西门子全国工业开关经销商

产品名称	西门子全国工业开关经销商
公司名称	浔之漫智控技术（上海）有限公司-西门子模组
价格	.00/件
规格参数	PLC:授权代理
公司地址	213室
联系电话	13817547326

产品详情

西门子全国工业开关经销商

工控机等工业自动化的设计、技术开发、项目选型安装调试等相关服务。西门子中国有限公司授权合作伙伴——浔之漫智控技术(上海)有限公司，作为西门子中国有限公司授权合作伙伴，浔之漫智控技术（上海）有限公司代理经销西门子产品供应全国，西门子工控设备包括S7-200SMART、S7-200CN、S7-300、S7-400、S7-1200、S7-1500、S7-ET200SP 等各类工业自动化产品。公司国际化工业自动化科技产品供应商，是专业从事工业自动化控制系统、机电一体化装备和信息化软件系统

集成和硬件维护服务的综合性企业。西部科技园，东边是松江大学城，西边和全球**芯片制造商台积电毗邻，作为西门子授权代理商，西门子模块代理商，西门子一级代理商，西门子PLC代理商，西门子PLC模块代理商，

，建立现代化仓

储基地、积累充足的产品储备、引入万余款各式工业自动化科技产品与此同时，我们

向北5公里是佘山国家旅游度假区。轨道交通9号线、沪杭高速公路、同三国道、松闵路等

交通主干道将松江工业区与上海市内外连接，交通十分便利。

建立现代化仓

储基地、积累充足的产品储备、引入万余款各式工业自动化科技产品，我们以持续的卓越与服务，取得了年销

售额10亿元的佳绩，凭高满意的服务赢得了社会各界的好评及青睐。与西门子品牌合作，只为能给中国的客户提供值得信赖的服务体系，我们

的业务范围涉及工业自动化科技产品的设计开发、技术服务、安装调试、销售及配套服务领域。

菜单命令 SCT：“ 选项 > 用户管理 ”(Options > User management)，“ 角色 ”(Roles)
选项卡，“ 属性... ”(Properties...) 或“ 添加... ”(Add...) 按钮。 STEP 7 菜单命令：“ 用户 >
启动用户管理 ”(Users > Start of user administration)，“ 运行 ”(Run)
按钮。也可以从各个选项卡中调用用户管理。 创建并分配用户自定义角色 1. 输入角色名称。 2.
从权限模板中选择一个系统定义的角色（默认值：“ 诊断 ”）。选择中不显示用户自定义 角色。
结果：根据所选角色，项目中使用的每个安全模块的权限都显示在权限列表中。项目
中未使用的安全模块的权限呈灰显状态。 3.
对于每个安全模块，启用或禁止要分配给用户自定义角色的权限。 4.
根据需要为要创建的角色输入注释和*长会话时间。 5. 单击“ 应用 ”(Apply)
按钮可保存所选内容，也可以单击“ 确定 ”(OK) 保存并关闭窗口。 6. 将角色分配给用户。
复制安全模块的角色权限 在安全模块的快捷键菜单中，选择“ 复制权限 ”(Copy rights)
命令并使用“ 粘贴权限 ”(Paste rights) 命令将这些权限分配给其它模块。组态权限 administrator standard diagnostics 诊断安全 x x x 组态安全 x x - 管理用户和角色 x - - X 启用权限 - 禁用权限 模块权限
“ 服务 ”(Service) 列显示受特定权限影响的系统。 根据角色类型，为每个安全模块提供下列模块权限以供选择：为了能够使用该功能，还必须启用模块权限“ Web：访问 Web 诊断和 CP 文件系统 ”(Web: Access web diagnostics and CP file system)。 ** 为了能够使用该功能，还必须启用模块权限“ FTP：从 CP 文件系统读取文件 ”(FTP: Read files from CP file system)。 ***
为了能够使用该功能，还必须启用模块权限“ FTP：将文件写入 CP 文件系统 ”(FTP: Write files to CP file system)。 **** 要能够使用该功能，也必须启用组态权限“ 诊断安全 ”(Diagnose security)。在创建安全模块前后设置模块权限
在用户自定义的角色中，每个安全模块的模块权限是单独定义的。如果在创建安全模块后
添加角色，并且其模块权限将在相应角色内加以定义，则此安全模块的模块权限会根据所
选的权限模板自动完成设置，并在必要时可以进行调整。如果在创建角色后添加安全模块，则 SCT
不会设置任何权限。在这种情况下，需要自行设置安全模块的所有模块权限。
还可以通过复制将现有模块权限传送至另一安全模块，必要时再进行调整。为此，可在模
块权限的快捷菜单中选择任一安全模块，然后选择“ 复制权限 ”(Copy rights) 或“ 粘贴权限 ”(Paste rights) 菜单命令。组态密码策略 含义 使用密码策略可以规定给新用户分配密码时需要考虑的规范。
如何访问此功能 选择菜单命令“ 选项 > 用户管理... ”(Options > User management...)，“ 密码策略 ”(Password policies) 选项卡。
选中一个复选框后，将激活相应的策略，必要时可以通过相关输入框加以调整。 参数 含义 *短密码长度 要求密码含有的*少字符数。 默认会选中相应复选框且无法禁用。 *小值： 8 个字符 *大值： 32 个字符 *少数字个数 要求密码含有的*少数字个数。 *小值： 1 个数字 *大值： 32 个数字 *少特殊字符数 要求密码含有的*少特殊字符数。 特殊字符是指非字母或数字的任意字符。 *小值： 1 个特殊字符 *大值： 32 个特殊字符 不能再使用的密码个数 在*近使用的密码中，不能用作新密码以更改密码的个数。 *小值： 1 个密码 *大值： 10 个密码 至少有一个大写和一个小写字符
如果选择此复选框，则密码必须包含至少一个大写 字母和一个小写字母。RADIUS（Remote Authentication Dial-In User
Service，拨入用户远程认证服务）是通过集中存储用户数据的服务器来验证用户的协议 。 使用 RADIUS 服务器可以进一步保护用户名称、已分配的角色以及密码。 使用 RADIUS 服务器的情形
可在激活用户特定的 IP 规则集时执行通过 RADIUS 服务器进行验证以上显示的网络布局只是一个示例。 RADIUS 服务器还可以位于安全模块的内部网络或 DMZ 网络中。 下文介绍组态选项时，已假定 RADIUS 服务器在 SCT 中组态，并已分配给相关的安全模块。
除此以外，还必须对一个用户或角色组态了“ RADIUS ”验证方法。
有关详细信息，请参见以下各部分： ● 定义 RADIUS 服务器 (页 93) ● 将 RADIUS 服务器分配给安全模块 (页 94) ● 创建用户 (Create users) (页 79) ● 创建角色 (页 80) 有关用户特定 IP 规则集的一般信息，请参见以下部分： ● 用户特定的 IP 规则集 (页 171)要使用 RADIUS 服务器验证用户，有两个组态选项可供使用： ●
用户和用户角色对于安全模块而言是已知的，只有用户密码在 RADIUS 服务器上管理。 用户和密码在 RADIUS 服务器上组态。 – 组态使用“ RADIUS ”验证方法的用户。 – 将该用户分配给用户特定的 IP 规则集。 结果： – 用户登录安全模块的 Web 页面时，验证查询会转发至 RADIUS 服务器。 – RADIUS 服务器执行密码检查并将结果发送回安全模块。 – 如果成功通过了密码检查，用户特定的 IP

规则集会激活。 ● 角色对于安全模块而言是已知的，用户管理通过 RADIUS 服务器进行。
用户和密码在 RADIUS 服务器上组态。 – 将用户自定义的角色或系统定义的角色分配给用户特定的 IP 规则集。 – 在安全模块的“ RADIUS ”选项卡中，启用“ 允许 RADIUS 验证非组态用户 ”(Allow RADIUS authentication of non-configured users) 和“ 验证需要过滤器 ID ”(Filter ID is required for authentication) 复选框。 结果： – 用户登录到安全模块的 Web 页面时，验证和授权查询会转发至 RADIUS 服务器。 – RADIUS 服务器执行密码检查并将结果发送回安全模块。 – 情况 a： 如果在 RADIUS 服务器上也组态了此角色名称： RADIUS 服务器会将已分配给用户的角色名称返回给安全模块。 – 情况 b： 如果未在 RADIUS 服务器上组态该角色名称： 安全模块会给用户分配系统定义的角色“ radius ”。 – 如果成功通过了密码检查，用户特定的 IP 规则集会激活。 有关 RADIUS 服务器的约定 ● RADIUS 服务器可以位于与安全模块相连的任意网络内。 ● 每个安全模块*多可以组态两个 RADIUS 服务器。 运行期间只有一个 RADIUS 服务器处于激活状态。 ● 定义 RADIUS 服务器时，还可以使用 FQDN 取代 IP 地址