

C1312B 用户使用手册

V1.0

1 产品概述	3
1.1 外观	3
1.2 接口	3
1.1.1 串口	4
1.2.2 网口	4
1.2.3 USB 口	4
1.2.4 按键	4
1.2.5 指示灯	4
2 首次连接与登录	5
2.1 连接管理终端	5
2.2 登录与语言切换	5
2.3 首次配置建议	6
3 Web 管理界面	7
3.1 页面组成	7
3.2 应用、撤销与校验	7
4 设备概览	8
4.1 系统信息与资源	8
4.2 流量监控	9
4.3 网络状态与蜂窝信息	10
5 网络管理	11
5.1 网络切换	11
5.2 蜂窝网络	13
5.2.1 链路状态	13
5.2.2 连接配置	14
5.3 无线网络	15
5.4 网口管理	16
5.5 WAN	17
5.6 LAN	18
5.7 静态路由	20
5.8 VPN	22

5.8.1 开关、运行状态与通用操作	22
5.8.2 IPSec	23
5.8.3 OpenVPN	25
5.8.4 L2TP.....	27
5.8.5 PPTP.....	28
5.9 防火墙.....	30
6 物联网关	33
6.1 Node-RED 图形编辑.....	33
6.2 修改 Node-RED 密码.....	34
7 系统管理	35
7.1 系统时间.....	35
7.2 配置管理.....	36
7.2.1 网页恢复出厂设置	38
7.2.2 物理按键恢复出厂设置.....	39
7.3 系统升级.....	40
7.4 用户管理.....	41
7.5 系统重启.....	42
7.6 系统参数.....	44
7.7 远程管理.....	45
7.7.1 软方云服务.....	45
7.7.2 私有 FRP 服务.....	46
7.8 管理工具.....	47
7.8.1 SSH 服务	47
7.8.2 ADB 服务	48
8 使用注意事项	49
8.1 账号与会话	49
8.2 网络与远程访问	49
8.3 配置与升级	49

1 产品概述

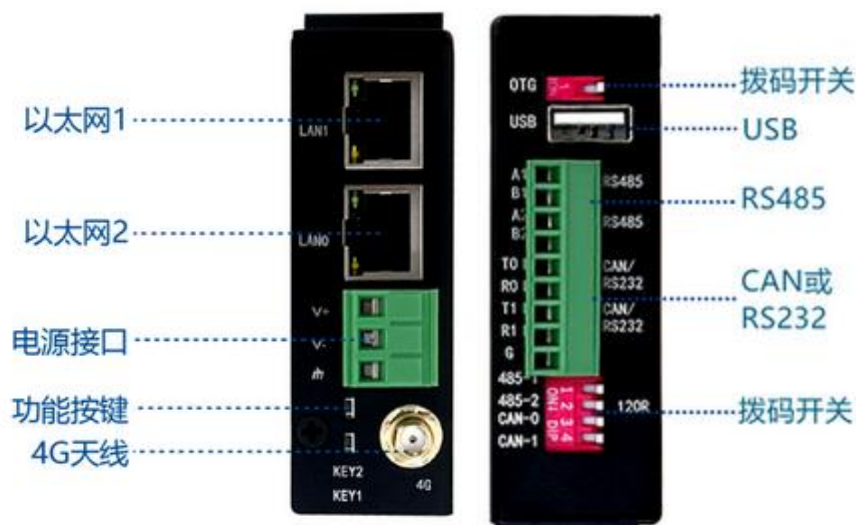
C1312B 面向工业现场的多链路接入与远程管理场景，提供以太网、Wi-Fi、蜂窝网络、VPN、防火墙、系统维护和配置备份等功能。

1.1 外观



1.2 接口





1.1.1 串口

C1312B 提供 2 路 RS485 串口和 2 路 CAN FD 接口，通过 9PIN 的 3.5mm 间距单层凤凰端子连接,并且分别提供 120R 终端电阻可供选择。

1.2.2 网口

C1312B 提供 2 路网口，支持内网、外网同时工作。

1.2.3 USB 口

C1312B 提供一路 USB OTG 接口，通过拨码开关切换 USB Host 和 USB Device 功能。

1.2.4 按键

C1312B 提供 2 个按键 key1 和 key2。短按 KEY1，设备重启，长按 8 秒 KEY2，恢复出厂设置。

1.2.5 指示灯

指示灯	显示含义
485-*	485 口通讯指示灯，收到数据时闪烁。
LINK	正在建立网络连接时闪烁；联网成功后常亮；没有可用连接且未在连接时熄灭。
RUN	网关程序启动后常亮；程序停止时熄灭。上电后请等待程序启动完成。
POW	设备上电后常亮。

2 首次连接与登录

首次使用建议从 ETH0 接入。本章给出出厂配置下的连接方法；若设备由项目预配置，请使用交付文档提供的实际地址。

2.1 连接管理终端

1. 给设备供电，等待系统完成启动。
2. 使用网线把管理 PC 连接到 ETH0，ETH0 在当前产品中固定为 LAN 角色。
3. 出厂 LAN 地址为 192.168.10.1/24，DHCP 地址分配默认启用。将 PC 网卡的 IP 地址和 DNS 设置为自动获取，等待获得 192.168.10.x 地址。
4. 在浏览器地址栏输入 http://192.168.10.1/。如果项目已修改 LAN 地址，应输入修改后的地址。

电脑使用手动地址时

电脑连接 ETH0 后，可将 IP 地址设置为 192.168.10.2、子网掩码设置为 255.255.255.0，再访问 192.168.10.1。电脑地址应与其他终端不同。设备已配置过时，请使用实际 LAN 网段和管理地址。

2.2 登录与语言切换



1. 在右上角语言列表选择“简体中文”或“English”。
2. 登录页面的账号和密码默认留空，请手动输入。出厂用户名为 admin，密码为 admin；已配置设备使用现有账号和密码。首次登录后，请在“系统管理 > 用户管理”修改默认密码。
3. 点击“登录”进入管理界面。退出登录或登录过期后，重新输入账号和密码；浏览器若已保存登录信息，仍可能按浏览器设置自动填充。
4. 登录后可在页面顶部继续切换语言；主机名称属于用户配置，不会被翻译。

单会话规则

同一个用户同一时间只允许一个活动会话。如果该账号在另一台电脑或另一个浏览器重新登录，旧会话会立即退出，并提示检测到新的登录。为便于审计，不要多人共用同一账号。

2.3 首次配置建议

推荐的首次配置顺序



配置前备份

设备投入现场前，在“系统管理 > 配置管理”导出一份已验收配置。当前备份包含登录凭据、连接密码、密钥和证书等敏感内容；仅由授权人员保管，不要通过公开或不可信渠道发送。

3 Web 管理界面

管理界面由顶部栏、可折叠侧边栏和内容区组成。所有修改项在保存前都只存在于当前页面草稿中。

3.1 页面组成

- 顶部栏：显示主机名称、语言、当前用户和“退出”。
- 侧边栏：显示产品型号及设备概览、网络管理、物联网关、系统管理入口；可通过顶部箭头收起或展开。
- 子菜单：点击“网络管理”“物联网关”或“系统管理”，展开或收起对应功能项。
- 内容区：上方显示运行状态，下方填写参数。提交成功后相关状态会刷新；不要在保存过程中重复操作。

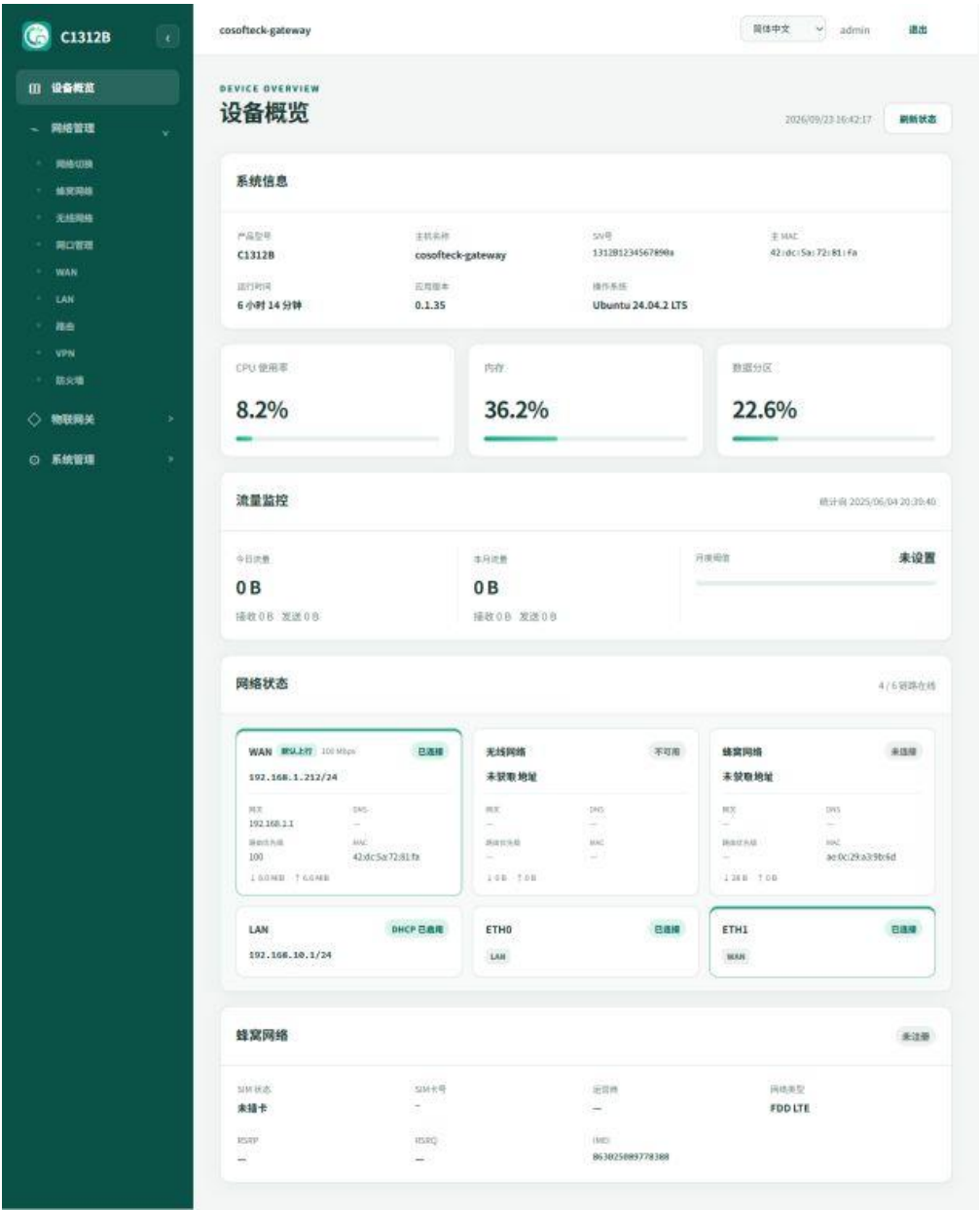
3.2 应用、撤销与校验

操作	处理方法
填写参数	在相应页面修改需要调整的字段。
检查并应用	点击“应用”；如字段下方出现错误提示，修正后再次提交。
确认结果	看到设置成功提示后检查最新状态；必要时使用新的网络地址重新访问。

- 参数发生变化后，可点击“应用”提交。处理期间按钮不可重复点击，并显示相应的处理状态。
- 字段格式错误会显示在对应控件下方；修正字段后再次应用。
- “撤销”恢复到最近一次读取或保存成功的值，不会恢复更早历史。
- 设置成功后配置即保存生效，页面显示成功提示，无需再次确认。
- 网络相关修改可能改变当前管理路径。保存前应确认存在可用的备用访问方式。

4 设备概览

“设备概览”用于快速查看系统信息、资源使用、链路状态和蜂窝流量，是日常巡检的首选页面。



4.1 系统信息与资源

区域	含义与建议
系统信息	显示产品型号、主机名称、SN 号、主 MAC、运行时间、应用版本及操作系统。
CPU 使用率	表示处理器当前的使用比例，用于观察设备运行负载。

区域	含义与使用建议
内存	显示当前内存使用比例，用于观察设备资源状态。
数据分区	显示数据存储空间的使用比例。

主 MAC 显示当前默认上网接口的 MAC 地址。默认上行从以太网切换到其他网络时，主 MAC 可能随之改变。

4.2 流量监控

流量监控只统计蜂窝网络的接收和发送流量，显示今日、本月及流量月度阈值。阈值单位为 MB，可在“系统参数 > 通用”修改；1 MB 等于 1,000,000 字节。

- 未识别到蜂窝设备时，流量显示为 0。
- 今日和本月为累计统计值。取出 SIM 卡不会清除此前已产生的流量；统计结果供使用参考，实际计费以运营商账单为准。

流量达到阈值时

- 当本月蜂窝流量达到设置的阈值，管理页面会弹窗警告。阈值设为 0 时不启用此限制。
- 有可用的以太网或 Wi-Fi 备用网络时，系统停用蜂窝连接并切换到备用网络。
- 没有可用备用网络时，为避免设备完全离线，系统保持蜂窝连接并提示风险；后续仍可能产生流量费用。备用网络恢复可用后，系统再执行保护。
- 因阈值被停用后，如需继续使用蜂窝，请先调整流量月度阈值，或在新月份按需重新启用蜂窝连接。

4.3 网络状态与蜂窝信息

网络状态按 WAN、Wi-Fi、蜂窝网络、LAN、ETH0、ETH1 的固定顺序显示。默认上行标识位于网络名称右侧。

项目	显示内容
WAN	以太网 WAN 的连接状态、IP、网关、DNS 等；作为默认上行时显示相应标识。
Wi-Fi	无线连接状态和 IP 等信息；未检测到无线设备时保留卡片并显示停用。
蜂窝网络	蜂窝数据连接状态和 IP 等信息；无可用数据连接时，不代表已经接入互联网。
LAN	局域网 IP；标题旁显示 DHCP 是否启用。
ETH0 / ETH1	LAN/WAN 角色及网线连接状态。

蜂窝网络卡片显示 SIM 状态、SIM 卡号、运营商、网络类型、RSRP 和 RSRQ 等。SIM 卡号用于识别卡片，不是手机电话号码。未插卡或无法识别 SIM 时，运营商显示横杠。

5 网络管理

网络管理菜单用于设置网口角色、LAN/WAN 地址、多网络切换、防火墙和 VPN。建议先确定网口角色和 LAN 地址，再配置上行及安全策略。

5.1 网络切换

cosofteck-gateway

简体中文admin退出

NETWORK / FAILOVER

网络切换

刷新状态

网络优先级

优先级数值越小，默认路由优先级越高

以太网

192.168.1.212/24

当前使用

● 链路在线

互联网可用

优先级100

无线网络

—

已停用

蜂窝网络

未获取地址

等待地址

优先级700

切换策略

☒ 网络探测已启用

探测模式

ICMP Ping

探测周期

10秒

Ping 包大小

32字节

Ping 超时

2秒

连续失败阈值

3次

连续成功阈值

2次

回切等待时间

30秒

参考地址 1

223.5.5.5

参考地址 2

119.29.29.29

撤销

应用

以太网、Wi-Fi、蜂窝网络始终按固定顺序显示。优先级数值越小，默认路由优先级越高。页面保留不可用或停用的网络卡片，以便硬件恢复后继续使用原配置。

参数	作用与填写要求
优先级	数值越小越优先；可按 100、200、300 等有间隔的数值规划。每条可配置上行须使用不同数值；重复时页面会提示，不能应用。
网络探测	启用后检查上行能否访问参考地址；停用时不进行网络探测。

参数	作用与填写要求
探测周期	2 – 300 秒，两轮探测的间隔。频率过高会增加流量。
Ping 包大小	8 – 1400 字节；一般保持默认值。
Ping 超时	1 – 30 秒，单次探测允许等待的时间。
连续失败阈值	1 – 20 次，连续失败达到该次数后尝试其他可用网络。
连续成功阈值	1 – 20 次，连续成功达到该次数后认为网络恢复。
回切等待时间	0 – 3600 秒，高优先级网络恢复后等待稳定，再回切。
参考地址	填写可稳定访问的 IPv4 地址；应能从所选上行到达。

探测顺序

系统先探测优先级最高且已配置、已启用的网络。如果该网络可用，则本周期不再探测其他网络；不可用的硬件或停用链路会被跳过。

5.2 蜂窝网络

cosofteck-gateway简体中文admin退出

NETWORK / CELLULAR

蜂窝网络刷新状态

链路状态已停用

SIM 状态	运营商	网络类型	信号强度 (RSRP)
未插卡	—	FDD LTE	—
信号质量 (RSRQ)	IP	默认网关	DNS
—	—	—	—

连接配置连接已停用

APN

留空时由运营商自动分配

PDP 协议

IPv4 / IPv6 双栈

网络模式

仅 4G LTE

认证方式

无认证

用户名

运营商未要求时留空

认证密码

未设置

DNS 获取方式

运营商自动下发

主 DNS

例如 223.5.5.5

备用 DNS

可选

MTU

1500

信号阈值 (RSRP)

-110

检查周期

30

撤销

应用

5.2.1 链路状态

链路状态显示 SIM 状态、运营商、网络类型、RSRP、RSRQ、IP、默认网关和 DNS。运营商以名称显示；未插卡或无法识别 SIM 时显示横杠。

RSRP 表示接收信号强度，单位 dBm，数值越接近 0 通常信号越强；RSRQ 表示信号质量，单位 dB。两者应结合观察，不能只凭单个数值判断网络是否可用。

硬件与 SIM 状态

未识别到蜂窝模块时，状态字段显示横杠，连接开关不可启用。使用蜂窝网络前，请确认设备具备相应模块并已安装可用的 SIM 卡。

5.2.2 连接配置

参数	说明
连接开关	启用或停用蜂窝数据连接。未检测到硬件时不可启用。
APN	运营商接入点；留空时由运营商自动分配。专网 SIM 应填写项目提供的 APN。
PDP 协议	IPv4、IPv6 或 IPv4/IPv6 双栈，需与运营商网络匹配。
认证方式	无认证、PAP、CHAP 或自动；用户名和密码仅在运营商要求时填写。
网络模式	当前型号仅支持 4G LTE，控件为只读。
DNS 获取方式	运营商自动下发，或手动填写主/备用 DNS。
MTU	蜂窝链路最大传输单元。无明确要求时保持默认 1500。
信号阈值	RSRP 低于该 dBm 值时判定为弱信号，用于状态判断。
检查周期	系统重新采集并判断蜂窝信号状态的间隔，范围 10 – 3600 秒；默认 30 秒。

修改认证密码

已保存的认证密码不会明文显示。无需修改密码时保持输入框为空；需要变更时填写新密码。

5.3 无线网络

cosofteck-gateway

简体中文

admin

退出

NETWORK / WIFI

无线网络

刷新状态

链路状态

当前 SSID	IP	信号强度	默认网关
—	—	—	—
DNS	频段 / 频率	连接速率	MAC 地址
—	—	—	—

连接配置

☐ 连接已停用

网络名称 (SSID)

扫描选择或手动输入

加密方式

Wi-Fi 密码

请输入网络密码

☐ 这是隐藏网络, 主动探测此 SSID

IP 获取方式

DHCP 自动获取

IP 地址

例如 192.168.10.20

前缀长度

24

默认网关

例如 192.168.10.1

DNS 获取方式

随 DHCP 自动获取

主 DNS

例如 223.5.5.5

备用 DNS

可选

锁定接入点 (BSSID)

扫描选择时自动填写

撤销

应用

可用无线网络

扫描网络

无线网络页面用于把网关作为 Wi-Fi 客户端接入现有无线网络。链路状态显示当前 SSID、IP、信号强度、网关、DNS、频段/频率、连接速率和 MAC 地址。

1. 打开页面后，可用无线网络列表默认不展开。滚动到页面底部并点击“扫描”。
2. 从扫描结果选择目标 SSID；硬件不支持的加密方式不会显示。
3. 选择加密方式并输入密码；隐藏网络应勾选“这是隐藏网络，主动探测此 SSID”。
4. 选择 DHCP 自动获取或静态 IP；静态模式需填写 IP、前缀长度、网关和 DNS。
5. 如需固定接入点，可填写 BSSID；否则留空以允许漫游。
6. 启用连接并点击“应用”。成功后页面会自动刷新链路状态。

避免断开管理

通过 Wi-Fi 管理设备时，修改 SSID、密码或 IP 可能中断当前连接。建议先用网线连接 ETH0，再进行无线参数修改。

5.4 网口管理

cosofteck-gateway

简体中文 admin 退出

NETWORK / PORTS

网口管理

以太网口

ETH0

已连接

网口角色

LAN

ETH1

已连接

网口角色

WAN

撤销

应用

端口	允许角色	使用说明
ETH0	LAN	固定用于局域网连接，不可改为 WAN。
ETH1	LAN / WAN	出厂为 WAN；改为 LAN 后与 ETH0 共用 LAN 地址配置。

角色切换影响

ETH1 从 WAN 改为 LAN 后，不再承担以太网上行；从 LAN 改为 WAN 后，接在该口的局域网终端可能失去连接。应用前确认管理电脑接在 ETH0，并记录上行设置。

5.5 WAN

cosofteck-gateway

简体中文admin退出

NETWORK / WAN

WAN

刷新状态

网口状态

已连接

IP 地址	IP 获取方式	默认网关	DNS
192.168.1.212/24	静态地址	192.168.1.1	—
MAC 地址	链路速率	累计流量	MTU / 路由优先级
42:dc:5a:72:81:fa	100 Mbps	↓ 1.4 MiB · ↑ 3.5 MiB	1500 / 100

网络配置

IP 获取方式

IP 地址

前缀长度

默认网关

DNS 获取方式

主 DNS

备用 DNS

MTU

撤销应用

WAN 页面只管理被分配为 WAN 角色的以太网口，与 Wi-Fi 和蜂窝网络配置相互独立。若当前没有以太网 WAN，页面仍可显示相应状态，但网络切换页中的“以太网”候选卡片不会消失。

参数	说明
IP 获取方式	选择 DHCP 自动获取或静态地址；自动获取时由上级网络分配。
IP 地址 / 前缀长度	静态模式填写；前缀长度为 1 - 30，应与上级网络规划一致。
默认网关	填写所连接上级路由器的 IP 地址。
DNS 获取方式	选择自动获取，或手动填写主 DNS 和备用 DNS。
MTU	范围 576 - 1500；没有特殊要求时保持默认值。

5.6 LAN

cosofteck-gateway

简体中文admin退出

NETWORK / LAN

LAN

刷新状态

网口状态

已启用

IP 地址	MAC 地址	DHCP 服务	DNS 转发
192.168.10.1/24	12:34:56:78:90:a3	运行中	未启用

网络配置

LAN IP 地址

前缀长度

☒ 启用 DHCP 地址分配

地址池起始

地址池结束

租期 (秒)

☐ 由设备提供 DNS 转发

上游 DNS 1

上游 DNS 2

静态租约

添加静态租约

暂无静态租约

撤销

应用

DHCP 活动租约

暂无活动租约

所有设为 LAN 的以太网口共用同一组 LAN 地址、DHCP 地址分配和 DNS 转发设置。更改 LAN IP 会同时影响这些端口上的客户端。

参数	说明
IP 地址 / 前缀长度	设备在局域网中的地址；前缀长度 1 - 30。出厂为 192.168.10.1/24。
启用 DHCP 地址分配	自动为局域网终端分配 IP；出厂启用。接入已有局域网前，确认不会与其他 DHCP 服务冲突。

参数	说明
地址池起始 / 结束	出厂为 192.168.10.100 – 192.168.10.200。必须位于 LAN 网段内，起始地址不大于结束地址，不能包含设备自身地址。
租期	出厂为 43200 秒（12 小时）。允许 60 – 604800 秒；到期后客户端可续租。
由设备提供 DNS 转发	启用后局域网客户端可通过本设备查询域名。
上游 DNS	可手动指定。启用 DNS 转发且留空时使用系统上游 DNS；关闭转发时请确认客户端能获取有效的 DNS。
静态租约	按终端 MAC 固定分配 IP；IP 和 MAC 不得重复。最多 64 条，地址需属于 LAN 网段。
DHCP 活动租约	只读显示已分配的地址及终端信息；无记录时显示“暂无活动租约”。

修改 LAN 地址

保存后应把管理 PC 切换到新网段，并使用新的 LAN IP 重新打开页面。该操作会影响所有 LAN 客户端。

5.7 静态路由

cosofteck-gateway

简体中文

admin

退出

NETWORK / ROUTES

路由

刷新状态

静态路由

添加

尚未配置静态路由

路由表

目标网络	网关	接口	跃点数	类型
0.0.0.0/0	192.168.1.1	WAN	100	默认路由
192.168.1.0/24	直连	WAN	100	直连路由
192.168.10.0/24	直连	LAN	425	直连路由

添加静态路由

接口

LAN · 已连接

目标网络

例如 10.20.0.0/16

网关

例如 192.168.1.1

跃点数

200

取消

添加

上方“静态路由”列表显示已保存的设置，下方“路由表”显示当前生效的 IPv4 路由。点击“添加”或某条记录后的“编辑”打开参数对话框；点击“删除”后需在确认框中确认。

参数	说明
接口	选择 LAN、WAN、Wi-Fi 或蜂窝；应选择能够到达目标网络的出口。
目标网络	填写 IPv4 网段，例如 10.20.0.0/16。只访问一台主机时可使用 /32。
网关	填写所选接口能够直接到达的下一台路由器 IP；直连路由可按页面要求留空。
跃点数	范围 1 - 32766；相同目标的路由通常数值越小越优先。

已保存与已生效的区别

连接断开或网络地址变化时，已保存的静态路由可能暂时不出现在下方路由表。先确认对应网络已连接，再检查路由表；不要因为暂时未生效而反复添加相同路由。

5.8 VPN

VPN 页面分为 IPSec、OpenVPN、L2TP、PPTP 四个选项卡，每种协议保留一套配置。页面顶部为 VPN 总开关，协议标题右侧为该服务的独立开关。使用某种协议时，两个开关都需启用。

5.8.1 开关、运行状态与通用操作

进入相应选项卡，上方查看连接状态、服务器地址、虚拟地址、连接时长、隧道接口、绑定上行及收发流量；下方填写连接参数。未连接时，尚未获得的信息显示为横杠。

1. 向 VPN 服务提供方获取服务器地址、认证资料以及对应协议参数。
2. 打开 VPN 总开关和当前协议的“服务”开关，填写本选项卡的参数。
3. 点击本选项卡底部“应用”，等待提示设置成功，再查看运行状态。
4. 显示已连接后，从需要使用 VPN 的终端访问对端业务地址，确认实际业务可用。

参数	说明
服务器地址	填写服务方提供的域名或 IP，不要带 http://、路径或空格。
服务器端口	与服务方一致；IPSec 和 L2TP 页面使用固定端口，其他协议按要求填写。
绑定上行	“自动选择”跟随当前默认上行；选择 WAN、Wi-Fi 或蜂窝时，请确认该网络已可用。
MTU	范围 576 - 1500；一般保持默认 1400，或按服务方要求填写。
连接检查	启用后检查连接情况；无特殊要求时保持启用。
密码与密钥	已保存的密码、预共享密钥及私钥不会明文显示；无需修改时保持为空。

停用范围

关闭某协议的服务开关并应用，仅停用该协议；关闭 VPN 总开关并应用，将停用全部 VPN。重新启用总开关后，仅已启用的协议会尝试连接。

5.8.2 IPSec

cosofteck.gateway 简体中文 admin 退出

NETWORK / VPN

VPN ☐ VPN 已停用

IPSec ☐ 服务已停用

运行状态

连接状态	服务器地址	虚拟地址	连接时长
已停用	—	—	—
隧道接口	绑定上行	接收流量	发送流量
—	自动选择	0 B	0 B

连接配置

服务器地址

域名或 IP 地址

服务器端口

500

绑定上行

自动选择

MTU

1400

IKE 版本

IKEv2 (推荐)

认证方式

预共享密钥 (PSK)

本端 ID

留空使用本机地址

对端 ID

留空使用服务器地址

IKE 提议

AES-256 / SHA-256 / MODP2048

ESP 提议

AES-256 / SHA-256 / PFS2048

DPD 周期

30 秒

DPD 超时

120 秒

预共享密钥

请输入 PSK

本端子网

每行一个 CIDR，例如 192.168.10.0/24

对端子网

每行一个 CIDR，例如 10.20.0.0/16

☒ 连接检查

撤销

应用

IPSec 用于与兼容的 VPN 服务器或对端网关建立连接。双方的 IKE 版本、认证信息、加密选项和子网必须相互匹配。

参数	说明
服务器端口	固定显示 500。
IKE 版本	选择 IKEv2 或 IKEv1，与服务端一致。
认证方式 / 预共享密钥	使用服务方提供的预共享密钥（PSK），注意大小写及空格。
本端 ID / 对端 ID	用于双方身份识别；按服务方要求填写，不能把用户名直接当作 ID 使用。
IKE 提议 / ESP 提议	选择双方共同支持的加密和认证组合；必须与服务方配置匹配。
DPD 周期	每次检查对端是否仍在线的间隔，10 - 3600 秒。
DPD 超时	判定对端无响应前允许等待的时间，不小于 DPD 周期，最大 7200 秒。
本端子网	需要通过 VPN 访问对端的本地网段，例如 192.168.10.0/24。
对端子网	通过 VPN 访问的远端网段，由服务方提供；避免与本地网段重叠。

按照服务方提供的参数填写本端和对端信息，点击“应用”。连接建立后，可在运行状态区域查看结果，再访问约定的业务地址。

5.8.3 OpenVPN

cosofteck.gateway

简体中文admin退出

NETWORK / VPN

VPN

☐ VPN 已停用

IPSecOpenVPNL2TPPPTP

OpenVPN

☐ 服务已停用

运行状态

连接状态

已停用

服务器地址

—

虚拟地址

—

连接时长

—

隧道接口

—

绑定上行

自动选择

接收流量

0 B

发送流量

0 B

连接配置

服务器地址

域名或 IP 地址

服务器端口

1194

绑定上行

自动选择

MTU

1400

传输协议

UDP (推荐)

隧道模式

TUN (三层)

认证方式

用户名和密码

保活周期

10 秒

用户名

密码

请输入密码

MSS

0

☐ 接管默认路由

CA 证书 (PEM)

-----BEGIN CERTIFICATE-----

tls-crypt 密钥 (可选)

可选

☒ 连接检查

编辑应用

OpenVPN 可使用用户名密码、证书或两者组合认证。不同认证方式会显示不同的凭据输入项，请按服务方资料选择。

参数	说明
服务器端口	范围 1 – 65535，常见值为 1194，以服务方为准。
传输协议	UDP 或 TCP，必须与服务器一致。
隧道模式	TUN 或 TAP，与服务端要求一致。
认证方式	用户名和密码、客户端证书，或用户名密码加客户端证书。
用户名 / 密码	由 VPN 服务方分配，仅在所选认证方式需要时填写。
CA 证书	粘贴服务方提供的 PEM 证书全文，保留开头、结尾和换行。
客户端证书 / 私钥	证书认证时填写配套资料，不可使用其他用户的私钥。
tls-crypt 密钥	可选；服务端要求时填写完整内容，否则留空。
保活周期	5 – 3600 秒，用于保持和检查连接。
MSS	0 表示使用默认处理；手动指定时不应大于 MTU。
接管默认路由	启用后将默认网络访问经 VPN 转发；服务方须允许此用途，可能改变原有上网路径。

证书资料

证书和密钥内容应完整粘贴，避免遗漏首尾行。设备时间明显错误时可能影响证书认证，请先检查“系统时间”。

5.8.4 L2TP

cosofteck-gateway

简体中文admin退出

NETWORK / VPNVPN

VPN 已停用

IPSecOpenVPN

L2TP

PPTP

L2TP

服务已停用

运行状态

连接状态	服务器地址	虚拟地址	连接时长
已停用	—	—	—
隧道接口	绑定上行	接收流量	发送流量
—	自动选择	0 B	0 B

连接配置

服务器地址

域名或 IP 地址

服务器端口

1701

绑定上行

自动选择

MTU

1400

用户名

密码

请输入密码

隧道密码（可选）

可选

☐ 设为默认路由

对端子网

每行一个 CIDR；可选

☒ 连接检查

撤销

应用

参数	说明
服务器端口	固定显示 1701。
用户名 / 密码	服务方提供的 L2TP 登录账号。
隧道密码（可选）	仅在服务方要求时填写；它与登录密码不是同一字段。

参数	说明
设为默认路由	启用后默认网络访问经此 VPN 转发。
对端子网	不接管默认路由时，填写需要经 VPN 访问的远端网段。

填写参数并应用后，检查连接状态和虚拟地址。L2TP 不等同于 IPSec 加密连接；对保密性有要求时，请向服务方确认连接方案。

5.8.5 PPTP

cosofteck-gateway 简体中文 admin 退出

NETWORK / VPN

VPN ☐ VPN 已停用

IPSec OpenVPN L2TP **PPTP**

PPTP ☐ 服务已停用

运行状态

连接状态

已停用

服务器地址

—

虚拟地址

—

连接时长

—

隧道接口

—

绑定上行

自动选择

接收流量

0 B

发送流量

0 B

连接配置

服务器地址

域名或 IP 地址

服务器端口

1723

绑定上行

自动选择

MTU

1400

用户名

密码

请输入密码

☒ 启用 MPPE-128

☐ 设为默认路由

对端子网

每行一个 CIDR；可选

☒ 连接检查

删除

应用

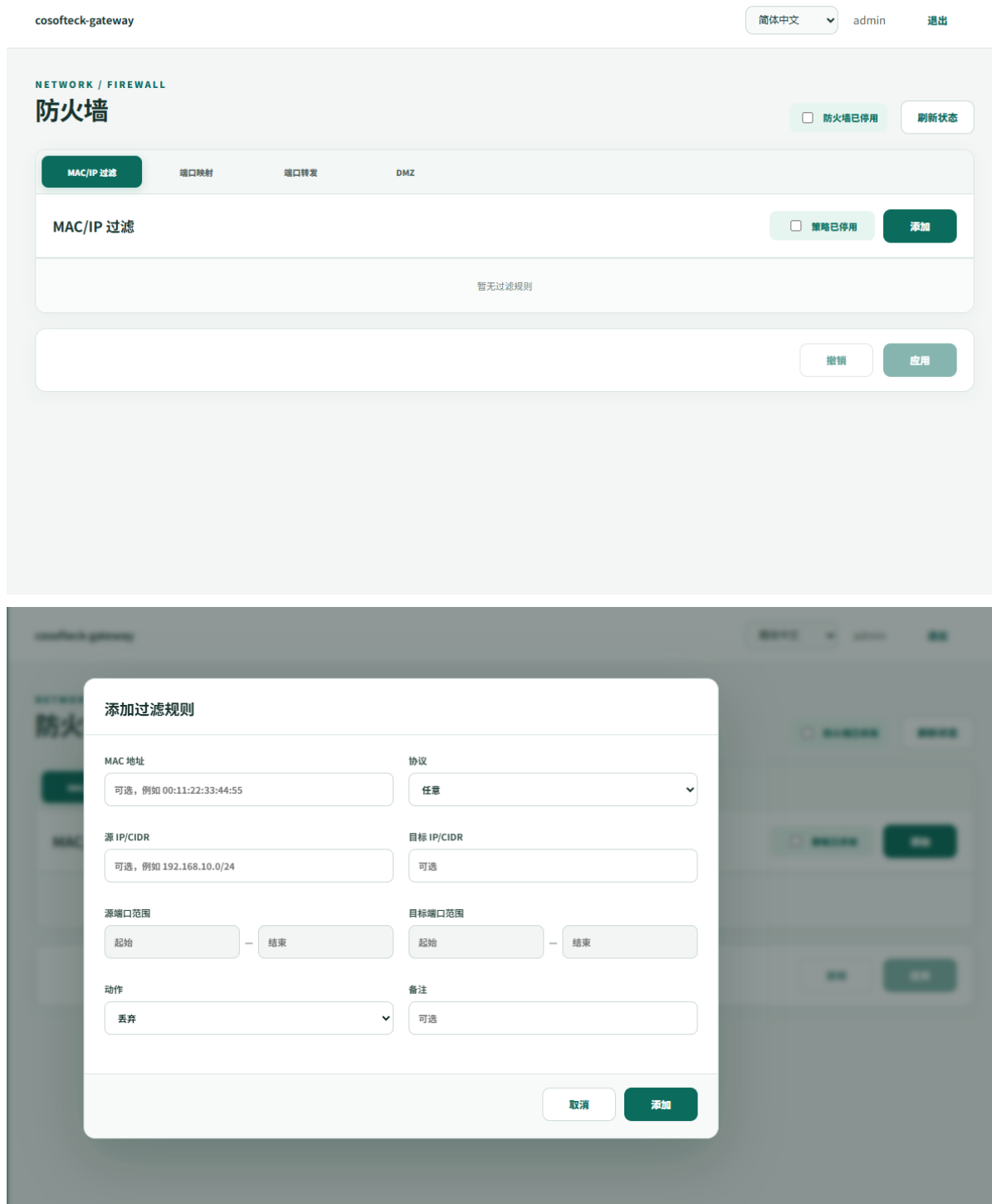
参数	说明
服务器端口	常见值为 1723，按服务方要求填写。
用户名 / 密码	服务方提供的 PPTP 登录账号。

参数	说明
启用 MPPE-128	按服务端要求选择数据加密选项。
设为默认路由	启用后默认网络访问经此 VPN 转发。
对端子网	填写需要通过 VPN 访问的远端网段。

兼容性用途

PPTP 主要用于兼容已有旧系统，不建议承载敏感业务。条件允许时优先使用 IPSec 或 OpenVPN。

5.9 防火墙



防火墙包含总开关，以及 MAC/IP 过滤、端口映射、端口转发、DMZ 四种独立策略开关。总开关停用时各策略配置仍保留，但不会应用。

出厂设置下，“MAC/IP 过滤”策略默认停用。需要过滤时先检查规则内容，再启用该策略并应用；仅填写列表不会自动启用策略。

策略	作用	适用地址
MAC/IP 过滤	按 MAC、源/目标 IP、协议和端口设置接受、丢弃或拒绝；同一条规则不能混用 IPv4 和 IPv6 地址。	IPv4 / IPv6
端口映射	将指定上行的外部端口对应到 LAN 主机及内部端口，适合发布某一项局域网服务。	IPv4
端口转发	按上行、外部来源和端口条件将访问转到 LAN 目标，适合限制指定来源的访问。	IPv4
DMZ	把未由其他规则处理的相关入站访问转向指定 LAN 主机；只填写一个目标 IP。	IPv4

DMZ 风险

“LAN 目标 IP”是接收 DMZ 入站流量的内网主机。启用后该主机暴露面显著增加，应在目标主机上继续启用主机防火墙，并优先用精确端口映射替代 DMZ。

- MAC/IP 过滤、端口映射和端口转发使用“添加”“编辑”“删除”对话框。对话框中的添加、保存或删除先更新页面列表，完成后还需点击页面底部“应用”才能生效。“撤销”放弃未应用的修改。
- 端口映射和端口转发选择 WAN、Wi-Fi 或蜂窝网络作为入口，并填写相应 LAN 目标。DMZ 不需要添加规则，启用策略后填写“LAN 目标 IP”，再点击“应用”。

应用前检查管理电脑不会被过滤规则阻断，且目标设备地址正确。范围端口应按从小到大填写，单个端口可填写相同的起止值。

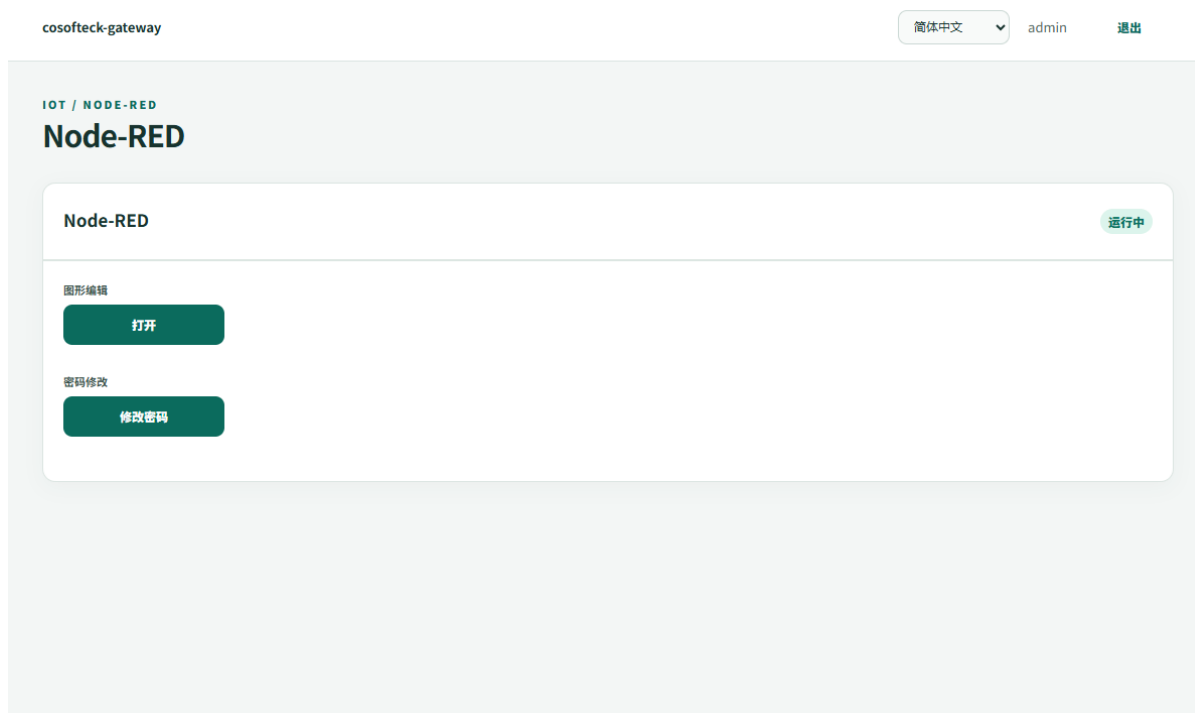
字段	填写方法
MAC 地址	用于识别指定终端；使用页面要求的 MAC 格式。
源 / 目标 IP 或 CIDR	可填写单个地址或网段，例如 192.168.10.20 或 192.168.10.0/24。
协议	按业务选择 TCP、UDP 等；端口条件仅对相应的端口协议有意义。
端口 / 端口范围	有效范围 1 - 65535；映射时区分外部访问端口和内部服务端口。

字段	填写方法
动作	“接受” 允许访问；“丢弃” 不响应；“拒绝并响应” 拒绝并返回响应。
备注	为规则填写便于识别的用途说明，最多 96 个字符。

6 物联网关

“物联网关”位于“网络管理”下方，当前提供 Node-RED 页面。此页面用于打开图形编辑器，以及修改 Node-RED 登录密码。

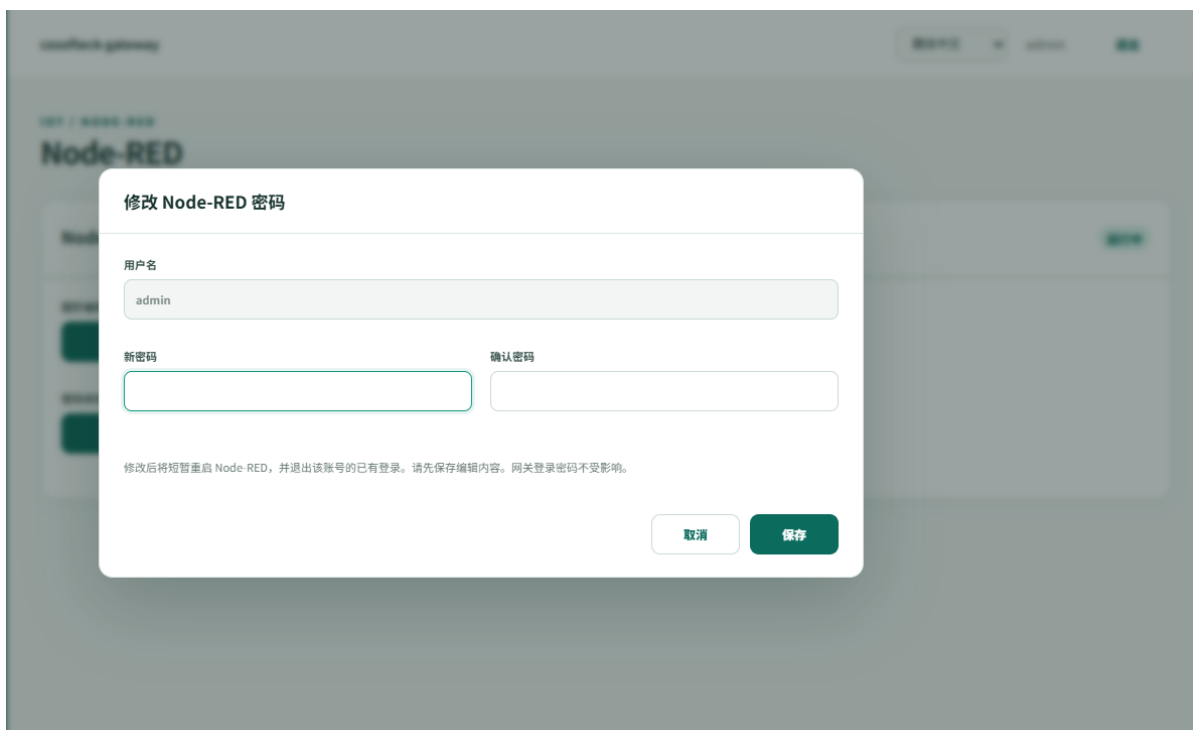
6.1 Node-RED 图形编辑



- 在侧边栏选择“物联网关 > Node-RED”，查看服务是否运行。
- 点击“图形编辑”后的“打开”，浏览器会在新标签页打开 Node-RED 编辑器。若被浏览器拦截，请允许本设备打开新标签页。
- 使用 Node-RED 账号登录。出厂账号和密码为 admin / admin；已配置设备使用修改后的密码。
- 在编辑器中进行流程编辑，保存需要保留的内容；完成后按编辑器提供的操作部署流程。

Node-RED 与网关管理页面使用各自的登录密码。修改其中一个密码，不会同步修改另一个密码。远程访问时，应使用服务方确认的 Node-RED 访问地址。

6.2 修改 Node-RED 密码



- 管理员点击“修改密码”，确认弹窗中显示的用户名。
- 输入新密码并再次确认。密码至少 6 个字符，且包含大写字母、小写字母、数字、特殊字符中的至少两类；总长度不超过 72 字节，中文等字符会占用多个字节。
- 点击“保存”。若字段下方出现错误，修正后再提交；不修改时点击“取消”。

修改前保存编辑内容

保存密码会短暂重启 Node-RED，并退出该账号已有的 Node-RED 登录。请先保存编辑内容，再使用新密码重新登录。网关管理网页的登录密码不受影响。

通过网页或物理按键恢复出厂设置后，Node-RED 登录账号和密码均恢复为 admin / admin。恢复后请及时修改默认密码。

7 系统管理

系统管理菜单用于时间同步、配置备份、应用升级、用户、重启、通用参数、远程服务、SSH 和 ADB 管理。部分高权限页面仅管理员可访问。

7.1 系统时间

The screenshot shows the 'System Time' configuration page. At the top, it says 'cosofteck-gateway' and '简体中文 admin 退出'. The main heading is 'SYSTEM / TIME 系统时间'. Below it, the current time and time zone are displayed: '2026/09/23 11:40:41 Asia/Shanghai · UTC+08:00'. The 'Time Configuration' section has a 'NTP Enabled' checkbox checked. It includes a 'Time Zone' dropdown set to 'Asia/Shanghai · UTC+08:00', a 'Manual Setting' field with '2026/09/23 11:40:40' and a 'Use Browser Time' button, two 'NTP Server' fields with 'ntp.aliyun.com' and 'ntp.ntsc.ac.cn', and a 'Maximum Update Cycle' dropdown set to '1024 秒'. At the bottom right are 'Cancel' and 'Apply' buttons.

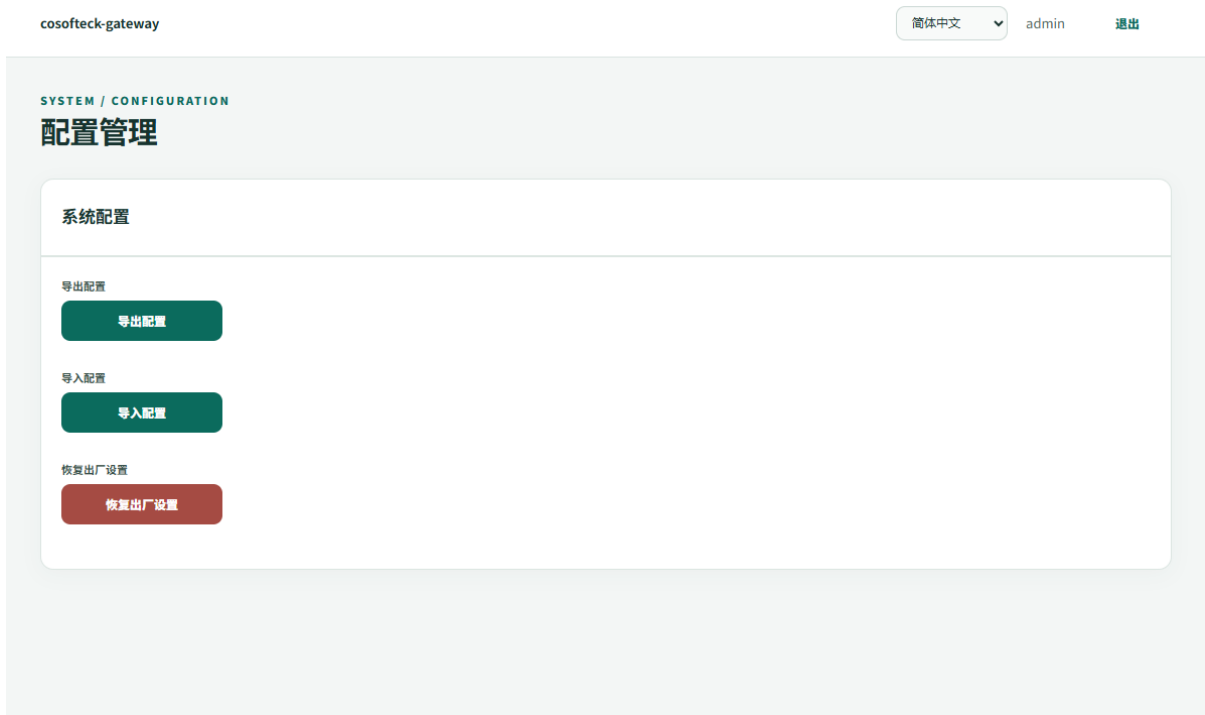
页面标题下显示设备当前时间、时区及 UTC 偏移。时区影响显示时间和每日定时重启时间；NTP 用于通过网络自动校时。

1. 选择时区。下拉项同时显示城市区域和 UTC 偏移。
2. 自动校时：启用 NTP，填写至少一个可访问的 NTP 服务器，并选择“最大更新周期”。可填写服务方提供的域名或 IP 地址。
3. 手动校时：先停用 NTP，输入时间；可点击“使用浏览器时间”把当前管理终端时间写入控件。
4. 点击“应用”保存。启用 NTP 后，系统根据服务器响应调整时间；页面显示设置成功，并不等于已立即完成一次时间同步。

最大更新周期

可选择 64、128、256、512、1024、2048 或 4096 秒，表示自动校时的最大查询间隔。实际间隔随同步情况调整，不是固定倒计时。

7.2 配置管理



操作	使用方法
导出配置	点击“导出配置”，保存下载的 .rkcfg 文件。备份保留设备型号，并包含当前可恢复的配置和相关凭据。
导入配置	点击“导入配置”选择 .rkcfg 文件。校验通过后，在确认框点击“确认恢复”，等待恢复完成。请使用相同产品型号导出的完整配置文件。
恢复出厂设置	点击“恢复出厂设置”，在确认框点击“确认”。设备恢复出厂业务配置；保留当前管理员账号及密码，清除其他 Web 用户。

妥善保管配置文件

导出的配置文件未加密，包含密码、密钥、证书和用户登录凭据。请保存在受保护的位置，仅向授权人员提供，不要上传公开网盘或通过公开渠道发送。

备份范围

配置类别	包含内容
网络设置	网络优先级与探测、蜂窝和无线连接及认证资料、网口角色、WAN、LAN、DHCP/DNS 和静态租约。
路由与防火墙	静态路由；防火墙总开关、各策略开关、MAC/IP 过滤、端口映射、端口转发和 DMZ 设置。
VPN	VPN 总开关、四种协议的服务开关和参数，以及已配置的密码、预共享密钥、证书和私钥。
系统与远程服务	系统时间、定时重启、主机名称、流量月度阈值、软方云、私有 FRP、SSH 和 ADB 启停设置。
用户与登录	Web 用户列表、角色、启停状态和密码；Node-RED 登录凭据。恢复后使用备份时的账号与密码。
不包含的内容	设备 SN 和硬件身份、当前登录会话、运行日志、流量统计、应用软件本体及 Node-RED 流程。配置备份不能替代这些内容的单独备份。

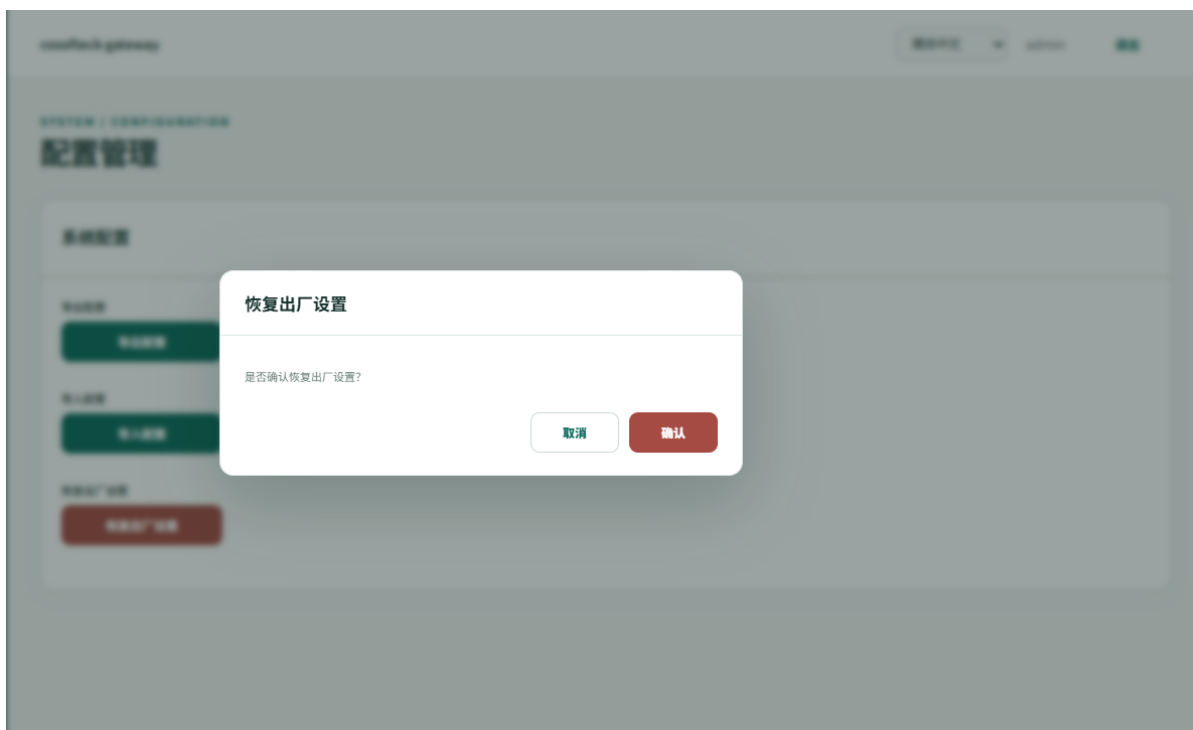
导入配置的操作步骤

- 先导出当前配置，记录设备当前地址，并确认持有备份文件中管理员的登录密码。用于其他设备时，应选择相同产品型号，并核对现场网络条件。
- 选择需要恢复的 .rkcfg 文件。校验通过后显示恢复确认框；确认前核对所选文件，保留原始导出文件，不要手工修改。
- 点击“确认恢复”，保持供电并等待完成。导入会覆盖相应设置，可能改变设备 IP、网络连接、维护服务和登录凭据，当前页面也可能退出登录。
- 按备份中的网络地址重新连接，使用备份时的 Web 用户及密码登录。检查路由、防火墙、VPN、远程服务、SSH/ADB 和 Node-RED 是否符合预期。

恢复后的检查

按备份中的地址和账号重新登录，检查网络连接、VPN、防火墙和远程服务是否符合现场用途。用于其他设备时，还应核对接线、SIM 卡及服务账号。

7.2.1 网页恢复出厂设置



恢复后的重新连接

用网线将电脑连接 ETH0，网卡设置为自动获取 IP 和 DNS，再访问 <http://192.168.10.1/>。出厂 DHCP 已启用，ETH0 为 LAN，ETH1 为自动获取地址的 WAN。网页恢复后使用保留的管理员账号和密码登录；Node-RED 使用 admin / admin。SSH 和 ADB 均为停用状态。

7.2.2 物理按键恢复出厂设置

忘记 Web 登录密码或无法进入管理页面时，可使用设备上的物理按键恢复出厂设置。此操作会清除现有网络和业务设置，请先确认可以中断当前业务。

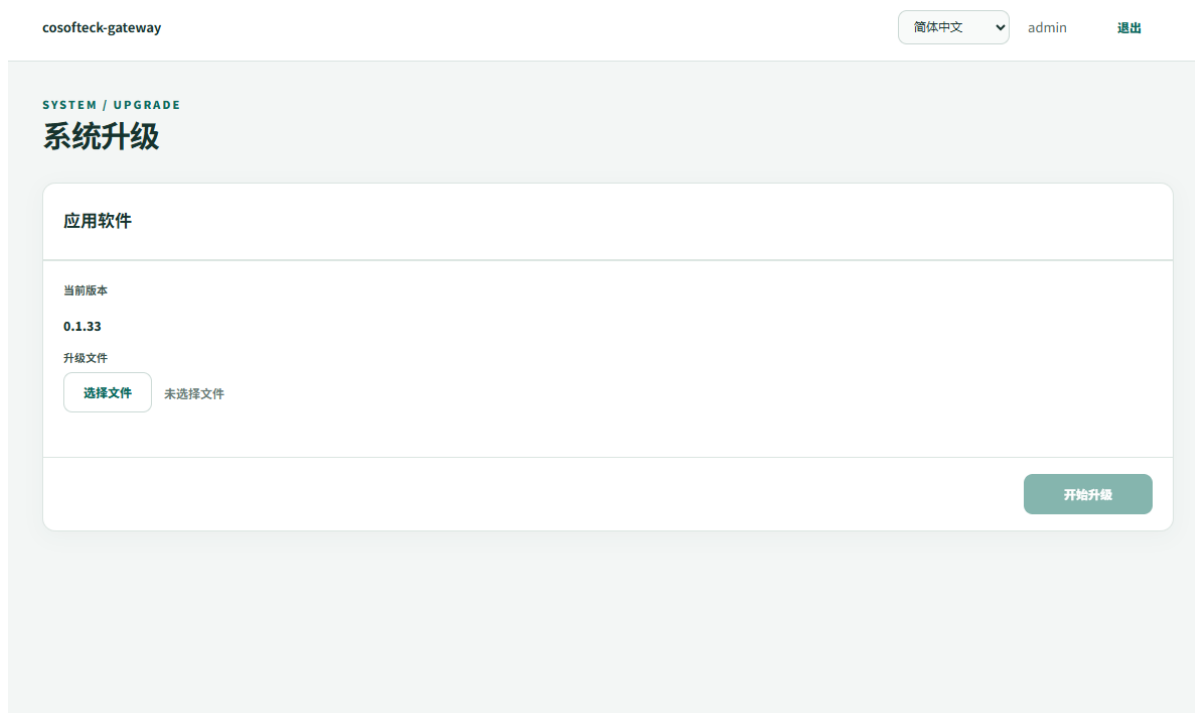
1. 保持设备可靠供电，等待设备正常运行。若上电时已按住按键，先松开，再重新按住。
2. 连续按住物理按键至少 8 秒，达到触发时间后松开。短按或未满 8 秒松开不会触发恢复。
3. 等待设备完成恢复，不要断电或连续重复按键。
4. 按上一节的方法通过 ETH0 访问 <http://192.168.10.1/>，使用 admin / admin 登录。
5. 立即修改默认密码，再重新配置业务；也可导入已保存的配置，导入后使用备份中的账号与密码。

项目	网页恢复出厂	长按物理按键 8 秒
确认方式	点击确认框中的“确认”	持续按键触发，无网页确认
Web 登录	保留当前管理员账号及密码	恢复为 admin / admin
其他 Web 用户	删除	删除
Node-RED 登录	恢复为 admin / admin	恢复为 admin / admin
LAN / 网口	192.168.10.1/24，DHCP 启用；ETH0 为 LAN，ETH1 为 WAN	与网页恢复相同
SSH / ADB	均停用	均停用
MAC/IP 过滤	停用	停用

不可撤销

两种恢复方式都会中断网络，并清除现有业务配置。请提前导出配置；物理按键恢复后务必更改默认密码。

7.3 系统升级



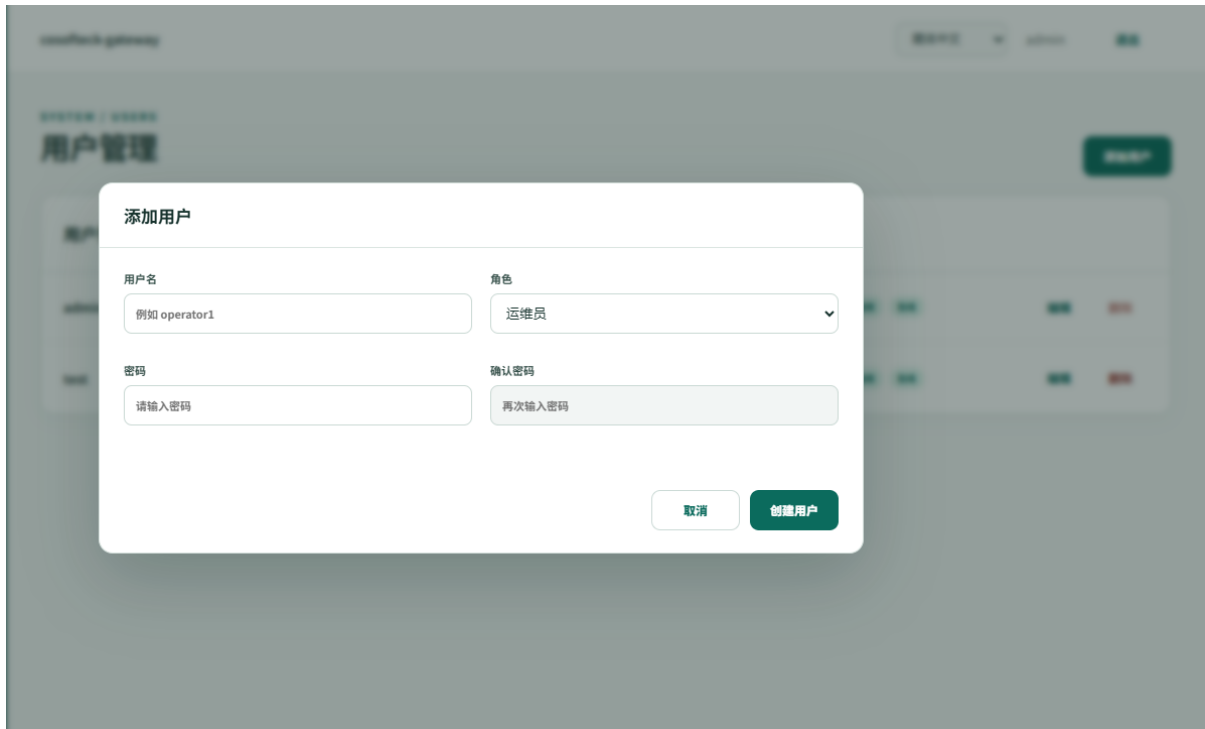
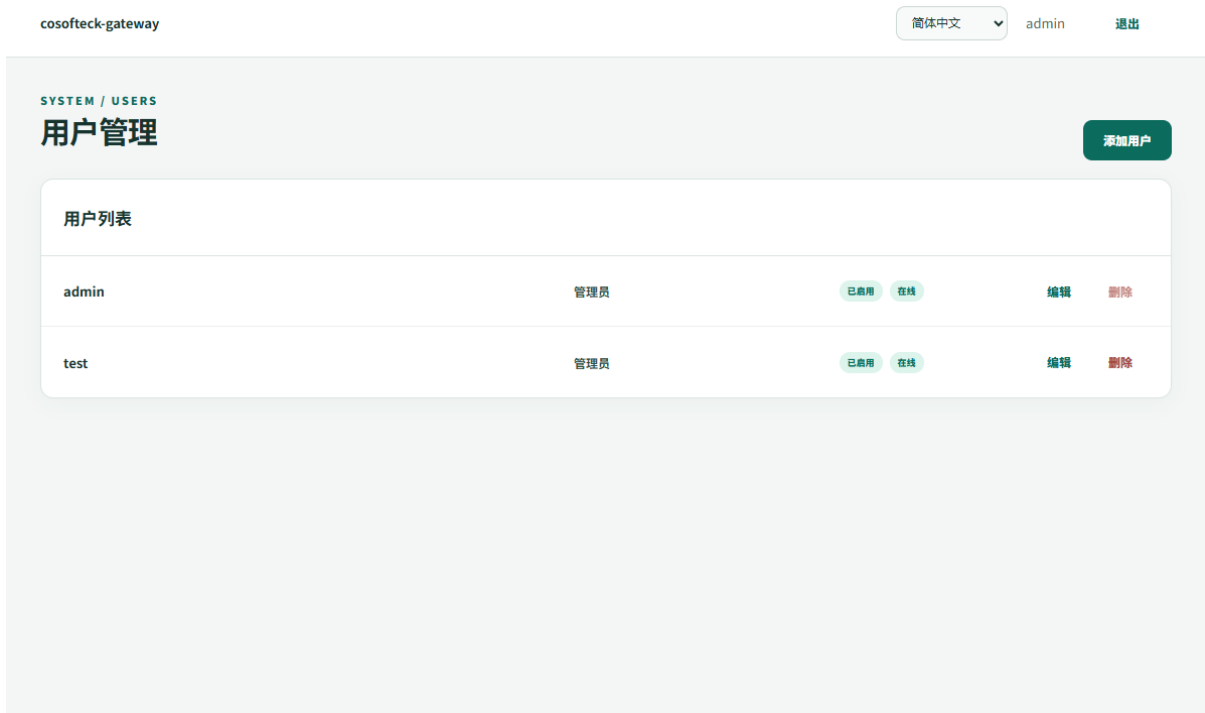
“应用软件”卡片用于升级设备的应用软件。页面显示当前版本，可选择与 C1312B 匹配的 .rkapp 升级文件。

1. 升级前导出系统配置，并确认设备电源和存储空间正常。
2. 在“升级文件”选择由可信渠道提供、与 C1312B 匹配的 .rkapp 包。
3. 点击“开始升级”。文件不适用或校验失败时，页面会给出提示，请勿更改文件后强行重试。
4. 升级期间不要断电、关闭页面或重复提交。服务可能短时重后，浏览器可稍后重新连接。
5. 升级完成并重新连接后，在“系统升级”或“设备概览”中查看应用版本，确认网络和常用业务可正常使用。

升级包来源

只使用软方电子科技或项目服务方明确提供给 C1312B 的升级包。不要改名、解压后重新压缩或修改文件内容。

7.4 用户管理



角色	权限范围
----	------

角色	权限范围
管理员	完整权限；可管理用户、配置备份/恢复、升级、重启、系统参数、远程管理、SSH 和 ADB。
运维员	可登录、查看状态并进行日常网络和时间等运维操作；不能访问管理员专属系统功能。

- 用户名为 3 - 32 个字符，以字母或数字开头，可使用字母、数字、点、下划线和短横线；不可与已有用户名重复。
- 密码为 6 - 128 个字符，至少包含大写字母、小写字母、数字、特殊字符中的两类。添加时再次输入确认密码；请为不同用户设置独立密码。
- 编辑用户可修改角色、重置密码及启停账户；账户启用开关位于编辑框标题栏。
- 用户列表状态区域显示“已启用/已停用”和“在线/离线”。
- 系统必须保留至少一个已启用的管理员；删除用户需要弹窗确认。

7.5 系统重启

cosofteck-gateway

简体中文admin退出

SYSTEM / REBOOT

系统重启

定时重启

☐ 重启已停用

执行时间

03:00

当前时区: Asia/Shanghai

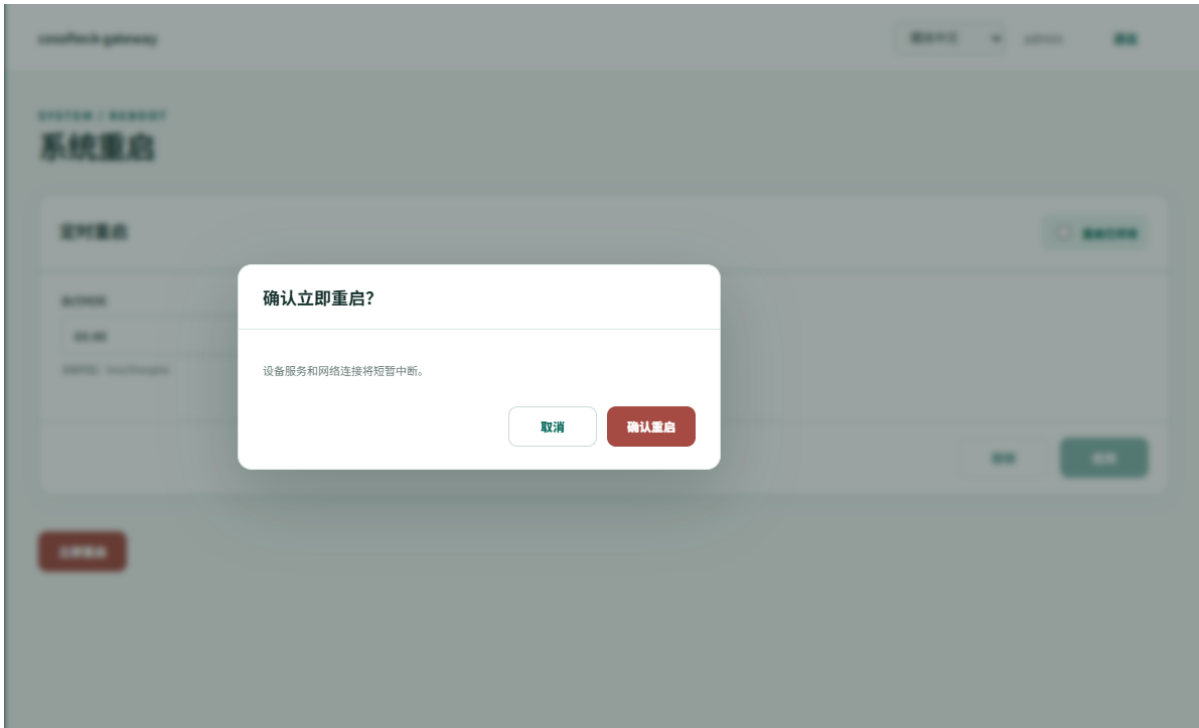
撤销

应用

立即重启

定时重启按设备当前时区每天执行。打开标题右侧开关、设置时间并点击“应用”即可保存，不再进行二次确认。

立即重启会中断全部网络和业务服务。点击红色“立即重启”后，在确认框确认即可，无需再次输入密码。



重启前检查

确认没有应用升级、配置恢复或其他重要操作正在进行，通知使用人员。确认重启后等待设备重新上线，再访问管理页面。

7.6 系统参数

cosofteck-gateway

简体中文admin退出

SYSTEM / PARAMETERS

系统参数

通用

主机名称

流量月度阈值

cosofteck-gateway

0MB

撤销

应用

参数	说明
主机名称	显示在页面顶部和设备概览中；支持中文，不要求以字母或数字开头或结尾。
流量月度阈值	设置蜂窝月度流量阈值，单位 MB；0 表示不设置阈值。达到阈值时弹窗警告：有可用备用网络则停用蜂窝并切换；没有备用网络则保持蜂窝连接。详见 4.2。

7.7 远程管理

cosofteck-gateway简体中文admin退出

SYSTEM / REMOTE

远程管理

软方云服务

服务已停用

用户名

☐ 发送心跳包

心跳包

心跳包间隔

30

秒

撤销

应用

私有FRP服务

服务已停用

服务器地址

服务器端口

协议

frp.example.com

7000

HTTP

撤销

应用

7.7.1 软方云服务

软方云服务用于设备接入软方云及相应的远程访问。启用后填写用户名和心跳参数，点击本卡片“应用”；停用后，软方云连接及其对应的默认远程访问会一并停止。

参数	说明
服务开关	启用后可填写本卡片参数；点击“应用”保存启停状态。
用户名	由软方云平台或项目管理员提供，最多 128 字节。
发送心跳包	开启后按设定间隔发送填写的心跳内容。
心跳包	按平台要求填写单行文本，最多 512 字节；关闭发送开关时不发送。
心跳包间隔	1 - 86400 秒；通常按平台要求设置，不宜设置过短。

7.7.2 私有 FRP 服务

私有 FRP 服务与软方云服务相互独立，可单独启停。先打开本卡片服务开关，填写服务方提供的“服务器地址”“服务器端口”，再选择 TCP 或 HTTP，最后点击本卡片“应用”。服务器端口范围为 1 - 65535。

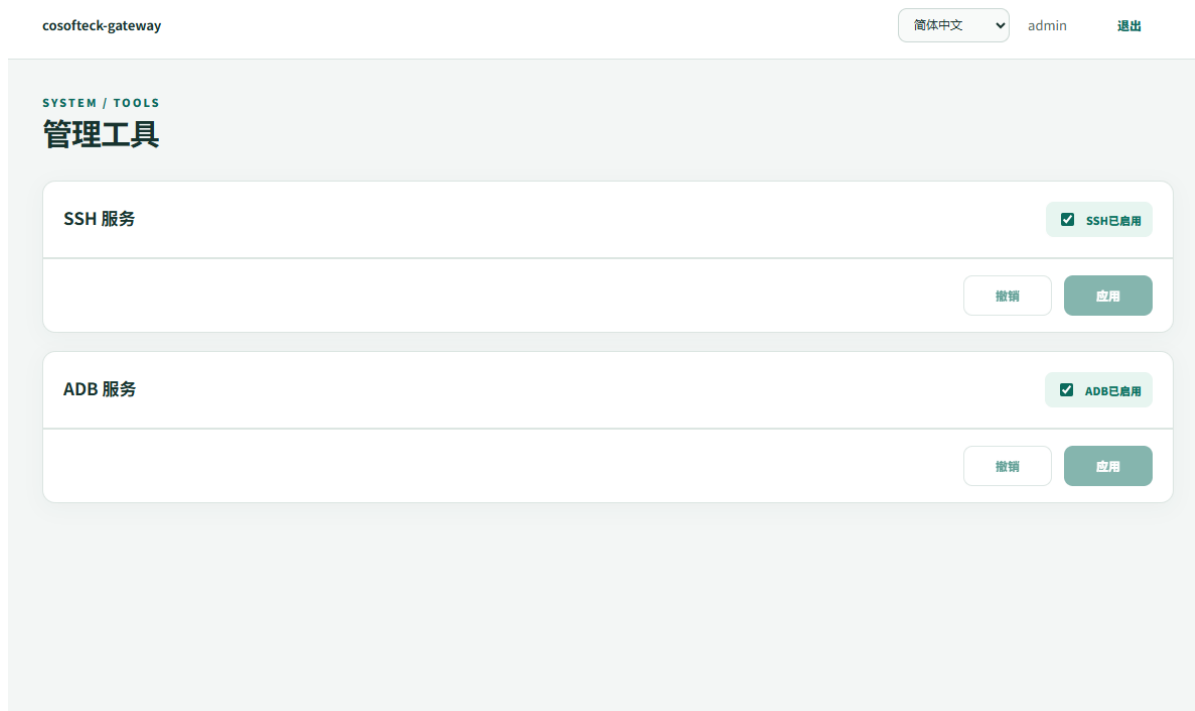
协议	页面设置	远程访问方法
TCP	填写“远程管理端口”，范围 1 - 65534；由服务方分配，不能与其他设备冲突。	Web 使用设置的远程管理端口；Node-RED 使用该端口加 1。两个端口均需由服务方分配并允许访问。
HTTP	不需要填写远程管理端口；使用服务方提供的 HTTP 访问条件。	使用服务方分配或确认的设备访问域名。

远程访问

应用后，使用服务方提供的访问地址，从外部网络打开设备管理页面或 Node-RED 页面。服务器地址和服务器端口应与服务方提供的信息一致。

7.8 管理工具

管理员进入“系统管理 > 管理工具”，可分别控制 SSH 服务和 ADB 服务。两个服务独立启停，日常网页管理不依赖它们；仅在需要维护设备时启用。



恢复出厂设置后，SSH 和 ADB 默认停用。需要维护时，请先在本页面启用对应服务并点击“应用”。

7.8.1 SSH 服务

SSH 用于远程终端维护。在“SSH 服务”区域调整开关后，点击“应用”使设置生效；点击“撤销”放弃尚未应用的修改。

- 停用 SSH 可能中断已有 SSH 连接。操作前确认仍能通过管理网页访问设备。

7.8.2 ADB 服务

ADB 用于设备维护。启用后，维护人员可通过 USB 数据线或可达的局域网连接设备；网络 ADB 的连接端口为 5555。同一个开关同时控制 USB ADB 和网络 ADB。

启用或停用

- 在“ADB 服务”区域调整标题右侧的开关，选择“ADB 已启用”或“ADB 已停用”。仅改变开关尚未生效。
- 点击该区域的“应用”。处理期间按钮显示“正在应用…”且不可重复点击，请等待操作完成。
- 出现设置成功提示后，检查开关状态是否与预期一致。成功应用的启停设置会保留，设备重启后继续生效。
- 如需放弃尚未应用的改动，点击“撤销”，恢复为已保存的设置。

连接与使用注意

- USB 连接：使用支持数据传输的 USB 线连接电脑与设备。启用 ADB 服务并应用后，由维护人员使用电脑上的 ADB 工具进行连接。
- 网络连接：在受信任的局域网中，维护人员可使用设备当前 IP 地址和 ADB 端口进行连接。请仅向授权人员开放维护入口。
- 停用 ADB 会同时关闭 USB ADB 与网络 ADB，并中断已有 ADB 连接；不会关闭管理网页或 SSH 服务。停用前先结束正在进行的 ADB 维护操作。
- 需要再次连接时，在管理网页中重新启用 ADB 并点击“应用”。请仅在可信网络和维护期间开启，维护完成后及时停用，不要将网络 ADB 暴露到互联网。

8 使用注意事项

使用设备时，请妥善保管账号和配置文件，按实际用途启用远程或维护服务，并在重要配置变更前完成备份。

8.1 账号与会话

- 为每位维护人员创建独立账号，不共享管理员账号。
- 投入使用后立即更改交付密码，并定期更换。
- 离开管理终端时点击“退出”；同一账号的新登录会撤销旧会话。
- 只给确需系统级操作的人员分配管理员角色，日常维护使用运维员。

8.2 网络与远程访问

- Web 管理入口只应从受信 LAN 或经过认证的 VPN/FRP 通道访问。
- 优先使用精确端口映射，不建议长期启用 DMZ。
- 新项目优先选择 IKEv2/IPsec 或 OpenVPN，不使用 PPTP。
- 远程管理服务应使用项目独立账号、域名和端口；变更后从外部网络实际验证。
- 网络和防火墙变更前导出配置，记录原地址，并安排能够通过 ETH0 重新接入的现场条件。

8.3 配置与升级

- 配置验收后、重大变更前、升级前分别导出 .rkcfg。
- 备份包含密码、密钥、证书和登录凭据，请限制文件访问权限并通过安全渠道保存与传递；不要将完整备份当作普通附件发送。
- 升级包必须验证来源和型号，升级期间保证稳定供电。
- 通过管理页面修改参数，修改后核对相关网络或服务状态。