# CPS – extrernal SQL DB

Conteg Pro Server manual

**DATABASE MANUAL** **EN**

# Table of Contents

## Preliminary steps

1. Configure SQL Server (including Express Editions) for remote access: enable TCP/IP protocol and the SQL Server Browser service.
2. Add exceptions in the Windows Firewall for sqlservr.exe and its ports.

We'll cover these steps below, using this blog as the source for information:

http://akawn.com/blog/2012/01/configuring-sql-server-2008-r2-express-edition-for-remote-access/

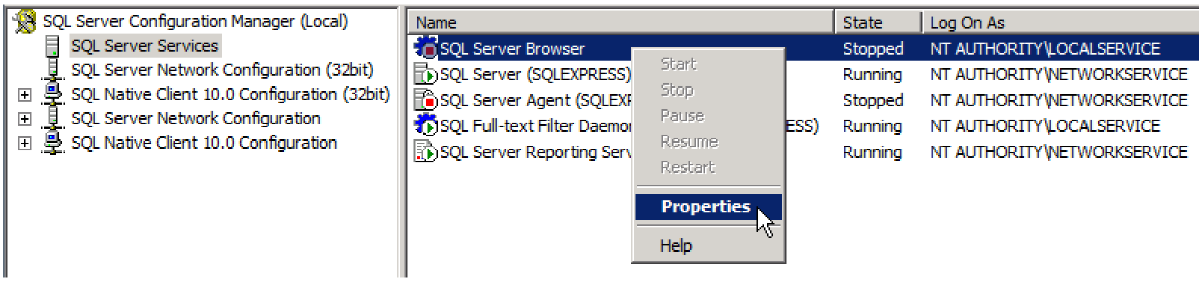
## Configuring SQL Server 2008 R2 Express Edition for remote access

Below are the steps to allow remote access to a SQL Server 2008 R2 x64 Express Edition instance after the default install steps where performed.

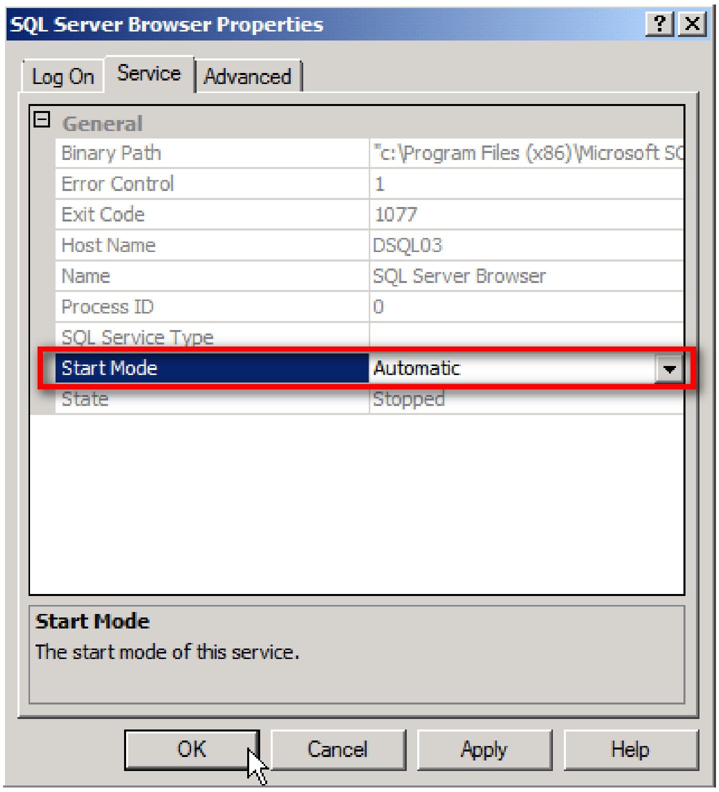
Also included are the additional configuration steps for SQL Server 2008 R2 x64 Express Edition with Advanced Services.

The steps were performed on Windows Server 2008 R2 64bit.

Start the **SQL Server Configuration Manager** from the Start menu, and choose Services.


SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
SQL Native Client 10.0 Configuration
Start
Stop
Pause
Resume
Restart
Properties
Help

| Name | State | Log On As |
|---|---|---|
| SQL Server Browser | Stopped | NT AUTHORITY\LOCALSERVICE |
| SQL Server (SQLEXPRESS) | Running | NT AUTHORITY\NETWORKSERVICE |
| SQL Server Agent (SQLEXF | Stopped | NT AUTHORITY\NETWORKSERVICE |
| SQL Full-text Filter Daemo ESS) | Running | NT AUTHORITY\LOCALSERVICE |
| SQL Server Reporting Serv | Running | NT AUTHORITY\NETWORKSERVICE |



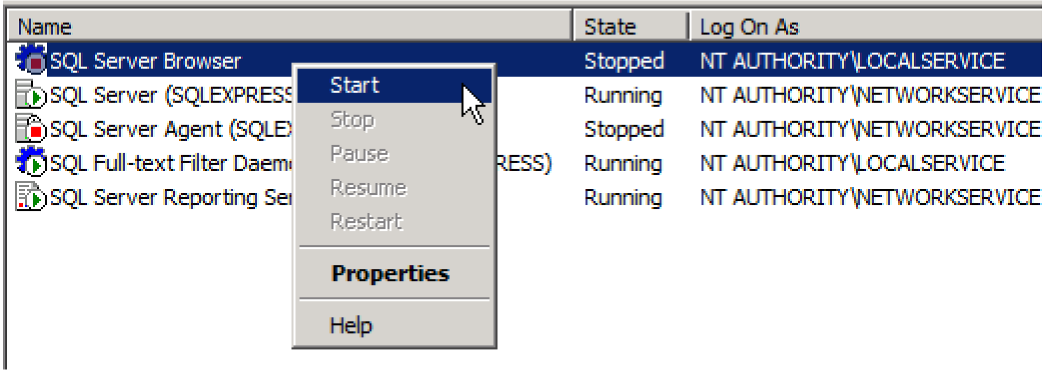
General

| | |
|---|---|
| Binary Path | "c:\Program Files (x86)\Microsoft SQ |
| Error Control | 1 |
| Exit Code | 1077 |
| Host Name | DSQL03 |
| Name | SQL Server Browser |
| Process ID | 0 |
| SQL Service Type | |
| Start Mode | Automatic |
| State | Stopped |

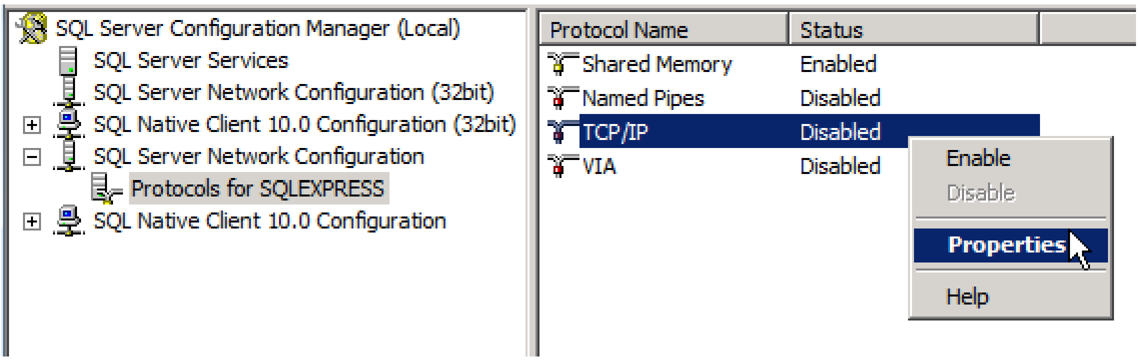
**Start Mode**

The start mode of this service.

Find the **SQL Server Browser** service and set its Start Mode to Automatic, then start it.



| Name | State | Log On As |
|---|---|---|
| SQL Server Browser | Stopped | NT AUTHORITY\LOCALSERVICE |
| SQL Server (SQLEXPRESS | Running | NT AUTHORITY\NETWORKSERVICE |
| SQL Server Agent (SQLE) | Stopped | NT AUTHORITY\NETWORKSERVICE |
| SQL Full-text Filter Daem RESS) | Running | NT AUTHORITY\LOCALSERVICE |
| SQL Server Reporting Se | Running | NT AUTHORITY\NETWORKSERVICE |



SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration
Enable
Disable
Properties
Help

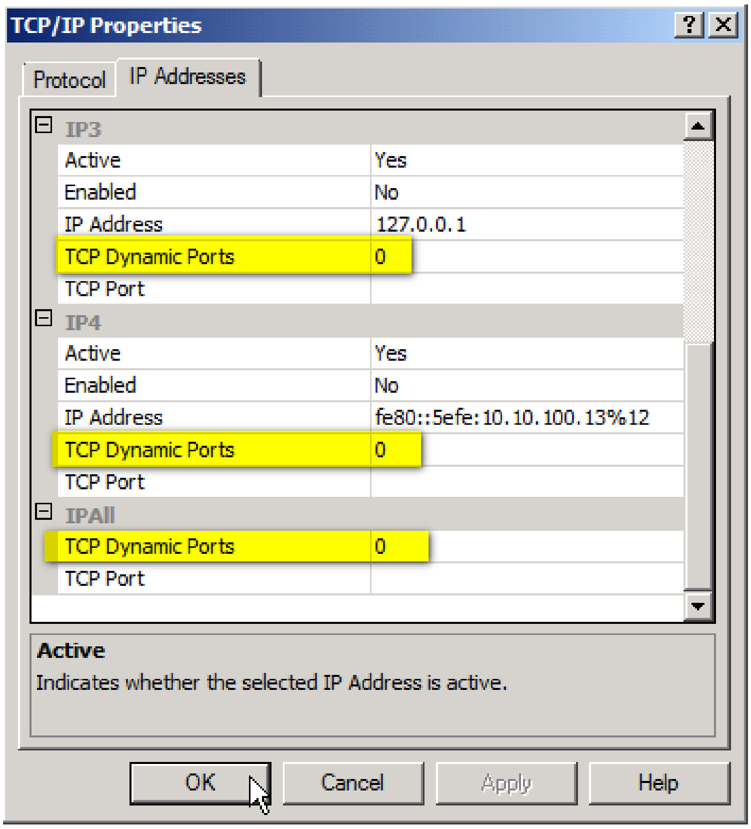
| Protocol Name | Status |
|---|---|
| Shared Memory | Enabled |
| Named Pipes | Disabled |
| TCP/IP | Disabled |
| VIA | Disabled |

Next go to **Protocols** in the Network Configuration, and find TCP/IP.

Below you can see that by default, SQL Server Express allocates a Dynamic port when SQL Server starts.

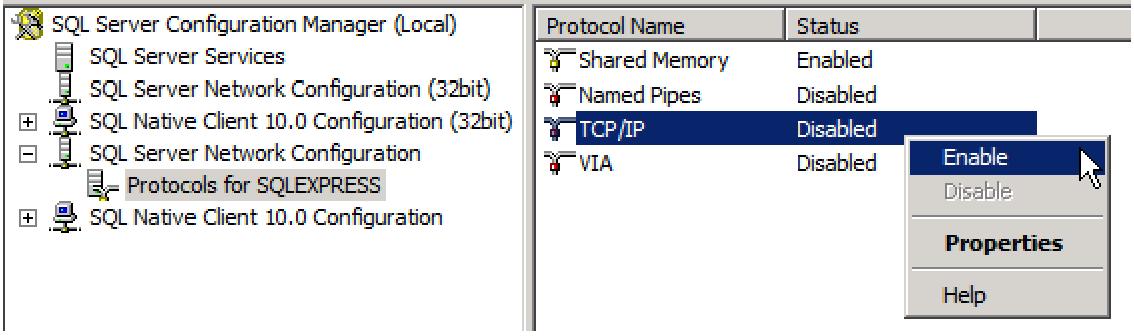
You can either keep this setting or change SQL Server to listen on a fixed TCP port e.g. TCP 1433. This can be achieved by removing 0 from all the 'TCP Dynamic Ports' rows and placing the fixed TCP port you want to use on all the 'TCP Port' rows below it.

***For this demo we will keep SQL Server allocating a Dynamic port on start-up and therefore we have not changed anything on this tab.***



| | |
|---|---|
| **IP3** | |
| Active | Yes |
| Enabled | No |
| IP Address | 127.0.0.1 |
| TCP Dynamic Ports | 0 |
| TCP Port | |
| **IP4** | |
| Active | Yes |
| Enabled | No |
| IP Address | fe80::5efe:10.10.100.13%12 |
| TCP Dynamic Ports | 0 |
| TCP Port | |
| **IPAll** | |
| TCP Dynamic Ports | 0 |
| TCP Port | |

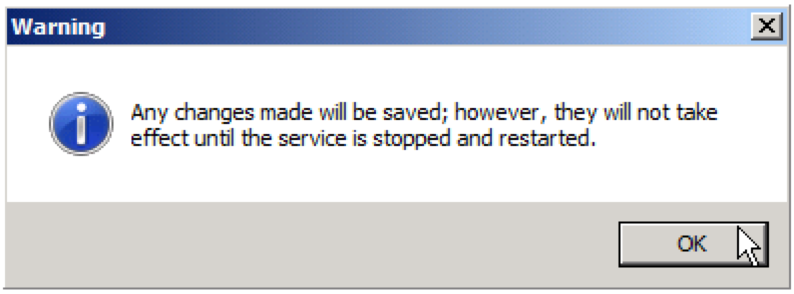
**Active**
Indicates whether the selected IP Address is active.



SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration
Enable
Disable
Properties
Help

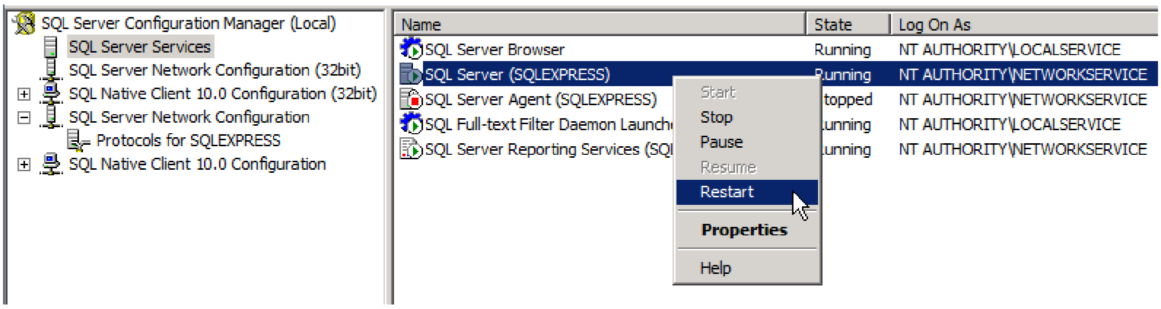
| Protocol Name | Status |
|---|---|
| Shared Memory | Enabled |
| Named Pipes | Disabled |
| TCP/IP | Disabled |
| VIA | Disabled |

Enable the protocol.



Warning

Any changes made will be saved; however, they will not take effect until the service is stopped and restarted.



SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for SQLEXPRESS
SQL Native Client 10.0 Configuration
Start
Stop
Pause
Resume
Restart
Properties
Help

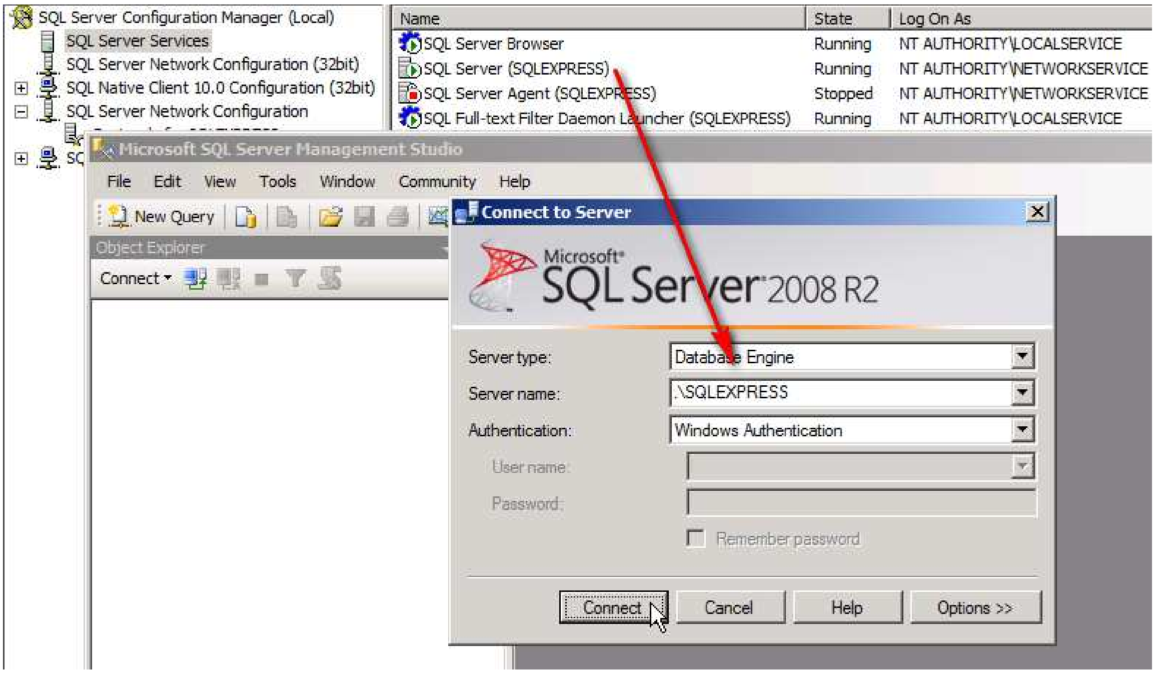
| Name | State | Log On As |
|---|---|---|
| SQL Server Browser | Running | NT AUTHORITY\LOCALSERVICE |
| SQL Server (SQLEXPRESS) | Running | NT AUTHORITY\NETWORKSERVICE |
| SQL Server Agent (SQLEXPRESS) | topped | NT AUTHORITY\NETWORKSERVICE |
| SQL Full-text Filter Daemon Launch | unning | NT AUTHORITY\LOCALSERVICE |
| SQL Server Reporting Services (SQL | unning | NT AUTHORITY\NETWORKSERVICE |

Finally, restart the SQL Server service to apply the changes.

Next, open the **SQL Server Management Studio**.

Connect to SQL Server Express on the server you installed it.

As below you can see the instance when SQL Server Express is installed is called SQLEXPRESS if you did not change it.



SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
Microsoft SQL Server Management Studio
File
Edit
View
Tools
Window
Community
Help
New Query
Object Explorer
Connect
Connect to Server
Microsoft SQL Server 2008 R2
Connect
Cancel
Help
Options >>

| Name | State | Log On As |
|---|---|---|
| SQL Server Browser | Running | NT AUTHORITY\LOCALSERVICE |
| SQL Server (SQLEXPRESS) | Running | NT AUTHORITY\NETWORKSERVICE |
| SQL Server Agent (SQLEXPRESS) | Stopped | NT AUTHORITY\NETWORKSERVICE |
| SQL Full-text Filter Daemon Launcher (SQLEXPRESS) | Running | NT AUTHORITY\LOCALSERVICE |

Server type: Database Engine

Server name: .\SQLEXPRESS

Authentication: Windows Authentication

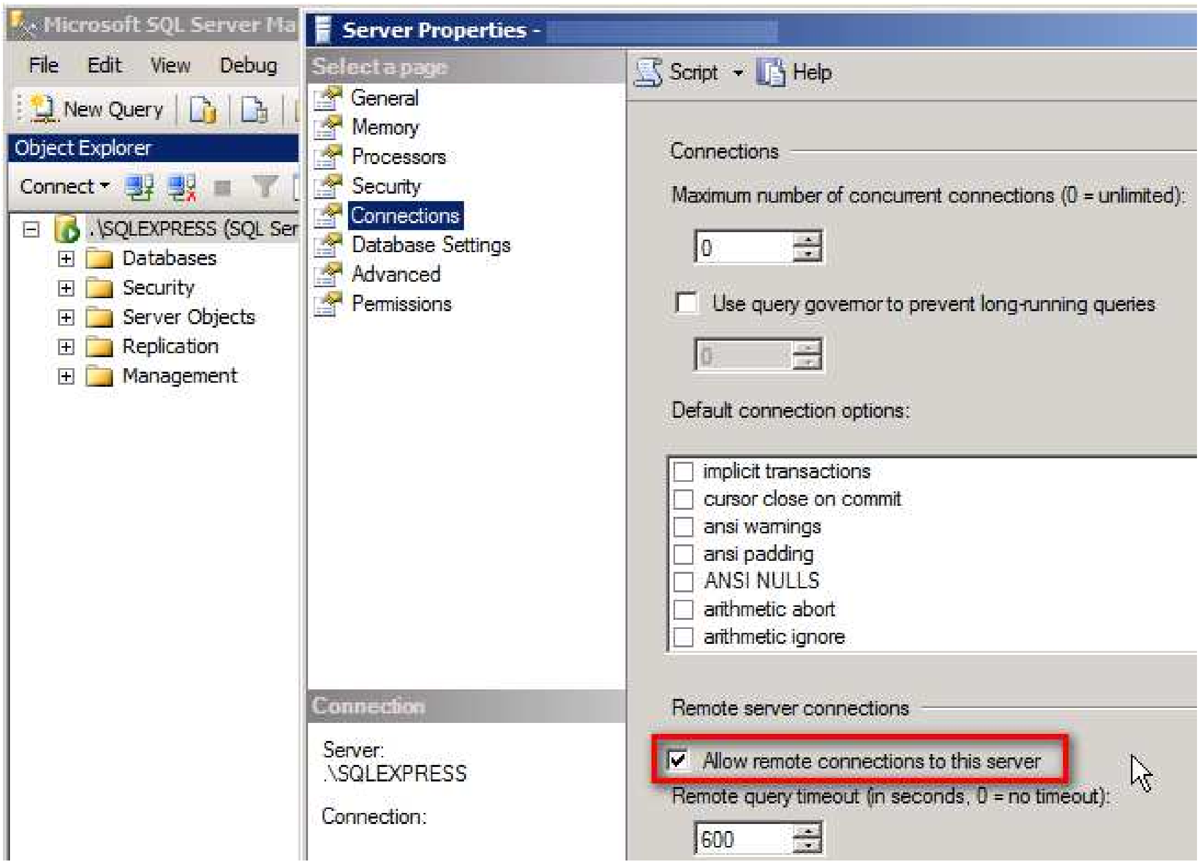
User name:

Password:

□ Remember password

Right click on the server, and select **Properties**.

The below should already be enabled, but if it isn’t, then enable it and restart the SQL Server service.



Server:
.\SQLEXPRESS

Connection:

Connections

Maximum number of concurrent connections (0 = unlimited):

0

☐ Use query governor to prevent long-running queries

0

Default connection options:

☐ implicit transactions
☐ cursor close on commit
☐ ansi warnings
☐ ansi padding
☐ ANSI NULLS
☐ arithmetic abort
☐ arithmetic ignore

Remote server connections

☑ Allow remote connections to this server

Remote query timeout (in seconds, 0 = no timeout):

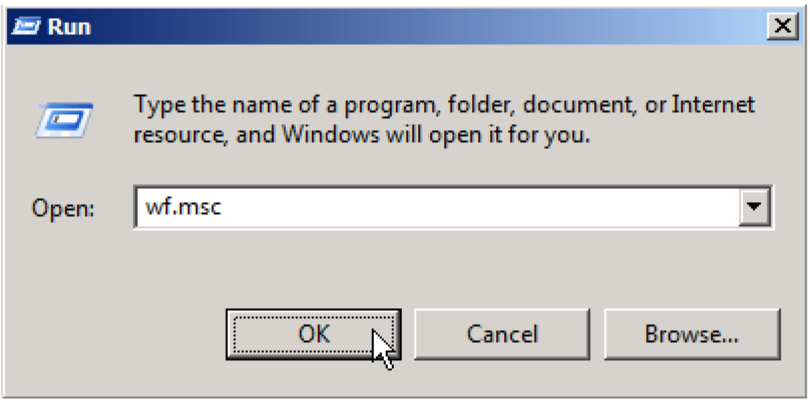
600

Check that **Allow remote connections to this server** is enabled

## Firewall configuration

If you have the Windows Firewall turned on, you’ll need to do the following steps.

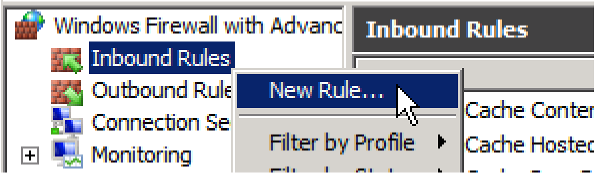
Start the **Windows Firewall with Advanced Services** configuration:

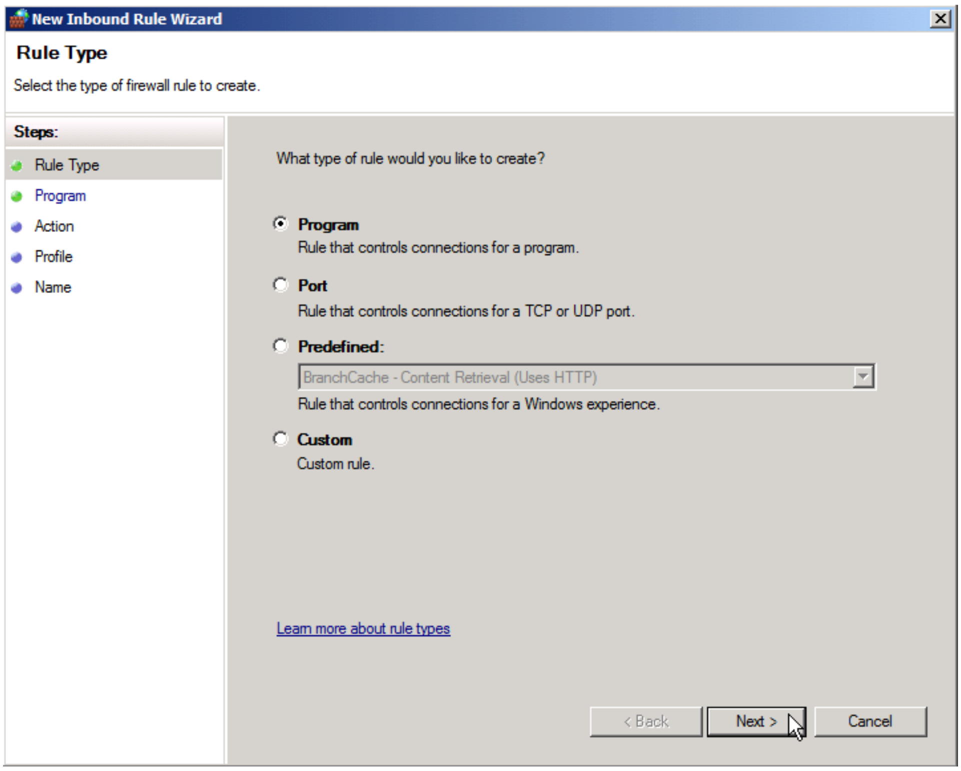


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wf.msc

Add a new rule:





**Rule Type**

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

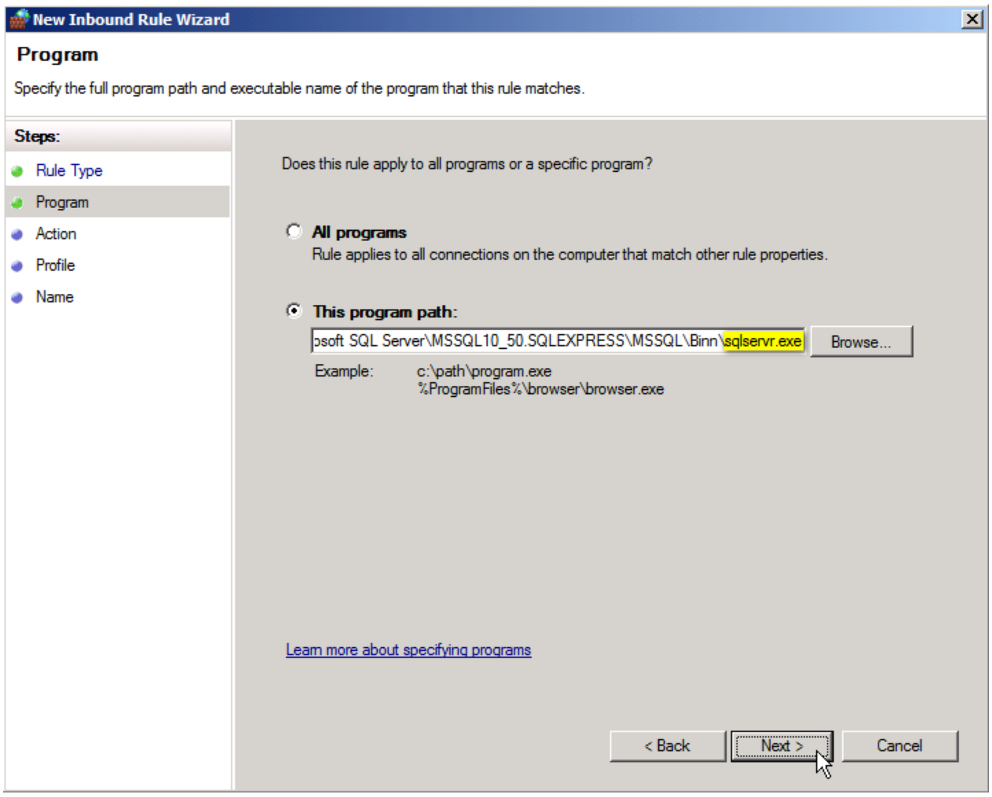
What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.



**Program**

Specify the full program path and executable name of the program that this rule matches.

Does this rule apply to all programs or a specific program?

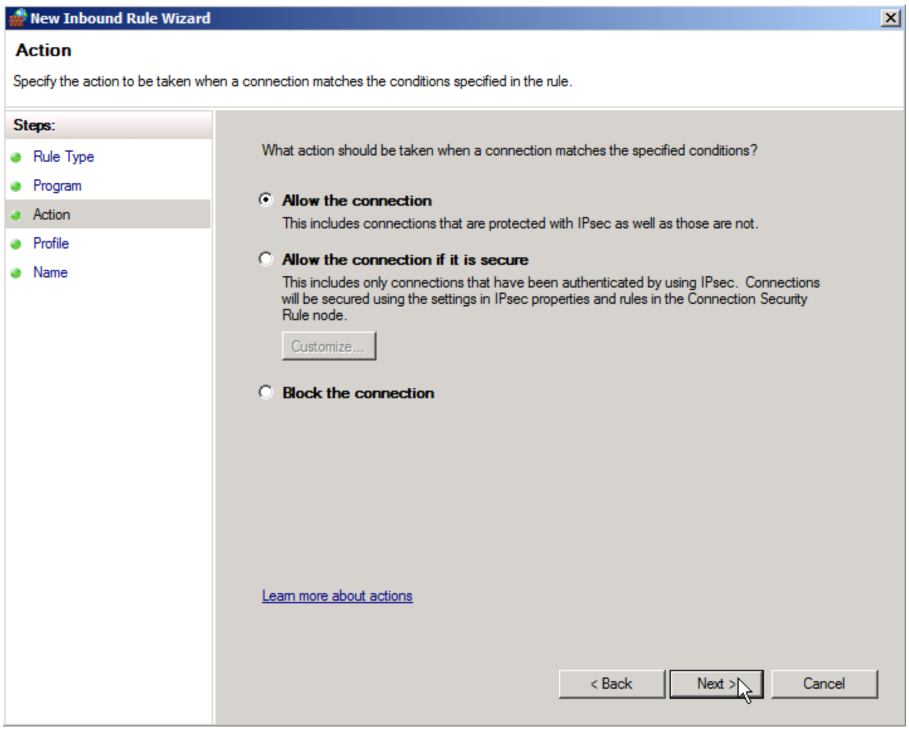
○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

● **This program path:**
osoft SQL Server\MSSQL10_50.SQLEXPRESS\MSSQL\Binn\sqlservr.exe

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Learn more about specifying programs

Choose the sqlservr.exe



**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

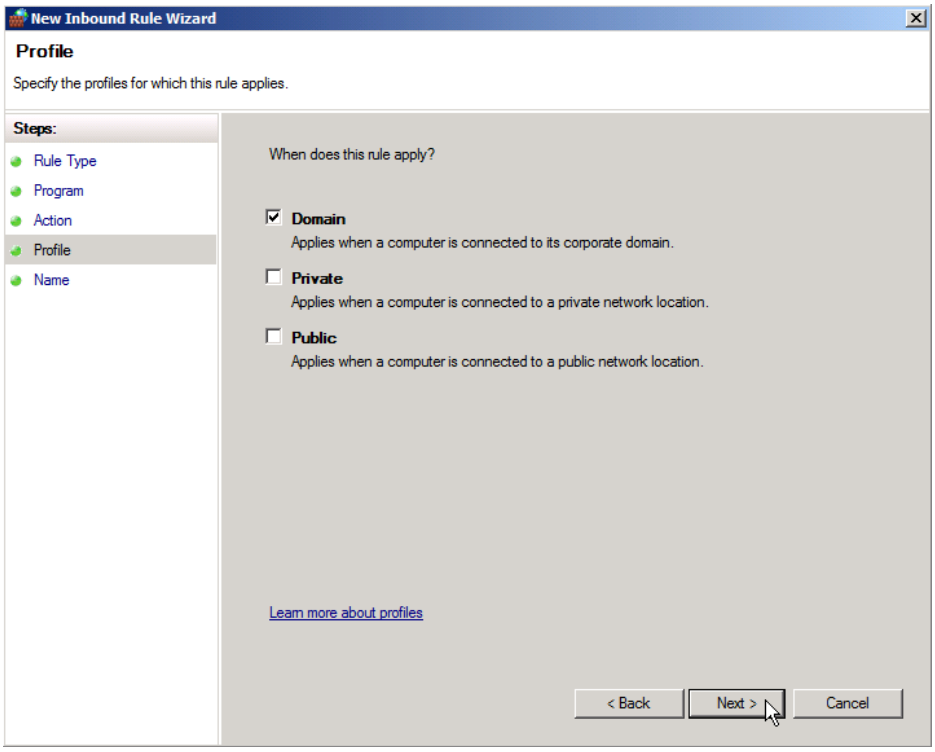
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **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.

○ **Block the connection**

Learn more about actions



New Inbound Rule Wizard

**Profile**

Specify the profiles for which this rule applies.

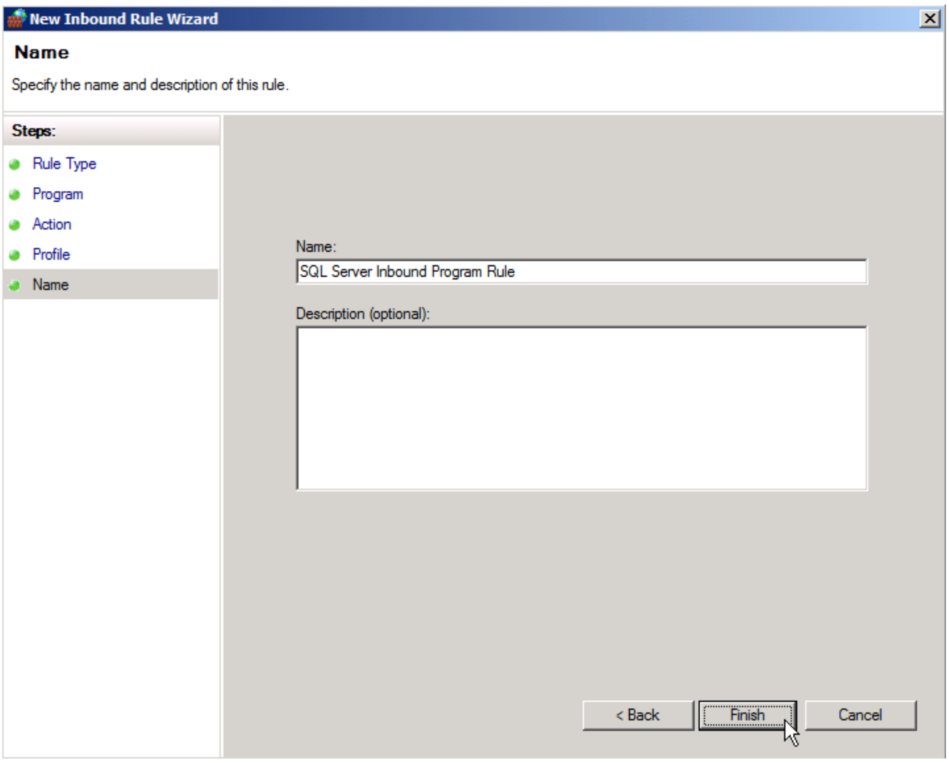
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

□ **Private**
Applies when a computer is connected to a private network location.

□ **Public**
Applies when a computer is connected to a public network location.

Select the network profiles where this rule applies.



New Inbound Rule Wizard

**Name**

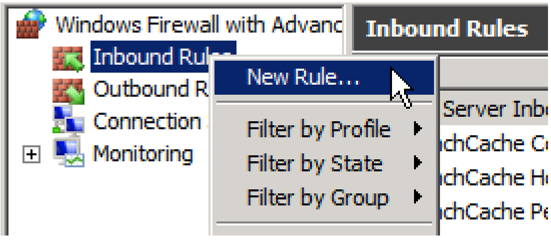
Specify the name and description of this rule.

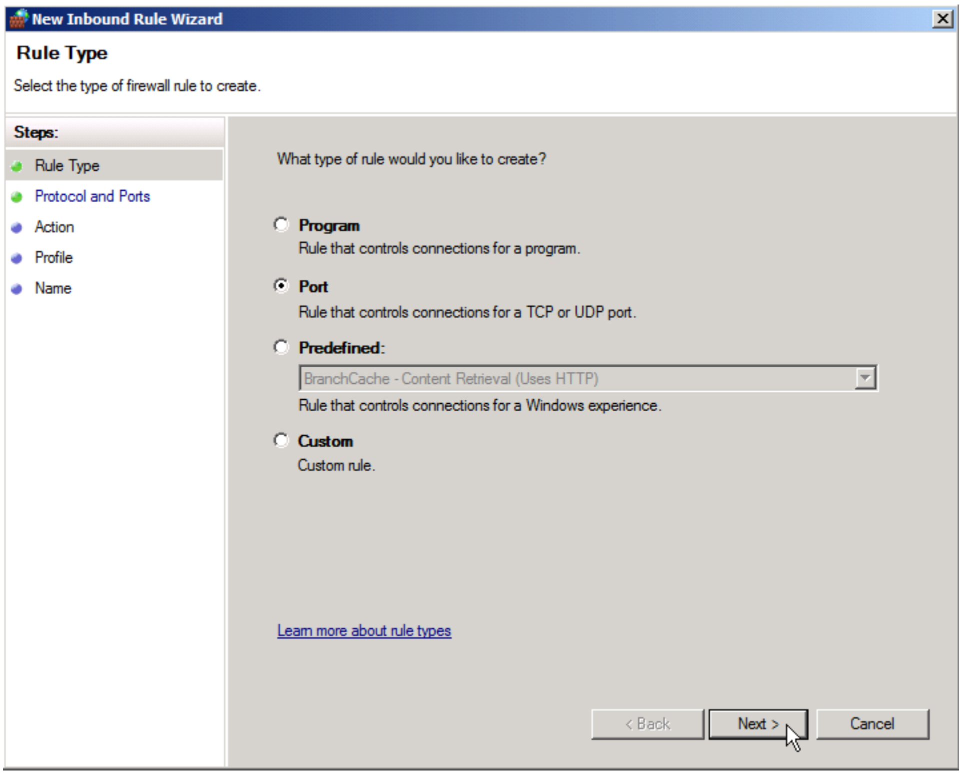
Name:
SQL Server Inbound Program Rule

Description (optional):

Finally, give it a name.

## Configure the required firewall ports





**Rule Type**

Select the type of firewall rule to create.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

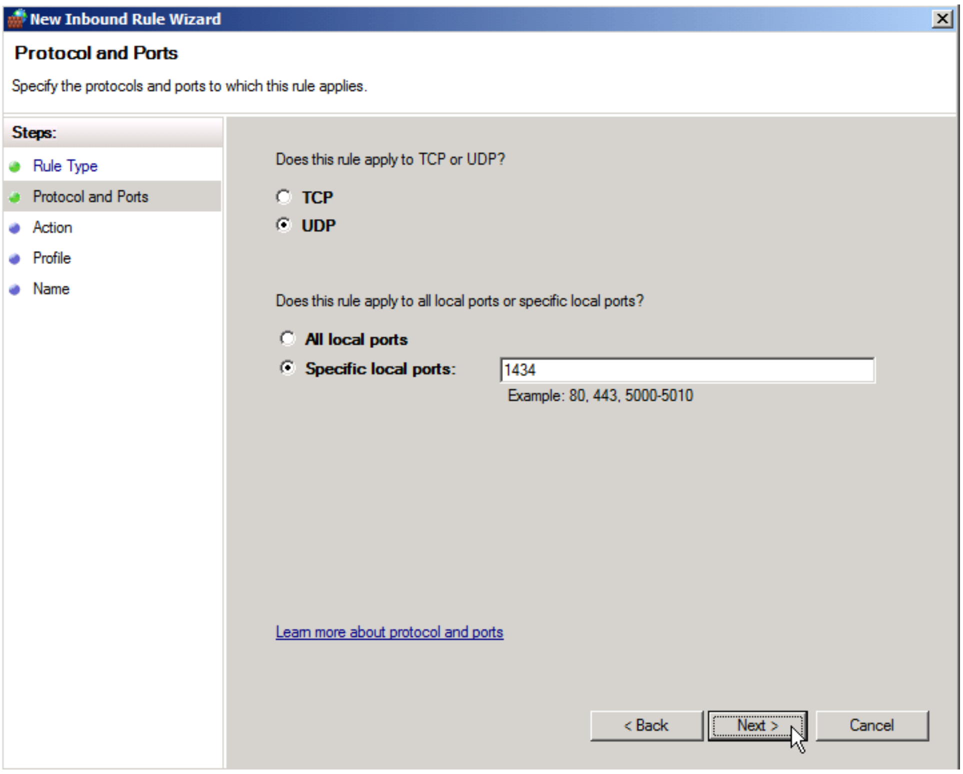
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Learn more about rule types

Choose Port



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

○ TCP

● UDP

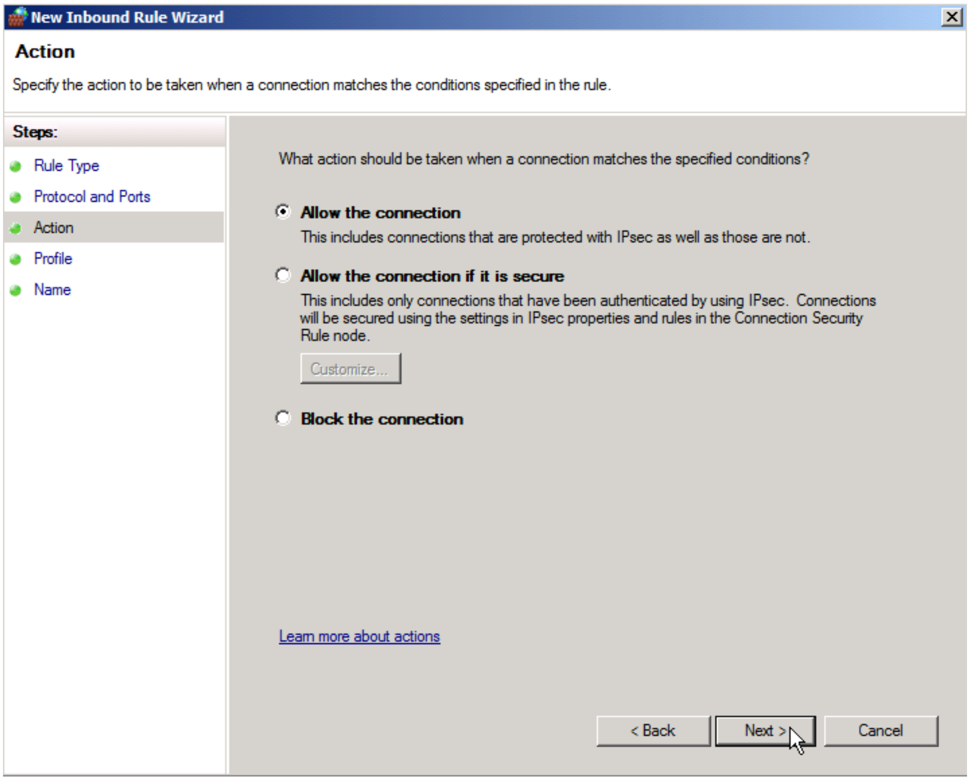
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 1434

Example: 80, 443, 5000-5010

The default port is UDP 1434



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

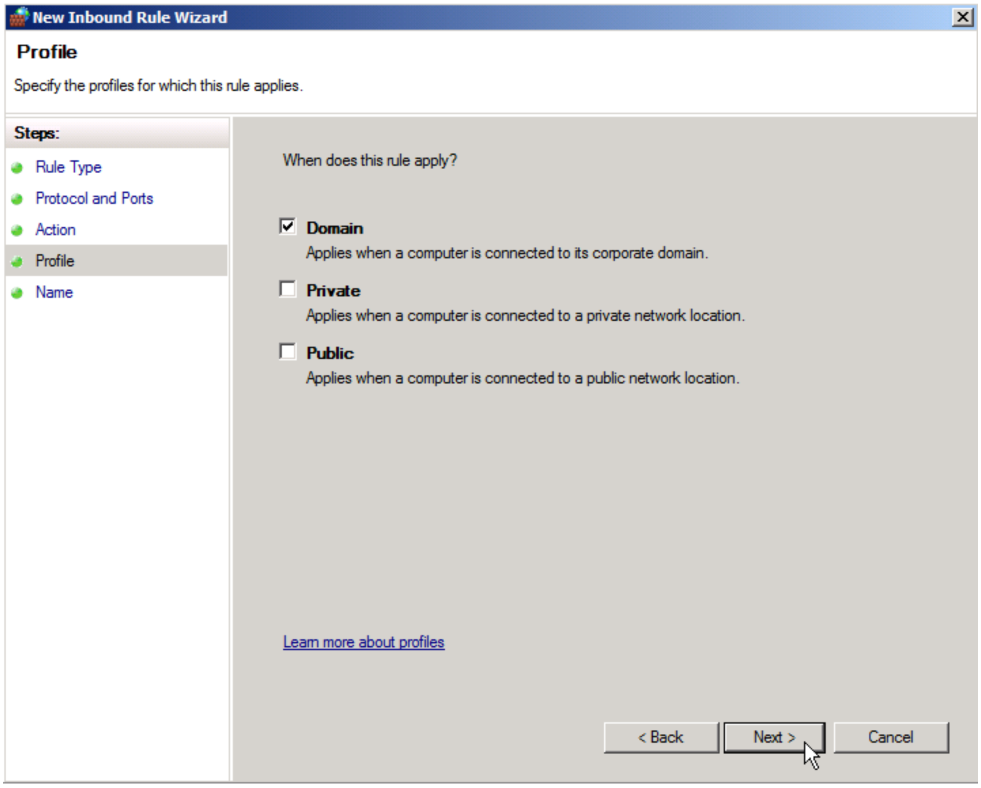
● Allow the connection

This includes connections that are protected with IPsec as well as those are not.

○ 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.

○ Block the connection



New Inbound Rule Wizard

**Profile**

Specify the profiles for which this rule applies.

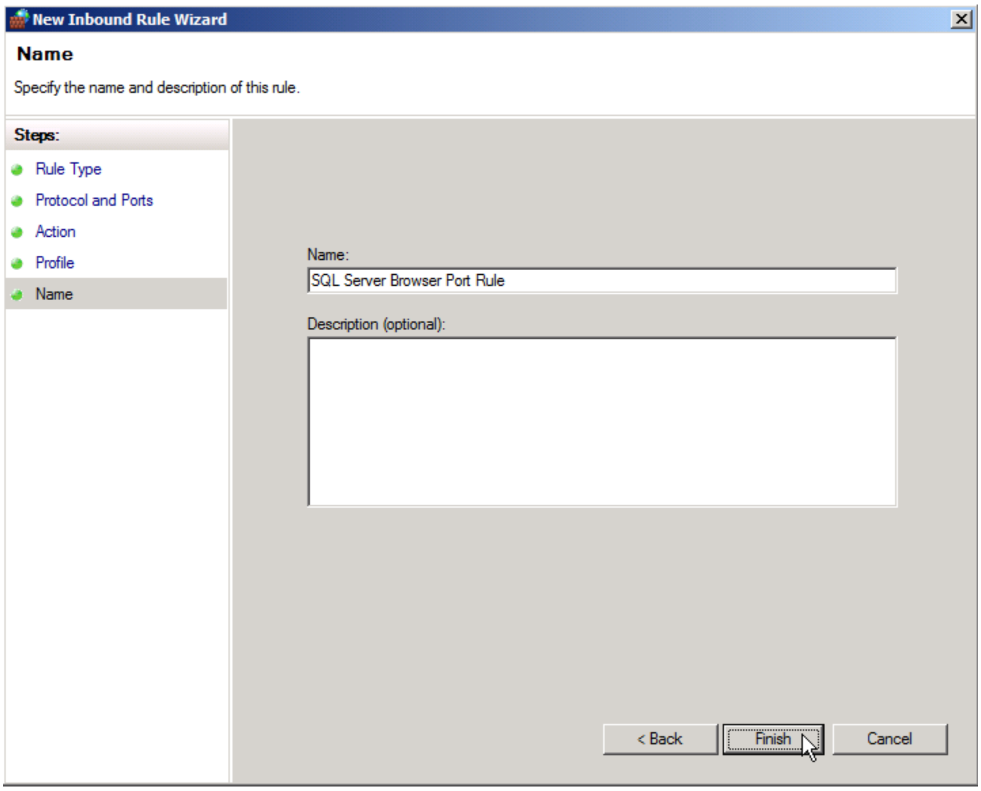
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☐ **Private**
Applies when a computer is connected to a private network location.

☐ **Public**
Applies when a computer is connected to a public network location.



New Inbound Rule Wizard

**Name**

Specify the name and description of this rule.

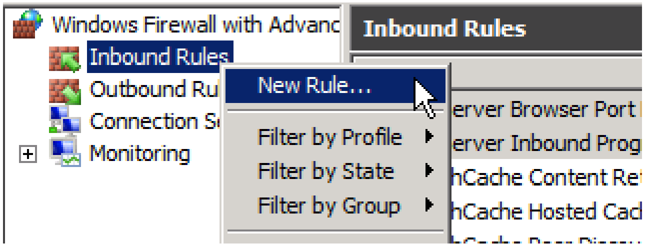
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

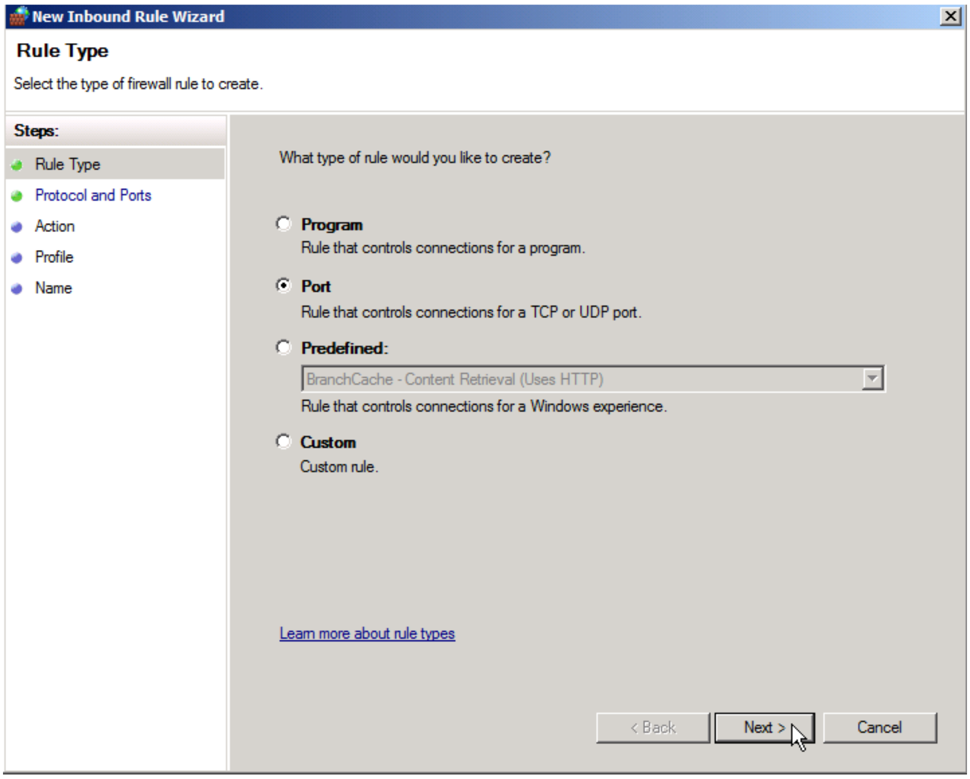
Name: SQL Server Browser Port Rule

Description (optional):

## Configuration options for SQL Server Reporting Services

The Firewall Port rule below is required only if you installed SQL Server Express with Advanced Services and selected the SQL Server Reporting Services feature.




New Inbound Rule Wizard

**Rule Type**

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

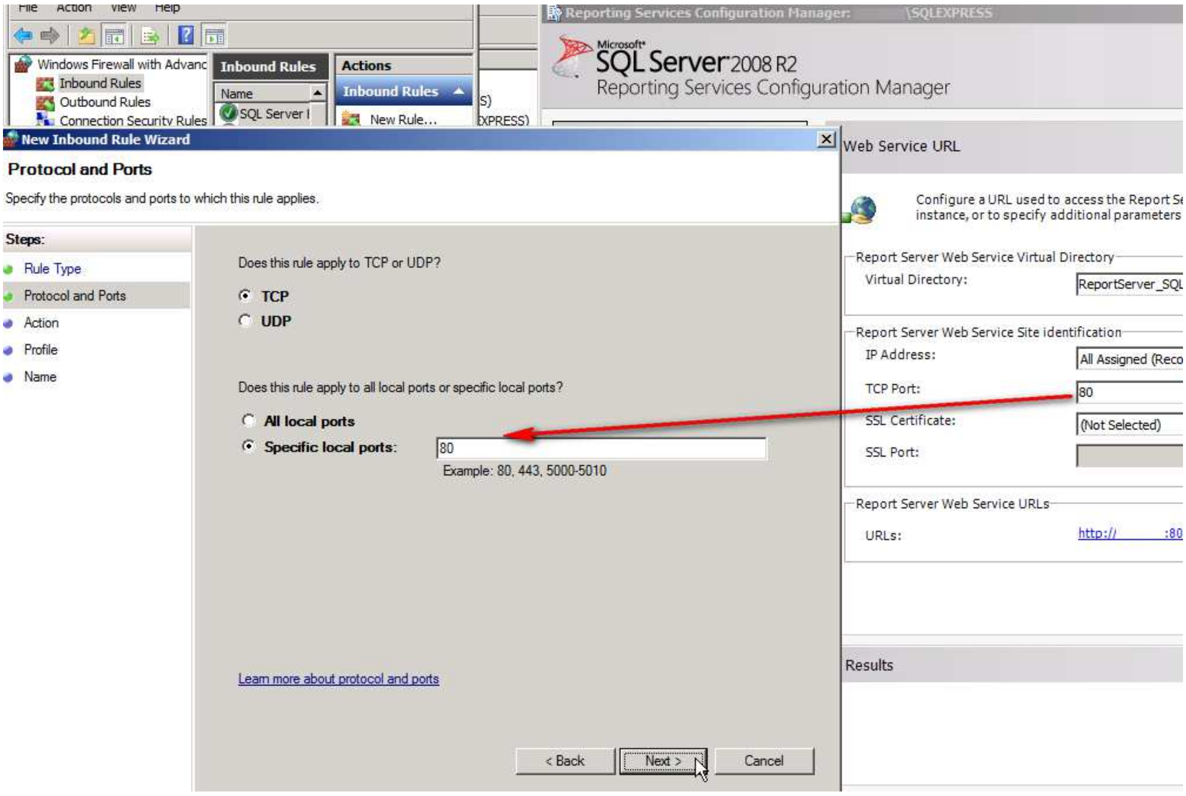
○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Learn more about rule types

< Back | Next > | Cancel

If you changed the HTTP TCP port from the default on 80, then you should enter the port you are using here.


File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Inbound Rules
Name
SQL Server I
Actions
Inbound Rules
New Rule...
Reporting Services Configuration Manager: \SQLEXPRESS
Microsoft SQL Server 2008 R2
Reporting Services Configuration Manager
New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 80

Example: 80, 443, 5000-5010

Configure a URL used to access the Report Se instance, or to specify additional parameters

Report Server Web Service Virtual Directory

Virtual Directory: ReportServer_SQL

Report Server Web Service Site identification

IP Address: All Assigned (Reco

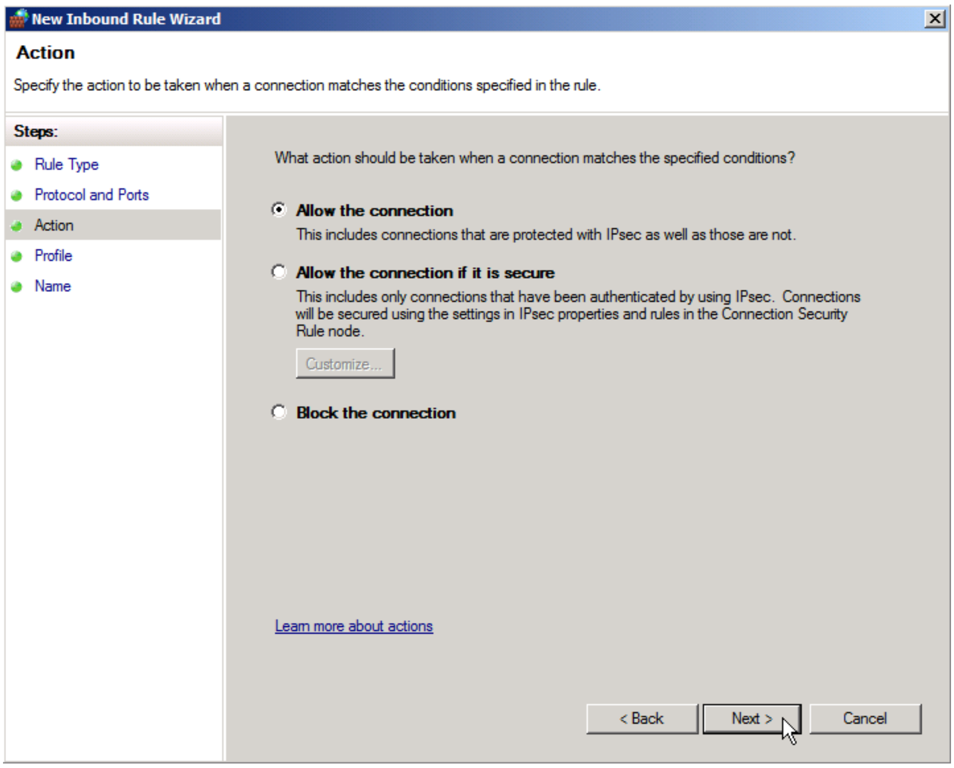
TCP Port: 80

SSL Certificate: (Not Selected)

SSL Port:

Report Server Web Service URLs

URLs: http:// :80



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

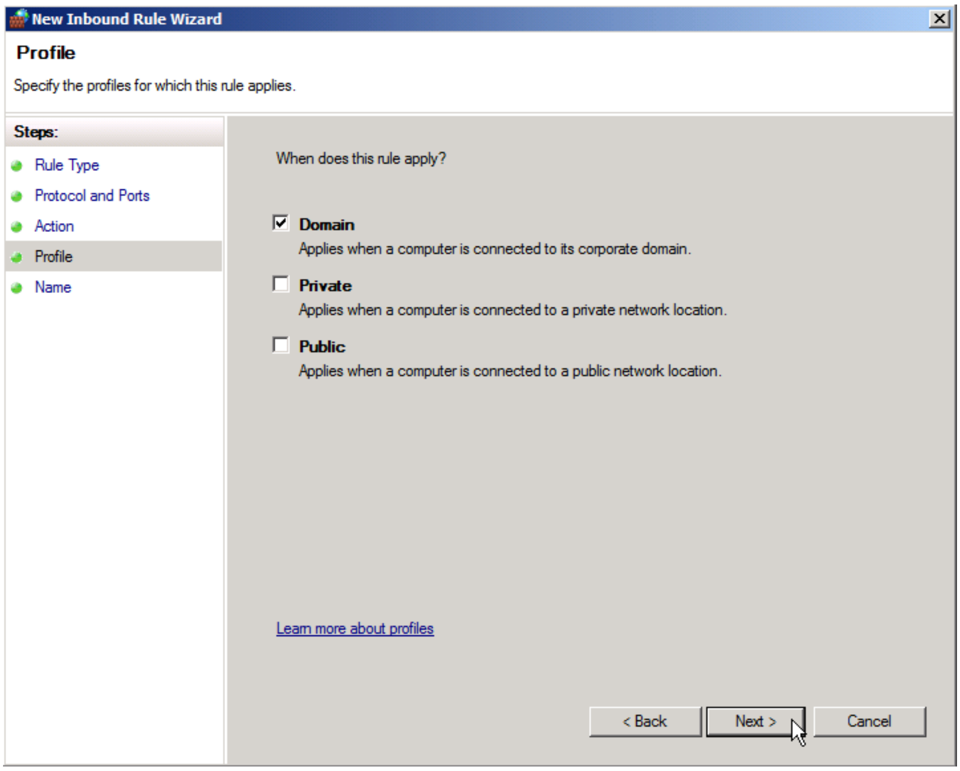
● Allow the connection

This includes connections that are protected with IPsec as well as those are not.

○ 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.

○ Block the connection



New Inbound Rule Wizard

**Profile**

Specify the profiles for which this rule applies.

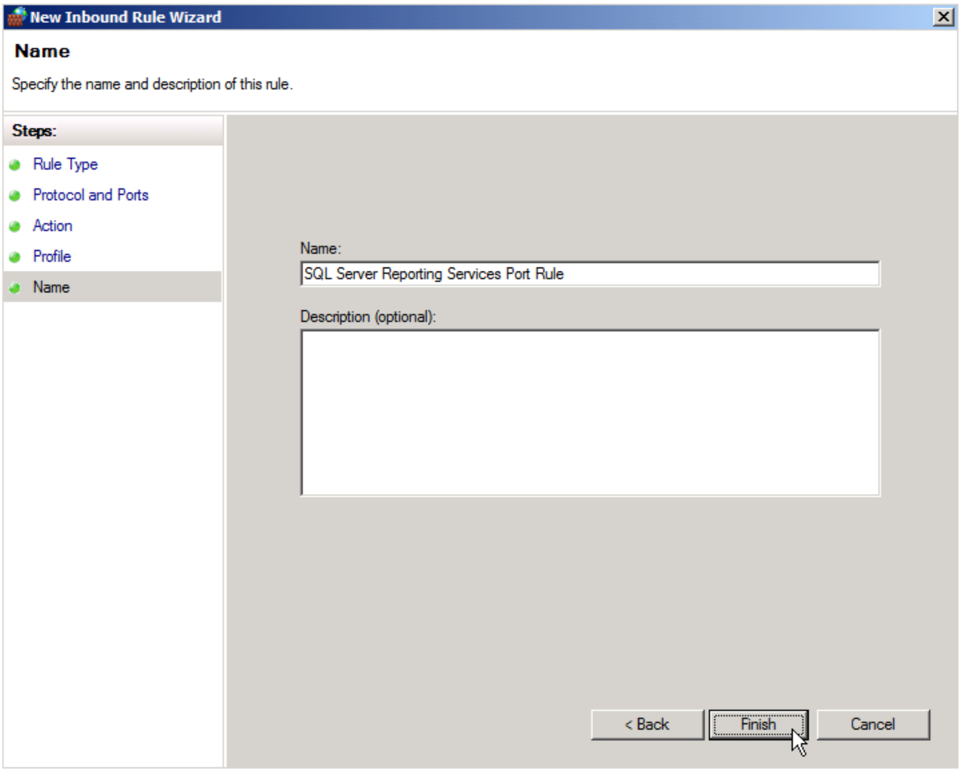
Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

□ **Private**
Applies when a computer is connected to a private network location.

□ **Public**
Applies when a computer is connected to a public network location.



New Inbound Rule Wizard

**Name**

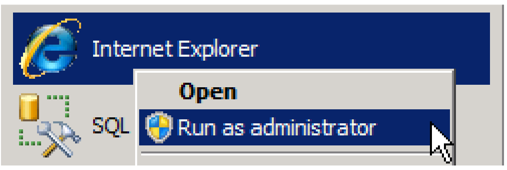
Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

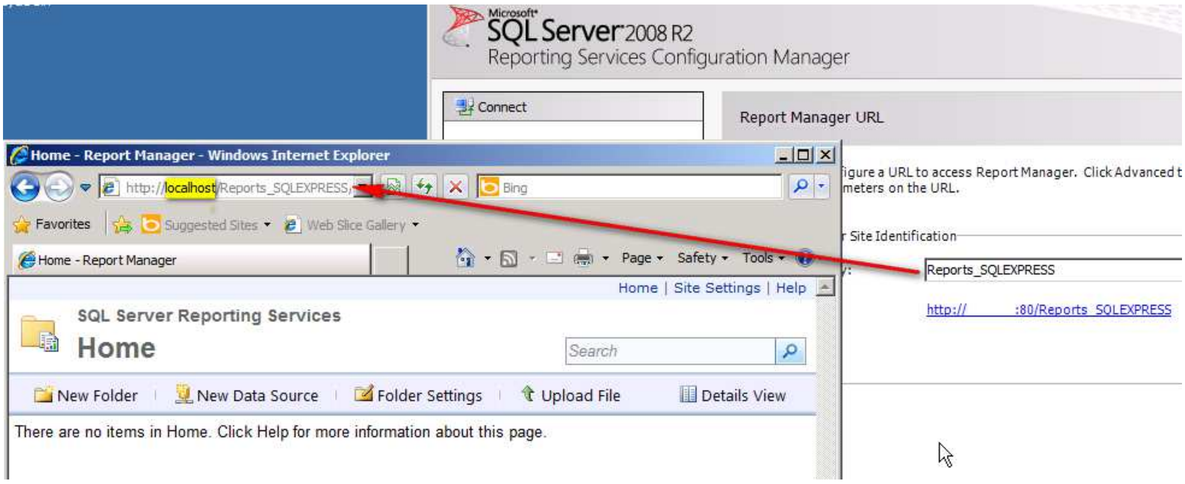
Name:
SQL Server Reporting Services Port Rule

Description (optional):

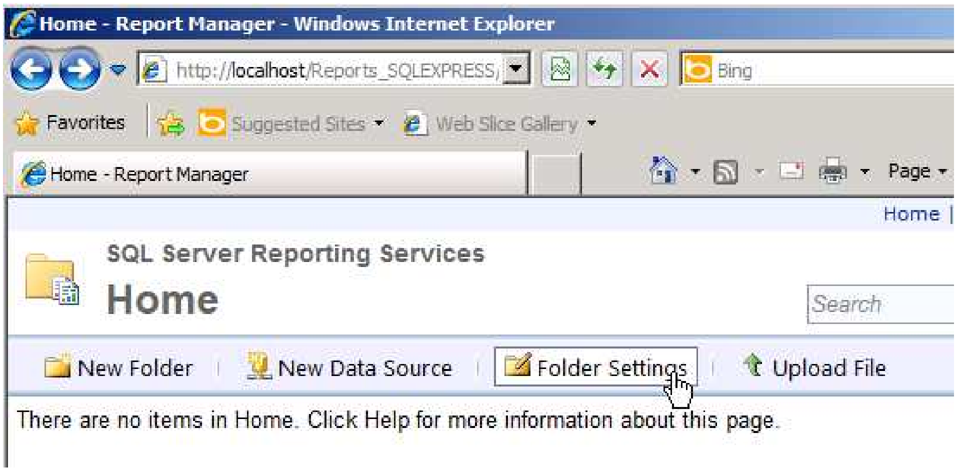
These steps show you how to give a user access to Reporting Services.



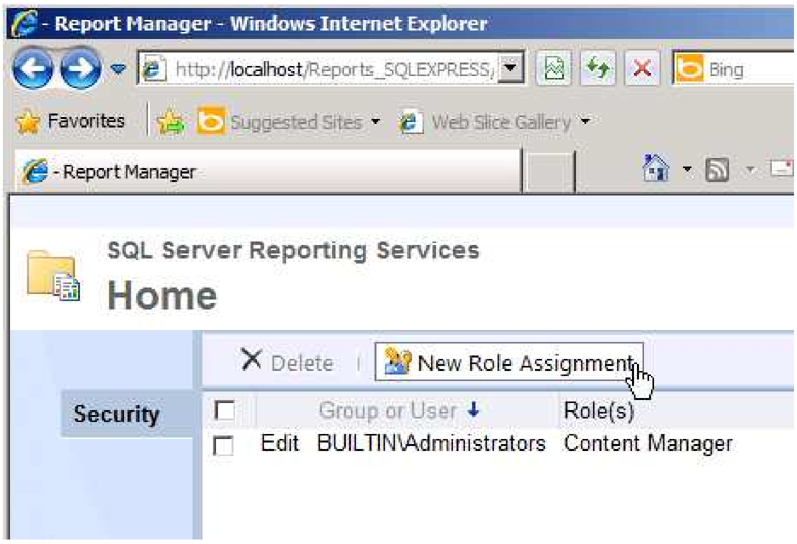
As below, make sure you use ***localhost*** and not the name of the SQL Server.


Microsoft SQL Server 2008 R2
Reporting Services Configuration Manager
Connect
Report Manager URL
Home - Report Manager - Windows Internet Explorer
http://localhost/Reports_SQLEXPRESS/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Home - Report Manager
Page
Safety
Tools
Home | Site Settings | Help
SQL Server Reporting Services
Home
Search
New Folder
New Data Source
Folder Settings
Upload File
Details View
igure a URL to access Report Manager. Click Advanced t
meters on the URL.
Site Identification
Reports_SQLEXPRESS
http:// :80/Reports_SQLEXPRESS

There are no items in Home. Click Help for more information about this page.

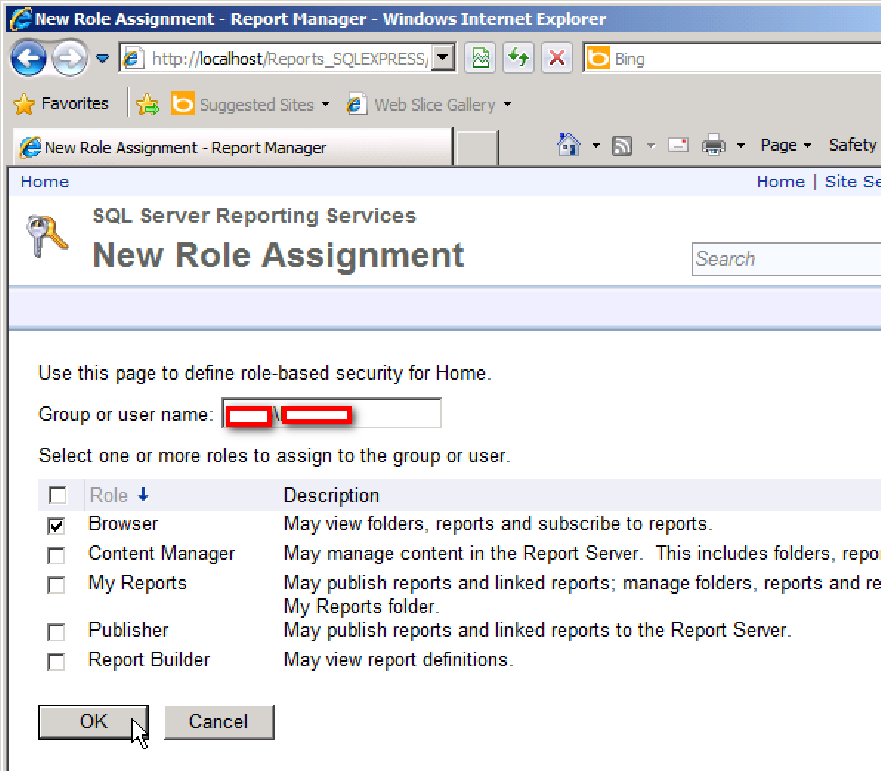


There are no items in Home. Click Help for more information about this page.


- Report Manager - Windows Internet Explorer
http://localhost/Reports_SQLEXPRESS/
Bing
Favorites
Suggested Sites
Web Slice Gallery
- Report Manager
SQL Server Reporting Services
Home
Delete
New Role Assignment
Security

| □ | Group or User ↓ | Role(s) |
|---|---|---|
| □ Edit | BUILTIN\Administrators | Content Manager |

Add the relevant windows user with the permissions they require.


New Role Assignment - Report Manager - Windows Internet Explorer
http://localhost/Reports_SQLEXPRESS/
Bing
Favorites
Suggested Sites
Web Slice Gallery
New Role Assignment - Report Manager
Page
Safety
Home
Home | Site Se

SQL Server Reporting Services

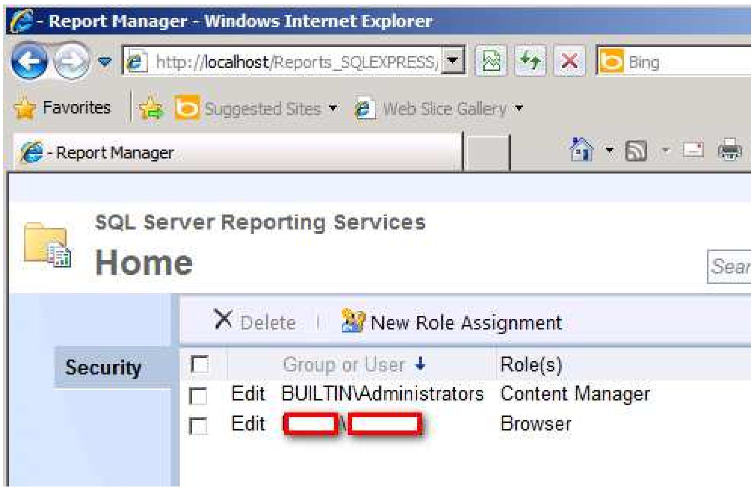
New Role Assignment

Use this page to define role-based security for Home.

Group or user name: [redacted]\[redacted]

Select one or more roles to assign to the group or user.

| □ | Role | Description |
|---|---|---|
| ☑ | Browser | May view folders, reports and subscribe to reports. |
| □ | Content Manager | May manage content in the Report Server.  This includes folders, repo |
| □ | My Reports | May publish reports and linked reports; manage folders, reports and re My Reports folder. |
| □ | Publisher | May publish reports and linked reports to the Report Server. |
| □ | Report Builder | May view report definitions. |

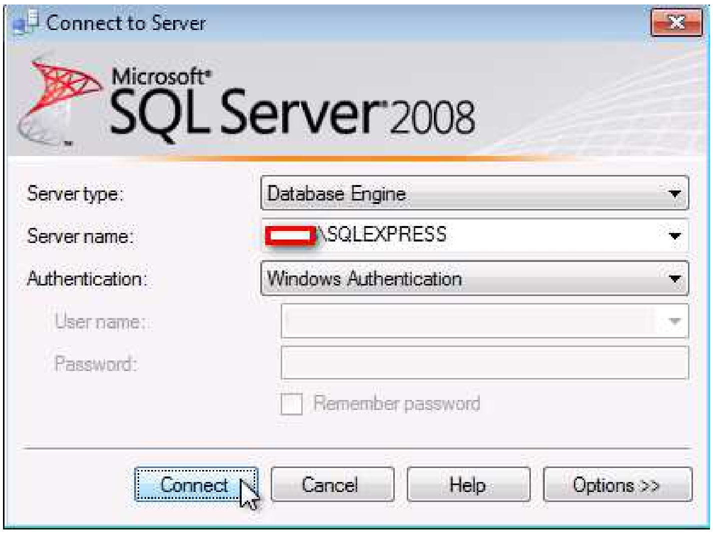

- Report Manager - Windows Internet Explorer
http://localhost/Reports_SQLEXPRESS/
Bing
Favorites
Suggested Sites
Web Slice Gallery
- Report Manager

SQL Server Reporting Services

Home

| □ | | Group or User | Role(s) |
|---|---|---|---|
| □ | Edit | BUILTIN\Administrators | Content Manager |
| □ | Edit | [redacted]\[redacted] | Browser |

Now test that you are able to connect from a remote computer.


Connect to Server

Microsoft® SQL Server 2008

Server type: Database Engine

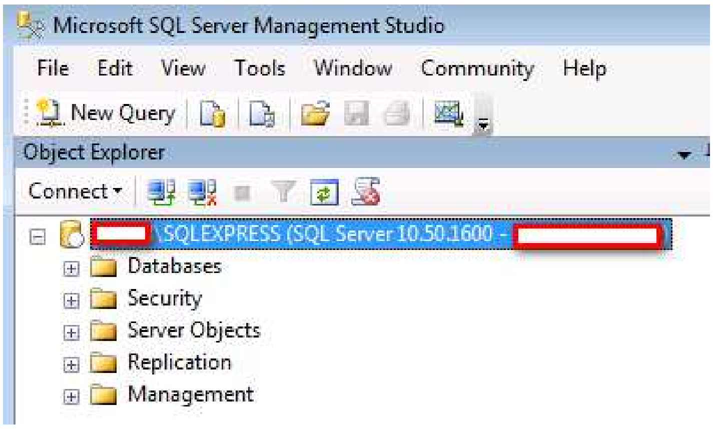
Server name: [redacted]\SQLEXPRESS

Authentication: Windows Authentication

User name:

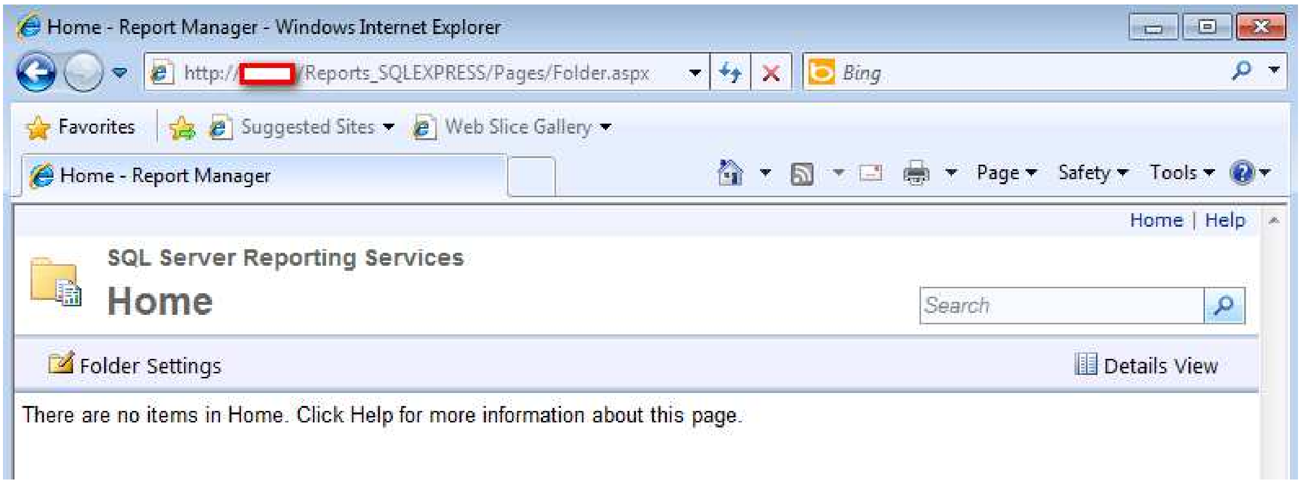
Password:

□ Remember password


Microsoft SQL Server Management Studio

[redacted]\SQLEXPRESS (SQL Server 10.50.1600 - [redacted]

Below shows a remote connection to Reporting Services. Above we used localhost when on the SQL Server, but remotely you should use the SQL Server name.


Home - Report Manager - Windows Internet Explorer

http://[redacted]/Reports_SQLEXPRESS/Pages/Folder.aspx

SQL Server Reporting Services

Home

There are no items in Home. Click Help for more information about this page.

## Enabling SQL authentication and sa user for database login

For security reasons, the SQL authentication method, and the database administrator **sa** user is disabled by default on newer SQL installations.

You have to manually enable them if you wish to use them.

We'll follow the instructions from this blog entry:

https://sudeeptaganguly.wordpress.com/2010/04/20/how-to-enable-sa-account-in-sql-server/

When you install the SQL Server using Windows Authentication mode, by default, the "**sa**" account is disabled. Sometimes, due to users/customers request, you may need to enable the **sa** account. You need to change the authentication mode for SQL server from *Windows Authentication Mode* to *SQL Server and Windows Authentication Mode* to use the **sa** account.

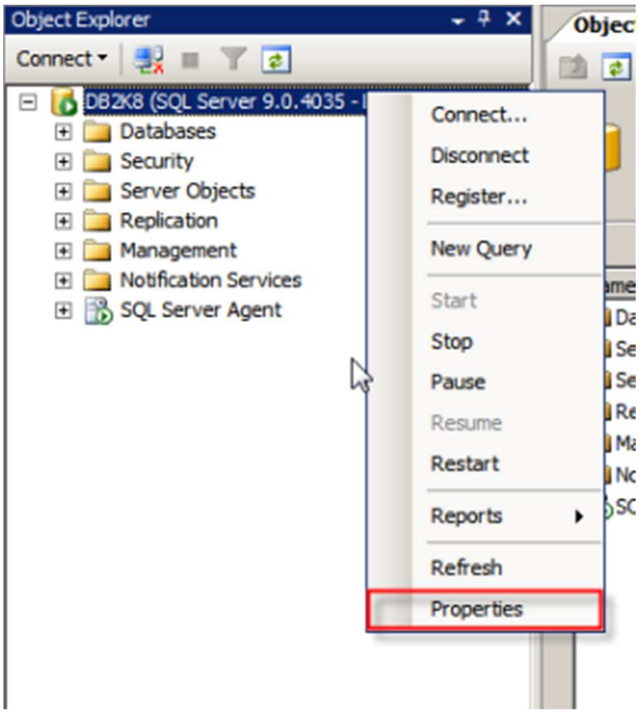
### To Change the Authentication Mode:

Follow the steps mentioned below to change the authentication mode from *Windows Authentication* to *SQL Server and Windows Authentication*.

You need to remember that, the **SQL Server service needs to restart to make this change effective**.

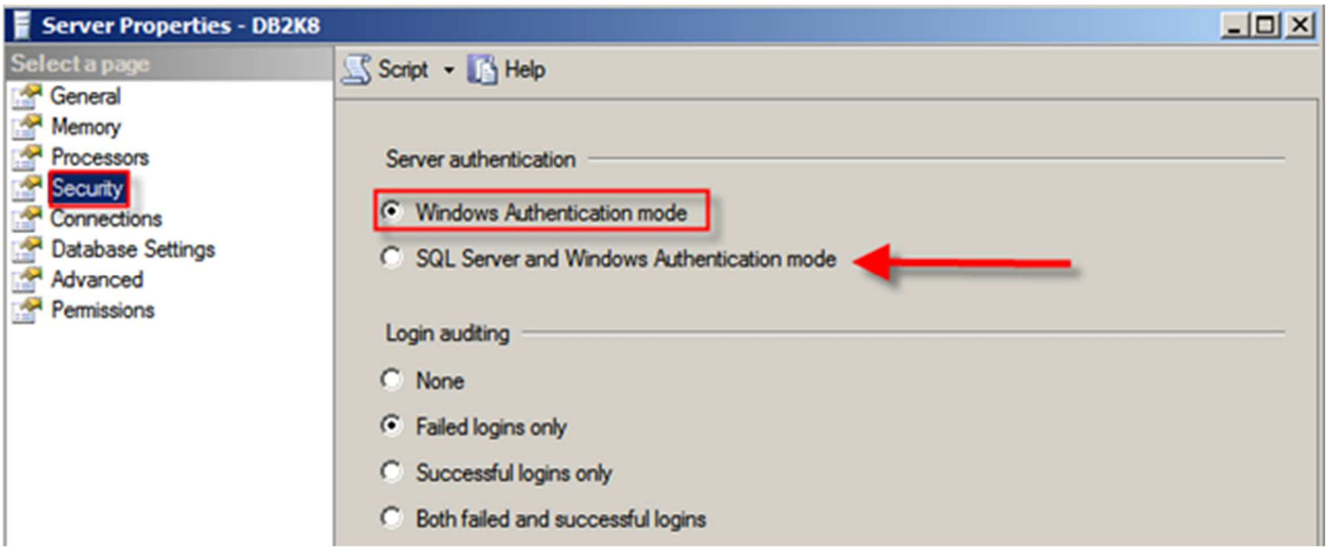
1. Login to the SQL server instance using SQL Server Management Studio.

Right-click on the database instance, and go to **Properties**.



2. On the Server Properties page, Click on **Security**.

Click on the radio button next to *SQL Server and Windows Authentication mode*, and click on OK to close the Server Properties page.



Server authentication

● Windows Authentication mode

○ SQL Server and Windows Authentication mode

Login auditing

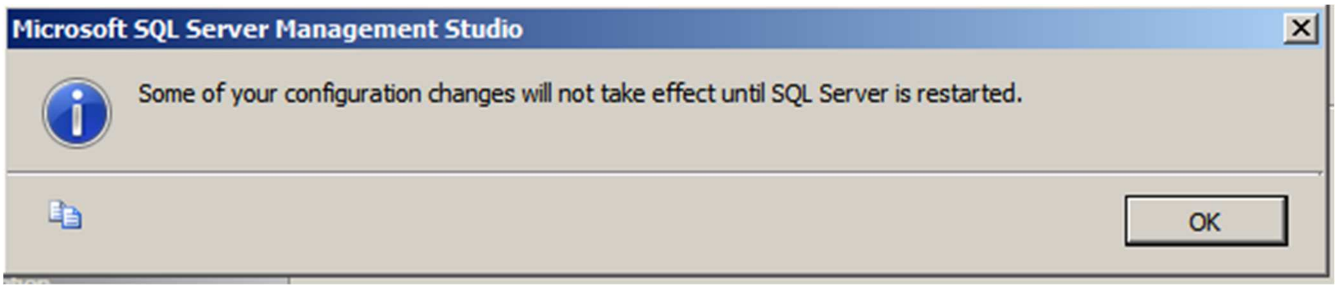
○ None

● Failed logins only

○ Successful logins only

○ Both failed and successful logins

3. Once you clicked on the Ok button, we will get the following screen:



Some of your configuration changes will not take effect until SQL Server is restarted.

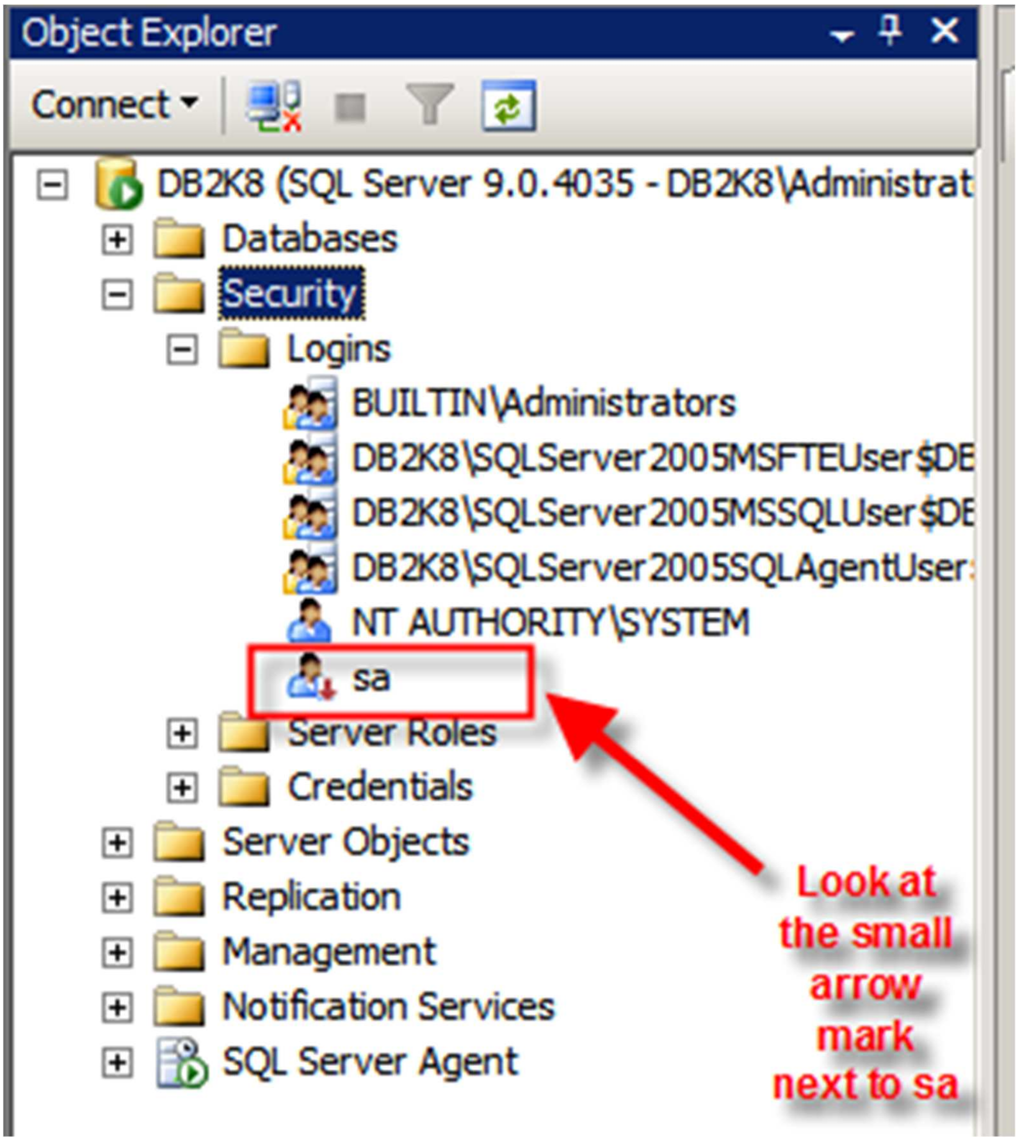
As discussed earlier, we need to restart the SQL Server service to make this change effective.

After restarting the SQL Server, the authentication mode will be changed to *SQL Server and Windows Authentication mode*.

**Enable the sa Login:**

1. Connect to the SQL Server instance using SSMS and go to **Security**. Expand Security, go to **Logins**.

2.  You can see the **sa** account is disabled when you install SQL Server using Windows Authentication mode.

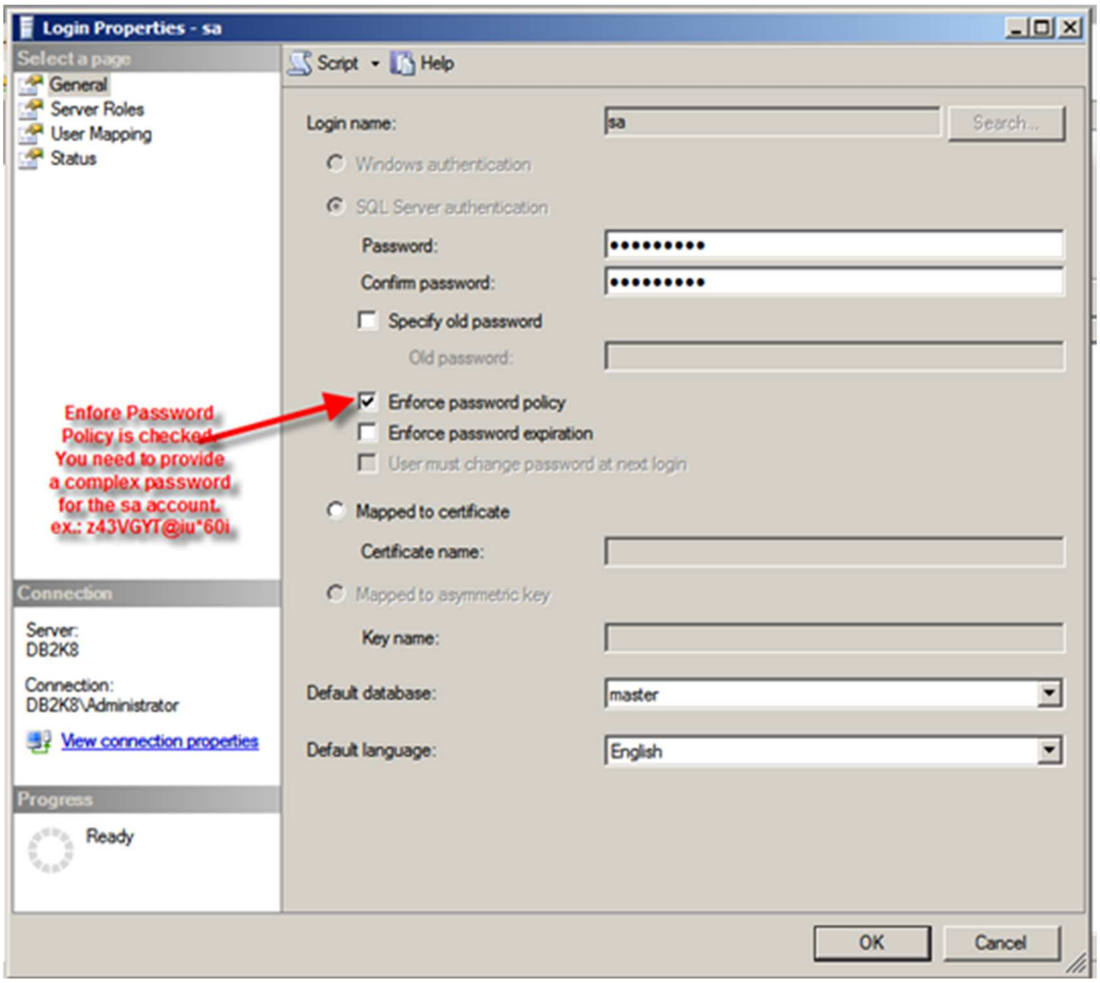


Look at the small arrow mark next to sa

3. Right-click on the **sa** account and go to **Login Properties**.

Specify a complex password for the sa account.

By default, the *Enforce password policy* is checked. (if you don’t want to provide a complex password for the sa account, you can uncheck this option. However, this is **not recommended**.)



Enfore Password Policy is checked
You need to provide a complex password for the sa account.
ex.: z43VGYT@iu*60i

Login name: sa

○ Windows authentication

● SQL Server authentication

Password: ••••••••••

Confirm password: ••••••••••

□ Specify old password

Old password:

☑ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

Certificate name:

○ Mapped to asymmetric key

Key name:

Default database: master

Default language: English

Server:
DB2K8

Connection:
DB2K8\Administrator

View connection properties

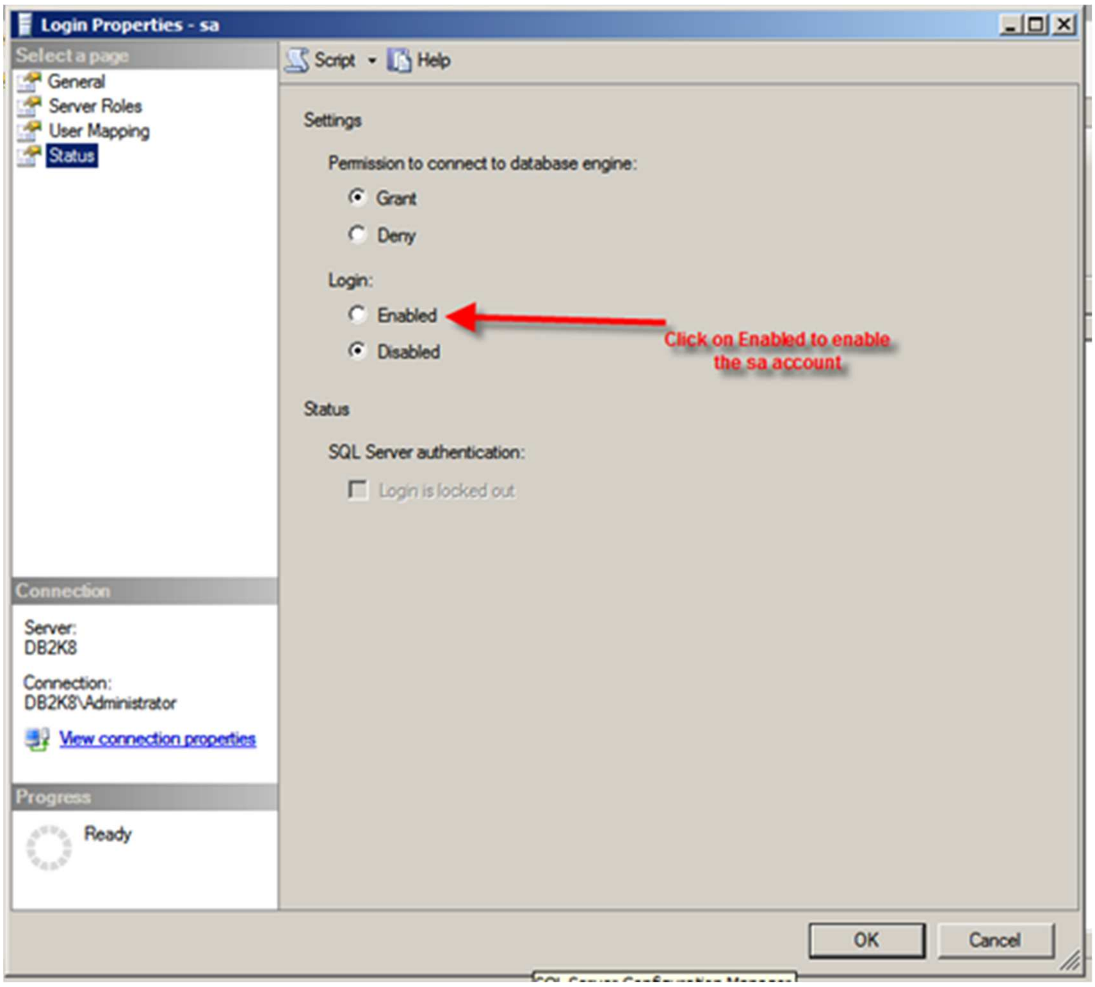
Ready

4. Click on the **Status** page.

By default, the sa account will be disabled.

Click on the **Enabled** button to enable the sa account.

Click on **Ok** to close the sa **Login Properties**.



Settings

Permission to connect to database engine:

● Grant

○ Deny

Login:

○ Enabled

● Disabled

Click on Enabled to enable the sa account

Status

SQL Server authentication:

□ Login is locked out

Server:
DB2K8

Connection:
DB2K8\Administrator

View connection properties

Thus, sa account is enabled and you will be able to login to the SQL instance using the sa account.

If you want to use a script to enable the **sa** account, you can use the script mentioned below:

```
1: USE [master]
2: GO
3: ALTER LOGIN [sa] WITH PASSWORD=N'z43VGYT@Iu*60i'
4: GO
5: ALTER LOGIN [sa] ENABLE
6: GO
```

## Notes for SQL Server 2012 and later versions

**SQL Server 2012 only**

The configuration process for SQL Server 2012 is the same as with the 2008R2 version, except that the **SQL Server Configuration Manager** is not added to the Start menu (in the 2014 version, it's added again).

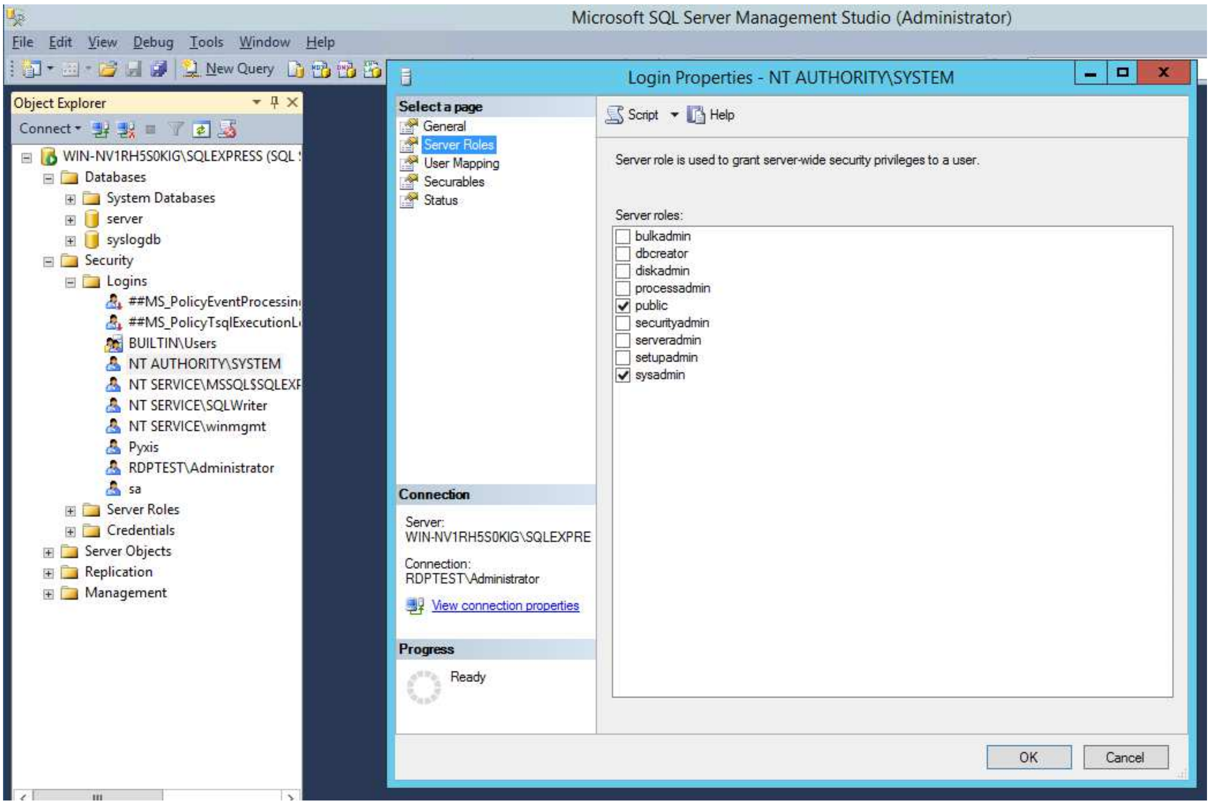
To run it, type **SQLServerManager11.msc** and proceed with the configuration.

**SQL Server 2012 and later**

Microsoft has further hardened the permissions of SQL Server, hence the SYSTEM user has less rights in a default configuration. This can result in the CPS service unable to start automatically.

More information on this link: [https://social.msdn.microsoft.com/Forums/sqlserver/en-US/94ff47eb-a0e0-4441-9799-b56b5ce3712b/sql-server-2012-ntauthoritysystem-sysadmin-is-not-checked-by-default](https://social.msdn.microsoft.com/Forums/sqlserver/en-US/94ff47eb-a0e0-4441-9799-b56b5ce3712b/sql-server-2012-ntauthoritysystem-sysadmin-is-not-checked-by-default)

As a fix, modify the user's rights that run the CPS service (by default the SYSTEM user) to include the **sysadmin** right:



Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

Server:
WIN-NV1RH5S0KIG\SQLEXPRE

Connection:
RDPTEST\Administrator

1. Open the **SQL Server Management Studio** and login as an SQL administrator.

2. Open the **Security/Logins** branch.

3. Find the user that runs the CPS service. By default this is the NT AUTHORITY\SYSTEM user.

4. Open the properties, go to the **Server Roles** page, and click the **sysadmin** privilege, then press OK.

## CPS Installation with MS SQL database

Upon installing CPS, at the Database Settings part, choose the **External RDBMS** option and specify the following:

**RDBMS Name:** SQL_SERVER

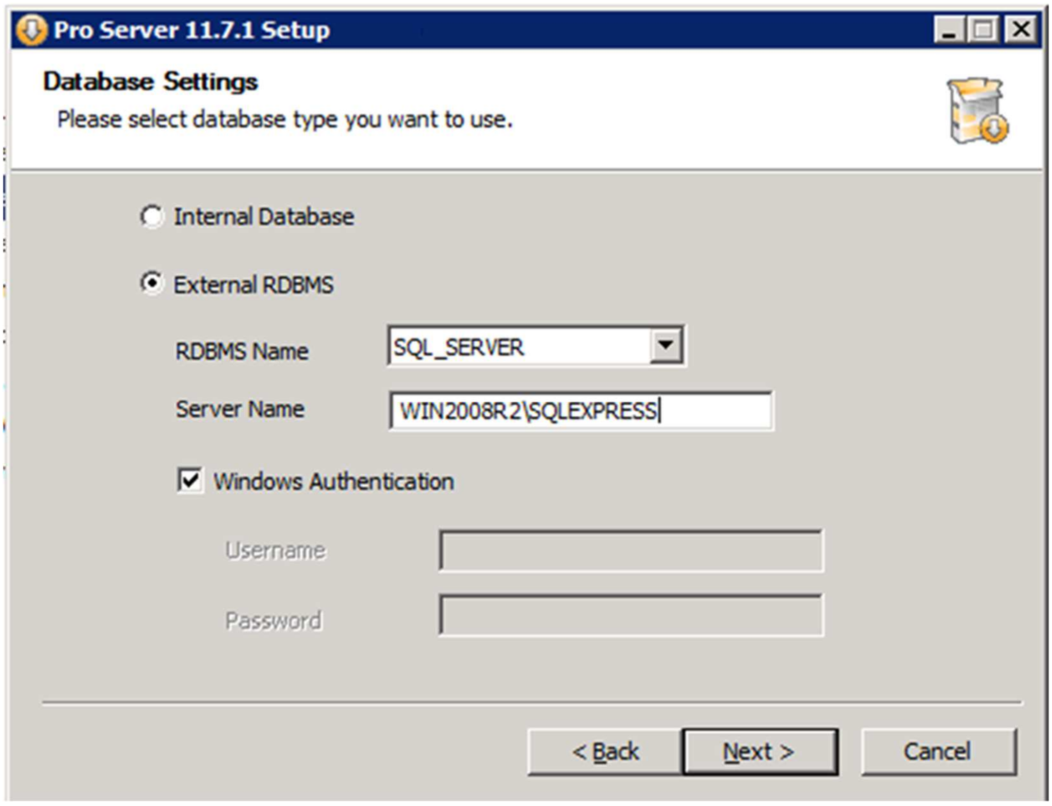
**Server Name:** [SERVER_NAME]\[INSTANCE_NAME]

*Important:* if you're not using the default DB instance but a named instance, you must specify it, otherwise the connection will fail!

In our test machine, the SERVER_NAME is Win2008R2 and the INSTANCE_NAME is SQLEXPRESS as we've used the Express version.

**Authentication:** Windows or SQL. This setting depends on your installed SQL server; by default newer versions are using the Windows authentication method as default.

*Note:* if you use SQL authentication, the ODBC connection's user and password will be saved (encrypted) in the CPS configuration file server.xml.



Pro Server 11.7.1 Setup

Database Settings

Please select database type you want to use.

○ Internal Database

● External RDBMS

RDBMS Name: SQL_SERVER

Server Name: WIN2008R2\SQLEXPRESS

☑ Windows Authentication

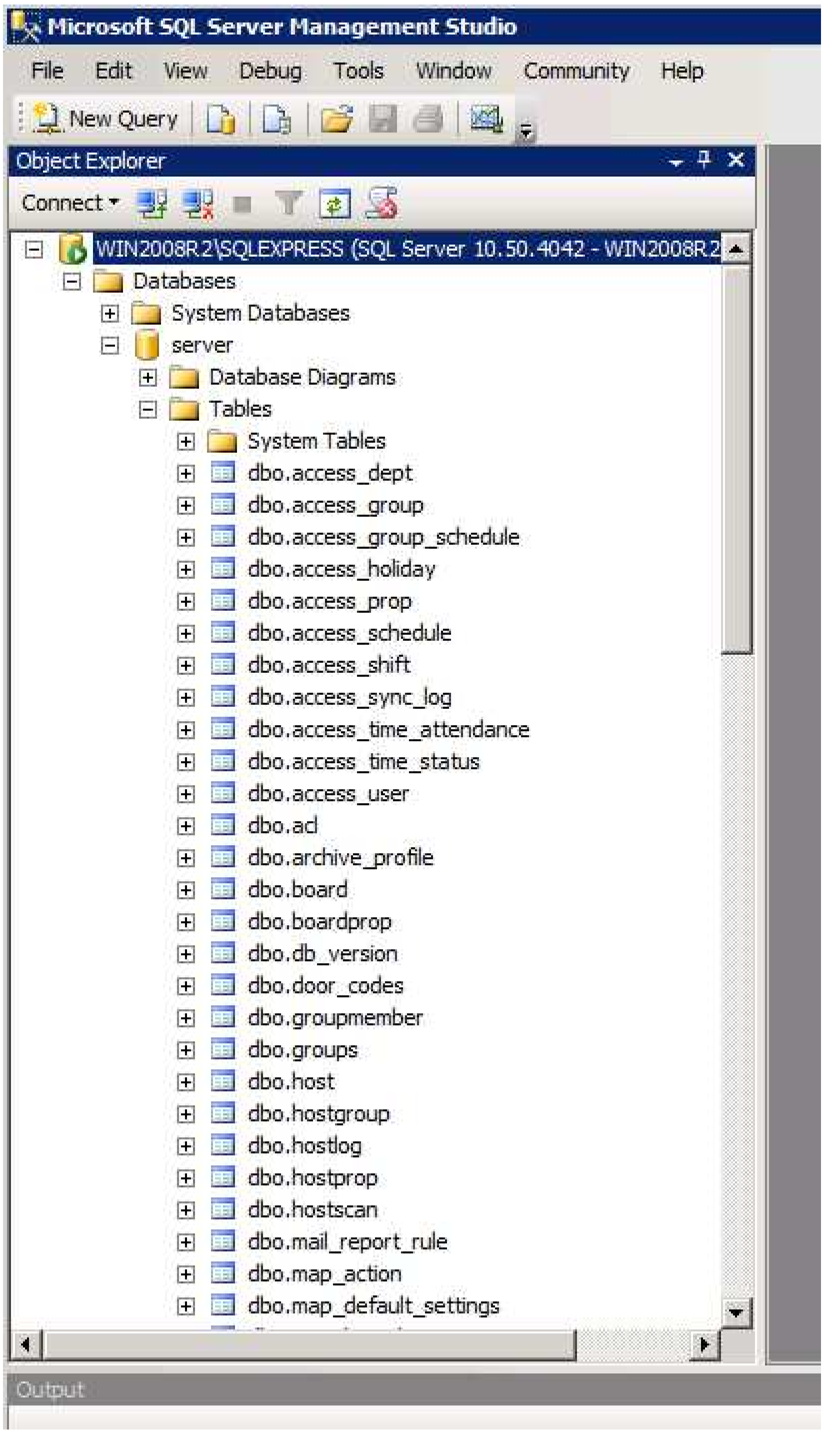
Username:

Password:

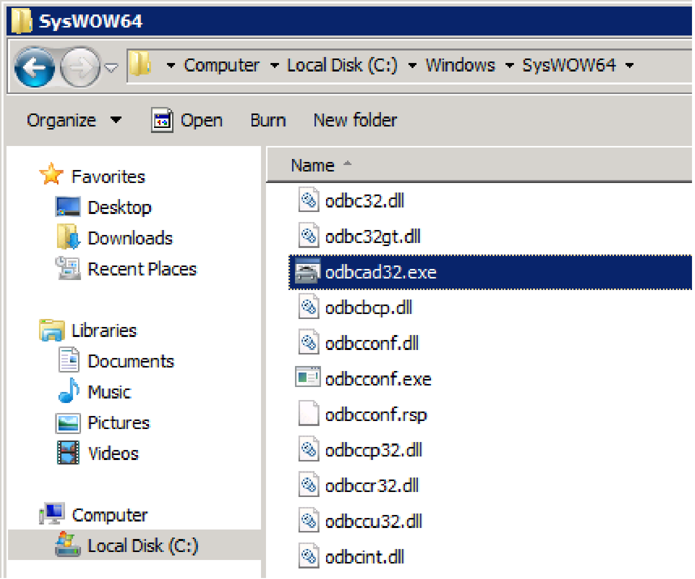
Click Next and allow CPS installation to proceed as normal.

Consult the CPS Installation Manual if you need further help.

You can verify that the CPS database has been created in SQL Management Studio, the CPS database is named "server":


Microsoft SQL Server Management Studio
File
Edit
View
Debug
Tools
Window
Community
Help
New Query
Object Explorer
Connect
WIN2008R2\SQLEXPRESS (SQL Server 10.50.4042 - WIN2008R2
Databases
System Databases
server
Database Diagrams
Tables
System Tables
dbo.access_dept
dbo.access_group
dbo.access_group_schedule
dbo.access_holiday
dbo.access_prop
dbo.access_schedule
dbo.access_shift
dbo.access_sync_log
dbo.access_time_attendance
dbo.access_time_status
dbo.access_user
dbo.acl
dbo.archive_profile
dbo.board
dbo.boardprop
dbo.db_version
dbo.door_codes
dbo.groupmember
dbo.groups
dbo.host
dbo.hostgroup
dbo.hostlog
dbo.hostprop
dbo.hostscan
dbo.mail_report_rule
dbo.map_action
dbo.map_default_settings
Output

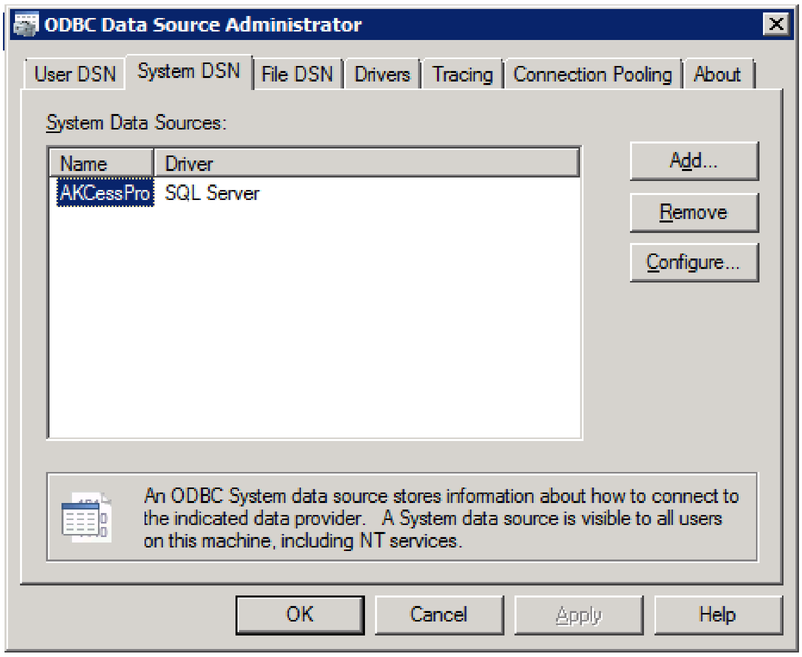
The CPS installer creates a 32-bit ODBC system connector. You can verify that this has been created using the 32-bit ODBC manager: start the **ODBC Data Sources (32-bit)** from **Administrative Tools**, or find the program manually:



odbc32.dll
odbc32gt.dll
odbcad32.exe
odbcbcp.dll
odbcconf.dll
odbcconf.exe
odbcconf.rsp
odbccp32.dll
odbccr32.dll
odbccu32.dll
odbcint.dll

On a 64-bit OS, start odbcad32.exe from **C:\Windows\SysWOW64**; the file in the System32 directory is the 64-bit version, which can’t show the 32-bit connectors on Windows Server 2008 and R2.

*Note:* On Windows Server 2012 and up, you will be able to see the data source but can’t modify it using the 64-bit ODBC manager.



System Data Sources:

| Name | Driver |
|---|---|
| AKCessPro | SQL Server |

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

The data source will be added as a System DSN

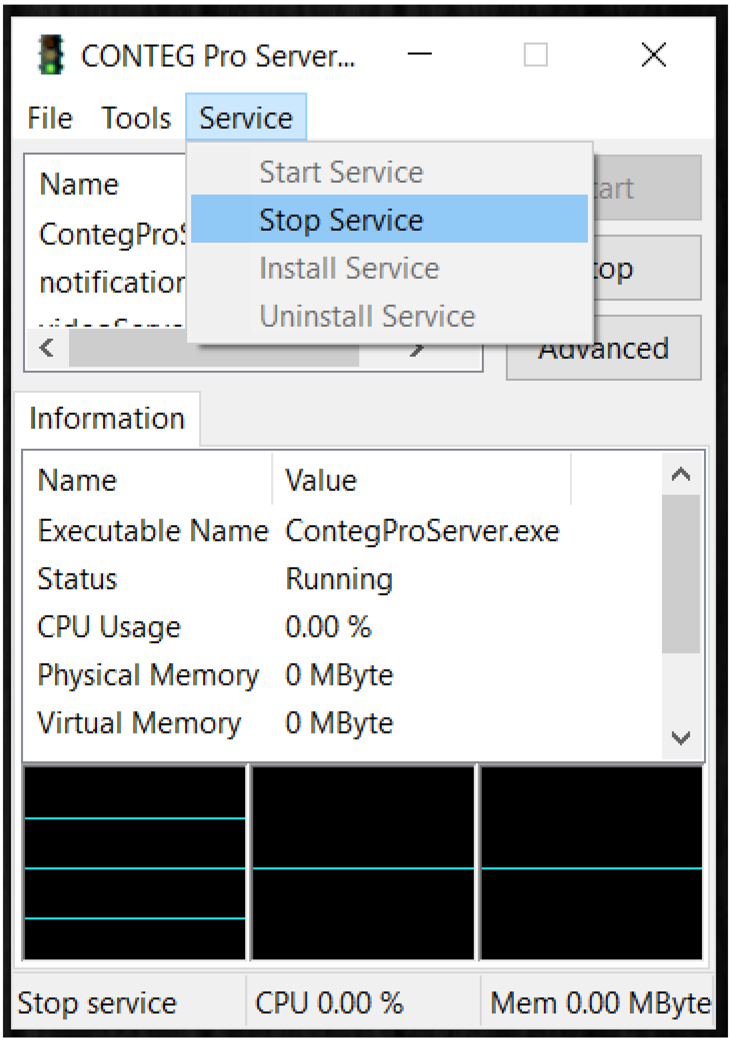
## Backup and restore of the CPS database with MS SQL Server

CPS provides the built-in backup/restore function only with the Internal Database option.

If you choose external DB then you'll have to use that software's backup/restore functions.

Below we'll cover the instructions for MS SQL (manual method only).

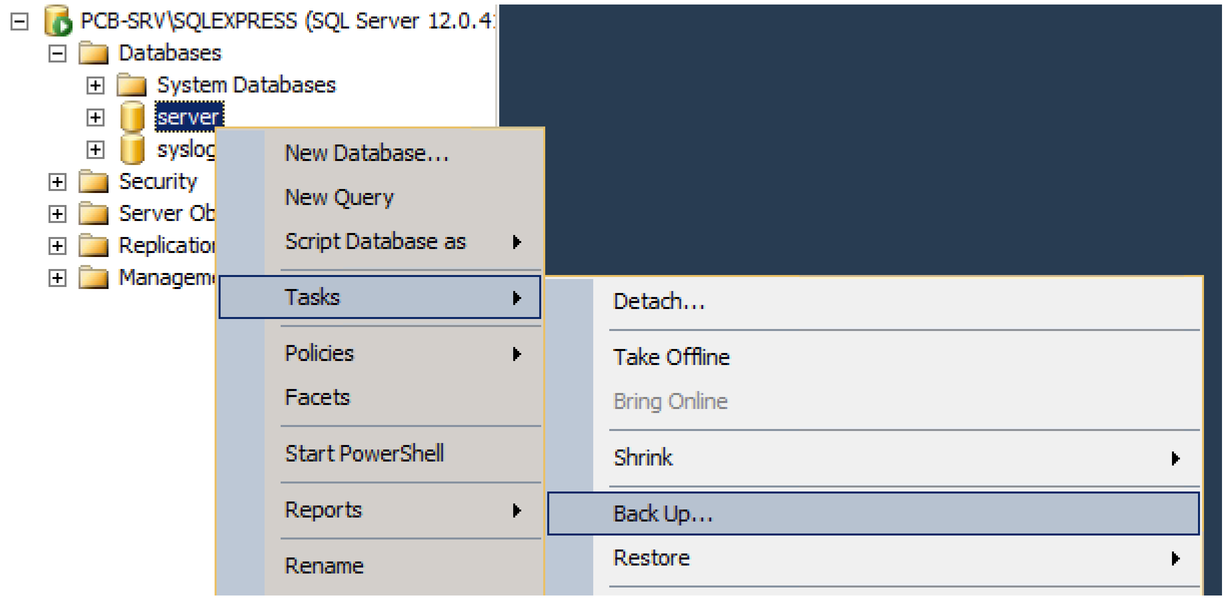
### Backing up



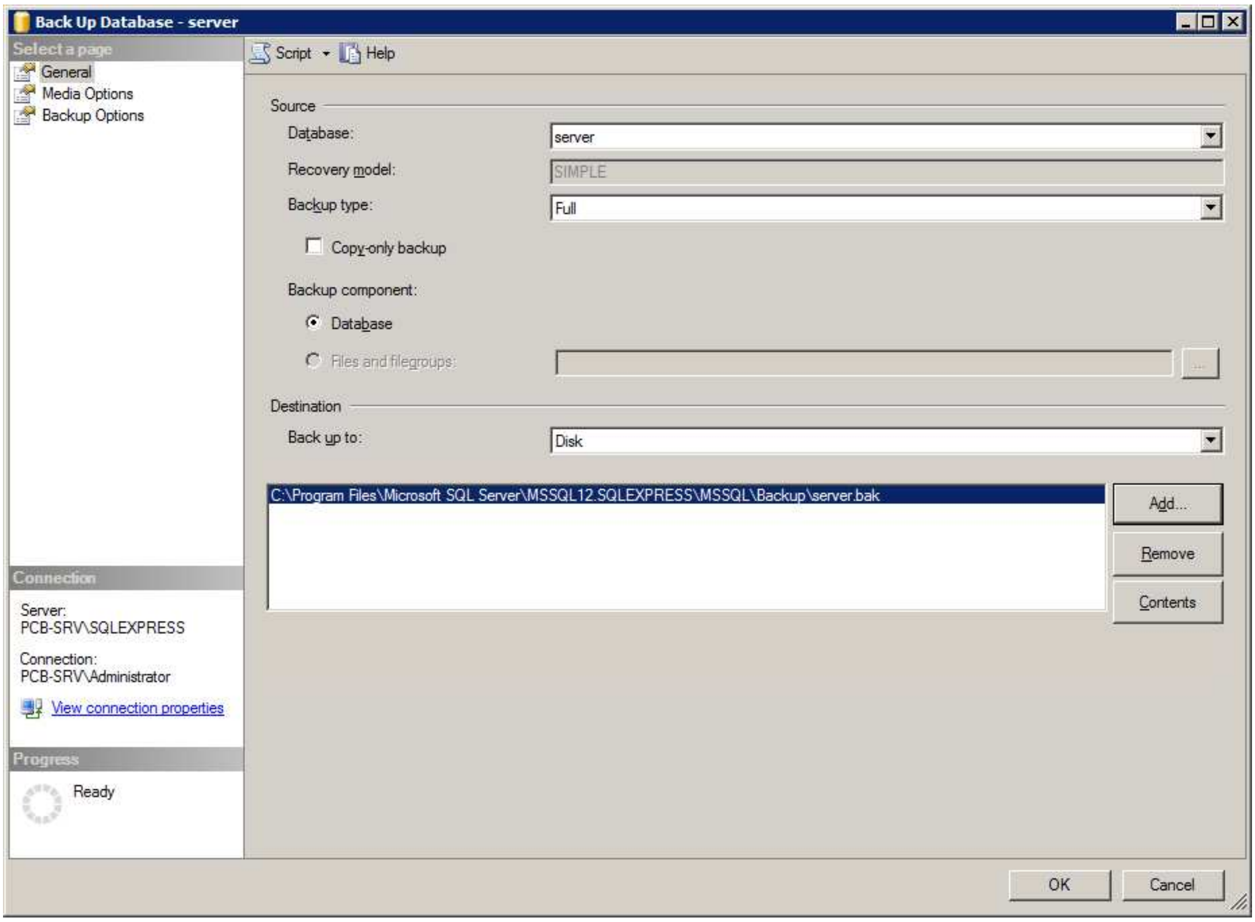
| Name | Value |
|---|---|
| Executable Name | ContegProServer.exe |
| Status | Running |
| CPU Usage | 0.00 % |
| Physical Memory | 0 MByte |
| Virtual Memory | 0 MByte |

To get a consistent state of the backup, it's recommended to first stop the CPS services using the **CONTEG Pro Server Manager**.

Next, start the **SQL Management Studio** and connect to the DB instance which stores the CPS databases (server and syslog).



Choose the server DB from the list, and select **Tasks / Back Up…**


Back Up Database - server

Select a page: General, Media Options, Backup Options

Script · Help

Source

Database: server

Recovery model: SIMPLE

Backup type: Full

☐ Copy-only backup

Backup component:

● Database

○ Files and filegroups:

Destination

Back up to: Disk

C:\Program Files\Microsoft SQL Server\MSSQL12.SQLEXPRESS\MSSQL\Backup\server.bak

Add... · Remove · Contents

Connection

Server:
PCB-SRV\SQLEXPRESS

Connection:
PCB-SRV\Administrator

View connection properties

Progress

Ready

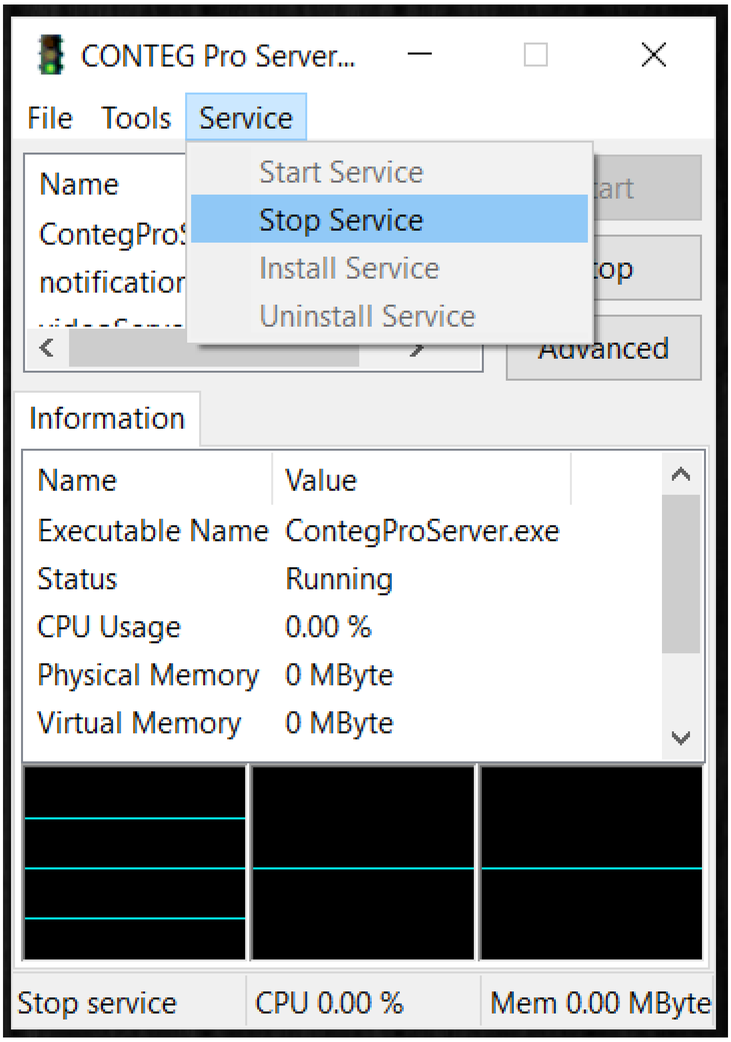
OK · Cancel

You could modify the backup file’s target, by default it goes to the SQL Server’s Backup directory.

Repeat the same process for the **syslog** DB.

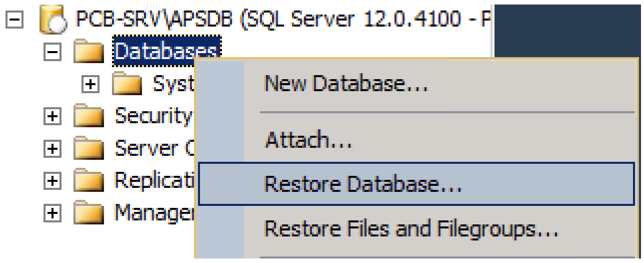
## Restoring

Prior to restoring you need to first stop the CPS services using the CPS Server Manager:

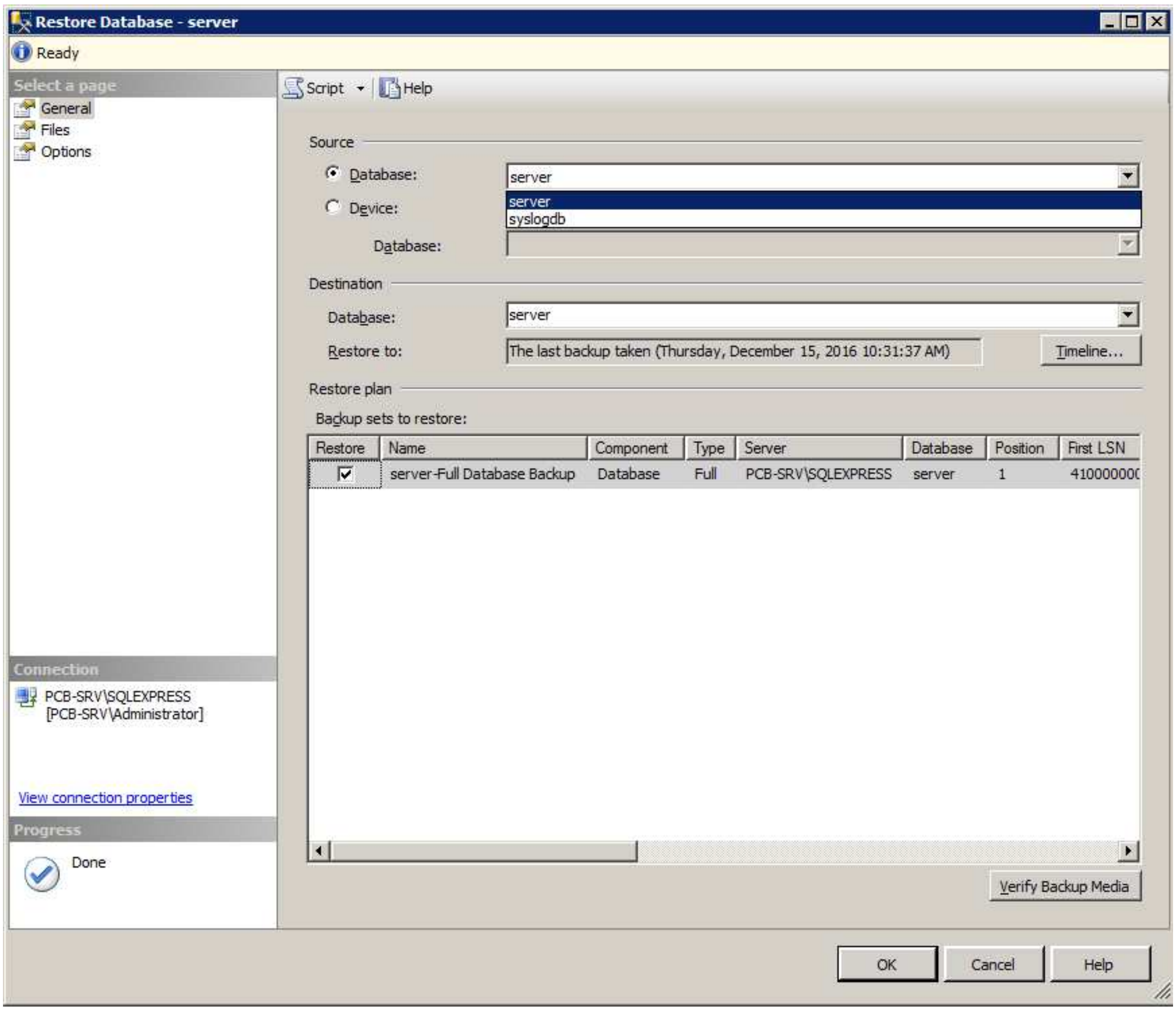


| Name | Value |
|---|---|
| Executable Name | ContegProServer.exe |
| Status | Running |
| CPU Usage | 0.00 % |
| Physical Memory | 0 MByte |
| Virtual Memory | 0 MByte |

Start the **SQL Management Studio** and connect to the DB instance which stores the CPS databases (server and syslog).



Right click on the **Databases** folder tree and select **Restore Database...**



Source

○ Database: server
server
syslogdb

○ Device:

Database:

Destination

Database: server

Restore to: The last backup taken (Thursday, December 15, 2016 10:31:37 AM)

Restore plan

Backup sets to restore:

| Restore | Name | Component | Type | Server | Database | Position | First LSN |
|---|---|---|---|---|---|---|---|
| ☑ | server-Full Database Backup | Database | Full | PCB-SRV\SQLEXPRESS | server | 1 | 41000000C |

Connection

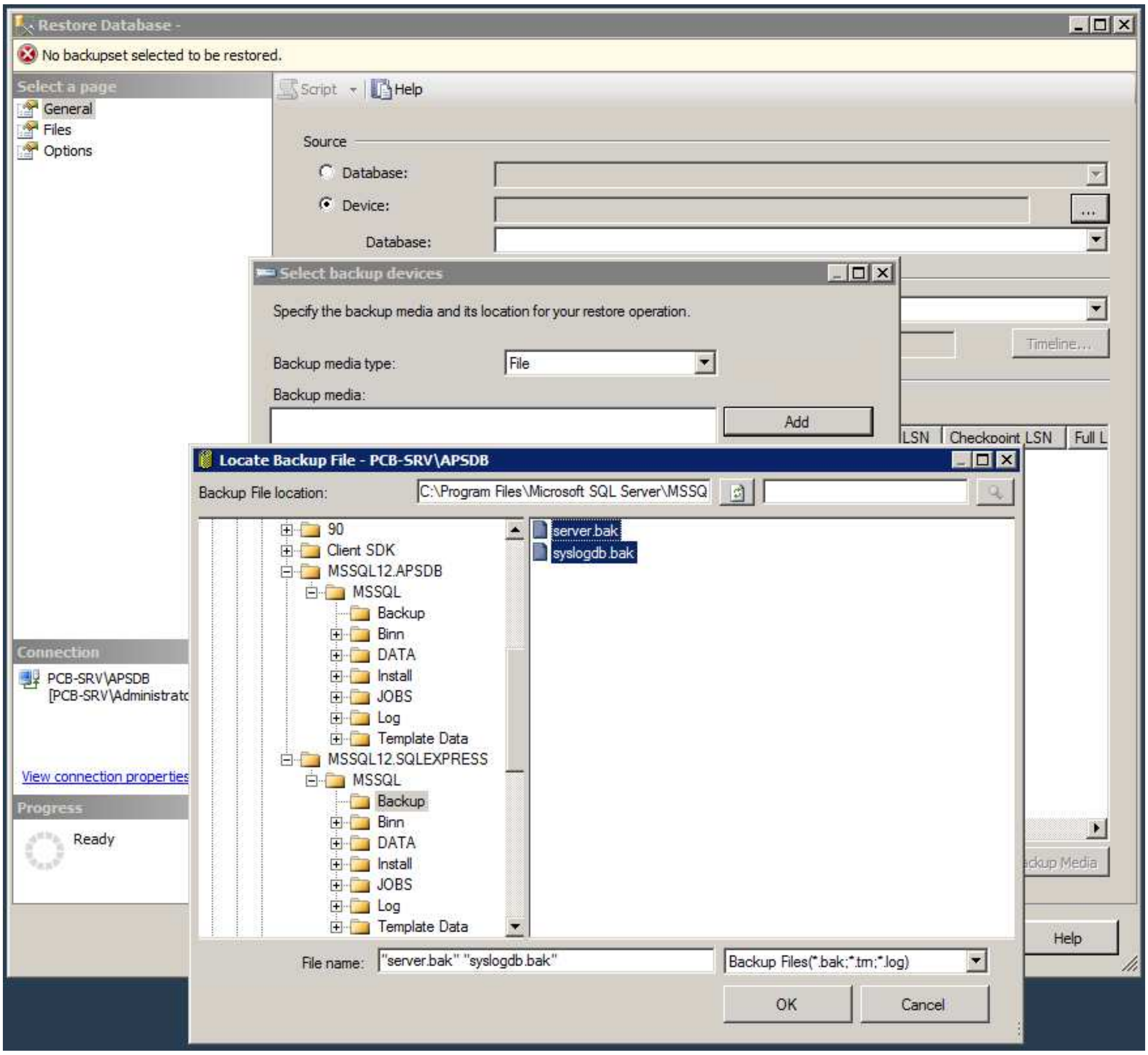
PCB-SRV\SQLEXPRESS
[PCB-SRV\Administrator]

View connection properties

Progress

Done

If you’ve made a backup before, you can directly select it from the list.



No backupset selected to be restored.

PCB-SRV\APSDB
[PCB-SRV\Administrato

Specify the backup media and its location for your restore operation.

Backup media type: File

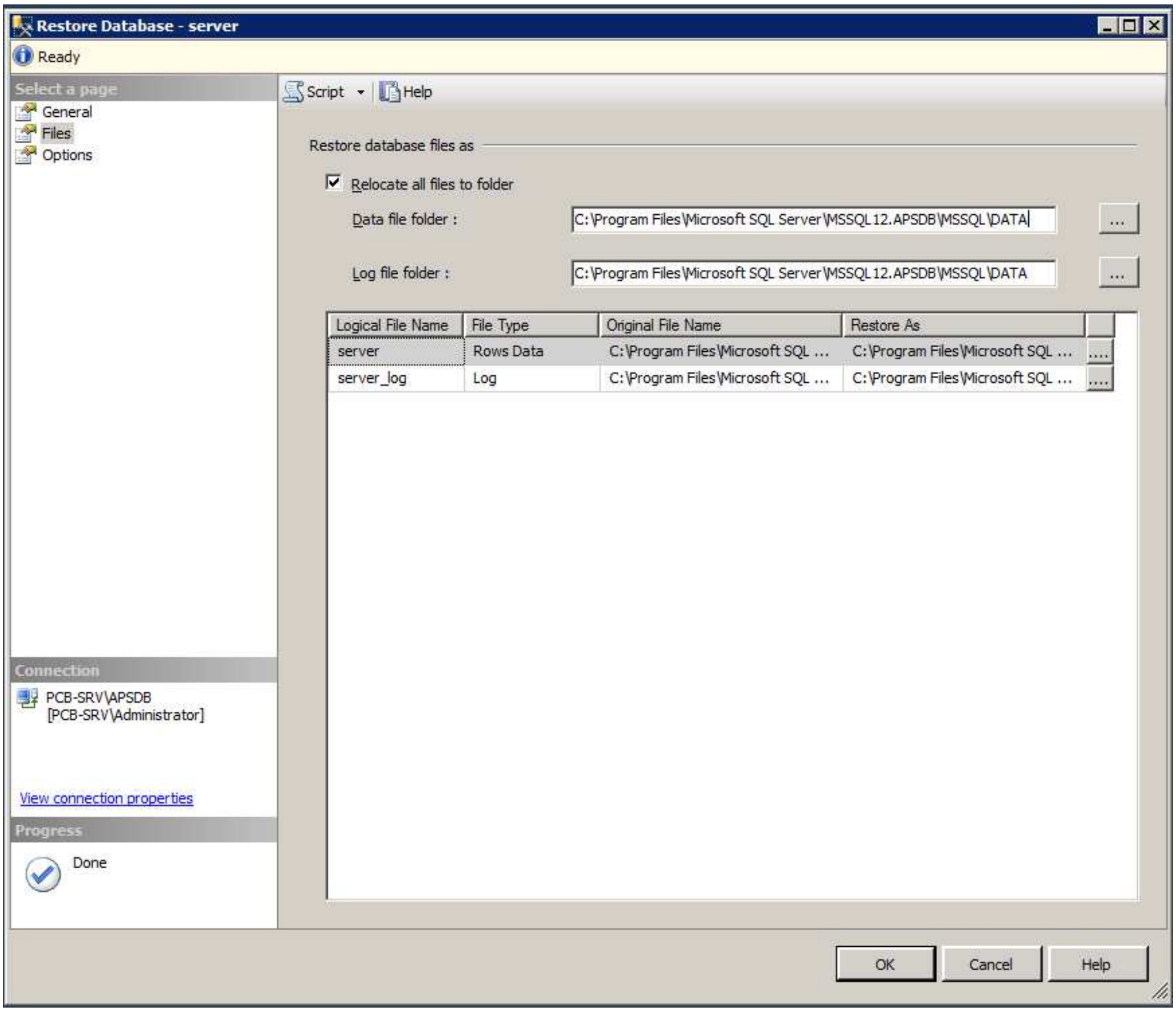
Backup media:

Backup File location: C:\Program Files\Microsoft SQL Server\MSSQ

File name: "server.bak" "syslogdb.bak"

Backup Files(*.bak;*.tm;*.log)

If the server has been reinstalled and there's no backup history, you'll need to locate the backup files manually.



Restore database files as

☑ Relocate all files to folder

Data file folder : C:\Program Files\Microsoft SQL Server\MSSQL12.APSDB\MSSQL\DATA

Log file folder : C:\Program Files\Microsoft SQL Server\MSSQL12.APSDB\MSSQL\DATA

| Logical File Name | File Type | Original File Name | Restore As |
|---|---|---|---|
| server | Rows Data | C:\Program Files\Microsoft SQL ... | C:\Program Files\Microsoft SQL ... |
| server_log | Log | C:\Program Files\Microsoft SQL ... | C:\Program Files\Microsoft SQL ... |

PCB-SRV\APSDB
[PCB-SRV\Administrator]

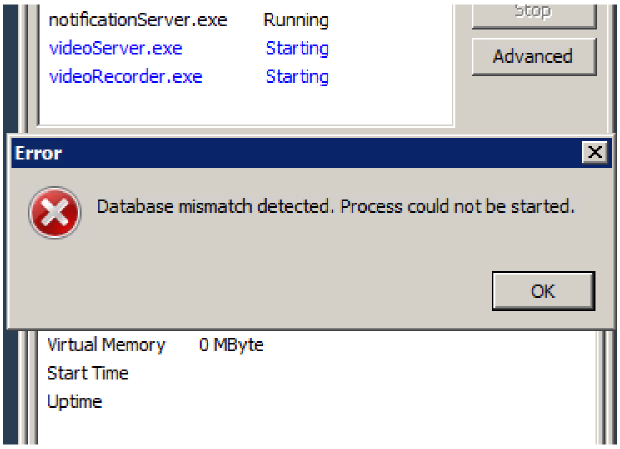
Done

Optionally you can relocate the DB files to another directory during the restore, under the **Files** page.

If you’re just doing a normal restore then this is not needed.

After the DBs have been restored, you can start the CPS service again.

***Important note:*** Renaming the DB instance and the server is not supported! If you attempt to do so, you’ll get the following error and CPS cannot start:



| | |
|---|---|
| notificationServer.exe | Running |
| videoServer.exe | Starting |
| videoRecorder.exe | Starting |

Database mismatch detected. Process could not be started.

Virtual Memory 0 MByte
Start Time
Uptime

If you need to change the server’s name or the instance name, you’ll need to:

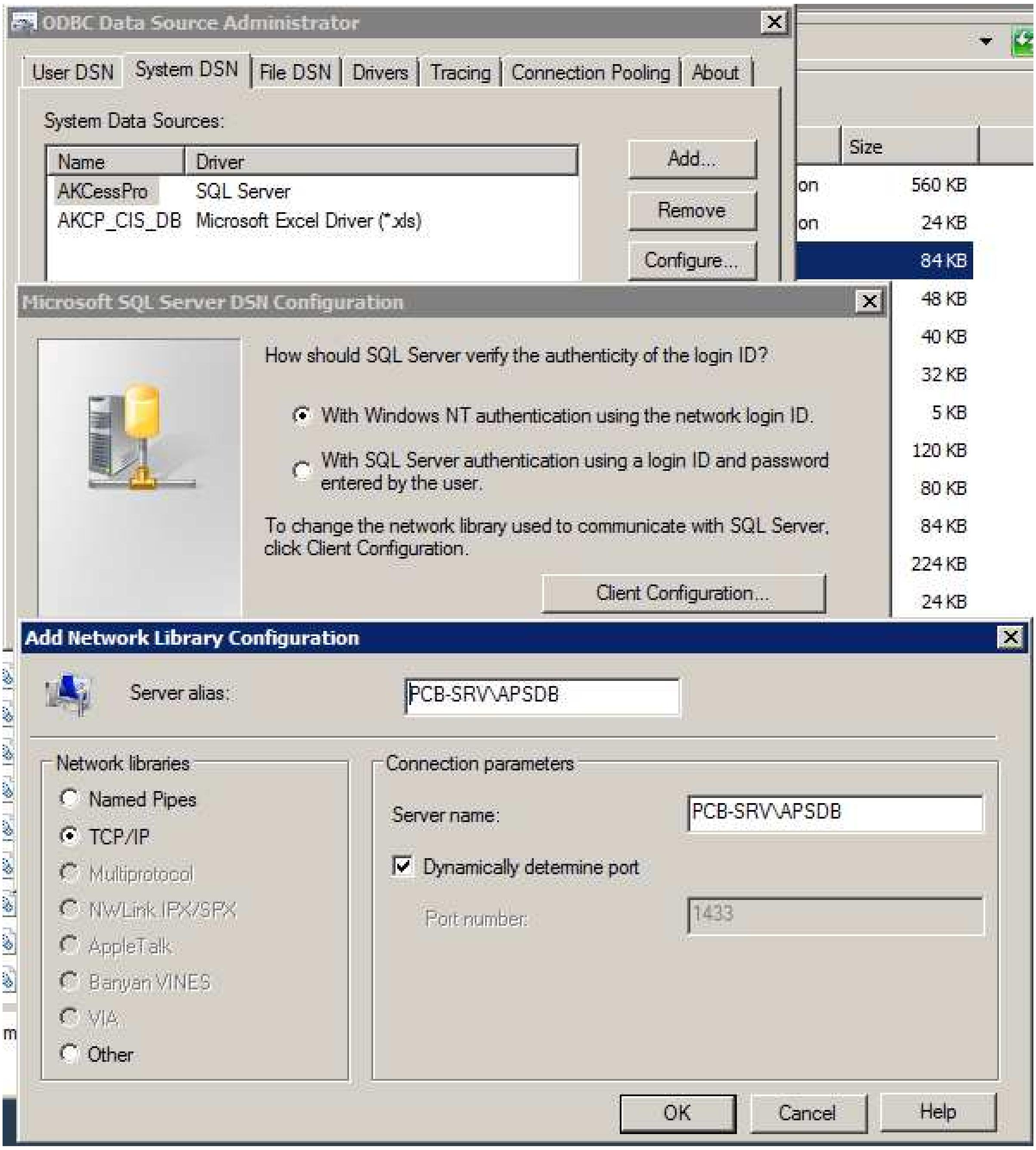
- remove the ODBC connector and uninstall CPS

- remove the existing CPS databases from the SQL server

- reinstall CPS cleanly and reconfigure it

## Used ports information

The port used for communication between the SQL server and CPS could be checked in the ODBC connector's configuration under Control Panel (the 32-bit ODBC app), and choose the CONTEGPro connector:



System Data Sources:

| Name | Driver |
|---|---|
| AKCessPro | SQL Server |
| AKCP_CIS_DB | Microsoft Excel Driver (*.xls) |

How should SQL Server verify the authenticity of the login ID?

● With Windows NT authentication using the network login ID.

○ With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

Server alias: PCB-SRV\APSDB

Network libraries

- ○ Named Pipes
- ● TCP/IP
- ○ Multiprotocol
- ○ NWLink IPX/SPX
- ○ AppleTalk
- ○ Banyan VINES
- ○ VIA
- ○ Other

Connection parameters

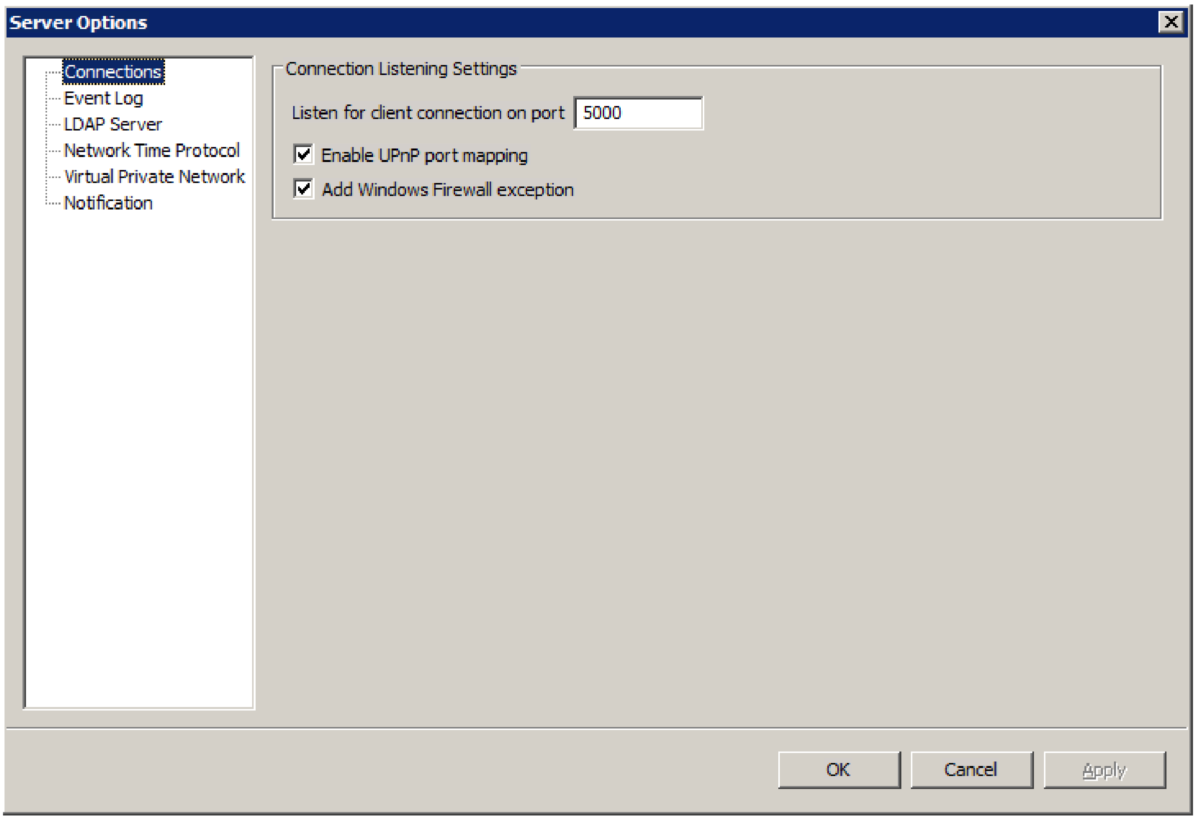
Server name: PCB-SRV\APSDB

☑ Dynamically determine port

Port number: 1433

The connector is under the System DSN tab. Click on **Configure…** then **Next** and choose **Client Configuration…**

By default the port is dynamic.



Server Options

Connection Listening Settings

Listen for client connection on port 5000

☑ Enable UPnP port mapping

☑ Add Windows Firewall exception

The generic CPS port that is used to communicate with Intelligent RAMOS devices is by default 5000 (TCP and UDP).

You can check and change this in the CPS Server Manager program, or under the CPS client **Settings menu / Server Options / Connections**.

## CPS database tables' explanation for sensors

Below, we'll explain the database tables in the CPS database which are dealing with sensors.

*Note:* In MS SQL database, these table names have a prefix **dbo.** for example: dbo.host

*Note 2:* We've only included the listed *reserved/unused* values in case you encounter a very old DB that still has these values; it's not an error if you see them.

*Note 3:* If the DB has some columns where the data type mismatches with the types written in this manual (INTEGER or VARCHAR, and length), that could mean you have a DB Sync issue or some other DB error.

1. **host** - contains all the network devices (including non- Intelligent RAMOS) under Monitoring/Sensors in CPS.

**hostid** (INTEGER, primary key) - CPS DB sequence number, unique for each device

**hostuid** (INTEGER) - reserved/unused

**mac** (VARCHAR, 20)- the device's MAC ID

**type** (INTEGER) - the device's type, see below for possible values

**name** (VARCHAR, 4000)- the device's IP address or DNS name

**port** (INTEGER) - SNMP monitoring port - note: the default port is also added for non-SNMP devices

**username** (VARCHAR, 4000)- SNMP username for the device

**community** (VARCHAR, 4000) - SNMP community (encoded) for the device

**enable** (INTEGER) - enabled (1) or disabled (0) device

**deleted** (INTEGER) - deleted device (1) or live device (0)

*Host type possible values:*

0 = Unknown Device

1 = Network Device

3 = Ramos Optima

6 = Axis Camera

7 = reserved/unused

8 = reserved/unused

9 = IP Camera

10 = Ramos Ultra

13 = Ramos Ultra ACS

14 = Onvif Compatible Camera

15 = Quaddrix IP Camera

16 = reserved for future product

17 = reserved/unused

18 = Template Device

2. **hostprop** - contains the network devices' property string values, such as device name and firmware version

**hostid** (INTEGER, primary key) - matches the hostid in the host table, per unique device

**name** (VARCHAR, primary key) - each device (hostid) can have multiple properties, these are listed here - for example: httpport, dhcp_enable, syscontact, firmware_version

**value** (VARCHAR, 4000) - the string value for each "name" field - following the previous example in order: 80, 0, System Contact, SEC-MX25V405a

*Example:*

| name | value |
|---|---|
| httpport | 80 |
| dhcp_enable | 0 |
| syscontact | System Contact |
| firmware_version | SEC-MX25V405a |

3. **board** - contains all board devices for each network device (every Intelligent RAMOS device that has at least a base board) and expansion boards

**hostid** (INTEGER) - matches the hostid in the host table, per unique device

**boardid** (INTEGER, primary key) - CPS DB sequence number, unique for each board

**board prop id** (INTEGER) - remote board id; the boardid in a device's own database, its value will match the board_ref_id property string in the boardprop table

**deleted** (INTEGER) - deleted board (1) or live board (0)

**property update id** (INTEGER) - used for checking that a board's property is modified or not; it will be 1 for the first time when you add an Intelligent RAMOS device to CPS, and increment when you edit a board- or sensor's setting

4. **boardprop** - contains the boards' property string values, such as expansion board name and type

**boardid** (INTEGER, primary key) - matches the boardid in the board table, per unique board

**name** (VARCHAR, 30, primary key) - each board (boardid) can have multiple properties, these are listed here - for example: desc, board_enable, type, revision

**value** (VARCHAR, 4000) - the string value for each "name" field - following the previous example in order: Main Module, 1, 8, 2

*Example:*

| **name** | **value** |
|---|---|
| desc | Main Module |
| board_enable | 1 |
| type | 8 |
| revision | 2 |

*Board type possible values:*

| | |
|---|---|
| 1 = | EX-I8 board |
| 3 = | EX-O16 board |
| 4 = | 8 sensors base board for Ramos Ultra |
| 8 = | Ramos Ultra ACS board |
| 9 = | RDU board |
| 10 = | EX-D64 board |
| 11 = | EX-D128 board |
| 12 = | EX-D192 board |

5. **service** - contains information about sensors

**hostid** (INTEGER) - matches the hostid in the host table, per unique device

**serviceid** (INTEGER, primary key) - CPS DB sequence number, unique for each sensor

**enable** (INTEGER) - enabled (1) or disabled (0) sensor

**interval** (INTEGER) - sensor polling interval (in seconds)

**type** (INTEGER) - the sensor's type, see below for possible values

**port** (INTEGER) - the sensor's port on a device; it can be physical or virtual, also for daisy chained sensors

**deleted** (INTEGER) - deleted sensor (1) or live sensor (0)

**boardid** (INTEGER) - matches the boardid in the board table, per unique board

**rboardid** (INTEGER) - remote board id; references the boardid on a remote device and matches the board_prop_id in the board table, it is used when CPS communicates with an Intelligent RAMOS device - CPS Server and CPS Client uses the boardid for communication

**rsensorid** (INTEGER) - remote sensor id; references the serviceid on a remote device’s database, it is used when CPS communicates with an Intelligent RAMOS device - CPS Server and CPS Client uses the serviceid for communication

**mode of reader** (INTEGER) - reserved/unused

CPS Server <--> CPS Client uses boardid / sensorid for communication

Device (SEC) <--> CPS Server uses rboardid / rsensorid for communication

*Sensor type possible values:*

2 = 4-20 mA

3 = Humidity

4 = Water Detector

5 = Digital Voltmeter

6 = Security

8 = Airflow

9 = Siren & Strobe Light

10 = Dry Contact

12 = AC Voltage

13 = Relay

14 = Motion Detector

15 = unused/reserved

16 = External Dry Contact

20 = unused/reserved

21 = unused/reserved

23 = Thermostat

24 = Smoke Detector

25 = Power

26 = RMS Current

27 = RMS Voltage

28 = Watt Meter

29 = External Relay

30 = Virtual Sensors

32 = Watt-Hour Meter

33 = Temperature Array

34 = Liquid Rope

35 = Fuel Level - deprecated

36 = Ultrasonic Fuel Level

37 = Door

39 = Reader

40 = Probe Switch

41 = Time Tracking

42 = Tamper

43 = Thermocouple

44 = Dry Contact expander

45 = Vibration

46 = Power Voltage

47 = 5 Input Dry Contact

128 = Sound Detector

129 = Software Motion Detector

132 = No Video Signal

134 = Power Meter

144 = Camera

61696 = Host Status

61697 = SNMP Get

61698 = Custom Script

61699 = Multiple Sensors

61701 = Software Motion Detector - deprecated

61702 = Map

61703 = Recording

61704 = Modbus TCP

61706 = Host on Map

6. **serviceprop** - contains the sensors' property string values, such as status description and sensor unit

**serviceid** (INTEGER, primary key) - matches the serviceid in the service table, per unique sensor

**name** (VARCHAR, 30, primary key) - each sensor (serviceid) can have multiple properties, these are listed here - for example: desc, on_desc, normalstate, ping_method

**value** (VARCHAR, 4000) - the string value for each "name" field - following the previous example in order: Host Status, Unreachable, 0, 0

*Example:*

| **name** | **value** |
|---|---|
| desc | Host Status |
| on_desc | Unreachable |
| normalstate | 0 |
| ping_method | 0 |

## Finding sensor data in the CPS database

In this example below, we'll find a test RAMOS OPTIMA unit's temperature/humidity sensors in the database.

We'll use the default SQLite DB format and the SQLite Database Browser program for demonstration purposes (downloadable from http://sqlitebrowser.org/).

This requires checking 3 database tables: **hostid** (devices), **service** (sensor IDs), and **serviceprop** (sensor properties).

*Note:* the default CPS SQLite database is stored at **C:\ProgramData\CONTEG\CONTEG Pro Server\server.db**

1. Open **server.db** file with the browser, and look through the **host** table to find the RAMOS OPTIMA device (we looked for its IP address in the name field):

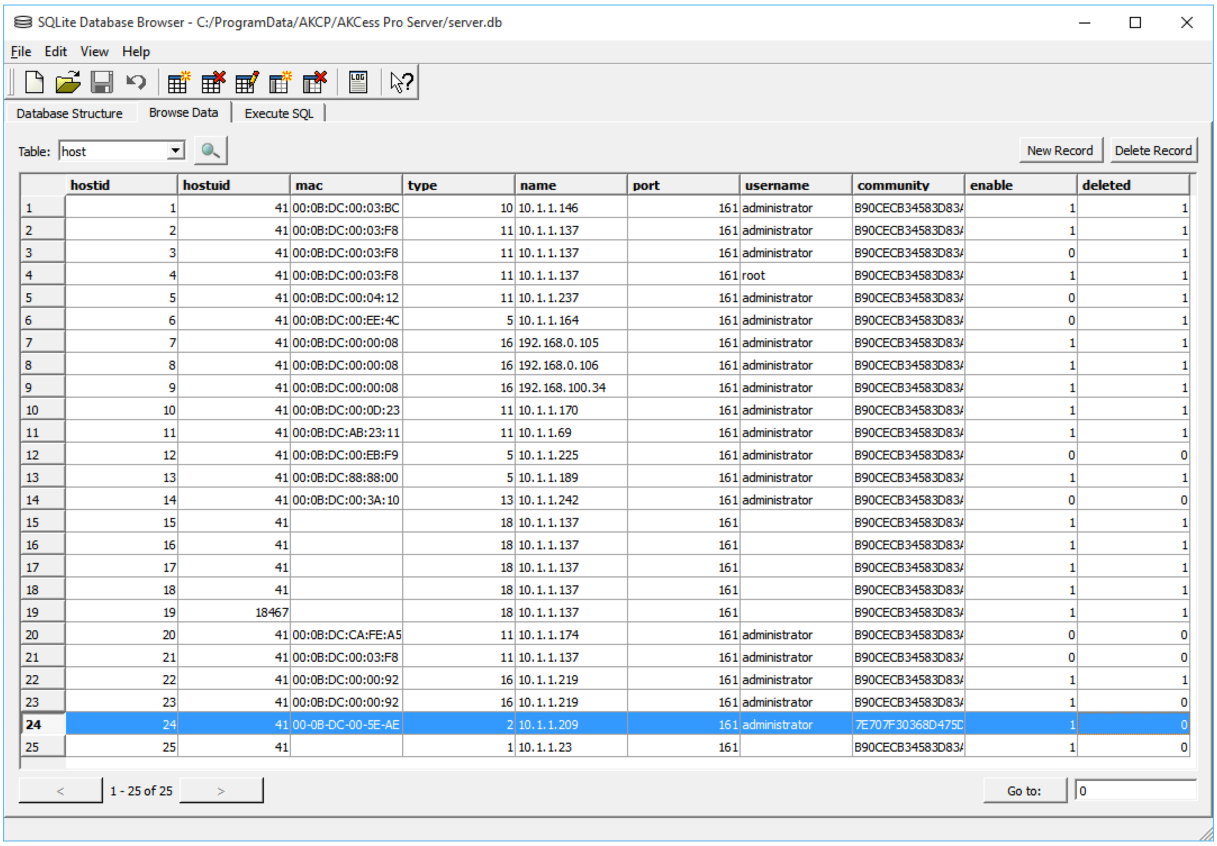


Table: host

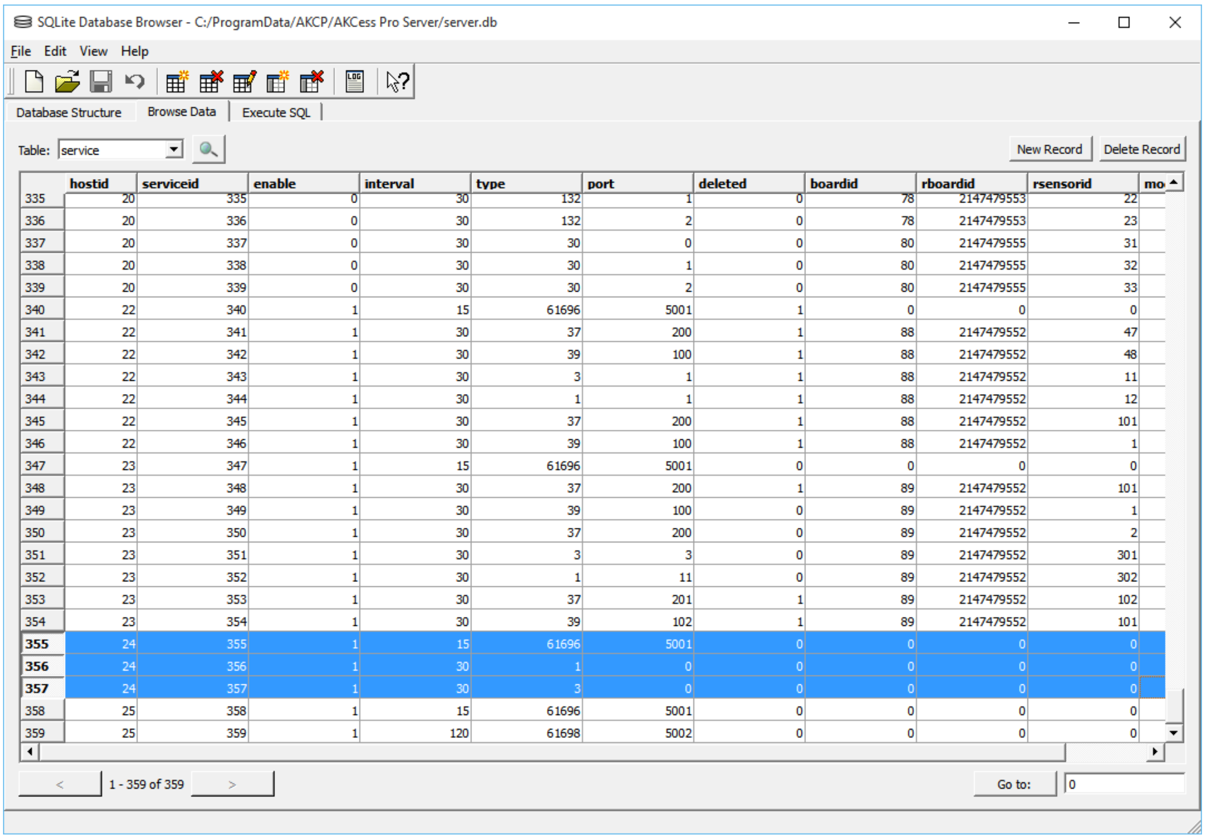
| | hostid | hostuid | mac | type | name | port | username | community | enable | deleted |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 41 | 00:0B:DC:00:03:BC | 10 | 10.1.1.146 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 2 | 2 | 41 | 00:0B:DC:00:03:F8 | 11 | 10.1.1.137 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 3 | 3 | 41 | 00:0B:DC:00:03:F8 | 11 | 10.1.1.137 | 161 | administrator | B90CECB34583D83 | 0 | 1 |
| 4 | 4 | 41 | 00:0B:DC:00:03:F8 | 11 | 10.1.1.137 | 161 | root | B90CECB34583D83 | 1 | 1 |
| 5 | 5 | 41 | 00:0B:DC:00:04:12 | 11 | 10.1.1.237 | 161 | administrator | B90CECB34583D83 | 0 | 1 |
| 6 | 6 | 41 | 00:0B:DC:00:EE:4C | 5 | 10.1.1.164 | 161 | administrator | B90CECB34583D83 | 0 | 1 |
| 7 | 7 | 41 | 00:0B:DC:00:00:08 | 16 | 192.168.0.105 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 8 | 8 | 41 | 00:0B:DC:00:00:08 | 16 | 192.168.0.106 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 9 | 9 | 41 | 00:0B:DC:00:00:08 | 16 | 192.168.100.34 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 10 | 10 | 41 | 00:0B:DC:00:0D:23 | 11 | 10.1.1.170 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 11 | 11 | 41 | 00:0B:DC:AB:23:11 | 11 | 10.1.1.69 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 12 | 12 | 41 | 00:0B:DC:00:EB:F9 | 5 | 10.1.1.225 | 161 | administrator | B90CECB34583D83 | 0 | 0 |
| 13 | 13 | 41 | 00:0B:DC:88:88:00 | 5 | 10.1.1.189 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 14 | 14 | 41 | 00:0B:DC:00:3A:10 | 13 | 10.1.1.242 | 161 | administrator | B90CECB34583D83 | 0 | 0 |
| 15 | 15 | 41 | | 18 | 10.1.1.137 | 161 | | B90CECB34583D83 | 1 | 1 |
| 16 | 16 | 41 | | 18 | 10.1.1.137 | 161 | | B90CECB34583D83 | 1 | 1 |
| 17 | 17 | 41 | | 18 | 10.1.1.137 | 161 | | B90CECB34583D83 | 1 | 1 |
| 18 | 18 | 41 | | 18 | 10.1.1.137 | 161 | | B90CECB34583D83 | 1 | 1 |
| 19 | 19 | 18467 | | 18 | 10.1.1.137 | 161 | | B90CECB34583D83 | 1 | 1 |
| 20 | 20 | 41 | 00:0B:DC:CA:FE:A5 | 11 | 10.1.1.174 | 161 | administrator | B90CECB34583D83 | 0 | 0 |
| 21 | 21 | 41 | 00:0B:DC:00:03:F8 | 11 | 10.1.1.137 | 161 | administrator | B90CECB34583D83 | 0 | 0 |
| 22 | 22 | 41 | 00:0B:DC:00:00:92 | 16 | 10.1.1.219 | 161 | administrator | B90CECB34583D83 | 1 | 1 |
| 23 | 23 | 41 | 00:0B:DC:00:00:92 | 16 | 10.1.1.219 | 161 | administrator | B90CECB34583D83 | 1 | 0 |
| 24 | 24 | 41 | 00-0B-DC-00-5E-AE | 2 | 10.1.1.209 | 161 | administrator | 7E707F30368D475D | 1 | 0 |
| 25 | 25 | 41 | | 1 | 10.1.1.23 | 161 | | B90CECB34583D83 | 1 | 0 |

1 - 25 of 25

Go to: 0

Its **hostid** is **24**. Next we'll look through the **service** table and find the entries with **hostid 24**.

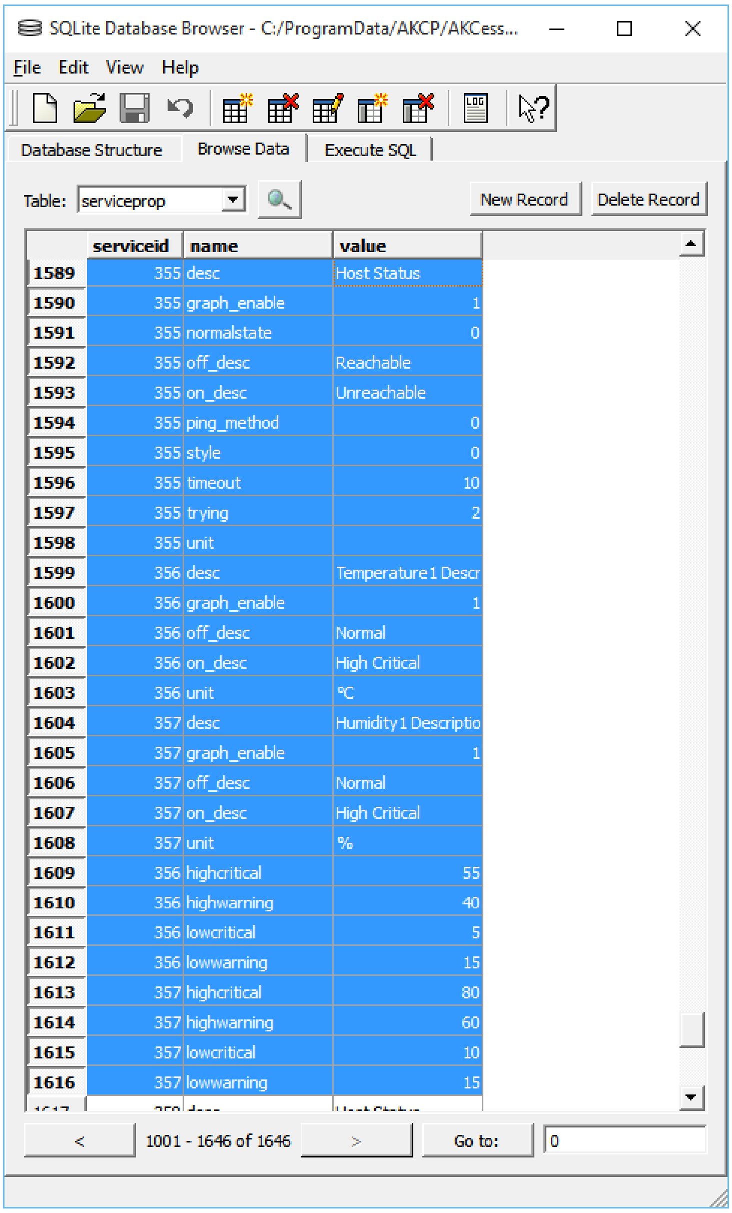
2. Browse the **service** table and look for **hostid 24**:



| | hostid | serviceid | enable | interval | type | port | deleted | boardid | rboardid | rsensorid | mo |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 335 | 20 | 335 | 0 | 30 | 132 | 1 | 0 | 78 | 2147479553 | 22 | |
| 336 | 20 | 336 | 0 | 30 | 132 | 2 | 0 | 78 | 2147479553 | 23 | |
| 337 | 20 | 337 | 0 | 30 | 30 | 0 | 0 | 80 | 2147479555 | 31 | |
| 338 | 20 | 338 | 0 | 30 | 30 | 1 | 0 | 80 | 2147479555 | 32 | |
| 339 | 20 | 339 | 0 | 30 | 30 | 2 | 0 | 80 | 2147479555 | 33 | |
| 340 | 22 | 340 | 1 | 15 | 61696 | 5001 | 1 | 0 | 0 | 0 | |
| 341 | 22 | 341 | 1 | 30 | 37 | 200 | 1 | 88 | 2147479552 | 47 | |
| 342 | 22 | 342 | 1 | 30 | 39 | 100 | 1 | 88 | 2147479552 | 48 | |
| 343 | 22 | 343 | 1 | 30 | 3 | 1 | 1 | 88 | 2147479552 | 11 | |
| 344 | 22 | 344 | 1 | 30 | 1 | 1 | 1 | 88 | 2147479552 | 12 | |
| 345 | 22 | 345 | 1 | 30 | 37 | 200 | 1 | 88 | 2147479552 | 101 | |
| 346 | 22 | 346 | 1 | 30 | 39 | 100 | 1 | 88 | 2147479552 | 1 | |
| 347 | 23 | 347 | 1 | 15 | 61696 | 5001 | 0 | 0 | 0 | 0 | |
| 348 | 23 | 348 | 1 | 30 | 37 | 200 | 1 | 89 | 2147479552 | 101 | |
| 349 | 23 | 349 | 1 | 30 | 39 | 100 | 0 | 89 | 2147479552 | 1 | |
| 350 | 23 | 350 | 1 | 30 | 37 | 200 | 0 | 89 | 2147479552 | 2 | |
| 351 | 23 | 351 | 1 | 30 | 3 | 3 | 0 | 89 | 2147479552 | 301 | |
| 352 | 23 | 352 | 1 | 30 | 1 | 11 | 0 | 89 | 2147479552 | 302 | |
| 353 | 23 | 353 | 1 | 30 | 37 | 201 | 1 | 89 | 2147479552 | 102 | |
| 354 | 23 | 354 | 1 | 30 | 39 | 102 | 1 | 89 | 2147479552 | 101 | |
| 355 | 24 | 355 | 1 | 15 | 61696 | 5001 | 0 | 0 | 0 | 0 | |
| 356 | 24 | 356 | 1 | 30 | 1 | 0 | 0 | 0 | 0 | 0 | |
| 357 | 24 | 357 | 1 | 30 | 3 | 0 | 0 | 0 | 0 | 0 | |
| 358 | 25 | 358 | 1 | 15 | 61696 | 5001 | 0 | 0 | 0 | 0 | |
| 359 | 25 | 359 | 1 | 120 | 61698 | 5002 | 0 | 0 | 0 | 0 | |

This **hostid** has 3 **serviceid** values: **355**, **356**, **357**. We'll look for these in the **serviceprop** table.

3. Browse the **serviceprop** table and look for the **serviceid** values:



| | serviceid | name | value |
|---|---|---|---|
| 1589 | 355 | desc | Host Status |
| 1590 | 355 | graph_enable | 1 |
| 1591 | 355 | normalstate | 0 |
| 1592 | 355 | off_desc | Reachable |
| 1593 | 355 | on_desc | Unreachable |
| 1594 | 355 | ping_method | 0 |
| 1595 | 355 | style | 0 |
| 1596 | 355 | timeout | 10 |
| 1597 | 355 | trying | 2 |
| 1598 | 355 | unit | |
| 1599 | 356 | desc | Temperature1 Descr |
| 1600 | 356 | graph_enable | 1 |
| 1601 | 356 | off_desc | Normal |
| 1602 | 356 | on_desc | High Critical |
| 1603 | 356 | unit | ºC |
| 1604 | 357 | desc | Humidity1 Descriptio |
| 1605 | 357 | graph_enable | 1 |
| 1606 | 357 | off_desc | Normal |
| 1607 | 357 | on_desc | High Critical |
| 1608 | 357 | unit | % |
| 1609 | 356 | highcritical | 55 |
| 1610 | 356 | highwarning | 40 |
| 1611 | 356 | lowcritical | 5 |
| 1612 | 356 | lowwarning | 15 |
| 1613 | 357 | highcritical | 80 |
| 1614 | 357 | highwarning | 60 |
| 1615 | 357 | lowcritical | 10 |
| 1616 | 357 | lowwarning | 15 |
| 1617 | 358 | desc | Host Status |

There are multiple matches found for these sensors. These are all the values for the T/HS sensor connected to this RAMOS OPTIMA.

Based on this information, you can get the **serviceid** value for a given sensor.

More entries would be present if more sensors are attached to a device.

**CONTEG, spol. s r.o.**

**Headquarters:**

Na Vitezne plani 1719/4
140 00 Prague 4
Czech Republic
Tel.: +420 261 219 182
conteg@conteg.com
www.conteg.com

**Production plant:**

K Silu 2179
393 01 Pelhrimov
Czech Republic
Tel.: +420 565 300 300

verze