Technical

Bulletin M2011001

MEGAsys – OPC Server for Remote OPC Client Setup Technical Notes

TN-207020118

v1.0

For MEGAsys GB/Big5/Eng Version 4.0/5.0

2011/01/01
Evertech Electronics Ltd.

OPC - OLE for Process Control 工業標準

OPC 全稱是 OLE for Process Control，它的出現爲基於 Windows 的應用程式和現場程序控制應用建立了橋樑。在過去，爲了存取現場設備的資料資訊，每一個應用軟體開發商都需要編寫專用的介面函數。由於現場設備的種類繁多，且產品的不斷升級，往往給用戶和軟體發展商帶來了巨大的工作負擔。通常這樣也不能滿足工作的實際需要，系統集成商和開發商急切需要一種具有高效性、可靠性、開放性、可互操作性的即插即用的設備驅動程式。在這種情況下，OPC 標準應運而生。OPC 標準以微軟公司的 OLE 技術爲基礎，它的制定是通過提供一套標準的 OLE/COM 介面完成的，在 OPC 技術中使用的是 OLE 2 技術，OLE 標準允許多台微機之間交換文檔、圖形等物件。

COM 是 Component Object Model 的縮寫，是所有 OLE 機制的基礎。COM 是一種爲了實現與編程語言無關的物件而制定的標準，該標準將 Windows 下的物件定義爲獨立單元，可 不受程式限制地訪問這些單元。這種標準可以使兩個應用程式通過物件化介面通訊，而不需要知道對方是如何創建的。例如，用戶可以使用 C++語言創建一個 Windows 物件，它支援一個介面，通過該介面，用戶可以訪問該物件提供的各種功能，用戶可以使用 Visual Basic，C，Pascal，Smalltalk 或其他語言編寫物件訪問程式。在 Windows NT4.0 作業系統下，COM 規範擴展到可訪問本機以外的其他物件，一個應用程式所使用的物件可分佈在網路上，COM 的這個擴展被稱爲 DCOM（Distributed COM）。

通過 DCOM 技術和 OPC 標準，完全可以創建一個開放的、可互操作的控制系統軟體。OPC 採用 客戶/伺服器模式，把開發訪問介面的任務放在硬體生產廠家或第三方廠家，以 OPC 伺服器的形式提供給用戶，解決了軟、硬體廠商的矛盾，完成了系統的集成， 提高了系統的開放性和可互操作性。

OPC 伺服器通常支援兩種類型的訪問介面，它們分別爲不同的編程語言環境提供訪問機制。這兩種介面是：自動化介面（Automation interface）；自定義介面（Custom interface）。自動化介面通常是爲基於腳本編 程語言而定義的標準介面，可以使用 VisualBasic、Delphi、PowerBuilder 等編程語言開發 OPC 伺服器的客戶應用。而自定義介面 是專門爲 C++等高級編程語言而制定的標準介面。OPC 現已成爲工業界系統互聯的缺省方案，爲工業監控編程帶來了便利，用戶不用爲通訊協定的難題而苦惱。 任何一家自動化軟體解決方案的提供者，如果它不能全方位地支援 OPC，則必將被歷史所淘汰。

1、在控制領域中，系統往往由分散的各子系統構成；並且各子系統往往採用不同廠家的設備和方案。用戶需要，將這些子系統集成，並架構統一的即時監控系統。
2、這樣的即時監控系統需要解決分散子系統間的資料共用，各子系統需要統一協調相應控制指令。
3、再考慮到即時監控系統往往需要升級和調整。
4、就需要各子系統具備統一的開放介面。
5、OPC(OLE for Process Control) 規範正是這一思維的產物。
6、OPC 基於 Microsoft 公司的 Distributed interNet Application (DNA) 構架和 Component Object Model (COM) 技術的，根據易於擴展性而設計的。OPC 規範定義了一個工業標準介面。

7、OPC 是以 OLE/COM 機制作爲應用程式的通訊標準。OLE/COM 是一種客戶/伺服器模式，具有語言無關性、代碼重用性、易於集成性等優點。OPC 規範了介面函數，不管現場設備以何種形式存在，客戶都以統一的方式去訪問，從而保證軟體對客 戶的透明性，使得用戶完全從低層的開發中脫離出來。

8、OPC 定義了一個開放的介面，在這個介面上，基於 PC 的軟體元件能 交換資料。它是基於 Windows 的 OLE——物件鏈結和嵌入、COM——部件物件模型(Component Object Model)和 DCOM——分散式 COM(Distributed COM)技術。因而，OPC 爲自動化層的典型現場設備連接工業應用程式和辦公室程式提供了一個理想的方法。

編輯本段 OPC 應用領域

1、工控解決方案用戶
2、樓控解決方案用戶
3、工控解決方案廠商
4、樓控解決方案廠商
5、工控解決方案集成商
6、樓控解決方案集成商
7、 All Automation Fields

OPC 是爲了連接資料源(OPC 伺服器)和資料的使用者(OPC 應用程式)之間的軟體介面標準。資料源可以是 PLC，DCS，條碼讀取器等控制設備。隨控制系統構成的不同，作爲資料源的 OPC 伺服器即可以是和 OPC 應用程式在同一台電腦上運行的本地 OPC 伺服器，也可以是在另外的電腦上運行的遠端 OPC 伺服器。

OPC 介面既可以適用於通過網路把最下層的控制設備的原始資料提供給作爲資料的使用者(OPC 應用程式)的 HMI(硬體監督介面)／SCADA(監督控制與資料獲取)，批次處理等自動化程式，以至更上層的歷史資料庫等應用程式，也可以適用于應用程式和物理設備的直接連接。所以 OPC 介面是適用於很多系統的具有高厚度柔軟性的介面標準。

OPC 解決了什麼

OPC 誕生以前，硬體的驅動器和與其連接的應用程式之間的介面並沒有統一的標準。例如，在 FA(FactoryAutomation)——工廠自動化領 域，連接 PLC(Programmable Logic Controller)等控制設備和 SCADA／HMI 軟體，需要不同的 FA 網路系統構成。根據某調查結果，在控制系統軟體發展的所需費用中，各種各樣機 器的應用程式設計占費用的 7 成，而開發機器設備間的連接介面則占了 3 成。此外，在 PA(Process Automation)——過程自動化領域，當希望把分散式控制系統(DCS——Distributed Control System)中所有的過程資料傳送到生產管理系統時，必須按照各個供應廠商的各個機種開發特定的介面，例如，利用 C 語言 DLL(動態鏈路資料庫)連接的 DDE(動態資料交換) 伺服器或者利用 FTP(檔傳送協定)的文本等設計應用程式。如由 4 種控制設備和與其連接的監視、趨勢圖以及表報 3 種應用程式所構成的系統時，必須花費大 量時間去開發分別對應設備 A，B，C，D 的監視，趨勢圖以及表報應用程式的介面軟體共計要用 12 種驅動器。同時由於系統中共存各種各樣的驅動器，也使維護 運轉環境的穩定性和信賴性更加困難。

MEGAsys OPC Client 參數設定

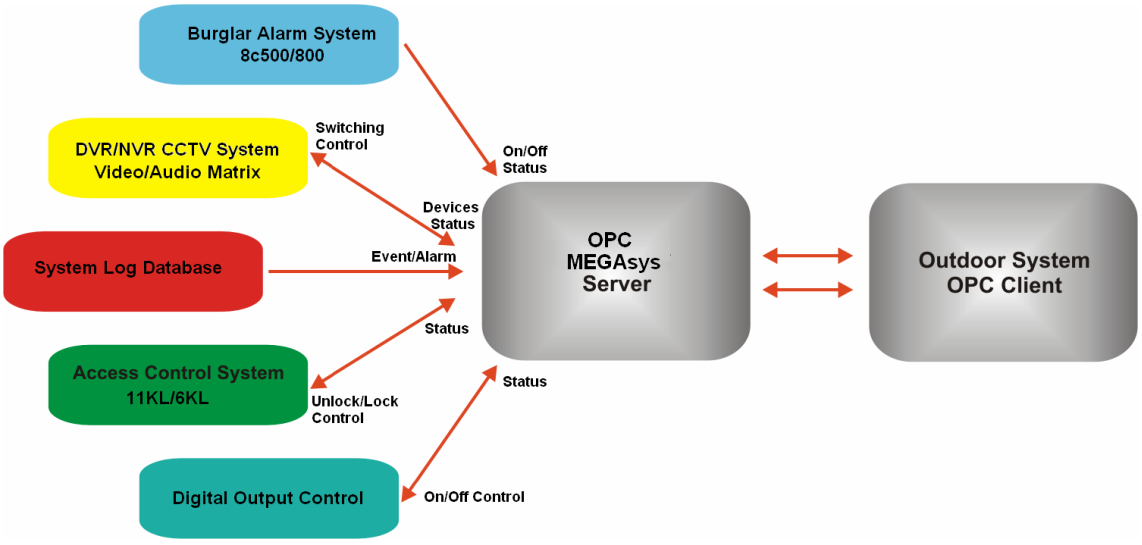
而 OPC 是爲了不同供應廠商的設備和應用程式之間的軟體介面標準化，使其間的資料交換更加簡單化的目的而提出的。作爲結果，從而可以向用戶提供不依靠于特定開發語言和開發環境的可以自由組合使用的程序控制軟體元件產品。

利用 OPC 的系統，是由按照應用程式(客戶程式)的要求提供資料獲取服務的 OPC 伺服器，使用 OPC 伺服器所必需的 OPC 介面，以及接受服務的 OPC 應用程式所構成。OPC 伺服器是按照各個供應廠商的硬體所開發的，使之可以吸收各個供應廠商硬體和 系統的差異，從而實現不依存於硬體的系統構成。同時利用一種叫做 Variant 的資料類型，可以不依存於硬體中固有資料類型，按照應用程式的要求提供資料 格式。

利用 OPC 使介面標準化可以不依存於各設備的內部結構及它的供應廠商來選用監視，趨勢圖以及表報應用程式。

爲什麼開發自主 OPC Server 和 OPC Gateway？

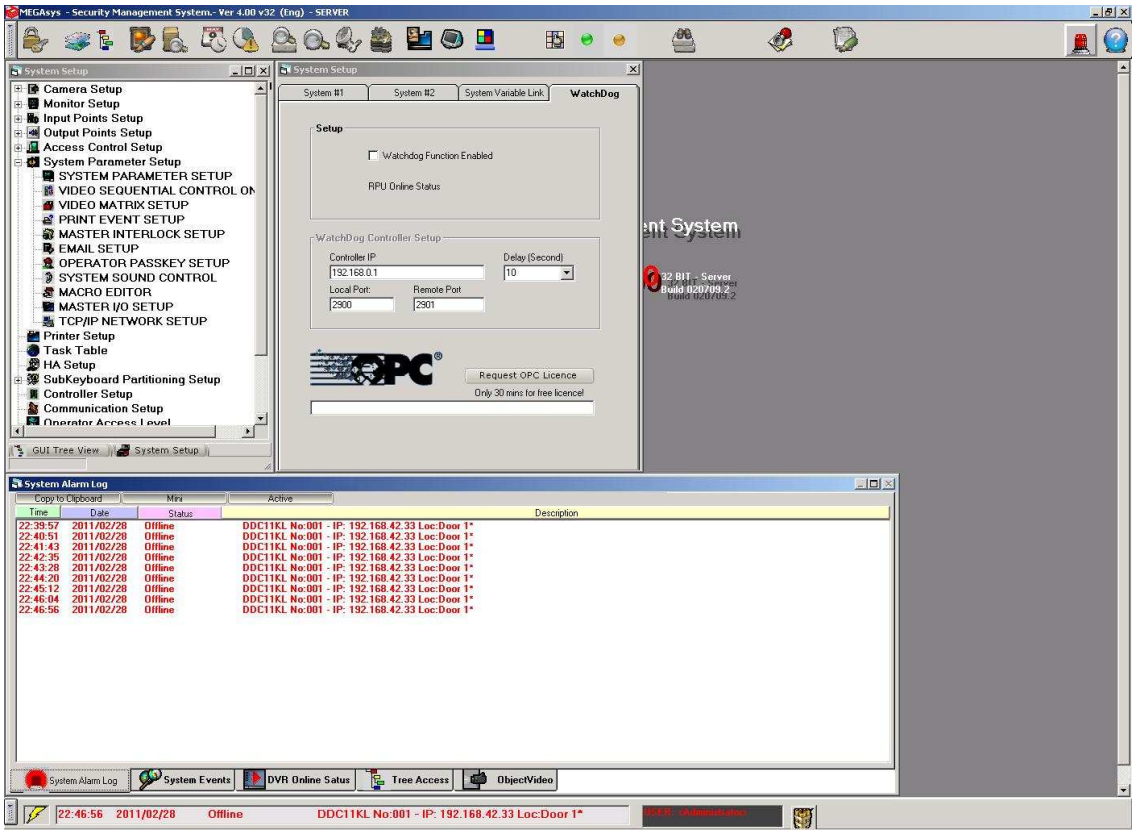
1、國外原廠商的高價格
2、國外原廠商面對項目的不靈活性
3、國內項目中子系統的多樣性難以提供 DRIVER
4、自主 OPC 伺服器追求的是穩定、即時、迅速。
5、眾多子系統的不規範性
6、總包項目在投標前後可能出現的不一致性
7、價格昂貴的原廠平臺伺服器軟體
8、總包商集成是否投入大量的人力開發
9、平臺和子系統的相容性
10、建立了 OPC 平臺和子系統的互通
11、解決廠商和集成商在專案集成的煩惱
12、解決廠商和集成商分散資源進行二次開發
13、解決專案中子系統廠商的困擾
14、爲上下位的資料通訊提供透明的通道



MEGAsys OPC Client 參數設定

設定和啓動 OPC 功能

i. System Parameter Setup > System Parameter Setup。
ii. 點選 'System Setup' 的第四頁 - Watchdog。
iii. 提取 OPC License, 點按 "Request OPC License" 鍵。
iv. 30 分鐘後, 用戶可以收到一個 free License, 請把 License code 貼在下方的 text bar。



<Setup-01>

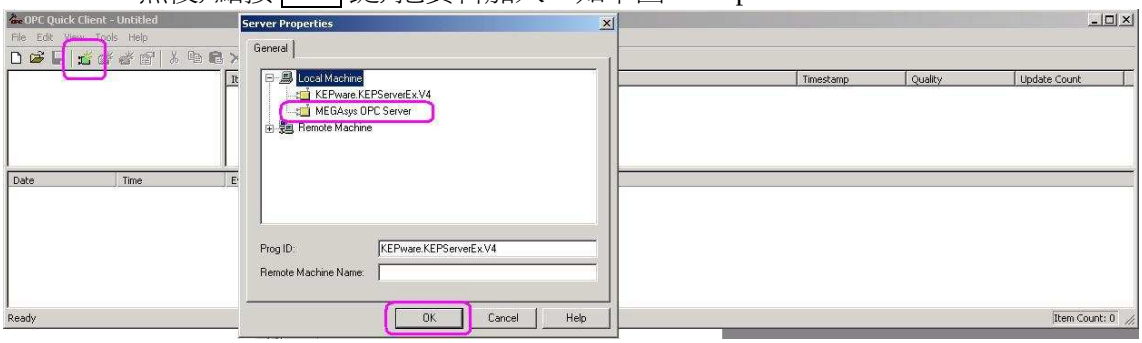
開啓 Remote OPC Quick Client 軟件, 出現以下視窗。

<Setup-02>

MEGAsys OPC Client 參數設定

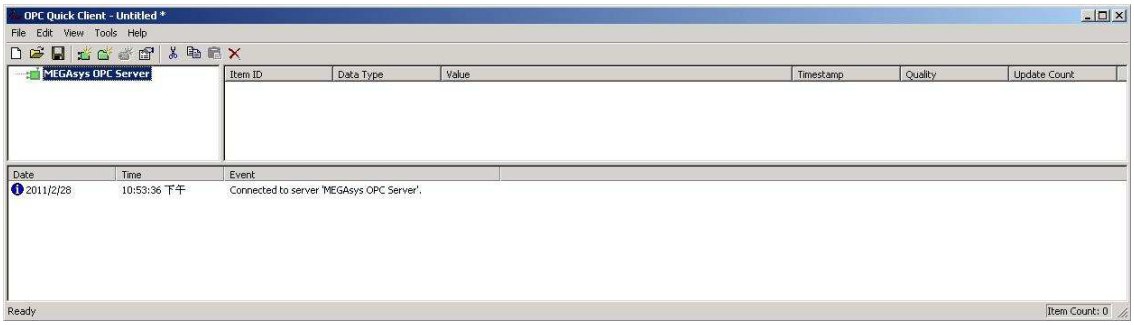
用戶可因應系統需要, 加入多個不同的 Server。以下會以加入 MEGAsys OPC Server 爲例子作說明。

1. 加入 New Server 資料。
   i. 點按 “New Server” 鍵。
   ii. 出現 ‘Server Properties’ 視窗。因爲現時 MEGAsys OPC Server 是安裝在本機中, 所以選擇路徑時點選 Local Machine > MEGAsys OPC Server。
   iii. 然後, 點按 OK 鍵, 把資料加入。如下圖<Setup-03>。



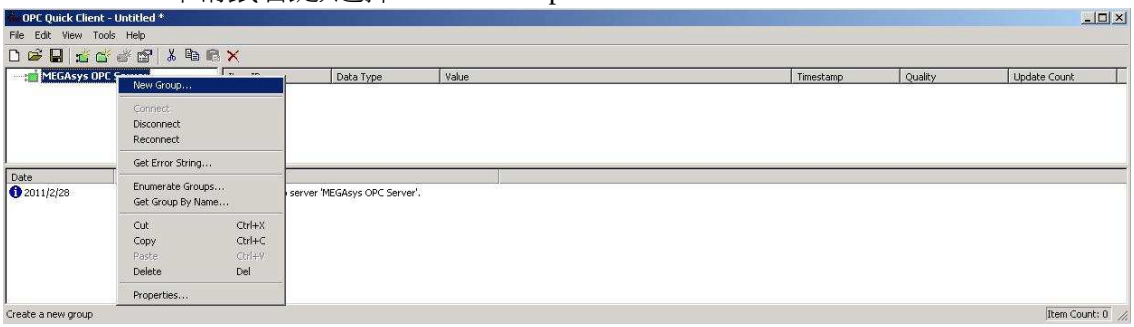
<Setup-03>

MEGAsys OPC Server 建立了。同時, 在視窗下方會顯示 “Connected to server …” 的資料。



<Setup-04>

2. 加入 New Group 資料。
   i. 爲 MEGAsys OPC Server 加入 “New Group” 。在 MEGAsys OPC Server 上按一下滑鼠右鍵, 選擇 “New Group…”。

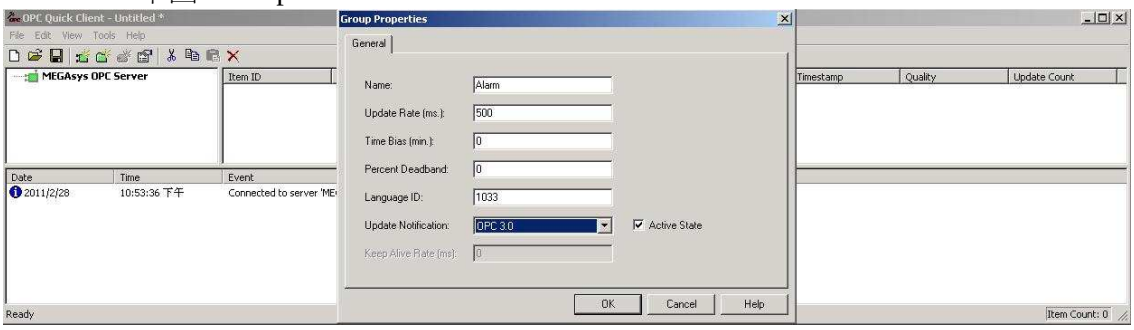


<Setup-05>

   ii. 在 Group Properties 視窗中, 填上 New Group 資料。
   iii. 爲 Group 加入 Name 資料。例如: Group Name - Alarm。
   iv. 設定 Update Rate、Update Notification 等資料。例如: Update Rate - 500、Update Notification – OPC 3.0。

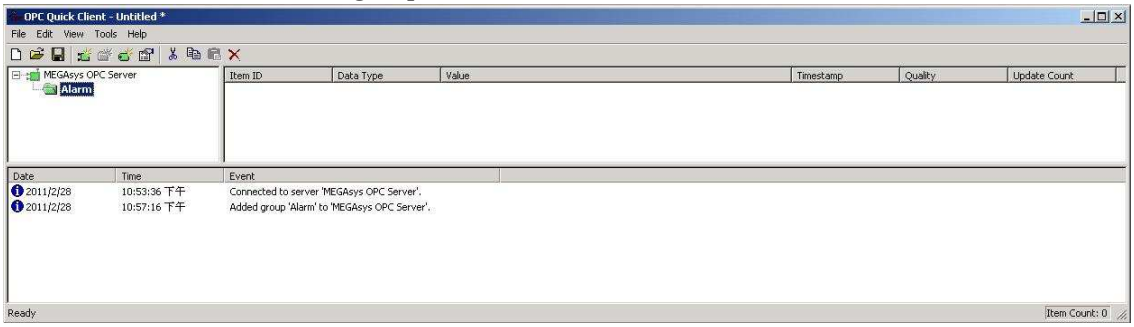
v. 剔選 “Active State” 。

vi. 完成後按 OK 鍵便可。Alarm group 便會加在 MEGAsys OPC Server 之下, 如下圖 <Setup-07>。



<Setup-06>

在視窗下方會顯示 “Added group …” 的資料。

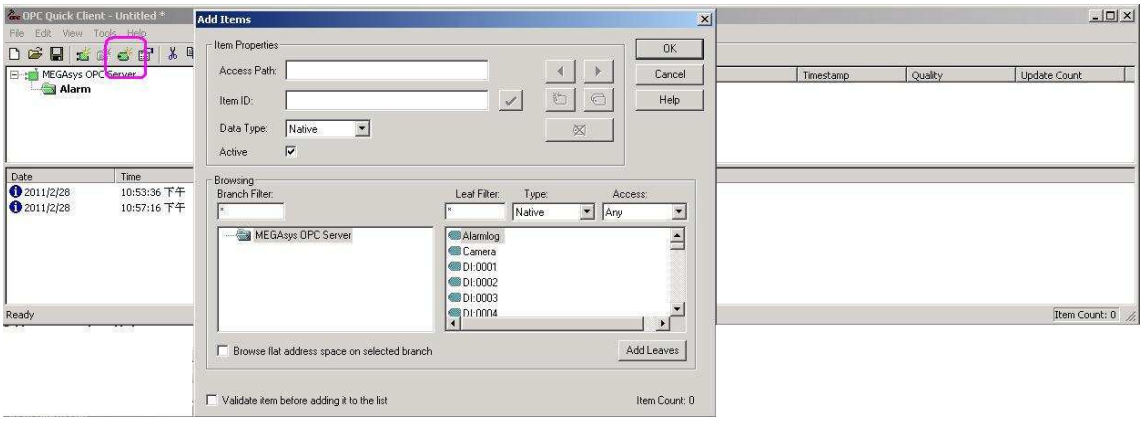


<Setup-07>

3. 加入 New Item 資料。

i. 加入屬於 Alarm group 的 Item 資料。點按 Add Item 鍵, 出現 ‘Add Items’ 視窗。

ii. 在 Alarm 上按一下滑鼠右鍵, 選擇 “New Items…”。



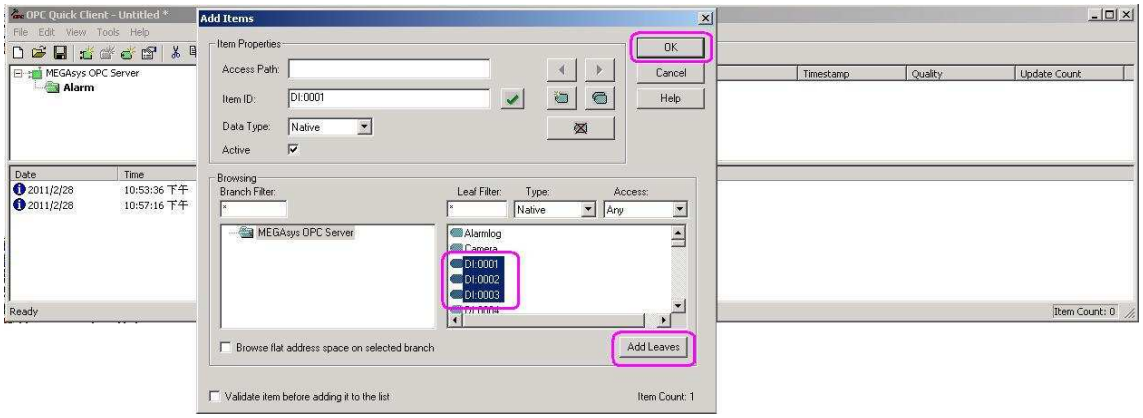
<Setup-08>

iii. 在 Add Items 視窗中, Browsing 方框內選擇合適的 Point。例如: DI0001、DI0002 和 DI0003。

iv. 點按 Add Leaves 鍵。

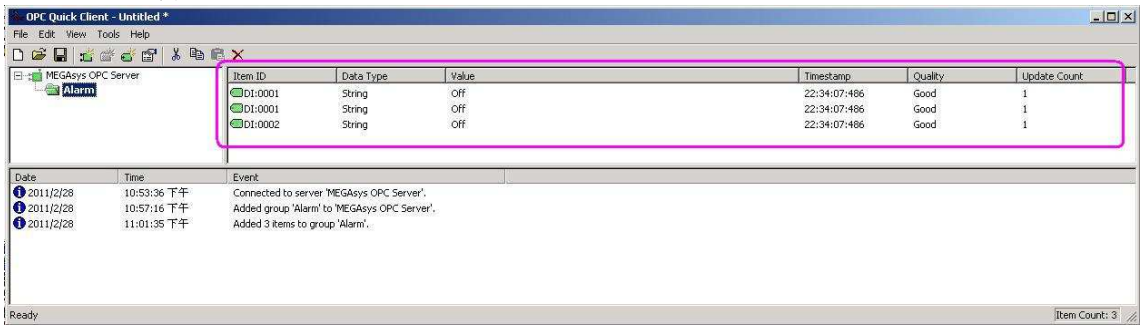
v. 再點按 OK 鍵, 把選擇的資料加入 Item List 中, 如 <Setup-10>。

MEGAsys OPC Client 參數設定



<Setup-09>

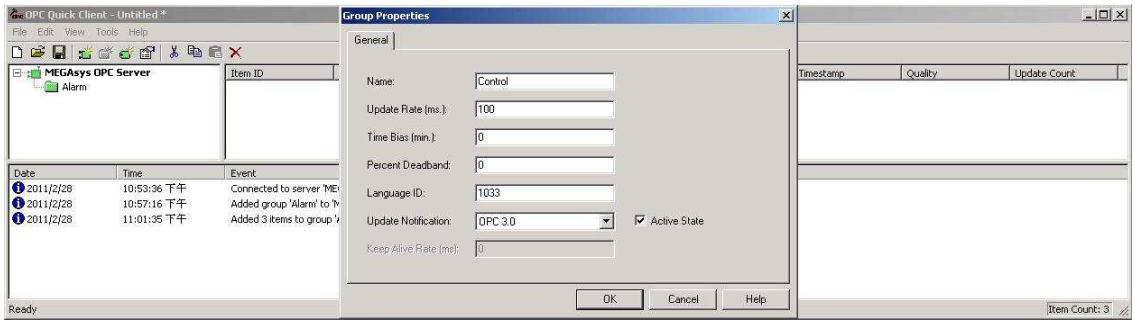
在視窗下方會顯示 “Added items …” 的資料。



<Setup-10>

完成第一組 Group 和 Item 的資料後, 如有其他 Group 需要加入, 可重覆以上的設定步驟。

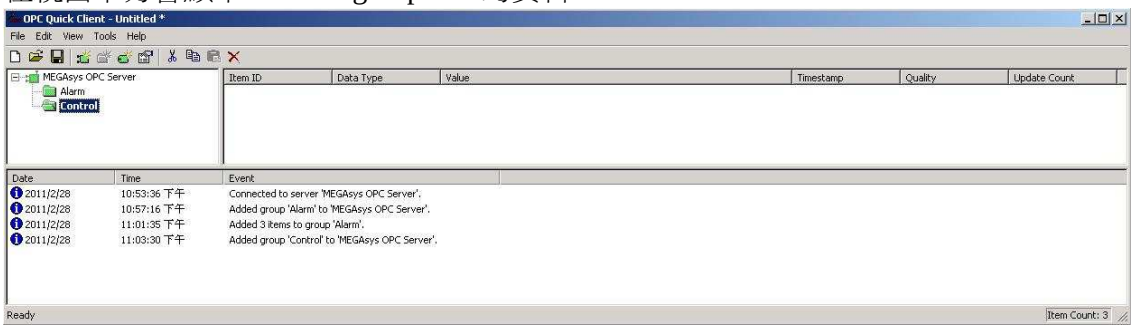
- 加入另一個 Group 資料。例如: Control group。
  - Name - Control 、Update Rate - 100、Update Notification – OPC 3.0。



<Setup-11>

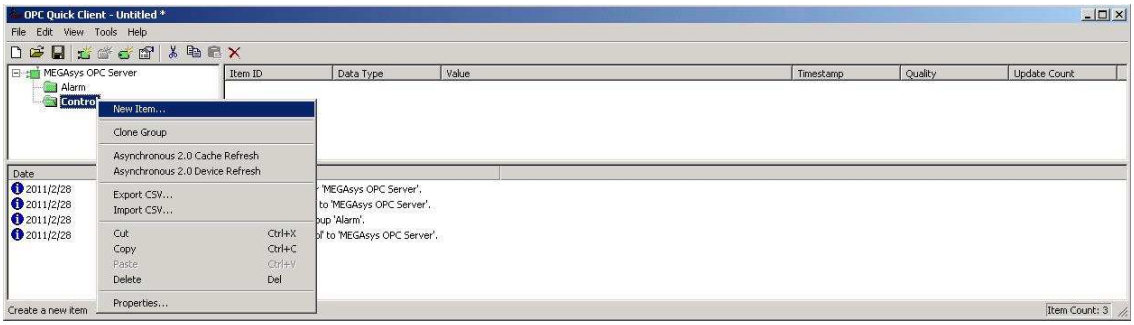
MEGAsys OPC Client 參數設定

在視窗下方會顯示 “Added group …” 的資料。

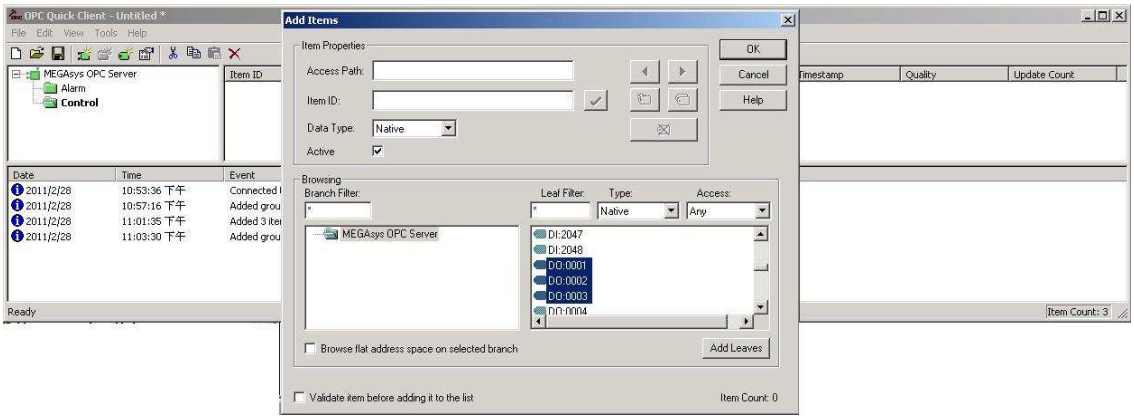


<Setup-12>

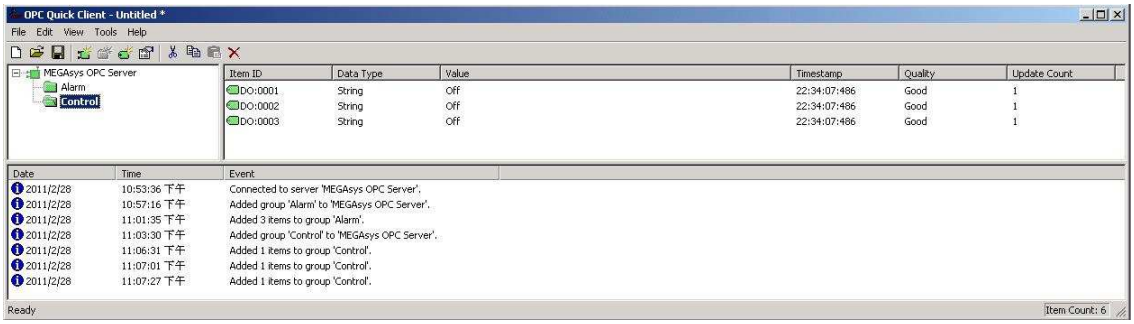
- 加入屬於 Control group 的 Item 資料。
- 在 Control 上按一下滑鼠右鍵, 選擇 “New Items…”。
- 選擇合適的 Point。例如: DO0001、DO0002 和 DO0003。



<Setup-13>



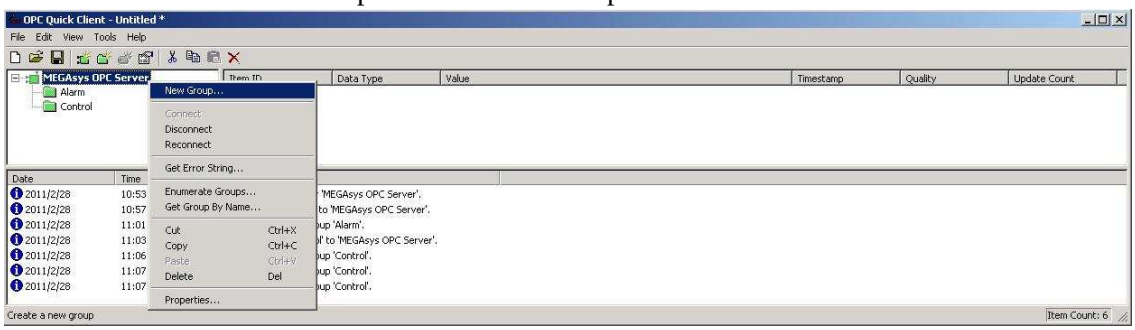
<Setup-14>



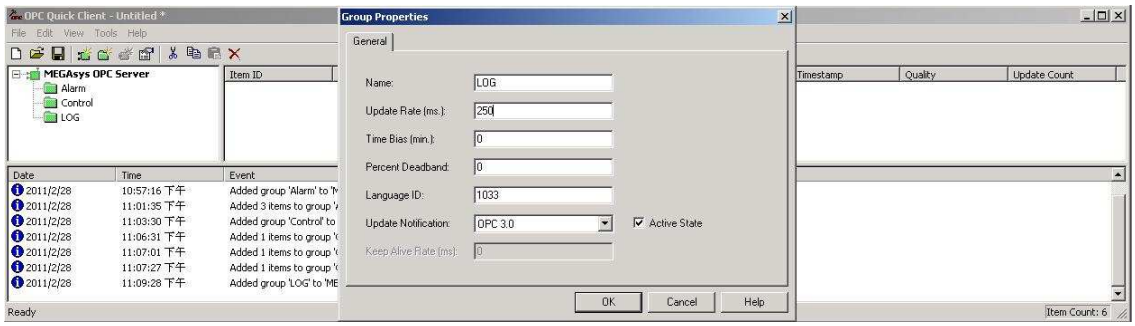
<Setup-15>

MEGAsys OPC Client 參數設定

- 加入下一個 Group 資料。例如: LOG group。
  - Name - LOG 、Update Rate - 250、Update Notification – OPC 3.0。



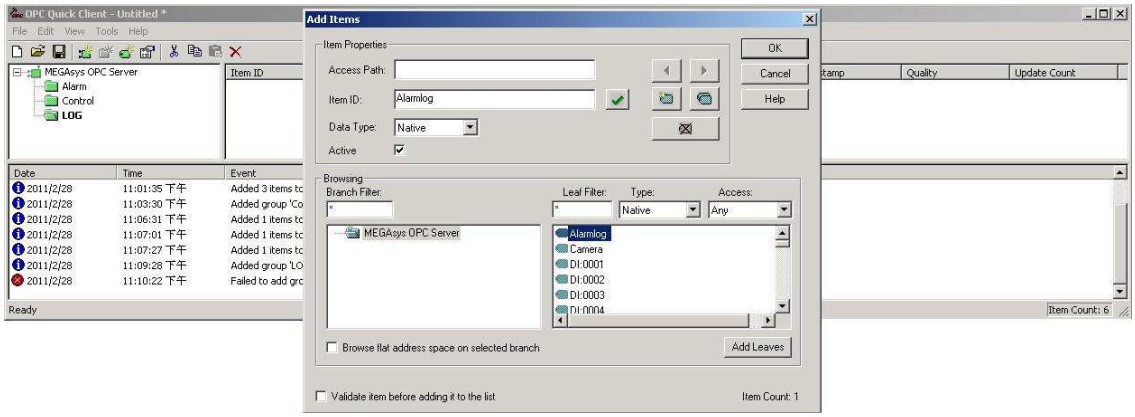
<Setup-16>



<Setup-17>

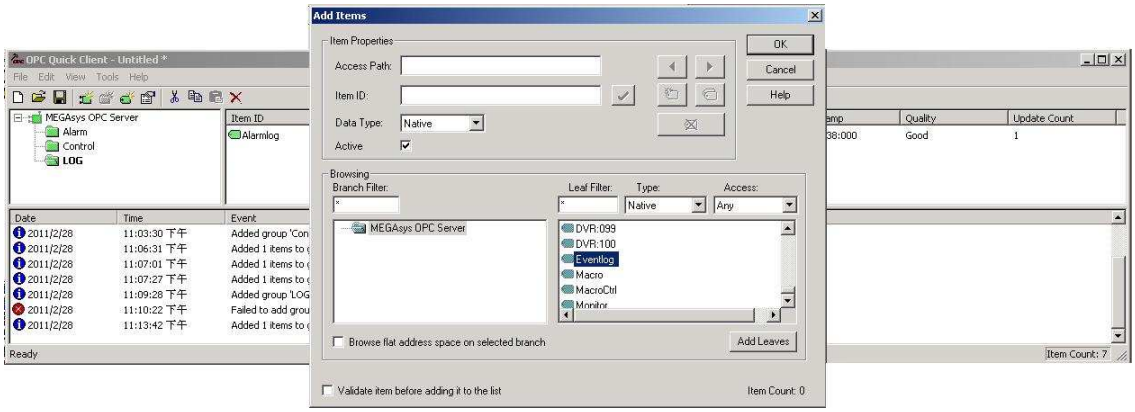
- 加入屬於 Control group 的 Item 資料。
- 點按 Add Item 鍵, 出現 'Add Item' 視窗。
- 選擇合適的 Point。例如: Alarmlog、Eventlog。

<Setup-18>



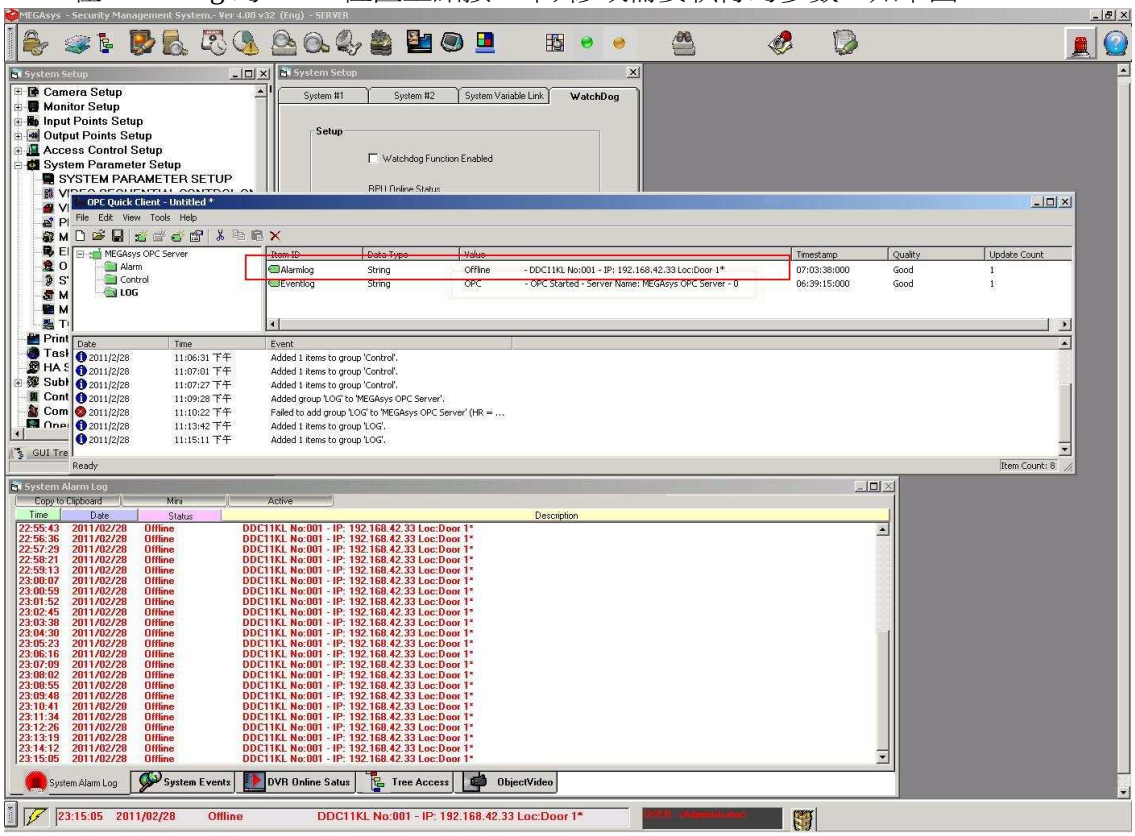
<Setup-19>

MEGAsys OPC Client 參數設定



<Setup-20>

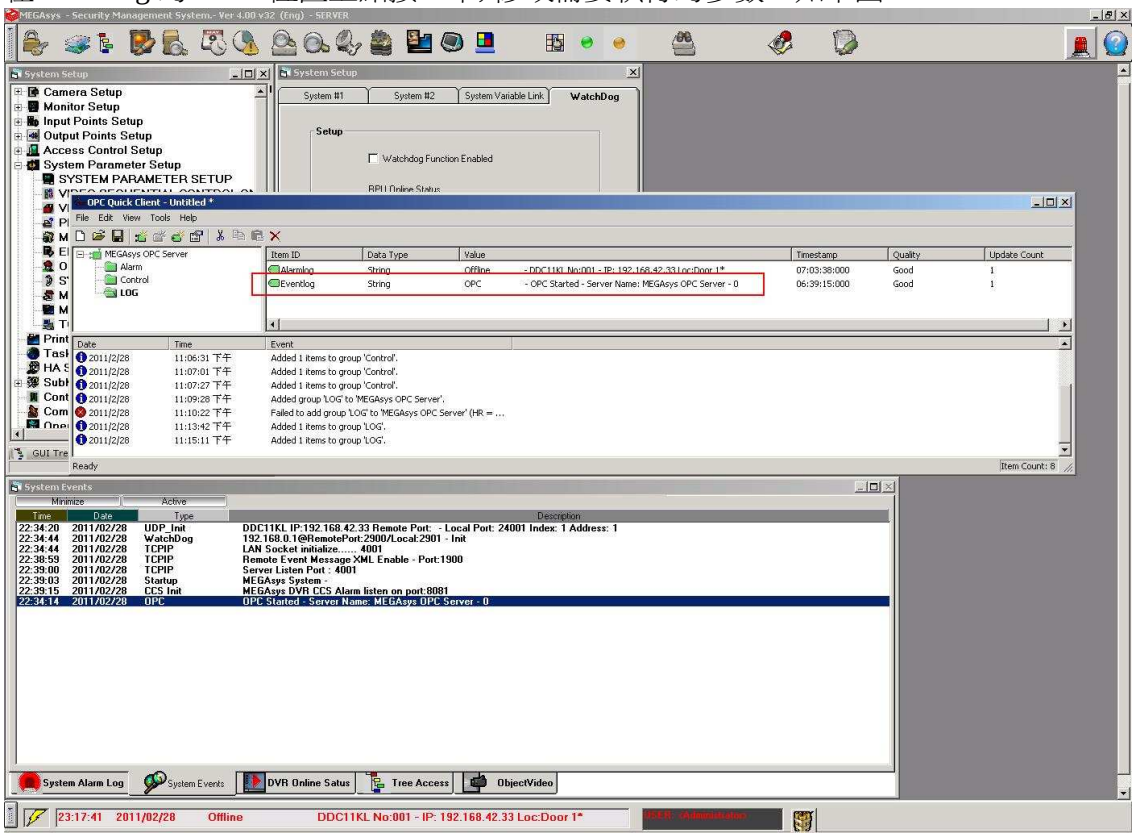
- 在 Alarmlog 的 value 位置上點按一下, 修改需要執行的參數。如下圖。



<Setup-21>

MEGAsys OPC Client 參數設定

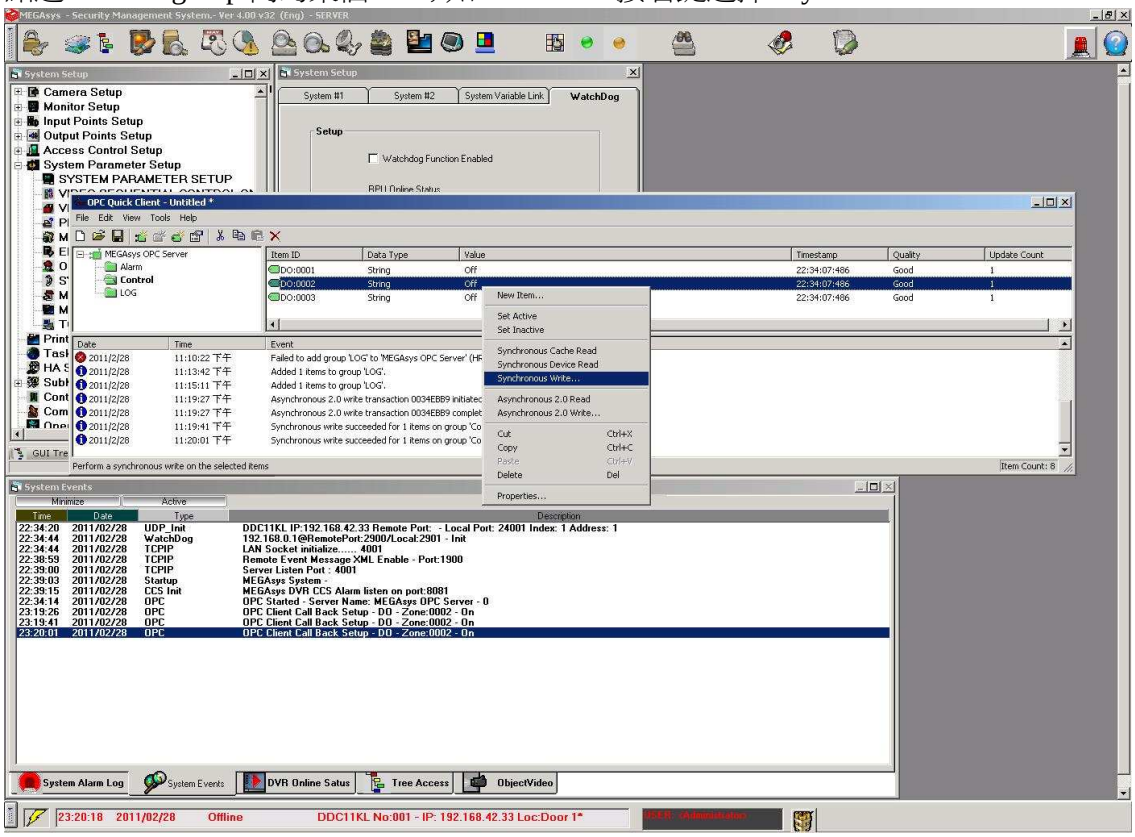
在 Eventlog 的 value 位置上點按一下, 修改需要執行的參數。如下圖。



<Setup-22>

MEGAsys OPC Client 參數設定

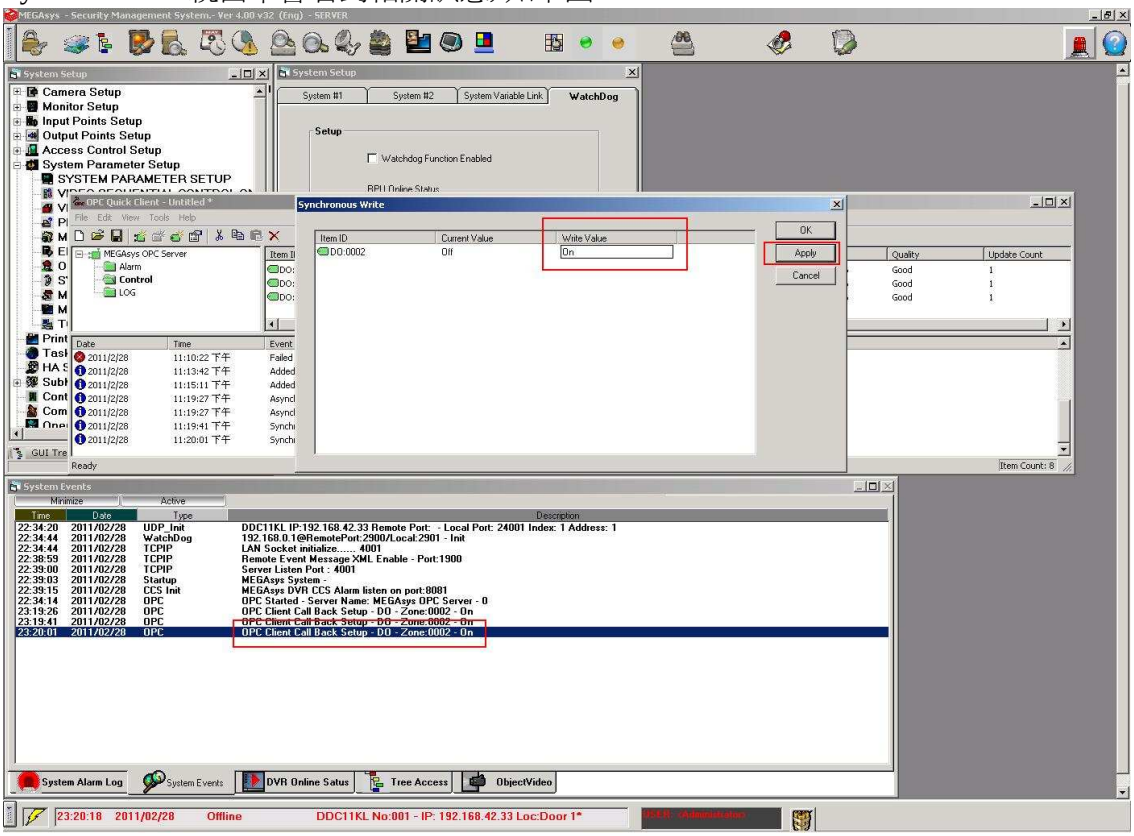
點選 Control group 內的某個 item, 如 DO0002。按右鍵選擇 'Synchronous Write'。



<Setup-23>

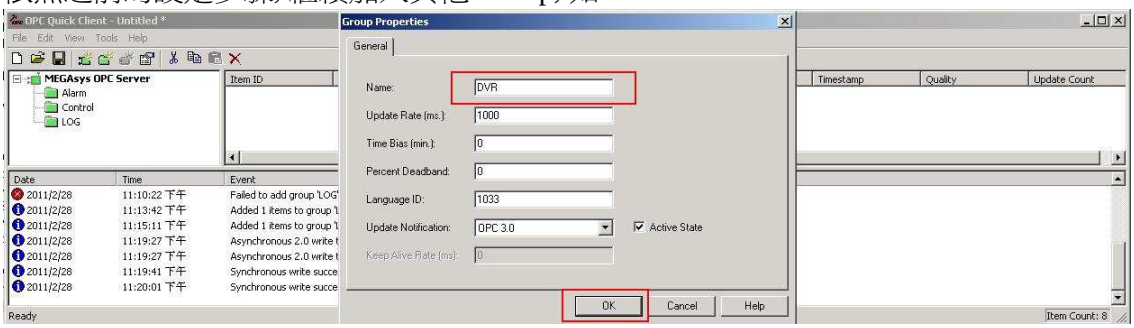
MEGAsys OPC Client 參數設定

在 Synchronous Write 視窗內修改參數。修改完畢後, 按 Apply 鍵便可。同時, 在 System Events 視窗中會看到相關訊息, 如下圖。

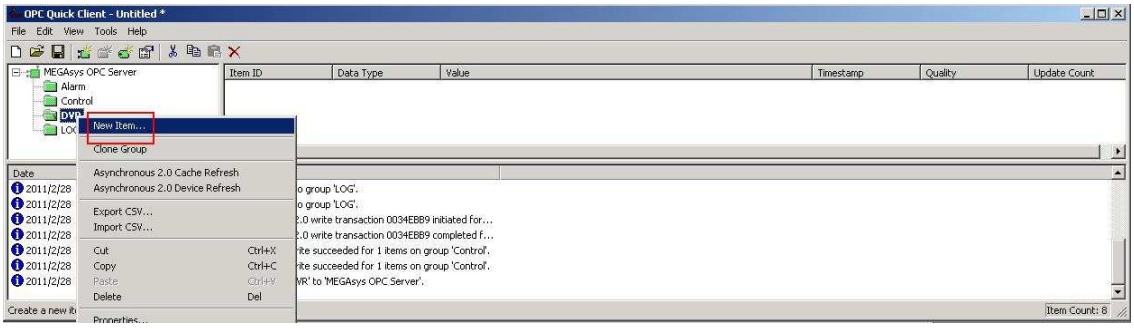


<Setup-24>

依照之前的設定步驟, 繼續加入其他 Group, 如: DVR。

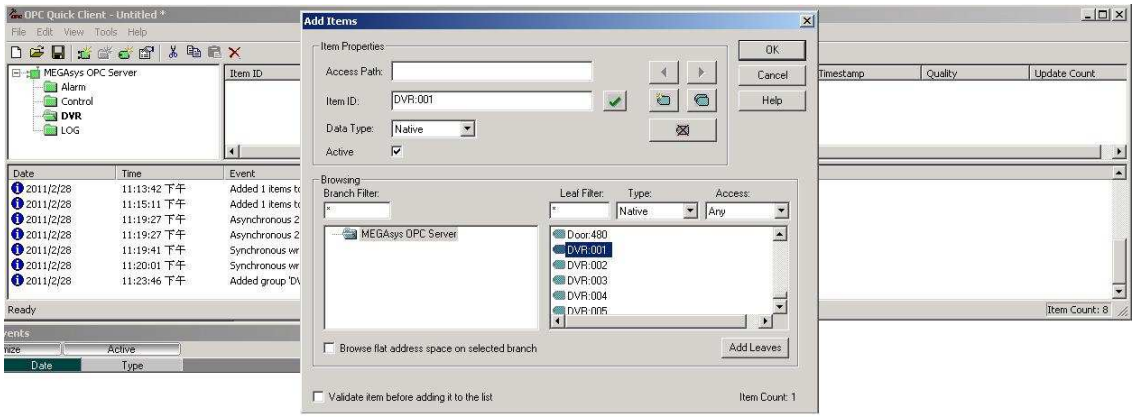


<Setup-25>

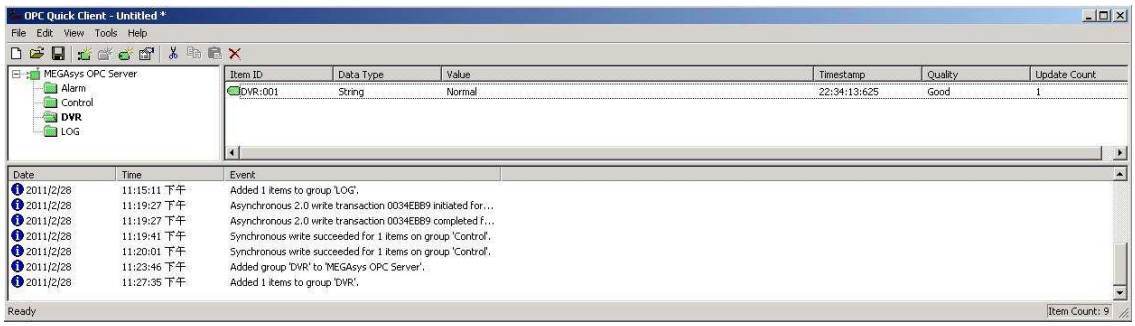


<Setup-26>

MEGAsys OPC Client 參數設定

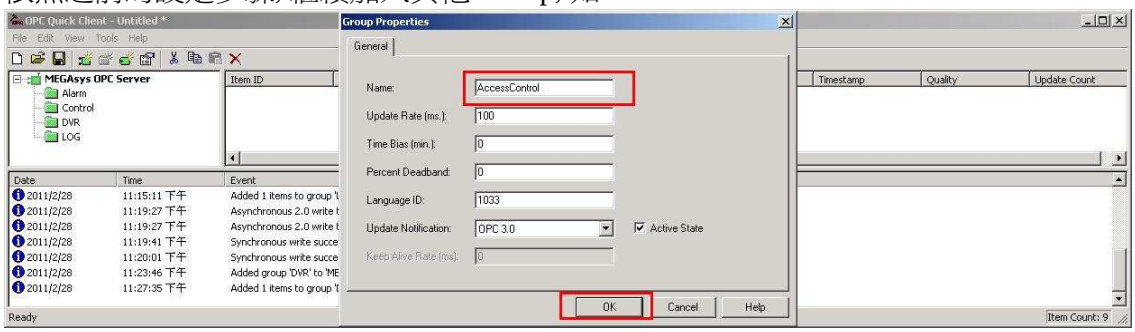


<Setup-27>

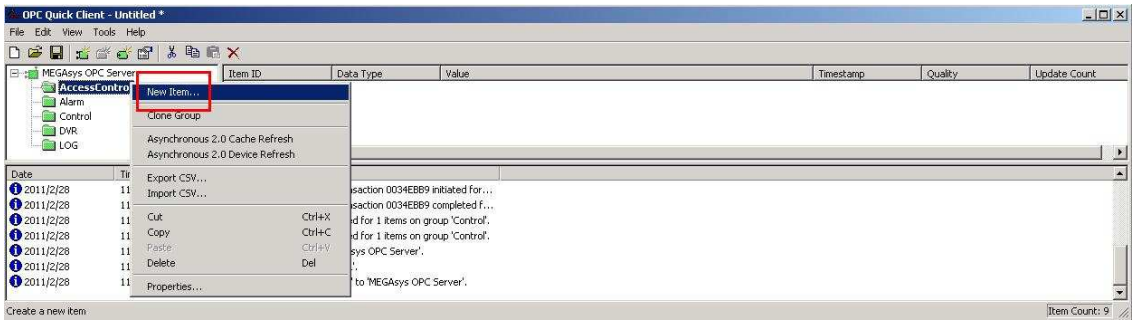


<Setup-28>

依照之前的設定步驟, 繼續加入其他 Group, 如: AccessControl。

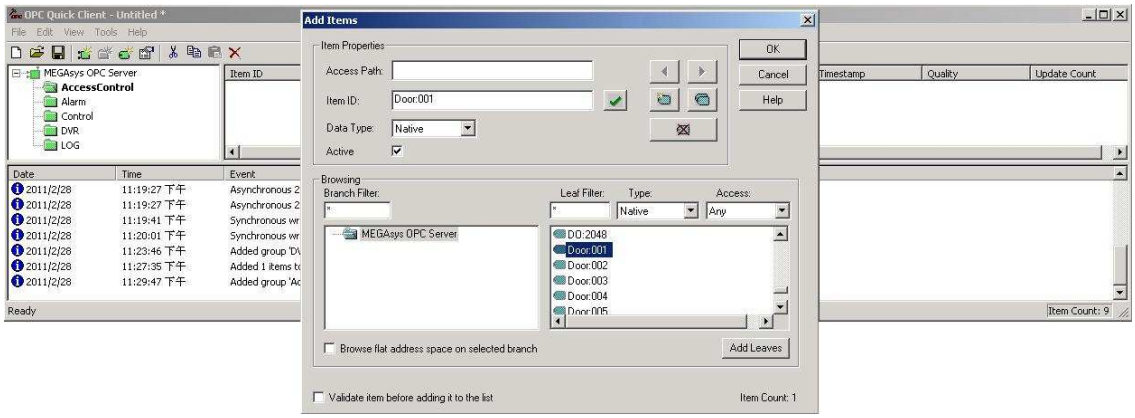


<Setup-29>

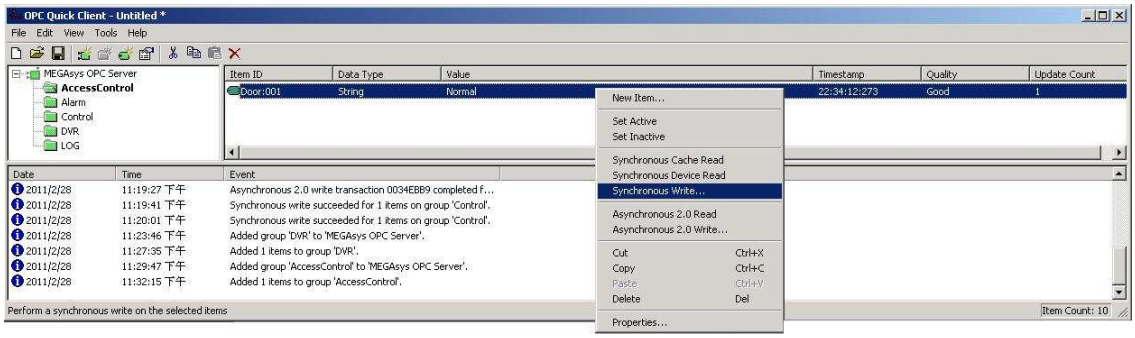


<Setup-30>

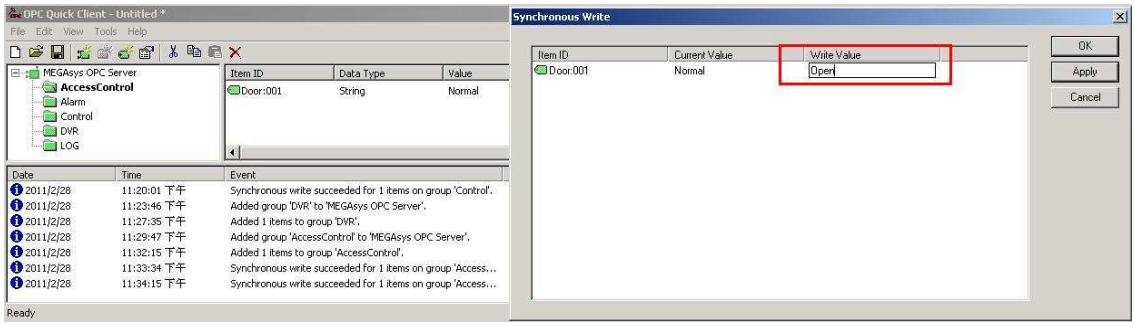
MEGAsys OPC Client 參數設定



<Setup-31>

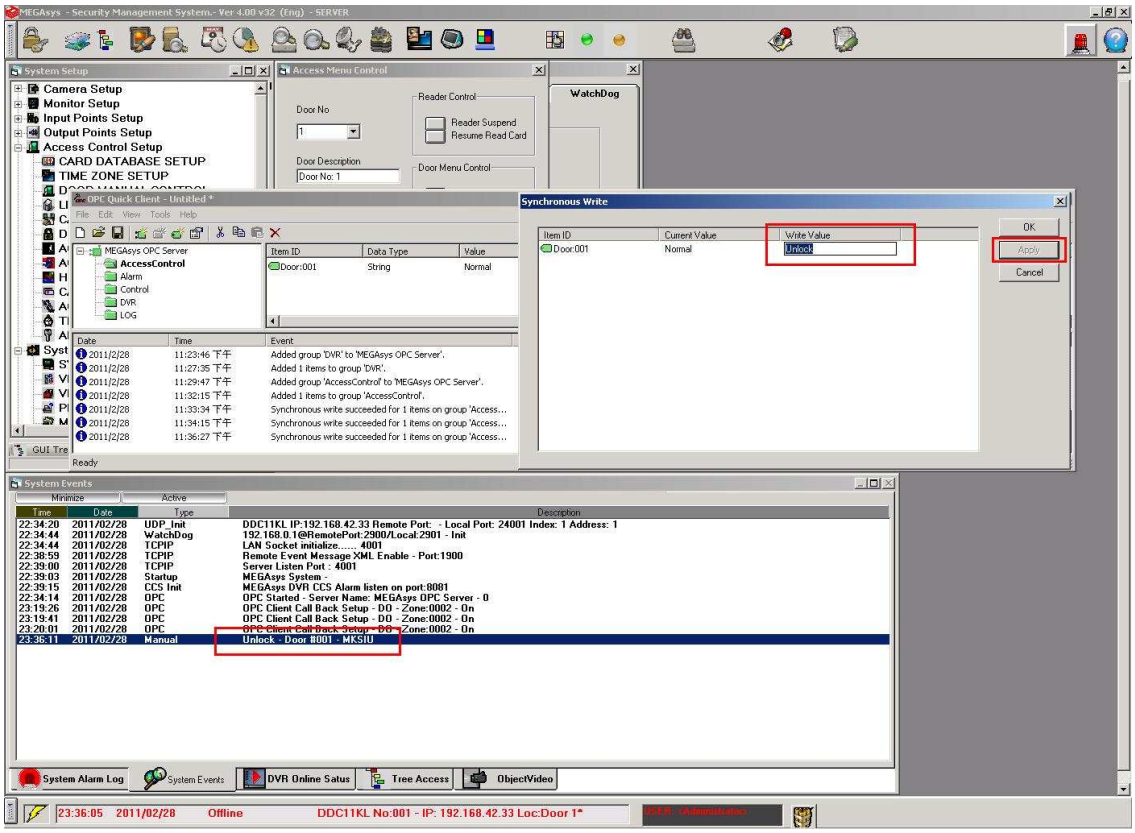


<Setup-32>



<Setup-33>

MEGAsys OPC Client 參數設定



<Setup-34>

APPENDIX A. DCOM Configure for Remote Client

DCOM Configuration Setup

This section is intended to provide general guidance on configuring DCOM settings for newer Operating Systems, which do differ slightly from Windows NT and 2000 Operating Systems.

This article will simply outline the steps to configure DCOM. If you would like to know and understand the reasons WHY some of these settings are so, then please read:

- NT/2000 User Security Permissions/Considerations
- Special considerations in multiple domain settings.

We will configure DCOM in 4 steps:

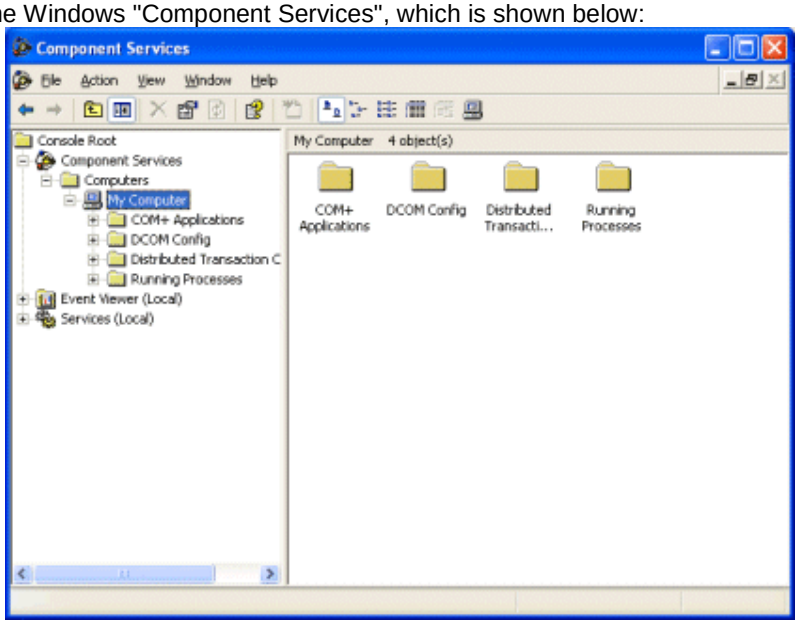
1. Configuring the general/default settings
2. Configuring the settings for OPCENUM
3. Configuring the settings for your OPC Server
4. Configuring the Local Security Policies

Starting DCOM Configuration

The DCOM Configuration utility can be accessed either in the Windows Control Panel -> Administrative Tools, or the Windows START button. To start it manually:

1. Click on the Windows START button
2. Click on the RUN option
3. Type "DCOMCNFG" (without the quotes) and press ENTER. (case does not matter)

This will load the Windows "Component Services", which is shown below:

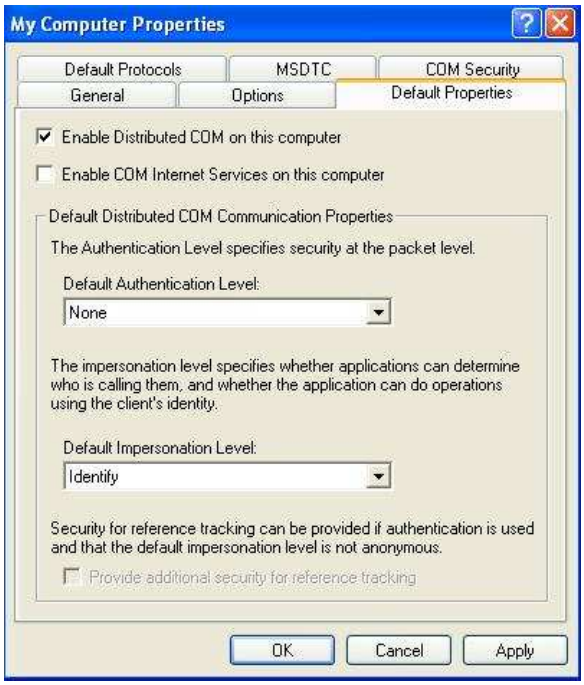


Step 1 - Configuring Default DCOM Security Options

The following screen is opened by:

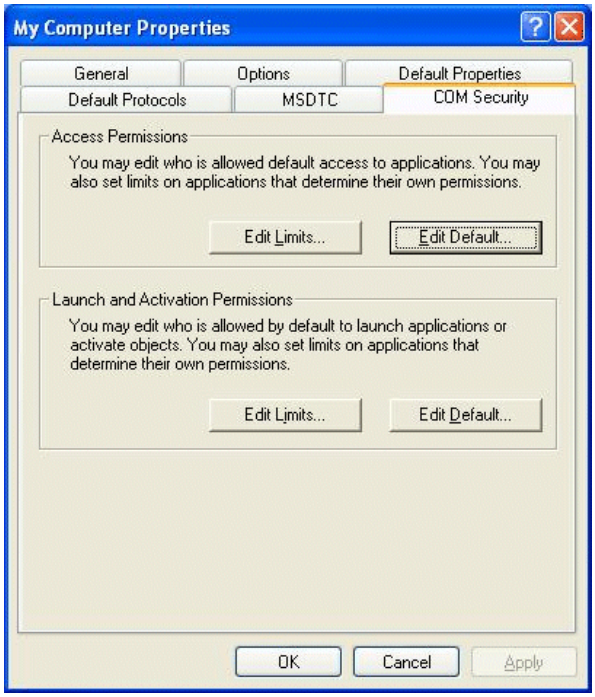
- Right-clicking on the "**My Computer**" node in the "Component Services" screen.
- Choosing "**Properties**" from the menu.
  Then click the "**Default Properties**" Tab.

MEGAsys OPC Client 參數設定



- The options available in this screen should be configured as:
  - The Enable Distributed COM on this computer MUST be checked.
  - The Default Authentication Level should be set to None.
  - The Default Impersonation Level should be set to Identity
- The next step is to click on the "**COM Security**" tab, which is shown below:

  As of XP SP2 there are four buttons in this screen. You **MUST** configure all four buttons.



  - Click on the "Edit Default" button within the "Access Permissions " area and make sure that the following accounts exist with the "Allow Access" permissions:
    - Everyone
    - Interactive
    - System
    - Network

- IWAM_<computer-name> *
- IUSR_<computer-name> *
- Guests
- Anonymous

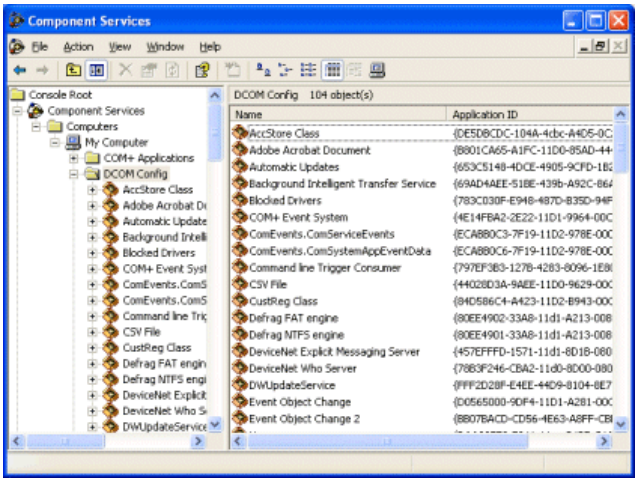
- Once that is complete, do the same with the "Edit Default" button in the " Launch Permissions" section and give the right "Allow Launch" to the same accounts as mentioned in the bullet-points above.
- Make the same settings under **both** "Edit Limits" buttons. If you do not set up these limits your DCOM will be limited based on these settings.

- Now click the OK button to save and close the window.

If you plan to use IIS (Internet Information Services) as an OPC Client, then its login context should be added to the list of trusted accounts as shown above.

Step 2 - Configuring DCOM Security Options for OPCENUM

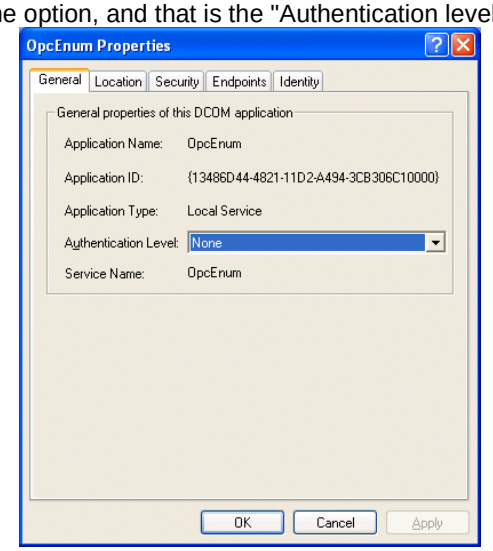
The next step is to locate OPCEnum in the list of COM components. Simply click on, or expand the "DCOM Config" section to show the objects available to configure:



Locate OPCEnum, and then open its properties by simply right-clicking on it, and choosing "Properties" from the menu.

General Tab

The General Tab has only one option, and that is the "Authentication level".

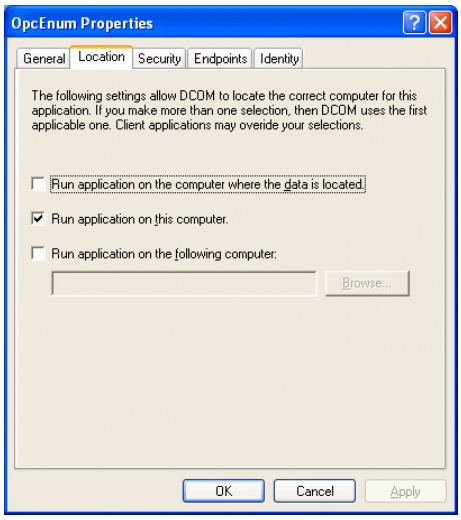


For each of use, you can select "None" as your option.

Location Tab

OPCEnum is a program that scans your registry for a list of OPC Servers on your computer.

MEGAsys OPC Client 參數設定



OPCEnum needs to run on the computer where it resides.. therefore the option of choice here is to check "**Run application on this computer**".

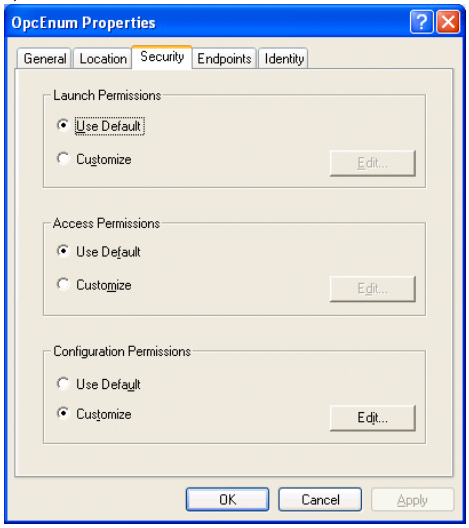
Security Tab

There are 3 options in the Security tab that need to be set.

Launch Permissions:
Select the option "Use Default".

Access Permissions:
Select the option "Use Default".

Configuration Permissions:
Select the option "**Customize** ", and then click the "**Edit**" button.



A window will open allowing to specify the accounts that do/don't have configuration permissions, simply add the same:

- *Network*
- *Interactive*
- *System*
- *Everyone*
- *Guests*
- *Anonymous*
- *IUSR_<computer-name> **
- *IWAM_<computer-name> **

Ensure that all of the accounts above receive "**Full Control**" rights.

* If you are using IIS (Internet Information Services) as an OPC Client.

Identity Tab

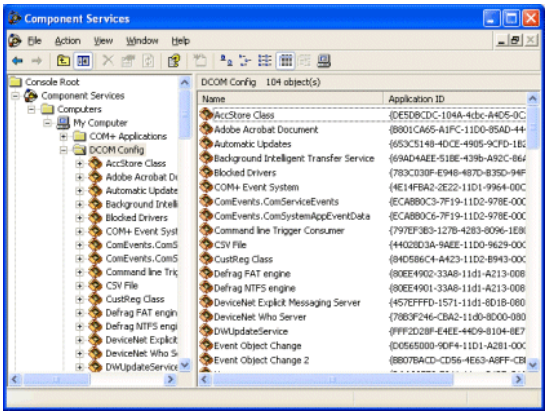
Use either the Interactive or System account.

Click OK to save and close the OPCENUM options window.

Step 4 - Configuring DCOM Security Options for the OPC Server

This step should only be followed if your computer has an OPC Server on it that you wish to allow OPC Clients to connect to.

At the "Component Services" window, click on or expand the "DCOM Config" node and locate your OPC Server from the list.



When you have found your OPC Server in this list, simply right-click on it and open its properties. Then follow the same steps as those listed for configuring OPCENUM.

Configuring Local Security Policy Settings

Overview

When making remote OPC connections there are some additional settings that should be checked. This is important when the two computers are not under the same domain when logged in.

Updates to newer operating systems have made changes to the local Policy settings and it is entirely possible that these updates have restricted systems that were otherwise once working.

This document assumes that all DCOM security settings are configured in accordance with our recommendations.

Local Security Settings

The settings outlined in this document must be checked on both the OPC Server and OPC Client computer(s).

The Local Security Settings can be found:

START > Control Panel > Administrative Tools > Local Security Settings

The Local Security Settings window is shown below:

Expand the Local Policies folder and go the Security Options (shown in gray).

DCOM Policies

Locate the following options:

- DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
- DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax

Both of these options should be set to "NOT DEFINED".
If either of these are defined, then you will need to work with an IT professional or network administrator who has the necessary rights to be able to access and modify these policies.

Network Access - Everyone Permissions

We need to to let Everyone permissions also apply to anonymous users. Locate the following options:

- Network access: Let Everyone permissions apply to anonymous users

These settings default to "disabled". We recommend enabling these options by right-clicking on them and changing the setting as shown below:

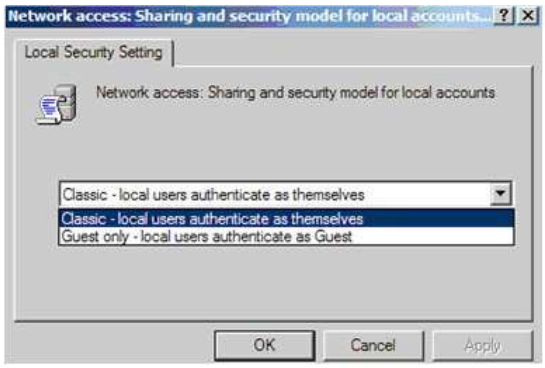
Click the OK button to save the setting and close the window.

Network Access - Sharing and Security Model

We need to configure the sharing and security model for local accounts. Locate the following options:

- Network access: Sharing and security model for local accounts

This setting now has a default value of "Guest only" which can prevent OPC connections. Right click on this policy and open its Properties:



Change the setting to "Classic" as shown above, then click OK to save and close the window.

Important Concepts and Examples Regarding Workgroups and Windows Domains

When configuring an OPC client and server to run on separate PCs, it is very important that you know whether the computers are running in a workgroup or in a domain. If you don't know how your PC's are setup, you will need to ask someone with Administrative rights and experience to look and see for you.

After reading this you should have a clear understanding of the **user account requirements** for your usage scenario. Setting up those user accounts is a function of your Windows administration and you or your system administrator will need to setup the user accounts.

Workgroups

If you will be using BOTH the OPC Client PC and the OPC Server PC in the SAME WORKGROUP, you will need to have the **same user account** setup on BOTH PCs with the **same password**.

Ideally you'd run the OPC Server and the OPC Client using the same user account, but if you cannot do that, then you'll have to make sure **both accounts are on each PC.**

Workgroups example:

OPC Client runs as local account "OPCClientUser" on Computer #1

OPC Server runs as local account "OPCServerUser" on Computer #2

The accounts "OPCClientUser" and "OPCServerUser" will have to exist on **both** computers as local accounts. Account "OPCClientUser" must have the same password on both PCs. Account "OPCServerUser" must have the same password on both PCs. The passwords for the two accounts "OPCServerUser" and "OPCClientUser" do not have to match.

Domains

Ideally if you are using computers that are in a Windows Domain, both computers will be in the same domain. If they are not in the same domain, you must setup a "trust relationship" between the two domains, which is outside the scope of this documentation.

If you are using domains, it is recommended that you **use domain user accounts** instead of local user accounts to run the OPC Server and the OPC Client. Some people don't realize that if they log into their PC as "JoeSmith" that is different from "MyDomain\JoeSmith". When logging into the PC or choosing user accounts in DCOM setup, be VERY CLEAR whether you are picking a domain account or local user account. If you do choose to use local user accounts, you have to be consistent and do that everywhere in all your DCOM settings.

The big difference in domains is that the Domain Controller will determine whether a user account name + password combination are valid or not. For that reason when using domain user accounts you **will not** go set user names and passwords on each PC in the domain. You will setup the accounts ONE TIME on the Domain Controller and then reference those domain accounts in your DCOM setup.

Workgroup to Domain Connections

Connecting workgroups to domains either client to server or server to client can be much more difficult to accomplish. For that reason we strongly recommend you do not try to do this unless your network and IT security setup constrains you.

The big thing to realize when trying to make workgroups interoperate with domains is that the workgroup has **no way to authenticate a domain user account!**

So to make workgroups and domains interoperate, you basically have to "fall back" to the workgroup to workgroup scenario and setup local user accounts on each PC. A couple of examples will help to illustrate this:

Example: OPC Client in Workgroup, OPC Server in Domain

Where this can get hard is if your OPC Server is setup to run as the interactive user, and the person logged in on the OPC server computer is using a domain account, and your OPC Client is in a workgroup, then the OPC Server will be running as a domain account user.

When subscription callbacks for data reads from the OPC server come back to the OPC client, the OPC Client PC will see the domain user account and say "I don't know you" and you won't get data.

The symptom of this will be that you can connect to the OPC Server, browse it, configure tags, but fail to get any data back from the OPC Server when it subscribes to tags.

The solution in this case would be to setup the OPC Server to run as a specific named local user on it's PC, instead of as the "interactive" user that is logged into the desktop which is a domain account. That specific named local user, if setup on the OPC Server PC in it's workgroup with the same password, would then be able to access the PC where the OPC Client is running.

Summary of requirements for this example to work:

- OPC Server must run as a local user account and that local user account must exist on the client and server PCs with the same username and password. This can be the same or a different local user account from the one used by the OPC Client.
- The OPC Client must run as a local user account on the client PC and that same local user account must exist on the OPC Server PC with the same username and password

- **Example: The OPC Client in Domain, OPC Server in Workgroup**
  The same concept applies if your OPC client is in a domain and the OPC Server is in a workgroup. The failure mode here though if you run the OPC Client under a domain account, is that the OPC Client won't connect to your OPC server PC, won't browse for servers, so you won't even be able to configure.

  The requirements for this example to work are identical to the prior Workgroup/Domain example above.

MEGAsys OPC Client 參數設定

User Permissions Considerations when setting up a DCOM Connection between An OPC Client and OPC Server

DCOM Tutorial Home

A key foundation for setting up a DCOM connection between two computers is to have the machines setup so that they have permission to access each other. This is a two way street. The client must have permissions to access the machine with the OPC server and vice versa. If you don't have permissions set both ways, then you will not have success. This article is not intended to be a substitute for good knowledge of the Microsoft Windows NT and Windows 2000 user accounts and security model. There are plenty of good books on the subject available at any local bookstore. This article is intended to point out some key things you need to have setup before you even try to configure a DCOM connection between an OPC client and an OPC server.

Types of Permissions:

There are some common types of permissions we discuss in our DCOM tutorial

- **Access** -- these permissions allow a client machine to connect to a server computer, retrieve a list of OPC servers and connect to a server. They also allow the OPC server to make what is known as a "callback" to your client. A callback occurs when you ask the OPC server to notify your client only when data changes. If you use these types of reads, sometimes called "subscription" or "exception" reads, then it is important that Access permissions be set right on the client machine.

- **Launch** - these permissions are what allows an OPC client application to start or "launch" an EXE running on the machine where the OPC server is located. There are 2 common EXEs that get launched: (1) OPCEnum.exe, a standard OPC common component that lists the available OPC servers on a machine and returns that list to a client and (2) the actual EXE that corresponds to the OPC server. For example, our TOP Server OPC server EXE is "servermain.exe", the INGEAR AB Server is "IGOPCAB.exe"

- **Configuration** - these permissions allow a remote client to change the configuration of the OPC servers setup in the registry - you should rarely have to touch these permissions and in fact should not unless you know what you are doing.

So, the most common permissions you will see us discuss are **Access** and **Launch** permissions.

Users and Groups:

This document is not meant to replace common books on NT/2000 security, but there are some key concepts we want to emphasize.

> ***Users:*** A user is a particular login name+password combination used to gain access to a machine running Windows NT/2000.
>
> ***Groups:*** A group contains one to many *users.* Groups are a useful way to combine a set of user accounts and grant them certain rights for access and launch. If the actual user names that you wish to have access to your OPC servers will change with any frequency, we recommend you use Groups when granting all rights. Then all you have to do is add/remove users from the Groups in the NT/2000 user manager and their rights to access OPC servers will carry along. Proper use of Groups, whether they be ones you create on your own or any of the NT/2000 default groups, is a great way to reduce your long term maintenance cost of the system
>
> ***Local Users/Groups:*** A Local user is an account that is known ONLY to the machine on which the account was setup. Likewise for a Local Group. If you need an account to have access to another machine, and the account is a Local User, you will need to create a Local user with the identical username+password on the remote machine. For this reason, we recommend running OPC Client - Server setups in a Domain if you can - the maintenance and setup is easier.

Domain Users/Groups: A Domain User account is one that can be used anywhere within an NT/2000 domain so long as the computer is a member of the domain. Authentication of the user is handled by a primary domain controller machine, thus allowing you to centralize your security management on the user/group level. A Domain Group is a group that is available to any computer that is a member of the domain. We recommend using Domain user accounts and Groups to setup your DCOM Config permissions when setting up OPC client/server connections-- the risk of problems is lower and the long term maintenance is much easier.

What's a Domain ?

In Windows NT there is the concept of a Domain (in in Win 2000 domains still applies, though the concept has been evolved to talk about Forests/Trees, something beyond the scope of this article). A domain is a group of machines that have reasons to need to be able to work together. For example, you might have the paint shop domain, the body shop domain, the accounting domain, the marketing domain, and sales domain in a large company. For the majority of their day to day work, the users in each domain need only to access the machines in their group but not others. The Windows NT concept of a Domain allows you to setup a Domain Server in the group and setup security in the Domain so that the users within the domain have common access to the Domain server and to some degree, to each other's machines. So for example, in the Paint Shop, you might have a Domain Server (also called a Primary Domain Controller or PDC in Microsoft-speak) and 10 Windows NT machines. When users login to their boxes, they log in to the Paint_Shop domain, which then gives them access to any shared resources (drives, printers, etc) in the Paint_Shop domain. Their user name and passwords are authenticated (validated, checked - pick your term) against a database of users stored on the Domain Server. Unless a special relationship called a "Domain Trust Relationship" has been setup, users in the Marketing domain would not have access to shared resources in the Paint_Shop domain. In a Domain Trust Relationship, the PDC (Primary Domain Controller) for the Paint_Shop domain agrees to trust the Marketing domain's users as if they were their own. Domain Trust relationships and their setup and maintenance is an advanced topic beyond this discussion - just be aware that if you have multiple domains, you have to be more careful with your access rights setup.

In Windows 2000, machines can still be a member of a Domain, but you can optionally also setup Windows 2000 machines to support the new Active Directory security model, a subject which is beyond the scope of this particular document.

Get in the Domain - if you can

Now that you have the idea of a domain, why does it matter to OPC? The primary benefit of both the OPC client computer and the OPC server computer being a member of a domain is that security is centralized. Both machines will trust accounts that are members of the domain, meaning their username/password combinations are found in the security database of the PDC machine. The downside is that if the PDC goes down, you might not be able to validate security after reboot of a machine in the domain until the PDC comes back. Fortunately you can have BDCs or "Backup Domain Controllers" in a Domain to decrease this risk.

When you run an OPC client application on an NT/2000 machine, that application, even if it is running as a service, has to run under some user name -- you'll hear this sometimes called "running in the context of user name JoeSmith" -- it means you are running the application as if it were launched after a user JoeSmith logged into that machine. The same applies to an OPC server -- it too runs under some user name or "context".

So if we have OPC client on machine A, running under username JoeSmith, and it wants to talk to an OPC server on machine B, that is running under the name BillJones, then DCOM security defaults require that JoeSmith have access to Machine B, and BillJones have access to MachineA. Without BOTH of those requirements met, you'll never get your DCOM connection to work, at least not without some major trickery that just isn't worth the hassle.

OK - so what -- how does a Domain help this situation ? Simple -- if Machine A and B are members of the Paint_Shop domain, and users JoeSmith and BillJones are both accounts in the domain Paint_Shop, then unless you have done something to abnormally restrict those user's rights (i.e. taken them out of the Domain Users group or other manual editing of rights), the permissions are already setup, you're done. This is because Machine A trusts the PDC of the Paint_Shop domain to advise it

that BillJones has access, and Machine B trusts the PDC of the Paint_Shop domain to advise it that JoeSmith has access.

Because of these relationships, getting an OPC client and OPC server on machines in the same domain is probably the easiest scenario.

No Domain - What do you do ?

If you don't have a domain, it's OK. The risk of the PDC or having to have a BDC to decrease that risk may be something your network design said doesn't work for you. If your NT/2000 machines are not members of a domain, then they are running as standalone machines. Every NT/2000 machine (even those in a domain) has it's own "local" database of trusted users. When a machine is not a member of the domain, the ONLY user accounts it will trust are those it finds in it's own "local" security database.

Here is how this can get you into trouble on setting up and OPC client to server connection. If machine A has an account JoeSmith and Machine B has an account BillJones, and that is all, then how can an OPC client running as JoeSmith on Machine A, gain access to an OPC server running as BIllJones on Machine B ? It can't -- when Machine B receives a request from the OPC client, embedded inside that request is the notation "this is from user JoeSmith on Machine A". Machine B says "I don't know any JoeSmith" and refuses the connection. The typical error message thrown is "Access Denied". A sure sign you have this issue is when you try to connect to a remote machine with an OPC client to browse available servers and you can't even connect to the machine through the browse dialog without getting and "Access Denied" error. That's a sure sign you have a permissions issue between your two boxes.

So what is the solution ? Well fortunately you can trick the boxes. All you need to do is create the EXACT SAME user account names AND passwords on BOTH BOXES. So on Machine A, you need to have an account JoeSmith AND BIllJones. On Machine B, you also need an account JoeSmith and BIllJones. The passwords for BOTH JoeSmith accounts MUST match. The passwords for the BillJones accounts must match on both boxes. JoeSmith and BillJones CAN have different passwords between the two account names, and should for good security measure. You should also make sure those accounts have identical access rights if you can.

Once you have that setup, when Machine A comes calling on Machine B with an OPC request and identifies himself as JoeSmith with some password (it's encrypted), Machine B will look in it's database, see the same accountname, the same password, and same "come on in request from Machine A". When Machine B goes to return it's data from the OPC server to the OPC client on machine B, the OPC server will go call Machine A as BillJones with a password -- Machine A will look in it's database, see that it has that account, and accept the call.

A good way to see if you have these permissions set right is to go to Network Neighborhood, browse from Machine A to Machine B and try to connect to Machine B. You may not have any shared folders or printers, but so what - if you can connect to the machine without error, even if no shared resources are available, you likely have solved the first phase of the Access permissions challenge, gaining access to the machine. Your next step would be to make sure that the users you've setup are granted the proper rights in the DCOM Config utility on the client side and server side.

We know this may sound like a lot but if you read over this a few times, think about the simple concept of Machine's A and B allowing people access to the machines, you can see why this permissions issue is so crucial to proper DCOM configurations and setup.

If you have your basic access permissions working (i.e. you can at least see the machine and see shared folders/shared printers), you can go on to DCOM Client setups or DCOM Server setups.

Configuring DCOM (Distributed COM) to Connect an OPC client to an OPC Server in multiple Domains.

Domain Trust Relationship Considerations

When you're going from one domain to another and browsing OPC servers, probably the biggest issue to be concerned with is domain trust relationships. When you have multiple domains, there are setups in BOTH domains that must be made so that Domain A trusts users from Domain B and vice versa. For DCOM to work properly you'd have to have the trust going both ways because there are DCOM calls going both ways and the security model will try and validate the security credentials of the user going both ways. It is beyond the scope of our free support to show users how to setup Domain Trusts, but the good news is any decent network administration book will address the issue.

Having said that, with Domain trusts setup properly, then you still have to have the Dcom permissions setup properly as we discuss in our Dcom Configuration appnote.

Software Toolbox Recommendations for Configuring DCOM

New DCOM Configuration Videos Available!!!

Having problems with "**Access Denied**" when trying to get your OPC Client/Server software communicating?

We have over 10 years of DCOM configuration and troubleshooting experience that we have tried to put within our DCOM tutorial.

Configuring DCOM

Windows 98, NT and 2000 DCOM Configuration	Windows XP, 2003, Vista, 2008 and Windows 7 - DCOM Configuration
Client side settings Server side settings • General settings • OPC Server Specific • OPCEnum settings	Introduction to DCOMCnfg 1. Default DCOM options 2. OPCEnum 3. OPC Server PC only 4. Local Security Policies Workgroups vs. Domains

Appendix B. OPC ITEM (Tag) name for MEGAsys

1) Alarm Input point
   Size: Points start from 0001 to 2048 (Max/Server)
   Name: **DI:0001**
   DI:0002
   -
   DI:2048
   Direction: From OPC MEGAsys Server and to MEGAsys OPC server
   Data: Normal/ACK/Alarm/Reset

2) Control Output Point
   Size: Points start from 0001 to 2048 zones for server
   Name: **DO:0001**
   DO:0002
   -
   DO:2048
   Direction: Form OPC server and to OPC Server (Input/Output)
   Data: On/Off

3) System Log
   Event log: All MEGAsys system event log
   Name: **Eventlog**
   Alarm log:All MEGAsys system alarm log
   Name: **Alarmlog**
   Direction:Form OPC Server (Input)
   Data: Refer MEGAsys Event/Alarm Log Data

4) System Macro Control
   Direct Macro control to MEGAsys Server
   Name: **MACRO**
   Direction: To MEGAsys OPC Server (Output)

   Name: **MacroCtrl**
   Direction: To MEGAsys OPC Server
   Control: On/Off switch the macro execute
   Data: Refer MEGAsys Macro Manual (All Macro Support)

5) CCTV Control
   Camera: Switch Camera for Matrix CCTV Control
   Name: **Camera**
   Size: 1 to 640 (Max/Server)
   Direction: To OPC Server (Output)
   Data: 1,2,3….640

   Monitor: Switch Control for Monitor Matrix CCTV Control
   Name: **Monitor**
   Size: 1 to 160 (Max/Server)
   Direction: To OPC Server (Output)
   Data: 1,2,3….160

DVR: DVR status message
Name: **DVR**
Size: 1 – 100 (Max/Server)
Direction: From MEGAsys OPC Server (Input)
Data: HD Fault/Cam n Fault/Cam Resume/HD Full/HD Resume/Cam Motion Alarm

6) Access Control System door control
Name: **Door:0001**
Door:0002
-
Door:0480 (Max/Server)
Size: 1-480 (Max/Server)
Direction: Form MEGAsys OPC Server and to MEGAsys OPC server
Command: On/Off (Door Open/Door Close)
Data: Unlock/Lock/Open/Close/Open Too Long Alarm/Unlock all Card/Resume All card