EventTracker
Secure. Comply. Succeed.

# Integrate MySQL Server

*EventTracker Enterprise*

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Publication Date: Nov. 3, 2016

# Abstract

This guide provides instructions to configure **MySQL** to send the logs to EventTracker Enterprise. It supports the following MySQL flavors: **MariaDB** and **Percona MySQL**.

# Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise**, and **MySQL Server 5.7, MariaDB 10.1 and Percona MySQL 5.6.31.**

# Target Audience

MySQL users, who wish to forward logs to EventTracker Manager.

# Table of Contents

# Overview

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation.

EventTracker collects and analyses the queries executed and enlightens an administrator about database management, user management and table management.

# Pre-requisite

- EventTracker Enterprise v7.x for reports and alerts should be installed.
- EventTracker Enterprise v8.x for configuring reports, alerts and flex dashboards should be installed.
- MySQL database should be installed.
- EventTracker agent should be installed on Windows MySQL database system.
- Syslog should be enabled on Centos 7 MySQL machine.
- Firewall between EventTracker manager and MySQL system should be off or made exception for port 14505.

**NOTE**: For **Percona MySQL** integration guide, Please check the following link:

**http://www.eventtracker.com/wp-content/support-docs/Integration-Guide-Percona-Server-MySQL.pdf**

**Below is the configuration for MySQL Server 5.7 and MariaDB 10.1.**

# Configuration for sending logs to EventTracker

**NOTE**: The below configuration applies to **MySQL 5.7** and **MariaDB 10.1** and is supported on **Microsoft Windows** and **Centos 7.**

1. On Windows: MySQL logs are consumed through **Log File Monitoring (LFM).**
2. On Centos 7: MySQL logs are forwarded using **Syslog**

# 1. MySQL Windows Configuration

a. To enable server auditing connect to MySQL database, login using administrative credentials.

```
C:\Program Files\MariaDB 10.1\bin>mysql -u root -p
Enter password: ********
```

Figure 1

b. **server_audit.dll** plugin is required to enable auditing, so check the plugins directory and run the query **SHOW VARIABLES LIKE 'plugin_dir';**

```
MariaDB [(none)]> SHOW VARIABLES LIKE 'plugin_dir';
+---------------+-----------------------------------------+
| Variable_name | Value                                   |
+---------------+-----------------------------------------+
| plugin_dir    | C:\Program Files\MariaDB 10.1\lib\plugin\ |
+---------------+-----------------------------------------+
1 row in set (0.00 sec)
```

Figure 2

c. If you do not find the plugin file inside your plugins directory, download it and place it in the plugins directory manually.

d. Install the plugin using command **install plugin server_audit soname 'server_audit.dll';**

e. To confirm the plugin is installed and enabled, run the query show plugins;

```
| SERVER_AUDIT                    | ACTIVE | AUDIT                | server_audit.dll
 | GPL      |
+-------------------------------+--------+---------------------+-----------------
```

Figure 3

f. Set the following on MySQL database

```
SET GLOBAL server_audit_events='CONNECT,QUERY,TABLE';
SET GLOBAL server_audit_logging=ON;
SET GLOBAL server_audit_output_type=FILE;
```

g. To see the currently set variables use the command **show global variables like "server_audit%";**

```
MariaDB [(none)]> show variables like 'server_audit%';
+-------------------------------+-----------------------+
| Variable_name                 | Value                 |
+-------------------------------+-----------------------+
| server_audit_events           | CONNECT,QUERY,TABLE   |
| server_audit_excl_users       |                       |
| server_audit_file_path        | server_audit.log      |
| server_audit_file_rotate_now  | OFF                   |
| server_audit_file_rotate_size | 1000000               |
| server_audit_file_rotations   | 9                     |
| server_audit_incl_users       |                       |
| server_audit_loc_info         |                       |
| server_audit_logging          | ON                    |
| server_audit_mode             | 0                     |
| server_audit_output_type      | file                  |
| server_audit_query_log_limit  | 1024                  |
| server_audit_syslog_facility  | LOG_USER              |
| server_audit_syslog_ident     | mysql-server_auditing |
| server_audit_syslog_info      |                       |
| server_audit_syslog_priority  | LOG_INFO              |
+-------------------------------+-----------------------+
16 rows in set (0.00 sec)
```

Figure 4

h. To verify auditing enabled, run query: **Show global status like 'server_audit%';**

```
MariaDB [(none)]> show global status like 'server_audit%';
+----------------------------+------------------+
| Variable_name              | Value            |
+----------------------------+------------------+
| Server_audit_active        | ON               |
| Server_audit_current_log   | server_audit.log |
| Server_audit_last_error    |                  |
| Server_audit_writes_failed | 0                |
+----------------------------+------------------+
4 rows in set (0.00 sec)
```

Figure 5

i. Now, click **my.ini** configuration setting file of MySQL.

j. In **my.ini** configuration setting file of MySQL, set the following:

**server_audit_logging=ON**

**server_audit_output_type=file**

**server_audit_events=CONNECT,QUERY,TABLE**

k. In Run, type '**services.msc"** and then click **OK**. Restart the MySQL service.

l. Now connect to MySQL database and execute the queries by performing activities, logs are written into **server_audit.log** file in the installation path of the MySQL.

# Configure log file monitor (LFM) for monitoring MySQL

To perform LFM configuration, deploy the EventTracker agent on MySQL machine. For this, please refer **EventTracker Agent installation guide.** After installation of the ET agent, check the steps to configure LFM.

1. Select the **Start** button, select **Prism Microsystems**, and then select **EventTracker Control Panel**.
2. Click the icon **EventTracker Agent Configuration.**

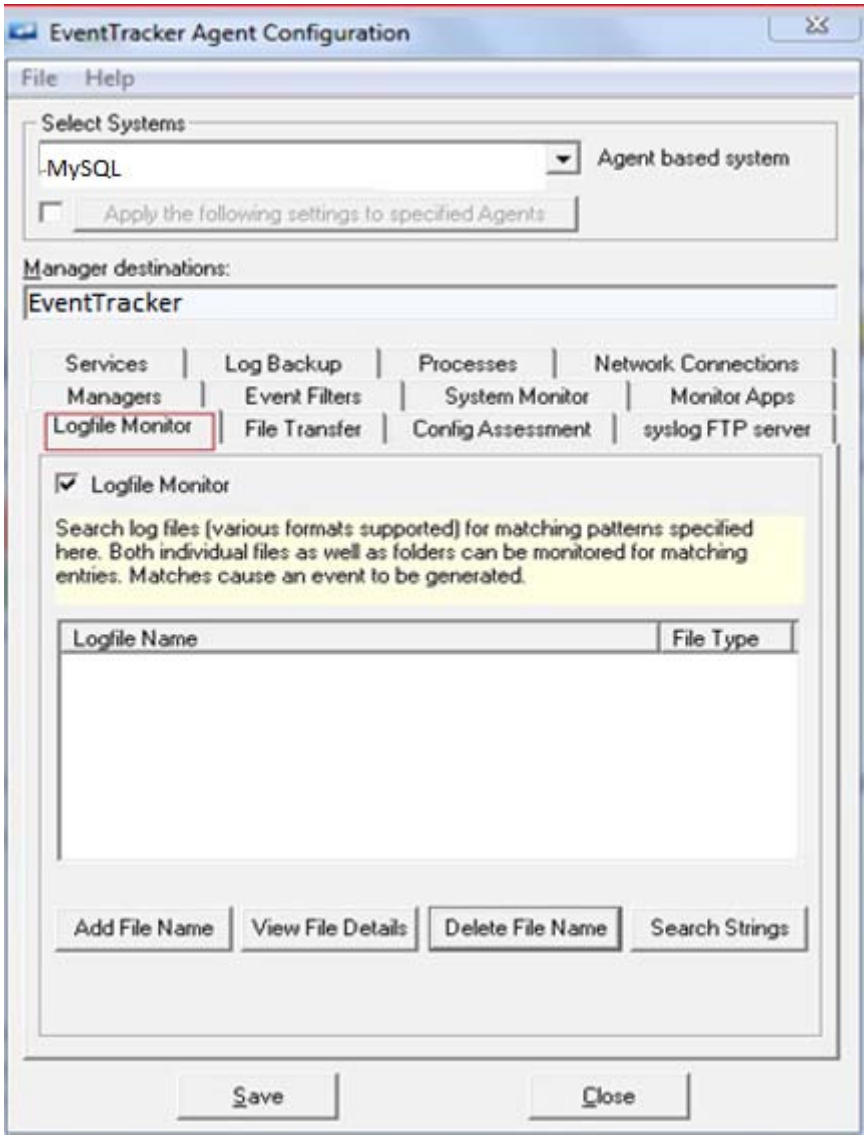


Figure 6

3. Click the button **Add File Name** and select the **server_audit.log file** which has been generated and then click **OK.**
4. Select **Get All Existing Log Files** option.
5. In **Select Log File Type** drop down, select the **Multiline** option.
6. Enter the path of the MySQL logs.

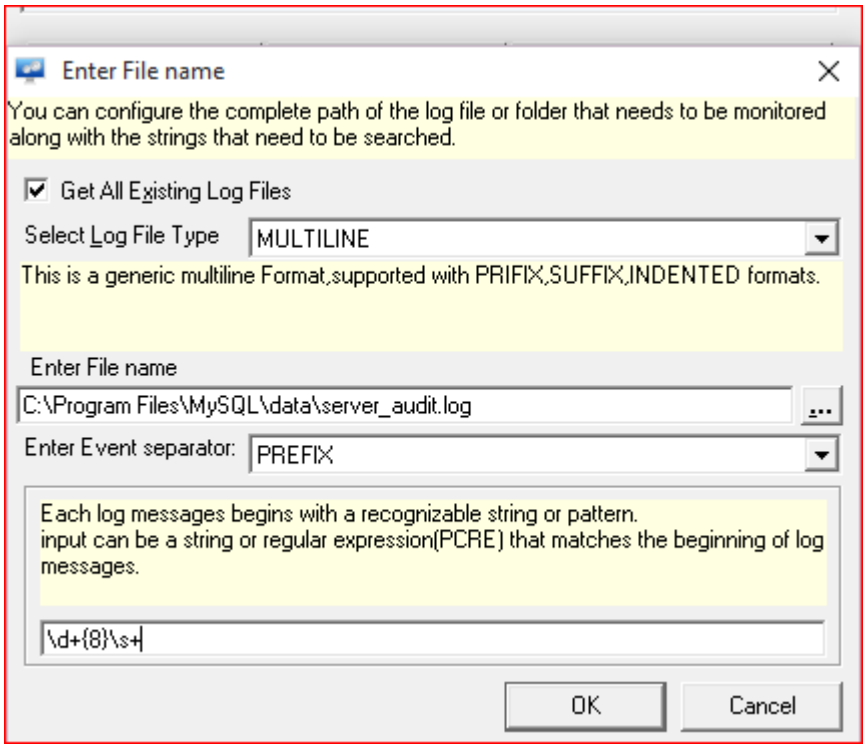


Figure 7

7. Click the **OK** button.
8. Now, click the **Search String** button.

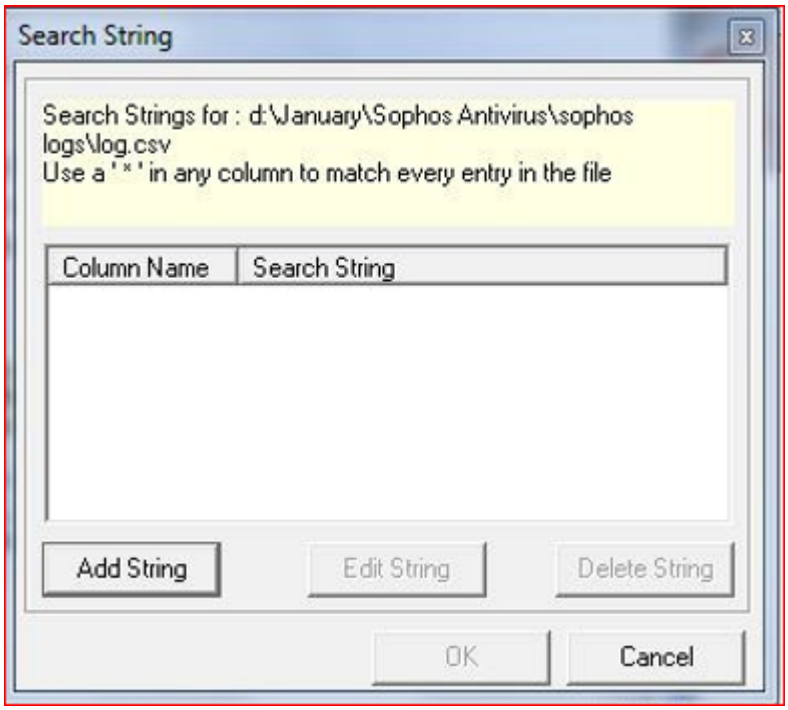


Figure 8

9. Select **Add String**.

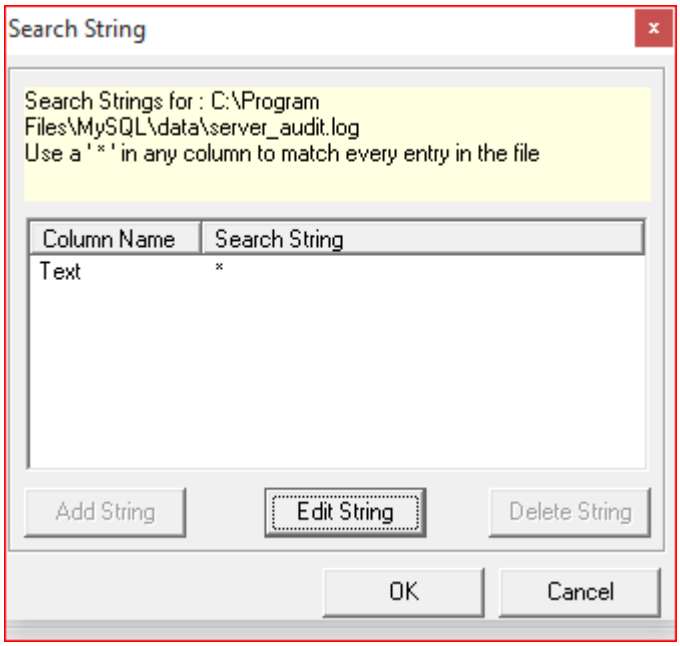


Figure 9

10. Select the string to configure, that needs to be searched in the selected logs. If any of the string matches, then a log is generated.

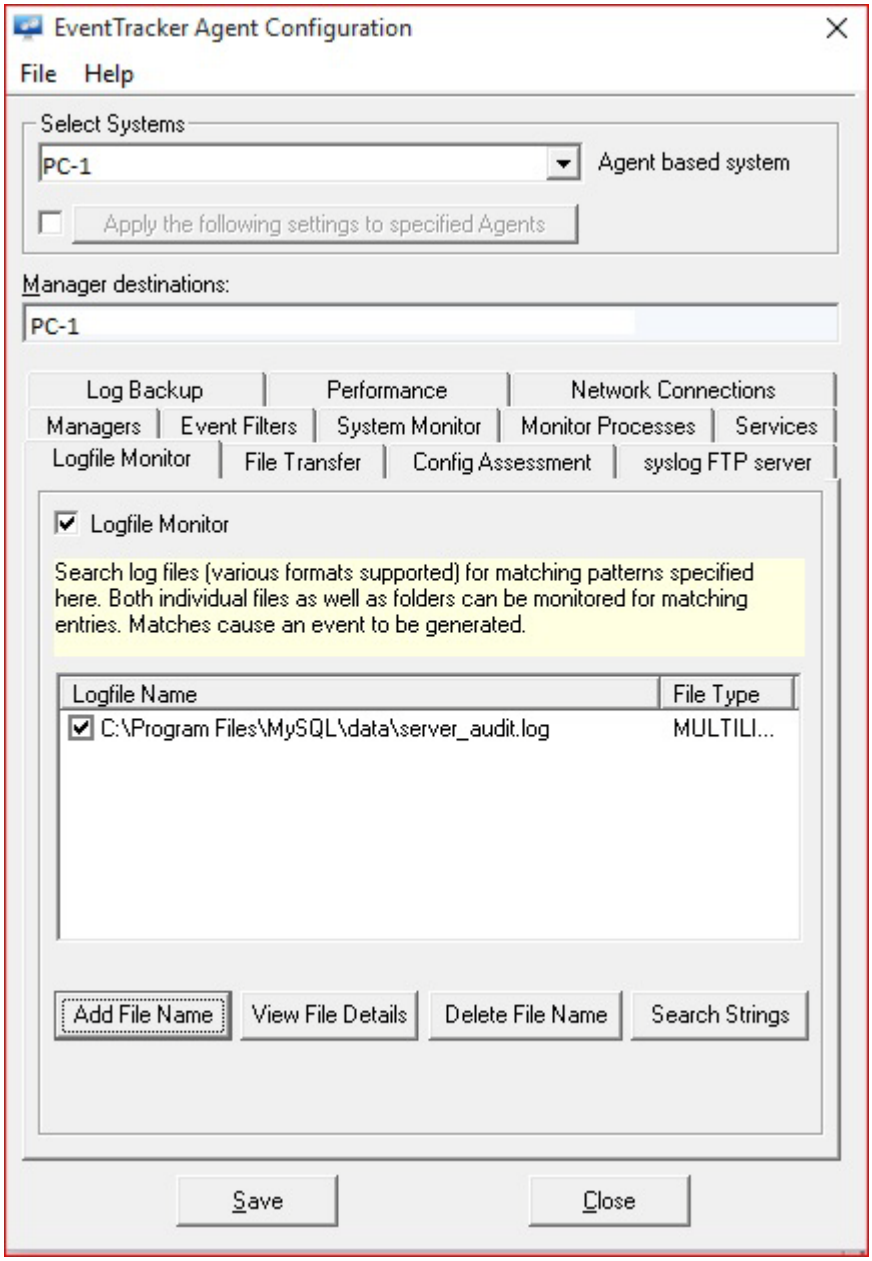


Figure 10

11. Click **Save**

**Logs will be sent to the EventTracker Enterprise.**

# 2. MySQL Centos 7 Configuration

a. Log into Centos machine with administrative privileges.
b. Connect to MySQL database and verify for the audit plugin.

```
[root@centos7-vm05 ~]# mysql -u root -p
Enter password:
```

Figure 11

c. **server_audit.so** plugin is required to enable auditing. So check the plugins directory and run the query **show variables like 'plugin_dir';**

```
MariaDB [(none)]> show variables like 'plugin_dir';
+---------------+-------------------------+
| Variable_name | Value                   |
+---------------+-------------------------+
| plugin_dir    | /usr/lib64/mysql/plugin/ |
+---------------+-------------------------+
1 row in set (0.28 sec)
```

Figure 12

d. If you do not find the plugin file inside your plugins directory, download it and place it in the plugins directory manually.

e. Install the plugin using command **install plugin server_audit soname 'server_audit.so';**

f. To confirm the plugin is installed and enabled, run the query **show plugins;**

```
| SERVER_AUDIT                  | ACTIVE    | AUDIT              | server_audit.s
o | GPL      |
```

Figure 13

g. Access **my.cnf** configuration file, available at **/etc** folder.

h. Edit using text editor **# vi my.cnf** file and enable the following:

**server_audit_events='CONNECT, QUERY, TABLE'**
**server_audit_file_path=server_audit.log**
**server_audit_logging = ON**
**server_audit_output_type = SYSLOG**
**server_audit_syslog_facility=LOG_LOCAL6**

i. To see the currently set variables with the command **show global variables like "server_audit%";**

```
MariaDB [(none)]> show variables like 'server_audit%';
+-------------------------------+-----------------------+
| Variable_name                 | Value                 |
+-------------------------------+-----------------------+
| server_audit_events           | CONNECT,QUERY,TABLE   |
| server_audit_excl_users       |                       |
| server_audit_file_path        | server_audit.log      |
| server_audit_file_rotate_now  | OFF                   |
| server_audit_file_rotate_size | 1000000               |
| server_audit_file_rotations   | 9                     |
| server_audit_incl_users       |                       |
| server_audit_loc_info         |                       |
| server_audit_logging          | ON                    |
| server_audit_mode             | 0                     |
| server_audit_output_type      | syslog                |
| server_audit_query_log_limit  | 1024                  |
| server_audit_syslog_facility  | LOG_LOCAL6            |
| server_audit_syslog_ident     | mysql-server_auditing |
| server_audit_syslog_info      |                       |
| server_audit_syslog_priority  | LOG_INFO              |
+-------------------------------+-----------------------+
16 rows in set (0.00 sec)
```

Figure 14

j. To verify auditing is enabled, run the query: **Show global status like 'server_audit%';**

```
MariaDB [(none)]> show global status like 'server_audit%';
+----------------------------+----------+
| Variable_name              | Value    |
+----------------------------+----------+
| Server_audit_active        | ON       |
| Server_audit_current_log   | [SYSLOG] |
| Server_audit_last_error    |          |
| Server_audit_writes_failed | 0        |
+----------------------------+----------+
4 rows in set (0.05 sec)
```

Figure 15

k. Access **rsyslog.conf** on folder **/etc**. Enable syslog using text editor **#vi rsyslog.conf** file.

**NOTE**: Syslog can be enabled using TCP or UDP protocol.

Syslog enabled with TCP

```
*.info;mail.none;authpriv.none;cron.none                @192.168.10.100
```

Figure 16

Syslog enabled with UDP

```
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
*.* @@:192.168.10.1 :514
```

Figure 17

**NOTE**: The IP address should be that of **EventTracker Manager Machine** and the port '**514**".

I. Restart **MySQL service # /etc/init.d/mysqld restart** and connect to MySQL database. Run the queries and the logs generated will be forwarded to EventTracker Manager Machine through Syslog.

# EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker; Reports and Alerts can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support MySQL.

## Category

- **MySQL: Authentication failure**
  This category provides information related to user authentication failure.

- **MySQL: Authentication success**
  This category provides information related to user authentication success.

- **MySQL: User logoff**
  This category provides information related to user logoff from the database.

- **MySQL: User password changed**
  This category provides information related to password reset to an existing user account.

- **MySQL: Root logins**
  This category provides information related to root logins.

- **MySQL: Root logon failure**
  This category provides information related to root logon failure.

- **MySQL: Create database**
  This category provides information related to creation of database by the user.

- **MySQL: Delete database**
  This category provides information related to database dropped by the user.

- **MySQL: Create user**
  This category provides information related to create and configure a database user.

- **MySQL: Delete user**
  This category provides information related to remove a database user and optionally remove the user's objects.

- **MySQL: Rename user**
  This category provides information related to rename existing MySQL user accounts.

- **MySQL: Create table**
  This category provides information related to create a table in a database.

- **MySQL: Delete table**
  This category provides information related to delete a table and all rows in the table.

- **MySQL: Rename Table**
  This category provides information related to when the tables are renamed by the user.

- **MySQL: Insert into Table**
  This category provides information related to insert new records in a table.

- **MySQL: Update Table**
  This category provides information related to update existing records in the table.

- **MySQL: Alter Table**
  This category provides information related to add, delete or modify columns in an existing table.

- **MySQL: Privileges change**
  This category provides information related to providing access or privileges and the removing access on the database objects to the users.

# Reports

- **MySQL- User authentication failed**
  This report provides the information related to the authentication failure, when user enters the wrong credentials and fails to connect the database.

**Logs Considered:**

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 9/8/2016 12:33:36 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160908 11:44:44,Esxwin2k12r2vm3,root,localhost,12,0,FAILED_CONNECT,,,1045
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

Figure 18

| LogTime | Computer | User Name | Client Host | Action | Database |
|---|---|---|---|---|---|
| 09/28/2016 12:36:05 PM | ESXWIN2K12R2VM311 | millet | PC7.Contoso.com | FAILED_CONNECT | kotak |
| 09/28/2016 12:36:05 PM | ESXWIN2K12R2VM311 | bob | PC9.Contoso.com | FAILED_CONNECT | kotak |

Figure 19

- **MySQL-User authentication success**
  This report provides the information related to authentication success, when user connects the database with valid credentials.

**Logs Considered:**

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160907 11:59:50,Esxwin2k12r2vm3,root,localhost,6,0,CONNECT,,,0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

Figure 20

| LogTime | Computer | User Name | Client Host | Database |
|---|---|---|---|---|
| 09/27/2016 06:14:08 PM | ESXWIN2K12R2VM311 | bob | PC7.Contoso.com | kotak |
| 09/27/2016 06:14:08 PM | ESXWIN2K12R2VM311 | peter | PC4.Contoso.com | mysql |
| 09/27/2016 06:14:08 PM | ESXWIN2K12R2VM311 | root | Crest.Contoso.com | iisc |

Figure 21

- **MySQL-User logoff**
  This report provides the information related to user logged off from the database.

**Logs Considered:**

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 9/28/2016 12:18:52 PM | 3230 | TOM / Esxwin2k12r2vm... | N/A | N/A | EventTracker |

**Event Type:** Information
**Log Type:** Application
**Category Id:** 0

**Description:**
ENTRY:20160927 15:57:13,Esxwin2k12r2vm3,millet,tom.toons.local,321,0,DISCONNECT,kotak,,0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINEFIELD: *

Figure 22

| LogTime | Computer | User Name | Client Host | Action | Database |
|---|---|---|---|---|---|
| 09/28/2016 10:54:41 AM | ESXWIN2K12R2VM311 | peter | PC3.Contoso.com | DISCONNECT | mysql |
| 09/28/2016 10:54:41 AM | ESXWIN2K12R2VM311 | bob | PC4.Contoso.com | DISCONNECT | kotak |

Figure 23

- **MySQL-User password changed**
  This report provides the information related to user password changed by the administrator.

**Logs considered:**

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 9/10/2016 10:48:27 AM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160910 10:47:09,Esxwin2k12r2vm3,root,localhost,17,186,QUERY,mysql,"SET PASSWORD FOR \"Mercy\"@\"localhost\" = PASSWORD(****)",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

| | | | | | |
|---|---|---|---|---|---|
| 9/10/2016 10:53:07 AM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160910 10:52:10,Esxwin2k12r2vm3,root,localhost,17,195,QUERY,mysql,"update user set password=PASSWORD("newpass") where User=\"Mercy\"",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

Figure 24

| LogTime | Computer | Client Host | Changed By | Action | Changed For | Database |
|---|---|---|---|---|---|---|
| 09/21/2016 07:49:46 PM | ESXWIN2K12R2VM3 | Crest.Contoso.com | root | UPDATE user SET password=PASSWORD | hillary | mysql |
| 09/21/2016 07:49:23 PM | ESXWIN2K12R2VM3 | Crest.Contoso.com | root | SET PASSWORD | bob | mysql |
| 09/29/2016 06:47:35 PM | ESXWIN2K12R2VM3 | Scub.Contoso.com | george | SET PASSWORD | george | mysql |

Figure 25

- **MySQL-Database management**
  This report provides information related to database management when user creates and drops the database.

  **Logs Considered:**

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 9/8/2016 6:26:19 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |
| **Event Type:** Information<br>**Log Type:** System<br>**Category Id:** 2 | **Description:**<br>ENTRY:20160908 18:26:19,Esxwin2k12r2vm3,root,localhost,13,116,QUERY,mysql,"drop database IISC",0<br>FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log<br>TYPE:MULTILINE<br>FIELD: * | | | | |
| 9/8/2016 6:26:19 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |
| **Event Type:** Information<br>**Log Type:** System<br>**Category Id:** 2 | **Description:**<br>ENTRY:20160908 18:25:51,Esxwin2k12r2vm3,root,localhost,13,115,QUERY,mysql,"create database IISC",0<br>FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log<br>TYPE:MULTILINE<br>FIELD: * | | | | |

Figure 26

| LogTime | Computer | User Name | Client Host | Action | Database Name |
|---|---|---|---|---|---|
| 09/21/2016 05:44:30 PM | ESXWIN2K12R2VM3 | tommy | PC1.Contoso.com | CREATE | sbh |
| 09/21/2016 06:58:09 PM | ESXWIN2K12R2VM3 | hillary | PC5.Contoso.com | CREATE | rbi |
| 09/21/2016 07:32:25 PM | ESXWIN2K12R2VM3 | root | Crest.Contoso.com | DROP | rbi |

Figure 27

- **MySQL-User management**
  This report provides the information related to user management when administrator creates, drops and renames the user details.

**Logs Considered:**

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 9/10/2016 10:09:51 AM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |
| **Event Type:** Information<br>**Log Type:** System<br>**Category Id:** 2 | **Description:**<br>ENTRY:20160910 10:09:09,Esxwin2k12r2vm3,root,localhost,14,126,QUERY,kotak,"create user \"Mary\"@\"localhost\" identified by *****",0<br>FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log<br>TYPE:MULTILINE<br>FIELD: * | | | | |
| 9/10/2016 10:08:55 AM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |
| **Event Type:** Information<br>**Log Type:** System<br>**Category Id:** 2 | **Description:**<br>ENTRY:20160910 10:07:44,Esxwin2k12r2vm3,root,localhost,14,124,QUERY,kotak,"drop user \"james\"@\"localhost\"",0<br>FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log<br>TYPE:MULTILINE<br>FIELD: * | | | | |
| 9/7/2016 10:35:31 AM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |
| **Event Type:** Information<br>**Log Type:** System<br>**Category Id:** 2 | **Description:**<br>ENTRY:20160907 10:30:32,Esxwin2k12r2vm3,root,localhost,5,19,QUERY,mysql,"rename user \"donald\" to \"david\"@\"localhost\", \"mickey\" to \"maria\"@\"localhost\"",0<br>FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log<br>TYPE:MULTILINE<br>FIELD: * | | | | |

Figure 28

| LogTime | Computer | User Name | Client Host | Action | User Details | Database | Query Executed |
|---|---|---|---|---|---|---|---|
| 09/22/2016 10:16:31 AM | ESXWIN2K12R2VM3 | boby | PC6.Contoso.com | CREATE | anne | mysql | CREATE USER \'anne\'@\'192.168.1.78\' IDENTIFIED BY ***** |
| 09/22/2016 11:11:00 AM | ESXWIN2K12R2VM3 | boby | PC6.Contoso.com | CREATE | jeff | mysql | CREATE USER \'jeff\'@\'localhost\' IDENTIFIED BY ***** |
| 09/22/2016 10:55:36 AM | ESXWIN2K12R2VM3 | boby | PC6.Contoso.com | DROP | palo | mysql | DROP USER \'palo\'@\'192.168.1.85\', \'minni\'@\'loclahost\' |
| 09/22/2016 10:59:26 AM | ESXWIN2K12R2VM3 | boby | PC6.Contoso.com | RENAME | donald | mysql | RENAME USER \'donald\' TO \'duck\'@\'localhost\', \'mickey\' TO \'mouse\'@\'localhost\' |

Figure 29

- **MySQL-Table management**
  This report provides information related to table management when user creates, drops, renames, updates, inserts and alters the table.

**Logs considered:**

| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 9/8/2016 12:33:36 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160907 12:21:55,Esxwin2k12r2vm3,root,localhost,10,44,QUERY,mysql,"CREATE TABLE students (SID varchar(10), FNamw varchar(20), LName varchar(20))",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

| | | | | | |
|---|---|---|---|---|---|
| 9/8/2016 12:33:36 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160907 12:44:58,Esxwin2k12r2vm3,root,localhost,10,69,QUERY,mysql,"UPDATE Books SET Author=\"Lev Nikolayevich Tolstoy\" WHERE Id=1",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

| | | | | | |
|---|---|---|---|---|---|
| 9/8/2016 12:33:36 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160907 12:25:00,Esxwin2k12r2vm3,root,localhost,10,46,QUERY,mysql,"alter table students add Contcat_id varchar(20) after LName",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

| | | | | | |
|---|---|---|---|---|---|
| 9/8/2016 12:33:36 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160907 12:46:22,Esxwin2k12r2vm3,root,localhost,10,73,QUERY,mysql,"drop table student",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

| | | | | | |
|---|---|---|---|---|---|
| 9/8/2016 12:33:36 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160907 12:25:00,Esxwin2k12r2vm3,root,localhost,10,46,QUERY,mysql,"alter table students add Contcat_id varchar(20) after LName",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

| | | | | | |
|---|---|---|---|---|---|
| 9/8/2016 12:33:36 PM | 3230 | TOM / ESXWIN2K12R2VM... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:20160907 12:42:39,Esxwin2k12r2vm3,root,localhost,10,61,QUERY,mysql,"INSERT INTO Books(Id, Title, Author) VALUES (2, \"The Brothers Karamazov\", \"Fyodor Dostoyevsky\")",0
FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log
TYPE:MULTILINE
FIELD: *

Figure 30

| LogTime | Computer | User Name | Client Host | Action | Database | Table Name |
|---|---|---|---|---|---|---|
| 09/21/2016 12:33:36 PM | ESXWIN2K12R2VM3 | root | localhost | rename | mysql | students to student |
| 09/21/2016 05:41:41 PM | ESXWIN2K12R2VM3 | bob | PC4.Contoso.com | DROP | kotak | pet |
| 09/21/2016 05:10:17 PM | ESXWIN2K12R2VM3 | bob | PC4.Contoso.com | INSERT | kotak | pet |
| 09/21/2016 05:33:47 PM | ESXWIN2K12R2VM3 | bob | PC4.Contoso.com | UPDATE | kotak | hr |
| 09/21/2016 05:35:17 PM | ESXWIN2K12R2VM3 | bob | PC4.Contoso.com | ALTER | kotak | hr ADD EID INT |

Figure 31

- **MySQL: Privilege management**
  This report provides information related to privilege management when administrator has granted or revoked the privileges from the particular user.

  **Logs Considered:**

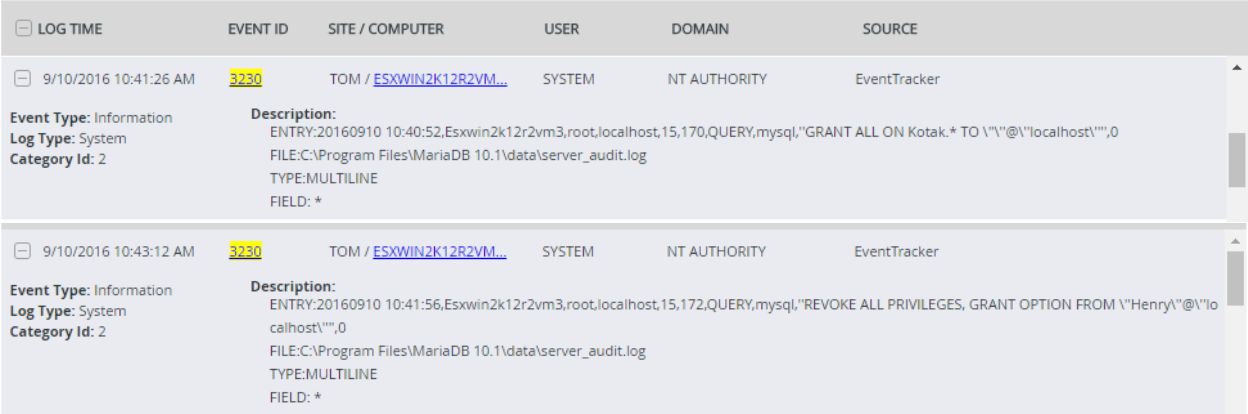


Figure 32

| LogTime | Computer | Client Host | User Name | Privileges | Database | User Details | Privileges On | Query Executed |
|---|---|---|---|---|---|---|---|---|
| 09/10/2016 10:13:37 AM | ESXWIN2K12R2VM3 | Crest.Contoso.com | root | GRANT ALL | kotak | Mercy | Mysql.* | GRANT ALL ON Mysql.* TO \'Mercy\'@\'localhost\ |
| 09/10/2016 10:19:06 AM | ESXWIN2K12R2VM3 | localhost | root | GRANT ALL | mysql | Henry | Kotak.employees | GRANT ALL ON Kotak.employees TO \'Henry\'@\'localhost\ |
| 09/21/2016 07:29:19 PM | ESXWIN2K12R2VM3 | Crest.Contoso.com | root | GRANT SELECT, INSERT | kotak | charles | kotak.employees | GRANT SELECT, INSERT ON kotak.employees TO \'charles\'@\'10.10.100.78\ |
| 09/21/2016 07:31:19 PM | ESXWIN2K12R2VM3 | Crest.Contoso.com | root | REVOKE SELECT, INSERT | kotak | charles | kotak.employees | REVOKE SELECT, INSERT ON kotak.employees FROM \'charles\'@\'10.10.100.78\ |
| 09/22/2016 10:11:48 AM | ESXWIN2K12R2VM3 | localhost | root | GRANT ALL PRIVILEGES | mysql | bob | mysql.* | GRANT ALL PRIVILEGES ON mysql.* TO \'bob\'@\'localhost\ |

Figure 33

# Alerts

- **MySQL: Service down -** This alert is generated when MySQL service is shutdown by the administrator.
- **MySQL: User authentication failed** – This alert is generated when user enters wrong credentials to connect MySQL database.
- **MySQL**: **Privilege change** – This alert is generated when administrator grants or revokes the privileges to the user.
- **MySQL**: **User created** – This alert is generated when administrator creates the user.

- **MySQL**: **Delete database** – This alert is generated when administrator deletes the database.
- **MySQL**: **Delete table** – This alert is generated when administrator deletes the table.
- **MySQL**: **User password reset** – This alert is generated when administrator resets the user password.

# Import MySQL Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility** icon, and then click the **Import** tab.

   **NOTE: Import the following KP items in the specified sequence.**

   - **Category**
   - **Alerts**
   - **Templates**
   - **Reports**

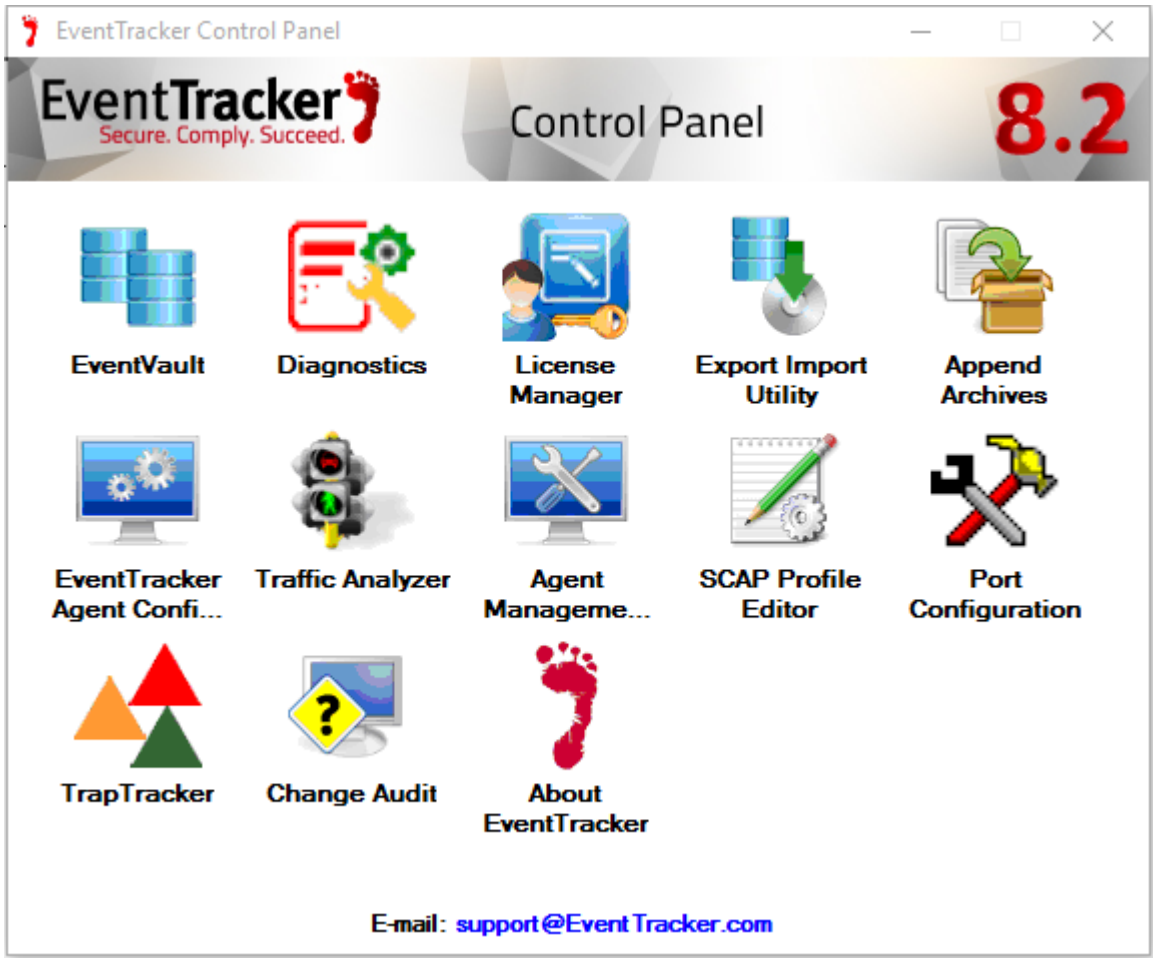


Figure 34

# Category

1. Click **Category** option, and then click the browse button.
2. Locate the **All MySQL group of categories.iscat** file, and then click the **Open** button.

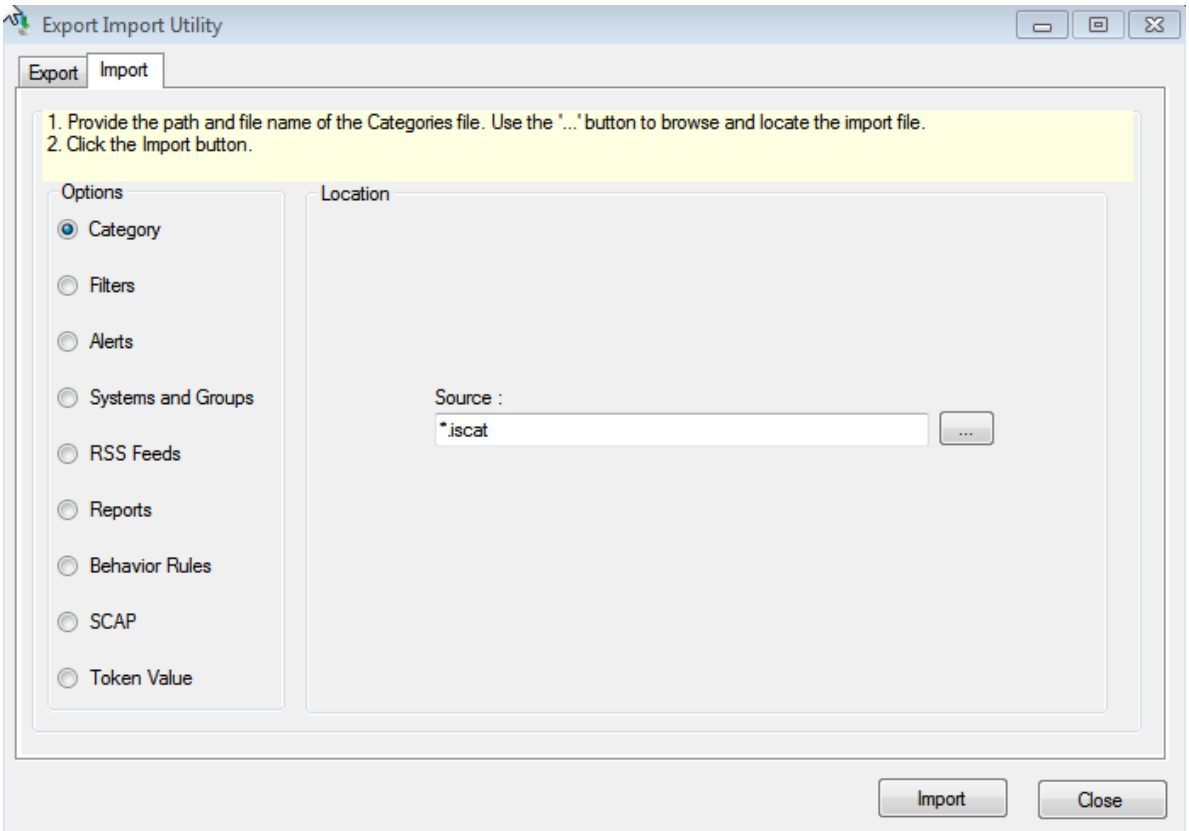


Figure 35

3. Click the **Import** button to import the categories.

   EventTracker displays success message.

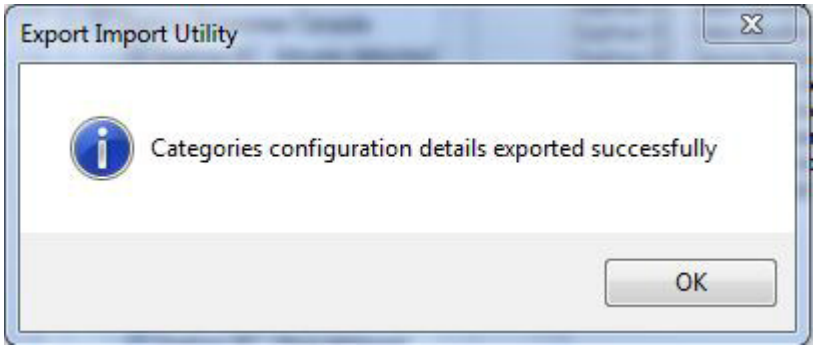


Figure 36

4. Click the **OK** button and then click the **Close** button.

# Alerts

1. Click **Alert** option, and then click the browse button.
2. Locate the **All MySQL group of alerts.isalt** file, and then click the **Open** button.

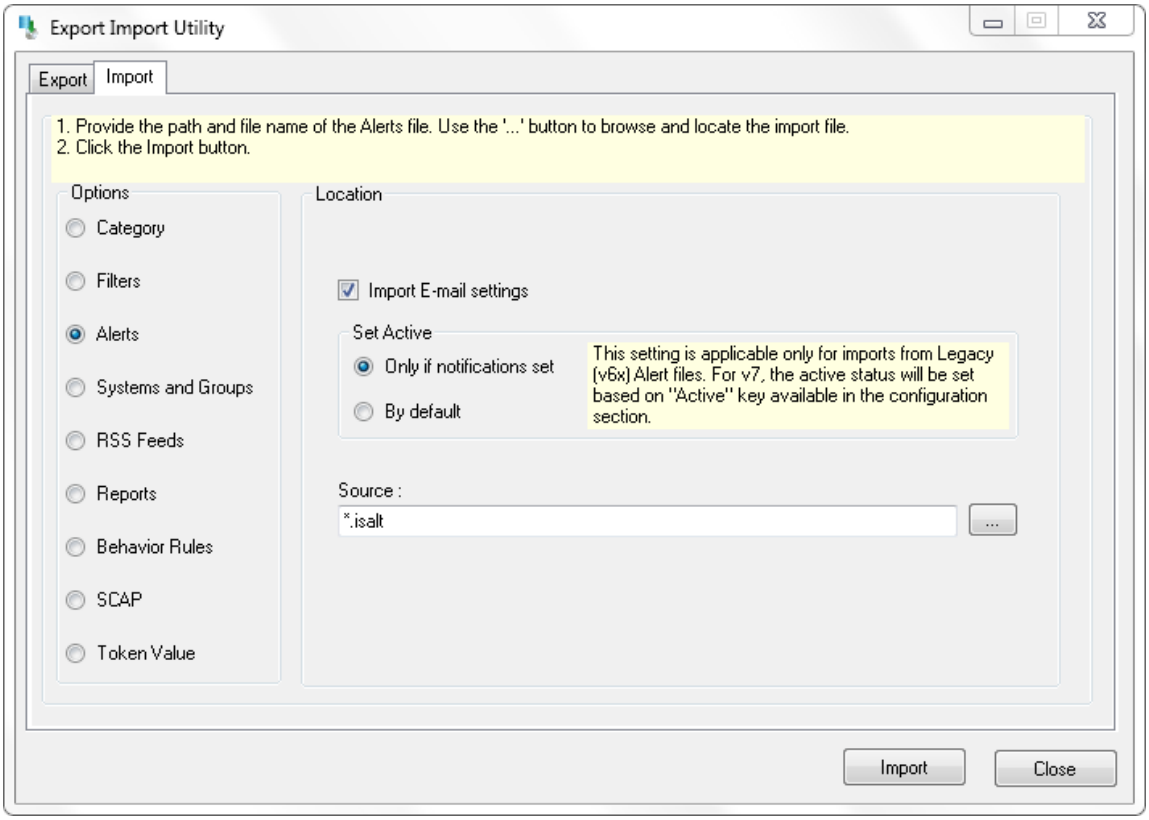


Figure 37

3. Click the **Import** button to import the alerts.

   EventTracker displays success message.

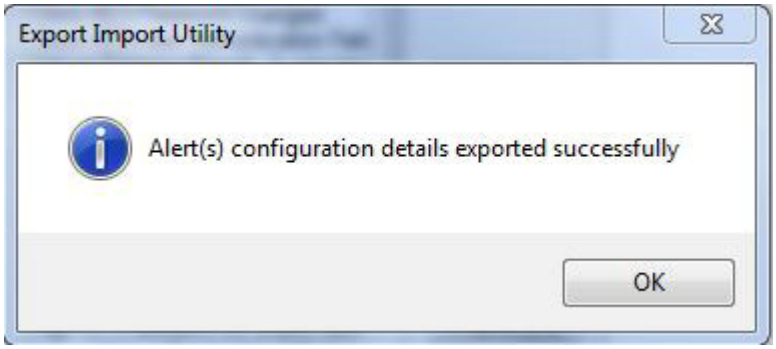


Figure 38

4. Click the **OK** button and then click the **Close** button.

# Templates

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on ' **Import**' option.

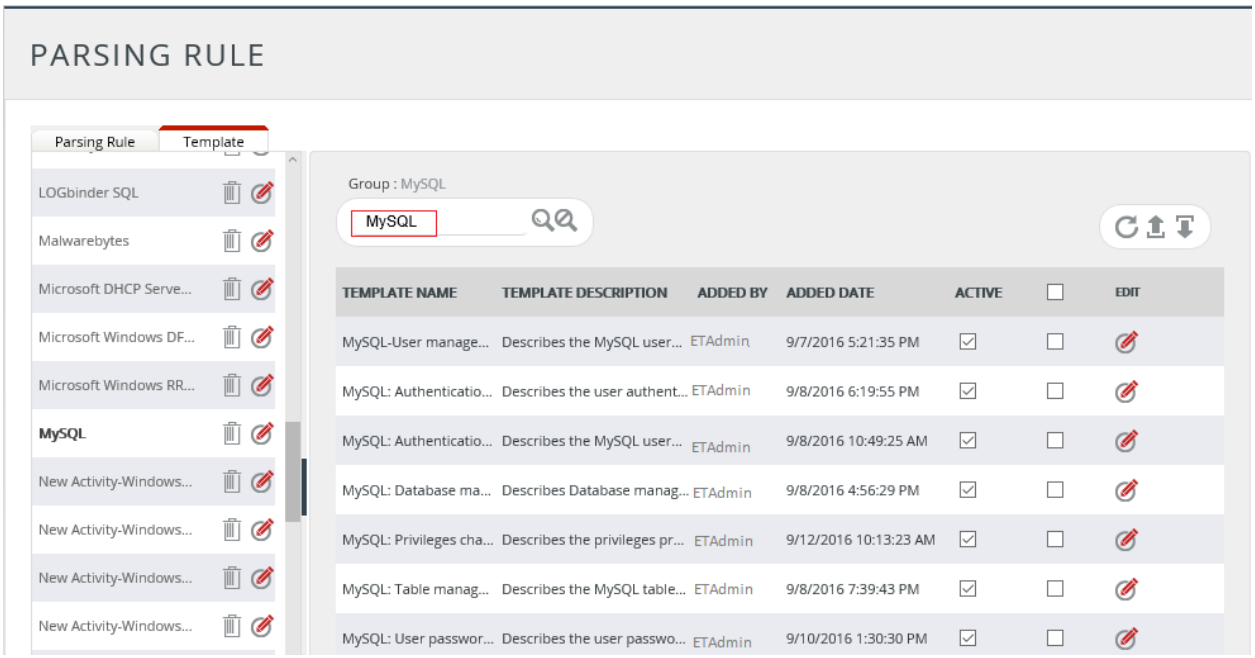

Figure 39

3. Click on **Browse** button.

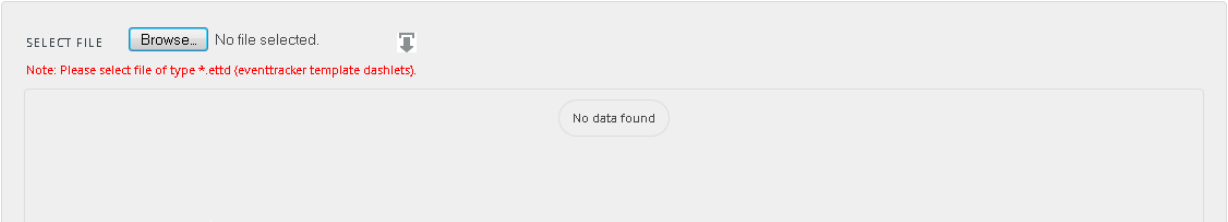

Figure 40

4. Locate **All MySQL group of templates.ettd** file, and then click the **Open** button.

SELECTED FILE IS: All MySQL group of templates.ettd

| TEMPLATE NAME | SEPARATOR | TEMPLATE DESCRIPTION | ADDED DATE | ADDED BY | GROUP NAME |
|---|---|---|---|---|---|
| Windows MySQL-Database management | FILE | Description: ENTRY:20160906 12:35:26,Esxwin2k12r2vm3,root,localhost,4,4,QUERY,,"create database Kotak",0 FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log TYPE:MULTILINE FIELD: * | 9/8/2016 4:56:29 PM | ETAdmin | MySQL |
| Windows MySQL-Privileges management | \t | "ENTRY:20160910 10:13:06,Esxwin2k12r2vm3,root,tom.toons.local,14,130,QUERY,kotak,'GRANT ALL ON Mysql.* TO \'Mercy\'@\'localhost\'',0 FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log TYPE:MULTILINE FIELD: *" | 10/4/2016 1:51:30 PM | ETAdmin | MySQL |
| Windows MySQL-Table management | FILE | Description: ENTRY:20160908 17:35:23,Esxwin2k12r2vm3,root,localhost,13,100,QUERY,iim,"create table Students(SID varchar(20), FName varchar(20), LName varchar(20))",0 FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log TYPE:MULTILINE FIELD: * | 9/8/2016 7:39:43 PM | ETAdmin | MySQL |
| Windows MySQL-User authentication failed | \t | Description: ENTRY:20160927 15:57:13,Esxwin2k12r2vm3,millet,tom.toons.local,321,0,FAILED_CONNECT,kotak,,1045 FILE:C:\Program Files\MariaDB 10.1\data\server_audit.log TYPE:MULTILINEFIELD: * | 9/28/2016 6:49:16 PM | ETAdmin | MySQL |

Figure 41

5. Now select the check box and then click on **'Import'** option. EventTracker displays success message.

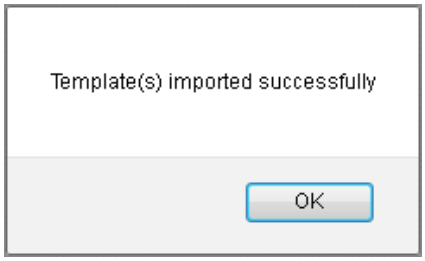


Figure 42

6. Click on **OK** button.

# Reports

1. Click **Report** option, and then click the browse button.
2. Locate **All MySQL group of reports.issch** file, and then click the **Open** button.

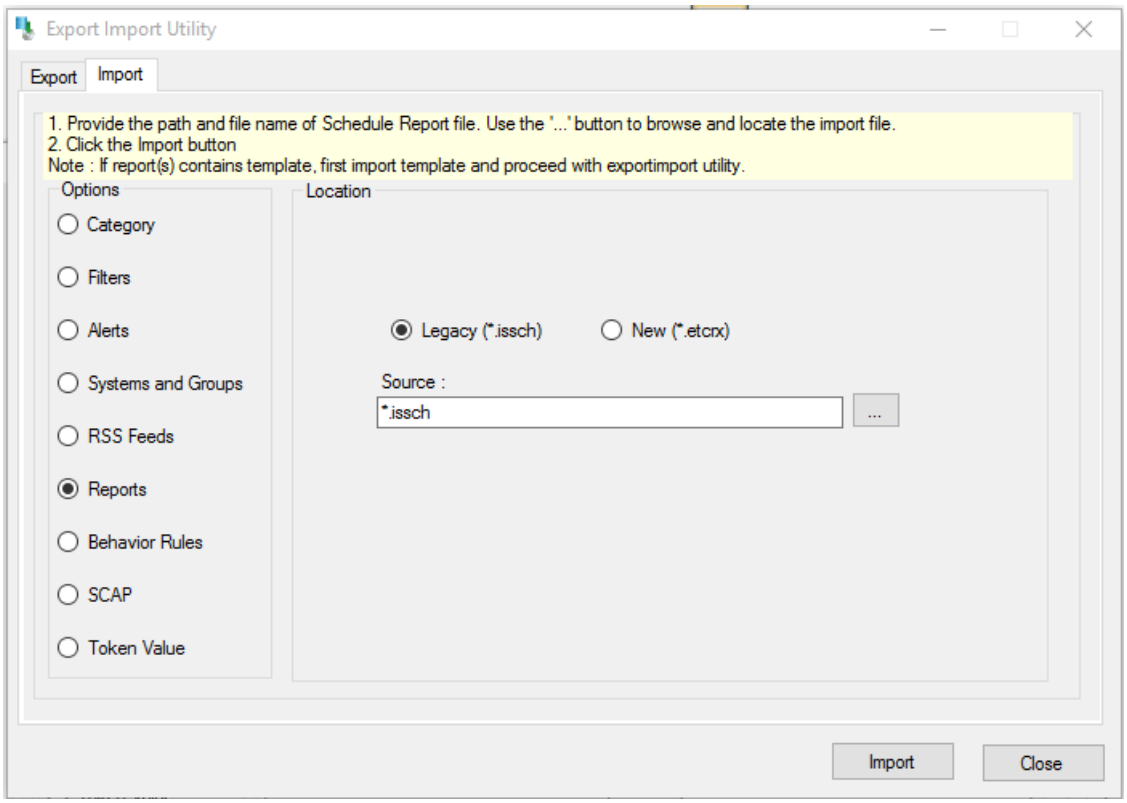


Figure 43

3. Click the **Import** button to import the reports.

   EventTracker displays success message.

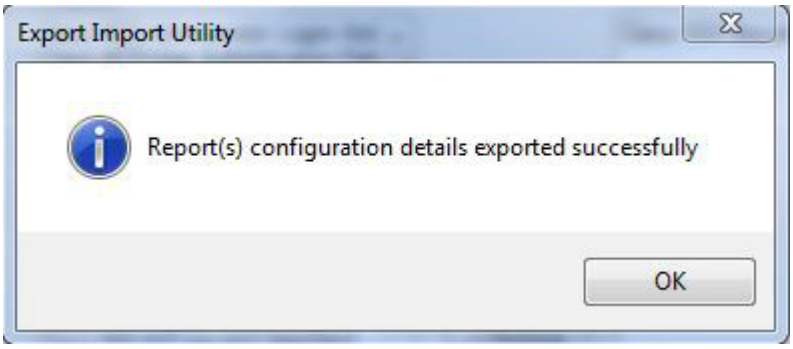


Figure 44

4. Click the **OK** button, and then click the **Close** button.

# Verify Knowledge Pack in EventTracker

## Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and select **Category**.
3. In the **Category Tree**, expand **MySQL** group folder to see the imported categories.

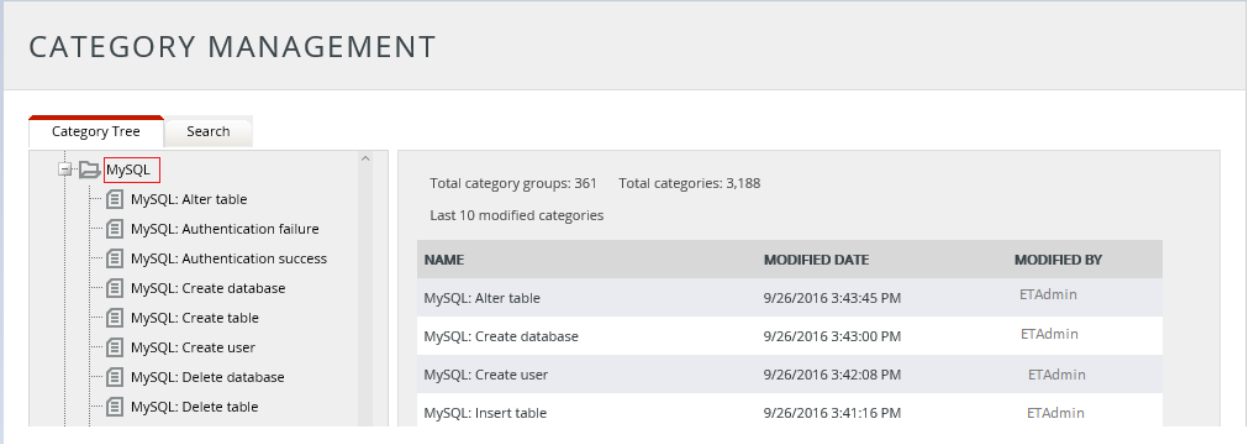


Figure 45

## Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In the **Search** field, enter **'MySQL'**, and then click the **Go** button.

   Alert Management page will display all the imported MySQL alerts.

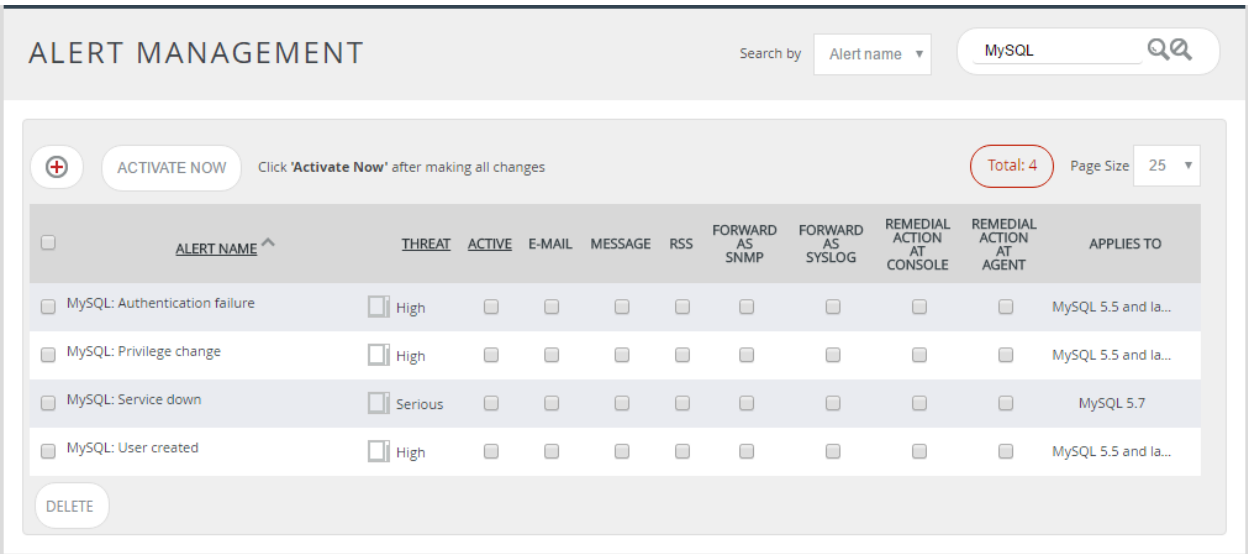


Figure 46

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

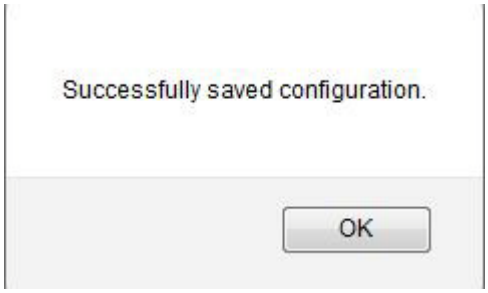


Figure 47

5. Click the **OK** button, and then click the **Activate now** button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

# Templates

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on ‘**Import**’ option.

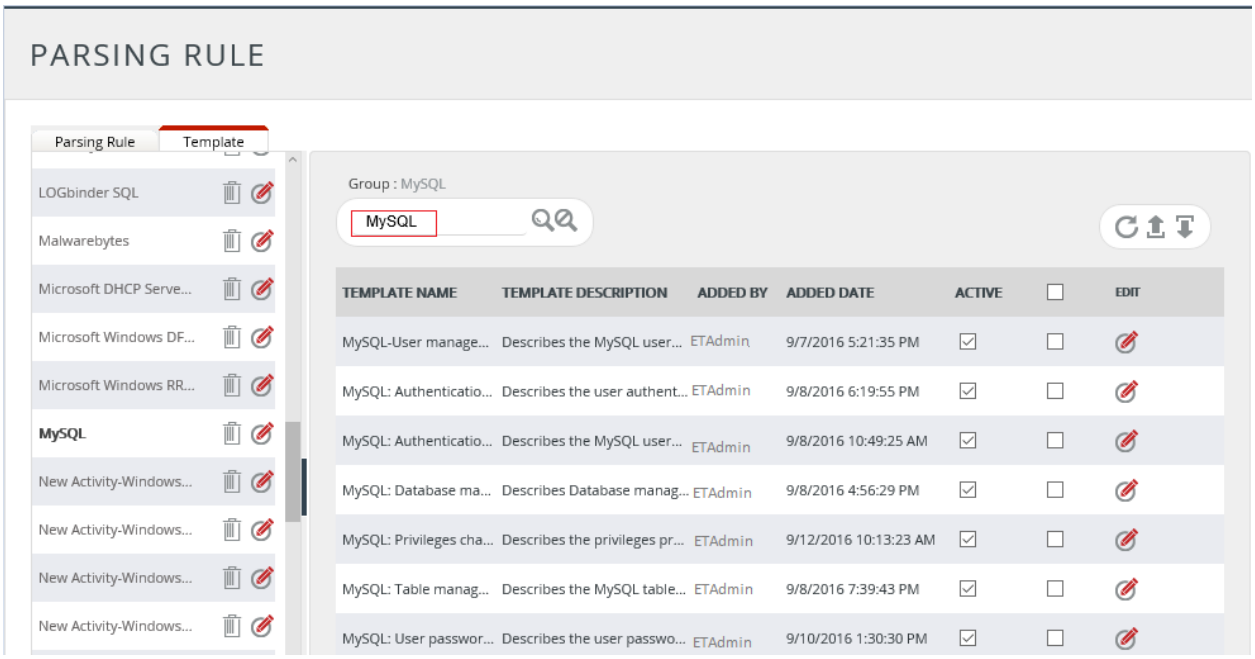


Figure 48

# Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **MySQL** group folder.

   Reports are displayed in the Reports configuration pane.

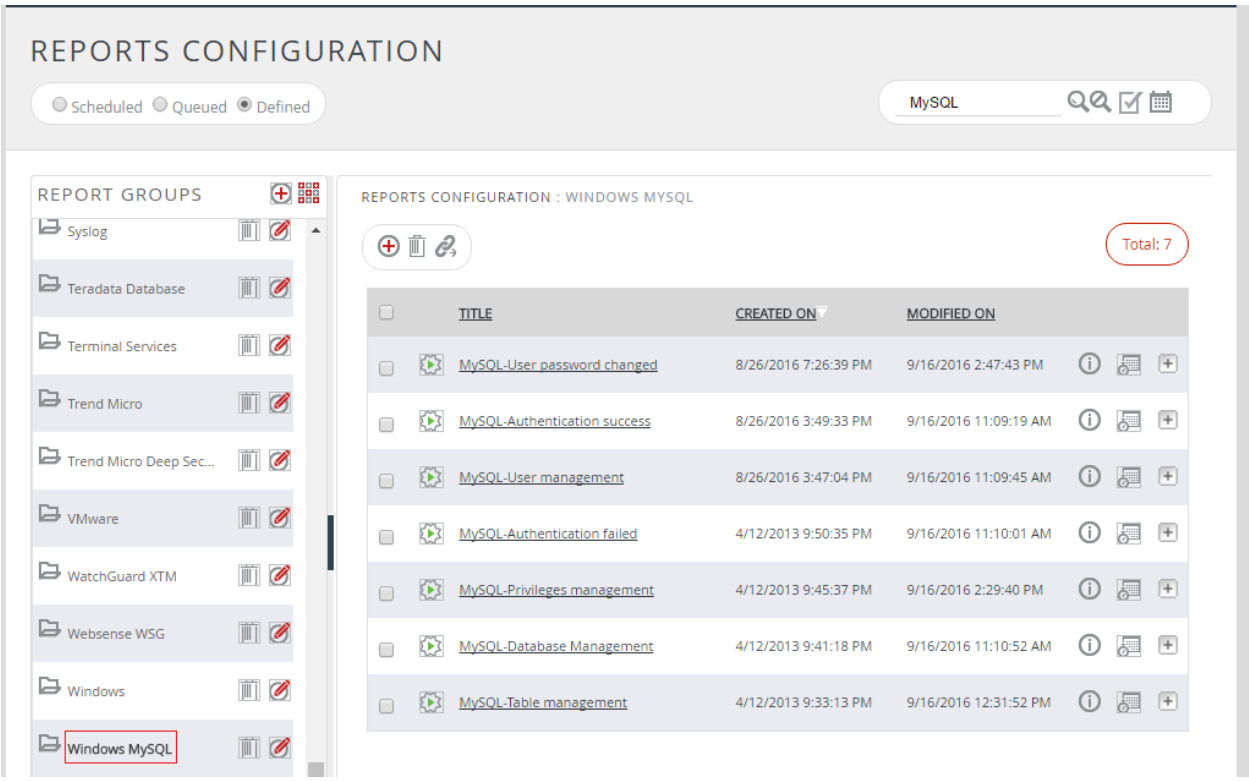


Figure 49

# Create Dashboards in EventTracker

## Schedule Reports

1. Open **EventTracker** in browser and logon.

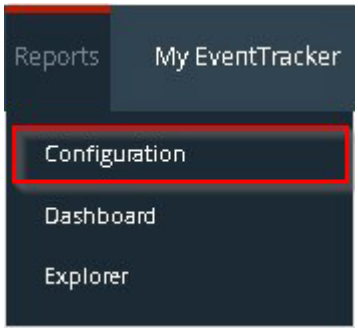


Figure 50

2. Navigate to **Reports>Configuration**.

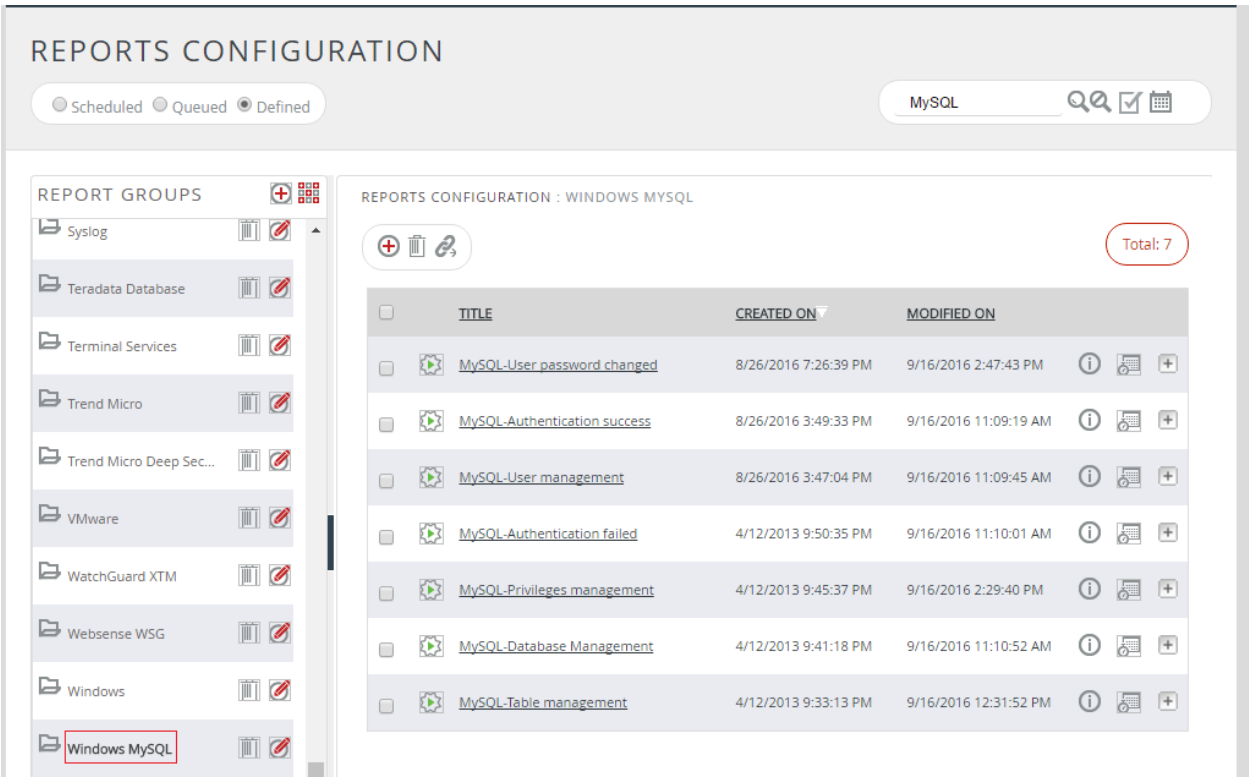


Figure 51

3. Select **MySQL** in report groups. Check '**Defined"** option.
4. Click on '**schedule**'  to plan a report for later execution.

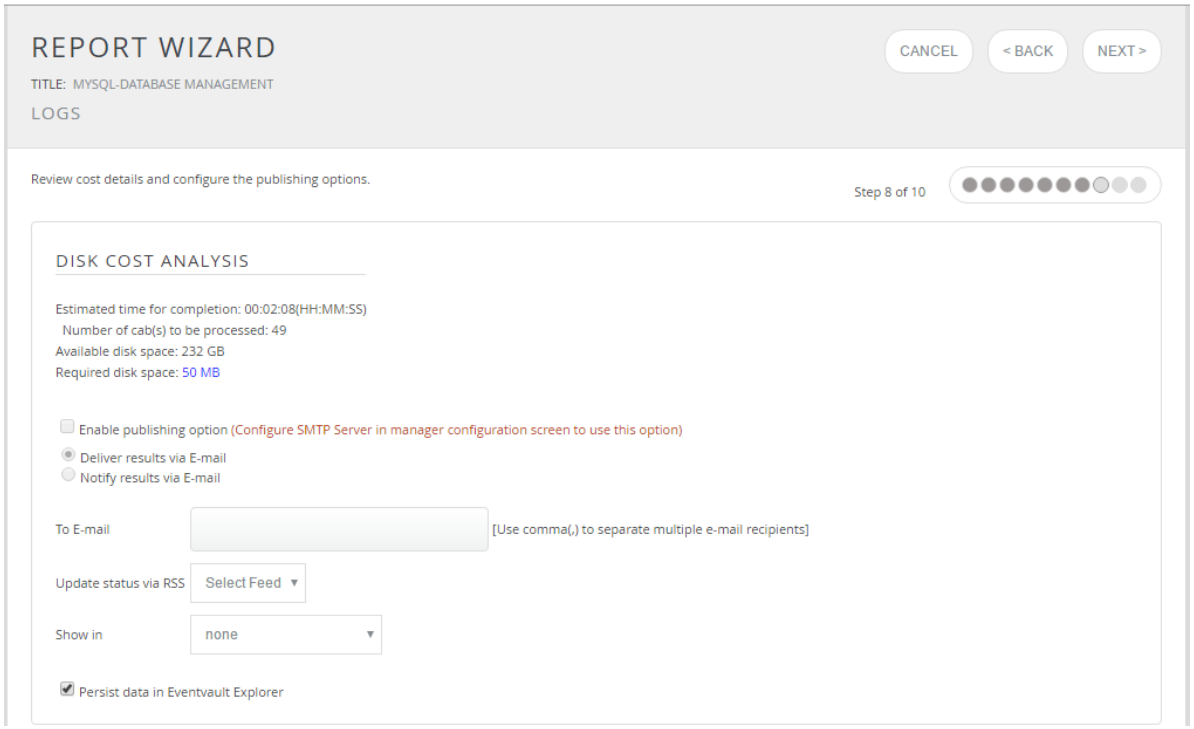


Figure 52

5. Choose appropriate time for report execution and in **Step 8** check '**Persist data in Eventvault explorer"** box.

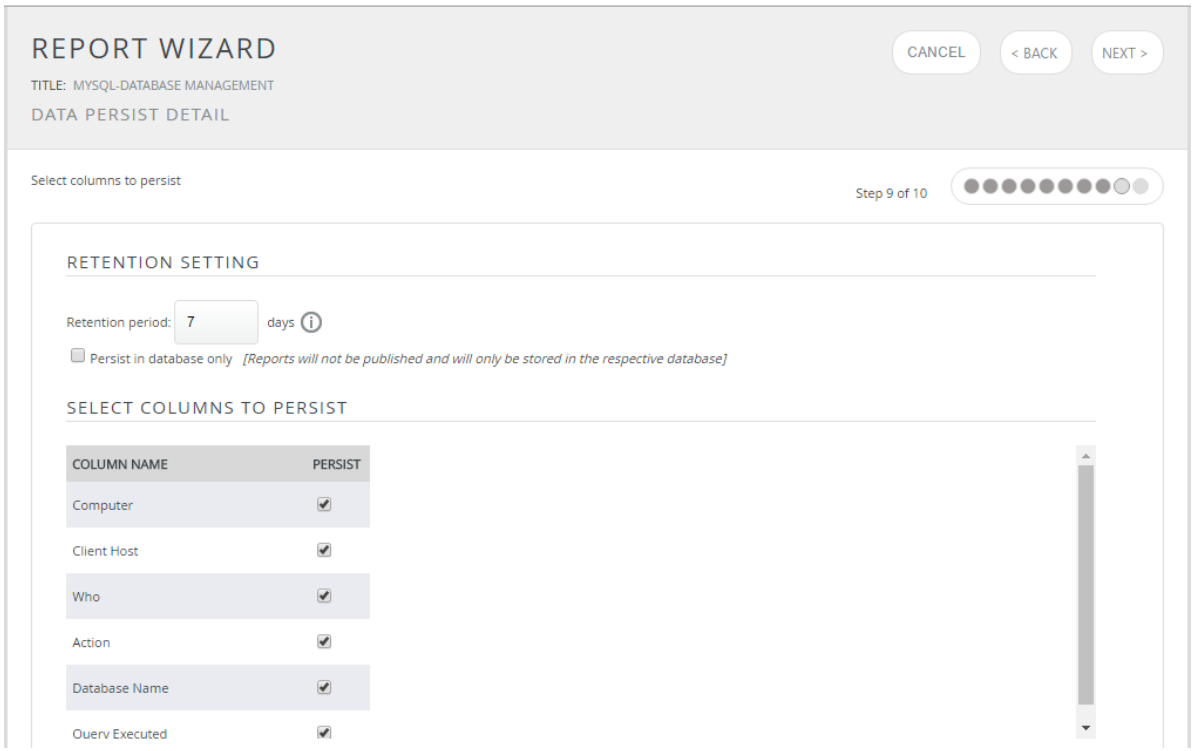


Figure 53

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

# Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.

2. Open **EventTracker** in browser and logon.

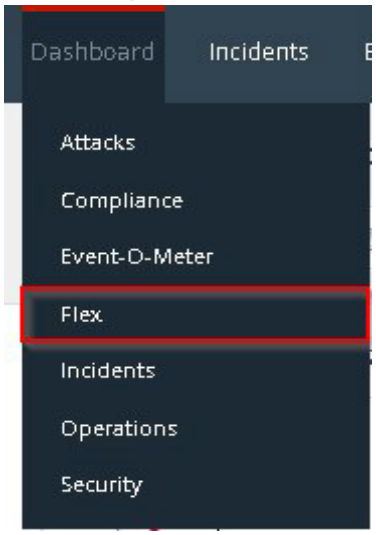


Figure 54

3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

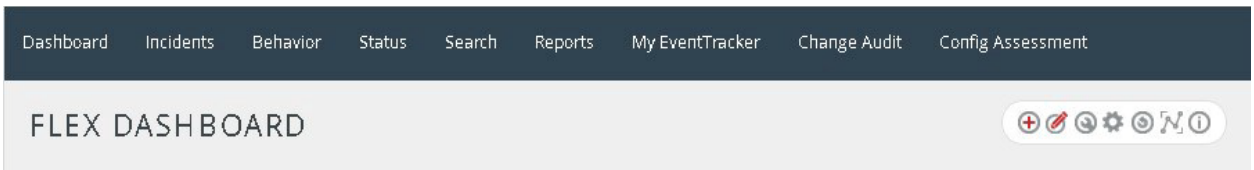


Figure 55

4. Click ⊕ to add a new dashboard.
   Flex Dashboard configuration pane is shown.

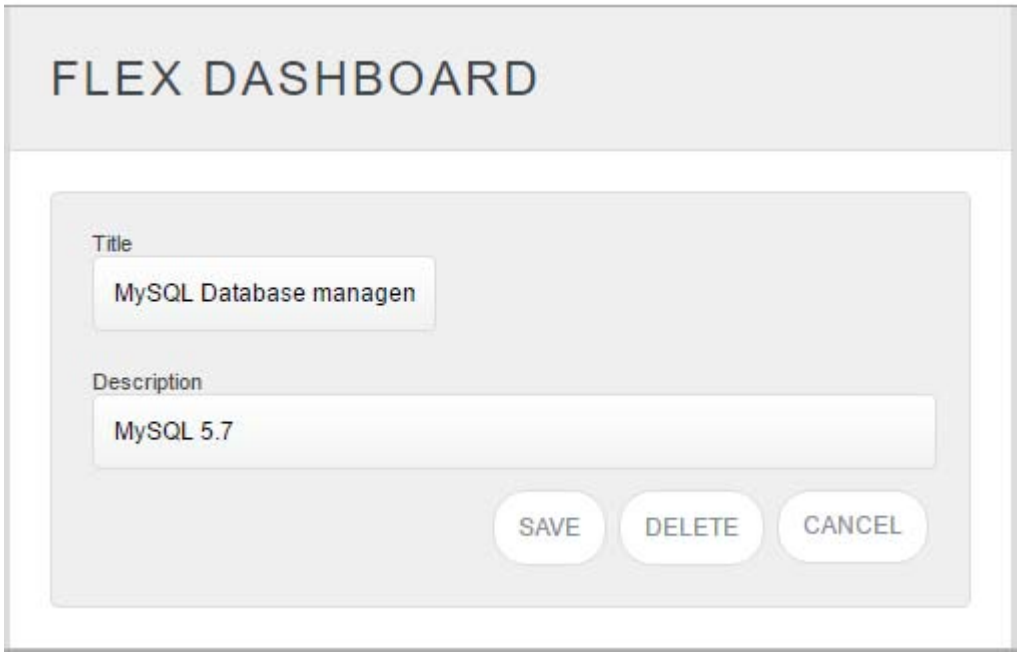


Figure 56

5. Fill fitting title and description and click **Save** button.
6. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.

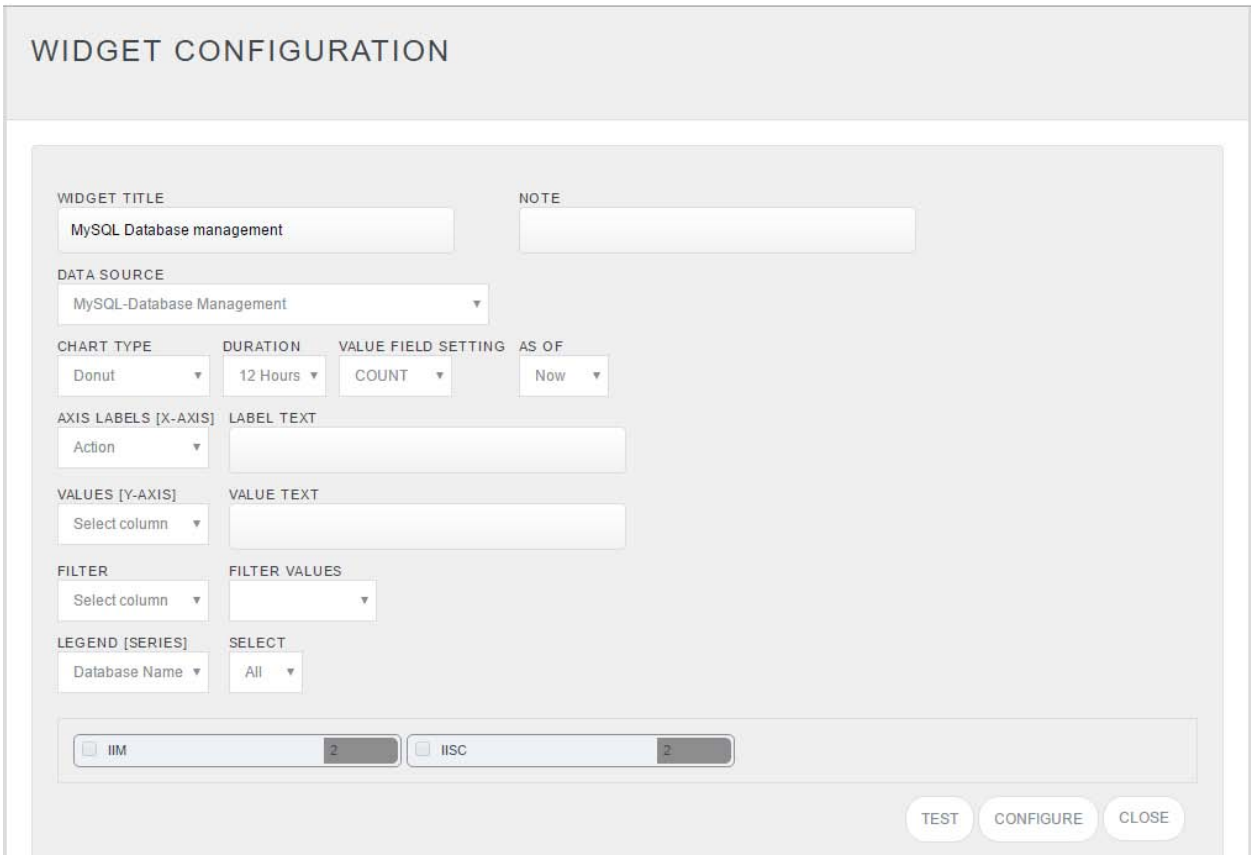


Figure 57

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate. Evaluated chart is shown.

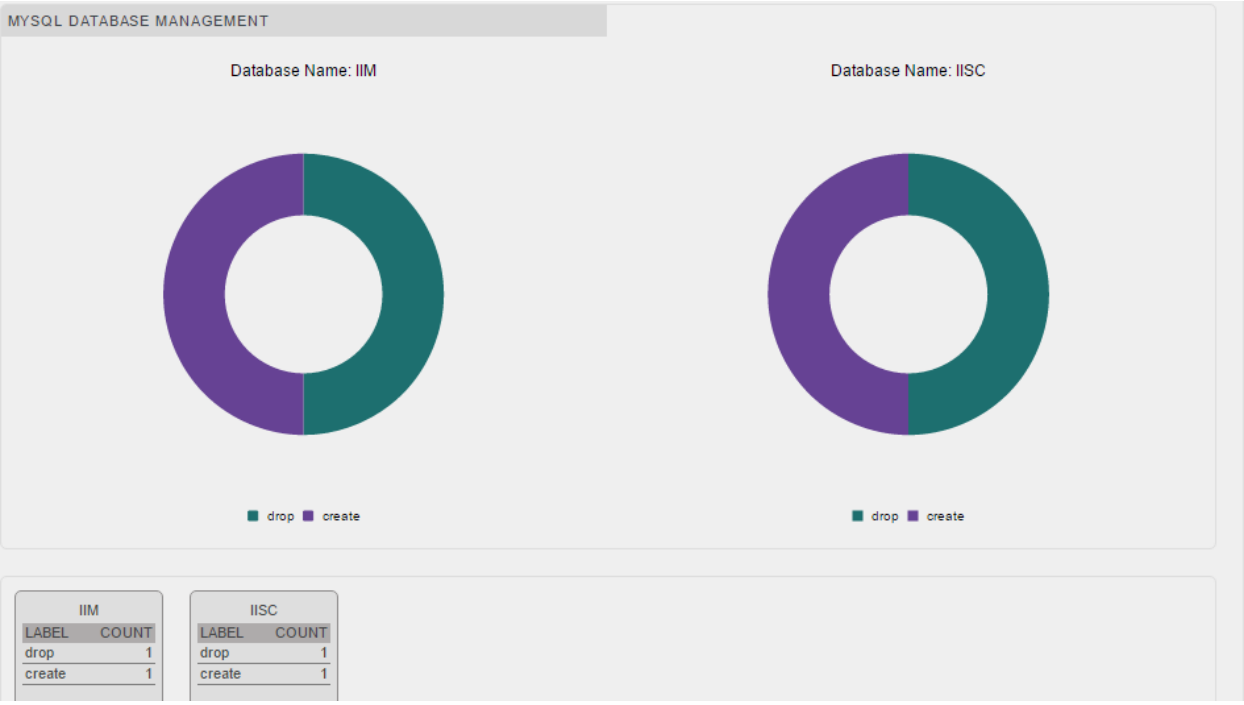


Figure 58

16. If satisfied, click **Configure** button.

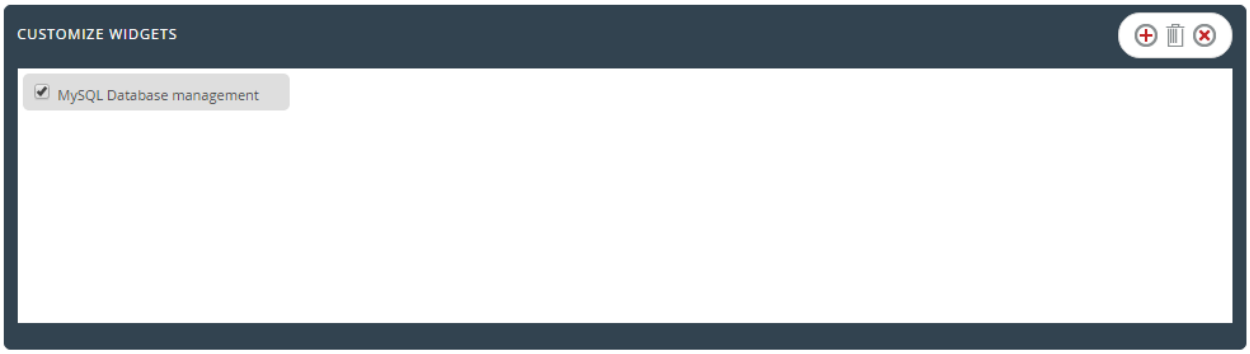


Figure 59

17. Click 'customize' to locate and choose created dashlet.
18. Click to add dashlet to earlier created dashboard.

# Sample Dashboards

For below dashboard **DATA SOURCE: MySQL: Database management**

1. **MySQL: Database management**

- **WIDGET TITLE:** MySQL Database management
  **CHART TYPE:** Donut
  **AXIS LABELS [X-AXIS]:** Database Name
  **Label Text:** Database Name
  **LEGEND [Series]:** Action
  **SELECT**: All

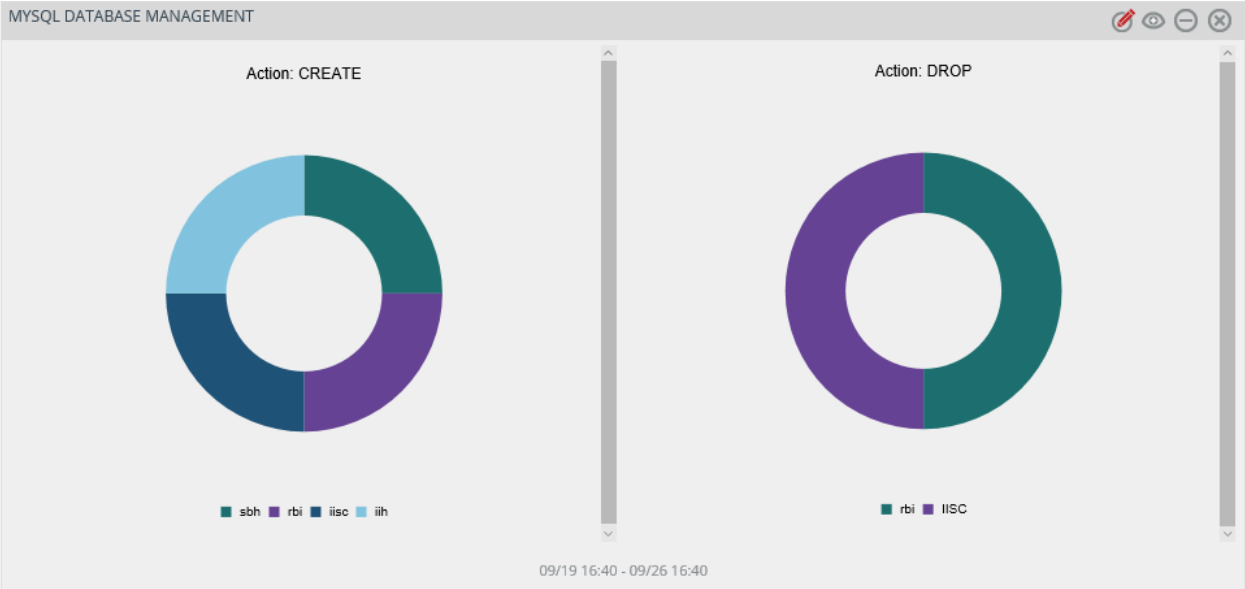


Figure 60

For below dashboard **DATA SOURCE: MySQL: User management**

**2. MySQL: User management**

- **WIDGET TITLE:** MySQL User management
  **CHART TYPE:** Donut
  **AXIS LABELS [X-AXIS]:** MySQL User Name
  **Label Text:** MySQL User Name
  **LEGEND [Series]:** Action
  **SELECT**: All


Figure 61