# GENESIS32 - DCOM on Windows in a Workgroup

APPLICATIONS NOTE

October 2013

**Description:** Guide to setup DCOM on a Windows Operating System when computers are in a workgroup on the Local Area Network.
**OS Requirement:** Windows XP / Windows Vista / Windows 7 / Windows 8 / Windows Server 2003 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012
**General Requirement:** In order to communicate OPC data between different PCs via DCOM in a workgroup, the following requirements apply:

- All GENESIS32 systems must be in the same workgroup on the LAN.
- All GENESIS32 systems must be logged in to the operating system with the same username and password.
- The password must not be blank or "admin".
- The user must have administrative privileges to the local PC to change the DCOM settings.

## Introduction

For GENESIS32 Applications to communicate via DCOM, it is necessary to allow Access and Launch permissions for specific users. For the most part, these permissions are configured after running the Application Setup Utility. If for some reason, you cannot run this utility, you can edit DCOM manually.

Also, ICONICS recommends using GenBroker communication instead of using DCOM when trying to connect to a remote OPC server. To learn more about GenBroker communication and its benefits, please refer to the application note *GenBroker - Introduction to GenBroker Communications*.

If you are unable to run the Application Setup Utility or use GenBroker to retrieve remote OPC data, you can use the steps described in this document to configure DCOM. You must have perfect DCOM setup for communication to remote OPC servers.

This application note explains how to setup DCOM on all GENESIS32 supported Operating Systems, for the most wide-open permissions. It is usually helpful to develop your application with wide-open communications on client as well as server side to be sure that it all works properly. After you have completed your development, you will want to tighten these permissions until you reach a desired level of security.

We use Windows 8 as an example for setting DCOM in this application note. The steps on other operating systems are similar.

## Editing DCOM Settings

1. Hit your Windows key and type in "DCOMCNFG" and hit enter. The Component Services window will open.
2. Expand Console Root → Component Services → Computers
3. Right-click on **My Computer** and select **Properties** to set the DCOM properties.

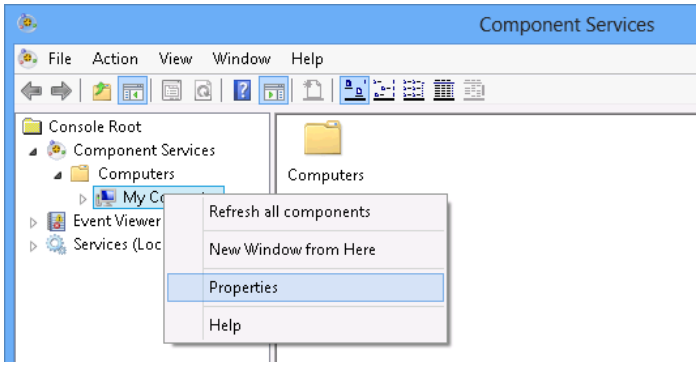


**Figure 1 - Component Services Console**

4. The My Computer Properties window will open. Click on the Default Properties tab, and match the properties as shown in Figure 2.

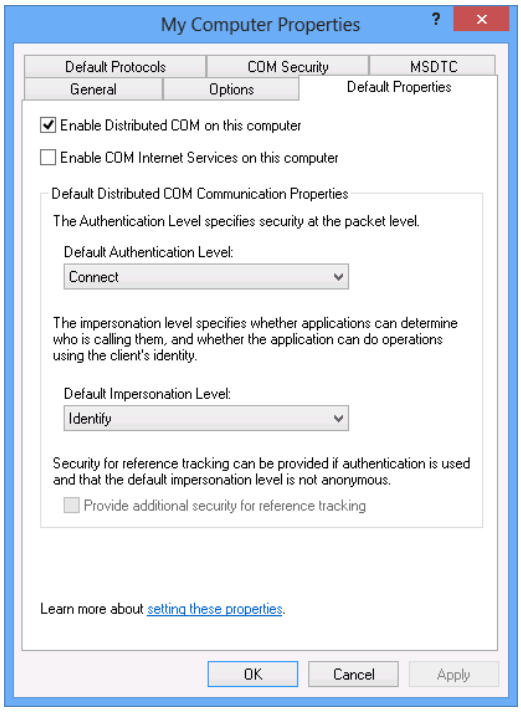


**Figure 2 - My Computer Default Properties**

5. Next we have to add user permissions to the Default Security. Go to the COM Security tab.
6. Click Edit Limit for Access Permission. Make sure the Access Limit Permissions Window includes at least the following entries:

- Administrators
- Everyone
- Interactive
- Network
- System

7. If these entries are not shown by default, click the "Add…" button and then Advanced to add them to the list.
8. **Administrators, Everyone**, **Interactive**, **Network**, and **System** are users on the local machine, so choose the local machine name as the **Location**. Click **Find Now**, select all four users while holding the Ctrl-key, and click **OK**.
9. Repeat Steps 6-8 to edit the Access Default Permission, the Launch Limit Permissions, and the Launch Default Permissions. Close the **My Components Properties** window, and the **Component Services** window when finished.

**NOTE:** You may not have any "Edit Limits" button. That is ok, in this case, just click on the "Edit Default" buttons and add the users for default permissions.

## Local Security Settings

1. Open Administrative Tools → Local Security Policy to open the Local Security Settings window. Expand the tree control and select Security Options in the left hand pane as shown in Figure 3.

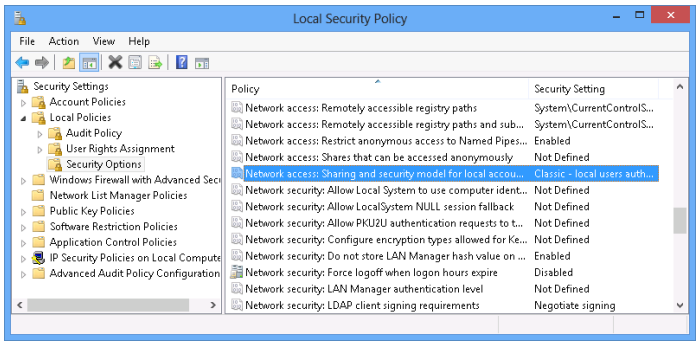


**Figure 3 - Local Security Settings**

2. In the right hand pane, scroll to find Network Access: Sharing and security settings for local accounts. Right-click and select Properties.
3. Select Classic - local users authenticate as themselves as shown in Figure 4, and click OK.

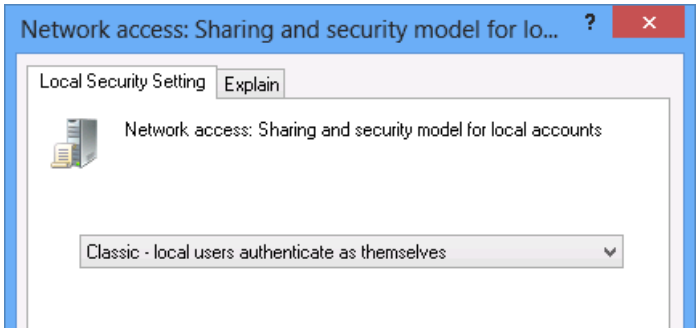


**Figure 4 - Sharing and Security for Local Accounts**

4. Double-click on "Network access: Let Everyone permissions apply to anonymous users".
5. Select Enabled and hit OK, then close the Local Security Policy window.
6. Restart the PC and login with a domain user name as mentioned in the **General Requirements** of this document. Please refer to **OS Requirements** and **General Requirements** on page 1 of this document to make sure everything is correct.

## Firewall Settings on the Server Side

1. Open Windows Firewall, click on Advanced Settings, and add a rule to allow TCP communication on port 135.
2. When finished you should add few more rules: Add an application rule for each OPC server application that you want to run on the machine that you want to be able to communicate over DCOM.
3. Next Add Program rule again and browse for the OPCENUM.EXE executable. This file is often located in \WINDOWS\System32 or \WINDOWS\SysWOW64.
4. Close the Windows Firewall control panel.

**NOTE:** If you are using a firewall other than the Windows Firewall then you will need to make similar exceptions in your firewall. If you have no other firewall and the Windows Firewall is disabled then you may skip this section.

## Network Discovery Setting on the Server Side

1. Go to Control Panel then go to Network and Sharing Center.
2. Go to Advanced Sharing settings and Turn on Network Discovery if it is disabled for the appropriate Network profile.