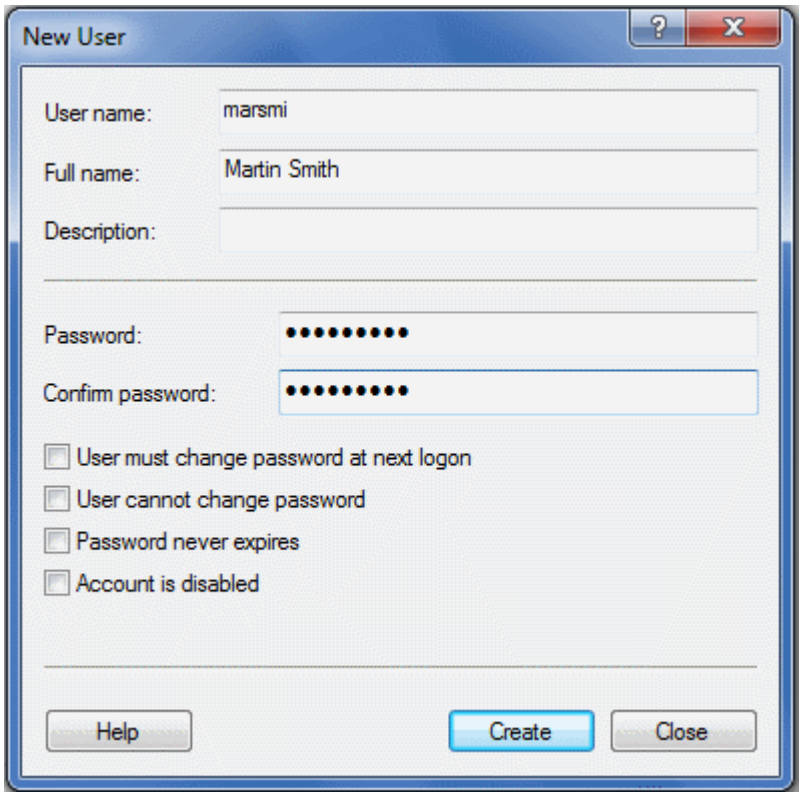
Configure the Teamwork Server side

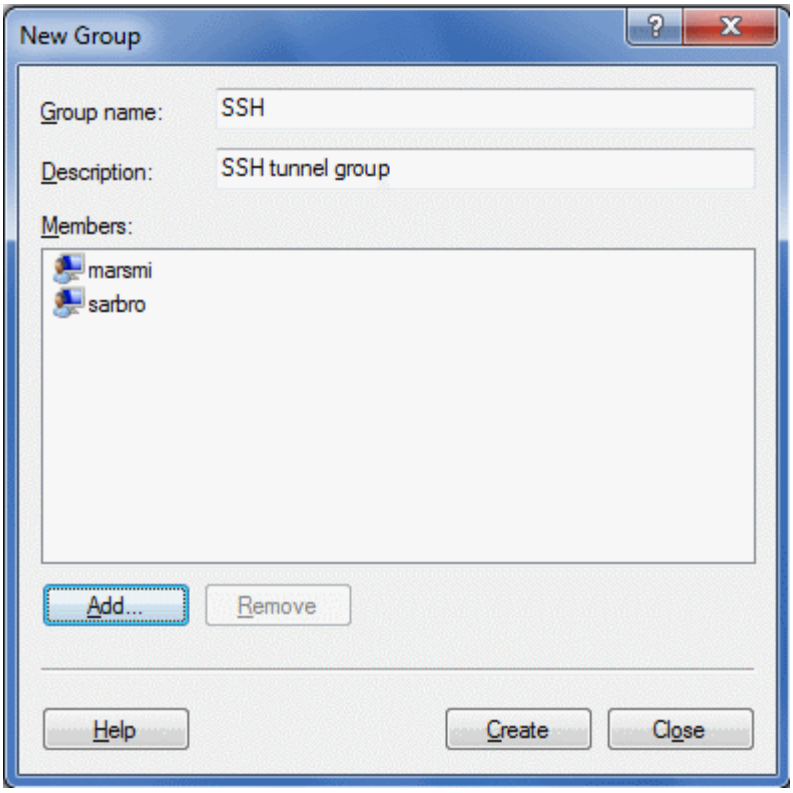
1. Log in to the Teamwork Server with administrator privileges.
2. Install OpenSSH with default settings. This will install the OpenSSH server and client on your Teamwork Server machine. A warning about editing password and group file will appear while installing. Click **OK**.
3. Create a local user for SSH tunnel. To do this correctly, click on **My Computer**, then select **Manage**. In the Local Users and Groups section right-click on **Users** and choose **New User**. The New User dialog opens.
    a. Enter a new username to log in into SSH service to establish tunneling. For example, *tunnel*.
    b. Enter the user password according to your local system policy.
    c. Clear the **User must change password at next logon** check box.
    d. Click **Create**. The local user will be created.

> This is not the same as the MagicDraw Teamwork Server user used to check out and commit UML models from/to the server. Use Teamwork Administrator to manage Teamwork users.



The New User dialog

4. Create a local group for SSH tunnel users. To do this right-click on **My Computer** and then select **Manage**. In the Local Users and Groups section, right-click on **Group** and choose **New Group**. The New Group dialog opens.
    a. Enter a new groupname, for example, *SSH*.
    b. Add the “tunnel” user to the SSH group.



The New Group dialog

5. Create SSH-aware local password file with 'tunnel' user entry. Any users in this password file will be able to log on with SSH. To create the SSH-aware local password file run command prompt (click "Start"-> "Run", then type "cmd" and click Enter) and then type the following commands:
   a. `cd C:\Program Files\OpenSSH\bin`

   b. `mkgroup -l >> ..\etc\group`

   c. `mkpasswd -l -u tunnel >> ..\etc\passwd`

6. Start OpenSSH Server service from your control panel. To do this right-click on **My Computer** and then select **Manage**. In the Services and Application section, under the Services item, right-click on the **OpenSSH Server** service and choose **Start**.
7. Test the SSH server.
   a. Type "*ssh tunnel@localhost*" from your command prompt.

> The following warning appears:
>
> ```
> The authenticity of host 'localhost (127.0.0.1)' can't be established. RSA key fingerprint is xx:xx:
> xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx. Are you sure you want to continue connecting (yes/no)?
> ```

   a. Type yes and press **Enter**. You must type the full word "yes," not just "y."
   b. Enter the password you created in step 3.
   c. A warning about nonexistent home directory appears. Please ignore it.
   d. Now you are logged in into localhost via SSH service and you can see the shell prompt.
   e. After the SSH server testing, exit the server by typing exit.

Another way to test if the SSH port (port 22) is opened on the server:

In the command prompt go to the C:\Program Files\OpenSSH\bin and type the 'netstat -na' command. You will get the list of all connections. The state of the port should be "LISTENING" while the SSH server is running.