SIEMENS

如何在 WINCC OA V3.12 中实现安全的 Web 访问

Getting-started	Edition (2015 年 10 月)

摘　要 在 WinCC OA V3.12 及以上版本，Web Client 的安全性能得到了很大的提升。本文介绍了实现安全 Web 访问的具体组态方法。

关键词 WinCC OA 、Web 服务器、Web 客户端、Internet、SSL、代理

Key Words WinCC OA, Web Server, Web Client, Internet, SSL, Proxy

目　录

1 实现安全的 Web 访问概述

在 WinCC OA V3.12 及以上版本，当创建新项目时，将默认增加一个管理器（Multiplexing Proxy Manager），该管理器用于实现使用 SSL 加密的安全的 Web 访问。Multiplexing Proxy 管理器负责通信的入口和出口，减少了网络服务的端口，并且代理服务器可以减轻 DoS 攻击（DoS 是 Denial of Service 的简称，即拒绝服务；造成 DoS 的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务）的影响。下图说明了 Proxy 与 Data Manager、Event Manager 和 Web Client 之间的关系：

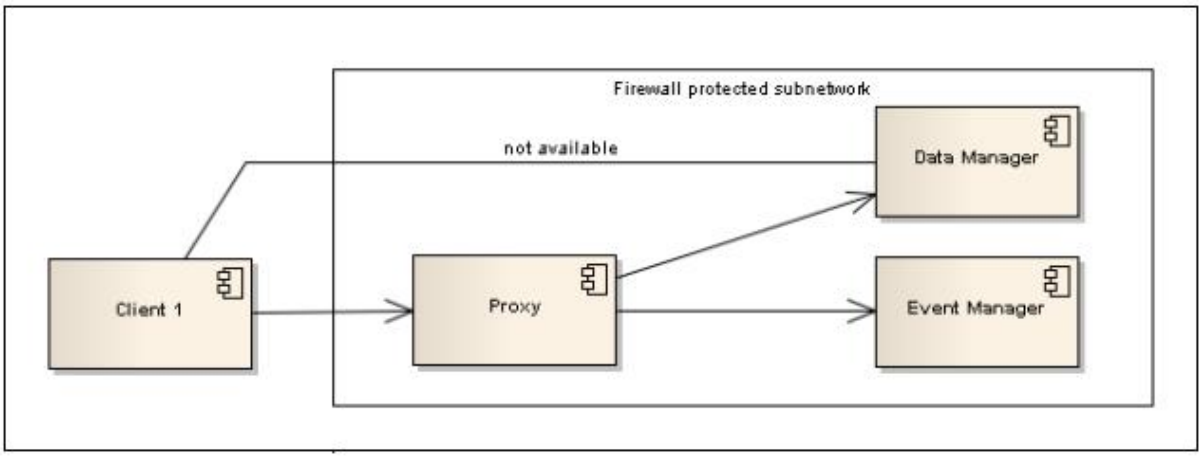

图 1 Proxy 与 Data Manager、Event Manager 和 Web Client 之间的关系

2 如何使用 Proxy 实现 Web 访问

在本示例中，将 Multiplexing Proxy 与 WinCC OA Server、Web Server 部署在同一台计算机上，该计算机的 IP 地址为“ 10.65.109.121”；WinCC OA Web Server 的外网发布地址为“ 222.128.29.196”。对于更多的配置方法，请参见帮助文档[Special functions] / [Security] / [Multiplexing Proxy] / [Configuration of the Multiplexing Proxy] 中的介绍。

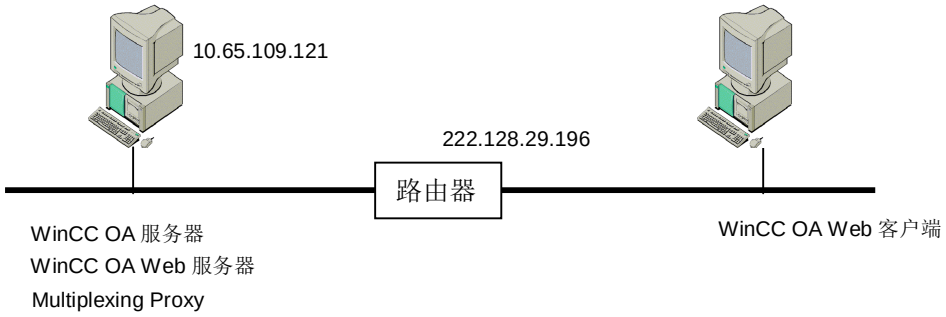

图 2：本示例的网络示意图

2.1 组态用于 Web 发布的项目

第一步：创建一个测试项目 TestWebClient，添加 Control Manager，在其 Options 选项中设置参数“ webclient_http.ctl”，并启动该 Control Manager 即启动 WinCC OA Web Server。

第二步：在项目 TestWebClient 的 config 文件中增加如下内容：

```
[general]
……
mxProxy = "10.65.109.121 10.65.109.121:5678 cert"

[proxy]
server="10.65.109.121:4998"
server="10.65.109.121:4897"
```

在[general]部分，参数“ mxProxy”为 Multiplexing Proxy 定义了通信接口，该参数的具体格式如下：

<host> <proxyHost>:<proxyPort> <ssl>

上述参数解释如下：

1）<host> 用于连接的主机名，即 WinCC OA Server 的 IP 地址。

2）<proxyHost> 是包含 Multiplexing Proxy 的主机名。Multiplexing Proxy 可以部署在另外一台计算机上，本示例中 Proxy 与 Web Server 部署在同一台计算机上。

3）<proxyPort> 是 Multiplexing Proxy 的端口号（默认端口号是 5678）。

4）<ssl > 是使用的安全模式。“ wincert”为用于通信的 Windows 认证；“ cert”为使用 SSL 安全连接。

[proxy] 部分的参数解释如下：参数“ server ” 定义了允许通过 proxy 连接的管理器列表。“ 10.65.109.121”为 WinCC OA Server 的 IP 地址，4897 和 4998 分别是 Data Manager 和 Event Manager 的默认端口号。

第三步：在项目 TestWebClient 的 config 文件夹中还需要创建一个新文件 config.webclient，在其中增加如下内容：

```
[general]
……
data="10.65.109.121"
event="10.65.109.121"

mxProxy="10.65.109.121 222.128.29.196:5678 cert"

[proxy]
server="222.128.29.196:4998"
server="222.128.29.196:4897"

server="10.65.109.121:4998"
server="10.65.109.121:4897"
```

上述设置的参数解释如下：首先在 [general] 中设置 Data 和 Event 的指向，为 WinCC OA Server 的 IP 地址；如果此处不设置 Data 和 Event 的指向，则默认值为 WinCC OA Server 的计算机名称。参数“ mxProxy”的含义与前面介绍的相同，只是对于 Web Client 而言，Multiplexing Proxy 的主机名为外网发布的地址。在[proxy]部分，定义了允许通过 proxy 连接的管理器列表。

注意， config.webclient 文件的内容用于生成 Web Client 项目的 config 文件，位于运行 Web Client 计算机的“ C:/Users/Administrator/.wincc_oa-cache/TestWebClient/config”文件夹中。

2.2 设置路由器

在 WinCC OA Web Server 一侧的路由器中，需要转发端口 80、443 和 5678。80、443 和 5678 端口分别是 HTTP、HTTPS 和 Multiplexing Proxy 的默认端口。请注意，如果默认端口发生更改，则在路由器中转发的端口也需要相应改变。

以一个 Cisco RV042 10/100 4-Port VPN Router 为例。登陆路由器后，找到 Setup 中的 Forwarding，在列表中加入下述三个端口：

HTTP [TCP/80~80]->10.65.109.121 [Enabled]
HTTPS [TCP/443~443]->10.65.109.121 [Enabled]
PROXY [TCP/5678~5678]->10.65.109.121 [Enabled]

图 3 设置路由器中的端口转发

需要注意以下几个问题：

1、如果禁用了 Multiplexing Proxy，则不需要转发端口 5678。

2、在 Web Client 一侧的路由器不需要转发端口。

2.3 访问 Web 服务器的画面

在局域网中，可以在浏览器中使用 https://10.65.109.121 或 https:// 222.128.29.196 访问 Web 服务器的画面。请注意，如果使用 https:// 222.128.29.196 访问时，需要 Web Client 所在的计算机可以访问外网。

访问 Web 服务器时会出现提示“ There is a problem with this website’s security certificate”，点击“ Continue to this website (not recommended)”，则弹出如下“ Security Problem”对话框：

图 4 “ Security Problem”对话框

显示上述对话框的原因是没有找到匹配的证书，在这里可以点击“ Accept once”暂时接受一次，则可以进入 Web Client 初始画面，但是地址栏的右侧会出现如下红色提示“ Certificate Error”，创建和安装 SSL 证书将会解决该问题，下一章将介绍具体的方法。此时，可以正常进入 Web 服务器的画面进行监控。

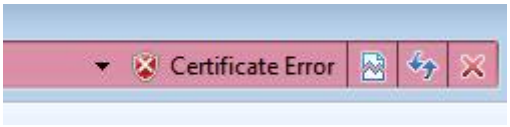

图 5 “ Certificate Error”提示信息

3 如何实现安全的 Web 访问

要实现安全的 Web 访问，就需要创建和安装 SSL 证书。在 WinCC OA 中，使用了两种类型的 SSL 证书，分别针对 Web Client 和 Multiplexing Proxy，针对每种类型都需要创建根证书和主机证书。 下面介绍如何创建自签名的 SSL 证书：

在 WinCC OA Server 所在的计算机上的“ System Management”中，点击“ Communication”属性页，找到“ SSL Certificates”，用于创建 SSL 证书。

3.1 创建 HTTP 根证书

在“ SSL Certificates ”对话框的“ Root certificate”一栏中，点击“ Create”，填写的示例内容如下图所示，详细的解释请参见帮助文档。请注意，“ IP Address”一栏的内容需要设置为外网发布的 IP 地址：

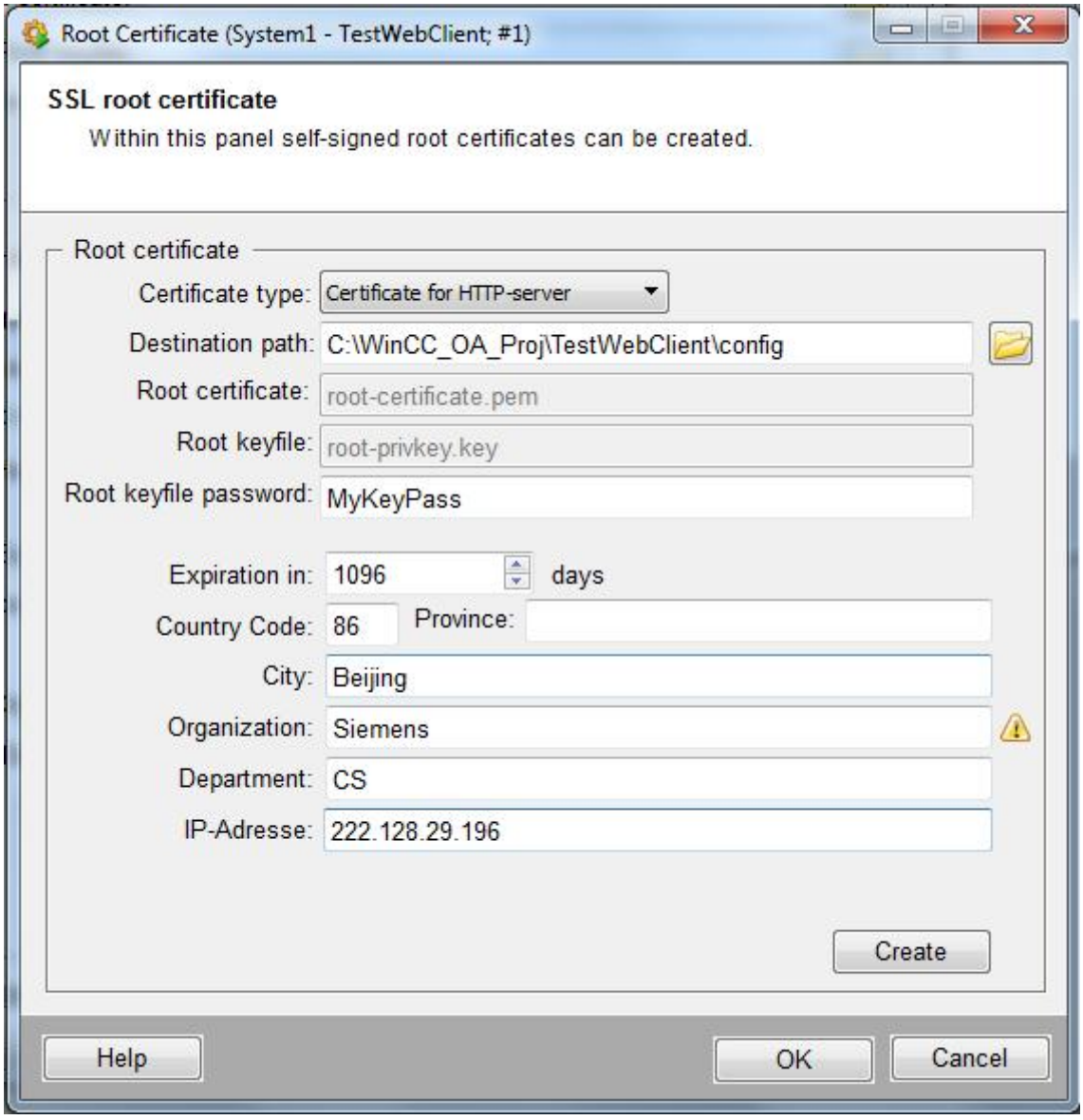

图 6 HTTP 根证书组态对话框

点击“ Create”按钮，在项目路径的 config 文件夹将创建两个证书文件：root-certificate.pem 和 root-privkey.key。

3.2 创建 HTTP 主机证书

在“ SSL Certificates”对话框的下方设置“ Host certificate”，填写的示例内容如下：

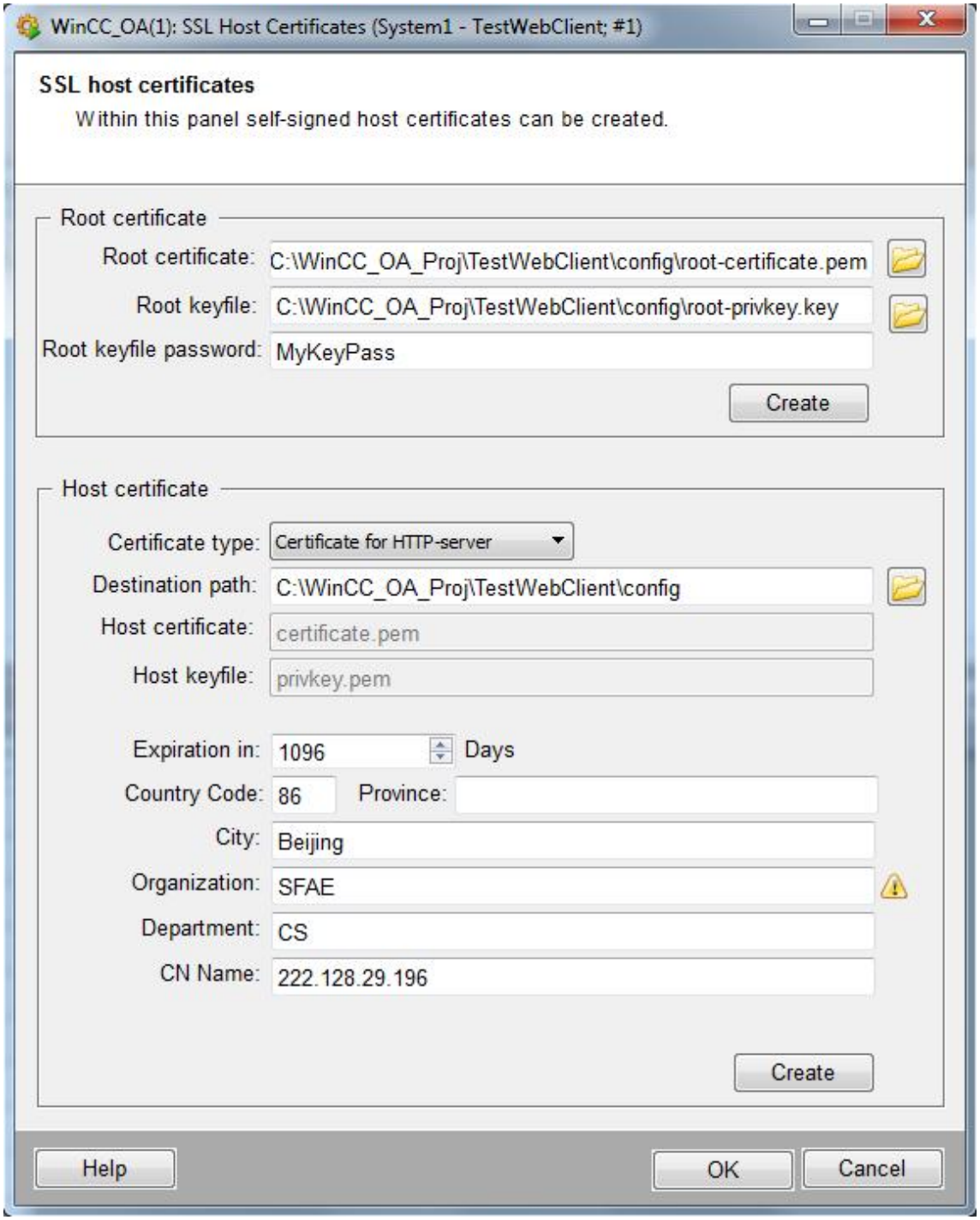

图 7 设置 HTTP 主机证书

注意，上图 7 中的“ Organization”与图 6 中的“ Organization ” 设置不能相同；“ CN Name ” 一栏的内容需要设置为外网发布的 IP 地址。

由于创建新项目时，在 WinCC OA 项目路径的 config 文件夹下会默认生成几个证书文件，因此点击“ Create”按钮后，会提示下面的对话框询问是否覆盖旧的证书文件，点击“ Yes”按钮确认覆盖。

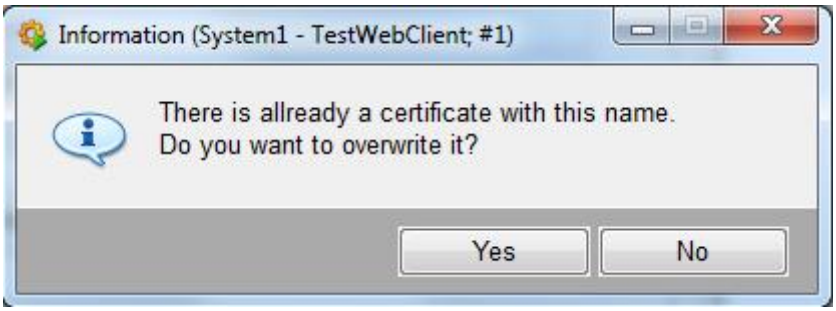

图 8 “确认覆盖已有同名证书”对话框

注意，需要等待弹出如下图 9 所示的消息对话框，并点击“ OK”按钮后，才能确保证书创建成功。然后，点击“ SSL Host Certificates”对话框中的“ OK”按钮关闭该对话框。在项目路径的 config 文件夹创建了两个证书文件： certificate.pem 和 privkey.pem。

图 9 “证书创建成功”对话框

3.3 创建 PROXY 根证书

在“ SSL Certificates”对话框 的“ Root certificate”一栏中，再次点击“ Create”创建 PROXY 根证书，填写的示例内容如下图所示：

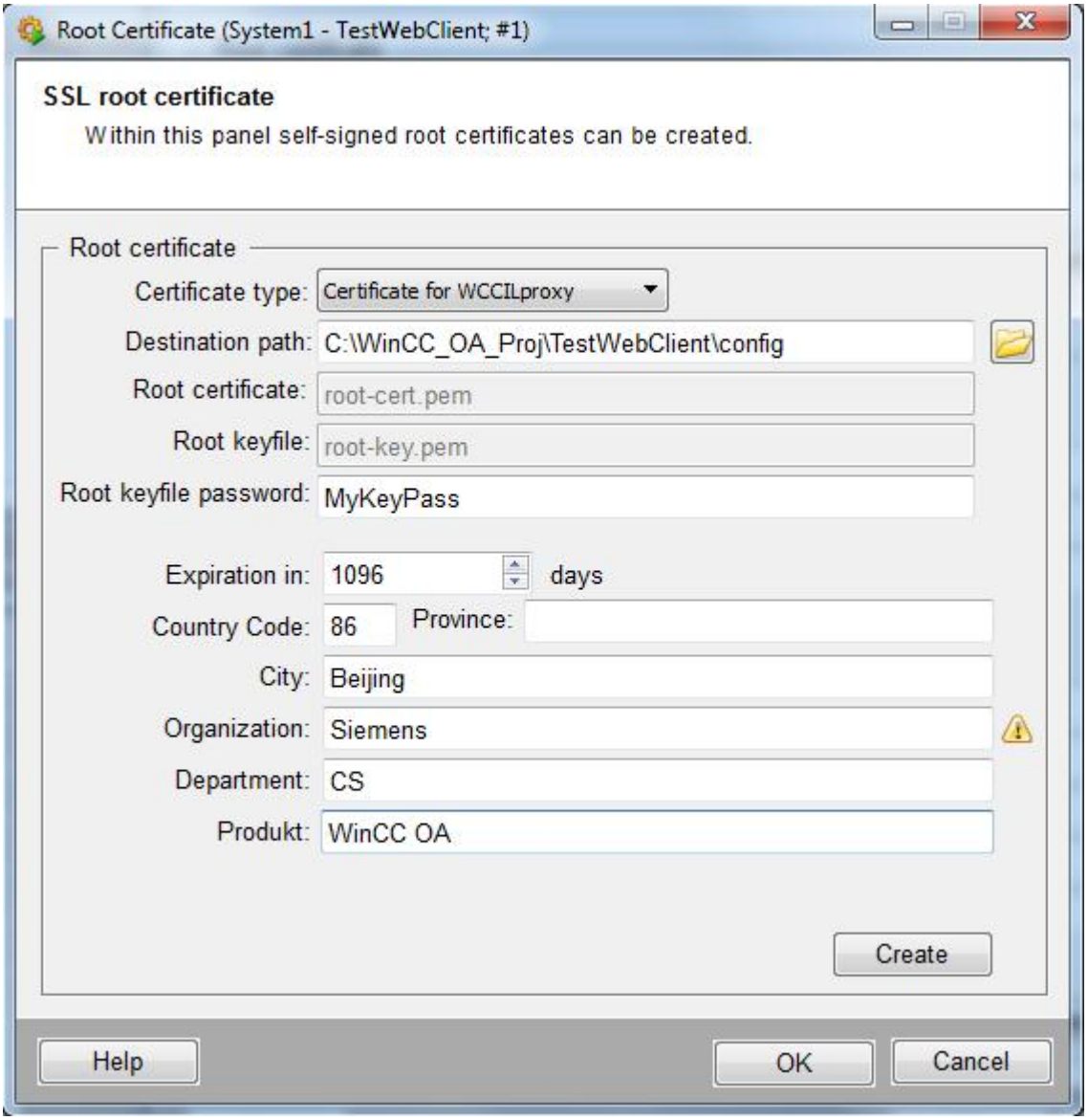

图 10 “ PROXY 根证书”对话框

点击“ Create”按钮，在项目路径的 config 文件夹创建了两个证书文件：root-cert.pem 和 root-key.pem。

3.4 创建 PROXY 主机证书

在“ SSL Certificates”对话框的下方设置“ Host certificate”，填写的示例内容如下：

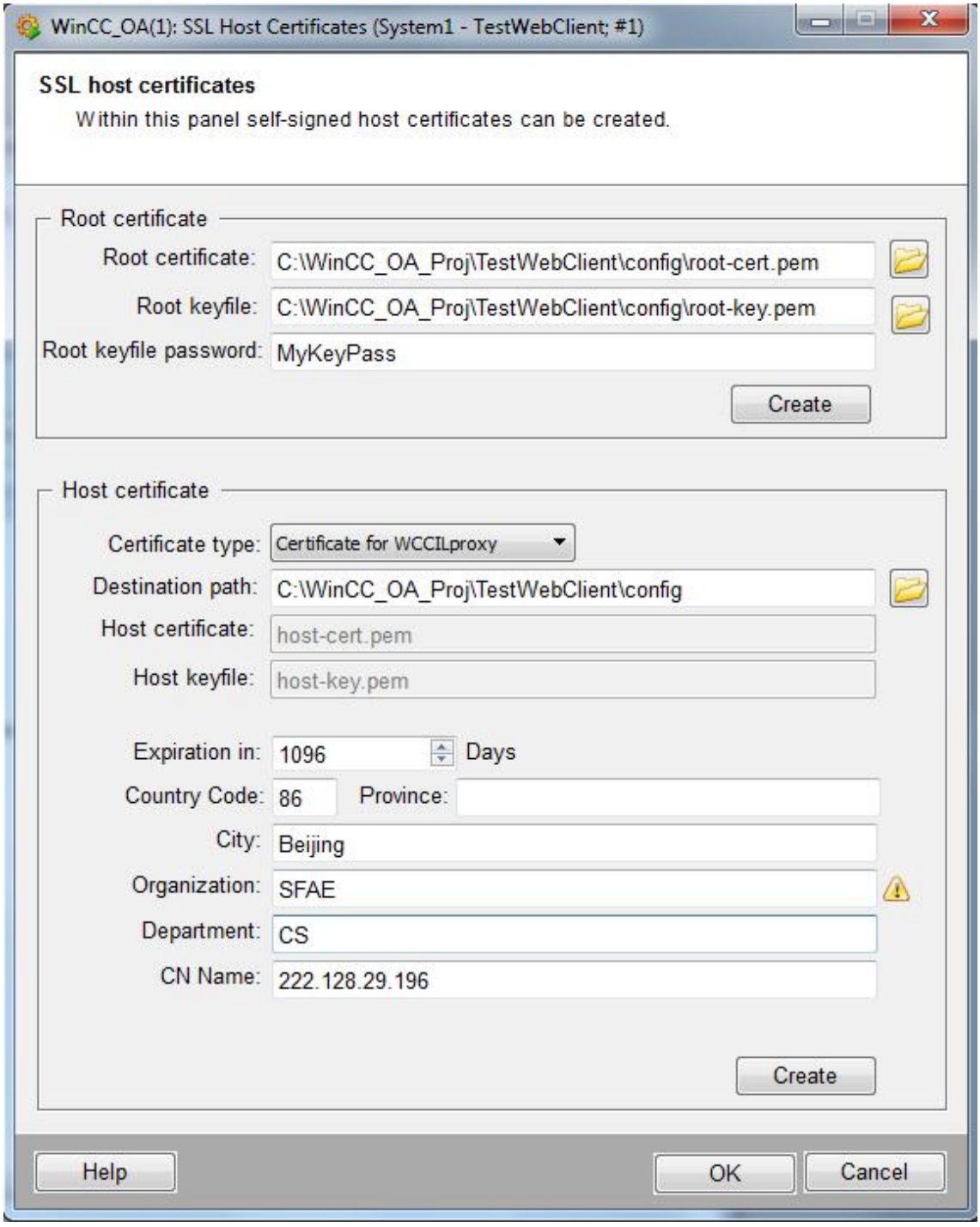

图 11 “ PROXY 主机证书”对话框

注意，上图 11 中的“ Organization”与图 10 中的“ Organization”设置不能相同；“ CN Name ”一栏的内容需要设置为外网发布的 IP 地址。

点击“ Create”按钮，参考 3.2 节，确认图 8 和图 9 中的两个对话框后，在项目路径的 config 文件夹创建了两个证书文件：host-cert.pem 和 host-key.pem。

注意，创建完成上述 4 对证书文件后，需要重启项目，并确保在日志文件中没有错误信息。

3.5 在 Web Client 计算机上安装证书

手动拷贝项目路径的 config 文件夹中的 root-certificate.pem 和 certificate.pem 两个文件到 Web Client 所在的计算机上，重命名为.crt 文件，双击并安装证书即可。请注意，在弹出的安装向导中，将证书安装到“ Trusted Root Certification Authorities”，如下图所示：

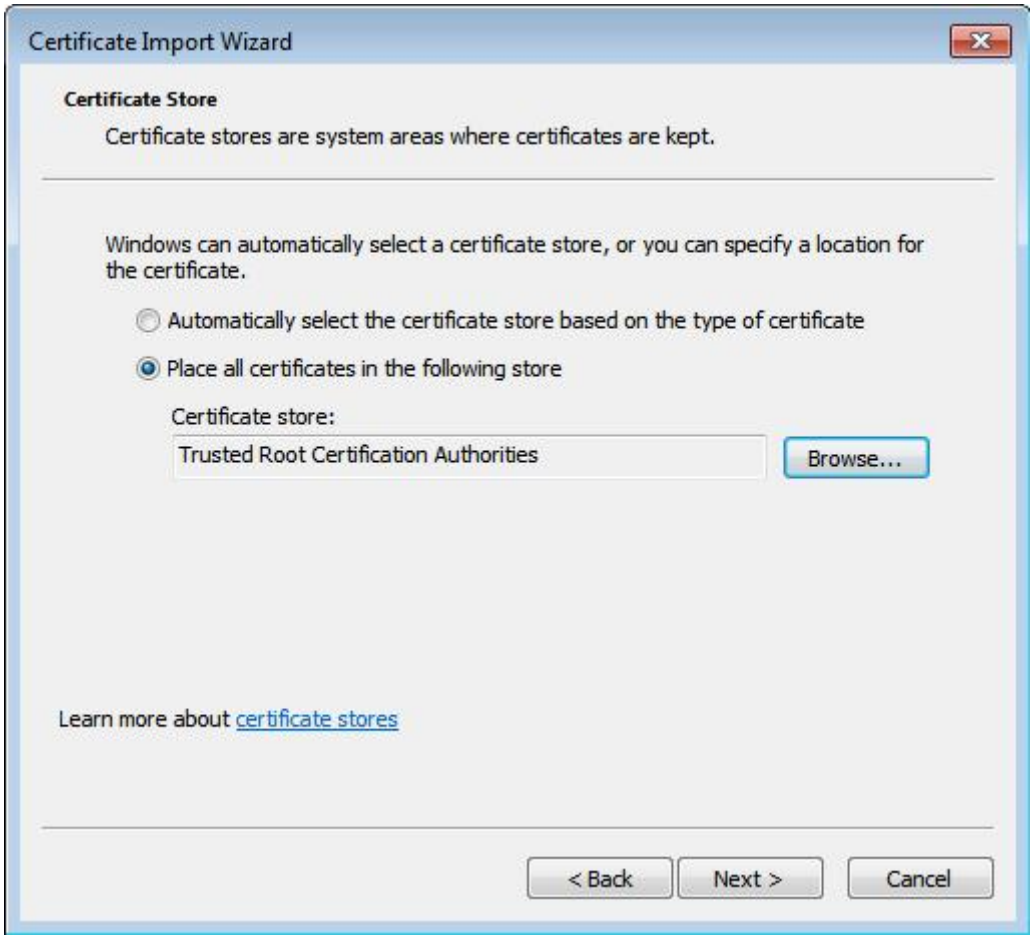

图 12 “安装证书”对话框

3.6 访问 Web 服务器的画面

在浏览器中再次运行 Web Client，则地址栏右上角没有“ certificate error”的错误提示，可以正常进入 Web 服务器的画面进行监控，如下图所示：

图 13 正常运行 Web Client 界面

此时，在 Web Client 的项目路径，可以找到三个证书文件 host-cert.pem、host-key.pem 和 root-cert.pem。

附录一推荐网址

WinCC OA （PVSS） 网站首页：
www.etm.at
WinCC OA 中文技术论坛：
http://www.ad.siemens.com.cn/club/bbs/bbs.aspx?b_id=65

注意事项

应用示例与所示电路、设备及任何可能结果没有必然联系，并不完全相关。应用示例不表示客户的具体解决方案。它们仅对典型应用提供支持。用户负责确保所述产品的正确使用。这些应用示例不能免除用户在确保安全、专业使用、安装、操作和维护设备方面的责任。当使用这些应用示例时，应意识到西门子不对在所述责任条款范围之外的任何损坏/索赔承担责任。我们保留随时修改这些应用示例的权利，恕不另行通知。如果这些应用示例与其它西门子出版物(例如，目录)给出的建议不同，则以其它文档的内容为准。

声明

我们已核对过本手册的内容与所描述的硬件和软件相符。由于差错难以完全避免，我们不能保证完全一致。我们会经常对手册中的数据进行检查，并在后续的版本中进行必要的更正。欢迎您提出宝贵意见。

西门子（中国）有限公司