

BESS 软件用户手册

版本 **1.0**，2025 年 1 月

www.moxa.com/products



© 2025 Moxa 公司版权所有。

BESS 软件用户手册

本手册中所述软件是根据许可协议提供的，并且只能根据该协议的条款使用。

版权声明

© 2025 Moxa 公司版权所有。

商标

MOXA 徽标为 Moxa Inc. 的注册商标。

本手册中出现的其他商标或注册商标归其各自制造商所有。

免责声明

- 本文件内容如有更改，恕不另行通知，且不构成 Moxa 的任何承诺。
- Moxa 按原样提供本文档，不作任何明示或暗示的担保，包括但不限于针对特定用途的适用性担保。Moxa 保留随时对本手册或本手册中所述产品和/或程序进行改进和/或更改的权利。
- 本手册中提供的信息力求准确、可靠。然而，Moxa 不对其使用或因其使用而导致的任何第三方权利侵害承担任何责任。
- 本产品可能存在非故意的技术或排版错误。我们将定期修改文中信息以纠正此类错误，并将这些修改纳入出版物的新版本中。

技术支持联系信息

www.moxa.com/support

文档版本状态

版本	说明	最后修订
1.0	初始版本	2025 年 3 月

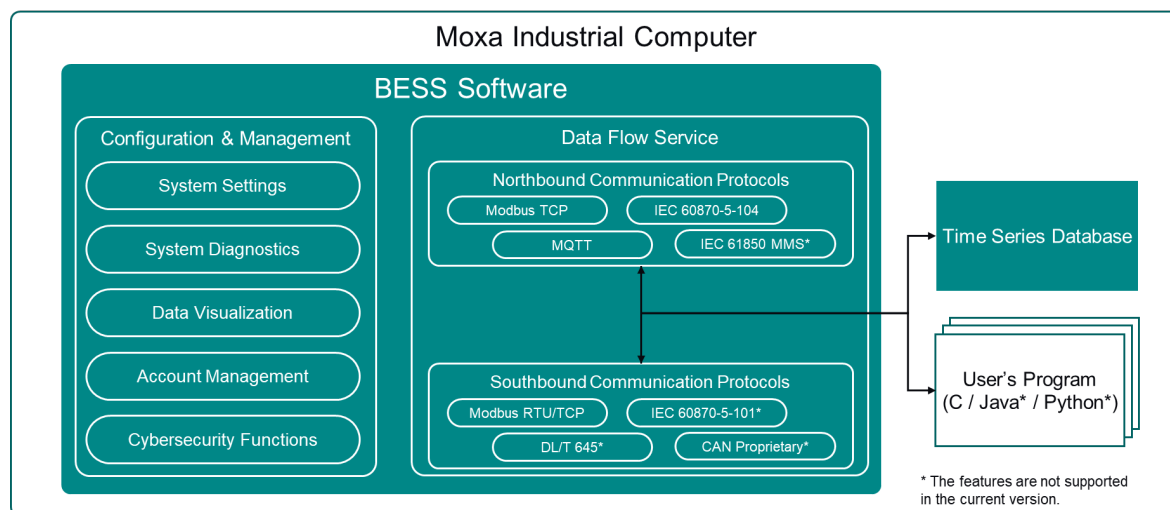
目录

1. 介绍	6
概述	6
2. 快速入门	7
访问 Web 控制台	7
首次登录流程	7
3. 网络安全注意事项	9
更新软件	9
关闭未使用的服务与端口	9
启用必要的服务	9
IP 访问限制	9
账户和密码	10
系统日志	10
设备部署	10
安全环境评估	10
4. Web 控制台配置与故障排除	11
标签仪表板	11
最新数据	11
历史数据	14
系统设置	16
通用	16
串口	17
I/O	17
数据保存	21
网络设置	22
以太网	23
蜂窝网络	24
网络管理	25
OpenVPN 客户端	26
协议设置	26
协议组合	26
Modbus 客户端	28
Modbus TCP 服务器	41
IEC 60870-5-104 服务器	45
MQTT 客户端	48
账户管理	60
账户	60
群组	63
密码策略	65
安全	66
服务	66
白名单	67
证书	68
登录设置	69
维护	70
配置导入/导出	70
软件升级	72
软件恢复默认设置	74
重启	75
诊断	75
系统日志	75
协议状态	78
网络监控	82

	Ping.....	82
A.	如何使用库进行开发.....	84
	前言	84
	准备开发环境	84
	快速入门：构建您的首个应用程序	85
	应用示例	86
	常见问题解答	96
B.	C 语言库函数引用	97
C.	高级 MQTT 发布主题配置	106
	概述	106
	影响发布性能的关键参数	106
	配置指南和示例	106
D.	安全强化指南	109
	介绍	109
	常规系统信息	109
	支持的设备和系统	109
	物理安全措施	109
	配置和强化信息.....	109
	TCP/UDP 端口和推荐服务	109
	串行端口和推荐服务	113
	HTTPS 和 SSL 证书	113
	软件补丁和升级.....	114
	补丁管理	114
	软件升级	115
	停用建议	115
	安全信息与漏洞反馈	115

概述

Moxa 的电池储能系统软件 **BESS Software** 为控制器提供了数据采集和数据上传功能。本文中简称为“该软件”。该软件包含两大核心功能：数据流服务和配置管理服务，如下图所示。



数据流服务支持储能系统常用通信协议，包括 Modbus RTU/TCP Client、Modbus TCP Server、IEC-60870-5-104 Server 及 MQTT。通过这些通信协议，该控制器可以实现对现场设备（例如 BMS、PCS、环境监测系统等）的数据采集和控制命令下发，以及与服务器端设备（例如上级 EMS 系统、SCADA 系统、云平台等）的数据同步和命令接收。此外，数据流服务还提供数据存储功能，将收集的数据保存在时序数据库中。通过附加软件库，用户开发的软件可以访问数据流服务中的实时数据和时序数据库中的历史数据，用于分析或决策。

配置管理服务包括系统设置、通信与系统诊断、数据可视化、帐户管理和网络安全功能。通过一站式网页界面，用户可以进行系统范围的设备操作。在储能系统的集成和运行阶段，网页界面还支持通信与系统诊断以及数据追踪。帐户管理和安全保护功能确保整个储能系统安全、稳定、可靠地运行。

访问 Web 控制台

下表列出了适用产品的默认 IP 地址。

型号	VM-1220-T-BESS	
LAN 端口	IP 地址	网络掩码
LAN 1	DHCP	-
LAN 2（默认）	192.168.4.127	255.255.255.0
LAN 3	192.168.5.127	255.255.255.0
LAN 4	192.168.6.127	255.255.255.0

要使用默认 IP 地址访问 Web 控制台，请执行以下操作：

- 1. 确保您的主机和设备位于同一子网中。连接到默认 LAN 端口（例如 LAN 2）并在您的网络浏览器中输入 **https://192.168.4.127:8443**。
- 2. 输入账号和密码信息。



首次登录流程

- 1. 出于网络安全考虑，Web 控制台没有默认用户名和密码，您需要在首次登录时创建首个帐户。首个帐户将拥有 Web 控制台的全部权限。请妥善保管账户名和密码。默认密码必须满足至少 8 个字符的最低复杂度要求。您可通过 **Account Management（账户管理）** 中的 **Password Policy（密码策略）** 功能进行修改。



Create account on
VM-1220-T-BESS_1000706

Account Name

New Password 

Confirm New Password 

Create

2. 请仔细阅读《MOXA 最终用户许可协议》。如果您同意协议条款，请勾选方框以表示您同意。然后输入正确的账户名和密码登录。



Sign in to
VM-1220-T-BESS_1000706

Account

Password 

☒ I have read and agree [end-user license agreement \(EULA\)](#)

Sign In

3. 网络安全注意事项

随着网络攻击的数量和复杂程度不断增加，网络设备供应商正在增加旨在保护敏感商业和个人信息的功能。Moxa 致力于通过开发安全标准措施，确保所有产品均符合安全标准，让客户可以放心使用 Moxa 的产品。部分措施 Moxa 无法独自完成，需客户与 Moxa 协同构建安全环境以抵御各类网络威胁。本章介绍增强 Moxa 产品网络安全性的基本步骤。客户可能需要参考用户手册中的其他章节，以获取具体设置或命令。

更新软件

当客户从 Moxa 或经销商处购买产品时，Moxa 可能已经发布了较新版本的软件，通常包含增强的安全功能。请联系您所在地区的销售代表，了解是否有更新版本的软件。如有，建议将软件升级到最新版本。

关闭未使用的服务与端口

想象一下住在一个有许多入口的房子里。如果所有门窗都没有锁，甚至敞开着，就等于在向人们传递欢迎入侵者的信号。我们始终建议关闭未使用的服务与端口，以减少受到攻击的概率。

参考**第 D 章：安全强化指南**获取更多配置指导。

启用必要的服务

建议启用某些服务，因为这些服务是软件的关键功能之一，并且其设计旨在应对网络安全威胁，且这些服务的通信在以太网网络上加密的。

- **Web 控制台 (HTTPS)**: 这是该软件的主要管理控制台，用于配置所有设置，其还为工程师提供了一些诊断工具来排查问题。

参考**第 D 章：安全强化指南**获取更多配置指导。



注意

如果所有 HTTPS/SSH/串口控制台都关闭，则没有其他途径可以访问该产品。恢复的唯一方法是重置设备重新配置。请参阅用户手册了解如何重置设备。

IP 访问限制

限制可以访问设备的 IP 地址数量是阻止未经授权的入侵者的最有效方法之一。如果仅有限数量的台式机、笔记本电脑或移动设备需要访问该设备，请授予这些 IP 地址访问权限。

该软件提供 **Allowlist（白名单）** 功能（**Security > Allowlist（安全 > 白名单）**），可授权单个 IP 或 IP 地址范围访问设备。用户可以为授权的 IP 地址添加规则，然后启用白名单功能，以确保只有这些 IP 地址才能访问运行该软件的特定设备。

白名单

Info

启用白名单后，仅允许白名单中启用的 IP 与设备进行通信。

☐ 白名单 ⓘ

[+ 添加规则](#)

编号	IPv4 地址	子网掩码	状态
没有可显示的规则。单击 添加规则 按钮创建第一条规则。			

账户和密码

- 该软件无默认账户名或密码。您需要按照首次登录流程为该设备的首个用户（即管理员用户）设置账户名和密码，以增强其安全性。
- 使用安全性强的密码。该软件支持 **Password Policy（密码策略）** 以检查密码强度。您可以启用此功能来帮助验证。
- 使用帐户登录失败锁定功能，防止未经授权的访问（**Security > Login Settings > Login Lockout（安全 > 登录设置 > 登录锁定）**）。

系统日志

系统日志可以记录设备上发生的各种情况，例如登录失败、IP 地址更改、密码更改、配置更改等。定期检查日志以发现任何异常行为。

设备部署

建议将运行该软件的设备部署在具有足够安全功能的安全防火墙网络后方，以确保网络免受内部和外部威胁。

确保设备和/或系统的物理保护符合应用程序的安全要求。根据环境和威胁情况，保护形式可能会存在很大差异。

安全环境评估

除了这些支持保护功能的设备之外，网络管理员还可以参考以下建议来保护网络和设备。

为防止未经授权访问设备，请遵循以下建议：

- 提供网络安全环境检查测试工具。一些工具提供有限的免费使用，例如 **Nessus**。这些工具有助于识别环境中的潜在安全漏洞。
- 该设备应在受防火墙或路由器保护的安全网络中运行，以阻止来自互联网的攻击。
- 对串行控制台的访问权限应与对设备的物理访问权限一样进行管控。
- 限制并发的 **Web** 服务器会话数。
- 定期更改密码。
- 定期备份配置文件并检查运行时设置的 **CRC** 值，以确保设备正常运行。
- 定期审核设备以确保符合建议和/或内部安全政策。
- 如果需要将设备退回 **Moxa**，请确保在退回之前已禁用加密并备份当前配置。



注意

免责声明：请注意，上述信息和指南（“信息”）仅供参考。我们不能保证完全免受网络威胁。这些指南旨在提升安全级别以防御网络交互，但不保证满足特定需求。以上信息按“原样”提供，我们对其准确性、完整性或性能不作任何明示、暗示或其他形式的保证。

4. Web 控制台配置与故障排除

本章简要概述了如何使用 Web 控制台配置软件。

标签仪表板

在软件中，通信协议中收集或使用的每个数据点都被标记为一个 **tag (标签)**。Tag Dashboard (标签仪表板) 提供集中视图来监控标签属性，包括：

- **Provider (提供者)** - 创建标签的协议或软件组件。
- **Source (来源)** - 与标签关联的特定设备或连接。
- **Name (名称)** - 标签标识符。
- **Data Type (数据类型)** - 存储值的格式 (例如，整数、浮点数、字符串)。
- **Access Permission (访问权限)** - 读取或修改标签的访问控制级别。
- **Value & Timestamp (数值与时间戳)** - 数据值及更新时间。

本节将指导您使用 **Tag Dashboard (标签仪表板)** 监控**实时**和**历史**标签数据，从而实现高效的故障排除和系统分析。

最新数据

要查看标签的实时值，请执行以下步骤：

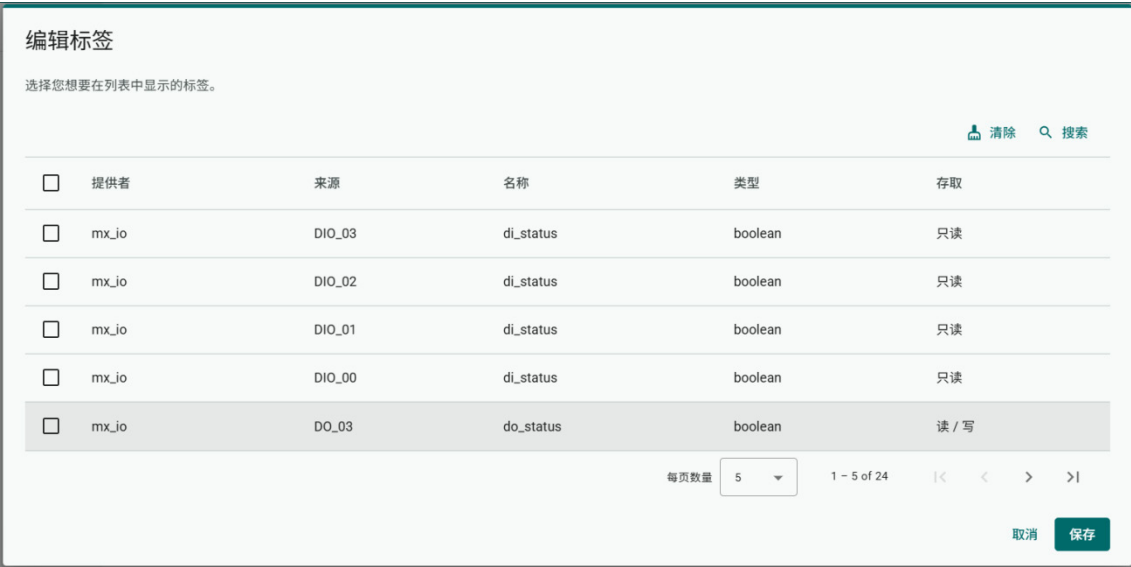
1. 在 **Tag Dashboard (标签仪表板)** 中单击 **Latest Data (实时数据)** 选项卡。



2. 单击 **+ Edit Tags (+ 编辑标签)**。



3. 使用 **Search（搜索）** 快速找到标签。（可选）



4. 在列表中选择要监控的标签。

编辑标签

选择您想要在列表中显示的标签。

24 标签已选定

清除 搜索

☒	提供者	来源	名称	类型	存取
☒	mx_io	DIO_03	di_status	boolean	只读
☒	mx_io	DIO_02	di_status	boolean	只读
☒	mx_io	DIO_01	di_status	boolean	只读
☒	mx_io	DIO_00	di_status	boolean	只读
☒	mx_io	DO_03	do_status	boolean	读 / 写

每页数量

5

1 - 5 of 24

< > >> <<

取消

保存

5. 单击 **Save**（保存）。
6. 按 “⋮” 图标来停止监控标签。（可选）

Home > 标签仪表盘

标签仪表盘

实时数据

历史数据

在这里添加标签并进行监控。您还可以通过点击设置可写标签的值。 “⋮” 这些值在几秒钟内生效。

标签监控中...

搜索 + 编辑标签

	提供者	来源	名称	类型	值	存取	最后更新	
	mx_io	DIO_00	di_status	boolean	0	只读	Aug 05, 2025, 14:11:15	⋮
	mx_io	DIO_01	di_status	boolean	0	只读	Aug 05, 2025, 14:11:15	写入值
	mx_io	DIO_02	di_status	boolean	0	只读	Aug 05, 2025, 14:11:15	停止监控
	mx_io	DIO_03	di_status	boolean	0	只读	Aug 05, 2025, 14:11:14	⋮
	mx_io	DI_00	di_status	boolean	0	只读	Aug 05, 2025, 14:11:13	⋮

每页数量

5

1 - 5 of 24

< > >> <<

7. 按 “⋮” 图标来写入值以直接控制标签。（可选）

Home > 标签仪表板

标签仪表板

实时数据 历史数据

在这里添加标签并进行监控。您可以通过点击设置可写标签的值。* : *

这些值在几秒钟内生效。

标签监控中...

🔍 搜索 + 编辑标签

	提供者	来源	名称	类型	值	存取	最后更新	
	mx_io	DI_02	di_status	boolean	0	只读	Aug 05, 2025, 14:12:49	⋮
	mx_io	DI_01	di_status	boolean	0	只读	Aug 05, 2025, 14:12:49	⋮
	mx_io	DI_00	di_status	boolean	0	只读	Aug 05, 2025, 14:12:49	⋮

每页数量 5 21 - 23 of 23 |< < 写入值 停止监控

历史数据

要查看标签的历史值，请执行以下步骤：

1. 在使用 **Historical Data**（历史数据）之前，请确保 **Data Persistence**（数据保存）已正确启用。（有关详细信息，请参阅 **System Settings**（系统设置）中的“**Data Persistence**（数据保存）”部分。）
2. 在 **Tag Dashboard**（标签仪表板）中单击 **Historical Data**（历史数据）选项卡。

Home > 标签仪表板

标签仪表板

实时数据 **历史数据**

☐ 自动滚动 ⚙️ 选择 开始

编号	值	时间戳
没有可显示的数据		

3. 单击 **Select**（选择）

Home > 标签仪表板

标签仪表板

实时数据 **历史数据**

☐ 自动滚动 ⚙️ 选择 开始

编号	值	时间戳
没有可显示的数据		

4. 选择您想要监控的标签和时间范围。

標籤选择

提供者

mx_io

24 标签

选定标签

di_status

时间窗口

☒ 多久前 ☐ 时间段

时间区间

1 分钟

取消

保存

参数	值	说明
提 供 者	功能模块名称	选择创建标签的协议或软件组件。
选 定 标签	标签名称	选择特定的标签进行监控。
时 间 窗口	上一次，时间段	上一次：从过去到现在的动态时间窗口 时间段：从开始时间到结束时间的静态时间窗口。
上 一 次	时间跨度 (1 分钟（默认）、2 分钟、5 分钟、10 分钟、15 分钟、30 分钟、1 小时、2 小时、5 小时、10 小时、12 小时、1 天、7 天、30 天)	-
时 间 段	开始时间、结束时间	-

5. 单击 **Save**（保存）。
6. 单击 **Start**（开始）监控选定标签。

Home > 标签仪表板

标签仪表板

实时数据

历史数据

标签名: modbus_tcp_client/windows/temperature

选择

开始

☐ 自动滚动

编号

值

时间戳

没有可显示的数据

7. 显示指定时间范围内标签的历史数据记录。

Home > 标签仪表板

标签仪表板

实时数据

历史数据

标签名: modbus_tcp_client/windows/temperature

自动滚动

正在捕获...

编号	值	时间戳
67	338	2025-08-05 06:25:18.081
68	339	2025-08-05 06:25:19.08
69	339	2025-08-05 06:25:19.08
70	340	2025-08-05 06:25:20.081
71	341	2025-08-05 06:25:21.077
72	342	2025-08-05 06:25:22.082



注意

- 1. 历史数据中显示的时间戳基于设备时区。
- 2. 最多可显示 100,000 条记录。如果数据超过 100,000 条，滚动行为将覆盖顶部最旧的记录。

系统设置

通用

Home > 系统设置 > 通用

通用

设备标识

日期和时间

设备名称

VM-1220-T-BESS-P_0B43

描述 - 可选

保存

标识

参数	值	说明
设备名称	字母数字字符串	输入一个可以帮助您唯一识别设备的名称。例如，可包含设备的名称和功能。
描述 - 可选	字母数字字符串	您可以添加有关该设备的其他描述，例如其功能和位置。

日期和时间

要管理系统时间，请切换到 **Date & Time（日期和时间）** 选项卡。您可以单击 **EDIT（编辑）** 按钮更改当前日期、时间和时区。

Home > 系统设置 > 通用

通用

设备标识

日期和时间

当前日期和时间

Aug 05, 2025 14:27:04

编辑

时区

Asia/Shanghai

编辑

参数	选项	说明
当前日期和时间	手动	使用此设置手动调整日期和时间。
	与 NTP 服务器同步	指定要同步的时间服务器的地址。 此可选字段指定网络上时间服务器的 IP 地址或域名。支持 SNTP（RFC-1769）进行自动时间校准。软件将按照设置的时间间隔向指定的时间服务器请求时间信息。
时区	用户可选择的时区	显示当前选择的时区并允许更改为不同的时区。夏令时将根据地区自动调整。

串口

该软件可以帮助您管理和配置设备的串口参数。串口支持 RS-232 和 RS-485 接口。在使用带有 Modbus RTU 或其他基于串行的协议的串口之前，您应该配置波特率、奇偶校验位、数据位和停止位。不正确的设置将导致通讯失败。

端口号	接口	波特率	校验位	数据位	停止位	流控	
1	RS-485-2W	9600	None	8	1	None	⋮
2	RS-485-2W	9600	None	8	1	None	⋮
3	RS-485-2W	9600	None	8	1	None	⋮
4	RS-485-2W	9600	None	8	1	None	⋮

参数	选项	说明
接口	RS-485 2 线，RS-232 (默认 = RS-485 2 线)	该字段配置串行端口的接口。
波特率	300、600、1200、1800、2400、4800、9600、19200、38400、57600、115200 (默认值 = 9600)	该字段配置串行端口的波特率。
校验位	无、奇数、偶数、标记、空格 (默认 = 无)	该字段配置奇偶校验位的参数。
数据位	5、6、7、8 (默认值 = 8)	该字段配置数据位参数。
停止位	1, 2 (默认值 = 1)	该字段配置停止位参数。
流控	无, XON/XOFF (默认 = 无)	该字段配置流量控制类型。

I/O

该软件使您能够管理和配置设备的 I/O 通道，其中包括：

- **数字输入 (DI)**
- **数字输出 (DO)**
- **数字输入/输出 (DIO)**：可配置为输入或输出。

每个通道关联一个 **tag**（**标签**），可通过**Tag Dashboard**（**标签仪表板**）访问。

DI

您可以在 Web UI 上监控每个 Digital Input（数字输入）的状态：

1. 导航至 **System Settings > I/O**（**系统设置 > I/O**）。
2. 单击 **DI**（**数字输入**）选项卡。

表格中显示各通道的 **Tag Name**（**标签名**）与 **Status**（**状态**）。

Home > 系统设置 > I/O

I/O 设置

DI DO DIO

通道	当前状态
DI_00 mx_io/DI_00/di_status	0
DI_01 mx_io/DI_01/di_status	0
DI_02 mx_io/DI_02/di_status	0
DI_03 mx_io/DI_03/di_status	0
DI_04 mx_io/DI_04/di_status	0
DI_05 mx_io/DI_05/di_status	0
DI_06 mx_io/DI_06/di_status	0
DI_07 mx_io/DI_07/di_status	0

DO

您可以在 Web UI 上监视和管理每个 Digital Output（数字输出）的状态：

1. 导航至 **System Settings > I/O**（**系统设置 > I/O**）。
2. 单击 **DO**（**数字输出**）选项卡。

管理 DO 通道：

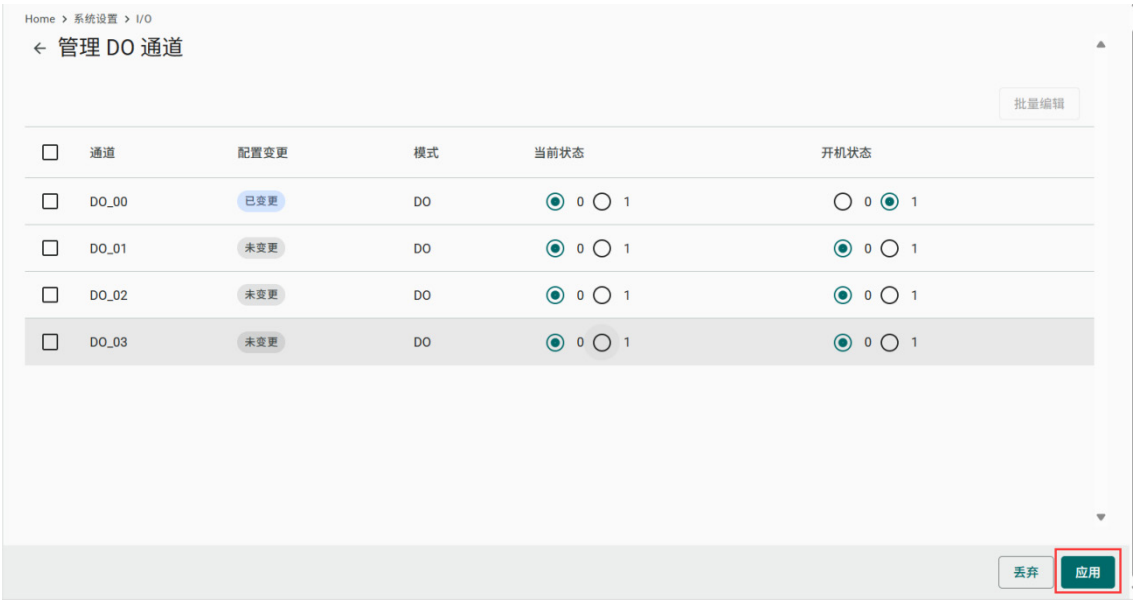
1. 单击 **Manage**（**管理**）按钮。



2. 配置目标通道的参数：

- **当前状态：** 设置通道的当前状态。
- **开机状态：** 定义上电后的初始状态。

3. 单击 **Apply**（应用）保存更改。



参数	选项	说明
当前状态	开启（高电压）	配置通道的状态。
	关闭（低电压）（默认）	
开机状态	开启（高电压）	配置上电后通道的状态。
	关闭（低电压）（默认）	

DIO

您可以在 Web UI 上监控和管理每个 DIO 通道的状态和模式：

1. 导航至 **System Settings > I/O**（系统设置 > I/O）。
2. 单击 **DIO**（数字输入/输出）选项卡。

管理 DIO Channels（数字输入/输出通道）：

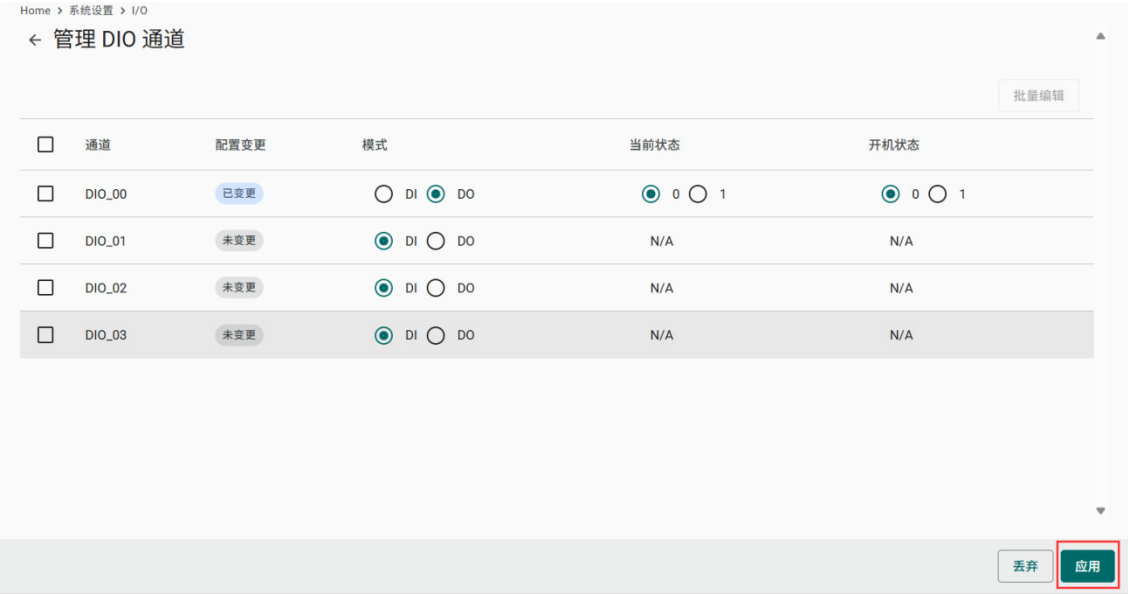
1. 单击 **Manage（管理）** 按钮。



2. 配置目标通道的参数：

- **模式：** 将通道设置为 DI（输入）或 DO（输出）。
- **当前状态：** 设置通道的当前状态。
- **开机状态：** 定义上电后的初始状态。

3. 单击 **Apply（应用）** 保存更改。



参数	选项	说明
当前状态	开启（高电压） 关闭（低电压）	配置通道的状态。
开机状态	开启（高电压） 关闭（低电压）	配置上电后通道的状态。
模式	DI（默认） DO	将通道设置为输入或输出模式。

数据保存

Data Persistence（数据保存）记录所有更新 **values**（值），标签的 **timestamps**（时间戳），并将它们存储在 SD 卡中。存储的数据可以通过 **Tag Dashboard**（标签仪表板）中的 **Historical Data**（历史数据）功能或通过软件库（详情请参考 **System Settings**（系统设置）中的“Data Persistence（数据保存）”部分或“**How to Use the Library for Development**（如何使用库进行开发）”）。

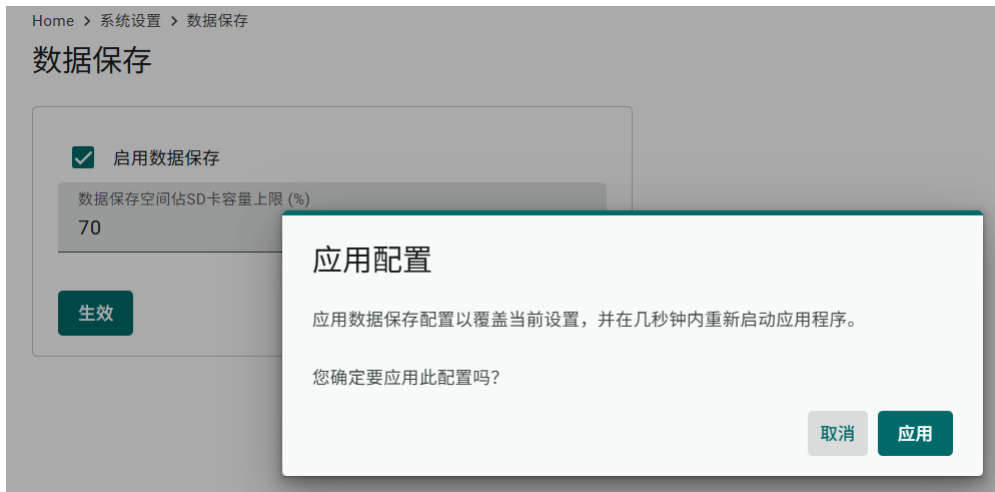
1. 使用 Data Persistence（数据保存）之前，请确保已插入 SD 卡，并且 SD 卡处于已正确启用的 **Service**（服务）中（请访问 **Security**（安全性）中的“**Service**（服务）”部分以启用服务）。
2. 启用 Data Persistence（数据保存）并设置 SD 卡的存储空间限制。



3. 单击 **Apply**（生效）。
4. Data Persistence（数据保存）仅支持 **EXT4** 格式的 SD 卡。如果您使用其他格式，请单击 **Format the SD card to EXT4**（将 SD 卡格式设置为 EXT4）在使用 Data Persistence（数据保存）之前将 SD 卡格式重新设置为 EXT4。（可选）



5. 单击 **Apply**（应用）应用配置。



6. 如果重新配置 SD 卡的存储空间限制，您将丢失先前的所有数据。（可选）



注意

1. 如果您需要 **replace the SD card**（更换 SD 卡）或 **update the device using an image**（使用图像更新设备），应使用 C API（`aegis_get_historical_data_file`）将历史数据导出为可读的 CSV 文件，以防止无法访问历史数据。
2. 如果您想在启用 Data Persistence（数据保存）的情况下移除 SD 卡，请先禁用 Data Persistence（数据保存），然后在 Service（服务）中禁用 SD 卡功能，以避免因不安全移除而导致 SD 卡意外损坏。

网络设置

以太网

要配置网络，请执行以下操作：

- 1. 从 LAN1 至 LAN4 中选择进行配置。
- 2. 选择 WAN（广域网）或 LAN（局域网）。
- 3. 选择 DHCP 或静态模式。
- 4. 配置 IP 地址、子网掩码、网关和 DNS。

Home > 网络设置 > 以太网

以太网

LAN1 LAN2 LAN3 LAN4

WAN (广域网)

模式

☐ DHCP：自动获取 IP 地址

☒ 静态：指定 IP 地址

IPv4 地址

10 . 90 . 62 . 64

子网掩码

255 . 255 . 254 . 0

网关

10 . 90 . 62 . 1

首选 DNS 服务器 - 可选

10 . 123 . 200 . 11

备用 DNS 服务器 - 可选

10 . 123 . 200 . 12

☐ 启用 DHCP 服务器 ⓘ

保存

参数	值	说明
连接类型	WAN、LAN	WAN：广域网 LAN：局域网
模式	DHCP，静态	DHCP：自动从 DHCP 服务器获取 IP 地址。 静态：手动指定 IP 地址。
IPv4 地址	LAN1 默认：DHCP LAN2 默认：192.168.4.127（或其他 32 位数字） LAN3 默认：192.168.5.127（或其他 32 位数字） LAN4 默认：192.168.6.127（或其他 32 位数字）	IP 地址标识 TCP/IP 网络上的设备。
子网掩码	默认：255.255.255.0（或其他 32 位数字）	子网掩码标识设备属于 A 类、B 类或 C 类网络。
网关	0.0.0.0（或其他 32 位数字）	提供设备 LAN 之外的网络访问的路由器的 IP 地址。当连接类型设置为 WAN 时，此参数可用。

首选 DNS 服务器	0.0.0.0（或其他 32 位数字）	主域名服务器的 IP 地址。当连接类型设置为 WAN 时，此参数可用。
备用 DNS 服务器	0.0.0.0（或其他 32 位数字）	辅助域名服务器的 IP 地址。当连接类型设置为 WAN 时，此参数可用。

DHCP 服务器

参数	值	说明
启用 DHCP 服务器	禁用、启用 (默认=禁用)	启用此功能将自动为本地网络上的设备分配 IP 地址和网络设置。
起始 IP	0.0.0.0（或其他 32 位数字）	这是 DHCP 服务器可以分配给客户端的范围内的第一个 IP 地址。
结束 IP	0.0.0.0（或其他 32 位数字）	这是 DHCP 服务器可以分配的范围内的最后一个 IP 地址。
租用时间模式	自定义，无限 (默认=自定义)	DHCP 服务器的租用时间可以自定义，也可以设置无限制。
租用时间	整数值大于 1。 (默认值 = 0)	设备的使用期限允许我们在必须续订租约之前使用 DHCP 服务器分配的 IP 地址。



注意

DHCP 服务器服务仅在 LAN 和静态 IP 接口上可用。

蜂窝网络

您可以在设备上启用或禁用蜂窝连接、创建配置文件、管理 **Profile Settings**（配置文件设置），并启用或禁用连接 **Check-alive**（存活检查）优化蜂窝连接的功能。

Home > 网络设置 > 蜂窝网络

蜂窝网络

CELLULAR1

☐ 启用蜂窝数据通信

配置文件设置

创建并管理 SIM 卡的配置文件。

选择要测试的 (秒)

120

配置文件列表

#1

Profile-1
SIM1

+ 创建

存活检查

☒ 启用存活检查

目标主机

223.5.5.5

Ping 间隔 (秒)

60

保存

您可以在 **Profile Settings**（配置文件设置）部分创建自定义蜂窝配置文件。显示系统中所有配置文件的列表。在此 **Create**（创建），**Edit**（编辑），或 **Delete**（删除）蜂窝配置文件。

要创建新的蜂窝连接配置文件，请执行以下操作：

1. 单击 **+ Create (+ 创建)**。
2. 指定唯一 **Profile Name (配置文件名称)**。
3. 指定目标 **SIM** 卡。
4. 如果您的 SIM 卡需要，请输入 **PIN Code (PIN 码)**。
5. 输入 **APN (接入点名称)**。



6. 单击 **Done (完成)**。
7. 在 **Cellular (蜂窝网络)** 设置页面，单击 **Save (保存)**。

当您在蜂窝部分单击 **Save (保存)** 时，设备将重新启动以应用更改。设备初始化成功后设置才会生效。

Check-alive (存活检查) 功能将通过定期 ping 互联网上的特定主机来帮助您维持设备与运营商服务之间的连接。



注意

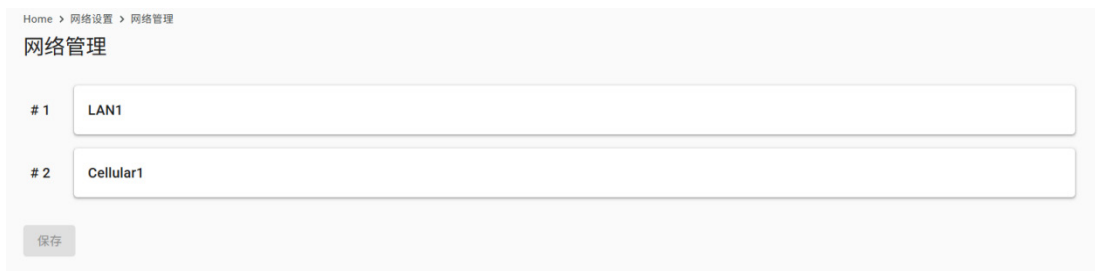
1. 为防止 SIM 卡因三次输入错误而被锁定，当 PIN 重试次数达到 2（仅剩一次尝试机会）时，软件中的机制会停止尝试解锁 SIM 卡。此时，将 SIM 卡插入另一台设备（例如手机）并尝试解锁。这样，当您 SIM 卡重新插入设备并重新启动时，PIN 重试计数将重置为 3。
2. 蜂窝模块可能不支持 SIM 卡热插拔；插入或取出 SIM 卡后需要重启设备。

网络管理

该软件允许您管理 **routing priority (路由优先级)** 不同的网络接口，例如 **cellular (蜂窝)** 和 **LAN (局域网)** 连接。调整优先级有助于优化网络性能。

- **Highest-priority interface (最高优先级接口)** 列在顶部（标记为 **#1**）。
- 一旦高优先级接口连接到互联网，它将被用作 **default gateway (默认网关)**。

要修改路由优先级，请根据您的喜好重新排列接口。



OpenVPN 客户端

OpenVPN 允许您通过互联网创建安全连接。其提供加密和身份验证以确保数据的机密性和完整性。OpenVPN 使用客户端-服务器架构，其中服务器充当 VPN 端点，客户端连接到服务器以建立安全连接。要启用该功能，请转至 **Network Settings（网络设置） > OpenVPN Client（OpenVPN 客户端）**，并执行以下操作：

1. 下载 OpenVPN 配置文件模板。
2. 通过输入您的 VPN 服务提供商提供的必要信息来修改配置文件。这些信息包括：
 - a. **远程服务器 IP**：这是您要连接的 VPN 服务器的地址。
 - b. **端口号**：将通过该端口建立 VPN 连接。默认值通常为 1194。
 - c. **协议**：用于 VPN 连接的协议，例如 UDP 或 TCP。
 - d. **验证方法**：用于验证连接的方法。
 - e. **加密设置**：用于保护 VPN 连接安全的加密算法。
3. 导入 OpenVPN 配置文件。您应该会在 OpenVPN 客户端中看到它。
4. 单击按钮即可启用 OpenVPN 客户端连接。

如果连接成功，您将连接到 VPN 网络，并且您的互联网流量将被加密并通过 VPN 服务器进行路由。

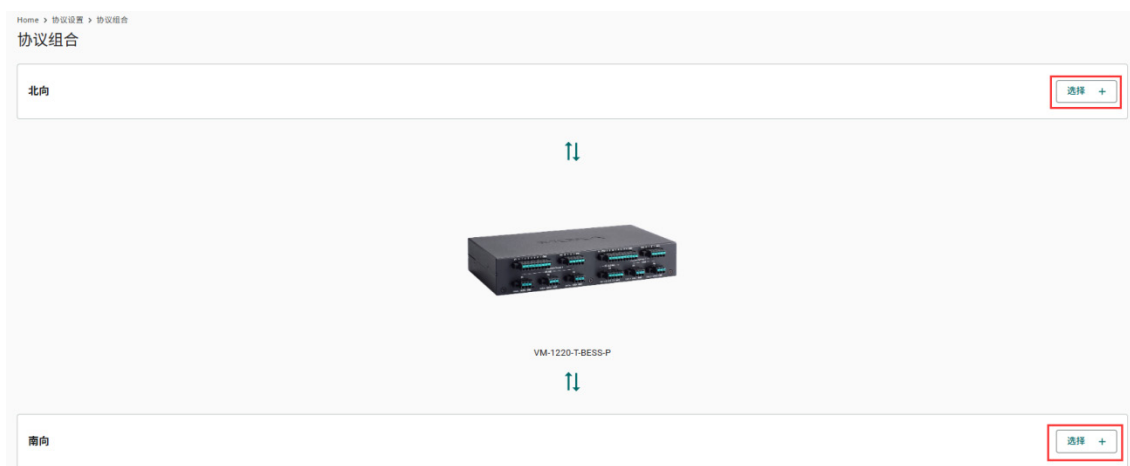


协议设置

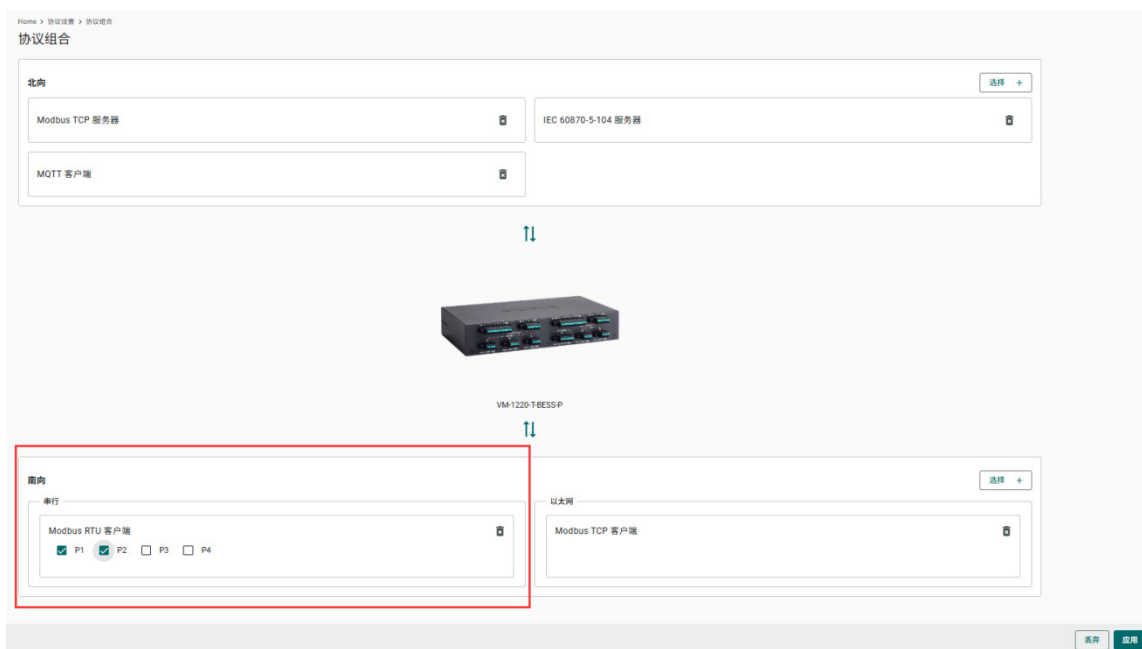
协议组合

协议组合用于启用或禁用设备上的协议模块。在此页面上，您可以配置可启用哪些北向和南向通信。

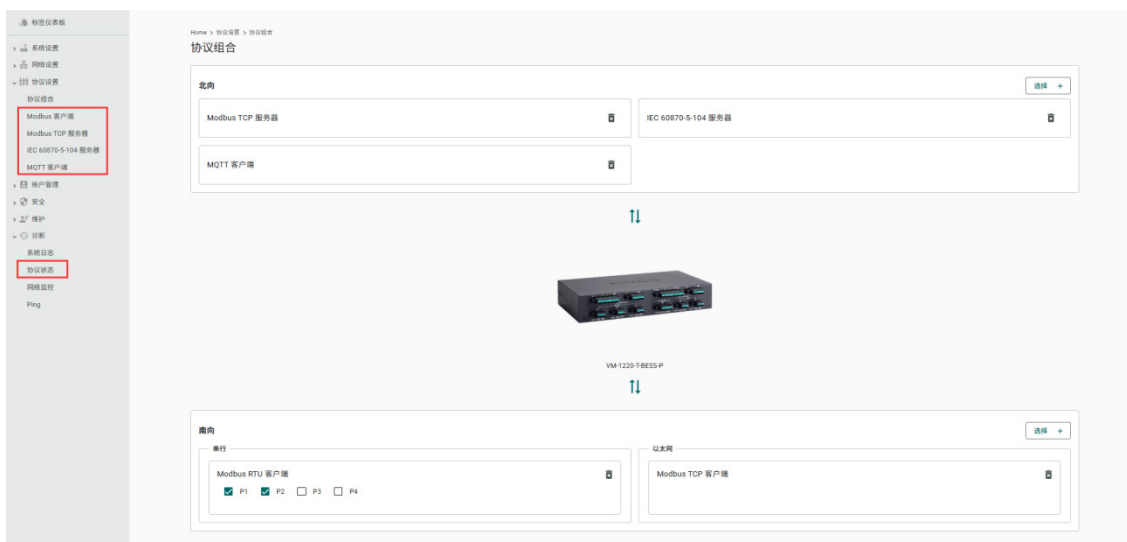
1. 单击 **Select（选择）** 启用北向和南向协议。



2. 如果您选择南向接口的协议为 **Serial（串口）** 或 **CAN**，则须进一步选择该现场总线协议将使用哪个端口。（可选）



3. 单击 **Apply（应用）** 应用设置。
4. 应用配置后，配置页面将出现在 **Protocol Settings（协议设置）** 类别，调试页面将出现在 **Diagnostics/Protocol Status（诊断/协议状态）** 页面下，具体取决于已启用哪些协议模块。



注意

通过协议组合启用协议模块可能会暴露特定的接口（例如，**Modbus TCP 服务器：TCP 端口 502**）并增加系统资源消耗（CPU、内存）。为了最大限度地降低安全风险并优化性能，**仅启用应用程序所需的协议**。

Modbus 客户端

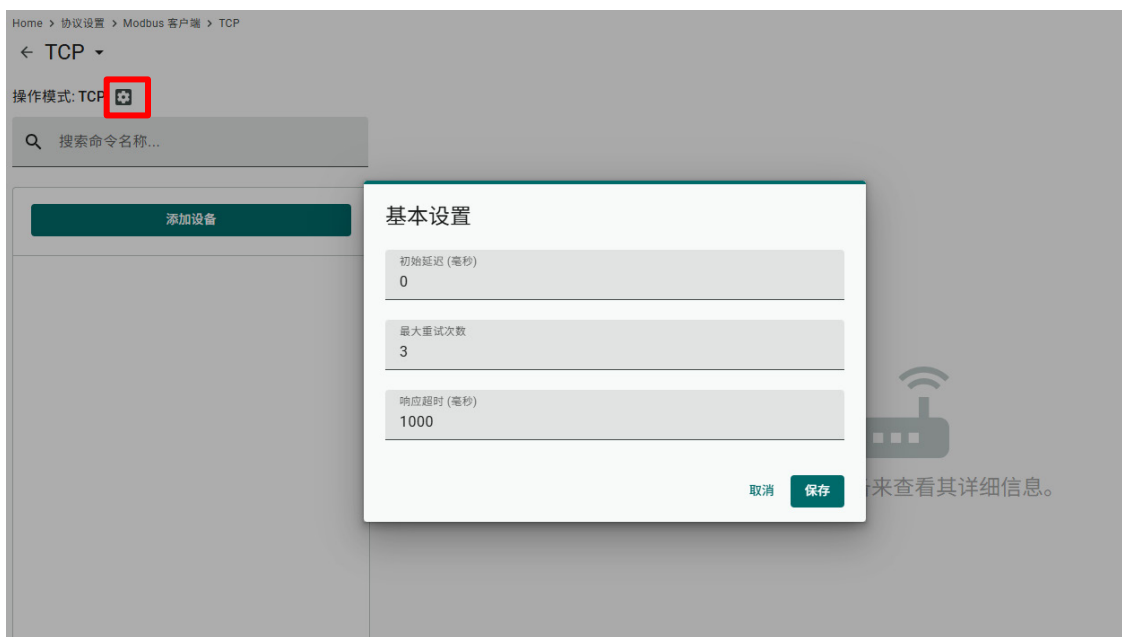
Modbus TCP

本节将指导您在软件中配置 Modbus TCP 设置。该设置由两个主要部分组成：

1. 基本设置 - Modbus 通信的常规配置。
2. Modbus 设备设置 - 用于从 Modbus 设备检索数据的参数。

基本设置

与 Modbus 设备通信之前，请先配置 TCP 操作模式的基本设置。



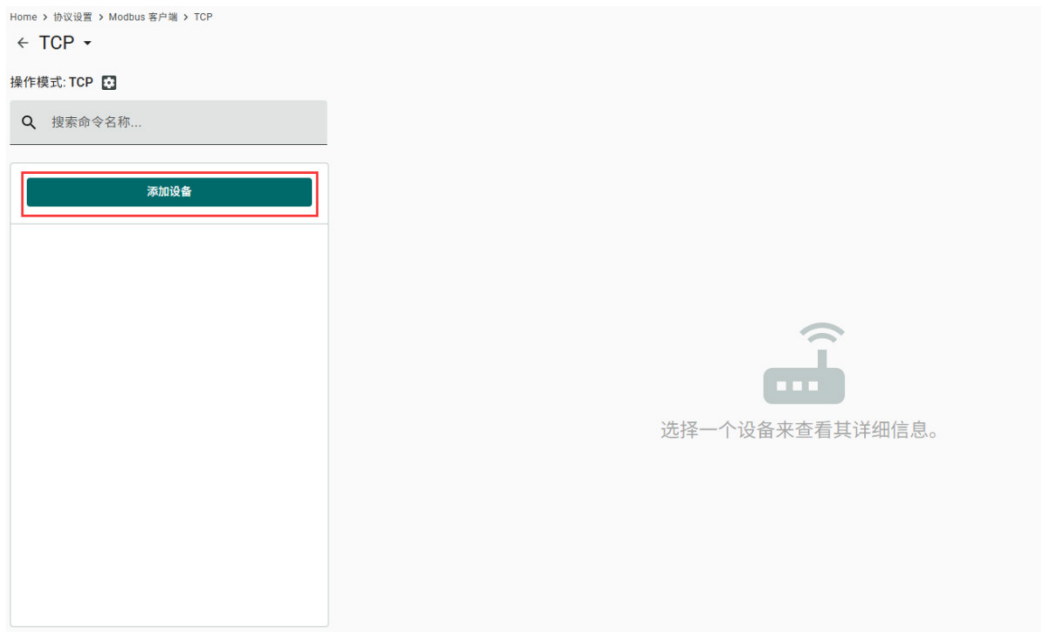
参数	值	说明
初始延迟（毫秒）	3 至 30,000 (默认值 = 0)	延迟启动后的第一个请求，以避免 Modbus 服务器启动缓慢出现异常。
最大重试次数	0 至 5 (默认值 = 3)	Modbus 命令超时时的重试次数。
响应超时（毫秒）	10 至 120,000 (默认值 = 1,000)	忽略请求之前等待 Modbus 服务器响应的的时间。

Modbus 设备设置

配置基本设置后，按照以下步骤添加和配置 **Modbus TCP device**（**Modbus TCP 设备**）。

第 1 步：添加设备

单击 **Add Device**（**添加设备**），然后按照安装向导进行操作。



Home > 协议设置 > Modbus 客户端 > TCP

← 创建新设备

1 基本设置

2 命令Optional

3 确认

☒ 启用此设备

设备名称
BMS_1

服务器 IP
192 . 168 . 4 . 100

服务器端口
502

服务器 ID
1

☐ 启用并发交易 ⓘ

取消 下一步 >

参数	值	说明
设备名称	字母数字、数字或特殊字符的组合 (~ . _)	Modbus 设备的名称。
服务器 IP	0.0.0.0 至 255.255.255.255	Modbus 设备的 IP 地址。
服务器端口	1 至 65,535 (默认值 = 502)	Modbus 通信的 TCP 端口。
服务器 ID	1 至 255	Modbus 设备的唯一 ID。
并发交易	启用、禁用 (默认=禁用)	启用：同时发送多个 Modbus 命令（减少延迟）。 禁用：按顺序发送命令。 注意：启用此选项之前，请确保您的 Modbus 设备支持并发交易。

第 2 步：配置命令

首次添加 Modbus 设备时：

1. 选择 **Manual（手动）** 模式。
2. 单击 **Add Command（添加命令）** 定义命令设置。

Home > 协议设置 > Modbus 客户端 > TCP

← 创建新设备

基本设置

2 命令Optional

3 确认

模式

☒ 手动 ☐ 导入配置

BMS_1

+ 添加命令

编号	命令名称	功能	地址、数量	触发	轮询间隔 (毫秒)	启用
----	------	----	-------	----	-----------	----

此设备中没有命令。单击 + 添加命令 在此设备中创建第一个命令。

每页数量 10 0 of 0 < >

Home > 协议设置 > Modbus 客户端 > TCP

← 创建新设备

基本设置

命令

Optional

确认

模式

☒ 手动
☐ 导入配置

+ 添加命令

BMS_1

编号	命令名称	功能	地址、数量	触发	轮询间隔 (毫秒)	启用
此设备中没有命令。单击 + 添加命令 在此设备中创建第一个命令。						

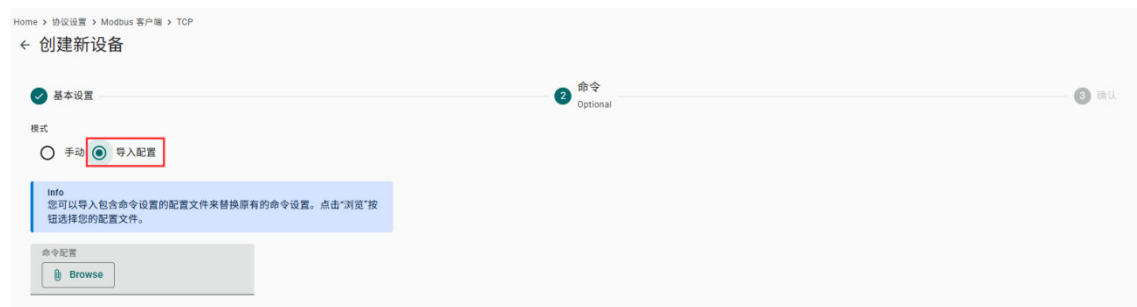
每页数量 10 0 of 0 |< < > >|

参数	值	说明
命令名称	字母数字、数字或特殊字符的组合 (~ ._)	命令的名称。
功能	01 - 读取线圈 02 - 读取离散输入 03 - 读取保持寄存器 04 - 读取输入寄存器 05 - 写入单个线圈 06 - 写入单个寄存器 15 - 写入多个线圈 16 - 写入多个寄存器 23 - 读取/写入多个寄存器 （默认值 = 03 - 读取保持寄存器）	定义如何从 Modbus 设备访问数据。
读取起始地址	0 至 65535 （默认值 = 0）	用于读取的第一个 Modbus 地址。
读取数量	读取线圈：1 至 2,000 读取离散输入：1 至 2,000 读取输入寄存器：1 至 125 读取保持寄存器：1 至 125 读取/写入多个寄存器：1 至 125 （默认值 = 10）	一个命令中要读取的线圈、输入或寄存器的数量。
写入起始地址	0 至 65,535 （默认值 = 0）	用于写入的第一个 Modbus 地址。
写入数量	写入多个线圈：1 至 1,968 写入多个寄存器：1 至 123 读取/写入多个寄存器：1 至 123 （默认值 = 1）	一个命令中要写入的线圈或寄存器的数量。
触发	循环，数据变化 （默认 = 循环）	循环：定期发送命令。 数据变化：仅当数据发生变化时才发送命令。
轮询间隔（毫秒）	100 至 86,400,000 （默认值 = 1,000）	循环命令的间隔。
字节序交换	大端字节序（AB CD > AB CD）	定义数据解释的字节顺序。

	大端字节交换 (AB CD > BA DC) 小端字节序 (AB CD > DC BA) 小端字节交换 (AB CD > CD AB) (默认 = 大端字节序)	
状态术语	暂停 继续 - 将数据清除为零 继续 - 设置为用户自定义值 (默认=暂停)	读取命令失败时的操作。
故障保护	暂停 继续 - 将数据清除为零 继续 - 设置为用户自定义值 (默认=暂停)	写入命令失败时的操作。
标签类型	原始、布尔值、int16、int32、int64、uint16、uint32、 uint64、浮点数、双精度、字符串 (默认 = 原始)	定义如何处理和存储命令数据。

导入配置

- 如果您有 Modbus 命令文件，请选择 **Import Configuration** (导入配置) 以加快设置速度。



第 3 步：确认并应用

- 检查已配置的设置。
- 单击 **Go to apply settings** (前往应用设置)。
- 单击 **Apply** (应用) 激活配置。

Home > 协议设置 > Modbus 客户端 > TCP

← 创建新设备

基本设置

命令Optional

3 确认

确认设备设置并点击完成以保存更改。在系统中创建设备后，您可以随时编辑设备设置。

设备名称BMS_1

服务器 ID1

服务器 IP192.168.4.100

服务器端口502

状态启用

命令数量0

命令配置

← 返回

取消完成

home > 协议设置 > Modbus 客户端 > TCP

← TCP

操作模式: TCP

搜索命令名称...

添加设备

BMS_1

启用

服务器 IP: 192.168.4.100

服务器端口: 502

服务器 ID: 1

BMS_1

+ 添加命令

导入

导出

编号	命令名称	功能	地址、数量	触发	轮询间隔 (毫秒)	启用	
>	1	voltage_1	3	读取 0、1	Cyclic	1000	启用

每页数量

10

1 - 1 of 1

<<<>>>

正在编辑 ...

前往应用设置

正在编辑...

前往应用设置

Home > 协议设置 > Modbus 客户端

Modbus 客户端

Modbus 客户端

管理

Modbus TCP

TCP

1 设备, 1 命令

Modbus RTU

COM1 (RTU)

未配置

COM2 (RTU)

未配置

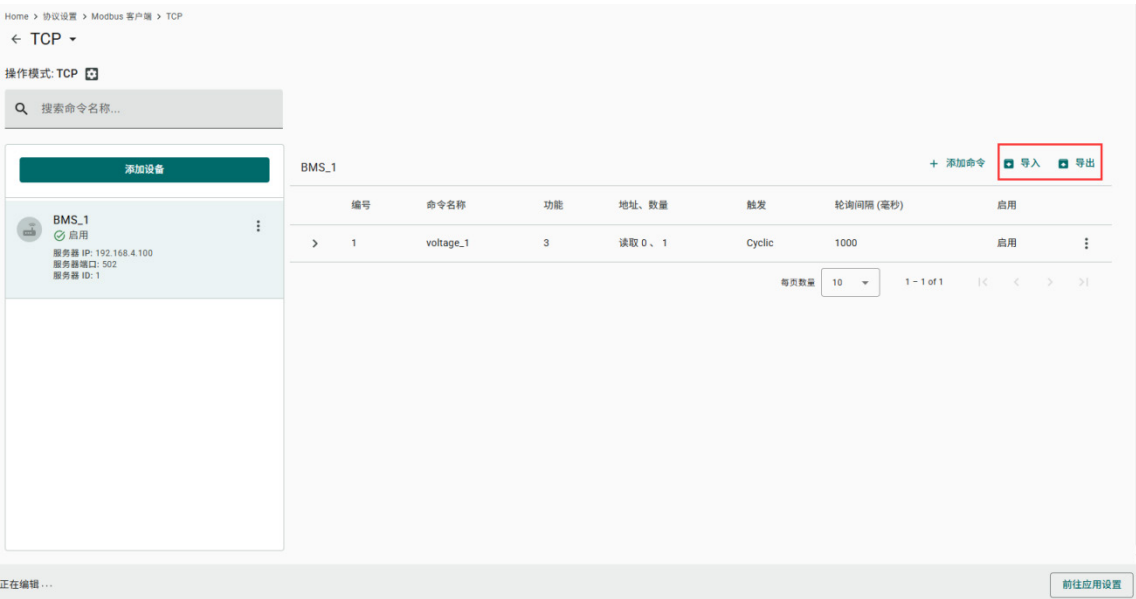
正在编辑...

丢弃应用

导出和导入以便轻松设置

该软件通过配置备份选项简化了安装和维护：

1. **Export**（导出）所有 Modbus 命令进行备份。
2. **Import**（导入）保存的配置（黄金样本）以减少设置时间。



Modbus RTU

本节将指导您在软件中配置 Modbus RTU 设置。该设置由两个主要部分组成：

1. 基本设置 - Modbus 通信的常规配置。
2. Modbus 设备设置 - 用于从 Modbus 设备检索数据的参数。

基本设置

与 Modbus 设备通讯前，请先配置 RTU 操作模式的基本设置。



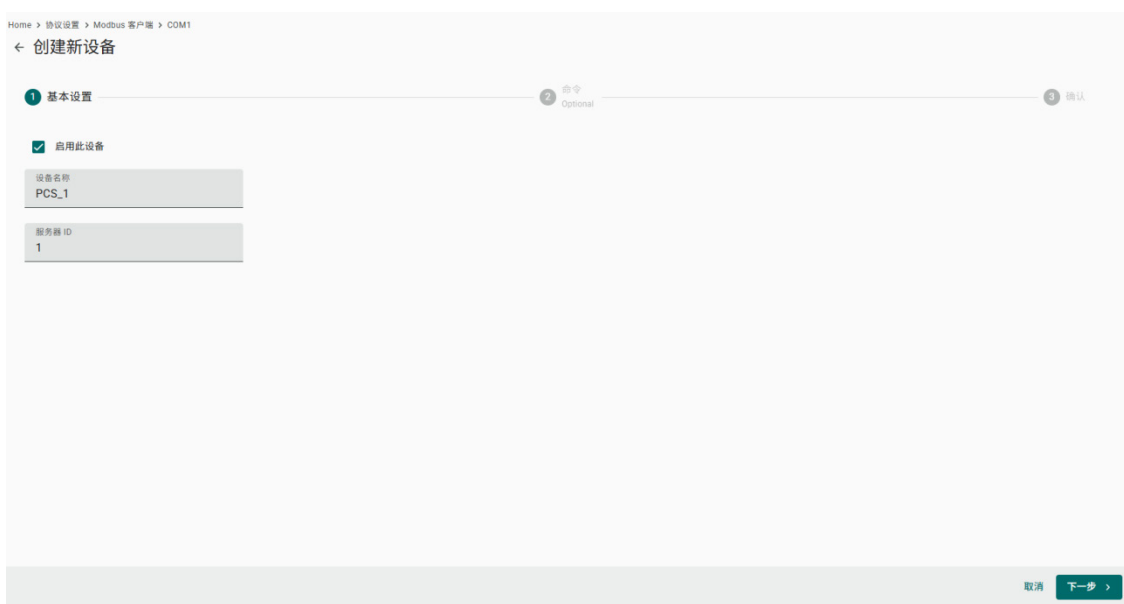
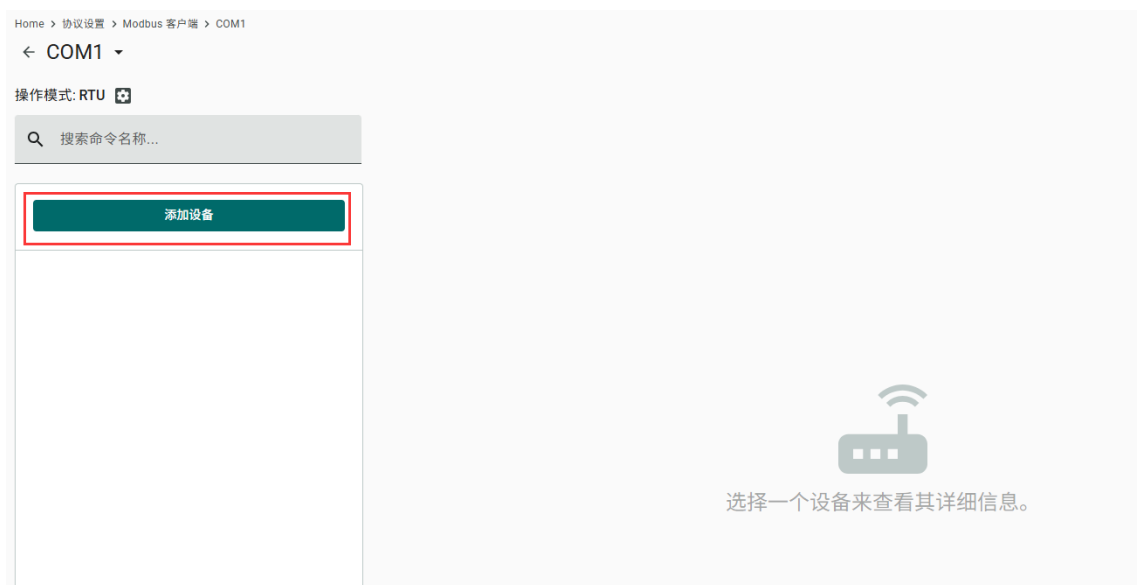
参数	值	说明
初始延迟（毫秒）	3 至 30,000 (默认值 = 0)	延迟启动后的第一个请求，以避免 Modbus 服务器启动缓慢出现异常。
最大重试次数	0 至 5 (默认值 = 3)	Modbus 命令超时时的重试次数。
响应超时（毫秒）	10 至 120,000 (默认值 = 1,000)	忽略请求之前等待 Modbus 服务器响应的的时间。
自动确定帧间延迟（ms）	启用、禁用：10 至 500 (默认=启用)	控制 Modbus 服务器响应和下一个请求之间的时间。 ● 启用：自动确定延迟。 ● 禁用：手动设置延迟时间。这确保了传统的 Modbus 服务器可以有效地处理数据包。
自动确定字符间超时（毫秒）	启用、禁用：10 至 500 (默认=启用)	定义 Modbus 响应中接收字符之间的超时间隔。 ● 启用：自动确定超时。 ● 禁用：手动设置超时以确保有效的数据接收。如果在设定的时间间隔内没有收到 RX 信号，则所有接收到的数据将被丢弃。

Modbus 设备设置

配置基本设置后，按照以下步骤添加和配置 **Modbus RTU device（Modbus RTU 设备）**。

第 1 步：添加设备

单击 **Add Device（添加设备）**，然后按照安装向导进行操作。



参数	值	说明
设备名称	字母数字、数字或特殊字符的组合 (~ . _)	Modbus 设备的名称。
服务器 ID	1 至 255	Modbus 设备的唯一 ID。

第 2 步：配置命令

首次添加 Modbus 设备时：

1. 选择 **Manual（手动）** 模式。
2. 单击 **Add Command（添加命令）** 定义命令设置。

Home > 协议设置 > Modbus 客户端 > COM1

← 创建新设备

基本设置

命令

Optional

确认

模式

☒ 手动
☐ 导入配置

+

 添加命令

PCS_1

编号	命令名称	功能	地址、数量	触发	轮询间隔 (毫秒)	应用
此设备中没有命令。单击 + 添加命令 在此设备中创建一个命令。						

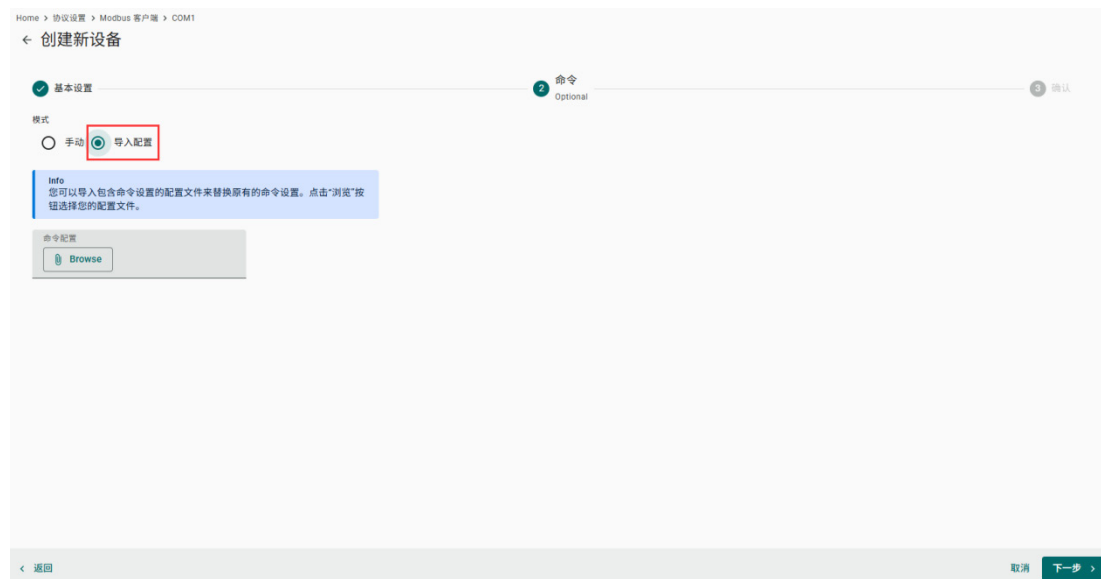
每页数量 10 0 of 0 << < > >>

参数	值	说明
命令名称	字母数字、数字或特殊字符的组合 (~ . _)	命令的名称。
功能	01 - 读取线圈 02 - 读取离散输入 03 - 读取保持寄存器 04 - 读取输入寄存器 05 - 写入单个线圈 06 - 写入单个寄存器 15 - 写入多个线圈 16 - 写入多个寄存器 23 - 读取/写入多个寄存器 (默认值 = 03 - 读取保持寄存器)	定义如何从 Modbus 设备访问数据。
读取起始地址	0 至 65535 (默认值 = 0)	用于读取的第一个 Modbus 地址。
读取数量	读取线圈: 1 至 2,000 读取离散输入: 1 至 2,000 读取输入寄存器: 1 至 125 读取保持寄存器: 1 至 125 读取/写入多个寄存器: 1 至 125 (默认值 = 10)	一个命令中要读取的线圈、输入或寄存器的数量。
写入起始地址	0 至 65,535 (默认值 = 0)	用于写入的第一个 Modbus 地址。
写入数量	写入多个线圈: 1 至 1,968 写入多个寄存器: 1 至 123 读取/写入多个寄存器: 1 至 123 (默认值 = 1)	一个命令中要写入的线圈或寄存器的数量。
触发	循环, 数据变化 (默认 = 循环)	循环: 定期发送命令。 数据变化: 仅当数据发生变化时才发送命令。
轮询间隔 (毫秒)	100 至 86,400,000 (默认值 = 1,000)	循环命令的间隔。
字节序交换	大端字节序 (AB CD > AB CD)	定义数据解释的字节顺序。

	大端字节交换 (AB CD > BA DC) 小端字节序 (AB CD > DC BA) 小端字节交换 (AB CD > CD AB) (默认 = 大端字节序)	
状态术语	暂停 继续 - 将数据清除为零 继续 - 设置为用户自定义值 (默认 = 暂停)	读取命令失败时的操作。
故障保护	暂停 继续 - 将数据清除为零 继续 - 设置为用户自定义值 (默认 = 暂停)	写入命令失败时的操作。
标签类型	原始、布尔值、int16、int32、int64、uint16、uint32、uint64、浮点数、双精度、字符串 (默认 = 原始)	定义如何处理和存储命令数据。

导入配置

- 如果您有 Modbus 命令文件，请选择 **Import Configuration (导入配置)** 以加快设置速度。



第 3 步：确认并应用

- 检查已配置的设置。
- 单击 **Go to apply settings (前往应用设置)**。
- 单击 **Apply (应用)** 激活配置。

Home > 协议设置 > Modbus 客户端 > COM1

← 创建新设备

基本设置

命令Optional

确认

确认设备设置并点击完成以保存更改。在系统中创建设备后，您可以随时编辑设备设置。

设备名称PCS_1

服务器 ID1

状态启用

命令数量0

返回

取消完成

Home > 协议设置 > Modbus 客户端 > COM1

← COM1

操作模式: RTU

搜索命令名称...

添加设备

PCS_1

启用

服务器 ID: 1

PCS_1

+ 添加命令

导入

导出

编号	命令名称	功能	地址、数量	触发	轮询间隔 (毫秒)	启用	
> 1	power_1	3	读取 0、10	Cyclic	1000	启用	⋮

每页数量101 - 1 of 1|<<>>|

正在编辑...

前往应用设置

Home > 协议设置 > Modbus 客户端

Modbus 客户端

Modbus 客户端管理

Modbus TCP

TCP1 设备, 1 命令

Modbus RTU

COM1 (RTU)1 设备, 1 命令

COM2 (RTU)未配置

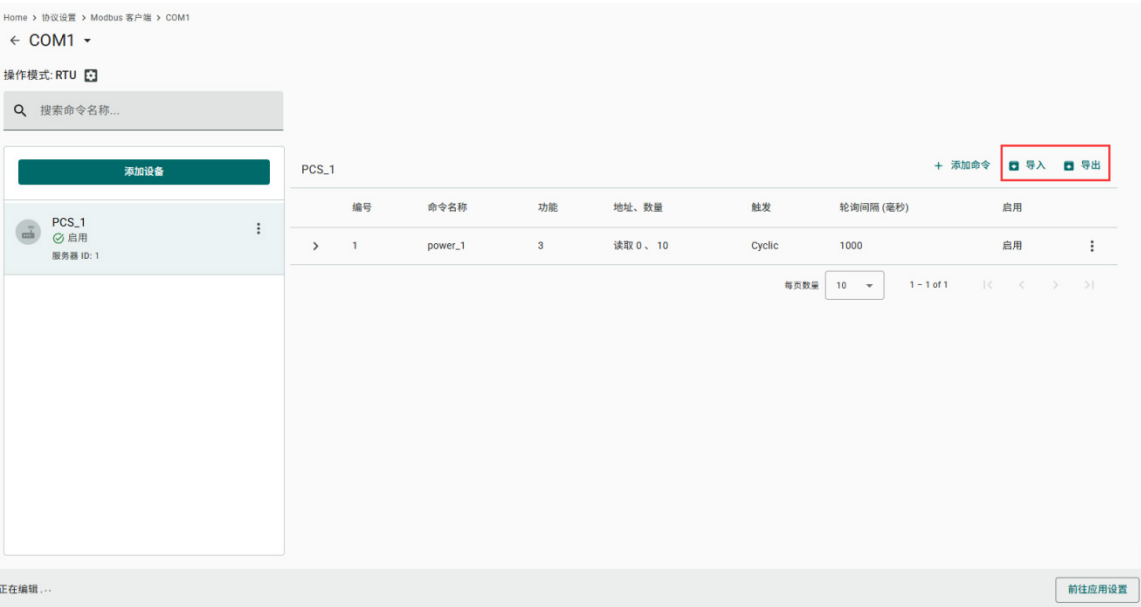
正在编辑...

丢弃应用

导出和导入以便轻松设置

该软件通过配置备份选项简化了安装和维护：

3. **Export**（导出）所有 Modbus 命令进行备份。
4. **Import**（导入）保存的配置（黄金样本）以减少设置时间。



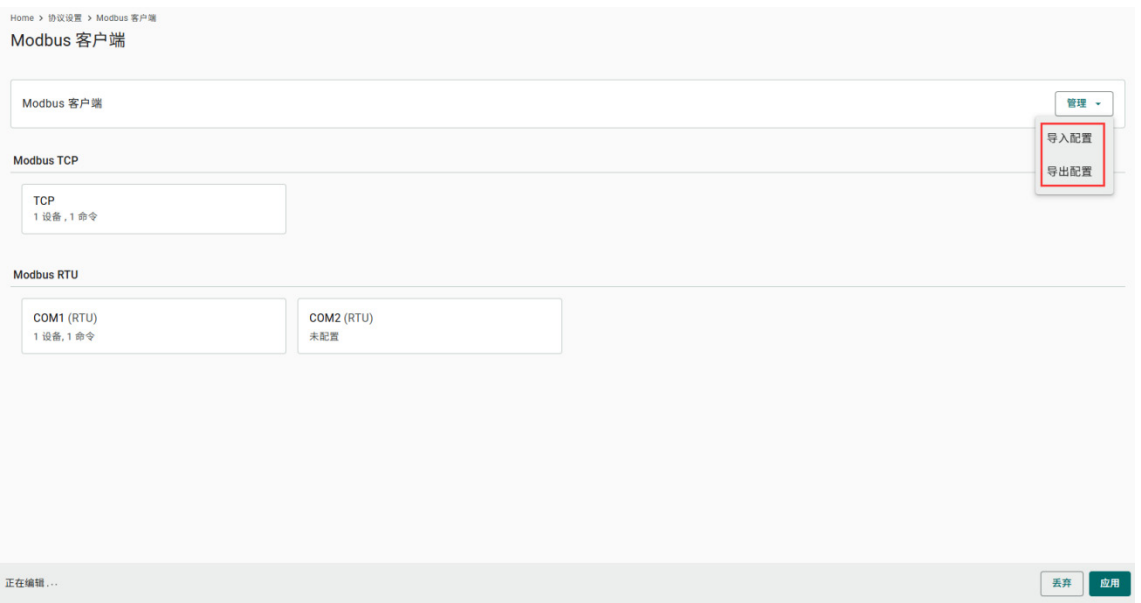
管理

该软件提供先进的管理功能以简化安装和维护。

导入/导出配置

您可以 **import**（导入）或 **export**（导出）CSV 格式的 Modbus 客户端设置。

- 可以使用 Excel 查看和编辑导出的文件。
- 导入配置文件允许您快速应用预配置的设置，从而减少设置时间。

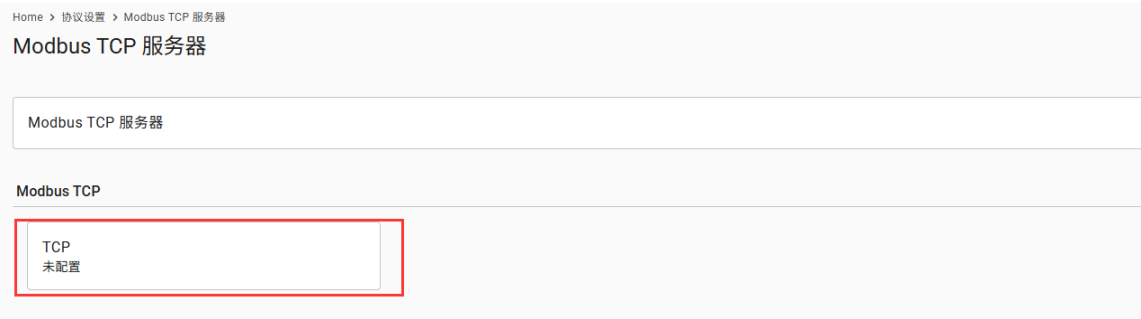


Modbus TCP 服务器

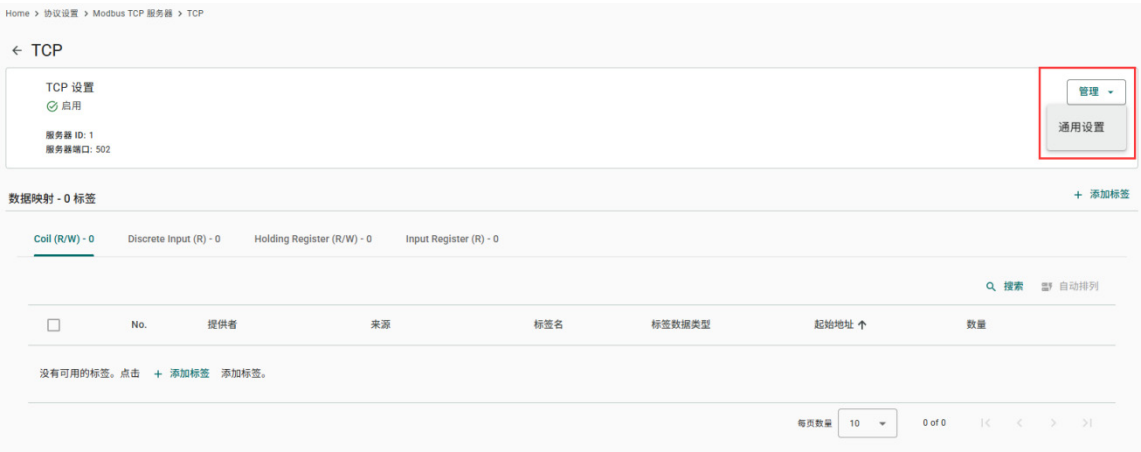
该软件提供了一个 **Modbus TCP server** (**Modbus TCP 服务器**) 允许与作为 **Modbus Clients** (**Modbus 客户端**) 的远程设备通信。按照以下步骤在软件中配置 **Modbus TCP server** (**Modbus TCP 服务器**)：

配置常规设置

1. 导航至 **Modbus TCP Server** (**Modbus TCP 服务器**) 页面并选择 **TCP**。



2. 单击 **Manage** (**管理**) > **General Settings** (**通用设置**) 并配置基本设置：

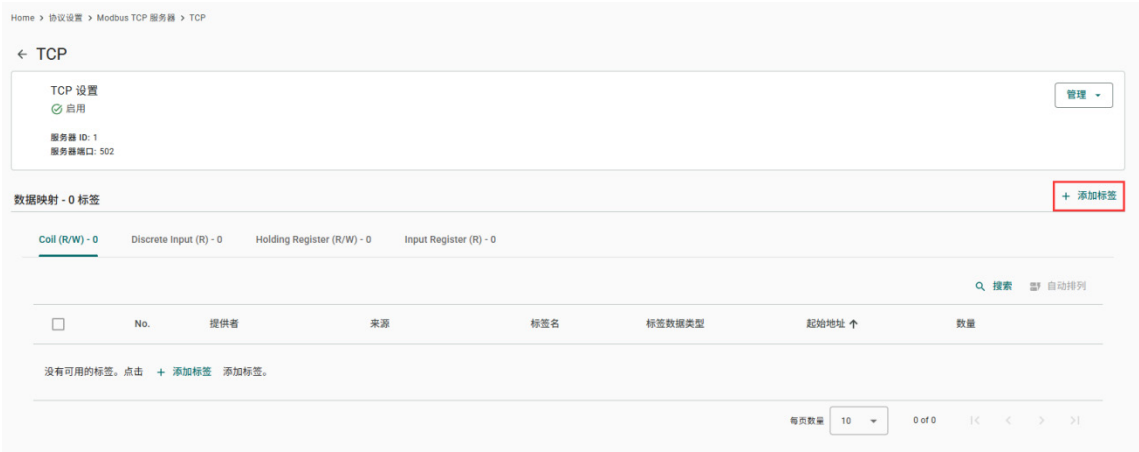


参数	值	说明
服务器 ID	1 至 255 (默认值 = 1)	此 Modbus 设备的唯一 ID。
服务器端口	1 至 65,535	Modbus 通信的 TCP 端口。

	(默认值 = 502)	
TCP活动检查时间 (分钟)	1 至 99 (默认值 = 1)	如果在此时间内未收到来自 Modbus 客户端的网络数据包，软件将断开连接。

添加数据映射标签

- 单击 **+Add Tags (+添加标签)** 映射 **tags (标签)** 和 **Modbus addresses (Modbus 地址)** 之间的数据。



- 配置以下参数：

添加标签

标签来源
参照标签

Info
选择要映射到 Modbus TCP 服务器的标签 (一次最多支持 512 个标签)。所选标签将根据标签类型和访问权限自动分类。有关详细信息，请参阅标签分类规则。

提供者
— 无 —

选定标签
— 无 —

0 标签

> 显示标签分类规则

取消 完成

添加标签

标签来源
自定义标签

自定义标签

Info
您可以进一步利用该标签进行计算。

子标签名称
tag

标签类型
raw

标签数量
1

Modbus 内存类型
保持寄存器 (读 / 写)

每个标签的数量
1

第一个标签起始地址
0

每个标签的字节序交换
大端 (AB CD → AB CD)

取消 完成

参数	值	说明
标签来源	参照标签、自定义标签 (默认 = 参照标签)	参照标签: 链接到其他协议的标签 (例如, Modbus TCP/RTU 客户端)。 自定义标签: 专为该协议创建的标签。

提供者	mx_io、modbus_tcp_client、 modbus_serial_client、iec104_server、 mqtt_client	选择提供标签的 protocol （协议）或 component （组件）。可以选择多个提供者。
选定标签	（基于提供者）	选择一个或多个要映射到该协议的标签。
子标签名称	字母数字、数字或特殊字符的组合 (~ . _)	为此协议创建的 custom （自定义）标签的名称。
标签类型	原始、布尔值、int16、int32、int64、uint16、 uint32、uint64、浮点数、双精度、字符串 （默认 = 原始）	定义软件如何处理和存储数据。
标签数量	1 至 500 （默认值 = 1）	要创建的 custom （自定义）标签的数量。
Modbus 内存类型	线圈（读/写）， 离散输入（只读）， 保持寄存器（读/写）， 输入寄存器（只读）	定义已创建标签的 Modbus memory mapping （Modbus 内存映射）。
第一个标签起始地址	0 至 65,535 （默认值 = 0）	Modbus 内存映射的起始地址。
每个标签的字节序交换	大端字节序（AB CD > AB CD）， 大端字节交换（AB CD > BA DC）， 小端字节序（AB CD > DC BA）， 小端字节交换（AB CD > CD AB） （默认 = 大端字节序）	定义数据解释的字节顺序。

3. 单击 **Done**（完成）以完成。

查看数据映射

- 在 **Data Mapping**（数据映射）下面，您可以查看全部 **selected tags**（选定标签），分为：
 - 线圈
 - 离散输入
 - 保持寄存器
 - 输入寄存器

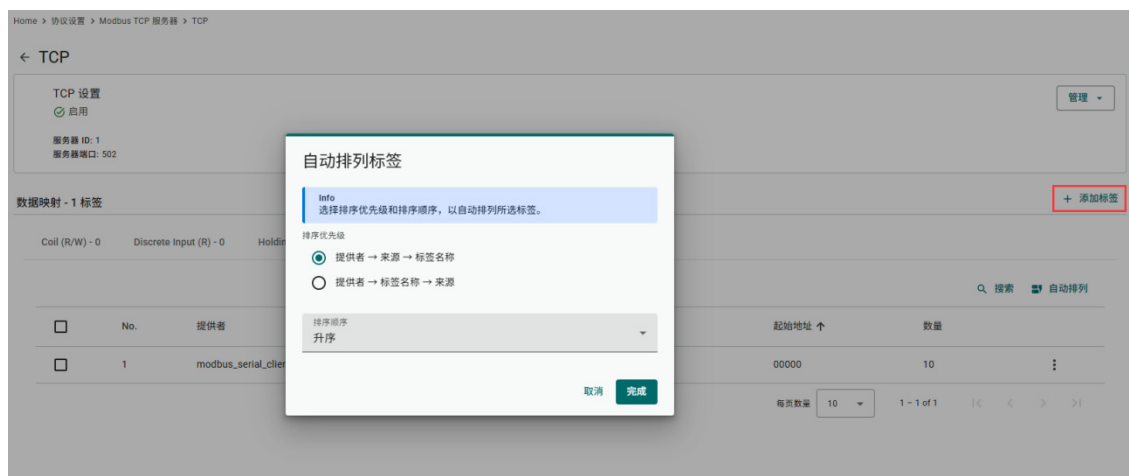


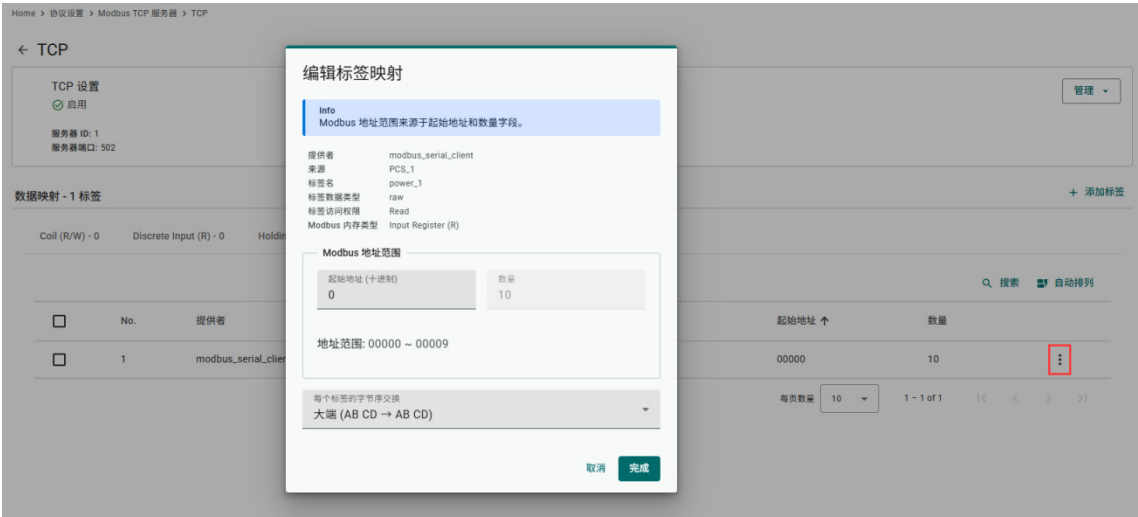
- 映射遵循 **Tag Type**（标签类型）和 **Access Permission**（访问权限）：

标签类型	标签访问权限	映射到 Modbus 内存
布尔值	读/写	线圈
布尔值	读取	离散输入
非布尔值	读/写	保持寄存器
非布尔值	读取	输入寄存器

分配 Modbus 地址

- 该软件基于 **Sorting Priorities**（排序优先级）和 **Sort Order**（排序顺序）将选定标签映射到 **Modbus addresses**（Modbus 地址）。
- 单击 **Auto Arrange**（自动排列）应用自动排序或手动 **编辑起始地址** 在映射表中。





IEC 60870-5-104 服务器

要创建 IEC 60870-5-104 服务器，请按照以下步骤操作：

1. 单击 **Server Settings**（服务器设置）下面的 **IEC 60870-5-104**。
2. 单击 **Edit > Edit Basic Settings**（编辑 > 编辑基本设置）修改下面的配置。（可选）

编辑基本设置

服务器端口

2404

ASDU 地址

3

链路地址 (COT) 长度

2

取消

保存

参数	值	说明
服务器端口	1,024 至 60,000 (默认值 = 2,404)	IEC 60870-5-104 服务器 TCP 端口。
ASDU 地址	1 至 65,534 (默认值 = 3)	ASDU 地址字段定义为站地址。 一条线路上所有站的 ASDU 地址必须不同。
COT 长度	1, 2 (默认值 = 2)	COT 字段用于控制通信网络上和站内的消息路由，由 ASDU 引导至正确的程序或任务进行处理。 客户端和服务器之间的大小必须一致。

3. 单击 **Edit > Edit Advanced Settings**（编辑 > 编辑高级设置）修改以下配置。（可选）
4. 单击 **+ Add Tags**（+ 添加标签），通过 **Referral Tags**（参照标签）选择标签或通过 **Custom Tags**（自定义标签）创建标签。

参数	值	说明
标签源	参照标签、自定义标签	参照标签：该标签由另一个模块定义并在本模块中引用。主要用例是直接 from 源读取数据或直接写入源而无需进行二次修改。 自定义标签：该标签由当前模块定义。主要用途是针对其他标签进行二次计算，并将计算结果写入本标签，或者使用多个该类型的标签进行决策，并将结果写入其他标签进行控制。

5. 选择 **Referral Tags（参照标签）**，以选择由另一个模块定义的标签，例如 Modbus TCP 客户端

The screenshot shows the 'Add Tag' dialog box. At the top, '标签来源' (Tag Source) is set to '参照标签' (Referral Tag). Below this, an 'Info' box states: '选择一个或多个标签提供者来获取其标签，并选择标签来映射数据。' (Select one or more tag providers to get their tags, and select tags to map data). Under '显示标签於' (Show tags at), three options are checked: '读取' (Read), '操作' (Operation), and '读取 / 操作' (Read / Operation). The '提供者' (Provider) dropdown is set to '无' (None). Below it, '已选的标签' (Selected tags) is also set to '无' (None). At the bottom right, there are '取消' (Cancel) and '完成' (Finish) buttons.

6. 选择 **Custom Tags（自定义标签）**，按当前模块创建标签。（可选）

The screenshot shows the 'Add Tag' dialog box with '自定义标签' (Custom Tag) selected under '标签来源' (Tag Source). An 'Info' box states: '您可以进一步利用该标签进行计算。' (You can further utilize this tag for calculation). Under '自定义标签设置' (Custom Tag Settings), the '子标签名称' (Sub-tag name) is 'single_point'. Below this, a note says: '默认标签名称将结合对象类型和 IOA。当标签数量大于 1 时，标签名称将为：single_point1, single_point2, single_point3, ...' (Default tag names will be combined with object type and IOA. When the number of tags is greater than 1, the tag names will be: single_point1, single_point2, single_point3, ...). The '标签类型' (Tag type) dropdown is set to 'boolean', and the '标签数量' (Tag count) is set to '1'. Under '点位设置' (Point Settings), the '信息对象数量' (Information object count) is set to '1'. At the bottom right, there are '取消' (Cancel) and '完成' (Finish) buttons.

7. 单击 **Done（完成）** 以完成设置。
8. 在 **Data Mapping（数据映射）** 下面，可查看之前添加的所有标签。

Home > 协议设置 > IEC 60870-5-104 服务器 > 服务器设置

← 服务器设置

IEC 60870-5-104 服务器

编辑

基本设置

ASDU 地址 3
链路地址 (COT) 长度 2
服务器端口 2404

高级设置

Info

没有数据点被设置自发响应

数据映射 - 1 个标签

搜索 刷新 + 添加标签

☐	编号	标签名	标签类型	信息对象类型	地址 (IOA)	自发的	方向
☐	1	iec104_server/local_device/single_point1	boolean	单点信息	1	☐	读取

每页数量 10 1 - 1 of 1 |< < > >|

编辑...

丢弃 应用

参数	值	说明
信息对象类型	- 单点 - 双点 - 步阶位置 32 位的位串 - 测量值（缩放） - 测量值（标准化） - 测量值（浮动） - 集成总量 （Object Type（对象类型）选项和默认值将根据 Tag Type（标签类型）确定。）	IEC 60870-5-104 服务器 ASDU 类型。
IOA	1 至 16,777,215 （默认：根据现有的 IOA 依次递增。）	IOA 用于构建信息对象地址，以定义特定系统内的明确地址。 对于以下 Object Types（对象类型），如果两个标签有相同的 Object Type（对象类型） 且其 Direction（方向） 分别设置为 Read（读取） 和 Operator（操作员），则可以被分配相同的 IOA。 - 单点 - 双点 - 步阶位置 32 位的位串 - 测量值（缩放） - 测量值（标准化） - 测量值（浮动）

自发	启用、禁用 (默认=禁用)	当标签值发生变化时，服务器会主动向客户端发送自发响应。
组	常规, Group1, ..., Group16 (默认=常规)	组用于区分客户端的询问。当设置为 Group1~Group16 时，表示该点仅在接收到特定组询问时才会发送响应。

9. 单击 **Apply** (应用) 应用配置

MQTT 客户端

该软件提供 MQTT 客户端功能，允许您：

- **Establish connections** (建立连接) 至远程 MQTT 服务器 (代理)
- **Publish tag data** (发布标签数据) 到服务器
- **Subscribe to topics** (订阅主题) 接收更新标签数据的消息

连接

本节将介绍如何建立新的 MQTT 连接。

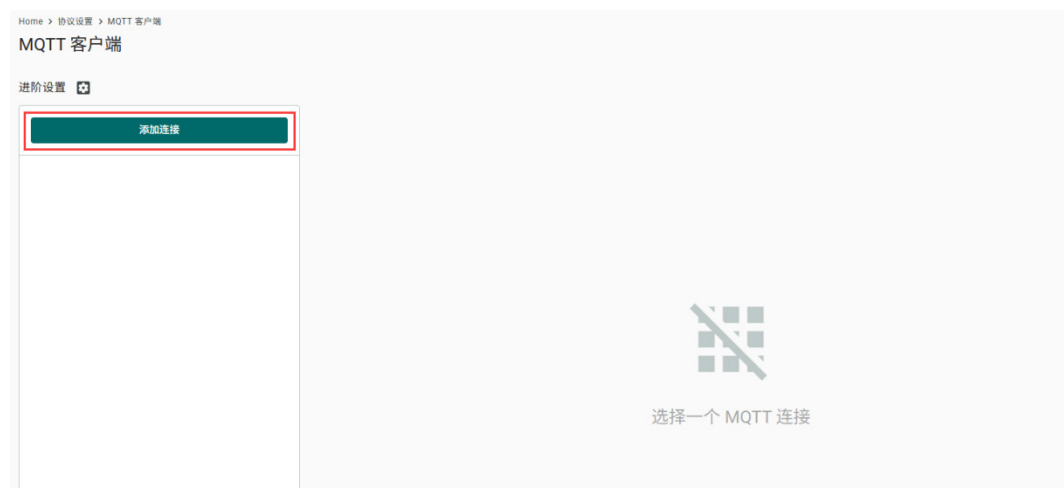
创建连接的步骤

1. 访问 MQTT 客户端页面

转到 Web 控制台中的 MQTT 客户端页面。

2. 添加新连接

单击 **Add Connection** (添加连接) 来建立新的连接。最多可以创建 5 个连接。



3. 配置常规设置

连接到新的 MQTT 服务器

通用

SSL/TLS

遗嘱

服务器名称

Server_1

服务器 IP/主机名

端口号

MQTT 版本

☒ 3.1.1

☐ 3.1

客户端 ID

0 / 65535

用户名

密码

保持连接计时器 (秒)

60

清除会话

☒ 断开连接后不要在服务器上保留消息。

取消

保存

参数	值	说明
服务器名称	字母数字、数字或特殊字符 (_ -) 的组合 (默认 = Server_1)	服务器的唯一名称。
服务器 IP/主机名	有效的 IPv4 地址或域名	MQTT 服务器的 IP 地址或域名。
服务器端口	1 至 65,535	用于 MQTT 通信的 TCP 端口。
MQTT 版本	3.1.1、3.1 (默认值 = 3.1.1)	要使用的 MQTT 协议版本。
客户端 ID	字符串 (最多 65,535 个字符)	客户端连接的标识符。
用户名	字符串 (最多 65,535 个字符)	用于连接认证的用户名。
密码	字符串 (最多 65,535 个字符)	连接认证的密码。
连接计时器 (秒)	10 至 65,536 (默认值 = 60)	发送 MQTT 数据包的间隔, 以避免连接超时。
清除会话	启用、禁用 (默认=启用)	确定连接时是否清除以前的会话设置。

4. 配置 SSL/TLS (可选)

为了保护您的连接, 请启用 SSL/TLS 并上传所需的文件。

连接到新的 MQTT 服务器

通用

SSL/TLS

遗嘱

SSL/TLS

☒ 启用 SSL/TLS

支持的最低 TLS 版本

☒ 1.2 ☐ 1.3

客户端证书 - 可选

 Browse

客户端密钥 - 可选

 Browse

受信任的根 CA - 可选

 Browse

☒ 忽略服务器证书

取消

保存

参数	值	说明
TLS 版本	1.2、1.1、1.0 (默认值 = 1.2)	支持的最低 TLS 版本；如果服务器使用较低版本，握手将停止。
客户端证书 - 可选	有效的 .pem 或 .cert 文件	用于客户端身份验证的证书。
客户端密钥 - 可选	有效的 .key 文件	与客户端证书配对的密钥文件。
受信任的根 CA - 可选	有效的 .pem 或 .cert 文件	用于服务器验证的根 CA 证书。
忽略服务器证书	启用、禁用 (默认：禁用)	选择是否在 TLS 握手期间跳过服务器证书验证。

5. 配置“遗嘱”（可选）

配置当客户端意外断开，由服务器发布该遗嘱消息。

连接到新的 MQTT 服务器

通用

SSL/TLS

遗嘱

遗嘱 ①

启用遗嘱标志

遗嘱主题

遗嘱信息

遗嘱 QoS 策略

至少一次 (1)

遗嘱保留策略

开关

取消

保存

参数	值	说明
遗嘱主题	字符串（最多 65,535 个字符）	遗嘱信息的主题。
遗嘱信息	字符串（最多 65,535 个字符）	断开连接时发布的消息。
QoS 策略	0、1、2 (默认： 1)	遗嘱消息的 QoS 级别。
遗嘱保留政策	启用、禁用 (默认：启用)	遗嘱信息是否应该保留在服务器上。

6. 保存并应用

单击 **Save**（保存）保存配置，然后单击 **Apply**（应用）发起连接。

7. 监控连接状态

Home > 协议设置 > MQTT 客户端

MQTT 客户端

进阶设置

添加连接

Server_1

10.0.20.107

正在连接

主题列表

服务器名称

Server_1

服务器 IP

10.0.20.107

主题数量

0

上次更新

2025/08/05 15:52:50

刷新

发布主题

订阅主题

编号	主题类型	主题名称	上次活动时间	上次活动状态	启用 / 禁用
没有可显示的数据。单击 + 发布主题 或 + 订阅主题 按钮创建一个条目。					

每页数量

10

0 of 0

<

>

连接状态	说明
连接中	客户端正在与服务器建立连接。

BESS 软件用户手册

51

已连接	客户端已成功连接到服务器。
断开	连接已断开。验证服务器状态。
连接失败	连接失败。检查您的设置是否正确。

发布主题

一旦建立连接，您就可以配置发布标签数据的主题。

创建发布主题的步骤

1. 选择连接

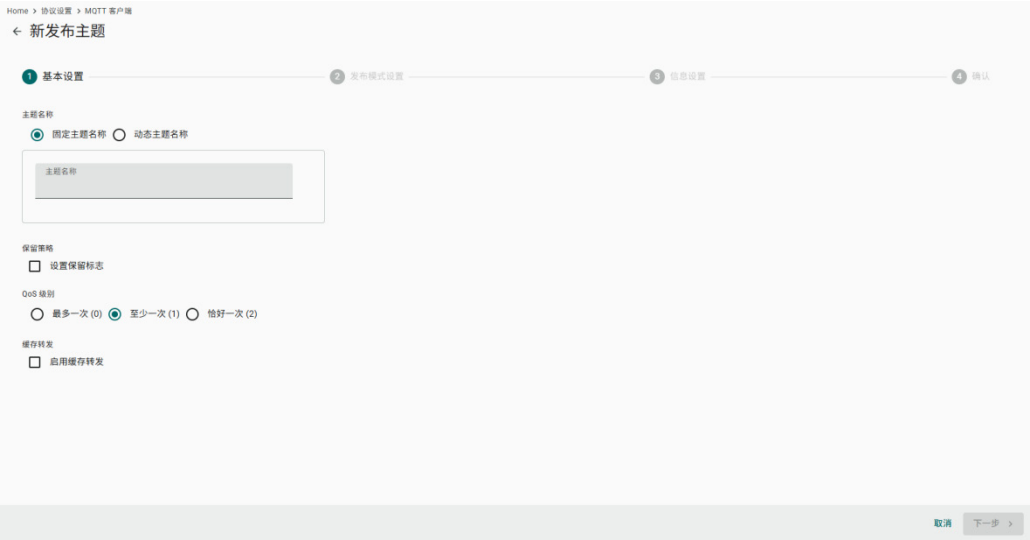
在 MQTT 客户端页面，单击已配置的连接。

2. 添加发布主题

单击 **+ Publish Topic (+ 发布主题)** 按钮。每个连接最多可创建 125 个主题。



3. 配置基本主题设置



参数	值	说明
主题名称	字符串（1 至 65,535 个字符）	发布消息的 MQTT 主题。

保留政策	启用、禁用 (默认: 禁用)	是否在服务器上保留该消息。
QoS 级别	最多一次 (0)、至少一次 (1)、恰好一次 (2) (默认: 至少一次 (1))	已发布消息的服务质量级别。

4. 设置发布模式

以下参数决定标签数据如何打包到 MQTT 消息中并发布到 MQTT 服务器。

参数	值	说明
发布模式	循环, 数据变化 (默认: 循环)	循环: 定期发布消息。 数据变化: 仅当标签数据发生变化时才发布消息。
发布间隔 (秒)	1 至 86,400	循环模式下发布消息的间隔。
采样模式	所有值、最新值、所有更改的值、最新更改的值 (默认: 所有值)	确定每条已发布消息中包含哪些标签数据: - 所有值: 包括自上次发布以来记录的每个标签值, 即使标签更新多次。 - 最新值: 仅包含每个标签的最新值。 - 所有更改的值: 包括自上次发布以来更新的每个标签的每个更改。 - 最新更改的值: 仅包含自上次发布以来更改的每个标签的最新更新。
根据采集的数据自定义采样率	启用、禁用 (默认: 禁用)	通过设置自定义采样率来跳过冗余标签值以减少消息大小的选项。
采样率 (秒)	0 至 86,400	获取消息打包时标签值的采样率。
仅发布更改的值	启用、禁用 (默认: 禁用)	如果启用, 则仅包含自上次发布以来发生变化的标签值。
启用最小发布间隔	启用、禁用	设置数据更改模式下发布消息之间的最小间隔, 以

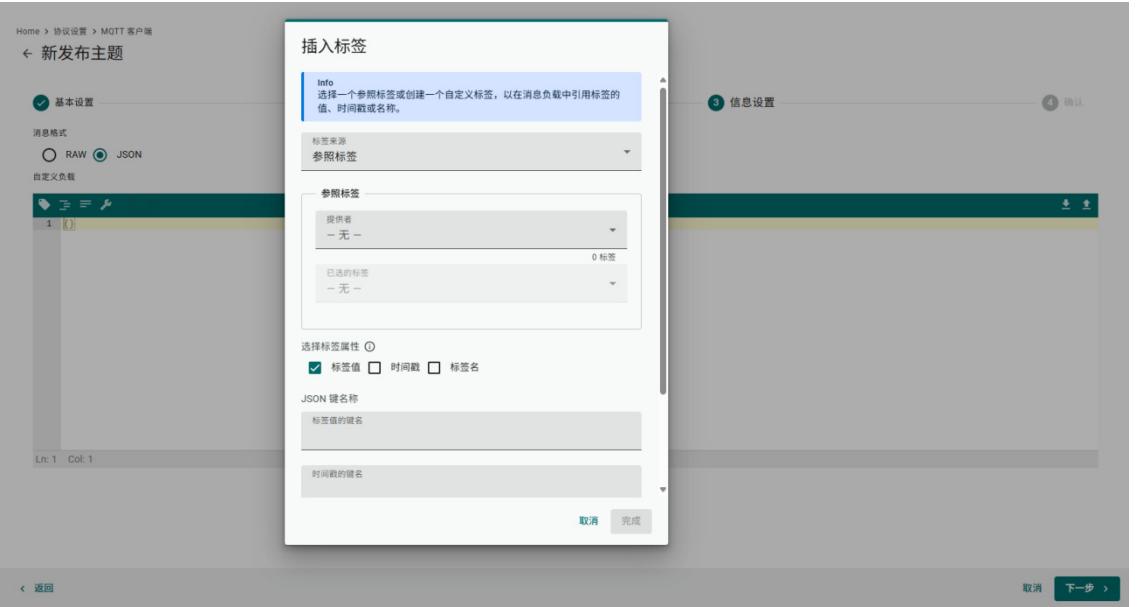
	(默认：禁用)	避免网络拥塞。
间隔（秒）	1 至 60	数据更改模式处于活动状态时发布消息之间的最小间隔。

5. 构建 JSON 格式的消息负载

MQTT 客户端支持带有标签引用的 JSON 格式的消息。您可以使用 UI 功能或手动编辑 JSON 将标签数据添加到有效负载。

使用 UI：

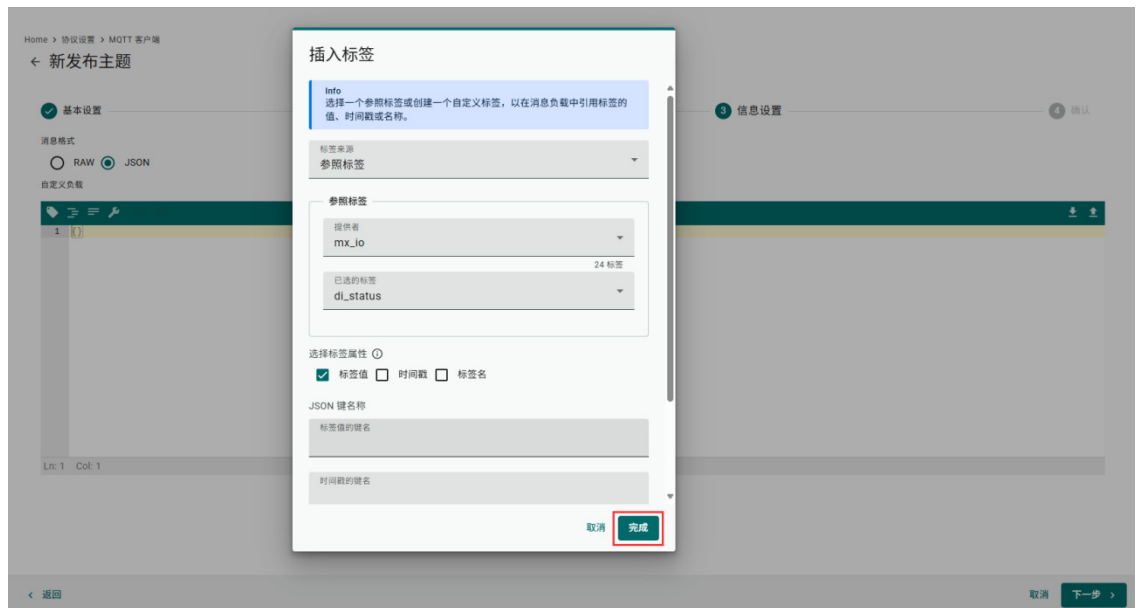
- 单击 **Insert Tag（插入标签）** 图标并填写设置：



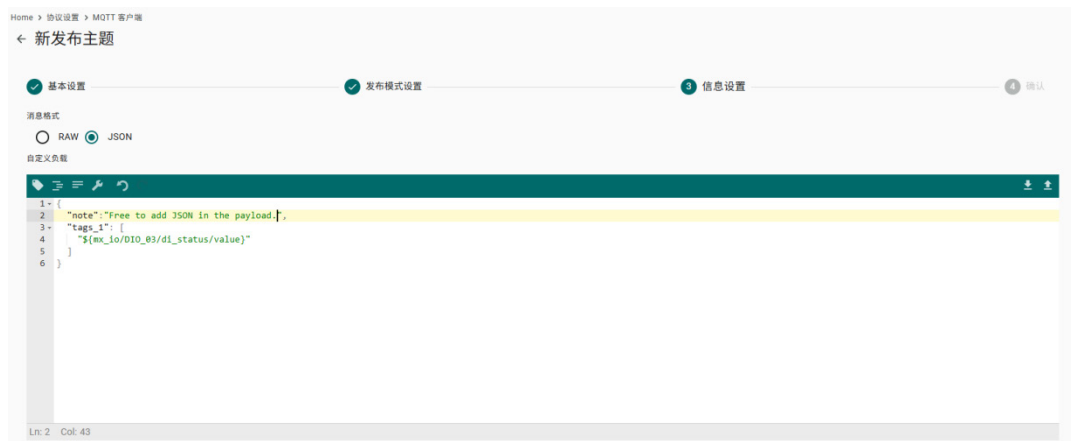
参数	值	说明
标签来源	参照标签、自定义标签 (默认 = 参照标签)	参照标签： 链接到其他协议的标签（例如，Modbus TCP/RTU 客户端）。 自定义标签： 专为 MQTT 创建的标签。
提供者	mx_io、modbus_tcp_client、 modbus_serial_client、iec104_server、 mqtt_client	为标签数据选择一个或多个提供者。
选定标签	(基于提供者)	选择一个或多个要引用的标签。
子标签名称	字母数字、数字或特殊字符的组合 (~ . _)	为 MQTT 创建的自定义标签的名称。
标签类型	原始、布尔值、int16、int32、int64、uint16、 uint32、uint64、浮点数、双精度、字符串 (默认 = 原始)	定义如何处理和存储标签数据。
标签数量	1 至 500 (默认值 = 1)	有效负载中包含的自定义标签的数量。
选择标签属性	标签值、时间戳、标签名称	指定要包含的标签属性（值、时间戳或完整标签名称）。

JSON 键名称	字符串（0 至 100 个字符）	插入的标签数据的 JSON 键。如果省略，标签引用将作为 JSON 数组添加。
标签插入位置	前置，后置 (默认：前置)	确定标签引用插入有效负载的哪个位置。

- 单击 **Done（完成）** 自动插入标签引用。



- 您可以根据需要拖放或编辑 JSON。

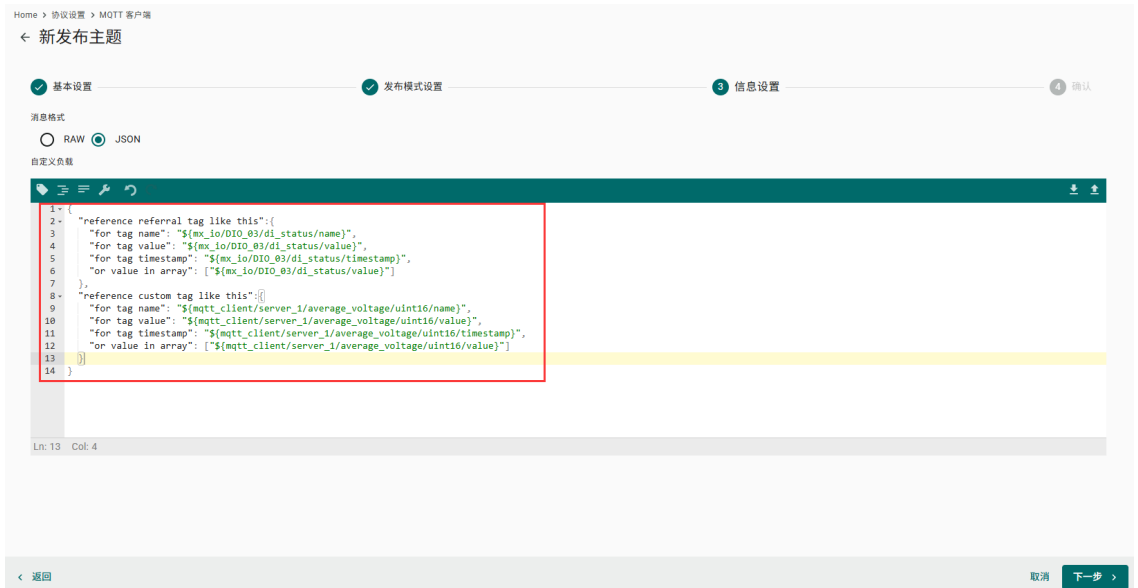


手动编辑 JSON 有效负载：

使用预定义格式直接编辑 JSON 有效负载：

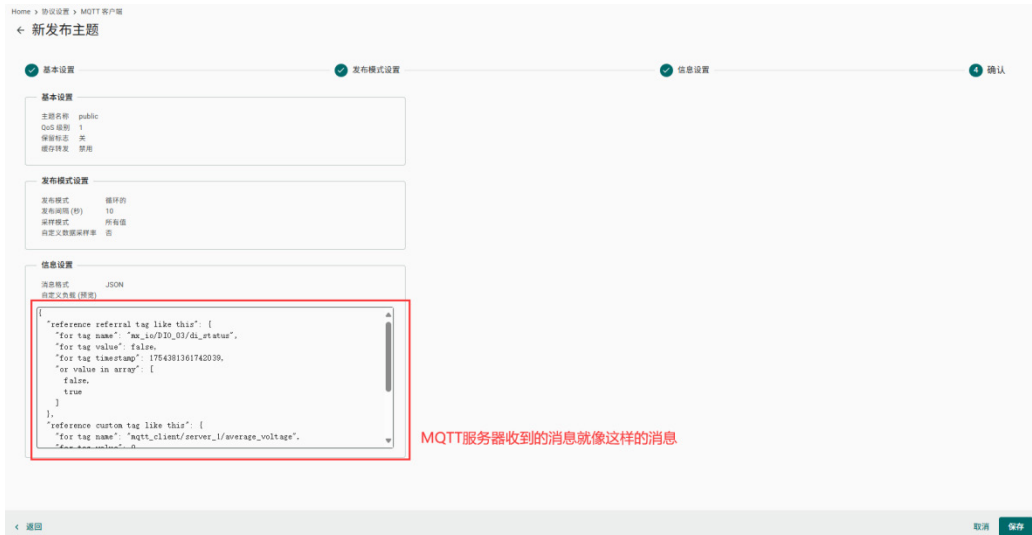
- 对于参照标签：
`"${provider_name/source_name/sub_tag_name/tag_property}"`
- 对于自定义标签：
`"${provider_name/source_name/sub_tag_name/tag_type/tag_property}"`
- 参数：

- 提供者名称：mx_io、modbus_tcp_client、modbus_serial_client、iec104_server、mqtt_client 之一（对于自定义标签，使用 mqtt_client）。
- 源名称：创建标签的设备/连接的名称。对于自定义标签，请在此连接中使用 MQTT 服务器名称。
- 子标签名称：标签的名称。
- 标签类型：数据类型（仅自定义标签需要）。支持原始、布尔、int16、int32、int64、uint16、uint32、uint64、float、double 和字符串类型。
- 标签属性：指定要引用的属性（值、时间戳或名称）。



6. 确认并保存

- 查看主题设置、发布模式和 JSON 有效负载预览。



- 单击 **Save（保存）** 保存配置，然后单击 **Apply（应用）** 发起连接和话题。
- 在 MQTT 客户端页面监控主题状态。



注意

1. JSON 结构和标签数据：

- 当标签被引用到 **JSON Array (JSON 数组)** 时，该软件会将该标签的所有数据（如果多次更新）附加到消息中的同一个数组中。
- 当标签被引用到 **JSON Object (JSON 对象)** 时，仅包含该标签的最新数据。
- 您可以在 **Confirm (确认)** 配置步骤中预览最终发布的消息。

2. 性能注意事项：

- 大量的发布主题和复杂的设置会给 MQTT 客户端带来沉重的负担。为了获得最佳性能，请参阅“**Advanced MQTT Publish Topic Configuration (高级 MQTT 发布主题配置)**”部分以获取更多建议

订阅主题

订阅主题允许 MQTT 客户端从 MQTT 服务器接收消息并相应地更新标签数据。

创建订阅主题的步骤

1. 选择连接

在 MQTT 客户端页面，单击已配置的连接。

2. 添加订阅主题

单击 **+ Subscribe Topic (+ 订阅主题)** 按钮。每个连接最多可以创建 125 个主题。



3. 配置基本主题设置

Home > 协议设置 > MQTT 客户端

← 新订阅主题

1 基本设置

2 信息设置

3 确认

主题名称

☒ 固定主题名称 ☐ 动态主题名称

主题名称

price

QoS 级别

☐ 最多一次 (0) ☒ 至少一次 (1) ☐ 恰好一次 (2)

取消 下一步 >

参数	值	说明
主题名称	字符串（1 至 65,535 个字符）	将从中接收消息的主题。
QoS 级别	最多一次 (0)、至少一次 (1)、恰好一次 (2) (默认: 至少一次 (1))	传入消息的服务质量级别。

4. 设置消息过滤

MQTT 客户端可以根据收到的消息更新标签值。客户端从纯文本消息中过滤数据并使用它来更新选定标签。配置以下内容:

Home > 协议设置 > MQTT 客户端

← 新订阅主题

1 基本设置

2 信息设置

3 确认

消息格式

☒ RAW ☐ JSON

数据过滤器

Info

选择参照标签或创建自定义标签。来存储从收到的消息中过滤的数据。确保负载类型与标签类型匹配, 以便进行正确的过滤。

标签来源

自定义标签

子标签名称

price

标签类型

float

返回 取消 下一步 >

参数	值	说明
标签来源	参照标签、自定义标签 (默认 = 参照标签)	参照标签: 链接到其他协议的标签 (例如, Modbus TCP/RTU 客户端)。 自定义标签: 专为 MQTT 创建的标签。
提供者	mx_io、modbus_tcp_client、 modbus_serial_client、iec104_server、 mqtt_client	选择提供标签的 protocol/component (协议/组件)。

选定 标签	(基于提供者)	选择一个标签，通过从收到的消息中提取的数据进行更新。
子标 签名 称	字母数字、数字或特殊字符的组合 (~ ._)	为 MQTT 创建的自定义标签的名称。
标签 类型	原始、布尔值、int16、int32、int64、uint16、uint32、uint64、浮点数、双精度、字符串 (默认 = 字符串)	定义如何处理标签数据。对于字符串/原始类型，数据大小不应超过 1,024 字节。



注意

- 标签数据与订阅消息的关系：
当在订阅主题上收到消息时，MQTT 客户端使用配置的数据过滤器从消息中提取纯文本信息。然后将该信息映射到选定标签，并在软件中更新其值。**确保收到的消息的格式与预期的数据格式相匹配，以便更新正确的标签值。**

5. 确认并保存

- 检查订阅主题设置和传入消息的预期格式。

- 单击 **Save (保存)** 保存配置，然后单击 **Apply (应用)** 激活订阅。
- 在 MQTT 客户端页面监控主题状态。



账户管理

出于安全考虑，不同的用户在一台设备上需要不同的账户和权限。该软件支持帐户管理，管理员可以添加/删除/更改用户帐户名，按不同组授予指定功能类别的 Web 控制台访问权限，并管理密码和登录策略，以确保控制台由预期用户使用。

账户

使用 Web 控制台时，用户可以访问的类别与管理员定义的用户组高度相关（有关组的管理，请参阅下一章节 **Groups（组）**）。管理员可在 **Accounts（账户）** 页面单击 **Create（创建）** 按钮来添加用户账户。



Create New Account（创建新帐户） 窗口将会弹出，供您输入帐户信息并为用户分配密码。此外，管理员必须为用户分配适当的组以限制他们使用 Web 控制台的权限。要添加、删除或编辑组，请前往菜单中的 **Groups（群组）** 部分。密码规则可以在 **Password Policy（密码策略）** 部分设置。

建立新帐户

帐户名称

群组

Administrator

密码

- 至少包含 8 个字符

确认密码

取消

保存

您也可以单击“:”图标来编辑现有用户上面提到的帐户设置。

Home > 帐户管理 > 帐户

帐户

创建

帐户名称	群组	状态	创建日期	
admin (您)	Administrator	启用	2025-07-29	:
postman	Administrator	启用	2025-08-04	:

每页数量 25 1 - 2 of 2

更改密码

更改群组

停用

删除

变更密码

作为管理员，您可以更改每个用户的密码。**Change Password（更改密码）**窗口将会弹出，您可以在其中输入两次新密码，然后 **SAVE（保存）** 新密码。密码将被更改。

作为一般用户，您只能更改自己的密码。单击“:”图标，然后选择 **Change password（更改密码）** 打开 “Change Password（更改密码）”窗口。然后输入两次新密码，**SAVE（保存）** 新密码。密码将被更改。

更改密码

帐户名称: admin
最后更新日期: 2025-07-29

密码

新密码

- 至少包含 8 个字符

确认新密码

取消 保存

更改群组

只有管理员用户可以更改用户帐户的组。单击“⋮”图标，然后选择 **Change group (更改群组)** 打开“Change Group (更改群组)”窗口。从下拉菜单中选择要移动到的组，然后单击 **SAVE (保存)** 按钮。用户帐户将被移动到新组。

变更群组

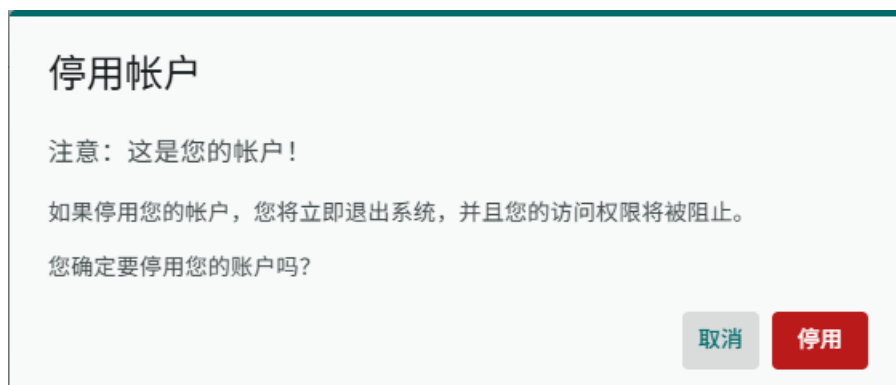
帐户名称: admin
创建日期: 2025-07-29

群组
Operator

取消 保存

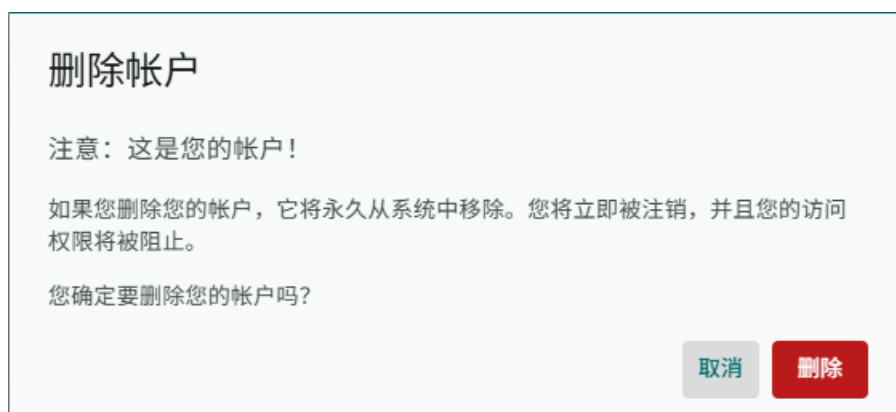
停用

只有管理员用户可以停用用户帐户。停用帐户时，该帐户仍然存在，但无法登录设备，直到管理员重新激活它。单击“⋮”图标，然后选择 **Deactivate (停用)** 打开“Deactivate Account (停用帐户)”窗口。单击 **DEACTIVATE (停用)** 按钮，用户帐户将被停用。



删除

只有管理员可以删除用户帐户。删除帐户时，该帐户将从设备配置中删除。在目标帐户名称上单击“:”图标，选择 **Delete**（删除）打开“Delete Account（删除帐户）”窗口。单击 **DELETE**（删除）按钮，用户帐户将被删除。



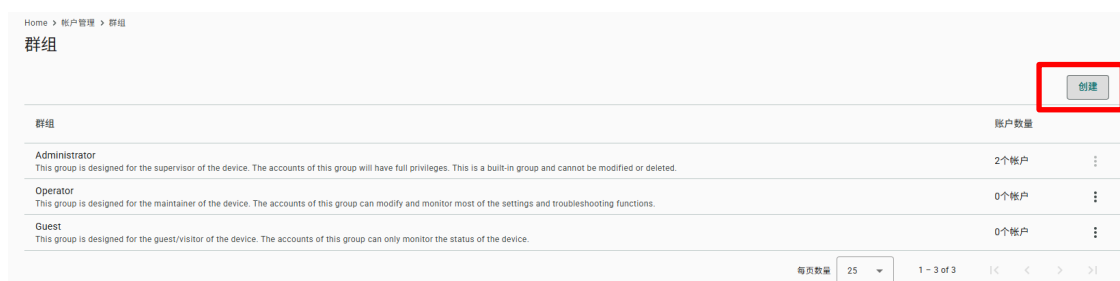
群组

该软件将根据用户帐户所属的组授予用户访问不同功能类别的权限。只有组管理员（默认情况下，或在帐户管理类别中授予读/写权限的任何组）才可以自定义不同组的访问权限。

最多可创建 8 个用户组，每个组最多可分配 16 个用户帐户。默认情况下，该软件有三个内置用户组：管理员、操作员和访客。

- 无法删除管理员组，也无法更改其名称。
- 可以删除操作员组，并可以更改其名称。
- 可以删除访客组，并可以更改其名称。

单击 Groups（群组）页面上的 **Create**（创建）按钮开始创建新组。



组名：用户将要创建的组的名称。组名是必填项。

组描述：用户可以为群组提供描述，以使其目的更容易理解。例如，如果用户创建一个名为“操作员”的组，其描述为“此组专为设备维护人员设计。该组中的帐户可以修改和监控大多数设置和故障排除功能。”此字段是可选的。

Web 控制台权限：请使用下拉菜单为每个类别分配权限。权限包括三种类型：

- **无显示：**该组中的用户在访问 Web 控制台时将看不到此功能类别。

- **只读：**该组内的用户只能查看此类别下的功能/设置，但不能进行任何修改。
- **读/写：**该组中的用户可以查看和修改此类别中的功能/设置。

功能分类如下：

- **系统设置：**包括设备时间、外设接口参数等设置。
- **网络设置：**包括与以太网 IP 地址、蜂窝连接等相关的设置。
- **协议设置：**包括北向、南向通信协议组合的选择及其参数配置。
- **账户管理：**包括与帐户和组相关的所有设置，例如创建/修改/删除帐户或组。
- **安全：**包括与网络安全相关的所有设置，如允许列表和登录设置。
- **维护：**包括与日常维护工作相关的所有设置，如软件升级和配置导入/导出。
- **诊断：**包括所有可以帮助用户排除故障的功能，如协议状态和网络流量监控。

创建新群组

基本信息

名称

描述 - 可选

Web控制台权限

标签仪表板

-- 选择一个 --

网络设置

-- 选择一个 --

系统设置

-- 选择一个 --

协议设置

-- 选择一个 --

安全

-- 选择一个 --

取消

保存

您可以在现有组 上单击 “:” 图标编辑其访问权限或删除该组。

Home > 帐户管理 > 群组

群组

创建

群组	帐户数量	
Administrator This group is designed for the supervisor of the device. The accounts of this group will have full privileges. This is a built-in group and cannot be modified or deleted.	2个帐户	⋮
Operator This group is designed for the maintainer of the device. The accounts of this group can modify and monitor most of the settings and troubleshooting functions.	0个帐户	⋮
Guest This group is designed for the guest/visitor of the device. The accounts of this group can only monitor the status of the device.	0个帐户	⋮

每页数量

25

1 - 3 of 3

<

>

>>

密码策略

针对日益强大的 PC 平台，用户担心密码可能遭到暴力攻击。为了降低网络安全风险，管理员可以通过启用密码策略功能来增强密码的复杂性。

Home > 帐户管理 > 密码政策

密码策略

为了增强您密码的安全级别，您可以选择设置最短密码长度和密码强度策略。

最短密码长度

8

密码强度策略

☐ 至少一位数字 (0-9)

☐ 混合大小写字母 (A-Z、a-z)

☐ 至少一个特殊字符 (~! @\$%^&* _+=`|\'(){}[];:'"<>,./?)

您可以通过设置密码有效期来增强帐户安全性。当帐户达到有效期阈值且用户登录时，系统将强制更改密码。

☒ 启用密码有效期

密码有效期 (天)

90

保存

参数	选项	说明
最小密码长度	8 至 256 个字符 (默认值 = 8)	定义登录密码的最小长度。
至少一个数字 (0-9)	启用、禁用 (默认=禁用)	启用此参数时，密码必须至少包含一个数字 (0-9)。
混合大小写字母 (A~Z、a~z)	启用、禁用 (默认=禁用)	启用此参数时，密码必须同时包含大写和小写字母。
至少一个特殊字符 (~! @\$%^&* _+=` \'(){}[];:'"<>,./?)	启用、禁用 (默认=禁用)	启用此参数时，密码必须至少包含一个特殊字符。
启用密码有效期	启用、禁用 (默认=启用)	通过设置密码有效期来增强帐户安全性。
密码有效期 (天)	1 至 180 天 (默认值 = 90)	可以指定密码有效期，如果启用该选项，将出现系统通知消息提醒用户更改密码。

完成设置后，请单击 **SAVE（保存）** 按钮保存更改并应用设置。

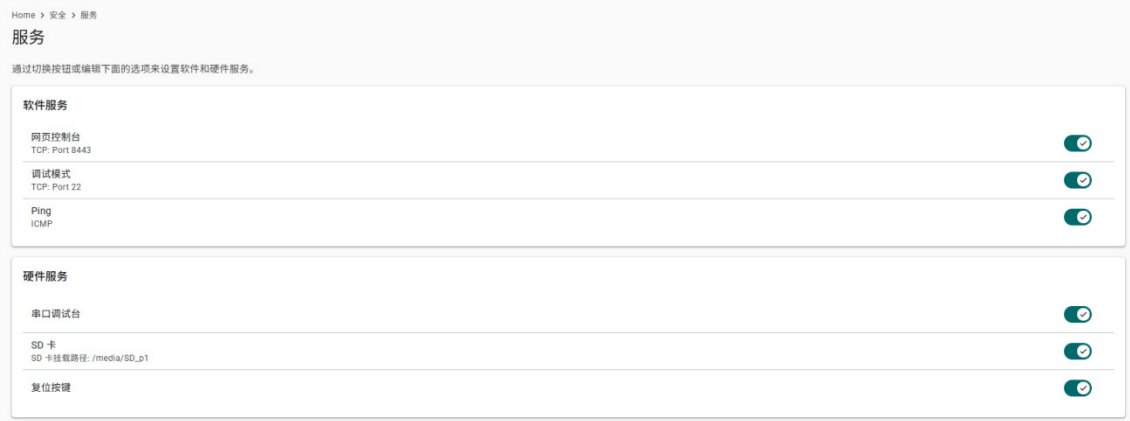
对于与登录失败相关的设置，例如在 5 次密码尝试失败后锁定 IP 地址，请前往 **Security > Login Settings > Login Lockout（安全 > 登录设置 > 登录锁定）** 部分。

安全

随着网络攻击的数量和复杂程度不断增长，设备供应商正在增加旨在保护敏感商业和个人信息的功能。所有相关功能均列于 **Security（安全）** 类别下。

服务

根据不同的使用场景，用户可能需要不同的服务来满足自己的需求。用户可以单击 **Security > Services（安全 > 服务）** 启用或禁用这些服务。



软件服务	值	说明
Web Console	启用、禁用 （默认=启用）	此设置用于启用或禁用 Web 控制台。出于安全原因，该软件仅支持使用 TLS v1.2 或更高版本进行网络通信的 HTTPS 控制台。Web 控制台提供对该软件支持的所有设置的访问，不建议禁用。
调试控制台 （SSH 连接）	启用、禁用 （默认=启用）	SSH 是一种加密的网络传输协议，用于管理和操作您的远程 Linux 系统设备。如果您的所有配置都可以通过该软件提供的 HTTPS 控制台进行处理，您可以考虑禁用此服务以进一步增强设备的安全性。
Ping	启用、禁用 （默认=启用）	禁用 Ping 服务可以减少设备信息在网络上的暴露，降低某些攻击的风险。然而，在实施该措施之前，必须权衡其对诊断和管理的影响，并将其纳入整体安全策略。

硬件服务	值	说明
本地控制台 （串口 console）	启用、禁用 （默认=启用）	Local Console（本地控制台）是一个强大的工具，可以协助完成各种任务，从系统开发和调试到运营管理。但是启用该接口可能会带来潜在的安全风险，因此根据您的具体需求评估是否启用或禁用该服务非常重要。
SD 卡	启用、禁用 （默认=启用）	该设置用于启用或禁用 SD 卡服务。如果您的设备安装了 SD 卡，启用该服务会自动将 SD 卡挂载到指定的系统路径下进行文件读写操作。当服务被禁用时，SD 卡将从系统中卸载。如果在卸载过程中正在读取或写入 SD 卡，则卸载将失败。请稍后重试。
复位按钮	启用、禁用 （默认=启用）	该设置用于启用或禁用重置按钮服务。重置按钮将执行当前系统设置的默认行为，但可以根据用户的需求进行配置。用户可以参考 MIL 3 用户手册 了解更多配置细节。

白名单

白名单是被授予特权访问权限的 IP 地址列表。启用该功能可以限制可以访问设备的 IP 地址数量，从而防止来自不受信任网络的未经授权的访问。



在启用白名单之前，您需要向列表中添加至少一条规则。另外，请确保主机的 IP 地址在列表中，否则您可能无法再次访问该设备。

添加 IPv4 规则

IPv4 地址

.

.

.

子网掩码

.

.

.

☒ 启用此规则

取消

保存

请单击 **ADD RULE（添加规则）** 按钮添加新规则。您可以在 IP 地址栏中输入 IP 地址，然后输入子网掩码来分配一个 IP 地址范围。我们建议启用此功能，以便在添加新规则时激活新规则。如果您不想启用此功能，请记住取消选中 **Enable this rule（启用此规则）** 复选框。

您可以通过使用 IP 地址和子网掩码的组合来添加特定地址或地址范围：

- **允许访问特定 IP 地址：**在相应的字段中输入 IP 地址；输入 255.255.255.255 作为网络掩码。
- **允许访问特定子网上的主机：**对于 IP 地址和网络掩码，最后一位数字均使用 0（例如，“192.168.1.0”和“255.255.255.0”）。
- **允许访问所有 IP 地址：**确保 **Allowlist（白名单）** 切换按钮已关闭。

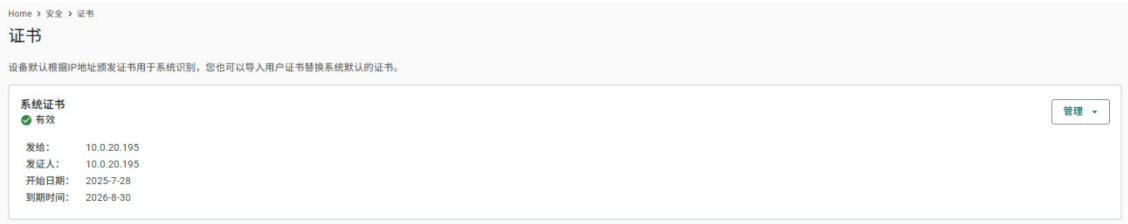
下表显示了其他配置示例：

所需 IP 范围	IP 地址	网络掩码
任何主机	禁用	启用
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 至 192.168.1.254	192.168.1.0	255.255.255.0

192.168.1.1 至 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 至 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 至 192.168.1.254	192.168.1.128	255.255.255.128

证书

该软件将自动为所有 TLS 会话生成自签名证书，包括 Web 控制台等服务。如果用户拥有公司生成或第三方验证的证书，请单击 **MANAGE**（管理）按钮导入证书，以降低网络安全风险。



当您单击 **MANAGE**（管理）按钮时,会出现四个选项：

- **下载系统证书**：PC 上的浏览器或软件可能会在建立安全连接之前要求目标设备提供有效的证书。此时用户需要从设备下载系统证书，然后上传到浏览器或软件中，即可建立安全连接。
- **重新生成系统证书**：如果系统证书已过期或不再安全，用户可以重新生成系统证书以建立新的安全连接。
- **导入用户证书**：如果用户拥有公司生成或第三方验证的证书，可以将该证书导入设备以建立新的安全连接。请单击 **Browse**（浏览）按钮找到 PC 上的证书，然后单击 **Import & Restart**（导入和重启）按钮以确保设备重新启动并使用导入的证书。
- **删除用户证书**：如果需要替换已导入的证书，您可以使用 **Import User Certificate**（导入用户证书）选项或 **delete**（删除）现有证书，提示系统重新生成新的系统证书。





注意

- 某些浏览器可能会将活动连接期间的证书更新解释为异常行为，这可能会导致 Web 控制台出现登录问题。如果您在更新证书（无论是导入新的用户证书还是删除现有证书）后遇到此类问题，请清除浏览器的缓存和 cookie，然后重新启动浏览器，再重新连接到 Web 控制台。

登录设置

当用户成功登录设备时，将显示 **Login Message（登录消息）** 栏。管理员可以输入最多 256 个字符的消息与用户进行沟通。

如果管理员想要向无法登录设备的用户发送消息，可以选择 **Customized Message（自定义消息）** 模式，然后在 **Message Text（消息内容）** 栏输入消息。当模式设置为 **Default Message（默认消息）** 时，设备将提供推荐消息供管理员参考。

Home > 安全 > 登录设置

登录设置

登录信息 登录锁定 会话控制

系统的登录页面上将显示以下文字说明。

登录信息

消息内容 - 可选

0 / 256

登录验证失败消息

模式
默认消息

消息内容
您输入的账号或密码不正确。(如果尝试次数过多, 您的账号将被暂时锁定)

34 / 256

保存

为了防止黑客反复尝试登录和破解密码，我们建议用户启用 **Login Lockout（登录锁定）** 功能。该功能默认启用。

Home > 安全 > 登录设置

登录设置

登录信息

登录锁定

会话控制

为了避免黑客反复登录该账号破解密码，您可以选择启用登录失败锁定功能并配置相关设置。

☒ 启用登录失败锁定

最大失败重试次数 (次)

5

☐ 定时清除登录失败计数

每达到倒数清除时间，登入失败次数将重新计数

锁定时间 (分钟)

5

保存

参数	值	说明
启用登录失败锁定	启用、禁用 (默认=启用)	勾选后，登录锁定功能将被启用。
最大失败重试次数 (次)	1 至 10 (默认值 = 5)	您可以指定重试失败的最大次数。如果重试次数超过此限制，则软件将锁定该帐户，使其无法登录
启用重置登录失败计数器	启用、禁用 (默认=禁用)	选中后，登录失败计数器将在您设置的重置期限后重新计算。
重置周期 (分钟)	1 至 1440 (默认值 = 10)	
锁定时间 (分钟)	1 至 60 (默认值 = 5)	当用户登录失败次数超过阈值时，无论后续输入的密码是否正确，软件将会锁定帐户一段时间，以防止用户不断尝试登录。

软件提供账号登录的会话控制，防止 Web 控制台被过多用户同时访问，导致硬件资源消耗过度，造成设备故障。还可以防止用户长时间占用 Web 控制台，确保其他用户可以登录并执行操作。

参数	值	说明
最大登录用户数	1 至 10 (默认值 = 5)	可同时登录 Web 控制台的帐户数量。一旦达到最大在线用户数，其他用户将无法登录。
会话超时 (分钟)	1 至 1440 (默认值 = 60)	登录 Web 控制台后每个帐户的连接时长。如果连续登录时间超过限制且没有任何活动，则软件将自动注销该帐户。

维护

配置导入/导出

使用导入和导出功能主要有三个原因：

- 将相同的软件配置应用于多个设备。导入/导出配置功能是将相同设置应用到设备的便捷方法。您可以将配置导出为文件，然后将配置文件导入到其他设备。
- 备份软件配置以供系统恢复。导出功能允许您导出配置文件，这些文件可以导入到其他设备以在几分钟内恢复故障系统。
- 故障排除。导出的软件配置文件可帮助管理员识别系统问题，并在请求维护访问时向 Moxa 技术服务团队提供有用的信息。

Home > 维护 > 配置导入/导出

配置导入/导出

配置文件在导出和导入时都会通过默认密码进行加密和验证，默认密码可以修改为自定义密码，以增强安全性。

文件认证

默认密码

管理

导入

导出

Browse

未选择文件

导入



注意

配置文件只能导入到同型号的 Moxa 工业计算机中。

文件验证

出于网络安全原因，您可以使用身份验证密钥导出配置文件，密钥长度为 8 至 16 个字符。如果导入的配置文件的密钥与导出的文件的密钥不同，则导入过程将失败。

单击 **Set custom password**（设置自定义密码），用户将为导出的配置文件分配自定义密码。此外，软件将使用此密码来解码导入的配置文件。

单击 **Reset to default password**（重置为默认密码），软件将使用默认密码对配置文件进行编码或解码。

管理

设置自定义密码

重置为默认密码

导入/导出配置文件

在 **Import**（导入）选项卡上，单击 **Browse**（浏览）按钮选择要导入的配置文件。



在 **Export (导出)** 选项卡上，单击 **Export (导出)** 按钮选择要保存配置文件的位置。



软件升级

Moxa 致力于**长期支持**，不断发布软件更新以增强**可靠性**和**安全性**。该软件提供 Web 控制台进行软件升级，具有两种升级方式：

- 仅升级 **BESS 软件**
- 升级 **OS 和 BESS 软件**

每种方法适用于不同的软件版本。在继续之前，**提供以下信息**给 **Moxa 技术支持**团队以收取相应的升级建议和文件：

- **当前镜像版本**
- **当前 BESS 软件版本**

Home > 维护 > 软件升级

软件升级

当前镜像版本: 1.0.0 Build 25020607

当前 BESS 软件版本: 1.1.1

选择升级类型，上传升级文件到设备。若需要获取升级文件，请联系 [Moxa 技术支持团队](#)。

✓ 仅限 BESS 软件

OS和BESS软件

升级文件 (.deb)

📎 Browse

保存

升级程序

仅升级 BESS 软件

1. 准备 .deb 升级文件。
2. 选择 **BESS Software Only** (仅限 BESS 软件)。
3. 单击 **Browse** (浏览) 上传文件并开始升级。

Home > 维护 > 软件升级

软件升级

当前镜像版本: 1.0.0 Build 25020607

当前 BESS 软件版本: 1.1.1

选择升级类型，上传升级文件到设备。若需要获取升级文件，请联系 [Moxa 技术支持团队](#)。

✓ 仅限 BESS 软件

OS和BESS软件

升级文件 (.deb)

📎 Browse

保存

升级 OS 和 BESS 软件

1. 准备 .tar 升级文件。
2. 选择 **OS and BESS Software** (OS 和 BESS 软件)。
3. 单击 **Browse** (浏览) 上传文件并开始升级。

Home > 维护 > 软件升级

软件升级

当前镜像版本: 1.0.0 Build 25020607

当前 BESS 软件版本: 1.1.1

选择升级类型, 上传升级文件到设备。若需要获取升级文件, 请联系 [Moxa 技术支持团队](#)。

仅限 BESS 软件

✓ OS和BESS软件

升级文件 (.tar)

Browse

保存



注意

1. **电源:** 确保设备在整个升级过程中**保持通电状态**以防止发生故障。
2. **升级时长:** 该过程大约需要**5 分钟**, 但可能因升级类型和补丁大小而异。

软件恢复默认设置

该功能将重置所有软件设置为出厂默认值, 包括控制台密码在内的原有配置将全部清除。若需保留设备的 IP 地址、子网掩码等网络配置, 请在恢复出厂设置前勾选“**Keep current device network settings** (保留当前设备网络设置)”选项。

Home > 维护 > 软件恢复默认设置

软件恢复默认设置

将所有设置重置为出厂默认值, 包括控制台账户和密码。

☐ 保留当前设备网络设置
保留的项目包括模式、IP 地址、网络掩码、网关和 DNS。

重置



注意

Software Reset to Default (软件恢复默认设置) 将彻底重置软件配置, 并且您保存的所有参数将被丢弃。除非您确定要完全重置软件, 否则请不要使用该功能。

重启

您可以通过单击“RESTART（重新启动）”按钮来重新启动系统。





注意

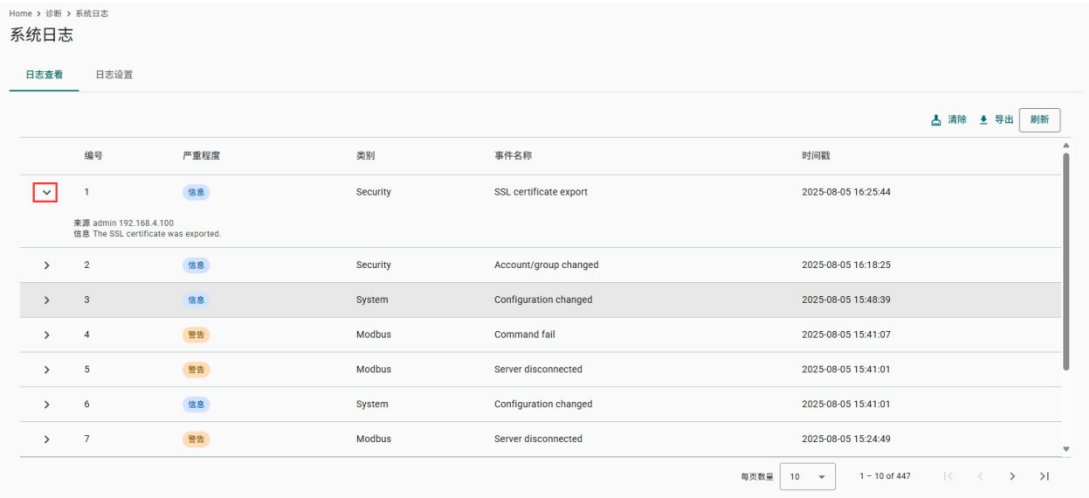
- 未保存的配置文件将在重启时被丢弃。
- 重启系统通常需要 1.5 到 2 分钟，请保持在同一网页上；系统准备就绪后，浏览器将自动重定向。

诊断

对于系统集成商或者技术工程师来说，有时候在设置一个新的应用程序或者系统运行一段时间后出现错误报告时，可能需要一些诊断工具来帮助排除故障。诊断功能聚合了相关工具以快速协助排除故障。

系统日志

在 **Log View（日志查看）** 选项卡中，将记录包含以下信息的事件：严重程度、类别、事件名称和时间戳。用户可以单击“>”图标阅读有关该活动的更多详细信息。



该软件还提供了一些管理功能，帮助用户方便地查看事件。

清除： 删除设备中的所有系统日志。

清除系统日志

此操作将清除设备上的所有系统日志，且无法恢复。您确定要继续吗？

取消

清除

导出： 导出系统日志以便排除故障。日志文件格式为 CSV。

刷新： 刷新页面以获取更多最新的日志记录。

在**Log Settings（日志设置）**选项卡中，当前日志容量将显示为百分比，以供参考。由于事件存储在本地存储中，因此可保存的事件数量有限。用户可以单击 **EDIT（编辑）** 按钮来管理设置。

Home > 诊断 > 系统日志

系统日志

日志查看

日志设置

日志设置

48 已启用的事件

当前日志容量: 4%

日志容量策略: 覆盖最旧的日志

编辑

事件设置

日志容量设置

事件设置

用户可以根据不同的事件类别和严重程度选择希望保存在本地系统日志中的事件。

Home > 诊断 > 系统日志 > 事件设置

< 事件设置

选择您想要保存在系统日志中的事件。您可以按不同的严重性筛选事件。
[请参见严重程度的详细信息](#)

严重性

通知

信息

警告

错误

搜索

System (12)

Network (9)

Security (17)

Maintenance (6)

Modbus (7)

DL/T 645 (2)

IEC 60870-5-104 (2)

IEC 61850 (4)

MQTT (2)

事件名称	严重性
Software ready	通知
Detect SD card	信息
SD card removed	警告
User trigger reboot	通知
Configuration changed	信息
Configuration changed failed	通知
NTP success	信息
NTP fail	警告
Manual setting time success	信息

事件分类如下。

类别	说明
系统	与系统相关的事件，如软件就绪。
网络	与以太网接口相关的事件，例如以太网链路已连接。
安全	这些事件可能被认为与安全有关；管理员可能需要弄清楚它发生的原因。例如登录失败事件。
维护	维护过程中通常会发生的事件，例如软件升级。

Modbus	与 Modbus 协议相关的事件，例如客户端连接、服务器连接。
IEC 60870-5-104	与 IEC 60870-5-104 协议相关的事件，例如客户端连接、客户端断开连接。
MQTT	与 MQTT 协议相关的事件，例如服务器已连接、服务器已断开连接。

事件严重程度分类如下。

优先事项	严重程度	说明
1	错误	表明存在问题的事件，但属于可能需要或不需要立即关注的类别。
2	警告	预警潜在问题的事件表明某些进一步的操作可能会导致严重错误。
3	注意	不是错误条件但可能需要特殊处理的事件。
4	信息类	确认程序按预期运行。

日志容量设置

容量管理：该软件提供 10,000 条审计记录。当本地系统日志已满时，用户可以单击 **Clear（清除）** 按钮清除日志。

策略设置：由于存储系统日志的容量有限，用户可以决定当日志容量达到极限时软件应该采取什么措施。

- **覆盖最旧的日志：**当系统日志已满时，新事件将自动覆盖旧事件。（默认选项）。
- **停止记录日志：**当系统日志已满时，新的事件记录将自动停止。

容量阈值（%）：当日志容量达到此处设置的值时，系统将通知用户或记录“日志阈值已达到”事件。默认值为 80%。

Home > 诊断 > 系统日志 > Log Capacity Settings

← 日志容量设置

容量管理

当前日志容量: 4%

设备最多可存储10,000条系统日志，您可以通过清除所有系统日志来管理日志容量。

清除

策略设置

请选择日志容量达到限制时的覆盖策略。

覆盖策略

☒ 覆盖最旧的日志

☐ 停止记录日志

系统将根据下面设置的值通知或记录“达到日志阈值”事件。

容量阈值 (%)

80

储存

协议状态

如果出现沟通问题，请访问**Diagnostic > Protocol Status**（**诊断 > 协议状态**）。该软件提供全面的故障排除工具，帮助您轻松识别问题。当您访问该页面时，您可以看到协议状态的概述。

Modbus 客户端

对于 Modbus 客户端故障排除，请执行以下操作：

1. 单击**Check**（**查看**）。
2. 选择 **TCP** 或 **COMx**。
3. 查看诊断信息。

← Modbus 客户端 - TCP ▾

状态检查诊断工具可帮助您识别连接问题。要编辑配置，请转到 [Modbus 客户端 TCP](#)

诊断 数据包监控

Modbus 总览 (1秒后自动刷新)

连接数量	1
已发送的请求	3121
收到的有效回复	3121
收到的无效回复	0
收到的异常	0
超时	0

连接 (1秒后自动刷新)

服务器ID	1
状态	OK
远程 IP / 端口	192.168.4.100:502
已发送的请求	3121
收到的有效回复	3121
收到的无效回复	0
收到的异常	0
超时	0

4. 单击“Traffic Monitoring（数据包监控）”选项卡来捕获流量日志。

Home > 诊断 > 协议状态 > Modbus 客户端 - TCP

← Modbus 客户端 - TCP ▾

状态检查诊断工具可帮助您识别连接问题。要编辑配置，请转到 [Modbus 客户端 TCP](#)

诊断 **数据包监控**

停止

正在捕获...

编号	时间	数据包类型	远程 IP / 端口	服务器ID	功能码 (十六进制)	数据
1	16:33:36.045	Request	192.168.4.100:502	1	3	0B 52 00 00 00 06 01 03 00 00 00 01
2	16:33:36.067	Response	192.168.4.100:502	1	3	0B 52 00 00 00 05 01 03 02 1F 61
3	16:33:37.045	Request	192.168.4.100:502	1	3	0B 53 00 00 00 06 01 03 00 00 00 01
4	16:33:37.068	Response	192.168.4.100:502	1	3	0B 53 00 00 00 05 01 03 02 1F 62
5	16:33:38.045	Request	192.168.4.100:502	1	3	0B 54 00 00 00 06 01 03 00 00 00 01
6	16:33:38.060	Response	192.168.4.100:502	1	3	0B 54 00 00 00 05 01 03 02 1F 63
7	16:33:39.045	Request	192.168.4.100:502	1	3	0B 55 00 00 00 06 01 03 00 00 00 01
8	16:33:39.064	Response	192.168.4.100:502	1	3	0B 55 00 00 00 05 01 03 02 1F 64
9	16:33:40.045	Request	192.168.4.100:502	1	3	0B 56 00 00 00 06 01 03 00 00 00 01
10	16:33:40.062	Response	192.168.4.100:502	1	3	0B 56 00 00 00 05 01 03 02 1F 65
11	16:33:41.045	Request	192.168.4.100:502	1	3	0B 57 00 00 00 06 01 03 00 00 00 01
12	16:33:41.058	Response	192.168.4.100:502	1	3	0B 57 00 00 00 05 01 03 02 1F 66

5. 导出流量日志并将其发送给经验丰富的工程师进行进一步分析。（可选）

Modbus TCP 服务器

对于 Modbus TCP 服务器故障排除，请执行以下操作：

1. 单击**Check**（查看）。
2. 查看诊断信息。

Home > 诊断 > 协议状态 > Modbus TCP 服务器

← Modbus TCP 服务器

状态检查诊断工具可帮助您识别连接问题。要编辑配置，请转到 [Modbus TCP 服务器](#)

诊断

数据包监控

Modbus 总览 (2秒后自动刷新)

连接数量

0

收到的有效请求

0

收到的无效请求

0

已发送的回复

0

已发送的异常

0

连接 (2秒后自动刷新)

尚无连接。

3. 单击“Traffic Monitoring（数据包监控）”选项卡来捕获流量日志。

Home > 诊断 > 协议状态 > Modbus TCP 服务器

← Modbus TCP 服务器

状态检查诊断工具可帮助您识别连接问题。要编辑配置，请转到 [Modbus TCP 服务器](#)

诊断

数据包监控

停止

正在捕获...

自动滚动

搜索 导出

编号	时间	数据包类型	远程 IP / 端口	服务器ID	功能码 (十六进制)	数据
----	----	-------	------------	-------	------------	----

4. 导出流量日志并将其发送给经验丰富的工程师进行进一步分析。（可选）

IEC 60870-5-104 服务器

对于 IEC 60870-5-104 服务器故障排除，请执行以下操作：

1. 单击**Check**（查看）。
2. 查看诊断信息。

Home > 诊断 > 协议状态 > IEC 60870-5-104 Server

← IEC 60870-5-104 服务器

状态检查诊断工具可帮助您识别连接问题。要编辑配置，请转到 [IEC 60870-5-104 服务器](#)

诊断

数据包监控

IEC 60870-5-104 总览 (1秒后自动刷新)

连接数量	0
发送非自发响应总数	0
发送自发响应总数	0
收到的请求总数	0
上次发送非自发响应的时间	N/A
上次发送自发响应的时间	N/A
上次收到请求的时间	N/A
内部指示	

连接 (1秒后自动刷新)

尚无连接。

3. 单击“Traffic Monitoring（数据包监控）”选项卡来捕获流量日志。

Home > 诊断 > 协议状态 > IEC 60870-5-104 Server

← IEC 60870-5-104 服务器

状态检查诊断工具可帮助您识别连接问题。要编辑配置，请转到 [IEC 60870-5-104 服务器](#)

诊断

数据包监控

停止

正在捕获 ...

☒ 自动滚动

搜索 导出 CSV 导出 PCAP

编号	时间	消息层	方向	连接的客户端 IP: 端口	数据
尚无数据包。请点击“开始”以捕获数据包。					

4. 导出流量日志并将其发送给经验丰富的工程师进行进一步分析。（可选）

网络监控

在 **Network Statistics**（网络统计）选项卡中，**Ethernet Packet Count**（以太网数据包统计）表显示每个网络端口的当前连接状态，并将以太网数据分为两个方向：发送和接收，计算每个数据包的数量。该**Protocol Packet Count**（协议数据包统计）表根据不同的协议对以太网数据进行分类，并统计 TCP、UDP、ICMP 和 IPv4 的数据包数量。

Home > 诊断 > 网络监控

网络监控

网络统计

网络连接

实时数据显示...

以太网数据包统计

✓ LAN1

LAN2

LAN3

LAN4

Cellular1

连接状态	已发送	接收
Connected	2473 (+0/s)	16457 (+3/s)

协议数据包统计

✓ TCP

UDP

ICMP

IPv4

已发送	已收到	丢失
26390 (+14/s)	14513 (+7/s)	0 (+0/s)

在 **Network Connections**（网络连接）选项卡中，该选项卡将显示所有 TCP 会话的状态。

Home > 诊断 > 网络监控

网络监控

网络统计

网络连接

实时数据显示...

协议	接收队列	发送队列	本地地址	远程主机地址	状态
TCP	0	0	*:502	*:0	LISTEN
TCP	0	0	*:22	*:0	LISTEN
TCP	0	0	*:8443	*:0	LISTEN
TCP	0	0	*:2404	*:0	LISTEN
TCP	0	0	192.168.4.127:8443	192.168.4.100:62797	TIME_WAIT
TCP	0	0	192.168.4.127:8443	192.168.4.100:62780	TIME_WAIT
TCP	0	0	192.168.4.127:8443	192.168.4.100:62800	TIME_WAIT
TCP	0	0	192.168.4.127:8443	192.168.4.100:62790	TIME_WAIT
TCP	0	0	192.168.4.127:8443	192.168.4.100:62811	ESTABLISHED
TCP	0	0	192.168.4.127:8443	192.168.4.100:62802	TIME_WAIT
TCP	0	0	192.168.4.127:8443	192.168.4.100:62782	TIME_WAIT

Ping

用户可以直接输入目标节点的 IP 地址或域名，单击 **Ping** 按钮。该软件将检查目标节点是否可以响应 ping 请求并将结果显示给用户。

Home > 诊断 > Ping

Ping

输入需要测试的IP地址或域名，点击“Ping”按钮并等待结果。

远程主机目标地址 ⓘ

Ping

结果

前言

该软件库支持您的自定义进程与数据流服务进行交互。简单来说，您可以使用库来**读取**或者**写入**来自软件中各种协议服务的数据（称为“标签”）。目前，该函数库支持 **C 语言**（未来计划增加对 C++、Python 和 Java 的支持）。本章提供快速指南，帮助您为工业或商业储能系统（ESS）开发一个简单的应用程序。

准备开发环境

该软件运行在 **MIL3 (Moxa 工业 Linux 3)** 上，是一款基于 Debian 11 且专为工业应用打造的操作系统。您可以使用以下两个推荐环境之一来开发您的应用程序：

在 Moxa (IPC) 设备上开发

由于您的应用程序最终将与软件一起在 Moxa 设备上运行，因此您可以直接在设备上进行编码、编译和测试。请按照以下步骤操作：

1. 设置您的 Moxa 设备并确保其已连接到互联网。
2. 登录到设备终端（使用 SSH 或串行控制台）。
3. 更新软件包列表：

```
moxa@moxa-tbzk1090923:~$ sudo apt update
```

4. 安装开发工具：

```
moxa@moxa-tbzk1090923:~$ sudo apt install gcc build-essential flex bison automake
```

在 Docker 环境中开发

如果您更喜欢在 PC 上进行开发，则可以使用 Moxa 提供的 Docker 环境：

1. 在您的工作机上**安装 Docker**。（有关详情，请访问 [Docker 官方网站](#)）。
2. 下载 Docker 图像：

```
moxa@moxa-tbzk1090923:~$ docker pull moxavma/aegis-sdk:latest-arm64
```

3. 启动 QEMU（模拟 ARM64 环境）：

```
moxa@moxa-tbzk1090923:~$ docker run -rm --privileged multiarch/qemu-user-static --reset -p yes
```

4. 运行并进入 Docker 容器：

```
moxa@moxa-tbzk1090923:~$ docker run -it moxavma/aegis-sdk:latest-arm64
```

快速入门：构建您的首个应用程序

按照以下步骤使用 C 语言库（libaegis）创建一个简单的应用程序：

1. 创建 C 语言源文件

将您的代码写入新文件中（例如，bess_app.c）。

```
/*
 * Include the Aegis library header file
 */
#include <aegis.h>
#include <stdlib.h>

int main(void)
{
    /*
     * Retrieve acquisition data:
     * (1) Use aegis_get_latest_tag_info() to obtain the tag information.
     *     "mx_io/DI_00/di_status" can be replaced with other tag names.
     * (2) Use aegis_get_tag_value() to get the acquired data for
     *     "mx_io/DI_00/di_status".
     */
    aegis_tag_info *tag = aegis_get_latest_tag_info("mx_io/DI_00/di_status");
    uint16_t data = *((uint16_t *)aegis_get_tag_value(tag));

    /*
     * Analyze and process the acquired data, then make control decisions:
     * (Develop according to the specific energy storage application scenario)
     */

    /*
     * Update the control decision or processed data to a data tag:
     * (1) Use aegis_write_latest_tag_value(). "Tag_B" can be replaced with
     *     another tag name.
     */
    uint16_t command = 0;
    aegis_write_latest_tag_value("Tag_B", &command, sizeof(uint16_t));

    /*
     * Release the memory allocated for the aegis_tag_info pointer after use
     */
    aegis_free_latest_tag_info(tag);

    return 0;
}
```

提示：有关 API 详细信息，请参阅“Application Example（应用示例）”和“C Library Function Reference（C 语言库函数引用）”部分。

2. 编译代码

运行以下命令（根据需要更新文件名）：

```
moxa@moxa-tbzk1090923:~$ gcc -o bess_app bess_app.c -laegis -I/opt/aegis/include -L/opt/aegis/lib
```

3. 部署可执行文件

如果您不是直接在 Moxa 设备上进行开发，请将可执行文件复制到该设备：

```
moxa@moxa-tbzk1090923:~$ scp ./bess_app moxa@192.168.4.127:/home/moxa
```

注意：将 `bess_app` 更新为您的可执行文件名称，并使用您的 Moxa 设备的正确 IP 地址。

4. 在 Moxa 设备上运行可执行文件

使用 root 权限执行应用程序来访问标签数据：

```
moxa@moxa-tbzk1090923:~$ sudo /home/moxa/bess_app
```

注意：访问标签数据需要使用 `sudo` 运行。

应用示例

示例 1：获取本地设备数据

目标：使用 C 语言库（libaegis）检索数据（例如，从 Modbus TCP 客户端）。

1. 配置 Modbus 客户端：

- 使用 Web 控制台添加设备并设置 Modbus 读取命令。



- 通过检查 Tag Dashboard（标签仪表盘）来验证是否创建了相应的标签。



2. 编写代码检索数据：

- 使用 C 语言库（libaegis）中的函数读取所需的标签数据。

```
/*
 * Include the Aegis library header file
 */
#include <aegis.h>

#include <stdlib.h>
#include <unistd.h>
#include <stdio.h>

int main(void)
{
    /*
     * Declare aegis_tag_info pointers to store the memory addresses returned
     * by aegis_get_latest_tag_info when retrieving tag information.
     */
    aegis_tag_info *tag1_info = NULL, *tag2_info = NULL;
    char *tag_raw_value;

    /*
     * Read the structure pointer for modbus_tcp_client/device1/tag_uint16
     */
    if ((tag1_info = aegis_get_latest_tag_info("modbus_tcp_client/device1/tag_uint16"))
```

```

== NULL)
{
    return -1;
}

/*
 * Retrieve various information from modbus_tcp_client/device1/tag_uint16
 * for logical operations:
 */
printf("value: %hu\n", *((uint16_t *)aegis_get_tag_value(tag1_info)));

/*
 * Debugging: Obtain tag details to diagnose potential issues.
 */
printf("tag name: %s\n", aegis_get_tag_name(tag1_info));
printf("written size: %d\n", aegis_get_tag_written_size(tag1_info));
printf("max size: %d\n", aegis_get_tag_max_size(tag1_info));
printf("type: %s\n", aegis_tag_type_to_str(aegis_get_tag_type(tag1_info)));
printf("access: %s\n", aegis_tag_access_to_str(aegis_get_tag_access(tag1_info)));
printf("unix timestamp: %ld\n", aegis_get_tag_timestamp(tag1_info));
printf("*****\n");

/*
 * Release the memory allocated for the aegis_tag_info pointer after use.
 */
aegis_free_latest_tag_info(tag1_info);

/*
 * Read the structure pointer for modbus_tcp_client/device1/tag_raw
 */
if ((tag2_info = aegis_get_latest_tag_info("modbus_tcp_client/device1/tag_raw")) ==
NULL)
{
    return -1;
}

/*
 * Retrieve various information from modbus_tcp_client/device1/tag_raw
 * for logical operations:
 */
tag_raw_value = (char *)aegis_get_tag_value(tag2_info);
printf("value: ");

for (uint32_t i = 0; i < aegis_get_tag_written_size(tag2_info); i++)
{
    printf("%x ", tag_raw_value[i]);
}

printf("\n");

/*
 * Debugging: Obtain tag details to diagnose potential issues.
 */
printf("tag name: %s\n", aegis_get_tag_name(tag2_info));
printf("written size: %d\n", aegis_get_tag_written_size(tag2_info));
printf("max size: %d\n", aegis_get_tag_max_size(tag2_info));
printf("type: %s\n", aegis_tag_type_to_str(aegis_get_tag_type(tag2_info)));
printf("access: %s\n", aegis_tag_access_to_str(aegis_get_tag_access(tag2_info)));
printf("unix timestamp: %ld\n", aegis_get_tag_timestamp(tag2_info));
printf("*****\n");

/*
 * Release the memory allocated for the aegis_tag_info pointer after use.
 */
aegis_free_latest_tag_info(tag2_info);

return 0;
}

```

- 在 Docker 容器中，您可以使用以下命令编译示例：

```
moxa@moxa-tbzk1090923:~$ make read_tag
```

3. 部署和测试：

- 将可执行文件复制到 Moxa 设备并运行以查看流程中的 Modbus 数据。

示例 2：控制本地设备

目标：使用 C 语言库（libaegis）通过 Modbus TCP 客户端更新本地设备上的数据。

1. 配置 Modbus 客户端：

在 Web 控制台中添加设备并设置 Modbus 写入命令。



检查 Tag Dashboard（标签仪表板）以确保标签正确映射。



2. 编写代码更新数据：

使用 C 语言库（libaegis）函数修改标签值。

```
/*
 * Include the Aegis library header file
 */
#include <aegis.h>

#include <stdlib.h>
#include <unistd.h>

int main(void)
{
    uint16_t tag_uint16_value = 1234;
    char tag_raw_value[] = {0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88};

    /*
     * Write the latest value to modbus_tcp_client/device1/tag_uint16
     */
    if (aegis_write_latest_tag_value("modbus_tcp_client/device1/tag_uint16", (void *) &
    (tag_uint16_value), 0))
    {
        return -1;
    }
}
```



```

    }

    /*
     * Write the latest value to modbus_tcp_client/device1/tag_raw
     */
    if (aegis_write_latest_tag_value("modbus_tcp_client/device1/tag_raw", (void
*)(tag_raw_value), sizeof(tag_raw_value)))
    {
        return -1;
    }

    return 0;
}

```

3. 使用以下代码编译示例:

```
make write_tag
```

4. 部署和验证:

将可执行文件复制到 Moxa 设备，运行，并确认标签值已更新。

您还可以使用类似的步骤与北向协议（例如，MQTT）进行交互以进行服务器通信。

BESS 应用：计算平均电压和 SoC

场景描述:

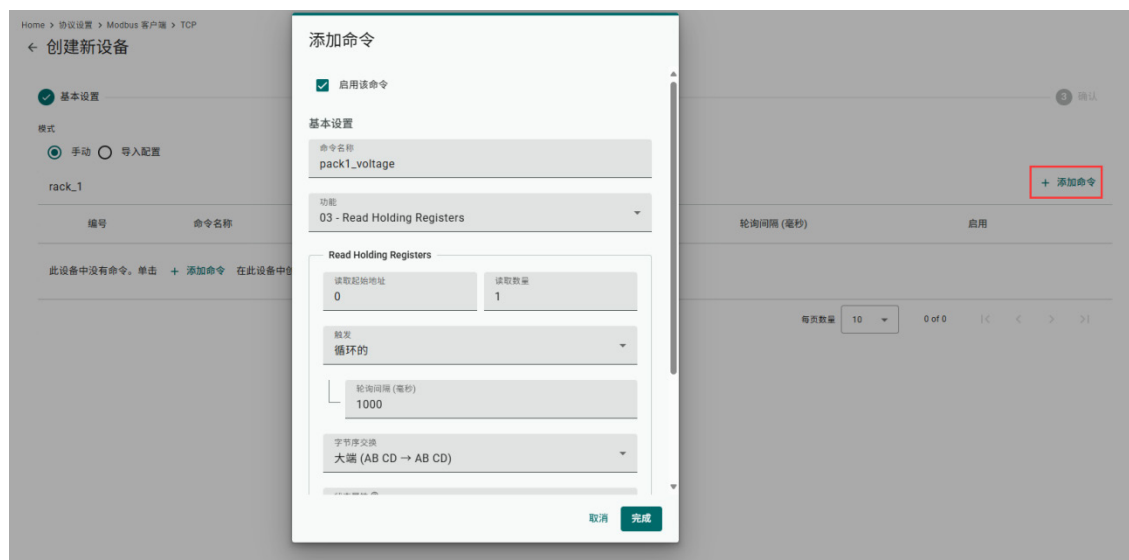
- **数据采集:** 使用 Modbus TCP 客户端从机架 BMS 设备收集电压数据。
- **数据处理:** 使用您的应用程序读取这些值，计算平均电压和充电状态（SoC），并将结果写回。
- **数据同步:** 然后，中央 EMS 系统（或云服务）可以通过 Modbus 获取平均数据。

指导步骤:

1. 配置 Modbus TCP 客户端:

- 在 Web 控制台中创建一个新设备。

- 设置读取命令以获取 BMS 数据。



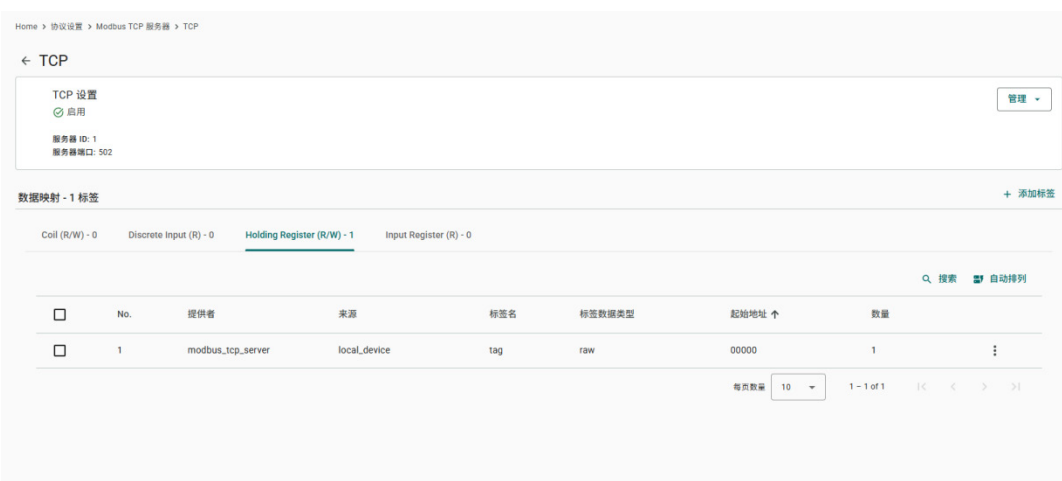
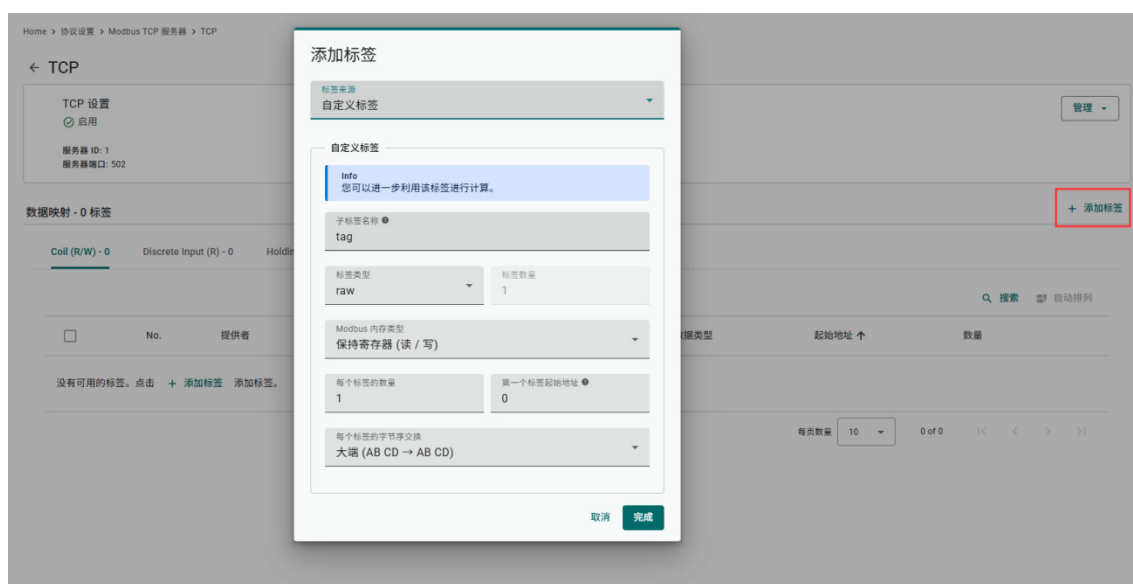
- 如果您有多个设备，请使用“clone（克隆）”功能复制配置。





2. 设置自定义标签：

- 在 Modbus 服务器中，创建映射到将存储平均值的内存地址的自定义标签。



3. 开发您的应用程序：

- 使用 C 语言库 (libaegis) 检索 BMS 电压和 SoC。
- 计算平均值。

- 将计算出的平均值写入自定义标签。
- 此示例代码在 SDK 中可用；使用 “*make voltage_soc*” 命令进行编译。

```

/*
 * Include the Aegis library header file
 */
#include <aegis.h>

#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <stdio.h>

/*
 * Number of battery racks
 */
#define RACK_COUNT      (3)
/*
 * Number of battery packs per rack
 */
#define PACK_COUNT      (10)

/*
 * Maximum length of a data tag name
 */
#define TAG_NAME_MAX_LEN (512)

int main(void)
{
    /*
     * Declare an aegis_tag_info pointer to store the memory pointer
     * returned by aegis_get_latest_tag_info when retrieving tag information.
     */
    aegis_tag_info *tag_info = NULL;

    char tag_name[TAG_NAME_MAX_LEN];
    float total_soc, average_voltage;
    uint16_t total_voltage;

    while (1)
    {
        /*
         * Iterate through all racks and use the Aegis library to retrieve
         * modbus-collected data for each rack.
         */
        for (int rack_idx = 1; rack_idx <= RACK_COUNT; rack_idx++)
        {
            total_voltage = 0;
            average_voltage = 0;
            total_soc = 0;

            /*
             * Iterate through all packs and use the Aegis library to retrieve
             * modbus-collected data for each pack.
             */
            for (int pack_idx = 1; pack_idx <= PACK_COUNT; pack_idx++)
            {
                /*
                 * Convert the modbus-collected voltage data tag name into a string.
                 */
                snprintf(tag_name, TAG_NAME_MAX_LEN,
"modbus_tcp_client/rack_%d/pack%d_voltage", rack_idx, pack_idx);

                /*
                 * Use aegis_get_latest_tag_info() from the Aegis library
                 * to retrieve the voltage data tag.
                 * tag_name - The full name of the data tag, composed as:
                 * acquisition protocol name/source device name/data name.
                 */
                if ((tag_info = aegis_get_latest_tag_info(tag_name)) == NULL)
                {
                    return -1;
                }
            }
        }
    }
}

```

```

    /*
     * Use aegis_get_tag_value() from the Aegis library to
     * obtain the value of the data tag.
     * After retrieving the value, convert the data type
     * and perform calculations.
     */
    total_voltage += *((uint16_t *)aegis_get_tag_value(tag_info));

    /*
     * Free the aegis_tag_info pointer memory to avoid memory leaks.
     */
    aegis_free_latest_tag_info(tag_info);

    /*
     * Convert the modbus-collected state of charge (SoC) data tag name
     * into a string.
     */
    snprintf(tag_name, TAG_NAME_MAX_LEN,
"modbus_tcp_client/rack_%d/ack%d_soc", rack_idx, pack_idx);

    /*
     * Use aegis_get_latest_tag_info() from the Aegis library to
     * retrieve the SoC data tag.
     * tag_name - The full name of the data tag, composed as:
     * acquisition protocol name/source device name/data name.
     */
    if ((tag_info = aegis_get_latest_tag_info(tag_name)) == NULL)
    {
        return -1;
    }

    /*
     * Use aegis_get_tag_value() from the Aegis library to
     * obtain the value of the data tag.
     * After retrieving the value, convert the data type
     * and perform calculations.
     */
    total_soc += *((float *)aegis_get_tag_value(tag_info));

    /*
     * Free the aegis_tag_info pointer memory to avoid memory leaks.
     */
    aegis_free_latest_tag_info(tag_info);
}

average_voltage = total_voltage / PACK_COUNT;

/*
 * Write the calculated value to the modbus TCP server's
 * average voltage tag.
 */
    snprintf(tag_name, TAG_NAME_MAX_LEN,
"modbus_tcp_server/local_device/rack%d_average_voltage", rack_idx);

    if (aegis_write_latest_tag_value(tag_name, (void *)&average_voltage,
sizeof(float)))
    {
        return -1;
    }

    /*
     * Write the calculated value to the modbus TCP server's total SoC tag.
     */
    snprintf(tag_name, TAG_NAME_MAX_LEN,
"modbus_tcp_server/local_device/rack%d_total_soc", rack_idx);

    if (aegis_write_latest_tag_value(tag_name, (void *)&total_soc,
sizeof(float)))
    {
        return -1;
    }
}

```

```

        /*
        * Execute the computation logic once per second.
        */
        sleep(1);
    }

    return 0;
}

```

4. 部署和验证:

- 在 Moxa 设备上运行可执行文件并检查 Tag Dashboard（标签仪表板）是否显示更新的平均值。

BESS 应用：检索历史数据

场景描述:

收集历史电压和 SoC 数据以进行分析、诊断或 AI 模型训练。

指导步骤:

1. 配置 Modbus TCP 客户端:

在 Web 控制台中设置设备和命令以收集 BMS 数据。

如果处理多个寄存器，使用 CSV 编辑来加快配置速度。

2. 启用数据保存:

激活“Data Persistence（数据保存）”功能，将所有标签数据存储在 SD 卡上。

详情请参阅系统设置中的“Data Persistence（数据保存）”部分。

3. 开发您的应用程序:

编写一个程序，使用 C 语言库（libaegis）函数将历史数据输出为 CSV 文件。

此示例代码在 SDK 中可用；使用“`make pack_historical_data`”命令进行编译。

```

/*
 * Include the Aegis library header file
 */
#include <aegis.h>

#include <stdio.h>
#include <stdlib.h>

int main(void)
{
    int ret;

    /* Define the structure variable for historical data query conditions */
    aegis_historical_query hist_query =
    {
        /*
        * Tag name format. In this example,
        * it represents querying all tags under the modbus TCP client
        * for the rack_1 device that start with "pack".
        */
        .tag_name = "modbus_tcp_client/rack_1/pack%",

        /*
        * Start timestamp.
        * NULL means retrieving the oldest timestamp in the historical data
        * for the specified tag name format.
        */
        .start_timestamp = NULL,

        /*
        * Time interval.

```

```

    /* Works together with the start timestamp to define a time range.
    */
    .interval = {.day = 0, .hour = 1, .min = 0, .sec = 0, .msec = 0},

    /*
    * Maximum number of data entries.
    * Limits the number of entries retrieved in sequence.
    * 0 means no limit.
    */
    .limit = 0,

    /*
    * Data offset.
    * Specifies the number of entries to skip in sequential retrieval.
    * 0 means no offset.
    */
    .offset = 0,

    /*
    * Data sorting order.
    * Arranges data by timestamp from oldest to newest.
    */
    .order = AEGIS_TIME_ASC
};

/* Define the file path */
char file_path[128] = {0};

/* Define the structure variable to store the historical data query results */
aegis_historical_result hist_result = {0};

int file_idx = 0;
while (1)
{
    /* Dynamically update the file name */
    snprintf(file_path, sizeof(file_path), "/home/moxa/historical_data_%d.csv",
file_idx);

    /* Retrieve historical tag data and write it to a file */
    if ((ret = aegis_get_historical_data_file(hist_query, file_path,
&hist_result)) != AEGIS_SUCCESS)
    {
        printf("aegis_get_historical_data_file write file(%s) error: %d\n",
file_path, ret);
        break;
    }

    printf("Saved historical data to %s\n", file_path);

    /*
    * Use the is_end_point_data flag in the historical data result structure to
check
    * if there are newer data points outside the current time range.
    */
    if (hist_result.is_end_point_data)
    {
        printf("Successfully retrieved all historical data\n");
        break;
    }

    /*
    * Use the end timestamp of this interval as the start timestamp for the next
interval
    * to fetch the next segment of historical data.
    */
    hist_query.start_timestamp = hist_result.end_timestamp;

    file_idx++;
}

return 0;
}

```

4. 部署和审查:

在 Moxa 设备上运行可执行文件。

验证 CSV 文件是否在指定文件夹中生成。

 historical_data_0.csv	9,610 KB	2024/10/16 下午 11:55:49	rw-r--r--
 historical_data_1.csv	9,622 KB	2024/10/16 下午 11:55:51	rw-r--r--
 historical_data_2.csv	9,623 KB	2024/10/16 下午 03:32:06	rw-r--r--
 historical_data_3.csv	9,622 KB	2024/10/16 下午 03:32:08	rw-r--r--
 historical_data_4.csv	9,621 KB	2024/10/16 下午 03:22:49	rw-r--r--
 historical_data_5.csv	9,622 KB	2024/10/16 下午 03:22:51	rw-r--r--
 historical_data_6.csv	9,622 KB	2024/10/16 下午 03:22:53	rw-r--r--
 historical_data_7.csv	9,622 KB	2024/10/16 下午 03:22:55	rw-r--r--
 historical_data_8.csv	9,623 KB	2024/10/16 下午 03:22:57	rw-r--r--
 historical_data_9.csv	9,507 KB	2024/10/16 下午 03:22:59	rw-r--r--
 historical_data_10.csv	9,615 KB	2024/10/16 下午 03:23:01	rw-r--r--
 historical_data_11.csv	9,597 KB	2024/10/16 下午 03:23:03	rw-r--r--
 historical_data_12.csv	9,620 KB	2024/10/16 下午 03:23:05	rw-r--r--

常见问题解答

问题 1.无法下载 “moxavma/aegis-sdk ” Docker 镜像。

回答 1.该镜像托管在 Dockerhub 上。如果您所在地区的网络问题阻碍了访问，请联系 Moxa 技术支持获取直接镜像文件。

问题 2.无法启动或运行 “moxavma/aegis-sdk ” Docker 容器。

回答 2.由于该镜像使用 QEMU 模拟 ARM64 环境，因此某些系统（例如 CentOS 7）可能不支持 QEMU。我们建议在 Windows、Debian 或 Ubuntu 上使用 WSL，或者联系 Moxa 技术支持寻求帮助。

问题 3.该示例在 Moxa 设备上运行后无法获取标签数据。

回答 3.确保以 root 权限（使用 sudo）运行可执行文件，因为访问标签数据需要更高的权限。

问题 4.用户进程运行一段时间后崩溃。

回答 4.崩溃通常是由于内存问题引起的。确保在使用后通过 aegis_free_latest_tag_info 释放指针。如果问题仍然存在，请添加调试代码或使用 GDB 等工具。

问题 5.我遇到了这里未列出的问题。

回答 5.请联系 Moxa 技术支持团队以获得进一步帮助。

aegis_get_latest_tag_info

原型:

```
aegis_tag_info *aegis_get_latest_tag_info(const char *tag_name);
```

说明:

检索指定标签的信息。返回的 *aegis_tag_info* 指针可以与其他 API 函数一起使用来获取:

- 标签名称: 通过 *aegis_get_tag_name*
- 最新标签值: 通过 *aegis_get_tag_value*
- 标签类型: 通过 *aegis_get_tag_type*
- 标签访问 (读/写权限): 通过 *aegis_get_tag_access*
- 写入大小 (以字节为单位): 通过 *aegis_get_tag_written_size*
- 最大可写大小 (以字节为单位): 通过 *aegis_get_tag_max_size*
- 上次更新时间戳 (Unix 时间戳): 通过 *aegis_get_tag_timestamp*

重要提示:

使用完标签信息后, 通过调用 *aegis_free_latest_tag_info* 释放已分配的内存。

输入参数:

- **[in] tag_name:** 表示标签名称的字符串。格式应为:

\${provider_name}/\${source_name}/\${sub_tag_name}

返回值:

- 当满足以下条件时, 将返回指向 *aegis_tag_info* 的指针:
 - *Tag_name* 不为 NULL, 并且
 - 具有指定名称的标签已存在。
- 否则, 返回 *NULL*。

aegis_write_latest_tag_value

原型:

```
aegis_ret_code aegis_write_latest_tag_value(const char *tag_name, const void *value, int written_size);
```

说明：

将新值写入指定标签。

- 对于**数字类型**（例如，boolean、int8、int16、...），*written_size* 可以是任意值；系统将使用创建标签时设置的最大大小。
- 对于**非数字类型**（例如字符串、字节数组、原始数据），*written_size* 必须反映正在写入的数据的大小。如果该值超出最大大小，将被截断。

注意：

- **截断：**如果输入值的长度超出了预设的大小或指定的 *written_size*，该值将被自动截断（例如，写入 9223372036854775807 放入 int16 标签可能会导致 -1）。
- **竞态条件：**为了避免多个写入者发生冲突，实际的写入操作是按照函数调用的顺序依次执行的。

输入参数：

- **[in] tag_name:** 表示标签名称的字符串。格式应为：

`${provider_name}/${source_name}/${sub_tag_name}`
- **[in] value:** 指向要写入的数据的指针。
- **[in] written_size:** 要写入的数据的大小（以字节为单位）。

返回值：

- 当满足以下条件时，将返回0：
 - *Tag_name* 不为 NULL，并且对应于现有标签。
 - 该标签具有写访问权限。
 - *Value* 不为 NULL。
 - 对于非数字类型（字符串、字节数组、原始数据），*written_size* 大于 0。
- 否则，返回非零错误代码。可能的错误代码包括：
 - *AEGIS_INVALID_PARAM* = 1（传入参数为 NULL）
 - *AEGIS_TAG_NOT_FOUND* = 3（未找到标签）
 - *AEGIS_TAG_ACCESS_FAILED* = 4（尝试写入只读标签）
 - *AEGIS_WRITE_SIZE_ERROR* = 5（无效的写入大小）
 - *AEGIS_INTERNAL_ERROR* = 6（内部错误）

aegis_get_tag_name

原型：

```
const char *aegis_get_tag_name(aegis_tag_info *tag_info);
```

说明:

从提供的 *tag_info* 检索标签名称。

输入参数:

- **[in] tag_info:** 从 *aegis_get_latest_tag_info* 获取的指针。

返回值:

- 返回标签名称（格式为: *\${provider_name}/\${source_name}/\${sub_tag_name}*），条件是 *tag_info* 是有效的。
- 否则，返回 *NULL*。

aegis_get_tag_value

原型:

```
void *aegis_get_tag_value(aegis_tag_info *tag_info);
```

说明:

检索标签的最新值。

注意:

返回值为 *void **。对于算术运算，将其转换为适当的类型。

输入参数:

- **[in] tag_info:** 从 *aegis_get_latest_tag_info* 获取的指针。

返回值:

- 如果 *tag_info* 是有效的，则返回指向最新标签的指针。
- 否则，返回 *NULL*。

aegis_get_tag_type

原型:

```
aegis_tag_type aegis_get_tag_type(aegis_tag_info *tag_info);
```

说明:

检索标签的类型。返回值可以使用 *aegis_tag_type_to_str* 转换为字符串。

输入参数:

- **[in] tag_info:** 从 *aegis_get_latest_tag_info* 获取的指针。

返回值:

- 如果 *tag_info* 有效，则返回以下标签类型常量之一:

- *AEGIS_TAG_TYPE_BOOLEAN* = 0 (布尔值)
- *AEGIS_TAG_TYPE_INT8* = 1
- *AEGIS_TAG_TYPE_INT16* = 2
- *AEGIS_TAG_TYPE_INT32* = 3
- *AEGIS_TAG_TYPE_INT64* = 4
- *AEGIS_TAG_TYPE_UINT8* = 5
- *AEGIS_TAG_TYPE_UINT16* = 6
- *AEGIS_TAG_TYPE_UINT32* = 7
- *AEGIS_TAG_TYPE_UINT64* = 8
- *AEGIS_TAG_TYPE_FLOAT* = 9
- *AEGIS_TAG_TYPE_DOUBLE* = 10
- *AEGIS_TAG_TYPE_STRING* = 11
- *AEGIS_TAG_TYPE_BYTEARRAY* = 12
- *AEGIS_TAG_TYPE_RAW* = 13
- 如果无效，则返回 *AEGIS_TAG_TYPE_ERROR* = -1。

aegis_get_tag_access

原型:

```
aegis_tag_access aegis_get_tag_access(aegis_tag_info *tag_info);
```

说明:

检索标签的读/写访问权限。您可以使用 *aegis_tag_access_to_str* 将结果转换为字符串。

输入参数:

- **[in] tag_info**: 从 *aegis_get_latest_tag_info* 获取的指针。

返回值:

- 如果 tag_info 有效，则返回:
 - *AEGIS_TAG_ACCESS_RW* = 0 (读写)
 - *AEGIS_TAG_ACCESS_RO* = 1 (只读)
- 否则，返回 *AEGIS_TAG_ACCESS_ERROR* = -1。

aegis_get_tag_written_size

原型:

```
uint32_t aegis_get_tag_written_size(aegis_tag_info *tag_info);
```

说明:

检索最新标签值写入的字节数。

- 对于**数字类型**（例如，boolean、int8、int16、……），此大小等于最大可写大小。
- 对于**非数字类型**（例如，字符串、字节数组、原始数据），此大小小于或等于最大可写大小。

输入参数:

- **[in] tag_info**: 从 *aegis_get_latest_tag_info* 获取的指针。

返回值:

- 如果 *tag_info* 是有效的，则返回最新写入值的大小（以字节为单位）。
- 否则，返回 0。

aegis_get_tag_max_size

原型:

```
uint32_t aegis_get_tag_max_size(aegis_tag_info *tag_info);
```

说明:

检索标签的最大可写大小（以字节为单位）。

输入参数:

- **[in] tag_info**: 从 *aegis_get_latest_tag_info* 获取的指针。

返回值:

- 如果 *tag_info* 是有效的，则返回最大可写大小（以字节为单位）。
- 否则，返回 0。

aegis_get_tag_timestamp

原型:

```
uint64_t aegis_get_tag_timestamp(aegis_tag_info *tag_info);
```

说明:

检索标签最新值更新时的时间戳（Unix 时间戳）。

输入参数:

- **[in] tag_info**: 从 *aegis_get_latest_tag_info* 获取的指针。

返回值:

- 如果 *tag_info* 是有效的，则返回时间戳。
- 否则，返回 0。

aegis_tag_type_to_str

原型:

```
const char *aegis_tag_type_to_str(aegis_tag_type tag_type);
```

说明:

将标签类型常量转换为其对应的字符串表示形式。

输入参数:

- **[in] tag_type:** 通过 *aegis_get_tag_type* 返回的标签类型值。

返回值:

- 如果 *tag_type* 是有效的，则返回相应的字符串。
- 否则，返回 “error”。

aegis_tag_access_to_str

原型:

```
const char *aegis_tag_access_to_str(aegis_tag_access tag_access);
```

说明:

将标签访问常量转换为其对应的字符串表示形式。

输入参数:

- **[in] tag_access:** 通过 *aegis_get_tag_access* 返回的标签访问值。

返回值:

- 如果 *tag_access* 是有效的，则返回相应的字符串。
- 否则，返回 “error”。

aegis_free_latest_tag_info

原型:

```
void aegis_free_latest_tag_info(aegis_tag_info *tag_info);
```

说明:

释放通过 *aegis_get_latest_tag_info* 获取的标签信息所分配的内存。

输入参数:

- **[in] tag_info**: 通过 *aegis_get_latest_tag_info* 返回的指针。

返回值:

- 无。

aegis_get_tag_name_list

原型:

```
aegis_tag_name_list *aegis_get_tag_name_list();
```

说明:

检索所有当前标签名称的链接列表。列表中的每个节点包含:

- *tag_name*: 标签名称。
- *next*: 指向列表中下一个节点的指针。

重要提示:

使用列表后, 通过 *aegis_free_tag_name_list* 释放其内存。

输入参数:

- 无。

返回值:

- 如果标签存在, 则返回指向链接列表的指针。
- 如果没有创建标签, 则返回 *NULL*。

aegis_free_tag_name_list

原型:

```
void aegis_free_tag_name_list(aegis_tag_name_list *tag_list);
```

说明:

释放通过 *aegis_get_tag_name_list* 获取的标签名称链表分配的内存。

输入参数:

- **[in] tag_list**: 指向标签名称链接列表的开头的指针。

返回值:

- 无。

aegis_get_historical_data_file

原型:

```
aegis_ret_code aegis_get_historical_data_file(aegis_historical_query hist_query, char
*file_path, aegis_historical_result *hist_result);
```

说明:

检索与指定命名模式匹配的标签的历史数据并将数据写入 CSV 文件。

输入参数:

- **[in] hist_query:** 包含查询参数的结构，其中包括：
 - **tag_name:** 标签名称字符串，格式为 `${provider_name}/${source_name}/${sub_tag_name}`。每个组件的最大长度为 128 个字符。允许的字符包括字母（az、AZ）、数字（0-9）和符号（. _ ~ \$）。支持通配符（%）。
- **示例:**
 - `"modbus_tcp_client/bms_1/battery_soc_1"`: 检索单个标签的历史数据。
 - `"modbus_tcp_client/bms_1/battery_soc_%"`: 检索与模式匹配的多个标签的历史数据。
 - `"modbus_tcp_client/bms_1/%"`: 检索设备 `bms_1` 的所有标签。
 - `"%/%%/%"`: 检索 Aegis 中所有标签的历史数据。
- **start_timestamp:** 开始时间戳（格式: “yyyy-mm-dd hh:mm:ss.SSS ± zz:zz”）。如果 `NULL`，则查询从第一个可用数据点开始。
- **interval:** 时间间隔（天数、小时数、分钟数、秒数、毫秒数），从 `start_timestamp` 开始计算。总间隔不得超过一天。
- **limit:** 检索的最大数据点数（0 表示无限制）。
- **offset:** 数据偏移量（0 表示无偏移）。
- **order:** 按时间戳对数据进行排序（升序: `AEGIS_TIME_ASC` 或降序: `AEGIS_TIME_DESC`）。
- **[in] file_path:** 将要写入历史数据的 CSV 文件的路径（例如，`/data/historical_data.csv`）。仅支持 CSV 格式。
- **[out] hist_result:** 指向将要填充查询结果的结构体的指针。成员包括：
 - **start_timestamp:** 检索到的数据范围的开始时间戳（UTC+0）。
 - **end_timestamp:** 检索到的数据范围的结束时间戳（UTC+0）。
 - **is_end_point_data:** 指示是否已达到最新历史数据的标志。

返回值:

满足以下条件，则返回 0（成功）:

- `Hist_query.tag_name` 不为 `NULL`，并且格式正确。
- `Hist_query.start_timestamp` 格式正确。

- *Hist_query.interval* 在允许范围内。
- *Hist_query.order* 是有效值。
- *File_path* 中指定的目录存在并且可写。
- 文件系统中有足够的空间。
- 文件扩展名为 *.csv*。

否则，返回非零错误代码。可能的错误代码包括：

- *AEGIS_INTERNAL_ERROR* = 6
- *AEGIS_TAG_NAME_INVALID* = 7
- *AEGIS_TIMESTAMP_INVALID* = 8
- *AEGIS_INTERVAL_INVALID* = 9
- *AEGIS_DATA_ORDER_INVALID* = 10
- *AEGIS_FILE_PATH_INVALID* = 11
- *AEGIS_WRITE_PERMISSION_DENIED* = 12
- *AEGIS_WRITE_OUT_OF_SPACE* = 13
- *AEGIS_WRITE_FILE_FORMAT_INVALID* = 14

这样就完成了 C 语言库函数引用。使用这些函数可以有效地与标签数据交互，确保按照描述正确处理错误和进行内存管理。如果您有任何其他问题或需要澄清任何功能，请联系技术支持团队。

C. 高级 MQTT 发布主题配置

概述

在 BESS 应用程序中，MQTT 客户端可用于将数千个标签的数据（例如来自 BMS、PCS 和仪表的数据）发布到云端。将大量标签数据打包到 MQTT 消息中会消耗大量 CPU、内存和网络资源。为了优化性能，有效配置 MQTT 发布主题至关重要。本节提供在不同 BESS 场景中配置 MQTT 主题的指导和示例。

影响发布性能的关键参数

配置 MQTT 主题时，请考虑以下因素：

- **主题数量：**

更多主题（用于发布和订阅）会增加 CPU 和内存使用率。

- **消息发布频率：**

频率越高，意味着 MQTT 客户端打包和发送消息的频率就越高，从而增加了 CPU 的负载。

- **标签数据采样率：**

采样率（以秒为单位）决定了每条消息的每个标签收集多少个数据点。更高的采样率意味着压缩的数据更多，消耗的内存也更多。

- **有效负载中引用的标签数量：**

消息中包含的标签越多，有效负载就越大，资源使用量也就越大。

配置指南和示例

主要建议

- **具有相同采样率的组标签：**

确保单个主题内的所有标签共享相同的数据采样率。

- **限制每条消息的总数据量：**

力求将每条消息中的“数据量”总量保持在 15,000 以下。

数据计数公式：

$$\text{数据量} \approx (\text{引用的标签数量}) \times (\text{标签数据采样率}) \times (\text{消息发布频率})$$

为了将数据数量保持在 15,000 以下，发布间隔应设置为：

$$\text{发布间隔} \leq (15,000 / \text{标签数}) \times (\text{采样率})$$

示例方法

1.集中配置

- 关键标签示例：
 - 场景：每 0.1 秒更新 300 个关键标签
 - 计算：
$$\text{发布间隔} \leq (15,000 / 300) \times 0.1 = 5 \text{ 秒}$$
 - 配置：
为这 300 个关键标签创建 1 个主题，并将发布间隔设置为 ≤ 5 秒。
- 普通标签示例：
 - 场景：每 1 秒更新 15,000 个普通标签
 - 计算：
$$\text{发布间隔} \leq (15,000 / 15,000) \times 1 = 1 \text{ 秒}$$
 - 配置：
为这 15,000 个普通标签创建 1 个主题，并将发布间隔设置为 ≤ 1 秒。

2.分布式配置

- 关键标签示例：
 - 场景：每 0.1 秒更新 300 个关键标签
 - 配置：
分为 5 个主题，每个主题有 60 个标签。
 - 计算：
$$\text{发布间隔} \leq (15,000 / 60) \times 0.1 = 25 \text{ 秒}$$
- 普通标签示例：
 - 场景：每 1 秒更新 15,000 个普通标签
 - 配置：
分为 20 个主题，每个主题有 750 个标签。
 - 计算：
$$\text{发布间隔} \leq (15,000 / 750) \times 1 = 20 \text{ 秒}$$

其他场景示例

场景	关键标签（更新率）	普通标签（更新率）	集中配置	分布式配置
A	250 个标签 （100 毫秒）	5,000 个标签 （30 秒）	1 个主题，250 个关键标签；发布间隔 ≤ 6 秒 1 个主题对应 5,000 个普通标签；发布间隔 ≤ 90 秒	5 个主题（每个主题 50 个关键标签）；发布间隔 ≤ 30 秒 20 个主题（每个主题 250 个普通标签）；发布间隔 ≤ 1,800 秒
B	250 个标签 （100 毫秒）	5,000 个标签 （10 秒）	1 个主题，250 个关键标签；发布间隔 ≤ 6 秒 1 个主题对应 5,000 个普通标签；发布间隔 ≤ 30 秒	5 个主题（每个主题 50 个关键标签）；发布间隔 ≤ 30 秒 20 个主题（每个主题 250 个普通标签）；发布间隔 ≤ 600 秒
C	200 个标签 （100 毫秒）	3,000 个标签 （30 秒）	1 个主题对应 200 个关键标签；发布间隔 ≤ 7 秒 1 个主题对应 3,000 个普通标签；发布间隔 ≤ 150 秒	5 个主题（每个主题 40 个关键标签）；发布间隔 ≤ 37 秒 20 个主题（每个主题 150 个普通标签）；发布间隔 ≤ 3,000 秒
D	100 个标签 （100 毫秒）	15,000 个标签 （30 秒）	1 个主题对应 100 个关键标签；发布间隔 ≤ 15 秒 1 个主题对应 15,000 个普通标签；发布间隔 ≤ 30 秒	5 个主题（每个主题 20 个关键标签）；发布间隔 ≤ 75 秒 20 个主题（每个主题 750 个普通标签）；发布间隔 ≤ 600 秒

介绍

本文档提供了有关如何配置软件和安全安装设备的指南。本文档推荐的步骤可作为大多数应用场景下的安全最佳实践。我们强烈建议您在现场应用之前彻底检查和评估设置，以确保安全的环境。

常规系统信息

支持的设备和系统

型号	操作系统	固件版本
VM-1220-T-BESS 系列	Moxa 工业 Linux 3	V1.0.0

物理安全措施

该设备应采用物理安全措施进行保护，例如闭路电视监控、保安人员、防护屏障、锁、门禁控制和周界入侵检测。应根据环境和物理攻击的风险级别确定适当的物理安全类型。

配置和强化信息

TCP/UDP 端口和推荐服务

请参阅下表，了解用于与其他设备通信的所有端口、协议和服务。

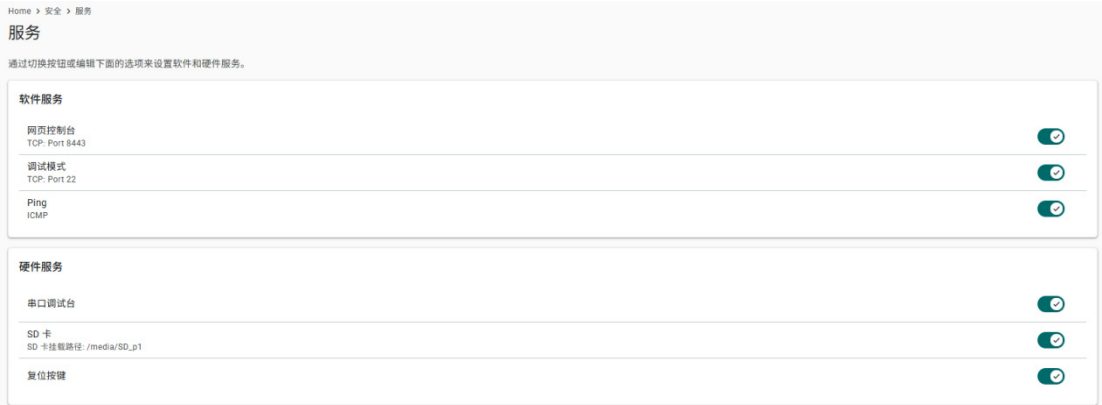
服务名称	选项	默认设置	类型	端口号	说明
HTTPS 服务器	启用、禁用	启用	TCP	8443	安全的 Web 控制台
SSH 服务器	启用、禁用	启用	TCP	22	SSH 控制台
DNS 客户端	启用	启用	UDP	53	处理 DNS 和 WINS（客户端）数据
DHCP 服务器	启用、禁用	禁用	UDP	67	为本地网络上的设备分配 IP 地址和网络设置。
DHCP Client	启用、禁用	启用	UDP	68	为设备手动分配 IP 地址
NTP 客户端	启用、禁用	禁用	UDP	123	网络时间协议，用于从服务器同步系统时间
Modbus TCP 服务器	启用、禁用	禁用	TCP	502	502 用于 Modbus 通信

IEC-104 服务器	启用、 禁用	禁用	TCP	2404	2404 用于 IEC-104 协议通信
--------------------	-----------	----	-----	------	----------------------

出于安全原因，请考虑禁用未使用的服务。初始设置后，使用安全性更强的服务进行数据通信。请参阅下表了解建议的设置。

服务名称	建议设置	类型	端口号	安全备注
HTTPS 服务器	启用	TCP	8443	安全的 Web 控制台
SSH	禁用	TCP	22	如果不需要远程访问设备进行配置，请禁用该服务
DNS 客户端	启用	UDP	53	获取 IP 的必要服务；无法禁用
DHCP 服务器	禁用	UDP	67	如果未使用，则禁用此服务
DHCP Client	禁用	UDP	68	为设备手动分配 IP 地址
NTP 客户端	禁用	UDP	123	如果未使用，则禁用此服务
Modbus TCP 服务器	禁用	TCP	502	如果不需要使用 Modbus TCP 服务器协议，请禁用此服务
IEC-104 服务器	禁用	TCP	2404	如果不需要使用 IEC-104 服务器协议，请禁用此服务

要启用或禁用 HTTPS 和 SSH 服务，请登录 HTTPS 控制台并访问 **SECURITY > Service**（安全 > 服务）



要禁用 NTP 服务，请登录 HTTPS 控制台，访问 **SYSTEM SETTINGS > General Settings > Date & Time**（系统设置 > 常规设置 > 日期和时间），并保持手动的时间设置。



要禁用 DHCP 客户端和服务，请登录 HTTPS 控制台并访问 **NETWORK SETTINGS > Ethernet**（网络设置 > 以太网），并保持模式为静态并禁用 DHCP 服务器。

Home > 网络设置 > 以太网

以太网

LAN1 LAN2 LAN3 LAN4

WAN (广域网)

模式

☐ DHCP: 自动获取 IP 地址

☒ 静态: 指定 IP 地址

IPv4 地址

.

.

.

子网掩码

.

.

.

网关

.

.

.

此值是必需的。

首选 DNS 服务器 - 可选

.

.

.

备用 DNS 服务器 - 可选

.

.

.

☐ 启用 DHCP 服务器 ⓘ

保存

要启用或禁用协议服务，请登录 HTTPS 控制台并访问 **PROTOCOL SETTINGS > Protocol Combination**（协议设置 > 协议组合）。

协议组合

北向

选择 +



VM-1220-T-BESS-P



南向

选择 +

串行端口和推荐服务

有关使用串行端口的所有通信协议，请参阅下表。

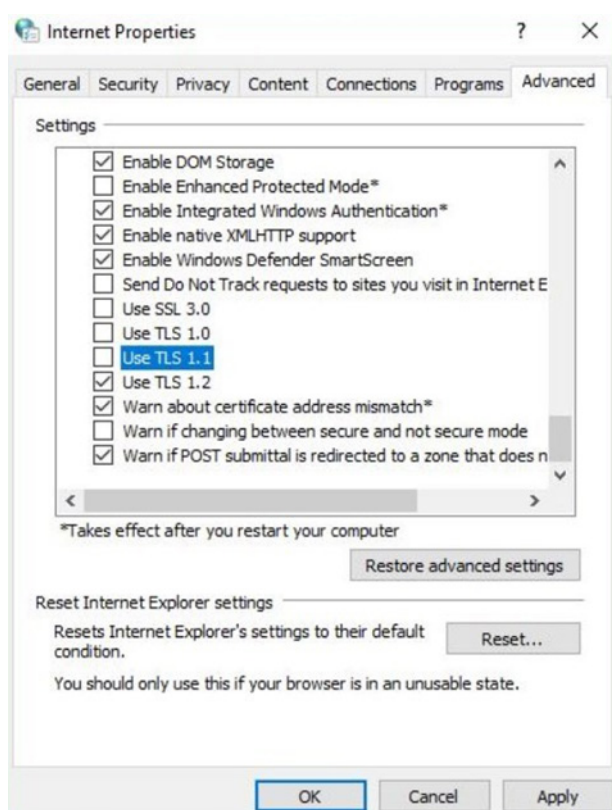
服务名称	选项	默认设置	类型	说明
Modbus RTU	启用、禁用	禁用	RS-232/485	Modbus 串行协议

出于安全原因，请考虑禁用未使用的服务。下表中建议的串行设置取决于不同的型号和用户偏好。确保串行连接和电缆受到物理保护。

服务名称	建议设置	类型	安全备注
Modbus RTU	禁用	RS-232/485	串行连接和电缆受到物理保护

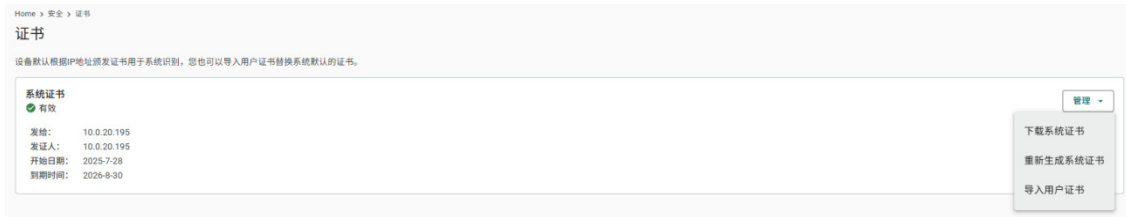
HTTPS 和 SSL 证书

HTTPS 是一种加密的通信通道。由于 TLS v1.1 及更低版本存在严重且易被利用的漏洞，因此该软件使用 TLS v1.2 进行 HTTPS 以保护数据传输。确保您的浏览器已启用 TLS v1.2。



要想使用 Web 控制台而不出现证书警告，您需要导入由第三方证书颁发机构颁发的受信任证书或将软件自签名证书导出到浏览器。

登录 Web 控制台并访问 **Security > Certificate**（安全 > 证书）。单击 **MANAGE**（管理）按钮导入用户证书。



系统证书在软件上的行为：

- 当 IP 地址更改时，软件将自动生成自签名 SSL 证书，或者您可以单击重新生成系统证书选项手动生成新的证书。建议您导入由受信任的第三方证书颁发机构 (CA) 或组织的 CA 认证的 SSL 证书。
- 软件自签名证书基于椭圆曲线加密 (ECC) 256 位算法编码，应该与大多数应用程序兼容。某些应用程序可能需要更长或更强的密钥，需要导入第三方证书。请注意，密钥越长，浏览 Web 控制台的速度就越慢，因为加密和解密通信数据的复杂性增加了。

导入第三方受信 SSL 证书：

要通过第三方生成 SSL 证书，步骤如下：

- 第 1 步：创建证书颁发机构 (根 CA)，例如 Microsoft AD Certificate Service (<https://mizitechinfo.wordpress.com/2014/07/19/step-by-step-installing-certificate-authority-on-windows-server-2012-r2/>)
- 第 2 步：找到一个工具来颁发证书签名请求 (CSR) 文件。从第三方 CA 公司（例如 DigiCert）获取证书 (<https://www.digicert.com/easycsr/openssl.htm>)。
- 第 3 步：将 CSR 文件提交给公共认证机构以获取签名的证书。
- 第 4 步：将证书导入软件。请注意，该软件仅接受使用 “.pem” 格式的证书，并支持以下加密算法：
 - RSA-1024、RSA-2048、RSA-3072、RSA-4096
 - ECC-256、ECC-384 和 ECC-521

一些知名第三方 Ca（证书颁发机构）公司供您参考
(https://en.wikipedia.org/wiki/Certificate_authority):

- IdenTrust (<https://www.identrust.com/>)
- DigiCert (<https://www.digicert.com/>)
- Comodo Cybersecurity (<https://www.comodo.com/>)
- GoDaddy (<https://www.godaddy.com/>)
- Verisign (<https://www.verisign.com/>)

软件补丁和升级

补丁管理

关于补丁管理，Moxa 每年都会发布版本增强功能，并附有详细的发布说明。

软件升级

有关软件升级的详细说明，请参阅 “**Web Console Configuration and Troubleshooting > Maintenance > Software Upgrade** (Web 控制台配置和故障排除 > 维护 > 软件升级)” 部分。

停用建议

停用设备时，请参阅 Moxa Industrial Linux 手册，并执行 **Decommissioning the System** (系统停用) 章节中的相关步骤。

安全信息与漏洞反馈

随着工业物联网 (IIoT) 的应用持续快速增长，安全性已成为重中之重。Moxa 产品安全事件响应团队 (PSIRT) 正在采取积极主动的方法来保护我们的产品免受安全漏洞的影响，并帮助我们的客户更好地管理安全风险。

请访问以下链接关注更新的 Moxa 安全信息：<https://www.moxa.com/en/support/product-support/security-advisory>