EventTracker

Actionable Security Intelligence

Integrate Microsoft SQL Server

EventTracker v8.x and above

Publication Date: April 18, 2017

Abstract

This guide provides instructions to configure Microsoft SQL server auditing and forward relevant events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, **Microsoft SQL Server 2008, 2012 and 2014 Enterprise** Edition.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

Introduction

MS SQL Server is Microsoft's relational database management system with a large number of features and services. With this coverage, there is a large surface area for attack and vulnerabilities.

SQL Server auditing can be utilized to address requirements for compliance, analyze database actions to troubleshooting problems and investigate suspicious activity.

EventTracker can employ both server audit specifications and extended events to receive relevant events for auditing. Configuration techniques for both methodologies are shown below. Please configure any method of your choice in accordance with your infrastructure and audit requirements. Both techniques are compared below:

Audit Types	Pro's	Con's
Audit Specifications (available in Microsoft SQL server 2008 or later)	• Alerts are received in real-time. • Events are received in Windows Event Viewer.	• Additional fields like client host name, client application name are missing.
Extended Events (available in Microsoft SQL server 2012 or later)	• Additionally, provides client host name, client application name and event category fields. • Lightweight and utilizes few performances resources.	• Alerts are received with a maximum delay of two hours.

Server audit specifications

Auditing, an instance of SQL Server or a SQL Server database involves tracking and logging events that occur on the system. **Below mentioned configuration must be applied on all workstations, where SQL audit is required.**

Prerequisites

1. **Microsoft SQL server 2008 or later** must be installed.
2. **Microsoft SQL Management Studio** for the respective version must be installed.
3. **EventTracker agent 8.x or later** must be installed on the SQL SERVER workstation.

Enable logging for logins*

1. Open **Microsoft SQL** management studio with appropriate credentials.
2. In **Object Explorer**, right-click on database server and select **Properties**.

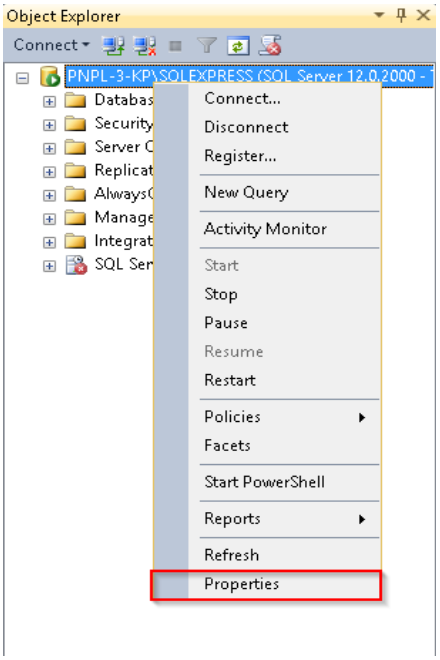
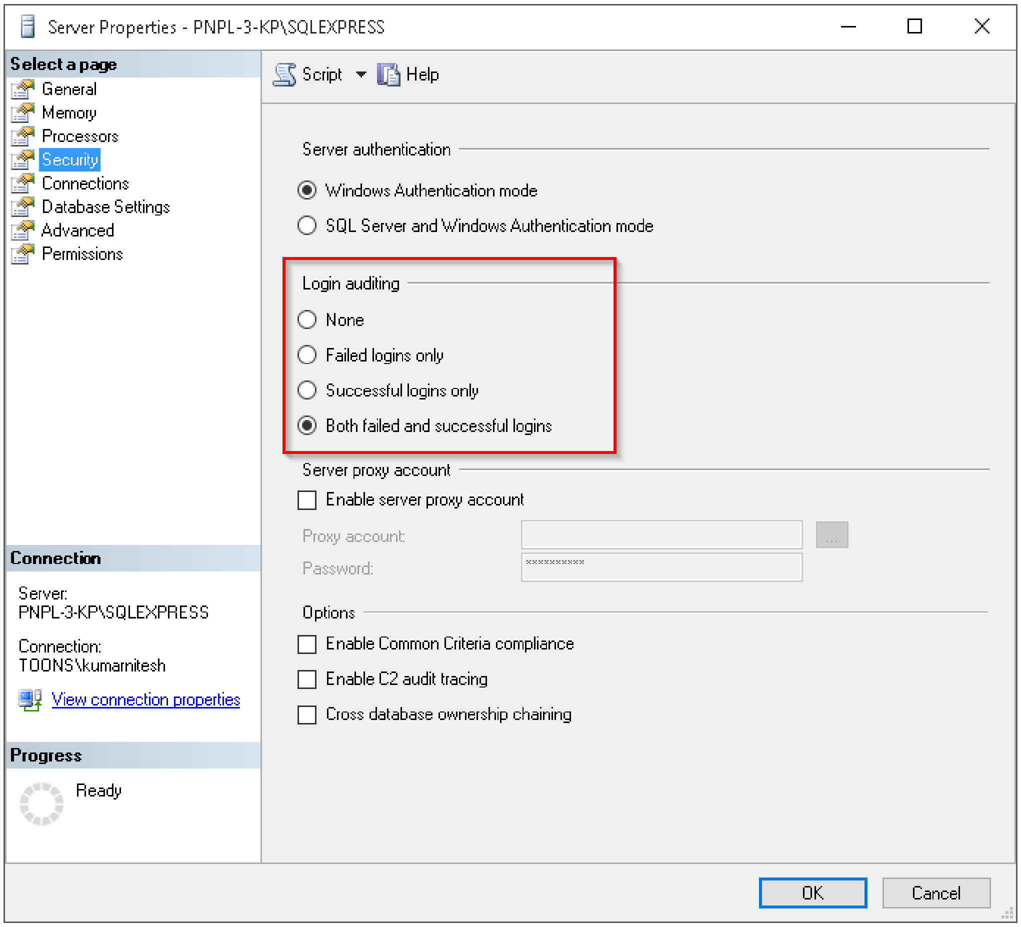


Figure 1

3. In **Properties** pane, select **Security** in **Select a page** section.
4. In **Login auditing**, select **Both failed and successful logins.**



Server Properties - PNPL-3-KP\SQLEXPRESS

Server authentication

● Windows Authentication mode

○ SQL Server and Windows Authentication mode

Login auditing

○ None

○ Failed logins only

○ Successful logins only

● Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: ***********

Options

□ Enable Common Criteria compliance

□ Enable C2 audit tracing

□ Cross database ownership chaining

Connection

Server:
PNPL-3-KP\SQLEXPRESS

Connection:
TOONS\kumarnitesh

Figure 2

5. Above configuration generates event id “**18453”** (login success) and “**18456**” (login failure).

***Login success events are very noisy, enable with caution.**

Enable server auditing

- Open **Microsoft SQL management studio** with appropriate credentials.
- In **Object explorer**, expand **Security** tab to view **Audits** and **Server Audit Specifications** options.

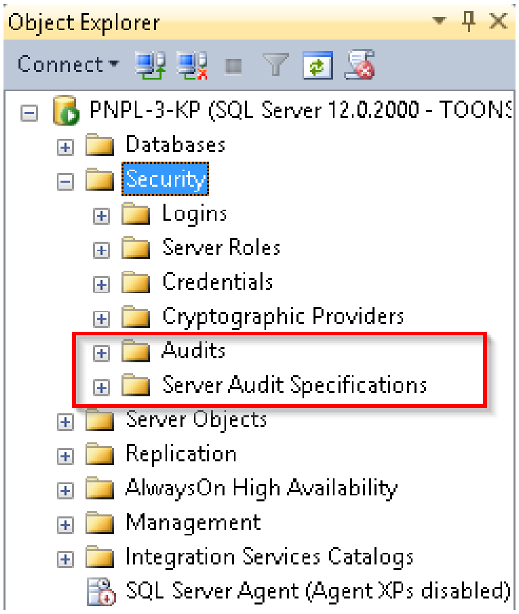

Object Explorer
Connect
PNPL-3-KP (SQL Server 12.0.2000 - TOONS
Databases
Security
Logins
Server Roles
Credentials
Cryptographic Providers
Audits
Server Audit Specifications
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalogs
SQL Server Agent (Agent XPs disabled)

Figure 3

Create audits

1. Right-click **Audits** to select **New Audit...**

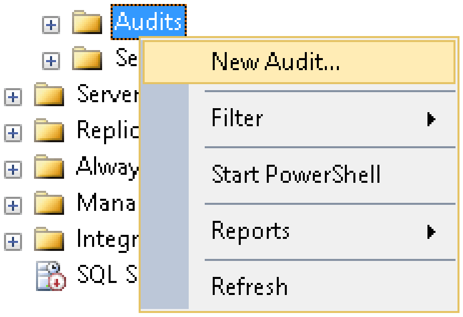
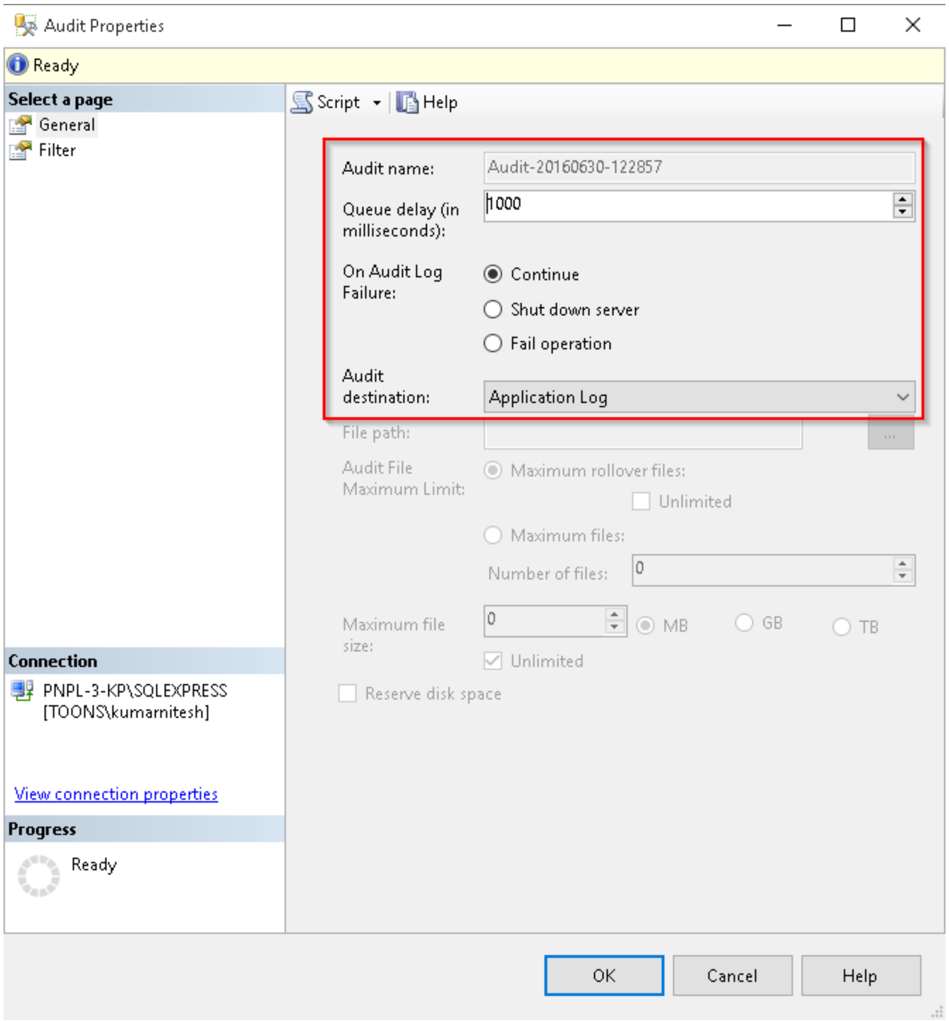


Figure 4

2. In **Audit Properties**, provide appropriate **audit name** and set audit destination as **application log**. Configured Audit properties pane is shown below:



Audit Properties

Ready

Select a page
- General
- Filter

Script ▾ | Help

Audit name: Audit-20160630-122857

Queue delay (in milliseconds): 1000

On Audit Log Failure:
- ● Continue
- ○ Shut down server
- ○ Fail operation

Audit destination: Application Log

File path:

Audit File Maximum Limit:
- ● Maximum rollover files:
  - □ Unlimited
- ○ Maximum files:

Number of files: 0

Maximum file size: 0 ● MB ○ GB ○ TB

☑ Unlimited

□ Reserve disk space

Connection

PNPL-3-KP\SQLEXPRESS [TOONS\kumarnitesh]

View connection properties

Progress

Ready

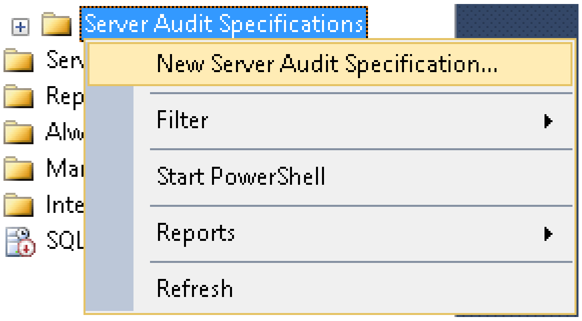
OK | Cancel | Help

Figure 5

3. Click **OK** to apply settings.

Create server audit specifications

1. Right-click **Server Audit Specifications** and select **New Server Audit Specification…**



Server Audit Specifications
Serv
Rep
Alw
Mar
Inte
SQL
New Server Audit Specification...
Filter
Start PowerShell
Reports
Refresh

Figure 6

2. In Server **Audit Specification Properties**, provide appropriate **specification name** and choose earlier created **audit name** from drop-down menu.
3. In **Actions** pane, select following specifications from **Audit Action Type*** drop-down.

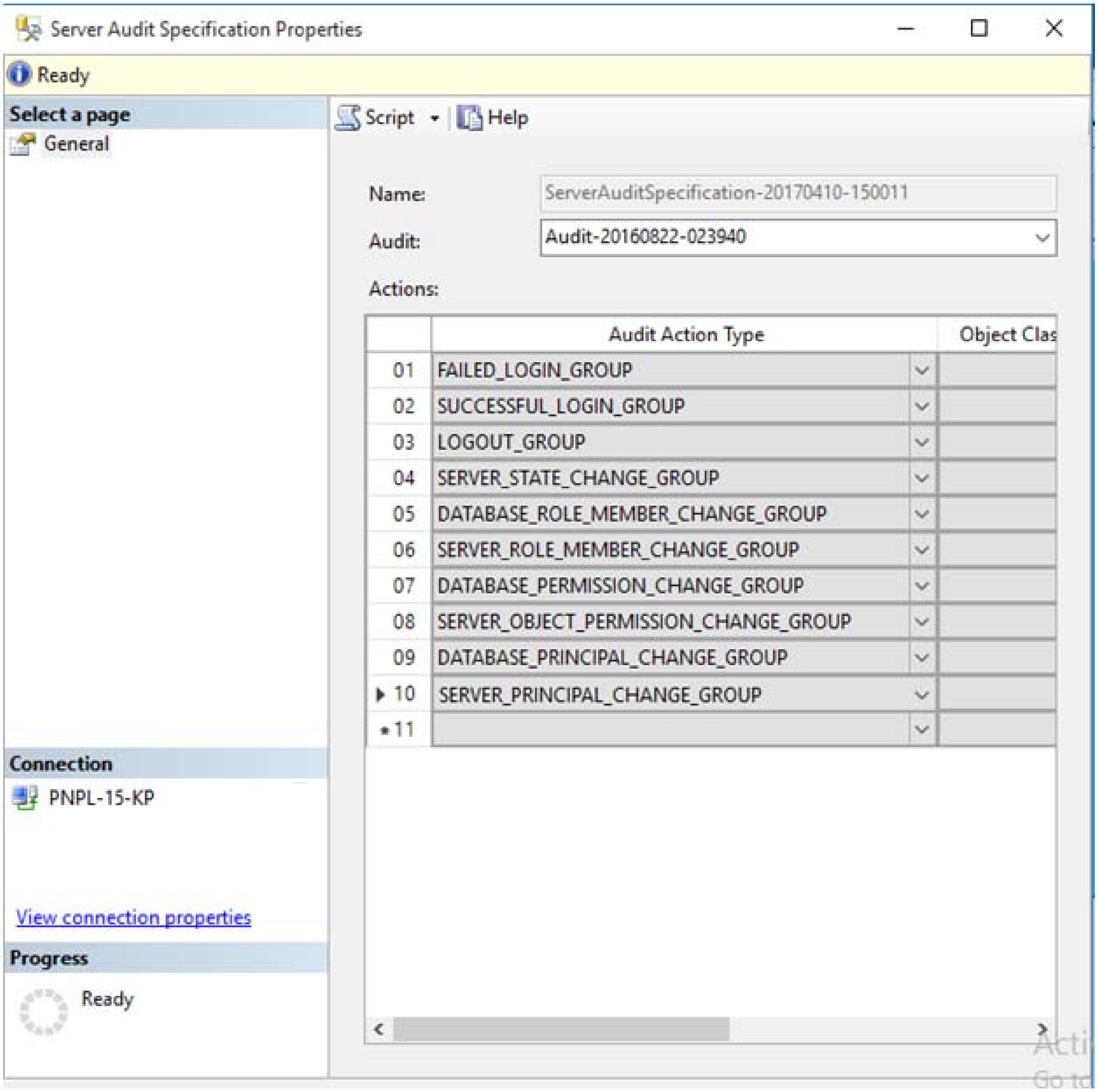
*** To improve performance, please enable action types consistent with your audit requirements.**

SN	Audit Action Type	Description
1.	**DATABASE_ROLE_MEMBER_CHANGE_GROUP**	This generates events whenever a login is added to or removed from a database role.
2.	**SERVER_ROLE_MEMBER_CHANGE_GROUP**	This generates events whenever a login is added or removed from a fixed server role.
3.	**BACKUP_RESTORE_GROUP**	This generates events whenever a backup or restore command is issued.
4.	**AUDIT_CHANGE_GROUP**	This generates events whenever any audit is created, modified or deleted.
5.	**DATABASE_PERMISSION_CHANGE_GROUP**	This generates events whenever a GRANT, REVOKE, or DENY is issued by any user in SQL Server for database-only events.
6.	**SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP**	This generates events whenever a grant, deny, or revoke is issued for a schema object.
7.	**SERVER_PERMISSION_CHANGE_GROUP**	This generates events when a GRANT, REVOKE, or DENY is issued for permissions in the server scope.
8.	**DATABASE_CHANGE_GROUP**	This generates events when a database is created, altered, or dropped.
9.	**DATABASE_OBJECT_CHANGE_GROUP**	This generates events when a CREATE, ALTER, or DROP statement is executed on database objects.
10.	**DATABASE_PRINCIPAL_CHANGE_GROUP**	This generates events when principals are created, altered, or dropped from a database.
11.	**SCHEMA_OBJECT_CHANGE_GROUP**	This generates events when a CREATE, ALTER, or DROP operation is performed on a schema.

12.	**SERVER_OBJECT_CHANGE_GROUP**	This generates events for CREATE, ALTER, or DROP operations on server objects.
13.	**SERVER_PRINCIPAL_CHANGE_GROUP**	This generates events when server principals are created, altered, or dropped.
14.	**APPLICATION_ROLE_CHANGE_PASSWORD_GROUP**	This generates events whenever a password is changed for an application role.
15.	**LOGIN_CHANGE_PASSWORD_GROUP**	This generates events whenever a login password is changed by ALTER LOGIN statement.
16.	**DATABASE_OWNERSHIP_CHANGE_GROUP**	This generates events when ALTER AUTHORIZATION statement is used to change the owner of a database.
17.	**SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP**	This generates events when the permissions to change the owner of schema object (such as a table, procedure, or function) is checked.
18.	**USER_CHANGE_PASSWORD_GROUP****	This generates events whenever the password of a contained database user is changed by using the ALTER USER statement.
19	**SUCCESSFUL_LOGON_GROUP**	This generates events whenever a successful logon is done
20	**LOGOUT_GROUP**	This generates events whenever a logout is done
21	**FAILED_LOGON_GROUP**	This generates events whenever a Logon failure happens.
22	**SERVICE_STATE_CHANGE_GROUP**	This generates events whenever any SQL service is stopped or started.

**** Only available in Microsoft SQL server 2012 or later**

Configured Server Audit Specification Properties pane is shown below:



Name: ServerAuditSpecification-20170410-150011

Audit: Audit-20160822-023940

Actions:

	Audit Action Type	Object Clas
01	FAILED_LOGIN_GROUP	
02	SUCCESSFUL_LOGIN_GROUP	
03	LOGOUT_GROUP	
04	SERVER_STATE_CHANGE_GROUP	
05	DATABASE_ROLE_MEMBER_CHANGE_GROUP	
06	SERVER_ROLE_MEMBER_CHANGE_GROUP	
07	DATABASE_PERMISSION_CHANGE_GROUP	
08	SERVER_OBJECT_PERMISSION_CHANGE_GROUP	
09	DATABASE_PRINCIPAL_CHANGE_GROUP	
▸ 10	SERVER_PRINCIPAL_CHANGE_GROUP	
* 11		

Figure 7

4. Click **OK** to apply settings.
5. Right- click on earlier created **audit** and select **Enable**.

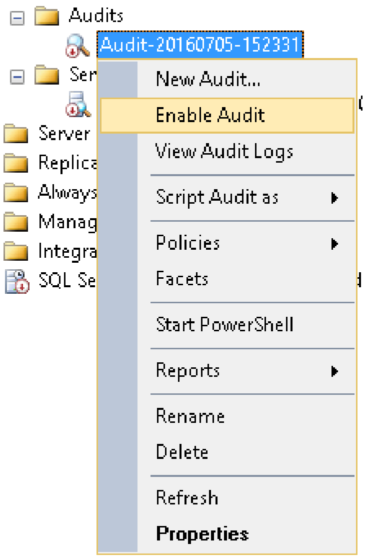


Figure 8

6. Right- click on earlier created **Server Audit Specification** and select **Enable Server Audit Specification**.

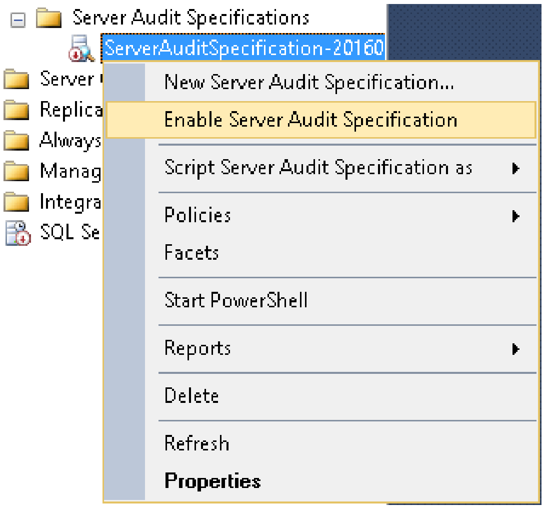

Server Audit Specifications
ServerAuditSpecification-20160
Server
Replica
Always
Manag
Integra
SQL Se
New Server Audit Specification...
Enable Server Audit Specification
Script Server Audit Specification as
Policies
Facets
Start PowerShell
Reports
Delete
Refresh
Properties

Figure 9

7. Above configuration generates event id “**33205**” for all configured audit specifications.

EventTracker agent configuration

Create Event Filters

All the events generated by SQL through audit specifications are **information** events and are reported late. Thus, to aid alerting of events in real-time event filters are to be configured. **Please note, log source matched in configurations below might change depending on the SQL instance name configured.**

1. Logon to EventTracker manager workstation.

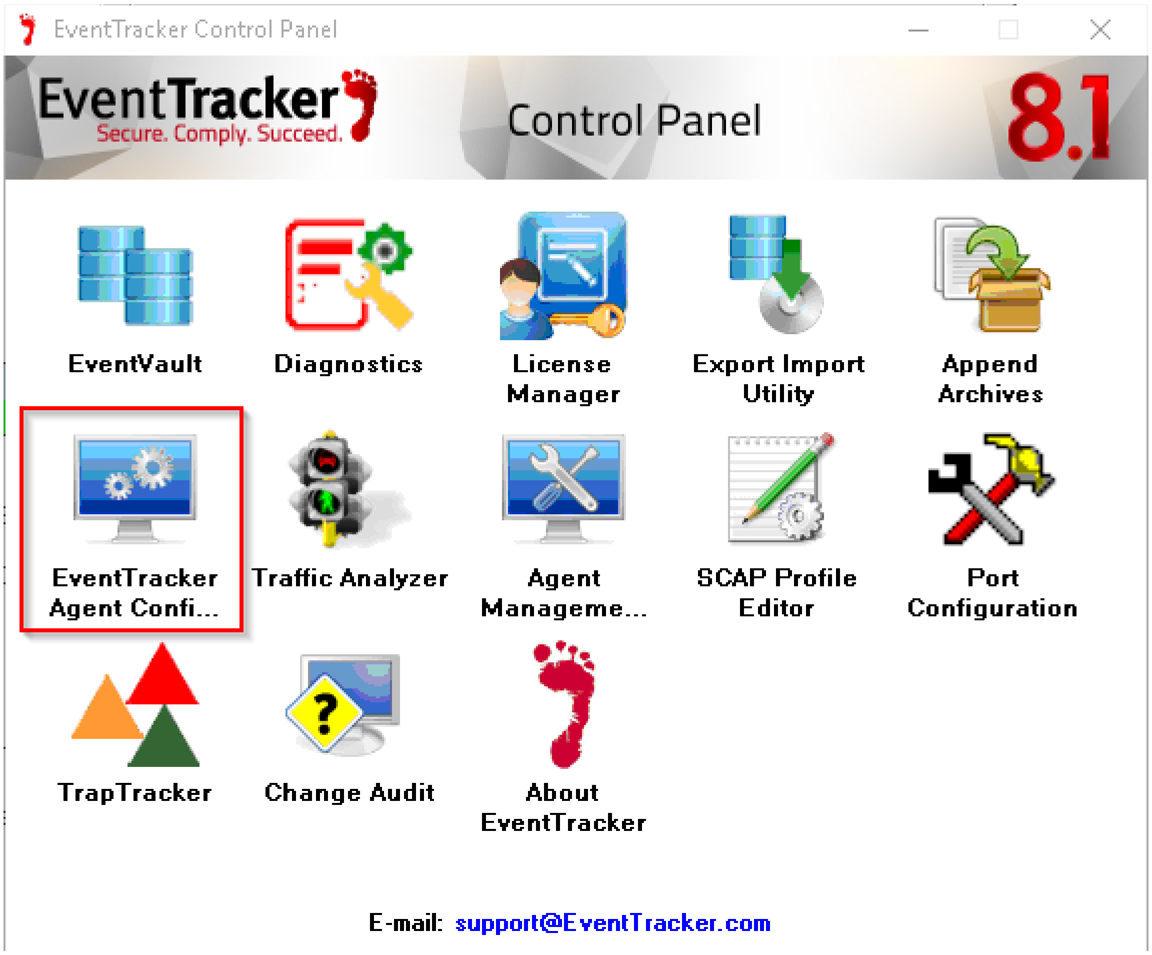
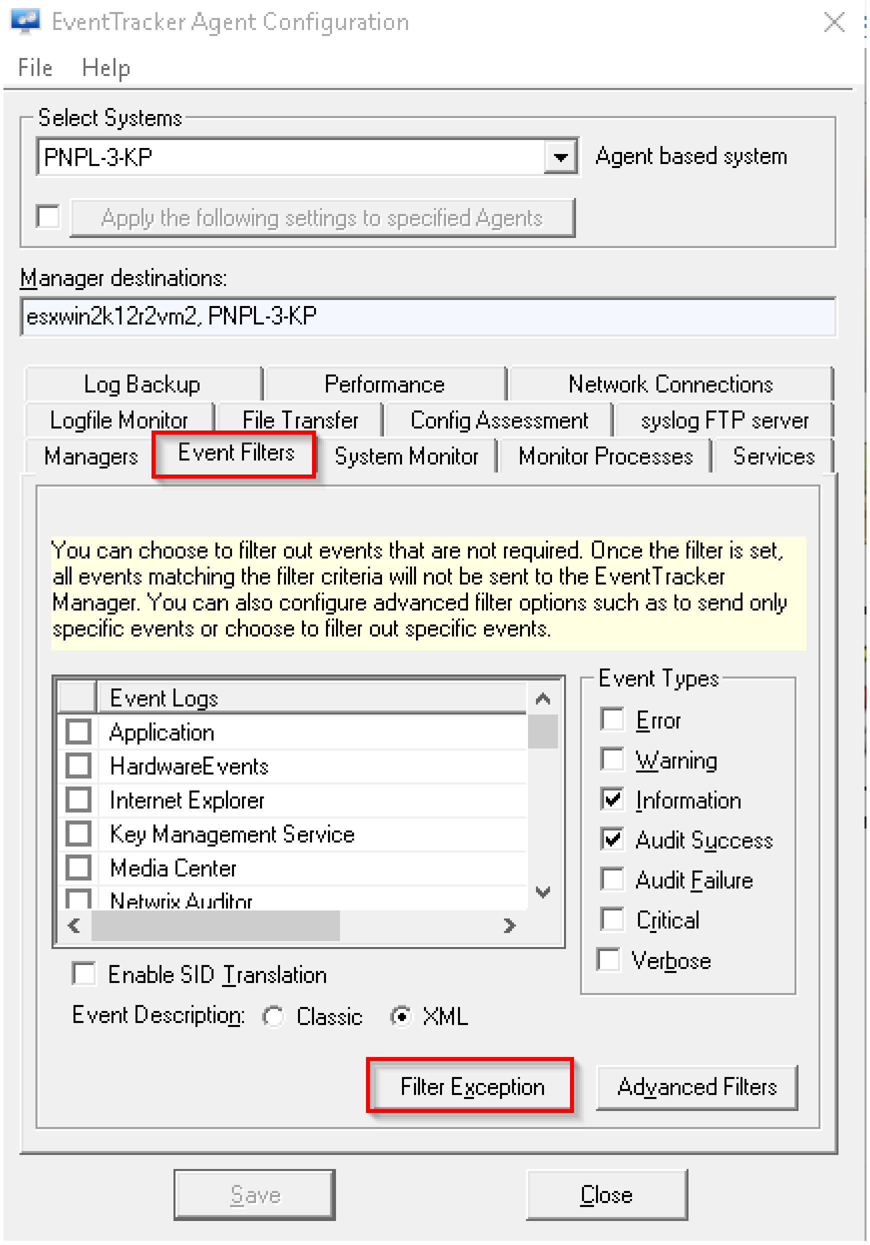


Figure 10

2. Open EventTracker control panel and click **EventTracker Agent Configuration**.



You can choose to filter out events that are not required. Once the filter is set, all events matching the filter criteria will not be sent to the EventTracker Manager. You can also configure advanced filter options such as to send only specific events or choose to filter out specific events.

Event Logs:
- □ Application
- □ HardwareEvents
- □ Internet Explorer
- □ Key Management Service
- □ Media Center
- □ Netwrix Auditor

Event Types:
- □ Error
- □ Warning
- ☑ Information
- ☑ Audit Success
- □ Audit Failure
- □ Critical
- □ Verbose

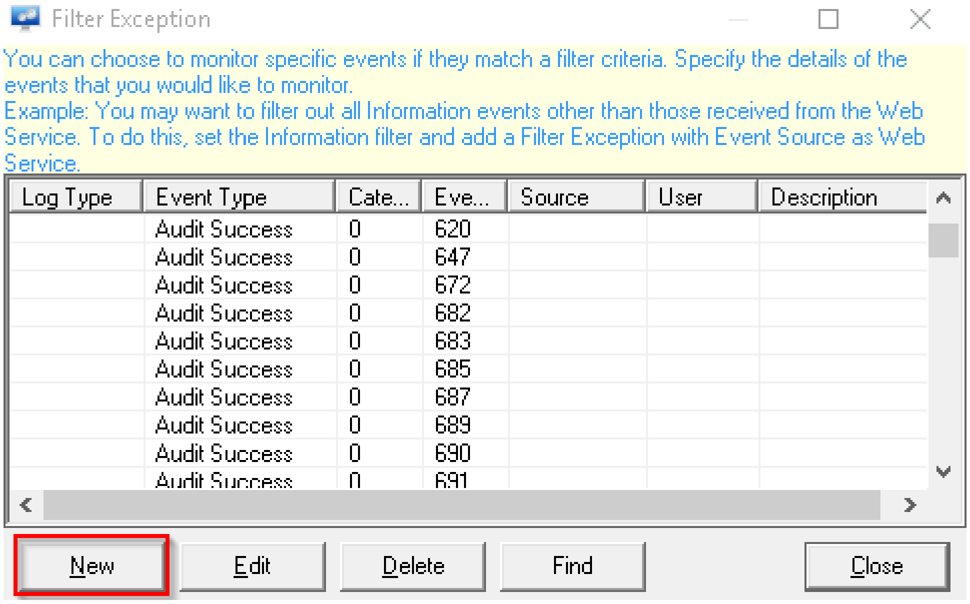
□ Enable SID Translation

Event Description: ○ Classic ● XML

Figure 11

3. Select **Event Filters** tab and click **Filter Exception**.

Filter exception window opens.

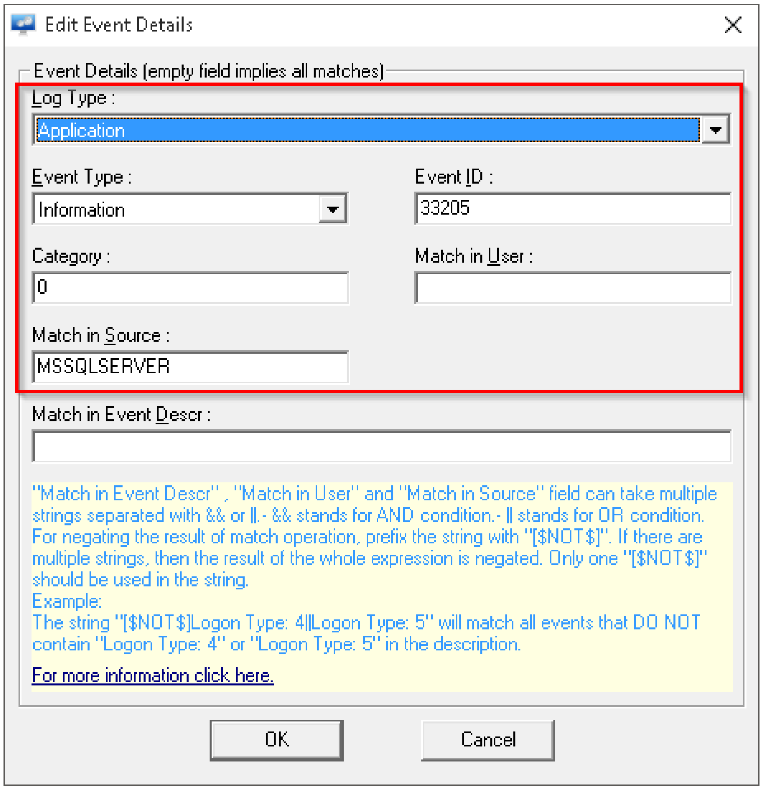

Filter Exception

You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
	Audit Success	0	620			
	Audit Success	0	647			
	Audit Success	0	672			
	Audit Success	0	682			
	Audit Success	0	683			
	Audit Success	0	685			
	Audit Success	0	687			
	Audit Success	0	689			
	Audit Success	0	690			
	Audit Success	0	691			

Figure 12

4. Click **New**, and configure as shown below:
5. Event filter properties for **audit events** are shown below:
6. For **Single Instance**, Match in Source should be named as corresponding instance name. For **multiple instances**, leave it blank.


Edit Event Details

Event Details (empty field implies all matches)

Log Type : Application

Event Type : Information

Event ID : 33205

Category : 0

Match in User :

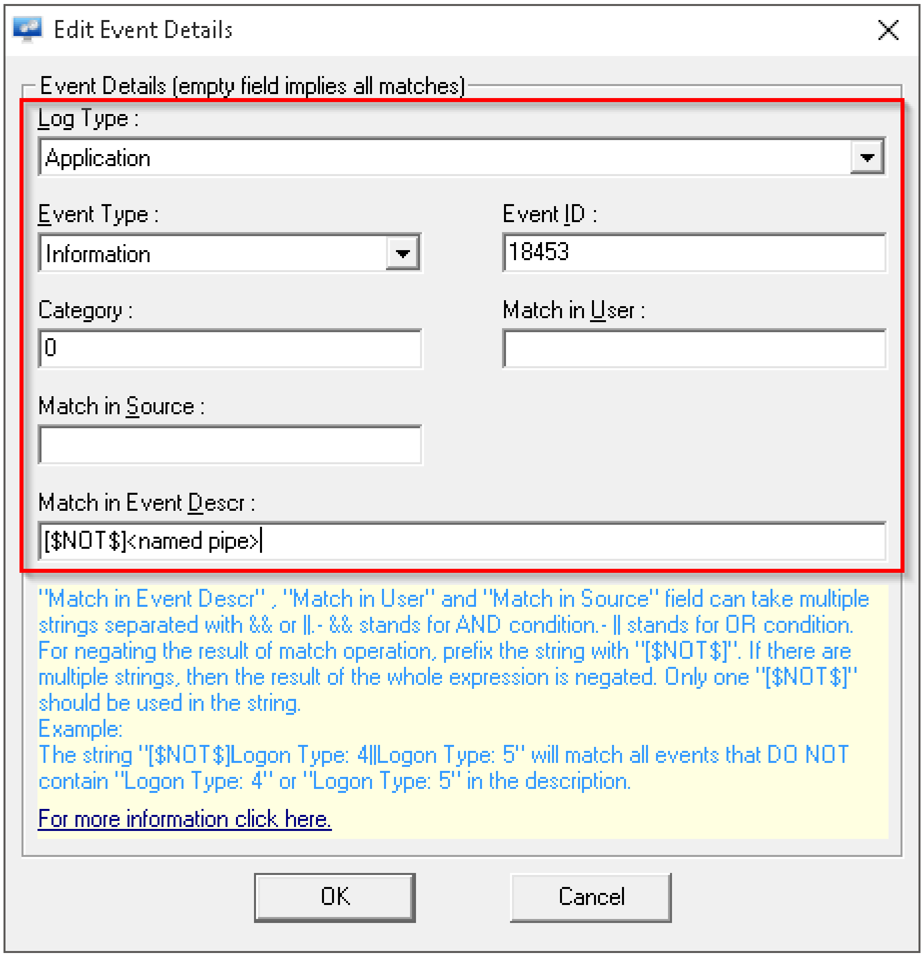
Match in Source : MSSQLSERVER

Match in Event Descr :

"Match in Event Descr" , "Match in User" and "Match in Source" field can take multiple strings separated with && or ||.- && stands for AND condition.- || stands for OR condition.
For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT]" should be used in the string.
Example:
The string "[NOT]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.
For more information click here.

Figure 13

7. Click **OK** to apply.
8. If events are enabled for **login success and failure**, create filters with configurations as shown below:
9. Event filter properties for **login success** event are shown below:



Log Type : Application

Event Type : Information

Event ID : 18453

Category : 0

Match in User :

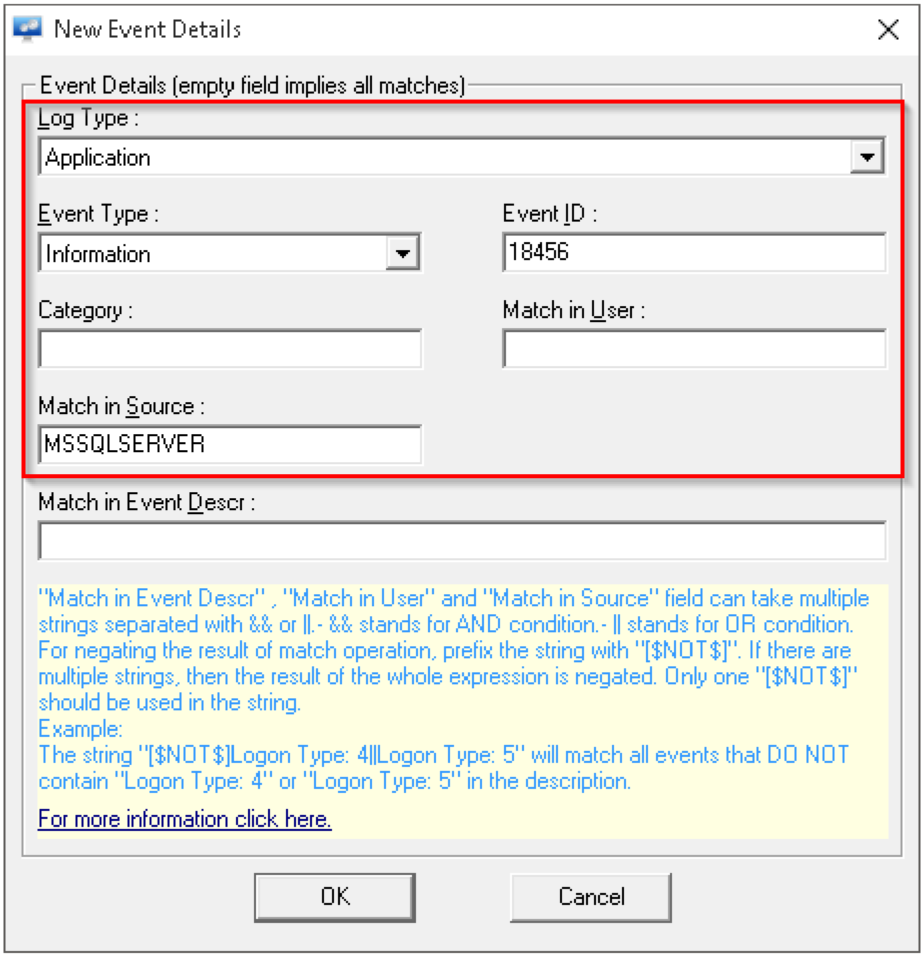
Match in Source :

Match in Event Descr : [NOT]<named pipe>

"Match in Event Descr" , "Match in User" and "Match in Source" field can take multiple strings separated with && or ||.- && stands for AND condition.- || stands for OR condition. For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT]" should be used in the string.
Example:
The string "[NOT]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.
For more information click here.

Figure 14

10. Event filter properties for **login failure** event are shown below:



New Event Details

Event Details (empty field implies all matches)

Log Type : Application

Event Type : Information

Event ID : 18456

Category :

Match in User :

Match in Source : MSSQLSERVER

Match in Event Descr :

"Match in Event Descr" , "Match in User" and "Match in Source" field can take multiple strings separated with && or ||.- && stands for AND condition.- || stands for OR condition. For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT]" should be used in the string.
Example:
The string "[NOT]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.

For more information click here.

Figure 15

11. Click **SAVE** in agent configuration window to apply changes.

Extended events

Extended Events is a lightweight performance monitoring system that uses very few performance resources. It enables auditing for different actions, providing much granularity in the setup process and wide coverage range of the SQL Server activity. **Below mentioned configuration must be applied on all the workstations, where SQL audit is required.**

Prerequisites

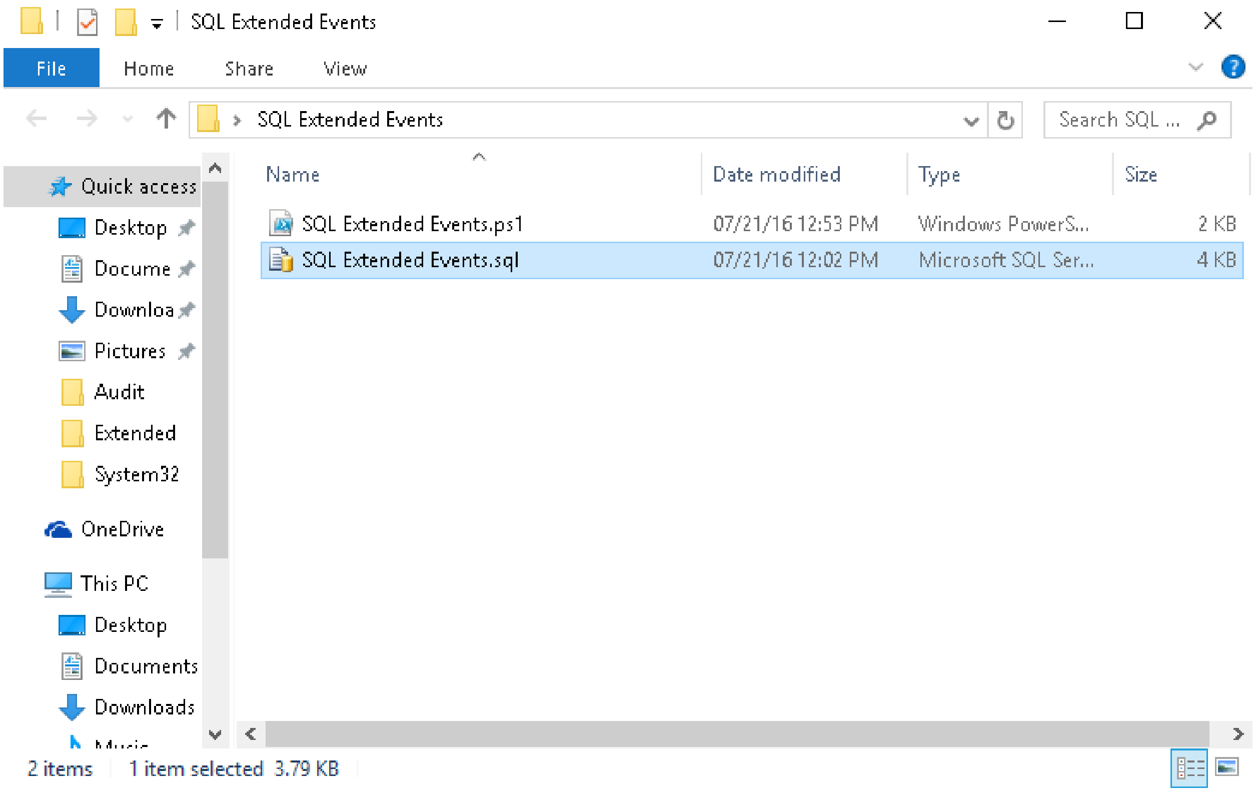
1. **Microsoft SQL server 2012 or later** must be installed.
2. **Microsoft SQL Management Studio** for the respective version must be installed.
3. **EventTracker agent 7.6 or later** must be installed on the SQL SERVER workstation.
4. **PowerShell 3.0 or later** must be installed**.**
5. **Administrative credentials** for script execution.

Create extended event session

1. Contact **Support** for the **SQL extended events script pack** and download.
2. Extract downloaded zip file to following path.

```
<EventTracker Installation Path>\EventTracker\ScheduledActionScripts\
```

3. From extracted file location, double-click to open “**SQL Extended Events.sql**”.

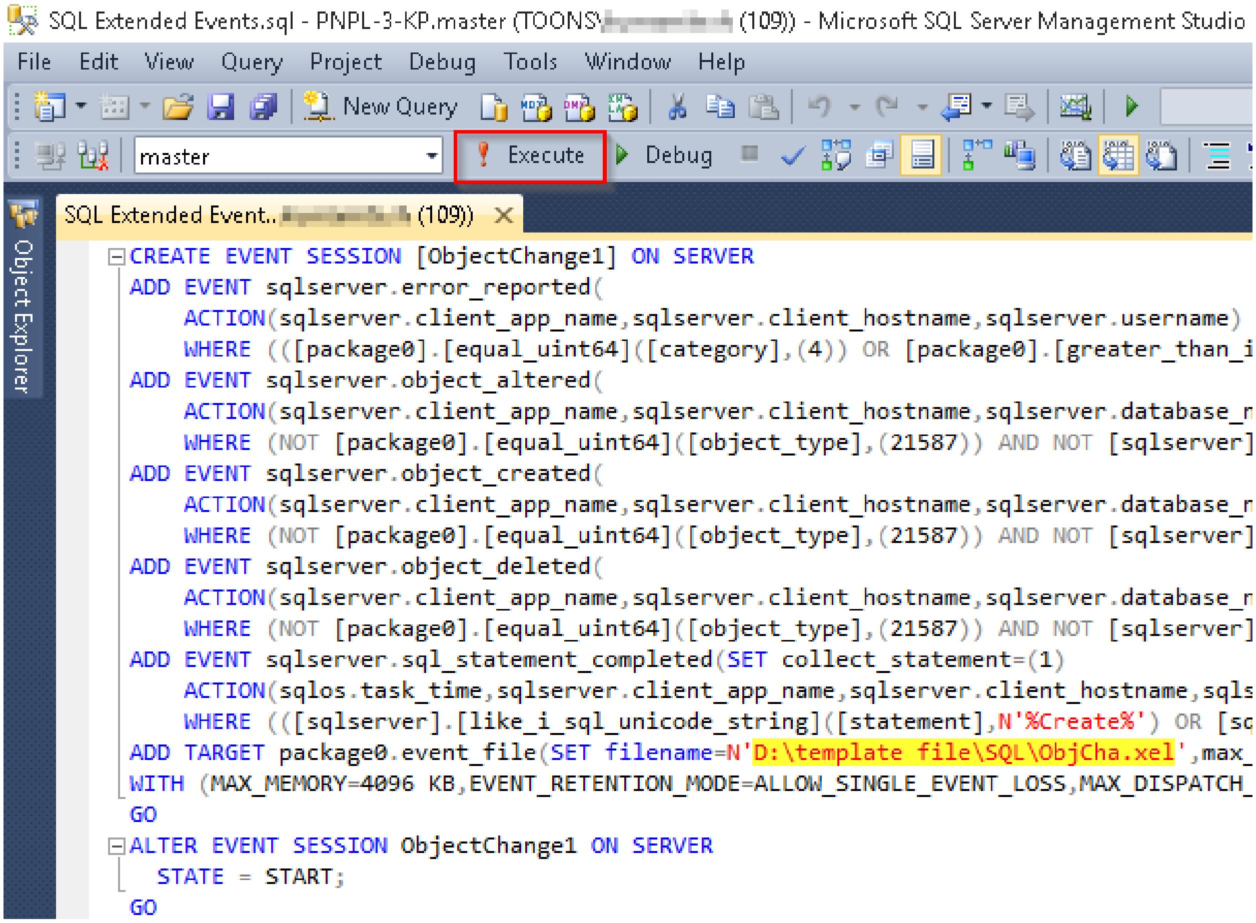


Name	Date modified	Type	Size
SQL Extended Events.ps1	07/21/16 12:53 PM	Windows PowerS...	2 KB
SQL Extended Events.sql	07/21/16 12:02 PM	Microsoft SQL Ser...	4 KB

2 items 1 item selected 3.79 KB

Figure 16

4. In **Microsoft SQL management studio**, login with appropriate credentials.
5. In the **SQL query**, change highlighted path to the desired location of “**.xel**” file. Click **Execute** to create and implement extended event session.


SQL Extended Events.sql - PNPL-3-KP.master (TOONS\[redacted] (109)) - Microsoft SQL Server Management Studio
File
Edit
View
Query
Project
Debug
Tools
Window
Help
New Query
master
Execute
Debug
SQL Extended Event..[redacted] (109))
Object Explorer

```
CREATE EVENT SESSION [ObjectChange1] ON SERVER
ADD EVENT sqlserver.error_reported(
    ACTION(sqlserver.client_app_name,sqlserver.client_hostname,sqlserver.username)
    WHERE (([package0].[equal_uint64]([category],(4)) OR [package0].[greater_than_i
ADD EVENT sqlserver.object_altered(
    ACTION(sqlserver.client_app_name,sqlserver.client_hostname,sqlserver.database_n
    WHERE (NOT [package0].[equal_uint64]([object_type],(21587)) AND NOT [sqlserver]
ADD EVENT sqlserver.object_created(
    ACTION(sqlserver.client_app_name,sqlserver.client_hostname,sqlserver.database_n
    WHERE (NOT [package0].[equal_uint64]([object_type],(21587)) AND NOT [sqlserver]
ADD EVENT sqlserver.object_deleted(
    ACTION(sqlserver.client_app_name,sqlserver.client_hostname,sqlserver.database_n
    WHERE (NOT [package0].[equal_uint64]([object_type],(21587)) AND NOT [sqlserver]
ADD EVENT sqlserver.sql_statement_completed(SET collect_statement=(1)
    ACTION(sqlos.task_time,sqlserver.client_app_name,sqlserver.client_hostname,sqls
    WHERE (([sqlserver].[like_i_sql_unicode_string]([statement],N'%Create%') OR [sq
ADD TARGET package0.event_file(SET filename=N'D:\template file\SQL\ObjCha.xel',max_
WITH (MAX_MEMORY=4096 KB,EVENT_RETENTION_MODE=ALLOW_SINGLE_EVENT_LOSS,MAX_DISPATCH_
GO
ALTER EVENT SESSION ObjectChange1 ON SERVER
  STATE = START;
GO
```

Figure 17

6. To view created session, navigate to **Object Explorer> Server Name> Management> Extended Events> Sessions> ObjectChange**.

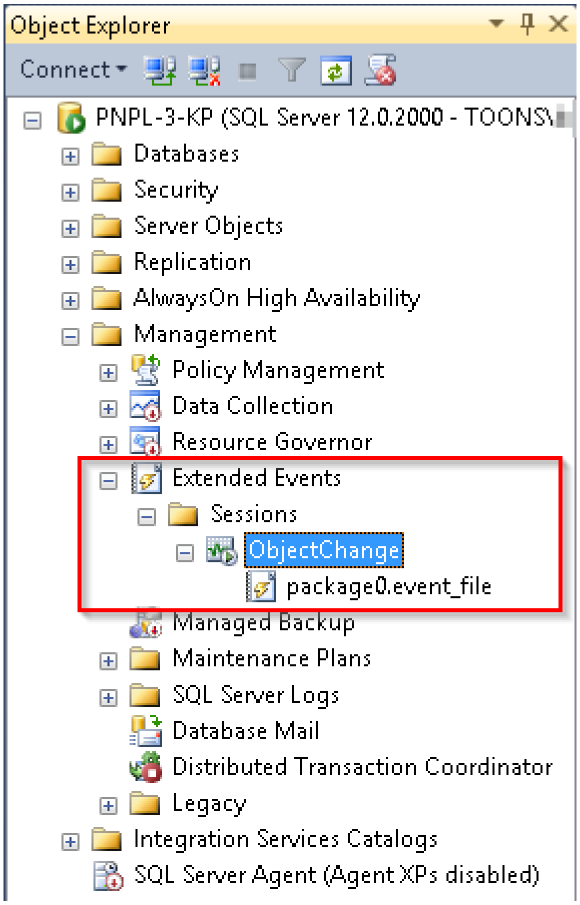


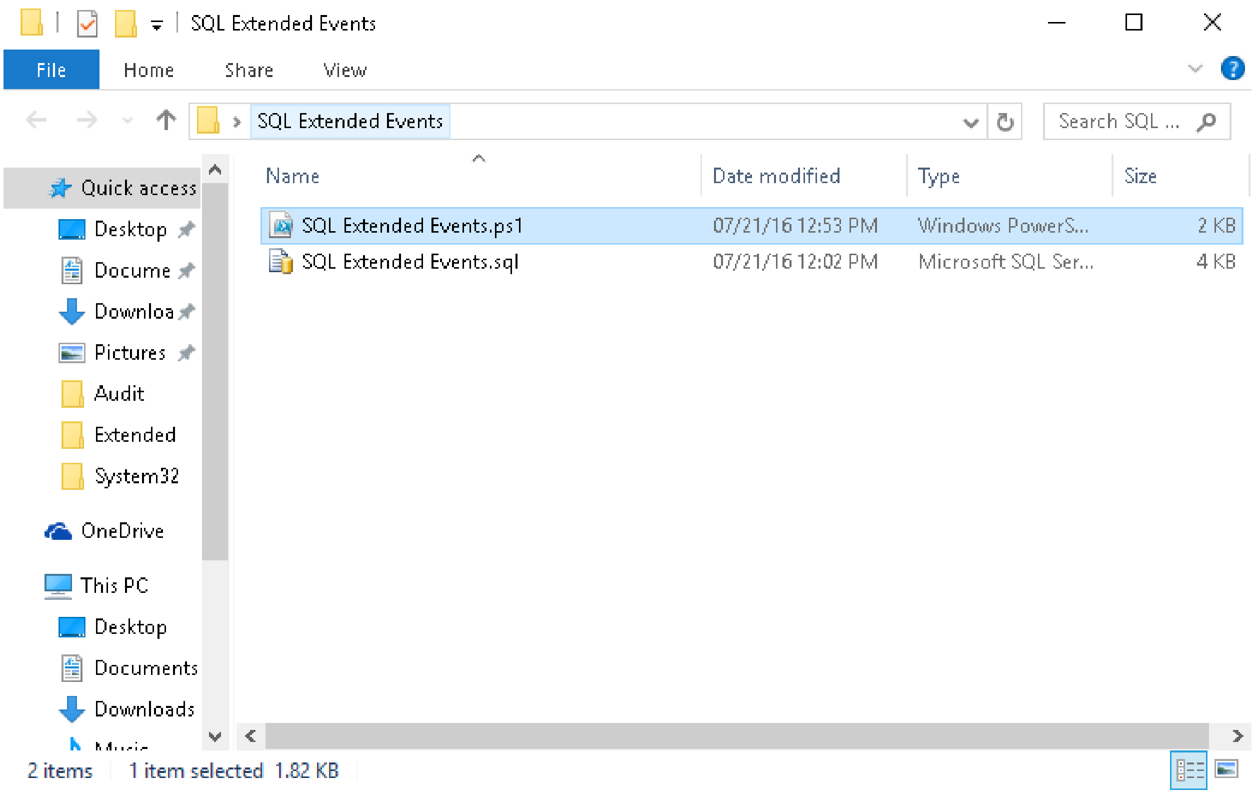
Figure 18

7. Above configuration will create "**. xel**" file with all relevant audit events at the earlier mentioned location.

Parse extended event session log file

Xel files are readable only through SQL management Studio. Thus, PowerShell is deployed for file format conversion and custom parsing in the interest of EventTracker.

1. From earlier mentioned extracted file location, find "**SQL Extended Events.ps1**".

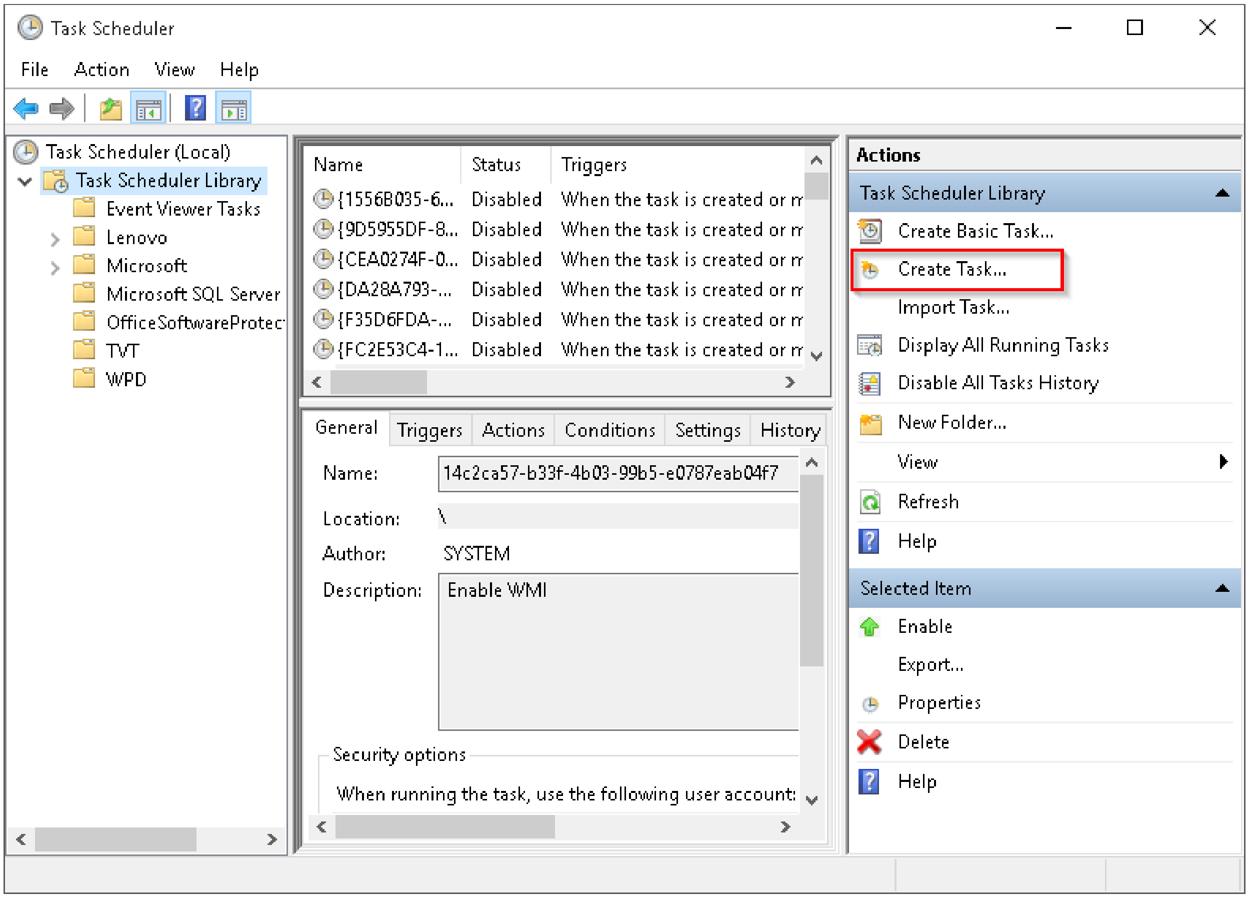


Name	Date modified	Type	Size
SQL Extended Events.ps1	07/21/16 12:53 PM	Windows PowerS...	2 KB
SQL Extended Events.sql	07/21/16 12:02 PM	Microsoft SQL Ser...	4 KB

2 items 1 item selected 1.82 KB

Figure 19

2. Logon to EventTracker Manager workstation with the administrative privileges.
3. Navigate to **Start>Administrative Tools>Task Scheduler**.



Name	Status	Triggers
{1556B035-6...	Disabled	When the task is created or m
{9D5955DF-8...	Disabled	When the task is created or m
{CEA0274F-0...	Disabled	When the task is created or m
{DA28A793-...	Disabled	When the task is created or m
{F35D6FDA-...	Disabled	When the task is created or m
{FC2E53C4-1...	Disabled	When the task is created or m

Name: 14c2ca57-b33f-4b03-99b5-e0787eab04f7

Location: \

Author: SYSTEM

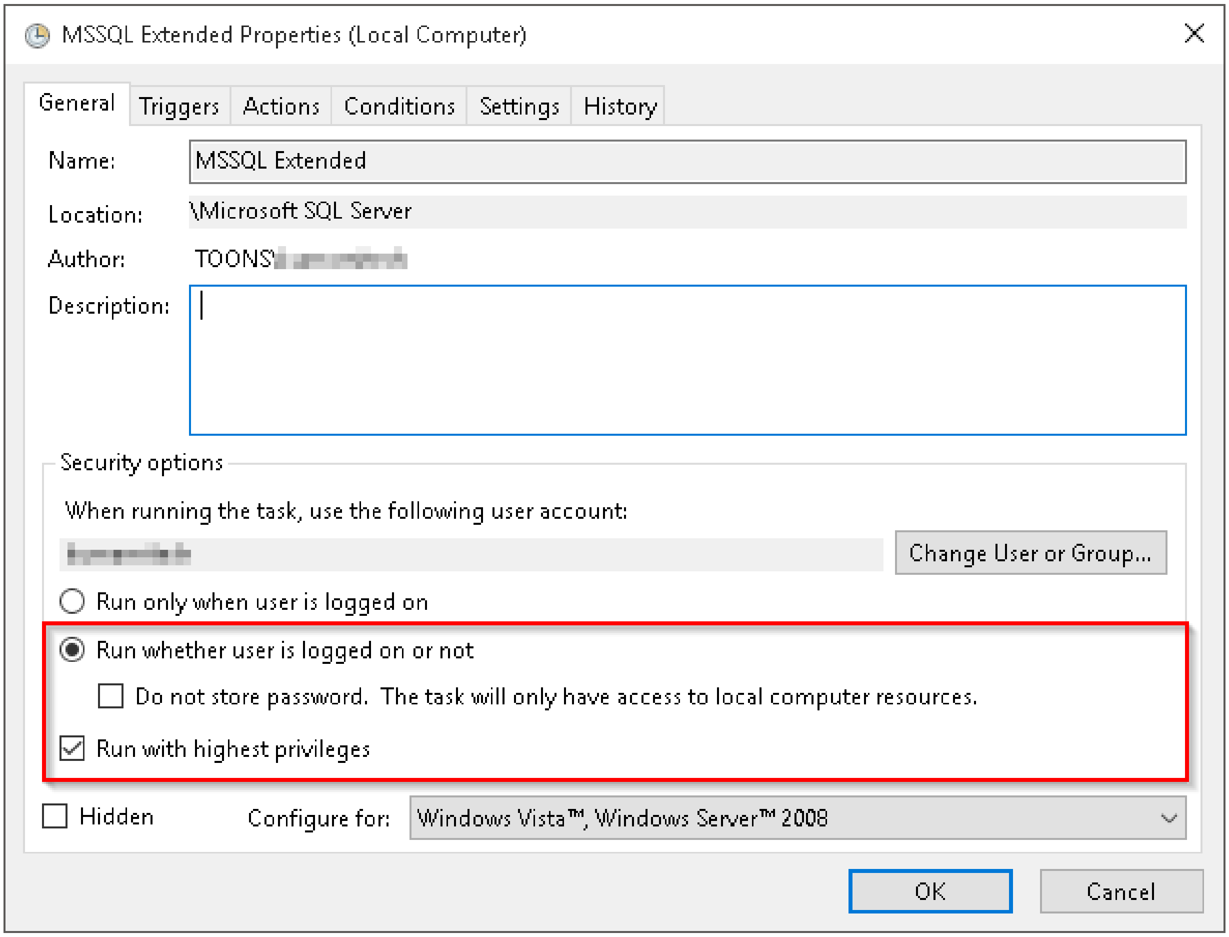
Description: Enable WMI

Security options

When running the task, use the following user account:

Figure 20

4. In the **Actions** tab, select **Create task**.
5. Configure Task properties as shown below:



MSSQL Extended Properties (Local Computer)

Name: MSSQL Extended

Location: \Microsoft SQL Server

Author: TOONS\[redacted]

Description:

Security options

When running the task, use the following user account:

[redacted]

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

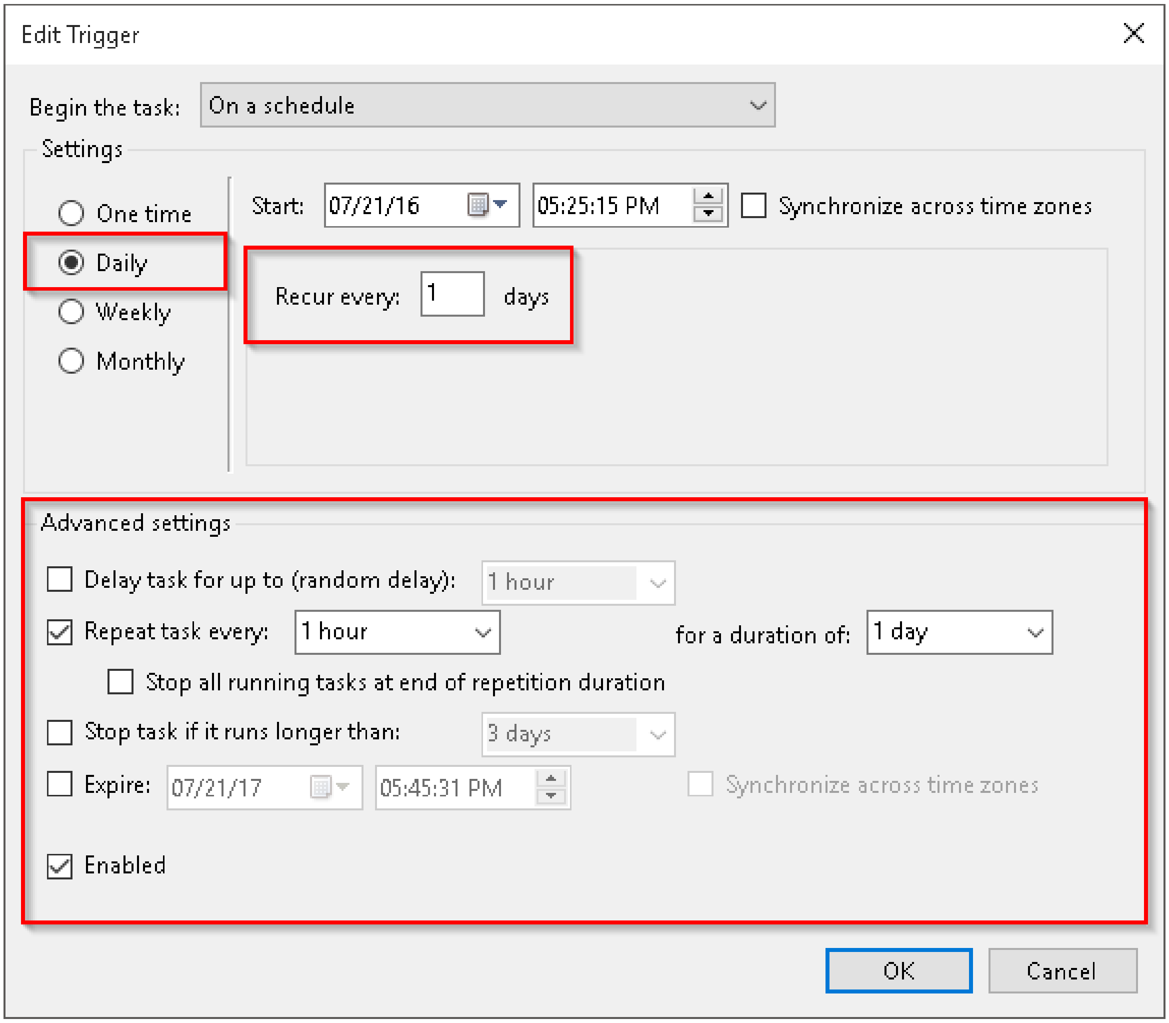
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

Figure 21

6. Select **General** tab, provide appropriate name and in **Security options** section, enable “**Run weather user is logged on or not**” and “**Run with highest privileges**” options.



Edit Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 07/21/16 05:25:15 PM □ Synchronize across time zones

Recur every: 1 days

Advanced settings

□ Delay task for up to (random delay): 1 hour

☑ Repeat task every: 1 hour for a duration of: 1 day

□ Stop all running tasks at end of repetition duration

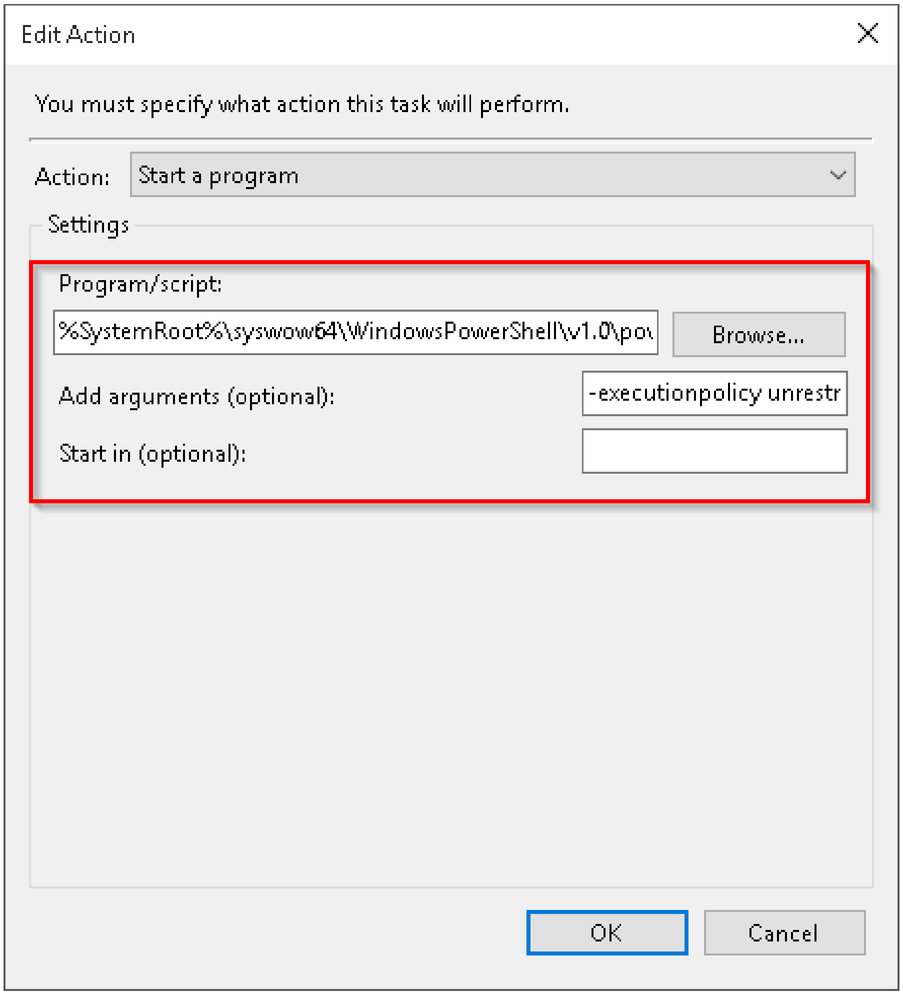
□ Stop task if it runs longer than: 3 days

□ Expire: 07/21/17 05:45:31 PM □ Synchronize across time zones

☑ Enabled

Figure 22

7. Select **Triggers** tab, select **Daily** with appropriate schedule settings to ensure hourly execution.



Edit Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: %SystemRoot%\syswow64\WindowsPowerShell\v1.0\pow

Add arguments (optional): -executionpolicy unrestr

Start in (optional):

Figure 23

8. Select **Actions** tab, enter “**%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe”** as program name and compose argument as given below:

```
-executionpolicy unrestricted -file "C:\SQL Extended Events\SQL Extended Events.ps1" –xelfile "C:\SQL Logs" –outfile "C:\SQL Extended Events\Logs\SQLFINAL.txt"
```

🟩 **PowerShell script location**

🟨 **XEL file location**

🟦 **Output TXT file location**

9. Click **OK** to save task.
10. Above configuration will convert XEL log file into TXT and extract useful fields will the same.

EventTracker Agent Configuration

Create Event Filters

All events generated by SQL through extended events are **off-line** events. Thus, alerting is not possible. **If alerts are to be configured for extended events, compose event filters are shown below, to aid alerting for off-line events with an hourly delay.**

1. Logon to EventTracker manager workstation.

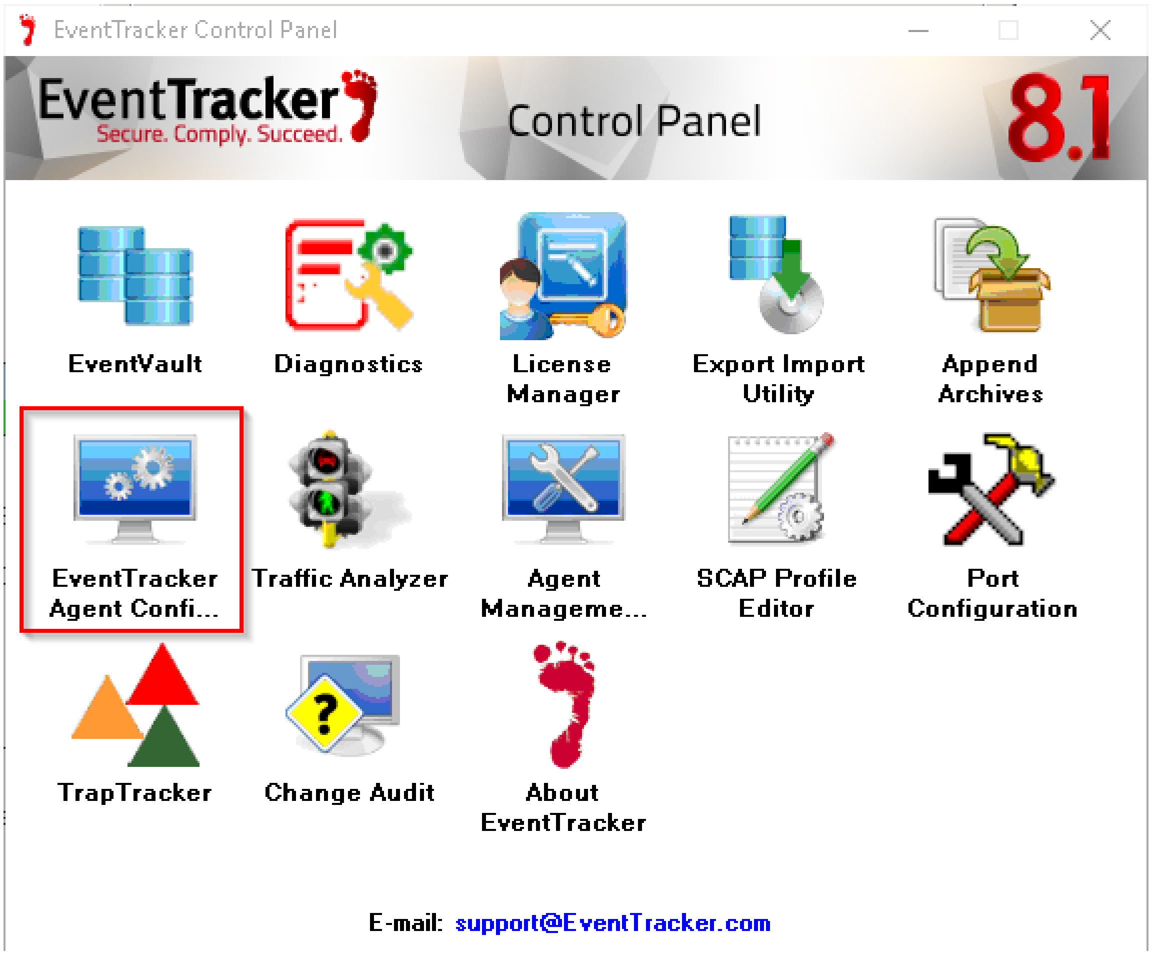
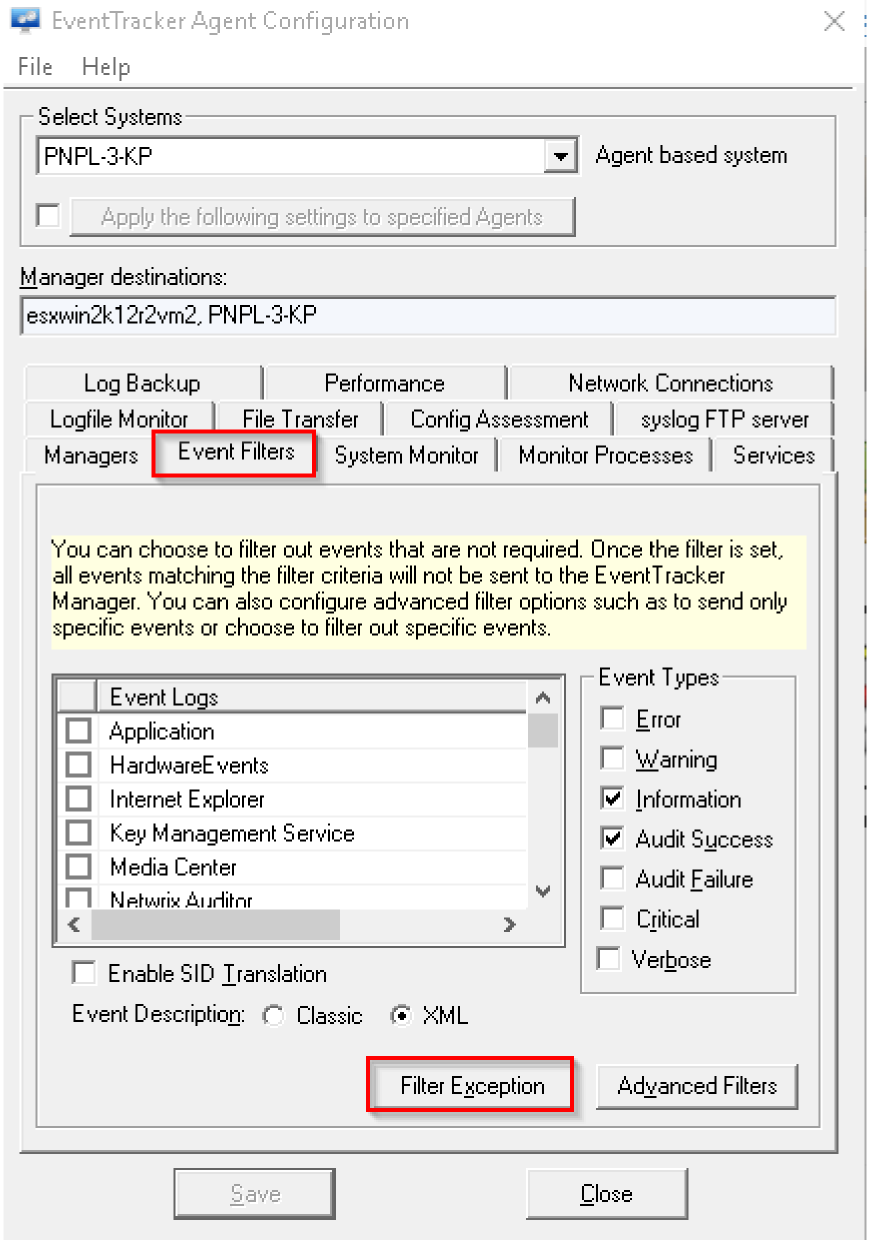


Figure 24

2. Open EventTracker control panel, click **EventTracker Agent Configuration**.



You can choose to filter out events that are not required. Once the filter is set, all events matching the filter criteria will not be sent to the EventTracker Manager. You can also configure advanced filter options such as to send only specific events or choose to filter out specific events.

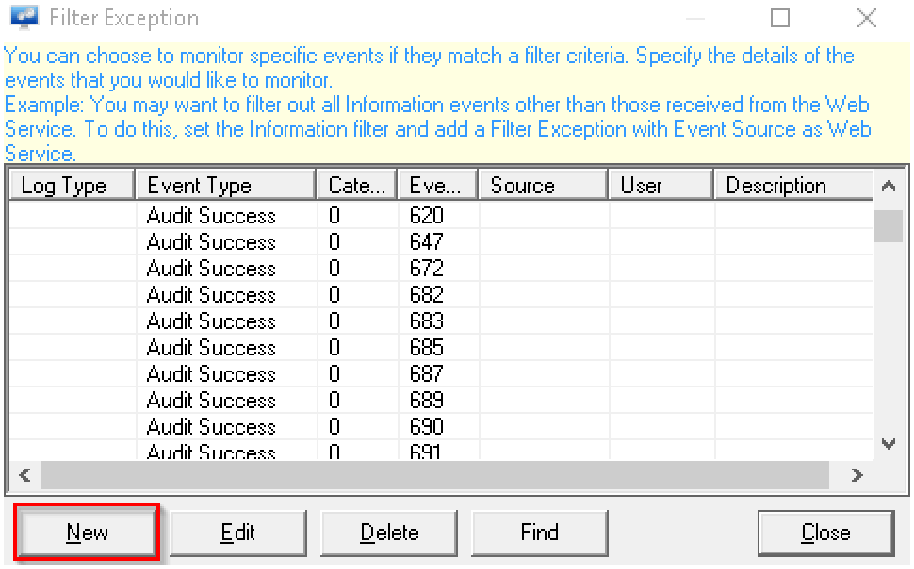
Event Types: □ Error □ Warning ☑ Information ☑ Audit Success □ Audit Failure □ Critical □ Verbose

Event Description: ○ Classic ● XML

Figure 25

3. Select **Event Filters** tab and click **Filter Exception**.

Filter exception window opens.



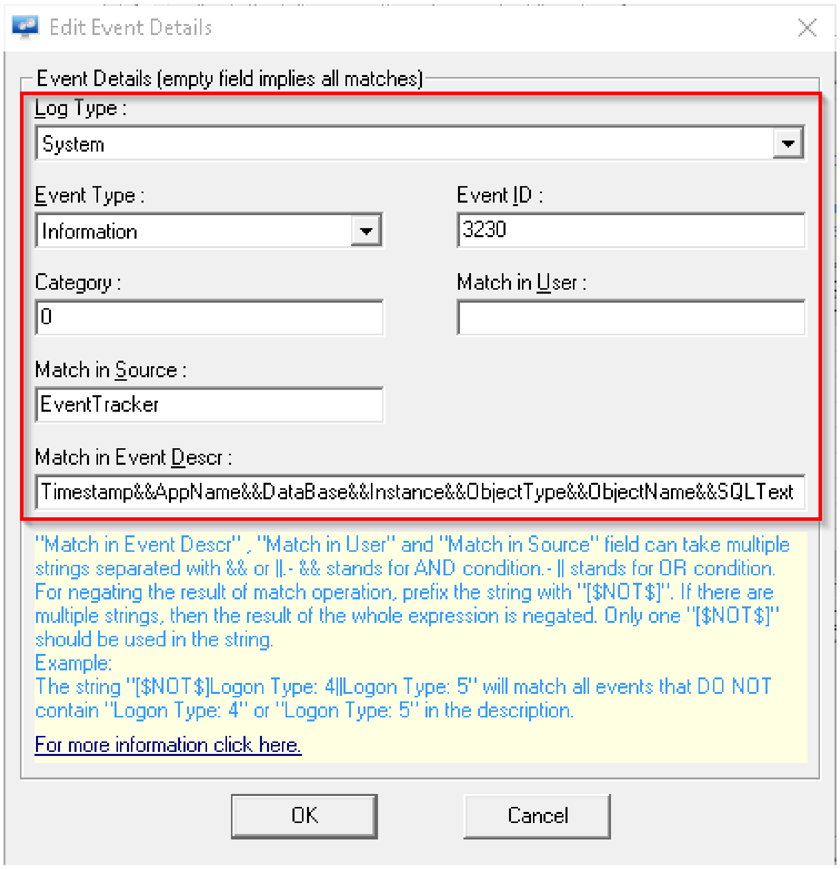
Filter Exception

You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
	Audit Success	0	620			
	Audit Success	0	647			
	Audit Success	0	672			
	Audit Success	0	682			
	Audit Success	0	683			
	Audit Success	0	685			
	Audit Success	0	687			
	Audit Success	0	689			
	Audit Success	0	690			
	Audit Success	0	691			

Figure 26

4. Click **New**, and configure event filter properties as shown below:



Edit Event Details

Event Details (empty field implies all matches)

Log Type : System

Event Type : Information

Event ID : 3230

Category : 0

Match in User :

Match in Source : EventTracker

Match in Event Descr : Timestamp&&AppName&&DataBase&&Instance&&ObjectType&&ObjectName&&SQLText

"Match in Event Descr" , "Match in User" and "Match in Source" field can take multiple strings separated with && or ||.- && stands for AND condition.- || stands for OR condition. For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT]" should be used in the string.
Example:
The string "[NOT]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.

For more information click here.

Figure 27

5. Enter following as matching description.

```
Timestamp&&AppName&&DataBase&&Instance&&ObjectType&&ObjectName&&SQLText
```

6. Click **OK** to apply.

Configure LFM

1. Logon to EventTracker manager workstation.

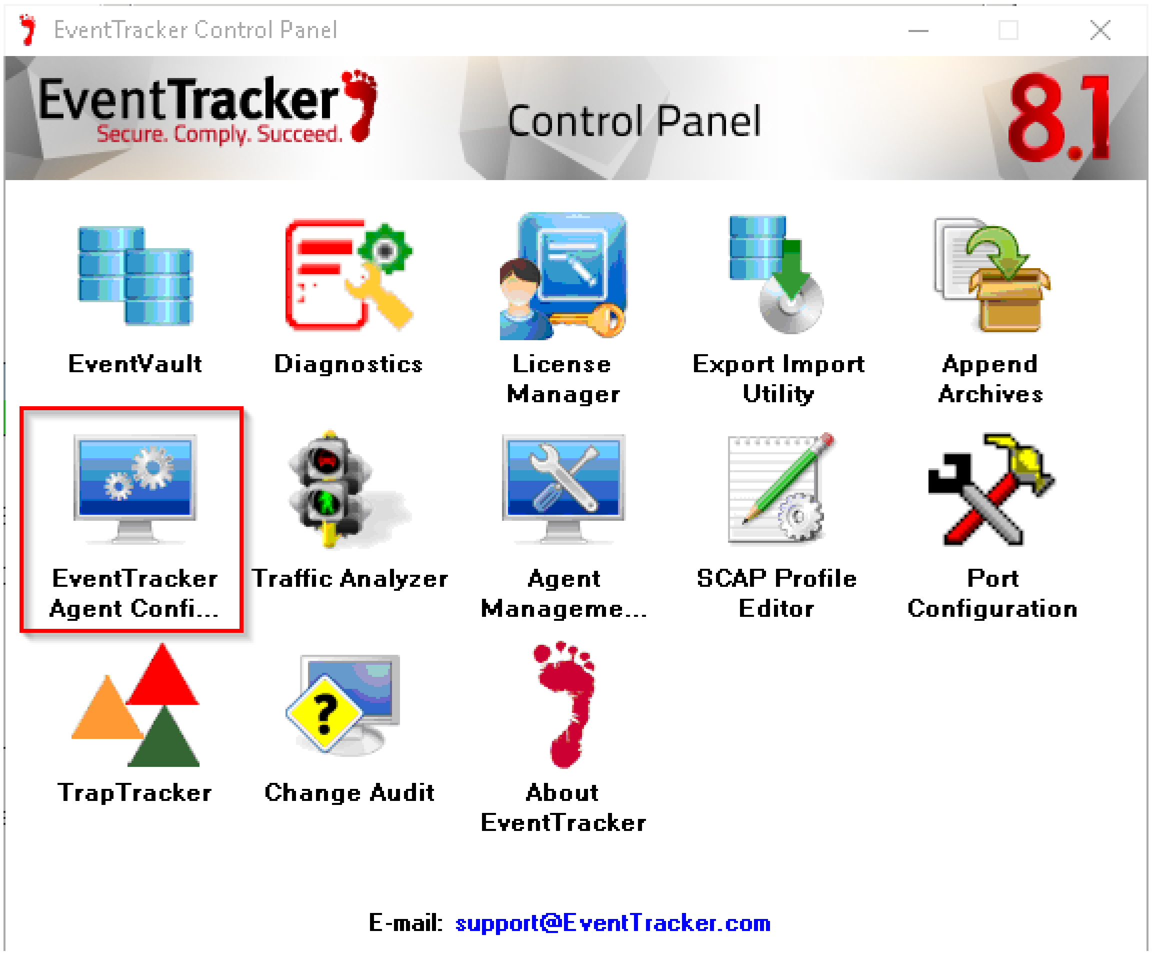
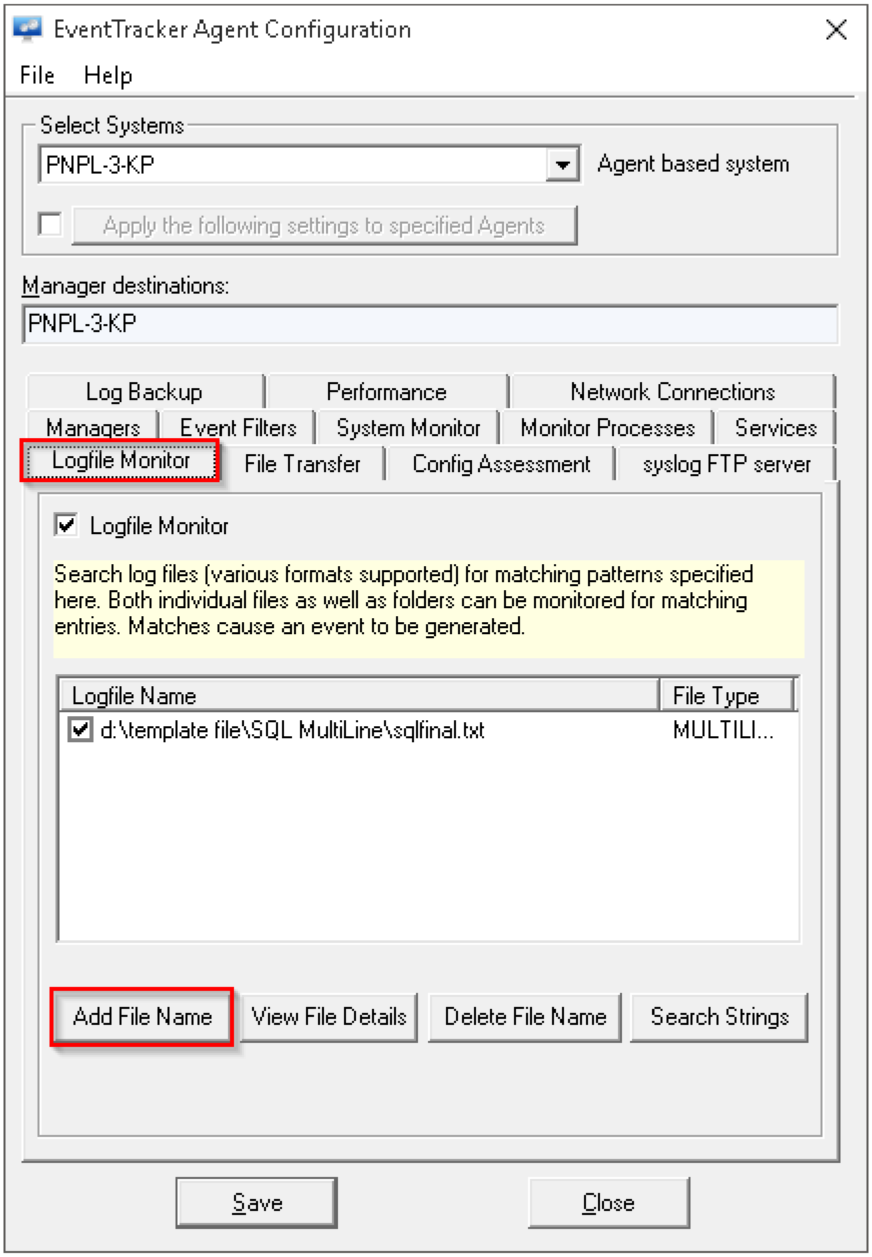


Figure 28

2. Open EventTracker control panel, click **EventTracker Agent Configuration**.



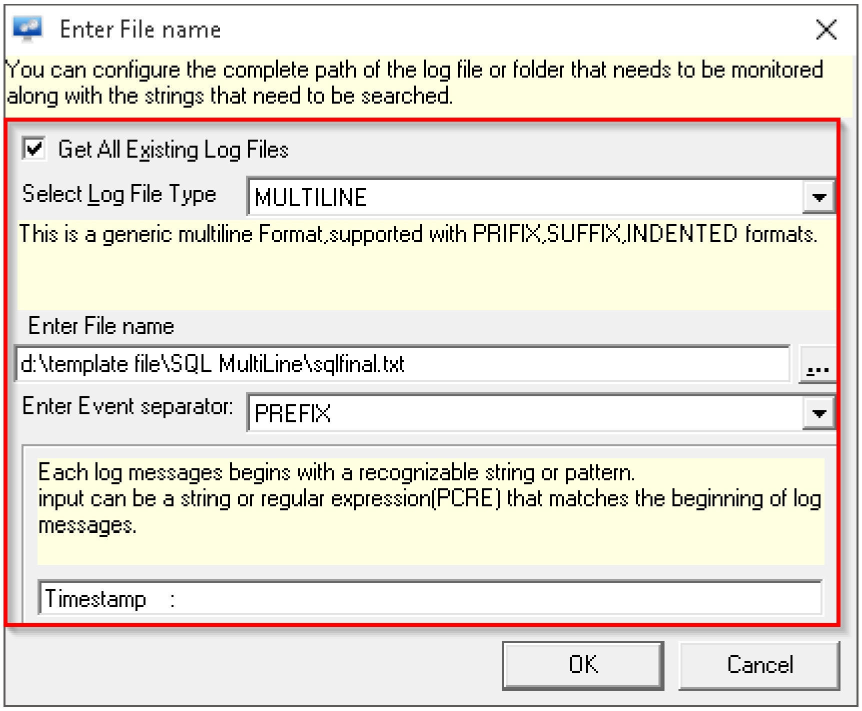
☑ Logfile Monitor

Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type
☑ d:\template file\SQL MultiLine\sqlfinal.txt	MULTILI...

Figure 29

3. Select **Logfile Monitor** tab and click **Add File Name**.



You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.

☑ Get All Existing Log Files

Select Log File Type: MULTILINE

This is a generic multiline Format,supported with PRIFIX,SUFFIX,INDENTED formats.

Enter File name: d:\template file\SQL MultiLine\sqlfinal.txt

Enter Event separator: PREFIX

Each log messages begins with a recognizable string or pattern.
input can be a string or regular expression(PCRE) that matches the beginning of log messages.

Timestamp :

Figure 30

4. Configure LFM settings as shown above. Browse and select **output txt** file from earlier configuration as **File Name** and enter “**Timestamp :** “as **PREFIX** for **MULTILINE** log file type.

5. Click **OK** to save.

EventTracker Knowledge Pack

Once MSSQL Server is configured to send audit logs to EventTracker Manager, either through audit specifications or extended events. EventTracker will process the received logs and aid an administrator with informative reports, effective alerts and dashboard visualizations.

Alerts

1. **MSSQL:Error detected* -** This alert is generated when SQL errors like syntax errors are generated.
2. **MSSQL:Audit created deleted or modified -** This alert is generated when audit, audit specification and extended event sessions are created, deleted or modified.
3. **MSSQL:Database backed up or restored -** This alert is generated when database backup is taken or it is restored.
4. **MSSQL: Database created or deleted or modified -** This alert is generated when a new database is created and older ones are deleted or modified.

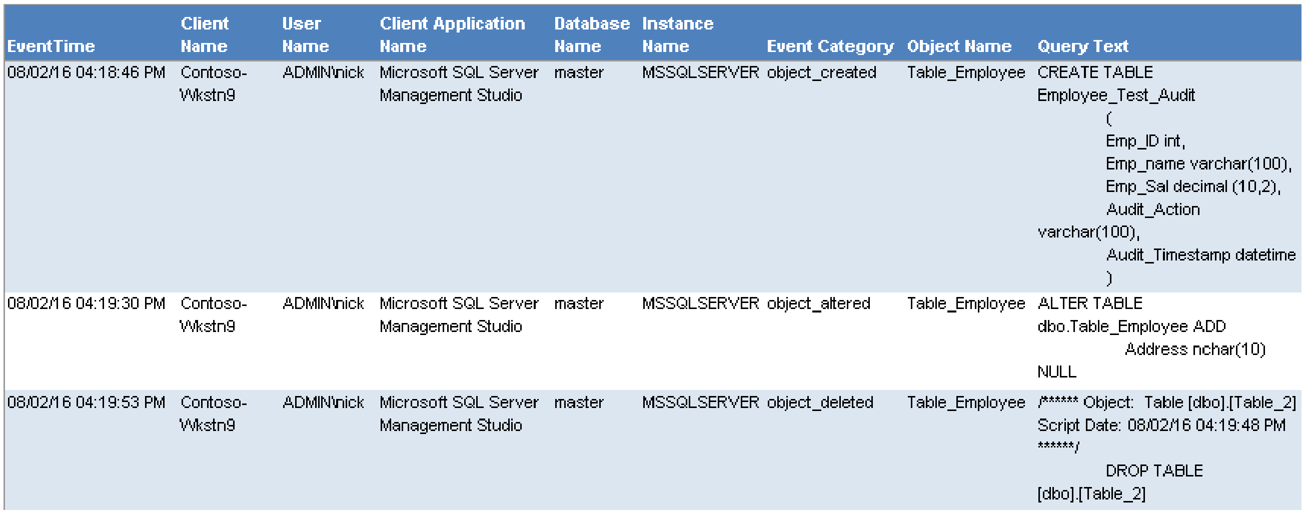
5. **MSSQL: Schema created or deleted or modified -** This alert is generated when new database schema is created and older ones are deleted or modified.
6. **MSSQL: View created or deleted or modified -** This alert is generated when new database view is created and older ones are deleted or modified.
7. **MSSQL: User enabled or disabled or unlocked -** This alert is generated when an existing login is enabled, disabled or unlocked.
8. **MSSQL: Permission granted or revoked or denied -** This alert is generated when permission is granted, revoked or denied to a login or user.
9. **MSSQL: Database and application role created or deleted or modified -** This alert is generated when new server or database role is created and older ones are deleted or modified.
10. **MSSQL: Stored procedure created or deleted or modified -** This alert is generated when new stored procedure is created and older ones are deleted or modified.
11. **MSSQL: Table created or deleted or modified -** This alert is generated when new table is created and older ones are deleted, truncated or modified.
12. **MSSQL: Index created or deleted or modified -** This alert is generated when new table view is created and older ones are deleted or modified.
13. **MSSQL: Trigger created or deleted or modified -** This alert is generated when new table or database trigger is created and older ones are deleted or modified.
14. **MSSQL: User created or deleted or modified -** This alert is generated when new login, user or credential is created and older ones are deleted or modified.
15. **MSSQL: User logon failure -** This alert is generated when an user fails to login SQL server.
16. **MSSQL: User and application role password reset or changed -** This alert is generated when password is changed or reset for login, credential or application role.

***Only available if extended events are enabled.**

Reports

Following reports are created using **extended session** events. Similar reports are available through audit specifications as well, but it will not have **Host Name, Application Name** and **event category** fields.

1. **MSSQL Extended-Table created or deleted or modified -** This report provides information related to table creation, deletion and alteration.

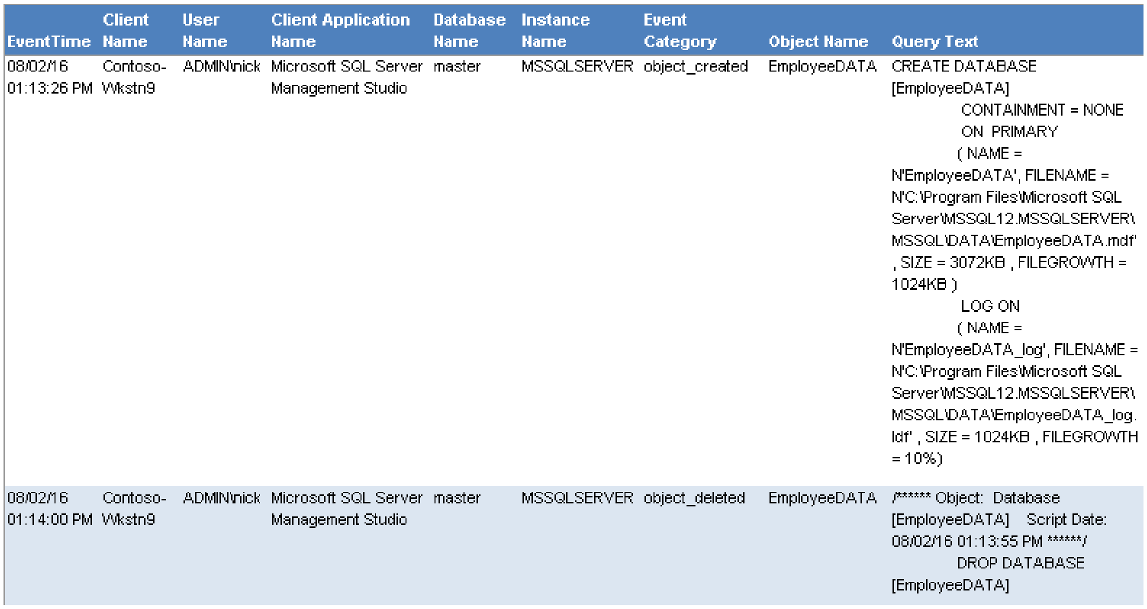


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text
08/02/16 04:18:46 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_created	Table_Employee	CREATE TABLE Employee_Test_Audit (Emp_ID int, Emp_name varchar(100), Emp_Sal decimal (10,2), Audit_Action varchar(100), Audit_Timestamp datetime)
08/02/16 04:19:30 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_altered	Table_Employee	ALTER TABLE dbo.Table_Employee ADD Address nchar(10) NULL
08/02/16 04:19:53 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_deleted	Table_Employee	/****** Object: Table [dbo].[Table_2] Script Date: 08/02/16 04:19:48 PM ******/ DROP TABLE [dbo].[Table_2]

Figure 31

```
ENTRY:Timestamp    : 08/02/16 04:19:30 PM
AppName      : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : object_altered
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   : USRTAB
ObjectName   : Table_Employee
Statement    :
SQLText      : ALTER TABLE dbo.Table_Employee ADD
               Address nchar(10) NULL
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

2. **MSSQL Extended-Database created or deleted or modified -** This report provides information related to database creation, deletion and alteration.

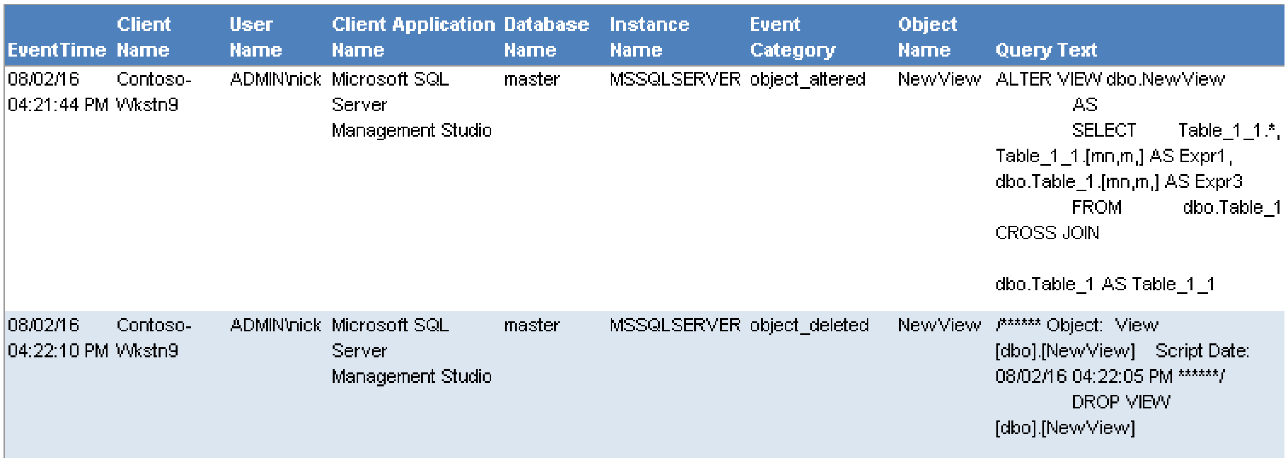


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text
08/02/16 01:13:26 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_created	EmployeeDATA	CREATE DATABASE [EmployeeDATA] CONTAINMENT = NONE ON PRIMARY (NAME = N'EmployeeDATA', FILENAME = N'C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\EmployeeDATA.mdf' , SIZE = 3072KB , FILEGROWTH = 1024KB) LOG ON (NAME = N'EmployeeDATA_log', FILENAME = N'C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\EmployeeDATA_log.ldf' , SIZE = 1024KB , FILEGROWTH = 10%)
08/02/16 01:14:00 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_deleted	EmployeeDATA	/****** Object: Database [EmployeeDATA] Script Date: 08/02/16 01:13:55 PM ******/ DROP DATABASE [EmployeeDATA]

Figure 32

```
ENTRY:Timestamp    : 08/02/16 01:14:00 PM
AppName      : Microsoft SQL Server Management Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : object_deleted
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   : DATABASE
ObjectName   : EmployeeDATA
Statement    :
SQLText      : /****** Object:  Database [EmployeeDATA]
Script Date: 08/02/16 01:13:55 PM ******/
            DROP DATABASE [EmployeeDATA]
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

3. **MSSQL Extended-View created or deleted or modified -** This report provides information related to database view creation, deletion and alteration.

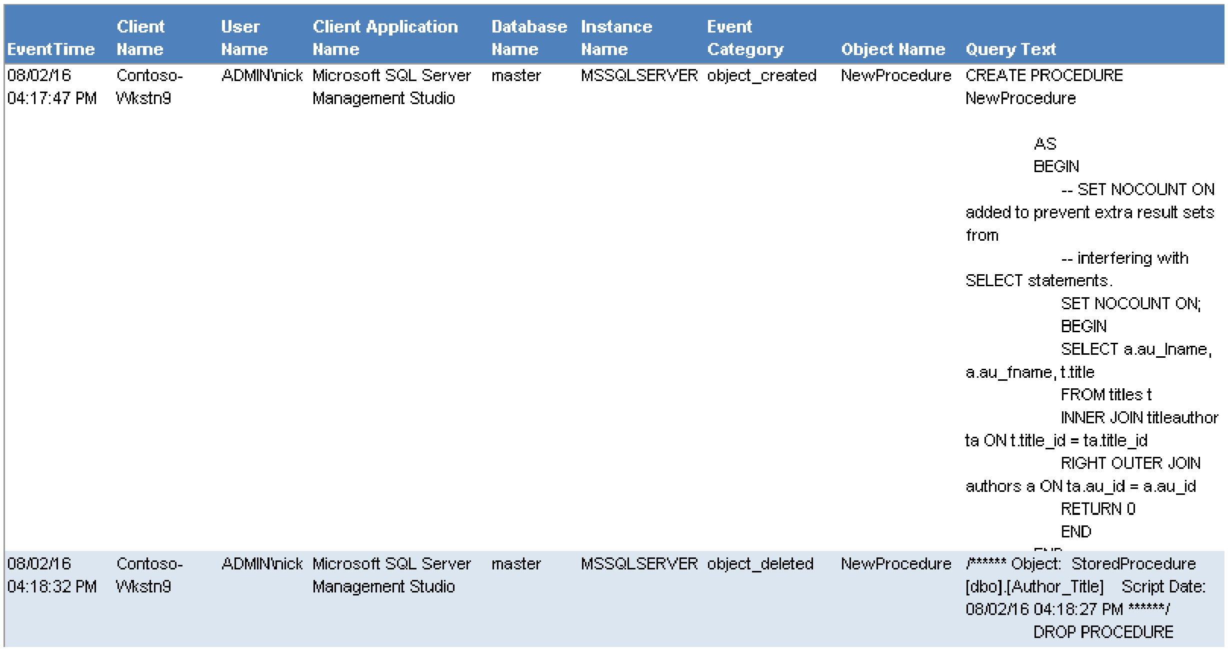


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text
08/02/16 04:21:44 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_altered	NewView	ALTER VIEW dbo.NewView AS SELECT Table_1_1.*, Table_1_1.[mn,m,] AS Expr1, dbo.Table_1.[mn,m,] AS Expr3 FROM dbo.Table_1 CROSS JOIN dbo.Table_1 AS Table_1_1
08/02/16 04:22:10 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_deleted	NewView	/****** Object: View [dbo].[NewView] Script Date: 08/02/16 04:22:05 PM ******/ DROP VIEW [dbo].[NewView]

Figure 33

```
ENTRY:Timestamp    : 08/02/16 04:22:10 PM
AppName        : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : object_deleted
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   : VIEW
ObjectName   : NewView
Statement    :
SQLText      : /****** Object:  View [dbo].[NewView]
Script Date: 08/02/16 04:22:05 PM ******/
             DROP VIEW [dbo].[NewView]
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

4. **MSSQL Extended-Stored procedure created or deleted or modified -** This report provides information related to stored procedure creation, deletion and alteration.



EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text

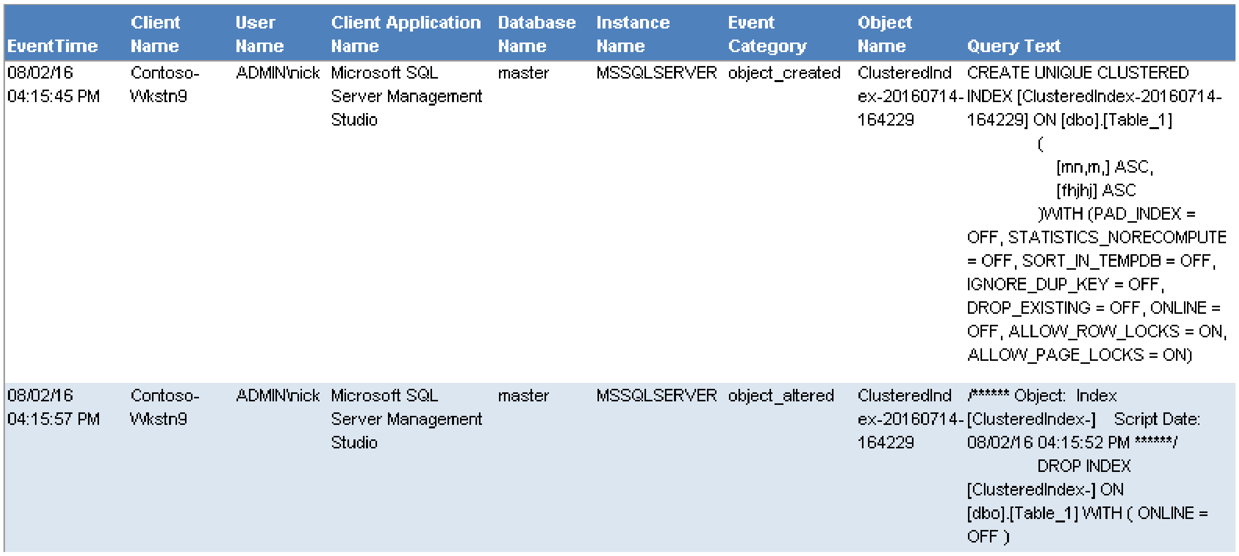
08/02/16 04:17:47 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_created	NewProcedure	CREATE PROCEDURE NewProcedure
								
								AS
								BEGIN
								-- SET NOCOUNT ON added to prevent extra result sets from
								-- interfering with SELECT statements.
								SET NOCOUNT ON;
								BEGIN
								SELECT a.au_lname, a.au_fname, t.title
								FROM titles t
								INNER JOIN titleauthor ta ON t.title_id = ta.title_id
								RIGHT OUTER JOIN authors a ON ta.au_id = a.au_id
								RETURN 0
								END

08/02/16 04:18:32 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_deleted	NewProcedure	/****** Object: StoredProcedure [dbo].[Author_Title] Script Date: 08/02/16 04:18:27 PM ******/ DROP PROCEDURE

Figure 34

```
ENTRY:Timestamp    : 08/02/16 04:18:32 PM
AppName          : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : object_deleted
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   : PROC
ObjectName   : NewProcedure
Statement    :
SQLText          : /****** Object:   StoredProcedure
[dbo].[Author_Title]    Script Date: 08/02/16 04:18:27
PM ******/
            DROP PROCEDURE [dbo].[NewProcedure]
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

5. **MSSQL Extended-Index created or deleted or modified -** This report provides information related to table index creation, deletion and alteration.

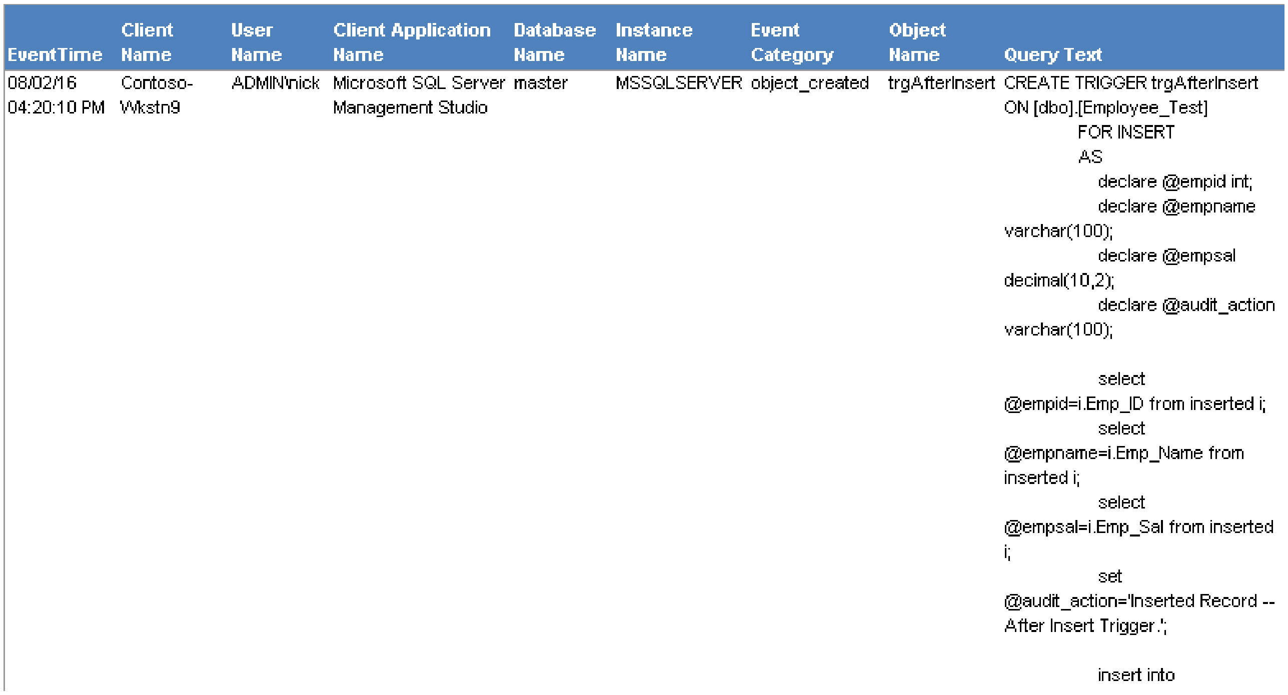


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text
08/02/16 04:15:45 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_created	ClusteredIndex-20160714-164229	CREATE UNIQUE CLUSTERED INDEX [ClusteredIndex-20160714-164229] ON [dbo].[Table_1] ([mn,m,] ASC, [fhjhj] ASC)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, DROP_EXISTING = OFF, ONLINE = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON)
08/02/16 04:15:57 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_altered	ClusteredIndex-20160714-164229	/****** Object: Index [ClusteredIndex-] Script Date: 08/02/16 04:15:52 PM ******/ DROP INDEX [ClusteredIndex-] ON [dbo].[Table_1] WITH (ONLINE = OFF)

Figure 35

```
ENTRY:Timestamp    : 08/02/16 04:15:57 PM
AppName          :  Microsoft  SQL  Server  Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : object_altered
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   : INDEX
ObjectName   : ClusteredIndex-20160714-164229
Statement    :
SQLText      : /****** Object:  Index [ClusteredIndex-]
Script Date: 08/02/16 04:15:52 PM ******/
           DROP      INDEX      [ClusteredIndex-]      ON
[dbo].[Table_1] WITH ( ONLINE = OFF )
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

6. **MSSQL Extended-Trigger created or deleted or modified -** This report provides information related to table and database trigger creation, deletion and alteration.



EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text

08/02/16 04:20:10 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_created	trgAfterInsert	CREATE TRIGGER trgAfterInsert ON [dbo].[Employee_Test]
								FOR INSERT
								AS
								declare @empid int;
								declare @empname varchar(100);
								declare @empsal decimal(10,2);
								declare @audit_action varchar(100);
								select @empid=i.Emp_ID from inserted i;
								select @empname=i.Emp_Name from inserted i;
								select @empsal=i.Emp_Sal from inserted i;
								set @audit_action='Inserted Record -- After Insert Trigger.';
								insert into

Figure 36

```
ENTRY:Timestamp    : 08/02/16 04:20:10 PM
AppName      : Microsoft SQL Server Management Studio
HostName      : Contoso-Wkstn9
UserName      : ADMIN\nick
EventDetails : object_created
DataBase      : master
Instance      : MSSQLSERVER
ObjectType   : TRIGGER
ObjectName   : trgAfterInsert
Statement    :
SQLText                  :   CREATE   TRIGGER   trgAfterInsert   ON
[dbo].[Employee_Test]
              FOR INSERT
              AS
                  declare @empid int;
                  declare @empname varchar(100);
                  declare @empsal decimal(10,2);
                  declare @audit_action varchar(100);

                  select @empid=i.Emp_ID from inserted i;
                  select @empname=i.Emp_Name from inserted i;
                  select @empsal=i.Emp_Sal from inserted i;
                  set  @audit_action='Inserted  Record  --  After  Insert
```

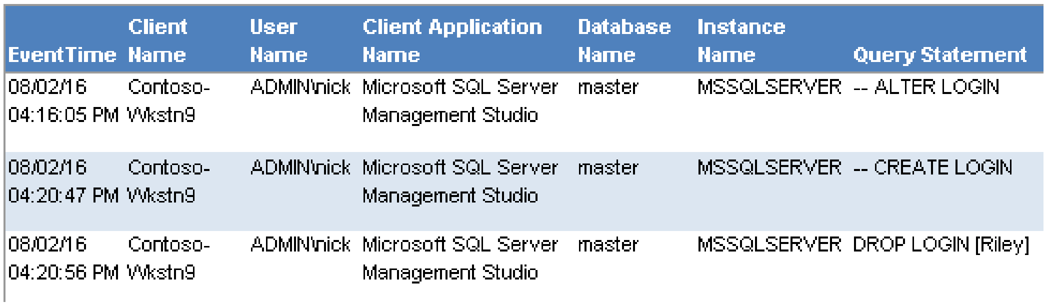
```
Trigger.';

                insert into Employee_Test_Audit

(Emp_ID,Emp_Name,Emp_Sal,Audit_Action,Audit_Timestamp)

values(@empid,@empname,@empsal,@audit_action,getdate())
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

7. **MSSQL Extended-User created or deleted or modified -** This report provides information related to login, user and credential creation, deletion and alteration.

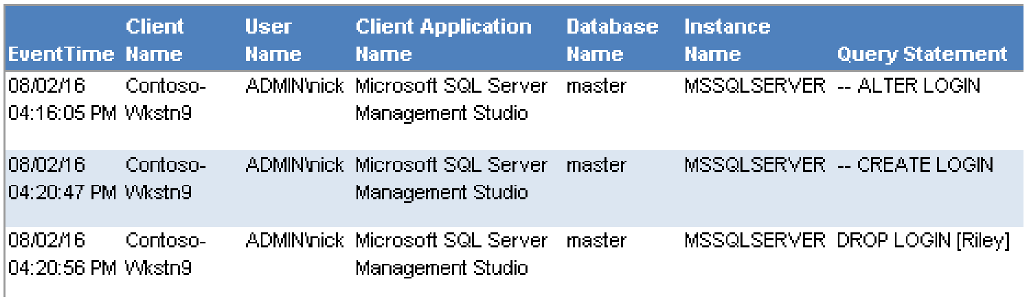


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Query Statement
08/02/16 04:16:05 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	-- ALTER LOGIN
08/02/16 04:20:47 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	-- CREATE LOGIN
08/02/16 04:20:56 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	DROP LOGIN [Riley]

Figure 37

```
ENTRY:Timestamp    : 08/02/16 04:16:05 PM
AppName      : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : sql_statement_completed
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   :
ObjectName   :
Statement    : -- ALTER LOGIN
SQLText      : *password--------------------------------------
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

8. **MSSQL Extended-Database and application role created or deleted or modified -** This report provides information related to server, database and application role creation, deletion and alteration.

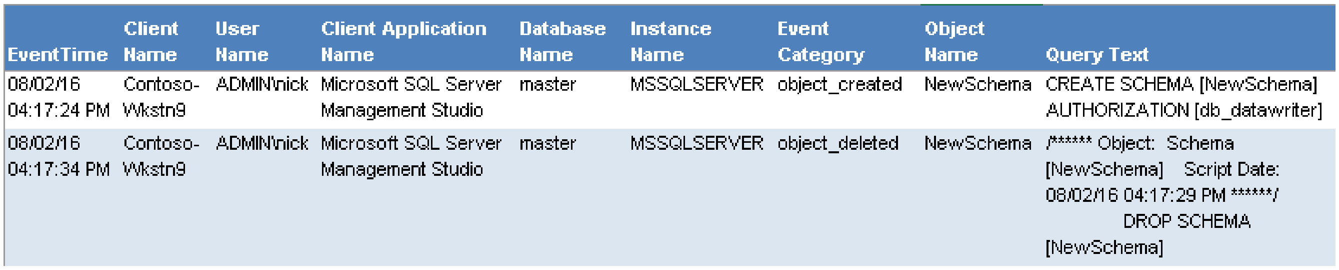


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Query Statement
08/02/16 04:16:05 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	-- ALTER LOGIN
08/02/16 04:20:47 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	-- CREATE LOGIN
08/02/16 04:20:56 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	DROP LOGIN [Riley]

Figure 38

```
ENTRY:Timestamp    : 08/02/16 04:16:42 PM
AppName      : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails :sql_statement_completed
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   :
ObjectName   :
Statement    : CREATE ROLE [New Role]
AUTHORIZATION [db_backupoperator]
SQLText      : CREATE ROLE [New Role]
AUTHORIZATION [db_backupoperator]
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

9. **MSSQL Extended-Schema created or deleted or modified -** This report provides information related to database schema creation, deletion and alteration.

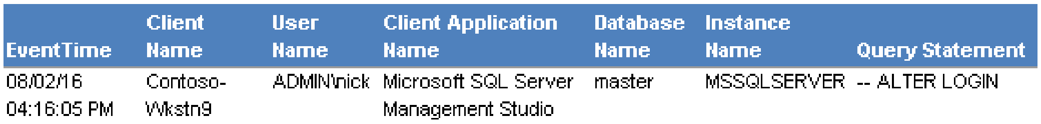


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text
08/02/16 04:17:24 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_created	NewSchema	CREATE SCHEMA [NewSchema] AUTHORIZATION [db_datawriter]
08/02/16 04:17:34 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_deleted	NewSchema	/****** Object: Schema [NewSchema] Script Date: 08/02/16 04:17:29 PM ******/ DROP SCHEMA [NewSchema]

Figure 39

```
ENTRY:Timestamp    : 08/02/16 04:17:34 PM
AppName          :  Microsoft  SQL  Server  Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : object_deleted
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   : SCHEMA
ObjectName   : NewSchema
Statement    :
SQLText       : /****** Object:   Schema  [NewSchema]
Script Date: 08/02/16 04:17:29 PM ******/
            DROP SCHEMA [NewSchema]
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

10. **MSSQL Extended-User and application role password reset or changed -** This report provides information related to login, credential and application role's creation, deletion and alteration.

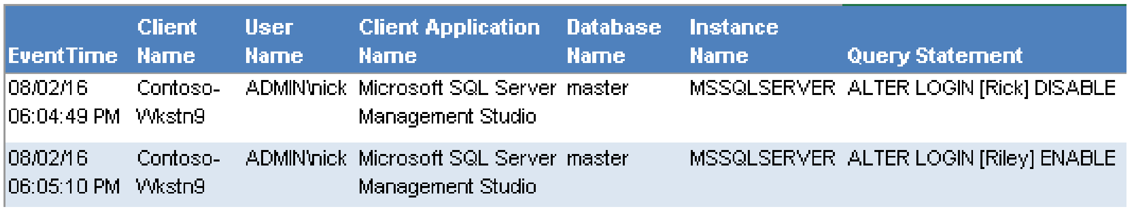


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Query Statement
08/02/16 04:16:05 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	-- ALTER LOGIN

Figure 40

```
ENTRY:Timestamp    : 08/02/16 04:16:05 PM
AppName      : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails :sql_statement_completed
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   :
ObjectName   :
Statement    : -- ALTER LOGIN
SQLText      : *password--------------------------------------
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

11. **MSSQL Extended-User enabled or disabled or unlocked -** This report provides information related to login account enabled, disabled and unlocked.

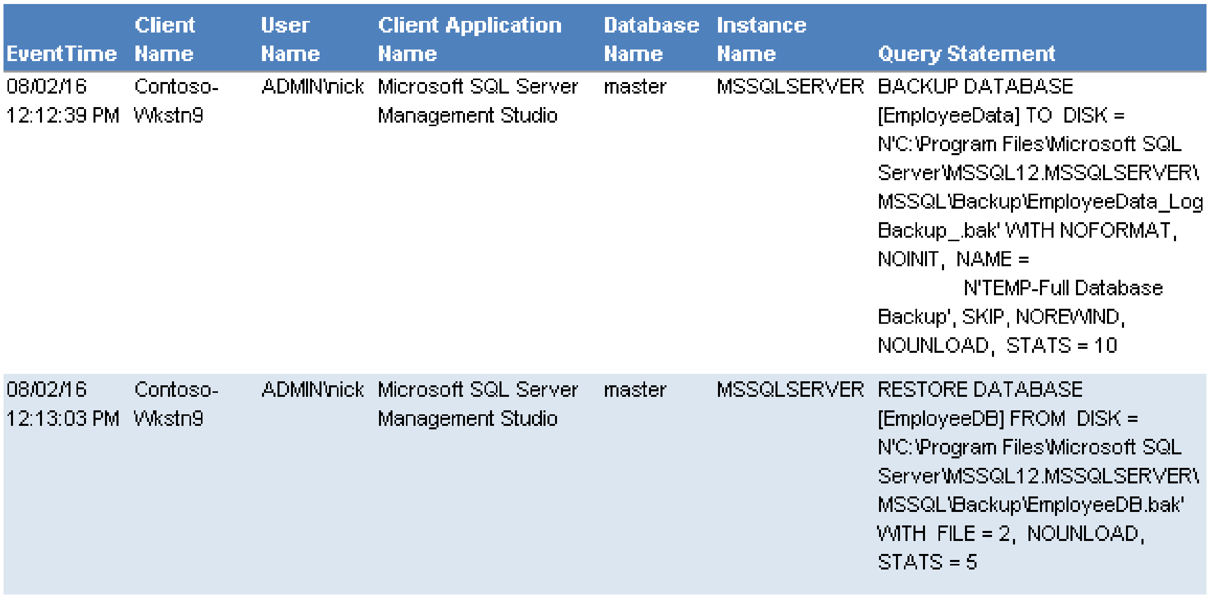


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Query Statement
08/02/16 06:04:49 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	ALTER LOGIN [Rick] DISABLE
08/02/16 06:05:10 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	ALTER LOGIN [Riley] ENABLE

Figure 41

```
ENTRY:Timestamp    : 08/02/16 06:04:49 PM
AppName      : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails :sql_statement_completed
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   :
ObjectName   :
Statement    : ALTER LOGIN [Rick] DISABLE
SQLText      : ALTER LOGIN [Rick] DISABLE
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

12. **MSSQL Extended-Database backed up or restored -** This report provides information related to database backup and restore.

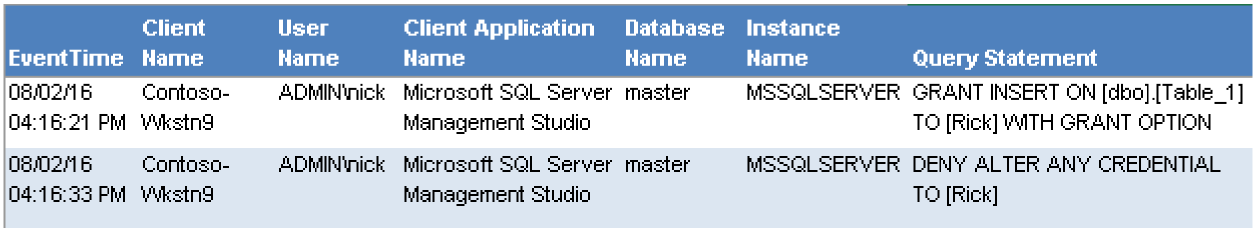


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Query Statement
08/02/16 12:12:39 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	BACKUP DATABASE [EmployeeData] TO DISK = N'C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Backup\EmployeeData_LogBackup_.bak' WITH NOFORMAT, NOINIT, NAME = N'TEMP-Full Database Backup', SKIP, NOREWIND, NOUNLOAD, STATS = 10
08/02/16 12:13:03 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	RESTORE DATABASE [EmployeeDB] FROM DISK = N'C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Backup\EmployeeDB.bak' WITH FILE = 2, NOUNLOAD, STATS = 5

Figure 42

```
ENTRY:Timestamp    : 08/02/16 12:13:03 PM
AppName      : Microsoft SQL Server Management Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : sql_statement_completed
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   :
ObjectName   :
Statement    : RESTORE DATABASE [EmployeeDB] FROM  DISK = N'C:\Program
Files\Microsoft SQL
Server\MSSQL12.MSSQLSERVER\MSSQL\Backup\EmployeeDB.bak' WITH  FILE
= 2,  NOUNLOAD,  STATS = 5
SQLText      :
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

13. **MSSQL Extended-Permission granted or revoked or denied -** This report provides information related to permission granted, revoked and denied to a user or login.

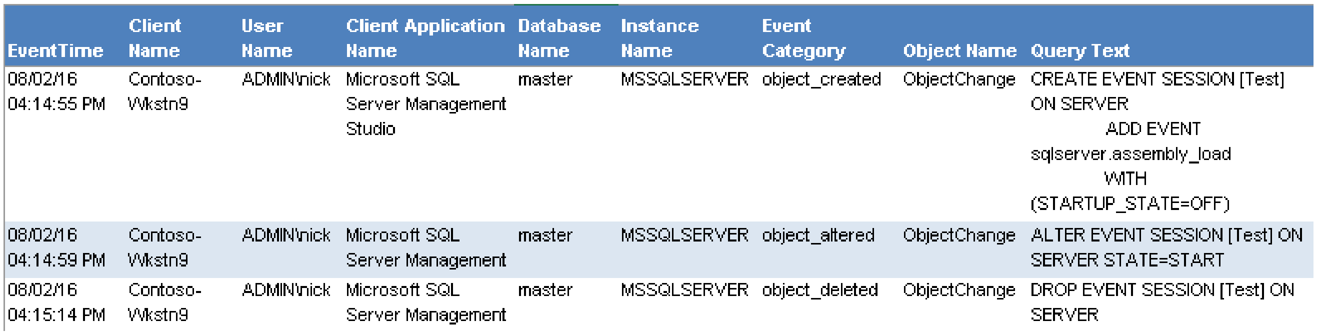


EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Query Statement
08/02/16 04:16:21 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	GRANT INSERT ON [dbo].[Table_1] TO [Rick] WITH GRANT OPTION
08/02/16 04:16:33 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	DENY ALTER ANY CREDENTIAL TO [Rick]

Figure 43

```
ENTRY:Timestamp    : 08/02/16 04:16:21 PM
AppName        : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails :sql_statement_completed
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   :
ObjectName   :
Statement     : GRANT INSERT ON [dbo].[Table_1] TO
[Rick] WITH GRANT OPTION
SQLText        : GRANT INSERT ON [dbo].[Table_1] TO
[Rick] WITH GRANT OPTION
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

14. **MSSQL Extended-Extended event session created or deleted or modified* -** This report provides information related to extended event session creation, deletion and alteration.



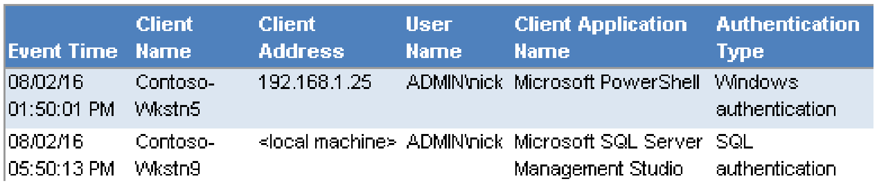
EventTime	Client Name	User Name	Client Application Name	Database Name	Instance Name	Event Category	Object Name	Query Text
08/02/16 04:14:55 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	master	MSSQLSERVER	object_created	ObjectChange	CREATE EVENT SESSION [Test] ON SERVER ADD EVENT sqlserver.assembly_load WITH (STARTUP_STATE=OFF)
08/02/16 04:14:59 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management	master	MSSQLSERVER	object_altered	ObjectChange	ALTER EVENT SESSION [Test] ON SERVER STATE=START
08/02/16 04:15:14 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management	master	MSSQLSERVER	object_deleted	ObjectChange	DROP EVENT SESSION [Test] ON SERVER

Figure 44

```
ENTRY:Timestamp    : 08/02/16 04:14:55 PM
AppName       : Microsoft SQL Server Management Studio
HostName      : Contoso-Wkstn9
```

```
UserName     : ADMIN\nick
EventDetails : object_created
DataBase     : master
Instance     : MSSQLSERVER
ObjectType   : SRVXESES
ObjectName   : ObjectChange
Statement    :
SQLText      : CREATE EVENT SESSION [Test] ON SERVER
             ADD EVENT sqlserver.assembly_load
             WITH (STARTUP_STATE=OFF)
Message      :
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

15. **MSSQL Extended-User logon success -** This report provides information related to user logon success.

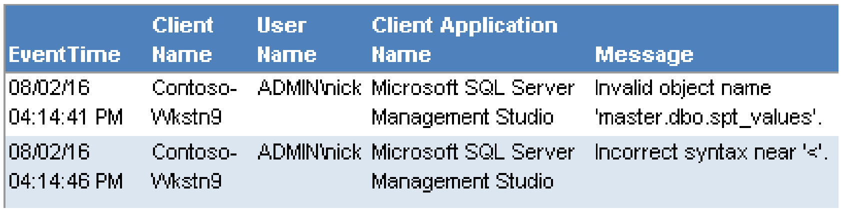


Event Time	Client Name	Client Address	User Name	Client Application Name	Authentication Type
08/02/16 01:50:01 PM	Contoso-Wkstn5	192.168.1.25	ADMIN\nick	Microsoft PowerShell	Windows authentication
08/02/16 05:50:13 PM	Contoso-Wkstn9	<local machine>	ADMIN\nick	Microsoft SQL Server Management Studio	SQL authentication

Figure 45

```
ENTRY:Timestamp    : 08/02/16 01:50:01 PM
AppName          :  Microsoft  SQL  Server  Management
Studio
HostName     : Contoso-Wkstn5
UserName     : ADMIN\nick
EventDetails : error_reported
DataBase     :
Instance     :
ObjectType   :
ObjectName   :
Statement    :
SQLText      :
Message      : Login succeeded for user ‘ADMIN\nick’.
Connection  made  using  Windows  authentication.
[CLIENT: 192.168.1.25]
```

16. **MSSQL Extended-Error details* -** This report provides information related to errors generated by SQL.

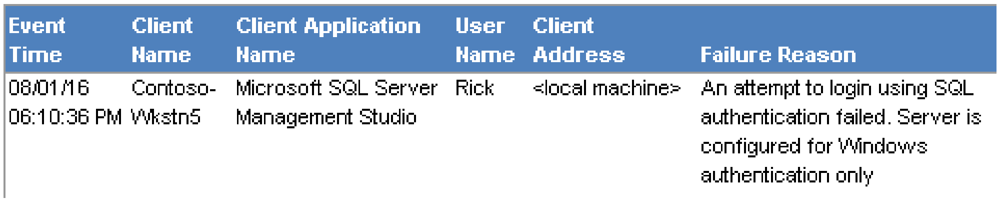


EventTime	Client Name	User Name	Client Application Name	Message
08/02/16 04:14:41 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	Invalid object name 'master.dbo.spt_values'.
08/02/16 04:14:46 PM	Contoso-Wkstn9	ADMIN\nick	Microsoft SQL Server Management Studio	Incorrect syntax near '<'.

Figure 46

```
ENTRY:Timestamp    : 08/02/16 04:14:46 PM
AppName      : Microsoft SQL Server Management
Studio
HostName     : Contoso-Wkstn9
UserName     : ADMIN\nick
EventDetails : error_reported
DataBase     :
Instance     :
ObjectType   :
ObjectName   :
Statement    :
SQLText      :
Message      : Incorrect syntax near '<'.
FILE:d:\SQL\sql logs.txt
TYPE:MULTILINE
FIELD: *
```

17. **MSSQL Extended-User logon failure -** This report provides information related to user logon failure.



Event Time	Client Name	Client Application Name	User Name	Client Address	Failure Reason
08/01/16 06:10:36 PM	Contoso-Wkstn5	Microsoft SQL Server Management Studio	Rick	<local machine>	An attempt to login using SQL authentication failed. Server is configured for Windows authentication only

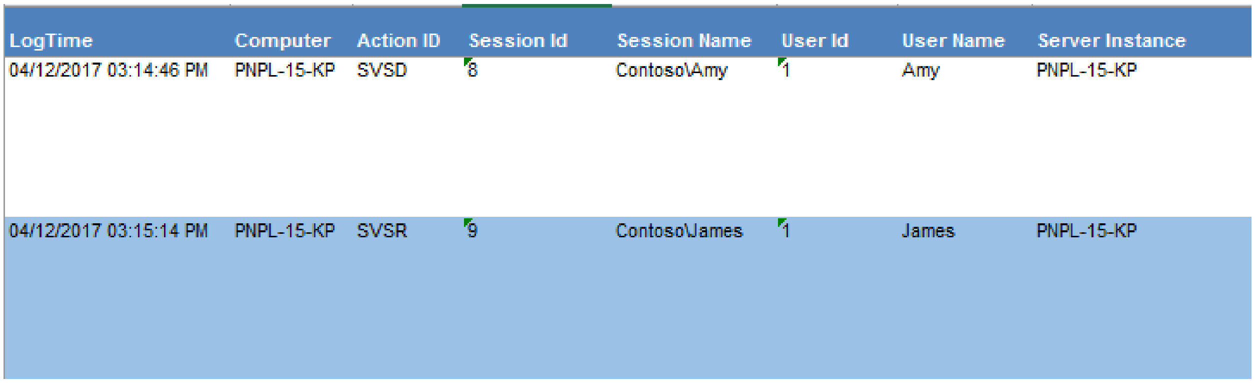
Figure 47

```
Timestamp    : 08/01/16 06:10:36 PM
AppName          :  Microsoft  SQL  Server  Management
Studio
HostName     : Contoso-Wkstn5
UserName     : ADMIN\rick
EventDetails : error_reported
DataBase     :
Instance     :
```

```
ObjectType   :
ObjectName   :
Statement    :
SQLText      :
Message      : Login failed for user ‘Rick’. An attempt to
login using SQL authentication failed. Server is
configured for Windows authentication only. [CLIENT:
<local machine>]
```

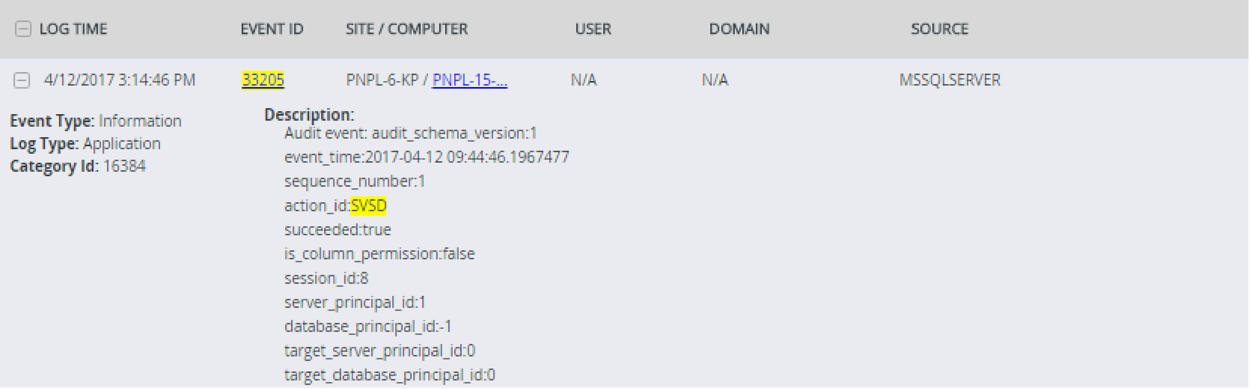
***Only available if extended events are enabled.**

18. MSSQL-Database start and shutdown- This report provides information related to MSSQL database Start and shutdown status.



LogTime	Computer	Action ID	Session Id	Session Name	User Id	User Name	Server Instance
04/12/2017 03:14:46 PM	PNPL-15-KP	SVSD	8	Contoso\Amy	1	Amy	PNPL-15-KP
04/12/2017 03:15:14 PM	PNPL-15-KP	SVSR	9	Contoso\James	1	James	PNPL-15-KP

Logs Considered



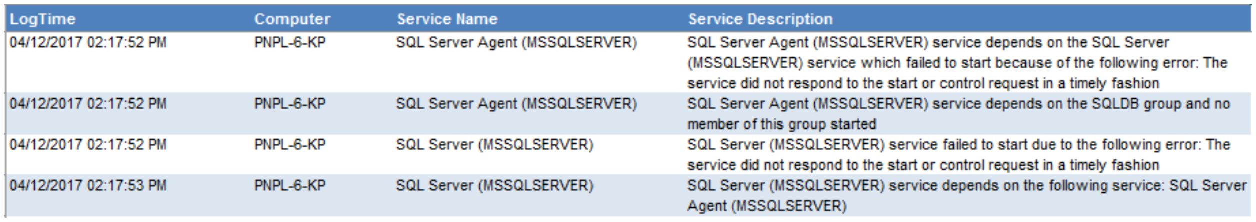
LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
4/12/2017 3:14:46 PM	33205	PNPL-6-KP / PNPL-15-...	N/A	N/A	MSSQLSERVER

Event Type: Information
Log Type: Application
Category Id: 16384

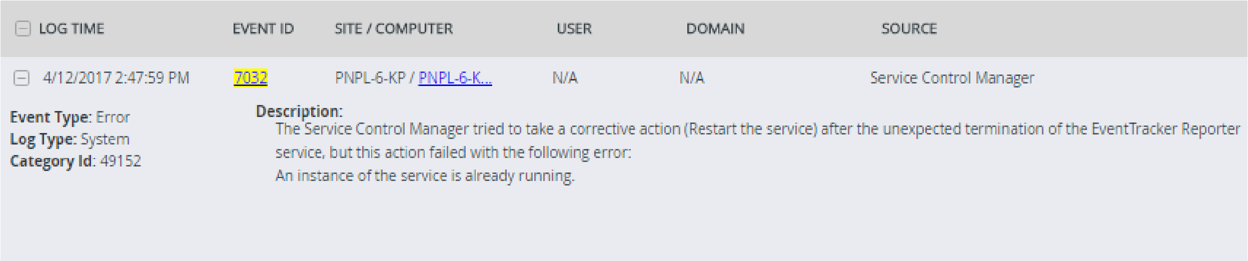
Description:

```
Audit event: audit_schema_version:1
event_time:2017-04-12 09:44:46.1967477
sequence_number:1
action_id:SVSD
succeeded:true
is_column_permission:false
session_id:8
server_principal_id:1
database_principal_id:-1
target_server_principal_id:0
target_database_principal_id:0
```

19.MSSQL-Service failures- This report provides information related to the MSSQL service failures.



LogTime	Computer	Service Name	Service Description
04/12/2017 02:17:52 PM	PNPL-6-KP	SQL Server Agent (MSSQLSERVER)	SQL Server Agent (MSSQLSERVER) service depends on the SQL Server (MSSQLSERVER) service which failed to start because of the following error: The service did not respond to the start or control request in a timely fashion
04/12/2017 02:17:52 PM	PNPL-6-KP	SQL Server Agent (MSSQLSERVER)	SQL Server Agent (MSSQLSERVER) service depends on the SQLDB group and no member of this group started
04/12/2017 02:17:52 PM	PNPL-6-KP	SQL Server (MSSQLSERVER)	SQL Server (MSSQLSERVER) service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion
04/12/2017 02:17:53 PM	PNPL-6-KP	SQL Server (MSSQLSERVER)	SQL Server (MSSQLSERVER) service depends on the following service: SQL Server Agent (MSSQLSERVER)



⊟ LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
⊟ 4/12/2017 2:47:59 PM	7032	PNPL-6-KP / PNPL-6-K...	N/A	N/A	Service Control Manager

Event Type: Error
Log Type: System
Category Id: 49152

Description:
The Service Control Manager tried to take a corrective action (Restart the service) after the unexpected termination of the EventTracker Reporter service, but this action failed with the following error:
An instance of the service is already running.

Dashboards

Following dashboards are created using **extended session** events. Similar dashboards are available through audit specifications as well, but it will not have **Host Name, Application Name** and **event category** fields.

1. **SQL Errors with client application name in last 24 hrs***

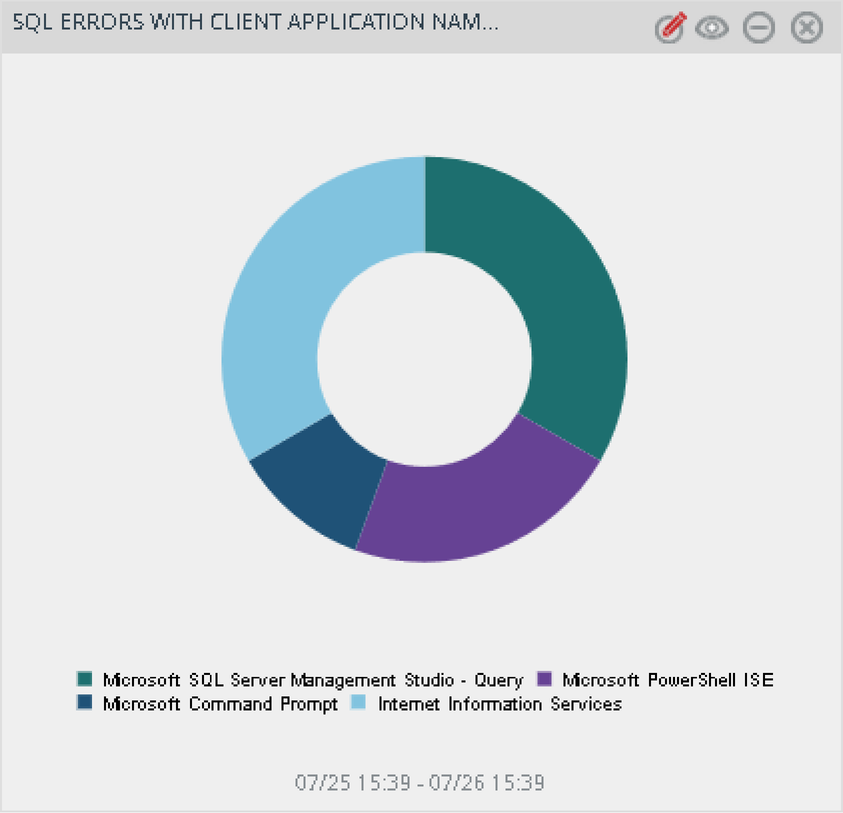


Figure 48

2. SQL logon status in last 24 hrs

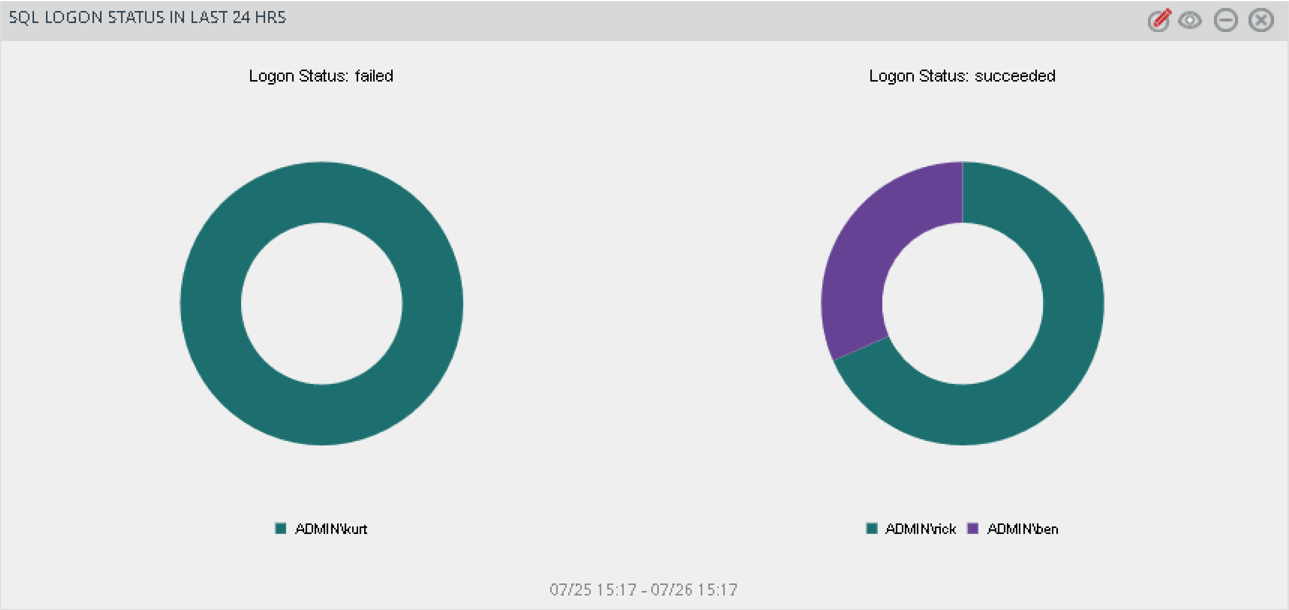


Figure 49

3. SQL permission change with client name in last 24 hrs

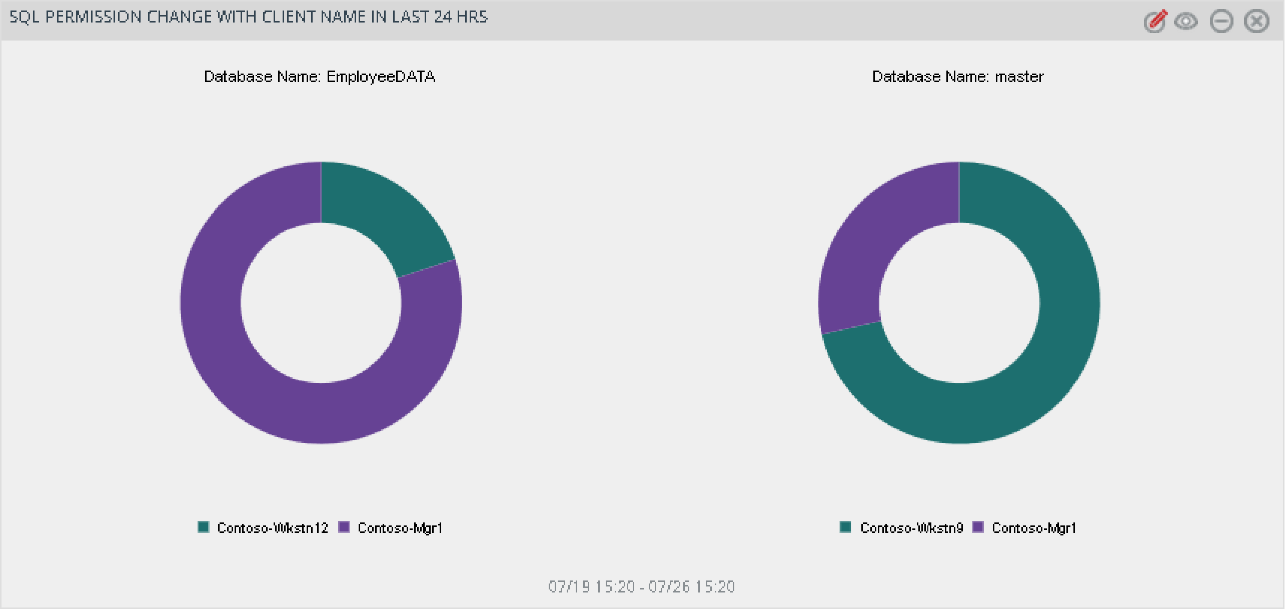


Figure 50

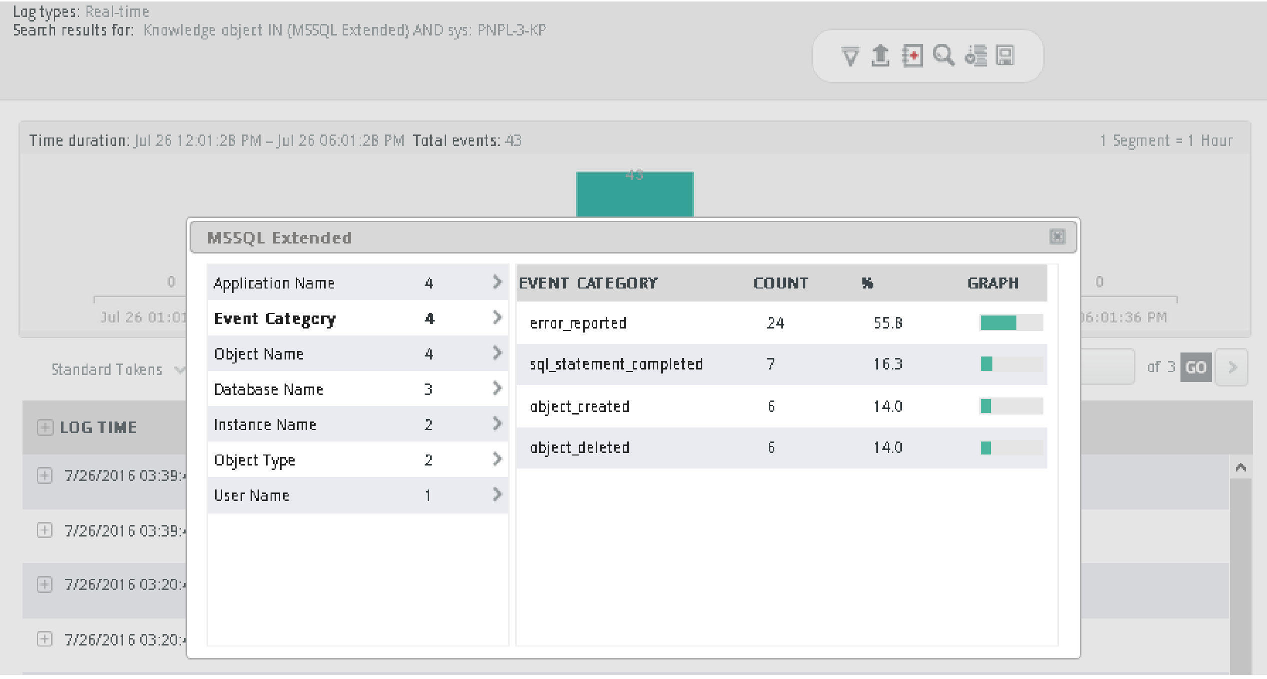
***Only available if extended events are enabled.**

Knowledge Objects

Following KO is created using **extended session** events. Similar KO is available through audit specifications as well, but it will not have **Host Name, Application Name** and **event category** fields.

1. **MSSQL Extended -** This KO aids an administrator to analyze and visualize all the audit events generated by SQL server.

Sample log search for SQL extended events using smart tokens is shown below:



Log types: Real-time
Search results for: Knowledge object IN (MSSQL Extended) AND sys: PNPL-3-KP

Time duration: Jul 26 12:01:28 PM – Jul 26 06:01:28 PM Total events: 43
1 Segment = 1 Hour

MSSQL Extended

Application Name	4	>
Event Category	**4**	>
Object Name	4	>
Database Name	3	>
Instance Name	2	>
Object Type	2	>
User Name	1	>

EVENT CATEGORY	COUNT	%	GRAPH
error_reported	24	55.8	🟩
sql_statement_completed	7	16.3	🟩
object_created	6	14.0	🟩
object_deleted	6	14.0	🟩

Figure 51

Configure Microsoft SQL Server KP

Below mentioned are the common steps for KP configuration. **Please use KP items corresponding to the integration method used.**

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

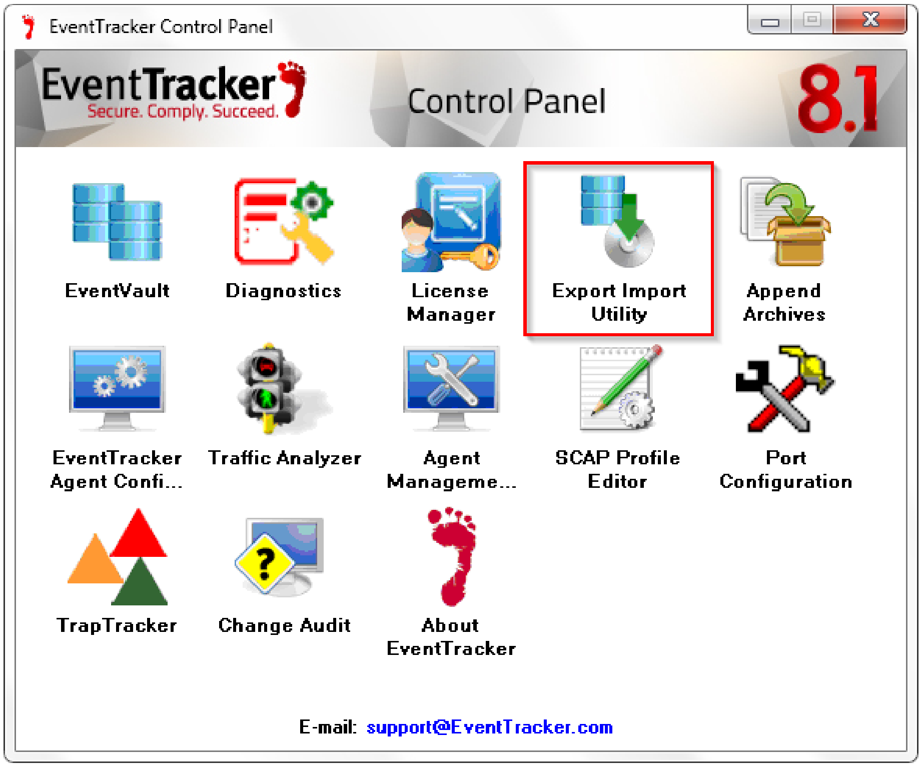


Figure 52

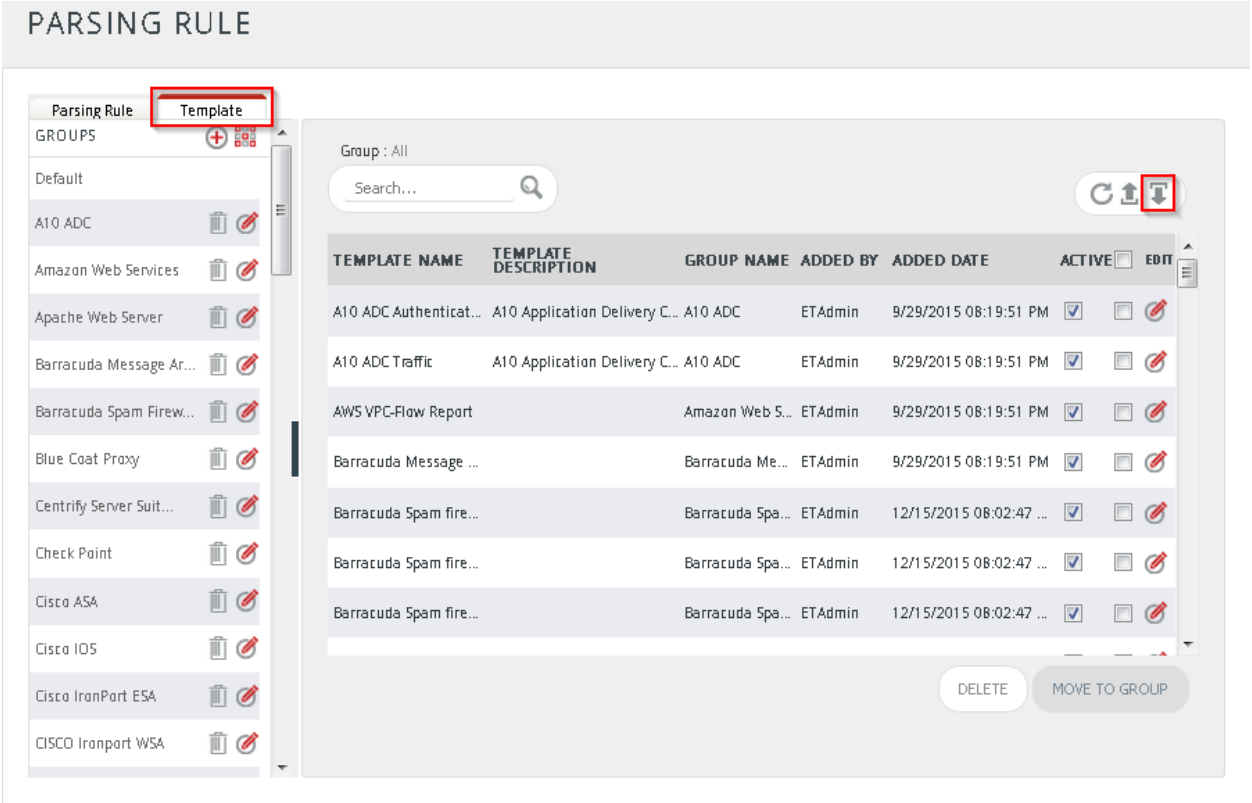
Please import KP items in the following sequence:

- **Token Templates**
- **Parsing Rules**
- **Behavior Rules**
- **Alerts**
- **Reports**
- **Knowledge Object**

Import **mentioned KP items** as given below:

Import Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on ⤓ ‘**Import**’ option.



PARSING RULE

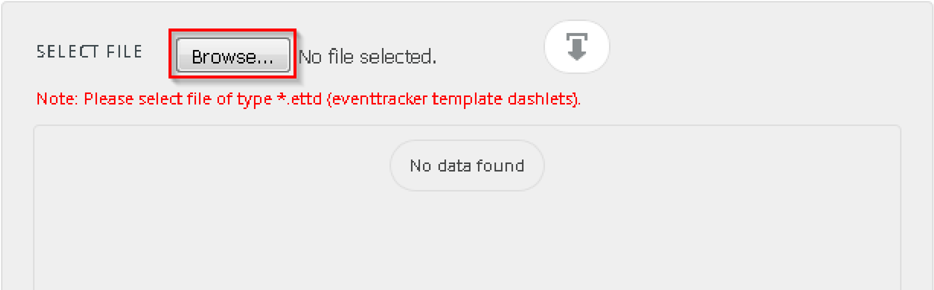
- Default
- A10 ADC
- Amazon Web Services
- Apache Web Server
- Barracuda Message Ar...
- Barracuda Spam Firew...
- Blue Coat Proxy
- Centrify Server Suit...
- Check Point
- Cisco ASA
- Cisco IOS
- Cisco IronPort ESA
- CISCO Ironport WSA

Group : All

TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE	□	EDIT
A10 ADC Authenticat...	A10 Application Delivery C...	A10 ADC	ETAdmin	9/29/2015 08:19:51 PM	☑	□	
A10 ADC Traffic	A10 Application Delivery C...	A10 ADC	ETAdmin	9/29/2015 08:19:51 PM	☑	□	
AWS VPC-Flow Report		Amazon Web S...	ETAdmin	9/29/2015 08:19:51 PM	☑	□	
Barracuda Message ...		Barracuda Me...	ETAdmin	9/29/2015 08:19:51 PM	☑	□	
Barracuda Spam fire...		Barracuda Spa...	ETAdmin	12/15/2015 08:02:47 ...	☑	□	
Barracuda Spam fire...		Barracuda Spa...	ETAdmin	12/15/2015 08:02:47 ...	☑	□	
Barracuda Spam fire...		Barracuda Spa...	ETAdmin	12/15/2015 08:02:47 ...	☑	□	

Figure 53

3. Click the **Browse** button.



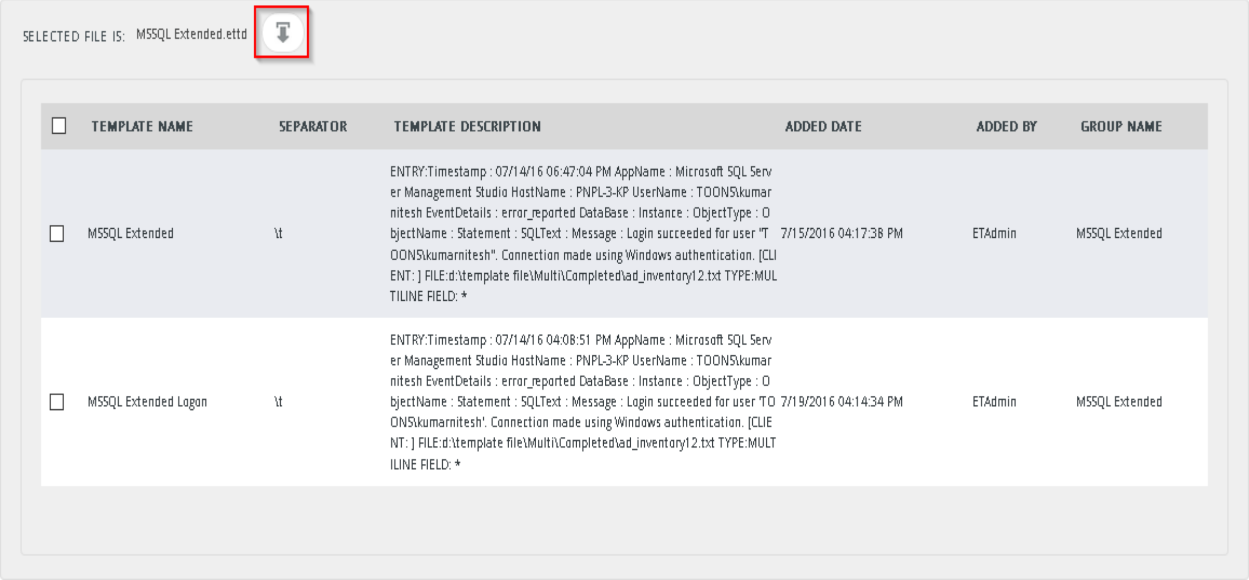
SELECT FILE Browse... No file selected.

Note: Please select file of type *.ettd (eventtracker template dashlets).

No data found

Figure 54

4. Locate **MSSQL Extended token template.ettd** or **MSSQL Audit token template.ettd** file, and then click the **Open** button.

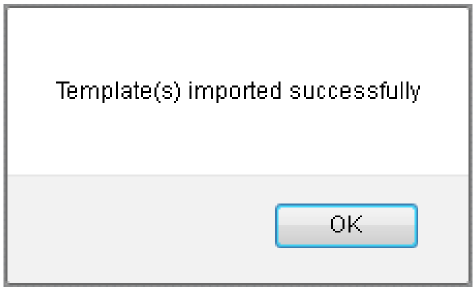


SELECTED FILE IS: MSSQL Extended.ettd ⤓

□	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
□	MSSQL Extended	\t	ENTRY:Timestamp : 07/14/16 06:47:04 PM AppName : Microsoft SQL Server Management Studio HostName : PNPL-3-KP UserName : TOONS\kumarnitesh EventDetails : error_reported DataBase : Instance : ObjectType : ObjectName : Statement : SQLText : Message : Login succeeded for user "TOONS\kumarnitesh". Connection made using Windows authentication. [CLIENT:] FILE:d:\template file\Multi\Completed\ad_inventory12.txt TYPE:MULTILINE FIELD: *	7/15/2016 04:17:38 PM	ETAdmin	MSSQL Extended
□	MSSQL Extended Logon	\t	ENTRY:Timestamp : 07/14/16 04:08:51 PM AppName : Microsoft SQL Server Management Studio HostName : PNPL-3-KP UserName : TOONS\kumarnitesh EventDetails : error_reported DataBase : Instance : ObjectType : ObjectName : Statement : SQLText : Message : Login succeeded for user 'TOONS\kumarnitesh'. Connection made using Windows authentication. [CLIENT:] FILE:d:\template file\Multi\Completed\ad_inventory12.txt TYPE:MULTILINE FIELD: *	7/19/2016 04:14:34 PM	ETAdmin	MSSQL Extended

Figure 55

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



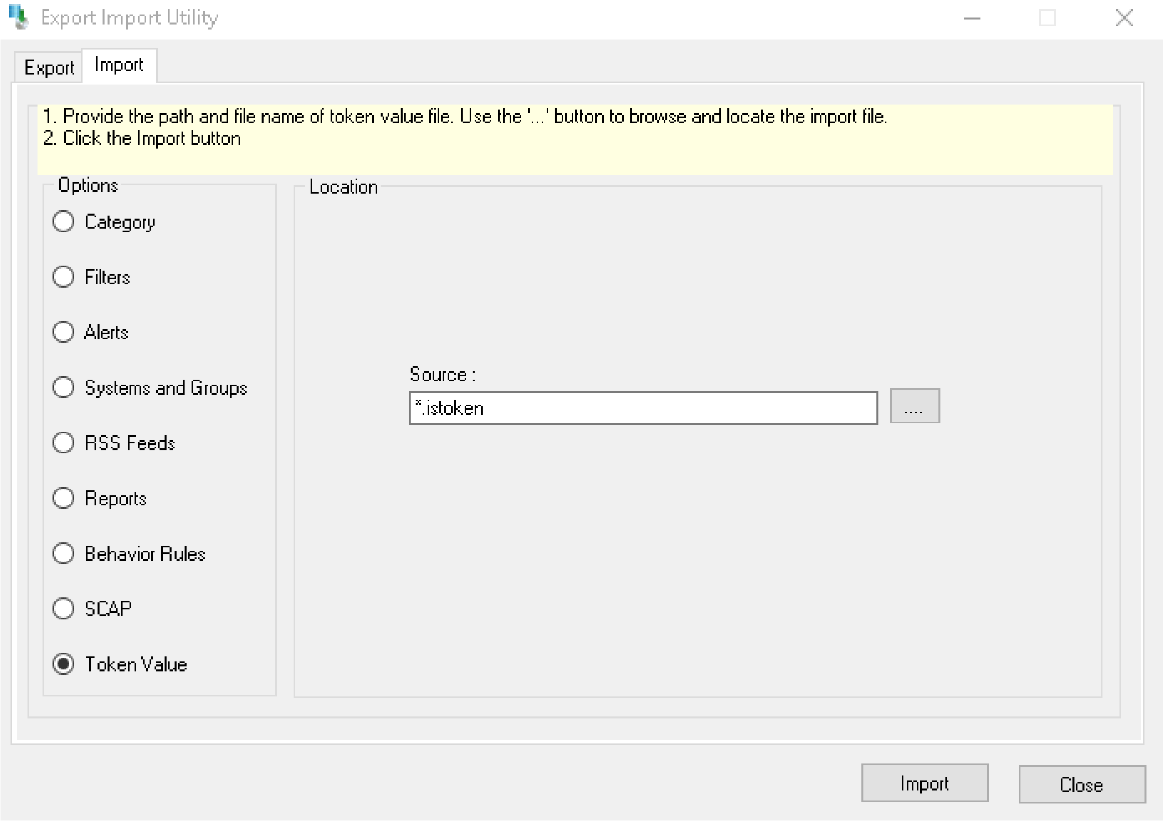
Template(s) imported successfully

Figure 56

6. Click on **OK** button.

Import Parsing Rules

1. Click **Token Value** option, and then click the **browse** … button.



1. Provide the path and file name of token value file. Use the '...' button to browse and locate the import file.
2. Click the Import button

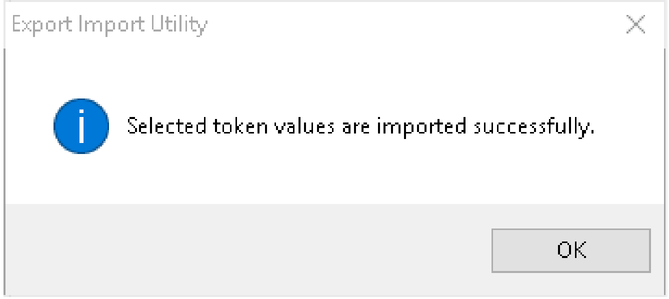
Options: ○ Category ○ Filters ○ Alerts ○ Systems and Groups ○ RSS Feeds ○ Reports ○ Behavior Rules ○ SCAP ● Token Value

Source : *.istoken

Figure 57

2. Locate **MSSQL Audit parsing rules.istoken** file, and then click the **Open** button.
3. To import the token value, click the **Import** button.

EventTracker displays success message.



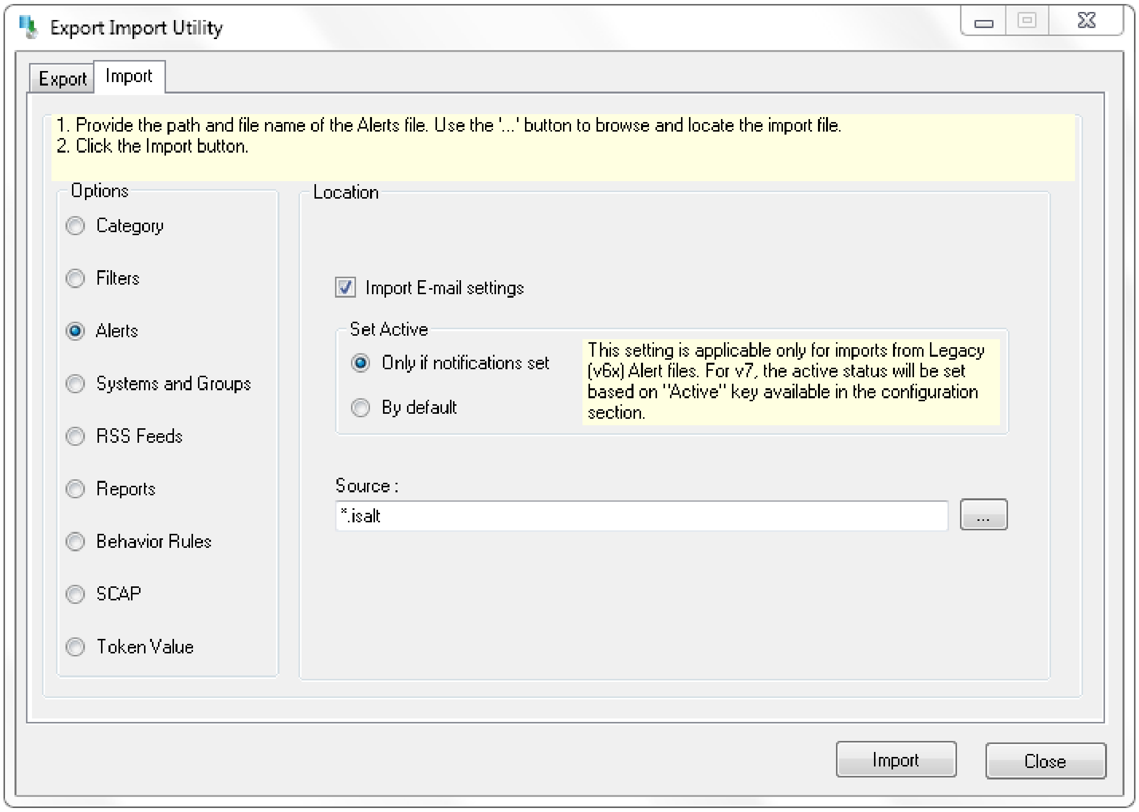
Selected token values are imported successfully.

Figure 58

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

Import Alerts

1. Click **Alerts** option, and then click the '**browse**' ... button.
2. Locate **MSSQL Audit alerts.isalt** file, and then click the **Open** button.



Export Import Utility

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

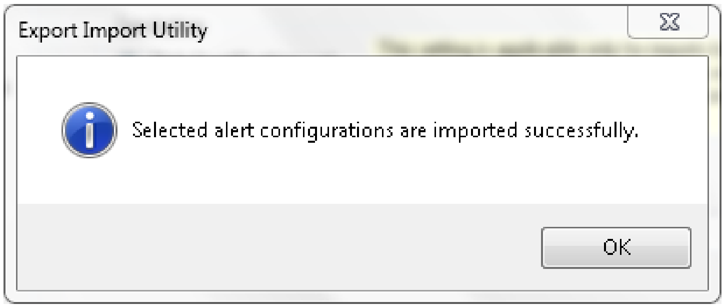
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 59

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

EventTracker displays success message.



Export Import Utility

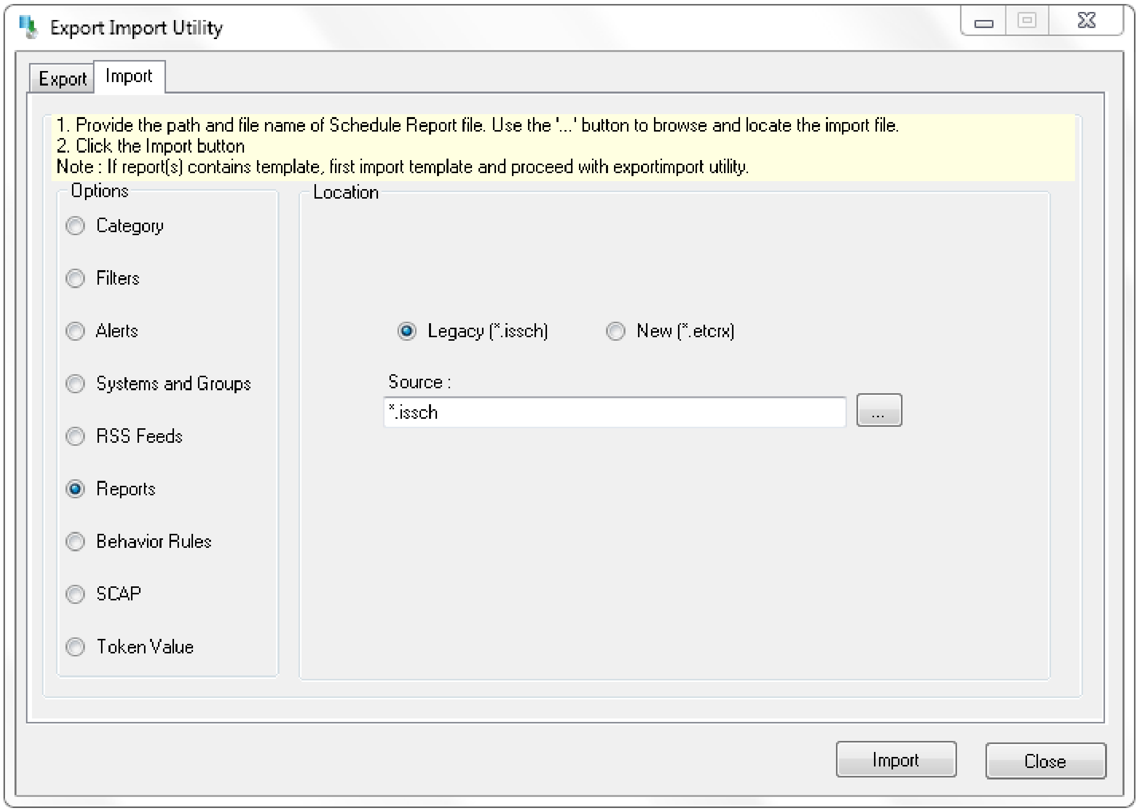
Selected alert configurations are imported successfully.

Figure 60

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

Import Flex Reports

1. Click **Reports** option, and then click the '**browse**' ... button.
2. Locate **MSSQL Extended reports.issch** or **MSSQL Auudit reports.issch** file, and then click the **Open** button.



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
● Reports
○ Behavior Rules
○ SCAP
○ Token Value

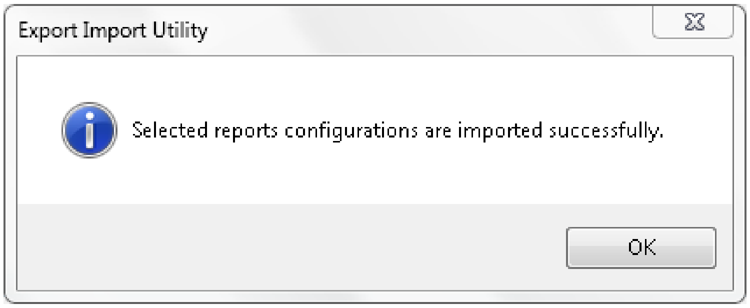
● Legacy (*.issch) ○ New (*.etcrx)

Source : *.issch

Figure 61

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

EventTracker displays success message.



Selected reports configurations are imported successfully.

Figure 62

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

Import Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on ⬇ '**Import**' icon.

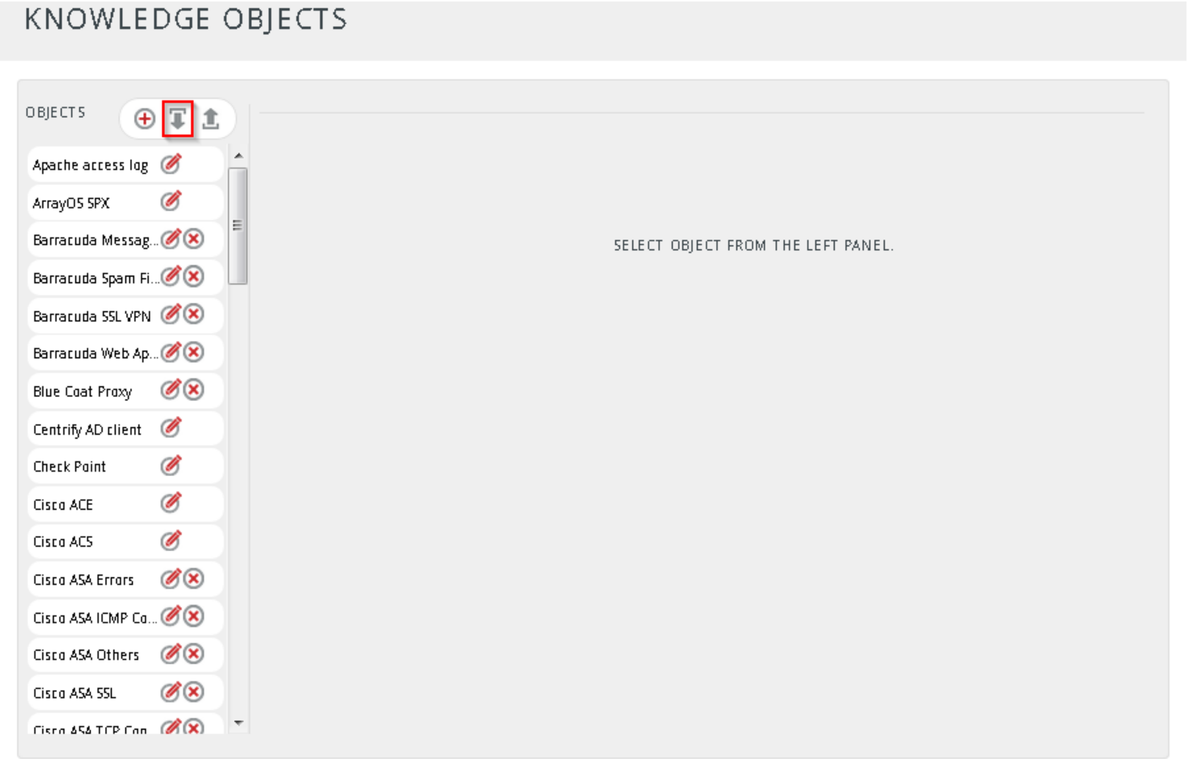


Figure 63

3. In **IMPORT** pane, click on **Browse** button.

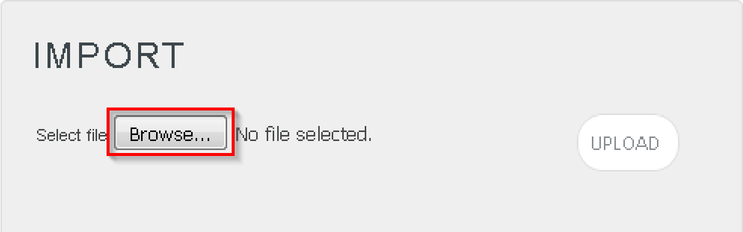
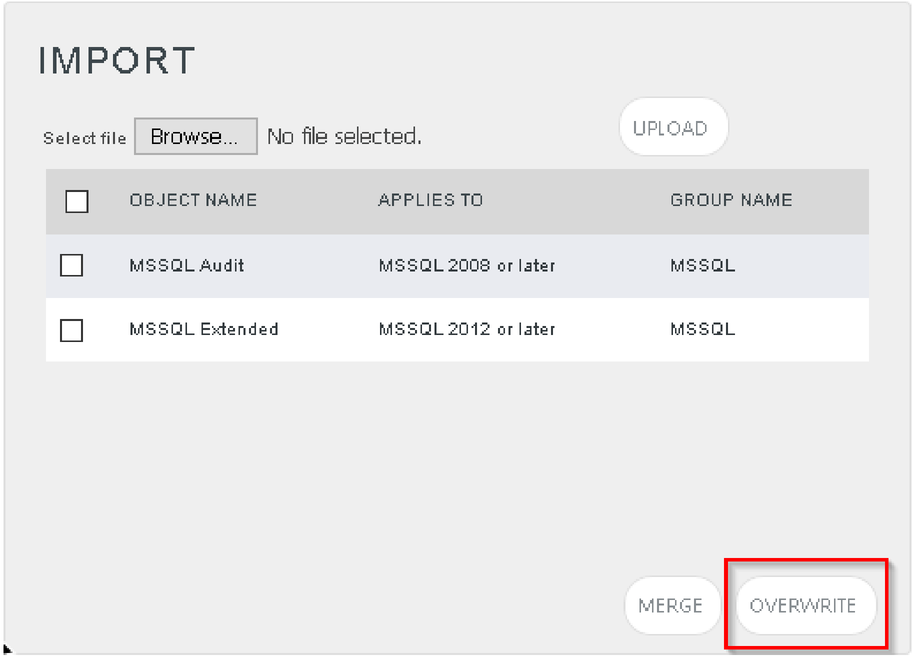


Figure 64

4. Locate **MSSQL Extended KO.etko** or **MSSQL Audit KO.etko** file, and then click the **UPLOAD** button.



No file selected.

□	OBJECT NAME	APPLIES TO	GROUP NAME
□	MSSQL Audit	MSSQL 2008 or later	MSSQL
□	MSSQL Extended	MSSQL 2012 or later	MSSQL

Figure 65

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

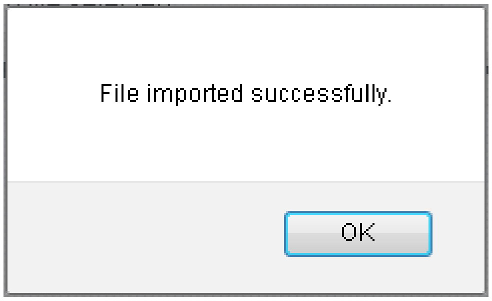

File imported successfully.

Figure 66

6. Click on **OK** button.

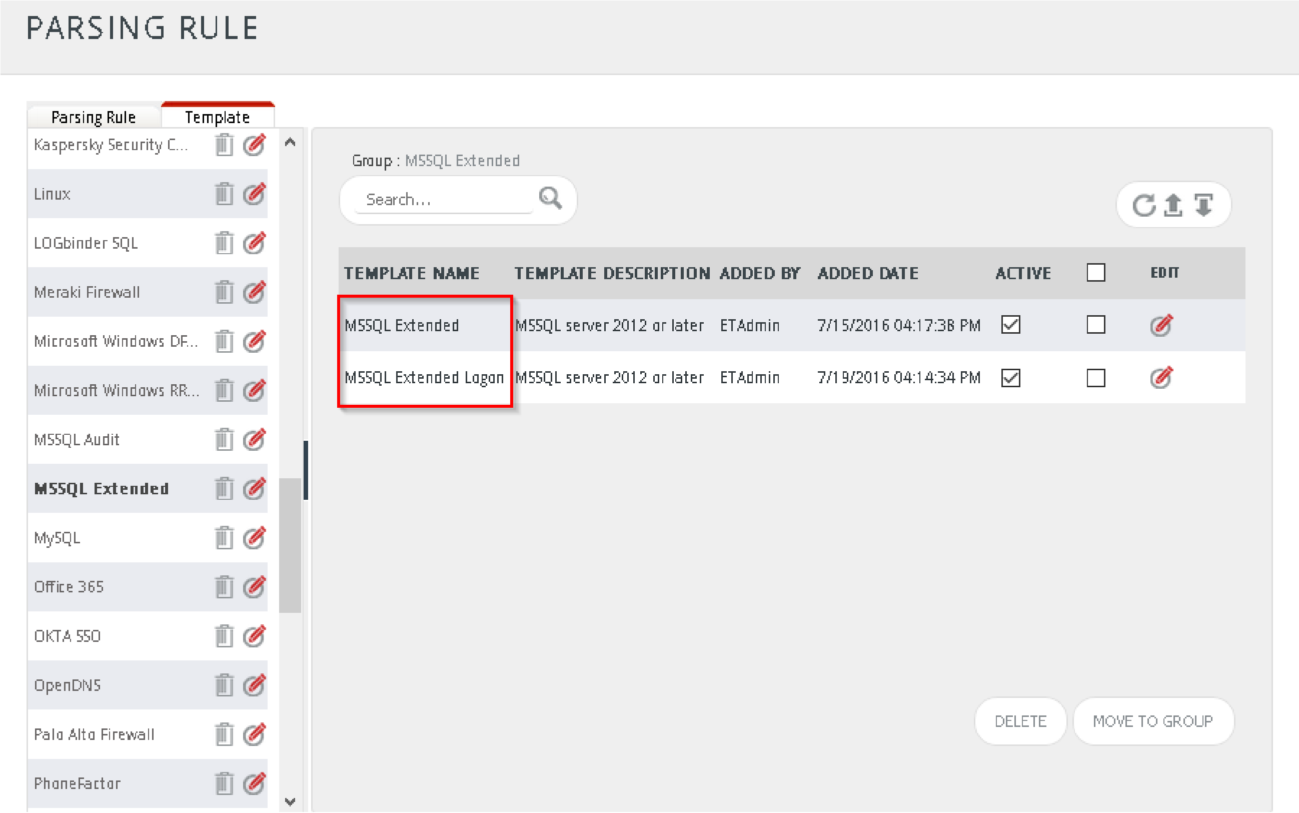
Verify Microsoft SQL SERVER KP

Token Templates

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing rule**.
3. Select **Template** tab.

4. In **Token Templates Groups Tree**, select **MSSQL Extended or MSSQL Audit** folder.

   Imported token templates are shown on the right pane.



Group : MSSQL Extended

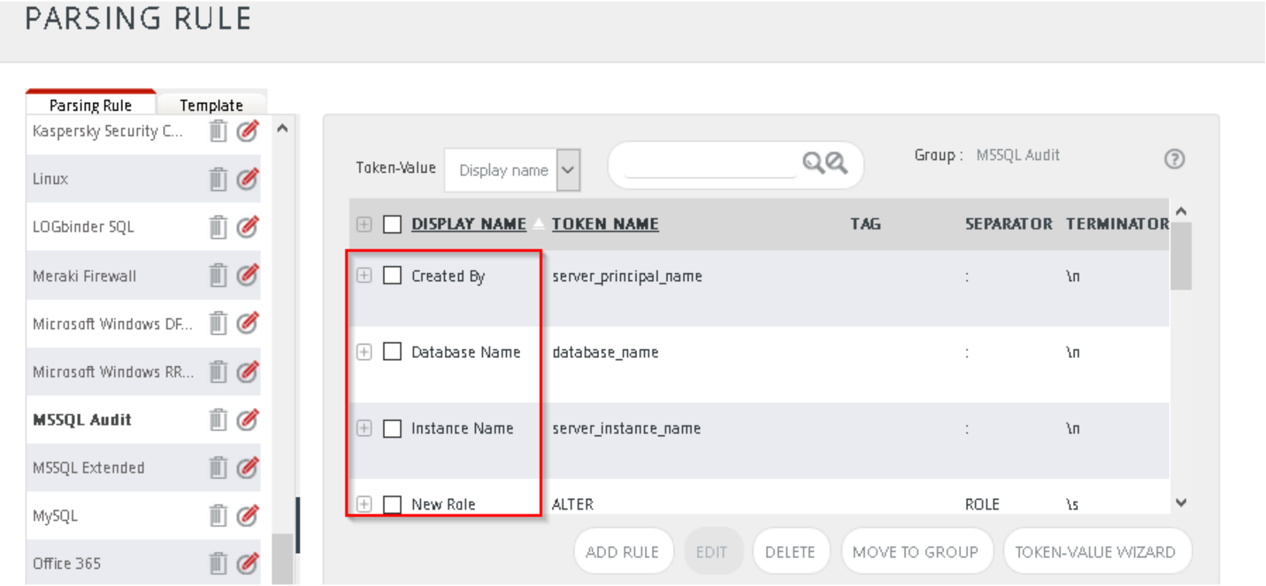
TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE	□	EDIT
MSSQL Extended	MSSQL server 2012 or later	ETAdmin	7/15/2016 04:17:38 PM	☑	□	
MSSQL Extended Logon	MSSQL server 2012 or later	ETAdmin	7/19/2016 04:14:34 PM	☑	□	

Figure 67

Parsing Rules

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing rule**.
3. Select **Parsing Rule** tab.
4. In **Parsing Rule Groups Tree**, select **MSSQL Audit** folder.

   Imported token templates are shown on the right pane.



PARSING RULE

- Kaspersky Security C...
- Linux
- LOGbinder SQL
- Meraki Firewall
- Microsoft Windows DF...
- Microsoft Windows RR...
- **MSSQL Audit**
- MSSQL Extended
- MySQL
- Office 365

Token-Value: Display name

Group : MSSQL Audit

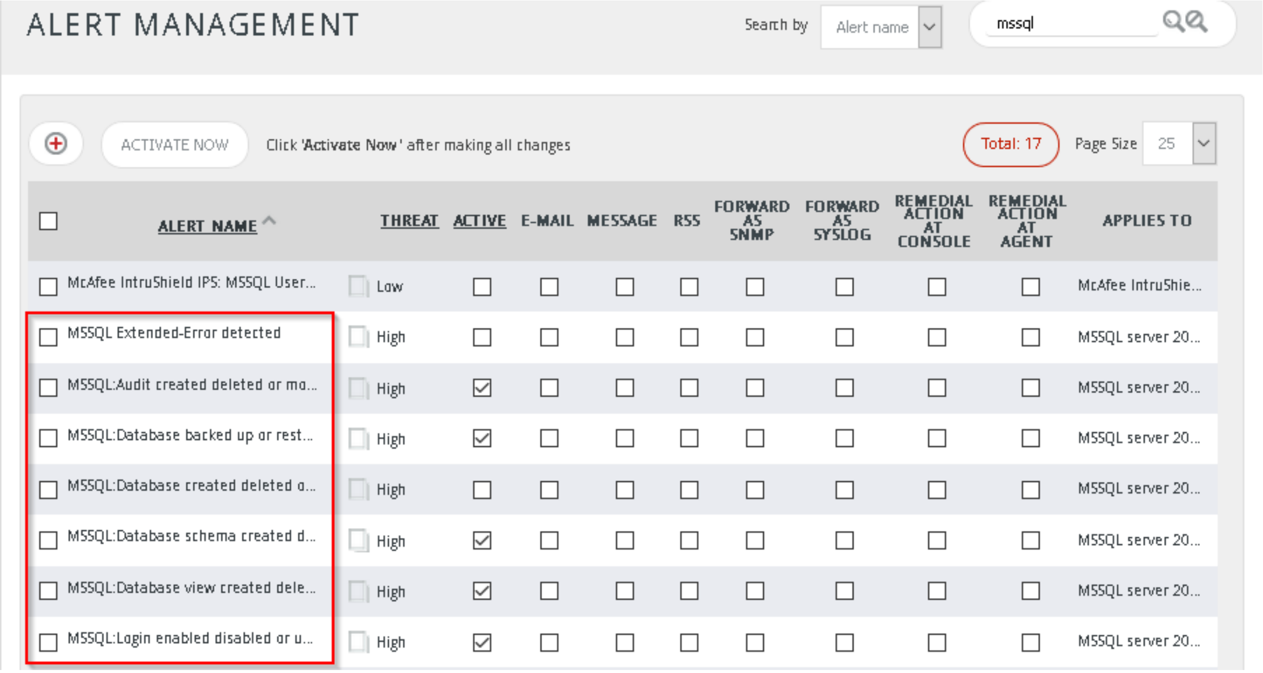
□	DISPLAY NAME	TOKEN NAME	TAG	SEPARATOR	TERMINATOR
□	Created By	server_principal_name		:	\n
□	Database Name	database_name		:	\n
□	Instance Name	server_instance_name		:	\n
□	New Role	ALTER		ROLE	\s

Figure 68

Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and select **Alerts**.
3. In **Search** field, type **‘MSSQL’**, and then click the 🔍 button.

Alert Management page will display all the imported Microsoft SQL SERVER alerts.



ALERT MANAGEMENT

Search by: Alert name — mssql

Click 'Activate Now' after making all changes

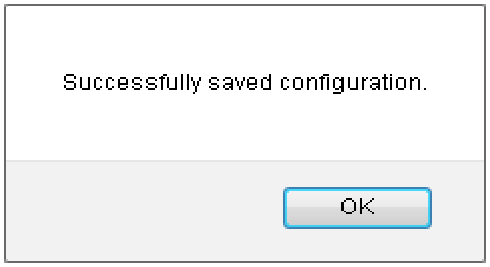
Total: 17   Page Size: 25

□	ALERT NAME	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
□	McAfee IntruShield IPS: MSSQL User...	Low	□	□	□	□	□	□	□	□	McAfee IntruShie...
□	MSSQL Extended-Error detected	High	□	□	□	□	□	□	□	□	MSSQL server 20...
□	MSSQL:Audit created deleted or mo...	High	☑	□	□	□	□	□	□	□	MSSQL server 20...
□	MSSQL:Database backed up or rest...	High	☑	□	□	□	□	□	□	□	MSSQL server 20...
□	MSSQL:Database created deleted o...	High	□	□	□	□	□	□	□	□	MSSQL server 20...
□	MSSQL:Database schema created d...	High	☑	□	□	□	□	□	□	□	MSSQL server 20...
□	MSSQL:Database view created dele...	High	☑	□	□	□	□	□	□	□	MSSQL server 20...
□	MSSQL:Login enabled disabled or u...	High	☑	□	□	□	□	□	□	□	MSSQL server 20...

Figure 69

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

   EventTracker displays message box.



Successfully saved configuration.

Figure 70

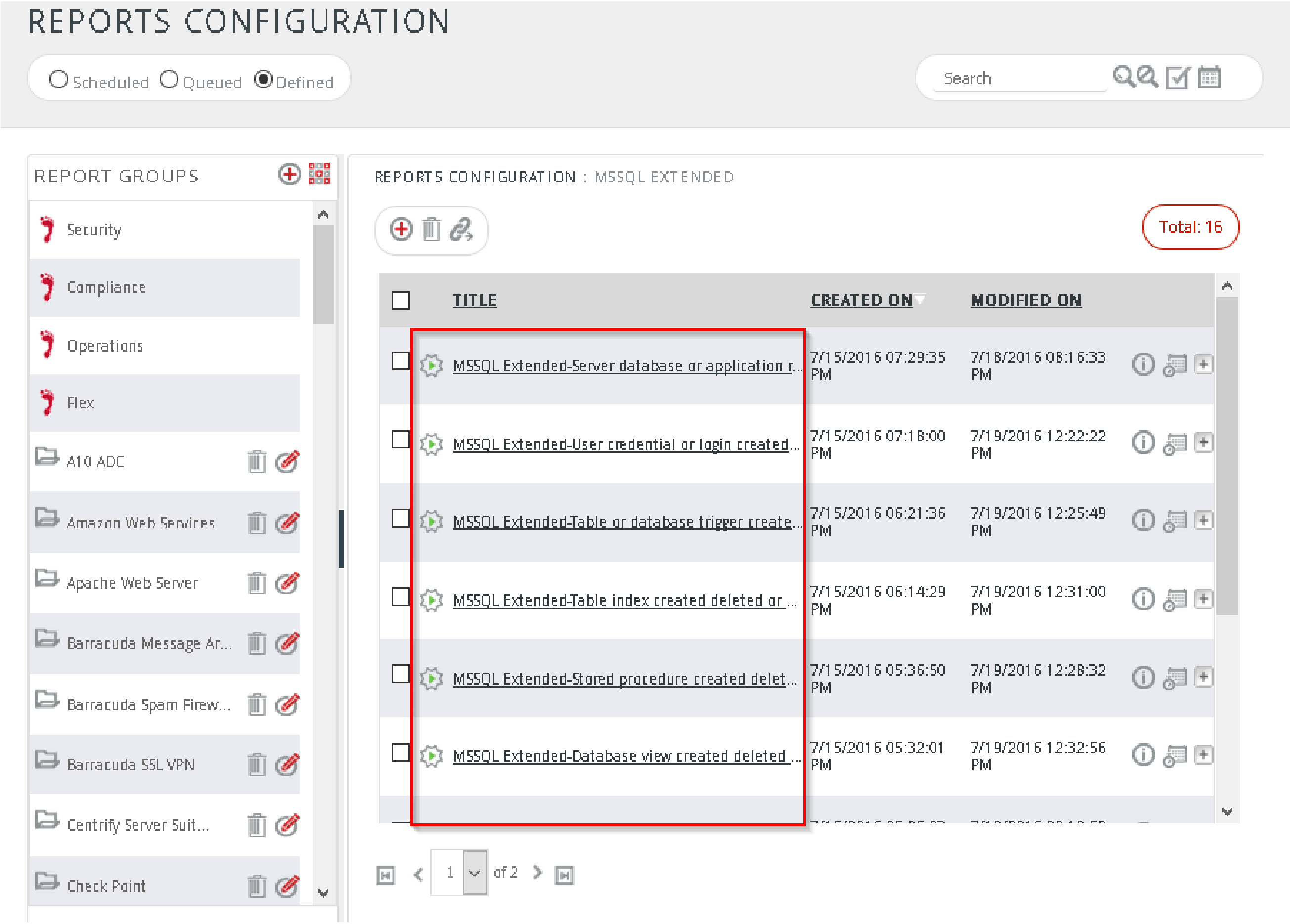
5. Click **OK**, and then click the **Activate Now** button.

NOTE: Please specify appropriate **systems** in **alert configuration** for better performance.

Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu and select **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree**, select **MSSQL Audit** or **MSSQL Extended group** folder.

Imported reports are displayed on the right pane.



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

Search

REPORT GROUPS

- Security
- Compliance
- Operations
- Flex
- A10 ADC
- Amazon Web Services
- Apache Web Server
- Barracuda Message Ar...
- Barracuda Spam Firew...
- Barracuda SSL VPN
- Centrify Server Suit...
- Check Point

REPORTS CONFIGURATION : MSSQL EXTENDED

Total: 16

□	TITLE	CREATED ON	MODIFIED ON
□	MSSQL Extended-Server database or application r...	7/15/2016 07:29:35 PM	7/18/2016 08:16:33 PM
□	MSSQL Extended-User credential or login created...	7/15/2016 07:18:00 PM	7/19/2016 12:22:22 PM
□	MSSQL Extended-Table or database trigger create...	7/15/2016 06:21:36 PM	7/19/2016 12:25:49 PM
□	MSSQL Extended-Table index created deleted or ...	7/15/2016 06:14:29 PM	7/19/2016 12:31:00 PM
□	MSSQL Extended-Stored procedure created delet...	7/15/2016 05:36:50 PM	7/19/2016 12:28:32 PM
□	MSSQL Extended-Database view created deleted ...	7/15/2016 05:32:01 PM	7/19/2016 12:32:56 PM

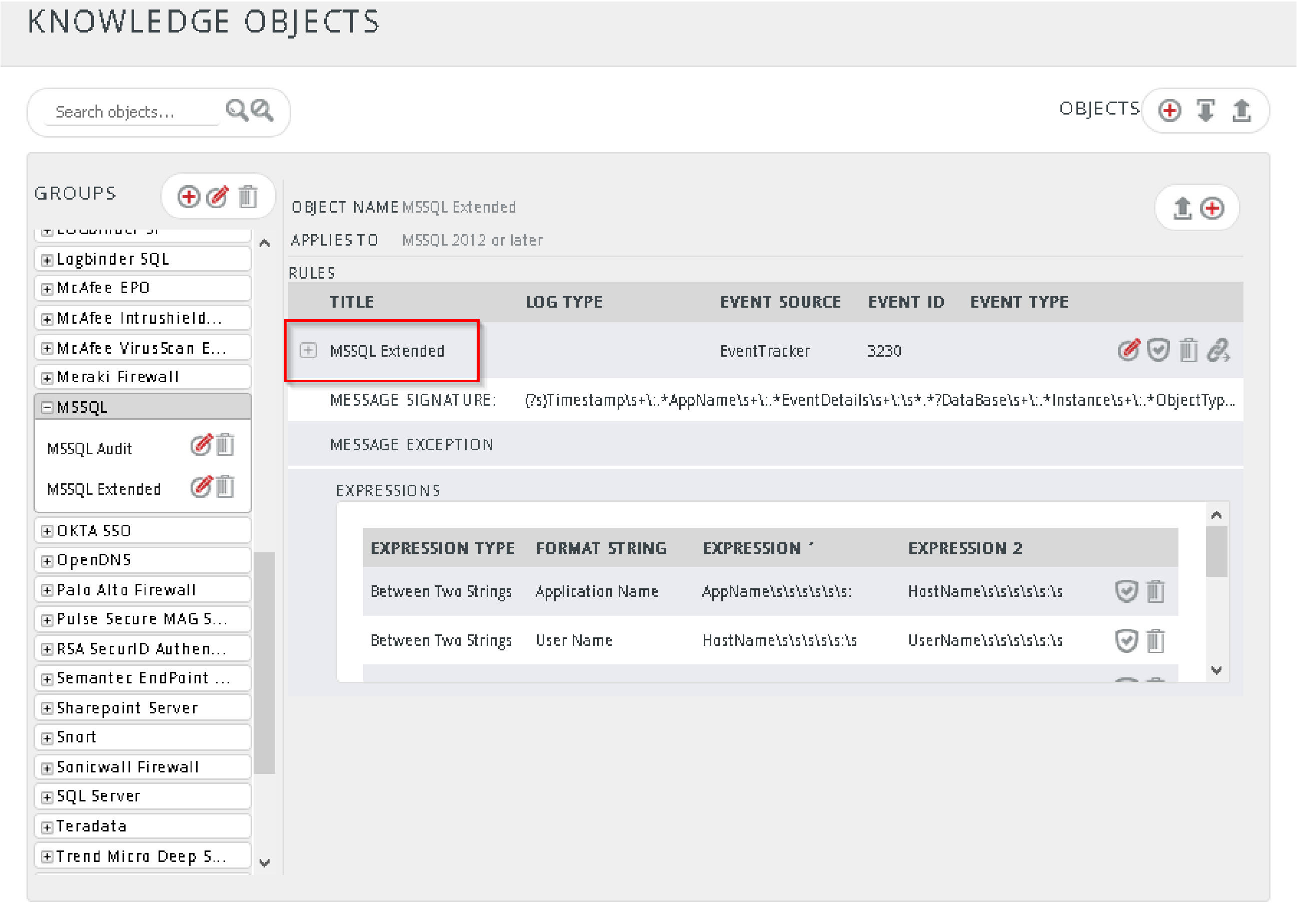
1 of 2

Figure 71

Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Objects.**
3. In **Group Tree**, select **MSSQL** folder and navigate to **MSSQL Audit** or **MSSQL Extended** object name.

   Imported **Microsoft SQL SERVER** objects are shown on the right pane.



OBJECT NAME MSSQL Extended

APPLIES TO MSSQL 2012 or later

RULES

TITLE	LOG TYPE	EVENT SOURCE	EVENT ID	EVENT TYPE
MSSQL Extended		EventTracker	3230	

MESSAGE SIGNATURE: (?s)Timestamp\s+\:.*AppName\s+\:.*EventDetails\s+\:\s*.*?DataBase\s+\:.*Instance\s+\:.*ObjectTyp...

MESSAGE EXCEPTION

EXPRESSIONS

EXPRESSION TYPE	FORMAT STRING	EXPRESSION ˊ	EXPRESSION 2
Between Two Strings	Application Name	AppName\s\s\s\s\s\s:	HostName\s\s\s\s\s:\s
Between Two Strings	User Name	HostName\s\s\s\s\s:\s	UserName\s\s\s\s\s:\s

Figure 72

Configure Log Filters

SQL events are very noisy. So, without application of efficient filtering, it is very difficult to retrieve relevant information from high volume of audit events generated. Although filter criteria have been provided in audit reports and the extended session configuration. Below mentioned steps aid in creation of custom filter criteria consistent with requirement.

Audit Specifications

As all events generated by audit specification do not have inbuilt filter criteria, filters can only be created in Event Tracker. Filter criteria for reports can be created as shown below:

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

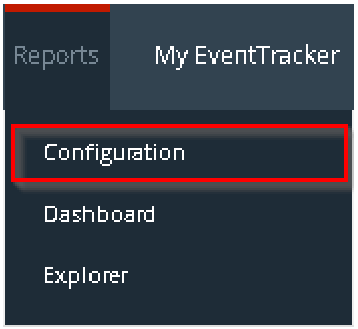
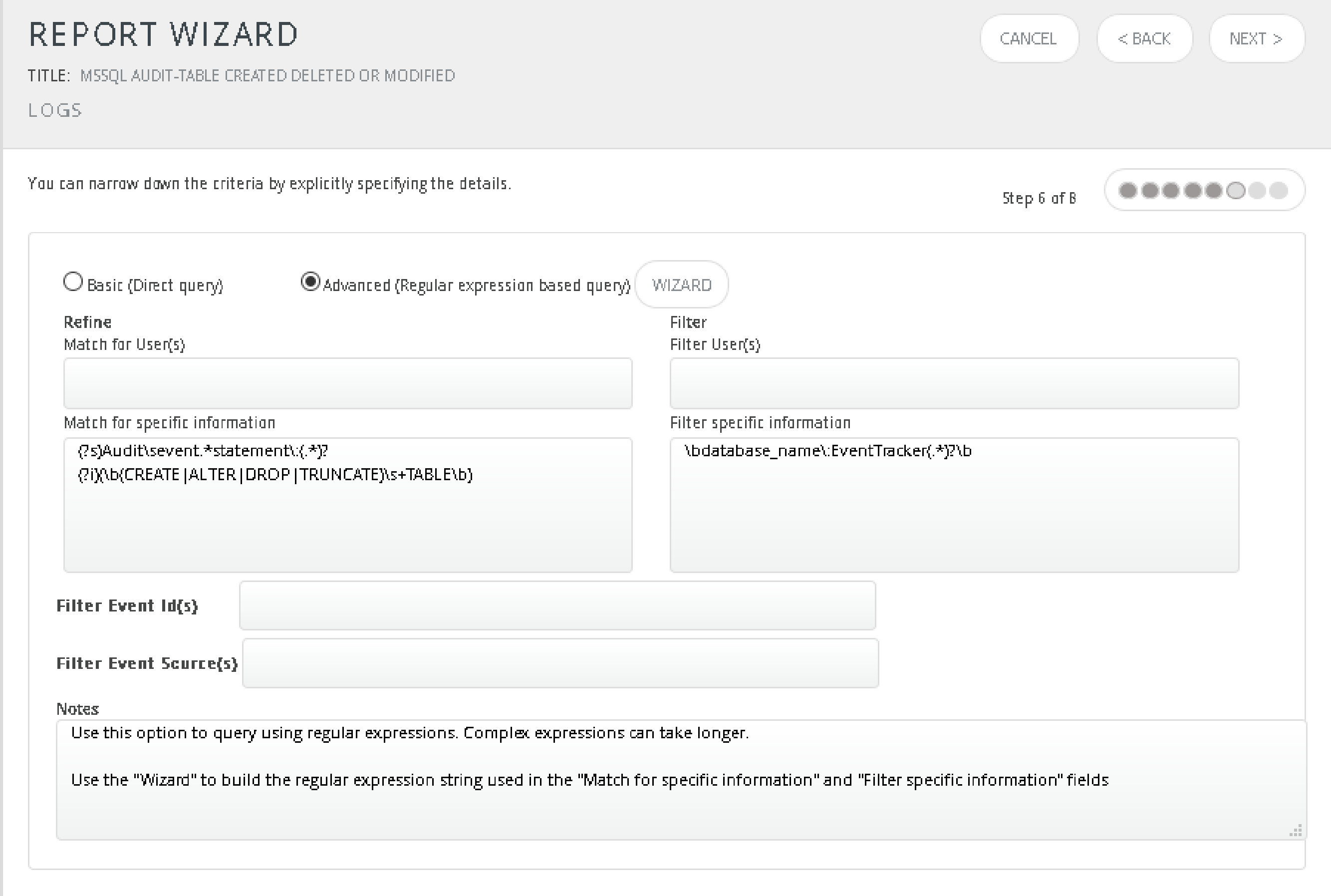


Figure 73

2. Navigate to **Reports>Configuration>Defined or Scheduled**.
3. Click any MSSQL report to open **report wizard**.
4. Click **Next** and navigate to Matching criteria page.



TITLE: MSSQL AUDIT-TABLE CREATED DELETED OR MODIFIED

You can narrow down the criteria by explicitly specifying the details.

○ Basic (Direct query) ● Advanced (Regular expression based query)

Refine

Match for User(s):

Match for specific information:

```
(?s)Audit\sevent.*statement\:(.*)?
(?i)(\b(CREATE|ALTER|DROP|TRUNCATE)\s+TABLE\b)
```

Filter

Filter User(s):

Filter specific information:

```
\bdatabase_name\:EventTracker(.*)?\b
```

Filter Event Id(s):

Filter Event Source(s):

Notes

Use this option to query using regular expressions. Complex expressions can take longer.

Use the "Wizard" to build the regular expression string used in the "Match for specific information" and "Filter specific information" fields

Figure 74

5. For example,
   - If one requires to filter events from databases named “**JunkDATA**” and “**EventTracker**”. The new filter criteria would be,

```
\bdatabase_name\:((EventTracker(.*)?)|JunkDATA)\b
```

- Additionally, if one requires filtering events from a user named” **Bob**”. The filter criteria can be further modified as,

```
\bdatabase_name\:((EventTracker(.*)?)|JunkDATA)\b|\bserver_principal_name\:.*?(?i)bob\b
```

6. Click **Next**, navigate to the final page and **SAVE**.

Extended events

Extended events have inbuilt filter criteria. Thus, to improve EventTracker performance, events can be filtered at the source. Steps below explain the same.

i. Open SQL Management Studio with appropriate credentials.
ii. Open object explorer and navigate to **Server>Management>Extended Events>Sessions>ObjectChange**.

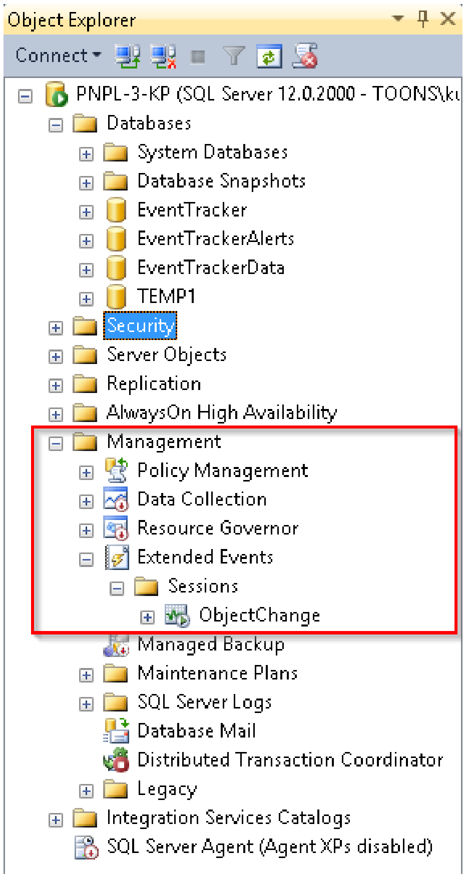
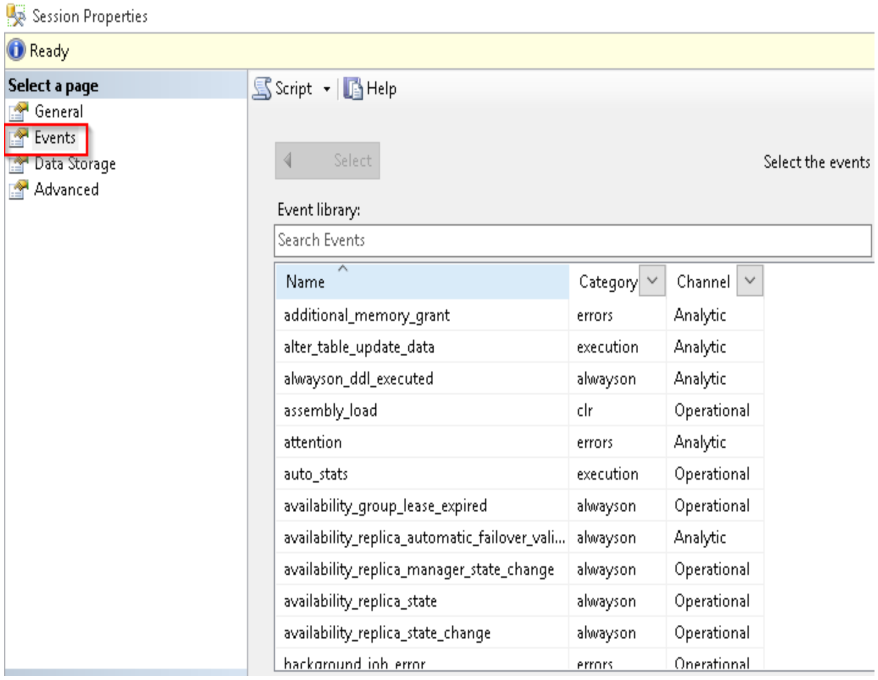


Figure 75

iii. Right-click session named **ObjectChange**, select **Properties**.

iv. In **Session properties** window, navigate to **Events>Configure**.



Session Properties

Ready

Select a page
- General
- Events
- Data Storage
- Advanced

Script ▾ | Help

Select

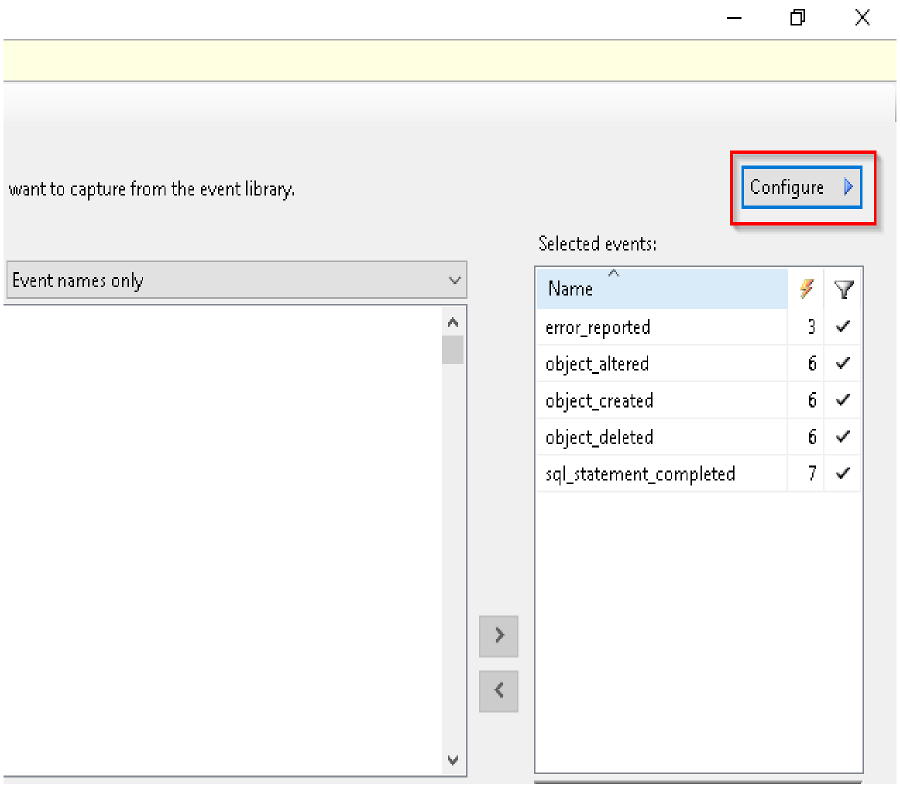
Select the events

Event library:

Search Events

Name	Category	Channel
additional_memory_grant	errors	Analytic
alter_table_update_data	execution	Analytic
alwayson_ddl_executed	alwayson	Analytic
assembly_load	clr	Operational
attention	errors	Analytic
auto_stats	execution	Operational
availability_group_lease_expired	alwayson	Operational
availability_replica_automatic_failover_vali...	alwayson	Analytic
availability_replica_manager_state_change	alwayson	Operational
availability_replica_state	alwayson	Operational
availability_replica_state_change	alwayson	Operational
background_job_error	errors	Operational

Figure 76



want to capture from the event library.

Configure

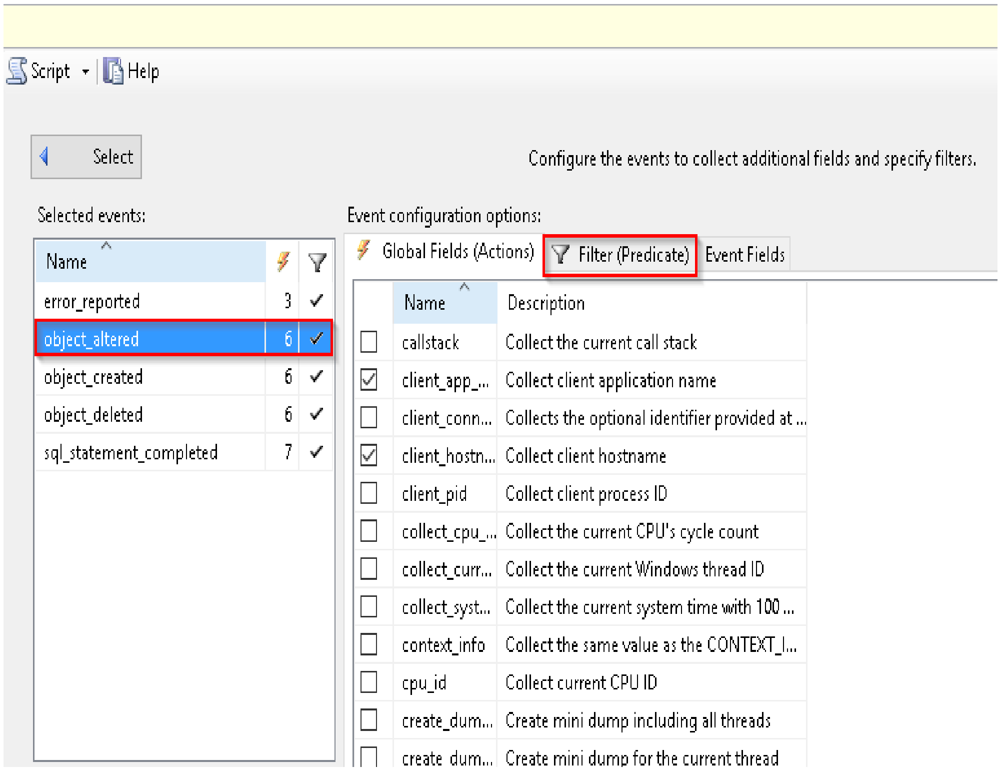
Event names only

Selected events:

Name	⚡	▽
error_reported	3	✓
object_altered	6	✓
object_created	6	✓
object_deleted	6	✓
sql_statement_completed	7	✓

Figure 77

2. In next window, select any **event type** and click **Filter(Predicate)** tab.



Configure the events to collect additional fields and specify filters.

Selected events:

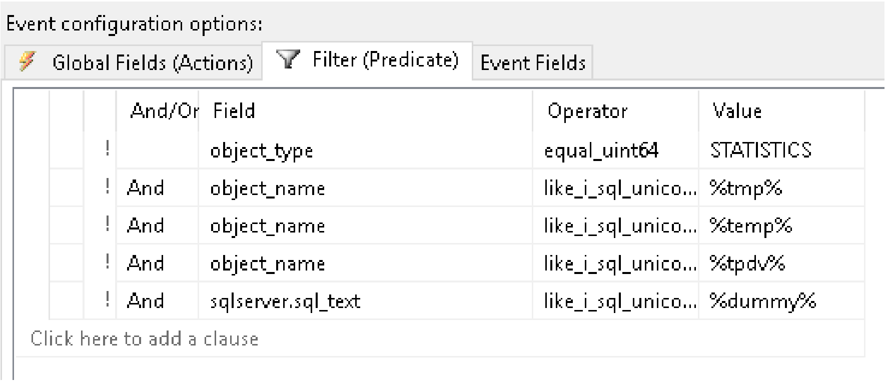
Name	⚡	Filter
error_reported	3	✓
object_altered	6	✓
object_created	6	✓
object_deleted	6	✓
sql_statement_completed	7	✓

Event configuration options:

	Name	Description
□	callstack	Collect the current call stack
☑	client_app_...	Collect client application name
□	client_conn...	Collects the optional identifier provided at ...
☑	client_hostn...	Collect client hostname
□	client_pid	Collect client process ID
□	collect_cpu_...	Collect the current CPU's cycle count
□	collect_curr...	Collect the current Windows thread ID
□	collect_syst...	Collect the current system time with 100 ...
□	context_info	Collect the same value as the CONTEXT_I...
□	cpu_id	Collect current CPU ID
□	create_dum...	Create mini dump including all threads
□	create_dum...	Create mini dump for the current thread

Figure 78

3. Filter will have in-built criteria, as shown:


Event configuration options:

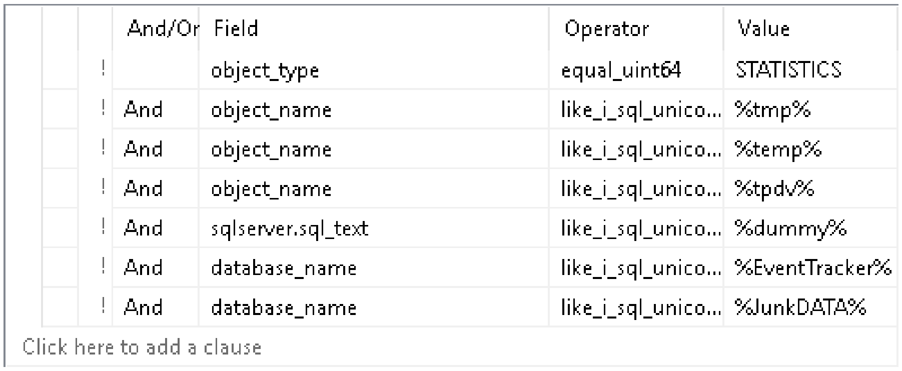
	And/Or	Field	Operator	Value
!		object_type	equal_uint64	STATISTICS
!	And	object_name	like_i_sql_unico...	%tmp%
!	And	object_name	like_i_sql_unico...	%temp%
!	And	object_name	like_i_sql_unico...	%tpdv%
!	And	sqlserver.sql_text	like_i_sql_unico...	%dummy%

Click here to add a clause

Figure 79

4. For example,

   i. If one needs to filter events from databases named “**JunkDATA**” and “**EventTracker**”, toggle filter columns to create criteria as shown:

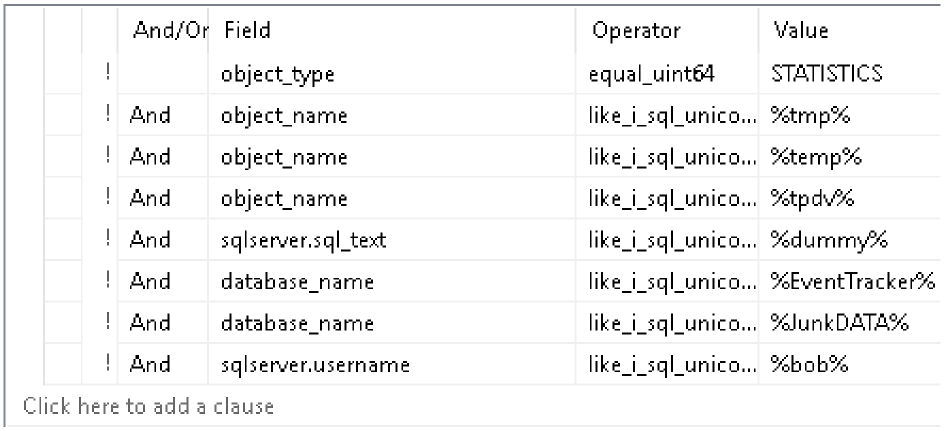


	And/Or	Field	Operator	Value
!		object_type	equal_uint64	STATISTICS
!	And	object_name	like_i_sql_unico...	%tmp%
!	And	object_name	like_i_sql_unico...	%temp%
!	And	object_name	like_i_sql_unico...	%tpdv%
!	And	sqlserver.sql_text	like_i_sql_unico...	%dummy%
!	And	database_name	like_i_sql_unico...	%EventTracker%
!	And	database_name	like_i_sql_unico...	%JunkDATA%

Click here to add a clause

Figure 80

ii. Additionally, if one requires to filter events from an user named **"Bob"**, toggle filter columns to create criteria as shown:



	And/Or	Field	Operator	Value
!		object_type	equal_uint64	STATISTICS
!	And	object_name	like_i_sql_unico...	%tmp%
!	And	object_name	like_i_sql_unico...	%temp%
!	And	object_name	like_i_sql_unico...	%tpdv%
!	And	sqlserver.sql_text	like_i_sql_unico...	%dummy%
!	And	database_name	like_i_sql_unico...	%EventTracker%
!	And	database_name	like_i_sql_unico...	%JunkDATA%
!	And	sqlserver.username	like_i_sql_unico...	%bob%

Click here to add a clause

Figure 81

5. Click **OK** to save the changes.

Create Dashboards in EventTracker

Prerequisites

1. **EventTracker 8.0 or later** must be installed.

Schedule Reports

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

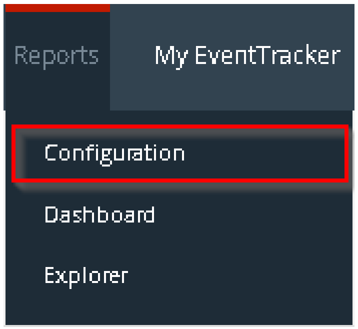
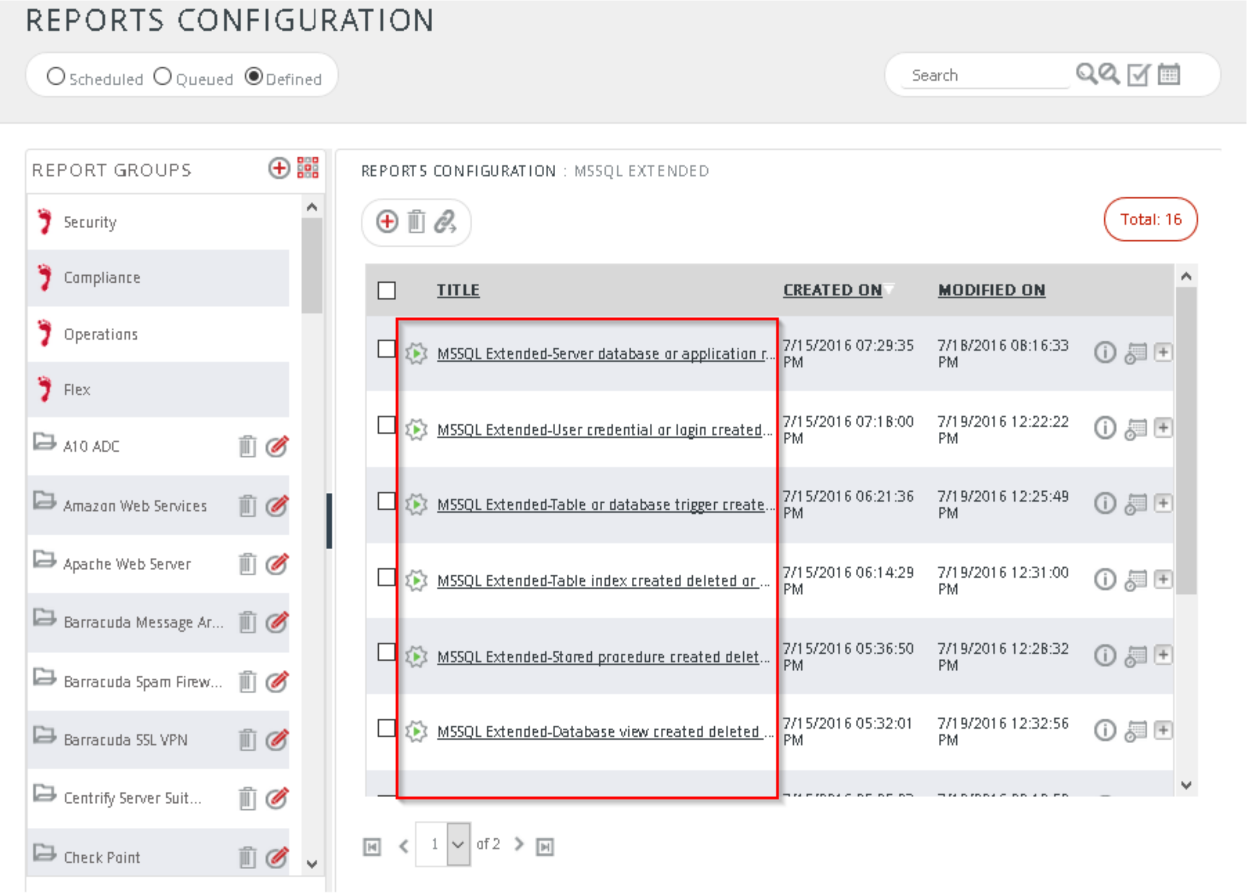


Figure 82

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

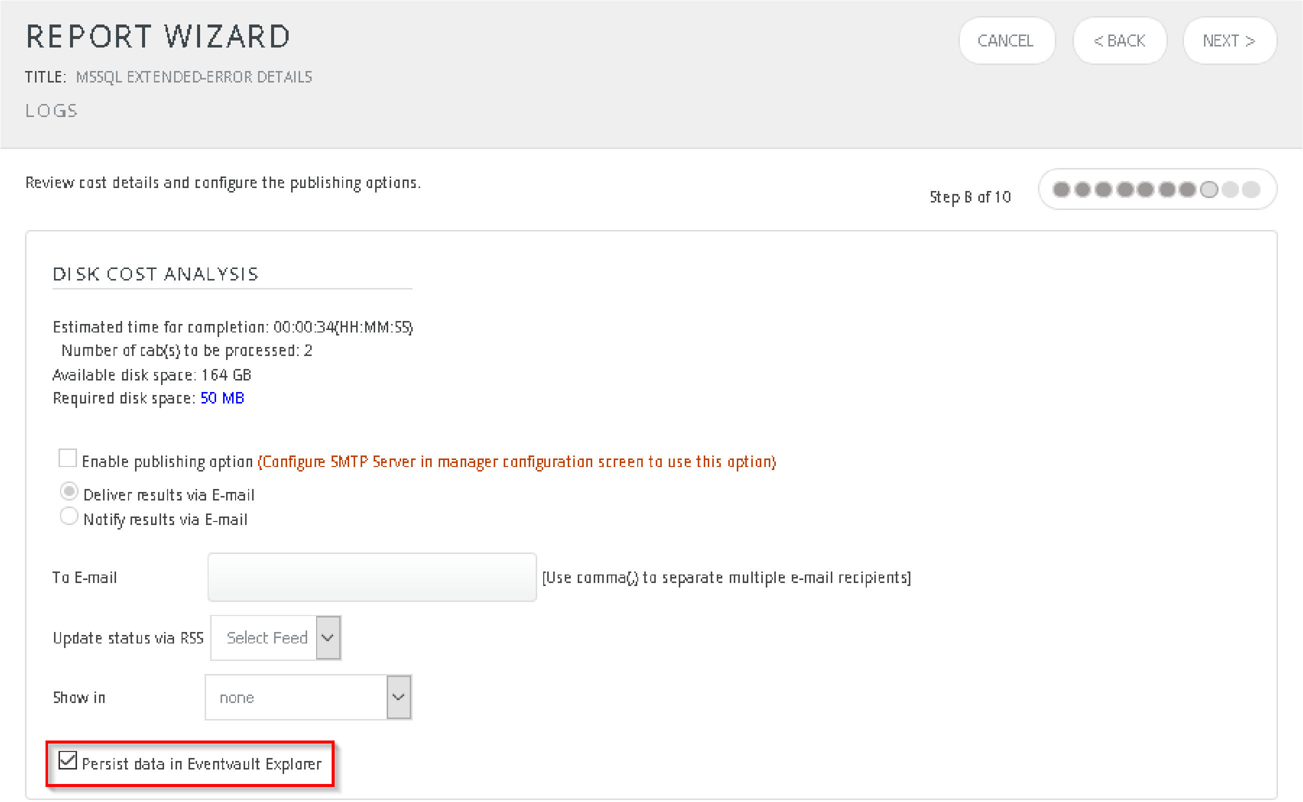


TITLE	CREATED ON	MODIFIED ON
MSSQL Extended-Server database or application r...	7/15/2016 07:29:35 PM	7/18/2016 08:16:33 PM
MSSQL Extended-User credential or login created...	7/15/2016 07:18:00 PM	7/19/2016 12:22:22 PM
MSSQL Extended-Table or database trigger create...	7/15/2016 06:21:36 PM	7/19/2016 12:25:49 PM
MSSQL Extended-Table index created deleted or ...	7/15/2016 06:14:29 PM	7/19/2016 12:31:00 PM
MSSQL Extended-Stored procedure created delet...	7/15/2016 05:36:50 PM	7/19/2016 12:28:32 PM
MSSQL Extended-Database view created deleted ...	7/15/2016 05:32:01 PM	7/19/2016 12:32:56 PM

Figure 83

3. Select **'MSSQL Extended'** or **'MSSQL Audit'** in report groups. Check **Defined** dialog box.

4. Click on '**schedule**' to plan a report for later execution.



REPORT WIZARD

TITLE: MSSQL EXTENDED-ERROR DETAILS

LOGS

Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:34(HH:MM:SS)
Number of cab(s) to be processed: 2
Available disk space: 164 GB
Required disk space: 50 MB

□ Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)

● Deliver results via E-mail
○ Notify results via E-mail

To E-mail [Use comma(,) to separate multiple e-mail recipients]

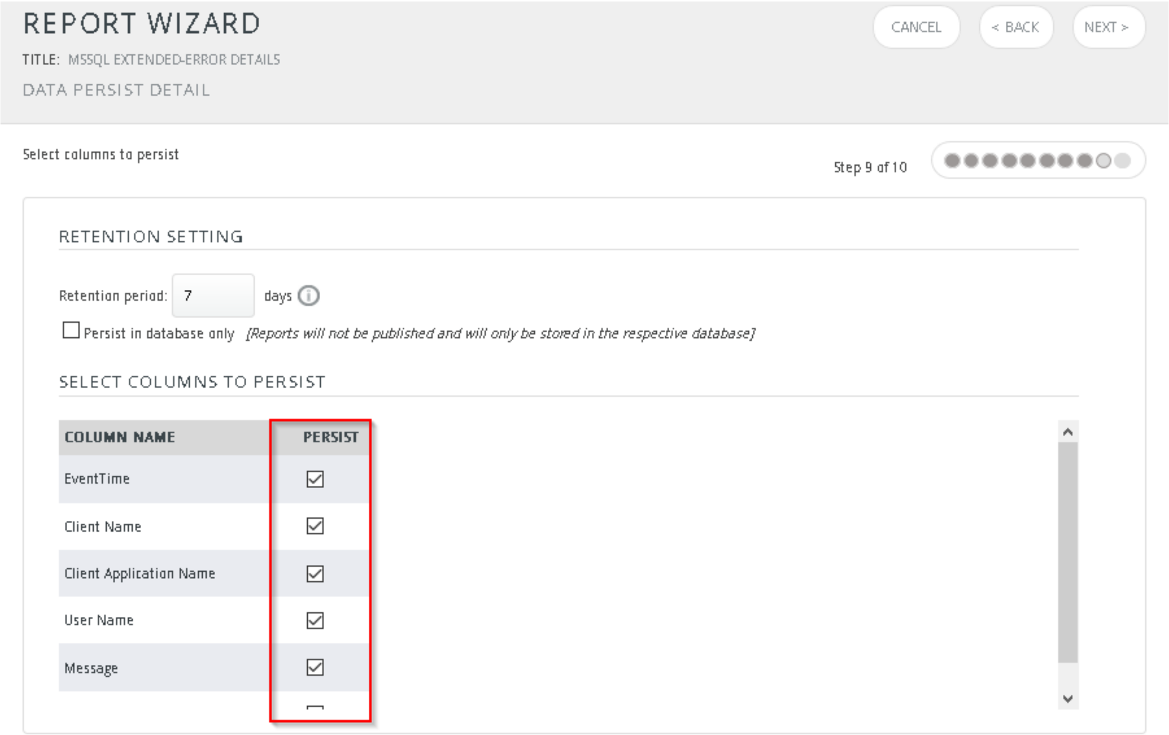
Update status via RSS: Select Feed

Show in: none

☑ Persist data in Eventvault Explorer

Figure 84

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in EventVault Explorer** box.



REPORT WIZARD

TITLE: MSSQL EXTENDED-ERROR DETAILS

DATA PERSIST DETAIL

Select columns to persist

Step 9 of 10

RETENTION SETTING

Retention period: 7 days

□ Persist in database only *[Reports will not be published and will only be stored in the respective database]*

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
EventTime	☑
Client Name	☑
Client Application Name	☑
User Name	☑
Message	☑

Figure 85

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

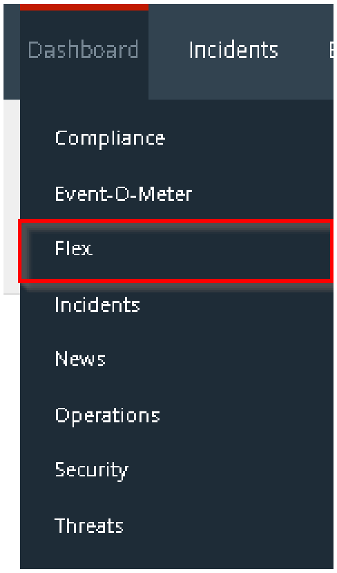


Figure 86

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

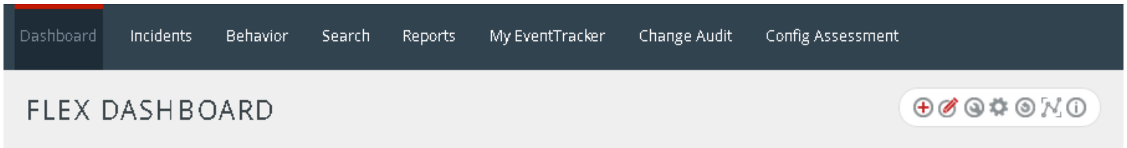
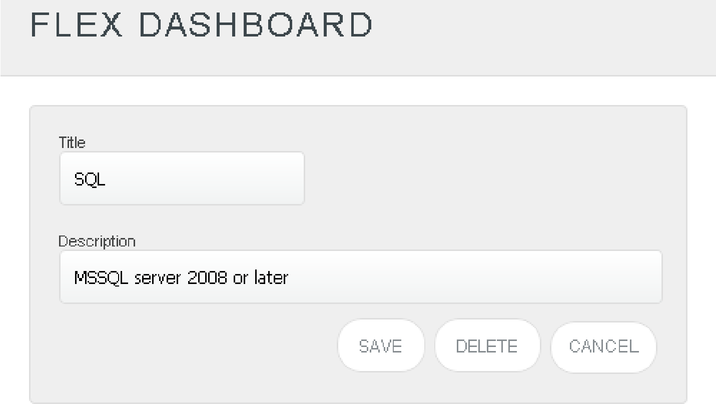


Figure 87

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



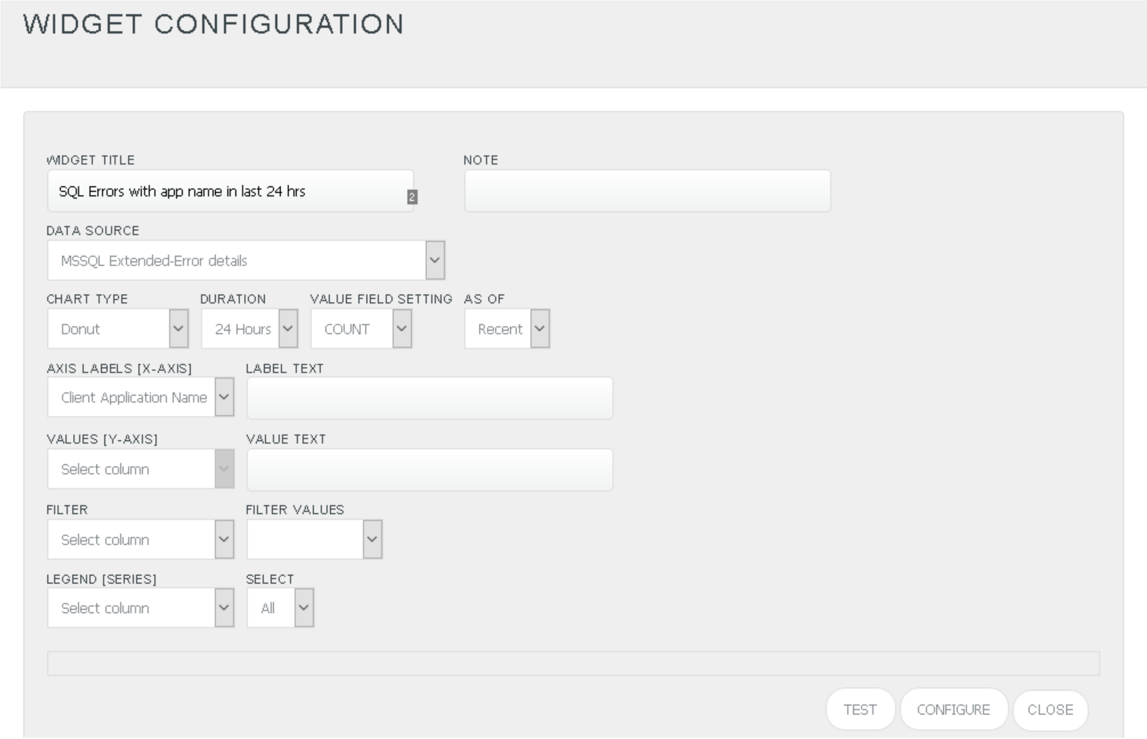
Title
SQL

Description
MSSQL server 2008 or later

Figure 88

4. Fill appropriate title and description and click **Save** button.
5. Click ⚙ to configure a new flex dashlet.

Widget configuration pane is shown.



WIDGET CONFIGURATION

WIDGET TITLE: SQL Errors with app name in last 24 hrs

NOTE:

DATA SOURCE: MSSQL Extended-Error details

CHART TYPE: Donut

DURATION: 24 Hours

VALUE FIELD SETTING: COUNT

AS OF: Recent

AXIS LABELS [X-AXIS]: Client Application Name

LABEL TEXT:

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Select column

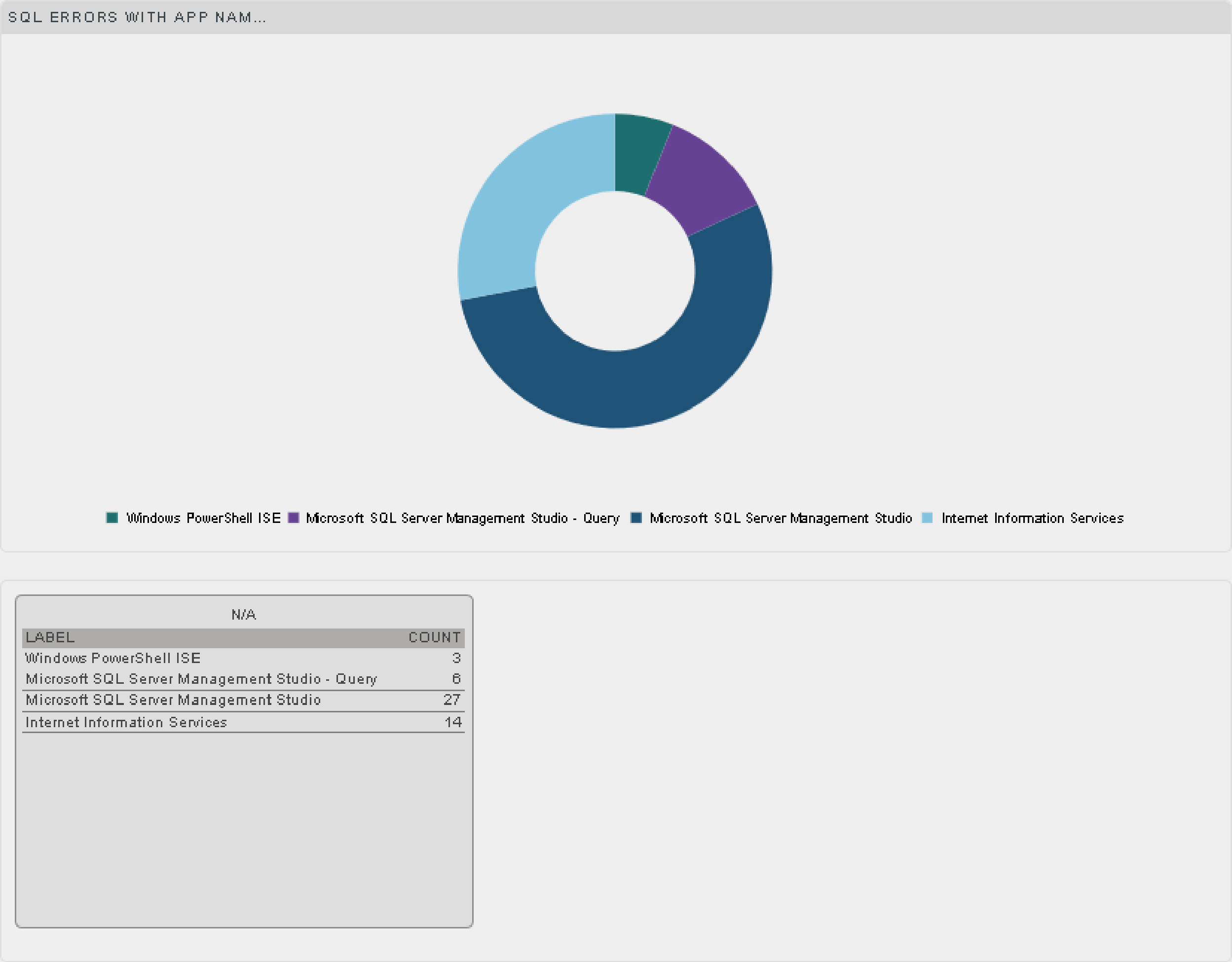
FILTER VALUES:

LEGEND [SERIES]: Select column

SELECT: All

Figure 89

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

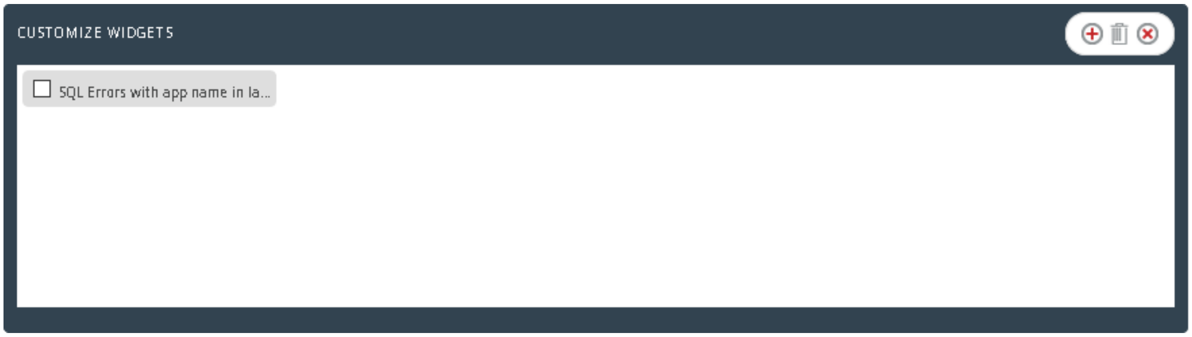

SQL ERRORS WITH APP NAM...
Windows PowerShell ISE
Microsoft SQL Server Management Studio - Query
Microsoft SQL Server Management Studio
Internet Information Services

N/A

LABEL	COUNT
Windows PowerShell ISE	3
Microsoft SQL Server Management Studio - Query	6
Microsoft SQL Server Management Studio	27
Internet Information Services	14

Figure 90

15. If satisfied, click **Configure** to create dashboard.


CUSTOMIZE WIDGETS

□ SQL Errors with app name in la...

Figure 91

16. Click ‘customize’ ⚙ to locate and choose created dashlet.

17. Click ⊕ to add dashlet to earlier created dashboard.

References

Microsoft SQL Audit Specifications

Microsoft SQL Audit Action ID

Microsoft SQL Extended Events