SmartPTT Enterprise 9.1

Radioserver Remote Database

elcomplus

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
Remote Database Connection 38
Connecting to Remote Event Log Database 38
Connecting to Remote Monitoring Database 45
Connecting to Remote Metadata Database 52

1 Remote Database

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

Before 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 http://www.microsoft.com/en-US/download/details.aspx?id=42299. 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. Run **Microsoft SQL Server Configuration Manager**.
2. Expand **SQL Server Network Configuration** node.

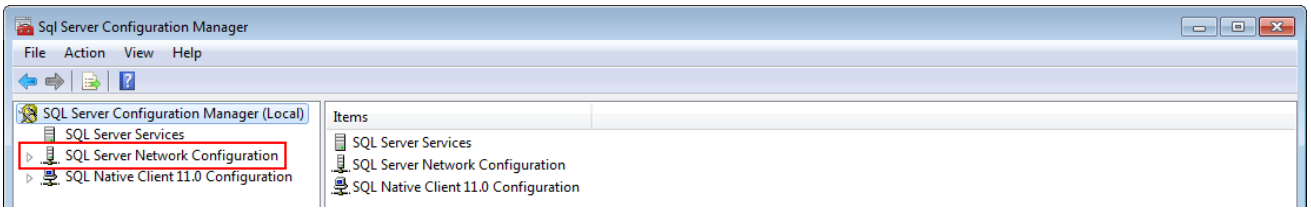


Figure 1 – SQL Server Network Configuration Node

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

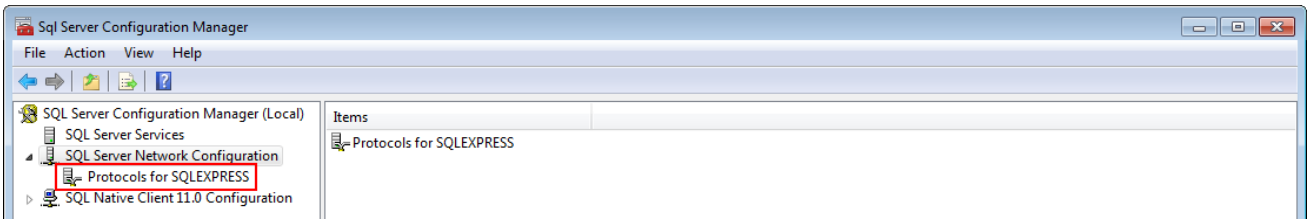


Figure 2 – Protocols for <Your SQL Server Name>

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

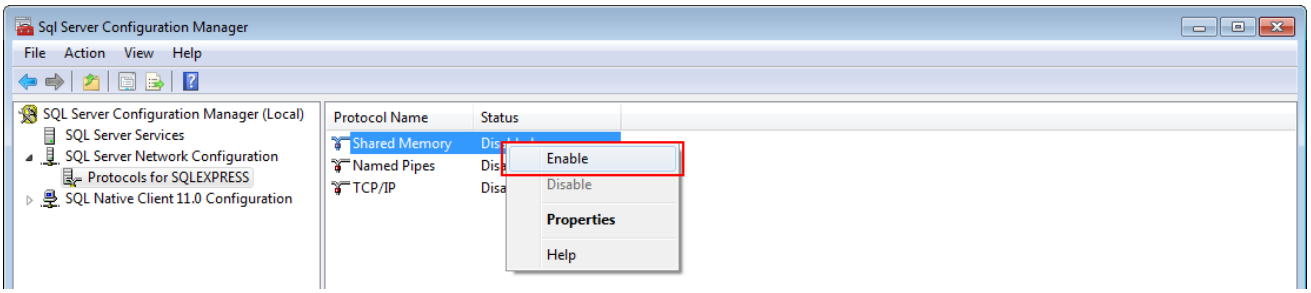


Figure 3 – Enabling Shared Memory

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

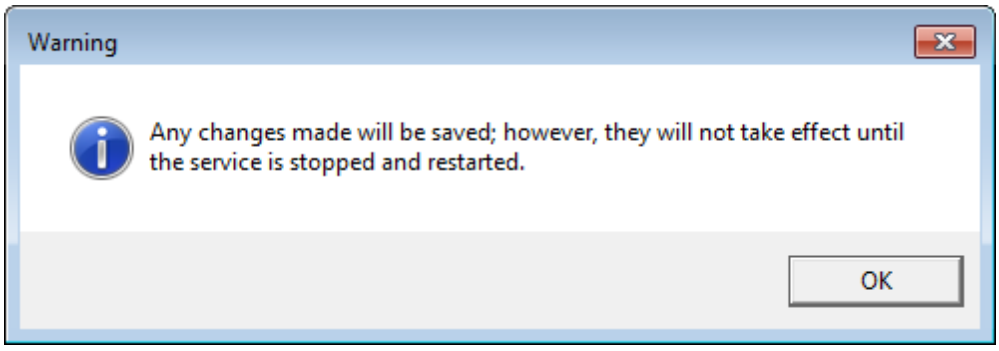


Figure 4 – Warning Window Confirmation

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

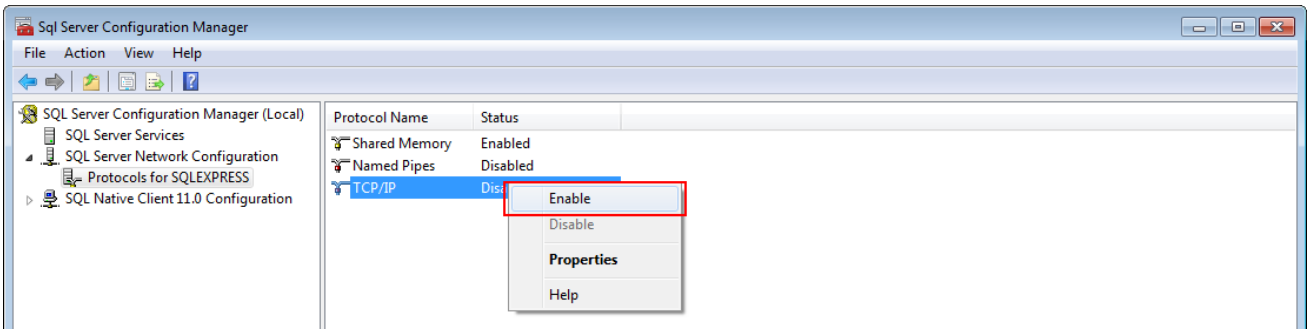


Figure 5 – Enabling TCP/IP

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

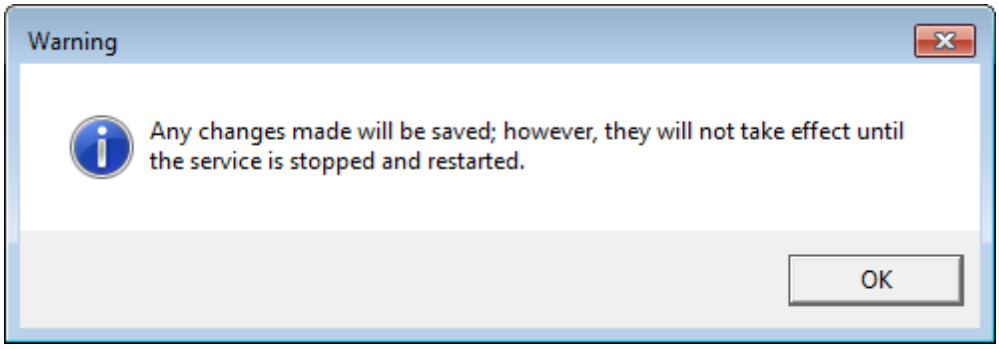


Figure 6 – Warning Window Confirmation

8. Configure Services.

Protocols configuration complete.

3 Configuring Services

To configure Services, perform the following actions:

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

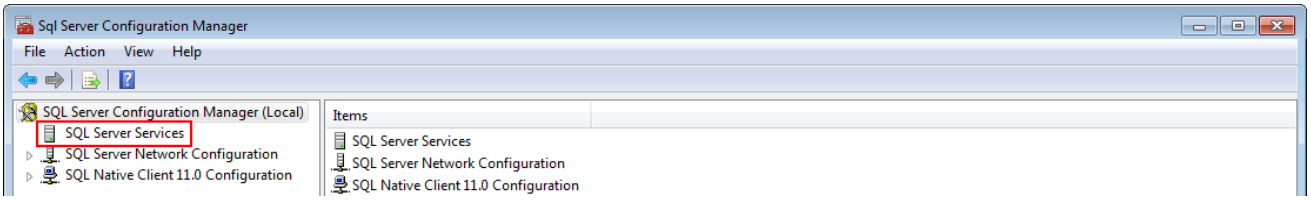


Figure 7 – SQL Server Services

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 click **Properties**.

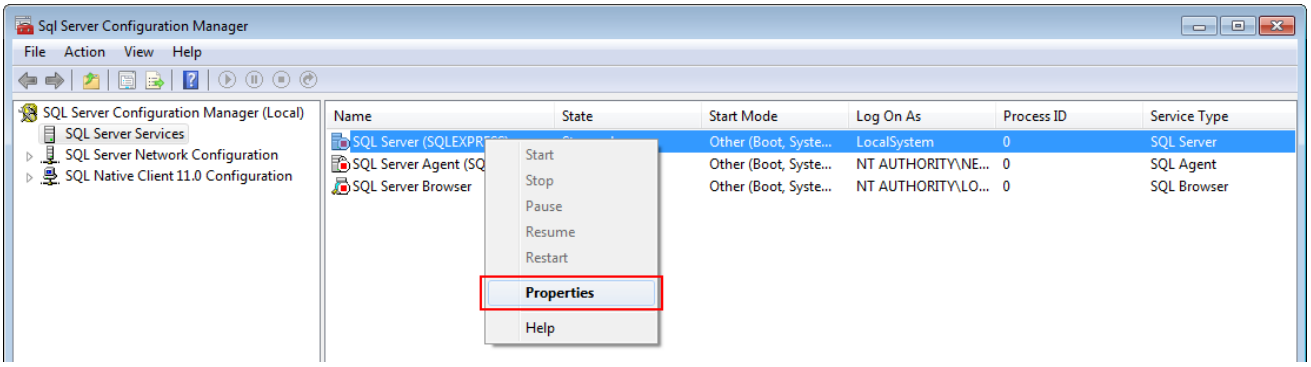


Figure 8 – Properties of SQL Server (<Your SQL Server Name>)

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

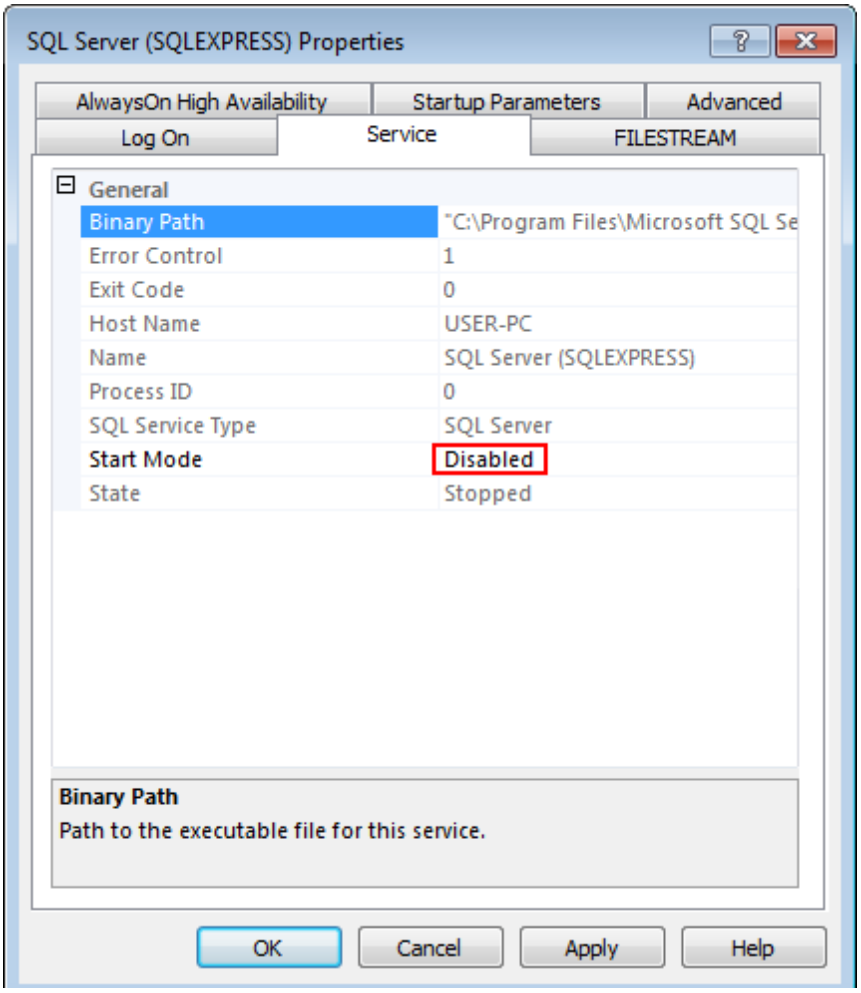


Figure 9 – Start Mode of SQL Server Properties

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

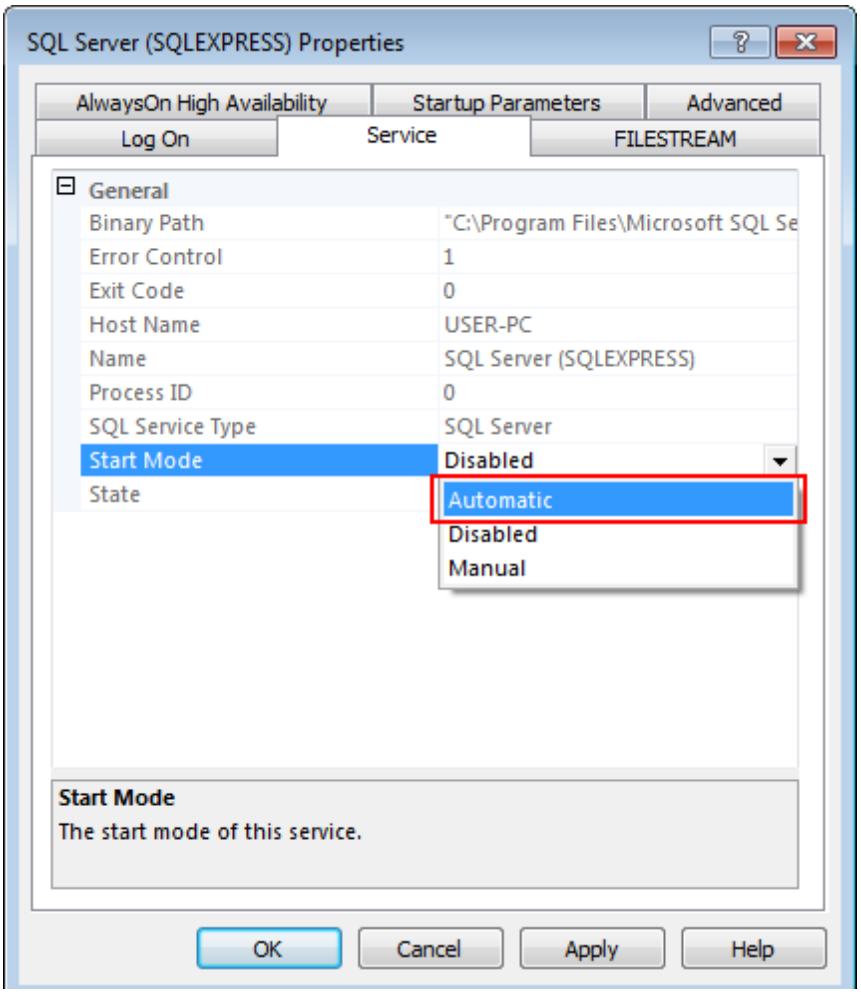


Figure 10 – Changing Start Mode

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

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

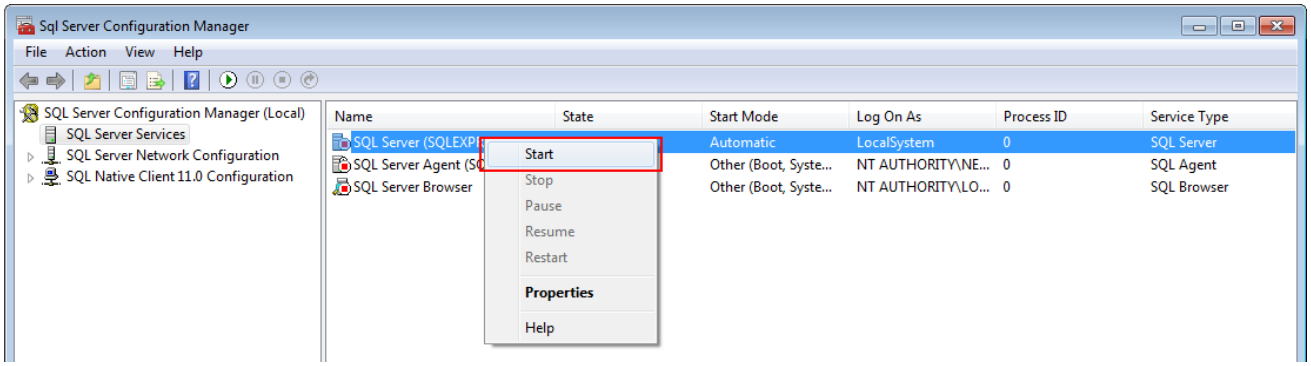


Figure 11 – Starting SQL Server (<Your SQL Server Name>)

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

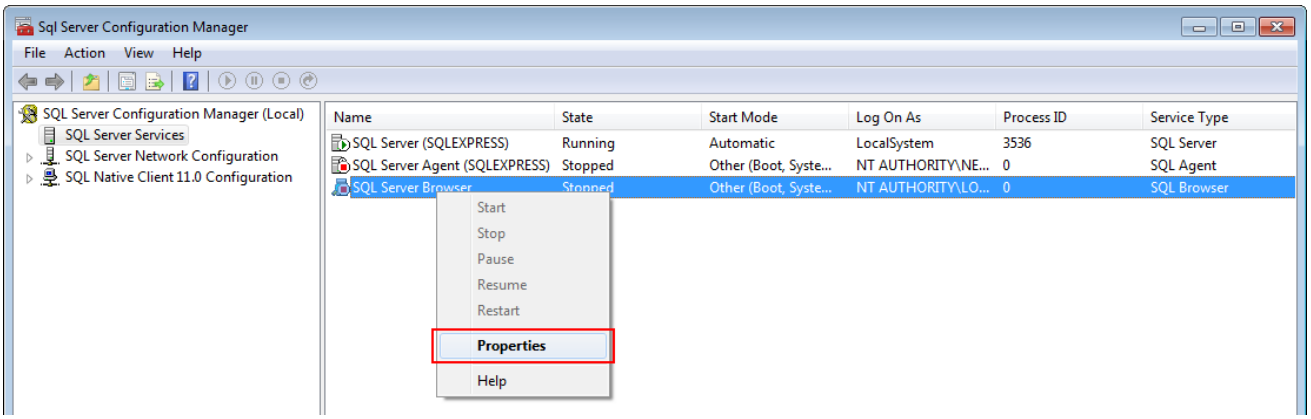


Figure 12 – Properties of SQL Server Browser

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

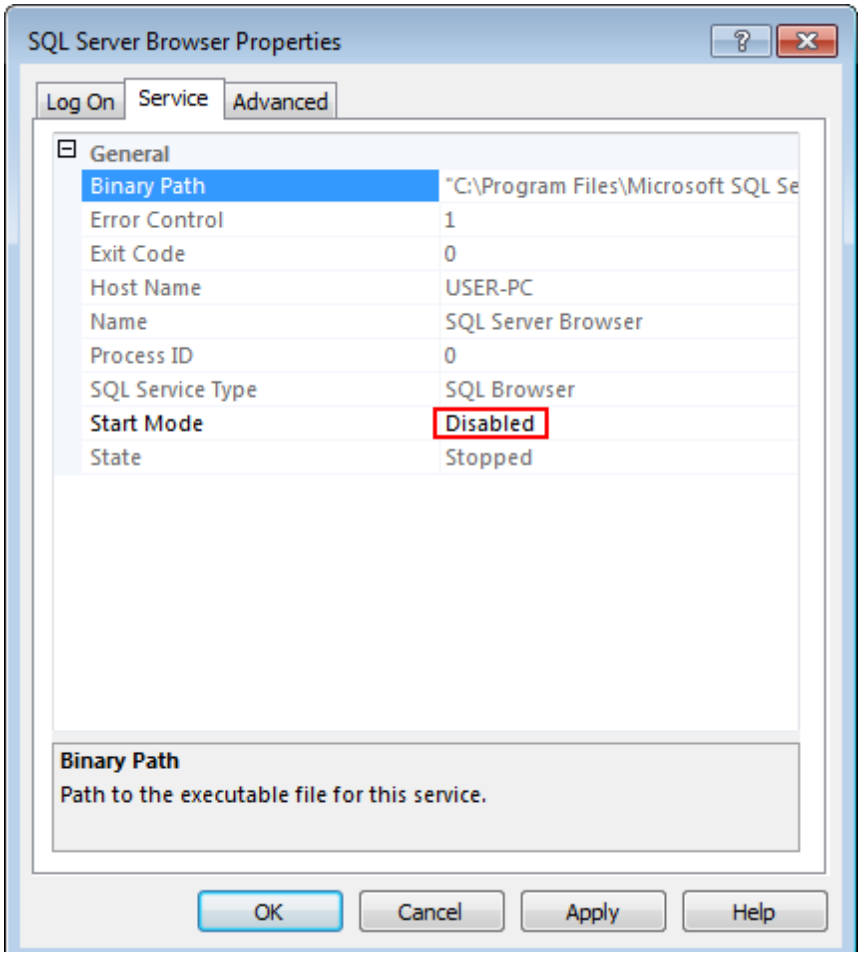


Figure 13 – Start Mode

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

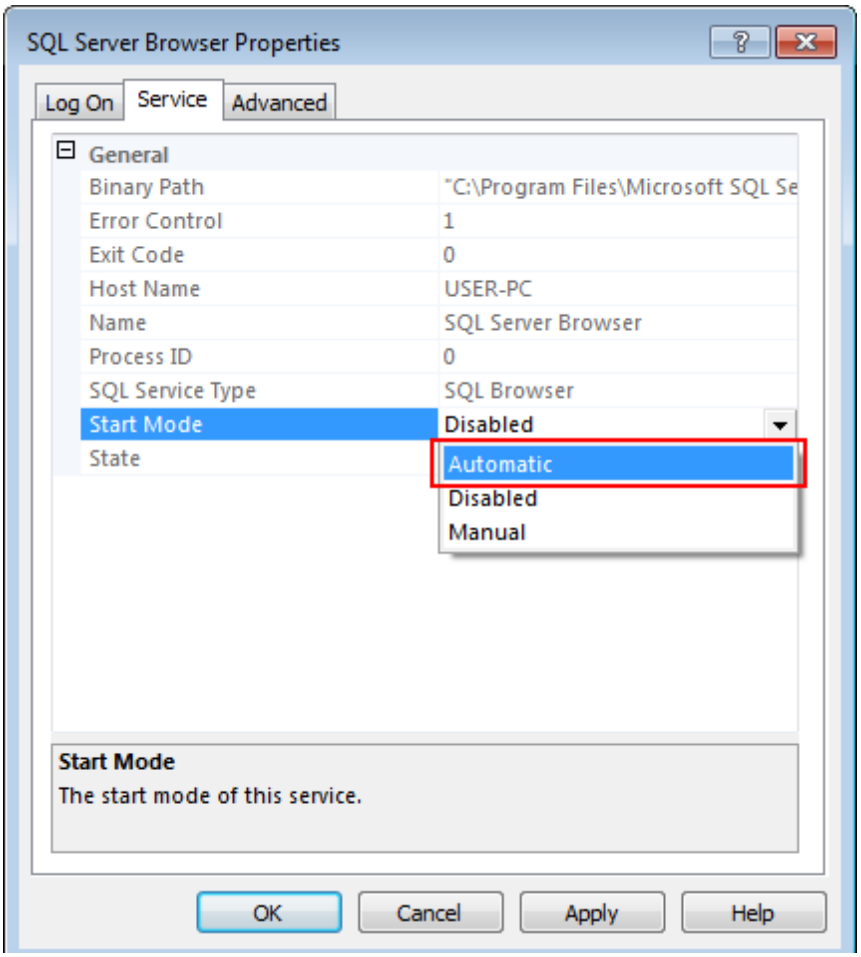


Figure 14 – Changing Start Mode

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

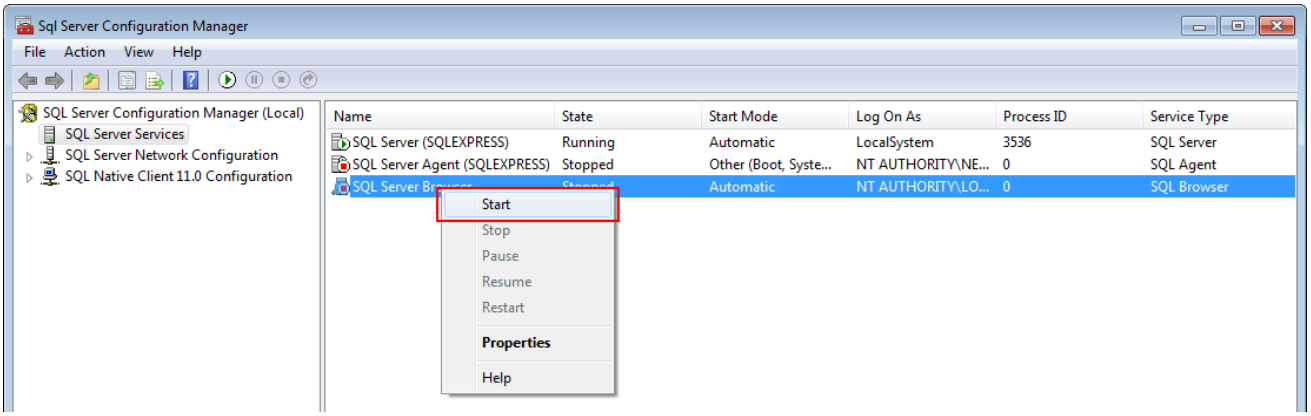


Figure 15 – Starting SQL Server Browser

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 server and click **Connect**.

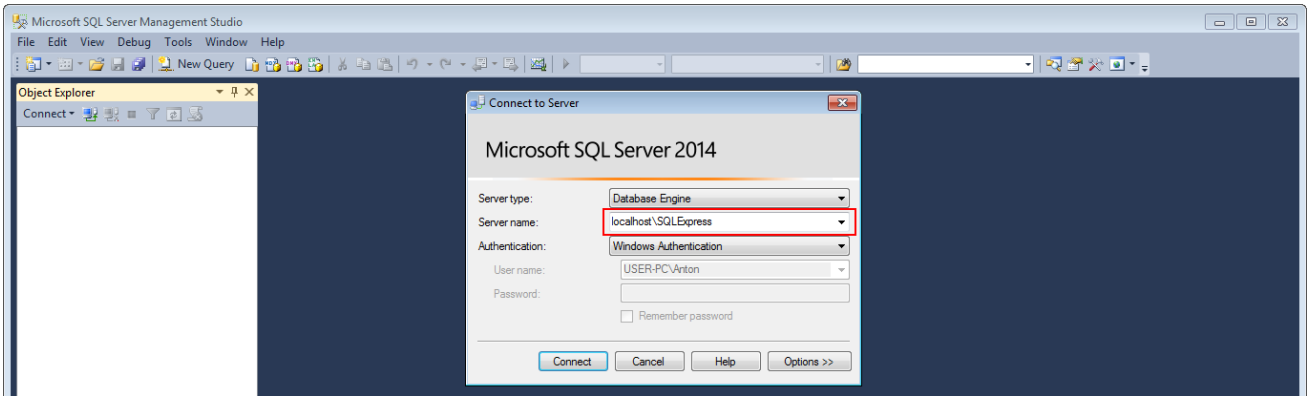


Figure 16 – Entering SQL Server Name

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

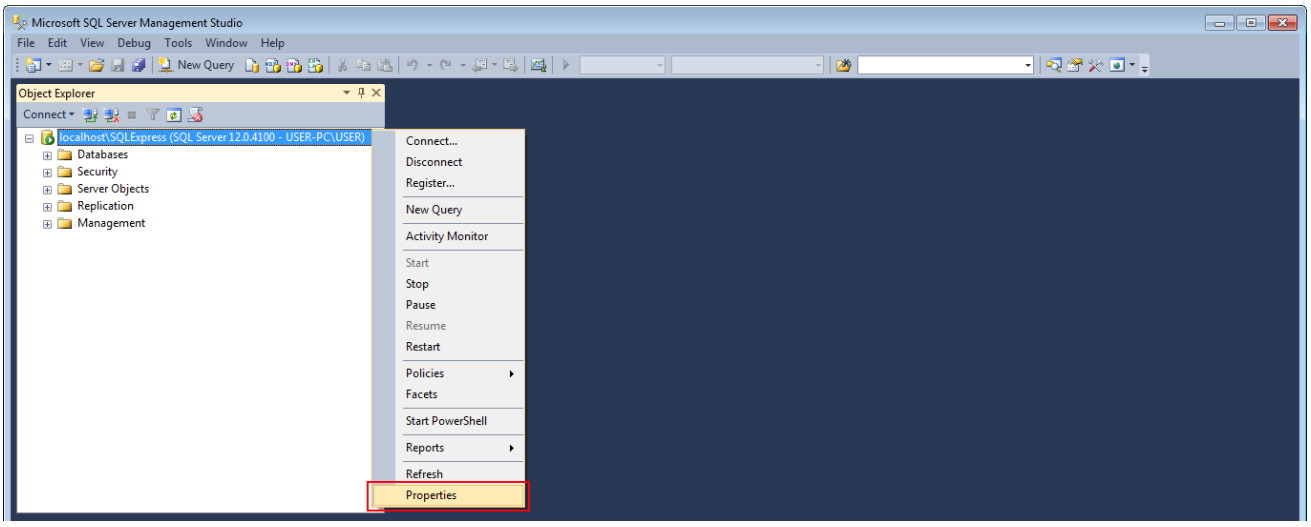


Figure 17 – SQL Server Properties

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

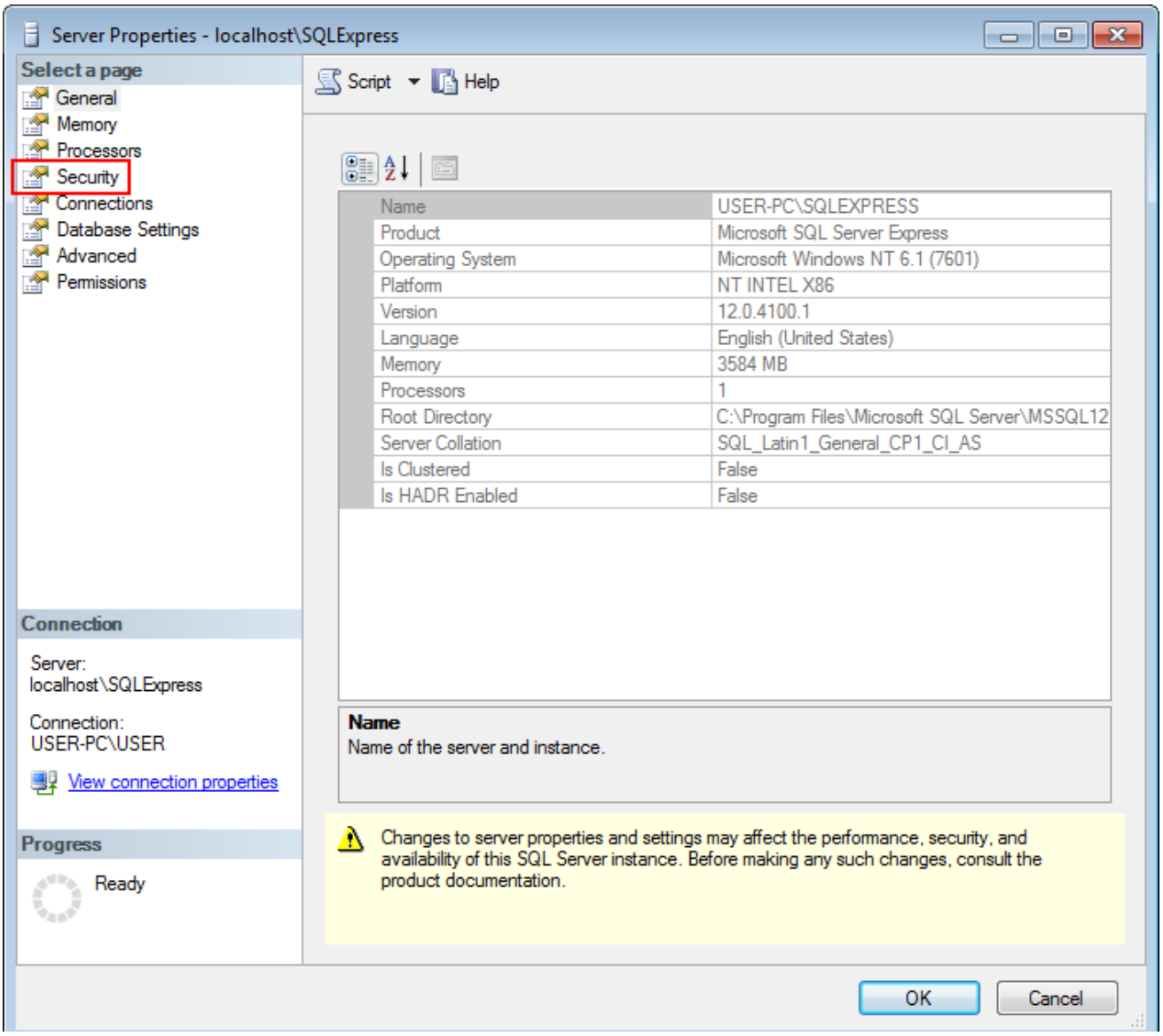


Figure 18 – Selecting SQL Server Security

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

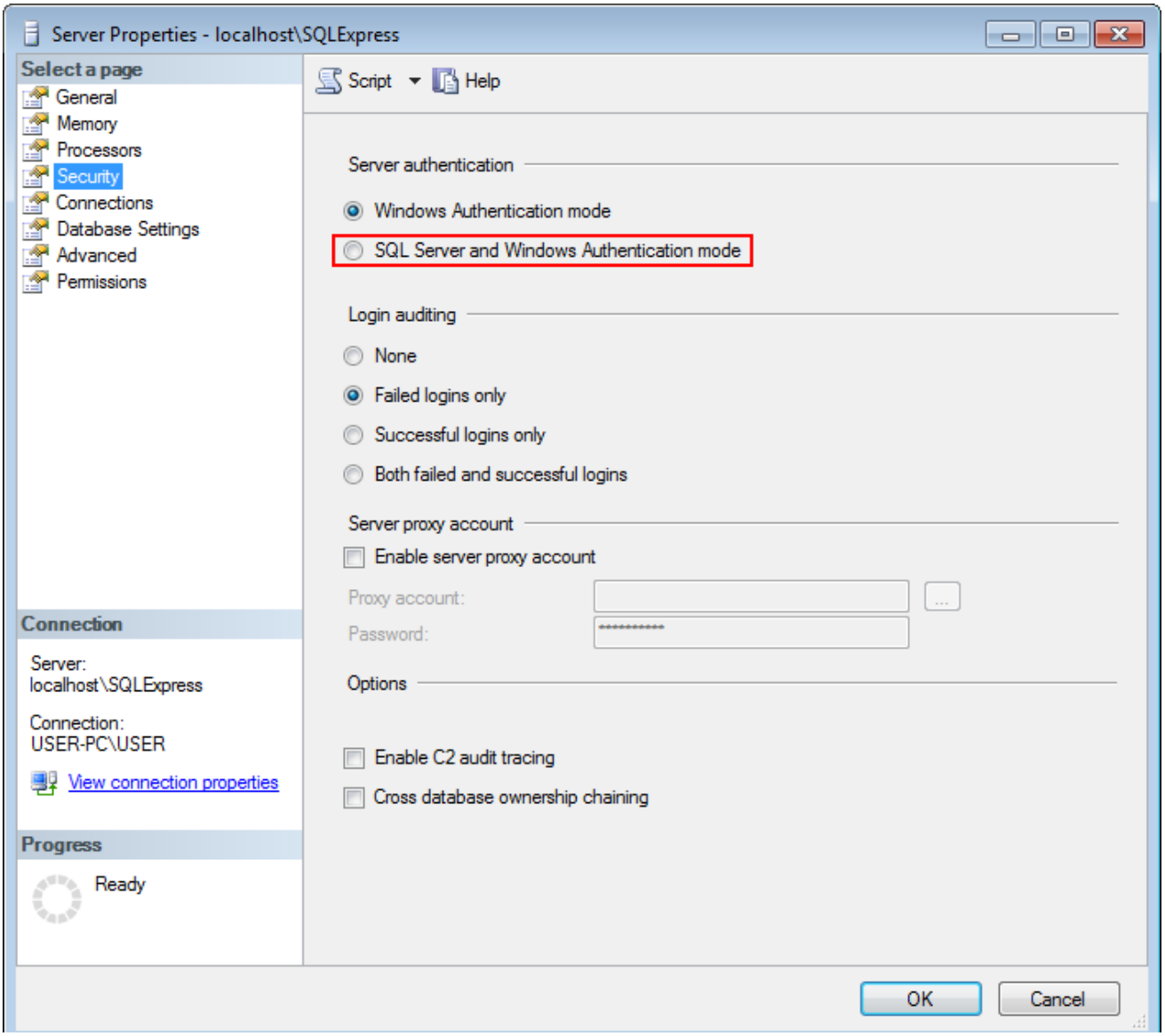


Figure 19 – SQL Server Authentication Mode

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

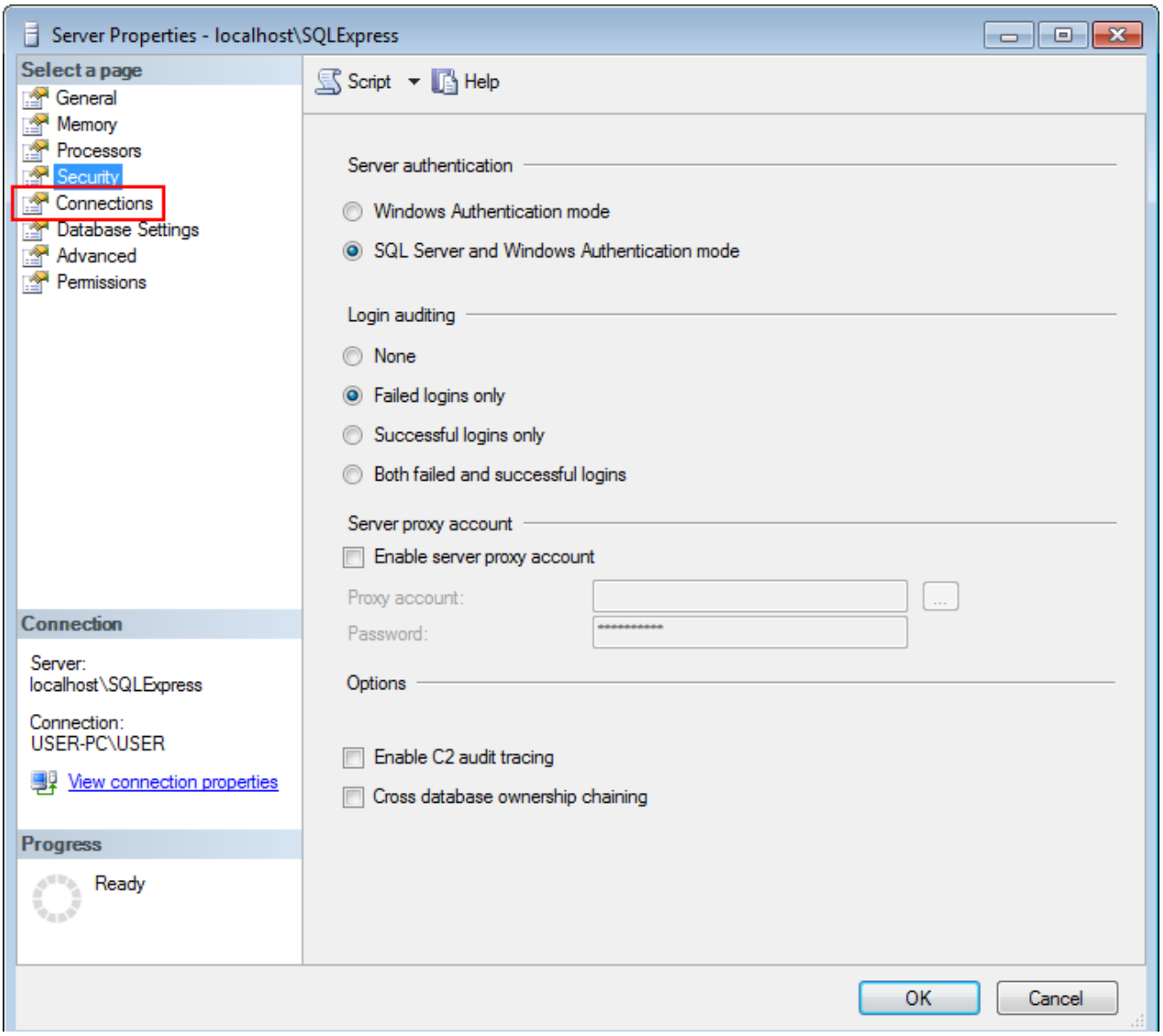


Figure 20 – Selecting SQL Server Connections

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

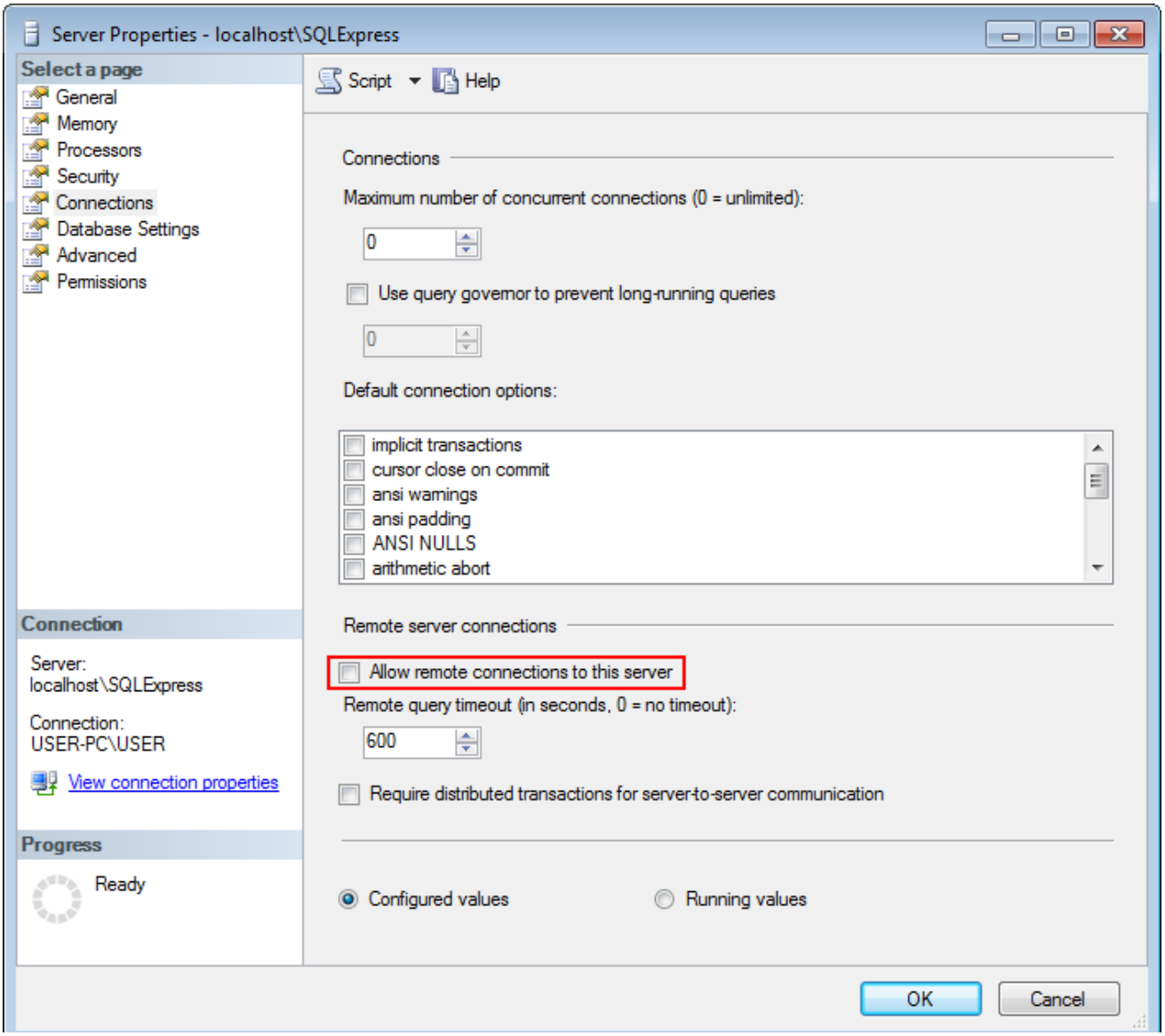


Figure 21 – Allowing Remote Server Connections

8. Click **OK** to close the window.

9. In the **Object Explorer** window, right-click the server name and click **Restart**.

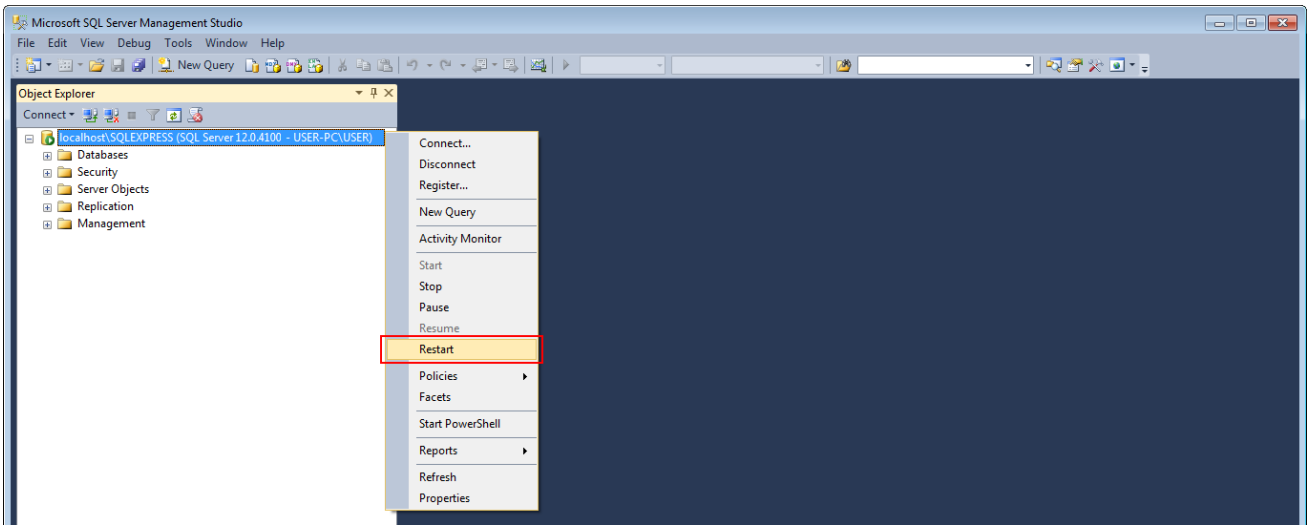


Figure 22 – SQL Server Restart

10. Add Windows[19] or SQL Server[23] accounts 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 Windows NT Authorization [42] 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**.

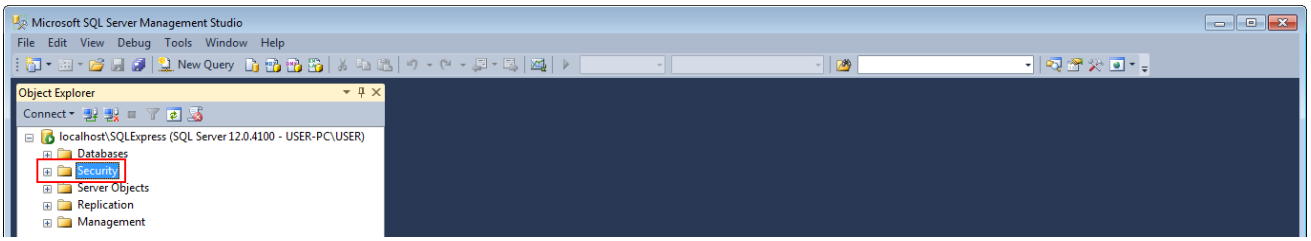


Figure 23 – Security Node

2. Right-click **Logins** and click **New Login**.

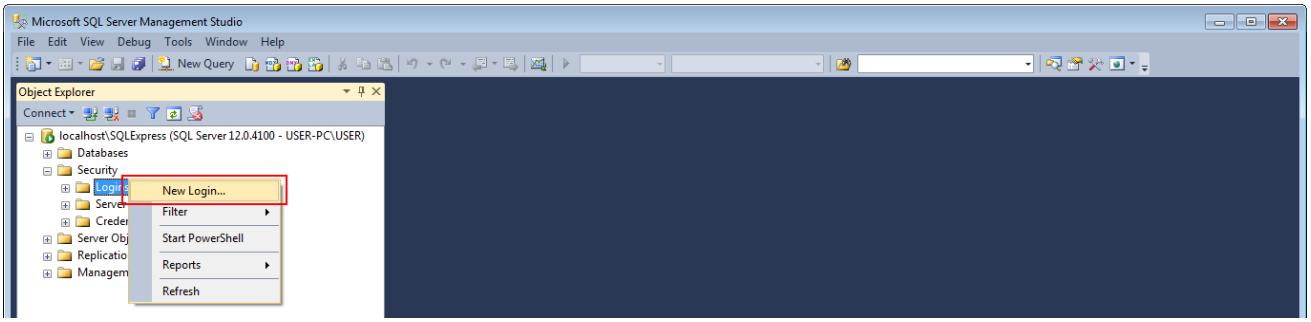


Figure 24 – New Login Creation

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

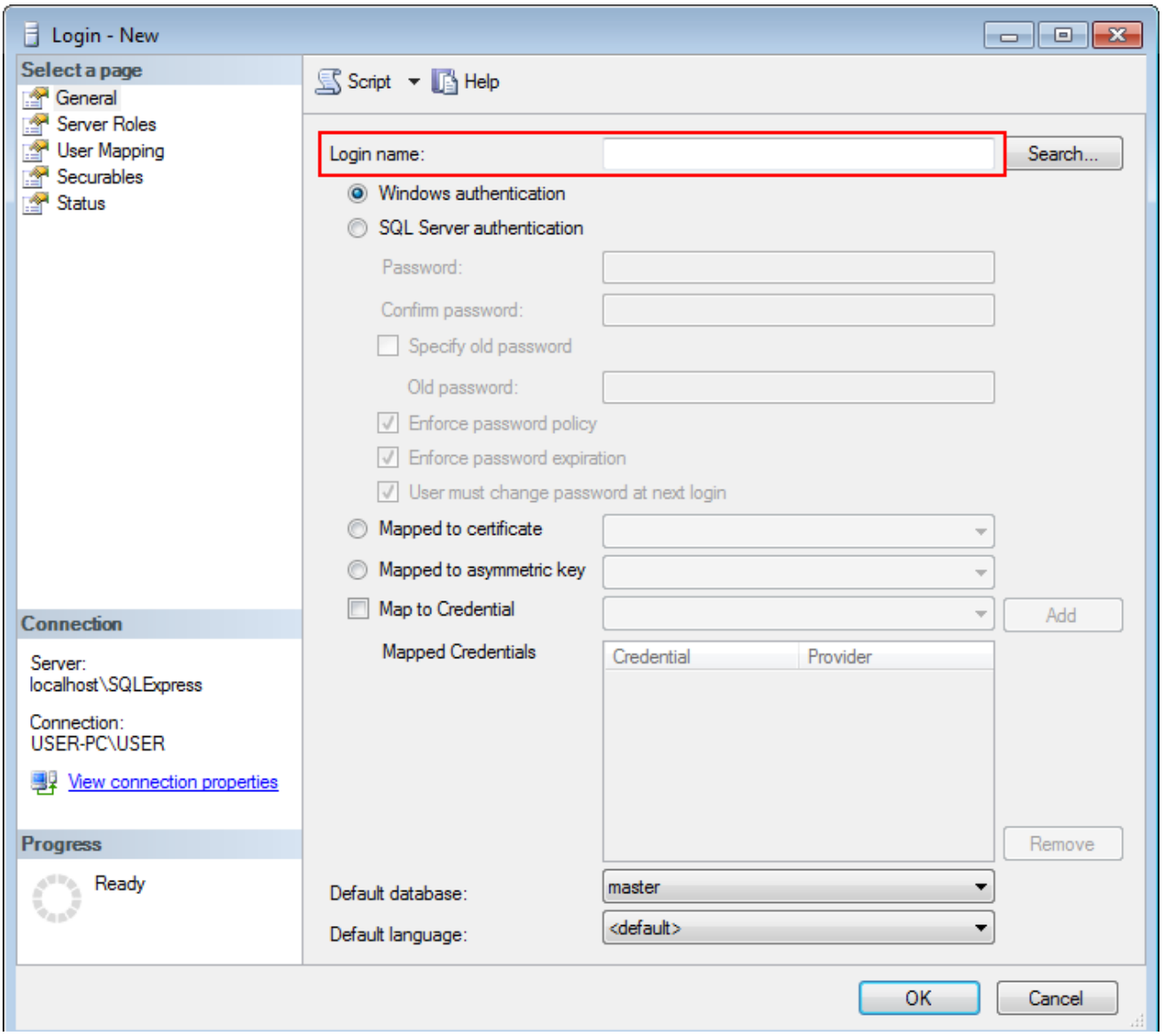


Figure 25 – Entering Login Name

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**.

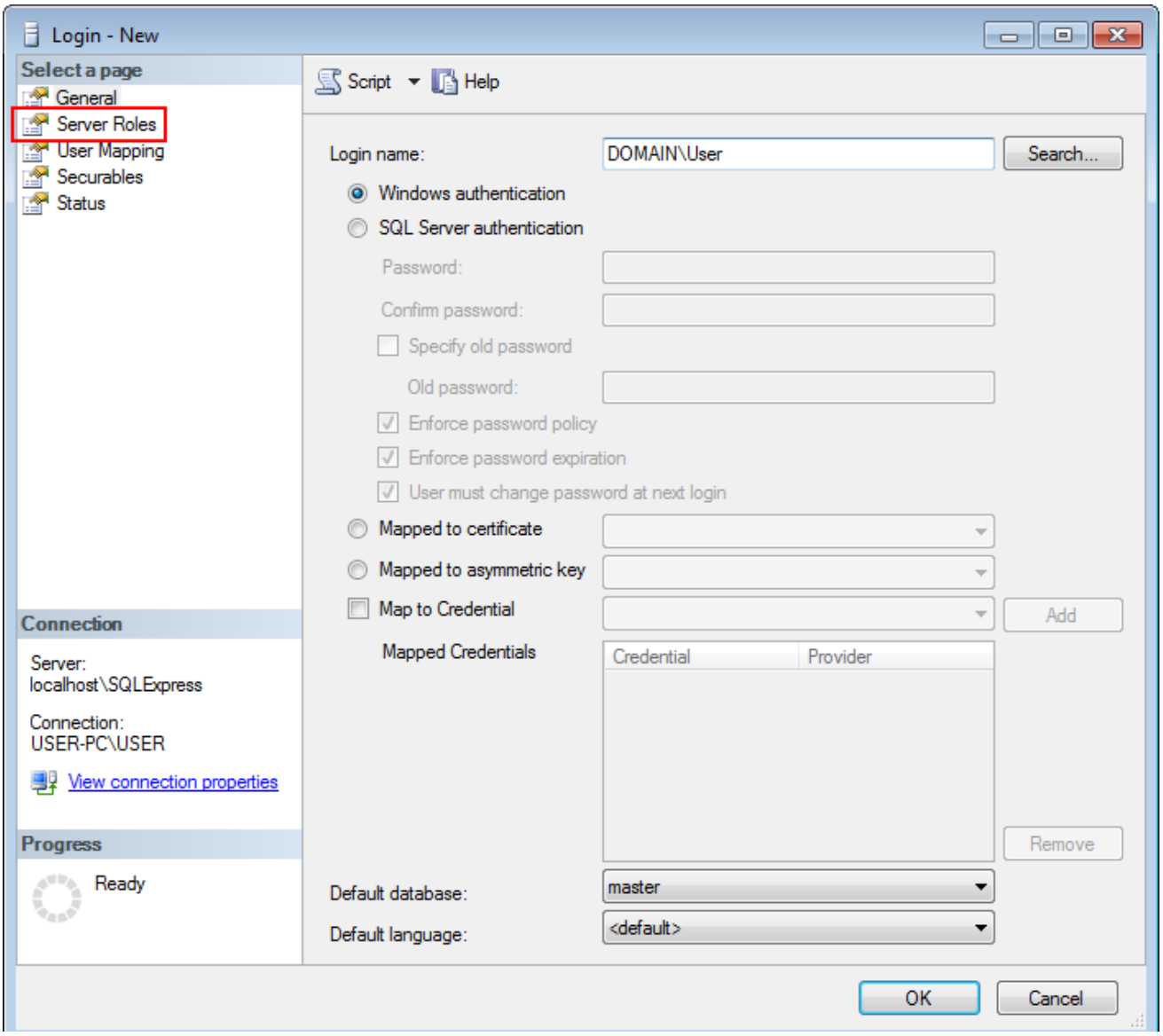


Figure 26 – Selecting Server Roles

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

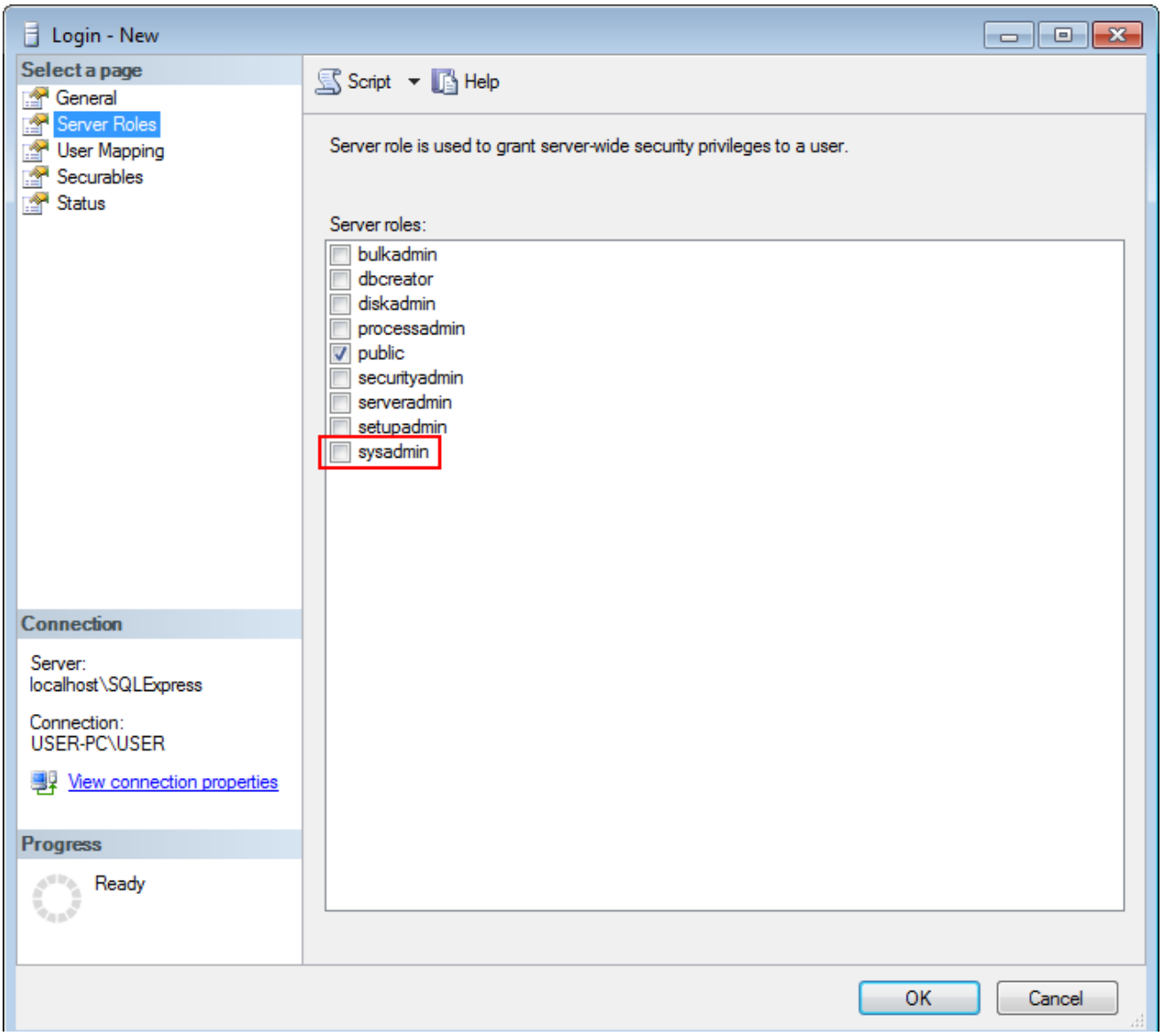


Figure 27 – Sysadmin Security Privelege

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 SQL Server authorization [42] mode, SQL account 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**.

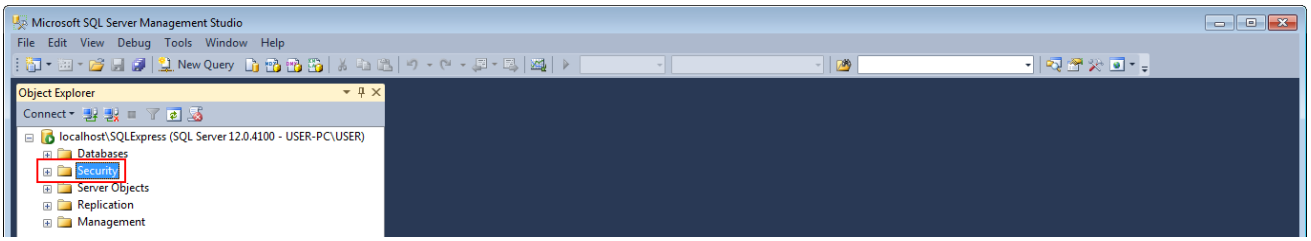


Figure 28 – Security Node

2. Right-click **Logins** and then click **New Login**.

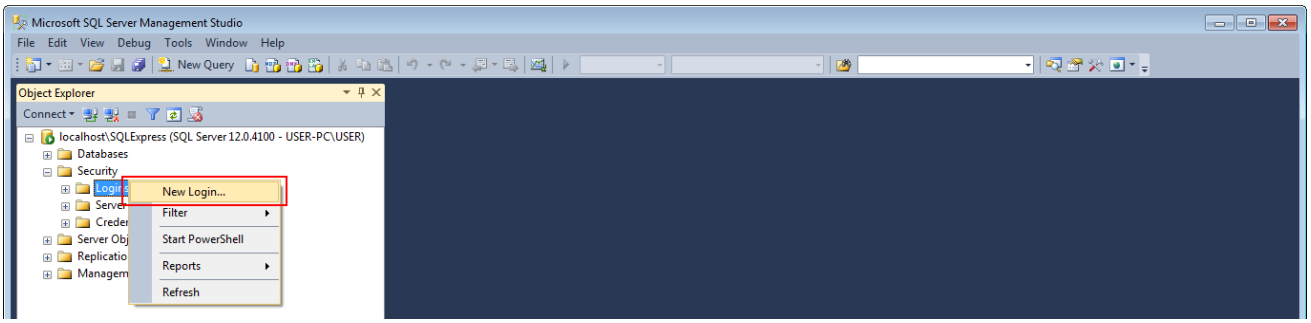


Figure 29 – New Login Creation

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

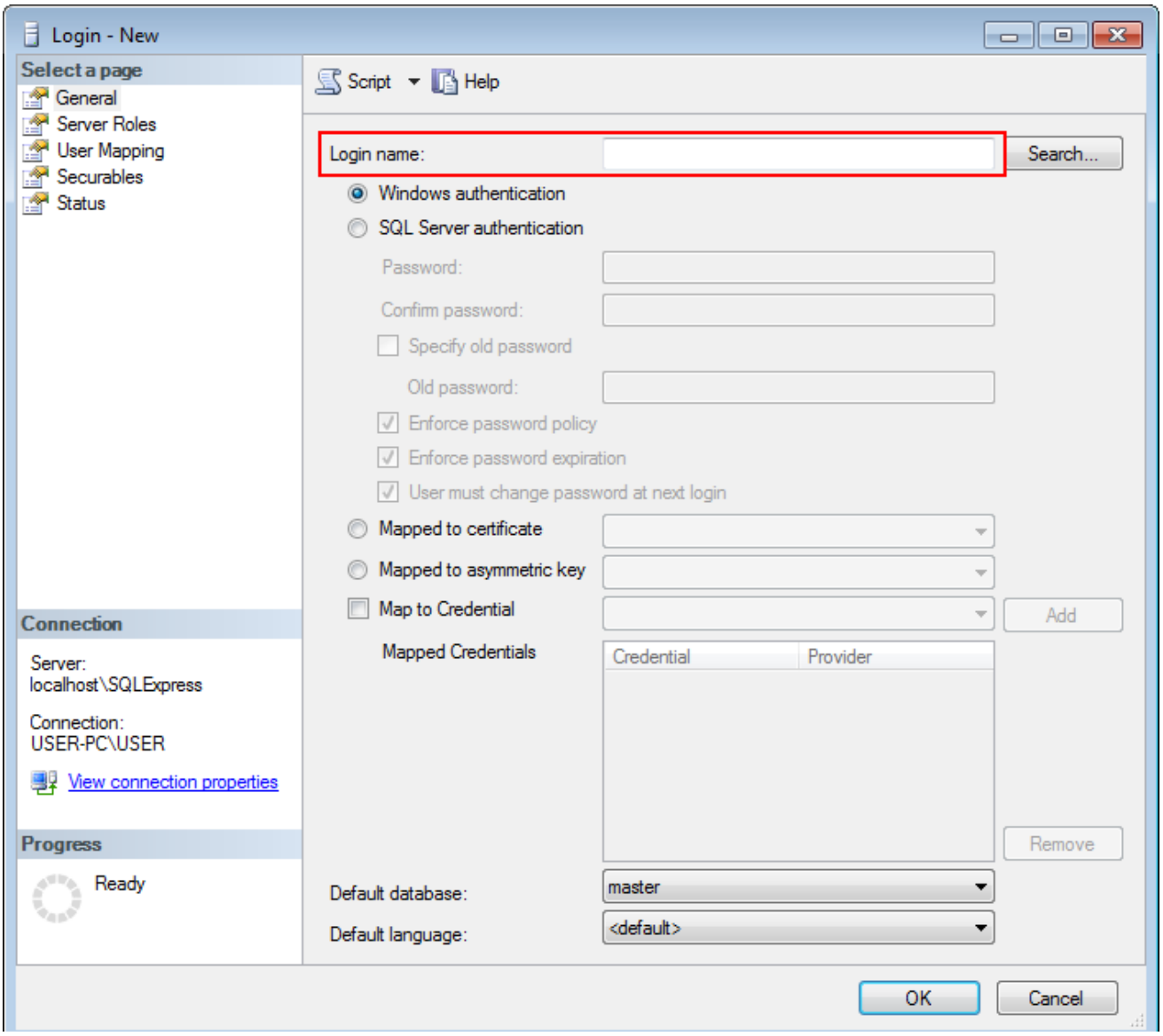


Figure 30 – Entering Login Name

4. Click **SQL server authentication**.

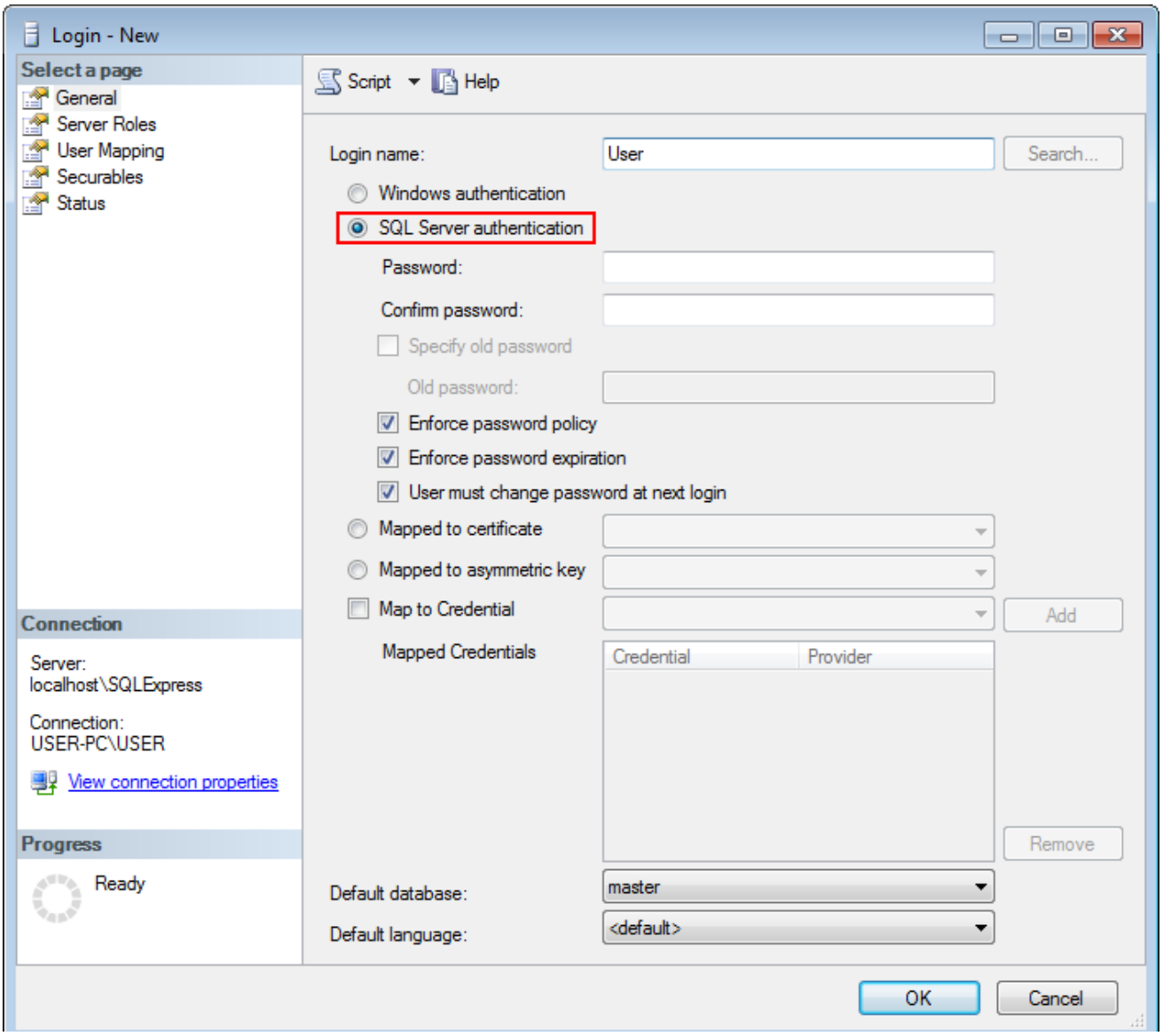


Figure 31 – SQL Server Authentication

5. Enter and confirm the password.

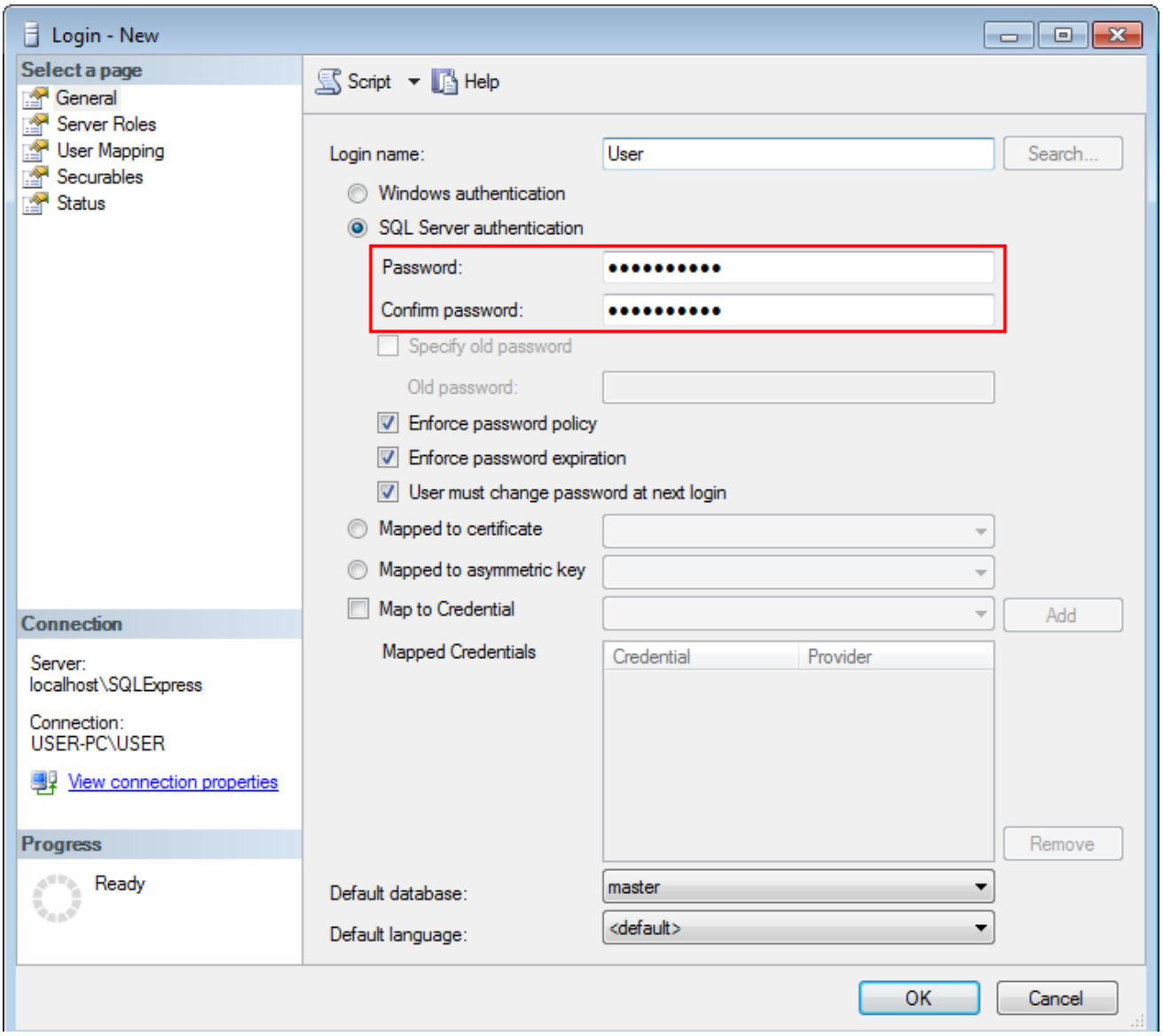


Figure 32 – Password Fields

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

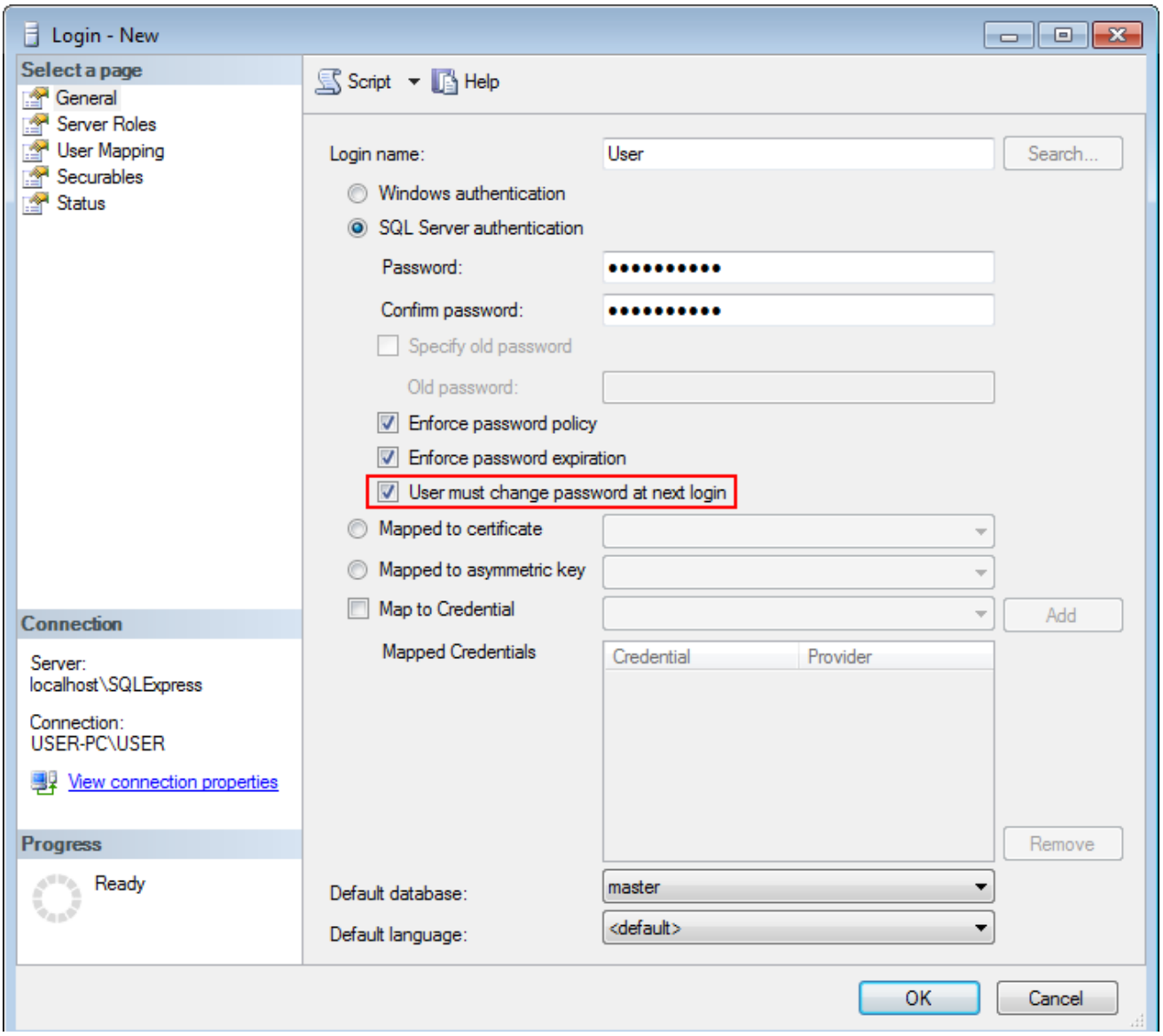


Figure 33 – Option for Password Keeping

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

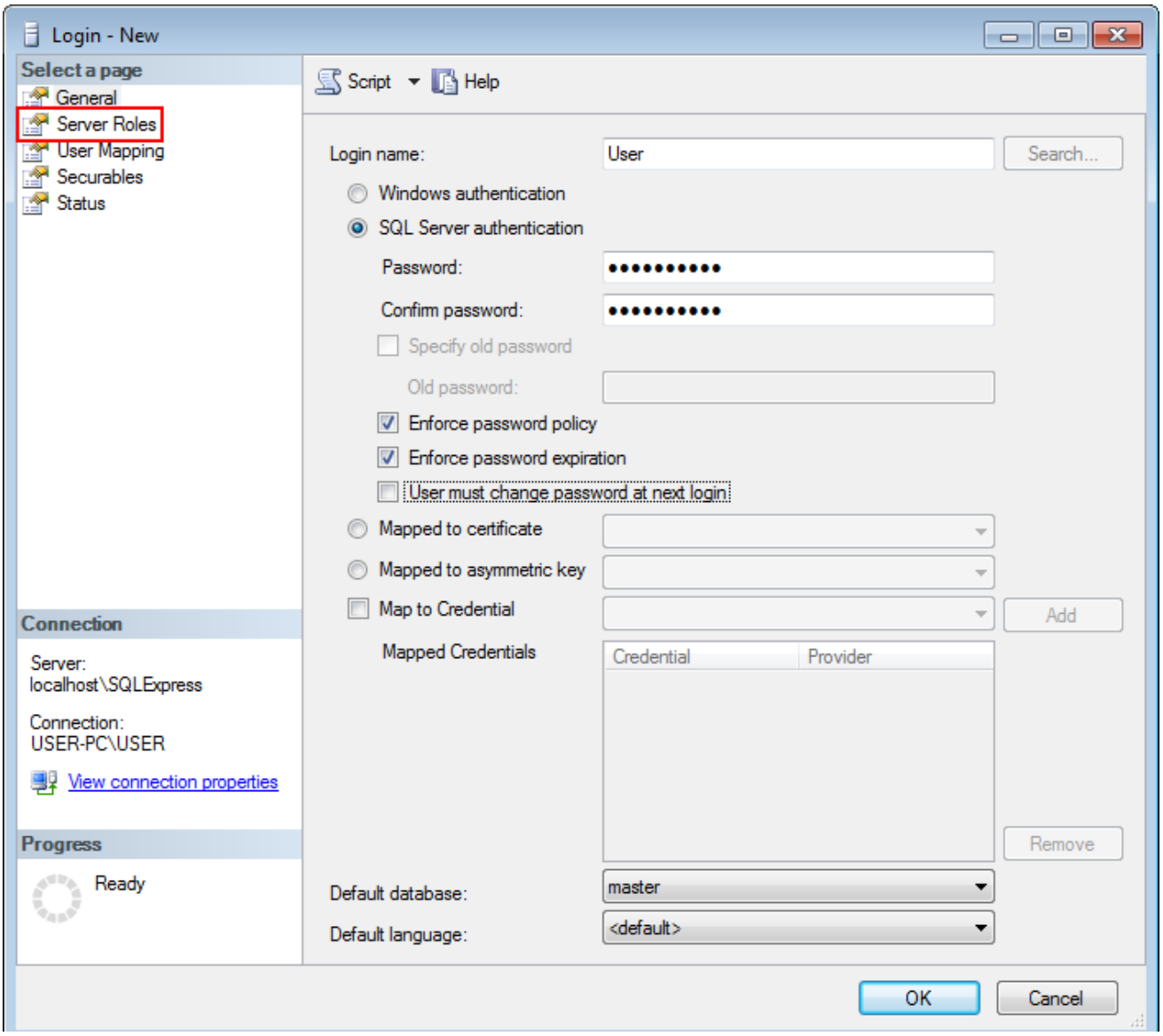


Figure 34 – Selecting Server Roles

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

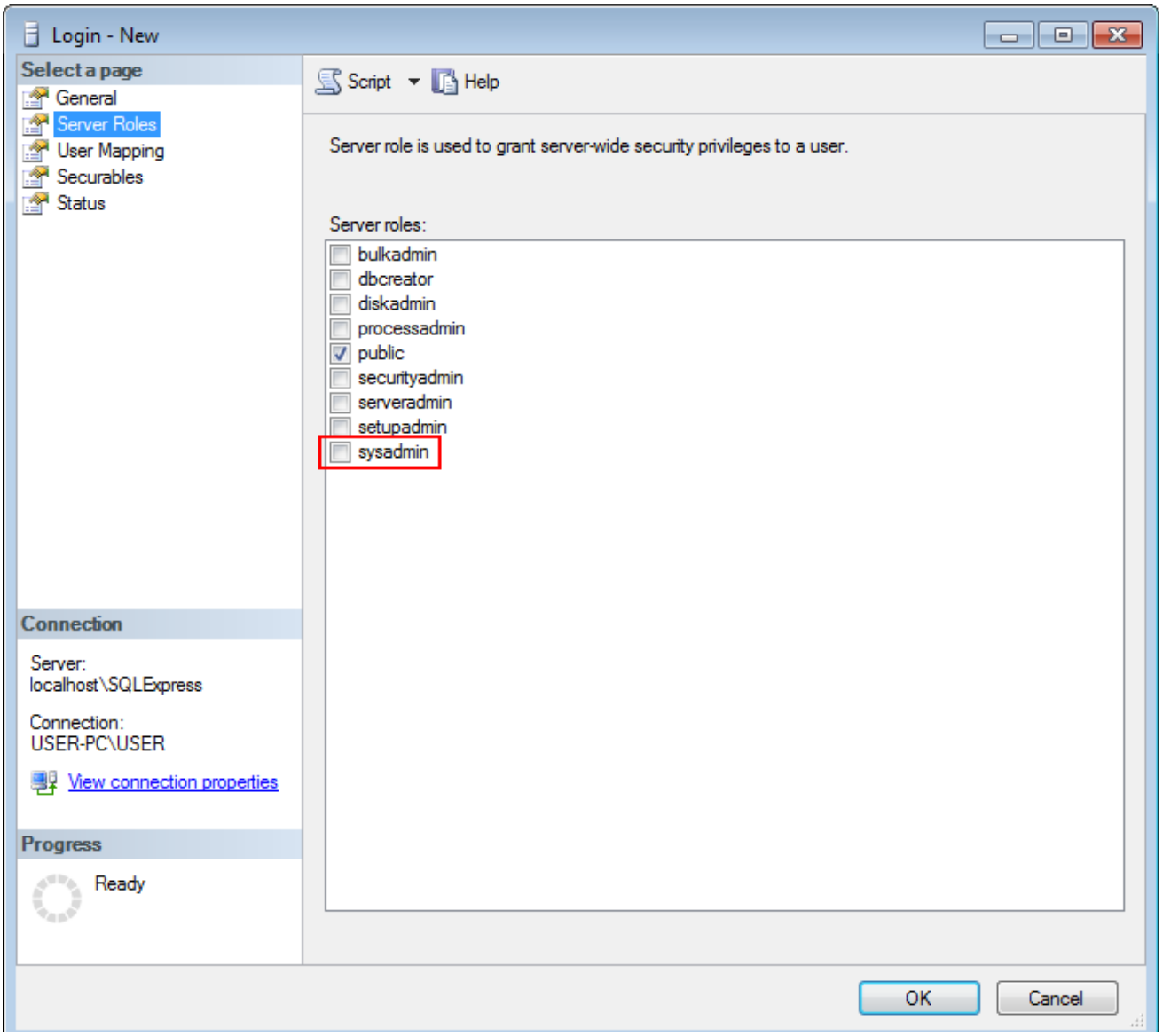


Figure 35 – Sysadmin Security Privelege

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**.

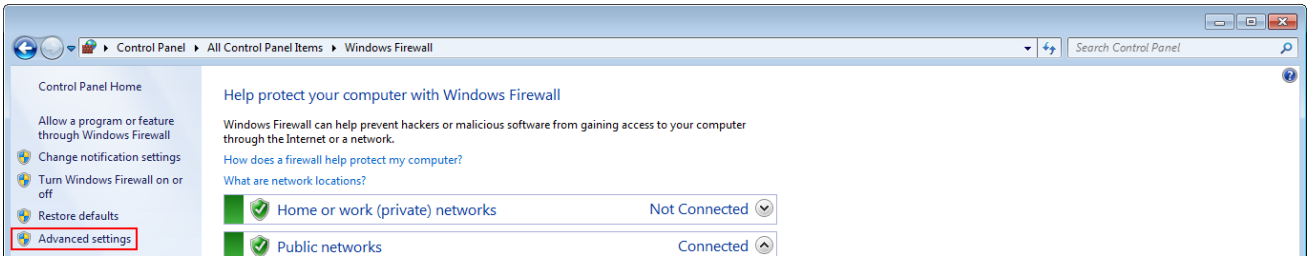


Figure 36 – Advanced Settings

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:

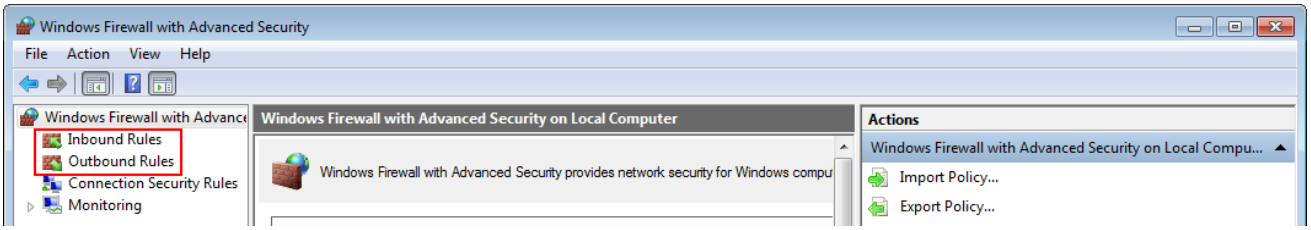


Figure 37 – Selecting Needed Group of Rules

- **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 and Outbound Rules. The following steps are presented for Inbound Rules.

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

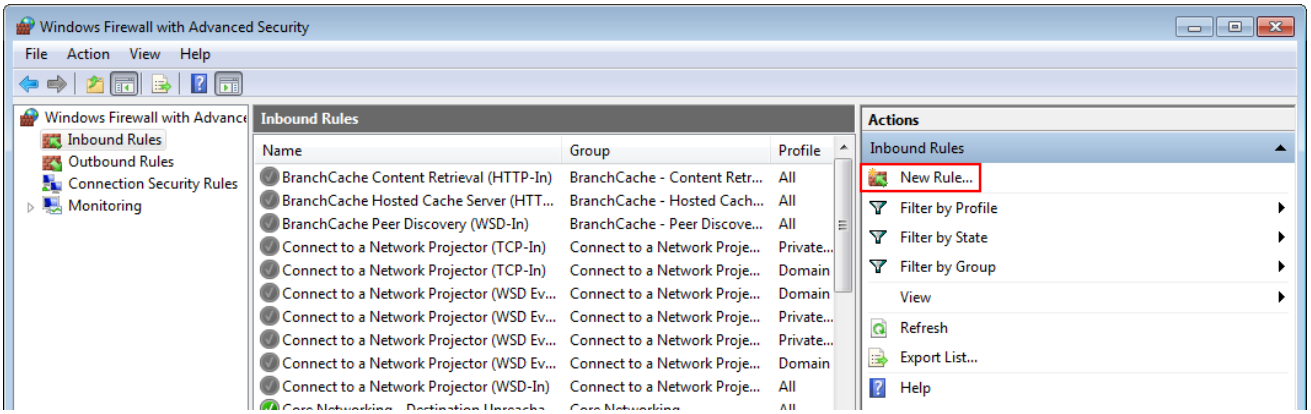


Figure 38 – Creating New Rule

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

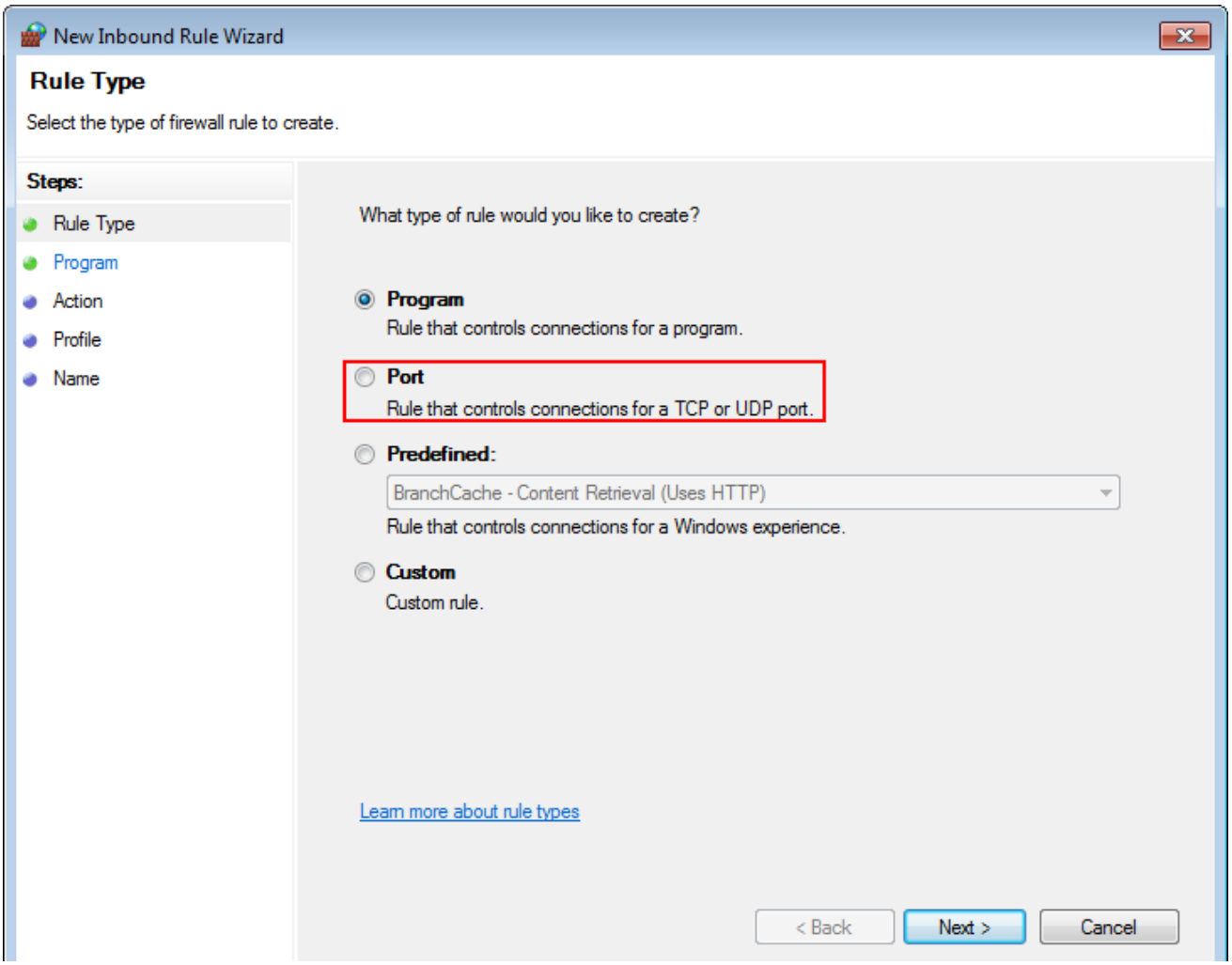


Figure 39 – Rule Type

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

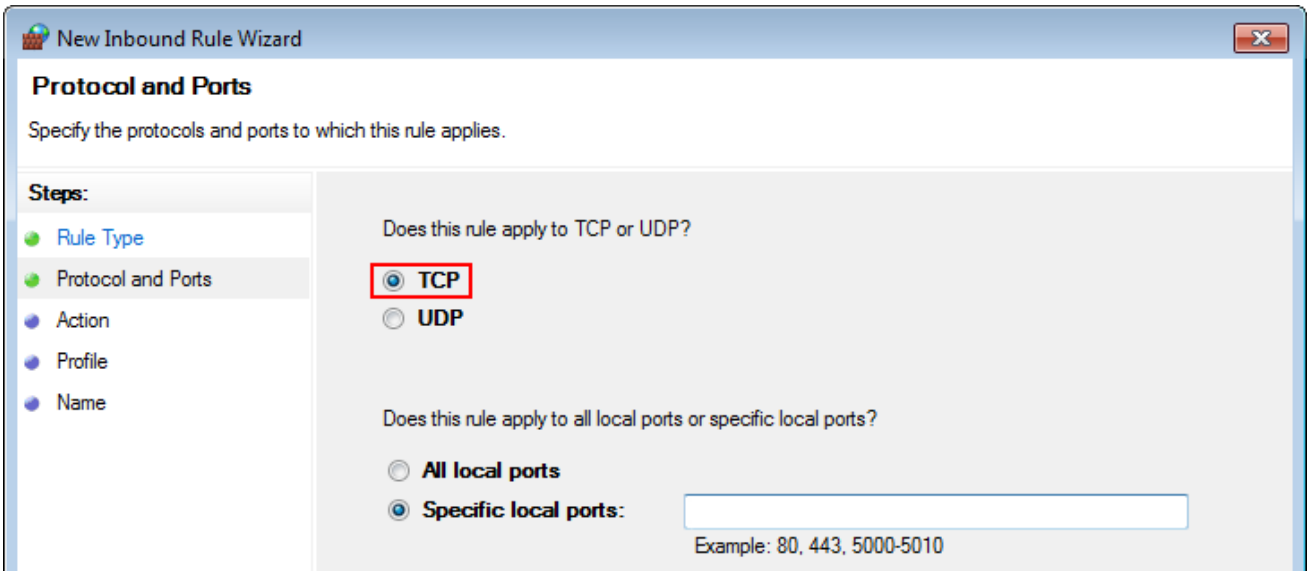


Figure 40 – Port Type

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

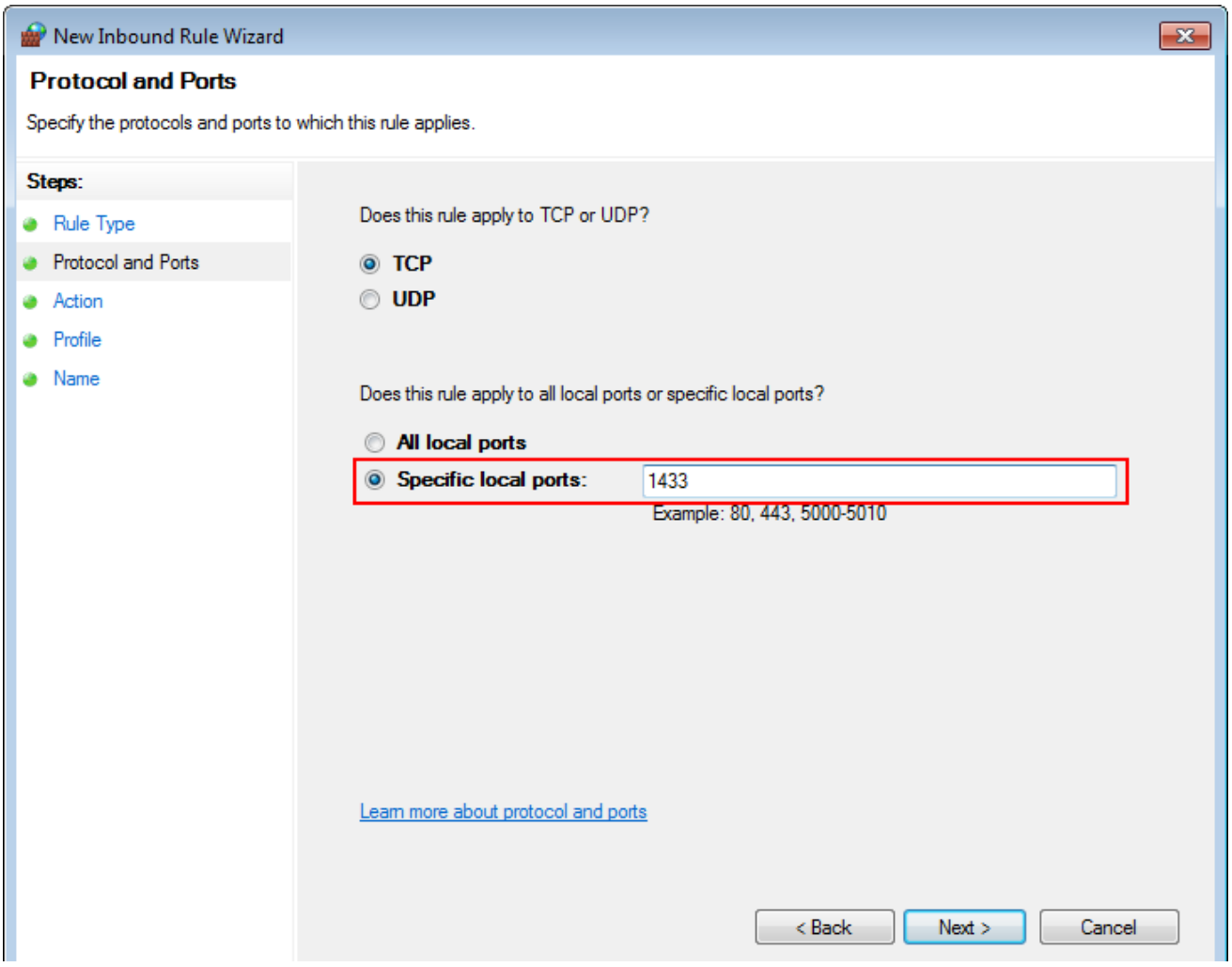


Figure 41 – Entering Port Number

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

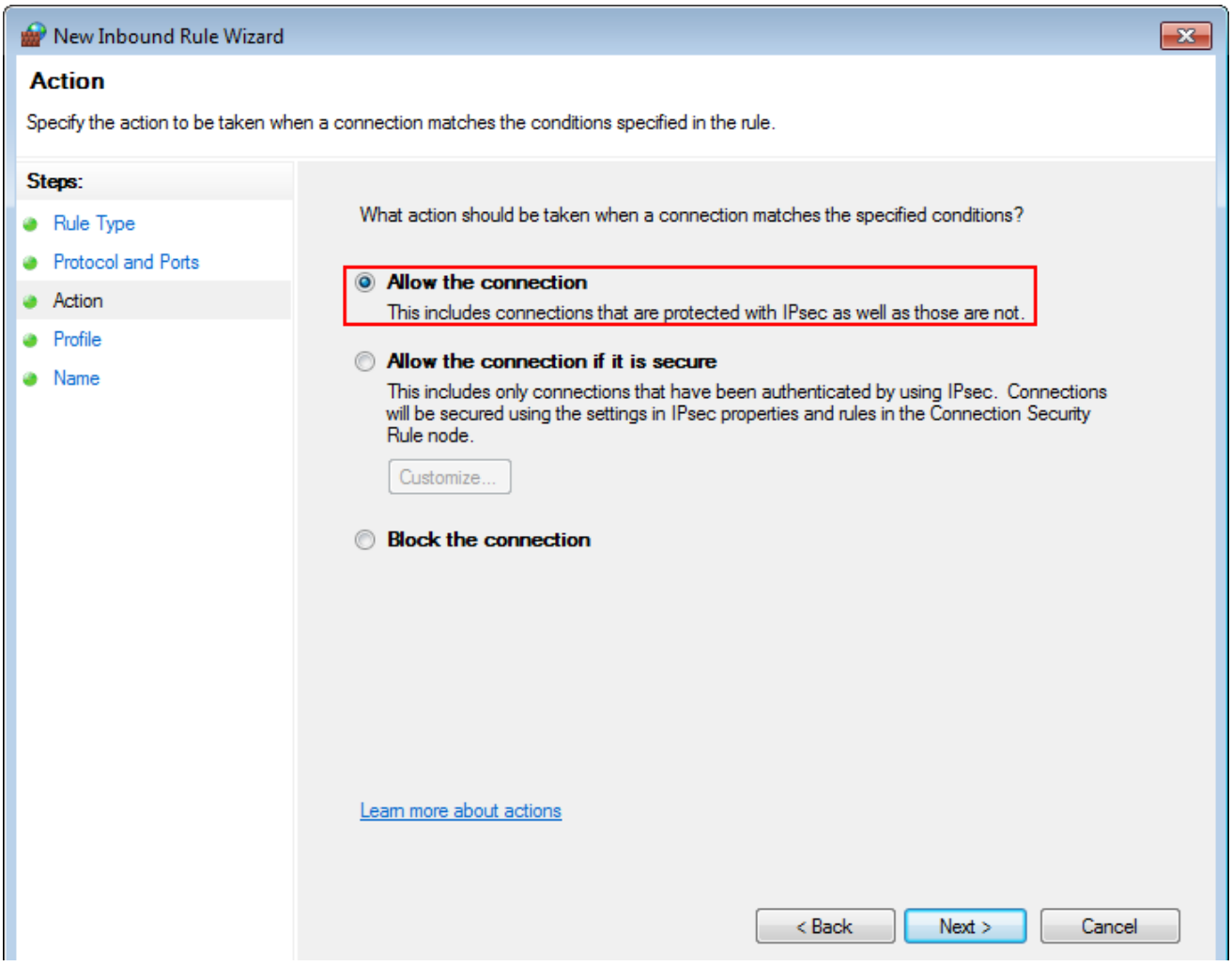


Figure 42 – Selecting Action

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

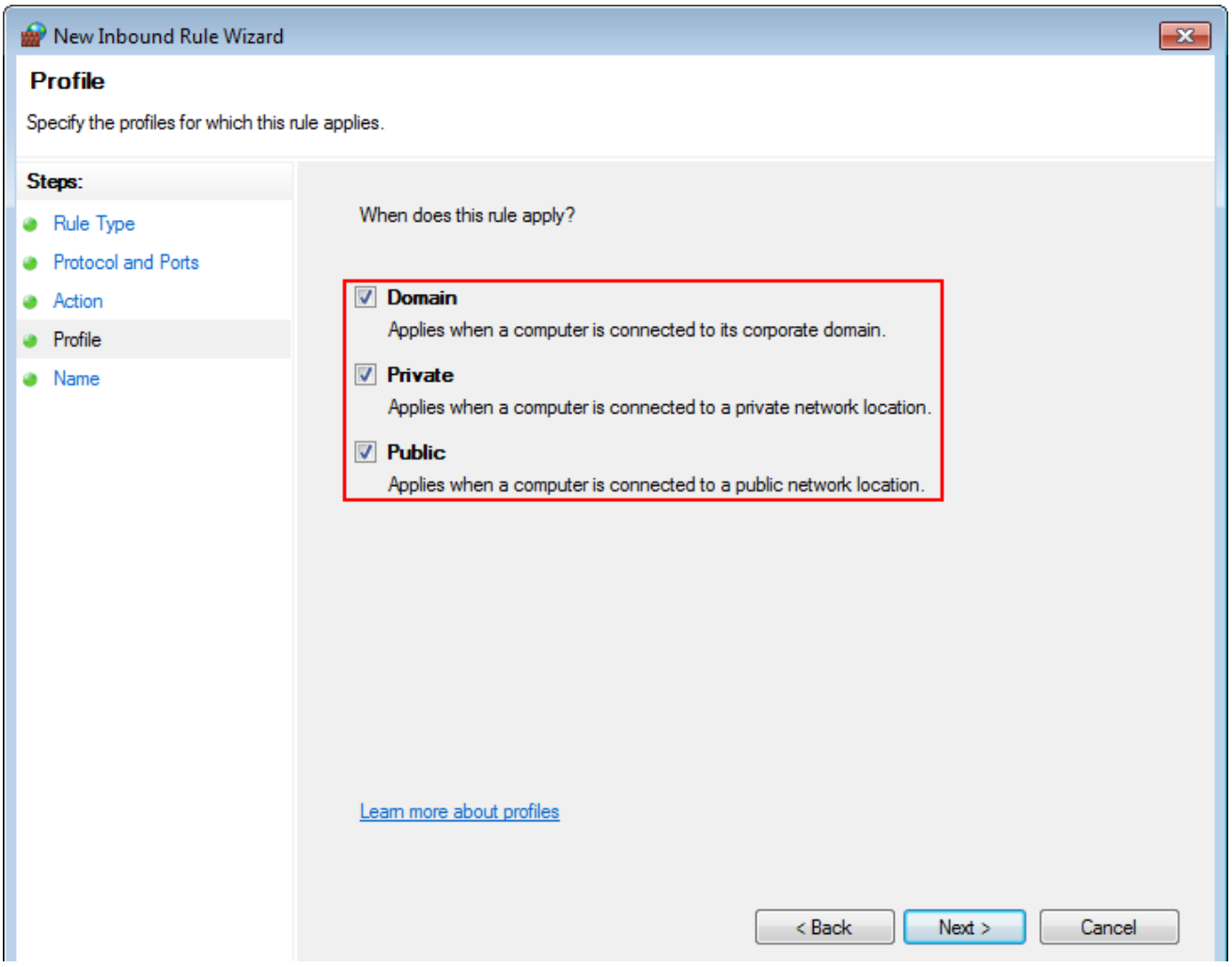


Figure 43 – Selecting Profile

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

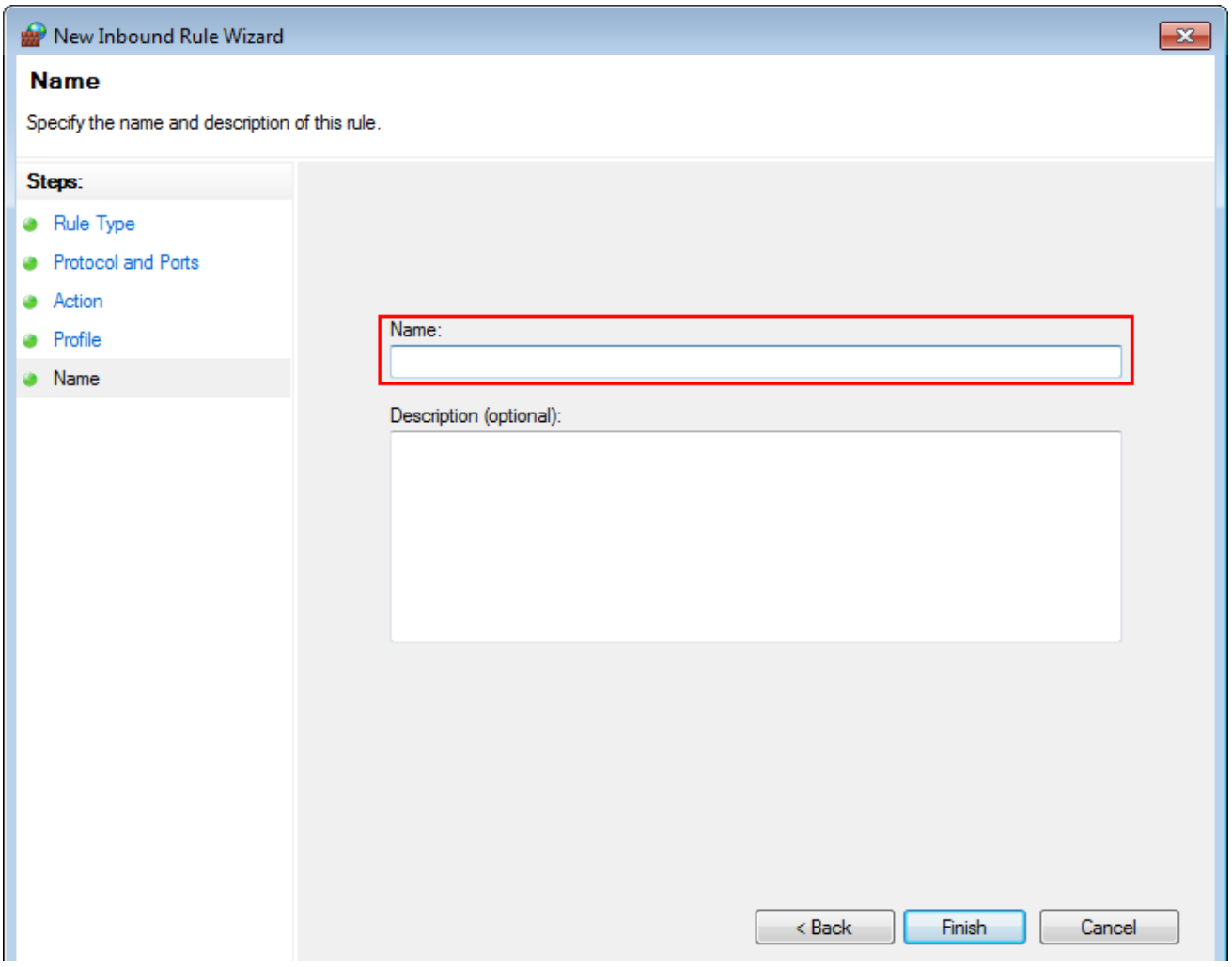


Figure 44 – Entering Name

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

Creation of firewall rules complete.

8 Remote Database Connection

8.1 Connecting to Remote Event Log Database

To connect to the remote Event Log database, perform the following actions:

1. In the left pane of the **Settings** tab, expand **Add-on Modules** node.
2. Click **Event Log**.

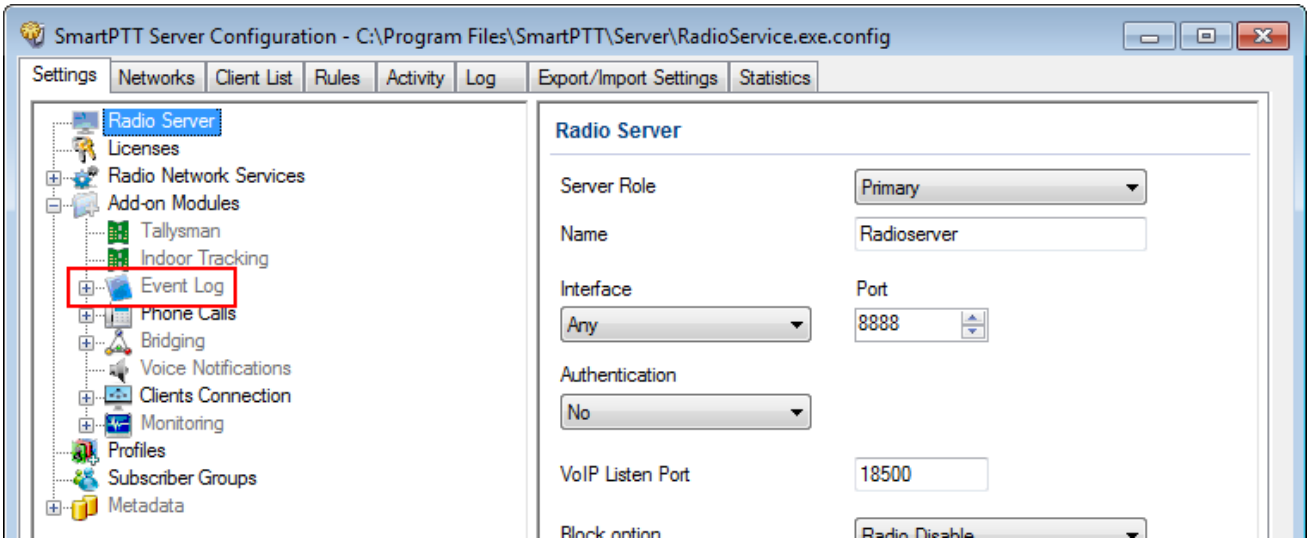


Figure 45 – Event Log Node

3. Make sure that the **Active** check box is selected in the **Event Log** pane.

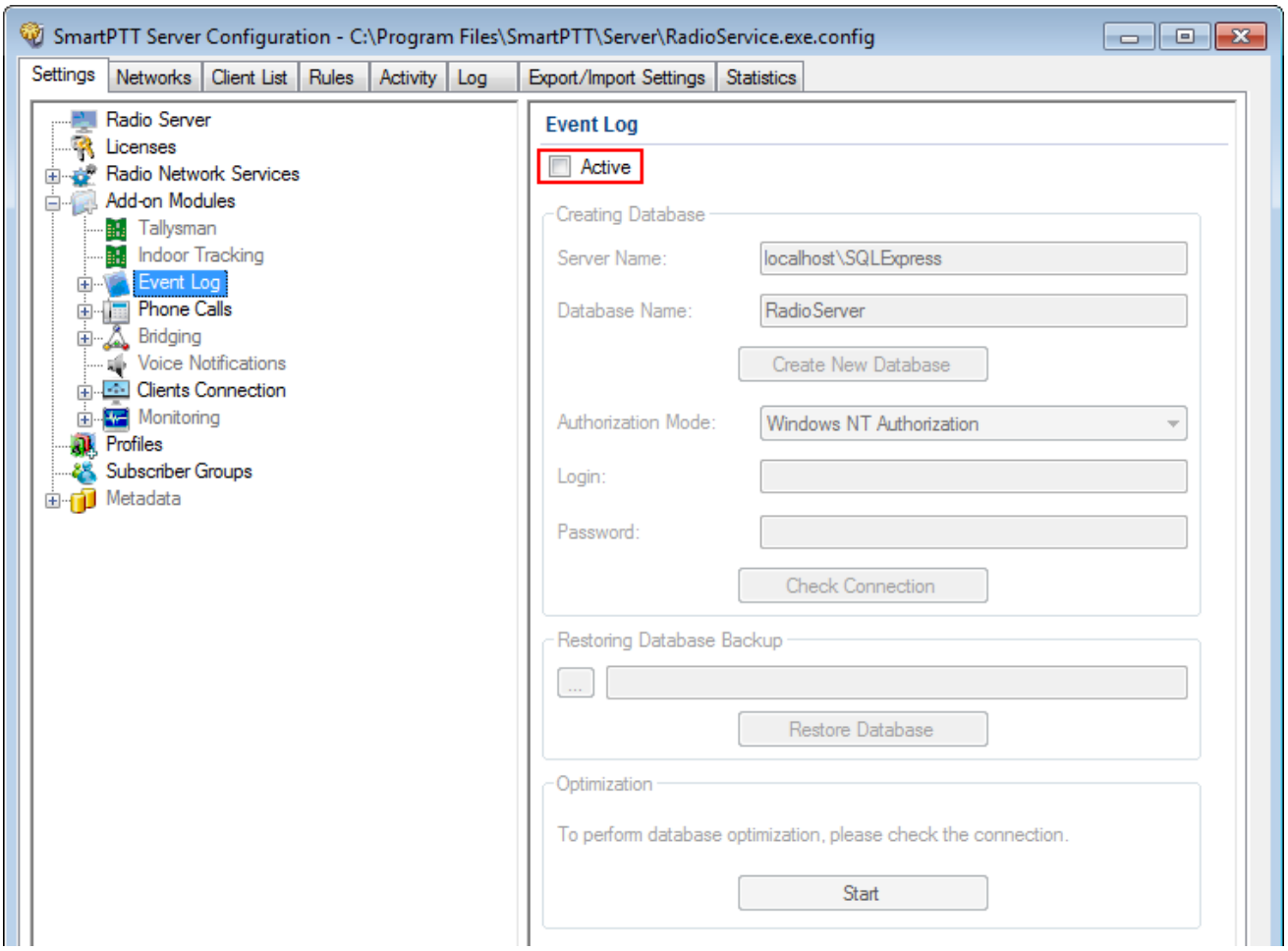


Figure 46 – Activation of Event Log

4. In the **Server name** field, enter the SQL Server name using the following format: <**IP address of a remote computer>\<Name of a remote SQL server>**.

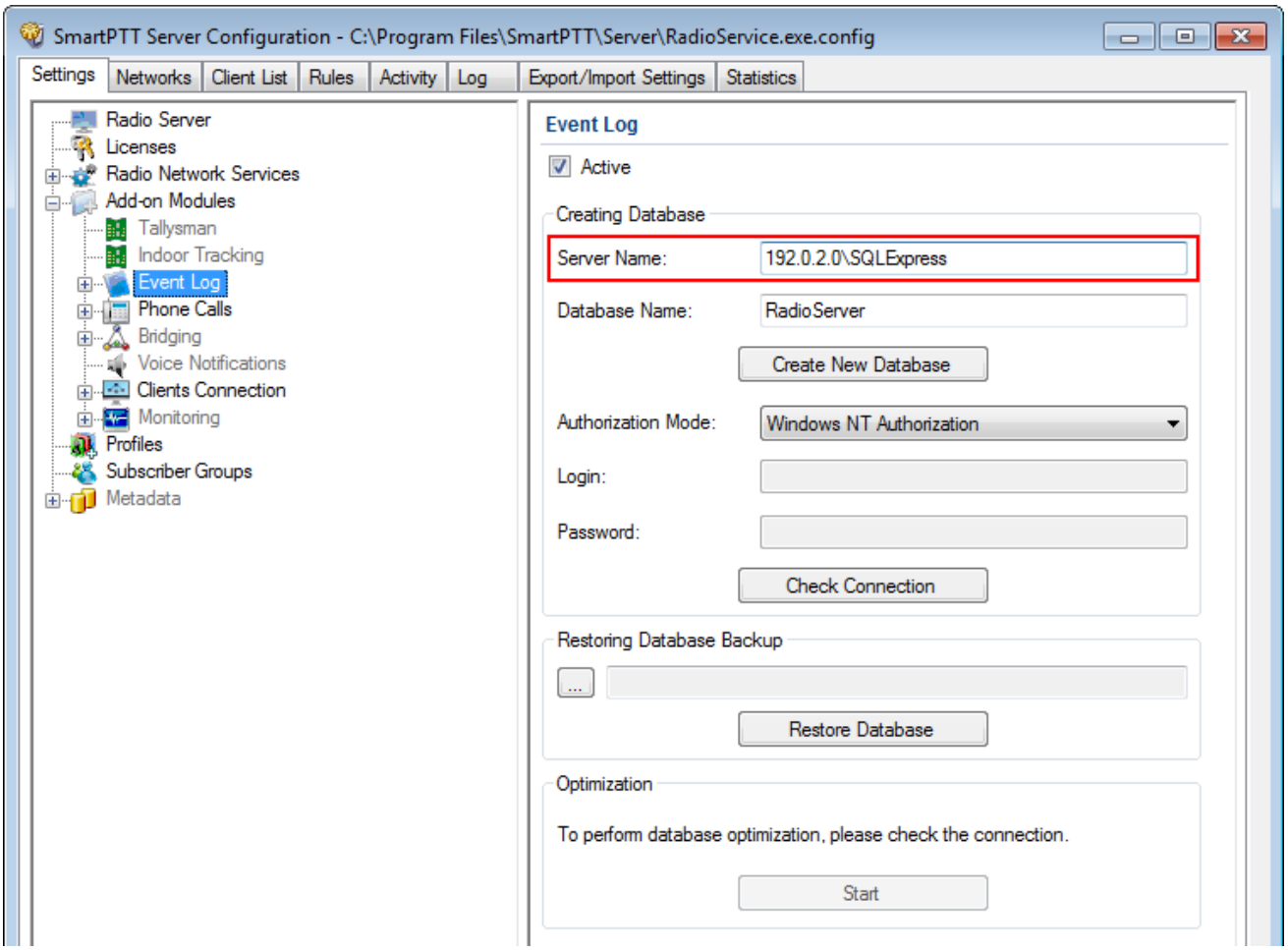


Figure 47 – Remote Database Server Name

5. In the **Database Name** field, enter the name of a remote Event Log database.

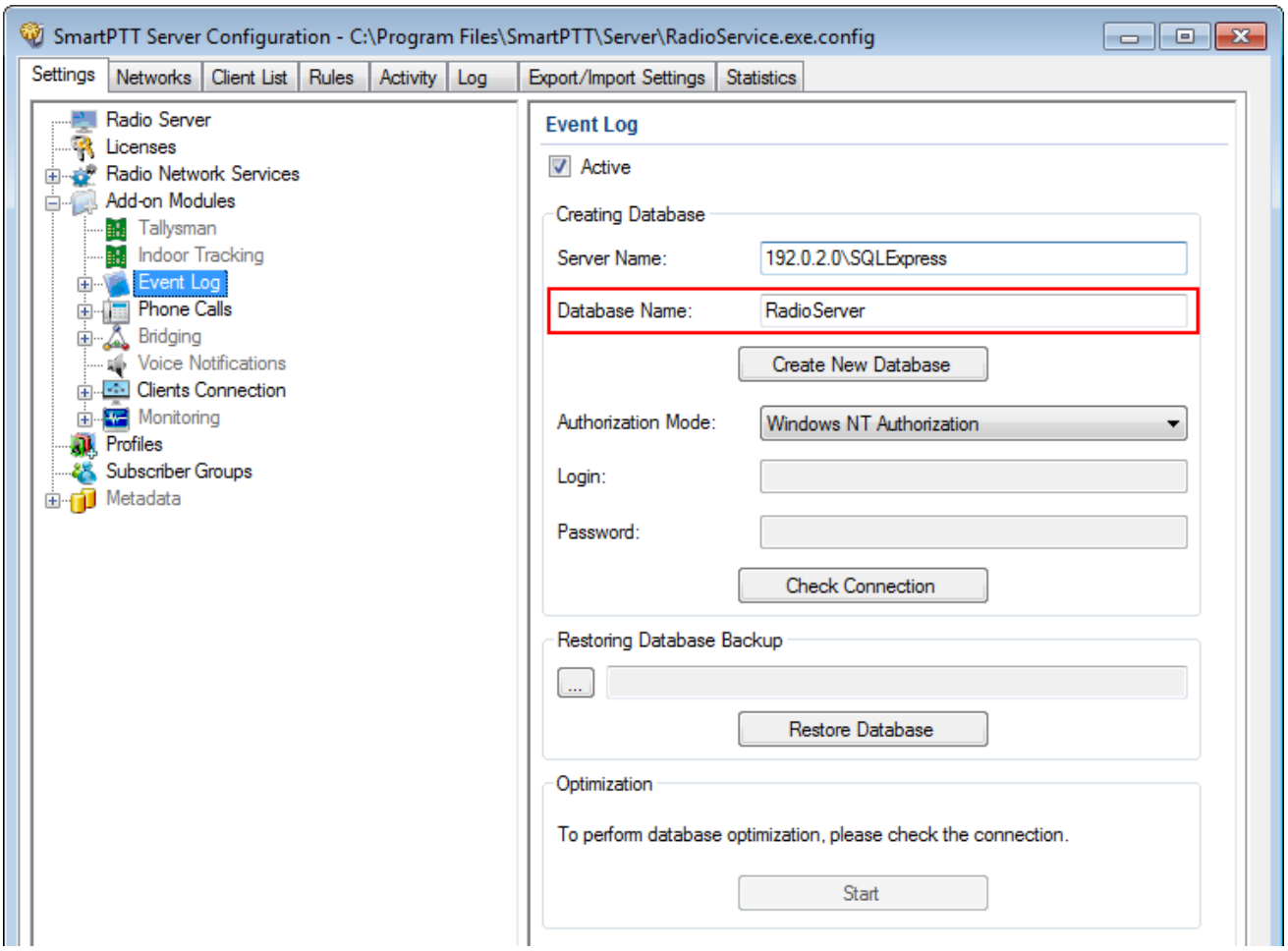


Figure 48 – Remote Database Name

6. In the **Authorization Mode** list, click the needed authorization type:

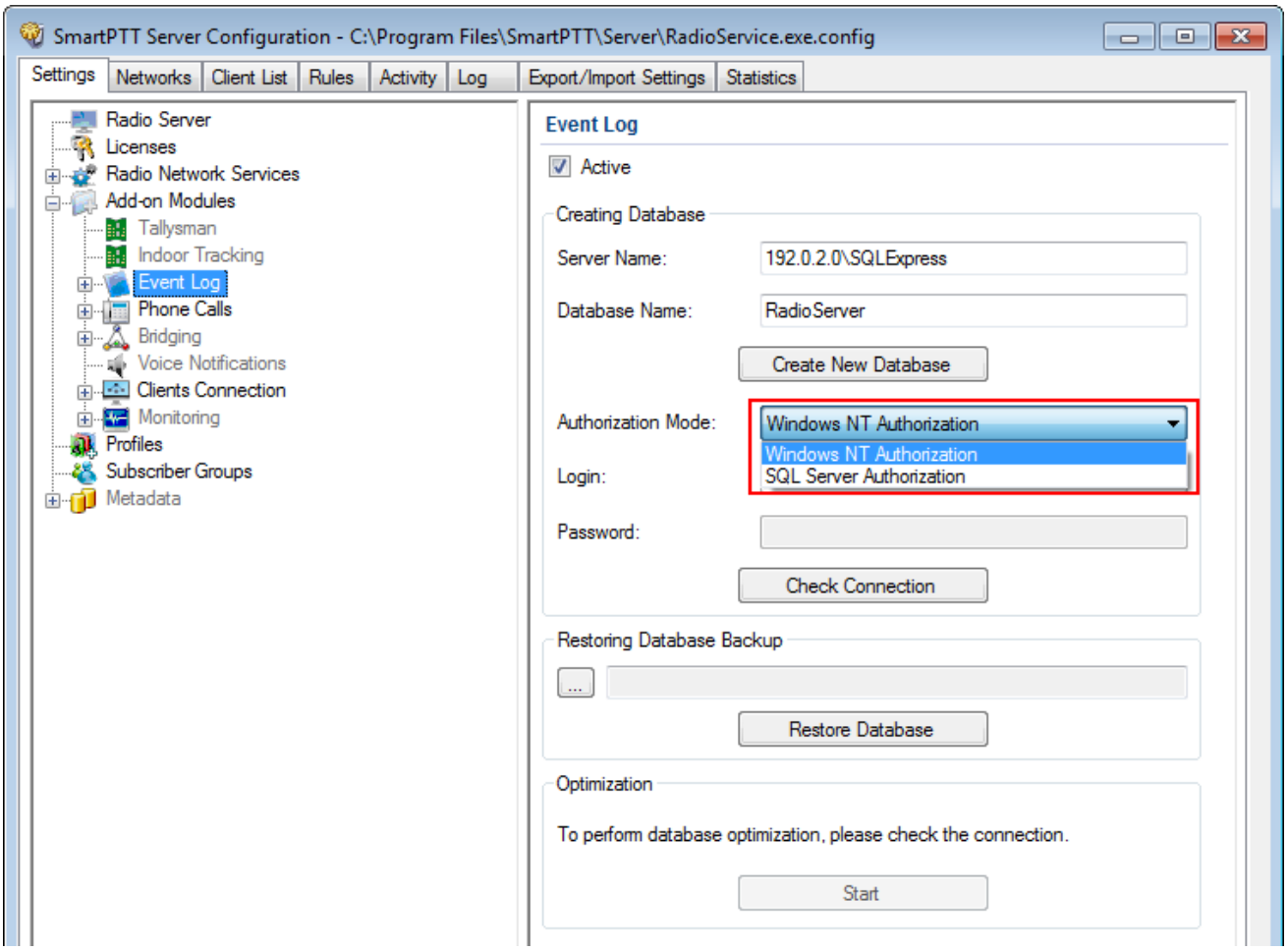


Figure 49 – Authorization Mode Selection

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

7. If **SQL Server Authorization** is selected, enter login and password.

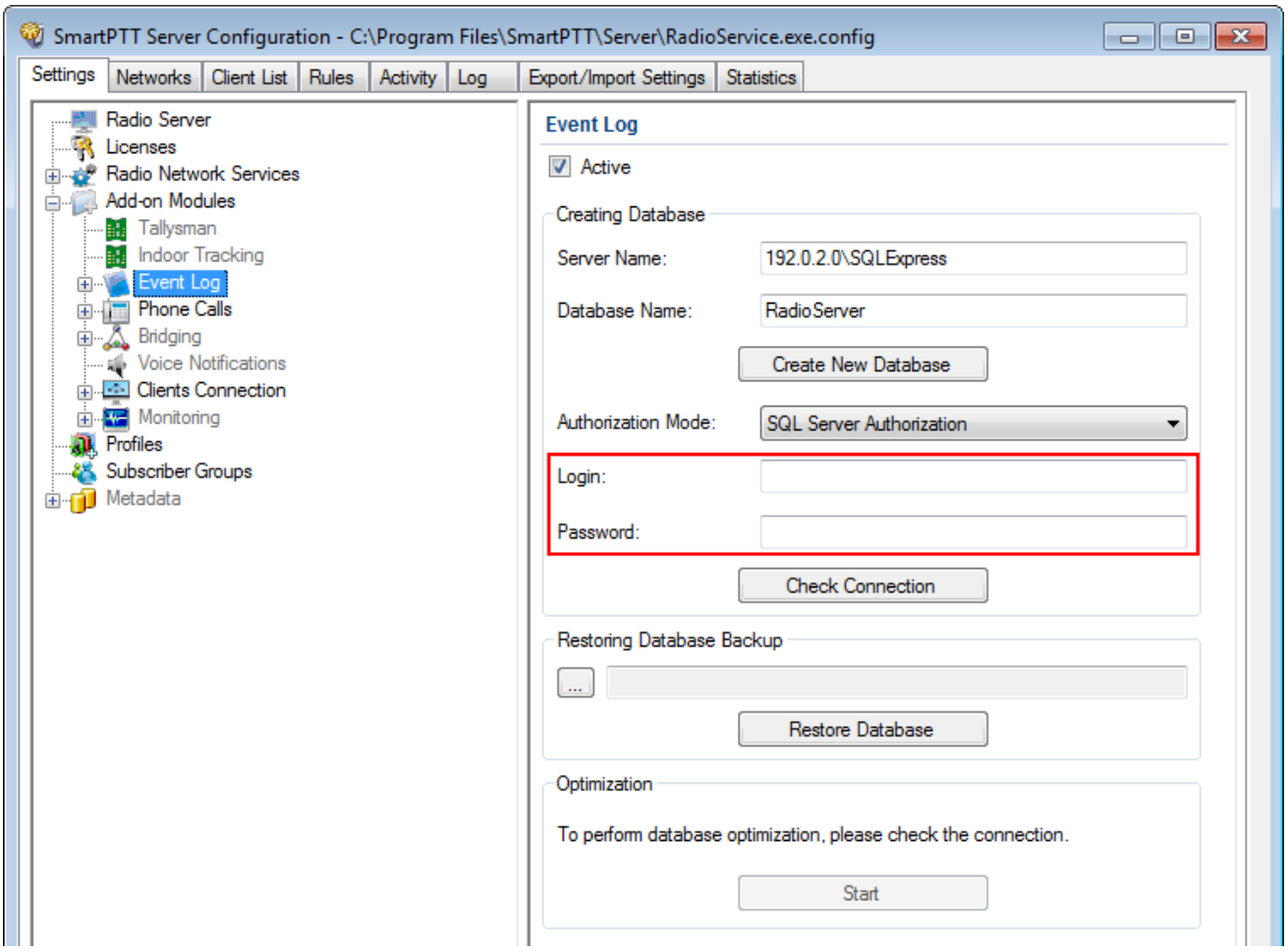


Figure 50 – Entering Login and Password

8. Click **Check Connection**.

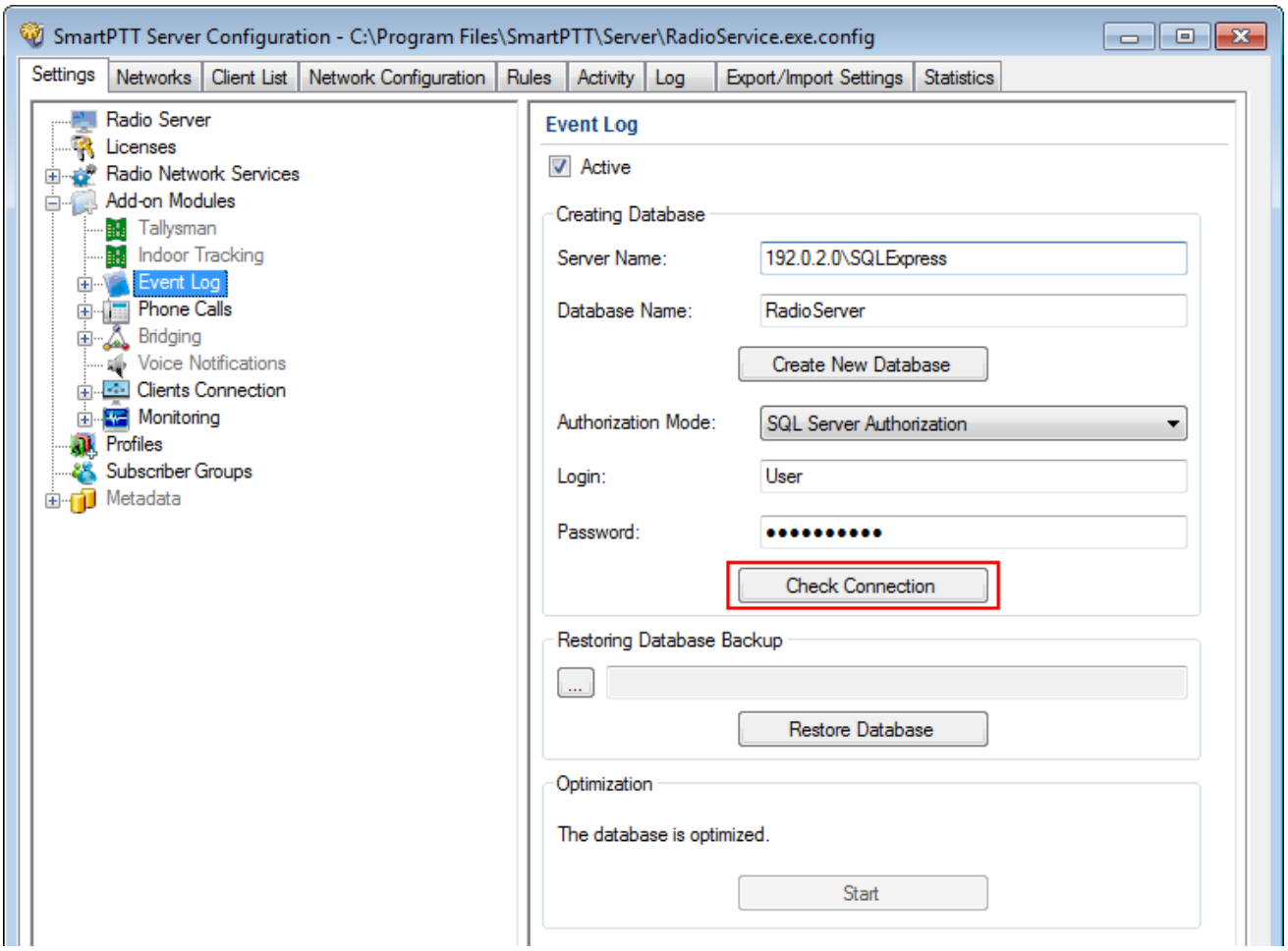


Figure 51 – Checking Remote Database Connection

If the connection is successful, the following message appears.

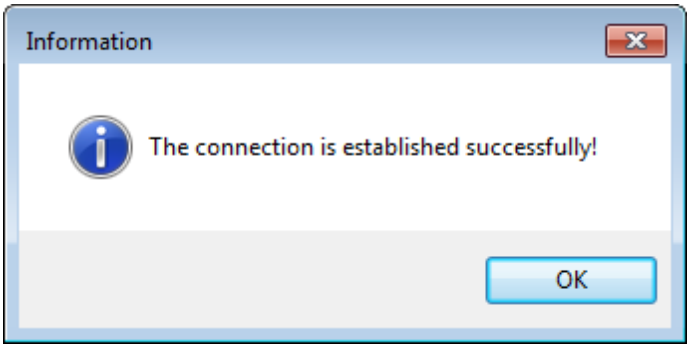


Figure 52 – Confirmation of Successful Remote Database Connection

9. Click **Save** to save changes and then click **Restart** to restart SmartPTT Radioserver.

Connection to the remote Event Log database complete.

8.2 Connecting to Remote Monitoring Database

To connect to the remote Monitoring database, perform the following actions:

1. In the left pane of the **Settings** tab, expand **Add-on Modules** node.
2. Click **Monitoring**.

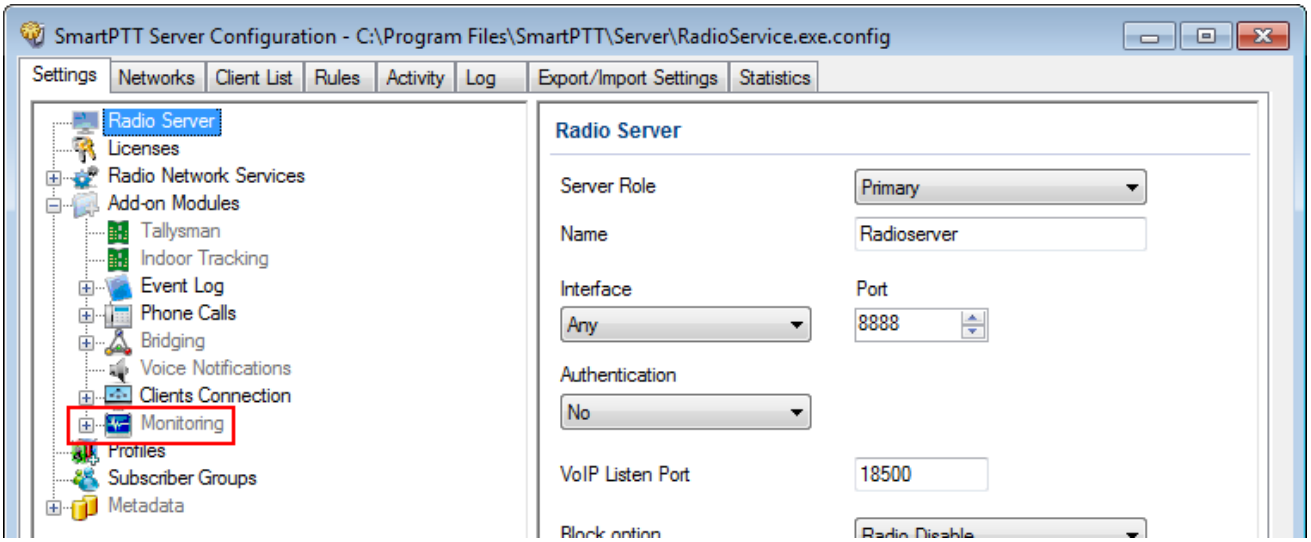


Figure 53 – Monitoring Node

3. Make sure that the **Active** check box is selected in the **Monitoring** pane.

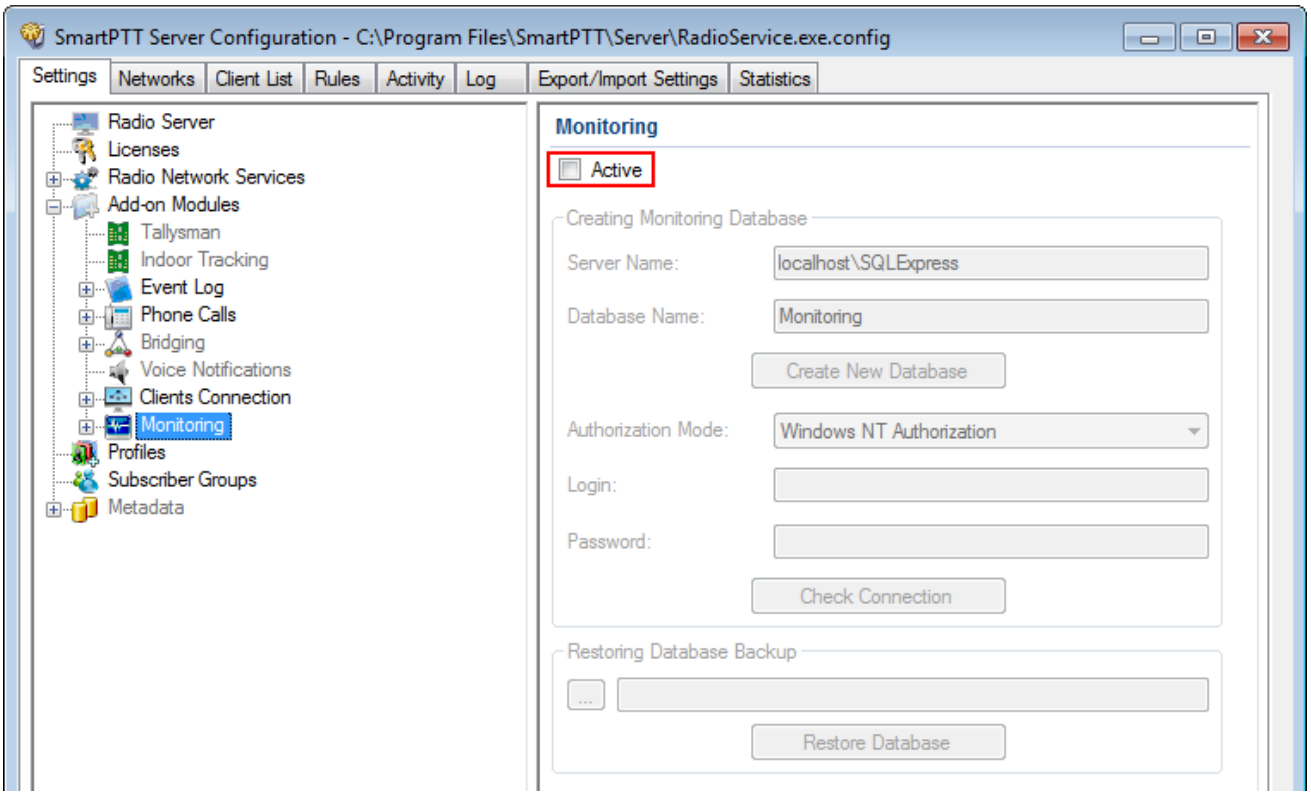


Figure 54 – Monitoring Activation

4. In the **Server name** field, enter the SQL server name using the following format: <**IP address of a remote computer>\<Name of a remote SQL server>**.

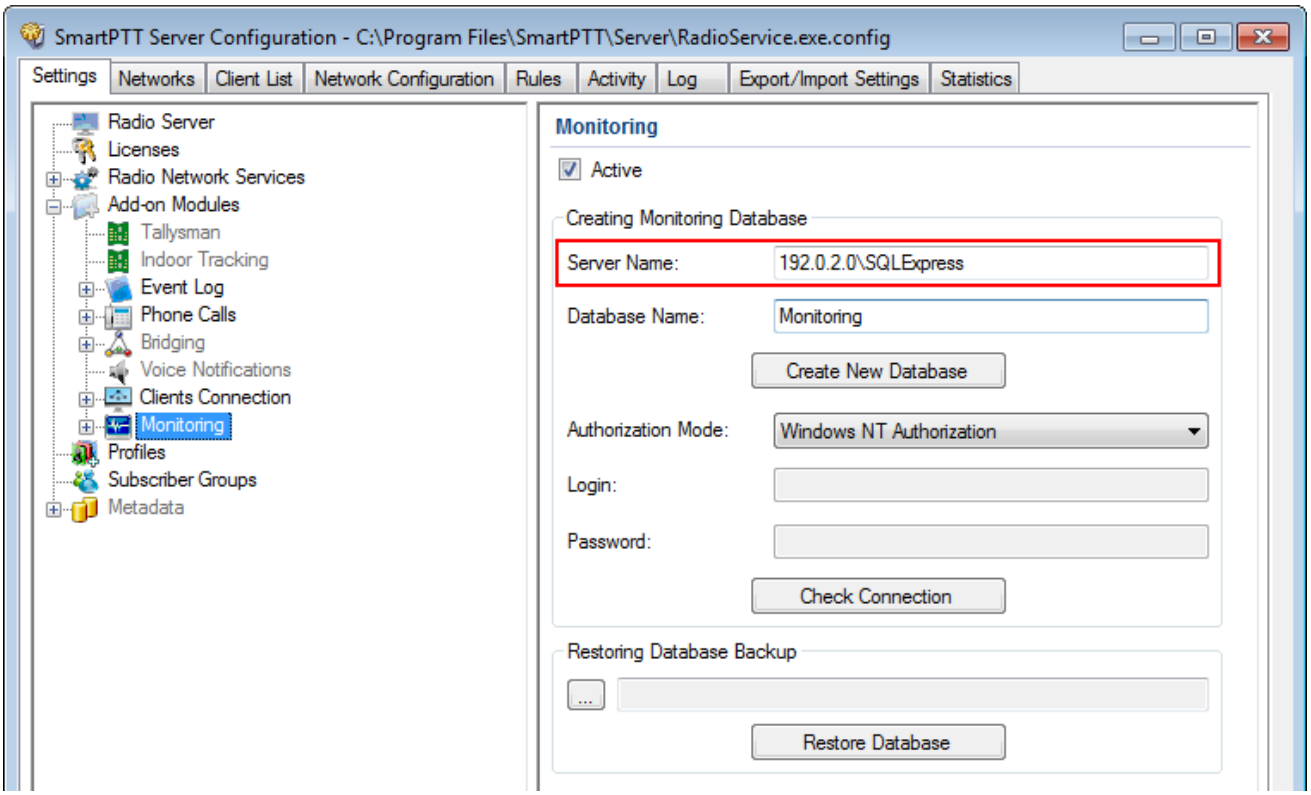


Figure 55 – Remote Database Server Name

5. In the **Database Name** field, enter the name of a remote Monitoring database.

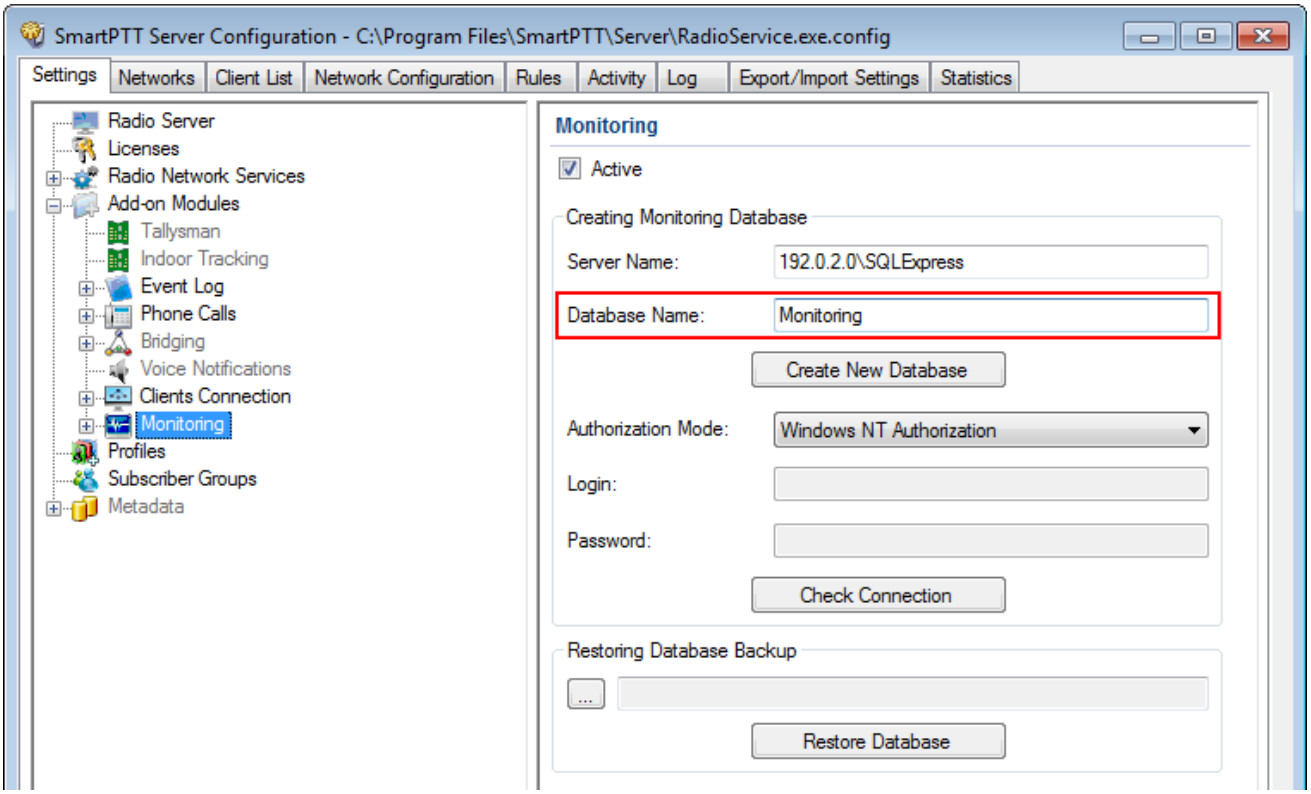


Figure 56 – Remote Database Name

6. In the **Authorization Mode** list, click the needed authorization type:

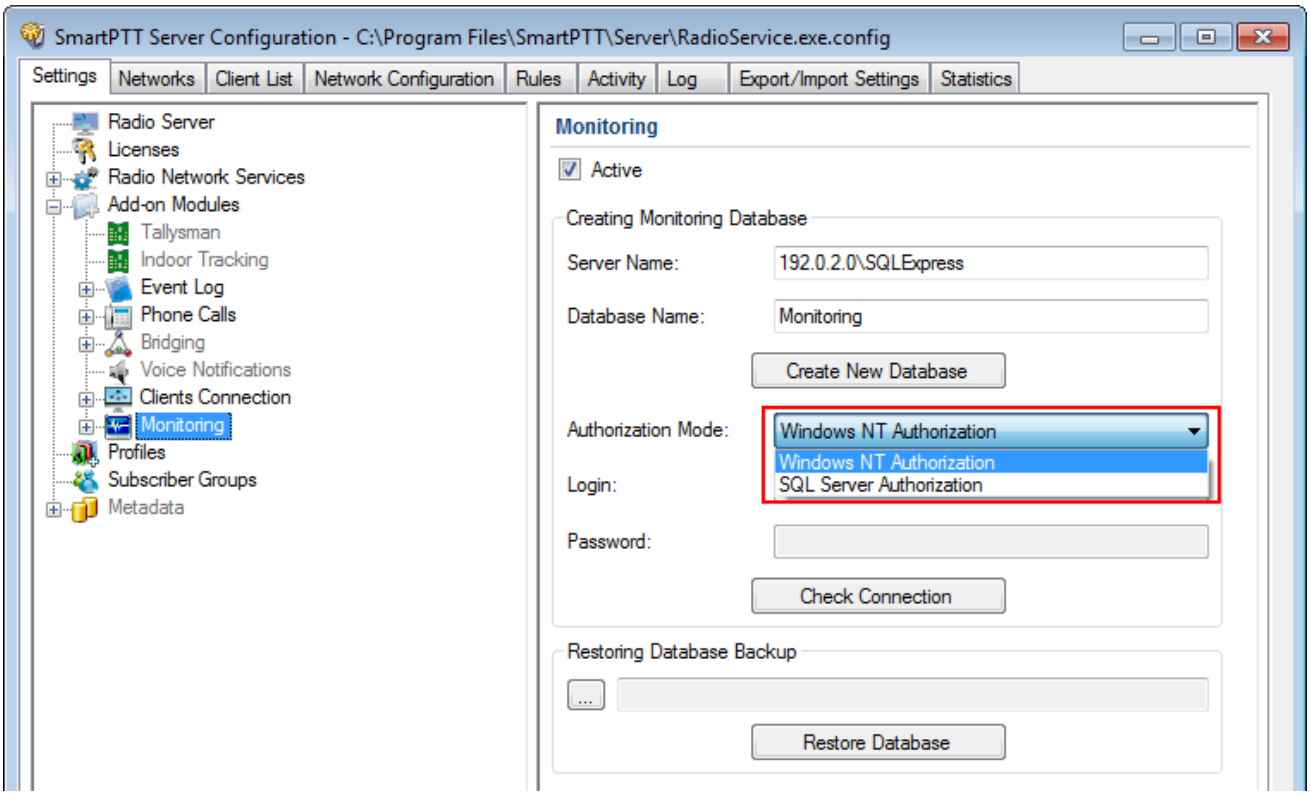


Figure 57 – Authorization Mode Selection

- **Windows NT Authorization**: Select to use your Windows login for connecting to a remote SQL Server from the same domain or if Windows Login is added [19].
- **SQL Server Authorization**: Select to use remote SQL Server login if SQL Server Login is added [23].

7. If **SQL Server Authorization** is selected, enter login and password.

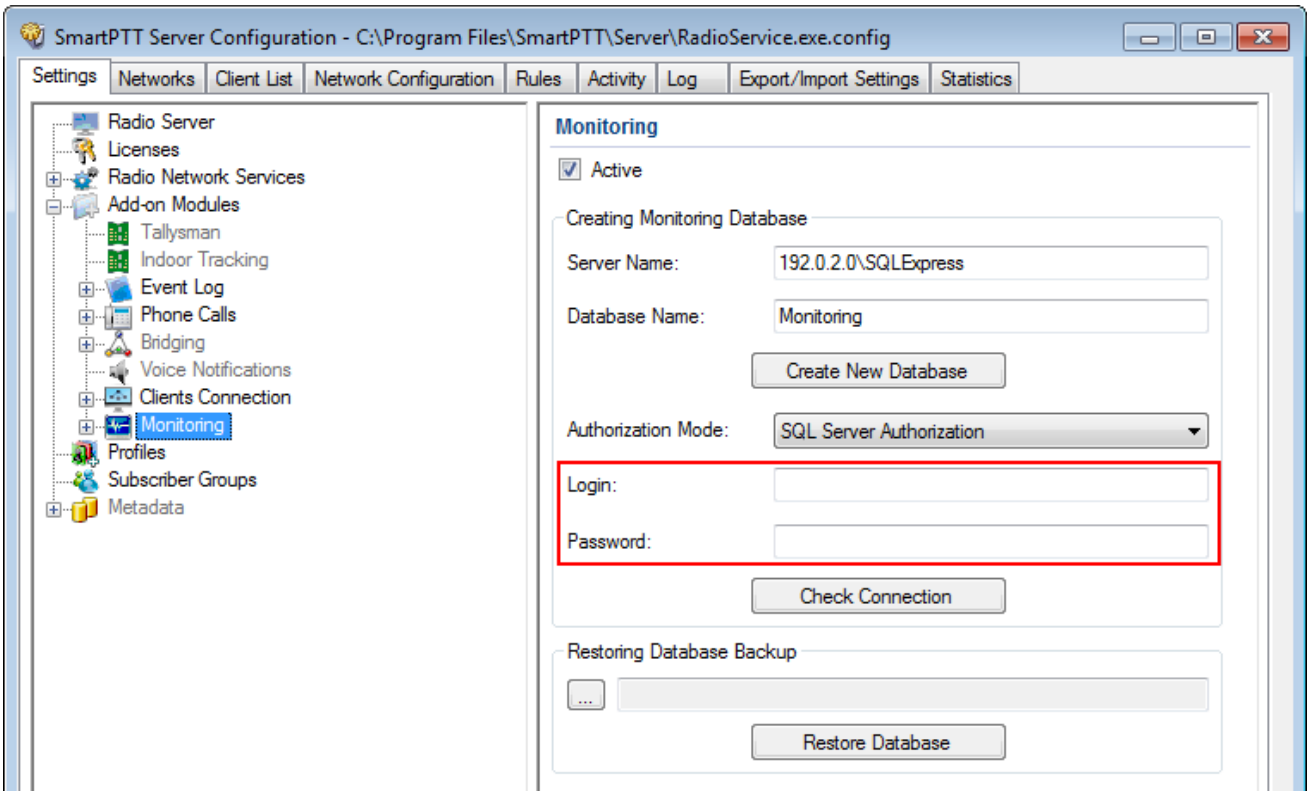


Figure 58 – Entering Login and Password

8. Click **Check Connection**.

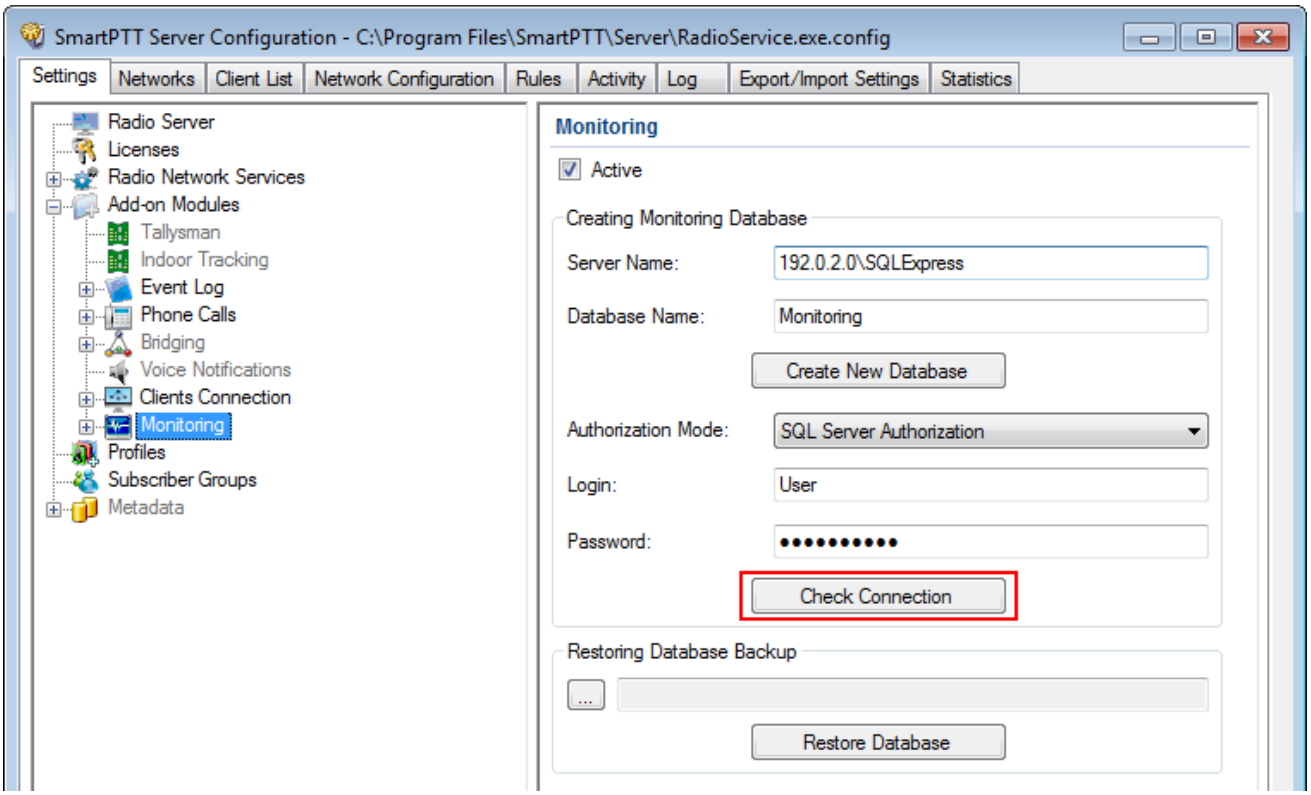


Figure 59 – Checking Remote Database Connection

If the connection is successful, the following message appears.

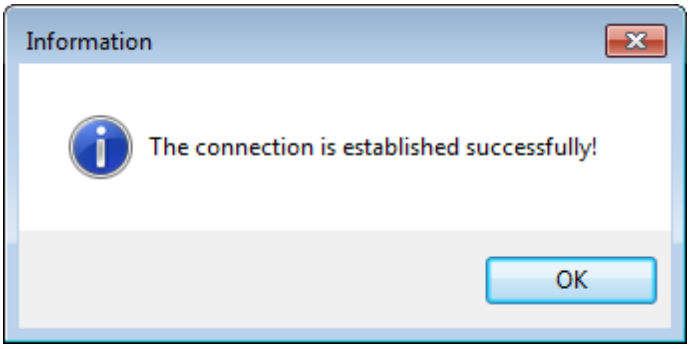


Figure 60 – Confirmation of Successful Remote Database Connection

9. Click **Save** to save changes and then click **Restart** to restart SmartPTT Radioserver.

Connection to the remote Monitoring database complete

8.3 Connecting to Remote Metadata Database

To connect to the remote Metadata database, perform the following actions:

1. Click **Metadata**.

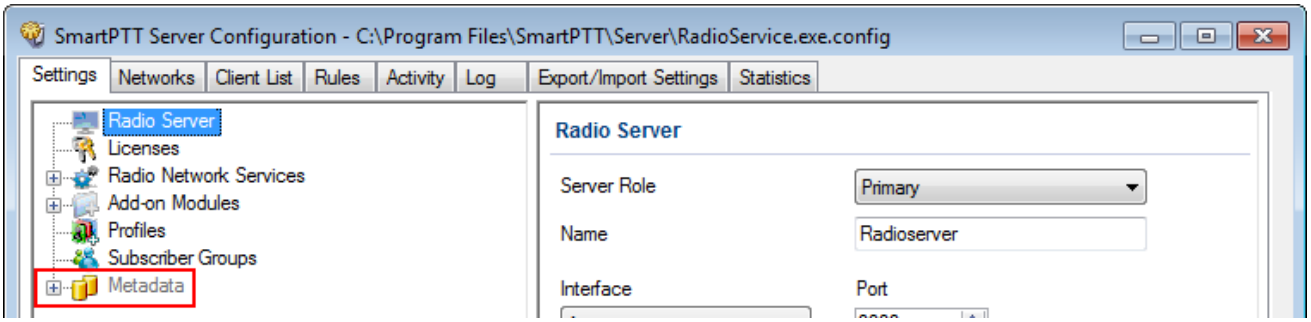


Figure 61 – Metadata Node

2. Make sure that the **Active** check box is selected in the **Metadata** pane.

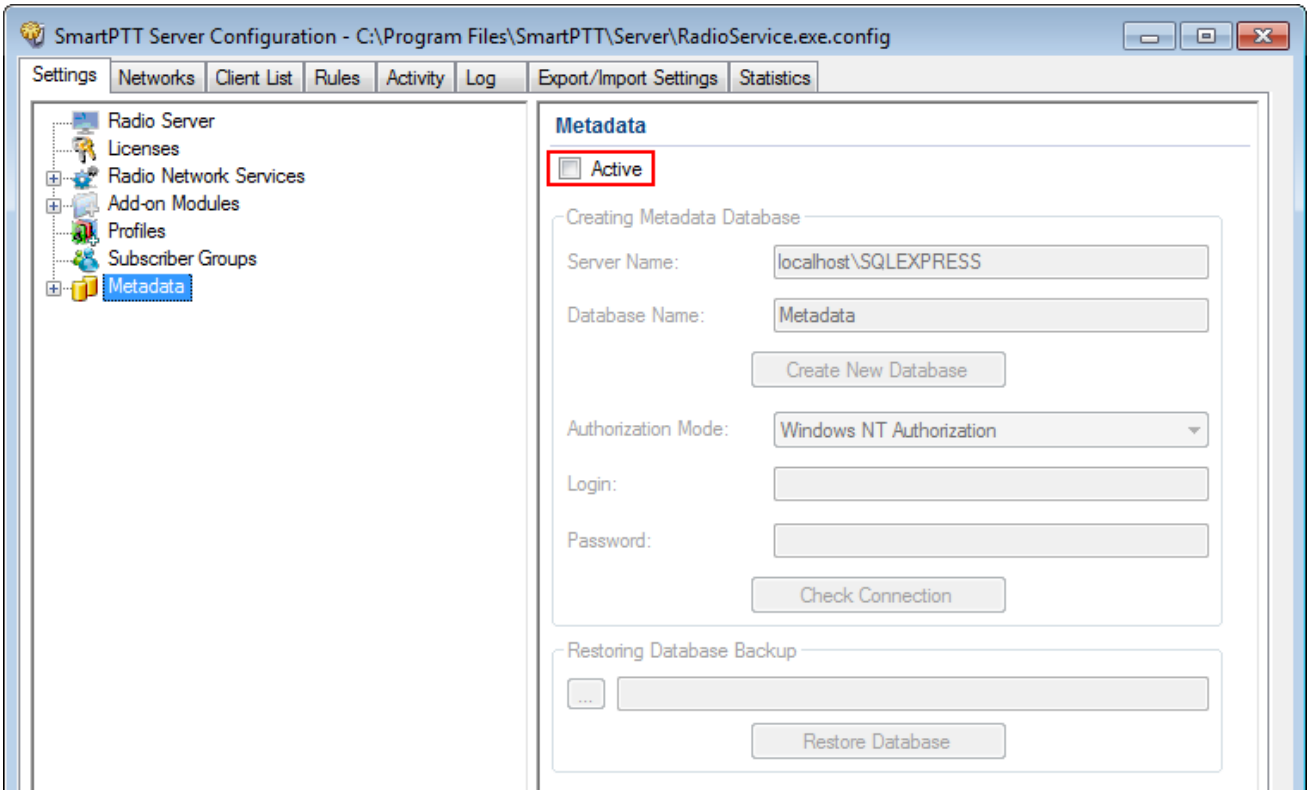


Figure 62 – Metadata Activation

3. In the **Server name** field, enter the SQL server name using the following format: <**IP address of a remote computer>\<Name of a remote SQL server>**.

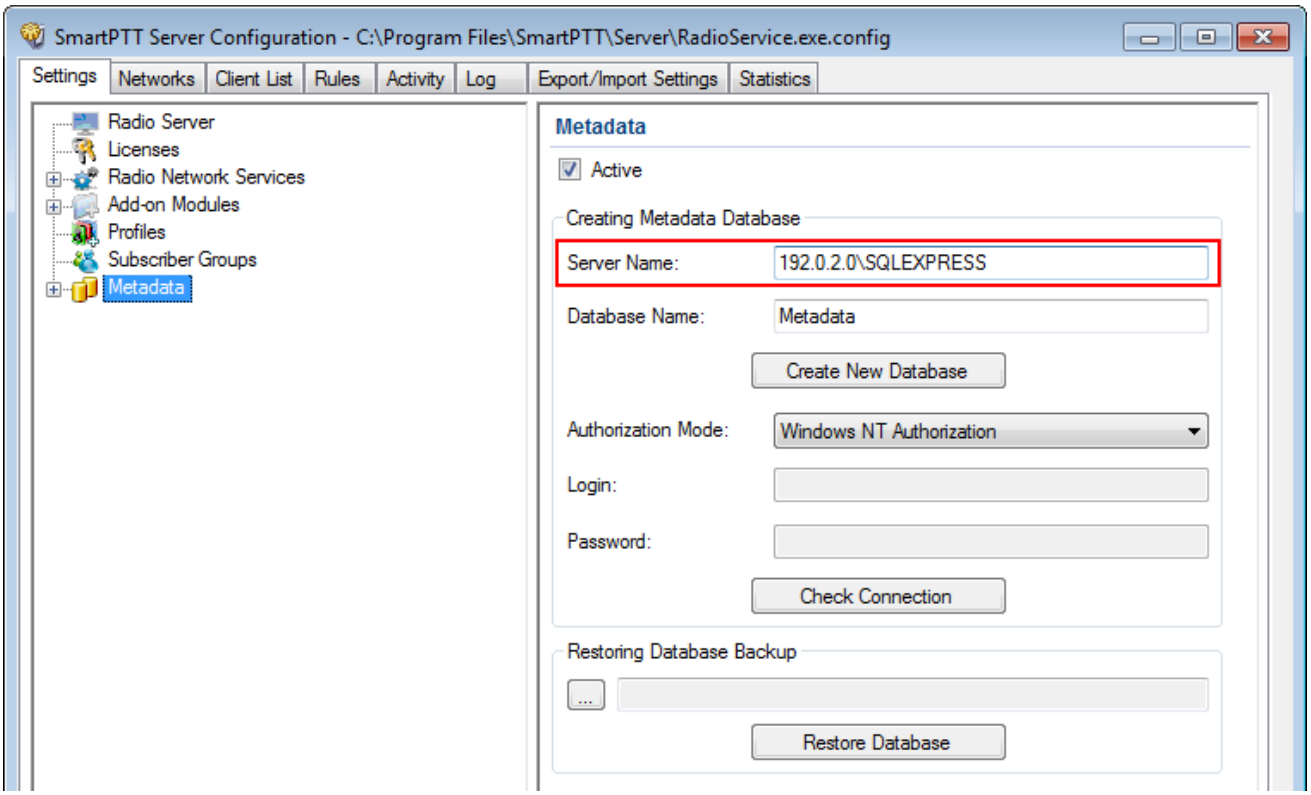


Figure 63 – Remote Database Server Name

4. In the **Database Name** field, enter the name of a remote Metadata database.

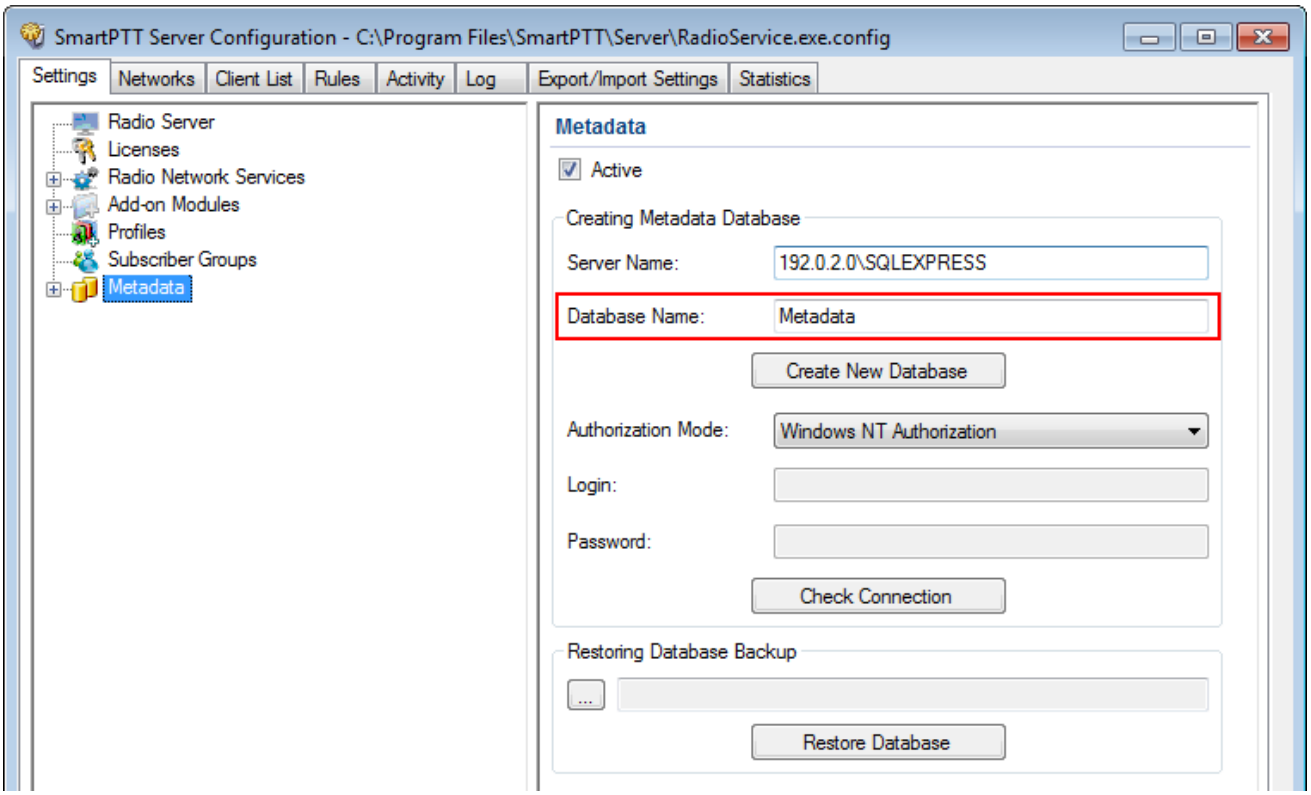


Figure 64 – Remote Database Name

5. In the **Authorization Mode** list, click the needed authorization type:

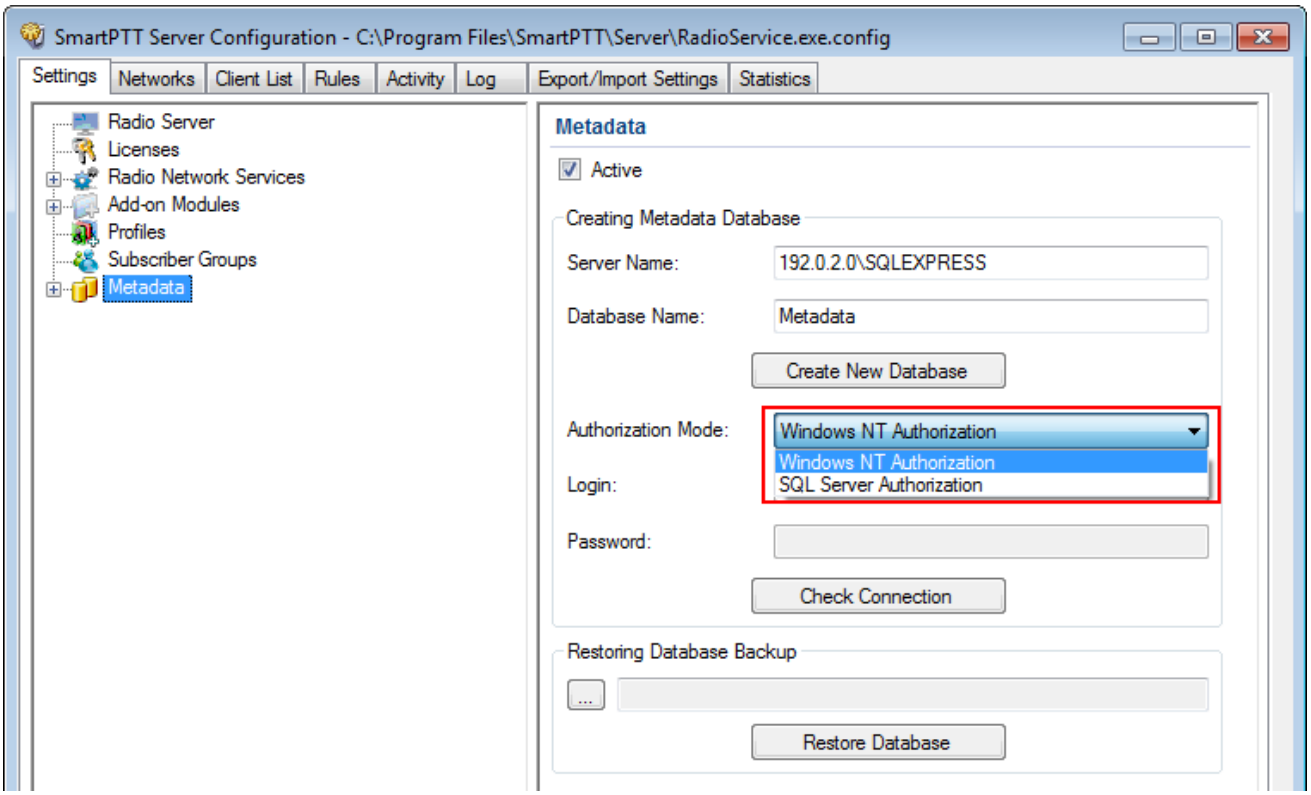


Figure 65 – Authorization Mode Selection

- **Windows NT Authorization**: Select to use your Windows account for connecting to a remote SQL Server from the same domain or if Windows Account is added[19].
- **SQL Server Authorization**: Select to use remote SQL Server account if SQL Server Authorization is added[23].

6. If **SQL Server Authorization** is selected, enter login and password.

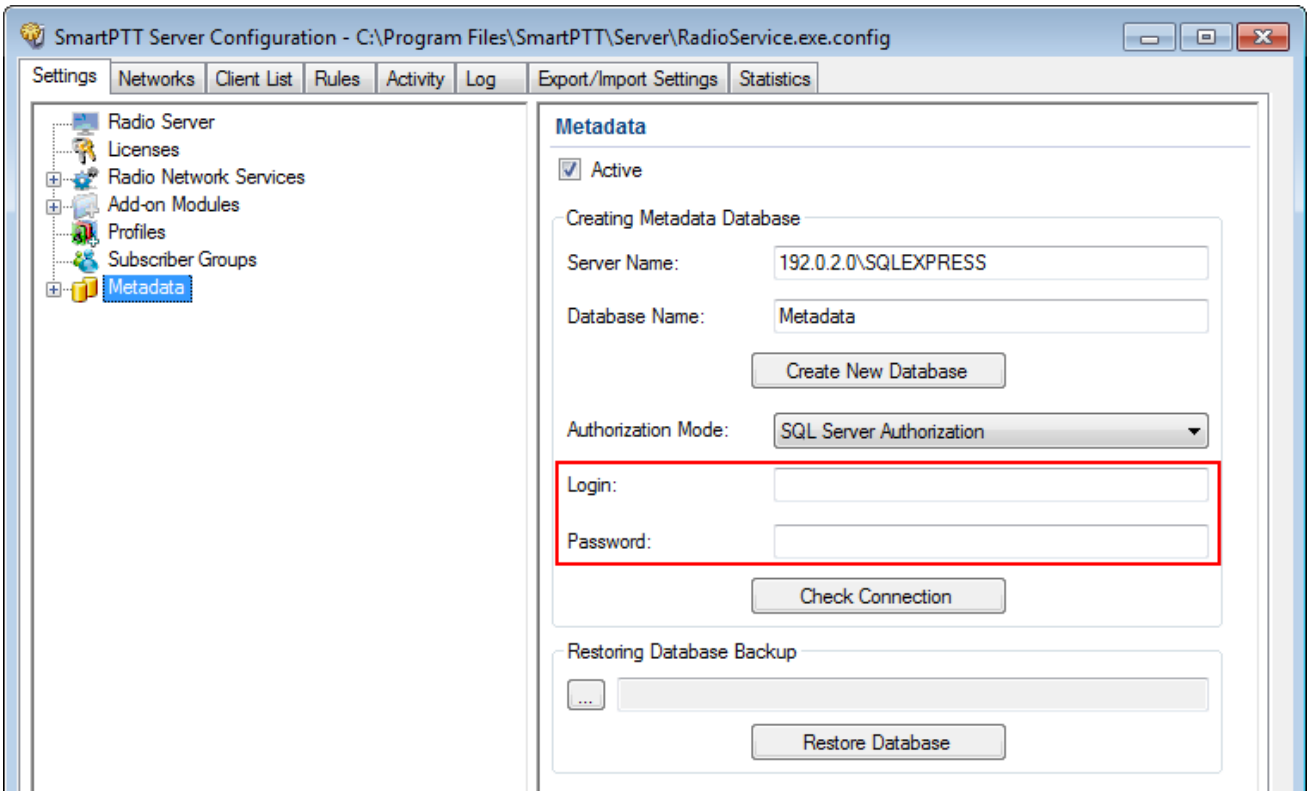


Figure 66 – Entering Login and Password

7. Click **Check Connection**.

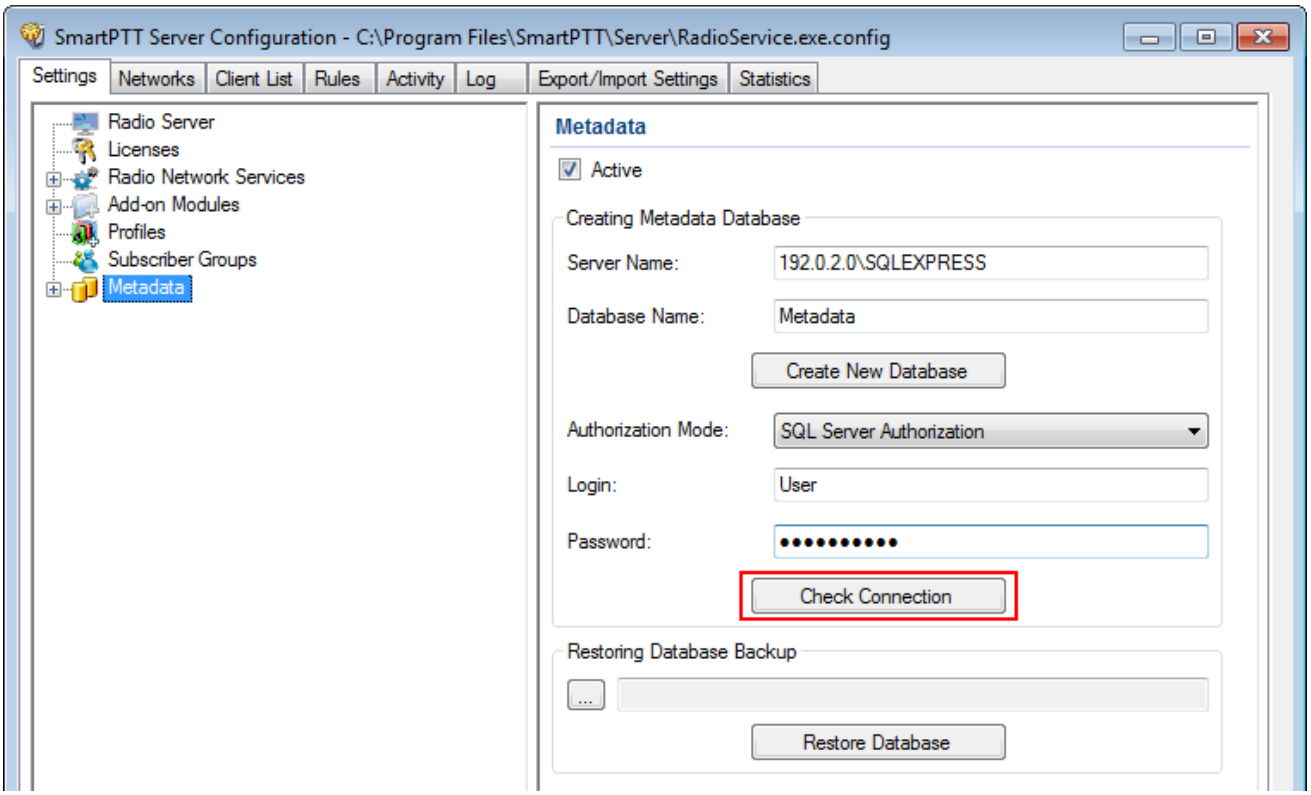


Figure 67 – Checking Remote Database Connection

If the connection is successful, the following message appears.

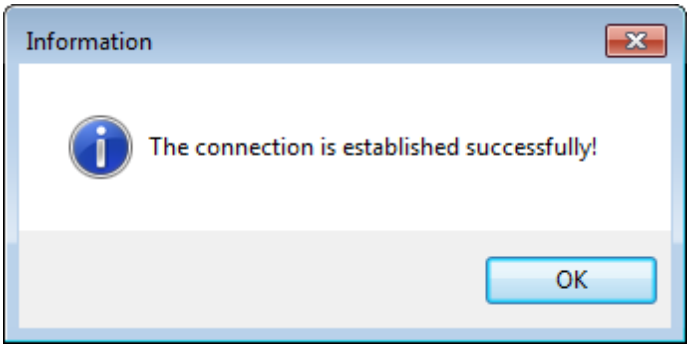
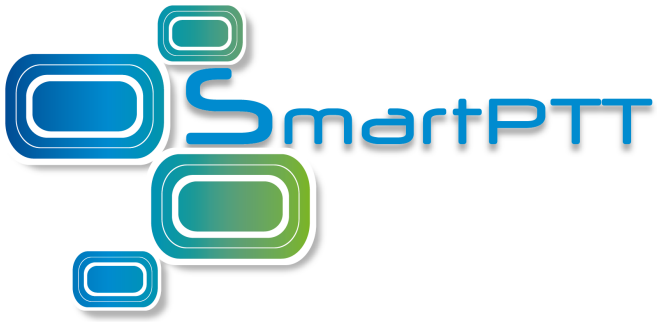


Figure 68 – Confirmation of Successful Remote Database Connection

8. Click **Save** to save changes and then click **Restart** to restart SmartPTT Radioserver.

Connection to the remote Metadata database complete.


SmartPTT

elcomplus