

**Description:** How to setup DCOM on a Windows XP or Windows 2003 Operating System when computers are in a workgroup on the Local Area Network. Please see additional application note if systems are in a domain.

OS Requirement: Windows XP with SP1, or Windows 2003.

**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 user name 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.
- Windows XP systems must have SP1 installed.

## Opening and Enabling DCOM

For GENESIS32 Applications to communicate via DCOM it is necessary to allow permissions (Access and Launch) for specific users. This application note explains how to setup DCOM on a Windows XP Operating System, for the most wide-open permissions. It is usually helpful to develop your application with wide-open communications to be sure it all works properly. After development is complete, you may want to tighten these permissions until you reach a desired level of security.

- 1. Click on Start Run and type in "DCOMCNFG". The Component Services window will open. Expand Console Root and you will see three items in the tree: Component Services, Event Viewer, and Services.
- 2. Expand Component Services and Computers to find My Computer listed. Right-click My Computer and select Properties to set the DCOM properties.

🚱 File Action View	Window Help			
🗢 🔿 🗈 💽 🗡	🖆 🔄 😭		6- 6-	語前
Console Root		My Com	puter	r 4 objec
Computers  Computers  My Comput  Computers  Computers	es Stop MS DTC Refresh all compo	inents	bns	DCOM
⊕	View New Window from	n Here		
	Properties Help			

Fig. 1: Component Services Console

- 3. The **My Computer Properties** window will open, containing six configurable tabs. We are only concerned with two of the tabs for now.
- 4. Click on the **Default Properties** tab, and match the properties as shown in **Fig. 2**.

Der	ult Protocols		MSDT	C	Default COM Securit
G	eneral		Options		Default Properties
En	able Distribute	d COM	on this co	mputer	
En	able COM Inte	anet Ser	vices on	this com	outer
	N.D. 1.3 . 1	coulo			
Ueta	ult Distributed	LUM L	ommunica	tion Prop	erties
The	Authentication	n Level s	specifies s	ecurity a	t the packet level.
De	rault Authenti	cation Le	evel:		$\mathbf{i}$
C	nnect	internet and	and and the		ノ
i ne	is calling them	ievei sp 1, and wi lentitu	hether the	applicat	ion can do operations
using	the client's in	untion I c	a unde		
Using De	the client's in ault Impersor	nation Le	evel:		$\geq$
	i the client's in fault Impersor entify	nation Le	evel:		Ç
De De Secu	i the client's in fault Impersor entify rity for referer hat the defau	nation Le nce track It impers	evel: king can t	be provide vel is not	ed if authentication is use anonymous.

Fig. 2: My Computer Default Properties

## **DCOM User Permissions**

5. Next we have to add user permissions to the Default Security. Click the **Default COM Security** tab as shown in **Fig. 3**:

General	Options	Default Properties
Default Protocols	MSDTC	Default COM Securit
Access Permissions You may edit who provide their own :	is allowed to access a settings.	pplications that do not Edit Default
Launch Permissions You may edit who	is allowed to launch ar	plications that do not
Log may call who		
provide their own	settings.	Edit Default
provide their own	settings.	Edit Default
provide their own a	settings.	Edit Default
provide their own :	settings.	Edit Default

Fig. 3: Default Com Security



- Click Edit Default for Access Permission and the Access Permissions window will open as shown in Fig. 4. Make sure the Access Permissions Window includes at least the following entries:
  - Administrators
  - Everyone
  - Interactive
  - Network
  - System
  - The user common to all GENESIS32 systems
- 7. If these entries are not shown by default, click the **Add...** button and then **Advanced** to add them to the list.
- 8. These are all users on the local machine, so choose the local machine name as the **Location**. Click **Find Now**, select all three users while holding the **CTRL** key, and click **OK**.

Select this object	type:	
Users, Groups, o	r Built-in security principals	Object Types
From this location	¢.	
COMPUTER_NAI	ME	Locations
Common Querie	35	
Name	Starts with	Columns
Description	Starts with ~	Find Now
Non expire	on naceword	
Days since las	tlogën,	OK Cancel
Days since las	In Folder	OK Cancel
Davis tince las Name (RDN) 12 Guests 14 HelpAssistant	In Folder COMPUTER, NAME COMPUTER, NAME	
Days lince los Name (RDN) 1 Guests 6 HelpAssistant 8 HelpServices.	In Folder COMPUTER_NAME COMPUTER_NAME COMPUTER_NAME	OK Cancel
Days lince las Name (RDN) 19 Guests HelpAssistant 19 HelpServices. 50 INTERACTIVE	In Folder COMPUTER_NAME COMPUTER_NAME	OK Cancel
Days lince les Name (RDN) 2 Guests HelpAssistant HelpServices. 50INTERACTIVE METUVORK		OK Cencel
Days lince las Name (RDN) If Guests HelpServices. MINTERACTIVE KINTERACTIVE Network Confit Power Users	In Folder COMPUTER, NAME COMPUTER, NAME COMPUTER, NAME	

Fig. 4: Select Users or Groups Advanced

9. When all users to be added are listed in the Select Users and Groups window, click OK to add them.

elect Users or Groups	? 🛛
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
COMPUTER_NAME	Locations
Enter the object names to select ( <u>examples</u> ):	
	Check Names
Advanced	Cancel

Fig. 5: Select Users or Groups

10. Repeat Steps 6-9 to edit the Launch Permissions. Close the My Components Properties window, and the Component Services window when finished.

## Local Security Settings

**<u>NOTE</u>**: Windows XP has advanced security features compared to Windows NT/2000.

 Click Start→Control Panel→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 Fig. 6.

File Action View Help		
Security Settings	Policy /	Security Setting
Account Policies     Local Policies	Network access: Let Everyone per Network access: Named Pipes that	Disabled COMNAP, COMNOD
H User Rights Assignmen	Network access: Remetely accession	System\CurrentCon COMCFG,DFS\$
Rublic Key Policies	Network access: Sharing and security	model for local accounts
Software Restriction Policie     The Security Policies on Loca	Network security: Force logoff wh	Disabled Disabled
I Socardy Foldos of Fold	Network security: LAN Manager a	Send LM & NTLM re
< >	Network security: LDAP client signi	Negotiate signing No minimum

Fig. 6: Local Security Settings

- 12. In the right hand pane, scroll to find Network Access: Sharing and security settings for local accounts. Right-click and select Properties.
- 13. Select Classic local users authenticate as themselves as shown in Fig. 6, and click OK. Close the Local Security Settings window when finished.

Network a	ccess: Sharing and s	ecurity model for local act	counts
Classic - local u	ers authenticate as	themselves	

Fig. 7: Sharing and Security Setting for Local Accounts

14. Restart the PC and login with the common user name and password 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.