

# Table of Contents

|   |           |
|---|-----------|
| <b>Part I Document Overview</b>                       | <b>2</b>  |
| <b>Part II Document Details</b>                       | <b>3</b>  |
| <b>Part III Setup</b>                                 | <b>4</b>  |
| 1 Download & Installation .....                       | 4         |
| 2 Configure MySQL Server .....                        | 6         |
| Windows XP Firewall Settings .....                    | 13        |
| 3 Additional Steps .....                              | 15        |
| <b>Part IV Setting up a Database, Table and Users</b> | <b>15</b> |
| 1 MySQL SQL Shell .....                               | 16        |
| 2 MySQL Administrator .....                           | 19        |
| Setting up MySQL Administrator .....                  | 20        |
| Setting up the Database .....                         | 23        |
| <b>Part V Appendix</b>                                | <b>26</b> |
| 1 Security Tips .....                                 | 26        |
| 2 ODBC Drivers .....                                  | 29        |
| 3 Security for root .....                             | 30        |
| 4 Apache 1.3x & PHP 5.x .....                         | 31        |
| <b>Index</b>  | <b>0</b>  |

# 1 Document Overview



**Author:** NETIKUS.NET Ltd  
**Date:** 1st November 2007  
**Revision:** 2.1

## MySQL Server Installation on Windows (with additional information for EventSentry)

|                         |  |
|-------------------------|--|
| <b>Title</b>            | MySQL Server Installation on Windows   |
| <b>Summary</b>          | How to install, setup and configure a MySQL installation on Windows. Includes instructions on how to setup a database for EventSentry, also covers the installation of Apache and PHP briefly. |
| <b>Software</b>         | MS Windows 2000 or higher<br>MySQL 5.x<br>Optional: Full or trial version of EventSentry   |
| <b>Hardware</b>         | Not applicable, system used for this guide is PIII 977MHz with 256Mb RAM   |
| <b>Skill Level</b>      | Beginner - Intermediate  |
| <b>Skills Required</b>  | - Basic understanding of Windows NT, 2000, 2003 or XP<br>- Basic understanding of databases<br>- Knowledge of basic SQL commands (select, update, ...) beneficial but not required             |
| <b>Acknowledgements</b> | Thanks to the MySQL database team for making a great database available for free   |
| <b>Download</b>         | <a href="http://www.netikus.net/">http://www.netikus.net/</a> (guides section)   |

## 2 Document Details

### Overview

This document describes how to install a MySQL database server on Windows 2000, mainly focusing on setting up the server with the EventSentry database and table.

The appendix also gives instructions on how to install Apache and PHP.

This guide is also useful if you are not using EventSentry as it covers mostly basic MySQL tasks.

### MySQL

MySQL is an open source relational database and can hence be used for free. It lacks some features of commercial database, but is an excellent solution for many needs, including EventSentry.

One of the downsides to MySQL is its lack of graphical administration interfaces, though this seems to be improving over time. We found the MySQL Control Center to be quite capable and easy to use, though not as appealing as other products including the MS Sql Enterprise manager.

### Why?

This guide was written to help EventSentry customers setup a reliable and affordable database server to store and consolidate event log records.

## 3 Setup

### 3.1 Download & Installation

#### Download

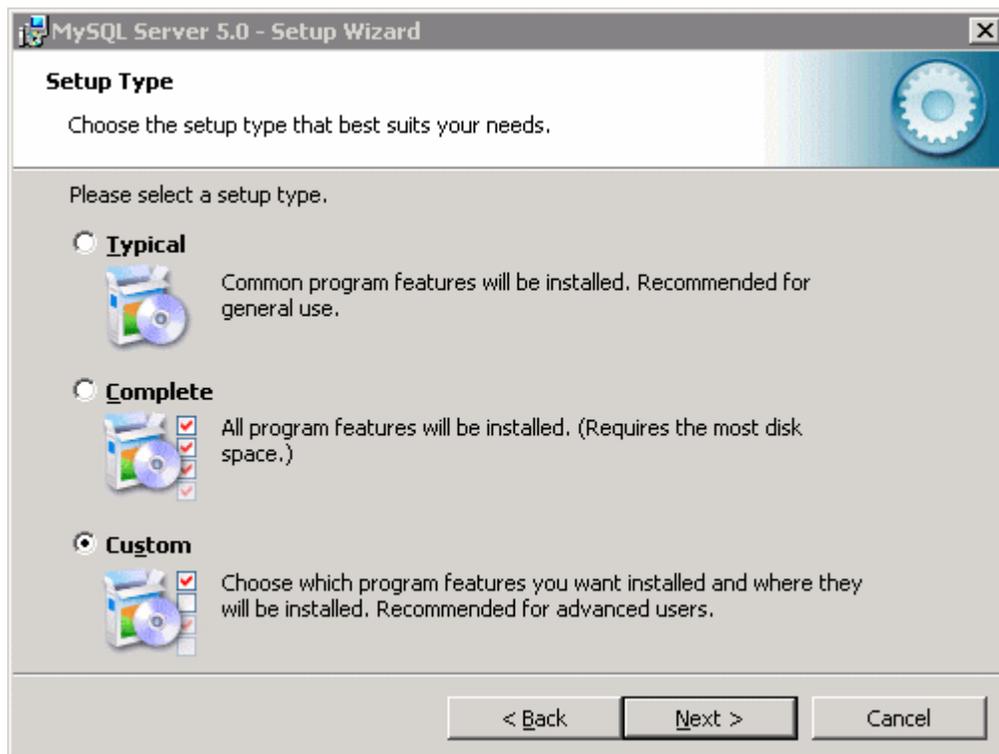
You can download the MySQL database from the MySQL website <http://www.mysql.com> by clicking on the [downloads](#) tab. Scroll down to the *MySQL database server & standard clients* section and select the latest production release of MySQL, **5.0.24a** at the time of writing.

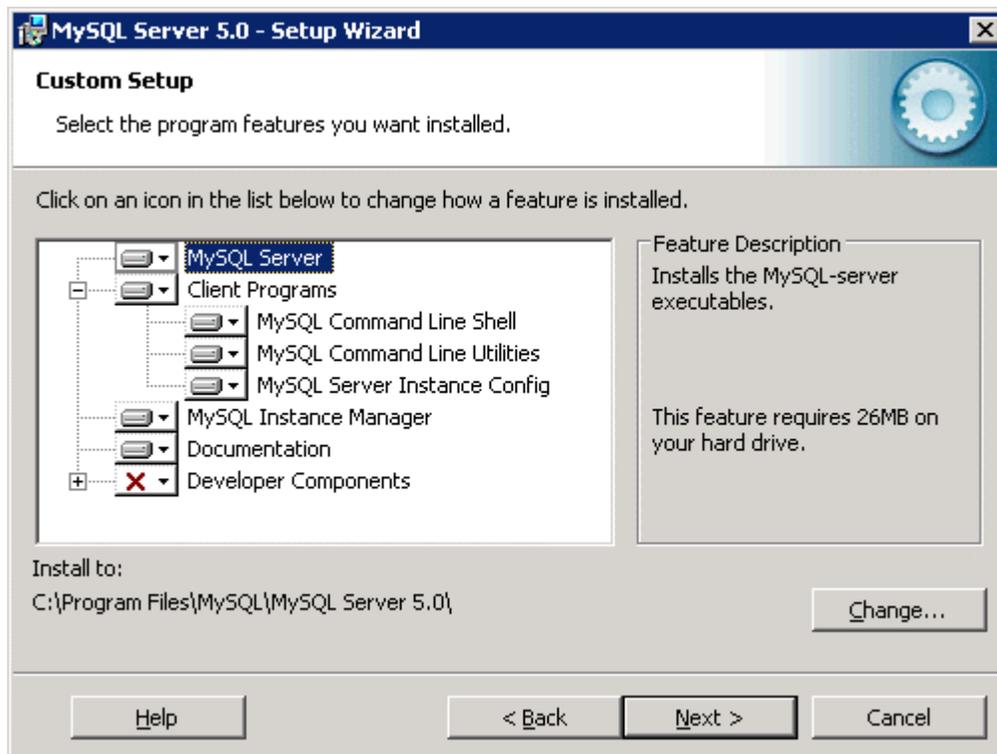


We also recommend downloading the [MySQL Administrator](#) and [MySQL Query Browser](#) from the downloads page. These applications allow you to administer your MySQL server with a graphical user interface. We will cover both ways of administration in this guide.

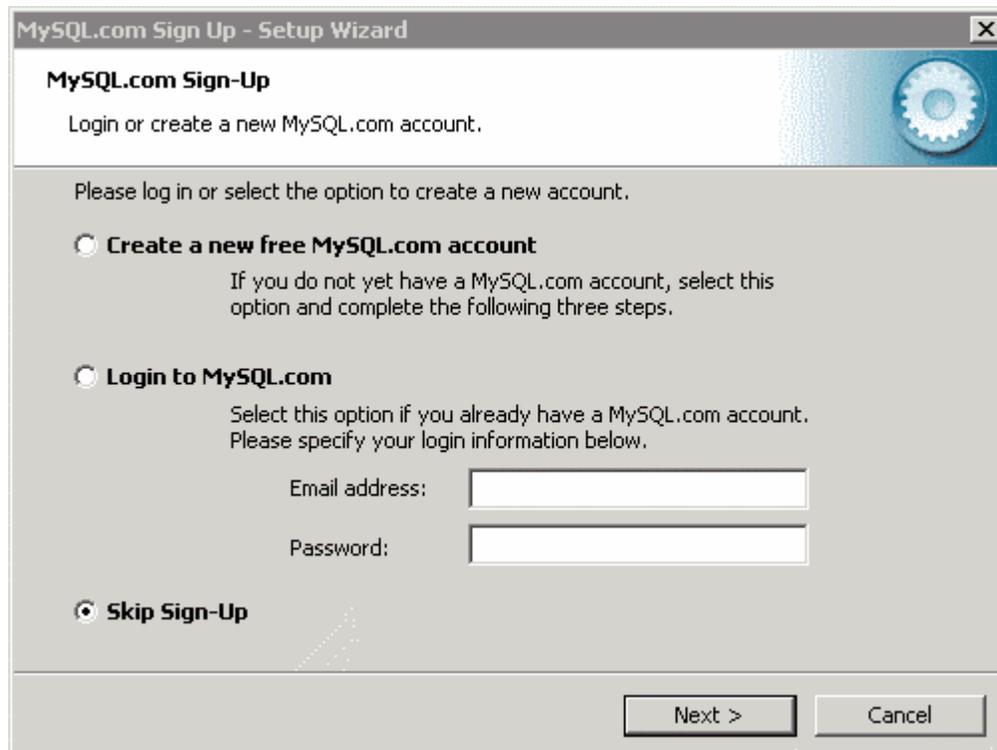
#### Installation of MySQL Server

Unzip the setup file and execute the downloaded **MSI** file. Follow the instructions below exactly when installing MySQL Server:





Review the selected packages



Skip Sign-Up



Check box to configure MySQL Server

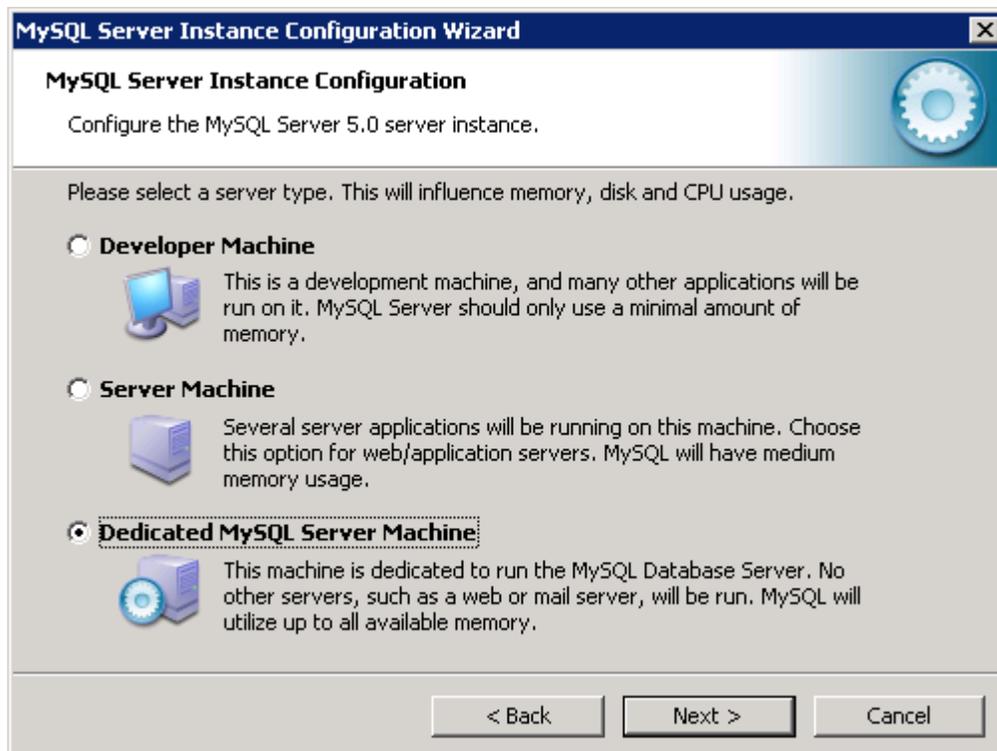
### 3.2 Configure MySQL Server

If you checked the **Configure the MySQL Server now** check box on the final dialog of the MySQL Server installation, then the **MySQL Server Instance Configuration Wizard** will automatically start.

Follow the instructions below carefully to configure your MySQL Server to run correctly with EventSentry.



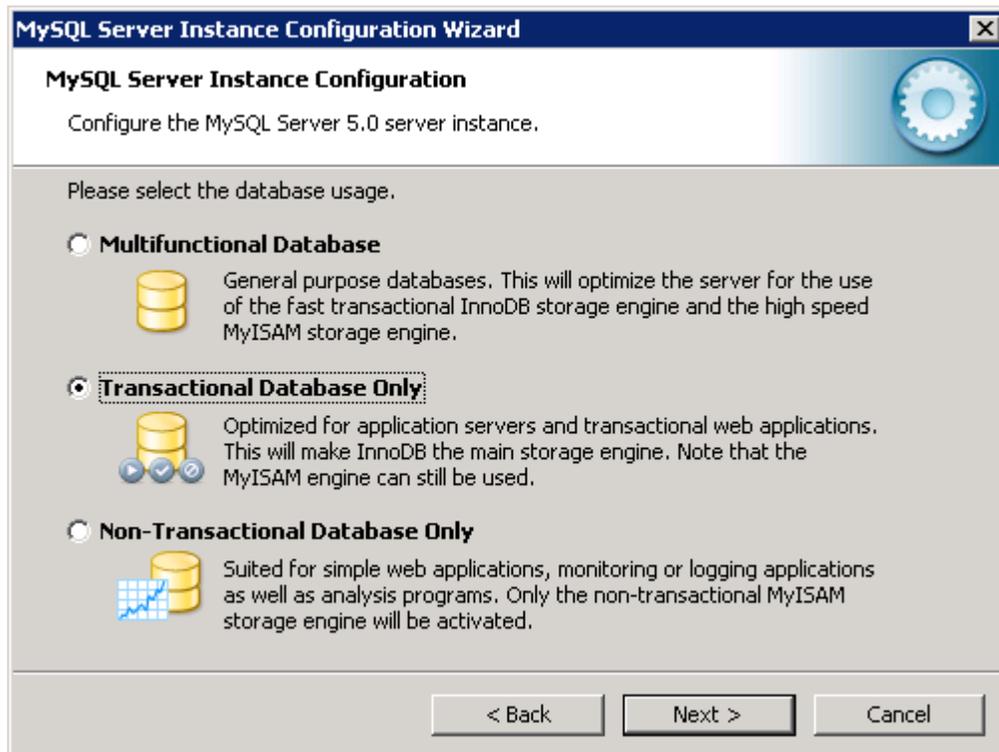
Select **Detailed Configuration**



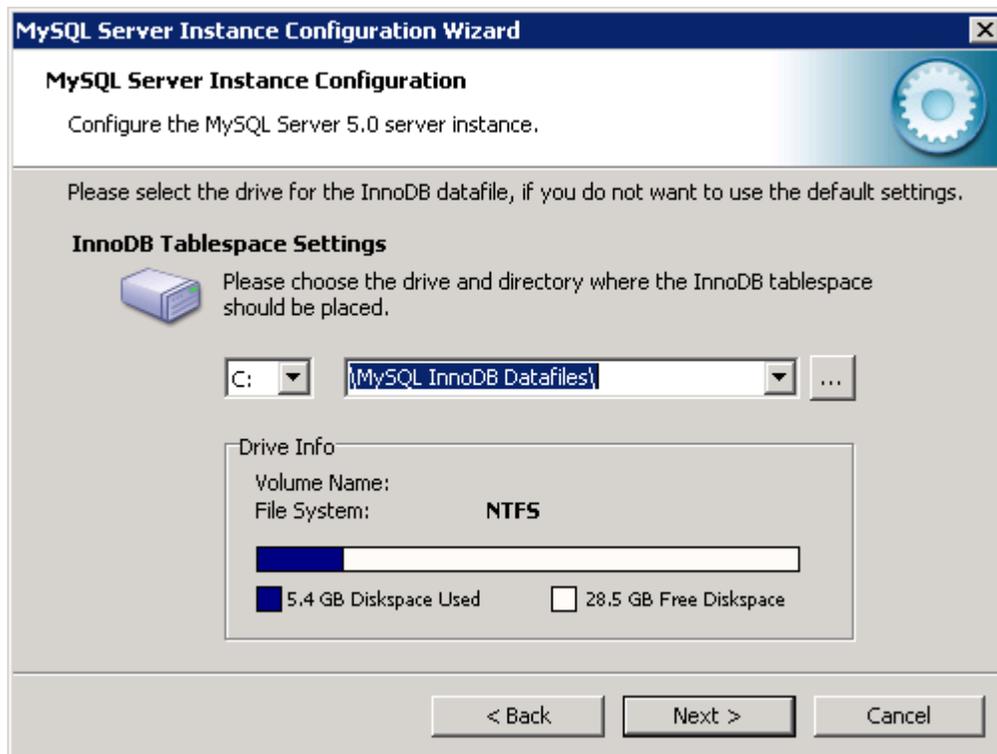
It is recommended that you use a **Dedicated MySQL Server Machine** for your MySQL database, if this is not an option then select "Server Machine".



If you selected **Dedicated MySQL Server Machine** and your MySQL service does not start after the wizard completes, then try to re-run the wizard (or re-install) MySQL, but this time select the **Server Machine** option.



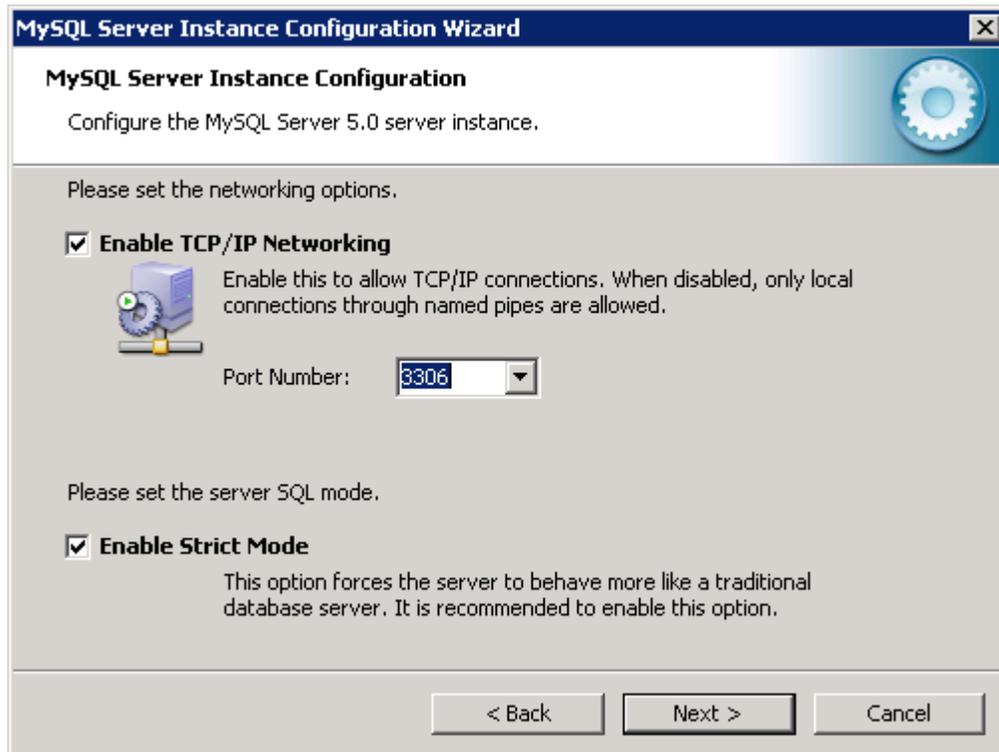
Select **Transactional Database Only**, this will make sure that **InnoDB** is the main storage engine.



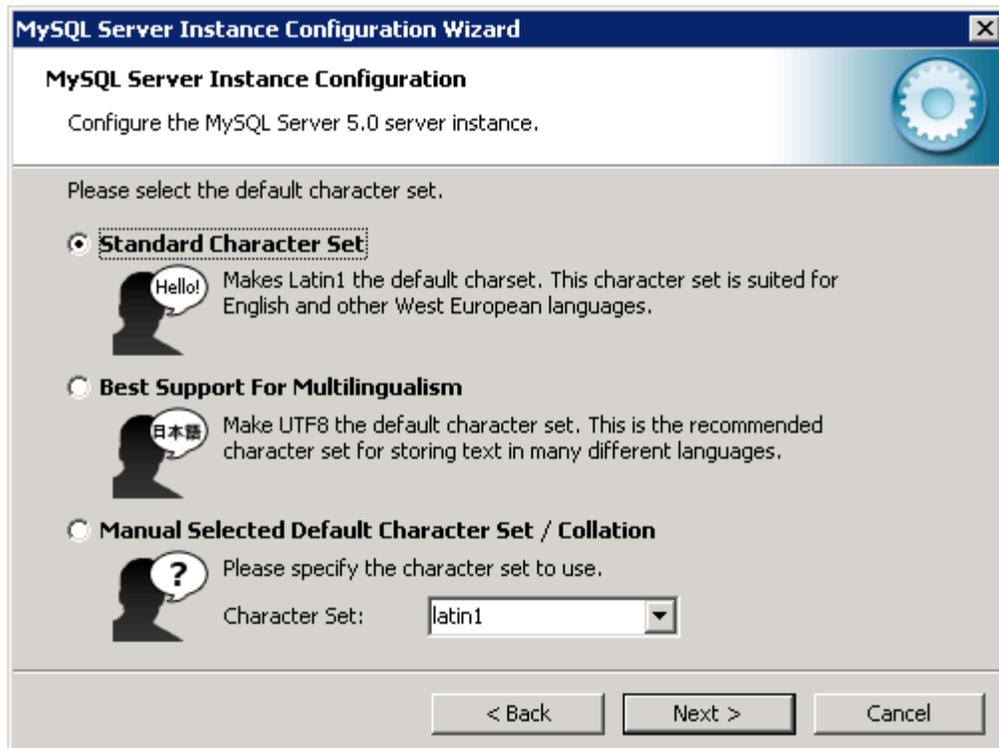
Select the drive where the database files will be stored.  
Select the drive on the fastest drive(s) on your server.



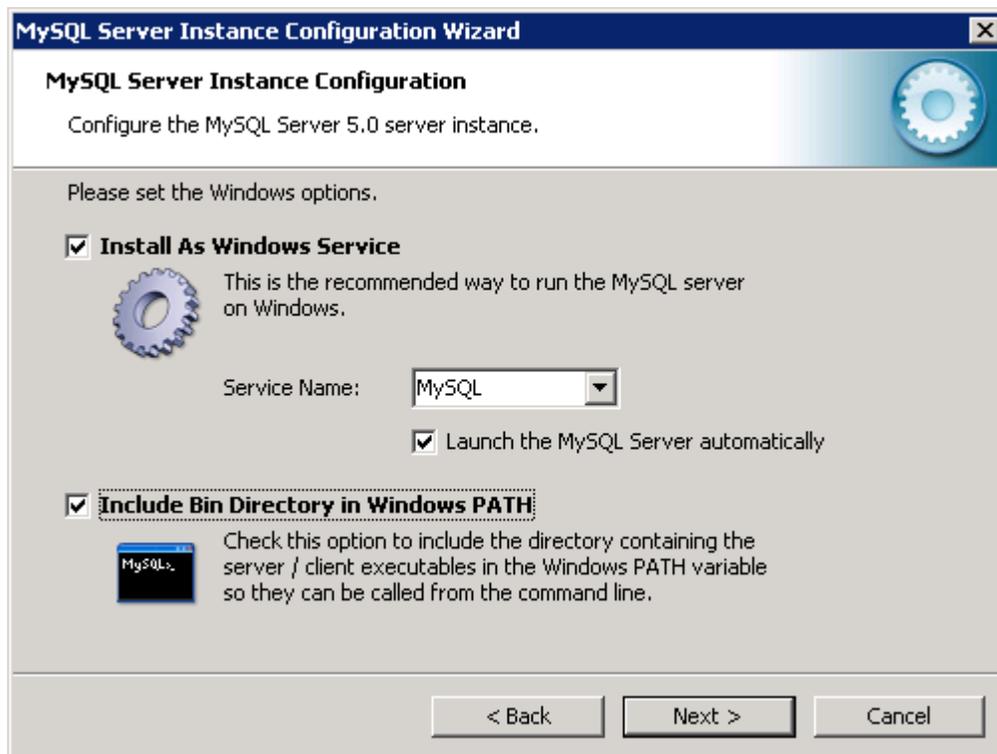
Enter the number of agents you are monitoring, multiplied by two.  
For example, if you are monitoring 20 servers then enter **40**.



It is recommended that you leave the default port **3306** in place, however EventSentry will also work with non-standard ports if necessary.



Select the **Standard Character Set** for EventSentry.



It is **highly recommended** that you run the MySQL Server as a Windows service and include the binary directory in the search path.

**MySQL Server Instance Configuration Wizard**

**MySQL Server Instance Configuration**  
Configure the MySQL Server 5.0 server instance.

Please set the security options.

**Modify Security Settings**

 New root password:  Enter the root password.

 Confirm:  Retype the password.

Enable root access from remote machines

**Create An Anonymous Account**

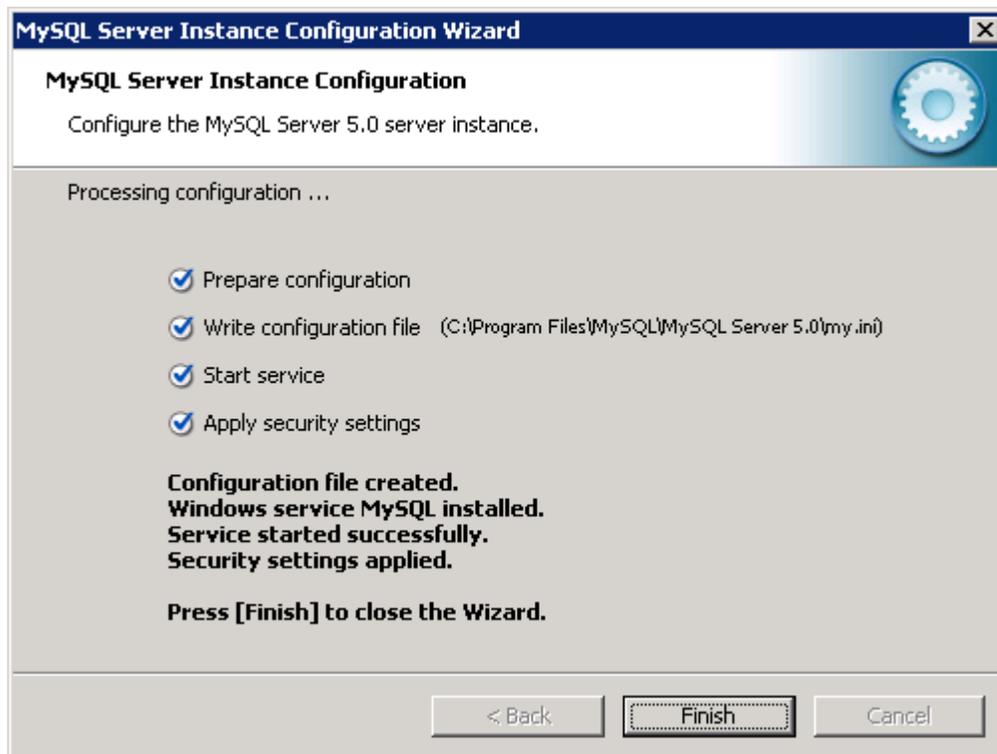
 This option will create an anonymous account on this server. Please note that this can lead to an insecure system.

< Back    Next >    Cancel

Specify a secure **root** password, you may want to check the box **Enable root access from remote machines** if you plan on administering your **MySQL** server from your workstation or other servers.



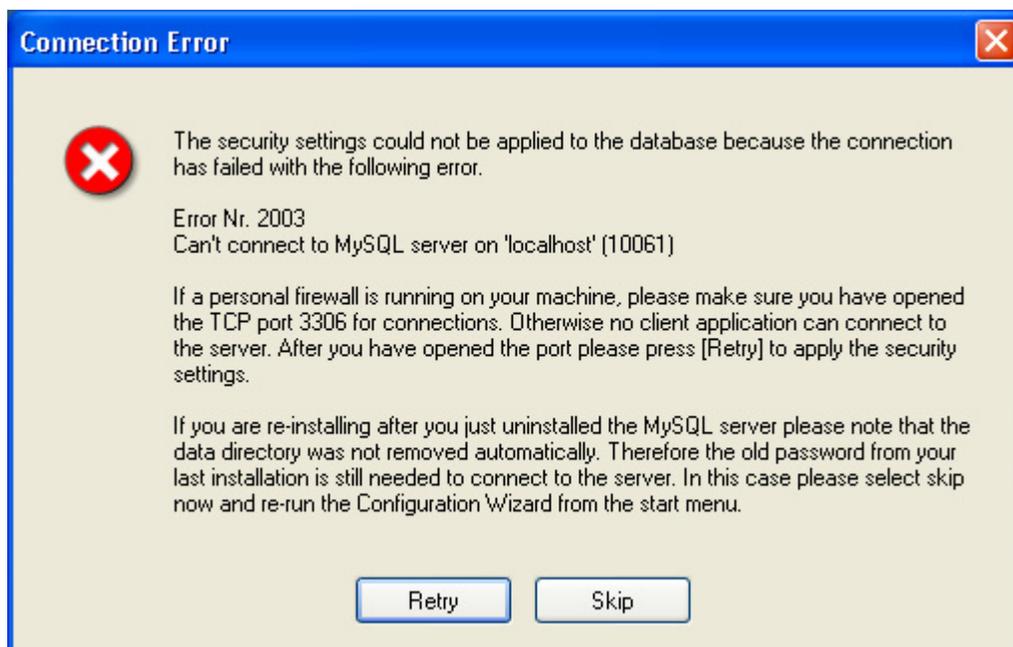
If you are getting an error message after clicking the **Next** button, then please see the [Windows XP Firewall Settings](#) chapter for more information.



If you see this dialog then your instance was setup correctly.

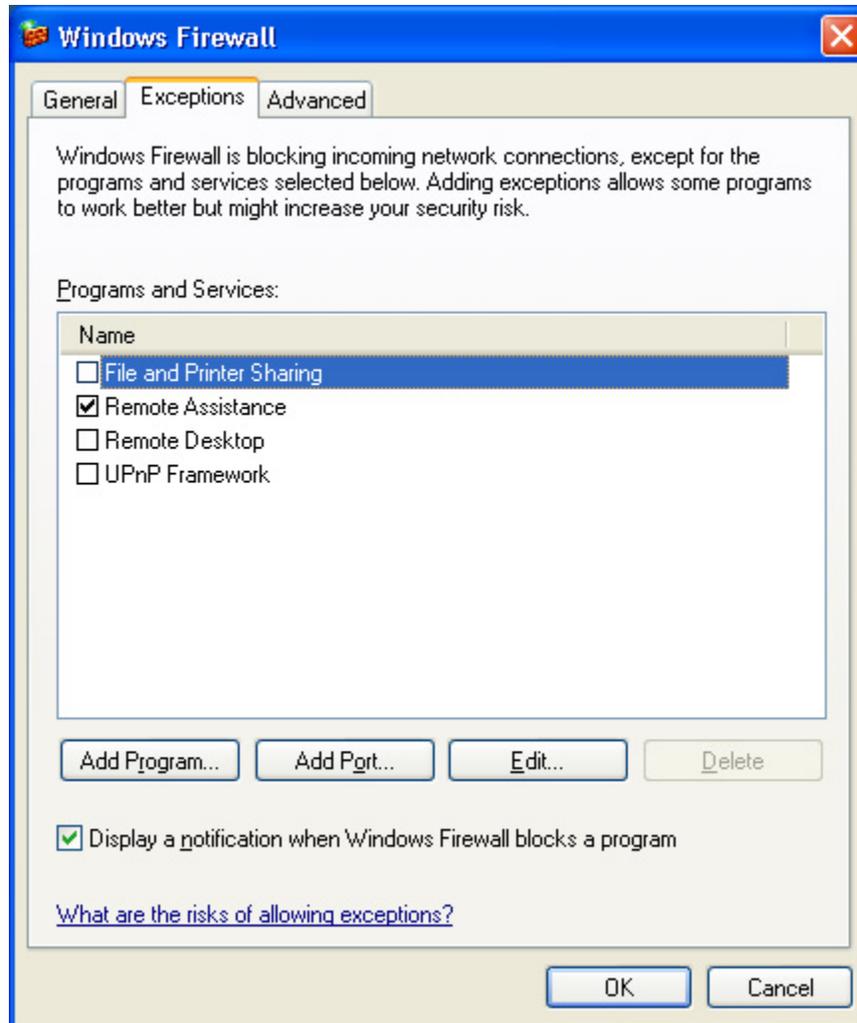
### 3.2.1 Windows XP Firewall Settings

If you are installing MySQL on a Windows XP workstation, or any other computer that has a firewall enabled, and the wizard fails with an error message similar to the one shown below (Can't connect to MySQL server on 'localhost'), then you will have to exclude the MySQL daemon from your firewall configuration.



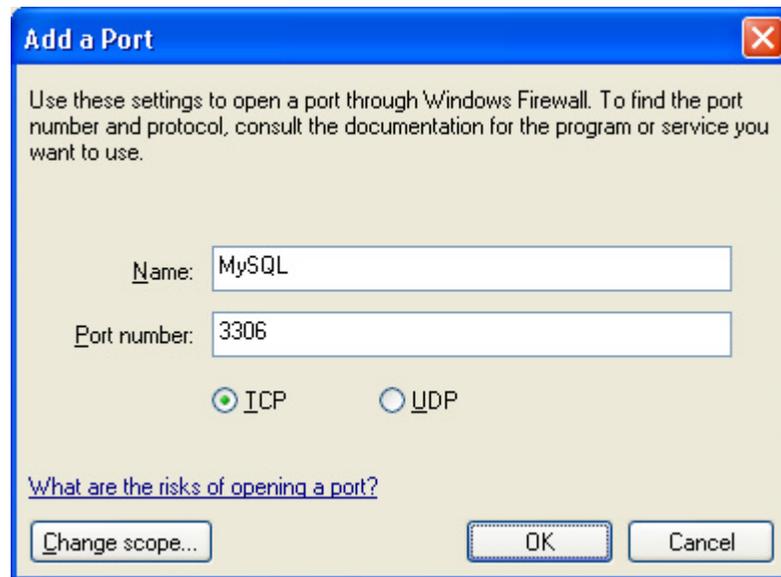
On Windows XP, you can exclude MySQL from the firewall by following the steps below:

1. Navigate to Start -> Settings -> Control Panel -> **Windows Firewall**



Select the **Exceptions** tab and click **Add Port**

2. In the resulting dialog, enter the information as shown in the screenshot:



After clicking OK twice, return to the MySQL error message and select **Retry**. MySQL should now be able to create the instance correctly.

### 3.3 Additional Steps

After you installed MySQL you will need to install the ODBC drivers on all machines which are running EventSentry and need to write any type of information to the MySQL database. We also recommend that you download and install the MySQL Administrator and MySQL Query Browser.

#### Installation of the MySQL ODBC Drivers

In order to setup the MySQL tables later, you will need to download and install the MySQL ODBC drivers. You can download the latest ODBC drivers for Windows from <http://dev.mysql.com/downloads/connector/odbc/3.51.html>. Simply run the setup application and install the ODBC drivers once you downloaded the file.

Please see [Rolling out the MYSQL ODBC Driver](#) for information on how to automatically install the MySQL ODBC driver on multiple machines in an ActiveDirectory environment.

#### Installation of the MySQL Administrator and Query Browser

Simply execute .msi files and follow the instructions on the screen. These applications uses little disk space and a restart is not required after the installation. Once installed you can launch the applications by double-clicking their respective icons on the desktop.

You can download both utilities from <http://dev.mysql.com/downloads/query-browser/index.html>.

## 4 Setting up a Database, Table and Users

Now that our core MySQL installation is pretty much complete we can create a separate database for EventSentry. You can follow these steps even if you are not planning on using EventSentry to learn the basics of creating a database, tables and users. You can delete this database again after you have completed the tutorial.

You can create the database, table and users either through the command-line mysql shell, or with the MySQL Control Center. For beginners we recommend choosing the SQL shell first and then taking a look at the MySQL Administrator.

In a nutshell we will have to perform the following tasks:

- Create a new database
- Run the EventSentry Database Setup Wizard

[1. MySQL SQL Shell](#)

[2. MySQL Control Center](#)

## 4.1 MySQL SQL Shell

start the SQL shell by typing

```
mysql -u root -p
```

Note that you will need to be in the c:\mysql\bin directory if you have not added the c:\mysql\bin directory to your path. All commands shown in this chapter will need to be typed in the SQL shell.

### Creating a New Database

Databases are always created with the **create database** command, so type

```
create database EventSentry;
```

to create the EventSentry database.

### Setting up the tables, indexes and views for EventSentry

Starting with version 2.50, the web reports of EventSentry require several tables to be setup. Unlike earlier versions where you had to setup the tables manually, EventSentry now ships with a [Database Setup Wizard](#) that will create all tables, indexes and users automatically for you.

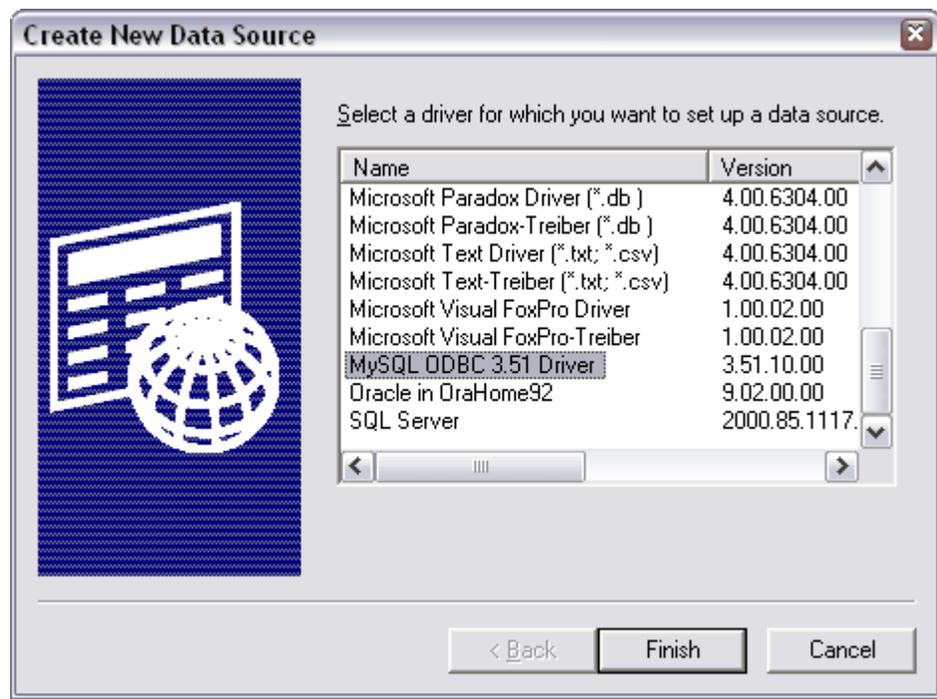
To setup the tables you will first have to create a system DSN and then run the database setup wizard.

#### 1. Installing the ODBC drivers

If you haven't already downloaded and installed the ODBC drivers, then you will need to do this now. Please see [Download & Installation](#) for more information.

#### 2. Creating a system DSN

Navigate to Start -> Programs -> Administrative Tools and select the **Data Sources (ODBC)**. Click on the **System DSN** tab and then click on **Add**. On the next screen, select the **MySQL ODBC 3.51 Driver** from the bottom of the list.



After clicking finish you should be presented with the ODBC setup dialog. Make sure that you enter all information correctly in this dialog and then click the **Test** button:



You will need to replace **mysql-srv** in the **server** field with the computer name of the host where you installed MySQL.

### 3. Running the Database Setup Wizard

If you installed EventSentry with database support, then you will find the **Database Setup Wizard** in **Start -> Programs -> EventSentry**. Run this wizard and follow the instructions. The wizard will ask you for the system DSN pointing to the database and the initial password for the **eventsentry\_svc** and **eventsentry\_web** user accounts.

Once the wizard has completed creating all the tables, indexes and user accounts, you can verify that all tables were created. First, change the current context to the EventSentry database by typing

```
use EventSentry;
```

and then display all tables with this command:

```
show tables;
```

command which should show output similar to this:

```
+-----+
| Tables_in_eventsentry |
+-----+
```

```
esapphistory
esappname
esapppublisher
esappstatus
esdiskspace
esenvironment
eseventlogcategory
eseventlogcomments
eseventlogcomputer
eseventlogdata
eseventlogfilename
eseventlogfilepath
eseventlogfilter
eseventloggroup
eseventlogid
eseventloglocation
eseventloglocationmapping
eseventloglog
eseventlogmain
eseventlogsource
eseventlogtype
eseventloguser
esgroupmapping
esheartbeathistory
esheartbeatldescription
esheartbeatlstatus
esheartbeatltype
esheartbeatpingtracking
esheartbeatstatus
eslogontracking
esmotiontracking
esnessuskb
esnessuslog
esnessusport
esperformance
esperformancecounter
esperformanceinstance
esperformancename
esprintcost
esprintdocuments
esprintprinters
esprintracking
espstracking
essearchadvanced
essearchsimple
esservicehistory
esservicekey
esservicename
esservicestatus
esstrings
essysinfo
```

```
+-----+
51 rows in set (0.00 sec)
```

## 4.2 MySQL Administrator

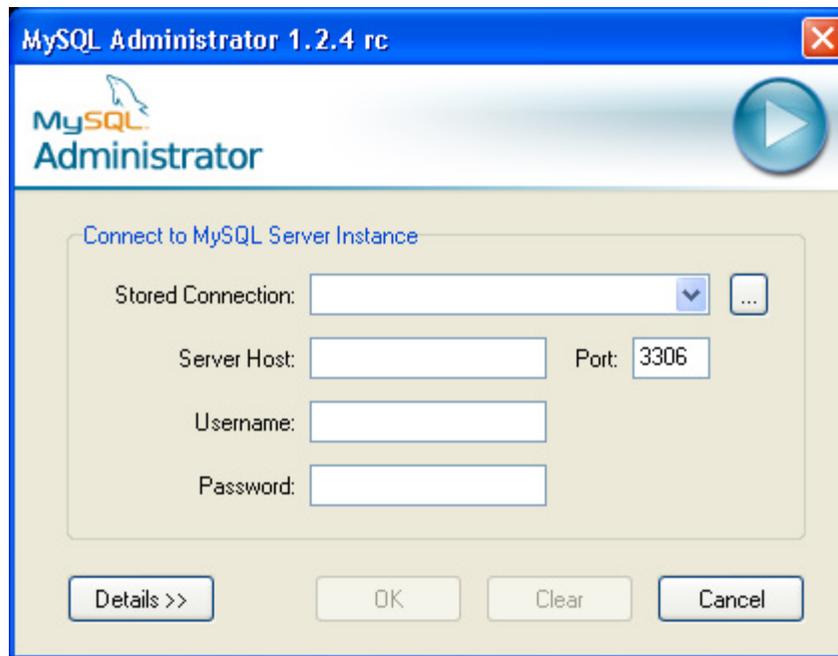
You don't have to use the command line interface to create databases, tables and change permissions. MySQL now also offers the **MySQL Administrator** which offers an attractive user interface to perform most tasks. This chapter describes how to setup the database, tables and permissions using the MySQL Administrator.

[1. Setting up MySQL Administrator](#)

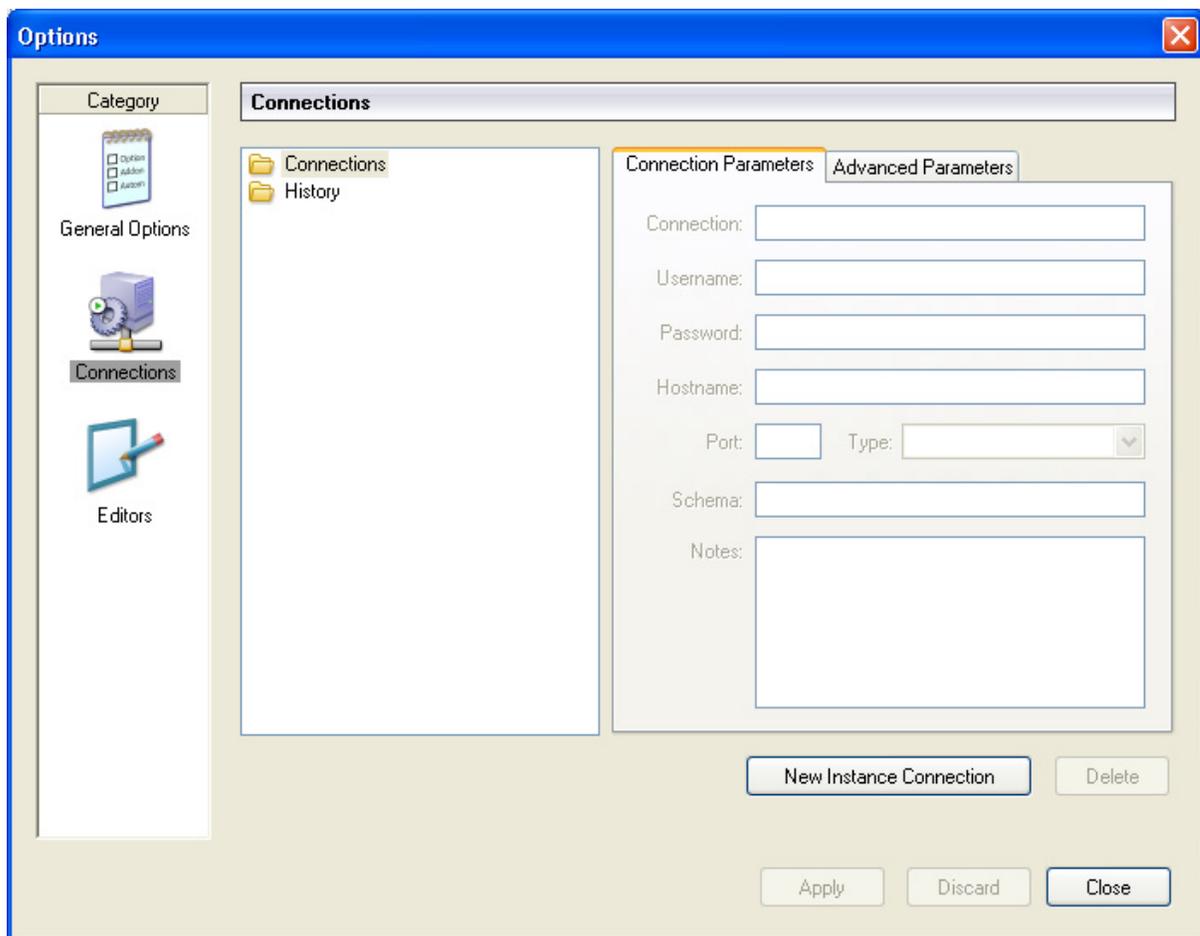
[2. Setting up the Database](#)

#### 4.2.1 Setting up MySQL Administrator

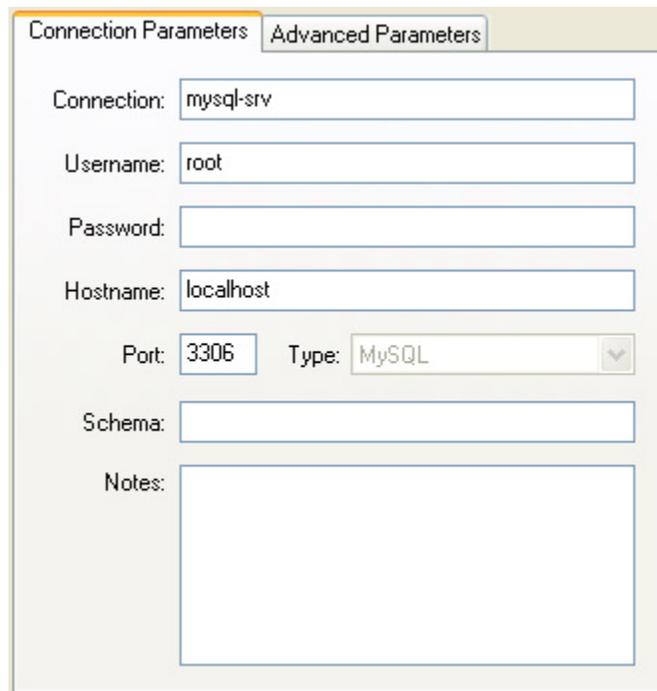
When you start MySQL Administrator for the first time then you will see a window similar to this:



We will now add and register our MySQL instance in the **MySQL Connections** window so that we don't have to type the hostname and username every time we need to connect to our server. Click on the button with the three dots to display the options dialog:



Fill in all the required information so that you have a screen similar to the one shown below and click the **Apply Changes** and **Close** button:



The screenshot shows the 'Connection Parameters' tab of the MySQL Administrator interface. The fields are filled with the following information:

- Connection: mysql-srv
- Username: root
- Password: (empty)
- Hostname: localhost
- Port: 3306
- Type: MySQL (dropdown menu)
- Schema: (empty)
- Notes: (empty text area)

Now you can connect to the server by filling in the password and clicking on the OK button:

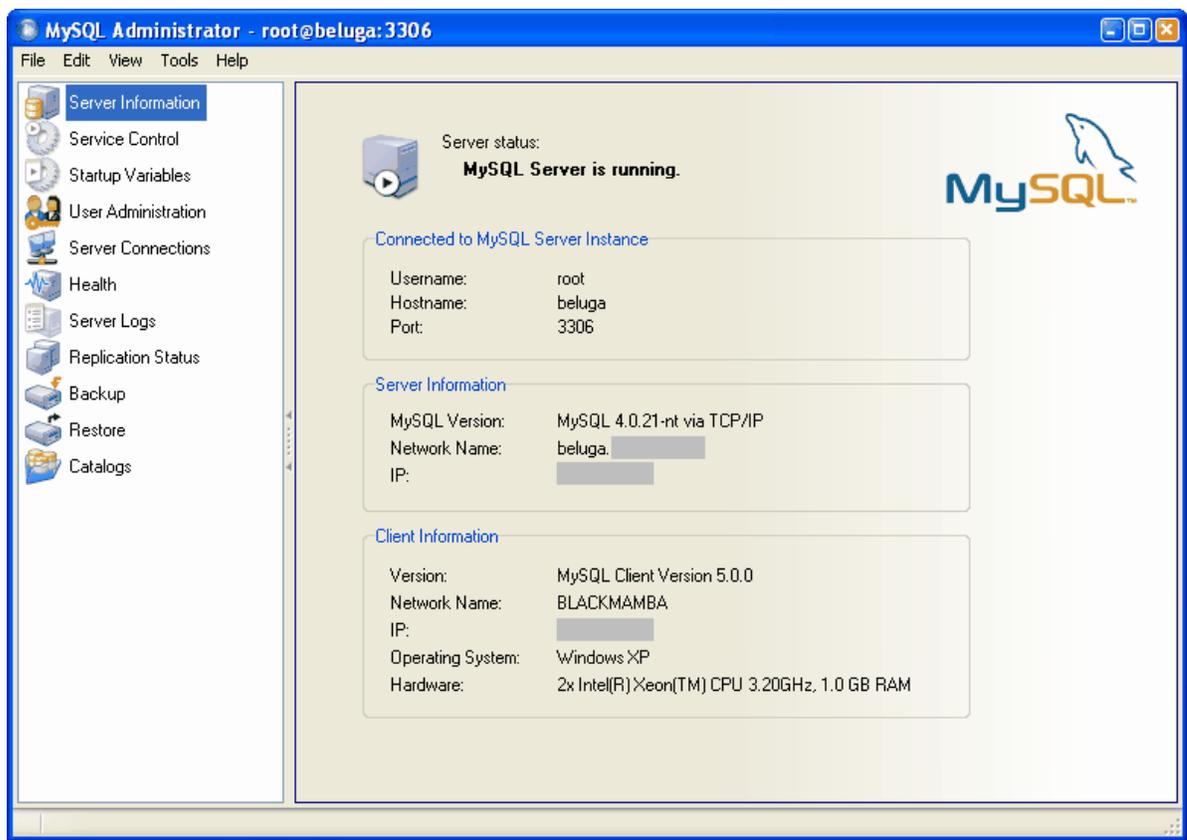


The screenshot shows the 'Connect to MySQL Server Instance' dialog box in the MySQL Administrator 1.2.4 rc application. The fields are filled with the following information:

- Stored Connection: mysql-srv (dropdown menu)
- Server Host: localhost
- Port: 3306
- Username: root
- Password: (masked with asterisks)

Buttons at the bottom: Details >>, OK, Clear, Cancel.

and you should be presented with the server information screen:

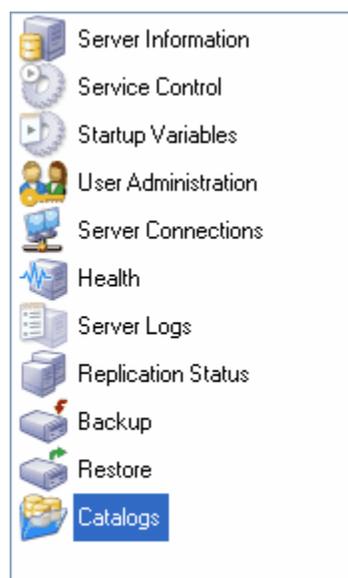


MySQL Administrator is now setup and we can start creating the database, tables etc.

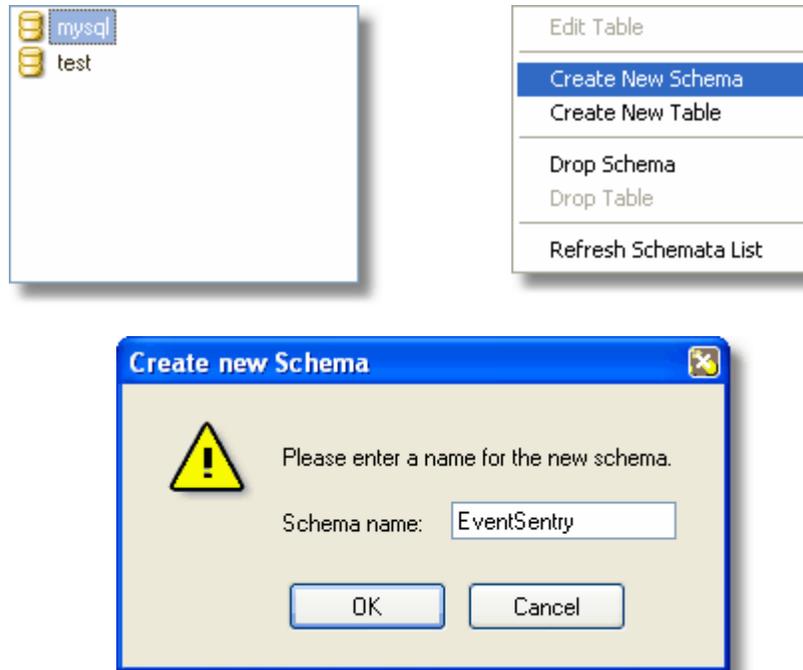
## 4.2.2 Setting up the Database

### Creating the Database

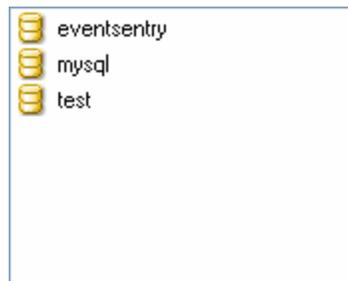
Creating the database is quite easy. First select **Catalogs** in the left pane



And then right-click into the lower left rectangle (Schemata) that will show the **mysql** and the **test** databases (schemas). From the drop-down menu select **Create New Schema** to create a new database for EventSentry:



The newly added **EventSentry** database will now show up in the list:



and we are ready to create the tables, indexes and users with the wizard.

### Setting up the tables, indexes and views for EventSentry

Starting with version 2.50, the web reports of EventSentry require several tables to be setup. Unlike earlier versions where you had to setup the tables manually, EventSentry now ships with a **Database Setup Wizard** that will create all tables, indexes and users automatically for you.

To setup the tables you will first have to create a system DSN and then run the database setup wizard.

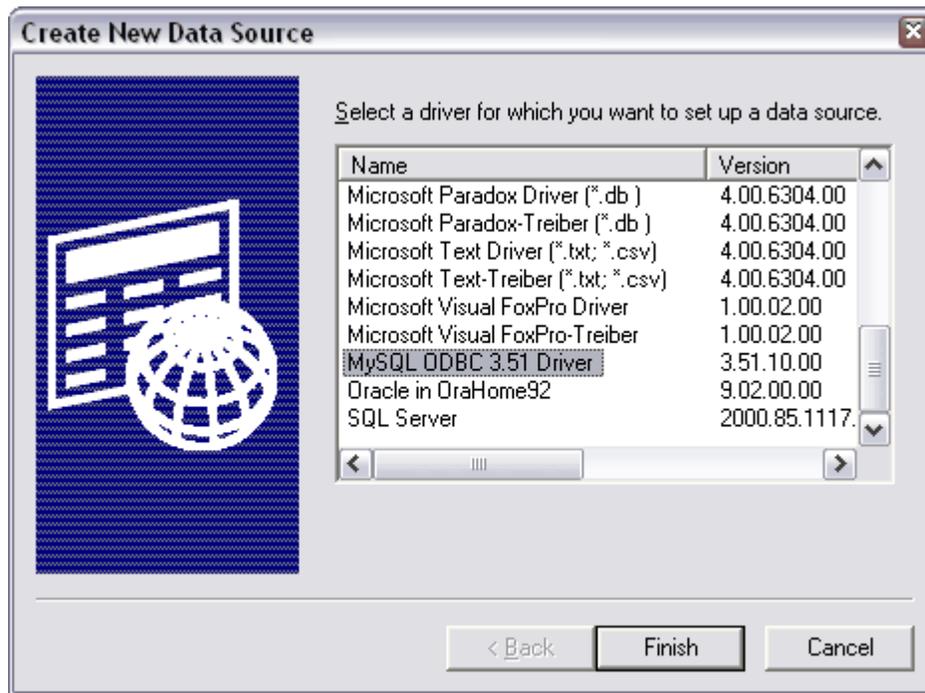
#### 1. Installing the ODBC drivers

If you haven't already downloaded and installed the ODBC drivers, then you will need to do this now. Please see [Download & Installation](#) for more information.

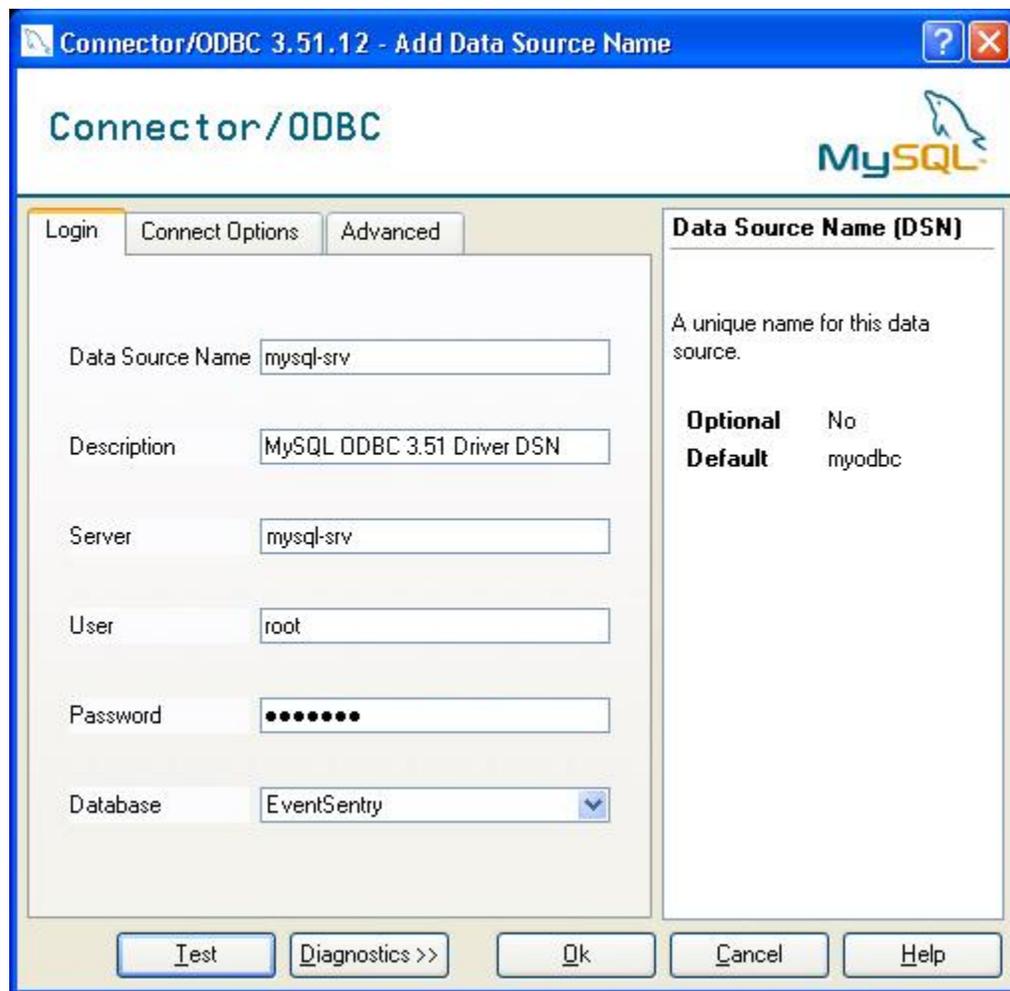
#### 2. Creating a system DSN

Navigate to Start -> Programs -> Administrative Tools and select the **Data Sources (ODBC)**. Click on the **System DSN** tab and then click on **Add**. On the next screen, select the **MySQL ODBC 3.51 Driver**

from the bottom of the list.



After clicking finish you should be presented with the ODBC setup dialog. Make sure that you enter all information correctly in this dialog and then click the **Test** button:



### 3. Running the Database Setup Wizard

If you installed EventSentry with database support, then you will find the **Database Setup Wizard** in **Start -> Programs -> EventSentry**. Run this wizard and follow the instructions. The wizard will ask you for the system DSN pointing to the database and the initial password for the **eventsentry\_svc** and **eventsentry\_web** user accounts.

## 5 Appendix

### 5.1 Security Tips

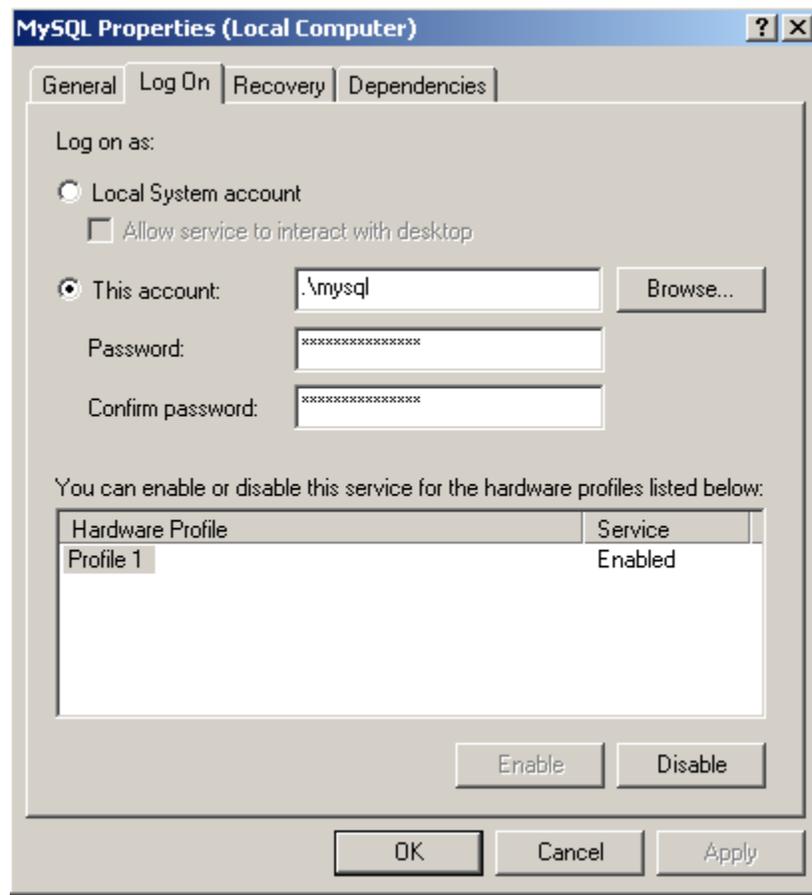
This chapter contains useful tips on how to secure a MySQL installation.

#### Changing the Service User Account

By default the MySQL service runs as the **LocalSystem** account which might a security problem if your database server is connected to non-trusted network. We recommend changing the service to run under a different user account.

1. Create a new user account, for example **MySQL** and give this user account **no special permissions**.
2. In the services control panel (Administrative Tools) double-click the MySQL service and select

the **Log On** tab. Click on **This account** and select the user account you just created, then click OK.

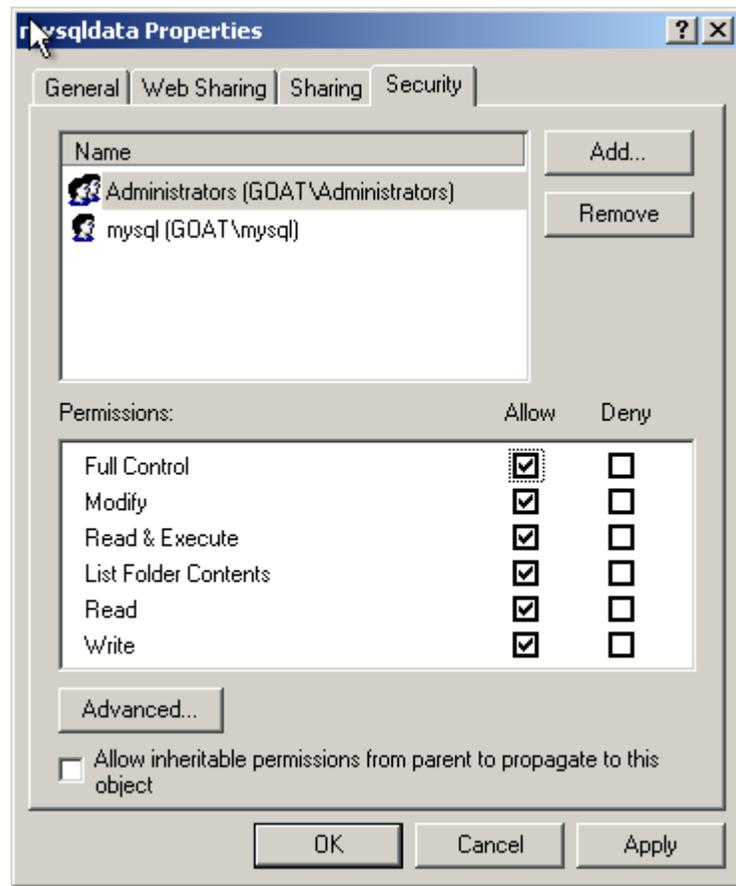


3. Restart the service to make the changes effective

### Adjusting Access Rights on the Data File directory

We also need to change the access permissions on the directory where the data files are stored, `C:\MySQL InnoDB Datafiles\` by default. This directory gives everybody full permissions by default.

This directory should really only be accessible to Administrators and the MySQL user account we just created. Configure the access rights as shown below, giving both **MySQL** and Administrators **FULL ACCESS** to the folder.



### Changing the default TCP port 3306

It is sometimes a good idea to change the default port MySQL is listening on for remote connections. This can be done by adding the line

```
port = 9754
```

to the my.ini file in the [mysqld] section. The **my.ini** file is usually located in the installation folder of your MySQL installation. You will need to restart the service for this change to become effective. You will also need to make sure that connections from untrusted networks, such as the Internet, are sufficiently protected with a firewall or similar device.

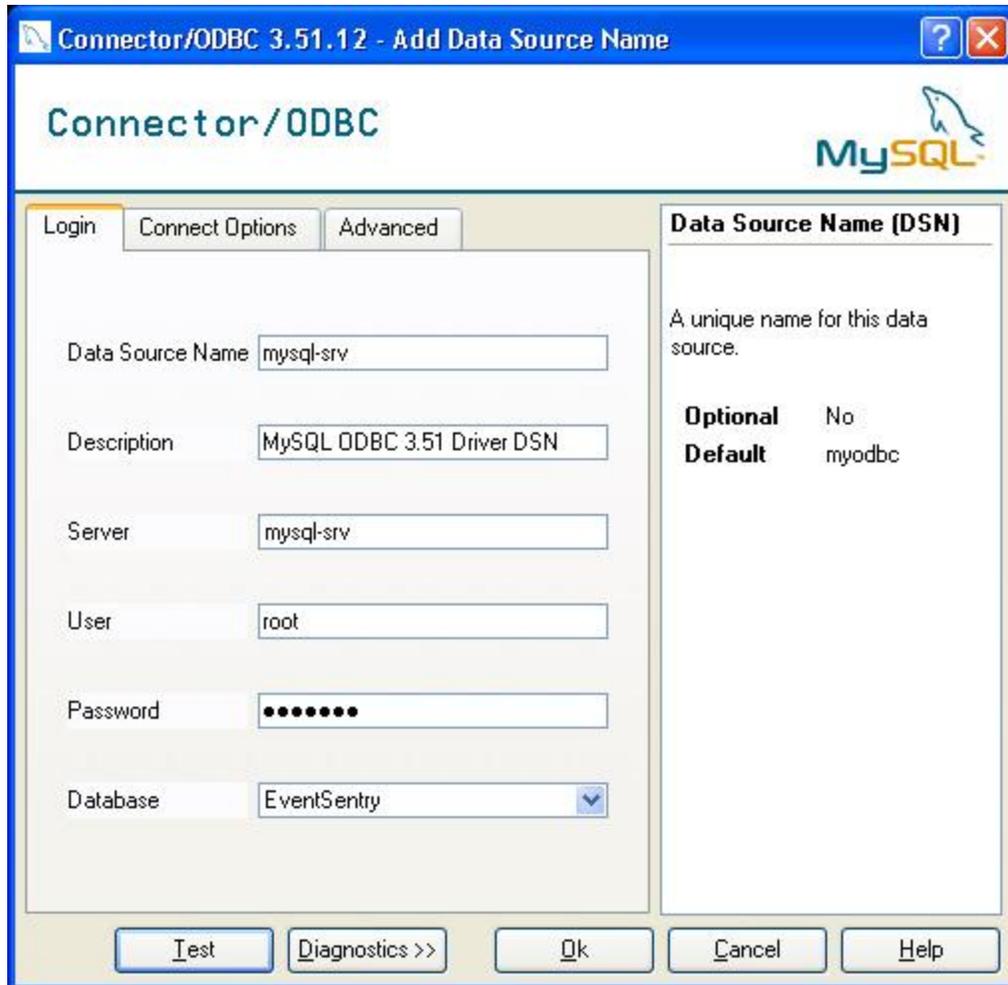
### Staying Up To Date

You need to apply patches and software updates as soon as they become available to avoid security problems and worm infections. To stay informed subscribe to the **low volume** [MySQL Announcement mailing list](#).

## 5.2 ODBC Drivers

A common way to access databases for Windows clients (including the EventSentry agent) is to use ODBC. Naturally, MySQL ODBC drivers are not shipped with the Windows Operating System and must be installed manually on the clients.

You can download the latest ODBC drivers from <http://dev.mysql.com/downloads/connector/odbc/3.51.html>. The installation and configuration are straightforward and do not require a reboot. The screenshot below shows the ODBC screen of MySQL.



We recommend using [AutoAdministrator](#) if you need to roll out MySQL ODBC drivers and DSN names to multiple machines. If you have Active Directory then you can also roll out the MySQL ODBC drivers using Group Policy, [click here for more information](#).

## 5.3 Security for root



This chapter applies to MySQL 4.x, which is no longer supported with EventSentry. The SQL commands shown in this chapter however still apply to MySQL 5.x and can be used to manipulate user accounts using the **MySQL shell**.

The root user does not have a password by default which is a security risk and needs to be changed immediately. We will change the root password from the command line using the mysql SQL shell. Open the command prompt and follow the instructions in the screenshot:

```

C:\WINNT\system32\cmd.exe

C:\mysql\bin>mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2 to server version: 4.0.17-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use mysql
Database changed
mysql> select user,host from user;
+-----+-----+
| user | host |
+-----+-----+
|      |      |
| root | build |
|      | build |
| root | localhost |
|      | localhost |
+-----+-----+
4 rows in set (0.06 sec)

mysql> update user set password=PASSWORD('complexpwdhere') where user='root';
Query OK, 2 rows affected (0.02 sec)
Rows matched: 2  Changed: 2  Warnings: 0

mysql> delete from user where user='';
Query OK, 2 rows affected (0.02 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.02 sec)

mysql> exit
Bye
C:\mysql\bin>_

```

- First we connect to the SQL instance as the **root** user by using the **-u** option. We do not have to specify a password since the root user does not have a password by default.
- Then we change the database to the built-in **mysql** database, that contains all usernames among other things.
- The select command here shows that four user accounts exist by default, two for the user root and two anonymous ones.
- We change the password of both root user accounts (explanation for both is below) by using a standard SQL update command. The **PASSWORD()** function is used to create the password hash, just specifying the password in quotes would not work.
- We then remove the anonymous user account with a delete statement.
- Changes to the user accounts do not always become effective immediately, so we force this internal update by issuing the **flush privileges** command.

After typing `exit` we have successfully remove two unneeded user accounts and set a password for the root user.

Unlike other database servers, MySQL allows you to link a database user with a hostname. This allows you to create different users (and hence different permissions) depending on where a user is connecting from.



For example, by default there are two root accounts with different **host** values. One account has the host value set to **localhost**, whereas the other has it set to **build**. This means that you can restrict from which users can log on using the **root** (or any account for that matter) account. The most commonly used host name is the percentage character **%** - a wildcard matching all host names.

This feature is not relevant to us right now since we set the same password for both root accounts, but it's important and helpful to know that this feature exists. When you connect to a MySQL database then the server will always perform a reverse lookup to match the correct username.

From now on we can no longer just type `mysql -u root`, but instead will need to specify the password we have just set above by typing `mysql -u root -p`. The `-p` switch tells the application to prompt us for the password.

```

C:\WINNT\system32\cmd.exe
C:\mysql\bin>mysql -u root
ERROR 1045: Access denied for user: 'root@localhost' (Using password: NO)
C:\mysql\bin>mysql -u root -p
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4 to server version: 4.0.17-nt
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> exit
Bye
C:\mysql\bin>

```

#### Connecting remotely with the MySQL Administrator or MySQL Query Browser

Please note that thus far you can only connect to the MySQL server from the localhost or a host with the name "build". You will need to run the following statements in order to get **root** access from remote hosts as well:

- `update user set host='%' where host='build';`
- `flush privileges;`

This will allow you to connect to your MySQL server from any host using the root user.

## 5.4 Apache 1.3x & PHP 5.x



Please note that the EventSentry web reports **no longer work with PHP and Apache**.

When running the MySQL database then you might also want to run the Apache web server using PHP as a scripting interpreter.

## Apache

Download the latest version of the 1.3 series of Apache from <http://httpd.apache.org/download.cgi>. Note that the 2.x series of Apache is preferable, however PHP does not officially support the 2.x release of Apache at the time of writing - though we did not experience any problems.

When installing Apache make sure that you select the option

**for All Users, on Port 80, as a Service -- Recommended.**

Also make sure that the Internet Information Server (IIS), if installed, is either reconfigured for a port other than 80 or not running to avoid conflicts with the Apache web server.

## PHP

You can download the latest version of PHP from <http://www.php.net/downloads.php>. Please note that the PHP pages included with EventSentry were tested with the 5.x release of PHP.

After installing the software you will need to make changes to both the Apache configuration file `httpd.conf` (usually found in the `c:\program files\apache group\apache\conf` directory) and the PHP configuration file `php.ini` (located in `%systemroot%`).

1. Add this line to the **httpd.conf** file below the other `LoadModule` lines:

```
LoadModule php5_module c:/php/php5apache.dll
```

2. Add this line to the **httpd.conf** file below the `ClearModuleList` command (this right below the line you just added)

```
AddModule mod_php5.c
```

3. Add these lines to the **httpd.conf** file, further down below where the `<IfModule>` sections start appearing

```
<IfModule mod_php5.c>
    AddType application/x-httpd-php .php
    SetEnv PHPRC c:/php
</IfModule>
```

4. Add the PHP installation directory to the system **PATH**.
  - Right-click "My Computer" and select "Properties"
  - Click the "Advanced" tab
  - Click "Environment Variables"
  - Locate and select the "Path" variable in the "System variables" area
  - Click on "Edit"
  - Append the text `;c:\php\` to the existing text
5. It is also recommended that you increase the maximum time a script is allowed to execute. Open the **php.ini** file in a text editor (this file is located in the `%SYSTEMROOT%` directory by default) and locate the line starting with **max\_execution\_time**. Change this value to something like **300**.
6. Restart the computer for the changes to become effective.