DEVICE STATUS GUARDIAN

设备状态守护系统
操作手册

设备接入 · 实时监控 · 告警闭环 · 通知联动 · 系统运维

实时监控	智能告警	自动联动
持续掌握设备连接与运行状态	规则、防抖、恢复和处置闭环	异常触发控制动作与通知

适用版本 Device Status Guardian 1.18.x 及后续兼容版本。本样稿用于确认官网在线预览样式。

RESPX · 2026

CONTENTS

目录

从快速部署到日常维护的完整操作路径。

阅读建议 首次部署请依次阅读第 2、3、4 章；值班人员可重点阅读告警处置和日常检查。

01 • OVERVIEW

系统概览

将设备数据转化为可发现、可通知、可处置、可追溯的现场事件。

核心能力

设备与采集	OPC UA 服务器、订阅分组、设备与点位组织。
监控与告警	实时状态、告警规则、防抖、确认、恢复和归档。
通知与联动	SignalR、插件通知渠道、联动规则与设备操作。
平台与运维	用户权限、审计日志、内网穿透、插件与在线升级。

典型工作流程

01	采集 持续读取设备与点位数据。
02	判断 规则引擎识别异常与恢复条件。
03	触达 通过实时消息、语音或插件渠道通知人员。
04	处置 人工确认或自动联动，并保留审计记录。

运行原则 先确保采集稳定，再配置告警；先验证通知渠道，再启用自动联动。

02 • QUICK START

快速开始

完成部署后的首次登录和基础健康检查。

部署前准备

- Windows 主机具备 .NET 10 运行环境，并准备可写的数据目录。
- 确认 OPC UA 服务器地址、认证方式、证书策略和防火墙端口。
- 生产环境通过 HTTPS 或反向代理访问，并定期备份数据库与配置。

首次启动

01	**启动服务** 运行 DeviceStatusGuardian.exe 或注册为 Windows 服务。
02	**创建管理员** 首次访问完成管理员账户初始化，并使用强密码。
03	**检查系统状态** 确认数据库、告警服务、通知服务和实时连接均正常。
04	**获取机器码** 在系统配置的许可证区域复制当前机器码。

建议 先在测试设备上完成完整链路验证，再批量导入生产点位。

日常登录后检查

- 首页设备在线率和活动告警是否符合现场情况。
- 系统日志中是否存在持续重连、认证失败或通知发送失败。
- 许可证有效期、点位使用量和版本更新状态是否正常。

03 • DEVICES

设备与订阅

建立从 OPC UA 服务器到监控点位的稳定数据链路。

添加 OPC UA 服务器

01	**填写端点** 输入 opc.tcp 地址、名称及连接超时。
02	**配置安全** 选择安全策略、认证方式并处理服务器证书。
03	**测试连接** 确认连接成功后再保存，观察是否持续在线。
04	**创建订阅** 按区域或业务创建订阅分组，添加需要监控的节点。

点位组织建议

> 设备分组按产线、车间或站点组织；订阅分组按业务和刷新频率组织。

> 点位名称应包含设备、部件和含义，避免只使用原始 NodeId。

> 高频点位与普通状态点分开订阅，降低无效数据压力。

连接异常 优先检查网络、防火墙、端点地址、系统时间和证书信任；不要在持续失败时反复创建重复服务器。

上线验收

> 断开网络后设备状态能及时变为离线。

> 恢复网络后订阅自动恢复且数值继续更新。

> 关键点位的数据类型、单位与现场实际值一致。

04 • ALARMS

告警与通知

让异常被准确识别、及时送达并形成处置闭环。

创建告警规则

01	选择目标 指定服务器、订阅和监控点位。
02	设置条件 配置比较方式、阈值、严重级别和提示内容。
03	设置防抖 通过持续时间过滤瞬时波动和通信抖动。
04	验证恢复 确认条件解除后能够生成恢复记录。

通知渠道

- 先在通道管理中完成配置测试，再关联到正式告警规则。
- 不同级别使用不同通知范围；严重告警建议使用至少两个渠道。
- 语音、短信、WxPusher、NapCat、DTU 等能力可通过插件扩展。

告警处置	活动告警应经过确认、处理和解决。恢复只表示触发条件解除，不等同于人员已完成处置。

避免告警风暴

- 为波动信号设置合理防抖和恢复阈值。
- 按设备或区域规划通知对象，避免所有人接收所有告警。
- 定期复盘高频告警，修正规则或处理设备根因。

05 • AUTOMATION

联动与权限

在可控范围内自动响应异常，并确保操作责任清晰。

联动规则

- 明确触发来源、执行目标、写入值和恢复动作。
- 启用前先使用测试点位验证，不直接操作关键生产设备。
- 为重复触发设置冷却或状态判断，避免频繁写入。

安全边界

联动控制不能替代 PLC 和安全仪表系统。紧急停机、安全联锁等功能必须由经过认证的现场控制系统承担。

角色与访问范围

角色	建议权限
管理员	系统配置、用户、设备、通道、插件和许可证管理。
高级用户	规则维护、订阅管理和告警分析。
值班人员	监控、确认告警和查看相关记录。
操作员	仅访问授权设备组、订阅组和允许的控制操作。

- 遵循最小权限原则，离职或岗位变化后及时回收权限。
- 定期检查审计日志，关注登录失败、配置变更和设备控制操作。

06 • MAINTENANCE

许可证与系统维护

完成许可证导入、数据备份、升级和常见故障处理。

许可证申请与导入

01	**复制机器码** 在系统配置的许可证区域获取完整机器码。
02	**领取许可证** 在官网许可证服务页输入授权 Key、客户名称和机器码。
03	**下载 .lic** 保存许可证文件，并妥善保管原授权 Key。
04	**导入验证** 回到系统配置导入许可证，确认版本、点位和有效期。

重要 许可证签发时间即开始时间，许可证与机器码绑定。更换主机或机器码变化时需要重新授权。

备份清单

- 主系统数据库、应用配置、插件配置和通知模板。
- 许可证文件和许可证导入审计记录。
- 许可证门户的 App_Data、私钥、Pepper 和存储加密密钥。

升级建议

- 升级前确认版本说明、完成数据库和配置备份。
- 先在测试环境验证插件兼容性，再升级生产环境。
- 升级后检查系统版本、服务状态、设备连接、告警和通知。

APPENDIX • TROUBLESHOOTING

快速排障

按现象快速定位网络、配置、授权和实时通信问题。

现象	检查方向
许可证校验失败	确认签发私钥与客户端公钥配对，机器码一致，时间在有效期内。
设备持续离线	检查网络、端点、安全策略、账号、证书和 OPC UA 服务状态。
告警未通知	检查规则是否触发、通道测试、模板、接收对象和发送日志。
页面数据不刷新	检查浏览器连接、SignalR、反向代理 WebSocket 和服务日志。
无法重新下载许可证	确认使用原授权 Key，许可证仍在有效期且未被管理员撤销。
升级后插件不可用	确认插件 API 兼容版本、启用状态、配置文件和插件加载日志。
远程访问异常	检查 FRP 配置、服务状态、映射端口和公网入口策略。

排障顺序 先确认服务状态和网络，再检查配置与权限，最后查看日志。修改前保留现场信息，避免一次调整多个变量。

需要准备的信息

- 系统版本、操作系统版本和问题发生时间。
- 相关设备、订阅、规则或通知通道名称。
- 浏览器控制台、系统日志和通道发送日志中的错误信息。

- 文档结束 -