This document provides detailed DCOM configuration for setting up one or more machines for using Total Vu as an OPC Server. The DCOM settings primarily address all the issues with enhanced security in Windows XP Service Pack 2. Some settings may be overkill for other Windows versions, but we have empirical evidence that these settings work.

1. Anti-Virus Software

DCOM and Anti-Virus software do not get along! The interim solution is to disable all anti-virus software. In the future, we will investigate exception settings which allow Total Vu/DCOM communications while maintaining a secure system.

Disable Windows Firewall

Go to Start ->Control Panel, Double-Click on Windows Firewall. Set to Off, as shown.



Select the Exceptions tab. At a minimum, specify the DCOM Port (135), and add the Total Vu program.

😺 Windows Firewall	×
General Exceptions Advanced	
Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.	
Programs and Services:	
Name	
☑ DCOM	
He and Printer Sharing	
✓ Remote Assistance	
I Slame	
I Total \/u	
Add Program Add Port Edit Delete)
Display a notification when Windows Firewall blocks a program	
What are the risks of allowing exceptions?	
OK Cancel	

Other Anti-Virus Software

Other anti-virus software (Norton Anti-Virus, etc.) must be disabled as well. See the appropriate software vendor's documentation.

2. Total Vu Server Registration

To register Total Vu as an OPC Server, go to Start->Run..., click Browse to locate TotalVu.exe. Add the parameter "-register" and click OK.



Once registered, Total Vu will display the following message.



NOTE to RSView32 Users

Rockwell Automation RSView®32[™] uses local registry entries to find information about OPC servers. Therefore, in a client-server PC network configuration, Total Vu must be installed and registered as an OPC Server on both the client and server PCs.

3. DCOM Settings

OPC uses ActiveX COM and DCOM for communication. To configure DCOM, go to Start->Run...; enter dcomcnfg; then click OK.

Run	? 🛛
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	dcomcnfg.
	OK Cancel <u>B</u> rowse

Go to Console Root->Component Services->Computers->My Computer. Right-click on My Computer and select Properties. Select the Default Properties Tab. Enable Distributed COM, set the Default Authentication Level to "None", and set the Default Impersonation Level to "Identify".

My Computer Prope	rties	? 🛛	
Default Protocols	MSDTC	COM Security	
General	Options	Default Properties	
Enable Distributed	COM on this computer		
Enable COM Inter	net Services on this com	nputer	
- Default Distributed C	OM Communication Pro	notion	
	OM Communication Pro	penies	
The Authentication	Level specifies security	at the packet level.	
Default Authentica	tion Level:		
None	None		
The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.			
Identify		_	
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.			
	ОК	Cancel Apply	

Select the COM Security Tab. For each of Edit Limits... and Edit Default..., in Access Permissions and Launch and Activation Permissions, check all the Allow check boxes for the following Groups or User Names: ANONYMOUS LOGON, Everyone, Interactive, NETWORK, SYSTEM, and an Administrator account. If the Group or User Name is not in the list, add it using the Add... button.

Access Permission		? 🔀
Default Security		
Group or user names:		
ANONYMOUS LOGON		^
Everyone		Ξ
M INTERACTIVE		
Jeff (WENDELLLAPTOP\We	ndell Ott)	~
	A <u>d</u> d	<u>R</u> emove
Permissions for Everyone	Allow	Deny
Local Access	~	
Remote Access		
	ок	Cancel

4. OpcEnum Properties

Run dcomcnfg, select Component Services->Computers->My Computer->DCOM Config. Rightclick on OpcEnum and select Properties. On the General Tab, set Authentication Level to "None".

OpcEnum Properties	? 🛛
General Location Secu	urity Endpoints Identity
General properties of th	nis DCOM application
Application Name:	OpcEnum
Application ID:	{13486D44-4821-11D2-A494-3CB306C10000}
Application Type:	Local Service
Authentication Level:	None
Service Name:	OpcEnum
	Cancer Apply

Select the Security Tab. For Launch and Activation Permissions, Access Permissions, and Configuration Permissions, select Customize and then click the Edit... button.

OpcEnum Properties
General Location Security Endpoints Identity
Launch and Activation Permissions
Access Permissions C Use Default C Customize Edit
Configuration Permissions C Use Default C Customize Edit
OK Cancel Apply

Check all the Allow check boxes for the following Groups or User Names: ANONYMOUS LOGON, Everyone, Interactive, NETWORK, SYSTEM, and an Administrator account. If the Group or User Name is not in the list, add it using the Add... button.

Change Configuration Permis	sion	? 🔀
Security		
Group or user names:		
	andall (tt)	
		<u>~</u>
<u>j</u>	A <u>d</u> d	<u>R</u> emove
Permissions for Administrators	Allow	Deny
Full Control Read Special Permissions	>	
For special permissions or for adva	1	
click Advanced.	inced settings,	Advanced

Select the Identity Tab, and select The interactive user.

OpcEnum Properties	? 🛛
General Location Security Endpoints Identity	
Which user account do you want to use to run this applic	cation?
The interactive user.	
C The Jaunching user.	
⊂ This <u>u</u> ser.	
Us <u>e</u> r:	<u>B</u> rowse
Password:	1
Co <u>n</u> firm password:	
C The system account (services only)	
OK Cance	el <u>A</u> pply

5. TotalVuServer Properties

Right-click on TotalVuServer and select Properties. On the General Tab, set Authentication Level to "Connect".

Te	otalVuS	Server Proper	ties 🤶 🔀
	General	Location Sec	urity Endpoints Identity
	Gene	ral properties of t	his DCOM application
	Арр	lication Name:	TotalVuServer
	Арр	lication ID:	{4C733CE0-D6BB-11DA-8314-002078153AE2}
	Арр	lication Type:	Local Server
	Auth	nentication Level	Connect
	Loc	al Path:	C:\Nomacorc\TotalVu.exe
			OK Cancel Apply

Select the Security Tab. For Launch and Activation Permissions and Access Permissions, select Use Default. For Configuration Permissions, select Customize and then click the Edit... button.

TotalVuServer Properties	×
General Location Security Endpoints Identity	
Launch and Activation Permissions Use Default Customize	
Access Permissions © Use De <u>f</u> ault © Custo <u>m</u> ize <u>Edit</u>	
Configuration Permissions Use Default Customize Edit	
OK Cancel Apply	

Check all the Allow check boxes for the following Groups or User Names: ANONYMOUS LOGON, Everyone, Interactive, NETWORK, SYSTEM, and an Administrator account. If the Group or User Name is not in the list, add it using the Add... button.

Change Configuration Permis	sion	? 🔀
Security		
Group or user names:		
	andall (tt)	
		<u>~</u>
<u>j</u>	A <u>d</u> d	<u>R</u> emove
Permissions for Administrators	Allow	Deny
Full Control Read Special Permissions	>	
For special permissions or for adva	1	
click Advanced.	inced settings,	Advanced

Select the Identity Tab and select The interactive user.

TotalVuServer Properties
General Location Security Endpoints Identity
Which user account do you want to use to run this application?
 The interactive user.
C The launching user.
C This <u>u</u> ser.
Us <u>e</u> r: Browse
Password:
Co <u>n</u> firm password:
C The system account (services only).
OK Cancel <u>A</u> pply

6. Data Execution Prevention

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. In Microsoft Windows XP, DEP must be disabled for OPC to function properly.

Go to Start, right-click on My Computer, and select Properties. Select the Advanced Tab and click on Settings under Performance.

System Properties ? 🔀													
1	System Res	System Restore		tic Updates	Remote								
Í	General	Compu	uter Name	Hardware	Advanced								
	You must be logged on as an Administrator to make most of these changes. Performance Visual effects, processor scheduling, memory usage, and virtual memory												
	- User Profiles	User Profiles											
	Desktop setti	ngs related	to your logon		Settings								
Startup and Recovery													
System startup, system failure, and debugging information Settings Environment Variables Error Reporting													
							OK Cancel Apply						

Select the Data Execution Prevention tab, and select the "Turn on DEP for essential $\ldots ''$ radio button.

Performance Options	? ×				
Visual Effects Advanced Data Execution Prevention					
Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?					
 <u>T</u>urn on DEP for essential Windows programs and services only T<u>urn on DEP for all programs and services except those I</u> select: 					
Add Remov	e				
OK Cancel A	pply				

7. Reboot

Reboot the machine to install the new DCOM settings. Once rebooted, OPC should function properly. In the event of problems, Matrikon offers several free tools from their web-site for diagnosing OPC/DCOM problems: <u>www.matrikonopc.com</u>.