

How to Setup OPC DCOM

BridgeWare +82-31-346-1981 info@opchub.com www.opchub.com



DCOM Setup Procedure

You need to configure DCOM on both server and client machines.

- Configure your computer to be a member of your Network
- System-wide DCOM Setup
- OPC Server-specific DCOM Setup
- OPCEnum Setup
- Configure Local Security Policies
- Add Firewall exceptions
- OS-specific Setup
 - Recommend to disable UAC & DEP on Win7, Win2008 & Win2012.
- Checks for In-proc OPC Server
 - Most OPC servers are out-of-Proc, Clients can connect to the server remotely.
 - In-proc OPC Servers do not allow connections from remote clients. You may need additional components (OPC Server for DA client) or DCOM Tunneller.



Network & User Account Setup

- Configure your computer to be a member of your network (Domain or Workgroup)
 - Workgroup users: <u>Client's logon account and password must be registered on the server PC</u>.
 And client must log-on by the registered account.
 **OPC Server & client PCs do not need to use the same account and password, though most DOCM manuals recommend to do so.
 - Domain users: Logon ID and PW will be managed by Domain Server. No need to add logon account on individual PCs.
- Add Windows user account
 - In the Start menu, type "lusrmgr.msc" and then click OK.
 - Add user account or group and setup **password** for that account.





- From the Start menu, type "dcomcnfg" in the run command and then click OK
- Alternatively, go to Control Panel > Administrative Tools > Component Services

📼 Run	X	. Component Services
Open:	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. dcomcnfg This task will be created with administrative privileges. OK Cancel Browse	 File Action View Window Help File Action View Window Help Console Root Component Services Computers Computers My Computer Event Viewer (Local) Services (Local) View New Window from Here Export List Properties Help



Default Protocols COM Security	MSDTC	ļ	General	Options	Defau	It Properties
General Options	Default Properties		Default Protocols	COM Sec	curity	MSDTC
Enable Distributed COM on this computer Enable COM Internet Services on this compute	۶r		DCOM Protocols	TCP/IP	-	
Default Distributed COM Communication Propert The Authentication Level specifies security at th Default Authentication Level: Connect Connect , if not specifically	ies e packet level.				-	
ent's identity. personation Level: reference tracking can be provided default impersonation level is not ar e additional security for reference tra	if authentication is used nonymous.	9	Add Remove Description The set of network pro ordering of the protoco with the top protocol ha	e Move Up tocols available to D ls reflects the priority aving first priority.	Move Down DCOM on this y in which the	Properties machine. The y will be used
the client's identity. fault Impersonation Level: entify nity for reference tracking can be provided hat the default impersonation level is not ar Provide additional security for reference tra	if authentication is used honymous.		Add Remove Description The set of network pro ordering of the protocol with the top protocol has Learn more about <u>setting</u>	e Move Up tocols available to I ils reflects the priority aving first priority.	Move Down	machine. The

www.opchub.com

BridgeWare

x

My Computer Properti	es	? ×				
General	Options	Default Properties				
Default Protocols	COM Security	MSDTC				
Access Permissions	1					
You may edit who also set limits on	o is allowed default access applications that determine	to applications. You may their own permissions.				
Caution of applic securely	: Modifying access permissio cations to start, connect, fur /.	ons can affect the ability nction and/or run				
	Edit Limits	Edit Default				
Launch and Activat	tion Permissions					
You may edit whe activate objects. determine their o	ois allowed by default to lau You may also set limits on a wn permissions.	unch applications or applications that				
Caution affect th and/or r	: Modifying launch and activ ne ability of applications to si run securely.	vation permissions can tart, connect, function				
	Edit Limits	Edit Default				
Learn more about <u>setting these properties</u> .						
	ОК	Cancel Apply				

• Give Anonymous Logon, Everyone, Interactive, System accounts (and your specific account) Access Rights.

Select Users or Groups	8 X
Select this object type:	
Users, Groups, or Built-in security principals From this location:	Object Types
WIN-38PNELHETG7	Locations
Enter the object names to select (<u>examples</u>):	
Everyone; SYSTEM; INTERACTIVE; ANONYMOUS LOGON	Check Names
Advanced OK	Cancel



Access Permission Default Security	and and a set of	? <mark>×</mark>		Acc	ess Permission ecurity Limits	faces and a	8 X
Group or user names: & Everyone & INTERACTIVE & SYSTEM & Administrators (WIN-38PNE & ANONYMOUS LOGON	LHETG7\Administrat	cors)			Group or user names: Administrators (WIN-38PNI Everyone SYSTEM INTERACTIVE ANONYMOUS LOGON	ELHETG 7\Administra	ators)
Permissions for SYSTEM Local Access Remote Access	Add Allow	Remove Deny	ġ		Permissions for SYSTEM Local Access Remote Access	Add Allow V	Remove Deny
Learn about access control and p	oermissions OK	Cancel			Learn about access control and	pemissions OK	Cancel

www.opchub.com

Launch and Activation Permission		Launch and Activation Permission
Default Security		Security Limits
Group or user names: Everyone SYSTEM Administrators (WIN-38PNELHETG7\Administrators) INTERACTIVE ANONYMOUS LOGON		Group or user names: Everyone SYSTEM Administrators (WIN-38PNELHETG7\Administrators) ANONYMOUS LOGON INTERACTIVE
Add Remove Permissions for Everyone Allow Deny	0	Add Remove Permissions for SYSTEM Allow Deny
Local Launch Remote Launch Local Activation Remote Activation	9	Local Launch Image: Constraint of the second seco
Leam about access control and permissions OK Cancel		Learn about access control and permissions OK Cancel

www.opchub.com

Q.

- Configure DCOM for OPCEnum which is almost ٠ same as System-wide DCOM setup
- OPCEnum enables OPC clients to browse OPC • server name and tag names



www.opchub.com

Component Services

File Action View

Component Services

Event viewer (Local)

b Services (Local)

a 🔝 My Computer

DCOM Config

Computers

Console Root

4

OpcEnum Properties	OpcEnum Properties
General Location Security Endpoints Identity	General Location Security Endpoints Identity
General properties of this DCOM application Application Name: OpcEnum Application ID: {13486D44-4821-11D2-A494-3CB306C10000} Application Type: Local Service	The following settings allow DCOM to locate the correct computer for this application. If you make more than one selection, then DCOM uses the first applicable one. Client applications may overide your selections.
Authentication Level: Default	Run application on this computer.
Default or None, if not specifically instructed	Run application on the following computer: Browse Browse
Learn more about <u>setting these properties</u> .	Learn more about <u>setting these properties</u> .
OK Cancel Apply	OK Cancel Apply

www.opchub.com

General Location Security Endpoints Identity		Security
Launch and Activation Permissions		Group or user names:
Ose Default		SYSTEM
Customize	Edit	& Administrators (WIN-38P
		Sers (WIN-38PNELHET
Assess Barrissians		ANONYMOUS LOGON
		at Everyone
Ose Default		
Customize	Edit	
		LOGON
Configuration Permissions		Full Control
── Use Default		Read
Customize		Special permissions
	Eoit	OPCEnum uses And for initial handsha
		For special permissions or adv click Advanced.
Learn more about <u>setting these properties</u> .		Learn about access control ar



www.opchub.com

OpcEnum Properties	OpcEnum Properties
General Location Security Endpoints Identity	General Location Security Endpoints Identity
DCOM Protocols and endpoints:	Which user account do you want to use to run this application?
Connection-oriented TCP/IP	The interactive user.
	The launching user.
	◯ This user.
	User: Browse
	Password:
Add Remove Properties Clear	The system account (services only)
The set of protocols and endpoints available for use by clients of this	
set of DCOM protocols and endpoints for the machine will be used.	OPCEnum is run as Windows Service
Learn more about setting these properties.	Learn more about <u>setting these properties</u> .
OK Cancel Apply	



Server-specific DCOM Setup (for Kepware OPC Server)

Kepware Communications Server 5.8 Properties	I	Launch and Activation Permission		
General Location Security Endpoints Identity Launch and Activation Permissions Use Default Edit O Customize Edit Access Permissions O Use Default Edit Customize Edit		Security Group or user names: SYSTEM Administrators (WIN-38PNELHETG7\Administrators) ANONYMOUS LOGON Kepware runs as Windows Service and uses System account. Make sure SYSTEM, Everyon are included in the list. You can remove Interactive account from the list, if not Kepwar runs in interactive mode		
Use Default Customize Edit		Remote Launch Local Activation Remote Activation		
 Add the followings to the Exception list, if fin Program "Server_Runtime.exe" TCP port "32402" 	rewall	enabled.		

www.opchub.com

Local Security Policies Setup

- In the Start menu, type "secpol.msc" and then click OK.
- Or In the Start menu, open the **Control Panel** > **Administrative Tools** and setup as below.
 - "Network access: Let Everyone Permission Apply to Anonymous Users \rightarrow " Enabled"
 - "Network access: Sharing and security model for local accounts" → "Classic: Local users authenticate as themselves"

Local Security Policy			
File Action View Help			
 Security Settings Account Policies Local Policies Audit Policy User Rights Assignment Security Options Windows Firewall with Advanced Security Network List Manager Policies 	Policy Microsoft network server: Disconnect clients when logon hours expire Microsoft network server: Server SPN target name validation level Network access: Allow anonymous SID/Name translation Network access: Do not allow anonymous enumeration of SAM accounts Network access: Do not allow anonymous enumeration of SAM accounts and shares Network access: Do not allow storage of passwords and credentials for network authe	Security Setting Enabled Not Defined Disabled Enabled Disabled Disabled	*
 Public Key Policies Software Restriction Policies Application Control Policies IP Security Policies on Local Compute Advanced Audit Policy Configuration 	Network access: Let everyone permissions apply to anonymous users Network access: Named Pipes that can be accessed anonymously Network access: Remotely accessible registry paths Network access: Remotely accessible registry paths and sub-paths Network access: Restrict anonymous access to Named Pipes and Shares Network access: Shares that can be accessed anonymously Network security: Allow Local System to use computer identity for NTLM Network security: Allow Local System NULL session fallback	System\CurrentControlS System\CurrentControlS Enabled Not Defined Classic - local users auth Not Defined Not Defined	ш



Local Security Policies Setup

Network access: Let Everyone permissions apply to anonymou	Network access: Sharing and security model for local accounts
Local Security Setting Explain	Local Security Setting Explain
Network access: Let Everyone permissions apply to anonymous users	Network access: Sharing and security model for local accounts
 Enabled Disabled 	Classic - local users authenticate as themselves -
OK Cancel Apply	OK Cancel Apply

www.opchub.com

Firewall Setups

- In the Start menu, type "firewall.cpl" and then click OK.
- Or go to Control Panel > Windows Firewall
- We recommend you turn off firewall before DCOM setups. Once DCOM setups done, you may need to turn your Firewall back on, if required.
- You need to add the followings to the Firewall Exceptions list.
 - In the Start menu, type "wf.msc" to add exceptions.
 - Inbound Rule > New Rule > Port > add TCP port 135 (for initial DCOM handshake)
 - Inbound Rule > New Rule > Program > add "OPCEnum.exe"
 - Inbound Rule > New Rule > Custom > Protocol and Port > add ICMPv4 (for PING command to work over firewall).
 - Add your OPC Server executable and port number which is used by the executable.
 ("Server_runtime.exe" and the port 32402 for Kepware OPC Server)
 - Add your OPC client executable and the port number which is used by the executable.
 - On Win7 or later, adding the above in the Inbound Rule is enough in most cases, if not, add them in the Outbound Rule as well.



Windows UAC (User Access Control) Setup

- In the Start menu, type ۲ "msconfig" and then click OK.
- From the Tools tab, select Change ۲ UAC Settings.
- And press Launch button.

User Account Control Settings

System Configuration	A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O	×
General Boot Services Sta	rtup Tools	
Tool Name	Description	*
About Windows	Display Windows version information.	
Change UAC Settings	Change User Account Control settings.	=
Action Center	Open the Action Center.	
Windows Troubleshooting	Troubleshoot problems with your computer.	
Computer Management	View and configure system settings and components.	
System Information	View advanced information about hardware and software settings.	
	View monitoring and troubleshooting messages.	
	Launch, add or remove programs and Windows components.	
	View basic information about your computer system settings	-

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

Tell me more about User Account Control settings

Always notify	
- [-	Never notify me when: • Programs try to install software or make changes to
	 I make changes to Windows settings
	 Not recommended. Choose this only if you need to use programs that are not certified for Windows 7 because they do not support User Account Control.
Never notify	

ountControlSettings.exe	
	Launch

Once done, you are prompted to ulletre-start your computer, but you do not need to do so in most cases.

www.opchub.com

BridgeWare

Þ.

DEP (Data Execution Protection) Setup

 Start Menu > Computer > Properties > Advanced System Settings > Advanced Tab





www.opchub.com

Contact Us

Thank You!

Jason Hwang

Phone+82-31-346-1981Emailinfo@opchub.comHomewww.opchub.com

BridgeWare