

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:		
f Everyone		
1 INTERACTIVE		
🕵 NETWORK		
🕵 SYSTEM		
	A <u>d</u> d	emove
Dereciacione (en Derecena		
Permissions for Everyone		Deny
Launch Permission	V	
	ОК	Cancel
ccess Permission		?
		?
Security		?>
Security		2
Security Group or user names:		?
Security <u>G</u> roup or user names: Everyone INTERACTIVE		?
Security <u>G</u> roup or user names: Everyone NTERACTIVE NETWORK		?
Security <u>G</u> roup or user names: Everyone INTERACTIVE		
Security <u>G</u> roup or user names: Everyone NTERACTIVE NETWORK		
Security <u>G</u> roup or user names: Everyone M INTERACTIVE M INTERACTIVE M NETWORK M SYSTEM		emove
Security <u>G</u> roup or user names: Everyone INTERACTIVE INTERACTIVE NETWORK SYSTEM Permissions for Everyone	Allow	emove
Security <u>G</u> roup or user names: Everyone M INTERACTIVE M INTERACTIVE M NETWORK M SYSTEM		
Security <u>G</u> roup or user names: Everyone INTERACTIVE INTERACTIVE NETWORK SYSTEM Permissions for Everyone	Allow	
Security <u>G</u> roup or user names: Everyone INTERACTIVE INTERACTIVE NETWORK SYSTEM Permissions for Everyone	Allow	
Security <u>G</u> roup or user names: Everyone INTERACTIVE INTERACTIVE NETWORK SYSTEM Permissions for Everyone	Allow	
Security <u>G</u> roup or user names: Everyone INTERACTIVE INTERACTIVE NETWORK SYSTEM Permissions for Everyone	Allow	
Security <u>G</u> roup or user names: Everyone INTERACTIVE INTERACTIVE NETWORK SYSTEM Permissions for Everyone	Allow	
Security <u>G</u> roup or user names: Everyone INTERACTIVE INTERACTIVE NETWORK SYSTEM Permissions for Everyone	Allow	

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:
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

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.



Image: Second Secon	
Event Object Change 2 HC HTML Application IIS Admin Crypto Extension IIS Admin Service IIS WAMREG admin Service Isctl Internet Explorer(Ver 1.0) Iogagent Logical Disk Manager Administrative Se Logical Disk Manager Remote Client Matrikon OPC Server for Simulation and Testing 0 or other transmission	<u>_ 8 ×</u>
 HC HTML Application IIS Admin Crypto Extension IIS Admin Service IIS WAMREG admin Service IIS WAMREG admin Service Internet Explorer(Ver 1.0) Internet Explorer(Ver 1.0) Iogagent Logical Disk Manager Administrative Se Logical Disk Manager Remote Client Matrikon Archiver Matrikon OPC Server for Matrikon Arct Media Player Media Player 	
Image: Second	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				u can decid	e if you wa
12) If you choose default pl				Launching	and Acce
Permissions. 13) Now that customize has permissions to contain t "System". 14) Make sure that all of these	ne following	users, "Ever			
Matrikon OPC Server for Sim	ulation and Te	sting Prop	. ? 🗙		
General Location Security En	dpoints 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			
	0K Ca	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.

File Edit View Favorites Tool	s Help		
3 Back - 🕥 - 🏂 🔎	Search 😥 Folders		
ddress 🔂 Control Panel	11		💌 🄁 Go
-	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	
	AspenTechLM	AspenTech License	
See Also 🏾 🍣	🍓 Automatic Updates	Set up Windows to	
A Windows Update	BDE Administrator	Configures the Borl	
	() Clock	Changes the appea	
Help and Support	🔗 Date and Time	Set the date, time,	
	🔄 🎯 Display	Change the appear	
	Giran Contions	Customize the displ	
	🔂 Fonts	Add, change, and	
	ame 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	
	a Keyboard	Customize your key	
	Mouse	Customize your mo	
	Setwork Connections	Connects to other c	
	🕥 Network Setup Wizard	Launch the Network	
	Phone and Modem Options	Configure your tele	
	A Power Options	Configure energy-s	
	Service and Faxes	Shows installed prin	
		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.

e <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u>	ools <u>H</u> elp			
Back 🔹 🕥 - 🏂 🍃	🔘 Search 😥 Folders 🔢 🕇			
ress 🦏 Administrative Tools				
	🔼 Name 🔺	Size	Туре	Date Modified
File and Folder Tasks 🔅	Component Services	2 KB	Shortcut	12/8/2004 12:04 AM
The Designer Altin Cile	Computer Management	2 KB	Shortcut	12/8/2004 12:07 AM
Rename this file	🚽 🗊 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
	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.

<u>File Action View H</u> elp			
← → 🖻 X 🗗 🖳 🕯	9		
Security Settings	Policy 🔺	Security Setting	
E 📴 Account Policies	B Accounts: Administrator account status	Enabled	
E 📴 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 Security Options	B Accounts: Rename administrator account	Administrator	
	Accounts: Rename guest account	Guest	
Folicies Software Restriction Policie	B Audit: Audit the access of global system objects	Disabled	
+ 🥷 IP Security Policies on Loca	B Audit: Audit the use of Backup and Restore privilege	Disabled	
	B 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	
	BDCOM: 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	
<	BDevices: Restrict CD-ROM access to locally logged-on user only	Disabled	

24) Set the following options in your configuration.

Access Permission	? 🔀
Security Limits	
Group or user names:	
	<u>^</u>
INTERACTIVE INTERACTIVE INTERACTIVE	
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."

Eile <u>A</u> ction <u>V</u> iew <u>H</u> elp			
⊢→ 🖻 🗙 🖀 🖆	9		
Security Settings	Policy 🔺	Security Setting	
Account Policies	BNetwork access: Allow anonymous SID/Name translation	Disabled	
🛛 🧰 Local Policies	👼 Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	
🗄 📴 Audit Policy	🔀 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	
	BNetwork access: Let Everyone permissions apply to anonymous users	Enabled	
Software Restriction Policie	BNetwork access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD	
IP Security Policies on Loca	B Network access: Remotely accessible registry paths	System\CurrentCon	
	BNetwork access: Shares that can be accessed anonymously	COMCFG,DFS\$	
	Retwork 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	
	Bill Network security: Force logoff when logon hours expire	Disabled	
	🔀 Network security: LAN Manager authentication level	Send LM & NTLM re	
	BBNetwork 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."

<u>File Action View H</u> elp			
← → 🖻 X 📽 🖫 1	3		
Security Settings	Policy A	Security Setting	
Account Policies Acco	B Microsoft network server: Digitally sign communications (always)	Disabled	
	Bill Microsoft network server: Digitally sign communications (if client agrees)	Disabled	
	BigMicrosoft network server: Disconnect clients when logon hours expire	Enabled	
	BNetwork access: Allow anonymous SID/Name translation	Disabled	
	BNetwork access: Do not allow anonymous enumeration of SAM accounts	Enabled	
	BNetwork access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	
	BNetwork access: Do not allow storage of credentials or .NET Passports for network	Disabled	
	Retwork access: Let Everyone permissions apply to anonymous users	Enabled	
	Network access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD	
	Network access: Remotely accessible registry paths	System\CurrentCon	
	Network access: Shares that can be accessed anonymously	COMCFG,DFS\$	
	BNetwork 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			
Enabled Enabled			
◯ Di <u>s</u> abled			
OK Cancel Apply			

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