

SmartPTT Enterprise 9.1 Dispatcher Remote Database



January 2017

Contents

Remote Database	3
Configuring Protocols	4
Configuring Services	6
Configuring SQL Server	13
Adding Windows Login	19
Adding SQL Server Login	23
Creating Firewall Rules	30
Connecting Remote Database	38

1 Remote Database

You can create or connect to the SmartPTT Dispatcher database on a remote computer (remote database).

Before creating or connecting, make sure the remote computer has the following software installed:

- Microsoft SQL Server,
- Microsoft SQL Server Configuration Manager,
- Microsoft SQL Server Management Studio.

You can download this software from <u>http://www.microsoft.com/en-</u> <u>US/download/details.aspx?id=42299</u>. For installation details, see the corresponding installation guides.

If both your computer and remote computer has the active firewall, make sure the following ports are unblocked:

- TCP port *1433*,
- UDP port *1434*.

2 Configuring Protocols

To configure Protocols, perform the following actions:

- 1. Start Microsoft SQL Server Configuration Manager.
- 2. Expand SQL Server Network Configuration node.



3. Click **Protocols for <Your SQL Server Name>**.



Figure 2 - Protocols for <Your SQL Server Name>

4. In the right pane of the **Sql Server Configuration Manager** window, right-click **Shared Memory** and click **Enable**.



Figure 3 – Enabling Shared Memory

5. In the **Warning** window, click **OK**.



Figure 4 – Warning Window Confirmation

6. In the right pane of the **Sql Server Configuration Manager** window, right-click **TCP/IP** and then click **Enable**.

Sql Server Configuration Manager						
File Action View Help						
🗢 🄿 🖄 🖾 🗟 🔒						
🕵 SQL Server Configuration Manager (Local)	Protocol Name	Status				
 SQL Server Services SQL Server Network Configuration Protocols for SQLEXPRESS SQL Native Client 11.0 Configuration 	 For a start of the start of the	Enabled Disabled	Enable Disable Properties Help			

Figure 5 – TCP/IP Enabling

7. In the **Warning** window, click **OK**.



Figure 6 – Warning Window Confirmation

8. Configure Services.

Protocols configuration complete.

3 Configuring Services

To configure Services, perform the following actions:

 In the left pane of the Sql Server Configuration Manager window, click SQL Server Services.

Sql Server Configuration Manager					
File Action View Help					
SQL Server Configuration Manager (Local) □ SQL Server Services ▷ □ SQL Server Network Configuration ▷ □ SQL Server Network Configuration ▷ □ SQL Native Client 11.0 Configuration	Items ■ SQL Server Services ■ SQL Server Network Configuration ■ SQL Native Client 11.0 Configuration				
Figure 7 – SQL Server Services					

- 2. In the right pane of the **Sql Server Configuration Manager** window, stop the following services if they are active:
 - SQL Server Services (<Your SQL Server Name>),
 - SQL Server Browser.
- 3. Right-click **SQL Server** (**<Your SQL Server Name>**) and then click **Properties**.

Sql Server Configuration Manager								
File Action View Help Image: Solution of the state Image: State State State Solution of the state State State State Dog On As Process ID Service Type								
SQL Server Configuration Manager (Local) Name SQL Server Services SQL Server Network Configuration SQL Server Network Configuration SQL Server Network Configuration SQL SQL Server Network Configuration SQL Server Network Configuration	SQL Server (SQLEXPR SQL Server Agent (SQ SQL Server Browser	Vame State SQL Server (SQLEXPR SQL Server Agent (SQ SQL Server Browser Pause Resume Restart	ie ime art		Start Mode Other (Boot, Syste Other (Boot, Syste Other (Boot, Syste	Log On As LocalSystem NT AUTHORITY\NE NT AUTHORITY\LO	0 0 0	SQL Server SQL Agent SQL Browser
		Prop Help	perties					

Figure 8 – Properties of SQL Server (<Your SQL Server Name>)

4. On the **Service** tab of the **SQL Server (<Your SQL Server Name>) Properties** window, click **Disabled**.

	Startup Para	meters	Advanced
Log On	Service	FI	ESTREAM
General			
Binary Path	"C:\Progr	am Files\N	licrosoft SQL Se
Error Control	1		
Exit Code	0		
Host Name	USER-PC		
Name	SQL Serve	er (SQLEXP	RESS)
Process ID	0		
SQL Service Type	SQL Serve	er	
Start Mode	Disabled		
State	Stopped		
Rinary Dath			

Figure 9 – Start Mode of SQL Server Properties

5. In the list, click **Automatic** and then click **OK**.

AlwaysOn High Availability	Start	ip Para	ameters	Advanced
Log On	Service		FIL	ESTREAM
General				
Binary Path	°C	:\Prog	ram Files\M	icrosoft SQL Se
Error Control	1			
Exit Code	0			
Host Name	09	SER-PC		
Name	SC)L Serv	er (SQLEXPF	RESS)
Process ID	0			
SQL Service Type	SC)L Serv	/er	
Start Mode	Di	sabled	i	•
State	A	utoma	tic	
	D	isable	d	
	M	anual		
Start Mode The start mode of this service	2.			

Figure 10 – Changing Start Mode

6. Click **OK** to apply changes and close the window.

In the right pane of the Sql Server Configuration Manager window, right-click
 SQL Server (<Your SQL Server Name>) and click Start.

Sql Server Configuration Manager File Action View Help										
SQL Server Configuration Manager (Local)	Name	State	Start Mode	Log On As	Process ID	Service Type				
SQL Server Services	💼 SQL Server (SQLEXPI	Chard	Automatic	LocalSystem	0	SQL Server				
SQL Server Network Configuration	👔 SQL Server Agent (S	Start	Other (Boot, Syste	NT AUTHORITY\NE NT AUTHORITY\LO	0 0	SQL Agent				
▷	👼 SQL Server Browser	Stop	Other (Boot, Syste			SQL Browser				
		Pause								
		Resume								
		Restart								
		Properties								
		Help								

Figure 11 – SQL Server (<Your SQL Server Name>) Starting

8. In the right pane of the **Sql Server Configuration Manager** window, right-click **SQL Server Browser** and click **Properties**.

Sql Server Configuration Manager								
File Action View Help								
SQL Server Configuration Manager (Local)	Name		State	Start Mode	Log On As	Process ID	Service Type	
SQL Server Services	SQL Server (S	QLEXPRESS)	Running	Automatic	LocalSystem	3536	SQL Server	
SQL Server Network Configuration	👔 SQL Server Ag	gent (SQLEXPRESS)	Stopped	Other (Boot, Syste	NT AUTHORITY\NE	0	SQL Agent	
	👼 SQL Server Br	owser	Stopped	Other (Boot, Syste	NT AUTHORITY\LO		SQL Browser	
		Start						
		Stop						
		Pause						
		Resume						
		Restart						
		Properties						
		Help						

Figure 12 - Properties of SQL Server Browser

 On the Service tab of the Sql Server Browser Properties window, click Disabled.

SQL Server Browser Properties	? 🔀					
Log On Service Advanced						
General						
Binary Path	"C:\Program Files\Microsoft SQL Se					
Error Control	1					
Exit Code	0					
Host Name	USER-PC					
Name	SQL Server Browser					
Process ID	0					
SQL Service Type	SQL Browser					
Start Mode	Disabled					
State	Stopped					
Binary Path						
Binary Path Path to the executable file for this service.						
ОК Са	Apply Help					

Figure 13 – Start Mode

10. In the list, click **Automatic** and then click **OK**.

SQL Server Browser Properties	? 🔀
Log On Service Advanced	
General	
Binary Path	"C:\Program Files\Microsoft SQL Se
Error Control	1
Exit Code	0
Host Name	USER-PC
Name	SQL Server Browser
Process ID	0
SQL Service Type	SQL Browser
Start Mode	Disabled 🔹
State	Automatic
	Disabled
	Manual
Start Mode	
The start mode of this service.	
ОК С	Cancel Apply Help

Figure 14 – Changing Start Mode

11. In the right pane of the **Sql Server Configuration Manager** window, right-click **SQL Server Browser** and click **Start**.

Sql Server Configuration Manager								
File Action View Help								
SQL Server Configuration Manager (Local)	Name	State	Start Mode	Log On As	Process ID	Service Type		
SQL Server Services	SQL Server (SQLEXPRESS)	Running	Automatic	LocalSystem	3536	SQL Server		
SQL Server Network Configuration	SQL Server Agent (SQLEXPRES	5) Stopped	Other (Boot, Syste	NT AUTHORITY\NE	0	SQL Agent		
》,호, SQL Native Client 11.0 Configuration	SQL Server B Start Stop Pause Resume Restart Propertie Help	5	Automatic	NT AUTHORITY\LO	0	SQL Browser		

Figure 15 – Starting SQL Server Browser

12. Close Sql Server Configuration Manager.

Services configuration complete.

4 Configuring SQL Server

To configure the SQL server, perform the following actions:

- 1. Run Microsoft SQL Server Management Studio.
- 2. In the **Server name** field of the **Connect to Server** window, enter the name of your SQL server and click **Connect**.

Kicrosoft SQL Server Management Studio					
File Edit View Debug Tools Window Help					
🗄 🔁 🕶 🗁 💭 🥔 🎴 💭 New Query 📑 📸 📸 🐇 💺 🛍 🛝 🔊 - (* -	· # • 🖳 🍇 > 🔄		- M	- N 😤 🛠 🔊	
Object Explorer 🝷 부 🗙	Connect to Server				
Connect - 🛃 📆 🔲 🍸 🛃	Sp connect to server				
	Microsoft SQ	L Server 2014			
	Server type:	Database Engine	-		
	Server name:	localhost\SQLExpress	-		
	Authentication:	Windows Authentication	•		
	User name:	USER-PC\Anton	*		
	Password:				
		Remember password			
	Connect	Cancel Help Opt	tions >>		

Figure 16 – Entering SQL Server Name

3. In the **Object Explorer** window, right-click the server name and click **Properties**.

14 Microsoft SQL Server Management Studio		
File Edit View Debug Tools Window Help		
🔢 🕈 🗃 🕶 🚰 💭 🥥 🔔 New Query 📑 📸 📸 👗 斗	월 19 - 연 - 문 4월 1월 1 - 1 - 1 28 - 19 - 19 - 19 - 19 - 19 - 19 - 19 - 1	
Object Explorer		
Connect 🕶 🛃 🔳 🍸 🙋 🎿		
Iocalhost\SQLExpress (SQL Server 12.0.4100 - USER-PC\USER)	Connect	
Databases	Disconnect	
Security Server Objects	Register	
E Replication	New Ouery	
🕀 🚞 Management	Artivity Manilar	
	Activity Monitor	
	Start	
	Stop	
	Pause	
	Resume	
	Restart	
	Policies	
	Facets	
	Start PowerShell	
	Reports >	
	Refrech	
	Properties	

Figure 17 – SQL Server Properties

4. In the **Select a page** pane of the **Server Properties** window, click **Security**.

Server Properties - localhost	SQLExpress	
Select a page	🔄 Script 🔻 📑 Help	
Memory		
Processors		
😭 Security		
Connections	Name	USER-PC\SQLEXPRESS
🚰 Database Settings	Product	Microsoft SQL Server Express
Advanced	Operating System	Microsoft Windows NT 6.1 (7601)
Permissions	Platform	NT INTEL X86
_	Version	12.0.4100.1
	Language	English (United States)
	Memory	3584 MB
	Processors	1
	Root Directory	C:\Program Files\Microsoft SQL Server\MSSQL12
	Server Collation	SQL Latin1 General CP1 CI AS
	Is Clustered	False
	Is HADR Enabled	False
Connection		
C		
Server: localhost\SQLExpress		
Connection: USER-PC\USER	Name Name of the server and instance.	
View connection properties		
Progress	Changes to server properties :	and settings may affect the performance, security, and
	availability of this SQL Server	instance. Before making any such changes, consult the
Ready	product documentation.	
		OK Cancel

Figure 18 – Selecting SQL Server Security

5. In the right pane of the Server Properties window, click SQL Server and Windows Authentication mode.

Server Properties - localhost\	SQLExpress
Select a page	Script 👻 📑 Help
General Memory Processors Connections Database Settings Advanced Permissions	Server authentication
Connection	Password:
Server: localhost\SQLExpress	Options
Connection: USER-PC\USER View connection properties Progress	 Enable C2 audit tracing Cross database ownership chaining
Ready	
	OK Cancel

Figure 19 – SQL Server Authentication Mode

6. In the **Select a page** pane of the **Server Properties** window, click **Connections**.

Server Properties - localhost	Server Properties - localhost\SQLExpress				
Select a page	Script 🔻 📑 Help				
Processors Security Connections Database Settings Advanced Permissions	Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing None Failed logins only Successful logins only Both failed and successful logins Server proxy account Enable server proxy account				
Connection	Password				
Server: localhost\SQLExpress	Options				
Connection: USER-PC\USER View connection properties	 Enable C2 audit tracing Cross database ownership chaining 				
Progress					
Ready					
	OK Cancel				

Figure 20 – Selecting SQL Server Connections

7. In the right pane of the **Server Properties** window, select **Allow remote connections to this server**.

🚦 Server Properties - localhost	SQLExpress	_ • ×
Select a page	Script 👻 📑 Help	
Memory Processors Security Connections Database Settings Advanced Permissions	Connections Maximum number of concurrent connections (0 = unlimited): Use query govemor to prevent long-running queries Default connection options: implicit transactions cursor close on commit ansi wamings ansi padding ANSI NULLS arithmetic abort	
Connection	Remote server connections	
Server: localhost\SQLExpress Connection: USER-PC\USER Wiew connection properties	 Allow remote connections to this server Remote query timeout (in seconds, 0 = no timeout): 600 Require distributed transactions for server-to-server communication 	
Progress		
Ready	Configured values	
	ОК	Cancel

Figure 21 – Allowing Remote Server Connections

- 8. Click **OK** to close the window.
- 9. In the **Object Explorer** window, right-click the server name and click **Restart**.



Figure 22 – SQL Server Restart

10. Add <u>Windows</u>⁽¹⁹⁾ or <u>SQL Server</u>⁽²³⁾ logins to the SQL Server.

Configuration of the SQL Server complete.

5 Adding Windows Login

This topic is alternative to the "Adding SQL Server Login⁽²³⁾".

To connect to a remote database using the <u>Windows NT Authorization</u>⁽⁴⁰⁾ mode, Windows login access should be configured. It is applicable only if remote computer is in the same domain as your computer.

To add a Windows login to the SQL Server, perform the following actions:

1. In the **Object Explorer** window, expand **<Your Server Name>** → **Security**.



Figure 23 – Security Node

2. Right-click Logins then click New Login.



Figure 24 – New Login Creation

3. In the **Login name** field of the **Login** window, enter login name.

🖥 Login - New				- • ×
Select a page	🔄 Script 🔻 🛐 Help			
General				
User Mapping	Login name:			Search
Securables	Windows authentication			
	SQL Server authentication			
	Password:			
	Confirm password:			
	Specify old password			
	Old password:			
	Enforce password policy			
	✓ Enforce password expirat	tion		
	✓ User must change passw	vord at next login		
	Mapped to certificate		•	
	Mapped to asymmetric key			
Connection	Map to Credential			Add
Server:	Mapped Credentials	Credential Provid	er	
localhost\SQLExpress				
Connection: USER-PC\USER				
View connection properties				
Progress				Remove
Ready	Default database:	master	•	
	Default language:	<default></default>	•	
			ОК	Cancel

Figure 25 – Entering Login Name

NOTE

The login name consists of domain name and user name. For example,

"DOMAIN\User".

4. In the **Select a page** pane of the **Login** window, click **Server Roles**.

🖥 Login - New		
Select a page	🔄 Script 🔻 🛐 Help	
Server Roles	Login name:	DOMAIN\User Search
Securables	Windows authentication	
	SQL Server authentication	
	Password:	
	Confirm password:	
	Specify old password	
	Old password:	
	✓ Enforce password policy	
	Enforce password expiration	tion
	✓ User must change passw	vord at next login
	Mapped to certificate	· · · · · · · · · · · · · · · · · · ·
	Mapped to asymmetric key	· · · · · · · · · · · · · · · · · · ·
Connection	Map to Credential	Add
Server: localhost\SQLExpress	Mapped Credentials	Credential Provider
Connection: USER-PC\USER		
View connection properties		
Progress		Remove
Ready	Default database:	master 💌
The state of the s	Default language:	<default></default>
	·	OK Cancel

Figure 26 – Selecting Server Roles

5. In the right pane of the **Login** window, select **sysadmin** and click **OK**.

🗄 Login - New		
Select a page	🕄 Script 💌 🖪 Help	
General Server Roles User Mapping Securables Status	Server role is used to grant server-wide security privileges to a user. Server roles: bulkadmin dbcreator diskadmin processadmin public securityadmin setupadmin setupadmin sysadmin	
Connection		
Server: localhost\SQLExpress Connection: USER-PC\USER Wiew connection properties		
Program		
Ready		
	ОК	Cancel

Figure 27 – Sysadmin Security Privelege

6. Close SQL Server Management Studio.

Adding Windows login complete.

6 Adding SQL Server Login

This topic is alternative to the "Adding Windows Login⁽¹⁹⁾".

To connect to a remote database using the <u>SQL Server authorization</u>⁽⁴⁰⁾ mode, SQL login access should be configured. This is a universal method of the remote database access.

To add a SQL Server login to the SQL Server, perform the following actions:

1. In the **Object Explorer** window, expand **<Your Server Name>** → **Security**.



Figure 28 – Security Node

2. Right-click Logins and click New Login.



Figure 29 – New Login

3. In the right pane of the **Login** window, enter **Login name**.

🗄 Login - New		[- • •
Select a page	🔄 Script 🔻 🛐 Help		
Server Roles			
User Mapping	Login name:		Search
Status	Windows authentication		-
_	SQL Server authentication		
	Password:]
	Confirm password:]
	Specify old password		
	Old password:]
	✓ Enforce password policy		- -
	Enforce password expirat	tion	
	✓ User must change passw	vord at next login	
	Mapped to certificate]
	Mapped to asymmetric key]
Connection	Map to Credential	~	Add
Server:	Mapped Credentials	Credential Provider	
localhost\SQLExpress			
Connection: USER-PC\USER			
View connection properties			
Progress			Remove
Ready	Default database:	(master 🗸]
1445°	Default language:	<default></default>]
		ОК	Cancel

Figure 30 – Entering Login Name

4. Click **SQL server authentication**.

🖥 Login - New		
Select a page	🔄 Script 🔻 📑 Help	
General Server Roles User Mapping Securables Status	Login name: Windows authentication SQL Server authentication Password: Confirm password: Specify old password Old password: Vindows authentication	User Search
	Enforce password expira	tion
	User must change passv	vord at next login
	Mapped to certificate	· · · · · · · · · · · · · · · · · · ·
	Mapped to asymmetric key	· · · · · · · · · · · · · · · · · · ·
Connection	Map to Credential	Add
Server: localhost\SQLExpress Connection: USER-PC\USER	Mapped Credentials	Credential Provider
View connection properties		
Progress		Remove
Ready	Default database: Default language:	master ▼ <default> ▼</default>
		OK Cancel

Figure 31 – SQL Server Authentication

SmartPTT Enterprise 9.1 Dispatcher Remote Database

5. Enter and confirm the password.

🖥 Login - New				(- • ×
Select a page	<u>S</u> Cript 🝷	Help			
Server Roles	Login name:		User		Search
Securables	 Windows 	authentication			
	SQL Serv	ver authentication			_
	Password	d:	•••••		
	Confirm p	assword:	•••••		
	Speci	fy old password			1
	Old pi	assword: ce password policy			
	✓ Enfor	ce password expira	tion		
	V User	must change passv	vord at next login		
	Mapped t	o certificate		-	
	Mapped t	o asymmetric key			
Connection	Map to Ci	redential		-	Add
Server: localhost\SQLExpress	Mapped	Credentials	Credential	Provider	
Connection: USER-PC\USER					
View connection properties					
Progress					Remove
Ready	Default databas	e:	master	-]
A ⁴ P _A	Default languag	e:	<default></default>	•]
				ОК	Cancel

Figure 32 – Password Fields

6. Clear **User must change the password at next login** to keep user password.

🖥 Login - New		
Select a page	🔄 Script 🔻 🛐 Help	
Server Roles User Mapping Securables Status	Login name: Vindows authentication SQL Server authentication	User Search
	Password:	•••••
	Confirm password:	•••••
	Specify old password	
	Old password:	
	Enforce password policy	
	Enforce password expiration	tion
	Mapped to certificate	
	Mapped to certificate	
	Mapped to asymmetric key	×
Connection		▼ Add
Server: localhost\SQLExpress	Mapped Credentials	Credential Provider
Connection: USER-PC\USER		
View connection properties		
Progress		Remove
Ready	Default database:	master 💌
1445°	Default language:	<default></default>
	·	OK Cancel

Figure 33 – Option for Password Keeping

7. In the left **Select a page** pane of the **Login** window, click **Server Roles**.

🖥 Login - New			- • ×
Select a page	🔄 Script 🔻 🛐 Help		
Server Roles User Mapping Securables Status	Login name: Windows authentication SQL Server authentication	User	Search
	Password:	•••••	1
	Confirm password:	•••••	
	Old password:		
	Enforce password policy	i	
	User must change passw	vord at next login	
	Mapped to certificate		1
	Mapped to asymmetric key		í l
Connection	Map to Credential		Add
Server: localhost\SQLExpress Connection: USER-PC\USER	Mapped Credentials	Credential Provider	
Progress			Remove
Ready	Default database:	master]
44 ¹⁰ 4	Default language:	<default></default>	
		ОК	Cancel

Figure 34 – Selecting Server Roles

8. In the right pane of the **Login** window, select **sysadmin** and click **OK**.

🖥 Login - New		- • ×
Select a page	🛒 Script 🔻 📑 Help	
General Server Roles User Mapping Securables Status	Server role is used to grant server-wide security privileges to a user. Server roles: bulkadmin dbcreator diskadmin processadmin public securityadmin setupadmin sysadmin	
Connection		
Server: localhost\SQLExpress Connection: USER-PC\USER		
Progress		
Ready		
	ОК	Cancel

Figure 35 – Sysadmin Security Privelege

9. Close SQL Management Studio.

Adding SQL Server login complete.

7 Creating Firewall Rules

You should allow the connection to the following ports of the remote and your computers:

- port 1433, TCP protocol,
- port *1434*, UDP protocol.

The following instruction describes Windows Firewall configuration. If you are using other firewall software, please refer to the corresponding user guides.

To create Rules for TCP/UDP ports in the Windows Firewall, perform the following actions:

- 1. Open Windows Firewall.
- 2. Click Advanced Settings.



3. Enter administrator password if required.

4. In the left pane of the **Windows Firewall with Advanced Security** window, select the needed group of rules:

Second Security	
File Action View Help	
Windows Firewall with Advance Windows Firewall with Advanced Security on Local Computer	Actions
🗱 Inbound Rules	Windows Firewall with Advanced Security on Local Compu 🔺
Connection Security Rules Windows Firewall with Advanced Security provides network security for Windows compu	🔊 Import Policy
> 🍇 Monitoring	🝯 Export Policy
Figure 27 Calenting Needed Crews of	Dulas

Figure 37 – Selecting Needed Group of Rules

- **Inbound Rules**: Should be created on the remote computer,
- **Outbound Rules**: Should be created on your computer.

NOTE

Creating and configuring rules are identical for both Inbound Rules and Outbound Rules. The following steps are presented for Inbound Rule.

5. In the right pane of the **Windows Firewall with Advanced Security** window, click **New Rule...**

Provide the second seco	I Security				
File Action View Help					
🗢 🔿 🖄 🖬 🔒 🛛 🖬					
I Windows Firewall with Advance	Inbound Rules			Actions	
Inbound Rules	Name	Group	Profile 🔺	Inbound Rules	
Source of the security Rules	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	🗽 New Rule	
Monitoring	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	Filter by Profile	•
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All ≡	V Filter by State	
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Private	Pinter by State	•
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Domain	Filter by Group	•
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain 🚽	View	•
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	G Refresh	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private		
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	Export List	
	Connect to a Network Projector (WSD-In)	Connect to a Network Proje	All	🛛 👔 Help	
	Caro Notworking Destination Unroacha	Care Networking	A11	1	

Figure 38 – Creating New Rule

 In the right pane of the New Inbound Rule Wizard or New Outbound Rule Wizard window (if you create rules on your computer), click Port and then click Next.

🔐 New Inbound Rule Wizard		×
Rule Type		
Select the type of firewall rule to cr	eate.	
Select the type of firewall rule to cr Steps: Program Action Profile Name	eate. What type of rule would you like to create? Program Rule that controls connections for a program. Pot Rule that controls connections for a TCP or UDP pot. Predefined: BranchCache - Content Retrieval (Uses HTTP) Rule that controls connections for a Windows experience. C Custom Custom rule.	
	Learn more about rule types < Back Next > Cancel	

Figure 39 – Rule Type

7. Click **TCP** and then click **Next**.

🔐 New Inbound Rule Wizard	
Protocol and Ports	
Specify the protocols and ports to	which this rule applies.
Steps:	
Rule Type	Does this rule apply to TCP or UDP?
Protocol and Ports	● TCP
Action	© UDP
Profile	
Name	Does this rule apply to all local ports or specific local ports?
	All local ports
	Specific local ports:
	Example: 80, 443, 5000-5010
	Figure 40 – Port Type

8. In the **Specific local ports** field, enter *1433* and click **Next**.

🔐 New Inbound Rule Wizard	
Protocol and Ports	
Specify the protocols and ports to v	which this rule applies.
Steps:	
Rule Type	Does this rule apply to TCP or UDP?
Protocol and Ports	() TCP
Action	© UDP
Profile	
Name	Does this rule apply to all local ports or specific local ports?
	Specific local ports: 1/22
	Example: 80, 443, 5000-5010
	• • • •
	Learn more about protocol and ports
	< Back Next > Cancel

Figure 41 – Entering Port Number

9. Click **Allow the connection** and then click **Next**.

🔐 New Inbound Rule Wizard		×
Action		
Specify the action to be taken who	en a connection matches the conditions specified in the rule.	
Steps:		
Rule Type	What action should be taken when a connection matches the specified conditions?	
Protocol and Ports		
Action	Allow the connection This includes connections that are protected with IPsec as well as those are not	
Profile		
 Action Profile Name 	 Allow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customize Block the connection 	
	< Back Next > Cancel	

Figure 42 – Selecting Action

10. Select the needed profiles according to their description and click **Next**.

🔐 New Inbound Rule Wizard		×
Profile		
Specify the profiles for which this n	ule applies.	
Steps:		
Rule Type	When does this rule apply?	
Protocol and Ports		
Action	V Domain	
Profile	Applies when a computer is connected to its corporate domain.	
Name	 Private Applies when a computer is connected to a private network location. Public Applies when a computer is connected to a public network location. 	
	Learn more about profiles < Back Next > Cancel	

Figure 43 – Selecting Profile

11. In the **Name** field, enter the name of the rule and click **Finish**.

🔐 New Inbound Rule Wizard			×
Name			
Specify the name and description o	f this rule.		
Steps:			
Rule Type			
Protocol and Ports			
Action			
Profile		Name:	
Name	L		
		Description (optional):	
		< Back Finish Cancel	

Figure 44 – Name Entering

12. Repeat step 6 to step 12 for *1434* port (UDP protocol).

Creation of firewall rules complete.

8 Connecting Remote Database

To connect to a remote SmartPTT Dispatcher database, perform the following actions:

- 1. If you are not started SmartPTT Dispatcher for the first time, click **Settings** and then click **Database**.
- In the Database server name field of the Database window, enter the name of the remote SQL Server using the following format: <IP address of a remote computer>\<Name of a remote SQL server>.

SmartPTT Enterprise 9.1 Dispatcher Remote Database

Configuration		×
Database Settings for connection	to MS SQL Server database	Ö
– Database server –		
Database server name	localhost\SQLExpress	
	For database server installed locally at SmartPTT Dispatcher PC enter name in the following way: Name of Computer\SQLExpress (e.g., MYCOMP\SQLExpress).	
Authorization mode	Windows NT Authorization	-
Account name		
Password		
	Connect	
Database		
To set up a database,	connect to the database server. Create database Restore database	
Current database		
Help	Cancel Back Next Finish	

Figure 45 – Local SQL Server Name

3. In the **Authorization Mode** list, click the needed authorization type and then click **Connect**:

Configuration	×
Database Settings for connection	to MS SQL Server database
Database server	
Database server name	192.0.2.0\SQLExpress
	For database server installed locally at SmartPTT Dispatcher PC enter name in the following way: Name of Computer\SQLExpress (e.g., MYCOMP\SQLExpress).
Authorization mode	Windows NT Authorization
Account name	Windows NT Authorization SQL Server Authorization
Password	
	Connect
Database	
To set up a database, o	Create database Restore database
Current database	
Help	Cancel Back Next Finish

Figure 46 – Authorization Mode

- Windows NT Authorization: Select to use your Windows login for connecting to a remote SQL Server from the same domain or if <u>Windows login is added</u>⁽¹⁹⁾.
- **SQL Server Authorization**: Select to use remote SQL Server login if <u>SQL Server</u> login is added^[23].

4. If **SQL Server Authorization** is selected, enter login and password and then click **Connect**.

Configuration X		
Database Settings for connection to MS SQL Server database		
Database server		
Database server name	192.0.2.0\SQLExpress	
	For database server installed locally at SmartPTT Dispatcher PC enter name in the following way: Name of Computer\SQLExpress (e.g., MYCOMP\SQLExpress).	
Authorization mode	SQL Server Authorization	
Account name	User	
Password	****	
	Connect	
Database		
To set up a database, o	Create database Restore database	
Current database		
Help	Cancel Back Next Finish	

Figure 47 – Login and Password of SQL Server Login

5. From the **Current database** list select the needed remote database.

Configuration X		
Database Settings for connection to MS SQL Server database		
Database server		
Database server name	192.0.2.0\SQLExpress	
	For database server installed locally at SmartPTT Dispatcher PC enter name in the following way: Name of Computer\SQLExpress (e.g., MYCOMP\SQLExpress).	
Authorization mode	SQL Server Authorization	
Account name	User	
Password	*******	
	Connect	
Database		
Connection to the database server is established.		
_	Create database Restore database	
Current database		
Help	Cancel Back Next Finish	

Figure 48 – Selecting Remote Database

6. Click **Finish** to connect to the database.

7. If the **Warning** window appears, click **OK** and restart the SmartPTT Dispatcher.



Figure 49 – Warning Window

Connection to the remote SmartPTT Dispatcher database complete.





smartptt.com