

Allowing Remote Connections to MySQL Instance

You do not need to specially create a user and allow remote connections to a MySQL Instance. While adding a MySQL Instance to the Policy, you can use the credentials of any MySQL user with full access to the MySQL server from `localhost`. For example, you can use a MySQL `'root@localhost'` account typically created during the MySQL server installation. See [Adding a MySQL Instance to a Policy](#).

Customers with both 3.14 Server and Agent can use `localhost` for their MySQL instance hostname. The CDP Server does not connect directly to MySQL and instead connects to MySQL through the agent connection.



Notice

There is no relationship between a MySQL user and a CDP user.



Notice

Admin access to the server and MySQL installation is required.



Tip

In CDP, end-user level MySQL backup is not supported. Only super-users can conduct MySQL backup. Sub-users are limited by agent user permission.

3.14 Version Limitation

Prerequisites:

- Multiple databases per MySQL Instance
- MySQL user with full access to one of the databases

The MySQL user can backup only databases that belong to him and cannot backup databases that do not belong to him.

Use the following command to allow the user to backup all databases:

```
GRANT ALL PRIVILEGES ON *.* to 'user1'@'localhost'  
IDENTIFIED by 'some-pass';
```

**Notice**

The command will allow you to backup databases, but not restore.

Allowing Remote Connections to MySQL Instance (Version 3.12 or Earlier)

By default, remote access to the MySQL database server is disabled for security reasons. Follow the instructions below to provide remote access to the database server.

**Important Notice**

For the MySQL Add-on to work, both the CDP Server and the Agent should have administrative permissions for the entire server. The CDP Server will backup the database data, while the Agent will lock and flush tables. Also, the CDP Server needs administrative permissions for restoring data. You can create a special user for backups in MySQL and limit access to MySQL from the CDP Server IP address. Also, you should provide access to this user from localhost and the 127.0.0.1 address for the Agent.

Using Command Line Interface | Using GUI Tools

Using Command Line Interface

1. First, log in over `ssh` to the remote MySQL database server. To do this, on Linux or Mac, open the terminal and execute the command:

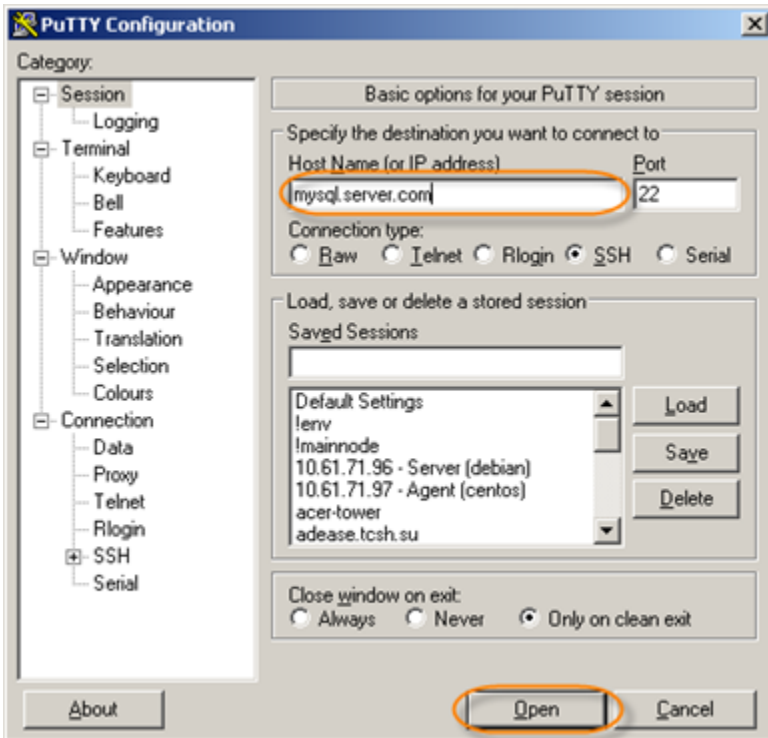
```
ssh user@mysql.server.com
```

Then you will be asked about an untrusted key. Enter "yes" and press <Enter>. Then enter the password.

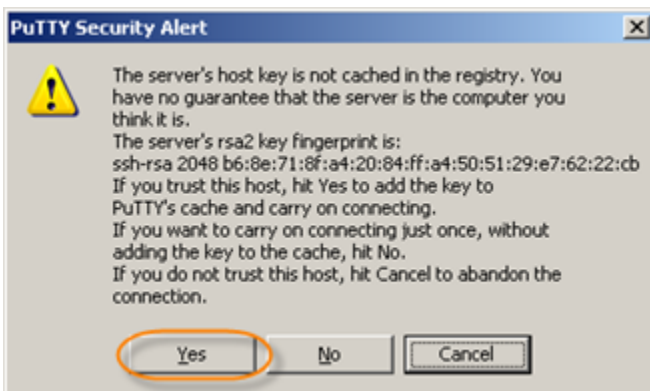
```
[08:01]:ubuntu@ubuntu:~> ssh user@mysql.server.com
The authenticity of host 'mysql.server.com (10.61.71.97)' can't be established.
RSA key fingerprint is b6:8e:71:8f:a4:20:84:ff:a4:50:51:29:e7:62:22:cb.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mysql.server.com,10.61.71.97' (RSA) to the list of k
nown hosts.
user@mysql.server.com's password:
Last login: Tue Jan 18 07:48:51 2011 from r1vpn.r1soft.com
```

On Windows, you can use the PuTTY utility. Download it from this page - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> - launch it, enter "mysql.server.com" in the "Host name (or IP address)" input field, and click on the "Open"

button.



When you are asked about an untrusted key, click on the "Yes" button.



Then enter the login and password.

```
login as: user
user@mysql.server.com's password:
Last login: Mon Jan 17 10:04:57 2011 from r1vpn.r1soft.com
[10:08] user@mysql.server.com: ~>
```

2. When the connection is established, you have to open the MySQL server configuration file `my.cnf` in a text editor such as `vim`.

i Tip

- If you are using Debian GNU/Linux, or installed MySQL using yum on Fedora/CentOS, the full path to the `my.cnf` file is `/etc/mysql/my.cnf`.
- If you are using Red Hat Linux/Fedora/Centos Linux and installed MySQL from rpms downloaded from `dev.mysql.com`, the full path to the `my.cnf` file is `/etc/my.cnf`.

```
# vim /etc/my.cnf
```

3. Open the file in a text editor and find the section starting with the line:

```
[mysqld]
```

Make sure the line `skip-networking` is commented (or remove the line) and add the following line:

```
bind-address = *
```

The entire section should look like this:

```
[mysqld]
character-set-server=utf8
collation_server=utf8_general_ci
skip-character-set-client-handshake
#skip-innodb
innodb_data_file_path=INNODBDATA1:4096M
innodb_log_file_size=512M
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
bind-address = *
#skip-networking
skip-external-locking
skip-name-resolve....
..
....
```

Where,

- `bind-address` - Contains an asterisk, meaning that the service should bind to all available IP addresses.
- `skip-networking` - Do not listen for the TCP port at all. All interactions with `mysqld` must be made via the Unix domain socket. This option is highly recommended for systems where only local requests are allowed because it provides more security. Since you need to allow a remote connection, this line should be removed from `my.cnf` or commented out.

```

1 [client]
2 port                = 3306
3 socket=/var/lib/mysql/mysql.sock
4 #default-character-set=cp1251
5 default-character-set=utf8
6
7 # Here follows entries for some specific programs
8
9 # The MySQL server
10 [mysqld]
11 #character-set-server=cp1251
12 character-set-server=utf8
13 #collation_server=cp1251_ukrainian_ci
14 collation_server=utf8_general_ci
15 skip-character-set-client-handshake
16 #skip-innodb
17 innodb_data_file_path=INNODBDATA1:4096M
18 innodb_log_file_size=512M
19 datadir=/var/lib/mysql
20 socket=/var/lib/mysql/mysql.sock
21 bind-address        = *
22 #skip-networking
23 #skip-external-locking
24 skip-name-resolve
25 key_buffer = 128M
26 max_allowed_packet = 2M
27 table_cache = 512
28 sort_buffer_size = 2M
29 read_buffer_size = 2M
30 read_rnd_buffer_size = 8M
31 myisam_sort_buffer_size = 24M
32 thread_cache_size = 8
33 query_cache_size = 24M
34 # Try number of CPU's*2 for thread_concurrency
35 thread_concurrency = 2
36 max-connections = 512
37 #log-bin
38 #log = /tmp/mysql-query.log
39 #server-id        = 1

```

4. Restart the `mysql` service.

```
# /etc/init.d/mysql restart
```

```
[16:28]:root@muscle:~:~:~# /etc/init.d/mysql restart
Shutting down MySQL..... SUCCESS!
Starting MySQL. SUCCESS! _
```

5. Grant access to the MySQL server from the IP address of the CDP Server. You should also grant access from IP address 127.0.0.1 and localhost, since the lock and flush operations during the snapshot will be performed by the agent running on the same host as MySQL service. The CDP Server will connect to MySQL as "r1soft" user.

Connect to the MySQL server by executing the following command:

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

```
[17:19]:root@mysql:~:~#>mysql -u root -p mysql
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.1.51-community MySQL Community Server (GPL)

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Enter the MySQL root password when prompted.

CDP should be able to backup all databases, so you should grant global privileges to the "r1soft" user.



Notice

There is no relationship between a MySQL user and a CDP sub-user.



Notice

Admin access to the server and MySQL installation is required.



Tip

In CDP, end-user level MySQL backup is not supported. Only super-users can conduct MySQL backup. Sub-users are limited by agent user permission.

In the following example, it is assumed that the IP address of the CDP Server is 202.202.200.20 and that the CDP Server will connect with username "r1soft" and password "r1soft" without quotes.

```
GRANT ALL PRIVILEGES ON *.* TO r1soft@'202.202.200.20' IDENTIFIED BY 'r1soft';
GRANT ALL PRIVILEGES ON *.* TO r1soft@'127.0.0.1' IDENTIFIED BY 'r1soft';
GRANT ALL PRIVILEGES ON *.* TO r1soft@'localhost' IDENTIFIED BY 'r1soft';
```

```
mysql> GRANT ALL PRIVILEGES ON *.* TO r1soft@'202.202.200.20' IDENTIFIED BY 'r1soft';
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO r1soft@'127.0.0.1' IDENTIFIED BY 'r1soft';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO r1soft@'localhost' IDENTIFIED BY 'r1soft';
Query OK, 0 rows affected (0.00 sec)
```

6. Log out of MySQL by typing the following command:

```
exit
```

```
mysql> exit
Bye
```

7. Make sure that there is no firewall that blocks connections to TCP port 3306 of the MySQL server from the CDP Server. It is not always possible to check all the firewalls between one server and the other. But you can always check local `iptables` firewall on the MySQL server. To add the rule that permits connections to TCP port 3306 from CDP Server with IP address 202.202.200.20, execute the following command:

```
iptables -A INPUT -s 202.202.200.20 -m tcp -p tcp --dport 3306 -j ACCEPT
```

If you have several CDP Servers that reside on IP subnet 202.202.200.0/24 and the MySQL server can be backed up by any of them, you can allow access to TCP port 3306 from the entire subnet in one command:

```
iptables -A INPUT -s 202.202.200.0/24 -m tcp -p tcp --dport 3306 -j ACCEPT
```

Finally, save firewall rules so they will be automatically reloaded when the server reboots:

```
# /etc/init.d/iptables save
```

```
[17:26]:root@mysql:~:~# iptables -A INPUT -s 202.202.200.20 -m tcp -p tcp --dport 3306 -j ACCEPT
[17:33]:root@mysql:~:~# iptables -A INPUT -s 202.202.200.0/24 -m tcp -p tcp --dport 3306 -j ACCEPT
[17:37]:root@mysql:~:~# /etc/init.d/iptables save
Saving firewall rules to /etc/sysconfig/iptables: [ OK ]
```

8. Test that your firewall settings and MySQL security settings allow you to connect to the MySQL server from the CDP Server. Execute the following command:

```
$ mysql -h mysql.server.com -u r1soft -p
```

Where,

- -h IP or hostname - `mysql.server.com` is the hostname (FQDN) of MySQL server.
- -u r1soft - Log in as MySQL user r1soft.
- -p - Prompt for password.

```
[16:38]:user@cdpserver:~>mysql -h mysql.server.com -u r1soft -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.1.51-community MySQL Community Server (GPL)
```

You can also test if port 3306 is reachable through the firewall using telnet:

```
$ telnet mysql.server.com 3306
```

```
[16:41]:user@cdpserver:~>telnet mysql.server.com 3306
Trying 10.0.0.156...
Connected to mysql.server.com.
Escape character is '^]'.
>
5.1.51-community      839`Z!6,y?n*8~k}Se&'Connection closed by foreign host.
```

If the port is reachable, you will see the following message:

```
Connected to mysql.server.com Escape character is ^]
```

Then some garbage characters along with the MySQL version string (here MySQL version is 5.1.51-community). To close the telnet, press the <Ctrl> + <]> keys or just wait until the connection is closed on timeout.

Using GUI Tools



Notice

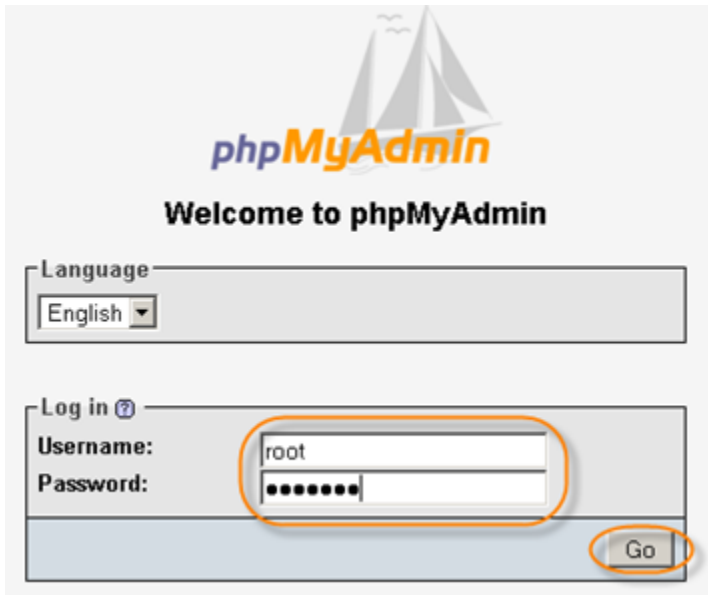
Using GUI tools described in this document only allows you to grant permissions on the MySQL server level. You still have to make sure that the MySQL server listens for network connections and that the firewall does not block its port. There are web applications that allow you to do this in GUI. For example, the popular hosting management panel Webmin allows you to edit firewall rules and text files as well as restart services. Another popular hosting management panel - Parallels Plesk - also allows you to edit firewall rules. Covering all available tools goes far beyond the scope of this documentation.

Granting Permissions Using phpMyAdmin

PhpMyAdmin (<http://www.phpmyadmin.net/>) is an open source web application written in PHP. It is very popular among web developers because of its intuitive interface and ease of use. A lot of web hosting management panels include phpMyAdmin in their interface.

In the following example, it is assumed that the IP address of the CDP Server is 202.202.200.20 and that the CDP Server will connect with username "r1soft" and password "r1soft" without quotes.

1. First, open phpMyAdmin in your browser and log in.



2. Click the "Privileges" link. Depending on the version of phpMyAdmin, this link can be found in different parts of the window.



3. Click the "Add a new User" link.

Server: 10.0.0.156

Databases SQL Status Variables Charsets Engines Privileges Processes Export

Import

User overview

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [Show all]

	User	Host	Password	Global privileges ¹	Grant	
<input type="checkbox"/>	Any	%	--	USAGE	No	
<input type="checkbox"/>	root	10.0.0.65	Yes	ALL PRIVILEGES	Yes	
<input type="checkbox"/>	root	10.0.0.8	Yes	ALL PRIVILEGES	Yes	
<input type="checkbox"/>	root	172.18.3.230	Yes	ALL PRIVILEGES	Yes	
<input type="checkbox"/>	root	172.18.3.231	Yes	ALL PRIVILEGES	Yes	
<input type="checkbox"/>	root	172.18.3.232	Yes	ALL PRIVILEGES	Yes	
<input type="checkbox"/>	root	localhost	Yes	ALL PRIVILEGES	Yes	

[Check All / Uncheck All](#)

[Add a new User](#)

4. On the "Add a New User" window, do the following:

- Enter "r1soft" in the "User name" field.
- Select the "Use text field" option from the drop-down menu next to "Host" and enter 202.202.200.20 in the field next to the option list.
- Enter "r1soft" in the "Password" and "Re-type" fields.
- Click "Check all" next to "Global privileges."

Add a new User

Login Information

User name:

Host:

Password:

Re-type:

Generate Password:

Database for user

None

Create database with same name and grant all privileges

Grant all privileges on wildcard name (username_%)

Global privileges

Note: MySQL privilege names are expressed in English

Scroll down and click on the "Go" button.

Global privileges ([Check All](#) / [Uncheck All](#))

Note: MySQL privilege names are expressed in English

Data	Structure	Administration
<input checked="" type="checkbox"/> SELECT	<input checked="" type="checkbox"/> CREATE	<input checked="" type="checkbox"/> GRANT
<input checked="" type="checkbox"/> INSERT	<input checked="" type="checkbox"/> ALTER	<input checked="" type="checkbox"/> SUPER
<input checked="" type="checkbox"/> UPDATE	<input checked="" type="checkbox"/> INDEX	<input checked="" type="checkbox"/> PROCESS
<input checked="" type="checkbox"/> DELETE	<input checked="" type="checkbox"/> DROP	<input checked="" type="checkbox"/> RELOAD
<input checked="" type="checkbox"/> FILE	<input checked="" type="checkbox"/> CREATE TEMPORARY TABLES	<input checked="" type="checkbox"/> SHUTDOWN
	<input checked="" type="checkbox"/> SHOW VIEW	<input checked="" type="checkbox"/> SHOW DATABASES
	<input checked="" type="checkbox"/> CREATE ROUTINE	<input checked="" type="checkbox"/> LOCK TABLES
	<input checked="" type="checkbox"/> ALTER ROUTINE	<input checked="" type="checkbox"/> REFERENCES
	<input checked="" type="checkbox"/> EXECUTE	<input checked="" type="checkbox"/> REPLICATION CLIENT
	<input checked="" type="checkbox"/> CREATE VIEW	<input checked="" type="checkbox"/> REPLICATION SLAVE
	<input checked="" type="checkbox"/> EVENT	<input checked="" type="checkbox"/> CREATE USER
	<input checked="" type="checkbox"/> TRIGGER	

Resource limits

Note: Setting these options to 0 (zero) removes the limit.

MAX QUERIES PER HOUR

MAX UPDATES PER HOUR

MAX CONNECTIONS PER HOUR

MAX USER_CONNECTIONS

You will be notified that the user has been successfully created.

Server: 10.0.0.156

[Databases](#) [SQL](#) [Status](#) [Variables](#) [Charsets](#) [Engines](#) [Privileges](#) [Processes](#) [Export](#)

[Import](#)

✔ You have added a new user.

```
CREATE USER 'rlsoft'@'202.202.200.20' IDENTIFIED BY '****';
GRANT ALL PRIVILEGES ON *.* TO 'rlsoft'@'202.202.200.20' IDENTIFIED BY '****' WITH GRANT OPTION MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0;
```

[Edit] [Create PHP Code]

5. Repeat steps 2-4. This time, type "127.0.0.1" instead of "202.202.200.20" in the "Host" field.

6. Repeat steps 2-4 again. This time select "Local" in the option list next to the "Host" field. You will not have to type "localhost" in the input field as it will appear there automatically.

Add a new User

Login Information

User name: Use text field: r1soft

Host: Local localhost

Password: Use text field:

Re-type:

Generate Password: Generate Copy

Database for user

None

Create database with same name and grant all privileges

Grant all privileges on wildcard name (username_%)

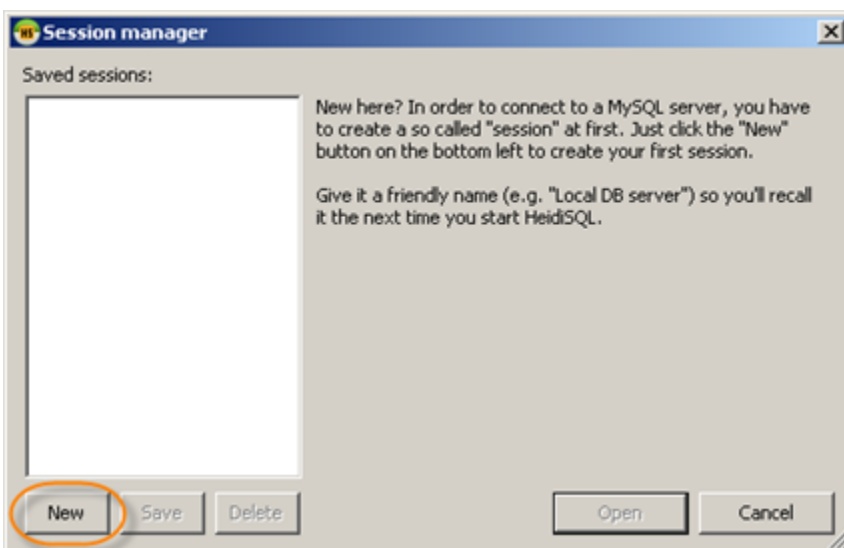
Global privileges [Check All](#) / [Uncheck All](#)

Granting Permissions Using HeidiSQL

HeidiSQL (<http://www.heidisql.com/>) is a freeware Windows application written in Delphi. It is popular among web developers because of its intuitive interface and ease of use. It can be installed on a laptop and can be used for managing MySQL servers that do not have phpMyAdmin installed.

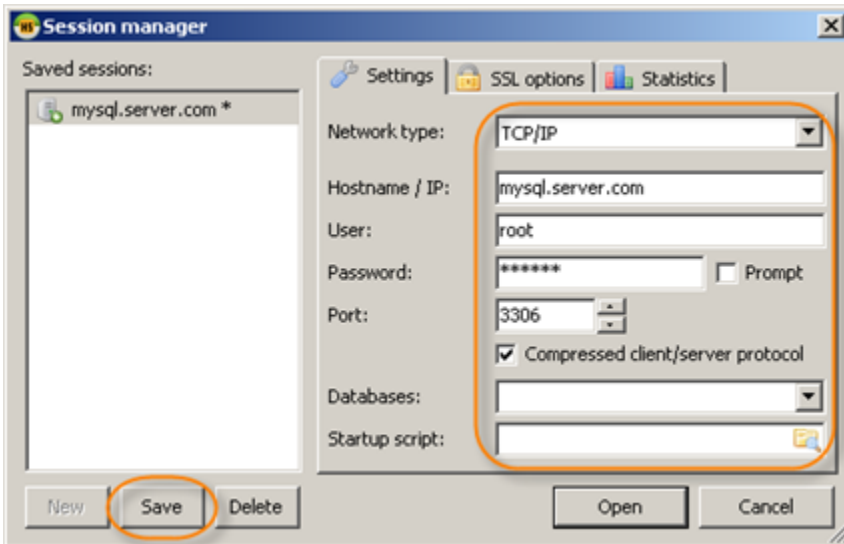
In the following example, it is assumed that the IP address of the CDP Server is 202.202.200.20 and that the CDP Server will connect with the username "r1soft" and password "r1soft" without quotes.

1. First, launch HeidiSQL and press the "New" button to enter MySQL server credentials.

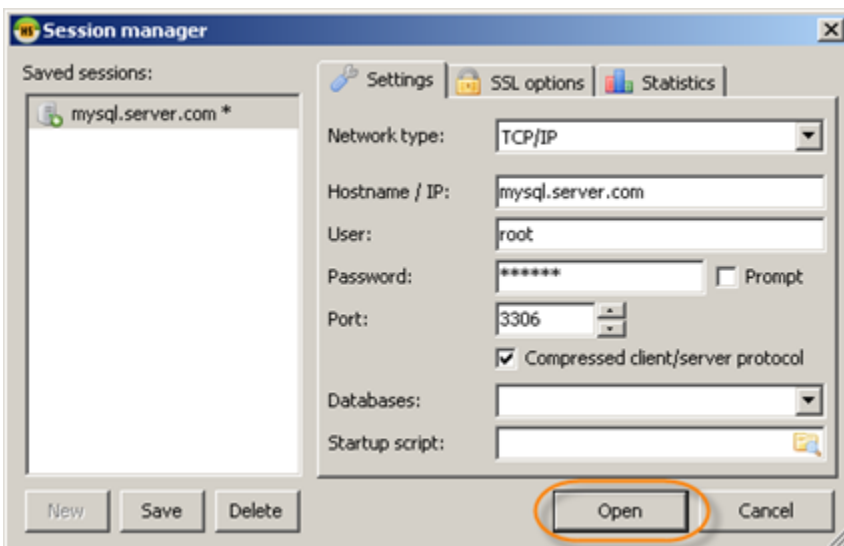


2. Enter the session name in the list on the left, the Hostname or IP address of the MySQL

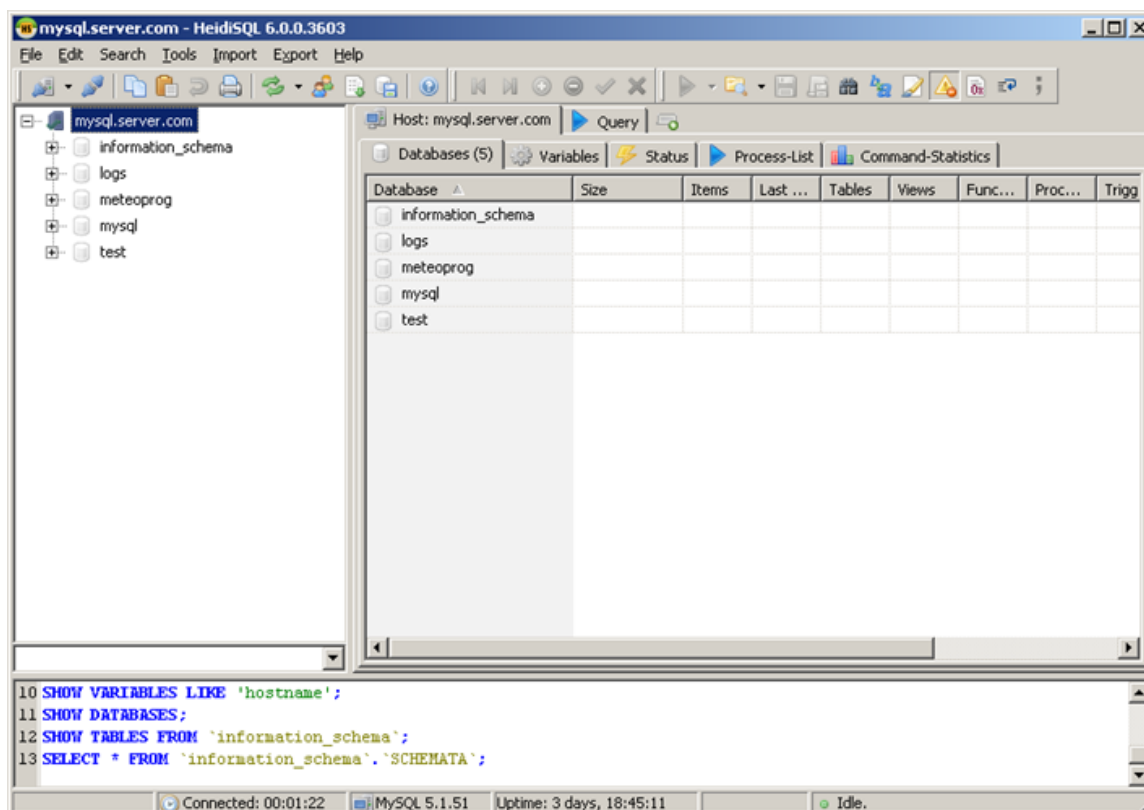
server, the username, and the password, and press "Save."



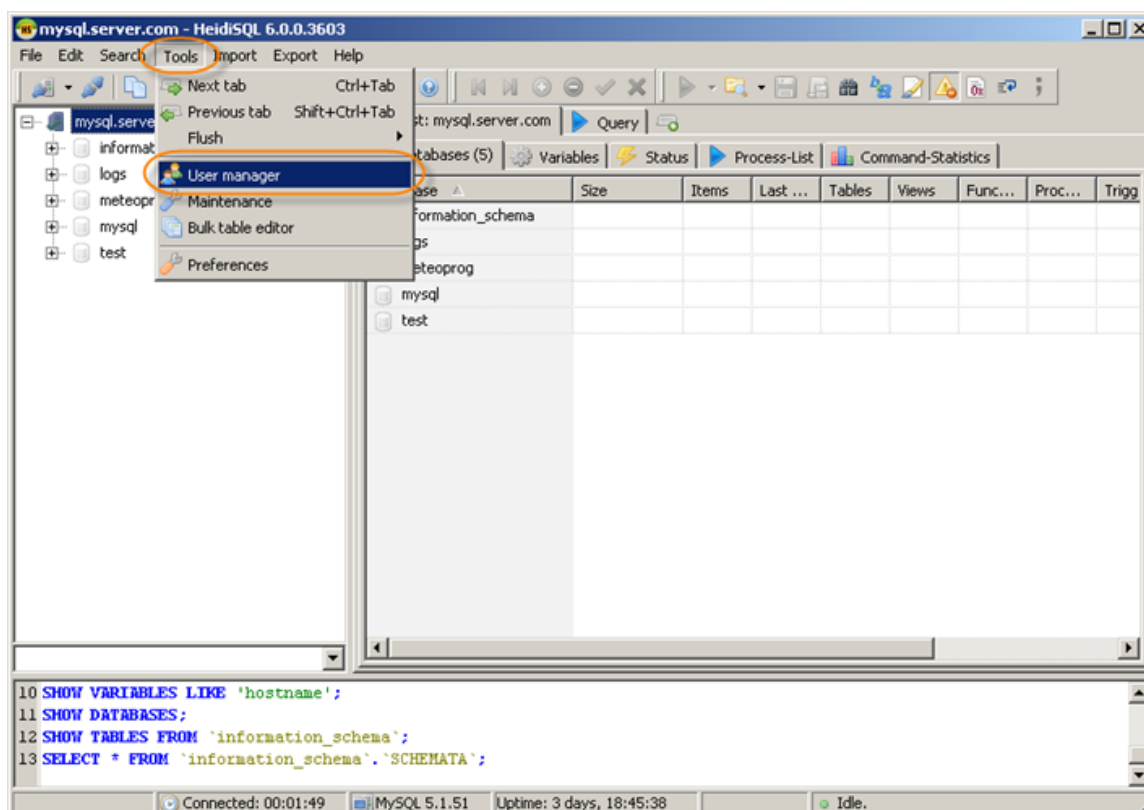
Then press "Open."



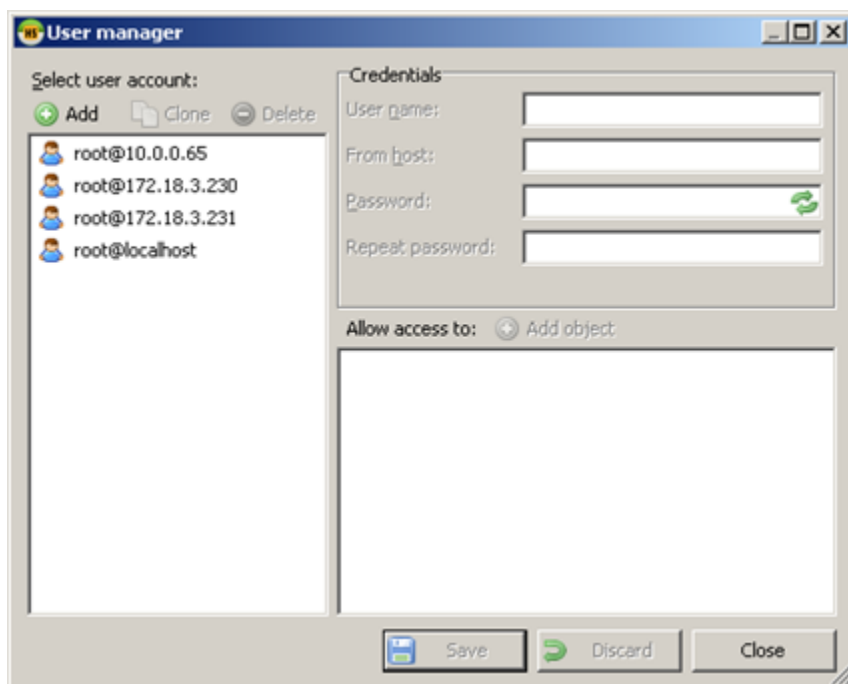
You will see the main window of the application.



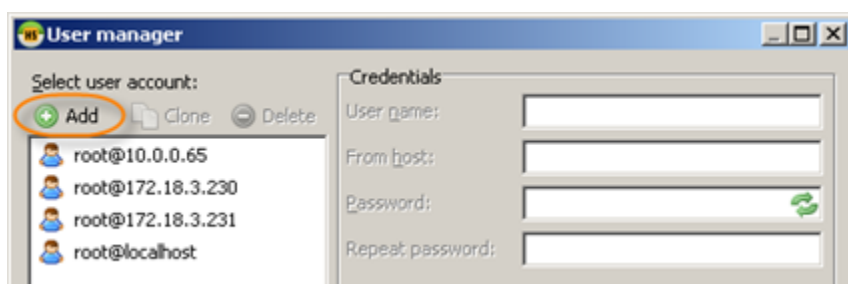
3. Select Tools > User manager from the application menu.



You will see the User manager window.

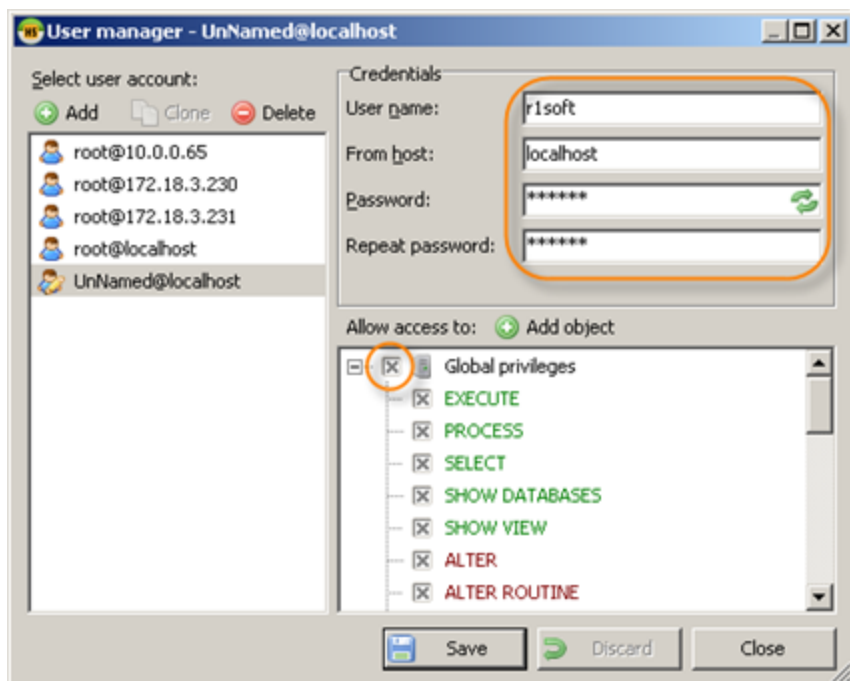


4. Click on the "Add" button.

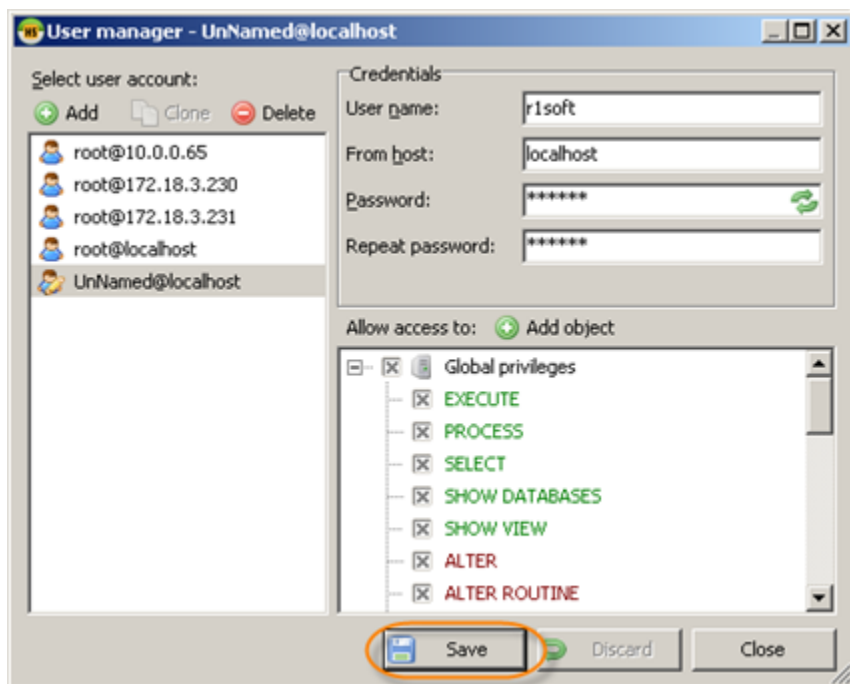


5. Then do the following:

- Enter "r1soft" in the "User name" field.
- Leave the default value "localhost" in the "From host" field.
- Enter "r1soft" in the "Password" and "Repeat password" fields.
- Check the box next to "Global privileges."



6. Click on the "Save" button.



7. Repeat step 4. This time enter 127.0.0.1 in the "From host" field.

8. Repeat step 4. This time enter 202.202.200.20 in the "From host" field.

9. Click on the "Close" button to close the "User manager" window.

