

Matrikon Inc. 10405 Jasper Avenue Suite 1800 Edmonton, AB T5J 3N4 Canada

Phone 780-448-1010

Fax 780-448-9191

Web www.matrikon.com

CANADA Edmonton, Alberta Calgary, Alberta Fort McMurray, Alberta Vancouver, British Columbia Toronto, Ontario Quebec City, Quebec

AUSTRALIA Newcastle, New South Wales Brisbane, Queensland Gladstone, Queensland Melbourne, Victoria Perth, Western Australia

USA St. Louis, Missouri Houston, Texas New York, New York

EUROPE Aberdeen, Scotland

MIDDLE EAST Al Khubar, Saudi Arabia

Windows XP DCOM Configuration For OPC

NOTE: These directions will open up DCOM to <u>all</u> users.

NOTE: These steps are used to make sure that communication **<u>can be</u>** established. After these steps have been followed to establish communication, DCOM permissions can be tightened to allow only the necessary users.

1) From the start menu go to run and type in dcomcnfg.



2) Component Services Dialog.





4) Now go to the Default COM Security Tab.

My Computer Properties	? 🔀
General Options Default Protocols MSDTC	Default Properties Default COM Security
Access Permissions You may edit who is allowed to access a provide their own settings.	applications that do not
Launch Permissions You may edit who is allowed to launch a provide their own settings.	pplications that do not Edit <u>D</u> efault
ОК	Cancel Apply

5) Make sure that both the Access and Launch Permissions have "Everyone", "Interactive", "Network" and "System" set to Allow.

aunch Permission		L
Security		
<u>G</u> roup or user names:		
Everyone		
1 INTERACTIVE		
🕵 NETWORK		
🕵 SYSTEM		
	A <u>d</u> d	emove
Dereciacione (en Derecena		I
Permissions for Everyone	Allow	Deny
Launch Permission		
	ОК	Cancel
ccess Permission		?
Security		?
Security		?>
Security		2
Security Group or user names: Security Group or user names: Security		?
Security Group or user names: Image: Everyone Image: NETWORK		?
Security Group or user names: Group or user names: Group or user names: METWORE SYSTEM		?
Security Group or user names: Group or user names: Security Everyone Security Everyone Security Everyone Security Everyone Security Everyone Security Everyone Security Everyone Security Security Everyone Security		
Security Group or user names: Group or user names: Everyone METWORK SYSTEM		
Security Group or user names: Security Group or user names: Security Everyone Security INTERACTIVE Security NETWORK Security	A <u>d</u> d	emove
Broup or user names: Group or user names: Everyone INTERACTIVE NETWORK SYSTEM	<u>Ad</u> d <u>E</u> Allow	emove
Access Permission Security Group or user names: Image: Everyone Image: InterActive Image: NETWORK Image: SYSTEM Permissions for Everyone Access Permission	<u>Ad</u> d Allow	<u>}</u> emove
Access Permission Security Group or user names: Image: Everyone Interactive Interactin <	<u>Ad</u> d <u> </u>	2emove Deny
Access Permission Security Group or user names: Image: Everyone Image: InterActive Image: InterA	Add <u>F</u> Allow	Aemove Deny
Access Permission Security Group or user names: Image: Everyone Access Permission	<u>Ad</u> d 	2emove Deny
Security Group or user names: Image: Everyone Image: Interactive Image: NETWORK Image: System Permissions for Everyone Access Permission	Add E	<u>Remove</u>
Security Group or user names: Image: Everyone Image: Interactive Image: NETWORK Image: System Permissions for Everyone Access Permission	Add Allow	<u>?</u> <u>A</u> emove Deny
Security Group or user names: Image: Everyone Image: InterActive Image: NETWORK Image: System Permissions for Everyone Access Permission	<u>Ad</u> d <u> </u>	<u>}</u> emove Deny

6) Back on the My Computer Properties Dialog. Click on the Default Properties Tab. Ensure that the settings on your machine match those in the screenshot below.

My Computer Properties 🛛 ? 🔀				
Default Protocols MSDTC Default COM Security General Options Default Properties				
Enable Distributed COM on this computer				
Enable COM Internet Services on this computer				
Default Distributed COM Communication Properties				
The Authentication Level specifies security at the packet level.				
Default Authentication Level:				
Connect				
The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.				
Default Impersonation Level:				
Identify _▼				
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.				
Provide additional security for reference tracking				
OK Cancel Apply				

7) Click OK. You should now be looking at the Component Services Panel.

8) Underneath My Computer in the component services panel, there is a DCOM Config Folder. Inside this folder are all of the DCOM Applications installed on the local machine. We need to ensure that all of our OPC Servers are using the appropriate permissions.

NOTE: Due to a limitation in the Windows XP DCOM Configuration tool, not all OPC Servers may be listed as their Application name, but instead as their Class ID number. If your OPC Server is being listed by its Class ID please contact our support line for additional help.



Eile Action View Window Help ← →	
 ← → È Event Object Change 2 HC HTML Application IIS Admin Crypto Extension IIS Admin Service IIS WAMREG admin Service IIS WAMREG admin Service IIS Namager Administrative Se Logical Disk Manager Administrative Se Logical Disk Manager Remote Client Matrikon OPC Server for Simulation OPC Server for Simulation and Testing Matrikon OPC Server for Matrikon Arch Matrikon OPC Server for Simulation and Testing 	<u>_ 8 ×</u>
Image: Sevent Object Change 2 Image: Sevent Object Change 2 <	
• MediaCatalogDB OLE DB Prov • Messenger Private Object • Microsoft Access Application • Microsoft Clip Organizer • Microsoft Excel Application • Microsoft FrontPage • New Window from Here • Microsoft Access Application • Properties • Microsoft Excel Application • Help • Microsoft FrontPage • • • • • • • • • • • • • • •	object(s)

9) Find your OPC Server(s) in the list. Right-Click on the OPC Server and select Properties.

Matrikon OPC Server (for Simulation and Testing Prop ?
General Location Secu	urity Endpoints Identity
General properties of th	nis DCOM application
Application Name:	Matrikon OPC Server for Simulation and Testing
Application ID:	{F8582CF3-88FB-11D0-8850-00C0F0104305}
Application Type:	Local Server
Authentication Level:	Connect
Local Path:	
	OK Cancel Apply

10) Please ensure that your Authentication Level is set to 'Connect'.

11) If you have successfully set this server to utilize the def	up the Defaul ault settings, c	Its for your sy or custom set	ystem, yo tinas.	u can decid	e if you wa
12) If you choose default pl	ease skip the	following s	steps for	Launching	and Acce
Permissions. 13) Now that customize has permissions to contain t "System". 14) Make sure that all of these	been selected ne following users are set t	, please edi users, "Ever o Allow.	t the def yone", "	ault launch Network", `	and acce `Interactive
Matrikon OPC Server for Sim	ulation and Te	sting Prop	. ? 🗙		
General Location Security En	points Identity				
- Launch Permissions					
⊂ <u>U</u> se Default					
Customize		<u> </u>			
Access Permissions					
C Use De <u>f</u> ault					
Customize		E <u>d</u> it			
Configuration Permissions					
C Use Defa <u>u</u> lt					
 Customize 		Edįt			
	ок Са	ancel	Apply		



15) Under the Identity Tab, please ensure that your OPC Server is running as T Interactive User.	The
Matrikon OPC Server for Simulation and Testing Prop 🕐 🔀	
General Location Security Endpoints Identity	
Which user account do you want to use to run this application?	
The interactive user.	
C The launching user.	
○ This <u>u</u> ser.	
Us <u>e</u> r: <u>B</u> rowse	
Password:	
Co <u>n</u> firm password:	
The system account (services only).	
OK Cancel Apply	

- 16) If your Server is running as a service you will not be able to select The Interactive User, it will be under The System Account.
- 17) Please repeat steps 8 -> 16 for all OPC Servers installed on the machine.
- 18) Please note that these steps may need to be done on remote machines as well, please repeat all steps as necessary.

If you are using SP 2 and are using workgroups instead of a domain the following steps may be needed in order to establish communication.

19) Open the Administrative Tools Control panel.

ile Edit View Favorites Toc	ls Help		
3 Back - 🕥 - 🏂 🔎	Search 🎼 Folders 🛄 🕶		
ddress 🔂 Control Panel			Image:
-	Name 🔺	Comments	
Control Panel	Accessibility Options	Adjust your comput	
	🕿 Add Hardware	Installs and trouble	
📴 Switch to Category View	Add or Remove Programs	Install or remove pr	
	Administrative Tools	Configure administr	
		AspenTech License	
See Also	🌯 Automatic Updates	Set up Windows to	
Mindows Lodata	BDE Administrator	Configures the Borl	
	() Clock	Changes the appea	
Help and Support	🚽 🧬 Date and Time	Set the date, time,	
	🚽 💁 Display	Change the appear	
	Folder Options	Customize the displ	
	🖾 Fonts	Add, change, and	
	🗁 Game Controllers	Add, remove, and c	
	🎂 IBM Java Plug-in 1.4.1	Java Plug-in Control	
	🗾 InterBase Manager	Starts, stops and c	
	Internet Options	Configure your Inte	
	🧓 Keyboard	Customize your key	
	🖔 Mouse	Customize your mo	
	Setwork Connections	Connects to other c	
	💁 Network Setup Wizard	Launch the Network	
	book and Modem Options	Configure your tele	
	Sections	Configure energy-s	
	Sector Printers and Faxes	Shows installed prin	
	💼 Program Updates	InstallShield Update	
	🚱 QuickTime	Configures QuickTi	
	🧶 Regional and Language Options	Customize settings	
	Scanners and Cameras	Add, remove, and c	

20) Open up the local security policy of this computer.

N 1 1 1 1 1 1 1				
Administrative Tools				
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ols <u>H</u> elp			at 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 199
🌀 Back 👻 🕥 - 🏂 🔎	Search 😥 Folders 🛄 🕶			
Address 🦏 Administrative Tools				💌 🄁 Go
	🔨 Name 🔺	Size	Туре	Date Modified
File and Folder Tasks \land	Component Services	2 KB	Shortcut	12/8/2004 12:04 AM
Departs this file	📕 Computer Management	2 KB	Shortcut	12/8/2004 12:07 AM
Rename unis nie	Data Sources (ODBC)	2 KB	Shortcut	1/10/2005 5:36 AM
Move this file	📕 🔛 Event Viewer	2 KB	Shortcut	12/8/2004 12:07 AM
Copy this file	Internet Information Services	2 KB	Shortcut	12/8/2004 7:28 AM
🔕 Publish this file to the	Local Security Policy	2 KB	Shortcut	6/7/2005 9:12 AM
Web	Microsoft .NET Framework 1	2 KB	Shortcut	12/8/2004 3:20 AM
🔀 E-mail this file	Microsoft .NET Framework 1	2 KB	Shortcut	12/8/2004 3:20 AM
🗙 Delete this file	M Performance	2 KB	Shortcut	12/8/2004 12:07 AM
	Server Extensions Administrator	2 KB	Shortcut	12/8/2004 7:26 AM
Other Places	Services	2 KB	Shortcut	5/21/2005 2:30 AM

- 21) In the left hand pane expand the Security policies.
 22) Expand the Local policies, and select the Security options.
 23) Find the two options that begin with "DCOM:". Double click on this option to enter the configuration.

😼 Local Security Settings			
<u>File Action View H</u> elp			
	8		
Security Settings	Policy 🛆	Security Setting	· · · · · · · · · · · · · · · · · · ·
Account Policies	🕮 Accounts: Administrator account status	Enabled	
E G Local Policies	🗒 Accounts: Guest account status	Disabled	
Audit Policy	B Accounts: Limit local account use of blank passwords to console logon only	Enabled	
User Rights Assignmen	🔀 Accounts: Rename administrator account	Administrator	
Decurity Options	BB Accounts: Rename guest account	Guest	
Software Restriction Policie	BB Audit: Audit the access of global system objects	Disabled	
IP Security Policies on Loca	BB Audit: Audit the use of Backup and Restore privilege	Disabled	
	Big Audit: Shut down system immediately if unable to log security audits	Disabled	
	COM: Machine Access Restrictions in Security Descriptor Definition Language (SDD	O:BAG:BAD:(A))CC	
	BCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDD	O:BAG:BAD:(A))CC	
	BDevices: Allow undock without having to log on	Enabled	
	BDevices: Allowed to format and eject removable media	Administrators	
	B Devices: Prevent users from installing printer drivers	Disabled	
< · · · >	Bevices: Restrict CD-ROM access to locally logged-on user only	Disabled	5

24) Set the following options in your configuration.

Access Permission	? 🔀
Security Limits	
Group or user names:	
	<u>^</u>
SERVICE	
	A <u>d</u> d <u>R</u> emove
Permissions for Everyone	Allow Deny
Local Access	
Remote Access	
	OK Cancel

- 25) Set the other DCOM configuration that was located in step 23 to the same settings as above.
- 26) In your Local Security Settings find the option for "Network Access: Sharing and security model for local accounts."

Local Security Settings			×
Eile Action View Help			
\leftarrow \rightarrow $ $ \bigcirc $ $ \times \textcircled{eff} \blacksquare $ $ \textcircled{eff}	<u>}</u>		
🝺 Security Settings	Policy 🔺	Security Setting	~
🕀 🧰 Account Policies	Network access: Allow anonymous SID/Name translation	Disabled	
E G Local Policies	👼 Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	
⊕	📆 Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	
User Rights Assignmen	🕮 Network access: Do not allow storage of credentials or .NET Passports for network	Disabled	
Bublic Key Policies	BigNetwork access: Let Everyone permissions apply to anonymous users	Enabled	
Generation Policies	BigNetwork access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD	
+	BigNetwork access: Remotely accessible registry paths	System\CurrentCon	
🗠 🌄 I. Docalit,	BigNetwork access: Shares that can be accessed anonymously	COMCFG,DFS\$	
	Wetwork access: Sharing and security model for local accounts	Classic - local users	
	🕮 Network security: Do not store LAN Manager hash value on next password change	Disabled	
	💐Network security: Force logoff when logon hours expire	Disabled	
	🔀 Network security: LAN Manager authentication level	Send LM & NTLM re	
	WNetwork security: LDAP client signing requirements	Negotiate signing	
< · · · >	Network security: Minimum session security for NTLM SSP based (including secure RP	No minimum	~

27) Set this option to use Classic mode.

Network access: Sharing and security model for local ? 🔀		
Local Security Setting		
Network access: Sharing and security model for local accounts		
Classic - local users authenticate as themselves		
OK Cancel Apply		

28) In your Local Security Settings find the option for "Network Access: Let everyone permissions apply to anonymous users."

Local Security Settings				
Eile Action <u>Vi</u> ew Help				
← → 🗈 🗙 🗗 🗟	2			
😥 Security Settings	Policy 🛆	Security Setting	·	
Account Policies	BigMicrosoft network server: Digitally sign communications (always)	Disabled		
E Cocal Policies	Big Microsoft network server: Digitally sign communications (if client agrees)	Disabled		
🕀 🧾 Audit Policy	Big Microsoft network server: Disconnect clients when logon hours expire	Enabled		
User Rights Assignmen	BNetwork access: Allow anonymous SID/Name translation	Disabled		
Dublic Key Policies	BONetwork access: Do not allow anonymous enumeration of SAM accounts	Enabled		
Public Key Policies	BNetwork access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled		
In The Security Policies on Loca	BONetwork access: Do not allow storage of credentials or .NET Passports for network	Disabled		
	Retwork access: Let Everyone permissions apply to anonymous users	Enabled		
	BigNetwork access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD		
	BigNetwork access: Remotely accessible registry paths	System\CurrentCon		
	Betwork access: Shares that can be accessed anonymously	COMCFG,DFS\$		
	B Network access: Sharing and security model for local accounts	Classic - local users		
	🞉 Network security: Do not store LAN Manager hash value on next password change	Disabled		
<	Network security: Force logoff when logon hours expire	Disabled	~	

29) Enable this option.

Network access: Let Everyone permissions apply to a ? 🔀			
Local Security Setting			
Network access: Let Everyone permissions apply to anonymous users			
◯ Di <u>s</u> abled			

Your **<u>DCOM</u>** is now setup to accept all incoming connections.

NOTE: DCOM has limitations for connectivity when operating on separate domains/workgroups. These steps may work but, depending on individual networks, additional settings and components may be required. Please contact OPC Support for additional information.

 Phone:
 (780) 945-4011

 E-Mail:
 OPC.Support@Matrikon.com