

## Remote Database Access

To allow another PC with SmartPTT installed on it to access your shared database, do the following settings on your PC (server):

- 1. Disable Firewall or allow access to the following ports:
  - TCP 1433
  - UDP 1434

To open some TCP or UDP ports, do the following settings:

## Windows XP

1. Click the Windows Start button and then click Control Panel. In Control Panel click Security

Center.

2. In the Windows Security Center dialog box, click Windows Firewall.



3. In the **Windows Firewall** dialog box, click the **Exceptions** tab and then click the **Add Port** button.

🎉 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
IFile and Printer Sharing     Network Diagnostics for Windows XP
Remote Assistance
Remote Desktop
UPnP Framework
Add P <u>r</u> ogram Add P <u>o</u> rt <u>E</u> dit <u>D</u> elete
Display a notification when Windows Firewall blocks a program
What are the risks of allowing exceptions?
OK Cancel



Add TCP and UDP port numbers for the incoming connections – 1433 and 1434 values accordingly.

Add a Port	Edit a Port
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.	Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.
Name:     TCP for SmartPTT       Port number:     1433       ICP     UDP	Name:     UDP for SmartPTT       Port number:     1434       O     ICP
What are the risks of opening a port?	What are the risks of opening a port?
Change scope OK Cancel	Change scope OK Cancel

## Windows 7

- 1. Open the System and Security window (Start > Control Panel > System and Security) and run Windows Firewall.
- 2. Select **Advanced Settings** in the left of the panel.
- 3. Enter the administrator password if required. Otherwise, skip the step.
- 4. Add the TCP (1433) and UDP (1434) port values to allow incoming connections. To do that, click Inbound Rules in the left side of the Windows Firewall with Advanced Security window. Click New Rule on the right side of the window. Select Port in the New Inbound Rule Wizard and then click Next. Specify the required rule protocols and ports.
- 2. Run SQL Server Configuration Manager (Start > Microsoft SQL Server 2008 > Configuration Tools > SQL Server Configuration Manager).



3. In the **Protocols for SQLEXPRESS** tab select *Enabled* in the **Shared Memory** and **TCP\IP** fields.

🗢 🔿   🚈   🖾 🧟 🗟   👔			
SQL Server Configuration Manager (Local)	Protocol Name	Status	
SQL Server Services	Shared Memory	Enabled	
SQL Server Network Configuration	Named Pipes	Disabled	
Protocols for SQLEXPRESS	TCP/IP	Enabled	
SQL Native Client 11.0 Configuration			

Set the automatic startup mode for SQL Server Browser. In order to do that, select Automatic value

in the Start Mode field of the SQL Server Services tab.

🗖 General	
Binary Path	"C:\Program Files\Microsoft SQL Se
Error Control	1
Exit Code	0
Host Name	GRISHINAEV
Name	SQL Server Browser
Process ID	5004
SQL Service Type	SQL Browser
Start Mode	Automatic 🗾 👻
State	Running



Run the service.

🗢 🏟 🞽 🖺 🔒 📔 🕟 🗉 💿 🕐					
<ul> <li>SQL Server Configuration Manager (Local)         <ul> <li>SQL Server Services</li> <li>SQL Server Network Configuration</li> <li>SQL Native Client 11.0 Configuration</li> </ul> </li> </ul>	Name	State	Start Mode	Log On As	Pro
	SQL Server (SQLEXPRESS)	Running Stopped	Automatic Other (Boot,	NT Service\MSSQL NT AUTHORITY\NE	164 0
	SQL Server Browser	Stopped	Automatic	NT AUTHORITY\LO Start	Î
				Stop	
				Pause Resume	

4. Set the automatic startup mode for **SQL Server (SQLEXPRESS)**. In order to do that, select *Automatic* value in the **Start Mode** field of the **SQL Server Services** tab. Restart the service.

🗢 🔿   🙇   🗟 📑					
SQL Server Configuration Manager (Local)	Name	State	Start Mode	Log On As	Pro
SQL Server Services	SQL Server (SQLEXPRESS)	Running	Automatic	NT Service\MSSQL	164
Je SQL Server Network Configuration     SQL Native Client 11.0 Configuration	SQL Server Agent (SQLEXPR	Stopped	Other (Boot,	NT AUTHORITY\NE	0
, <u>, , ,</u> oge nærre enent 110 conniguration	SQL Server Browser	Running	Automatic	NT AUTHORITY\LO	773

5. If Windows authentication is used, add user and then add created user to the **Administrators** group.

Note: Skip this step if both of the computers are in the same domain.

To allow another computer with SmartPTT Dispatcher installed on it to access your shared database (client):

- 1. Install the SmartPTT Dispatcher application on this PC. Installation of SQL Server Express is not required.
- 2. Disable Firewall or allow access to the following ports:
  - TCP 1433
  - UDP 1434

To do this, follow the instructions described in the step 2 of the server settings. If Windows 7, select

Outbound Rules in the left side of the Windows Firewall with Advanced Security window.

5



 If you use Windows authentication, add the user with the same name and password as the user of the PC where SQL Server Express is installed. The user should be added to the Administrators group.

Note: Skip the step if both of the computers are in the same domain.

3. Log on to the system under the created account as Administrator.

4. Run SmartPTT Dispatcher.

If the database server installed together with SmartPTT Dispatcher, enter the path to the database in the **Database Server Name** field of the **Database Connection** window (**Settings** > **Database Settings**) using the following format: *IP address PC\SQLExpress* (for example, *192.168.0.50 \SQLExpress*). Otherwise, specify IP address of the PC only (for example, *192.168.0.50*).