

SIEMENS

如何配置OPC DCOM

How to configure OPC DCOM

User Guide

Edition (2008 年 12 月)

摘要 本文档主要介绍如何能够正确在 OPC 通讯中的 DCOM

关键词 OPC DCOM

Key Words OPC DCOM

目 录

1. 移除Windows安全
2. 建立相互能识别的用户账号
3. 配置系统宽泛的DCOM设置
4. 配置Server 特殊的DCOM 设置
5. 恢复Windows安全

OPC 技术依赖于微软的 COM 和 DCOM 在自动化的硬件与软件之间进行数据交换；但对于一个新的用户正确的配置 DCOM 是件头痛的事。如果不能正常的建立 OPC 的连接或者是不能成功的传输 OPC 数据，可能与下面的 DCOM 问题相关。本文讲述如何正确配置 DCOM 的步骤并保证安全。

一个简单有效的配置并建立可靠的DOM通讯包括了下列的步骤：

1. 移除Windows安全
2. 建立相互能识别的用户账号
3. 配置系统宽泛的DCOM设置
4. 配置Server 特殊的DCOM 设置
5. 恢复Windows安全

1. 移除Windows 安全

为了能够建立DCOM通讯，第一步需要禁止Windows 防火墙的功能，这个功能从Windows XP Service Pack 2 或以后的版本缺省时是被打开的。防火墙能够阻止未被授权的访问（通常防止病毒，蠕虫，和不怀好意的或者粗心大意的操作）。如果计算机在一个安全的网络里，即使是防火墙在短的时间内关闭也不会有什么潜在的危害。可以向管理员确认临时的关闭防火墙是否安全。在第5步中还会恢复安全功能“恢复Windows安全，”。

关闭Windows防火墙，按下面的步骤：

- a. 点击Windows开始按钮，选择控制面板，最后点击Windows 防火墙。
- b. 在 General 标签里，选择“Off (not recommended)”（参考图 1）。

全部使用宋体五号字体或 10.5 号字，段落间隔均为 1.5 倍行距。

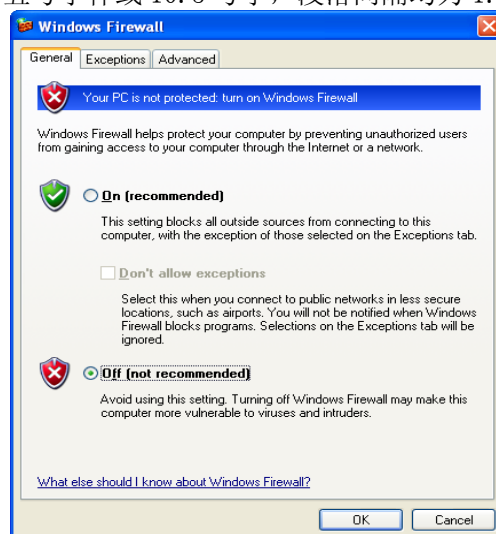


图 1

2. 建立相互能识别的用户账号

为了使计算机能正确的识别用户账号, 所以必须保证用户账号在OPC客户机和OPC服务器上都能够被识别, 这也包括Everyone这个用户账号在OPC访问上。

2.1 添加用户账户

确保所有的计算机有相同的用户名和密码的组合。 用户名与密码的匹配在 OPC 的访问是必须的。注意:

- 一个账户必须有一个用户名和密码。 如果一个账户没有密码是不能够建立通讯。
- 当使用的是Windows 工作组, 每个计算机上拥有自己全部的用户账户和密码
- 当使用单个域, 用户账户是由域控制器来同步。
- 当使用多域, 需要作域间的信任或者添加本地用户到受影响的计算机上

2.2 本地用户的认证

在 Windows XP 和 Windows Vista, 有一个设置需要修改。 在 Windows 2000 更早的版本没有必要修改。 在缺省情况下 Simple File Sharing 总是被开启的, Simple File Sharing 强制使远程的每个用户作为 Guest 账户来认证。 这种安全机制使的不能正常通讯, 有两种方法关闭。

方法 1: 关闭 Simple File Sharing

- a. 双击桌面上 “我的电脑”。
- b. 在工具菜单里, 点击文件夹选项。
- c. 点击 View 标签, 并去除勾选 “Use Simple File Sharing (Recommended)” 复选框来关闭 Simple File Sharing(参考图 2)

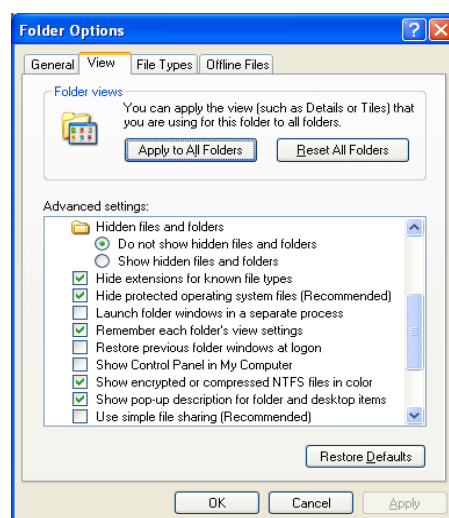


图 2

方法 2: 设置本地安全策略

- 点击 Windows 开始按钮, 选择控制面板 1, 管理工具, 本地策略。如果在控制面板中找不到管理工具, 可以选择点击 Windows 开始按钮; 选择运行菜单并输入 “secpol.msc”。
- 在目录树了, 找到安全设置, 本地安全, 最后选择安全选项文件夹 (参考图3)。
- 找到+ “Network access: Sharing and security model for local accounts” 选项设置 “Classic - local users authenticate as themselves”

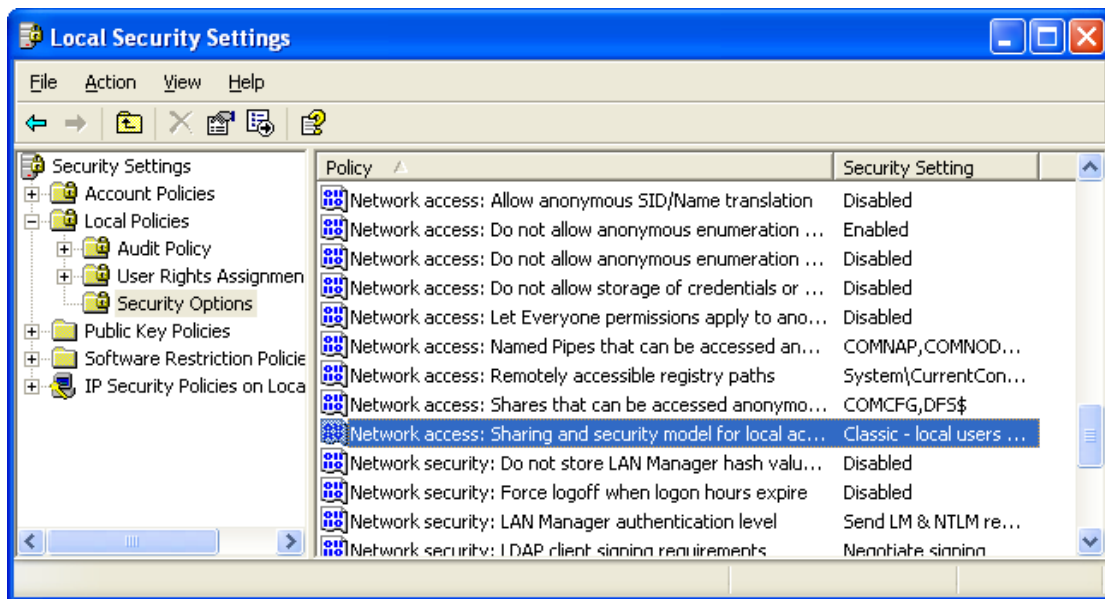


图 3

3. 配置系统宽泛的 DCOM 设置

系统的宽泛的 DCOM 设置影响着 Windows 的 DCOM 的应用, 包括 OPC 的应用, 由于 OPC 客户端没有自己的 DCOM 的设置, 所以它受缺省 DCOM 的配置的影响, 因此需要作必要的改变, 如下面的步骤所示:

- a. 点击 Windows 的开始按钮, 选择运行菜单命令。(参考图 4)

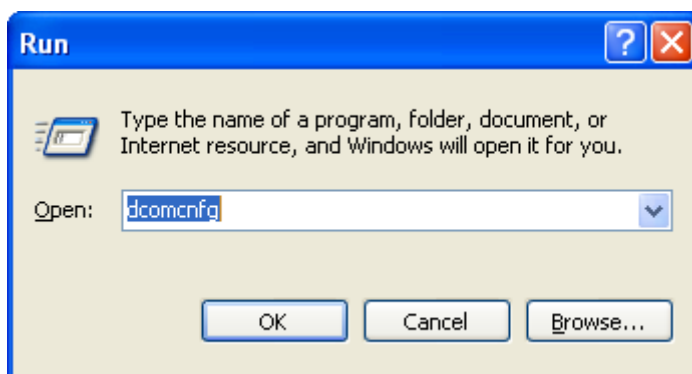


图 4

- b. 在弹出的对话框中输入“DCOMCNFG”初始化 DCOM 的配置过程，点击 OK 确认后，弹出组件服务的窗体。（参考图 5）

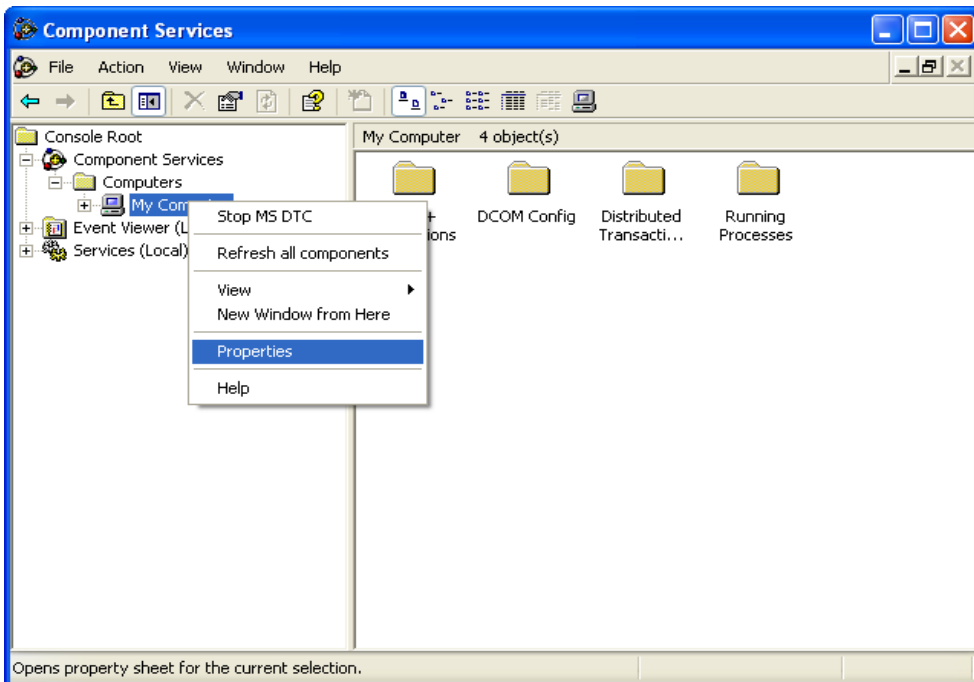


图 5

- c. 组件服务的窗口打开后，选择目录树中的 Console Root，然后选择 Component Services 下的 Computers，在选择其下的 My Computer。
- d. 右击 My Computer，注意不是桌面上的 My Computer，而是 Component Services 目录下的 My Computer。
- e. 选择 Properties 选项。

3.1 缺省属性

在缺省属性标签里，确保三个指定的选项设置如下（参考图 6）

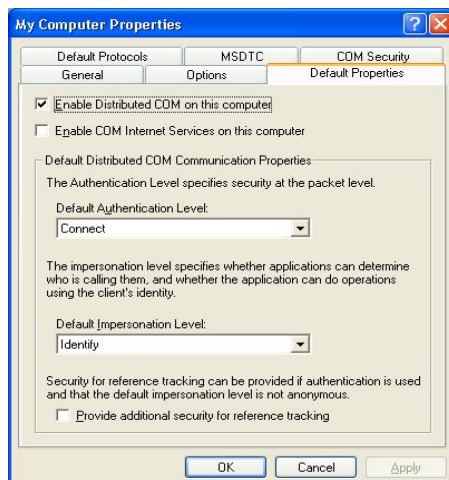


图 6

- 勾选“Enable Distributed COM on this computer”选项，注意，如果这一项做了改变需要重新启动计算机才能生效。
- 设置“Default Authentication Level”为 Connect，也可以使用列表里的其它设置项，但“Connect”选项是考虑安全的最小的权限。
- 设置“Default Impersonation Level”为 Identify，在缺省协议的标签里选择缺省的协议为“Connection- Oriented TCP/IP”， OPC 的通讯是仅需要“Connection- Oriented TCP/IP”，所以尽可能把其它协议删除，然而若其它的应用程序需要其它的协议，那么就必须保留其它协议。这样作是能够减小延时（参考图 7）

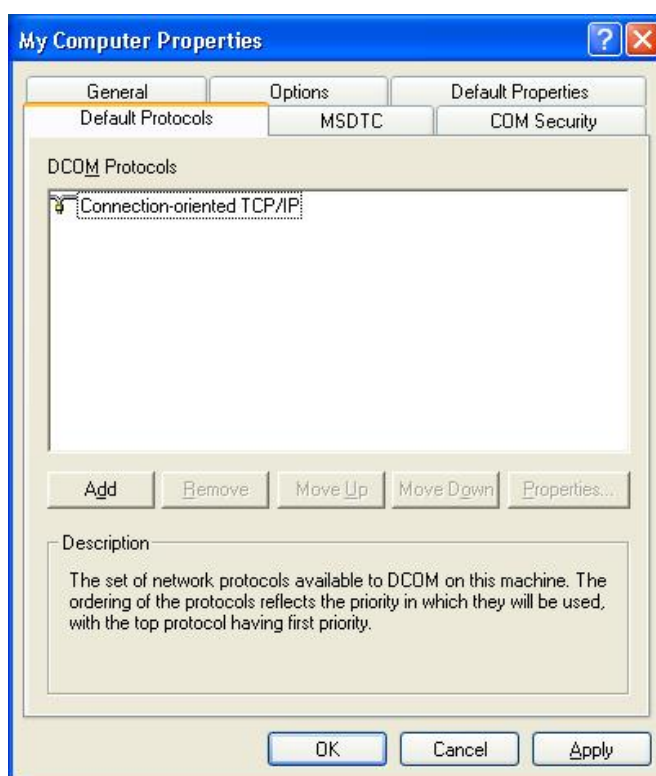


图 7

3.2 COM安全

Windows 用 COM 的安全标签设置所有对象的系统宽泛的访问控制列表（参考图 8），访问控制列表包括了 Launch/Activation 和访问权限，为了添加正确的允许权限。按下列的步骤操作。

- 在访问允许的组，点击“Edit Default...”按钮（参考图9），添加“Everyone”到“Group or usernames”，点击OK按钮。

- b. 在访问允许的组，点击“Edit Limits...”按钮（参考图9），添加“Anonymous Logon”和“Everyone”到“Group or usernames”，点击OK按钮。
- c. 在启动与激活允许的组里，点击“Edit Default...”按钮（参考图9），添加“Everyone”到“Group or usernames”，点击OK按钮。
- d. 在启动与激活允许的组里，点击“Edit Limits...”按钮（参考图9），添加“Everyone”到“Group or usernames”，点击OK按钮。



图 8

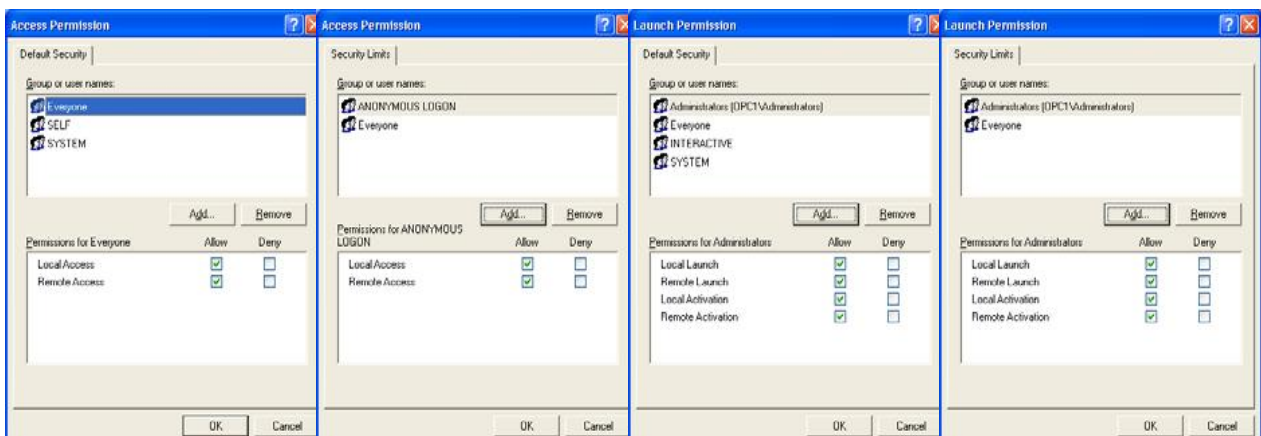


图 9

3. 配置Server的特殊DCOM 设置

一旦DCOM的宽泛配置设置完，就需要关注Server的DCOM的特殊设置，这里的设置最终将会不同于其它的OPC Server的设置。改变设置如下：

- 点击Windows的开始按钮，选择运行菜单选项（参考图4）
- 在弹出的运行窗口里，输入“DCOMCNFG”初始化DCOM的配置，点击ok后，组件服务的窗口就会出现参考图10）。
- 一旦组件服务的窗口打开后，点击Console Root文件夹，打开后点击组件服务文件夹，再点击计算机文件夹，在展开的目录里选择DCOM Config 文件夹。
- 在右边的Windows的窗口里，找到需要配置的OPC Server，右击该Server，在弹出的菜单里选择属性选项，进行OPC Server的特殊设置，在OPC Server的特殊设置里仅Identity 标签的内容需要修改，其它标签项可参考DCOM的宽泛设置（参考图11）。

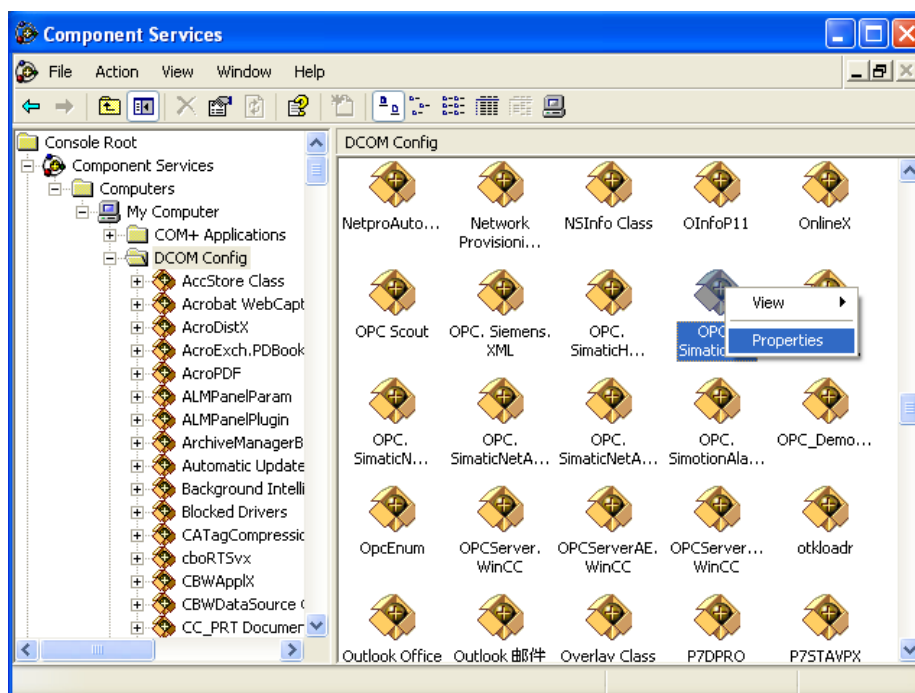
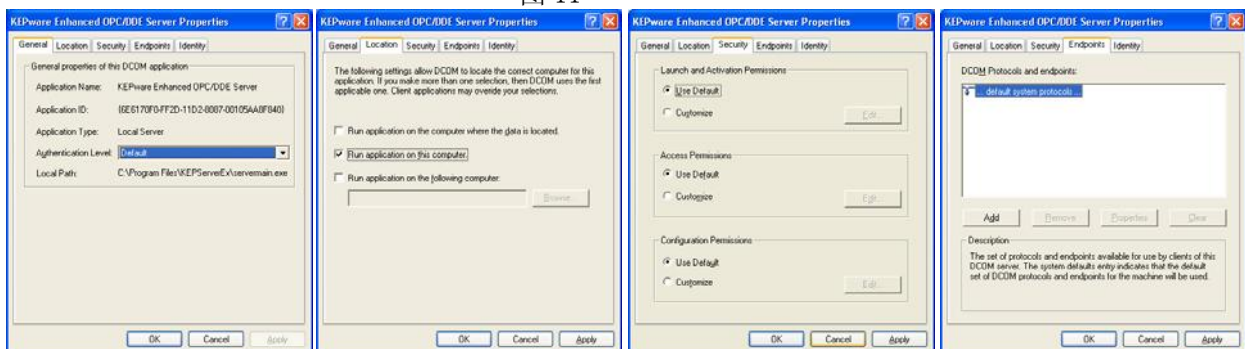


图 11



e. 但是需注意的是Identity 标签项的设置, Identity标签 (参考图12) 有四个选项:

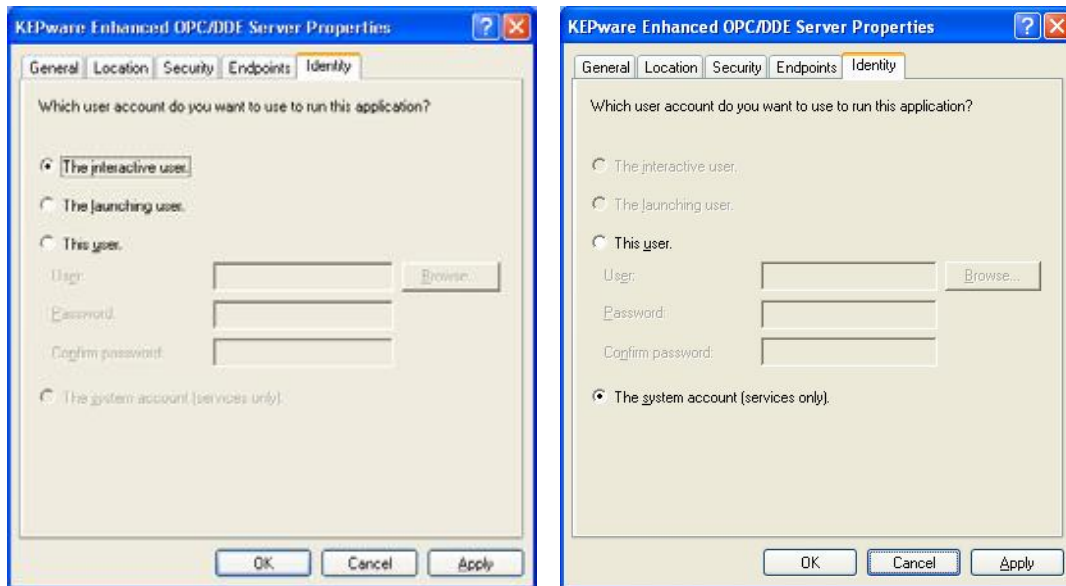


图 12

The interactive user: OPC Server 以交互的用户认证, 这个账户是当前登陆此计算机且驻留在OPC Server的计算机上, 也就是必须有账户登陆, 否则不能启动OPC Server, 当此用户注销时, OPC Server就会关闭, 即使是计算机的重新启动, 也会造成OPC Server的短暂的关闭。

The launching user: OPC Server以访问的用户认证, 操作系统会为每个访问的用户创建一个实例, 这样会有三个问题出现, 若OPC Server只允许一个用户访问时, 当系统中已经有了一个实例, 再有其它用户就无法访问。若是OPC Server允许多个用户访问时, 那么带来的问题是随着不同用户的访问, 就会打开多个实例, 这样就会占用更多的计算机的资源。另外的一个问题是硬件的抢占, 如串口, 当一个使用了, 其它的用户就无法再使用。

This user: OPC Server以指定的用户账户认证, 这种情况需要在OPC Server的计算机上存在着要指定的账户, 而且对于OPC Client必须知道此用户。否则无法访问。

The system account (services only): OPC Server以操作系统账户认证, 对于工作组还是域, 系统账户都能被识别, 也不需要用户登陆。但OPC server必须以服务的方式启动。

5 恢复Windows安全

一旦建立OPC Client和OPC Server的通讯，保证计算机的安全也是非常重要的，这包括下列的步骤：

- a. 再次开启计算机的防火墙，来阻止未授权的网络访问。而且需要做两个层次的例外处理：

应用程序：指定那些应用可以响应自动的请求

端口协议：指定对于TCP/IP或者UDP/IP的端口的允许或拒绝访问。

修改访问控制列表允许或者否决所需要，这即包括宽泛配置中的设置也包括 Server 的特殊配置，需要提醒的是 OPCenum 需要“Anonymous Logon”的访问权限。

附录一 推荐网址**NET**

西门子（中国）有限公司

工业自动化与驱动技术集团 客户服务与支持中心

网站首页: <http://www.ad.siemens.com.cn/Service/>

Net下载中心:

<http://www.ad.siemens.com.cn/download/DocList.aspx?Typeld=0&CatFirst=12&CatSecond=-1&CatThird=-1>

专家推荐精品文档: <http://www.ad.siemens.com.cn/Service/recommend.asp>

“找答案” Net版区:

<http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1031>

版权© 西门子（中国）有限公司 2001-2008 版权保留

复制、传播或者使用该文件或文件内容必须经过权利人书面明确同意。侵权者将承担权利人的全部损失。权利人保留一切权利，包括复制、发行，以及改编、汇编的权利。

西门子（中国）有限公司