SIEMENS西门子 S-1FL2高惯量型电机 1FL2310-2AC01-1SB0

产品名称	SIEMENS西门子 S-1FL2高惯量型电机 1FL2310-2AC01-1SB0
公司名称	浔之漫智控技术(上海)有限公司
价格	.00/件
规格参数	西门子:原装正品 驱动器电机电缆:假一罚十 德国:现货包邮
公司地址	上海市松江区石湖荡镇塔汇路755弄29号1幢一层A区213室
联系电话	15801815554 15801815554

产品详情

点击该图标，激活用户账号。
分配了此用户账号的用户可以访问全部或特定变频器的数据和功能。 提示
变频器数据和功能的显示取决于分配给用户账号的访问权限。 点击该图标，删除用户账号。
只有在相应对话框中确认安全提示后，用户账号才会被删除。 编辑 “ Anonymous ” 用户 前提条件
作为具有 “ 管理用户和角色 ” 权限的用户登录。 操作步骤 图标 说明
点击该图标，打开 “ 编辑用户 ” 对话框。 在此对话框中可更改用户的角色分配。
点击该图标，禁用用户。 只有通过身份验证才能访问变频器的数据和功能。 点击该图标，激活用户。
无需通过身份验证即可访问变频器的数据和功能。 提示 根据分配给 "Anonymous"
用户的权限，在未进行身份验证访问时显示变频器 的数据和功能。 检查角色以及对应的功能权限 简介
在 “ 角色 ” 功能视图中，可查看已有用户角色以及对应的功能权限。前提条件
作为具有 “ 管理用户和角色 ” 权限的用户登录。 操作步骤 通过 “ 系统 > 用户管理 >
角色 ” 调用 “ 角色 ” 功能视图。 更多信息
关于已有用户角色和功能权限对应关系的详细信息，可查看章节 “ 具有运行功能权限、可以
访问变频器的角色 (页 69) ” 。 配置密码规则 简介
在 “ 用户管理 ” 功能视图的 “ 密码规则 ” 选项卡中定义以下要求： 密码复杂度 密码定期修改
密码规则适用于所有需要进行身份验证的用户。
密码规则可以更改，并确定是否激活密码定期修改以及如何修改。
关于密码规则可配置性的更多信息，可查看章节 “ 配置访问 (页 59) ” 。 前提条件
作为具有 “ 管理用户和角色 ” 权限的用户登录。 操作步骤 1. 通过 “ 系统 > 用户管理 >
密码规则 ” 调用 “ 密码规则 ” 功能视图。 2. 配置密码复杂度设置。 3.
激活密码定期修改，进行所需的设置。 4. 使用 “ 应用 ” 确认输入。 5. 点击 ，掉电保存设置。
如果启用了 “ 自动保存 ” 功能，则不会显示保存图标。用户登录 简介
用户只能访问他们有权使用的数据和功能。 前提条件 UMAC 已激活。

需要有一个有效的用户账号，以访问网络服务器。 已登录网络服务器。 或者
在激活了会话超时且设置的时间经过后，用户已自动注销。
有关无活动会话超时可配置性的更多信息，参见章节“ 配置访问 (页 59) ”。 操作步骤 1.
在网络服务器的状态栏点击“ 登录 ”按钮。 – 访客权限已激活：
此时，“ Anonymous ”用户已激活并且具有“ 读取驱动数据或确认事件 ”权限。 对应的对话框打开。 –
访客权限未激活：
此时，“ Anonymous ”用户不会激活，或者虽然激活但不具有“ 读取驱动数据或确认事 件 ”权限。
“ 需要登录 ”页面显示。 2. 输入用户名和密码。 3. 点击“ 登录 ”。 结果
正确输入登录数据后，便成功登录。 变频器数据和功能的显示取决于分配给用户账号的访问权限。

切换用户 简介 如果以下功能之一处于活动状态，则无法切换用户： 快速调试 Safety
Integrated 调试 控制面板 固件更新 备份或恢复 前提条件 UMAC 已激活。 您已登录网络服务器。
操作步骤 1. 在状态栏中，点击登录用户的名称。 将弹出一个下拉列表。 2. 选择“ 切换用户 ”选项 。
登录对话框打开。 3. 输入用户名和密码。 4. 点击“ 登录 ”。 结果
如果您的用户账号无权访问最后显示的功能视图，则会显示网络服务器首页。 注销用户 概述
如果以下功能之一处于活动状态，则用户无法注销： 快速调试 安全调试 控制面板 固件更新 备份或恢复
前提条件 UMAC 已激活。 您已登录网络服务器。 操作步骤 1. 在状态栏中，点击登录用户的名称。
将弹出一个下拉列表。 2. 选择“ 注销 ”选项 。 如果您对配置进行了更改，则会出现提示“ 保存更改 ”。
3. 点击“ 保存 ”确认或注销而不保存。 更改自己的用户密码 简介
已激活用户账号的用户可以随时自行更改密码。但用户名只能由具有“ 管理用户和角色 ”权
限的用户更改。
激活密码定期修改后，用户需要按设定的时间间隔修改密码。如果密码已过期，将在用户下
次登录时提示更新密码。 前提条件 需要有一个有效的用户账号，以访问网络服务器和变频器。
操作步骤 1. 在网络服务器首页右上角点击用户账号名称。 将弹出一个下拉列表。
如果密码已过期，将显示“ 密码已过期 ”密码对话框。然后按照第 3 步中的说明进行操作。 2.
选择“ 更改密码 ”选项 。 弹出“ 更改密码 ”对话框。 3. 输入旧密码。4. 输入新密码。 5.
再次输入该新密码。 6. 按下“ 确定 ”确认输入。 7. 点击 ，掉电保存设置。
如果启用了“ 自动保存 ”功能，则不会显示保存图标。 结果 密码已更改。 端口和协议
激活/禁用端口和协议 简介
在“ 端口和协议 ”功能视图中配置用于访问变频器的接口。此处遵循按需使用功能的原则，
关闭在访问变频器时不需要的协议。
有关设置端口和协议的详细信息以及出厂设置请查看“ 端口和协议的最低功能 (页 72) ”一章。 前提条件
已作为具有“ 编辑设备配置和驱动应用 ”权限的用户登录。 操作步骤 1. 调用“ 保护 & 安全 ”功能视图。
“ 端口和协议 ”下拉列表默认展开。 2. 配置用于访问变频器的接口。 3. 点击 ，掉电保存设置。
如果启用了“ 自动保存 ”功能，则不会显示保存图标。 结果 设置保存在变频器中。
如果已禁用访问变频器的接口，会自动从变频器注销。通过激活的接口登录网络服务器。

基本信息 简介 在操作单元与网络服务器建立受保护的 HTTPS
连接时，必须具有一份有效证书。该证书在 变频器中自动生成。 证书类型
下表概括显示了使用的证书及其特点。 证书类型 说明 HTTPS 证书 首次调用网络服务器时自动生成。
包含用于通讯的接口 IP 地址。 – 更改 IP 地址时： 如果接口的 IP 地址在调试期间或之后发生更改，则
HTTPS 证书将失效。重新调 用网络服务器时，HTTPS 证书会自动替换为新的 HTTPS 证书。
根证书（Root CA） 指可信的根证书颁发机构签发的证书 该证书用于签发 HTTPS 证书。 有效期： 2199
天 – 证书过期后的响应： 当证书过期后，需要创建新的根证书（Root CA）。该证书在建立 HTTPS
连接时 使用，用于签发新的 HTTPS 证书。客户端要再次信任该证书，才能建立受保护的 HTTPS
连接。按以下章节的步骤操作：“ 与网络服务器建立受保护的 HTTPS 连接 (页 179) ”。 证书属性
证书包含了以下有关颁发者的信息。 属性 含义 示例 O 组织 西门子 C 国家/地区 ZH CN 常用名称
SINAMICS Embedded Issuing CA, 序列号=OU 组织单位 Copyright (C) SIEMENS AG 2022 All rights
reservedHTTPS 连接不安全时的安全警告
浏览器会将自动生成的服务器证书归类为不受信任的证书，在调用 HTTPS 连接时显示一条
安全警告。有关如何处理该安全警告的说明可查看章节“ 与网络服务器建立受保护的 HTTPS 连接

(页 179) ”。 证书管理 下表列出了主流浏览器和 Microsoft Windows
系统的证书管理功能结合使用时的一些重要特 性： 浏览器 1) 版本 引擎 证书管理 Google Chrome 版本 83
及以上 Chromium 基于 Chromium 的浏览器会访问 Microsoft Windows 系统证 书库中的证书。 Microsoft
Edge 版本 88 及以上 Mozilla Firefox 版本 91 及以上 Geko Mozilla Firefox
有自己的集成在浏览器中的证书管理功能。 1) 建议使用各浏览器的最新版本。
与网络服务器建立受保护的 HTTPS 连接 前提条件 变频器和操作单元相互连接。 可以在 “ 保护 &
安全 ” 功能视图中查看 X127 和 X150 接口的设置。 首次通过 HTTPS 连接调用网络服务器。
具备操作单元的管理员权限。 需要具备管理员权限才能更改 Microsoft Windows 系统的证书库。
操作步骤 1. 在操作单元中打开浏览器。在本示例中使用 Google Chrome 浏览器。 2. 通过变频器的 IP
地址调用网络服务器，例如：https://169.254.11.22。 浏览器将 HTTPS 连接归类为不安全的连接。6.
点击 “ 下一步 ”。 “ 欢迎使用安全向导 ” 页面显示。提供下列选项： – “ 配置安全设置 ”：
推荐采用该设置，提供全面保护。 – “ 继续使用低等级安全设置 ”：
如果选择 “ 继续使用低等级安全设置 ” 选项，变频器将在没有 UMAC 设置的情况下运
行。用户无需身份验证即可访问变频器数据和功能。 可以稍后通过 “ 保护 &
安全 ” 功能视图调用安全向导并进行所需的安全设置。 7.
选择了 “ 配置安全设置 ” 选项时，按照 “ 配置安全向导中的设置 (页 154) ” 章节描述的步骤操
作。然后调用 “ 保护 & 安全 ” 功能视图。 8.
如果选择了 “ 继续使用低等级安全设置 ” 选项，在点击 “ 下一步 ” 确认消息后会显示 “ 保护 &
安全 ” 功能视图。 9. 打开下拉列表 “ 证书 ”。 所显示的信息不可编辑。
10.点击 “ 向操作设备下载证书 ”。
“ ROOT_CERT.DER ” 被下载到操作单元的下载文件夹中。文件显示在浏览器的下载栏中。
11.可选：将文件移动到操作单元上的所需文件夹中。 选择一个所有本地用户都可以访问的文件夹。
12.直接从浏览器的下载栏打开文件。 显示证书信息。 13.可选：打开保存 "ROOT_CERT.DER"
文件的文件夹并双击该文件。 显示证书信息。 14.点击 “ 安装证书 ”。 显示 “ 证书导入向导 ”。
“ 当前用户 ” 选项被选中。 15.点击 “ 下一步 ”。 16.选择 “ 将所有证书保存在以下库中 ” 选项。
17.点击 “ 浏览 ”。 18.从证书库列表中选择 “ 受信任的根证书颁发机构 ” 库，然后点击 “ 确定 ”。