络环境隔离。

运行 Windows 11、Windows Vista、Windows XP 和 Windows Server 2003 的隔离计算机可以响应 ARP、ICMP 和 ICMPv6 请求，或者发送 RST 数据包以响应传入的 TCP 请求。此活动由操作系统发起，不受网络隔离组件的控制。此外，网络隔离组件不控制传输流量。

计算机网络隔离允许自动将计算机与网络隔离，以响应检测到的妥协的指标（IOC） - 这是*自动模式*。您还可以在调查检测到的威胁时手动暂时启用网络隔离，方法是启用*手动模式*。

启用网络隔离后，应用程序将终止计算机上所有活动的 TCP/IP 连接并阻止除以下连接之外的任何新 TCP/IP 连接：

- 网络隔离排除项中指定的连接
- 由 Kaspersky Industrial CyberSecurity for Nodes 服务启动的连接
- 由 Kaspersky Security Center 网络代理发起的连接

您仅可以在 Kaspersky Security Center Web Console 配置组件设置。

自动网络隔离模式

您可以将网络隔离配置为作为 IOC 检测响应的一部分自动启用。自动网络隔离模式是使用组策略配置的。

如何在检测到 IOC 时配置自动网络隔离

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“Kaspersky Industrial CyberSecurity for Nodes **IOC 扫描**”任务.
   任务属性窗口将打开。
   如果必要，请创建“*IOC 扫描*”任务。
3. 选择**应用程序设置**选项卡。
4. 在“**检测到 IOC 后的操作**”下，选择“**在发现 IOC 后采取响应操作**”和“**从网络隔离计算机**”复选框。
5. 保存更改。

结果，当检测到 IOC 时，应用程序从网络隔离计算机以防止威胁扩散。

您可以配置自动网络隔离，使其在一定时间后禁用。默认情况下，应用程序在网络隔离启用 8 小时后将其禁用。您还可以手动禁用网络隔离（请参阅下面的说明）。禁用网络隔离后，计算机可以在网络上不受限制地活动。

如何配置自动网络隔离禁用的时间段

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**遥测采集服务器** → **Endpoint Detection and Response (Industrial CyberSecurity)**”并点击“**配置**”。
5. 在**网络隔离**块，单击**配置计算机解锁设置**。
6. 这将打开一个窗口，在此窗口中，选择“**自动解锁隔离的计算机于**”复选框并输入自动关闭网络隔离的延时。
7. 保存更改。

手动网络隔离模式

您可以手动启用或禁用网络隔离。您可以使用 Kaspersky Security Center 管理控制台中的计算机属性配置手动网络隔离模式。

您可以通过以下方式启用网络隔离：

- 在警报详细信息中（仅适用于 EDR Optimum）。
  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详细信息的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。
- 使用本地应用程序设置。

如何手动启用计算机网络隔离

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 选择要为其配置本地应用程序设置的计算机。
   这将打开计算机的属性。
3. 选择**应用程序**选项卡。
4. 单击“**Kaspersky Industrial CyberSecurity for Nodes**”。
   这将打开本地应用程序设置。

5. 选择**应用程序设置**选项卡。
6. 转到“**遥测采集服务器** → Endpoint Detection and Response (Industrial CyberSecurity)”并点击“**配置**”。
7. 在“**网络隔离**”下，点击“**从网络隔离计算机**”按钮。
8. 单击“**确定**”。

您可以配置自动网络隔离，使其在一定时间后禁用。默认情况下，应用程序在网络隔离启用 8 小时后将其禁用。禁用网络隔离后，计算机可以在网络上不受限制地活动。

如何配置手动网络隔离禁用的时间段

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 选择要为其配置本地应用程序设置的计算机。
   这将打开计算机的属性。
3. 选择**任务**选项卡。
   这将显示计算机上可用的任务列表。
4. 选择“**网络隔离**”任务。
5. 选择**应用程序设置**选项卡。
6. 这将打开一个窗口；在此窗口中，指定关闭网络隔离的延迟。
7. 保存更改。

如何手动禁用计算机网络隔离

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 选择要为其配置本地应用程序设置的计算机。
   这将打开计算机的属性。
3. 选择**应用程序**选项卡。
4. 单击“Kaspersky Industrial CyberSecurity for Nodes”。
   这将打开本地应用程序设置。
5. 选择**应用程序设置**选项卡。
6. 转到“**遥测采集服务器** → Endpoint Detection and Response (Industrial CyberSecurity)”并点击“**配置**”。

7. 在“**网络隔离**”下，点击“**解除阻止从网络隔离的计算机**”按钮。

8. 保存更改。

您还可以使用**命令行**在本地禁用网络隔离。

禁用计算机的网络隔离或显示组件的当前设置。组件设置还包括添加到排除项的网络连接列表。

要运行命令，请转到 kavshell.exe 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法：

```
KAVSHELL isolation [/disable] [/show] [/login=<当前用户账户的名称>] [/PWD=</login 密码或 KLAdmin 密码（如果未指定 /login）>]
```

命令返回值：

- -1：计算机上安装的应用程序版本不支持该命令。
- 0：命令成功完成。
- 1：表示未将强制参数传递给命令。
- 2：一般错误。
- 4：语法错误。
- 9 - 错误操作（例如，在组件已禁用时尝试禁用该组件）。

网络隔离排除项

您可以配置网络隔离排除项。当启用网络隔离时，符合配置的规则的网络连接不会在计算机上被阻止。

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，排除项包括由规则组成的网络配置文件，这些规则确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备能够不间断地继续运行。您还可以管理标准网络配置文件的设置或手动指定排除项（参见以下说明）。

仅当应用程序作为威胁响应的一部分自动启用了网络隔离时，才会应用策略设置中配置的排除项。仅当在 Kaspersky Security Center 控制台的“计算机属性”中或警报详情中手动启用网络隔离时，才会应用“计算机属性”中配置的排除项。

活动策略不会阻止应用计算机属性中配置的网络隔离排除项，因为这些设置应用于不同的场景。

如何添加自动网络隔离排除项

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**遥测采集服务器** → Endpoint Detection and Response (Industrial CyberSecurity)”并点击“**配置**”。
5. 在**网络隔离排除项**块，单击**排除项**。
6. 这将打开一个窗户，在此窗口中，单击“**从配置文件添加**”，然后选择用于配置排除项的标准网络配置文件。
   配置文件中的网络连接将被添加到网络隔离排除项列表中。您可以查看网络连接的属性。如有必要，您可以编辑网络连接的设置。
7. 如有必要，请手动添加网络隔离排除项。为此，在包含排除项列表的窗口中，单击“**添加**”并手动指定网络排除项设置。
8. 保存更改。

如何添加手动网络隔离排除项

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 选择要为其配置本地应用程序设置的计算机。
   这将打开计算机的属性。
3. 选择**任务**选项卡。
   这将显示计算机上可用的任务列表。
4. 选择“**网络隔离**”任务。
5. 选择**应用程序设置**选项卡。
6. 这将打开一个窗口；在该窗口中，选择“**排除项**”。
7. 这将打开一个窗户，在此窗口中，单击“**从配置文件添加**”，然后选择用于配置排除项的标准网络配置文件。
   配置文件中的网络连接将被添加到网络隔离排除项列表中。您可以查看网络连接的属性。如有必要，您可以编辑网络连接的设置。
8. 如有必要，请手动添加网络隔离排除项。为此，在包含排除项列表的窗口中，单击“**添加**”并手动指定网络排除项设置。
9. 保存更改。

您还可以使用**命令行**在本地查看网络隔离排除项列表。为此，计算机必须被隔离。

禁用计算机的网络隔离或显示组件的当前设置。组件设置还包括添加到排除项的网络连接列表。

要运行命令，请转到 kavshell.exe 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法：

```
KAVSHELL isolation [/disable] [/show] [/login=<当前用户账户的名称>] [/PWD=</login 密码或 KLAdmin 密码（如果未指定 /login）>]
```

命令返回值：

- -1：计算机上安装的应用程序版本不支持该命令。
- 0：命令成功完成。
- 1：表示未将强制参数传递给命令。
- 2：一般错误。
- 4：语法错误。
- 9 - 错误操作（例如，在组件已禁用时尝试禁用该组件）。

Cloud Sandbox

Cloud Sandbox 是一种可以检测计算机上高级威胁的技术。Kaspersky Industrial CyberSecurity for Nodes 自动将检测到的文件转发到 Cloud Sandbox 进行分析。Cloud Sandbox 在隔离的环境中运行这些文件，以识别恶意活动并决定其信誉。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 Industrial CyberSecurity for Nodes 将在检测到此文件的所有计算机上执行适当的操作以消除此威胁。

要运行 Cloud Sandbox，您必须启用卡巴斯基安全网络。

如果您使用的是 卡巴斯基私有安全网络，则 Cloud Sandbox 技术不可用。

Cloud Sandbox 技术是永久启用的，可供所有卡巴斯基安全网络用户使用，无论他们使用的授权许可类型如何。如果您已经部署了 Endpoint Detection and Response 解决方案，您可以为 Cloud Sandbox 检测到的威胁启用单独的计数器。Cloud Sandbox 检测到的威胁计数器显示在 **Kaspersky Industrial CyberSecurity for Nodes** 节点工作区的应用程序控制台树中。使用 Cloud Sandbox 技术的威胁检测统计数据也将显示在 Kaspersky Security Center 管理控制台中的“*威胁报告*”中。

授权 EDR Optimum

Kaspersky Industrial CyberSecurity for Nodes 支持 Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) 的功能。为此，您必须购买授权许可才能使用该解决方案。添加单独的 EDR Optimum 插件密钥后，EDR Optimum 功能可用。

因此，计算机上将添加两个密钥：Kaspersky Industrial CyberSecurity for Nodes 密钥和 EDR Optimum 密钥。必须第一个添加 Kaspersky Industrial CyberSecurity for Nodes 密钥。

EDR Optimum 解决方案的激活方式与 Kaspersky Industrial CyberSecurity for Nodes 相同。您可以使用 *使用码激活* 任务或使用自动密钥分发功能来添加密钥。如果选中相关复选框，授权许可密钥将作为第二个活动密钥或备用密钥添加到应用程序中。

Endpoint Detection and Response Expert (on-premise)

Kaspersky Industrial CyberSecurity for Nodes 支持与 Kaspersky Endpoint Detection and Response Expert (on-premise) 解决方案集成。Kaspersky Endpoint Detection and Response Expert (on-premise) 是一款企业网络安全解决方案，其中包括卡巴斯基应用程序，可帮助组织防御大多数类型的网络风险并涵盖最重要的威胁传播场景。EDR Expert (on-premise) 组件部署在 Open Single Management Platform (OSMP) 上。该平台可在单一界面中运行跨平台方案，并允许将卡巴斯基应用程序与第三方应用程序集成到全面的安全系统中。

解决方案的核心要素之一是 *SIEM*。SIEM 跟踪来自所有组件的事件，并使用供应商和用户定义的规则将这些事件相互关联起来。EDR Expert (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，并允许使用统一的调查图来调查事件，该调查图结合了 EDR Expert (on-premise) 中采集的所有事件，包括来自卡巴斯基应用程序和第三方信息安全产品的事件。

对于高级事件的响应，EDR Expert (on-premise) 使用预设方案和用户自定义方案。您还可以使用来自第三方应用程序的响应操作以及涉及多个应用程序的响应方案。

威胁情报工具

Kaspersky Endpoint Detection and Response 使用以下威胁情报工具：

- 与卡巴斯基威胁情报门户集成，该系统包含并显示有关文件和网址信誉的信息。
- 卡巴斯基威胁数据库。
- 卡巴斯基安全网络云服务基础设施，提供对 Kaspersky 知识库中实时文件、网站和软件信誉信息的访问。使用卡巴斯基安全网络的数据可确保卡巴斯基应用程序对威胁做出更快响应，提高一些保护组件的性能，并降低误报可能性。

解决方案的工作原理

Kaspersky Industrial CyberSecurity for Nodes 安装在组织 IT 基础设施中包含的运行 Windows 的单个计算机上。应用程序不断监控进程、打开的网络连接和正在修改的文件。有关计算机上的事件、应用程序检测到的威胁以及处理这些威胁的结果的信息被发送到 EDR Expert（on-premise）服务器。

EDR Expert (on-premise) 集成在 Kaspersky Security Center Web 控制台中配置。然后使用 Open Single Management Platform (OSMP) 管理内置代理或端点代理配置，包括运行任务、管理隔离对象、查看报告和其他操作。

与 Kaspersky Anti Targeted Attack Platform 集成的 Kaspersky Industrial CyberSecurity for Nodes 配置

以下配置可用于使用 EDR Expert (on-premise)：

- [KICS+内置代理]。在此配置中，Kaspersky Industrial CyberSecurity for Nodes 既充当确保计算机安全的应用程序，又充当使用 EDR Expert (on-premise) 的应用程序。从 4.5 版本开始，内置代理支持与 EDR Expert (on-premise) 集成。
- [第三方 EPP+端点代理配置]。在此配置中，IT 基础设施的安全性由第三方端点保护平台（EPP）提供。Kaspersky Industrial CyberSecurity for Nodes 在端点代理配置中提供了与 EDR Expert（on-premise）的集成。从 4.5 版本开始，Endpoint Agent 配置支持与 EDR Expert (on-premise) 集成。

配置 EDR Expert (on-premise) 集成

> “Endpoint Detection and Response (Industrial CyberSecurity)”和“Endpoint Detection and Response Expert (on-premise)”组件彼此不兼容。

Endpoint Detection and Response Expert (on-premise) 必须满足以下条件才能工作：

- OSMP（Open Single Management Platform 已安装。
- 应用程序已激活，授权许可涵盖了该功能。
- Endpoint Detection and Response Expert (on-premise) 组件被开启。
- 确保 EDR Expert (on-premise) 运行的应用程序组件已启用并可运行。以下组件确保 EDR Expert (on-premise) 的运行：
  - 实时文件保护
  - 漏洞利用防御
  - 反加密
  - AMSI 保护
  - 卡巴斯基安全网络

设置 EDR Expert (on-premise) 集成涉及以下步骤：

1. **安装“Endpoint Detection and Response Expert (on-premise)”组件**

   在安装包设置或安装向导中，或通过更改 Windows 控制面板中的应用程序程序组件集，在必须选择要安装的应用程序组件的步骤中，选择以下内容：

   - **完整功能 → Endpoint Agent → Endpoint Detection and Response Expert (on-premise)**，对于内置代理
   - **Endpoint Agent → Endpoint Detection and Response Expert (on-premise)**，对于端点代理配置

要完成更改应用程序组件集，您必须重新启动计算机。

2 Endpoint Detection and Response Expert (on-premise) 激活

您需要为 EDR Expert (on-premise)（Kaspersky Endpoint Detection and Response Expert (on-premise) 加载项）购买单独的授权许可。

独立 Endpoint Detection and Response Expert (on-premise) 功能的授权与 Kaspersky Industrial CyberSecurity for Nodes 的授权相同。该功能将在为 Kaspersky Endpoint Detection and Response Expert (on-premise) 添加单独密钥后可用。因此，计算机上将添加两个密钥：Kaspersky Industrial CyberSecurity for Nodes 密钥和 Endpoint Detection and Response Expert (on-premise) 密钥。

确保授权许可中包含“Endpoint Detection and Response Expert (on-premise)”功能。

3 连接到遥测采集服务器和响应服务器

Kaspersky Endpoint Detection and Response Expert (on-premise) 需要 Kaspersky Endpoint Security 与两台服务器之间受信任连接：

- *遥测采集服务器* 是 SIEM 解决方案的一部分，用于收集、规范化、关联、分析和存储有关计算机上发生的事件的信息。
- *响应服务器* 是一个用于接收和扫描数据、研究对象行为和发布此类研究结果的服务器。

要配置可信连接，您必须使用 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premise) 帮助中的说明）。然后您必须将 TLS 证书添加到 Kaspersky Industrial CyberSecurity for Nodes（参见下面的说明）。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 仅检查服务器 TLS 证书。为了使连接更安全，您可以额外启用服务器上的计算机验证（双向身份验证）。要启用此验证，您必须在服务器和 Kaspersky Industrial CyberSecurity for Nodes 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*加密容器*是带有证书和私钥的 PFX 存档。您可以在 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premise) 帮助中的说明）。

如何使用 Web Console 将 Kaspersky Industrial CyberSecurity for Nodes 计算机连接到 EDR Expert (on-premise)

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**遥测采集服务器**”部分。
5. 在“Endpoint Detection and Response Expert (on-premise)”块中单击“**配置**”按钮。
   “Endpoint Detection and Response Expert (on-premise)”窗口将打开。
6. 选择**启用 Endpoint Detection and Response Expert (on-premise)**复选框。
7. 选择“**Endpoint Detection and Response Expert (版本 8.0 或后续版本)**”模式。

8. 配置遥测采集服务器连接：

   a. 在“**连接到遥测采集服务器**”区域，单击“**KATA 服务器连接设置**”链接。

   b. 在打开的窗口中，配置遥测采集服务器的连接：

      - “**超时(秒)**”。最大服务器响应超时。当超时用完时，Kaspersky Industrial CyberSecurity for Nodes 会尝试连接到不同的服务器。
      - “**服务器 TLS 证书**”。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premise) 帮助中的说明）。
      - “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premise) 帮助中的说明）。配置服务器设置后，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。

        加密容器必须受密码保护。无法添加密码为空的加密容器。

   c. 单击“**确定**”。

   d. 添加遥测采集服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

      您可以添加多个遥测采集服务器地址。Kaspersky Industrial CyberSecurity for Nodes 尝试在第一个 IP 地址处与服务器建立连接。如果连接建立失败，Kaspersky Industrial CyberSecurity for Nodes 将尝试在列表中的第二个 IP 地址处建立连接，以此类推。

   e. 如果有必要，配置遥测。

9. 配置响应服务器连接：

   a. 在“**连接到响应服务器**”块中，配置“**发送同步请求到服务器的间隔(分钟)**”设置。发送到服务器的同步请求的频率。在同步过程中，Kaspersky Industrial CyberSecurity for Nodes 接收威胁响应任务并发送任务结果。

   b. 单击**KATA 服务器连接设置**链接。

   c. 在打开的窗口中，配置响应服务器的连接：

      - “**超时(秒)**”。最大服务器响应超时。当超时用完时，Kaspersky Industrial CyberSecurity for Nodes 会尝试连接到不同的服务器。
      - “**服务器 TLS 证书**”。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premise) 帮助中的说明）。

- “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premise) 帮助中的说明）。配置服务器设置后，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。

  > 加密容器必须受密码保护。无法添加密码为空的加密容器。

d. 单击“**确定**”。

e. 添加响应服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

您可以添加多个遥测采集服务器地址。Kaspersky Industrial CyberSecurity for Nodes 尝试在第一个 IP 地址处与服务器建立连接。如果连接建立失败，Kaspersky Industrial CyberSecurity for Nodes 将尝试在列表中的第二个 IP 地址处建立连接，以此类推。

10. 保存更改。要在计算机上应用该策略，请关闭锁 。

因此，该计算机被添加到 Open Single Management Platform (OSMP) 中。

配置 EDR Expert (on-premise) 遥测设置

*遥测*是受保护计算机上发生的事件的列表。Kaspersky Industrial CyberSecurity for Nodes 在同步期间分析遥测数据并将其发送到遥测采集服务器。遥测事件几乎连续不断地到达服务器。当满足以下任一条件时，Kaspersky Industrial CyberSecurity for Nodes 启动与服务器的同步：

- 同步间隔已用完。
- 缓冲区中的事件数超过上限。

因此，默认情况下，应用程序每 30 秒或每当缓冲区包含 1024 个事件时同步一次。您可以在 Kaspersky Industrial CyberSecurity for Nodes 策略中配置同步行为并选择最佳值以匹配您的网络负载（请参阅下面的说明）。

如果 Kaspersky Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 可能会跳过一些事件。要启用此功能，您可以优化事件传输设置，例如，设置每小时最大事件数值（请参阅下面的说明）。

要配置遥测设置，请执行下列步骤：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**遥测采集服务器**”部分。

5. 在“Endpoint Detection and Response Expert (on-premise)”块中单击“**配置**”按钮。

   “Endpoint Detection and Response Expert (on-premise)”窗口将打开。

6. 确保在“**数据传输设置**”块中，“**将遥测发送到遥测采集服务器**”复选框被选中。

7. 如有必要，选中“**仅发送带有 IOA 的遥测**”复选框。*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。

8. 如果需要，请在“**数据传输设置**”块配置与服务器设置的同步：

   - “**最大事件传输延迟(秒)**”。应用程序在同步间隔到期后与服务器同步以发送事件。默认设置是 30 秒。
   - “**管理作为事务一部分传输的事件包的数量**”。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。

9. 如有必要，在“**限制**”块选择“**启用限制**”复选框。

   该功能有助于优化服务器上的负载。如果选中该复选框，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 Industrial CyberSecurity for Nodes 将停止发送事件。

0. 配置用于将事件发送到服务器的优化设置：

   - “**每小时最大事件数**”。如果事件流超过配置的每小时事件数限制，应用程序会分析遥测数据流并限制事件的发送。Kaspersky Industrial CyberSecurity for Nodes 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。
   - “**超出事件限制的百分比**”。该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Industrial CyberSecurity for Nodes 将恢复发送事件。默认设置为 15%。

1. 在“**连接到响应服务器**”块中，为“**发送同步请求到服务器的间隔(分钟)**”参数输入一个值。

2. 发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。

3. 保存更改。要在计算机上应用该策略，请关闭锁 🔒。

EDR Expert (on-premise) 遥测排除项

要提高性能并优化到遥测收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。

如果存储的过滤规则数量超过了支持的限制，则 EDR Expert (on-premise) 事件过滤规则将不会从策略传递到运行 Kaspersky Industrial CyberSecurity for Nodes 4.5 或更早版本的受管设备。应用程序将显示相应的警告。

要在 Web Console 中创建遥测排除项：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**补充**区域。
5. 在“**遥测设置**”块中单击“**配置**”按钮。
6. 选择**EDR Expert (on-premise) 遥测**选项卡。
7. 在“**常规排除项**”块中单击“**添加**”按钮。
   “**添加排除规则**”窗口将打开。
8. 如有必要，更改规则状态。默认启用该规则。
9. 输入规则的名称。
0. 选择触发规则时要执行的操作：
   - “**不采集**”。被过滤的事件将从发送的遥测数据中排除。
   - “**排除 IOA**”。IOA 规则触发器事件将从发送的遥测数据中排除。
1. 如果选中“**排除 IOA**”选项，请指定要添加到排除项中的 IOA 规则：
   - “**全部排除**”。当满足指定条件时，应用程序将从遥测数据中排除基于所有 IOA 规则生成的事件。
   - “**按 GUID 排除**”。指定 IOA 规则的 GUID。您可以指定多个由“`,`”符号分隔的 GUID。有关 IOA 规则的详细信息，请参阅 EDR Expert (on-premise) 帮助。
2. 指定过滤条件：
   a. 选择要过滤的字段名称。
   b. 选择一个运算符（见下表），并指定要与事件字段值进行比较的值。

条件运算符列表

运算符	描述
<	如果字段值小于条件中指定的值，则该事件将被过滤出来。
⩽	如果字段值小于或等于条件中指定的值，则该事件将被过滤出来。
=	如果字段值等于条件中指定的值，则该事件将被过滤出来。
⩾	如果字段值大于或等于条件中指定的值，则该事件将被过滤出来。
>	如果字段值大于条件中指定的值，则该事件将被过滤出来。
≠	如果字段值与条件中指定的值不相等，则该事件将被过滤出来。
类似	如果字段值与条件中指定的掩码匹配，则该事件将被过滤出来。输入掩码时，应用程序支持 `*` 字符和 `?` 字符。
不类似	如果字段值与条件中指定的掩码不匹配，则该事件将被过滤出来。输入掩码时，应用程序支持“`*`”字符和“`?`”字符：
之一	如果字段值与条件中指定的列表中的某个值匹配，则该事件被视为已过滤。

运算符	描述
没有一个	如果字段值与列表中指定的任何值都不匹配，则该事件被视为已过滤。
类似其中之一	如果字段值与条件中指定的某个掩码匹配，则该事件将被过滤出来。输入掩码时，Kaspersky Endpoint Security 支持 * 字符和 ? 字符。
不类似其中之一	如果字段值与条件中指定的任何掩码都不匹配，则该事件将被过滤出来。输入掩码时，Kaspersky Endpoint Security 支持 * 字符和 ? 字符。
存在	如果条件中指定的字段包含在事件中，则该事件将被过滤出来。
不存在	如果条件中指定的字段不包含在事件中，则该事件将被过滤出来。
包含	如果条件中指定的值包含在字段的值中，则该事件将被过滤出来。
等于	如果字段值等于条件中指定的值，则该事件将被过滤出来。检查不区分大小写。
按位和	如果字段值与指定条件值之间的 Bitwise AND (&) 运算结果为 1，则该事件将被过滤出来。

3. 如有必要，您可以通过添加多个过滤条件和条件组来创建复杂的过滤条件。您还可以向条件组中添加嵌套条件和条件组。您可以使用以下运算符：

   - **且** – 过滤器会选择符合所有指定条件的事件。
   - **或** – 过滤器会选择符合指定条件之一的事件。
   - **非**（要使用此运算符，请选择 **在此之前加非** 选项）– 该过滤器选择不匹配所有指定条件的事件。

   一级条件和条件组通过 **且** 运算符组合。

4. 如果计算机由 OSMP 管理，您可以检查已创建的过滤规则。要执行检查，请单击“**检查规则**”按钮。

   在打开的“Threat hunting”窗口中，将显示使用创建的规则过滤的事件表。更多详情请参见 EDR Expert (on-premise) 帮助。

5. 如有必要，在“**所有事件类型**”下，按事件类型添加遥测排除项：

   a. 点击事件类型名称。

   b. 单击打开的窗口中的“**手动设置**”按钮。

   c. 如有必要，请使用“**发送事件**”开关配置所选事件类型的遥测发送。默认情况下，所有事件类型均启用遥测数据发送。

   d. 在“**排除规则**”块中单击“**添加**”按钮。

   “**添加排除规则**”窗口将打开。

   e. 对每条新增规则，请按照步骤 7-13 操作。

6. 对于某些事件类型，您还可以添加包含规则来扩展收集到的遥测数据：

   a. 在“**排除规则**”块中单击“**添加**”按钮。

   “**添加包含规则**”窗口将打开。

   b. 输入规则的名称。

   c. 在“**条件**”块中，在显示的字段中输入值。可用字段类型取决于所选事件。

排除规则优先于包含规则。

7. 保存更改。要在计算机上应用该策略，请关闭锁 。

导出和导入 EDR Expert（on-premise）事件过滤器

可以将排除列表导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。还可以使用导出和导入功能备份事件过滤器或将列表迁移到其他服务器。

如何在 Kaspersky Security Center 管理控制台中导出和导入事件过滤器

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，转到“**补充**”区域。
4. 在“**EDR Expert（on-premise）的遥测设置**”块中单击“**设置**”按钮。
5. 导出 EDR Expert（on-premise）遥测设置：
   a. 单击“**导出**”。
   b. 在打开的窗口中，指定您要将设置导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。
   c. 保存文件。
   Kaspersky Industrial CyberSecurity for Nodes 会将设置导出到 JSON 文件。
6. 要导入遥测设置：
   a. 单击“**导入**”。
   b. 选择要从中导入事件过滤器的 JSON 文件。
   c. 打开文件。
   d. 在显示的对话框中，确认修改 EDR Expert（on-premise）遥测设置。
7. 点击“**确定**”保存更改。

如何在 Web Console 中导出和导入事件过滤器

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。
4. 转到“**补充 → 遥测设置**”并点击“**配置**”按钮。
5. 选择**EDR Expert (on-premise) 遥测**选项卡。
6. 点击 **导出** 导出 EDR Expert (on-premise) 遥测设置。

   Kaspersky Industrial CyberSecurity for Nodes 在标准下载文件夹中保存了一个名为 filterExport.json 的文件。
7. 要导入遥测设置：
   a. 单击“**导入**”。
   b. 选择要从中导入事件过滤器的 JSON 文件。
   c. 打开文件。
   d. 选择您希望如何导入事件过滤规则：添加到现有规则或丢弃现有规则并用新规则替换。
   e. 保存更改。

      JSON 文件中包含的规则将显示在列表中。

[如何在 Application Console 中导出和导入事件过滤器]

1. 在应用程序控制台树中，选择“**遥测设置**”节点。
2. 在“**EDR Expert (on-premise) 的遥测设置**”块中单击“**设置**”按钮。
3. 导出 EDR Expert (on-premise) 遥测设置：
   a. 单击“**导出**”。
   b. 在打开的窗口中，指定您要将设置导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。
   c. 保存文件。

   Kaspersky Industrial CyberSecurity for Nodes 会将设置导出到 JSON 文件。
4. 要导入遥测设置：
   a. 单击“**导入**”。
   b. 选择要从中导入事件过滤器的 JSON 文件。
   c. 打开文件。
   d. 在显示的对话框中，确认修改 EDR Expert（on-premise）遥测设置。
5. 点击“**确定**”保存更改。

您还可以在命令行上导出或导入事件过滤器。

YARA 扫描

*YARA 扫描*是 Kaspersky Industrial CyberSecurity for Nodes 使用 YARA 文件在设备上查找恶意的活动特征的过程。扫描在本地磁盘上递归执行。不支持扫描网络、可移动和云资源。

要执行 YARA 扫描，您需要一个 EDR Expert (on-premise) 的有效授权许可。

*YARA 文件*是包含 YARA 规则的 YARA 或 YAR 扩展名的文件。*YARA 规则*描述针对企业 IT 基础设施的针对性攻击和入侵的特征。Kaspersky Industrial CyberSecurity for Nodes 使用这些规则来扫描对象。如果对象与规则匹配，分析器就会诊断出感染并在日志中记录详细信息。

请注意使用 YARA 文件时的以下要求和限制：

- Kaspersky Industrial CyberSecurity for Nodes 支持带有 YARA 或 YAR 扩展名的 YARA 文件，这些文件遵循 YARA 4.2.3 开放标准，用于描述入侵指标。
- 如果您使用 Kaspersky Industrial CyberSecurity for Nodes 不支持或包含语法错误的 YARA 文件运行 YARA 扫描，则扫描将中止并显示相应的错误通知。
- YARA 扫描任务中使用的 YARA 文件的 ID 必须是唯一的。如果存在具有相同标识符的 YARA 文件，则可能会影响任务执行结果。
- 在找到 128 个符合 YARA 规则中描述的标记的匹配项后，YARA 扫描结束。有必要限制 YARA 扫描任务报告中的条目数量，以便于分析，并防止由于不精确制定的 YARA 规则而产生大量匹配而导致报告变得太大。

我们建议每个 YARA 文件创建一条规则。这种方法提高了 YARA 扫描结果的可读性。

您只能在命令行上运行 YARA 扫描。

YARA 扫描可能需要很长时间。根据磁盘大小、任务设置、磁盘上的对象数量，YARA 扫描可能花费几分钟到几小时。扫描正在进行时，应用程序不会显示进度指示器。您不能中断或取消 YARA 扫描。我们建议等到 YARA 扫描的结果准备好。

要运行 YARA 扫描：

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，命令提示符 cmd.exe）。
2. 使用 `cd` 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如，输入命令 `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0` 并按 **ENTER**。
3. 执行以下命令：

   `KAVSHELL YARA <YARA 文件的完整路径>|path=<包含 YARA 文件的文件夹路径> [/<附加参数>]`

必需参数	描述
/< YARA 文件的完整路径 >	您要用于扫描的 YARA 文件的完整路径。您可以指定多个由空格分隔的路径。 例如，/C:\Users\Admin\Desktop\YARA\file.yar C:\Users\Admin\Desktop\YARA\file1.yar。
/path=< YARA 文件的文件夹路径 >	您要用于扫描的 YARA 文件的文件夹路径。 例如，/path=C:\Users\Admin\Desktop\YARA。

可选参数	描述
/fastscan=<on|off>	快速 YARA 扫描。对于每个对象，应用程序都会记录一次检测到的指标。应用程序隐藏日志中检测到的指标的重复项。快速 YARA 扫描可以更快地扫描大文件。 如果未指定此参数，应用程序将运行标准 YARA 扫描。在这种模式下，应用程序反映日志中检测到的指标的重复项。
/maxrules=< 最大扫描规则数 >	当达到唯一触发规则的限制时，应用程序将停止 YARA 扫描。 如果未指定此参数或将其设置为“0”，应用程序执行无限制的 YARA 扫描。
/timeout=< N 秒 >	YARA 扫描持续时间的限制（以秒为单位）。此后，应用程序将停止 YARA 扫描。 如果未指定此参数或将其设置为“0”，应用程序执行无限制的 YARA 扫描。
/recursive=<on|off>	此参数启动对 /scanfolders 参数设置的范围内的子文件夹的递归扫描。
/scanfolders=< YARA 扫描文件夹的路径 >	此参数启动对指定文件夹列表中的文件的 YARA 扫描。您可以指定多个由空格分隔的路径。 您可以使用 ？ 和 * 字符输入掩码，以及 **@ 字符作为带有参数值的文件的链接**。 具有参数值的文件是一个 UTF-8 文本文件，其中包含要使用相应命令行参数处理的对象列表。 例子： my_rules.txt 文件包含两行： • C:\trusted*.* • *.abc Rules2.txt 包含一行： • img_*.jpg 如果您使用 /scan-folders /exclude *.txt @my_rules.txt *.xml @rules2.txt 参数运行扫描，将扫描所有磁盘上的所有文件，但带有 TXT 扩展名的文件、C:\trusted 文件夹中的文件、带有 ABC 扩展名的文件、带有 XML 扩展名的文件以及与 img_*.jpg 掩码匹配的文件除外。 如果未指定此参数，则对除网络、云和可移动驱动器之外的所有本地磁盘递归执行 YARA 扫描。
/scanmemory=<on|off>	扫描所有正在运行的进程的内存。
/scanprocess=< 进程可执行文件的完整路径 >	仅扫描列出的进程的内存。指定以空格分隔的进程可执行文件的完整路径。您也可以使用 ？ 和 * 字符来输入掩码。
/maxsize=< 大小（以字节为单位） >	YARA 扫描的文件大小限制。应用程序会跳过较大的文件。

/excludes=< 从 YARA 扫描中排除的对象的路径 >	从 YARA 扫描中排除文件和文件夹。您可以指定多个由空格分隔的对象。 您可以使用 ? 和 * 字符输入掩码，以及 **@ 字符作为带有参数值的文件的链接**。 具有参数值的文件是一个 UTF-8 文本文件，其中包含要使用相应命令行参数处理的对象列表。 例子： my_rules.txt 文件包含两行： • C:\trusted*.* • *.abc Rules2.txt 包含一行： • img_*.jpg 如果您使用 /scan-folders /exclude *.txt @my_rules.txt *.xml @rules2.txt 参数运行扫描，将扫描所有磁盘上的所有文件，但带有 TXT 扩展名的文件、C:\trusted 文件夹中的文件、带有 ABC 扩展名的文件、带有 XML 扩展名的文件以及与 img_*.jpg 掩码匹配的文件除外。 您可以指定以下对象： • 文件名 • 文件路径 • 文件名称掩码 • 文件路径掩码 您必须同时使用 scanfolders 参数指定排除项。 例如： /scanfolders=C:*.* /excludes=readme.txt C:\trusted*.* *.xml 告诉应用程序在 C: 驱动器的根文件夹中运行 YARA 扫描，排除 readme.txt 文件、C:\trusted 文件夹中的所有文件以及所有具有 XML 扩展名的文件。
/logfolder=< 扫描结果保存路径 >	如果您指定文件夹路径，应用程序会将扫描结果保存在指定路径下名为 yara_<计算机名称>_<扫描完成时间>.txt 的文件中。 如果您指定特定 TXT 文件的路径，应用程序会将扫描结果保存在该文件中。 例如：/logfolder=C:\test 或 /logfolder=C:\test\abc.txt。 扫描结果将输出到命令行，无论是否指定了 /logfolder 选项。

命令返回值：

- -1：计算机上安装的应用程序版本不支持该命令。
- 0：命令成功完成。
- 1：表示未将强制参数传递给命令。
- 2：一般错误。
- 4：语法错误。
- 5：找不到参数中指定的一个或多个 YARA 规则文件。

如果命令已成功完成（返回值 0）并检测到 YARA 规则中描述的签名，应用程序向命令行输出以下任务结果信息：

Offset	被扫描对象的偏移。
Data	应用程序在 YARA 扫描中寻找的签名。
Object Name	被扫描对象的名称。
Rule Name	应用程序用于 YARA 扫描的规则的名称。

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform 是一种用于保护组织 IT 基础设施并及早发现零日攻击、针对性攻击和高级持续性威胁（以下也称为 APT）等威胁的解决方案。

Kaspersky Anti Targeted Attack Platform 解决方案包括三个功能单元：

- Kaspersky Anti Targeted Attack（以下也称为 KATA） – 保护企业的 IT 基础设施外围。
- Kaspersky Endpoint Detection and Response（以下也称为 KEDR） – 保护组织本地网络中的计算机。
- Network Detection and Response，保护企业局域网。

有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

解决方案的工作原理

Kaspersky Industrial CyberSecurity for Nodes 安装在组织 IT 基础设施中包含的运行 Windows 的单个计算机上。应用程序不断监控进程、打开的网络连接和正在修改的文件。有关计算机上的事件、应用程序检测到的威胁以及处理这些威胁的结果的信息被发送到 Central Node 服务器。

与 KEDR (KATA) 的集成在 Kaspersky Security Center 管理控制台或 Kaspersky Security Center Web Console 中进行配置。然后使用 Kaspersky Anti Targeted Attack Platform 控制台管理内置代理或 Endpoint Agent 配置，包括运行任务、管理隔离对象、查看报告和其他操作。

与 Kaspersky Anti Targeted Attack Platform 集成的 Kaspersky Industrial CyberSecurity for Nodes 配置

Kaspersky Industrial CyberSecurity for Nodes 可以与作为 Kaspersky Anti Targeted Attack Platform 解决方案的一部分的 Kaspersky Endpoint Detection and Response 集成。有以下配置：

- [KICS+内置代理]。在此配置中，Kaspersky Industrial CyberSecurity for Nodes 既充当确保计算机安全的应用程序，又充当使用 KEDR 的应用程序。从 4.5 版开始，Kaspersky Industrial CyberSecurity for Nodes 中就有内置代理。
- [第三方 EPP+端点代理配置]。在此配置中，IT 基础设施的安全性由第三方端点保护平台（EPP）提供。Kaspersky Industrial CyberSecurity for Nodes 在端点代理配置中提供了与 KEDR 的集成。从 4.5 版开始，Kaspersky Industrial CyberSecurity for Nodes 中提供了端点代理配置。

对以前版本的 Kaspersky Industrial CyberSecurity for Nodes 的支持

Kaspersky Industrial CyberSecurity for Nodes 4.5 支持使用内置代理或端点代理配置与 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案的集成；您无需安装 Kaspersky Endpoint Agent。

如果您使用 Kaspersky Industrial CyberSecurity for Nodes 4.5 之前的版本与 Kaspersky Anti Targeted Attack Platform (EDR) 集成，则必须单独安装 Kaspersky Endpoint Agent。

配置 KATA 集成

Endpoint Detection and Response (KSC) 和 Endpoint Detection and Response Expert (on-premise) 的组件彼此不兼容。

Kaspersky Industrial CyberSecurity for Nodes 内置代理与 KATA 集成必须满足以下条件：

- 必须在企业 IT 基础设施中部署 Kaspersky Anti Targeted Attack Platform 5.0 或更高版本。
- 必须在企业 IT 基础设施中部署 Kaspersky Security Center 14.2 或更高版本。
- 向 KATA 发送数据的应用程序组件必须已启用并正常运行：
  - 实时文件保护。
  - 漏洞利用防御。
  - 反加密。
  - AMSI 保护。
  - 卡巴斯基安全网络。

要将 Endpoint Agent 配置与企业 IT 基础架构中的 KATA 集成，必须部署以下内容：

- Kaspersky Anti Targeted Attack Platform 版本 5.0 或更高版本。
- Kaspersky Security Center 版本 14.2 或更高版本。

设置 KATA 集成涉及以下步骤：

1. **安装“Endpoint Detection and Response Expert (on-premise)”组件**

   在安装包设置或安装向导中，或通过更改 Windows 控制面板中的应用程序程序组件集，在必须选择要安装的应用程序组件的步骤中，选择以下内容：

   - **完整功能 → 端点代理 → Endpoint Detection and Response Expert (on-premise)**，对于内置代理
   - **端点代理 → Endpoint Detection and Response Expert (on-premise)**，对于端点代理配置

   要完成更改应用程序组件集，您必须重新启动计算机。

2. **Endpoint Detection and Response Expert (on-premise) 激活**

   您需要为 KATA（例如，Kaspersky Endpoint Detection and Response （KATA）加载项）购买单独的授权许可。

   独立 Endpoint Detection and Response Expert (on-premise) 功能的授权与 Kaspersky Industrial CyberSecurity for Nodes 的授权相同。该功能将在您为 Kaspersky Endpoint Detection and Response （KATA）添加单独密钥后可用。因此，计算机上将添加两个密钥：Kaspersky Industrial CyberSecurity for Nodes 密钥和 Endpoint Detection and Response Expert (on-premise) 密钥。

确保授权许可中包含“Endpoint Detection and Response Expert (on-premise)”功能。

3 连接到 Central Node

对于 Kaspersky Anti Targeted Attack Platform，您可以在 Kaspersky Industrial CyberSecurity for Nodes 和 Central Node 组件之间建立可信连接。要配置可信连接，您必须使用 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）。然后您必须将 TLS 证书添加到 Kaspersky Industrial CyberSecurity for Nodes（参见下面的说明）。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 仅检查 Central Node 的 TLS 证书。为了使连接更安全，您可以额外启用 Central Node 上的计算机额外验证。要启用此验证，您必须在 Central Node 和 Kaspersky Industrial CyberSecurity for Nodes 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*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）。

如何使用 Kaspersky Security Center 管理控制台 将 Kaspersky Industrial CyberSecurity for Nodes 计算机连接到 Central Node

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，打开“**策略**”文件夹。
3. 选择一个用于管理应用程序的策略，然后双击它以打开其设置窗口。
4. 选择“**遥测采集服务器**”部分。
5. 在“**KATA 整合**”块中单击“**设置**”按钮。

   “**KATA 整合**”窗口将打开。
6. 选择**KATA 整合**复选框。
7. 在“**连接设置**”下，点击“**添加**”添加一个或多个 Central Node 服务器。对于每个服务器，指定用于连接服务器的地址（IPv4、IPv6）和端口。

   Kaspersky Industrial CyberSecurity for Nodes 尝试在第一个 IP 地址处与服务器建立连接。如果连接建立失败，Kaspersky Industrial CyberSecurity for Nodes 将尝试在列表中的第二个 IP 地址处建立连接，以此类推。
8. 单击“**服务器连接设置**”。

   “**服务器连接设置**”窗口将打开。
9. 配置服务器连接：

   - “**超时(秒)**”。最大 Central Node 服务器响应超时。当超时用完时，Kaspersky Industrial CyberSecurity for Nodes 会尝试连接到不同的 Central Node 服务器。
   - “**服务器 TLS 证书**”。用于与 Central Node 服务器建立可信连接的 TLS 证书。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Anti Targeted Attack Platform 帮助中的说明）。

- **“使用双向认证”**。在 Kaspersky Industrial CyberSecurity for Nodes 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 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 Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

  > 加密容器必须受密码保护。无法添加密码为空的加密容器。

10. 单击**“确定”**。
11. 如果有必要，配置遥测。
12. 保存更改。

如何使用应用程序控制台将 Kaspersky Industrial CyberSecurity for Nodes 计算机连接到 Central Node

1. 在应用程序控制台树中，选择**“遥测采集服务器 → KATA 整合”**部分。
2. 在结果窗格中单击**“属性”**链接。

   将打开**“属性: Endpoint Detection and Response Expert (on-premise)”**窗口的**“常规”**选项卡。
3. 选择**KATA 整合**复选框。
4. 在**“连接设置”**下，点击**“添加”**添加一个或多个 Central Node 服务器。对于每个服务器，指定用于连接服务器的地址（IPv4、IPv6）和端口。

   Kaspersky Industrial CyberSecurity for Nodes 尝试在第一个 IP 地址处与服务器建立连接。如果连接建立失败，Kaspersky Industrial CyberSecurity for Nodes 将尝试在列表中的第二个 IP 地址处建立连接，以此类推。
5. 单击**“服务器连接设置”**。

   “服务器连接设置”窗口将打开。
6. 配置服务器连接：

   - **“超时(秒)”**。最大 Central Node 服务器响应超时。当超时用完时，Kaspersky Industrial CyberSecurity for Nodes 会尝试连接到不同的 Central Node 服务器。
   - **“服务器 TLS 证书”**。用于与 Central Node 服务器建立可信连接的 TLS 证书。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Anti Targeted Attack Platform 帮助中的说明）。

- **“使用双向认证”**。在 Kaspersky Industrial CyberSecurity for Nodes 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 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 Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

  加密容器必须受密码保护。无法添加密码为空的加密容器。

7. 单击**“确定”**。
8. 如果有必要，配置遥测。
9. 保存更改。

如何使用 Kaspersky Security Center Web Console 将 Kaspersky Industrial CyberSecurity for Nodes 计算机连接到 Central Node

1. 在 Web Console 的主窗口中，选择**“资产(设备)”** → **“策略和配置文件”**。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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**“遥测采集服务器”**部分。
5. 在**“KATA 整合”**块中单击**“配置”**按钮。
   “KATA 整合”窗口将打开。
6. 选择**启用 KATA 整合**复选框。
7. 在**“连接设置”**下，点击**“添加”**添加一个或多个 Central Node 服务器。对于每个服务器，指定用于连接服务器的地址（IPv4、IPv6）和端口。
   Kaspersky Industrial CyberSecurity for Nodes 尝试在第一个 IP 地址处与服务器建立连接。如果连接建立失败，Kaspersky Industrial CyberSecurity for Nodes 将尝试在列表中的第二个 IP 地址处建立连接，以此类推。
8. 单击**“服务器连接设置”**。
   “服务器连接设置”窗口将打开。
9. 配置服务器连接：

   - **“超时(秒)”**。最大 Central Node 服务器响应超时。当超时用完时，Kaspersky Industrial CyberSecurity for Nodes 会尝试连接到不同的 Central Node 服务器。
   - **“服务器 TLS 证书”**。用于与 Central Node 服务器建立可信连接的 TLS 证书。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Anti Targeted Attack Platform 帮助中的说明）。

- “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 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 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 Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

  > 加密容器必须受密码保护。无法添加密码为空的加密容器。

10. 单击“**确定**”。
11. 如果有必要，配置遥测。
12. 保存更改。

结果，Kaspersky Industrial CyberSecurity for Nodes 计算机被使用 Kaspersky Anti Targeted Attack Platform 控制台添加。

配置遥测

*遥测*是受保护计算机上发生的事件的列表。Kaspersky Industrial CyberSecurity for Nodes 分析遥测数据并在同步期间将其发送到 Kaspersky Anti Targeted Attack Platform。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 Industrial CyberSecurity for Nodes 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。

您可以在 Kaspersky Industrial CyberSecurity for Nodes 策略中配置同步行为并选择最佳值以匹配您的网络负载。

如果 Kaspersky Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 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 Industrial CyberSecurity for Nodes 可能会跳过一些事件。要启用此功能，您可以优化事件传输设置，例如，设置每小时最大事件数值。

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 的遥测。这使您可以优化这些解决方案的服务器负载。例如，如果您部署了 Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 解决方案，则可以在 Kaspersky Anti Targeted Attack Platform 中创建威胁响应任务时使用 Managed Detection and Response 遥测。

如何在 Kaspersky Security Center 管理控制台中配置遥测

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”文件夹。
3. 选择一个用于管理应用程序的策略，然后双击它以打开其设置窗口。

4. 选择“**遥测采集服务器**”部分。

5. 在“**KATA 整合**”块中单击“**设置**”按钮。

   “**属性: Endpoint Detection and Response Expert (on-premise)**”窗口将打开。

6. 配置“**发送同步请求到 KATA 服务器的间隔(分钟)**”设置。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。

7. 确保在“**数据传输设置**”块中，“**发送遥测数据到 KATA**”复选框被选中。

8. 如果必要，配置“**最大事件传输延迟(秒)**”设置：当指定的时间用完时，Kaspersky Industrial CyberSecurity for Nodes 将再次尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

9. 如果必要，配置“**事件包的最大数量**”设置：此设置规范可以作为一个事务的一部分发送的最大数据包数。默认值为 1024。

10. 如有必要，在“**请求限制**”块选择“**启用请求限制**”复选框。

    该功能有助于优化服务器上的负载。如果选中该复选框，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 Industrial CyberSecurity for Nodes 将停止发送事件。

11. 配置用于将事件发送到服务器的优化设置：

    - “**每小时最大事件数**”。如果事件流超过配置的每小时事件数限制，应用程序会分析遥测数据流并限制事件的发送。 Kaspersky Industrial CyberSecurity for Nodes 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。

    - “**超出事件限制的百分比**”。该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Industrial CyberSecurity for Nodes 将恢复发送事件。默认设置为 15%。

12. 保存更改。

如何在应用程序控制台中配置遥测

1. 在应用程序控制台树中，选择“**遥测采集服务器 → KATA 整合**”部分。

2. 在结果窗格中单击“**属性**”链接。

   “**属性: Endpoint Detection and Response Expert (on-premise)**”窗口将打开。

3. 配置“**发送同步请求到 KATA 服务器的间隔(分钟)**”设置。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。

4. 确保在“**数据传输设置**”块中，“**发送遥测数据到 KATA**”复选框被选中。

5. 如果必要，配置“**最大事件传输延迟(秒)**”设置：当指定的时间用完时，Kaspersky Industrial CyberSecurity for Nodes 将再次尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

6. 如果必要，配置“**事件包的最大数量**”设置：此设置规范可以作为一个事务的一部分发送的最大数据包数。默认值为 1024。

7. 如有必要，在“**请求限制**”块选择“**启用请求限制**”复选框。

   该功能有助于优化服务器上的负载。如果选中该复选框，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 Industrial CyberSecurity for Nodes 将停止发送事件。

8. 配置用于将事件发送到服务器的优化设置：

   - “**每小时最大事件数**”。如果事件流超过配置的每小时事件数限制，应用程序会分析遥测数据流并限制事件的发送。 Kaspersky Industrial CyberSecurity for Nodes 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。

   - “**超出事件限制的百分比**”。该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Industrial CyberSecurity for Nodes 将恢复发送事件。默认设置为 15%。

9. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置遥测

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**遥测采集服务器**”部分。

5. 在“**KATA 整合**”块中单击“**配置**”按钮。

   “**属性: Endpoint Detection and Response Expert (on-premise)**”窗口将打开。

6. 配置“**发送同步请求到 KATA 服务器的间隔(分钟)**”设置。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。

7. 确保在“**数据传输设置**”块中，“**发送遥测数据到 KATA**”复选框被选中。

8. 如果必要，配置“**最大事件传输延迟(秒)**”设置：当指定的时间用完时，Kaspersky Industrial CyberSecurity for Nodes 将再次尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

9. 如果必要，配置“**事件包的最大数量**”设置：此设置规范可以作为一个事务的一部分发送的最大数据包数。默认值为 1024。

10. 如有必要，在“**请求限制**”块选择“**启用请求限制**”复选框。

    该功能有助于优化服务器上的负载。如果选中该复选框，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 Industrial CyberSecurity for Nodes 将停止发送事件。

11. 配置用于将事件发送到服务器的优化设置：

    - **“每小时最大事件数”**。如果事件流超过配置的每小时事件数限制，应用程序会分析遥测数据流并限制事件的发送。 Kaspersky Industrial CyberSecurity for Nodes 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。

    - **“超出事件限制的百分比”**。该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Industrial CyberSecurity for Nodes 将恢复发送事件。默认设置为 15%。

12. 保存更改。

EDR 遥测排除项

要提高性能并优化到遥测服务器的数据传输，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。

[在 Kaspersky Security Center 管理控制台中创建 EDR 遥测排除项]

1. 在 Kaspersky Security Center 管理控制台树中，选择**“策略”**文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择**“补充 → KATA 整合/与 KICS for Networks 整合的遥测设置”**并点击**“设置”**。
4. 在打开的窗口中，配置遥测排除项（见下表）。
5. 保存更改。

[在 Kaspersky Security Center Web Console 中创建 EDR 遥测排除项]

1. 在 Web Console 的主窗口中，选择**“资产(设备)” → “策略和配置文件”**。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**“补充 → KATA 整合/与 KICS for Networks 整合的遥测设置”**并点击**“配置”**按钮。
5. 在打开的窗口中，配置遥测排除项（见下表）。
6. 保存更改。

[在应用程序控制台中创建 EDR 遥测排除项]

1. 在应用程序控制台树中，选择“Kaspersky Industrial CyberSecurity for Nodes”节点并从节点的上下文菜单中选择“KATA 整合/与 KICS for Networks 整合的遥测设置”。
2. 在打开的窗口中，配置遥测排除项（见下表）。
3. 保存更改。

参数	描述
排除的进程	**“优化要发送的遥测大小”**。Kaspersky Industrial CyberSecurity for Nodes 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。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • **“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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符； • **“命令行文本”**。用于运行文件的命令。 • **“描述”**。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • **“原始文件名称”**。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • **“版本”**。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • **“文件校验和”**。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。 **用于以下事件类型**： • **“文件修改”**。 • **“网络事件”**。 • **“进程：控制台交互式输入”**。 • **“模块已加载”**。 • **“注册表已修改”**。 • **“DNS 日志”**。 • **“进程访问”**。 • **“代码注入”**。 • **“WMI 查询”**。 • **“管道”**。 • **“LDAP”**。 • **“AMSI”**。
排除的网络通信	• **“规则名称”**。规则的名称。 • **“方向”**。传入或传出的事件。 • **“协议”**。协议类型。 • **“原始套接字”**。是否使用原始套接字。 • **“协议号”**。协议号。 • **“TLS 证书”**。用于使用 TLS 协议加密客户端和服务器之间的连接的数字证书。 • **“本地端口或范围”**。特定端口或可能的本地端口范围。 • **“远程端口或范围”**。特定端口或可能的远程端口范围。 • **“本地地址”**。Kaspersky Industrial CyberSecurity for Nodes 从网络流量中排除遥测的计算机的网络地址。 • **“远程地址”**。Kaspersky Industrial CyberSecurity for Nodes 从网络流量中排除遥测的计算机的网络地址。 IP 地址仅支持 IPv4 格式。 • **“应用程序”**。Kaspersky Industrial CyberSecurity for Nodes 从网络流量中排除 EDR 遥测的应用程序的可执行文件列表。
排除的文件操作	• **“规则名称”**。规则的名称。 • **“文件名或掩码”**。文件或文件夹的名称或掩码；当访问此文件或文件夹时，Kaspersky Industrial CyberSecurity for Nodes 将应用排除规则。输入掩码时，Kaspersky Industrial CyberSecurity for Nodes 支持 `*` 字符和 `?` 字符： • **“操作类型”**。文件操作的类型，例如创建文件或编辑文件属性。 • **“先前路径”**。文件的先前路径。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • **“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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • **“命令行文本”**。用于运行文件的命令。 • **“父目录”**。包含文件的文件夹路径。 • **“描述”**。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • **“原始文件名称”**。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。

参数	描述
	• “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。
排除的 DNS 操作	• “**规则名称**”。规则的名称。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • “**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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • “**命令行文本**”。用于运行文件的命令。 • “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。 DNS： • “**DNS 服务器 IP 地址**”。处理 DNS 查询的服务器地址。 • “**查询选项**”。规范 DNS 查询的格式和条件的参数。 • “**状态**”。DNS 操作的当前状态。 • “**域名**”。正在处理查询的域名。 • “**设置类型 ID**”。DNS 设置类型的唯一 ID。 • “**相应数据**”。服务器响应 DNS 查询而返回的数据。
排除的 LDAP 操作	• “**规则名称**”。规则的名称。 • “**LDAP 搜索范围**”。执行 LDAP 搜索的范围。 • “**过滤器**”。用于过滤 LDAP 对象的搜索条件。 • “**LDAP 对象搜索的可分辨名称**”。LDAP 搜索对象的唯一名称。 • “**对象属性**”。LDAP 查询中将提取的对象的属性。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • “**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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • “**命令行文本**”。用于运行文件的命令。 • “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。

参数	描述
排除的进程访问查询	“**规则名称**”。规则的名称。 “**操作类型**”。进程访问操作的类型，例如“任何”或“打开”。 “**进程访问请求**”。对该进程的访问级别。 “**调用堆栈跟踪**”。与访问进程相关的函数调用序列的信息。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情**、**父进程详细信息**、**目标进程**、**源进程文件** 和 **目标进程文件**。 • “**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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • “**命令行文本**”。用于运行文件的命令。 • “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。
排除的代码注入	• “**规则名称**”。规则的名称。 • “**访问方法**”。用于代码注入的访问方法。 • “**调用堆栈**”。与代码注入相关的函数调用序列。 • “**修改的命令行**”。被注入修改的命令行。 • “**注入地址**”。注入发生的内存位置。 • “**注入的 DLL 名称**”。用于注入的动态链接库 (DLL) 的名称。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • “**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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • “**命令行文本**”。用于运行文件的命令。 • “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。
排除的 WMI 查询	• “**规则名称**”。规则的名称。 • “**WMI 操作类型**”。使用 WMI 执行的操作类型。 • “**远程查询**”。有关 WMI 查询是否远程执行的信息。 • “**执行 WMI 命令的计算机的名称**”。发起查询的计算机的名称。 • “**WMI 用户账户**”。用于 WMI 查询的用户账户。 • “**执行的 WMI 命令**”。通过 WMI 执行的特定命令。 • “**WMI 名字空间**”。执行 WMI 操作的命名空间。 • “**WMI 事件使用者过滤器**”。用于处理 WMI 中的事件的过滤器。 • “**创建的 WMI 事件使用者的名称**”。使用 WMI 创建的事件消费者的名称。 • “**WMI 事件使用者源代码**”。用于创建 WMI 事件消费者的代码。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • “**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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • “**命令行文本**”。用于运行文件的命令。 • “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。

参数	描述
	• “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。
排除的管道操作	• “**规则名称**”。规则的名称。 • “**管道名称**”。管道的名称。 • “**操作类型**”。管道操作类型，例如创建或连接。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • “**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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • “**命令行文本**”。用于运行文件的命令。 • “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。
被排除的注册表更改	• “**规则名称**”。规则的名称。 • “**操作类型**”。对注册表执行的操作类型，例如添加、删除、修改。 • “**路径**”。发生更改的注册表项的路径。 • “**值名称**”。已修改的注册表值的名称。 • “**值**”。新的或修改的注册表值。 • “**注册表文件全称**”。进行修改的注册表文件的完整路径。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。 **进程详情** 和 **父进程详细信息**： • “**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 Industrial CyberSecurity for Nodes 支持环境变量和 `*` 以及 `?` 字符： • “**命令行文本**”。用于运行文件的命令。 • “**描述**”。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • “**原始文件名称**”。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • “**版本**”。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • “**文件校验和**”。MD5 和 SHA256。 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。 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` 文件的参数。这种行为是由操作系统的特性决定的。
排除的设备操作	• “**规则名称**”。规则的名称。 • “**设备类型**”。设备类型：本地打印机、可移动驱动器、CD/DVD 驱动器等。有关详细信息，请参阅设备访问规则。

参数	描述
	• “**设备 ID**”。可用于识别设备特定实例的唯一 ID。 • “**设备名称**”。设备的名称。 Kaspersky Industrial CyberSecurity for Nodes 将规则触发条件与逻辑 AND 相结合。

与 Kaspersky Industrial CyberSecurity for Networks 集成

Kaspersky Industrial CyberSecurity for Networks 旨在保护工业企业的基础设施免受信息安全威胁，并确保技术流程的连续性。Kaspersky Industrial CyberSecurity for Networks 可以分析工业网络流量，以检测技术参数值的偏差、检测网络攻击的迹象并监控网络上设备的运行和当前状态。该应用程序是 Kaspersky Industrial CyberSecurity 解决方案的一部分。有关 Kaspersky Industrial CyberSecurity for Networks 的完整信息，请参阅 *Kaspersky Industrial CyberSecurity for Networks 帮助*。

Kaspersky Industrial CyberSecurity for Nodes 支持与 Kaspersky Industrial CyberSecurity for Networks 集成。Kaspersky Industrial CyberSecurity for Nodes 接收的有关设备事件的数据将被发送到 Kaspersky Industrial CyberSecurity for Networks 服务器。应用程序之间的集成增强了 Kaspersky Industrial CyberSecurity for Networks 调查和应对工业网络威胁的能力。

与 Kaspersky Industrial CyberSecurity for Networks 集成的 Kaspersky Industrial CyberSecurity for Nodes 配置

有以下配置：

- [KICS+内置代理]。在此配置中，Kaspersky Industrial CyberSecurity for Nodes 既充当确保计算机安全的应用程序，又充当使用 Kaspersky Industrial CyberSecurity for Networks 的应用程序。从 4.5 版开始，Kaspersky Industrial CyberSecurity for Nodes 中就有内置代理。
- [第三方 EPP+端点代理配置]。在此配置中，计算机的安全由第三方端点保护平台（EPP）提供。与 Kaspersky Industrial CyberSecurity for Networks 的集成由 Kaspersky Industrial CyberSecurity for Nodes 在端点代理配置中提供。从 4.5 版开始，Kaspersky Industrial CyberSecurity for Nodes 中提供了端点代理配置。

为了将 Kaspersky Industrial CyberSecurity for Nodes 内置代理与 Kaspersky Industrial CyberSecurity for Networks 集成，必须满足以下条件：

- Kaspersky Industrial CyberSecurity for Networks 已部署。
- Kaspersky Security Center 版本 14.2 或更高版本已部署。
- 向 Kaspersky Industrial CyberSecurity for Networks 发送数据的以下应用程序组件必须启用并运行：漏洞利用防御、修复引擎、反加密勒索。

要将 Endpoint Agent 配置与 Kaspersky Industrial CyberSecurity for Networks 集成，必须部署以下内容：

- Kaspersky Industrial CyberSecurity for Networks。
- Kaspersky Security Center 版本 14.2 或更高版本。

对以前版本的 Kaspersky Industrial CyberSecurity for Nodes 的支持

Kaspersky Industrial CyberSecurity for Nodes 4.5 支持使用内置代理或端点代理配置与 Kaspersky Industrial CyberSecurity for Networks 集成；您无需安装 Kaspersky Endpoint Agent。

如果您使用 Kaspersky Industrial CyberSecurity for Nodes 4.5 之前的版本与 Kaspersky Industrial CyberSecurity for Networks 集成，则必须单独安装 Kaspersky Endpoint Agent。

配置与 Kaspersky Industrial CyberSecurity for Networks 的集成

与 Kaspersky Industrial CyberSecurity for Networks 的集成包括以下步骤：

1. **安装 Kaspersky Industrial CyberSecurity for Networks 集成组件**

   在安装包设置或安装向导中，或通过更改 Windows 控制面板中的应用程序程序组件集，在必须选择要安装的应用程序组件的步骤中，选择以下内容：

   - **完整功能 — 端点代理 — 与 KICS for Networks 整合**，对于内置代理
   - **端点代理 — 与 KICS for Networks 整合**，对于端点代理配置

   > 要完成更改应用程序组件集，您必须重新启动计算机。

2. **激活 Kaspersky Industrial CyberSecurity for Networks 集成组件**

   确保您的授权许可涵盖激活 Kaspersky Industrial CyberSecurity for Networks 集成的功能。

3. **启用并配置 Kaspersky Industrial CyberSecurity for Networks 集成组件**

   Kaspersky Industrial CyberSecurity for Nodes 支持在具有数据二极管的网络中与 KICS for Networks 集成。数据二极管是用于受保护网段和外部设备之间通信的单向网关。应用程序支持软件 MQTT 服务器（例如，Mosquitto）作为 MQTT 代理。对于通过数据二极管进行通信，Kaspersky Industrial CyberSecurity for Nodes 使用 MQTT 协议。MQTT（Message Queuing Telemetry Transport）是一种在 TCP/IP 上工作的简化网络协议。该协议遵循“发布者-订阅者”模型。您可以将应用程序配置为订阅者和发布者。配置为 MQTT 发布者时，应用程序将遥测数据发送到数据二极管。

   > 发送到 MQTT 代理服务器的遥测可能包含机密信息。为了控制对数据的访问，您必须采取措施确保遥测的安全。

   > 在 Windows XP 计算机上，遥测数据无法发送到 MQTT 代理服务器。

如何在 Kaspersky Security Center 管理控制台中配置与 Kaspersky Industrial CyberSecurity for Networks 的集成

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 选择“**遥测采集服务器**”部分。
4. 在“**与 KICS for Networks 整合**”块中单击“**设置**”按钮。
   “**与 KICS for Networks 整合**”窗口将打开。
5. 选择**与 KICS for Networks 整合**复选框。
6. 在“**常规**”选项卡中，选择遥测模式：
   - “**发送遥测到 KICS for Networks 服务器**”。Kaspersky Industrial CyberSecurity for Nodes 将遥测数据直接发送到 Kaspersky Industrial CyberSecurity for Networks 服务器（标准模式）。
     要在“*标准模式*”下发送遥测数据，请管理以下设置：
     - **地址** 和 **端口**。要将遥测数据发送到的 Kaspersky Industrial CyberSecurity for Networks 的 IP 地址和端口。
     - “**发送同步请求到 KICS for Networks 服务器的间隔(分钟)**”。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。默认值为 5 分钟。
     - “**服务器连接设置**”。管理以下设置：
       - “**超时(秒)**”。最大服务器响应超时。超时后，Kaspersky Industrial CyberSecurity for Nodes 会重新连接到服务器。默认设置是 10 秒。
       - “**服务器 TLS 证书**”。用于与 Kaspersky Industrial CyberSecurity for Networks 服务器建立受信任连接的 TLS 证书。您可以使用 Kaspersky Industrial CyberSecurity for Networks 管理界面获取 TLS 证书。
       - “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 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 Kaspersky Industrial CyberSecurity for Networks 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。配置 Kaspersky Industrial CyberSecurity for Networks 设置后，您还需要在 Kaspersky Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。
         加密容器必须受密码保护。无法添加密码为空的加密容器。
   - “**发送遥测到数据二极管作为 MQTT 发布者**”。Kaspersky Industrial CyberSecurity for Nodes 将遥测数据发送到内置于软件数据二极管（*MQTT 发布者*）的 MQTT 代理服务器。
     要在“*MQTT 发布者模式*”下发送遥测数据，请管理以下设置：
     a. 输入用于在 MQTT 代理服务器上进行身份验证的凭据。
     b. 输入 MQTT 代理服务器的 IP 地址和端口。

7. 配置数据传输（请参阅下表）。

8. 如有必要，以混杂模式配置遥测。

   默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。

   > 并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。

   a. 在“**遥测采集**”选项卡上，如果要为安装了应用程序的计算机的所有网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**为应用程序和主机网络接口启用混杂模式**”复选框。

   b. 如果要为以下列表中的子网配置的网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**在混杂模式下仅使用为指定子网配置的主机网络接口**”复选框。

   c. 如果有必要，创建子网列表。

9. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置与 Kaspersky Industrial CyberSecurity for Networks 的集成

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**遥测采集服务器**”部分。

5. 在“**与 KICS for Networks 整合**”块中单击“**配置**”按钮。

   “**与 KICS for Networks 整合**”窗口将打开。

6. 选择**与 KICS for Networks 整合**复选框。

7. 在“**常规**”选项卡中，选择遥测模式：

   - “**发送遥测到 KICS for Networks 服务器**”。Kaspersky Industrial CyberSecurity for Nodes 将遥测数据直接发送到 Kaspersky Industrial CyberSecurity for Networks 服务器（标准模式）。

     要在“*标准模式*”下发送遥测数据，请管理以下设置：

     - **地址** 和 **端口**。要将遥测数据发送到的 Kaspersky Industrial CyberSecurity for Networks 的 IP 地址和端口。

     - “**发送同步请求到 KICS for Networks 服务器的间隔(分钟)**”。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。默认值为 5 分钟。

- “**服务器连接设置**”。管理以下设置：
  - “**超时(秒)**”。最大服务器响应超时。超时后，Kaspersky Industrial CyberSecurity for Nodes 会重新连接到服务器。默认设置是 10 秒。
  - “**服务器 TLS 证书**”。用于与 Kaspersky Industrial CyberSecurity for Networks 服务器建立受信任连接的 TLS 证书。您可以使用 Kaspersky Industrial CyberSecurity for Networks 管理界面获取 TLS 证书。
  - “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 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 Kaspersky Industrial CyberSecurity for Networks 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。配置 Kaspersky Industrial CyberSecurity for Networks 设置后，您还需要在 Kaspersky Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

    加密容器必须受密码保护。无法添加密码为空的加密容器。

- “**发送遥测到数据二极管作为 MQTT 发布者**”。Kaspersky Industrial CyberSecurity for Nodes 将遥测数据发送到内置于软件数据二极管（*MQTT 发布者*）的 MQTT 代理服务器。

  要在“*MQTT 发布者模式*”下发送遥测数据，请管理以下设置：

  a. 输入用于在 MQTT 代理服务器上进行身份验证的凭据。

  b. 输入 MQTT 代理服务器的 IP 地址和端口。

8. 配置数据传输（请参阅下表）。
9. 如有必要，以混杂模式配置遥测。

   默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。

   > 并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。

   a. 在“**遥测采集**”选项卡上，如果要为安装了应用程序的计算机的所有网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**为应用程序和主机网络接口启用混杂模式**”复选框。

   b. 如果要为以下列表中的子网配置的网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**在混杂模式下仅使用为指定子网配置的主机网络接口**”复选框。

   c. 如果有必要，创建子网列表。

10. 保存更改。

如何在应用程序控制台中配置与 Kaspersky Industrial CyberSecurity for Networks 的集成

1. 在应用程序控制台树中，选择“**遥测采集服务器 → 与 KICS for Networks 整合**”部分。
2. 在结果窗格中单击“**属性**”链接。

   将打开“**属性: 与 KICS for Networks 整合**”窗口的“**常规**”选项卡。

3. 选择**与 KICS for Networks 整合**复选框。

4. 在“**常规**”选项卡中，选择遥测模式：

   - “**发送遥测到 KICS for Networks 服务器**”。Kaspersky Industrial CyberSecurity for Nodes 将遥测数据直接发送到 Kaspersky Industrial CyberSecurity for Networks 服务器（标准模式）。

     要在“*标准模式*”下发送遥测数据，请管理以下设置：

     - **地址** 和 **端口**。要将遥测数据发送到的 Kaspersky Industrial CyberSecurity for Networks 的 IP 地址和端口。

     - “**发送同步请求到 KICS for Networks 服务器的间隔(分钟)**”。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。默认值为 5 分钟。

     - “**服务器连接设置**”。管理以下设置：

       - “**超时(秒)**”。最大服务器响应超时。超时后，Kaspersky Industrial CyberSecurity for Nodes 会重新连接到服务器。默认设置是 10 秒。

       - “**服务器 TLS 证书**”。用于与 Kaspersky Industrial CyberSecurity for Networks 服务器建立受信任连接的 TLS 证书。您可以使用 Kaspersky Industrial CyberSecurity for Networks 管理界面获取 TLS 证书。

       - “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 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 Kaspersky Industrial CyberSecurity for Networks 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。配置 Kaspersky Industrial CyberSecurity for Networks 设置后，您还需要在 Kaspersky Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

         加密容器必须受密码保护。无法添加密码为空的加密容器。

   - “**发送遥测到数据二极管作为 MQTT 发布者**”。Kaspersky Industrial CyberSecurity for Nodes 将遥测数据发送到内置于软件数据二极管（*MQTT 发布者*）的 MQTT 代理服务器。

     要在“*MQTT 发布者模式*”下发送遥测数据，请管理以下设置：

     a. 输入用于在 MQTT 代理服务器上进行身份验证的凭据。

     b. 输入 MQTT 代理服务器的 IP 地址和端口。

5. 配置数据传输（请参阅下表）。

6. 如有必要，以混杂模式配置遥测。

   默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。

并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。

a. 在“**遥测采集**”选项卡上，如果要为安装了应用程序的计算机的所有网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**为应用程序和主机网络接口启用混杂模式**”复选框。

b. 如果要为以下列表中的子网配置的网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**在混杂模式下仅使用为指定子网配置的主机网络接口**”复选框。

c. 如果有必要，创建子网列表。

7. 保存更改。

如何在命令行上配置与 Kaspersky Industrial CyberSecurity for Networks 的集成

要在命令行上配置集成，必须启用密码保护。

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，Command Prompt cmd.exe）。

2. 使用 `cd` 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如，输入命令 `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0` 并按 **ENTER**。

3. 要在标准模式下配置 Kaspersky Industrial CyberSecurity for Nodes 与 Kaspersky Industrial CyberSecurity for Networks 的集成，请运行以下命令：

   `KAVSHELL KICS /enable /servers:<地址>:<port> [/pinned-certificate:<TLS 证书文件的完整路径>] [/client-certificate:<加密容器的完整路径>] [/client-password:<加密容器的密码>] [/timeout:<最大服务器响应超时>] [/sync-period:<同步请求周期>] [/events-sent-period:<发送事件的最大延迟>] [/events-limit:<1|0>] [/events-per-hour:<每小时最大事件数>] [/virtual-span-enable] [/virtual-span-disable] [/virtual-span-add-rules:<子网 ID>] [/virtual-span-remove-rules:<子网 ID>] [/login:<当前用户账户的名称>] [/pwd:</login 密码或 KLAdmin 密码（如果未指定 /login）>]`

4. 要在 MQTT 发布者模式下配置 Kaspersky Industrial CyberSecurity for Nodes 与 Kaspersky Industrial CyberSecurity for Networks 的集成，请运行以下命令：

   `KAVSHELL KICS /enable /kics-mode:mqtt-publisher /mqtt-server:<地址>:<port> [/mqtt-user:<用于在 MQTT 代理授权的登录名>] [/mqtt-password:<用于在 MQTT 代理上进行授权的密码>] [/login:<当前用户账户的名称>] [/pwd:</login 密码或 KLAdmin 密码（如果未指定 /login）>]`

Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 之间的集成设置

参数	描述
`KICS`	必需参数。 指定 Kaspersky Industrial CyberSecurity for Networks 作为要集成的应用程序。
`/<enable|disable|show>`	必需参数。 允许启用、禁用和查看 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 之间的集成状态。
`/servers:<地址>:<端口>`	必需参数。 允许您指定 Kaspersky Industrial CyberSecurity for Networks 服务器的地址和端口或 MQTT 发布者的地址。

/kics-mode:<telemetry|mqtt-publisher>	可选参数。 允许选择应用程序与 Kaspersky Industrial CyberSecurity for Networks 的集成模式。 • telemetry 将遥测数据直接发送到 Kaspersky Industrial CyberSecurity for Networks 服务器。 • mqtt-publisher 是用于将遥测数据发送到 MQTT 代理服务器的模式。 默认值为“telemetry”。
/pinned-certificate:< TLS 证书文件的完整路径 >	可选参数。 允许您添加 TLS 证书，用于将 Kaspersky Industrial CyberSecurity for Nodes 与 Kaspersky Industrial CyberSecurity for Networks 服务器连接。
/client-certificate:< 加密容器的完整路径 >	可选参数。 允许您添加一个*加密容器*，用于存储加密的客户端证书，以保护 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 服务器之间的连接。
/client-password:< 加密容器的密码 >	必需参数，如果 /CLIENT-CERTIFICATE 被传递。 允许您为加密容器指定密码。
/timeout:< 最大服务器响应超时 >	可选参数。 允许您指定 Kaspersky Industrial CyberSecurity for Networks 服务器的最大响应超时时间（以秒为单位）。 超时用完后，如果有多个 Industrial CyberSecurity for Networks 服务器，Kaspersky Industrial CyberSecurity for Nodes 将尝试连接到另一个 Industrial CyberSecurity for Networks 服务器。
/sync-period:< 同步请求周期 >	可选参数。 允许您指定向 Kaspersky Industrial CyberSecurity 服务器发送同步请求的时间间隔（分钟）。在同步期间，应用程序会发送有关修改的应用程序和任务设置的信息。
/events-sent-period:< 发送事件时的最大延迟 >	可选参数。 允许您指定向 Kaspersky Industrial CyberSecurity for Networks 服务器发送事件时的最大延迟。当指定的时间用完时，该应用程序将尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。
/events-limit:<1|0>	可选参数。 让您限制发送的事件数量。如果事件数量超过配置的限制，应用程序将停止发送事件。
/events-per-hour:< 每小时最大事件数 >	必需参数，如果 /EVENTS-LIMIT:1 被传递。 允许您指定每小时发送的最大事件数。
/pwd:< 密码 >	可选参数。 允许您指定 KLAdmin 用户或具有足够权限配置集成的用户的密码。 如果未指定此选项，应用程序将在下一行提示您输入密码。
/login:< 用户名 >	可选参数。 允许您指定具有足够权限来配置集成的用户名。 如果未指定此选项，应用程序将在下一行提示您输入用户名。 如果您输入了 KLAdmin 密码，则无需输入此值。
/virtual-span-enable	可选参数。 启用遥测的混杂模式。 默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。 并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。
/virtual-span-disable	可选参数。 禁用遥测的混杂模式。

/virtual-span-add-rules:< 计算机网络接口的 IPv4 地址 >	可选参数。 您可以将子网添加为计算机网络接口的地址（应用程序通过网络接口的子网掩码识别相应的子网）或具有 IPv4 格式的子网的网络接口地址。 应用程序仅以混杂模式收集为指定子网配置的网络接口的网络流量。 例如：/VIRTUAL-SPAN-ADD-RULES:198.51.100.0; 198.51.100.0/24。
/virtual-span-remove-rules:< 子网 ID >	可选参数。 允许您删除具有指定 ID 的子网。可以使用 /VIRTUAL-SPAN-SHOW 命令显示添加的子网及其 ID 的列表。
/mqtt-subscriber-enable	可选参数。 启用 MQTT 订阅者模式以从数据二极管接收遥测数据。 默认禁用 MQTT 订阅者模式。
/mqtt-subscriber-disable	可选参数。 禁用 MQTT 订阅者模式。
/mqtt-server:< 地址 >:< 端口 >	必需参数，如果已传递“/kics-mode:mqtt-publisher”或“/mqtt-subscriber:enable.”参数。 指定 MQTT 代理的地址和端口。 MQTT 代理的默认端口为 1883。
/mqtt-user:< 登录名 >	在 MQTT 代理上配置登录名和密码授权的必需参数。 指定用于 MQTT 代理授权的登录名。
/mqtt-password:< 密码 >	在 MQTT 代理上配置登录名和密码授权的必需参数。 指定用于在 MQTT 代理上进行授权的密码。

作为 MQTT 订阅者，应用程序从数据二极管接收遥测数据，以将其发送到 KICS for Network。

当没有与 KICS for Networks 服务器的连接时，不保证通过数据二极管从 Kaspersky Industrial CyberSecurity for Nodes 接收的消息的传输。

如何在 Kaspersky Security Center 管理控制台中将应用程序配置为 MQTT 订阅者

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点，然后选择计算机所属的组。
2. 在结果窗格中，选择“**设备**”选项卡。
3. 双击以打开计算机属性窗口。
4. 转到**应用程序**区域。
5. 在计算机上安装的卡巴斯基应用程序列表中，选择“Kaspersky Industrial CyberSecurity for Nodes”并双击以打开应用程序属性。
6. 选择“**遥测采集服务器**”部分。
7. 在“**与 KICS for Networks 整合**”块中单击“**设置**”按钮。
   “**与 KICS for Networks 整合**”窗口将打开。
8. 选择**与 KICS for Networks 整合**复选框。
9. 在“**常规**”选项卡上，选择“**发送遥测到 KICS for Networks 服务器**”。

10. 管理以下设置：

    - **地址** 和 **端口**。要将遥测数据发送到的 Kaspersky Industrial CyberSecurity for Networks 的 IP 地址和端口。
    - **“发送同步请求到 KICS for Networks 服务器的间隔(分钟)”**。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。默认值为 5 分钟。
    - **“服务器连接设置”**。管理以下设置：
        - **“超时(秒)”**。最大服务器响应超时。超时后，Kaspersky Industrial CyberSecurity for Nodes 会重新连接到服务器。默认设置是 10 秒。
        - **“服务器 TLS 证书”**。用于与 Kaspersky Industrial CyberSecurity for Networks 服务器建立受信任连接的 TLS 证书。您可以使用 Kaspersky Industrial CyberSecurity for Networks 管理界面获取 TLS 证书。
        - **“使用双向认证”**。在 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 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 Kaspersky Industrial CyberSecurity for Networks 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。配置 Kaspersky Industrial CyberSecurity for Networks 设置后，您还需要在 Kaspersky Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

          加密容器必须受密码保护。无法添加密码为空的加密容器。
    - 选择**从数据二极管接收遥测作为 MQTT 订阅者**复选框。
    - 输入用于在 MQTT 代理服务器上进行身份验证的凭据。
    - 输入 MQTT 代理服务器的 IP 地址和端口。

11. 配置数据传输（请参阅下表）。

12. 如有必要，以混杂模式配置遥测。

    默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。

    > 并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。

    a. 在**“遥测采集”**选项卡上，如果要为安装了应用程序的计算机的所有网络接口启用从所有可用子网收集网络流量的混杂模式，请选中**“为应用程序和主机网络接口启用混杂模式”**复选框。

    b. 如果要为以下列表中的子网配置的网络接口启用从所有可用子网收集网络流量的混杂模式，请选中**“在混杂模式下仅使用为指定子网配置的主机网络接口”**复选框。

    c. 如果有必要，创建子网列表。

13. 保存更改。

如何在 Kaspersky Security Center Web Console 中将应用程序配置为 MQTT 订阅者

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**受管理设备**”。
2. 单击计算机名称。
3. 在显示的计算机属性窗口中，选择“**应用程序**”选项卡。
4. 点击“**Kaspersky Industrial CyberSecurity for Nodes (4.5.0)**”。
5. 选择**应用程序设置**选项卡。
6. 选择“**遥测采集服务器**”部分。
7. 在“**与 KICS for Networks 整合**”块中单击“**配置**”按钮。
   “**与 KICS for Networks 整合**”窗口将打开。
8. 选择**与 KICS for Networks 整合**复选框。
9. 在“**常规**”选项卡上，选择“**发送遥测到 KICS for Networks 服务器**”。
10. 管理以下设置：
    - **地址** 和 **端口**。要将遥测数据发送到的 Kaspersky Industrial CyberSecurity for Networks 的 IP 地址和端口。
    - “**发送同步请求到 KICS for Networks 服务器的间隔(分钟)**”。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。默认值为 5 分钟。
    - “**服务器连接设置**”。管理以下设置：
      - “**超时(秒)**”。最大服务器响应超时。超时后，Kaspersky Industrial CyberSecurity for Nodes 会重新连接到服务器。默认设置是 10 秒。
      - “**服务器 TLS 证书**”。用于与 Kaspersky Industrial CyberSecurity for Networks 服务器建立受信任连接的 TLS 证书。您可以使用 Kaspersky Industrial CyberSecurity for Networks 管理界面获取 TLS 证书。
      - “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 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 Kaspersky Industrial CyberSecurity for Networks 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。配置 Kaspersky Industrial CyberSecurity for Networks 设置后，您还需要在 Kaspersky Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

        加密容器必须受密码保护。无法添加密码为空的加密容器。
    - 选择**从数据二极管接收遥测作为 MQTT 订阅者**复选框。
    - 输入用于在 MQTT 代理服务器上进行身份验证的凭据。
    - 输入 MQTT 代理服务器的 IP 地址和端口。

11. 配置数据传输（请参阅下表）。

12. 如有必要，以混杂模式配置遥测。

    默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。

    > 并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。

    a. 在“**遥测采集**”选项卡上，如果要为安装了应用程序的计算机的所有网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**为应用程序和主机网络接口启用混杂模式**”复选框。

    b. 如果要为以下列表中的子网配置的网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**在混杂模式下仅使用为指定子网配置的主机网络接口**”复选框。

    c. 如果有必要，创建子网列表。

13. 保存更改。

如何在应用程序控制台中将应用程序配置为 MQTT 订阅者

1. 在应用程序控制台树中，选择“**遥测采集服务器 → 与 KICS for Networks 整合**”部分。

2. 在结果窗格中单击“**属性**”链接。

   将打开“**属性: 与 KICS for Networks 整合**”窗口的“**常规**”选项卡。

3. 选择**与 KICS for Networks 整合**复选框。

4. 在“**常规**”选项卡上，选择“**发送遥测到 KICS for Networks 服务器**”。

5. 管理以下设置：

   - **地址** 和 **端口**。要将遥测数据发送到的 Kaspersky Industrial CyberSecurity for Networks 的 IP 地址和端口。

   - “**发送同步请求到 KICS for Networks 服务器的间隔(分钟)**”。发送到服务器的同步请求的频率。在同步期间，Kaspersky Industrial CyberSecurity for Nodes 发送有关修改的应用程序设置和任务的信息。默认值为 5 分钟。

   - “**服务器连接设置**”。管理以下设置：

     - “**超时(秒)**”。最大服务器响应超时。超时后，Kaspersky Industrial CyberSecurity for Nodes 会重新连接到服务器。默认设置是 10 秒。

     - “**服务器 TLS 证书**”。用于与 Kaspersky Industrial CyberSecurity for Networks 服务器建立受信任连接的 TLS 证书。您可以使用 Kaspersky Industrial CyberSecurity for Networks 管理界面获取 TLS 证书。

- “**使用双向认证**”。在 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 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 Kaspersky Industrial CyberSecurity for Networks 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。配置 Kaspersky Industrial CyberSecurity for Networks 设置后，您还需要在 Kaspersky Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。

  加密容器必须受密码保护。无法添加密码为空的加密容器。

- 选择**从数据二极管接收遥测作为 MQTT 订阅者**复选框。
- 输入用于在 MQTT 代理服务器上进行身份验证的凭据。
- 输入 MQTT 代理服务器的 IP 地址和端口。

6. 配置数据传输（请参阅下表）。
7. 如有必要，以混杂模式配置遥测。

   默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。

   > 并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。

   a. 在“**遥测采集**”选项卡上，如果要为安装了应用程序的计算机的所有网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**为应用程序和主机网络接口启用混杂模式**”复选框。

   b. 如果要为以下列表中的子网配置的网络接口启用从所有可用子网收集网络流量的混杂模式，请选中“**在混杂模式下仅使用为指定子网配置的主机网络接口**”复选框。

   c. 如果有必要，创建子网列表。

8. 保存更改。

如何在命令行上将应用程序配置为 MQTT 订阅者

> 要在命令行上配置集成，必须启用密码保护。

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，Command Prompt cmd.exe）。
2. 使用 `cd` 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如，输入命令 `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0` 并按 **ENTER**。

3. 执行以下命令：

KAVSHELL KICS /enable /servers:<地址>:<port> [/pinned-certificate:<TLS 证书文件的完整路径>] [/client-certificate:<加密容器的完整路径>] [/client-password:<加密容器的密码>] [/timeout:<最大服务器响应超时>] [/sync-period:<同步请求周期>] [/events-sent-period:<发送事件的最大延迟>] [/events-limit:<1|0>] [/events-per-hour:<每小时最大事件数>] [/virtual-span-enable] [/virtual-span-disable] [/virtual-span-add-rules:<子网 ID>] [/virtual-span-remove-rules:<子网 ID>] /mqtt-subscriber-enable /mqtt-server:<地址>:<port> [/mqtt-user:<用于在 MQTT 代理授权的登录名>] [/mqtt-password:<用于在 MQTT 代理上进行授权的密码>] [/login:<当前用户账户的名称>] [/pwd:</login 密码或 KLAdmin 密码（如果未指定 /login）>]

Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 之间的集成设置

参数	描述
KICS	必需参数。 指定 Kaspersky Industrial CyberSecurity for Networks 作为要集成的应用程序。
/<enable|disable|show>	必需参数。 允许启用、禁用和查看 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 之间的集成状态。
/servers:< 地址 >:< 端口 >	必需参数。 允许您指定 Kaspersky Industrial CyberSecurity for Networks 服务器的地址和端口或 MQTT 发布者的地址。
/kics-mode:<telemetry|mqtt-publisher>	可选参数。 允许选择应用程序与 Kaspersky Industrial CyberSecurity for Networks 的集成模式。 • telemetry 将遥测数据直接发送到 Kaspersky Industrial CyberSecurity for Networks 服务器。 • mqtt-publisher 是用于将遥测数据发送到 MQTT 代理服务器的模式。 默认值为“telemetry”。
/pinned-certificate:< TLS 证书文件的完整路径 >	可选参数。 允许您添加 TLS 证书，用于将 Kaspersky Industrial CyberSecurity for Nodes 与 Kaspersky Industrial CyberSecurity for Networks 服务器连接。
/client-certificate:< 加密容器的完整路径 >	可选参数。 允许您添加一个*加密容器*，用于存储加密的客户端证书，以保护 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Networks 服务器之间的连接。
/client-password:< 加密容器的密码 >	必需参数，如果 /CLIENT-CERTIFICATE 被传递。 允许您为加密容器指定密码。
/timeout:< 最大服务器响应超时 >	可选参数。 允许您指定 Kaspersky Industrial CyberSecurity for Networks 服务器的最大响应超时时间（以秒为单位）。 超时用完后，如果有多个 Industrial CyberSecurity for Networks 服务器，Kaspersky Industrial CyberSecurity for Nodes 将尝试连接到另一个 Industrial CyberSecurity for Networks 服务器。
/sync-period:< 同步请求周期 >	可选参数。 允许您指定向 Kaspersky Industrial CyberSecurity 服务器发送同步请求的时间间隔（分钟）。在同步期间，应用程序会发送有关修改的应用程序和任务设置的信息。
/events-sent-period:< 发送事件时的最大延迟 >	可选参数。 允许您指定向 Kaspersky Industrial CyberSecurity for Networks 服务器发送事件时的最大延迟。当指定的时间用完时，该应用程序将尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。
/events-limit:<1|0>	可选参数。 让您限制发送的事件数量。如果事件数量超过配置的限制，应用程序将停止发送事件。
/events-per-hour:< 每小时最大事件数 >	必需参数，如果 /EVENTS-LIMIT:1 被传递。 允许您指定每小时发送的最大事件数。

/pwd:< 密码 >	可选参数。 允许您指定 KLAdmin 用户或具有足够权限配置集成的用户的密码。 如果未指定此选项，应用程序将在下一行提示您输入密码。
/login:< 用户名 >	可选参数。 允许您指定具有足够权限来配置集成的用户名。 如果未指定此选项，应用程序将在下一行提示您输入用户名。 如果您输入了 KLAdmin 密码，则无需输入此值。
/virtual-span-enable	可选参数。 启用遥测的混杂模式。 默认情况下，Kaspersky Industrial CyberSecurity for Nodes 收集到达计算机网络接口并发往安装应用程序的计算机的网络流量。在混杂模式下，应用程序收集来自所有可用子网的计算机网络接口的网络流量。该应用程序使用收集到的流量来生成扩展遥测。 并非所有网络适配器都支持Promiscuous mode。扩展遥测收集在这些网络适配器上不起作用。
/virtual-span-disable	可选参数。 禁用遥测的混杂模式。
/virtual-span-add-rules:< 计算机网络接口的 IPv4 地址 >	可选参数。 您可以将子网添加为计算机网络接口的地址（应用程序通过网络接口的子网掩码识别相应的子网）或具有 IPv4 格式的子网的网络接口地址。 应用程序仅以混杂模式收集为指定子网配置的网络接口的网络流量。 例如：/VIRTUAL-SPAN-ADD-RULES:198.51.100.0; 198.51.100.0/24。
/virtual-span-remove-rules:< 子网 ID >	可选参数。 允许您删除具有指定 ID 的子网。可以使用 /VIRTUAL-SPAN-SHOW 命令显示添加的子网及其 ID 的列表。
/mqtt-subscriber-enable	可选参数。 启用 MQTT 订阅者模式以从数据二极管接收遥测数据。 默认禁用 MQTT 订阅者模式。
/mqtt-subscriber-disable	可选参数。 禁用 MQTT 订阅者模式。
/mqtt-server:< 地址 >:< 端口 >	必需参数，如果已传递“/kics-mode:mqtt-publisher”或“/mqtt-subscriber:enable.”参数。 指定 MQTT 代理的地址和端口。 MQTT 代理的默认端口为 1883。
/mqtt-user:< 登录名 >	在 MQTT 代理上配置登录名和密码授权的必需参数。 指定用于 MQTT 代理授权的登录名。
/mqtt-password:< 密码 >	在 MQTT 代理上配置登录名和密码授权的必需参数。 指定用于在 MQTT 代理上进行授权的密码。

数据传输设置

参数	描述
最大事件传输延迟(秒)	应用程序在指定时间后与服务器同步以发送事件。默认设置是 30 秒。
启用限制	该功能有助于优化服务器上的负载。如果选中该复选框，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 Industrial CyberSecurity for Nodes 将停止发送事件。

参数	描述
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 Industrial CyberSecurity for Nodes 在一小时后恢复发送事件。默认设置是每小时 3000 个事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。
超出事件限制的百分比	该应用程序按类型对事件进行排序（例如，“注册表中的更改”事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Industrial CyberSecurity for Nodes 将恢复发送事件。默认设置为 15%。

监控 EDR 操作

*EDR 操作监控中心*是一个控制台，您可以在其中查看所有 Kaspersky Detection and Response 解决方案的威胁响应历史记录。如果您的组织部署了多个 Detection and Response，Kaspersky Industrial CyberSecurity for Nodes 将显示所有解决方案的威胁响应历史记录。这使您可以在单独的计算机上分析 Detection and Response 解决方案的性能并优化这些解决方案的设置。

监控中心提供以下信息：

- 有关威胁响应任务（例如“*终止进程*”任务）的信息
- 网络隔离和执行防护规则的变化

如果威胁响应遇到与访问网络共享相关的错误，则会从显示的威胁响应历史记录中省略此类错误。

要打开 EDR 操作监控中心控制台：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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 **遥测采集服务器** → **响应历史**。

   这将打开 EDR 操作监控中心控制台。您可以使用控制台查看威胁响应任务状态、任务持续时间、规则更改和发起者详细信息。

与 SIEM 集成

Kaspersky Industrial CyberSecurity for Nodes 允许连接到 SIEM 系统以发送事件，以便分析和响应潜在威胁。SIEM 系统允许您在安全威胁对组织造成危害之前检测、分析和消除它们。

与 SIEM 系统集成意味着安装在运行 Windows 操作系统的计算机上（作为组织 IT 基础设施的一部分）的 Kaspersky Industrial CyberSecurity for Nodes 会将有关安全事件和 Windows 事件日志事件的数据发送到 SIEM 服务器。

设置 SIEM 集成涉及以下步骤：

1. **安装 SIEM 集成组件**

   在安装包设置或安装向导中，或通过更改 Windows 控制面板中的应用程序组件集，在必须选择要安装的应用程序组件的步骤中，选择以下内容：**完整功能 → 端点代理 → SIEM 整合**。

2. **启用并配置 SIEM 整合组件**

   默认情况下，不使用 SIEM 集成。您可以启用和禁用 SIEM 集成，并配置相关设置。

   通过配置到多个 SIEM 服务器的连接，您可以降低事件无法发送到 SIEM 服务器的风险。Kaspersky Industrial CyberSecurity for Nodes 连接到列表中第一个 SIEM 服务器。如果连接尝试失败，Kaspersky Industrial CyberSecurity for Nodes 会尝试逐个连接到列表中的其他服务器。Kaspersky Industrial CyberSecurity for Nodes 还使用系统审核事件来通知您尝试连接 SIEM 服务器不成功以及将事件发送到 SIEM 服务器时出错。

   如何在 Kaspersky Security Center 管理控制台中配置 SIEM 集成

   1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
   2. 选择必要的策略并双击以打开策略属性。
   3. 选择“**遥测采集服务器**”部分。
   4. 在“**SIEM 整合**”块中单击“**设置**”按钮。
      “**SIEM 整合**”窗口将打开。
   5. 选择**SIEM 整合**复选框。
   6. 配置 SIEM 服务器连接以发送安全事件：
      a. 转到“**安全事件传输设置**”选项卡。
      b. 单击“**添加**”。
      c. 这将打开“**添加服务器**”窗口，在该窗口中，输入 SIEM 服务器地址（IPv4、DNS）、端口和连接协议。
      d. 单击“**TCP 连接安全设置**”。
      e. 这将打开“**TCP 连接安全设置**”窗口；在该窗口中，管理 SIEM 服务器连接设置（请参阅下表）。

f. 如有必要，在“**事件传输到 SIEM 服务器的设置**”块选择“**删除已发送到远程 syslog 服务器的事件的本地副本**”复选框。如果选中该复选框，则应用程序在事件被成功发布到 SIEM 服务器后删除事件的本地副本。推荐在低性能设备上使用此模式。如果清除该复选框，则应用程序仅将事件发送到 SIEM 服务器。日志的副本将继续保存在本地。默认下，复选框被清除。

应用程序永远不会删除安全日志的本地版本。

g. 在“**事件格式**”块中，选择您要将应用程序事件转换成的格式，以便能够将它们发送到 SIEM 服务器。**将事件转换为 STRUCTURED-DATA** 默认选中该选项。建议根据使用的 SIEM 服务器的配置来选择事件的格式。

7. 配置 SIEM 服务器连接以发送 Windows 事件日志事件：

a. 转到“**Windows 事件传输设置**”选项卡。

b. 如果您需要为 Kaspersky Industrial CyberSecurity for Nodes 和 SIEM 服务器之间的连接启用加密，请在“**SIEM 服务器连接设置**”下，选中“**使用 TLS 加密**”复选框。

c. 单击“**添加**”。

d. 这将打开“**SIEM 服务器**”窗口，在该窗口中，输入 SIEM 服务器地址（IPv4、DNS）、端口和连接协议。

e. 单击“**SIEM 服务器连接设置**”。

f. 这将打开“**SIEM 服务器连接设置**”窗口；在该窗口中，管理 SIEM 服务器连接设置（请参阅下表）。

g. 如有必要，在“**数据传输设置**”块配置“**最大事件传输延迟(秒)**”设置。当指定的时间用完时，Kaspersky Industrial CyberSecurity for Nodes 将再次尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

8. 关闭挂锁以将策略应用于计算机。

9. 点击“**确定**”保存更改。

如何在 Kaspersky Security Center Web Console 中配置 SIEM 集成

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**遥测采集服务器**”部分。

5. 在“**SIEM 整合**”块中单击“**配置**”按钮。
“**SIEM 整合**”窗口将打开。

6. 选择**"启用 SIEM 整合"**复选框。

7. 配置 SIEM 服务器连接以发送安全事件：

   a. 转到“**安全事件传输设置**”选项卡。

   b. 单击“**添加**”。

   c. 这将打开“**SIEM 服务器**”窗口，在该窗口中，输入 SIEM 服务器地址（IPv4、DNS）、端口和连接协议。

   d. 在“**连接保护**”区域，单击“**SIEM 服务器连接设置**”链接。

   e. 这将打开“**SIEM 服务器连接设置**”窗口；在该窗口中，管理 SIEM 服务器连接设置（请参阅下表）。

   f. 在“**事件格式**”区域中，指定您要将应用程序事件转换成的格式，以便能够将它们发送到 SIEM 服务器。**将事件转换为 STRUCTURED-DATA** 默认选中该选项。建议根据使用的 SIEM 服务器的配置来选择事件的格式。

   g. 如有必要，在“**连接设置**”块选择“**删除已发送到远程 syslog 服务器的事件的本地副本**”复选框。如果选中该复选框，则应用程序在事件被成功发布到 SIEM 服务器后删除事件的本地副本。推荐在低性能设备上使用此模式。如果清除该复选框，则应用程序仅将事件发送到 SIEM 服务器。日志的副本将继续保存在本地。默认下，复选框被清除。

      应用程序永远不会删除安全日志的本地版本。

8. 配置 SIEM 服务器连接以发送 Windows 事件日志事件：

   a. 转到“**Windows 事件传输设置**”选项卡。

   b. 单击“**添加**”。

   c. 这将打开“**SIEM 服务器**”窗口，在该窗口中，输入 SIEM 服务器地址（IPv4、DNS）、端口和连接协议。

   d. 在“**连接保护**”区域，单击“**SIEM 服务器连接设置**”链接。

   e. 这将打开“**SIEM 服务器连接设置**”窗口；在该窗口中，管理 SIEM 服务器连接设置（请参阅下表）。

   f. 如有必要，在“**连接设置**”块配置“**最大事件传输延迟(秒)**”设置。当指定的时间用完时，Kaspersky Industrial CyberSecurity for Nodes 将再次尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

9. 点击“**确定**”保存更改。

如何在应用程序控制台中配置 SIEM 集成

1. 在应用程序控制台树中，选择“**Endpoint Agent 遥测 → SIEM 整合**”部分。

2. 在结果窗格中单击“**属性**”链接。
   “**属性: SIEM 整合**”窗口将打开。

3. 选择**SIEM 整合**复选框。

4. 配置 SIEM 服务器连接以发送安全事件：

   a. 转到“**安全事件传输设置**”选项卡。

   b. 单击“**添加**”。

   c. 这将打开“**添加服务器**”窗口，在该窗口中，输入 SIEM 服务器地址（IPv4、DNS）、端口和连接协议。

   d. 单击“**TCP 连接安全设置**”。

   e. 这将打开“**TCP 连接安全设置**”窗口；在该窗口中，管理 SIEM 服务器连接设置（请参阅下表）。

   f. 如有必要，在“**事件传输到 SIEM 服务器的设置**”块选择“**删除已发送到远程 syslog 服务器的事件的本地副本**”复选框。如果选中该复选框，则应用程序在事件被成功发布到 SIEM 服务器后删除事件的本地副本。推荐在低性能设备上使用此模式。如果清除该复选框，则应用程序仅将事件发送到 SIEM 服务器。日志的副本将继续保存在本地。默认下，复选框被清除。

      应用程序永远不会删除安全日志的本地版本。

5. 在“**事件格式**”块中，选择您要将应用程序事件转换成的格式，以便能够将它们发送到 SIEM 服务器。**将事件转换为 STRUCTURED-DATA** 默认选中该选项。建议根据使用的 SIEM 服务器的配置来选择事件的格式。

6. 配置 SIEM 服务器连接以发送 Windows 事件日志事件：

   a. 转到“**Windows 事件传输设置**”选项卡。

   b. 如果您需要为 Kaspersky Industrial CyberSecurity for Nodes 和 SIEM 服务器之间的连接启用加密，请在“**SIEM 服务器连接设置**”下，选中“**使用 TLS 加密**”复选框。

   c. 单击“**添加**”。

   d. 这将打开“**SIEM 服务器**”窗口，在该窗口中，输入 SIEM 服务器地址（IPv4、DNS）、端口和连接协议。

   e. 单击“**SIEM 服务器连接设置**”。

   f. 这将打开“**SIEM 服务器连接设置**”窗口；在该窗口中，管理 SIEM 服务器连接设置（请参阅下表）。

   如有必要，在“**数据传输设置**”块配置“**最大事件传输延迟(秒)**”设置。当指定的时间用完时，Kaspersky Industrial CyberSecurity for Nodes 将再次尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

7. 点击“**确定**”保存更改。

SIEM 服务器连接设置

参数	描述
超时(秒)	最大 SIEM 服务器响应超时。当超时用完时，Kaspersky Industrial CyberSecurity for Nodes 会尝试连接到不同的 SIEM 服务器。
服务器 TLS 证书	用于与 SIEM 服务器建立受信任连接的 TLS 证书。您可以使用 SIEM 管理界面获取 TLS 证书。
使用双向认证	在 Kaspersky Industrial CyberSecurity for Nodes 和 SIEM 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 SIEM 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。配置 SIEM 设置后，您需要使用复选框在 Kaspersky Industrial CyberSecurity for Nodes 设置中启用双向身份验证并加载受密码保护的加密容器。 加密容器必须受密码保护。无法添加密码为空的加密容器。

过滤要发送到 SIEM 的事件

为了提高性能并优化向 SIEM 服务器的数据传输，您可以手动从遥测中添加或排除单个事件。例如，您可以排除 Sysmon 事件。

Kaspersky Industrial CyberSecurity for Nodes 支持多达 1500 个包含和排除规则，用于过滤总共的遥测事件。

如何在 Kaspersky Security Center 管理控制台中创建要发送到您的 SIEM 的事件列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，转到“**补充**”区域。
4. 在“**SIEM 遥测**”块中单击“**设置**”按钮。
5. 在显示的窗口中，配置要发送给 SIEM 的事件过滤器。
   您可以为标准*Application*、*Security*、*System*日志配置事件过滤器或手动添加另一个日志。
   a. 点击“**添加**”或通过单击“**编辑**”打开日志属性。
   b. 选择事件发送模式：
      - “**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）。
      - “**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。

c. 为相关事件发送模式创建排除规则或包含规则列表。

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。要指定多个事件 ID，请使用逗号（,）。

6. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Web Console 中创建要发送到 SIEM 的事件列表

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**补充**”部分。
5. 在“**遥测设置**”块中单击“**配置**”按钮。
   “**遥测设置**”窗口将打开。
6. 转到“**SIEM 遥测**”选项卡。
7. 配置事件过滤器以发送到 SIEM。
   您可以为标准*Application*、*Security*、*System*日志配置事件过滤器：
   a. 单击您要对其配置规则的日志名称。
   b. 这打开了一个窗户；在该窗口中，选择一个事件发送模式：
      - “**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）。
      - “**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。
   c. 为相关事件发送模式创建排除规则或包含规则列表。
   要添加规则，您需要指定规则名称和 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。要指定多个事件 ID，请使用逗号（,）。如果必要，您可以添加规则的描述。
8. 保存更改。要在计算机上应用该策略，请关闭锁 。

导出和导入遥测事件过滤规则

Kaspersky Industrial CyberSecurity for Nodes 允许使用遥测事件过滤规则导入和导出 JSON 文件。

Kaspersky Industrial CyberSecurity for Nodes 支持多达 1500 个包含和排除规则，用于过滤总共的遥测事件。

如果计算机上已经存在事件过滤规则，Kaspersky Industrial CyberSecurity for Nodes 会在导入时替换这些规则。

例子：可以将排除列表导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。还可以使用导出和导入功能备份事件过滤器或将列表迁移到其他服务器。

如何在 Kaspersky Security Center 管理控制台中导出和导入事件过滤规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，转到“**补充**”区域。
4. 在“**SIEM 遥测**”块中单击“**设置**”按钮。
5. 要导出事件过滤器：
   a. 选择您想要导出的带有过滤器的事件日志。
   b. 单击 按钮打开上下文菜单并选择“**导出**”。
   c. 这将打开一个窗口；在该窗口中，指定要将事件过滤器导出到的文件的名称，并选择要在其中保存该文件的文件夹。
   d. 保存文件。

   Kaspersky Industrial CyberSecurity for Nodes 会将事件过滤器导出到 JSON 文件。
6. 要导入事件过滤器：
   a. 单击 按钮打开上下文菜单并选择“**导入**”。
   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。
   c. 打开文件。
7. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Security Center Web Console 中导出和导入事件过滤规则

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**补充**”部分。
5. 在“**遥测设置**”块中单击“**配置**”按钮。
   “**遥测设置**”窗口将打开。
6. 转到“**SIEM 遥测**”选项卡。
7. 要导出事件过滤器：
   a. 选择您想要导出的带有过滤器的事件日志。
   b. 单击“**导出**”。
   c. 这将打开一个窗口；在该窗口中，指定要将事件过滤器导出到的文件的名称，并选择要在其中保存该文件的文件夹。
   d. 保存文件。
   Kaspersky Industrial CyberSecurity for Nodes 会将事件过滤器导出到 JSON 文件。
8. 要导入事件过滤器：
   a. 单击“**导入**”。
   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。
   c. 打开文件。
9. 保存更改。要在计算机上应用该策略，请关闭锁 。

如何在 Kaspersky Industrial CyberSecurity for Nodes 控制台中导出和导入事件过滤规则。

1. 在应用程序控制台树中，选择“**遥测设置**”节点。
2. 在“**SIEM 遥测**”块中单击“**设置**”按钮。

3. 要导出事件过滤器：

   a. 单击“**导出**”。

   b. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。

   c. 保存文件。

   Kaspersky Industrial CyberSecurity for Nodes 会将事件过滤器导出到 JSON 文件。

4. 要导入事件过滤器：

   a. 单击“**导入**”。

   b. 在显示的对话框中，确认修改 SIEM 遥测设置。

   c. 选择要从中导入事件过滤器的 JSON 文件。

   d. 打开文件。

5. 点击“**确定**”保存更改。

如何在命令行上导出和导入事件过滤规则

1. 使用本地管理员权限运行命令行解释器（例如，命令提示符 cmd.exe）。

2. 要运行命令，请转到 kavshell.exe 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

3. 要导出事件过滤器，运行以下命令：

   `KAVSHELL TELEMETRYFILTERS /EXPORT <文件名>`

   如果命令仅包含要导出设置的文件的名称，则应用程序将按如下方式放置文件：

   - 如果将 kavshell.exe 的路径添加到 %PATH% 系统变量中，则应用程序会将文件放在运行命令的文件夹中。
   - 如果从应用程序安装文件夹运行该命令，则导出将失败，因为应用程序的自我保护会阻止在应用程序文件夹中创建新文件。要将应用程序设置导出到文件，请输入文件路径。

4. 要导入事件过滤规则，运行以下命令：

   `KAVSHELL TELEMETRYFILTERS /IMPORT <JSON 文件的完整路径>`

使用 Sigma 规则进行异常检测

如果存在具有 EDR Optimum 和 ICS 遥测许可对象的活动 Kaspersky Industrial CyberSecurity for Nodes 授权许可密钥，则此功能可在运行 Windows 7 或更高版本或 Windows Server 2008 R2 或更高版本的计算机上使用。

对于使用 Sigma 规则进行异常检测，您必须启用以下组件：实时文件保护、漏洞利用防御、修复引擎。

Sigma 是一种描述异常检测规则的格式，Kaspersky Industrial CyberSecurity for Nodes 使用它来分析来自内部事件和事件日志的数据。以 Sigma 格式编写的规则称为 Sigma 规则。每个 Sigma 规则都存储在单独的 YAML 文件中。

Sigma 规则以 YAML 编写，具有统一的结构。这允许专门创建的转换器根据 Sigma 规则生成各种 SIEM 系统的语法规则。

Sigma 规则结构

该表包含有关 Sigma 规则的属性和部分的基本信息，这些信息由 Kaspersky Industrial CyberSecurity for Nodes 进行解释。要了解更多详细信息，请关注此链接。

属性值区分大小写。例如，Kaspersky Industrial CyberSecurity for Nodes 将可执行文件 AnyDesk.exe 和 anyDesk.exe 的名称视为不同。

Sigma 规则结构

<table>
<tr><th>属性/部分</th><th>必需的</th><th>描述</th></tr>
<tr><td>logsource</td><td>是</td><td>在此部分中，您可以定义应用程序将搜索异常的事件来源。本部分的主要属性是“category”、“product”和“service”。
Kaspersky Industrial CyberSecurity for Nodes 支持的事件源
Kaspersky Industrial CyberSecurity for Nodes 支持的事件源
<table><tr><th>来源（logsource）</th><th>事件</th></tr><tr><td>category: process_creation
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析内部进程启动事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 1，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。</td></tr><tr><td>category: driver_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析内部驱动程序加载事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 6，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。</td></tr><tr><td>category: image_load
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 7，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。</td></tr><tr><td>category: registry_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析内部事件实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的事件 EventID 12、EventID 13 和 EventID 14，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。</td></tr><tr><td>category: dns_query
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 22，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。</td></tr><tr><td>category: file_rename
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Windows 跟踪服务提供商 Microsoft-Windows-Kernel-File 的日志中的事件，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。</td></tr><tr><td>category: file_event
product: windows</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 11，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。</td></tr><tr><td>product: windows
service: application</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/Application 日志的事件。</td></tr><tr><td>product: windows
service: security</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/Security 日志的事件。</td></tr><tr><td>product: windows
service: system</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/System 日志的事件。</td></tr><tr><td>category: chronicle_journal
product: deltav</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析与 Emerson DeltaV 系统事件日志中的规范化数据相关的内部事件实例。
源事件未链接到外部事件日志。</td></tr><tr><td>product: windows
service: powershell-classic</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析来自 Windows PowerShell 日志的事件。</td></tr><tr><td>product: windows
service: powershell</td><td>Kaspersky Industrial CyberSecurity for Nodes 分析来自 Microsoft-Windows-PowerShell/Operational 日志的事件。</td></tr></table>在 Microsoft Windows 7 中，对于category: dns_query，service: powershell-classic，service: powershell您缺少一些内部事件，或者事件中可能缺少某些字段或必要的数据。因此，Sigma 规则可能不会触发。
在此链接阅读更多内容。</td></tr>
<tr><td>title</td><td>是</td><td>规则名称，表明它检测什么。最大长度为 256 个字符。
例如：
title: 创建新的 RAT 服务</td></tr>
<tr><td>id</td><td>否</td><td>该规则的全局唯一标识符。例如：
id: 929a690e-bef0-4204-a928-ef5e620d6fcc</td></tr>
<tr><td>status</td><td>否</td><td>规则状态。可能的值：stable，test，experimental，deprecated，unsupported。
例如：
status: test</td></tr>
<tr><td>description</td><td>否</td><td>规则的描述以及它可以检测到的恶意的活动。最大长度为 65,535 个字符。
例如：
description: 检测新远程实用工具主机应用程序服务的安装。</td></tr>
<tr><td>license</td><td>否</td><td>根据 SPDX ID 规范的授权许可 ID。该规则是根据指定授权许可类型的条款发布的。</td></tr>
</table>

author	否	任何指明规则作者的说明符。例如名字、姓氏、昵称、社交网络 ID。
reference	否	规则来源的链接。例如，博客文章或白皮书。
date	否	规则创建的日期，格式为 YYYY/MM/DD。
modified	否	以下某个规则属性发生更改时的日期（采用 YYYY/MM/DD 格式）：`title`，`status`，`logsource`，`detection`，`level`。
tags	否	用于对规则进行分类的标签。在此链接阅读更多内容。

category	否	定义应用程序在其事件日志中搜索异常的产品类别。例如：防火墙、互联网、反病毒或通用。
		`logsource:`
		`  category: firewall`

product	否	定义应用程序在其事件日志中搜索异常的软件产品或操作系统。例如：
		`logsource:`
		`  product: Windows`

service	否	定义一个服务，应用程序会在其事件日志中搜索异常。例如：
		`logsource:`
		`  service: AppLocker`

definition	否	应用程序搜索异常的事件日志来源的具体描述。
detection	是	此部分包含一个或多个用于搜索事件日志中的异常的条件以及规则触发条件。列表、词典或它们的组合可用作搜索条件。 Kaspersky Industrial CyberSecurity for Nodes 不支持`windash`值修饰符。

list	否	事件日志中任何参数的值的列表，通过逻辑 OR 组合而成。例如：
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		根据条件，将搜索以下匹配项：`OriginalFileName='AnyDesk.exe'` OR `OriginalFileName='TeamViewer.exe'`.

dictionary	否	*事件日志参数-值* 对。它们通过逻辑“AND”连接起来。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		根据条件，将搜索以下匹配项：EventLog=’Security’ AND Event ID=517。

列表和字典的组合	否	由事件日志设置值和词典组成的列表。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		根据条件，将搜索以下匹配项：EventLog=’Security’ AND (Event ID=517 OR Event ID=1102)

condition	是	规则触发条件。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

fields	否	事件日志中的某些行可能引起分析师对后续事件分析的兴趣。

falsepositives	否	可能错误触发规则的已知场景列表。例如：
		`falsepositives:`
		`- 系统管理员使用实用程序`

level	否	使用该规则可以发现的异常严重程度的指标。可能的值：`informational`，`low`，`medium`，`high`，`critical`。

Sigma 规则示例

```yaml
title: 使用 CertUtil.exe 下载文件
id: 89346938-3b2f-46c7-bb38-b9f244e3fad0
status: test
description: 使用 CertUtil.exe 检测文件下载。
references:
  - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil
author: Kaspersky
date: 2024-05-22
tags:
  - attack.defense_evasion
  - attack.t1027
logsource:
  category: process_creation
  product: windows
detection:
  selection_image:
    - Image|endswith: '\certutil.exe'
    - OriginalFileName: 'CertUtil.exe'
  selection_http:
    CommandLine|contains: 'http'
condition: all of selection_*
falsepositives:
  - 系统管理员的合法行为。
level: low
```

*Sigma 规则集合*是一组定义类似事件的 Sigma 规则。

Kaspersky Industrial CyberSecurity for Nodes 使用卡巴斯基提供的 Sigma 规则集合和应用程序数据库以及用户创建的 Sigma 规则集合来分析内部事件和事件日志中的数据以查找异常。

当使用某些 Sigma 规则时，应用程序可以对受保护计算机的安全审计策略（本地 Windows 安全策略的一部分）进行更改。

使用 Sigma 规则进行异常检测的特殊考虑和限制

使用 Sigma 规则的异常检测功能具有以下限制：

- 为了使“DeltaV 主机上的 Windows 事件日志修改或删除”Sigma 规则正常工作，在安装“使用 Sigma 规则进行异常检测”组件后，必须重新启动计算机或停止 Windows 事件日志服务并再次启动它。

  1. 启动 Windows 服务应用程序 (services.msc)。
  2. 在服务列表中，找到 Windows 事件日志。
  3. 在 Windows 事件日志服务的上下文菜单中，选择“**停止**”停止服务。
  4. 在 Windows 事件日志服务的上下文菜单中，选择“**启动**”启动服务。

- 不支持以下值修饰符：`base64offset`、`cidr`、`lt`、`windash`。
- 不支持正则表达式。
- 不支持转义通配符。

- 应用程序将 `?` 通配符视为 `*`。
- 不支持“`condition: not selection`”结构，但支持“`condition: selection and not filter`”结构。
- 不支持没有指定一个或多个 `EventID` 参数值作为搜索 Windows 事件日志异常条件的规则。
- 对于描述文件操作的 Sigma 规则，报告包括前 50 次检测。如果某个进程对具有相似路径的文件执行操作，则每个进程的检测次数将分别计数。
- 该应用程序支持 Windows XP 和 Windows Server 2003 计算机上的 Sigma 规则，但有一些限制。在运行这些操作系统的计算机上打开检测警报详细信息可能会失败，出现“*打开警报详情失败。可能的原因：主机离线、网络问题、警报存储期过期。*”错误。您可以使用 Kaspersky Industrial CyberSecurity for Networks 打开警报详细信息。

使用 Sigma 规则启用异常检测

要使用 Sigma 规则启用异常检测：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**使用 Sigma 规则的异常检测**”区域中，选择“**启用使用 Sigma 规则的异常检测**”复选框。
5. 添加一个或多个 Sigma 规则集合。
6. 单击“**保存**”按钮。
   Kaspersky Industrial CyberSecurity for Nodes 将使用启用的 Sigma 规则集合搜索异常。

添加 Sigma 规则集合

要添加 Sigma 规则集合：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**使用 Sigma 规则的异常检测**”区域中单击“**添加**”。
   “**添加规则集合**”窗口将打开。

5. 使用“**选择规则集合**”下拉列表做以下事情之一：

   - 选择一个预定义的 Sigma 规则集合。

     如果未显示预定义的 Sigma 规则集合，请确保使用具有 EDR Optimum 和 ICS 遥测对象的授权许可密钥激活应用程序。您还可以运行“*将更新下载至管理服务器存储库*”任务以更新预定义集合。

   - 选择“**自定义规则集合**”选项以添加自定义 Sigma 规则集合。

6. 如果您要添加自定义 Sigma 规则集合，请在相应字段中输入该集合的唯一名称。

7. 单击“**确定**”。

   在“**使用 Sigma 规则的异常检测设置**”部分中，会出现一行，其中包含已创建的规则集合的名称，该集合默认启用（集合名称左侧的切换按钮位于“**已启用**”位置）。当您创建自定义 Sigma 规则集合时，它最初不包含任何规则。

更改 Sigma 规则集合的状态

默认情况下，添加 Sigma 规则集合后，该集合将处于启用状态 - 集合名称左侧的切换按钮位于“**已启用**”位置。您可以更改 Sigma 规则集合的状态。

要更改 Sigma 规则集合的状态：

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在“**使用 Sigma 规则的异常检测**”部分中，将切换按钮的位置更改为要更改其状态的 Sigma 规则集合名称左侧的位置：

   - **已启用** — 该收集已启用并用于检测异常。

   - **已禁用** — 该收集已被禁用并且不用于异常检测。

5. 单击“**保存**”。

Kaspersky Industrial CyberSecurity for Nodes 使用已启用的 Sigma 规则集合来搜索异常。

将 Sigma 规则添加到自定义集合

要将 Sigma 规则添加到自定义集合：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**使用 Sigma 规则的异常检测**”部分中，使用集合名称旁边的复选框选择要向其中添加一个或多个 Sigma 规则的自定义 Sigma 规则集合。
5. 单击“**编辑**”。
   “**更改 Sigma 规则集合**”窗口将打开。
6. 通过以下方式之一添加 Sigma 规则：
   - 手动：
     a. 单击“**添加**”。
        “**更改 Sigma 规则**”窗口将打开。
     b. 在编辑器中，**实用 Sigma 格式**描述规则。

        该表包含有关 Sigma 规则的属性和部分的基本信息，这些信息由 Kaspersky Industrial CyberSecurity for Nodes 进行解释。要了解更多详细信息，请关注此链接。

        属性值区分大小写。例如，Kaspersky Industrial CyberSecurity for Nodes 将可执行文件 AnyDesk.exe 和 anyDesk.exe 的名称视为不同。

Sigma 规则结构

属性/部分	必需的	描述
logsource	是	在此部分中，您可以定义应用程序将搜索异常的事件来源。本部分的主要属性是“category”、“product”和“service”。 **Kaspersky Industrial CyberSecurity for Nodes 支持的事件源** Kaspersky Industrial CyberSecurity for Nodes 支持的事件源 来源（logsource）：事件 category: process_creation, product: windows：Kaspersky Industrial CyberSecurity for Nodes 分析内部进程启动事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 1，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: driver_load, product: windows：Kaspersky Industrial CyberSecurity for Nodes 分析内部驱动程序加载事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 6，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: image_load, product: windows：Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 7，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: registry_event, product: windows：Kaspersky Industrial CyberSecurity for Nodes 分析内部事件实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的事件 EventID 12、EventID 13 和 EventID 14，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: dns_query, product: windows：Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 22，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: file_rename, product: windows：Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Windows 跟踪服务提供商 Microsoft-Windows-Kernel-File 的日志中的事件，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: file_event, product: windows：Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 11，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 product: windows, service: application：Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/Application 日志的事件。 product: windows, service: security：Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/Security 日志的事件。 product: windows, service: system：Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/System 日志的事件。 category: chronicle_journal, product: deltav：Kaspersky Industrial CyberSecurity for Nodes 分析与 Emerson DeltaV 系统事件日志中的规范化数据相关的内部事件实例。源事件未链接到外部事件日志。 product: windows, service: powershell-classic：Kaspersky Industrial CyberSecurity for Nodes 分析来自 Windows PowerShell 日志的事件。 product: windows, service: powershell：Kaspersky Industrial CyberSecurity for Nodes 分析来自 Microsoft-Windows-PowerShell/Operational 日志的事件。 在 Microsoft Windows 7 中，对于 category: dns_query，service: powershell-classic，service: powershell 您缺少一些内部事件，或者事件中可能缺少某些字段或必要的数据。因此，Sigma 规则可能不会触发。 在此链接阅读更多内容。
title	是	规则名称，表明它检测什么。最大长度为 256 个字符。 例如： `title: 创建新的 RAT 服务`
id	否	该规则的全局唯一标识符。例如： `id: 929a690e-bef0-4204-a928-ef5e620d6fcc`
status	否	规则状态。可能的值：stable，test，experimental，deprecated，unsupported。 例如： `status: test`
description	否	规则的描述以及它可以检测到的恶意的活动。最大长度为 65,535 个字符。 例如： `description: 检测新远程实用工具主机应用程序服务的安装。`

license	否	根据 SPDX ID 规范的授权许可 ID。该规则是根据指定授权许可类型的条款发布的。
author	否	任何指明规则作者的说明符。例如名字、姓氏、昵称、社交网络 ID。
reference	否	规则来源的链接。例如，博客文章或白皮书。
date	否	规则创建的日期，格式为 YYYY/MM/DD。
modified	否	以下某个规则属性发生更改时的日期（采用 YYYY/MM/DD 格式）：title，status，logsource，detection，level。
tags	否	用于对规则进行分类的标签。在此链接阅读更多内容。

category	否	定义应用程序在其事件日志中搜索异常的产品类别。例如：防火墙、互联网、反病毒或通用。
		`logsource:`
		`  category: firewall`

product	否	定义应用程序在其事件日志中搜索异常的软件产品或操作系统。例如：
		`logsource:`
		`  product: Windows`

service	否	定义一个服务，应用程序会在其事件日志中搜索异常。例如：
		`logsource:`
		`  service: AppLocker`

definition	否	应用程序搜索异常的事件日志来源的具体描述。
detection	是	此部分包含一个或多个用于搜索事件日志中的异常的条件以及规则触发条件。列表、词典或它们的组合可用作搜索条件。 Kaspersky Industrial CyberSecurity for Nodes 不支持windash值修饰符。

list	否	事件日志中任何参数的值的列表，通过逻辑 OR 组合而成。例如：
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		根据条件，将搜索以下匹配项：OriginalFileName='AnyDesk.exe' OR OriginalFileName='TeamViewer.exe'.

dictionary	否	*事件日志参数-值* 对。它们通过逻辑“AND”连接起来。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		根据条件，将搜索以下匹配项：EventLog='Security' AND Event ID=517。

列表和字典的组合	否	由事件日志设置值和词典组成的列表。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		根据条件，将搜索以下匹配项：EventLog='Security' AND (Event ID=517 OR Event ID=1102)

condition	是	规则触发条件。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

fields	否	事件日志中的某些行可能引起分析师对后续事件分析的兴趣。

falsepositives	否	可能错误触发规则的已知场景列表。例如：
		`falsepositives:`
		`- 系统管理员使用实用程序`

level	否	使用该规则可以发现的异常严重程度的指标。可能的值：informational，low，medium，high，critical。

c. 单击“**确定**”。

所描述的 Sigma 规则将显示在集合中的规则列表中。该规则默认启用（规则名称左侧的切换按钮位于“**已启用**”位置）。

d. 对每个手动添加的规则重复步骤 a-c。

- 来自文件：

a. 单击“**添加文件**”。

b. 在打开的窗口中，选择一个或多个描述 Sigma 规则的 YAML 文件。

c. 单击“**打开**”。

YAML 文件中描述的 Sigma 规则将显示在集合中的规则列表中。规则默认启用（规则名称左侧的切换开关位于“**已启用**”位置）。

> 如果 Sigma 规则包含语法错误或缺少强制属性，则该规则将不会添加到集合中。

7. 单击“**确定**”。

用户账户控制

使用 Sigma 规则的异常检测组件使用 Sigma 规则的预定义集合（*用户账户控制 (UAC) 日志分析的规则收集*）提供用户账户控制功能。

Sigma 规则集合涵盖以下事件：

- 添加新用户
- 将用户添加到管理员组
- 用户权限提升
- 用户登录名
- 用户登录尝试
- 用户退出

ID 列表见下表。

应用程序的行为取决于计算机是否属于域：

- 如果计算机属于域，则应用程序不会生成用户账户控制 Sigma 规则集合的事件。
- 如果计算机不属于域，则应用程序将修改某些本地策略设置。禁用 Sigma 规则集合后，应用程序将本地策略设置还原为其原始值。

要启用用户账户控制：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**使用 Sigma 规则的异常检测**”区域中单击“**添加**”。
   “**添加规则集合**”窗口将打开。
5. 在“**选择规则集合**”下拉列表中，选择“**用户账户控制 (UAC) 日志分析的规则收集**”Sigma 规则集合。
6. 单击“**确定**”。

当来自集合的 Sigma 规则触发时，应用程序生成一个事件，并将其发送到 Kaspersky Security Center 和 Kaspersky Industrial CyberSecurity for Nodes for Network。

用户账户控制 Sigma 规则集合中的事件 ID

事件	Windows XP	Windows 7 及更高版本
添加新用户	624	4720
将用户添加到管理员组	632 636 660	4728 4732 4756
用户权限提升	576 633 637 639 641 659 661	4729 4733 4735 4737 4755 4757 4672 4964
用户登录名	528 540	4624
用户登录尝试	529 530 531 532 533 534 535 536 537 539	4625
用户退出	538	4634

导出和导入自定义集合的 Sigma 规则

要从自定义集合导出或导入 Sigma 规则：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在“**使用 Sigma 规则的异常检测**”部分中，使用集合名称旁边的复选框选择要向其中添加一个或多个 Sigma 规则的自定义 Sigma 规则集合。

5. 单击“**编辑**”。

   “**更改 Sigma 规则集合**”窗口将打开。

6. 点击“**导出**”按钮从自定义集合中导出 Sigma 规则。

   Kaspersky Industrial CyberSecurity for Nodes 在标准下载文件夹中保存了一个名为 sigma.zip 的存档。

7. 将 Sigma 规则导入自定义集合：

   a. 单击“**导入**”。

   b. 在打开的窗口中，选择包含所述 Sigma 规则的 YAML 文件的 ZIP 存档。

   c. 单击“**打开**”。

   > 如果 Sigma 规则包含语法错误或缺少强制属性，则该规则将不会添加到集合中。

   存档中包含的 Sigma 规则将显示在集合中的规则列表中。

   > 如果导入的 ZIP 存档包含集合中已存在的重复 Sigma 规则，则这些规则将不会被覆盖。

8. 单击“**确定**”。

更改 Sigma 规则

您可以对自定义 Sigma 规则进行任何更改。您只能添加或删除排除项以及更改卡巴斯基实验室提供的 Sigma 规则的状态。

要编辑 Sigma 规则：

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在“**使用 Sigma 规则的异常检测**”部分中，使用集合名称旁边的复选框来选择要编辑的 Sigma 规则的集合。

5. 单击“**编辑**”。

   “**更改 Sigma 规则集合**”窗口将打开。

6. 使用规则名称旁边的复选框选择要编辑的规则。

7. 如有必要，使用规则名称上方的“**已启用/已禁用**”切换按钮更改规则状态。

8. 单击“**编辑**”。

   “**更改 Sigma 规则**”窗口将打开。

9. 如果您正在编辑卡巴斯基实验室提供的作为集合一部分的 Sigma 规则，请添加或删除规则的排除项。

0. 如果您正在编辑自定义 Sigma 规则，请在整个**规则结构**中进行必要的更改。

该表包含有关 Sigma 规则的属性和部分的基本信息，这些信息由 Kaspersky Industrial CyberSecurity for Nodes 进行解释。要了解更多详细信息，请关注此链接。

属性值区分大小写。例如，Kaspersky Industrial CyberSecurity for Nodes 将可执行文件 AnyDesk.exe 和 anyDesk.exe 的名称视为不同。

Sigma 规则结构

属性/部分	必需的	描述
logsource	是	在此部分中，您可以定义应用程序将搜索异常的事件来源。本部分的主要属性是“category”、“product”和“service”。 **Kaspersky Industrial CyberSecurity for Nodes 支持的事件源** Kaspersky Industrial CyberSecurity for Nodes 支持的事件源 来源 (logsource) / 事件 category: process_creation, product: windows — Kaspersky Industrial CyberSecurity for Nodes 分析内部进程启动事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 1，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: driver_load, product: windows — Kaspersky Industrial CyberSecurity for Nodes 分析内部驱动程序加载事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 6，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: image_load, product: windows — Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 7，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: registry_event, product: windows — Kaspersky Industrial CyberSecurity for Nodes 分析内部事件实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的事件 EventID 12、EventID 13 和 EventID 14，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: dns_query, product: windows — Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 22，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: file_rename, product: windows — Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Windows 跟踪服务提供商 Microsoft-Windows-Kernel-File 的日志中的事件，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 category: file_event, product: windows — Kaspersky Industrial CyberSecurity for Nodes 分析内部事件的实例，该事件的内容对应于 Microsoft-Windows-Sysmon/Operational 日志中的 EventID 11，并通过 Kaspersky Industrial CyberSecurity for Nodes 字段进行丰富。 product: windows, service: application — Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/Application 日志的事件。 product: windows, service: security — Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/Security 日志的事件。 product: windows, service: system — Kaspersky Industrial CyberSecurity for Nodes 分析来自 WEL/System 日志的事件。 category: chronicle_journal, product: deltav — Kaspersky Industrial CyberSecurity for Nodes 分析与 Emerson DeltaV 系统事件日志中的规范化数据相关的内部事件实例。 源事件未链接到外部事件日志。 product: windows, service: powershell-classic — Kaspersky Industrial CyberSecurity for Nodes 分析来自 Windows PowerShell 日志的事件。 product: windows, service: powershell — Kaspersky Industrial CyberSecurity for Nodes 分析来自 Microsoft-Windows-PowerShell/Operational 日志的事件。 在 Microsoft Windows 7 中，对于category: dns_query, service: powershell-classic, service: powershell您缺少一些内部事件，或者事件中可能缺少某些字段或必要的数据。因此，Sigma 规则可能不会触发。 在此链接阅读更多内容。
title	是	规则名称，表明它检测什么。最大长度为 256 个字符。 例如： `title: 创建新的 RAT 服务`
id	否	该规则的全局唯一标识符。例如： `id: 929a690e-bef0-4204-a928-ef5e620d6fcc`
status	否	规则状态。可能的值：stable, test, experimental, deprecated, unsupported。 例如： `status: test`
description	否	规则的描述以及它可以检测到的恶意的活动。最大长度为 65,535 个字符。 例如： `description: 检测新远程实用工具主机应用程序服务的安装。`

license	否	根据 SPDX ID 规范的授权许可 ID。该规则是根据指定授权许可类型的条款发布的。
author	否	任何指明规则作者的说明符。例如名字、姓氏、昵称、社交网络 ID。
reference	否	规则来源的链接。例如，博客文章或白皮书。
date	否	规则创建的日期，格式为 YYYY/MM/DD。
modified	否	以下某个规则属性发生更改时的日期（采用 YYYY/MM/DD 格式）：title，status，logsource，detection，level。
tags	否	用于对规则进行分类的标签。在此链接阅读更多内容。

category	否	定义应用程序在其事件日志中搜索异常的产品类别。例如：防火墙、互联网、反病毒或通用。
		`logsource:`
		`  category: firewall`

product	否	定义应用程序在其事件日志中搜索异常的软件产品或操作系统。例如：
		`logsource:`
		`  product: Windows`

service	否	定义一个服务，应用程序会在其事件日志中搜索异常。例如：
		`logsource:`
		`  service: AppLocker`

definition	否	应用程序搜索异常的事件日志来源的具体描述。
detection	是	此部分包含一个或多个用于搜索事件日志中的异常的条件以及规则触发条件。列表、词典或它们的组合可用作搜索条件。 Kaspersky Industrial CyberSecurity for Nodes 不支持windash值修饰符。

list	否	事件日志中任何参数的值的列表，通过逻辑 OR 组合而成。例如：
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`
		根据条件，将搜索以下匹配项：OriginalFileName='AnyDesk.exe' OR OriginalFileName='TeamViewer.exe'.

dictionary	否	*事件日志参数-值* 对。它们通过逻辑“AND”连接起来。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		根据条件，将搜索以下匹配项：EventLog=’Security’ AND Event ID=517。

列表和字典的组合	否	由事件日志设置值和词典组成的列表。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		根据条件，将搜索以下匹配项：EventLog=’Security’ AND (Event ID=517 OR Event ID=1102)

condition	是	规则触发条件。例如：
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

fields	否	事件日志中的某些行可能引起分析师对后续事件分析的兴趣。

falsepositives	否	可能错误触发规则的已知场景列表。例如：
		`falsepositives:`
		`- 系统管理员使用实用程序`

level	否	使用该规则可以发现的异常严重程度的指标。可能的值：informational，low，medium，high，critical。

1. 点击“**确定**”保存更改。

Sigma 规则中的排除项

应用程序数据库提供的 Sigma 规则的内容对用户不可用。这是因为这些规则的触发条件是卡巴斯基的知识产权，不能披露。

在与应用程序数据库一起提供的 Sigma 规则的编辑器中，您只能通过在“detection”部分中指定排除项设置来添加规则排除项。

排除项模板定义如下：

```
detection:
   exclude1:
        - ...
   condition: not 1 of exclude*
```

此模板假定排除项是使用“exclude*”属性指定的，并且规则触发条件假定对用户隐藏的条件得到满足，并且指定的排除项均不匹配。

例如：

```
detection:
   exclude1:
     Image|endswith:
       - '\chrome.exe'
       - '\tor.exe'
   exclude2:
     QueryName|endswith: 'api.parsec.app'
   condition: not 1 of exclude*
```

在规则集合内过滤 Sigma 规则

如果集合中的 Sigma 规则数量很大，并且您需要显示具有特定参数的 Sigma 规则列表，则可以使用过滤器。

要过滤集合中的 Sigma 规则：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**使用 Sigma 规则的异常检测**”部分中，使用集合名称旁边的复选框选择要应用规则过滤器的集合。
5. 单击“**编辑**”。
   “**更改 Sigma 规则集合**”窗口将打开。
6. 单击“**筛选器**”。
   将打开一个带有过滤条件的窗口。

7. 指定您需要的过滤条件的值：

   - “**规则包含文本**”条件根据片段不区分大小写的匹配来选择规则。您可以输入任何规则属性和/或其值。
   - “**规则状态**”条件根据其状态选择规则。
   - “**排除项的可用性**”条件根据排除项的存在来选择规则。

     此条件仅适用于卡巴斯基提供的集合中的过滤规则。

8. 单击“**确定**”。

   符合过滤条件的规则将显示在集合中的规则列表中。

在命令行中使用 Sigma 规则配置异常检测

要通过命令行界面使用 Sigma 规则配置异常检测：

1. 在设备上，使用本地管理员的权限运行命令行解释器（例如，命令提示符 cmd.exe）。
2. 使用 `cd` 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如，输入命令 `cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0` 并按 **ENTER**。
3. 输入以下命令：

   `kavshell.exe sigma /<enable|disable|add|remove|show> [/collection:<rat|deltav|uac|siemens|yokogawa|custom>] [/name:<集合名称>] [/source:<YAML 文件的文件夹完整路径>] [/login:<当前用户账户的名称>] [/pwd:</login 密码或 KLAdmin 密码（如果未指定 /login）>`
4. 按 ENTER 键。

使用 Sigma 规则管理异常检测的命令参数

参数	描述
`sigma /<enable|disable|add|remove|show>`	必需参数。 指定以下操作之一： • `enable` – 使用 Sigma 规则启用异常检测 • `disable` – 使用 Sigma 规则禁用异常检测 • `add` – 添加 Sigma 规则集合 • `remove` – 删除 Sigma 规则集合 • `show` – 显示使用 Sigma 规则的异常检测的当前设置

参数	描述
/collection:<rat|deltav|uac|siemens|yokogawa|custom>	如果指定了“sigma /<add|remove>”，则需要此参数。 指定要添加或删除的 Sigma 规则集合的类型： • rat – 检测管理工具的规则集合(Remote Administration Tool，RAT) • deltaV – Emerson DeltaV Distributed Control System (DCS) 日志分析规则集合 • uac – 分析用户活动日志的规则集合(User Account Control，UAC) • siemens – 分析 Siemens 工业软件日志的规则集合 • yokogawa – 分析 Yokogawa Centum VP Distributed Control System (DCS) 日志的规则集合 • custom – 自定义规则集合 您还可以指定 test。添加或删除了一条专为 AO Kaspersky Lab 内部测试而设计的规则。
/name:< 集合名称 >	如果指定了“sigma /<add|remove>”和“/collection:custom”，则需要此参数。 指定自定义 Sigma 规则集合的名称。
/source:< YAML 文件的文件夹完整路径 >	如果指定了“sigma /add”和“/collection:custom”，则需要此参数。 指定包含描述自定义 Sigma 规则的 YAML 文件的文件夹的完整路径。

对象隔离和备份

本节提供了有关在清除或删除之前备份检测到的恶意对象的信息，以及有关隔离疑似感染对象的信息。

隔离可能已感染对象。隔离

在应对威胁时，Kaspersky Industrial CyberSecurity for Nodes 可能会创建“*移动文件到隔离区*”任务。这对于将威胁的后果降至最低是必要的。隔离区是计算机上的一个特别的本地存储区。管理员可以隔离其认为对计算机有危险的文件。隔离的文件以加密形式存储，因此不会危害您设备的安全。Kaspersky Industrial CyberSecurity for Nodes 仅在与 Endpoint Detection and Response (KSC)、Kaspersky Anti Targeted Attack Platform (KATA) 和 Kaspersky Industrial CyberSecurity for Networks 配合使用时使用隔离区。在其他情况下，Kaspersky Industrial CyberSecurity for Nodes 将相关文件置于备份中。

您可以用以下方式创建*移动文件到隔离区*任务：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  警报详情是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

- 使用任务向导。

  您必须输入文件路径或校验和以及文件夹路径。

“移动文件到隔离区”任务具有以下限制：

- 文件大小不得超过 100 MB。
- 系统关键对象(SCO)无法被隔离。SCO 是操作系统和 Kaspersky Industrial CyberSecurity for Nodes 应用程序运行所需的文件。
- 您可以在 Kaspersky Security Center Web Console 中为 EDR Optimum 配置任务。

如何在 Web Console 中创建“移动文件到隔离区”任务

1. 在 Web Console 的主窗口中，选择“**设备**” → “**任务**”。
   任务列表打开。
2. 单击“**添加**”。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”。
   b. 在“**任务类型**”下拉列表中，选择“**移动文件到隔离区**”。
   c. 在“**任务名称**”字段中，输入任务的简要说明并单击“**下一步**”。
4. 在“**任务范围**”部分，选择受管理设备并单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。
   默认下，Kaspersky Industrial CyberSecurity for Nodes 以系统用户账户 (SYSTEM) 启动任务。
6. 单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。
7. 单击新任务。任务属性窗口将打开。
8. 选择**应用程序设置**选项卡。
9. 在文件列表中，单击“**添加**”。文件添加向导将启动。
10. 要添加文件，您必须输入文件的完整路径或文件夹路径的校验和。

    如果文件位于网络驱动器上，请输入以“\\”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现未找到文件错误。

11. 在任务属性窗口中，选择“**计划**”选项卡。配置任务计划。

    LAN 唤醒不可用于此任务。确保计算机已打开以运行任务。

12. 单击“**保存**”。
13. 选中任务旁边的复选框，然后单击“**启动**”按钮。

结果，Kaspersky Industrial CyberSecurity for Nodes 将文件移动到隔离区。

如果文件被其他进程锁定，则任务显示为“**已通过**”，但文件本身只有在计算机重新启动后才会被隔离。重新启动计算机后，确认文件已删除。

如果试图隔离太大的文件，则“*移动文件到隔离区*”任务可能会以“*隔离区存储空间不足*”错误结束。清空隔离区或增加其大小。然后再次尝试。

您可以使用 Kaspersky Security Center Web Console 从隔离区恢复文件或清空隔离区。

查看隔离对象

您可以在 Kaspersky Security Center 管理控制台和 Web Console 中查看隔离的对象。

[如何在 Kaspersky Security Center 管理控制台中查看隔离的对象]

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**附加**” → “**存储**”。
3. 转到“**隔离区**”文件夹。
4. 有关已隔离对象的信息显示在控制台的右侧窗格中。

如何在 Kaspersky Security Center Web Console 中查看已隔离对象

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**隔离区**”文件夹。
4. 有关已隔离对象的信息显示在控制台的右侧窗格中。

要在已隔离对象列表中查找所需对象，

排序或者过滤对象。

排序隔离的对象

默认情况下，已隔离对象列表中的对象按照隔离日期倒序排列。要查找所需对象，可以按包含对象信息的列来排序对象。要排序对象：

如何在 Kaspersky Security Center 管理控制台中对隔离区中的文件进行排序

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**附加**” → “**隔离区**”。
3. 在文件列表中，选择想要用于排序对象的列标题。

   将基于选定标准排序隔离区中的文件。

如何在 Kaspersky Security Center Web Console 中对隔离区中的文件进行排序

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**隔离区**”。
3. 在文件列表中，选择想要用于排序对象的列标题。

   将基于选定标准排序隔离区中的文件。

筛选隔离的对象

要查找所需的已隔离对象，可以筛选列表中的对象，例如只显示满足您指定的筛选标准（筛选器）的那些对象。

如何在 Kaspersky Security Center 管理控制台中对隔离区中的文件进行过滤

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**附加**” → “**存储**”。
3. 转到“**隔离区**”文件夹。
4. 在右侧窗格中，单击“**未指定过滤器**”链接。
5. 点击”**调整过滤器**”并在”**过滤设置**”窗口中，选择要过滤的列。
6. 为选定的列指定运算符和值。
7. 将保存已创建的筛选器。
8. 要再次显示所有隔离对象，请在”**过滤设置**”窗口中，单击“**全部清除**”。

如何在 Kaspersky Security Center Web Console 中对隔离区中的文件进行排序

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**隔离区**”文件夹。
4. 点击过滤器图标，然后点击“**过滤器**”选项卡上的“**添加**”按钮。
5. 选择要按其过滤的属性。
6. 为选定的属性指定条件和值。
7. 单击“**应用**”。
   过滤器设置被保存。
8. 要恢复显示所有隔离对象，请单击“**过滤器**”选项卡上的“**全部清除**”。

还原已隔离的对象

Kaspersky Industrial CyberSecurity for Nodes 以加密形式将疑似感染对象放入隔离文件夹中，以保护受保护设备免受任何可能的有害影响。

如果您认为对象对于受保护的设备来说是安全的并且想要使用它，您可以从隔离区恢复它。如果您不希望 Kaspersky Industrial CyberSecurity for Nodes 在后续扫描期间将该对象隔离，您可以将该对象从“实时文件保护”任务和“按需扫描”任务的处理中排除，或者，您可以将对象添加到受信任区域。

从隔离区还原对象可能会导致受保护设备感染。

您可以还原一个或多个对象。

在 Kaspersky Security Center 管理控制台中从隔离区恢复对象

1. 在 Kaspersky Security Center 管理控制台树中，选择“**附加**” → “**存储**”文件夹。
2. 转到“**隔离区**”文件夹。
3. 执行下列操作之一：
   - 要恢复一个对象，请从对象名称的上下文菜单中选择“**恢复**”。
   - 要恢复多个对象，请使用 CTRL 或 SHIFT 键选择想要恢复的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**恢复**”。
4. 该对象将被恢复至原始文件夹。

在 Kaspersky Security Center Web Console 中从隔离区恢复对象

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**隔离区**”文件夹。
4. 从列表中选择对象并单击“**恢复**”按钮。
5. 该对象将被恢复至原始文件夹。

从隔离删除对象

您可以在 Kaspersky Security Center 管理控制台和 Web Console 中从隔离区删除对象。

如何在 Kaspersky Security Center 管理控制台中从隔离区删除对象

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**附加**” → “**存储**”。

3. 转到“**隔离区**”文件夹。

4. 执行下列操作之一：

   - 要删除一个对象，请从对象的上下文菜单中选择“**删除**”。
   - 要删除多个对象，请使用 CTRL 或 SHIFT 键选择想要删除的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**删除**”。

5. 对象将被从隔离区中删除。

如何在 Kaspersky Security Center Web Console 中从隔离区删除对象

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**隔离区**”文件夹。
4. 从列表中选择对象并单击“**删除**”按钮。
5. 确认删除。
6. 选定的对象被从备份中删除。

发送疑似感染对象到 Kaspersky 以供分析

如果某个对象的行为使您怀疑该对象可能包含威胁，并且 Kaspersky Industrial CyberSecurity for Nodes 认定该对象是清洁的，则您可能遇到未知威胁，而该威胁的签名尚未添加到数据库。您可以将此对象发送到卡巴斯基以供分析。Kaspersky 的反病毒分析人员将对文件进行分析，如果检测到文件中包含新威胁，则将在数据库中添加记录标识该威胁。当您在数据库更新之后重新扫描对象时，有可能 Kaspersky Industrial CyberSecurity for Nodes 将此对象标识为已感染，并能够将其清除。您不仅能够保留对象，而且能够阻止病毒爆发。

要在 Kaspersky Security Center 管理控制台中将对象发送给卡巴斯基专家进行分析

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**附加**” → “**存储**”。
3. 前往“**隔离区**”或者“**备份**”文件夹。
4. 执行下列操作之一：

   - 要发送一个对象，请从对象名称的上下文菜单中选择“**发送到卡巴斯基**”。
   - 要发送多个对象，请使用 CTRL 或 SHIFT 键选择想要发送的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**发送到卡巴斯基**”。

5. 选择计算机上用于保存对象的文件夹。
6. 此后，系统会提示您前往卡巴斯基威胁情报门户并上传已保存的对象以获取有关它的完整信息。

要在 Kaspersky Security Center Web Console 中将对象发送给卡巴斯基专家进行分析

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 前往“**隔离区**”或者“**备份**”文件夹。
4. 从列表中选择对象并单击“**发送到卡巴斯基**”按钮。
5. 选择计算机上用于保存对象的文件夹。
6. 此后，系统会提示您前往卡巴斯基威胁情报门户并上传已保存的对象以获取有关它的完整信息。

如果隔离和备份对象是在应用程序 4.0 或更早版本升级到 4.5 或更高版本后迁移的，或者这些对象是由 Kaspersky Anti Targeted Attack Platform 或 Kaspersky Industrial CyberSecurity for Networks 放置在存储中的，则 Kaspersky Security Center Web Console 或管理控制台不能用于将隔离和备份对象发送到卡巴斯基进行分析。

配置隔离设置

您可配置隔离设置。保存后将立即应用新的隔离设置。

如何在 Kaspersky Security Center 管理控制台中配置隔离设置

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**补充** → **存储**”并点击“**设置**”。
4. 选择**隔离区**选项卡。
5. 指定隔离设置：
   - 限制隔离区大小为

     该复选框用于启用或禁用监控存储在隔离文件夹中的对象的总大小的功能。如果超过指定的值（默认值为 200 MB），Kaspersky Industrial CyberSecurity for Nodes 会记录“*已超过隔离区最大容量*”事件，并根据此事件类型的通知设置发布通知。

     如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控置于隔离的对象的总大小。

如果清除该复选框，Kaspersky Industrial CyberSecurity for Nodes 不会监控置于隔离的对象的总大小。

默认下，复选框被清除。

- 可用空间阈值

  该复选框用于启用或禁用监控隔离区中的最小可用空间大小（默认值为 50 MB）的功能。如果可用空间大小下降到低于指定阈值，Kaspersky Industrial CyberSecurity for Nodes 会记录“*已超过隔离区可用空间阈值*”事件，并根据此事件类型的通知设置发布通知。

  如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控隔离区中的可用空间的大小。

  如果选中“**限制隔离区大小为**”复选框被选中，则“**可用空间阈值**”复选框被激活。

  默认选中该复选框。

  如果隔离中的对象大小超过最大隔离容量或超过可用空间阈值，在您继续将对象放入隔离时，Kaspersky Industrial CyberSecurity for Nodes 将通知您此情况。

6. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置隔离设置

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**补充** → **存储**”并点击“**配置**”按钮。
5. 转到“**隔离区**”选项卡。
6. 指定隔离设置：

   - 限制隔离区大小为

     该复选框用于启用或禁用监控存储在隔离文件夹中的对象的总大小的功能。如果超过指定的值（默认值为 200 MB），Kaspersky Industrial CyberSecurity for Nodes 会记录“*已超过隔离区最大容量*”事件，并根据此事件类型的通知设置发布通知。

     如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控置于隔离的对象的总大小。

     如果清除该复选框，Kaspersky Industrial CyberSecurity for Nodes 不会监控置于隔离的对象的总大小。

     默认下，复选框被清除。

- 可用空间阈值

  该复选框用于启用或禁用监控隔离区中的最小可用空间大小（默认值为 50 MB）的功能。如果可用空间大小下降到低于指定阈值，Kaspersky Industrial CyberSecurity for Nodes 会记录“*已超过隔离区可用空间阈值*”事件，并根据此事件类型的通知设置发布通知。

  如果选中该复选框，Kaspersky Industrial CyberSecurity for Nodes 会监控隔离区中的可用空间的大小。

  如果选中“**限制隔离区大小为**”复选框被选中，则“**可用空间阈值**”复选框被激活。

  默认选中该复选框。

  如果隔离中的对象大小超过最大隔离容量或超过可用空间阈值，在您继续将对象放入隔离时，Kaspersky Industrial CyberSecurity for Nodes 将通知您此情况。

7. 保存更改。

制作对象的备份副本。备份

Kaspersky Industrial CyberSecurity for Nodes 将已清除或删除的对象的加密副本保存在“备份”文件夹。

如果该对象是复合对象的一部分（例如压缩文件的一部分），Kaspersky Industrial CyberSecurity for Nodes 会将此复合对象整体保存在备份中。例如，如果 Kaspersky Industrial CyberSecurity for Nodes 检测到邮件数据库中的其中一个对象感染病毒，则会备份整个邮件数据库。

Kaspersky Industrial CyberSecurity for Nodes 放入备份中的大型文件可能会降低系统速度，并减少硬盘驱动器上的可用磁盘空间。

您可以将文件从备份恢复到其原始文件夹或恢复到受保护设备上的其他文件夹。文件可以从备份区还原，例如，如果某个已感染文件包含重要信息，但 Kaspersky Industrial CyberSecurity for Nodes 无法在不破坏其完整性和丢失信息的前提下清除病毒。

从备份区还原文件可能导致受保护设备感染。

查看备份中的对象

本节提供有关如何查看备份中的文件列表的信息。

如何在 Kaspersky Security Center 管理控制台中查看备份对象

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**附加**” → “**存储**”。

3. 转到“**备份区**”文件夹。

4. 有关置于备份中的对象的信息显示在控制台的右侧窗格中。

如何在 Kaspersky Security Center Web Console 中查看备份对象

1. 打开 Web Console。

2. 在控制台树中，选择“**操作**” → “**存储**”。

3. 转到“**备份区**”文件夹。

4. 有关置于备份中的对象的信息显示在控制台的右侧窗格中。

如何在应用程序控制台中查看备份对象

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**存储**” → “**备份区**”。

2. 有关置于备份中的对象的信息显示在控制台的右侧窗格中。

若要在备份中的对象列表中查找所需对象，

排序或者过滤对象。

排序备份中的文件

默认情况下，按备份日期倒序排序备份中的文件。要查找所需文件，可以根据结果窗格中任意列的内容排序文件。

如何在 Kaspersky Security Center 管理控制台中对备份中的文件进行排序

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**附加**” → “**存储**”。

3. 转到“**备份区**”文件夹。

4. 在文件列表中，选择想要用于排序对象的列标题。

   将基于选定标准排序备份中的文件。

如何在 Kaspersky Security Center Web Console 中对备份中的文件进行排序

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**备份区**”文件夹。
4. 在文件列表中，选择想要用于排序对象的列标题。

   将基于选定标准排序备份中的文件。

如何在应用程序控制台中对备份中的文件进行排序

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**存储**” → “**备份区**”。
2. 在文件列表中，选择想要用于排序对象的列标题。

   将基于选定标准排序备份中的文件。

筛选备份中的文件

要在备份中查找文件，您可以过滤文件以使列表仅显示满足您指定的过滤条件（过滤器）的文件。

在 Kaspersky Security Center 管理控制台中过滤备份中的文件

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**补充**” → “**存储**”。
3. 转到“**备份**”文件夹。
4. 在右侧窗格中，单击“**未指定过滤器**”链接。
5. 点击”**调整过滤器**”并在”**过滤设置**”窗口中，选择要过滤的列。
6. 为选定的列指定运算符和值。
7. 将保存已创建的筛选器。
8. 要再次显示备份中的所有对象，请在”**过滤设置**”窗口中，单击“**全部清除**”。

在 Kaspersky Security Center Web Console 中过滤备份中的文件

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**备份区**”文件夹。
4. 点击过滤器图标，然后点击“**过滤器**”选项卡上的“**添加**”按钮。
5. 选择要按其过滤的属性。
6. 为选定的属性指定条件和值。
7. 单击“**应用**”。
   过滤器设置被保存。
8. 要再次显示备份中的所有对象，请在“**过滤器**”选项卡上，点击“**全部清除**”。

如何在应用程序控制台中过滤备份中的文件

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**存储**” → “**备份区**”。
2. 在文件表中，选择列标题并单击左上角的过滤器图标。
3. 配置过滤器并点击“**确定**”。
   过滤器设置被保存。

从备份还原文件

Kaspersky Industrial CyberSecurity for Nodes 以加密形式将文件存储在备份文件夹中，以保护受保护设备免受可能的有害影响。

所有文件都可以从备份还原。

在下列情况下可能需要还原对象：

- 原始受感染文件包含了重要信息，而 Kaspersky Industrial CyberSecurity for Nodes 无法保持其完整性，因而该文件中的信息变得不可用。
- 您认为文件对受保护设备无害并且要使用它。如果您不希望 Kaspersky Industrial CyberSecurity for Nodes 将该文件视为已感染，则在后续扫描期间，可以将其从“实时文件保护”任务和“按需扫描”任务的处理中排除。

从备份区还原文件可能导致受保护设备感染。

恢复文件时，您可以选择用于保存文件的位置：原始位置（默认）、受保护设备上用于存储已恢复对象的特殊文件夹、或者安装应用程序控制台的受保护设备上的自定义文件夹。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 还原文件时，会在备份区中生成文件的副本。还原之后，您可以从备份删除文件副本。

从 Kaspersky Security Center 管理控制台中的备份恢复文件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**附加**” → “**存储**”文件夹。
2. 转到“**备份区**”文件夹。
3. 执行下列操作之一：
   - 要恢复一个对象，请从对象名称的上下文菜单中选择“**恢复**”。
   - 要恢复多个对象，请使用 CTRL 或 SHIFT 键选择想要恢复的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**恢复**”。
4. 该对象将被恢复至原始文件夹。

从 Kaspersky Security Center Web Console 中的备份恢复文件

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**备份区**”文件夹。
4. 从列表中选择对象并单击“**恢复**”按钮。
5. 该对象将被恢复至原始文件夹。

从应用程序控制台中的备份恢复文件

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**存储**” → “**备份区**”。
2. 在“**备份区**”节点的结果窗格中执行以下操作之一：
   - 要还原一个对象，请从要还原的对象的上下文菜单中选择“**恢复**”。
   - 要恢复多个对象，请使用 CTRL 或 SHIFT 键选择想要恢复的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**恢复**”。
3. 在“**恢复对象**”窗口中，为每个选定对象指定将保存还原对象的文件夹。

   对象的名称显示在窗口上部的“**对象**”字段中。如果选定了多个对象，系统将显示选定对象列表中第一个对象的名称。

4. 执行下列操作之一：

   - 要将对象还原到原始位置，请选择“**恢复到源文件夹**”。
   - 要将对象恢复到在应用程序安装过程中指定为恢复对象位置的文件夹，请选择“**恢复到默认恢复文件夹**”。
   - 要将对象保存在安装了应用程序控制台的受保护设备上的其他文件夹，请选择“**恢复到本地计算机上的文件夹**”，然后选择所需文件夹或指定文件夹路径。

5. 如果您不希望于还原之后在备份文件夹中保存文件的副本，请选中“**恢复对象后从存储删除对象**”复选框（默认情况下，清除此复选框）。

6. 要为其余选定对象应用指定的还原条件，请选中“**应用到所有选定对象**”复选框。

7. 单击“**确定**”。

8. Kaspersky Industrial CyberSecurity for Nodes 将开始还原选定对象的第一个对象。

9. 如果指定位置已存在拥有该名称的对象，则系统将打开“**拥有该名称的对象已存在**”窗口。

   a. 选择以下 Kaspersky Industrial CyberSecurity for Nodes 操作之一：

      - **更换**，将现有对象替换为还原对象。
      - **重命名**，使用其他名称保存还原的对象。在输入字段中输入新还原对象的文件名和完整路径。
      - “**通过添加后缀重命名**”，通过为对象文件名添加后缀重命名还原对象。在输入字段中输入后缀。

   b. 如果选择了多个对象进行恢复，则选中“**应用到所有选定对象**”复选框以将选定操作（**更换**或**重命名**）应用于其余选定对象。如果选择了“**重命名**”，“**应用到所有选定对象**”复选框将不可用。

   c. 单击“**确定**”。

      对象将被还原。有关还原操作的信息将记录到系统审核日志中。

如果您在“**恢复对象**”窗口中未选中“**应用到所有选定对象**”，“**恢复对象**”窗口可能再次打开。使用该窗口可指定保存下个选定对象的位置。

从备份删除文件

在 Kaspersky Security Center 管理控制台中删除备份中的文件

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**附加**” → “**存储**”。

3. 转到“**备份区**”文件夹。右侧窗格显示备份中的对象列表。

4. 执行下列操作之一：

   - 要删除一个对象，请从对象的上下文菜单中选择“**删除**”。
   - 要删除多个对象，请使用 CTRL 或 SHIFT 键选择想要删除的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**删除**”。

5. 选定的对象被从备份中删除。

从 Kaspersky Security Center Web Console 中的备份中删除文件

1. 打开 Web Console。
2. 在控制台树中，选择“**操作**” → “**存储**”。
3. 转到“**备份区**”文件夹。
4. 从列表中选择对象并单击“**删除**”按钮。
5. 选定的对象被从备份中删除。

从应用程序控制台中的备份中删除文件

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**存储**” → “**备份区**”。
2. 右侧窗格显示备份中的对象列表。
3. 执行下列操作之一：

   - 要删除一个对象，请从对象的上下文菜单中选择“**删除**”。
   - 要删除多个对象，请使用 CTRL 或 SHIFT 键选择想要删除的对象，右键单击其中一个选定的对象，并在上下文菜单中选择“**删除**”。

4. 选定的对象被从备份中删除。

配置备份设置

如何在 Kaspersky Security Center 管理控制台中配置备份设置

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择“**补充 → 存储**”并点击“**设置**”。
4. 选择**备份**选项卡。
5. 指定备份设置。
   - 存储对象时间不超过
   - 限制备份区大小为
   - 将可用空间阈值限制为

     如果备份中的对象大小超过最大备份容量或超过可用空间阈值，在您继续将对象放入备份时，Kaspersky Industrial CyberSecurity for Nodes 将通知您此情况。
6. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置备份设置

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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“**补充 → 存储**”并点击“**配置**”按钮。
5. 选择**备份区**选项卡。
6. 指定备份设置。
   - 存储对象时间不超过
   - 限制备份区大小为

     如果备份中的对象大小超过最大备份容量，在您继续将对象放入备份时，Kaspersky Industrial CyberSecurity for Nodes 将通知您此情况。
7. 保存更改。

如何在应用程序控制台中配置备份设置

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**存储**” → “**备份**”。
2. 在“**备份**”节点的结果窗格中，单击“**属性**”。
3. 在“**属性：备份**”窗口中，指定备份设置：
   - 存储对象时间不超过
   - 限制备份区大小为
   - 将可用空间阈值限制为

     如果备份中的对象大小超过最大备份容量或超过可用空间阈值，在您继续将对象放入备份时，Kaspersky Industrial CyberSecurity for Nodes 将通知您此情况。
4. 保存更改。

备份统计

您可以查看有关当前备份状态的信息，即备份统计。

若要查看备份统计：

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**存储**” → “**备份区**”。
2. 在“**备份区**”节点的结果窗格中，单击“**统计信息**”。

   这将打开“**备份**”。“**统计数据**”窗户。“**备份：统计**”窗口将显示有关当前备份状态的信息（请参见下表）。

有关当前备份状态的信息

字段	描述
当前备份容量	备份文件夹中的数据总大小；应用程序以加密形式计算文件大小。
对象总数	备份中当前的对象总数。

阻止访问网络资源。被阻止的网络会话

本节介绍如何阻止远程设备和配置被阻止网络会话列表的设置。

被阻止的网络会话列表

默认情况下，如果安装了以下任何组件：网络威胁防护、反加密，则可以使用被阻止的网络会话列表。这些组件根据被阻止的网络会话列表，发现对受保护设备或网络附加存储共享文件夹中的对象进行加密、打开或执行的远程尝试。有关所有受保护设备上被阻止的网络会话的信息将发送到 Kaspersky Security Center。Kaspersky Industrial CyberSecurity for Nodes 会阻止当前会话，并且就当前会话而言，使共享文件夹或网络附加存储文件夹不可用。

在活动模式下启动至少一个以下任务（在指定条件下）时，将填充被阻止的网络会话列表：

- 对于“*网络威胁防护*”任务：检测到典型的网络攻击活动。

  > 当应用程序重启和网络威胁防护设置被更改时，Kaspersky Industrial CyberSecurity for Nodes 清空阻止列表。

- 对于“*Anti-Cryptor*”任务：检测到访问网络文件资源的设备的恶意加密。

在检测到恶意活动或加密尝试后，该任务会将攻击网络会话的相关信息发送到被阻止的网络会话列表，并且应用程序会为攻击主机的当前会话创建一个*警告*事件。该会话访问受保护共享网络文件夹的尝试都将被阻止。

如果发起攻击网络会话的主机的本地唯一标识符 (LUID) 已添加到被阻止的网络会话列表中，Kaspersky Industrial CyberSecurity for Nodes 会确定该主机的 IP 地址，并将其添加到被阻止的网络会话列表中来替换攻击主机的 LUID。

默认情况下，当被阻止的网络会话被添加到列表 30 分钟后，Kaspersky Industrial CyberSecurity for Nodes 将从列表中删除该被阻止的网络会话。当网络会话从被阻止的网络会话列表中删除后，对网络文件资源的访问权限将自动恢复。您可以指定在此之后被阻止的网络会话会被自动解除阻止的时间段。

> 请注意，当限制任何用户账户对存储管理的访问权限时，被阻止的网络会话列表仍将可用。被阻止的网络会话的设置无法更改，除非所选用户账户具有可管理 Kaspersky Industrial CyberSecurity for Nodes 的**编辑权限**。

管理被阻止的网络会话列表

要将出现任何恶意或加密活动的网络会话添加到被阻止的网络会话列表并阻止访问这些会话的网络文件资源，必须启用至少一个以下组件：

- 网络威胁防护
- 反加密

在 Kaspersky Security Center 管理控制台中启用对不受信任主机的阻止

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择“**网络活动控制 → 网络威胁防护设置**”并点击“**设置**”。

4. 在打开的窗口中，选中“**网络威胁防护**”复选框。

5. 在“**常规**”选项卡，启用“**阻止**”模式。

6. 选择“**阻止攻击设备**”复选框并指定阻止时长。

7. 保存更改。

要在策略属性中为反加密组件配置对不受信任的网络会话的阻止：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择“**实时计算机保护 → 反加密**”并点击“**设置**”。

4. 在打开的窗口中，选中“**反加密**”复选框。

5. 转到“**共享文件夹的保护**”选项卡，然后选择“**保护共享文件夹**”复选框。

6. 选择“**阻止连接时间**”并指定阻止持续时间。

7. 如有必要，请通过 IP 地址和掩码指定保护范围和排除项。

8. 保存更改。

在 Kaspersky Security Center Web Console 中启用对不受信任主机的阻止

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**网络活动控制 → 网络威胁防护**”并点击“**配置**”按钮。

5. 在打开的窗口中，选中“**启用网络威胁防护**”复选框。

6. 启用“**阻止**”模式。

7. 选择“**阻止攻击设备**”复选框并指定阻止时长。

8. 如果有必要，请按 IP 地址指定排除项。

9. 保存更改。

要为反加密组件配置不受信任的网络会话阻止：

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**实时计算机保护** → **反加密勒索**”并点击“**配置**”按钮。
5. 在打开的窗口中，选中“**启用反加密勒索**”复选框。
6. 转到“**共享文件夹的保护**”选项卡，然后选择“**启用共享文件夹对外部加密的防护**”复选框。
7. 选择“**阻止连接**”并在“**检测到共享文件夹的外部加密时**”部分指定阻止持续时间。
8. 如有必要，请通过 IP 地址和掩码指定保护范围和排除项。
9. 保存更改。

在应用程序控制台中启用对不受信任主机的阻止

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**实时计算机保护**” → “**网络威胁防护**”。
2. 在“**网络威胁防护**”节点的结果窗格中，单击“**属性**”。
   “**属性：网络威胁防护**”窗口将打开。
3. 在打开的窗口中，选中“**网络威胁防护**”复选框。
4. 在“**常规**”选项卡，启用“**阻止**”模式。
5. 选择“**阻止攻击设备**”复选框并指定阻止时长。
6. 保存更改。

要为反加密组件配置不受信任的网络会话阻止：

1. 在 Kaspersky Industrial CyberSecurity for Nodes 控制台树中，选择“**实时计算机保护**” → “**反加密勒索**”。
2. 点击“**反加密**”节点的结果窗格中的“**属性**”。
3. 在打开的窗口中，选中“**反加密**”复选框。
4. 转到“**共享文件夹的保护**”选项卡，然后选择“**保护共享文件夹**”复选框。
5. 选择“**阻止连接时间**”并指定阻止持续时间。

6. 如有必要，请通过 IP 地址和掩码指定保护范围和排除项。
7. 保存更改。

在应用程序控制台中配置被阻止的会话列表

1. 在应用程序控制台树中，展开“**存储**”节点。
2. 选择“**阻止的网络会话**”子节点。
3. 在结果窗格中，单击“**属性**”按钮。
4. 在打开的窗口中，选择“**阻止攻击设备**”复选框并指定阻止持续时间。
5. 要恢复对所有被阻止的网络会话的访问，请单击窗口上部的“**全部解除阻止**”。
   所有网络会话都将从列表删除并解除阻止。
6. 要从阻止的网络会话列表中删除网络会话，请在结果窗格的列表中选择一个或多个会话，然后单击窗口上部的“**解除阻止选定项目**”。
   将解除阻止选定的网络会话。

事件注册。Kaspersky Industrial CyberSecurity for Nodes 日志

本节提供有关使用 Kaspersky Industrial CyberSecurity for Nodes 日志的信息。

注册 Kaspersky Industrial CyberSecurity for Nodes 事件的方式

Kaspersky Industrial CyberSecurity for Nodes 的事件分为两组：

- 与应用程序组件操作、Kaspersky Industrial CyberSecurity for Nodes 任务中的对象处理相关的事件。
- 与管理 Kaspersky Industrial CyberSecurity for Nodes（例如启动应用程序、创建或删除任务，或者编辑任务设置）有关的事件。

Kaspersky Industrial CyberSecurity for Nodes 使用以下方式来记录事件：

- **应用组件运行日志**。日志包含有关应用程序组件运行期间发生的事件的信息。
- **系统审核日志**。系统审核日志包含有关与管理 Kaspersky Industrial CyberSecurity for Nodes 相关的事件的信息。也包含有关与受保护设备上的安全入侵或安全入侵尝试相关的事件的信息。
- **事件日志**。事件日志包含有关诊断 Kaspersky Industrial CyberSecurity for Nodes 运行故障所需的事件的信息。可在 Microsoft Windows 事件查看器中查看事件日志。

可通过以下链接下载的文件包含具有以下类别的 Kaspersky Industrial CyberSecurity for Nodes 事件完整列表的表格：

- Kaspersky Industrial CyberSecurity for Nodes 写入事件日志的事件。

  下载 WEL-EVENTS .ZIP
- Kaspersky Industrial CyberSecurity for Nodes 发送到管理服务器的事件。

  下载 KSC-EVENTS.ZIP

配置日志设置

您可以编辑 Kaspersky Industrial CyberSecurity for Nodes 日志的以下设置：

- 事件在任务日志和系统审核日志中存储的时间长度。
- Kaspersky Industrial CyberSecurity for Nodes 在其中存储任务日志文件和系统审核日志文件的文件夹的位置。

- *数据库已过期*、*数据库严重过期* 和 *已很长时间未执行关键区域扫描* 的事件生成阈值。
- Kaspersky Industrial CyberSecurity for Nodes 在事件查看器中将保存到任务日志、系统审核日志和 Kaspersky Industrial CyberSecurity for Nodes 事件日志中的事件。
- 用于将审核事件和任务执行事件通过 Syslog 协议发布到 syslog 服务器的设置。

如何在 Kaspersky Security Center 管理控制台中配置日志设置

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**日志和通知**”。
4. 在“**任务日志**”区域中单击“**设置**”。
   “**通知**”窗口将打开。
5. 在此窗口中，选择要配置的日志并指定单个事件的设置：
   - 事件保存的位置：本地报告或 Windows 事件日志。
   - 事件通知：通过电子邮件通知、通过使用终端服务通知和/或通过运行可执行文件通知。
   - 您是否要将事件发送到 SIEM 服务器和/或 Kaspersky Security Center。
6. 单击“**事件生成阈值设置**”配置事件生成阈值。
7. 这将打开一个窗口；在该窗口中，指定在多少天后必须注册以下事件：“*数据库已过期*”、“*数据库严重过期*”和“*已很长时间未执行关键区域扫描*”。
8. 通过点击“**SIEM 通知设置**”配置 SIEM 服务器连接。
9. 单击“**电子邮件通知设置**”配置电子邮件通知。
10. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置日志设置

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**日志和通知** → **任务日志**”并点击“**配置**”按钮。

5. 这将打开一个窗口；在这个窗口中，在“**通知**”选项卡上，选择要配置的日志并指定单个事件的设置：
   - 事件保存的位置：本地报告或 Windows 事件日志。
   - 事件通知：通过电子邮件通知、通过使用终端服务通知和/或通过运行可执行文件通知。
   - 您是否要将事件发送到 SIEM 服务器和/或 Kaspersky Security Center。
6. 在“**电子邮件通知设置**”选项卡上配置电子邮件通知。
7. 在“**SIEM 整合**”选项卡上配置 SIEM 服务器连接。
8. 保存更改。

如何在应用程序控制台中配置日志设置：

1. 在应用程序控制台树中，打开“**日志和通知**”节点的上下文菜单。
2. 选择“**属性**”。
   “**通知**”窗口将打开。
3. 在此窗口中，选择要配置的日志并指定单个事件的设置：
   - 事件保存的位置：本地报告或 Windows 事件日志。
   - 事件通知：通过电子邮件通知、通过使用终端服务通知和/或通过运行可执行文件通知。
   - 您是否要将事件发送到 SIEM 服务器和/或 Kaspersky Security Center。
4. 单击“**事件生成阈值设置**”配置事件生成阈值。
5. 这将打开一个窗口；在该窗口中，指定在多少天后必须注册以下事件：“*数据库已过期(天)*”、“*数据库严重过期(天)*”和“*已很长时间未执行关键区域扫描(天)*”。
6. 通过点击“**SIEM 通知设置**”配置 SIEM 服务器连接。
7. 单击“**电子邮件通知设置**”配置电子邮件通知。
8. 保存更改。

对日志中的事件进行排序

默认情况下，日志中的事件按时间倒序显示。

要在日志中排序事件：

1. 在应用程序控制台树中，打开“**日志和通知**”节点的上下文菜单。
2. 选择所需的日志。
3. 在结果窗格中，选择要用于排序列表中事件的列标题。

   在您下次查看日志前，将保存排序的结果。

过滤日志中的事件

您可以将日志配置为仅显示满足指定过滤条件（过滤器）的事件记录。

要在日志中过滤事件：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择要配置过滤器的日志，然后在结果窗格中单击“**过滤器**”。
   “**过滤器设置**”窗口将打开。
3. 若要添加筛选器，请执行以下步骤：
   a. 在“**字段名称**”列表中，选择要用于过滤事件的列。
   b. 在“**操作员**”列表中选择过滤条件。过滤条件因您在“**字段名称**”列表中选定的项目而有所不同。
   c. 在“**字段值**”中，选择过滤器值。
   d. 单击“**添加**”。

   已添加的过滤器将出现在“**过滤器设置**”窗口的过滤器列表中。
4. 如有必要，请执行以下操作之一：
   - 要使用逻辑运算符“AND”组合多个过滤器，请选择“**如果满足所有条件**”。
   - 要使用逻辑运算符“OR”组合多个过滤器，请选择“**如果满足任何条件**”。
5. 单击“**确定**”按钮以保存日志事件的筛选条件。

   日志的事件列表将仅显示满足筛选条件的事件。在您下次查看日志前，将保存筛选结果。

禁用筛选器：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择要删除过滤器的日志，然后单击“**删除过滤器**”。

   日志将显示所有事件。

从日志中删除事件

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 会保留 30 天的日志记录。您可以更改日志中记录的存储期间。

要删除日志中的事件：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择要从中删除事件的日志，然后在结果窗格中单击“**清除**”。
3. 确认清除操作。

   日志已清除。

导出日志中的信息

您可以将日志中的数据导出至 CSV 或 TXT 文件中。

要从日志导出事件：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。
2. 选择一个日志，然后在结果窗格中单击“**导出日志**”按钮。
   “**另存为**”窗口将打开。
3. 指定要将数据从日志导出到的文件的名称、位置和类型。
4. 单击“**保存**”。

   日志中的信息保存到指定的文件中。

系统审核日志

Kaspersky Industrial CyberSecurity for Nodes 执行与 Kaspersky Industrial CyberSecurity for Nodes 管理有关的事件的系统审核。应用程序会记录有关启动应用程序、启动和停止 Kaspersky Industrial CyberSecurity for Nodes 任务、更改任务设置、创建和删除按需扫描任务的信息。应用程序还记录有关与受保护设备上的安全入侵或安全入侵尝试相关的事件的信息。当您在应用程序控制台中选择“**系统审计**”节点时，所有这些事件的记录都会显示在结果窗格中。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 会存储系统审核日志中的记录 30 天。您可以更改日志中记录的存储期间。

您可以指定一个文件夹以供 Kaspersky Industrial CyberSecurity for Nodes 用来存储包含系统审核日志的文件，而不使用默认值。

任务日志

当您在“**日志和通知**”部分选择具有组件或任务名称的节点时，Kaspersky Industrial CyberSecurity for Nodes 组件和任务的运行信息将显示在应用程序控制台的结果窗格中。

默认情况下，Kaspersky Industrial CyberSecurity for Nodes 会在组件和任务的日志中保留 30 天的记录。对于任务，从完成的那一刻起。您可以更改任务日志和组件日志中记录的存储期间。

您可以指定 Kaspersky Industrial CyberSecurity for Nodes 存储包含任务日志和组件日志的文件所使用的文件夹，而不使用默认的文件夹。您还可以选择 Kaspersky Industrial CyberSecurity for Nodes 将在任务日志和组件日志中记录的事件。

在任务日志中查看有关 Kaspersky Industrial CyberSecurity for Nodes 任务的统计和信息

在任务日志中，可以查看自任务开始以来任务中发生的所有事件的详细信息，以及任务执行统计和任务设置。

要查看有关 Kaspersky Industrial CyberSecurity for Nodes 任务的统计和信息：

1. 在应用程序控制台树中，展开“**日志和通知**”节点。

2. 在结果窗格中选择任务，选择“**统计信息**”选项卡。

在事件查看器中查看 Kaspersky Industrial CyberSecurity for Nodes 事件日志

您可以使用 Microsoft 管理控制台的 Microsoft Windows 事件查看器管理单元来查看 Kaspersky Industrial CyberSecurity for Nodes 的事件日志。该日志包含由 Kaspersky Industrial CyberSecurity for Nodes 记录且诊断运行故障所需的事件。

可以根据以下标准选择将记录在事件日志中的事件：

- **按事件类型**。
- **按详细级别**。详细级别与日志中记录的事件重要性级别相对应（信息、重要或严重事件）。最详细的级别是“信息”级别，将记录所有事件。最不详细的级别是“关键”级别，只记录关键事件。

要查看 Kaspersky Industrial CyberSecurity for Nodes 事件日志：

1. 单击“**开始**”按钮，在搜索栏中输入 `mmc` 命令，然后按 ENTER 键。
   Microsoft 管理控制台打开。

2. 选择“**文件** > **添加或删除管理单元**”。
   将打开“**添加或删除管理单元**”窗口。

3. 在可用管理单元列表中，选择“**事件查看器**”管理单元并单击“**添加**”按钮。

   将打开“**选择计算机**”窗口。

4. 在“**选择计算机**”窗口中，指定已安装 Kaspersky Industrial CyberSecurity for Nodes 的受保护设备，然后单击“**确定**”。

5. 在“**添加和删除管理单元**”窗口中，单击“**确定**”。

   在 Microsoft 管理控制台树中，将出现“**事件查看器**”节点。

6. 展开“**事件查看器**”节点，并选择“**应用程序和服务日志** > **Kaspersky Industrial CyberSecurity for Nodes**”子节点。

   将打开 Kaspersky Industrial CyberSecurity for Nodes 事件日志。

管理员和用户通知方式

您可以将应用程序配置为将 Kaspersky Industrial CyberSecurity for Nodes 运行中的以下事件和设备的反病毒保护状态通知给管理员和访问设备的用户。

- 管理员可以收到有关选定类型事件的信息。
- 访问设备的 LAN 用户和终端设备用户可以收到有关“实时文件保护”任务中“*检测到对象*”类型的事件的信息。

可以使用多种方式激活管理员或用户通知：

- 终端服务工具。

  如果受保护设备用作终端，则可以应用此方法来通知终端受保护设备。

- 运行可执行文件。

  此方法是在发生事件时运行受保护设备本地驱动器上存储的可执行文件。

- 通过电子邮件发送。

  该方式使用电子邮件传输消息。

您可以为单个事件类型创建消息文本。它可以包括用以说明事件的消息字段。默认情况下，应用程序使用默认消息通知用户。

配置管理员和用户通知

事件通知设置使您可以选择配置和编写消息文本的方式。

如何在 Kaspersky Security Center 管理控制台中配置事件通知

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略属性窗口中，选择“**日志和通知**”。

4. 在“**任务日志**”区域中单击“**设置**”。

   “**通知**”窗口将打开。

5. 选择您要为其选择通知方式的事件，并单击“**通知设置**”。

   “**通知设置**”窗口将打开。

6. 对于电子邮件通知，请在“**电子邮件**”选项卡上，添加事件通知消息的文本。

   若要添加有关事件信息的字段，请单击“**变量**”按钮，然后从下拉列表中选择相关字段。事件信息字段在本部分中的表中有所说明。

   若要还原默认事件消息文本，请单击“**默认**”按钮。

7. 对于运行可执行文件的通知，请在“**可执行文件**”选项卡上选择受保护设备的本地驱动器上的文件或输入文件的完整路径。事件发生时，该文件将在受保护设备上运行。输入用于执行文件的用户名和密码。

   指定可执行文件的路径时可使用系统环境变量；不允许使用用户环境变量。

8. 对于使用终端服务的通知，在“**终端服务**”选项卡上，您可以添加事件通知消息的文本。

   若要添加有关事件信息的字段，请单击“**变量**”按钮，然后从下拉列表中选择相关字段。事件信息字段在本部分中的表中有所说明。

   若要还原默认事件消息文本，请单击“**默认**”按钮。

9. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置事件通知

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**日志和通知 → 任务日志**”并点击“**配置**”按钮。

5. 这将打开一个窗口；在该窗口中，单击您想要选择通知方法的事件。

   “**通知设置**”窗口将打开。

6. 对于电子邮件通知，在“**通知用户**”部分，选择“**通过发送电子邮件**”复选框并添加事件通知消息的文本。

   若要添加有关事件信息的字段，请单击“**添加变量**”按钮，然后从列表中选择相关项目。事件信息字段在本部分中的表中有所说明。

   若要还原默认事件消息文本，请单击“**重置**”按钮。

7. 对于通过运行可执行文件发出的通知，在“**通知管理员**”部分，选择“**通过运行可执行文件**”复选框并输入受保护设备本地磁盘上文件的完整路径。事件发生时，该文件将在受保护设备上运行。输入用于执行文件的用户名和密码。

   指定可执行文件的路径时可使用系统环境变量；不允许使用用户环境变量。

8. 对于使用终端服务的通知，在“**通知管理员**”部分，选择“**通过使用终端服务**”复选框并添加事件通知消息的文本。

   若要添加有关事件信息的字段，请单击“**添加变量**”按钮，然后从列表中选择相关项目。事件信息字段在本部分中的表中有所说明。

   若要还原默认事件消息文本，请单击“**重置**”按钮。

9. 保存更改。

如何在应用程序控制台中配置事件通知

1. 在应用程序控制台树中，打开“**日志和通知**”节点的上下文菜单。
2. 选择“**属性**”。

   “**通知**”窗口将打开。
3. 选择您要为其选择通知方式的事件，并单击“**通知设置**”。

   “**通知设置**”窗口将打开。
4. 对于电子邮件通知，请在“**电子邮件**”选项卡上，添加事件通知消息的文本。

   若要添加有关事件信息的字段，请单击“**变量**”按钮，然后从下拉列表中选择相关字段。事件信息字段在本部分中的表中有所说明。

   若要还原默认事件消息文本，请单击“**默认**”按钮。
5. 对于运行可执行文件的通知，请在“**可执行文件**”选项卡上选择受保护设备的本地驱动器上的文件或输入文件的完整路径。事件发生时，该文件将在受保护设备上运行。输入用于执行文件的用户名和密码。

   指定可执行文件的路径时可使用系统环境变量；不允许使用用户环境变量。
6. 对于使用终端服务的通知，在“**终端服务**”选项卡上，您可以添加事件通知消息的文本。

   若要添加有关事件信息的字段，请单击“**变量**”按钮，然后从下拉列表中选择相关字段。事件信息字段在本部分中的表中有所说明。

   若要还原默认事件消息文本，请单击“**默认**”按钮。
7. 保存更改。

事件信息字段

变量	描述
%EVENT_TYPE%	事件类型。
%EVENT_TIME%	事件时间。
%EVENT_SEVERITY%	重要性级别。
%OBJECT%	对象名称（在“实时计算机保护”和“按需扫描”任务中）。 “软件模块更新”任务包括更新的名称和带有更新信息的网页地址。
%VIRUS_NAME%	根据病毒百科全书分类确定的对象名称。该名称包含在 Kaspersky Industrial CyberSecurity for Nodes 检测对象时返回的检测到的对象全名中。您可以在任务日志中查看检测到的对象的全名。
%VIRUS_TYPE%	根据 Kaspersky 分类确定的检测到的对象类型，例如“病毒”或“木马”。它包含在 Kaspersky Industrial CyberSecurity for Nodes 发现被感染的对象或疑似感染的对象时返回的检测到的对象全名中。您可以在任务日志中查看检测到的对象的全名。
%USER_COMPUTER%	在“实时文件保护”任务和“RPC 网络存储保护”任务中，访问了设备上对象的用户的受保护设备的名称。
%USER_NAME%	在“实时文件保护”任务和“RPC 网络存储保护”任务中，访问了设备上的对象的用户的名称。

变量	描述
%FROM_COMPUTER%	发出通知的受保护设备的名称。
%EVENT_REASON%	发生事件的原因（某些事件没有该字段）。
%ERROR_CODE%	错误代码（仅用于“内部任务错误”事件）。
%TASK_NAME%	任务名称（仅适用于与任务性能相关的事件）。
%PROTOCOL%	正在使用的协议。
%MESSAGE%	消息的文本。
%DEVICE_INSTANCEPATH%	设备实例的路径。
%DEVICE_VID%	设备的供应商 ID。
%DEVICE_PID%	控制器的类型。
%DEVICE_SERIALNUMBER%	设备的序列号。

配置电子邮件通知

如何在 Kaspersky Security Center 管理控制台中配置电子邮件通知

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**日志和通知**”。
4. 在“**任务日志**”区域中单击“**设置**”。
   “**通知**”窗口将打开。
5. 单击“**电子邮件通知设置**”。
6. 在打开的窗口中，选中“**发送事件通知**”复选框。
7. 在“**发送通知时所使用的身份**”下，指定发件人信息：发件人地址、SMTP 服务器、SMTP 服务器端口、用户名和密码。
8. 在“**通知收件人**”下，指定收件人电子邮件地址。
9. 指定发送模式：**如果发生事件** 或者 **根据计划(计划未指定)**。要配置计划，请单击“**编辑**”。
10. 保存更改。

如何在 Kaspersky Security Center Web Console 中配置电子邮件通知

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。
4. 转到“**日志和通知** → **任务日志**”并点击“**配置**”按钮。
5. 这将打开一个窗口；在该窗口中，选择“**电子邮件通知设置**”选项卡。
6. 选择**发送事件通知**复选框。
7. 指定发件人信息：发件人地址、SMTP 服务器、SMTP 服务器端口、用户名和密码。
8. 指定收件人的电子邮件地址。
9. 指定发送模式：**如果发生事件** 或者 **根据计划**。如果适用，配置计划。
10. 保存更改。

如何在应用程序控制台中配置电子邮件通知

1. 在应用程序控制台树中，打开“**日志和通知**”节点的上下文菜单。
2. 选择“**属性**”。
   “**通知**”窗口将打开。
3. 单击“**电子邮件通知设置**”。
4. 在打开的窗口中，选中“**发送事件通知**”复选框。
5. 在“**发送通知时所使用的身份**”下，指定发件人信息：发件人地址、SMTP 服务器、SMTP 服务器端口、用户名和密码。
6. 在“**通知收件人**”下，指定收件人电子邮件地址。
7. 指定发送模式：**如果发生事件** 或者 **根据计划(计划未指定)**。要配置计划，请单击“**编辑**”。
8. 保存更改。

配置与管理服务器的交互

您必须选择 Kaspersky Industrial CyberSecurity for Nodes 将其有关信息发送到 Kaspersky Security Center 管理服务器的对象类型。

如何在 Kaspersky Security Center 管理控制台中配置与管理服务器的集成

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在“**日志和通知**”部分中，单击“**与管理服务器交互** ”子部分中的“**设置**”按钮。

4. 这将打开一个窗口；在该窗口中，选择 Kaspersky Industrial CyberSecurity for Nodes 要将其有关信息发送到 Kaspersky Security Center 管理服务器的对象类型：
   - **关于隔离区文件**
   - **关于备份区中的文件**
   - **关于未处理的文件**
   - **关于已安装的设备**
   - **关于威胁发展链**
   - **关于 PLC 项目**
5. 保存更改。

   Kaspersky Industrial CyberSecurity for Nodes 会将有关选定对象类型的信息发送到管理服务器。

如何在 Kaspersky Security Center Web Console 中配置与管理服务器的集成

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**日志和通知**”部分中，单击“**与管理服务器交互** ”子部分中的“**配置**”按钮。
5. 这将打开一个窗口；在该窗口中，选择 Kaspersky Industrial CyberSecurity for Nodes 要将其有关信息发送到 Kaspersky Security Center 管理服务器的对象类型：
   - **已隔离的文件**
   - **已备份的文件**
   - **关于未处理的文件**
   - **阻止的网络会话**
   - **设备和 Wi-Fi 网络**
   - **关于威胁发展链**
   - **PLC 项目版本**
6. 保存更改。

配置事故生成

管理服务器数据库存储有关在受管理的受保护设备上发生的应用程序事件的信息。

如何在 Kaspersky Security Center 管理控制台中配置事故生成

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”文件夹。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略属性窗口中，选择“**日志和通知**”。
4. 在“**事故**”区域中单击“**设置**”。
5. 这将打开一个窗口；在该窗口中，如有必要，编辑下表中的事件选择，Kaspersky Industrial CyberSecurity for Nodes 将使用这些事件生成事故：
6. 保存更改。
   将保存配置的事故生成设置。

如何在 Kaspersky Security Center Web Console 中配置事故生成

1. 在 Web Console 的主窗口中，选择“**资产(设备)**” → “**策略和配置文件**”。
2. 单击 Kaspersky Industrial CyberSecurity for Nodes 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**日志和通知 → 事故**”并点击“**配置**”按钮。
5. 这将打开一个窗口；在该窗口中，如有必要，编辑下表中的事件选择，Kaspersky Industrial CyberSecurity for Nodes 将使用这些事件生成事故：
6. 保存更改。
   将保存配置的事故生成设置。

事故生成的事件列表

事件	默认值
PLC 项目与参考项目不匹配	选中
将 PLC 项目与参考项目匹配时出错	选中
获取 PLC 项目信息时出错	选中
授权许可已到期	未选择
已违反最终用户授权许可协议	选中

更新失败	未选择
数据库受损	未选择
数据库严重过期	未选择
数据库已过期	未选择
网络会话被列为不信任	选中
应用程序启动被拒绝	未选择
仅统计模式：应用程序启动被拒绝	选中
处理应用程序启动时出错	未选择
检测到不受信任的外部设备并限制该设备	选中
仅统计：检测到不受信任的外部设备	选中
处理设备连接时出错	选中
检测到受感染或其他对象	选中
检测到对象(找到 KSN 不信任的对象)	选中
对象未清除	未选择
对象未备份	未选择
检测到网络攻击	未选择

联系技术支持

本节介绍了获得技术支持的方法以及需要满足的条件。

如何获取技术支持

如果您无法在文档中或其他 Kaspersky Industrial CyberSecurity for Nodes 相关信息源中找到您问题的解决方案，建议您联系技术支持。技术支持将回答您关于 Kaspersky Industrial CyberSecurity for Nodes 安装和使用的问题。

Kaspersky 在应用程序的生存周期提供对 Kaspersky Industrial CyberSecurity for Nodes 的支持（参见应用程序生存周期页）。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：

- 通过访问技术支持网站
- 通过 Kaspersky CompanyAccount 门户向卡巴斯基实验室技术支持发送请求

通过 Kaspersky CompanyAccount 获取技术支持

Kaspersky CompanyAccount 是一个为使用 Kaspersky 应用程序的公司提供的门户。Kaspersky CompanyAccount 设计用于方便用户与 Kaspersky 专家之间通过在线请求进行交互。通过使用 Kaspersky CompanyAccount 门户，您可以监视 Kaspersky 专家处理电子请求的进度并存储电子请求的历史记录。

可以在 Kaspersky CompanyAccount 上的单个用户账户中注册您组织的所有员工。通过使用单个账户，您可以集中管理注册的员工发送到 Kaspersky 的电子请求，以及通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 适用于以下语言：

- 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

您可以在技术支持网站上了解有关 Kaspersky CompanyAccount 的更多信息。

向技术支持专家提供扩展诊断信息

为了更有效地支持和解决应用程序问题，技术支持专家可能会要求您暂时更改应用程序设置，以便在诊断期间进行调试。这可能需要执行以下操作：

- 激活处理和存储扩展诊断信息的功能。
- 微调各个软件组件的设置，这些设置无法通过标准用户界面元素获得。
- 更改已处理的诊断信息的存储和传输的设置。
- 配置网络流量的拦截和记录。

执行列出的操作所需的所有信息（步骤顺序的描述、可更改的设置、配置文件、脚本、附加命令行功能、调试模块、专用实用程序等），以及为调试目的分析的数据组成，将由技术支持专家公布。高级诊断信息存储在用户的计算机中。不会自动将存储的数据传输至卡巴斯基。

向技术支持专家报告问题后，他们可能会要求您生成一个包含有关 Kaspersky Industrial CyberSecurity for Nodes 运行情况的信息的报告，然后将该报告发送到技术支持部门。卡巴斯基技术支持专家可能还会要求您创建跟踪文件和发送内存转储文件。

在分析您发送的数据后，技术支持专家可以创建一个 AVZ 脚本并将其发给您。通过使用 AVZ 脚本，可以分析活动进程以查找威胁，扫描计算机以查找威胁，清除或删除感染的文件以及创建系统扫描报告。

上述操作只能在技术支持专家的指导下按照他们的指示进行。如果以应用程序文档中或技术支持专家的建议中未描述的方式对应用程序设置进行无人协助的修改，则可能会导致操作系统速度变慢和出现故障，降低计算机保护级别，以及破坏所处理信息的可用性和完整性。

应用程序操作跟踪

*应用程序跟踪*是应用程序执行的操作以及有关应用程序运行期间发生的事件的消息的详细记录。在跟踪过程中，应用程序创建带有有关不同应用程序组件的操作的数据的一组文件。

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。

只要应用程序在使用中，就会在计算机中存储跟踪文件，当应用程序被删除后，跟踪文件将被永久删除。您也可以手动删除跟踪文件。为此，您必须禁用跟踪并停止应用程序。

已保存的跟踪文件可能包含机密数据。要控制对数据的访问，必须单独确保跟踪文件的安全。

默认情况下，除身份验证代理跟踪文件外，跟踪文件都存储在文件夹 %ProgramData%\Kaspersky Lab\KICS.4.5\Traces。

跟踪文件按如下方式命名：KICS<4.5_dateXX.XX_timeXX.XX_pidXXX.><跟踪文件类型>.log。
您可以查看跟踪文件中保存的数据。

所有跟踪文件都包含下列通用数据：

- 事件时间
- 执行线程编号

  > 身份验证代理跟踪文件不包含该信息。

- 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。

> Kaspersky Industrial CyberSecurity for Nodes 仅以加密形式将用户密码保存到跟踪文件中。

如何在 Kaspersky Security Center 管理控制台中启用和配置应用程序跟踪

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在策略属性窗口中，转到“**故障诊断**”区域。
6. 在“**故障排除设置**”块中单击“**设置**”按钮。
   将打开“**故障排除设置**”窗口的“**应用程序跟踪设置**”选项卡。
7. 选择**启用跟踪**复选框。
8. 如果必要，在“**跟踪文件文件夹**”字段中，指定 Kaspersky Industrial CyberSecurity for Nodes 将保存跟踪文件的本地文件夹的完整路径。

   > 该文件夹必须提前创建并且可由 SYSTEM 账户写入。您不能指定网络文件夹、驱动器或环境变量。

9. 在“**详细级别**”下拉列表中，选择调试信息的详细级别。
   - **关键**，意味着跟踪文件仅保存有关致命错误的消息。
   - **诊断**，意味着跟踪文件保存有关所有错误和警告的消息。

- **重要**，意味着跟踪文件保存有关所有错误、警告和附加信息的消息。
- **正常**，意味着跟踪文件保存有关所有错误、警告的消息，以及有关应用程序正常运行的信息（默认）。
- **详细**，意味着跟踪文件保存有关应用程序运行的所有信息。

技术支持代表确定解决任何潜在问题所需的详细级别。

10. 默认的详细级别设置为“**正常**”。
11. 指定**跟踪文件的最大大小 (MB)**。
    可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小为 100 MB。
12. 要在达到最大文件数时删除旧的跟踪文件，请选中“**删除旧的跟踪文件**”复选框。
13. 指定**一个跟踪日志的最大文件数**。
    可用值：1 到 999。默认情况下，最大文件数为 5。如果选中“**删除旧的跟踪文件**”复选框，则该字段可用。
14. 保存更改。
15. 重新启动 Kaspersky Industrial CyberSecurity for Nodes。

要停止跟踪应用程序：

在策略属性中，在“**故障排除设置**”窗口中，“**应用程序跟踪设置**”选项卡上，清除“**启用跟踪**”复选框。

如何在应用程序控制台中启用和配置应用程序跟踪

1. 在应用程序控制台树中，选择“Kaspersky Industrial CyberSecurity for Nodes”节点并执行以下操作之一：
   - 在节点的结果窗格中，单击“**应用程序属性**”链接。
   - 在节点的上下文菜单中选择“**应用程序属性**”。

   “**应用程序属性**”窗口将打开。
2. 选择**故障诊断**选项卡。
3. 在“**故障排除设置**”块中单击“**设置**”按钮。
   “**故障排除设置**”窗口将打开。
4. 选择“跟踪设置”选项卡：
   - “**应用程序跟踪设置**”。Kaspersky Industrial CyberSecurity for Nodes 开始跟踪应用程序。
   - “**应用程序控制台跟踪设置**”。如果应用程序控制台和 Kaspersky Industrial CyberSecurity for Nodes 安装在不同的计算机上，则只能开始跟踪应用程序控制台。

5. 选择**启用跟踪**复选框。

   “跟踪文件文件夹”字段包含 Kaspersky Embedded Systems Security 默认保存跟踪文件的本地文件夹的完整路径。您可以指定另一个路径。

6. 在**“详细级别”**下拉列表中，选择调试信息的详细级别。

   - **关键**，意味着跟踪文件仅保存有关致命错误的消息。
   - **诊断**，意味着跟踪文件保存有关所有错误和警告的消息。
   - **重要**，意味着跟踪文件保存有关所有错误、警告和附加信息的消息。
   - **正常**，意味着跟踪文件保存有关所有错误、警告的消息，以及有关应用程序正常运行的信息（默认）。
   - **详细**，意味着跟踪文件保存有关应用程序运行的所有信息。

   技术支持代表确定解决任何潜在问题所需的详细级别。

   默认的详细级别设置为**“正常”**。

7. 指定**跟踪文件的最大大小 (MB)**。

   可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小为 100 MB。

8. 要在达到最大文件数时删除旧的跟踪文件，请选中**“删除旧的跟踪文件”**复选框。

9. 指定**一个跟踪日志的最大文件数**。

   可用值：1 到 999。默认情况下，最大文件数为 5。如果选中**“删除旧的跟踪文件”**复选框，则该字段可用。

10. 保存更改。

11. 重新启动 Kaspersky Industrial CyberSecurity for Nodes。

要停止跟踪应用程序：

在应用程序属性中，**“故障排除设置”**窗口中，**“应用程序跟踪设置”**选项卡上，清除**“启用跟踪”**复选框。

如何在 Kaspersky Security Center Web Console 中启用和配置应用程序跟踪

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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**“故障诊断”**部分。

5. 在**“故障排除设置”**块中，选中**“启用应用程序跟踪”**复选框。

6. 如果必要，指定 Kaspersky Industrial CyberSecurity for Nodes 将保存跟踪文件的本地文件夹的完整路径。

   该文件夹必须提前创建并且可由 SYSTEM 账户写入。您不能指定网络文件夹、驱动器或环境变量。

7. 在“级别”下拉列表中，选择调试信息的详细级别。

8. 指定**跟踪文件的最大大小 (MB)**。

   可用值：1 到 4095 MB。默认情况下，跟踪文件的最大大小为 100 MB。

9. 要在达到最大文件数时删除旧的跟踪文件，请选中“**删除旧的跟踪文件**”复选框。

10. 指定**一个跟踪日志的最大文件数**。

    可用值：1 到 999。默认情况下，最大文件数为 5。如果选中“**删除旧的跟踪文件**”复选框，则该字段可用。

11. 保存更改。

12. 重新启动 Kaspersky Industrial CyberSecurity for Nodes。

要停止跟踪应用程序：

在您正在配置的策略的属性中，在“**故障诊断**”部分，清除“**启用应用程序跟踪**”复选框。

如何在小型诊断窗口中启用和配置应用程序跟踪

如何在命令行上启用和配置应用程序跟踪

1. 以管理员身份运行命令行解释器 (cmd.exe)。

2. 使用 cd 命令，导航到 kavshell.exe 文件所在的文件夹。

   例如：`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Industrial CyberSecurity for Nodes.4.5.0`。

3. 运行以下命令：

   `KAVSHELL TRACE /ON|/OFF /F:<存储跟踪文件的文件夹> [/LVL:debug|info|warning|error|critical] [/S:<跟踪文件的最大大小（以兆字节为单位）>] [/R:<在用新文件替换之前的最大跟踪文件数量>]`

记录内存转储

内存转储文件包含应用程序发生故障时 Kaspersky Industrial CyberSecurity for Nodes 进程的工作内存的所有信息。

只要应用程序在使用中，就会在计算机中存储内存转储文件，当应用程序被卸载后，内存转储文件将被永久删除。

已保存的转储文件可能包含机密数据。要控制对数据的访问，必须单独确保内存转储文件的安全。

默认情况下，内存转储文件存储在以下文件夹中：%ProgramData%\Kaspersky Lab\KICS.4.5\Trace。

如何在 Kaspersky Security Center 管理控制台中启用或禁用内存转储记录

1. 在 Kaspersky Security Center 管理控制台树中，展开“**受管理设备**”节点。
2. 选择要为其配置任务的管理组。
3. 选择“**策略**”选项卡。
4. 双击要配置的策略名称。
5. 在策略属性窗口中，转到“**故障诊断**”区域。
6. 在“**故障排除设置**”块中单击“**设置**”按钮。
   将打开“**故障排除设置**”窗口的“**应用程序跟踪设置**”选项卡。
7. 选择**应用程序转储设置**选项卡。
8. 选择或清除“**创建转储文件**”复选框用于在发生故障时启用或禁用内存转储。
9. 如果必要，在“**转储文件文件夹**”字段中，输入 Kaspersky Industrial CyberSecurity for Nodes 将保存内存转储文件的本地文件夹的完整路径。

   该文件夹必须提前创建并且可由 SYSTEM 账户写入。您不能指定网络文件夹、驱动器或环境变量。
10. 保存更改。

如何在应用程序控制台中启用或禁用内存转储记录

1. 在应用程序控制台树中，选择“**Kaspersky Industrial CyberSecurity for Nodes**”节点并执行以下操作之一：
   - 在节点的结果窗格中，单击“**应用程序属性**”链接。
   - 在节点的上下文菜单中选择“**应用程序属性**”。

   “**应用程序属性**”窗口将打开。
2. 选择**故障诊断**选项卡。
3. 在“**故障排除设置**”块中单击“**设置**”按钮。
   “**故障排除设置**”窗口将打开。

4. 选择“转储设置”选项卡：

   - **“应用程序转储设置”**。Kaspersky Industrial CyberSecurity for Nodes 记录应用程序的所有转储。

   - **“应用程序控制台转储设置”**。如果应用程序控制台和 Kaspersky Industrial CyberSecurity for Nodes 安装在不同的计算机上，则只能记录应用程序控制台的转储。

5. 选择或清除**“创建转储文件”**复选框用于在发生故障时启用或禁用内存转储。

   默认情况下，内存转储文件存储在以下文件夹中：%ProgramData%\Kaspersky Lab\KICS.4.5\Trace。您可以指定另一个路径。

6. 保存更改。

如何在 Kaspersky Security Center Web Console 中启用或禁用内存转储记录

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

2. 单击 Kaspersky Industrial CyberSecurity for Nodes 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**“故障诊断”**部分。

5. 在**“转储文件设置”**下，选择或清除**“创建转储文件”**复选框以在发生故障时启用或禁用内存转储。

6. 如果必要，指定 Kaspersky Industrial CyberSecurity for Nodes 将保存内存转储文件的本地文件夹的完整路径。

   该文件夹必须提前创建并且可由 SYSTEM 账户写入。您不能指定网络文件夹、驱动器或环境变量。

7. 保存更改。

您还可以在小型诊断窗口中启用或禁用内存转储记录。

有关 Kaspersky Industrial CyberSecurity for Nodes 的信息来源

您可以使用以下来源查找有关 Kaspersky Industrial CyberSecurity for Nodes 的信息：

- Kaspersky 网站上的 Kaspersky Industrial CyberSecurity for Nodes 页面
- 技术支持网站（知识库）上的 Kaspersky Embedded Systems Security 页面
- 在线帮助
- 在论坛上讨论应用程序

需要具有 Internet 连接才能使用在线信息来源。

Kaspersky 网站上的 Kaspersky Industrial CyberSecurity for Nodes 页面

在 Kaspersky Industrial CyberSecurity for Nodes 页面上，您可以查看有关该应用程序及其功能和特性的常规信息。

Kaspersky Industrial CyberSecurity for Nodes 页面包含在线商店的链接。您可以在其中购买应用程序或续订授权许可。

知识库中的 Kaspersky Industrial CyberSecurity for Nodes 页面

知识库是技术支持网站的一部分。

在知识库中的 Kaspersky Industrial CyberSecurity for Nodes 页面上，可以找到一些文章，其中提供了有用的信息和建议，并解答了如何购买、安装和使用该应用程序的常见问题。

知识库文章不仅可以解答与 Kaspersky Industrial CyberSecurity for Nodes 有关的问题，还可以解答与其他卡巴斯基应用程序有关的问题。知识库文章可能还包含技术支持新闻。

Kaspersky Industrial CyberSecurity for Nodes 在线帮助

在线帮助包含有关配置和使用 Kaspersky Industrial CyberSecurity for Nodes 的信息。

在论坛上讨论应用程序

如果您的问题不需要紧急回答，您可以在我们的论坛上与卡巴斯基专家和其他用户讨论。

在论坛中，您可以查看现有主题、发表您自己的评论以及创建新的讨论主题。

术语表

事件重要性

在卡巴斯基应用程序运行过程中遇到的事件的属性。有四个重要性级别：

- 严重事件。
- 功能故障。
- 警告。
- 信息性消息。

同一类型的事件可能有不同的重要性级别，具体取决于发生事件时的情况。

任务

卡巴斯基应用程序作为任务执行的功能，例如：实时文件保护、全盘扫描、数据库更新。

任务设置

特定于每种任务类型的应用程序设置。

保护状态

当前的保护状态，表征设备的安全级别。

卡巴斯基安全网络 (KSN)

云服务基础设施，提供对卡巴斯基有关文件、Web 资源和软件信誉的在线知识库的访问。使用卡巴斯基安全网络的数据可确保卡巴斯基应用程序对威胁做出更快响应，提高一些保护组件的性能，并降低误报可能性。

反病毒数据库

数据库包含截至反病毒数据库发布时 Kaspersky 已知的计算机安全威胁的信息。反病毒数据库特征码有助于检测扫描对象中的恶意代码。反病毒数据库由 Kaspersky 专家创建并且每小时都会更新。

受感染的对象

一个对象，其中一段代码与已知威胁的一段代码完全匹配。卡巴斯基专家不建议您处理此类对象。

可感染的文件

基于文件的结构或格式，某些文件可能会作为存储和传播恶意代码的“容器”而成为入侵者的工具。一般来说，此类文件是可执行文件，例如扩展名为 .com、.exe 和 .dll 的文件。恶意代码入侵此类文件的风险相当高。

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，可能会导致操作系统无法启动等问题。

启发式分析

用于检测其信息尚未添加到卡巴斯基数据库中的威胁的技术。启发式分析用于检测行为方式可能对操作系统构成安全威胁的对象。启发式分析检测到的对象将被视为可能已感染。例如，如果一个对象包含恶意对象通常具有的命令序列（打开文件、写入到文件），则可能会将该对象视为可能已感染。

备份

用于在清除或删除对象之前保存对象的备份副本的特殊存储。

存档

打包到单一压缩文件的一个或几个文件。需要一个名叫 archiver 的应用程序以打开和解包数据。

安全信息与事件管理（SIEM）

安全信息和事件管理的缩写。用于管理组织的安全系统中的信息和事件的解决方案。

安全级别

安全级别是一组预定义的组件设置。

实时保护

一种应用程序操作模式，在该模式下，可以实时扫描对象是否存在恶意代码。

应用程序会拦截所有打开任何对象（读取、写入或执行）的尝试，并扫描该对象是否存在威胁。未感染的对象被传递给用户；包含威胁的对象或可能被感染的对象将根据任务设置进行处理（消毒、删除或隔离）。

对象链接与嵌入（OLE）对象

附加到其他文件或通过使用对象链接与嵌入 (OLE) 技术嵌入其他文件的对象。一个 OLE 对象示例是嵌入到 Microsoft Office Word 文档中的 Microsoft Office Excel® 电子表格。

授权许可期限

您可以使用应用程序功能和附加服务的时间段。可用功能和附加服务的范围取决于授权许可类型。

文件掩码

使用通用字符表示文件名。文件掩码中使用的主要字符为 * 和 ?（其中 * 表示任意数量的任意字符，? 表示单个任意字符）。

更新

替换或添加从卡巴斯基更新服务器检索的新文件（数据库或应用程序模块）的过程。

本地任务

在单台客户端计算机上定义并运行的任务。

活动密钥

程序当前正在使用的密钥。

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。

漏洞

恶意软件制造者可能会利用操作系统或应用程序中存在的缺陷，侵入操作系统或应用程序，破坏其完整性。操作系统中存在的大量漏洞会使其变得不可靠，因为侵入操作系统的病毒可能会破坏操作系统和已安装的应用程序。

策略

策略定义应用程序设置，并管理在管理组内的计算机上配置该应用程序的能力。必须为每个应用程序创建单独策略。您可以为每个管理组内的计算机上安装的应用程序创建多个策略，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，用于集中存储有关公司网络上安装的卡巴斯基应用程序的信息，并管理这些应用程序。

误报

卡巴斯基应用程序将未感染的对象视为受感染的情况，因为该对象的代码与病毒的代码相似。

隔离

卡巴斯基应用程序将检测到的可能已感染对象移动到的文件夹。为避免对计算机造成任何影响，对象会以加密的形式存储在隔离区。

有关第三方代码的信息

有关第三方代码的信息包含在应用程序安装文件夹中的 legal_notices.txt 文件中。

商标通知

注册商标和服务标志均为其各自拥有者的财产。

Bluetooth 字样、标记和徽标归 Bluetooth SIG, Inc. 所有。

Pentium 是英特尔公司或其子公司的商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft、Active Directory、Excel、Forefront、Hyper-V、Internet Explorer、JScript、Lync、Outlook、PowerShell、SharePoint、SQL Server、Windows、Windows Server、Windows Vista、Windows XP 是 Microsoft 集团公司的商标。

Schneider Electric 是施耐德电气的商标。

Siemens、Simatic 和 WinCC 是西门子股份公司 (Siemens AG) 的注册商标。

UNIX 是在美国和其他国家/地区的注册商标，通过 X/Open Company Limited 独家授权。

附录

本节包含的信息是对文档正文的补充。

用于快速扫描的文件扩展名

com - 大小不超过 64 KB 的应用程序的可执行文件

exe - 可执行文件或自解压存档

sys - Microsoft Windows 系统文件

prg - dBase™ 程序文字、Clipper 或 Microsoft Visual FoxPro®，或 WAVmaker 程序

bin - 二进制文件

bat - 批文件

cmd - Microsoft Windows NT 的命令文件（与 DOS 批处理文件类似）、OS/2

dpl - 压缩的 Borland Delphi 库

dll - 动态链接库

scr - Microsoft Windows 屏保

cpl - Microsoft Windows 控制面板模块

ocx - Microsoft OLE（对象链接和嵌入）对象

tsp - 以分时模式运行的程序

drv - 设备驱动程序

vxd - Microsoft Windows 虚拟设备驱动程序

pif - 程序信息文件

lnk - Microsoft Windows 链接文件

reg - Microsoft Windows 系统注册表键文件

ini - 包含 Microsoft Windows、Windows NT 和某些应用程序配置数据的配置文件

cla - Java 类

vbs - Visual Basic® 脚本

vbe - BIOS 视频扩展程序

js, jse - JavaScript source text

htm - 超文本文档

htt - Microsoft Windows 超文本标头

hta - Microsoft Internet Explorer® 超文本程序

asp - Active Server Pages 脚本

chm - 编撰的 HTML 文件

pht - 带有 PHP 脚本的 HTML 文件

php - 集成到 HTML 文件的脚本

wsh - Microsoft Windows Script Host 文件

wsf - Microsoft Windows 脚本

the - Microsoft Windows 95 桌面壁纸文件

hlp - Win 帮助文件

msg - Microsoft Mail 邮件

plg - 邮件

mbx - 已保存的 Microsoft Office Outlook 邮件

doc* - Microsoft Office Word 文档，例如：doc（Microsoft Office Word 文档）、docx（带 XML 支持的 Microsoft Office Word 2007 文档）、docm（带宏支持的 Microsoft Office Word 2007 文档）

dot* - Microsoft Office Word 文档模块，例如 dot（Microsoft Office Word 文档模板）、dotx（Microsoft Office Word 2007 文档模板）、dotm（带宏支持的 Microsoft Office Word 2007 文档模板）

fpm - 数据库程序，Microsoft Visual FoxPro 启动文件

rtf - 富文本格式文档

shs - Windows Shell Scrap Object Handler 片段

dwg - AutoCAD® 图纸数据库

msi - Microsoft Windows Installer 安装包

otm - 适用于 Microsoft Office Outlook 的 VBA 项目

pdf - Adobe Acrobat 文档

swf - Shockwave® Flash 数据包文档

jpg, jpeg - 压缩图像格式

emf – 增强元文件格式文件；

ico – 对象图标文件

ov? – Microsoft Office Word 可执行文件

xl* – Microsoft Office Excel 文档和文件，例如：xla 对应 Microsoft Office Excel、xlc 对应图表、xlt 对应文档模板、xlsx 对应 Microsoft Office Excel 2007 工作簿、xltm 对应支持宏的 Microsoft Office Excel 2007 工作簿、xlsb 对应二进制格式（非 XML）的 Microsoft Office Excel 2007 工作簿、xltx 对应于 Microsoft Office Excel 2007 模板、xlsm 对应于支持宏的 Microsoft Office Excel 2007 模板、xlam 对应于支持宏的 Microsoft Office Excel 2007 插件

pp* – Microsoft Office PowerPoint® 文档和文件，例如：pps 代表 Microsoft Office PowerPoint 幻灯片、ppt 代表幻灯片、pptx 代表 Microsoft Office PowerPoint 2007 幻灯片、pptm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、potx 代表 Microsoft Office PowerPoint 2007 幻灯片模板、potm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppsx 代表 Microsoft Office PowerPoint 2007 幻灯片、ppsm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppam 代表支持宏的 Microsoft Office PowerPoint 2007 插件

md* – Microsoft Office Access® 文档和文件，例如：mda 代表 Microsoft Office Access 工作组，mdb 代表数据库

sldx – Microsoft PowerPoint 2007 幻灯片

sldm – 支持宏的 Microsoft PowerPoint 2007 幻灯片

thmx – Microsoft Office 2007 主题

应用程序组件规则中的用户账户

要配置某些应用程序组件，您需要添加特殊规则，您可以在其中选择应用程序将为其应用规则的用户。

必须添加规则来配置以下应用程序组件：

- 应用程序启动控制
- 设备控制
- 反加密
- 系统完整性监控

您可以通过以下方式添加用户：

- 从 Active Directory 中选择（推荐）
- 从 Kaspersky Security Center 用户列表中选择
- 手动添加

卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。使用本地账号的安全风险请参见微软知识库。如果使用本地用户账户，您对计算机的安全承担全部责任；特别是，这包括控制和限制对应用程序设置的访问的责任。

应用程序使用用户的 SID（安全标识符）来识别用户。当使用 Active Directory 或 Kaspersky Security Center 用户列表中的用户账户时，应用程序将确定管理服务器上的 SID。这意味着应用程序不会给计算机带来额外的负载来识别用户。如果您向应用程序规则添加了超过 1000 个本地用户账户，应用程序将联系域控制器来识别用户。这意味着计算机的负载增加了。为了优化对计算机性能的影响，我们建议使用 Active Directory 或 Kaspersky Security Center 用户列表中的用户账户。

Kaspersky Industrial CyberSecurity for Nodes 支持规则中的嵌入式用户和组账户（例如“所有人”组）。由于用户 SID 检测的特殊性，应用程序仅允许使用从 Active Directory 或 Kaspersky Security Center 用户列表添加的嵌入式账户。手动添加嵌入式账户的规则不起作用。