

SIEMENS西门子 CPU中央处理器 6ES7511-1AK02-0AB0

产品名称	SIEMENS西门子 CPU中央处理器 6ES7511-1AK02-0AB0
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:代理销售商 S7-1500:全新原装 假一罚十 德国:正品现货 实体经营
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

下图显示了 OPC UA 服务器的 IP 地址条目：4. 如果 OPC UA 服务器不使用标准端口 4840，则必须在此插入端口号。例如，如果要与之建立连接的 OPC UA 服务器使用该端口号，则在字段中输入数字 65535。 5. 此外，还接受会话超时（30 秒）和监视时间（5 秒）的默认设置。 设置安全参数 1. 单击“组态” (Configuration) 选项卡中的“安全” (Security) 区域。此区域包含与 OPC UA 服务器的连接的所有安全设置。可进行以下设置，例如：“常规” (General) 区域安全模式：从下拉列表中选择与 OPC UA 服务器的连接必须达到的安全模式。如果服务器不满足所选模式的要求，将不建立连接。可进行以下设置：不安全：无安全连接！签名：OPC UA 服务器和 OPC UA 客户端对数据传输进行签名（所有消息）：因此可检测到修改。签名并加密：OPC UA 服务器和 OPC UA 客户端对数据传输进行签名和加密（所有消息）：安全策略：设置将为消息签名和加密使用的加密技术。可进行以下设置：不安全要组态安全连接，必须注意以下事项：需要为客户端使用证书才能建立安全连接。需要让服务器知晓该客户端证书。相关操作步骤，请参见“处理客户端和服务证书 (页 202)”部分“OPC UA 客户端的证书”下的内容。“证书” (Certificates) 区域 客户端证书：证书确认 OPC UA 客户端的真实性。要选择证书，请单击以下符号：STEP 7 会显示证书列表。选择已让服务器知晓的证书。单击带有绿色复选标记的符号。或者创建新证书。此时，可单击“添加” (Add) 符号。如果创建新证书，必须让服务器知晓该证书。“用户认证” (User authentication) 区域 可为用户身份认证进行以下设置：访客用户名和密码用户 (TIA Portal - 安全设置) 更多信息，请参见“具有 OPC UA 功能权限的用户和角色 (页 210)”。设置语言 String 类型的 UA 变量可通过 OPC UA 进行本地化，也就是说，文本 (UA 变量的值) 能够以不同的语言形式提供给服务器。例如，本地化文本可用于 DisplayName (节点名称) 和 Description (描述)。例如，在“组态” (Configuration) 选项卡的“语言” (Languages) 区域，可通过以下操作改变服务器返回文本的语言：在“语言” (Languages) 区域中，输入连接建立期间服务器传送到客户端的语言数。在第一行中输入的语言或与之关联的本地

ID (“ 语言代码 ”) 是客户端的shouxuan语言。如果服务器能够以请求的语言提供 UA 变量，则会将该变量传送到客户端。如果服务器不能以请求的语言提供 UA 变量，则会检查能否以在第二行中输入的语言 (第一替代语言) 提供 UA 变量。服务器会逐个检查列表中的各条目，如果服务器既不能提供请求的语言，也不能提供替代语言，则将提供默认语言。S7-1500 CPU 的客户端证书处理 客户端证书来自何处？如果使用 S7-1500 CPU 的 OPC UA 客户端 (OPC UA 客户端已启用) ，则可按照以下章节中的详细介绍，使用 STEP 7 V15.1 及更高版本为这些客户端创建证书。如果使用来自制造商或 OPC 基金会的 UA 客户端，则会在安装期间或在首次调用程序时自动生成客户端证书。在 STEP 7 中，需要通过全局证书管理器导入这些证书，并在相应的 CPU 中使用。如果自行编写 OPC UA 客户端程序，则可以通过程序生成证书。也可通过工具生成证书 (如，使用 OpenSSL 或 OPC 基金会的证书生成器) ：有关使用 OpenSSL 的操作步骤，请参见此处：“用户自己生成 PKI 密钥对和证书 (页 158) ”。有关使用 OPC 基金会的证书生成器的步骤，请参见此处：“创建自签名证书 (页 157) ”。S7-1500 CPU 的 OPC UA 客户端证书仅当 OPC UA 服务器将 OPC UA 客户端证书归类为可信任证书时，服务器与客户端之间才能建立安全连接。因此，需要让服务器知晓该客户端证书。在以下章节中，将介绍最初如何为 S7-1500 CPU 的 OPC UA 客户端生成证书，并提供给服务器。

1.生成并导出客户端证书

要进行安全连接，需生成一个客户端证书，如果服务器和客户端位于不同项目中，还需要导出该证书。如果客户端和服务器位于相同项目中，则无需导出客户端以及进行后续导入。要求 CPU 的 IP 接口已组态，IP 地址可用。背景：在“主题备用名称 (SAN)” (Subject Alternative Name (SAN)) 中，输入用于访问系统中该 CPU 的 IP 地址。创建 OPC UA 客户端接口为 S7-1500 CPU 生成客户端证书的最简单方法是组态一个客户端接口。

为选择或生成客户端证书而提供的客户端接口的组态，参见“创建和组态连接 (页 292) ”。或者可按以下方法生成客户端证书：1. 在项目树中，选择将用作客户端的 CPU。2. 双击“设备组态” (Device configuration)。3. 在该 CPU 的属性中，单击“保护和安全性 > 证书管理器” (Protection & Security > Certificate manager)。4. 在“设备证书” (Device certificates) 表格中，双击“