**练习 – 启动S7-1500 OPC UA服务器**

**练习任务**:

* 基于练习 (1)
* 在此练习中，尝试将S7-1500 CPU 2.0的OPC UA服务器配置为严格的安全验证，非预定义的客户端不允许连接
* 需要安全的OPC连接
* OPC UA 服务器要设置为仅允许的客户端可以连接
* 需要验证用户名及其密码
* 只允许加密的连接目标
* 使PLC可以通过OPC访问

**目标**：

* 熟悉证书管理过程
* 属性不同的安全设置方式

**练习设计：**

系统中使用了一个CPU1511C和一个CPU1516，分别启用OPC UA服务器，使用UAExpert客户端同时连接。

由于配置服务器需要安全连接而且必须验证客户端，非验证客户端不允许连接，因此需要将UAExpert客户端的证书导入两个PLC中。

CPU1511C的IP地址设为192.168.10.21

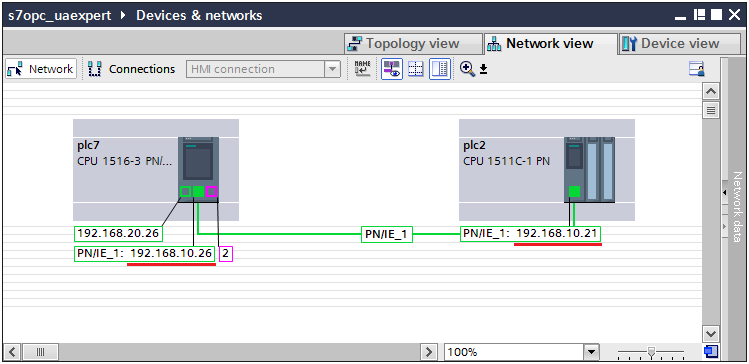
CPU1516 接口1的IP地址设为192.168.10.26

运行UAExpert的PC网卡IP地址为192.168.10.0网段

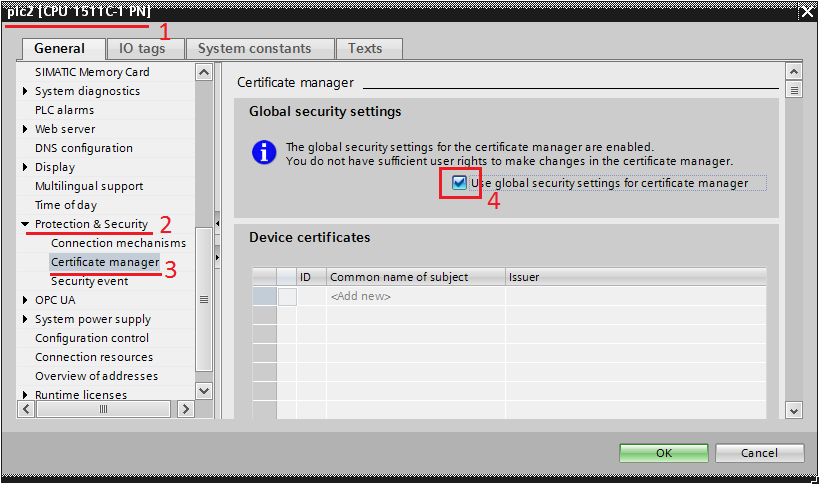
PC – CPU1511C – CPU1516连成局域网

**任务 - 步骤分解**

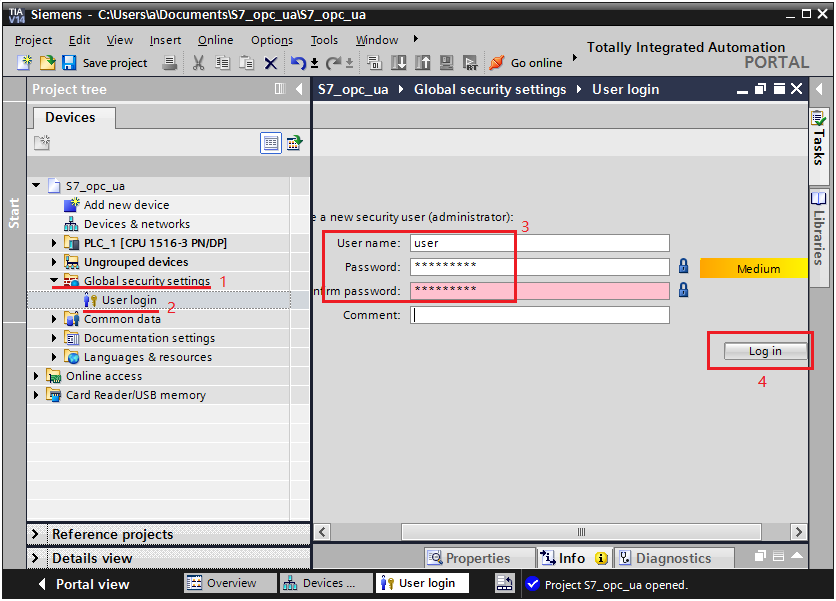
1. 在Step7 V14里配置加入两个CPU站点，IP地址如下图：



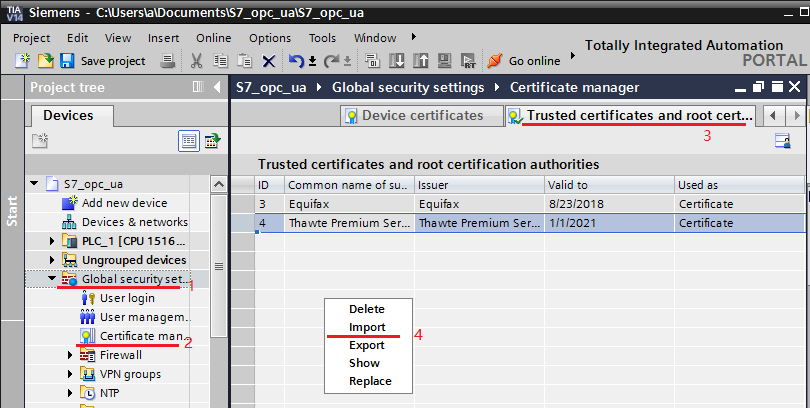
1. 在每个CPU的属性中，保护与安全 > 证书管理，启用”使用证书管理全局安全设置“，在项目中统一管理证书



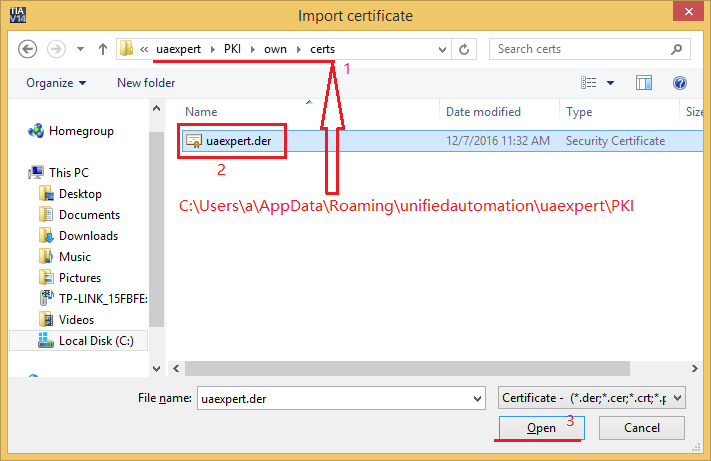
1. 在项目树的”全局安全设置 > 用户登录”，设置管理帐号与密码，然后登录



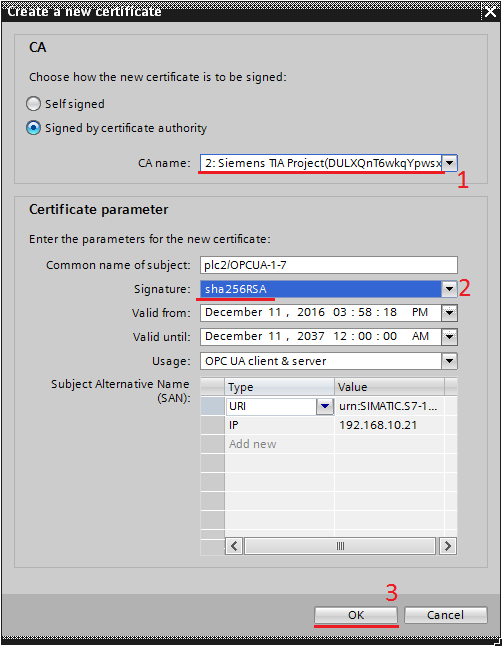
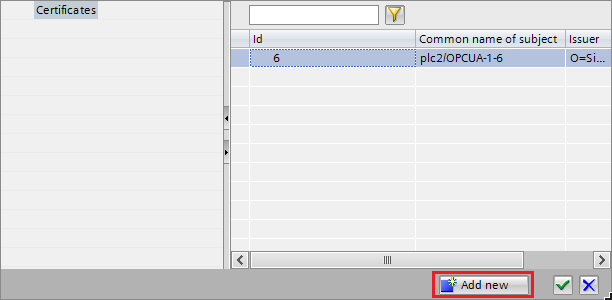
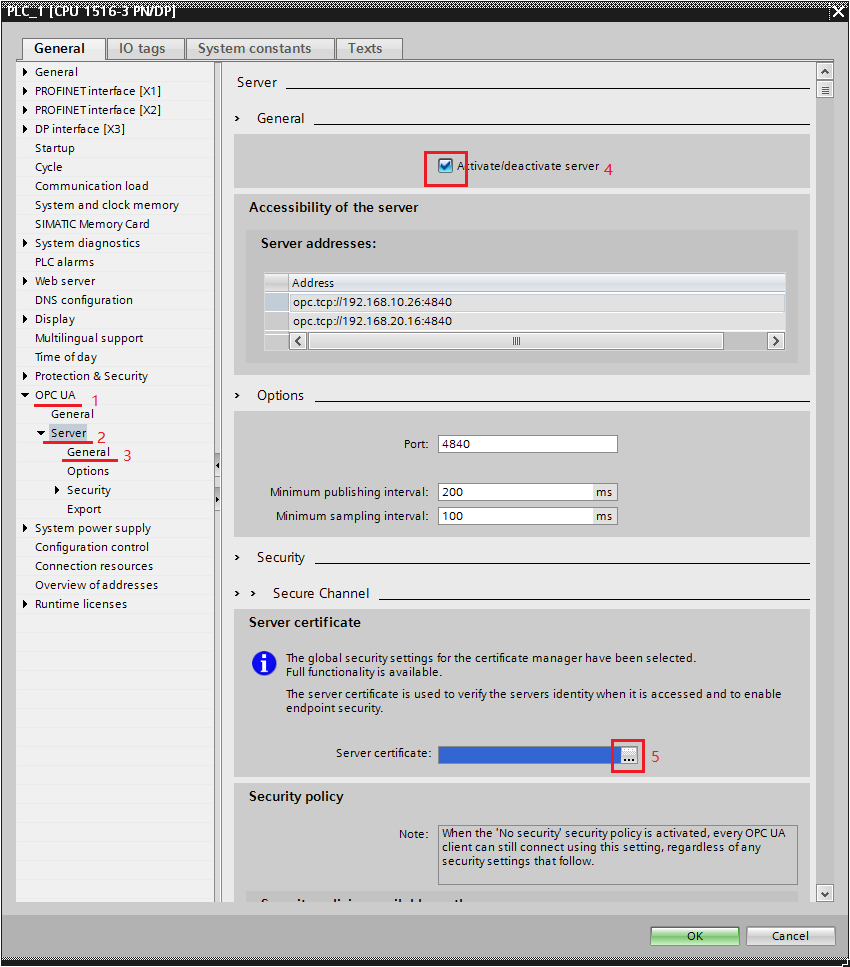
1. 导入客户端证书。在“全局安全设置 > 证书管理”> 受信任的证书与根证书，右键选”导入”



1. 在UAExpert默认安装条件下，其证书路径如下图。选中”uaexpert.der”打开，证书将导入。

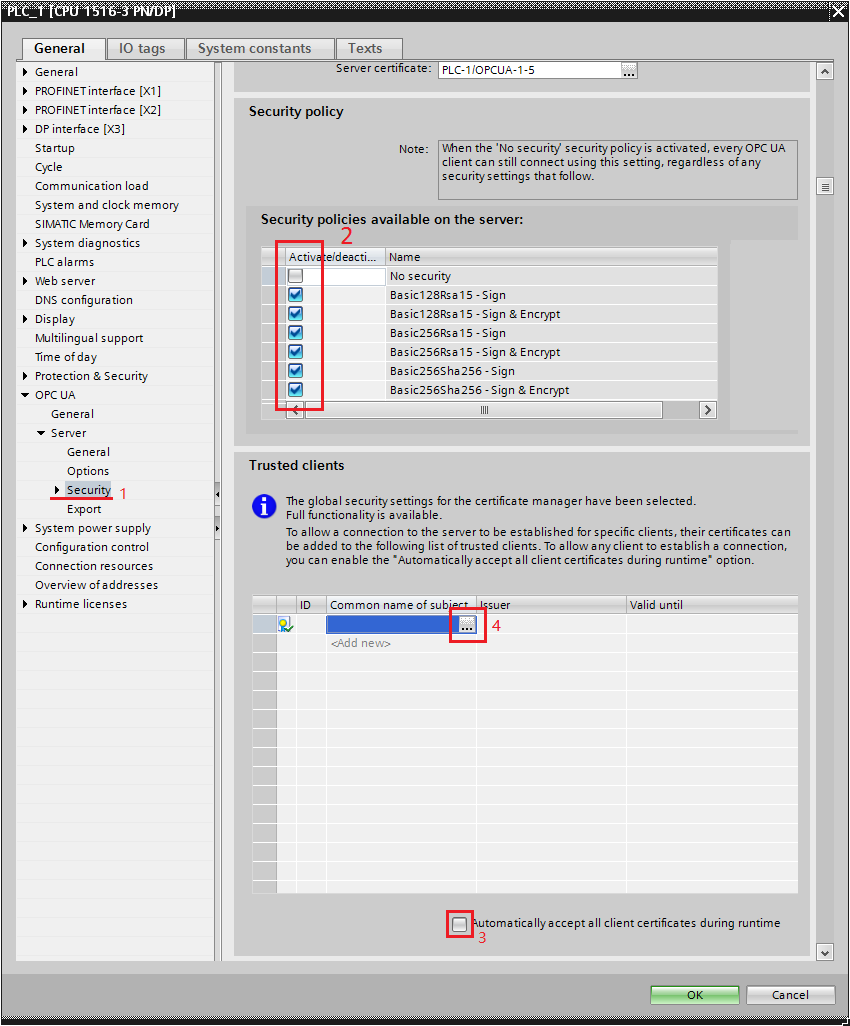


1. 在每个CPU属性中启用OPC UA服务器功能， 然后重新生成服务器证书（此练习我们使用安全性最高的Basic256Sha25策略，其他策略不是必要的步骤）：

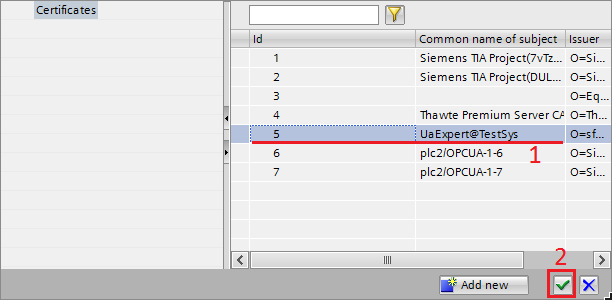


,

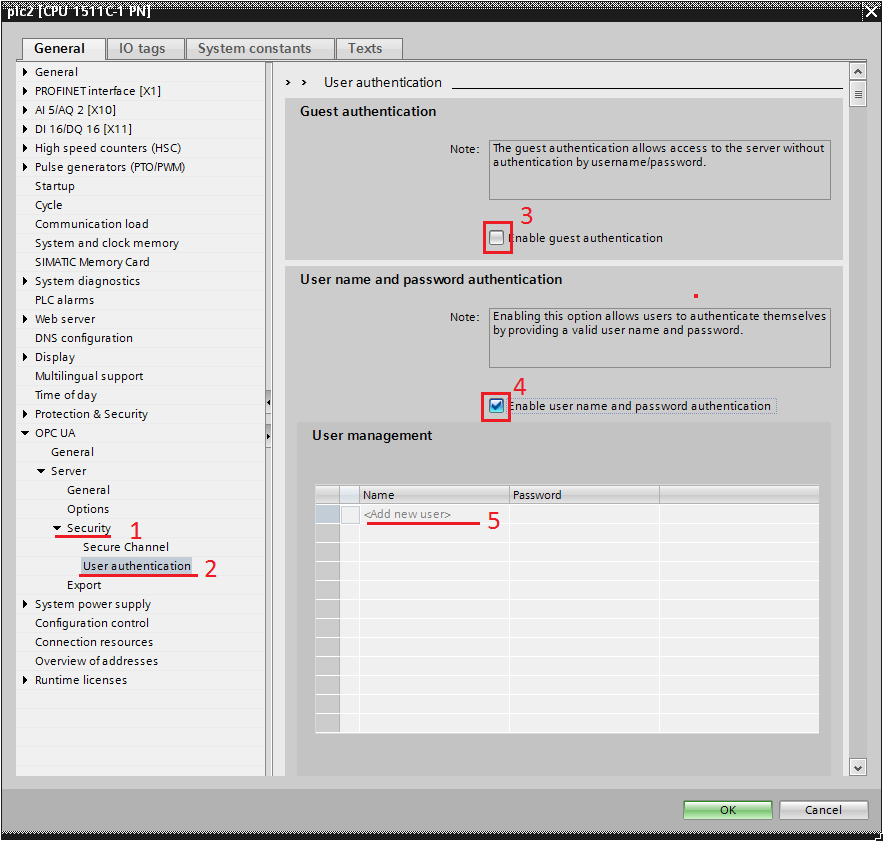
1. 安全策略禁用”No security“， 选上后面的两个”Basic256Sha256”；禁用”自动接受客户端证书”，然后导入指定的客户端证书：

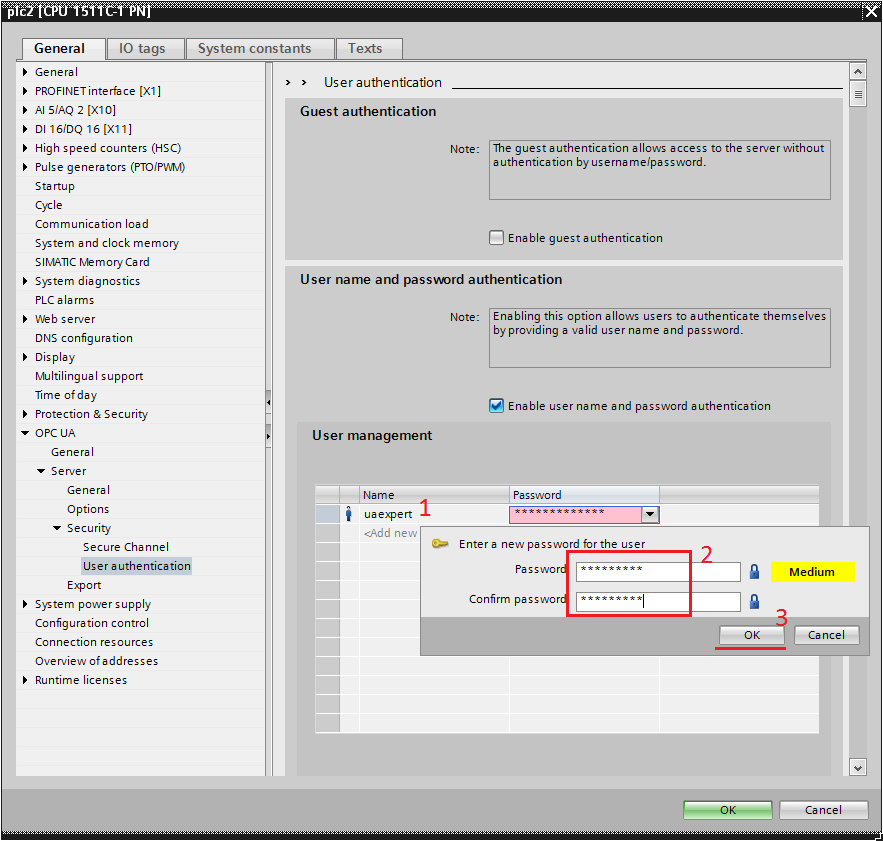


(UaExpert证书我们在前面的第4，5步在全“局安全设置 > 证书管理“中所导入)

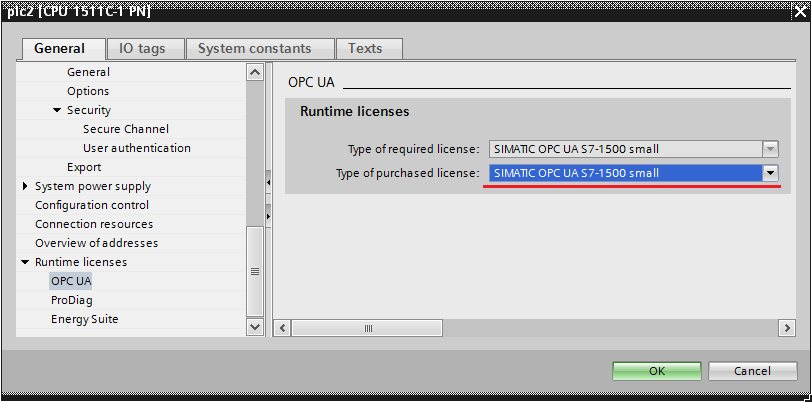


1. 在”OPC UA > 服务器 > 安全　> 用户认证”添加用于客户端连接所使用的用户名和密码：

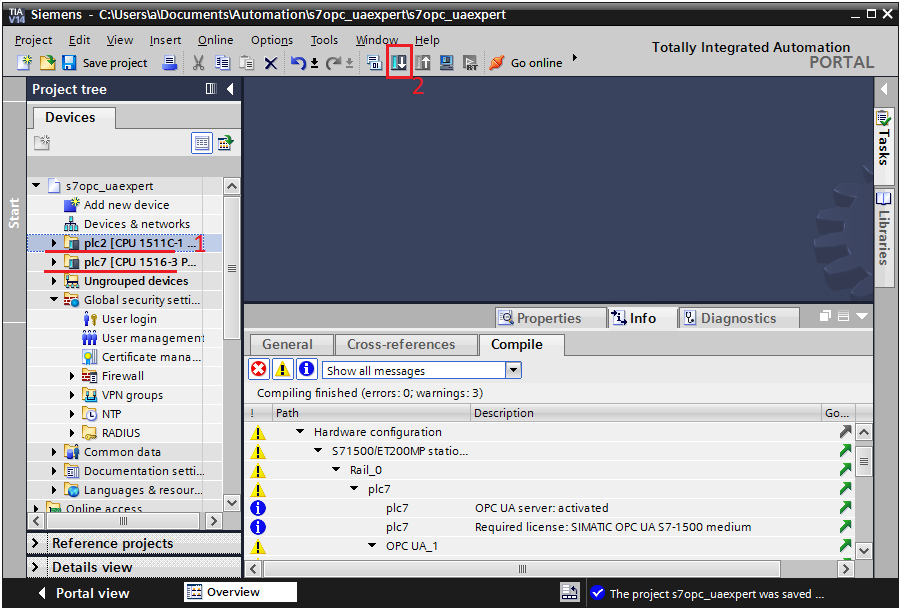




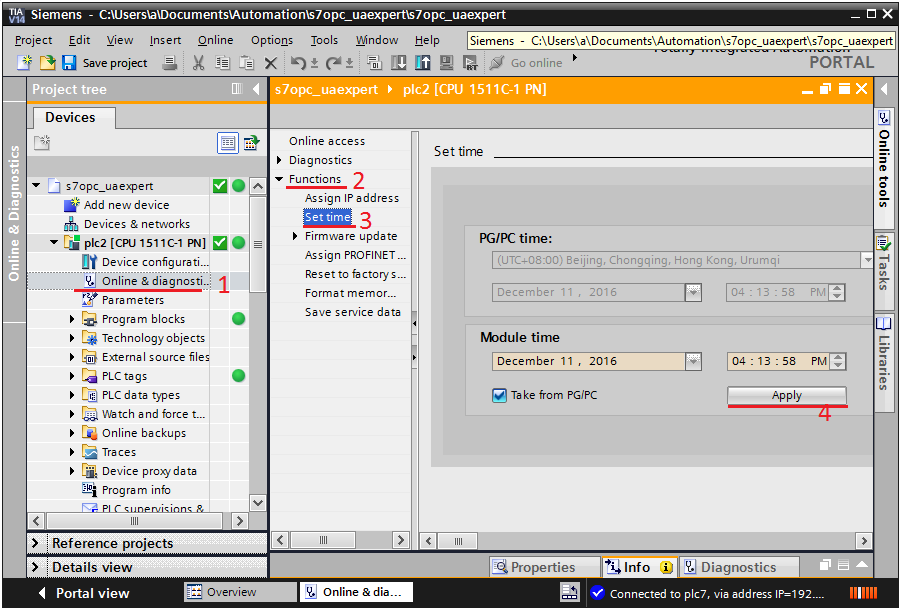
1. 在两个CPU的属性 “运行时授权 > OPC UA”中分别设置证书授权类型:



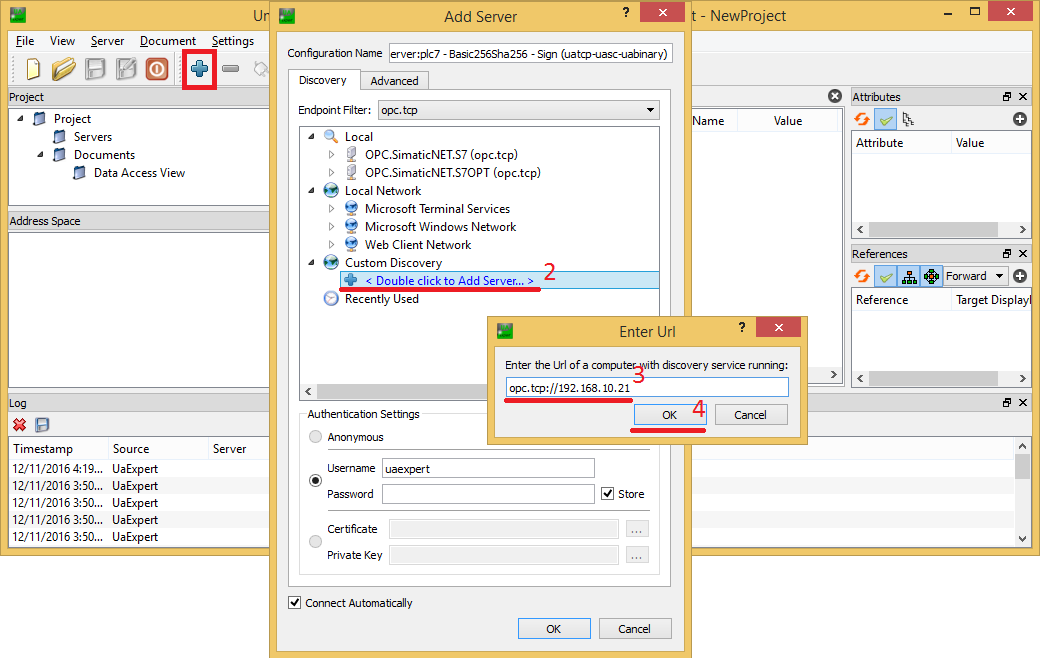
1. PLC的OPC UA服务器及其安全设置已经设完，把两个PLC站点都下载到相应的PLC中：



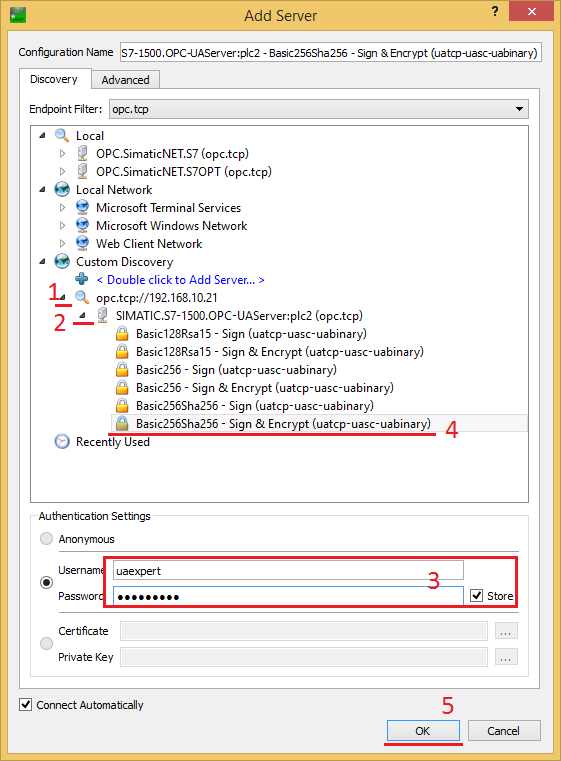
1. 项目树里，每个CPU的”在线与诊断 >功能 > 设置时间“，点应用将PLC时间与PC同步一次，作用是使各相关证书不至于超出有效时间



1. 运行UAExpert, 添加服务器，输入相应的客户端帐号密码，然后浏览服务器

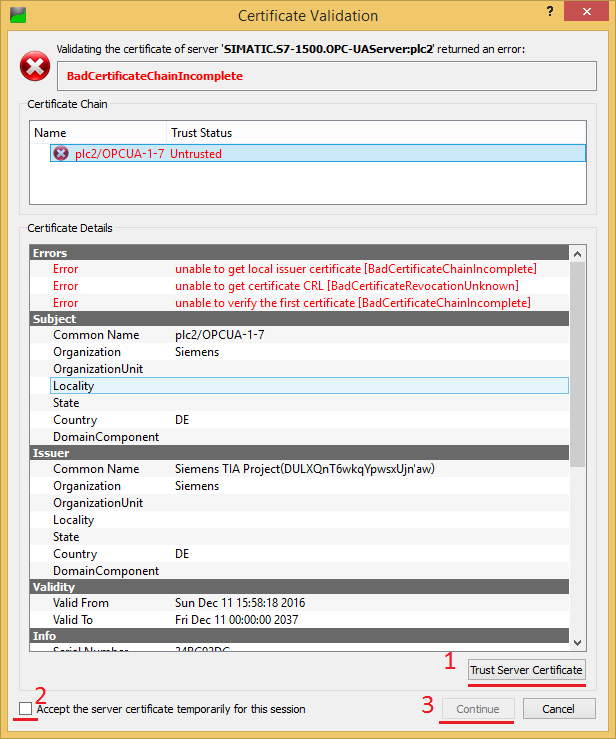


1. 选中”Basic256Sha256 - Sign”或”Basic256Sha256 – Sign & Encrypt”进行连接

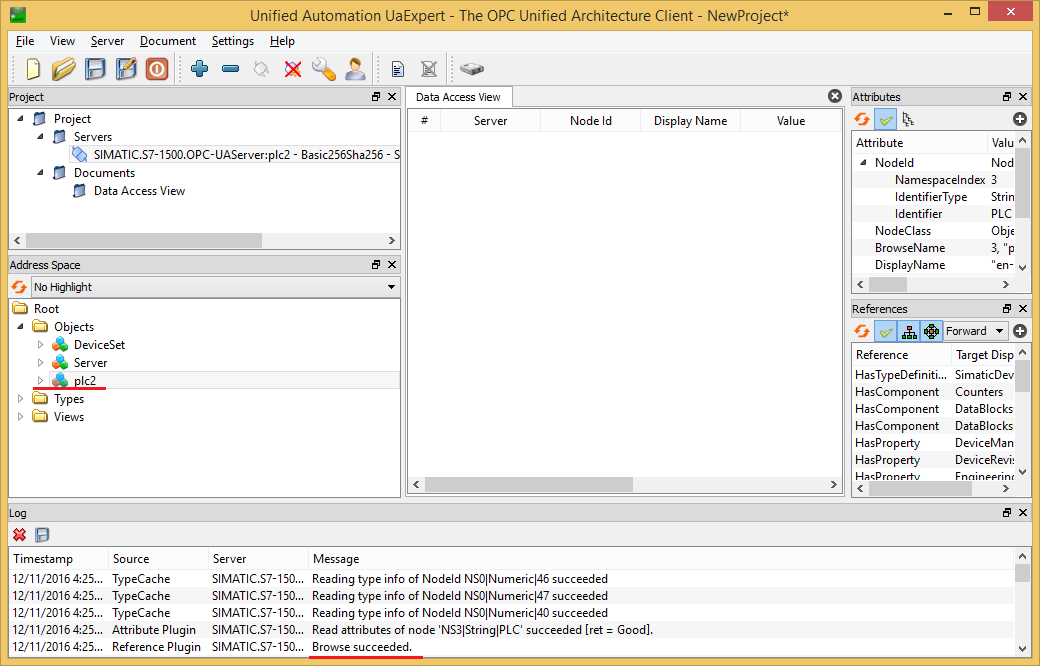


1. 弹出对话框提示消息为：是否要信任所连接的服务器证书？

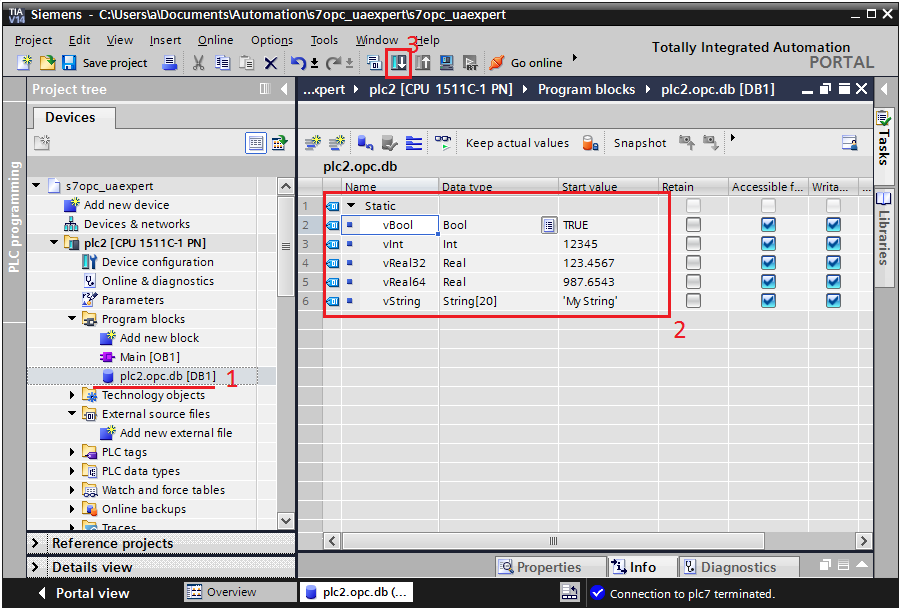
点”Trust Server Certificate, 勾选Accept the server certificate temporarily for this session, 然后”Continue”



1. 下图的状态即可认为连接可以建立的状态。



1. 在两个PLC分别加入一个DB用于客户端连接测试：



1. 在每个PLC的OPC UA服务器，浏览”Address Space”，在Plc名 > DataBlocksGlobal可以看到刚才下载的DB块，展开DB，把里面的变量拖到右侧的”Data Access View”即可订阅，Status = “Good”说明数据已经读取成功：

