

DCOM Settings

Start Up Document
English

Beijer Electronics OPC Server Setup

Foreword

This document describes how to set up the DCOM (Distributed Component Object Model) settings in a Windows XP environment in order to communicate using Beijer Electronics OPC Server. It is also supported to use an iX Panel from Beijer Electronics as DCOM client.

Order no: SUEN281

Copyright © 2011-04 Beijer Electronics AB. All rights reserved.

The information in this document is subject to change without notice and is provided as available at the time of printing. Beijer Electronics AB reserves the right to change any information without updating this publication. Beijer Electronics AB assumes no responsibility for any errors that may appear in this document. All examples in this document are only intended to improve understanding of the functionality and handling of the software. Beijer Electronics AB cannot assume any liability if these examples are used in real applications.

In view of the wide range of applications for this software, users must acquire sufficient knowledge themselves in order to ensure that it is correctly used in their specific application. Persons responsible for the application and the equipment must themselves ensure that each application is in compliance with all relevant requirements, standards, and legislation in respect to configuration and safety. Beijer Electronics AB will accept no liability for any damage incurred during the installation or use of this software. Beijer Electronics AB prohibits all modification, changes, or conversion of the software.

Contents

1	Introduction	4
1.1	System Requirements	4
2	Server Setup	5
2.1	Prerequisites	5
2.2	Configuring Windows Firewall	5
2.3	Setting Up User Account Recognition	8
2.4	Running OPCEnum as a Service	9
2.5	DCOM Configuration of My Computer	10
2.5.1	Default Properties	12
2.5.2	Default Protocols	13
2.5.3	COM Security	14
2.6	DCOM Configuration of Beijer Electronics OPC Server	16
2.6.1	General	17
2.6.2	Location	18
2.6.3	Security	19
2.6.4	Identity	20
2.7	DCOM Configuration of OPCEnum	21
2.7.1	General	21
2.7.2	Location	22
2.7.3	Security	23
2.7.4	Identity	24
2.8	Restarting the PC	24
3	Client Setup	25
3.1	Prerequisites	25
3.2	Configuring Windows Firewall	25
3.3	Setting Up User Account Recognition	25
3.4	DCOM Configuration of My Computer	26
3.4.1	Default Properties	27
3.4.2	COM Security	28
3.5	Restarting the PC	28
4	iX Panel Setup	29
5	Identity Options Description	30
5.1	The Interactive User	30
5.2	The Launching User	31
5.3	This User	31
5.4	The System Account (Services Only)	32

1 Introduction

This Start Up document describes how to set up DCOM (Distributed Component Object Model) settings for two computers, where one acts as DCOM server with Beijer Electronics OPC Server installed, and the other one as DCOM client. It is also supported to use an iX Panel from Beijer Electronics as DCOM client.

1.1 System Requirements

The following operating system and software is required:

Operating system/ software specification	DCOM server	DCOM client
Microsoft Windows XP, SP3, Windows Update enabled	Required	Required if using a PC as client
Beijer Electronics OPC Server	Required	Not required

2 Server Setup

2.1 Prerequisites

Beijer Electronics OPC Server has to be installed on the PC acting as server.

This chapter describes the following required server settings:

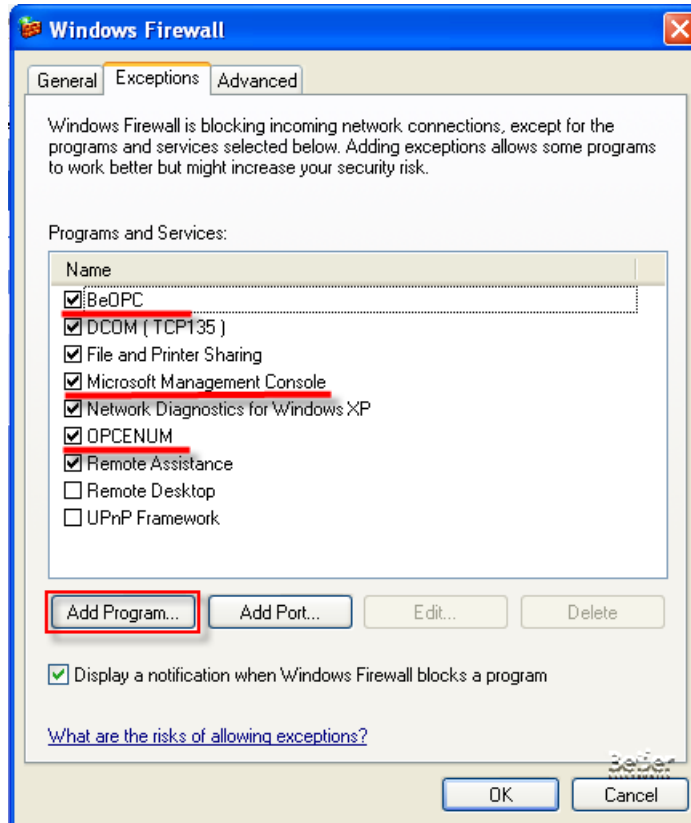
- [*Configuring Windows Firewall*](#)
- [*Setting Up User Account Recognition*](#)
- [*Running OPCEnum as a Service*](#)
- [*DCOM Configuration of My Computer*](#)
- [*DCOM Configuration of Beijer Electronics OPC Server*](#)
- [*DCOM Configuration of OPCEnum*](#)

Related information
<i>System Requirements</i>

2.2 Configuring Windows Firewall

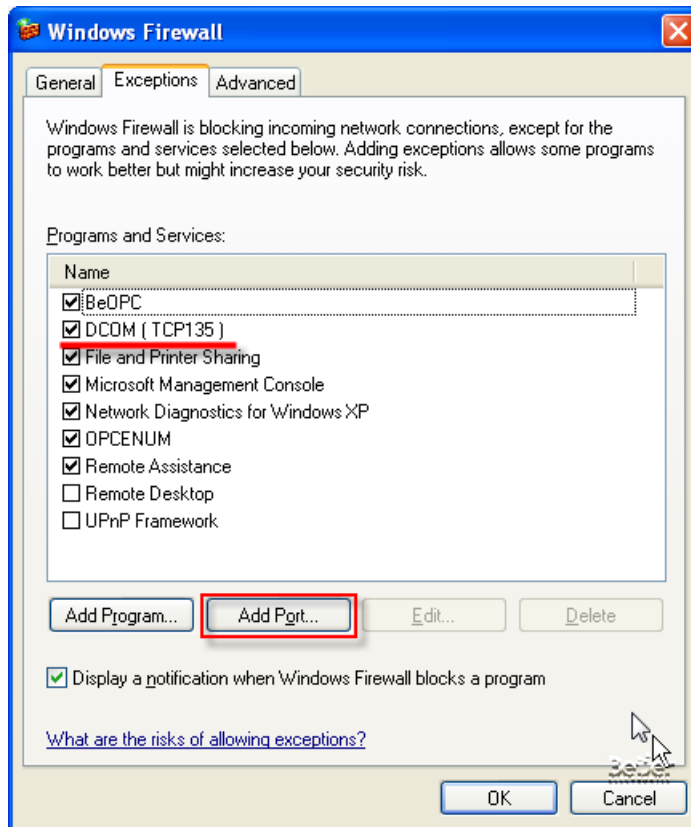
1. Open Windows Firewall from the Control Panel.

2. Select the **Exceptions** tab and add **BeOPC** (Beijer Electronics OPC Server) to the exceptions list. Also add **Microsoft Management Console** (mmc.exe) and the OPC utility **OPCENUM** (OPCEnum.exe) found in the Windows\System32 directory.



Most applications that are installed on the PC are listed when clicking **Add Program**. To find executable files that are not listed, click **Browse**.

3. Click **Add Port**.



4. In the **Add Port** dialog, fill in the fields according to below:
- Name: **DCOM (TCP135)**
 - Port number: **135**
 - Choose the **TCP** radio button.
5. Select the **Advanced** tab of the Windows Firewall, and enable **Allow incoming echo requests**, found in **Settings for ICMP**.

2.3 Setting Up User Account Recognition

To enable both computers to properly recognize each other's user accounts, it is necessary to ensure that user accounts are recognized on both the server as well as the client computers. This includes all user accounts that will require OPC access.

1. Make sure that all user names and passwords on the DCOM server and DCOM client match for all accounts that require OPC access.

Note:

A user account must have a user name and a password. It is not possible to establish communication if a user account does not have a password.

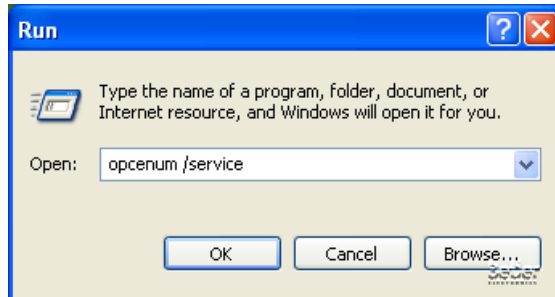
When using Windows Workgroups, each computer must have a complete list of all user accounts and passwords.

When using a single Windows domain, user accounts are properly synchronized by the domain controller.

When using multiple Windows domains, you will either have to establish a trust between the domains, or add a local user account to the computers that will communicate via DCOM.

2.4 Running OPCEnum as a Service

1. Click on the Windows **Start** button, and select **Run**. In the Run dialog box, type “**opcenum /service**” and click **OK**.



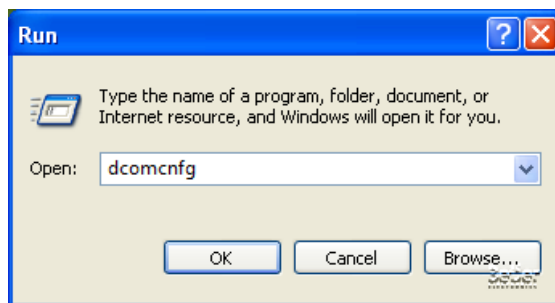
2. Click on the Windows **Start** button, and select **Run** once again. In the Run dialog box, type “**dcomcnfg**” and click **OK**.
3. Open the Control Panel and select **Services (local)**.
4. Right-click on the OpcEnum service and select **Properties**.
5. Change start type to **Automatic**.
6. If the service is not already running, click **Start**.
7. Click **OK** to close Services.

2.5 DCOM Configuration of My Computer

OPC specifications that precede OPC Unified Architecture (OPC UA) depend on Microsoft's DCOM for the data transportation. Consequently, you must configure DCOM settings properly. It is possible to configure the default system-wide DCOM settings, as well as for a specific OPC server. The system-wide changes affect all Windows applications that use DCOM, including OPC applications. In addition, since OPC Client applications do not have their own DCOM settings, they are affected by changes to the default DCOM configuration.

To make necessary changes, follow the steps below:

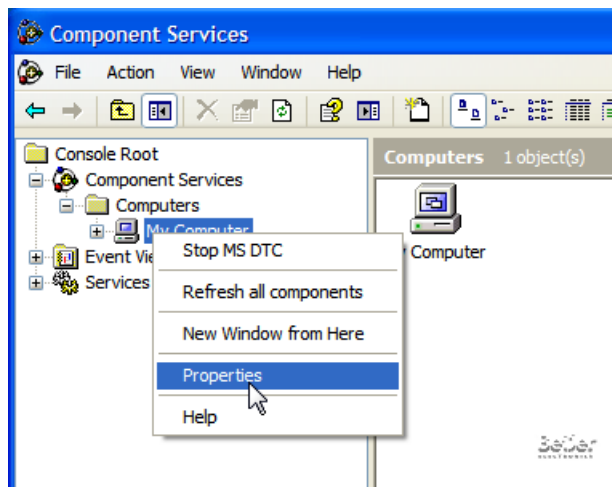
1. Click on the Windows **Start** button, and select **Run**. In the Run dialog box, type "**dcomcnfg**" and click **OK**.



The Component Services window opens.

2. In the Component Services window, navigate inside the Console Root folder to the Component Services folder, and then to the Computers folder. Finally, you will see the My Computer tree control inside the Computers folder.

3. Right-click on **My Computer** and select **Properties**.



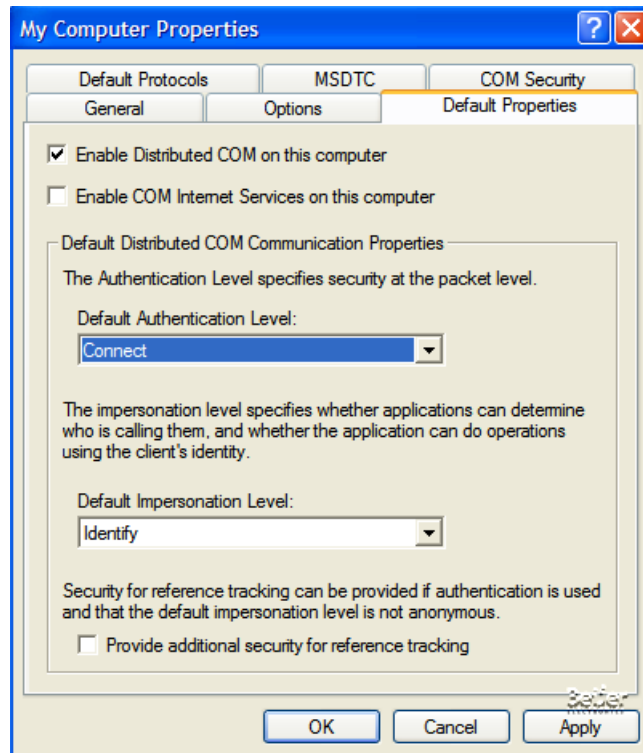
Note:

This is not equivalent to the “My Computer” icon on your desktop; but the “My Computer” tree control in the Component Services application.

2.5.1 Default Properties

Make sure that the following options are set on the Default Properties tab:

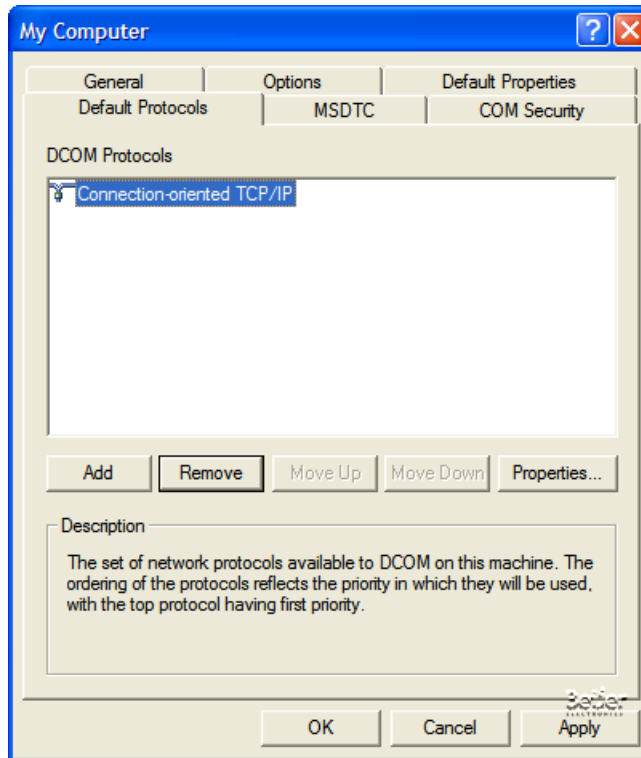
1. Check **Enable Distributed COM on this computer**. Note, that you will have to reboot the computer if you make changes to this check box.
2. Set the Default Authentication Level to **Connect**. It is possible to use other settings in the list, but the Connect option is the minimum level of security that you should consider.
3. Set the Default Impersonation Level to **Identify**.



2.5.2 Default Protocols

Make the following setting on the Default Protocols tab:

1. Set the DCOM Protocols to **Connection-oriented TCP/IP**.

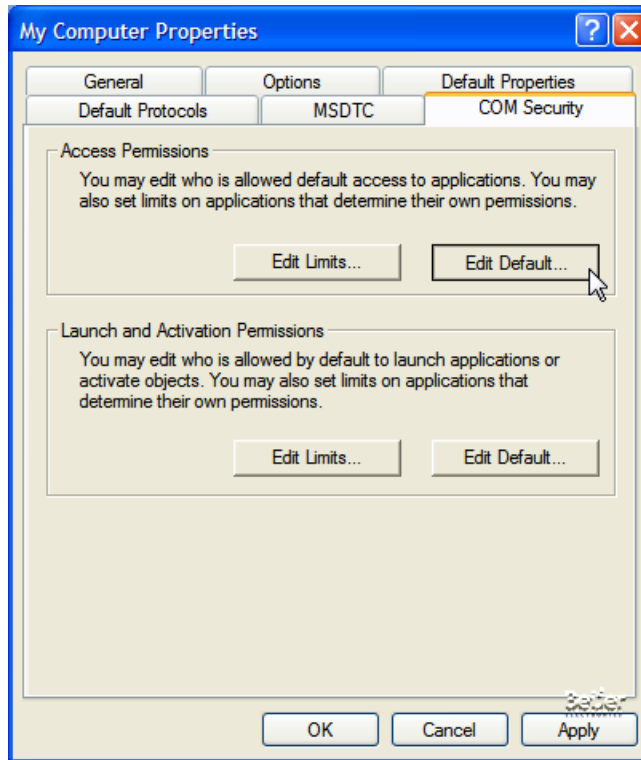


OPC communication only requires connection-oriented TCP/IP, so you may consider to delete the rest of DCOM protocols. However, if these protocols are required for non-OPC applications, you can leave them there. The only consequence is that timeouts may take a little longer to reach.

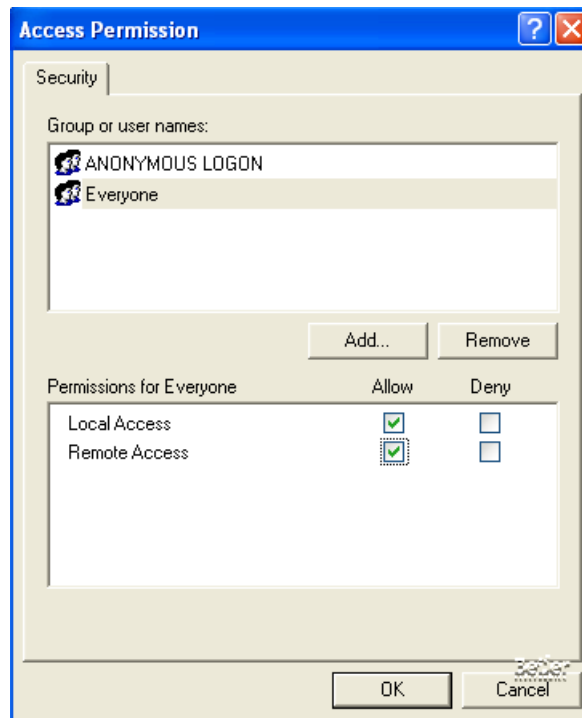
2.5.3 COM Security

In Windows, the system-wide Access Control List (ACL) is configured for all objects on the COM Security tab. The ACLs include Launch and Activation Permissions (ability to start an application), and Access Permissions (ability to exchange data with an application).

Make the following settings on the COM Security tab:



1. Click **Edit Limits...** for the Access Permissions group. Add **Everyone** and **ANONYMOUS LOGON** to the list of Group or user names. Change their permissions to **Allow**, and click **OK**.



2. Click **Edit Limits...** for the Launch and Activation Permissions group. Add **ANONYMOUS LOGON** to the list of Group or user names. Change its permissions to **Allow**.
3. Change the permissions for **Everyone** to **Allow**.
4. Click **OK**.

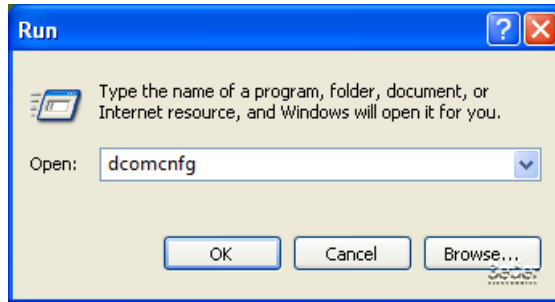
Note:

On some computers, the Edit Limits buttons may not be available.

2.6 DCOM Configuration of Beijer Electronics OPC Server

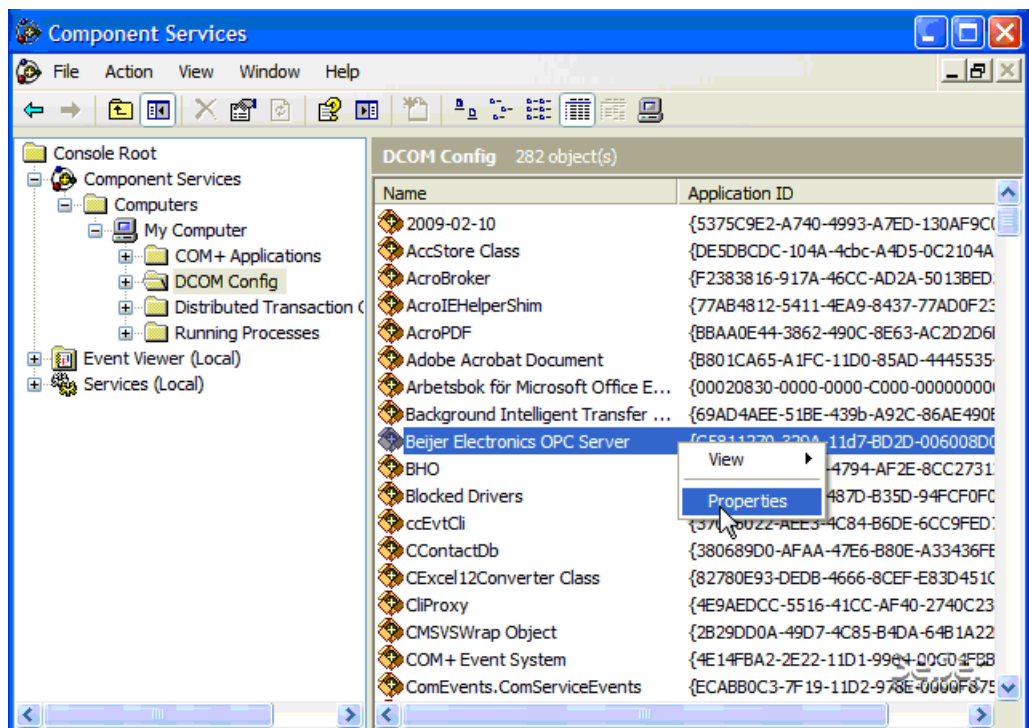
To make necessary changes, follow the steps below:

1. Click on the Windows **Start** button, and select **Run**. In the Run dialog box, type “**dcomcnfg**” and click **OK**.



The Component Services window opens.

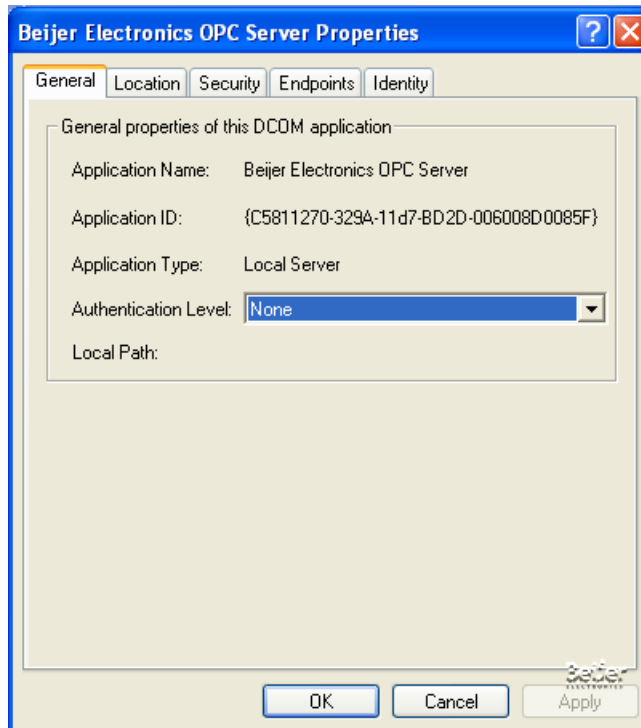
2. In the Component Services window, navigate inside the Console Root folder to the Component Services folder, and then to the Computers folder. Expand My Computer and click on the DCOM Config folder.
3. Right-click on Beijer Electronics OPC Server in the list of objects in the right window pane, and select **Properties**.



2.6.1 General

Make the following setting on the General tab:

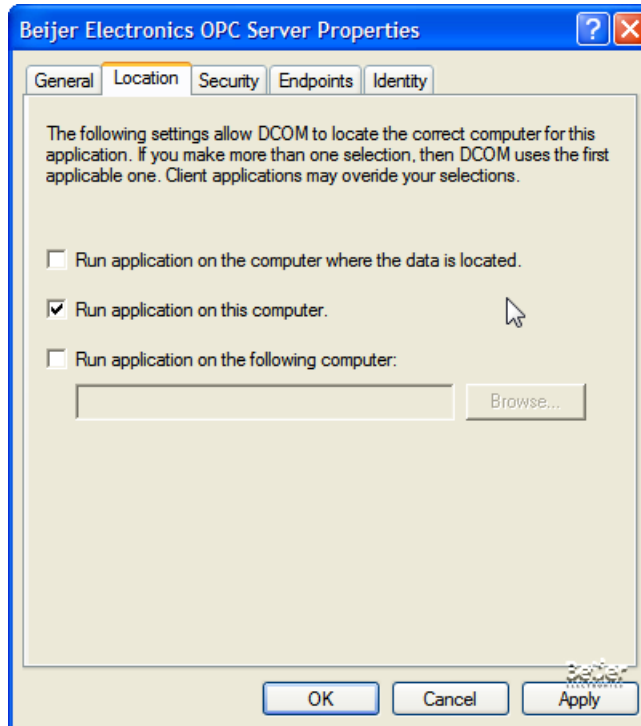
1. Set Authentication Level to **None**.



2.6.2 Location

Make the following setting on the Location tab:

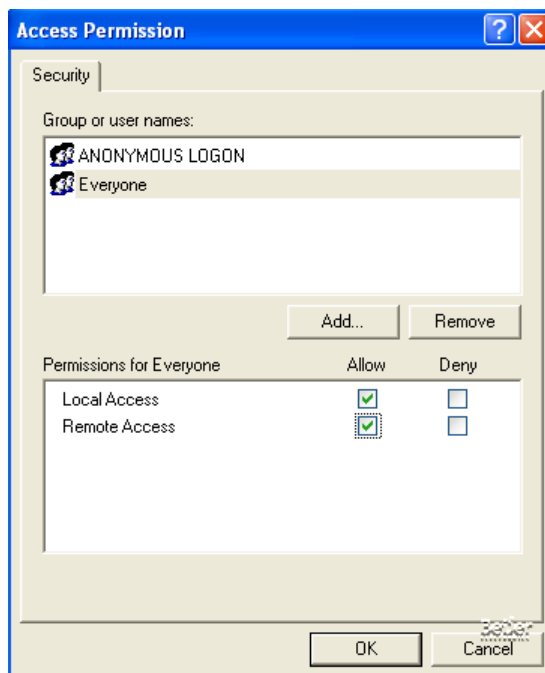
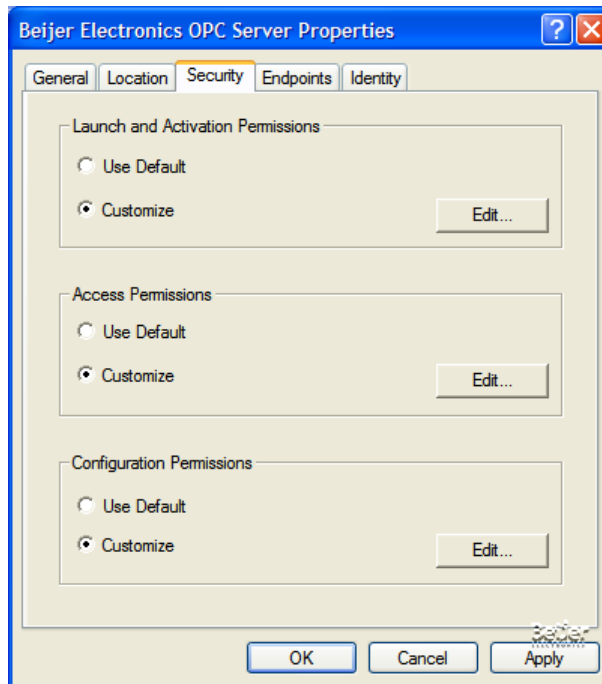
1. Check **Run application on this computer**.



2.6.3 Security

Make the following settings on the Security tab:

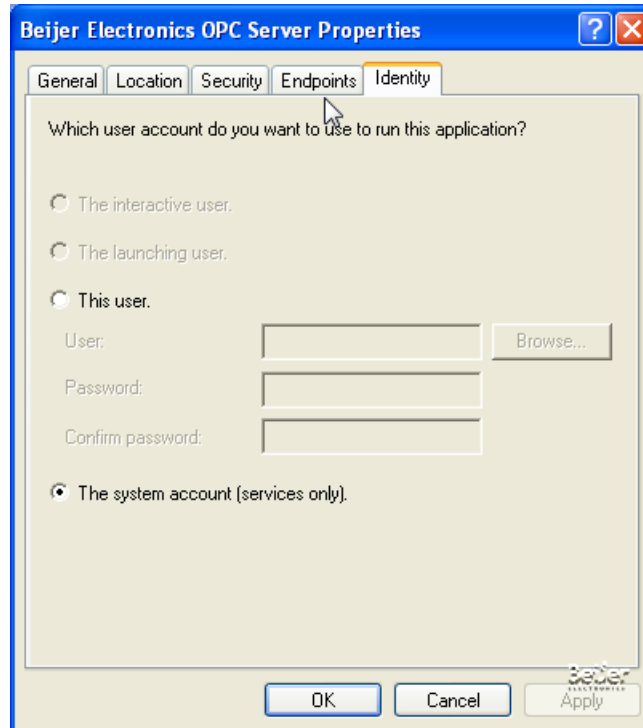
1. Select **Customize** and click **Edit** for Launch and Activation Permissions, Access Permissions and Configuration Permissions, and add **Everyone** and **ANONYMOUS LOGON** to the list of Group or user names. Change their permissions to **Allow** and click **OK**.



2.6.4 Identity

Make the following setting on the Identity tab:

1. Select the **The system account (services only)** option, and click **OK**.



Note:

The system account option is available only if the Beijer Electronics OPC Server is started as a service. If this option is greyed out, make settings as described in section [The System Account \(Services Only\)](#). After that, a restart may be required in order for the system account option to become available.

Related information
Identity Options Description

2.7 DCOM Configuration of OPCEnum

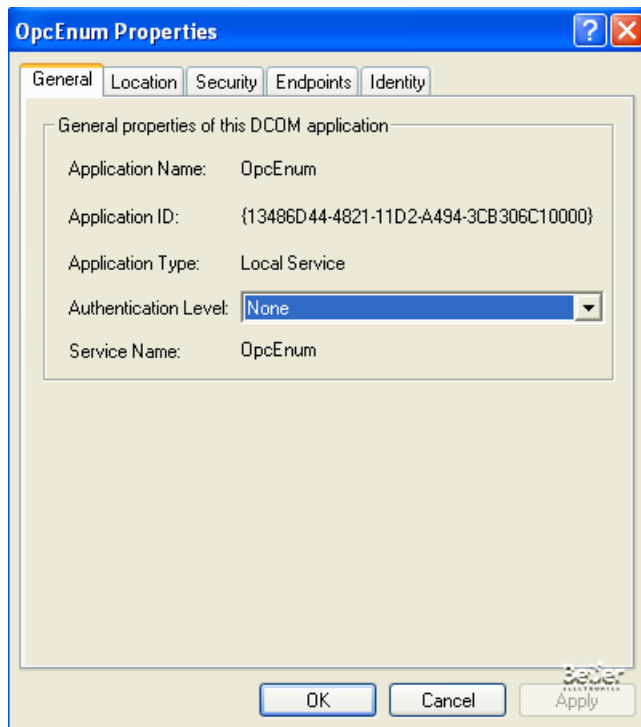
To make necessary changes, follow the steps below (steps 1 and 2 similarly to *DCOM Configuration of Beijer Electronics OPC Server*):

1. Open the Component Services window again by using the “**dcomcnfg**” command in the **Run** dialog box.
2. In the Component Services window, navigate inside the Console Root folder to the Component Services folder, and then to the Computers folder. Expand My Computer and click on the DCOM Config folder.
3. Right-click on OPCEnum in the list of objects in the right window pane, and select **Properties**.

2.7.1 General

Make the following setting on the General tab:

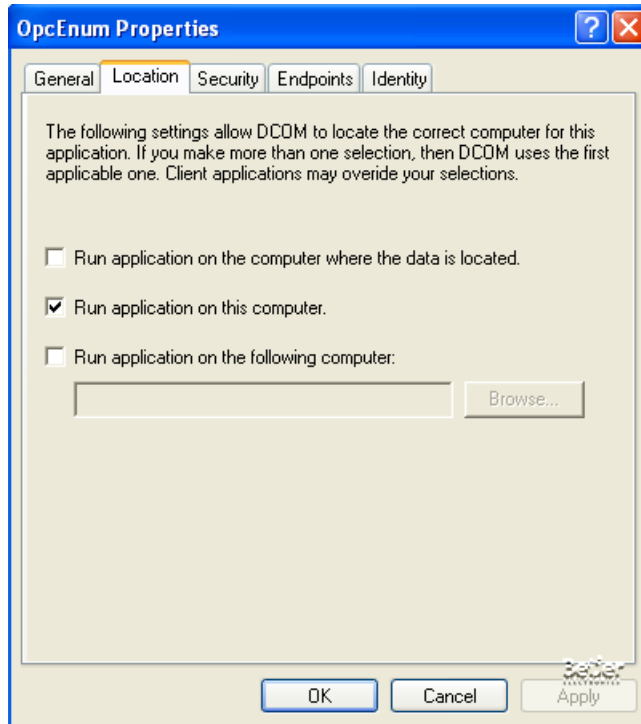
1. Set Authentication Level to **None**.



2.7.2 Location

Make the following setting on the Location tab:

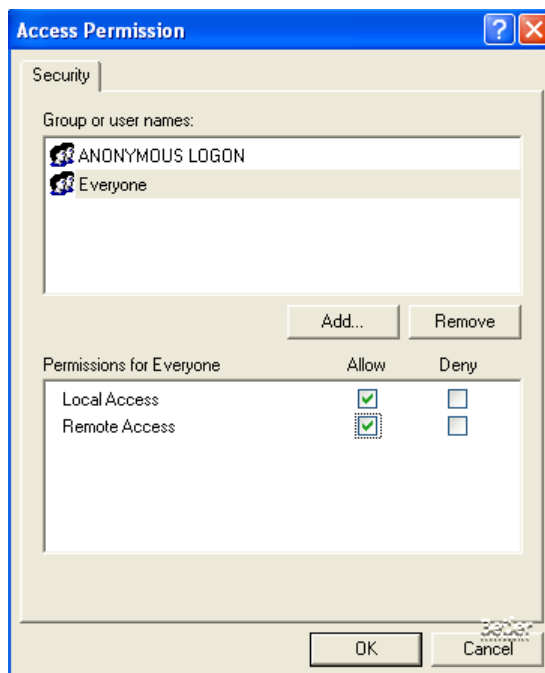
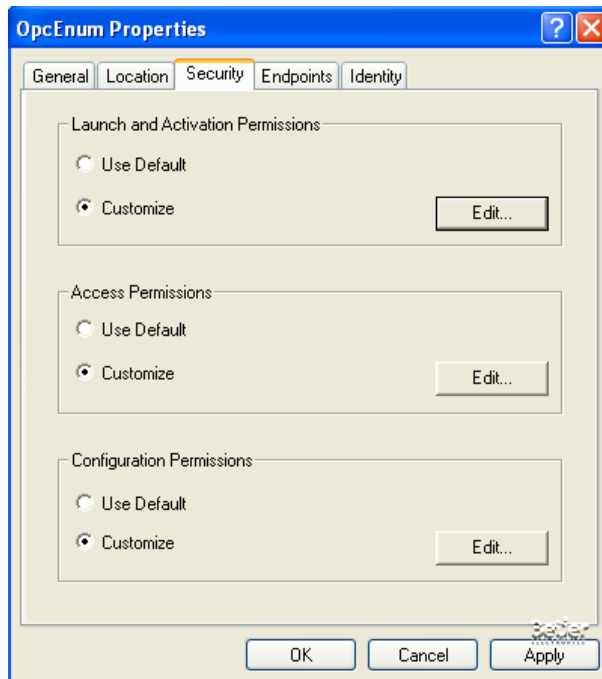
1. Check **Run application on this computer.**



2.7.3 Security

Make the following settings on the Security tab:

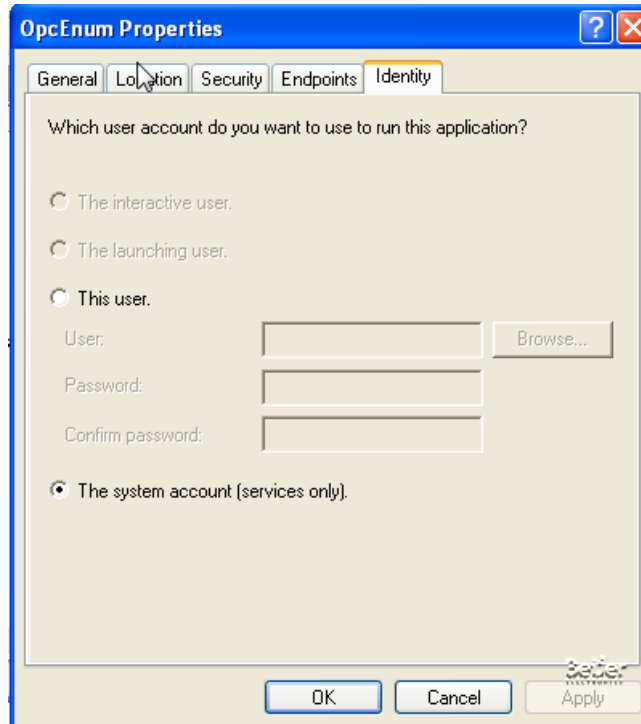
1. Select **Customize** and click **Edit** for Launch and Activation Permissions, Access Permissions and Configuration Permissions, and add **Everyone** and **ANONYMOUS LOGON** to the list of Group or user names. Change their permissions to **Allow** and click **OK**.



2.7.4 Identity

Make the following setting on the Identity tab:

1. Select the **The system account (services only)** option, and click **OK**.



Related information

[Identity Options Description](#)

2.8 Restarting the PC

1. Restart the PC in order for all settings to have impact on the system.

3 Client Setup

3.1 Prerequisites

If a PC is used as client, iX Developer has to be installed on it. Using another OPC client may not be supported and has not been tested by Beijer Electronics.

This chapter describes the following required client settings:

- [Configuring Windows Firewall](#)
- [Setting Up User Account Recognition](#)
- [DCOM Configuration of My Computer](#)

Related information
System Requirements

3.2 Configuring Windows Firewall

Make the same settings as for the server, except editing exception for Beijer Electronics OPC Server.

Related information
Configuring Windows Firewall on the server

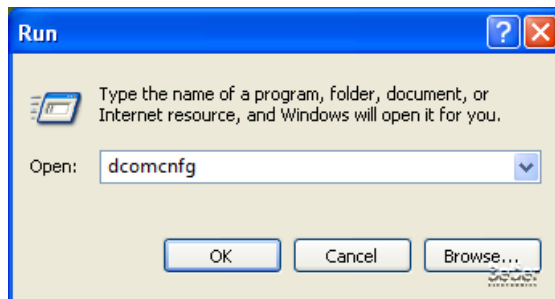
3.3 Setting Up User Account Recognition

Make the same settings as for the server.

Related information
Setting Up User Account Recognition on the server

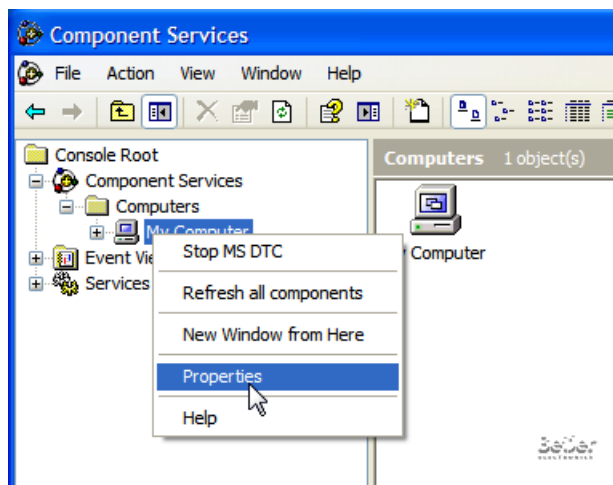
3.4 DCOM Configuration of My Computer

1. Click on the Windows **Start** button, and select **Run**. In the Run dialog box, type “**dcomcnfg**” and click **OK**.



The Component Services window opens.

2. In the Component Services window, navigate inside the Console Root folder to the Component Services folder, and then to the Computers folder. Finally, you will see the My Computer tree control inside the Computers folder.
3. Right-click on **My Computer** and select **Properties**.



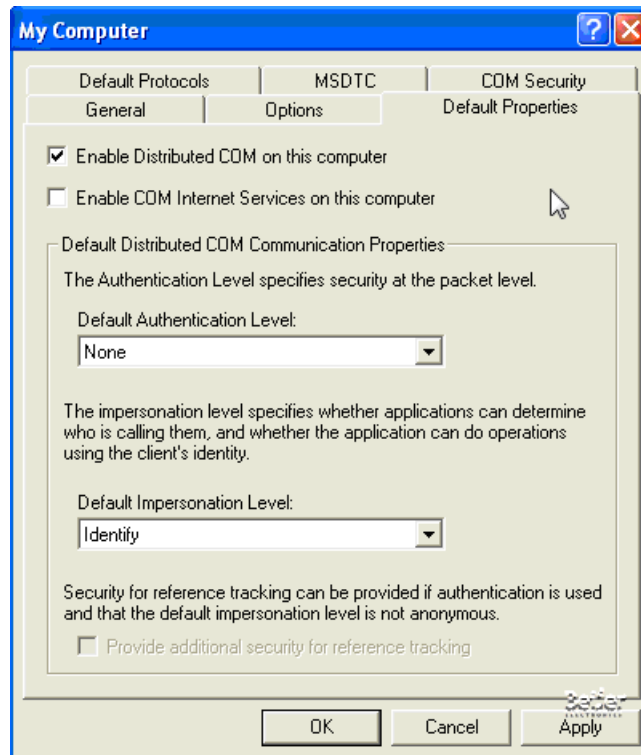
Note:

This is not equivalent to the “My Computer” icon on your desktop; but the “My Computer” tree control in the Component Services application.

3.4.1 Default Properties

Make sure that the following options are set on the Default Properties tab:

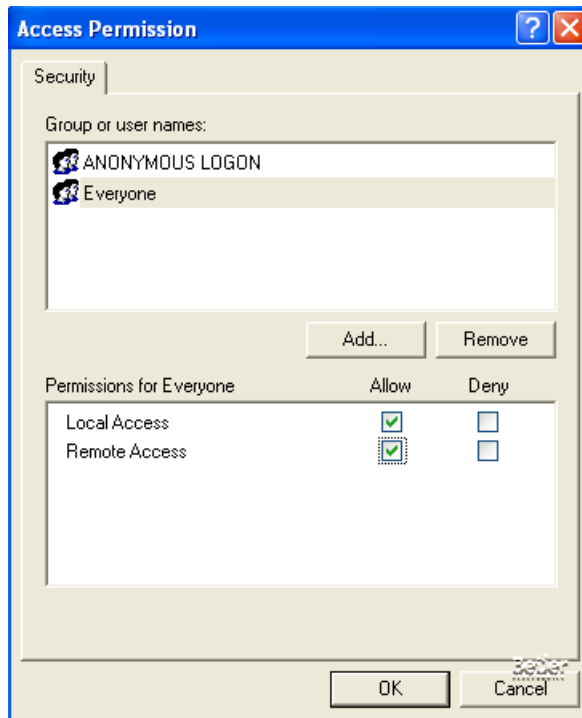
1. Check **Enable Distributed COM on this computer**. Note, that you will have to reboot the computer if you make changes to this check box.
2. Set the Default Authentication Level to **None**. It is possible to use other settings in the list, but the Connect option is the minimum level of security that you should consider.
3. Set the Default Impersonation Level to **Identify**.



3.4.2 COM Security

Make sure that the following options are set on the COM Security tab:

1. Click **Edit Limits...** for the Access Permissions group. Add **Everyone** and **Anonymous Logon** to the list of Group or user names. Change their permissions to **Allow**, and click **OK**.



2. Click **Edit Default...** for the Access Permissions group. Add **Everyone** to the list of Group or user names. Change its permissions to **Allow**, and click **OK**.
3. Click **Edit Limits...** for the Launch and Activation Permissions group. Add **Everyone** to the list of Group or user names. Change its permissions to **Allow**, and click **OK**.
4. Click **Edit Default...** for the Launch and Activation Permissions group. Add **Everyone** to the list of Group or user names. Change its permissions to **Allow**, and click **OK**.

Note:

On some computers, the Edit Limits buttons may not be available.

3.5 Restarting the PC

1. Restart the PC in order for all settings to have impact on the system.

4 iX Panel Setup

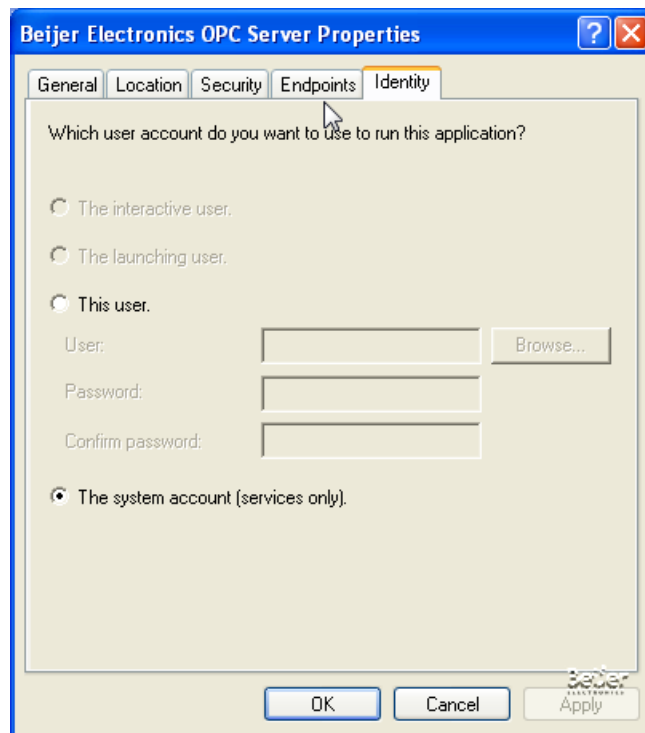
No changes are required in the iX Panel if the server is configured as described in this document.

5 Identity Options Description

Four identity options are available:

- *The Interactive User*
- *The Launching User*
- *This User*
- *The System Account (Services Only)*

The following sections describe how each of these options affects Beijer Electronics OPC Server.



Beijer Electronics OPC Server executed as a service

5.1 The Interactive User

The OPC server will assume the identity of the interactive user. This is the person who is currently logged on and using the computer on which the OPC server resides.

Note that someone must be logged on. If no one is logged on to the computer, the OPC server will fail to launch.

In addition, if someone is currently logged on, the OPC server will shut down as soon as the person logs off.

Last, in the case of a reboot, the OPC server will not launch until someone logs on.

Consequently, this is typically a poor setting for OPC servers. OPCTI does not recommend that you use this setting unless the OPC server vendor specifies this setting explicitly.

5.2 The Launching User

The OPC server will take the identity of the user account that launched it. With this setting, the operating system will attempt to initiate a new instance for every launching user.

There are three general problems with this setting:

1. Some OPC servers will only allow a single instance to execute. Consequently, the second user will be unable to make the connection because an instance of the OPC server is already running on the computer.
2. Some OPC server vendors allow more than one instance of the OPC server to execute concurrently. In this case, the computer on which the OPC server resides will have multiple copies of the OPC server executing concurrently, which will consume a significant portion of the computer resources and might have an adverse effect on the computer's performance. In addition, some system resources might be unavailable to any instances of the OPC server that follow the first. For example, the first launching user will be able to connect to a serial port, while every other launching user will simply receive bad quality data. OPCTI does not recommend that you use this setting unless the OPC server vendor specifies this setting explicitly.
3. The launching user must have administrative rights on the OPC server computer, and cannot be configured as a "limited" user.

5.3 This User

The OPC server will take the identity of a specific user account. This setting might be required when the OPC server is tightly coupled with the underlying data source. In this case, the OPC server must assume a specific Identity to exchange data with the data source.

However, since the OPC server uses a specific user account, it is possible that the computer running the OPC client does not recognize the OPC server's user account. In this case, all callbacks will fail and all OPC data subscriptions (asynchronous data updates) will fail. If this is indeed the case, you will have to add the OPC server account on the computer running the OPC client application.

Various DCS vendors require this setting for their OPC servers. OPCTI does not recommend that you use this setting unless the OPC server vendor specifies this setting explicitly.

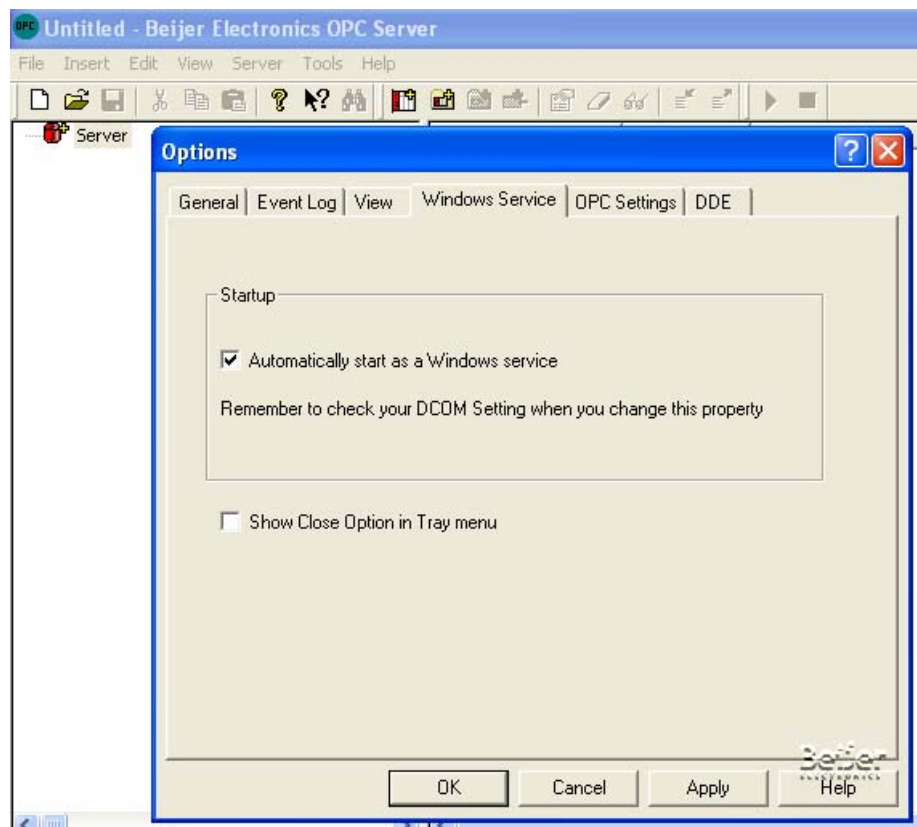
5.4 The System Account (Services Only)

The OPC Server will take the identity of the Operating System (or System for short). This is typically the desired setting for the OPC Server as the System Account is recognized by all computers on the Workgroup or Domain.

In addition, no one needs to be logged on the computer, so the OPC Server can execute in an unattended environment. OPCTI recommends configuring the Identity of the OPC Server with this setting, unless the OPC Server vendor specifies a different setting explicitly.

Note that Windows disables this option if the OPC Server is not setup to execute as a Windows Service. If this is the case, simply configure the Beijer Electronics OPC Server to execute as a service before configuring this setting. To change this setting, follow the steps below:

1. Open the **Tools** menu within Beijer Electronics OPC Server, and select **Options**.
2. On the Windows Service tab, check the **Automatically start as a Windows service** option. You need to reboot for changes to take effect.





Head office

Beijer Electronics AB

Box 426

201 24 Malmö, Sweden

www.beijerelectronics.com / +46 40 358600