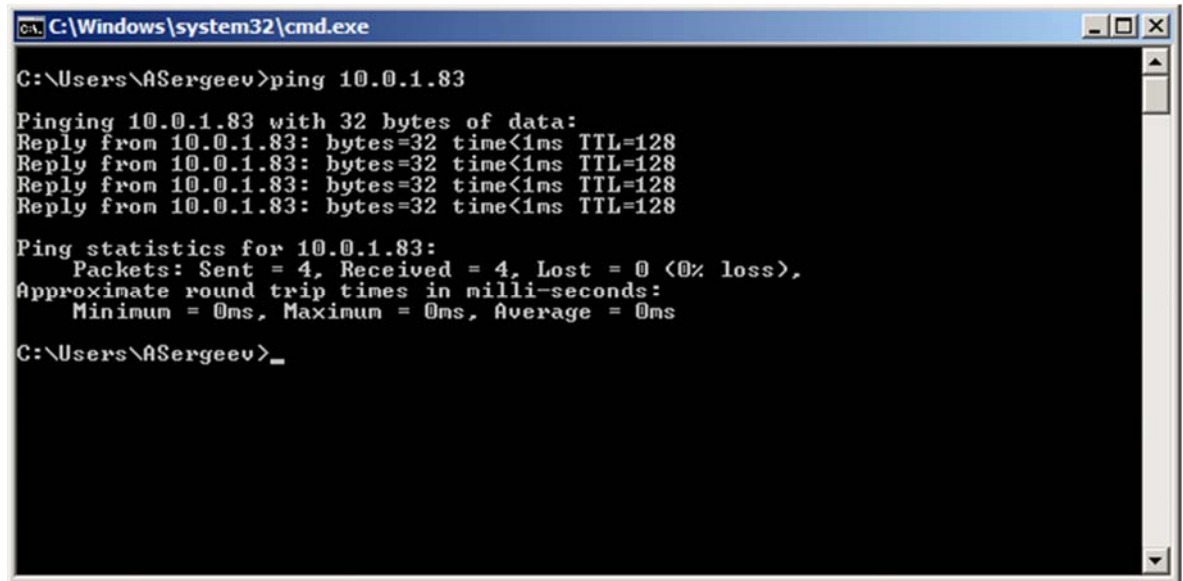


How to resolve connection problems between server and workstation

1. Check network connection

Make sure you have network connection between workstation and server. Run command line on workstation and type 'ping xxx.xxx.xxx.xxx', where xxx.xxx.xxx.xxx – IP address of server. If you have connection you should receive reply packages from server.

Example:

A screenshot of a Windows command prompt window. The title bar reads "C:\Windows\system32\cmd.exe". The command prompt shows the user "ASergeev" at the "C:\Users\ASergeev" directory. The command entered is "ping 10.0.1.83". The output shows four successful replies from 10.0.1.83, each with 32 bytes of data, a time of less than 1ms, and a TTL of 128. Below the replies, the ping statistics are displayed: 4 packets sent, 4 received, 0 lost (0% loss), and approximate round trip times of 0ms for minimum, maximum, and average.

```
C:\Windows\system32\cmd.exe
C:\Users\ASergeev>ping 10.0.1.83
Pinging 10.0.1.83 with 32 bytes of data:
Reply from 10.0.1.83: bytes=32 time<1ms TTL=128
Reply from 10.0.1.83: bytes=32 time<1ms TTL=128
Reply from 10.0.1.83: bytes=32 time<1ms TTL=128
Reply from 10.0.1.83: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.1.83:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\ASergeev>_
```

Otherwise contact your system administrator to set up network connection.

2. Check ODBC (ODBC for x64 bit operating system)

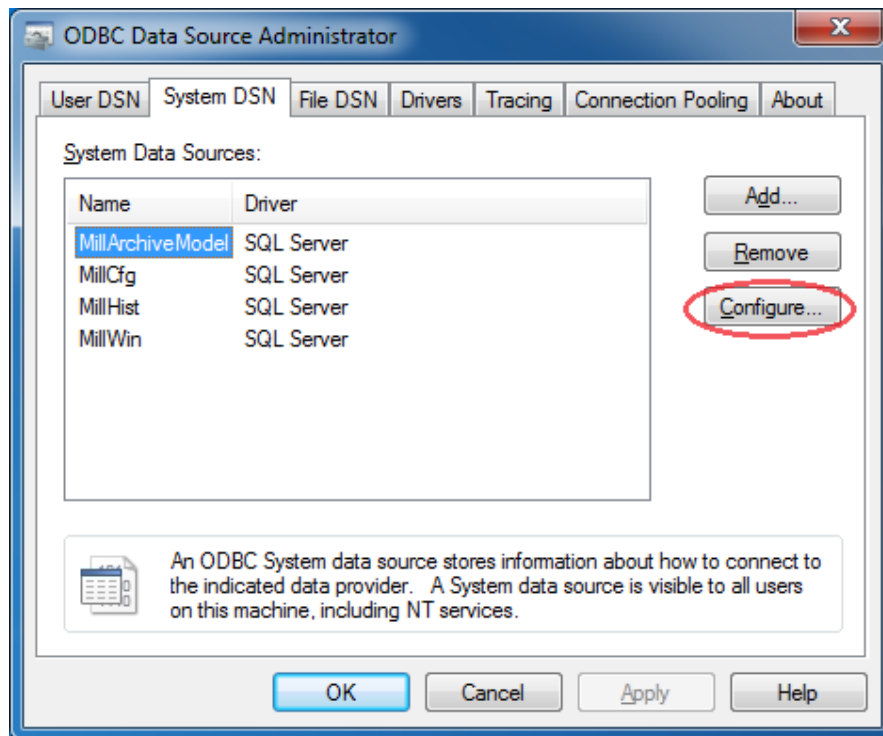
If you are using 32-bit operating system then run ODBC Administrator from control panel: "Control panel" -> "Administrative tools" -> "Data source (ODBC)".

If you are using 64-bit operating system then run ODBC Administrator from Windows installation folder:

%SystemRoot%\SysWOW64\odbcad32.exe, where %SystemRoot% is the windows installation folder, generally it is "C:\Windows".

On the ODBC Administrator window switch to the "System DSN" tab. You will see four data sources: "MillArchiveModel", "MillCfg", "MillHist", "MillWin". For each of them perform next operations:

Select data source and press "Configure" button.



On first screen in field "Server" enter full name of SQL Server instance. For example: "%ComputerName%\SQLEXPRESS". If you installed SQL Server from Millennium installation CD then just type the name of the server.

Make sure that workstation user can connect to SQL Server using windows authentication. Otherwise you can setup connection using SQL Server authentication. In this case you will need to enter Login ID and Password in ODBC driver configuration. This login should have access to SQL Server.

Click "Next" on next screens until "Finish" button appears.

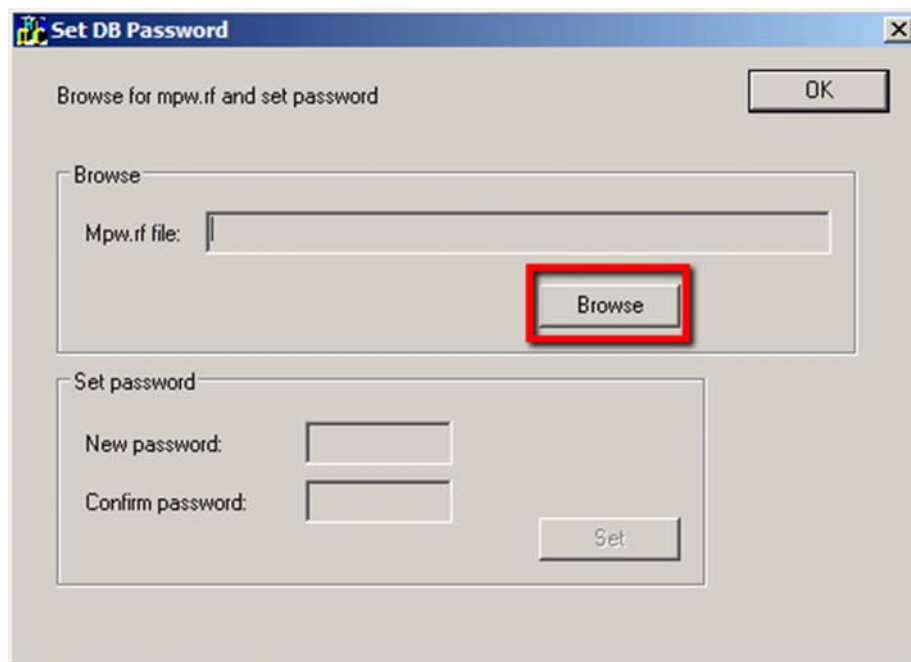
Click "Finish". On new screen click "Test Data Source...". If message "TESTS COMPLETED SUCCESSFULLY!" appears then data source configured correctly.

Click "OK".

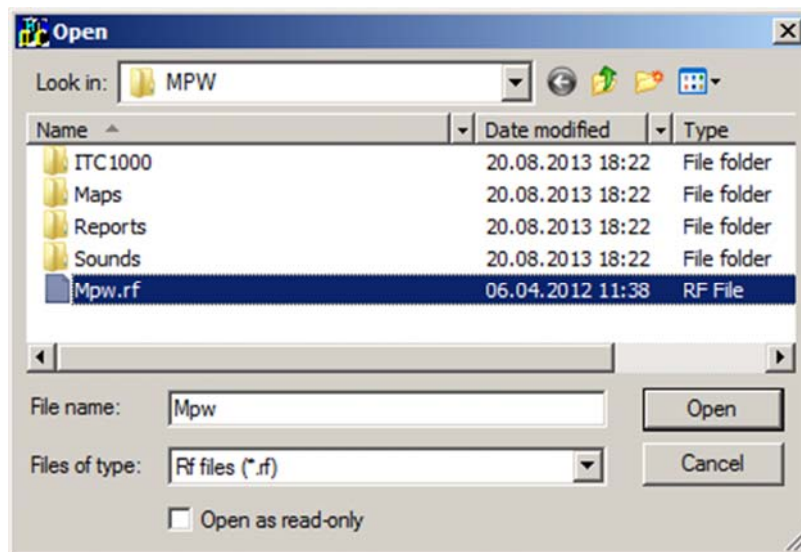
Repeat this procedure for all four data sources.

3. If SQL authentication is used, enter password using rfsetpswd.exe

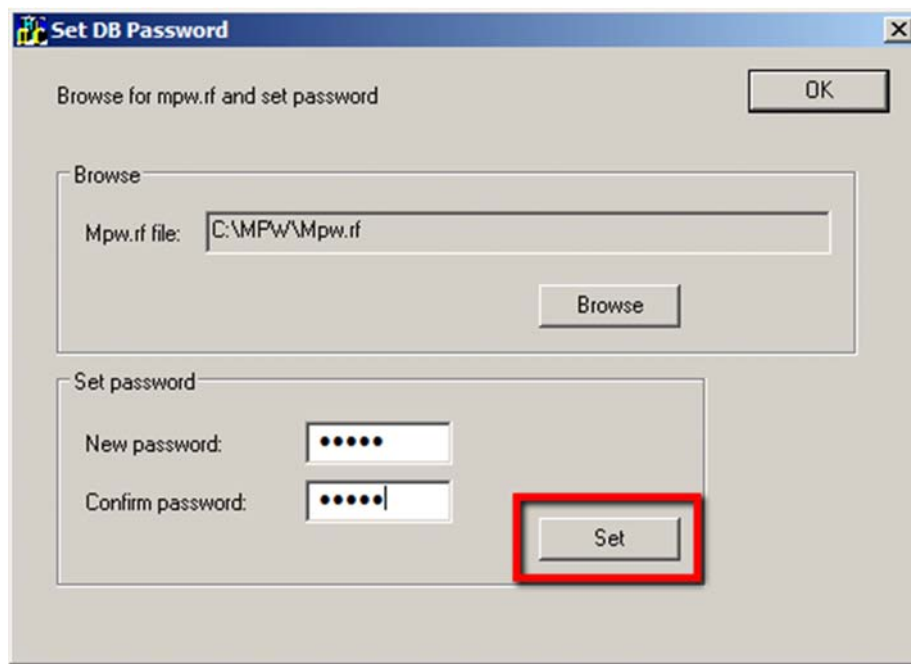
If you are using SQL Server authentication then you will need to add password to MPW.rf file. Go to server. From folder C:\MPW\Scripts (replace C:\MPW with your installation path if you enter different during installation) copy file 'RfSetPswd.exe' to installation folder on workstation. Run this file. Click "Browse".



Select MPW.rf file from workstation installation folder. Click “Open”.



Enter password for Login ID that you entered in ODBC Driver configuration and click “Set”.



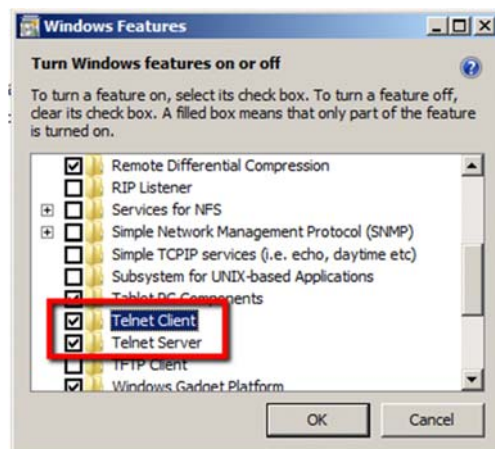
System will prompt you that password successfully set. Click “Ok” and close program.

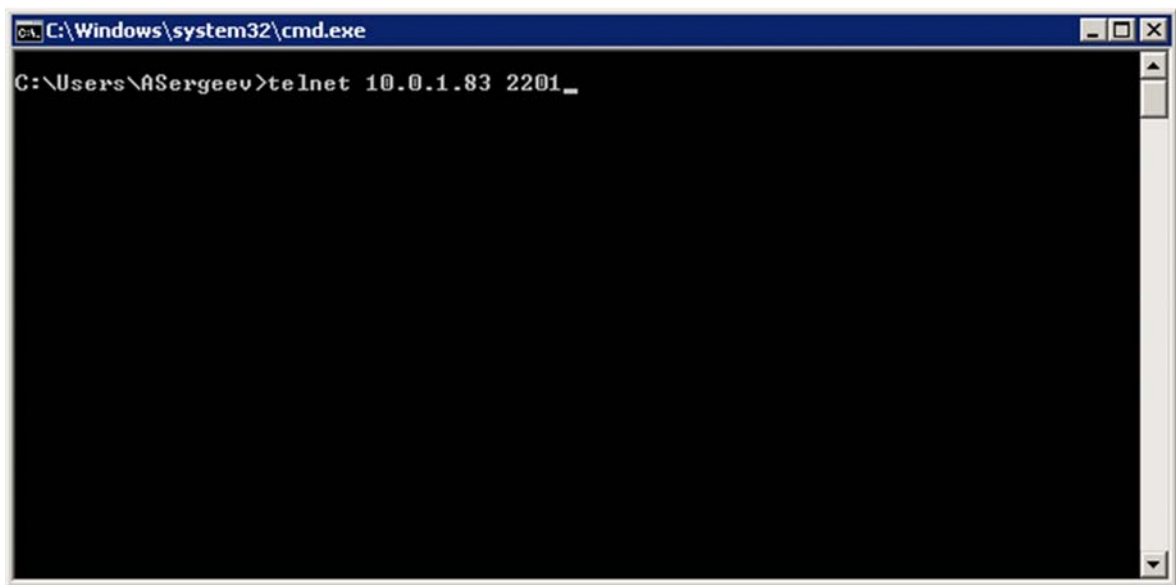


4. Check Windows Firewall. Disable for test, add rule.

Windows Firewall might block connection to server from workstation. To ensure that you can connect to TCP port that Millennium using for connection you can do following:
Run command line, enter ‘telnet xxx.xxx.xxx.xxx 2201’, where xxx.xxx.xxx.xxx – Server IP address.

If telnet command wasn’t recognized, you can enable telnet feature in Control Panel -> Programs and Features (Add or Remove Programs) -> Turn Windows features on or off. Enable Telnet Client and Telnet Server features. Click Ok. Windows will install Telnet feature.



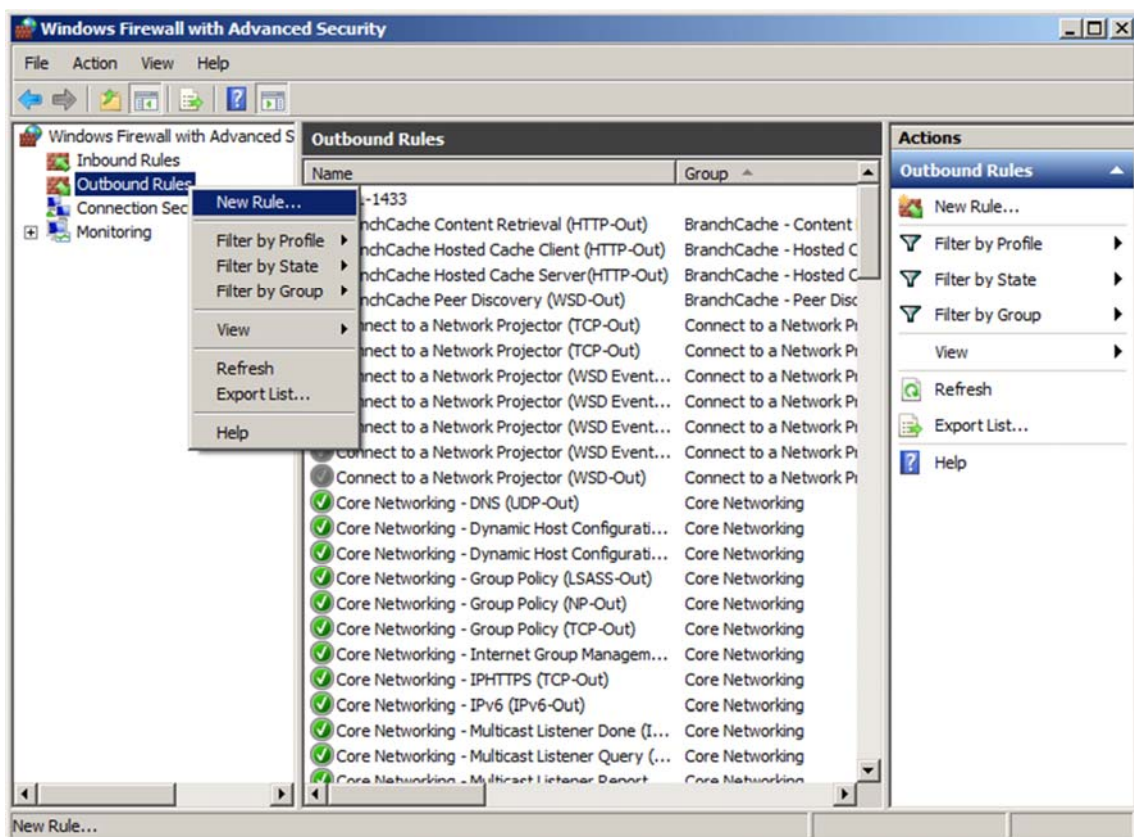


Press enter. If connection was successful you should see blank screen. It means that Telnet connected to TCP port.

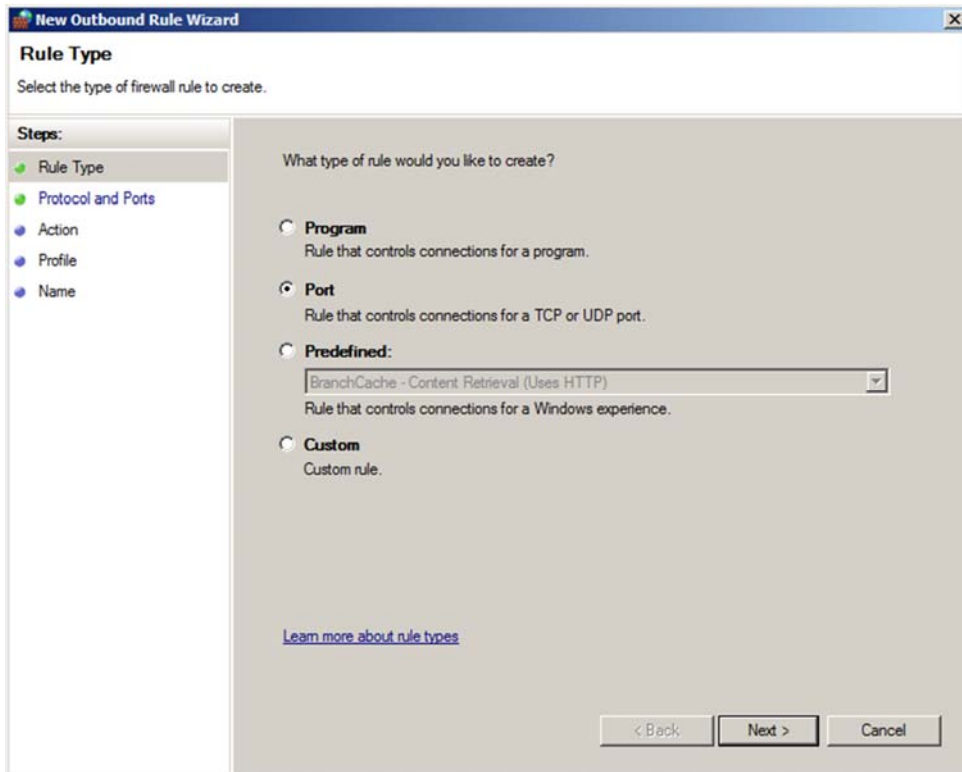
If connection wasn't successful you should check Windows Firewall settings.

Try to disable Firewall at the workstation and at the server and repeat telnet command. Run Millennium at the workstation. If you can connect to server it means that you should add rules to Windows Firewall.

To add rule at the workstation go to Windows Firewall -> Advanced Settings. Right click on 'Outbound rules' item -> New rule:

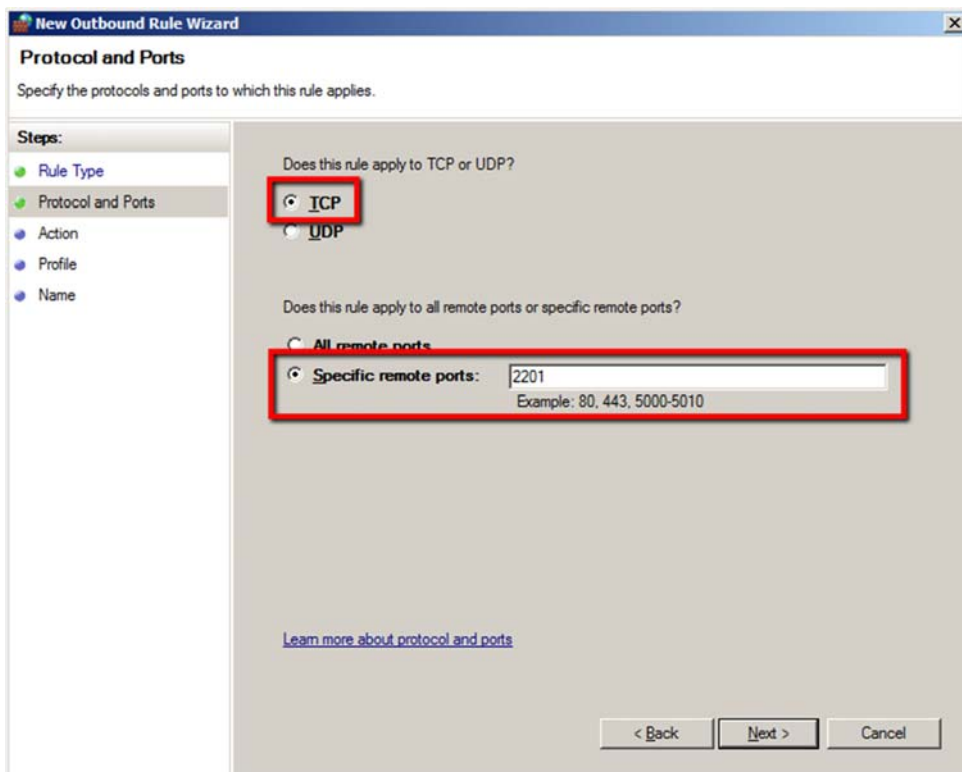


Select rule type – Port and click Next:



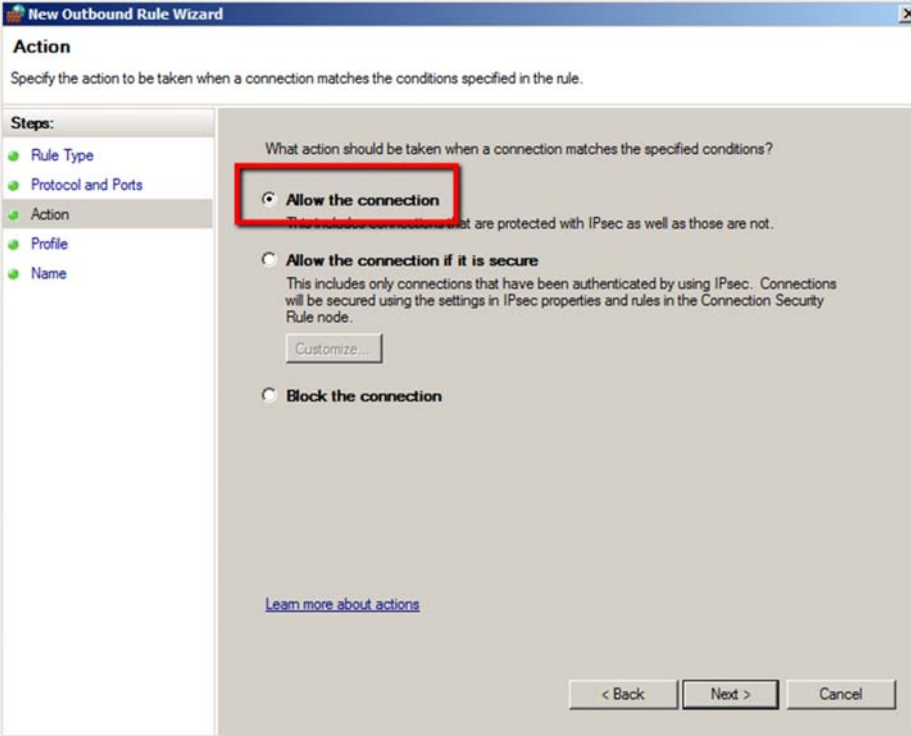
The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Rule Type' step. The title bar reads 'New Outbound Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name', with 'Rule Type' being the active step. The main area asks 'What type of rule would you like to create?' and offers four radio button options: 'Program' (Rule that controls connections for a program.), 'Port' (Rule that controls connections for a TCP or UDP port.), 'Predefined:' (with a dropdown menu showing 'BranchCache - Content Retrieval (Uses HTTP)' and the description 'Rule that controls connections for a Windows experience.'), and 'Custom' (Custom rule.). A link 'Learn more about rule types' is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

Apply this rule to TCP and specify port number 2201. Click Next



The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The title bar reads 'New Outbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, the 'Steps:' pane shows 'Rule Type' and 'Protocol and Ports' as completed steps, with 'Protocol and Ports' being the active step. The main area asks 'Does this rule apply to TCP or UDP?' with radio buttons for 'TCP' and 'UDP'; 'TCP' is selected and highlighted with a red box. Below, it asks 'Does this rule apply to all remote ports or specific remote ports?' with radio buttons for 'All remote ports' and 'Specific remote ports:'. The 'Specific remote ports' option is selected and highlighted with a red box, with a text input field containing '2201' and an example 'Example: 80, 443, 5000-5010' below it. A link 'Learn more about protocol and ports' is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

Select 'Allow the connection' and click Next



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The 'Action' step is currently selected. The main area asks 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (which is selected and highlighted with a red rectangle), 'Allow the connection if it is secure', and 'Block the connection'. Below the 'Allow the connection if it is secure' option is a 'Customize...' button. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about actions' is located at the bottom left of the main area.

New Outbound Rule Wizard

Action

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

Steps:

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

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 that are not.

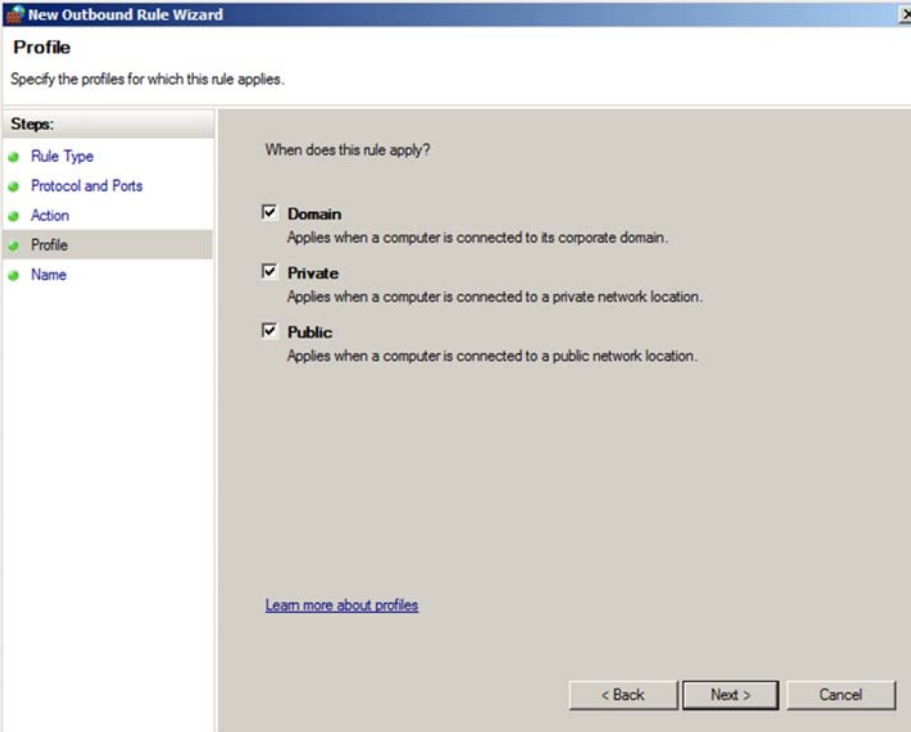
☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

[Learn more about actions](#)

< Back Next > Cancel

Select all, Domain, Private and Public networks. Click Next.



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Profile' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The 'Profile' step is currently selected. The main area asks 'When does this rule apply?'. There are three checked checkboxes: 'Domain', 'Private', and 'Public'. Each checkbox has a description: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'. A link 'Learn more about profiles' is located at the bottom left of the main area.

New Outbound 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.

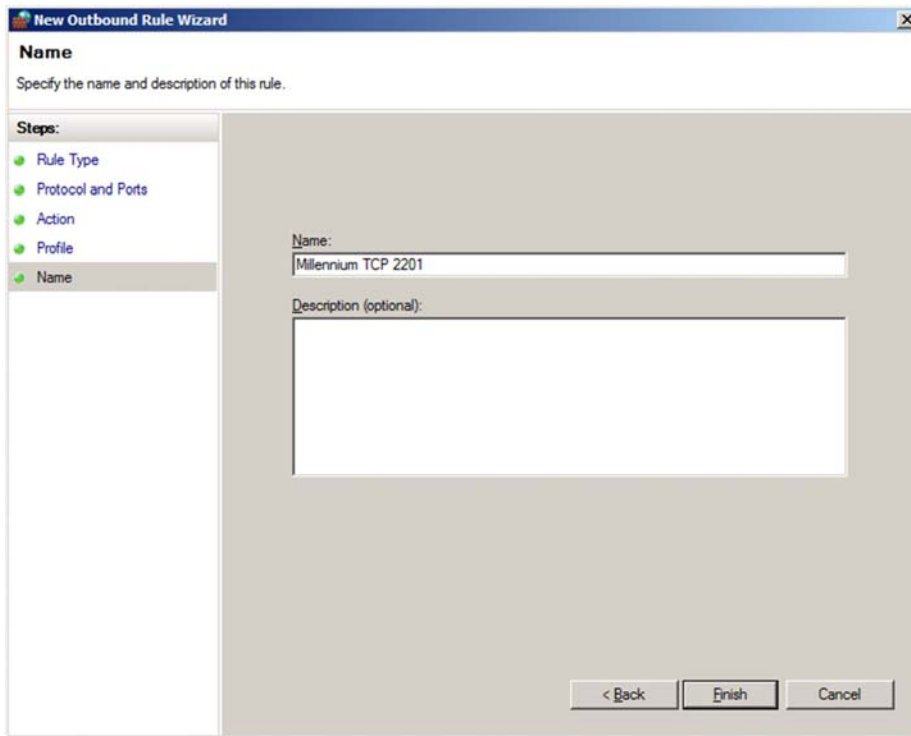
☒ **Private**
Applies when a computer is connected to a private network location.

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

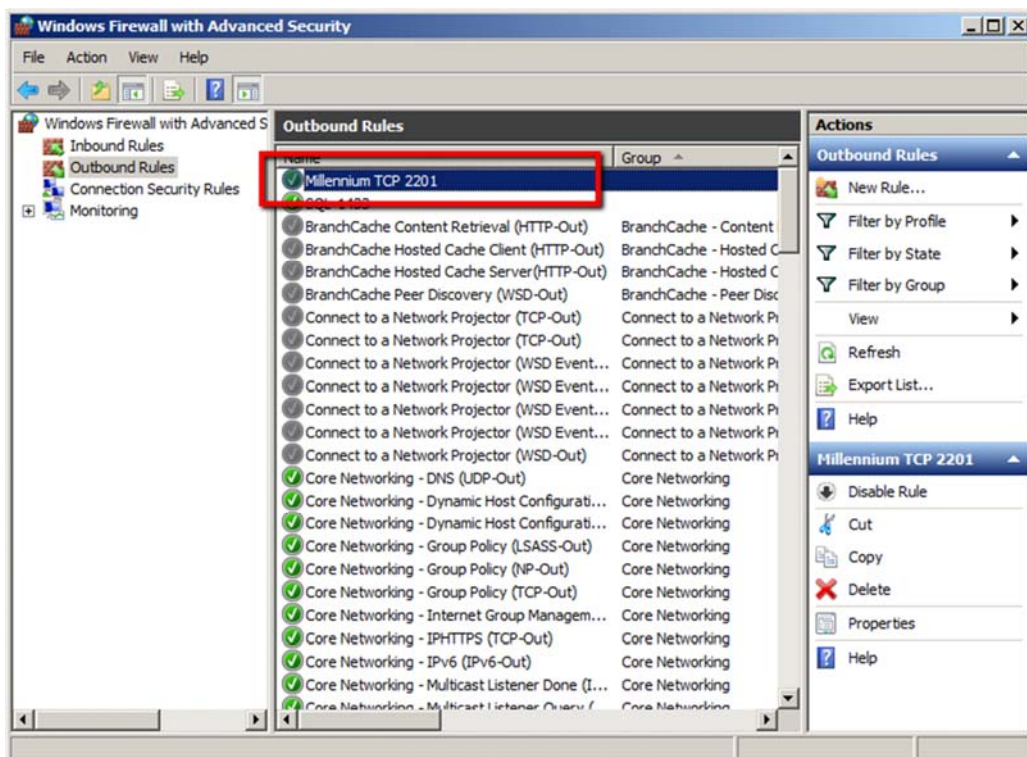
[Learn more about profiles](#)

< Back Next > Cancel

Enter name for rule and click Finish.

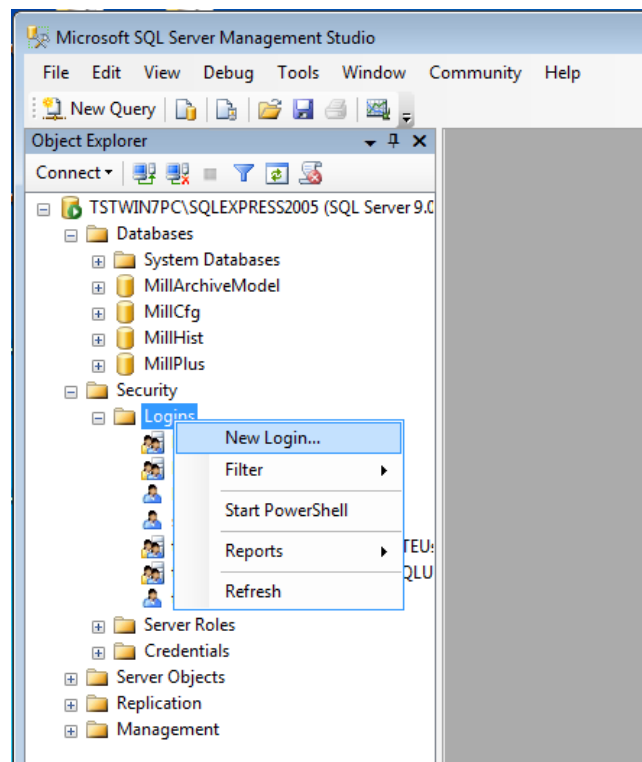


Rule should appear in the list of rules:

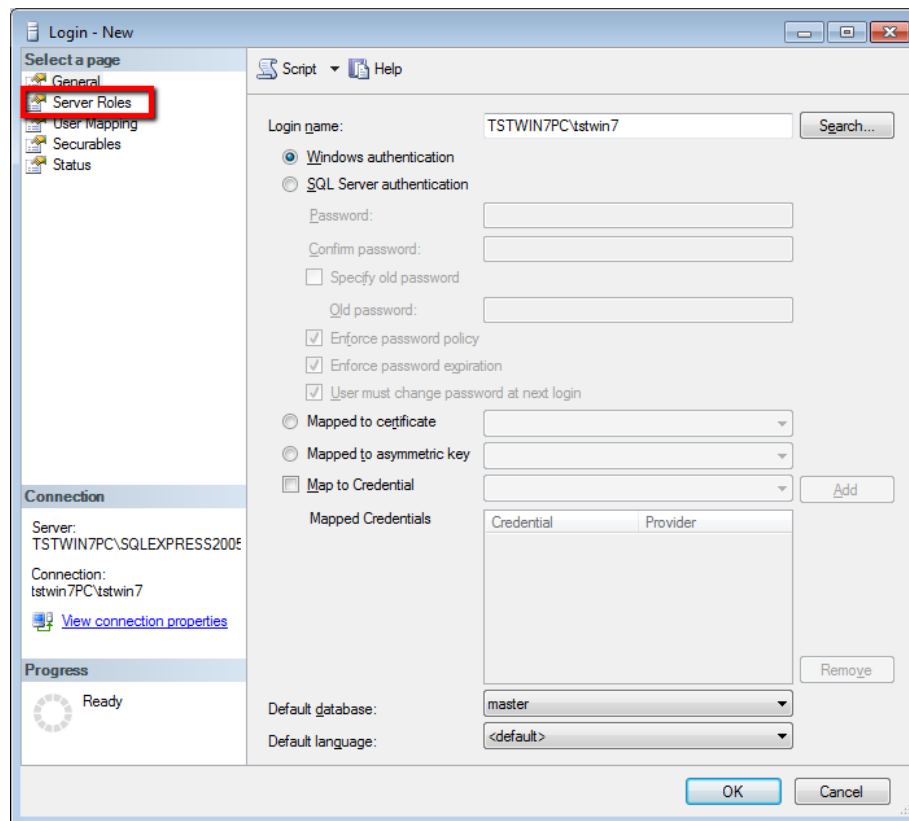


Do the same procedure at the server, but instead of creating Outbound rule you should create Inbound rule with the same options.

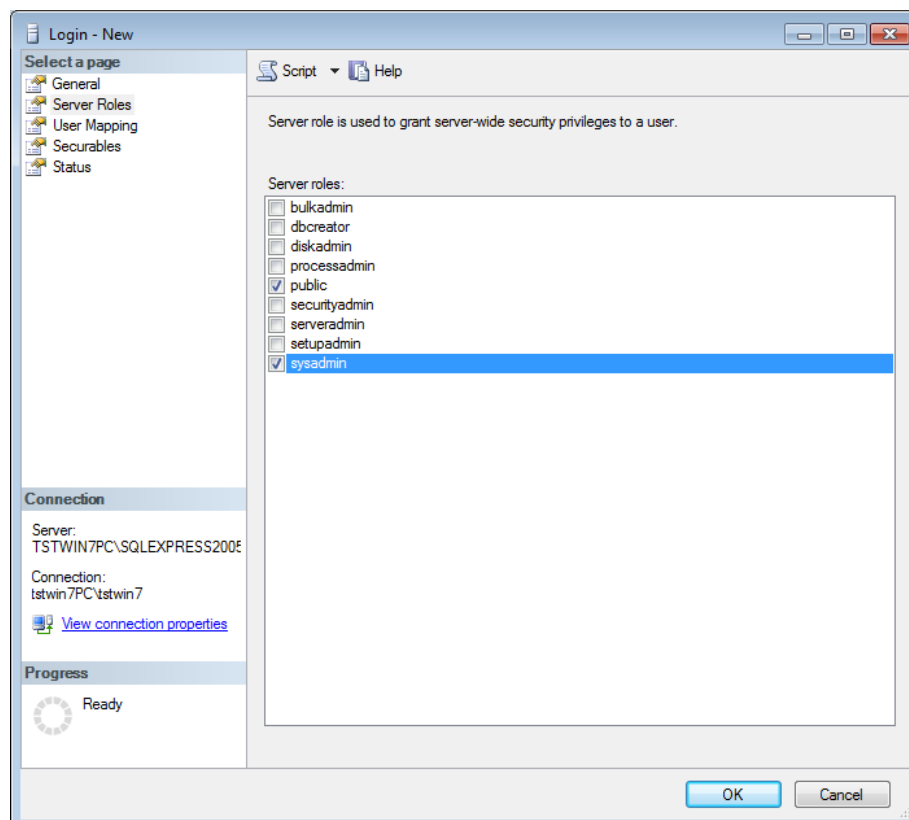
5. Copy MPW.rf from server to workstation
You should have same mpw.rf file at the server and at each workstation. Make sure you have copied mpw.rf file from server to workstation.
6. Check if the Millennium running as a service. If it does, Millennium shouldn't run as application.
7. Make sure your user exists in SQL Server security.
To add user to SQL Server security do following:
Start Management Studio and connect to server
Go to Security -> Logins -> right click on Logins -> New Login...



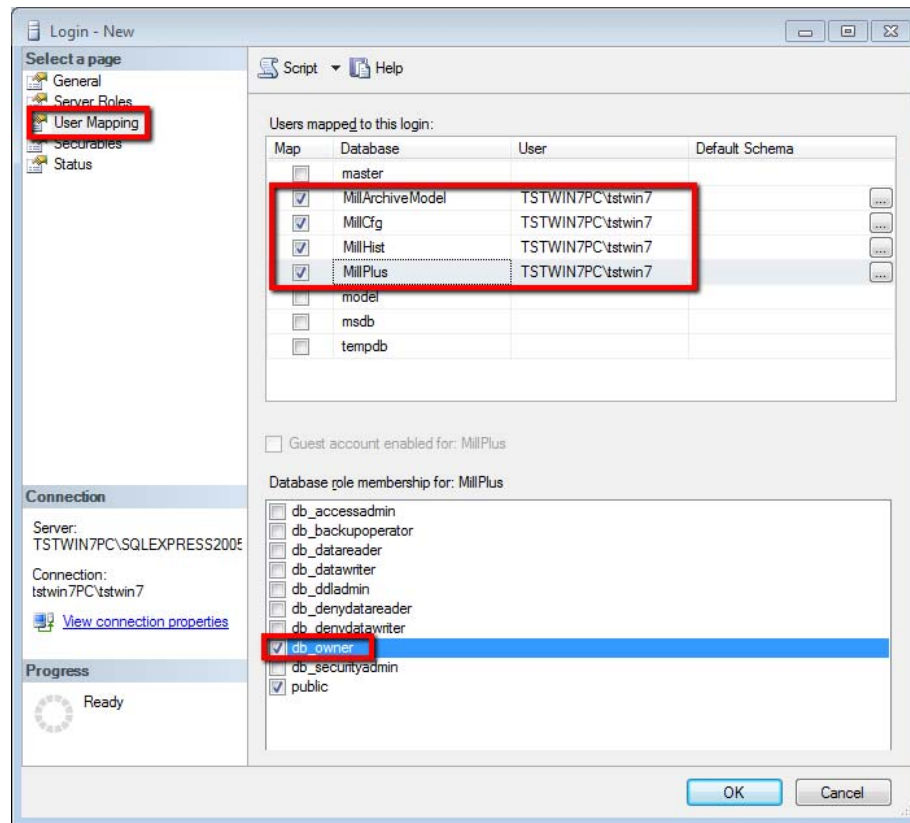
Select user login and go to Server Roles page



Check option 'sysadmin'



Go to page User Mapping. Check 4 Millennium databases. For each database check option 'db_owner'.



Click Ok.