

SIEMENS西门子 S-1FL2高惯量型电机 1FL2310-2AC01-1HB0

产品名称	SIEMENS西门子 S-1FL2高惯量型电机 1FL2310-2AC01-1HB0
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

禁用 Startdrive 项目的 UMAC 功能说明 项目保护是 TIA Portal 用户管理和访问控制 (UMAC) 的一部分。在 TIA Portal 中，一旦为某个 Startdrive 项目激活了项目保护，便无法禁用该保护。恢复 Startdrive 项目的 UMAC 配置 功能说明 Startdrive 项目中的 UMAC 配置是项目的一部分，无法传送到另一个项目中。配置访问 简介 驱动器提供了用户管理和访问控制 (UMAC) 功能。利用该功能可以为驱动创建并管理用户账号和角色。“角色”捆绑了对驱动的不同访问权限。不同的用户可通过“角色”被授予不同的功能和数据访问权限。注意，驱动上激活的用户管理和访问控制完全独立于 TIA Portal 项目中激活的用户管理和访问控制。但也可以在 TIA Portal 项目为特定驱动激活用户管理和访问控制，然后通过下载将它传送到驱动中。功能说明 针对驱动访问有以下配置选项：设置 / 功能 说明 密码复杂度 默认配置 激活 默认设置 最短密码长度：8 个字符 数字字符最少数目 (0-9)：1 特殊字符最少数目：0 至少一个大写字母和一个小写字母：是 可配置性 可为除“Anonymous”用户以外的所有用户账号全局配置设置。权限 每个具有“管理用户和角色”功能权限的用户 有效值 最短密码长度：8 至 32 个字符 数字字符最少数目 (0-9)：0 至 32 特殊字符最少数目：0 至 32 至少一个大写字母和一个小写字母：是/否 建议 我们建议设置至少含 12 个字符的复杂密码。安全功能 8.3 用户管理和访问控制 (UMAC) 工业网络安全 配置手册, 03/2024, FW V6.3, A5E52484547F AC 59 设置 / 功能 说明 防止重复使用的 当前已使用的密 码个数：默认配置 始终激活 默认设置 5 可配置性 可为除“Anonymous”用户以外的所有用户账号全局 配置设置。权限 每个具有“管理用户和角色”功能权限的用户 有效值 1 至 10 密码时效 默认配置 未激活 默认设置 功能激活后的预设值如下：密码有效期限：60 天 密码修改提醒周期：7 天 可配置性 可为除“Anonymous”用户以外的所有用户账号全局配置设置。权限 每个具有“管理用户和角色”功能权限的用户 有效值 密码有效期限：1 到 365 天 密码修改提醒周期：0 到 365 天 隐藏密码 设定或查询登录数据时，密码显示为模糊处理。要检查输入，用户可以通过点击眼睛图标以简明文本形式查看输入。登录失败时的反馈

反馈不会指出，在登录失败时是密码错误还是用户名错误。登录失败时的响应 登录失败后，在 3 秒内会禁止用户通过相同连接再次登录。登录数据的传输 默认情况下，HTTPS 通讯激活，用于在变频器和网络服务器之间进行数据传输。此时，登录数据会通过 HTTPS 连接以受保护的方式传输。但如果使用可选的 HTTP 传输协议，登录数据将不受保护地传输。这会导致登录数据更容易被窥探。变频器和 Startdrive 之间的数据通过“安全的 S7 协议 Startdrive”以受保护的方式传输。安全功能 8.3 用户管理和访问控制 (UMAC) 工业网络安全 60 配置手册, 03/2024, FW V6.3, A5E52484547F AC 设置 / 功能说明 无活动时会话超时/实时固件超时 默认设置 Anonymous:从不除 "Anonymous" 以外的任何用户：30 分钟 可配置性 可为除 "Anonymous" 用户以外的所有用户账号单独配置设置。权限 每个具有“管理用户和角色”功能权限的用户 有效值 1 到 600 分钟 无活动时会话超时/实时固件超时只针对网络服务器连接，不针对 Startdrive 连接。如果用户的无活动状态超过设置的时间，该用户将自动注销。在此之前，系统会通知用户即将注销。

即将注销的通知时间不可配置。默认情况下设置以下时间：如果设置的超时时间 10 分钟，则为 5 分钟 如果设置的超时时间 3 分钟但 < 10 分钟，则为 1 分钟 如果设置的超时时间 < 3 分钟，无消息 在以下情况下会暂停会话超时：

当进程比较长时，例如：固件更新。进程结束后恢复。

当控制面板被激活时无身份验证、无权限检查的访问 功能说明

在以下情形下，访问不会经过身份验证和权限检查：“Anonymous”用户通过现场总线协议访问：- PROFINET、EtherNet/IP 和 Modbus TCP 循环通讯期间 - 通过 DCP 读访问时

关于通过现场总线协议访问的更多信息，可查看章节“通过现场总线协议访问变频器时的扩展角色 (页 69)”。 “Anonymous”用户通过 SINAMICS SDI Standard 面板访问

关于通过现场总线协议访问的更多信息，可查看章节“通过 SINAMICS SDI Standard 面板

访问变频器时的扩展角色 (页 71)”。插入存储卡上电时：无论 UMAC

设置如何配置，存储卡上的文件都会传送到变频器中。

管理员简介

在本文档中，管理员分为“项目经理”和“驱动管理员”两种。驱动管理员是具有“Drive Administrator”角色的用户。可配置性 属性说明 用户账号 该用户账号在 UMAC 配置过程中创建和激活。用户名 该用户账号的用户名在 UMAC 配置过程中确定。密码 该用户账号的密码在 UMAC 配置过程中确定。无论何种情况，至少都要有一个具有“管理用户和角色”权限的用户（“Anonymous”除外）激活。因此，UMAC

激活时，具有“管理用户和角色”权限的最后一个用户无法删除。无需身份验证的用户 简介

“Anonymous”用户无需身份验证即可开展访问。一些通讯协议不支持身份验证。在通过此类协议访问驱动时，“Anonymous”是在访问控制功能中唯一可使用的用户。

关于不支持身份验证的通讯协议的更多信息，可查看章节“端口和协议的最低功能 (页 72)”。可配置性 属性说明 用户账号 具有“管理用户和角色”功能权限的用户可以激活/禁用该用户。默认

情况下，该用户账号处于激活状态。该用户帐户无法删除，但可以在用户管理中停用。用户名

该用户账号的“用户名”无法配置。密码 该用户不需要密码，也不需要进行身份验证。

角色和功能权限 该用户账号默认分配到“Drive Ext. Role Fieldbus”和“Drive Ext. Role SDI Standard/Adv”角色。角色和权限的标准配置

使用默认设置运行安全向导后，“Anonymous”用户具有以下角色：Drive Ext. Role Fieldbus

关于通过现场总线协议访问时权限的更多信息，可查看章节“通过现场总线协议访问变

频器时的扩展角色 (页 69)”。Drive Ext. Role SDI Standard/Adv 关于通过 SINAMICS SDI Standard 面板访问时权限的更多信息，可查看章节“通过 SINAMICS SDI Standard

面板访问变频器时的扩展角色 (页 71)”。扩大或缩小权限 说明

我们建议，在信息安全风险评估中检查为“Anonymous”用户分配的权限是否适宜，并采取风险评估得出的措施。某些功能，例如非循环现场总线通讯，需要使用“Anonymous”用户。由于该用户无需身份

验证即可访问变频器，会增加未经授权访问的攻击范围。激活了“Anonymous”用户后，安全性

就会降低到授予该用户权限的程度。设置 最大角色数量 针对对应变频器具有实时固件功能

权限的自定义角色的最大数量 除了具有实时固件功能权限的系统定义角色外，最多

可以针对对应变频器创建和配置 20 个具有实时固件功能权限的自定义角色。每个用户的最大角色数量

针对对应变频器，可以为一个用户分配最多 10 个具有实时固件功能权限的角色。Startdrive 中的验证将离线设置载入变频器时，会检查含用户配置在内的 UMAC 设置。如果一个或多个用户的配置不符合规则，则会显示相应的消息。Startdrive 和网络服务器之间的关系 将包括 UMAC 设置在内的离线设置加载到变频器上时，Startdrive 会访问与网络服务器相同的用户数据库。因此，Startdrive 中用户的配置必须符合上述规定。

尤其是可以创建和配置的用户最大数量。示例 如果在 Startdrive 中已配置 64 个对相应变频器有访问权限的用户，则在将离线设置加载到

变频器中后无法再在网络服务器中创建更多用户。禁用驱动的 UMAC 功能说明 激活驱动的 UMAC 配置后，便无法再禁用该功能。更改/删除 UMAC 配置 功能说明 在以下情形下驱动中的 UMAC 配置会被更改/删除：将 UMAC 配置载入驱动 固件降级 完全复位所有设备设置到出厂设置 更多信息可查看章节“删除变频器上的客户数据 (页 87)”。

从加密的备份文件恢复变频器设置恢复驱动的 UMAC 配置 功能说明 UMAC

设置是驱动配置的一部分，和所有其他项目数据一同备份并恢复。数据的备份和恢复方式有：Startdrive、网络服务器或存储卡。如果驱动是通过 Startdrive 配置的，在下载时会覆盖该驱动的数据。Startdrive 中具有工程配置功能权限的角色 简介 在 Startdrive

中，对功能的访问是通过权限控制的，通常情况下，这些权限整合为系统定义的角色。

在执行用户操作之前，Startdrive 会检查用户的权限（假设已启用项目保护）。缺少对应权限时便显示对应的消息。“Engineering-Administrator”角色 角色为“Engineering-

Administrator”的用户拥有“管理用户和角色”的权限。具有“管理用

户和角色”权限的用户可以创建更多用户，并根据需要以任意组合为该用户分配角色。

角色和权限的对应关系 软件默认提供以下系统定义的角色。