



TianshanOS

▽ The device management system for RM-01

ROOT / USER DOCUMENTATION

TianshanOS

运维指南

Root Operations Guide

编写依据版本：0.6.3 / Based on version 0.6.3

本指南依据 TianshanOS 0.6.3 编写。后续版本中未变化的功能和操作，仍可参考本指南。若界面、提示或操作结果不同，请查阅所用版本的说明。

This guide is based on TianshanOS 0.6.3. It can still be used with later versions where features and steps remain unchanged. If controls, messages, or results differ, check the guidance for your installed version.

目录 / Contents

点击章节名称即可跳转。 / Select a chapter to jump to it.

TianshanOS root 运维指南4

第一部分：日常功能4

1. 开始使用4

2. 系统状态与常用操作5

3. 设备面板6

4. 风扇管理8

5. LED 管理10

6. 网络管理10

7. 文件管理12

8. OTA 更新14

9. 安全管理入口16

第二部分：root 专属功能16

10. 终端与系统日志16

11. 管理和运行远程指令18

12. 自动化管理21

13. 配置与备份28

TianshanOS Root Operations Guide32

Part I: Routine Functions32

1. Getting Started32

2. System Status and Routine Operations33

- 3. Device Panel 35
- 4. Fan Management 36
- 5. LED Management 38
- 6. Network Management 39
- 7. File Management 41
- 8. OTA Updates 42
- 9. Security Management Entry 44
- Part II: Root-only Functions 45
 - 10. Terminal and System Logs 45
 - 11. Manage and Run Remote Commands 46
 - 12. Automation Management 50
 - 13. Configuration and Backup 58

TianshanOS root 运维指南

本指南面向使用 root 账户的用户。第一部分包含日常功能，第二部分介绍终端、远程指令、自动化和配置备份。root 操作可能影响设备和远程主机；执行前确认目标和正在运行的任务。安全管理请参阅单独的安全指南。

按设备页面显示的功能操作。部分选项需要指定硬件或配置才会出现。电脑上将指针停在图标按钮上，可查看按钮名称。手机表格较宽时，在表格内左右滑动查看其他列。

第一部分：日常功能

1. 开始使用

进入 WebUI

1. 在浏览器中打开管理员提供的设备网页地址（WebUI）。
2. 点击页面右上角的“登录”。
3. 输入 root 和设备提供的 root 密码。
4. 点击“登录”。登录成功后，右上角会显示当前用户名。

使用默认密码登录后，页面会显示“安全提醒”。输入当前密码，再输入两次新密码，点击“立即修改”。两次新密码必须一致。点击“稍后修改”可关闭提醒。

使用完毕后，点击右上角的“退出登录”。再次操作设备时需要重新登录。

切换语言

点击页面顶部的语言按钮，在菜单中选择中文或 English。页面内容和按钮名称会立即切换到所选语言。

页面导航

root 可使用以下入口：

- “系统”：查看设备状态，控制模组、风扇和 LED，并进入 OTA 升级。
- “网络”：查看以太网和 DHCP 状态，设置 WiFi 和 NAT 网络转发。
- “文件”：管理 SD 卡和 SPIFFS 中的文件。
- “终端”：执行设备命令并查看系统日志。
- “指令”：管理和运行远程 SSH 指令。
- “自动化”：配置任务并保存应急副本。
- “安全”：进入单独的安全管理页面，详细操作请查看安全指南。

2. 系统状态与常用操作

点击顶部导航中的“系统”进入系统页面。

查看资源与服务状态

“带外管理芯片资源监控”显示管理芯片的 CPU、DRAM 和 PSRAM 使用情况。这些读数不代表 AGX 或 LPMU 的资源使用率。

- 点击“详情”，查看内存总量、已用和空闲空间等信息。
- “服务”按钮显示运行中的服务数和服务总数。点击后可查看各项服务的状态和启动阶段。
- 服务状态异常时，先刷新。需要重启的服务按下方“重启单项服务”操作。

查看系统与电源信息

“系统总览”显示芯片、固件版本、ESP-IDF 版本和运行时间。日常使用主要核对固件版本；ESP-IDF 是设备所用系统框架的版本。

卡片右侧显示输入电压、内部电压、电流、功率和保护状态。

网络、风扇、温度和灯光等系统设置保存在设备内部。插入旧 SD 卡不会自动恢复这些设置。自动化配置另行管理，不要把应急副本当作整机备份。

保护状态旁的开关用于启用或停用低电压保护。启用后，设备会按保存的电压和等待时间，在低电压时关机、供电恢复后重新启动。

查看网络与时间

“网络与时间”显示以太网、WiFi、IP 地址、当前时间、同步状态、时间源和时区。

- 点击“同步时间”，将浏览器当前时间同步到设备。
- 点击“时区”，选择预设时区或填写页面支持的时区设置，然后保存。
- 点击“OTA 升级”，进入固件升级页面。

高级操作

重启 TianshanOS

重启会暂时中断 WebUI 和设备管理功能。先完成正在进行的操作，再点击“重启”并确认。等待设备恢复，然后重新打开 WebUI。

重启单项服务

重启服务会暂时中断该服务提供的功能。在“服务状态”中找到异常服务，点击该行的“重启”。操作完成后重新查看服务状态。

调整关机设置

这些设置决定设备在低电压时何时关机，以及供电恢复后何时重新启动。请按设备的供电要求填写电压和等待时间。

点击“关机设置”，可以调整以下内容：

- “低电压阈值”：低于该电压后开始关机倒计时。
- “恢复电压阈值”：高于该电压后开始恢复流程。
- “关机倒计时”：检测到低电压后等待多久执行关机。
- “恢复保持时间”：电压恢复后等待多久确认供电稳定。
- “风扇停止延迟”：关机后等待多久关闭风扇。

保存后，页面会应用新的保护设置。

切换顶部 USB 连接目标

切换 USB 目标可能使当前连接的外设暂时断开。确认目标设备和正在进行的工作后再操作。

设备提供 USB 切换功能时，页面会显示“USB”按钮。每点击一次，顶部 USB 接口按 ESP、AGX、LPMU 的顺序切换到下一个目标。查看按钮上的目标名称和页面提示，确认切换结果。

3. 设备面板

“设备面板”位于“系统”页面，包含模组电源控制、快捷操作和数据组件。

控制 AGX 和 LPMU

关闭模组前，先保存其中的工作并完成正常关机流程。强制断电可能造成未保存的数据丢失。

- “AGX 电源”显示电源控制状态。点击按钮可上电或断电；操作后等待页面确认。
- “LPMU 电源”显示“在线”“离线”或“未知”。在线表示网络能够连通，离线表示网络无法连通。这些状态不能单独证明模组已开机或关机。
- 点击 LPMU 按钮会触发一次与物理电源按钮相同的操作。随后等待检测和页面提示；结果未知时，先检查模组和网络，不要连续点击。

使用快捷操作

快捷操作卡片由 root 用户配置。显示卡片和允许手动运行是两项设置；看得到卡片，不代表可以启动任务。

1. 查看卡片名称和说明，确认将要执行的任务。
2. 点击卡片，阅读结果提示。处理中不要再次启动。
3. 提示已执行或已排队后，还要确认目标设备或任务的实际结果。需要核验、查看日志或停止后台服务时，点击“后台运行”，步骤见第 11 章。

无法启动时，按提示处理，不要连续点击：

- 规则已停用，或不允许手动触发：在“自动化”检查规则设置，方法见第 12 章。看得到卡片，不代表可以运行。
- 任务或后台操作正在处理：等待结果，不要重复启动。
- 同一任务已有后台运行记录：在“后台运行”核验原任务，确认结束后再启动。
- 配置尚未加载、缺少关联项或自动化已暂停：在“自动化”检查配置和启停状态，方法见第 12、13 章。

完成一次点击后，等待几秒再启动其他操作。关闭页面、删除卡片或重启 TianshanOS，都不会替你停止远程主机上的后台服务。

长按卡片，出现排序提示后拖动，可以调整显示顺序。

没有卡片时，先阅读说明。配置加载中就等待；页面报告无法加载时，保留原因，在“终端”打开“系统日志”检查。只是没有配置快捷操作时，点击“打开自动化”，检查规则的“显示在面板”设置。

规则修改或导入后，当前配置会更新，不需要为了切换规则而重启。卡片任务刚被调整时，先核对规则的条件、动作和目标，再执行。

不要为了恢复卡片，自行重启正在提供服务的设备。

管理数据组件

数据组件用于在“设备面板”中持续显示设备数据。

1. 点击“组件管理”。
2. 选择刷新闻隔，或关闭自动刷新。
3. 添加预设组件，或选择页面提供的组件样式和数据来源。
4. 根据需要编辑名称、显示方式和单位，然后保存。

已有组件可以编辑、删除和调整顺序。也可以直接点击组件卡片进入编辑界面。长按组件后拖动，可以改变它在面板中的位置。

4. 风扇管理

“风扇控制”位于“系统”页面。卡片显示设备提供的风扇。设置曲线前，核对风扇编号。

查看风扇状态

顶部显示“有效温度”和“当前输出”。卡片上的大百分比是设备确认已设置的调速值，不是实测转速。RPM 表示测得的每分钟转数，没有有效读数时不显示。大百分比显示 --，表示当前输出尚未确认。

拖动手动滑块时，滑块旁显示准备设置的值，大百分比仍显示当前输出。松开滑块后，查看提示和更新后的读数。“请求设置”与当前输出不同，说明不能只凭请求值判断调速已经生效。

智能模式会显示运行状态，例如“智能模式”“按曲线运行”“保护介入”或“温度失效”。页面还提供“安全参考”“45 秒预测”和“升温速度”。

出现“温度失效”时，检查温度来源是否仍在更新。设备会采用温度失效时的保护调速。点击“TTI”可查看智能热控说明。

点击区域顶部的刷新按钮，重新获取状态。出现“未能完成风扇调节”或输出未确认时，检查设备状态后再决定是否重试。

选择运行模式

模式	作用
“关闭”	停止风扇。
“手动”	用滑块设置固定的调速百分比，范围为 0-100%。
“曲线”	按已设置的温度与调速百分比对应关系运行。
“智能”	以基础曲线为参考，根据温度趋势和过去的调速情况调整散热；需要保护时采用保护调速。

关闭风扇或设置过低的手动值会降低散热能力。执行前确认设备负载和温度，并持续观察。只有在手动模式且当前输出已确认时，滑块才可调节。

设置风扇曲线

点击“风扇控制”区域顶部的“曲线”，打开“风扇曲线管理”。卡片内的“曲线”只切换运行模式。

1. 在“风扇”中选择要调整的编号，并与系统页卡片核对。
2. 在“温度变量绑定”中点击“添加变量”，选择温度来源并填写权重。
3. 点击“绑定”。绑定的温度来源由曲线、智能模式的风扇共用，修改会影响使用该来源的风扇。
4. 在“曲线节点”中添加或编辑节点。每条曲线至少需要 2 个节点，最多支持 10 个。
5. 设置“最小转速”和“最大转速”。这里填写的是调速百分比，最小值不能高于最大值。
6. 设置“温度回差”和“最小调节间隔”。回差范围为 0-20° C，可减少温度小幅波动造成的频繁调速。间隔范围为 500-30000 ms，1000 ms 等于 1 秒。
7. 点击“保存曲线”。成功后，设置被保存，所选风扇切换到曲线模式。若希望继续使用智能热控，返回风扇卡片点击“智能”。

保存失败时，先查看具体提示并检查当前状态，再决定是否重试。解除温度绑定后，也应检查有效温度和风扇状态。

导入和导出曲线

- 点击“导入配置”，选择曲线 JSON 文件。JSON 是保存曲线数据的文件格式。检查载入的节点、限制和风扇编号，再点击“保存曲线”使其生效。
- 点击“导出配置”，浏览器会下载当前曲线，并尝试将副本保存到 SD 卡的 /sdcard/config 目录。分别检查浏览器下载结果和页面提示的 SD 卡保存结果。

使用测试温度

测试温度会临时替代正常温度来源，并影响曲线或智能调速。测试期间持续观察风扇和设备状态。

1. 在“测试温度”中输入 0-100° C。
2. 点击“测试”，观察当前输出、状态和风扇响应。
3. 测试结束后点击“清除测试”，恢复正常温度来源，并确认有效温度已恢复。

5. LED 管理

“LED 控制”位于“系统”页面，只显示设备提供的 LED。不同 LED 可用的功能不同。

常用控制

- 使用卡片底部的灯泡按钮开启或关闭 LED。
- 拖动“亮度”滑块调整亮度，或选择颜色和预设色。
- 点击动画按钮进入“LED 设置”，在“程序动画”中选择动画并使用对应的播放或停止按钮。
- 点击卡片右下角的保存图标，保存当前 LED 配置。
- 点击“全部关闭”关闭所有 LED，并查看页面报告的结果。部分关闭失败时，检查对应设备。

LED 矩阵高级功能

矩阵设备的卡片提供相应功能图标，打开后可在“LED 设置”中切换分组：

- “程序动画”：选择和运行动画。
- “图像/QR码”：从 SD 卡选择图像，或输入内容生成 QR 码。
- “文本显示”：填写文字，并设置字体、对齐、滚动、前景色和背景。
- “后处理滤镜”：选择滤镜及参数，再应用或停止。
- “色彩校正”：调整显示效果，并按页面按钮重置、导入或导出设置。

操作后检查灯光或矩阵画面。只使用页面提供的功能。设置失败时，按提示检查文件、输入和设备状态。

6. 网络管理

点击顶部导航中的“网络”进入“网络设置”。修改网络模式、热点或 NAT 设置可能断开 WebUI。保存前，确认能用新的网络地址重新连接设备。

查看网络状态

页面顶部显示以太网、WiFi 客户端和 WiFi 热点的连接状态。进入对应面板，可以查看 IP 地址、子网掩码、网关、DNS、MAC 地址、SSID、信号和接入设备数量等信息。

以太网面板用于查看当前链路和地址信息，不提供地址修改入口。

选择 WiFi 模式

模式	作用
“关闭”	关闭 WiFi。
“站点 (STA)”	让设备连接现有 WiFi 网络。
“热点 (AP)”	让设备提供 WiFi 热点。
“STA+AP”	同时连接现有 WiFi，并保留设备热点。

选择模式后等待页面刷新状态。切换模式期间，当前无线连接可能暂时断开。

连接 WiFi

1. 将 WiFi 模式设置为“站点 (STA)”或“STA+AP”。
2. 在“站点连接”中点击“扫描”。
3. 从列表中选择网络。列表会显示 SSID、信号强度、信道和认证方式。
4. 输入密码并确认。开放网络可以将密码留空。
5. 等待状态变为“已连接”，并确认页面显示新的 IP 地址。

点击“断开”可以结束当前 WiFi 客户端连接。

配置 WiFi 热点

1. 将 WiFi 模式设置为“热点 (AP)”或“STA+AP”。
2. 在“热点”区域点击“配置”。
3. 填写 SSID。密码留空会创建开放热点；设置密码时至少输入 8 位字符。
4. 选择信道，并根据需要启用“隐藏 SSID”。
5. 点击“应用”，等待热点状态更新。

点击“设备”可以查看当前连接到热点的设备。

设置主机名

在“网络服务”的“主机名”区域输入新名称，然后点击“设置”。主机名更新后，页面会显示当前名称。

查看 DHCP 客户端

DHCP 会自动为接入设备分配网络地址。点击“客户端”，选择“WiFi AP”或“Ethernet”，查看当前分配记录。点击刷新按钮可以重新加载列表。

高级网络操作

设置 NAT 网关

NAT 用于在设备的网络接口之间转发网络流量。启用或停用 NAT 后，点击“保存”保留当前设置。操作完成后检查 WiFi 和 Ethernet 状态。

通过 LPMU 接入上层网络

此操作通过已配置的 LPMU 主机接入网络。先确认能连接 LPMU、网络线缆已接好，再准备该主机 SSH 账号的 `sudo` 密码。这个密码用于允许账号修改系统设置，可能与 WebUI 登录密码不同。

1. 在“接入上层网络”区域点击“通过 LPMU 接入”。
2. 在弹窗中输入“LPMU sudo 密码”，再点击接入按钮。密码仅用于本次操作，不保存；下次执行需要重新输入。
3. 等待处理结束，不要重复启动。
4. 结果窗口显示互联网连接正常和网络配置已完成时，才表示接入成功。
5. 失败或结果未确认时，先阅读具体原因；需要更多信息时展开“执行日志”。密码错误时核对密码，找不到互联网连接时检查网络接线与上层网络。

状态获取失败不等于脚本已经停止。先点击页面提供的“刷新状态”确认当前执行情况，再决定是否重新接入。

7. 文件管理

点击顶部导航中的“文件”进入“文件管理”。

SD 卡是可插拔存储，SPIFFS 是设备内部文件存储。点击“SD 卡”或“SPIFFS”切换位置。页面上方显示当前文件夹路径；点击路径中的文件夹名称，可以返回上一级或更早的目录。

浏览和管理文件

- 点击文件夹名称进入该目录。
- 点击文件右侧的下载按钮，将文件保存到浏览器的下载位置。
- 点击重命名按钮，输入新名称并确认。
- 点击“新建文件夹”，输入文件夹名称并创建。
- 点击刷新按钮重新加载当前目录和存储状态。

上传文件

文件只能上传到 SD 卡，不能上传到 SPIFFS。先确认 SD 卡已挂载。

1. 点击“SD 卡”，进入要上传文件的目录。
2. 点击“上传文件”。
3. 点击上传区域选择一个或多个文件，或将文件拖入该区域。
4. 检查上传列表，移除不需要的文件。
5. 点击“上传”，等待每个文件显示完成状态。

上传 `.tscfg` 配置包后，页面会显示配置包的验证和应用步骤。但当前文件上传入口不会应用包中的设置；上传或验证成功，不代表设置已经生效。

规则配置包请从“自动化”页面导入，步骤见第 12 章。不要用普通文件上传代替规则导入。其他配置包的来源和签名说明见安全指南。

批量操作

勾选文件或文件夹后，页面会显示批量工具栏。

- “批量下载”下载选中的文件。文件夹不会加入下载内容。
- “批量删除”删除选中的文件和文件夹。
- “取消选择”清除当前选择。

删除文件或文件夹

删除操作无法从 WebUI 撤销。删除文件夹时，其中的全部内容也会被删除。确认名称和路径后，再点击“删除”或“批量删除”并确认。

自动化管理的文件受到保护。向 `/sdcard/config/automation` 上传或覆盖文件，以及删除、重命名这个目录或包含它的父目录，可能被拒绝。看到“这是自动化使用的配置文件”时，请从“自动化”的“配置与备份”或对应列表处理，不要改用终端绕过限制。

挂载和卸载 SD 卡

卸载后，SD 卡中的文件会暂时无法访问。先确认上传、下载等文件操作已结束，再点击“卸载 SD”。

卸载或换卡可能让自动化改用内部应急配置。这份配置可能较旧，已启用的自动规则仍可能运行；没有可用副本时，自动化可能无法运行。先核对应急配置和任务，确认允许卸载，方法见第 13 章。卡上的图片、字体和日志会暂时无法访问。

SD 卡未挂载时，页面会显示“挂载 SD”。点击该按钮，等待存储状态变为“已挂载”，随后重新进入 SD 卡目录。

挂载成功不等于已改用卡内自动化配置。重新插卡后，按第 13 章选择使用哪份配置，不会自动覆盖或合并。

8. OTA 更新

在“系统”页面的“网络与时间”区域点击“OTA 升级”，进入“固件升级”。

更新过程中设备会重启，WebUI 会暂时断开。开始前应保存正在进行的工作，并保持设备供电稳定。升级进度尚未完成时不要关闭设备。

首次从旧版本升级到 0.6.3

首次从 0.6.2 等旧存储布局升级时，需要发行方确认的配套 USB / 串口升级包。只上传主固件或 WebUI，不能完成这次升级。请设备管理员或提供方按包内说明操作，不要自行全片擦除或使用旧分区表。

升级前保存重要文件，保留原 SD 卡。首次启动会迁移原配置，期间不要断电。完成后，检查登录、网络、风扇、灯光、SSH 主机和自动化规则。不要在尚未确认规则内容时测试带有断电、重启或远程命令的任务。

该配套包会更新两个应用槽，不能假定另一个槽仍保留旧版本。忘记 root 密码时，只使用提供方确认与 0.6.3 布局匹配的恢复方案，不要刷入旧版密码重置固件。

下面的网页更新方法用于发行方确认可通过 OTA 安装的版本，不能代替首次布局升级。

从 OTA 服务器检查更新

1. 查看页面显示的“当前版本”。
2. 在“OTA 服务器”中输入管理员或发行方提供的服务器地址。
3. 点击“保存”，随后点击“检查更新”。
4. 页面会显示“发现新版本”“已是最新版本”“服务器版本较旧”或错误信息。
5. 确认目标版本后，点击“立即升级”或页面显示的升级按钮。
6. 等待下载、安装和重启完成。需要中止时，使用页面显示的中止按钮；只在按钮可用的阶段操作。
7. 等待页面确认升级后的固件，再重新连接 WebUI，核对“当前版本”和设备状态。

“升级进度”单独显示当前阶段。进度达到 100% 或显示文件已写入，不代表重启和版本核对已完成。出现“升级结果未确认”或“启动的固件与升级目标不符”时，保留提示，检查设备当前版本；不要直接重复升级。无法确认时，先查看系统日志，需要时联系设备提供方。

升级同时包含 WebUI 时，固件和 WebUI 会依次更新。请使用同一发布版本的配套主固件和 WebUI 资源。升级后仍显示旧界面时，尝试强制刷新浏览器，再核对版本和页面。

手动升级

展开“手动升级”后，可以选择以下方式：

- “从 URL 升级”：填写固件 URL，根据发布说明勾选“同时升级 www”，然后点击“升级”。www 指设备网页界面的资源文件。
- “从 SD 卡升级”：填写固件文件路径，例如 /sdcard/firmware.bin。勾选“同时升级 www”时，确保同目录中也有该版本的 www.bin。

从 URL 升级时，“跳过证书校验”用于跳过 HTTPS 服务器证书验证。勾选后，设备无法通过该证书确认下载服务器的身份。日常升级请保持未勾选；遇到证书错误时，请先联系管理员检查服务器地址和证书。

分区管理与回滚

“分区管理”显示当前运行分区和其他可用分区。

- “标记有效”会确认当前运行版本，并取消该版本的自动回滚保护。确认当前版本运行正常后再执行。
- “回滚到此版本”会选择另一可启动版本，并通过重启切换。回滚会中断当前服务，执行前应确认目标版本和相关数据兼容。

操作完成并重启后，重新打开 WebUI，核对当前版本和设备状态。

0.6.3 改变了配置保存方式和设备分区布局。不要直接回退到不兼容的旧固件。确需降级时，请设备提供方确认完整的固件、布局和配置恢复方案。

回滚不会恢复旧配置格式，也不保证旧规则可用。

9. 安全管理入口

点击顶部导航中的“安全”进入安全管理页面。SSH 密钥、远程主机、主机指纹、HTTPS 证书、配置包和账户管理的操作请查看《TianshanOS 安全指南》。本指南不重复这些内容。

遇到失败或结果未确认

字段旁出现红色错误说明时，按提示修正后再保存。标记消失不代表已经保存成功；还要检查保存提示和列表。

先看哪项操作失败，再阅读原因和下一步。提示没有说明原因时，不要猜测。

有“详情”时，点击查看。点击“收起”可隐藏详情。页面提供 × 时，可点击它关闭提示。需要进一步检查时，保留提示和详情，在“终端”打开“系统日志”检查。

出现“结果未确认”时，先刷新并检查设备、文件或任务状态。超时或断开连接不代表操作没有执行；不要立即重复断电、删除、启动任务或升级。仍无法确认时，在“终端”打开“系统日志”查看原因。

批量操作后，分别核对成功、失败和未确认的项目。下载文件后，检查浏览器下载列表。

第二部分：root 专属功能

10. 终端与系统日志

“终端”只对 root 显示。它可以直接执行设备控制台命令，也可以查看设备日志。命令可能立即改变设备状态，输入前应确认命令来源、参数和影响。

连接并使用终端

1. 点击顶部导航中的“终端”。
2. 等待页面显示“已连接到设备”和 `tianshan>` 提示符。
3. 输入 `help`，查看当前固件提供的命令。
4. 输入命令并按 `Enter`。等待输出结束并重新出现提示符。

页面显示“未连接到设备”时，输入不会执行。连接断开后页面会提示重新连接；恢复连接后再提交命令，避免重复执行。

终端提供以下键盘操作：

操作	作用
Ctrl+C	清除当前输入，并请求中断命令；能否停止取决于命令是否支持中断。
Ctrl+L	清屏。
↑ / ↓	查看本次页面会话中的命令历史。
← / →	在当前输入中移动光标。

页面顶部的“清屏”只清除当前显示，不会撤销已经执行的命令。“断开”会结束当前终端连接。

进入远程 SSH Shell

SSH Shell 会把后续键盘输入发送到远程主机。连接前应确认目标地址、用户和认证方式，并完成安全指南中的 SSH 准备工作。

1. 输入 `ssh --help`，查看 SSH 命令说明。
2. 按以下格式填写实际主机地址和用户名：`ssh --host <主机地址> --user <用户名> --shell`。尖括号及其中的文字都需要替换。需要指定端口时，在 `--shell` 前添加 `--port <端口>`。
3. 等待终端显示远程连接成功，再输入远程命令。
4. 按 `Ctrl+\` 退出 SSH Shell，返回 `tianshan>` 提示符。

不要在屏幕共享、录屏或可被他人查看的终端中输入明文凭据。

查看系统日志

点击终端页顶部的“系统日志”打开日志窗口。

- “级别”控制最低显示级别。选择 `ERROR`、`WARN+`、`INFO+` 或 `DEBUG+` 可以缩小日志范围。
- “TAG”按日志来源筛选。
- “搜索”按关键词筛选当前日志。
- “自动滚动”开启时，页面会跟随最新日志。
- 刷新按钮会重新读取历史日志。
- 清除按钮只清除当前窗口中的日志显示。

筛选后没有内容时，可以先清空 TAG 和关键词，再调整级别。关闭日志窗口不会停止设备服务。

查询自动化保存位置

需要命令行检查时，可输入 `auto --config status` 查看当前配置位置和副本状态。其他可用选项以 `auto --help` 为准。旧的 `config --sync` 已移除；日常备份和恢复请使用第 13 章的网页操作。

11. 管理和运行远程指令

“指令”用于保存可重复使用的 SSH 命令，并在选定的远程主机上运行。远程主机及其认证信息在“安全”页面管理；具体操作请查看安全指南。

连接前核对主机指纹

指纹用于核对你连接的是哪台主机。以下步骤适用于网页“安全”中的 SSH 主机测试，不是终端 SSH Shell 的确认流程。提示主机指纹未登记或发生变化时，不要反复执行指令。进入“安全”，找到目标 SSH 主机，点击“测试”。

首次连接时，确认框会显示主机地址和指纹。通过可信渠道向主机管理员核对，确认一致后才点击“信任并连接”。

指纹变化时，确认框会显示已保存的指纹和当前指纹，默认选中“取消”。重装系统可能改变指纹，也可能是连接到了其他主机或有人冒充主机。

核对地址，并通过可信渠道确认变化原因。不能确认时，点击“取消”。不要删除旧指纹来跳过核对。确认新指纹可信后，才点击“更新主机密钥”。

选择主机并查看指令

1. 点击顶部导航中的“指令”。
2. 在“选择主机”中选择页面显示的主机。
3. 在“命令列表”中查看该主机已有的指令。

“孤儿命令”表示指令引用的主机已经不存在，不能执行。先核对主机配置。需要保留任务时，在有效主机下重建指令，更新使用它的模板和规则，检查结果后再清理孤儿命令。

新建或编辑指令

保存的指令会在远程主机上执行。创建前应先在目标主机上人工确认命令及权限，避免把删除、关机、重启或覆盖文件等操作配置成容易误触的指令。

1. 选择主机后点击“新建指令”。编辑现有指令时，点击该指令的编辑按钮。
2. 填写“指令 ID”。ID 必须唯一，只能使用字母、数字、下划线和连字符，且不能以下划线或连字符开头或结尾。
3. 填写“指令名称”和“SSH 命令”。多行命令每行填写一条。
4. 根据需要填写描述，并选择图标或 SD 卡中的图像。
5. 检查运行方式和输出匹配选项，然后点击“保存”。

名称帮助你辨认指令，ID 用于让自动化找到它。编辑现有指令时，ID 不能修改。要使用新 ID，请新建指令，并更新使用它的动作模板和数据源。

执行并查看结果

1. 点击指令卡片上的执行按钮。
2. 在“执行结果”中观察输出和状态。
3. 页面显示“取消”时，可以请求中断当前执行会话。随后查看状态和输出，确认是否已停止；已完成的远程操作不会撤销。
4. 点击“清除”移除当前结果显示。

“清除”不会撤销远程主机已经完成的操作。执行结果中的成功、失败、提取内容和最终状态取决于指令的匹配设置。

配置结果匹配

结果匹配用于把远程输出转换为容易判断的状态。

- “期望匹配”：输出包含指定文本时标记成功。
- “失败匹配”：输出包含指定文本时标记失败。
- “提取正则”：使用一个 (.*) 捕获组保存输出中的目标内容。
- “命中即停止”：匹配成功后终止仍在持续运行的命令。
- “超时 (秒)”：等待匹配结果的时间，以秒为单位。该设置仅在配置成功或失败匹配模式，或启用“命中即停止”时生效。
- “变量名”：保存状态和提取结果，供自动化页面选择。

成功和失败文本应选择稳定、明确的输出。过于宽泛的文字可能造成误判。保存后先执行一次并检查“匹配结果”，再把变量用于规则。

使用后台执行和服务模式

`nohup` 表示命令在远程主机后台继续运行，SSH 断开后仍可继续。后台任务不会因为关闭 WebUI 自动停止。

后台运行需要 SSH 密钥认证。先在“安全”完成公钥部署，再选择关联主机。不要在后台命令中保存明文密码。需要停止或核验原任务时，对应的密钥也必须仍然可用。

启用“后台运行 (nohup)”并执行后，从“指令”页点击“后台运行”。系统页的 root 入口和“自动化”页也可以打开同一列表。

1. 按任务名称、用户名、主机地址和端口找到原任务。
2. 点击“核验远端状态”，连接原主机检查这次运行。列表“刷新”只读取已知记录，不代替核验。
3. 点击“查看日志”读取原主机日志的最近 100 行。需要持续查看时，点击“实时查看”；“停止查看”只停止页面刷新。
4. 需要结束任务时，点击该记录的“停止”并确认。等待结果，再核验是否已停止；不要直接重复启动。

设备重启后，原记录会显示“待检查”。“无法确认远端状态”表示尚无法判断任务是已停止还是仍在运行。“上次结果”只说明上一次确认的结果，不保证此刻仍然相同。

读取失败不等于日志没有内容，也不代表进程已经退出。先检查原主机连接、日志路径和 SSH 密钥，恢复后再核验；不要因为检查失败而重新启动任务。

删除命令、更换主机配置或切换自动化配置，不会结束已运行的远端进程。原任务仍从“后台运行”管理；重建同名、同 ID 的命令，不会接管原任务。不要删除仍需用来控制原任务的密钥。

“服务模式”用于持续观察后台任务是否进入可用状态。启用后，必须填写“就绪匹配”和“变量名”；失败匹配和等待设置可按需要调整：

- “就绪匹配”：日志出现这些文字时标记为就绪，可用 | 分隔多个模式。
- “失败匹配”：日志出现这些文字时标记为失败。
- “就绪超时 (秒)”：等待就绪状态的最长时间，以秒为单位。
- “检测间隔 (毫秒)”：检查日志的间隔，1000 毫秒等于 1 秒。
- “变量名”：保存 checking、ready、timeout 等状态。

服务模式任务可能显示启动中、核验中、停止中或结果未确认。请求被接受后继续等待最终结果。若提示已有后台运行记录，回到原记录核验；确认任务结束后再启动。自动规则仍启用且条件满足时，服务可能再次启动；需要保持停止时，先停用这条自动规则。

导入和导出指令

- 点击指令的导出按钮，可以导出该指令，并按页面选项包含依赖的主机配置。
- 点击“导入指令”，选择 .tscfg 配置包，预览内容，再决定是否覆盖已有配置。

导入可能同时带入远程主机，并覆盖同 ID 配置。先核对预览中的指令、主机和覆盖内容，再确认导入。保存到当前配置后生效，不需要为此重启。已有远端进程不会因此停止或迁移到新主机。

新包导入会检查来源、签名、签发权限和目标设备。导出成功不保证能再次导入；设备证书仅用于 HTTPS 时，可能没有签发配置包的权限。遇到这类提示，请配置提供方处理，不要关闭验证。

删除指令前检查影响

点击删除后，先查看关联模板和规则。可以选择可用指令替换关联，或解除关联并停用相关规则；完整步骤见第 12 章。删除只修改当前使用的配置，另一份应急副本不会自动更新。

删除配置与停止远端服务是分开的操作。删除按钮不会停止服务，也不会撤销已经完成的操作。需要结束远端任务时，另到“后台运行”停止并确认结果。

12. 自动化管理

“自动化”把数据和操作连接成可重复执行的流程。先建立数据源和动作模板，再用规则决定何时执行。

自动执行：数据源 → 变量 → 规则判断 → 执行动作

手动执行：系统页快捷操作 → 执行动作

数据源读取数据，变量保存值，规则判断条件，动作模板定义任务。规则是否显示在设备面板、是否允许手动触发分别设置；自动规则也可以显示在面板中。

查看和控制自动化引擎

页面顶部显示引擎状态、规则数、变量数、数据源数、触发次数和运行时长。

操作	影响
“启动”	启动已停止的引擎；只有当前配置允许运行时，才会执行已启用规则。
“暂停”	暂停后续自动判断，已有动作可能继续。需要恢复时先停止，再启动。
“停止”	尝试停止规则判断、数据读取和后续动作安排，保留配置。等待确认；超时不表示已停止。
“重载”	重新读取当前使用位置的配置。先保存编辑内容，检查结果；已有的配置暂停设置不会因此解除。

操作前检查是否影响散热、告警或其他持续任务。停止引擎不能代替停止远程后台进程；远程任务需要在“后台运行”中停止并确认。

“配置与备份”中的“停用自动化”和引擎“暂停”不是同一项操作。页面显示“自动化已暂停”时，先检查配置，再点击“启用自动化”。仅重启设备、重载或停止再启动引擎，不会解除这项配置暂停。详见第 13 章。

完成一条最小自动化流程

1. 创建数据源，用测试功能确认连接及需要读取的字段。
2. 启用数据源，点击该行的“查看变量”图标，检查数值和更新时间。
3. 创建动作模板，检查参数后点击“测试”。测试会立即执行动作，先确认设备和远程主机允许本次操作。
4. 创建规则，暂时关闭“立即启用”，设置条件、冷却时间、动作顺序、延迟和重复方式。
5. 按需要设置“显示在面板”和“允许手动触发”。
6. 保存后再启用，观察变量、触发次数及实际结果。

管理数据源

点击“数据源”区域的“添加”，选择类型：

类型	用途
“REST API”	定期读取一个 HTTP 地址返回的数据。
“WebSocket”	接收持续连接推送的数据。
“Socket.IO”	接收 Socket.IO 服务的事件数据。
“指令变量”	读取已配置远程指令的结果。

1. 填写唯一 ID、显示标签和该类型要求的连接信息。
2. 使用测试功能确认连接。网络地址、认证和字段以数据提供方的信息为准。
3. 对前三种类型，从测试结果选择需要的数据字段。Socket.IO 事件名称留空时，测试可尝试发现事件。
4. 对“指令变量”，选择主机及已经配置变量名的指令，再设置检测间隔。
5. 在表单中检查启用开关，保存后用该行的“查看变量”检查结果。

数据源行提供启用开关、查看变量、导出和删除。停用或删除前，检查哪些规则还在使用它，以免影响任务。

导入和导出使用配置包。导入前预览 ID、类型及覆盖内容，按安全指南检查来源和信任要求。

查看变量

点击数据源行的眼睛图标“查看变量”，在弹窗中查看名称、类型、值和更新时间。远程指令也可从其变量入口查看结果。

- 确认名称和数据源正确，值与类型适合规则比较。
- 检查更新时间是否符合预期。窗口中的时间用于判断数据是否仍在更新。
- 没有数据时，检查数据源是否启用，再测试连接和字段选择；远程指令变量还需检查对应指令的执行结果。

创建和测试动作模板

点击“动作模板”区域的“添加”，选择任务类型：

类型	作用
“CLI 命令”	执行设备本地控制台命令。
“SSH 命令”	执行“指令”页已保存的远程指令。
“LED 控制”	控制 LED 的颜色、动画或矩阵内容。
“日志记录”	按指定级别写入日志。
“设置变量”	为自动化变量赋值。
“Webhook”	页面保留此选项，但当前动作执行功能尚未实现，不能用于发送请求。

填写唯一 ID、名称和当前类型要求的参数，可设置执行延迟与“异步执行”。异步操作在后台继续，提交后还需通过日志、变量或目标设备检查最终结果。

- CLI：填写命令行，可按需要设置结果变量和超时。
- SSH：选择已配置主机和指令，并核对预览。
- LED：选择设备和支持的功能，填写颜色、动画、亮度、文本、图像、QR 码或滤镜参数。
- 日志：选择级别并填写消息，可引用变量。
- 设置变量：填写变量名和值。
- Webhook：当前暂不可用，请选择其他已支持的动作。含 Webhook 的规则包也不能导入。

“测试”会执行动作。涉及断电、重启、远程命令或外部请求时，先确认影响，再测试。提示“已排队”只表示任务已接收，不代表执行成功；还要查看系统日志和目标设备的结果。

编辑后保存，再检查参数。保存失败，请保留草稿并按提示修正。导入可能覆盖已有模板；删除前检查影响清单。缺少图片或字体时，插入原 SD 卡，或重新选择可用资源。应急副本不会保存这些文件。

删除和替换关联配置

规则、动作模板、SSH 命令和主机的删除，会影响其他配置。删除前先保存所需应急副本；删除后不能从页面撤销。

1. 在对应列表点击删除图标，核对目标名称和受影响项。
2. 没有关联时，确认删除。有其他配置使用它时，按页面选择可用替换项，或选择“解除关联并停用相关规则”。
3. 确认后刷新列表。检查目标已移除，并核对关联模板、规则和启用状态。

删除动作模板时，解除关联会从相关规则中移除该动作，并停用规则。删除 SSH 命令时，关联模板会保留为停用草稿并清空命令引用；相关规则解除关联并停用。使用替换项时，先核对替换后的目标和动作，不能只看名称相似。

删除主机时，也要检查受影响的指令和数据源。缺少主机的指令不能执行；在有效主机下重建需要的指令并更新关联，检查后再使用。不要把删除本地主机配置与撤销远端公钥当作同一操作，具体见安全指南。

需要最终强制删除时

普通方式无法完成时，可选择“最终强制删除”。阅读说明后再确认；它会删除目标，并清理能确认的关联、停用受影响规则。强制删除不会停止远端后台服务。

影响无法完整确认时，页面会要求勾选“我确认暂停自动化，并继续删除。”。确认后自动化保持暂停。检查剩余配置并修正问题，再从“配置与备份”点击“启用自动化”。不要靠重启恢复运行。

配置在确认期间变化时，点击“重新检查删除影响”，重新核对清单，再确认。存储写入失败时，强制删除也不能保证完成；重新读取列表检查，不要把卡片消失当作删除已保存。

创建规则

1. 点击“规则列表”区域的“添加”，填写唯一规则 ID、名称和图标。
2. 选择“条件逻辑”：**AND** 表示所有条件都满足；**OR** 表示任一条件满足。
3. 设置“冷却时间”，限制自动触发的频率。页面单位为 ms，1000 ms 等于 1 秒。
4. 添加条件，选择变量、比较方式和值。支持等于、不等于、大于、大于等于、小于、小于等于、值变化和包含；比较值的类型应与变量相符。
5. 添加动作模板，并设置顺序所需的延迟、重复和动作条件。
6. 决定是否开启“显示在面板”及“允许手动触发”。前者控制系统页是否出现卡片，后者控制能否手动运行。
7. 检查后保存，再启用。初次配置可先关闭“立即启用”。

保存、启用或停用成功后，当前配置会更新，不需要为此重启。若整套自动化已暂停，保存不会自动恢复运行。刷新列表并检查实际结果；重要调整完成后，按第 13 章更新应急副本。

最多保存 64 条规则。这不是同时运行任务的数量保证；命令长度、条件和动作数量也会影响空间和内存。容量不足时，先删除不需要的配置或减少内容，再保存。

比较值要符合所选类型。数字填写具体数值，不要填写无穷大或 NaN（无效数字）。文本、布尔值（真或假）和空值按对应类型填写。不要把整段 JSON 对象或数组作为比较值。页面报错时，检查变量、比较方式和值，修正后再保存。

配置动作重复和执行条件

方式	含义
“单次”	每次触发执行一次。
“条件持续时重复”	按单个动作的条件重复，每轮最多 100 次。
“指定次数”	按设置次数和间隔重复；每次执行前仍检查动作条件。

动作条件与规则触发条件分别设置。“条件持续时重复”未设置动作条件时，会重复到每轮上限；规则以后仍可能再次触发。

停用规则会阻止新的触发，已经开始的一轮动作可能继续。要停止安排后续动作，点击引擎“停止”并等待确认。已发出的动作和远程进程仍需检查；完成的操作不会撤销。

创建快捷操作

“仅手动触发”“显示在面板”“允许手动触发”分别决定是否只手动运行、是否显示卡片、是否允许用户执行。

1. 填写规则 ID、名称和图标，开启“仅手动触发”。这种规则不需要自动触发条件。
2. 添加动作模板，检查延迟、重复及动作条件。
3. 开启“显示在面板”和“允许手动触发”，保存并启用规则。
4. 返回“系统”的设备面板，确认卡片名称和状态，再执行一次并检查结果。

自动规则也可显示在面板；显示卡片不会把它改成仅手动运行。停用规则仍可能显示卡片，但不能启动。面向 **admin** 提供操作时，名称应说明会发生什么，并告诉用户需要核验或停止后台任务时联系谁。**root** 从“后台运行”查看日志、核验和停止服务。

导入规则配置包

规则配置包请从“自动化”导入，不要用安全页“仅验证”或文件上传代替。此入口会检查签发方、目标设备和规则需要的配置。每个包都要在对应入口验证，不能沿用另一个包的结果。

导入前准备好以下内容：

- 确认当前使用 SD 卡配置还是内部应急配置，并确认该位置可以保存。查看方法见第 13 章。
- 设备已安装有效证书、匹配的私钥和 CA 链，时间已确认。CA 链用于核验证书来源，安装方法见安全指南。
- 部署管理员已指定可信签发方。**root** 登录或安装 HTTPS 证书不等于完成这项设置；缺少时请部署管理员处理。
- 规则使用的动作模板、指令和主机已经准备好。导入不会自动补齐这些配置。缺少哪项，先补齐哪项。规则已启用时，还要核对所用配置的启用状态。

导入保存后会更新当前配置，不需要重启。点击确认前，检查启用状态、条件、动作和目标，确认允许执行。已有的配置暂停设置会保留；暂不允许运行时，可先停用整套自动化，或向提供方取得禁用版本。

1. 在“规则列表”点击导入图标，打开“导入规则配置”，选择 `.tscfg` 文件。页面会开始验证并显示预览。
2. 等待“来源、目标设备和规则内容已验证。”；核对名称、规则 ID 和“规则摘要”。在“查看规则内容”中检查条件、动作、目标和启用状态，不要只看文件名。
3. 已有同 ID 配置时，核对替换内容。确定要覆盖，才勾选“覆盖已存在的配置”。预览后文件、凭证或配置有变化，点击“重新检查配置包”；页面要求重开时，关闭后重新打开并验证。
4. 点击“确认导入”，等待保存结果，再核对规则列表、启用状态和所需变量。不要把保存成功当成任务已经执行成功。
5. 规则允许手动执行且能安全检查时，执行一次并核对目标设备或主机。其他规则观察正常触发后的日志和结果。需要解除整套自动化的暂停时，检查后再点击“启用自动化”。

导入后的规则可以编辑、启停和删除。修改后检查当前配置，并按需要更新应急副本。再次导入仍要重新验签，本地编辑权限不代表可以跳过验证。

仅用于 HTTPS 的证书不一定有配置包签发权限。即使本机导出成功，也可能无法导回；请配置提供方按提示处理证书用途，不要关闭验证或反复导入。

导入和修改不会撤销已经执行的动作，也不会停止远端后台进程。需要结束任务时，在“后台运行”单独处理并确认。

导入未完成时怎么办

验证未通过

提示内容	下一步
签发信任根未指定、签名者不可信或无签发权限	请部署管理员或配置提供方核对签发来源和证书权限；不要用安全页“仅验证”代替或关闭检查。
此包属于另一台设备	请提供方用本设备证书重新导出，不要改包内设备名称。更换本设备证书前，安排匹配的新包。
设备时间尚未确认	在“系统”的“网络与时间”确认时间并同步，再重新验证。
配置正在加载	等待完成，再重新验证。
配置加载失败	查看系统日志，处理原因并恢复配置，再重新验证。
规则需要的配置缺失	补齐页面指出的动作模板、指令或主机，再重新验证。
规则需要的配置已禁用	核对是否应启用这些配置。确认允许执行后，启用并重新验证。
不支持包中的动作	请配置提供方调整。当前规则包导入不支持 Webhook；模板选择器有此选项不代表可以导入。
预览后文件、凭证或配置发生变化	点击“重新检查配置包”，按提示重新打开编辑器或选择文件，再核对并确认。

保存未完成

提示内容	下一步
当前存储位置不可用或空间不足	在“配置与备份”确认位置，检查存储，减少不需要的内容后再验证。
当前配置或保存位置已经改变	保留并复制草稿，重新打开后核对最新配置，再提交。不要连续点击保存。
保存结果尚未确认	刷新并核对规则内容和启用状态；仍无法确认时查系统日志。保留原包，不要重复导入。

条件变量暂时没有采样值，不一定是缺少配置；请检查它何时更新。配置本身无法读取时，先保留原文件并查看系统日志，不要当作空配置覆盖。

维护规则和配置

- 手动执行要求规则已启用且允许手动触发，并且没有正在执行的同一规则。它不等待自动条件，也不受自动触发冷却时间限制；动作条件、延迟和重复仍生效。
- 停用规则不会撤销已完成的动作；删除也不能从页面撤销。
- 编辑前检查哪些规则使用了这些数据源、模板和指令。修改配置不会停止原来的远端任务；需要停止时，单独核验和停止。
- 每种配置包使用对应列表的导入入口并核对预览；签名和账户管理的完整步骤见安全指南。
- 保存失败时查看提示并保留草稿；保存已成功但列表刷新失败时，先刷新核对，不要直接重复创建。

13. 配置与备份

在“自动化”页点击“配置与备份”。先看“当前使用”，再决定保存、恢复或切换哪份配置。操作前检查是否影响散热、告警或远端任务。

分清三类内容

内容	保存方式
网络、风扇、温度、灯光等系统设置	保存在设备内部，不随自动化副本恢复。
当前自动化配置	日常使用 SD 卡时，新增、修改和删除保存到卡；应急模式下保存到设备内部。
内部应急副本	使用 SD 卡时，点击“保存应急副本”才更新；应急模式下的编辑直接更新这份内部配置。

应急副本整套保存规则、动作模板、SSH 命令、关联主机、数据源和用户变量的初始定义。它不保存私钥、图片、字体、日志或远端运行状态。主机设置只记住使用哪个密钥，不复制密钥本身。

这不是整机备份。重要文件和密钥应按各自的方法保管；副本恢复不代表远端服务已经停止，也不保证规则依赖的文件都可用。

保存应急副本

1. 确认“当前使用”为“SD 卡配置”，并检查当前规则和任务。
 2. 点击“保存应急副本”，等待完成提示。
 3. 检查“内部保存时间”和“副本状态”。“已包含当前修改”表示这份内部副本与当前配置相符。
- 保存会替换上一次应急副本。之后继续修改 SD 卡配置，不会自动更新内部副本；显示“尚未包含最新修改”时，先核对当前内容，再决定是否重新保存。
- 当前使用“内部应急配置”时，编辑已经直接保存在内部，无需再点一次“保存应急副本”。

从应急副本恢复

- 恢复会用内部副本替换当前 SD 卡配置，副本可能较旧。需要保留当前内容时，先导出所需配置和文件。不要先保存应急副本，否则会覆盖准备恢复的旧副本。
1. 在使用 SD 卡配置时，点击“从应急副本恢复”。
 2. 核对新增、修改和移除的项目，以及完成后是否保持暂停。
 3. 确认恢复，等待完成。列表会更新，不需要为恢复配置而重启。
 4. 检查规则、主机、变量和启用状态，确认任务结果。仍暂停时，先检查配置，再点击“启用自动化”。
- 恢复不会改变网络、风扇或密钥。已启动的远端服务不会被恢复操作结束；需要时从“后台运行”处理。

没有可用 SD 卡时

有可用内部配置时，设备会改用它。已启用的自动规则仍按条件运行；手动规则仍需点击。内部副本可能较旧，切换前应核对其中哪些任务允许运行。

应急模式可以新增、修改和删除，保存直接写入设备内部。没有可用内部配置时，先阅读页面原因；可以从有效的新配置开始，但不要把损坏文件当作空配置覆盖。

网络、风扇等系统设置仍从设备内部读取。SD 卡中的图片、字体和日志不会随应急配置恢复；缺资源时插入原卡，或为动作选择可用文件。没有卡不代表所有功能都会停止，也不代表所有任务都能继续。

重新插卡后选择配置

插入可用 SD 卡后，点击“检查 SD 卡”，再查看下面两个选择。插卡不会自动切换或合并；关闭面板可以继续使用内部配置，重启也不会替你完成这次选择。

按钮	会发生什么
“使用 SD 卡配置”	读取并改用卡内配置。内部配置保留，不会自动复制到卡上。
“将当前配置保存到 SD 卡并使用”	用当前内部配置替换卡内配置，然后改用 SD 卡。卡内原配置会被覆盖。

1. 核对当前使用位置，并决定要保留哪份配置。
2. 点击对应按钮，阅读替换内容及启停提示。需要写卡时，先检查新增、修改和移除清单。
3. 确认后等待完成。检查“当前使用”已变为“SD 卡配置”，再核对列表和任务结果。

卡内没有配置或配置为空，不会自动从内部补回。选择卡内空配置前，确认这正是你想使用的内容。预览后换卡或修改配置时，按提示重新检查，不要沿用旧的确认窗口。

分清保存、切换和运行结果

页面提示或情况	下一步
已保存到 SD 卡，但尚未切换	当前仍使用内部配置。选择“使用 SD 卡配置”完成切换，不要重复覆盖写卡。
配置已保存，但自动化仍暂停	检查配置后，点击“启用自动化”；不要重复保存或靠重启解除暂停。
删除没有保存成功，自动化已暂停	先核对目标是否仍在、存储是否可用；修正并检查配置后，再决定是否启用。
保存结果未确认	重新读取保存位置和内容，无法确认时查系统日志。不要直接重复提交。
当前输入与最新配置不一致	先复制需要的草稿，再关闭、重新打开编辑器，核对后填写。页面不会替你合并草稿。

来源切换、恢复或保存成功后，还要确认任务是否允许运行、是否完成。整套配置的暂停会保留；需要恢复时，检查后明确点击“启用自动化”。普通“停用自动化”或强删导致的暂停，不会因重启或切换配置而自动解除。

TianshanOS Root Operations Guide

This guide covers routine functions in Part I and terminal access, remote commands, Automation, and configuration backup in Part II. Root operations can affect the device and remote hosts; check the target and active tasks before proceeding. See the separate Security Guide for security management.

Use the controls shown on your device. Some need specific hardware or configuration. On a computer, hover over an icon button to see its name. On a phone, swipe within a wide table to view its other columns.

Part I: Routine Functions

1. Getting Started

Open the WebUI

1. Open the device's web interface (WebUI) using the address provided by your administrator.
2. Select "Login" in the upper-right corner.
3. Enter `root` and the root password supplied with the device.
4. Select "Login." After a successful login, the current username appears in the upper-right corner.

Logging in with the default password opens a "Security Reminder." Enter the current password, then enter the new password twice and select "Change Now." Both new-password entries must match. Select "Later" to close the reminder.

When you have finished, select "Logout" in the upper-right corner. You will need to sign in again to use the device.

Switch Languages

Select the language button at the top of the page, then choose Chinese or English. Page content and control labels switch immediately.

Page Navigation

Root users can access these pages:

- “System”: View device status, control modules, fans, and LEDs, and open OTA Update.
- “Network”: Check Ethernet status and DHCP clients, configure WiFi, and manage NAT forwarding.
- “Files”: Manage files on the SD Card and SPIFFS.
- “Terminal”: Run device commands and view system logs.
- “Commands”: Manage and run remote SSH commands.
- “Automation”: Configure tasks and save an emergency backup.
- “Security”: Open the separate security management page. See the Security Guide for instructions.

2. System Status and Routine Operations

Select “System” in the top navigation.

View Resource and Service Status

“Management Chip Resources” shows CPU, DRAM, and PSRAM usage on the management chip. These readings do not show resource usage on AGX or LPMU.

- Select “Details” to view total, used, and free memory and other memory information.
- “Services” shows the number of running services and the total. Select it to view each service’s state and startup stage.
- If a service reports a problem, refresh its status. To restart it, follow “Restart One Service” below.

View System and Power Information

“System Overview” shows the chip, firmware version, ESP-IDF version, and uptime. For routine use, check the firmware version. ESP-IDF is the version of the system framework used by the device.

The right side of the card shows input voltage, internal voltage, current, power, and protection status.

System settings such as networking, fans, temperature, and lighting are saved inside the device. Inserting an old SD card does not restore them. Automation configuration is managed separately; its emergency backup is not a full-device backup.

The switch beside the protection status enables or disables low-voltage protection. When enabled, the device uses the saved voltages and delays to shut down at low voltage and restart after power recovers.

View Network and Time

“Network & Time” shows Ethernet, WiFi, IP address, current time, sync status, time source, and timezone.

- Select “Sync Time” to copy the browser's current time to the device.
- Select “Timezone,” choose a preset or enter a supported timezone setting, then save.
- Select “OTA Update” to open the firmware update page.

Advanced Operations

Reboot TianshanOS

A reboot temporarily interrupts the WebUI and device management. Finish active operations, then select “Reboot” and confirm. Wait for the device to recover, then reopen the WebUI.

Restart One Service

Restarting a service temporarily interrupts the function it provides. Open “Service Status,” find the affected service, and select “Reboot” on that row. Check its status again when the operation finishes.

Change Shutdown Settings

These settings control when the device shuts down after a voltage drop and when it starts again after power recovers. Use values that match your device's power requirements.

Select “Shutdown Settings” to change:

- “Low Voltage Threshold”: Starts the shutdown countdown below this voltage.
- “Recovery voltage threshold”: Starts recovery above this voltage.
- “Shutdown Countdown”: Sets the delay before shutdown after low voltage is detected.
- “Recovery hold time”: Sets the wait time used to confirm stable power recovery.
- “Fan Stop Delay”: Sets the delay before fans stop after shutdown.

Save the form to apply the updated protection settings.

Switch the Top USB Target

Switching the USB target may temporarily disconnect an attached device. Confirm the target and finish active work before continuing.

Devices that support USB switching show a “USB” button. Each click switches the top USB port to the next target: ESP, AGX, then LPMU. Check the target shown on the button and the page message to confirm the result.

3. Device Panel

The “Device Panel” is on the “System” page. It contains module power controls, Quick Actions, and data widgets.

Control AGX and LPMU

Save work on the module and complete its normal shutdown process before removing power. Forced power-off can cause loss of unsaved data.

- “AGX Power” shows the power-control state. Select it to switch power on or off, then wait for confirmation.
- “LPMU Power” shows “Online,” “Offline,” or “Unknown.” These states come from a network check. Online means the module is reachable; offline means it is not. Neither state alone confirms whether the module is powered on or off.
- Selecting the LPMU button triggers the same action as pressing its physical power button. Wait for the check and the displayed result. If the result is unknown, check the module and network before pressing the button again.

Use Quick Actions

A root user configures Quick Action cards. Card visibility and manual execution are separate settings. Seeing a card does not mean you can start its task.

1. Read the card name and description to identify the task.
2. Select the card and read the result. Do not start it again while processing.
3. An executed or queued message still needs an actual result check on the target device or task. Use “Background runs” to verify, view logs, or stop a background service (Chapter 11).

If starting is blocked, follow the reason shown. Do not keep selecting start:

- Rule disabled or manual triggering not allowed: Check the rule settings on “Automation” (Chapter 12). A visible card is not permission to run it.
- A task or background operation is in progress: Wait for its result. Do not start it again.
- A background run record already exists for the task: Verify the original task in “Background runs” and confirm that it has ended before starting again.
- Configuration not loaded, a required item missing, or Automation paused: Check the configuration and enable state on “Automation” (Chapters 12 and 13).

After triggering one action, wait a few seconds before starting another. Closing the page, deleting a card, or restarting TianshanOS does not stop background services on remote hosts.

Press and hold a card until the reorder indicator appears, then drag it to change the display order.

If no cards appear, read the explanation. Wait if configuration is loading. If loading failed, keep the reason and check “System Logs” on Terminal. If no Quick Actions are configured, select “Open Automation” and check the rules’ “Show on panel” setting.

Editing or importing a rule updates the current configuration; a restart is not needed to switch rules. If a card's task was changed, review its conditions, actions, and targets before running it.

Do not restart a device providing active services just to restore a card.

Manage Data Widgets

Data widgets continuously display device data in the “Device Panel.”

1. Select “Widget Manager.”
2. Choose a refresh interval or disable automatic refresh.
3. Add a preset widget, or choose a component style and data source offered by the page.
4. Edit its label, display style, and unit as needed, then save.

Existing widgets can be edited, deleted, and reordered. You can also select a widget card to edit it. Press and hold a widget, then drag it to a new position.

4. Fan Management

“Fan Control” is on the “System” page. Fan cards show the fans provided by your device. Check the fan number before changing a curve.

View Fan Status

The status bar shows “Effective Temp” and “Current output.” The large percentage is the control setting confirmed by the device, not the measured speed. RPM is the measured speed in revolutions per minute and is hidden without a valid reading. A large -- means the current output is unconfirmed.

While you drag the manual slider, the value beside it shows the proposed setting. The large percentage continues to show the current output. Release the slider, then check the message and updated reading to confirm the change. If a requested setting differs from the current output, do not assume it has already taken effect.

Smart mode shows its operating state, such as “Smart Mode,” “Following curve,” protection, or an invalid temperature. It also provides a safety reference, a 45-second forecast, and the rate of temperature change.

If the temperature becomes invalid, check that its source is still updating. The device switches to protective control for temperature loss. Select “TTI” for an explanation of Smart thermal control.

Use the refresh button in the section header to fetch the current state. If adjustment fails or the output is unconfirmed, check the device before deciding whether to retry.

Select an Operating Mode

Mode	Purpose
“Off”	Stops the fan.
“Manual”	Uses a fixed control percentage set with the 0-100% slider.
“Curve”	Follows the configured temperature-to-control-percentage curve.
“Smart”	Uses the base curve, temperature trends, and past adjustments to control cooling. Uses protective control when needed.

Stopping a fan or setting a low manual value reduces cooling. Check the load and temperature first, and keep monitoring them. The slider is available only in Manual mode when the current output is confirmed.

Configure a Fan Curve

Select “Curve” in the Fan Control section header to open “Fan Curve Management.” The “Curve” button inside a card only changes the operating mode.

1. Under “Fan,” choose the number to adjust and check it against the System page.
2. Under “Temperature variable binding,” add temperature variables and assign weights.
3. Select “Bind.” The temperature source is shared by fans in Curve and Smart modes, so changing it affects the fans using that source.
4. Add or edit “Curve nodes.” Each curve needs at least 2 nodes and supports up to 10.
5. Set “Minimum speed” and “Maximum speed” as control percentages. The minimum must not exceed the maximum.
6. Set “Temperature hysteresis” and “Minimum interval.” Hysteresis accepts 0-20°C and reduces frequent adjustments caused by small temperature changes. The interval accepts 500-30000 ms; 1000 ms is 1 second.
7. Select “Save curve.” After a successful save, the selected fan switches to Curve mode. To use Smart thermal control, return to the card and select “Smart.”

If saving fails, read the message and check the current state before retrying. After unbinding temperature variables, check the effective temperature and fan state as well.

Import and Export a Curve

- Select “Import Config” and choose a curve JSON file. JSON is the file format used to store curve data. Review the nodes, limits, and fan number, then select “Save curve” to apply them.
- Select “Export Config” to download the current curve. The page also attempts to save a copy under `/sdcard/config` on the SD card. Check the browser download and the reported SD-card result separately.

Use a Test Temperature

A test temperature temporarily replaces the normal source and affects Curve or Smart control. Monitor the fan and device throughout the test.

1. Enter 0-100°C under “Test Temp.”
2. Select “Test” and observe the current output, state, and fan response.
3. Select “Clear Test” when finished. Check that the effective temperature has returned to its normal source.

5. LED Management

“LED Control” is on the “System” page and shows the LEDs provided by the device. Available features vary by LED.

Routine Controls

- Use the light-bulb button at the bottom of a card to turn the LED on or off.
- Move the “Brightness” slider, or choose a color or preset.
- Use the animation button to open “LED Settings.” Select an animation under “Programmatic Animation,” then use its play or stop control.
- Select the save icon at the bottom right of the card to save the current LED configuration.
- Select “All Off” to turn off all LEDs and check the reported result. If some fail, check those devices.

Advanced LED Matrix Features

Matrix cards provide icons for the available features. Open one, then switch between these groups in “LED Settings”:

- “Programmatic Animation”: Select and run an animation.
- “Image/QR Code”: Choose an image from the SD card or enter content for a QR code.
- “Text Display”: Set text, font, alignment, scrolling, foreground, and background.
- “Post-processing Filter”: Choose a filter and parameters, then apply or stop it.
- “Color Correction”: Adjust the display and use the available reset, import, or export controls.

Check the actual light or matrix display after applying a change. Use only the features shown. If a setting fails, follow the message to check the file, input, or device state.

6. Network Management

Select “Network” in the top navigation to open “Network Settings.” Changing the network mode, hotspot, or NAT settings may interrupt the current WebUI connection. Before saving, make sure you can reconnect through the new network address.

View Network Status

The top of the page shows the state of Ethernet, the WiFi client, and the WiFi AP. Open the related panel to view IP address, subnet mask, gateway, DNS, MAC address, SSID, signal, and connected-device counts when available.

The Ethernet panel displays the current link and address information. It does not provide address editing controls.

Select a WiFi Mode

Mode	Purpose
“Off”	Turns WiFi off.
“Station (STA)”	Connects the device to an existing WiFi network.
“Access Point (AP)”	Makes the device provide a WiFi hotspot.
“STA+AP”	Connects to an existing WiFi network while keeping the device hotspot available.

After choosing a mode, wait for the page to refresh the state. The current wireless connection may be interrupted during the switch.

Connect to WiFi

1. Set the WiFi mode to “Station (STA)” or “STA+AP.”
2. Under “Station,” select “Scan.”
3. Choose a network from the list. The list shows SSID, signal strength, channel, and authentication type.
4. Enter the password and confirm. Leave the password blank for an open network.
5. Wait for the state to change to “Connected,” then confirm the new IP address.

Select “Disconnect” to end the current WiFi client connection.

Configure the WiFi AP

1. Set the WiFi mode to “Access Point (AP)” or “STA+AP.”
2. Under “Hotspot,” select “Config.”
3. Enter the SSID. A blank password creates an open hotspot; a protected hotspot requires at least 8 characters.
4. Select a channel and enable “Hide SSID” if needed.
5. Select “Apply” and wait for the hotspot state to update.

Select “Devices” to view clients currently connected to the hotspot.

Set the Hostname

Enter a new name in the “Hostname” section under “Network Services,” then select “Set.” The page shows the current hostname after it updates.

View DHCP Clients

DHCP automatically assigns network addresses to connected devices. Select “Clients,” choose “WiFi AP” or “Ethernet,” and view the current leases. Use the refresh button to reload the list.

Advanced Network Operations

Configure the NAT Gateway

NAT forwards network traffic between the device's network interfaces. Enable or disable NAT, then select “Save” to retain the setting. Check the WiFi and Ethernet status afterward.

Access the Upstream Network via LPMU

This operation uses the configured LPMU host to set up network access. Before starting, confirm that LPMU is reachable and the network cables are connected. Obtain the sudo password for the SSH account on that host. This password authorizes system changes and may differ from the WebUI password.

1. Under “Upstream Network Access,” select “Access via LPMU.”
2. Enter the LPMU sudo password and select the access button. The password is used only for this run and is not saved; enter it again for a later run.
3. Wait for the operation to finish. Do not start it again while processing.
4. Access is confirmed only when the result reports both an internet connection and completed network configuration.
5. If it fails or the result is unconfirmed, read the reason first. Expand “Execution Log” for more detail. Check the password for a password error, or the cabling and upstream network if no internet connection is found.

A failed status request does not mean the script has stopped. Use the available “Refresh Status” control to check the current run before deciding whether to try again.

7. File Management

Select “Files” in the top navigation to open “File Manager.”

The SD Card is removable storage, and SPIFFS is internal device file storage. Select “SD Card” or “SPIFFS” to switch locations. The path at the top shows your current folder. Select a folder name in the path to go back to it.

Browse and Manage Files

- Select a folder name to open it.
- Select the download button beside a file to save it to the browser's download location.
- Select the rename button, enter a new name, and confirm.
- Select “New Folder,” enter a folder name, and create it.
- Select the refresh button to reload the current directory and storage state.

Upload Files

Files can only be uploaded to the SD Card, not SPIFFS. Confirm that the SD Card is mounted first.

1. Select “SD Card” and open the folder where you want to upload the files.
2. Select “Upload Files.”
3. Select one or more files, or drag files into the upload area.
4. Review the upload list and remove unwanted files.
5. Select “Upload” and wait for each file to show completion.

Uploading a `.tscfg` package opens verification and application steps. However, this file-upload page does not yet apply the package's settings. Successful upload or verification does not mean the settings are in effect.

Import rule packages on Automation, as described in Chapter 12. Ordinary file upload is not a substitute for rule import. See the Security Guide for source and signature guidance for other packages.

Batch Operations

After selecting files or folders, the batch toolbar appears.

- “Batch Download” downloads selected files. Folders are not included.
- “Batch Delete” deletes selected files and folders.
- “Clear Selection” clears the current selection.

Delete a File or Folder

Deletion cannot be undone in the WebUI. Deleting a folder also deletes all of its contents. Confirm the name and path before selecting “Delete” or “Batch Delete” and approving the prompt.

Files managed by Automation are protected. Uploading or overwriting files in `/sdcard/config/automation`, or deleting or renaming that folder or a parent containing it, may be refused. If the message says that Automation manages the file, use “Configuration & backup” on Automation or the relevant list. Do not use Terminal to bypass the restriction.

Mount and Unmount the SD Card

Unmounting makes SD files temporarily unavailable. Finish uploads, downloads, and other file operations, then select “Unmount SD.”

Unmounting or replacing the card may switch Automation to its internal emergency configuration. That copy may be older, and enabled automatic rules may still run. Without a usable copy, Automation may be unavailable. Review the emergency configuration and tasks before unmounting (Chapter 13). Card-based images, fonts, and logs become unavailable.

When the SD Card is not mounted, the page shows “Mount SD.” Select it, wait for the state to change to “Mounted,” then open the SD Card directory again.

Mounting the card does not mean Automation has switched to its configuration. After reinserting a card, choose which configuration to use as described in Chapter 13. Nothing is overwritten or merged automatically.

8. OTA Updates

On the “System” page, select “OTA Update” in the “Network & Time” section to open “Firmware Upgrade.”

The device reboots during an update, temporarily disconnecting the WebUI. Save active work and keep device power stable before starting. Do not power off the device while update progress is incomplete.

First Upgrade from an Older Version to 0.6.3

The first upgrade from an older storage layout, such as 0.6.2, needs a matched USB / serial package approved by the publisher. Uploading only the firmware or WebUI cannot complete this upgrade. Ask the device administrator or provider to follow the package instructions. Do not erase the whole flash or use an old partition table.

Save important files and keep the original SD card installed. The first startup migrates existing configuration; keep power connected. Afterward, check login, networking, fans, lighting, SSH hosts, and Automation rules. Review rules before testing any task that controls power, restarts a device, or runs remote commands.

The matched package updates both application slots. Do not assume that the other slot still contains the old version. If the root password is lost, use only a recovery method confirmed by the provider to match the 0.6.3 layout. Do not flash an old password-reset image.

The web update methods below apply only to versions the publisher has approved for OTA. They do not replace the first layout upgrade.

Check for Updates from an OTA Server

1. Review the “Current Version.”
2. Enter the OTA server address supplied by an administrator or publisher.
3. Select “Save,” then select “Check Update.”
4. The page reports “Update Available,” “Already up to date,” an older server version, or an error.
5. Confirm the target version, then select “Upgrade Now” or the upgrade control shown by the page.
6. Wait for download, installation, and reboot to finish. To cancel, use the “Abort” button when it is available. Not every stage supports cancellation.
7. Wait for the page to confirm the firmware after the upgrade. Reconnect to the WebUI and check “Current Version” and device status.

“Upgrade Progress” shows the current stage in its own section. A 100% reading or a message that files were written does not confirm a completed restart and version check. If the result is unconfirmed or the running firmware differs from the target, keep the message and check the current version. Do not repeat the upgrade without checking. Check System Logs and contact the provider if needed.

When “Also upgrade www” is enabled, the firmware and WebUI are updated in sequence. Use matched firmware and WebUI resources from the same release. If the old interface remains after upgrading, force-refresh the browser and check the version and page again.

Manual Upgrade

Expand “Manual Upgrade” and choose one of these methods:

- “Upgrade from URL”: Enter the firmware URL, set “Also upgrade www” according to the release instructions, then select “Upgrade.” Here, www refers to the device’s web-interface resources.
- “Upgrade from SD Card”: Enter a firmware path such as `/sdcard/firmware.bin`. If “Also upgrade www” is enabled, ensure that `www.bin` from the same release is in that directory.

For an upgrade from a URL, “Skip certificate check” skips verification of the HTTPS server certificate. This removes the certificate check used to confirm the download server’s identity. Leave it unchecked for routine updates. If you see a certificate error, ask your administrator to check the server address and certificate.

Partition Management and Rollback

“Partition Management” shows the running partition and other available partitions.

- “Mark Valid” confirms the running version and disables automatic rollback protection for that version. Use it after confirming that the current version operates correctly.
- “Rollback to This Version” selects another bootable version and switches through a reboot. Rollback interrupts current services. Confirm the target version and data compatibility first.

After the operation and reboot complete, reopen the WebUI and verify the current version and device state.

Version 0.6.3 changes configuration storage and the device partition layout. Do not return directly to incompatible old firmware. If a downgrade is needed, ask the device provider to confirm a complete firmware, layout, and configuration recovery procedure.

Rollback does not restore the old configuration format or guarantee that old rules will work.

9. Security Management Entry

Select “Security” in the top navigation to open security management. Use the TianshanOS Security Guide for SSH keys, remote hosts, known-host fingerprints, HTTPS certificates, configuration packages, and account management. These procedures are not repeated here.

Failed or Unconfirmed Operations

A red field error tells you what to correct. Fix it, then save. A cleared error mark does not confirm a successful save; check the message and list.

Check which operation failed, then read the reason and next step. If the message gives no reason, do not guess.

Select “Details” when available. Select “Hide” to hide the details. If a × button is shown, select it to dismiss the message. For further checks, keep a record of the message and details, then open “System Logs” on Terminal to investigate.

If the result is unconfirmed, refresh and check the device, file, or task state. A timeout or lost connection does not mean the operation failed to run. Do not immediately repeat power, delete, task-start, or upgrade operations. If the result remains unclear, open “System Logs” on Terminal to investigate.

Check successful, failed, and unconfirmed batch results separately. Confirm saved files in the browser’s download list.

Part II: Root-only Functions

10. Terminal and System Logs

“Terminal” is shown only to root. It can run device console commands directly and display device logs. A command may change device state immediately. Confirm its source, parameters, and impact before entering it.

Connect to and Use Terminal

1. Select “Terminal” in the top navigation.
2. Wait for “Connected to device” and the `tianshan>` prompt.
3. Enter `help` to view the commands provided by the current firmware.
4. Enter a command and press Enter. Wait for its output to finish and the prompt to return.

Input is not executed while the page shows “Not connected to device.” After a disconnect, wait for the reconnection message before submitting a command again to avoid duplicate execution.

Terminal supports these keyboard controls:

Control	Purpose
Ctrl+C	Clear the current input and request an interrupt. The command must support interruption for it to stop.
Ctrl+L	Clear the screen.
↑ / ↓	Browse command history from the current page session.
← / →	Move the cursor within the current input.

“Clear” at the top of the page only clears the display. It does not undo commands that have already run. “Disconnect” ends the current Terminal connection.

Open a Remote SSH Shell

An SSH Shell sends subsequent keyboard input to a remote host. Confirm the target address, user, and authentication method, and complete the SSH preparation described in the Security Guide before connecting.

1. Enter `ssh --help` to view the SSH command options.
2. Enter `ssh --host <host> --user <user> --shell`, replacing each placeholder, including its angle brackets, with the actual value. To specify a port, add `--port <port>` before `--shell`.
3. Wait for the remote connection confirmation before entering remote commands.
4. Press `Ctrl+\` to leave the SSH Shell and return to the `tianshan>` prompt.

Do not enter plaintext credentials while the terminal is being shared, recorded, or viewed by another person.

View System Logs

Select “System Logs” at the top of Terminal to open the log window.

- “Level” sets the minimum displayed level. Use `ERROR`, `WARN+`, `INFO+`, or `DEBUG+` to narrow the output.
- “TAG” filters by log source.
- “Search” filters the current logs by keyword.
- “Auto Scroll” follows new log entries when enabled.
- The refresh button reloads historical logs.
- The clear button clears only the logs currently shown in the window.

If filtering produces no output, clear TAG and Search first, then change Level. Closing the log window does not stop device services.

Check Where Automation Is Saved

For a command-line check, enter `auto --config status` to view the current configuration location and backup status. Use `auto --help` for the available options. The old `config --sync` option has been removed. Use the web steps in Chapter 13 for routine backup and recovery.

11. Manage and Run Remote Commands

“Commands” stores reusable SSH commands and runs them on a selected remote host. Remote hosts and their authentication information are managed on the “Security” page. See the Security Guide for those procedures.

Check the Host Fingerprint Before Connecting

A fingerprint helps identify the host you are connecting to. These steps apply to SSH host tests on the web “Security” page, not to the Terminal SSH Shell confirmation flow. If the message says that the fingerprint is unregistered or has changed, do not keep executing the command. Open “Security,” find the target SSH host, and select “Test.”

For a first connection, the confirmation dialog shows the host address and fingerprint. Check them with the host administrator through a trusted channel. Select “Trust & connect” only after confirming a match.

If the fingerprint has changed, the dialog shows both the stored and current fingerprints, with “Cancel” selected by default. Reinstalling the host can change its fingerprint, but a change may also mean that you have reached another host or an impersonator.

Check the address and confirm the reason through a trusted channel. Select “Cancel” if you cannot confirm it. Do not delete the old fingerprint to skip this check. Select “Update Host Key” only after confirming that the new fingerprint is trusted.

Select a Host and View Commands

1. Select “Commands” in the top navigation.
2. Choose a host currently shown under “Select Host.”
3. Review its saved items under “Command List.”

“Orphan Commands” reference hosts that no longer exist and cannot run. Check the host configuration. To keep the task, recreate the command under a valid host, update the templates and rules that use it, and check the result before removing the orphan.

Create or Edit a Command

A saved command runs on a remote host. Verify the command and required permissions on that host before saving it. Take extra care with commands that delete data, shut down or restart a host, or overwrite files.

1. Select a host, then select “New Command.” Use the edit button on an existing command to change it.
2. Enter a unique “Command ID.” It may contain letters, numbers, underscores, and hyphens, and cannot begin or end with an underscore or hyphen.
3. Enter “Command Name” and “Command.” Put each command on a separate line when using multiple lines.
4. Add a description and choose an icon or an image from the SD Card if needed.
5. Review the run mode and output-matching options, then select “Save.”

The name helps you recognize a command; Automation uses its ID to find it. You cannot change an existing command's ID. To use a new ID, create a command and update the templates and sources that use it.

Execute a Command and Review the Result

1. Select the execute control on a command card.
2. Watch the output and status under “Execution Result.”
3. When “Cancel” is shown, use it to request interruption of the current session. Check the state and output to confirm whether it stopped. Completed remote operations are not undone.
4. Select “Clear” to remove the current result display.

“Clear” does not undo work already completed on the remote host. Success, failure, extracted content, and final status depend on the command's matching settings.

Configure Result Matching

Result matching converts remote output into a status that is easier to use.

- “Expected match”: Marks the result successful when the output contains the configured text.
- “Fail Match”: Marks the result failed when the output contains the configured text.
- “Extract regex”: Uses one (. *) capture group to save selected output.
- “Stop on match”: Ends a continuing command after a successful match.
- “Timeout (s)”: Sets how long to wait for a match, in seconds. It applies only when a success or failure pattern is set, or “Stop on match” is enabled.
- “Variable Name”: Saves status and extracted output for use on the Automation page.

Choose stable, specific success and failure text. Broad text can produce incorrect matches. Execute the command once and review “Match Results” before using its variables in a rule.

Use Background Execution and Service Mode

nohup means a command continues to run in the remote host's background after the SSH connection closes. Closing the WebUI does not stop a background task.

Background runs require SSH key authentication. Deploy the public key on “Security,” then select the associated host. Do not save plaintext passwords in background commands. The same key must remain available to stop or verify the original task.

After enabling “Run in background (nohup)” and executing the command, select “Background runs” on Commands. The root-only control on System and the control on Automation open the same list.

1. Find the original task by its name, user, host address, and port.
2. Select “Verify remote state” to check this run on the original host. “Refresh” only reads known records; it does not replace verification.
3. Select “View Log” to read the last 100 lines from the original host. Select “Follow log” for updates. “Stop following” stops only the page updates.
4. To end the task, select “Stop” on its record and confirm. Wait for the result, then verify that it has stopped. Do not start it again without checking.

After a device restart, old records show “Not checked.” “Remote state unconfirmed” means it is not known whether the task is stopped or running. “Last result” describes the last confirmed result, not a guarantee of the current state.

A failed read does not mean the log is empty or the process has exited. Check the original host connection, log path, and SSH key. Verify again after resolving the issue; do not restart a task just because its status check failed.

Deleting a command, changing its host configuration, or switching Automation configurations does not end a remote process. Manage the original task from “Background runs.” Recreating a command with the same name or ID does not take over the original task. Keep any key still needed to control it.

“Service Mode” watches a background task until it becomes available. Provide “Ready match” and “Variable Name.” Adjust the optional failure pattern and timing settings as needed:

- “Ready match”: Marks the service ready when the configured text appears. Use | to separate multiple patterns.
- “Fail Match”: Marks the service failed when the configured text appears.
- “Ready timeout (s)”: Sets the longest wait for the ready state, in seconds.
- “Check interval (ms)”: Sets how often the log is checked, in milliseconds; 1000 ms is 1 second.
- “Variable Name”: Stores states such as checking, ready, and timeout.

Service-mode tasks may be starting, verifying, stopping, or unconfirmed. Wait for the final result after a request is accepted. If a background run record already exists, verify that original run and confirm it has ended before starting again. An enabled automatic rule may start the service again. Disable that rule first if the service must stay stopped.

Import and Export Commands

- Use the export button on a command to export it and, when selected, include its dependent host configuration.
- Select “Import Command,” choose a `.tscfg` configuration package, preview its contents, and decide whether to overwrite existing configuration.

Import may include a remote host and replace configuration with the same ID. Review the command, host, and replacements in the preview before confirming. Saving updates the current configuration without a restart. Existing remote processes do not stop or move to the new host.

New imports check the source, signature, signing permission, and target device. A successful export does not guarantee a later import. A device certificate intended only for HTTPS may lack permission to sign configuration packages. Ask the configuration provider to resolve this; do not disable verification.

Check the Impact Before Deleting a Command

After selecting delete, review the linked templates and rules. Choose an available replacement command, or unlink the affected configuration and disable its rules. See Chapter 12 for the steps. Deletion changes only the configuration in use; it does not update the other emergency copy.

Deleting configuration and stopping a remote service are separate operations. Deleting does not stop the service or undo completed operations. To end a remote task, stop it from “Background runs” and confirm the result.

12. Automation Management

“Automation” connects data and operations into repeatable workflows. Create data sources and action templates, then use rules to decide when to run them.

Automatic: Data source → Variable → Rule evaluation → Actions

Manual: System-page Quick Action → Actions

Sources read data, variables hold values, rules evaluate conditions, and templates define tasks. Showing a rule on the panel and allowing manual execution are separate settings. Automatic rules can also appear on the panel.

View and Control the Automation Engine

The top of the page shows the engine state, rule, variable, and source counts, trigger count, and runtime.

Control	Effect
“Start”	Starts a stopped engine. Enabled rules run only if the current configuration permits execution.
“Pause”	Pauses further automatic evaluation. Existing actions may continue. To resume through the page, stop the engine, then start it.
“Stop”	Attempts to stop rule checks, data reading, and scheduling later actions, while keeping configuration. Wait for confirmation; a timeout does not mean the engine has stopped.
“Reload”	Reads configuration again from the location in use. Save edits and check the result. An existing configuration pause remains in place.

Check whether cooling, alerts, or other ongoing tasks depend on Automation. Stopping the engine does not stop a remote background process. Stop remote tasks from “Background runs” and confirm the result.

“Disable automation” under “Configuration & backup” is separate from the engine's “Pause” control. If the configuration is paused, review it before selecting “Enable automation.” Restarting the device, reloading, or stopping and starting the engine does not clear this configuration pause. See Chapter 13.

Build a Minimal Automation Workflow

1. Create a source and use its test to check the connection and selected fields.
2. Enable it, then use the row's “View Variables” icon to check values and update times.
3. Create a template, review its parameters, and select “Test.” Testing runs the action immediately; confirm that the device and host can accept it.
4. Create a rule with “Enable immediately” off. Set conditions, cooldown, action order, delays, and repetition.
5. Set “Show on panel” and “Allow manual trigger” as needed.
6. Save, then enable the rule. Check variables, trigger counts, and actual results.

Manage Data Sources

Select “Add” under “Data Sources” and choose a type:

Type	Purpose
“REST API”	Periodically reads data from an HTTP address.
“WebSocket”	Receives data pushed over a persistent connection.
“Socket.IO”	Receives events from a Socket.IO service.
“Command Variable”	Reads the results of a configured remote command.

1. Enter a unique ID, display label, and the required connection information.
2. Use the test to check the connection. Obtain addresses, authentication details, and field information from the data provider.
3. For the first three types, select fields from the test response. Leaving a Socket.IO event name blank lets the test attempt event discovery.
4. For a Command Variable, select the host and a command with a configured variable name, then set the polling interval.
5. Check the enable switch in the form, save, and use “View Variables” on its row to check the result.

Source rows provide an enable switch, variable viewer, export, and delete controls. Check which rules use a source before disabling or deleting it, so you do not disrupt their tasks.

Import and export use configuration packages. Preview IDs, types, and replacements before import, and follow the Security Guide for source and trust requirements.

View Variables

Select the eye-shaped “View Variables” icon on a source row. The window shows names, types, values, and update times. Remote-command variables can also be viewed from the command’s variable control.

- Confirm the names and source, and check that values and types suit the rule’s comparisons.
- Check whether update times match the expected data frequency.
- If no data is available, check that the source is enabled, then test the connection and fields. For command variables, check the command’s execution result too.

Create and Test Action Templates

Select “Add” under “Action Templates” and choose a task type:

Type	Purpose
“CLI Command”	Runs a local device-console command.
“SSH Command”	Runs a remote command saved on the Commands page.
“LED Control”	Controls LED colors, effects, or matrix content.
“Log”	Writes a message at the selected level.
“Set Variable”	Assigns a value to an Automation variable.
“Webhook”	The option remains visible, but action execution is not implemented. It cannot currently send a request.

Enter a unique ID, a name, and the type-specific parameters. Set a delay or “Async Execution” if needed. An asynchronous action continues in the background; check its final result through logs, variables, or the target device.

- CLI: Enter the command, with an optional result variable and timeout.
- SSH: Choose a configured host and command, and check the preview.
- LED: Choose a device and supported color, effect, brightness, text, image, QR-code, or filter operation.
- Log: Choose a level and message; the message can reference variables.
- Set Variable: Enter the variable name and value.
- Webhook: Currently unavailable. Choose a supported action instead. Rule packages containing Webhook actions cannot be imported either.

“Test” runs the action. Check the effect of power, reboot, remote-command, or external-request operations before testing. A queued message means the task was accepted, not that it succeeded. Check System Logs and the target device too.

After editing, save and check the parameters. If saving fails, keep the draft and correct the reported issue. Imports may replace templates; review the deletion impact before removing one. If an image or font is missing, insert the original SD card or select an available resource. The emergency backup does not save these files.

Delete Configuration and Handle Its Links

Deleting a rule, template, SSH command, or host can affect other configuration. Save an emergency backup first if you will need it. Deletion cannot be undone from the page.

1. Select delete in the relevant list. Review the target name and affected items.
2. Confirm deletion if there are no links. Otherwise, choose an available replacement or “Unlink and disable affected rules.”
3. Refresh the list afterward. Confirm removal and check the linked templates, rules, and enable states.

Unlinking a deleted template removes its action from affected rules and disables those rules.

Deleting an SSH command leaves linked templates as disabled drafts with the command reference cleared; affected rules are unlinked and disabled. Before choosing a replacement, check its target and action, not just a similar name.

When deleting a host, also review affected commands and sources. A command without a host cannot run. Recreate needed commands under a valid host and update their links, then check them before use. Deleting local host configuration is separate from revoking a remote public key; see the Security Guide.

Use Force Delete When Needed

If ordinary deletion cannot complete, select “Force delete.” Read the explanation before confirming. It deletes the target, clears links it can identify, and disables affected rules. It does not stop remote background services.

If the full impact cannot be confirmed, the page asks you to check “I agree to pause automation and continue deleting.” Automation stays paused afterward. Review and repair the remaining configuration, then select “Enable automation” in “Configuration & backup.” Do not rely on a restart to resume it.

If configuration changes during confirmation, select “Review deletion impact,” review the new list, and confirm again. Force delete cannot guarantee completion when storage writes fail. Read the list again to check; a disappearing card does not prove the deletion was saved.

Create a Rule

1. Select “Add” under “Rules” and enter a unique ID, name, and icon.
2. Choose “Logic”: AND requires all conditions; OR requires any condition.
3. Set the cooldown for automatic triggers. Values are in ms; 1000 ms is 1 second.
4. Add conditions and choose a variable, comparison, and value. Comparisons include equal, not equal, greater than, greater or equal, less than, less or equal, value changed, and contains. Match the value type to the variable.
5. Add templates and set any action delays, repetition, and action-level conditions.
6. Set “Show on panel” and “Allow manual trigger.” The first controls card visibility on System; the second controls manual execution.
7. Review, save, and then enable the rule. Leave “Enable immediately” off while configuring it for the first time.

Saving, enabling, or disabling a rule updates the current configuration without a restart. If Automation is paused, saving does not resume it. Refresh the list and check the result. Update the emergency backup after important changes, as described in Chapter 13.

You can save up to 64 rules. This is not a guarantee that 64 tasks can run at once. Command length and the number of conditions and actions also affect storage and memory. If capacity is insufficient, remove unneeded configuration or reduce its content before saving.

Match the value to the selected type. For a number, enter a specific value, not infinity or NaN (an invalid number). Enter text, a boolean (true or false), or null for the other types. Do not enter a whole JSON object or array. If the page reports an error, check the variable, comparison, and value before saving again.

Configure Repetition and Action Conditions

Mode	Meaning
"Once"	Runs once per trigger.
"Repeat while true"	Repeats while the action's condition holds, up to 100 times per run.
"Fixed count"	Repeats for the configured count and interval, checking the action condition before each execution.

Action conditions are separate from rule-trigger conditions. Without an action condition, "Repeat while true" continues to the per-run limit. The rule may trigger another run later.

Disabling a rule prevents new triggers; a run already started may continue. To stop scheduling later actions, select the engine's "Stop" control and wait for confirmation. Check actions already sent and remote processes separately. Completed operations are not undone.

Create a Quick Action

"Manual Trigger Only," "Show on panel," and "Allow manual trigger" control whether a rule runs only manually, whether its card is visible, and whether users may execute it.

1. Enter the ID, name, and icon, then enable "Manual Trigger Only." Such a rule needs no automatic trigger conditions.
2. Add templates and review delays, repetition, and action conditions.
3. Enable "Show on panel" and "Allow manual trigger," then save and enable the rule.
4. Return to the System Device Panel. Check the card's name and state, run it once, and review the result.

Automatic rules can also appear on the panel. Showing a card does not make its rule manual-only. A disabled rule may remain visible but cannot start. Give admin-facing actions names that explain their effect, and tell users whom to contact to verify or stop background tasks. Root users view logs, verify, and stop services from "Background runs."

Import a Rule Configuration Package

Import rule packages on Automation, not through Security's "Verify Only" or file upload. This control checks the signer, target device, and required configuration. Verify each package through its own import control; another package's result does not apply.

Before importing, prepare:

- Confirm whether the SD card or internal emergency configuration is in use, and that it can be saved. See Chapter 13.
- The device has a valid certificate, its matching private key, and a CA chain; its time is verified. A CA chain checks certificate origins. See the Security Guide for installation steps.
- The deployment administrator has selected a trusted signer. Root login or installing HTTPS certificates does not complete this setting. Ask the deployment administrator to configure it if it is missing.
- The rule's templates, commands, and hosts are ready. Import does not install these for you. Add any missing configuration first. If the rule is enabled, also check the enable state of the configuration it uses.

Saving an import updates the current configuration without a restart. Before confirming, check the enable state, conditions, actions, and targets, and confirm that execution is safe. An existing configuration pause remains in place. To prevent execution, disable Automation first or ask the provider for a disabled version.

1. Select the import icon under “Rules” to open “Import Rule Configuration,” then choose the `.tscfg` file. Verification starts and the page displays a preview.
2. Wait for “Signing trust, target device and rule content verified.” Check the name, rule ID, and “Rule summary.” Expand “View rule content” to review conditions, actions, targets, and enable state; do not rely on the filename.
3. If the same ID exists, review what will be replaced. Select “Overwrite existing configuration” only if you intend to replace it. If the file, credentials, or configuration change after preview, select “Check package again.” Close and reopen the editor if the page asks you to, then verify again.
4. Select “Confirm Import” and wait for the save result. Check the rule list, enable state, and required variables. A successful save does not prove successful task execution.
5. If the rule permits a safe manual check, run it once and check the device or host. For other rules, watch the logs and results after a normal trigger. To clear a configuration pause, review the configuration before selecting “Enable automation.”

Imported rules can be edited, enabled, disabled, and deleted. Check the current configuration after edits and update the emergency backup if needed. A later import still requires signature verification; permission to edit locally does not bypass it.

A certificate intended only for HTTPS may not authorize configuration signing. A successful local export may still be rejected on import. Ask the provider to resolve the certificate-purpose issue; do not disable verification or repeat the import.

Imports and edits do not undo completed actions or stop remote background processes. End those tasks separately from “Background runs” and confirm the result.

If Import Does Not Complete

Verification Failed

Message or issue	Next step
Signing root not selected, signer untrusted, or signer unauthorized	Ask the deployment administrator or configuration provider to check the signing source and certificate permissions. Do not substitute Security's "Verify Only" or disable verification.
Package targets another device	Ask the provider to export it using this device's certificate; do not change the name inside the package. Arrange matching replacement packages before changing this device's certificate too.
Device time is unverified	Check and synchronize time under "Network & Time" on System, then verify the file again.
Configuration loading	Wait for it to finish, then verify the package again.
Configuration failed to load	Check System Logs, resolve the cause, and restore configuration before verifying again.
Required configuration missing	Add the template, command, or host named by the page, then verify again.
Required configuration disabled	Check whether it should be enabled. Once it is safe to run, enable it and verify again.
Unsupported action	Ask the provider to revise the package. Rule-package import currently rejects Webhook actions; their presence in the template selector does not mean the package can be imported.
File, credentials, or configuration changed after preview	Select "Check package again." Reopen the editor or select the file as instructed, then review and confirm.

Save Incomplete

Message or issue	Next step
Current storage unavailable or full	Check the location in “Configuration & backup.” Resolve the storage issue or reduce unneeded content, then verify again.
Current configuration or save location changed	Keep and copy the draft. Reopen the editor, review the latest configuration, and submit again. Do not keep selecting save.
Save outcome unconfirmed	Refresh and check the rule content and enable state. If still unclear, inspect System Logs. Keep the original package and do not repeat the import.

A condition variable without a sample is not necessarily missing configuration; check when it will update. If configuration cannot be read, keep the original files and check System Logs. Do not overwrite damaged content as though it were empty.

Maintain Rules and Configuration

- Manual execution requires an enabled rule that permits manual triggers, with no run of the same rule already in progress. It bypasses automatic trigger conditions and cooldown, but still applies action conditions, delays, and repetition.
- Disabling does not undo completed actions. Deletion cannot be undone from the page.
- Before editing sources, templates, or commands, check which rules use them. Configuration edits do not stop existing remote tasks. Verify and stop those tasks separately if needed.
- Import each package through its relevant list and review the preview. See the Security Guide for full signature and account procedures.
- If saving fails, read the message and retain the draft. If saving succeeded but refreshing failed, refresh and check the list before creating another item.

13. Configuration and Backup

Select “Configuration & backup” on Automation. Check “Currently using” before saving, restoring, or choosing a configuration. First review any effect on cooling, alerts, or remote tasks.

Distinguish the Three Types of Content

Content	How it is saved
System settings such as networking, fans, temperature, and lighting	Saved inside the device. An Automation backup restore does not change them.
Current Automation configuration	Additions, edits, and deletions go to the SD card during normal SD use, or to internal storage in emergency mode.
Internal emergency backup	While using the SD card, it updates only when you select “Save emergency backup.” Emergency-mode edits update this internal configuration directly.

The emergency backup saves rules, action templates, SSH commands, associated hosts, sources, and initial definitions of user variables together. It does not save private keys, images, fonts, logs, or remote run states. Host settings only remember which key to use; the key itself is not copied.

This is not a full-device backup. Keep important files and keys through their own backup methods. A restore does not mean remote services have stopped or that every file needed by a rule is available.

Save an Emergency Backup

1. Confirm that “Currently using” shows “SD card configuration,” then review the current rules and tasks.
2. Select “Save emergency backup” and wait for completion.
3. Check “Last internal save” and “Backup status.” “Includes the current changes” means the internal copy matches the current configuration.

Saving replaces the previous emergency backup. Later SD-card edits do not update it. If it does not include the latest changes, review the current content before deciding whether to save again.

While using “Internal emergency configuration,” edits are saved internally. You do not need to select “Save emergency backup” again.

Restore an Emergency Backup

A restore replaces the current SD-card configuration with the internal copy, which may be older. Export any current configuration and files you need first. Do not save an emergency backup first; that would overwrite the old copy you intend to restore.

1. While using the SD-card configuration, select “Restore emergency backup.”
2. Review added, changed, and removed items, and whether Automation will stay paused.
3. Confirm and wait for completion. The lists update without a device restart.
4. Check rules, hosts, variables, enable states, and task results. If still paused, review the configuration before selecting “Enable automation.”

A restore does not change networking, fans, or keys. It does not end running remote services. Manage them from “Background runs” if needed.

When No Usable SD Card Is Available

If a usable internal configuration exists, the device switches to it. Enabled automatic rules still follow their conditions; manual rules still need a click. The internal copy may be older, so check which tasks may run before a planned switch.

Emergency mode permits additions, edits, and deletions. Saves go directly to internal storage. If no usable internal configuration exists, read the reason first. You can start with a valid new configuration, but do not overwrite damaged files as though they were empty.

Networking, fans, and other system settings still load from internal storage. Emergency configuration does not restore SD-card images, fonts, or logs. Insert the original card or select available files if resources are missing. A missing card does not mean all functions stop, or that every task can continue.

Choose a Configuration After Reinserting the Card

Insert a usable SD card and select “Check SD card,” then review the two choices below. Insertion does not switch or merge configurations. Close the panel to keep using internal configuration. Restarting does not make the choice for you.

Button	What happens
“Use SD card configuration”	Reads and switches to the card's configuration. Internal configuration is kept, not copied to the card.
“Save current configuration to SD card and use it”	Replaces the card's configuration with the current internal configuration, then switches to the card. The old card configuration is overwritten.

1. Check the current location and decide which configuration to keep.
2. Select the relevant button and review the replacement and enable-state notice. Before writing to the card, check the added, changed, and removed items.
3. Confirm and wait. Check that “Currently using” shows “SD card configuration,” then review the lists and task results.

Missing or empty card configuration is not filled from internal storage automatically. Confirm that an empty configuration is what you want before choosing it. If the card or configuration changes after preview, check again as instructed; do not reuse the old confirmation.

Distinguish Save, Switch, and Run Results

Message or situation	Next step
Saved to SD card, but not switched	Internal configuration is still in use. Select “Use SD card configuration” to finish switching. Do not overwrite the card again.
Configuration saved, Automation still paused	Review the configuration, then select “Enable automation.” Do not save again or rely on a restart to clear the pause.
Deletion not saved, Automation paused	Check whether the target is still present and storage is available. Repair and review the configuration before deciding whether to enable it.
Save outcome unconfirmed	Read the location and content again. Check System Logs if needed. Do not submit the same change again without checking.
Current input differs from the latest configuration	Copy any draft you need before closing and reopening the editor. Review the latest content and enter your edits. The page does not merge drafts for you.

After a successful switch, restore, or save, check whether tasks are allowed to run and whether they finish. A configuration pause remains in place; review and select “Enable automation” to resume. A pause caused by “Disable automation” or force deletion is not cleared by restarting or switching configurations.