Integrating LOGbinder SQL

EventTracker v7.x

Publication Date: Sep 5, 2014

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

Abstract

This guide helps you in configuring **LOGbinderSQL** and EventTracker to receive LOGbinderSQL events. You will find the detailed procedures required for monitoring LOGbinderSQL.

Intended audience

Administrators who are assigned the task to monitor and manage events using EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and LOGbinderSQL, Version 2.0.2 and later.

Table of Contents

LOGbinder SQL

LOGbinder SQL runs as a Windows service on a Windows server. It translates audit log entries from Microsoft SQL Server, and outputs them to the LOGbinder SQL event log, the Windows Security Log, Syslog, or Syslog in CEF.

Overview

To monitor LOGbinder SQL in EventTracker, configure LOGbinder SQL to send all events as Windows Security Log to the EventTracker system.

Pre-requisites

- EventTracker v7.x should be installed.
- SQL Server Enterprise should be installed.
  Visit http://www.logbinder.com/PublicFiles/LBSQLGettingStartedGuide
- Install 'LOGbinder SQL' on SQL Server.

Configure LOGbinder SQL to forward all the logs to EventTracker

Install EventTracker Agent on LOGbinder SQL system. Please refer EventTracker Agent Deployment Manual for more details in order to install the Agent.

EventTracker Agent configuration

1. Launch EventTracker Agent configuration
2. Click **Event Filters** tab, and then click **Filter Exception**.

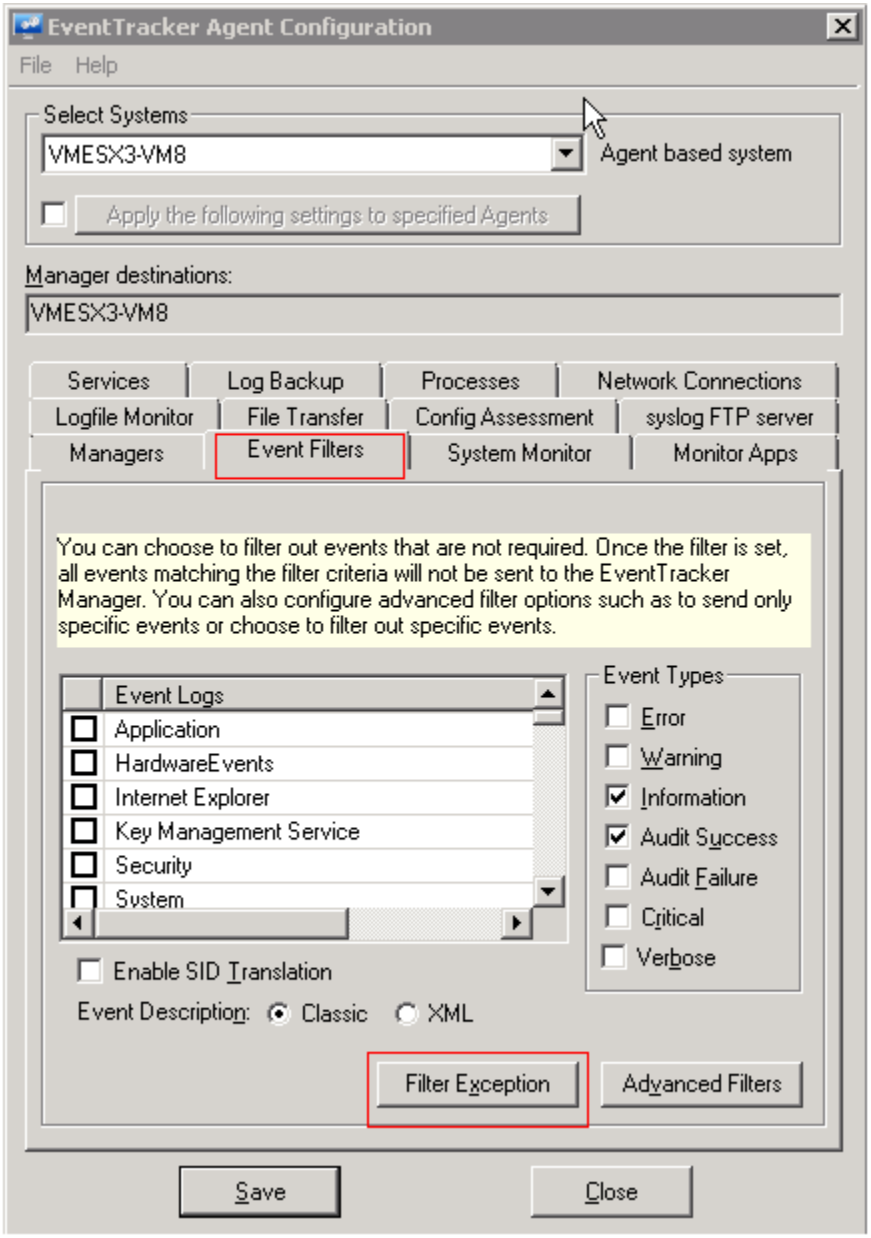

Figure 1

3. Click the **New** button.

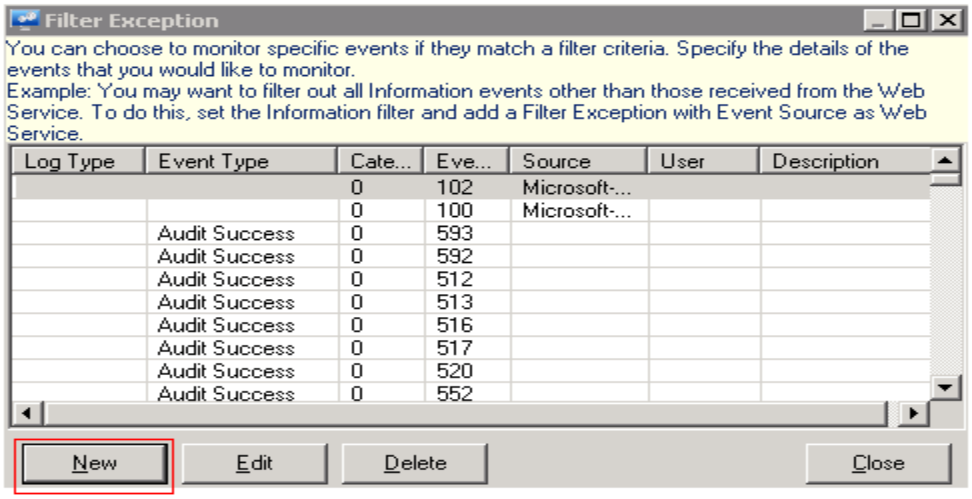

Figure 2

Event Details window displays.

4. In **Match in Source** box, enter **LOGbndSQ.**

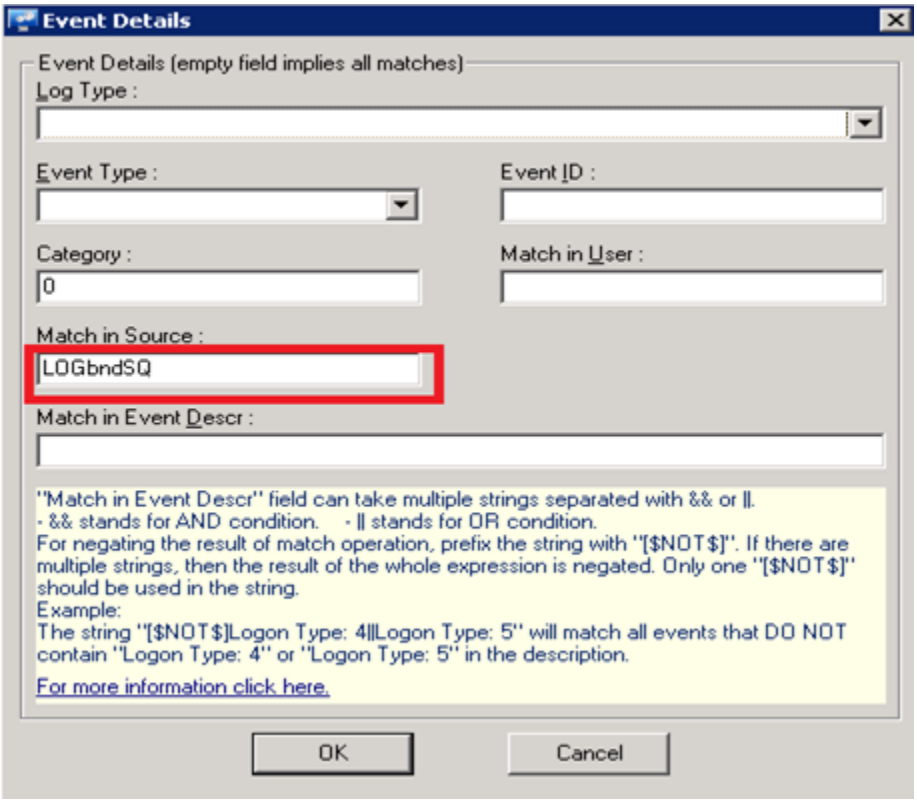

Figure 3

Similarly add **LOGbndSD** in **Match in Source:**.

5. Click **OK**, and then click the **Save** button.

EventTracker Knowledge Pack

Once LOGbinder SQL events are enabled and LOGbinder SQL events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support LOGbinder SQL monitoring.

Categories

- **LOGbinder SQL: Account unlocked -** This category based report provides information related to user account unlocked.
- **LOGbinder SQL: Alter command issued -** This category based report provides information related to alter command issued.
- **LOGbinder SQL: Assembly command issued -** This category based report provides information related to assembly command issued.
- **LOGbinder SQL: Audit change command issued -** This category based report provides information related to audit change command issued.
- **LOGbinder SQL: Audit failure -** This category based report provides information related to audit failure.
- **LOGbinder SQL: Audit session changed -** This category based report provides information related to audit session changed.
- **LOGbinder SQL: Backup command issued -** This category based report provides information related to backup command issued.
- **LOGbinder SQL: Bulk administration command issued -** This category based report provides information related to bulk administration command issued.
- **LOGbinder SQL: Change command issued -** This category based report provides information related to change command issued.
- **LOGbinder SQL: Create command issued -** This category based report provides information related to create command issued.

- **LOGbinder SQL: Delete command issued -** This category based report provides information related to delete command issued.
- **LOGbinder SQL: Login command issued -** This category based report provides information related to login command issued.
- **LOGbinder SQL: Login failed -** This category based report provides information related to user login failed.
- **LOGbinder SQL: Login successful -** This category based report provides information related to user login successful.
- **LOGbinder SQL: Logout successful -** This category based report provides information related to user logout successful.
- **LOGbinder SQL: Database role member addition failed -** This category based report provides information related to member added to database role failed.
- **LOGbinder SQL: Database role member addition success -** This category based report provides information related to member added to database role successful.
- **LOGbinder SQL: Server role member addition failed -** This category based report provides information related to member added to server role failed.
- **LOGbinder SQL: Server role member addition success -** This category based report provides information related to member added to server role successful.
- **LOGbinder SQL: Member deleted from database role failed -** This category based report provides information related to member deleted from database role failed.
- **LOGbinder SQL: Member deleted from database role successful -** This category based report provides information related to member deleted from database role successful.
- **LOGbinder SQL: Member deleted from server role failed -** This category based report provides information related to member deleted from server role failed.
- **LOGbinder SQL: Member deleted from server role successful -** This category based report provides information related to member deleted from server role successful.
- **LOGbinder SQL: Password change failed -** This category based report provides information related to user password change failed.
- **LOGbinder SQL: Password change successful -** This category based report provides information related to user password change successful.

- **LOGbinder SQL: Password expired -** This category based report provides information related to user password expired.
- **LOGbinder SQL: Privileges change successful -** This category based report provides information related to privileges change successful.
- **LOGbinder SQL: Privileges change command issued -** This category based report provides information related to privileges change command issued.
- **LOGbinder SQL: Privileges change failed -** This category based report provides information related to privileges change failed.
- **LOGbinder SQL: Restore command issued -** This category based report provides information related to restore command issued.
- **LOGbinder SQL: Scope command issued -** This category based report provides information related to scope command issued.
- **LOGbinder SQL: Security command issued -** This category based report provides information related to security command issued.
- **LOGbinder SQL: Server principal disable command issued -** This category based report provides information related to server principal disable command issued.
- **LOGbinder SQL: Server principal enable command issued -** This category based report provides information related to server principal enable command issued.
- **LOGbinder SQL: Server state command issued -** This category based report provides information related to server state command issued.

Alerts

- **LOGbinder SQL: Audit change command issued -** This alert is generated when audit change command is issued.
- **LOGbinder SQL: Audit failure -** This alert is generated when user audit failed.
- **LOGbinder SQL: Change command issued -** This alert is generated when change command is issued.
- **LOGbinder SQL: Delete command issued -** This alert is generated when delete command is issued.

- **LOGbinder SQL: Login failed -** This alert is generated when user login failed.
- **LOGbinder SQL: Database role member addition success-** This alert is generated when member added to database role successful.
- **LOGbinder SQL: Server role member addition success -** This alert is generated when member added to server role successful.
- **LOGbinder SQL: Member deletion from database role successful-** This alert is generated when member remove from database role successful.
- **LOGbinder SQL: Member deletion from server role successful-** This alert is generated when member remove from server role successful.
- **LOGbinder SQL: Password expired -** This alert is generated when user password expired.
- **LOGbinder SQL: Privileges change successful -** This alert is generated when privileges change is successful.
- **LOGbinder SQL: Privileges change command issued -** This alert is generated when privileges change command is issued.

Import LOGbinder SQL knowledge pack into EventTracker

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

   Import **Category/Alert/Tokens/ Flex Reports** as given below.

Import Category

1. Click **Category** option, and then click the browse  button.

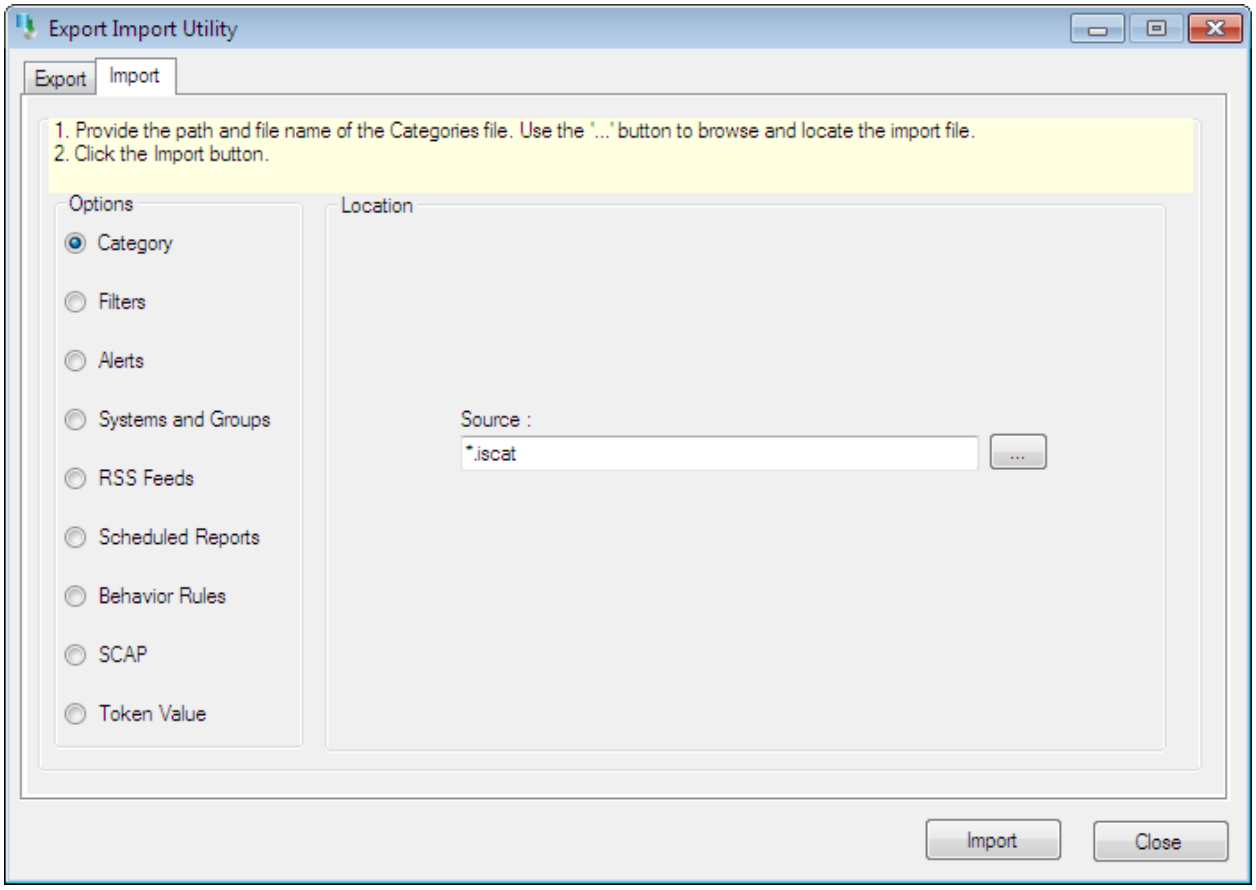

Figure 4

2. Locate **All LOGbinder SQL group of Categories.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button.

   EventTracker displays success message.

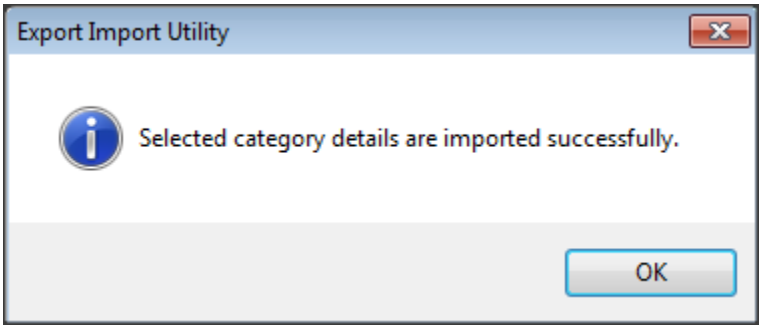

Figure 5

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

Import Alerts

1. Click **Alerts** option, and then click the **browse**  button.

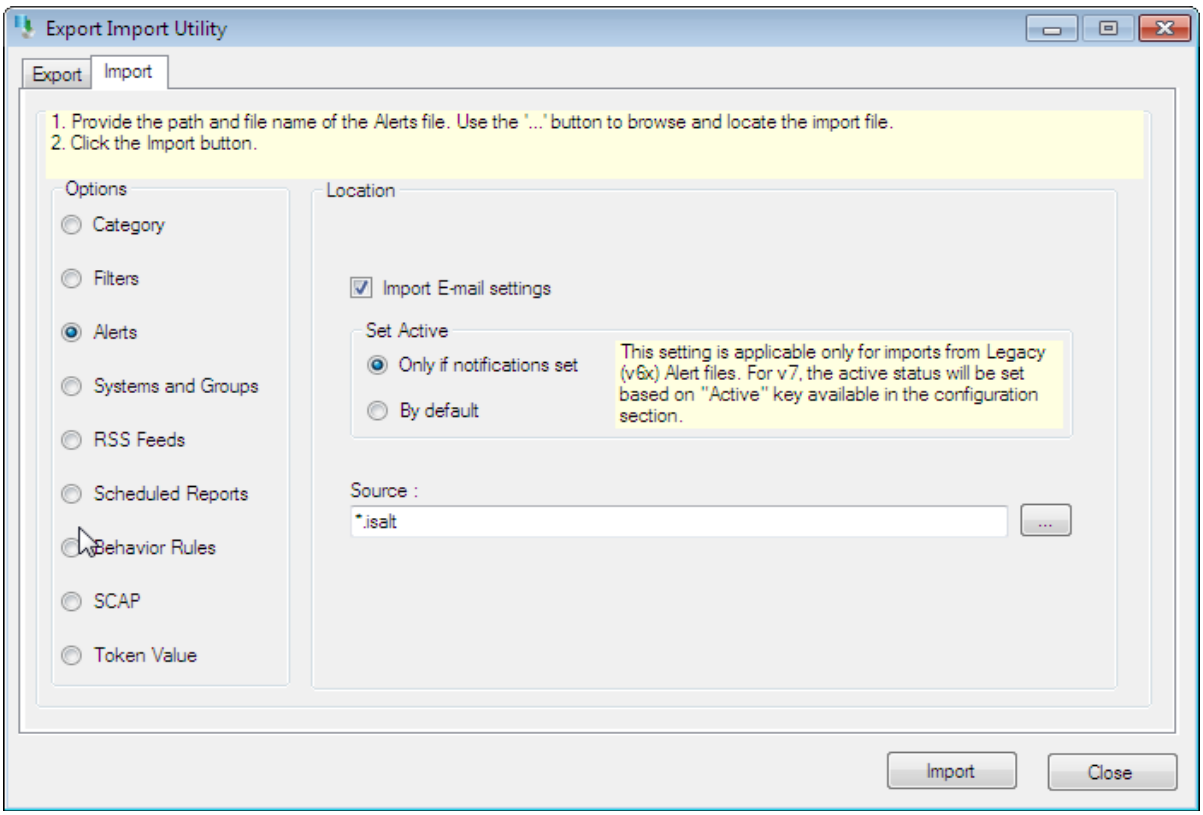

Figure 6

2. Locate **All LOGbinder SQL group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   EventTracker displays success message.

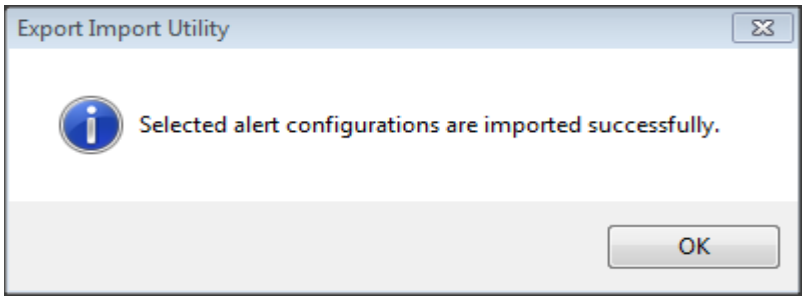

Figure 7

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

Verify LOGbinder SQL knowledge pack in EventTracker

Verify LOGbinder SQL Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **LOGbinder SQL** group folder to view the imported categories.

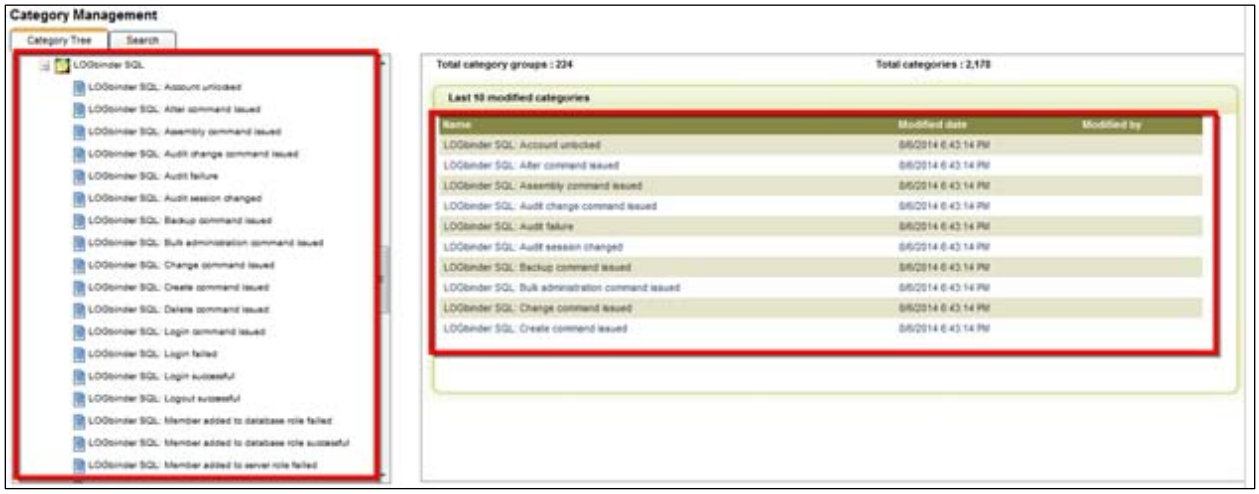

Figure 8

Verify LOGbinder SQL Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**LOGbinder SQL** ', and then click the **Go** button.

   Alert Management page will display all the imported LOGbinder SQL alerts.

Figure 9

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

   EventTracker displays message box.

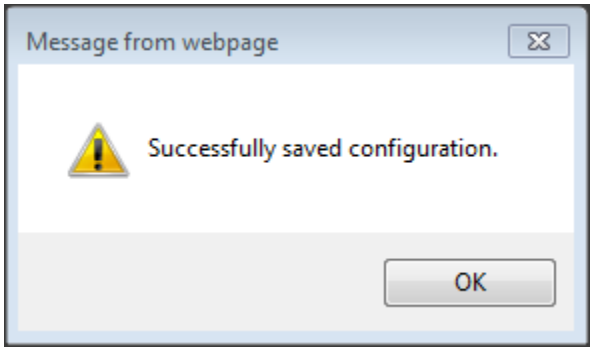

Figure 10

5. Click **OK**, 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.

Sample Reports

When the incident occurs, it is displayed in Incidents/Tabular Dashboard, Keyword Dashboard.

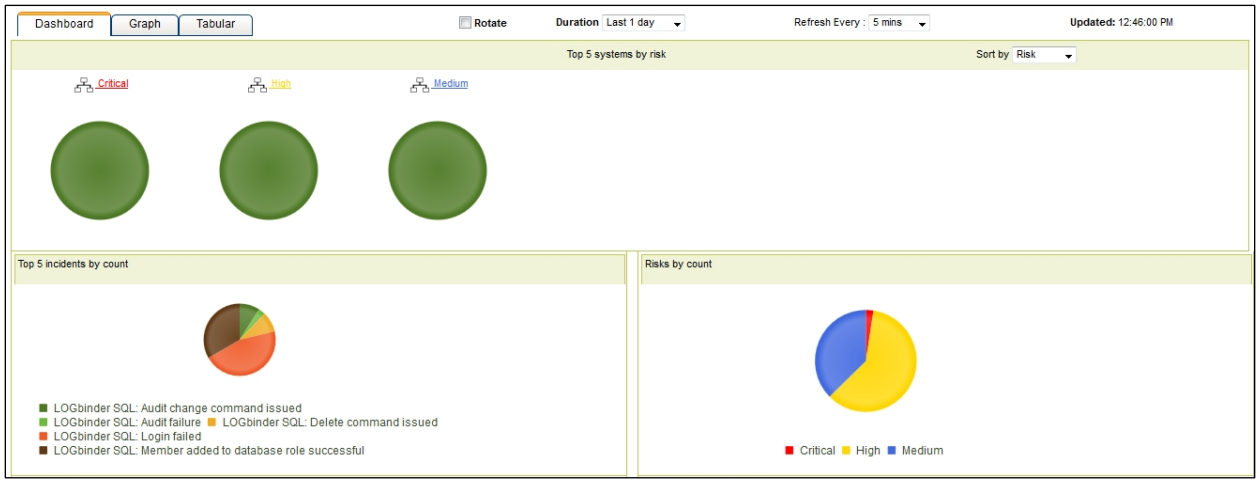

Figure 11

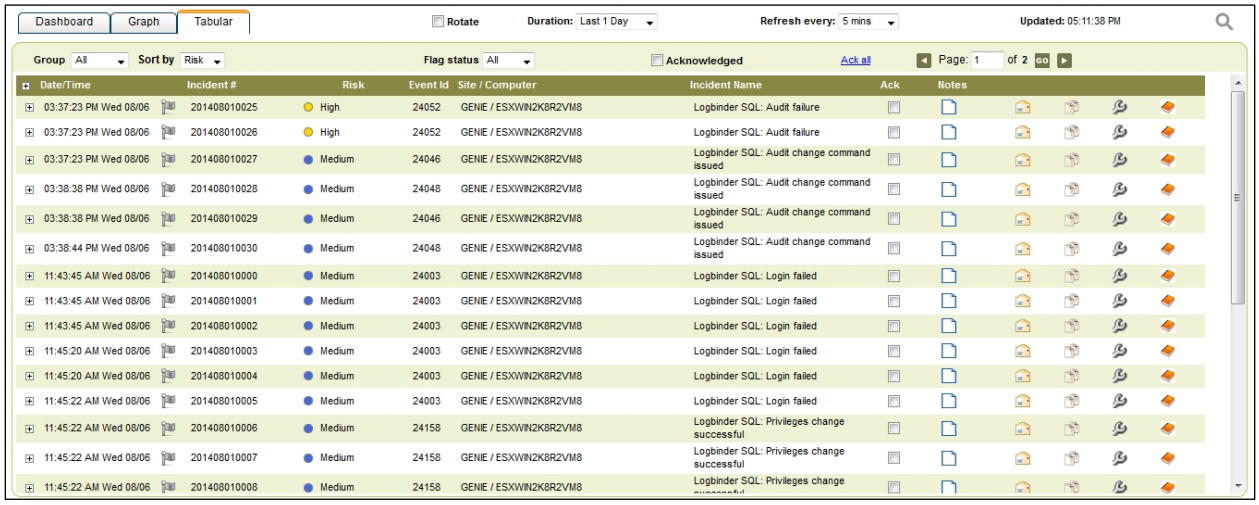

Figure 12

Figure 13

Some sample reports generated in EventTracker are given below.

LOGbinder SQL-Authentication failed report

Event Time	Action Groupname	SQL Server Name	Username	Reason
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM2\EVENTTRACKER	James	An attempt to login using SQL authentication failed
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM4\EVENTTRACKER	Mark	Password did not match that for the login provided
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM3\SQL	joeb	An attempt to login using SQL authentication failed
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM7\EVENTTRACKER	Smith	An attempt to login using SQL authentication failed
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM3\SQL	David	Password did not match that for the login provided
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM2\EVENTTRACKER	James	An attempt to login using SQL authentication failed
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM8	Richard	Password did not match that for the login provided
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM2\EVENTTRACKER	Thomas	Password did not match that for the login provided
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM2\EVENTTRACKER	James	Password did not match that for the login provided
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM2\EVENTTRACKER	Paul	Password did not match that for the login provided
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM2\EVENTTRACKER	Mark	Password did not match that for the login provided
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM3\SQL	Matt	An attempt to login using SQL authentication failed
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM3\SQL	Jason	An attempt to login using SQL authentication failed
7/29/2014 8:58:49.0000000 AM	FAILED_LOGIN_GROUP	ESXWIN2K8R2VM3\SQL	Mark	An attempt to login using SQL authentication failed

Figure 14

LOGbinder SQL-Database Privileges Change Failed Report

Event Time	Action Groupname	SQL Server Name	User Name	Session ID	Database Name	Target Object Name	Statement
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	MSSQL	Contoso\Administrator	67	EmployeeDatabase	n/a	REVOKE VIEW DEFINITION TO Kevin_dummy CASCADE
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	Esxwin2k8r2vm2	Contoso\James	67	SalesDatabase	n/a	REVOKE GRANT OPTION FOR CREATE VIEW FROM Kevin_dummy CASCADE;; -- 24195: Issued deny database object permissions command
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	Esxwin2k8r2vm3\Eventtracker	Contoso\Administrator	67	IT AdminDatabase	n/a	REVOKE CREATE CERTIFICATE TO Kevin_dummy
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	MSSQL	Contoso\Smith	67	Eventtracker	n/a	DENY VIEW DEFINITION TO Kevin_dummy CASCADE
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	Esxwin2k8r2vm3\Eventtracker	Contoso\Paul	67	EmployeeDatabase	n/a	DENY CREATE CERTIFICATE TO Kevin_dummy
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	MSSQL	Contoso\Jason	67	IT AdminDatabase	n/a	GRANT CREATE VIEW TO Kevin_dummy WITH GRANT OPTION
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	Esxwin2k8r2vm3\Eventtracker	Contoso\Smith	67	SalesDatabase	n/a	GRANT ALTER ANY ASSEMBLY TO Kevin_dummy
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	MSSQL	Contoso\Paul	67	FinancialDatabase	n/a	REVOKE VIEW DEFINITION TO Kevin_dummy CASCADE
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	Esxwin2k8r2vm3\Eventtracke	Contoso\Administrator	67	EmployeeDatabase	n/a	REVOKE GRANT OPTION FOR CREATE VIEW FROM Kevin_dummy CASCADE;; -- 24195: Issued deny database object permissions command
8/22/2013 6:07:51.0000000 PM	DATABASE_PERMISSION_CHANGE_GROUP	MSSQL	Contoso\Administrator	67	FinancialDatabase	n/a	REVOKE CREATE CERTIFICATE TO Kevin_dummy

Figure 15