kaspersky

Kaspersky Industrial CyberSecurity for Networks

© 2026 AO Kaspersky Lab

目录

关于 Kaspersky Industrial CyberSecurity for Networks
- 分发包
- 硬件和软件要求
- 适用于 Kaspersky Industrial CyberSecurity for Networks 的安全建议

新增功能

Kaspersky Industrial CyberSecurity for Networks - 网络安全的功能概览
- 资产发现
- 高级资产管理
- 安全审计
- 威胁和异常检测
- 扩展威胁检测和响应
- 生态系统和集成

应用程序体系结构

常见部署方案
- 安装不带外部探测器的服务器
- 安装服务器和外部探测器
- 通过数据二极管将 Kaspersky Industrial CyberSecurity for Networks 连接到工业网络
- 从 Kaspersky SD-WAN 组件接收工业网络流量

开始：基本场景

安装和删除应用程序
- 用于组件安装和操作的端口
- 集中安装和卸载应用程序组件
  - 应用程序组件的集中安装要求
  - 准备集中安装组件
  - 集中安装应用程序组件
  - 在非交互模式下集中安装应用程序组件
  - 集中安装菜单命令
  - 应用程序组件的重新配置和集中重新安装
  - 集中删除应用程序组件
- 本地安装和卸载应用程序组件
  - 应用程序组件的本地安装要求
  - 准备本地安装服务器或探测器
  - 使用脚本进行应用程序组件的本地安装
  - 使用脚本本地删除应用程序组件
- 加强已安装应用程序组件的计算机的安全性
- 在服务器和 Sensor 节点上配置防火墙
- 为 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Networks 管理插件
- 服务器安装后应用程序的启动配置
- Kaspersky Industrial CyberSecurity for Networks 中使用的证书
  - 更新 Kaspersky Industrial CyberSecurity for Networks 服务器的主证书
  - 更新用于通过 Web 界面连接到服务器的证书
  - 通过 Kaspersky Industrial CyberSecurity for Networks API 更新用于连接服务器的证书

更新用于连接连接器的证书
更新用于与端点代理软件组件连接的证书
使用数据迁移脚本更新
安装带有补丁的更新的应用程序版本
启动和停止应用程序
通过 Web 界面连接服务器
通过 Web 界面终止服务器连接会话
通过 Web 界面连接到传感器
应用程序界面
关于 Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面
关于 Kaspersky Industrial CyberSecurity for Networks Sensor Web 界面
应用程序启动配置期间的服务器 Web 界面菜单
应用程序正常操作期间的服务器 Web 界面菜单
“初始配置”部分
“控制板”部分
“资产”部分
“网络地图”部分
“事件”部分
“报告”部分
“过程控制”部分
“允许规则”部分
“检测规则”部分
“风险”部分
“安全审计”部分
“设置”区域
许可应用程序
关于最终用户授权许可协议
关于隐私政策
关于授权许可
关于授权授权许可书
关于授权许可密钥
关于授权许可密钥文件
通过 Web 界面连接到服务器时添加授权许可密钥
查看有关添加的授权许可密钥的信息
删除授权许可密钥
数据提供
用于存储应用程序数据的文件夹
关于日志
Kaspersky Industrial CyberSecurity for Networks 的管理
部署节点
添加和删除传感器
使用传感器 Web 界面添加和连接传感器
使用通信数据包添加和连接探测器
通过网络自动添加和连接探测器
为传感器创建新的通信数据包
删除传感器

- 更改主节点设置
  - 更改节点上的应用程序数据存储设置
  - 重命名已安装应用程序组件的节点
  - 连接和配置流量转储文件的外部存储
- 管理节点上的监控点
  - 添加监控点
  - 启用监控点
  - 禁用监控点
  - 重命名监控点
  - 正在删除监控点
  - 识别与网络接口关联的以太网端口
- 管理技术
  - 启用和禁用技术
  - 配置技术操作模式
  - 管理技术继承
- 下载节点监控点收到的流量

监控 Kaspersky Industrial CyberSecurity for Networks 的状态

- 当通过 Web 界面连接时监控应用程序状态
- 查看应用程序消息
- 查看用户活动审计条目
- 查看已安装应用程序组件的节点以及节点上的网络接口的信息
  - 详细信息中显示的节点信息
  - 详细信息中显示的网络接口信息
- 查看支持应用程序组件运行的服务状态
- 重新启动安装了应用程序组件的计算机
- 使用测试网络数据包验证事件注册
- 正在检查应用程序模块的完整性
- 将 Kaspersky Industrial CyberSecurity for Networks 节点的时间与工业网络设备使用的时间源同步

更新数据库和应用程序模块

- 手动启动更新
- 配置自动更新
- 查看有关更新安装的信息
- 安装 OpenSSL 库更新后重新启动节点上的服务

分配对应用程序功能的访问权限

- 关于应用程序用户账户
- 通过 Web 界面连接到服务器时可用的应用程序功能
- 查看有关应用程序用户账户的信息
- 创建应用程序用户账户
- 更改应用程序用户账户的角色
- 管理员发起的密码更改
- 管理用户锁定
- 删除应用程序用户账户

配置资产管理

- 资产管理方法与模式
- 选择漏洞数据的来源

手动添加设备
使用设备表时添加设备
使用拓扑图时添加设备
根据网络交互图上的未知设备节点添加设备
根据拓扑图上非管理交换机添加设备
正在合并设备
使用设备表时合并设备
使用网络交互图和拓扑图时合并设备
正在删除设备
使用设备表时删除设备
使用网络交互图和拓扑图时移除设备
手动更改设备状态
使用设备表时更改设备状态
使用网络交互图和拓扑图时更改设备状态
关于将设备分组
根据特定标准自动分组设备
根据特定标准自动对设备进行分组，从组树中层次结构的顶层开始
自动将设备分组到选定的设备组中：
手动将设备分组
将一台设备添加到组
将多个设备添加到组
从组中删除一台设备
从组中删除多个设备
将节点和组移动到网络交互图上的其他组
手动创建设备组树
添加组
重命名组
删除组
移动组
搜索组
更新树
添加和删除设备标签
为单个设备添加标签
为多个设备添加标签
删除一台设备上的标签
清除多个设备的标签列表
编辑设备信息
添加、编辑和删除设备的自定义字段
删除设备用户
删除设备可执行文件
配置地址空间
关于地址空间规则
关于地址空间子网
添加地址空间

- 生成用于资产管理的子网列表
  - 添加子网
  - 编辑子网设置
  - 删除子网
- 查看所选子网中具有 IP 地址的设备的信息
- 更改地址空间
- 删除地址空间

配置过程控制
- 支持的设备和协议
- 过程控制设备
  - 设备的过程控制设置
  - 关于自动检测设备的进程控制设置
  - 手动添加设备的过程控制设置
  - 编辑设备的过程控制设置
  - 选择受监控的系统命令
  - 正在清除为设备定义的进程控制设置
  - 正在从外部项目导入设备和标记配置
  - 支持导入的项目类型
- 标记
  - 关于未知标记检测
  - 手动添加标记
  - 编辑标记参数
  - 将标记添加到收藏夹列表
  - 正在删除标记
- 过程控制规则
  - 具有标记值定义条件的规则
  - 使用 Lua 脚本的规则
  - 过程控制规则学习模式
  - 查看过程控制规则表
  - 创建具有条件设置的过程控制规则
  - 创建使用 Lua 脚本的过程控制规则
  - 编辑过程控制规则设置
  - 创建、查看和编辑全局 Lua 脚本
  - 删除过程控制规则

配置交互控制
- 交互控制技术的学习模式
- 交互控制技术的监控模式
- 在学习模式下自动生成交互控制规则
- 从外部项目导入配置时自动生成交互控制规则
- 在允许规则表中查看交互控制规则
- 针对单个设备进行微调交互控制
- 手动创建交互控制规则
  - 使用空白设置或模板中的设置创建交互控制规则
  - 从现有规则创建交互控制规则
  - 根据为网络完整性控制或命令控制技术注册的事件创建规则
- 编辑交互控制规则设置
- 启用和禁用交互控制规则

暂停和恢复设备网络交互的监控
删除交互控制规则
配置入侵检测和网络异常检测
管理入侵检测规则集
启用和禁用入侵检测规则集
加载和替换用户定义的入侵检测规则集
删除用户定义的入侵检测规则集
使用其他入侵检测方法
管理网络异常检测规则
创建网络异常检测规则
更改网络异常检测规则
为网络异常检测规则生成 SQL 查询文本
查看网络异常检测规则表：
启用和禁用网络异常检测规则
手动启动和停止网络异常检测规则
查看有关网络异常检测规则触发器的一般信息
删除网络异常检测规则
管理网络异常检测规则字典
添加字典
查看字典表
编辑字典设置
删除字典
管理日志
管理在服务器数据库中存储日志的设置
管理在服务器数据库中保存流量的设置
管理保存流量转储文件的设置
启用和禁用用户活动审计
更改进程的日志记录级别
使用 EPP 应用程序配置操作
准备从 EPP 应用程序接收数据的场景
添加集成服务器
创建用于集成服务器客户端的通信数据包
集成服务器表
在必要模式下启用和禁用集成服务器
编辑集成服务器设置
删除集成服务器
管理 Kaspersky Industrial CyberSecurity for Networks 中的响应操作
触发事件响应动作
使用设备可执行文件时触发响应操作
触发设备响应动作
使用注册的响应操作时触发响应操作
查看响应操作表
启动进程时从标准输出和错误流下载包含数据的文件
删除响应操作
管理连接器
关于可管理和不可管理的连接器
关于将事件、应用程序消息和审核条目转发到接收系统

- 通过 Cisco 交换机连接器自动控制设备的网络访问
- 添加连接器
- 查看连接器表
- 启用和禁用连接器
- 编辑连接器设置
- 为连接器创建新的通信数据包
- 正在删除连接器
- 添加和删除连接器类型
  - 查看连接器类型表
  - 添加连接器类型
  - 删除连接器类型

管理安全审计作业

- 漏洞和合规性审计作业
  - 添加漏洞和合规性审计作业
  - 编辑漏洞和合规性审计作业
  - 查看漏洞和合规性审计作业表
  - 手动启动和停止漏洞和合规性审计作业
  - 查看有关漏洞和合规性审计作业运行的常规信息
  - 在漏洞和合规性审计作业中停止设备扫描
  - 删除漏洞和合规性审计作业
  - 管理漏洞和合规性审计作业运行的存储设置
- 配置控制作业
  - 添加配置控制作业
  - 编辑配置控制作业
  - 查看配置控制作业表
  - 手动启动和停止配置控制作业
  - 查看有关配置控制作业运行的常规信息
  - 分配黄金设备配置
  - 在配置控制作业中停止设备扫描
  - 删除配置控制作业
- 主动设备轮询作业
  - 添加主动轮询作业
  - 编辑主动轮询作业
  - 查看主动轮询作业表
  - 启动和停止主动轮询作业
  - 查看有关主动轮询作业运行的一般信息
  - 查看有关主动轮询作业执行的报告
  - 删除主动轮询作业

形成拓扑图

- 拓扑图上的节点
- 拓扑图上的链接
- 查看拓扑图上对象的详细信息
- 将节点添加到拓扑图
- 手动将链接添加到拓扑图
  - 为选定节点添加链接并配置附加拓扑设置
  - 添加所选节点的链接而不配置附加拓扑设置
- 编辑节点的拓扑设置

- 重命名不受管理的交换机的节点
- 从拓扑图中删除对象
- 更改拓扑图比例
- 拓扑图的定位
- 在拓扑图上固定和取消固定节点
- 手动更改拓扑图上节点的位置
- 自动在拓扑图上排列节点
- 过滤拓扑图上的对象
- 保存和加载拓扑图显示设置
  - 添加新视图，同时保存当前拓扑图显示设置
  - 在保存当前拓扑图显示设置的同时更新视图
  - 重命名拓扑图视图
  - 删除拓扑图视图
  - 在拓扑图上应用保存的视图设置
- 搜索拓扑图上的节点

配置事件类型
- 查看事件类型表
- 编辑系统事件类型的设置
- 配置自动保存系统事件类型的流量
- 配置通过连接器转发事件
- Kaspersky Industrial CyberSecurity for Networks 中用于替换值的常用变量

配置风险类型
- 查看风险类型表
- 更改风险类型的基本分数
- 管理存储风险的设置

管理漏洞和合规性审计作业的规则集
- 漏洞和合规性审计规则
- 查看漏洞和合规性审计规则集表
- 导入漏洞和合规性审计规则集
- 更改漏洞和合规性审计规则集
- 删除漏洞和合规性审计规则集

管理远程连接的账户凭据 Secret
- 添加 Secret
- 查看 Secret 表
- 连接到远程设备时防止 Secret 泄漏
- 更改 Secret 的设置
- 删除 Secret

管理报告和报告模板
- 复制报告模板
- 编辑报告模板
- 删除报告模板
- 删除报告
- 取消生成报告
- 管理存储报告文件的设置

管理安全策略
- 在服务器 Web 界面中导出安全策略
- 使用导出实用程序导出安全策略

- 从文件中导入安全策略
- 清除当前安全策略
- 从先前版本的应用程序转换安全策略

使用 Kaspersky Industrial CyberSecurity for Networks API

- 使用 Kaspersky Industrial CyberSecurity for Networks API 时确保交互安全
- 创建并使用 Kaspersky Industrial CyberSecurity for Networks API 的连接器
- 通过 WebSocket 协议订阅有关标记值的通知

执行常见任务

- 在线模式下的系统监控
  - 添加小组件
  - 配置小组件的显示方式
    - 移动小组件
    - 更改小组件的大小
    - 更改小组件中数据的显示设置
  - 事件小组件中的信息
  - 事件小组件中的信息
  - 决定 EPP 应用程序小部件保护中如何考虑设备的条件
  - 移除小组件
- 资产管理
  - 设备表
  - 查看设备信息
  - 自动添加和更新设备
  - 自动合并设备
  - 自动分配设备状态
  - 设备组树
  - 监控设备的网络行为
  - 正在重置设备网络行为的偏差
  - 监控 PLC 项目的读写
  - 监控 OT 设备部件
  - 监控 Windows 和 Linux 设备部件
  - 监控设备用户
  - 监控设备应用程序和补丁
  - 启动设备上的可执行文件的控制
  - 设备配置控制
  - 保存的设备配置比较
- 使用网络交互图
  - 网络交互图上的节点
  - 网络交互图上的设备组
  - 网络交互图上的链接
  - 查看对象的详细信息
  - 改变网络交互图的比例
  - 定位网络交互图
  - 固定和取消固定节点和组
  - 手动更改节点和组的位置
  - 自动排列节点和群组
  - 搜索网络地图上的节点

过滤网络交互图上的对象
节点和链接的全面过滤
使用时间尺度上的时间段进行过滤
按已注册事件进行过滤
节点过滤
按设备状态过滤节点
按设备安全状态过滤节点
按设备类别过滤节点
启用和禁用与过滤节点关联的节点的显示
过滤链接
按严重性分数过滤链接
按通信协议过滤链接
按 OSI 模型层过滤链接
重置过滤器设置
保存和加载网络交互图显示设置
添加新视图，同时保存当前网络交互图显示设置
在保存当前网络交互图显示设置的同时更新视图
重命名网络交互图视图
删除网络交互图视图
在网络交互图上应用保存的视图设置
使用网络交互图时下载流量
网络会话监控
网络会话表
查看网络会话详细信息
下载网络会话流量
监控事件和突发事件
事件的分数和严重性
事件注册技术
事件状态
已注册事件表
查看突发事件中包含的事件
查看事件详细信息
更改事件状态
查看 EDR 事件的详细信息
为事件创建允许规则
使用空白设置或模板中的设置创建允许规则
从现有规则创建允许规则
从已注册事件创建允许规则
设置标记
将事件复制到文本编辑器
下载事件流量
将活动事件数据导出到入侵指标文件中
创建用于将事件导出至网络资源的文件夹
监控风险
关于漏洞类别中的风险
实施持续风险管理流程的场景
查看风险表

查看风险详细信息
手动更改风险状态
使用设备表时查看风险详细信息
是深度包检测
监控过程参数值
标签的设置
查看标记表
连接设备时检测默认密码
获取报告
查看报告表
将报告导出到文件
基于模板的报告
查看报告模板表
查看报告模板详细信息
根据模板手动生成报告
漏洞和合规性审计作业报告
生成手动作业运行的报告
生成手动设备扫描的报告
检测加密协议中的安全问题
使用数据表时的典型操作
查看数据表
配置列的显示和顺序
基于标准时间段的过滤
根据指定时间段进行过滤
按列过滤
表搜索
重置定义的过滤器和搜索设置
表排序
选择数据表中的元素
导航到其他 Web 界面部分中的相关项目
将数据从表导出到文件
更新数据表
更改您的账户密码
通过 Kaspersky Security Center 管理应用程序
启用并配置与 Kaspersky Security Center 的交互
从 Kaspersky Security Center 向 Kaspersky Industrial CyberSecurity for Networks 添加授权许可密钥
从 Kaspersky Security Center 管理服务器接收更新
通过 Kaspersky Security Center 监控事件
Kaspersky Security Center 中针对 Kaspersky Industrial CyberSecurity for Networks 事件的事件类型
Kaspersky Security Center 事件严重性级别对应关系
监控 ICS 安全状态：Kaspersky Security Center和 SCADA
从 Kaspersky Security Center 连接到服务器计算机
从 Kaspersky Security Center Web Console 使用 Kaspersky Industrial CyberSecurity for Networks 集中监控系统
关于更新 Kaspersky Industrial CyberSecurity for Networks 管理 Web 插件
单点登录（SSO）技术使用准备场景
授予 Kaspersky Security Center 用户与其在 Kaspersky Industrial CyberSecurity for Networks 中的用户角色相对应的访问权限

用于监控系统和 Kaspersky Industrial CyberSecurity for Networks 服务器的小部件
KICS for Networks 中状态的小部件
KICS for Networks 中关键事件的小部件
KICS for Networks 中存在问题的设备的小部件
KICS for Networks 最新事件的小部件
KICS for Networks 部署图的小部件
KICS for Networks 服务器信息的小部件
在 Kaspersky Industrial CyberSecurity for Networks 服务器数据库中搜索设备和事件
配置设备搜索设置
配置事件搜索设置
查看搜索结果表
Kaspersky Industrial CyberSecurity for Networks 的映射组件。
生成主地图的站点列表
添加站点
重命名站点
删除站点
更改地图的背景图像
生成站点内的服务器列表
将服务器添加到站点
从站点中删除服务器
管理地图上对象的排列
在 Web Console 中将服务器静音
在地图上查看有关服务器的信息
疑难解答
应用程序组件无法安装在选定的节点上
检测到应用程序问题
新的应用程序消息
硬盘驱动器上没有足够的可用空间
启用监控点时出现错误
监控点无流量
未加载事件或事故的流量
ICS 上的预防性维护和调整操作
意料之外的系统重新启动
更改或添加服务器 IP 地址后，连接器和远程连接功能不可用
未收到来自 Kaspersky Security Center 管理服务器的更新
重新安装 Kaspersky Security Center 管理服务器后，网络代理无法同步
无法通过 Web 界面连接到服务器
连接到服务器时，浏览器会显示证书警告
联系技术支持
如何获得技术支持
通过 Kaspersky CompanyAccount 获得技术支持
收集获取技术支持所需的信息
有关应用程序的信息源

附录
安装和配置 CentOS Stream 9 操作系统
通过 NTP 和 PTP 协议配置时间同步
在 CentOS 中通过 NTP 协议配置时间同步
在 CentOS 中通过 PTP 协议配置时间同步
支持 IEC 60870-5-104 和 IEC 60870-5-101 标准协议中的 ASDU 类型识别
加载、处理和管理设备和标记配置，支持 IEC 61850 标准协议
将 Kaspersky Industrial CyberSecurity for Networks 事件传输到 SIEM 系统
使用 HP ArcSight 系统验证事件转发（作为示例）
转发到 SIEM 系统的消息格式
使用脚本更改 Kaspersky Industrial CyberSecurity for Networks 配置设置
将 Kaspersky Industrial CyberSecurity for Networks节点连接为 Kaspersky Security Center 中的连接网关的详细信息
用于导入通用项目的文件
包含设备描述的文件：devices.csv
连接描述文件：connections.csv
包含标记和变量描述的文件：variables.csv
包含枚举描述的文件：enums.csv
包含数据集（标记集）描述的文件：datasets.csv
包含 MMS 协议报告描述的文件：iec61850_mms_reports.csv
Kaspersky Industrial CyberSecurity for Networks 中的系统事件类型
基于深度数据包检测技术的系统事件类型
基于命令控制技术的系统事件类型
基于资产管理技术的系统事件类型
基于网络完整性控制技术的系统事件类型
基于入侵检测技术的系统事件类型
基于外部技术的系统事件类型
基于 Endpoint Protection Platform 的系统事件类型
Kaspersky Industrial CyberSecurity for Networks 中的系统命令类别
Kaspersky Industrial CyberSecurity for Networks 中使用地址空间的示例
支持的通用协议
使用配置控制任务检索设备类型配置的详细信息
运行 Windows 操作系统的设备的配置
运行 Linux 操作系统的设备的配置
归类为网络部件的设备的配置
使用主动轮询连接器接收的 PLC 和其他设备的配置
安全审计作业中用于扫描 Linux 设备的命令。
支持执行设备主动轮询的设备操作系统
检测 Kaspersky Industrial CyberSecurity for Networks 中的属性和典型设备交互
为 Kaspersky Industrial CyberSecurity for Networks 配置端口镜像
为 Cisco Access and Distribution 交换机配置端口镜像
为 Cisco Small Business™ 交换机配置端口镜像
为 Hirschmann Industrial Ethernet 交换机配置端口镜像
为 Siemens SCALANCE 交换机配置端口镜像
为 Siemens RUGGEDCOM i800, i801, i802, i803 交换机配置端口镜像
词汇表
ARP 欺骗
CVE

EPP 应用程序
ICS
IOC
IOC 文件
Kaspersky Industrial CyberSecurity for Networks 传感器
Kaspersky Industrial CyberSecurity for Networks 服务器
Kaspersky Industrial CyberSecurity 专用网络
PLC 项目
SCADA
SIEM
不受管理的交换机
不受管理的连接器
事件
事件
事件关联规则
事件类型
交互控制规则
入侵检测
入侵检测规则
单点登录 (SSO) 技术
可管理的连接器
可编程逻辑控制器 (PLC)
命令控制
地址空间 (AS)
外部
安全策略
工业网络
拓扑图
是深度包检测
智能电子设备 (IED)
标记
监控点
端点保护平台
端点保护平台 (EPP)
系统命令
网络交互图
网络地图上的链接
网络完整性控制
网络异常检测规则
网络行为偏差
节点
设备
设备漏洞
账户角色
资产管理
过程控制规则

风险
风险类型
有关第三方代码的信息
商标声明
MITRE 公司使用条款

关于 Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks 是一款旨在保护工业企业的基础设施免受信息安全威胁，并确保流程不间断的应用程序。Kaspersky Industrial CyberSecurity for Networks 分析工业网络流量，以识别过程参数值的偏差，检测网络攻击的迹象，并监控网络上的操作和当前设备状态。该应用程序是 Kaspersky Industrial CyberSecurity 解决方案的一部分。

Kaspersky Industrial CyberSecurity for Networks 可执行以下功能：

- 通过监控其工业网络设备来保护公司资产。基于从网络数据包分析和/或从执行保护工作站和服务器功能的卡巴斯基应用程序接收的数据，检测设备活动和设备信息。
- 根据设备的 MAC 地址或 IP 地址与地址空间的关联来控制设备及其之间的交互。
- 扫描工业网络设备之间的通信，以检查它们是否符合定义的交互控制规则。交互控制规则可以通过在学习模式下运行应用程序自动生成。
- 将工业网络设备之间的交互显示为网络交互映射。显示的对象根据各种属性（例如，有问题的对象）进行视觉区分。
- 将工业网络中设备之间的物理连接图显示为拓扑图。显示的对象根据各种属性（例如，根据状态）在视觉上进行区分。
- 根据流量分析和收到的设备信息检测风险。
- 使用漏洞和合规性审计、配置控制和主动轮询作业实现设备安全审计。
- 从网络数据包中提取工业控制系统（以下简称“ICS”）控制的工艺过程的参数值，并根据定义的过程控制规则检查这些值的可接受性。流程控制规则可以通过在学习模式下运行应用程序自动生成。
- 监控流量，以检测过程自动化设备发送或接收的系统命令。提供有关检测到的未经授权的系统命令或可能是工业网络安全违规迹象的情况的通知。
- 使用来自工业网络流量的数据监控可编程逻辑控制器的项目读写操作。
- 在不影响工业网络或引起潜在攻击者注意的情况下，分析工业网络流量以寻找攻击迹象。使用入侵检测规则、基于内置算法的入侵检测方法和网络异常检测规则来检测攻击迹象。
- 注册设备创建的网络会话，以便与其他设备连接。
- 注册事件并将有关事件的信息中继到接收方系统和 Kaspersky Security Center。
- 分析已注册的事件，并在检测到某些事件序列后，根据嵌入的关联规则注册事故。事故可将具有某些共同特征或与同一过程相关的事件分组。
- 将与已注册事件相关联的流量保存在数据库中。流量可以自动保存（如果为事件的流量启用了自动保存）或通过请求下载流量来保存。
- 从作为 Endpoint Protection Platform (EPP) 一部分的应用程序接收、处理和提供数据。提供在使用 EPP 应用程序的设备上触发响应操作的功能。

- 使用来自各种来源的数据监控设备上的硬件、用户、应用程序、补丁、可执行文件和其他配置类型列表。每当这些列表被修改时，Kaspersky Industrial CyberSecurity for Networks 都会记录事件。
- 提供有关设备状态和系统安全性的报告，以及安全审计的结果。
- 提供从流量转储文件存储中下载流量的功能。内部节点存储（自动创建）和外部节点存储（如果连接到节点上）都可以用于下载流量。
- 可用于与 GUI 和 API 一起工作。
- 从 Kaspersky Security Center Web Console 为 Kaspersky Industrial CyberSecurity for Networks 系统的集中监控提供数据。

分发包

Kaspersky Industrial CyberSecurity for Networks 4.5 分发包包含以下文件：

- 包含应用程序分发套件的所有文件的档案：kics4net-release_<应用程序版本>.tar.gz 该档案包含以下文件：
  - ZIP 档案，包含应用程序内置连接器类型的描述（位于“connector-types”软件包目录中）
  - 用于安装、验证和删除应用程序组件的脚本和软件包（位于“linux-centos”软件包目录中）
  - 用于安装适用于 Kaspersky Security Center 的 Kaspersky Industrial CyberSecurity for Networks 管理插件和适用于 Kaspersky Security Center Web Console 的 Kaspersky Industrial CyberSecurity for Networks 管理网络插件的软件包 (位于“sc_plugin”软件包目录中)
  - 包含描述 Kaspersky Industrial CyberSecurity for Networks API 的请求和规范的文档的档案（位于“sdk”软件包目录中）
  - 包含最终用户授权许可协议文本的文件，支持以下本地化语言：英语和俄语
  - 包含隐私策略文本的文件，支持以下本地化语言：英语和俄语
  - 包含版本信息（发行说明）的文件，支持以下本地化语言：英语和俄语
- kics4net-release_<应用程序版本>.tar.gz 档案中包含的文件副本：
  - 用于安装适用于 Kaspersky Security Center 的 Kaspersky Industrial CyberSecurity for Networks 管理插件和适用于 Kaspersky Security Center Web Console 的 Kaspersky Industrial CyberSecurity for Networks 管理网络插件的软件包
  - 包含最终用户授权许可协议文本的文件，支持以下本地化语言：英语和俄语
  - 包含隐私策略文本的文件，支持以下本地化语言：英语和俄语
  - 包含版本信息（发行说明）的文件，支持以下本地化语言：英语和俄语

Kaspersky Industrial CyberSecurity for Networks 4.5.1 分发包包含以下文件：

- 包含应用程序分发套件的所有文件的档案：kics4net-release_<应用程序版本>.tar.gz 该档案包含以下文件：
  - ZIP 档案，包含应用程序内置连接器类型的描述（位于“connector-types”软件包目录中）
  - 用于安装、验证和删除应用程序组件的脚本和软件包（位于“linux-centos”软件包目录中）
  - 用于安装适用于 Kaspersky Security Center 的 Kaspersky Industrial CyberSecurity for Networks 管理插件和适用于 Kaspersky Security Center Web Console 的 Kaspersky Industrial CyberSecurity for Networks 管理网络插件的软件包 (位于“sc_plugin”软件包目录中)
  - 包含描述 Kaspersky Industrial CyberSecurity for Networks API 的请求和规范的文档的档案（位于“sdk”软件包目录中）
  - 包含最终用户授权许可协议文本的文件，支持以下本地化语言：英语、俄语和简体中文
  - 包含隐私策略文本的文件，支持以下本地化语言：英语、俄语和简体中文
  - 包含版本信息（发行说明）的文件，支持以下本地化语言：英语、俄语和简体中文
- kics4net-release_<应用程序版本>.tar.gz 档案中包含的文件副本：
  - 用于安装适用于 Kaspersky Security Center 的 Kaspersky Industrial CyberSecurity for Networks 管理插件和适用于 Kaspersky Security Center Web Console 的 Kaspersky Industrial CyberSecurity for Networks 管理网络插件的软件包
  - 包含最终用户授权许可协议文本的文件，支持以下本地化语言：英语、俄语和简体中文
  - 包含隐私策略文本的文件，支持以下本地化语言：英语、俄语和简体中文
  - 包含版本信息（发行说明）的文件，支持以下本地化语言：英语、俄语和简体中文

硬件和软件要求

硬件要求

Kaspersky Industrial CyberSecurity for Networks 对于将在其上安装应用程序组件的计算机有以下最低硬件要求：

- 执行服务器功能的计算机：
  - CPU：Intel Core i7 或同等产品（建议使用最高单核频率配置）
  - 内存：32 GB
  - 硬盘可用空间：500 GB（建议使用 SSD）

- 执行探测器功能的计算机：
  - CPU：Intel Core i5 / i7 或同等级别（建议使用最大核心配置）
  - RAM：8 GB，使用此计算机上的监控点时需额外 4 GB（适用于任意数量的监控点）
  - 硬盘可用空间：250 GB（建议使用 SSD）

我们建议使用服务器和外部传感器进行分布式部署。配置工业网络流量以发送到传感器监控点。传感器通过流量预处理和数据存储减轻了应用程序服务器的负载。

所有工业网络流量必须在服务器和传感器之间进行负载平衡，以实现稳定的性能。建议的服务器节点的最大传入流量速率为 500 Mbit/s，探测器节点的最大传入流量速率为 250 Mbit/s。

避免向服务器或探测器节点发送重复的流量，并正确配置网络部件以传输流量的副本（有关配置某些交换机型号的端口镜像的示例，请参阅附录）。当检测到重复流量时，应用程序会自动丢弃重复的网络数据包，这会增加计算机硬件资源的负载，在某些情况下可能会减慢流量处理速度。

使用探测器时，服务器与每个探测器之间的专用 Kaspersky Industrial CyberSecurity 网络的带宽必须至少为 1 Mbit/s（不包括到达探测器监控点的流量速度）。考虑到进入监测点的流量速度，探测器和服务器之间的通道带宽必须至少增加到探测器总传入流量的 50%（对于探测器的所有监测点）。

示例：
正在使用两个探测器监测点，其中一个接收 100 Mbit/s，另一个接收 200 Mbit/s。在这种情况下，探测器和服务器之间的带宽必须至少为 151 Mbit/s (1+(200+100)/2=151)。

软件要求

Kaspersky Industrial CyberSecurity for Networks 对于将在其上安装应用程序组件的计算机有以下软件要求：

- CentOS Stream 9 操作系统。

  要安装和配置操作系统，您可以参考附录中的说明。

  安装操作系统时，建议将整个硬盘（减去启动和交换分区所需的最小空间）分配给系统（根）分区。为了提高软件的性能，您还可以将 /var/ 文件夹挂载到高速硬盘上（如果您有额外的驱动器，例如 SSD 驱动器）。如果选择这样做，必须将 /var/ 文件夹完全挂载到另一个驱动器。/var/ 文件夹内的子文件夹（例如 /var/opt/）不能挂载到不同的驱动器。

- 所有安装应用程序组件的计算机必须安装相同版本的操作系统。
- 要在 CentOS 操作系统中安装应用程序组件，必须满足以下条件（这些条件的满足由指定操作系统安装和配置说明最后阶段的操作确保）：
  - 已安装 glibc-langpack-zh 软件包（仅 Kaspersky Industrial CyberSecurity for Networks 4.5.1 需要）。
  - 安装了 Chrony 时间同步包 3.1 或更高版本。
  - SELinux 访问控制执行系统被禁用。
  - dnf-utils 包已安装。

- compat-openssl 包已安装。
- 已安装包含 LTTng 库的 lttng-ust 软件包。

- 为确保将执行服务器功能的计算机上的应用程序组件正常运行， CentOS 操作系统还必须满足以下条件（这些条件的满足由指定操作系统安装和配置说明最后阶段的操作确保）：
  - 已安装 EPEL 软件仓库以及 Python® 语言解释器软件包 python3-psycopg2、python3-cryptography 和 python3-paramiko，这些软件包是连接器和数据转换脚本运行所必需的（如果连接器将在其他计算机上运行，则还必须在这些计算机上安装软件仓库和软件包）。
  - 安装了邮件服务器（邮件传输代理 (MTA)）以便通过电子邮件连接器发送电子邮件和通过电子邮件发送报告（例如，Postfix）。
  - 安装了 Perl 解释器 5.10 或更高版本（如果正在安装 Kaspersky Security Center 网络代理）。

对于应用程序组件安装，建议使用仅安装操作系统软件的单独计算机。如果计算机上安装了第三方应用程序，Kaspersky Industrial CyberSecurity for Networks 的组件的性能可能会降低。

您可以使用以下浏览器通过 Web 界面进行连接：

- Google Chrome™ 版本 115 或更高版本。
- Mozilla™ Firefox™ 115 或更高版本。
- Microsoft® Edge® 版本 115 或更高版本。

受支持的 Kaspersky Security Center 版本

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

- Kaspersky Industrial CyberSecurity for Networks 4.5 与 Kaspersky Security Center 15.1（版本 15.1.0.20748）和 Kaspersky Security Center 16 Linux 兼容。支持的 Kaspersky Security Center 网络代理版本：16.0.0-254。
- Kaspersky Industrial CyberSecurity for Networks 4.5.1 与 Kaspersky Security Center 15.1（版本 15.1.0.22239）和 Kaspersky Security Center 16.1 Linux 兼容。支持的 Kaspersky Security Center 网络代理版本：16.1.0-6517。

与 EPP 应用程序集成

Kaspersky Industrial CyberSecurity for Networks 支持与以下应用程序集成运行，这些应用程序可执行功能保护工作站和服务器（EPP 应用程序）：

- Kaspersky Industrial CyberSecurity for Nodes 版本 4.0 和 4.5。

  安装在设备上的 Kaspersky Endpoint Agent 促进了 Kaspersky Industrial CyberSecurity for Networks 与 Kaspersky Industrial CyberSecurity for Nodes 4.0 之间的交互。支持的 Kaspersky Endpoint Agent 版本：4.0。Kaspersky Industrial CyberSecurity for Nodes 4.5 内置的软件模块促进了 Kaspersky Industrial CyberSecurity for Networks 与 Kaspersky Industrial CyberSecurity for Nodes 4.5 之间的交互。

- Kaspersky Industrial CyberSecurity for Linux Nodes 版本 1.5（Kaspersky Industrial CyberSecurity for Networks 4.5 必须已使用版本 1.5.0.2558）和版本 2.0。

  Kaspersky Industrial CyberSecurity for Linux Nodes 内置的软件模块促进了 Kaspersky Industrial CyberSecurity for Networks 与该应用程序之间的交互。

使用 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 2.0 时，可获得最大集成模式功能。根据您使用的 EPP 应用程序版本，Kaspersky Industrial CyberSecurity for Networks 的以下功能可能无法使用集成模式功能：

- 使用 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 1.5 时接收 EDR 事故的威胁发展链详细信息。
- 使用 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 1.5 时管理任何响应操作。
- 如果使用 Kaspersky Industrial CyberSecurity for Nodes，则管理响应操作**删除文件**、**终止进程**和**启动进程**。
- 在使用 Kaspersky Industrial CyberSecurity for Linux Nodes 时对设备进行补丁管理。
- 使用 Kaspersky Industrial CyberSecurity for Linux Nodes 时，通过 TCP 使用 MQTT 协议，经由数据二极管接收遥测数据。
- 如果您使用的是 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 1.5 或 Kaspersky Industrial CyberSecurity for Nodes，则可以通过数据二极管使用 UDP 协议接收遥测数据。

与 Kaspersky SD-WAN 集成

Kaspersky Industrial CyberSecurity for Networks 支持与 Kaspersky SD-WAN 2.2 或更高版本的集成。

适用于 Kaspersky Industrial CyberSecurity for Networks 的安全建议

为了确保企业安装 Kaspersky Industrial CyberSecurity for Networks 后应用程序的安全运行，建议加强安装了 Kaspersky Industrial CyberSecurity for Networks 服务器和探测器的计算机的安全性。操作系统及其保护工具必须支持确保应用程序安全运行所需的安全级别。为了维护应用程序的安全，建议定期安装 Kaspersky Industrial CyberSecurity for Networks 应用程序模块和数据库的更新以及操作系统的安全更新。

建议限制对运行应用程序的硬件的物理访问，以防止以下潜在的安全问题：

- 未经授权关闭硬件（或断开网络）
- 连接可拦截传输数据的工具
- 窃取含有数据的硬盘
- 使用其他设备破坏或替换硬盘上的数据

当部署 Kaspersky Industrial CyberSecurity for Networks 时，建议您执行以下操作：

- 限制对安装了 Kaspersky Industrial CyberSecurity for Networks 组件的计算机进行远程和本地访问。

  每次使用脚本集中安装应用程序组件（包括集中删除或加强计算机安全）后，必须出于安全目的阻止通过 SSH 协议访问计算机。您可以在操作系统控制台中使用以下命令来阻止访问：`sudo systemctl disable --now sshd`。要恢复通过 SSH 协议进行访问（如果您需要重用脚本来集中安装应用程序组件），您可以使用以下命令：`sudo systemctl enable --now sshd`。

- 定期检查并更新已安装应用程序组件的计算机操作系统中活跃用户账户的密码策略。密码策略必须符合确保操作系统所需安全级别的建议。
- 确保只有获得授权安装和配置应用程序的人员以及使用该应用程序执行标准任务的用户（操作员）才能访问应用程序界面。
- 使用硬件或安全服务来控制对运行应用程序的设备和所使用的网络设备的物理访问。
- 使用视频监控和报警系统来监控受限制的房间。

为确保本地内联网系统中的数据传输安全，建议您定期更新使用的数字证书。此外，推荐您将默认用于通过 Web 界面连接服务器以及通过 Kaspersky Industrial CyberSecurity for Networks API 进行连接的自签名证书，替换为由受信任证书颁发机构颁发的数字证书。此外，为了保持应用程序的认证状态，我们建议使用经过认证或官方批准的加密保护工具来增强对以下网络连接的保护：

- 在安装了应用程序组件（服务器和 Sensor）的机器之间
- 通过 Web 界面访问应用程序组件
- 通过第三方系统通过特殊软件模块（连接器）连接到 Kaspersky Industrial CyberSecurity for Networks
- 从专用的 Kaspersky Industrial CyberSecurity 网络到外部网络

我们建议在使用应用程序管理工具时采取以下安全控制措施：

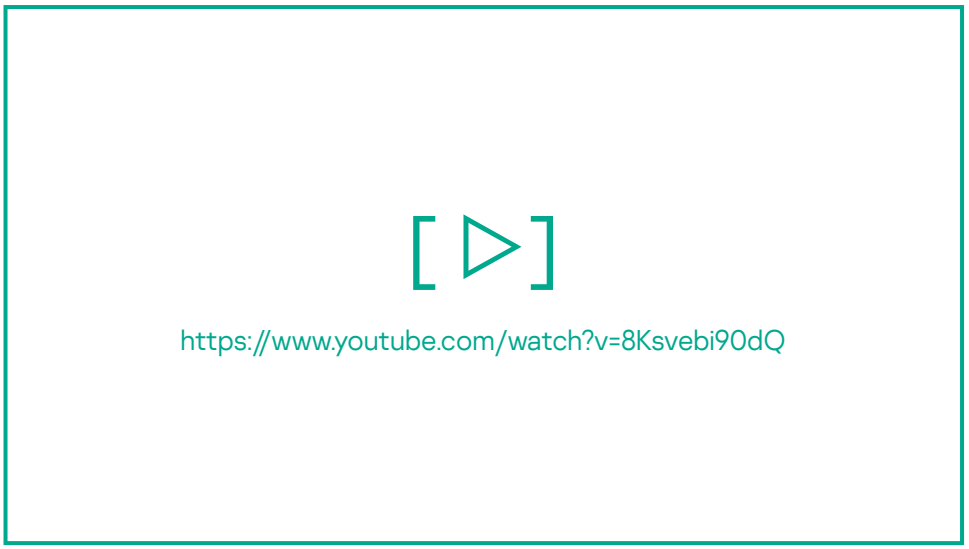
- 使用符合应用程序用户帐户的用户名和密码要求的帐户凭据。
- 确保密码保密且唯一。

  如果存在密码被泄露的风险，应用程序用户必须及时更改密码。
- Kaspersky Industrial CyberSecurity for Networks 节点上的自定义时间同步。
- 关闭浏览器之前，终止 Web 界面连接会话。

  要强制终止连接会话，请在**用户菜单登出**“注销”。

新增功能

观看视频了解 Kaspersky Industrial CyberSecurity for Networks 4.5 的新功能。



2025 年主要变化概述

Kaspersky Industrial CyberSecurity for Networks 4.5 具有以下新功能和改进：

- 新增了基于规则检测网络异常的功能：网络异常检测规则旨在分析已注册网络会话中接收的协议属性。通过使用规则检测流量异常，即使对其他流量检测系统看来流量像是设备的正常网络活动，您也能识别出边界内的复杂定向攻击。
- 在以 TCP 模式运行的 EPP 应用程序的集成服务器上，如果客户端身份验证证书已创建，则应用程序不允许您禁用对此类证书的验证。必须使用这些证书来加强客户端与集成服务器之间连接的安全性。添加集成服务器或更改其设置时，建议至少保留一个已创建的 TCP 模式证书，以便集成服务器可以检查已连接的客户端。
- 现在，当在集成模式下使用 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 2.0 时，可以接收有关 EDR 事故的威胁发展链的信息。
- 扩展了支持的响应操作列表：当在集成模式下使用 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 2.0 时，您可以启动所有支持的响应操作，包括以下新操作：**删除文件**、**终止进程**和**启动进程**。
- 增加了对 Siemens SIMATIC S7-1200 和 S7-1500 设备以及基于 CODESYS V3 平台的 PLC（例如：Prosoft-Systems Regul R500）的工业设备硬件控制的支持。
- 增加了为 Schneider Electric Modicon M340/M580 设备连接设置密码的功能，作为配置控制作业和主动轮询作业的一部分。
- 增加了对通过数据二极管从 EPP 应用程序接收遥测数据的 UDP 协议的支持：要通过此协议从 Endpoint Agent 组件接收数据，必须在集成服务器上配置并启用 UDP 模式。
- 现在，您可以使用 ERSPAN（封装远程 SPAN）技术接收镜像流量。为此，安装了应用程序组件（服务器或 Sensor）的节点必须作为通过通用路由封装（GRE）协议创建的隧道的端点。
- 新增了监控设备网络行为的功能：您可以为每台设备微调网络交互控制或重置网络行为偏差。如有必要，您可以暂时停止对单个设备的网络交互进行监控。

- 配置控制任务中可以接收、保存和比较配置的设备和数据列表得到扩展。为运行 Windows 和 Linux 操作系统的设备添加了新的配置类型（以前称为"配置组件"）。新增了 Hirschmann RS20 和 MACH 系列、Moxa EDS 系列以及 Siemens RUGGEDCOM RSG2100 系列网络设备。新增了基于 CODESYS V3 平台的 Siemens SIMATIC S7-1200 和 S7-1500 控制器和 PLC（例如：Prosoft-Systems Regul R500）。

- 应用程序用户账户的角色列表得到了扩展，包括以下角色：**安全官**、**基础设施专家**和 **ICS 专家**。

- 增加了关于数据存储空间不足的警告：如果应用程序检测到节点硬盘上的可用空间太少，则会在 Web 界面菜单顶部显示通知。

- 增强了 Kaspersky Industrial CyberSecurity for Networks 软件模块的保护，以抵御各种类型的攻击（例如本地权限提升攻击和其他攻击）。

Kaspersky Industrial CyberSecurity for Networks 版本 4.5.1 具有以下新功能和改进：

- 配置控制作业中可接收、保存和比较配置的设备列表已扩展，包含运行 MikroTik RouterOS 操作系统的网络设备以及 DES 和 DGS 系列的 D-Link® 设备。

- **控制板**部分新增了多个小部件 — 在监控系统时，您现在可以在线获取所选时间段内基于设备状态的设备分布信息以及基于检测到的协议的流量分布信息。

- 现在支持简体中文。

Kaspersky Industrial CyberSecurity for Networks - 网络安全的功能概览

Kaspersky Industrial CyberSecurity for Networks 的功能可以保护工业企业的基础设施，它是确保工业网络弹性和安全性的一套综合解决方案的一部分。您可以通过访问以下网址查看整套解决方案的描述，以及有关可用于检测和消除工业企业系统和网络各层级威胁的工具的信息。

应用程序的功能由 Kaspersky Industrial CyberSecurity for Networks 的相应部分启用。您可以根据系统的具体条件和部件级别有选择地使用该功能。但是，当您充分利用所提供的全部功能并正确配置时，您可以通过 Kaspersky Industrial CyberSecurity for Networks 获得最有效的保护。

Kaspersky Industrial CyberSecurity for Networks 的部分功能可以暂时分为几组，以确保应用程序的功能能够按预期使用。

资产发现

Kaspersky Industrial CyberSecurity for Networks 功能的以下部分提供了工业网络资产清单：

- 资产管理包括根据通过监控点接收的流量中包含的设备信息创建设备表。
- 基于流量所含数据的风险控制，包括利用设备信息检测设备漏洞。
- 使用针对应用级协议和通用协议的主动轮询方法获取有关设备及其配置的最准确、完整的信息的主动设备轮询。
- 使用显示系统状态的小工具进行在线监控。
- 网络交互图基于来自监控点的流量数据，能够查看不同时间段内设备之间的通信信息。
- 显示设备表中的设备以及通过主动轮询或手动添加的连接的拓扑图。
- 网络会话监控包括创建网络会话表。
- 保存流量转储文件，允许随后将流量下载到文件，例如网络会话流量。

您可以观看教程视频（见下方）来熟悉其功能。



https://www.youtube.com/watch?v=K012WnfC_os

资产发现

高级资产管理

高级资产管理使用 Kaspersky Industrial CyberSecurity for Networks 功能的以下部分请求和接收的数据：

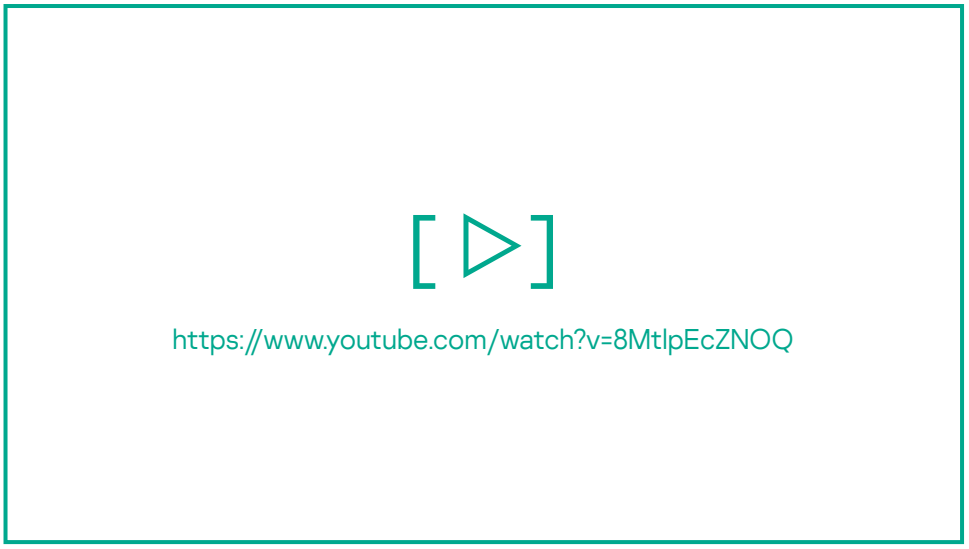
- 包括丰富设备信息和从 EPP 应用程序收到的数据添加新设备的资产管理。
- 根据收到的有关在设备操作系统中注册的账户的信息进行的设备用户控制。
- 根据收到的有关在设备操作系统中安装和注册的软件的信息进行的设备应用程序和补丁监控。
- 基于收到的有关设备上运行的可执行文件的信息进行的设备可执行文件监控。
- 与 EPP 应用程序的互操作性，用于注册工作站和服务器安全事件、显示安装了 EPP 应用程序的设备之间的通信以及接收其他网络活动数据。

安全审计

设备安全审计使用 Kaspersky Industrial CyberSecurity for Networks 功能的以下部分请求和接收的数据：

- 评估设备设置是否符合安全标准，并搜索漏洞的漏洞和合规性审计。
- 用于获取和保存有关设备配置的详细信息，并比较配置的变化的配置控制。
- 出于安全审计目的而主动进行设备轮询并检查设备是否存在风险。
- 遵循漏洞和合规性审计作业以及主动设备轮询作业进行的风险控制。

您可以观看教程视频（见下方）来熟悉其功能。



https://www.youtube.com/watch?v=8MtlpEcZNOQ

安全审计

威胁和异常检测

Threat and Anomaly Detection 由 Kaspersky Industrial CyberSecurity for Networks 功能的以下部分提供：

- 利用入侵检测规则、基于内置算法的入侵检测方法和网络异常检测规则检测入侵、攻击和各种异常情况。
- 交互控制用于检测不符合网络完整性控制规则的未经授权的网络交互。
- 深度包检测（以下也称为过程控制）用于根据过程控制规则监控流量中的过程参数，并监控正在发送的系统命令。您可以在使用命令控制的交互控制规则中指定允许发送的系统命令。
- 事件监控，基于各种技术并根据 MITRE ATT&CK 知识库中的攻击技术描述进行注册，并随后根据 Endpoint Detection and Response 关联规则记录事故。

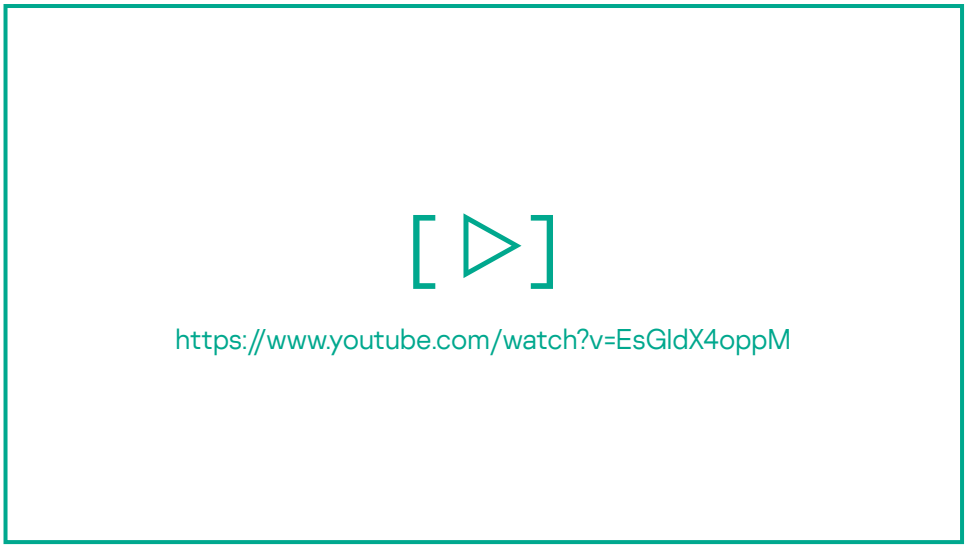
为了深入分析工业网络流量并尽早发现异常，您可以使用Kaspersky Machine Learning for Anomaly Detection 连接器。

扩展威胁检测和响应

扩展威胁检测和响应 (XDR) 由 Kaspersky Industrial CyberSecurity for Networks 功能的以下部分提供：

- 监控事件时显示 EDR 事故信息，以确定检测处理的状态并分析威胁演变。信息以活动图和表格形式显示。
- 事件丰富，包括事件注册条件发生时正在运行的应用程序的信息、启动应用程序的用户的信息以及其他信息。
- 管理安装了 Endpoint Agent 的设备上的响应操作。根据操作触发条件，您可以启用设备网络隔离、阻止文件运行、终止和启动进程以及删除或隔离文件。
- 利用网络交换机连接器自动阻止未经授权的设备访问网络。

您可以观看教程视频（见下方）来熟悉其功能。



威胁检测、分析和响应

生态系统和集成

您可以配置 Kaspersky Industrial CyberSecurity for Networks，以便与以下卡巴斯基应用程序和解决方案进行互操作：

- Kaspersky Security Center。
- Kaspersky Industrial CyberSecurity for Nodes 或 Kaspersky Industrial CyberSecurity for Linux Nodes 提供的 EPP 应用程序。
- Kaspersky SD-WAN。

此外，您还可以使用连接器和 Kaspersky Industrial CyberSecurity for Networks API 功能与包括第三方产品在内的许多其他应用程序和解决方案进行互操作。例如支持与以下软件产品的互操作：

- Kaspersky Unified Monitoring and Analysis Platform。
- Kaspersky Machine Learning for Anomaly Detection。
- Cisco™ 交换机。

如果您希望 Kaspersky Industrial CyberSecurity for Networks 与内置连接器不支持的软件产品进行互操作，您可以向应用程序添加新的连接器类型。

应用程序体系结构

Kaspersky Industrial CyberSecurity for Networks 包含以下组件：

- *服务器*是接收数据、处理数据并将其提供给应用程序用户的主要组件。接收到的信息（例如事件和设备信息）保存在服务器上的数据库中。每个 Kaspersky Industrial CyberSecurity for Networks 部署方案中只能使用一台服务器。

- *探测器*是由服务器管理的组件，它接收并分析来自连接到探测器计算机网络接口的计算机网络的数据。探测器将数据分析结果转发给服务器。根据来自服务器的具体请求，探测器可以用与接收数据相同的格式转发数据以供分析（例如，与已注册事件相关的流量）。探测器安装在不同的计算机上。探测器不能安装在执行服务器功能的计算机上。该应用程序最多可包含 50 个探测器。

服务器和探测器之间的连接通过使用证书来保护。使用证书还可以确保与应用程序组件的其他连接的安全（例如，通过 Web 界面与组件的连接或通过称为*连接器*的专门应用程序模块与接收系统的连接）。

如果受监控网络的计算机上安装了执行工作站和服务器保护功能的卡巴斯基应用程序（EPP 应用程序），则可以在 Kaspersky Industrial CyberSecurity for Networks 中配置与这些应用程序的集成。配置集成后，服务器和/或探测器从 EPP 应用程序接收数据并可以与它们交互。

当使用安全审计作业时，服务器和/或探测器可以远程连接到设备进行扫描并接收结果。

Kaspersky Industrial CyberSecurity for Networks 可执行以下功能：

- 管理探测器并从其接收对所接收数据的分析结果。

- 处理并保存收到的有关设备及其交互的信息。

- 注册并保存事件。

- 对累积信息进行额外分析以检测威胁和事件（例如，根据事件关联规则）。

- 监控应用程序性能。

- 监控应用程序用户的活动。

- 处理通过 Web 界面和连接器提交的传入请求并提供所请求的数据。

Kaspersky Industrial CyberSecurity for Networks 可执行以下功能：

- 分析传入的工业网络流量：

  - 从流量中提取有关设备通信和过程参数的信息。

  - 识别流量中的攻击迹象。

- 根据数据分析结果注册事件。

- 将事件、流量信息、设备信息和过程参数中继到 Kaspersky Industrial CyberSecurity for Networks 服务器中。

应用程序组件从*监控点*接收工业网络流量的副本。监控点既可以用于探测器上，也可以用于服务器上。您可以将监控点添加到安装了应用程序组件的节点上检测到的网络接口上。监控点必须添加到中继工业网络流量的网络接口上。

所有包含添加监控点的网络接口连接到工业网络的方式都必须排除任何对工业网络造成影响的可能性。例如，您可以使用配置为传输镜像流量（交换端口分析器，SPAN）的工业网络交换机上的端口进行连接。

Kaspersky Industrial CyberSecurity for Networks 支持接收镜像流量，包括使用封装远程 SPAN (ERSPAN) 技术。如果采用 ERSPAN 技术，则安装了应用程序组件（服务器或传感器）的节点将充当使用通用路由封装 (GRE) 协议创建的隧道的端点。欲了解更多信息，您可以联系技术支持。

应用程序对监控点数量有以下限制：

- 监测点总数：最多 50 个
- 服务器上监控点数：最多 4 个
- 每个传感器的监控点数：最多 8 个

运行与 Kaspersky SD-WAN 集成时，每个节点或所有安装了应用程序组件的节点上最多可使用 100 个监控点。

建议使用*专用的 Kaspersky Industrial CyberSecurity 网络*将服务器连接到探测器和 Kaspersky Industrial CyberSecurity 的其他组件（Kaspersky Industrial CyberSecurity for Nodes/Kaspersky Industrial CyberSecurity for Linux Nodes、Kaspersky Security Center）。专用网络中用于各组件之间交互的网络设备必须与工业网络分开安装。通常，以下计算机和设备应连接到专用网络：

- Kaspersky Industrial CyberSecurity for Networks 服务器节点。
- Kaspersky Industrial CyberSecurity for Networks 探测器节点。
- 用于通过网络界面连接服务器和探测器的计算机。
- 安装了 Kaspersky Industrial CyberSecurity for Nodes/Kaspersky Industrial CyberSecurity for Linux Nodes 和端点代理软件组件的计算机。
- 作为安全审计作业的一部分，为扫描而建立远程连接的设备。
- 托管连接器应用程序模块的计算机。
- 托管 Kaspersky Security Center 的计算机。
- 网络交换机。

常见部署方案

Kaspersky Industrial CyberSecurity for Networks 支持以下组件安装场景：

- 安装不带外部探测器的服务器
- 安装服务器和外部探测器

如有必要，可以使用数据二极管将服务器和/或探测器连接到工业网络。

无论采用哪种安装方式，都建议使用专门的专用网络来连接 Kaspersky Industrial CyberSecurity 套件组件（Kaspersky Industrial CyberSecurity for Networks、Kaspersky Industrial CyberSecurity for Nodes/Kaspersky Industrial CyberSecurity for Linux Nodes、Kaspersky Security Center）。硬件和软件要求文章中提供了安装 Kaspersky Industrial CyberSecurity for Networks 服务器和探测器的专用网络最低带宽要求。

安装不带外部探测器的服务器

当安装没有外部 Sensor 的服务器时，所有要处理和分析的数据仅由执行服务器功能的计算机接收。如果计算机具有足够数量的网络接口来接收来自各种来源的数据，则可以应用此安装方法。

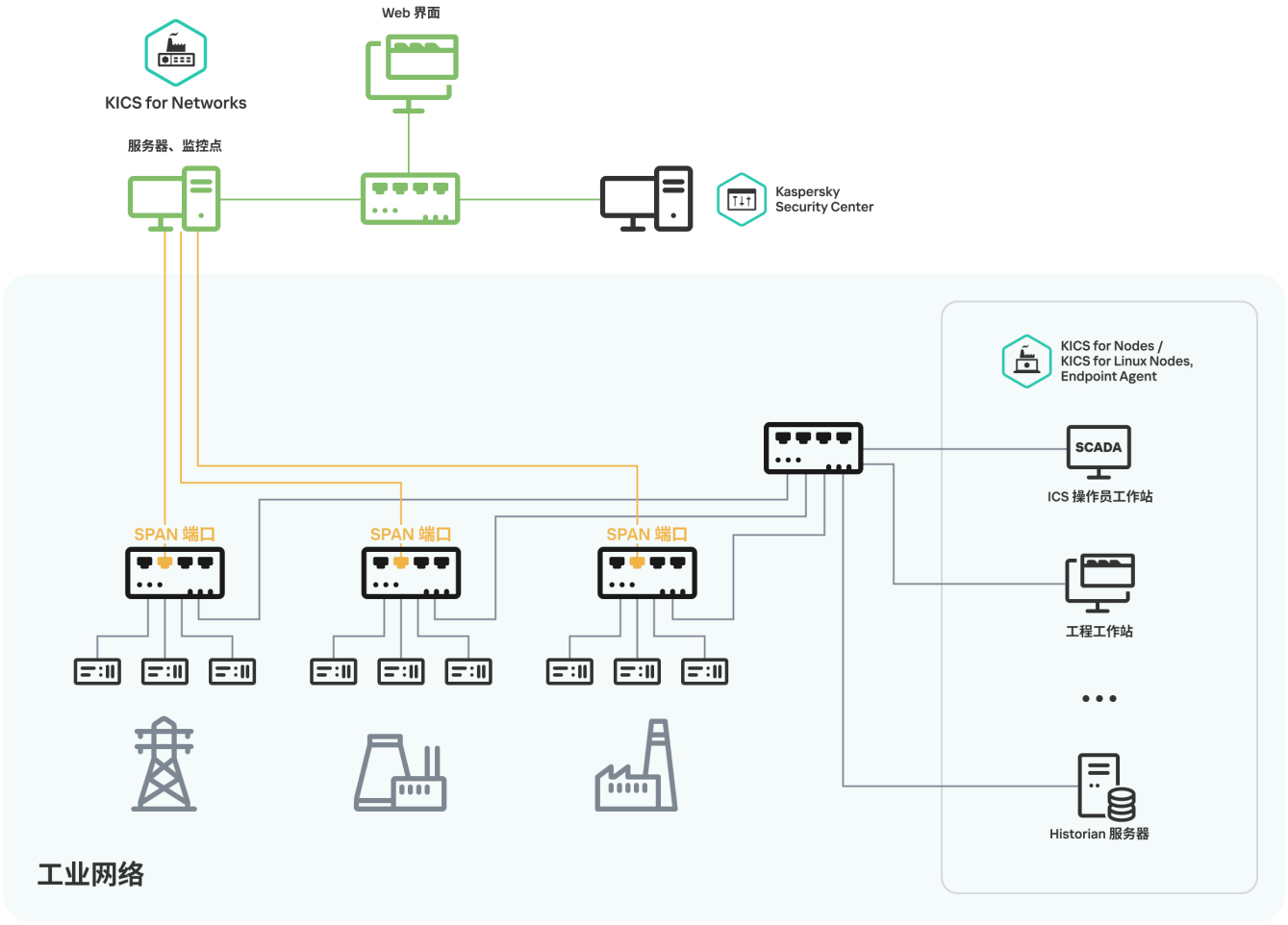
对于对具有少量流量源的单一站点的监控，建议选择不带外部探测器的服务器部署方案。在分布式网络基础架构的情况下，建议选择服务器和外部探测器部署方案。

如果在分布式网络基础架构中使用流量聚合工具（如聚合交换机或网络数据包代理）将流量传输到服务器，则可能会丢失有关信息安全事件起源的重要数据。另外，如果在不同的网段中使用相同的设备地址，如果不额外配置流量聚合工具和应用程序，这些地址就无法正确匹配到设备上。此外，应用程序中可能无法监控个别网段和设备，并且在使用某些应用程序功能（特别是审计、主动轮询和威胁响应的功能）时可能会出现错误。

计算机必须具备网络接口才能接收来自所有工业网络段的监控点的流量。由于服务器上监控点数量的限制，这些网络接口不能超过 4 个。

该计算机还必须再配有一个网络接口，以便其他计算机可以通过 Web 界面连接到服务器。此网络接口上一定不能有任何监控点。如果计算机上没有更多可用的网络接口，则同一网络接口还可以用于来自专用 Kaspersky Industrial CyberSecurity 网络的其他连接。

下图显示了部署没有探测器的服务器的示例场景。执行服务器功能的计算机的网络接口连接到网络交换机的 SPAN 端口（SPAN 端口和连接标记为黄色），并接收来自工业网络三个段的流量副本。专用的 Kaspersky Industrial CyberSecurity 网络以绿线表示。



无探测器的服务器部署示例

安装服务器和外部探测器

安装带有外部 Sensor 的服务器时，可以使用多台计算机来安装应用程序组件。服务器安装在其中一台计算机上。将从计算机网络接收数据的探测器安装在其他计算机上。该应用程序最多可包含 50 个探测器。

为了接收来自工业网络的流量，必须在计算机上添加监控点：

- 一个探测器上最多可设 8 个监控点
- 服务器上监控点不超过 4 个
- 总计，应用程序中的监控点不超过 50 个

监控点必须添加到从工业网络段接收流量的网络接口上。每个监控点每台计算机必须有一个网络接口。

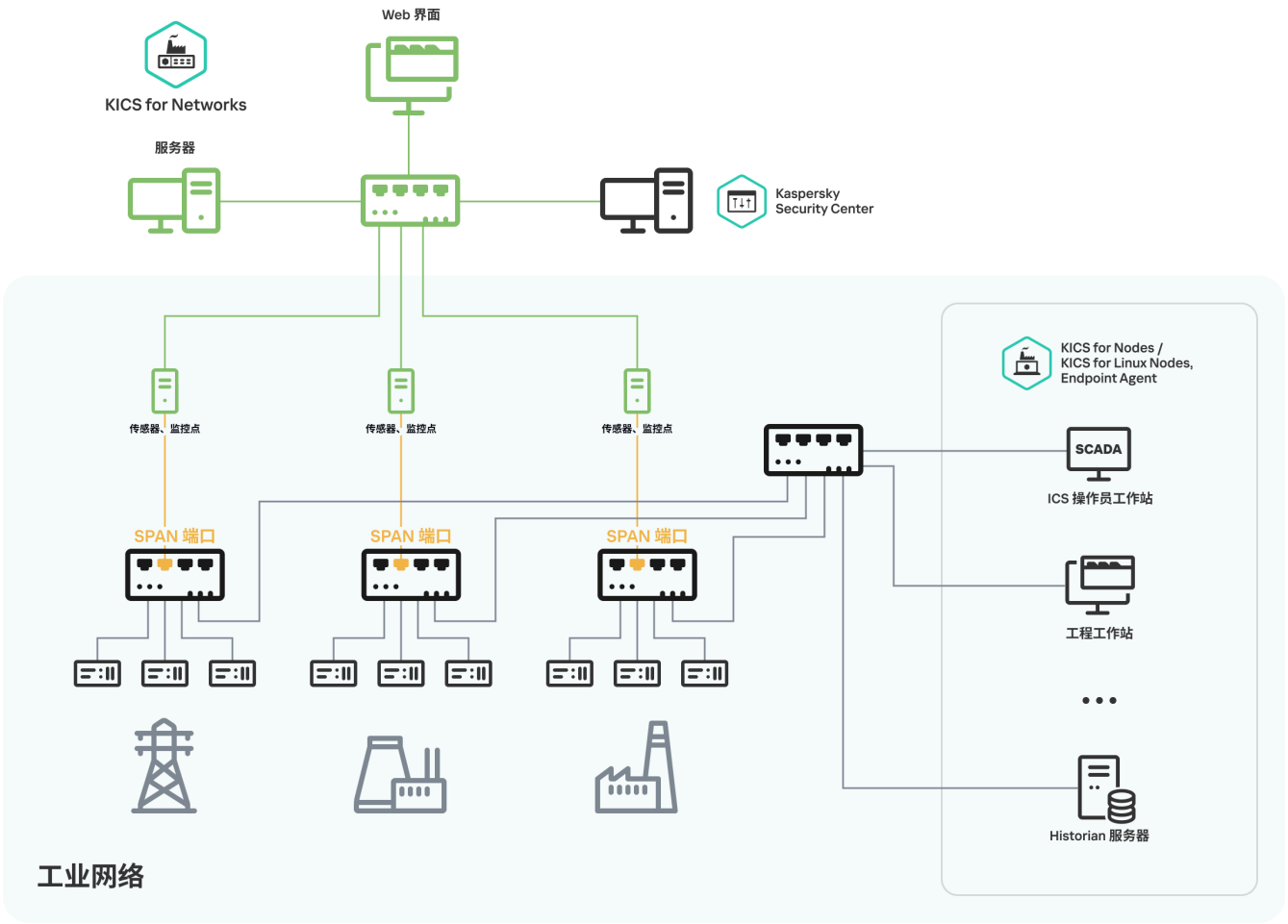
计算机还必须具有单独的网络接口，用于以下目的：

- 与服务器的连接（在执行探测器功能的计算机上）
- 通过 Web 界面与其他计算机连接
- 来自专用 Kaspersky Industrial CyberSecurity 网络的其他连接

为了这些目的，每台计算机可以使用多个单独的网络接口或一个共享的网络接口。这些网络接口上一定不能有监控点。

建议将 Kaspersky Industrial CyberSecurity for Networks 探测器安装在流量源附近和/或安装 Kaspersky Industrial CyberSecurity for Nodes 和/或 Kaspersky Industrial CyberSecurity for Linux Nodes 的同一网段中。这种方法简化了应用程序之间的集成配置，不需要额外的步骤来设置设备访问权限和配置网络部件的访问权限，并最大限度地减少各个段之间的网络连接。

下图显示了部署一台服务器和三个探测器的示例场景。执行探测器功能的计算机的网络接口连接到网络交换机的 SPAN 端口（SPAN 端口和连接标记为黄色）并从工业网络的各自段接收流量的副本。专用的 Kaspersky Industrial CyberSecurity 网络以绿线表示。



一台服务器和三个探测器的部署示例

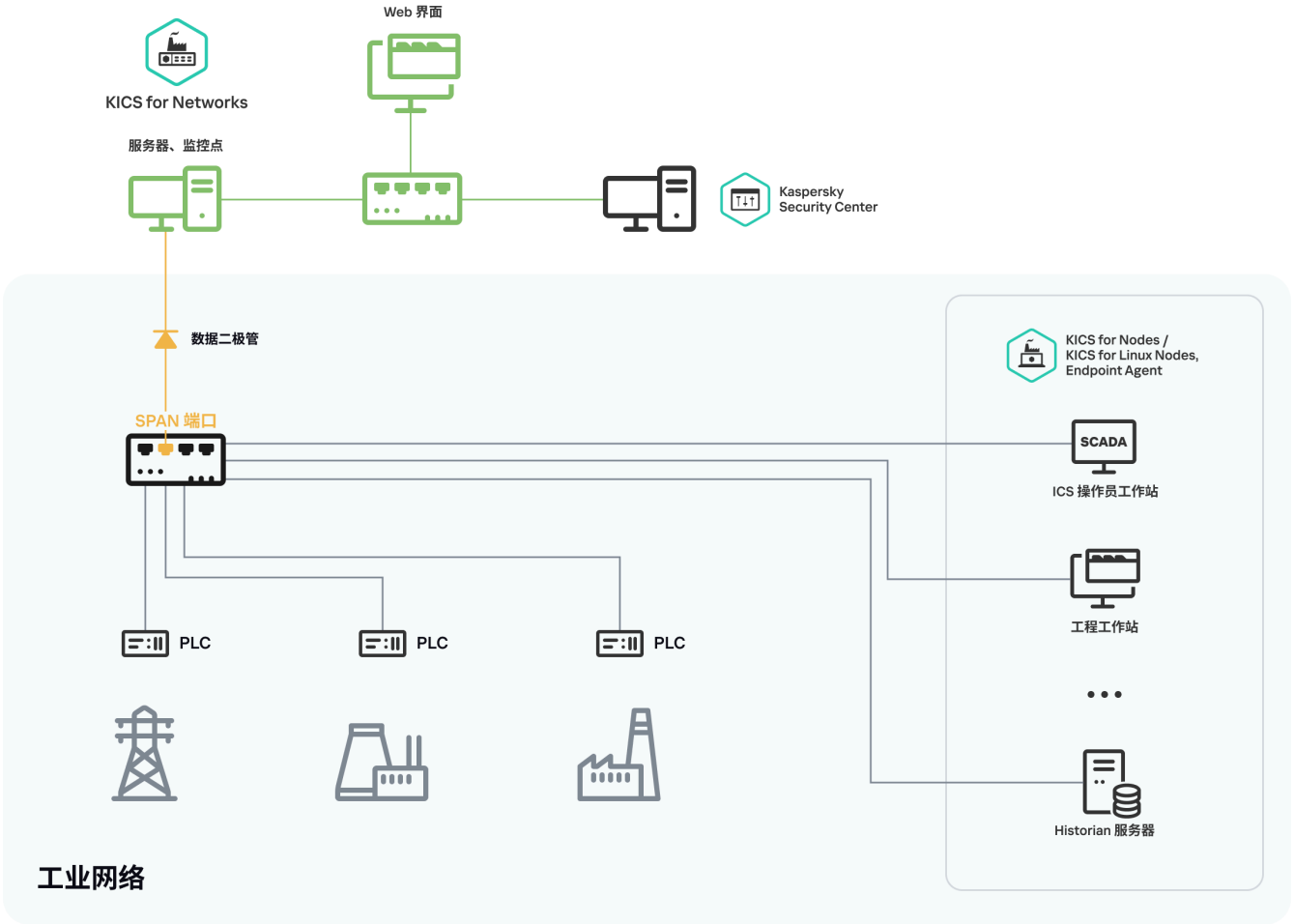
通过数据二极管将 Kaspersky Industrial CyberSecurity for Networks 连接到工业网络

要将 Kaspersky Industrial CyberSecurity for Networks 连接到工业网络，您还可以使用提供工业网络单向数据传输的特殊设备。这些设备被称为*数据二极管*。

通过数据二极管接收工业网络流量

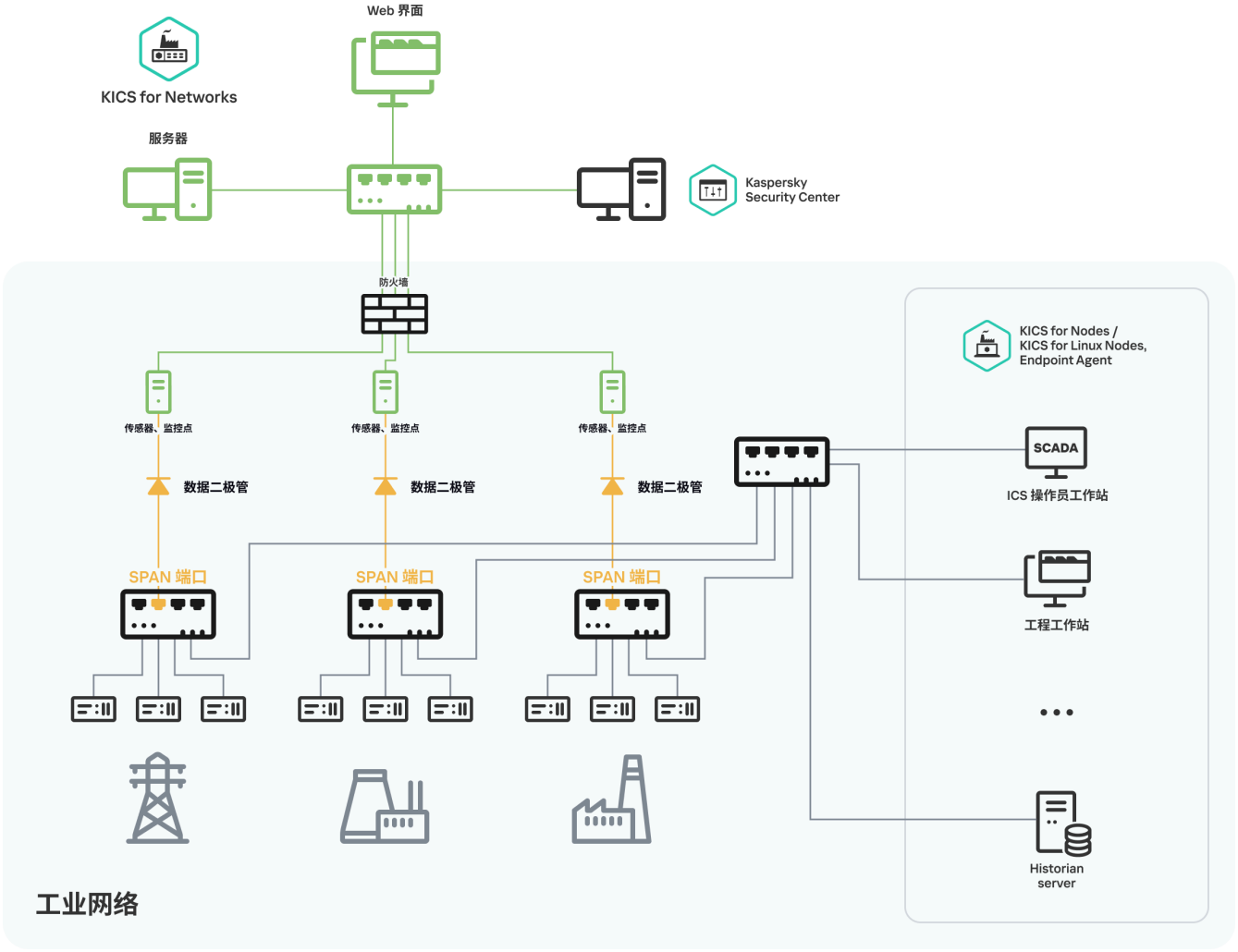
为了将工业网络流量传输到 Kaspersky Industrial CyberSecurity for Networks，数据二极管必须支持所有链路层协议（包括服务协议）的网络数据包的未过滤传输。数据二极管安装在 Kaspersky Industrial CyberSecurity for Networks 监控点的连接链接上以及网络交换机的 SPAN 端口上。

下图显示了通过数据二极管连接到服务器上的监控点的部署场景。数据二极管传输来自工业网络中的网络交换机的 SPAN 端口的流量。在这种场景中，服务器安装时无需外部探测器。



通过数据二极管连接服务器的标准场景

下图显示了多个 Kaspersky Industrial CyberSecurity for Networks 探测器通过数据二极管连接的部署场景。数据二极管传输来自工业网络中的网络交换机的 SPAN 端口的流量。在这种场景中，服务器安装了三个探测器。



通过数据二极管连接探测器的标准场景

如果您想要将安装探测器的工业网络的区段与安装服务器的专用的 Kaspersky Industrial CyberSecurity 的区段额外分开，您可以在探测器和服务器之间的连接链接上使用防火墙。

通过数据二极管接收来自 EPP 应用程序的遥测数据

与 EPP 应用程序交互的 Endpoint Agent 软件组件可以通过数据二极管发送遥测数据。Kaspersky Industrial CyberSecurity for Networks 节点必须通过未用作监控点的网络接口接收遥测数据。因此，要同时接收遥测数据和工业网络流量，您需要安装单独的数据二极管，连接到 Kaspersky Industrial CyberSecurity for Networks 节点的相应网络接口。遥测数据必须发送到普通网络接口，来自 SPAN 端口的流量必须发送到监控点的网络接口。

根据 EPP 应用程序的版本，Endpoint Agent 组件可以使用以下协议通过数据二极管发送遥测数据：

- MQTT over TCP

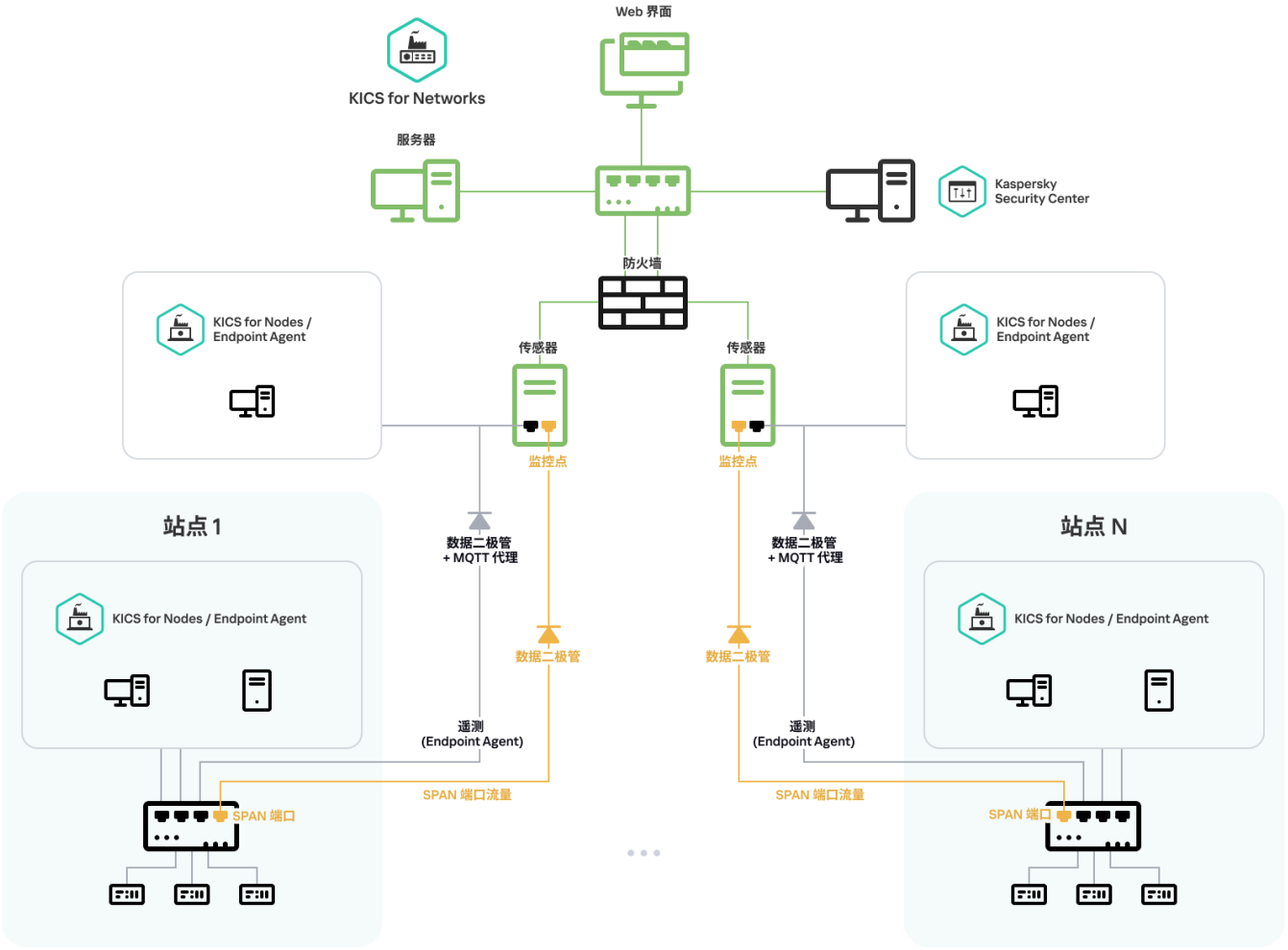
  当在集成模式下使用 Kaspersky Industrial CyberSecurity for Nodes 时，会使用此协议。有关配置 EPP 应用程序以使用这种数据传输方法的详细信息，请参阅相应的帮助系统：Kaspersky Industrial CyberSecurity for Nodes 4.5 或Kaspersky Endpoint Agent 4.0。

- UDP

  在集成模式下使用 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 2.0 时，使用此协议。有关配置 EPP 应用程序以使用这种数据传输方法的详细信息，请参阅Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 的帮助系统。

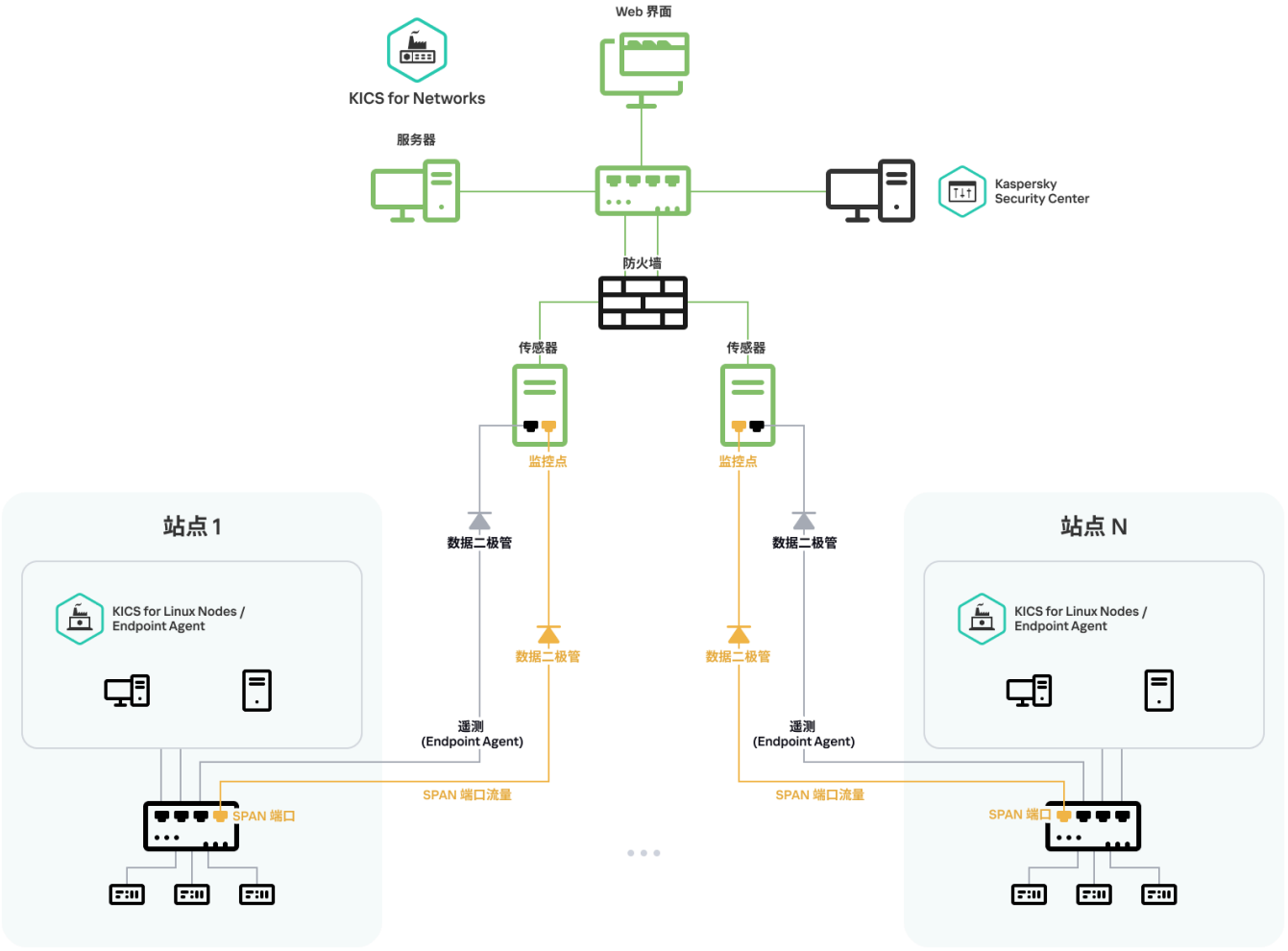
在 Kaspersky Industrial CyberSecurity for Networks 中，集成服务器有助于从 EPP 应用程序接收遥测数据。要接收来自 Endpoint Agent 组件的数据，必须在集成服务器上配置并启用与所用数据传输协议（TCP 模式或 UDP 模式）对应的模式。

下图显示了通过 TCP 上的 MQTT 协议从 EPP 应用程序接收遥测数据的部署场景，以及从多个工业站点的网络交换机的 SPAN 端口发送到 Kaspersky Industrial CyberSecurity for Networks 传感器的流量。在这种情况下，遥测数据通过 MQTT 消息传输。要通过数据二极管传输 MQTT 消息，该二极管必须支持 MQTT 代理功能。要接收和处理数据二极管之后的 MQTT 消息，您必须使用安装了 EPP 应用程序的其他订户计算机。



通过 TCP 使用 MQTT 协议接收来自 EPP 应用程序的流量和数据

下图显示了从 EPP 应用程序通过 UDP 协议接收遥测数据的部署场景，以及从多个工业站点的网络交换机的 SPAN 端口发送到 Kaspersky Industrial CyberSecurity for Networks 传感器的流量。此方案不需要额外的安装了 EPP 应用程序的订户计算机。



通过 UDP 接收来自 EPP 应用程序的流量和数据。

从 Kaspersky SD-WAN 组件接收工业网络流量

Kaspersky Industrial CyberSecurity for Networks 可与 Kaspersky SD-WAN 集成运行。在此模式下运行时，如果在远程站点上安装了用户终端部件 (CPE)（Kaspersky SD-WAN 组件），Kaspersky Industrial CyberSecurity for Networks 将接收通过这些站点交换机的镜像流量。您可以使用 CPE 设备通过将工业网络流量从远程站点转发到应用程序来实现 Kaspersky Industrial CyberSecurity for Networks 的某些功能。数据通过安全通道发送到应用程序。

直接在远程站点接收镜像流量的 CPE 设备会加密流量，然后将其转发到与 Kaspersky Industrial CyberSecurity for Networks 节点共享网络的其他（接收）CPE 设备。如果仅允许通过网关进行发送镜像流量的设备之间的通信，则必须为接收 CPE 设备分配 SD-WAN 网关角色。我们建议将接收 CPE 设备放置在专用的 Kaspersky Industrial CyberSecurity 网络上。这些设备将镜像流量中继到 Kaspersky Industrial CyberSecurity for Networks 节点的网络接口。

Kaspersky Industrial CyberSecurity for Networks 节点网络接口从各种 CPE 设备接收的流量通过根据 IEEE 802.1q 标准添加到网络数据包的虚拟局域网 (VLAN) ID 进行识别。在配置 Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky SD-WAN 之间的集成时，请确保 Kaspersky SD-WAN 组件使用的 VLAN ID 与安装了 Kaspersky Industrial CyberSecurity for Networks 组件的计算机使用的 VLAN ID 相匹配。每个接收具有特定 VLAN ID 的流量的网络接口必须是具有匹配 ID 的 VLAN 接口。

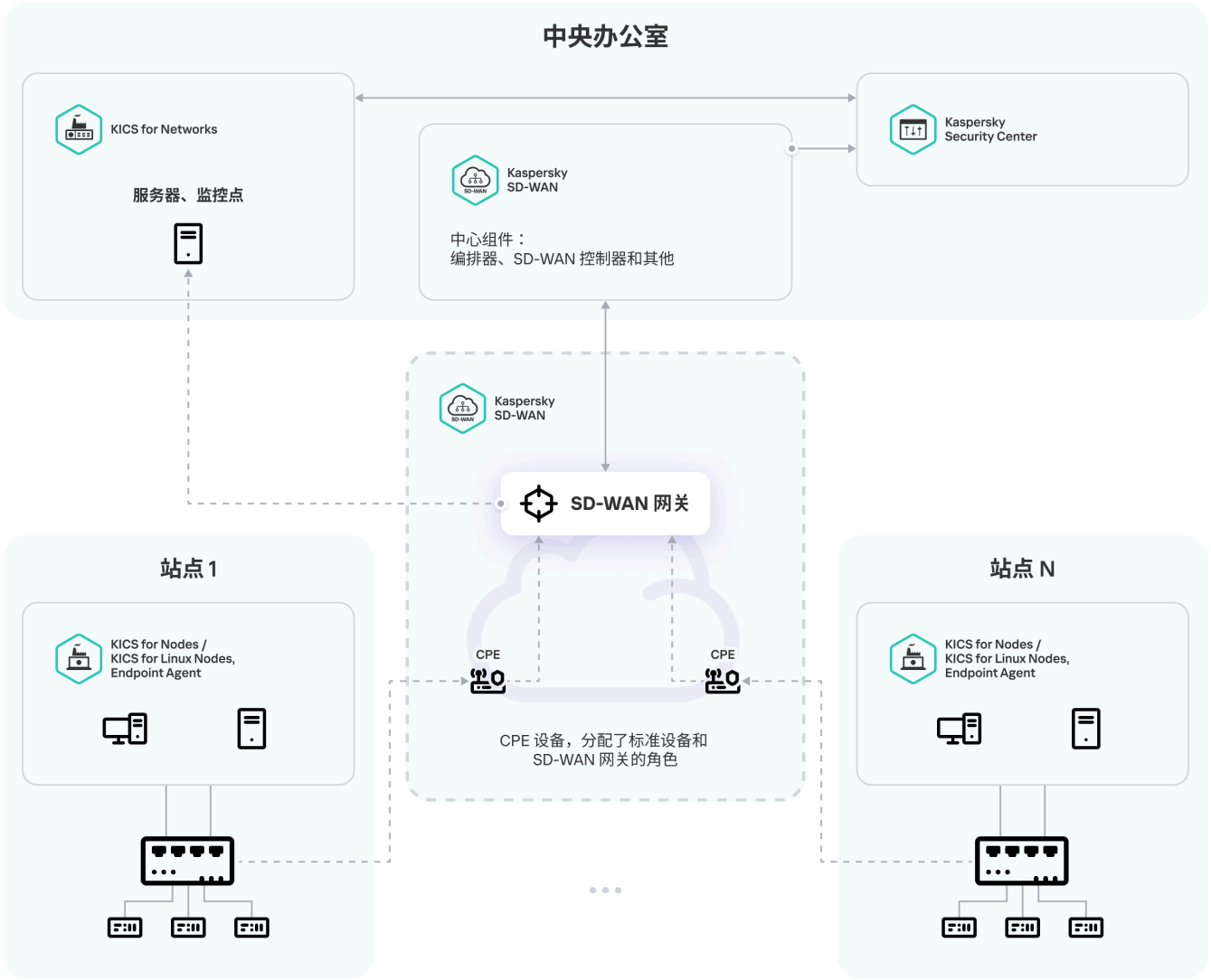
为了有效集成，您可以通过软件组件的额外配置来放宽应用程序中监控点数量的限制。与 Kaspersky SD-WAN 集成的最大可能限制：

- 每个节点最多 100 个监控点
- 总计，应用中的监控点不超过 100 个

Kaspersky Industrial CyberSecurity for Networks 组件的其余部署要求与其他典型部署模式类似，例如无需外部探测器的服务器安装。

> 有关配置软件组件以在集成模式下运行的更多信息，请联系您的技术客户经理 (TAM)。

下图显示了当来自多个站点的镜像流量通过单个 SD-WAN 网关传输到 Kaspersky Industrial CyberSecurity for Networks 服务器时，Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky SD-WAN 的示例部署模式。连接到专用 Kaspersky Industrial CyberSecurity 网络的计算机和安装了中央 SD-WAN 组件的计算机位于公司总部。虚线表示镜像流量从远程站点的交换机所采用的路径。



包含 Kaspersky SD-WAN 的部署模式示例

开始：基本场景

要部署 Kaspersky Industrial CyberSecurity for Networks，您可以按照本帮助文章中的步骤进行操作。点击每个步骤中的链接，即可跳转到包含详细说明的相应帮助文章。

1 准备安装

1.1 → 选择部署方案	1.2 → 选择集中式或本地安装	1.3 → 准备用于集中式或本地安装的计算机
1.4 → 准备网络交换机以将流量复制到 SPAN 端口	1.5 配置已用端口和协议的可用性	

2 安装和初始配置

2.1 → 集中式或本地安装和更新	2.2 → 安装应用程序后加强计算机安全	2.3 → 在节点上配置防火墙
2.4 → 在节点上配置时间同步	2.5 → 安装 Kaspersky Security Center 的管理插件	2.6 安装后应用程序的初始配置

3 正在启动

3.1 → 添加和连接探测器	3.2 → 添加应用程序用户	3.3 → 添加授权许可密钥
3.4 → 配置与 Kaspersky Security Center 的交互	3.5 → 开始安装更新并配置自动更新	3.6 → 添加监控点
3.7 → 启用技术并培训应用程序	3.8 → 添加用于与第三方系统交互的连接器	

3.9

配置应用程序的主要功能：

- 与 EPP 应用程序集成
- 资产管理
- 过程控制
- 交互控制
- 检测规则
- 安全审计

完成 Kaspersky Industrial CyberSecurity for Networks 的部署步骤后，建议您熟悉应用程序保存已收集数据和已定义设置的功能。例如，您可以使用 kics4net-backup.sh 数据迁移脚本配置日志存储设置、连接外部存储以保存流量转储文件、导出和导入安全策略，以及保存和加载数据备份副本。有关应用程序设置的说明，请参阅“Kaspersky Industrial CyberSecurity for Networks 管理帮助”部分。

使用应用程序时，用户可根据其分配的角色执行相应的操作。检查用于完成应用程序用户的以下核心任务的功能：

- 在小部件中监控系统
- 查看网络地图
- 监控网络会话
- 监控事件
- 监控标记值
- 获取报告
- 控制风险以及检测设备上使用的默认密码和不安全的加密协议
- 启动响应操作
- 监控应用程序的状态

安装和删除应用程序

本节包含有关 Kaspersky Industrial CyberSecurity for Networks 安装准备、安装、更新和移除应用程序组件的说明。本节还提供了组件安装后如何执行推荐操作的说明。

您可以集中式或本地安装、更新和移除应用程序组件。执行这些操作的合适方法取决于网络基础设施的准备情况、计算机的远程性和可用性，以及之前选择的应用程序组件安装方法（用于更新或移除操作）。

选择 Kaspersky Industrial CyberSecurity for Networks 的部署方案后，您可以根据以下条件选择合适的应用程序组件安装方法：

- 集中式安装允许您使用一个控制节点，通过一次操作，远程在不同的计算机上安装服务器和 Sensor 组件。要将控制节点连接到计算机，必须在这些计算机上打开 SSH 协议访问权限。请注意，应用程序的安装包将通过网络发送到计算机，在通信速度较慢的情况下，这可能需要一些时间。

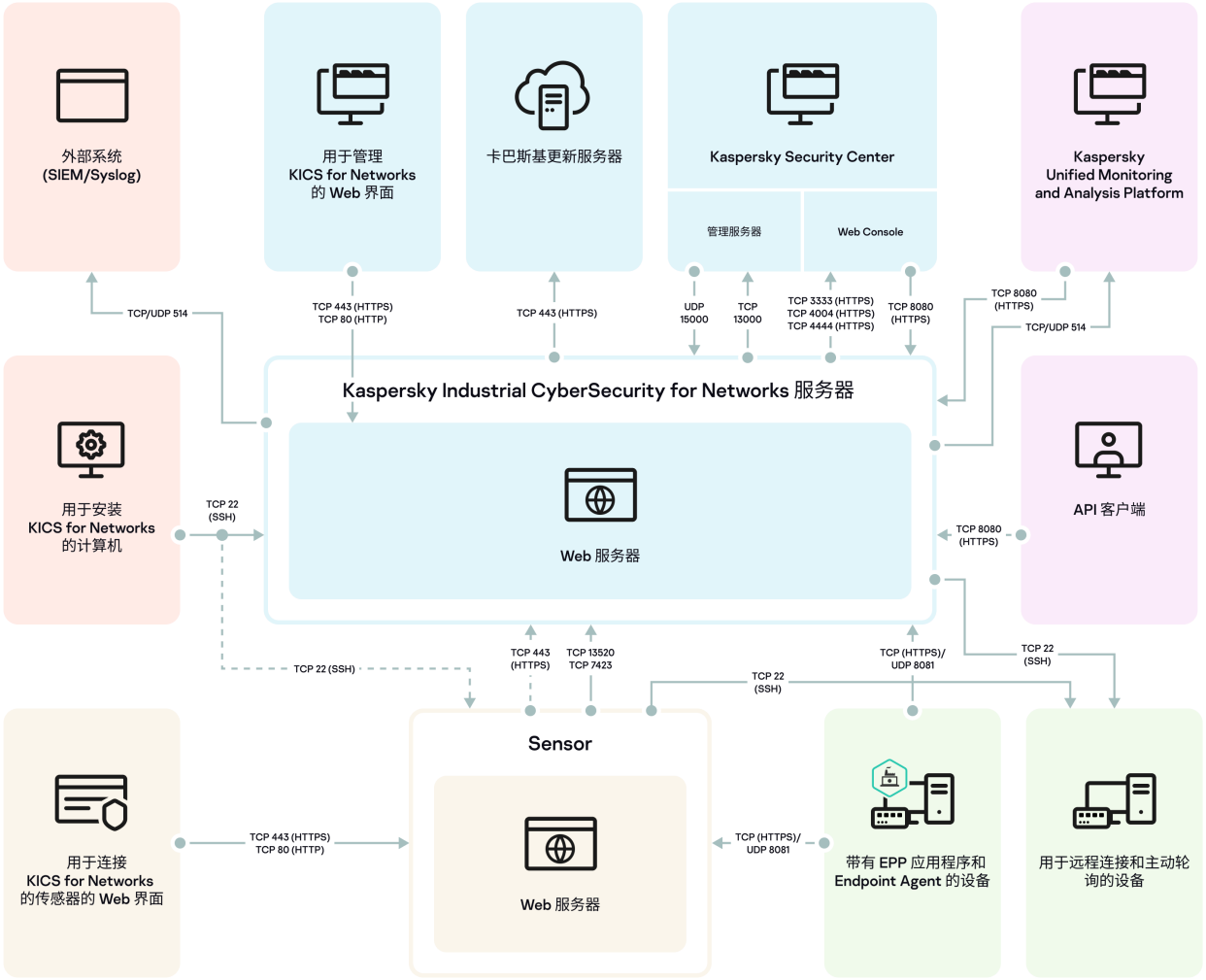
- 如果您需要预先准备服务器节点和 Sensor，然后再将其直接发送到工业站点，那么本地安装是一个便捷的选项。此外，在计算机网络连接受限的情况下，此选项还允许您在现场安装应用程序组件。在这种情况下，应用程序组件将分别安装在每台计算机上。

用于组件安装和操作的端口

为了确保成功安装和运行 Kaspersky Industrial CyberSecurity for Networks 组件，必须提供用于数据传输的特定端口和协议。您需要在用于监控网络流量的网络硬件或软件设置中配置这些端口和协议的使用。尤其需要注意的是，在安装服务器和 Sensor 之后，可能需要对这些计算机上的防火墙进行额外配置，才能使相应功能正常工作。

如果必要的端口和协议被网络设备或软件阻止，Kaspersky Industrial CyberSecurity for Networks 将无法使用需要这些端口进行网络交互的功能。例如，如果服务器计算机的 TCP/UDP 端口 514 不可用，则应用程序将无法通过 **Syslog** 和 **SIEM** 连接器发送数据。

下图显示了应用程序组件使用的端口和协议。



使用的端口和协议

下表描述了所用端口的用途。

所用端口的用途

端口	协议	描述
安装应用程序组件的计算机		
22	TCP (SSH)	该端口用于连接节点并安装服务器和探测器组件。
执行服务器功能的计算机		
22	TCP (SSH)	此端口用于以下用途： • 与安装了应用程序组件的计算机进行交互 • 作为安全审计作业的一部分，通过远程或连接器辅助连接到设备进行扫描
80	TCP (HTTP)	此端口用于通过 Web 界面进行连接。
443	TCP (HTTPS)	此端口用于以下用途： • 通过 Web 界面的连接 • 到卡巴斯基更新服务器的连接 • 通过网络上的 Web 界面自动连接探测器
514	TCP/UDP	此端口用于通过 **Syslog** 和 **SIEM** 连接器发送数据。

端口	协议	描述
3333 4004 4444	TCP (HTTPS)	用于在使用单点登录 (SSO) 技术时与 Kaspersky Security Center Web Console 中的身份和访问管理器组件进行交互。
7423	TCP	该端口用于探测器的连接。
8080	TCP (HTTPS)	此端口用于以下用途： • 通过 Kaspersky Industrial CyberSecurity for Networks API （包括 KUMA 连接器）进行连接 • 连接 Kaspersky Security Center Web Console
8081	TCP (HTTPS) / UDP	如果服务器节点上分别启用了 TCP 或 UDP 模式的集成服务器，则可以使用该功能从 EPP 应用程序接收数据。
13000	TCP	此端口用于将网络代理连接到 Kaspersky Security Center 管理服务器。
13520	TCP	该端口用于探测器的连接。
15000	UDP	用于从 Kaspersky Security Center 管理服务器向网络代理发送控制信号。
执行探测器功能的计算机		
22	TCP (SSH)	此端口用于以下用途： • 与安装了应用程序组件的计算机进行交互 • 作为安全审计作业的一部分，通过远程或连接器辅助连接到设备进行扫描
80	TCP (HTTP)	此端口用于通过 Web 界面进行连接。
8081	TCP (HTTPS) / UDP	如果传感器节点上分别启用了 TCP 或 UDP 模式的集成服务器，则可以使用该功能从 EPP 应用程序接收数据。

集中安装和卸载应用程序组件

本节提供有关在一台计算机上集中安装和卸载应用程序组件的信息。使用名为 kics4net-deploy-<应用程序版本号>.bundle.sh 的脚本可以集中安装和卸载 Kaspersky Industrial CyberSecurity for Networks 服务器和 Sensor。

如果在执行集中安装后需要安装或卸载特定组件，您可以使用应用程序分发包中包含的本地安装或卸载脚本。

应用程序组件的集中安装流程包含以下步骤：

1. **满足集中安装要求**

   在此步骤中，请确保已满足集中安装要求。

2. **应用程序安装准备**

   在此阶段，请为 Kaspersky Industrial CyberSecurity for Networks 组件的集中安装准备好计算机。

3. **集中安装应用程序组件**

   在此步骤中，使用名为 kics4net-deploy-<应用程序版本号>.bundle.sh 的脚本执行应用程序组件的集中安装。集中安装可以通过以下模式进行：

   - 交互模式。在此模式下，运行 kics4net-deploy-<应用程序版本号>.bundle.sh 脚本并按照脚本中的说明进行操作。
   - 非交互模式。在此模式下，准备安装设置文件，并使用 `silent-mode` 参数运行 kics4net-deploy-<应用程序版本号>.bundle.sh 脚本。

   等待脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 完成。

4. **加强已安装应用程序组件的计算机的安全性**

   安装 Kaspersky Industrial CyberSecurity for Networks 后，建议您加强已安装应用程序组件的计算机的操作系统的安全性。集中安装期间，操作系统加强将使用名为 kics4net-deploy-<应用程序版本号>.bundle.sh 的脚本执行。

5. **为 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Networks 管理插件**

   如果您需要使用 Kaspersky Security Center 的功能来操作 Kaspersky Industrial CyberSecurity for Networks，请安装 Kaspersky Industrial CyberSecurity for Networks 管理插件。我们提供以下管理插件：

   - Kaspersky Security Center Web Console 的 Web 管理插件 - 此插件旨在用于 Kaspersky Security Center Linux，以及 Kaspersky Security CenterWindows 中的高级集中控制和单点登录技术。您可以使用 Kaspersky Security Center Web Console 界面中提供的方法之一来安装此插件。

   - 基于 Microsoft 管理控制台 (MMC) 的管理控制台管理插件 - 此插件旨在用于 Kaspersky Security Center Windows。或者，您也可以将插件本地安装在安装了 Kaspersky Security Center 管理服务器的计算机上。

6. **服务器安装后应用程序的启动配置**

   安装服务器后，请在 Kaspersky Industrial CyberSecurity for Networks 的 Web 界面中完成初始配置。完成初始配置后，Web 界面页面将打开并进入应用程序的正常操作模式。

安装应用程序组件后，即可准备运行该应用程序。

应用程序组件的集中安装要求

在将集中安装组件的计算机上，验证是否满足以下条件：

- 计算机满足硬件和软件要求。
- 计算机的部件、硬件和软件符合所有操作安全建议。
- 为了确保应用程序组件正常运行，请使用仅安装了操作系统软件的专用计算机。

  如果计算机上安装了第三方应用程序，Kaspersky Industrial CyberSecurity for Networks 的组件的性能可能会降低。

- 计算机可以访问网络，并且已配置并打开通过 SSH 进行的访问。
- 计算机具有带 root 权限的用户账户（应用程序组件将安装在这些用户账户下）。
- 计算机没有为应用程序组件之间的交互保留的具有以下名称的任何用户帐户或组（如果这些帐户存在，则在安装应用程序后，它们可以获得提升的访问权限，甚至是 root 权限）：
  - kics4net
  - kics4net-anomaly-hunter
  - kics4net-apm
  - kics4net-asset-config-repo
  - kics4net-asset-inventory

- kics4net-blob-storage
- kics4net-cli
- kics4net-clickhouse
- kics4net-config-control-orch
- kics4net-connectors
- kics4net-connectors-launcher
- kics4net-email-gateway
- kics4net-epp-proxy
- kics4net-fts
- kics4net-nats
- kics4net-nats-server
- kics4net-oval-facade
- kics4net-postgresql
- kics4net-report-builder
- kics4net-report-data-source
- kics4net-report-renderer
- kics4net-report-tc
- kics4net-report-tcv
- kics4net-responses-manager
- kics4net-risk-oval-detector
- kics4net-scap-manager
- kics4net-scap-manager-view
- kics4net-scan-oval-manager
- kics4net-scheduler
- kics4net-secrets
- kics4net-task-m
- kics4net-task-mv
- kics4net-telemetry-proxy

- kics4net-vault
- kics4net-websensor
- kics4net-webserver

准备集中安装组件

在准备计算机以安装应用程序组件之前，请确保已满足集中安装要求。

若要准备计算机以安装应用程序组件：

1. 在所有将要安装应用程序组件的计算机上，为具有 root 权限的用户账户设置相同的密码（应用程序组件将安装在该用户账户下）。默认情况下，使用 root 用户帐户来执行安装。记住用户名和密码。您需要在应用程序安装脚本运行时提供这些数据。

   > 应用程序组件安装后，建议您更改这些用户的密码。

2. 查找并保存有关计算机的以下信息：

   - 将执行服务器功能的计算机的名称和 IP 地址。
   - 将执行探测器功能的计算机的 IP 地址。
   - 安装有 Kaspersky Security Center 的计算机的名称或 IP 地址和 SSL 端口。

   要显示计算机名称，可以在命令行中输入`hostname`命令。要显示有关 IP 地址和网络接口的信息，可以在命令行中输入`sudo ifconfig`命令（在 Windows 操作系统中，使用`ipconfig`命令）。

3. 在将执行集中安装的计算机上，使用 SSH 协议连接到将安装应用程序组件的每台计算机。需要建立连接来验证通过 SSH 进行的访问。

   若要连接：

   a. 在命令行中输入以下命令：

   ```
   ssh <用户名>@<计算机 IP地址>
   ```

   b. 输入此命令后，根据操作系统提示执行必要的操作。

   c. 要终止连接会话，请使用以下命令：

   ```
   exit
   ```

4. 将分发套件中的 kics4net-release_<应用程序版本>.tar.gz 档案复制到将要执行安装的计算机。

5. 转到包含复制档案的文件夹并输入以下命令来解压它：

```
tar -zxvf kics4net-release_<应用程序版本>.tar.gz
```

解压后的文件夹和文件将出现在子文件夹 kics4net-release_<application version> 中。

6. 如果您要连接到 Kaspersky Security Center，而安装服务器的计算机上未安装 Kaspersky Security Center 网络代理，请将网络代理安装包 (klnagent64-<网络代理版本>.x86_64.rpm) 复制到 kics4net-release_<应用程序版本号>/linux-centos。

您可以从 Kaspersky Endpoint Security for Business 应用程序下载页面 下载 Kaspersky Security Center 网络代理安装包。要下载软件包，请打开 **Kaspersky Security Center**，并在子部分列表中找到**"版本 <最新版本号> | Red Hat Enterprise Linux x64 |** 网络代理"这一行。然后，在该子部分中，选择 Kaspersky Security Center Linux 的受支持版本（之后，该行将显示相应的网络代理版本）以及网络代理的本地化语言。要开始下载，请点击该子部分中的**"下载"**按钮。

集中安装应用程序组件

本文介绍使用名为 kics4net-deploy-<应用程序版本号>.bundle.sh 的脚本进行应用程序组件集中安装的过程。

在集中安装组件之前，您必须执行必要的操作以准备应用程序安装。

应用程序组件集中安装脚本使用保存在安装设置文件中的数据。运行脚本不需要从其执行安装的计算机上的当前用户帐户具有 root 权限。

若要在计算机上集中安装 Kaspersky Industrial CyberSecurity for Networks 的组件：

1. 在将执行集中安装的计算机上，转到包含用于安装、验证和删除应用程序组件的脚本和包的解压文件的文件夹（包含在分发套件中）。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。

2. 输入运行应用程序组件集中安装脚本的命令：

```
bash kics4net-deploy-<应用程序版本号>.bundle.sh
```

屏幕上将显示语言菜单。

3. 选择您的语言。

所选语言将用于集中安装菜单和 Kaspersky Industrial CyberSecurity for Networks 组件。服务器安装完成后，应用程序组件将使用在此阶段选择的语言。

4. 在选择安装选项的菜单中，选择**运行全新安装**。

屏幕上将显示集中安装主菜单。

5. 执行以下操作：

a. 点击菜单中的**添加服务器**，添加服务器节点并配置该节点的主要设置。

b. 如果要为服务器节点配置其他设置，请选择**更改服务器设置**并配置相关设置。

c. 安装带有探测器的服务器时，在菜单中选择**添加 Sensor**来添加探测器节点。

d. 如果要为添加的探测器节点配置额外设置，请选择**更改 Sensor 设置**并为每个添加的节点配置相关设置。

e. 在菜单中选择**更改运行安装的用户**以指定具有 root 权限的用户帐户，该帐户将用于应用程序组件的集中安装。此用户帐户将用于配置高级设置时未指定其他帐户的节点。

6. 完成配置设置后，选择**保存设置并开始安装**。

   您将被提示输入运行安装的用户的密码。

7. 输入运行安装的用户的密码。必须输入密码两次：第一次在`SSH password`提示符中输入，第二次在`BECOME password`提示符中输入。

   安装脚本将开始安装组件。在安装过程中，屏幕将显示有关操作完成的服务消息。

等待脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 完成。

Kaspersky Industrial CyberSecurity for Networks 组件安装完成后，该应用程序尚未准备好监控您的工业网络。要使用该应用程序，您需要执行必要的操作来准备该应用程序的运行。

在非交互模式下集中安装应用程序组件

您可以以非交互（静默）模式集中安装应用程序组件，这意味着无需交互式输入安装设置。对于非交互式集中安装，当运行应用程序组件集中安装脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 时必须使用特殊设置。

您必须准备一个用于非交互式集中安装的安装设置文件。您可以使用脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 准备安装设置文件。

要使用脚本准备集中安装设置文件：

1. 通过完成安装过程的步骤 1-5 来配置集中安装设置。

2. 通过选择**保存设置并退出而不安装**来保存安装设置文件。

   名为 inventory.json 的安装设置文件保存在 /home/<user>/.config/kaspersky/kics4net-deploy/ 文件夹中（应用程序组件不会被安装）。

3. 如有必要，将集中安装设置文件复制到不同文件夹中。

准备好集中安装设置文件后，就可以采用非交互方式集中安装应用程序组件。

要在非交互模式下集中安装应用程序组件：

1. 在将执行集中安装的计算机上，转到包含用于安装、验证和删除应用程序组件的脚本和包的解压文件的文件夹（包含在分发套件中）。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。

2. 输入以下命令：

```
bash kics4net-deploy-<应用程序版本号>.bundle.sh --silent-mode
```

`--silent-mode` – 启用非交互安装模式（强制参数）。

除了必需参数外，您还可以添加以下参数来运行安装脚本：

- `-i <安装设置文件的路径>`表示集中安装设置文件的完整路径和名称。如果该设置未定义，则使用位于 /home/<user>/.config/kaspersky/kics4net-deploy/ 文件夹中的 inventory.json 文件。
- `--enable-debug-grpc-server` – 安装调试 gRPC 服务器。此 gRPC 服务器用于测试目的，对于应用程序的正常使用不是必需。

  如果脚本使用`--enable-debug-grpc-server`参数运行，则应用程序将失去其认证状态。

输入脚本运行命令后，屏幕会提示您输入运行集中安装的用户的密码。

3. 输入运行集中安装的用户的密码。密码必须输入两次：先在`SSH password`提示符中，然后在`BECOME password`提示符中。

   集中安装脚本将开始安装组件。在安装过程中，屏幕将显示有关操作完成的服务消息。

等待脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 完成。

集中安装菜单命令

本文提供有关集中安装菜单中主要命令的信息。菜单在运行应用程序组件集中安装脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 时显示。该文件必须在应用程序安装准备期间创建的文件夹中运行。

您可以使用集中安装菜单来创建或修改应用程序安装配置并运行安装或删除组件的过程。

安装菜单具有分层的项目结构。第一级包含主菜单的项目。要选择必要的选项，您必须输入其编号并按**ENTER**。如果所选项目带您进入另一组项目，则屏幕上会出现子菜单。

定义设置值的菜单项可能具有默认值或先前定义的值。这些值显示在项目名称后的括号中。

主菜单中的命令被组织成组。

服务器安装管理命令

您可以使用以下安装菜单命令来管理服务器安装：

- **添加服务器** – 添加将被分配服务器功能的新节点。如果尚未添加服务器，则此项可用。如果选择此选项，则当出现以下提示时，您需要指定服务器的主要设置：
  - **输入要安装的节点的 IP 地址** – 定义用于通过 SSH 协议连接计算机并安装服务器的 IP 地址。
  - **使用 Kaspersky Security Center 添加应用程序交互功能** – 添加允许使用 Kaspersky Security Center 管理服务器接收授权许可密钥和下载更新，以及将事件和应用程序状态中继到 Kaspersky Security Center 的功能。您不必添加此功能来将事件中继到其他接收系统。

    如果添加了应用程序与 Kaspersky Security Center 交互的功能，则在安装应用程序时会安装 Kaspersky Security Center 的网络代理组件。这需要准备集中安装组件时创建的 kics4net-release_<应用程序版本>/linux-centos 目录包含网络代理安装包。

如果另一个卡巴斯基应用程序正在使用此组件，则不会安装网络代理（以避免破坏此应用程序和 Kaspersky Security Center 管理服务器之间的交互）。此外，如果安装的网络代理的版本与卡巴斯基工业网络安全解决方案 — 网络安全分发包中提供的该组件的版本不同，卡巴斯基工业网络安全解决方案 — 网络安全与 Kaspersky Security Center 之间的交互功能可能会受到限制。

- **启用服务器和 Sensor 之间的时间同步** — 启用服务器和探测器节点之间的自动时间同步。

- **更改服务器设置** — 修改已添加服务器的设置。您可以使用此菜单项更改可编辑的主要组件设置并配置高级设置。选择此项后，您将看到一个子菜单，您可以在其中更改以下设置：

  - **指定其他用户以运行安装** — 定义将用于在服务器节点上运行安装的其他用户帐户。如果此节点上具有 root 权限的用户名与**更改运行安装的用户**下定义的用户名不同，则需要指定其他用户帐户。将被用于运行安装的所有用户帐户的密码必须匹配。

  - **启用硬件 Watchdog** — 启用硬件看门狗的使用。*硬件看门狗*是一个由硬件实现的用于控制系统挂起的系统。如果节点具有硬件看门狗，您可以在 Kaspersky Industrial CyberSecurity for Networks 中启用它。如果启用了硬件看门狗，请在**指定硬件 Watchdog 的路径**下指定其路径。

  - **禁用硬件 Watchdog** — 禁用硬件看门狗的使用。

  - **使用 Kaspersky Security Center 添加应用程序交互功能** — 添加使应用程序能够与 Kaspersky Security Center 交互的功能（除非已经添加）。此菜单项相当于**使用 Kaspersky Security Center 添加应用程序交互功能**菜单中的**添加服务器**项。

  - **使用 Kaspersky Security Center 删除应用程序交互功能** — 删除允许应用程序与 Kaspersky Security Center 交互的功能。

  - **启用服务器和 Sensor 之间的时间同步** — 启用服务器和节点之间的自动时间同步（除非已启用）。该菜单项相当于**启用服务器和 Sensor 之间的时间同步**菜单中的**添加服务器**项。

  - **禁用服务器和 Sensor 之间的时间同步** — 禁用服务器和节点之间的自动时间同步。

  - **重新创建数据库** — 在重新安装应用程序期间删除现有数据库并创建一个新的数据库。

    如果选择此菜单项，服务器安装后现有数据库中的信息将会丢失。

- **删除服务器** — 删除服务器节点。

探测器安装管理命令

您可以使用以下安装菜单命令来管理探测器的安装：

- **添加 Sensor** — 添加一个新节点以分配探测器功能。如果选择此选项，则在出现**输入要安装的节点的 IP 地址**提示时，需要指定探测器的主要设置。在此提示中，您可以定义用于通过 SSH 协议连接计算机并安装探测器的 IP 地址。

- **更改 Sensor 设置** — 修改添加的探测器的设置。您可以使用此菜单项更改可编辑的主探测器设置并配置高级设置。选择此菜单项将显示在其上已添加探测器的节点列表。选择节点后，您将看到一个子菜单，您可以在其中更改以下设置：

  - **指定其他用户以运行安装** — 定义一个将用于在探测器节点上运行集中安装的其他用户账户。如果此节点上具有 root 权限的用户名与**更改运行安装的用户**下定义的用户名不同，则需要指定其他用户帐户。将被用于运行安装的所有用户帐户的密码必须匹配。

  - **启用硬件 Watchdog** — 启用硬件看门狗的使用。*硬件看门狗*是一个由硬件实现的用于控制系统挂起的系统。如果节点具有硬件看门狗，您可以在 Kaspersky Industrial CyberSecurity for Networks 中启用它。如果启用了硬件看门狗，请在**指定硬件 Watchdog 的路径**下指定其路径。

- **删除 Sensor** — 移除探测器节点。选择此项将显示在其上已添加探测器的节点列表。

常规安装命令

常规安装菜单命令包括以下命令：

- **更改运行安装的用户** — 定义运行应用程序组件集中安装的具有 root 权限的用户名。必须在所有计算机上为运行安装的用户帐户设置相同的密码。安装组件时必须输入密码。

- **查看应用程序安装设置** — 显示安装设置及其值的列表。

安装菜单退出命令

您可以使用以下命令退出集中安装菜单：

- **保存设置并开始安装** — 根据定义的安装设置安装 Kaspersky Industrial CyberSecurity for Networks 应用程序组件。定义的设置保存在安装设置文件中。应用程序集中安装脚本将安装设置文件保存在运行该脚本的每台计算机上。

- **保存设置并退出而不安装** — 保存对安装设置文件的更改，终止集中安装脚本，退出而不安装组件。

- **退出而不保存设置** — 终止集中安装脚本而不保存对安装设置文件的更改。

应用程序组件的重新配置和集中重新安装

您可以集中重新安装 Kaspersky Industrial CyberSecurity for Networks 的组件。例如，在以下情况下可能需要重新安装组件：

- 添加新探测器。
- 更改可在集中安装菜单中定义的设置。

为了集中重新安装应用程序组件，名为 kics4net-deploy-<应用程序版本号>.bundle.sh 的脚本将使用保存在计算机上的安装设置文件。如果此计算机上的安装设置文件已损坏或在其原始文件夹中丢失，则应用程序集中安装脚本将在该计算机和安装了应用程序组件的其他计算机上搜索该文件的副本。

要集中重新安装 Kaspersky Industrial CyberSecurity for Networks 组件：

1. 通过完成安装过程的步骤 1-3 来运行应用程序集中安装脚本。
2. 在选择安装选项的菜单中，选择**编辑当前安装设置**。

   屏幕上将显示集中安装主菜单。
3. 根据所需的结果，执行以下操作：
   - 在菜单中选择**更改服务器设置**来指定服务器设置。

     您不能更改服务器的 IP 地址。要更改 IP 地址，请先删除现有服务器，然后通过选择菜单中的**添加服务器**使用新 IP 地址再次添加它（如果尚未添加服务器，则会出现此选项）。
   - 如果服务器安装了探测器，请在菜单中选择**更改 Sensor 设置**来指定探测器的设置。

     您无法更改先前添加的探测器的 IP 地址。要更改 IP 地址，请先删除现有探测器，然后通过选择菜单中的**添加 Sensor**使用新 IP 地址再次添加它。您还可以使用此菜单项添加新的探测器。
   - 在菜单中选择**更改运行安装的用户**，以指定用于在计算机上集中安装应用程序组件的具有 root 权限的账户的用户名。此帐户将用于在配置服务器或探测器的高级设置时未指定其他帐户的节点。
4. 完成配置设置后，选择**保存设置并开始安装**。

   您将被提示输入运行安装的用户的密码。
5. 输入运行安装的用户的密码。必须输入密码两次：第一次在`SSH password`提示符中输入，第二次在`BECOME password`提示符中输入。

   安装脚本将开始安装组件。在安装过程中，屏幕将显示有关操作完成的服务消息。

等待脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 完成。

集中删除应用程序组件

Kaspersky Industrial CyberSecurity for Networks 组件可以使用 kics4net-deploy-<应用程序版本号>.bundle.sh 进行集中删除。该脚本可让您从服务器或探测器的单个节点中删除应用程序组件，或完全卸载应用程序的当前版本以及以前的版本（从 2.0 版开始）。

为了删除组件，脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 使用保存在计算机上的集中安装设置文件。如果此计算机上的集中安装设置文件已损坏或在其原始文件夹中丢失，则应用程序安装脚本将在该计算机和安装了应用程序组件的其他计算机上搜索该文件的副本。

要从单个节点集中删除应用程序组件：

1. 通过完成安装过程的步骤 1-3 来运行应用程序组件集中安装脚本。
2. 在选择安装选项的菜单中，选择**编辑当前安装设置**。

   屏幕上将显示集中安装主菜单。
3. 根据所需的结果，执行以下操作：
   - 在菜单中选择**删除服务器**以删除服务器节点。

     删除服务器节点后，需要添加不同的服务器节点以确保应用程序正常运行。
   - 在菜单中选择**删除 Sensor**以删除探测器节点。如果应用程序中添加了多个探测器，请在已添加探测器的节点列表中选择相关节点。
4. 完成配置设置后，选择**保存设置并开始安装**。
5. 在`SSH password`和`BECOME password`提示中，输入执行应用程序组件集中删除的用户帐户的密码。

   等待脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 完成。

要完全删除应用程序：

1. 通过完成安装过程的步骤 1-3 来运行应用程序组件集中安装脚本。
2. 在选择安装选项的菜单中，选择**编辑当前安装设置**。

   屏幕上将显示集中安装主菜单。
3. 在菜单中选择**删除服务器**以删除服务器节点。
4. 如果探测器已被添加到应用程序中，请在菜单中选择**删除 Sensor**以逐个删除所有探测器节点。

5. 在菜单中选择**删除设置**来配置集中删除的高级设置。当选择此项时，会出现以下提示：

   - **将应用程序与数据一起删除吗 (y/n)?**如果要删除系统中应用程序保存的所有数据，请输入`y`。如果不需要删除数据，请输入`n`。

   - **删除网络代理吗 (y/n)?**如果您想要删除 Kaspersky Security Center 网络代理组件，请输入`y`。如果不需要删除此组件，请输入`n`。如果检测到已安装的网络代理，则会显示此提示。

6. 选择**保存设置并开始安装**。

7. 在`SSH password`和`BECOME password`提示中，输入执行集中删除的用户帐户的密码。

等待脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 完成。

删除 Kaspersky Industrial CyberSecurity for Networks 不会自动删除分发套件中复制和解压的文件。如果有必要，可以手动删除这些文件。

本地安装和卸载应用程序组件

本节提供有关使用以下脚本在本地安装和卸载应用程序组件的信息：

- kics4net-install.sh 是用于本地安装应用程序组件的脚本。
- kics4net-remove.sh 是用于本地移除应用程序组件的脚本。

本地安装应用程序组件的方案包括以下步骤：

1. **满足本地安装要求**

   在此步骤中，请确保已满足本地安装要求。

2. **应用程序安装准备**

   在此步骤中，准备计算机以在本地安装 Kaspersky Industrial CyberSecurity for Networks 组件。

3. **本地安装应用程序组件**

   在此步骤中，使用 kics4net-install.sh 脚本在所有计算机上执行应用程序组件的本地安装。应用程序组件本地安装脚本只能在计算机上安装其中一个组件（服务器或探测器）。

4. **加强已安装应用程序组件的计算机的安全性**

   安装 Kaspersky Industrial CyberSecurity for Networks 后，建议您加强已安装应用程序组件的计算机的操作系统的安全性。通过使用 kics4net-harden.sh 本地启动脚本来加强安全性，该脚本位于安装了应用程序组件的计算机上的 /opt/kaspersky/kics4net/sbin/ 目录中。

5. **为 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Networks 管理插件**

如果您需要使用 Kaspersky Security Center 的功能来操作 Kaspersky Industrial CyberSecurity for Networks，请安装 Kaspersky Industrial CyberSecurity for Networks 管理插件。我们提供以下管理插件：

- Kaspersky Security Center Web Console 的 Web 管理插件 - 此插件旨在用于 Kaspersky Security Center Linux，以及 Kaspersky Security CenterWindows 中的高级集中控制和单点登录技术。您可以使用 Kaspersky Security Center Web Console 界面中提供的方法之一来安装此插件。
- 基于 Microsoft 管理控制台 (MMC) 的管理控制台管理插件 - 此插件旨在用于 Kaspersky Security Center Windows。或者，您也可以将插件本地安装在安装了 Kaspersky Security Center 管理服务器的计算机上。

6. **服务器安装后应用程序的启动配置**

   安装服务器后，请在 Kaspersky Industrial CyberSecurity for Networks 的 Web 界面中完成初始配置。完成初始配置后，Web 界面页面将打开并进入应用程序的正常操作模式。

安装应用程序组件后，即可准备运行该应用程序。

应用程序组件的本地安装要求

在将安装服务器或探测器的计算机上，验证是否满足以下条件：

- 计算机满足硬件和软件要求。
- 计算机的部件、硬件和软件符合所有操作安全建议。
- 为了确保应用程序组件正常运行，请使用仅安装了操作系统软件的专用计算机。

  如果计算机上安装了第三方应用程序，Kaspersky Industrial CyberSecurity for Networks 的组件的性能可能会降低。

- 可以通过网络访问计算机。
- 计算机有一个拥有 root 权限的用户账户（本地安装脚本将在此用户账户下运行）。
- 计算机没有为应用程序组件之间的交互保留的具有以下名称的任何用户帐户或组（如果这些帐户存在，则在安装应用程序后，它们可以获得提升的访问权限，甚至是 root 权限）：
  - 如果要安装服务器：
    - kics4net
    - kics4net-anomaly-hunter
    - kics4net-apm
    - kics4net-asset-config-repo
    - kics4net-asset-inventory
    - kics4net-blob-storage
    - kics4net-cli
    - kics4net-clickhouse

- kics4net-config-control-orch
- kics4net-connectors
- kics4net-connectors-launcher
- kics4net-email-gateway
- kics4net-epp-proxy
- kics4net-fts
- kics4net-nats
- kics4net-nats-server
- kics4net-oval-facade
- kics4net-postgresql
- kics4net-report-builder
- kics4net-report-data-source
- kics4net-report-renderer
- kics4net-report-tc
- kics4net-report-tcv
- kics4net-responses-manager
- kics4net-risk-oval-detector
- kics4net-scap-manager
- kics4net-scap-manager-view
- kics4net-scan-oval-manager
- kics4net-scheduler
- kics4net-secrets
- kics4net-task-m
- kics4net-task-mv
- kics4net-telemetry-proxy
- kics4net-vault
- kics4net-webserver

- 如果要安装探测器：
  - kics4net
  - kics4net-apm
  - kics4net-connectors
  - kics4net-connectors-launcher
  - kics4net-epp-proxy
  - kics4net-nats
  - kics4net-nats-server
  - kics4net-oval-facade
  - kics4net-telemetry-proxy
  - kics4net-websensor

准备本地安装服务器或探测器

在准备计算机以安装应用程序组件之前，请确保已满足本地安装要求。

要准备计算机以本地安装服务器或探测器：

1. 查找并保存有关计算机的以下信息：
   - 具有 root 权限的账户的用户账户凭据，将用于运行本地安装脚本。
   - 计算机的名称和 IP 地址（用于后续连接到该计算机）。

   要显示计算机名称，可以在命令行中输入`hostname`命令。要显示有关 IP 地址和网络接口的信息，可以在命令行中输入`sudo ifconfig`命令。
2. 将 kics4net-release_<应用程序版本>.tar.gz 档案从分发套件复制到计算机。
3. 转到包含复制档案的文件夹并输入以下命令来解压它：

   ```
   tar -zxvf kics4net-release_<应用程序版本>.tar.gz
   ```

   解压后的文件夹和文件将出现在子文件夹 kics4net-release_<application version> 中。
4. 如果您要连接到 Kaspersky Security Center，而安装服务器的计算机上未安装 Kaspersky Security Center 网络代理，请将网络代理安装包 (klnagent64-<网络代理版本>.x86_64.rpm) 复制到 kics4net-release_<应用程序版本号>/linux-centos。

   您可以从 Kaspersky Endpoint Security for Business 应用程序下载页面 下载 Kaspersky Security Center 网络代理安装包。要下载软件包，请打开 **Kaspersky Security Center**，并在子部分列表中找到**"版本 <最新版本号> | Red Hat Enterprise Linux x64 |** 网络代理"这一行。然后，在该子部分中，选择 Kaspersky Security Center Linux 的受支持版本（之后，该行将显示相应的网络代理版本）以及网络代理的本地化语言。要开始下载，请点击该子部分中的**"下载"**按钮。

使用脚本进行应用程序组件的本地安装

本文介绍使用 kics4net-install.sh 脚本在计算机上本地安装应用程序组件（服务器或探测器）的过程。

在本地安装组件之前，您必须执行必要的操作以准备应用程序安装。

应用程序组件本地安装脚本只能在计算机上安装其中一个组件（服务器或探测器）。如果计算机上已经安装了应用程序组件（例如服务器），则无法在该计算机上安装不同类型的组件（在本例中为探测器）。如果您尝试安装已在计算机上安装的类型的组件，本地安装脚本将重新安装该组件。

安装服务器时，Kaspersky Security Center 网络代理组件会自动安装。这需要准备本地安装组件时创建的 kics4net-release_<应用程序版本> /linux-centos 目录包含网络代理安装包。

如果另一个卡巴斯基应用程序正在使用此组件，则不会安装 Kaspersky Security Center 网络代理（以避免破坏此应用程序和 Kaspersky Security Center 管理服务器之间的交互）。此外，如果安装的网络代理的版本与 Kaspersky Industrial CyberSecurity 解决方案 — 网络安全分发包中提供的该组件的版本不同，Kaspersky Industrial CyberSecurity 解决方案 — 网络安全与 Kaspersky Security Center 之间的交互功能可能会受到限制。

要本地安装 Kaspersky Industrial CyberSecurity for Networks 服务器：

1. 使用要用于运行本地安装脚本的具有 root 权限的用户账户的账户凭据登录系统。
2. 转到包含用于安装、验证和删除分发包中的应用程序组件的脚本和包的文件的文件夹。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。
3. 输入运行服务器本地安装的命令：

   ```
   bash kics4net-install.sh --server
   ```

   其中，`--server` 是启用服务器安装模式的设置（必需设置）。

   此外，您还可以指定以下参数来运行安装脚本：

   `--product-language=<语言>` 定义应用程序本地化语言。该设置可以采用以下值：

   - `english`—英语
   - `russian`—俄语
   - `chinese-simplified` – 简体中文（仅支持 Kaspersky Industrial CyberSecurity for Networks 版本 4.5.1）。

   `--enable-debug-grpc-server` – 安装调试 gRPC 服务器。此 gRPC 服务器用于测试目的，对于应用程序的正常使用不是必需。

   如果脚本使用`--enable-debug-grpc-server`参数运行，则应用程序将失去其认证状态。

4. 如果启动命令不包含 `--product-language=<语言>` 参数，则应用程序组件的语言选择如下：

   - 如果计算机上没有安装任何组件，则在安装过程之前会出现一个菜单，您需要在其中指定所需语言的编号。
   - 如果发现计算机上安装了服务器组件，则重新安装该组件时，脚本将使用上次安装时选择的语言。

   该脚本将开始安装该组件。在安装过程中，屏幕将显示有关操作完成的服务消息。

   等待 kics4net-install.sh 脚本完成。

要在本地安装 Kaspersky Industrial CyberSecurity for Networks 探测器：

1. 使用要用于运行本地安装脚本的具有 root 权限的用户账户的账户凭据登录系统。
2. 转到包含用于安装、验证和删除分发包中的应用程序组件的脚本和包的解压缩文件的文件夹。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。
3. 输入启动探测器本地安装的命令：

   ```
   bash kics4net-install.sh --sensor
   ```

   其中，`--sensor` 是启用探测器安装模式的设置（必需设置）。

   该脚本将开始安装该组件。在安装过程中，屏幕将显示有关操作完成的服务消息。

   等待 kics4net-install.sh 脚本完成。

使用脚本本地删除应用程序组件

本文介绍了使用 kics4net-remove.sh 脚本从计算机本地删除应用程序组件（服务器或探测器）的过程。

要从计算机本地删除 Kaspersky Industrial CyberSecurity for Networks 的组件：

1. 使用要用于运行本地删除脚本的具有 root 权限的用户账户的账户凭据登录系统。
2. 转到包含用于安装、验证和删除分发包中的应用程序组件的脚本和包的解压缩文件的文件夹。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。
3. 输入运行应用程序组件本地删除脚本的命令：

   - 如果要删除已安装的组件文件以及应用程序在系统中保存的所有数据，请输入命令：

     ```
     bash kics4net-remove.sh --full
     ```

   - 如果只想删除已安装的组件文件，输入命令：

     ```
     bash kics4net-remove.sh
     ```

该脚本将开始删除该组件。在删除过程中，屏幕将显示有关操作完成的服务消息。

等待 kics4net-remove.sh 脚本完成。

加强已安装应用程序组件的计算机的安全性

安装 Kaspersky Industrial CyberSecurity for Networks 后，建议加强已安装应用程序组件的计算机的操作系统的安全性。您可以使用以下脚本之一来强化安全性：

- 应用程序组件集中安装脚本 kics4net-deploy-<应用程序版本号>.bundle.sh，该脚本是在准备集中安装组件时获得的。
- 安全强化本地启动脚本 kics4net-harden.sh，该脚本位于安装了应用程序组件的计算机上的 /opt/kaspersky/kics4net/sbin/ 目录中。

您可以使用 kics4net-deploy-<应用程序版本号>.bundle.sh 脚本或 kics4net-harden.sh 脚本执行以下操作：

- 启用阻止启动应用程序组件运行不需要的操作系统服务（例如，avahi-daemon 和 cups）。
- 更改影响操作系统安全的网络配置设置（例如，启用通过 ICMP 协议重定向网络数据包处理的阻止功能）。

使用 kics4net deploy-<应用程序版本>.bundle.sh 脚本集中加强计算机的安全性：

应用程序组件集中安装脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 会对所有已安装应用程序组件的计算机执行强化安全性的操作。

为了加强安全性，该脚本使用保存在计算机上的集中安装设置文件。如果此计算机上的集中安装设置文件已损坏或在其原始文件夹中丢失，则该脚本将在该计算机和安装了应用程序组件的其他计算机上搜索该文件的副本。

为了在集中安装应用程序组件后加强计算机安全：

1. 在从其执行安装的计算机上，转到包含用于安装、验证和删除应用程序组件（包含在分发套件中）的脚本和包的解压文件的目录。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。
2. 输入以下命令：

```
bash kics4net-deploy-<应用程序版本号>.bundle.sh --harden <参数>
```

其中<参数>是以下启动参数之一：

- -s 启用阻止操作系统服务的启动。
- -n 修改网络配置设置。
- -a 启用阻止操作系统服务的启动并修改网络配置设置。

3. 在“SSH 密码”和“BECOME 密码”提示中，输入正在运行集中安装的用户账户的密码。

等待脚本完成。如果成功完成，则会显示有关在安装了应用程序组件的计算机上执行的操作的信息。

使用 kics4net-harden.sh 脚本在本地强化计算机安全性

如果您尚未执行计算机的集中强化，则可以使用 kics4net-harden.sh 脚本在本地强化计算机的安全性。必须在每台已安装应用程序组件的计算机上执行本地强化过程。

为了在本地安装应用程序组件后加强计算机安全：

1. 在安装了应用程序组件的计算机上，使用具有 root 权限的用户账户凭据登录系统。
2. 进入 /opt/kaspersky/kics4net/sbin/ 目录，然后输入以下命令：

```
sudo bash kics4net-harden.sh <参数>
```

其中<参数>是以下启动参数之一：

- -s 启用阻止操作系统服务的启动。
- -n 修改网络配置设置。
- -a 启用阻止操作系统服务的启动并修改网络配置设置。

等待脚本完成。如果成功完成，则会显示关于所执行操作的信息。

在服务器和 Sensor 节点上配置防火墙

安装 Kaspersky Industrial CyberSecurity for Networks 后，建议您检查已安装应用程序服务器和 Sensor 的计算机上必要端口和协议的可用性。在安装这些组件期间，应用程序会自动在操作系统防火墙规则中为使用的主要端口和协议创建必要的排除项。在某些情况下，您可能需要打开 Kaspersky Industrial CyberSecurity for Networks 中可使用的端口和协议列表中的其他端口。

要检查并微调节点上的防火墙规则中定义的排除项：

1. 在安装了应用程序组件的计算机上，使用具有 root 权限的用户账户凭据登录系统。
2. 打开操作系统控制台并输入以下命令：

```
sudo firewall-cmd --list-all
```

3. 检查 端口 行中显示的端口和协议排除项列表。

   默认情况下，该列表包含对主要使用的端口和协议的排除项。您需要检查此列表是否包含 Kaspersky Industrial CyberSecurity for Networks 特定功能所需的必要端口。例如，要使用与 Kaspersky Security Center 交互的功能，服务器计算机上的防火墙必须至少为 TCP 端口 13000 和 UDP 端口 15000 定义排除项。

4. 添加必要端口和协议的排除项。为此，请使用以下命令按顺序指定数据：

```
sudo firewall-cmd --zone=public --permanent --add-port=<端口号>/<协议>
```

示例

```
sudo firewall-cmd --zone=public --permanent --add-port=15000/udp --add-port=13000/tcp
```

5. 重新启动防火墙服务。为此，请输入以下命令：

```
sudo firewall-cmd --reload
```

为 Kaspersky Security Center 安装 Kaspersky Industrial CyberSecurity for Networks 管理插件

Kaspersky Industrial CyberSecurity for Networks 的管理插件可让您使用Kaspersky Security Center 的功能与 Kaspersky Industrial CyberSecurity for Networks 一起工作。根据 Kaspersky Security Center 的版本以及您想要使用 Kaspersky Security Center 执行的操作，您可以安装以下管理插件：

- 基于 Microsoft 管理控制台 (MMC) 的管理控制台管理插件 - 此插件旨在用于 Kaspersky Security Center Windows。

  基于 MMC 的管理控制台的管理插件必须本地安装在安装 Kaspersky Security Center 管理服务器的计算机上。要安装，您需要使用 Kaspersky Industrial CyberSecurity for Networks 套件中的文件。

- Kaspersky Security Center Web Console 的 Web 管理插件 - 此插件旨在用于 Kaspersky Security Center Linux，以及 Kaspersky Security CenterWindows 中的高级集中控制和单点登录技术。

  您必须在已安装 Kaspersky Security Center Web Console 的计算机上安装 Web 插件。所有可通过浏览器访问 Kaspersky Security Center Web Console 的管理员均可使用 Web 插件功能。卡巴斯基应用程序发布新版本后，您可以更新已安装的 Web 插件版本。

安装基于 MMC 的管理控制台的管理插件

您可以通过下列方式之一安装基于 MMC 的管理控制台的管理插件：

- 使用安装向导
- 从命令行

在安装基于 MMC 的管理控制台的管理插件之前，请将应用程序分发工具包存档中的 kics4net-sc-plugin_<插件版本号>_<本地化代码>.msi 文件复制到安装了管理服务器的计算机。使用与 Kaspersky Security Center 的本地化语言相匹配的本地化代码运行该文件。您可以将文件从包含 kics4net-release_<应用程序版本>.tar.gz 存档的解压缩文件的目录复制到已完成应用程序安装准备的计算机。解压缩档案后，管理插件的安装文件位于 kics4net-release_<应用程序版本>/sc_plugin 子文件夹中。

管理插件需要使用属于本地管理员组的账户来安装。

要使用向导安装管理插件：

1. 在安装了 Kaspersky Security Center 管理服务器的计算机上，运行名为 kics4net-sc-plugin_<插件版本号>_<本地化代码>.msi 的文件。

   完成准备操作后，插件安装向导将启动。

2. 按照安装向导的说明进行操作。当被 Windows 用户账户控制 (UAC) 提示进行更改时，单击**"是"**，并在必要时输入本地管理员凭据。

安装向导完成后，Kaspersky Industrial CyberSecurity for Networks 的管理插件会出现在 Kaspersky Security Center 管理服务器属性中已安装的管理插件列表中（基于 MMC 的管理控制台中的管理服务器属性窗口，**高级→有关已安装应用程序管理插件的详情**部分）。

要从命令行安装管理插件：

1. 在安装了 Kaspersky Security Center 管理服务器的计算机上，打开命令行界面。
2. 转到包含名为 kics4net-sc-plugin_<插件版本号>_<本地化代码>.msi 的文件的文件夹。

3. 在命令行中输入以下命令：

```
msiexec /package kics4net-sc-plugin_<插件版本号>_<本地化代码>.msi
```

完成准备操作后，插件安装向导将启动。

4. 按照安装向导的说明进行操作。当被 Windows 用户账户控制 (UAC) 提示进行更改时，单击**"是"**，并在必要时输入本地管理员凭据。

安装向导完成后，Kaspersky Industrial CyberSecurity for Networks 的管理插件会出现在 Kaspersky Security Center 管理服务器属性中已安装的管理插件列表中（基于 MMC 的管理控制台中的管理服务器属性窗口，**高级**→**有关已安装应用程序管理插件的详情**部分）。

使用命令行界面时，您可以使用为 Windows Installer 提供的其他标准插件安装程序启动参数。例如，如果需要，您可以使用相应的启动选项来卸载管理插件。要获取有关可用启动参数的信息，请输入`kics4net-sc-plugin_<插件版本号>_<本地化代码>.msi /help`命令。

安装 Kaspersky Security Center Web Console 的管理 Web 插件

您可以使用以下任意方法安装 Web 插件：

- 从 Kaspersky Security Center Web Console 中的可用分发包列表中安装 Web 插件。

  要安装 Web 插件，请在 Kaspersky Security Center Web Console 界面中选择 Web 插件分发包：**控制台设置** → **Web 插件**。卡巴斯基应用程序的新版本发布后，可用分发包的列表会自动更新。

- 从 Kaspersky Security Center 的可用分发包、插件和修补程序列表中下载分发包。

  要安装 Web 插件，请在 Kaspersky Security Center Web Console 界面中选择 Web 插件分发包：**操作** → **卡巴斯基应用程序** → **当前应用程序版本**。卡巴斯基应用程序的新版本发布后，可用分发包的列表会自动更新。

- 使用 Kaspersky Industrial CyberSecurity for Networks 分发包中提供的文件安装 Web 插件（见下文）。

要使用应用程序分发包中提供的文件安装 Web 插件，您需要将 kics4net-web-ksc-plugin_<Web 插件版本号>.zip 文件复制到已安装 Kaspersky Security Center Web Console 服务器的计算机上。您可以将文件从包含 kics4net-release_<应用程序版本>.tar.gz 存档的解压缩文件的目录复制到已完成应用程序安装准备的计算机。解压缩存档文件后，用于安装 Web 插件的文件位于kics4net-release_<应用程序版本号>/sc_plugin 子目录中。

要使用应用程序分发包中的文件安装 Kaspersky Security Center Web Console 的管理 Web 插件，请执行以下操作：

1. 在 Kaspersky Security Center Web Console 服务器计算机上，解压缩已复制的 kics4net-web-ksc-plugin_<Web 插件版本号>.zip 文件。

2. 在 Kaspersky Security Center Web Console 界面中，转到**控制台设置** → **Web 插件**，然后点击用于从文件添加 Web 插件的按钮。

3. 按顺序指定解压缩存档目录中的文件：plugin.zip 和 signature.txt。

4. 在打开的窗口中，验证 Web 插件安装过程中的操作是否成功，然后关闭窗口。

   Kaspersky Industrial CyberSecurity for Networks Web 插件将出现在已安装的 Web 插件列表中。

服务器安装后应用程序的启动配置

使用集中安装脚本或其他方法安装服务器后，应用程序等待完成启动配置。任何通过 Web 界面连接到服务器的用户都可以完成启动配置。

要在安装服务器后执行应用程序的启动配置：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks Server。使用服务器计算机的 IP 地址进行连接。

2. 选择**启动配置**。

3. 选择程序 Web 界面的本地化语言。

   之后，您可以在正常模式下选择其他 Web 界面语言。

4. 在**管理员账户**"设置组中，定义第一个应用程序用户的用户账户名和密码。管理员角色将被分配给该用户。该用户不必在服务器计算机或其他计算机上注册为操作系统账户。

   对于账户名称，您可以使用英文字母的大小写、数字、点以及以下特殊字符输入任意唯一名称：_ 和 -（例如，Admin_1）。名称必须包含 3 到 20 个字符，必须以字母开头，并以除点之外的任何受支持的字符结尾。

   密码必须满足以下要求：

   - 必须包含 8 到 256 个 ASCII 字符。
   - 必须包含一个或多个英语字母的大写字母。
   - 必须包含一个或多个拉丁字母的小写字母。
   - 必须包含一个或多个数字。
   - 不得包含超过三个连续重复字符。

5. 在"**应用程序服务器**"字段中，输入 Kaspersky Industrial CyberSecurity 中使用的服务器的名称。

   服务器名称必须是唯一的（与其他节点上的传感器名称不匹配）并且包含的字符不得超过 100 个。您可以使用英文字母、数字、空格以及以下特殊字符：_ 和 -（例如，`Server_1`）。服务器名称必须以空格以外的任何允许的字符开始和结束。

6. 请阅读最终用户授权许可协议和隐私策略的条款。为此，请单击以下复选框名称中的相应链接打开每个文档：**我确认我已完全阅读、理解并接受本协议的条款和条件**本**最终用户授权许可协议**，并且**我了解并同意我的数据将按照本协议中的描述进行处理和传输（包括传输到第三国）**我的数据将按照**隐私策略。我确认我已完全阅读并理解本协议的条款隐私策略**的条款：

7. 如果您完全同意最终用户授权许可协议和隐私策略的条款，请选中两个复选框。

   如果您不同意最终用户授权许可协议和/或隐私策略的条款，请关闭 Web 界面页面并从计算机中删除已安装的应用程序组件。

8. 单击"**继续**"。

应用定义的设置后，Web 界面页面将打开并进入应用程序的正常运行模式。第一个应用程序用户的账户凭据将用于当前连接会话。

您可以使用 kics4net-reset-to-defaults.sh 脚本将服务器恢复到初始状态。该脚本位于安装了应用程序组件的计算机的 /opt/kaspersky/kics4net/sbin/ 文件夹中。

Kaspersky Industrial CyberSecurity for Networks 中使用的证书

为确保连接安全，Kaspersky Industrial CyberSecurity for Networks 使用数字证书。应用程序会在安装过程中（集中式或本地）以及添加需要证书才能交互的对象时自动创建必要的证书。所有自动生成的证书均在应用程序服务器端进行自签名。

关于使用的证书

为确保连接安全，Kaspersky Industrial CyberSecurity for Networks 使用以下证书：

- 主服务器证书和应用程序服务证书（包括应用程序 Sensor 上的 Web 服务器服务证书）。
- 通过 Web 界面连接到服务器的证书
- 用于通过 Kaspersky Industrial CyberSecurity for Networks API 连接到服务器的证书
- 用于连接连接器的证书。
- 用于与端点代理软件组件连接的证书。

您可以将一些自动生成的证书替换为由受信任的证书颁发机构颁发的数字证书。当以下证书更新时，将执行替换过程：

- 通过 Web 界面连接到服务器的证书
- 用于通过 Kaspersky Industrial CyberSecurity for Networks API 连接到服务器的证书

使用数据迁移脚本更新应用程序时，无法保存当前已使用的证书。执行此过程时，应用程序会创建新的证书，就像正常安装后一样。因此，先前创建的连接器将停止在应用程序中工作。要恢复其运行，您需要更新用于连接连接器的证书。

更新 SSL 连接证书

自动生成的证书的有效期会超过当前应用程序版本的生命周期（请参阅"应用程序生命周期"页面）。但是，为了确保应用程序的安全运行，不推荐长时间使用相同的证书。应定期更新证书，将自动生成的证书替换为新的证书。

建议在以下情况下更新应用程序中已使用的证书：

- 当前证书已遭到侵害。
- 证书已过期。
- 证书需要根据企业的信息安全要求定期更新。

根据已使用证书的应用范围，更新步骤可能有所不同。更新证书后的后续步骤也存在差异。

更新 Kaspersky Industrial CyberSecurity for Networks 服务器的主证书

应用程序服务器的主证书用于 Kaspersky Industrial CyberSecurity for Networks 节点之间的连接。该证书与其他证书一样，是在应用程序安装过程中自动生成的。在更新过程中替换此证书会影响应用程序中已使用且依赖于主证书的大多数其他证书的有效性。因此，在应用程序中执行主服务器证书更新过程时，还必须更新以下证书：

- 应用程序服务证书（包括应用程序 Sensor 上的 Web 服务器服务证书）：自动更新。
- 通过 Web 界面连接服务器的证书：自动更新。
- 用于通过 Kaspersky Industrial CyberSecurity for Networks API 连接到服务器的证书：自动更新。
- 用于连接连接器的证书：手动更新。

当主服务器证书被替换时，应用程序 Sensor 的旧证书将失效。这将导致 Sensor 与服务器之间的连接终止。要作为证书续订过程的一部分恢复连接，您需要重新添加并重新连接所有传感器。您还需要更新用于连接连接器的证书。

主服务器证书更新完成后，应用程序将使用自签名证书通过 Web 界面连接到服务器，并通过 Kaspersky Industrial CyberSecurity for Networks API 进行连接。要将这些证书替换为由受信任的证书颁发机构颁发的数字证书，您还必须完成以下步骤：更新用于通过 Web 界面连接服务器的证书，以及更新用于通过 Kaspersky Industrial CyberSecurity for Networks API 连接服务器的证书。

要更新主服务器证书及其依赖证书：

1. 在服务器计算机上，转到 /opt/kaspersky/kics4net/sbin/ 文件夹并输入命令以启动本地证书更新脚本：

   ```
   sudo bash kics4net-update-certs.sh
   ```

2. 等待脚本完成。
3. 在每台安装了 Sensor 的计算机上，将 Sensor 重置为初始状态。为此，请转到 /opt/kaspersky/kics4net/sbin/ 目录，并输入命令以运行脚本，将节点本地切换到其初始状态：

   ```
   sudo bash kics4net-reset-to-defaults.sh
   ```

4. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器，然后重新添加并连接 Sensor。

5. 如果已向应用程序添加了连接器，请更新证书以连接这些连接器。

更新用于通过 Web 界面连接到服务器的证书

应用程序在安装过程中会自动创建用于通过 Web 界面连接应用程序服务器的证书，并且在更新主服务器证书或使用数据迁移脚本更新应用程序时也会自动创建该证书。自动生成的证书是应用程序服务器端的自签名证书。

不推荐长期使用自签名证书连接服务器。您可以临时使用此类证书（例如，在 Kaspersky Industrial CyberSecurity for Networks 的测试操作期间）。对于长期使用，推荐将此证书替换为由受信任的证书颁发机构颁发的证书。

应用程序支持从 PFX 文件下载证书。您可以向组织系统管理员寻求帮助以获取受信任的证书文件。

要更新通过 Web 界面连接服务器的证书，请执行以下操作：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 选择“**设置**” → “**连接服务器**”。

3. 在**Web 服务器**选项卡上，使用**浏览**按钮指定证书文件的本地路径。

4. 在“**证书访问密码**”字段中，输入证书访问密码。

5. 单击“**应用**”。

6. 在请求窗口中，确认要应用指定的参数并连接到服务器。

通过 Kaspersky Industrial CyberSecurity for Networks API 更新用于连接服务器的证书

在安装过程中，以及更新主服务器证书或使用数据迁移脚本更新应用程序时，应用程序会自动创建一个用于通过 Kaspersky Industrial CyberSecurity for Networks API 连接到应用程序服务器的证书。自动生成的证书是应用程序服务器端的自签名证书。

不推荐长期使用自签名证书连接服务器。您可以临时使用此类证书（例如，在 Kaspersky Industrial CyberSecurity for Networks 的测试操作期间）。对于长期使用，推荐将此证书替换为由受信任的证书颁发机构颁发的证书。

应用程序支持从 PFX 文件下载证书。您可以向组织系统管理员寻求帮助以获取受信任的证书文件。

当用于通过 Kaspersky Industrial CyberSecurity for Networks 连接到服务器的证书被替换后，用于连接连接器的旧证书将失效。这将导致连接器与服务器之间的连接终止。要恢复连接，您需要更新连接器的证书。

要更新用于通过 Kaspersky Industrial CyberSecurity for Networks API 连接服务器的证书：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接服务器**”。
3. 在“**REST API 服务器**”选项卡上，使用**浏览**按钮指定证书文件的本地路径。
4. 在“**证书访问密码**”字段中，输入证书访问密码。
5. 单击“**应用**”。
6. 在提示窗口中，确认要应用指定的参数。
7. 如果已向应用程序添加了连接器，请更新证书以连接这些连接器。

更新用于连接连接器的证书

当连接器添加到应用程序时，应用程序会自动为每个连接器生成一个连接证书。所有连接器的证书在完成以下步骤之一之前均为有效：

- 更新 Kaspersky Industrial CyberSecurity for Networks 服务器的主证书
- 通过 Kaspersky Industrial CyberSecurity for Networks API 更新用于连接服务器的证书
- 更新 Kaspersky Industrial CyberSecurity for Networks 或使用数据迁移脚本从备份副本恢复

完成上述任一步骤后，您需要更新已添加到应用程序的所有连接器的证书。此外，根据证书更新建议，您可能还需要更新连接器证书，而无需执行上述步骤。

每个连接器的证书更新步骤取决于连接器是受管理的还是不受管理的。对于不受管理的连接器，证书更新过程仅影响连接器的运行服务。这些连接器无需移除即可更新其证书。更新受管理连接器的证书时，您需要从应用程序中移除这些连接器，然后重新添加。

通用和 KUMA 连接器始终为不受管理的连接器。应用程序内置的其他类型连接器可以是受管理的，也可以是不受管理的。创建此类连接器时，用户可以启用忽略受管理的连接器的功能的模式，这将使创建的连接器变为不受管理的连接器。在连接器表中，**可管理的**列中会显示每个连接器的受管理连接器指示器。

要更新不受管理的连接器的连接证书，请执行以下操作：

1. 完成为连接器创建新的通信数据包的步骤。
2. 在连接器服务中注册新的证书。为此，请在连接器部署节点（已安装服务器或 Sensor 的节点）上完成以下操作：
   - 如果 **syslog**、**SIEM**、**通用**、**电子邮件**或 **Cisco 交换机**连接器的证书已更新，请转到 /opt/kaspersky/kics4net-connectors/libexec/ 目录并输入以下命令，以启动用于使用连接器的脚本：

     ```
     sudo python3 default_connectors_registrar.py update
     ```

     当被脚本提示提供连接器数据时，请输入连接器的名称、通信数据包的路径以及连接器证书访问密码。

     等待脚本运行完成，然后输入命令以重启连接器服务：

     ```
     sudo systemctl restart kics4net-connectors@{<连接器的名称>}
     ```

   - 如果**主动轮询**连接器的证书已更新，请转到 /opt/kaspersky/kics4net-apm/src/ 目录并输入以下命令以运行用于使用连接器的脚本：

     ```
     sudo python3 register.py -p "<通信数据包的完整路径>"
     ```

     等待脚本运行完成，然后输入命令以重启主动轮询连接器服务：

     ```
     sudo systemctl restart kics4net-apm
     ```

要更新用于连接受管理连接器的证书：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **连接器**，然后在**连接器**选项卡中选择所需的连接器。

   详细信息区域显示在 Web 界面窗口的右侧部分。
3. 检查当前定义的连接器设置，并在移除此连接器后，按照步骤在新的连接器中恢复必要的设置。

   例如，您可以使用任何文本编辑器保存 **Cisco 交换机**连接器的名称和公钥，或者保存**电子邮件**连接器的地址和特定模板。详细信息区域中的所有文本内容都可以使用鼠标选择，并使用浏览器和操作系统自带的工具（通过上下文菜单或使用剪贴板快捷键）进行复制。
4. 删除连接器吗。
5. 将相同的连接器重新添加到应用程序中。

更新用于与端点代理软件组件连接的证书

在 Kaspersky Industrial CyberSecurity for Networks 中，集成服务器使用证书来连接 Endpoint Agent 软件组件。如果集成服务器运行在 TCP 模式下，则需要证书。集成服务器及其客户端的证书由应用程序服务器颁发。这些证书可能需要根据证书更新建议进行更新。

要更新集成服务器的证书：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接服务器**”。
3. 在“**集成服务器**”选项卡上，选择要为其客户端更新已使用证书的服务器。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 要为集成服务器颁发新的证书，请单击“**重新颁发证书**”按钮。
   更换集成服务器证书后，旧证书将失效。
5. 要为集成服务器的客户端颁发新的证书，请在**客户端证书 (TCP 模式)**部分完成以下操作：
   a. 使用位于包含证书指纹的字段右侧的 × 图标删除旧证书。
   b. 使用**创建新证书**按钮添加新的证书。
6. 单击**保存**。
7. 创建通信数据包并将其下载到客户端计算机。

使用数据迁移脚本更新

您可以使用当前（新）版本应用程序的分发包中的 kics4net-backup.sh 数据迁移脚本升级以前版本的 Kaspersky Industrial CyberSecurity for Networks。应用程序版本 4.0 或更高版本支持使用 kics4net-backup.sh 脚本升级到当前版本的功能。

kics4net-backup.sh 脚本允许您从以前的应用程序版本迁移以下数据：

- 安全策略
- 有关技术和方法的状态和/或操作模式的数据
- 用于更新应用程序模块和数据库的设置
- 有关添加的授权许可密钥的信息
- 审计条目
- 应用程序消息
- 漏洞风险
- 注册的活动
- 为事件保存的流量
- 网络地图数据

- 已注册的网络会话及其保存的协议属性
- 可执行文件的数据

您还可以使用 kics4net-backup.sh 脚本备份当前应用程序版本的数据。除了获取上面列出的数据之外，该脚本还允许您在安装了应用程序组件的节点计算机上额外备份以下数据：

- 应用程序服务的配置
- 计算机名称
- 应用程序版本号：

kics4net-backup.sh 脚本可用于创建数据的备份副本，并从运行该脚本的计算机上的本地备份副本下载数据。因此，要创建数据的备份副本和从备份副本下载数据，请在每台安装了应用程序组件的计算机上按顺序运行该脚本。您可以使用托管服务器和 Sensor 的计算机来执行创建数据备份副本和按任意顺序从备份副本下载数据的步骤。例如，您可以先在服务器计算机上运行脚本，然后在 Sensor 计算机上运行脚本，反之亦然。

使用 kics4net-backup.sh 脚本从应用程序的早期版本升级的场景包含以下步骤：

1. **在服务器和传感器计算机上创建先前应用程序版本的数据备份副本**

   要创建以前应用程序版本的数据的备份副本，请在每台安装了应用程序组件的计算机上执行以下操作：

   1. 在已安装先前版本应用程序组件的计算机上，将当前（新）应用程序版本的分发包中的名为 kics4net-release_<应用程序版本号>.tar.gz 的压缩档案复制到您选择的目录中。
   2. 转到包含复制档案的文件夹并输入以下命令来解压它：

      ```
      tar -zxvf kics4net-release_<应用程序版本号>.tar.gz
      ```

      解压后的文件夹和文件将出现在子文件夹 kics4net-release_<application version> 中。
   3. 转到包含解压的脚本和包文件的文件夹，以便安装、验证和删除应用程序组件。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。
   4. 运行 kics4net-backup.sh 脚本：

      - 要在服务器计算机上创建数据的备份副本，请输入以下命令：

        ```
        sudo bash kics4net-backup.sh -b -p <备份文件路径> <可选设置>
        ```

      - 要在传感器计算机上创建数据的备份副本，请输入以下命令：

        ```
        sudo bash kics4net-backup.sh -s -p <备份文件路径> <可选设置>
        ```

      其中：

      - `-b` 是一个允许将服务器数据记录到备份文件的设置（服务器在计算机上运行时的强制设置）。
      - `-p` 是指示创建的备份文件的完整路径和名称的设置（必需设置）。
      - `-s` 是一个允许将传感器数据记录到备份文件的设置（传感器在计算机上运行时的强制设置）。
      - `<可选设置>` 参考下面列出的一个或多个可选设置。

您可以在运行脚本的命令中使用以下可选设置来创建备份文件：

- `-t` 是禁用流量保留的设置（如果未指定此设置，则会保存流量）。
- `-e` 是禁用已注册事件保留的设置（如果未指定该设置，则会保存事件）。仅当在服务器计算机上创建数据备份副本时才可以指定此设置。
- `-n` 是禁用网络地图数据保留的设置（如果未指定该设置，则保存网络地图数据）。仅当在服务器计算机上创建数据备份副本时才可以指定此设置。
- `-x` 是用于禁用与可执行文件相关的数据的保留的设置（如果未指定该设置，则会保存可执行文件的数据）。仅当在服务器计算机上创建数据备份副本时才可以指定此设置。
- `-a`是一个用于禁用在已注册的网络会话中保留协议属性的设置（如果未指定此设置，则会保存协议属性）。仅当在服务器计算机上创建数据备份副本时才可以指定此设置。
- `-d` 是停止应用程序服务的设置（如果未指定此设置，则应用程序服务将在脚本完成后启动）。

脚本运行命令的一个可选设置是 `-f` 设置，该设置旨在创建应用程序当前版本数据的备份副本，并保存节点的所有可用数据。如果指定此设置，则保存的数据只能在同一节点和同一版本的应用程序中（包含相同的版本号）完全加载。当使用 `-f` 参数时，应用程序将网络会话中的流量（除非使用 `-t` 参数禁用流量保留）、事件、网络地图数据、可执行文件的数据、协议属性以及以下数据保持到备份文件：节点部署参数（包括监控点的参数和在节点上存储数据的设置）、应用程序用户列表、连接器的设置、连接器类型的设置、连接服务器的设置、与 Kaspersky Security Center 交互的设置、已安装的应用程序模块和数据库更新的数据、记录节点上进程活动的日志级别以及用于在线系统监控的小部件的设置。

示例

```
sudo bash kics4net-backup.sh -b -p ./old_kics4net_data -t
```

该脚本将开始数据备份过程。等待 kics4net-backup.sh 脚本完成并保存创建的备份文件。

2 删除应用程序的先前版本

如果要将应用程序当前版本的组件安装到安装了先前版本的组件的同一节点，则必须执行此步骤。

如果当前版本的服务器或传感器安装在单独的计算机上（而不是托管先前版本组件的节点上），请将创建的备份文件复制到该计算机。

可以通过以下方式删除应用程序先前版本的组件：

- 集中在安装了先前版本的应用程序的所有节点上。

  此选项通过集中删除过程使用应用程序组件集中安装脚本。

- 在本地安装了应用程序先前版本的组件的每个节点上。

  此选项使用应用程序组件本地删除脚本（如果应用程序先前版本的组件提供本地安装和本地删除功能）。

删除应用程序先前版本的组件后，请确保计算机满足安装当前版本的硬件和软件要求。如有必要，请安装支持的操作系统版本并准备计算机上的硬件和软件。

3 安装当前版本的 Kaspersky Industrial CyberSecurity for Networks 并使应用程序部分准备好使用

在此步骤中，您需要安装 Kaspersky Industrial CyberSecurity for Networks 当前版本的组件。为此，您可以执行集中安装过程或使用应用程序组件本地安装脚本来安装组件。

安装组件后，需要完成以下步骤来部分准备应用程序以使其能够运行：

- 应用程序的初始配置
- 添加和连接探测器
- 添加监控点
- 添加应用程序用户

将监控点添加到与先前版本的应用程序中使用的相同网络接口时，建议将监控点命名为与先前版本的应用程序中的名称相同。这将使您在从备份加载数据时保留事件和新监控点之间的链接（否则，如果在新版本中找不到相同的名称，旧监控点的名称将在事件中标记为已删除）。

4 安装新版本应用程序后从备份加载数据

要从创建的备份文件下载数据，请在每台安装了应用程序组件的计算机上执行以下步骤：

1. 在安装了当前版本的应用程序组件的计算机上，进入 kics4net-backup.sh 脚本所在的目录。您可以转到在步骤 1 中打开的同一文件夹，也可以转到文件夹 /opt/kaspersky/kics4net/sbin/。
2. 运行 kics4net-backup.sh 脚本：
   - 要从服务器计算机上的备份副本下载数据，请输入以下命令：

     ```
     sudo bash kics4net-backup.sh -r -p <备份文件路径> <可选设置>
     ```

   - 要从传感器计算机上的备份副本下载数据，请输入以下命令：

     ```
     sudo bash kics4net-backup.sh -l -p <备份文件路径> <可选设置>
     ```

   其中：

   - `-r` 是一个允许从服务器备份文件读取和下载数据的设置（在服务器计算机上运行时为强制设置）。
   - `-p` 是指示备份文件的完整路径和名称的设置（必需设置）。
   - `-l` 是一个允许从传感器备份文件读取和下载数据的设置（在传感器计算机上运行时的强制设置）。
   - `<可选设置>` – `-d` 是停止应用程序服务的设置（如果未指定此设置，则应用程序服务将在脚本完成后启动）。

   脚本运行命令的一个可选设置是 `-f` 参数，该参数旨在从应用程序当前版本数据的备份副本中恢复所有可用的节点数据（如果在该场景的第 1 阶段已使用 `-f` 设置获得了备份副本）。但是，只有从保存数据的同一节点上的备份副本加载并处于同一应用程序版本（包含相同的版本号）时，才能完全恢复所有数据。

针对使用 kics4net-backup.sh 脚本的特定场景，提供了额外的运行命令设置 `--restore-database` 和 `--restore-clickhouse-database`。这些设置仅用于从备份文件恢复相应的服务器数据库。这些设置不适用于从应用程序的先前版本升级的情况。`-r` 设置（见上文）用于从服务器备份文件中读取和加载数据，包括用于恢复数据库的数据。

示例

```
sudo bash kics4net-backup.sh -r -p ./old_kics4net_data
```

该脚本将开始将数据从备份文件加载到应用程序中。等待 kics4net-backup.sh 脚本完成。从所有节点上的备份加载数据后，通过 Web 界面连接到服务器并检查“**设置→部署**”下的节点部署设置。如果需要的话添加 Sensor。

如果应用程序中恢复了连接器，请更新证书以连接它们。

安装带有补丁的更新的应用程序版本

在某些情况下，卡巴斯基专家可能会使用已应用的*补丁*来准备更新的应用程序文件。补丁用于添加或修复应用程序的功能（如果无法通过更新数据库和应用程序模块来应用此类更改）。

具有所应用的补丁的更新的应用程序文件(下文中也称为“更新的应用程序文件”)以类似于应用程序分发工具包中包括的存档的存档形式提供。

如果计算机上尚未安装应用程序组件，您可以使用包含更新的应用程序文件的存档来安装应用程序，这与分发工具包中的存档相同。为此，在准备应用程序安装时，请解压包含更新的应用程序文件的存档，而不是分发工具包中的存档。您可以执行所有其他操作来安装组件，其方式与使用分发工具包中的存档时相同。

如果计算机上已经安装了当前应用程序版本的组件，要使用补丁安装更新的应用程序文件，请使用补丁安装脚本 kics4net-install-patch.sh。kics4net-install-patch.sh 脚本允许您将已安装的当前版本的应用程序组件替换为更新版本的应用程序组件，并迁移当前应用程序版本积累的数据。如果替换已安装组件时发生错误，脚本将回滚更新的应用程序文件的安装，并将应用程序返回到脚本运行时的状态。

当使用更新版本的应用程序组件替换已安装的当前版本的应用程序组件时，kics4net-install-patch.sh 脚本允许您传输以下累积数据：

- 安全策略
- 有关技术和方法的状态和/或操作模式的数据
- 用于更新应用程序模块和数据库的设置
- 有关添加的授权许可密钥的信息
- 审计条目
- 应用程序消息
- 漏洞风险
- 注册的活动
- 为事件保存的流量
- 网络地图数据，包括已保存协议属性的网络会话
- 流量转储文件
- 节点部署设置，包括监控点设置和节点上的数据存储设置

- 程序使用者列表
- 连接器设置
- 连接器类型设置
- 连接服务器参数
- 与 Kaspersky Security Center 的交互设置
- 有关已安装的数据库和应用程序模块更新的数据
- 节点上运行的进程的日志记录级别
- 实时系统监控小部件的设置

kics4net-install-patch.sh 脚本包含在应用程序分发工具包中，并且与更新的应用程序文件一起位于存档中。

您可以使用 kics4net-install-patch.sh 脚本安装当前版本或任何 4.1 及更高版本的更新应用程序文件，前提是更新的应用程序文件与已安装的操作系统和 Kaspersky Industrial CyberSecurity for Networks 版本兼容。

kics4net-install-patch.sh 脚本将更新的应用程序文件本地安装在运行该脚本的计算机上。因此，要更新所有应用程序组件（服务器和传感器），请在每台已安装应用程序组件的计算机上按顺序运行 kics4net-install-patch.sh 脚本。可以按任何顺序更新组件：您可以首先更新服务器计算机上的应用程序文件，然后更新传感器计算机上的应用程序文件，反之亦然。

要在安装了 Kaspersky Industrial CyberSecurity for Networks 服务器或传感器的计算机上安装更新的应用程序文件：

1. 准备目录来存储上次用于安装组件或上次用于更新应用程序文件的存档中的旧文件。

   如果计算机上已存在旧的解压文件目录（例如，本地安装组件后未删除该目录），则可以使用该目录进行进一步操作。如果没有该目录，请执行以下操作来准备它：

   a. 将上次用于安装组件或更新应用程序文件的存档复制到您选择的目录。

   b. 转到包含复制档案的文件夹并输入以下命令来解压它：

   ```
   tar -zxvf <存档文件名>
   ```

   解压后的目录和文件出现在一个子目录中，该子目录的名称与存档文件的名称相匹配。

   在进一步操作的描述中，这个准备好的目录被称为*具有旧文件的目录*。

2. 准备目录来存储收到的存档中的新解压文件以及更新的应用程序文件。

   要准备目录：

   a. 将包含更新的应用程序文件的存档复制到您的计算机。

   b. 转到包含复制档案的文件夹并输入以下命令来解压它：

   ```
   tar -zxvf <存档文件名>
   ```

   解压后的目录和文件出现在一个子目录中，该子目录的名称与存档文件的名称相匹配。

在进一步操作的描述中，这个准备好的目录被称为*具有新文件的目录*。

3. 在包含新文件的目录中，转到 <存档文件名>/linux-centos 子目录。该目录包含用于安装、验证和删除应用程序组件的脚本和包文件。

4. 运行 kics4net-install-patch.sh 脚本：

   - 要在服务器计算机上安装更新的应用程序文件，请输入以下命令：

     ```
     sudo bash kics4net-install-patch.sh -o <包含旧文件的目录的路径>/linux-centos -n <包含新文件的目录的路径>/linux-centos -b <备份副本的目录的路径> --backup-traffic
     ```

   - 要在传感器计算机上安装更新的应用程序文件，请输入以下命令：

     ```
     sudo bash kics4net-install-patch.sh -s -o <包含旧文件的目录的路径>/linux-centos -n <包含新文件的目录的路径>/linux-centos -b <备份副本的目录的路径> --backup-traffic
     ```

   其中：

   - `-o` 是一个参数，指定包含脚本和包文件的目录的完整路径，用于安装、验证和删除具有旧文件的目录中的应用程序组件（强制参数）。

   - `-n` 是一个参数，指定包含脚本和包文件的目录的完整路径，用于安装、验证和删除具有新文件的目录中的应用程序组件（强制参数）。

   - `-b` 是一个参数，指定用于创建备份副本的目录的完整路径（默认情况下，脚本会在临时目录中创建备份副本，并在更新的应用程序文件安装成功，或由于脚本操作期间出现错误而安装被回滚时自动删除创建的文件）。

     建议使用此参数将备份副本保存在正确的目录中，无论 kics4net-install-patch.sh 脚本执行结果如何。如果应用程序中积累了大量数据，请使用 `-b` 参数指定不同硬盘上的挂载目录，避免系统（根）分区溢出。

   - `--backup-traffic` 是一个参数，用于将流量转储文件添加到备份中，并在安装更新的应用程序文件后进一步恢复这些文件。默认情况下，流量转储文件不会复制到备份目录；这些文件保留在其原始位置，并且在安装成功后可用。此参数允许您在因 kics4net-install-patch.sh 脚本执行错误而导致更新的应用程序文件安装回滚的情况下自动恢复流量转储文件。

     如果您想保存流量转储文件并且在安装更新的应用程序文件期间存在出错的风险，建议使用此参数。通常，应用程序存储流量转储文件的目录需要大量磁盘空间。使用 `--backup-traffic` 参数时，kics4net-install-patch.sh 脚本会将这些文件复制到备份目录，这可能需要大量额外的磁盘空间。此外，脚本运行时间可能会显着增加。

   - `-s` 是用于启用安装更新的传感器文件的参数；当 kics4net-install-patch.sh 脚本在传感器计算机上运行时应用。

   示例

   ```
   sudo bash kics4net-install-patch.sh -o /tmp/kics4net-release_<应用程序版本号>/linux-centos -n /tmp/kics4net-patch1_<应用程序版本号>/linux-centos -b ./old_kics4net_data --backup-traffic
   ```

该脚本开始安装更新的应用程序文件。等待 kics4net-install-patch.sh 脚本完成。

要查看服务器上的应用程序版本并在安装更新的文件后开始使用该应用程序：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks Server。使用服务器计算机的 IP 地址进行连接。

2. 选择“**关于**”并查看服务器上安装的应用程序的版本。

3. 选择“**启动配置**”。

4. 请阅读最终用户授权许可协议和隐私策略的条款。为此，请单击以下复选框名称中的相应链接打开每个文档：**我确认我已完全阅读、理解并接受本协议的条款和条件**本**最终用户授权许可协议**，并且**我了解并同意我的数据将按照本协议中的描述进行处理和传输（包括传输到第三国）**我的数据将按照**隐私策略。我确认我已完全阅读并理解本协议的条款隐私策略**的条款：

5. 如果您完全同意最终用户授权许可协议和隐私策略的条款，请选中两个复选框。

   如果您不同意最终用户授权许可协议和/或隐私策略的条款，请关闭 Web 界面页面并从计算机中删除已安装的应用程序组件。

6. 单击“**继续**”。

启动和停止应用程序

当加载计算机的操作系统时，安装在计算机上的应用程序的组件会自动启动。必须配置应用程序组件才能使其正常工作。当应用程序准备运行时，组件就被配置。

如果该应用程序通过监控点接收流量，则执行工业网络流量分析功能。您可以禁用或启用监控点以暂停或恢复对这些监控点接收的流量的分析。

如果在安装了 Kaspersky Industrial CyberSecurity for Networks 组件的节点上添加了集成服务器，则这些节点会接收并处理来自 EPP 应用程序的数据。您可以禁用和启用集成服务器以分别暂停和恢复从 EPP 应用程序接收数据。

应用程序允许您执行设备的主动轮询，作为主动轮询作业和配置控制作业的一部分。主动轮询是使用连接器执行的，它允许您获取有关设备的各种信息，包括用于生成拓扑图的信息。您可以启用和禁用连接器以暂停和恢复通过这些连接器发送和接收数据。

要管理应用程序的操作并查看信息，您可以通过 Web 界面连接到服务器。当您完成服务器的工作后，建议您正确终止连接会话。

要配置探测器和服务器之间的连接并查看有关连接状态的信息，您可以通过 Web 界面连接到探测器。连接到探测器时，您无需输入用户账户凭据。因此，您不需要执行任何操作来终止连接会话。

通过 Web 界面连接服务器

您可以使用任何受支持的浏览器通过 Web 界面连接到服务器。您可以从任何具有网络访问权限的计算机连接到托管 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机。

要连接到 Kaspersky Industrial CyberSecurity for Networks 服务器：

1. 打开浏览器并在地址栏中输入以下内容：
   `https://<Server name>:<port>`
   其中：
   - `<Server name>` 是服务器计算机上的 Web 服务器使用的 IP 地址或计算机名称。
   - `<port>` 是为 Web 服务器指定的端口号。

   如果未指定端口号（在应用程序启动配置之前）或者为 Web 服务器指定了默认端口号（443），则只需在地址栏中输入服务器的 IP 地址或计算机名称。在这种情况下，HTTPS 协议和端口号将被自动确定。

2. 当账户凭证输入页面打开时，输入应用程序用户名和密码，然后单击**登录**。

   输入用户名和密码时请小心。如果用户密码连续多次输入错误，具有管理员角色的用户将在 Web 界面收到通知。随后反复尝试输入无效密码可能会触发 30 分钟的自动锁定，从而阻止通过 Web 界面连接到服务器。

   如果管理员在账户创建后用户第一次连接到应用程序时和/或管理员更改密码后启用了账户的强制密码更改，则账户凭据输入页面上将显示“**新密码**和**重新输入新密码**”字段，以更改应用程序用户的密码。

3. 当出现更改应用程序用户密码的字段时，输入新的密码并单击“**登录**”按钮。

   新的密码必须满足账户凭据输入页面上列出的条件。当您输入密码时，您所满足的条件会被自动标记。

   在连接应用程序时正确输入用户名和密码或更改用户密码后，Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面页面将在您的浏览器窗口中打开。Web 界面页面的浏览器书签名称将显示安装后在应用程序启动配置期间定义的服务器名称。

服务器连接会话有时间限制。默认情况下，会话保持打开状态 10 小时（如有必要，您可以通过运行 kics4net-params 脚本来更改会话时间限制）。如果自连接建立以来已超过 10 小时，应用程序 Web 界面的当前页面将切换到输入账户凭据的页面。如果发生这种情况，若要继续工作，您需要重新输入应用程序用户名和密码。

通过 Web 界面终止服务器连接会话

当您通过 Web 界面完成使用 Kaspersky Industrial CyberSecurity for Networks 服务器后，请确保关闭浏览器中的连接会话。

如果您关闭浏览器窗口但没有先结束连接会话，会话将保持活动状态。默认情况下，会话保持活动状态 10 小时。在此期间，只要该连接由同一台计算机、浏览器和操作系统帐户使用，应用程序就可以授予对 Kaspersky Industrial CyberSecurity for Networks 服务器的 Web 界面的访问权限，而无需提示出具用户帐户凭据。如有必要，您可以通过运行 kics4net-params 脚本来更改会话时间限制。

要关闭与 Kaspersky Industrial CyberSecurity for Networks 服务器的连接会话：

1. 在 Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面页面上，打开用户菜单：
   - 如果菜单折叠，请单击按钮。
   - 如果菜单展开，请单击当前用户姓名右侧的按钮。
2. 在用户菜单中，选择**登出**。

   浏览器窗口将显示输入帐户凭据的页面。

通过 Web 界面连接到传感器

当您通过 Web 界面连接到探测器时，可以在探测器 Web 界面页面上执行以下操作：

- 下载通信数据包到探测器，用于连接 Kaspersky Industrial CyberSecurity for Networks 服务器。
- 如果探测器通过网络自动连接到服务器，查看证书签名请求的指纹，并将其与服务器 Web 界面页面上的指纹进行比较。
- 查看探测器与服务器之间的连接状态信息。

要更改探测器设置，管理监控点和技术以及监控节点的状态，通过 Web 界面连接到应用程序服务器。

您可以使用任何受支持的浏览器通过 Web 界面连接到服务器。可以从通过网络访问探测器计算机的计算机建立此连接。

要连接到 Kaspersky Industrial CyberSecurity for Networks 探测器：

打开浏览器并在地址栏中输入以下内容：
`https://<探测器名称>:<端口>`

其中：

- <探测器名称>是探测器的 Web 服务器使用的探测器计算机的 IP 地址或名称。
- <端口>是探测器的 Web 服务器使用的端口号。

如果探测器 Web 服务器使用默认端口号 (443)，则只需在地址栏中输入探测器的 IP 地址或计算机名称。在这种情况下，HTTPS 协议和端口号将被自动确定。

Kaspersky Industrial CyberSecurity for Networks 探测器 Web 界面页面将在浏览器窗口中打开。Web 界面页面的浏览器选项卡显示添加探测器时定义的探测器名称。

应用程序界面

本节介绍应用程序的主要界面元素。

您可以通过 Web 界面连接到应用程序组件（服务器和 Sensor）。连接时必须使用受支持的浏览器。连接到应用程序组件后，浏览器窗口会加载一个包含界面元素的页面。您看到的具体界面元素取决于您连接的组件、该组件的特定状态以及其他因素。

在 Kaspersky Industrial CyberSecurity for Networks 服务器的 Web 界面页面上，界面元素分为不同的功能部分。这些部分用于配置应用程序、管理其运行以及查看数据。您可以使用 Web 界面的菜单选择相关部分。可供选择的部分数量取决于应用程序模式和用户账户的角色。

在 Kaspersky Industrial CyberSecurity for Networks Sensor 的 Web 界面页面上，始终只使用两个部分来分组界面元素。在这些部分中，您可以获取有关 Sensor 和服务器之间连接的信息，并查看有关应用程序的简要信息。

关于 Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面

当您通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器时，服务器 Web 界面页面会在您的浏览器中打开。Web 界面页面的内容取决于应用程序的运行模式和所连接的用户帐户的具体角色。

根据应用程序的操作模式，Web 界面页面可能包含以下管理元素或消息：

- 应用程序的启动配置模式 – 用于安装后配置服务器以及查看和接受最终用户授权许可协议和隐私策略的管理元素。
- 应用程序的正常运行模式 – 用于配置和利用应用程序功能的管理元素。
- 应用程序维护 – 有关在服务器可供连接之前必须完成的操作的消息。

当应用程序在正常运行模式下运行时，其在 Web 界面页面上可用的功能取决于所连接的用户帐户的角色。如果用户角色没有授予使用应用程序管理功能的权限，则相应的管理元素不会显示在 Web 界面页面上或不可用。

关于 Kaspersky Industrial CyberSecurity for Networks Sensor Web 界面

当您通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 探测器时，探测器 Web 界面页面会在您的浏览器中打开。Web 界面页面的内容取决于探测器和应用程序服务器之间的连接状态。

根据探测器和应用程序服务器之间的连接状态，Web 界面页面可能包含以下管理元素或数据：

- 在将传感器连接到服务器之前——管理元素，用于选择通信数据包和/或数据，以便通过网络自动连接传感器。
- 将传感器连接到服务器后——服务器和传感器上的数据（包括转到服务器 Web 界面页面的能力）以及连接状态。

应用程序启动配置期间的服务器 Web 界面菜单

安装应用程序后首次通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器时，系统不会提示您输入用户账户凭据进行登录。您看到的不是账户凭据输入页面，而是包含用于配置服务器以及查看和接受最终用户授权许可协议和隐私策略的管理元素的页面。

菜单显示在 Web 界面页面的左侧。所选部分的内容显示在右侧。

Web 界面菜单包含以下项目：

- – 展开和折叠菜单。如果菜单折叠，则显示的项目不带文字描述。
- – 打开“**启动配置**”部分。
- – 打开包含有关该应用程序的简要信息的部分。

应用程序正常操作期间的服务器 Web 界面菜单

当应用程序以正常运行模式运行时，通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器后，将打开一个 Web 界面页面，提供使用该应用程序的工具。可用的工具及其功能取决于建立与服务器连接的用户的角色。

菜单显示在 Web 界面页面的左侧。所选部分的内容显示在右侧。

Web 界面菜单包含以下项目：

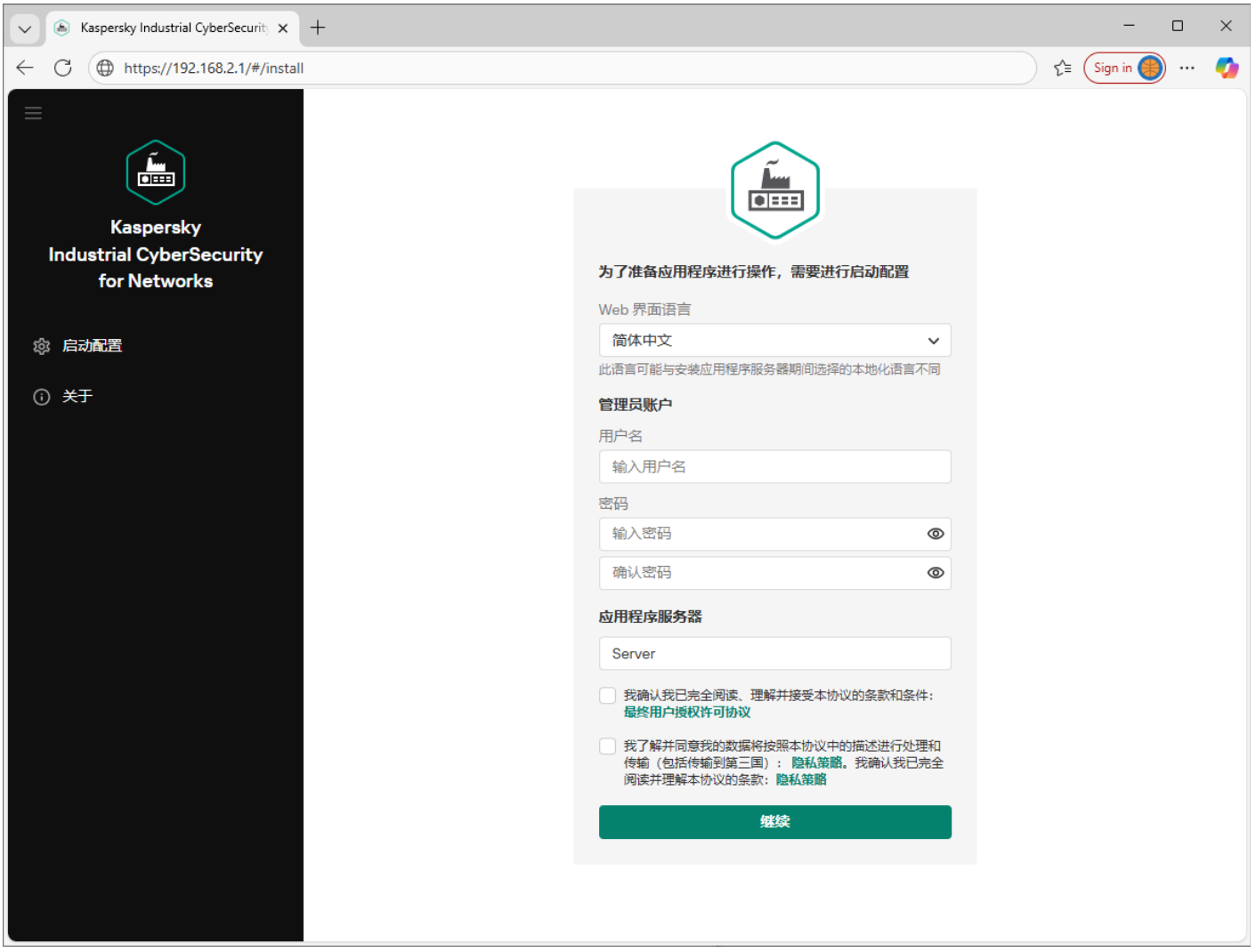
- – 展开和折叠菜单。如果菜单折叠，则显示的项目不带文字描述。
- – 打开有关应用程序操作问题的通知列表。通知的可用性由图标指示，图标的颜色与通知的状态相对应。
- – 打开后台操作列表。此列表包含有关需要很长时间的操作的信息（例如，在导出大量事件时创建文件）。活动后台操作的数量及其进度状态通过图标表示。如果有操作导致错误，则图标为红色。
- – 打开“**控制板**”部分。
- – 打开“**资产**”部分。
- – 打开“**网络地图**”部分。
- – 打开“**事件**”部分。
- – 打开“**报告**”部分。
- – 打开“**过程控制**”部分。
- – 打开“**允许规则**”部分。
- – 打开“**检测规则**”部分。
- – 打开“**风险**”部分。

- – 打开“**安全审计**”部分。
- – 打开**设置**部分。
- – 打开包含有关该应用程序的简要信息的部分。
- – 如果某些应用程序功能被禁用或者功能启用了学习模式，则显示。当菜单最大化时，会显示“**不是所有保护服务都在运行**”通知。单击此图标或文本将打开一个窗口，其中包含有关禁用的保护功能的信息。
- **连接服务器** – 显示建立连接的服务器的名称（安装后应用程序启动配置期间定义的名称）。
- – 打开或关闭用户菜单（如果菜单折叠）。如果菜单展开，您将在附近看到当前用户的名称及其角色（在这种情况下，您可以使用右侧的按钮打开和关闭用户菜单）。用户菜单由以下部分组成：
  - **语言** – 让您选择应用程序 Web 界面的语言。

    应用程序 Web 界面所选的本地化语言不会影响 Kaspersky Industrial CyberSecurity for Networks 服务器的本地化语言。该组件使用在安装或重新安装 Kaspersky Industrial CyberSecurity for Networks 期间定义的本地化语言。因此，服务器提供的数据的本地化语言可能与 Web 界面选择的本地化语言不同。例如，从服务器收到的事件和消息（包括一些错误消息）以服务器的本地化语言显示。
  - **主题** – 允许您选择 Web 界面页面的颜色设计主题：
    - **浅色** – 对象显示在白色背景上。
    - **深色** – 对象显示在深色背景上。
  - **用户账户**–对使用当前用户账户执行操作的菜单项进行分组：
    - **更改密码** – 打开更改当前用户密码的窗口。
    - **登出** – 结束服务器连接会话并打开输入账户凭据进行连接的页面。
  - **附加信息** – 包含转到 Kaspersky Industrial CyberSecurity for Networks 在线帮助页面的**帮助**选项。

“初始配置”部分

在服务器 Web 界面的“**启动配置**”部分（见下图），您可以指定安装后启动应用程序所需的主要应用程序服务器设置。

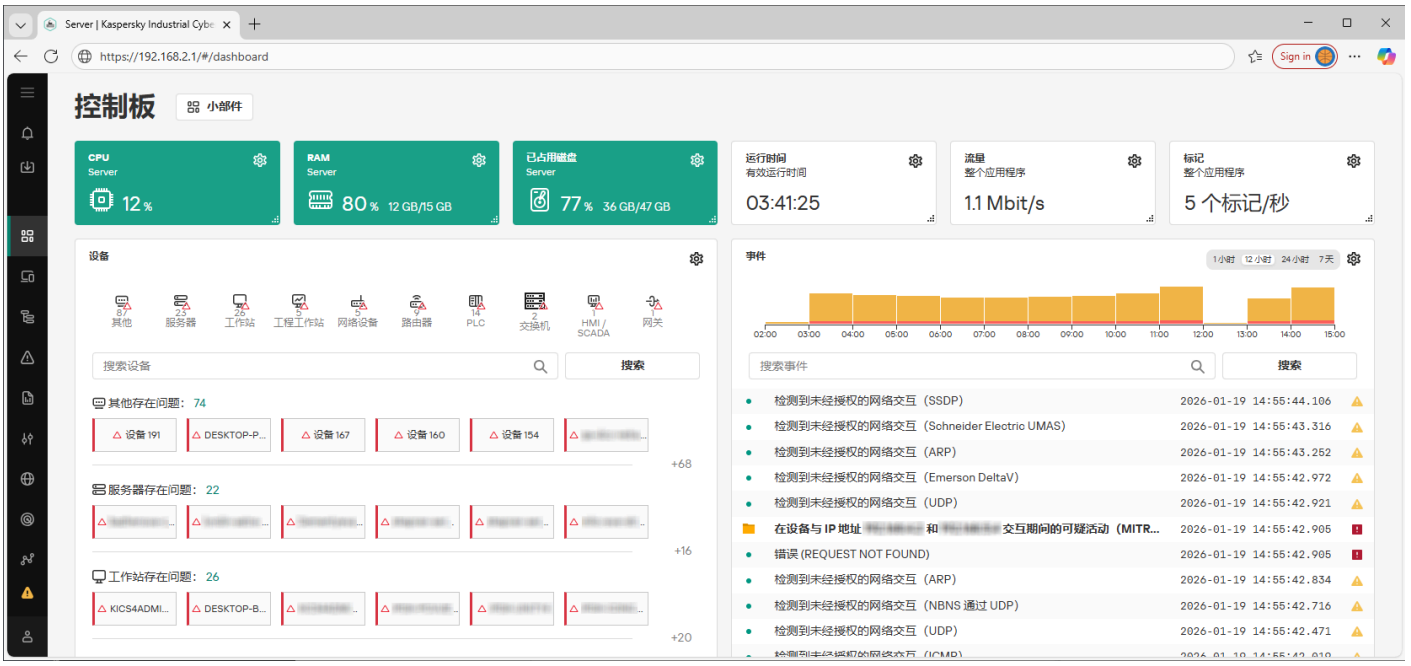


“**启动配置**”部分

此部分包含一个窗口，您可以使用它来配置服务器的主要设置，创建具有管理员角色的第一个用户，并仔细阅读并接受最终用户授权许可协议和隐私策略的条款。完成这些操作后，此 Web 界面页面将自动关闭（与通过 Web 界面进行的其他服务器连接会话一起），并且您将进入应用程序正常运行模式的服务器 Web 界面页面。

“控制板”部分

在应用程序服务器 Web 界面的“**控制板**”部分（见下图），您可以在离线模式查看有关系统当前状态的信息。



“**控制板**”部分

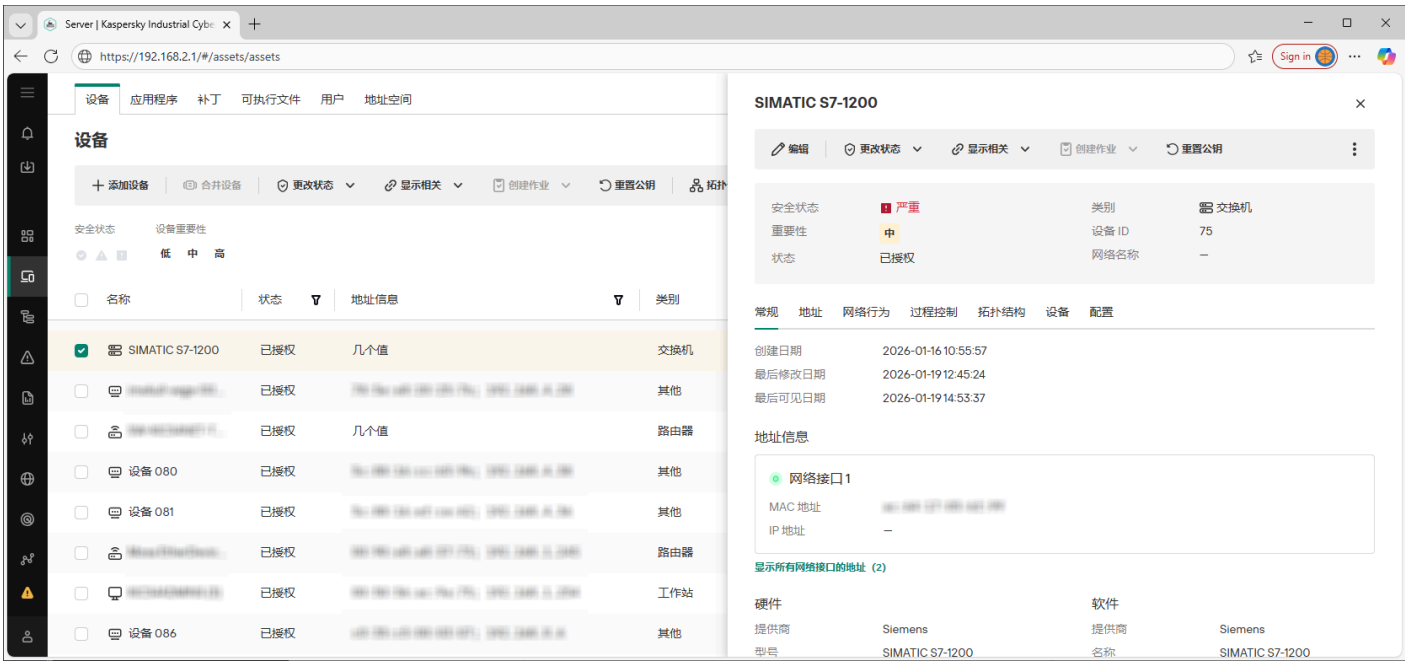
您可以观看教程视频（见下方）来熟悉其功能。

https://www.youtube.com/watch?v=zxP9OniGjkM

控制板概览

“资产”部分

在应用程序服务器 Web 界面的“**资产**”部分（见下图），您可以查看和编辑有关设备和其主对象的信息以及设备地址空间的设置。



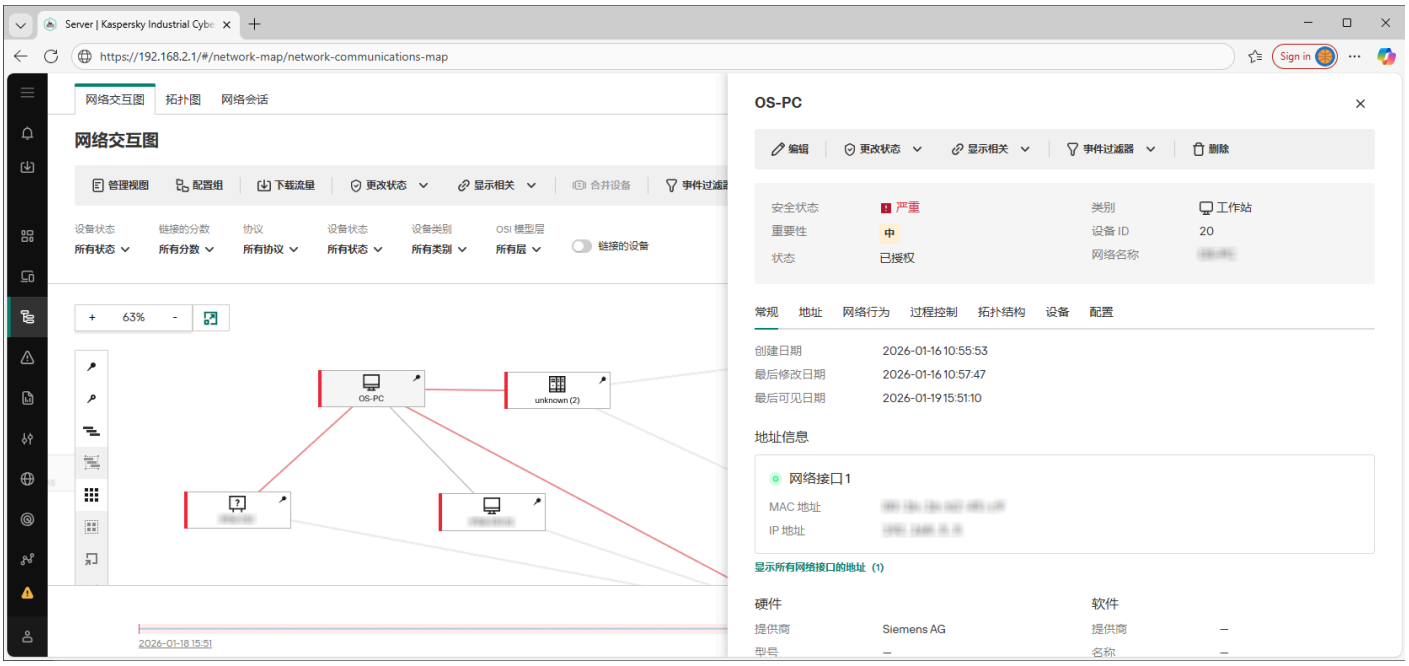
“**资产**”部分

“**资产**”部分包含一个带有设备表的选项卡、带有设备上主要对象（应用程序、补丁、可执行文件和用户）表的选项卡以及一个带有地址空间信息的选项卡。

选择资产后，详细信息区域将在该部分的右侧打开。当选择一个地址空间时，将打开一个块，其中包含有关其规则和子网的信息。选择设备或子网后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选对象及其管理工具的信息。

“网络地图”部分

在应用程序服务器 Web 界面的“**网络地图**”部分（见下图），您可以查看网络图上和网络会话表中的交互信息，以及生成拓扑图。



“**网络地图**”部分

“**网络地图**”部分包含网络交互图、拓扑图和网络会话表的选项卡。网络交互图和拓扑图的选项卡包含上部的主工具栏、用于显示网络地图上的对象的区域以及用于管理对象位置的附加工具栏。“**网络交互图**”选项卡的下部包含按时间段过滤对象的时间尺度。

选择对象后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选对象及其管理工具的信息。

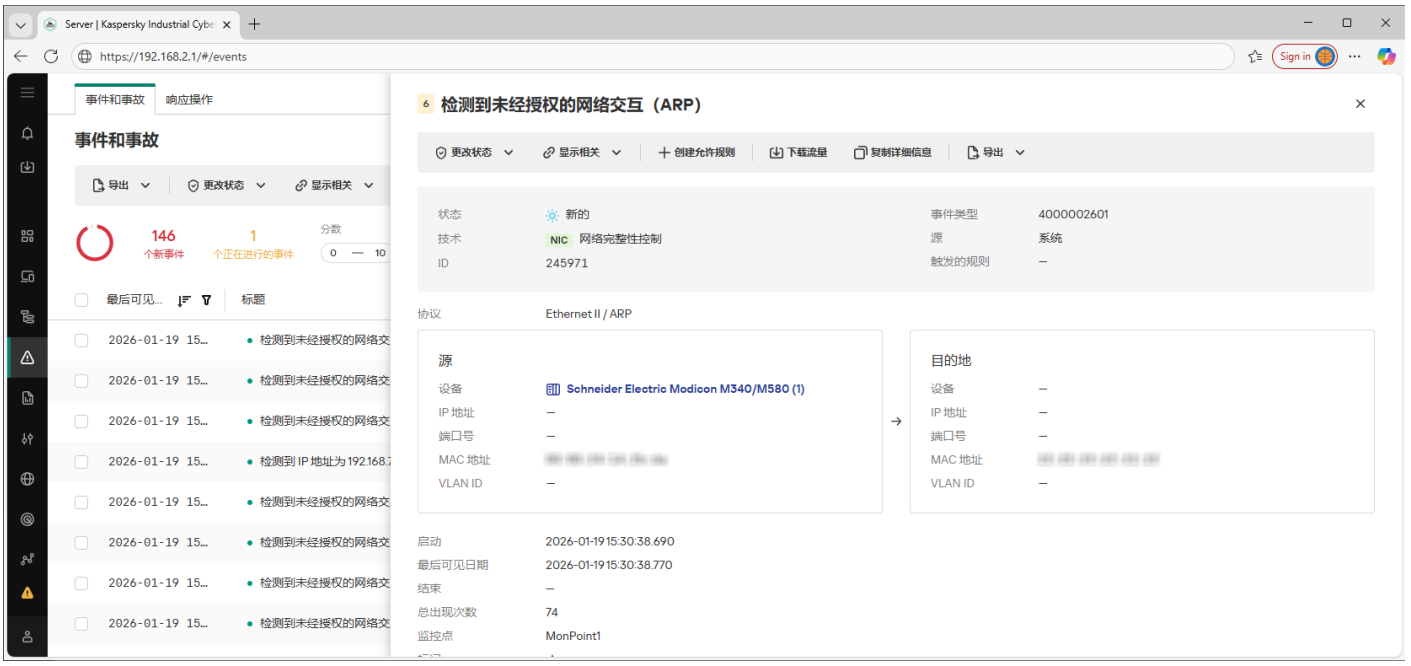
您可以观看教程视频（见下方）来熟悉其功能。

https://www.youtube.com/watch?v=5uPjUMi5Qjo

网络清单

“事件”部分

在应用程序服务器 Web 界面的“**事件**”部分（见下图），您可以查看和处理事件和事故，并管理威胁响应操作。



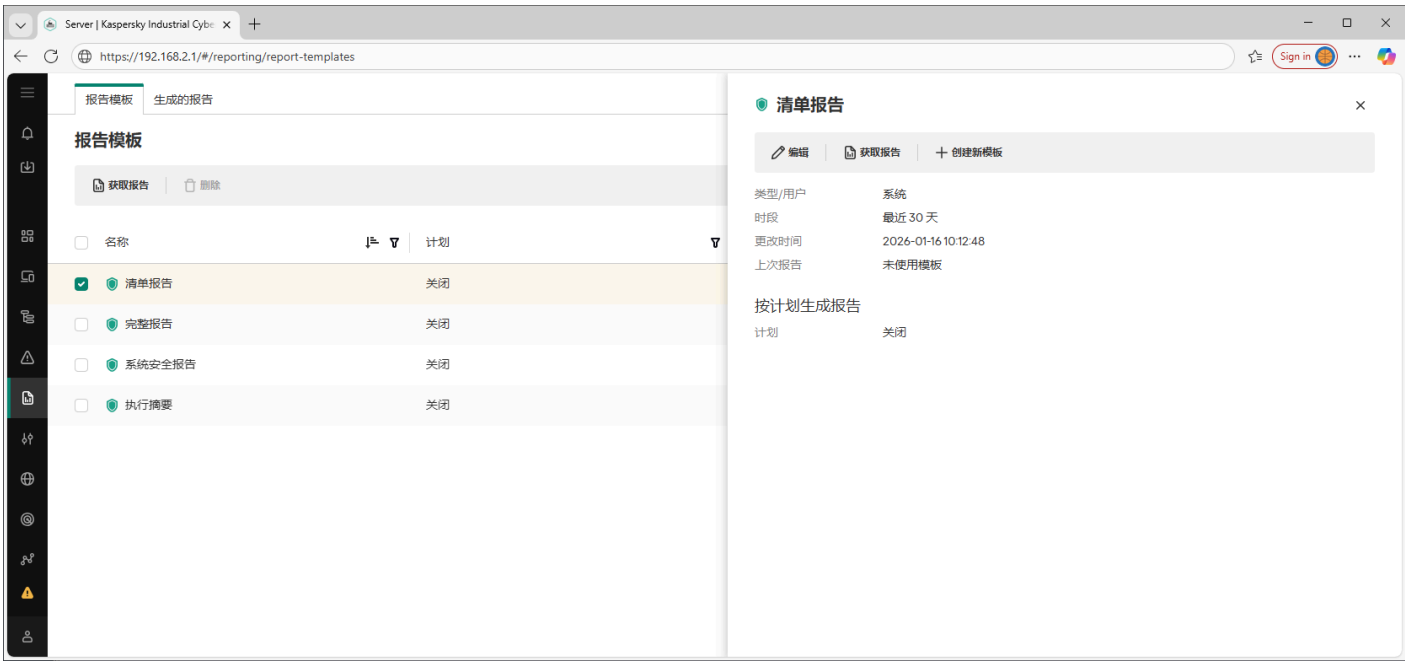
“**事件**”部分

“**事件**”部分包含事件表和响应操作表的选项卡。

选择事件或操作后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选对象及其管理工具的信息。

“报告”部分

在应用程序服务器 Web 界面的“**报告**”部分（见下图），您可以查看生成的报告和报告模板，以及管理报告和报告模板。



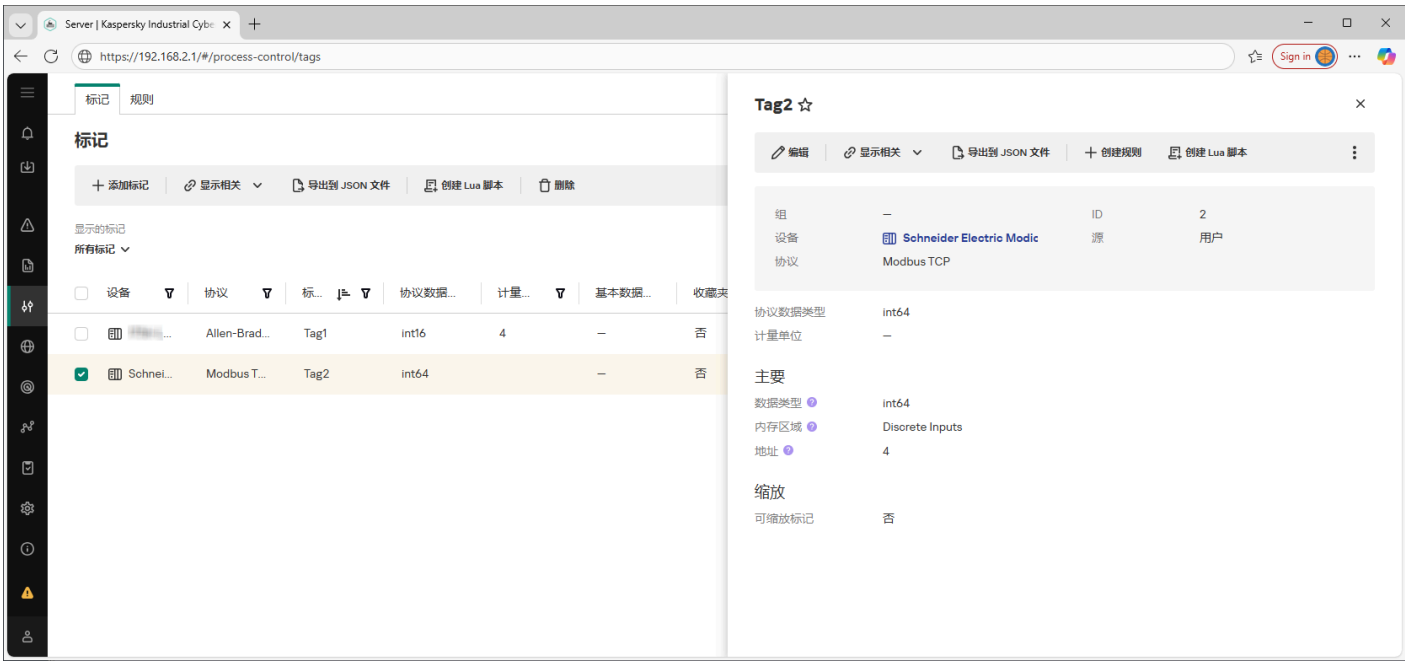
“**报告**”部分

“**报告**”部分包含报告模板表和生成的报告的选项卡。

选择报告模板或生成的报告后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选对象及其管理工具的信息。

“过程控制”部分

在应用程序服务器 Web 界面的“**过程控制**”部分（见下图），您可以查看工业过程参数（标签）的值，以及配置过程控制的标签和规则。



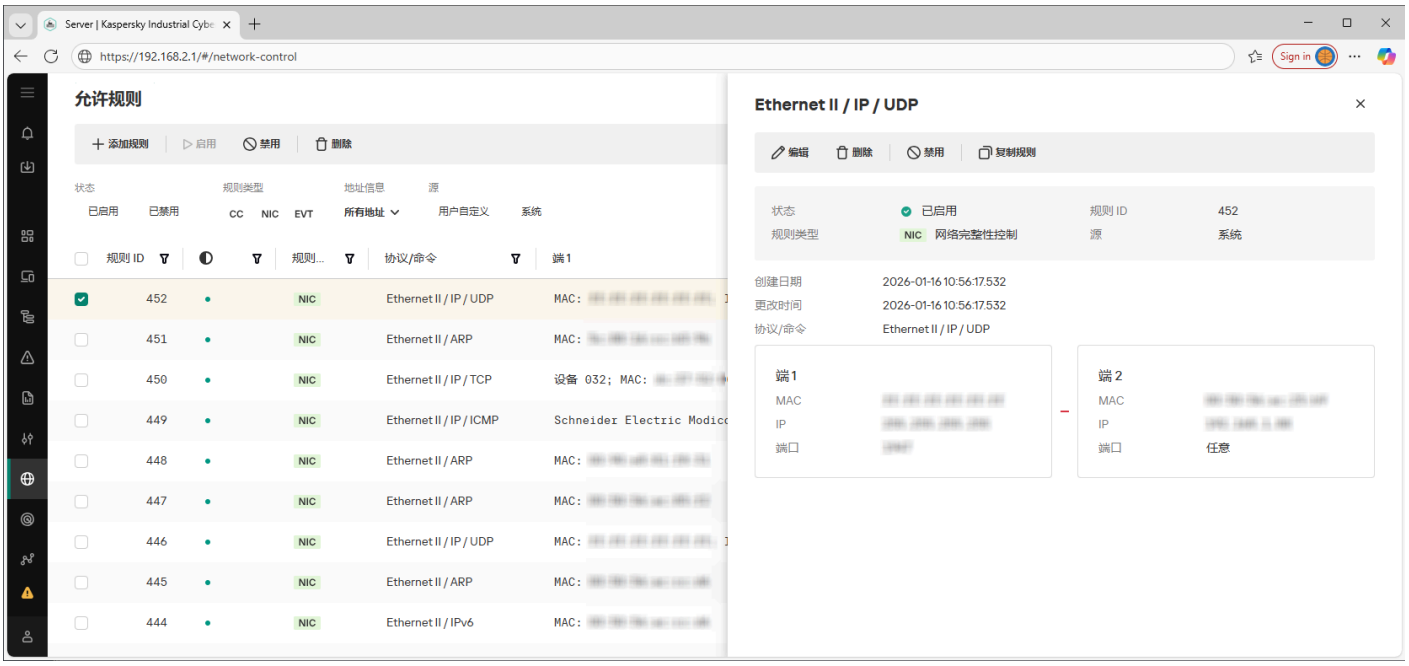
“**过程控制**”部分

“**过程控制**”部分包含标签表和过程控制规则的选项卡。

选择标签或规则后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选对象及其管理工具的信息。

“允许规则”部分

在应用程序服务器 Web 界面的“**允许规则**”部分（见下图），您可以查看和编辑网络交互和事件的允许规则。



“**允许规则**”部分

“**允许规则**”部分包含允许规则表。

选择一条规则后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选规则及其管理工具的信息。

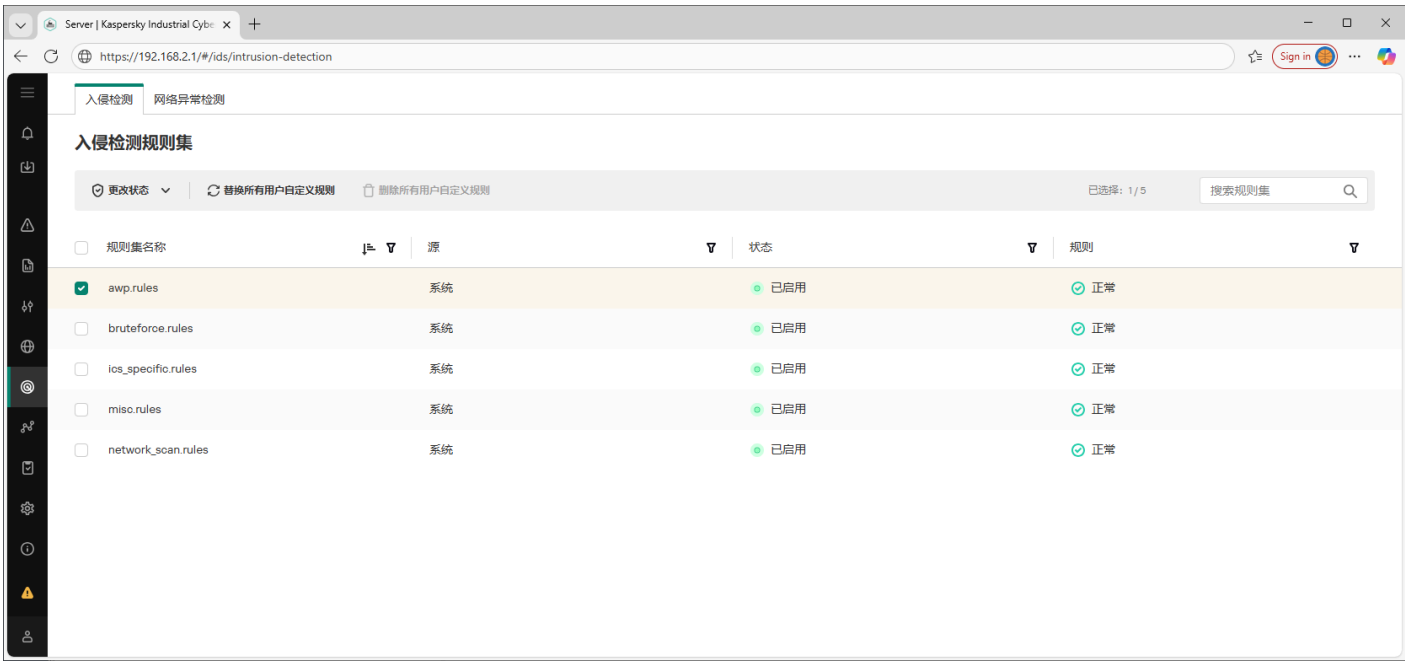
您可以观看教程视频（见下方）来熟悉其功能。

https://www.youtube.com/watch?v=bluRipsZtO8

工业协议深度包检测

“检测规则”部分

在应用程序服务器 Web 界面的“**检测规则**”部分（见下图），您可以管理入侵检测和网络异常检测规则集。



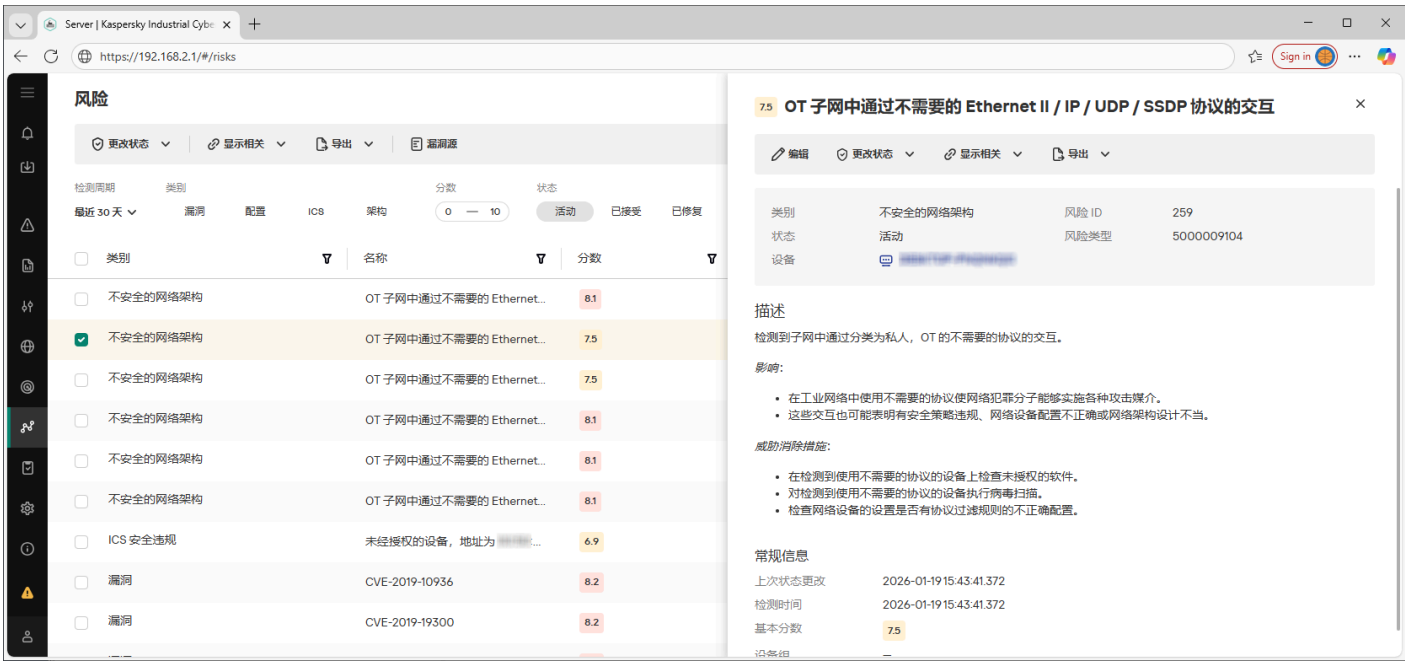
“**检测规则**”部分

检测规则部分包含多个选项卡，每个选项卡包含多个表格，显示入侵检测规则集和网络异常检测规则集。

当您在网络异常检测规则表中选择一条规则时，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选对象及其管理工具的信息。

“风险”部分

在应用程序服务器 Web 界面的“**风险**”部分（见下图），您可以查看和处理应用程序检测到的风险。



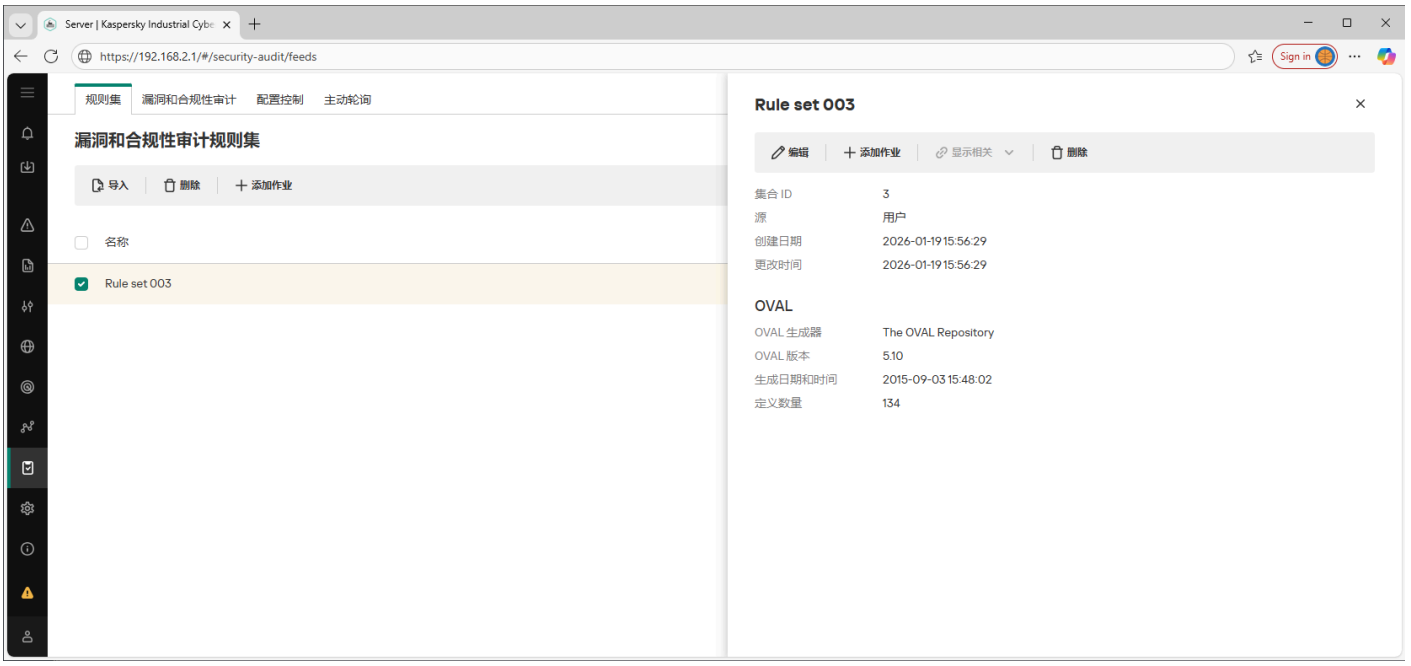
“**风险**”部分

“**风险**”部分包含风险表。

选择风险后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选风险及其管理工具的信息。

“安全审计”部分

在应用程序服务器 Web 界面的“**安全审计**”部分（见下图），您可以管理安全审计作业和漏洞和合规性审计作业规则集。



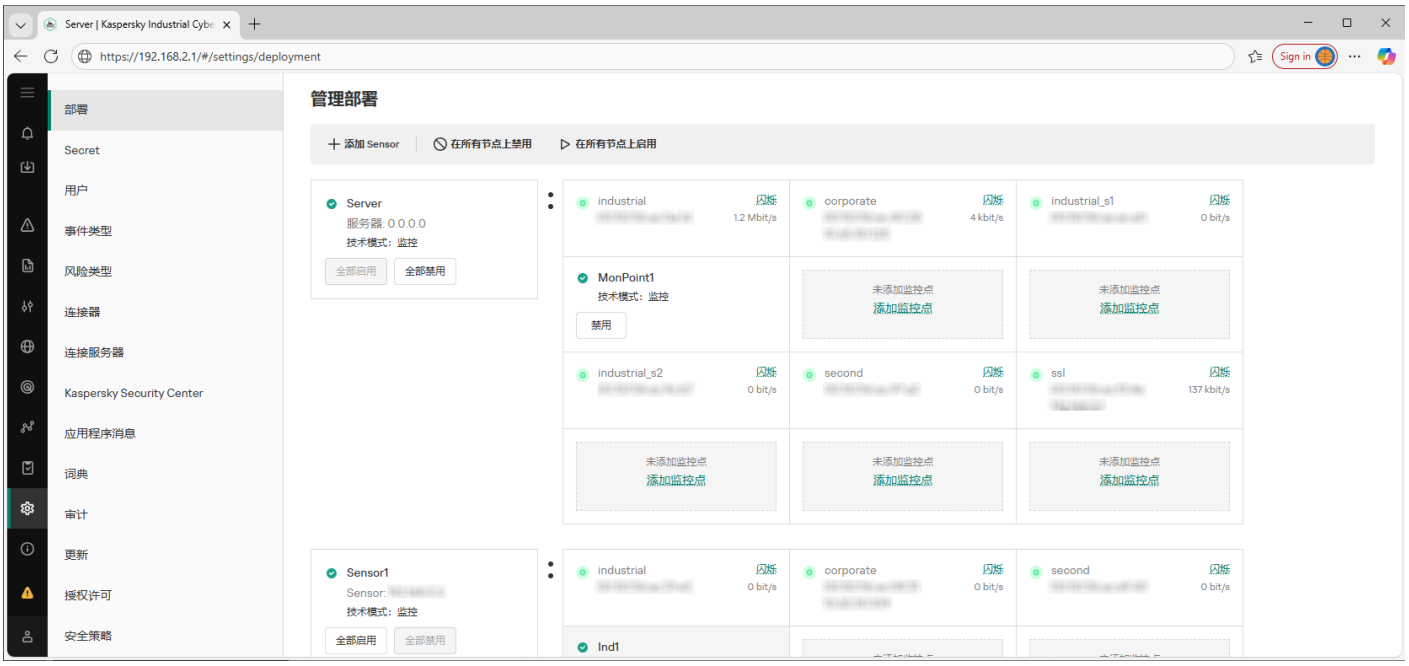
“**安全审计**”部分

“**安全审计**”部分包含带有各种类型的规则集和作业表的选项卡。

选择一个规则集或作业后，详细信息区域将在该部分的右侧打开。详细信息区域包含有关所选对象及其管理工具的信息。

“设置”区域

在应用程序服务器 Web 界面的“**设置**”部分（见下图），您可以查看和编辑应用程序设置。



“**设置**”部分

当您选择**设置**部分时，Web 界面页面上会出现一个附加菜单。在此菜单中，您可以转到以下子部分：

- **部署**。

  在本部分中，您可以查看已安装应用程序组件的节点信息，以及节点上的监控点信息。如果使用管理员账户连接到服务器，您也可以在此部分管理部署设置。

- **Secret**。

  在本节中，您可以管理包含用于远程连接的账户凭据的 Secret。如果使用除操作员角色之外的任何角色的账户建立与服务器的连接，则会显示**Secret**部分。

- **用户**。

  在本部分中，您可以管理应用程序用户账户。如果使用管理员账户连接到服务器，则会显示“**用户**”部分。

- **事件类型**。

  在本部分中，您可以查看和编辑事件类型的设置。

- **风险类型**。

  在本部分中，您可以查看和编辑风险类型的设置。

- **连接器**。

  在本部分中，您可以管理应用程序的连接器。

- **连接服务器**。

  在本部分中，您可以查看和编辑托管应用程序服务器的计算机上的 Web 服务器的设置（例如，用受信任证书替换当前证书）、REST API 服务器设置和节点上的集成服务器设置。

- **Kaspersky Security Center**。

  在本部分中，您可以查看和编辑与 Kaspersky Security Center 交互的设置。

- **应用程序消息**。

  在本部分中，您可以查看应用程序消息。

- **词典**。

  在本节中，您可以管理网络异常检测规则的字典。

- **审计**。

  在本节中，您可以查看审核日志条目。如果使用具有管理员角色的用户账户连接到服务器，则会显示“**审计**”部分。

- **更新**。

  在本部分中，您可以配置和运行应用程序模块和数据库的更新。如果使用管理员账户连接到服务器，则会显示“**更新**”部分。

- **授权许可**。

  在本部分中，您可以管理应用程序的授权许可密钥。

- **安全策略**。

  在本部分中，您可以管理应用程序安全策略。

- **日志记录**。

  在本部分中，您可以配置进程日志的日志记录级别。

许可应用程序

本节包含有关 Kaspersky Industrial CyberSecurity for Networks 授权许可的信息。

关于最终用户授权许可协议

*最终用户授权许可协议*是您和 AO Kaspersky Lab 之间的绑定协议，规定了您使用该应用程序的条款。

在开始使用该应用程序之前，请仔细阅读并接受最终用户授权许可协议的条款。

您可以通过以下方式查看最终用户授权许可协议的条款：

- 在应用程序的启动配置期间。
- 通过打开 license_en.txt，它是应用程序分发工具包的一部分（该文档的副本也保存在应用程序安装文件夹中）。

在应用程序的启动配置期间阅读并接受最终用户授权许可协议的条款。如果不接受最终用户授权许可协议的条款，您必须取消应用程序的启动配置，不得使用该应用程序。

关于隐私政策

*隐私政策*是一个告知您您的数据将被如何处理的文档。

在开始使用应用程序之前，请仔细阅读并接受隐私政策的条款。

您可以按如下方式查看隐私策略的条款：

- 在应用程序的启动配置期间。
- 通过打开 privacy_policy_en.txt，它是应用程序分发工具包的一部分（该文档的副本也保存在应用程序安装文件夹中）。

请在应用程序启动配置期间阅读并接受隐私策略的条款。如果不接受隐私策略的条款，您必须取消应用程序的初始配置，不得使用该应用程序。

关于授权许可

*授权许可*授予您根据最终用户授权许可协议使用应用程序的权利。如果您购买授权许可证书，则可以使用应用程序的功能。

当前应用程序版本提供以下类型的授权许可：

- 更新和补充：在授权许可期限内无限制使用应用程序的基本功能，并使用应用程序模块和数据库的更新功能。

  此类授权许可用于授权服务器和所有使用的应用程序探测器。添加具有有效"更新和补充"类型的授权许可密钥或具有用于应用程序先前版本的有限更新类型的授权许可密钥后，应用程序中的更新功能将被激活。

- 安全审计：无限制使用应用程序的基本功能，并在授权许可期限内使用安全审计功能和设备主动轮询功能。

  此类授权许可仅用于授权应用程序服务器。要授权您将使用的探测器，您必须另外购买"更新和补充"授权许可。添加具有安全审计类型有效授权许可的授权许可密钥或具有用于先前应用程序版本的主动轮询类型有效授权许可的授权许可密钥后，将在应用程序中激活指定的功能。

- 远程收集器：在集成模式规定的场景中与卡巴斯基 SD-WAN 联合使用。

  此类授权许可不需要您向应用程序添加授权许可密钥。但是，如果您没有购买远程收集器授权许可，则无法将 Kaspersky Industrial CyberSecurity for Networks 与卡巴斯基 SD-WAN 集成使用。

通过使用授权许可密钥，您可以仅激活 Upd&Sup 授权许可类型的功能，或者同时激活 Upd&Sup 授权许可类型的功能和安全审计授权许可类型的功能。只能向应用程序添加一个授权许可密钥。通过 Web 界面连接到服务器时，您可以查看有关已添加的授权许可密钥的信息。

当授权许可到期时，应用程序将继续运行，但相应的功能将不可用。要在授权许可过期后继续使用相应的功能，您需要添加具有所需类型的有效授权许可的新授权许可密钥。

该软件的更新功能（包括提供反病毒签名更新和代码库更新）可能无法在美国境内使用。

如果有活动的技术支持协议，您将得到技术支持服务。为了获得技术支持服务，您必须指定有权提出技术支持服务请求的联系人。

关于授权授权许可书

*授权许可证书*是确认您有权使用应用程序的文件。当购买授权许可时，您会被提供此文档。

Kaspersky Industrial CyberSecurity for Networks 授权许可证书包含以下信息：

- 授权许可 ID 或订单号
- 被授予授权许可的用户的信息
- 有关授权许可涵盖的应用程序和组件的信息
- 许可单元数量限制（例如探测器数量）
- 授权许可期限的开始日期
- 授权许可到期日期或授权许可期限
- 授权许可类型

关于授权许可密钥

授权许可密钥（以下也简称为*密钥*）是一系列位，您可以使用它来激活并使用由授权许可类型决定的功能。授权许可密钥由卡巴斯基专家生成。

您可以使用*授权许可密钥文件*向应用程序添加授权许可密钥。将授权许可密钥添加到应用程序后，授权许可密钥将作为唯一的字母数字序列显示在应用程序界面中。

卡巴斯基可以阻止违反最终用户授权许可协议的授权许可密钥。如果授权许可密钥被阻止，您必须添加不同的授权许可密钥才能使用相应的应用程序功能。

关于授权许可密钥文件

*授权许可密钥文件*是您从卡巴斯基收到的带有 KEY 扩展名的文件。授权许可密钥文件用于添加激活相应应用程序功能的授权许可密钥。

购买 Kaspersky Industrial CyberSecurity for Networks 后，您会收到一个授权许可密钥文件。接收授权许可密钥文件的方法由您从其购买该应用程序的卡巴斯基经销商决定（例如，授权许可密钥文件可能会发送到您指定的电子邮件地址）。

您还可以从购买 Kaspersky Industrial CyberSecurity for Networks 的先前版本时收到的授权许可密钥文件添加授权许可密钥。授权许可密钥可以在到期之前被添加到应用程序中。

您无需连接到卡巴斯基激活服务器即可使用授权许可密钥文件激活应用程序功能。

通过 Web 界面连接到服务器时添加授权许可密钥

您可以通过以下方式之一将授权许可密钥添加到 Kaspersky Industrial CyberSecurity 解决方案：通过 Web 界面连接到服务器时或使用向 Kaspersky Security Center 自动分配授权许可密钥的功能。本文介绍通过 Web 界面连接到服务器时添加授权许可密钥的过程。

通过 Web 界面连接到服务器时，只有具有管理员角色的用户才能添加授权许可密钥。

要添加授权许可密钥：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **授权许可**。
3. 单击**添加授权许可密钥**。如果授权许可密钥已添加到应用程序，则此按钮不存在。

   这将打开用于选择授权许可密钥文件的标准浏览器窗口。

4. 指定以 KEY 为扩展名的授权许可密钥文件的路径。

5. 单击打开文件的按钮。

所选密钥文件中的授权许可密钥将被加载到应用程序中。密钥加载完成后，相应的应用程序功能将被激活。您可以查看关于已添加的授权许可密钥的信息。

查看有关添加的授权许可密钥的信息

通过 Web 界面连接到服务器时，您可以查看有关已添加的授权许可密钥的信息。有关授权许可密钥的信息显示在**设置** → **授权许可**下。有关应用程序运行问题的通知列表也可能显示有关授权许可密钥状态的警告。

要查看有关授权许可密钥的信息：

选择**设置** → **授权许可**。

以下信息将为添加的授权许可密钥显示：

- **密钥** — 唯一的字母数字序列。
- **描述** — 有关可用功能的信息。
- **激活日期** — 授权许可密钥被首次添加到应用程序的日期。
- **有效期** — 授权许可密钥的到期日期。
- **到期** — 距到期还剩的天数。
- 有关密钥状态的信息或问题警告。

删除授权许可密钥

当通过 Web 界面连接到服务器时，您可以从应用程序中删除添加的授权许可密钥（例如，如果您需要用其他密钥替换当前授权许可密钥）。授权许可密钥被删除后，应用程序中的相应功能将不再可用。下次添加授权许可密钥时，此不可用的功能将被重新激活。

只有具有管理员角色的用户才能删除授权许可密钥。

要删除已添加的授权许可密钥：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 选择**设置** → **授权许可**。

3. 单击**删除**。

   将打开一个带有确认提示的窗口。

4. 确认删除授权许可密钥。

   授权许可密钥将被从应用程序中删除。

数据提供

最终用户授权许可协议的条款和条件描述为提供正确的应用程序操作而自动处理的数据。权利持有人根据隐私政策，特别是其中描述数据保护措施、处理地点和数据主体权利的内容处理所提供的数据。在某些国家，根据法律规定，某些提供的数据可被归类为个人数据。

应用程序不会将用户的个人数据发送给卡巴斯基。用户的个人数据在安装应用程序组件的计算机上进行处理。

应用程序处理并保存与用户个人数据相关的以下数据：

- 在应用程序中创建的用户账户的名称（应用程序用户）。
- 安装了应用程序组件的计算机的 IP 地址或名称。
- 应用程序接收的 IP 地址、MAC 地址和其他设备信息。
- 有关地址空间和子网的数据。
- 过程控制规则中的工业流程设置数据。
- Kaspersky Security Center 所在计算机的 IP 地址或名称。
- 通过连接器连接到应用程序的计算机的 IP 地址或名称。
- 电子邮件连接器和报告模板中指明的收件人的电子邮件地址。
- 生成的应用程序报告中的数据。
- 设备之间传输的工业网络流量中的数据，其中包含用户的个人数据（该数据在分析工业网络流量时与其他数据一起由应用程序处理）。
- 有关可能影响工业系统资源的检测到的风险的数据。
- 有关从 EPP 应用程序收到的可能被感染的对象或潜在威胁的数据，包含 IP 地址、网址和电子邮件地址。
- 从 EPP 应用程序收到的或作为安全审计作业结果的应用程序和补丁的数据。
- 从 EPP 应用程序收到的或作为安全审计作业结果的可执行文件数据。
- 从 EPP 应用程序收到的或作为安全审计作业结果的用户账户数据。
- 使用漏洞和合规性审计规则对设备执行检查的结果数据。
- 作为安全审计作业结果收到的设备配置数据。
- 网络会话和协议属性数据。
- 应用程序用户输入并保存在 Secret 存储中的身份和身份验证信息。

对列出的数据进行处理是为了确保应用程序的运行，以便分析技术流程的违规行为并检测网络流量中可能存在攻击迹象的威胁和异常。

应用程序将收到到的数据保存在日志中。

如果应用程序管理员已配置将应用程序数据转发到接收系统，则收到的数据将根据其功能和目的进行处理并存储在接收系统中。

如果使用应用程序集中安装脚本创建了文件以向卡巴斯基技术支持提供信息，则这些文件中将保存以下数据：

- 用于存储应用程序数据的文件夹的内容：
  - 应用程序组件、DBMS 和入侵检测系统的进程日志文件。
  - 服务器和探测器的工作数据文件。
  - 应用程序集中安装脚本创建的安装设置文件。
  - 应用程序消息日志和审计日志。
- 在服务器上应用的安全策略。
- 支持应用程序组件运行的服务的当前状态信息：
  - kics4net
  - kics4net-anomaly-hunter
  - kics4net-apm
  - kics4net-asset-config-repo
  - kics4net-asset-inventory
  - kics4net-blob-storage
  - kics4net-clickhouse
  - kics4net-config-control-orchestrator
  - kics4net-connectors
  - kics4net-connectors-launcher
  - kics4net-email-gateway
  - kics4net-epp-proxy
  - kics4net-fts
  - kics4net-nats-server
  - kics4net-oval-facade
  - kics4net-postgresql
  - kics4net-risk-oval-detector
  - kics4net-report-builder

- kics4net-report-data-source
- kics4net-report-renderer
- kics4net-report-templates-catalog
- kics4net-report-templates-catalog-view
- kics4net-responses-manager
- kics4net-scan-oval-manager
- kics4net-scap-manager
- kics4net-scap-manager-view
- kics4net-scheduler
- kics4net-secrets
- kics4net-suricata
- kics4net-task-manager
- kics4net-task-manager-view
- kics4net-telemetry-proxy
- kics4net-vault
- kics4net-webserver
- kics4net-websensor
- klnagent

- 安装有应用程序组件的计算机的操作系统版本及分发包的信息（`uname -a`命令被用于接收信息）。
- 安装了应用程序组件的计算机上的网络接口信息（`ifconfig`命令被用于接收信息）。
- auditd 服务在文件 /var/log/audit/audit.log 中保存的条目。
- 操作系统中防火墙的设置、状态和运行模式。
- 如果定义了相应的设置，则运行应用程序集中安装脚本时还会保存以下文件和数据：
  - 流量转储文件。
  - 有关入侵检测系统配置的数据。
  - Kaspersky Industrial CyberSecurity for Networks 中使用的证书数据（由受信任证书颁发机构发布的证书除外）。

应用程序不监控对应用程序集中安装脚本创建的安装设置文件的访问。但是，应用程序确实会跟踪应用程序组件的启动以及涉及用户凭据验证的服务器的其他连接。

当从卡巴斯基服务器接收更新时，应用程序会传输自动选择相关更新所需的数据。传输的数据不包含用户的任何个人数据。应用程序传输以下数据：

- Kaspersky Industrial CyberSecurity for Networks 的版本。
- Kaspersky Industrial CyberSecurity for Networks 组件的本地化语言代码。
- 已更新元素的 ID。
- Kaspersky Industrial CyberSecurity for Networks 安装 ID。
- 操作系统类型、版本和比特率的 ID。

任何收到的信息均根据法律规定的要求和卡巴斯基的现行规定受到卡巴斯基保护。数据通过加密通信渠道进行传输。

用于存储应用程序数据的文件夹

删除或修改这些文件夹中的任何文件会影响该应用程序的运行。

在 Kaspersky Industrial CyberSecurity for Networks 伺服器上，应用程序使用以下文件夹和子文件夹来存储数据：

- 组件和服务安装文件夹：
  - /opt/kaspersky/kics4net/ – 用于服务器。
  - /opt/kaspersky/kics4net-anomaly-hunter/ – 用于基于规则的网络异常检测服务。
  - /opt/kaspersky/kics4net-apm/ – 用于主动轮询连接器。
  - /opt/kaspersky/kics4net-asset-config-repo/ – 用于设备配置存储服务。
  - /opt/kaspersky/kics4net-asset-inventory/ – 用于使用 OVAL® 规则处理扫描设备属性结果的服务。
  - /opt/kaspersky/kics4net-blob-storage/ – 用于存储二进制数据数 (Binary Large Object，BLOB) 组的服务。
  - /opt/kaspersky/kics4net-cli/ – 用于安全策略导出实用程序。
  - /opt/kaspersky/kics4net-clickhouse/ – 用于存储协议属性的数据库管理系统。
  - /opt/kaspersky/kics4net-config-control-orchestrator/ – 用于管理配置控制和主动轮询过程的服务。
  - /opt/kaspersky/kics4net-connectors/ – 用于系统连接器。
  - /opt/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
  - /opt/kaspersky/kics4net-email-gateway/ – 用于电子邮件通知转发服务。
  - /opt/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式的 EPP 应用程序集成服务。

- /opt/kaspersky/kics4net-fts/ – 用于全文搜索系统。
- /opt/kaspersky/kics4net-nats-server/ – 用于消息代理。
- /opt/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则执行远程设备扫描的服务。
- /opt/kaspersky/kics4net-postgresql/ – 用于包含服务器数据库的 DBMS。
- /opt/kaspersky/kics4net-report-builder/ – 用于报告生成服务。
- /opt/kaspersky/kics4net-report-data-source/ – 用于提供报告数据的服务。
- /opt/kaspersky/kics4net-report-renderer/ – 用于提供报告中数据块的可视化呈现的服务。
- /opt/kaspersky/kics4net-report-templates-catalog/ – 用于报告模板管理服务。
- /opt/kaspersky/kics4net-report-templates-catalog-view/ – 用于提供报告模板数据的服务。
- /opt/kaspersky/kics4net-task-manager/ – 用于响应任务管理服务。
- /opt/kaspersky/kics4net-risk-oval-detector/ – 用于使用 OVAL 规则处理设备风险扫描结果的服务。
- /opt/kaspersky/kics4net-scan-oval-manager/ – 用于使用 OVAL 规则管理设备扫描的服务。
- /opt/kaspersky/kics4net-scap-manager/ – 用于安全审计管理服务。
- /opt/kaspersky/kics4net-scap-manager-view/ – 用于提供安全审计数据的服务。
- /opt/kaspersky/kics4net-scheduler/ – 用于任务调度服务。
- /opt/kaspersky/kics4net-secrets/ – 用于 Secret 存储库接口服务。
- /opt/kaspersky/kics4net-suricata/ – 用于入侵检测系统。
- /opt/kaspersky/kics4net-task-manager/ – 用于任务管理服务。
- /opt/kaspersky/kics4net-task-manager-view/ – 用于提供任务数据的服务。
- /opt/kaspersky/kics4net-epp-proxy/ – 用于 UDP 模式的 EPP 应用程序集成服务。
- /opt/kaspersky/kics4net-vault/ – 用于将 Secret 存储在存储库中的服务。
- /opt/kaspersky/kics4net-webserver/ – 用于 Web 服务器。
- /opt/kaspersky/klnagent64/ – 用于网络代理（如果安装）。

- 存储证书和操作数据的文件夹：
  - /opt/kaspersky/kics4net/share/ids/ – 用于入侵检测系统。
  - /var/opt/kaspersky/kics4net/ – 用于服务器。
  - /var/opt/kaspersky/kics4net-anomaly-hunter/ – 用于基于规则的网络异常检测服务。
  - /var/opt/kaspersky/kics4net-apm/ – 用于主动轮询连接器。

- /va/opt/kaspersky/kics4net-asset-config-repo/ – 用于设备配置存储服务。
- /var/opt/kaspersky/kics4net-asset-inventory/ – 用于使用 OVAL 规则处理设备风险扫描结果的服务。
- /var/opt/kaspersky/kics4net-blob-storage/ – 用于 BLOB 服务。
- /var/opt/kaspersky/kics4net-cli/ – 用于安全策略导出实用程序。
- /var/opt/kaspersky/kics4net-clickhouse/ – 用于存储协议属性的数据库管理系统。
- /var/opt/kaspersky/kics4net-config-control-orchestrator/ – 用于管理配置控制和主动轮询过程的服务。
- /var/opt/kaspersky/kics4net-connectors/ – 用于系统连接器。
- /var/opt/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
- /var/opt/kaspersky/kics4net-email-gateway/ – 用于电子邮件通知转发服务。
- /var/opt/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式的 EPP 应用程序集成服务。
- /var/opt/kaspersky/kics4net-fts/ – 用于全文搜索系统。
- /var/opt/kaspersky/kics4net-nats-server/ – 用于消息代理。
- /var/opt/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则扫描远程设备的服务。
- /var/opt/kaspersky/kics4net-postgresql/ – 用于包含服务器数据库的 DBMS。
- /var/opt/kaspersky/kics4net-report-builder/ – 用于报告生成服务。
- /var/opt/kaspersky/kics4net-report-data-source/ – 用于提供报告数据的服务。
- /var/opt/kaspersky/kics4net-report-renderer/ – 用于在报告中呈现数据块的服务。
- /var/opt/kaspersky/kics4net-report-templates-catalog/ – 用于报告模板管理服务。
- /var/opt/kaspersky/kics4net-report-templates-catalog-view/ – 用于提供报告模板数据的服务。
- /var/opt/kaspersky/kics4net-responses-manager/ – 用于响应任务管理服务。
- /var/opt/kaspersky/kics4net-risk-oval-detector/ – 用于使用 OVAL 规则处理设备风险扫描结果的服务。
- /var/opt/kaspersky/kics4net-scan-oval-manager/ – 用于使用 OVAL 规则管理设备扫描的服务。
- /var/opt/kaspersky/kics4net-scap-manager/ – 用于安全审计管理服务。
- /var/opt/kaspersky/kics4net-scap-manager-view/ – 用于提供安全审计数据的服务。
- /var/opt/kaspersky/kics4net-scheduler/ – 用于任务调度服务。
- /var/opt/kaspersky/kics4net-secrets/ – 用于 Secret 存储库接口服务。
- /var/opt/kaspersky/kics4net-task-manager/ – 用于任务管理服务。
- /var/opt/kaspersky/kics4net-task-manager-view/ – 用于提供任务数据的服务。

- /var/opt/kaspersky/kics4net-telemetry-proxy/ – 用于 UDP 模式下的 EPP 应用程序集成服务。
- /var/opt/kaspersky/kics4net-vault/ – 用于将 Secret 存储在存储库中的服务。
- /var/opt/kaspersky/kics4net-webserver/ – 用于 Web 服务器。
- /var/opt/kaspersky/klnagent/ – 用于网络代理（如果安装）。

- 存储过程日志的文件夹：
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – 用于存储安装过程日志和安装设置文件的文件夹（如果应用程序组件是从此计算机集中安装的）。
  - /var/log/kaspersky/kics4net/ – 用于服务器。
  - /var/log/kaspersky/kics4net-anomaly-hunter/ – 用于基于规则的网络异常检测服务。
  - /var/log/kaspersky/kics4net-apm/ – 用于主动轮询连接器。
  - /var/log/kaspersky/kics4net-asset-config-repo/ – 用于设备配置存储服务。
  - /var/log/kaspersky/kics4net-asset-inventory/ – 用于使用 OVAL 规则处理设备属性扫描结果的服务。
  - /var/log/kaspersky/kics4net-blob-storage/ – 用于 BLOB 服务。
  - /var/log/kaspersky/kics4net-cli/ – 用于安全策略导出实用程序。
  - /var/log/kaspersky/kics4net-clickhouse/ – 用于存储协议属性的数据库管理系统。
  - /var/log/kaspersky/kics4net-config-control-orchestrator/ – 用于管理配置控制和主动轮询过程的服务。
  - /var/log/kaspersky/kics4net-connectors/ – 用于系统连接器。
  - /var/log/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
  - /var/log/kaspersky/kics4net-email-gateway/ – 用于电子邮件通知转发服务。
  - /var/log/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式下的 EPP 应用程序集成服务。
  - /var/log/kaspersky/kics4net-fts/ – 用于全文搜索系统。
  - /var/log/kaspersky/kics4net-local-deploy/ – 用于存储本地安装进程的日志（如果服务器已安装在此计算机上）。
  - /var/log/kaspersky/kics4net-nats-server/ – 用于消息代理。
  - /var/log/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则执行远程设备扫描的服务。
  - /var/log/kaspersky/kics4net-postgresql/ – 用于包含服务器数据库的 DBMS。
  - /var/log/kaspersky/kics4net-report-builder/ – 用于报告生成服务。
  - /var/log/kaspersky/kics4net-report-data-source/ – 用于提供报告数据的服务。
  - /var/log/kaspersky/kics4net-report-renderer/ – 用于在报告中呈现数据块的服务。

- /var/log/kaspersky/kics4net-report-templates-catalog/ – 用于报告模板管理服务。
- /var/log/kaspersky/kics4net-report-templates-catalog-view/ – 用于提供报告模板数据的服务。
- /var/log/kaspersky/kics4net-responses-manager/ – 用于响应任务管理服务。
- /var/log/kaspersky/kics4net-risk-oval-detector/ – 用于使用 OVAL 规则处理设备风险扫描结果的服务。
- /var/log/kaspersky/kics4net-scan-oval-manager/ – 用于使用 OVAL 规则管理设备扫描的服务。
- /var/log/kaspersky/kics4net-scap-manager/ – 用于安全审计管理服务。
- /var/log/kaspersky/kics4net-scap-manager-view/ – 提供安全审计数据的服务。
- /var/log/kaspersky/kics4net-scheduler/ – 用于任务调度服务。
- /var/log/kaspersky/kics4net-secrets/ – 用于 Secret 存储库接口服务。
- /var/log/kaspersky/kics4net-suricata/ – 用于入侵检测系统。
- /var/log/kaspersky/kics4net-task-manager/ – 用于任务管理服务。
- /var/log/kaspersky/kics4net-task-manager-view/ – 用于提供任务数据的服务。
- /var/log/kaspersky/kics4net-telemetry-proxy/ – 用于 UDP 模式下的 EPP 应用程序集成服务。
- /var/log/kaspersky/kics4net-vault/ – 用于将 Secret 存储在存储库中的服务。
- /var/log/kaspersky/kics4net-webserver/ – 用于 Web 服务器（Web 服务器还将进程数据保存在操作系统的系统日志中）。
- /var/log/kaspersky/klnagent64/ – 用于网络代理（如果安装）。

- 存放配置文件的文件夹：
  - /etc/opt/kaspersky/kics4net/ – 用于服务器。
  - /etc/var/opt/kaspersky/kics4net-anomaly-hunter/ – 用于基于规则的网络异常检测服务。
  - /etc/opt/kaspersky/kics4net-asset-config-repo/ – 用于设备配置存储服务。
  - /etc/opt/kaspersky/kics4net-asset-inventory/ – 用于使用 OVAL 规则处理设备属性扫描结果的服务。
  - /etc/opt/kaspersky/kics4net-blob-storage/ – 用于 BLOB 服务。
  - /etc/opt/kaspersky/kics4net-cli/ – 用于安全策略导出实用程序。
  - /etc/opt/kaspersky/kics4net-clickhouse/ – 用于存储协议属性的数据库管理系统。
  - /etc/opt/kaspersky/kics4net-config-control-orchestrator/ – 用于管理配置控制和主动轮询过程的服务。
  - /etc/opt/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
  - /etc/opt/kaspersky/kics4net-email-gateway/ – 用于电子邮件通知转发服务。

- /etc/opt/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式的 EPP 应用程序集成服务。
- /etc/opt/kaspersky/kics4net-fts/ – 用于全文搜索系统。
- /etc/opt/kaspersky/kics4net-nats-server/ – 用于消息代理。
- /etc/opt/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则执行远程设备扫描的服务。
- /etc/opt/kaspersky/kics4net-report-builder/ – 用于报告生成服务。
- /etc/opt/kaspersky/kics4net-report-data-source/ – 用于提供报告数据的服务。
- /etc/opt/kaspersky/kics4net-report-renderer/ – 用于在报告中呈现数据块的服务。
- /etc/opt/kaspersky/kics4net-report-templates-catalog/ – 用于报告模板管理服务。
- /etc/opt/kaspersky/kics4net-report-templates-catalog-view/ – 用于提供报告模板数据的服务。
- /etc/opt/kaspersky/kics4net-responses-manager/ – 用于响应任务管理服务。
- /etc/opt/kaspersky/kics4net-risk-oval-detector/ – 用于使用 OVAL 规则处理设备风险扫描结果的服务。
- /etc/opt/kaspersky/kics4net-scan-oval-manager/ – 用于使用 OVAL 规则管理设备扫描的服务。
- /etc/opt/kaspersky/kics4net-scap-manager/ – 用于安全审计管理服务。
- /etc/opt/kaspersky/kics4net-scap-manager-view/ – 用于提供安全审计数据的服务。
- /etc/opt/kaspersky/kics4net-scheduler/ – 用于任务调度服务。
- /etc/opt/kaspersky/kics4net-secrets/ – 用于 Secret 存储库接口服务。
- /etc/opt/kaspersky/kics4net-task-manager/ – 用于任务管理服务。
- /etc/opt/kaspersky/kics4net-task-manager-view/ – 用于提供任务数据的服务。
- /etc/opt/kaspersky/kics4net-telemetry-proxy/ – 用于 UDP 模式下的 EPP 应用程序集成服务。
- /etc/opt/kaspersky/kics4net-vault/ – 用于将 Secret 存储在存储库中的服务。
- /etc/opt/kaspersky/kics4net-webserver/ – 用于 Web 服务器。
- /etc/opt/kaspersky/klnagent/ – 用于网络代理（如果安装）。
- /usr/lib/systemd/system/ – 用于存储 Kaspersky Industrial CyberSecurity for Networks 服务的配置文件（例如，kics4net.service）。
- /var/opt/kaspersky/kics4net-deploy/ – 用于存储在应用程序集中安装期间创建的安装设置文件副本的文件夹。
- /var/run/ – 用于加载后在文件夹本身（例如，klnagent.pid 文件）或子文件夹（例如，/kics4net/ 子文件夹）中存储系统健康数据变量。

在 Kaspersky Industrial CyberSecurity for Networks 探测器上，应用程序使用以下文件夹和子文件夹来存储数据：

- 组件和服务安装文件夹：
  - /opt/kaspersky/kics4net/ – 用于探测器。
  - /opt/kaspersky/kics4net-apm/ – 用于主动轮询连接器。
  - /opt/kaspersky/kics4net-connectors/ – 用于系统连接器。
  - /opt/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
  - /opt/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式的 EPP 应用程序集成服务。
  - /opt/kaspersky/kics4net-nats-server/ – 用于消息代理。
  - /opt/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则执行远程设备扫描的服务。
  - /opt/kaspersky/kics4net-suricata/ – 用于入侵检测系统。
  - /opt/kaspersky/kics4net-epp-proxy/ – 用于 UDP 模式的 EPP 应用程序集成服务。
  - /opt/kaspersky/kics4net-websensor/ – 用于 Web 服务器。
  - /opt/kaspersky/klnagent64/ – 用于网络代理（如果安装）。
- 存储证书和操作数据的文件夹：
  - /opt/kaspersky/kics4net/share/ids/ – 用于入侵检测系统。
  - /var/opt/kaspersky/kics4net/ – 用于探测器。
  - /var/opt/kaspersky/kics4net-apm/ – 用于主动轮询连接器。
  - /var/opt/kaspersky/kics4net-connectors/ – 用于系统连接器。
  - /var/opt/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
  - /var/opt/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式的 EPP 应用程序集成服务。
  - /var/opt/kaspersky/kics4net-nats-server/ – 用于消息代理。
  - /var/opt/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则（不使用网络代理）的设备扫描服务。
  - /var/opt/kaspersky/kics4net-telemetry-proxy/ – 用于 UDP 模式下的 EPP 应用程序集成服务。
  - /var/opt/kaspersky/kics4net-websensor/ – 用于 Web 服务器。
  - /var/opt/kaspersky/klnagent/ – 用于网络代理（如果安装）。

- 存储过程日志的文件夹：
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – 用于存储安装过程日志和安装设置文件的文件夹（如果应用程序组件是从此计算机集中安装的）。
  - /var/log/kaspersky/kics4net/ – 用于探测器。
  - /var/log/kaspersky/kics4net-apm/ – 用于主动轮询连接器。
  - /var/log/kaspersky/kics4net-connectors/ – 用于系统连接器。
  - /var/log/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
  - /var/log/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式下的 EPP 应用程序集成服务。
  - /var/log/kaspersky/kics4net-local-deploy/ – 用于存储本地安装进程的日志（如果此计算机上已安装 Sensor）。
  - /var/log/kaspersky/kics4net-nats-server/ – 用于消息代理。
  - /var/log/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则执行远程设备扫描的服务。
  - /var/log/kaspersky/kics4net-suricata/ – 用于入侵检测系统。
  - /var/log/kaspersky/kics4net-telemetry-proxy/ – 用于 UDP 模式下的 EPP 应用程序集成服务。
  - /var/log/kaspersky/kics4net-websensor/ – 用于 Web 服务器（Web 服务器还将进程数据保存在操作系统的系统日志中）。
  - /var/log/kaspersky/klnagent64/ – 用于网络代理（如果安装）。
- 存放配置文件的文件夹：
  - /etc/opt/kaspersky/kics4net/ – 用于探测器。
  - /etc/opt/kaspersky/kics4net-connectors-launcher/ – 用于注册和启动可管理连接器的服务。
  - /etc/opt/kaspersky/kics4net-epp-proxy/ – 用于 TCP 模式的 EPP 应用程序集成服务。
  - /etc/opt/kaspersky/kics4net-nats-server/ – 用于消息代理。
  - /etc/opt/kaspersky/kics4net-oval-facade/ – 用于使用 OVAL 规则执行远程设备扫描的服务。
  - /etc/opt/kaspersky/kics4net-telemetry-proxy/ – 用于 UDP 模式下的 EPP 应用程序集成服务。
  - /etc/opt/kaspersky/kics4net-websensor/ – 用于 Web 服务器。
  - /etc/opt/kaspersky/klnagent/ – 用于网络代理（如果安装）。
  - /usr/lib/systemd/system/ – 用于存储 Kaspersky Industrial CyberSecurity for Networks 服务的配置文件（例如，kics4net.service）。

- /var/opt/kaspersky/kics4net-deploy/ – 用于存储在应用程序集中安装期间创建的安装设置文件副本的文件夹。
- /var/run/ – 用于加载后在文件夹本身或子文件夹中存储系统健康数据变量。

修改应用程序文件需要操作系统的根权限。

关于日志

Kaspersky Industrial CyberSecurity for Networks 会将运行数据保存到日志中。根据日志的类型，应用程序将数据保存在服务器数据库中或服务器或探测器节点上的本地文件夹中的文件中。

日志保存在服务器数据库中

应用程序在服务器数据库中保存以下日志：

- 事件和突发事故日志
- 审计日志
- 应用程序消息日志

对于每个日志，您可以在日志存储设置中设置存储记录的大小限制。

该程序监控日志记录。如果程序的审计日志或消息日志的占用空间接近指定的限制，程序会在 Web 界面菜单中显示通知。该通知显示在具有管理员角色的用户的打开的连接会话中。

为了防止由于自动删除旧条目而丢失日志中的重要性信息，您可以将条目导出到文件中。该程序还允许您配置通过连接器将数据从日志自动传输到第三方系统。

日志保存在文件中

有关应用程序进程的信息以文件形式保存在本地文件夹中。进程日志文件可能包含以下信息：

- 有关 Kaspersky Industrial CyberSecurity for Networks 进程启动和停止的数据。
- 联系技术支持时可能需要的诊断消息。
- 错误消息。

有关进程的信息根据定义的进程记录级别进行存储。

您可以使用文本编辑器查看包含进程日志的文件。提供日志存取权限需要操作系统的根权限。

包含进程日志的文件以非加密形式存储。建议您确保信息不受未经授权的访问。

Kaspersky Industrial CyberSecurity for Networks 的管理

本节包含有关 Kaspersky Industrial CyberSecurity for Networks 的管理操作的信息。

部署节点

要部署已安装应用程序组件的节点，您可以添加或删除探测器、配置在节点上存储应用程序数据的设置以及管理保护功能。

如果您使用的服务器没有外部探测器，则安装应用程序后无需添加探测器。在这种情况下，必须仅为服务器节点配置部署设置。要安装服务器和外部探测器，您可以在使用 Web 界面连接到服务器时添加探测器。该应用程序仅使用添加到应用程序并连接的探测器。

默认情况下，在服务器和探测器上存储应用程序数据的设置是为了确保长期存储和最佳地利用可用磁盘空间。如果有必要，您可以根据系统的具体情况（例如，如果计算机硬件不完全满足要求）更改任何节点上的数据存储设置。

该应用程序监控可用监控点和所提供技术的运行，以便及时通知用户应用程序的非活动保护功能。如果任何监控点或技术被禁用，应用程序将显示有关禁用的保护功能的消息。对于处于学习模式的技术操作，也会显示此消息（某些技术可用此模式）。建议禁用监控点和技术，以及在有限的时间内使用技术学习模式。例如，您可以在工业网络相应段中在维护和调试期间禁用某个监控点。

您可以在 Kaspersky Industrial CyberSecurity for Networks Web 界面的“设置”**设置**“部署”**部署查看有关节点的信息**和管理部署设置。只有具有管理员角色的用户才能管理部署设置。

添加和删除传感器

安装并完成 Kaspersky Industrial CyberSecurity for Networks 服务器的启动配置后，您可以将 Sensor 添加到应用程序。探测器被添加到服务器 Web 界面页面上。

要在计算机上添加探测器，必须从应用程序分发工具包安装相应的软件包。您可以使用应用程序组件集中安装脚本或本地安装脚本来安装这些包。

您可以从应用程序中删除探测器。当探测器被删除时，该探测器的注册数据将从应用程序服务器中删除，这将导致探测器无法连接到该服务器。

但是，删除探测器后，探测器组件文件将保留在该节点上。您稍后可以再次将此节点添加为探测器，而无需安装相应的软件包。您可以将探测器添加到当前服务器或您可以连接的任何其他 Kaspersky Industrial CyberSecurity for Networks 服务器。

使用传感器 Web 界面添加和连接传感器

添加探测器时，服务器上会生成一个包含探测器证书和配置数据的配置包。添加的探测器通过探测器 Web 界面进行连接。探测器 Web 界面允许您下载配置包并使用以下方法连接探测器：

- 使用通信数据包。使用此方法时，配置包将保存为受密码保护的证书的文件。该文件被称为*通信数据包*。通信数据包必须安全地传送到可以通过网络访问探测器计算机的计算机，然后必须在探测器 Web 界面页面上下载。下载通信数据包后，探测器会自动连接到创建该文件的服务器。

- 自动通过网络。此方法可让您通过网络将配置包转发到探测器计算机的指定 IP 地址。探测器处理配置包，使用它生成证书签名请求 (CSR)，并将该请求发送到服务器。在接收到请求后，服务器 Web 界面页面将接收到的请求的指纹以字符序列的形式显示出来。相同的请求指纹也同时显示在探测器 Web 界面页面上。在完成探测器的添加之前，您必须确保这些指纹是相同的。

使用通信数据包添加和连接探测器

要使用通信数据包添加并连接探测器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 选择**设置 → 部署**。

3. 单击“**添加 Sensor**”。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 在“**使用通信数据包**”选项卡上：

   a. 输入代表 Kaspersky Industrial CyberSecurity for Networks 中探测器的探测器名称。

   探测器名称必须是唯一的（不得与其他探测器或服务器的名称匹配）并且包含的字符不得超过 100 个。您可以使用英文字母、数字、空格以及以下特殊字符：_ 和 -（例如，`Sensor_1`）。探测器名称必须以空格以外的任何允许的字符开始和结束。

   b. 输入探测器用于连接服务器的服务器 IP 地址。

   c. 输入探测器计算机上的 Web 服务器使用的 IP 地址。

   d. 输入保护通讯数据包中的证书的密码。

   密码必须符合以下要求：

   - 必须包含 8 到 256 个 ASCII 字符。
   - 必须包含一个或多个英语字母的大写字母。
   - 必须包含一个或多个拉丁字母的小写字母。
   - 必须包含一个或多个数字。
   - 不得包含超过三个连续重复的字符。

5. 单击“**创建通信数据包**”。您的浏览器将保存下载的文件。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。

6. 通过 Web 界面连接探测器

7. 在探测器 Web 界面页面上，单击“**选择文件**”。
   这将打开用于选择文件的标准浏览器窗口。

8. 指定通信数据包的路径。

9. 单击打开文件的按钮。

10. 下载文件内容后，输入访问通信数据包中的探测器证书的密码。

探测器将连接到服务器，然后有关连接的信息将显示在服务器和探测器 Web 界面页面上。

通过网络自动添加和连接探测器

要通过网络自动添加和连接探测器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks Server。

2. 选择**设置** → **部署**。

3. 单击“**添加 Sensor**”。
   详细信息区域出现在 Web 界面窗口的右侧。

4. 在**自动通过网络**选项卡上：

   a. 输入代表 Kaspersky Industrial CyberSecurity for Networks 中探测器的探测器名称。
      探测器名称必须是唯一的（不得与其他探测器或服务器的名称匹配）并且包含的字符不得超过 100 个。您可以使用英文字母、数字、空格以及以下特殊字符：_ 和 -（例如，`Sensor_1`）。探测器名称必须以空格以外的任何允许的字符开始和结束。

   b. 输入探测器用于连接服务器的服务器 IP 地址。

   c. 输入探测器计算机上的 Web 服务器使用的 IP 地址。

5. 单击“**连接并添加 Sensor**”。
   该应用程序将与探测器计算机建立连接，然后服务器 Web 界面页面将显示提示，以确认证书签名请求的接收指纹。

6. 通过 Web 界面连接探测器
   探测器 Web 界面页面将显示一条消息，其中包含有关发送到服务器的证书请求指纹的信息。

7. 确保探测器和服务器的 Web 界面页面上代表证书请求指纹的字符序列相同。

8. 在服务器 Web 界面页面上，单击按钮确认收到的证书请求指纹。

探测器将连接到服务器，然后有关连接的信息将显示在服务器和探测器 Web 界面页面上。

为传感器创建新的通信数据包

如有必要，您可以为 Sensor 创建新的通信数据包（例如，如果您需要更新用于将 Sensor 连接到服务器的证书）。

要为探测器创建新的通信数据包：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 选择要为其创建新的通信数据包的探测器的节点图块。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击“**获取新的通信数据包**”。如果工具栏上未显示该按钮，请单击 ⋮ 按钮并在打开的菜单中选择所需的项目。
5. 在打开的“**生成新的通信数据包**”窗口中：
   a. 输入探测器用于连接服务器的服务器 IP 地址。
   b. 输入保护通讯数据包中的证书的密码。
      密码必须符合以下要求：
      - 必须包含 8 到 256 个 ASCII 字符。
      - 必须包含一个或多个英语字母的大写字母。
      - 必须包含一个或多个拉丁字母的小写字母。
      - 必须包含一个或多个数字。
      - 不得包含超过三个连续重复的字符。
6. 单击“**创建文件**”。
   服务器为选定的探测器生成新的通信数据包，然后浏览器保存下载的文件。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。
7. 在探测器计算机上，使用 kics4net-reset-to-defaults.sh 脚本将探测器返回到初始状态，该脚本将节点恢复到初始状态。该脚本位于安装了应用程序组件的计算机的 /opt/kaspersky/kics4net/sbin/ 文件夹中。
8. 通过 Web 界面连接探测器
9. 在探测器 Web 界面页面上，上传新的通信数据包。
   新的通信数据包的上传方式与使用通信数据包添加探测器时上传的方式相同。

删除传感器

只有具有管理员角色的用户才能删除传感器。

要删除探测器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 选择要删除的探测器的节点图块。
   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，单击**确定**。

更改主节点设置

对于服务器和添加的传感器，您可以更改以下主要设置：

- 用于在节点上存储应用程序数据的设置
- 节点名称
- 使用外部存储存储流量转储文件的设置

更改节点上的应用程序数据存储设置

您可以更改用于在节点上存储应用程序数据的最大空间的限制。

要更改最大空间限制：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 选择相关节点的图块。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
   详细信息区域将显示用于配置节点参数的选项卡。
5. 在“**常规**”选项卡的“**存储设置**”部分中，定义应用程序数据的最大空间限制。可供配置的数据类型集取决于节点的类型（服务器或探测器）。
   您可以选择空间限制的计量单位：**MB** 或 **GB**。
   对于某些数据类型（例如事件），您可以定义以天为单位的存储时间限制。
6. 单击**保存**。

重命名已安装应用程序组件的节点

您可以更改托管已安装应用程序组件（服务器或探测器）的节点的定义名称。

只有具有管理员角色的用户才能更改节点名称。

要更改节点名称：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置 → 部署**。
3. 选择相关节点的图块。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
5. 在包含节点当前名称的字段中，输入新名称。
   节点名称必须是唯一的（不得与其他节点的名称匹配）并且包含的字符不得超过 100 个。您可以使用英文字母、数字、空格以及特殊字符 _ 和 -（例如，Server_1）。节点名称必须以任何允许的字符开头和结尾（空格除外）。
6. 单击**保存**。

连接和配置流量转储文件的外部存储

应用程序将通过监控点接收到的流量保存为流量转储文件。该应用程序使用每个节点的内部存储来在线存储文件并分析这些文件中保存的流量。应用程序根据为节点指定的内部存储设置在内部存储中保存和删除文件。在节点上连接并配置外部存储，以保证流量转储文件的长期存储。存储在外部存储中的流量转储文件可用于将流量下载到 PCAP 文件，例如，如果该流量的转储文件已从节点上的内部存储中删除，则可以从网络会话下载流量。

使用节点计算机本地文件系统中的目录作为外部存储。该目录必须挂载到具有足够可用空间且不包含 /var/ 目录的硬盘上。对于外部存储，还可以使用另一台计算机的共享网络资源挂载的目录，例如类似于将事件导出到网络资源的目录。本地文件系统中的目录必须被授予 kics4net 账户的权限，包括创建嵌套目录的权限。

为外部存储创建和挂载目录的操作是使用节点计算机的标准操作系统工具执行的。

要连接并配置节点上流量转储文件的外部存储：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置 → 部署**。
3. 选择相关节点的图块。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
   详细信息区域将显示用于配置节点参数的选项卡。
5. 选择“**外部存储**”选项卡，然后使用“**连接流量转储文件的外部存储**”开关启用外部存储模式。
6. 指定节点本地文件系统中用于外部存储的目录的路径。
7. 在“**最大大小**”下设置存储流量转储文件的空间限制。
   您可以选择空间限制的计量单位：**MB** 或 **GB**。

8. 如有必要，在“**过滤存储的流量**”部分中，启用过滤并根据网络数据包的地址设置使用 Berkeley Packet Filter (BPF) 技术输入过滤表达式。

   过滤通过跳过与过滤器不匹配的网络数据包来减少存储的流量。但是，在这种情况下，当您稍后查看流量转储文件或从这些文件下载流量时，您将无法下载保存流量时跳过的网络数据包。

9. 如有必要，在“**储存时限**”部分中，对文件的最短存储时间进行限制，并指定相关的天数。

10. 单击**保存**。

管理节点上的监控点

监控点用于接收和处理 Kaspersky Industrial CyberSecurity for Networks 中的工业网络流量。监控点可以在任何安装了应用程序组件的节点（包括执行服务器功能的节点）上进行添加或删除。添加或删除它们时，不需要重新启动安装了应用程序组件的计算机或在计算机上重新安装组件。

每个监控点必须与一个网络接口相关联，该网络接口接收来自特定工业网络段的流量副本。若要添加监控点，可以使用满足以下条件的网络接口：

- 网络接口类型：以太网。
- MAC 地址：与 00:00:00:00:00:00 不同。
- 该网络接口用于接收工业网络流量的副本，并且该网络接口不用于其他目的（例如，连接已安装了应用程序组件的节点）。

监控点可以被启用或禁用。您可以禁用监控点以暂时停止监控将流量副本中继到网络接口的工业网段。当需要恢复该工业网段的监控时，您可以启用该监控点。

禁用或删除监控点后，应用程序可能仍会在一段时间内注册与该监控点相关的事件。这是因为当服务器负载较高时，处理传入流量可能会出现延迟。

添加监控点

为了接收和处理从工业网络流向某个节点网络接口的流量，需要在这个网络接口上添加监控点。

只有具有管理员角色的用户才能在网络接口添加监控点。

要向网络接口添加监控点：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 通过单击相关网络接口的图块中的**添加监控点**来打开详细信息区域。如果尚未向网络接口添加监控点，则会显示该链接。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 在详细信息区域上方的输入栏中，输入监控点的名称。
   您可以使用英文大写和小写字母、数字以及_和 - 字符。
   监测点名称必须符合以下要求：

   - 必须是唯一的（未分配给另一个监测点）。
   - 必须包含 1 到 100 个字符。

5. 单击**添加监控点**。

启用监控点

应用程序不接收也不处理通过禁用的监控点的网络接口传输的流量。如果您想恢复接收和处理流量，则需要启用监控点。

您可以单独启用监控点，也可以在一个节点或所有节点上同时启用所有监控点。

只有具有管理员角色的用户才能启用监控点。

启用监控点：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 执行以下操作之一：

   - 如果要启用一个监控点，请单击包含该监控点的网络接口图块中的**启用**。如果监控点被禁用，则此按钮可用。
   - 如果要启用节点上的所有监控点，请单击托管已禁用监控点的节点图块中的**全部启用**。如果节点具有包含已禁用监控点的网络接口，则该按钮可用。
   - 如果要启用所有节点上的所有监控点，请点击工具栏上的**在所有节点上启用**。

4. 等待更改得到应用。

禁用监控点

如果您需要临时暂停某个监控点网络接口上的流量接收和处理，您可以禁用该监控点。

您可以单独禁用监控点，也可以同时禁用一个节点上的所有监控点或所有节点上的监控点。

只有具有管理员角色的用户才能禁用监控点。

禁用监控点：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。

3. 执行以下操作之一：

   - 如果要禁用一个监控点，请单击包含该监控点的网络接口图块中的**禁用**。监控点启用后该按钮可用。
   - 如果要禁用某个节点上的所有监控点，请单击托管已启用监控点的节点图块中的**全部禁用**。如果节点具有启用监控点的网络接口，则该按钮可用。
   - 如果要禁用所有节点上的所有监控点，请点击工具栏上的**在所有节点上禁用**。

4. 等待更改得到应用。

重命名监控点

您可以重命名链接到网络接口的监控点。

> 监控点的新名称将出现在重命名后注册的事件中。先前注册的事件中显示监测点的旧名称。

只有具有管理员角色的用户才能重命名监控点。

要重命名监控点：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks Server。
2. 选择“**设置**” → “**部署**”。
3. 选择包含要重命名的监控点的网络接口图块。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**编辑**，然后在出现的字段中输入新名称。
   您可以使用英文大写和小写字母、数字以及 _ 和 - 字符。
   监测点名称必须符合以下要求：
   - 必须是唯一的（未分配给另一个监测点）。
   - 必须包含 1 到 100 个字符。
5. 单击“**保存**”。

正在删除监控点

您可以删除链接到网络接口的监控点。如果该网络接口不再用于接收工业网络流量，则可能需要删除监控点。

如果需要临时暂停监控点网络接口的流量接收（例如，执行预防性维护和调整操作时），您可以禁用该监控点而不删除它。

> 在删除监控点之前从该监控点接收到的流量不会被从数据库中删除。该监控点的信息也被保存在已注册事件表中。

只有具有管理员角色的用户才能删除监控点。

若要删除监控点：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置 → 部署**。
3. 选择包含要删除的监控点的网络接口图块。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 在详细信息区域中，单击**删除**。
   将打开一个带有确认提示的窗口。如果监控点已启用，应用程序将提示您禁用该监控点。
5. 在提示窗口中，确认删除监控点。

识别与网络接口关联的以太网端口

安装有应用程序组件的计算机可能有多个用于连接局域网的以太网端口。您可以使用该应用程序为网络接口启用闪烁模式，并识别哪个以太网端口与该接口相关联。启用闪烁模式时，以太网端口旁边的 LED 指示灯将闪烁 15 秒。

如果网络接口不支持 LED 闪烁模式（例如，以太网端口旁边没有 LED 指示灯，或者网络接口是逻辑绑定接口），则启用闪烁模式时会出现错误。

只有具有管理员角色的用户才能启用以太网端口闪烁模式。

要确定哪个以太网端口链接到网络接口：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置 → 部署**。
3. 单击网络接口图块中的**闪烁**。
   如果网络接口支持 LED 指示灯，则网线连接图标将开始在网络接口图块上闪烁。同时，计算机对应网卡上以太网端口旁边的 LED 指示灯开始闪烁。

当为一个网络接口启用闪烁模式时，您不能为同一节点上的另一个网络接口启用闪烁模式。

管理技术

Kaspersky Industrial CyberSecurity for Networks 使用各种技术来分析工业网络流量。您可以启用或禁用单个技术的使用。对于某些技术，您可以选择运行模式：学习模式或监控模式。

建议启用技术学习模式一段时间，以便应用程序在适当的时刻自动将技术切换到监控模式。监控模式是一种标准的技术操作模式（与学习模式相反，学习模式中应用程序仅积累数据以供进一步使用）。配置学习模式时，您可以设置技术自动切换到监控模式的所需时间。

您可以在所有节点和监控点上配置相同的技术使用设置，也可以为所需的节点和监控点配置特定设置。技术使用设置可以自动从父对象继承到子对象。如果为节点或监控点启用了技术继承，则为父对象（服务器或探测器）配置的技术使用设置将应用于该对象。如果禁用技术继承，您可以在此节点或监控点上配置特定的技术使用设置。

应用程序安装后，除 PLC 项目控制和未知标签检测之外的所有技术均默认启用。对于支持模式更改的技术，学习模式是默认启用的。当向应用程序添加探测器和监控点时，默认为它们启用为父对象设置的技术继承。

启用和禁用技术

您可以启用或禁用服务器、传感器和监控点的技术。如果禁用了传感器和监控点的技术继承，则可以启用或禁用这些对象上的技术。

某些技术包括可以单独启用或禁用的方法。如果禁用某项技术或方法，则应用程序不会监控使用该技术或方法的设备的通信。您可以配置与禁用的技术或方法相关的应用程序设置（例如，添加或编辑规则）。

可以启用和禁用以下技术和方法：

- 资产管理：
  - 设备活动检测
  - 设备信息检测
  - PLC 项目控制
  - 网络会话检测
  - 风险检测（仅在服务器节点）
- 网络控制：
  - 网络完整性控制
  - 命令控制
- 过程控制：
  - 基于规则的过程控制
  - 未知标签检测
  - 过程控制的设备发现
  - 获取协议的属性
- 入侵检测：
  - 基于规则的入侵检测
  - ARP 欺骗检测
  - IP 协议异常检测
  - TCP 协议异常检测
  - 蛮力攻击和扫描检测

本文介绍在服务器节点上启用和禁用技术的过程。在传感器节点和监控点上启用或禁用技术的操作在禁用这些对象的技术继承后以相同的方式执行。

具有管理员或安全官角色的用户可以启用和禁用节点上的技术。

要更改服务器节点上的技术和方法的状态：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**部署**”。
3. 选择服务器图块。
   详细信息区域出现在 Web 界面窗口的右侧。“**管理技术**”选项卡显示可以启用或禁用的技术和方法的列表。

   如果当前无法改变技术和方法的状态，则列表中的开关被禁用。在这种情况下，建议检查服务器计算机上 kics4net 服务的状态。如果该服务未激活，您必须启动它。
4. 使用左侧的切换开关来启用或禁用相关技术和/或方法的使用。您可以通过单击“**全部启用**”或“**全部禁用**”来同时启用或禁用所有技术和方法。
5. 启用或禁用技术或方法后，等待更改应用。切换开关在完成切换到其他状态之前不可用。

配置技术操作模式

您可以配置技术学习模式，也可以手动启用服务器、传感器和监控点的监控模式。如果禁用了这些对象的技术继承，则这些操作可用于传感器和监测点。

您可以更改以下技术和方法的模式：

- 设备活动检测
- 命令控制
- 基于规则的过程控制
- 网络完整性控制

本部分描述在服务器节点上更改和配置技术模式的过程。禁用技术继承后，在传感器节点和监测点上更改和配置技术模式的操作以相同的方式执行。

具有管理员或安全官角色的用户可以更改和配置节点上的技术和方法模式。

要更改和配置服务器节点上的技术和方法的模式：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**部署**”。
3. 选择服务器图块。
   详细信息区域出现在 Web 界面窗口的右侧。“**管理技术**”选项卡显示可以启用或禁用的技术和方法的列表。

如果当前无法更改技术和方法的操作模式，则列表中的开关被禁用。在这种情况下，建议检查服务器计算机上 kics4net 服务的状态。如果该服务未激活，您必须启动它。

4. 对于支持在学习模式下操作的技术和方法，在技术或方法名称右侧的下拉列表中，选择相关模式（“**学习**”或“**监控**”）。如果您想为所有这些技术和方法选择相同的模式，请使用“**模式**”下拉列表。

   如果选择了不同的模式，“**模式**”下拉列表将显示“**混合**”值。

5. 选择模式后，等待应用更改。在应用该模式之前，下拉列表中将显示“**更改**”状态。

6. 对于在学习模式下运行的技术和方法，指定它们自动切换到监控模式的日期和时间。为此，请单击“**设置截止日期**”并选择日期和时间。如果之前配置了日期和时间，则它们将显示在模式名称旁边。

管理技术继承

如果您希望传感器或监控点自动获取为父对象配置的技术使用设置，您可以启用技术继承。在这种情况下，传感器获取为服务器定义的技术使用设置，监控点获取为添加监控点的节点（针对服务器或传感器）定义的设置。

如有必要，您可以禁用传感器或监控点的技术继承。这允许您为此对象配置特定的技术使用设置。

具有管理员或安全官角色的用户可以启用和禁用传感器或监控点上的技术继承。

要启用或禁用传感器节点上的技术继承：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 选择探测器图块。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 将“**继承服务器技术**”开关设置到所需位置。

要在监控点上启用或禁用技术继承：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 选择包含要启用或禁用技术继承的监控点的网络接口图块。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 将技术继承开关设置到所需位置。

下载节点监控点收到的流量

您可以通过节点上的监控点下载应用程序接收到的流量。流量被下载到 PCAP 文件中。您可以配置网络包过滤来下载相关数据。

应用程序从流量转储文件存储下载流量。每个节点的内部存储（在节点上安装应用程序组件时自动创建）和外部存储（如果连接在节点上）都可以用于下载流量。

流量转储文件临时存储在存储中，并在收到新流量时自动删除。文件删除的频率取决于收到的流量以及指定的应用程序数据存储设置。如果从存储库中删除相应的流量转储文件，则无法下载流量。

要下载节点监控点收到的流量：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **部署**。
3. 执行以下操作之一：
   - 要下载某个节点的监控点接收到的流量，请选择该节点的图块。
   - 要下载特定监控点接收到的流量，请选择该监控点的网卡。

   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**下载流量**。如果工具栏上未显示该按钮，请单击⋮按钮并在打开的菜单中选择所需的项目。
5. 在打开的窗口中执行以下操作：
   - 要下载特定时间段内的流量，请使用“**要下载的流量周期**”设置定义所需的边界。

     默认期限为一小时。
   - 在“**下载量限制**”部分设置用于下载流量的最大量的限制。

     如果下载的流量超过指定的限制，则稍后到达的流量将被跳过。
   - 选择节点图块时，如有必要，请在“**按监控点过滤**”部分中启用过滤，并指定接收流量的节点的监控点（如果选择节点图块，则会显示此部分）。

     默认情况下，指定所选节点上所有可用的监控点。
   - 如有必要，请在“**按地址空间过滤**”部分中启用过滤，并指定网络数据包中的地址所属的地址空间（如果向应用程序添加了其他地址空间，则会显示此部分）。

     默认情况下，指定应用程序中创建的所有地址空间。
   - 如有必要，请在“**使用 BPF 进行过滤**”部分启用过滤，并根据网络数据包的地址设置使用 Berkeley Packet Filter (BPF) 技术输入过滤表达式。

     过滤表达式示例

     ```
     tcp port 102 or tcp port 502
     ```
   - 如有必要，请在“**使用正则表达式进行过滤**”部分中启用过滤，并输入根据网络数据包中的负载数据进行过滤的表达式。

     过滤表达式示例

     ```
     ^test.+xABxCD
     ```
6. 单击“**下载**”。

7. 如果创建文件的时间较长（超过 15 秒），则文件创建操作将转入后台操作列表。在这种情况下，要下载文件：

   a. 点击应用程序 Web 界面菜单中的 按钮。
   出现后台操作列表。

   b. 等待文件生成操作完成。

   c. 单击“**下载文件**”。

您的浏览器将保存下载的文件。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。

监控 Kaspersky Industrial CyberSecurity for Networks 的状态

本节包含有关监控应用程序状态的说明。

当通过 Web 界面连接时监控应用程序状态

通过 Web 界面连接到服务器时，您可以查看有关应用程序当前状态的信息。应用程序状态通过使用控制板**控制板小部件**来监控。

应用程序还会告知已禁用的保护功能和操作问题。

有关被禁用保护功能的信息

如果某些保护功能被禁用，则应用程序 Web 界面页面菜单下方将显示**不是所有保护服务都在运行**通知。在以下情况下会显示通知：

- 一个或多个监控点被禁用。
- 一个或多个保护功能（例如，基于规则的入侵检测）被禁用。
- 学习模式为一个或多个保护功能（例如，网络完整性控制技术）启用。

要查看被禁用保护功能的信息：

1. 单击**不是所有保护服务都在运行**通知。
   不提供保护的组件窗口将打开。

2. 选择以下选项卡之一：

- **服务器**– 查看被禁用的服务器保护服务的详细信息。

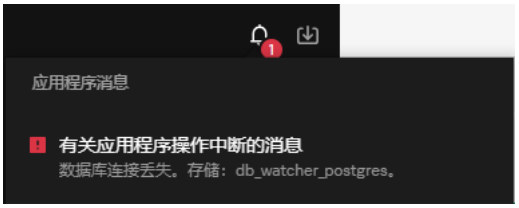
  如果在探测器和监控点的节点上启用了技术继承，则在**启用了所有组件上的技术继承**选项卡的右上角会显示**服务器**消息。

- **Sensor** – 查看已禁用的探测器保护服务的详细信息。

- **监控点** – 查看已禁用的监控点防护服务的详细信息。

应用程序运行问题通知

Web 界面菜单的上部包含一个按钮，用于打开有关应用程序运行中问题的通知列表（见下图）。



浏览器窗口中关于应用程序运行问题的通知列表

如果列表包含有关严重问题的通知（例如，有关应用程序运行中断的消息），会显示红色图标。如果列表仅包含有关非严重问题的通知，则会显示黄色图标。

列表仅包含最新的通知。如果问题已解决（例如，与服务器丢失的连接已恢复），则相应的通知将被自动从列表中删除。

您可以查看有关通知的详细信息（有关服务器或数据库不可用的通知除外）。

要查看有关通知的信息：

1. 在菜单中，单击按钮。
2. 在通知列表中，单击通知文本。

浏览器窗口将显示包含与通知相关信息的部分（例如，在**设置→应用程序消息**下）。

查看应用程序消息

应用程序消息日志存储有关应用程序运行中的错误以及 Kaspersky Industrial CyberSecurity for Networks 系统进程执行的操作中的错误的信息。

当通过 Web 界面连接到服务器时，您可以查看应用程序消息。如果需要，您还可以配置通过连接器将应用程序消息转发到接收系统。

查看应用程序消息：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置→应用程序消息**。

   该表将显示与定义的过滤器和搜索设置相匹配的应用程序消息。

应用程序消息的设置显示在表的以下列中：

- **日期和时间**
  应用程序消息的注册日期和时间。
- **状态**
  消息的状态。消息可以有以下状态：
  - *正常操作*– 用于信息性消息。
  - *未知*、*故障*– 有关非严重应用程序错误的消息。
  - *中度故障*、*严重故障*、*致命故障*– 有关应用程序故障的消息。
- **节点**
  消息来源节点的名称或 IP 地址。
- **系统进程**
  触发了消息注册的应用程序进程。
- **消息**
  消息的数字标识符和文本。

查看应用程序消息表时，您可以使用过滤、搜索和排序功能以及导出数据。

查看用户活动审计条目

Kaspersky Industrial CyberSecurity for Networks 可以保存有关用户在应用程序中执行的操作的信息。如果启用了用户活动审计，信息将保存在审计日志中。

当通过 Web 界面连接到服务器时，您可以查看审计条目。如有必要，您还可以配置通过连接器将审计条目转发到接收系统。

只有具有管理员角色的用户才能查看审计条目。

要查看审计条目：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置 → 审计**。

   该表将显示与定义的过滤器和搜索设置相匹配的审计条目。

审计条目的设置显示在表的以下列中：

- **日期和时间**
  用户操作数据的注册日期和时间。
- **操作**
  用户尝试执行的操作。
- **结果**
  已注册操作的结果（成功或未成功）。
- **用户**
  执行操作的用户的名称。
- **用户角色**
  执行操作的用户的角色。
- **用户节点**
  尝试在其上执行操作的节点的 IP 地址。
- **描述**
  已注册的操作代码和结果描述。

查看审计条目表时，您可以使用配置、过滤、搜索和排序功能以及导出数据。

查看已安装应用程序组件的节点以及节点上的网络接口的信息

任何角色的用户都可以查看已安装应用程序组件的节点以及节点上的网络接口的信息。

查看有关节点和网络接口的信息：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置 → 部署**。
   Web 界面窗口将显示节点图块（在左侧）和在这些节点上检测到的网络接口图块（在每个节点的右侧）。
3. 如果要查看有关节点或网络接口的详细信息，请选择相关节点或网络接口的图块。
   详细信息区域出现在 Web 界面窗口的右侧。

显示的已安装应用程序组件的节点的信息

节点图块显示以下信息：

- 当前节点状态。
  - *正常*该节点可用，未从该节点收到有关非严重故障或操作中断的应用程序消息。
  - *非关键故障*。该节点可用，从该节点接收到状态为*未知*或*故障*的应用程序消息。
  - *操作中断*。该节点可用，从该节点收到了状态为*中度故障*、*严重故障*或*致命故障*的应用程序消息。
  - *没有连接*。该节点不可用。
- 节点名称。
- 安装在节点上的应用程序组件：**服务器**或**Sensor**。
- 用于连接节点的 IP 地址（地址 0.0.0.0 对应计算机上所有可能的 IP 地址）。
- 可以为其选择操作模式的技术的当前模式。如果所有技术都在该模式下运行，则图块包含模式名称（*学习*或*监控*）。如果为技术选择了不同的模式，则会显示*混合*值。
- 如果为探测器禁用服务器技术继承，则显示图标。

显示的有关网络接口的信息

网络接口图块显示以下信息：

- 显示网线是否连接到网络接口的以太网端口的图标：
  - – 网线已连接。
  - – 网线已断开连接。

  当以太网端口闪烁模式启用时，该图标闪烁。
- 操作系统中的网络接口名称。
- MAC 地址。
- 网络接口接收的传入流量的速率。

- 监测点信息（若已添加）：
  - 监测点现状：
    - *正常*。监测点可用。
    - *切换*。监控点运行模式正在改变。
    - *错误*。切换监控点操作模式时检测到错误。
  - 监控点名称。
  - 监测点当前运行模式：
    - 若监控点被禁用，则显示*已禁用*值。
    - 如果监控点已启用，则会显示可以为其选择操作模式的当前技术模式。如果所有技术都在该模式下运行，则图块包含模式名称（*学习*或*监控*）。如果为技术选择了不同的模式，则会显示*混合*值。
  - 如果对某个监控点禁用了节点技术的继承，则显示图标。

详细信息中显示的节点信息

详细信息区域显示所选节点的以下信息：

- 节点名称。
- **管理技术**选项卡显示可以在节点上启用或禁用的技术和方法的列表。

  对于具有可选择操作模式的技术，显示当前模式：**学习**或**监控**。如果启用学习模式，则自动切换到监控模式的日期和时间将显示在模式名称的右侧（如果未设置自动切换时间，则不显示日期和时间）。
- **设置**选项卡显示以下信息：
  - **状态** – 由图标和文本描述指示的当前节点状态（与节点图块上的相同）。
  - **节点类型** – 安装在节点上的应用程序组件：**服务器**或Sensor。
  - **应用程序当前使用的磁盘空间** – 应用程序文件占用的磁盘空间。这包括已安装的文件和应用程序运行时创建的文件。
  - **应用程序可使用的最大磁盘空间** – 应用程序文件可占用的磁盘空间。这包括已安装的文件和数据存储规则中定义的所有卷限制的总和。该值不能超出可用的磁盘空间。
  - **已占用磁盘** – 所有文件使用的磁盘空间。这包括应用程序文件和操作系统及其他应用程序的文件。该空间量是根据节点的文件系统中包含 /var/ 文件夹的驱动器计算的。
  - **可用磁盘空间** – 未被文件使用的磁盘空间。该空间量是根据节点的文件系统中包含 /var/ 文件夹的驱动器计算的。
  - **总磁盘空间** – 节点的文件系统中包含 /var/ 文件夹的驱动器上的磁盘空间总量。
  - **技术的继承** – 指示服务器技术继承是否被启用或禁用的标志（仅适用于探测器节点）。

- **BPF 过滤** 指示节点是否已启用或禁用基于网络数据包中的地址参数使用 Berkley Packet Filter (BPF) 技术的过滤。
- **保留规则** – 以下设置的当前值和最大值：应用程序数据的数量、项目数和存储时间。

详细信息中显示的网络接口信息

对于未向其添加监控点的网络接口，详细信息区中显示以下信息：

- **网络接口** – 操作系统中网络接口的名称。
- **连接** – 表示网线已连接到网络接口的以太网端口的图标：
  - – 网线已连接。
  - – 网线已断开连接。

  当以太网端口闪烁模式启用时，该图标闪烁。
- **MAC 地址** – 网络接口的 MAC 地址。
- **IP 地址** – 网络接口的 IP 地址。如果在网络接口上检测到多个 IP 地址，则详细信息区域最多显示 16 个 IP 地址。

如果网络接口上已经添加了监控点，则会显示以下信息：

- 监控点名称。
- **状态** – 由图标和文字描述指示的监测点的当前状态：
  - *正常*。监测点可用。
  - *切换*。监控点运行模式正在改变。
  - *错误*。切换监控点操作模式时检测到错误。
- **连接** – 表示网线已连接到网络接口的以太网端口的图标：
  - – 网线已连接。
  - – 网线已断开连接。

  当以太网端口闪烁模式启用时，该图标闪烁。
- **网络接口** – 操作系统中网络接口的名称。
- **模式** – 监测点当前的运行模式：
  - *已启用*。
  - *已禁用*。

- **管理技术**选项卡显示可以在监控点上启用或禁用的技术和方法的列表。

  对于具有可选择操作模式的技术，显示当前模式：*学习*或*监控*。如果启用学习模式，则自动切换到监控模式的日期和时间将显示在模式名称的右侧（如果未设置自动切换时间，则不显示日期和时间）。

- 在**设置**选项卡上：

  - **技术的继承** — 指示节点技术继承是否启用或禁用的标志。
  - **MAC 地址** — 网络接口的 MAC 地址。
  - **IP 地址** — 网络接口的 IP 地址。如果在网络接口上检测到多个 IP 地址，则详细信息区域最多显示 16 个 IP 地址。

查看支持应用程序组件运行的服务状态

您可以查看支持应用程序组件运行的服务的状态。如果服务处于活动状态，则表示它已成功启动。

查看服务状态：

1. 在安装有应用程序组件的计算机上，打开操作系统控制台。
2. 输入以下命令：

   ```
   sudo service <服务名称> status
   ```

   其中`<服务名称>`是您要查看其信息的服务的名称。您可以指定以下服务：

   - `kics4net` — 主要服务（仅在执行服务器功能的计算机上运行）。
   - `kics4net-anomaly-hunter` – 用于基于规则检测网络异常的服务（运行在执行服务器功能的计算机上）。
   - `kics4net-apm` – 主动轮询连接器服务（在执行服务器或探测器功能的计算机上运行）。
   - `kics4net-asset-config-repo` – 设备配置存储服务（在执行服务器功能的计算机上运行）。
   - `kics4net-asset-inventory` – 使用 OVAL 规则处理扫描设备属性结果的服务（仅在执行服务器功能的计算机上运行）。
   - `kics4net-blob-storage` – 用于存储二进制数据阵列的服务（仅在执行服务器功能的计算机上运行）。
   - `kics4net-clickhouse` – 数据库管理系统服务，用于存储协议属性（仅在执行服务器功能的计算机上运行）。
   - `kics4net-config-control-orchestrator` – 用于管理配置控制和主动轮询过程的服务（仅在执行服务器功能的计算机上运行）。
   - `kics4net-connectors-launcher` – 注册和启动可管理连接器服务（在执行服务器功能或探测器功能的计算机上运行）
   - `kics4net-email-gateway` – 用于发送电子邮件通知的服务（仅在执行服务器功能的计算机上运行）。

- `kics4net-epp-proxy` – 用于在 TCP 模式下与 EPP 应用程序集成的服务（在执行服务器或传感器功能的计算机上运行）。
- `kics4net-fts` – 全文搜索系统服务（仅在执行服务器功能的计算机上运行）。
- `kics4net-nats-server` – 消息代理服务（在执行服务器功能或探测器功能的计算机上运行）。
- `kics4net-oval-facade` – 使用 OVAL 规则扫描远程设备的服务（在执行服务器或探测器功能的计算机上运行）。
- `kics4net-postgresql` – DBMS 服务（仅在执行服务器功能的计算机上运行）
- `kics4net-report-builder` – 生成报告的服务（仅在执行服务器功能的计算机上运行）。
- `kics4net-report-data-source` – 为报告提供数据的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-report-renderer` – 用于在报告中直观显示数据块的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-report-templates-catalog` – 用于管理报告模板的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-report-templates-catalog-view` – 用于提供有关报告模板数据的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-responses-manager` – 用于管理响应作业的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-risk-oval-detector` – 使用 OVAL 规则处理设备风险扫描结果的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-scan-oval-manager` – 使用 OVAL 规则管理设备扫描的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-scap-manager` – 用于管理安全审计的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-scap-manager-view` – 用于提供安全审计数据的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-scheduler` – 任务调度服务（仅在执行服务器功能的计算机上运行）。
- `kics4net-secrets` – secret 存储库外观服务（仅在执行服务器功能的计算机上运行）
- `kics4net-task-manager` – 任务管理服务（仅在执行服务器功能的计算机上运行）
- `kics4net-task-manager-view` – 用于提供有关任务数据的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-telemetry-proxy` – 用于在 UDP 模式下与 EPP 应用程序集成的服务（在执行服务器或传感器功能的计算机上运行）。
- `kics4net-vault` – 用于在存储库中存储 secret 的服务（仅在执行服务器功能的计算机上运行）
- `kics4net-websensor` – 网络服务器服务（仅在执行探测器功能的计算机上运行）。

- `kics4net-webserver` – 网络服务器服务（仅在执行服务器功能的计算机上运行）。
- `klnagent` – 网络代理服务（仅在执行服务器功能的计算机上运行）。

示例

```
sudo service kics4net status
```

如果服务没有激活，您可以重新启动计算机或者重新启动服务。

重新启动安装了应用程序组件的计算机

重新启动执行服务器或探测器功能的计算机时，应用程序组件会自动启动。重启不会影响这些组件的后续操作（除了某些意外重启后出现故障的情况）。

以下情况下可能需要重新启动：

- 计算机硬盘上没有足够的可用空间。
- 计算机意外重启，此后应用程序组件的运行未恢复。
- 其中一个应用程序服务未处于活动状态。
- 服务器与探测器之间丢失的连接尚未恢复。在这种情况下，您应该重新启动执行探测器功能的计算机。

您可以使用操作系统的标准命令来重新启动已安装应用程序组件的计算机。

如果计算机由于某种原因无法重新启动，您可以重新启动支持应用程序组件运行的服务。

要重新启动服务：

1. 打开操作系统控制台。
2. 根据计算机执行的功能，执行以下操作：

   - 如果计算机执行服务器功能，请输入以下命令序列：

```
sudo service kics4net-postgresql restart
sudo service kics4net-config-control-orchestrator restart
sudo service kics4net-asset-inventory restart
sudo service kics4net-blob-storage restart
sudo service kics4net-email-gateway restart
sudo service kics4net-fts restart
sudo service kics4net-report-builder restart
sudo service kics4net-report-data-source restart
sudo service kics4net-report-renderer restart
sudo service kics4net-report-templates-catalog restart
sudo service kics4net-report-templates-catalog-view restart
sudo service kics4net-responses-manager restart
sudo service kics4net-risk-oval-detector restart
sudo service kics4net-scap-manager restart
sudo service kics4net-scap-manager-view restart
sudo service kics4net-scan-oval-manager restart
sudo service kics4net-scheduler restart
sudo service kics4net-secrets restart
sudo service kics4net-task-manager restart
sudo service kics4net-task-manager-view restart
sudo service kics4net-vault restart
sudo service kics4net-webserver restart
sudo service kics4net-asset-config-repo restart
sudo service kics4net-anomaly-hunter restart
sudo service kics4net-clickhouse restart
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-telemetry-proxy restart
sudo service kics4net-nats-server restart
sudo service kics4net-oval-facade restart
sudo service klnagent restart
```

   - 如果计算机执行探测器功能，请输入以下命令序列：

```
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-telemetry-proxy restart
sudo service kics4net-nats-server restart
sudo service kics4net-oval-facade restart
sudo service kics4net-websensor restart
```

使用测试网络数据包验证事件注册

要验证 Kaspersky Industrial CyberSecurity for Networks 中事件的注册情况，您可以使用测试网络数据包。当在流量中检测到此类数据包时，应用程序会根据以下技术注册测试事件：

- 深度包检测 无论是否存在过程控制规则或标记，都会注册事件。
- 网络完整性控制 无论是否存在交互控制规则，都会注册事件。必须启用网络完整性控制技术。
- 入侵检测 无论是否存在入侵检测规则，都会注册事件。必须启用基于规则的入侵检测。
- 资产管理 无论设备表中是否存在已知设备，都会注册事件。必须启用设备活动检测。

这些事件使用被分配了以下代码的系统事件类型进行注册。

- 4000000001 表示基于深度包检测技术的事件。
- 4000000002 表示基于网络完整性控制技术的事件。
- 4000000003 表示基于入侵检测技术的事件。
- 4000000004 表示基于资产管理技术的事件。

您可以在已注册事件表中查看测试事件。

为了验证审计功能，Kaspersky Industrial CyberSecurity for Networks 会在审计日志中保存有关测试事件注册的信息。为每个注册事件创建一个审计条目，该条目指定注册该测试事件所使用的技术。

测试网络数据包是一个带有某些参数值的 UDP 协议数据包。参数的定义方式是排除在正常工业网络流量中接收这种数据包的概率。

测试网络包的参数中必须定义以下数据：

- 以太网 II 标头：
  - 源 MAC 地址：`00:00:00:00:00:00`
  - 目的 MAC 地址：`ff:ff:ff:ff:ff:ff`
  - EtherType：`0x0800 (IPv4)`
- IP 标头：
  - 源 IP 地址：`127.0.20.20`
  - 目的 IP 地址：`127.0.20.20`
  - ID: `20`
  - TTL: `20`
  - 协议类型：`17（UDP）`
  - 标志：`0x00`
- UDP 标头：
  - 源端口：`20`
  - 目的端口：`20`
- 数据包内容：
  - 数据包内容的长度（以字节为单位）：`20`
  - 数据包内容：“`KICS4Net Sentinel 20`”

要生成并发送测试网络数据包，您可以使用网络数据包生成器程序，例如Scapy。您需要从其流量由 Kaspersky Industrial CyberSecurity for Networks 控制的节点发送测试网络数据包。

要使用 Linux® 操作系统中的 Scapy 程序发送测试网络数据包：

1. 在计算机的操作系统控制台中，输入命令以交互模式运行 Scapy：

```
sudo scapy
```

2. 输入发送测试网络包的命令：

```
sendp(
Ether(src='00:00:00:00:00:00', dst='ff:ff:ff:ff:ff:ff')/
IP(src='127.0.20.20', dst='127.0.20.20', id=20, ttl=20)/
UDP(sport=20, dport=20)/
"KICS4Net Sentinel 20",
iface="<接口名称>"
)
```

其中<接口名称>是连接到工业网络的网络接口的名称（例如，`eth0`）。

在流量中检测到数据包后，Kaspersky Industrial CyberSecurity for Networks 会注册测试事件。

正在检查应用程序模块的完整性

您可以检查已安装软件模块的完整性，以确保安装后这些模块没有更改。此检查是通过将已安装的应用程序模块的校验和与其参考值进行比较来执行的。完整性检查必须在承载已安装应用程序模块的每个节点上单独运行。

您可以通过以下方式对节点运行完整性检查：

- 使用 kics4net-manifest-checker-<应用程序版本>.bundle.sh 脚本在本地运行检查。
- 通过 Web 界面连接到服务器时运行。

使用脚本在本地运行完整性检查

kics4net-manifest-checker-<应用程序版本>.bundle.sh 脚本包含在 Kaspersky Industrial CyberSecurity for Networks 分发工具包中。该脚本根据存储在 *manifest 文件*中的特殊列表检查应用程序模块文件。manifest 文件包含在应用程序安装包中，并包含相应包的文件列表。每个应用程序包都有一个相应的 manifest 文件。manifest 文件经过数字签名，其完整性也得到验证。

如果您对 kics4net-manifest-checker-<应用程序版本号>.bundle.sh 脚本文件进行任何更改，其结果可能无效。要获得有效的结果，请仅使用 Kaspersky Industrial CyberSecurity for Networks 分发工具包中包含的脚本版本。

在运行时，脚本会依次检查操作系统中安装的应用程序包中的文件的校验和。

要使用 kics4net-manifest-checker-<应用程序版本>.bundle.sh 脚本检查节点计算机上应用程序模块的完整性：

1. 将脚本文件 kics4net-manifest-checker-<应用程序版本号>.bundle.sh 从包含未打包脚本文件的文件夹复制到任何文件夹。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。

2. 在操作系统控制台中，转到包含脚本文件的文件夹，然后输入以下命令：

   ```
   sudo bash kics4net-manifest-checker-<应用程序版本号>.bundle.sh
   ```

   有关检查结果的信息显示在操作系统控制台中。

如果满足以下两个条件，则认为计算机上的软件模块完整性检查结果是成功的：

- kics4net-manifest-checker-<应用程序版本号>.bundle.sh 脚本终止，并显示消息：`已成功检查包含 manifest 文件的已安装包的所有文件。`
- 应根据其正确功能安装在计算机上的所有应用程序包都不会返回错误消息，或者至少不会返回以下消息之一：
  - `该包未安装在操作系统中。`
  - `找不到包的 manifest 文件。`

通过 Web 界面连接到服务器时运行完整性检查

当通过 Web 界面连接到服务器时，您可以在节点上运行应用程序模块的完整性检查。以这种方式启动的完整性检查是使用与 kics4net-manifest-checker-<应用程序版本>.bundle.sh 脚本类似的方法执行的。

通过 Web 界面连接到服务器时，要检查节点计算机上应用程序模块的完整性：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 选择**设置** → **部署**。

3. 选择相关节点的图块。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击“**检查完整性**”。如果工具栏上未显示该按钮，请单击 ⋮ 按钮并在打开的菜单中选择所需的项目。

   您将看到一条消息，通知您已启动完整性检查，有关其进度的信息将在一段时间内显示在后台操作列表中。如有必要，您可以通过单击应用程序 Web 界面菜单中的 按钮来查看当前后台操作列表。

5. 要查看完整性检查结果，请转到“**设置**” → “**应用程序消息**”。

如果应用程序消息列表中包含相应节点的以下消息，则认为计算机上的应用程序模块完整性检查结果成功：`节点上应用程序模块的完整性检查已成功完成。`

如果应用程序消息列表不包括指示成功的完整性检查的消息，而是包含错误消息，则完整性检查被视为不成功。您可以使用 kics4net-manifest-checker-<应用程序版本>.bundle.sh 脚本（请参阅上文）来识别未通过完整性检查的应用程序包。

将 Kaspersky Industrial CyberSecurity for Networks 节点的时间与工业网络设备使用的时间源同步

为了正确地将事件的注册时间与事件在工业网络中发生的时间关联起来，系统中的时间必须同步。安装了 Kaspersky Industrial CyberSecurity for Networks 组件的节点的时间必须与工业网络设备使用的公共时间源同步。

当集中安装 Kaspersky Industrial CyberSecurity for Networks 时，您可以启用在服务器与安装探测器的节点之间自动进行时间同步。在这种情况下，安装服务器的节点将充当安装探测器的节点的时间源。建议使用执行服务器功能的计算机操作系统中的软件工具来配置服务器与工业网络中设备使用的公共时间源之间的时间同步。对于服务器时间同步，您可以使用称为网络时间协议 (NTP) 和精确时间协议 (PTP) 的标准协议。

NTP 用于服务器与其他节点之间的自动时间同步。在这种情况下，您无法配置与其他时间源的同步或在安装了探测器的节点上使用 PTP 协议。

如果使用 kics4net-install.sh 脚本在本地安装了探测器，则此节点上不会执行与服务器的自动时间同步。如果是这种情况，您必须在服务器和所有包含本地安装的探测器的节点上配置时间同步。

有关配置时间同步的操作示例序列，请参阅附录。

更新数据库和应用程序模块

Kaspersky Industrial CyberSecurity for Networks 提供更新以下数据库和应用程序模块的功能：

- 系统入侵检测规则。
- 网络异常检测规则模板。
- 用于处理工业过程控制目的的应用层协议的模块。
- 用于注册突发事件的事件关联规则。
- 用于获取有关设备和通信协议的信息的规则。
- 工业设备漏洞数据库。
- 卡巴斯基数字签名 (KDS) 证书吊销列表。
- 应用程序功能配置。
- 漏洞和合规性审计作业的规则系统集。
- OpenSSL 加密模块。
- 用于 SCADA 的卡巴斯基 ICS 证书漏洞数据库。
- 根据系统命令检测事件识别潜在攻击技术的方法。

安装卡巴斯基发布的更新后，应用程序模块和数据库会得到更新。

及时安装更新可确保最大程度的保护使用 Kaspersky Industrial CyberSecurity for Networks 的工业网络。此外，这些更新可以增强和更新涉及为应用程序提供安全性的应用程序模块。随着时间的推移，如果不定期安装更新，将会因新威胁的出现而增加应用程序安全的风险。您还必须为特定操作系统安装安全更新。

建议在安装 Kaspersky Industrial CyberSecurity for Networks 组件后立即手动开始安装更新。您可以配置自动计划启动设置以定期安装更新。

您可以使用以下更新源：

- 卡巴斯基更新服务器。
- Kaspersky Security Center 管理服务器。

对于更新源，如果手动启动更新安装，您还可以使用来自本地资源的文件。

当通过 Web 界面连接到服务器时，您可以配置设置并开始安装更新。

数据库和应用程序模块的更新受以下限制和特殊考虑约束：

- 更新功能在添加授权许可密钥后可用。有效安全审计授权许可密钥可用于更新所有应用程序模块和数据库。如果添加的是更新和支持授权许可密钥，则应用程序不会激活用于更新漏洞和合规性审计任务的系统规则集的功能。

  该软件的更新功能（包括提供反病毒签名更新和代码库更新）可能无法在美国境内使用。

- 安装 OpenSSL 库更新后，请在已安装应用程序组件的节点上重新启动服务。
- 要从卡巴斯基更新服务器下载更新，您必须可以访问互联网。当从执行 Kaspersky Industrial CyberSecurity for Networks 服务器功能的计算机连接到更新服务器时，连接通过 HTTPS 协议建立（不支持通过代理服务器连接）。
- 要从 Kaspersky Security Center 管理服务器下载更新至 Kaspersky Industrial CyberSecurity for Networks 服务器，必须添加应用程序与 Kaspersky Security Center 交互的功能。您可以在安装或重新安装 Kaspersky Industrial CyberSecurity for Networks 期间添加此功能。更新从管理服务器存储库下载，该存储库通过 Kaspersky Security Center 中的相应任务获取其更新。

手动启动更新

您可以随时运行更新。添加授权许可密钥后即可运行更新。

只有具有管理员角色的用户才能手动启动更新。

要手动开始更新：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **更新**。

3. 在**手动更新源**下，选择以下更新源选项之一：

   - 本地更新源 – 可让您通过特定的本地路径从文件下载更新。您可以单击**浏览**指定文件的本地路径。
   - **卡巴斯基更新服务器**– 用于从卡巴斯基更新服务器下载更新。
   - **Kaspersky Security Center 管理服务器**– 用于从 Kaspersky Security Center 管理服务器下载更新。如果已添加应用程序与 Kaspersky Security Center 交互的功能，则此选项可用。

4. 单击**立即更新**。

配置自动更新

添加授权许可密钥后，您可以按计划配置自动更新。

只有具有管理员角色的用户才能配置按计划进行自动更新。

要按计划启用和配置自动更新：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **更新**。
3. 使用**根据计划运行更新**切换按钮来启用自动更新。
4. 在**计划更新的源**下，选择以下更新源选项之一：

   - **卡巴斯基更新服务器**– 用于从卡巴斯基更新服务器下载更新。
   - **Kaspersky Security Center 管理服务器**– 用于从 Kaspersky Security Center 管理服务器下载更新。如果已添加应用程序与 Kaspersky Security Center 交互的功能，则此选项可用。

5. 定义更新计划设置。为此：

   a. 在**频率**下拉列表中，定义更新必须发生的时间。选择以下选项之一：**每小时**、**每天**、**每周**或**每月**。

   b. 根据所选的选项，指定定义精确的更新运行计划的设置值。

6. 单击**保存设置**。

查看有关更新安装的信息

您可以查看有关更新安装的常规信息和详细信息。

有关已安装更新的常规信息

常规信息提供已更新应用程序模块和数据库的发布日期和时间。

要查看有关已安装更新的常规信息：

在应用程序 Web 界面页面上，选择**关于**部分。

有关更新安装的详细信息

详细信息包含有关已启动的更新安装进程的信息。应用程序保存以下详细信息：

- 更新进程启动的日期和时间
- 更新运行模式
- 更新过程中安装的数据库和应用程序模块的发布日期和时间（如果更新成功）
- 错误信息（如果更新失败）
- 更新的数据库和应用程序模块列表

有关更新安装的详细信息保存在应用程序消息日志中。

安装 OpenSSL 库更新后重新启动节点上的服务

如果在安装应用程序组件的节点上安装了 OpenSSL 库更新，请重新启动确保这些节点上应用程序组件运行的服务。传感器节点上的服务将自动重新启动。如果需要重新启动服务器节点上的服务，则应用程序会在服务器 Web 界面页面上显示有关该服务的通知。在这种情况下，要重新启动服务，您可以重新启动服务器计算机或在 Web 界面页面上启动重新启动。

关于需要重新启动服务器节点上的服务的通知显示在关于应用程序操作中的问题的通知列表中，以及“**设置**”→“**更新**”下。

只有具有管理员角色的用户才能在 Web 界面页上启动服务器服务的重新启动。

要使用服务器 Web 界面重新启动服务器节点上的服务，请执行以下操作：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **更新**。
3. 在“**需要重新启动**”通知中，单击“**重新启动服务器**”。

   服务重新启动过程开始。在重新启动过程完成之前，应用程序服务器不可用于连接。在服务重新启动过程中，应用程序 Web 界面页面会显示一个名为“**应用程序维护**”的特殊部分。

分配对应用程序功能的访问权限

在 Kaspersky Industrial CyberSecurity for Networks中，您可以根据特定用户的任务限制用户对应用程序功能的访问。

以下用户账户可用于访问该应用程序：

- 在应用程序中创建的用户账户。
- 为单点登录 (SSO) 配置的 Kaspersky Security Center 用户账户。

无法使用其他用户账户或匿名连接来连接到服务器。

有权访问该应用程序的用户账户不必在服务器计算机上注册为操作系统用户账户。

在 Kaspersky Industrial CyberSecurity for Networks 的启动配置期间，必须创建第一个应用程序用户账户。然后，您可以创建用于在应用程序中执行操作的其他用户账户。

根据您通过 Web 界面连接的组件，可以使用以下功能集：

- 连接到服务器时的应用程序功能
- 连接到探测器时的应用程序功能

当连接到服务器时，应用程序根据建立连接的用户角色提供对功能的访问。

关于应用程序用户账户

基于角色的访问控制 (RBAC) 用于限制对应用程序功能的访问。应用程序用户账户的角色决定了用户可以执行的操作集。为应用程序用户账户提供了以下角色：

- **管理员**。

  拥有此角色的用户拥有管理应用程序、管理其运行、执行监控和查看信息所需的所有访问权限。该用户还可以访问管理在应用程序中创建的用户账户的功能。

- **安全官**。

  建议将此角色分配给负责工业设施安全的员工。拥有此角色的用户拥有监控系统和管理已注册事件和事件所需的访问权限。该用户有权在应用程序中发起响应操作。

- **基础设施专家**。

  建议将此角色分配给负责工业设施基础设施（网络设备、工作站等）的员工。拥有此角色的用户拥有接收有关设备及其交互的信息以及配置允许规则所需的访问权限。

- **ICS 专家**。

  建议将此角色分配给负责工业设施控制系统操作的员工。拥有此角色的用户拥有监控工业网络资产和设备相关风险所需的访问权限。为了更新员工有关设备、SCADA 和 PLC 项目的可用信息，该用户能够配置和运行安全审计作业。

- **操作员**。

  建议将此角色分配给担任安全系统操作员的员工。拥有此角色的用户拥有监控和查看信息所需的最低访问权限。该用户还可以根据事件和事故的处理结果，为其分配“活动”状态。

管理员角色被分配给在应用程序启动配置期间创建的第一个用户账户。

在添加后续用户账户时，您可以为其分配适当的角色。您可以为应用程序的用户创建最多 100 个用户账户（不包括配置了单点登录的 Kaspersky Security Center 用户）。

当连接到服务器时，用户将获得与其用户账户角色相对应的访问权限。如果应用程序用户的角色在用户工作时被另一个用户（已被分配管理员角色）更改，则所连接用户的访问权限将以在线模式更新。例如，以管理员角色连接到服务器的用户在为其用户账户分配操作员角色后将失去访问应用程序管理功能的权限。

只有具有管理员角色的用户才能管理用户账户并查看其信息。有关在应用程序中创建的用户账户的信息显示在 Kaspersky Industrial CyberSecurity for Networks Web 界面的“**设置**” → “**用户**”下。

通过 Web 界面连接到服务器时可用的应用程序功能

本文介绍了用户通过 Web 界面连接到服务器时可用的应用程序功能（见下表）。

根据用户角色可用的应用程序功能

应用程序功能	管理员	安全官	基础设施官	ICS 官	操作员
当通过 Web 界面连接时监控应用程序状态	✓	✓	✓	✓	✓
查看应用程序消息	✓	✓	✓	✓	✓
启用和禁用用户活动审计	✓				
查看用户活动审计条目	✓				
查看已安装应用程序组件的节点以及节点上的网络接口的信息	✓	✓	✓	✓	✓
通过 Web 界面连接到服务器时运行应用程序模块完整性检查	✓	✓			
添加和删除传感器	✓				
更改主节点设置	✓				
管理节点上的监控点	✓				
管理技术	✓	✓			
下载节点监控点收到的流量	✓	✓	✓	✓	✓
查看有关添加的授权许可密钥的信息	✓	✓	✓	✓	✓
添加授权许可密钥	✓				
删除授权许可密钥	✓				
配置自动更新	✓				
手动启动更新	✓				
查看有关更新安装的信息	✓	✓	✓	✓	✓
查看有关应用程序用户账户的信息	✓				
创建应用程序用户账户	✓				
更改应用程序用户账户的角色	✓				
管理员发起的密码更改	✓				
管理用户锁定	✓				
删除应用程序用户账户	✓				
更改您的账户密码	✓	✓	✓	✓	✓
查看数据表时的功能	✓	✓	✓	✓	✓
查看设备信息	✓	✓	✓	✓	✓
选择设备漏洞监控的来源	✓	✓			
配置地址空间	✓	✓	✓		
手动添加设备	✓	✓	✓	✓	
合并设备	✓	✓	✓	✓	

应用程序功能	管理员	安全官	基础设施官	ICS 官	操作员
删除设备	✓	✓	✓	✓	
更改设备状态	✓	✓	✓	✓	
创建设备组树	✓	✓	✓	✓	
根据特定标准自动分组设备	✓	✓	✓	✓	
手动将设备分组	✓	✓	✓	✓	
添加和删除设备标签	✓	✓	✓	✓	
编辑设备信息	✓	✓	✓	✓	
添加、编辑和删除设备的自定义字段	✓	✓	✓	✓	
删除设备用户	✓	✓			
删除设备可执行文件	✓	✓			
分配黄金设备配置	✓	✓	✓	✓	
保存的设备配置比较	✓	✓	✓	✓	✓
正在重置设备网络行为的偏差	✓	✓	✓	✓	✓
查看地址空间规则	✓	✓	✓	✓	✓
查看地址空间子网	✓	✓	✓	✓	✓
查看所选子网中具有 IP 地址的设备的信息	✓	✓	✓	✓	✓
管理设备的过程控制设置	✓	✓	✓	✓	
管理标签	✓	✓		✓	
管理过程控制规则	✓	✓		✓	
监控过程参数值	✓	✓	✓	✓	✓
在允许规则表中查看交互控制规则	✓	✓	✓	✓	✓
针对单个设备进行微调交互控制	✓	✓	✓	✓	
手动创建交互控制规则	✓	✓	✓	✓	
编辑交互控制规则设置	✓	✓	✓	✓	
启用和禁用交互控制规则	✓	✓	✓	✓	
暂停和恢复设备网络交互的监控	✓	✓	✓	✓	
删除交互控制规则	✓	✓	✓	✓	
启用和禁用入侵检测规则集	✓	✓			
加载和替换用户定义的入侵检测规则集	✓	✓			
删除用户定义的入侵检测规则集	✓	✓			
管理网络异常检测规则	✓	✓			
管理网络异常检测规则字典	✓	✓			
管理在数据库中存储日志条目的设置	✓				
管理在数据库中保存流量的设置	✓				
管理保存流量转储文件的设置	✓				
管理存储报告文件的设置	✓				
更改进程的日志记录级别	✓				
使用 EPP 应用程序配置操作	✓				
管理响应操作	✓	✓			
启用并配置与 Kaspersky Security Center 的交互	✓				
管理连接器	✓				

应用程序功能	管理员	安全官	基础设施官	ICS 官	操作员
添加和删除连接器类型	✓				
管理漏洞和合规性审计作业	✓	✓	✓	✓	
接收漏洞和合规性审计作业报告	✓	✓	✓	✓	✓
查看有关漏洞和合规性审计作业运行的常规信息	✓	✓	✓	✓	✓
管理漏洞和合规性审计作业运行的存储设置	✓				
管理漏洞和合规性审计作业的规则集	✓	✓			
管理配置控制作业	✓	✓	✓	✓	
查看有关配置控制作业运行的常规信息	✓	✓	✓	✓	✓
管理主动设备轮询作业	✓	✓	✓	✓	
查看有关主动轮询作业运行的一般信息	✓	✓	✓	✓	✓
管理远程连接的账户凭据 Secret	✓	✓	✓	✓	
配置事件类型	✓				
更改风险类型的基本分数	✓				
管理存储风险的设置	✓				
将安全策略导出到文件	✓	✓	✓	✓	✓
从文件中导入安全策略	✓				
清除当前安全策略	✓				
实时系统监控	✓	✓	✓	✓	✓
使用网络交互图	✓	✓	✓	✓	✓
将节点和组移动到网络交互图上的其他组	✓	✓	✓	✓	
使用网络交互图时下载流量	✓	✓	✓	✓	✓
查看网络会话详细信息	✓	✓	✓	✓	✓
下载网络会话流量	✓	✓	✓	✓	✓
形成拓扑图	✓	✓	✓	✓	
查看拓扑图上对象的详细信息	✓	✓	✓	✓	✓
监控事件和突发事件	✓	✓	✓	✓	✓
管理报告和报告模板	✓	✓			
手动生成报告	✓	✓	✓	✓	✓
将报告导出到文件	✓	✓	✓	✓	✓
查看风险详细信息	✓	✓	✓	✓	✓
手动更改风险状态	✓	✓	✓	✓	

查看有关应用程序用户账户的信息

通过 Web 界面连接到服务器时，您可以查看有关在应用程序中创建的用户账户的信息。该应用程序不显示有关配置了单点登录 (SSO) 的 Kaspersky Security Center 用户账户的信息。

只有具有管理员角色的用户才能查看用户账户信息。

要查看有关应用程序用户账户的信息：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**用户**”。

   该表显示符合过滤和搜索条件的用户。

以下列显示用户设置：

- **名称**
  指定的用户名
- **角色**。
  指定的用户角色
- **状态**
  用户当前状态。可使用以下状态：
  - **已允许**：该账户尚未被管理员锁定，或者该账户已被解锁。
  - **已阻止**：该账户已被管理员锁定。

    应用程序仅在管理员执行操作后才会将账户状态设置为**已阻止**。暂时限制某个账户通过 Web 界面连接到服务器不会导致该账户的状态成为“**已阻止**”。
  - **可疑活动**：用户连续多次输入错误的账户密码。
- **创建日期**
  将用户添加到应用程序的日期和时间。
- **更改时间**
  上次修改用户设置的日期和时间。

查看用户表时，您可以使用配置、过滤、搜索和排序。

创建应用程序用户账户

只有具有管理员角色的用户才能创建应用程序用户账户。

要创建应用程序用户账户：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**用户**”。
3. 单击“**添加用户**”打开详细信息。
4. 在用户名输入字段中，输入要创建的账户的用户名。

您可以使用英文大写和小写字母、数字、点以及 _ 和 - 字符。
用户账户名称必须符合以下要求：

- 在应用程序用户名列表中必须是唯一的（不区分大小写）。
- 必须包含 3 至 20 个字符。
- 必须以字母开头。
- 必须以除点之外的任何受支持的字符结尾。

5. 在下拉列表中，选择必要的用户角色。
6. 在密码输入字段中，输入您要为用户账户设置的密码。
密码必须符合以下要求：
   - 必须包含 8 到 256 个 ASCII 字符。
   - 必须包含一个或多个英语字母的大写字母。
   - 必须包含一个或多个拉丁字母的小写字母。
   - 必须包含一个或多个数字。
   - 不得包含超过三个连续重复的字符。
7. 如果您希望用户在第一次连接应用程序时更改密码，请选中“**下次登录时需要更改密码**”复选框。
8. 单击**保存**。

用户表中将出现一个新用户账户。

更改应用程序用户账户的角色

通过 Web 界面连接到服务器时，您可以更改在应用程序中创建的用户账户的角色。此角色修改方法不适用于配置了单点登录 (SSO) 的 Kaspersky Security Center 用户账户。

只有具有管理员角色的用户才能更改用户账户的角色。

具有管理员角色的用户可以更改任何用户账户的角色，但不能更改其自己的用户账户的角色。

要更改应用程序用户账户的角色：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**用户**”。
3. 选择您想要更改其角色的用户。
详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击“**编辑**”。

5. 在下拉列表中，选择必要的用户账户角色。

6. 单击“**保存**”。

管理员发起的密码更改

管理员可以为任何其他用户设置新的密码。要更改自己的密码，管理员和其他用户一样，必须遵循密码更改程序。

管理员只能为在应用程序中创建的账户设置新的密码。此密码更改方法不适用于配置了单点登录 (SSO) 的 Kaspersky Security Center 用户账户。

我们建议在以下情况下更改用户密码：

- 用户账户已解锁。
- 密码已被泄漏。
- 该账户已被分配“**可疑活动**”状态，或者 Web 界面菜单顶部会显示用户登录尝试失败的通知。

要为账户设置新密码：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**用户**”。
3. 选择您要为其设置新密码的用户。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**设置新密码**。如果工具栏上未显示该按钮，请单击 ⋮ 按钮并在打开的菜单中选择所需的项目。
   出现**更改用户密码**窗口。
5. 在“**新密码**”和“**重新输入新密码**”字段中输入新的密码。
   新的密码必须符合“**更改用户密码**”中列出的要求。当您输入密码时，您所满足的条件会被自动标记。
6. 如果您希望用户在下次连接应用程序时更改密码，请选中**下次登录时需要更改密码**复选框。
7. 在“**确认密码**”字段中输入您的密码。
8. 单击**保存**。

用户下次通过 Web 界面连接时将需要新的密码。

管理用户锁定

管理员可以锁定任何其他用户的账户。一旦解决了管理员发起的锁定的原因，管理员就可以解锁账户。

当账户被锁定时，应用程序会重置密码到期日期并终止用户的当前会话。一旦账户解锁，密码到期日期仍被重置。因此，解锁后，用户需要设置新的密码。

解锁用户账户后，我们建议立即设置新密码，以防止恶意的操作者猜测旧密码并劫持解锁的账户。管理员可以设置新密码或监督用户计算机上的密码更改。

管理员只能锁定或解锁在应用程序中创建的账户。已配置单点登录 (SSO) 的 Kaspersky Security Center 用户账户无法执行这些操作。

要锁定用户账户：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**用户**”。
3. 选择您要锁定的用户。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**阻止**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，单击**确定**。

要解锁先前被管理员锁定的用户：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**用户**”。
3. 选择您要解锁的用户。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**解除阻止**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，单击**确定**。

删除应用程序用户账户

通过 Web 界面连接到服务器时，您可以删除在应用程序中创建的用户账户。此删除方法不适用于配置了单点登录 (SSO) 的 Kaspersky Security Center 用户账户。

只有具有管理员角色的用户才能删除应用程序用户账户。

具有管理员角色的用户可以删除除他们自己的用户账户之外的任何用户账户。

要删除应用程序用户账户：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**用户**”。

3. 选择您要删除的用户。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**删除**。如果工具栏上未显示该按钮，请单击⋮按钮并在打开的菜单中选择所需的项目。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，单击**确定**。

配置资产管理

Kaspersky Industrial CyberSecurity for Networks 让您可以监控以工业网络设备为代表的公司资产。应用程序根据设备的 MAC 地址和/或 IP 地址来识别设备。应用程序可以在执行以下操作时接收设备数据：

- 处理通过监控点到达的流量
- 处理从EPP 应用程序收到的数据

创建设备表是为了在应用程序中进行资产管理。该表根据应用程序中配置的地址空间进行填充。

应用程序可以自动获取有关设备的信息。只有能被应用程序识别的信息才会被自动获取和更新（例如，设备的地址信息）。

为了检测设备活动并自动更新信息，必须启用相应的资产管理方法。如有必要，您可以手动指定特定数据的值并禁用其自动更新以锁定当前值（例如，如果当前定义的类别与自动确定的类别不同，则可以锁定设备类别）。

某些设备信息必须手动指定，因为它无法自动更新。例如，您可以在设备表中保存特定的设备信息，添加任何缺少的设备排序和筛选标准。您还可以使用手动定义的信息将设备排列在组树中的各个组中，或者根据设备标签过滤和搜索设备。

您可以在“**设备**”选项卡的“**资产**”部分配置资产管理和编辑设备信息。您还可以在使用网络交互图和拓扑图时查看有关设备之间交互的信息，并对设备执行各种操作。为了方便地呈现设备之间的交互信息并实现按子网自动分组设备，您可以根据公司网络中设备的具体 IP 寻址在地址空间中生成子网列表。

资产管理方法与模式

Kaspersky Industrial CyberSecurity for Networks 使用以下方法进行资产管理：

- 设备活动检测 此方法允许您根据获得的设备的 MAC 和/或 IP 地址来监控工业网络流量中设备的活动。
- 设备信息检测 此方法可让您使用从流量或其他来源收到的数据作为基础，自动获取和更新有关应用程序已知的设备的信息。
- PLC 项目控制。此方法使您能够检测流量中有关 PLC 项目的信息，将这些信息保存在应用程序中，并将其与以前获得的信息进行比较。
- 风险检测。此方法使您能够根据有关设备及其交互的信息来检测信息安全风险。
- 网络会话检测。此方法分析工业网络流量以检测设备为连接其他设备而创建的网络会话。

您可以启用或禁用单独的资产管理方法。

关于设备活动检测方法

设备活动检测方法有以下几种模式：

- 学习模式。此模式仅供临时使用。在这种模式下，所有在流量中检测到活动的设备都被视为获得应用程序的授权。您只能为设备活动检测方法启用学习模式。设备活动检测方法可以与其他资产管理方法一起应用。
- 监控模式。此模式适合持续使用。在这种模式下，当检测到设备活动时，应用程序仅将那些已分配“*已授权*”状态的设备视为已授权。

根据所选的模式，应用程序自动为设备分配状态。

在学习模式下，当应用程序检测到设备活动或设备信息自动更新时，它不会注册事件。

您可以配置设备活动检测方法的学习模式。必须启用资产管理学习模式足够长的时间来检测相关设备的活动。这个时间取决于工业网络中的设备数量以及它们的运行和维修频率。我们建议您启用学习模式至少一个小时。在大型工业网络中，可以启用学习模式一段时间（从一天到几天），以检测所有必需设备的活动。

接收到的设备 MAC 地址和 IP 地址会经过以下特殊考虑进行处理：

- 对于起到工业网段之间网络交换机功能的设备，必须设置路由器指示器。如果应用程序未自动定义该指示器，则必须手动设置。否则，应用程序可能无法使用通过此路由设备在不同工业网络段中交互的设备填充设备表。设置指示器后，当有相应的流量涉及到交互设备时，交互设备将被添加到设备表中。
- 如果在流量中仅检测到设备 IP 地址（该 IP 地址无法与特定的 MAC 地址匹配），则会根据应用程序已知的子网列表检查该 IP 地址。设备活动检测方法仅忽略属于“**公共**”子网的 IP 地址。

关于设备信息检测方法

当启用设备信息检测方法时，应用程序会自动更新已知设备的信息。例如，当应用程序检测到设备流量中的更新数据时，它可以更新设备上安装的操作系统的名称。

默认情况下，所有信息均启用自动更新。对于某些类型的信息，您可以在设备设置中在以下情况下禁用自动更新：手动添加设备、合并设备和更改设备信息。

为了自动获取有关设备的信息，应用程序可以使用：

- 内置的*用于检测设备和设备通信协议信息的规则*。

  安装后，应用程序使用默认规则来识别有关设备的信息以及设备之间的通信协议。为了提高识别信息的精确性，卡巴斯基专家会定期更新包含规则集的数据库。您可以通过安装更新来更新规则。

- 来自 EPP 应用程序的数据包含有关设备的信息。

  应用程序处理来自 EPP 应用程序的数据，其中包含有关设备的信息（例如，部件信息）。

- 根据来自“*Kaspersky ICS CERT vulnerabilities database for SCADA*”的规则处理来自 EPP 应用程序的数据。

  来自“Kaspersky ICS CERT vulnerabilities database for SCADA”的规则可以对从 EPP 应用程序收到的数据进行额外分析。根据分析结果，应用程序可以间接确定有关设备的一些信息（例如，设备类别）。“**用于 SCADA 的卡巴斯基 ICS CERT 漏洞数据库**”是一套基于系统的安全审计规则。这些规则集与数据库和应用程序模块更新一起提供和更新。因此，要使用此集合中的规则，请安装更新。

关于应用方法时注册的事件

在监控模式下，应用程序根据资产管理技术注册相应的事件。根据所应用的方法，可以在以下情况下注册事件：

- 检测未知设备或状态为*已存档*的设备的活动。
- 设备信息的自动更改。
- 检测项目和 PLC 项目块的读/写操作。
- 检测漏洞风险以及与这些风险相关的变化。

当启用“PLC 项目控制”时，应用程序可能会注册大量与检测项目或块的读/写操作相关的事件。通常，使用此方法时，初始阶段会注册大量事件。为了减少注册事件的总数，应用程序安装后默认禁用 PLC 项目控制方法。您可以随时启用此方法。

选择漏洞数据的来源

在监控风险时，应用程序通过使用已知漏洞数据库中的信息来检测设备的漏洞。卡巴斯基专家将各种数据源的漏洞信息上传到数据库。

默认情况下，应用程序根据从所有来源上传到数据库的信息来检测设备的漏洞。如果需要，您可以选择相关来源，仅根据这些来源的信息来检测设备的漏洞。

只有具有管理员或安全官角色的用户才能选择设备漏洞检测源。

要启用或禁用使用源进行漏洞检测：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**风险**”部分中，单击“**漏洞源**”以打开用于选择来源的窗口。
3. 启用或禁用特定来源的使用。该列表包含已知漏洞数据库中的所有来源。
4. 单击“**应用**”。

手动添加设备

本节提供有关手动添加设备的说明。您可以手动将新设备添加到设备表中。对于添加的设备，您必须指定其 MAC 地址和/或 IP 地址。

> 添加的设备的 MAC 地址和 IP 地址在包含这些地址的地址空间内必须是唯一的。如果向应用程序添加了额外的地址空间，则可以将具有相同地址的设备添加到不同的地址空间。

具有除操作员角色之外的任何角色的用户都可以手动添加设备。

添加设备后，您可以为该设备添加过程控制设置。

使用设备表时添加设备

要添加设备到设备表：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**设备**部分的**资产**选项卡上，单击**添加设备**打开详细信息区域。

3. 在详细信息区域的**设置**选项卡上，在标识设备信息的字段中指定相关值。

4. 在详细信息区域中的**地址信息**选项卡上，指定设备的 MAC 和/或 IP 地址。

5. 如果向应用程序添加了额外的地址空间，请指定地址的地址空间的名称。

6. 您可以为设备的同一个网络接口指定多个 IP 地址。要生成 IP 地址列表，请执行以下操作之一：

   - 如果要添加 IP 地址，请单击**添加 IP 地址**。
   - 如果要删除 IP 地址，请单击位于包含 IP 地址的字段右侧的图标。

7. 如果设备有多个网络接口，请生成设备的网络接口列表并为它们指定相应的 MAC 和/或 IP 地址。

   为此，请执行以下操作之一：

   - 如果要添加网络接口，请单击设备最后一个网络接口的设置组下的**添加接口**。
   - 如果要删除网络接口，请单击设备网络接口名称右侧显示的图标（如果有两个或更多网络接口）。
   - 如果要为网络接口定义不同的名称，请单击位于当前名称右侧的图标，然后在打开的字段中输入网络接口的新名称。

8. 在详细信息区域中的**设置**和**地址信息**选项卡上，启用或禁用设备相关信息的自动更新。为此，请使用和图标。在**设置**选项卡上，和图标位于字段的左侧。在**地址信息**选项卡上，和图标位于网络接口名称的右侧。

9. 在详细信息区域的**自定义字段**选项卡上，根据需要创建自定义字段列表。

10. 单击**保存**。

    如果在设备设置中未指定所有必需的信息或定义了无效值，则此按钮不可用。包含需要更正值的设置的选项卡以图标标记。

设备表将显示状态为“*已授权*”的新设备。

使用拓扑图时添加设备

使用拓扑图时，您可以将新设备添加到设备表中。

使用拓扑图时将新设备添加到设备表：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**拓扑图**部分的**网络地图**选项卡上的**添加节点**下拉列表中，选择**新建设备**。

   窗口右侧将显示一个包含设备设置的详细信息区域。

3. 在详细信息区域的**设置**选项卡上，在标识设备信息的字段中指定相关值。

4. 在详细信息区域中的**地址信息**选项卡上，指定设备的 MAC 和/或 IP 地址。

5. 如果向应用程序添加了额外的地址空间，请指定地址的地址空间的名称。

6. 您可以为设备的同一个网络接口指定多个 IP 地址。要生成 IP 地址列表，请执行以下操作之一：

   - 如果要添加 IP 地址，请单击**添加 IP 地址**。
   - 如果要删除 IP 地址，请单击位于包含 IP 地址的字段右侧的图标。

7. 如果设备有多个网络接口，请生成设备的网络接口列表并为它们指定相应的 MAC 和/或 IP 地址。

   为此，请执行以下操作之一：

   - 如果要添加网络接口，请单击设备最后一个网络接口的设置组下的**添加接口**。
   - 如果要删除网络接口，请单击设备网络接口名称右侧显示的图标（如果有两个或更多网络接口）。
   - 如果要为网络接口定义不同的名称，请单击位于当前名称右侧的图标，然后在打开的字段中输入网络接口的新名称。

8. 在详细信息区域中的**设置**和**地址信息**选项卡上，启用或禁用设备相关信息的自动更新。为此，请使用和图标。在**设置**选项卡上，和图标位于字段的左侧。在**地址信息**选项卡上，和图标位于网络接口名称的右侧。

9. 在详细信息区域的**自定义字段**选项卡上，根据需要创建自定义字段列表。

10. 单击**保存**。

    如果在设备设置中未指定所有必需的信息或定义了无效值，则此按钮不可用。包含需要更正值的设置的选项卡以图标标记。

设备表将显示状态为“*已授权*”的新设备。

根据网络交互图上的未知设备节点添加设备

当使用网络交互图时，您可以使用代表对应用程序未知的设备的节点将新设备添加到设备表中。

要将未知设备的节点添加到设备表：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**网络交互图**部分的**网络地图**选项卡上，选择代表对应用程序未知的设备的相关节点。

   详细信息区域出现在 Web 界面窗口的右侧。

3. danji **添加到设备表**。

   详细信息区域将显示用于配置新设备设置的选项卡。

4. 配置新设备的设置，无需更改为节点指定的 MAC 地址和/或 IP 地址。

   有关如何配置这些设置的说明，请参阅使用设备表时手动添加设备的过程。

5. 单击**保存**。

设备表将显示状态为"*已授权*"的新设备。以前代表对应用程序未知的设备的节点现在将代表网络交互图上的设备。

根据拓扑图上非管理交换机添加设备

当使用拓扑图时，您可以使用代表非管理交换机的节点将新设备添加到设备表中。

要将非管理交换机的节点添加到设备表：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**拓扑图**部分的**网络地图**选项卡上，选择代表非管理交换机的相关节点。

   详细信息区域出现在 Web 界面窗口的右侧。

3. danji **添加到设备表**。

   详细信息区域将显示用于配置新设备设置的选项卡。

4. 指定设备的 MAC 地址和/或 IP 地址并配置所有其他设置。

   有关如何配置这些设置的说明，请参阅使用设备表时手动添加设备的过程。

5. 单击**保存**。

设备表将显示状态为"*已授权*"的新设备。先前代表非管理交换机的节点现在将代表拓扑图上的已知设备。

正在合并设备

工业设备、服务器和工作站可能具有多个网络接口，用于冗余或在不同网段运行。这些网络接口的地址通常会被设备在不同时间使用。因此，如果在流量中检测到这些地址，应用程序可能会添加多个具有不同网络接口的设备，而不是单个设备。此外，应用程序可能并非总能匹配流量中某个设备的网络接口的 IP 和 MAC 地址，这也会导致具有这些地址的不同设备被添加到设备表中。

针对这种情况，应用程序提供了设备合并功能。这样，您只需控制一个设备，而不是之前添加的多个设备。设备可以自动合并，也可以手动合并。仅当"设备活动检测"方法在学习模式下启用，并且满足特定条件时，设备才能自动合并；因此，在某些情况下，设备只能手动合并。您可以在使用设备表或网络地图时合并设备。

要定义要在应用程序中合并的设备，您可以使用过程控制系统随附文档中提供的地址信息来搜索设备（例如，在详细的网络设计规范或 HMI 和 PLC 系统的配置中）。

要将多台设备合并到一台设备中，新的设备中的网络接口总数不得超过 512 个。

具有除操作员角色之外的任何角色的用户都可以手动合并设备。

使用设备表时合并设备

合并设备表中的设备：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

3. 在**设备**选项卡上，选择要合并的设备。

4. 单击**合并设备**。

   窗口右侧将显示详细信息区域，其中包含用于配置新设备设置的选项卡。

5. 检查新设备的设置，并根据需要进行编辑：

   - 在详细信息区域的**设置**选项卡上，选定设备中包含冲突值的所有字段都会被有关冲突值的消息标记。在这种情况下，文本字段中的不同值将合并为一个值（例如，包含设备名称的字段）。
   - 在详细信息区域的**地址信息**选项卡上，所选设备的 MAC 地址和 IP 地址由各个网络接口分配。如有必要，请更改地址、地址空间和网络接口名称的值。
   - 详细信息区域中的**自定义字段**选项卡上的列表包含所选设备的所有自定义字段。

6. 检查需要重新启用自动更新的特定设备信息。如果已禁用自动更新，请启用必要设置的自动更新。

   例如，建议您启用包含设备硬件和软件版本值的设置的自动更新，因为这些值是在检测设备漏洞时使用的特定值。因此，及时更新此类信息对于通过应用程序进行风险管理至关重要。

   已禁用自动更新的设置由 图标标识。启用自动更新后，该设置由 图标标识。

7. 单击**合并**。

   将打开一个带有确认提示的窗口。

8. 在提示窗口中，单击**确定**。

设备表将显示状态为“*已授权*”的新设备。

使用网络交互图和拓扑图时合并设备

使用网络交互图和拓扑图时，您可以将图上的多个节点合并为设备表的一个新设备。

您可以单个选择相关节点，也可以将其作为包括相关设备的折叠组的一部分进行选择。如果选择了折叠的组，则任何嵌套级别的子组中的所有设备也将被包括在设备选择中。

WAN 节点无法合并。

要合并图上节点所代表的设备：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择**网络地图**部分。

3. 在“**网络交互图**”或“**拓扑图**”选项卡上，选择代表节点和/或折叠组的几个对象。

   要选择多个节点和/或组，请执行以下操作之一：

   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。

4. 单击**合并设备**。

   窗口右侧将显示详细信息区域，其中包含用于配置新设备设置的选项卡。

5. 检查新设备的设置，并根据需要进行编辑：

   - 在详细信息区域的**设置**选项卡上，选定设备中包含冲突值的所有字段都会被有关冲突值的消息标记。在这种情况下，文本字段中的不同值将合并为一个值（例如，包含设备名称的字段）。
   - 在详细信息区域的**地址信息**选项卡上，所选设备的 MAC 地址和 IP 地址由各个网络接口分配。如有必要，请更改地址、地址空间和网络接口名称的值。
   - 详细信息区域中的**自定义字段**选项卡上的列表包含所选设备的所有自定义字段。

6. 检查需要重新启用自动更新的特定设备信息。如果已禁用自动更新，请启用必要设置的自动更新。

   例如，建议您启用包含设备硬件和软件版本值的设置的自动更新，因为这些值是在检测设备漏洞时使用的特定值。因此，及时更新此类信息对于通过应用程序进行风险管理至关重要。

   已禁用自动更新的设置由 图标标识。启用自动更新后，该设置由 图标标识。

7. 单击**合并**。

   将打开一个带有确认提示的窗口。

8. 在提示窗口中，单击**确定**。

设备表将显示状态为“*已授权*”的新设备。网络地图将显示一个合并的节点，而不是之前选择的多个节点。

正在删除设备

本节提供有关移除设备的说明。您可以从设备表中删除一个或多个设备。

具有除操作员角色之外的任何角色的用户都可以删除设备。

有关已删除设备的信息不会保存在应用程序中。如果已删除的设备再次开始在工业网络中显示活动，应用程序会将它们作为新设备添加到设备表中，并根据当前资产管理模式将状态设置为“*已授权*”或“*未授权*”。

使用设备表时删除设备

要从设备表中删除设备：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

3. 在**设备**选项卡上，选择要删除的设备。

4. 右键单击即可打开所选设备之一的上下文菜单。

5. 在上下文菜单中，选择下列选项之一：

   - 如果选择了一个设备，则**删除设备**。
   - 如果选择了多个设备，则**删除设备**。

   将打开一个带有确认提示的窗口。

6. 如果您已经为包含其地址信息的设备创建了交互控制规则，并且想要同时删除这些规则，请选中“**删除与设备相关的允许规则**”复选框。

7. 在提示窗口中，确认删除所选设备。

使用网络交互图和拓扑图时移除设备

使用网络交互图和拓扑图时，您可以使用图上代表这些设备的节点从设备表中删除设备。

要在使用地图时移除设备：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择**网络地图**部分。

3. 在“**网络交互图**”或“**拓扑图**”选项卡上，选择代表要删除的设备的节点。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**删除**。

   将打开一个带有确认提示的窗口。

5. 如果您为包含其地址信息的设备创建了交互控制规则，并且想要同时删除这些规则，请选中“**删除与设备相关的允许规则**”复选框。

6. 在提示窗口中，确认删除设备。

手动更改设备状态

应用程序在监控工业网络中的设备活动时，会自动为设备分配状态。在某些情况下，您可能需要手动更改自动分配的设备状态。例如，如果某个设备是工业过程支持所必需的，但该设备未活动且在学习模式下运行时未添加到应用程序中，则可能需要手动更改状态。当在监控模式下检测到此类设备时，应用程序会将该设备的状态分配为*未授权*。“未授权”状态只能手动更改。

具有除操作员角色之外的任何角色的用户都可以手动更改设备的状态。

您可以一次更改一个或多个选定设备的状态（更改为*已授权*、*未授权*或*已存档*）。如果要更改某个选定设备的状态，您可以启用或禁用为该设备自动将状态更改为已存档。

Cisco 交换机连接器可能会自动限制处于“*未授权*”状态的设备的网络访问。为了避免由于状态变化而阻止必要的设备，请检查为此连接器类型定义的设置。

如果*已存档*设备显示活动，应用程序会自动更改其状态。根据当前的资产管理模式，应用程序为检测到的设备分配*已授权*或*未授权*状态。

使用设备表时更改设备状态

要在使用表格时更改设备的状态：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**设备**部分中选择**资产**选项卡。

3. 在设备表中，选择您想要更改状态的设备。

4. 打开工具栏中的**更改状态**下拉列表。

5. 在下拉列表中，选择命令来分配所需的状态。

   将打开一个带有确认提示的窗口。

6. 如果您正在为设备分配“*已授权*”状态，并且想要同时微调这些设备的交互控制，请选中相关设置的复选框（确认窗口显示微调交互控制时已使用的设置）。

7. 在提示窗口中，确认所选设备的状态变化。

使用网络交互图和拓扑图时更改设备状态

使用网络交互图和拓扑图时，您可以更改地图上节点所代表的已知设备的状态。

您可以单个选择相关节点，也可以将其作为包括相关设备的折叠组的一部分进行选择。如果选择了折叠的组，则任何嵌套级别的子组中的所有设备也将被包括在设备选择中。

要在使用地图时更改设备的状态：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择**网络地图**部分。

3. 在“**网络交互图**”或“**拓扑图**”选项卡上，选择代表已知应用程序和/或折叠组的节点的对象。

   要选择多个节点和/或组，请执行以下操作之一：

   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。

4. 打开工具栏中的**更改状态**下拉列表。

5. 在下拉列表中，选择命令来分配所需的状态。

   将打开一个带有确认提示的窗口。

6. 如果您正在为设备分配“*已授权*”状态，并且想要同时微调这些设备的交互控制，请选中相关设置的复选框（确认窗口显示微调交互控制时已使用的设置）。

7. 在提示窗口中，确认所选设备的状态变化。

关于将设备分组

您可以使用设备组树将设备分组。设备组树最多支持六层嵌套。

可以将设备放入层次结构任意级别的组中。但是，每个设备只能添加到树中的一个组。

树还具有不超过 1000 个组的限制。

在将设备添加到特定组之前，有关该设备的信息不包含有关设备具体位置的任何信息。该设备被分配到组树中层次结构的顶层。将设备添加到组后，应用程序会将该设备的位置保存为组树中该组的完整路径。

可以按照以下方式将设备分组：

- 基于特定标准自动分组设备。

  使用这种类型的设备分组，应用程序可以自动将组添加到设备组树中。当应用程序检测到信息与所选分组标准相匹配的设备时，就会添加组。组的名称是根据所选标准的一系列特定值分配的（例如，按类别分组时根据设备类别的名称）。

- 手动将设备分组。

  您可以手动将设备分组，包括将设备添加到相关组中以及将其从其他组中排除。必要时，您可以利用可用的手动形成设备组树的功能来更改设备组树。

根据特定标准自动分组设备

本节包含有关按指定标准自动分组设备的说明。您可以根据以下标准之一自动对设备组树中的设备进行分组：

- IP 地址与应用程序已知的子网的关联
- 设备类别
- 设备供应商

具有除操作员角色之外的任何角色的用户都可以执行设备自动分组。

根据特定标准自动对设备进行分组，从组树中层次结构的顶层开始

要根据特定标准自动对设备进行分组（从组树中层次结构的顶层开始）：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，单击位于网络交互图显示区域左侧的工具栏中的以下按钮之一以选择分组标准：

   - – 按子网对设备进行分组。
   - – 按类别对设备进行分组。
   - – 根据供应商对设备进行分组。

   将打开一个窗口，提示您选择分组选项。

3. 要根据地址空间按类别和供应商对设备进行分组，请在提示窗口中选中“**考虑地址空间**”复选框。

4. 根据所需结果单击以下按钮之一：

   - 要按子网对设备进行分组，请单击**组**。
   - 要根据设备组树中所有组中的地址空间按类别和供应商对设备进行分组，请单击“**带有子组**”。
   - 要仅根据设备组树层次结构顶层的地址空间按类别和供应商对设备进行分组，请单击“**仅限选定组**”。

应用程序将识别符合所选分组标准的设备，为这些设备创建组，并将设备放入这些组中。

自动将设备分组到选定的设备组中：

要自动将设备分组到选定的设备组中：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，选择您想要自动分组设备的组。

3. 右键单击以打开上下文菜单。

4. 在上下文菜单中，选择下列选项之一：

   - **按子网分组**。
   - **按类别分组**。
   - **按供应商分组**。

   将打开一个窗口，提示您选择分组选项。

5. 要根据地址空间按类别和供应商对设备进行分组，请在提示窗口中选中“**考虑地址空间**”复选框。

6. 在提示窗口中，根据所需结果单击以下按钮之一：

   - 要按子网对设备进行分组，请单击**组**。
   - 如果要按类别或供应商对选定组的所有子组中的设备进行分组，请单击**带有子组**。
   - 如果您只想按类别或供应商对选定组中的设备进行分组，请单击“**仅限选定组**”。

   应用程序将识别符合所选分组标准的设备，为这些设备创建组，并将设备放入这些组中（但是，已经在其他组中的设备将不会被放入新组中）。

手动将设备分组

本节包含有关如何手动管理组树中设备位置的说明。具有除操作员角色之外的任何角色的用户都可以管理设备在设备组树中的位置。

将一台设备添加到组

要将设备添加到表中的组：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**资产**”部分的“**设备**”选项卡上，或在“**网络地图**”部分中选择设备。

   在“**网络地图**”部分，您可以选择设备以添加到网络交互图和拓扑图上的组。

   详细信息区域显示在 Web 界面窗口的右侧部分。

3. 单击**编辑**。

4. 在详细信息区域中，转到“**设置**”选项卡。

5. 单击“**组**”字段右侧的 图标。

   将出现“**在树中选择组**”窗口。

6. 在设备组树中，选择相关组。

   如果相关组不在树中，您可以将其添加到当前打开的“**在树中选择组**”窗口中。

7. 单击**选择**。

   所选组的路径将出现在**组**字段中。

8. 单击详细信息区域中的**保存**。

   如果在设备设置中未指定所有必需的信息或定义了无效值，则此按钮不可用。包含需要更正值的设置的选项卡以 图标标记。

将多个设备添加到组

使用设备表时，您可以将多个设备添加到一个组中。

使用网络交互图时，您还可以将图上节点所代表的多个已知设备添加到一个组中。您可以单个选择相关节点，也可以将其作为包括相关设备的折叠组的一部分进行选择。如果选择了折叠的组，则任何嵌套级别的子组中的所有设备也将被包括在设备选择中。

要在使用表格时将多个设备添加到一个组：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

3. 在“**设备**”选项卡上，选择您要添加到组的设备。

4. 右键单击以打开上下文菜单。

5. 在上下文菜单中，选择“**组管理**” → “**移动到组**”。

   将出现“**在树中选择组**”窗口。

6. 在设备组树中，选择相关组。

   如果相关组不在树中，您可以将其添加到当前打开的“**在树中选择组**”窗口中。

7. 单击**选择**。

   所选组的路径将显示在**组**列中。

要在使用网络交互图时将多个设备添加到一个组：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，选择已知设备和/或折叠组的相关节点。

   要选择多个节点和/或组，请执行以下操作之一：

   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。

3. 右键单击以打开上下文菜单。

4. 在上下文菜单中，选择**移动到组**。

   将出现“**在树中选择组**”窗口。

5. 在设备组树中，选择相关组。

   如果相关组不在树中，您可以将其添加到当前打开的“**在树中选择组**”窗口中。

6. 单击**选择**。

   代表已知设备的选定节点将显示在选定的组内。

从组中删除一台设备

要从表的组中删除设备：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**资产**”部分的“**设备**”选项卡上，或在“**网络地图**”部分中选择设备。

   在“**网络地图**”部分，您可以选择设备以从网络交互图和拓扑图上的组中删除。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 单击**编辑**。

4. 在详细信息区域中，转到“**设置**”选项卡。

5. 在“**组**”字段中，单击字段中的 × 图标（如果定义了组，则会显示图标）删除组路径。

6. 单击**保存**。

   如果在设备设置中未指定所有必需的信息或定义了无效值，则此按钮不可用。包含需要更正值的设置的选项卡以 • 图标标记。

保存设备更改后，其“**组**”值将被清除，并且该设备将被分配到组树中层次结构的顶层。

从组中删除多个设备

使用设备表时，您可以从组中删除多个设备。选择从组中删除的设备可能是同一组的一部分，也可能是不同组的一部分。

使用网络交互图时，您还可以从组中删除图上节点所代表的多个已知设备。您可以单个选择相关节点，也可以将其作为包括相关设备的折叠组的一部分进行选择。如果选择了折叠的组，则任何嵌套级别的子组中的所有设备也将被包括在设备选择中。

要在使用表格时从组中删除多个设备：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

3. 在“**设备**”选项卡上，选择要从组中删除的设备。

4. 右键单击以打开上下文菜单。

5. 在上下文菜单中，选择“**组管理**” → “**从组中删除**”。

   将打开一个带有确认提示的窗口。

6. 在提示窗口中，确认从组中删除设备。

对于所有选定的设备，“**组**”值将被清除，并且这些设备将被分配到组树中层次结构的顶层。

要在使用网络交互图时从组中删除多个设备：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，选择展开组和/或折叠组中的节点。

   要选择多个节点和/或组，请执行以下操作之一：

   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。

3. 右键单击以打开上下文菜单。

4. 在上下文菜单中，选择“**从组中删除**”。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认从组中删除设备。

对于所有选定的设备，“**组**”值将被清除并且这些设备将显示在组之外。

将节点和组移动到网络交互图上的其他组

您可以通过拖动网络交互图上的对象来更改设备组树中节点和组的位置。移动后，节点和组会改变其在设备组树中的位置，就像向组中添加设备和从组中删除设备一样。

具有除操作员角色之外的任何角色的用户都可以将节点和组移动到其他组。

要将节点和/或组移动到其他组：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，选择已知设备和/或折叠组的相关节点。

   要选择多个节点和/或组，请执行以下操作之一：

   - 按住 **SHIFT** 键并使用鼠标选择包含相关对象的矩形区域。
   - 按住 **CTRL** 键并使用鼠标选择相关对象。

3. 将光标移到选定的对象（代表已知设备的组或节点）上。

4. 按住 **CTRL** 键并将选定的对象拖到相关组（如果要将选定的对象移动到组树中层次结构的顶层，则拖动到组外的任何地方）。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认移动所选的对象。

手动创建设备组树

您可以在使用设备表、网络交互图和拓扑图时创建设备组树。可以在“**创建组树**”或“**在树中选择组**”窗口中使用树创建功能。

具有除操作员角色之外的任何角色的用户都可以创建设备组树。

要使用创建设备组树的功能：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**资产**选项卡上的**设备**部分或**网络地图**部分中，执行以下操作之一：

   - 单击“**创建组树**”，打开“**配置组**”窗口。

     在“**资产**”部分中，工具栏中的“**配置组**”下拉列表中提供了“**组管理**”按钮。

     在“**网络地图**”部分中，“**配置组**”按钮仅在“**网络交互图**”选项卡上可用。

   - **将设备添加到组在树中选择组**在树中选择组”窗口。您也可以在按“**组**”列过滤设备表时打开此窗口。

在“**创建组树**”或“**在树中选择组**”窗口中对设备组树所做的任何更改都会立即应用。

本节提供有关使用生成设备组树的功能的说明。

添加组

要将组添加到设备组树：

1. 在“**创建组树**”或“**在树中选择组**”窗口中，通过以下方式之一添加新组：
   - 如果树是空的，而您想要添加第一个组，请单击**添加**，或者按 **INSERT** 或 **ENTER**。
   - 如果要添加与现有组处于同一层次结构的组，请选择该组并按 **ENTER**。
   - 如果要将子组添加到现有组，请选择该组并单击“**添加**”或按 **INSERT**。
2. 在输入字段中，输入组名称。
   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`。
   组名称必须符合以下要求：
   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 必须包含 255 个字符或更少。
   - 不得与同一父组下的任何其他组的名称匹配（不区分大小写）。
3. 点击输入字段右侧的 ✓ 图标。

重命名组

要重命名设备组树中的组：

1. 在“**创建组树**”或“**在树中选择组**”窗口中，选择要重命名的组。
2. 单击“**重命名**”或按 **F2**。
3. 在输入字段中，输入组的新名称。
   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`。
   组名称必须符合以下要求：
   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 必须包含 255 个字符或更少。
   - 不得与同一父组下的任何其他组的名称匹配（不区分大小写）。
4. 点击输入字段右侧的 ✓ 图标。

新的组名将出现在添加到该组或其子组的设备信息中。

删除组

删除组时，添加到该组的设备不会被删除。相反，已删除组中的设备将被移动到设备树层次结构中已删除组所在的同一级别。

要从设备组树中删除组：

1. 在“**创建组树**”或“**在树中选择组**”窗口中，选择要删除的组。
2. 点击 图标。
   这将打开一个窗口提示您选择删除选项。
3. 在提示窗口中，根据所需结果单击以下按钮之一：
   - 如果您只想删除选定的组并保留其子组，请单击“**仅选定**”。
   - 如果您要删除选定组及其所有子组，请单击**带有子组**。

   将打开一个带有确认提示的窗口。
4. 在提示窗口中，单击**确定**。

移动组

要在设备组树中移动组：

1. 在“**创建组树**”或“**在树中选择组**”窗口中，选择要移动的组。
2. 使用箭头图标或其相应的组合键 **ALT+↓**、**ALT+↑**、**ALT+←** 或 **ALT+→** 来相对于树的其他元素移动组。如果无法执行操作，则该操作的图标不可用。

搜索组

您可以使用“**搜索组**”或“**创建组树**”窗口中的“**在树中选择组**”字段在设备组树中找到相关组。符合搜索条件的组将显示在设备组树中。对于子组，还会显示其父组。

更新树

当您使用树时，可以在服务器上更改设备组树中组的组成（例如，它可以由连接到服务器的另一个用户更改）。

您可以使用“**创建组树**”或“**在树中选择组**”窗口中的 图标手动更新树。

添加和删除设备标签

本节提供有关添加或删除设备标签的说明。您可以为设备分配任何用户定义的标签。

*设备标签*包含文本描述，可帮助您快速查找或筛选表中的设备。任何方便的文本描述都可以保存为标签。您最多可以为一个设备分配 16 个标签。每个设备可以有自己的一组标签。

设备标签列表显示在设备表的“**标签**”列中。单元格中的标签按字母顺序排序。

具有除操作员角色之外的任何角色的用户都可以设置和删除设备标签。

为单个设备添加标签

要为设备设置标签：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**资产**”部分的“**设备**”选项卡上，或在“**网络地图**”部分中选择设备。

   在“**网络地图**”部分，您可以选择设备以在网络交互图和拓扑图上添加标签。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 单击**编辑**。

4. 在详细信息区域中，转到“**设置**”选项卡。

5. 在“**标签**”字段中，输入您想要用作标签的文本描述。要分隔标签，您可以使用 **ENTER** 键或 **;** 字符。

   您可以使用大写和小写字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。

   标签名称必须满足以下要求：

   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 在设备标签列表中是唯一的（不区分大小写）。
   - 包含 1 至 255 个字符。

6. 如有必要，单击“**复制标签**”以复制标签列表。如果标签列表不为空，则会显示链接。

7. 单击**保存**。

   如果在设备设置中未指定所有必需的信息或定义了无效值，则此按钮不可用。包含需要更正值的设置的选项卡以 . 图标标记。

为多个设备添加标签

使用设备表时，您可以为多个设备添加标签。

使用网络交互图和拓扑图时，您可以为地图上的节点表示的已知设备添加标签。您可以单个选择相关节点，也可以将其作为包括相关设备的折叠组的一部分进行选择。如果选择了折叠的组，则任何嵌套级别的子组中的所有设备也将被包括在设备选择中。

要在使用表格时为多个设备添加标签：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
   除操作员角色外，任何角色的用户都可以执行此操作。
2. 选择“**资产**”部分。
3. 在“**设备**”选项卡上，选择您要添加标签的设备。
4. 右键单击即可打开所选设备之一的上下文菜单。
5. 在上下文菜单中，选择“**添加标签**”。
   将打开“**添加标签**”窗口。
6. 在“**标签**”字段中，输入您想要用作标签的文本描述。要分隔标签，您可以使用 **ENTER** 键或 **;** 字符。
   您可以使用大写和小写字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   标签名称必须满足以下要求：
   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 在设备标签列表中是唯一的（不区分大小写）。
   - 包含 1 至 255 个字符。
7. 如有必要，单击“**复制标签**”以复制标签列表。如果标签列表不为空，则会显示链接。
8. 如果要清除选定设备的当前标签列表并仅为这些设备提供新标签，请选中“**删除现有**”复选框。

   > 如果清除**删除现有**复选框，则当前标签列表将保留在每台设备上。新标签将添加到所有选定设备的标签列表中。在这种情况下，部分选定设备的标签总数可能会超出限制（每台设备最多 16 个标签）。应用程序在添加新标签之前会检查此限制。

9. 单击**确定**。
   如果输入的标签名称不符合要求，或者标签列表为空且未选中**删除现有**复选框，则该按钮不可用。

要在使用地图时为多个设备添加标签：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
   除操作员角色外，任何角色的用户都可以执行此操作。
2. 选择**网络地图**部分。
3. 在“**网络交互图**”或“**拓扑图**”选项卡上，选择已知设备和/或折叠组的相关节点。
   要选择多个节点和/或组，请执行以下操作之一：
   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。
4. 右键单击以打开所选对象之一的上下文菜单。

5. 在上下文菜单中，选择“**添加标签**”。
   将打开“**添加标签**”窗口。

6. 在“**标签**”字段中，输入您想要用作标签的文本描述。要分隔标签，您可以使用 **ENTER** 键或 **;** 字符。
   您可以使用大写和小写字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   标签名称必须满足以下要求：

   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 在设备标签列表中是唯一的（不区分大小写）。
   - 包含 1 至 255 个字符。

7. 如有必要，单击“**复制标签**”以复制标签列表。如果标签列表不为空，则会显示链接。

8. 如果要清除选定设备的当前标签列表并仅为这些设备提供新标签，请选中“**删除现有**”复选框。

   > 如果清除**删除现有**复选框，则当前标签列表将保留在每台设备上。新标签将添加到所有选定设备的标签列表中。在这种情况下，部分选定设备的标签总数可能会超出限制（每台设备最多 16 个标签）。应用程序在添加新标签之前会检查此限制。

9. 单击**确定**。
   如果输入的标签名称不符合要求，或者标签列表为空且未选中**删除现有**复选框，则该按钮不可用。

删除一台设备上的标签

要删除设备标记：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**资产**”部分的“**设备**”选项卡上，或在“**网络地图**”部分中选择设备。
   在“**网络地图**”部分，您可以选择设备以在网络交互图和拓扑图上删除标签。
   详细信息区域显示在 Web 界面窗口的右侧部分。

3. 单击**编辑**。

4. 在详细信息区域中，转到“**设置**”选项卡。

5. 在“**标签**”字段中，删除不再需要的标签：

   - 如果要删除特定标签，请使用标签名称旁边的 × 图标。
   - 如果要删除所有标签，请使用“**标签**”字段右侧的 × 图标。

6. 单击**保存**。
   如果在设备设置中未指定所有必需的信息或定义了无效值，则此按钮不可用。包含需要更正值的设置的选项卡以 . 图标标记。

清除多个设备的标签列表

使用设备表时，您可以清除多个设备的标签列表。

使用网络交互图和拓扑图时，您可以清除由地图上的节点表示的已知设备的标签列表。您可以单个选择相关节点，也可以将其作为包括相关设备的折叠组的一部分进行选择。如果选择了折叠的组，则任何嵌套级别的子组中的所有设备也将被包括在设备选择中。

要在使用表格时清除多台设备的标签列表：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

3. 在“**设备**”选项卡上，选择您要清除标签列表的设备。

4. 右键单击即可打开所选设备之一的上下文菜单。

5. 在上下文菜单中，选择“**添加标签**”。

   将打开“**添加标签**”窗口。

6. 选中“**删除现有**”复选框。

7. 单击**确定**。

要在使用地图时清除多台设备的标签列表：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择**网络地图**部分。

3. 在“**网络交互图**”或“**拓扑图**”选项卡上，选择已知设备和/或折叠组的相关节点。

   要选择多个节点和/或组，请执行以下操作之一：

   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。

4. 右键单击以打开所选对象之一的上下文菜单。

5. 在上下文菜单中，选择“**添加标签**”。

   将打开“**添加标签**”窗口。

6. 选中“**删除现有**”复选框。

7. 单击**确定**。

编辑设备信息

具有除操作员角色之外的任何角色的用户都可以编辑设备信息。

要手动编辑设备信息：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**设备**”部分的“**资产**”选项卡上，选择相关设备。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 单击**编辑**。

   详细信息区域将显示以下选项卡，用于查看和编辑设备信息：**设置**、**地址信息**和**自定义字段**。

4. 在详细信息区域的**设置**选项卡上，在标识设备信息的字段中指定相关值。

5. 在详细信息区域中的**地址信息**选项卡上，指定设备的 MAC 和/或 IP 地址。

6. 如果向应用程序添加了额外的地址空间，请指定地址的地址空间的名称。

7. 您可以为设备的同一个网络接口指定多个 IP 地址。要生成 IP 地址列表，请执行以下操作之一：

   - 如果要添加 IP 地址，请单击**添加 IP 地址**。
   - 如果要删除 IP 地址，请单击位于包含 IP 地址的字段右侧的图标。

8. 如果设备有多个网络接口，请生成设备的网络接口列表并为它们指定相应的 MAC 和/或 IP 地址。

   要生成设备的网络接口列表，请执行以下操作之一：

   - 如果要添加网络接口，请单击设备最后一个网络接口的设置组下的**添加接口**。
   - 如果要删除网络接口，请单击设备网络接口名称右侧显示的图标（如果有两个或更多网络接口）。
   - 如果要为网络接口定义不同的名称，请单击位于当前名称右侧的图标，然后在打开的字段中输入网络接口的新名称。

9. 在详细信息区域中的**设置**和**地址信息**选项卡上，启用或禁用设备相关信息的自动更新。为此，请使用和图标。在**设置**选项卡上，和图标位于字段的左侧。在**地址信息**选项卡上，和图标位于网络接口名称的右侧。对于**状态**字段，您可以借助图标启用或禁用自动更改设备状态。

10. 在详细信息区域的**自定义字段**选项卡上，创建自定义字段及其值的列表（如有必要）。

11. 单击**保存**。

    如果在设备设置中未指定所有必需的信息或定义了无效值，则此按钮不可用。包含需要更正值的设置的选项卡以图标标记。

保存设备信息更改后，您可以添加或编辑设备的过程控制设置。

添加、编辑和删除设备的自定义字段

您可以添加、编辑和删除包含有关设备信息的自定义字段。当选择设备时，自定义字段将显示在详细信息区域中。

对于自定义字段，适用以下限制：

- 单台设备自定义字段数量不得超过 16 个。
- 字段名称的字符数不能超过 100 个。
- 字段值的字符数不能超过 1024 个。

具有除操作员角色之外的任何角色的用户都可以添加、编辑和删除自定义字段。

要添加、编辑或删除自定义字段：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**设备**”部分的“**资产**”选项卡上，选择相关设备。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 单击**编辑**。

   详细信息区域将显示以下选项卡，用于查看和编辑设备信息：**设置**、**地址信息**和**自定义字段**。

4. 转到“**自定义字段**”选项卡并执行以下操作之一：

   - 如果要添加自定义字段，请单击“**添加自定义字段**”，然后在打开的字段中输入自定义字段的名称和值。
   - 如果您想编辑自定义字段，请输入相关自定义字段的新名称和/或值。
   - 如果您要删除自定义字段，请点击位于自定义字段名称右侧的 × 图标。

5. 单击“**保存**”。

删除设备用户

当使用设备用户监控时，应用程序可以自动从用户表中删除过时的账户。只有先前从**外部源**和 OVAL **扫描**源接收数据、但在从这些源接收的新数据中不存在的用户才会被自动删除。

如果有必要，您可以手动从用户表中删除过时的账户。

具有管理员或安全官角色的用户可以删除设备用户账户。

要从用户表中删除账户：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**资产**选项卡的**用户**下，选择要删除的用户账户。
3. 单击**删除**。
   将打开一个带有确认提示的窗口。
4. 在提示窗口中，单击**确定**。

删除设备可执行文件

当使用设备上的可执行文件的启动控制时，应用程序可以自动从可执行文件表中删除有关该文件的信息。当文件数量或存储时间达到限制时，就会自动删除。

如有必要，您可以手动从可执行文件表中删除过时的文件。

具有管理员或安全官角色的用户可以删除设备可执行文件。

要从可执行文件表中删除文件：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**可执行文件**”部分的“**资产**”选项卡上，选择要删除的文件。
3. 单击**删除**。
   将打开一个带有确认提示的窗口。
4. 在提示窗口中，单击“**删除**”。

配置地址空间

Kaspersky Industrial CyberSecurity for Networks 监控设备及其交互，同时考虑其地址空间（以下也称为“AS”）。*地址空间*旨在基于特定属性（例如，基于设备的特定网段）将设备的地址排列成多个集合。

规则和子网的列表用于描述应用程序中的地址空间。

*地址空间规则*是一组参数，用于定义将地址包括在特定地址空间中的条件。要将地址绑定到地址空间，每个 MAC 或 IP 地址必须至少满足一个地址空间规则。应用程序将地址绑定到地址空间，地址空间的规则定义了该地址的附属的最具体条件（例如，如果在规则中明确指定了地址）。

*地址空间子网*用于验证应用程序检测到的 IP 地址。根据检测到的 IP 地址所属的子网类型，应用程序可能会对资产管理和设备交互控制采取不同的操作。

您可以在“**地址空间**”选项卡的“**资产**”部分配置地址空间。每个地址空间被呈现为包含关于地址空间的信息的数据块。此数据块由标头和嵌套块组成，嵌套块包含规则表和子网。查看有关地址空间的信息时，您可以展开和折叠数据块的内容。

“**默认**”地址空间

默认情况下，在应用程序中定义一个名为“**默认**”的共享地址空间。此地址空间包含一个规则，其设置被配置为将任何 MAC 和 IP 地址绑定到此特定地址空间。默认情况下，“**默认**”地址空间的子网列表包含组织中最常用的一组标准子网。

您不能编辑“**默认**”地址空间的规则或将其他规则添加到此地址空间。但是，具有管理员、安全官或基础设施官角色的用户可以编辑此地址空间中的子网列表，以生成一组子网，同时考虑组织网络中设备的特定 IP 地址。如果 Kaspersky Industrial CyberSecurity for Networks 接收到来自 EPP应用程序的数据，应用程序可以使用这些数据自动将子网添加到子网列表中。

附加地址空间

如有必要，除“**默认**”地址空间外，您还可以配置多个地址空间。您可以为添加的地址空间生成用户定义的规则和子网集。满足添加的地址空间条件的地址将绑定到这些地址空间。所有其他地址仍将绑定到“**默认**”地址空间。

例如，当使用不同网段中具有相同地址的设备时，您可能需要添加地址空间。在这种情况下，在添加和配置地址空间之后，应用程序将能够基于应用程序将以地址空间名称的形式添加到地址的附加属性来区分地址信息。

有关使用地址空间的示例，请参阅“附录”。

将地址绑定到地址空间

当使用多个地址空间时，应用程序会将包含地址空间名称的属性添加到应用程序对象中指示的所有地址，包括设备、风险、规则、事件和其他对象。如果从应用程序中删除了所有添加的地址空间，则不再为地址显示包含地址空间名称的属性（地址空间的属性仅针对事件中的地址和与设备相关的某些风险中的地址）。

包含地址空间名称的属性表示地址和地址空间之间的链接。绑定到地址空间的地址将依赖于这些地址空间。

删除与地址绑定的地址空间时，应用程序会自动删除与要删除的地址空间绑定的所有地址。这些地址将从除事件之外的所有应用程序对象中删除。从对象中删除地址时，应用程序会检查该对象中的任何其他剩余地址。如果没有其他剩余地址，应用程序也会删除对象（如设备）。

关于地址空间规则

地址空间的规则显示在地址空间描述内的“**规则**”块中。有关规则的信息显示在地址空间标头和规则表中。

地址空间规则的设置显示在表格的以下列中：

- **源**

传入地址信息的来源类型和所选数据源的列表。可以使用以下类型的数据源：

- **监控点** – 为规则选择的监控点。
- **集成服务器** – 为规则选择的集成服务器（从所选集成服务器接收到的地址信息数据将满足地址空间规则）。
- **主动轮询模块** – 为规则选择的主动轮询模块连接器（从所选择的主动轮询模块接收到的地址信息的数据将满足地址空间规则）。

> 将要用作源的对象添加到应用程序后，必须在地址空间规则中指定数据源。例如，在添加“**主动轮询**”类型的连接器后，必须指定**主动轮询模块**数据源的连接器。

- **OSI 模型层**

  地址空间规则的开放系统互连 (OSI) 模型的选定层。可以为以下 OSI 层的地址配置规则：

  - **数据链路 (L2)** – MAC 地址。
  - **网络 (L3)** – IP 地址。
  - **数据链路和网络 (L2 和 L3)** – MAC 地址和 IP 地址。

- **VLAN ID**

  根据 IEEE 802.1q 标准使用 VLAN 技术时应用的虚拟局域网 (VLAN) ID。当用于地址空间规则时，**VLAN ID** 可以采用以下值：

  - **使用任意** – VLAN 技术用于设备之间的网络交互，可以使用任何 VLAN ID。
  - **未使用** – VLAN 技术不用于设备之间的网络交互。
  - **任意或未使用** – VLAN 技术要么不用于设备之间的网络交互，要么与任何 VLAN ID 一起使用。
  - 带有 VLAN ID 列表的**固定值** – VLAN 技术用于设备之间的网络交互，地址空间只能包含具有列出的 VLAN ID 之一的地址信息。

- **IP 地址**

  包含在地址空间中的 IP 地址。地址可以单独指定为范围或以 CIDR 子网地址格式指定。

查看规则表时，您可以使用配置功能（通过单击 ⚙ 图标）和搜索功能。

关于地址空间子网

地址空间的子网显示在地址空间描述内的“**子网**”块中。

该应用程序根据地址空间子网列表检查检测到的 IP 地址，并根据 IP 地址是否属于特定类型的子网执行以下操作：

- 将具有其检测到的 IP 地址的设备添加到设备表中并监控该设备的活动。
- 在网络交互图和拓扑图上显示具有其检测到的 IP 地址的设备作为其对应的节点类型（已知设备、未知设备或 WAN 节点）。

- 显示网络交互图链接，其中交互的一方是具有检测到的 IP 地址的设备。
- 根据定义的规则（交互控制规则、入侵检测规则和关联规则）验证设备与检测到的 IP 地址的交互。
- 忽略具有检测到的 IP 地址的设备的活动。

地址空间子网的设置显示在表的以下列中：

- **子网**

  无类域间路由 (CIDR) 格式的子网地址：<子网的基地址>/<掩码中的位数>。子网地址以树的形式显示，以显示子网的嵌套层次结构。

- **类型**

  子网类型决定了其用途。提供以下类型：

  - **私人，IT** – 用于作为信息技术 (IT) 资源的设备（例如文件服务器）的子网。
  - **私人，OT** – 与操作技术（OT）相关的设备（例如 PLC）的子网。
  - **私人，DMZ** – 位于非军事区 (DMZ) 网络段内的设备的子网，例如处理来自外部网络的请求的服务器。
  - **公共** – 被视为其他类型子网中设备的外部（全局）网络的子网。该子网的 IP 地址由网络交互图上的 WAN 节点表示。
  - **本地链路** – 局域网（未路由）一段内网络交互的子网。

- **范围**。

  子网中的 IP 地址范围。

- **忽略 MAC 地址**。

  指示在为涉及子网中的 IP 地址的网络交互创建允许规则时是否忽略检测到的 MAC 地址。如果启用此选项，则在学习模式下，与子网中的 IP 地址一起检测到的 MAC 地址将不会添加到网络完整性控制规则中。

- **自动添加子网**。

  指示是否根据从 EPP 应用程序收到的数据自动添加嵌套子网。如果启用此模式，应用程序将根据从 EPP 应用程序收到的数据添加嵌套子网。

查看子网表时，您可以使用配置功能（通过单击 ⚙ 图标）和过滤、搜索以及排序功能。

添加地址空间

如果您需要根据特定属性（例如设备的特定网段）对设备地址进行分组，您可以向应用程序添加地址空间。

应用程序中的最大地址空间数 – 100。

具有管理员、安全官或基础设施官角色的用户可以添加地址空间。

要添加地址空间：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或基础设施官角色的用户执行。

2. 选择“**资产**”部分。

3. 在“**地址空间**”选项卡上，通过单击“**添加 AS**”打开详细信息区域。

4. 输入地址空间的名称。

   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。

   地址空间名称必须满足以下要求：

   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 必须包含 255 个字符或更少。
   - 不得与其他地址空间的名称匹配（不区分大小写）。

   > 建议设置长度不超过 6-8 个字符的地址空间名称。如果名称包含较多字符，某些数据表（例如设备表）的单元格中可能无法完整显示地址信息。

5. 如有必要，请输入地址空间的文本描述。

6. 配置第一个地址空间规则的设置。

7. 如有必要，请单击“**添加规则**”添加并配置附加地址空间规则。

   地址空间中的规则总数不能超过 10 条。

8. 单击**保存**。

   如果未指定所有必需的值或设置中存在无效值，则此按钮不可用。

地址空间选项卡的下部将显示一个单独的块，其中包含有关添加的地址空间的信息。

生成用于资产管理的子网列表

本节包含有关可用于生成资产管理子网列表的功能的信息。

您可以生成地址空间的子网列表，同时考虑组织网络内设备的特定寻址。本节提供有关使用功能生成子网列表的说明。

如果 Kaspersky Industrial CyberSecurity for Networks 接收来自 EPP应用程序的数据，应用程序可以使用这些数据自动将子网添加到适当的地址空间中。如果检测到的子网嵌套在启用了自动添加子网的子网内，应用程序会自动添加这些子网。

具有管理员、安全官或基础设施官角色的用户可以生成子网列表。

添加子网

要添加子网：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或基础设施官角色的用户执行。

2. 选择“**资产**”部分。

3. 在“**地址空间**”选项卡上，展开包含有关要添加子网的地址空间的信息的块。

4. 在“**子网**”块的标题中，点击 + 图标。

   详细信息区域出现在 Web 界面窗口的右侧。

5. 在“**子网**”字段中，以 CIDR 格式输入子网地址：<子网的基地址>/<掩码中的位数>。

6. 在“**类型**”下拉列表中，根据子网的用途选择子网的类型。

7. 将以下切换按钮设置到必要的位置：

   - **忽略 NIC 规则的 MAC 地址** – 基于网络完整性控制技术创建允许规则时启用和禁用跳过检测到的 MAC 地址的模式。

     如果启用此选项，则在学习模式下，与子网中的 IP 地址一起检测到的 MAC 地址将不会添加到网络完整性控制规则中。

   - **自动添加子网** – 根据从 EPP 应用程序收到的数据启用和禁用自动添加嵌套子网。

     如果启用此模式，应用程序将根据从 EPP 应用程序收到的数据在此子网内添加嵌套子网。默认情况下，为当前子网选择的类型会指示给这些嵌套子网。

8. 单击**保存**。

子网列表将在树中的层次结构的相应级别显示新子网。

编辑子网设置

要编辑子网设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或基础设施官角色的用户执行。

2. 选择“**资产**”部分。

3. 在“**地址空间**”选项卡上，展开包含有关要编辑子网设置的地址空间的信息的块。

4. 展开“**子网**”块并选择相关子网。

   详细信息区域显示在 Web 界面窗口的右侧部分。

5. 单击“**编辑**”。

6. 根据必要的结果，执行以下操作：

   - 在“**子网**”字段中，以 CIDR 格式输入子网地址：<子网的基地址>/<掩码中的位数>。

     根子网的地址无法编辑。

   - 在“**类型**”下拉列表中，根据子网的用途选择子网的类型。

     更改子网类型时，请记住新类型的子网可能会影响应用程序可以使用该子网的 IP 地址执行的可访问操作。例如，如果您选择“**公共**”类型，网络交互图将不再显示从该子网分配 IP 地址的设备的链接。

   - 将以下切换按钮设置到必要的位置：

     - **忽略 NIC 规则的 MAC 地址** – 基于网络完整性控制技术创建允许规则时启用和禁用跳过检测到的 MAC 地址的模式。

       如果启用此选项，则在学习模式下，与子网中的 IP 地址一起检测到的 MAC 地址将不会添加到网络完整性控制规则中。

     - **自动添加子网** – 根据从 EPP 应用程序收到的数据启用和禁用自动添加嵌套子网。

       如果启用此模式，应用程序将根据从 EPP 应用程序收到的数据在此子网内添加嵌套子网。默认情况下，为当前子网选择的类型会指示给这些嵌套子网。

7. 单击“**保存**”。

如果更改了“**子网**”值，则子网的树形层次结构级别也可能会更改。

删除子网

在地址空间的子网列表中，您可以删除树中除根子网（子网 0.0.0.0/0）之外的任何子网。

若要删除子网：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或基础设施官角色的用户执行。

2. 选择“**资产**”部分。

3. 在“**地址空间**”选项卡上，展开包含要从中删除子网的地址空间信息的块。

4. 展开“**子网**”块并选择要删除的子网。

   详细信息区域出现在 Web 界面窗口的右侧。

5. 单击**删除**。

   将打开一个带有确认提示的窗口。

6. 在提示窗口中，确认删除子网。

已删除的子网将不再显示在子网列表中。如果删除的子网包含嵌套子网，这些子网将保留在列表中（但这些子网的树层次结构级别将发生变化）。

查看所选子网中具有 IP 地址的设备的信息

您可以查看有关在地址空间中选定子网中分配有 IP 地址的设备的信息。有关设备的信息显示在设备表中。设备表会根据子网地址自动应用过滤器。

要查看设备表中有关设备的信息：

1. 选择“**资产**”部分。
2. 在“**地址空间**”选项卡上，展开带有包含相关子网的地址空间的信息的块。
3. 展开“**子网**”块并选择您想要查看设备信息的子网。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击“**显示设备**”。

在“**资产**”部分中打开“**设备**”选项卡。设备表将根据设备地址信息中的 IP 地址进行过滤。

更改地址空间

您可以更改添加的地址空间的名称、文本描述和地址空间规则的设置。无法对“**默认**”地址空间进行这些更改。

您还可以为任何地址空间生成子网列表（包括“**默认**”地址空间的子网列表）。

更改地址空间规则的设置时，必须考虑此地址空间与应用程序对象（包括设备、风险、规则、事件和其他对象）中指示的地址之间已建立的链接。如果更改地址空间规则中的设置导致删除此地址空间和地址之间的链接，则应用程序会自动删除这些地址。如果应用程序对象（如设备）没有其他剩余地址，这可能导致删除这些对象。

具有管理员、安全官或基础设施官角色的用户可以更改地址空间规则的名称、文本描述和设置。

要更改地址空间规则的名称、文本描述或设置，请执行以下操作：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
   此操作可由具有管理员、安全官或基础设施官角色的用户执行。
2. 选择“**资产**”部分。
3. 在“**地址空间**”选项卡上，单击包含相关地址空间信息的块中的 图标。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 根据所需的结果，执行以下操作：
   - 输入地址空间的名称。
     您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。

地址空间名称必须满足以下要求：

- 必须以任何允许的字符开头和结尾（空格除外）。
- 必须包含 255 个字符或更少。
- 不得与其他地址空间的名称匹配（不区分大小写）。

> 建议设置长度不超过 6-8 个字符的地址空间名称。如果名称包含较多字符，某些数据表（例如设备表）的单元格中可能无法完整显示地址信息。

- 输入地址空间的描述。
- 配置地址空间规则的设置。
- 如有必要，请单击“**添加规则**”添加和配置其他地址空间规则，或使用 × 图标删除任何不必要的规则。
  地址空间中的规则总数不能超过 10 条。

5. 单击**保存**。
   如果未指定所有必需的值或设置中存在无效值，则此按钮不可用。
6. 在提示窗口中，确认已更改的地址空间设置。

删除地址空间

您可以删除已添加的地址空间。您不能删除“**默认**”地址空间。

> 删除地址空间时，必须考虑此地址空间与应用程序对象（包括设备、风险、规则、事件和其他对象）中指示的地址之间已建立的链接。如果删除地址空间导致删除该地址空间和地址之间的链接，则应用程序会自动删除这些地址。如果应用程序对象（如设备）没有其他剩余地址，这可能导致删除这些对象。

具有管理员、安全官或基础设施官角色的用户可以删除地址空间。

要删除地址空间：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 此操作可由具有管理员、安全官或基础设施官角色的用户执行。
3. 选择“**资产**”部分。
   在“**地址空间**”选项卡上，单击包含要删除的地址空间信息的块中的 图标。
   将打开一个带有确认提示的窗口。
4. 在提示窗口中，确认删除地址空间。

配置过程控制

Kaspersky Industrial CyberSecurity for Networks 可以通过跟踪工业网络流量中传输的过程参数和系统命令来监控工业过程。该应用程序会跟踪设备表中显示的、已定义过程控制设置的设备的这些数据。

过程控制设置可以根据应用程序支持的设备类和协议进行配置。

为了实现工业过程的自动控制，您可以采用过程控制规则和系统命令监控功能。您还可以实时跟踪过程参数。

*过程控制规则*是一组定义标记值条件的设置。过程控制规则包含必须在工业网络流量中检测的情况的描述（例如，当标记超过指定值时）。

当规则中定义的条件得到满足时，Kaspersky Industrial CyberSecurity for Networks 会记录一个事件。您可以在配置过程控制规则时定义相关的事件注册设置（例如，事件标题）。

*监控系统命令*可确保在流量中检测到传输的系统命令时注册事件。在配置设备的过程控制设置时，您可以选择要监控的相关系统命令。无论过程控制规则如何，都可以使用此功能。

具有管理员、安全官或 ICS 官角色的用户可以配置设备的过程控制设置并生成被监控标记和过程控制规则的列表。所有用户都可以查看和导出数据。

您可以在**过程控制**部分的服务器 Web 界面页面中生成被监控标记和过程控制规则的列表。您可以在使用**资产**部分和**网络地图**部分中的设备时配置设备的过程控制设置。

支持的设备和协议

Kaspersky Industrial CyberSecurity for Networks 可分析用于过程自动化的以下设备类的流量：

- 可编程逻辑控制器 (PLC)：
  - ABB™ AC 700F
  - ABB AC 800M
  - ABB B&R
  - Allen-Bradley® ControlLogix® 系列
  - Allen-Bradley CompactLogix™ 系列
  - AutomationDirect DirectLOGIC
  - BECKHOFF® CX 系列
  - CHINT MAS400
  - CHINT MAS9600
  - Emerson DeltaV M 系列

- Emerson DeltaV S 系列
- Emerson ControlWave 系列
- General Electric RX3i
- 用于 Experion PKS 控制系统的 Honeywell C300
- 用于 PlantCruise 控制系统的 Honeywell C300
- Honeywell ControlEDGE 900 系列
- IPU950
- Mitsubishi System Q E71
- OMRON CJ2M
- Schneider Electric Foxboro FCP270
- Schneider Electric Foxboro FCP280
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Schneider Electric Modicon Momentum
- Siemens SIMATIC® S7-200
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- 支持 YARD 协议的 YCU
- 支持 YARD 协议的 ELC
- Yokogawa CENTUM
- Yokogawa ProSafe-RS
- OWEN PLC100 系列
- Prosoft-Systems Regul R500
- Tecon MFK
- KNX® 设备
- Valmet DNA 控制系统中的设备

    - 支持 Allen-Bradley EtherNet/IP 协议的设备
    - 支持 COS 协议的设备
    - 支持 DTS 协议的设备
    - 支持 FEU 协议的设备
    - 支持 VNIIA 协议的设备
    - 支持 PK4 协议的设备
    - 支持 PNU20 协议的设备
    - 支持 CODESYS V2 协议的设备
    - 支持 CODESYS V3 协议的设备
    - 支持 ISaGRAF 协议的设备
    - 支持 Siemens S7comm 协议的设备
    - 支持 Siemens S7comm-plus 协议的设备
    - 支持 PROFINET IO 标准协议的设备
- 智能电子设备（以下简称 IED）：
    - ABB Relion™ REF615
    - ABB Relion RED670
    - ABB Relion REL670
    - ABB Relion RET670
    - General Electric Multilin B30
    - General Electric Multilin C60
    - MiCOM C264
    - Schneider Electric P545
    - Schneider Electric Sepam 80 NPP 系列
    - Siemens SIPROTEC™ 4 6MD66
    - Siemens SIPROTEC 4 7SA52
    - Siemens SIPROTEC 4 7SJ64
    - Siemens SIPROTEC 4 7SS52
    - Siemens SIPROTEC 4 7UM62

    - Siemens SIPROTEC 4 7UT63
    - Relematika TOR 300
    - EKRA 200 系列
    - EKRA BE2502 系列
    - EKRA BE2704 系列
    - 支持 DNP3 协议的设备
    - 支持 Schneider Electric UMAS 协议的设备
    - 支持 IEC 60870-5-101 / IEC 60870-5-103 协议的设备
    - 支持 IEC 60870-5-104 协议的设备
    - 支持 IEC 61850-8-1 GOOSE 协议的设备
    - 支持 IEC 61850-8-1 MMS 协议的设备
    - 支持 IEC 61850-9-2 采样值协议的设备
    - 支持 Modbus TCP 协议的设备
- 测量设备：
    - 支持 DLMS/COSEM 协议的设备
- 安装了服务器软件的设备：
    - FTP 服务器
    - OPC DA 服务器
    - OPC UA 服务器
    - Siemens SICAM PAS 服务器
    - TASE.2 服务器
    - 支持加密的服务器
    - ARMS SCADA 系统设备
- 归类为网络部件的设备：
    - Moxa NPort series
    - 支持 BACnet™ 协议的 I/O 设备
    - 支持 FTP 协议的 I/O 设备
    - 支持 IEC 60870-5-101 / IEC 60870-5-103 协议的 I/O 设备

- 支持 IEC 60870-5-104 协议的 I/O 设备
- 支持 Modbus TCP 协议的 I/O 设备
- 支持 OPC DA 协议的 I/O 设备；支持 WMI 设备交互协议的 I/O 设备
- 支持 OPC UA 二进制设备交互协议的 I/O 设备
- 支持服务器 Telnet 控制命令的设备

Kaspersky Industrial CyberSecurity for Networks 还具有用于过程控制的*通用类*设备：**通用 PLC**、**通用 IED**和**通用网关**。使用这些设备类，您可以配置 Kaspersky Industrial CyberSecurity for Networks 来分析不在支持类列表中的设备的流量。对于通用设备类，您可以从可编程逻辑控制器、智能电子设备和网络网关相关的设备上支持的协议列表中指定任意应用程序级协议的组合。

对于受支持的设备类，Kaspersky Industrial CyberSecurity for Networks 会分析通过以下应用程序级协议的通信：

- ABB SPA-Bus
- Allen-Bradley EtherNet/IP
- Bacnet
- BECKHOFF ADS/AMS
- BSAP
- CODESYS V2
- CODESYS V3 GATEWAY over TCP
- CODESYS V3 GATEWAY over UDP
- COS
- DLMS/COSEM
- DMS for ABB AC 700F 设备
- DNP3
- Emerson ControlWave Designer
- Emerson DeltaV，包括用于更新嵌入式软件（固件）的协议
- FTP
- General Electric EGD
- General Electric SRTP
- IEC 60870-5-101 / IEC 60870-5-103
- IEC 60870-5-104
- IEC 61850-8-1 GOOSE

- IEC 61850-8-1 MMS（包括 MMS 已报告）
- IEC 61850-9-2 采样值
- INA2000
- ISaGRAF IXL
- ISaGRAF SNCP
- KNXnet/IP
- Mitsubishi MELSEC System Q
- MMS (ISO 9506-2)
- Modbus TCP
- OMRON FINS over TCP
- OMRON FINS over UDP
- OMRON FINS over EtherNet/IP
- OPC DA，通过 WMI 技术进行设备交互的协议
- OPC UA Binary
- PROFINET DCP
- PROFINET IO
- RPC for PROFINET IO
- Schneider Electric UMAS
- Siemens S7comm
- Siemens S7comm-plus
- TASE.2 / IEC 60870-6
- TwinCAT3
- YARD
- Yokogawa Vnet/IP
- VNIIA
- Relematika BDUBus
- PK4
- PNU20

- ABB AC 800M 设备的 MMS 协议修改
- 修改 EKRA 200 设备的 Modbus TCP 协议
- 自动辐射监测系统 (ARMS) 协议
- Siemens SICAM PAS 与 SICAM SCC 的交互协议（基于 SIMATIC WinCC®）
- AutomationDirect DirectLOGIC 设备交互协议
- CHINT MAS400 设备通讯协议
- CHINT MAS9600 设备通讯协议
- Foxboro FCP270 设备交互协议
- Foxboro FCP280 设备交互协议
- IPU-FEU - 设备交互协议
- MiCOM C264 - 设备交互协议
- Valmet DNA - 设备交互协议
- Prosoft-Systems 设备初始设置协议
- Data Transfer Systems (DTS) 协议
- Siemens DIGSI 4 系统软件设备协议
- Honeywell Experion PKS / PlantCruise 控制系统中设备交互的协议
- Moxa NPort 系列设备的启动配置和交互协议
- Honeywell ControlEDGE 900 系列设备检测和交互协议

为了分析设备的流量和交互，该应用程序使用专门的模块来处理应用程序级协议。Kaspersky Industrial CyberSecurity for Networks 分发套件中包含的模块为列出的设备类和应用程序级协议提供支持。您可以通过安装更新来更新协议处理模块。安装应用程序更新时，可能会添加支持其他设备类和/或应用层协议的新模块。

Kaspersky Industrial CyberSecurity for Networks 还分析通过常见协议传输的流量。有关受支持的常见协议列表，请参阅附录。

过程控制设备

出于工业过程控制的目的，您可以使用定义了过程控制设置的设备表中的设备。

Kaspersky Industrial CyberSecurity for Networks 支持使用各种设备类和应用层协议进行过程控制。

您可以在 Kaspersky Industrial CyberSecurity for Networks 网络界面的**资产**部分或**网络地图**部分中选择的设备的详细信息区域中查看和编辑过程控制设置。

设备的过程控制设置

当在设备表、网络交互图或拓扑图上选择设备时，设备的过程控制设置将显示在详细信息区域中。如果设备设置了过程控制设置，则详细信息区域中的"**过程控制**"选项卡包含以下信息：

- **设备类** – 来自过程控制支持的设备类列表的设备类。
- **协议** ——所用协议的名称。为每个协议显示以下信息：
  - **系统命令** ——跟踪协议的系统命令的主要设置。此字段显示协议的系统命令总数以及被监控的系统命令的数量，如果被检测到，这些命令将导致应用程序注册事件。
  - 地址信息 – 根据所选的协议，该字段包含 IP 地址和端口、MAC 地址或域 ID（对于 IEC 61850：GOOSE 协议）。如果在应用程序中添加了额外的地址空间，则必须为地址指明特定的地址空间（并且为地址空间规则选择的 OSI 模型层必须与该地址匹配）。
  - 取决于所选协议的附加设置。如果应用程序允许您配置该协议的系统命令和地址信息以外的内容，则会显示附加设置。

    示例：
    当选择 Modbus TCP 协议时，还会显示附加设置"**翻转 Registers 的顺序**"。此设置允许您启用或禁用对 32 位数据值的寄存器（机器字）的反转序列的支持。

    当选择 IEC 60870-5-101 协议时，将显示以下附加设置：

    - **二字节 ASDU 地址** ——允许您启用或禁用应用程序服务数据单元 (ASDU) 的双字节寻址模式。如果禁用此模式，则使用单字节寻址。
    - **发起人** ——允许您启用或禁用数据块 ID 中发起者地址的附加字节。
    - **通道地址块（字节）** ——数据链路层地址块中的字节数。
    - **对象地址块（字节）** ——信息对象地址块中的字节数。

您可以通过以下方式为设备添加过程控制设置：

- 自动
- 手动
- 从外部项目导入

关于自动检测设备的进程控制设置

Kaspersky Industrial CyberSecurity for Networks 可以自动识别设备的过程控制设置并将这些设置保存在设备信息中。通过分析流量来识别设置，以检测工业过程中涉及的设备的协议命令。

应用程序会自动添加或编辑已添加到设备表的设备的过程控制设置。如果资产管理启用了设备活动检测方法，设备也可以自动添加到设备表中。

自动添加的过程控制设置被视为*系统*设置。如果在流量中检测到具有更新的参数信息的协议命令，应用程序可以更改这些设置。

被用户手动添加的过程控制设置被视为*自定义设置*。应用程序不会更改用户定义的过程控制设置。如果用户手动更改过程控制的系统设置，这些设置也将成为自定义设置。

当使用基于深度数据包检测技术的过程控制设备发现方法时，会自动检测设备的过程控制设置。您可以启用或禁用此方法。

为了自动检测过程控制设置，应用程序采用了处理应用层协议的模块。应用程序安装了内置模块，可以确定应用程序支持的设备类和协议列表中指示的多个设备和协议的主要设置。您可以通过安装更新来更新协议处理模块。

手动添加设备的过程控制设置

当使用设备表、网络交互图或拓扑图时，您可以手动添加设备的过程控制设置。为设备添加的过程控制设置被视为自定义设置。当自动检测设备的过程控制设置时，用户定义的设置不会改变。

具有除操作员角色之外的任何角色的用户都可以添加过程控制设置。

若要添加设备的过程控制设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**资产**”部分的“**设备**”选项卡上或“**网络地图**”部分中选择相关设备。

   在“**网络地图**”部分，您可以在网络交互图和拓扑图上选择相关设备。

   详细信息区域显示在 Web 界面窗口的右侧部分。

3. 在详细信息区域右上角，单击⋮图标并选择**过程控制设置**→**添加**。

   添加过程控制设置窗口将出现。

4. 配置过程控制设置：

   a. 选择设备类。

   b. 选择用于与工业流程内的设备交互的协议。

   c. 如果有必要，请编辑通过所选协议监控系统命令的设置。默认情况下，应用程序会监控除设备正常运行期间经常遇到的命令之外的所有系统命令。

   d. 如果需要为所选协议配置其他设置（例如与设备交互的地址信息），请在出现的字段中指定相关值。

   e. 如果您想要另外指定不同的协议（所选设备类支持的协议）或先前选择的协议的不同设置组合（当在一个设备内使用多个连接的模块时），请单击“**添加协议**”链接来添加此协议的设置。

5. 单击“**保存**”。

   如果未指定所有必需值或设置中存在无效值，则此按钮不可用。

在“**过程控制**”选项卡的详细信息区域中，将显示具有指定设置的专用部分。

编辑设备的过程控制设置

如果为设备添加了过程控制设置，则可以在使用设备表、网络交互图或拓扑图时手动编辑这些设置。保存更改后，设备的过程控制设置将被视为自定义设置。当自动检测设备的过程控制设置时，用户定义的设置不会改变。

具有除操作员角色之外的任何角色的用户都可以编辑过程控制设置。

若要编辑设备的过程控制设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**资产**”部分的“**设备**”选项卡上或“**网络地图**”部分中选择相关设备。

   在“**网络地图**”部分，您可以在网络交互图和拓扑图上选择相关设备。

   详细信息区域显示在 Web 界面窗口的右侧部分。

3. 在详细信息区域右上角，单击⋮图标并选择**过程控制设置→编辑**。

   编辑过程控制设置窗口将出现。

4. 配置过程控制设置。您可以编辑单个设置（例如，编辑特定协议的跟踪系统命令的设置）或按照添加过程控制设置时的顺序重新配置所有设置。

   当您编辑先前创建的标签中使用的设置时，应用程序会自动删除这些标签及其相关的过程控制规则。例如，如果您删除一个协议，则在保存设置后，应用程序将删除所有包含该设备和已删除协议的标签（与这些标签相关的过程控制规则也将被删除）。

5. 单击“**保存**”。

   如果未指定所有必需值或设置中存在无效值，则此按钮不可用。

在“**过程控制**”选项卡的详细信息区域中，具有先前定义的设置的部分中的信息将被刷新。

选择受监控的系统命令

您可以配置过程控制设备发送和接收的系统命令的流量监控。

在 Kaspersky Industrial CyberSecurity for Networks 中，系统命令包括管理命令（例如，START PLC）以及与设备操作相关或包含数据包分析结果的系统消息（例如，REQUEST NOT FOUND）。Kaspersky Industrial CyberSecurity for Networks 中的系统命令根据附录中列出的类别进行分类。

当检测到受监控的系统命令时，Kaspersky Industrial CyberSecurity for Networks 会为命令控制技术注册一个事件。事件是使用分配了代码 4000002602 的系统事件类型进行注册的。您可以配置此类事件的设置。

具有除操作员角色之外的任何角色的用户都可以配置设备的系统命令监控。

要配置设备的系统命令监控：

1. 在**设备**部分的**资产**选项卡或**网络地图**部分中，选择具有定义的过程控制设置的相关设备。

   在“**网络地图**”部分中，您可以在网络交互地图和拓扑地图上选择设备。

   如果没有为设备定义过程控制设置，请添加设置。

2. 在详细信息区域右上角，单击⋮图标并选择**过程控制设置→编辑**。

   编辑过程控制设置窗口将出现。

3. 指定第一个协议的相关系统命令。为此，展开**系统命令**字段下的**协议**列表，然后选择要监控的系统命令的复选框。选择系统命令后，单击**确定**。

4. 如果在过程控制设置中另外指明了不同的协议，或者是相同的协议但具有不同的地址信息，请选择通过该协议进行通信时将监控的系统命令。为此，请使用包含此协议名称的字段下的**系统命令**下拉列表。同样，配置设备所有其他指定协议的系统命令监控。

5. 单击**保存**。

   如果未指定所有必需值或设置中存在无效值，则此按钮不可用。

在“**过程控制**”选项卡的详细信息区域中，具有先前定义的设置的部分中的信息将被刷新。

正在清除为设备定义的进程控制设置

当使用设备表、网络交互图或拓扑图时，您可以清除设备的过程控制设置。

清除为设备定义的过程控制设置时，应用程序会自动删除为该设备创建的所有标签。除了标签之外，所有与其相关的过程控制规则也被删除。

具有除操作员角色之外的任何角色的用户都可以清除设备的过程控制设置。

若要清除设备的过程控制设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**资产**”部分的“**设备**”选项卡上或“**网络地图**”部分中选择相关设备。

   在“**网络地图**”部分，您可以在网络交互图和拓扑图上选择相关设备。

   详细信息区域显示在 Web 界面窗口的右侧部分。

3. 在详细信息区域的右上角，单击 ⋮ 图标并选择“**过程控制设置**” → “**删除**”。

   将打开一个带有确认提示的窗口。

4. 在提示窗口中，确认删除设置。

“过程控制”设置部分已从详细信息区域中的“**过程控制**”选项卡中删除。

正在从外部项目导入设备和标记配置

设备和标记的过程控制设置配置可以从外部项目文件导入到卡巴斯基 Kaspersky Industrial CyberSecurity for Networks 中。在 Kaspersky Industrial CyberSecurity for Networks 的情况下，*外部项目*是包含由其他系统（例如 SCADA 系统）保存的设备和标记数据的项目。

要导入外部项目的文件，文件必须被打包成 ZIP 档案（内容由 ZIP 档案组成的某些项目的文件除外）。您只能从属于受支持的外部项目类型的文件导入设备和标签配置。

您可以通过安装更新来更新和扩展支持的项目类型。

若要从外部项目导入设备和标记的配置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

   在设备表上方工具栏中的“**设备**”选项卡上，打开“**导入**”下拉列表。

3. 在下拉列表中，选择具有相关项目类型的选项。

   屏幕上将出现**“导入 <项目类型>”**窗口。

4. 在**要导入的文件**字段中，单击**浏览**来选择项目文件。

5. 为您现有的设备和标记配置选择相关选项。为此，请单击以下按钮之一：

   - **添加**– 将导入的设备配置和标记添加到现有的设备配置和标记中。
   - **替换**– 导入新的设备配置和标记，并删除与为其导入新配置和标记的设备相关的预先存在的配置和标记（不会删除具有用户定义过程控制规则的标记）。

6. 通过单击“**继续**”确认导入。

   数据导入过程开始。正在运行的导入操作的信息显示在后台操作列表中。此过程完成后，导入的设备和标签配置将可以在设备表和标签表中上传。

7. 如果您想查看导入结果报告：

   a. 在应用程序 Web 界面菜单中点击。

      后台操作列表打开。

   b. 等待导入操作完成。

   c. 单击**显示报告**。

支持导入的项目类型

设备和标记的配置可以从包含以下类型项目的数据文件中导入：

- 通用格式项目。

  此类项目可以从任何来源获取，通过将其数据转换并保存为 CSV 格式的带分隔符的文本文件。有关通用项目中文件的信息，请参阅附录。

- OPC 服务器的 AC 800M 配置文件。

  此类项目可通过 ABB AC 800M 设备管理软件获得。

- Control Builder M 项目。

  此类项目可通过 ABB Control Builder M 软件获得。

- COS 设备配置存档。

  该类项目可通过支持 COS 协议的设备管理软件获取。

设备的配置文件不包含这些设备使用的网络 IP 地址。从配置文件添加设备后，您需要验证应用程序中有关设备的信息，并在必要时手动为这些设备定义正确的 IP 地址。

- DeltaV 项目。

  此类项目可以通过 Emerson DeltaV 设备管理软件获得。

- DirectSOFT6 项目。

  此类项目可通过 DirectLOGIC 设备管理软件获得。

- ABB Freelance 2016 Engineering 标记列表。

  此类项目可通过 ABB Freelance 2016 Engineering 软件获得。

- IEC 61850 设备项目。

  此类项目可通过支持 IEC 61850 标准协议的设备管理软件获得。

  支持导入按照 IEC 61850-6 标准准备的 SCD、CID 和 ICD 文件类型。有关应用程序在处理和管理这些文件中保存的配置方面的功能的更多信息，请参阅附录。

- RSLogix 5000® 项目（以 CSV 或 ACD 文件形式提供）。

  此类项目可通过 RSLogix 5000 设备管理软件获得。

  导入包含 RSLogix 5000 项目的 CSV 文件时，应用程序会忽略该项目中的结构化和自定义类型的标记。如果想将这些标记添加到应用程序中，您可以导入包含 RSLogix 5000 项目的 ACD 文件或启用未知标记检测以从流量中添加标记。

- SICAM PAS V7 项目（由描述 TXT 文件或 PXD 文件表示）。

  此类项目可通过 Siemens SICAM PAS 版本 7 软件获得。

- TIA Portal V12/V13 项目。

  此类项目可通过 Siemens TIA Portal 版本 12 或 13 软件获得。

- Schneider Electric Unity 项目。

  此类项目可以通过 Schneider Electric Modicon 设备管理软件获得。项目可以作为 ZEF 或 XEF 文件提供（如果项目以 ZEF 文件形式提供，则该文件无需打包到 ZIP 存档中即可导入）。

  导入 Schneider Electric Unity 项目时，添加的设备会被分配导入时文件的名称。您可以在编辑设备信息时手动定义这些设备的名称。

- WinCC 项目（包括 WinCC OA、WinCC Flexible）。

  该类型的项目可以通过 Siemens SIMATIC WinCC、WinCC OA 或 WinCC Flexible 软件获得。

- YARD 配置文件。

  此类项目可通过支持 YARD 协议的设备管理软件获得。

- CIMPLICITY 导出 CSV 文件。

  此类项目可通过 CIMPLICITY 软件获得。

- Valmet DNA 配置文件。
  此类项目可通过 Valmet DNA 软件获得。
- EGD 配置 XML 文件。
  此类项目可通过导出通过 General Electric EGD 协议进行数据交换的配置来获得。
- ControlWave 项目 SIG 文件。
  该文件包含在 Emerson ControlWave 系列设备使用的项目中。
- Honeywell Control Builder 项目。
  此类项目可通过 Honeywell Control Builder 软件获得。
- PcVue V10/V11 项目
  此类项目可通过 PcVue 10 或 11 版本软件获得。
- Proficy 导出 CSV 文件。
  此类项目可以通过 Proficy 软件获得。
- Foxboro IACC 导出文件项目。
  此类项目可通过 Foxboro IACC 软件获得。
- PNU20 配置文件。
  此类项目可通过支持 PNU20 协议的设备管理软件获得。
- CHINT MAS400 项目。
  此类项目可以通过CHINT MAS400 设备管理软件获得。
- CHINT MAS9600 项目。
  此类项目可以通过CHINT MAS9600 设备管理软件获得。
- 包含 ISaGRAF 项目调试信息的 XWS 文件。
  此类项目可通过支持 ISaGRAF 协议的设备管理软件获得。
- CSV 文件。
  此类项目可从任何支持将设备信息导出为 CSV 文件的来源获取。CSV 文件中的数据必须以与从 Kaspersky Industrial CyberSecurity for Networks 导出的设备数据 CSV 文件相同格式的记录呈现。

标记

标签是在工业网络中传输的过程参数（例如，控制的温度）。标签的值通过特定协议由设备传输和接收。

您可以通过以下方式向应用程序添加标签：

- 手动
- 检测到未知标签时自动
- 从外部项目导入

在以下条件下可以添加标签：

- 设备表包含与正在添加的标签相关联的设备。
- 设备已定义过程控制设置，其中指明了所添加标签的协议。

在应用程序中添加标签后，该标签可以在过程控制规则中使用。根据过程控制规则中定义的条件，应用程序将注册相应的事件，其中可以保存接收到的标签值。

在监控过程参数时，不需要将此标签添加到过程控制规则中来控制标签值。

您可以在**过程控制**选项卡的**标记**部分查看和编辑标签。

关于未知标记检测

Kaspersky Industrial CyberSecurity for Networks 可以分析流量以检测并保存有关未知标签的信息。未知标签是标签表中不存在的标签。

如果满足添加标签的条件，应用程序会将检测到的标签添加到标签表中。如果其中一个条件不满足，则会忽略检测到的标签（例如，如果标签在过程控制设置中没有为设备指定关联协议）。

使用基于深度数据包检测技术的未知标签检测方法从流量中获取有关未知标签的信息。您可以启用或禁用此方法。

> 当使用未知标签检测方法时，应用层协议处理模块的性能可能会略有下降。因此，应用程序安装后，未知标签检测默认处于禁用状态。建议启用未知标签检测方法一段时间，以检测可能与具有指定过程控制设置的设备相关联的所有标签。建议在将检测到的标签添加到表后禁用此方法。

以下协议支持未知标签检测：

- Allen-Bradley EtherNet/IP
- Bacnet
- BSAP
- CODESYS V3 Gateway
- DMS for ABB AC 700F 设备
- DNP3
- Emerson DeltaV
- IEC 60870：IEC 60870-5-101、IEC 60870-5-104
- Modbus TCP
- OPC DA
- OPC UA Binary

- Schneider Electric UMAS
- Siemens S7comm
- TASE.2
- Yokogawa Vnet/IP
- PNU20
- Foxboro FCP270 和 FCP280 设备交互协议

手动添加标记

具有管理员、安全官或 ICS 官角色的用户可以手动添加标签。

若要手动添加新标记：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**标记**选项卡上，单击**添加标记**打开详细信息区域。

4. 单击**选择设备**打开设备选择窗口。

5. 在设备选择窗口中，选择要为其创建标记的设备，然后单击**确定**。

   设备选择窗口包含一个表，您可以在其中配置列的布局和顺序，还可以像“资产”部分中的**资产**一样进行过滤、搜索和排序。

6. 选择所选设备的过程控制设置中指示的协议。您必须选择支持标记传输的协议。

   如果没有必要的协议，您可以配置过程控制设置并指定必要的协议。要打开设置窗口，请使用协议选择字段右侧的按钮。过程控制设置的配置与使用设备表时添加或编辑设置的配置相同。

7. 如果有必要，更改标记名称。根据模板的默认名称是**Tag <设备标记计数器的值>**。

   您可以使用英文字母、数字和以下特殊字符：`( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`。标记名称必须以空格以外的任何允许的字符开始和结束。

8. 配置其他标记参数。

   必须为标记指定必需参数（例如标记名称和数据类型）。根据所选的协议和数据类型，也许可以配置其他参数（例如测量单位和缩放限制）。

9. 单击**保存**。

   如果未指定所有必需值或设置中存在无效值，则此按钮不可用。

新的标记出现在标记表中。

编辑标记参数

具有管理员、安全官或 ICS 官角色的用户可以编辑标签设置。

要编辑标记设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**标记**选项卡上，选择相关标记。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**编辑**。

5. 如果有必要，更改标记名称。

   您可以使用英文字母、数字和以下特殊字符：`( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`。标记名称必须以空格以外的任何允许的字符开始和结束。

6. 配置其他标记参数。

   必须为标记指定必需参数（例如标记名称和数据类型）。根据所选的协议和数据类型，也许可以配置其他参数（例如测量单位和缩放限制）。

7. 单击**保存**。

   如果未指定所有必需的值或设置中存在无效值，则此按钮不可用。

将标记添加到收藏夹列表

如果您想创建一个最重要的标签列表并快速导航到该列表（例如，以查看这些标签的当前值），您可以将标签添加到收藏夹列表中。您可以自行决定将标签添加到收藏夹列表或从中删除标签。收藏夹列表中的标签数量不受限制。

要显示收藏夹标签列表，您可以在查看标签表时按“**收藏夹**”列进行过滤。

创建的标签默认不会添加到收藏夹列表。

要将标签添加到收藏夹列表：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在“**标记**”选项卡上，选择要添加到收藏夹列表的标签。

4. 右键单击以显示所选标签之一的上下文菜单。

5. 在上下文菜单中，选择“**添加到收藏夹列表**”。

在标签表中，“**是**”列中所有选定的标签均显示**收藏夹**。

要从收藏夹列表删除标签：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**标记**选项卡上，选择要从收藏夹列表中删除的标签。

4. 右键单击以显示所选标签之一的上下文菜单。

5. 在上下文菜单中，选择“**从收藏夹列表删除**”。

在标签表中，“**否**”列中所有选定的标签均显示“**收藏夹**”。

正在删除标记

具有管理员、安全官或 ICS 官角色的用户可以删除标签。

若要删除标记：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**标记**卡上，选择要删除的标记。

4. 在标记表上方的工具栏上，单击“**删除**”。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认删除标记。

过程控制规则

应用程序可以采用以下过程控制规则来监视标记的值：

- 具有定义条件的规则。这些规则包含用来跟踪标记值的条件。每个规则可以包含所提供的条件类型之一。如果满足规则中定义的条件，应用程序就会注册一个事件。已注册事件的设置也在规则中进行定义。

- 使用 Lua 脚本的规则。这些规则包含用于检查标记值的算法的描述。这些算法是在 Lua 编程语言中使用Lua 脚本的函数和变量进行编译的。当包含 Lua 脚本的规则中的算法被触发时，应用程序会注册一个事件（注册事件的设置在规则中进行定义）。如果您使用 Lua 脚本执行流程控制规则，则可以使用*全局 Lua 脚本*来初始化全局 Lua 变量和函数。您可以在任何规则的 Lua 脚本中使用这些全局变量和函数。默认情况下，全局 Lua 脚本为空，不包含可执行代码。应用程序一次只能有一个全局 Lua 脚本。

应用程序在使用基于深度数据包检测技术的基于规则的过程控制方法时应用过程控制规则。您可以启用或禁用此方法。

过程控制规则可以启用或禁用。启用的规则在流量分析期间予以应用。禁用的规则不被应用，也不被考虑。

当过程控制在学习模式下运行时，应用程序可以自动创建具有定义条件的过程控制规则。

您可以在的**规则**部分的**过程控制**选项卡中查看和编辑过程控制规则。

具有标记值定义条件的规则

为了监控标记的值，您可以采用过程控制规则，其中为标记的值定义条件。每个规则可以包含所提供的条件类型之一。一条规则只能绑定到一个标记。不过，您最多可以为一个标记创建 20 条具有不同类型条件的规则。

当过程控制在学习模式下运行时，应用程序可以自动创建具有定义条件的规则。您还可以手动创建和编辑具有针对标记值的定义条件的规则。

对于过程控制规则，您可以选择以下类型的条件之一：

- **值已更改**– 受控标记的值已完全改变或在特定位中改变。

  如果没有专门监控某个值的特定位，则可以使用此条件来监控任意类型标记的值。您还可以指定标记的已保存（允许）值的数量，这些标记的检测不会导致注册事件。对于一条规则，您可以指定从 1 到 10 的已保存值的数量（检测到新值时，已保存的值将会更新）。默认情况下，只保存最新值。

  如果要专门监视某个值的特定位，则可以使用此条件仅监视 int 和 unsigned int 标记。出于监控目的，您需要指定标记中被监控位的序列号（对应于所选标记的数据类型的范围内的整数：从 1 到 8、16、32 或 64）。

- **标记丢失** – 在定义的时间段内，在监控的流量中未检测到受控标记。

  您可以使用此条件来监控任何类型的标记。

- **检测** – 在监控的流量中检测到受控标记。

  您可以使用此条件来监控任何类型的标记。

- **在范围中** – 受控标记的值在指定范围内。

  您可以使用此条件仅监控 int 和 float 标记。

  您可以定义范围的下限和/或上限值。限制的定义值可以包含在范围内，也可以排除在范围之外。

- **超出范围** – 受控标记的值超出指定的范围。

  您可以使用此条件仅监控 int 和 float 标记。

  您可以定义范围的下限和/或上限值。限制的定义值可以包含在范围内，也可以排除在范围之外。

- **等于** – 受控标记的值完全或在特定位等于定义的值之一。

  如果没有特别监视值的特定位，则可以使用此条件来监控 int、bool 和 string 标记的值。您可以定义 1 到 10 个值进行比较。

  如果要专门监视某个值的特定位，则可以使用此条件仅监视 int 和 unsigned int 标记。出于监控目的，您需要指定标记中监控位的序列号（对应于所选标记的数据类型的范围内的整数：从 1 到 8、16、32 或 64）以及用于比较的位的值（表示为两个整数之一：零或一）。

- **不等于**– 受控标记的值不完全等于定义的值之一，也不在特定位上等于该值。

  如果没有特别监视值的特定位，则可以使用此条件来监控 int、bool 和 string 标记的值。您可以定义 1 到 10 个值进行比较。

  如果要专门监视某个值的特定位，则可以使用此条件仅监视 int 和 unsigned int 标记。出于监控目的，您需要指定标记中监控位的序列号（对应于所选标记的数据类型的范围内的整数：从 1 到 8、16、32 或 64）以及用于比较的位的值（表示为两个整数之一：零或一）。

- **单调变化违规** – 受控标记的值违反了值的单调增加或减少的序列。

  您可以使用此条件仅监控 int 和 float 标记。

对于监控标记值的规则，您需要考虑应用程序如何处理由非规范化数字表示的值（接近于零的低阶数字，例如，如果该值以双精度表示，则为 2.22507e-308）。该应用程序将非规范化的数字转换为零值。

对于任何条件，您都可以选择应用程序将监控标记值的操作。根据对标记执行的操作，可以使用以下监控选项：

- **读取标记时监控** – 从设备读取标记时检查该值。
- **写入标记时监控** – 将标记写入设备时检查该值。

使用 Lua 脚本的规则

用 Lua 编程语言编写的脚本可用于描述检查过程控制规则中标记值的算法。Lua 脚本不仅可以检查标记的值，而且可以向已注册的事件和流程日志添加各种信息。

Lua 脚本必须由一个或多个函数组成。在所有包含 Lua 脚本的规则中，函数名称必须是唯一的。用于跟踪标记值的函数称为*触发函数*。触发函数必须返回`true`值才能注册事件。

如果在脚本中指定了变量，则该变量必须在该特定脚本中（仅在该脚本中应用）或在单独的全局脚本中（在所有具有 Lua 脚本的规则中应用）进行初始化。全局脚本还可以包含可在 Lua 脚本规则中使用的辅助函数。

只要函数中使用的任何标记的值发生更改，该函数就会被调用。当接收到函数中使用的标记的所有值时，将首次调用该函数。

为了获取标记的值，函数代码包含如下所示的条目：

```
tag'main_tag_parameters[:field_name][@modifier]'[.transmission_direction]
```

其中：

- `main_tag_parameters`是识别应用程序中标记的强制性参数。主要参数由标记表中的以下参数组成：
  - **设备**
    此参数与下一个参数以冒号(`:`)分隔。
  - **标记名称**
    此参数与下一个参数以斜线(`/`)分隔。
  - **标记 ID**
- `field_name` 是标记表中**结构值**中定义的标记字段结构内的字段的名称。如果某个字段被嵌入到其他字段中，则其名称将与所有父字段的名称一起显示，以冒号分隔。如果未指定`field_name`参数，则检查标记字段结构内的主值。
- `修饰符` 决定数据如何被表示和获取。可使用修饰符：
  - `type` 表示传递的值是获取的值的数据类型。
  - `str` 表示获取的值被转换成字符串值。
  - `loc` 表示传递的值是为获取的值分配的本地化名称（如果没有本地化名称，获取的值将被转换为字符串值）。
  - `ts` 用于获取最后标签值更新的时间戳（UTC，从 1970.01.01 开始以微秒为单位）。修饰符不适用于字段。

  如果没有指定修饰符，则使用实际获得的值。在这种情况下，值的数据类型不会改变。
- `transmission_direction`定义获取的值的传输方向。传输方向可以通过下列参数之一来定义：
  - `r` 表示从设备读取该值时已收到该值。
  - `w` 表示在将值写入设备时已收到该值。
  - `rw` 表示获取的值的任意方向。

  如果未定义传输方向，则使用从任意方向获取的值。

示例

```
tag'BayController:BayControllerQ.T1MMXU1.PhV.phsA/73:cVal:mag:f'
```

其中：

- `BayController` 是设备名称。
- `BayControllerQ.T1MMXU1.PhV.phsA` 是标签名称。
- `73` 是标签 ID。
- `cVal:mag:f` 是字段名称与父字段名称的组合。

获取标记值的记录可用于表达式（例如，为变量分配值或比较值）。

要使用 Lua 脚本执行各种操作，可以使用服务器支持的*辅助功能*。辅助功能的名称以下划线 (_) 开头。

通过 Lua 脚本添加信息的主要辅助功能如下：

- 添加参数以用作事件中的附加变量的功能：

  ```
  _AddEventParam('parameter_name', parameter_value)
  ```

  可以为参数定义任何名称和值。要在事件中使用参数及其值，必须在事件类型参数中指定此参数，如下所示：`$extra.<parameter_name>`。

- 向 Lua 脚本在其中执行的进程日志添加条目的函数（此进程的名称前面通常带有 `Filter` 字样）。将向该日志中添加由函数的参数（变量或常量）定义的记录：

  - 要创建具有*错误*级别的记录：

    ```
    _WriteErrorLog(function_argument)
    ```

  - 要创建*警告*级别的记录：

    ```
    _WriteWarningLog(function_argument)
    ```

  - 要创建具有*信息*级别的记录：

    ```
    _WriteInfoLog(function_argument)
    ```

  - 要创建具有*调试*级别的记录：

    ```
    _WriteDebugLog(function_argument)
    ```

  - 要创建一个可能包含函数的多个参数的*调试*级别的记录：

    ```
    print(function_argument1, function_argument2,…)
    ```

    函数参数定义的变量或常量在日志记录中以制表符分隔。

  如果记录级别低于为该进程设置的日志记录级别，则不会在日志中创建记录。

过程控制规则学习模式

为了减少重复操作并实现规则创建和配置的自动化，应用程序使用了机器学习方法和基线模型。应用程序分析流量处理过程中检测到的标记值变化中的各种模式，并生成可直接使用的过程控制规则。启用规则学习模式后，将使用机器学习方法。

在过程控制规则学习模式中，应用程序自动生成带有标签值条件的过程控制规则。为了生成规则，应用程序会分析流量以仅监控已添加到标签表中的标签的值。

在学习模式中自动添加的过程控制规则称为*系统*规则。对于这些规则，“**源**”值被设置为“**系统**”。系统规则自动创建时，**事件分数**默认设置为6.0。

手动创建的规则称为*用户*规则。对于这些规则，“**源**”设置为“**用户**”。如果手动更改系统规则，该规则也将成为用户规则。

应用程序将学习模式下添加的规则的状态指定为*已禁用*。如果系统规则在学习模式下更新，则该规则将保留更新前的状态：“*已启用*”或“*已禁用*”。

在学习模式下添加或更新过程控制规则时，应用程序为其定义以下条件之一：

- **不等于**。

  如果未找到针对检测到的标签值的其他系统规则，或者收到最多十个不同的标签值（布尔或浮点数据类型的标签除外），则添加规则时定义此条件。

- **超出范围**。

  如果接收到具有浮点数据类型的标签的新值或接收到具有整数数据类型的标签的十个以上不同的值，则此条件将替换规则中的先前条件。

- **单调变化违规**。

  如果检测到的标签值仅增加或仅减少，而没有任何其他变化，则此条件将取代规则中的先前条件。当学习模式结束时，此条件将取代整数或浮点数据类型标签规则中的先前条件。

在学习模式下，应用程序还会在以下情况下删除系统过程控制规则：

- 该规则是为具有布尔数据类型的标签创建的，检测到的值和保存的值不匹配（仅对前十个检测到的值进行比较，所有其他值都被忽略）。
- 该规则是针对具有字符串数据类型的标签创建的，并且收到了十多个不同的值。

您可以配置基于规则的过程控制方法的学习模式。

必须启用过程控制规则学习模式足够长的时间来检测相关标签的所有可能值。这个时间取决于标签在流量中流通的频率、设备在工业网络中运行的频率以及工业过程的其他细节。我们建议您启用学习模式至少一个小时。在大型工业网络中，可以启用学习模式一段时间（从一天到几天），以积累最大量数据。

查看过程控制规则表

过程控制规则表显示在“**过程控制**”选项卡的“**规则**”部分中。该表提供了规则以及与规则相关的标签和设备的常规设置。

规则的设置显示在表格的以下列中：

- **规则 ID**

  规则的唯一 ID。

- **设备组**

  包含与标签关联的设备的组的名称（包含组的名称以及设备组树中其所有父组的名称）。

- **设备**

  与标签关联的设备的名称。

- **协议**
  用于传输标签的协议的名称。
- **标记名称**
  创建规则的标签的定义名称。
- **规则**
  规则的定义名称。
- **规则描述**
  规则定义的描述。
- **状态**
  规则的当前状态（*已启用*或*已禁用*）。
- **创建日期**
  规则创建的日期和时间。
- **更改时间**
  规则最后修改的日期和时间。
- **条件类型**
  为规则选择的条件类型。
- **事件标题**
  触发规则时注册的事件的标题。
- **事件分数**
  触发规则时注册的事件的评估分数。事件的评分范围为 0.0 到 10.0。
- **事件描述**。
  规则触发时注册的事件的描述。
- **源**
  有关规则来源的信息。

当查看设备表时，您可以使用配置、过滤、搜索和排序功能，以及导航到相关项目。

创建具有条件设置的过程控制规则

以下选项可用来创建具有条件设置的过程控制规则：

- 为标记创建新规则。
- 根据现有规则创建附加规则。

要为标记创建新规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**标记**选项卡上，选择要为其创建过程控制规则的标记。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 在详情区域右上角，单击**创建规则**。

   这将打开**规则**选项卡，其中包含已创建的过程控制规则的详细信息区域。

5. 执行以下操作：

   a. 使用**启用**切换按钮来定义规则的状态：*已启用*或*已禁用*。

   b. 输入规则名称和描述。

      您可以使用英文字母、数字和以下特殊字符：`( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`。规则名称必须以空格以外的任何允许的字符开始和结束。

   c. 选择条件类型并根据所选类型配置设置。

   d. 配置规则触发时注册事件的设置（事件标题、描述和分数以及流量节省设置）。

6. 单击**保存**。

要基于现有规则创建附加过程控制规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**规则**选项卡上，选择要用作为同一标记创建另一个规则的基础的规则。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**创建新规则**。

   您将看到已创建的过程控制规则的详细信息区域。对于新规则，您将看到从所选规则的设置中收到的有关设备、协议和标记的信息。

5. 执行以下操作：

   a. 使用**启用**切换按钮来定义规则的状态：*已启用*或*已禁用*。

   b. 输入规则名称和描述。

c. 选择条件类型并根据所选类型配置设置。

d. 配置规则触发时注册事件的设置（事件标题、描述和分数以及流量节省设置）。

6. 单击**保存**。

创建使用 Lua 脚本的过程控制规则

要使用 Lua 脚本创建规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**规则**选项卡上，单击**添加 Lua 脚本**打开详细信息区域。

4. 执行以下操作：

   a. 使用**启用**切换按钮来定义规则的状态：*已启用*或*已禁用*。

   b. 输入规则名称和描述。

   c. 在**规则的 Lua 脚本**字段中，使用 Lua 语言输入脚本代码。

   输入文本时，建议或可用值会自动出现在光标附近（例如，输入识别标记的设置时，会出现设备和标记的相关名称）。

   如果脚本代码不适合**规则的 Lua 脚本**字段，您可以单击打开一个单独的窗口来显示代码。

   d. 配置规则触发时注册事件的设置（事件标题、描述和分数以及流量节省设置）。

5. 单击**保存**。

编辑过程控制规则设置

要编辑过程控制规则设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**规则**选项卡上，选择要编辑的规则。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**编辑**。

5. 根据需要更改设置。您可以使用与创建具有条件或Lua 脚本的过程控制规则时可用的相同操作来编辑设置。

创建、查看和编辑全局 Lua 脚本

全局 Lua 脚本中定义的变量和函数可以在具有 Lua 脚本的规则中使用。

具有管理员、安全官或 ICS 官角色的用户可以创建和修改过程控制规则的全局 Lua 脚本。具有任何角色的用户都可以查看全局 Lua 脚本的内容。

要创建或编辑全局 Lua 脚本：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**规则**选项卡上，单击**Global Lua 脚本**打开全局 Lua 脚本编辑窗口。

4. 使用 Lua 语言输入脚本代码。

5. 单击**保存**。

删除过程控制规则

要删除过程控制规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   此操作可由具有管理员、安全官或 ICS 官角色的用户执行。

2. 选择“**过程控制**”部分。

3. 在**规则**选项卡上，选择要删除的规则。

4. 单击**删除**。如果工具栏上未显示该按钮，请单击 ⋮ 按钮并在打开的菜单中选择所需的项目。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认删除规则。

配置交互控制

Kaspersky Industrial CyberSecurity for Networks 可以监控工业网络中设备的网络交互。*交互控制规则*用于定义已授权和未授权的网络交互。所有检测到的不满足活动交互控制规则的网络交互都被视为未经授权。当检测到未经授权的交互时，应用程序会注册相应的事件。

交互控制规则可以通过以下技术之一进行应用：

- 网络完整性控制 – 该规则描述使用一组特定协议和连接设置的设备之间的网络交互。
- 命令控制 – 该规则描述在设备之间通过过程控制支持的协议之一进行通信期间的被监控系统命令。

交互控制规则包含有关交互/通信的以下信息：

- 参与网络交互的各方。
- 允许的协议或系统命令。

设备之间的网络交互根据设备的 MAC 地址和/或 IP 地址进行识别。如果应用程序中添加了额外的地址空间，则可以为相关地址空间的地址配置交互控制规则。

在分析网络完整性控制的网络交互时，应用程序还会检查这些交互中的 IP 地址，看它们是否属于已知子网。已为所有 IPv4 交互已验证 IP 地址。仅当必须根据下表控制每次交互时，应用程序才会根据网络完整性控制规则检查每次交互（并在必要时注册相应的事件）。

交互受到控制的 IP 地址子网

源子网	目标子网				
	私人，IT	私人，OT	私人，DMZ	公共	本地链路
私人，IT	否	是	否	否	是
私人，OT	是	是	是	是	是
私人，DMZ	否	是	否	否	是
公共	否	是	否	否	是
本地链路	是	是	是	是	否

示例
在基于网络完整性控制技术控制交互时，应用程序会检查网络数据包的源或目标具有来自**私人，**OT子网的 IP 地址的所有交互。应用程序不检查网络数据包的目标具有来自**私人，**DMZ子网的 IP 地址、而网络数据包源具有来自**私人，**IT子网的 IP 地址的交互。

无论包含系统命令的网络数据包的源和目标 IP 地址属于哪个特定子网，都应用命令控制技术。

交互控制规则可以被启用或禁用。

默认情况下，规则在创建后处于启用状态并被应用以允许所描述的通信。当应用程序检测到启用规则中描述的交互时，它不会注册事件。

禁用的规则旨在描述不必要的网络交互。在交互控制技术的学习模式下，禁用的规则会阻止自动创建描述相同网络交互的新启用规则。在监控模式下，被禁用的规则不被考虑。

如果启用了网络完整性控制和命令控制技术，则应用程序将根据这些技术处理交互控制规则。您还可以为这些技术配置学习模式。

以下方法可用来创建交互控制规则列表：

- 在学习模式下自动生成规则
- 从外部项目导入配置时自动生成规则

- 针对单个设备进行微调交互控制
- 手动创建规则

您可以在 Kaspersky Industrial CyberSecurity for Networks 网络界面的**允许规则**部分配置交互控制规则。本节包含基于网络完整性控制和命令控制技术的交互控制规则表。该规则表可能还包含为事件创建的允许规则。

基于网络完整性控制和命令控制技术注册的事件被归类为系统事件。

您可以在已注册事件表中查看交互控制事件。基于网络完整性控制技术注册的事件具有*高*严重性。基于命令控制技术注册的事件会被分配一个严重性，该严重性取决于为检测到的系统命令定义的严重性级别。

交互控制技术的学习模式

为了减少重复操作并实现规则创建和配置的自动化，应用程序使用了机器学习方法和基线模型。应用程序分析在流量处理过程中检测到的设备网络活动中的各种模式，并生成可直接使用的交互控制规则。机器学习方法仅在启用学习模式时才会使用。

在交互控制学习模式下，应用程序执行以下操作：

- 如果启用网络完整性控制技术，应用程序将基于该技术生成规则。规则针对所有必须根据交互控制的 IP 地址子网表控制的 IPv4 交互生成。当应用程序检测到与禁用规则匹配的网络交互时，它会根据网络完整性控制技术注册事件。这些事件使用被分配了代码 4000002601 的系统事件类型进行注册。
- 如果启用命令控制技术，应用程序将基于该技术生成规则。当应用程序检测到与禁用规则匹配的系统命令时，它会根据命令控制技术注册未授权的系统命令检测事件。事件是使用分配了代码 4000002602 的系统事件类型进行注册的。

当基于交互控制技术生成规则时，应用程序会添加通过分析工业网络流量中的网络交互和系统命令获得的新规则。对于这些规则，**源** 值被设置为 **系统**。如果您手动更改规则设置，**源**将被设置为**用户**。

在流量分析期间检测到的网络交互会被检查是否符合当前的交互控制规则。如果检测到的交互与任何规则都不匹配，应用程序将创建新规则。在这种情况下，不会注册交互检测事件。新规则创建后，应用程序会启用它并根据收到的有关网络交互的数据添加设置值。

如果检测到的交互仅与禁用的规则匹配，则应用程序将根据与该规则对应的技术注册事件。在这种情况下，不会创建新规则。

在学习过程中，应用程序可以优化交互控制规则列表。优化包括将两个或多个具体规则组合成一个通用规则，或者如果有通用规则可用则删除具体规则。满足以下条件的规则将被优化：

- 规则已启用。
- **源**被设置为**系统**。
- 这些规则与同一项技术相关。

如果得到的一般规则仅与检测到的网络交互相对应而与其他交互无关，则规则在优化过程中被合并。例如，在两个设备交互期间检测到系统命令后，一条交互控制规则得到创建。然后在同一设备之间交互时检测到另一个系统命令。在这种情况下，优化后只剩下一条一般规则。它将描述这些设备之间的网络交互期间检测到的两个系统命令。

在学习模式下运行时，应用程序会定期优化相应的交互控制技术的规则。优化频率为每分钟一次。如果在工业网络流量中检测到新的交互，则进行优化。为了使规则表保持最新，您必须更新规则。

学习模式被禁用后，将再进行一次优化。

学习模式被禁用后，交互控制规则的优化可能会有延迟。延迟的长度取决于应用程序接收的数据量，可能持续长达三分钟。在此期间，建议不要对基于网络完整性控制和命令控制技术的学习模式期间生成的规则进行任何更改。

交互控制学习模式必须被启用足够长的时间才能接收有关网络交互的所有必要信息。这个时间取决于工业网络中的设备数量以及它们的运行和维修频率。我们建议您启用学习模式至少一个小时。在大型工业网络中，可以启用学习模式一段时间（从一天到几天），以积累最大量数据。

交互控制技术的监控模式

在交互控制监控模式下，应用程序执行以下操作：

- 如果启用网络完整性控制技术，应用程序将检查设备的网络交互是否符合基于该技术的规则。当应用程序检测到没有启用规则的网络交互时，它会根据网络完整性控制技术注册未经授权的通信检测事件。这些事件使用被分配了代码 4000002601 的系统事件类型进行注册。

- 如果启用命令控制技术，应用程序将检查设备的网络交互是否符合基于该技术的规则。当应用程序检测到没有启用规则的系统命令时，它会根据命令控制技术注册未经授权的系统命令检测事件。事件是使用分配了代码 4000002602 的系统事件类型进行注册的。

与不同技术相关的规则彼此独立应用。因此，为了允许使用系统命令，允许规则表必须为该系统命令和传输该命令的网络数据包创建规则（自动或手动）。

在学习模式下自动生成交互控制规则

在学习模式下，Kaspersky Industrial CyberSecurity for Networks 会自动生成交互控制规则。如果检测到的网络交互与允许规则表中的任何规则都不匹配，则应用程序会创建新规则。

创建规则时，应用程序会定义从与检测到的网络交互有关的流量中接收的参数值。

如果正在为交互创建网络完整性控制规则，其中通信一方的 IP 地址位于应用程序已知的子网中，则应用程序可能不会将与此 IP 地址一起检测到的 MAC 地址添加到规则设置中。如果在**子网设置忽略 NIC 规则的 MAC 地址**忽略 NIC 规则的 MAC 地址切换按钮，则会添加检测到的子网 IP 地址的 MAC 地址。

在学习模式下，应用程序可以自动创建交互控制规则，允许传输 Kaspersky Industrial CyberSecurity for Nodes/Kaspersky Industrial CyberSecurity for Linux Nodes 的系统命令。为了方便在集成的 Kaspersky Industrial CyberSecurity 解决方案中联合使用应用程序需要这些规则。要在启用学习模式之前自动创建规则，您必须在同一工业网络中安装了 Kaspersky Industrial CyberSecurity for Nodes/Kaspersky Industrial CyberSecurity for Linux Nodes 的计算机上启用 PLC 项目完整性检查组件。有关启用此组件的详细信息，请参阅 Kaspersky Industrial CyberSecurity for Nodes/Kaspersky Industrial CyberSecurity for Linux Nodes 的帮助系统。

从外部项目导入配置时自动生成交互控制规则

Kaspersky Industrial CyberSecurity for Networks 在从 IEC 61850 设备项目导入配置时会自动生成交互控制规则。应用程序根据正在导入的配置中的设备信息创建新规则。

加载项目后，Kaspersky Industrial CyberSecurity for Networks 会检查设备之间交换的流量中的数据是否符合导入的配置。如果 Kaspersky Industrial CyberSecurity for Networks 检测到流量异常，就会记录事件。

如果正在被导入的配置定义了设备之间通信的协议和连接设置，应用程序就会创建网络完整性控制规则。当应用程序检测到与禁用规则匹配的网络交互时，它会根据网络完整性控制技术注册事件。

如果正在被导入的配置定义了用于设备间通信的系统命令，应用程序就会创建命令控制规则。当检测到与禁用规则匹配的系统命令时，它会使用命令控制记录未经授权的系统命令的检测。

对于从 IEC 61850 设备的项目导入配置时创建的规则，**源**被设置为**系统**。如果您手动更改规则设置，**源**将被设置为**用户**。

在允许规则表中查看交互控制规则

交互控制规则显示在应用程序 Web 界面的**允许规则**部分的允许规则表中。交互控制规则包括以下类型：

- 基于网络完整性控制技术的 NIC 规则。
- 基于命令控制技术的 CC 规则。

交互控制规则的设置显示在表格的以下列中：

- **规则 ID**

  规则的唯一 ID。

- **状态**（◐ 图标）

  规则的当前状态（*已启用*或*已禁用*）。

- **规则类型**

  对于交互控制规则，这表示规则的技术（NIC 或 CC）。EVT 类型适用于禁用事件注册的规则。

- **协议/命令**

  对于与网络完整性控制技术（NIC 类型）相关的规则或禁用事件注册（EVT 类型）的规则，这是所使用的协议集。对于与命令控制技术（CC 类型）相关的规则，这是协议和系统命令。应用程序根据网络数据包的内容确定的协议以斜体表示。

- **端 1**

  网络交互一方的设备名称/地址信息。您可以使用以下设置启用或禁用地址信息的地址和端口的显示：**MAC 地址**、**IP 地址**和**端口号**。如果向应用程序添加了其他地址空间，您可以使用以下设置启用或禁用地址空间名称的显示：

  - **MAC 地址的 AS** – 包含交互控制规则中的 MAC 地址的地址空间。只有当地址空间具有数据链 (L2)**数据链路 (L2)地址空间规则**时，此设置才能包含地址空间的名称。
  - **IP 地址的 AS** – 包含交互控制规则中的 IP 地址的地址空间。只有当地址空间具有**网络 (L3)**被选为 OSI 模型层的地址空间规则时，此设置才能包含地址空间的名称。

- **端 2**

  网络交互对方的设备名称/地址信息。地址信息的显示可以按照与**端 1**列相同的方式配置。

- **注释**

  关于规则的其他信息。

- **创建日期**

  规则创建的日期和时间。

- **更改时间**

  规则最后修改的日期和时间。

- **事件中的规则**

  必须在事件中指明的过程控制规则或入侵检测规则的名称（对于 EVT 规则）。

- **监控点**

  事件中必须指明的监控点名称（针对 EVT 规则）。

- **事件类型**

  事件类型的 ID 和标题（针对 EVT 规则）。

- **源**

  有关规则来源的信息。

查看规则表时，您可以使用配置、过滤、搜索和排序功能。

针对单个设备进行微调交互控制

当交互控制技术在监控模式下运行时，只要检测到的设备之间的交互不符合启用的交互控制规则，应用程序就会注册事件。此类事件被视为设备*网络行为的偏差*。您可以使用这些事件来微调（重新培训）应用于各个设备的交互控制。微调包括使用网络完整性控制和命令控制技术根据注册事件自动创建允许规则。

如果尚未为这些事件分配*已解决*"状态，则会自动为与所选设备相关的事件创建网络行为偏差的允许规则。自动创建允许规则后，应用程序会为这些事件分配*已解决*状态。

您可以查看在监控设备网络交互时注册的未处理事件的数量信息。该信息显示在"**网络行为**"选项卡上的设备详细信息区域中。要查看有关已注册事件的详细信息，您可以使用"**学习质量**"小部件导航到事件表。

要微调单个设备的交互控制：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择"**资产**"部分。

3. 在**设备**选项卡上，选择您想要根据已注册事件创建允许规则的设备。

4. 右键单击以打开上下文菜单。

5. 在上下文菜单中，选择下列选项之一：

   - 如果选择了一个设备，则**完成设备学习**。
   - 如果选择了多个设备，则**完成设备学习**。

   将打开一个带有确认提示的窗口。

6. 如果选定设备的网络行为偏差事件存在相关风险，并且您想要同时为所有这些风险分配*已接受*状态，请选中**为与事件相关的风险分配"已接受"状态**复选框。

7. 在提示窗口中，确认对所选设备进行交互控制的微调。

手动创建交互控制规则

本节包含有关手动创建交互控制规则的说明。

使用空白设置或模板中的设置创建交互控制规则

要使用空白设置或模板中的设置创建交互控制规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**允许规则**部分，单击**添加规则**打开详细信息区域。

3. 如果要从模板中定义设置值，请在详细信息区域中单击**使用模板**，在打开的窗口中选择必要的模板，然后单击**应用**。

4. 在详细信息区域中，选择相关交互控制技术对应的规则类型：

   - 如果要创建基于网络完整性控制技术的规则，请单击**NIC**。
   - 如果要创建基于命令控制技术的规则，请单击**CC**。

5. 在**协议**字段中，指定用于设备之间交互的协议。

   当选择**协议**字段时，一个窗口将打开，其中显示以协议堆栈树形式显示的受支持协议表。您可以使用包含后续层协议的协议名称旁边的**+**和**-**按钮来管理树元素的显示方式。

   如有必要，请使用表格上方的搜索字段查找相关协议。

   要指定协议：

   a. 在协议表中，选择要为规则指定的协议。要选择相关协议，请单击协议表左列中显示的按钮。

   > 对于网络完整性控制规则，您可以选择受支持协议表中显示的任何协议。对于命令控制规则，您只能从受支持的过程控制协议中选择一个协议。

   b. 单击**确定**。

   如果您选择了应用程序可以根据网络数据包的内容识别的协议，则**协议**字段下方会出现有关此协议的通知。

6. 如果为规则选择了命令控制技术，请在**命令**字段中指定相关的系统命令。

选择**命令**字段后，一个窗口将打开，其中列出适用于所选协议的系统命令。要指定命令：

a. 在系统命令列表中，选中应被允许的命令旁边的复选框。如果要允许所有命令，您可以选中所有复选框或清除所有命令的复选框。

b. 单击**确定**。

7. 如果需要，请在**注释**字段中输入有关该规则的其他信息。

8. 在**端 1**和**端 2**设置组中，指定网络交互参与者（各方）的可编辑地址信息。根据所选的协议（或协议集），地址信息可能包含 MAC 地址、IP 地址和/或端口号。如果向应用程序添加了额外的地址空间，则可以为地址指定地址空间的名称。

为了自动填充网络交互一方的地址信息，您可以选择对应用程序已知的设备。为此：

a. 单击**指定设备地址**打开设备选择窗口。

b. 在设备选择窗口中，选中要使用的设备旁边的复选框。

设备选择窗口包含一个表，您可以在其中配置列的布局和顺序，还可以像“资产”部分中的**资产**一样进行过滤、搜索和排序。

c. 在设备选择窗口中单击**确定**。

9. 在详细信息区域中，单击**保存**。

应用程序将检查当前的交互控制规则列表。

10. 如果交互控制规则包含其中所有设置匹配的已启用规则，您将看到有关存在匹配规则的警告。在这种情况下，关闭警告并更改已创建规则的设置。

11. 如果交互控制规则包含具有更多常规设置的已启用规则，您将看到有关存在常规规则的警告。如果存在一般规则，则应用程序中将不会使用新的具体规则。警告将包含保存新的特定规则的提示。要创建具有已定义设置的新规则，请在提示窗口中确认您的决定（例如，如果您想要删除常规规则）。

新规则将被添加到允许规则表中。

12. 如果交互控制规则包含具有更具体设置的已启用规则，您将看到有关存在更具体规则的警告。通用规则出现后，具体规则将不再用于应用程序中。警告将包含删除特定规则的提示。要删除特定规则，请在提示窗口中确认您的决定。

如果规则表包含具有更具体或匹配设置的已禁用规则，应用程序将从列表中删除这些规则。删除这些规则时应用程序不会显示提示。

13. 对于基于命令控制技术的新规则，如果尚未启用允许设备之间网络交互的规则，则系统将提示您创建基于网络完整性控制技术的相应规则。在这种情况下，建议您在创建当前规则的同时创建附加规则。为此，请在提示窗口中确认您的决定并执行必要的操作以基于网络完整性控制技术创建新规则。

从现有规则创建交互控制规则

要从现有交互控制规则创建交互控制规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**允许规则**部分，选择要用作创建新规则的基础的规则。

3. 右键单击以打开上下文菜单。

4. 在上下文菜单中，选择“**复制规则**”。

   规则编辑模式下的详细信息区域将出现在 Web 界面窗口的右侧。新规则的设置将采用从所选规则的设置中获取的值。

5. 根据需要更改设置。为此，请完成创建规则过程中所述的设置初始值为空的步骤 4-9。

根据为网络完整性控制或命令控制技术注册的事件创建规则

从网络完整性控制或命令控制注册的事件创建交互控制规则。

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**事件**”部分。

3. 在已注册事件表中，选择要用作创建交互控制规则基础的事件。

   详细信息区域显示在 Web 界面窗口的右侧部分。

4. 在详细信息区域中，单击**创建允许规则**。

   允许规则部分在浏览器窗口中打开。规则编辑模式下的详细信息区域将出现在 Web 界面窗口的右侧。新规则的设置将采用从有关事件的已保存信息中接收的值。

5. 如有必要，编辑新规则的设置。为此，请完成创建规则过程中所述的设置初始值为空的步骤 4-9。如果不需要更改新规则的设置，请单击**保存**来保存该规则。

编辑交互控制规则设置

您可以编辑已启用的交互控制规则的设置。您不能编辑已禁用的规则。

要编辑交互控制规则的设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**允许规则**部分，选择相关的 NIC 或 CC 规则以编辑其设置。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 单击**编辑**。

4. 按需要更改设置。

启用和禁用交互控制规则

可以为交互控制规则分配*已启用*或*已禁用*状态。规则创建后默认已启用。

您可以禁用当交互控制技术在监控模式下运行时不应被使用的规则。

要更改交互控制规则的状态：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**允许规则**部分，选择您想要更改状态的交互控制规则。

3. 单击**启用**或**禁用**可启用或禁用规则。显示的按钮取决于其对应操作是否与一个或多个选定规则相关。

   如果选择了所有满足当前过滤和搜索设置的规则，且选定规则的数量超过 1000 条，则应用程序不会检查规则状态。如果是这种情况，详细信息区域将显示用于更改规则状态的两个按钮。

暂停和恢复设备网络交互的监控

默认情况下，交互控制技术的监控模式应用于工业网络中的所有设备。如有必要，您可以暂时暂停对单个设备的网络交互监控（例如，如果设备正在进行维护和调试工作）。如果暂停对某个设备的网络交互监控，应用程序不会为此设备注册未经授权的交互警报事件或未经授权的系统命令警报事件。

设备恢复正常操作后，您可以恢复对该设备的网络交互的监控。

对于在工业网络段之间执行网络交换功能的设备（路由设备），不建议暂停对网络交互的监控。如果暂停对此类路由设备的监控，可能会对通过该路由设备在不同工业网络段上进行通信的设备的交互控制规则的应用产生负面影响。

您可以在“网络行为**网络行为有关设备网络行为的信息**。设备网络交互的当前监控状态显示在“**网络交互控制**”小部件中。有关在监控设备网络交互时注册的未处理事件数量的信息显示在“**学习质量**”小部件中。小部件中的某些定量值允许您导航到应用程序 Web 界面的相应部分。例如，要查看有关未处理事件的详细信息，您可以从“**学习质量**”小部件导航到事件表。

要暂停或恢复对设备网络交互的监控：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

3. 在**设备**选项卡上，选择要暂停或恢复网络交互监控的设备。

4. 右键单击打开上下文菜单。

5. 在上下文菜单中，选择相关选项：**网络行为 → 暂停监控**或**网络行为 → 恢复监控**。

   将打开一个带有确认提示的窗口。

6. 在提示窗口中，确认是否要暂停或恢复对网络交互的监控。

删除交互控制规则

您可以有选择地删除一个或多个交互控制规则。被删除的规则不再适用于交互控制技术，无论是在监控模式还是学习模式下。

删除交互控制规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择**允许规则**部分。

3. 在规则表中，选择要删除的交互控制规则。

4. 单击**删除**。

   将打开一个带有确认提示的窗口。根据所选规则的状态，提示将建议以下选项：

   - 如果所有选定的规则都已启用，应用程序将提示您删除选定的规则、禁用它们或取消操作。如果选择了所有满足当前过滤和搜索设置的规则，且选定规则的数量超过 1000 条，则不会检查此条件。
   - 如果选定的规则中有已禁用的规则或选择了所有满足当前过滤和搜索设置的规则，且选定的规则数量超过 1000 条，应用程序将提示您删除选定的规则或取消操作。

5. 在提示窗口中，确认删除规则。

配置入侵检测和网络异常检测

Kaspersky Industrial CyberSecurity for Networks 可以分析传入的工业网络流量，以发现入侵、攻击和各种异常情况的迹象。为此，您可以使用入侵检测规则、基于内置算法的入侵检测方法和网络异常检测规则。如果在流量分析期间触发了规则或内置算法，则应用程序使用入侵检测技术来记录事件。

通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器时，可以配置相关方法和规则。可配置的入侵检测规则和网络异常检测规则集显示在**检测规则**部分中。应用程序允许您在**设置 → 部署**中启用或禁用检测技术和方法的使用。

您可以在已注册事件表中查看入侵检测和网络异常检测事件。

管理入侵检测规则集

"*入侵检测规则*"描述表征工业网络中可能存在攻击迹象的流量异常情况。规则包含入侵检测系统用于分析流量的条件。

入侵检测规则存储在服务器和探测器上。

当使用基于规则的入侵检测方法时，应用程序应用入侵检测规则。您可以启用或禁用此方法。

入侵检测规则根据某些属性被分组为规则集。例如，规则可以根据用途进行分组，包括在旨在检测某些类型入侵的集合中。您可以使用以下类型的规则集：

- 系统规则集。这些规则集由卡巴斯基提供，用于检测最常遇到的攻击或不必要的网络活动的迹象。系统规则集在应用程序安装后立即可用。您可以通过安装更新来更新系统规则集。
- 用户定义的规则集。这些规则集由用户单独加载到应用程序中。要加载它们，您需要使用包含定义入侵检测规则的数据结构的文件。这些文件必须位于同一文件夹中，具有 RULES 扩展名。用户定义的规则集的名称必须与从其加载这些规则集的文件的名称相匹配。

应用程序支持在所有加载的规则集中累计应用不超过 50000 条规则。加载的规则集数量限制为 100。

> 从用户定义的规则集加载的规则可能包含流量分析条件，当这些规则被触发时，应用程序将记录过多的事件。在这种情况下，请记住记录太多事件可能会影响入侵检测系统的性能。

入侵检测规则集可以被启用或禁用。如果启用了基于规则的入侵检测方法，则在流量分析期间将应用已启用集中的规则。如果禁用某个规则集，则不会应用该规则集中的规则。

加载规则集时，应用程序会验证规则集中的规则。如果在验证的规则中检测到错误，应用程序将阻止应用这些规则。如果在规则集的所有规则中检测到错误或规则集不包含任何规则，则应用程序将禁用此规则集。

有关规则集和检测到的错误的信息，请参阅**检测规则 → 入侵检测**部分。

当在流量中检测到已启用规则集的规则中定义的条件时，应用程序会注册规则触发事件。这些事件使用被分配了以下代码的系统事件类型进行注册。

- 4000003000 – 针对触发系统规则集的规则时发生的事件。
- 4000003001 – 针对触发用户定义规则集的规则时发生的事件。

用户定义的规则集可能包含从其他入侵防御和检测系统收到的规则。当处理这些规则时，应用程序不会执行其定义的操作，这些操作原本会被应用于网络数据包（例如，*丢弃*和*拒绝*操作）。当 Kaspersky Industrial CyberSecurity for Networks 中有入侵检测规则被触发时，仅执行事件注册。

Kaspersky Industrial CyberSecurity for Networks 事件的分数与入侵检测规则中的特定优先级相对应（见下表）。

将规则优先级映射到事件分数

入侵检测规则优先级	Kaspersky Industrial CyberSecurity for Networks 事件分数值
4 或更高	2.5
3	4.5

入侵检测规则优先级	Kaspersky Industrial CyberSecurity for Networks 事件分数值
2	6.5
1	9

启用和禁用入侵检测规则集

可以为入侵检测规则集分配*已启用*或*已禁用*状态。如果一组规则被禁用，则该组中的规则将不用于入侵检测。

只要在安装了应用程序组件（服务器和探测器）的所有计算机上启用或禁用选定的规则集，入侵检测系统就会重新启动。需要重新启动才能应用更改。

具有管理员或安全官角色的用户可以更改入侵检测规则集的状态。

要更改入侵检测规则集的状态：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**检测规则** → **入侵检测**部分，选择您想要更改其状态的规则集。
3. 右键单击以打开上下文菜单。
4. 在上下文菜单中，选择下列选项之一：
   - 如果要从所选规则集中启用所有已禁用的规则集，**启用**。
   - 如果要禁用所选规则集中所有已启用的规则集，**禁用**。
   - 如果要反转所有选定规则集的状态，请**更改所选规则集的状态**。此选项可让您在安装了应用程序组件的所有计算机上快速启用或禁用具有不同状态的选定规则集，因为入侵检测系统只需在所有计算机上重新启动一次即可一起应用所有更改。

   将打开一个带有确认提示的窗口。
5. 在提示窗口中，单击**确定**。

加载和替换用户定义的入侵检测规则集

您可以将文件中的入侵检测规则集加载到应用程序中。包含入侵检测规则描述的文件必须位于同一文件夹中，并且具有规则扩展名，然后才能加载到应用程序中。文件名称不得包含以下字符：`\ / : * ? , " < > |`。

从文件加载入侵检测规则后，这些规则将作为用户定义的规则集保存在应用程序中。规则集的名称与从其加载该规则集的文件的名称相匹配。

> 从文件加载规则集时，当前用户定义的规则集将被从表中删除并用新的规则集替换。不过，系统规则集（其**源**列显示**系统**值）不会被从表中删除。

具有管理员或安全官角色的用户可以加载用户定义的入侵检测规则集。

要加载和替换用户定义的入侵检测规则集：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**检测规则→入侵检测**。
3. 单击工具栏中的**替换所有用户自定义规则**打开用于选择包含入侵检测规则文件的文件夹的窗口。
4. 当提示窗口出现时，单击**确定**。
5. 在您使用的浏览器的标准窗口中，选择包含必要文件的文件夹，然后单击用于从该文件夹传输文件的按钮。

   包含规则集的表显示新的用户定义的规则集。对于这些规则集，**源**列显示**用户**值。所有未检测到错误的规则集都将被启用。
6. 检查已加载的规则集中的规则是否存在错误。

   有关检测到的错误的信息显示在**规则**列中。如果没有错误，则会显示*正常*状态。如果规则集包含错误，您可以点击**详细信息**查看有关它们的详细信息。
7. 如有必要，更改规则集的状态（包括*某些规则中的错误*的规则集）。

删除用户定义的入侵检测规则集

您可以从文件中删除已加载到应用程序的所有用户定义的入侵检测规则集。您不能有选择地删除单个用户定义的规则集。如果您只想使用应用程序中现有的某些规则集，可以将包含这些规则集的文件复制到单独的文件夹中，用该文件夹中的规则集替换所有用户定义的规则集。

具有管理员或安全官角色的用户可以删除用户定义的入侵检测规则集。

要删除用户定义的入侵检测规则集：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**检测规则→入侵检测**。
3. 通过单击工具栏中的**删除所有用户自定义规则**来开始删除用户定义的规则集。

   将打开一个带有确认提示的窗口。
4. 在提示窗口中，单击**确定**。

所有用户定义的入侵检测规则集都将被从表中删除。

使用其他入侵检测方法

您可以应用以下附加方法进行入侵检测：

- 检测 ARP 数据包中伪造地址的迹象（ARP 欺骗）。

  如果启用了检测 ARP 数据包中伪造地址的迹象，Kaspersky Industrial CyberSecurity for Networks 会扫描 ARP 数据包中指示的地址并检测低级中间人 (MITM) 攻击的迹象。在使用 ARP 协议的网络中，此类攻击的特点是流量中存在伪造的 ARP 消息。

当应用程序检测到 ARP 数据包中存在伪造地址的迹象时，应用程序会根据入侵检测技术注册事件。这些事件使用被分配了以下代码的系统事件类型进行注册。

- 4000004001 – 用于检测与 ARP 请求无关的多个 ARP 回复。
- 4000004002 – 用于检测从同一 MAC 地址到不同目的地的多个 ARP 请求。

- TCP 协议异常检测

  如果启用了 TCP 协议异常检测，Kaspersky Industrial CyberSecurity for Networks 扫描受支持的应用程序级协议中数据流的 TCP 段。

  当检测到包含不同内容的重叠 TCP 段的数据包时，应用程序会根据入侵检测技术注册一个事件。这些事件使用被分配了代码 4000002701 的系统事件类型进行注册。

- IP 协议异常检测

  如果启用了 IP 协议异常检测，Kaspersky Industrial CyberSecurity for Networks 将扫描碎片化的 IP 数据包。

  当应用程序检测到 IP 数据包组装中的错误时，它会注册入侵检测技术事件。这些事件使用被分配了以下代码的系统事件类型进行注册。

  - 4000005100 用于检测组装 IP 数据包时的数据冲突（IP 片段重叠）。
  - 4000005101 用于检测超出最大允许大小的 IP 数据包（IP 片段溢出）。
  - 4000005102 用于检测其初始片段小于预期（IP 片段太小）的 IP 数据包。
  - 4000005103 用于检测 IP 数据包的错误关联片段。

- 蛮力攻击和扫描检测

  如果启用了暴力攻击和扫描检测，Kaspersky Industrial CyberSecurity for Networks 会分析网络活动统计数据，以检测对帐户凭据、拒绝服务、扫描、网络服务欺骗和其他异常的暴力攻击迹象。

  此方法使用内置规则。当规则被触发时，应用程序会根据入侵检测技术注册一个事件。这些事件使用被分配了代码 4000003002 的系统事件类型进行注册。

您可以启用或禁用这些方法。无论入侵检测规则的可用性和状态如何，您都可以应用其他入侵检测方法。嵌入式算法用于附加的扫描方法。

管理网络异常检测规则

*网络异常检测规则*有助于检测在网络层面上可能与正常设备活动无法区分的流量异常。为了检测此类异常情况，应用程序会分析已注册网络会话中接收到的协议属性。如果发现规则中描述的任何属性、其值和/或模式，则会触发网络异常检测规则。当规则被触发时，Kaspersky Industrial CyberSecurity for Networks 会记录一个事件。

协议属性包括网络会话中流量的各种特征。这些属性保存在 Kaspersky Industrial CyberSecurity for Networks 服务器的单独数据库中。用于存储协议属性的数据库能够高速处理传入数据及其分析请求。为了确保基于规则的分析对数据库管理系统和应用程序的整体性能的影响最小，属性搜索查询在 SQL 中执行。您可以自行在规则中生成必要的 SQL 查询，也可以使用带有现成 SQL 查询的规则模板。

网络异常检测规则分析支持以下协议的属性：

- DCE/RPC
- DNS

- Kerberos
- LDAP

当使用获取协议属性的方法时，应用程序会将协议属性保存到数据库中。您可以启用或禁用此方法。要使用获取协议属性的方法，还必须启用网络会话检测方法。这两种方法必须在所有安装了用于接收信息的应用程序组件的节点上启用。

在特定时间间隔内，对数据库中接收到的协议属性执行基于规则的网络异常搜索。每条规则的时间间隔持续时间由**搜索深度**参数定义。持续时间从间隔结束边界的时刻开始计算。根据规则的启动方式，间隔结束边界的时间可以定义如下：

- 当规则按照配置的运行计划自动启动时，时间间隔的结束边界与规则启动的时间一致。
- 手动启动规则时，您可以手动定义间隔结束的日期和时间。

要快速配置已创建的网络异常检测规则的设置，可以使用内置的规则模板。这些模板由卡巴斯基提供。应用程序安装完成后，即可立即查看应用程序中内置的模板列表。您可以通过安装更新来更新内置模板列表。

如果在创建规则时未选择内置模板，则必须完全手动配置规则设置（包括编写 SQL 查询以在数据库中搜索协议属性）。在这种情况下，**用户自定义**模板将显示为规则所使用的模板。如果您选择了一个内置模板，然后更改了确保操作逻辑符合所选内置模板的设置（特别是 SQL 查询文本或主要事件注册设置），则会显示同一个模板。如果更改规则的其他设置（例如，自动计划启动设置或 SQL 查询变量中的阈值），并且规则中的所有模板值未解锁，则规则与所选内置模板之间的链接将得到保留。

网络异常检测规则的最大数量为 200 条。

网络异常检测规则可以启用或禁用。如果某条规则被禁用，应用程序将不会按照配置的计划启动该规则，并且还会阻止手动启动该规则的功能。

您可以在**检测规则 → 网络异常检测**下管理网络异常检测规则。如果需要在 SQL 查询中使用字典值（例如，IP 地址列表）作为变量，您可以在**设置 → 词典**下创建包含必要数据的字典。

当触发网络异常检测规则时，会使用系统事件类型注册一个事件，该事件被分配代码 4000003003。

创建网络异常检测规则

建议您使用合适的内置模板来创建网络异常检测规则。这些模板包含用于检测典型异常的已配置设置（包括现成的 SQL 查询）。大多数情况下，选择内置模板后，您可能只需要对已创建规则的某些值进行一些微调。例如，可能只需要对 SQL 查询变量进行模板值的微调，以更改阈值或指定创建的字典。

创建网络异常检测规则：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**检测规则 → 网络异常检测**部分，单击**添加规则**打开详细信息区域。
3. 在**模板**下拉列表中，选择已创建规则所需的模板。
   规则设置的值将根据所选模板进行定义。

   如果选择**用户自定义**模板，则需要完全手动配置规则设置（包括编写 SQL 查询文本以在数据库中搜索协议属性）。

4. 输入规则名称和描述。

5. 使用**搜索深度**参数来指定在数据库中接收的协议属性中搜索网络异常的时间间隔的持续时间。您可以以秒、分钟、小时或天为单位指定时间间隔。

6. 要根据计划运行规则，请启用“**根据计划运行作业**”选项并配置计划设置：

   a. 在“**频率**”下拉列表中，选择运行作业的频率：**每秒**、**每分钟**、**每小时**、**每天**、**每周**、**每月**。

   b. 根据所选选项，指定设置值以定义精确的作业启动时间。

7. 如果您需要更改 Kaspersky Industrial CyberSecurity for Networks 重新注册规则触发事件的时间间隔，请打开**更改默认值**切换开关，并指定必要的事件重新生成周期。

8. 在**主要事件注册设置**块中，检查规则触发时的事件注册设置，并根据需要配置设置。如果为规则选择了内置模板，则设置将被锁定且无法编辑。在这种情况下，要更改这些设置的值，您必须首先单击包含所选模板的字段上方的**解锁所有模板值**按钮。

   > 单击**解锁所有模板值**按钮后，创建的规则与选定的内置模板之间的链接将被断开。为规则指定了**用户自定义**模板，而不是之前选择的模板。

   在**主要事件注册设置**块中，您可以为应用程序在规则触发时要注册的事件的以下设置指定值：

   - 事件标题和描述。

     当您输入事件的标题或描述时，工具提示或可选择的常规变量会自动出现在光标旁边。

   - 事件分数值。

9. 单击**SQL 特定查询**选项卡。

   选项卡的内容取决于在步骤 3 中选择的模板：

   - 如果选择了内置模板，则**SQL 特定查询**选项卡包含从该模板加载的 SQL 查询文本。SQL 查询中指定的变量列在**使用的变量**块中。

   - 如果选择了**用户自定义**模板，则该选项卡不包含任何数据。在这种情况下，请手动生成 SQL 查询文本（参见步骤 12）。

10. 如果**SQL 特定查询**选项卡包含 SQL 查询文本，请测试此查询在数据库中的运行情况。为此，请单击**执行**按钮。

    验证 SQL 查询是否完成窗口将出现，显示一个包含 SQL 查询验证结果的表格。要控制窗口的显示，请使用右上角的按钮。

11. 如有必要，可通过更改 SQL 查询中使用的变量值来微调 SQL 查询。这些变量显示在**使用的变量**设置块中。您可以显式定义变量的值，也可以使用先前添加的字典来定义变量的值。要替换字典中变量的值，请单击变量旁边的 并选择正确的目录。

    您可以使用目录来存储"date"、"time"、"IP"、"port"、"string"或者"weekday"数据类型的变量。字典不支持数据类型为“int”的变量。

12. 在**SQL 特定查询**字段中，检查 SQL 查询文本并生成任何必要的文本。如果为规则选择了内置模板，则 SQL 查询文本将被锁定，无法编辑。在这种情况下，要更改文本，必须先单击包含所选模板的字段上方的**解锁所有模板值**按钮。

单击**解锁所有模板值**按钮后，创建的规则与选定的内置模板之间的链接将被断开。为规则指定了**用户自定义**模板，而不是之前选择的模板。

生成 SQL 查询文本后，再次执行步骤 10-11。

13. 单击“**保存**”。

更改网络异常检测规则

您可以通过更改设置来微调已创建的网络异常检测规则。例如，您可以更改 SQL 查询变量中的阈值，或者为其指定其他字典。如果规则仍然链接到选定的内置模板（换句话说，没有指定**用户自定义**模板），则无法更改事件注册设置，此规则中不提供 SQL 查询文本。如果要将该规则与其他事件注册设置或不同的 SQL 查询一起使用，可以禁用当前规则并创建具有必要设置的新规则。

具有管理员或安全官角色的用户可以更改网络异常检测规则。

要更改网络异常检测规则的设置：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**检测规则** → **网络异常检测**下，选择要编辑的规则。
   详细信息区域显示在 Web 界面窗口的右侧部分。
3. 单击“**编辑**”。
4. 输入规则名称和描述。
5. 使用**搜索深度**参数来指定在数据库中接收的协议属性中搜索网络异常的时间间隔的持续时间。您可以以秒、分钟、小时或天为单位指定时间间隔。
6. 要根据计划运行规则，请启用“**根据计划运行作业**”选项并配置计划设置：
   a. 在“**频率**”下拉列表中，选择运行作业的频率：**每秒**、**每分钟**、**每小时**、**每天**、**每周**、**每月**。
   b. 根据所选选项，指定设置值以定义精确的作业启动时间。
7. 如果您需要更改 Kaspersky Industrial CyberSecurity for Networks 重新注册规则触发事件的时间间隔，请打开**更改默认值**切换开关，并指定必要的事件重新生成周期。
8. 在**主要事件注册设置**块中，检查规则触发时的事件注册设置，并根据需要进行配置。如果为规则选择了内置模板，则设置将被锁定且无法编辑。
   如果设置可以编辑，您可以为应用程序在规则触发时要注册的事件的以下设置指定值：
   - 事件标题和描述。
     当您输入事件的标题或描述时，工具提示或可选择的常规变量会自动出现在光标旁边。
   - 事件分数值。
9. 单击**SQL 特定查询**选项卡。

10. 如有必要，测试 SQL 查询在数据库中的运行情况。为此，请单击**执行**按钮。

    验证 SQL 查询是否完成窗口将出现，显示一个包含 SQL 查询验证结果的表格。要控制窗口的显示，请使用右上角的按钮。

11. 如有必要，可通过更改 SQL 查询中使用的变量值来微调 SQL 查询。这些变量显示在**使用的变量**设置块中。您可以显式定义变量的值，也可以使用先前添加的字典来定义变量的值。要替换字典中变量的值，请单击变量旁边的 并选择正确的目录。

    您可以使用目录来存储"date"、"time"、"IP"、"port"、"string"或者"weekday"数据类型的变量。字典不支持数据类型为“int”的变量。

12. 在**SQL 特定查询**字段中，检查 SQL 查询文本并生成任何必要的文本。如果为规则选择了内置模板，则 SQL 查询文本将被锁定，无法编辑。

    生成 SQL 查询文本后，再次执行步骤 10-11。

13. 单击“**保存**”。

为网络异常检测规则生成 SQL 查询文本

在创建或修改网络异常检测规则时，您可以手动生成 SQL 查询的文本。查询旨在搜索、提取和分析已注册网络会话中接收的协议的属性。协议属性存储在 Kaspersky Industrial CyberSecurity for Networks 服务器上的一个单独数据库中。要访问此数据库，您需要使用结构化查询语言 (SQL) 生成查询，ClickHouse DBMS 支持 SQL。有关用于执行数据提取和分析操作的支持查询的信息，请参阅ClickHouse 帮助。

建议您使用内置规则模板之一来生成 SQL 查询文本。您可以在创建规则时选择模板。您可以选择与要执行的任务用途最相似的模板。选择内置模板生成其他 SQL 查询文本后，需要点击**解锁所有模板值**按钮。

当您在窗口中输入 SQL 查询字符串时，合适的函数、运算符和设置列表会自动显示。您可以从这些列表中选择所需的项目，以便快速将其插入到 SQL 查询文本中。

网络异常检测规则的 SQL 查询中使用的主要函数和运算符

函数	描述
`选择`	包含网络会话信息表中各个字段的枚举。所列字段均基于 SQL 查询进行访问。查询结果的一部分或全部用于创建一个临时表格，其中包含活动报名数据。临时表格的字段通过别名赋值机制填充值。支持聚合函数（如`sum`）和算术运算符（如`+`）。 请参见下方表格字段列表。
`自`	指定数据来源。数据源可以被指定为以下视图之一，这些视图用于查询数据库中包含网络会话信息的表格，该数据库用于存储协议属性： • `{{sessions}}`根据特定时间间隔进行筛选并提取数据。 • `{{sessions_symmetric}}`是`{{sessions}}`视图的扩展变体，它添加了对称网络会话（源-目标方向相反）。
`其中`	包含对从源接收的数据进行过滤的条件。过滤器表达式可以包含比较运算、逻辑运算符和特殊函数`PARAM_EQ`。 `PARAM_EQ`函数可让您将表中的值与规则中定义的变量进行比较。如果选择字典来替换变量值，则必须在 SQL 查询中指定`PARAM_EQ`函数。 `PARAM_EQ`函数的通用语法如下： `PARAM_EQ(column_value, {{param_name:param_type}})` 其中： • `column_value`是要比较的字段或表达式。 • `{{param_name:param_type}}`指 SQL 查询规则中定义的变量及其类型。
`GROUP BY`	将查询切换到聚合模式，并指定要按其对返回的数据进行分组的字段或别名列表。

函数	描述
`HAVING`	包含用于筛选使用`GROUP BY`运算符获得的结果的条件。
`ORDER BY`	包含一个用于对返回数据进行排序的列表。对于列表项，您可以指定修饰符来确定排序方向： • `DESC`按降序排序。 • `ASC`按升序排序。

包含网络会话信息的表格字段

在用于存储协议属性的数据库中，包含网络会话信息的表包含以 15 秒为间隔接收的数据块 (chunk) 的行。表中每个已注册的网络会话都以单独的数据块形式呈现，SQL 查询中的调用必须在这些数据块内进行。

包含网络会话信息的表包含以下字段，这些字段可以在 SQL 查询中调用：

- `session_id`，类型`UInt64`：网络会话的唯一标识符
- `chunk_start_time`，类型`DateTime64(6, 'UTC')`：与网络会话相关的数据块 (chunk) 的开始时间，精确到微秒。
- `partition_id`，类型`UInt64`：数据块 (chunk) 中分区的 ID
- `start_time`，类型`DateTime64(6, 'UTC')`：数据块 (chunk) 中第一个数据包的时间，精确到微秒。
- `end_time`，类型`DateTime64(6, 'UTC')`：数据块 (chunk) 中最后一个数据包的时间，精确到微秒。
- `sip`，类型`IPv4`：源 IP 地址（端 1）
- `dip`，类型`IPv4`：目标 IP 地址（端 2）
- `sport`，类型`UInt16`：源端口（端 1）
- `dport`，类型`UInt16`：目标端口（端 2）
- `smac`，类型`FixedString(17)`：源 MAC 地址（端 1），格式为 XX:XX:XX:XX:XX:XX。
- `dmac`，类型`FixedString(17)`：目标 MAC 地址（端 2），格式为 XX:XX:XX:XX:XX:XX。
- `smac_as_id`，类型`UInt64`：源 MAC 地址（端 1）转换为 64 位整数
- `dmac_as_id`，类型`UInt64`：目标 MAC 地址（端 2）转换为 64 位整数
- `sip_as_id`，类型`UInt64`：源 IP 地址（端 1）转换为 64 位整数
- `dip_as_id`，类型`UInt64`：目标 IP 地址（端 2）转换为 64 位整数
- `vlanid`，类型`UInt16`：VLAN ID
- `ether_type`，类型`UInt16`：以太网帧类型（例如：IPv4 为 2048）
- `ipv4_type`，类型`UInt8`：IPv4 类型（8 位值）
- `protocol`，类型`LowCardinality(String)`：表中应用层协议的名称（例如：`GenericDceRpc`、`Ssh`）

- `transport_protocol`，类型`LowCardinality(String)`：表中传输层协议的名称（例如：`Tcp`、`Udp`）
- `bytes_sent_delta`，类型`UInt64`：数据块 (chunk) 期间发送的数据量
- `packets_sent_delta`，类型`UInt64`：数据块 (chunk) 期间发送的数据包数量
- `bytes_received_delta`，类型`UInt64`：数据块 (chunk) 期间接收到的数据量
- `packets_received_delta`，类型`UInt64`：数据块 (chunk) 期间接收到的数据包数量
- `dpi_dns`，类型 `Array(Map(String, String))`：DNS 协议流量中网络事件的结构化数据
- `dpi_dns_raw`，类型 `Array(String)`：DNS 协议流量中网络事件的 JSON 格式数据
- `dpi_krb`，类型 `Array(Map(String, String))`：关于 Kerberos 协议流量的结构化数据
- `dpi_krb_raw`，类型 `Array(String)`：关于 Kerberos 协议流量的 JSON 格式数据
- `dpi_dcerpc`，类型 `Array(Map(String, String))`：关于 DCE/RPC 协议流量的结构化数据
- `dpi_dcerpc_raw`，类型 `Array(String)`：关于 DCE/RPC 协议流量的 JSON 格式数据
- `dpi_ldap`，类型 `Array(Map(String, String))`：关于 LDAP 协议流量的结构化数据
- `dpi_ldap_raw`，类型 `Array(String)`：关于 LDAP 协议流量的 JSON 格式数据
- `total_attributes`，类型`UInt32 MATERIALIZED`：`dpi_dns_raw`、`dpi_krb_raw`、`dpi_dcerpc_raw`和`dpi_ldap_raw`字段中的属性总数
- `dpi_attributes_raw`，类型`Array(String) MATERIALIZED`：属性的 JSON 格式数据的组合数组

包含活动报名数据的表格字段

包含活动报名数据的表可包含以下字段，这些字段的值通过 SQL 查询中的别名赋值机制进行填充：

- 必填字段：
  - `aggregation_id`，类型`String`：用于标识事件的唯一聚合标识符
  - `session_ids`，类型`Array(UInt64)`：与事件关联的网络会话 ID 数组
  - `时间戳`，类型`DateTime64(6, 'UTC')`：事件首次发生的日期和时间
  - `protocol`，类型`String`：包含网络会话信息的表中的协议名称（例如：`Ssh`）
- 用于在事件中存储地址信息和其他网络交互数据的字段（可选字段，可在 SQL 查询中填写）：
  - `sip`，类型`IPv4`：源 IP 地址
  - `dip`，类型`IPv4`：目标 IP 地址

- `运动`，类型`UInt16`：源端口
- `dport`，类型`UInt16`：目标端口
- `smac`，类型`FixedString(17)`：源 MAC 地址，格式为 XX:XX:XX:XX:XX:XX
- `dmac`，类型`FixedString(17)`：目标 MAC 地址，格式为 XX:XX:XX:XX:XX:XX
- `smac_as_id`，类型`UInt64`：源 MAC 地址的地址空间标识符
- `dmac_as_id`，类型`UInt64`：目标 MAC 地址的地址空间标识符
- `sip_as_id`，类型`UInt64`：源 IP 地址的地址空间标识符
- `dip_as_id`，类型`UInt64`：目标 IP 地址的地址空间标识符
- `vlanid`，类型`UInt16`：VLAN ID
- `ether_type`，类型`UInt16`：以太网帧类型
- `ipv4_type`，类型`UInt8`：IPv4 类型

- 任意命名的字段，用于在事件中使用variable `$extra.<paramName>`指定它们的值。

包含网络会话信息的表中的协议名称

协议栈树中的路径	表中的协议名称
Ethernet I	EthernetI
Ethernet I \ LLC \ Cisco 发现协议 (CDP)	Cdp
Ethernet I \ LLC \ Emerson Ovation：通过 LLC 进行交互	Emerson_Ovation_OverLlc
Ethernet I \ LLC \ Foxboro FCP280/FCP270：设备交互	`FoxboroHps`
Ethernet I \ LLC \ HiDiscovery	`HiDiscovery`
Ethernet I \ LLC \ IS-IS over Ethernet I	`IsIsOverEthernetI`
Ethernet I \ LLC \ ISO 8073 \ Siemens S7comm	`SiemensIndustrialEthernet`
Ethernet I \ LLC \ VNIIA	`Vniia`
Ethernet II	`EthernetII`
Ethernet II \ ARP	`ARP`
Ethernet II \ IEC 61850: GOOSE	`IEC61850_GOOSE`
Ethernet II \ IEC 61850: 采样值	`SAMPLED_VALUES`
Ethernet II \ IP	`IPv4`
Ethernet II \ IP \ 3PC	`ip34`
Ethernet II \ IP \ 主动网络	`ip107`
Ethernet II \ IP \ ARIS	`ip104`
Ethernet II \ IP \ AX.25	`ip93`
Ethernet II \ IP \ BBN RCC 监控	`ip10`

Ethernet II \ IP \ BNA	`ip49`
Ethernet II \ IP \ BR-SAT-MON	`ip76`
Ethernet II \ IP \ CBT	`ip7`
Ethernet II \ IP \ CFTP	`ip62`
Ethernet II \ IP \ CHAOS	`ip16`
Ethernet II \ IP \ Compaq-Peer	`ip110`
Ethernet II \ IP \ CPHB	`ip73`
Ethernet II \ IP \ CPNX	`ip72`
Ethernet II \ IP \ CRTP	`ip126`
Ethernet II \ IP \ CRUDP	`ip127`
Ethernet II \ IP \ DCCP	`ip33`
Ethernet II \ IP \ DCN-MEAS	`ip19`
Ethernet II \ IP \ DDP	`ip37`
Ethernet II \ IP \ DDX	`ip116`
Ethernet II \ IP \ DGP	`ip86`
Ethernet II \ IP \ DSR	`ip48`
Ethernet II \ IP \ EGP	`ip8`
Ethernet II \ IP \ EIGRP	`EIGRP`
Ethernet II \ IP \ EMCON	`ip14`
Ethernet II \ IP \ ETHERIP	`ip97`
Ethernet II \ IP \ FCIP	`ip133`
Ethernet II \ IP \ FIRE	`ip125`
Ethernet II \ IP \ GGP	`ip3`
Ethernet II \ IP \ GMTP	`ip100`
Ethernet II \ IP \ GRE	`GRE`
Ethernet II \ IP \ HMP	`ip20`
Ethernet II \ IP \ IATP	`ip117`
Ethernet II \ IP \ ICMP	`Icmp`
Ethernet II \ IP \ IDPR	`ip35`
Ethernet II \ IP \ IDPR-CMTP	`ip38`
Ethernet II \ IP \ IDRP	`ip45`
Ethernet II \ IP \ IFMP	`ip101`
Ethernet II \ IP \ IGMP	`IGMP`
Ethernet II \ IP \ IGP	`ip9`
Ethernet II \ IP \ I-NLSP	`ip52`
Ethernet II \ IP \ Internet Link	`ip40`
Ethernet II \ IP \ IPComp	`ip108`
Ethernet II \ IP \ IPCV	`ip71`
Ethernet II \ IP \ IPIP	`ip94`
Ethernet II \ IP \ IPLT	`ip129`
Ethernet II \ IP \ IPPC	`ip67`

Ethernet II \ IP \ IPv4 Encapsulated	`ip4`
Ethernet II \ IP \ IPv6 Encapsulated	`IPv6encapsulated`
Ethernet II \ IP \ IPX-in-IP	`ip111`
Ethernet II \ IP \ IRTP	`ip28`
Ethernet II \ IP \ IS-IS over IPv4	`IsIsOverIp`
Ethernet II \ IP \ ISO-IP	`ip80`
Ethernet II \ IP \ ISO-TP4	`ip29`
Ethernet II \ IP \ Kryptolan	`ip65`
Ethernet II \ IP \ L2TP	`ip115`
Ethernet II \ IP \ LARP	`ip91`
Ethernet II \ IP \ MANET	`ip138`
Ethernet II \ IP \ MERIT-INP	`ip32`
Ethernet II \ IP \ MFE-NSP	`ip31`
Ethernet II \ IP \ MICP	`ip95`
Ethernet II \ IP \ MOBILE	`ip55`
Ethernet II \ IP \ MPLS-in-IP	`ip137`
Ethernet II \ IP \ MTP	`ip92`
Ethernet II \ IP \ MUX	`ip18`
Ethernet II \ IP \ NARP	`ip54`
Ethernet II \ IP \ NETBLT	`ip30`
Ethernet II \ IP \ NSFNET-IGP	`ip85`
Ethernet II \ IP \ NVP-II	`ip11`
Ethernet II \ IP \ 开放最短路径优先 (OSPF)	`Ospf`
Ethernet II / IP / 性能透明协议	`ip123`
Ethernet II \ IP \ PGM	`ip113`
Ethernet II \ IP \ PIM	`PIM`
Ethernet II \ IP \ PIPE	`ip131`
Ethernet II \ IP \ PNNI	`ip102`
Ethernet II \ IP \ PRM	`ip21`
Ethernet II \ IP \ PUP	`ip12`
Ethernet II \ IP \ PVP	`ip75`
Ethernet II \ IP \ QNX	`ip106`
Ethernet II / IP / 可靠数据协议	`RDP`
Ethernet II \ IP \ ROHC	`ip142`
Ethernet II \ IP \ RSVP	`ip46`
Ethernet II \ IP \ RSVP-E2E-IGNORE	`ip134`
Ethernet II \ IP \ RVD	`ip66`
Ethernet II \ IP \ SAT-EXPAK	`ip64`
Ethernet II \ IP \ SAT-MON	`ip69`
Ethernet II \ IP \ SCC-SP	`ip96`
Ethernet II \ IP \ SCPS	`ip105`

Ethernet II \ IP \ SCTP	`SCTP`
Ethernet II \ IP \ SDRP	`ip42`
Ethernet II \ IP \ SECURE-VMTP	`ip82`
Ethernet II \ IP \ SMP	`ip121`
Ethernet II \ IP \ SNP	`ip109`
Ethernet II \ IP \ Sprite-RPC	`ip90`
Ethernet II \ IP \ SPS	`ip130`
Ethernet II \ IP \ SRP	`ip119`
Ethernet II \ IP \ SSCOPMCE	`ip128`
Ethernet II \ IP \ STP	`STP`
Ethernet II \ IP \ SUN-ND	`ip77`
Ethernet II \ IP \ TCF	`ip87`
Ethernet II \ IP \ TCP	`Tcp`
Ethernet II \ IP \ TCP \ ABB SPA-Bus	`ABB_SpaBus`
Ethernet II \ IP \ TCP \ AeroAdmin over TCP	`AeroAdmin`
Ethernet II \ IP \ TCP \ AFP	`SrvTcp_AFP`
Ethernet II \ IP \ TCP \ Allen-Bradley EtherNet/IP	`AB_EtherNet_IP`
Ethernet II \ IP \ TCP \ Ammyy Admin over TCP	`AmmyyAdmin`
Ethernet II \ IP \ TCP \ AnyDesk over TCP	`AnyDesk`
Ethernet II \ IP \ TCP \ ARMS 控制协议	`AsrkScada`
Ethernet II \ IP \ TCP \ BECKHOFF ADS/AMS	`Beckhoff`
Ethernet II \ IP \ TCP \ Bitcoin over TCP	`Bitcoin_OverTcp`
Ethernet II \ IP \ TCP \ BitTorrent over TCP	`BittorrentOverTCP`
Ethernet II \ IP \ TCP \ CIMPLICITY-Historian over TCP	`CIMPLICITYHistorian`
Ethernet II \ IP \ TCP \ CIMPLICITY-HMI/SCADA over TCP	`CIMPLICITYNetwork_OverTcp`
Ethernet II \ IP \ TCP \ CODESYS V2	`CodesysV2`
Ethernet II \ IP \ TCP \ CODESYS V3 Gateway	`CodesysGatewayV3Tcp`
Ethernet II \ IP \ TCP \ COS	`Cos`
Ethernet II \ IP \ TCP \ Dameware® MRC	`SrvTcp_DameWare_Mini_Remote_Control`
Ethernet II \ IP \ TCP \ DCE/RPC	`GenericDceRpc`
Ethernet II \ IP \ TCP \ DICOM® over TCP	`DICOM_over_TCP`
Ethernet II \ IP \ TCP \ DLMS/COSEM	`DlmsCosem`
Ethernet II \ IP \ TCP \ DMS for ABB AC 700F	`ABB_AC700F_DMS`
Ethernet II \ IP \ TCP \ DNP3	`Dnp3`
Ethernet II \ IP \ TCP \ DNS	`SrvTcp_DNS`
Ethernet II \ IP \ TCP \ DNS/LLMNR over TCP	`DnsLlmnr_OverTcp`
Ethernet II \ IP \ TCP \ Dogecoin over TCP	`Dogecoin`
Ethernet II \ IP \ TCP \ Emerson ControlWave Designer	`EmersonControlWaveDesigner`
Ethernet II \ IP \ TCP \ Emerson DeltaV - 固件更新	`EmersonDeltaVFirmware`
Ethernet II \ IP \ TCP \ EtherNet/IP \ OMRON FINS	`OmronFinsEthernetIp`
Ethernet II \ IP \ TCP \ Ether-S-IO over TCP	`Esio_OverTcp`

Ethernet II \ IP \ TCP \ Finger	`SrvTcp_FINGER_PROTOCOL`
Ethernet II \ IP \ TCP \ 闪存媒体服务器	`SrvTcp_Flash_Media_Server`
Ethernet II \ IP \ TCP \ FTP	`Ftp`
Ethernet II \ IP \ TCP \ FTP Data	`SrvTcp_FTP_DATA`
Ethernet II \ IP \ TCP \ General Electric SRTP	`Srtp`
Ethernet II \ IP \ TCP \ HL7® v2 over TCP	`HL7_ver2_over_TCP`
Ethernet II \ IP \ TCP \ HL7 v3 over TCP	`HL7_ver3_over_TCP`
Ethernet II \ IP \ TCP \ Honeywell ControlEDGE 900：设备交互	`HoneywellControlEdge`
Ethernet II \ IP \ TCP \ Honeywell Experion CDA	`HoneywellExperionCdaComm`
Ethernet II \ IP \ TCP \ Honeywell Experion EpicMo	`HoneywellExperionEpicMo`
Ethernet II \ IP \ TCP \ HTTP	`SrvTcp_HTTP`
Ethernet II \ IP \ TCP \ HTTP/2	`HTTP2`
Ethernet II \ IP \ TCP \ HTTPS	`SrvTcp_HTTPS`
Ethernet II \ IP \ TCP \ IBM® DB2®	`SrvTcp_IBM_DB2`
Ethernet II \ IP \ TCP \ Ident	`SrvTcp_Ident`
Ethernet II \ IP \ TCP \ IEC 60870-5-101	`IEC_60870_5_101`
Ethernet II \ IP \ TCP \ IEC 60870-5-104	`IEC_60870_5_104`
Ethernet II \ IP \ TCP \ IMAP	`SrvTcp_IMAP`
Ethernet II \ IP \ TCP \ IPU-FEU：设备交互	`Feu`
Ethernet II \ IP \ TCP \ IRC	`Irc`
Ethernet II \ IP \ TCP \ ISaGRAF IXL	`IsagrafIxl`
Ethernet II \ IP \ TCP \ ISaGRAF SNCP	`IsagrafSncp`
Ethernet II \ IP \ TCP \ ISO TSAP	`SrvTcp_Iso8072`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ IEC 61850: MMS	`IEC61850_MMS`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ MMS for ABB AC 800M	`ABB_AC800M_MMS`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ Siemens S7comm	`SiemensS7Comm`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ Siemens S7comm-plus	`SiemensS7CommPlus`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ TASE.2	`Tase2`
Ethernet II \ IP \ TCP \ Jabber® XMPP® over TCP	`Jabber`
Ethernet II \ IP \ TCP \ Kerberos over TCP	`SrvTcp_Kerberos`
Ethernet II \ IP \ TCP \ LDAP(S) over TCP	`SrvTcp_LDAP_S_`
Ethernet II \ IP \ TCP \ Litecoin over TCP	`Litecoin`
Ethernet II \ IP \ TCP \ Mitsubishi MELSEC System Q	`MitsubishiMelsecSystemQProtocol`
Ethernet II \ IP \ TCP \ MMS (ISO 9506-2)	`MmsBase`
Ethernet II \ IP \ TCP \ Modbus	`ModbusTCP`
Ethernet II \ IP \ TCP \ Modbus TCP for EKRA 200 series	`Ekra243Modbus`
Ethernet II \ IP \ TCP \ Moxa NPort：设备配置	`MoxaNportFirmware`
Ethernet II \ IP \ TCP \ Moxa NPort：设备交互	`MoxaNportIa5000aSystem`
Ethernet II \ IP \ TCP \ MQTT over TCP	`MQTT`
Ethernet II \ IP \ TCP \ MSNP	`SrvTcp_MSNP`
Ethernet II \ IP \ TCP \ MS SQL Server®	`SrvTcp_MS_SQL_Server`

Ethernet II \ IP \ TCP \ MySQL	`SrvTcp_MySQL`
Ethernet II \ IP \ TCP \ Napster	`SrvTcp_Napster`
Ethernet II \ IP \ TCP \ NetBIOS	`SrvTcp_NetBIOS`
Ethernet II \ IP \ TCP \ NFS	`SrvTcp_NFS`
Ethernet II \ IP \ TCP \ OMRON FINS	`OmronFinsTcp`
Ethernet II \ IP \ TCP \ ONVIF® over TCP	`ONVIF_over_TCP`
Ethernet II \ IP \ TCP \ OPC DA	`OpcDa`
Ethernet II \ IP \ TCP \ OPC UA Binary	`OpcUaBinary`
Ethernet II \ IP \ TCP \ Oracle DB	`SrvTcp_Oracle`
Ethernet II \ IP \ TCP \ POP3	`SrvTcp_POP3`
Ethernet II \ IP \ TCP \ PPTP	`SrvTcp_PPTP`
Ethernet II \ IP \ TCP \ Radmin 基于 TCP 的应用协议	`Radmin_OverTcp`
Ethernet II \ IP \ TCP \ RDP	`SrvTcp_RDP`
Ethernet II \ IP \ TCP \ Relematika BDUBus	`BDUBus`
Ethernet II \ IP \ TCP \ Remote Utilities® over TCP	`RemoteUtilities`
Ethernet II \ IP \ TCP \ Rlogin	`SrvTcp_RLOGIN`
Ethernet II \ IP \ TCP \ RSH	`SrvTcp_RSH`
Ethernet II \ IP \ TCP \ RTSP over TCP	`RTSP_over_TCP`
Ethernet II \ IP \ TCP \ SAIA S-Bus over TCP	`Saia_OverTcp`
Ethernet II \ IP \ TCP \ Schneider Electric UMAS	`Umas`
Ethernet II \ IP \ TCP \ SFTP	`SrvTcp_SFTP`
Ethernet II \ IP \ TCP \ Siemens SICAM SCC：与 SICAM PAS 的交互	`NwChannel`
Ethernet II \ IP \ TCP \ SMB	`SrvTcp_SMB`
Ethernet II \ IP \ TCP \ SMB v2 over TCP	`Smb2_OverTcp`
Ethernet II \ IP \ TCP \ SMB v3 over TCP	`Smb3_OverTcp`
Ethernet II \ IP \ TCP \ SMTP	`SrvTcp_SMTP`
Ethernet II \ IP \ TCP \ SNMP	`SrvTcp_SNMP`
Ethernet II \ IP \ TCP \ SSH	`Ssh`
Ethernet II \ IP \ TCP \ SSL/TLS	`SslTls`
Ethernet II \ IP \ TCP \ SSL v2	`SslV2`
Ethernet II \ IP \ TCP \ SSL v3	`SslV3`
Ethernet II \ IP \ TCP \ SuiteLink over TCP	`SuiteLink`
Ethernet II \ IP \ TCP \ Syslog	`SrvTcp_Syslog`
Ethernet II \ IP \ TCP \ TeamViewer	`SrvTcp_TeamViewer`
Ethernet II \ IP \ TCP \ Telegram MTProto over TCP	`Telegram`
Ethernet II \ IP \ TCP \ Telnet	`Telnet`
Ethernet II \ IP \ TCP \ TFTP over TCP	`Tftp_OverTcp`
Ethernet II \ IP \ TCP \ TLS v1.0	`TlsV10`
Ethernet II \ IP \ TCP \ TLS v1.1	`TlsV11`
Ethernet II \ IP \ TCP \ TLS v1.2	`TlsV12`
Ethernet II \ IP \ TCP \ TLS v1.3	`TlsV13`

Ethernet II \ IP \ TCP \ TNS over TCP	`Tns_OverTcp`
Ethernet II \ IP \ TCP \ Tor® over TCP	`Tor_OverTcp`
Ethernet II \ IP \ TCP \ VNC	`SrvTcp_VNC`
Ethernet II \ IP \ TCP \ WebSocket	`WebSocket_OverTcp`
Ethernet II / IP / TCP / WMI 技术：设备交互	`Wmi`
Ethernet II \ IP \ TLSP	`ip56`
Ethernet II \ IP \ TP++	`ip39`
Ethernet II \ IP \ UDP	`UDP`
Ethernet II \ IP \ UDP \ BACnet	`Bacnet`
Ethernet II \ IP \ UDP \ BECKHOFF ADS/AMS	`BeckhoffUdp`
Ethernet II \ IP \ UDP \ BitTorrent over UDP	`BittorrentOverUdp`
Ethernet II \ IP \ UDP \ BSAP	`Bsap`
Ethernet II \ IP \ UDP \ CHINT MAS400：设备交互	`ChintMas400`
Ethernet II \ IP \ UDP \ CHINT MAS9600：设备交互	`ChintMas9600`
Ethernet II \ IP \ UDP \ CIMPLICITY-HMI/SCADA over UDP	`CIMPLICITYNetwork_OverUdp`
Ethernet II \ IP \ UDP \ CODESYS V3 Gateway	`CodesysGatewayV3Udp`
Ethernet II \ IP \ UDP \ 数据传输系统 (DTS)	`Dts`
Ethernet II \ IP \ UDP \ DHCP	`Dhcp`
Ethernet II \ IP \ UDP \ DirectLOGIC：设备交互	`DirectLogicEcom`
Ethernet II \ IP \ UDP \ DNS	`SrvUdp_DNS`
Ethernet II \ IP \ UDP \ DNS/LLMNR over UDP	`DnsLlmnr_OverUdp`
Ethernet II \ IP \ UDP \ Dropbox LAN Sync over UDP	`Dropbox_sync_OverUdp`
Ethernet II \ IP \ UDP \ Emerson DeltaV	`EmersonDeltaV`
Ethernet II \ IP \ UDP \ Emerson Ovation：基于 UDP 的多播	`Emerson_Ovation_OverUdp_Mcast`
Ethernet II \ IP \ UDP \ Emerson Ovation：基于 UDP 的交互	`Emerson_Ovation_OverUdp`
Ethernet II \ IP \ UDP \ Ether-S-IO over UDP	`Esio_OverUdp`
Ethernet II \ IP \ UDP \ General Electric EGD	`Egd`
Ethernet II \ IP \ UDP \ GLBP over UDP	`GLBP_OverUdp`
Ethernet II \ IP \ UDP \ Honeywell ControlEDGE 900：设备检测	`HoneywellControlEdgeDiscovery`
Ethernet II \ IP \ UDP \ Honeywell Experion：设备检测	`HoneywellExperionDiscovery`
Ethernet II \ IP \ UDP \ Honeywell Experion：获取设备网络配置	`HoneywellExperionNameServer`
Ethernet II \ IP \ UDP \ HSRP over UDP	`HSRP_OverUdp`
Ethernet II \ IP \ UDP \ INA2000	`Ina2000`
Ethernet II \ IP \ UDP \ Kerberos over UDP	`SrvUdp_Kerberos`
Ethernet II \ IP \ UDP \ KNXnet/IP	`Knx`
Ethernet II \ IP \ UDP \ LDAP(S) over UDP	`SrvUdp_LDAP_S_`
Ethernet II \ IP \ UDP \ LDP	`SrvUdp_LDP`
Ethernet II \ IP \ UDP \ mDNS over UDP	`mDNS_OverUdp`
Ethernet II \ IP \ UDP \ MikroTik Neighbor Discovery Protocol (MNDP)	`Mndp`
Ethernet II \ IP \ UDP \ Moxa NPort：设备检测	`MoxaNportDiscovery`
Ethernet II \ IP \ UDP \ MSNP	`SrvUdp_MSNP`

Ethernet II \ IP \ UDP \ 基于 UDP 的 NBNS	`NBNS_OverUdp`
Ethernet II \ IP \ UDP \ NetBIOS	`SrvUdp_NetBIOS`
Ethernet II \ IP \ UDP \ NFS	`SrvUdp_NFS`
Ethernet II \ IP \ UDP \ NTP	`SrvUdp_NTP`
Ethernet II \ IP \ UDP \ OMRON FINS	`OmronFins`
Ethernet II \ IP \ UDP \ PK4	`Pk4`
Ethernet II \ IP \ UDP \ PNU20	`Pnu20`
Ethernet II \ IP \ UDP \ QTP	`SrvUdp_QTP`
Ethernet II \ IP \ UDP \ RADIUS over UDP	`RadiusUdp`
Ethernet II \ IP \ UDP \ RDP	`SrvUdp_RDP`
Ethernet II \ IP \ UDP \ RIP	`RIP`
Ethernet II \ IP \ UDP \ SAIA S-Bus over UDP	`Saia_OverUdp`
Ethernet II \ IP \ UDP \ SCIYON 默认通过 UDP 传输	`Sciyon`
Ethernet II \ IP \ UDP \ Siemens DIGSI 4	`SiemensDigsi4`
Ethernet II \ IP \ UDP \ SIP over UDP	`Sip`
Ethernet II \ IP \ UDP \ SMB over UDP	`Smb_OverUDP`
Ethernet II \ IP \ UDP \ SMB v2 over UDP	`Smb2_OverUdp`
Ethernet II \ IP \ UDP \ SMB v3 over UDP	`Smb3_OverUdp`
Ethernet II \ IP \ UDP \ SNMP	`SrvUdp_SNMP`
Ethernet II \ IP \ UDP \ SNMP v1 over UDP	`Snmpv1_OverUdp`
Ethernet II \ IP \ UDP \ SNMP v2 over UDP	`Snmpv2_OverUdp`
Ethernet II \ IP \ UDP \ SNMP v3 over UDP	`Snmpv3_OverUdp`
Ethernet II \ IP \ UDP \ SSDP	`SrvUdp_SSDP`
Ethernet II \ IP \ UDP \ Syslog over UDP	`Syslog_OverUdp`
Ethernet II \ IP \ UDP \ TeamViewer	`SrvUdp_TeamViewer`
Ethernet II \ IP \ UDP \ TFTP over UDP	`Tftp_OverUdp`
Ethernet II \ IP \ UDP \ TNS over UDP	`Tns_OverUdp`
Ethernet II \ IP \ UDP \ Tor over UDP	`Tor_OverUdp`
Ethernet II \ IP \ UDP \ Valmet DNA：设备交互	`Valmet`
Ethernet II \ IP \ UDP \ YARD	`Yard`
Ethernet II \ IP \ UDP \ Yokogawa Vnet/IP	`VnetIP`
Ethernet II \ IP \ UDPLite	`ip136`
Ethernet II \ IP \ UTI	`ip120`
Ethernet II \ IP \ VINES	`ip83`
Ethernet II \ IP \ VISA	`ip70`
Ethernet II \ IP \ VMTP	`ip81`
Ethernet II \ IP \ VRRP	`ip112`
Ethernet II \ IP \ VRRP over IPv4	`VRRP_OverIpv4`
Ethernet II \ IP \ WB-EXPAK	`ip79`
Ethernet II \ IP \ WB-MON	`ip78`
Ethernet II \ IP \ WESP	`ip141`

Ethernet II \ IP \ WSN	`ip74`
Ethernet II \ IP \ XNET	`ip15`
Ethernet II \ IP \ XNS-IDP	`ip22`
Ethernet II \ IP \ XTP	`ip36`
Ethernet II \ IPv6	`IPv6`
Ethernet II \ IPX	`IPX`
Ethernet II \ IS-IS over Ethernet II	`IsIsOverEthernetII`
Ethernet II \ Link Layer Discovery Protocol (LLDP)	`Lldp`
Ethernet II \ Loopback	`Loopback`
Ethernet II \ MiCOM C264	`MicomC264`
Ethernet II \ MPLS	`MPLS`
Ethernet II \ MPLS 组播	`MPLS_multi`
Ethernet II \ 精确时间协议	`PTP`
Ethernet II \ PROFINET IO	`ProfinetIo`
Ethernet II \ Prosoft-Systems：设备初始安装	`ProsoftSystemsDeviceDiscovery`
Ethernet II \ PRP	`PRP`
Ethernet II \ RARP	`RARP`
Ethernet II \ RPC for PROFINET IO	`ProfinetRpc`

使用变量

您可以将以下类型的变量添加到 SQL 查询文本中：

- `string`：文本字符串
- `date`：YYYY-MM-DD 格式的日期
- `time`：hh:mm 格式的时间
- `weekday`：星期几的数字（1-7：1为星期一）
- `ip`：格式为 XXX.XXX.XXX.XXX 的 IPv4 地址
- `port`：端口号（0–65535）
- `int`：64 位整数

要指定变量及其类型，请使用`{{param_name:param_type}}`格式的条目。如果未指定变量类型（在格式为`{{param_name}}`的条目中），默认情况下使用字符串类型。添加的变量显示在**使用的变量**设置块中 SQL 查询文本的下方。在这个模块中，您可以定义变量的值，或者选择包含该变量值的字典。

在向 SQL 查询中添加变量时，请记住 SQL 查询中变量的最大数量为 30。

查看网络异常检测规则表：

网络异常检测规则表显示在**检测规则**的**网络异常检测**选项卡中。

具有管理员、安全专业人员或操作员角色的用户可以查看网络异常检测规则表。

在**网络异常检测**选项卡上，工具栏下方会显示**流量接收延迟**计数器。该计数器包含数据库接收到的传入流量数据的动态变化延迟时间，该数据库用于存储协议属性。如果应用程序检测到严重延迟时间，计数器旁边的绿色图标将不再显示。在这种情况下，自动运行在此期间发生的规则可能会导致错误结果。在将计数器恢复到正常状态之前，建议手动运行规则，同时考虑可用于分析协议属性的范围。

规则的设置显示在表格的以下列中：

- **规则 ID**
  Kaspersky Industrial CyberSecurity for Networks 分配的规则 ID。
- **名称**
  规则的定义名称。
- **状态**
  规则的当前状态（*已启用*或*已禁用*）。
- **创建日期**
  规则创建的日期和时间。
- **更改时间**
  规则最后修改的日期和时间。
- **模板名称**
  与规则关联的模板名称。如果规则未与内置模板关联，则为该规则指定**用户自定义**模板。
- **搜索深度**。
  在协议属性中搜索网络异常的时间间隔持续时间。
- **描述**
  规则描述。
- **计划**
  有关应用程序自动启动规则的计划的信息。
- **上次运行**
  规则上次开始的日期和时间。
- **上次运行状态**
  规则上次运行时的结果状态。
- **事件数量**。
  规则运行时记录的事件数量。

- **事件标题**

  触发规则时注册的事件的标题。

- **事件分数**

  触发规则时注册的事件的评估分数。事件的评分范围为 0.0 到 10.0。

- **事件描述**。

  规则触发时注册的事件的描述。

查看网络异常检测规则表时，您可以使用配置、过滤和排序功能。

启用和禁用网络异常检测规则

要启用或禁用网络异常检测规则，您可以更改其状态。每条规则都可以被赋予*已启用*或*已禁用*状态。默认情况下，规则创建后，其状态会被设置为*已启用*。

如果将*已禁用*状态分配给某个规则，应用程序将取消该规则的最后一次运行，并将**已取消**状态分配给本次运行。如果规则被禁用时，最后一次运行的状态为**新的**、**等待数据**、**等待发送**或**正在运行**，则该规则的最后一次运行将被取消。

更改网络异常检测规则的状态：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**检测规则**。
3. 在**网络异常检测**选项卡上，选择要更改状态的规则。
4. 打开工具栏中的**更改状态**下拉列表。
5. 在下拉列表中，选择命令来分配所需的状态。

手动启动和停止网络异常检测规则

您可以手动启动和停止网络异常检测规则。只有已启用的规则才能停止或启动。

如果规则处于**新的**、**等待发送**、**等待数据**或**正在运行**状态，则无法运行。

若要触发网络异常检测规则：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**检测规则**。
3. 在**网络异常检测**选项卡上，选择要触发的规则。

   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**间歇运行**。如果无法生成规则，则该按钮将被禁用。

   配置规则运行栏显示在右侧。面板的上半部分显示有关可用于分析协议属性的范围的信息。范围仅限于用于存储协议属性的数据库中最早和最晚到达的流量数据。

5. 使用**搜索深度**参数来指定在协议属性中搜索网络异常的时间间隔的持续时间。要手动运行规则，此值可能与创建规则时或更改设置时定义的值不同。

6. 在**间隔结束**字段中，指定时间间隔结束的日期和时间。

7. 单击**运行**。

如果规则处于以下状态之一，则可以停止规则：**新的**、**等待发送**、**等待数据**或**正在运行**。

要停止执行网络异常检测规则：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 选择**检测规则**。

3. 在“**网络异常检测**”选项卡上，选择要停止的规则。
   详细信息区域显示在 Web 界面窗口的右侧部分。

4. 单击**停止**（如果此时无法停止规则，则此按钮将被禁用）。

查看有关网络异常检测规则触发器的常规信息

在查看规则表时，您可以查看网络异常检测规则触发方式的概述。该表格显示有关最近规则运行的信息。

具有管理员、安全专业人员或操作员角色的用户可以查看有关网络异常检测规则触发器的常规信息。

您可以在详细信息区域的**规则运行**设置块中查看有关规则运行的常规信息。有关运行网络异常检测规则的常规信息包括以下内容：

- 规则上次开始的日期和时间。
- 下次规则运行的日期和时间。
- 上次规则运行状态
  可使用以下状态：
  - **从不运行**：已创建一条新规则，但尚未为此规则创建任何运行。
  - **新的**：已创建规则的新运行，但尚未基于此规则执行协议属性分析。
  - **等待数据**：Kaspersky Industrial CyberSecurity for Networks 正在等待流量数据到达用于存储协议属性的数据库（在用于搜索网络异常的已定义时间间隔结束时，所有数据尚未到达）。
  - **等待发送**：规则已进入运行队列。
  - **没有数据**：根据规则，在用于搜索网络异常的时间间隔内没有流量数据。
  - **正在运行**：规则正在运行。
  - **已取消**：规则已停止。
  - **已完成**：规则已成功完成。

- **错误**：运行规则时发生错误。
- **部分成功**：规则运行结果部分成功：在指定的时间间隔内未收到完整的流量数据。

- 规则运行的次数。
- 规则上次运行时 SQL 查询的执行持续时间。
- 规则上次运行时，搜索网络异常的时间间隔。
- 规则上次运行时记录的事件数。

删除网络异常检测规则

您可以删除网络异常检测规则。但是，您不能删除上次运行状态为**新的**、**等待发送**、**等待数据**或**正在运行**的规则。

删除网络异常检测规则的状态：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**检测规则**。
3. 在“**网络异常检测**”选项卡上，选择要删除的规则。
4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，确认删除规则。
   在选定的规则中，您只可以删除上次运行状态不是**新的**、**等待发送**、**等待数据**和**正在运行**的规则。如果所选规则中包含状态为**新的**、**等待发送**、**等待数据**或**正在运行**的规则，屏幕上将显示相关消息。要删除此类规则，请首先停止这些规则。

管理网络异常检测规则字典

Kaspersky Industrial CyberSecurity for Networks 实现了网络异常检测规则字典值的存储。您可以在规则中使用存储的字典值作为 SQL 查询中变量的值。*字典*用于存储字典值。

应用程序提供各种类型的字典。不同类型的字典用于存储 IP 地址、端口号、日期和其他数据。根据 SQL 查询中变量的类型，您可以在创建或更改网络异常检测规则的设置时选择相应类型的字典。

您可以在“**设置**”→“**词典**”部分管理字典。您最多可以向应用程序添加 1000 个字典。向每个字典添加的项目不能超过 500 个。

具有管理员或安全官角色的用户可以管理字典。

添加字典

您可以添加字典，并将其中保存的元素用作 SQL 查询中网络异常检测规则的变量值。

要添加字典：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **词典**。
3. 单击“**添加词典**”打开详细信息。
4. 输入字典名称和说明。
5. 选择字典类型并定义其项目。
   您可以选择以下类型的字典：
   - **日期**，用于存储日期。对应于 SQL 查询中的“date”数据类型。
   - **IP 地址**，用于存储 IP 地址。对应于 SQL 查询中的“ip”数据类型。
   - **端口**，用于存储端口号。对应于 SQL 查询中的“port”数据类型。
   - **文本**，用于存储字符串值。对应于 SQL 查询中的“string”数据类型。
   - **时间**，用于存储时间范围。对应于 SQL 查询中的“time”数据类型。
   - **周中的天**，用于存储星期几。对应于 SQL 查询中的“weekday”数据类型。
6. 单击“**保存**”。

查看字典表

网络异常检测规则字典表显示在应用程序 Web 界面的**设置** → **词典**部分中。

具有管理员、安全专业人员或操作员角色的用户可以查看字典表。

有关字典的信息显示在表的以下列中：

- **词典 ID**。
  由 Kaspersky Industrial CyberSecurity for Networks 分配的字典 ID。
- **名称**
  用于在应用程序中代表字典的名称。
- **类型**
  字典类型。

- **项目数量**。
  字典中的项目数量。
- **创建日期**
  将字典添加到应用程序的日期和时间。
- **更改时间**
  应用程序中上次修改字典的日期和时间。
- **描述**
  字典描述。

查看字典表时，您可以使用配置、过滤和排序功能。

编辑字典设置

更改字典的设置时，您可以更改其名称、描述和/或条目的值。

如果字典已经在网络异常检测规则中使用，则字典元素的新值仅在下次运行该规则时才会应用。

更改字典设置：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **词典**。
3. 选择您要更改的字典。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**编辑**。
5. 根据需要更改设置。有关设置的说明，请参阅添加字典的说明。

删除字典

您可以删除网络异常检测规则中未使用的字典。

要删除字典：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **词典**。
3. 选择您要删除的字典。
   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，确认删除字典。

管理日志

本节包含有关 Kaspersky Industrial CyberSecurity for Networks 管理日志的信息。

只有具有管理员角色的用户才能管理 Kaspersky Industrial CyberSecurity for Networks 的日志。

管理在服务器数据库中存储日志的设置

您可以更改在服务器数据库中存储日志条目的设置。

要更改服务器数据库中存储日志的设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**部署**”。
3. 选择服务器图块。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**编辑**。
   详细信息区域将显示用于配置服务器参数的选项卡。
5. 在**常规**选项卡上，在**事件**、**审计条目**和**应用程序消息**部分配置以下设置：
   a. 使用**最大量**设置来定义存储记录的大小限制。您可以选择值的计量单位：**MB**或**GB**。
      更改此设置的值时，请注意指定空间量的预计最大条目数。您还需要记住所有卷限制的总和不能超过节点定义的最大存储容量。
   b. 如有必要，请使用“**储存时间(天)**”设置启用条目的最短存储时间，并指定存储他们的最短天数。
6. 单击**保存**。

管理在服务器数据库中保存流量的设置

应用程序可以保存事件注册时收到的流量。当注册流量保存已启用的事件时，流量将被保存在服务器数据库中。应用程序还可以通过请求使用临时流量转储文件加载流量，直接将流量保存在服务器数据库中。

应用程序以块的形式保存流量数据。如果一个流量块与多个事件相关（当事件在短时间间隔内注册时），则该流量块不会在数据库中重复。

要更改在服务器数据库中保存流量的设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**部署**”。
3. 选择服务器图块。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**编辑**。
   详细信息区域将显示用于配置服务器参数的选项卡。
5. 在“**常规**”选项卡上，转到“**事件流量**”并使用“**最大量**”设置来定义存储流量的大小限制。
   您可以选择空间限制的计量单位：**MB** 或 **GB**。
   更改此设置的值时，需要记住所有卷限制的总和不能超过节点定义的最大存储卷。
6. 单击**保存**。

管理保存流量转储文件的设置

应用程序将通过监控点接收到的流量保存为流量转储文件。应用程序使用这些文件来分析传入流量。您还可以使用这些文件在应用程序中执行以下操作：

- 下载节点监控点收到的流量
- 使用网络交互图时下载流量
- 下载网络会话流量
- 下载事件流量（流量转储文件允许您下载事件流量，即使相应事件类型禁用了流量保存）

流量转储文件存储在安装应用程序组件的节点上的存储中。在每个节点上，节点的内部存储（在节点上安装应用程序组件时自动创建）和外部存储（如果连接在节点上）都可以使用。

应用程序临时存储流量转储文件。当流量到达时，如果文件总量接近为存储设置的限制，则应用程序会自动从存储中删除最旧的流量转储文件。

对于每个节点，您可以配置将流量保存到内部存储的设置。您还可以连接节点的外部存储，并配置将流量保存到外部存储的设置。

要配置将流量转储文件保存到节点内部存储的设置，请执行以下操作：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置 → 部署**。
3. 选择相关节点的图块。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
   详细信息区域将显示用于配置节点参数的选项卡。

5. 如有必要，在“**常规**”选项卡上的“**过滤存储的流量**”部分中，启用过滤并根据网络数据包的地址设置使用 Berkeley Packet Filter (BPF) 技术输入过滤表达式。

   过滤通过跳过与过滤器不匹配的网络数据包来减少存储的流量。然而，在使用过滤时，请记住，应用程序可能无法在过滤后的流量中接收到高质量流量分析所需的所有数据。配置过滤，以便根据应用程序功能进行流量分析所需的所有网络数据包都保存在流量转储文件中。

6. 转到“**流量转储文件**”设置组，并使用“**最大量**”设置来定义存储流量转储文件的大小限制。

   您可以选择空间限制的计量单位：**MB** 或 **GB**。

   更改此设置的值时，需要记住传入流量的数量和速率以及所有空间限制的总和不能超过为节点定义的最大存储限制。

7. 单击**保存**。

启用和禁用用户活动审计

您可以启用和禁用应用程序用户活动审计。

用户活动审计默认已启用。

要启用或禁用用户活动审计：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **审计**。
3. 使用工具栏中的“**审计**”切换按钮来启用或禁用用户活动审计。
4. 等待更改得到应用。切换开关在完成切换到其他状态之前不可用。

更改进程的日志记录级别

如果节点上安装了应用组件，则这些节点会有正在运行的进程，这些进程可能会将其操作数据保存日志中。下表描述了您要管理其操作数据日志存储的应用程序进程。

已记录日志的应用程序进程

Process	服务器计算机	Sensor 计算机	描述	日志存储目录
EntityManager	✓	✓	控制应用程序其他主要进程启动的进程	/var/log/kaspersky/kics4net/traces/EntityManager
过滤器	✓	✓	执行基本流量分析并接收来自 EPP 应用程序的遥测数据的进程	/var/log/kaspersky/kics4net/traces/Filter
KisClient	✓	—	下载更新的进程	/var/log/kaspersky/kics4net/traces/KisClient
NetworkDumper	✓	✓	捕获、过滤流量并将其保存到磁盘的进程	/var/log/kaspersky/kics4net/traces/NetworkDumper

Process	服务器计算机	Sensor 计算机	描述	日志存储目录
ProductServer	✓	—	所有 Kaspersky Industrial CyberSecurity for Networks 的节点都连接到的服务器。该进程提供以下功能： • 接收来自 Sensor 的数据。 • 维护资产列表。 • 提供对 Web 服务器的访问权限。 • 写入数据库。 • 对从过滤器进程接收的数据执行详细分析。	/var/log/kaspersky/kics4net/traces/ProductServer
Watchdog	✓	✓	用于监控主应用程序进程的状态的进程，并提供对系统计数器和操作系统统计信息的访问。	/var/log/kaspersky/kics4net/traces/Watchdog
WebServer	✓	—	Kaspersky Industrial CyberSecurity for Networks Web 界面	/var/log/kaspersky/kics4net-webserver/traces

对于每一个进程，可以分配以下日志级别之一：

- **关闭**。进程数据未保存在日志中。此级别可用于在紧急情况下禁用日志记录，例如，当由于错误或环境相关情况导致大量条目保存到日志中时。

- **错误**。日志仅存储由严重违规（通常会导致数据丢失）引起的进程操作错误数据。有时，**错误**级别的条目表示某些应用程序模块无法运行。通常，此级别的日志条目会以应用程序消息的形式向用户发出警告。此级别可用于临时从另一个日志记录级别切换，例如，如果日志条目生成的强度阻止了对应用程序问题的检测。

  示例

  ```
  ERR [PDS] [PWS] ReadDbRuleFromCursor Custom value is empty for db protocol stack id: 227408
  ```

  此示例显示了协议词典中某个协议的问题条目。该条目被分配了**错误**级别，因为该问题影响所有使用指定协议的会话。

- **警告**（默认）。日志存储"**错误**级别的数据以及不影响应用程序性能的轻微内部违规数据。有时，此级别的条目包含信息性消息，例如，可用于跟踪应用程序加载过程。

  示例

  ```
  WRN [AMS] [AssetDiscovery] Ignore rule "TELNET Protocol" (id=200075).Wrong protocol stack table key.
  ```

  此示例显示了一条关于数千条检测规则之一的问题条目，该规则使用了错误的协议名称。该条目被分配了**警告**级别，因为该问题不影响协议的处理方式或 Kaspersky Industrial CyberSecurity for Networks 的整体功能。

- **信息**。日志存储**警告**级别的数据以及重要的调试消息，这些消息提供有关应用程序执行阶段的信息。当在**调试**级别生成过多日志条目时，可以使用此级别来调试应用程序。

  在此级别记录日志可能会对 Kaspersky Industrial CyberSecurity for Networks 的性能产生不利影响。

  示例

  ```
  INF [FILTER] [EKAIPC] Start: starting EkaIPCProvider...
  ```

  此示例显示了一条关于应用程序模块启动的信息性条目。

- **调试**。日志存储**信息**级别的数据以及调试应用程序时可能需要的所有进程操作数据（例如，有关解析每个网络会话数据包的步骤的信息）。此级别的条目包含有关应用程序运行的详细信息。此级别用于在技术支持专家要求下分析故障时使用。

在此级别记录日志会对硬盘造成很大的负载，并显著降低 Kaspersky Industrial CyberSecurity for Networks 的性能。
启用此日志记录级别可能会导致根据定义的条目存储空间限制快速删除先前的条目。在此级别下，只能在短时间内调查错误情况的原因。

示例

```
DBG [SPDKP] [SiemensS7Comm Parser/0x576b87f0a888] Cyclic response detected: pduSequence = 0, sequence = 2,
items size = 2
DBG [NP3] Session 800000103cdb87f0a88b87f0a88e9200: reports sys command id #2405 on gpid: 164e8e5dec10c5
DBG [SPDKP] [SiemensS7Comm Protocol/0x576bcabd3d58] Packet info: #127, 192.168.2.0:102 ==> 198.51.100.0:55671,
Plc ==> Scada [82], time: 1779892008648825
```

此示例显示了有关处理 S7comm 协议的调试条目。条目包含协议处理程序和会话的标识符、此会话的 IP 地址和端口、系统命令检测时间以及需要处理的流量范围指示。

例如，当联系技术支持时，可能需要更改日志记录级别。

只有具有管理员角色的用户才能更改日志记录级别。

对于其他不太重要的应用程序进程，会记录**警告**级别的条目。您无法更改此类过程的日志级别。这些进程的日志存储在相应本地目录的“traces”子目录中。例如，基于规则的网络异常检测服务的日志存储在 /var/log/kaspersky/kics4net-anomaly-hunter/traces 目录中。

要更改 Kaspersky Industrial CyberSecurity for Networks 进程的日志记录级别：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置** → **日志记录**。
3. 根据需要更改日志记录级别：
   - 要为所有节点上的所有进程定义相同的日志记录级别，请单击包含所需级别名称的列的标题。
   - 要为一个节点上的所有进程定义相同的日志记录级别，请单击包含节点名称的行中包含所需级别名称的列中的单元格。
   - 要为某个进程定义不同于其他进程定义的日志级别，请展开**节点和进程**列中相关节点的进程列表，然后单击包含进程名称的行中包含必要级别名称的列中的单元格。
4. 请等待更改应用（进度指示器会显示，直到更改完全得到应用）。

使用 EPP 应用程序配置操作

Kaspersky Industrial CyberSecurity for Networks 可以接收和处理来自卡巴斯基应用程序的数据，这些应用程序可以保护工作站和服务器。这些应用程序包含在端点保护平台 (EPP) 中，并安装到企业 IT 基础设施内的端点设备。

EPP 应用程序的数据传输由 *Endpoint Agent* 软件组件执行。根据所支持的 EPP 应用程序版本，以下软件可以执行端点代理功能：

- 嵌入到 EPP 应用程序中的软件模块。
- Kaspersky Endpoint Agent 应用程序。

为了在运行过时操作系统（例如 Windows 7）的设备上连接到 Kaspersky Endpoint Agent，Kaspersky Industrial CyberSecurity for Networks 可能会依赖过时且可能存在漏洞的加密协议和算法。如果您的网络上没有运行过时操作系统的设备，或者不需要连接此类设备，我们建议在 Kaspersky Industrial CyberSecurity for Networks 中禁用过时且可能存在漏洞的协议和加密算法。欲了解更多信息，您可以联系技术支持。

可以从其接收和处理 EPP 应用程序数据的计算机的最大数量为 1000 台。

安装了 Endpoint Agent 软件组件的计算机的数据通过*集成服务器*转发到 Kaspersky Industrial CyberSecurity for Networks。任何安装了 Kaspersky Industrial CyberSecurity for Networks 组件（服务器或探测器）的节点都可以执行集成服务器功能。为了与 Endpoint Agent 集成，请将集成服务器添加到从具有 Endpoint Agent 的计算机接收数据的节点。

集成服务器可以在 TCP 和 UDP 模式下运行。根据节点上集成服务器使用的模式，Kaspersky Industrial CyberSecurity for Networks 实施以下服务之一以便与 EPP 应用程序集成：

- kics4net-epp-proxy（如果为集成服务器启用了 TCP 模式）。
- kics4net-telemetry-proxy（如果为集成服务器启用了 UDP 模式）。

在每个集成服务器上，您可以单独或同时使用 TCP 和 UDP 模式。服务的安装包包含在 Kaspersky Industrial CyberSecurity for Networks 的分发包中。

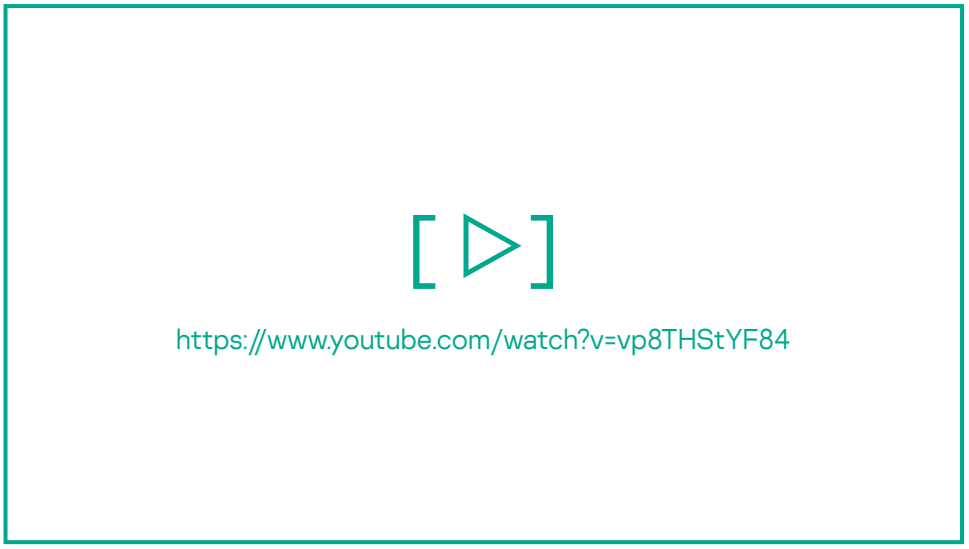
在 TCP 模式下，集成服务器接收来自 EPP 应用程序的数据并确认收到该数据。此模式允许您对托管 Endpoint Agent 的设备执行各种操作。在 UDP 模式下，来自 EPP 应用程序的数据通过 UDP 协议发送，无需确认接收。由于 UDP 上的单向数据传输，当运行 Endpoint Agent 的计算机通过数据二极管向集成服务器传输数据时，您可以使用 UDP 模式。但是，与 TCP 模式相比，UDP 模式下的功能有所降低。

下表列出了根据您使用的模式可用的操作。

与 EPP 应用程序配合使用时可用的操作

操作	TCP 模式	UDP 模式
基于 EPP 技术注册事件（工作站和服务器保护事件）	✓	✓
使用托管已安装的 EPP 应用程序的设备（以及与此类设备进行过双向交互的设备）填充设备表。	✓	✓
使用托管已安装的 EPP 应用程序的设备的信息（例如，操作系统版本、型号或开发商的信息）更新设备表。	✓	✓
在网络交互图的节点和拓扑图的节点上显示特殊图标，指示 EPP 应用程序的存在和连接状态	✓	✓
网络会话注册	✓	✓
监控设备器材	✓	—
监控设备用户	✓	—
监控设备应用程序和补丁	✓	—
设备配置控制	✓	—
设备上的可执行文件启动控制	✓	—
作为漏洞和合规性审计作业以及配置控制作业的一部分扫描设备	✓	—
如果在 Endpoint Agent 中为这些事件构建了威胁开发链，则使用 EPP 技术记录事件时触发响应操作	✓	—

您可以观看教程视频（见下方）来熟悉其功能。



无 SPAN 模式

HTTPS over TCP 协议用于将运行 Endpoint Agent 的计算机安全地连接到 TCP 模式下的集成服务器。HTTP 连接通过使用 Kaspersky Industrial CyberSecurity for Networks 服务器颁发的证书来保护安全。以下证书可用于 TCP 模式下的连接：

- 集成服务器证书。每次建立连接时，Endpoint Agent 计算机都会验证此证书。直到证书验证成功完成时才建立连接。
- 客户端证书。此证书用于对具有 Endpoint Agent 的计算机集成服务器客户端进行身份验证。同一个客户端证书可以被多台装有 Endpoint Agent 的计算机使用。默认情况下，集成服务器不会验证客户端的证书，但您可以启用客户端证书验证来加强连接的安全性。

在 UDP 模式下工作时，建议通过加密来确保传输数据的保护。要加密数据，运行 Endpoint Agent 的计算机必须使用从 Kaspersky Industrial CyberSecurity for Networks 收到的加密密钥。

证书和公钥（用于 TCP 模式）或加密密钥（用于 UDP 模式）通过 Kaspersky Security Center 传输到运行 Endpoint Agent 的计算机。为了预加载这些数据，Kaspersky Security Center 使用通信数据包，这些数据包是包含相应文件的压缩文件。添加集成服务器后，必须在 Kaspersky Industrial CyberSecurity for Networks 中创建通信数据包。

只有具有管理员角色的用户才能配置来自 EPP 应用程序的数据接收。

准备从 EPP 应用程序接收数据的场景

准备从 EPP 应用程序接收数据的场景包括以下阶段：

1. **在受监控网络的计算机上安装 EPP 应用程序**

   在此阶段，您需要安装执行保护工作站和服务器功能的卡巴斯基应用程序（EPP 应用程序）。您需要在 Kaspersky Industrial CyberSecurity for Networks 中接收其数据的所有计算机上安装 EPP 应用程序。这些计算机必须位于工业网络之外（其流量通过监控点进行监控），或者与另一个网络有额外连接，该网络包含安装了 Kaspersky Industrial CyberSecurity for Networks 组件的节点之一（例如，与 Kaspersky Industrial CyberSecurity 专用网络的连接）。

   如果 EPP 应用程序的 Endpoint Agent 软件组件的功能由 Kaspersky Endpoint Agent 执行，则还必须在相应的计算机上安装该应用程序。

Kaspersky Industrial CyberSecurity for Networks 支持与以下 EPP 应用程序集成：Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Linux Nodes。要了解支持的 EPP 应用程序版本，请参考“硬件和软件要求”文章。

2 为 Kaspersky Industrial CyberSecurity for Networks 节点添加集成服务器

此阶段涉及完成将集成服务器添加到装有 Endpoint Agent 软件组件的计算机将连接到的节点的过程。节点与这些计算机之间的网络交互仅可通过未用作监控点的网络接口来实现。没有为集成服务器配置特定的网络接口和 IP 地址，因为计算机的任何可用网络接口和 IP 地址都可以用于与集成服务器的外部连接。

3 为集成服务器客户端创建通信数据包

在此阶段，您需要创建和下载通信数据包，应用程序在其中保存用于客户端和集成服务器之间连接的证书和/或密钥。

用于在 TCP 模式下连接到 Endpoint Agent 计算机的每个通信数据包都是一个包含以下数据的存档：

- 集成服务器的公共证书密钥。
- 集成服务器客户端的证书（带有私钥）。如果集成服务器上启用了客户端证书验证，则会添加此证书。证书和密钥以加密形式保存，密码是在创建通信数据包时指定的。

在 UDP 模式下，通信数据包是一个包含加密密钥的存档。加密密钥以加密形式保存，密码是在创建通信数据包时指定的。

4 将集成服务器连接数据上传至客户端计算机

装有 Endpoint Agent 软件组件的计算机作为 Kaspersky Industrial CyberSecurity for Networks 集成服务器的客户端。

在这个阶段，使用 Kaspersky Security Center 将数据上传到客户端计算机。要执行它，使用 Endpoint Agent 管理插件将通信数据包中的证书和/或密钥上传到 Kaspersky Security Center 管理服务器。然后，您可以在 Kaspersky Security Center 中创建策略，以便将数据上传到 Endpoint Agent 计算机。有关处理数据和创建策略的信息，请参阅 EPP 应用程序文档或 Kaspersky Endpoint Agent 文档。必须为每个集成服务器创建至少一个策略。

5 在必要的模式下启用集成服务器

应用策略并将数据上传到 Endpoint Agent 计算机后，此阶段即完成。在此阶段，您必须为所有将接收 EPP 应用程序数据的集成服务器启用 TCP 和/或 UDP 模式。启用集成服务器后，节点上将激活以下服务：

- kics4net-epp-proxy – 当集成服务器以 TCP 模式启用时。
- kics4net-telemetry-proxy – 当集成服务器以 UDP 模式启用时。

6 通过数据二极管接收遥测数据的附加配置

如果运行 Endpoint Agent 的计算机必须通过数据二极管向 Kaspersky Industrial CyberSecurity for Networks 发送遥测数据，则需要执行此步骤。

根据 EPP 应用程序的版本，Endpoint Agent 组件可以使用以下协议通过数据二极管发送遥测数据：

- MQTT over TCP。

  当在集成模式下使用 Kaspersky Industrial CyberSecurity for Nodes 时，会使用此协议。要通过此协议接收遥测数据，必须在集成服务器上启用 TCP 模式。有关配置 EPP 应用程序以使用这种数据传输方法的详细信息，请参阅相应的帮助系统：Kaspersky Industrial CyberSecurity for Nodes 4.5 或 Kaspersky Endpoint Agent 4.0。要通过数据二极管传递 MQTT 消息，您可能需要根据制造商的文档在数据二极管端配置 MQTT 代理功能。

- UDP

在集成模式下使用 Kaspersky Industrial CyberSecurity for Linux Nodes 版本 2.0 时，使用此协议。要通过此协议接收遥测数据，必须在集成服务器上启用 UDP 模式。有关配置 EPP 应用程序以使用这种数据传输方法的详细信息，请参阅Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 的帮助系统。

此外，推荐执行以下步骤来配置节点和网络部件：

- 在运行 EPP 应用程序的计算机的 ARP 表中指定托管集成服务器的节点的 IP 地址和 MAC 地址。
- 使用备份网络时，请为托管集成服务器的节点分配不属于任何备份网络的 IP 地址。
- 在运行 EPP 应用程序的节点的路由表中，指定指向托管集成服务器的节点的静态路由。
- 在运行 EPP 应用程序的节点上，每次切换到备用网络后，通过运行以下命令停止并重新启动 Kaspersky Industrial CyberSecurity for Networks 集成任务：

```
sudo kics-control --stop-task 23
sudo kics-control --start-task 23
```

- 在每个数据二极管的配置中，将最大传输单元 (MTU) 的值增加到 1514 字节。
- 在位于运行 EPP 应用程序的节点和数据二极管之间的每个网络交换机的配置中，将托管集成服务器的节点的静态地址添加到 MAC 地址表中。必须为网络交换机的出站端口指定节点 MAC 地址。

当此场景实现时，Kaspersky Industrial CyberSecurity for Networks 将开始接收和处理来自 EPP 应用程序的数据。

添加集成服务器

要添加集成服务器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接服务器**”。
3. 在“**集成服务器**”选项卡上，单击“**添加 Endpoint Agent 集成服务器**”打开详细信息。
4. 在“**节点**”下拉列表中，选择需要添加集成服务器的已安装应用程序组件（服务器或探测器）的节点。

   您只能选择尚未添加集成服务器的节点。
5. 如果您需要在 TCP 模式下运行时启用客户端身份验证的证书验证，请为集成服务器客户端创建一个或多个证书。为此，请单击“**创建新证书**”部分中的“**客户端证书 (TCP 模式)**”按钮。

   您可以为集成服务器客户端创建 10 个证书。如有必要，您可以使用包含证书指纹的字段右侧的 × 图标从列表中删除不必要的证书。

   若您创建了多个客户端证书，您可以在创建通讯数据包时选择相关的证书。
6. 如果您需要在 UDP 模式下从 EPP 应用程序接收加密数据，请创建一个或多个加密密钥。为此，请点击**创建加密密钥**部分中的**加密密钥 (UDP 模式)**按钮。

   您可以创建 10 个加密密钥。如有必要，您可以使用包含密钥指纹的字段右侧的 × 图标从列表中删除不必要的密钥。
7. 单击**保存**。

创建用于集成服务器客户端的通信数据包

添加集成服务器或更改其设置后，您需要为该服务器的客户端创建并下载通信数据包。

要为集成服务器客户端创建新的通信数据包：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接服务器**”。
3. 在“**集成服务器**”选项卡上，选择要为其客户端创建新的通信数据包的服务器。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 点击“**获取通信数据包**”按钮。
5. 如果为集成服务器启用了客户端证书验证或传输数据的加密，则会打开“**生成新的通信数据包**”窗口。执行以下操作：
   a. 执行以下操作之一：
      a. 如果您需要使用 HTTPS over TCP 配置与集成服务器客户端的安全连接，请从“**连接类型**”下拉列表中选择 **TCP**，然后从“**客户端证书**”下拉列表中选择用于集成服务器客户端身份验证的必要证书。
      b. 如果您需要使用 UDP 从 EPP 应用程序接收加密数据，请从“**连接类型**”下拉列表中选择 **UDP**，然后从“**加密密钥**”下拉列表中选择用于数据加密的必要加密密钥。
   b. 指定访问所选证书或加密密钥的密码。使用定义的密码，证书或加密密钥将被加密在通信数据包中。
   c. 单击“**创建通信数据包**”。

Kaspersky Industrial CyberSecurity for Networks 服务器为所选集成服务器的客户端生成新的通信数据包，然后浏览器保存下载的文件。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。

您需要将新的通信数据包的内容上传到集成服务器客户端计算机。这些上传是使用 Kaspersky Security Center 管理服务器策略执行的。在 Kaspersky Security Center 策略中，您需要指定用于连接到集成服务器的 IP 地址（为此，您可以使用所选集成服务器的详细信息区域中指示的可用 IP 地址之一）。

在配置与 EPP 应用程序的集成时，会创建并配置 Kaspersky Security Center 策略。有关配置集成的信息，请参阅 EPP 应用程序文档或 Kaspersky Endpoint Agent 文档。

集成服务器表

集成服务器表显示在“**设置**” → “**连接服务器**”下，“**集成服务器**”选项卡上。此表显示有关添加到安装了应用程序组件的节点的集成服务器的信息。

集成服务器表包含以下信息：

- **节点名称** – 安装了应用程序组件的节点的名称。
- **IP 地址** – 节点所有网络接口上的 IP 地址列表（未为集成服务器配置特定网络接口和 IP 地址，因为计算机的任何可用网络接口和 IP 地址都可用于到集成服务器的外部连接）。
- **TCP 模式**- TCP 模式下集成服务器运行的当前状态。
- **验证客户端证书** – 指示是否在 TCP 模式下启用或禁用客户端证书验证（如果禁用验证，则表单元格为空）。
- **每秒请求数** – 从客户端到集成服务器的成功处理请求的平均数量。
- **UDP 模式**- UDP 模式下集成服务器运行的当前状态。
- **UDP 加密**- 指示是否在 UDP 模式下运行时启用或禁用加密数据接收（如果禁用加密数据接收，则表格单元格为空）。

在必要模式下启用和禁用集成服务器

集成服务器可以在 TCP 和 UDP 模式下运行。集成服务器创建后，TCP 和 UDP 模式默认处于禁用状态。因此，Kaspersky Industrial CyberSecurity for Networks 不会处理该服务器客户端的数据。

您可以单独或同时使用 TCP 和 UDP 模式。

要启用或禁用与运行 Endpoint Agent 的计算机的连接：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接服务器**”。
3. 在“**集成服务器**”选项卡上，选择要为其启用或禁用 EPP 应用程序连接的服务器。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 如果需要在 TCP 模式下启用或禁用集成服务器，请单击“**启用 TCP 模式**”或“**禁用 TCP 模式**”按钮。
5. 如果需要在 UDP 模式下启用或禁用集成服务器，请单击“**启用 UDP 模式**”或“**禁用 UDP 模式**”按钮。

编辑集成服务器设置

编辑集成服务器设置时，您可以替换集成服务器本身的证书，也可以编辑客户端的证书和加密密钥列表。

要编辑集成服务器设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接服务器**”。
3. 在“**集成服务器**”选项卡上，选择要更改其客户端设置的服务器。
   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**编辑**。

5. 如果您想要为同一集成服务器替换（颁发新的）证书，请单击“**重新颁发证书**”按钮。

   更换集成服务器证书后，旧证书将失效。

6. 如果您想要在 TCP 模式下修改客户端的证书列表，请单击“**创建新证书**”和/或位于包含证书指纹的字段的右侧的 × 图标。

7. 如果您要编辑在 UDP 模式下运行 Endpoint Agent 的计算机的加密密钥列表，请使用“**创建加密密钥**”按钮和/或位于包含密钥指纹的字段右侧的 × 图标。

8. 单击**保存**。

如果为集成服务器颁发了新证书或创建了新的客户端证书或加密密钥，您需要再次创建并下载通信数据包，以将有关这些证书和/或加密密钥的数据发送到客户端计算机。

删除集成服务器

您可以删除已添加的集成服务器。删除集成服务器后，Kaspersky Industrial CyberSecurity for Networks 将不再接收来自链接的 EPP 应用程序的数据。

要删除集成服务器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 选择“**设置**” → “**连接服务器**”。

3. 在**集成服务器**选项卡上，选择要删除的服务器。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**删除**。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，单击**确定**。

管理 Kaspersky Industrial CyberSecurity for Networks 中的响应操作

如果在 Kaspersky Industrial CyberSecurity for Networks 中配置了与 EPP 应用程序的联合操作，您可以在设备上触发响应操作。响应操作允许防止或最小化检测到的来自工业网络中的设备的威胁的后果。当使用应用程序中的相应对象时，每个响应操作都是手动触发的。

具有 Endpoint Agent 软件组件的设备可以使用触发响应操作的功能。当触发响应操作时，Kaspersky Industrial CyberSecurity for Networks 会将有关该操作的信息传输到 Endpoint Agent。Endpoint Agent 软件组件执行接收到的命令，并向 Kaspersky Industrial CyberSecurity for Networks 发送完成通知。

根据设备上检测到的威胁的性质，您可以触发以下响应操作：

- **将设备与网络隔离**。

启用设备的网络隔离后，Endpoint Agent 软件组件会终止设备上的所有活动 TCP/IP 网络连接，并阻止所有新连接，但以下连接除外：

- Endpoint Agent 中从网络隔离中排除的连接。
- 由与 Endpoint Agent 兼容的 EPP 应用程序的服务启动的连接。
- 由 Endpoint Agent 服务启动的连接。
- 由 Kaspersky Security Center 网络代理启动的连接。

在 Kaspersky Industrial CyberSecurity for Networks 中禁用网络隔离之前，设备网络隔离一直处于活动状态。如果未手动禁用网络隔离，则会在启用后 9999 小时自动禁用。

- **阻止运行**。

  您可以配置规则以阻止可执行文件和脚本的启动，以及在选定设备上打开 Office 格式的文件。例如，您可以阻止在运行 Endpoint Agent 软件组件的选定设备上启动您认为不安全的应用程序。应用程序使用 MD5 和 SHA256 哈希算法通过文件路径或校验和来识别文件。

  在启动阻止的事件中，会向用户通知触发的启动阻止规则。如果设备用户没有关闭弹出通知，它将在弹出通知出现 60 秒后自动关闭。

- **移动到隔离区**。

  *隔离区*是运行 Endpoint Agent 软件组件的设备上的指定本地存储，用于存储可能感染病毒或在检测时无法清除的文件。隔离文件是加密存储的，不会对设备安全造成威胁。

  Kaspersky Security Center 在运行 Endpoint Agent 的设备上生成隔离对象的通用列表。设备网络代理将有关隔离文件的信息传输到管理服务器。

  Kaspersky Security Center 网络代理不会将隔离的文件复制到管理服务器。所有对象都位于运行 Endpoint Agent 的受保护设备上。对象已从受保护设备上的隔离区中恢复。

- **删除文件**。

  系统关键对象 (SCO) 无法删除。SCO 是操作系统和 EPP 应用程序正常运行所需的文件。

  从设备文件系统中删除文件可能会被推迟，直到设备重新启动（例如，如果该文件正在被其他进程使用）。如果文件删除被推迟到设备重新启动，EPP 应用程序会将此事通知 Kaspersky Industrial CyberSecurity for Networks。在这种情况下，触发响应操作后，Kaspersky Industrial CyberSecurity for Networks 会显示有关推迟文件删除的警告。建议重启设备后检查文件是否删除成功。

- **终止进程**。

  您可以远程终止设备上运行的进程。EPP 应用程序终止从为响应操作指定的文件路径处的文件启动的进程。进程名称中的字符区分大小写（进程名称必须与响应操作中的文件名完全匹配）。

  系统关键对象 (SCO) 无法终止。

  设备可能有多个进程在为响应操作指定的文件路径上运行。在这种情况下，EPP 应用程序会尝试终止所有此类进程，同时考虑到可以终止的进程数量的限制（如果应用程序中指定了这样的限制）。因此，如果从单个可执行文件运行大量进程，EPP 应用程序可能无法终止其中一些进程。

- **启动进程**。

  在设备上，您可以远程运行可执行文件、脚本、实用程序和应用程序的进程（包括通过"**终止进程**"响应操作终止的进程）。要启动一个进程，必须指定启动命令。您还可以指定命令行参数和工作目录的路径。请注意，要使用设备上的 Kaspersky Industrial CyberSecurity for Linux 节点 EPP 应用程序启动进程，您可能需要配置 SELinux 系统。

  命令执行后，Endpoint Agent 软件组件在进程启动时会将包含标准输出和错误流数据的文本文件发送到 Kaspersky Industrial CyberSecurity for Networks（每个文件的数据不超过 100 KB）。

对于“**将设备与网络隔离**、**阻止运行**和**移动到隔离区**响应操作，您可以在 Kaspersky Industrial CyberSecurity for Networks 中触发相应的反向操作。此功能允许您在触发的响应操作完成并且威胁从设备中消除后恢复正常的设备功能。可以进行以下反向操作：

- **禁用网络隔离**。
- **禁用运行阻止**。
- **从隔离区恢复**。

Kaspersky Industrial CyberSecurity for Networks 注册触发了响应操作和相应的反向操作。已注册的操作显示在“**事件**”部分的“**响应操作**”选项卡上。

您可以通过选择相关事件、可执行文件或设备来触发响应操作。您还可以使用已注册并完成的响应操作来触发新的响应操作，只要所选操作允许触发反向操作即可。

可用的操作取决于选定的对象。例如，如果选择了带有 Endpoint Agent 软件组件的设备，则只能管理该设备的网络隔离和进程的启动。所有其他响应操作均在其他条件下可用。

只有具有管理员或安全官角色的用户才能触发响应操作和相应的反向操作。

触发事件响应动作

您可以使用与设备关联的注册事件来触发设备上的响应操作。要触发响应操作，必须使用 EPP 技术注册一个事件，并在 Endpoint Agent 中为该事件构建威胁发展链（该事件为 EDR 事故）。

触发 EDR 事故中设备的响应操作：**将设备与网络隔离**

您可以针对任何 EDR 事故触发**将设备与网络隔离**响应操作。

要从网络中隔离与 EDR 事故关联的设备：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**事件和突发事件**部分中选择**事件**选项卡。
3. 在事件表中，选择是 EDR 事故的相关事件。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 在详细信息区域中，打开“**威胁响应**”下拉列表并选择“**将设备与网络隔离**”。
   将打开一个带有确认提示的窗口。
5. 在请求窗口中确认响应操作的开始。

应用程序将注册一个新的响应操作。您可以在“**事件**”部分的“**响应操作**”选项卡上查看有关此操作的信息。

触发 EDR 事故活动事件中对象的响应操作：**阻止运行**、**移动到隔离区**、**删除文件**或**终止进程**。

对于威胁发展链中具有“**文件创建**”或“**启动进程**”类型的活动事件的 EDR 事故，您可以触发“**阻止运行**”、“**移动到隔离区**”或“**删除文件**”响应操作。此外，对于具有“**启动进程**”类型的活动事件，应用程序提供了触发“**终止进程**”响应操作的能力。

对于指定的活动事件类型，您可以使用以下选项来触发响应操作：

- 触发关键活动事件中的威胁检测对象：响应操作从支持类型的关键活动事件应用于威胁检测对象。
- 触发任何受支持类型的活动事件：响应操作应用于威胁发展链中选定活动事件的对象。

要触发威胁检测对象的响应操作：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**事件和突发事件**部分中选择**事件**选项卡。
3. 在事件表中，选择是 EDR 事故的相关事件。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 在详细信息区域中，打开“**威胁响应**”下拉列表并选择适当的项目：
   - 如果威胁检测对象的活动事件具有“**文件创建**”类型，则可以选择以下响应操作：“**阻止运行**”、“**移动到隔离区**”和“**删除文件**”。
   - 如果威胁检测对象的活动事件具有“**启动进程**”类型，则可以选择以下响应操作：“**阻止运行**”、“**移动到隔离区**”、“**删除文件**”和“**终止进程**”。

   将打开一个带有确认提示的窗口。
5. 如果响应操作要求您使用密码已确认操作，请输入您的密码。
6. 在请求窗口中，确认响应操作的开始。

应用程序将注册一个新的响应操作。您可以在“**事件**”部分的“**响应操作**”选项卡上查看有关此操作的信息。

要触发对任何受支持类型的活动事件的响应操作：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**事件和突发事件**部分中选择**事件**选项卡。
3. 在事件表中，选择是 EDR 事故的相关事件。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 在详细信息区域中，转到“**所有活动事件**”选项卡并选择适当的活动事件。
   您可以选择具有“**文件创建**”或“**启动进程**”类型的任何活动事件。关键活动事件（带有威胁检测对象）用“**检测**”图标标记。

5. 在打开的活动事件详细信息窗口中，单击相应的按钮：

   - 如果选择了“**文件创建**”类型的活动事件，则可以使用带有“**阻止运行**”、“**移动到隔离区**”和“**删除文件**”响应操作的按钮。
   - 如果选择了“**启动进程**”类型的活动事件，则可以使用具有“**阻止运行**”、“**移动到隔离区**”、“**删除文件**”和“**终止进程**”响应操作的按钮。

   将打开一个带有确认提示的窗口。

6. 如果响应操作要求您使用密码已确认操作，请输入您的密码。
7. 在请求窗口中，确认响应操作的开始。

应用程序将注册一个新的响应操作。您可以在“**事件**”部分的“**响应操作**”选项卡上查看有关此操作的信息。

触发 EDR 事故中设备的响应操作：**启动进程**

您可以针对任何 EDR 事故触发“**启动进程**”响应操作。

要在与 EDR 事故关联的设备上启动进程：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在**事件和突发事件**部分中选择**事件**选项卡。
3. 在事件表中，选择是 EDR 事故的相关事件。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 在详细信息区域中，打开“**威胁响应**”下拉列表并选择“**启动进程**”。
   这将打开用于配置响应操作的窗口。
5. 配置在设备上运行该进程的设置。为此，请输入以下设置的值：

   - 可执行文件、脚本、实用程序或应用程序的完整路径。
   - 工作目录（可选）。
   - 附加启动键（可选）。

6. 在“**操作确认密码**”字段中输入您的密码。
7. 单击**运行**。

应用程序将注册一个新的响应操作。您可以在“**事件**”部分的“**响应操作**”选项卡上查看有关此操作的信息。

使用设备可执行文件时触发响应操作

您可以触发可执行文件的响应操作，有关该操作的信息是在设备上启动可执行文件控制期间收到的。要触发响应操作，可执行文件必须与具有 Endpoint Agent 软件组件并准备从 EPP 应用程序接收数据的设备相关联。

使用可执行文件表时，您可以触发以下响应操作：

- **阻止运行**。
- **移动到隔离区**。
- **删除文件**。
- **终止进程**。

要触发可执行文件的响应操作：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**资产**”部分中选择“**可执行文件**”选项卡。
3. 在可执行文件表中，选择您需要的文件。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 在详细信息区域中，打开“**威胁响应**”下拉列表以触发所需的响应操作。
   如果在与可执行文件相关的设备上安装了 Endpoint Agent 软件组件，则“**威胁响应**”下拉列表中的项目可用。
   将打开一个带有确认提示的窗口。
5. 如果响应操作要求您使用密码已确认操作，请输入您的密码。
6. 在请求窗口中，确认响应操作的开始。

应用程序将注册一个新的响应操作。您可以在“**事件**”部分的“**响应操作**”选项卡上查看有关此操作的信息。

触发设备响应动作

您可以触发“**将设备与网络隔离**”响应操作及其相应的反向操作“**禁用网络隔离**”，以及“**启动进程**”操作。要触发响应操作，设备必须运行 Endpoint Agent 软件组件，并且必须准备好从 EPP 应用程序接收数据。

要触发设备的网络隔离操作：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**资产**”部分的“**设备**”选项卡上，或在“**网络地图**”部分中选择设备。
   在“**网络地图**”部分中，您可以在网络交互地图和拓扑地图上选择设备。
   详细信息区域出现在 Web 界面窗口的右侧。
3. 在详细信息区域中，打开“**威胁响应**”下拉列表并选择适当的项目：
   - **将设备与网络隔离** – 如果您想要将所选设备与网络隔离。
   - **禁用网络隔离** – 如果您想要禁用之前触发了“**将设备与网络隔离**”操作的设备的网络隔离。

   如果设备上安装了 Endpoint Agent 软件组件，则“**威胁响应**”下拉列表中的项目可用。

将打开一个带有确认提示的窗口。

4. 在请求窗口中确认响应操作的开始。

应用程序将注册一个新的响应操作。您可以在“**事件**”部分的“**响应操作**”选项卡上查看有关此操作的信息。

要在设备上启动进程：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**资产**”部分的“**设备**”选项卡上，或在“**网络地图**”部分中选择设备。
   在“**网络地图**”部分中，您可以在网络交互地图和拓扑地图上选择设备。
   详细信息区域显示在 Web 界面窗口的右侧部分。
3. 在详细信息区域中，打开“**威胁响应**”下拉列表并选择“**启动进程**”。
   如果设备上安装了 Endpoint Agent 软件组件，则“**威胁响应**”下拉列表中的项目可用。
   这将打开用于配置响应操作的窗口。
4. 配置在设备上运行该进程的设置。为此，请输入以下设置的值：
   - 可执行文件、脚本、实用程序或应用程序的完整路径。
   - 工作目录（可选）。
   - 附加启动键（可选）。
5. 在“**操作确认密码**”字段中输入您的密码。
6. 单击**运行**。

应用程序将注册一个新的响应操作。您可以在“**事件**”部分的“**响应操作**”选项卡上查看有关此操作的信息。

使用注册的响应操作时触发响应操作

如果在 Kaspersky Industrial CyberSecurity for Networks 中触发了“将设备与网络隔离”**将设备与网络隔离**“阻止运行”**阻止运行**“移至隔离区”**移动到隔离区响应操作**，您可以在“响应**事件**选项卡上的**响应操作**部分中触发相应的反向操作。例如，如果为某个设备触发了“**将设备与网络隔离**”操作，则您可以在使用已注册的操作时触发该设备的“**禁用网络隔离**”操作。

注册反向操作后，您可以使用它来触发同一设备或对象的下一个响应操作。例如，如果您想在禁用网络隔离后再次将设备与网络隔离。

对于“**禁用运行阻止**”和“**从隔离区恢复**”注册操作，您可以触发“**阻止运行**”和“**移动到隔离区**”作为反向操作。

要触发与已注册操作相反的响应操作：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**事件**”部分的“**响应操作**”选项卡上选择操作。
   详细信息区域出现在 Web 界面窗口的右侧。

3. 在详细信息区域中，单击反向操作启动按钮。例如，如果您选择了“**将设备与网络隔离**”操作，请单击“**禁用网络隔离**”按钮以触发反向操作。

   如果选择了以下响应操作之一，则可以使用触发反向操作的按钮：

   - **将设备与网络隔离**。
   - **阻止运行**。
   - **移动到隔离区**。
   - **禁用网络隔离**。
   - **禁用运行阻止**。
   - **从隔离区恢复**。

   将打开一个带有确认提示的窗口。

4. 在请求窗口中确认响应操作的开始。

应用程序将注册一个新的响应动作。

查看响应操作表

响应操作表显示在“**事件**”部分的“**响应操作**”选项卡上。下表显示了在 Kaspersky Industrial CyberSecurity for Networks 中触发响应操作时注册的响应操作。

相应操作设置显示在表的以下列中：

- ID

  已注册操作的唯一 ID。

- **启动**

  操作启动日期和时间。

- **结束**

  完成操作或收到操作确认的日期和时间。如果应用程序尚未收到操作的确认，则会显示要执行的操作的超时期限到期的日期和时间。

- **操作类型**

  已注册操作的类型。提供了以下类型：

  - **将设备与网络隔离**。
  - **阻止运行**。
  - **移动到隔离区**。
  - **禁用网络隔离**。
  - **禁用运行阻止**。

- **从隔离区恢复**。
- **删除文件**。
- **终止进程**。
- **启动进程**。

- **状态**
  操作完成状态。可使用以下状态：
  - **等待发送** – 尚未发送启动操作的命令。
  - **正在运行** – 操作正在启动或正在进行中。
  - **成功** – 操作成功完成。
  - **失败** – 执行操作时发生错误，或者由于接收确认的期限到期而取消了操作。
- **设备**
  为其触发操作的设备的名称。
- **事件标题**
  如果操作是在处理事件时触发的，则为事件标题。
- **对象类型**
  为其触发操作的对象的类型。
- **对象**
  为其触发操作的对象的名称。

查看响应操作表时，您可以使用配置、过滤、搜索和排序功能，以及导航到相关项目。

启动进程时从标准输出和错误流下载包含数据的文件

“**启动进程**”响应操作成功完成后，Endpoint Agent 软件组件会在进程启动时将包含来自标准输出和错误流的数据的 stdout 和 stderr 文本文件发送到 Kaspersky Industrial CyberSecurity for Networks。如果设备接收到相应数据，则会发送文件。

发送的文件有数据大小限制。如果源文件大小大于 100 KB，Endpoint Agent 软件组件会删除发送文件的部分数据，以将文件大小减小到 100 KB。

下载 stdout 和 stderr 文件时，必须考虑以下事项：

- 包含进程启动数据的文件临时存储在服务器数据库中，存储七天后自动删除。
- 具有管理员或安全官角色的用户可以下载文件。

要下载包含标准输出或错误流数据的文件：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**事件**”部分的“**响应操作**”选项卡上选择操作。
   详细信息区域出现在 Web 界面窗口的右侧。
3. 在详细信息区域中，打开“**下载数据**”下拉列表并选择相关项：**标准输出流 (stdout)**或**标准错误流 (stderr)**。
   如果选择了“**启动进程**”响应操作并且包含相应数据的文件存储在服务器数据库中，则下拉列表和项目可用。

您的浏览器将保存下载的文件。根据您的浏览器设置，屏幕可能会显示一个窗口，您可以在其中更改已保存文件的路径和名称。

删除响应操作

您可以删除已注册的响应操作。但是，您无法删除状态为 *“正在进行”*的操作。

> 在删除响应操作之前，应用程序会检查该操作的当前状态。但是，在删除操作期间和删除操作之后，应用程序不会监控在设备上执行的该操作的操作，并且不会取消已经开始的操作。因此，即使该操作在删除时处于“**等待发送**”状态，也可以在设备上执行响应操作。

删除已注册的操作不会覆盖在设备上执行的操作的结果。例如，如果删除了成功完成的“**将设备与网络隔离**”操作，则删除该操作后，设备的网络隔离将继续。要禁用网络隔离，必须触发“**禁用网络隔离**”操作。

在 Kaspersky Industrial CyberSecurity for Networks 中删除“**启动进程**”响应操作后，执行该操作时收到的标准输出和错误流文件也会被删除。

要删除响应操作：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**事件**”部分的“**响应操作**”选项卡上选择操作。
3. 单击“**删除**”。
   将打开一个带有确认提示的窗口。
4. 在提示窗口中，确认删除操作。

管理连接器

本节包含有关管理 Kaspersky Industrial CyberSecurity for Networks 中的连接器的信息。*连接器*是专门的应用程序模块，可促进与 Kaspersky Industrial CyberSecurity for Networks 的数据交换，并可提供直接在应用程序中或通过使用应用程序执行管理任务的功能。

连接器扩展了应用程序与接收系统（包括 Kaspersky Security Center）交互的功能。根据其功能目的，连接器可以将数据传输到接收系统（例如，将事件、应用程序消息和审计条目中继到 SIEM 系统）或从接收系统接收数据（例如，在应用程序中注册外部事件）。应用程序还可以使用连接器对设备进行主动轮询。

使用名为 **Kaspersky Security Center Connector** 的专用连接器，以便应用程序可以与 Kaspersky Security Center 进行交互。此连接器在应用程序中默认创建，无法删除。为了确保连接器正常运行，必须将应用程序与 Kaspersky Security Center 交互的功能添加到 Kaspersky Industrial CyberSecurity for Networks 服务器中。

运行连接器应用程序模块的计算机称为*连接器部署节点*。连接器部署节点可以是任何能够通过网络访问应用程序服务器计算机的计算机（例如安装了应用程序组件的节点，包括服务器的实际计算机）。

连接器的功能能力取决于所选的*连接器类型*。您可以在向应用程序添加连接器时选择相关的连接器类型。应用程序默认具有以下内置连接器类型：

- **Syslog**

  此连接器类型支持将数据转发到 Syslog 服务器。

  添加 **Syslog** 连接器或更改其设置时，请配置连接器的常规设置以及**详细信息**下的附加设置：

  - Syslog 服务器地址
  - Syslog 服务器端口
  - 数据传输协议

- **SIEM**

  此连接器类型支持将数据转发到 SIEM 系统。

  添加 **SIEM** 连接器或更改其设置时，请同时配置连接器的常规设置以及**详细信息**下的附加设置：

  - SIEM 系统服务器地址
  - SIEM 系统服务器端口
  - 数据传输协议

- **一般**

  此连接器类型提供了连接使用 Kaspersky Industrial CyberSecurity for Networks API 的应用程序的功能。

- **电子邮件**

  此连接器类型提供通过电子邮件转发数据的功能。

  添加**电子邮件**连接器或更改其设置时，请同时配置连接器的常规设置以及**详细信息**下的附加设置：

  - 表示电子邮件发件人的地址。
  - 电子邮件的收件人地址。
  - 事件、应用程序消息和审计条目的电子邮件消息的主题。
  - 事件、应用程序消息、审计条目、网络交互以及包含通知的整个消息的文本描述模板。模板通过使用变量形成。
  - 已发送通知的数量达到最大时发出通知电子邮件主题和正文。
  - 每天发送的电子邮件的最大数量。
  - 每条消息中的最大通知数。定义可放入一封电子邮件中的一种类型（事件、应用程序消息或审核条目）的已注册通知的最大数量。如果注册的通知数量超出最大数量，则会生成额外的电子邮件消息（在每日限制内）。

- **主动轮询**

  此连接器类型提供了具有配置控制和主动轮询作业的主动设备轮询功能。

  添加**活动轮询**连接器或更改其设置时，需要配置连接器的常规设置以及**详细信息**下的附加设置：

  - 使用连接器时应用程序用户可以使用的主动轮询方法。
  - 允许或拒绝主动轮询的设备的被允许和被拒绝 IP 地址范围。地址`0.0.0.0`对应所有可能的 IP 地址。如果某个地址同时位于被允许和拒绝的 IP 地址范围内，Kaspersky Industrial CyberSecurity for Networks 会将其视为被拒绝的 IP 地址。
  - 其对应设备可用于主动轮询的地址空间的名称。如有必要，在**L3 地址空间**字段中选择 IP 地址的地址空间，在**L2 地址空间**字段中选择 MAC 地址的地址空间。

    如果选择的地址空间与**默认**地址空间不同，请为该地址空间添加新规则（或更改现有规则）。该规则必须指定选择此地址空间的连接器。当地址空间改变时，规则设置就会被配置。

- KUMA

  此连接器类型提供与 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的集成。此类连接器的软件模块由 Kaspersky Industrial CyberSecurity for Networks 单独提供。使用这种类型的连接器，您可以将有关设备和风险的信息发送给 KUMA，以及使用命令更改 KUMA 中的设备状态。添加连接器后，在 KUMA 中配置集成（创建与 Kaspersky Industrial CyberSecurity for Networks 的连接）。KUMA 连接器和服务器之间的交互是使用 Kaspersky Industrial CyberSecurity for Networks API 执行的。

  KUMA 连接器通过发送有关设备和风险的信息以及应用命令来更改设备状态来提供集成。要将事件发送到 KUMA，请向 Kaspersky Industrial CyberSecurity for Networks 添加 **Syslog** 或 **SIEM** 连接器，并为该连接器指定连接到 KUMA 服务器的数据。添加连接器后，在 KUMA 端配置收集器。

- Cisco **交换机**

  此连接器类型通过 Cisco 网络交换机为设备提供自动网络访问控制支持。

  添加 Cisco **交换机**连接器或更改其设置时，请配置连接器的常规设置以及**详细信息**下的附加设置：

  - 在记录涉及连接器的操作的应用程序事件日志中使用的交换机名称。
  - 将连接器连接到交换机的寻址信息：IP 地址和 SSH 端口。
  - 通过 SSH 连接到交换机的凭据。
  - 建立 SSH 连接前，用于验证的公钥匹配接收到的网络交换机的公钥，以防止网络中此设备被欺骗（若该值为空，则不进行验证）。
  - 用于限制设备网络访问的方法。应用程序提供了基于 MAC 地址（MAC ACL）、IP 地址（IP ACL）在交换机访问控制列表中创建拒绝规则的方法，以及通过禁用设备连接到的以太网端口的方法。

    要使用禁用以太网端口的方法，请配置交换机连接以防止多个设备连接到一个端口。否则，禁用以太网端口以阻止一个设备也会阻止使用该端口连接到网络的所有设备的网络访问。

  - 控制当限制网络访问的方法发生变化时是否重置拒绝规则的选项。如果启用该选项，更改方法将重置先前定义的拒绝规则。
  - 控制**网络设备**、**防火墙**、**交换机**、**虚拟交换机**、**路由器**、**虚拟路由器**和 **Wi-Fi** 的网络访问限制排除项的选项。如果启用该选项，这些类别的设备将被排除在访问限制方法之外。

- 控制拒绝规则是否仅适用于新设备的选项。如果启用该选项，该方法仅适用于已注册检测到新的 4000005003 设备事件的未授权的设备。
- 设备表中“*已授权*”和“*未授权*”设备的轮询间隔。
- 控制连接器重启时是否发送有关被阻止设备的通知的设置。如果启用该选项，则在连接器打开或重新启动后，应用程序会将已应用网络访问限制的设备列表发送到服务器。

如有必要，您可以添加其他类型的连接器，以促进数据交换或在应用程序与其他接收系统交互时提供执行管理任务的功能。

某些端口和协议用于将连接器连接到服务器。

接收系统代表其中一个应用程序用户通过连接器进行连接。建议为每个连接器使用单独的用户账户。这将使得根据审计条目分析通过连接器执行的操作变得更加方便。

连接器表和连接器类型表显示在应用程序 Web 界面的“**设置**”→“**连接器**”下。只有具有管理员角色的用户才能管理连接器和连接器类型。

应用程序中连接器的最大数量 – 20。连接器类型的最大数量 – 100。

关于可管理和不可管理的连接器

应用程序中可以使用可管理和不可管理的连接器。

如果连接器的应用程序模块可以在*添加*连接器后访问自动注册和启动的功能，并且在启用或禁用连接器或删除连接器时可以访问管理这些模块的功能，则该连接器是可管理的。只有安装了应用程序组件的节点才能充当可管理连接器的部署节点。

*不可管理的连接器*不提供可管理的连接器的功能。此类连接器的注册以及其应用程序模块的启动、停止和删除必须在连接器部署节点上手动执行。当启用或禁用无法管理的连接器时，将分别允许或阻止与服务器端此连接器的交互。

连接器和应用程序服务器之间的连接通过使用证书进行保护。当这些连接器添加到应用程序时，将为连接器创建证书。应用程序自动转发为可管理连接器的应用程序模块创建的证书。添加不可管理的连接器时（或添加配置为忽略可管理连接器功能的可管理连接器时），必须使用通信数据包手动上传该连接器的应用程序模块的证书。如果您需要更换（颁发新的）此类连接器的证书，则必须创建新的通信数据包并使用此文件上传新证书。可管理连接器的证书只能通过删除这些连接器然后重新添加来替换。

关于将事件、应用程序消息和审核条目转发到接收系统

您可以使用连接器配置将事件、应用程序消息或审计条目（以下也称为“已注册的通知”）转发到接收系统。对于名为 **Syslog**、**SIEM**、**电子邮件**和 **Kaspersky Security Center Connector** 的连接器类型，默认情况下启用转发已注册通知的功能。对于 KUMA **连接器类型**，如果安装了应用程序模块，则可以转发已注册通知。当使用添加到应用程序的其他类型的连接器时，此功能是否可用取决于为这些特定连接器类型定义的设置。

转发已注册通知的设置为每个连接器单独配置。配置事件类型时，您可以选择相关的事件类型通过连接器转发。创建连接器或更改其设置时，您可以启用或禁用通过此连接器转发所有应用程序消息和所有审计条目。

某些类型的连接器提供限制传输数据量的功能。此限制适用于从服务器时区 0:00 开始的 24 小时时间段。您可以为以下系统类型的连接器设置传输数据量限制：

- **Email**。对于此类连接器，您可以定义有关新注册通知的电子邮件消息的最大数量以及每封消息中注册通知的最大数量。如果已发送最大数量的电子邮件，则收件人将收到一条消息，通知他们已超出最大数量。此后，直到当天结束才会发送新消息。

- **Kaspersky Security Center 连接器**。对于此类连接器，您可以定义可转发的最大注册通知数量。如果注册的通知数量超出此最大数量，则当天结束前注册的超出部分通知将不会被发送到 Kaspersky Security Center。

包含多个网络交互信息的事件将如下所示特别转发。当通过**Kaspersky Security Center 连接器**转发时，每个事件都被视为一个项目。不过，在转发时，事件会被转换为多个注册的通知，每个通知代表一次网络交互。因此，**Kaspersky Security Center 连接器**的已注册通知列表可能包含比确定最大通知数量的设置所定义的通知数量更多的通知。

通过**Syslog**和**SIEM**连接器转发的已注册通知的信息的内容和顺序可能与 Kaspersky Industrial CyberSecurity for Networks Web 界面页面上显示的信息的内容和顺序不同。

通过**电子邮件**连接器转发的电子邮件消息针对每种类型的注册通知分别生成。换句话说，会生成单独的电子邮件消息来转发事件、应用程序消息和审计条目。

通过 Cisco 交换机连接器自动控制设备的网络访问

您可以通过 **Cisco 交换机**连接器为设备配置自动网络访问控制。这种类型的连接器与交换机交换信息，以发送命令来添加或删除连接到交换机的设备的网络访问拒绝规则（限制）。

设备的网络访问控制由其状态驱动。连接器在交换机上为状态为*未授权*的设备创建拒绝规则，并在为设备分配*已授权*状态后删除规则。

每个连接器只能与一个网络交换机连接。

Cisco 交换机连接器用于仅限制那些详细信息包含其 MAC 地址的设备的网络访问。而且，这些 MAC 地址必须存储在网络交换机的 ARP 表中。也就是说，具有这些 MAC 地址的设备必须连接到连接器所连接的网络交换机。

连接器可以使用各种方法来限制设备的网络访问。应用程序提供了基于 MAC 地址（MAC ACL）、IP 地址（IP ACL）在交换机访问控制列表中创建拒绝规则的方法，以及通过禁用设备连接到的以太网端口的方法。

要使用禁用以太网端口的方法，请配置交换机连接以防止多个设备连接到一个端口。否则，禁用以太网端口以阻止一个设备也会阻止使用该端口连接到网络的所有设备的网络访问。

为了最大限度地降低连接器影响合法过程设备网络访问的风险，您可以在配置期间启用以下设置：

- 控制**网络设备**、**防火墙**、**交换机**、**虚拟交换机**、**路由器**、**虚拟路由器**和 **Wi-Fi** 的网络访问限制排除项的选项。如果启用该选项，这些类别的设备将被排除在访问限制方法之外。

- 控制拒绝规则是否仅适用于新设备的选项。如果启用该选项，该方法仅适用于已注册检测到新的 4000005003 设备事件的未授权的设备。

连接器通过 SSH 与网络交换机连接。SSH 连接凭证在连接器配置中指定并存储。为了保护这些对于识别和身份验证至关重要的敏感凭证，连接器会根据存储的值验证它收到的交换机公钥，以防止交换机欺骗。在验证收到的公钥与连接器中保存的公钥匹配后，识别和身份验证详细信息将发送到交换机。

在操作期间，连接器根据执行的操作的结果在应用程序中记录事件。这些事件通过外部技术记录。生成以下事件标题：

- 重置<交换机名称>的设备拒绝规则

  当连接器由于网络访问限制方法的改变而重置设备先前定义的拒绝规则时，会记录此类事件。

- 根据来自<交换机名称>的数据，更新了关于<设备名称>的信息，地址为<设备 MAC 地址>

  此类事件表示连接器从交换机接收到某个设备连接到某个端口的信息。

- 在<交换机名称>上为<设备名称>添加了设备拒绝规则

  当连接器限制未经授权的设备的网络访问时，会记录此类事件。

- 删除了<交换机名称>上<设备名称>的拒绝规则

  当连接器成功删除特定设备的网络访问限制时，会记录此类事件。

- <交换机名称>先前已添加拒绝规则

  此类事件表明，连接器在打开或重新启动时发现特定交换机上存在预先存在的拒绝规则。

- 在未验证公钥的情况下与<交换机名称>建立了 SSH 连接

  当连接器成功与交换机建立 SSH 连接但无法验证其公钥时，会记录此类事件。我们建议验证网络上没有欺骗设备，然后在连接器设置中保存新的公钥。

- 检测到<交换机名称>的公钥不匹配

  当连接器检测到交换机存储的公钥和接收的公钥不匹配时，就会记录此类事件。这会阻止与交换机的 SSH 连接。我们建议验证网络上没有欺骗设备，并且交换机公钥确实已更改，然后在连接器设置中保存新的公钥。

- 与交换机<交换机名称>建立 SSH 连接失败：凭证不正确

  当连接器由于连接器设置中指定的凭据（用户名和/或密码）不正确而无法与交换机建立 SSH 连接时，会记录此事件。

- 特权模式操作没有在交换机<交换机名称>上执行：密码不正确

  当连接器没有特权模式功能来添加和删除交换机上的设备拒绝规则时，会记录此事件。这种情况下，请在连接器设置中输入正确的特权模式密码。

添加连接器

您可以根据应用程序中可用的连接器类型之一添加连接器。

要使用所有 KUMA 集成功能，请添加两种类型的连接器。要将有关设备和风险的信息发送到 KUMA 并已使用命令更改设备状态，请添加 **KUMA** 连接器。要将 Kaspersky Industrial CyberSecurity for Networks 事件发送到 KUMA，请添加 **Syslog** 或 **SIEM** 连接器并指定用于连接到此连接器的 KUMA 服务器的数据。

在添加连接器之前，建议您创建一个单独的用户帐户，接收系统将使用该帐户连接到应用程序。

要添加连接器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接器**”。

3. 在**连接器**选项卡上，单击**添加连接器**打开详细信息区域。

4. 配置连接器常规设置：

   a. 选择相关的连接器类型并输入连接器名称。

   b. 如果要添加不可管理的连接器（或配置为忽略可管理连接器功能的连接器），请输入访问连接器证书的密码。

   使用定义的密码，证书将被加密在连接器的通信数据包中。

   c. 指定应用服务器的地址。

   连接器将连接到指定地址的服务器。

   d. 指定连接器部署节点：

   - 如果要添加可管理的连接器，您可以使用已安装应用程序组件的节点之一作为连接器部署节点。
   - 如果要添加不可管理的连接器，则需要输入将运行连接器应用程序模块的计算机的 IP 地址。

   e. 选择接收系统将用于通过连接器连接到应用程序的用户帐户。您必须指明其中一位应用程序用户的名称。

5. 在**详细信息**块中，根据连接器的类型指定高级设置。如果连接器类型不允许配置高级设置，则**详细信息**块不会显示在详细信息区域中。

6. 如果连接器类型提供转发应用程序消息和审计条目的功能，请使用相应的复选框来启用或禁用此数据的转发。

   如果通过连接器连接的用户具有操作员角色，则无法传输审计记录。

7. 如果需要，输入连接器描述。

8. 单击**保存**。

   新的连接器将出现在连接器表中。

   如果添加了不可管理的连接器，服务器将为新的连接器生成通信数据包。然后浏览器会保存下载的文件。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。您需要将新的通信数据包的内容上传到将使用连接器的应用程序。

9. 对于不可管理的连接器，请在托管该连接器的节点上创建服务。为此，您可以使用相应的脚本：

   - 如果已添加**Syslog**、**SIEM**、**通用**或**电子邮件**连接器，则可以使用位于托管已安装应用程序组件的节点计算机上的目录 /opt/kaspersky/kics4net-connectors/libexec/ 中的 default_connectors_registrar.py 脚本创建服务。要运行该脚本，请在操作系统控制台中输入以下命令：

     ```
     sudo python3 default_connectors_registrar.py create
     ```

     当被脚本提示提供连接器数据时，请输入连接器的名称、通信数据包的路径以及连接器证书访问密码。

- 如果已添加**主动轮询**连接器，则可以使用位于托管已安装应用程序组件的节点计算机上的目录 /opt/kaspersky/kics4net-apm/src/ 中的 register.py 脚本创建服务。要运行该脚本，请在操作系统控制台中输入以下命令：

```
sudo python3 register.py -p "<通信数据包的完整路径>"
```

查看连接器表

连接器表显示在“**连接器**” → “**设置**”部分的“**连接器**”选项卡上。

连接器设置显示在表格的以下列中：

- **名称**

  连接器的定义名称。

- **连接器 ID**

  连接器创建时指定的 ID。

- **已启用**

  指示服务器是否已准备好与连接器的应用程序模块交互。如果此设置的值为“**否**”，则服务器不接受来自连接器应用程序模块的请求。

- **状态**

  连接器应用程序模块的运行状态。可使用以下状态：

  - **等待注册** – 添加无法管理的连接器或为无法管理的连接器创建新的通信数据包后，尚未通过此连接器建立连接。
  - **切换** – 连接器的应用程序模块的运行状态从“**关闭**”切换到“**开启**”，反之亦然。
  - **关闭** – 服务器不接受来自连接器应用程序模块的请求。如果连接器可管理，则停止运行的命令将发送到其应用程序模块。
  - **开启** – 使用为此连接器创建的证书通过此连接器成功建立了连接。
  - **错误** – 尝试使用连接器的应用程序模块执行操作时发生错误。

- **类型**

  连接器类型的图标和名称。

- **上次连接**

  上次通过此连接器连接的日期和时间。

- **可管理的**

  指示连接器是可管理的。如果此设置的值为“**否**”，则连接器无法管理或者被配置为忽略可管理连接器的功能。

- **更改时间**

  连接器设置最后修改的日期和时间。

- **描述**
  连接器的定义描述。

查看连接器表时，您可以使用配置、过滤、搜索和排序功能。

启用和禁用连接器

如果您想暂时阻止连接器的应用程序模块连接到服务器，您可以禁用该连接器。要恢复连接，您必须启用连接器。

要启用或禁用连接器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接器**”。
3. 在“**连接器**”选项卡上，选择要启用或禁用的连接器。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击相关的“**启用**”或“**禁用**”。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，单击**确定**。

编辑连接器设置

要编辑连接器设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接器**”。
3. 在**连接器**选项卡上，选择相关的连接器。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
5. 您可以按照添加连接器时相同的方式编辑设置。
   并非所有设置都可供编辑。例如，所选的连接器类型无法更改。
6. 单击**保存**。

更改将显示在连接器表的相应列中。如果您更改了连接器名称，新名称将显示在事件类型表的列标题中。

当不可管理连接器的某些设置发生更改时，服务器将为该连接器生成新的通信数据包（例如，如果您更改被配置为忽略可管理连接器功能的**Syslog**连接器的服务器地址，就会发生这种情况）。根据浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的通信数据包的路径和名称。您需要将新的通信数据包的内容上传到使用连接器的应用程序。否则，该应用程序将无法通过连接器建立新的连接。

为连接器创建新的通信数据包

当添加不可管理的连接器时，会自动为该连接器创建通信数据包。如有必要，您可以为连接器创建一个新的通信数据包（例如，如果先前通信数据包中的证书已被泄露，并且您不得不更新用于连接连接器的证书）。

创建新的通信数据包后，旧通信数据包中的证书将失效。因此，下次通过此连接器连接接收系统时，您必须使用新的通信数据包。

要为无法管理的连接器创建新的通信数据包：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接器**”。
3. 在**连接器**选项卡上，选择要为其创建新的通信数据包的不可管理的连接器。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击“**获取新的通信数据包**”。
   将打开“**生成新的通信数据包**”窗口。
5. 指定生成通信数据包的设置：
   - 接收系统将用于通过连接器连接到应用程序的用户名。您必须指明其中一位应用程序用户的名称。
     建议指定添加连接器时指示的用户名。如果需要指定其他用户的名称，建议您选择未用于其他连接器且未用于通过 Web 界面连接到服务器的应用程序用户账户。
   - 连接器应用程序模块正在运行的节点的地址。
   - 访问连接器证书的密码。使用定义的密码，证书将被加密在连接器的通信数据包中。
6. 单击“**创建通信数据包**”。

服务器为选定的连接器生成新的通信数据包，然后浏览器保存下载的文件。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。您需要将获取的通信数据包的内容上传到使用该连接器的应用程序。否则，该应用程序将无法通过连接器建立新的连接。

正在删除连接器

当可管理连接器被删除时，其应用程序模块将被自动停止并从连接器部署节点中删除。

在删除不可管理的连接器（或被配置为忽略可管理连接器功能的连接器）之前，您首先需要手动停止它并删除其应用程序模块。

要准备删除不可管理的连接器：

在部署连接器的节点上，根据需要执行以下操作之一：

- 对于**Syslog**、**SIEM**、**Generic**或**Email**连接器，请使用位于托管已安装应用程序组件的节点计算机上的目录 /opt/kaspersky/kics4net-connectors/libexec/ 中的 default_connectors_registrar.py 脚本。要运行该脚本，请在操作系统控制台中输入以下命令：

  ```
  sudo python3 default_connectors_registrar.py delete
  ```

  启动脚本后，当被脚本提示时指定连接器的名称。

- 对于**主动轮询**连接器，在操作系统控制台中输入以下命令：

  ```
  sudo systemctl disable kics4net-apm
  ```

要删除连接器：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接器**”。
3. 在**连接器**选项卡上，选择要删除的连接器。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，确认删除所选的连接器。

添加和删除连接器类型

连接器类型决定了连接器的可用功能以及在这些功能范围内可以实现的特定功能。您可以使用卡巴斯基已经内置到应用程序中的连接器类型，也可以使用其他供应商提供的其他连接器类型。

要将连接器类型添加到应用程序，您必须从供应商处获得以下文件：

- 用于安装连接器的应用程序模块的文件
- 连接器类型描述文件

如果第三方供应商的连接器类型允许您将用户账户凭据保存在连接器中以访问收件人系统，则建议采取措施防止这些账户凭据受到损害。为了最大限度地降低账户凭据受损时的风险，建议仅提供这些用户账户通过连接器进行连接所需的最低权限。

内置连接器类型的文件包含在应用程序分发工具包中。这些文件用于在安装应用程序组件期间自动添加连接器类型。如果由于某种原因从应用程序中删除了内置连接器类型，则可以使用分发工具包中的文件重新添加这些连接器类型。

连接器类型表显示在“**设置**” → “**连接器**”，“**连接器类型**”选项卡上。

查看连接器类型表

连接器类型表显示在“**设置**” → “**连接器**”，“**连接器类型**”选项卡上。

连接器设置显示在表的以下列中：

- **名称**
  由供应商定义的连接器类型名称。
- **提供商**
  连接器类型供应商的名称。
- **版本**
  连接器类型版本号。
- **代码**
  连接器类型的唯一编号。
- **能力**
  此类型连接器可用的功能列表。

查看连接器类型表时，您可以使用配置、过滤、搜索和排序功能。

添加连接器类型

您可以使用该连接器类型的供应商提供的描述文件将连接器类型添加到应用程序。连接器类型的描述文件必须位于 ZIP 存档中。

必须使用该连接器类型的供应商提供的文件手动执行添加的连接器类型的连接器的应用程序模块的安装。应用程序模块需要安装在添加连接器时指定为连接器部署节点的计算机上。

要添加连接器类型：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接器**”。
3. 在“**连接器类型**”选项卡上，单击“**添加连接器类型**”打开详细信息。
4. 使用“**浏览**”选择连接器类型描述文件。
5. 单击**保存**。

新的连接器类型将出现在连接器表中。

删除连接器类型

从应用程序中删除连接器类型时，应用程序还会删除有关此连接器类型的信息以及使用此连接器类型添加的所有连接器。

要删除连接器类型：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**连接器**”。
3. 在“**连接器类型**”选项卡上，选择要删除的连接器类型。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，确认删除所选连接器类型。
6. 如果应用程序具有这种类型的连接器，还应确认已删除这些连接器。

管理安全审计作业

使用 Kaspersky Industrial CyberSecurity for Networks，您可以对监控设备进行安全审计。安全审计是通过运行为所选设备创建的作业来执行的。安全审计作业可以是以下类型：

- 漏洞和合规性审计。
  漏洞和合规性审计作业允许您评估设备是否符合安全标准，并执行其他检查（例如，搜索漏洞或检测设备上安装的软件）。
- 配置控制。
  配置控制作业允许您接收有关设备配置的详细信息并将其保存在应用程序中，还可以使用应用程序比较设备配置的更改。
- 主动轮询。
  主动轮询作业允许您直接从设备本身获取有关设备及其配置的最准确、最完整的信息。

具有除操作员角色之外的任何角色的用户都可以管理安全审计作业。

使用安全审计功能时，请考虑以下特殊注意事项和限制：

- 此功能在添加授权许可密钥后才可以使用。
- 安装了应用程序组件并用于安全审计作业中的设备扫描的节点必须具有对设备的网络访问权限，才能发送和接收数据。为了提供对设备的网络访问，节点计算机必须具有提供这些设备到网络的连接的网络接口。如果监控点的网络接口接收镜像的工业网络流量（例如，来自网络交换机的 SPAN 端口），则这些网络接口不能用于此目的。

漏洞和合规性审计作业

您可以使用漏洞和合规性审计作业对受监控的设备进行安全审计。您可以手动运行安全审计作业，也可以配置计划以自动运行每个作业。

当一项作业启动时，应用程序将启动对该作业所涵盖的设备的扫描。您可以通过电子邮件接收作业执行结果，也可以在应用程序 Web 界面中查看和下载相关数据。根据作业执行结果和扫描结果，应用程序可以执行以下操作：

- 生成包含有关结果信息的报告。

  该应用程序生成 PDF 格式的报告文件。如果在作业设置中启用了通过电子邮件发送报告，则应用程序会自动生成每个作业执行的报告，并将这些报告发送给指定的收件人。如有必要，您可以手动生成已完成作业或单个设备扫描的报告，然后将报告导出到文件中。

- 注册漏洞类别的检测到的风险。

  对于基于漏洞和合规性审计作业结果注册的风险，应用程序指示 **OVAL** 漏洞的来源。如果在作业设置中启用了检测到的漏洞的注册，则应用程序会注册此类风险。同时，具有指定 **OVAL** 漏洞来源的风险将被注册和处理，而不考虑其他漏洞来源的指定风险。因此，风险表可以显示具有相同 CVE ID（或不同漏洞数据库的 ID）但具有不同漏洞源的风险。

漏洞和合规性审计作业必须指定用于进行审计的规则。规则可以用 OVAL 语言编写，也可以使用 OVAL 定义用 XCCDF 语言编写。

您可以使用以下设备轮询方法之一作为作业的一部分执行设备扫描：

- **本地代理**

  如果 Endpoint Agent 软件组件安装在为作业选择的设备上，并且 EPP 应用程序和 Kaspersky Industrial CyberSecurity for Networks 之间的集成已配置，则可以使用此方法。此方法用于在每台设备上使用 Endpoint Agent 进行扫描。

- **远程连接**

  如果为作业选择的设备没有安装 Endpoint Agent 软件组件，但可以通过确保安全管理和数据传输的协议连接到这些设备，请使用此方法。对于此方法，在作业设置中指定已安装应用程序组件的节点之一，从该节点建立与设备的连接。另外，指定远程连接的凭据（凭据作为 Secret 存储在应用程序中）。

在运行 Linux 操作系统的设备上，使用运行 Linux 设备标准诊断实用程序的命令执行扫描。

您可以在“**安全审计**”部分的“**漏洞和合规性审计**”选项卡上管理漏洞和合规性审计作业。如果使用**远程连接**方法扫描设备，则可以在“**设置**” → “**Secret**”下使用必要的凭据创建 Secret。

作业启动且设备扫描完成后，您可以获得有关已执行的扫描的信息。

添加漏洞和合规性审计作业

对于现有的漏洞和合规性审计规则集，您可以添加应用程序用于执行设备扫描的作业。

具有除操作员角色之外的任何角色的用户都可以添加漏洞和合规性审计作业。

使用向导配置漏洞和合规性审计作业。向导将引导您逐步完成所有必需作业设置的配置。配置完成后，您可以等待计划的扫描在设备上启动，也可以手动启动扫描作业。

当添加漏洞与合规性审计作业时，您可以通过以下方式调用配置向导：

- 为所选规则集添加作业。为此：

  1. 选择“**安全审计**”部分。
  2. 在“**规则集**”选项卡上，选择要为其添加漏洞和合规性审计作业的规则集。
  3. 单击“**添加作业**”。

  在配置向导设置中，选定的规则集被指定为默认规则集。

- 添加具有空白设置的作业。为此：

  1. 选择“**安全审计**”部分。
  2. 在“**漏洞和合规性审计**”选项卡上，单击“**添加作业**”。

  配置向导设置没有默认值。

- 从现有作业中添加作业。为此：

  1. 选择“**安全审计**”部分。
  2. 在“**漏洞和合规性审计**”选项卡上，选择要添加新漏洞和合规性审计作业的作业。
  3. 单击“**复制**”。

  配置向导设置的默认值设置为现有作业设置的值。

- 为所选设备添加作业。为此：

  1. 选择“**资产**”部分。
  2. 在“**设备**”选项卡上，选择要为其添加漏洞和合规性审计作业的设备。
  3. 在设备表上方的工具栏中，打开“**创建作业**”下拉列表，然后选择“**漏洞和合规性审计**”。

  在配置向导设置中，默认情况下会生成由所选设备组成的设备列表。

要在配置向导窗口中配置作业设置，请执行以下操作：

1. 在“**选择规则**”部分中，执行以下操作：

   a. 为作业选择所需的规则集（编辑作业时不可用）。

   b. 指定所选规则集的配置文件。

   c. 选择用于执行扫描的规则，如有必要，为变量指定所需的值。

2. 在“**选择设备**”部分，创建一个设备列表，以便在作业执行期间运行扫描。为作业选择最多 1000 台设备。

   您可以使用“**添加到作业**”和“**从作业中删除**”按钮创建设备列表。添加设备时，应用程序会打开一个窗口，其中包含可供选择的设备表。您可以对表格进行过滤和排序，以显示所需的设备。

3. 在“**作业配置**”部分，配置其余作业设置：

   a. 输入作业名称和说明。

      您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`作业名称必须以任何允许的字符开头和结尾（空格除外）。

      作业名称不得超过 256 个字符作业描述不得超过 4096 个字符

   b. 选择以下方法之一轮询设备：

      - **本地代理**

        如果 Endpoint Agent 软件组件安装在为作业选择的设备上，并且 EPP 应用程序和 Kaspersky Industrial CyberSecurity for Networks 之间的集成已配置，则可以使用此方法。此方法用于在每台设备上使用 Endpoint Agent 进行扫描。

      - **远程连接**

        如果为作业选择的设备没有安装 Endpoint Agent 软件组件，但可以通过确保安全管理和数据传输的协议连接到这些设备，请使用此方法。此方法需要以下附加数据：

        - 安装了应用程序组件并用于连接设备的节点。
        - 用于远程连接的账户凭据 Secret

          您只能为作业选择一个具有一组凭据的 Secret。存储在所选 Secret 中的凭据必须适用于为作业选择的所有设备：可以使用 Secret 中的相同凭据连接到这些设备。请记住，某些类型的系统数据（例如操作系统用户的密码）只有被具有足够高权限的用户请求时才能获取。要获取这些数据，您需要在 Secret 中指定具有适当权限级别的用户的凭据，例如具有 root 访问权限的用户或 /etc/sudoers 中列出的用户。

        > 如果尚未将具有所需凭据的 Secret 添加到应用程序中，您可以在不关闭配置向导窗口的情况下在浏览器中打开新选项卡，连接到服务器并添加 Secret，然后使用配置向导窗口中的按钮刷新 Secret 列表。

   c. 如有必要，可根据作业执行结果检测漏洞类别的风险。为此，请选中“**注册检测到的漏洞**”复选框。

   d. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：

      - 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
      - 根据所选选项，指定设置值以定义精确的作业启动时间。

      > 应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果计划作业应该开始运行时，该作业的先前运行状态仍为“*正在运行*”，则应用程序将跳过计划作业的启动。

   e. 若要在作业开始时通过电子邮件发送报告，请启用“**通过电子邮件发送**”选项并指定收件人的地址。

      报告收件人的最大数量为 10。

4. 单击“**创建作业**”关闭向导。

指定的设置显示在作业详细信息的“**设置**”、“**规则**”和“**设备**”选项卡上。

编辑漏洞和合规性审计作业

具有除操作员角色之外的任何角色的用户都可以编辑漏洞和合规性审计作业。

要编辑漏洞和合规性审计作业：

1. 选择“**安全审计**”部分。
2. 在“**漏洞和合规性审计**”选项卡上，选择要更改其设置的作业。
3. 单击**编辑**。

   配置向导启动。配置向导设置的默认值被设置为所选作业设置的值。
4. 在“**选择设备**”部分，创建一个设备列表，以便在作业执行期间运行扫描。为作业选择最多 1000 台设备。

   您可以使用“**添加到作业**”和“**从作业中删除**”按钮创建设备列表。添加设备时，应用程序会打开一个窗口，其中包含可供选择的设备表。您可以对表格进行过滤和排序，以显示所需的设备。
5. 在“**作业配置**”部分，配置其余作业设置：

   a. 输入作业名称和说明。

   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`作业名称必须以任何允许的字符开头和结尾（空格除外）。

   作业名称不得超过 256 个字符作业描述不得超过 4096 个字符

   b. 选择以下方法之一轮询设备：

   - **本地代理**

     如果 Endpoint Agent 软件组件安装在为作业选择的设备上，并且 EPP 应用程序和 Kaspersky Industrial CyberSecurity for Networks 之间的集成已配置，则可以使用此方法。此方法用于在每台设备上使用 Endpoint Agent 进行扫描。

   - **远程连接**

     如果为作业选择的设备没有安装 Endpoint Agent 软件组件，但可以通过确保安全管理和数据传输的协议连接到这些设备，请使用此方法。此方法需要以下附加数据：

     - 安装了应用程序组件并用于连接设备的节点。
     - 用于远程连接的账户凭据 Secret

       您只能为作业选择一个具有一组凭据的 Secret。存储在所选 Secret 中的凭据必须适用于为作业选择的所有设备：可以使用 Secret 中的相同凭据连接到这些设备。请记住，某些类型的系统数据（例如操作系统用户的密码）只有被具有足够高权限的用户请求时才能获取。要获取这些数据，您需要在 Secret 中指定具有适当权限级别的用户的凭据，例如具有 root 访问权限的用户或 /etc/sudoers 中列出的用户。

     如果尚未将具有所需凭据的 Secret 添加到应用程序中，您可以在不关闭配置向导窗口的情况下在浏览器中打开新选项卡，连接到服务器并添加 Secret，然后使用配置向导窗口中的按钮刷新 Secret 列表。

c. 如有必要，可根据作业执行结果检测漏洞类别的风险。为此，请选中“**注册检测到的漏洞**”复选框。

d. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：

- 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
- 根据所选选项，指定设置值以定义精确的作业启动时间。

> 应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果计划作业应该开始运行时，该作业的先前运行状态仍为“*正在运行*”，则应用程序将跳过计划作业的启动。

e. 若要在作业开始时通过电子邮件发送报告，请启用“**通过电子邮件发送**”选项并指定收件人的地址。

报告收件人的最大数量为 10。

6. 单击“**保存**”关闭向导。

指定的设置显示在作业详细信息的“**设置**”、“**规则**”和“**设备**”选项卡上。

查看漏洞和合规性审计作业表

漏洞和合规性审计作业表显示在“**安全审计**”部分的“**漏洞和合规性审计**”选项卡上。

作业设置显示在表格的以下列中：

- **作业 ID**
  Kaspersky Industrial CyberSecurity for Networks 分配的作业 ID。
- **名称**
  用于在应用程序中代表作业的名称。
- **描述**
  作业描述。
- **创建日期**
  将作业添加到应用程序的日期和时间。
- **更改时间**
  应用程序中上次修改作业的日期和时间。
- **规则集**
  与作业关联的规则集的名称。
- **配置文件**
  配置文件的名称，用于定义作业执行期间用于扫描的一组规则和变量。
- **集合中的 XCCDF 规则**
  为作业选择的规则数量以及规则集中的规则总数。

- **所选设备**

  为该作业选择的设备数量。

- **轮询方法**

  选择以扫描设备的轮询方法：“**本地代理**”或“**远程连接**”。

- **注册表漏洞**

  指示是否根据作业结果启用漏洞类别风险检测的标志。

- **计划**

  有关应用程序自动启动作业的计划的信息。

- **上次运行状态**

  上次运行作业时所有设备扫描的结果状态。

- **上次运行**

  作业上次启动的日期和时间。

- **下次运行**

  作业下次计划开始的日期和时间。

查看漏洞和合规性审计作业表时，您可以使用配置、过滤、搜索和排序功能，以及导航到相关项目。

手动启动和停止漏洞和合规性审计作业

您可以手动启动和停止漏洞和合规性审计作业。当您启动或停止一项作业时，应用程序将启动或停止为此作业选择的设备上的所有扫描。

您可以根据上次作业运行的状态停止或启动该作业。例如，如果作业上次运行的状态为“*正在运行*”，则无法启动该作业。

具有除操作员角色之外的任何角色的用户都可以手动启动和停止漏洞和合规性审计作业。

要启动漏洞和合规性审计作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。

3. 在“**漏洞和合规性审计**”选项卡上，选择您要启动的作业。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**运行**。如果无法启动作业，则该按钮将被禁用。

Kaspersky Industrial CyberSecurity for Networks 启动作业。您可以在作业详细信息中的**运行**选项卡上查看正在进行的设备扫描的相关信息。

要停止漏洞和合规性审计作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。

3. 在“**漏洞和合规性审计**”选项卡上，选择您要停止的作业。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击“**停止**。如果作业无法停止，则该按钮将被禁用。

查看有关漏洞和合规性审计作业运行的常规信息

您可以在作业表中查看有关漏洞和合规性审计作业运行的常规信息。该表显示有关最近的作业运行的信息，但不包括有关设备扫描的信息。要查看所有作业运行的一般信息（包括有关设备扫描的信息），请选择该作业，然后在详细信息区域中打开**运行**选项卡。

有关漏洞和合规性审计作业运行的一般信息包括以下内容：

- 作业开始状态。

  可使用以下状态：

  - “**新的**”或“**从不运行**”：已创建新的作业运行，但尚未运行任何扫描。
  - **等待发送**：扫描命令已准备好发送。
  - **正在运行**：作业正在开始。
  - **正在取消**：作业启动正在停止。
  - **已取消**：作业启动已停止。
  - **已完成**：所有扫描已成功完成。
  - **错误**：所有扫描均遇到错误。
  - **部分成功** – 作业已完成，但部分成功：某些扫描的状态为“**已完成**”，而某些扫描的状态为“**已取消**”或“**错误**”。

- 设备扫描状态。

  可使用以下状态：

  - **等待发送**：扫描命令已准备好发送。
  - **正在运行**：扫描正在进行中。
  - **正在取消**：扫描正在停止。
  - **已取消**：扫描已停止。

- **已完成**：扫描已成功完成。
- **错误**– 扫描期间发生错误。

- 启动日期和时间。
- 结束日期和时间。
- 执行持续时间。

在漏洞和合规性审计作业中停止设备扫描

作为漏洞和合规性审计作业的一部分，您可以手动停止设备扫描。当设备扫描停止时，应用程序不会停止此作业中的其他设备扫描。

具有除操作员角色之外的任何角色的用户都可以手动停止设备扫描。

要停止漏洞和合规性审计作业中的设备扫描，请执行以下操作：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。
3. 在“**漏洞和合规性审计**”选项卡上，选择要停止设备扫描的作业。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 在详细信息区域中，转到**运行**选项卡。
5. 选择所需的扫描，然后单击出现的扫描详细信息区域中的**停止**。如果无法停止扫描，则该按钮将被禁用。

删除漏洞和合规性审计作业

您可以删除漏洞和合规性审计作业。但是，您不能删除上次运行状态为**正在运行**或**等待发送**的作业。

具有除操作员角色之外的任何角色的用户都可以删除漏洞和合规性审计作业。

要删除漏洞和合规性审计作业，请执行以下操作：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。
3. 在“**漏洞和合规性审计**”选项卡上，选择要删除的作业。
4. 单击**删除**。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认删除该作业。

   您只能删除上次运行状态不是“**正在运行**”或**等待发送**的作业。如果选定的作业中存在状态为**正在运行**或**等待发送**的作业，则会显示相应的消息。要删除此类作业，请先停止这些作业。

管理漏洞和合规性审计作业运行的存储设置

Kaspersky Industrial CyberSecurity for Networks 将有关漏洞和合规性审计作业运行的信息保存在服务器上的数据库中。有关作业运行的信息将一直存储，直到作业被删除或超出指定的限制。如果有关作业运行的信息量超过指定的限制，应用程序会自动删除 10% 的最旧记录。如果启用了最短存储时间限制，并且应用程序删除了存储时间小于定义限制的条目，则应用程序消息日志中会出现相应的消息。您可以配置用于存储有关作业运行的信息的设置。

要更改漏洞和合规性审计作业运行的存储设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**部署**”。
3. 选择服务器图块。

   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**编辑**。

   详细信息区域将显示用于配置服务器参数的选项卡。
5. 在“**常规**”选项卡上，转到“**漏洞和合规性审计**”部分，然后使用“**最大量**”设置来定义存储有关作业运行的信息的大小限制。

   您可以选择空间限制的计量单位：**MB** 或 **GB**。

   更改此设置的值时，需要记住所有卷限制的总和不能超过节点定义的最大存储卷。
6. 如有必要，请使用“**储存时间(天)**”设置启用有关作业运行的信息的最短存储时间，并指定最短天数。
7. 单击“**保存**”。

配置控制作业

使用配置控制作业，您可以对受监控设备的接收、保存和比较设备配置进行安全审计。配置控制作业还允许您将数据上传到 Kaspersky Industrial CyberSecurity for Networks，以进行设备用户控制、设备应用程序和补丁监控以及 OT 设备硬件监控。

应用程序可以监控以下设备类型：

- **Windows 操作系统** – 包括带有 Windows 操作系统的设备的配置。
- **Linux 操作系统** – 包括带有 Linux 操作系统的设备的配置。
- **网络设备**– 包括归类为网络部件的设备配置（例如路由器和交换机）。
- **PLC** – 包括可编程逻辑控制器的配置或可以使用**主动轮询**类型的连接器接收其配置的任何其他设备的配置。

有关根据所选设备类型检索数据的详细信息，请参阅附录。

您可以手动运行安全审计作业，也可以配置计划以自动运行每个作业。

当一项作业启动时，应用程序将启动对该作业所涵盖的设备的扫描。如果设备扫描检测到设备配置更改，应用程序将注册一个事件。根据为作业选择的配置处理模式，事件包含收到的配置与设备先前配置或其黄金配置的比较结果。

为配置控制作业提供了以下配置处理模式：

- **仅更新** – 每个设备仅保存最后收到的配置。
- **存档版本** – 每个设备的所有唯一配置都已保存。
- **与黄金配置进行比较** – 每个设备的所有唯一配置都保存，同时将新收到的配置与黄金配置进行比较（默认情况下，这是第一个加载的设备配置）。

仅当您使用**主动轮询**PLCPLC"设备类型的配置。提供了以下设备轮询方法来获取其余的设备类型：

- **本地代理**

  如果 Endpoint Agent 软件组件安装在为作业选择的设备上，并且 EPP 应用程序和 Kaspersky Industrial CyberSecurity for Networks 之间的集成已配置，则可以使用此方法。此方法用于在每台设备上使用 Endpoint Agent 进行扫描。

- **远程连接**

  如果为作业选择的设备没有安装 Endpoint Agent 软件组件，但可以通过确保安全管理和数据传输的协议连接到这些设备，请使用此方法。该方法支持获取"**Linux 操作系统**"和"**网络设备**"设备类型的配置。对于此方法，在作业设置中指定已安装应用程序组件的节点之一，从该节点建立与设备的连接。另外，指定远程连接的凭据（凭据作为 Secret 存储在应用程序中）。

您可以在"**配置控制**"部分的"**安全审计**"选项卡上管理配置控制作业。如果使用"**主动轮询**"连接器或"**远程连接**"方法来扫描设备，则可以在"**设置** → **Secret**"下使用必要的凭据创建 Secret。

作业运行且设备扫描完成后，您可以在"配置"**配置设备详细信息区域**中查看有关收到的设备配置的信息。此选项卡上还提供比较配置和分配黄金配置的选项。

当通过 Web 界面连接到服务器时，您可以查看有关已注册事件的信息。

添加配置控制作业

对于应用程序已知的设备，您可以添加作业来接收、保存和比较设备配置。

具有除操作员角色之外的任何角色的用户都可以添加配置控制作业。

配置控制作业是使用向导进行配置的。向导将指导您逐步完成所有必需作业设置的配置。配置完成后，您可以等待计划的扫描在设备上启动，也可以手动启动扫描作业。

添加配置控制作业时，您可以通过以下方式调用配置向导：

- 添加具有空白设置的作业。为此：

  1. 选择"**安全审计**"部分。
  2. 在"**配置控制**"选项卡上，单击"**添加作业**"。

配置向导设置没有默认值。

- 为所选设备添加作业。为此：

  1. 选择“**资产**”部分。
  2. 在**设备**选项卡上，选择要添加配置控制作业的设备。
  3. 您可以选择不超过 100 台设备。
  4. 在设备表上方的工具栏中，打开“**创建作业**”下拉列表，然后选择“**配置控制**”。

  在配置向导设置中，默认情况下会生成由所选设备组成的设备列表。

要在配置向导窗口中配置作业设置，请执行以下操作：

1. 在“**选择设备**”部分，创建一个设备列表，以便在作业执行期间运行扫描。为作业选择最多 100 台设备。

   您可以使用“**添加到作业**”和“**从作业中删除**”按钮创建设备列表。添加设备时，应用程序会打开一个窗口，其中包含可供选择的设备表。您可以过滤和排序表格以显示所需的设备。

2. 在“**选择设置**”部分中，执行以下操作：

   a. 选择执行作业时要接收的“设备类型”。

   b. 如果您选择了 **PLC** 设备类型，请在出现警告窗口时阅读主动轮询注意事项，并确认您接受使用主动轮询模块所带来的风险。

   c. 配置所选设备类型的设置。根据所选类型，您可以指定所需的配置类型（例如“**用户**”）或指定连接详细信息（例如连接器和用于远程连接的账户凭据 Secret，如果选择了 **PLC** 设备类型）。

   > 如果尚未将具有所需凭据的 Secret 添加到应用程序中，您可以在不关闭配置向导窗口的情况下在浏览器中打开新选项卡，连接到服务器并添加 Secret，然后使用配置向导窗口中的按钮刷新 Secret 列表。

3. 在“**作业配置**”部分，配置其余作业设置：

   a. 输入作业名称和说明。

   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`作业名称必须以任何允许的字符开头和结尾（空格除外）。

   作业名称不得超过 256 个字符作业描述不得超过 4096 个字符

   b. 选择配置处理模式。

   c. 如果在“**选择设置**”部分中选择了“**Windows 操作系统**”、“**Linux 操作系统**”或“**网络设备**”设备类型，请选择以下方法之一来轮询设备：

   - **本地代理**

     如果 Endpoint Agent 软件组件安装在为作业选择的设备上，并且 EPP 应用程序和 Kaspersky Industrial CyberSecurity for Networks 之间的集成已配置，则可以使用此方法。此方法用于在每台设备上使用 Endpoint Agent 进行扫描。

   - **远程连接**

如果为作业选择的设备没有安装 Endpoint Agent 软件组件，但可以通过确保安全管理和数据传输的协议连接到这些设备，请使用此方法。该方法支持获取“**Linux 操作系统**”和“**网络设备**”设备类型的配置。此方法需要以下附加数据：

- 安装了应用程序组件并用于连接设备的节点。
- 用于远程连接的账户凭据 Secret

  您只能为作业选择一个具有一组凭据的 Secret。存储在所选 Secret 中的凭据必须适用于为作业选择的所有设备：可以使用 Secret 中的相同凭据连接到这些设备。请记住，某些类型的系统数据（例如操作系统用户的密码）只有被具有足够高权限的用户请求时才能获取。要获取这些数据，您需要在 Secret 中指定具有适当权限级别的用户的凭据，例如具有 root 访问权限的用户或 /etc/sudoers 中列出的用户。

如果尚未将具有所需凭据的 Secret 添加到应用程序中，您可以在不关闭配置向导窗口的情况下在浏览器中打开新选项卡，连接到服务器并添加 Secret，然后使用配置向导窗口中的按钮刷新 Secret 列表。

d. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：

- 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
- 根据所选选项，指定设置值以定义精确的作业启动时间。

应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果计划作业应该开始运行时，该作业的先前运行状态仍为“*正在运行*”，则应用程序将跳过计划作业的启动。

4. 单击“**创建作业**”关闭向导。

指定的设置显示在**设置**和**设备**选项卡的作业详细信息区域中。

编辑配置控制作业

具有除操作员角色之外的任何角色的用户都可以编辑配置控制作业。

要编辑配置控制作业：

1. 选择“**安全审计**”部分。
2. 在“**配置控制**”选项卡上，选择要更改设置的作业。
3. 单击**编辑**。

   配置向导启动。配置向导设置的默认值被设置为所选作业设置的值。
4. 在“**作业配置**”部分，配置作业设置：

   a. 输入作业名称和说明。

   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`作业名称必须以任何允许的字符开头和结尾（空格除外）。

   作业名称不得超过 256 个字符作业描述不得超过 4096 个字符

b. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：

- 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
- 根据所选选项，指定设置值以定义精确的作业启动时间。

> 应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果计划作业应该开始运行时，该作业的先前运行状态仍为“*正在运行*”，则应用程序将跳过计划作业的启动。

5. 单击“**保存**”关闭向导。

指定的设置显示在**设置**和**设备**选项卡的作业详细信息区域中。

查看配置控制作业表

配置控制作业表显示在“**配置控制**”部分的“**安全审计**”选项卡上。

作业设置显示在表格的以下列中：

- **作业 ID**
  Kaspersky Industrial CyberSecurity for Networks 分配的作业 ID。
- **名称**
  用于在应用程序中代表作业的名称。
- **描述**
  作业描述。
- **创建日期**
  将作业添加到应用程序的日期和时间。
- **更改时间**
  应用程序中上次修改作业的日期和时间。
- **设备类型**
  为作业选择的设备类型的名称。
- **所选设备**
  为该作业选择的设备数量。
- **轮询方法**
  为设备扫描选择的轮询方法：**本地代理**、**远程连接**或**主动轮询连接器**。
- **计划**
  有关应用程序自动启动作业的计划的信息。
- **上次运行状态**
  上次运行作业时所有设备扫描的结果状态。

- **上次运行**

  作业上次启动的日期和时间。

- **下次运行**

  作业下次计划开始的日期和时间。

查看配置控制作业表时，您可以使用配置、过滤、搜索和排序功能，以及导航到相关项目。

手动启动和停止配置控制作业

您可以手动启动和停止配置控制作业。当您启动或停止一项作业时，应用程序将启动或停止为此作业选择的设备上的所有扫描。

您可以根据上次作业运行的状态停止或启动该作业。例如，如果作业上次运行的状态为“*正在运行*”，则无法启动该作业。

具有除操作员角色之外的任何角色的用户都可以手动启动和停止配置控制作业。

要启动配置控制作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。

3. 在“**配置控制**”选项卡上，选择要启动的作业。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**运行**。如果无法启动作业，则该按钮将被禁用。

Kaspersky Industrial CyberSecurity for Networks 启动作业。您可以在作业详细信息中的**运行**选项卡上查看正在进行的设备扫描的相关信息。

要停止配置控制作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。

3. 在“**配置控制**”选项卡上，选择要停止的作业。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击“**停止**。如果作业无法停止，则该按钮将被禁用。

查看有关配置控制作业运行的常规信息

您可以在作业表中查看有关配置控制作业运行的常规信息。该表显示有关最近的作业运行的信息，但不包括有关设备扫描的信息。要查看所有作业运行的一般信息（包括有关设备扫描的信息），请选择该作业，然后在详细信息区域中打开**运行**选项卡。

有关配置控制作业运行的常规信息包括以下内容：

- 作业开始状态。
  可使用以下状态：
  - “**新的**”或“**从不运行**”：已创建新的作业运行，但尚未运行任何扫描。
  - **等待发送**：扫描命令已准备好发送。
  - **正在运行**：作业正在开始。
  - **正在取消**：作业启动正在停止。
  - **已取消**：作业启动已停止。
  - **已完成**：所有扫描已成功完成。
  - **错误**：所有扫描均遇到错误。
  - **部分成功** – 作业已完成，但部分成功：某些扫描的状态为“**已完成**”，而某些扫描的状态为“**已取消**”或“**错误**”。
- 设备扫描状态。
  可使用以下状态：
  - **等待发送**：扫描命令已准备好发送。
  - **正在运行**：扫描正在进行中。
  - **正在取消**：扫描正在停止。
  - **已取消**：扫描已停止。
  - **已完成**：扫描已成功完成。
  - **错误**– 扫描期间发生错误。
- 启动日期和时间。
- 结束日期和时间。
- 执行持续时间。

分配黄金设备配置

应用程序在运行配置控制作业时存储每个设备捕获的配置。如果配置处理模式设置为“**与黄金配置进行比较**”，应用程序将把第一个加载的设备配置视为黄金。您可以将任何其他已保存的设备配置设置为黄金。

如有必要，您可以在分配黄金配置之前比较已保存的设备配置。

要设置黄金设备配置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**设备**”部分的“**资产**”选项卡上，选择相关设备。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 在“**配置**”选项卡的详细信息区域中，选择具有所需配置类型的表行，例如存储用户数据的“**用户**”。选定类型在“**配置总数**”列中的值必须至少为 2。

   您将看到一个窗口，其中包含有关所选配置类型的详细信息。

4. 在下拉列表中，选择接收要设置为黄金配置的配置的日期和时间。

   窗口将显示有关所选类型的已保存配置的详细信息。

5. 单击“**设置为黄金配置**”。

6. 在提示窗口中确认黄金配置的分配。

在配置控制作业中停止设备扫描

您可以手动停止作为配置控制作业的一部分的设备扫描。当设备扫描停止时，应用程序不会停止此作业中的其他设备扫描。

具有除操作员角色之外的任何角色的用户都可以手动停止设备扫描。

要在配置控制作业中停止设备扫描：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。

3. 在“**配置控制**”选项卡上，选择您想要停止设备扫描的作业。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 在详细信息区域中，转到**运行**选项卡。

5. 选择所需的扫描，然后单击出现的扫描详细信息区域中的**停止**。如果无法停止扫描，则该按钮将被禁用。

删除配置控制作业

您可以删除配置控制作业。但是，您不能删除上次运行状态为**正在运行**或**等待发送**的作业。

具有除操作员角色之外的任何角色的用户都可以删除配置控制作业。

要删除配置控制作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。

3. 在“**配置控制**”选项卡上，选择要删除的作业。

4. 单击**删除**。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认删除该作业。

   您只能删除上次运行状态不是“**正在运行**”或**等待发送**的作业。如果选定的作业中存在状态为**正在运行**或**等待发送**的作业，则会显示相应的消息。要删除此类作业，请先停止这些作业。

主动设备轮询作业

使用主动轮询作业，您可以直接从设备本身接收有关设备及其配置的准确完整信息，从而对受监控的设备进行安全审计。主动轮询使用连接器执行。要对设备进行主动轮询，必须向应用程序中添加一个或多个**主动轮询**连接器。

连接器提供了进行主动轮询的各种方法。可用的*主动轮询方法取*决于所使用的协议以及这些协议的命令和功能。应用程序的内置**主动轮询**连接器类型包含一组方法，这些方法支持通过应用层协议和通用协议进行主动轮询。Kaspersky Industrial CyberSecurity for Networks 支持以下方法来主动轮询设备：

- 通过 ARP 轮询（仅适用于内核版本 4.3 或更高版本的计算机）
- 通过 DNP3 轮询
- 获取进程控制设置和标签（仅适用于内核版本 4.3 或更高版本的计算机）
- 通过 IEC 61850: MMS 轮询
- 通过 Modbus TCP 轮询
- 通过 BECKHOFF ADS/AMS over UDP 轮询
- 通过 PROFINET DCP 轮询（仅适用于内核版本 4.3 或更高版本的计算机）
- 通过 Siemens S7comm over Industrial Ethernet 轮询
- 通过 Siemens S7comm over TCP 轮询

- 获取 Schneider Electric Modicon M340/M580 的扩展配置
- 获取 Siemens SIMATIC S7-300/S7-400 扩展配置
- 获取 Emerson DeltaV 扩展配置
- 获取 Rockwell Automation Allen-Bradley 扩展配置
- 通过 SMB 轮询
- 通过 SNMP 轮询
- 通过 SSH 轮询
- 通过 WinRM HTTP 轮询
- 通过 WinRM HTTPS 轮询
- 通过 WMI 轮询
- 通过 SSH 对 Cisco 设备的风险分析
- 通过 SSH 对 Linux 设备的风险分析

这些方法的区别在于它们获得的特定设备信息。您可以选择所需的相关信息以及配置主动轮询设置时要使用的方法。

一些方法使用 Secret 来连接设备。设备连接是使用添加到应用程序的 Secret 的凭证建立的。

使用这些方法时，应用程序可以根据主动轮询结果自动更新以下设备信息：

- 用于代表应用程序中的设备的名称。
- 用于表示网络中设备的名称（网络名称）。
- 设备硬件供应商的名称。
- 设备型号名称。
- 设备硬件版本号。
- 设备软件供应商的名称。
- 设备软件名称。
- 设备软件版本号。
- 设备的网络接口的地址信息。
- 设备上安装的操作系统的名称（仅适用于运行 Windows 和 Linux 操作系统的设备）。
- 过程控制设置和标记的配置。
- 工业设备的高级配置。

“附录”中提供了设备主动轮询应用程序支持的操作系统列表。

禁用自动更新的数据（显示 🔒），每当添加设备或更改设备详细信息时，不会自动更新。该应用程序还评估接收到的设备信息的真实性，并且在某些情况下可能拒绝先前接收到的信息的不可靠更新。

一些主动轮询方法支持检测风险和基于获得的设备信息对拓扑图进行更改的功能。

您可以手动运行安全审计作业，也可以配置计划以自动运行每个作业。具有除操作员角色之外的任何角色的用户都可以运行设备主动轮询作业。

要使用主动轮询功能，您需要考虑以下特殊注意事项和限制：

- 此功能在添加授权许可密钥后才可以使用。
- 用于对设备进行主动轮询的连接器的应用程序模块必须具有对设备的网络访问权限，以便它们可以发送请求并从设备接收数据。如果应用程序模块在安装了应用程序组件的节点上运行，为了确保对设备的网络访问，此计算机必须具有与这些设备的网络进行连接的网络接口。如果监控点的网络接口接收镜像的工业网络流量（例如，来自网络交换机的 SPAN 端口），则这些网络接口不能用于此目的。
- 主动轮询可能会导致设备出现一些不可预见的问题，因为这些设备可能会错误地解释传入的主动轮询命令。这些问题可能是由设备的不适当或高度专业化配置引起的。由于在设备之间的正常交互期间不明显的网络配置中的潜在错误，也可能出现问题。因此，主动轮询会对设备造成以下潜在影响风险：
  - 设备关闭
  - 与设备的连接丢失
  - 设备完全或部分故障
  - 运行速度比正常情况下慢
  - 网络和器材中的其他潜在故障

添加主动轮询作业

对于应用程序已知的设备，您可以添加活动轮询作业。

具有除操作员角色之外的任何角色的用户都可以添加主动轮询作业。添加授权许可密钥后，才可以添加主动轮询作业。

使用向导配置主动轮询作业。向导将指导您逐步完成所有必需作业设置的配置。配置完成后，您可以等待计划的扫描在设备上启动，也可以手动启动扫描作业。

添加活动轮询作业时，您可以通过以下方式调用配置向导：

- 添加具有空白设置的作业。为此：
  1. 选择“**安全审计**”部分。
  2. 在“**主动轮询**”选项卡上，单击“**添加作业**”。

  配置向导设置没有默认值。

- 为所选设备添加作业。为此：

  1. 选择“**资产**”部分。

  2. 在“**设备**”选项卡上，选择要为其添加主动轮询作业的设备。您可以选择不超过 100 台设备。

  3. 在设备表上方的工具栏中，打开“**创建作业**”下拉列表，然后选择“**主动轮询**”。

  在配置向导设置中，默认情况下会生成由所选设备组成的设备列表。

要在配置向导窗口中配置作业设置，请执行以下操作：

1. 阅读警告窗口中的主动轮询注意事项，并确认您接受使用主动轮询模块所带来的风险。

2. 在向导的“**选择设备**”部分，创建要执行主动轮询的设备列表。最多可选择 100 台设备。

   您可以使用“**添加到作业**”和“**从作业中删除**”按钮创建设备列表。添加设备时，应用程序会打开一个窗口，其中包含可供选择的设备表。您可以过滤和排序表格以显示所需的设备。

3. 在向导的“**选择设置**”部分，选中要使用主动轮询更新的特定设备信息的复选框。您还可以启用风险检测（“**风险**”复选框）和发现设备的拓扑设置（“**拓扑设置**”复选框。

4. 在向导的“**选择方法**”部分，执行以下操作：

   a. 选择一个主动轮询模块。

   b. 选中要用于获取设备信息、风险检测和/或读取拓扑设置的特定方法的复选框。

   根据提供设备主动轮询功能的连接器对可用方法进行分组。该列表仅包含能够获得所选信息的方法。如果连接器不能用于所选设备的主动轮询，则不会显示此连接器的可用方法（例如，如果连接器被禁用，或者如果为连接器选择了不包含所选设备地址的地址空间）。

   c. 根据需要配置每个连接器的方法。例如，对于“**通过 SSH 轮询**”，指定端口和凭证 Secret。

   > 如果尚未将具有所需凭据的 Secret 添加到应用程序中，您可以在不关闭配置向导窗口的情况下在浏览器中打开新选项卡，连接到服务器并添加 Secret，然后使用配置向导窗口中的按钮刷新 Secret 列表。

   需要配置设置的方法以红色突出显示。要更新设置，请单击所需方法右侧的 按钮。

5. 在向导的“**作业配置**”部分，配置其余作业设置：

   a. 输入作业名称和说明。

   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`作业名称必须以任何允许的字符开头和结尾（空格除外）。

   作业名称不得超过 256 个字符作业描述不得超过 4096 个字符

   b. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：

   - 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
   - 根据所选选项，指定设置值以定义精确的作业启动时间。

应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果在启动计划作业时，其上次启动的状态为“*正在运行*”，则应用程序将跳过计划作业的启动。

6. 单击“**创建作业**”或“**创建并运行**”关闭向导。

指定的设置显示在作业详细信息中。

编辑主动轮询作业

具有除操作员角色之外的任何角色的用户都可以编辑主动轮询作业。

要编辑主动轮询作业：

1. 选择“**安全审计**”部分。
2. 在“**主动轮询**”选项卡上，选择要更改其设置的作业。
3. 单击“**编辑**”。
   配置向导启动。配置向导设置的默认值被设置为所选作业设置的值。
4. 在向导的“**作业配置**”部分，配置其余作业设置：
   a. 输入作业名称和说明。
      您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`作业名称必须以任何允许的字符开头和结尾（空格除外）。
      作业名称不得超过 256 个字符作业描述不得超过 4096 个字符
   b. 要根据计划运行作业，请启用“**根据计划运行作业**”选项并配置计划设置：
      - 在“**频率**”下拉列表中，选择运行作业的频率：**每小时**、**每天**、**每周**或**每月**。
      - 根据所选选项，指定设置值以定义精确的作业启动时间。

   应用程序根据计划运行作业，前提是此作业的上一次运行已完成。如果计划作业应该开始运行时，该作业的先前运行状态仍为“*正在运行*”，则应用程序将跳过计划作业的启动。

5. 单击“**保存**”关闭向导。

指定的设置显示在作业详细信息中。

查看主动轮询作业表

主动轮询作业表显示在“**主动轮询**”部分的“**安全审计**”选项卡上。

作业设置显示在表格的以下列中：

- **作业 ID**
  Kaspersky Industrial CyberSecurity for Networks 分配的作业 ID。

- **名称**
  用于在应用程序中代表作业的名称。
- **描述**
  作业描述。
- **创建日期**
  将作业添加到应用程序的日期和时间。
- **更改时间**
  应用程序中最后修改的日期和时间。
- **所选设备**
  为该作业选择的设备数量。
- **计划**
  有关应用程序自动启动作业的计划的信息。
- **上次运行状态**
  上次运行作业时所有设备扫描的结果状态。
- **上次运行**
  作业上次启动的日期和时间。
- **下次运行**
  作业下次计划开始的日期和时间。

查看主动轮询作业表时，您可以使用配置、过滤、搜索和排序功能。

启动和停止主动轮询作业

您可以手动启动和停止主动轮询作业。当您启动或停止一项作业时，应用程序将启动或停止为此作业选择的设备上的所有扫描。

您可以根据上次作业运行的状态停止或启动该作业。例如，如果作业上次运行的状态为“*正在运行*”，则无法启动该作业。

具有除操作员角色之外的任何角色的用户都可以手动启动和停止主动轮询作业。

要启动主动轮询作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
   除操作员角色外，任何角色的用户都可以执行此操作。
2. 选择“**安全审计**”部分。
3. 在**主动轮询**选项卡上，选择要启动的作业。
   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**运行**。如果无法启动作业，则该按钮将被禁用。

   Kaspersky Industrial CyberSecurity for Networks 启动作业。您可以在作业详细信息中的**运行**选项卡上查看正在进行的设备扫描的相关信息。

要停止主动轮询作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**安全审计**”部分。

3. 在**主动轮询**选项卡上，选择要停止的作业。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击“**停止**。如果作业无法停止，则该按钮将被禁用。

查看有关主动轮询作业运行的一般信息

您可以在作业表中查看有关主动轮询作业运行的一般信息。该表显示有关最近运行的信息，但不包括有关设备扫描的信息。要查看所有作业运行的一般信息（包括有关设备扫描的信息），请选择该作业，然后在详细信息区域中打开**运行**选项卡。

有关主动轮询作业运行的一般信息包括以下内容：

- 作业状态或设备扫描状态。

  可使用以下状态：

  - **等待发送** – 尚未发送开始扫描的命令。
  - **正在运行** – 作业正在启动，或扫描正在进行中。
  - **正在取消** – 作业或扫描的启动正在停止。
  - **已取消** – 作业或扫描的启动已停止。
  - **已完成** – 扫描成功完成或作业运行中的所有扫描均已成功完成。
  - **错误** – 扫描期间发生错误或作业运行中的所有扫描都发生错误。
  - **部分成功** – 作业已完成，但部分成功：某些扫描的状态为“**已完成**”，而某些扫描的状态为“**已取消**”或“**错误**”。

- 启动日期和时间。
- 结束日期和时间。
- 执行持续时间。

查看有关主动轮询作业执行的报告

查看主动轮询作业运行的详细信息时，您可以查看包含设备扫描结果的报告。应用程序将为已完成的作业生成以下状态的报告：**已完成**、**部分成功**、**已取消**和**错误**。

报告中显示以下详细信息：

- 被扫描的设备的名称。
- 设备设置更新状态。
- 按更新状态分组的设备设置列表。
- 按执行状态分组的方法列表。如果在使用某种方法时发生错误，应用程序将显示其原因。

要查看有关主动轮询作业执行的报告：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**安全审计**”部分。
3. 在**主动轮询**选项卡上，选择要查看运行报告的作业。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 在详细信息区域中，转到**运行**选项卡并选择所需的作业运行。
   详细信息区域出现在 Web 界面窗口的右侧。详细信息区域显示有关所选作业运行的详细信息。

删除主动轮询作业

您可以删除主动轮询作业。但是，您不能删除上次运行状态为**正在运行**或**等待发送**的作业。

具有除操作员角色之外的任何角色的用户都可以删除主动轮询作业。

要删除主动轮询作业：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
   除操作员角色外，任何角色的用户都可以执行此操作。
2. 选择“**安全审计**”部分。
3. 在**主动轮询**选项卡上，选择要删除的作业。
4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，确认删除该作业。
   您只能删除上次运行状态不是“**正在运行**”或**等待发送**的作业。如果选定的作业中存在状态为**正在运行**或**等待发送**的作业，则会显示相应的消息。要删除此类作业，请先停止这些作业。

形成拓扑图

拓扑图是工业网络中设备之间物理连接的可视化表示。与网络交互图相反，拓扑图旨在显示设备之间通过连接到网络接口端口的网络电缆的实际连接。生成拓扑图后，您将看到一个或多个图形，这些图形通过交换机、集线器、路由器等网络设备直观地显示设备之间的连接结构。

以下对象可能会显示在拓扑图上：

- 节点。这些对象表示设备和网络设备。
- 链接。这些对象表示节点之间的物理连接。

无论这些节点是否与其他节点连接，节点都会不断显示在拓扑图上。可以对节点进行过滤，以便更方便地显示。根据节点的类型、状态和与节点相关的事件，节点在拓扑图上也以各种方式进行区分。

为节点添加链接后，您可以根据拓扑生成过程在拓扑图上排列这些节点。

拓扑图显示在“**网络地图**”部分的“**拓扑图**”选项卡上。

如果使用了相应的轮询方法（例如，通过 SNMP 进行轮询），则可以根据设备的主动轮询结果自动获得用于向拓扑图添加连接的数据。您也可以手动添加连接。

拓扑图上的节点

拓扑图上的节点可以是以下类型：

- 应用程序已知的设备。这种类型的节点代表设备表中列出的设备。
- 不受管理的交换机。这种类型的节点代表 MAC 地址和 IP 地址不可用或未知的设备。由于缺少地址信息，该设备无法添加到设备表中。然而，这样的设备仍然可以链接到其他设备。例如，如果主动轮询检测到不同设备到同一设备的一个端口的多个连接，则这种类型的节点可能会出现在拓扑图上。如果是这种情况，应用程序将确定网络中存在未识别的交换设备（例如集线器），并自动为该设备创建节点。不能向应用程序添加超过 1000 个不受管理的交换机。

  如果您能够识别不受管理的交换机节点的 MAC 和/或 IP 地址，则可以使用此不受管理的交换机节点手动添加新设备到设备表中。

显示的代表设备的节点信息

当拓扑图比例最大化时，代表已知设备的节点将显示以下信息：

- 分配的设备名称。
- 设备类别图标。
- 设备的网络名称或地址（如果未分配 IP 地址，则显示 MAC 地址）。

- 各种图标取决于对以下条件的满足：
  - 如果设备设置了路由器指示灯。
  - 如果设备上安装了 EPP 应用程序（图标的颜色取决于连接状态）。
  - 如果设备具有“*已存档*”状态。
- 根据设备的安全状态，节点左边框上的粗线具有以下颜色之一：
  - 绿色表示“*正常*”安全状态。
  - 黄色表示“*警告*”安全状态。
  - 红色表示“*严重*”安全状态。

如果设备具有“*未授权*”状态，则该节点具有红色背景。

显示的代表不受管理的交换机的节点的信息

当拓扑图比例最大化时，代表不受管理的交换机的节点将显示以下信息：

- 定义的节点名称。
- 不受管理的交换机图标。

代表不受管理的交换机的节点具有灰色背景。

拓扑图上的链接

拓扑图上的链接显示了节点之间的物理连接。每个链接代表通过网线连接的设备上的网络接口端口之间的连接。

链接在拓扑图上显示为水平线或垂直线。从地图共享部分上的一个节点延伸的多条链接线显示为表示网络总线的粗线。

查看拓扑图上对象的详细信息

有关拓扑图上显示的对象的详细信息显示在详细信息区域中。要显示详细信息，可以通过单击对象来选择对象。

将显示所选节点的以下信息：

- 如果节点表示已知设备，则详细信息区域显示与在设备表中选择设备时显示的信息相同的信息。
- 如果节点表示不受管理的交换机，则详细信息区域将显示以下信息：
  - 不受管理的交换机节点的名称
  - 节点类型（不受管理的交换机）
  - "**拓扑设置**"部分包含已添加或可能添加与其他节点的链接的端口列表

将为所选连接显示其中一个链接节点的名称以及该节点与其他节点连接的端口列表。如果选择了总线，您将看到在所选总线中具有最高链路数的节点的端口列表。

将节点添加到拓扑图

生成拓扑图时，应用程序可以自动将检测到的节点添加到拓扑图中。如果应用程序未自动添加某些相关节点，您可以在使用拓扑图时手动添加它们。

具有除操作员角色之外的任何角色的用户都可以手动添加节点。

如果您知道要作为节点添加到拓扑图的设备的 MAC 和/或 IP 地址，则可以手动添加该设备。如果节点的地址信息未知或丢失（例如，如果设备是集线器），您可以添加不受管理的交换机节点。

要添加不受管理的交换机到拓扑图中：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在"**网络地图**"部分中的"**拓扑图**"选项卡上，选择"**添加节点**"下拉列表中的"**新建不受管理的交换机**"。

   窗口右侧会显示包含不受管理的交换机设置的详细信息区域。

3. 输入节点名称。

   节点名称必须是唯一的（不得与其他不受管理的交换机的名称匹配）并且包含的字符不得超过 100 个。您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`。节点名称必须以任何允许的字符开头和结尾（空格除外）。

4. 单击**保存**。

不受管理的交换机节点将出现在拓扑图上。然后您将能够添加此节点与其他节点的链接。

手动将链接添加到拓扑图

本节提供有关向拓扑图添加链接的说明。使用设备表或拓扑图时，您可以手动添加链接并配置其设置。

具有除操作员角色之外的任何角色的用户都可以添加连接并配置其设置。

为选定节点添加链接并配置附加拓扑设置

如果要为一个节点添加与其他节点的多个链接（例如，为交换机添加所有链接），则此功能非常方便。使用此方法添加链接时，还可以配置设备的所有拓扑设置。

要为节点添加链接并配置附加拓扑设置，请执行以下操作：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络地图**”部分的“**拓扑图**”选项卡上选择节点。

   您还可以在“**网络交互图**”选项卡或“**设备**”部分的“**资产**”选项卡上选择相关节点代表的设备。但是，在这些选项卡上，您将无法选择不受管理的交换机节点。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 在详细信息区域的右上角，单击 ⋮ 图标并选择“**拓扑设置**” → “**配置设置**”。

   将显示配置所选节点的端口和连接的窗口。

4. 在“**物理端口**”设置组中，添加有关与其他节点的链接的信息。有关每个链接的信息必须在单独的行中提供，您可以在其中指定以下设置：

   - 网线连接的物理端口名称（可选设置）
   - VLAN ID（可选设置）
   - 端口连接的网络接口地址（可选设置）
   - 将充当连接第二端的节点（要选择节点，您将看到一个窗口，其中包含可用节点和节点上的端口的表）

5. 如有必要，请在“**虚拟端口**”设置组中提供有关设备虚拟端口的信息。

   有关虚拟端口的信息不用于生成拓扑图。

6. 单击“**保存**”。

添加所选节点的链接而不配置附加拓扑设置

如果您想为多个节点添加与一个节点的链接（例如，为每个选定节点添加与交换机的链接），则此功能非常方便。使用此方法添加链接时，这些链接的附加设置将保持未定义状态。例如，您无法在节点上为要添加的连接选择端口。编辑节点的拓扑设置时，您可以在添加链接后配置链接的附加设置。

如果选择的规则不超过 50 个，则可以添加链接。

要添加节点的链接而不配置附加链接设置，请执行以下操作：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络地图**”部分的“**拓扑图**”选项卡上选择一个或更多节点。

   要选择多个节点，请执行以下操作之一：

   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。

   您还可以在“**网络交互图**”选项卡或“**设备**”部分的“**资产**”选项卡上选择由相关节点表示的设备。但是，在这些选项卡上，您将无法选择不受管理的交换机节点。

3. 右键单击以打开上下文菜单。

4. 在上下文菜单中，选择“**添加与节点的连接**”。

   您将看到一个窗口，其中包含可供选择的节点表。

5. 在表中选择相关节点，然后单击“**确定**”。

编辑节点的拓扑设置

编辑拓扑设置时，您可以添加、配置和删除节点的链路，以及配置虚拟节点的设置。

具有除操作员角色之外的任何角色的用户都可以编辑拓扑设置。

配置节点的拓扑设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络地图**”部分的“**拓扑图**”选项卡上选择节点。

   您还可以在“**网络交互图**”选项卡或“**设备**”部分的“**资产**”选项卡上选择相关节点代表的设备。但是，在这些选项卡上，您将无法选择不受管理的交换机节点。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 在详细信息区域的右上角，单击**⋮**图标并选择“**拓扑设置**” → “**配置设置**”。

   将显示配置所选节点的端口和连接的窗口。

4. 在“**物理端口**”设置组中，提供有关与其他节点的链接的信息。有关每个链接的信息必须在单独的行中提供，您可以在其中指定以下设置：

   - 网线连接的物理端口名称（可选设置）
   - VLAN ID（可选设置）
   - 端口连接的网络接口地址（可选设置）
   - 将充当连接第二端的节点（要选择节点，您将看到一个窗口，其中包含可用节点和节点上的端口的表）

5. 如有必要，请在“**虚拟端口**”设置组中提供有关设备虚拟端口的信息。

   有关虚拟端口的信息不用于生成拓扑图。

6. 单击“**保存**”。

重命名不受管理的交换机的节点

您可以重命名自动或手动添加到拓扑图中的不受管理的交换机节点。

具有除操作员角色之外的任何角色的用户都可以重命名非托管交换机节点。

要重命名拓扑图上的不受管理的交换机节点，请执行以下操作：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络地图**”部分的“**拓扑图**”选项卡上，选择不受管理的交换机节点。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 单击**编辑**。

4. 在包含节点当前名称的字段中，输入新名称。

   节点名称必须是唯一的（不得与其他不受管理的交换机的名称匹配）并且包含的字符不得超过 100 个。您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`。节点名称必须以任何允许的字符开头和结尾（空格除外）。

5. 单击**保存**。

从拓扑图中删除对象

使用拓扑图时，可以删除节点和连接。当表示已知设备的节点被删除时，这些设备将被从设备表中删除。

具有除操作员角色之外的任何角色的用户都可以从拓扑图中删除对象。

要删除节点，请执行以下操作：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络地图**”部分的“**拓扑图**”选项卡上，选择要删除的节点。

   详细信息区域出现在 Web 界面窗口的右侧。

3. 单击**删除**。

   将打开一个带有确认提示的窗口。

4. 在提示窗口中，确认删除所选节点。

要删除链接或总线（多个链接）：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在“**网络地图**”部分的“**拓扑图**”选项卡上，选择链接或总线。

3. 单击**删除**。

   将打开一个带有确认提示的窗口。

4. 在提示窗口中，确认删除所选链接。

更改拓扑图比例

拓扑图可以按 1–100% 的比例显示。当前比例值显示在位于拓扑图显示区域左侧的工具栏中。

要更改拓扑图的比例，请执行以下操作：

使用鼠标滚轮或位于当前比例值旁边工具栏中的 **+** 和 **–** 按钮。

减小地图的比例会减少节点中显示的信息量。

如果显示比例小于 25%，则不会在节点中显示图标和文本信息。使用这种缩小的比例，在表示已知设备的每个节点上，右上角以以下颜色之一的三角形显示设备状态：

- 绿色表示设备处于“*已授权*”状态。
- 红色表示设备处于“*未授权*”状态。
- 灰色表示设备处于“*已存档*”状态。

拓扑图的定位

如有必要，您可以手动或自动更改拓扑图的位置。自动定位允许您移动地图并更改其比例，以显示满足定义的过滤器设置的所有节点。

要手动定位拓扑图：

1. 将鼠标光标放置在拓扑图上未被对象占据的任何部分上。
2. 单击并按住鼠标左键拖动拓扑图图像。

要自动定位拓扑图：

点击拓扑图显示区域左侧工具栏中的 按钮。

地图的位置和比例将更改以显示所有节点。

在拓扑图上固定和取消固定节点

默认情况下，节点未固定在网络地图上。未固定的节点可以自动排列，以实现其他对象的最佳显示。

当手动更改节点位置时，节点将被固定。您还可以固定显示对象的当前位置而不移动它们。

要固定和取消固定对象而不移动它们，可以使用位于拓扑图显示区域左侧的工具栏中的按钮。您可以使用 和 按钮以固定和取消固定拓扑图上显示的所有节点。如果拓扑图包含可以应用相应操作的对象，则这些按钮可用。

固定节点位置后， 图标出现在该元素的右上角（如果拓扑图的比例小于 25%）。您还可以使用此图标取消固定对象。

保留固定节点的位置。如果固定节点从拓扑图中消失（例如，应用过滤器后），则该节点下次出现时将显示在同一位置（或附近，如果该位置已被另一个固定节点占用）。

手动更改拓扑图上节点的位置

您可以使用最方便的排列方法手动更改拓扑图上节点的位置。

排列完成后，节点将固定在新位置。如有必要，您可以取消固定这些对象。

要更改拓扑图上节点的位置：

1. 在拓扑图上选择一个或多个节点。

   要选择多个节点，请执行以下操作之一：

   - 按住**SHIFT**键并使用鼠标选择包含相关对象的矩形区域。
   - 按住**CTRL**键并使用鼠标选择相关对象。

2. 使用鼠标将选定的对象拖动到所需的位置。

   移动后，节点仍保持固定状态。 图标出现在这些对象中。

自动在拓扑图上排列节点

为了在拓扑图上实现对象的最佳排列，您可以使用算法自动更改节点的位置（自动排列）。该算法允许您根据拓扑层次结构排列与其他节点有链接的未固定节点。

要在拓扑图上排列节点：

点击拓扑图显示区域左侧工具栏中的 按钮。

自动排列后，未固定的节点将不会固定在新位置。如有必要，您可以手动固定这些对象。

过滤拓扑图上的对象

要限制拓扑图上显示的节点数，您可以使用下面描述的功能：

按设备状态过滤

要按设备状态过滤拓扑图上的对象：

1. 在拓扑图上方的工具栏中，打开“**设备状态**”下拉列表。
   您将看到一个列表，其中包含已知设备的状态名称（“*未授权*”、“*已授权*”和“*已存档*”）以及不受管理的交换机的“*不受管理的交换机*”状态。
2. 在下拉列表中，选中需要在拓扑图上显示的设备状态的复选框。
3. 单击**确定**。

拓扑图将仅显示具有选定状态的节点。

按设备安全状态过滤

要按设备安全状态过滤拓扑图上的对象：

1. 在拓扑图上方的工具栏中，打开“**设备状态**”下拉列表。
   您将看到一个列表，其中包含设备的安全状态名称（“*正常*”、“*警告*”和“*严重*”）。
2. 在下拉列表中，选中需要在拓扑图上显示的设备的安全状态的复选框。
3. 单击**确定**。

拓扑图将仅显示那些表示具有选定安全状态的设备的节点。

按设备类别过滤

要按设备类别过滤拓扑图上的对象：

1. 在拓扑图上方的工具栏中，打开“**设备类别**”下拉列表。
   您将看到一个列表，其中包含已知设备的类别名称，以及不受管理的交换机的单个类别。

2. 在下拉列表中，选中需要在拓扑图上显示的设备类别的复选框。

3. 单击**确定**。

拓扑图将仅显示表示所选设备类别的那些节点。

在拓扑设置中按 VLAN ID 进行过滤

要按拓扑设置中的 VLAN ID 过滤拓扑图上的对象：

1. 在拓扑图上方的工具栏中，打开“**VLAN ID**”下拉列表。
   您将看到一个窗口，其中包含一个用于输入 VLAN ID 的字段。

2. 输入需要在拓扑图上显示的设备的一个或多个 VLAN ID。
   可以指定多个用逗号分隔的标识符，也可以指定为一个范围（例如：`1、2、4-6、8`）。

3. 单击**确定**。

拓扑图将仅显示那些拓扑设置包括具有定义的 VLAN ID 的端口的节点。

启用和禁用不具有到其他节点的链接的节点的显示

默认情况下，拓扑图显示所有节点，而不管这些节点是否具有到其他节点的链接。如有必要，可以禁用显示与拓扑图上其他节点没有链接的所有节点。

要启用或禁用未链接到其他节点的节点的显示，请执行以下操作：

使用位于拓扑图上方的工具栏中的“**显示未链接的节点**”切换开关。

重置过滤器设置

可以将定义的节点过滤设置重置为默认状态。

要重置拓扑图上定义的过滤器设置，请执行以下操作：

在拓扑图上方的工具栏中，单击“**默认过滤器**”（如果已定义过滤器设置，则会显示此按钮）。

保存和加载拓扑图显示设置

本节介绍拓扑图显示自定义功能。

该应用程序允许您保存当前的拓扑图显示设置。一组保存的显示设置称为*视图*。您可以使用视图在拓扑图上应用其保存的设置（例如，在进行某些更改后快速恢复显示设置，或在不同计算机上使用拓扑图）。

保存拓扑图视图时，会保存以下显示设置：

- 缩放比例
- 拓扑图的定位
- 固定节点的位置
- 节点过滤

应用程序可以保存和使用不超过 10 组提供不同拓扑图视图的设置。

所有用户都可以管理拓扑图视图列表（包括保存当前显示设置）。

添加新视图，同时保存当前拓扑图显示设置

要在保存当前拓扑图显示设置的同时添加新视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**网络地图**”部分的“**拓扑图**”选项卡上，配置拓扑图显示设置。
3. 单击“**管理视图**”打开“**配置网络地图视图**”窗口。
4. 单击“**添加**”。
5. 在输入字段中输入视图名称。
   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`。
   视图名称必须满足以下要求：
   - 必须以空格以外的任何允许的字符开始和结束。
   - 必须包含 100 个字符或更少。
   - 不得与不同视图的名称匹配（不区分大小写）。
6. 点击输入字段右侧的 ✓ 图标。

在保存当前拓扑图显示设置的同时更新视图

要在保存当前拓扑图显示设置的同时更新视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**网络地图**”部分的“**拓扑图**”选项卡上，配置拓扑图显示设置。
3. 单击“**管理视图**”打开“**配置网络地图视图**”窗口。
4. 选择要保存当前拓扑图显示设置的视图。

5. 单击“**覆盖**”。
   将打开一个带有确认提示的窗口。
6. 在提示窗口中，确认您要保存所选视图中的当前设置。

重命名拓扑图视图

要重命名拓扑图视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**拓扑图**”部分中的“**网络地图**”选项卡上，通过单击“**管理视图**”按钮打开“**配置网络地图视图**”窗口。
3. 选择要重命名的视图。
4. 点击当前视图名称右侧的 图标。
5. 在输入字段中，输入视图的新名称。
   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`
   视图名称必须满足以下要求：
   - 必须以空格以外的任何允许的字符开始和结束。
   - 必须包含 100 个字符或更少。
   - 不得与不同视图的名称匹配（不区分大小写）。
6. 点击输入字段右侧的 图标。

删除拓扑图视图

要删除拓扑图视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**拓扑图**”部分中的“**网络地图**”选项卡上，通过单击“**管理视图**”打开“**配置网络地图视图**”窗口。
3. 选择要删除的视图。
4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，确认删除所选视图。

在拓扑图上应用保存的视图设置

要在拓扑图上应用保存的视图设置：

1. 在“**拓扑图**”部分中的“**网络地图**”选项卡上，通过单击“**管理视图**”按钮打开“**配置网络地图视图**”窗口。
2. 在列表中选择相关视图。
3. 单击“**应用**”。
   将打开一个带有确认提示的窗口。
4. 在提示窗口中，确认视图的应用。

搜索拓扑图上的节点

您可以根据有关这些节点的信息在拓扑图上搜索这些节点。此搜索将涉及符合当前过滤器设置的所有节点，包括位于拓扑图显示部分之外的节点。

对于表示已知设备的节点，将在设备表的所有列中执行搜索，但“**状态**”、“**安全状态**”、**最后可见日期**”、“**最后修改日期**”和“**创建日期**”除外。搜索也在设备的自定义字段的值中执行。

要在拓扑图上查找相关节点，请执行以下操作：

在“**网络地图**”部分的“**拓扑图**”选项卡上，在“**搜索节点**”字段中输入搜索查询。当您在搜索字段中键入字符时，将启动搜索。

如果找到满足搜索查询的节点，这些节点的轮廓将以黄色突出显示。同时，“**搜索节点**”字段的右侧将显示以下项目：

- 搜索结果中当前所选节点的序列号。
- 找到的节点总数。
- 用于在找到的节点之间移动的箭头。箭头移动按找到的对象名称的字母顺序进行。当移动到下一个节点时，拓扑图会自动定位以显示此节点。

配置事件类型

*事件类型*定义注册事件时使用的设置，包括其标题、描述、基本分数和注册设置。在 Kaspersky Industrial CyberSecurity for Networks 中，您可以查看事件类型的设置、更改事件类型的设置以及配置自动保存流量和通过连接器传输已注册事件。

查看事件类型表

应用程序中提供的事件类型显示在应用程序 Web 界面的"**设置**"→"**事件类型**"下。

事件类型表包含*系统事件类型*。这些事件类型是由应用程序在安装过程中创建的，不能从列表中删除。各种系统事件类型集合用于应用程序中采用的事件注册技术。

某些系统事件类型可以用作配置*用户定义的事件设置*的基础，这些设置将在特定情况下注册事件时使用。可以为以下事件类型定义用户定义的设置：

- 基于深度数据包检测技术的事件类型，代码为 4000002900，用于根据"过程控制"规则注册事件。
- 基于外部技术的事件类型，代码为 4000005400，用于 Kaspersky Industrial CyberSecurity for Networks API 注册事件。

注册事件时，用户定义的设置优先。如果没有用户定义的设置，则使用系统事件类型中定义的设置。

以下设置可用于事件类型：

- **代码** – 事件类型的唯一编号（标识符）。在事件类型表中，编号与事件标题一起显示在"**标题模板**"列中。在已注册事件表中，事件类型标识符显示在"**事件类型**"列中。
- **标题** – 以文本和/或变量形式呈现的事件标题的内容。系统事件类型仅可以针对这些事件类型使用特定变量（例如，"命令控制"技术的事件类型中的 $systemCommandShort 变量），或者是也可以在用户定义的设置中使用的通用变量（例如"网络完整性控制"技术的事件类型中的 $top_level_protocol 变量）。在事件类型表中，标题的内容与事件类型编号一起显示在"**标题模板**"列中。在已注册事件表中，标题文本和/或接收到的变量值显示在"**标题**"列中。
- **基本分数** – 用于计算注册事件的分数的初始值。如果一个事件类型可以有不同的基本分数，则会显示最大值。此设置显示在事件类型表中。
- **技术** – 用于事件注册的技术。此设置显示在事件类型表中。
- **描述** – 描述事件类型的附加文本。与标题一样，描述可能包含变量。此设置不显示在事件类型表中（您可以在所选事件类型的详细信息区域中查看描述）。在已注册事件表中，描述文本和/或接收到的变量值显示在"**描述**"列中。
- **<收件人连接器名称>** – 应用程序用于将事件转发到收件人系统的连接器的名称。应用程序仅向收件人系统发送配置为通过连接器转发的那些类型的事件。配置为将事件转发到第三方系统的每个连接器都显示在风险类型表的单独列中。此设置不会显示在所选事件类型的详细信息区域中。
- **事件再生周期** – 允许再次注册事件的最长时间间隔。如果在指定的时间段过去之前重复事件注册的条件，则不注册新的事件，但是会增加先前注册的事件的重复次数的计数器，并且会更新事件最后发生的日期和时间。经过这段时间后，当重复事件注册条件时，应用程序将注册此类型的新事件。重复事件超时期从上次注册此类型的事件时开始。例如，如果定义的时间段为 8 小时，并且在前一事件发生两小时后检测到注册此类事件的条件，则不会注册新事件。当在 8 小时或更长时间后检测到事件注册条件时，将注册新事件。此设置不显示在事件类型表中（您可以在所选事件类型的详细信息区域中查看和配置此设置）。

  对于已注册的事件，事件重新生成周期可能早于指定的周期。如果将"*已解决*"状态分配给事件，并且执行服务器功能的计算机已重新启动，则允许在定义的时间段之前重新注册事件。

- **节省流量** – 此设置启用或禁用在注册事件时自动保存流量。此设置不显示在事件类型表中（您可以在所选事件类型的详细信息区域中查看和配置此设置）。

  如果禁用了流量的自动保存，则可以在注册此类事件后一段时间手动加载流量。当应用程序收到加载流量的请求时，它会在应用程序临时创建的流量转储文件中搜索网络数据包。如果在流量转储文件中找到相关的网络数据包，则在将其首次保存到数据库中后加载这些数据包。

查看事件类型表时，您可以使用配置、过滤、搜索和排序功能。

编辑系统事件类型的设置

要编辑系统事件类型的设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置→事件类型**。
3. 在事件类型表中，选择要编辑的事件类型。

   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
5. 配置可编辑的设置，例如事件再生周期和流量节省设置。
6. 单击**保存**。

配置自动保存系统事件类型的流量

当编辑事件类型时，您可以启用或禁用注册事件时自动保存流量的功能。如果启用了流量保存，则导致事件注册的网络数据包、以及在事件注册之前和之后接收的数据包以及在注册事件的网络会话中检测到的数据包将被保存到数据库中。流量保存设置决定了保存的网络数据包数量和时间限制。

如果某种事件类型的流量自动保存功能被禁用（并且该事件类型未定义启用流量自动保存的用户定义设置），则您只有在注册该类型的事件后等待一段时间才能手动加载流量。在这种情况下，应用程序使用流量转储文件来加载流量（这些文件临时保存，随着收到越来越多的流量会被自动删除）。从这些文件加载流量时，数据库会保存在启用事件类型的流量保存时默认定义的特定数量的网络数据包。

仅当注册事件时，应用程序才会在数据库中保存流量。如果在事件重新生成超时期间重复注册此事件的条件，则此时间点的流量不会保存在数据库中。

您可以启用和配置任何事件类型的流量保存，除了被分配代码 4000002700 的系统事件类型之外。当监控点没有流量时，会注册代码为 4000002700 的事件。因此，预计此类事件不会有流量。

如果为突发事件启用了流量保存（即对于分配了代码 8000000001 的系统事件类型），则应用程序会在注册突发事件时保存该突发事件的所有嵌入事件的流量。当保存嵌入式事件的流量时，将应用为突发事件定义的设置。不过，直接为突发事件中嵌入的事件类型定义的流量存储设置优先于为突发事件定义的设置。这意味着突发事件的嵌入式事件的流量将根据为这些事件的特定类型定义的设置进行保存。如果未定义这些设置，则嵌入式事件的流量将根据为突发事件定义的设置进行保存。

要启用并配置保存事件类型的流量的设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置→事件类型**。
3. 在事件类型表中，选择要编辑的事件类型。
   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
5. 将**节省流量**切换开关设置为*已启用*。
6. 配置在注册事件前保存流量。为此，请在**事件之前的数据包总数**和/或**距离事件之前的时间(毫秒)**中指定相关值。如果该值为零，则不应用设置。如果这两个字段都定义了值，则应用程序将保存与其中一个定义值相对应的最小数量的数据包。
7. 配置在注册事件后保存流量。为此，请在**事件之后的数据包总数**和/或**距离事件之后的时间(毫秒)**中指定相关值。如果该值为零，则不应用设置。如果这两个字段都定义了值，则应用程序将保存与其中一个定义值相对应的最小数量的数据包。

   对于某些技术（特别是深度包检测），事件中保存的注册后数据包数量可能会少于保存流量设置所定义的数量。这源于流量监控的技术特性。

8. 单击**保存**。

配置通过连接器转发事件

当配置系统事件类型时，您可以指定 Kaspersky Industrial CyberSecurity for Networks 将通过其将已注册事件转发到接收系统（例如，Kaspersky Security Center）的连接器。Kaspersky Industrial CyberSecurity for Networks 可同时通过多个连接器中继事件信息。

要配置通过连接器将事件转发到接收系统：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置→事件类型**。
3. 确保事件类型表显示带有相关连接器的列。
   如果没有具有所需连接器的列，请检查列显示设置。如果连接器尚未被添加到连接器列表中，请添加它。
4. 在事件类型表中，选择您想要启用或禁用通过连接器转发的事件类型。
   如果您选择一种事件类型，详细信息区域将显示在 Web 界面窗口的右侧。
5. 执行以下操作之一：
   - 如果选择一种事件类型，请单击详细信息区域中的**选择连接器**。
   - 如果选择多种事件类型，请单击窗口上部的**选择连接器**。

   事件收件人连接器窗口将打开。

6. 选择要用于将事件转发到接收系统的连接器旁边的复选框。如果要禁用通过连接器转发事件，请清除该连接器旁边的复选框。

7. 单击“**确定**”。

   在事件类型表中，复选框会显示在已选择用于转发事件的连接器的列单元格中。

Kaspersky Industrial CyberSecurity for Networks 中用于替换值的常用变量

您可以使用通用值来替代 Kaspersky Industrial CyberSecurity for Networks 中的当前值。您可以在以下设置中使用常用变量：

- 用于注册事件（例如，在过程控制规则中）的用户定义设置中的事件标题和描述。
- 通过电子邮件连接器转发事件、应用程序消息或审计条目的设置。

要将常用变量插入到条目字段中：

开始输入以 $ 字符开头的变量名称，然后在出现的列表中选择适当的常用变量。

根据其目的，可以使用常用变量来替换各种设置中的值（见下表）。

用于替换值的常用变量

变量	目的	使用地方
`$closed`	分配*已解决*状态时的日期和时间或事件重新生成期间的日期和时间（对于非突发事件的事件），或事件中包含的最后一个事件的注册日期和时间（对于突发事件）。	• 通过连接器转发事件的设置。
`$communications`	描述网络交互的字符串（每个网络交互一行），指示网络数据包源和目标的协议和地址。	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。
`$count`	事件或事故被触发的次数。	• 通过连接器转发事件的设置。
`$description`	描述	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$dst_address`	网络数据包目的地的地址（取决于协议中可用的数据，可以是 IP 地址、端口号、MAC 地址和/或其他地址数据）。	• 用于注册事件的用户定义的设置。
`$extra.<paramName>`	使用`AddEventParam`函数为外部系统或Lua 脚本添加的附加变量，或由网络异常检测规则的`SQL 查询`中的SELECT生成的变量。	• 用于注册事件的用户定义的设置。
`$id`	已注册事件、应用程序消息或审计条目的唯一 ID。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$message_category`	已传输数据的类别（事件、应用程序消息或审计条目）。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$message_count`	传输的事件、应用程序消息或审计条目的数量。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$messages`	由包含数据列表的块组成的模板。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$monitoring_point`	其流量触发了事件注册的监控点的名称。	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。
`$msg_line_templ`	电子邮件通知字符串模板	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$node`	包含发送数据的已安装应用程序组件的节点。	• 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$occurred`	注册的日期和时间。	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$protocol`	注册事件时正在被监控的应用程序层协议的名称。	• 用于注册事件的用户定义的设置。
`$result`	审计条目中的操作结果。	• 通过连接器转发审计条目的设置。
`$rule_description`	网络异常检测规则描述	• 用于注册事件的用户定义的设置。
`$rule_max_value`	在过程控制规则中分配的最大值。	• 用于注册事件的用户定义的设置。
`$rule_min_value`	在过程控制规则中分配的最小值。	• 用于注册事件的用户定义的设置。
`$rule_name`	网络异常检测规则名称	• 用于注册事件的用户定义的设置。
`$rule_values`	过程控制规则的值列表（已授权或未授权）。	• 用于注册事件的用户定义的设置。
`$scanned_interval`	分析网络会话的时间间隔	• 用于注册事件的用户定义的设置。
`$score`	事件分数值。	• 通过连接器转发事件的设置。
`$severity`	事件严重性级别。	• 通过连接器转发事件的设置。

`$src_address`	网络数据包源的地址（取决于协议中可用的数据，可以是 IP 地址、端口号、MAC 地址和/或其他地址数据）。	• 用于注册事件的用户定义的设置。
`$status`	应用程序消息状态。	• 通过连接器转发应用程序消息的设置。
`$system_process`	触发了消息注册的应用程序进程。	• 通过连接器转发应用程序消息的设置。
`$tags`	过程控制规则中指示的所有标记名称和值的列表。	• 用于注册事件的用户定义的设置。
`$technology`	与事件相关的技术。	• 通过连接器转发事件的设置。
`$technology_rule`	事件中规则的名称。	• 用于注册事件的用户定义的设置。 • 通过连接器转发事件的设置。
`$template_name`	网络异常检测规则中的模板名称	• 用于注册事件的用户定义的设置。
`$title`	事件标题、消息文本或已注册的操作。	• 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$top_level_protocol`	顶级协议的名称。	• 用于注册事件的用户定义的设置。
`$type_id`	事件类型、应用程序消息或审计条目的代码。	• 用于注册事件的用户定义设置（也可以使用 `$event_type_id` 变量）。 • 通过连接器转发事件的设置。 • 通过连接器转发应用程序消息的设置。 • 通过连接器转发审计条目的设置。
`$user`	执行注册的操作的用户的名称。	• 通过连接器转发审计条目的设置。

配置风险类型

*风险类型*定义在 Kaspersky Industrial CyberSecurity for Networks 中注册风险时使用的设置：风险的名称、类别和基本分数。您可以查看风险类型的设置，并根据需要编辑某些风险类型的基本分数值。

安装应用程序后，将使用原始风险类型列表。您可以通过安装更新来更新和扩展支持的风险类型。

查看风险类型表

风险类型表显示在应用程序 Web 界面的“**设置**” → “**风险类型**”下。

风险类型的设置显示在表的以下列中：

- **代码**

  风险类型的唯一编号。在已注册风险表中，风险类型的编号显示在所选风险的详细信息区域。

- **名称**

  风险类型表中显示的风险类型的名称。注册风险时，其名称可能与所用风险类型的名称不完全匹配。某些风险类型的名称可以完全替换为已注册风险的其他名称。例如，具有此类名称的风险类型包括“**来自外部系统的风险**”类型的风险。如果此类型的风险用于注册风险，则应用程序会保存风险信息源中指定的风险名称（例如，在使用 Kaspersky Industrial CyberSecurity for Networks API 的第三方应用程序中）。

- **类别**

  风险类别的名称。

- **基本分数**

  用于计算注册风险得分的初始值。在注册除外部系统风险外的所有风险时，将应用基本分数的定义值。名为“**来自外部系统的风险**”的风险类型的基本得分为零。必须在使用 Kaspersky Industrial CyberSecurity for Networks API 注册风险的接收者应用程序中指定这些风险的基本分数。

查看风险类型表时，您可以使用配置、过滤、搜索和排序功能。

更改风险类型的基本分数

无法更改名为“**来自外部系统的风险**”的风险类型的基本分数。如果使用此类风险类型来注册风险，则必须从有关风险的信息源定义该风险的基本分数（例如，通过使用 Kaspersky Industrial CyberSecurity for Networks API 的接收应用程序）。

要更改风险类型的基本分数：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**风险类型**”。
3. 在风险类型表中，选择要编辑其基本分数的风险类型。

   详细信息区域出现在 Web 界面窗口的右侧。
4. 单击**编辑**。
5. 指定基本分数的必要值。
6. 单击“**保存**”。

管理存储风险的设置

您可以更改用于存储风险的最大空间的限制。

要编辑风险存储设置：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**部署**”。
3. 选择服务器图块。

   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**编辑**。

   详细信息区域将显示用于配置服务器参数的选项卡。
5. 在“**常规**”选项卡上，转到“**风险**”并使用“**最大量**”设置来定义存储风险数据的大小限制。

   您可以选择空间限制的计量单位：**MB** 或 **GB**。

更改此设置的值时，需要记住所有卷限制的总和不能超过节点定义的最大存储卷。

6. 如有必要，请使用“**储存时间(天)**”设置启用风险的最短存储时间，并指定最短天数。

7. 单击“**保存**”。

管理漏洞和合规性审计作业的规则集

您可以在“**安全审计**”部分的“**规则集**”选项卡上管理漏洞和合规性审计作业规则集。安装数据库和应用程序模块更新后，默认情况下会使用漏洞和合规性审计作业的系统规则集。

具有管理员或安全官角色的用户可以管理漏洞和合规性审计作业的规则集。

漏洞和合规性审计规则

Kaspersky Industrial CyberSecurity for Networks 支持以以下语言编写的漏洞和合规性审计规则：

- OVAL (Open Vulnerability and Assessment Language) 是一种用于描述漏洞和评估信息系统配置的开放语言。该语言规范了信息的呈现方式、分析系统的过程以及结果的格式。

  仅使用这种语言的规则是 OVAL 定义，它形式化了信息系统的需求，提供了自动处理这些需求的能力。

- XCCDF（可扩展配置检查表描述格式）是一种基于 XML 的语言，用于描述安全设置的检查表。XCCDF 文档通常包含一组信息系统需求。

  使用这种语言的规则是具有配置文件和数据组的文档形式的高级需求列表。对于自动化处理，此类规则必须包含相关的 OVAL 定义。

漏洞和合规性审计规则被分组为若干组。您可以使用以下类型的规则集：

- 系统规则集。这些规则集与数据库和应用程序模块更新一起提供和更新。若要使用系统规则集，请安装更新。

  > 系统规则集包含由卡巴斯基和第三方组织开发的描述。从第三方组织获得并包含在系统规则集中的描述和措辞会按原样分发。

- 用户定义的规则集。这些规则集由用户通过文件导入加载到应用程序中。

加载规则集时，应用程序会验证规则集中的规则。如果在验证的规则中检测到错误，应用程序将阻止应用这些规则。如果在集合的所有规则中检测到错误，或者该集合不包含任何规则，则应用程序将阻止应用整个集合。

创建或编辑漏洞和合规性审计作业时，可以选择执行扫描所依据的规则。

查看漏洞和合规性审计规则集表

漏洞和合规性审计规则集表显示在“**安全审计**”部分的“**规则集**”选项卡上。

规则集设置显示在表的以下列中：

- **ID**
  由 Kaspersky Industrial CyberSecurity for Networks 分配的规则集 ID。
- **名称**
  在应用程序中表示规则集的名称。
- **描述**
  规则集的描述。
- **发布者**
  XCCDF 文档发布者的名称（如果指定）。
- **XCCDF 文档版本**
  有关 XCCDF 文档版本的信息（如果指定）。
- **XCCDF 状态**
  为 XCCDF 文档指定的最终状态。
- **XCCDF 配置文件**
  XCCDF 文档中的配置文件数。
- **集合中的 XCCDF 规则**
  XCCDF 文档中的规则数。
- **OVAL 定义**
  OVAL 定义的数量。
- **创建日期**
  将规则集添加到应用程序的日期和时间。
- **更改时间**
  上次在应用程序中修改规则集的日期和时间。
- **源**
  确定如何将规则集加载到应用程序中的规则集的类型：系统规则集或用户规则集。

查看规则集表时，您可以使用配置、过滤、搜索和排序功能，以及导航到相关项目。

导入漏洞和合规性审计规则集

您可以将文件中的漏洞和合规性审计规则导入 Kaspersky Industrial CyberSecurity for Networks。文件可以包含以 OVAL 语言或使用 OVAL 定义的 XCCDF 语言编写的规则。

导入的规则集称为*自定义*规则集。对于这些规则集，“**源**”设置为“**用户**”。

要导入文件，必须将它们打包到 ZIP 存档中。ZIP 存档内容支持的选项：

- XCCDF 包文件，以 XML 格式表示 XCCDF 文档和 OVAL 定义。如果包中包含 CPE (Common Platform Enumeration) 格式的字典文件，则还必须将这些文件添加到存档中。
  文件必须位于存档的根目录下。存档中文件的名称必须与以下名称掩码匹配：
  - `*-xccdf.xml` – XCCD F文档文件名称的掩码（例如，SCAP1-xccdf.xml）
  - `*-oval.xml` – 具有 OVAL 定义的文件名称的掩码（例如，SCAP1-oval.xml）
  - `*-cpe-dictionary.xml` – CPE 字典文件名称的掩码（例如，SCAP1-cpe-dictionary.xml）
  - `*-cpe-oval.xml` – 具有 OVAL 定义和 CPE 词典（例如，SCAP1-cpe-oval.xml）的文件名称的掩码
- 包含 OVAL 定义并且不属于 XCCDF 包的文件（使用该文件不需要 XCCDF 文档）。
  该文件必须位于存档的根目录下。存档中文件的名称必须与掩码匹配：`*-oval.xml`（例如，SCAP2-oval.xml）。

要导入一组漏洞和合规性审计规则：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**安全审计**”部分。
3. 在“**规则集**”选项卡上，单击工具栏上的“**导入**”。
4. 单击“**浏览**”并指定 ZIP 存档的本地路径。
5. 单击**导入**。
   数据导入过程开始。正在运行的导入操作的信息显示在后台操作列表中。
6. 要切换到新的规则集，请执行以下操作：
   a. 在应用程序 Web 界面菜单中点击。
   后台操作列表打开。
   b. 等待导入操作完成。
   c. 单击“**显示**”。

更改漏洞和合规性审计规则集

您可以修改自定义漏洞和合规性审计规则集的名称和文本描述。这样的更改不适用于系统规则集。

要更改规则集的名称或文本描述，请执行以下操作：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**安全审计**”部分。
3. 在“**规则集**”选项卡上，选择相关的规则集。
   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**编辑**。

5. 输入规则集的名称和说明。

   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . ' - " _`。规则集名称必须以任何允许的字符开头和结尾（空格除外）。

   规则集名称不得超过 1024 个字符规则集描述包含的字符数不得超过 4096 个。

6. 单击“**保存**”。

删除漏洞和合规性审计规则集

您可以删除自定义和系统漏洞及合规性审计规则集。但是，您不能删除具有关联作业的规则集。

要删除规则集：

1. 使用管理员或安全官账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 选择“**安全审计**”部分。

3. 在“**规则集**”选项卡上，选择要删除的规则集。

4. 单击**删除**。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认删除该规则集。

   您只能删除没有关联漏洞和合规性审计作业的规则集。如果所选规则集中存在与安全审计作业关联的规则集，则会出现相应的消息。要删除此类规则集，请首先删除关联的作业。

管理远程连接的账户凭据 Secret

Secret 存储在 Kaspersky Industrial CyberSecurity for Networks 中实现。*Secret* 使您能够安全地存储和使用应用程序自动远程连接到设备所需的标识和身份验证信息。Secret 用于选择了“远程连接**远程连接主动轮询**”连接器的**安全审计**作业。

应用程序提供各种类型的 Secret。根据 Secret 的用途，您可以在添加或编辑 Secret 设置时选择相关类型并输入适当的数据。

将使用远程连接协议进行设备远程连接所需的凭据保存在 Secret。使用**远程连接**方法轮询设备的安全审计作业使用 SSH 协议进行远程连接。根据所选的轮询方法，**主动轮询**连接器可以使用各种协议进行远程连接。

> 为了确保安全地使用存储在 Secret 中的身份和身份验证详细信息，该应用程序实施了在连接到远程设备时防止 Secret 泄漏的保护。在应用程序中保存从设备收到的公钥后，它会监控这些设备的所有后续远程连接，并且在网络上发生设备欺骗时不会发送任何来自 Secret 的信息。

关键的 Secret 信息，例如用于身份验证的密码或私钥，只能以明文形式提供一次：即在您创建 Secret 时输入这些信息时。一旦保存了 Secret，就无法查看关键信息。只有在更改 Secret（例如，输入新密码）时，才能替换 Secret 中的关键信息。

您可以在“**设置**”→“**Secret**”部分管理 Secret。不能向应用程序添加超过 500 个 Secret。

具有除操作员角色之外的任何角色的用户都可以管理 Secret。

添加 Secret

您可以将 Secret 添加到应用程序 Secret 存储中。

要添加 Secret：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**设置**” → “**Secret**”。

3. 单击“**添加 Secret**”打开详细信息。

4. 输入 Secret 名称。

   Secret 名称必须是唯一的（不得与其他 Secret 的名称匹配）并且必须包含最多 256 个字符。您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`。Secret 名称必须以任何允许的字符开头和结尾（空格除外）。

5. 选择 Secret 类型并配置其设置。

   您可以选择以下类型的 Secret：

   - **仅密码**：如果仅需要具有相关权限的用户的密码即可访问设备配置数据，则使用此类 Secret。
   - **用户名和密码**：如果需要用户名和密码才能从设备接收数据，则使用此类 Secret。
   - **用户名和密码，根密码**：如果需要用户名和密码才能从设备接收数据，而对于具有管理员（root）权限的连接，还需要 root 密码或以管理员权限处理请求的账户的密码，则使用此类 Secret。
   - **用户名和密码，加密密码**：如果需要用户名和密码才能从设备接收数据，并且还需要加密密码才能建立加密连接，则使用此类 Secret。
   - **混合**：此类 Secret 用于漏洞和合规性审计作业或配置控制作业中的**远程连接**设备轮询方法。您可以为此类 Secret 指定以下设置：

     - 用于远程连接设备的用户名。

       用户名可以包含拉丁字符、数字、句点和以下特殊字符：`_`和`-`。名称必须以字母开头，并以除句点之外的任何受支持的字符结尾。

     - **用户密码**：是否使用用户密码进行身份验证。

       密码必须包含最多 256 个 ASCII 字符。

     - **私钥**：是否使用私钥进行身份验证。

       您可以手动输入组成密钥的字符序列，或者通过单击**从文件复制**从文件上传密钥。支持使用 CRT、PEM、CER 格式的文件上传私钥。如果私钥文件受密码短语保护，请在上传密钥之前在“**密码短语**”字段中输入密码短语。

要使用私钥，请将对应的公钥复制到将使用该 Secret 建立远程连接的所有设备。将公钥复制到设备是在没有 Kaspersky Industrial CyberSecurity for Networks 参与的情况下执行的。

根用户密码：如果以管理员 (root) 权限连接网络部件时需要额外的密码。在这种情况下，会代表 root 账户或代表在网络部件上设置的账户来请求访问，以处理具有管理员权限的请求。

6. 单击**创建日期**。

查看 Secret 表

远程连接 Secret 表显示在应用程序 Web 界面的“**设置**”→“**Secret**”部分。

有关 Secret 的信息显示在表的以下列中：

- **Secret 名称**
  用于代表应用程序中的 Secret 的名称。
- **创建日期**
  将 Secret 添加到应用程序的日期和时间。
- **更改时间**
  上次在应用程序中修改 Secret 的日期和时间。

查看 Secret 表时，您可以使用配置、过滤、搜索和排序功能。

连接到远程设备时防止 Secret 泄漏

Secret 中的识别和身份验证详细信息仅应用于与选定用于安全审计作业的设备的远程连接。为了保护这些信息在设备欺骗的情况下免遭可能的泄漏，应用程序会在发送信息之前检查从设备收到的公钥。设备使用公钥建立 SSH 连接。公钥可帮助应用程序验证是否与正确的设备建立了 SSH 连接。验证收到的公钥与应用程序中保存的公钥匹配后，识别和身份验证详细信息将被发送到设备。

保存的设备公钥显示在“**常规**”选项卡上所选设备的详细信息区域中。

在应用程序中接收并保存设备公钥

默认情况下，Kaspersky Industrial CyberSecurity for Networks 中未定义设备公钥。当首次与设备建立 SSH 连接以进行扫描时，会接收并保存设备公钥，这是使用“**远程连接**”轮询或“**主动轮询**”连接器的安全审计作业的一部分。所选秘密的识别和身份验证详细信息将发送到设备，而无需检查收到的公钥。因此，在首次对选定的设备启动安全审计工作并与其建立 SSH 连接之前，请确保网络上没有被欺骗的设备。为此，您可以运行 `ifconfig` 来检查应用程序中定义的设备 IP 地址是否与实际设备网络接口上的 IP 地址相匹配。

重置已保存的设备公钥

设备上的 SSH 连接密钥可能会随着时间而改变。当设备用户当前的私钥面临泄漏风险时，他们可能会生成新密钥。

当设备上的私钥发生变化时，相应的公钥也会发生变化。更改公钥后，应用程序将停止将 Secret 信息发送到该设备，因为新的公钥不再与应用程序中保存的指纹匹配。因此，作为安全审计作业一部分的任何后续设备扫描都会以错误结束。

更改设备上的公钥后，重置应用程序中存储的设备当前保存的公钥。这将允许在远程连接设备时再次使用这些 Secret。

重置保存的公钥后，应用程序将在下次与设备建立 SSH 连接时保存新收到的公钥。检查网络上没有欺骗设备，类似于最初接收和保存公钥时。

具有除操作员角色之外的任何角色的用户都可以重置已保存的设备公钥。

要重设保存的设备公钥：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**资产**”部分。

3. 在**设备**选项卡上，选择要重置已保存的公钥的设备。

4. 右键单击即可打开所选设备之一的上下文菜单。

5. 在上下文菜单中，选择“**重置公钥**”。

   将打开一个带有确认提示的窗口。

6. 在提示窗口中，单击**确定**。

更改 Secret 的设置

编辑 Secret 设置时，您可以更改其类型和/或设置不同的凭据。

更改 Secret 设置（包括 Secret 名称）后，新设置将应用到使用该 Secret 的安全审计作业中。如果您更改 Secret 类型，如果新 Secret 类型与作业设置不匹配，则后续作业运行期间可能会出现错误。

要编辑 Secret 设置：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**设置**” → “**Secret**”。

3. 选择您要更改的 Secret。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 单击**编辑**。

5. 根据需要更改设置。更改 Secret 设置时可用的选项与添加 Secret 时可用的选项相同。

   关键 Secret 信息，例如密码和身份验证私钥，不会以纯文本形式显示。您只能使用凭据字段上方的链接将关键信息替换为新信息。

删除 Secret

您可以 Kaspersky Industrial CyberSecurity for Networks 的 Secret 存储库中删除 Secret。

在删除 Secret 之前，建议在使用此 Secret 的安全审计作业中指定其他 Secret 或轮询方法。如果在安全审计作业中指定了已删除的 Secret，则下次运行作业时会出现错误。

要删除 Secret：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 选择“**设置**” → “**Secret**”。

3. 选择您要删除的 Secret。

4. 单击**删除**。

   将打开一个带有确认提示的窗口。

5. 在提示窗口中，确认删除 Secret。

管理报告和报告模板

Kaspersky Industrial CyberSecurity for Networks 可以生成报告，其中包含有关设备和系统安全状态的信息、监控的技术流程参数和系统命令，以及有关检测到的风险和与第三方设备的交互的信息。应用程序基于*报告模板*生成此类报告。报告模板是一组参数，用于确定生成报告的条件。模板可以是系统模板（在安装应用程序期间创建），也可以是用户定义的模板（通过复制模板创建）。

在“**报告**”部分，具有管理员或安全官角色的用户可以复制模板以创建用户定义的报告模板、编辑和删除报告模板、删除生成的报告以及取消报告生成。

报告以 PDF 格式保存。

Kaspersky Industrial CyberSecurity for Networks 还可以生成带有设备扫描结果的报告，作为漏洞和合规性审计作业的一部分，以及整个漏洞和合规性审计作业运行的报告。在“**安全审计**”部分中开始生成报告。您可以在“**生成的报告**”选项卡上查看生成的报告。

复制报告模板

在当前版本的 Kaspersky Industrial CyberSecurity for Networks 中，您可以通过复制现有的报告模板来创建用户定义的模板。您可以复制系统模板和用户定义的模板。复制模板时，您不能更改报告中信息块的组成和布局。

应用程序中的最大模板数为 5000。

具有管理员或安全官角色的用户可以复制报告模板。

要复制报告模板，请执行以下操作：

1. 选择“**报告**”部分。
2. 在“**报告模板**”选项卡上，选择相关模板。
   详细信息区域出现在 Web 界面窗口的右侧。
3. 单击“**创建新模板**”
4. 在“**名称**”字段中，输入报告模板的名称。
   您可以使用英语和俄语字母、数字、空格以及字符 -、– 和 _。
   报告模板名称必须满足以下要求：
   - 不得与其他报告模板的名称匹配（不区分大小写）。
   - 必须包含 100 个字符或更少。

   根据更新后的模板生成的报告名称将与模板的新名称匹配。
5. 在“**数据周期**”下拉列表中，选择您想要在报告中获取系统信息的时间周期。
   您可以生成包含应用程序在过去 24 小时、7 天、30 天、一年或手动定义的时间段内收到的信息的报告。
6. 如果您需要根据计划生成报告，请打开“**按计划生成报告**”切换按钮并设置计划：
   a. 在“**频率**”下拉列表中，选择生成报告的频率：**每小时**、**每天**、**每周**或**每月**。
   b. 根据所选的选项，指定设置值以定义精确的启动报告生成的时间。
7. 如有必要，请使用“**目的地地址**”字段输入要将生成的报告发送到的电子邮件地址。如果您需要指定报告的其他收件人，请单击“**添加目标地址**”并输入电子邮件地址。
   报告收件人的最大数量为 20。
8. 单击**保存**。

新的报告模板将显示在报告模板表中。

编辑报告模板

具有管理员或安全官角色的用户可以编辑报告模板设置。

要编辑报告模板设置：

1. 选择“**报告**”部分。
2. 在“**报告模板**”选项卡上，选择相关模板。
   详细信息区域出现在 Web 界面窗口的右侧。
3. 单击**编辑**。
4. 在“**名称**”字段中，输入报告模板的名称。
   您可以使用英语和俄语字母、数字、空格以及字符 -、– 和 _。
   报告模板名称必须满足以下要求：
   - 不得与其他报告模板的名称匹配（不区分大小写）。
   - 必须包含 100 个字符或更少。

   根据更新后的模板生成的报告名称将与模板的新名称匹配。
5. 在“**数据周期**”下拉列表中，选择您想要在报告中获取系统信息的时间周期。
   您可以生成包含应用程序在过去 24 小时、7 天、30 天、一年或手动定义的时间段内收到的信息的报告。
6. 如果您需要根据计划生成报告，请打开“**按计划生成报告**”切换按钮并设置计划：
   a. 在“**频率**”下拉列表中，选择生成报告的频率：**每小时**、**每天**、**每周**或**每月**。
   b. 根据所选的选项，指定设置值以定义精确的启动报告生成的时间。
7. 如有必要，请使用“**目的地地址**”字段输入要将生成的报告发送到的电子邮件地址。如果您需要指定报告的其他收件人，请单击“**添加目标地址**”并输入电子邮件地址。
   报告收件人的最大数量为 20。
8. 单击**保存**。

更改将显示在“报告模板表”的相应列中。

删除报告模板

只能删除用户定义的报表模板。

具有管理员或安全官角色的用户可以删除报告模板。

要删除报告模板，请执行以下操作：

1. 选择“**报告**”部分。
2. 在“**报告模板**”选项卡上，选择一个或多个要删除的报告模板。

3. 单击**删除**。

   您无法删除系统报告模板。在报告模板表中，系统模板显示为 图标。

4. 在打开的提示窗口中，确认删除报告模板。

删除报告

具有管理员或安全官角色的用户可以删除应用程序中的报告。

要删除报告，请执行以下操作：

1. 选择“**报告**”部分。
2. 在“**生成的报告**”选项卡上，选择一个或多个要删除的报告。

   报告表中的报告是根据上次在当前服务器连接会话中运行的报告的 ID 进行过滤的。要显示所有生成的报告，请单击“**默认过滤器**”重置过滤器设置。如有必要，您可以根据特定的时间段配置筛选。

   详细信息区域出现在 Web 界面窗口的右侧。
3. 单击**删除**。
4. 在打开的提示窗口中，确认删除报告。

取消生成报告

您只能取消状态为“**进行中**”的报告的报告生成。

如有必要，具有管理员或安全官角色的用户可以取消由应用程序的任何用户启动的报告生成。

要取消生成报告，请执行以下操作：

1. 选择“**报告**”部分。
2. 在“**生成的报告**”选项卡上，选择要取消的状态为“**进行中**”的报告。

   详细信息区域出现在 Web 界面窗口的右侧。
3. 单击“**取消**”.
4. 在打开的提示窗口中，确认取消生成报告。

   完成此请求后，报告状态将更改为“**已取消**”。

管理存储报告文件的设置

您可以更改用于存储报告文件的最大空间的限制。

要编辑报告文件存储设置，请执行以下操作：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks Server。
2. 选择“**设置**” → “**部署**”。
3. 选择服务器图块。
   详细信息区域显示在 Web 界面窗口的右侧部分。
4. 单击**编辑**。
   详细信息区域将显示用于配置服务器参数的选项卡。
5. 在“**常规**”选项卡上，转到“**报告**”设置组，并使用“**最大量**”设置来定义用于存储报告文件的空间限制。
   您可以选择空间限制的计量单位：**MB** 或 **GB**。
   更改此设置的值时，您需要记住所有卷限制的总和不能超过为节点定义的最大存储卷。
6. 如有必要，使用“**储存时间(天)**”设置来启用报告文件的最短存储时间，并指定最短天数。
7. 单击“**保存**”。

管理安全策略

*安全策略*是一组数据，用于定义应用程序的以下操作设置：

- 用户定义的入侵检测规则集
- 网络异常检测规则和字典
- 允许交互控制和事件的规则
- 用于资产管理和过程控制的设备和标记的设置
- 网络地图显示设置
- 设备上的“用户”设置
- 设备上的“应用程序和补丁”设置
- 地址空间设置
- 事件类型设置
- 风险类型设置

所有其他应用程序设置都不属于安全策略的一部分，并且与其分开应用。这包括已安装组件的节点的设置、应用程序用户列表、设备表中链接事件和设备的对象以及其他设置。

安全策略存储在服务器上，每次修改应用程序设置时都会自动更新（例如，添加交互控制规则时）。

您可以将安全策略导出到文件，也可以从文件导入安全策略。您还可以清除服务器上的当前安全策略以删除所有先前保存的设置。

导出、导入或清除安全策略时，您可以选择要导出、导入或清除的策略的特定部分。例如，您可以仅导出设备并允许规则。

导出安全策略时，应用程序会创建一个文件，其中包含有关所选应用程序设置的信息。要导入设置，您可以选择之前导出的文件。

如果您从修改后的文件导入安全策略，更改安全策略文件的内容可能会导致 Kaspersky Industrial CyberSecurity for Networks 出现故障。应用程序可能会停止执行工业网络保护功能。

在服务器 Web 界面中导出安全策略

通过Web 界面连接到服务器时，您可以将安全策略中包含的设置导出到文件。您可以导出整个安全策略或其单个部分。

必要时，您可以从包含已保存的安全策略的文件中导入相关的应用程序设置。

若要导出当前的安全策略：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择**设置→安全策略**。
3. 单击**导出**。
   您将看到安全策略树，您可以在其中选择要导出的必要部分。
4. 选中安全策略相关部分的复选框。
5. 单击**导出**。
6. 如果文件生成耗时较长（超过 15 秒），则操作将移至后台。如果是这种情况，请按照以下步骤下载文件：
   a. 单击应用程序 Web 界面菜单中的 。
      后台操作列表打开。
   b. 等待文件生成操作完成。
   c. 单击“**下载文件**”。

您的浏览器将保存下载的文件。根据您的浏览器设置，屏幕可能会显示一个窗口，您可以在其中更改已保存文件的路径和名称。

使用导出实用程序导出安全策略

要导出安全策略中包含的设置，您可以使用 kics4net-cli 安全策略导出实用程序。该实用程序将整个安全策略导出到指定目录中的文件中。必要时，您可以从包含已保存的安全策略的文件中导入相关的应用程序设置。

该实用程序会自动安装在服务器计算机的 /opt/kaspersky/kics4net-cli/bin/ 处。您可以使用内置的操作系统工具配置 kics4net-cli 自动运行以创建定期安全策略备份。

该实用程序通过添加到应用程序的连接器连接到应用程序服务器。

要准备应用程序以使用安全策略导出实用程序，请执行以下操作：

1. 在应用程序中，添加安全策略导出实用程序将要用以连接到应用程序服务器的连接器。指定连接器的**通用**系统类型。

   添加连接器后，应用程序会生成新的通信数据包。通信数据包是一个存档。

2. 在安装了 kics4net-cli 的计算机上，准备一个目录来应用通信数据包的内容。

   要准备目录：

   a. 建立随机目录，将通信数据包复制到其中。

   b. 转到包含通信数据包副本的文件夹并输入以下命令将其解压：

   ```
   unzip <通信数据包名称>
   ```

   解压后的文件将出现在目录中。

   c. 输入以下命令创建 clientcert.crt 证书文件：

   ```
   sudo openssl pkcs12 -in certificates.pfx -nodes -clcerts -nokeys -out clientcert.crt
   ```

   当提示输入密码时，请输入密码以访问连接器证书。这是您在添加连接器或为连接器创建新的通信数据包时设置的密码。

   d. 输入以下命令创建 clientcert.key 文件：

   ```
   sudo openssl pkcs12 -in certificates.pfx -nocerts -nodes -out clientcert.key
   ```

   当提示输入密码时，请输入密码以访问连接器证书。

   e. 输入以下命令将 webserver.pem 复制到 kics4net-cli 证书目录 /var/opt/kaspersky/kics4net-cli/certs/：

   ```
   sudo cp webserver.pem /var/opt/kaspersky/kics4net-cli/certs
   ```

3. 在安装了 kics4net-cli 的计算机上，准备一个目录来保存导出的文件。

   要准备目录：

   a. 创建一个随机目录。要通过计算机的本地文件系统将文件保存到网络共享，您可以使用目录将文件保存到网络共享。

   b. 如果该目录未嵌套在 /var/opt/kaspersky/kics4net/shared/ 内，请将 kics4net 用户指定为所有者。为此，请输入以下命令：

   ```
   sudo chown kics4net:kics4net <目录路径>
   ```

更新连接器证书时，还需要替换从先前通信数据包中获得的文件。否则，由于旧文件中的无效证书，kics4net-cli 实用程序将无法连接到应用程序服务器。要替换文件，请使用新的通信数据包重复上述步骤 2。

若要导出当前的安全策略：

1. 在安装了 kics4net-cli 的计算机上，打开操作系统控制台并转到 /opt/kaspersky/kics4net-cli/bin/。
2. 在命令行中输入以下命令：

```
sudo ./kics4net-cli exec exportsecuritypolicy \
--client-cert=<clientcert.crt 文件路径> \
--client-key=<clientcert.key 文件路径> \
--export-path=<保存文件的目录路径> \
--timeout=<超时时间>
```

其中：

- `exec` 是运行实用程序支持的命令的参数（强制参数）
- `exportsecuritypolicy` 是将安全策略导出到文件的命令（强制参数）
- `<clientcert.crt 文件路径>`是应用通信数据包的内容的目录中的 clientcert.crt 证书文件的完整路径和名称（必填设置）。
- `<clientcert.key 文件路径>`是应用通信数据包的内容的目录中的 clientcert.key 文件的完整路径和名称（必填设置）。
- `<目标目录>`是导出文件将保存到的目录的完整路径（必填设置）。
- `<超时>`是命令执行结果超时时间，单位为秒（默认 900 秒），如果由于安全策略中的数据量太大导致上次导出尝试失败，则可以通过此参数增加超时时间。

示例

```
sudo ./kics4net-cli exec exportsecuritypolicy --client-cert=/home/user1/certs/clientcert.crt --client-
key=/home/user1/certs/clientcert.key --export-path=/var/opt/kaspersky/kics4net/shared/policy/
```

实用程序运行完成后，验证文件是否位于目标目录中。

3. 如果必须将结果文件复制到另一个位置，请授予复制该文件的权限。默认情况下只有所有者才拥有该权限。要授予权限，请输入以下命令：

```
sudo chmod o+r <策略文件路径>
```

从文件中导入安全策略

您可以从包含已保存的安全策略的文件中导入应用程序设置。对于导入，您可以使用通过以下方法之一导出安全策略时获得的文件：

- 通过 Web 界面连接到服务器
- 使用导出实用程序

导入安全策略部分时，应用程序首先清除这些部分的当前内容，然后将数据导入这些部分。

如果文件包含安全策略的多个部分，您可以选择相关部分进行导入。

如果当前正在安装更新或正在运行另一个导入过程，则无法导入安全策略。

只有具有管理员角色的用户才能从文件导入安全策略。

要从文件导入安全策略：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 禁用服务器、探测器和监控点节点上的所有技术和方法的使用。
3. 选择**设置→安全策略**。
4. 单击**导入**。
   这将打开用于选择文件的标准浏览器窗口。
5. 指定安全策略文件的路径。
6. 单击打开文件的按钮。
   检查文件内容后，您将看到一个安全策略树，其显示可以导入的部分。
7. 选中要导入应用程序的安全策略部分的复选框。
8. 单击**导入**。

   安全策略导入过程开始。在导入过程完成之前，应用程序服务器无法连接。在导入过程中，应用程序 Web 界面页面会显示一个名为**应用程序维护**的特殊部分。当应用程序 Web 界面恢复正常运行模式后，重新启用必要的技术和方法。

清除当前安全策略

您可以清除当前属于安全策略的设置。这可以针对整个安全策略或其某些单独部分进行。

安全策略被清除后，即使您事先导出该安全策略，也将无法恢复部分数据。例如，清除包含设备信息的部分后，设备表中链接事件和设备的所有对象都将被永久删除。

如果当前正在安装更新或数据导入过程正在运行，则无法清除安全策略。

只有具有管理员角色的用户才能清除安全策略。

要清除安全策略：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 禁用服务器、探测器和监控点节点上的所有技术和方法的使用。
3. 选择**设置→安全策略**。

4. 单击**清空**。

   您将看到安全策略树，您可以在其中选择要清除的相关部分。

5. 选中要清除的安全策略部分的复选框。

6. 单击**清空**。

   安全策略清除过程开始。在清算过程完成之前，应用服务器无法进行连接。在清算过程中，应用程序 Web 界面页面会显示一个名为**应用程序维护**的特殊部分。当应用程序 Web 界面恢复正常运行模式后，重新启用必要的技术和方法。

从先前版本的应用程序转换安全策略

如果您要将包含已保存的安全策略的文件从应用程序的先前版本导入到应用程序的当前版本，则需要使用 policy_updater.py 策略转换脚本来转换此文件。该脚本位于服务器计算机的 /opt/kaspersky/kics4net/sbin/ 文件夹中。

policy_updater.py 脚本用于转换导出到 Kaspersky Industrial CyberSecurity for Networks 3.0 及更高版本的安全策略。

要转换包含在应用程序先前版本中创建的安全策略的文件：

1. 打开服务器计算机上的操作系统控制台并转到 /opt/kaspersky/kics4net/sbin/ 文件夹。

2. 在命令行中输入以下命令：

   ```
   python3 ./policy_updater.py -i <原始策略文件的路径> -o <转换后的策略文件的路径>
   ```

   示例

   ```
   python3 ./policy_updater.py -i /home/user1/policy_2025-11-01_12-00 -o /home/user1/policy_for_4_5
   ```

获取的文件可以导入到应用程序的当前版本中。

使用 Kaspersky Industrial CyberSecurity for Networks API

Kaspersky Industrial CyberSecurity for Networks 具有应用程序编程接口 (API)，可为外部应用程序（以下称为“接收应用程序”）提供对应用程序功能的访问。

Kaspersky Industrial CyberSecurity for Networks 分发套件包括一个包，其中包含表示向 REST API 服务器发送的请求中的数据的规范描述。*REST API 服务器*在 Kaspersky Industrial CyberSecurity for Networks 服务器计算机上运行，并使用称为 REST（表述性状态传输）的交互架构风格处理请求。对 REST API 服务器的查询通过 HTTPS 协议发送。您可以在**设置→连接服务器**下配置 REST API 服务器设置（包括用受信任证书替换默认的自签名证书）。

JSON 格式用于表示请求和响应中的数据。

包含基于 REST 架构风格的请求描述的文档作为“在线帮助指南”发布在“卡巴斯基在线帮助”页面上。本文档充当开发人员指南。开发人员指南还提供了被发送到 REST API 服务器的请求中可用的调用元素的示例代码和详细描述。

打开描述对 REST API 服务器的请求的文档，版本 3

打开描述对 REST API 服务器的请求的文档，版本 4

接收应用程序可以使用 Kaspersky Industrial CyberSecurity for Networks API 执行以下操作：

- 在对应用程序已知的设备上接收数据。
- 添加、修改和删除设备。
- 接收有关已注册事件的数据。
- 将事件发送到 Kaspersky Industrial CyberSecurity for Networks（代码为 4000005400 的系统事件类型用于注册事件）。
- 接收有关标记和标记参数的数据。
- 订阅有关收到的标记值的通知。
- 接收有关检测到的漏洞的数据。
- 接收应用程序消息和审计条目。
- 接收有关允许规则的数据。
- 启用、禁用和删除允许规则。
- 接收与设备相关的风险数据。
- 接收有关地址空间的数据。
- 将网络拓扑图报告发送至 Kaspersky Industrial CyberSecurity for Networks。

- 发送、接收和删除有关设备上用户的信息。
- 发送和接收有关设备上的应用程序和补丁的信息。
- 发送和删除有关设备上的可执行文件的信息。
- 发送设备日志的内容。
- 接收以下应用程序数据：
  - 安装了应用程序组件的节点列表
  - 监控点及其参数列表
  - 支持的协议栈及其参数列表
  - 事件类型及其参数列表
  - 技术现状及运作模式
  - 应用程序版本和已安装更新的发布日期
  - 有关添加的授权许可密钥的信息
  - 应用程序本地化语言

向 REST API 服务器版本 4 发出请求时，所有列出的操作均可用。向 REST API 服务器版本 3 发出请求时，其中一些操作不受支持。

使用 Kaspersky Industrial CyberSecurity for Networks API 的接收应用程序可以通过连接器连接到应用程序服务器。连接器使用证书来建立安全连接。对于每个将向 REST API 服务器发送请求的接收应用程序，您需要在 Kaspersky Industrial CyberSecurity for Networks 中创建一个单独的连接器。

接收应用程序必须使用身份验证令牌与 Kaspersky Industrial CyberSecurity for Networks 建立连接。应用程序根据接收应用的请求发出身份验证令牌，对于此令牌，它使用为此接收应用创建的连接器的证书。身份验证令牌的有效期为 10 小时。接收应用程序可以通过特殊请求更新身份验证令牌。

包含身份验证令牌操作查询描述的文档作为在线帮助指南发布在“卡巴斯基在线帮助”页面上。本文档充当开发人员指南。

打开描述身份验证令牌操作查询的文档，版本 3

打开描述身份验证令牌操作查询的文档，版本 4

Kaspersky Industrial CyberSecurity for Networks API 提供使用接收应用程序的以下选项：

- 基于 REST 架构风格的交互
- 通过 WebSocket 协议进行交互

接收应用程序可以使用 WebSocket 协议在 Kaspersky Industrial CyberSecurity for Networks API 中进行交互，以创建对应用程序收到的修改值的订阅。例如，这种交互方式可以让您订阅有关收到的特定标记值的通知。

使用 Kaspersky Industrial CyberSecurity for Networks API 时确保交互安全

接收应用程序在通过 HTTPS 协议建立加密连接后，使用 Kaspersky Industrial CyberSecurity for Networks API 访问应用程序功能。连接通过使用 Kaspersky Industrial CyberSecurity for Networks 服务器颁发的证书来保护安全。服务器为被接收应用程序用来连接到服务器的连接器颁发证书。

必须为每个接收应用程序创建单独的证书。只有使用服务器颁发并保存在该连接器的通信数据包中的特定证书才能通过连接器建立连接。如果接收应用程序使用来自不同连接器或不同 Kaspersky Industrial CyberSecurity for Networks 服务器的证书，或者使用用于其他连接的证书（例如探测器证书），则无法建立连接。

建立加密连接后，接收应用程序必须为连接器请求*身份验证令牌*，接收应用程序将在发送到 REST API 服务器的请求中指示该令牌。在签发身份验证令牌之前，服务器会验证连接器创建时指示的应用程序用户帐户的当前状态。如果应用程序用户帐户已被删除或阻止，服务器将不会签发身份验证令牌。

身份验证令牌由服务器发出后 10 小时内有效。如果令牌需要使用更长时间，则接收应用程序必须在令牌过期之前请求延长时间。

有关 Kaspersky Industrial CyberSecurity for Networks 服务器 API 中提供的请求和方法的信息，请参阅 Kaspersky Industrial CyberSecurity for Networks API 文档。

当服务器在身份验证令牌的有效期内收到来自接收应用程序的请求时，服务器将验证创建连接器时指示的应用程序用户账户的存在及其当前访问权限。如果未找到用户账户（已从应用程序中删除），或者用户账户没有足够的权限执行操作（用户账户角色与执行的操作不匹配），则不会执行接收应用程序的请求中指示的方法。

在处理来自接收应用程序的请求时，应用程序使用审计日志来存储有关尝试执行以下操作的信息：

- 接收身份验证令牌。
- 延长身份验证令牌的有效期。
- 将设备添加到设备表中。
- 编辑设备信息。
- 删除设备。
- 查询审计日志（加载 Web 服务器后第一次通过连接器读取审计条目时）。

创建并使用 Kaspersky Industrial CyberSecurity for Networks API 的连接器

为了使接收应用程序能够使用 Kaspersky Industrial CyberSecurity for Networks API 与应用程序交互，您需要为此应用程序添加一个连接器。创建连接器时，您必须指明连接器的**一般**系统类型。

当添加连接器并为此连接器创建新的通信数据包时，服务器会生成一个通信数据包，您需要使用该数据包使连接器工作。

通信数据包是一个包含以下文件的存档：

- certificates.pfx – 包含服务器的公共证书密钥和服务器为连接器颁发的证书（带有私钥）的加密文件。文件内容使用添加连接器时或为此连接器创建新的通信数据包时设置的密码加密。
- metadata.json – 包含连接器的配置数据。数据以 JSON 格式呈现。

必须使用列出的文件通过连接器连接接收应用程序。要解密 certificates.pfx 文件并应用其中的证书和密钥，您可以使用处理此格式的文件的标准方法（例如，`openssl`命令）。连接器工作以及向 REST API 服务器发送请求需要 metadata.json 文件中指示的地址。

通信数据包中的证书和配置数据一直有效，直到创建新的通信数据包或者从应用程序中移除连接器为止。

通过 WebSocket 协议订阅有关标记值的通知

当使用 Kaspersky Industrial CyberSecurity for Networks API 时，接收应用程序可以创建有关特定标签修改值的通知订阅。WebSocket 协议用于创建订阅和接收通知。

接收应用程序的订阅包括以下步骤：

1. **接收应用程序使用 REST API 服务器通过此应用程序的连接器与 Kaspersky Industrial CyberSecurity for Networks 服务器建立连接。**

   成功连接到服务器后，连接器会收到一个身份验证令牌。连接器在此会话中与服务器的所有后续交互（特别是从服务器请求其配置）上都使用此身份验证令牌。

2. **接收应用程序使用 WebSocket 进行连接并发送请求以创建有关相关标签接收值的通知订阅。**

   Kaspersky Industrial CyberSecurity for Networks 服务器接收请求并创建订阅。使用 WebSocket 协议提供的适当功能发送请求。

3. **Kaspersky Industrial CyberSecurity for Network 在读取或写入标记时，会检测流量中的新标记值。**

4. **Kaspersky Industrial CyberSecurity for Networks 将获取的标签值发送给已有效订阅该标签值相关通知的接收应用程序。**

订阅的主要功能：

- 在接收应用程序指示 Kaspersky Industrial CyberSecurity for Networks 的相关标签后，服务器将发送有关获取这些标签值的功能的确认。然后接收应用程序等待通过建立的连接接收这些标签的值。
- 订阅的创建和维护依赖于 WebSocket 协议和 REST API 服务器使用的同一地址上的连接。
- Kaspersky Industrial CyberSecurity for Networks 服务器支持不超过一个标签值的活动订阅。如果已创建并正在使用一个活动订阅，而您尝试创建另一个订阅，则会看到连接数过多的错误提示。
- 接收应用程序可以随时关闭已建立的订阅连接以停止接收标签值。
- 如果接收应用程序故意关闭订阅或者连接中断，则订阅将停止。如果 Kaspersky Industrial CyberSecurity for Networks 服务器暂时不可用（断开连接）且未转发订阅的标签值，则接收应用程序必须在恢复连接后重新订阅标签值。

使用 WebSocket 连接

要通过订阅接收标签，您可以使用 WebSocket 的标准功能以及 SignalR Core 库。使用 SignalR Core 库的软件包适用于最常见的编程语言：C++、C#、Java、Python、Go 和 JavaScript/TypeScript。

要通过 WebSocket 连接，您需要指定以下地址：

```
<通信数据包中的公共 API 地址>/kics4net/api/v4/tag-values
```

但是，地址字符串中指示的协议取决于用于连接的功能。

如果使用 SignalR Core 库，地址字符串以 `https://` 开头。例如：

```
https://kics-server:8080/kics4net/api/v4/tag-values
```

如果使用 WebSocket 标准功能，则需要将地址字符串中的 `https` 替换为 `wss`。例如：

```
wss://kics-server:8080/kics4net/api/v4/tag-values
```

如果连接时未提供身份验证令牌（或者提供的令牌未通过验证），则服务器在响应打开连接的请求时返回代码 401。

创建标签值订阅

要创建订阅，您必须使用 `GetTagValuesStream` 方法名称发出请求。

请求参数示例

```
{
"tagIdentifiers": [
{ "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
{ "tagName": "Asdu_1_object_1003", "assetName": "Asset 079" }
],
"streamConfig": {
"samplingRateHz": 1
}
}
```

请求参数由以下字段组成：

- `tagIdentifiers` – 包含订阅所需值的标签 ID 数组。
- `assetName`、`tagName` – 代表设备名称和标签名称的值（用于识别包含订阅所需值的标签）。
- `samplingRateHz` – 标签值采样率（用于减少传输数据量）。如果为该字段定义了空值，则不会执行采样。

如果订阅创建参数不满足字段的要求，则会返回错误并附上问题描述。

订阅创建参数的错误示例

```
HubException: GetTagValuesStreamRequest 有验证错误：
TagIdentifiers:
TagName 字段是必填的。
StreamConfig 字段是必填的。
```

确认订阅

在确认订阅时，服务器会针对请求中与 `tagIdentifiers` 值匹配的每个标签返回确认结果。

订阅确认示例

```
{
"confirmation": {
"result": "ok",
"tagIdentifier": { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
"tagId": 102
}
}
```

包含订阅确认的响应包含以下字段：

- `result` – 标签值订阅的状态。可能值：
  - `ok` – 订阅已成功创建。
  - `notFound` – 未找到具有指定 `assetName` 或 `tagName` 的标签。
- `tagIdentifier` – 标签 ID，相当于订阅创建请求的参数 `tagIdentifiers` 数组中的一个值。
- `tagId` – 应用程序中标签的唯一ID。这可用于通过 Kaspersky Industrial CyberSecurity for Networks API 接收有关标签的信息，或在包含其值的响应中识别标签。

按订阅的标签值

应用程序按字段结构内的订阅发送标签值。以下字段显示在结构的顶层：

```
{
"value": {
 "tagId": <应用程序中标签的唯一 ID>
 "tagValue": "<包含标签数据的 JSON 对象>"
}
}
```

有关标签新值的信息以 JSON 格式发送到接收应用程序。发送的数据对象包含以下字段：

- `n` – 由 `TagStructure` 中的名称表示的标签数据类型。
- `ts` – 标签值最后更新注册的时间。以从 1970 年 1 月 1 日开始的微秒表示。

- `dn` – 传输方向。可能的值：`r`、`w`、`rw`。
- `mp` – 监测点 ID。
- `d` – 标签字段的内容。

`d` 属性代表一个字典，其中每个键都是空层次标签字段的名称。每个字段值均具有以下属性：

- `t` – 必填属性，指示以下数据类型之一：
  - `u` – UINT64
  - `i` – INT64
  - `b` – BOOL
  - `d` – DOUBLE
  - `s` – UTF8 字符串
  - `t` – 从 1970 年 1 月 1 日开始的时间（以微秒为单位）
  - `e` – ENUM。该字段还包含以下属性：
    - `n` – ENUM 类型的名称
    - `v` – ENUM 的原始值
    - `s` – ENUM 的字符串值
  - `st` – 结构
  - `un` – UNION
- `v` – 强制属性，指示标签字段值
- `n` – `TagStructure` 中的 ENUM 类型名称（仅适用于 `e` 类型 – ENUM）
- `s` – ENUM 的字符串值（仅适用于 `e` 类型 – ENUM）

  示例

  ```
  - enum:
  name: OpType # ENUM 类型的名称（'n' 属性）
  data:
   0: NUL # 0 写入 'v' 属性，NUL 写入 's' 属性
  1: PULSE_ON
  2: PULSE_OFF
  ```

- `x` – 标识标签的主值。
  格式：`"x": 1`
  标签的所有其他字段均不存在 `x` 属性。

- `m` – 标记参数的特殊标记。这对应于具有以下字段的`标记`属性：
  - `q` – 质量属性的值。
  - `ts` – 时间戳状态显示其准确性、临时状态或验证期间出现错误的原因。
  - `ds` – 数据状态。
  - `o` – 值或命令的来源。
  - `t` – 标签值最后更新的时间（从流量中获取）。
  - `ct` – 传输原因。

格式：`"m": "q"`

以 JSON 格式转发的标签值示例


```
{
"n": "TagStructure1",
"ts": 1784035816,
"dn": "r",
"mp": 1,
"d":
{
"value":
{
"t": "d",
"v": 3.1415,
"x": 1
},
"quality":
{
"t": "s",
"v": "good",
"m": "q"
},
"mask":
{
"t": "u",
"v": 1784035816
},
"enumfield":
{
"t": "e",
"n": "SwitchState",
"v": 0,
"s": "Off"
},
"strucfield":
{
"t": "st",
"v":
{
"v1":
{
"t": "d",
"v": 3.1415
},
"q2":
{
"t": "s",
"v": "good",
"m": "q"
}
}
},
"unionfield":
{
"t": "un",
"v":
{
"_":
{
```

```
"t": "u",
"v": 42
},
"low4bits":
{
"t": "u",
"v": 10
},
"high4bits":
{
"t": "u",
"v": 2
}
}
}
}
}
```

通过订阅接收标签值的示例

下面是使用 Python 中的标准 WebSocket 功能通过订阅接收标签值的示例。

您必须先运行以下命令：

```
pip install websocket_client
```

使用标准 WebSocket 功能的订阅示例

```
import json, ssl, websocket


def on_message(ws, message):
print(message)


def on_error(ws, error):
print(f' 错误: {error}')


def on_close(ws):
print("### 已关闭 ###")


def on_open(ws):
print("连接已打开，握手已接收，准备发送消息")

# 所有发送的消息必须以此字符结尾
message_separator = chr(30)

# 设置 json 作为消息格式
protocol_selection_args = {
'protocol': 'json',
'version': 1
}
ws.send(json.dumps(protocol_selection_args) + message_separator)

# creating subscription
args = {
'arguments': [
{
'tagIdentifiers': [
{
'tagName': 'tag_01',
'assetName': 'asset_02'
}
],
'streamConfig': {
'samplingRateHz': 5
}
}
```

```
],
'invocationId': '0', # 将包含在响应消息中
'target': 'getTagValuesStream',
'type': 4 # 对于传出消息，必须等于 4
}

ws.send(json.dumps(args) + message_separator)


def login():
token = "您应该在这里获取 API 的访问令牌"
return token


if __name__ == "__main__":
server_url = "wss://localhost:8091/kics4net/api/v4/tag-values"
auth = "Authorization: Bearer " + login()

# 用于故障排除，取消注释下一行
# websocket.enableTrace(True)
ws = websocket.WebSocketApp(server_url,
on_message=on_message,
on_error=on_error,
on_close=on_close,
header=[auth])

print(f'打开到 {server_url} 的连接')
ws.on_open = on_open
ws.run_forever(
# 仅当服务器具有自签名证书时才使用它
sslopt={"cert_reqs": ssl.CERT_NONE}
)
```

下面是使用 Python 中的 SignalR Core 库通过订阅接收标签值的示例。

您必须先运行以下命令：

```
pip install signalrcore
```

使用 SignalR Core 库的订阅示例

```
import logging
from signalrcore.hub_connection_builder import HubConnectionBuilder

TOKEN = '您应该在此处获取 API 访问令牌'
IP = '192.168.2.7'
PORT = '8080'
HUB = 'kics4net/api/v4/tag-values'

class WebsocketConnection(HubConnectionBuilder):
def __init__(self, url: str = None, options: dict = None, verify_ssl: bool = False):
super().__init__()
self.with_url(url, options=options)
self.configure_logging(logging.WARNING)
self.with_automatic_reconnect({
"type": "raw",
"keep_alive_interval": 10,
"reconnect_interval": 5,
"max_attempts": 5
})
self.verify_ssl = verify_ssl

def on_tag_stream_value(self, m):
result.append(m)
print(f'on_new_tag_value, {m}')

def on_tag_strean_error(self, e):
print(f'onError, {e}')

def on_tag_stream_complete(self, q):
print(f'onComplete, {q}')

def subscribe_tags(self):
print("连接已打开，握手已接收，准备发送消息")

args = {
'tagIdentifiers': [
```

```
{
'tagName': 'tag_01',
'assetName': 'asset_02'}
],
'streamConfig': {
'samplingRateHz': 5
}
}

self.stream("GetTagValuesStream", [args]) \
.subscribe({
"next": self.on_tag_stream_value,
"complete": self.on_tag_stream_complete,
"error": self.on_tag_strean_error
})

def main():
server_url = "https://{}:{}/{}".format(IP, PORT, HUB)
login = 'bearer {}'.format(TOKEN)

conn = WebsocketConnection(url=server_url, options={"headers": {"authorization": login}})
conn.build()

logging.info(f'打开到 {server_url} 的连接')
conn.on_open(conn.subscribe_tags)
conn.start()

logging.info('关闭连接')
conn.stop()


if __name__ == '__main__':
main()
```

执行常见任务

本节包含常见用户任务的描述以及如何执行这些任务的说明。

在线模式下的系统监控

Kaspersky Industrial CyberSecurity for Networks 在应用程序 Web 界面的**控制板**部分显示用于监控系统当前状态的数据。数据在联机模式下自动更新。

控制板部分的数据以称为*小部件*的单独区块形式呈现。根据其用途，小组件可能包含有关应用程序当前状态的可更新值或消息，或提供有关最新数据的扩展信息。

控制板部分可能会显示以下小组件：

- 包含用于监控系统当前状态和最重要变化的信息的小部件：
  - **具有安全状态的设备**（在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 中，该小部件称为**设备安全状态**） – 按安全状态对设备进行分布。
  - **事件分数** – 根据所选期间内事件的得分排列事件的直方图。直方图的列对应事件分数的整数值。您可以更改按严重性级别排列事件的饼图上的数据的显示方式。根据分数，事件的严重程度可能为*低*（分数为 0.0-3.9）、*中*（4.0-7.9）或*高*（8.0-10.0）。
  - **按技术分类的事件**（在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 中，该小部件称为**事件技术**） – 按事件注册技术对选定期间的事件进行定量分布。
  - **事件中经常遇到的应用程序用户** – 根据所选期间的 EPP 应用程序数据显示事件中最常注册的用户名。
  - **事件中经常遇到的应用程序** – 根据选定期间的 EPP 应用程序数据显示事件中最常注册的收件人应用程序。
  - **事件中经常遇到的设备** – 显示选定时间段内事件中最常注册的设备。
  - **按风险计数排名靠前的设备** – 显示选定时间段内检测到的风险中注册最频繁的设备。
  - **风险分数** – 根据选定期间的风险评分排列风险的直方图。直方图的列对应事件分数的整数值。您可以更改按严重性级别排列风险的饼图上的数据的显示方式。根据分数，风险的严重程度可能为*低*（分数为 0.0-3.9）、*中*（分数为 4.0-7.9）或*高*（分数为 8.0-10.0）。
  - **设备状态**（仅在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 中可用） – 按状态分布设备。
  - **设备** – 包含有关工业网络上的设备的信息（按设备类别排列）。
  - **事件**– 包含有关事件和事故的信息，这些事件和事故具有上次发生的日期和时间的最新值。
  - **态势感知** – 显示有关当前已识别的系统安全威胁的通知（例如，**检测到 10 次未经授权的网络交互**）。此小组件按严重性顺序显示通知。

- **EPP 应用程序的保护** — 受 EPP 应用程序保护的计算机与未受 EPP 应用程序保护的计算机的数量比率。饼图中心显示的是总数。符合特定条件的设备在小部件中会被计入受保护和未受保护的计算机数量。

- **按协议排名的流量**（仅适用于 Kaspersky Industrial CyberSecurity for Networks 4.5.1 版本）— 显示所选时间段内检测到的协议的流量分布情况。该小部件会显示其右侧所选协议的流量图。在图表中，协议以不同颜色填充的独立图层显示。在小部件右侧选择协议时，最多可显示 14 种不同的协议（流量非零但未包含在小部件主列表中的协议由附加的常规元素**其他协议**表示）。如果您希望小部件仅显示特定协议的数据，可以在更改小部件中的数据显示设置时选择这些协议。

- 包含有关应用程序以及服务器和探测器的硬件资源的信息的小部件：

  - **流量** — 传入流量的速率。该小组件可以显示所有安装了应用组件的节点的所有监控点的数据、选定节点的监控点的数据或单个监控点的数据。

  - **CPU** — 安装了应用程序组件的选定节点上的处理器利用。

  - **RAM** — 安装了应用程序组件的选定节点上正在使用的物理 RAM 数量。

  - **性能** — 有关应用程序性能当前状态的信息。此小组件可以显示以下值：

    - **正常** — 没有关于性能问题的消息，或者所有性能问题已解决。

    - **非关键故障** — 有关于非严重故障的消息（一直显示到性能问题得到解决）。

    - **操作中断** — 有关于应用程序性能问题的消息（此消息会一直显示到性能问题得到解决）。

    - **维护模式** — 应用程序正在维护模式下运行。

  - **标记** — 应用程序检测到的标签的处理速率。该小组件可以显示所有安装了应用组件的节点的所有监控点的数据、选定节点的监控点的数据或单个监控点的数据。

  - **存储**—有关安装了应用程序组件的选定节点上的本地文件系统中的驱动器的信息。在此小组件上，您可以选择显示以下数据：

    - **磁盘使用** — 处理数据读/写操作所花费的时间百分比。

    - **已占用磁盘**— 已使用的磁盘空间量。

    - **从磁盘读取** — 从磁盘读取数据的速率。

    - **写入到磁盘** — 将数据写入磁盘的速率。

  - **流量处理延迟** — 从流量到达节点的监控点开始的当前处理延迟（显示从所有启用的监控点收到的最大延迟时间）。该小工具可以显示所有安装有应用组件的节点的所有监控点数据，或者显示选定节点上的监控点数据。

  - **功能状态** — 有关应用程序中保护功能当前状态的一般信息。此小组件可以显示以下值：

    - **已启用所有** — 所有为持续使用而设计的技术和方法都已启用，所有创建的监控点都已启用。

    - **未启用全部** — 某些保护功能被禁用或在学习模式下启用，或者并非所有监控点都启用。

- **运行时间** — Kaspersky Industrial CyberSecurity for Networks 的运行时间。在此小组件上，您可以选择显示以下数据：
  - **有效运行时间** — 自最近一次启动到当前时刻，应用程序正常运行（无故障）的持续时间。
  - **总运行时间** — 自应用程序首次启动到当前时间的总运行时间（包括正常运行时间和应用程序运行出现故障的时间）。
  - **自应用程序首次启动以来**（在 Kaspersky Industrial CyberSecurity for Networks 版本 4.5.1 中，此设置名为"**自首次运行以来的时间**"） — 从应用程序首次启动到当前时间所经过的总时间（包括应用程序正常操作期间、故障期间和无法运行期间）。
- 不含动态更新信息的小组件。您可以创建具有用户定义内容的小组件。这些小组件被称为*自定义*小组件。例如，您可以使用自定义小组件在**控制板**部分中以逻辑方式分隔小组件组。

根据传入的数据，小组件提供各种方式来吸引您的注意力。例如，如果信息需要引起注意（例如，当硬件资源上的负载接近临界负载时），包含有关应用程序和硬件资源信息的小组件可以自动改变颜色。

小组件仅显示主要信息，信息动态更新。如果您需要查看更详细的信息（例如，有关有问题的设备的信息），您可以从**控制板**部分继续转到应用程序 Web 界面的其他部分。您可以使用鼠标选择小组件的界面元素在各个部分之间切换。

添加小组件

要添加小部件：

1. 在**控制板**部分中，单击**小部件**。
   将打开**添加小部件**窗口。
2. 点击小部件名称右侧的"**添加**"，添加相关小部件。
   新的小部件将占据小部件显示区域中的空闲空间。
3. 单击"**关闭**"窗口中的**添加小部件**。

添加小部件后，您可以配置小部件的显示方式。

配置小组件的显示方式

本节提供有关自定义小部件显示的说明。

移动小组件

要移动小部件：

1. 在**控制板**部分，将光标移到相关小部件的上部（例如，小部件名称上）。
   光标将变为  。
2. 将小部件拖拽至小部件显示区域的适当位置。

更改小组件的大小

要调整小部件的大小：

1. 在**控制板**部分，将光标移到相关小组件的右下角。
2. 单击并按住鼠标左键来设置小组件边框的大小。

更改小组件中数据的显示设置

添加小组件后，将使用默认设置在窗口小组件中显示数据。您可以根据需要更改显示设置（例如，指示相关来源或选择在**存储**小组件中显示的其他数据）。

要配置小部件显示设置：

1. 在**控制板**部分中，单击小组件右上角的⚙打开小组件管理窗口。
2. 在小组件管理菜单中，选择**配置**。
   这将打开用于配置显示设置的窗口。
3. 配置小组件设置。
   根据所选的小组件，窗口可能包含以下设置：
   - **更改名称** – 如果选中**更改名称**复选框，您可以在**小部件名称**字段中为小组件定义任何名称（不同于默认名称）。自定义小组件中没有**更改名称**设置。
   - **小部件名称** – 用于输入与默认名称不同的小组件名称的字段。
   - **更改描述**– 如果选中**更改描述**复选框，您可以在**小部件描述**字段中为小组件提供任何描述（不同于默认描述）。自定义小组件中缺少**更改描述**设置。
   - **小部件描述** – 用于输入与默认描述不同的小部件描述的字段。
   - **刷新周期(秒)** – 定义显示数据的刷新频率（时间间隔以秒为单位）。
   - **协议** – 指定应在小部件中显示其数据的协议。您可以像按"**协议**"列筛选数据表一样选择所需的协议。
   - **显示**– 定义显示数据的类型（对于允许您选择显示哪些数据的小部件）。
   - **数据源**– 定义安装了应用程序组件的节点，组件的数据显示在小组件中。如果选择了**整个应用程序**，小组件将显示来自所有节点的数据。
   - **监控点**– 定义所选节点用于显示数据的监控点。如果选择了**所有监控点**，小组件将显示所选节点的所有监控点的数据。
   - **根据状态更改颜色**– 如果选中此复选框，小部件的背景颜色将根据传入数据的严重性自动改变。红色背景表示数据的严重性至关重要（最大）。如果清除此复选框，则背景颜色被禁用。
   - **定义的背景**– 定义自定义小组件的背景颜色。您可以选择与严重性级别 (**信息**、**警告**或**严重**) 相对应的背景颜色，或选择**中性的**以禁用背景颜色。

- **显示模式**– 决定数据在小组件中的显示方式。您可以配置小部件以直方图或饼图显示数据。
- **考虑状态为"已解决"的事件** – 如果选择了**考虑状态为"已解决"的事件**，则小组件会显示所有事件的数据。
- **包括已修复和已接受的风险** – 如果选择**包括已修复和已接受的风险**，小部件将显示所有风险的数据。

4. 单击**确定**。

事件小组件中的信息

设备部分中的**控制板**小组件显示有关已知设备列表中包含的设备的信息。

该小组件提供以下信息：

- 每个类别中对于应用程序已知的设备数量的数据。该数据以类别图标的形式显示于小组件的上部。每个类别的图标下方标明了该类别的设备数量。如果设备列表包含有问题的设备，则会在这些设备的类别图标上显示警告图标。
- 有问题的设备类别列表。如果存在此类设备，则该数据将显示在小组件的中间部分。用于显示图形元素的空间受小组件的大小限制。

存在问题的设备

在下列任何情况下，应用程序确定设备需要引起注意：

- 设备的状态为*已授权*，安全状态不是*正常*。
- 设备具有"*未授权*"状态。

如果有出现问题的设备，则为列表中的每个类别显示以下信息：

- 包含类别图标、文本注释和包含有问题的设备数量的链接的行。
- 包含表示设备的图形元素的行。如果小部件中有足够的可用空间，则显示此行。行中的图形元素的数量取决于浏览器窗口的当前大小。如果出现问题的设备数量多于行中显示的图形元素数量，则隐藏设备的数量将以"+<设备数量>"的格式显示在右侧。

设备的图形元素

表示设备的图形元素包含以下信息：

- 设备名称。
- 设备状态。如果设备的状态为"*未授权*"，则显示为图标。
- 设备安全状态。这显示为图形元素左边框上的一条彩色线。线的颜色对应于"*正常*"、"*警告*"或"*严重*"状态。

图形元素按以下顺序显示：

1. 设备被分配“*未授权*”状态。
2. 带有“*严重*”安全状态的设备。
3. 带有“*警告*”安全状态的设备。

从小组件导航到其他部分

您可以使用**设备**小组件界面的元素导航到设备表并显示设备的详细信息。可以使用以下选项来实现此目的。

转到设备表并筛选表格

转到设备表并查看所选类别中的所有设备的信息：

在**设备**小组件的上部，单击相关类别的图标。

这将打开包含设备表的**资产**部分。该表将根据所选的设备类别进行筛选。

要前往设备表并查看具有特定类别问题的设备的信息：

在包含有问题设备的类别列表中，单击显示相关类别中设备数量的链接。此链接显示在行末，带有类别图标和**带有问题的**文本注释。

这将打开包含设备表的**资产**部分。该表将根据具有特定类别问题的设备的 ID 进行筛选。

> 设备表将根据您前往设备表时在**设备**小组件中显示的设备的 ID 进行筛选。切换到设备表后，筛选器设置不会更新。如果想查看当前有问题的设备数量，您可以再次转到**控制板**部分。

要转到设备表并查看有关有问题的设备的信息：

在**设备**小组件中，单击代表相关设备的图形元素。

这将打开包含设备表的**资产**部分。该表将根据设备 ID 进行过滤：

要转到设备表而不更改当前的表格筛选设置：

单击**显示所有设备**小组件中的**设备**。

这将打开包含设备表的**资产**部分。该表将显示满足设备表中先前定义的筛选设置的设备。

转到设备表并搜索表格

要转到设备表并在表中查找设备：

1. 在**设备**小组件中，在**搜索设备**字段中输入搜索查询。
2. 单击**搜索**。

这将打开包含设备表的**资产**部分。该表将显示符合搜索条件的设备。

事件小组件中的信息

事件部分中的**控制板**小组件显示有关事件和事故的一般信息，这些事件和事故具有上次发生的日期和时间的最新值。

该小组件显示以下元素：

- 选定时间段内的事件和事故的直方图。该数据显示在小组件的上部。直方图根据其严重级别显示事件和事故的分布情况。
- 包含已注册事件和事故信息的列表按上次发生的日期和时间排序。该数据显示在小组件的中间部分。

事件和事故统计

在显示事件和事故分布的直方图上，各列对应每个时间间隔的事件总数。在列中，事件和事故的严重性通过颜色区分。以下颜色对应严重级别：

- 蓝色。此颜色用于表示严重级别*低*的事件和事故。
- 黄色。此颜色用于表示*中*严重级别的事件和事故。
- 红色。此颜色用于表示*高*严重级别的事件和事故。

要显示有关直方图某列的信息，请将鼠标光标移到该列上。弹出窗口显示间隔的日期和时间以及按严重级别划分的事件和事故的数量。

时间间隔的持续时间取决于所选的显示时间段。您可以使用以下按钮选择生成直方图的相关时间段：

- **1h** — 一小时周期，分为一分钟的间隔。
- **12h** — 12 小时周期，分为一个小时的间隔。
- **24h** — 24 小时周期，分为一个小时的间隔。
- **7d** — 七天的时间，分为一天的间隔。

事件和事故列表

“**事件**”小部件中的事件和事故列表会实时更新。具有最后发生的日期和时间的最新值的事件和事故被放置在列表的开头。

事件和事故列表中显示的元素数量受小组件大小的限制。

为列表中的每个事件或事故提供以下信息：

- 事件或事故的标题。
- 最后发生的日期和时间
- 表示事件或事故严重级别的图标：
  - – *低*严重级别
  - – *中*严重级别
  - – *高*严重级别

列表中的事件用图标标记。

从小组件导航到其他部分

您可以使用**事件**小组件界面的元素转到事件表并显示有关事件和事故的详细信息。可以使用以下选项来实现此目的。

转到事件表并过滤表格

您可以通过单击**事件**小组件列表中的相关事件或事故来查看有关事件或事故的详细信息。这样做将打开**事件**部分，其中的表格将被根据所选事件或事故的 ID 进行过滤。从事件或事故登记的日期和时间到当前时刻的时间段（不指示该时间段的结束边界）也将为过滤器定义。

如果您想要继续前往事件表而不更改**事件**部分中的当前表格过滤器设置，请单击**显示所有事件**小组件中的**事件**。

转到事件表并搜索表格

要转到设备表并在表中查找设备：

1. 在**事件**小部件中，在**搜索事件**字段中输入您的搜索查询。
2. 单击**搜索**。

事件部分将打开。事件表显示符合搜索条件的事件和事故。

决定 EPP 应用程序小部件保护中如何考虑设备的条件

EPP 应用程序的保护小部件显示受 EPP 应用程序保护的设备数量以及可能受 EPP 应用程序保护的未受保护设备的数量。

如果 Kaspersky Industrial CyberSecurity for Networks 掌握了以下所有条件的信息，则该设备被视为受 EPP 应用程序保护，并被列入**具有活动 EPP 应用程序的计算机**列表中：

- 计算机上已安装 EPP 应用程序，并且该应用程序已配置为与 Kaspersky Industrial CyberSecurity for Networks 配合使用。
- 正在为 EPP 应用程序执行实时保护任务。
- EPP 应用程序与*集成服务器之间活动*活动连接。
- 该设备已被分配除*已存档*"状态之外的任何状态（仅在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 版本中考虑）。

如果设备未包含在受 EPP 应用程序保护的设备列表中，且未被分配"*已存档*"状态，并且满足以下条件之一，则该设备被视为未受 EPP 应用程序保护，并被列入"**没有 EPP 应用程序的计算机**"列表中：

- 该设备属于以下类别之一：
  - **服务器**
  - **工作站**
  - **HMI/SCADA**（仅在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 版本中考虑）
  - **工程工作站**（仅在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 版本中考虑）
- EPP 应用程序已将信息从此设备发送到集成服务器（仅在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 版本中考虑）。
- 设备信息会显示已安装的操作系统名称（任何版本的 Windows 操作系统名称）（Kaspersky Industrial CyberSecurity for Networks 4.5.1 版本不考虑此信息）。

移除小组件

要删除小部件：

1. 在**控制板**部分中，单击小组件右上角的⚙打开小组件管理窗口。
2. 在小部件管理菜单中，选择“**删除**”。
   将打开一个带有确认提示的窗口。
3. 在提示窗口中，确认删除所选的小部件。

资产管理

Kaspersky Industrial CyberSecurity for Networks 让您可以监控被视为公司资产的工业网络设备。要管理这些资产，您可以查看 Kaspersky Industrial CyberSecurity for Networks Web 界面的“资产**资产设备表**”。您还可以在使用网络交互图和拓扑图时查看有关设备之间交互的信息，并对设备执行各种操作。

设备表

创建设备表是为了在应用程序中进行资产管理。表中的所有设备被认为对应用程序已知。您可以在**资产**选项卡的**设备**部分中查看设备表。

设备表对元素数量有以下限制：

- *已授权*或*未授权*状态的设备总数不能超过 10 万台。
  如果达到*已授权*或*未授权*状态的设备的最大数量，则具有这些状态的新设备不会被添加到表中。如果是这种情况，要向表中添加新设备，您需要删除之前添加的设备之一。
- 状态为*已存档*的设备数量最多为 10 万台。
  如果达到具有 “*已存档*”状态的设备的最大数量，则具有此状态的新设备将被添加到表中，以替换最长时间没有显示任何活动的设备。

当设备表过满时，应用程序会显示相应消息。

设备表包含以下信息：

- **名称** — 应用程序中的设备的名称。
- **设备 ID** — Kaspersky Industrial CyberSecurity for Networks 中分配的设备 ID。

- **状态** — 资产状态，确定设备活动在工业网络中是否被允许。设备可以具有以下状态之一：
  - *已授权*。此状态分配给在工业网络中允许活动的设备。
  - *未授权*。此状态分配给工业网络中不允许活动的设备。
  - *已存档*。如果设备不再使用或不得在工业网络中使用，或者设备未显示任何活动且设备信息长时间（30 天或更长时间）未发生变化，则会为设备分配此状态。
- **地址信息** — 设备的 MAC 和/或 IP 地址。如果设备有多个网络接口，则您可以在不同的网络接口上为设备指定不同的 MAC 地址和/或 IP 地址（设备信息中最多可指示 512 个网络接口）。如果向应用程序添加了额外的地址空间，则可以在配置设备表时使用“**显示地址空间**”设置来启用或禁用地址空间名称的显示。当查看有关设备的信息时，有关设备的 MAC 和/或 IP 地址以及地址空间的信息将显示在**地址**选项卡上。
- **类别** — 确定设备功能用途的类别名称。Kaspersky Industrial CyberSecurity for Networks 支持以下类别的设备：
  - **PLC** — 可编程逻辑控制器。
  - **IED** — 智能电子设备。
  - **HMI/SCADA** — 安装了人机界面 (HMI) 系统或 SCADA 系统软件的计算机。
  - **工程工作站** — 安装了软件的计算机，供 ICS 工程师使用。
  - **服务器** — 安装了服务器软件的设备。
  - **网络设备** — 网络设备（例如路由器或交换机）。
  - **工作站** — 台式个人计算机或操作员工作站。
  - **移动设备** — 具有计算机功能的便携式电子设备。
  - **笔记本电脑** — 便携式个人计算机。
  - **HMI 面板** — 使用人机界面来管理单个设备或工业流程操作的设备。
  - **打印机** — 打印设备。
  - **UPS** — 连接到计算机网络的不间断电源装置。
  - **网络摄像头** — 执行视频监控功能并传输数字图像的设备。
  - **网关** — 通过转换使用不同数据传输介质和不同协议的网络内的各种接口（例如，串行/以太网）来连接网络的设备。
  - **存储系统** — 用于在存储系统中存储信息的设备。
  - **防火墙** — 执行防火墙功能以检查和阻止不需要的流量的设备。
  - **交换机** — 用于 LAN 节点之间的物理连接的设备。
  - **虚拟交换机** — 逻辑上合并物理交换机的设备，或用于虚拟化系统的软件实现的交换机。
  - **路由器** — 在计算机网络各段之间重定向网络数据包的设备。

- **虚拟路由器** — 逻辑上合并物理路由器的设备，或利用多个独立路由表的路由器。
- **Wi-Fi** — 为 Wi-Fi 网络的设备提供无线连接的访问点。
- **Historian 服务器** — 存档数据服务器。
- **其他** — 不属于上述类别的设备。

- **组** — 设备组树中包含设备的组的名称（包含组的名称及其所有父组的名称）。
- **安全状态** — 设备安全状态，由与设备链接的事件的存在决定。有以下安全状态可用：
  - *严重*。与设备相关的事件的严重程度等级为 8.0–10.0。
  - *警告*。与设备相关的事件的严重程度等级为 4.0–7.9。
  - *正常* 与设备相关的事件的严重性等级为 0.0–3.9，或者设备没有相关事件。
- **重要性** — 设备对企业的重要性。重要性根据设备类别分配。有以下设备重要性级别：
  - *高*。分配给以下类别的设备：**PLC**、**IED**、**HMI/SCADA**或**服务器**。
  - *中*。分配给以下类别的设备：**工程工作站**、**网络设备**、**工作站**、**HMI 面板**、**网关**、**存储系统**、**防火墙**、**交换机**、**虚拟交换机**、**路由器**、**虚拟路由器**、**Wi-Fi**或**Historian 服务器**。
  - *低*。分配给以下类别的设备：**移动设备**、**笔记本电脑**、**打印机**、**UPS**、**网络摄像头**或**其他**。
- **最后可见日期** — 设备最后一次活动注册的日期和时间。
- **风险** — 检测到的设备风险类别。默认情况下，设备表仅显示当前风险的信息。要显示所有风险的信息，请在配置设备表时选中“**显示已补救和已接受的风险**”复选框。
- **最后修改日期** — 上次修改设备信息的日期和时间。
- **创建日期** — 设备添加到设备表的日期和时间。
- **OS** — 设备上安装的操作系统的名称。
- **硬件提供商** — 设备硬件供应商的名称。在详细信息区域中，此设置被称为“**提供商**”，并显示在“**常规**”设置组中的“**硬件**”选项卡上。
- **硬件型号** — 设备型号名称。在详细信息区域中，此设置被称为“**型号**”，并显示在“**常规**”设置组中的“**硬件**”选项卡上。
- **硬件版本** — 设备硬件版本号。在详细信息区域中，此设置被称为“**版本**”，并显示在“**常规**”设置组中的“**硬件**”选项卡上。
- **软件提供商** — 设备软件供应商的名称。在详细信息区域中，此设置被称为“**提供商**”，并显示在“**常规**”设置组中的“**软件**”选项卡上。
- **软件名称** — 设备软件的名称。在详细信息区域中，此设置被称为“**名称**”，并显示在“**常规**”设置组中的“**软件**”选项卡上。
- **软件版本** — 设备软件版本号。在详细信息区域中，此设置被称为“**版本**”，并显示在“**常规**”设置组中的“**软件**”选项卡上。

- **网络名称** – 用于表示网络中的设备的名称。
- **标签** – 分配给设备的标签列表。
- **过程控制设置** – 指示是否为设备定义了过程控制设置。在详细信息区域中，为设备配置的"过程控制设置"显示在"**过程控制**"选项卡上。
- **EPP 应用程序** – 设备上安装的 EPP 应用程序的简洁名称（如果该应用程序的数据是在 Kaspersky Industrial CyberSecurity for Networks 中收到的）。
- **EPP 连接** – 集成服务器和设备上安装的 EPP 应用程序之间的连接状态。可使用以下状态：
  - *活动*。自应用程序和集成服务器上次连接以来过去不到 24 小时。
  - *不活动*。自程序和集成服务器上次连接以来超过 24 小时。
  - *N/A*。连接状态未知。
- **最后一次连接到 EPP** – 集成服务器和设备上安装的 EPP 应用程序之间的上次连接日期。

当查看设备表时，您可以使用配置、过滤、搜索和排序功能，并导航到相关项目。

查看设备信息

有关设备的详细信息包括来自设备表的信息以及以下字段（如果这些字段有值）：

- **路由器** – 路由设备指示器。

  如果路由器指示器没有自动确定，则必须手动设置，例如，对于执行工业网络段之间网络交换机功能的设备。该属性允许应用程序使用附加算法来检测通过路由器相互交互的设备。特别是，如果为连接具有多个 PLC 的段和具有 SCADA 系统的计算机段的网络交换机设置了路由器指示器（无论是自动还是手动），则应用程序能够检测并将第一段中的所有新设备添加到设备表中，这些新设备与第二段中具有 SCADA 系统的计算机进行交互。

- **附加信息** – 应用程序用户指定的有关设备的附加信息（例如，设备部署位置的描述）。
- **自定义字段** – 应用程序用户定义的一组非标准设备信息（例如，设备保护的类别和级别）。最多可以为一个设备指定 16 个自定义字段。
- **动态字段** – 采用设备信息检测方法时在流量中检测到的扩展设备信息集。如果应用程序检测到扩展信息，则会显示此字段。
- **Endpoint Agent**– 有关设备上端点代理软件组件的信息。
- **公钥**是在建立 SSH 连接和作为安全审计作业的一部分扫描设备之前用于设备验证的保存值。
- **网络行为** – 选项卡包含基于网络交互规则的设备控制信息、设备培训质量指标（检测到的交互是否符合活动允许规则）以及设备网络交互统计数据。
- **拓扑结构** – 选项卡包含有关最后一次主动轮询设备的信息，以及有关设备与其他节点的连接的信息。

- **设备** – 选项卡包含有关 BIOS 应用程序和设备处理器的信息、有关设备本地驱动器上的可用 RAM 和内存量的信息以及有关所使用的 USB 设备和光驱的信息。如果通过部件监控获得该信息，则会显示该信息。
- **配置** – 该选项卡包含有关收到的设备配置的信息。如果信息是配置控制作业的结果，则会显示该信息。

查看设备信息：

在“**设备**”部分的“**资产**”选项卡上，选择相关设备。

详细信息区域出现在 Web 界面窗口的右侧。详细信息区域会显示具有定义值的所有数据。

自动添加和更新设备

应用程序可以自动将设备添加到表中并更新有关设备的信息。要在 Kaspersky Industrial CyberSecurity for Networks 中自动添加和更新设备，您必须启用以下资产管理方法：

- 设备活动检测。使用此方法时，应用程序会根据获取的设备的 MAC 和/或 IP 地址将新检测到的设备添加到表中。如果应用程序检测到已知设备的活动，它可能会根据当前资产管理模式更改其状态。
- 设备信息检测。使用此方法时，应用程序会根据从流量或EPP 应用程序接收的数据更新有关已知设备的信息。根据从流量收到的数据，应用程序会更新在设备设置中为其启用了自动更新的信息（默认启用，直到应用程序用户手动更改值）。如果设备信息检测被禁用，应用程序将不会根据从流量或 EPP 应用程序收到的数据更新或扩充可用的设备信息。

添加设备时，应用程序会根据默认模板分配设备名称：**设备 <内部设备计数器的值>**。设备名称中的内部计数器的值可能与**设备 ID**列中显示的设备 ID 不同。

使用设备信息检测，应用程序可以在收到以下信息后更新设备名称：

- 设备型号名称。
- 用于在网络上表示设备的网络名称（更新期间设备的网络名称优先）。

应用程序可以根据设备的 MAC 地址自动更新与网络设备供应商相关的信息。为了根据 MAC 地址识别供应商，应用程序会将设备的 MAC 地址与国际电气电子工程师学会（IEEE）的公共数据库中注册的地址范围进行比较。如果网络部件供应商通过 MAC 地址识别，则应用程序将使用与 IEEE 数据库中显示的相同供应商名称。

应用程序安装后，它会使用 IEEE 数据库的副本，其中包含有关 MAC 地址和供应商的信息，信息在当前版本的应用程序发布时最新。您可以通过安装更新来使 IEEE 数据库的本地副本保持最新。

自动合并设备

应用程序可以将添加到设备表中的多台设备合并为一台设备。在学习模式下启用设备活动检测方法时，设备可以自动合并。

如果应用程序检测到一台设备的 MAC 地址与另一台设备的 IP 地址之间存在关联，则会自动合并这些设备。此外，还可以根据主动轮询的结果或从 EPP 应用程序接收的数据建立设备地址之间的链接。如果在合并设备上的数据中定义的值之间发生冲突，则新设备将保留为以下设备定义的值：

- 已保存 IP 地址的设备 – 如果检测到 IP 地址与另一设备的 MAC 地址之间存在关联。

  > 在启用学习模式之前（以及在此模式下工作时），如果设备可以自动与已定义 IP 地址的设备合并，则建议不要更改仅为其定义了 MAC 地址的设备的信息。

- 具有 IP 地址并安装了 Endpoint Agent 软件组件的设备 – 如果基于 EPP 应用程序的数据检测到与其他设备的关联。
- IP 地址最多的设备。
- 地址最多的设备 – 如果所有合并的设备都没有 IP 地址。

当设备合并时，合并设备的某些信息可能不会保存在新设备中（例如，动态字段和拓扑参数的内容）。

自动分配设备状态

当监控工业网络中设备的活动时，该应用程序可以根据获取的设备的 MAC 和/或 IP 地址自动为检测到的设备分配状态。状态根据当前资产管理模式予以指定。

在学习模式下，应用程序为所有检测到的设备分配*已授权*状态（包括新设备以及之前添加到设备表中的设备）。如果之前为检测到的设备分配了*未授权*状态，则其状态不会改变。

在监控模式下，分配的状态取决于显示活动的设备对于应用程序来说是已知还是未知。在此模式下，状态根据以下规则进行分配：

- 如果设备是新的（检测到时不在设备表中），则会为其分配*未授权*状态。
- 如果设备在设备表中且状态为*已授权*或*未授权*，则状态不会改变。
- 如果设备在设备表中的状态为*已存档*，则为该设备分配*未授权*状态。

默认情况下，如果状态为*已授权*的设备在 30 天内没有显示任何活动，并且设备信息在此期间没有发生变化，则会为该设备分配*已存档*状态。您可以禁用*手动更改设备状态已存档*已存档（例如，为了防止很少连接的设备自动将已*已授权*更改为*已存档*）。

Cisco 交换机连接器可能会自动限制处于“*未授权*”状态的设备的网络访问。为了避免由于状态变化而阻止必要的设备，请检查为此连接器类型定义的设置。

当设备表中出现状态为*未授权*的设备时，您需要确定这些设备是否都是工业流程支持所必需的。做出此确定后，建议为每个设备手动分配以下状态之一：

- *已授权*– 如果工业流程支持需要该设备。
- *已存档* – 如果设备不应在工业网络中使用。

> 您可以*删除该设备已存档*"已存档"状态。不过，该设备的所有指定信息也将被删除。如果再次检测到已删除的设备，应用程序将仅提供自该设备被重新添加到设备表以来收到的信息（首次检测到该设备的日期和时间也会更新）。

设备组树

设备组树用于根据设备的用途、位置或任何其他属性来排列设备。可以手动（例如，指定设备在设施的工业结构中的位置）或自动（基于设备 IP 地址的子网、根据设备类别或按供应商）将设备分组。

如果设备未添加到任何组中，则该设备将被分配到组树层次结构的顶层。默认情况下，自动添加到表中的设备不会被分组。

具有除操作员角色之外的任何角色的用户都可以将设备放置在组中。

查看设备表时，您可以找出哪些设备属于组。组的路径在**组**列中指明。设备组也显示在网络交互图上。但是，如果这些组中的设备不满足在网络交互图上过滤对象的设置，则可能不会显示。

监控设备的网络行为

对于应用程序已知的每个设备，您可以通过查看有关该设备的网络行为的信息来监控其网络活动。该信息显示在"**网络行为**"选项卡上的设备详细信息区域中。

小部件用于显示有关设备网络行为的信息。小部件中的数据以在线模式更新。

"**网络行为**"选项卡包含以下小部件：

- **网络交互控制**。在此小部件中，应用程序显示以下信息：
  - 根据交互控制规则监控设备网络交互的当前状态（*已启用*或*已暂停*）
  - 指定设备地址信息的交互控制规则的数量（总数、启用规则数、禁用规则数）。
- **学习质量**。在此小部件中，应用程序显示以下信息：
  - 检测到的设备交互与启用的交互控制规则的当前合规状态（*正常*或*检测到异常*）
  - 由于检测到的设备交互不符合启用的交互控制规则而注册的未处理事件的数量（总数、网络完整性控制 (NIC) 事件的数量、命令控制 (CC) 事件的数量）

- **网络统计数据**。在此小部件中，应用程序显示以下信息：
  - 设备接收的数据量。
  - 设备发送的数据量。
  - 活动网络会话的数量。

小部件中的某些定量值允许您导航到应用程序 Web 界面的相应部分。例如，您可以使用鼠标选择显示的网络会话数，以在“**网络会话**”选项卡上的“**网络地图**”部分中查看有关这些会话的详细信息。

为了清楚地显示“**网络交互控制**”和“**学习质量**”小部件中的当前状态，应用程序使用适当的颜色突出显示小部件左侧边框上的线条。当配置了交互控制时，这两个小部件左侧边框上的绿线表示应用程序正在监控设备的网络行为，并且所有检测到的交互都符合该设备当前的允许规则。

如果“**网络交互控制**”和/或“**学习质量**”小部件左侧边框上的线条颜色不是绿色，则需要检查此设备是否正常运行，并将其恢复到正常运行模式（如有必要）。例如，如果设备涉及预防性维护和调试操作，应用程序可能会根据网络完整性控制或命令控制技术注册事件，从而导致切换到“*检测到异常*”小部件中的“**学习质量**”状态。在这种情况下，您可以等到预防性和调试操作结束，然后设备将继续正常操作。

检查设备是否正常运行后，具有适当权限的用户可以执行以下操作：

- 要返回“*已启用*”小部件中的“**网络交互控制**”状态，请恢复监控以跟踪设备的网络交互。
- 要在“*正常*”小部件中返回“**学习质量**”状态，请完成设备学习或重置网络行为偏差。

正在重置设备网络行为的偏差

当交互控制技术在监控模式下运行时，只要检测到的设备之间的交互不符合启用的交互控制规则，应用程序就会注册事件。此类事件被视为设备*网络行为的偏差*。如果在注册事件时设备未处于正常运行模式（例如，当设备参与维护和调试操作时），则可以重置此设备的网络行为偏差。

重置网络行为偏差后，应用程序会将*已解决*状态分配给所有与选定设备相关的偏差事件。但是，允许规则不会根据这些事件自动创建。

您可以查看在监控设备网络交互时注册的未处理事件的数量信息。该信息显示在“**网络行为**”选项卡上的设备详细信息区域中。要查看有关已注册事件的详细信息，您可以使用“**学习质量**”小部件导航到事件表。

要重置设备网络行为的偏差：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**资产**”部分。
3. 在“**设备**”选项卡上，选择您要重置网络行为偏差的设备。
4. 右键单击打开上下文菜单。
5. 在上下文菜单中，选择“**重置异常**”。
   将打开一个带有确认提示的窗口。

6. 如果选定设备的网络行为偏差事件存在相关风险，并且您想要同时为所有这些风险分配*已接受*状态，请选中**为与事件相关的风险分配"已接受"状态**复选框。

7. 在提示窗口中，确认您要重置所选设备的网络行为偏差。

监控 PLC 项目的读写

Kaspersky Industrial CyberSecurity for Networks 可以监控工业网络流量以获取有关 PLC 项目的信息，并将此信息与之前收到的有关 PLC 项目的信息进行比较。

PLC 项目是为 PLC 编写的微程序。PLC 项目存储在 PLC 内存中，并作为使用 PLC 的工业过程的一部分运行。PLC 项目可能由块组成，这些块在读取或写入项目时通过网络单独传输和接收。

当应用程序检测到从 PLC 读取项目/块或将项目/块写入 PLC 的操作时，它可能会收到有关 PLC 项目/块的信息。获取的信息保存在 Kaspersky Industrial CyberSecurity for Networks 中。下次检测到项目/块写入或读取操作时，应用程序会将收到的有关项目/块的信息与保存的信息进行比较。如果收到的项目/块的信息与该项目/块的最新保存的信息不匹配（包括没有保存的信息时），应用程序会注册相应的事件。

以下设备类支持接收有关 PLC 项目的信息：

- Emerson DeltaV
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- Siemens SIPROTEC 4 系列

您不需要添加设备的过程控制设置来监控 PLC 项目的读/写。对所有检测到的所列设备类监控 PLC 项目的读/写。

对于每个设备，该应用程序保存不超过 100 种不同的 PLC 项目变体。如果 PLC 项目通过单独的块进行传输或接收，则每个块最多可保存 100 种不同的变体。

如果设备已达到保存的 PLC 项目（或具有相同名称的 PLC 项目块）的最大数量，则应用程序将保存新检测到的项目/块来代替最旧的项目/块。

在监控 PLC 项目的读/写时，应用程序根据资产管理技术注册事件。这些事件使用被分配了以下代码的系统事件类型进行注册。

- 读取 PLC 项目/块时的事件类型代码：
  - 4000005200 – 检测到从 PLC 读取了项目的未知块（如果没有保存有关此块的信息）。
  - 4000005201 – 检测到从 PLC 读取了项目的已知块（如果保存了有关此块的信息，但获取的信息与有关此块的最新保存的信息不匹配）。

- 4000005204 – 检测到从 PLC 读取了未知项目（如果没有保存有关此项目的信息）。
- 4000005205 – 检测到从 PLC 读取了已知项目（如果保存了有关此项目的信息，但获取的信息与有关此项目的最新保存的信息不匹配）。

- 项目/块写入 PLC 时的事件类型代码：
  - 4000005202 – 检测到将项目的新块写入 PLC（如果没有保存有关此块的信息）。
  - 4000005203 – 检测到将项目的已知块写入 PLC（如果保存了有关此块的信息，但获取的信息与有关此块的最新保存的信息不匹配）。
  - 4000005206 – 检测到将新项目写入 PLC（如果没有保存有关此项目的信息）。
  - 4000005207 – 检测到将已知项目写入 PLC（如果保存了有关此项目的信息，但获取的信息与有关此项目的最新保存的信息不匹配）。

您可以在“**设置**” → “**事件类型**”下配置“事件类型”的可用设置。

当通过 Web 界面连接到服务器时，您可以查看有关已注册事件的信息。

监控 OT 设备部件

Kaspersky Industrial CyberSecurity for Networks 可以监控专用 OT 设备（例如 PLC）上用于自动化流程的部件。以下设备类支持部件监控：

- Emerson DeltaV
- Rockwell Automation Allen-Bradley ControlLogix 系列
- Rockwell Automation Allen-Bradley CompactLogix 系列
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- 基于 CODESYS V3 平台的 PLC（例如 Prosoft-Systems Regul R500）

应用程序通过**主动轮询**连接器接收有关 OT 设备部件的信息。将连接器添加到应用程序后，您可以在运行以下类型的安全审计作业时使用这些连接器获取信息：

- 配置控制作业。如果您想使用“**存档版本**”或“**与黄金配置进行比较**”配置过程以获取有关连接到 OT 设备的部件的信息，我们建议使用此作业类型。要获取部件信息，请在**添加配置控制作业**时选择 PLC 设备类型。
- 主动轮询作业。如果您希望从提供的主动轮询方法中获取更多信息以及部件信息，我们建议您采用这种作业类型。要获取有关 OT 设备部件的信息，请选择“**工业设备扩展配置**”，然后在添加主动轮询作业时根据所选设备选择获取高级配置的适当方法。

作为配置控制或主动轮询作业的一部分扫描 OT 设备后，应用程序会更新设备的部件信息。添加设备或更改设备信息时禁用自动更新的信息不会更新。对于某些部件详细信息，禁用自动更新的功能不可用。

监控 OT 设备部件有助于应用程序获取下表列出的信息。

监控 OT 设备部件时获取的信息

信息类型	显示在设备详细信息区域的选项卡上	能够禁用自动更新
插槽中模块的图形布局	**设备**	—
各模块详细信息	**设备**、**配置**	—
以密钥条目和密钥值形式表现的高级设备信息，例如内存状态和设备安全设置	**设备**、**配置**	—
PLC 项目和项目块的详细信息	**配置**	—
硬件提供商	**常规**	✓
硬件模型	**常规**	✓
硬件版本	**常规**	✓
软件版本	**常规**	✓

除了上面列出的信息之外，存储在中央处理单元 (CPU) 模块中的日志内容也可以下载到应用程序中。如果设备连接了多个 CPU 模块，则会下载 Kaspersky Industrial CyberSecurity for Networks 连接器所连接的模块的特别日志。您可以使用设备详细信息区域中“**设备**”选项卡上的链接下载包含设备日志的文件。

监控 Windows 和 Linux 设备部件

Kaspersky Industrial CyberSecurity for Networks 可以监控运行 Windows 和 Linux 的设备上的部件。在监视部件时，应用程序会自动接收有关设备部件的信息，并在部件或其特性发生变化时注册事件。

Windows 和 Linux 设备上的部件监控取决于设备上是否存在端点代理以及 EPP 应用程序与 Kaspersky Industrial CyberSecurity for Networks 之间是否正在建立整合。因此，要使用部件监控功能，请准备应用程序以从 EPP 应用程序接收数据。但是，必须在集成服务器节点上启用用于设备活动检测和设备信息检测的资产管理方法。

Windows/Linux 部件信息每天更新一次。添加设备或更改设备信息时禁用自动更新的信息不会更新。对于某些器材详细信息，禁用自动更新的功能不可用。

Windows 和 Linux 部件监控可帮助应用程序获取下表列出的信息。

通过监控 Windows 和 Linux 设备上的部件获得的信息

信息类型	显示在设备详细信息区域的选项卡上	能够禁用自动更新
处理器	**设备**	—
BIOS	**设备**	—
RAM	**设备**	—

信息类型	显示在设备详细信息区域的选项卡上	能够禁用自动更新
本地驱动器	**设备**	—
光盘驱动器	**设备**	—
USB 设备	**设备**	—
具有 MAC 地址的网络接口	**地址**	✓
硬件提供商	**常规**	✓
硬件模型	**常规**	✓
硬件版本	**常规**	✓

在监控 Windows 和 Linux 设备上的部件时，应用程序通过资产管理记录事件。这些事件使用被分配了以下代码的系统事件类型进行注册。

- 4000005015 – 用于添加、更改或删除以下任何类型信息的事件：
  - 处理器
  - BIOS
  - RAM
  - 本地驱动器
  - 光盘驱动器
  - USB 设备
- 4000005008 – 用于接收有关网络接口的新信息的事件。
- 4000005004 – 用于接收有关供应商、型号或硬件版本的新信息的事件。

您可以在“设置**设置**事件类型**事件类型配置事件类型的可用设置**。

当通过 Web 界面连接到服务器时，您可以查看有关已注册事件的信息。

监控设备用户

Kaspersky Industrial CyberSecurity for Networks 可以监控其已知设备上的用户账户。在监控用户时，它会自动接收这些设备的操作系统中注册的账户信息。应用程序使用这些详细信息来创建用户表。

收到账户详细信息后，该应用程序会使用此信息监控设备上的所有用户账户，但某些只能由操作系统服务使用的本地系统账户除外。例如，该应用程序不控制 Windows 操作系统设备上使用的 LocalSystem 和 NetworkService 账户。

要使用用户监控功能，必须启用设备活动检测和设备信息检测的资产管理方法。必须在安装了从其接收信息的应用程序组件的所有节点上启用这些方法。

用户监控依赖于以下来源类型的数据：

1. **OVAL 扫描**：根据内置 OVAL 规则扫描设备的软件组件，例如 EPP 应用程序可根据需求将扩展的设备数据发送到 Kaspersky Industrial CyberSecurity for Networks，或安装了应用程序组件的节点，这些节点在作为配置监控作业的一部分扫描设备时远程连接到设备。

2. **遥测 (Endpoint Agent)**：将设备和正在运行的进程的基本数据（遥测数据）发送到 Kaspersky Industrial CyberSecurity for Networks 的 EPP 应用程序。

3. **流量**：监控点，根据用于识别设备信息的规则和设备之间的通信协议分析传入的流量。

4. **外部源**：使用 Kaspersky Industrial CyberSecurity for Networks API 并向 Kaspersky Industrial CyberSecurity for Networks 发送用户详细信息的应用程序。

这些来源按其数据优先级的降序排列。在处理用户详细信息时，应用程序遵循数据源优先级。来自较高优先级来源的用户详细信息可以覆盖来自其他来源的信息。应用程序还会自动从表中删除先前从**外部源**和 **OVAL 扫描**接收其详细信息，但这些信息在从这些源接收的新数据中不存在的用户账户。

如果需要，具有管理员或安全官角色的用户可以手动删除用户账户。

您可以在**资产**选项卡的**用户**"部分查看有关用户的信息。查看用户表时，您可以配置、过滤、搜索和排序记录，以及导航到相关项目。

所有用户表限制为 200000 个项目。

应用程序在表格和所选用户的详细信息区域中显示以下设备用户详细信息：

- **用户 ID**：Kaspersky Industrial CyberSecurity for Networks 中分配的用户标识符
- **用户名**：不指定设备域或网络名称的用户账户名
- **全名**：指定设备域名或网络名称的用户账户名
- **组**：用户账户所属的用户组的名称
- **设备**：设备名称和地址
- **源**：用户数据源类型
- **SID**：用户安全标识符
- **账户状态**：反映接收到的启用和禁用账户使用的参数值的状态
- **锁定**：反映已接收到的账户锁定参数值的状态
- **下次登录时更改密码**：指示用户下次登录时是否需要重置密码的标志
- **阻止用户更改密码**：指示是否禁止用户更改密码的标志
- **密码有效期**：反映收到的密码到期启用/禁用值的状态
- **数据接收日期**：上次收到账户详细信息的日期和时间
- **描述**：为账户设置的描述

在监控用户时，应用程序使用资产管理技术进行事件记录。这些事件是使用分配了代码 4000005600 的系统事件类型进行注册的。当设备上的用户账户自动添加、修改或删除时，会记录事件。

您可以在"设置**设置**事件类型**事件类型配置事件类型的可用设置**。

当通过 Web 界面连接到服务器时，您可以查看有关已注册事件的信息。

监控设备应用程序和补丁

Kaspersky Industrial CyberSecurity for Networks 可以监控其已知设备上安装的应用程序和补丁。在监控应用程序和补丁时，它会自动接收有关在设备操作系统中安装和注册的软件的信息。应用程序使用这些详细信息来生成应用程序和补丁表。

要使用应用程序和补丁监控功能，必须启用设备活动检测和设备信息检测的资产管理方法。必须在安装了从其接收信息的应用程序组件的所有节点上启用这些方法。

应用程序和补丁监控依赖于以下来源类型的数据：

1. **OVAL 扫描**：根据内置 OVAL 规则扫描设备的软件组件，例如 EPP 应用程序可根据需求将扩展的设备数据发送到 Kaspersky Industrial CyberSecurity for Networks，或安装了应用程序组件的节点，这些节点在作为配置监控作业的一部分扫描设备时远程连接到设备。

2. **外部源**：使用 Kaspersky Industrial CyberSecurity for Networks API 并向 Kaspersky Industrial CyberSecurity for Networks 发送应用程序和补丁详细信息的应用程序。

这些来源按其数据优先级的降序排列。在处理应用程序和补丁详细信息时，应用程序遵循数据源优先级。来自较高优先级来源的应用程序和补丁详细信息可以覆盖来自其他来源的信息。应用程序还会自动从表中删除那些之前已收到其详细信息的应用程序和补丁，但此类应用程序或补丁并不存在于从这些来源收到的新数据中。

您可以在下表中查看应用程序和补丁的详细信息：

- "**资产**"选项卡上"**应用程序**"下的所有应用程序表。

  该表显示有关应用程序已接收其数据的所有应用程序的信息。查看所有应用程序表时，您可以配置、过滤、搜索和排序，以及导航到相关项目。

- **资产**选项卡上**补丁**下的所有补丁表。

  该表显示有关应用程序已接收其数据的所有补丁的信息。查看所有补丁表时，您可以配置、过滤、搜索和排序，以及导航到相关项目。

所有应用程序和所有补丁表限制为各 200000 个项目。

应用程序在表格和所选应用程序的详细信息区域中显示以下设备应用程序详细信息：

- **应用程序 ID**：Kaspersky Industrial CyberSecurity for Networks 中分配的应用程序标识符
- **名称**：应用程序名称
- **提供商**：应用程序供应商名称
- **设备**：设备名称和地址
- **源**：应用程序数据源类型

- **已安装**：应用程序安装的日期和时间
- **大小**：应用程序文件使用的磁盘空间量
- **版本**：应用程序版本号
- **数据接收日期**：上次收到应用程序详情的日期和时间
- **描述**：为应用程序设置的描述

应用程序在表格和所选补丁的详细信息区域中显示以下设备补丁详细信息：

- **补丁 ID**：Kaspersky Industrial CyberSecurity for Networks 中分配的补丁标识符
- **名称**：补丁名称
- **产品**：修补的软件产品的名称
- **版本**：补丁版本号
- **提供商**：补丁供应商名称
- **设备**：设备名称和地址
- **源**：补丁数据源类型
- **已安装**：补丁安装的日期和时间
- **数据接收日期**：上次收到补丁详细信息的日期和时间
- **描述**：为补丁设置的描述

在监控应用程序和补丁时，应用程序使用资产管理技术进行事件记录。这些事件是使用分配了以下代码的系统事件类型进行注册的。

- 4000005601：用于应用程序添加或删除事件
- 4000005602：用于补丁添加或删除事件

您可以在"设置**设置**事件类型**事件类型配置事件类型的可用设置**。

当通过 Web 界面连接到服务器时，您可以查看有关已注册事件的信息。

启动设备上的可执行文件的控制

Kaspersky Industrial CyberSecurity for Networks 可以控制应用程序已知的设备上可执行文件的启动。可执行文件启动的监控依赖于来自 EPP 应用程序或使用 Kaspersky Industrial CyberSecurity for Networks API 的应用程序的数据。应用程序使用接收到的数据来创建可执行文件表。

带有 Endpoint Agent 的设备可以自动接收有关可执行文件启动的数据，Endpoint Agent 与 EPP 应用程序通信并将设备和正在运行的进程的基本数据（遥测数据）发送到 Kaspersky Industrial CyberSecurity for Networks。应用程序指定该数据的**遥测 (Endpoint Agent)**源。如果仅从使用 Kaspersky Industrial CyberSecurity for Networks API 的应用程序接收有关可执行文件运行的数据，则应用程序会将此文件的数据源值设置为**外部源**。

要从**遥测 (Endpoint Agent)**源接收有关可执行文件运行的数据，必须启用资产管理方法来检测设备活动和设备信息。必须在安装了接收 EPP 应用程序信息的应用程序组件的所有节点上启用这些方法。

可执行文件表对于元素的数量和存储时间有如下限制：

- 可执行文件总数不能超过 10 万个。

  如果达到最大可执行文件数量，应用程序会自动删除 10% 的最旧记录。

- 可执行文件在收到该文件的下一次执行数据之前的最长存储时间不能超过 90 天。

  如果在最大存储时间到达之前没有收到有关可执行文件运行的新数据，应用程序将自动删除有关该文件的条目。

如果需要，具有管理员或安全官角色的用户可以手动删除可执行文件。

您可以在“**可执行文件**”部分的“**资产**”选项卡上查看有关可执行文件的信息。查看可执行文件表时，您可以配置、过滤、搜索、排序和导航到相关项。

应用程序在表格和所选文件的详细信息区域中显示以下设备可执行文件的详细信息：

- **文件 ID**：Kaspersky Industrial CyberSecurity for Networks 中分配的文件标识符。
- **设备**：设备名称和地址。
- **名称**：应用程序名称和版本，或文件名。
- **数据接收日期**：上次收到文件详细信息的日期和时间。
- **产品**：设备操作系统中保存的软件产品名称。
- **产品版本**：设备操作系统中保存的软件产品版本。
- **提供商**：应用程序供应商的名称。
- **路径**：文件的完整路径。
- **文件大小**：文件使用的磁盘空间量。
- **MD5 哈希**：使用 MD5 哈希算法得到的文件校验和。
- **SHA256 哈希**：使用 SHA256 哈希算法得到的文件校验和。
- **签名**是文件数字签名验证的结果。它要么**有效**（如果数字签名验证成功），要么**无效**（例如，如果证书已过期）。
- **创建日期**：文件创建的日期和时间。
- **更改时间**：文件最后修改的日期和时间。
- **源**：文件数据源类型。
- **属性**：文件属性列表。
- **描述**：文件的描述集。

设备配置控制

Kaspersky Industrial CyberSecurity for Networks 提供了查看配置控制作业所获得的设备配置信息的功能。您可以在"配置**配置设备详细信息区域**中查看有关所选设备的配置的信息。

应用程序在表中的"**配置**"选项卡上显示有关收到的所选设备的配置的以下信息：

- **配置类型** – 收到的配置类型的名称（例如，"**用户**"，其中存储了有关设备用户的信息）。
- **接收的最后配置** – 如果启用了显示上次接收的配置，则显示上次接收配置类型的日期和时间。
- **接收的黄金配置** – 如果启用了显示黄金配置，则为收到黄金配置的日期和时间。
- **配置总数** – 配置控制作业期间获得的类型配置总数。该计数包括潜在的重复配置数据，这些数据可能仅随时间戳而变化。

黄金配置类型以皇冠图标 标记。

当您选择一个配置类型时，您将看到一个包含有关该类型的详细信息的窗口。

为了方便查看设备配置信息，您可以使用 Kaspersky Industrial CyberSecurity for Networks 比较已保存的配置。

在控制设备配置时，应用程序使用资产管理技术进行事件记录。这些事件使用被分配了以下代码的系统事件类型进行注册。

- 4000005603 – 根据设备扫描结果与以前的配置进行比较时检测到变化的事件（对于在**仅更新**和/或**存档版本**配置处理模式下运行的作业）。
- 4000005604 – 根据设备扫描结果与黄金配置进行比较时检测变化的事件（对于在**与黄金配置进行比较**处理模式下运行的作业）。

您可以在"设置**设置**事件类型**事件类型配置事件类型的可用设置**。

当通过 Web 界面连接到服务器时，您可以查看有关已注册事件的信息。

保存的设备配置比较

根据作为配置控制作业一部分的设备扫描结果，应用程序可以保存每个设备收到的配置。使用设备表时，您可以比较已保存的设备配置。

与设备配置控制的更改检测和事件注册算法不同，当使用比较已保存配置的功能时，您可以比较任何已保存的设备配置（而不仅仅是将最后收到的配置与之前或黄金配置比较）。如果设备存储了运行作业后捕获的配置，则此选项可用。

比较设备配置时，请记住应用程序收到的配置会保留一段有限的时间，并会在新配置进入时自动删除。删除频率取决于输入的数据量和频率。只有黄金和最后收到的配置不会被自动删除。如果需要，具有除操作员角色之外的任何角色的用户都可以将任何已保存的配置设置为黄金配置。

要比较已保存的设备配置：

1. 在“**设备**”部分的“**资产**”选项卡上，选择相关设备。

   详细信息区域出现在 Web 界面窗口的右侧。

2. 在“**配置**”选项卡的详细信息区域中，选择具有所需配置类型的表行，例如存储用户数据的“**用户**”。选定类型在“**配置总数**”列中的值必须至少为 2。

   您将看到一个窗口，其中包含有关所选配置类型的详细信息。

3. 单击“**比较**”。

   您将看到一个窗口，其中包含所选配置类型与之前或黄金配置的比较结果。收到比较配置的日期和时间显示在窗口上部。

4. 执行以下操作：

   - 要与另一个已保存的配置进行比较，请从下拉列表中选择收到所需配置的日期和时间。
   - 如果需要，可更改所比较配置的相对位置。为此，请使用日期和时间下拉列表之间的按钮。
   - 如果有必要，可禁用比较配置中未修改块的显示。

使用网络交互图

网络交互图是工业网络中设备之间检测到的通信的直观表示。您可以使用网络交互图查看不同时间段内设备之间的通信信息。

以下对象可能会显示在网络交互图上：

- 节点。这些对象指定网络数据包的源和目的地。
- 设备组。这些对象与设备组树中的组相对应。组包含代表设备和嵌入在这些组中的子组的节点。
- 链接。这些对象表示节点之间的连接。

节点和链接根据特定时间间隔内从流量或 EPP 应用程序接收的数据出现在网络交互图上。设备组连续显示。

如果需要，您可以过滤节点和链接。默认情况下，网络交互图以一小时的定义过滤期实时显示对象。

在网络交互图上，可以直观地区分存在问题的对象。该应用程序认为以下对象存在问题：

- 节点，如果与此节点关联的未处理事件得分为 4.0 或更高，或者此节点代表状态为“*未授权*”的设备。
- 连接，如果与此连接相关的事件得分为 4.0 或更高。在定义的对象过滤期间内注册的事件将被考虑在内。然而，事件的当前状态并未被考虑在内。
- 包含有问题的设备或其节点的链接有问题的组。这包括组内以及所有嵌套级别的任何子组内的对象。

网络交互图上的节点

网络交互图上的节点可以是以下类型：

- 应用程序已知的设备。这种类型的节点代表设备表中列出的设备。
- 应用程序已知的设备。此类节点代表具有唯一 IP 地址或 MAC 地址（不在设备表中）的设备。例如，如果使用 `ping` 命令将网络数据包发送到不存在的设备的地址，则这样的节点可能会出现在网络交互图上。如果未知设备对应的节点总数不超过 100 个（根据网络交互图上当前的过滤器设置），则会单独显示。如果节点数超出此限制，则会显示一个未知设备的合并节点。
- WAN。这种类型的节点代表工业网络设备所连接的广域网的设备。WAN 设备是其 IP 地址仅属于**应用程序已知的公共**公共子网的任何设备。

显示的代表设备的节点信息

当网络交互图最大化时，将显示已知设备对应的节点的以下信息：

- 分配的设备名称。
- 设备类别图标。
- 设备的 IP 地址（如果未分配 IP 地址，则显示 MAC 地址）。
- 各种图标取决于对以下条件的满足：
  - 如果设备设置了路由器指示灯。
  - 如果设备上安装了 EPP 应用程序（图标的颜色取决于连接状态）。
  - 如果设备具有“*已存档*”状态。
- 根据设备的安全状态，节点左边框上的粗线具有以下颜色之一：
  - 绿色表示“*正常*”安全状态。
  - 黄色表示“*警告*”安全状态。
  - 红色表示“*严重*”安全状态。

如果设备的状态为*未授权*或安全状态与*正常*不同，则节点的背景为红色。

表示未知设备的节点上显示的信息

当网络交互图最大化时，将显示与未知设备对应的节点的以下信息：

- 如果节点代表一个未知设备，则会显示该设备的 IP 地址或 MAC 地址。对于未知设备的合并节点（组合了 100 个以上未知设备的节点），显示“**未知设备**”。
- 未知设备及其状态的图标 。

表示应用程序未知的设备的节点具有灰色背景。

WAN 节点上显示的信息

当网络交互图最大化时，将显示 WAN 节点的以下信息：

- 节点名称：**WAN**。
- WAN 节点图标。

网络交互图上的设备组

属于设备组树的组可以在网络交互图上折叠或展开。折叠的组显示为类似于节点的图标。扩展的组显示为包含其嵌入节点和其他组的窗口。

显示的折叠组的信息

如果某个组被折叠，则当网络交互图最大化时会显示以下信息：

- 组名称。
- 网络交互图上满足当前过滤设置的设备数量。此数量包括组内及其子组内所有嵌套级别的设备。
- 所有嵌套级别中的子组的数量。

如果某个组包含有问题的设备或链接（包括在任何嵌套级别的子组中），则该组的边框为红色。

显示的扩展组的信息

扩展组的窗口包含一个带有组名的标题和一个用于显示对象的区域。组窗口显示该组中包含的设备，以及下一嵌套级别的子组。在组中包含的设备中，只有符合当前过滤设置的设备才会显示在网络交互图上。

如果某个组包含有问题的设备或链接（包括在任何嵌套级别的子组中），则窗口会显示红色背景。

折叠和扩展组

如果某个组处于折叠状态，您可以通过双击该组的图标来展开它。如果某个组已展开，您可以通过双击该组窗口的标题或单击标题中的 按钮来折叠它。

要同时展开多个折叠的组：

1. 在网络交互图上，通过执行以下操作之一选择多个折叠组：
   - 按住 **SHIFT** 键并使用鼠标选择包含相关组的矩形区域。
   - 按住 **CTRL** 键并使用鼠标选择相关折叠组。
2. 点击位于网络交互图显示区域左侧的工具栏中的 （如果选择了至少一个折叠组，则该按钮可用）。

要同时折叠所有展开的组：

点击位于网络交互图显示区域左侧的工具栏中的 （如果至少展开了一个组，则该按钮可用）。

网络交互图上的链接

根据检测到的网络数据包来识别网络交互图上的链接，可以将该网络数据包的源地址和目标地址映射到节点的地址。

每个链接都显示了通信的两方。链接中的通信方可能是网络交互图上的下列对象之一：

- 以下类型节点之一：
  - 应用程序已知的设备。
  - 应用程序已知的设备。
  - 未知设备的合并节点 – 如果链接显示与该节点的一个或多个未知设备的通信。
  - WAN 节点 – 如果链接显示通信中网络数据包的来源是 WAN 设备（IP 地址仅属于**应用程序已知的公共**公共网络）。
- 折叠组，如果链接显示与此组中一个或多个设备的通信。

根据检测到通信时注册的事件的分数，链接可能具有以下颜色之一：

- 灰色 – 通信未导致事件注册，或仅注册了分数为 0.0–3.9 的事件。
- 红色 – 通信导致注册分数为 4.0–10.0 的事件。

在定义的对象过滤期间内注册的事件将被考虑在链接中。然而，事件的当前状态并未被考虑在内。

应用程序会将连接数据保存在服务器的数据库中。保存的条目总量不能超出定义的限制。如果数量超出定义的限制，应用程序会自动删除 10% 的最旧条目。在服务器节点上配置数据存储设置时，您可以设置网络交互图的最大体量限制。

查看对象的详细信息

有关网络交互图上显示的对象的详细信息显示在详细信息区域中。要显示详细信息，您可以使用鼠标选择一个对象（如果要查看有关某个组的信息，则必须先折叠该组）。

将显示节点的以下信息：

- 如果节点表示已知设备，则详细信息区域显示与在设备表中显示的信息相同的信息。
- 如果一个节点代表一个未知设备，则详细信息区域将显示该设备的 MAC 地址和/或 IP 地址（如果向应用程序添加了其他地址空间，则包括地址空间的名称）。
- 如果选择了未知设备的合并节点，则会显示以下信息：
  - 当前过滤设置下此节点所组合的节点数。
  - **IP 地址** – 未知设备的 IP 地址数量和前 100 个 IP 地址（如果向应用程序添加了额外的地址空间，则包括地址空间的名称）。如果未知设备的节点中存在具有 IP 地址的节点，则会显示此部分。
  - **MAC 地址** – 未知设备的 MAC 地址数量和前 100 个 MAC 地址（如果在应用程序中添加了额外的地址空间，则包括地址空间的名称）。如果未知设备的节点中存在具有 MAC 地址的节点，则会显示此部分。

显示组的以下信息：

- **父组** – 设备组树中组的路径。如果组属于顶级层次结构，则显示**N/A (这是一个顶级组)**。
- 选定组及其所有嵌套级别的子组内的设备和组的数量。
- 有关所选组及其所有嵌套级别的子组中存在问题的对象数量的信息。如果不存在这样的对象，则显示“*正常*”安全状态。

对于链接，将显示以下信息：

- **严重性** – 对应与链接相关的事件的最高严重性级别的图标。如果没有与链接关联的事件，则显示“**无事件**”。在定义的对象过滤期间内注册的事件将被考虑在内。然而，事件的当前状态并未被考虑在内。
- 包含有关通信第一方和第二方的基本信息的部分：
  - 如果通信方是已知设备的节点或未知设备的节点，则该部分显示设备/设备的名称或地址、类别和地址信息（对于已知设备，仅为通信期间使用的网络接口提供地址信息）。还显示已知设备的设备状态。
  - 如果通信方是一个折叠组，则该部分会显示该组的名称以及其中的设备和子组的数量。
  - 如果通信方是未知设备的合并节点，则该部分将显示**未知设备**节点名称和该节点内组合的节点数。
- **协议** – 包含用于通信的协议列表的部分。为每个协议指定了针对检测到的网络数据包计算的传输数据量。如果通信一方是未知设备的合并节点，则不显示此部分。

改变网络交互图的比例

网络交互图可以按 1–100% 的比例显示。当前比例值显示在位于网络交互图显示区域左侧的工具栏中。

要更改网络交互图的比例，请执行以下操作：

使用鼠标滚轮或位于当前比例值旁边工具栏中的 **+** 和 **–**按钮。

减小网络交互图的比例会减少显示节点和折叠组的信息量。

如果显示比例小于 25%，则不会在节点和折叠组中显示图标和文本信息。节点和折叠组的外观可能会发生如下变化：

- 在表示应用程序（设备）已知的设备的节点上，右上角以以下颜色之一的三角形显示设备状态：
  - 绿色表示设备处于“*已授权*”状态。
  - 红色表示设备处于“*未授权*”状态。
  - 灰色表示设备处于“*已存档*”状态。
- 节点左边框的一条粗黑线出现在 WAN 节点上。
- 在折叠组中，右上角会显示一个三角形，表示存在问题的对象。三角形具有以下颜色之一：
  - 绿色表示该组不包含有问题的对象。
  - 红色表示该组包含有问题的对象。

定位网络交互图

如有必要，您可以手动或自动更改网络交互图的位置。自动定位使您能够移动网络交互图并更改其比例以显示满足定义的过滤器设置的所有节点以及所有扩展组。

要手动定位网络交互图：

1. 将鼠标光标放置在网络交互图上未被对象占据的任何部分上。
2. 单击并按住鼠标左键拖动网络交互图。

要自动定位网络交互图：

点击网络交互图显示区域左侧工具栏中的  按钮。

网络交互图的定位和比例将发生变化，以显示所有节点和扩展组。

固定和取消固定节点和组

默认情况下，节点和折叠组未固定在网络交互图上。未固定的节点和折叠组可以自动排列，以实现其他对象的最佳显示。

当手动改变节点和组的位置或自动排列时，节点和组将被固定。您还可以固定显示对象的当前位置而不移动它们。

要在不移动对象的情况下固定和取消固定对象，您可以使用以下界面元素：

- 网络交互图显示区域左侧工具栏中的按钮。您可以使用 和 按钮固定和取消固定网络交互图上显示的所有节点和组（包括扩展组中的节点）。
- 扩展组的窗口标题中的按钮。您可以使用 和 按钮仅固定和取消固定扩展组窗口中的节点和组（但不用于嵌套组的窗口）。

如果网络交互图包含可以应用相应操作的对象，则这些按钮可用。

固定节点或折叠组的位置后， 图标出现在该元素的右上角（如果网络交互图的比例不小于 25%）。您还可以使用此图标取消固定对象。

保留固定节点或固定组的位置。如果固定节点从网络交互图中消失（例如，由于过滤），则该节点下次出现时将显示在同一位置。

手动更改节点和组的位置

您可以以最方便的方式排列网络交互图上的节点和组，手动更改它们的位置。

排列完成后，节点和组将固定在新位置。如有必要，您可以取消固定这些对象。

包含在组中的对象只能在这些组的窗口内移动。

要更改节点和/或折叠组的位置：

1. 在网络交互图上，选择一个或多个与节点和/或折叠组相对应的对象。
   要选择多个节点和/或折叠组，请执行以下操作之一：
   - 按住 **SHIFT** 键并使用鼠标选择包含相关对象的矩形区域。
   - 按住 **CTRL** 键并使用鼠标选择相关对象。
2. 使用鼠标将选定的对象拖动到所需的位置。

移动后，节点和折叠组将保持固定状态。 图标出现在这些对象中。

要更改展开组的位置：

将光标移到扩展组的窗口标题上，单击左键并将窗口拖动到所需的位置。

自动排列节点和群组

为了在网络交互图上实现对象的最佳排列，您可以使用算法自动更改节点和组的位置（排列）。提供以下算法：

- 径向排列。
- 网格对齐排列。

您可以对以下对象使用自动排列算法：

- 组树中层次结构顶层的所有显示节点和组。使用位于网络交互图显示区域左侧的工具栏中的 （径向排列）按钮和 （网格对齐排列）按钮进行自动排列。
- 扩展组内显示的所有节点和组。自动排列通过使用扩展组窗口标题中的 （径向排列）按钮和 （网格对齐排列）按钮执行。
- 仅选定的节点和折叠组。执行自动排列之前，您需要在展开的组内或层次结构的顶层选择至少三个节点和/或折叠组。要选择多个对象，您可以在按住 **SHIFT** 键的同时用鼠标选择包含相关对象的矩形区域，或者在按住 **CTRL** 键的同时用鼠标选择相关对象。使用位于网络交互图显示区域左侧的工具栏中的 （径向排列）按钮和 （网格对齐排列）按钮进行自动排列。

自动排列后，节点和组将被锁定（固定）在新的位置。 图标出现在这些对象中。如有必要，您可以取消固定这些对象。

搜索网络地图上的节点

您可以根据有关节点的信息在网络交互图上搜索这些节点。此搜索将涉及符合当前过滤器设置的所有节点，包括那些位于折叠组中或网络交互图的显示部分之外的节点。

对于表示已知设备的节点，将在设备表的所有列中执行搜索，但“**状态**”、“**安全状态**”、**最后可见日期**”、“**最后修改日期**”和“**创建日期**”除外。搜索也在设备的自定义字段的值中执行。

要查找网络交互图上的节点：

在“**网络地图**”部分中，在“**搜索节点**”字段中输入搜索查询。当您在搜索字段中键入字符时，将启动搜索。

如果找到满足搜索查询的节点，这些节点的轮廓将以黄色突出显示。发现节点的折叠组的轮廓以相同的方式突出显示。同时，“**搜索节点**”字段的右侧将显示以下项目：

- 搜索结果中当前选定的对象（节点或包含找到的节点的折叠组）的序列号。
- 找到的对象总数（节点和/或包含找到的节点的折叠组）。

  折叠组中的节点数不计入找到的对象总数。如果您希望组中的节点也计入搜索结果中，请展开折叠组。

- 用于在找到的对象之间移动的箭头。箭头移动按找到的对象名称的字母顺序进行。当移动到下一个对象时，网络交互图会自动定位以显示此对象。

过滤网络交互图上的对象

本节提供有关过滤网络交互图上的对象以限制显示的节点和链接数量的说明。

节点和链接的全面过滤

本节包含有关节点和链接全面过滤的说明。

使用时间尺度上的时间段进行过滤

要过滤节点和链接，您可以在时间尺度上选择相关的时间段。时间尺度显示在“**网络交互图**”部分的“**网络地图**”选项卡的下部。

时间尺度包含以下项目：

- 时间尺度开始日期和时间。
- 注册了分数为 4.0 及以上的事件的时间段。这些时间段在时间尺度的下部显示为红色条纹。如果时间尺度定义的持续时间超过七天，则不会显示时间段。
- 过滤时间段。此时间段显示为一条黄色带，内有用于移动边界的按钮。
- 应用程序处理的流量图表。如果时间尺度定义的持续时间超过七天，则不会显示图表。
- 时间尺度的结束。根据过滤时间段的安排，时间尺度的结束显示为日期和时间（如果定义了日期和时间）或“**现在**”链接。

提供以下类型的过滤时间段：

- 与当前时刻相关的时间段。该时间段的右侧边界对应于表示当前时刻的时间尺度边界。
- 时间段与当前时刻无关。此类型的时间段可安排在时间尺度的任意部分。

要按与当前时刻相关的时间段配置对象过滤：

1. 单击时间尺度右侧的**现在**。如果该时间段已经与当前时刻相关，则不会显示此按钮。
2. 如果需要指定不同的时间段长度，请执行以下操作之一：
   - 将时间段黄色带的左边界移动到必要的位置（时间段的最长持续时间为 7 天）。
   - 单击时间段黄色带上方的按钮打开配置窗口，选中**锚定到边界**复选框，选择必要的持续时间（**小时**、**天**或**7 天**），然后单击**确定**。

网络交互图仅显示自指定时间段开始到当前时刻检测到通信的节点和链接。

要配置按与当前时刻不相关的时间段进行过滤：

1. 如果必要时间段不在时间尺度内，请更改时间尺度的开始和/或结束日期和时间的值：

   a. 要更改时间尺度的开始日期和时间，请单击时间尺度左侧的链接打开窗口，然后选择以下选项之一：

   - **天**。
   - **7 天**。
   - **30 天**。
   - **指定日期**。对于此选项，请在打开的字段中指定日期和时间。

   b. 要更改时间尺度结束的日期和时间，请单击时间尺度右侧的链接打开窗口，然后选择以下选项之一：

   - **现在**。
   - **指定日期**。对于此选项，请在打开的字段中指定日期和时间。

2. 指定必要的时间段。为此，请执行以下操作之一：

   - 使用鼠标将时间段移动到时间尺度上的相关位置。
   - 将时间段黄色带的一条或两条边框移动到时间尺度的必要部分（时间段的最长持续时间为 7 天）。
   - 单击时间段黄色带上方的按钮打开配置窗口，选择必要的持续时间（**小时**、**天**或 **7 天**），然后单击“**确定**”。

3. 如果某个时间段被自动锚定到当前时刻（将时间段移动到最右边的位置时，时间尺度右侧的**现在**按钮不再显示），请禁用将时间段自动锚定到时间尺度边界的功能。为此，请单击时间段黄色带上方的按钮打开配置窗口，清除**锚定到边界**复选框，然后单击**确定**。

按已注册事件进行过滤

您可以配置网络交互图以显示与所选节点相关的事件中保存其信息的节点和链接。

如果在网络交互图上选择的节点不超过 200 个，则可以按事件进行过滤。您可以单个选择相关节点，也可以将其作为包括相关设备的折叠组的一部分进行选择。如果选择了折叠的组，则任何嵌套级别的子组中的所有设备也将被包括在设备选择中。

您可以使用以下方法按事件进行过滤：

- 按事件进行初步过滤。如果您需要根据仅与选定节点相关的事件来过滤对象，则可以应用此方法。
- 按事件进行额外过滤。如果已经执行了按事件进行的初步过滤（例如，从事件表切换到网络交互图时），并且您还需要从网络交互图上显示的节点列表中过滤与另外选择的节点相关的事件，则应用此方法。

要使用按事件进行的初步过滤来显示节点和链接：

1. 在网络交互图上，选择一个或多个与节点和/或折叠组相对应的对象。

要选择多个节点和/或组，请执行以下操作之一：

- 按住 **SHIFT** 键并使用鼠标选择包含相关对象的矩形区域。
- 按住 **CTRL** 键并使用鼠标选择相关对象。

2. 在网络交互图上方的工具栏中，打开“**事件过滤器**”下拉列表。
3. 在下拉列表中，选择**过滤器**。

网络交互图仅显示与所选节点相关的事件中包含其信息的节点和链接。位于网络交互图上方的工具栏显示一个包含事件 ID 的列表（ID 按检测到其相关事件的顺序列出）。

要使用按事件进行的附加过滤将节点和链接添加到显示的对象：

1. 确保已执行了按事件进行的初步过滤。为此，请检查网络交互图上方的工具栏中是否有包含事件 ID 的列表。
2. 在网络交互图上显示的节点中，选择您想要向过滤器添加关联事件的节点。

   详细信息区域出现在 Web 界面窗口的右侧。
3. 在网络交互图上方的工具栏中，打开“**事件过滤器**”下拉列表。
4. 在下拉列表中，选择“**添加到过滤器**”。

网络交互图还显示与所选节点相关的事件中包含其信息的节点和链接。检测到的事件的 ID 被添加到工具栏中包含 ID 的列表中。

节点过滤

本节提供有关过滤节点的说明。

按设备状态过滤节点

要按设备状态过滤节点：

1. 在网络交互图上方的工具栏中，打开“**设备状态**”下拉列表。

   您将看到一个列表，其中包含已知设备状态的名称（*未授权*、*已授权*和*已存档*）以及应用程序未知的设备的“*未知设备*”状态。
2. 在下拉列表中，选中需要在网络交互图上显示的设备状态的复选框。
3. 单击“**确定**”。

网络交互图仅显示与所选状态的设备相对应的节点。

按设备安全状态过滤节点

要按设备安全状态过滤节点：

1. 在网络交互图上方的工具栏中，打开“**设备状态**”下拉列表。
   您将看到一个列表，其中包含设备的安全状态名称（“*正常*”、“*警告*”和“*严重*”）。
2. 在下拉列表中，选中需要在网络交互图上显示的节点的安全状态的复选框。
3. 单击**确定**。

网络交互图仅显示与所选安全状态的设备相对应的节点。

按设备类别过滤节点

要按设备类别过滤节点：

1. 在网络交互图上方的工具栏中，打开“**设备类别**”下拉列表。
   您将看到一个列表，其中包含已知设备的类别名称，以及未知设备和 WAN 节点的各自类别。
2. 在下拉列表中，选中需要在网络交互图上显示的设备类别的复选框。
3. 单击“**确定**”。

网络交互图仅显示与所选类别的设备相对应的节点。

启用和禁用与过滤节点关联的节点的显示

过滤节点后，网络交互图仅显示满足定义的过滤设置的节点。此外，要使节点显示在网络交互图上，它必须与另一个显示的节点有连接（链接）。如果根据指定的过滤参数，网络交互图未显示与某个节点交互的任何节点，则该节点也不会显示在网络交互图上。对于属于未知设备合并节点的节点，也同样应用过滤：如果网络地图未显示与未知设备节点交互的所有节点，则该节点将被从未知设备合并节点内的节点列表中删除。

如有必要，您可以启用网络交互图来显示与过滤节点相关的所有节点。除了满足定义的节点过滤标准的节点之外，网络交互图还显示这些节点与之有交互的所有节点（无论定义的过滤器设置如何）。

例如，如果按 **PLC** 类别过滤节点，并且您启用了链接节点的显示，则网络交互图将显示所有与 **PLC** 类别设备通信的节点。如果禁用链接节点的显示，网络交互图将仅显示与已相互通信的 **PLC** 类别设备相对应的节点。

要启用或禁用与已过滤节点关联的节点的显示：

使用位于网络交互图上方工具栏中的“**链接的设备**”切换开关。

过滤链接

本节提供有关过滤链接的说明。

按严重性分数过滤链接

要按关键性分数过滤网络交互图上的链接：

1. 在网络交互图上方的工具栏中，打开“**链接的分数**”下拉列表。

   显示的列表包含事件严重性级别的名称及其分数范围（低（0.0-3.9）、中（4.0-7.9）、高（8.0-10.0））以及“**无事件**”元素，其允许您过滤未注册事件的连接。

2. 在下拉列表中，选中您要用于过滤链接的严重性级别的复选框。

3. 单击**确定**。

网络交互图仅显示与具有所选严重性级别的事件相关的链接。

按通信协议过滤链接

要按通信协议过滤网络交互图上的链接：

1. 在网络交互图上方的工具栏中，打开“**协议**”下拉列表。

   您将看到一个窗口，其中包含以协议堆栈树形式显示的受支持协议表。您可以使用包含后续层协议的协议名称旁边的**+**和**-**按钮来管理树元素的显示方式。

   表列提供以下信息：

   - **协议** – 协议栈树中协议的名称。
   - **以太网类型** – 以太网协议中下一级协议的编号（如果协议有定义的编号）。它以十进制格式显示。
   - **IP 编号** – IP 协议中下一级协议的编号（如果协议有定义的编号）。它仅针对 IP 协议结构内的协议进行指示。它以十进制格式显示。

2. 如有必要，请使用表格上方的搜索字段查找相关协议。

3. 在协议列表中，选中您要用来过滤事件的协议旁边的复选框。

   如果选中或清除包含嵌套协议的协议的复选框，则也会自动选中或清除嵌套协议的复选框。

4. 单击**确定**。

网络交互图仅显示使用所选协议的链接。

按 OSI 模型层过滤链接

您可以根据与网络协议栈的 OSI (Open Systems Interconnection) 模型的各层相对应的通信级别来过滤链接。

要根据 OSI 网络模型的层次过滤网络交互图上的链接，请执行以下操作：

1. 在网络交互图上方的工具栏中，打开“**OSI 模型层**”下拉列表。

您将看到一个包含 OSI 模型层名称的列表：

- **数据链路**。该层包括使用 MAC 地址与设备进行通信的通信链路。
- **网络**。该层包括使用 IP 地址与设备通信的链接。

2. 在下拉列表中，选中其链接需要在网络交互图上显示的 OSI 模型层的复选框。
3. 单击**确定**。

交互网络图仅显示与所选 OSI 模型层相关的链接。

重置过滤器设置

您可以将过滤节点和链接的已定义设置重置为其默认状态。

要重置网络交互图上定义的过滤器设置，请执行以下操作：

在网络交互图上方的工具栏中，单击“**默认过滤器**”（如果已定义过滤器设置，则会显示此按钮）。

网络交互图将显示在指定时间段内检测到通信的所有节点和链接。

保存和加载网络交互图显示设置

本节介绍网络交互图显示自定义功能。

应用程序允许您保存当前的网络交互图显示设置。一组保存的显示设置称为*视图*。您可以使用视图应用保存的网络交互图的显示设置（例如，在进行某些更改后快速恢复显示设置，或在不同计算机上使用网络交互图）。

当保存了网络交互图视图时，会保存以下显示设置：

- 刻度
- 网络交互图定位
- 固定节点和组的位置
- 节点和链接的过滤

应用程序可以为不同的网络交互图视图保存和使用不超过 10 组设置。

所有用户都可以管理网络交互图视图列表（包括保存当前显示设置）。

添加新视图，同时保存当前网络交互图显示设置

要在保存当前网络交互图显示设置的同时添加新视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，配置网络交互图的显示设置。
3. 单击“**管理视图**”打开“**配置网络地图视图**”窗口。
4. 单击“**添加**”。
5. 在输入字段中输入视图名称。
   您可以使用字母、数字、空格和以下特殊字符：`! @ # № $ % ^ & ( ) [ ] { } ' ; , . - _`。
   视图名称必须满足以下要求：
   - 必须以空格以外的任何允许的字符开始和结束。
   - 必须包含 100 个字符或更少。
   - 不得与不同视图的名称匹配（不区分大小写）。
6. 点击输入字段右侧的 ✓ 图标。

在保存当前网络交互图显示设置的同时更新视图

要在保存当前网络交互图显示设置的同时更新视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，配置网络交互图的显示设置。
3. 单击“**管理视图**”打开“**配置网络地图视图**”窗口。
4. 选择要保存当前网络交互图显示设置的视图。
5. 单击“**覆盖**”。
   将打开一个带有确认提示的窗口。
6. 在提示窗口中，确认您要保存所选视图中的当前设置。

重命名网络交互图视图

要重命名网络交互图视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**网络交互图**”部分中的“**网络地图**”选项卡上，通过单击“**配置网络地图视图**”按钮打开“**管理视图**”窗口。
3. 选择要重命名的视图。
4. 点击当前视图名称右侧的 图标。
5. 在输入字段中，输入视图的新名称。
   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`
   视图名称必须满足以下要求：
   - 必须以空格以外的任何允许的字符开始和结束。
   - 必须包含 100 个字符或更少。
   - 不得与不同视图的名称匹配（不区分大小写）。
6. 点击输入字段右侧的 图标。

删除网络交互图视图

要删除网络交互图视图：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**网络交互图**”部分中的“**网络地图**”选项卡上，通过单击“**配置网络地图视图**”按钮打开“**管理视图**”窗口。
3. 选择要删除的视图。
4. 单击**删除**。
   将打开一个带有确认提示的窗口。
5. 在提示窗口中，确认删除所选视图。

在网络交互图上应用保存的视图设置

要在网络交互图上应用保存的视图设置：

1. 在“**网络交互图**”部分中的“**网络地图**”选项卡上，通过单击“**配置网络地图视图**”按钮打开“**管理视图**”窗口。
2. 在列表中选择相关视图。

3. 单击“**应用**”。
   将打开一个带有确认提示的窗口。

4. 在提示窗口中，确认视图的应用。

使用网络交互图时下载流量

使用网络交互地图时，您可以通过监控点下载应用程序接收的流量。流量被下载到 PCAP 文件中。您可以配置网络包过滤来下载相关数据。

应用程序从流量转储文件存储下载流量。每个节点的内部存储（在节点上安装应用程序组件时自动创建）和外部存储（如果连接在节点上）都可以用于下载流量。

流量转储文件临时存储在存储中，并在收到新流量时自动删除。文件删除的频率取决于收到的流量以及指定的应用程序数据存储设置。如果从存储库中删除相应的流量转储文件，则无法下载流量。

要在使用网络交互图时下载流量：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

2. 在“**网络交互图**”部分的“**网络地图**”选项卡上，单击“**下载流量**”。
   详细信息区域出现在 Web 界面窗口的右侧。

3. 执行以下操作：

   - 要下载特定时间段内的流量，请使用“**要下载的流量周期**”设置定义所需的边界。
     默认情况下，周期设置为为按时间刻度指定的过滤配置的周期。

   - 在“**下载量限制**”部分设置用于下载流量的最大量的限制。
     如果下载的流量超过指定的限制，则稍后到达的流量将被跳过。

   - 如有必要，在“**按监控点过滤**”部分中启用过滤，并指定接收所需流量的监控点。
     默认情况下，会指定已安装应用程序组件的节点上可用的所有监视点。

   - 如有必要，请在“**按地址空间过滤**”部分中启用过滤，并指定网络数据包中的地址所属的地址空间（如果向应用程序添加了其他地址空间，则会显示此部分）。
     默认情况下，指定应用程序中创建的所有地址空间。

   - 如有必要，请在“**使用 BPF 进行过滤**”部分启用过滤，并根据网络数据包的地址设置使用 Berkeley Packet Filter (BPF) 技术输入过滤表达式。

     过滤表达式示例

     ```
     tcp port 102 or tcp port 502
     ```

   - 如有必要，请在“**使用正则表达式进行过滤**”部分中启用过滤，并输入根据网络数据包中的负载数据进行过滤的表达式。

     过滤表达式示例

     ```
     ^test.+xABxCD
     ```

4. 单击“**下载**”。

5. 如果创建文件的时间较长（超过 15 秒），则文件创建操作将转入后台操作列表。在这种情况下，要下载文件：

   a. 点击应用程序 Web 界面菜单中的 按钮。

   出现后台操作列表。

   b. 等待文件生成操作完成。

   c. 单击“**下载文件**”。

您的浏览器将保存下载的文件。根据您的浏览器设置，屏幕可能会显示一个窗口，您可以在其中更改已保存文件的路径和名称。

网络会话监控

Kaspersky Industrial CyberSecurity for Networks 可以检测设备创建的用于与工业网络流量中的其他设备连接的网络会话。当检测到网络会话时，应用程序会注册这些会话并保存相关信息。与网络交互图上的连接不同，注册的网络会话提供有关设备交互的更详细信息，包括因为在交互中使用的不同端口和协议的会话的单独注册。

在分析监控点接收到的流量以及从 EPP 应用程序接收数据时，可以执行网络会话检测。每个注册的网络会话都包含有关作为交互方的两个设备之间的连接的信息。网络会话的特征是交互方的地址信息（MAC 和/或 IP 地址）、端口号以及用于连接的应用协议。网络会话中的第一个设备通常是发起向其他设备发送网络数据包的设备。

保存的网络会话信息可以用于分析设备的网络活动，包括通过使用网络异常检测规则。网络异常检测规则分析可利用网络会话中保存的协议属性（应用程序支持保留 DCE/RPC、DNS、Kerberos 和 LDAP 协议的属性）。您还可以从流量转储文件中下载有关已传输网络数据包的数据。

如果启用以下方法，应用程序将注册网络会话并保存信息，以便分析设备的网络活动：

- 利用资产管理技术进行网络会话检测。
- 利用过程控制技术获取协议属性。

如果在该会话内一分钟内没有发送网络数据包，或者在相应节点或监控点上禁用了网络会话检测技术，则认为该网络会话已完成。

如果检测到过多的网络会话，应用程序将应用以下会话注册限制：

- 使用同一应用协议的交互双方的注册会话数不超过每分钟 1000 个
- 交互双方的注册会话总数不超过每分钟 5000 次

应用程序将网络会话数据保存在服务器上的数据库中。保存的条目总量不能超出定义的限制。如果数量超出定义的限制，应用程序会自动删除 10% 的最旧条目。在“**网络会话**”部分的服务器节点上配置数据存储设置时，您可以设置网络会话的最大数量限制。

您可以在“**网络地图**”部分的“**网络会话**”选项卡上查看有关网络会话的信息。

网络会话表

网络会话表显示在“**网络地图**”部分的“**网络会话**”选项卡上。

网络会话表包含以下信息：

- ID 是 Kaspersky Industrial CyberSecurity for Networks 中分配的网络会话标识符。
- **状态** – 网络会话状态。注册的网络会话可以具有以下状态之一：
  - **活动**。此状态是在注册网络会话时分配的，并且只要该会话中的设备发送网络数据包，该状态就会保留。
  - **已关闭**。如果在该会话内一分钟内没有发送网络数据包，或者在相应节点或监控点上禁用了网络会话检测技术，则将该状态分配给该网络会话。
- **端 1** – 第一个网络交互面的 MAC 和/或 IP 地址。MAC 和 IP 地址可以启用和禁用。
- **端 1 端口** – 交互第一面的端口号。
- **端 2** – 第二网络交互面的 MAC 和/或 IP 地址。MAC 和 IP 地址可以启用和禁用。
- **端 2 端口** – 交互第二面的端口号。
- **设备 1** – 第一交互面的地址信息对应的应用程序已知的设备名称。
- **设备 2** – 第二交互面的地址信息对应的应用程序已知的设备名称。
- **传输协议** – 网络会话中使用的传输协议。
- **应用程序协议** – 网络会话中使用的应用层协议。
- **当前速度** – 网络会话中的当前数据传输速率。
- **平均速度** – 网络会话中的平均数据传输速率。
- **传输总量** – 网络会话中传输的字节数。
- **监控点** – 接收网络会话流量的监控点的名称。
- **启动** – 网络会话中第一个网络数据包的日期和时间或从 EPP 应用程序接收数据的时间间隔的开始日期和时间。
- **上次交互** – 网络会话中最后一个网络数据包的日期和时间或从 EPP 应用程序接收数据的时间间隔的到期日期和时间（如果网络会话中仅接收到一个数据包，则该值与“**启动**”值相同）。
- **数据包数** – 网络会话中传输的网络数据包数量。

当查看网络会话表时，您可以使用配置、过滤、搜索和排序功能，导航到相关项目，以及导出数据。

将网络会话导出为 JSON 格式时，该文件还包含提取的协议属性列表（应用程序可以使用网络异常检测规则中的 SQL 查询来分析这些属性）。

查看网络会话详细信息

有关网络会话的详细信息包括来自网络会话表的信息以及以下字段（如果这些字段有值）：

- 在**设置**选项卡上的**应用程序**：网络会话启动时正在运行的应用程序的名称。
- 在**属性**选项卡上包含协议属性的文本字段：网络会话中接收到的协议属性列表（应用程序可以使用网络异常检测规则中的 SQL 查询对其进行分析）。

要查看有关网络会话的信息：

在“**网络地图**”部分的“**网络会话**”选项卡上，选择所需的网络会话。

详细信息区域显示在 Web 界面窗口的右侧部分。详细信息区域显示所有收到的有关网络会话的信息。

下载网络会话流量

查看网络会话表时，您可以下载与所选网络会话相关的流量。流量被下载到 PCAP 文件中。您可以配置网络包过滤来下载相关数据。

应用程序从流量转储文件存储下载网络会话流量。节点的内部存储（在节点上安装应用程序组件时自动创建）和外部存储（如果连接在节点上）都可以用于下载流量。

下载网络会话流量时，请考虑以下注意事项：

- 仅对于在分析监控点接收到的流量期间注册的网络会话才可以下载流量。如果网络会话是基于从 EPP 应用程序接收到的数据注册的，则应用程序无法下载该会话的流量。
- 流量转储文件临时存储在存储中，并在收到新流量时自动删除。文件删除的频率取决于收到的流量以及指定的应用程序数据存储设置。如果从存储库中删除相应的流量转储文件，则无法下载网络会话流量。

要下载网络会话流量：

1. 通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 在“**网络地图**”部分的“**网络会话**”选项卡上，选择要下载流量的网络会话。

   您可以选择不超过 100 个网络会话。
3. 单击**下载流量**。

   详细信息区域出现在 Web 界面窗口的右侧。
4. 执行以下操作：

   - 要下载特定时间段内的流量，请使用“**要下载的流量周期**”设置定义所需的边界。

     默认情况下，指定最大可能的时间段，从最早网络会话的开始日期和时间到所选会话中最新会话的结束日期和时间。如果需要，您可以在该时间段内设置边界，或者将其中一个边界设置为空值（例如，让右侧边界下载尚未完成的会话的新流量）。

- 在“**下载量限制**”部分设置用于下载流量的最大量的限制。

  如果下载的流量超过指定的限制，则稍后到达的流量将被跳过。

- 如有必要，在“**按监控点过滤**”部分中启用过滤，并指定接收所需流量的监控点。

  默认情况下，指定接收所选网络会话流量的监控点。

- 如有必要，请在“**按地址空间过滤**”部分中启用过滤，并指定所选网络会话的网络数据包中的地址所属的地址空间（如果向应用程序添加其他地址空间，则会显示此部分）。

  默认情况下，指定应用程序中创建的所有地址空间。

- 如有必要，在“**使用 BPF 进行过滤**”部分启用过滤，并根据所选网络会话的网络数据包的地址设置，使用 Berkeley Packet Filter (BPF) 技术输入过滤表达式。

  过滤表达式示例

  ```
  tcp port 102 or tcp port 502
  ```

- 如有必要，请在“**使用正则表达式进行过滤**”部分中启用过滤，并输入用于根据所选网络会话的网络数据包中的负载数据进行过滤的表达式。

  过滤表达式示例

  ```
  ^test.+xABxCD
  ```

5. 单击“**下载**”。

6. 如果创建文件的时间较长（超过 15 秒），则文件创建操作将转入后台操作列表。在这种情况下，要下载文件：

   a. 点击应用程序 Web 界面菜单中的 按钮。

   出现后台操作列表。

   b. 等待文件生成操作完成。

   c. 单击“**下载文件**”。

您的浏览器将保存下载的文件。根据您的浏览器设置，屏幕可能会显示一个窗口，您可以在其中更改已保存文件的路径和名称。

监控事件和突发事件

在分析工业网络流量时，应用程序会记录事件和事故。

Kaspersky Industrial CyberSecurity for Networks 中的*事件*是一个条目，其中包含有关检测工业网络流量中需要 ICS 安全官注意的某些变化或条件的信息。事件会被注册并传输到 Kaspersky Industrial CyberSecurity for Networks 服务器。服务器会处理收到的事件并将其保存在数据库中。

*突发事件*是一种特殊类型的事件，在收到特定序列的事件时会被注册。事故对具有某些共同特征或与同一过程相关的事件进行分组。

应用程序根据事件关联规则注册突发事件。*事件关联规则*描述了检查事件序列的条件。当应用程序检测到与规则条件匹配的事件序列时，它会注册一个突发事件，指示触发规则的名称。突发事件使用分配了代码 8000000001 的系统事件类型进行注册。

事件关联规则嵌入在应用程序中，无论安全策略如何都会应用。

安装后，应用程序使用默认的事件关联规则。为了提高规则的有效性，卡巴斯基专家会定期更新包含规则集的数据库。您可以通过安装更新来更新关联规则。

Kaspersky Industrial CyberSecurity for Networks 服务器根据为注册事件类型定义的设置来注册事件和突发事件。您可以在事件类型部分（针对所有事件类型）以及配置过程控制规则时（仅针对触发过程控制规则时注册的事件）配置这些设置。

为了减少不需要操作员注意的频繁重复事件的数量，您可以创建事件允许规则。满足允许规则的事件不会被注册。例如，您可以使用允许规则暂时禁用来自特定监控点的所有事件的注册。您可以在**允许规则**部分中查看事件的允许规则。为这些规则指明了 EVT 类型。

应用程序会将事件和突发事件保存在服务器的数据库中。保存的条目总量不能超出定义的限制。如果数量超出定义的限制，应用程序会自动删除 10% 的最旧条目。如果启用了最短存储时间限制，并且应用程序删除了存储时间小于定义限制的条目，则应用程序消息日志中会出现相应的消息。您可以配置存储事件和突发事件的设置。

数据库文件保存在服务器上的DBMS 文件夹中。删除或修改这些文件夹中的任何文件可能会导致应用程序性能中断。

您可以在 Kaspersky Industrial CyberSecurity for Networks 网页界面的以下部分中查看有关事件和突发事件的信息：

- **控制板**部分显示有关应用程序注册的最新事件和突发事件的一般信息。
- **事件和突发事件**部分的**事件**选项卡显示有关事件和突发事件的详细信息，并允许从服务器数据库下载任何时期的信息。

事件的分数和严重性

Kaspersky Industrial CyberSecurity for Networks 中的事件和事故的评分范围是 0.0 到 10.0。

如果某个事件与某个设备相关联，应用程序会根据有关该设备的可用信息计算分数的数值。在这种情况下计算分数时，应用程序会考虑设备的重要性级别以及与该设备相关的风险。

计算分数的起始值是*事件类型表*中为特定事件类型定义或在配置过程控制规则时定义的基本分数（仅针对过程控制规则被触发时注册的事件）。

如果事件未与设备链接，则该事件的分数等于基础分数。

该分数决定了事件的严重级别。根据分数的数值，事件可能具有以下严重性之一：

- *低*（分数 0.0–3.9）

  低严重性的事件通常不需要立即响应。

- *中*（分数 4.0–7.9）

  中严重性的事件包含需要引起注意的信息。这些事件可能需要作出响应。

- *高*（分数 8.0–10.0）

  高严重性的事件包含可能对工业过程产生重大影响的信息。这些事件需要立即作出响应。

为了确保与应用程序先前版本中使用的事件*严重性级别*兼容，Kaspersky Industrial CyberSecurity for Networks 的当前版本将这些严重性级别转换为以下分数：

- 具有*信息*严重性的事件的分数为 3.0。
- 具有*警告*严重性的事件的分数为 6.0。
- 严重性为*严重*的事件的分数为 9.0。

事件注册技术

Kaspersky Industrial CyberSecurity for Networks 基于以下技术之一注册事件：

- *是深度包检测*(DPI)

  该技术用于记录与过程违规相关的事件（例如，超过指定温度的事件）。

- *网络完整性控制*(NIC)

  该技术用于记录与工业网络完整性或通信安全性相关的事件（例如，通过对工业网络设备而言是新协议的设备之间的通信检测事件）。

- *入侵检测*(IDS)

  该技术用于注册与流量异常检测相关的事件（例如，检测 ARP 欺骗迹象的事件），这些事件是攻击迹象。

- *命令控制*(CC)

  该技术用于注册与流量中的设备系统命令检测相关的事件（例如，检测未经授权的系统命令的事件）。

- *外部*(EXT)

  该技术用于 Kaspersky Industrial CyberSecurity for Networks 使用 Kaspersky Industrial CyberSecurity for Networks API 方法从接收系统接收到的突发事件和事件。

- *资产管理*(AM)

  该技术用于注册与在流量中或从 EPP 应用程序接收的数据中检测设备信息相关的事件（例如，检测设备新 IP 地址的事件）。

- *端点保护平台*(EPP)

  该技术用于注册与卡巴斯基应用程序检测到的威胁相关的事件，这些应用程序执行保护工作站和服务器的功能（例如，恶意软件检测事件）。

事件状态

事件和事故的状态使应用程序能够显示 ICS 安全官处理信息的进展。

可以为事件和事故分配以下状态：

- *新的*

  当所有事件和事故在 Kaspersky Industrial CyberSecurity for Networks 中注册时，都会被分配此状态。

- *进行中*

  您可以将此状态分配给当前正在处理（进行中）的事件和事故，例如，在调查注册这些事件和事故的原因时。

- *已解决*

  您可以将此状态分配给已处理的事件和事故（例如，对其注册原因的调查已完成）。

  在确定设备表和*网络交互图*已解决"已解决"的事件和事故。

事件和事故的状态是手动改变的。您可以按照从*新的*到*已解决*的顺序依次分配状态（但是，您不需要分配中间的*进行中*状态）。事件或事故的状态改变后，您无法为其分配以前的状态。

已注册事件表

您可以在**事件和突发事件**部分的**事件**选项卡上查看已注册事件和突发事件的表格。

默认情况下，已注册事件和突发事件表会实时更新。表格的开头显示事件和突发事件以及最后可见的最新日期和时间。

事件或突发事件最后可见的日期和时间可能与其注册的日期和时间不同（注册日期和时间显示在**启动**列中）。对于某个事件，最后可见的日期和时间可能会在该类型事件的事件重新生成期间过程中更新。对于某个突发事件，最后可见的日期和时间根据该突发事件组成部分的事件最后发生的日期和时间进行更新。

事件和突发事件的设置显示在表格的以下列中：

- **启动**

  对于非突发事件的事件 - 事件注册日期和时间。对于突发事件 – 事件中包含的第一个事件的注册日期和时间。在表格中，您可以同时查看日期和时间，或者仅查看日期或时间。要选择显示的信息，请选中**日期**和/或**时间**设置对面的复选框。

- **最后可见日期**

  对于非突发事件的事件，这是事件最后发生的日期和时间。它可能包含事件注册的日期和时间，或者如果在事件重新生成超时期间重复事件注册条件，则包含事件重新生成计数器值增加的日期和时间。重新生成计数器的值显示在**总出现次数**列中。对于某个突发事件，这是突发事件中事件最后一次发生的最新日期和时间。就像**启动**列一样，您可以一起查看日期和时间，或者仅查看日期或时间。

- **标题**

  为事件类型定义的标题。

- **分数**

事件分数的计算值。事件严重级别通过数字分数来指定。根据严重程度，分数可能具有以下颜色之一：

- 红色表示事件严重程度*高*。
- 黄色表示事件严重程度*中*。
- 蓝色表示事件严重程度*低*。

- **源**

  网络数据包的源地址。您可以使用以下设置来显示或隐藏地址和端口（表格单元格的缩写在括号中列出）：**IP 地址**、**端口号(P)**、**MAC 地址**、**VLAN ID (VID)**、**应用程序级地址**。如果向应用程序添加了额外的地址空间，则可以在配置设备表时使用"**显示地址空间**"设置来启用或禁用地址空间名称的显示。

- **目的地**

  网络数据包的目标地址。地址信息的显示可以按照与**源**列相同的方式配置。

- **协议**

  应用程序注册事件时正在监控的应用层协议。

- **技术**

  此图标与用于注册事件的技术相对应。

- **总出现次数**

  对于非突发事件的事件，这是在事件重新生成超时时间内注册事件后的重新生成计数器的值。大于 1 的值表示事件注册条件重复了 N – 1 次。此列中显示该突发事件的数值 1。

- ID

  已注册事件或突发事件的唯一 ID。

- **应用程序**

  有关事件注册条件发生时正在运行的应用程序的信息。事件保存从EPP 应用程序收到的应用程序数据。

- **应用程序用户**

  有关用于启动**应用程序**列中指定的应用程序的用户账户的信息。

- **状态**

  此图标对应事件或突发事件的状态。

- **描述**

  为事件类型指定的描述。

- **结束**

  对于非突发事件的事件，这是分配*"已解决"*状态时的日期和时间，或事件重新生成超时的日期和时间。对于某个突发事件，这是该突发事件中事件结束的最近日期和时间。就像**启动**列一样，您可以一起查看日期和时间，或者仅查看日期或时间。

- **触发的规则**

  对于非突发事件的事件，这是其触发导致了事件注册的过程控制规则或入侵检测规则的名称。对于突发事件，这是其触发导致了事件注册的关联规则的名称。

- **监控点**
  其流量触发了事件注册的监控点。
- **事件类型**
  分配给事件类型的数字代码。
- **标记**
  这是您可以为任何事件或突发事件设置的图标分类，以便您可以根据表中没有的标准轻松找到事件和突发事件。

当查看事件和突发事件表时，您可以使用配置、过滤、搜索和排序功能，并导航到相关项目。

查看突发事件中包含的事件

为了查看事故中包含的事件，事件表中提供了以下模式：

- 简单的查看模式。在这种模式下，事件表显示所有事件，而不考虑事件如何嵌套在事故中。
- 树形显示模式。在此模式下，事件显示为树结构，可以使用事故标题旁边的 ＋ 和 － 按钮进行折叠和展开。

您可以在配置事件表时更改显示模式。

查看事件详细信息

有关事件和突发事件的详细信息显示在应用程序 Web 界面的**事件**部分的详细信息区域中。

要查看事件或突发事件的详细信息：

在**事件和突发事件**部分的**事件**选项卡上，选择相关事件或突发事件。

Web 界面窗口的右侧将显示详细信息区域，其中显示有关所选事件或突发事件的详细信息。

更改事件状态

您可以更改以下事件和事故的状态：

- *新的*。此状态可更改为“*进行中*”或“*已解决*”。
- *进行中*。此状态可更改为*已解决*。

“*已解决*”的状态无法更改。

如果某个事件与风险相关，您可以在为该事件分配“已解决”*已接受将风险状态更改为已解决*。

要在使用事件表格时更改事件或事故的状态：

1. 在**事件和突发事件**部分中选择**事件**选项卡。
2. 在事件表中，选择您想要更改其状态的事件和/或事故。
3. 打开工具栏中的**更改状态**下拉列表。
4. 在下拉列表中，选择命令来分配所需的状态。
   下列情况下，某些下拉列表项不可用：
   - 如果选定的项目不包含状态为**进行中**的事件或事故，则*新的*项目不可用。
   - 如果选定的项目不包含状态为**已解决**或*新的*的事件或事故，则*进行中*项目不可用。

   > 如果选择了所有满足当前过滤和搜索设置的事件和事故，且选定项目的数量超过 1000 条，则应用程序不会检查它们的状态。在这种情况下，**进行中**和**已解决**项目均可用。但是，**进行中**项目仅可用于为状态为*进行中*的事件和事故分配*新的*状态。

   将打开一个带有确认提示的窗口。
5. 如果选定的事件与风险相关，并且您想要同时为这些风险分配*已接受*状态，请选中**为与事件相关的风险分配“已接受”状态**（如果选择了一个事件）或“**为与事件相关的风险分配“已接受”状态**（如果选择了多个事件）。
   当应用程序基于资产管理技术注册某些类型的事件时，可能会存在与事件相关的风险。
6. 在提示窗口中，单击**确定**。

查看 EDR 事件的详细信息

EPP 事件可能包含从 Endpoint Agent 软件组件接收到的有关威胁发展链的信息。如果为某个事件建立了威胁发展链，Kaspersky Industrial CyberSecurity for Networks 将该事件视为*端点检测和响应*事故（EDR 事故）。

威胁发展链是与检测到的威胁相关联的设备上的一系列活动事件。威胁开发链中的一个关键活动事件是具有威胁检测对象的活动事件。链中的所有其他活动事件（在关键活动事件之前和之后）都会保存下来，以便进行进一步的威胁发展分析。

> 有关所建立的威胁发展链的信息不得与该事件的注册同时添加到该事件中。应用程序将此信息添加到事件的最大延迟为注册后 10 小时。如果事件的状态为“*已解决*”，则不会添加该信息。

EDR 事故在事件表中用 **EDR** 图标进行标记。对于每个 EDR 事故，您可以在详细信息区域查看威胁发展链的信息。信息显示在详细信息区域的以下选项卡上：

- **活动事件图表**提供了有关威胁发展链中涉及的对象的可视化信息。活动事件在图上表示为节点。根据已识别的威胁发展过程，节点位于不同的级别。关键活动事件位于图形的最低级别。此级别还可以显示按类型对其他活动事件进行分组的节点。在此级别之上，应用程序最多可以显示四个具有活动事件节点的级别。
- **所有活动事件**显示有关威胁发展链中包括的所有活动事件的信息的表格视图，并在活动事件图中显示为节点。

查看 EDR 事故的详细信息时，您可以通过查看检测处理状态来确定潜在威胁状态。应用程序显示威胁开发链的此状态。状态的背景颜色取决于威胁检测对象处理的结果：

- 如果检测到的威胁在处理后被认为已经消除（例如，受感染的对象已经被 EPP 应用程序清除），则该应用程序在绿色背景上显示检测处理状态；
- 在所有其他情况下，检测处理状态显示在红色背景上。

活动事件图中的关键活动事件具有与检测处理状态相同的颜色。

如果检测处理状态显示在红色背景上，则可以防止可能的威胁进一步发展，例如，通过触发 Kaspersky Industrial CyberSecurity for Networks 中的响应操作。

在任何情况下，无论显示的检测处理状态如何，您都必须调查发生 EDR 事件的原因和可能的后果。

您可以在选择活动事件时打开的详细信息窗口中查看有关活动事件的详细信息。查看详细信息时，您可以使用带有文件和 URL 哈希的链接在卡巴斯基威胁情报门户网站上获取这些对象的信誉信息。

如果威胁开发链包含您希望在 EPP 应用程序的下一次检查中检测的活动事件，您可以将这些活动事件的数据导出到 IOC 文件（入侵指标文件）。

为事件创建允许规则

如果需要禁用具有特定指标的事件（例如，来自某个监控点的所有事件）的注册，则可以创建事件的允许规则。本节包含有关创建事件允许规则的说明。

具有除操作员角色之外的任何角色的用户都可以为事件创建允许规则。

使用空白设置或模板中的设置创建允许规则

要使用空白设置或模板中的设置创建允许规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**允许规则**部分，单击**添加规则**打开详细信息区域。

3. 如果要从模板中定义设置值，请在详细信息区域中单击**使用模板**，在打开的窗口中选择必要的模板，然后单击**应用**。

4. 在详细信息区域中，单击“**EVT**”。

5. 在“**协议**”字段中，指定将在事件中指示的协议。

   当选择**协议**字段时，一个窗口将打开，其中显示以协议堆栈树形式显示的受支持协议表。您可以使用包含后续层协议的协议名称旁边的**+**和**-**按钮来管理树元素的显示方式。

   如有必要，请使用表格上方的搜索字段查找相关协议。

要指定协议：

a. 在协议表中，选择要为规则指定的协议。要选择相关协议，请单击协议表左列中显示的按钮。

b. 单击**确定**。

如果您选择了应用程序可以根据网络数据包的内容识别的协议，则**协议**字段下方会出现有关此协议的通知。

6. 如果需要，请在**注释**字段中输入有关该规则的其他信息。

7. 在**端 1**和**端 2**设置组中，指定网络交互参与者（各方）的可编辑地址信息。根据所选的协议（或协议集），地址信息可能包含 MAC 地址、IP 地址和/或端口号。如果向应用程序添加了额外的地址空间，则可以为地址指定地址空间的名称。

为了自动填充网络交互一方的地址信息，您可以选择对应用程序已知的设备。为此：

a. 单击**指定设备地址**打开设备选择窗口。

b. 在设备选择窗口中，选中要使用的设备旁边的复选框。

设备选择窗口包含一个表，您可以在其中配置列的布局和顺序，还可以像“资产”部分中的**资产**一样进行过滤、搜索和排序。

c. 在设备选择窗口中单击**确定**。

8. 在“**事件类型**”字段中，指定事件中指示其数字代码的事件类型。

选择“**事件类型**”字段将打开一个窗口，其中包含允许规则中可能指示的事件类型列表。如有必要，请使用表格上方的搜索字段查找相关事件类型。要指定事件类型，请在列表中选择它并单击**应用**。

9. 在“**监控点**”字段中指定事件中指示的监控点名称。

选择“**监控点**”字段将打开一个窗口，其中包含已安装应用程序组件的所有节点上的所有监控点的列表。如有必要，请使用列表上方的搜索字段查找相关监控点的名称。要指定监控点名称，请在列表中选择它并单击**应用**。

10. 在“**事件中的规则**”字段中，输入指示为事件中触发的规则的名称（或名称的一部分）。

11. 在详细信息区域中，单击**保存**。

新规则将被添加到允许规则表中。

从现有规则创建允许规则

要从现有规则创建允许规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**允许规则**部分，选择要用作创建新规则的基础的规则。

3. 右键单击以打开上下文菜单。

4. 在上下文菜单中，选择“**复制规则**”。

   规则编辑模式下的详细信息区域将出现在 Web 界面窗口的右侧。新规则的设置将采用从所选规则的设置中获取的值。

5. 根据需要更改设置。为此，请完成创建设置初始值为空的规则的过程中所述的步骤 4-9。

从已注册事件创建允许规则

要从已注册事件创建允许规则：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 在**事件和突发事件**部分中选择**事件**选项卡。

3. 在已注册事件表中，选择要用作创建事件允许规则的基础的事件。

   详细信息区域出现在 Web 界面窗口的右侧。

4. 在详细信息区域中，单击**创建允许规则**。

   允许规则部分在浏览器窗口中打开。规则编辑模式下的详细信息区域将出现在 Web 界面窗口的右侧。新规则的设置将采用从有关事件的已保存信息中接收的值。

5. 如有必要，编辑新规则的设置。为此，请完成创建设置初始值为空的规则的过程中所述的步骤 4-9。如果不需要更改新规则的设置，请单击**保存**来保存该规则。

设置标记

您可以在应用程序 Web 界面的**事件**部分为事件和突发事件分配特定标记。

*标记*是一个图标，可让您根据表中缺少的标准轻松找到事件和突发事件。

要为事件或突发事件设置标记：

1. 在**事件和突发事件**部分的**事件**选项卡上，单击左键即可打开包含相关事件或突发事件的行的**标记**列单元格中的上下文菜单。

2. 在上下文菜单中，选择要为此事件或突发事件设置的标记。

   您可以从应用程序提供的七个标记中选择一个。您可以自行选择每个标记的用途。

3. 如果需要删除标记，请在上下文菜单中选择**没有标记**。

将事件复制到文本编辑器

您可以将事件表中显示的事件和事故信息复制到任何文本编辑器。该信息从表中当前显示的列中复制。

如果选择的事件和事故不超过 200 个，则可以进行复制。

要将事件和/或事故复制到文本编辑器：

1. 在**事件和突发事件**部分中选择**事件**选项卡。
2. 在事件表中，选择要将其信息复制到文本编辑器的事件和/或事故。
3. 右键单击即可显示所选事件之一的上下文菜单。
4. 在上下文菜单中，选择下列选项之一：
   - 如果选择了一个事件或事故，则**复制事件的详细信息**。
   - 如果选择了多个事件和/或事故**复制所选事件的详细信息**。
5. 打开任意文本编辑器。
6. 将其粘贴到文本编辑器窗口中（例如，通过按组合键 **CTRL+V**）。

可在文本编辑器中编辑复制的事件详细信息。多个事件的信息将以空行分隔。

下载事件流量

查看事件表时，您可以加载与已注册事件和/或突发事件相关的流量。流量被加载到 PCAP 文件中（当选择一个事件时）或包含 PCAP 文件的 ZIP 存档中（当选择多个事件或突发事件时）。

如果在事件表中选择的事件不超过 200 个（包括事件内的事件），则可以加载流量。

事件的流量从应用程序数据库加载。仅当注册启用了流量保存的事件时，数据库才会保存流量。应用程序还可以通过请求使用流量转储文件加载流量，直接将流量保存在数据库中。这些文件用于临时保存流量，随着从工业网络接收到越来越多的流量，它们会被自动删除（文件删除的频率取决于接收到的流量量和定义的应用程序数据存储设置）。为了确保流量得到加载，建议启用相关事件类型的流量保存功能，并根据流量速率和事件注册情况配置数据库中保存流量的设置。

要加载事件和/或突发事件的流量文件：

1. 在**事件和突发事件**部分的**事件**上，选择您想要下载流量的事件和/或突发事件。
2. 单击**下载流量**。
3. 如果文件生成需要很长时间（超过 15 秒），则操作将移至后台。如果是这种情况，请按照以下步骤下载文件：
   a. 单击应用程序 Web 界面菜单中的 。
   后台操作列表打开。
   b. 等待文件生成操作完成。
   c. 单击“**下载文件**”。

您的浏览器将保存下载的文件。根据您的浏览器设置，屏幕可能会显示一个窗口，您可以在其中更改已保存文件的路径和名称。

将活动事件数据导出到入侵指标文件中

查看EDR 事故的详细信息时，如果您希望在 EPP 应用程序的下一次检查期间检测此类活动事件，则可以将活动事件的数据导出到 IOC 文件。您可以在使用 Endpoint Agent 软件组件执行的 IOC 搜索任务中使用收到的 IOC 文件。

要将活动事件数据导出到 IOC 文件：

1. 在“**事件**”部分的“**事件和突发事件**”选项卡上，选择包含具有适当的活动事件的威胁开发链的 **EDR** 事故（标有 EDR 图标的事件）。

   详细信息区域显示在 Web 界面窗口的右侧部分。

2. 在详细信息区域中，转到“**所有活动事件**”选项卡并选择适当的活动事件。

   您可以选择以下类型的活动事件：**文件创建**、**启动进程**或**注册表更改**。

3. 单击“**导出到 IOC 文件**”。

4. 在打开的窗口中，选择检测入侵指标的条件：

   - **OR (检测到任何 IOC)**如果您希望在检测到 IOC 文件中的任何入侵指标时触发 IOC 搜索任务。
   - **AND (检测到所有 IOC)**如果您希望在检测到 IOC 文件中的所有入侵指标时触发 IOC 搜索任务。

5. 查看将导出到 IOC 文件的信息。

   仅当任何“**文件创建**”、“**启动进程**”和“**注册表更改**”字段显示计数器非零值时，导出才可用。“**无法导出**”字段包含其数据无法导出到 IOC 文件的选定活动事件的数量。

6. 单击“**导出**”。

7. 如果文件生成耗时较长（超过 15 秒），则操作将移至后台。如果是这种情况，请按照以下步骤下载文件：

   a. 单击应用程序 Web 界面菜单中的 。

   后台操作列表打开。

   b. 等待文件生成操作完成。

   c. 单击“**下载文件**”。

您的浏览器将保存下载的文件。根据您的浏览器设置，屏幕可能会显示一个窗口，您可以在其中更改已保存文件的路径和名称。

创建用于将事件导出至网络资源的文件夹

您可以导出事件并将包含导出事件的文件保存在服务器计算机的网络资源上。您可以使用网络文件系统 (NFS) 协议来共享网络资源，该协议用于将另一台计算机的共享网络资源（例如 NFS 服务器导出点）挂载到服务器计算机的本地文件系统中。操作系统的标准工具可用于创建文件夹和挂载共享网络资源。

当使用 NFS 协议时，rpcbind 软件包会被在操作系统中激活。请记住，网络犯罪分子可能会尝试使用该软件包进行某些类型的 DDoS 攻击。为了消除渗透威胁，必须正确配置防火墙。在 CentOS Stream 操作系统中，建议您使用称为 Firewalld 的网络安全配置应用程序。

手动创建文件夹并挂载共享网络资源

要创建用于保存文件到网络资源的文件夹：

1. 打开操作系统控制台。
2. 创建用于挂载共享网络资源的本地文件夹。为此，请输入以下命令：

```
mkdir <本地目录的完整路径>
```

示例

```
mkdir ~/nfsshare
```

3. 创建文件夹后，输入以下命令挂载网络资源：

```
sudo mount -t nfs <远程计算机名称或 IP 地址>:<共享网络资源的完整路径> <本地目录的完整路径>
```

示例

```
sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare
```

4. 使用以下命令检查挂载结果：

```
mount | grep <本地目录的完整路径>
```

示例

```
mount | grep ~/nfsshare
```

如果挂载成功，您将看到包含远程计算机的名称或 IP 地址、共享网络资源的名称以及父文件夹的名称的数据。

自动挂载共享网络资源

在 CentOS 操作系统中配置共享资源的自动挂载：

用 root 权限打开 /etc/fstab 文件进行编辑，并将以下字符串添加到文件文本中：

```
<远程计算机的名称或 IP 地址>:<共享网络资源的完整路径> <本地目录的完整路径> nfs defaults 0 0
```

示例

```
nfs-server.example:/nfsshare /home/user1/nfsshare nfs defaults 0 0
```

监控风险

Kaspersky Industrial CyberSecurity for Networks 可以检测可能影响信息系统资源的风险。该应用程序根据流量分析和接收到的设备信息来检测风险。

检测到的风险可能属于以下类别：

- 漏洞。此类别包括检测到的设备漏洞。
- 配置问题。此类别包括由于错误配置而影响设备安全运行的风险以及写入和读取设备配置时数据泄露的风险。
- ICS 安全漏洞。此类别包括自动化工业控制系统中信息安全漏洞的风险。
- 不安全的网络架构。此类别包括与检测不安全的网络交互、设备、协议和软件相关的风险，授权设备不活动带来的风险，以及设备上 EPP 应用程序缺失或操作不当带来的风险。

每个风险的评分范围为 0.0 到 10.0。应用程序根据与检测到的风险关联的设备的可用信息来计算该数字风险评分值。计算风险评分时，应用程序会考虑设备的重要性级别以及与该设备相关的其他风险。*基本分数*用作计算的初始值。漏洞类别中的风险基本评分根据通用漏洞评分系统 (CVSS) 确定。所有其他风险类别均使用风险类型表中定义的基本分数。

有关风险的信息将上传至 Kaspersky Industrial CyberSecurity for Networks Server 上的风险数据库中。数据库中保存的条目总数不能超过定义的限制。如果数量超出定义的限制，应用程序会自动删除 10% 的最旧条目。在服务器节点上配置数据存储设置时，您可以设置检测到的风险的最大数量限制。

风险数据库的内容显示在应用程序 Web 界面的“**风险**”部分中。您还可以在“**资产**”部分中的“**设备**”选项卡上查看有关与设备相关的风险的一般信息。

关于漏洞类别中的风险

当应用程序检测到受监控的工业网络设备中的漏洞时，就会记录漏洞风险。*漏洞*是设备硬件或软件中的缺陷或瑕疵，黑客可以利用它来影响信息系统的运行或获取未经授权的信息访问。

该应用程序通过分析有关设备的可用信息来检测漏洞。将用于查找设备已知漏洞的相关信息与*已知漏洞数据库*中的特定字段进行比较。已知漏洞数据库内置于应用程序中。该数据库由卡巴斯基专家创建，他们在其中填充了有关工业网络设备最新或最常遇到的漏洞的信息。

已知漏洞数据库包含漏洞的描述以及受这些漏洞影响的设备的描述。该数据库还包含以文本或公开资源链接形式提供的系统安全建议。来自各种来源的描述和建议被上传到已知漏洞数据库。这些来源可能是设备或软件的制造商，或者是各种专门从事工业安全的组织。数据库中的描述和建议以英文提供。

应用程序安装后，将使用初始预配置的已知漏洞数据库。您可以通过安装更新来使数据库保持最新。

Kaspersky Industrial CyberSecurity for Networks 将可用的设备信息与已知漏洞数据库中描述受漏洞影响的设备的特定字段进行比较。为了检测漏洞，该应用程序使用有关设备的以下信息：

- **硬件提供商**。
- **硬件型号**。
- **硬件版本**。
- **软件提供商**。如果在设备信息中未检测到软件供应商数据，Kaspersky Industrial CyberSecurity for Networks 将使用“**硬件提供商**”字段的值。
- **软件名称**。如果在设备信息中未检测到软件名称，Kaspersky Industrial CyberSecurity for Networks 将使用“**硬件型号**”字段的值。
- **软件版本**。

在已知漏洞数据库中，设备的描述以 CPE (Common Platform Enumeration) 语言格式存储。应用程序将可用的设备信息与这些描述进行比较，自动将信息转换为 CPE 语言格式。

对于每个漏洞，在“**匹配的 CPE**”部分的风险详细信息区域中提供了匹配的描述。

如果设备信息与已知漏洞数据库中的相应字段匹配，应用程序将注册漏洞风险并将有关漏洞的信息上传到检测到的风险数据库。

用于识别漏洞的主要参数是其在 Common Vulnerabilities and Exposures (CVE) 列表中的识别号。此识别号称为“*CVE ID*”。如果漏洞尚未分配 CVE ID，则通过从包含漏洞描述的其他公开资源获取的识别号来识别。

Kaspersky Industrial CyberSecurity for Networks 可让您获取俄罗斯联邦技术和出口管制局 (FSTEC) 在信息安全威胁数据库 (也称为 BDU) 中提供的标识符和漏洞描述链接。如果下载的漏洞信息包含来自 FSTEC BDU 的此类信息，则应用程序会以 BDU 格式将此信息显示为其相应的标识符：<年>-<号码>。

实施持续风险管理流程的场景

风险检测功能可让您在信息系统中实施持续（周期性）的风险管理。出于风险管理目的，Kaspersky Industrial CyberSecurity for Networks 提供了有关检测到的风险的信息，您可以根据这些信息采取适当措施消除或减轻这些风险。

实施持续风险管理流程的场景包括以下阶段：

1 设备清单

此阶段通过使用设备活动检测和设备信息检测方法（这些方法必须启用）来实现。在此阶段，应用程序会自动检测新设备并更新设备信息。如果工业网络包含未自动检测到的设备，则需要手动添加或从外部项目导入它们。

对于定义设备分类和操作规格的所有信息（例如有关设备型号和软件版本的信息），您必须在设备设置中启用自动更新。如果由于某种原因无法完成该信息的自动更新，则应手动更新该信息。

2 通过被动和主动扫描进行风险检测

该应用程序利用可用的设备信息，被动地扫描设备是否存在风险。该应用程序还通过分析工业网络流量中的网络交互来检测风险。风险检测采用风险检测方法实现（必须启用该方法）。

您还可以对设备进行主动轮询，以快速获取有关这些设备的信息。在对设备进行主动轮询时，如果选择了相应的风险分析方法，您还可以检测特定类型的风险。要对设备进行主动轮询，必须向应用程序中添加一个或多个**主动轮询**连接器。

漏洞风险在已知漏洞数据库更新后，或增加、修改用于比对的设备信息后（如保存设备型号和软件版本信息后）被自动检测。

3 对检测到的风险进行评估和分类

该应用程序会计算每个检测到的风险的分数值。该分数决定了风险的严重级别。根据分数，风险的严重程度可能为*低*、*中*或*高*。

您可以根据检测到的风险的严重程度和分数进行分类，也可以根据与信息系统中使用的设备的操作细节相关的其他因素进行分类。如果您评估某个风险可以忽略不计，则可以手动将其状态从*活动*（默认分配给检测到的风险）更改为*已接受*。例如，如果无法重现利用漏洞的条件，则可以这样做。当改变风险状态时，建议添加或编辑该风险的评论。

所有需要采取额外行动的风险都应保持为*活动*。

4 风险缓解

在此阶段，您需要采取行动来帮助消除检测到的风险或最大限度地减少与这些风险的潜在实现相关的威胁。为此，请检查所有检测到的、状态为"*活动*"的风险，从得分最高的风险开始。在您的信息系统中执行必要的操作（例如，消除设备漏洞、安装所需的软件更新；如果无法更新，则将该设备与外部网络隔离）。有关建议的缓解措施的信息针对特定风险（例如漏洞）提供。

> 对检测到的风险采取的修复操作无需 Kaspersky Industrial CyberSecurity for Networks 的参与。

5 风险缓解验证

这个阶段类似于通过扫描检测风险。当此阶段完成后，风险表将不再包含任何"*活动*"风险。

如果检测到这些风险的条件不再满足，则应用程序在被动扫描期间检测到的大多数风险（例如漏洞）都会自动分配*已修复*状态。例如，在设备上的软件版本发生变化后，应用程序会将因软件先前版本存在漏洞而注册的漏洞风险分配为*已修复*状态。对于已知漏洞数据库中不再具有描述的风险（例如，如果在*上传更新已修复*"已修复"状态。

删除设备时，应用程序也会删除与这些设备相关的风险。

如果您已采取措施降低风险，但风险检测条件没有改变（例如，某个易受攻击的设备已与外部网络隔离，但该设备的信息没有改变），您可以手动将此风险状态指定为*已接受*。当改变风险状态时，建议添加或编辑该风险的评论。

某些风险无法自动分配*已修复*状态（例如，无法将*已修复*自动分配给在设备主动轮询期间检测到的风险）。对于这些类型的风险，您还必须在采取风险缓解措施后手动分配*已接受*状态。

如果某个风险与某个事件相关联，您可以在将事件状态更改为"*已解决*"的同时，为该风险分配"*已接受*"状态。

查看风险表

风险表显示在应用程序 Web 界面的“**风险**”部分。

风险设置显示在表格的以下列中：

- **类别**

  风险类别的名称。

- **名称**

  风险名称。检测到的漏洞的 CVE ID 用于表示漏洞风险（如果没有 CVE ID，则通过从其他包含漏洞描述的公开资源中获取的识别号来识别）。

- **CVE**

  对于漏洞风险：检测到的漏洞的 CVE ID。

- **BDU**

  对于漏洞风险：BDU 数据库中的漏洞 ID。如果一个具有 CVE ID 的漏洞与 BDU 数据库中具有不同 ID 的多个漏洞匹配，则此列包含所有 ID。

- **风险 ID**

  风险的唯一 ID。

- **分数**

  风险评估的计算值。风险的严重程度通过数值分数来表示。根据严重程度，分数可能具有以下颜色之一：

  - 红色表示*高*严重级别风险。
  - 黄色表示*中*严重级别风险。
  - 蓝色表示*低*严重级别风险。

  对于状态为*活动*的风险，分数会以鲜艳的颜色显示。对于“*已修复*”或“*已接受*”的风险，评分颜色较淡。

  在详细信息区域中，此设置被称为“**基本分数**”。

- **端 1**

  网络交互一方的地址信息（针对某些风险类型有注明）。MAC 地址和 IP 地址可以单独启用和禁用。如果向应用程序添加了额外的地址空间，则可以在配置风险表时使用“**显示地址空间**”设置来启用或禁用地址空间名称的显示。

- **端 2**

  网络交互对方的地址信息（针对某些风险类型有注明）。地址信息的显示可以按照与**端 1**列相同的方式配置。

- **设备组**

  包含检测到风险的设备的组的名称（包含组的名称及其所有父组的名称）。

- **设备**

  设备名称和地址。

- **源**

  对于漏洞风险：上传到已知漏洞数据库的信息来源的名称。在详细信息区域中，此设置被称为“**漏洞源**”。

- **状态**

  风险的当前状态。可使用以下状态：

  - 首次检测到风险时，默认状态为“*活动*（如果风险的状态为“*已修复*”，则重复检测时也为“活动”）。您还可以手动为当前“*活动*”的风险分配*已接受*状态。
  - 如果风险检测条件不再存在，则自动分配“*已修复*”状态。
  - 如果风险评估为可以忽略不计，或风险缓解措施未导致自动分配*已接受*，则手动分配给风险的状态为“*已修复*”。

- **检测时间**

  风险注册的日期和时间。

- **上次状态更改**

  风险状态最后更改的日期和时间。

- **匹配的 CPE**

  对于漏洞风险：来自已知漏洞数据库的设备描述。这些是与设备表中的设备信息匹配的描述。

当查看风险表时，您可以使用配置、过滤、搜索和排序功能，以及导航到相关项目。

查看风险详细信息

风险详细信息包括风险表和以下字段的信息：

- **风险类型** – 风险类型代码。
- **描述** – 为风险类型或相应漏洞定义的描述。
- **基本分数** – 用于计算风险分数数值的初始值。

对于漏洞风险，以下字段和字段组中会显示附加信息：

- **CVSS 矢量** – 用于计算 CVSS 漏洞分数的指标记录。
- **攻击条件** – 漏洞利用条件的描述。
- **影响** – 描述利用漏洞可能造成的影响。
- **缓解** – 修复漏洞的建议（例如，应在设备上安装哪个软件版本）。
- **链接** – 包含有关漏洞的更多信息的公开资源的链接。
- **CVE 历史** – 在公开来源中识别、确认和发布漏洞的日期。

要查看有关风险的信息：

选择风险表中的相关风险。

在 Web 界面窗口的右侧，您将看到包含有关风险的详细信息的区域。

*要在"**设备**"部分的"**资产**"选项卡上查看漏洞风险的详细信息：*

单击**风险**列中或存在此风险的设备的详细信息区域中的漏洞名称（显示为 CVE ID 或漏洞的其他识别号）。

您将看到一个窗口，其中包含有关漏洞的详细信息。

手动更改风险状态

在**风险**部分操作时，您可以手动将任何风险的状态从*活动*更改为*已接受*，反之亦然。在"**资产**"部分操作时，您只能更改漏洞风险的状态，并且只能从*活动*更改为*已接受*。

在将与该风险相关的事件分配已接受"已解决"状态时，您还可以为该风险分配*已解决*"状态。

要手动更改风险状态：

1. 通过 Web 界面，使用已分配具有此操作权限的角色的用户账户连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。

   除操作员角色外，任何角色的用户都可以执行此操作。

2. 打开风险详细信息区域或包含风险详细信息的窗口。

3. 打开"**更改状态**"下拉列表。

4. 根据您想要分配给风险的状态，在下拉列表中选择以下项目之一：

   - 如果您想将风险状态从"*活动*"更改为"*已接受*"，请选择"**已接受**"。
   - 如果您想将风险状态恢复为"*活动*"，请选择"**活动**"。

   将打开一个带有确认提示的窗口。

5. 如果事件与选定风险相关，并且您想要同时为所有这些事件分配*已解决*状态，请选中"**将"已解决"状态分配给所有相关事件**"复选框。

   当应用程序基于资产管理技术注册某些类型的事件时，可能会存在与事件相关的风险。

6. 在提示窗口中，单击**确定**。

使用设备表时查看风险详细信息

使用设备表时，您可以查看有关在设备上检测到的风险的信息。显示每个包含漏洞风险的设备检测到的漏洞名称（标识为 CVE ID 或其他漏洞识别号）。如果在设备上检测到其他类别的风险，则会显示该设备的这些风险类别的名称。当选择设备时，漏洞和风险类别的名称将显示在**风险**列和详细信息区域中。

默认情况下，设备表仅显示分配有*活动*状态的风险的信息。如有必要，您可以通过在**配置设备表显示已补救和已接受的风险**"显示已修复和已接受的风险"来显示有关所有风险的信息。

为了标明风险的严重级别，漏洞名称和类别会以下列颜色之一显示：

- 红色表示*高*严重级别风险。
- 黄色表示*中*严重级别风险。
- 蓝色表示*低*严重级别风险。

对于状态为*活动*的风险，名称会以鲜艳的颜色显示。对于状态为*已修复*或*已接受*的风险，名称会呈现淡淡的颜色。

如果同一类别的风险与某个设备相关联，则该类别的名称将以所有这些风险中严重级别最高的颜色显示。

如果您想查看风险的详细信息，可以使用显示的漏洞名称和风险类别。单击漏洞名称（显示为 CVE ID 或其他漏洞识别号）可打开该漏洞的详细信息窗口。当您单击风险类别的名称时，应用程序会切换到风险表并应用过滤器来显示与设备相关的所选类别的风险。

查看设备表时，您可以根据相关风险配置设备过滤设置。您还可以根据漏洞名称（标识为 CVE ID 或其他漏洞识别号）搜索设备。

是深度包检测

Kaspersky Industrial CyberSecurity for Networks 可为您提供有关工业网络流量中传输的过程参数和系统命令的信息，从而让您监控工业过程。该应用程序会跟踪设备表中显示的、已定义过程控制设置的设备的这些数据。

您可以在“**过程控制**”部分的服务器 Web 界面页面中查看被监控的标签和现有过程控制规则。当您在“**资产**”部分和“**网络地图**”部分选择相应的设备时，设备的过程控制设置可用。

监控过程参数值

Kaspersky Industrial CyberSecurity for Networks 可实时显示过程参数（标记）的值。

要显示这些值，您必须将相关标记添加到应用程序。您可以在配置过程控制时添加标记。

应用程序不会保存实时显示的标记值。标记的名称和值可以保存在基于深度包检测技术注册的事件中（事件注册时收到的标记值保存在事件中）。为了保存标记的名称和值，事件类型的设置中必须存在变量 $tags。

要查看过程参数值：

通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器，选择**标记**部分中的**过程控制**选项卡。

浏览器窗口将显示一个包含标记及其当前值的表格。以下标记参数显示被动态修改的值：

- **基本数据类型**
- **读/写**
- **接收时间**

- **时间戳**
- **时间戳状态**
- **数据状态**
- **发起人**
- **值**
- **结构值**
- **传输原因**

要监控标记的值，您可以使用查看标记表时可用的所有功能。

标签的设置

当选择一个标签时，用于过程控制的标签设置将显示在标签表和详细信息区域中。

根据选择显示的列，标签表可能会显示以下设置：

- **设备组** ——包含与标签关联的设备的组的名称（包含组的名称以及设备组树中所有父组的名称）。在详细信息区域中，此设置被称为“**组**”。
- **设备** ——与标签关联的设备的名称。
- **协议** ——用于传输标签的协议名称。
- **标记名称** ——标记的定义名称。
- **协议数据类型** ——标签数据类型指示协议操作的特定名称（如果协议支持此类名称，例如 IEC 60870-5-104 和 IEC 60870-5-101 协议）或用标准数据类型名称表示（例如，int32）。
- **计量单位** ——标记所代表的过程设置的度量单位。
- **基本数据类型** ——标签字段结构中主要值的数据类型（由标准数据类型名称表示）。
- **读/写** ——收到标签值时的传输方向（从设备读取时为 R，写入设备时为 W，两个方向为 RW）。
- **收藏夹** ——指示标签是否已添加到收藏夹列表。
- **描述** ——关于标签的附加信息。
- **标记地址** ——标签在设备内存中的硬件地址。
- **标记 ID** ——标签的序号。将自动分配标记 ID。在详细信息区域中，此设置被称为“**ID**”。
- **接收时间** ——应用程序上次接收标签值的日期和时间。
- **时间戳** ——标签值（从流量接收）上次修改或更新的日期和时间。
- **时间戳状态** ——标签值上次修改或更新的日期和时间的状态。

- **数据状态** ——接收到的标签值的当前状态。
- **发起人** ——接收标签值或发送命令的来源的名称。
- **值** ——操作过程中动态修改的标签值。
- **可缩放标记** ——输入和输出值的最小值和最大值范围内的标签缩放指标。
- **输入（最小）** ——输入值的最小边界。
- **输入（最大）** ——输入值的最大边界。
- **输出（最小）** ——输出值的最小边界。
- **输出（最大）** ——输出值的最大边界。
- **结构值**：所有标签字段的名称和值的列表。列表项以逗号和空格分隔（例如：`field1: <value1>, field2: <value2>`）。嵌套字段的名称由所有父字段的名称和实际字段的名称生成，以冒号分隔（例如：`parent1:parent2:field: <value>`）。字符串值必须用引号引起来。
- **传输原因** ——修改或传输标签值（从流量中接收）的原因。
- **源** ——有关标签创建来源的信息。当标签自动创建时，“**源**”设置为“**系统**”。如果标签由用户创建或修改，则“**源**”设置为“**用户**”。

所选标签的详细信息区域还可能显示由设备和协议确定的其他设置，例如“**内存区域**”。

在通过 IEC 60870-5-104 和 IEC 60870-5-101 标准协议进行交互的设备上，深度数据包检测支持组成应用程序服务数据单元 (ASDU) 的帧类型。有关这些协议中支持的 ASDU 类型标识的信息，请参阅附录。

查看标记表

标签表显示在“**标记**”部分的“**过程控制**”选项卡上。该表提供了标签以及与标签关联的设备的常规参数。

当查看设备表时，您可以使用配置、过滤、搜索和排序功能，以及导航到相关项目。

连接设备时检测默认密码

当监控过程控制设备的通信时，Kaspersky Industrial CyberSecurity for Networks 可以确定何时使用默认密码。如果使用针对特定设备类设置的默认密码连接到设备，则应用程序会注册相应的事件。为了注册默认密码检测事件，应用程序使用系统事件类型来检测系统命令。

Kaspersky Industrial CyberSecurity for Networks 在以下情况下检测默认密码：

- 尝试使用默认密码成功，或该尝试的结果未确定。在这种情况下，将注册一个事件以检测 DEFAULT PASSWORD ENTRY 系统命令。
- 与默认密码匹配的新密码得到设置。在这种情况下，将注册一个事件来检测 DEFAULT PASSWORD SET 系统命令。
- 默认密码在从设备读取连接账户凭证时收到。在这种情况下，将注册一个事件以检测 DEFAULT PASSWORD READ 或 DEFAULT PASSWORD READ WITH TYPE 系统命令（如果密码详细信息表明其类型，这决定可以使用此密码对设备执行的操作）。

某些设备类和应用程序级协议支持检测默认密码（见下表）。

具有默认密码的受支持设备和协议

设备	协议	系统命令
ABB Relion 系列：RED670、REL670、RET670	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET
BECKHOFF CX 系列	BECKHOFF ADS/AMS	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
Emerson ControlWave 系列	Emerson ControlWave Designer	DEFAULT PASSWORD ENTRY
General Electric Multilin 系列：B30, C60	Modbus TCP	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD READ WITH TYPE DEFAULT PASSWORD SET
Mitsubishi System Q E71	Mitsubishi MELSEC System Q	DEFAULT PASSWORD SET
Schneider Electric Modicon: M580, M340	Modbus TCP	DEFAULT PASSWORD READ WITH TYPE
Siemens SIMATIC S7-200, S7-300, S7-400	Siemens Industrial Ethernet Siemens S7comm	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ
Siemens SIMATIC S7-1200, S7-1500	Siemens Industrial Ethernet Siemens S7comm-plus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
基于 CODESYS V3 平台的 PLC（例如 Prosoft-Systems Regul R500）	CODESYS V3 Gateway	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
EKRA 200 系列	Modbus TCP for EKRA 200 系列设备	DEFAULT PASSWORD READ DEFAULT PASSWORD SET
EKRA BE2502、BE2704 系列	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET

要注册默认密码检测事件，必须满足以下条件：

- 交互控制已在监控模式下启用，命令控制技术已应用。
- 允许规则表不包含任何允许使用默认密码的系统命令的命令控制技术规则。例如，应用程序可以在交互控制学习模式下自动创建这些规则。如果这些规则存在于允许规则表中，建议您禁用它们。
- 对于相关设备，具有默认密码的系统命令跟踪已启用。

获取报告

使用 Kaspersky Industrial CyberSecurity for Networks，您可以生成包含应用程序保存的各种信息的报告。Kaspersky Industrial CyberSecurity for Networks 生成 PDF 格式的报告文件。应用程序可以将报告文件发送到具有管理员或安全官角色的用户指示的电子邮件地址。您也可以在服务器 Web 界面页面上下载报告。

Kaspersky Industrial CyberSecurity for Networks 支持以下类型的报告：

- 基于模板的报告。

  这些报告包含有关设备及其状态、系统安全、监控的技术流程参数和系统命令的累积信息，以及有关检测到的风险和与第三方设备的交互的信息。

- 漏洞和合规性审计作业报告。

  这些报告包含有关漏洞和合规性审计作业运行结果的信息。

您可以查看有关生成的报告的信息，并在“**报告**”部分的“**生成的报告**”选项卡上将其导出到文件中。

查看报告表

您可以在应用程序 Web 界面的“**生成的报告**”选项卡上的“**报告**”部分中查看报告表。

报告设置显示在表格的以下列中：

- ID

  报告的唯一标识符。

- **报告名称**

  生成的报告的名称。

- **模板名称**

  用于生成报告的模板的名称。

- **运行**

  开始生成报告的日期和时间。

- **状态**

  报告完成状态。提供以下报告完成状态：

  - **等待发送**。该报告位于创建队列中。当同时生成多个报告时，报告可能会处于*待处理*状态。
  - **进行中**。目前正在生成该报告。
  - **错误**。生成报告时发生错误。
  - **完成**。报告生成完成。

- **正在取消**。正在取消报告生成。
- **已取消**。报告生成已取消。

- **用户**
  开始生成报告或配置基于模板生成报告的计划的用户的名称。
- **运行类型**
  报告生成启动的类型：手动或按计划。
- **已完成**
  报告生成完成的日期和时间。

查看报告表时，您可以使用配置、过滤和排序功能。

将报告导出到文件

您可以将生成的报告导出为 PDF 格式的文件。

要将报告导出到文件，请执行以下操作：

1. 选择“**报告**”部分。
2. 在“**生成的报告**”选项卡，选择相关报告。
   报告将根据上次在当前服务器连接会话中运行的报告的 ID 进行筛选。要显示所有生成的报告，请单击“**默认过滤器**”重置过滤器设置。如有必要，您可以根据特定的时间段配置筛选。
   详细信息区域出现在 Web 界面窗口的右侧。
3. 单击**导出**。

   您的浏览器将保存报告文件。默认情况下，报告文件的命名格式为<报告名称>_<报告生成日期和时间>。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。

基于模板的报告

Kaspersky Industrial CyberSecurity for Networks 中的报告模板有以下类型：

- 系统模板在应用程序安装期间自动创建。在报告模板表中，系统模板显示为 图标。您不能删除系统模板。
  Kaspersky Industrial CyberSecurity for Networks 支持以下用于生成报告的系统模板：
  - **清单报告**。
    报告包含有关设备、监控的工艺过程参数和系统命令、使用的协议以及检测到的设备风险的信息。
  - **系统安全报告**。
    报告包含有关设备安全状态、注册事件、检测到的风险以及与外部网络设备交互的信息。

- **执行摘要**

  报告包含有关设备和系统安全状态的简要信息。

- **完整报告**

  报告包含有关设备和系统安全状态的全面信息。

- 用户定义模板是通过复制模板手动创建的。系统模板和用户定义模板可以复制。具有管理员或安全官角色的用户可以复制模板。

报告中的数据以单独的信息块形式呈现。对于每份报告，Kaspersky Industrial CyberSecurity for Networks 使用固定的信息块集合和布局。。报告中使用的信息块及其描述如下表所示。

报告中信息块的使用

信息块名称	清查报告	系统安全报告	执行摘要	完整报告
设备类别	✓	–	✓	✓
设备供应商	✓	–	✓	✓
设备操作系统	✓	–	✓	✓
监控的工艺过程参数	✓	–	–	✓
风险最多的设备	✓	✓	–	✓
最易受攻击的工业设备	✓	✓	–	✓
系统命令源	✓	–	–	✓
态势感知	–	✓	✓	✓
网络中的新设备	✓	–	–	✓
流量最大的协议	✓	–	–	✓
与其他节点连接最多的设备	✓	–	–	✓
网络流量	✓	–	✓	✓
通用协议	✓	–	✓	✓
工业协议	✓	–	✓	✓
系统命令接收方	✓	–	–	✓
设备安全状态	–	✓	✓	✓
按状态分布的设备	–	✓	–	✓
事件统计信息	–	✓	–	✓
按检测技术分布的事件	–	✓	–	✓
事件最多的设备	–	✓	–	✓
最关键的事件	–	✓	–	✓
最频繁触发的恶意活动检测规则	–	✓	–	✓
工业网络中的异常协议	–	✓	–	✓
具有访问公共资源标志的设备	–	✓	–	✓
通过远程控制协议进行的连接	–	✓	–	✓

信息块名称	清查报告	系统安全报告	执行摘要	完整报告
工业设备程序修改	–	✓	–	✓
活动风险	–	✓	✓	✓

查看报告模板表

您可以在应用程序 Web 界面的“**报告模板**”选项卡的“**报告**”部分中查看报告模板表。

报告模板的设置显示在表的以下列中：

- **名称**

  报告模板名称。 图标显示在系统报告模板名称旁边。

- **计划**

  有关 Kaspersky Industrial CyberSecurity for Networks 用于根据模板自动生成报告的计划的信息。如果具有管理员或安全官角色的用户在报告模板中配置了计划设置，则会显示计划信息。如果未定义计划设置，则该列将显示值“**关闭**”。

- **类型/用户**

  最后修改报告模板的用户的名称。对于具有默认设置的系统模板，将显示“**系统**”值。

- **上次报告**。

  上次根据报告模板开始生成报告的日期和时间。

- **目的地**

  此图标表示有报告的电子邮件收件人。提供以下图标：

  - – 定义了报告接收者。
  - – 未定义报告接收者。

查看报告模板表时，您可以使用配置和排序功能。

查看报告模板详细信息

要查看有关报告模板的信息：

在“**报告**”部分的“**报告模板**”选项卡上，选择相关模板。

详细信息区域出现在 Web 界面窗口的右侧。详细信息区域会显示具有定义值的所有数据。

报告模板详细信息包括以下字段：

- **名称** – 报告模板名称。
- **类型/用户** – 最后修改报告模板的用户的名称。对于具有默认设置的系统模板，将显示“**系统**”值。
- **时段** – Kaspersky Industrial CyberSecurity for Networks 基于模板生成报告时所涵盖的时间段。

- **更改时间** – 模板最近更改的时间。
- **上次报告** – 基于模板生成最后一个报告的时间。
- **下次运行** – 基于模板开始生成下一个报告的时间。如果为报告模板定义了计划设置，则会显示此设置。
- **计划** – 有关 Kaspersky Industrial CyberSecurity for Networks 用于根据模板自动生成报告的计划的信息。如果为报告模板定义了计划设置，则会显示此设置。
- **目的地地址** – Kaspersky Industrial CyberSecurity for Networks 将生成的报告发送到的电子邮件地址。如果为报告模板定义了收件人地址，则显示此设置。

根据模板手动生成报告

您可以基于模板手动启动报告生成。任何角色的用户都可以手动开始生成报告。

要开始生成报告，请执行以下操作：

1. 选择“**报告**”部分。
2. 在“**报告模板**”选项卡上，选择要用于生成报告的一个或多个模板。

   当选择多个模板时，应用程序会同时基于这些模板生成报告。您可以选择不超过 10 个模板。
3. 单击位于报告模板表上方的工具栏中的“**获取报告**”。

   Kaspersky Industrial CyberSecurity for Networks 将启动报告生成过程。如有必要，您可以联系具有管理员或安全官角色的用户以取消生成报告。

您将进入“**生成的报告**”选项卡，该选项卡将显示正在生成的报告的进度。生成报告后，Kaspersky Industrial CyberSecurity for Networks 将 PDF 格式的报告文件发送到报告模板中指示的电子邮件地址。如果报告模板中未定义电子邮件地址，则可以在“**生成的报告**”选项卡上手动将生成的报告单独导出到文件中。报告文件的最大大小为 10 MB。

漏洞和合规性审计作业报告

Kaspersky Industrial CyberSecurity for Networks 可以生成报告，其中包含有关漏洞和合规性审计作业运行结果的信息。具有管理员或安全官角色的用户可以配置通过电子邮件自动发送报告。如有必要，您可以手动生成已完成作业运行或已完成设备扫描的报告，然后将报告导出到文件中。

生成手动作业运行的报告

您可以手动生成关于漏洞和合规性审计作业运行的报告。该报告是根据使用作业设置中选择的漏洞和合规性审计规则对设备执行的扫描结果生成的。

提供了以下关于漏洞和合规性审计作业运行的报告：

- **完整报告**

  此报告包含有关执行的扫描以及使用的漏洞和合规性审计规则的详细信息。

- **执行摘要**

  此报告包含最重要的扫描结果摘要。

要生成报告，漏洞和合规性审计作业的运行必须具有以下状态之一：**已完成**、**部分成功**、**已取消**或**错误**。

要开始生成报告，请执行以下操作：

1. 选择“**安全审计**”部分。
2. 在**漏洞和合规性审计**选项卡上，选择要为其生成报告的作业。

   详细信息区域出现在 Web 界面窗口的右侧。
3. 在详细信息区域中，转到**运行**选项卡。
4. 选择所需的作业运行。
5. 在显示的作业运行详细信息区域中，打开“**获取报告**”下拉列表，然后选择所需的报告：“**完整报告**”或“**执行摘要**”。如果无法生成报告，则下拉列表不可用。

   Kaspersky Industrial CyberSecurity for Networks 将启动报告生成过程。

转到“**报告**”部分的“**生成的报告**”选项卡。漏洞和合规性审计报告显示在生成的报告表中。成功生成报告后，您可以将生成的报告导出到文件中。

生成手动设备扫描的报告

您可以在漏洞和合规性审计作业中手动生成设备扫描报告。该报告是根据使用作业设置中选择的漏洞和合规性审计规则在设备上执行扫描的结果生成的。该报告包含有关执行的扫描以及使用的漏洞和合规性审计规则的详细信息。

要生成报告，设备扫描必须具有以下状态之一：**已完成**、**已取消**或**错误**。

要开始生成报告，请执行以下操作：

1. 选择“**安全审计**”部分。
2. 在**漏洞和合规性审计**选项卡上，选择执行所需设备扫描的作业。

   详细信息区域出现在 Web 界面窗口的右侧。
3. 在详细信息区域中，转到**运行**选项卡。
4. 选择所需的扫描，然后在显示的扫描详细信息区域中单击“**获取报告**”。如果无法生成报告，则该按钮将被禁用。

   Kaspersky Industrial CyberSecurity for Networks 将启动报告生成过程。

转到“**报告**”部分的“**生成的报告**”选项卡。漏洞和合规性审计报告显示在生成的报告表中。成功生成报告后，您可以将生成的报告导出到文件中。

检测加密协议中的安全问题

如果工业网络中使用加密协议（如 SSL/TLS 或 SSH），Kaspersky Industrial CyberSecurity for Networks 可以检测使用这些协议的网络交互中的各种安全问题。当检测到安全问题时，应用程序会注册适当的事件。用于检测系统命令的系统事件类型用于注册这些事件。

当应用程序检测到加密协议中存在以下安全问题时，它会注册事件：

- 使用过时的加密协议版本 (DEPRECATED PROTOCOL VERSION)。
- 使用弱的加密算法 (WEAK CIPHER TYPE)。
- 使用过时的证书 (OUTDATED CERTIFICATE)。
- 使用自签名的证书 (SELF-SIGNED CERTIFICATE)。

检测到的安全问题列表取决于特定的加密协议。

安装后，该应用程序使用支持有限数量的加密协议的原始协议处理模块。您可以通过安装更新来更新协议处理模块。

您不需要为设备添加过程控制设置来检测加密协议中的安全问题。应用程序分析所有检测到的交互中的加密协议。

要注册安全问题检测事件，必须满足以下条件：

- 交互控制已在监控模式下启用，命令控制技术已应用。
- 允许规则表不包含任何阻止注册与加密协议中的安全问题有关的事件的命令控制技术规则。例如，应用程序可以在交互控制学习模式下自动创建这些规则。如果这些规则存在于允许规则表中，建议您禁用它们。

使用数据表时的典型操作

本部分包含有关使用应用程序 Web 界面的不同部分中显示的数据表（例如设备表、事件表或标签表）时执行的典型操作的信息。

查看数据表

本节介绍在应用程序 Web 界面部分查看数据表时可用的功能。

配置列的显示和顺序

根据应用程序 Web 界面的特定部分，您可以启用和禁用表中特定数据的显示，并配置要显示的列和顺序。

要配置表格显示设置：

1. 点击 图标打开用于配置表显示方式的窗口。
2. 如果该表可以启用和禁用特定数据的显示（例如，在设备表中显示已修复和已接受的风险），请在窗口的上部配置设置。
3. 在“**显示的列**”设置组中，选中与要在表中查看的设置相对应的复选框。您必须至少选择一项设置。
4. 如果要更改列的显示顺序，请选择需要在表中向左或向右移动的列的名称，然后使用包含向上或向下箭头图像的按钮。

选定的列将按照您指定的顺序显示在表中。

基于标准时间段的过滤

要按标准时间段过滤数据表：

1. 使用应用程序 Web 界面部分中的表时，打开工具栏中的“**时段**”、“**运行周期**”或“**时段**”下拉列表。
2. 在下拉列表中，选择标准时间段之一（例如，**最近 24 小时**）。

该表将显示您指定的时间段内的数据。

根据指定时间段进行过滤

按指定时间段过滤数据表：

1. 在应用程序 Web 界面部分的表格中，在工具栏上，打开“**时段**”、“**时段**”或“**运行周期**”下拉列表。
2. 在下拉列表中，选择“**指定期间**”。

   过滤周期的开始和结束日期和时间显示在下拉列表的右侧。
3. 单击时间段的开始或结束日期。

   日历打开。
4. 在日历中，指定过滤时间段的开始和结束边界的日期。为此，请在日历中选择一个日期（将指示当前时间）或以 DD-MM-YYYY hh:mm:ss 格式手动输入值。如果不需要指定过滤时间段结束边界的日期和时间，可以选择不选择日期，也可以删除当前值。
5. 单击**确定**。

该表将显示您指定的时间段内的数据。

按列过滤

要按特定列过滤表：

1. 在应用程序 Web 界面的某个部分的表格中，单击相关列中的过滤图标。
   将打开“过滤”窗口。
2. 根据需要使用过滤器窗口中的界面元素来配置设置。以下是在某些列中配置过滤器时的一些特殊注意事项。
3. 单击“**确定**”。

如果过滤器窗口包含“**复杂**”字段

使用“**复杂**”字段指定由逻辑运算符 AND 组合的多个值。要添加不同类型的值，请单击“**添加条件 (AND)**”。

如果有一列用于设备组

1. 在过滤器窗口中，单击字段右侧的 图标以选择组。
   将出现“**在树中选择组**”窗口。
2. 在设备组树中，选择相关组并单击“**选择**”按钮。
   所选组的路径显示在过滤器窗口的字段中。

如果有与设备相关的风险列

1. 在过滤器窗口中，使用“**排除有风险的设备**”切换按钮来配置表中设备的显示：
   - 要仅查看无风险设备，请打开切换按钮。
   - 要查看存在风险的设备并配置按风险过滤的设置，请关闭切换按钮。
2. 如有必要，请使用以下控件来配置过滤有风险的设备的设置：
   - **风险分数** – 允许您定义一系列风险评分值，以显示其风险的评分在指定范围内的设备。
   - **状态** – 允许您基于风险状态启用和禁用过滤（如果在设备表显示设置中选中“**显示已补救和已接受的风险**”，则会显示相应按钮）。

如果有显示支持的应用程序协议的“**协议**”列

1. 在过滤器窗口中，在“**协议**”字段中指定必要的协议。为此，请开始输入协议名称，然后从下拉列表中选择相关协议（当“**协议**”字段中的值更改时，合适协议的列表会自动展开）。
2. 如有必要，请单击“**排序**”对打开的协议列表进行排序。
3. 如果要添加其他协议，请单击“**添加协议**”并在打开的字段中指定其他协议。
4. 如果要删除指定协议之一，请单击过滤器窗口中的 图标。您还可以通过单击过滤器窗口中的“**默认过滤器**”来删除所有指定的协议。

如果有一个“**协议**”栏，以协议栈树的形式显示所有支持的协议

1. 在过滤器窗口，使用包含后续层协议的协议名称旁边的 **+** 和 **-** 按钮配置相关树元素的显示方式。

   表列提供以下信息：

   - **协议** – 协议栈树中协议的名称。
   - **以太网类型** – 以太网协议中下一级协议的编号（如果协议有定义的编号）。它以十进制格式显示。
   - **IP 编号** – IP 协议中下一级协议的编号（如果协议有定义的编号）。它仅针对 IP 协议结构内的协议进行指示。它以十进制格式显示。
2. 如有必要，请使用表格上方的搜索字段查找相关协议。
3. 在协议列表中，选中您要用来过滤事件的协议旁边的复选框。

   如果选中或清除包含嵌套协议的协议的复选框，则也会自动选中或清除嵌套协议的复选框。

如果允许基于表格单元格值进行过滤

1. 选择数据表中的相关项目。
2. 将鼠标光标移到所选项目之一的相关列的单元格上。
3. 右键单击打开上下文菜单。
4. 在上下文菜单中，选择显示包含特定参数值的所有项目的命令。

用于过滤事故中的事件的模式

以树形显示模式过滤事件表时，满足过滤条件的事故可能会以以下形式呈现：

- 与所有嵌套元素一起显示
- 仅与也满足定义的过滤条件的嵌套元素一起显示

您可以在配置表时使用“**过滤时显示嵌入的事件**”复选框来选择事故的相关显示选项。

表搜索

在应用程序 Web 界面的某个部分的表格中，您可以使用“**搜索<显示项目的类型>**”字段查找相关项目。该字段显示在该部分的右侧部分。

可以对选定的表列运行搜索。

重置定义的过滤器和搜索设置

在应用程序 Web 界面的某个部分的表格中，您可以通过单击工具栏中的“**默认过滤器**”重置定义的过滤器和搜索设置。如果定义了搜索或过滤器设置，则会显示该按钮。

表排序

要对表格进行排序：

1. 在应用程序 Web 界面的某个部分的表格中，单击要作为排序依据的列的标题。

   可排序的列标题显示为链接。

2. 如果基于显示不同值类型的列（例如“**风险**”部分中的“**端 1**”列）执行排序，请使用列标题的下拉列表选择将用于排序的设置。

3. 如果需要根据多列对表格进行排序，请按住 **SHIFT** 键，同时单击要作为排序依据的列的标题。

   该表将按所选列排序。按多列排序时，表的行按照列选择的顺序排序。在用于排序的列标题旁边，您将看到显示当前排序顺序的图标：按值的升序或降序排列。

选择数据表中的元素

在应用程序 Web 界面的某个部分的表格中，您可以选择任何显示的项目来查看其详细信息并管理这些项目。当您选择表中的项目时，您将在 Web 界面窗口的右侧看到详细信息区域。

要选择表中的相关项目，请执行以下操作之一：

- 如果要选择一项，请选中包含此项的行左侧的复选框或使用鼠标选择表格行。
- 如果要选择多个项目，请选中包含相关项目的行左侧的复选框，或在按住 **CTRL** 或 **SHIFT** 键的同时选择它们。
- 如果要选择满足当前过滤器和搜索设置的所有项目，请执行以下操作之一：
  - 选择表中的任意项目并按组合键 **CTRL+A**。
  - 选中表最左列标题中的复选框。

如果选择了多个项目，则其编号数据将显示在 Web 界面页面的右上角。显示的所选项目的精确数量不超过特定限制（例如，最多 2000 个项目）。如果选择更多项目，则不会显示精确的数字（在上面的示例中，将显示 `2000+`）。如果表中未选择任何项目，则页面右上角将显示数据表中的总项目数。

表最左列的标题显示项目选择复选框。根据所选项目的数量，复选框可以具有以下状态之一：

- ☐ – 未在表中选择满足当前过滤器和搜索设置的任何项目。在这种情况下，可以使用行左侧的复选框或使用 **CTRL** 或 **SHIFT** 键在表中选择一个或多个项目。
- ☑ – 在表中选择了满足当前过滤器和搜索设置的所有项目。
- ▣ – 在表中选择了满足当前过滤器和搜索设置的所有项目，但随后清除了某些项目的复选框。如果清除了以这种方式选择的所有项目的复选框（因为所选项目的数量可能会发生变化），也会保留此状态。

如果选择了满足过滤器和搜索设置的所有项目，则所选项目的数量可能会自动更改。例如，这可能是由于用户在另一个连接会话中的操作或发现新项目时发生的。建议您配置过滤器和搜索设置，以便您只看到选择中的相关项目。

导航到其他 Web 界面部分中的相关项目

应用程序 Web 界面的某些部分（特别是数据表中）的项目可以与包含表或数据结构的其他部分中的项目相关联。例如，事件可能与设备或风险相关。处理此类项目时，您可以导航至其他部分中的相关项目以查看详细信息。

要查看有关相关项目的信息：

1. 选择您想要查看其相关项目信息的项目。

   建议选择有限数量的项目（最多 200 个）。当您选择大量项目时，您可能无法导航以查看相关项目。

2. 打开工具栏中的“**显示相关**”下拉列表。
3. 在下拉列表中，选择所需的项目类型（例如，**设备**）。

   一个部分将打开，其中包含所选类型的项目（在此示例中为“**资产**”部分中的设备表）。应用相应的过滤来显示相关项目。

将数据从表导出到文件

应用程序 Web 界面某些部分的数据表提供了将数据导出为以下格式的文件的功能：

- CSV

  导出为此格式时，文件会保存表中当前显示的列中的信息。表中未显示的某些数据（例如，附加字段和设备信息中的过程控制设置）也可以以这种格式存储。

- JSON

  以这种格式导出文件时，将保存表项的所有数据，包括数据库中的服务信息（例如与设备相关联的事件信息）。

您可以导出满足当前过滤和搜索设置的所有项目的信息，也可以选择性地导出表中显示的项目的信息。

要导出满足当前过滤和搜索设置的所有项目的数据，请执行以下操作：

1. 单击数据表上方工具栏中的“**导出**”以打开菜单，并选择具有所需文件格式的项目：CSV 或 JSON。
2. 如果保存补充设置的选项可用于导出，请在显示的窗口中，选中要导出的设置的复选框。

   文件创建过程开始。
3. 如果文件生成需要很长时间（超过 15 秒），则操作将移至后台。如果是这种情况，请按照以下步骤下载文件：

   a. 单击应用程序 Web 界面菜单中的 。

   后台操作列表打开。

   b. 等待文件生成操作完成。

   c. 单击“**下载文件**”。

您的浏览器将保存下载的文件。根据您的浏览器设置，您的屏幕可能会显示一个窗口，您可以在其中更改保存的文件的路径和名称。

要导出所选项目的数据，请执行以下操作：

1. 选择要将其信息导出到文件中的项目。
2. 右键单击可显示其中一个选定项目的上下文菜单。
3. 在上下文菜单中，选择相关的文件格式选项：CSV 或 JSON。
4. 如果保存补充设置的选项可用于导出，请在显示的窗口中，选中要导出的设置的复选框。

   文件创建过程开始。
5. 如果创建文件需要很长时间（超过 15 秒），请执行步骤 3 的必要操作，如导出所有项目的数据的过程中所述。

更新数据表

当您查看表时，可能会在服务器上更改应用程序 Web 界面某一部分的表中显示的特定数据（例如，当注册了新项目或在连接到服务器的不同会话中修改了数据时）。有些表支持自动更新数据。

要启用或禁用表中数据的自动更新，请执行以下操作：

在数据表上方的工具栏中，使用“**更新**”切换开关。

更改您的账户密码

通过 Web 界面连接到服务器后，您可以更改用于建立连接的用户账户的密码。只有在应用程序中创建的用户账户才能在 Kaspersky Industrial CyberSecurity for Networks Web 界面页面上更改用户密码。此密码更改方法不适用于配置了单点登录 (SSO) 的 Kaspersky Security Center 用户账户。

建议您在以下情况下修改密码：

- 用户自创建或解锁账户以来首次连接，或者密码已被管理员更改。

  如果管理员在账户创建后您第一次连接到应用程序时和/或管理员更改密码后为您的账户启用了强制密码更改，则账户凭据输入页面上将显示“**新密码**和**重新输入新密码**”字段，以更改密码。

- 当前密码已被泄漏。
- 密码即将过期。

要更改您自己的用户账户的密码：

1. 在 Kaspersky Industrial CyberSecurity for Networks Web 界面页面上，打开用户菜单：
   - 如果菜单折叠，请单击按钮。
   - 如果菜单展开，请单击当前用户姓名右侧的按钮。
2. 在用户菜单中，选择“**更改密码**”。

   出现**更改密码**窗口。
3. 在“**当前密码**”字段中，输入您的当前密码。
4. 在“**新密码**”和“**重新输入新密码**”字段中输入新的密码。

   新密码必须符合**更改密码**窗口中列出的条件。当您输入密码时，您所满足的条件会被自动标记。
5. 单击**编辑**。输入当前密码和新密码并满足新密码的所有要求后，此按钮可用。

下次通过 Web 界面连接到服务器时将需要输入新密码。

通过 Kaspersky Security Center 管理应用程序

Kaspersky Security Center 的集中管理功能可扩展 Kaspersky Industrial CyberSecurity for Networks 的管理功能，并使应用程序更易于使用。此外，Kaspersky Security Center 还通过策略为 Kaspersky Industrial CyberSecurity 解决方案的其他组件（例如 Kaspersky Industrial CyberSecurity for Nodes 和 Kaspersky Industrial CyberSecurity for Linux Nodes）提供集中管理功能。在 Kaspersky Security Center 的管理下，EPP 应用程序会扫描设备以查找入侵指标。如果检测到入侵指标，结果将发送到 Kaspersky Industrial CyberSecurity for Networks。

Kaspersky Security Center 管理服务器可以作为应用程序已安装更新的源。在这种情况下，您无需手动下载、复制和安装更新，也无需为服务器计算机提供互联网访问权限。

本节包含有关配置应用程序与 Kaspersky Security Center 之间的交互的信息，以及有关使用 Kaspersky Security Center 功能与 Kaspersky Industrial CyberSecurity for Networks 进行工作的信息。您可以使用 Kaspersky Security Center 执行以下操作：

- 向 Kaspersky Industrial CyberSecurity for Networks 添加授权许可密钥。
- 下载应用程序模块和数据库的更新至 Kaspersky Industrial CyberSecurity for Networks。
- 在 Kaspersky Security Center 管理控制台中查看 Kaspersky Industrial CyberSecurity for Networks 事件。
- 在管理控制台或 SCADA 系统中监控 ICS 安全状态。
- 远程连接到 Kaspersky Industrial CyberSecurity for Networks 服务器计算机。
- 从 Kaspersky Security Center Web Console 使用 Kaspersky Industrial CyberSecurity for Networks 的集中系统监控的高级功能。
- 当 Kaspersky Security Center Web Console 用户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器时，使用单点登录技术对其进行身份验证。

可用操作列表的内容取决于当前的 Kaspersky Security Center 版本的功能。您可以在Kaspersky Security Center 帮助系统中查看有关 Kaspersky Security Center 各个版本的主要功能的信息。

为了实现 Kaspersky Industrial CyberSecurity for Networks 与 Kaspersky Security Center 之间的交互，必须满足以下条件：

- 在集中式或本地安装 Kaspersky Industrial CyberSecurity for Networks 服务器期间，添加了应用程序与 Kaspersky Security Center 交互的功能。
- 在 Kaspersky Industrial CyberSecurity for Networks 中，与 Kaspersky Security Center 交互的功能已启用并配置。
- Kaspersky Industrial CyberSecurity for Networks 管理插件安装在 Kaspersky Security Center 中（一个或两个插件，具体取决于 Kaspersky Security Center 的版本以及您希望使用 Kaspersky Security Center 执行的操作）。

- 在上面安装了 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机包含在 Kaspersky Security Center 管理组（**受管理设备**或其子组中）中。当在基于 MMC 的管理控制台中工作时，或者当在 Kaspersky Security Center Web Console 中注册 Kaspersky Industrial CyberSecurity for Networks 时，您可以将设备移动到管理组。

- 用于在 Kaspersky Industrial CyberSecurity for Networks 服务器与 Kaspersky Security Center 管理服务器或 Kaspersky Security Center Web Console 之间进行连接和交互的某些端口和协议可用。

启用并配置与 Kaspersky Security Center 的交互

在集中式或本地安装过程中，将与 Kaspersky Security Center 交互的功能添加到应用程序后，该功能默认处于禁用状态。

要启用并配置应用程序与 Kaspersky Security Center 交互的功能：

1. 使用管理员账户通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器。
2. 选择“**设置**” → “**Kaspersky Security Center**”。
3. 使用“**已启用**”拨动开关启用与 Kaspersky Security Center 的交互。
4. 在“**连接器设置**”块中，配置 **Kaspersky Security Center 连接器**：
   - Kaspersky Security Center 管理服务器所在计算机的 IP 地址/网络名称。
   - 用于连接的 SSL 端口。
   - 每天中继事件的最大数量，从 Kaspersky Industrial CyberSecurity for Networks Server 所在时区的 0:00 开始。默认值是 2000。您可以根据系统架构、规模和部件的具体功能更改此参数的值。输入值范围：0–65535。
5. 在 **Kaspersky Security Center Web Console 的 Web 插件设置**块中，配置来自 Kaspersky Security Center Web Console 的连接设置：
   - 当从 Kaspersky Security Center Web Console 注册操作时，将在审核日志条目中指示 Kaspersky Industrial CyberSecurity for Networks 用户名。
   - Kaspersky Industrial CyberSecurity for Networks 服务器计算机上的 Web 服务器的 IP 地址/网络名称。
   - Kaspersky Industrial CyberSecurity for Networks 服务器计算机上的 REST API 服务器的 IP 地址/网络名称。
6. 单击“**应用**”。
7. 保存设置后，请验证是否满足条件，并完成通过 Kaspersky Security Center 监控事件的其他配置。

8. 检查网络代理与 Kaspersky Security Center 管理服务器之间的连接。为此，请在执行 Kaspersky Industrial CyberSecurity for Networks 服务器功能的计算机上，打开操作系统控制台并输入以下命令：

```
sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

屏幕将显示有关管理服务器连接的信息。如果成功完成这些步骤，屏幕上会显示以下消息：

```
正在连接到服务器...确定
正在连接到管理代理...确定
```

从 Kaspersky Security Center 向 Kaspersky Industrial CyberSecurity for Networks 添加授权许可密钥

您可以使用自动向 Kaspersky Security Center 分发授权许可密钥的功能，将授权许可密钥添加到 Kaspersky Industrial CyberSecurity for Networks。以这种方式收到的授权许可密钥在 Kaspersky Industrial CyberSecurity for Networks 中的处理方式与在应用程序中手动添加的授权许可密钥相同。

如果满足 Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky Security Center 之间通信的所有条件，自动授权许可密钥分发就会有效。

要分发授权许可密钥，您需要先将其添加到 Kaspersky Security Center 管理服务器存储库。您可以使用基于 MMC 的管理控制台或 Kaspersky Security Center Web Console 将授权许可密钥添加到存储中。要添加，请使用授权许可密钥文件。

将授权许可密钥添加到管理服务器存储库后，您可以在基于 MMC 的管理控制台中或在 Kaspersky Security Center Web Console 中创建授权许可密钥分发任务。

从 Kaspersky Security Center 管理服务器接收更新

您可以使用 Kaspersky Security Center 管理服务器作为 Kaspersky Industrial CyberSecurity for Networks 数据库和应用程序模块的更新源。例如，如果您需要从卡巴斯基服务器下载更新，而托管 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机无法访问互联网，则可能需要这种接收更新的方法。

准备将 Kaspersky Security Center 管理服务器用作更新源的方案包括以下步骤：

1. **在 Kaspersky Security Center 中创建任务以将更新下载到管理服务器存储库**

   您可以在基于 MMC 的管理控制台或 Kaspersky Security Center Web Console 中创建任务。

2. **在 Kaspersky Industrial CyberSecurity for Networks 中选择管理服务器作为更新源**

   通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks 服务器时，您可以在手动启动更新过程和/或配置自动更新时选择 Kaspersky Security Center 管理服务器作为更新源。

通过 Kaspersky Security Center 监控事件

在 Kaspersky Security Center 中，有关 Kaspersky Industrial CyberSecurity for Networks 事件的信息显示在事件表的以下列中：

- **时间**或**事件发生时间**是指在安装 Kaspersky Security Center 的计算机所在的时区中，Kaspersky Industrial CyberSecurity for Networks 事件的注册时间。
- **设备**是指 Kaspersky Security Center（安装了 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机）中受管理设备的名称。
- **事件**是指为 Kaspersky Industrial CyberSecurity for Networks 事件定义的 Kaspersky Security Center 事件类型的名称。
- **描述**是指 Kaspersky Industrial CyberSecurity for Networks 事件的标题和简要描述。
- **组**或**管理组**是管理组的名称，该组包含位于 Kaspersky Security Center 管理控制台树中**受管理设备**文件夹中托管 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机。
- **应用程序**是指应用程序名称（Kaspersky Industrial CyberSecurity for Networks）。
- **版本号**即应用程序的版本号。
- **重要级别**或**严重级别**是指事件的重要性级别，取决于 Kaspersky Security Center 的事件重要性分类。
- **注册日期**或**事件注册时间**是指事件在Kaspersky Security Center 数据库中注册的时间。

从 Kaspersky Industrial CyberSecurity for Networks 中继的事件的参数值根据 Kaspersky Industrial CyberSecurity for Networks 的本地化设置予以显示。这些参数不考虑 Kaspersky Security Center 的本地化语言。

如果 Kaspersky Industrial CyberSecurity for Networks 事件包含有关多个网络交互的信息，该事件将被转换为 Kaspersky Security Center 事件表中的单独项目。这样，Kaspersky Security Center 中就会为 Kaspersky Industrial CyberSecurity for Networks 事件中指定的每个网络交互创建单个事件。

在 Kaspersky Security Center 事件中显示 Kaspersky Industrial CyberSecurity for Networks 事件：

1. 确保 Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky Security Center 中安装了所需的组件。
2. 确保用于连接托管 Kaspersky Security Center的计算机的端口在托管 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机上已开启且可访问。
3. 当在 Kaspersky Security Center 中配置网络代理策略设置时，启用将相关事件保存到管理服务器数据库并定义事件保留期。

   当在基于 MMC 的管理控制台中工作或在 Kaspersky Security Center Web Console 中工作时，您可以在网络代理策略设置中配置事件注册和保留。
4. 在 Kaspersky Industrial CyberSecurity for Networks 中，配置通过 Kaspersky Security Center 连接器**转发事件**。

当特定事件类型在 Kaspersky Industrial CyberSecurity for Networks 中注册时，这些事件也将显示在 Kaspersky Security Center 事件表中。

Kaspersky Security Center 中针对 Kaspersky Industrial CyberSecurity for Networks 事件的事件类型

Kaspersky Security Center 使用一组固定的事件类型来接收 Kaspersky Industrial CyberSecurity for Networks 事件。Kaspersky Security Center 中的事件类型与Kaspersky Industrial CyberSecurity for Networks 中特定的事件类型相对应，并且可以根据事件的严重程度注册为 Kaspersky Security Center 事故（见下图）。

Kaspersky Security Center 中用于接收 Kaspersky Industrial CyberSecurity for Networks 事件的事件类型

显示的事件类型名称	Kaspersky Security Center 事件类型的代码	注册为 Kaspersky Security Center 事故	Kaspersky Industrial CyberSecurity for Networks 中的对应事件类型代码
已达到报告事件的最大数量	32769	是的，带有“*警告*”严重级别	–
测试事件 (DPI)	32770	否	4000000001
测试事件 (NIC)	32771	否	4000000002
测试事件 (IDS)	32772	否	4000000003
测试事件 (AM)	32773	否	4000000004
检测到未经授权的网络交互	32774	否	4000002601
检测到系统命令	32775	仅限严重级别为“*严重*”的事件	4000002602
监控点无流量	32776	否	4000002700
检测到 TCP 协议异常：重叠 TCP 段中的内容替换	32777	否	4000002701
违反过程控制规则	32778	仅限严重级别为“*严重*”的事件	4000002900
系统规则集中的入侵检测规则被触发	32779	否	4000003000
用户定义的规则集中的入侵检测规则被触发	32780	否	4000003001
在 ARP 回复中检测到 ARP 欺骗的征兆	32781	是	4000004001
在 ARP 请求中检测到 ARP 欺骗的征兆	32782	是	4000004002
在网络上检测到新设备	32783	是	4000005003
检测到新的设备设置	32784	否	4000005004
检测到 IP 地址冲突	32785	是	4000005005
从具有存档状态的设备中检测到活动	32786	否	4000005006
检测到新的设备 IP 地址	32787	是	4000005007
检测到新的设备 MAC 地址	32788	是	4000005010
添加了设备的 MAC 地址	32789	否	4000005008
添加了设备的 IP 地址	32790	否	4000005009
PLC 项目控制：检测到从 PLC 读取未知块	32791	否	4000005200
PLC 项目控制：检测到从 PLC 读取已知块	32792	否	4000005201
PLC 项目控制：检测到向 PLC 写入新块	32793	否	4000005202

显示的事件类型名称	Kaspersky Security Center 事件类型的代码	注册为 Kaspersky Security Center 事故	Kaspersky Industrial CyberSecurity for Networks 中的对应事件类型代码
PLC 项目控制：检测到向 PLC 写入已知块	32794	否	4000005203
PLC 项目控制：检测到从 PLC 读取未知项目	32795	否	4000005204
PLC 项目控制：检测到从 PLC 读取已知项目	32796	否	4000005205
PLC 项目控制：检测到向 PLC 写入新项目	32797	否	4000005206
PLC 项目控制：检测到向 PLC 写入已知项目	32798	否	4000005207
检测到 IP 协议异常：组装 IP 数据包时发生数据冲突	32799	否	4000005100
检测到 IP 协议异常：超过分段 IP 数据包大小	32800	否	4000005101
检测到 IP 协议异常：IP 数据包的初始片段的大小小于预期	32801	否	4000005102
检测到 IP 协议异常：误相关片段	32802	否	4000005103
已注册关联规则事件	32803	仅限严重级别为 *"严重"* 的事件	8000000001
来自外部系统的事件	32804	仅限严重级别为 *"严重"* 的事件	4000005400
在从 EPP 应用程序接收的数据中发现设备的不同 MAC 地址	32805	是	4000005011
在从 EPP 应用程序接收的数据中发现设备的新地址信息	32806	是	4000005012
从 EPP 应用程序接收数据后，在设备地址中检测到冲突	32807	是	4000005013
根据 EPP 应用程序的数据添加了子网	32808	是	4000005014
检测到设备更改	32809	否	4000005015

Kaspersky Security Center 事件严重性级别对应关系

Kaspersky Security Center 中事件的严重性与 Kaspersky Industrial CyberSecurity for Networks 事件的严重性级别相对应（见下表）。对于 Kaspersky Industrial CyberSecurity for Networks 事件的严重性级别，指定了以前应用程序版本中使用的严重性级别的对应名称。

事件严重性之间的对应关系

Kaspersky Security Center 事件严重性	Kaspersky Industrial CyberSecurity for Networks 事件严重性
信息	*低（信息）*
警告	*中（警告）*
严重	*高（严重）*

监控 ICS 安全状态：Kaspersky Security Center和 SCADA

Kaspersky Industrial CyberSecurity for Networks 可以将有关 ICS 安全状态的数据转发到 Kaspersky Security Center。要将数据传输到 Kaspersky Industrial CyberSecurity for Networks 和 Kaspersky Security Center，必须安装所需的组件。

如果已配置将 ICS 安全状态数据传输到 Kaspersky Security Center，您可以配置 SCADA 系统以从 Kaspersky Security Center 接收相应信息。

要配置 SCADA 系统以接收和显示 ICS 安全状态：

1. 在托管 Kaspersky Security Center 的计算机上，安装 Kaspersky Security Gateway。

   在"*Kaspersky Security Gateway 管理员指南*"中，可找到有关安装和配置 Kaspersky Security Gateway 的详细信息。

2. 在 SCADA 系统中，创建可反映安装有 Kaspersky Industrial CyberSecurity for Networks 的计算机的状态的控制元素。

3. 配置创建的控制元素以通过 OPC DA 2.0 或 IEC 60870-5-104 协议接收数据。

   "*Kaspersky Security Gateway 管理员指南*"中提供了有关配置控制元素的说明。

从 Kaspersky Security Center 连接到服务器计算机

您可以从 Kaspersky Security Center 管理控制台远程连接到 Kaspersky Industrial CyberSecurity for Networks 服务器计算机。这需要使用基于 MMC 的管理控制台。虚拟网络计算 (VNC) 远程桌面访问系统被用来建立连接。

若要连接，您必须安装并配置以下 VNC 组件：

- VNC 服务器。它安装在执行 Kaspersky Industrial CyberSecurity for Networks 服务器功能的计算机上。配置 VNC 服务器时，需要设置用于 VNC 连接的密码。如果计算机上启用了防火墙，您还需要打开 VNC 和 SSH 协议的端口。

- VNC 客户端。它安装在具有 Kaspersky Security Center 管理控制台的计算机上。

若要从 Kaspersky Security Center 访问 Kaspersky Industrial CyberSecurity for Networks 服务器电脑：

1. 打开 Kaspersky Security Center 管理控制台。

2. 在 Kaspersky Security Center 管理控制台树中的**受管理设备**文件夹中，选择包含安装了 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机的管理组。

3. 在工作区中的**设备**选项卡中，选择托管 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机，然后在计算机的上下文菜单中选择**自定义工具→ VNC**。

默认情况下，VNC 工具不存在于外部工具列表中。要添加该工具，请在计算机的上下文菜单中选择**自定义工具→配置自定义工具**。在**自定义工具**窗口中，单击**添加**按钮并指定以下设置值：

- 在**工具名称**字段中，为工具输入任意名称（例如，`VNC`）。
- 在**可执行文件名称**段中，输入 VNC 客户端的可执行文件的完整路径（例如，`C:\Program Files\TightVNC\tvnviewer.exe`）。
- 在**工作文件夹**字段中，输入 VNC 客户端的工作文件夹的完整路径（例如，`C:\Program Files\TightVNC\`）。
- 在**命令行**字段中，输入以下值：`<A>:<P>`。
- 选择**为下面指定的 TCP 端口创建通道**复选框，然后输入 VNC 服务器上的 VNC 端口号（例如，如果 VNC 服务器使用屏幕：3，则输入 VNC 端口号`5903`）。

4. 外部 VNC 工具启动后，会出现一个密码提示窗口。输入用于 VNC 连接的密码。

打开的窗口显示安装了 Kaspersky Industrial CyberSecurity for Networks 服务器的计算机的桌面。

从 Kaspersky Security Center Web Console 使用 Kaspersky Industrial CyberSecurity for Networks 集中监控系统

Kaspersky Security Center Web Console（以下也称为“Web Console”）提供了扩展功能，用于集中监控运行 Kaspersky Industrial CyberSecurity for Networks 的信息系统的安全状态。在 Web Console 中使用 Kaspersky Industrial CyberSecurity for Networks 管理 Web 插件（以下也称为“Web 插件”）时，可以使用这些扩展功能。要使用 Web 插件，必须将其安装在安装了 Kaspersky Security Center Web Console 的计算机上。

安装并配置 Web 插件后，您可以在 Web Console 中执行以下操作：

- 通过使用专为使用 Kaspersky Industrial CyberSecurity for Networks 而设计的小部件，监控 Kaspersky Industrial CyberSecurity for Networks 控制的系统和 Kaspersky Industrial CyberSecurity for Networks 服务器。
- 使用各种过滤条件在选定 Kaspersky Industrial CyberSecurity for Networks 服务器的数据库中搜索设备和事件。
- 在地理、原理图或其他图像上映射 Kaspersky Industrial CyberSecurity for Networks 的组件和组件组，以根据对象的位置排列对象。
- 将 Kaspersky Industrial CyberSecurity for Networks 的组件分组为组织单位（以下也称为“站点”），这些组织单位在逻辑上界定 Kaspersky Industrial CyberSecurity for Networks 的控制和/或部署区域。

使用上面列出的功能时，您可以快速从 Web Console 切换到通过 Web 界面连接到必要的 Kaspersky Industrial CyberSecurity for Networks 服务器。如果使用单点登录技术，则在 Kaspersky Industrial CyberSecurity for Networks 中创建的用户在连接到 Kaspersky Industrial CyberSecurity for Networks 服务器时无需输入其账户凭据。登录 Web Console 的用户也可以完成身份验证。

关于更新 Kaspersky Industrial CyberSecurity for Networks 管理 Web 插件

已安装的 Kaspersky Industrial CyberSecurity for Networks 管理 Web 插件有助于应用程序和 Kaspersky Security Center Web Console 之间的交互。

您可以在 Web 控制台界面中查看已安装的 Web 插件的列表：**控制台设置** → **Web 插件**。

如果新版本的 Web 插件可用，则 Web Console 将显示“*更新可用于已使用的插件*”通知。您可以通过此 Web Console 通知继续更新 Web 插件版本。您也可以在 Web Console 界面中手动检查新的 Web 插件更新（**控制台设置**→ **Web 插件**）。更新过程中将自动删除以前版本的 Web 插件。

更新 Web 插件时，将保存现有组件（如添加的小部件或地图图像）。实现 Kaspersky Industrial CyberSecurity for Networks 新功能的组件的新设置将具有默认值。

您可以使用以下任意方法更新 Web 插件：

- 在联机模式下，在 Web 插件列表中更新 Web 插件。

  要更新网络插件，请在 Web Console 界面中选择 Kaspersky Industrial CyberSecurity for Networks 插件的分发包，然后启动更新（**控制台设置** → **Web 插件**）。Web Console 检查卡巴斯基服务器上的可用更新并下载相关更新。

- 从文件更新 Web 插件。

  要更新 Web 插件，请在 Web Console 界面中选择 Kaspersky Industrial CyberSecurity for Networks Web 插件的分发包的 ZIP 存档：**控制台设置** → **Web 插件**。例如，Web 插件的分发包可以从卡巴斯基网站下载。对于应用程序的本地版本，还需要下载包含签名的文本文件。

  您只能将 Web 插件更新到新版本。Web 插件无法更新到旧版本。

单点登录（SSO）技术使用准备场景

与 Kaspersky Security Center 结合使用时，您可以使用单点登录 (SSO) 技术。这使得已登录 Kaspersky Security Center Web Console 的用户在通过 Web 界面连接到 Kaspersky Industrial CyberSecurity for Networks Server 时也能成功完成身份验证。这意味着任何被允许使用 Kaspersky Security Center Web Console 的用户账户（包括 Active Directory® 用户）都可以使用自己的账户凭据连接到服务器。

单点登录技术可在 Kaspersky Security Center 的兼容版本中与 Kaspersky Industrial CyberSecurity for Networks 一起使用：

单点登录（SSO）技术使用准备场景包括以下步骤：

1. **验证并满足 Kaspersky Industrial CyberSecurity for Networks 与 Kaspersky Security Center 之间交互所需的条件**

   在此步骤中，您需要验证是否满足 Kaspersky Industrial CyberSecurity for Networks 与 Kaspersky Security Center 之间交互的所有条件。如果任何条件未满足，请确保满足这些条件。例如，如果 Kaspersky Industrial CyberSecurity for Networks 中未配置与 Kaspersky Security Center 交互的功能，请启用并配置此功能。

2. **启用和配置 Kaspersky Security Center Web Console 身份和访问管理器 (IAM) 组件**

   在此步骤中，将按照 Kaspersky Security Center 帮助系统 中的说明执行启用身份和访问管理器的方案。

   配置 IAM 组件时，建议仅当可从 Kaspersky Industrial CyberSecurity for Networks Server 所在计算机通过该名称访问此计算机时，才将此计算机的 DNS 名称指定为设备的网络名称。如果只能通过 IP 地址访问，请指定此 IP 地址而不是 DNS 名称。

3. **将 Kaspersky Industrial CyberSecurity for Networks Server 注册为 IAM 组件的客户端**

   在此步骤中，IAM 组件会检测准备注册为本组件客户端的 Kaspersky Industrial CyberSecurity for Networks 服务器。检测到服务器注册请求后，您需要接受该请求。检测到并注册的 IAM 组件客户端显示在一个表中，您可以在 Kaspersky Security Center Web Console 的“**控制台设置**” → “**整合**” → “**身份和访问管理器**”下打开该表。要注册服务器，请通过单击包含已注册客户端信息的部分中的“**设置**”链接打开表，选中相关服务器旁边的复选框，然后单击“**批准**”。

   确认注册 IAM 组件客户端后，您需要等待准备过程完成。当 IAM 组件与客户端之间的同步完成后，将显示该客户端的就绪状态。如果状态未更改，请单击“**刷新**”按钮。

   > IAM 组件需要一些时间来检测客户端并与它们同步。根据 Kaspersky Security Center 管理服务器和 Kaspersky Industrial CyberSecurity for Networks Server 的工作负载，完成这些操作最多可能需要 15 分钟。

4. **为用户准备连接到 Kaspersky Industrial CyberSecurity for Networks 的访问权限**

   在此阶段，您需要根据 Kaspersky Industrial CyberSecurity for Networks 中用户的角色（管理员、安全官、基础设施官、ICS 官和操作员）授予 Kaspersky Security Center 用户访问权限。为此，您可以使用现有用户账户或专门为仅授予这些权限而创建的用户和组的新账户。

当此场景实现时，Kaspersky Industrial CyberSecurity for Networks 将能够使用 Kaspersky Security Center 用户的账户凭据通过 Web 界面连接到服务器。为此，您可以使用 Kaspersky Industrial CyberSecurity for Networks Web 界面的账户凭据输入页面上的“**Kaspersky Security Center 用户**”按钮。连接到服务器后，如果用户被授予相应的权限，则可以在应用程序中执行操作。应用程序不会要求这些用户输入密码来执行需要密码确认的操作（例如，启动某些响应操作）。

> 如果在使用 Kaspersky Security Center Web Console 配置连接设置时为 Web 服务器和 REST API 服务器指定了完全限定域名 (FQDN)，则在使用单点登录技术连接到 Kaspersky Industrial CyberSecurity for Networks Server 时，用户还必须在浏览器的地址栏中指定该名称。

授予 Kaspersky Security Center 用户与其在 Kaspersky Industrial CyberSecurity for Networks 中的用户角色相对应的访问权限

要利用单点登录技术并在 Web 控制台中执行特定操作，必须为 Kaspersky Security Center 用户授予与其在 Kaspersky Industrial CyberSecurity for Networks 中的用户角色相对应的访问权限。将包含 Kaspersky Industrial CyberSecurity for Networks 的基于权限的访问控制模型 (RBAC) 的配置的文件上传到 Kaspersky Security Center 管理服务器后，您可以授予这些权限。

安装 Kaspersky Industrial CyberSecurity for Networks 管理 Web 插件后会自动加载配置。如果配置已上传到管理服务器，则名为 KICS4NET_<文件版本号>.conf 的文件将保存在文件夹 %ProgramData%\KasperskyLab\adminkit\1093\dat\rbac\ 中。如果指定的文件夹不包含名为 KICS4NET_<文件版本号>.conf 的文件，请创建并配置“将更新下载到管理服务器存储库”任务。您可以选择卡巴斯基更新服务器作为更新源。

加载 Kaspersky Industrial CyberSecurity for Networks 的 RBAC 配置后，Kaspersky Security Center 将提供为用户分配对应于 Kaspersky Industrial CyberSecurity for Networks 中的管理员、安全官、基础设施官、ICS 官和操作员角色的权限的功能。

Kaspersky Industrial CyberSecurity for Networks 中的用户角色在 Kaspersky Security Center 的 "**Kaspersky Industrial CyberSecurity for Networks：常规功能**"功能范围内具有以下相应的访问权限：

- **读取**：适用于管理员、安全官、基础设施官、ICS 官和操作员角色
- **写入**：适用于管理员、安全官、基础设施官和 ICS 官角色
- **执行**：适用于管理员和安全官角色
- **管理证书**：适用于管理员角色
- **修改对象 ACL**：适用于管理员角色
- **编辑事件记录设置**：适用于管理员和安全官角色
- **编辑事件通知设置**：适用于管理员角色
- **配置管理服务器层级**：适用于管理员角色
- **在管理员工作站上保存设备文件**：适用于管理员、安全官和 ICS 官角色
- **导出密钥文件**：适用于管理员角色
- **删除事件**：适用于管理员角色
- **为设备分类执行操作**：适用于管理员和安全官角色

除这些权限外，还必须为用户分配功能范围**Kaspersky Security Center 管理服务器：常规功能：基本功能**中的所有权限（此功能范围包括**读取**、**写入**、**执行**和**为设备分类执行操作**的权限）。

如果通过 Kaspersky Security Center 角色向用户分配访问权限，则您必须将包含安装了 Kaspersky Industrial CyberSecurity for Networks Server 的计算机的管理组添加到角色范围。为此，请在角色分配向导的"**定义范围**"页面上，选择"**受管理设备**"管理组。

用于监控系统和 Kaspersky Industrial CyberSecurity for Networks 服务器的小部件

您可以使用小部件来监控由 Kaspersky Industrial CyberSecurity for Networks 控制的系统和 Kaspersky Industrial CyberSecurity for Networks 服务器。Kaspersky Security Center Web Console 在控制板中显示小部件（在"**监控和报告**"→ "**控制板**"下）。默认情况下，控制板不显示 Kaspersky Industrial CyberSecurity for Networks 的小部件。安装 Kaspersky Industrial CyberSecurity for Networks 管理 Web 插件后，您可以添加必要的小部件。

小部件允许您在控制板中显示以下信息：

- KICS for Networks 中的状态。
- KICS for Networks 中的关键事件。
- KICS for Networks 中存在问题的设备。

- KICS for Networks 的最新事件。
- KICS for Networks 部署地图。
- 有关 KICS for Networks 服务器的信息。

Kaspersky Industrial CyberSecurity for Networks 的小部件包括在 Web Console 的可用小部件列表中的“**其他**”类别中。

显示在小部件中的信息每 1-2 分钟自动更新一次。如果两分钟后没有从服务器接收到任何数据，则会隐藏小部件中的过期数据。如有必要，您可以使用小部件菜单中的相关选项手动更新显示的信息。

KICS for Networks 中状态的小部件

Web Console 的“**KICS for Networks 中的状态**”小部件显示分配给 Kaspersky Industrial CyberSecurity for Networks 服务器的当前状态的比率。仅提供相关状态的信息（如果没有具有特定状态的服务器，则此状态不会显示在小部件中）。

以下状态可用于小部件中的服务器：

- *严重*

  如果至少满足以下条件之一，则会将此状态分配给服务器：

  - 服务器有关于应用程序操作中断的消息。
  - 服务器数据库中存在严重性为“*严重*”的未解析事件。
  - 存在具有“*未授权*”状态的设备。
  - 授权许可密钥已到期。
- *警告*

  如果没有满足分配“*严重*”状态的任何条件，但至少满足以下条件之一，则会将此状态分配给服务器：

  - 服务器有关于非关键故障的消息。
  - 服务器数据库中存在严重性为“*警告*”的未解析事件。
  - 授权许可密钥将在 14 天后到期。
- *正常*

  在所有其他情况下（如果服务器可访问并且正在接收数据进行处理），此状态都会分配给服务器。
- *维护*

  如果应用程序当前正在维护中（例如，导入安全策略时），则会将此状态分配给服务器。

如果无法确定服务器的状态，则会显示该服务器的“*未知*”状态。

默认情况下，小部件显示 Kaspersky Security Center 管理组中所有服务器的状态信息。如果两分钟后未从服务器收到数据，则过时信息将不再显示在小部件中。如有必要，您可以使用小部件设置菜单来选择应在小部件中显示其数据的服务器。

KICS for Networks 中关键事件的小部件

Web Console 的“**KICS for Networks 中的关键事件**”小部件显示 Kaspersky Industrial CyberSecurity for Networks 服务器上严重性为“*高*”（对应于“*严重*”严重级别）的未解决事件的比例。对于其数据库包含*高*严重性（对应于“*严重*”严重级别）的未解决事件的每个服务器，将显示这些事件的数量。

小部件中呈现的数据的不同颜色与事件的严重性没有任何关系。小部件图表上的颜色仅用于直观地区分不同服务器的事件。

默认情况下，小部件根据 Web Console 从 Kaspersky Security Center 管理组中的所有服务器接收的数据显示信息。如果两分钟后未从服务器收到数据，则过时信息将不再显示在小部件中。如有必要，您可以使用小部件设置菜单来选择应在小部件中显示其数据的服务器。

KICS for Networks 中存在问题的设备的小部件

Web Console 的“**KICS for Networks 中存在问题的设备**”小部件显示 Kaspersky Industrial CyberSecurity for Networks 应用程序检测到的有问题的设备的信息。在以下任何情况下，设备需要注意（指定为“存在问题”）：

- 设备的安全状态与“*正常*”不同。
- 设备的状态为*未授权*。

如果有设备出现问题，则小部件包含以下信息：

- 有问题的设备数量（在每个设备类别中）。该数据显示在小部件的上部，设备类别图标下。显示的类别数量取决于小部件中的可用空间。如果要显示更多类别，可以通过单击“**显示所有**”打开包含所有类别的窗口。
- 有问题的设备类别列表。该数据显示在小组件的中间部分。将为列表中的每个类别显示以下信息：
  - 包含类别图标和注释的行。行的末尾提供了一个链接，其中包含有问题的设备的数量。
  - 包含代表设备的图形元素的行。如果小组件中有足够的可用空间，则会显示此行。如果出现问题的设备数量多于行中显示的图形元素数量，则隐藏设备的数量将以+<设备数量>格式显示在右侧。

默认情况下，小部件根据 Web Console 从 Kaspersky Security Center 管理组中的所有服务器接收的数据显示信息。如果两分钟后未从服务器收到数据，则过时信息将不再显示在小部件中。如有必要，您可以使用小部件设置菜单来选择应在小部件中显示其数据的服务器。

设备的图形元素

表示设备的图形元素包含以下信息：

- 设备名称。
- 设备状态。如果设备的状态为“*未授权*”，则显示为图标。
- 设备安全状态。这显示为图形元素左边框上的一条彩色线。线的颜色对应于“*正常*”、“*警告*”或“*严重*”状态。

图形元素按以下顺序显示：

1. 设备被分配“*未授权*”状态。
2. 带有“*严重*”安全状态的设备。
3. 带有“*警告*”安全状态的设备。

从小部件导航

您可以使用小部件界面的元素来显示有关设备的详细信息。可以使用以下选项来实现此目的。

在服务器 Web 界面页面的设备表中显示有关所选设备的信息。

在“**KICS for Networks 中存在问题的设备**”小部件中，单击表示相关设备的图形元素。

Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面页面将在浏览器窗口中的新选项卡上打开。打开的选项卡的名称将是安装后应用程序启动配置期间定义的服务器名称。

如果正在使用单点登录技术并且 Web Console 用户有权连接到此服务器，则将授予对服务器 Web 界面的访问权限，而不会提示用户输入其用户账户凭据。

在服务器 Web 界面页面上，“**资产**”部分会自动打开以显示设备表。该表将根据设备 ID 进行筛选。

在 Web Console 的搜索结果表中显示有关选定类别的设备的信息

要显示有关所选类别的所有设备的信息，请执行以下操作：

在“**KICS for Networks 中存在问题的设备**”小部件的上部，单击相关类别的图标。

Web Console 的“**KICS for Networks**” → “**搜索**”部分将打开，显示事件搜索结果表。该表将根据以下条件进行过滤：

- 选定的设备类别
- 小部件中考虑其数据的所有服务器

要显示有关属于特定类别的所有有问题的设备的信息，请执行以下操作：

在包含有问题的设备的类别列表中，单击包含相关类别的设备数量的链接。

Web Console 的“**KICS for Networks**” → “**搜索**”部分将打开，显示事件搜索结果表。该表将根据以下条件进行过滤：

- 选定的设备类别
- 小部件中考虑其数据的所有服务器
- 有问题的设备的指示器

在 Web Console 的搜索结果表中显示有关所有设备的信息

在“**显示所有设备**”小部件中，单击“**KICS for Networks 中存在问题的设备**”。

Web Console 的“**KICS for Networks**” → “**搜索**”部分将打开，显示事件搜索结果表。该表将针对其数据在小部件中被考虑在内的所有服务器进行过滤。

KICS for Networks 最新事件的小部件

Web Console 的“**KICS for Networks 的最新事件**”的小部件显示有关 Kaspersky Industrial CyberSecurity for Networks 事件的一般信息，这些事件具有上次发生的日期和时间的最新值。

小部件包含以下信息：

- 所选期间的事件柱状图。该数据显示在小组件的上部。柱状图按严重级别显示事件的分布情况。
- 已注册事件的列表。该数据显示在小组件的中间部分。事件按上次发生的日期和时间排序。

默认情况下，小部件根据 Web Console 从 Kaspersky Security Center 管理组中的所有服务器接收的数据显示信息。如果两分钟后未从服务器收到数据，则过时信息将不再显示在小部件中。如有必要，您可以使用小部件设置菜单来选择应在小部件中显示其数据的服务器。

事件柱状图

在显示事件分布的柱状图上，条形对应于每个时间间隔的事件总数。在条形内，事件的严重性通过颜色来区分。以下颜色对应严重级别：

- 蓝色 – *低*严重性事件（对应于*信息*严重性级别）。
- 黄色 – *中*严重性的事件（对应于*警告*严重性级别）。
- 红色 – *高*严重性事件（对应于*严重*严重性级别）。

当您将鼠标指针移到柱状图的某个条上时，会显示一个弹出窗口，其中按严重性级别显示事件数量。

时间间隔的持续时间取决于所选的显示时间段。要构建相关柱状图，您可以从小部件菜单中选择以下时间段之一：

- 1 小时。该时间段被划分为一分钟间隔。
- 12 小时，24 小时。这些时间段被划分为一小时的间隔。
- 7 天。该时间段被划分为 12 小时间隔。

事件列表

事件列表中显示的元素数量受小部件大小的限制。

为每个事件提供以下信息：

- 事件标题
- 严重级别
- 托管 Kaspersky Industrial CyberSecurity for Networks Server 的计算机的名称

从小部件导航

您可以使用小部件界面的元素来显示有关事件的详细信息。可以使用以下选项来实现此目的。

在服务器 Web 界面页面的事件表中显示有关所选事件的信息

单击“**KICS for Networks 的最新事件**”的小部件中的相关事件。

Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面页面将在浏览器窗口中的新选项卡上打开。打开的选项卡的名称将是安装后应用程序启动配置期间定义的服务器名称。

如果正在使用单点登录技术并且 Web Console 用户有权连接到此服务器，则将授予对服务器 Web 界面的访问权限，而不会提示用户输入其用户账户凭据。

在服务器 Web 界面页面上，“**事件**”部分会自动打开以显示设备表。该表将根据所选事件的 ID 进行过滤。还将为过滤器定义从事件注册的日期和时间到当前时刻的时间段（不指示该时间段的结束边界）。

在 Web Console 的搜索结果表中显示有关选定时间段内所有事件的信息。

单击“**显示所有事件**”的小部件中的“**KICS for Networks 的最新事件**”。

Web Console 的“**KICS for Networks**” → “**搜索**”部分将打开，显示事件搜索结果表。该表将根据以下条件进行过滤：

- 当前选择的用于在小部件中构建柱状图的时间段
- 小部件中考虑其数据的所有服务器

KICS for Networks 部署图的小部件

Web Console 的“**KICS for Networks 部署地图**”小部件显示了一张地图，描绘了 Kaspersky Industrial CyberSecurity for Networks 组件所在站点的地理分布。小部件使用 Web Console 的“KICS for Networks**KICS for Networks**地图**地图主地图**的较小副本。

地图上的站点由图标指定，图标的颜色取决于站点的状态。以下状态可用于站点：

- *严重*

  如果站点至少包含一个状态为“*严重*”的服务器，则会将此状态分配给该站点。

- *警告*

  如果站点至少包含一个状态为“*警告*”的服务器，且不包含状态为“*严重*”或“*未知*”的服务器，则会将此状态分配给该站点。

- *正常*

  如果站点至少包含一个状态为“*正常*”的服务器，且不包含状态为“*严重*”、“*警告*”、“*未知*”或“*维护*”的服务器，则会将此状态分配给该站点。

- *维护*

  如果站点至少包含一个状态为“*维护*”的服务器，且不包含状态为“*严重*”、“*警告*”或“*未知*”的服务器，则会将此状态分配给该站点。

- *已忽略*

  如果站点仅包含状态为“*已忽略*”的服务器，则会将此状态分配给该站点。

- *未知*

  如果站点至少包含一个状态为“*未知*”的服务器，且不包含状态为“*严重*”的服务器，则会将此状态分配给该站点。

- *没有服务器*

  如果站点不包含任何服务器，则会将此状态分配给该站点。

您可以转到 Web Console 的“**KICS for Networks**” → “**地图**”部分中的主地图，方法是单击地图的任何部分（站点图标除外）。

您可以通过在小部件中单击此站点的图标来转到站点地图。

KICS for Networks 服务器信息的小部件

Web Console 的“**有关 KICS for Networks 服务器的信息**”小部件显示有关 Kaspersky Industrial CyberSecurity for Networks 服务器的当前状态的一般信息。

为每个服务器提供以下信息：

- **服务器名称** – 用于表示 Kaspersky Security Center 中的服务器的名称（管理组中的设备名称）。
- **功能** – 有关 Kaspersky Industrial CyberSecurity for Networks 保护功能的当前状态的信息。有以下值可用：
  - **全部打开** – 启用了为持续使用而设计的所有技术和方法，并启用了所有创建的监控点。
  - **并非全部打开** – 某些保护功能在学习模式下被禁用或启用，或者并非所有监控点都启用。
- **状态** – 服务器的当前状态。
- **应用程序消息** – 最后的应用程序消息或附加的状态信息。

默认情况下，小部件根据 Web Console 从 Kaspersky Security Center 管理组中的所有服务器接收的数据显示信息。如有必要，您可以使用小部件设置菜单来选择应在小部件中显示其数据的服务器。

您可以单击包含服务器名称的链接，打开所选 Kaspersky Industrial CyberSecurity for Networks 服务器的 Web 界面页面。打开的浏览器选项卡的名称将是安装后应用程序启动配置期间定义的服务器名称。

如果正在使用单点登录技术并且 Web Console 用户有权连接到此服务器，则将授予对服务器 Web 界面的访问权限，而不会提示用户输入其用户账户凭据。

在 Kaspersky Industrial CyberSecurity for Networks 服务器数据库中搜索设备和事件

在 Kaspersky Security Center Web Console 中，您可以使用 Kaspersky Industrial CyberSecurity for Networks Web 插件创建接收特定设备和事件分类的请求。基于这些请求，直接在 Kaspersky Industrial CyberSecurity for Networks 服务器数据库中执行搜索。这是 Web 插件功能与标准工具提供的搜索功能之间的主要区别，这些标准工具用于在 Web Console 中接收设备和事件的分类（例如，在“资产（**设备**” → **设备分类**和“**监控和报告**” → “**事件分类**”下）。使用 Web Console 中的标准工具时，将在管理服务器数据库中执行对设备和事件的搜索。

Web Console 的“**KICS for Networks**” → “**搜索**”部分用于配置发送到 Kaspersky Industrial CyberSecurity for Networks 服务器的搜索请求的设置，并显示搜索结果。对设备的搜索请求必须与对事件的搜索请求分开制定。

Kaspersky Industrial CyberSecurity for Networks 服务器处理搜索请求并提供这些请求的信息，但有以下限制：

- 与来自每个服务器的搜索请求（设备或事件）匹配的返回项目数不能超过 200。
- 它们只提供实际可以搜索的信息。例如，设备搜索结果将包含设备的 MAC 和 IP 地址，但不包含有关设备型号和制造商的信息。

在任何情况下，当您需要获得有关任何找到的设备或事件的完整信息时，您可以使用“**KICS for Networks**” → “**搜索**”下的界面元素转到服务器的 Web 界面页面。服务器 Web 界面页面会自动打开相应的部分（“**资产**”或“**事件**”），这些部分将根据搜索请求的标准或获得的结果进行过滤。

配置设备搜索设置

当直接从“KICS for Networks 中带有问题的设备**KICS for Networks 中存在问题的设备进行导航**时，您可以手动配置设备搜索设置或使用自动应用的过滤条件。

要手动配置这些设置，您需要打开搜索请求详细信息区域中的“**设备**”选项卡。

*要打开搜索请求详细信息区域中的“**设备**”选项卡，请执行以下操作：*

1. 转到 Web Console 的“**KICS for Networks**” → “**搜索**”部分。
2. 执行以下操作之一：
   - 如果在当前会话期间没有创建搜索请求，并且此部分没有显示搜索结果表，请单击“**查找事件或设备**”。
   - 如果在当前会话中创建了搜索请求，并且此部分显示搜索结果表，请单击工具栏中的“**搜索**”。
     “**搜索**”按钮显示当前搜索请求的筛选条件（定义的设置）的数量。
3. 在搜索请求详细信息区域中，转到“**设备**”选项卡。

配置设置后，可以通过单击“**查找**”开始在服务器的数据库中搜索设备。

您可以在设备搜索请求中配置以下设置：

- **名称** – 表示 Kaspersky Industrial CyberSecurity for Networks 服务器设备表中设备的名称。必须指定完整的名称。
- **服务器** – 表示 Kaspersky Security Center 中的服务器的名称（管理组中的设备名称）。
- **地址** – 设备MAC 和/或 IP 地址。必须提供完整的地址。
- **状态** – 设备状态，其确定在工业网络中是否允许设备的活动。
- **安全状态** – 设备安全状态，由与设备相关的已注册事件的严重性和当前漏洞决定。
- **类别** – 决定设备功能用途的类别的名称。
- **存在问题** – 指示设备是否存在需要注意的问题。

您可以通过单击“**重置过滤器**”来清除搜索请求中定义的设置。

配置事件搜索设置

当直接从“KICS for Networks 的最新事件**KICS for Networks 的最新事件进行导航**时，您可以手动配置事件搜索设置或使用自动应用的过滤条件。

要手动配置这些设置，您需要打开搜索请求详细信息区域中的“**事件**”选项卡。

*要打开搜索请求详细信息区域中的"**事件**"选项卡，请执行以下操作：*

1. 转到 Web Console 的"**KICS for Networks**" → "**搜索**"部分。
2. 执行以下操作之一：
   - 如果在当前会话期间没有创建搜索请求，并且此部分没有显示搜索结果表，请单击"**查找事件或设备**"。
   - 如果在当前会话中创建了搜索请求，并且此部分显示搜索结果表，请单击工具栏中的"**搜索**"。
     "**搜索**"按钮显示当前搜索请求的筛选条件（定义的设置）的数量。
3. 在搜索请求详细信息区域，转到"**事件**"选项卡。

配置设置后，您可以通过单击"**查找**"开始在服务器的数据库中搜索事件。

您可以在事件搜索请求中配置以下设置：

- **标题** – 为 Kaspersky Industrial CyberSecurity for Networks 中的事件类型定义的标题。必须指定完整的标题。
- **服务器** – 表示 Kaspersky Security Center 中的服务器的名称（管理组中的设备名称）。
- **最后可见日期** – 按上次出现的日期和时间筛选事件的时间段。
- **源** – 网络数据包的发送者的地址信息（MAC/IP 地址或端口号）。
- **目的地** – 网络数据包的接收方的地址信息（MAC/IP 地址或端口号）。
- **技术** – 用于注册事件的图标和技术名称。
- **严重性** – 事件严重性级别的图标和名称。

您可以通过单击"**重置过滤器**"来清除搜索请求中定义的设置。

查看搜索结果表

设备或事件的搜索结果表显示在 Web Console 的 "**KICS for Networks**" → "**搜索**"部分。该表仅显示可用于执行设备搜索或事件搜索的数据。任何找到的项目都会根据其各自的服务器进行分组。

查看表格时，您可以使用以下功能：

- 过滤搜索结果。
  要过滤搜索结果表，可以使用工具栏中的以下界面元素：
  - **安全状态**
    此过滤器在设备搜索的结果表中可用。您可以使用过滤器按钮来隐藏一些找到的设备，具体取决于它们的安全状态。
  - **严重性**
    此过滤器在事件搜索的结果表中可用。您可以使用过滤按钮来隐藏某些已找到的事件，具体取决于它们的严重性级别。

- **技术**

  此过滤器在事件搜索的结果表中可用。您可以使用过滤器按钮来隐藏一些找到的事件，具体取决于用于注册这些事件的技术。

- **服务器**

  此下拉列表允许您选择用于显示搜索结果的特定服务器。

- 更新搜索结果。

  当您查看搜索结果表时，可以在服务器上更改有关设备或事件的信息。“**上次更新**”字段显示上次加载结果的日期和时间。

  单击工具栏中的“**更新**”，可以重复搜索请求以更新结果。

- 在服务器 Web 界面页面上显示信息。

  执行以下操作之一：

  - 要接收有关某个已找到项目的详细信息，请单击包含设备名称或事件标题的链接，打开相应服务器的 Web 界面页面。

  - 要接收有关所有找到的符合搜索请求条件的项目的信息，请单击“**转到服务器**”打开相应服务器的 Web 界面页。

  Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面页面将在浏览器窗口中的新选项卡上打开。打开的选项卡的名称将是安装后应用程序启动配置期间定义的服务器名称。

  如果正在使用单点登录技术并且 Web Console 用户有权连接到此服务器，则将授予对服务器 Web 界面的访问权限，而不会提示用户输入其用户账户凭据。

  在服务器 Web 界面页面上，相关部分会自动打开以显示设备表或事件表。该表将根据对应的条件进行过滤：

Kaspersky Industrial CyberSecurity for Networks 的映射组件。

该 Web 插件可让您在 Kaspersky Security Center Web Console 中创建描述 Kaspersky Industrial CyberSecurity for Networks 服务器和传感器部署的地图。您可以使用地图根据这些项目的地理位置来排列这些项目，并在您方便的视图中监控它们的状态。

Web Console 的“**KICS for Networks**” → “**地图**”部分设计用于处理地图。此部分显示以下地图（一次只能选择一张地图）：

- 主地图。该地图描述了各个站点（用于对 Kaspersky Industrial CyberSecurity for Networks 组件进行分组的组织单位）。服务器和传感器不显示在此级别。

- 站点地图。每个站点地图都包含该特定站点中包含的应用程序组件（服务器和传感器）。

在地图上，站点和应用程序组件由包含这些对象名称的图标表示。长名称缩写为其第一个字符的组合。

背景图像可以以各种比例显示。要管理显示比例，您可以使用位于 Web Console 的“**KICS for Networks**” → “**地图**”部分上部的工具栏。

从主地图导航到站点地图后，您可以使用箭头按钮返回主地图。

只有被授予 Kaspersky Industrial CyberSecurity for Networks 管理员角色访问权限的 Kaspersky Security Center 用户才能创建地图并在这些地图上排列对象。配置完成后，具有操作员角色访问权限的用户可以使用 Web Console 中“**KICS for Networks**” → “**地图**”下的地图以及“**KICS for Networks 部署地图**”小部件中的地图来跟踪对象的状态。

生成主地图的站点列表

本节介绍生成主地图站点列表的功能。

使用 Web Console 的“**KICS for Networks**” → “**地图**”部分中的主地图时，您可以生成站点列表，用于界定 Kaspersky Industrial CyberSecurity for Networks 的控制和/或部署区域。您可以添加相关服务器并使用这些服务器及其在站点内的传感器执行操作。

最大站点数量为 100。

站点列表只能由已被授予与 Kaspersky Industrial CyberSecurity for Networks 管理员角色相对应的访问权限的 Kaspersky Security Center 用户生成。

添加站点

要为主地图添加站点：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。
   “**站点**”窗口将出现在该部分的右侧。
4. 单击“**添加**”。
   将出现一个用于输入站点名称的窗口。
5. 输入站点名称。
   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`
   站点名称必须符合以下要求：
   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 必须包含 255 个字符或更少。
   - 不得与其他站点的名称匹配。

   “**站点**”窗口将显示包含新站点名称的一行。
6. 如果包含站点名称的行未出现在列表中，这可能是由于应用了基于站点状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”启用显示所有站点，或者通过单击“**没有服务器**”启用显示没有服务器的站点。
7. 将站点添加到主地图。为此，请将光标移到包含站点名称的行上，然后单击 按钮。
8. 将站点图标移动到地图上的必要位置。

重命名站点

要重命名主地图的站点：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。

   “**站点**”窗口将出现在该部分的右侧。
4. 如果包含相关站点名称的行未显示在列表中，这可能是由于应用了基于站点状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”或单击分配给相关站点的状态的名称来启用所有站点的显示。
5. 将光标移到包含站点名称的行上，然后单击 按钮。

   将出现一个用于输入站点名称的窗口。
6. 输入站点名称。

   您可以使用字母、数字、空格和以下字符：`! @ # № $ % ^ & ( ) [ ] { } ' , . - _`

   站点名称必须符合以下要求：

   - 必须以任何允许的字符开头和结尾（空格除外）。
   - 必须包含 255 个字符或更少。
   - 不得与其他站点的名称匹配。

删除站点

要删除主地图上的站点：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。

   “**站点**”窗口将出现在该部分的右侧。
4. 如果包含相关站点名称的行未显示在列表中，这可能是由于应用了基于站点状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”或单击分配给相关站点的状态的名称来启用所有站点的显示。
5. 将光标移到包含站点名称的行上，然后单击 × 按钮。
6. 在信息提示窗口中，单击“**确定**”。

更改地图的背景图像

创建地图后，地图将使用默认的背景图像。您可以将背景图像更改为所需的任何图像。例如，您可以使用任意地域的地理地图图片作为主地图，您可以上传车间和工作区的器材部署示意图作为站点地图。

对于地图背景，可以使用从 JPG 或 PNG 文件上传的图像。上传文件的最大大小为 50 MB。上传文件中图像的最小大小为 600x600 像素。上传新图像后，将删除旧图像，并清除地图上所有对象的位置。

地图上的背景图像只能由已被授予与 Kaspersky Industrial CyberSecurity for Networks 管理员角色相对应的访问权限的 Kaspersky Security Center 用户更改。

要更改主地图的背景图像，请执行以下操作：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**替换图像**”。

   您将看到一个窗口，提示您拖动图像文件或选择一个文件。
4. 使用任何方便的方法上传文件。

要更改站点地图的背景图像，请执行以下操作：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。

   “**站点**”窗口将出现在该部分的右侧。
4. 单击包含相关站点名称的行。

   站点地图打开。
5. 单击“**替换图像**”。

   您将看到一个窗口，提示您拖动图像文件或选择一个文件。
6. 使用任何方便的方法上传文件。

生成站点内的服务器列表

本节介绍可用于生成站点内服务器列表的功能。

在 Web Console 的“**KICS for Networks**” → “**地图**”下的已创建站点的地图上，您需要根据 Kaspersky Industrial CyberSecurity for Networks 的控制和/或部署的定界区域生成驻留在这些站点的服务器列表。驻留在站点的任何服务器也包括与这些服务器相关联的传感器。

每个 Kaspersky Industrial CyberSecurity for Networks 服务器只能包含在一个站点中。任何未添加到网站的服务器都将保留在“**网站外**”列表中，直到它包含在网站中为止。

站点服务器列表只能由已被授予与 Kaspersky Industrial CyberSecurity for Networks 管理员角色相对应的访问权限的 Kaspersky Security Center 用户生成。

将服务器添加到站点

要将服务器添加到站点：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。
   “**站点**”窗口将出现在该部分的右侧。
4. 单击包含相关站点名称的行。
   站点地图打开。
5. 单击“**显示服务器列表**”。
   包含站点名称的窗口将出现在该部分的右侧。
6. 选择“**站点外**”选项卡。
7. 如果包含相关服务器的行未显示在列表中，这可能是由于应用了基于服务器状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”或单击包含分配给相关服务器的状态名称的按钮来启用所有服务器的显示。
8. 将光标移到包含服务器名称的行上，然后单击 + 按钮。
   服务器行将不再显示在“**站点外**”选项卡上。
9. 选择“**站点中**”选项卡。
10. 如果包含添加的服务器的行未出现在列表中，这可能是由于应用了基于服务器状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”或单击包含分配给服务器的状态名称的按钮来启用所有服务器的显示。
11. 将服务器添加到站点地图中。为此，请将光标移到包含服务器名称的行上，然后单击 按钮。
    在执行该操作之后，按钮中的图标的亮度发生变化。
12. 如果存在与服务器相关联的传感器，并且您希望启用这些传感器的显示，请展开“**Sensor**”并使用 按钮添加它们。
13. 将对象的图标移动到其在地图上的正确位置。

从站点中删除服务器

要从站点中删除服务器：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。
   “**站点**”窗口将出现在该部分的右侧。
4. 单击包含相关站点名称的行。
   站点地图打开。
5. 单击“**显示服务器列表**”。
   包含站点名称的窗口将出现在该部分的右侧。
6. 选择“**站点中**”选项卡。
7. 如果包含相关服务器的行未显示在列表中，这可能是由于应用了基于服务器状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”或单击包含分配给相关服务器的状态名称的按钮来启用所有服务器的显示。
8. 将光标移到包含服务器名称的行上，然后单击 × 按钮。
   服务器将显示在“**站点外**”选项卡上。

管理地图上对象的排列

在 Web Console 的“**KICS for Networks**” → “**地图**”部分，Kaspersky Industrial CyberSecurity for Networks 的站点和组件由地图上的图标表示。

地图上的对象排列只能由已被授予与 Kaspersky Industrial CyberSecurity for Networks 管理员角色相对应的访问权限的 Kaspersky Security Center 用户管理。

可以将对象的图标移动到它们在地图上的必要位置。但是，地图上的所有图标必须单独显示，而不能完全重叠。

如有必要，可以禁用地图上不相关对象的显示。从显示中禁用后，对象不会从地图对象列表中删除。您可以稍后重新启用此对象的显示。

要启用或禁用主地图上站点的显示，请执行以下操作：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。
   “**站点**”窗口将出现在该部分的右侧。

4. 如果包含相关站点名称的行未显示在列表中，这可能是由于应用了基于站点状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”或单击分配给相关站点的状态的名称来启用所有站点的显示。

5. 将光标移到包含站点名称的行上，然后单击 按钮。

   在执行该操作之后，按钮中的图标的亮度发生变化。

要在站点地图上启用或禁用服务器或传感器的显示，请执行以下操作：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。

2. 选择“**KICS for Networks**” → “**地图**”。

3. 单击“**显示站点列表**”。

   “**站点**”窗口将出现在该部分的右侧。

4. 单击包含相关站点名称的行。

   站点地图打开。

5. 单击“**显示服务器列表**”。

   包含站点名称的窗口将出现在该部分的右侧。

6. 选择“**站点中**”选项卡。

7. 如果包含相关服务器的行未显示在列表中，这可能是由于应用了基于服务器状态的过滤器所致。如果是这种情况，请通过单击“**所有状态**”或单击包含分配给相关服务器的状态名称的按钮来启用所有服务器的显示。

8. 如果存在与服务器相关联的传感器，并且您希望启用或禁用这些传感器的显示，请展开包含相关服务器名称的行中的“**Sensor**”列表。

9. 将光标移到包含相关服务器或传感器名称的行上，然后单击 按钮。

   当您禁用服务器的显示时，这将同时启用与该服务器相关联的所有传感器的显示。

   在执行该操作之后，按钮中的图标的亮度发生变化。

在 Web Console 中将服务器静音

如果 Kaspersky Security Center Web Console 正在接收来自多个 Kaspersky Industrial CyberSecurity for Networks 服务器的数据，并且来自特定服务器的数据在一段时间内不需要监控（例如，在 ICS 中的预防性维护和调整操作期间），则可以将该服务器排除在监控之外（“静音”服务器）。将服务器静音后，Web Console 将停止接收来自该服务器的数据，并将其分配为“*已静音*”状态。但是，Kaspersky Security Center 管理服务器将继续从该服务器接收和保存数据（包括事件）。

服务器将保持静音状态，直到您重新启用对此服务器的监控（“取消静音”服务器）。

服务器只能由已被授予与 Kaspersky Industrial CyberSecurity for Networks 管理员角色相对应的访问权限的 Kaspersky Security Center 用户静音和取消静音。

要对服务器静音或取消静音，请执行以下操作：

1. 使用在 Kaspersky Industrial CyberSecurity for Networks 中具有管理员权限的账户登录 Kaspersky Security Center Web Console。
2. 选择“**KICS for Networks**” → “**地图**”。
3. 单击“**显示站点列表**”。
   “**站点**”窗口将出现在该部分的右侧。
4. 单击包含相关站点名称的行。
   站点地图打开。
5. 单击“**显示服务器列表**”。
   包含站点名称的窗口将出现在该部分的右侧。
6. 单击包含相关服务器名称的行。
   一个包含有关服务器详细信息的窗口将出现在该部分的右侧。
7. 如果要将服务器静音，请单击“**忽略**”。如果服务器已经静音，并且您想取消静音，请单击“**取消忽略**”。
8. 在信息提示窗口中，单击“**确定**”。

在地图上查看有关服务器的信息

Kaspersky Industrial CyberSecurity for Networks 服务器的状态影响服务器显示图标的颜色和 Web Console 的“**KICS for Networks**” → “**地图**”部分中地图上站点的图标。如果传感器的图标显示在站点地图上，这些图标的颜色取决于包含传感器的节点的当前状态。这使您可以根据地图上表示对象的图标的颜色来跟踪 Kaspersky Industrial CyberSecurity for Networks 组件的状态。

如有必要，您可以查看有关每台服务器的详细信息。详细信息窗口提供有关服务器当前状态的主要数据、有关应用程序模块和数据库的已安装更新的信息、有关硬件资源使用情况的数据以及授权许可密钥详细信息。

要查看有关服务器的详细信息，请执行以下操作：

1. 选择“**KICS for Networks**” → “**地图**”。
2. 单击“**显示站点列表**”。
   “**站点**”窗口将出现在该部分的右侧。
3. 单击包含相关站点名称的行。
   站点地图打开。
4. 单击“**显示服务器列表**”。
   包含站点名称的窗口将出现在该部分的右侧。
5. 单击包含相关服务器名称的行。
   一个包含有关服务器详细信息的窗口将出现在该部分的右侧。
6. 如果您要转到服务器的 Web 界面页面，请单击“**转到服务器**”。
   浏览器将打开一个选项卡，显示安装后应用程序启动配置期间定义的服务器名称。

疑难解答

本节包含有关 Kaspersky Industrial CyberSecurity for Networks 操作中可能遇到的问题及其解决方法的说明。

应用程序组件无法安装在选定的节点上

问题

在集中安装应用程序组件时，出现由于无法通过 SSH 协议连接而导致节点无法进行组件安装的消息。此节点上未安装该组件。

解决方案

如果在将要安装组件的节点上配置通过 SSH 协议访问后，计算机的地址信息或网络名称发生变化，则无法集中安装应用程序组件。要集中安装应用程序组件，您必须恢复通过 SSH 协议对远程计算机的访问。

要恢复通过 SSH 协议的访问并安装应用程序组件：

1. 在执行应用程序组件集中安装的计算机上，更新用于通过 SSH 协议连接节点的密钥。为此，请使用用于安装应用程序的用户账户的账户凭据登录系统，然后在操作系统控制台中输入以下命令：

   ```
   sudo ssh-keygen -R <节点 IP 地址>
   ```

2. 使用相同的安装设置重新安装该应用程序。重新安装期间，请确保没有出现提示该节点不可用于安装组件的消息。

检测到应用程序问题

问题

通过 Web 界面连接到服务器时，应用程序 Web 界面菜单的上部会在按钮旁边显示一个红色图标。

解决方案

Kaspersky Industrial CyberSecurity for Networks 的这一状态表示某个应用程序过程发生故障。

恢复应用程序的运行：

1. 请等待 20-30 秒。

   应用程序可以自动恢复正常运行。如果应用程序恢复正常运行，红色图标将不再显示。

2. 如果故障仍然存在，请联系卡巴斯基技术支持。根据技术支持代表的要求，准备发送 Kaspersky Industrial CyberSecurity for Networks 的进程日志和其他系统数据。进程日志位于用于存储应用程序数据的文件夹文章中列出的文件夹中。提供日志存取权限需要操作系统的根权限。

新的应用程序消息

问题

在**设置→应用程序消息**下会出现一条新的应用程序消息。

需要引起注意的消息通过网络界面菜单中的按钮旁边的红色或黄色图标表示。如果显示该图标，则表示存在有关应用程序运行中断或非严重故障的消息，并且该问题尚未解决。要查看信息，您可以当它的旁边显示红色或黄色图标时点击转到**设置→应用程序消息**。

解决方案

应用程序消息表明应用程序中发生了某些事件。

在**设置→应用程序消息**下阅读消息中的简明信息。根据这些信息，您可以决定采取必要的行动。

下一步取决于消息状态。消息可以有以下状态：

- *正常操作* – 大多数情况下，消息不需要响应。然而，有些情况可能需要进一步澄清具体情况。例如，当您收到有关成功应用安全策略的消息但不知道为什么采取此操作时，这可能是必要的。
- *未知*、*故障* – 如果该消息刚刚出现，请等待 20-30 秒并检查应用程序的当前状态。
- *中等故障*、*严重故障*、*重大故障* – 应用程序发生故障。如果问题无法解决，请联系卡巴斯基技术支持。根据技术支持代表的要求，准备发送 Kaspersky Industrial CyberSecurity for Networks 的进程日志和其他系统数据。进程日志位于用于存储应用程序数据的文件夹文章中列出的文件夹中。提供日志存取权限需要操作系统的根权限。

硬盘驱动器上没有足够的可用空间

问题

在安装应用程序服务器或探测器的计算机上，硬盘驱动器上没有足够的可用空间。

解决方案

计算机必须满足硬件和软件要求以确保应用程序组件正常运行。

为使应用程序正常运行：

1. 在计算机硬盘上，释放足够的空间以满足最低可用磁盘空间要求。
2. 重新启动支持应用程序组件运行的服务。

启用监控点时出现错误

问题

监控点切换为“*已启用*”后，显示“*错误*”状态。因此，与该监控点关联的节点将显示*操作中断*状态。应用程序运行问题的通知列表还显示有关由于监控点检测到的问题而导致运行中断的消息。

解决方案

监控点的“*错误*”状态可能与网络接口不受支持的操作状态有关。当启用监控点时，为了成功完成扫描，网络接口必须具有“*已启用*”运行状态。如果网络接口处于不同的运行状态，例如“*未知*”，应用程序会为监控点分配一个“*错误*”状态，因为在接收或处理网络数据包时可能出现问题。

您可以使用 `ip link` 命令检查节点计算机上网络接口的当前运行状态。当前运行状态的信息显示在包含接口名称的字符串中，格式如下：`state <状态>`。有问题的网络接口最有可能的运行状态如下：

- *已禁用*。在这种情况下，您可以使用以下命令将接口切换为“*已启用*”操作状态：

  ```
  sudo ip link set <接口名称> up
  ```

- *未知*。此运行状态可能是由于错误添加的接口造成的。例如，VMware™ 虚拟机上默认添加的网络接口可能在“*未知*”状态下运行。在这种情况下，建议使用管理网络接口的相应资源重新添加（创建）具有正确设置的网络接口。

当网络接口切换为“*已启用*”运行状态时，检查添加到此网络接口的监控点的状态。如果监控点仍然显示“*错误*”状态，请禁用然后重新启用该监控点。

监控点无流量

问题

应用程序注册了一个事件，其描述中包含以下文本：`监控点无流量`。事件描述包括没有流量的持续时间、监控点的名称以及未接收流量的网络接口。

解决方案

流量要到达监控点，必须满足以下条件：

- 监控点已启用，当前状态为*正常*。
- 在监控点网络接口上，网线已连接到以太网端口。
- 监控点网络接口的入站流量速率大于 0 bps。

您可以通过**设置→部署**下的网页界面查看连接到服务器时的监控点和网络接口的信息。

如果监控点网络接口显示的入流量速率为 0 bps，请检查是否满足以下条件：

- 监控点的网络接口在操作系统中得到正确配置。
- 当网络接口连接到工业网络交换机时，必须在网络交换机上正确配置通过连接端口（SPAN）传输镜像流量。

未加载事件或事故的流量

问题

无法加载所选事件和/或事故的流量。事件表不显示用于加载流量的工具（例如，当选择一个事件时，详细信息区域中缺少“**下载流量**”），或者显示“所选事件没有流量”消息（尝试加载流量时）。

解决方案

所选事件和/或事故的已保存流量可能会因以下原因之一而丢失：

- 流量未保存。
- 流量已从数据库中删除。
- 流量转储文件已被删除。

如果针对特定类型的事件启用了流量保存功能，则应用程序会在事件注册期间保存流量。默认情况下，所有事件类型的流量保存功能都是禁用的。您可以启用并配置相关事件类型的流量保存。

当达到某个流量存储限制时（例如，达到数据库中保存的流量的最大量），应用程序会删除已注册事件的已保存流量。在其他数据包之前保存的流量数据包将被从数据库中删除。如果保存的流量删除得太快，并且您没有时间为相关事件加载流量，则可以增加流量存储设置的最大值。

当存储的流量转储文件达到限制时，应用程序将删除早于其他文件保存的临时流量转储文件。如果删除流量转储文件的速度比从这些文件加载流量的速度快，则可以增加流量转储文件存储设置的最大值或在节点上连接外部存储。

ICS 上的预防性维护和调整操作

问题

在 ICS 上执行预防性维护和调整操作会在 Kaspersky Industrial CyberSecurity for Networks 中创建大量的重要和关键事件。

解决方案

在进行预防性维护和调整操作时，您可以选择以下选项之一来解决此问题：

- 保持服务器和应用程序探测器上的所有监控点和所有技术处于启用状态。在这种情况下，在查看有关设备事件和交互的信息时，请考虑要进行的预防性维护和调整操作的时间和列表。
- 禁用监控点或在从将进行预防性维护和调整操作的工业网络段接收流量的监控点上禁用使用技术。例如，如果工作只在一家商店进行，您可以禁用接收来自这家商店的流量的监控点，并保持所有其他监控点处于启用状态。
- 禁用所有安装有应用组件的节点上的所有监控点。如果要对整个工业网络进行预防性维护和调整操作，则可以选择此选项。

如果您已经禁用监控点或技术，若要恢复对受保护 ICS 的控制，您需要在完成预防性维护和调整操作后立即重新启用监控点或技术。

请注意，在 ICS 维护和调试操作期间，入侵者可能会在未经授权的情况下，尝试获取对网络的访问权限。在决定禁用监控点或技术时，应遵循贵企业既有的安全规章和规程。

如果在进行预防性维护和调整操作时，工业网络设备的组成或设置发生了变化（例如，MAC 地址和 IP 地址发生了变化），请对过程控制、交互控制和资产管理进行适当的更改。例如，您可以为相应的监控点配置技术学习模式。

意料之外的系统重新启动

问题

托管 Kaspersky Industrial CyberSecurity for Networks 套件组件的计算机意外重启。

解决方案

等待计算机完成重新启动。计算机重启后，Kaspersky Industrial CyberSecurity for Networks 可能处于以下状态：

- Kaspersky Industrial CyberSecurity for Networks 已恢复正常运行。

  应用程序运行正常。
- Kaspersky Industrial CyberSecurity for Networks 未恢复正常运行。

  该应用程序会告知检测到的操作问题。

如果故障仍然存在，请重新启动支持应用程序组件运行的服务。如果重启后问题仍未解决，请联系卡巴斯基技术支持。根据技术支持代表的要求，准备发送 Kaspersky Industrial CyberSecurity for Networks 的进程日志和其他系统数据。进程日志位于用于存储应用程序数据的文件夹文章中列出的文件夹中。提供日志存取权限需要操作系统的根权限。

更改或添加服务器 IP 地址后，连接器和远程连接功能不可用

问题

如果在服务器计算机上更改或添加了通过 Web 服务器连接的 IP 地址，则由于证书验证错误，连接器无法连接到新 IP 地址的服务器。使用**远程连接**轮询方法时，无法使用应用程序传感器进行设备扫描。

解决方案

若要使用新的服务器 IP 地址，您需要更换用于保护与连接器和应用程序组件服务的连接的主服务器证书。

主服务器证书被替换后，旧的应用程序 Sensor 证书将无效，从而终止任何 Sensor 与服务器的连接。要作为证书续订过程的一部分恢复连接，您需要重新添加并重新连接所有传感器。您还需要更新用于连接连接器的证书。

未收到来自 Kaspersky Security Center 管理服务器的更新

问题

使用选定的更新源启动数据库和应用程序模块更新过程时，**Kaspersky Security Center 管理服务器**会显示消息：由于错误中断了更新过程，更新安装失败。

解决方案

如果 Kaspersky Industrial CyberSecurity for Networks 与 Kaspersky Security Center 之间的通信条件得到满足，则可以从 Kaspersky Security Center 管理服务器下载更新。如果任何条件未满足，请确保满足这些条件。例如，如果没有安装 Kaspersky Security Center 的 Kaspersky Industrial CyberSecurity for Networks 管理插件的当前版本，请安装该插件。

在某些情况下，更新安装错误可能与无法从 Kaspersky Security Center 存储库下载更新有关。如果 Kaspersky Industrial CyberSecurity for Networks 的更新已上传到更新存储库，但无法下载，您可以按照 Kaspersky Security Center 知识库 中的说明执行清除存储库的步骤。

重新安装 Kaspersky Security Center 管理服务器后，网络代理无法同步

问题

如果重新安装 Kaspersky Security Center 管理服务器后未恢复备份副本中的设置，Kaspersky Security Center 管理控制台不会显示安装了 Kaspersky Industrial CyberSecurity for Networks 的计算机。

解决方案

要恢复网络代理的同步，您可以使用 klbackup 实用程序恢复 Kaspersky Security Center 管理服务器的设置。klbackup 工具包含在 Kaspersky Security Center 分发包中。有关备份和恢复 Kaspersky Security Center 管理服务器设置的详细信息，请参阅 Kaspersky Security Center 帮助系统。

如果由于某种原因无法使用 klbackup 实用程序恢复 Kaspersky Security Center 管理服务器的设置，您可以使用网络代理中包含的 klmover 实用程序恢复网络代理的同步。

要使用 klmover 实用程序恢复网络代理的同步：

1. 在执行 Kaspersky Industrial CyberSecurity for Networks 服务器功能的计算机上，打开操作系统控制台并转到文件夹 /opt/kaspersky/klnagent64/bin/。
2. 在命令行中输入以下命令：

   ```
   sudo ./klmover -address <IP 地址或计算机名称>
   ```

   其中 `<IP 地址或计算机名称>` 是装有 Kaspersky Security Center 的计算机的 IP 地址或名称。
3. klmover 实用程序运行完成后，检查网络代理与 Kaspersky Security Center 管理服务器的连接。为此，请在命令行中输入以下命令：

   ```
   sudo ./klnagchk
   ```

   屏幕将显示有关管理服务器连接的信息。

网络代理同步成功恢复后，Kaspersky Security Center 管理控制台将显示安装了 Kaspersky Industrial CyberSecurity for Networks 的计算机。

无法通过 Web 界面连接到服务器

问题

当尝试连接到服务器时，Kaspersky Industrial CyberSecurity for Networks Web 界面页面未加载。

解决方案

可能的情况：

- 无法通过网络访问安装了 Web 服务器的 Kaspersky Industrial CyberSecurity for Networks 服务器计算机。根据指定的服务器名称检查与计算机的连接（例如，使用`ping`命令）。
- 浏览器地址栏中输入了错误的数据。输入在**设置→连接服务器**下为 Web 服务器指定的服务器的 IP 地址或计算机名称。如果设置了默认端口 443，则不必指定端口号。如果指定了不同的端口号，请在地址栏中以`https://<Server name>:<port>`格式输入完整地址。
- 浏览器中禁用了 JavaScript。连接失败警告页面上会显示有关此情况的消息。在浏览器设置中，启用 JavaScript 的执行并刷新页面。
- 防火墙阻止了对服务器计算机的访问。正确配置正在使用的防火墙。

连接到服务器时，浏览器会显示证书警告

问题

当尝试连接到安装了 Kaspersky Industrial CyberSecurity for Networks 组件的计算机时，浏览器会显示一条警告，提示安全证书或正在建立的连接不受信任。警告内容取决于所使用的具体浏览器。

解决方案

该警告意味着 Web 服务器上正在使用自签名证书。

您可以暂时使用自签名证书连接到服务器（例如，当测试 Kaspersky Industrial CyberSecurity for Networks 的运行时）。使用自签名证书时，在浏览器警告窗口中选择可让您继续连接的选项。

为了确保长期使用，推荐将自签名证书替换为受信任的证书。您可以在通过 Web 界面更新连接服务器的证书时，同时替换当前证书。

联系技术支持

本节介绍获取技术支持的途径和提供技术支持的条件。

如何获得技术支持

如果您无法在应用程序文档或有关 Kaspersky Industrial CyberSecurity for Networks 的其他信息源中找到问题的解决方案，我们建议您联系技术支持。我们的技术支持专家将回答您有关安装和使用 Kaspersky Industrial CyberSecurity for Networks 的问题。

卡巴斯基在应用程序生命周期内为 Kaspersky Industrial CyberSecurity for Networks 提供支持（请参阅应用程序生命周期页面）。在联系技术支持之前，请阅读技术支持规则。

您可以通过下列方式之一与技术支持专家联系：

- 访问技术支持网站
- 通过 Kaspersky CompanyAccount 门户向卡巴斯基技术支持发送请求。

通过 Kaspersky CompanyAccount 获得技术支持

Kaspersky CompanyAccount 是使用卡巴斯基应用程序的组织的门户。Kaspersky CompanyAccount 门户旨在使用户能够方便地通过在线请求与卡巴斯基专家进行互动。利用 Kaspersky CompanyAccount 门户，您可以监控卡巴斯基专家处理电子请求的进度，并存储电子请求的历史记录。

在 Kaspersky CompanyAccount 上，您可以在单一账户下注册贵组织的所有员工。单一用户账户允许您集中管理已注册员工向卡巴斯基发送的电子请求，并通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户可适用于以下语言：

- 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

要了解有关 Kaspersky CompanyAccount 的更多信息，请访问技术支持网站。

收集获取技术支持所需的信息

卡巴斯基技术支持专家可能要求您提供 Kaspersky Industrial CyberSecurity for Networks 日志和其他系统数据。

日志位于安装了 Kaspersky Industrial CyberSecurity for Networks 组件的计算机上。用于存储日志的文件夹的相关信息在用于存储应用程序数据的文件夹文章中提供。

提供日志存取权限需要操作系统的根权限。

卡巴斯基技术支持专家可能还会要求提供有关应用程序组件的其他数据。这些数据可以通过使用名为 kics4net-deploy-<应用程序版本号>.bundle.sh 的应用程序组件集中安装脚本或通过在本地运行 kics4net-gather-artefacts.sh 脚本来获取，脚本位于安装了应用程序组件的计算机上的 /opt/kaspersky/kics4net/sbin/ 文件夹中。

要使用 kics4net-deploy-<应用程序版本>.bundle.sh 脚本获取有关应用程序组件的信息：

1. 在从其执行集中安装的计算机上，转到包含用于安装、验证和删除应用程序组件（包含在分发套件中）的脚本和包的解压文件的文件夹。这些文件位于 kics4net-release_<应用程序版本>/linux-centos 子文件夹中。
2. 输入以下命令：

   ```
   bash kics4net-deploy-<应用程序版本号>.bundle.sh --gather-artefacts -<参数> <目录名称>
   ```

   其中：

   - `-<parameter>` – 确定数据采集模式。

     提供以下参数：

     - `-a` – 接收所有数据。
     - `-c` – 接收证书数据。
     - `-i` – 接收有关入侵检测配置的数据。
     - `-t` – 接收流量转储文件。
   - `<目录名称>` – 用于复制存档数据文件的目录名称。

   示例

   ```
   bash kics4net-deploy-<应用程序版本号>.bundle.sh --gather-artefacts -a /tmp/data_for_support
   ```

3. 在`SSH password`和`BECOME password`提示中，输入用于运行应用程序组件安装的用户帐户的密码。

等待脚本 kics4net-deploy-<应用程序版本号>.bundle.sh 完成。成功完成后，文件将在指定文件夹中创建。

要使用 kics4net-gather-artefacts.sh 脚本获取计算机上安装的应用程序组件的数据：

1. 使用具有 root 权限的用户帐户的帐户凭据登录系统。
2. 转到 /opt/kaspersky/kics4net/sbin/ 文件夹并输入以下命令，运行脚本来接收应用程序组件上的数据：

   ```
   bash kics4net-gather-artefacts.sh -<参数> <目录名称>
   ```

   其中：

   - `-<parameter>` – 确定数据采集模式。
     提供以下参数：
     - `-a` – 接收所有数据。
     - `-c` – 接收证书数据。
     - `-i` – 接收有关入侵检测配置的数据。
     - `-t` – 接收流量转储文件。
   - `<目录名称>` – 用于复制存档数据文件的目录名称。

   示例

   ```
   bash kics4net-gather-artefacts.sh -a /tmp/data_for_support
   ```

等待 kics4net-gather-artefacts.sh 脚本完成。成功完成后，文件将在指定文件夹中创建。

有关应用程序的信息源

在 Kaspersky Industrial CyberSecurity for Networks 页面上，您可以查看有关应用程序、应用程序功能和特性的常规信息。

在线帮助指南包含有关 Kaspersky Industrial CyberSecurity for Networks 管理的信息。在线帮助指南还提供有关用户可用来完成常见任务的应用程序功能的信息。

在线帮助包括 Kaspersky Industrial CyberSecurity for Networks API 的文档。本文档作为 Kaspersky Industrial CyberSecurity for Networks API 的开发人员指南。在《Kaspersky Industrial CyberSecurity for Networks API 开发人员指南》中，您可以找到有关执行以下任务的信息：

- 准备使用 Kaspersky Industrial CyberSecurity for Networks API。
- 处理从 Kaspersky Industrial CyberSecurity for Networks 接收数据以及向应用程序发送数据的请求。

如果您无法自行找到问题的解决方案，请联系卡巴斯基技术支持。

附录

本节提供的信息通过示例、参考信息和附加数据对主要文档文本进行了补充。

安装和配置 CentOS Stream 9 操作系统

本节介绍在将要安装 Kaspersky Industrial CyberSecurity for Networks 的计算机上安装和配置操作系统的基本步骤：服务器或 Sensor。

要安装和配置 CentOS Stream 9 操作系统：

1. 从 CentOS 项目的官方页面下载用于安装 CentOS Stream 9 操作系统的 ISO 镜像：https://centos.org/download/。
2. 使用 ISO 镜像创建可启动介质（例如在 USB 驱动器上）。
   例如，您可以使用 Rufus 实用程序创建可启动介质。
3. 将可启动介质连接到要安装操作系统的计算机，然后从该介质启动计算机。
4. 在操作选择菜单中，选择**“安装 CentOS Stream 9”**。
5. 选择操作系统的本地化语言。
   在后续操作的描述中，我们使用英语作为我们选择的本地化语言。
6. 设置日期和时间。
7. 如有必要，打开**键盘布局**窗口并选择其他键盘布局。
8. 在主菜单的**“软件选择”**部分，保留默认值**“带图形用户界面的服务器”**。
9. 点击主菜单的**“安装目标”**部分，选择要安装操作系统的驱动器，并将**“存储配置”**参数设置为**“自定义”**。
10. 下一步，点击“**点击此处自动创建分区”**链接解锁设置，并将 /home 分区的大小设置为不超过 10-15 GB，其余空间分配给系统（根）分区。引导分区和交换分区保留默认值。
11. 点击主菜单的**“网络和主机名”**部分，输入计算机名称（例如：`kics4net1`）。
12. 点击主菜单的**“根账户密码”**部分，输入根账户密码。
13. 创建一个具有 root 权限的用户来管理操作系统。对于此根账户，选中**“将此用户设为管理员”**和**“使用此账户需要密码”**复选框。
14. 在主菜单窗口中，点击“**开始安装”**按钮，等待操作系统安装完成。
15. 安装完成后，计算机重启，使用您创建的用户凭证登录。

16. 配置计算机的网络接口设置。为此，打开屏幕右上角的快速配置菜单，然后执行以下操作：

    a. 选择“**设置**”选项。在打开的窗口中，转到“**网络**”区域。

    b. 按顺序配置可用网络接口的设置：

    - 对于将用于通过 Web 界面连接以及与 Kaspersky Industrial CyberSecurity 解决方案其他组件连接的网络接口，选中**“自动连接”**和**“对其他用户可用”**复选框，指定一个静态 IPv4 地址（**手动**），禁用 IPv6 协议，并在**“安全”**选项卡上保持安全功能禁用状态。
    - 对于将用作监控点的网络接口，选中**“自动连接”**和**“对其他用户可用”**复选框，禁用 IPv4 和 IPv6 协议，并在**“安全”**选项卡上保持安全功能禁用状态。

17. 重启计算机并使用您创建的用户账户凭证登录。

18. 打开操作系统控制台并输入用于安装和配置所需软件包的命令：

    - 要安装 glibc-langpack-zh 软件包（仅 Kaspersky Industrial CyberSecurity for Networks 4.5.1 需要）：

      ```
      sudo dnf install glibc-langpack-zh
      ```

    - 要安装 chrony 时间同步软件包：

      ```
      sudo dnf install chrony
      sudo systemctl enable chronyd
      sudo systemctl start chronyd
      ```

    - 要禁用 SELinux 访问控制强制系统：

      1. 在文本编辑器（例如：`mcedit`）中打开 `/etc/selinux/config` 配置文件。
      2. 将 `SELINUX` 参数设置为 `已禁用`。
      3. 保存并关闭配置文件。

    - 要安装 dnf-utils 包：

      ```
      sudo dnf install dnf-utils
      ```

    - 要安装 compat-openssl 包：

      ```
      sudo dnf install compat-openssl11
      ```

    - 要安装包含 LTTng 库的 lttng-ust 包：

      ```
      sudo dnf install lttng-ust.x86_64
      ```

- 安装 EPEL 软件仓库以及连接器和数据转换脚本运行所需的 Python 解释器软件包 python3-psycopg2、python3-cryptography 和 python3-paramiko：

```
sudo dnf config-manager --set-enabled crb
sudo dnf install epel-release epel-next-release
sudo dnf install python3-psycopg2 python3-cryptography python3-paramiko
```

- 要安装 Postfix 邮件服务器（可能仅在执行服务器功能的计算机上需要）：

```
sudo dnf -y install postfix
sudo systemctl start postfix
sudo systemctl enable postfix
```

- 要更新 Perl 解释器（可能仅在执行服务器功能的计算机上需要，并且如果已安装 Kaspersky Security Center 网络代理）：

```
sudo dnf upgrade perl
```

19. 重新启动计算机。

通过 NTP 和 PTP 协议配置时间同步

本节介绍通过 NTP 和 PTP 配置时间同步的可用操作。

安装了 Kaspersky Industrial CyberSecurity for Networks 组件的节点的时间必须与工业网络设备使用的公共时间源同步。为了进行同步，您可以使用称为网络时间协议 (NTP) 和精确时间协议 (PTP) 的标准协议。

在服务器节点上，无论该组件如何安装（集中安装后以及本地安装后），都必须配置时间同步。

在安装了探测器的节点上，必须在以下情况下配置时间同步：

- 在集中安装 Kaspersky Industrial CyberSecurity for Networks 期间，未启用服务器和探测器之间的自动时间同步。
- 使用 kics4net-install.sh 脚本在本地安装了探测器。

配置时间同步所需的步骤可能因操作系统版本和特定协议的不同而有所不同。

在 CentOS 中通过 NTP 协议配置时间同步

要在 CentOS 中通过 NTP 配置时间同步：

1. 打开操作系统控制台。
2. 检查称为 chrony 的标准时间同步服务的状态。为此，请输入以下命令：

```
systemctl status chronyd
```

3. 如果未找到该服务，请输入以下命令来添加包并启用该服务：

```
sudo dnf install chrony
sudo systemctl enable chronyd
sudo systemctl start chronyd
```

4. 打开服务配置文件。为此，请输入以下命令：

```
sudo mcedit /etc/chrony.conf
```

5. 指定用于时间同步的 NTP 服务器。要指定服务器，只需要添加以下字符串：

```
server <服务器名称或 IP 地址> iburst
```

6. 保存并关闭配置文件。

7. 重新启动服务。为此，请输入以下命令：

```
sudo systemctl restart chronyd
```

8. 验证指定的 NTP 服务器是否在同步源列表中。为此，请输入以下命令：

```
chronyc sources
```

在 CentOS 中通过 PTP 协议配置时间同步

要在 CentOS 中通过 PTP 配置时间同步：

1. 打开操作系统控制台。

2. 检查 linuxptp 包是否已安装。为此，请输入以下命令：

```
dnf list installed
```

3. 如果未安装 linuxptp 包，请输入以下命令添加该包并启用 ptp4l 时间同步服务：

```
sudo dnf install linuxptp
sudo systemctl enable ptp4l
sudo systemctl start ptp4l
```

4. 打开服务配置文件。为此，请输入以下命令：

```
sudo mcedit /etc/ptp4l.conf
```

5. 对于 `slaveOnly` 参数，输入 `1`。

6. 保存并关闭配置文件。

7. 打开包含服务常规设置的文件。为此，请输入以下命令：

```
sudo mcedit /etc/sysconfig/ptp4l
```

8. 在 `OPTIONS` 字符串中，指定参数如下：

```
OPTIONS="-f <配置文件> -i <接口名称> -S -s"
```

其中：

- `-f <配置文件>` – 配置文件的默认名称和完整路径。
- `-i <接口名称>` – 用于时间同步的网络接口的名称。
- `-S` – 允许使用基于软件的时间戳。如果您想使用基于硬件的时间戳，可以跳过此参数。但是，首先要确保部件支持此功能。
- `-s` – 启用下属时间同步。

示例 OPTIONS 字符串

```
OPTIONS="-f /etc/ptp4l.conf -i eth0 -S -s"
```

9. 保存并关闭常规设置文件。
10. 允许防火墙使用端口 319 和 320 来运行 UDP 协议。为此，请输入以下命令：

```
sudo firewall-cmd --permanent --add-port=319/udp
sudo firewall-cmd --permanent --add-port=320/udp
```

11. 重新启动防火墙服务。为此，请输入以下命令：

```
sudo systemctl restart firewalld
```

12. 重新启动时间同步服务。为此，请输入以下命令：

```
sudo systemctl restart ptp4l
```

支持 IEC 60870-5-104 和 IEC 60870-5-101 标准协议中的 ASDU 类型识别

本文介绍了 Kaspersky Industrial CyberSecurity for Networks 支持的 ASDU 类型识别（见下表）。在通过 IEC 60870-5-104 和 IEC 60870-5-101 标准协议进行交互的设备上，深度数据包检测期间会处理列出的帧类型。

帧类型 ID	操作	描述	主值/系统命令类型
1. 监控方向的处理信息			
<1>	M_SP_NA	单点信息	布尔（0 - 关闭，1 - 开启）
<2>	M_SP_TA	单点信息（带时间标签）	布尔（0 - 关闭，1 - 开启）
<3>	M_DP_NA	双点信息	unsigned int8（0 – 不确定或中间，1 – 关闭，2 – 开启，3 – 不确定）
<4>	M_DP_TA	双点信息（带时间标签）	unsigned int8（0 – 不确定或中间，1 – 关闭，2 – 开启，3 – 不确定）
<5>	M_ST_NA	步骤位置信息	int8（-64...+64）
<6>	M_ST_TA	步骤位置信息（带时间标签）	int8（-64...+64）
<7>	M_BO_NA	32 位字符串	unsigned int32
<8>	M_BO_TA	32 位字符串（带时间标签）	unsigned int32
<9>	M_ME_NA	测量值，标准化值	float
<10>	M_ME_TA	测量值，标准化值（带时间标签）	float
<11>	M_ME_NB	测量值、标度值	float
<12>	M_ME_TB	测量值、标度值（带时间标签）	float
<13>	M_ME_NC	测量值，短浮点数	float
<14>	M_ME_TC	测量值，短浮点数（带时间标签）	float
<15>	M_IT_NA	综合总数	int32
<16>	M_IT_TA	综合总数（带时间标签）	int32
<17>	M_EP_TA	保护部件事件（带时间标签）	unsigned int8（0 – 不确定，1 – 关闭，2 – 开启，3 – 不确定）
<18>	M_EP_TB	保护部件分组启动事件（带时间标签）	unsigned int8（符合标准的位集）
<19>	M_EP_TC	保护部件分组输出回路信息（带时间标签）	unsigned int8（符合标准的位集）
<20>	M_PS_NA	带有状态更改检测的分组单点信息	unsigned int16
<21>	M_ME_ND	测量值，不含质量描述符的标准化值	float
<30>	M_SP_TB	单点信息（带时间标签 CP56Time2a）	布尔（0 - 关闭，1 - 开启）
<31>	M_DP_TB	双点信息（带时间标签 CP56Time2a）	unsigned int8（0 – 不确定或中间，1 – 关闭，2 – 开启，3 – 不确定）
<32>	M_ST_TB	步骤位置信息（带时间标签 CP56Time2a）	int8（-64...+64）
<33>	M_BO_TB	32 位字符串（带时间标签 CP56Time2a）	unsigned int32
<34>	M_ME_TD	测量值，标准化值（带时间标签 CP56Time2a）	float
<35>	M_ME_TE	测量值，缩放值（带时间标签 CP56Time2a）	float
<36>	M_ME_TF	测量值，短浮点数（带时间标签 CP56Time2a）	float
<37>	M_IT_TB	综合总数（带时间标签 CP56Time2a）	int32
<38>	M_EP_TD	保护部件事件（带时间标签 CP56Time2a）	unsigned int8（0 – 不确定，1 – 关闭，2 – 开启，3 – 不确定）
<39>	M_EP_TE	保护部件分组启动事件（带时间标签 CP56Time2a）	unsigned int8（符合标准的位集）
<40>	M_EP_TF	保护部件分组输出回路信息（带时间标签 CP56Time2a）	unsigned int8（符合标准的位集）
2. 控制方向的处理信息			
<45>	C_SC_NA	单一命令	布尔（0 - 关闭，1 - 开启）
<46>	C_DC_NA	双重命令	unsigned int8（0 – 不允许，1 – 关闭，2 – 开启，3 – 不允许）
<47>	C_RC_NA	调节步进命令	unsigned int8（0 – 不允许，1 – 下一步向上，2 – 下一步向下，3 – 不允许）

帧类型 ID	操作	描述	主值/系统命令类型
<48>	C_SE_NA	设定点命令，标准化值	float
<49>	C_SE_NB	设定点命令，缩放值	float
<50>	C_SE_NC	设定点命令，短浮点数	float
<51>	C_BO_NA	32 位字符串	int32
<58>	C_SC_TA	单个命令（带时间标签 CP56Time2a）	布尔（0 - 关闭，1 - 开启）
<59>	C_DC_TA	双重命令（带时间标签 CP56Time2a）	unsigned int8（0 – 不允许，1 – 关闭，2 – 开启，3 – 不允许）
<60>	C_RC_TA	调节步进命令（带时间标签 CP56Time2a）	unsigned int8（0 – 不允许，1 – 下一步向上，2 – 下一步向下，3 – 不允许）
<61>	C_SE_TA	设定点命令，标准化值（带时间标签 CP56Time2a）	float
<62>	C_SE_TB	设定点命令，缩放值（带时间标签 CP56Time2a）	float
<63>	C_SE_TC	设定点命令，短浮点数（带时间标签 CP56Time2a）	float
<64>	C_BO_TA	32 位字符串（带时间标签 CP56Time2a）	int32
3. 监控方向的系统信息			
<70>	M_EI_NA	初始化结束	END OF INITIALIZATION 系统命令
4. 控制方向的系统信息			
<100>	C_IC_NA	询问命令	INTERROGATION 系统命令
<101>	C_CI_NA	反询问命令	COUNTER INTERROGATION 系统指令
<102>	C_RD_NA	读命令	READ 系统命令
<103>	C_CS_NA	时钟同步命令	CLOCK SYNCHRONIZATION 系统命令
<104>	C_TS_NA	测试命令	TEST 系统命令
<105>	C_RP_NA	重置进程命令	RESET PROCESS ACTIVATION / RESET PROCESS CONFIRMATION 系统命令
<106>	C_CD_NA	延迟采集命令	DELAY ACQUISITION 系统命令
<107>	C_TS_TA	测试命令（带时间标签 CP56Time2a）	检测到 TEST WITH TIME TAG 系统命令
5. 控制方向参数			
<110>	P_ME_NA	测量值参数，标准化值	float
<111>	P_ME_NB	测量值参数，缩放值	float
<112>	P_ME_NC	测量值参数，短浮点数	float
<113>	P_AC_NA	参数激活	PARAMETER ACTIVATION 系统命令
6. 文件传输			
<120>	F_FR_NA	文件就绪	没有处理
<121>	F_SR_NA	部分已准备好	没有处理
<122>	F_SC_NA	调用目录、选择文件、调用文件、调用部分	CALL DIRECTORY、SELECT FILE、CALL FILE、CALL SECTION 系统命令
<123>	F_LS_NA	最后部分，最后段	没有处理
<124>	F_AF_NA	确认文件，确认部分	没有处理
<125>	F_SG_NA	段	没有处理
<126>	F_DR_TA	目录	没有处理

加载、处理和管理设备和标记配置，支持 IEC 61850 标准协议

Kaspersky Industrial CyberSecurity for Networks 中已使用的工业网络流量分析技术提供了有关支持 IEC 61850: IEC 61850-8-1 (GOOSE, MMS) 标准协议的设备的参数和交互的基本信息。但是，为了获取和保存有关这些设备的最完整数据，包括其原始结构化格式的标记，推荐将按照 IEC 61850-6 标准准备的文件内容加载到应用程序中。通过导入 IEC 61850 设备的项目来加载此类文件的内容。

导入 IEC 61850 设备项目时，Kaspersky Industrial CyberSecurity for Networks 会检查项目文件内容的语法和格式，并分析项目中的设备配置是否符合 IEC 61850 标准的要求和建议。成功导入项目后，应用程序会分析流量是否符合导入的配置。如果流量显示的交互与保存的配置有偏差（设备交互或传输的设置与配置中的描述不匹配），则应用程序会注册事件。

这样，用于处理和管理 IEC 61850 设备配置的内置工具可让您将 Kaspersky Industrial CyberSecurity for Networks 用作防范信息安全威胁的应用程序，也可以用作扫描包含配置描述的文件的工具。根据文件中的数据，应用程序允许您检测 IEC 61850 设备组设计中的错误和缺陷。您可以逐步消除已识别的错误和设计缺陷。

支持的项目类型和协议处理模块随着应用程序模块和数据库的更新而更新。您需要安装更新才能使用应用程序支持的所有功能来分析设备配置和分析 IEC 61850 协议上的流量。

使项目符合 IEC 61850 标准的方案包括以下步骤：

1. **将 IEC 61850 设备项目导入 Kaspersky Industrial CyberSecurity for Networks。**

   在此步骤中，您必须导入 IEC 61850 设备的项目。导入项目中的设备配置必须以 SCL（系统配置语言）描述，并保存在符合 IEC 61850 标准而使用的一个或多个文件中。支持导入此类项目的 SCL 文件类型 *.SCD、*.CID 和 *.ICD。

   在导入过程结束时，应用程序提供查看结果报告的功能。要查看报告，您必须通过单击应用程序 Web 界面菜单中的 按钮打开后台操作列表，然后在导入过程完成后单击“**显示报告**”按钮。

   如果在扫描和分析导入的文件期间检测到错误或缺陷（不一致），则有关它们的信息将显示在报告窗口的以下部分中：

   - **语法和格式错误**。
   - **不符合标准**（显示检测到的不符合项不超过 100 个）。

   如果报告窗口不包含任何指定的部分，则可以继续执行步骤 3。否则，请仔细阅读报告窗口中的错误和不一致列表，然后继续执行步骤 2。

2. **根据导入报告解决错误和不一致问题**

   导入过程中检测到的错误和不一致的重要性可能有所不同。一些错误（例如，不同修订版的语法错误）导致无法加载文件并阻止导入整个项目内容。其他错误和不一致可能是由导入项目中的逻辑错误以及已使用部件的特定设置引起的（如果部件的操作能力允许您为其设置参数而不遵守使用 IEC 61850 标准的某些建议）。应用程序会在导入报告中针对这些错误和不一致显示适当的警告。

   在审查导入过程中发现的错误和不一致列表后，您需要决定在项目中进行哪些必要的改进。使用适当的软件工具来解决错误和不一致问题。

   如果您对项目进行了任何修改或添加，请保存项目文件并再次执行步骤 1 以导入更新的文件。如果不需要修改项目，请跳至步骤 3。

3 扫描因项目导入而在 Kaspersky Industrial CyberSecurity for Networks 中创建的对象

在此步骤中，您需要检查导入后应用程序中的更改，并在必要时对应用程序中的对象执行其他操作。

如果导入的项目包含相关数据，应用程序将执行以下操作：

- 添加新的设备（或更新现有的设备），同时指示网络交互参与者的地址信息。
- 为设备添加过程控制设置并在这些设置中保存以下内容：
  - 受监控的系统命令
  - MMS 和 GOOSE 协议的订阅和数据块
- 在原有的结构化标记格式上添加 MMS 和 GOOSE 协议的标记。
- 根据导入的配置中的设备信息生成交互控制规则。

> 对于结构化格式的标记，无法定义条件过程控制规则来跟踪值。如果您想使用应用程序检查标记的值，您可以使用带有 Lua 脚本的规则来实现此目的。

4 在检测到流量与保存的配置有偏差时记录的跟踪事件

应用程序使用保存的配置来分析工业网络流量。如果流量显示的交互与保存的配置有偏差（设备交互或传输的设置与配置中的描述不匹配），应用程序会根据网络完整性控制和命令控制技术注册事件。

在分析 IEC 61850: GOOSE 协议上的交互时，应用程序会在以下情况下记录事件：

- 检测到消息源和接收者的 MAC 地址不一致。
- 检测到工厂配置（GOOSE 消息中的 goID 相同）。
- 检测到 ConfRev 版本不一致。
- 检测到 GOOSE 消息状态不一致。
- 检测到 GOOSE 消息包主要参数不一致。
- 检测到信号质量设置不一致。
- 检测到消息传输顺序不一致。
- 检测到来自未描述设备的 GOOSE 消息。
- 检测到来自所描述设备的未描述的 GOOSE 消息。
- 检测到 GOOSE 消息中数据包结构的变化。
- 检测到 GOOSE 消息中 VLAN ID 的使用不一致。
- 检测到标记值和创建的过程控制规则之间的不一致。

在分析 IEC 61850: MMS 协议上的交互时，应用程序会在以下情况下注册事件：

- 检测到 IP 或 MAC 地址不一致（考虑通过路由器的交互）。
- 检测到重复的姓名/地址。

- 检测到 ConfRev 版本不一致。
- 检测到执行的系统命令序列不一致。
- 检测到标记值和创建的过程控制规则之间的不一致。
- 检测到客户端到服务器连接方法（读/写或通过订阅）不一致。

事件跟踪阶段的持续时间取决于工业过程中设备交互的频率和操作模式的变化。如果您的评估表明所有受监控的设备都已执行其预期操作，并且应用程序未因上述原因注册任何事件，则可以认为使项目符合 IEC 61850 标准的方案已完成。否则，如果事件已注册，则转至步骤 5。

5. **微调项目以消除与保存的配置的偏差**

   在调查事件注册原因时，首先要核实是否存在信息安全威胁、是否存在工业过程违规行为。

   在您确信事件是由于保存的配置中的错误或不一致而注册的之后，您需要决定在项目中进行必要的改进。使用适当的软件工具来解决错误和不一致问题。

   如果您对项目进行了任何修改，请保存项目文件并从步骤 1 开始重复此场景中的步骤。

在采取所有必要措施使项目符合 IEC 61850 标准后，您可以在监控模式下使用 Kaspersky Industrial CyberSecurity for Networks 的所有功能。但是，推荐通过以下应用程序功能定期评估工业网络基础设施的安全性和性能：

- 监控网络会话并执行在线监控以评估当前网络拥塞情况（包括使用“**流量**”和“**标记**”小部件）。
- 使用“资产管理”、“交互控制”和“基于规则的网络异常检测和入侵检测”来监控网络上具有新地址的设备的出现。
- 监控事件以跟踪基于命令控制技术在事件中注册的未描述消息，并跟踪基于入侵检测技术在事件（系统事件类型代码 4000005100、4000005101、4000005102、4000005103 和 4000002701）中和基于资产管理技术在事件（系统事件类型代码 4000005005）中注册的故障和网络错误。

将 Kaspersky Industrial CyberSecurity for Networks 事件传输到 SIEM 系统

本节介绍发送到 SIEM 系统的事件。

在 Kaspersky Industrial CyberSecurity for Networks 中，您可以使用连接器将数据发送到 SIEM 系统服务器。添加连接器后，您需要配置通过该连接器转发事件。

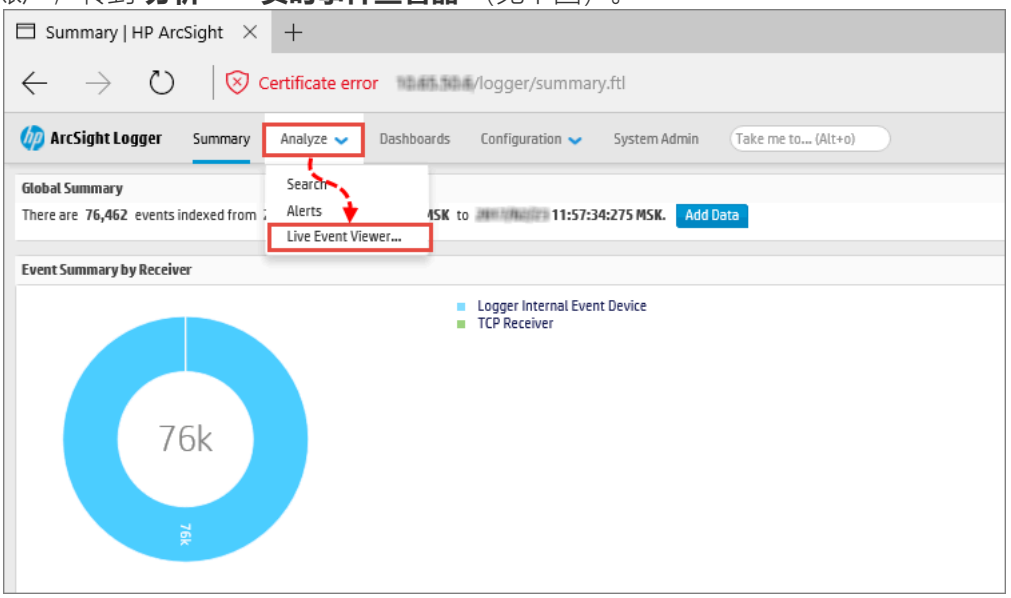
转发到 SIEM 系统的事件信息显示的内容和顺序可能与 Kaspersky Industrial CyberSecurity for Networks 服务器 Web 界面的“**事件和突发事件**”部分的“**事件**”选项卡上显示的数据不同。

使用 HP ArcSight 系统验证事件转发（作为示例）

要使用 HP ArcSight 系统验证事件转发（作为示例）：

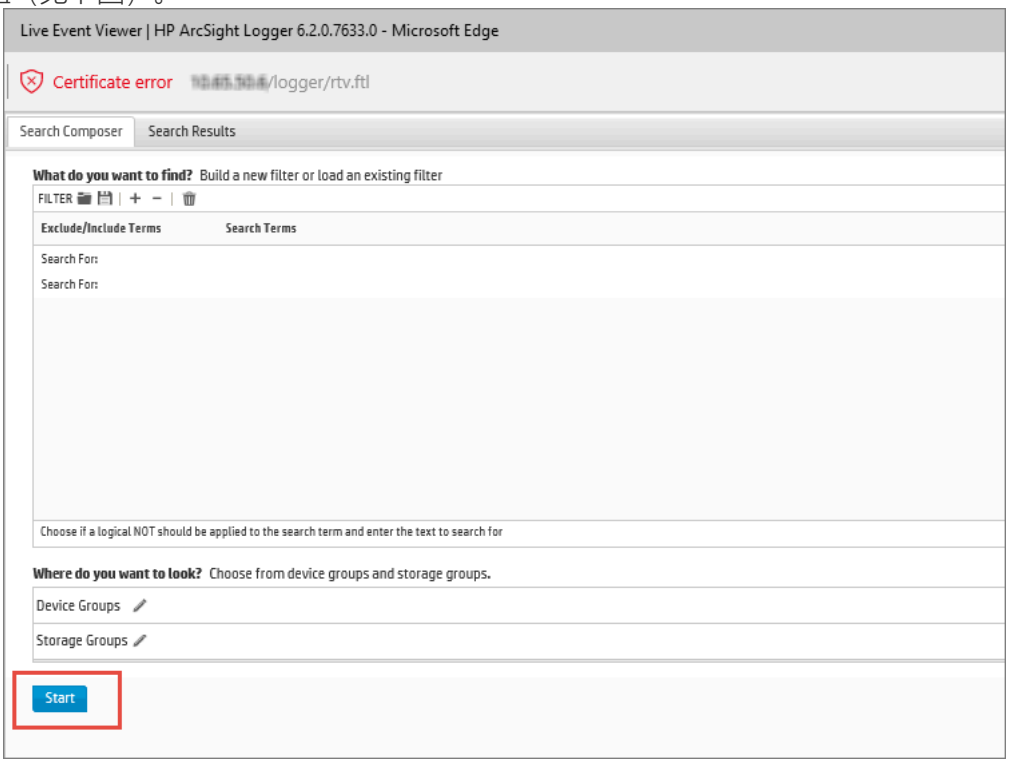
1. 确保使用 HP ArcSight 系统的标准工具配置了用于接收来自 Kaspersky Industrial CyberSecurity for Networks 的消息的通道。
2. 打开浏览器并输入 HP ArcSight 系统的地址。

3. 登录您的用户账户，转到“**分析**” → “**实时事件查看器**”（见下图）。



在 HP ArcSight 系统中打开“**实时事件查看器**”部分

4. 单击“**开始**”按钮（见下图）。



在 HP ArcSight 系统中启动“**实时事件查看器**”

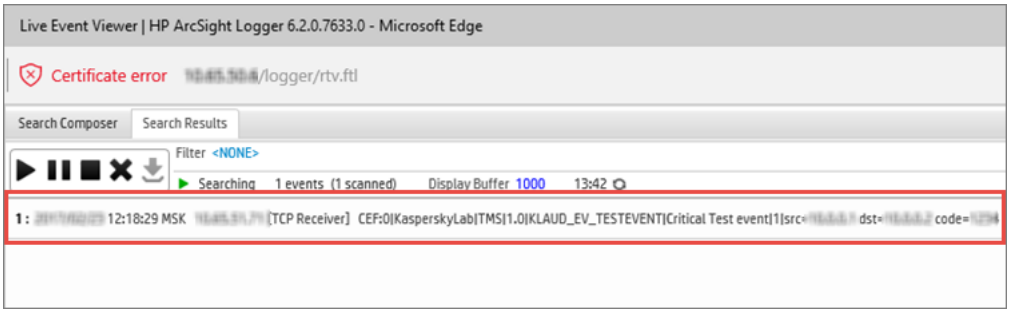
5. 打开命令行界面，输入以下命令，以通过 Telnet 协议连接服务器：

```
telnet <ArcSight 服务器地址> <端口>
```

6. 发送 CEF 格式的测试消息：

```
CEF:0|KasperskyLab|TMS|1.0|KLAUD_EV_TESTEVENT|Critical Test event|1|src=10.0.0.1 dst=10.0.0.2 code=1234
```

如果与 HP ArcSight 系统有连接，“**实时事件查看器**”部分将显示内容与发送的消息匹配的事件（见下图）。



验证操作结果

转发到 SIEM 系统的消息格式

该应用程序以 CEF 20 格式将数据传输到 SIEM 系统。以下内部结构用于数据传输：

- `EventMessage` – 用于事件。
- `ApplicationMessage` – 用于应用程序消息。
- `AuditMessage` – 用于审计条目。

收到的消息不会转换为系统日志协议格式。

EventMessage 结构的格式

下表提供了以下列的数据：

- EventMessage – 消息中的字段名称。
- 事件 – Kaspersky Industrial CyberSecurity for Networks 中事件的对应字段或特定值。
- 描述 – 字段描述。

EventMessage	事件	描述
dateTime	开始	捕获事件触发网络数据包的日期和时间（精确到毫秒）。
hostname	Kaspersky Industrial CyberSecurity for Networks 服务器地址	Kaspersky Industrial CyberSecurity for Networks 服务器的地址。
cefVersion	0	CEF 版本号。
deviceVendor	Kaspersky Lab	提供商。
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	产品名称。
deviceVersion	示例：4.5.0.247	Kaspersky Industrial CyberSecurity for Networks 的版本。
messageType	事件	已发送消息类型。
signatureId	事件类型	事件类型 ID。
name	标题	事件描述。

severity	事件严重性级别： • 9 – 分数 8.0–10.0 • 6 – 分数 4.0–7.9 • 3 – 分数 0.0–3.9	事件严重性级别。 值从 3 到 9，其中 9 代表最严重事件。
score	事件分数	事件分数值。
extension	在扩展字段表中指示	针对每种消息类型单独确定。

日期和时间按以下格式发送： `YYYY-MM-DD T hh:mm:ss.ms Z`。示例：2025-10-30T22:14:15.030Z – 事件发生的时间，即 2025 年 10 月 30 日 22 时 14 分 15 秒 030 毫秒。

Extension 字段的内容

下表提供了以下列的数据：

- Extension – 消息中的字段名称。
- 相关事件 – 发送特定字段的事件。
- 描述 – 字段描述。

Extension	相关事件	描述
cnt	事件的公共字段	事件注册后重复该事件的次数计数器。
dmac	事件的公共字段	目的 MAC 地址。
dmacas	事件的公共字段	目标 MAC 地址的地址空间。
dpt	事件的公共字段	目的端口。
dst	事件的公共字段	目的 IP 地址。
das	事件的公共字段	目标 MAC 地址的地址空间（如果向应用程序添加了额外的地址空间）。
end	事件的公共字段	事件结束时间。
smac	事件的公共字段	源 MAC 地址。
smacas	事件的公共字段	源 MAC 地址的地址空间。
spt	事件的公共字段	源端口。
src	事件的公共字段	源 IP 地址。
srcas	事件的公共字段	源 MAC 地址的地址空间（如果向应用程序添加了额外的地址空间）。
start	事件的公共字段	事件注册时间。
technology	事件的公共字段	用于注册事件的技术。
triggeredRule	事件的公共字段	触发的规则。
protocol	事件的公共字段	协议。
vlanId	事件的公共字段	VLAN ID。
monitoringPoint	事件的公共字段	其流量触发了事件注册的监控点。
sourceIndustrialAddress	事件的公共字段	源的应用程序级地址。
destinationIndustrialAddress	事件的公共字段	目标的应用程序级地址。
eventIdentifier	事件的公共字段	事件 ID。
noTrafficDuration	监控点无流量	无流量时段。
tagId	无效的标签类型	标签 ID。

expectedTagType	无效的标签类型	标签的预期数据类型。
actualTagType	无效的标签类型	标签的实际数据类型。
ruleName	• 违反过程控制规则 • 触发了系统规则集中的入侵检测规则	规则名称。
tags	违反过程控制规则	标签。
msg	触发了系统规则集中的入侵检测规则	消息。
substitutedIpAddress	• 在 ARP 回复中检测到的 ARP 欺骗迹象 • 在 ARP 请求中检测到的 ARP 欺骗迹象	网络数据包的源 IP 地址。
targetIpAddress	• 在 ARP 回复中检测到的 ARP 欺骗迹象 • 在 ARP 请求中检测到的 ARP 欺骗迹象	网络数据包的目标 IP 地址。
attackStartTimestamp	• 在 ARP 回复中检测到的 ARP 欺骗迹象 • 在 ARP 请求中检测到的 ARP 欺骗迹象	显示攻击迹象的活动的开始时间。
ownerMac	• 检测到 IP 地址冲突 • 检测到的新 IP 地址 • 检测到的新设备 • 收到的新信息 • 从 MAC 地址检测到的流量 • MAC 地址已添加到设备 • IP 地址已添加到设备	所有者的 MAC 地址。
ownerIp	• 检测到的新设备 • MAC 地址已添加到设备 • IP 地址已添加到设备 • 检测到 IP 地址冲突 • 检测到的新 MAC 地址	所有者的 IP 地址。
challengerMac	检测到 IP 地址冲突	挑战者的 MAC 地址。
newIpAddress	检测到的新 IP 地址	新 IP 地址。
newMacAddress	检测到的新 MAC 地址	新 MAC 地址。
oldIpAddress	检测到的新 IP 地址	旧 IP 地址。
assetName	检测到的新设备	设备名称。

设备设置

下表提供了有关设备设置的数据。

如果发现一台或两台设备存在交互，Kaspersky Industrial CyberSecurity for Networks 还会将有关一台或两台设备的已知信息发送到 SIEM 系统。

如果在检测到的交互中识别出多个设备，则消息会重复，包含不同的地址信息和不同的设备设置（如果设备不同）。

Extension	设备设置
srcAssetName	源设备的名称。
srcVendor	源设备的供应商。
srcOS	源设备的操作系统。
srcNetworkName	源设备的网络名称。

srcModel	源设备的型号。
dstAssetName	目标设备的名称。
dstVendor	目标设备的供应商。
dstOS	目标设备的操作系统。
dstNetworkName	目标设备的网络名称。
dstModel	目标设备的型号。

ApplicationMessage 结构的格式

下表提供了以下列的数据：

- EventMessage — 消息中的字段名称。
- 应用程序消息 — Kaspersky Industrial CyberSecurity for Networks 中应用程序消息的对应字段或特定值。
- 描述 — 字段描述。

EventMessage	应用程序消息	描述
dateTime	发生日期和时间	检测到导致消息记录的情况的日期和时间（精确到毫秒）。
hostname	Kaspersky Industrial CyberSecurity for Networks 服务器或探测器的地址	Kaspersky Industrial CyberSecurity for Networks 服务器或探测器的节点地址。
cefVersion	0	CEF 版本号。
deviceVendor	Kaspersky Lab	提供商。
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	产品名称。
deviceVersion	示例：4.5.0.247	Kaspersky Industrial CyberSecurity for Networks 的版本。
messageType	应用程序消息	已发送消息类型。
severity	应用程序消息严重性级别： • 10 表示以下状态：*中度故障*、*严重故障*或*致命故障*。 • 5 表示以下状态：*未知*、*故障*。 • 0 表示“*正常操作*”状态。	应用程序消息的严重性级别。 值从 0 到 10，其中 10 是最严重的消息。
address	节点地址	消息来源节点的地址。
systemProcess	进程名称	触发了消息注册的应用程序进程。
msg	消息	消息的数字标识符和文本。

AuditMessage 结构的格式

下表提供了以下列的数据：

- EventMessage — 消息中的字段名称。
- 审计消息 — Kaspersky Industrial CyberSecurity for Networks 中审计条目的对应字段或特定值。
- 描述 — 字段描述。

EventMessage	审计消息	描述
dateTime	发生日期和时间	检测到导致审计条目记录的情况的日期和时间（精确到毫秒）。
hostname	Kaspersky Industrial CyberSecurity for Networks 服务器地址	Kaspersky Industrial CyberSecurity for Networks 服务器的节点地址。
cefVersion	0	CEF 版本号。
deviceVendor	Kaspersky Lab	提供商。
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	产品名称。
deviceVersion	示例：4.5.0.247	Kaspersky Industrial CyberSecurity for Networks 的版本。
messageType	审计消息	已发送消息类型。
address	用户节点	在其中执行已注册操作的节点地址。
user	用户	执行注册的操作的用户的名称。
action	操作	用户执行的已注册操作。
result	结果	已注册操作的结果（成功或未成功）。
msg	描述	关于已注册操作的附加信息。

使用脚本更改 Kaspersky Industrial CyberSecurity for Networks 配置设置

在 Kaspersky Industrial CyberSecurity for Networks 中，您可以更改下表列出的应用程序配置设置。设置在服务器计算机的 /opt/kaspersky/kics4net/sbin/ 处的 kics4net-params 脚本的帮助下进行编辑。

Kaspersky Industrial CyberSecurity for Networks 配置设置

配置设置（设置的别名）	默认值	值范围	描述
`-t (--logon_session_timeout)`	600 分钟（相当于 10 小时）	1 至 43,200 分钟	通过 Web 界面进行的服务器连接会话和 Kaspersky Industrial CyberSecurity for Networks API 中的身份验证令牌的有效期。 该值以分钟为单位显示。
`-l (--max_password_ttl_in_days)`	90 天。	1 至 366 天	需要更改密码的最长密码使用期限。 该值以天数表示。
`-a (--attempts_to_login_limit)`	3	从 1 到 100	触发向管理员发出通知的登录尝试失败次数。

您可以使用 kics4net-params 脚本查看和调整配置设置。

要查看运行配置设置：

1. 在服务器计算机上，使用要用于运行 kics4net params 脚本的具有 root 权限的用户账户的账户凭据登录系统。
2. 转到 /opt/kaspersky/kics4net/sbin/ 文件夹并输入以下命令运行脚本以查看当前定义的值：

```
sudo python kics4net-params get -n <配置设置>
```

其中：

- `-n` 禁用显示用于表示应用程序配置中的值的内部名称。如果未定义设置，则值将与名称一起显示（例如：`logon_session_timeout=<值>`）。
- `<配置设置>`是屏幕上将显示其值的配置设置（必填设置）。

显示密码最大使用期限的示例命令

```
sudo python kics4net-params get -n -l
```

要调整配置设置：

1. 在服务器计算机上，使用要用于运行 kics4net params 脚本的具有 root 权限的用户账户的账户凭据登录系统。
2. 转到 /opt/kaspersky/kics4net/sbin/ 文件夹并输入以下命令运行脚本以更改值：

```
python kics4net-params set -r <配置设置>=<值>
```

其中：

- `-r` 应用新的值后，允许自动重新启动服务器计算机上的应用程序服务。如果未定义此参数，则必须在脚本完成后手动重新启动服务器计算机或重新启动服务。
- `<配置设置>=<值>`是配置设置的新值（必填设置）。

更改密码最大使用期限的示例命令

```
sudo python kics4net-params set -r -l=100
```

将 Kaspersky Industrial CyberSecurity for Networks节点连接为 Kaspersky Security Center 中的连接网关的详细信息

您可以使用已安装应用程序组件（服务器和传感器）的节点作为 Kaspersky Security Center 中的连接网关。分发点充当连接 Kaspersky Security Center 管理服务器的网关。使用分发点与受管理设备进行通信的图表允许您优化数据库、应用程序模块和卡巴斯基应用程序更新流量并在 Kaspersky Security Center 中配置 IP 范围的流量限制。如果 Kaspersky Industrial CyberSecurity for Networks Server 或传感器节点提供管理服务器与位于隔离网络上的受管理设备之间的唯一可用连接，则该节点上的连接网关角色允许您为管理服务器提供与这些设备的网络连接。

本文介绍了配置和扫描 Kaspersky Industrial CyberSecurity for Networks 节点以充当 Kaspersky Security Center 中的连接网关的场景。该场景包含以下步骤：

1 在节点上安装网络代理

如果在服务器安装期间添加了应用程序与 Kaspersky Security Center 之间的通信功能，网络代理会自动安装在 Kaspersky Industrial CyberSecurity for Networks Server 节点上。添加通信功能后，在 Kaspersky Industrial CyberSecurity for Networks 中启用并配置该功能。

在将服务器上的网络代理配置为连接网关之前，您必须启用并配置 Kaspersky Industrial CyberSecurity for Networks 中的通信功能。在服务器上配置网络代理后启用通信功能将重置指定的配置设置并禁用节点上的连接网关角色。在这种情况下，要恢复作为连接网关的节点操作，请重复场景中的步骤，从网络代理配置开始。

在集中或本地安装 Kaspersky Industrial CyberSecurity for Networks 组件时，网络代理不会默认安装在 Sensor 节点上。如果 Sensor 节点上没有安装网络代理，请借助 klnagent64-<网络代理版本号>.x86_64.rpm 包进行安装，该包在准备安装应用程序时被保存到 kics4net-release_<应用程序版本号>/linux-centos 目录。

要安装网络代理，请在安装了 Sensor 的计算机上执行以下操作：

1. 复制 klnagent64-<网络代理版本>.x86_64.rpm 网络代理安装包到任意目录
2. 在操作系统控制台中，转到包含包文件的文件夹，然后输入以下命令：

```
sudo rpm -i klnagent64-<网络代理版本号>.x86_64.rpm
```

等待网络代理安装过程完成。

2 允许使用端口

在此步骤中，您必须允许使用网络代理节点计算机上的防火墙端口。您可以使用以下命令来启用端口使用：

```
sudo firewall-cmd --permanent --add-port=13000/tcp
sudo firewall-cmd --permanent --add-port=13295/tcp
sudo systemctl restart firewalld
```

3 配置网络代理

此步骤将激活管理代理上的连接网关模式。当激活此模式并随后添加节点作为分发点时，Kaspersky Security Center 会更改使用此设备作为连接网关的标识和身份验证详细信息。

如果更改了凭据和身份验证信息，要在之前配置的网络上将新分发点用作连接网关，您需要在要连接到新添加的连接网关的所有设备上重新安装网络代理。这包括以前使用该节点作为连接网关的那些设备。在这些设备上重新安装网络代理之前，它们将无法连接到新添加的连接网关。

要在网络代理上激活连接网关模式，请在节点计算机上执行以下操作：

1. 运行安装后脚本来配置网络代理本地环境。为此，请输入以下命令：

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

2. 请仔细阅读最终用户授权许可协议。要转到包含最终用户授权许可协议文本的下一个屏幕，请按**空格键**。
3. 查看完后，如果您完全同意最终用户授权许可协议的条款，请接受这些条款。为此，请输入 y。
4. 输入管理服务器名称或 IP 地址。
5. 如果需要，请更改与管理服务器的未加密和加密连接的默认端口。
6. 选择连接到管理服务器的模式。为此，请输入适当的字符：

   y ： 通过 SSL 进行安全连接

   n ： 未加密的连接。

7. 在请求网络代理操作模式的步骤中，选择“**用作连接网关**”。

8. 等待脚本完成。脚本运行完成两到三分钟后，检查网络代理和管理服务器之间的连接。为此，请输入以下命令：

```
sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

屏幕将显示有关管理服务器连接的信息。如果配置成功应用，屏幕上将显示以下消息：

```
HostId: <字母数字序列的 ID >
该主机已安装为连接网关，但尚未在服务器上注册
正在连接到服务器...确定
正在连接到管理代理...确定
```

4 在 Kaspersky Security Center 中添加节点作为分发点

Kaspersky Industrial CyberSecurity for Networks 节点在 Kaspersky Security Center 中添加为分发点后将开始充当连接网关。为此，请执行以下操作：

1. 连接到 Kaspersky Security Center 管理服务器。

2. 在控制台树中，打开“**管理服务器**”节点的上下文菜单并选择“**属性**”。

3. 在管理服务器属性窗口中，选择“**分发点**”部分。

4. 在窗口右侧，选择“**手动分配分发点**”，然后单击“**添加**”。

   “**添加分发点**”窗口打开。

5. 要指定充当分发点的设备，请选择添加连接网关的选项，然后输入 Kaspersky Industrial CyberSecurity for Networks 节点的 IP 地址或计算机名称。

6. 要指定分发点的范围，请选择“**管理组**”选项并指定其设备将使用连接网关的管理组。

7. 将节点添加到分发点列表后，请确保为该节点启用与管理服务器的持久连接。为此，请打开节点属性窗口并检查“**常规**”部分中的“**不断开与管理服务器的连接**”复选框是否已选中。该复选框必须自动选中，不得手动清除或选择。

5 验证网络代理与 Kaspersky Security Center 之间的连接是否成功

您可以验证在节点计算机上添加连接网关和分发点所涉及的步骤是否成功。为此，请输入以下命令：

```
sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

屏幕将显示有关管理服务器连接的信息。如果成功完成这些步骤，屏幕上会显示以下消息：

```
主机是连接网关
主机是分发点
与服务器的连接：活动
与服务器的 CG 连接：活动
```

用于导入通用项目的文件

您可以使用通用格式项目将设备和标签的过程控制配置导入卡巴斯基 Kaspersky Industrial CyberSecurity for Networks。通用项目可以使用带分隔符的文本文件（CSV 文件）导入。CSV 格式是一种用于表示表格数据的文本格式。

您可以使用所选择的任何方法（例如，从 SCADA 系统）创建数据文件。要将创建的文件导入应用程序，您需要将文件打包到 ZIP 存档中。

用于导入通用项目的文件集可能由以下 CSV 文件组成：

- devices.csv.包含设备的描述。
- connections.csv.包含连接的描述。
  “*连接*”是指设备、一组设备协议以及通过此类协议中继转发的一组设备标记之间已命名的关联。
- variables.csv.包含连接的变量和标记的描述。
- enums.csv.包含 IEC 61850 标准的枚举描述。
- datasets.csv.包含 IEC61850 标准的数据集描述。
- iec61850_mms_reports.csv.包含 IEC 61850：MMS 协议的报告描述。

使用通用格式项目时，您无法在其原始结构化标签视图中导入 IEC 61850 MMS 和 GOOSE 标签。如果标签包含字段结构，则该结构的每个字段都必须作为应用程序的单独标签进行描述。要向应用程序添加结构化标签，请使用以下专门设计的项目类型：**IEC 61850 设备项目**。

在使用数据文件时，应考虑以下特殊注意事项：

- 数据文件必须采用 UTF-8 编码。
- Variables.csv 文件中的标签列表具有“连接”分组属性。
- 您可以在 connections.csv 文件中为一个连接指定多个不同的协议和地址。
- 协议可以具有一个或多个地址。
- 一台设备可以具有采用不同标记集的多个连接。
- 在导入数据文件时，仅考虑指定参数的值。将忽略未指定值的参数。如果数据文件中缺少某些字符串，且数据文件集中的其他文件包含对这些字符串的引用，则在导入过程中，将忽略相关字符串。
- 仅当为 IEC 61850 标准的 MMS 和 GOOSE 协议描述枚举和数据集时，才会填充 enums.csv 和 datasets.csv 文件中包含参数值的行。对于其他协议，enums.csv 和 datasets.csv 文件仅包含标题行。请注意，enums.csv 和 datasets.csv 文件必须包含在用于导入的文件集中。

包含设备描述的文件：devices.csv

包含设备描述的文件中列出了设备、设备类和连接 ID。设备描述文件中的连接 ID 在连接描述文件中指定，用于将协议链接到设备。

如果为不同的标记集使用不同的协议，则必须为单台设备使用多个连接。在 devices.csv 文件的每一行中，连接 ID 必须是唯一的。

该文件应以标头字符串开头，标头字符串包含处理文件所需的数据。

devices.csv 文件的示例标头字符串

```
'Devices
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Device;Type;Connection
```

devices.csv 文件的标头字符串包含以下值：

- `设备`

  在此字符串中指定 CSV 文件的名称。`Devices` – 设备描述文件的名称。数据文件名称与文件用途相对应，并在设置中为每个文件进行定义。

- `Format Version;KICS Importer Version`

  此字符串指定文件格式的版本以及创建该文件所使用的工具的版本。请为参数 `Format version` 指定值 V1.0.0.0。然后，建议指定创建该 CSV 文件所使用的工具的名称和版本。

- `Field separator: ; Decimal separator: .Text quotes: " Var name separator: .`

  使用此字符串可指定该数据文件中所使用的分隔符：

  - `字段分隔符：;`
  - `小数分隔符：.`
  - 行终止符：`Text quotes: "`
  - 标记名称中的字段分隔符：`Var name separator: .`

- `Device;Type;Connection`

  此字符串包含数据列的名称。文件中的数据应按照以下列顺序指定：

  - `Device` – 设备名称。
  - `Type` – 设备类代码。可使用以下代码：
    - 0 – SIEMENS SIMATIC S7-300
    - 1 – SIEMENS SIMATIC S7-400
    - 2 – SCHNEIDER ELECTRIC MOMENTUM
    - 3 – SCHNEIDER ELECTRIC M340

- 4 – MITSUBISHI SYSTEM Q
- 5 – ALLEN-BRADLEY CONTROL LOGIX 5000
- 6 – SIEMENS SIPROTEC
- 7 – IEC 61850 GOOSE, MMS device
- 8 – IEC 60870-5-104 device
- 9 – ABB RELION 670
- 10 – GENERAL ELECTRIC RX3I
- 11 – SIEMENS SIMATIC S7-1500
- 12 – IEC 61850 SAMPLED VALUES device
- 13 – SIEMENS SIPROTEC 6MD66
- 14 – SIEMENS SIPROTEC 7SS52
- 15 – SIEMENS SIPROTEC 7UM62
- 16 – SIEMENS SIPROTEC 7SA52
- 17 – SIEMENS SIPROTEC 7SJ64
- 18 – SIEMENS SIPROTEC 7UT63
- 19 – GENERAL ELECTRIC MULTILIN B30
- 20 – GENERAL ELECTRIC MULTILIN C60
- 21 – EMERSON DELTAV
- 22 – SCHNEIDER ELECTRIC M580
- 23 – RELEMATIKA TOR 300
- 24 – EKRA 200 series
- 25 – EKRA BE2704 / BE2502
- 26 – OMRON CJ2M
- 27 – ABB AC 800M
- 28 – YOKOGAWA CENTUM
- 29 – CODESYS V3 设备
- 30 – DNP3 设备
- 31 – OPC UA 服务器

- 32 – ABB AC 700F
- 33 – SIEMENS SIMATIC S7-1200
- 34 – OPC DA 服务器
- 35 – BECKHOFF CX 系列
- 36 – PROSOFT-SYSTEMS REGUL R500
- 37 – EMERSON CONTROLWAVE
- 38 – IEC 60870-5-101 设备
- 39 – MOXA NPORT IA 5000 系列
- 40 – I/O 设备
- 41 – ABB RELION REF615
- 42 – SIEMENS SIMATIC S7-200
- 43 – MODBUS TCP 设备
- 44 – SCHNEIDER ELECTRIC SEPAM 80 NPP
- 45 – YOKOGAWA PROSAFE-RS
- 46 – SCHNEIDER ELECTRIC FOXBORO FCP280 / FCP270
- 47 – HONEYWELL CONTROLEDGE 900 系列
- 48 – HONEYWELL EXPERION C300
- 49 – SCHNEIDER ELECTRIC MICOM C264
- 50 – UMAS device
- 51 – TASE.2 server
- 52 – PROFINET device
- 53 – DIRECTLOGIC
- 54 – 支持加密的服务器
- 55 – BACNET 设备
- 56 – SCHNEIDER ELECTRIC P545
- 57 – YCU/ELC
- 58 – FEU 设备
- 59 – 通用 IED

- 60 – 通用网关
- 61 – 通用 PLC
- 62 – VALMET DNA 设备
- 63 – IPU 设备
- 64 – OWEN PLC100 系列
- 65 – 基于 CODESYS V2 的设备
- 66 – PNU20 设备
- 67 – KNX 设备
- 68 – DTS 设备
- 69 – B&R
- 70 – SIEMENS SICAM PAS 服务器
- 71 – TELNET 服务器
- 72 – VNIIA 设备
- 73 – CHINT MAS400
- 74 – CHINT MAS9600
- 75 – ISaGRAF 设备

- `Connection` – 来自包含连接描述的connections.csv文件的连接 ID。

标头字符串后面是文件正文，其中包含参数值（设备名称、设备类代码、连接 ID）。

示例 devices.csv 文件

```
'Devices
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Device;Type;Connection
"ms_plc";4;"ms_plc"
"mc_SysQ";8;"mc_SysQ"
```

连接描述文件：connections.csv

连接描述文件包含连接的 ID、应用层协议的编码、设备的完整网络地址。

该文件应以标头字符串开头，标头字符串包含处理文件所需的数据。

connections.csv 文件的示例标头字符串

```
'Connections
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
```

```
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;Protocol;Address
```

前三个标头字符串与devices.csv文件中的标头字符串相同。

字符串 `Connection;Protocol;Address` 包含数据列的名称：

- `Connection` — 描述文件的连接 ID。
  连接 ID 用于将协议链接到设备和标记。
- `Protocol` – 应用程序层协议的代码。可使用以下协议代码：
  - 0 – MODBUS TCP
  - 1 – SIEMENS S7COMM over TCP
  - 2 – SIEMENS S7COMM over INDUSTRIAL ETHERNET
  - 3 – MITSUBISHI MELSEC SYSTEM Q
  - 4 – ALLEN-BRADLEY ETHERNET/IP
  - 5 – IEC 61850 MMS
  - 6 – IEC 61850 GOOSE
  - 7 – IEC 60870-5-104
  - 8 – GENERAL ELECTRIC SRTP
  - 9 – IEC 61850 SAMPLED VALUES
  - 10 – SIEMENS S7COMMPLUS over TCP
  - 11 – EMERSON DELTAV
  - 12 – OMRON FINS over UDP
  - 13 – MMS for ABB AC 800M
  - 14 – YOKOGAWA VNET/IP
  - 15 – CODESYS V3 GATEWAY over TCP
  - 16 – DNP3
  - 17 – OMRON FINS over TCP
  - 18 – OPC UA BINARY
  - 19 – DMS for ABB AC 700F
  - 20 – OPC DA
  - 21 – OMRON FINS over ETHERNET/IP

- 22 – CODESYS V3 GATEWAY over UDP
- 23 – BECKHOFF ADS/AMS
- 24 – IEC 60870-5-101
- 25 – FOXBORO FCP280 / FCP270 INTERACTION
- 26 – BSAP
- 27 – HONEYWELL CONTROLEDGE 900 INTERACTION
- 28 – WMI INTERACTION
- 29 – HONEYWELL EXPERION INTERACTION
- 30 – MiCOM C264 INTERACTION
- 31 – SCHNEIDER ELECTRIC UMAS
- 32 – TASE.2
- 33 – PROFINET IO
- 34 – DIRECTLOGIC INTERACTION
- 35 – BACNET
- 36 – YARD
- 37 – COS
- 38 – IPU-FEU INTERACTION
- 39 – VALMET DNA INTERACTION
- 40 – CODESYS V2
- 41 – PNU20
- 42 – GENERAL ELECTRIC EGD
- 43 – KNXnet/IP
- 44 – DTS
- 45 – INA2000
- 46 – SIEMENS SICAM SCC - INTERACTION with SICAM PAS
- 47 – TELNET
- 48 – VNIIA
- 49 – CHINT MAS400

- 50 – CHINT MAS9600
- 51 – ISaGRAF IXL
- 52 – ISaGRAF SNCP

- `Address` – 包含设备的完整网络地址的字符串，特定于给定的协议。

  示例：
  与 Schneider Momentum 控制器的连接（一个 IP 地址）：
  `"Barline1";0;"IP-Address=192.168.2.7;Port=502"`

  与 Mitsubishi System Q 控制器的连接（一个 IP address，两个端口）：
  `"Station1";3;"IP-Address=192.168.2.8;Port=5001 Network=0;Station=0;PC=255"`
  `"Station1";3;"IP-Address=192.168.2.8;Port=5002 Network=0;Station=0;PC=255"`

  与冗余 Siemens S7-400 控制器的连接，两个控制器（两个 IP 地址，一个标记集）：
  `"S7$Program";1;"IP-Address=192.168.2.21;Port=102;Rack=0;Slot=2"`
  `"S7$Program";1;"IP-Address=192.168.2.22;Port=102;Rack=0;Slot=2"`

  与 Siemens S7-400 控制器的连接使用两个协议：通过 TCP/IP 堆栈的 S7Comm，以及通过 Industrial Ethernet 网络的 S7Comm（一个标记集）：
  `"S7$Program";1;"IP-Address=192.168.2.21;Port=102;Rack=0;Slot=2"`
  `"S7$Program";2;"MAC=00:01:02:03:04:05;Rack=0;Slot=2"`

标头字符串后面是文件正文，其中包含参数值（连接 ID、应用程序层协议代码、设备的完整网络地址）。

示例 connections.csv 文件

```
'Connections
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;Protocol;Address
"ms_plc";3;"IP-Address=192.168.2.77;Port=1025"
"mc_SysQ";7;"IP-Address=192.168.2.77;Port=2404;Asdu=555"
```

在 connections.csv 文件中，设备的网络地址格式取决于所使用的协议类型。

示例：
可以为 Kaspersky Industrial CyberSecurity for Networks 支持的协议使用以下地址格式：

- MODBUS TCP：
  `"IP-Address=192.168.2.7;Port=502"`
- SIEMENS S7COMM over TCP：
  `"IP-Address=192.168.2.7;Port=502;Rack=0;Slot=2"`
- SIEMENS S7COMM over INDUSTRIAL ETHERNET：
  `"MAC=00:01:02:03:04:05;Rack=0;Slot=2"`
- MITSUBISHI MELSEC SYSTEM Q：
  `"IP-Address=192.168.2.7;Port=502;Network=0;Station=0;PC=255"`
- ALLEN-BRADLEY ETHERNET/IP：
  `"IP-Address=192.168.2.7;Port=44818"`
- IEC 61850 MMS：
  `"IP-Address=192.168.2.7;Port=502;Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`
- IEC 61850 GOOSE：
  `"Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`
- IEC 60870-5-104：
  `"IP-Address=192.168.2.7;Port=104;Asdu=2"`
- GENERAL ELECTRIC SRTP：
  `"IP-Address=192.168.2.50;Port=18245"`
- IEC 61850 SAMPLED VALUES：
  `"MAC=00:01:02:03:04:05;Domains=IED_TRANSFORMER1;Vendor=TMW;Model=IED"`
- SIEMENS S7COMMPLUS over TCP：
  `"IP-Address=192.168.2.22;Port=102"`
- EMERSON DELTAV：
  `"IP-Address=192.168.2.38;Port=18507"`
- OMRON FINS over UDP：
  `"IP-Address=192.168.2.1;Port=9600"`
- MMS for ABB AC 800M：
  `"IP-Address=192.168.2.60;Port=102"`
- YOKOGAWA VNET/IP：
  `"IP-Address=192.168.2.4;Port=5313"`

- CODESYS V3 GATEWAY over TCP:
  `"IP-Address=192.168.2.4;Port=11740"`
- DNP3:
  `"IP-Address=192.168.2.10;Port=20000"`
- OMRON FINS over TCP:
  `"IP-Address=192.168.2.1;Port=9600"`
- OPC UA BINARY:
  `"IP-Address=192.168.2.213;Port=49320"`
- DMS for ABB AC 700F:
  `"IP-Address=192.168.2.7;Port=9991"`
- OMRON FINS over ETHERNET/IP:
  `"IP-Address=192.168.2.1;Port=44818"`
- OPC DA:
  `"IP-Address=192.168.2.7;Port=135"`
- WMI INTERACTION:
  `"IP-Address=192.168.2.7;Port=135"`
- CODESYS V3 GATEWAY over UDP:
  `"IP-Address=192.168.2.7;Port=1740"`
- BECKHOFF ADS/AMS:
  `"IP-Address=192.168.2.7;Port=48898"`
- IEC 60870-5-101:
  `"IP-Address=192.168.2.7;Port=950"`
- FOXBORO FCP270, FCP280 INTERACTION:
  `"MAC=00:01:02:03:04:05"`
- BSAP:
  `"IP-Address=192.168.2.7;Port=1234"`
- HONEYWELL CONTROLEDGE 900 INTERACTION:
  `"IP-Address=192.168.2.99;Port=41103"`
- HONEYWELL EXPERION INTERACTION:
  `"IP-Address=192.168.2.10;Port=55553"`
- SCHNEIDER ELECTRIC UMAS:
  `"IP-Address=192.168.2.7;Port=502"`

- TASE.2 :
  `"IP-Address=192.168.2.20;Port=102"`
- PROFINET IO :
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.2.20\;Frame=IDS_TEL352"`
- DIRECTLOGIC INTERACTION :
  `"IP-Address=192.168.2.70;Port=28784"`
- BACNET :
  `"IP-Address=192.168.2.200;Port=47808"`
- YARD :
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.2.1\;Port=2002"`
- COS :
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.2.131\;Port=3077"`
- IPU-FEU INTERACTION :
  `"IP-Address=192.168.2.200;Port=57005"`
- VALMET DNA INTERACTION :
  `"IP-Address=192.168.2.11;Port=2519"`
- CODESYS V2 :
  `"IP-Address=192.168.2.200;Port=1210"`
- PNU20 :
  `"IP-Address=192.168.2.200;Port=43962"`
- GENERAL ELECTRIC EGD :
  `"IP-Address=192.168.2.51;Port=18246"`
- KNXnet/IP :
  `"IP-Address=192.168.2.76;Port=3671"`
- DTS :
  `"IP-Address=192.168.2.11;Port=30000"`
- INA2000 :
  `"IP-Address=192.168.2.1;Port=11159"`
- SIEMENS SICAM SCC - INTERACTION with SICAM PAS :
  `"IP-Address=192.168.2.1;Port=10501"`
- TELNET :
  `"IP-Address=192.168.2.250;Port=23"`

- VNIIA：
  `"MAC=00:01:02:03:04:05"`

- CHINT MAS400：
  `"IP-Address=192.168.2.50;Port=46286"`

- CHINT MAS9600：
  `"IP-Address=192.168.2.50;Port=46286"`

- ISaGRAF IXL：
  `"IP-Address=192.168.2.50;Port=1131"`

- ISaGRAF SNCP：
  `"IP-Address=192.168.2.50;Port=1132"`

包含标记和变量描述的文件：variables.csv

变量和标记描述文件列出了标记、标记参数以及与标记关联的连接。

该文件应以标头字符串开头，标头字符串包含处理文件所需的数据。

variables.csv 文件的示例标头字符串

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
```

前三个标头字符串与devices.csv文件中的标头字符串相同。

字符串
`ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;E`
包含数据列的名称：

- `ID` – 标记的唯一数字 ID。
  需要标记 ID 来创建指向datasets.csv文件中的标记的链接。

- `Varname` – 标记的完整名称（例如，`Drain.8450PT00058.value20`）。

- `Connection` – 与标记关联的连接的 ID。
  连接 ID 在连接描述文件中指定，用于将协议链接到标记。

- `Address` – 标记的地址（采用字符串格式）。
  该地址取决于与标记关联的协议的类型（例如，对于 S7comm 协议，地址值为“`M2.7`, `DB575:82.0`”，对于 Modbus TCP 协议，地址值为“`400537`, `123`, `300001`”）。

- `Datatype` – 标记数据类型的数字代码。可使用以下代码：
  - 0 – BOOL
  - 1 – INT8
  - 2 – UINT8
  - 3 – INT16
  - 4 – UINT16
  - 5 – INT32
  - 6 – UINT32
  - 7 – INT64
  - 8 – UINT64
  - 9 – FLOAT
  - 10 – DOUBLE
  - 11 – STRING
  - 12 – ENUM
  - 13 – BOOL ARRAY
  - 14 – 未指定
- `Length` – 字符串类型的标记的字符串长度（以字节为单位）。
- `InLo;InHi;OutLo;OutHi` – 用于缩放标记值的参数。

  如果用于缩放标记值的所有参数的值均等于零，则不适用缩放标记值功能。如果为参数指定了数字值，则使用以下公式来计算标记值：TagValue = OutLo + (TagValue – InLo) * (OutHi – OutLo) / (InHi – InLo)，其中 TagValue 为标记值。
- `Description` – 标记描述（例如，“1 号锅炉出口的蒸汽压力”）。
- `EngUnits` – 与标记对应的物理量的度量单位（例如，m/s、J）。
- `EnumName` – 来自 enums.csv 文件的枚举名称，它定义标记的值。

  可以为具有 ENUM、INT* 或 UINT* 数据类型的标记填写“`EnumName`”字段。“`EnumName`”字段包含指向 enums.csv 文件中的枚举的链接。

  variables.csv 文件中的“EnumName”字段

  ```
  EnumName = "OnOffSwitch"
  ```

  enums.csv 文件中的枚举描述

  ```
  "OnOffSwitch"; 0; "On"
  "OnOffSwitch"; 1; "Off"
  ```

标头字符串后面是文件正文，其中包含参数值（例如，标记 ID、标记名称、连接 ID）。

示例 variables.csv 文件

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
5;"System.mitsub_n.ms_plc.Bit01";"ms_plc";"W0";4;0;0;0;0;0;"System.mitsub_n.ms_plc.Bit01";"";""
6;"System.mitsub_n.ms_plc.Register01";"ms_plc";"W20";9;0;0;0;0;0;"System.mitsub_n.ms_plc.Register01";"";""
1;"systemQ.Bit01";"mc_SysQ";"10";0;0;0;0;0;0;"systemQ.Bit01";"";""
```

“`Address`”字段中的标记地址结构取决于所使用的协议。

对于支持的协议，可使用以下地址结构：

- MODBUS TCP：整数（例如，离散输入的地址：从 100001 开始）。
- SIEMENS S7COMM over TCP 和 S7COMM over INDUSTRIAL ETHERNET：格式为`[Area][ByteAddress].[BitAddress]` 的的字符串。

  如果满足条件 `MemArea=DataBlocks`，则将为地址增加数据块编号。字符串更改为 `[DB17]:[ByteAddress].[BitAddress]`，其中：

  - `Area` – 根据协议标准对内存区域代码的枚举：M、I、O、DB、C、T。
  - `ByteAddress` – 采用整数表示的字节地址。
  - `BitAddress` – 字节内的位地址，用整数表示。
- MITSUBISHI MELSEC SYSTEM Q：格式为`[Area][Address]`的字符串，其中：
  - `Area`– 根据协议规范对内存区域代码的枚举：SM、SD、M、L、F、V、D、TS、TC、TN、SS、SC、SN、CS、CC、CN、S、Z、R、X、Y、B、W、SB、SW、DX、DY、ZR。
  - `Address` – 地址值。该地址是一个介于与数据区域相应的范围内的整数。
- ALLEN-BRADLEY ETHERNET/IP：带有标记名称的字符串。
- IEC 61850 MMS 和 GOOSE：依照 IEC 61850 标准 – `DOMAIN=Domain;LN=LnName;CO=CoName;DA=FullTagName;CDC=CdcName;LNCDC=LNClassName` 格式的字符串，其中：
  - `DOMAIN` – 包含设备名称和逻辑设备名称的参数。
  - `LN` – 逻辑节点名称。
  - `CO` – 功能约束名称。
  - `DA` – 标记名称。
  - `CDC` – 属性公共数据类名称。
  - `LNCDC` – 逻辑节点公共数据类名称。

- IEC 60870-5-104 和 IEC 60870-5-101：格式为`[ASDU]:[Address]`的的字符串，其中：
  - `ASDU` — 用整数表示的 ASDU 编号。
  - `Address`– 用整数表示的 InformationObject 编号。
- GENERAL ELECTRIC SRTP：格式为`[Area][ByteAddress].[BitAddress]`的的字符串，其中：
  - `Area`– 根据协议标准对内存区域代码的枚举：I、Q、T、M、G、AI、AQ、R、P、L、W。
  - `ByteAddress` – 采用整数表示的字节地址。
  - `BitAddress` – 字节内的位地址，用整数表示。
- SIEMENS S7COMMPLUS over TCP：格式为`LID=LidValue;RID=RidValue`的的字符串，其中`LidValue`和`RidValue`是 TiaPortal 项目中标记的内部标识符。
- EMERSON DELTAV：包含标记名称的字符串。
- OMRON FINS over UDP、OMRON FINS over TCP 和 OMRON FINS over ETHERNET/IP：格式为`[Area][ByteAddress].[BitAddress]`的的字符串，其中：
  - `Area`– 根据协议标准对内存区域代码的枚举：A、CIO、C、CS、D、DR、E、H、IR、TK、T、TS、W。
  - `ByteAddress` – 采用整数表示的字节地址。
  - `BitAddress` – 字节内的位地址，用整数表示。
- YOKOGAWA VNET/IP：带有标记名称的字符串。
- DNP3：格式为`[GROUP]:[INDEX]`的的字符串，其中：
  - `GROUP`是特定群组。
  - `INDEX`是特定索引。
- DMS for ABB AC 700F：整数。
- MMS for ABB AC 800M：格式为`[Application]:[POUInstance].[VarOffset]`的字符串，其中：
  - `Application`是应用程序的名称。
  - `POUInstance`是 POU 实例。
  - `VarOffset`是变量偏移量。
- CODESYS V3 GATEWAY over TCP 和 CODESYS V3 GATEWAY over UDP：带有标记名称的字符串。
- OPC UA BINARY：带有标记名称的字符串。
- OPC DA：包含标记名称的字符串。

- BSAP：格式为`[MSD_VERSION]:[MSD]`的字符串，其中：
  - `MSD_VERSION`是一个范围在 0–65535 之间的整数，用于比较 PLC 和 SCADA 系统中的项目/标记的版本。
  - `MSD`是标记 ID，用 0~65535 范围内的整数表示。
- FOXBORO FCP280 / FCP270 INTERACTION：包含标记名称的字符串。
- HONEYWELL EXPERION INTERACTION：字符串格式为`[EEC_ID]:[IOC_ID]:[DOC_ID]:[PC_ID]`，其中：
  - `EEC_ID`是 PLC 程序中运行时环境的 ID（执行环境代码），用 0-65535 范围内的整数表示。
  - `IOC_ID`是 PLC 程序中 I/O 模块的 ID（输入和输出代码），用 0-65535 范围内的整数表示。
  - `DOC_ID`是 PLC 程序中子块的 ID（相关对象代码），用 0-65535 范围内的整数表示。
  - `PC_ID`是 PLC 程序中块参数的 ID（属性代码），用 0-65535 范围内的整数表示。
- DIRECTLOGIC INTERACTION：格式为`[Area][ByteAddress].[BitAddress]`的的字符串，其中：
  - `Area`是根据协议规范对内存区域代码的枚举：X，Y，C，S，T，CT，GX，GY，V，P，SP，B，PB。
  - `ByteAddress` – 采用整数表示的字节地址。
  - `BitAddress` – 字节内的位地址，用整数表示。
- BACNET：格式为`[OBJECT_TYPE]:[OBJECT_ID]`的的字符串，其中：
  - `OBJECT_TYPE`是根据协议规范的对象类型。
  - `OBJECT_ID`是对象的序列号，用 0–4194303 范围内的整数表示。
- PROFINET IO：格式为`[IO]:[SubSlot]:[Index]:[Offset].[BitAddress]`的字符串，其中：
  - `IO`是变量方向（输入，输出）。
  - `SubSlot`是用整数表示的子槽编号。
  - `Index`是用整数表示的标记索引。
  - `Offset` – 采用整数表示的标记字节。
  - `BitAddress`是字节内的位地址，用整数表示（仅用于具有 bool 数据类型的标记）。

  此外，为了正确加载协议参数，必须为特定设备指定 GSDML 文件。
- YARD：格式为`[Controller Address]:[Index]:[Size]:[Config]:[MessageType]`的的字符串，其中：
  - `Controller Address` – 用十六进制整数表示的对象控制器的地址。
  - `Index` – 用整数表示的位标记索引。
  - `Size` – 用整数表示的位大小。

- `Config` – 对象控制器上的跳线位置，以十六进制整数表示。
- `MessageType` – 消息类型（`Order` 或 `Status`）。

另外，为了正确加载协议参数，您可能需要为特定设备指定配置文件。

- COS：格式为 `[Object ID]:[Variable ID]` 的字符串，其中：
  - `Object ID` – 用整数表示的对象标识符。
  - `Variable ID` – 用整数表示的变量标识符。

  此外，为了正确加载协议参数，必须指定站的配置文件。文件名必须是“specific.zip”。
- VALMET DNA INTERACTION：包含标记名称的字符串。
  此外，为了正确加载协议参数，您必须指定包含 PLC 启动日志的文件。文件名必须是“specific.zip”。
- PNU20：0–65535 范围内的整数。
- GENERAL ELECTRIC EGD：格式为 `[ExchangeId]:[RefAddress]` 的的字符串，其中：
  - `ExchangeId` – 订阅 ID，用 0–4294967295 范围内的整数表示。
  - `RefAddress` – 标记地址偏移量（以字节为单位），用 0-65535 范围内的整数表示。
- KNXnet/IP：0-65535 范围内的整数。
- SIEMENS SICAM SCC - 与 SICAM PAS 交互：0-65535 范围内的整数。
- CHINT MAS400：0–4294967295 之间的整数。
- CHINT MAS9600：0-4294967295 之间的整数。
- ISaGRAF IXL：正整数。
- ISaGRAF SNCP：正整数。

包含枚举描述的文件：enums.csv

枚举描述文件包含当前数据文件集中使用的 IEC 61850 标准的所有枚举的所有元素。

该文件应以标头字符串开头，标头字符串包含处理文件所需的数据。

`enums.csv` 文件的示例标头字符串

```
'Enums
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;EnumName;IntValue;TextValue
```

前三个标头字符串与devices.csv文件中的标头字符串相同。

字符串 `Connection;EnumName;IntValue;TextValue` 包含数据列的名称：

- `Connection` – 该元素所属的连接的 ID。
- `EnumName` – 枚举的名称。
- `IntValue` – 枚举的数字值。
- `TextValue` – 与枚举的数字值对应的文本描述。

标头字符串后面是文件正文，其中包含参数值（连接 ID、枚举的名称、枚举的数字值、文本描述）。

示例 enums.csv 文件

```
'Enums
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;EnumName;IntValue;TextValue
"AA1J1Q01A2";"Beh";1;"on"
"AA1J1Q01A2";"Beh";2;"blocked"
"AA1J1Q01A2";"Beh";3;"test"
"AA1J1Q01A2";"Beh";4;"test/blocked"
"AA1J1Q01A2";"Beh";5;"off"
```

包含数据集（标记集）描述的文件：datasets.csv

包含数据集描述文件（标记集）包含 IEC 61850 标准协议的数据集参数。

该文件应以标头字符串开头，标头字符串包含处理文件所需的数据。

datasets.csv 文件的示例标头字符串

```
'Datasets
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;DatasetName;Deprecated;ItemName
```

前三个标头字符串与devices.csv文件中的标头字符串相同。

字符串 `Connection;DatasetName;Deprecated;ItemName` 包含数据列的名称：

- `Connection` – datasets.csv 文件所属的连接的 ID。
- `DatasetName` – 数据集的名称。
- `Deprecated` – 未使用的数据（零值）。
- `ItemName` – 设备型号元素的全名。这可以是标记的最终名称或树顶部分支的名称。

标头字符串后面是包含参数值（连接 ID、数据集名称、未使用的值和设备型号元素的名称）的文件正文。

示例 datasets.csv 文件

```
'Datasets
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;DatasetName;Deprecated;ItemName
```

```
"S7UTDZD";"S7UTDZDPROT/LLN0$DataSet";0;"S7UTDZDPROT/PTRC1$ST$Tr"
"S7UTDZD";"S7UTDZDPROT/LLN0$DataSet";0;"S7UTDZDMEAS/M1_MMXU1$MX$A$phsA"
```

包含 MMS 协议报告描述的文件：iec61850_mms_reports.csv

带有 MMS 协议报告描述的文件包含 IEC 61850：MMS 协议的报告服务的参数。

该文件应以标头字符串开头，标头字符串包含处理文件所需的数据。

iec61850_mms_reports.csv 文件的示例标头字符串

```
报告
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
```

前三个标头字符串与devices.csv文件中的标头字符串相同。

字符串 `Connection;ReportName;ReportId;DataSetName;IsBuffered` 包含数据列的名称：

- `Connection` – 与文件 iec61850_mms_reports.csv 中的设置字符串关联的连接的 ID。
- `ReportName` – 报告的名称。
- `ReportId` – 报告的 ID。
- `DataSetName` – 与此报告相关的数据集的名称。
- `IsBuffered` – 指示报告是否得到缓冲。它采用 *已缓冲* 或 *未缓冲* 值。

标题字符串后面是包含参数值（连接 ID、报告名称、报告 ID、报告的数据集名称和缓冲区指示符）的文件正文。

iec61850_mms_reports.csv 文件示例

```
报告
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: .Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
"IED24151LD";"IED24151LD/LLN0$BR$brcbST01";"brcbST01";"IED24151LD/LLN0$DSList";"Buffered"
"IED24151LD";"IED24151LD/LLN0$RP$urcbMX01";"urcbMX01";"IED24151LD/LLN0$MXList";"Unbuffered"
```

Kaspersky Industrial CyberSecurity for Networks 中的系统事件类型

在 Kaspersky Industrial CyberSecurity for Networks 中，使用在应用程序安装期间自动创建的系统事件类型来注册事件。

每种事件类型都对应一种特定的事件注册技术。

基于深度数据包检测技术的系统事件类型

本文提供与深度数据包检测技术相关的系统事件类型的描述（请参见下表）。

基于深度数据包检测技术 (DPI) 的系统事件类型

代码	事件类型的标题	报名条件
4000002900	$technology_rule	过程控制规则已触发。 系统事件类型的标题和描述中使用了以下变量： • $technology_rule – 规则的名称。 • $tags – 接收的规则中定义其条件的标签的值。 触发的过程控制规则中指定的用户定义设置用于已注册事件的标题、描述和评分。
4000000001	测试事件 (DPI)	检测到测试网络数据包。

基于命令控制技术的系统事件类型

本文提供与命令控制技术相关的系统事件类型的描述（请参见下表）。

基于命令控制技术 (CC) 的系统事件类型

代码	事件类型的标题	报名条件
4000002602	$systemCommandShort	检测到受监控的系统命令（并且没有为该系统命令启用交互控制规则）。 事件类型的标题和描述中使用了以下变量： • $systemCommandShort – 检测到的系统命令的简要描述。 • $systemCommandFull – 检测到的系统命令的详细描述。 • $attackTechniques – MITRE ATT&CK 知识库中列出的可能技术，网络犯罪分子可使用这些技术使用此系统命令进行攻击。

基于资产管理技术的系统事件类型

本文提供与资产管理技术相关的系统事件类型的描述（请参见下表）。

基于资产管理技术 (AM) 的系统事件类型

代码	事件类型的标题	报名条件
4000005003	检测到地址为 ' + $owner_ip_or_mac + ' 的新设备'	资产管理监控模式会根据检测到的 IP 地址或 MAC 地址自动添加新设备，而该地址尚未为表中的其他设备指定。 应用程序在注册该事件的时候，可能会同时为该设备注册名为“**未授权的设备**”风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备的指定名称。 • $assigned_mac – 分配的 MAC 地址（如果已定义） • $owner_ip – 分配的 IP 地址（如果已定义） • $asset_id – 设备的 ID。
4000005004	收到关于地址为 ' + $owner_ip_or_mac + ' 的设备的新信息'	资产管理监控模式根据从流量获得的数据自动更新设备信息。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称。 • $updated_params – 更新信息列表 • $asset_id – 设备的 ID。

代码	事件类型的标题	报名条件
4000005005	检测到 IP 地址 $owner_ip 冲突	在资产管理监控模式下，应用程序检测到另一个设备正在使用与指定该 IP 地址的设备不同的 IP 地址。 事件类型的标题和描述中使用了以下变量： • $owner_ip – IP 地址 • $challenger_asset_name – 使用该 IP 地址的设备名称 • $challenger_mac – 使用该 IP 地址的设备的 MAC 地址 • $asset_name – 在其设置中指定了该 IP 地址的设备的名称 • $owner_mac – 在其设置中指定了该 IP 地址的设备的 MAC 地址 • $challenger_ips_list：使用该 IP 地址的设备的其他 IP 地址列表 • $asset_id – 在其设置中指定了该 IP 地址的设备的 ID • $challenger_id – 使用该 IP 地址的设备的 ID
4000005006	检测到来自地址 $owner_ip_or_mac 的流量，该地址被分配给具有"已存档"状态的设备	在资产管理监控模式下，或根据从 EPP 应用程序接收的数据，检测到分配了"*已存档*"状态的设备的活动。 应用程序在注册该事件的时候，可能会同时为该设备注册名为"**未授权的设备**"风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称。 • $last_seen_timestamp – 设备最后一次出现在网络中的日期和时间 • $asset_id – 设备的 ID。
4000005007	检测到 MAC 地址为 $owner_mac 的设备的新 IP 地址 $new_ip_addr	在资产管理监控模式下，检测到设备使用的新 IP 地址。 事件类型的标题和描述中使用了以下变量： • $new_ip_addr – 检测到的 IP 地址 • $owner_mac – 设备的 MAC 地址 • $asset_name – 设备名称。 • $owner_ips_list – 设备的其他 IP 地址列表 • $asset_id – 设备的 ID。
4000005008	MAC 地址 $owner_mac 被添加到 IP 地址为 $owner_ip 的设备	资产管理监控模式导致为仅指定了 IP 地址的网络接口自动添加 MAC 地址（设备状态为 *未授权*或*已存档*）。 事件类型的标题和描述中使用了以下变量： • $owner_mac – 检测到的设备的 MAC 地址 • $owner_ip – 设备的 IP 地址 • $asset_name – 设备名称。 • $asset_id – 设备的 ID。
4000005009	IP 地址 $owner_ip 被添加到 MAC 地址为 $owner_mac 的设备	资产管理监控模式导致为仅指定了 MAC 地址的网络接口自动添加 IP 地址（设备状态为 *未授权*或*已存档*）。 事件类型的标题和描述中使用了以下变量： • $owner_ip – 检测到的设备的 IP 地址 • $owner_mac – 设备的 MAC 地址 • $asset_name – 设备名称。 • $asset_id – 设备的 ID。
4000005010	检测到 IP 地址为 $owner_ip 的设备的新 MAC 地址 $new_mac_addr	在资产管理监控模式下，检测到设备使用的新 MAC 地址。 事件类型的标题和描述中使用了以下变量： • $new_mac_addr – 检测到的 MAC 地址 • $owner_ip – 设备的 IP 地址 • $asset_name – 设备名称。 • $asset_id – 设备的 ID。
4000005011	在从 EPP 应用程序接收到的设备信息中检测到 MAC 地址 $owner_mac 更改为 $challenger_mac	已根据从 EPP 应用程序接收的数据更新了设备的 MAC 地址。 事件类型的标题和描述中使用了以下变量： • $owner_mac – 设备的旧 MAC 地址 • $challenger_mac – 设备的新 MAC 地址 • $asset_name – 设备名称。 • $asset_id – 设备的 ID。
4000005012	在从 EPP 应用程序接收的数据中发现设备 $asset_name 的新地址信息	在从 EPP 应用程序接收的数据中检测到设备的新地址信息。如果设备地址信息的更改未被应用程序处理为代码为 4000005009 或 4000005010 的事件，则会注册此类事件。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $detected_epp_addresses – 地址信息 • $asset_id – 设备的 ID。

代码	事件类型的标题	报名条件
4000005013	从 EPP 应用程序接收数据后，在设备 $conflicted_epp_assets 的地址中检测到冲突	根据从 EPP 应用程序接收的数据，检测到 Kaspersky Industrial CyberSecurity for Networks 中多个设备的地址存在冲突。根据来自 EPP 应用程序的数据，这些地址属于同一设备。 事件类型的标题和描述中使用了以下变量： • $conflicted_epp_assets – 检测到具有冲突地址的设备 • $unaccepted_epp_addresses – 属于同一设备的地址。
4000005014	根据来自 EPP 应用程序的数据添加了子网 $subnet_mask	从 EPP 应用程序接收数据后，新子网会自动添加到已知子网列表中。该子网被添加到一个地址空间，其中数据源可以是从 EPP 应用程序接收数据的集成服务器。如果有多个可用的地址空间，应用程序将选择包含最合适子网的地址空间来自动添加新的嵌套子网。 事件类型的标题和描述中使用了以下变量： • $subnet_mask – 子网地址 • $subnet_type – 子网类型
4000005015	检测到具有以下地址的设备发生部件变化：$owner_ip_or_mac	根据从 EPP 应用程序接收的数据，使用部件监控功能更新了设备部件信息。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID。 • $added_asset_hardware – 已添加的部件列表 • $modified_asset_hardware – 已修改的部件列表 • $removed_asset_hardware – 已删除的部件列表
4000005200	PLC 项目控制：检测到从 PLC $asset_name 读取未知块	PLC 项目控制读/写监控导致检测到从 PLC 读取了项目的未知块（如果没有保存有关此块的信息）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**从 PLC 读取未知项目块**的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $block_name – 数据块的名称 • $saved_date_time – 检测到操作的日期和时间
4000005201	PLC 项目控制：检测到从 PLC $asset_name 读取已知块	PLC 项目控制读/写监控导致检测到从 PLC 读取了项目的已知块（如果保存了有关此块的信息，但收到的信息与有关此块的最新保存的信息不匹配）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**从 PLC 读取已知项目块**”的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $block_name – 数据块的名称 • $saved_date_time – 在应用程序中保存块的日期和时间
4000005202	PLC 项目控制：检测到向 PLC $asset_name 写入新数据块	PLC 项目控制读/写监控导致检测到从 PLC 写入了项目的未知块（如果没有保存有关此块的信息）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**将新项目块写入 PLC**的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $block_name – 数据块的名称 • $saved_date_time – 检测到操作的日期和时间
4000005203	PLC 项目控制：检测到向 PLC $asset_name 写入已知块	PLC 项目控制读/写监控导致检测到从 PLC 写入了项目的已知块（如果保存了有关此块的信息，但收到的信息与有关此块的最新保存的信息不匹配）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**将已知项目块写入 PLC**的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $block_name – 数据块的名称 • $saved_date_time – 在应用程序中保存块的日期和时间
4000005204	PLC 项目控制：检测到从 PLC $asset_name 读取未知项目	PLC 项目控制读/写监控导致检测到从 PLC 读取了未知项目（如果没有保存有关此项目的信息）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**从 PLC 读取未知项目**的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $saved_date_time – 检测到操作的日期和时间

代码	事件类型的标题	报名条件
4000005205	PLC 项目控制：检测到从 PLC $asset_name 读取已知项目	PLC 项目控制读/写监控导致检测到从 PLC 读取已知项目（如果已保存有关该项目的信息，但收到的信息与有关该项目的最新保存的信息不匹配）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**从 PLC 读取已知项目**”的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $saved_date_time – 应用程序中保存项目的日期和时间
4000005206	PLC 项目控制：检测到向 PLC $asset_name 写入新项目	PLC 项目控制读/写监控导致检测到将新项目写入 PLC（如果没有保存有关此项目的信息）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**将新项目写入 PLC**的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $saved_date_time – 检测到操作的日期和时间
4000005207	PLC 项目控制：检测到向 PLC $asset_name 写入已知项目	PLC 项目控制读/写监控导致检测到将已知项目写入 PLC（如果已保存有关该项目的信息，但收到的信息与有关该项目的最新保存的信息不匹配）。 在注册该事件的时候，应用程序可能会同时为该设备注册名为“**将已知项目写入 PLC**的风险。在这种情况下，风险与事件相关。 事件类型的标题和描述中使用了以下变量： • $asset_name – 设备名称。 • $saved_date_time – 应用程序中保存项目的日期和时间
4000005600	检测到地址为 $owner_ip_or_mac 的设备上的用户列表发生变化	在设备上控制用户时检测到用户信息发生变化。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_users – 已添加的用户列表 • $modified_asset_users – 修改的用户列表 • $removed_asset_users – 已删除的用户列表
4000005601	在地址为 $owner_ip_or_mac 的设备上的应用程序列表中检测到更改	在监控设备上的应用程序和补丁时检测到有关设备上应用程序的信息被修改。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_apps – 已添加的应用程序列表 • $removed_asset_apps – 已删除的应用程序列表
4000005602	在地址为 $owner_ip_or_mac 的设备上检测到补丁列表中的更改	在监控设备上的应用程序和补丁时检测到设备补丁信息被修改。 事件类型的标题和描述中使用了以下变量： • $owner_ip_or_mac – 设备的 IP 或 MAC 地址 • $asset_name – 设备名称 • $asset_id – 设备的 ID • $added_asset_patches – 已添加补丁的列表 • $removed_asset_patches – 已删除补丁的列表
4000005603	在设备上的配置类型 $inventory_loc_key 中检测到更改	在监控设备配置时，根据设备扫描结果与以前的配置进行比较时检测到配置类型中的更改（对于在“**仅更新**”和/或“**存档版本**”配置处理模式下运行的作业）。 事件类型的标题和描述中使用了以下变量： • $inventory_loc_key – 配置类型的名称 • $device_config_inventory_changed_format – 在配置类型中检测到的更改
4000005604	检测到与设备上的黄金配置 $inventory_loc_key 存在差异	在监控设备配置时，根据设备扫描结果发现与黄金配置相比存在差异（对于在“**与黄金配置进行比较**”处理模式下运行的作业）。 事件类型的标题和描述中使用了以下变量： • $inventory_loc_key – 配置类型的名称 • $device_config_diverged_format – 与黄金配置相比检测到的差异

代码	事件类型的标题	报名条件
4000005700	远程连接到设备时检测到公钥不匹配	在扫描或主动轮询设备时，检测到接收到的设备公钥与应用程序中存储的值不匹配。该程序已取消对该设备的扫描或主动轮询。 事件类型描述中使用以下变量： • $asset_name – 设备名称 • $new_asset_sshpublickey – 收到的公钥 • $old_asset_sshpublickey – 存储的公钥
4000000004	测试事件 (AM)	检测到测试网络数据包（启用了设备活动检测方法）。

基于网络完整性控制技术的系统事件类型

本文提供与网络完整性控制技术相关的系统事件类型的描述（请参见下表）。

基于网络完整性控制技术 (NIC) 的系统事件类型

代码	事件类型的标题	报名条件
4000002601	检测到未经授权的网络交互 ($top_level_protocol)	检测到未在已启用的交互控制规则中指定的网络交互。 事件类型的标题和描述中使用了以下变量： • $top_level_protocol – 顶级协议的名称。 • $protocol – 应用程序层协议的名称。
4000002700	监控点 ' + $monitoringPoint + ' 无流量'	链接到监控点的网络接口已超过 15 秒没有收到流量。 事件类型的标题和描述中使用了以下变量： • $monitoringPoint – 监测点名称。 • $interface – 链接到监控点的网络接口的名称。 • $duration – 没有流量的时间段（以秒为单位）。
4000000002	测试事件(NIC)	检测到测试网络数据包（当启用网络完整性控制时）。

基于入侵检测技术的系统事件类型

本文提供与入侵检测技术相关的系统事件类型的描述（请参见下表）。

基于入侵检测 (IDS) 技术的系统事件类型

代码	事件类型的标题	报名条件
4000002701	检测到 TCP 协议异常: 重叠 TCP 段中的内容替换	检测到 TCP 协议异常：数据包包含内容各异的重叠 TCP 段。
4000003000	来自 ' + $fileName + ' 集（系统规则集）的规则被触发	来自系统规则集的入侵检测规则被触发。 事件类型的标题和描述中使用了以下变量： • $fileName – 规则集的名称。 • $category – 规则的类别。 • $ruleName – 规则的名称。 • $signature_id – 规则 ID (sid)。
4000003001	来自 ' + $fileName + ' 集（用户自定义规则集）的规则被触发。	来自用户自定义规则集中的入侵检测规则被触发。 事件类型的标题和描述中使用了以下变量： • $fileName – 规则集的名称。 • $category – 规则的类别。 • $ruleName – 规则的名称。 • $signature_id – 规则 ID (sid)。 • $action – 要对规则中定义的网络数据包执行的操作类型（Kaspersky Industrial CyberSecurity for Networks 不执行 丢弃 或 拒绝 操作）。
4000003002	检测到暴力攻击或扫描的迹象	用于检测扫描或暴力攻击的规则被触发。 在事件类型描述中，$ruleName 变量用于规则名称。

代码	事件类型的标题	报名条件
4000003003	网络异常检测规则被触发	网络异常检测规则被触发。 当事件被注册时，事件会收到来自网络异常检测规则的标题、分数和描述。
4000004001	在 ARP 回复中检测到 ARP 欺骗的症状	检测到 ARP 数据包中存在伪造地址的迹象：多个与 ARP 请求无关的 ARP 回复。 事件类型描述中使用以下变量： • $senderIp – 替换的 IP 地址。 • $targetIp – 目标节点的 IP 地址。 • $attackStartTimestamp – 检测到第一个 ARP 回复的时间。
4000004002	在 ARP 请求中检测到 ARP 欺骗的症状	检测到 ARP 数据包中存在伪造地址的迹象：从同一 MAC 地址向不同目的地发出的多个 ARP 请求。 事件类型描述中使用以下变量： • $senderIp – 替换的 IP 地址。 • $targetIp – 目标节点的 IP 地址。 • $attackStartTimestamp – 检测到第一个 ARP 回复的时间。
4000005100	检测到 IP 协议异常: 组装 IP 数据包时发生数据冲突	检测到 IP 协议异常：覆盖 IP 数据包片段时数据不匹配。
4000005101	检测到 IP 协议异常: 超过碎片 IP 数据包大小	检测到 IP 协议异常：碎片 IP 数据包组装后的实际总大小超出了可接受的限制。
4000005102	检测到 IP 协议异常: IP 数据包的初始片段的大小小于预期	检测到 IP 协议异常：IP 数据包的初始片段的大小小于允许的最小值。
4000005103	检测到 IP 协议异常: 误相关片段	检测到 IP 协议异常：组装的 IP 数据包的片段包含与碎片数据包长度相冲突的数据。
4000000003	测试事件 (IDS)	检测到测试网络数据包（启用了基于规则的入侵检测）。

基于外部技术的系统事件类型

本文提供与外部技术相关的系统事件类型的描述（请参见下表）。

基于外部技术 (EXT) 的系统事件类型

代码	事件类型的标题	报名条件
8000000001	事件	检测到满足关联规则条件的事件序列。 当事件被注册时，事故会从关联规则中接收标题和描述。
4000005400	来自外部系统的事件	使用 Kaspersky Industrial CyberSecurity for Networks API 从外部系统接收到一个事件。 当注册事件时，标题和描述的内容由外部系统确定。

基于 Endpoint Protection Platform 的系统事件类型

本文提供与 Endpoint Protection Platform 技术相关的系统事件类型的描述（请参见下表）。

基于 Endpoint Protection Platform (EPP) 的系统事件类型

代码	事件类型的标题	报名条件
4000005500	特定于网络攻击的活动	集成服务器接收到指示 EPP 应用程序的网络威胁防护组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005501	连接不受信任的外部设备	集成服务器接收到指示 EPP 应用程序的设备控制组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005502	尝试运行未经授权或不受信任的应用程序	集成服务器接收到指示 EPP 应用程序的应用程序启动控制组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。

代码	事件类型的标题	报名条件
4000005503	指定监控范围中被禁止的文件操作	集成服务器接收到指示 EPP 应用程序的文件完整性监控组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005504	指定监控范围内的文件被修改	集成服务器接收到指示 EPP 应用程序的基线文件完整性监控组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005505	网络连接不被防火墙规则允许	集成服务器接收到指示 EPP 应用程序的防火墙管理组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005506	指定监视范围内的系统注册表修改	集成服务器接收到指示 EPP 应用程序的注册表访问监控组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005507	日志分析规则被触发	集成服务器接收到指示 EPP 应用程序的日志检查组件的规则被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005508	尝试利用受保护进程中的漏洞	集成服务器接收到指示 EPP 应用程序的漏洞利用防御组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005509	尝试恶意加密网络文件资源	集成服务器接收到指示 EPP 应用程序的反加密组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005510	尝试连接到 Wi-Fi 网络	集成服务器接收到指示 EPP 应用程序的 Wi-Fi 控制组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005511	PLC 项目与基线相比进行了修改	集成服务器接收到指示 EPP 应用程序的 PLC 项目完整性检查组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005512	检测到受感染或可能受感染的对象	集成服务器接收到指示 EPP 应用程序的实时文件保护组件被触发的数据。 事件类型描述使用变量 $epp_event_description 代表 EPP 应用程序中的数据。
4000005513	Sigma 规则 $sigmaAlertTitle 已触发	集成服务器收到有关触发端点代理组件 Sigma 规则的数据。 事件类型的标题和描述中使用了以下变量： • $sigmaAlertTitle – Sigma 规则名称 • $sigma_detection_type – 检测技术 • $sigma_object_type – 触发 Sigma 规则的对象类型 • $sigma_object_name – 触发 Sigma 规则的对象名称或第一个触发的 Sigma 规则的名称 • $sigma_status – 检测状态

Kaspersky Industrial CyberSecurity for Networks 中的系统命令类别

本文列出了 Kaspersky Industrial CyberSecurity for Networks 在分析工业网络流量时支持的系统命令类别（见下表）。

系统命令的类别

系统命令的类别	描述
连接	连接管理命令。
身份验证	身份验证命令。
操作模式更改	用于更改设备操作模式的命令。
下载程序	用于下载设备程序的命令。
上传程序	用于上传备程序的命令。
控制命令	智能电子设备（IED）协议的标准化命令。
修改程序	用于更改设备控制程序的命令。
报警信号管理	用于管理报警信号的命令。

系统命令的类别	描述
实时模式	用于在实时或调试模式下使用设备程序的命令。
修改标记	用于强制修改标记值的命令。
读取标记和数据	用于接收标记值、订阅标记和请求设备程序数据的命令。
更新固件	用于修改设备固件的命令。
读取设备配置	用于读取或请求设备信息的命令。
更改设备配置	用于修改设备设置的命令。
文件操作	用于管理设备的文件和目录的命令。
服务命令	用于维修设备的命令。
日期和时间管理	用于管理设备上的日期和时间的命令。
诊断消息	关于流量中的错误或不匹配数据的诊断消息。
通过 DCOM 进行交互	使用 DCOM 技术的协议的命令（例如，OPC DA）。
消息解析错误	分析消息时出错。
其他	未分配给其他特定类别的命令。

Kaspersky Industrial CyberSecurity for Networks 中使用地址空间的示例

地址空间（AS）使得 Kaspersky Industrial CyberSecurity for Networks 能够在具有相同地址的设备用于不同网段的情况下进行操作。本文提供了在不同网段中复制设备地址时为以下选项使用地址空间的示例：

- IP 地址重复
- MAC 地址重复
- MAC 地址的重复和使用相同范围的 IP 地址

用于复制设备 IP 地址的地址空间

本例考察了一家拥有 16 个工业现场的公司，这些现场有多组 PLC。每个工业站点使用相同范围的 IP 地址：10.4.0.0/16、10.5.0.0/16、10.8.0.0/16、10.9.0.0/16。这意味着不同站点的设备可能具有相同的 IP 地址。

工业站点的网段与主要企业网络完全隔离。每个段包含可操作 PLC、工程工作站和执行应用程序站功能的计算机（以下简称“应用程序站”计算机）。一个网段通过应用程序站计算机与主企业网络集成。这台计算机在主企业网络上有一个具有唯一 IP 地址的专用网络接口。

为了确保 Kaspersky Industrial CyberSecurity for Networks 在该配置中正常运行，必须为每个工业站点段添加以下对象：

- 段内流量接收监控点
- 从应用程序站计算机接收流量的监控点
- 包含一个规则的地址空间

例如，您可以为第一个段添加具有以下名称的对象：

- **MPoint_1-1**
- **MPoint_1-2**
- **Site_1**

下表描述了每个段的地址空间设置。

AS 用于具有相同 IP 地址的段

AS 名称	数据源	OSI 模型层	VLAN ID	IP 地址
Site_1	**监控点**： MPoint_1-1 MPoint_1-2	**网络 (L3)**	**任意或未使用**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_2	**监控点**： MPoint_2-1 MPoint_2-2	**网络 (L3)**	**任意或未使用**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_3	**监控点**： MPoint_3-1 MPoint_3-2	**网络 (L3)**	**任意或未使用**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
...				
Site_16	**监控点**： MPoint_16-1 MPoint_16-2	**网络 (L3)**	**任意或未使用**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16

用于复制设备 MAC 地址的地址空间

此示例检查使用 VLAN 技术的工业网络。该网络具有用于工业站点的两个专用段，通过 ID VLAN 3910 和 3915 进行区分。网段包含具有手动分配的 MAC 地址的设备（设备及其软件支持此功能）。这意味着不同网段中的设备可能具有相同的 MAC 地址。

为了确保 Kaspersky Industrial CyberSecurity for Networks 在这种配置中正常运行，必须为每个段添加一个地址空间。例如，可以将名称“**Site_1**”和“**Site_2**”分配给地址空间。地址空间每个可以包含一个规则。

下表描述了每个段的地址空间设置。

具有相同 MAC 寻址的段的 AS

AS 名称	数据源	OSI 模型层	VLAN ID	IP 地址
Site_1	**监控点**： **任意**	**数据链路 (L2)**	3910	**任何**
Site_2	**监控点**： **任意**	**数据链路 (L2)**	3915	**任何**

用于复制具有相同 IP 地址范围的设备的 MAC 地址的地址空间

此示例检查使用 VLAN 技术的工业网络。该网络具有用于工业站点的两个专用段，通过 ID VLAN 3910 和 3915 进行区分。网段包含具有手动分配的 MAC 地址的设备（设备及其软件支持此功能）。每个段中的 IP 地址都在相同的地址范围内：140.80.0.0/16。这意味着不同网段中的设备可以具有相同的 MAC 地址和/或相同的 IP 地址。

为了确保 Kaspersky Industrial CyberSecurity for Networks 在这种配置中正常运行，必须为每个段添加一个地址空间。例如，可以将名称“**Site_1**”和“**Site_2**”分配给地址空间。地址空间每个可以包含一个规则。

下表描述了每个段的地址空间设置。

AS，用于具有相同 MAC 地址和相同 IP 地址范围的段

AS 名称	数据源	OSI 模型层	VLAN ID	IP 地址
Site_1	**监控点**：**任意**	**数据链路和网络 (L2 和 L3)**	3910	140.80.0.0/16
Site_2	**监控点**：**任意**	**数据链路和网络 (L2 和 L3)**	3915	140.80.0.0/16

支持的通用协议

Kaspersky Industrial CyberSecurity for Networks 支持对 137 种通用协议进行流量监控。应用程序监控以下协议：

1. AeroAdmin over TCP
2. AFP
3. Ammyy Admin over TCP
4. AnyDesk over TCP
5. ARP
6. Bitcoin over TCP
7. BitTorrent over TCP
8. BitTorrent over UDP
9. BOOTP / DHCP
10. Dameware MRC
11. DCE/RPC
12. DICOM over TCP
13. DNS
14. DNS/LLMNR over TCP

15. DNS/LLMNR over UDP
16. Dogecoin over TCP
17. Dropbox LAN Sync over UDP
18. EIGRP
19. Ethernet I
20. Ethernet II
21. Ether-S-IO over TCP
22. Ether-S-IO over UDP
23. Finger
24. Flash Media Server
25. FTP
26. FTP Data
27. GLBP over UDP
28. GRE
29. HiDiscovery
30. HL7 v2 over TCP
31. HL7 v3 over TCP
32. HSRP over UDP
33. HTTP
34. HTTP/2
35. HTTPS
36. IBM DB2
37. ICMP
38. Ident
39. IGMP
40. IMAP
41. IPv6
42. IPv6 Encapsulated

43. IPX
44. IRC
45. IS-IS over Ethernet I
46. IS-IS over Ethernet II
47. IS-IS over IPv4
48. ISO TSAP (ISO 8072)
49. Jabber XMPP over TCP
50. Kerberos over TCP
51. Kerberos over UDP
52. LDAP(S) over TCP
53. LDAP(S) over UDP
54. LDP
55. Link Layer Discovery Protocol (LLDP)
56. Litecoin over TCP
57. Loopback
58. mDNS over UDP
59. MikroTik Neighbor Discovery Protocol (MNDP)
60. MPLS
61. MPLS multicast
62. MQTT over TCP
63. MS SQL Server
64. MSNP over TCP
65. MSNP over UDP
66. MySQL
67. Napster
68. NBNS over UDP
69. NetBIOS
70. 网络时间协议 (NTP)

71. NFS over TCP
72. NFS over UDP
73. ONVIF over TCP
74. Open Shortest Path First (OSPF)
75. Oracle DB
76. PIM
77. POP3
78. PPTP
79. 精确时间协议 (PTP)
80. PRP
81. QTP
82. RADIUS over UDP
83. RARP
84. RDP over TCP
85. RDP over UDP
86. Reliable Data Protocol
87. Remote Utilities over TCP
88. RIP
89. Rlogin
90. RSH
91. RTSP over TCP
92. SAIA S-Bus over TCP
93. SAIA S-Bus over UDP
94. SCTP
95. SFTP
96. SIP over UDP
97. SMB
98. SMB v2 over TCP

99. SMB v2 over UDP

00. SMB v3 over TCP

101. SMB v3 over UDP

02. SMB over UDP

03. SMTP

04. SNMP

05. SNMP v1 over UDP

06. SNMP v2 over UDP

07. SNMP v3 over UDP

08. SSDP

09. SSH

110. SSL v2

111. SSL v3

112. SSL/TLS

113. STP

114. SuiteLink over TCP

115. Syslog

116. Syslog over UDP

117. TCP

118. TeamViewer over TCP

119. TeamViewer over UDP

20. Telegram MTProto over TCP

121. Telnet

22. TFTP over TCP

23. TFTP over UDP

24. TLS v1.0

25. TLS v1.1

26. TLS v1.2

27. TLS v1.3

28. TNS over TCP

29. TNS over UDP

30. Tor over TCP

31. Tor over UDP

32. UDP

33. VNC

34. VRRP over IPv4

35. WebSocket

36. Cisco discovery protocol (CDP)

37. Radmin over TCP

使用配置控制任务检索设备类型配置的详细信息

添加配置控制作业时，您可以选择应用程序在设备扫描期间接收数据的设备类型。

本节包含有关接收不同设备类型的配置的特殊功能的信息。

运行 Windows 操作系统的设备的配置

您可以获取运行 **Kaspersky Endpoint AgentWindows 操作系统**Windows 操作系统类型设备的配置。适用 Kaspersky Industrial CyberSecurity for Networks 集成场景。

对于“**Windows 操作系统**”设备类型，您可以指定以下用于接收数据的配置类型：

- **用户**。
- **组**。
- **应用程序**。
- **补丁**。
- **服务**。
- **驱动器**。
- **计划任务**。
- **网络共享资源**。

- **IP 到网络名称一致性**。
- **IP 到 NetBIOS 名称一致性**。
- **启动项目**。
- **密码策略**。
- **审计策略**。
- **高级审计策略**。
- **ARP 表项目**。
- **路由表**。

可检索的用户数据

如果为配置控制作业指定了“**用户**”配置类型，则在扫描设备时会读取设备上的用户账户数据。应用程序允许您接收每个用户账户的以下数据：

- 用户名格式为“域\用户名”。
- 用户的唯一 ID。
- 用户的全名（例如，`John Smith`）。
- 指示用户账户是否处于活动。
- 指示用户账户是否被阻止。
- 指示用户账户密码是否可能过期。
- 指示密码是否已过期。
- 指示用户是否可以更改其密码。
- 包含该用户的组列表。

可检索的群组数据

如果为配置控制作业指定了“**组**”配置类型，则在扫描设备时会读取设备上的组账户数据。应用程序允许您接收每个组账户的以下数据：

- 格式为“域\组名”的组名称。
- 组的唯一 ID。

- 组中包含的用户列表。列表中的每个项目都包含以下数据：
  - 组成员的唯一 ID。
  - 组成员的姓名。

可检索的应用程序数据

如果为配置控制作业指定了“**应用程序**”配置类型，则在扫描设备时会读取设备上已安装的应用程序的数据。应用程序允许您接收每个应用程序的以下数据：

- 应用程序名称。
- 应用程序供应商。
- 应用程序的大小（以字节为单位）。
- 应用程序版本。
- 应用程序安装的日期和时间。

可检索的补丁数据

如果为配置控制作业指定了“**补丁**”配置类型，则在扫描设备时会读取设备上已安装的应用程序补丁的数据。应用程序允许您接收每个补丁的以下数据：

- 补丁名称。
- 应用程序供应商。
- 安装了补丁的应用程序。
- 补丁版本。

可检索的服务数据

如果为配置控制作业指定了“**服务**”配置类型，则在扫描设备时会读取设备上已注册服务的数据。应用程序允许您接收每个服务的以下数据：

- 服务名称。
- 服务的全名。
- 启动类型。

- 启动命令。
- 依赖服务的名称。

可检索的驱动器数据

如果为配置控制作业指定了“**驱动器**”配置类型，则在扫描设备时会读取设备上已安装驱动程序的数据。应用程序允许您接收每个驱动程序的以下数据：

- 驱动程序名称。
- 驱动程序的全名。
- 启动类型。
- 驱动程序文件的路径。
- 依赖驱动程序的名称。

可检索的计划任务数据

如果为配置控制作业指定了“**计划任务**”配置类型，则在扫描设备时会读取设备上任务调度程序注册的任务的数据。应用程序允许您接收每个任务的以下数据：

- 任务名称。
- 任务状态。
- 描述。
- 创建者。
- 任务启动时执行的命令（与运行可执行代码相关的操作）。

可检索的共享网络资源数据

如果为配置控制作业指定了“**网络共享资源**”配置类型，则在扫描设备时会读取设备上创建的共享网络资源的数据。应用程序允许您接收每个共享网络资源的以下数据：

- 共享资源的网络名称。
- 网络资源的本地路径。
- 描述。

- 网络资源的类型。
- 最大连接数。

可检索的 IP 到网络名称的映射表的数据

如果为配置控制作业指定了“**IP 到网络名称一致性**”配置类型，则在扫描设备时会读取设备上的 IP 到网络名称映射表 (\etc\hosts) 中的项目数据。应用程序允许您接收每个表项的以下数据：

- IP 地址。
- 网络名称。

可检索的 IP 到 NetBIOS 名称的映射表的数据

如果为配置控制作业指定了“**IP 到 NetBIOS 名称一致性**”配置类型，则在扫描设备时会读取设备上的 IP 到 NetBIOS 名称映射表 (\etc\lmhosts) 中的项目数据。应用程序允许您接收每个表项的以下数据：

- IP 地址。
- 网络名称。
- 指示条目是否已加载到名称缓存中。
- 条目的特定域。
- Lmhosts 包含文件。

可检索的启动项数据

如果为配置控制作业指定了“**启动项目**”配置类型，则在扫描设备时会读取设备上操作系统启动项的数据。应用程序允许您接收每个启动项的以下数据：

- 有关启动点的信息（例如，系统注册表中的路径）。
- 可执行命令或文件（COM 对象）。

可检索的密码策略数据

如果为配置控制作业指定了“**密码策略**”配置类型，则在扫描设备时读取设备的密码策略数据。应用程序允许您接收每个密码策略的以下数据：

- 密码最长使用期限。
- 密码最短使用期限。
- 最小密码长度。
- 历史记录中存储的旧密码数量。
- 指示密码是否必须满足密码复杂性要求。
- 指示密码加密是否可逆。

可检索的审计策略数据

如果为配置控制作业指定了“**审计策略**”配置类型，则在扫描设备时读取设备的审计策略数据。应用程序允许您接收每个审计策略的以下数据：

- 账户登录审计的级别。
- 账户管理审计的级别。
- 用于访问 Active Directory 域服务中的对象的审计级别。
- 登录审计的级别。
- 用于访问不在 Active Directory 域服务中的对象的审计级别。
- 策略变更的审计级别。
- 特权使用的审计级别。
- 详细跟踪的审计级别。
- 系统事件的审计级别。

可检索的高级审计策略数据

如果为配置控制作业指定了“**高级审计策略**”配置类型，则在扫描设备时读取设备的高级审计策略数据。应用程序允许您接收每个高级审计策略的以下数据：

- 用于进行高级审计的基本策略。
- 基本策略的子类别。
- 审计级别。

可检索的 ARP 表项数据

如果为配置控制作业指定了“**ARP 表项目**”配置类型，则在扫描设备时会读取设备上 ARP 表项的数据。应用程序允许您接收每个表项的以下数据：

- IP 地址。
- 硬件地址。
- 网络接口或适配器的名称。
- 硬件地址类型。
- 条目类型。

可检索的路由表数据

如果为配置控制作业指定了“**路由表**”配置类型，则在扫描设备时会读取设备上路由表项的数据。应用程序允许您接收每个表项的以下数据：

- 接口名称或 IP 地址。
- 目标子网。
- 目标子网掩码。
- 网关（远程网络中下一个路由器的地址）。
- 协议。

运行 Linux 操作系统的设备的配置

在**使用命令运行 Linux 设备标准诊断实用程序Linux 操作系统**Linux 操作系统”设备类型。

对于“**Linux 操作系统**”设备类型，您可以指定以下用于接收数据的配置类型：

- **用户**。
- **应用程序**。
- **ARP 表项目**。
- **IP 到网络名称一致性**。
- **IP 到 NetBIOS 名称一致性**。
- **计划任务**。
- **服务**。
- **路由表**。
- **特权组和用户的权限**。

可检索的用户数据

如果为配置控制作业指定了“**用户**”配置类型，则在扫描设备时会读取设备上的用户账户数据。应用程序允许您接收每个用户账户的以下数据：

- 用户名格式为“域\用户名”。
- 用户的唯一 ID。
- 用户的全名（例如，`John Smith`）。
- 指示用户账户是否处于活动。
- 指示用户账户是否被阻止。
- 指示用户账户密码是否可能过期。
- 指示密码是否已过期。
- 指示用户是否可以更改其密码。
- 包含该用户的组列表。

可检索的应用程序数据

如果为配置控制作业指定了“**应用程序**”配置类型，则在扫描设备时会读取设备上已安装的应用程序的数据。应用程序允许您接收每个应用程序的以下数据：

- 应用程序名称。
- 应用程序的大小（以字节为单位）。
- 应用程序版本。
- 应用程序安装的日期和时间。

可检索的 ARP 表项数据

如果为配置控制作业指定了“**ARP 表项目**”配置类型，则在扫描设备时会读取设备上 ARP 表项的数据。应用程序允许您接收每个表项的以下数据：

- IP 地址。
- 硬件地址。
- 网络接口或适配器的名称。
- 硬件地址类型。

可检索的 IP 到网络名称的映射表的数据

如果为配置控制作业指定了“**IP 到网络名称一致性**”配置类型，则在扫描设备时会读取设备上的 IP 到网络名称映射表 (来自 \etc\hosts 文件) 中的项目数据。应用程序允许您接收每个表项的以下数据：

- IP 地址。
- 网络名称。

可检索的 IP 到 NetBIOS 名称的映射表的数据

如果为配置控制作业指定了“**IP 到 NetBIOS 名称一致性**”配置类型，则在扫描设备时会读取设备上的 IP 到 NetBIOS 名称映射表 (来自 /etc/lmhosts 文件) 中的项目数据。应用程序允许您接收每个表项的以下数据：

- IP 地址。
- 网络名称。

可检索的计划任务数据

如果为配置控制作业指定了“**计划任务**”配置类型，则在扫描设备时会读取设备上任务调度程序注册的任务的数据。应用程序允许您接收每个任务的以下数据：

- 任务名称。
- 任务状态。
- 任务开始计划。
- 创建者。
- 可执行命令。

可检索的服务数据

如果为配置控制作业指定了“**服务**”配置类型，则在扫描设备时会读取设备上服务的数据。应用程序允许您接收每个服务的以下数据：

- 服务名称。
- 启动类型。
- 启动命令。

可检索的路由表数据

如果为配置控制作业指定了“**路由表**”配置类型，则在扫描设备时会读取设备上路由表项的数据。应用程序允许您接收每个表项的以下数据：

- 接口名称或 IP 地址。
- 目标子网。
- 目标子网掩码。
- 网关（远程网络中下一个路由器的地址）。

可检索特权组和用户的权限数据

如果为配置控制作业指定了“**特权组和用户的权限**”配置类型，则在扫描设备时会读取设备上的特权组和用户权限（来自 \etc\sudoers 文件）的数据。应用程序允许您接收有关特权组和用户的权限的以下数据：

- \etc\sudoers 文件的完整路径。
- \etc\sudoers 文件或通过 `include` 和 `includedir` 指令包含的附加文件的文本表示。

归类为网络部件的设备的配置

应用程序的当前版本允许您接收以下设备的“**网络设备**”设备类型配置：

- Cisco IOS™ 设备。
- Eltex MES 系列。
- Hirschmann MACH and RS20 系列。
- Moxa PT 和 EDS 系列。

  > 当设备处于默认设置模式（菜单模式）时，不支持 Moxa PT 系列设备的配置检索功能。

- 支持 SSH 协议的 Siemens RUGGEDCOM® RSG2100 和 SCALANCE 系列。
- D-Link® DES 和 DGS 系列（仅在 Kaspersky Industrial CyberSecurity for Networks 4.5.1 版本中受支持）。
- MikroTik RouterOS 设备（仅支持 Kaspersky Industrial CyberSecurity for Networks 版本 4.2.1）

对于“**网络设备**”设备类型，您可以指定以下用于接收数据的配置类型：

- **用户**。
- ARP **表项目**。
- **平台版本**。
- **可执行进程**。
- **启动配置**。
- **运行配置**。
- **路由表**。
- MAC **表**。
- **网络接口**。

Cisco IOS 设备上的可检索数据

应用程序在扫描 Cisco IOS 设备时检索以下数据：

- 用户数据：
  - 用户名格式为“域\用户名”。
  - 用户的唯一 ID。
  - 指示是否设置了 SSH 密钥。
  - 指示是否已配置密码。
  - 指示是否已为用户配置 Secret。
  - 用户权限级别。
- ARP 表项数据：
  - IP 地址。
  - 硬件地址。
  - 网络接口或适配器的名称。
  - 硬件地址类型。
  - 条目类型。
- 操作系统版本。
- 正在运行的进程数据：
  - 进程的唯一 ID。
  - 进程名称。
- 启动配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示。
- 运行配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示。
- 路由表数据：

    - 接口名称或 IP 地址。
    - 目标子网。
    - 目标子网掩码。
    - 网关（远程网络中下一个路由器的地址）。
    - 协议。
- MAC 表数据：
    - VLAN 编号。
    - MAC 地址。
    - MAC 地址的类型。
    - MAC 地址的端口。
- 网络接口数据：
    - 描述。
    - 指示网络接口是否启用。
    - MAC 地址。
    - 名称。
    - 指示网络接口是否是物理接口。
    - 分配的 IP 地址。

Eltex MES 系列设备上的可检索数据

应用程序在扫描 Eltex MES 系列设备时会检索以下数据：

- ARP 表项数据：
    - IP 地址。
    - 硬件地址。
    - 网络接口或适配器的名称。
    - 硬件地址类型。
    - 条目类型。
- 操作系统版本。

- 启动配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示（`show startup-config` 命令的输出）。
- 运行配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示。
- 路由表数据：
  - 接口名称或 IP 地址。
  - 目标子网。
  - 目标子网掩码。
- MAC 表数据：
  - VLAN 编号。
  - MAC 地址。
  - MAC 地址的类型。
  - MAC 地址的端口。
- 网络接口数据：
  - 描述。
  - 指示网络接口是否启用。
  - MAC 地址。
  - 名称。
  - 指示网络接口是否是物理接口。

Hirschmann RS20 和 MACH 系列设备上的可检索数据

应用程序在扫描 Hirschmann RS20 和 MACH 系列设备时会检索以下数据：

- 用户数据：
  - 用户名格式为“域\用户名”。
  - 操作员访问模式。

    - 身份验证类型。
    - 加密类型。
    - 用户访问模式。
- ARP 表项数据：
    - IP 地址。
    - 硬件地址。
    - 网络接口或适配器的名称。
    - 硬件地址类型。
- 操作系统版本。
- 运行配置数据：
    - 参数部分的名称。
    - 部分参数的文本表示。
- MAC 表数据：
    - VLAN 编号。
    - MAC 地址。
    - MAC 地址的类型。
    - MAC 地址的端口。

Moxa EDS 和 PT 系列设备上的可检索数据

应用程序在扫描 Moxa EDS 和 PT 系列设备时会检索以下数据：

- 操作系统版本。
- 启动配置数据：
    - 参数部分的名称。
    - 部分参数的文本表示（`show startup-config` 命令的输出）。
- 运行配置数据：
    - 参数部分的名称。
    - 部分参数的文本表示。

- MAC 地址表详情（仅支持 Moxa EDS 系列设备）：
  - VLAN 编号。
  - MAC 地址。
  - MAC 地址的类型。
  - MAC 地址的端口。

支持 SSH 协议的 Siemens RUGGEDCOM RSG2100 和 SCALANCE 系列设备上的可检索数据

应用程序在扫描 Siemens RUGGEDCOM RSG2100 和 SCALANCE 系列设备时会检索以下数据：

- ARP 表项数据：
  - IP 地址。
  - 硬件地址。
  - 网络接口或适配器的名称。
  - 硬件地址类型。
  - 记录类型（仅支持 Siemens SCALANCE 系列设备）。
- 操作系统版本。
- 启动配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示（Siemens SCALANCE 系列设备的不同嵌套级别的 `info` 命令的输出）。
- 运行配置详情（仅支持 Siemens RUGGEDCOM RSG2100 系列设备）：
  - 参数部分的名称。
  - 部分参数的文本表示。
- MAC 地址表详情（仅支持 Siemens RUGGEDCOM RSG2100 系列设备）：
  - VLAN 编号。
  - MAC 地址。
  - MAC 地址的类型。
  - MAC 地址的端口。

D-Link DES 和 DGS 设备的可检索数据

应用程序在扫描 D-Link DES 和 DGS 设备时会检索以下数据：

- ARP 表项数据：
  - IP 地址。
  - 硬件地址。
  - 网络接口或适配器的名称。
  - 硬件地址类型。
  - 条目类型。
- 操作系统版本。
- 启动配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示。
- 运行配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示。
- 路由表数据：
  - 接口名称或 IP 地址。
  - 目标子网。
  - 目标子网掩码。
  - 网关（远程网络中下一个路由器的地址）。
  - 协议。
- MAC 表数据：
  - VLAN 编号。
  - MAC 地址。
  - MAC 地址的类型。
  - MAC 地址的端口。

MikroTik RouterOS 设备的可检索数据

应用程序在扫描 MikroTik RouterOS 设备时会检索以下数据：

- 用户数据：
  - 用户名。
  - 用户账户描述。
  - 指示用户账户是否处于活动。
- ARP 表项数据：
  - IP 地址。
  - 硬件地址。
  - 网络接口或适配器的名称。
  - 硬件地址类型。
  - 条目类型。
- 操作系统版本。
- 运行配置数据：
  - 参数部分的名称。
  - 部分参数的文本表示。
- 路由表数据：
  - 接口名称或 IP 地址。
  - 目标子网。
  - 目标子网掩码。
  - 网关（远程网络中下一个路由器的地址）。
- MAC 表数据：
  - VLAN 编号。
  - MAC 地址。
  - MAC 地址的类型。
  - MAC 地址的端口。
- 网络接口数据：

- 指示网络接口是否启用。
- MAC 地址。
- 名称。

使用主动轮询连接器接收的 PLC 和其他设备的配置

内置“**主动轮询**”连接器类型可以接收以下设备的 **PLC** 设备类型配置：

- Emerson DeltaV
- Rockwell Automation Allen-Bradley
- Schneider Electric Modicon: M580, M340
- Siemens SIMATIC S7-300, S7-400
- Siemens SIMATIC S7-1200, S7-1500
- 基于 CODESYS V3 平台的 PLC（例如 Prosoft-Systems Regul R500）

可检索的 Emerson DeltaV 设备的数据

当使用**主动轮询**连接器扫描 Emerson DeltaV 设备时，应用程序允许您接收以下数据：

- 常规设置：
  - 设备型号或系列。
  - PLC 设备系列。
  - PLC 冗余指示器。
- CPU 模块及各接收卡的设置：
  - 包含卡的插槽编号（在所有运营商中）。
  - CPU 模块供应商。
  - 模块或卡的类型。
  - 模块型号（CPU 模块或 I/O 卡的型号）。
  - I/O 卡的简要描述。
  - 唯一的字母数字部件编号、目录编号。
  - 硬件版本。

- 控制器和卡的 IDE 和固件版本。
- 用户在 IDE 中定义的控制器的唯一名称。
- IDE 中分配的控制器的唯一 ID。
- PLC CPU 模块的序列号。

- 每个接收到的 PLC 项目文件的设置：
  - 项目模块（文件）的名称。
  - 每个配置文件加载到 PLC 的日期。
  - 项目模块的校验和。

可检索的 Rockwell Automation Allen-Bradley 设备的数据

当使用**主动轮询**连接器扫描 Rockwell Automation Allen-Bradley 设备时，应用程序允许您接收以下数据：

- 每个接收模块的设置：
  - 包含模块的机架中的插槽号。
  - 模块供应商。
  - 模块类型。
  - 产品（模块）代码。
  - 有关模块型号的信息。
  - 固件版本。
  - 用户在 IDE 中定义的控制器的唯一名称。
  - 模块的序列号。
  - 模块的复合状态。
- PLC 项目的常规设置：
  - 分配给项目的模块插槽号。
  - 用户自定义名称。
  - 用户自定义描述。

- PLC 项目各个程序及例程的设置：
  - 项目任务的名称。
  - 项目任务的类型。
  - 项目任务的优先级。
  - 项目程序的名称。
  - 项目程序中的例程名称。
  - 例程的校验和。

可检索的 Schneider Electric Modicon 设备的数据

当使用**主动轮询**连接器扫描 Schneider Electric Modicon 设备时，应用程序允许您接收以下数据：

- 常规设置：
  - PLC 型号或系列。
  - 用于配置设备的自动化系统开发软件。
  - PLC 安装中的机架数量。
- 每个接收模块的设置：
  - 包含模块的机架编号。
  - 包含模块的机架中的插槽号。
  - CPU 模块供应商。
  - 模块类型。
  - 有关模块型号的信息。
  - 模块固件版本。
  - 模块的唯一 ID。
  - CPU 模块的运行模式或状态。
- PLC 项目的常规设置：
  - 用户自定义名称。
  - 哈希值。
  - 上次完整构建项目的开发环境 (IDE) 的名称和版本。

    - 项目最后一次完整构建的日期和时间。
    - 执行项目最后部分构建的开发环境 (IDE) 的名称和版本（针对单个项目块）。
    - 项目最后一次部分构建的日期和时间。
    - 项目的用户定义版本。
- 每个接收到的 PLC 项目块的设置：
    - 分配给块的任务设置类型。
    - 用户自定义名称。
    - 块的类型以及编写该块的助记图的语言。
    - 校验和。

可检索的 Siemens S7-300 和 S7-400 系列 SIMATIC 设备的数据

当使用**主动轮询**连接器扫描 SIMATIC S7-300 和 S7-400 系列设备时，应用程序允许您接收以下数据：

- 常规设置：
    - PLC 型号或系列。
    - 用于配置设备的自动化系统开发软件。
    - PLC 安装中的机架数量。
    - 内存状态。
    - 安全设置。
- 每个接收模块的设置：
    - 包含模块的机架编号。
    - 包含模块的机架中的插槽号。
    - CPU 模块供应商。
    - 模块类型。
    - 有关模块型号的信息。
    - 基于 Siemens 目录的模块 ID。
    - Siemens 模块 (MLFB) 的唯一字母数字代码。
    - 模块硬件版本。

    - 模块固件版本。
    - 初始引导加载程序版本。
    - CPU 模块的序列号。
    - 请求的 CPU 模块操作模式（由于转换而应启用的模式）。
    - CPU 模块的当前运行模式。
- PLC 项目的哈希值。
- 每个接收到的 PLC 项目块的设置：
    - 类型。
    - ID。
    - 编写块的助记图的语言。
    - 校验和。
    - 编译日期。
    - 有关创建者或开发环境的信息。

Siemens SIMATIC S7-1200 和 S7-1500 系列设备上的可检索数据

当使用**主动轮询**连接器扫描 Siemens SIMATIC S7-1200 和 S7-1500 系列设备时，应用程序允许您接收以下数据：

- 常规设置：
    - PLC 型号或系列
    - 内存状态。
    - 安全设置。
- 每个接收模块的设置：
    - 包含模块的机架中的插槽号。
    - CPU 模块供应商。
    - 模块类型。
    - 有关模块型号的信息。
    - Siemens 模块 (MLFB) 的唯一字母数字代码。
    - 模块固件版本。

    - CPU 模块的序列号。
    - CPU 模块的当前运行模式。
- PLC 项目的哈希值。
- 每个接收到的 PLC 项目块的设置：
    - 类型。
    - ID。
    - 编写块的助记图的语言。
    - 校验和。
    - 编译日期。

基于 CODESYS V3 平台的 PLC 上的可检索数据

当已使用**主动轮询**连接器扫描基于 CODESYS V3 平台的 PLC 时，该应用程序允许您接收以下数据：

- 常规设置：
    - PLC 模型。
    - PLC 制造商。
    - 固件版本。
- 每个接收项目的设置：
    - PLC 项目名称。
    - PLC 项目的哈希值。
    - 修改日期和时间。
- PLC 项目中各个软件组件的设置：
    - 类型。
    - 名称。
    - 指定软件组件内存中位置地址的设置。
    - 指定软件组件的校验和的设置。

安全审计作业中用于扫描 Linux 设备的命令。

作为漏洞和合规性审计作业或配置控制作业的一部分，扫描运行 Linux 操作系统的设备时，使用命令启动以下实用程序，在每台设备上获取必要的数据：

- blkid
- cat
- df
- dmidecode
- ethtool
- 剩余
- hwinfo
- ip
- ls
- lsblk
- lshw
- lsusb

所有上述实用程序都必须在设备操作系统中安装并可用。如果缺少某个实用程序，则无法接收仅由该实用程序提供的数据。

所有上述实用程序均默认预安装在 Kaspersky Industrial CyberSecurity for Linux Nodes 支持的大多数操作系统中。您可以通过在设备操作系统的控制台中运行适当的命令来检查实用程序。

要检查 CentOS 中的实用程序：

1. 在计算机的操作系统控制台中，运行以下命令：

   ```
   which blkid cat df dmidecode ethtool free hwinfo ip ls lsblk lshw lsusb
   ```

   已安装实用程序的文件路径列表将显示。

2. 确保列表包含所有必需实用程序的路径。

如果缺少实用程序，请安装包含该实用程序的包。

要在 CentOS 中安装 dmidecode 包，

在计算机的操作系统控制台中，运行以下命令：

```
sudo dnf install dmidecode
```

支持执行设备主动轮询的设备操作系统

本文列出了用于主动轮询设备的应用程序支持的设备操作系统。

Windows 操作系统

Kaspersky Industrial CyberSecurity for Networks 支持对运行以下 Windows 版本的设备执行主动轮询：

- 桌面操作系统：
  - Windows XP 专业版 SP2 x86/x64
  - Windows XP 专业版 SP3 x86
  - Windows Vista® SP2 x86/x64
  - Windows 7 企业版 SP1 x86/x64
  - Windows 7 专业版 SP1 x86/x64
  - Windows 7 旗舰版 SP1 x86/x64
  - Windows 8 企业版 x86/x64
  - Windows 8 专业版 x86/x64
  - Windows 8.1 企业版 x86/x64
  - Windows 8.1 专业版 x86/x64
  - Windows 10 LTSC 2015，版本 1507 x86/x64
  - Windows 10 LTSC 2016，版本 1607 x86/x64
  - Windows 10 Education RS4，版本 1803 x86/x64
  - Windows 10 Enterprise RS4，版本 1803 x86/x64
  - Windows 10 Home RS4，版本 1803 x86/x64
  - Windows 10 Pro RS4，版本 1803 x86/x64

- Windows 10 Education RS5，版本 1809 x86/x64
- Windows 10 Enterprise RS5，版本 1809 x86/x64
- Windows 10 Home RS5，版本 1809 x86/x64
- Windows 10 Pro RS5，版本 1809 x86/x64
- Windows 10 LTSC 2019，版本 1809 x86/x64
- Windows 10 Education 19H1，版本 1903 x86/x64
- Windows 10 Enterprise 19H1，版本 1903 x86/x64
- Windows 10 Home 19H1，版本 1903 x86/x64
- Windows 10 Pro 19H1，版本 1903 x86/x64
- Windows 10 Education 20H1，版本 2004 x86/x64
- Windows 10 Enterprise 20H1，版本 2004 x86/x64
- Windows 10 Home 20H1，版本 2004 x86/x64
- Windows 10 Pro 20H1，版本 2004 x86/x64
- Windows 10 Education 20H2，版本 2009 x86/x64
- Windows 10 Enterprise 20H2，版本 2009 x86/x64
- Windows 10 Home 20H2，版本 2009 x86/x64
- Windows 10 Pro 20H2，版本 2009 x86/x64
- Windows 10 Education 21H1，版本 21H1 x86/x64
- Windows 10 Enterprise 21H1，版本 21H1 x86/x64
- Windows 10 Home 21H1，版本 21H1 x86/x64
- Windows 10 Pro 21H1，版本 21H1 x86/x64
- Windows 10 Education 21H2，版本 21H2 x86/x64
- Windows 10 Enterprise 21H2，版本 21H2 x86/x64
- Windows 10 Home 21H2，版本 21H2 x86/x64
- Windows 10 Pro 21H2，版本 21H2 x86/x64
- Windows 10 Education 22H2，版本 22H2 x86/x64
- Windows 10 Enterprise 22H2，版本 22H2 x86/x64
- Windows 10 Home 22H2，版本 22H2 x86/x64

- Windows 10 Pro 22H2，版本 22H2 x86/x64
- Windows 10 LTSC 2021，版本 21H2 x86/x64
- Windows 11 Education 21H2，版本 21H2 x64
- Windows 11 Enterprise 21H2，版本 21H2 x64
- Windows 11 Home 21H2，版本 21H2 x64
- Windows 11 Pro 21H2，版本 21H2 x64
- Windows 11 Education 22H2，版本 22H2 x64
- Windows 11 Enterprise 22H2，版本 22H2 x64
- Windows 11 Home 22H2，版本 22H2 x64
- Windows 11 Pro 22H2，版本 22H2 x64

- 服务器操作系统：
  - Windows Server® 2003 Enterprise SP1 x86/x64
  - Windows Server 2003 Standard SP1 x86/x64
  - Windows Server 2003 Enterprise SP2 x86/x64
  - Windows Server 2003 Standard SP2 x86/x64
  - Windows Server 2003 Enterprise R2 x86/x64
  - Windows Server 2003 Standard R2 x86/x64
  - Windows Server 2008 Enterprise SP2 x86/x64
  - Windows Server 2008 Standard SP2 x86/x64
  - Windows Server 2008 R2 Enterprise SP1 x86/x64
  - Windows Server 2008 R2 Standard SP1 x86/x64
  - Windows Server 2012 Datacenter x64
  - Windows Server 2012 Essentials x64
  - Windows Server 2012 Foundation x64
  - Windows Server 2012 Standard x64
  - Windows Server 2012 R2 Datacenter x64
  - Windows Server 2012 R2 Essentials x64
  - Windows Server 2012 R2 Foundation x64

- Windows Server 2012 R2 Standard x64
- Windows Server 2016 Datacenter，版本 1709 x64
- Windows Server 2016 Essentials，版本 1709 x64
- Windows Server 2016 Standard，版本 1709 x64
- Windows Server 2016 Datacenter，版本 1803 x64
- Windows Server 2016 Essentials，版本 1803 x64
- Windows Server 2016 Standard，版本 1803 x64
- Windows Server 2019 Datacenter，版本 1809 x64
- Windows Server 2019 Essentials，版本 1809 x64
- Windows Server 2019 Standard，版本 1809 x64
- Windows Server 2019 Datacenter，版本 1903 x64
- Windows Server 2019 Essentials，版本 1903 x64
- Windows Server 2019 Standard，版本 1903 x64
- Windows Server 2019 Datacenter，版本 1909 x64
- Windows Server 2019 Essentials，版本 1909 x64
- Windows Server 2019 Standard，版本 1909 x64
- Windows Server 2019 Datacenter Core，版本 2004 x64
- Windows Server 2019 Standard Core，版本 2004 x64
- Windows Server 2019 Datacenter Core，版本 20H2 x64
- Windows Server 2019 Standard Core，版本 20H2 x64
- Windows Server 2022 Datacenter Core，版本 21H2 x64
- Windows Server 2022 Standard Core，版本 21H2 x64

- 嵌入式操作系统：
  - Windows XP Embedded SP2 WEPOS x86/x64
  - Windows XP Embedded SP3 x86 (POS Ready 2009)
  - Windows Embedded 7 SP1 x86/x64 (POS Ready 7)
  - Windows Embedded 8.0 Industry Pro x86/x64
  - Windows Embedded 8.1 Industry Pro x86/x64

- Windows 10 IoT Enterprise 21H1 x86/x64
- Windows 10 IoT Enterprise 21H2 x86/x64
- Windows 10 IoT Enterprise 22H2 x86/x64
- Windows 10 IoT Enterprise，版本 1803 x86/x64
- Windows 10 IoT Enterprise，版本 1809 x86/x64
- Windows 10 IoT Enterprise，版本 1903 x86/x64
- Windows 11 IoT Enterprise，版本 21H2 x64
- Windows 11 IoT Enterprise，版本 22H2 x64

Linux 操作系统

Kaspersky Industrial CyberSecurity for Networks 支持具有以下 Linux 版本的活动设备：

- 32 位操作系统：
  - Debian GNU / Linux 10.1
  - Debian GNU / Linux 11
- 64 位操作系统：
  - AlmaLinux OS 8
  - AlmaLinux OS 9
  - ALT Linux 8 SP Workstation
  - ALT Linux 8 SP Server
  - ALT Linux Workstation 10
  - ALT Linux Server 10
  - AlterOS® 7.5
  - Astra Linux 1.4
  - Astra Linux Common Edition（定期更新 2.12）
  - Astra Linux Special Edition RUSB.10015-01（定期更新 1.5）
  - Astra Linux Special Edition RUSB.10015-01（操作更新 1.6）
  - Astra Linux Special Edition RUSB.10015-01（操作更新 1.7）

- Astra Linux Special Edition RUSB.10015-16（版本 1）（定期更新 1.6）
- Astra Linux Special Edition RUSB.10015-01（操作更新 1.8）
- Astra Linux Orel 2.12
- CentOS 5.2
- CentOS 5.4
- CentOS 6.5 (内核版本 2.6.32-432)
- CentOS 6.6
- CentOS 6.7
- CentOS 7.2
- CentOS 8.0
- CentOS Stream 9
- Debian 4
- Debian GNU / Linux 10.1
- Debian GNU / Linux 11
- EulerOS 2.0 SP5
- Linux Mint 19.2
- Linux Mint 20.3
- openSUSE Leap 15.0
- Oracle® Linux 7.3
- Oracle Linux 8.0
- Oracle Sun Solaris 5.10
- Red Hat® 7.0 Guinness
- Red Hat Enterprise Linux® 6.3
- Red Hat Enterprise Linux 6.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 9
- Red Hat Enterprise Linux Server 5.7

- Red Hat Enterprise Linux Server 6.9
- Red Hat Enterprise Linux Workstation 6.7
- RedOS 7.3
- Rocky Linux™ 8.5
- Ruby duck 5.6 (内核版本 2.6.32.-504)
- SUSE® Linux Enterprise Server 12.5
- SUSE Linux Enterprise Server 15
- Tenix WS (Gentoo 系列)
- Ubuntu 10.04
- Ubuntu 16.04
- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 20.04
- Ubuntu 20.04 LTS
- Ubuntu 22.04
- Ubuntu 22.04 LTS
- Ubuntu Core
- GosLinux 7.17
- GosLinux 7.2

检测 Kaspersky Industrial CyberSecurity for Networks 中的属性和典型设备交互

Kaspersky Industrial CyberSecurity for Networks 可以通过被动分析工业网络中的设备活动来检测网络流量中有关基础设施的重要信息，并保存有关检测到的网络设备、其属性和交互的信息。

为确保 Kaspersky Industrial CyberSecurity for Networks 能够获取有关过程控制系统组件、其属性以及典型网络交互的最准确和完整的信息，建议在控制系统中执行各种维护和日常操作。这些可以是任何被认为可接受的操作。操作必须安全，不得以其他方式中断或影响正常工艺流程。

这些操作可能包括但不限于：

- 网络设备轮询。
- 启动 SCADA 服务器、Historian、HMI 和 PLC 之间的操作。
- 使用适当的工程软件连接到 PLC 和 IED。
- 上传和下载 PLC 项目。
- 请求有关 PLC 配置和固件版本的信息。
- 重新启动 SCADA 服务器、Historian、操作员和工程师工作站。
- 重新启动 PLC 和/或 IED。

有关如何执行操作的说明，请参阅过程控制系统的软件和硬件文档。

为 Kaspersky Industrial CyberSecurity for Networks 配置端口镜像

为了正确操作，Kaspersky Industrial CyberSecurity for Networks 必须接收从配置为将镜像网络数据包传输到指定网络端口的工业网络交换机发送的网络流量副本。这种网络流量镜像技术称为交换端口分析器（SPAN）或端口镜像。

对于流量镜像，建议您使用支持千兆以太网标准的接口。

配置端口镜像时，应配置网络交换机设置，以避免发送到 Kaspersky Industrial CyberSecurity for Networks 的流量重复。重复流量会导致应用程序节点上的磁盘空间占用增加。如果启用从所有源端口到单个目标端口的数据传输，则仅使用单向传输：入口（接收，rx）。否则，SPAN 端口会将连接到交换机不同端口且彼此交换数据的设备的流量重复传输。

本节包含可用于工业网络基础设施的几种以太网交换机型号的端口镜像配置示例。您可以在网络部件的文档中获取有关配置其他型号交换机的类似信息。

为 Cisco Access and Distribution 交换机配置端口镜像

您可以使用交换机命令行界面为 Cisco Access and Distribution 交换机（例如 Cisco Catalyst™ 2960 和 Cisco Catalyst 3850）配置 SPAN 会话。为此，请通过以太网或控制台端口访问目标交换机并打开交换机管理功能。在设置模式下，创建一个新的监控会话，选择镜像流量源，设置目标端口，并保存设置。

有关为 Cisco Access and Distribution 交换机配置端口镜像的更多信息，请参阅 Cisco 硬件文档。

要为 Cisco Access and Distribution 交换机配置流量镜像：

1. 使用以下命令启用特权 EXEC 模式：

```
enable
```

2. 从特权 EXEC 模式，使用以下命令进入全局配置模式：

```
conf t
```

3. 要查看现有的监控会话，请输入以下命令：

```
show monitor session all
```

4. 如有必要，删除现有的监控会话：

```
no monitor session <会话编号>
```

其中`<会话编号>`是要删除的监控会话的编号。您可以指定 1 到 66 之间的值。您可以使用以下关键字代替会话号：

- `all` – 删除所有监控会话
- `local` – 删除本地监控会话
- `remote` – 删除远程监控会话

5. 指定镜像流量源：

- 如果源是交换机端口，请使用以下命令：

```
monitor session <会话编号> source interface <源端口>
```

其中：

- `<会话号>` – 监控会话号
- `<source ports>` – 要监控的交换机端口（您可以指定多个值，用逗号分隔或指定范围）。

- 如果源是具有特定 VLAN ID 的虚拟局域网，请使用以下命令：

```
monitor session <会话编号> source vlan <VLAN sources>
```

其中：

- `<会话号>` – 监控会话号
- `<VLAN sources>` – 要监控的 VLAN ID（您可以指定多个值，用逗号分隔或指定范围）。

6. 指定目标端口：

```
monitor session <会话编号> destination interface <目标端口> encapsulation replicate
```

其中：

- `<会话号>` – 监控会话号
- `<destination port>` – 将网络流量副本发送到的端口。

7. 使用以下命令返回特权 EXEC 模式：

```
end
```

8. 要检查监控会话配置，请输入以下命令：

```
show monitor
```

9. 要在重新启动交换机后激活 SPAN 设置，请将监控会话配置保存到配置文件中：

```
copy running-config startup-config
```

命令序列中定义的值示例

```
enable
conf t
monitor session 1 source interface gigabitethernet0/1 - 23
monitor session 1 destination interface gigabitethernet0/24 encapsulation replicate
end
copy running-config startup-config
```

为 Cisco Small Business™ 交换机配置端口镜像

有关配置 Cisco Small Business 交换机的更多信息，请参阅 Cisco 文档。

要为 Cisco Small Business 交换机配置端口镜像：

1. 连接到交换机并在交换机 Web 界面中打开端口镜像设置。
2. 选择“**管理**” → “**诊断**” → “**端口和 VLAN 镜像**”部分。
3. 添加源接口并选择目标接口。
4. 保存更改。

为 Hirschmann Industrial Ethernet 交换机配置端口镜像

有关为 Hirschmann Industrial Ethernet 交换机配置端口镜像的更多信息，请参阅 Hirschmann 部件文档。

要为 Hirschmann Industrial Ethernet 交换机配置端口镜像：

1. 连接到交换机。
2. 在交换机 Web 界面中，选择“**诊断**” → “**端口镜像**”。
3. 作为源，选择所有必要的 RX 和 TX 端口进行 ingress 和 egress 监控。
4. 选择要连接到 Kaspersky Industrial CyberSecurity for Networks 设备的目标端口。
5. 要启用镜像，请在“**操作**”部分中选择“**开**”，然后选择“**设置**”。
   更改将应用于设备的易失性存储器 (RAM)。
6. 要永久保存更改，请打开对话框窗口并单击“**保存**”。

为 Siemens SCALANCE 交换机配置端口镜像

有关为 Siemens SCALANCE 交换机配置端口镜像的更多信息，请参阅 Siemens 部件文档。

要为 Siemens SCALANCE 交换机配置端口镜像：

1. 连接到交换机 Web 界面并选择“**二层**” → “**镜像**”。
2. 要创建镜像会话：
   a. 选择“**常规**”选项卡。
   b. 启用镜像。
   c. 要在表中创建记录，请单击**“创建”**按钮。
      将自动分配会话 ID。
   d. 在**“会话类型”**下拉列表中，选择**“基于端口”**值。
   e. 单击“**设置值**”按钮。
   f. 在“**目标端口**”列中，选择目标端口。
      例如，**P0.8**。
   g. 单击“**设置值**”按钮。
3. 选择“**端口**”选项卡。
4. 在**“端口”**选项卡中执行以下步骤：
   a. 在“**会话 ID**”下拉列表中，选择您之前在“**常规**”选项卡中创建的会话的 ID。
   b. 要监控端口的所有数据流量，请在 **Ingress** 和 **Egress** 列中选择表中的所有端口。
   c. 单击“**设置值**”按钮。

为 Siemens RUGGEDCOM i800, i801, i802, i803 交换机配置端口镜像

有关为 Siemens RUGGEDCOM 交换机配置端口镜像的更多信息，请参阅 Siemens 部件文档。

要为 Siemens RUGGEDCOM i800, i801, i802, i803 交换机配置端口镜像：

1. 连接到交换机 Web 界面。
   通过 IP 地址 192.168.0.1/24 建立与设备的默认连接。
2. 选择“**以太网端口**” → “**配置端口镜像**”。
3. 对于“**端口镜像**”设置，选择“**启用**”。
4. 在“**源端口**”设置中指定源端口号。
5. 对于“**源方向**”设置，选择 **Egress 和 Ingress**。
6. 在“**目标端口**”设置中指定目标端口号。
7. 单击“**应用**”按钮。

词汇表

ARP 欺骗

犯罪分子用来对使用 ARP（地址解析协议）的网络进行“中间人”攻击的技术。

CVE

Common Vulnerabilities and Exposures 的缩写。公开已知漏洞和信息安全风险的数据库。此数据库中描述的漏洞被分配了格式为 CVE-<年>-<数字> 的标识号。

EPP 应用程序

端点保护平台 (EPP) 中包含的应用程序。EPP 应用程序安装到企业 IT 基础设施内的端点设备（例如移动设备、计算机或笔记本电脑）。EPP 应用程序的一个示例是 Kaspersky Endpoint Security for Windows，它包含在被称为卡巴斯基网络安全解决方案的 EPP 解决方案中。

ICS

Industrial Control System 的缩写。一组设计用于工业企业加工部件自动化控制的硬件和软件。

IOC

入侵指标。有关恶意对象或操作的一组数据。

IOC 文件

包含一组 IOC 指示器的文件，如果匹配，则应用程序将事件视为检测。如果检查发现对象数据与多个 IOC 文件完全匹配，则检测的可能性可能会增加。

Kaspersky Industrial CyberSecurity for Networks 传感器

Kaspersky Industrial CyberSecurity for Networks 组件。传感器安装在单独的计算机上（而不是安装在执行 Kaspersky Industrial CyberSecurity for Networks 服务器功能的计算机上）。传感器接收并分析来自连接到传感器计算机的网络接口的计算机网络的数据。要接收和分析工业网络流量，必须将监控点添加到网络接口。探测器将数据分析结果转发给服务器。

Kaspersky Industrial CyberSecurity for Networks 服务器

Kaspersky Industrial CyberSecurity for Networks 组件。服务器接收数据、处理数据并将其提供给应用程序的用户。服务器可以接收来自传感器的数据，或者独立地从连接到服务器计算机的网络接口的计算机网络获取和分析数据。

Kaspersky Industrial CyberSecurity 专用网络

计算机网络，由设计用于运行属于 Kaspersky Industrial CyberSecurity 解决方案一部分的应用程序的计算机以及支持计算机之间交互的网络器材组成。专用网络不能从其他网络访问。

PLC 项目

为 PLC 编写的微程序。它存储在 PLC 内存中，并作为使用 PLC 的工业过程的一部分运行。PLC 项目可能由块组成，这些块在读取或写入项目时通过网络单独传输和接收。

SCADA

监控与数据采集的缩写。使操作员能够实时控制工业过程的软件套件。

SIEM

Security Information and Event Management 的缩写。这是用于管理组织安全系统中的信息和事件的解决方案。

不受管理的交换机

没有地址信息的设备，其拓扑图上的连接已被检测到或可能可用。

不受管理的连接器

手动控制的软件模块，用于与应用程序进行数据交换。

事件

在 Kaspersky Industrial CyberSecurity for Networks 中，事故是指收到特定事件序列时注册的事件。事故对具有某些共同特征或与同一过程相关的事件进行分组。Kaspersky Industrial CyberSecurity for Networks 根据事件关联规则注册事故。

事件

包含需要 ICS 安全官员注意的信息的记录。Kaspersky Industrial CyberSecurity for Networks 将注册事件保存在数据库中。要查看已注册的事件，您必须连接到应用程序服务器。如有必要，您可以配置向 Kaspersky Security Center 和收件人系统传输事件。

事件关联规则

用于检查 Kaspersky Industrial CyberSecurity for Networks 中的事件序列的条件集。当 Kaspersky Industrial CyberSecurity for Networks 检测到一系列满足事件关联规则条件的事件时，应用程序会注册一个事故。

事件类型

定义了用于在 Kaspersky Industrial CyberSecurity for Networks 中注册事件的参数集。每个事件类型都会分配一个唯一的编号（事件类型代码）。

交互控制规则

工业网络设备授权通信的描述。当 Kaspersky Industrial CyberSecurity for Networks 检测到满足启用的交互控制规则的网络交互时，应用程序不会注册事件。

入侵检测

用于注册与检测作为攻击迹象的流量异常相关的事件的技术（例如，检测 ARP 欺骗的迹象）。

入侵检测规则

入侵检测系统用来分析流量的一组条件。该规则描述了可能是工业网络中攻击迹象的流量异常。

单点登录 (SSO) 技术

允许用户使用同一用户帐户访问多个软件资源的机制。

可管理的连接器

与应用程序进行数据交换的软件模块；它提供自动注册、启动和控制功能。只有安装了应用程序组件的节点才能充当可管理连接器的部署节点。

可编程逻辑控制器 (PLC)

用于实现企业过程自动化的工业控制器。

命令控制

用于注册与流量中设备的系统命令检测相关的事件（例如，检测未经授权的系统命令）的技术。

地址空间 (AS)

由确定地址组、VLAN 标识符或监控点的规则定义的网段。

外部

用于注册 Kaspersky Industrial CyberSecurity for Networks 从使用 Kaspersky Industrial CyberSecurity for Networks API 方法的接收系统接收的事故和事件的技术。

安全策略

确定 Kaspersky Industrial CyberSecurity for Networks 运行设置的数据集。

工业网络

连接工业企业自动化工业控制系统节点的计算网络。

拓扑图

工业网络中设备之间物理连接方案的视觉表示模型。拓扑图包含以下对象：代表设备和网络器材的节点，以及代表节点物理连接的链路。

是深度包检测

用于注册与过程违规相关的事件（例如，已超出设定的温度值）的技术。

智能电子设备 (IED)

确保及时将故障电力设施从电力系统中断开，并执行必要操作以保证电力系统在自动或半自动运行模式下正常运行的一组设备。

标记

包含特定过程参数（例如，温度）的值的变量。

监控点

接收传入数据的点。它被添加到托管 Kaspersky Industrial CyberSecurity for Networks 的服务器或探测器的节点的网络接口，用于接收工业网络流量的副本（例如，从配置为传输镜像流量的网络交换机端口）。

端点保护平台

用于注册与卡巴斯基应用程序检测到的威胁相关的事件（例如，恶意软件检测事件）的技术，卡巴斯基应用程序执行保护工作站和服务器的功能。

端点保护平台 (EPP)

通过使用各种安全技术提供全面的端点保护（例如移动设备、计算机或笔记本电脑）的集成系统。端点保护平台的一个示例是卡巴斯基网络安全解决方案。

系统命令

工业网络流量中的数据块，包含控制命令（例如，START PLC）或与设备操作相关的系统消息或包含数据包分析结果（例如，REQUEST NOT FOUND）。

网络交互图

直观地表示检测到的设备之间的通信的模型。网络交互图包含以下对象：设备对应的节点、设备组以及节点/设备组之间的链接。

网络地图上的链接

网络地图上的对象由连接节点的线表示。在网络交互图上，显示了节点的交互。在拓扑图上，显示了节点的物理连接。

网络完整性控制

用于注册与工业网络完整性或通信安全相关的事件的技术（例如，通过未经授权的协议检测设备之间的通信）。

网络异常检测规则

一组用于分析流量中协议属性的条件，旨在检测在网络层面上可能与设备正常活动难以区分的异常情况。当规则被触发时，Kaspersky Industrial CyberSecurity for Networks 会记录一个事件。

网络行为偏差

由于不符合已启用的交互控制规则，导致设备间发生网络交互并被注册为事件。基于网络行为偏差事件，您可以微调应用于各个设备的交互控制。

节点

安装了 Kaspersky Industrial CyberSecurity for Networks Server 或传感器的计算机，或网络地图上代表一台或多台设备的对象。

设备

连接到计算机网络并通过可保存在 Kaspersky Industrial CyberSecurity for Networks 中的地址信息进行识别的设备（例如，可编程逻辑控制器、远程终端或智能电子设备）。

设备漏洞

设备硬件或软件中的缺陷，黑客可利用该缺陷影响信息系统的运行或获得对信息的未经授权的访问。

账户角色

一组访问权限，用于确定用户连接到应用程序服务器时可以执行的操作。Kaspersky Industrial CyberSecurity for Networks 提供以下角色：管理员、安全官、基础设施官、ICS 官和操作员。

资产管理

用于注册与流量或从 EPP 应用程序接收的数据中的设备信息检测相关的事件（例如，用于检测来自先前未知设备的活动的事件）的技术。

过程控制规则

标记值的一组条件。当满足过程控制规则的条件时，Kaspersky Industrial CyberSecurity for Networks 会注册一个事件。

风险

分析流量和设备信息时检测到的对信息系统资源的潜在威胁。

风险类型

定义的用于在 Kaspersky Industrial CyberSecurity for Networks 中注册风险的参数集。每个风险类型都会分配一个唯一的编号（风险类型代码）。

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 文件内。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

Adobe、Flash 是 Adobe 在美国和/或其他国家/地区的注册商标或商标。

BACnet 是美国采暖、制冷与空调工程师学会的注册商标。

Apache 是 Apache 软件基金会在美国和/或其他国家/地区的注册商标或商标。

iPad、iPhone、Mac、Mac OS、macOS 和 OS X 是 Apple Inc. 的商标。

AXIS 和 AXIS COMMUNICATIONS 是 Axis AB 在不同司法辖区的注册商标或商标申请。

BitTorrent 是 BitTorrent, Inc. 的商标。

Bluetooth 字样、标记和徽标归 Bluetooth SIG, Inc. 所有。

Ubuntu 和 LTS 是 Canonical Ltd 的注册商标。

Cisco、Cisco AnyConnect、Cisco Catalyst、Cisco Small Business、Aironet、AnyConnect、IOS 和 Jabber 是 Cisco Systems, Inc. 和/或其附属公司在美国和其他某些国家的注册商标或商标。

Docker 和 Docker 徽标是 Docker, Inc. 在美国和/或其他国家/地区的商标或注册商标。Docker, Inc. 和其他方也可能拥有此处使用的其他条款中描述的商标权。

Dropbox 是 Dropbox, Inc. 的商标。

Radmin 是 Famatech 的注册商标。

Fortinet、FortiGate 和 FortiOS 是 Fortinet, Inc. 在美国和/或其他国家/地区的注册商标或商标。

FreeBSD 是 FreeBSD 基金会的注册商标。

General Electric 和 Multilin 是通用电气公司的注册商标。

Google、Android、Chrome、Chromium、Google Chrome 和 Nexus 是 Google LLC 的商标。

OPPO 是广东 OPPO 移动通信有限公司的商标或注册商标。

HL7 是 Health Level Seven International 的注册商标，其使用并不构成 HL7 的认可。

Hitachi 是日立有限公司的商标。

HUAWEI 和 EulerOS 是华为技术有限公司的商标。

Intel、Atom、Core 和 Itanium 是英特尔公司或其子公司的商标。

IBM 和 DB2 是国际商业机器公司的商标，在全球许多司法管辖区注册。

Node.js 是 Joyent, Inc. 的商标。

Juniper 是 Juniper Networks, Inc. 在美国和其他国家的商标或注册商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Microsoft、Active Desktop、Active Directory、ActiveX、AppLocker、Authenticode、BitLocker、BizTalk、Cortana、InPrivate、Internet Explorer、Microsoft Edge、Outlook、PowerShell、SmartScreen、SpyNet、SQL Server、Visual Basic、Visual FoxPro、Win32、Windows、Windows Media、Windows PowerShell、Windows Server、Windows Store、Windows Vista 和 Windows XP 是 Microsoft 集团公司的商标。

MOXA 是 Moxa Inc. 的注册商标。

Mozilla 和 Firefox 是 Mozilla 基金会在美国和其他国家的商标。

DICOM 是美国电气制造商协会针对医疗信息数字通信相关标准出版物的注册商标。

KALI LINUX 是 OffSec 的商标。

ONVIF 是 ONVIF, Inc. 的商标。

OpenSSL 是 OpenSSL 软件基金会的商标。

OpenVPN 是 OpenVPN, Inc. 的注册商标。

Oracle、Java、JavaScript 和 Solaris 是 Oracle 和/或其附属公司的注册商标。

Python 是 Python 软件基金会的商标或注册商标。

Red Hat、Red Hat Enterprise Linux、CentOS 和 Fedora 是 Red Hat, Inc. 或其子公司在美国和其他国家/地区的商标或注册商标。

Remote Utilities 是 Remote Utilities LLC 在美国和/或其他国家/地区的注册商标。

BlackBerry 商标归 Research In Motion Limited 所有，已在美国注册，并且可能正在其他国家申请或已注册。

SAMSUNG 是三星电子有限公司在美国或其他国家的商标。

Schneider Electric 是 Schneider Electric 的商标。

Sendmail 和其他名称和产品名称是 Sendmail, Inc. 的商标或注册商标。

Siemens、Simatic 和 WinCC 是西门子股份公司 (Siemens AG) 的注册商标。

Ruggedcom 是西门子加拿大有限公司的商标。

OpenWRT 是软件自由保护组织（SFC）的商标。Kaspersky Industrial CyberSecurity for Networks 与 OpenWrt 没有任何关联。

Debian 是 Software in the Public Interest, Inc. 的注册商标。

Dameware 是 SolarWinds Worldwide, LLC 或其附属公司拥有的商标，在美国专利商标局注册，并且可能在其他国家/地区注册或正在等待注册。

SUSE 是 SUSE LLC 在美国和其他国家/地区的注册商标。

OpenAPI 是 The Linux Foundation 的商标。

Rocky Linux 是 Rocky Enterprise Software Foundation 的商标。

用于识别 UserGate 产品和服务的名称、图像和徽标是 UserGate 和/或其子公司或关联公司的商标，这些产品是 UserGate 的财产。

VMware 是 VMware, Inc. 在美国和其他国家/地区的注册商标和/或商标。

VxWorks 是 Wind River Systems, Inc. 的注册商标 (®) 或服务标志 (SM)。该产品与本文提及的第三方商标所有者没有任何关联，亦未得到其认可、赞助或支持。

ClickHouse 是 YANDEX LLC 的商标。

MITRE 公司使用条款

授权许可

MITRE 公司 (MITRE) 特此授予您非排他性、免版税的授权许可，允许您将 ATT&CK® 用于研究、开发和商业目的。您为此类目的进行的任何复制操作均被授权，前提是您在任何此类副本中保留了 MITRE 的版权标记和本授权许可。

“© 2025 MITRE 公司。该产品的复制和分发得到了 MITRE 公司的许可。"

免责声明

MITRE 并未声称 ATT&CK 框架已囊括其攻击方模型及技术框架体系中所记载的各类行动与行为的所有可能性。借助 ATT&CK 框架中的信息应对各类攻击技术，或对这些技术进行全面防控，并不足以保障防御无死角 —— 因为可能存在 ATT&CK 框架未记载的未公开技术，或是现有技术的衍生变体。

所有文档及其包含的全部信息均按“原样”提供。贡献者、其所属或赞助机构（如有）、MITRE 公司、其董事会成员、管理人员、代理人与雇员均否认所有明示或暗示的担保，包括但不限于关于信息使用不侵犯任何权利的担保，以及对适销性或特定用途适用性的任何暗示担保。