The OECD QSAR Toolbox for Grouping Chemicals into Categories

# **User manual**

Toolbox 2.2 Client-Server Configuration

## **Document history**

Version	Comment
Version 1.0	30/10/2010, First version
Version 1.1	31/01/2011, Domain controller setup
Version 1.2	16/02/2010, Minor update on server side configuration
Version 1.3	03/06/2011, Trouble shooting section

**Issue date:** June 2011

Language: English

If you have questions or comments that relate to this document, please send them to <a href="mailto:ehscont@oecd.org">ehscont@oecd.org</a> or visit the QSAR Toolbox discussion forum at <a href="https://community.oecd.org/community/toolbox">https://community.oecd.org/community/toolbox</a> forum.

#### **Table of Contents**

1	Introduction 4
2	Prerequisites
2.1.	1 Hardware requirements 4
2.1.	2 Software requirements 4
3	Installation of the Toolbox Server4
3.1.	1 Server Firewall settings:
3.1.	2 Server DCOM configuration:
3.1.	3 Server running domain controller DCOM configuration:
4	Installation of the Toolbox Client14
4.1	Configuration of the Toolbox Client computer14
4.1.	1 Client Firewall settings 14
4.1.	2 Client DCOM configuration: 14
4.2	Configuration of the client application16
4.3	Connecting to the Toolbox Server17
4.3.	1 Non Domain client 17
4.3.	2 Domain Client
4.4	Troubleshooting DCOM18
4.4.	1 Configuration check list 18
4.4.	2 Common errors 19

## **1** Introduction

Toolbox Server is distributed as a Windows MSI package. It contains the files comprising the Toolbox Server and a Database to be used by the client Toolbox installations. The installation procedure performs only basic COM registration and does not perform any setting up of security permissions/policies needed for the working of the server.

The administrator of the server has the responsibility for configuring the security permissions used for the server's communication.

## **2 Prerequisites**

## 2.1 Hardware requirements

The computer hosting Toolbox server must have at least:

RAM: 2 GB (recommended 4 GB)

Hard disk space: 10GB (recommended 20 GB)

CPU: 2 GHz, 32 or 64 bit architecture(recommended multi-core CPU)

Network adapter 100 Mbps (recommended 1Gbps)

## 2.2 Software requirements

Firebird 2.1 32 bit and 64bit\* installation.

\* Toolbox uses native client library (fbclient.dll) provided within the firebird installation as toolbox server is 32 bit application is able to load only 32 bit client library to access firebird server. To be able to use 64 bit server you should provide 32bit version of fbclient.dll.

## **3 Installation of the Toolbox Server**

Please unzip the Toolbox Server installation package on your local disk and run the StartInstall.exe

## **3.1 Configuration of the Toolbox Server computer**

Toolbox 2.0 server is Distributed Component Object Module (DCOM) automation server.

In this respect all common rules for the DCOM applications are also valid for the Toolbox 2.0 server.

#### 3.1.1 Server Firewall settings:

Add Toolbox Server application to the exceptions list

Add TCP port 135 to firewall exceptions list

### **3.1.2 Server DCOM configuration:**

• Authentication policy:

Define a single user on the server machine that all client applications then use to authenticate themselves to the server machine's operating system. For the purpose of this document this user will be called "*ToolboxSvr"*.

#### 1. Start **DCOMCNFG** utility



Note: For the 64bit versions of the Windows please use Start -> Run -> mmc

comexp.msc /32 to run DCOM configure utility in 32bit mode

2. Select properties from the popup menu for "My Computer".

Component Services		→ _□×
Eile Action Yiew Window Help		_8×
Console Root	My Computer 4 object(s)	
Wy Computer     Event Viewer (Local)     Services (Local)	COM+ DCOM Config Distributed Running Applications Transacti Processes	

3. Go to the "**DCOM config**" item on the left-hand side tree-view, right click on the

"ToolboxServer Object" and select Properties.



4. On the **Security** tab select "**Customize**" and click on the **Edit** button for the "**Launch** and Activation Permissions" section. Add *ToolboxSvr* to the list and check Allow for "Remote Launch" and "Remote Activation" permissions for the user.

5. On the security tab section select "Customize" and click on the Edit button for Access

Permission section. Add ToolboxSvr to the list and check Allow for "Remote

**Activation**" permission for the user.

ToolboxServer Object Properties
General Location Security Endpoints Identity
Launch and Activation Permissions
O ∐se Default
Customize
Access Permissions
O Use De <u>f</u> ault
Customize     Edit
Configuration Permissions
O Use Defa <u>u</u> lt
Customize
OK Cancel Apply

6. From the **Identity** tab select **"The interactive user**". These are the recommended

settings. The different **Identity** settings are explained bellow.

ToolboxServer Object 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 user.
Us <u>e</u> r: <u>B</u> rowse
Password:
Co <u>n</u> firm password:
C The system account (services only).
Learn more about setting these properties.
OK Cancel Apply

The interactive user: server is started in the session of the current user logged onto

the system.

pros: Application is started with user interface

cons: If there is more than one logged user the server is not able to start. The logged user may not have the security rights to activate or access the server.

The launching user - not recommended to use

This user - server is started in separate session of the specified user

pros: Application always starts

cons: The user interface is not accessible Document Version 1.3 June 2011

#### **3.1.3 Server running domain controller DCOM configuration:**

Domain User who will used the server should be added to the "Distributed COM Users"

group. The domain is tested on windows 2008R2 Server.

From "Administrative tools" open "Active Directory Users and Computers".

On the right tab select "Users"

In the left tab select user and click on right mouse button

On appeared context menu select "Add to a group" menu item.



4. Enter "**Distributed COM Users**" in the edit box and then click on "OK" button.

Select Groups		? ×
Select this object type:		
Groups or Built-in security principals		<u>O</u> bject Types
From this location:		
intranet.oasis-Imc.org		Locations
Enter the object names to select ( <u>examples</u> ):		
Distributed COM Users		Check Names
1		
<u>A</u> dvanced	ОК	Cancel
		///

5. Repeat steps 3 and 4 for all users wich have to access Toolbox server.

6. Start DCOMCNFG utility Start->RUN ->DCOMCNFG

Note: For the 64bit versions of the Windows please use **Start -> Run -> mmc** comexp.msc /32 to run DCOM configure utility in 32bit mode 7. Expand Component Services, expand Computers, and right-click My Computer. Select

#### Properties

Component Services	5	
🥺 <u>F</u> ile <u>A</u> ction <u>V</u> iew	<u>W</u> indow <u>H</u> elp	
💠 🔿 🛛 📅 🗙	1 🗟 🔒 🔽 🖬	
Console Root  Component Service Computers  C	Refresh all components View New Window from Here Export List Properties Help	

8. Click Default COM Security

My Computer Proper	ties			1	? ×
General Default Protocols	Opti s	ons COM Se	Def Def	ault Properties	
Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions. Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.					
	Ed	it <u>L</u> imits		Edit Default	
Launch and Activation Permissions         You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.         Image: Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.					
	Ed	it L <u>i</u> mits		Edit <u>D</u> efault	
Leam more about <u>setting these properties</u> .					
		OK	Cance	Apply	

9. Under Default Access Permissions click Edit Default. Make sure "Distributed COM

Users" and provide all have Local and Remote Access permissions.

Access Permission		? ×
Default Security		
<u>G</u> roup or user names:		
용       SELF         용       SYSTEM         ふ       Acount for Toolbox (Toolbox:         용       Administrators (INTRANET)         용       Administrators (INTRANET)         용       Distributed COM Users (INTRANET)	Svr@intranet.oasis dministrators) RANET\Distributed	s-Imc.org) I COM Users)
Permissions for Distributed COM Users	Add	<u>R</u> emove Deny
Local Access Remote Access	N N	
Learn about access control and p	emissions	
	ОК	Cancel

10. Under Default Access Permissions click Edit Limits. Make sure "Distributed COM Users" and provide all have Local and Remote Access permissions.

11. Under Default Launch Permissions click Edit Default. Make sure Distributed **COM User** " and the user whose authentication credentials will be used to access the COM application all have Local and Remote Launch permissions, as well as Local and Remote Activation permissions.

12. Under Default Launch Permissions click Edit Limits.. Make sure Distributed COM Users" and the user whose authentication credentials will be used to access the COM Document Version 1.3 Page 13 of 21

application all have Local and Remote Launch permissions, as well as Local and

Remote Activation permissions

## **4** Installation of the Toolbox Client

Standalone version of the toolbox can be also used a Toolbox client.

Please unzip the Toolbox installation package on your local disk and run the StartInstall.exe.

## **4.1 Configuration of the Toolbox Client computer**

## **4.1.1 Client Firewall settings**

Add Toolbox 2.0 application to firewall's exceptions list. Add TCP port 135 to firewall exceptions list.

## **4.1.2 Client DCOM configuration:**

1. Start the DCOMCNFG utility (Start Menu -> Control Panel -> Administrative tools ->

Component Services or invoke "DCOMCNFG" from the Start Menu's Run menu item)

2. Right click on "My Computer" and select Properties from the popup menu.



3. Go to **"COM Security**" tab and from the **"Access Permission**" section use the **"Edit Default...**" and **"Edit Limits...**" buttons to change the permissions for security principal **"Everyone**" and **"ANONYMOUS LOGON**".

Document Version 1.3 June 2011

4. Check "Local Access" as well as "Remote Access" for "Security Limits".

Access Permission		? 🗙
Security Limits		
Group or user names:		
ANONYMOUS LOGON		
🕵 Everyone		
	A <u>d</u> d	<u>R</u> emove
Permissions for Everyone	Allow	Deny
Local Access	<b>~</b>	
Remote Access	<b>~</b>	
	ОК	Cancel

5. Check "Local Access" as well as "Remote Access" for "Default Security".

Access Permission		? 🔀
Default Security		
<u>G</u> roup or user names:		
🕵 Everyone		
SELF		
STSIEM		
	A <u>d</u> d	<u>R</u> emove
Permissions for Everyone	Allow	Deny
Permissions for Everyone	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow V	Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access		Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access		Deny

## 4.2 Configuration of the client application

Toolbox standalone application can also act as a Toolbox client application. Configuring this requires Toolbox to have "Remote connect" set instead of the default "Local connection" in the Toolbox options. When "Remote connect" is selected for the **Database** the user needs to specify the name or address of machine where Toolbox Server is installed. After this change Toolbox needs to be restarted.

When Toolbox is started as client application the database importing features are disabled. These functions are delegated to the Toolbox server only.

Options			- • ×	
Main Modules Units Reports				
Data matrix	Chemical browser	Structural space mode		
Title column width 350	Column count 5	2D (ignore stereo information)		
Depiction height 100	·	② 2.5D (preserve stereo information)		
Database				
Local Connect     Database in use     C:\Progra	m Files\Common Files\QSAR Toolbox\Ver 2.0	DB\TB20DB_21.10.2010.FDB	<b>E</b>	
Remote Connect Server 172.17.8-	4.248			
Folder for user models       E:\Work\QSAR Toolbox\Ver 2.0\UserDir\       Edit scale definitions         12 (Q)SAR display/ranking       Do not use parameter cache       Edit scale definitions				
Profiling Data consiste Timeout [sec] 300 Reprofile timeout structures Do not use profiling cache	ncy criteria Basis for the BCF Body weight (offsprin Body weight and food or transferred referer Caculation basis fect Clinical signs (offspring	<ul> <li>✓ Clinical signs (parental animals)</li> <li>g) ✓ Compartment</li> <li>d consume ✓ Concentration</li> <li>✓ Concentration based on</li> <li>g) ✓ Cytotoxicity</li> </ul>		
✓ OK X Cancel	C Restore default			

## 4.3 Connecting to the Toolbox Server

After the client side DCOM is properly set up the Toolbox Client application only needs the IP address (or name) of the Toolbox server.

#### 4.3.1 Non Domain client:

When the Toolbox starts the user is asked to provide credentials for the Toolbox server.

Select "As User" and enter username and password of the account who have defined

access to the Toolbox Server application on the remote machine for this presentation is

the **ToolboxSvr.** 

Remote Toolbox server 172.17.84.248		
Server Identity		
🔘 As current user	💽 As User	
Usernam	e:	
Passwore	d:	
🗸 ок	X Cancel	

## 4.3.2 Domain Client

On the toolbox remote wizard leave the selection "**As current user**" and then click "**OK**" the current user will be used to log to the server.

## **4.4 Troubleshooting DCOM**

#### 4.4.1 Configuration check list

Common for domain and non domain configurations:

DCOM is enabled on both client and the server

Toolbox Server is configured to run in "Interactive mode" (it is possible to define it "as user" but the user interface will not be accessible)

Firewall does not block connections on both client and server.

On the client the firewall is configured to allow Toolbox application inbound and outbound connections and TCP/IP port 135 is open for outbound connections

On the server the firewall is configured to allow ToolboxServer application inbound and outbound connections and TCP/IP port 135 is open for outbound connections

When in Non-Domain configuration:

There is defined user account (for instance "ToolboxSvr") on server and client with same name and password.

The Toolbox account ("ToolboxSvr") is logged into the server.

Toolbox account has privileges in the DCOM configure section to access, launch and activate ToolboxSvr object on both client and the server.

Clients connecting to the server provide user name and password

When in Domain configuration:

All domain users have granted DCOM access, launch and activation rights

The server object runs under an account granted with access, launch and activate rights.

Clients access the server from Toolbox start-up screen as "current user"

#### 4.4.2 Common errors

Error	Possible Issues	Solution
The RPC server	The computer really doesn't	Add Toolbox server application to
unavailable	exist.	the firewall's exceptions list and
	The Windows Firewall on the	open TCP/IP port 135.
	server is blocking the connection	
Access denied	DCOM is not enabled.	1. Check if server and client
	Client firewall blocks connection.	firewalls allow connections.
	The user does not have remote	2. Check if server runs under
	access to the computer through	account that has DCOM rights.
	DCOM.	
Client is compiled	The client and server versions	Update Toolbox server and
with different server	does not match	Toolbox Client to the latest
access library		version
Interface not	The implementation Toolbox	Update Toolbox server and

## QSAR Toolbox User Manual Toolbox 2.2 Client-Server Configuration

supported	Server interface of the server	Toolbox Client to the latest
	differs from the client	version.
	implementation or the client.	
Unable to bind client	Client does not allow callbacks	Grant access, launch and activate
ITBNotify callback	from the server. The server runs	permissions to the server's user
interface to the	under user account with no	account on the client.
server	defined granted DCOM rights on	
	the client.	
The server process	There is no logged user on the	Option 1 :
could not be started	server or the logged user does	Change the settings of the
because the	not have granted DCOM rights on	toolbox server object from
configured identity is	the Toolbox Server.	DCOMCNFG to work "as user"
incorrect. Check the		from the identity.
User name and		
Password.		
		Option 2: Grant DCOM access,
		launch and activate to the
		current user logged the system.

#### OECD

2, rue André Pascal 75775 Paris Cedex 16 France Tel.: +33 1 45 24 82 00 Fax: +33 1 45 24 85 00

ehscont@oecd.org