

Configuring OPC and DCOM



SAE – Automation, s.r.o. Nová Dubnica Solid And Effective partner at development of your products and industry automation Configuring OPC and DCOM for OPC server and client applications from SAE – Automation, s.r.o.

# Configuring OPC and DCOM for OPC server and client applications from SAE – Automation, s.r.o.

The purpose of the article is to give answers and useful recommendations on the most frequently asked questions from our customers, which relate with the DCOM configuration of OPC Servers and OPC Clients located on the local or remote computers.

#### Introduction

OPC is based on Microsoft's COM and DCOM technology for data exchange between applications. The architecture of OPC is a client-server model. OPC servers and OPC clients may be provided by different vendors (vendor independence).

To establish reliable DCOM communication, in some cases e.g. communication between different network domain, workgroups, operating systems, etc., may be sometimes very frustrating.

Finally, this document should perform as a user guide which will lead you step-by-step through your DCOM configuration in order to establish reliable and secure OPC connection.

# STEP 1: Turn off the "Windows Firewall" (only temporary)

The first step to establish DCOM communication is to disable the Windows Firewall, which is turned on by default in Windows XP Service Pack 2 and later. Otherwise, for not relevant windows operating systems is possible the point to skip and continue with the next step.

The Windows Firewall protects your computers from unauthorized access. Please contact and discuses about possibility to turn off the Windows Firewall on short time with the network Administrator.

Note that: You will turn on the Windows Firewall back in step 5 (STEP 5: Turn on the "Windows Firewall").

To turn off **Windows Firewall**, please do the following (see Figure 1):

- 1. Click on the Windows Start ⇒ Control Panel ⇒ Windows Firewall.
- 2. In the General tab, select the Off (not recommended).
- 3. Click on OK button.

w w	indows Firewall 🛛 🔯
Ger	eral Exceptions Advanced
	Your PC is not protected: turn on Windows Firewall
W	ndows Firewall helps protect your computer by preventing unauthorized users m gaining access to your computer through the Internet or a network.
	On (recommended)
	This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
	Don't allow exceptions
	Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
	🗿 💿 Off (not recommended)
emprarily turn off	Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
indows Firewall.	ndows Firewall is using your domain settings.
W	hat else should I know about Windows Firewall?
	OK Cancel

Figure 1: Windows Firewall is turn off.

http://www.saeautom.sk, sae-automation@saeautom.sk, tel.:+421-(0)42-445 07 01, fax: +421-(0)42-445 07 02, Adresa: Sady Cyrila a Metoda, 21/18, 018 51 Nová Dubnica, Slovakia

# **STEP 2: User Accounts**

To enable both computers to properly recognize User Accounts, it is necessary to ensure that User Accounts are recognized on both the OPC Client and OPC Server computers. This includes all the User Accounts that will require OPC access.

#### STEP 2.1: Add the "User Accounts"

Ensure that both computers have access to the same User Name and Password combinations. User Names and Passwords must match on all computers that require OPC access.

Recommendations:

- A User Account must have a User Name and Password. It is not possible to establish communication if a User Account does not have a Password.
- When using Windows Workgroups, each computer must have a complete list of all User Accounts and Passwords.
- When using a single Windows Domain, User Accounts are properly synchronized by the Domain controller.
- When using multiple Windows Domains, you will either have to establish a Trust between the Domains, or add a Local User Account to the affected computers.

To add a new **User Account**, please do the following (see Figure 2):

- 1. Click on the Windows Start ⇒ Control Panel ⇒ User Account.
- 2. In the Users tab, click on Add...
- 3. Click on OK button.

Sers Advanced Use the list belo computer, and Users for this computer:	ow to grant or deny to change password	users access to your Is and other settings.
User Name	Domain	Group
ACTUser	SAE25	Users
🜆 Administrator	SAE25	Administrators 👘 📒
<b>E</b> amyopc	SAE25	Administrators
ASPNET	Add a U	Jser Account.
-Password for amyopc	Add	Remove Properties
To change th	e password for amy	opc, click Reset Password. Reset Password

Figure 2: Add a new user account.

#### STEP 2.2: Select the "Local users authenticate as themselves"

In Windows XP and Windows Vista, there is another setting that you should modify. This is not necessary in Windows 2000 or earlier.

Simple File Sharing is always turned on in Windows XP Home Edition-based computers. By default, the Simple File Sharing user interface is turned on in Windows XP Professional-based computers that are joined to a workgroup. Windows XP Professional-based computers that are joined to a domain use only the classic file sharing and security interface.

Simple File Sharing forces every remote user to Authenticate as the Guest User Account. This will not enable you to establish proper security.

To select the **Classic – local users authenticate as themselves** option, please do the following (see Figure 3):

- 1. Click on the Windows Start ⇔ Control Panel ⇔ Administrative Tools ⇔ Local Security Policy. (Or click on the Windows Start ⇔ Run and type "secpol.msc".)
- 3. Select the option Classic local users authenticate as themselves.
- 4. Click on OK button.

#### 4

http://www.saeautom.sk, sae-automation@saeautom.sk, tel.:+421-(0)42-445 07 01, fax: +421-(0)42-445 07 02, Adresa: Sady Cyrila a Metoda, 21/18, 018 51 Nová Dubnica, Slovakia

Docal Security Settings		
File Action View Help		
Security Settings Account Policies Account Policies Account Policies Account Policies Account Policies Security Options Public Key Policies Software Restriction Policies IP Security Policies on Lonetwork Local Security	Policy A Ref Network access: Let Everyone permissions apply to anonymous users Network access: Named Pipes that can be accessed anonymously Network access: Shares that can be accessed anonymously Network access: Sharing and security model for local accounts Network security: Do not store LAN Manager hash value on next password cha access: Sharing and security model for local ? Network access: Sharing and security model for local accounts Network access: Sharing and security model for local accounts Network access: Sharing and security model for local accounts Network access: Sharing and security model for local accounts	nge
Select the option "Classic - users authenticate as themse	ssic - local users authenticate as themselves	

Figure 3: Select the local users authenticate as themselves.

# **STEP 3: Configuration of general DCOM settings**

The general DCOM settings affect all Windows applications that use DCOM, **including OPC application**. In addition, since OPC Client applications do not have their own DCOM settings, they are affected by changes to the default DCOM configuration.

DCOM settings are possible to set through the DCOMCNFG utility which is supplied as part of operating system.

To start **DCOMCNFG** utility, please do the following (see Figure 4):

- 1. Click on the Windows Start ⇒ Control Panel ⇒ Administrative Tools ⇒ Component Services. (Or click on the Windows Start ⇒ Run and type DCOMCNFG.)
- 2. Click on OK button.

	? 🛛
Type the name of a program, folder, c Internet resource, and Windows will op	locument, or pen it for you.
DCOMCNEG	<b>~</b>
OK Cancel	Browse
	Type the name of a program, folder, of Internet resource, and Windows will o

Figure 4: Start the DCOMCNFG utility.

To open My Computer Properties dialog, please do the following (see Figure 5, Figure 6):

- 2. Click on Properties.



Figure 5: To open My Computer Properties dialog.

#### **STEP 3.1: Default Properties**

To set up **Default Properties** as necessary, please do the following (see Figure 6):

- 1. Select Default Properties tab.
- 2. Select the Enable Distributed COM on this computer menu option. It specifies that DCOM is available for all COM applications installed on this computer. (Note that you will have to reboot the computer if you make changes to this checkbox).
- 3. Set the Default Authentication Level to Connect. There is possibility to use other settings in the list, but the Connect option is the minimum level of security that you should consider.
- 4. Set the Default Impersonation Level to Identify.

	My Computer Propertie	es	? 🛛
	Default Protocols	MSDTC	COM Security
	General	Options	Default Properties
1. Select to specify that	Enable Distributed CO	IM on this computer Services on this comput	ter
COM is available for all COM applications installed on this computer.	Default Distributed COM The Authentication Lev	1 Communication Proper rel specifies security at tl	ties he packet level.
	Default Authentication	n Level:	-
2. Select the level of security that COM client and server application use to verify each other. "Connect" should be minimum level.	The impersonation leve who is calling them, and using the client's identity Default Impersonation	l specifies whether appli d whether the application y. n Level:	ications can determine n can do operations
3. Set the "Default Impersonation Level" to "Identify".	Security for reference tr and that the default imp	acking can be provided ersonation level is not a I security for reference tr	if authentication is used nonymous. acking
		ОК	Cancel Apply

Figure 6: To set up Default Properties.

# **STEP 3.2: Default Protocols**

To set up **Default Protocols** as necessary, please do the following (see Figure 7):

- 1. Select the Default Protocols tab.
- 2. Set the DCOM Protocols to Connection-Oriented TCP/IP.

ly Computer Propert	ies	? 🛛	
General	Options	Default Properties	
Default Protocols	MSDTC	COM Security	
DCOM Protocols			
Connection-oriented			
Connection-oriented	ISPX		
	OPC	communication use	_
	Conne	ction-Oriented TCP/I	P".
			-
1			
Add Berrow	Mayello May		
		- Toperdes	
Description			
The set of network pr	otocols available to DCON	1 on this machine. The	
ordering of the protoc	ols reflects the priority in w	hich they will be used,	
with the top protocol	naving hist phonty.		
	ОК	Cancel Apply	

Figure 7: To set up Default Protocol to Connection-Oriented TCP/IP.

### STEP 3.3: COM Security

Windows uses the COM Security tab to set the system-wide Access Control List (ACL) for all objects. The ACLs define permissions on **Launch and Activation** and **Access** of applications.

To Add Access Permissions as necessary, please do the following (see Figure 8):

- 1. Select the COM Security tab.
- 2. Click on the Edit Default... button in the Access Permissions group.
- 3. Add the Everyone to the list of Group or user names.
- 4. Click on the OK button.

Note that on some systems is available the **Edit Limits**... button then please go on as follows (see Figure 8):

- 5. Click on the Edit Limits... button in the Access Permissions group.
- 6. Add the Everyone to the list of Group or user names.
- 7. Add the Anonymous Logon to the list of Group or user names. The Anonymous Logon account is required for the OPCEnum application.
- 8. Click on the OK button.

Access Permission		? 🛛	Access Permission		? 🛛
Default Security		1	Security Limits		1
Group or user names:			Group or user names:		
ASP.NET Machine Accou	nt (SAE25\ASPNET)		ANONYMOUS LOGON		
Everyone			E veryone		
SYSTEM					
	Add	Remove		Add	Remove
Permissions for Everyone	Allow	Deny	Permissions for Everyone	Allow	Deny
Local Access			Local Access		
Remote Access	1		Remote Access	$\checkmark$	
1		10	<u>1</u>		
	ОК	Cancel		ОК	Cancel

Figure 8: To set up Access Permissions of DCOM Security.

To Add Launch Permissions as necessary, please do the following (see Figure 9):

- 1. Select the COM Security tab.
- 2. Click on the Edit Default... button in the Launch Permissions group.
- 3. Add the Everyone to the list of Group or user names.
- 4. Click on the OK button.

Note that on some systems is available the **Edit Limits**... button then please go on as follows (see Figure 8):

- 5. Click on the Edit Limits... button in the Access Permissions group.
- 6. Add the Everyone to the list of Group or user names.
- 7. Click on the OK button.

Launch Permission		? 🛛	Launch Permission		? 🔀
Default Security			Security Limits		
Group or user names:			Group or user names:		
Administrators (SAE25\Ad     Administrators (SAE25\Ad     ASP.NET Machine Accou	ministrators) int (SAE25\ASPNET)		Administrators (SAE25\Ad	lministrators)	
Everyone     Everyone     INTERACTIVE     SYSTEM			Offer Remote Assistance	Helpers (SAE25\Offer Rem	iote Ass
Permissions for Everyone	Add	Remove	, Permissions for Everyone	Add Ri Allow D	emove
Local Launch Remote Launch Local Activation Remote Activation			Local Launch Remote Launch Local Activation Remote Activation		
	0K	Cancel		ОК	Cancel

Figure 9: To set up Launch Permissions of DCOM Security.

# **STEP 4: Configuration of server specific DCOM settings**

If the general DCOM settings are properly configured then it is possible to set up server specific DCOM settings. Why the server specific DCOM settings? Because of, these settings may be different for every OPC Server installed on the computer. To set up server specific DCOM settings, it is possible again to use the DCOMCNFG utility (please see above).

To open OPC Server specific dialog, please do the following (see Figure 10, Figure 11):

- 2. Click on Properties.



Figure 9: To open OPC Server specific dialog.

The first four tabs refer to general DCOM settings (please see above) and it is not necessary to change them. (see Figure 10)

OpcDbGateway DA and OpcDbGateway AE Properties 🛛 💽 🔀	OpcDbGateway DA and OpcDbGateway AE Properties 💦 🛛 🕅
General Location Security Endpoints Identity	General Location Security Endpoints Identity
General properties of this DCOM application Application Name: OpcDbGateway DA and OpcDbGateway AE Application ID: {BE729BC7-C2C3-4DA4-9007-16AC887A56FD} Application Type: Local Server Authentication Level: Default Local Path:	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.  Run application on the computer where the data is located.  Run application on this computer.  Run application on the following computer:  Browse
OK Cancel Apply	OK Cancel Apply
OncDhGateway DA and OncDhGateway AF Properties	OpcDbGateway DA and OpcDbGateway AF Properties
OpcDbGateway DA and OpcDbGateway AE Properties ?X General Location Security Endpoints Identity	OpcDbGateway DA and OpcDbGateway AE Properties ?
OpcDbGateway DA and OpcDbGateway AE Properties ? X General Location Security Endpoints Identity Launch and Activation Permissions	OpcDbGateway DA and OpcDbGateway AE Properties ? General Location Security Endpoints Identity DCOM Protocols and endpoints:
OpcDbGateway DA and OpcDbGateway AE Properties  General Location Security Endpoints Identity Launch and Activation Permissions  Use Default	OpcDbGateway DA and OpcDbGateway AE Properties  General Location Security Endpoints Identity DCOM Protocols and endpoints:
OpcDbGateway DA and OpcDbGateway AE Properties       Image: Constraint of the security         General       Location       Security       Endpoints       Identity         Launch and Activation Permissions       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security       Image: Constraint of the security         Image: Constraint of the s	OpcDbGateway DA and OpcDbGateway AE Properties  General Location Security Endpoints Identity DCOM Protocols and endpoints:
OpcDbGateway DA and OpcDbGateway AE Properties       Image: Constraint of the security         General Location       Security       Endpoints       Identity         Launch and Activation Permissions       Image: Constraint of the security       Image: Constraint of the security         Customize       Edit         Access Permissions       Image: Customize       Edit         Customize       Edit         Customize       Edit	OpcDbGateway DA and OpcDbGateway AE Properties  General Location Security Endpoints Identity DCOM Protocols and endpoints:
OpcDbGateway DA and OpcDbGateway AE Properties       Image: Construction Security Endpoints Identity         General Location Security Endpoints Identity         Launch and Activation Permissions         Image: Customize         Access Permissions         Image: Customize         Edit         Access Permissions         Image: Customize         Edit         Configuration Permissions         Image: Customize         Edit         Edit         Edit	OpcDbGateway DA and OpcDbGateway AE Properties       Image: Constraint of the system         General Location       Security       Endpoints       Identity         DCOM       Protocols and endpoints:       Image: Constraint of the system protocols       Image: Constraint of the system protocols         Add       Remove       Properties       Clear         Description       The set of protocols and endpoints available for use by clients of this DCOM server. The system defaults entry indicates that the default set of DCOM protocols and endpoints for the machine will be used.

*Figure 10*: The first four tabs refer to general DCOM settings and it is not necessary to change them.

Only the **Identity** tab may be changed from the default settings. An application's Identity is the account that is used to run the application. The Identity can be that of the user that is currently logged on (the interactive user), the user that launched the server, a specified user, or a service. (see Figure 11)

<sup>12</sup> 

http://www.saeautom.sk, sae-automation@saeautom.sk, tel.:+421-(0)42-445 07 01, fax: +421-(0)42-445 07 02, Adresa: Sady Cyrila a Metoda, 21/18, 018 51 Nová Dubnica, Slovakia

OpcDbGat	eway D/	and Op	ocDbGatev	way AE F	Properti	es [?	
General	Location	Security	Endpoints	Identity			_
Which us	er accour	nt do you v	vant to use ti	o run this a	application	17	
<ul> <li>The is</li> </ul>	nteractive	user.					
C The l	aunching	user.					
C This u	user.						
User:		ſ				Browse	
Passwo	ord:	Γ					
Confirm	passwor	i: [					
C The s	ystem acc	count (serv	ices only).				
		(	OK	<b>C</b>	ancel	Apply	,

Figure 11: The Identity tab.

- The interactive user is the user that is currently logged on to the machine where the OPC Server is running. If the identity is set to be the interactive user, all OPC Clients use the same instance of the OPC server. If no user is logged on, the server will not run. SAE Automation, s.r.o. recommends this setting as one of possible for their OPC Servers.
- The launching user is the default setting for the application identity. When the launching user is chosen for the application's identity, each OPC Client account gets a new instance of the OPC server. SAE Automation, s.r.o. does not recommend this setting for their OPC Servers.
- This user: Specifying a particular user (and the user's password) is the preferred identity for OPC server. The reason this identity is preferred is that no one has to be logged on the machine where the server is running for the server to run and every OPC Client talks to the same instance of the OPC server. SAE Automation, s.r.o. recommends this setting as one of possible for their OPC Servers.

http://www.saeautom.sk, sae-automation@saeautom.sk, tel.:+421-(0)42-445 07 01, fax: +421-(0)42-445 07 02, Adresa: Sady Cyrila a Metoda, 21/18, 018 51 Nová Dubnica, Slovakia

 The system account (service only): Choosing this identity causes the OPC Server application to be run as a service. SAE – Automation, s.r.o. does not offer OPC Servers implemented as service therefore does not recommend this setting for their OPC Servers.

## STEP 5: Turn on the "Windows Firewall"

Once you establish communication between OPC Client and OPC Server, then it is important to secure the computers again. The turning Windows Firewall from Off to On will block all unauthorized network traffic and therefore you will also need to provide exceptions on two main levels (It is relevant to Windows XP Service Pack 2 and later):

- **Program** specifies which applications are able to respond to unsolicited requests.
- **Port** specifies that the firewall should allow or deny traffic on a specific port for either TCP or UDP traffic.

To turn on **Windows Firewall**, please do the following (see Figure 12, Figure 13, Figure 14):

- 1. Click on the Windows Start ⇒ Control Panel ⇒ Windows Firewall.
- 2. In the General tab, select the On (recommended).
- 3. Select the Exeptions tab and add all OPC Servers and OPC Clients to the exception list and the OPC utility OPCEnum.exe found in the Windows\System32 directory.

Here is available list of OPC Servers and OPC Clients which are offered by SAE- Automation, s.r.o. and may be necessary to add them between programs:

- OpcDbGateway.exe (OPC Server and OPC Client),
- OpcDbGatewayConfigurator.exe (OPC Client),
- SNMPRuntime.exe (OPC Server),
- SNMPConf.exe (OPC Client),
- OPCSimRuntime.exe (OPC Server)
- OPCAdapter.exe (OPC Client),
- OPCAdapterService.exe (OPC Client).
- 4. In the Exeptions tab click on Add Port and in the associated dialog fill out the fields as follows:
  - Name: DCOM
  - Port number: 135
  - Select the TCP radio button.
- 5. Click on OK button.



Figure 12: Windows Firewall is turn on.

eneral Exceptions Adv	anced		
Windows Firewall is turned from outside sources such General tab and select On.	off. Your computer as the Internet. We	is at risk of attacks and recommend that you cl	intrusions ick the
Programs and Services:			~
Microsoft Office Outlo	ok		
Network Diagnostics	or Windows XP		
OPC Monitor Demo			
OPC Toolbox Demo C	lient		
✓ OpcDbGateway	aller -		
OpcEnum			
OPCSimRuntime			
Peer Name Resolution	Protocol (PNRP)		
🗹 Remote Assistance			
🗹 Remote Desktop			100000
I RPC			×
Add Program	dd Port	Edit	)elete
V Display a notification w	nen Windows Firew	all blocks a program	
What are the risks of allow	ng exceptions?		

*Figure 13*: Windows Firewall, the tab Exceptions (added e.g.OpcDbGateway.exe, OpcEnum.exe, OPCSimRuntime.exe, etc.).

Add a Port	
Use these settings number and protoc want to use.	to open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you
Name:	ОСОМ
Port number:	135
	⊙ TCP O UDP
What are the risks	of opening a port?
Change scope	OK Cancel

*Figure 14*: Adding exception for port number 135 which use DCOM.

http://www.saeautom.sk, sae-automation@saeautom.sk, tel.:+421-(0)42-445 07 01, fax: +421-(0)42-445 07 02, Adresa: Sady Cyrila a Metoda, 21/18, 018 51 Nová Dubnica, Slovakia

#### Disclaimer

The information contained in these pages is based on our testing and practices experience. SAE – Automation, s.r.o. and the authors of this document assume no responsibility for direct, indirect, or consequential liability for its accuracy or suitability for a user's particular application. The reader is responsible for proper application to their particular situation.

http://www.saeautom.sk, sae-automation@saeautom.sk, tel.:+421-(0)42-445 07 01, fax: +421-(0)42-445 07 02, Adresa: Sady Cyrila a Metoda, 21/18, 018 51 Nová Dubnica, Slovakia