Netsurion™ | EventTracker

Integrate Symantec Data Loss Prevention

EventTracker v8.x and above

Publication Date: April 8, 2019

Abstract

This guide provides instructions to configure Symantec Data Loss Prevention to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Symantec DLP usage.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and Symantec DLP.

Audience

IT Admins, Symantec Data Loss Prevention administrators and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using EventTracker Enterprise.

Table of Contents

Overview

EventTracker Knowledge pack for Symantec DLP captures important and critical activities in Symantec DLP alerts, Symantec DLP Audit logs, Symantec DLP Access logs and Symantec DLP policy name details. Monitoring these activities is critical from a security aspect and is required for compliance and operational reasons.

The Symantec Data Loss Prevention Enforce Server is the central management platform that enables you to define, deploy, and enforce data loss prevention and security policies. The Enforce Server administration console provides a centralized, web-based interface for deploying detection servers, authoring policies, remediating incidents, and managing the system.

As your data spreads across a wider range of devices and storage environments, the ability to consistently define and enforce policies becomes even more critical. Symantec DLP features a unified management console, the DLP Enforce Platform, and a business intelligence reporting tool, IT Analytics for DLP, which allows you to write policies once and then enforce them everywhere, and measurably reduce information risks.

EventTracker helps you to monitor day to day activities like alerts, user audits, access log and policy violation.

Prerequisites

- **EventTracker v8.x or above** should be installed.
- **EventTracker Agent** should be installed on Symantec DLP enforce server system.
- **Symantec DLP** 14.5 or above versions. For all version, we need to customize the syslog format according to policy rule and policy name.

Configure Symantec DLP Syslog

1. Logon to the Symantec DLP enforce server.
2. Click **Manage** go to **policies** and go to **Response rules.**

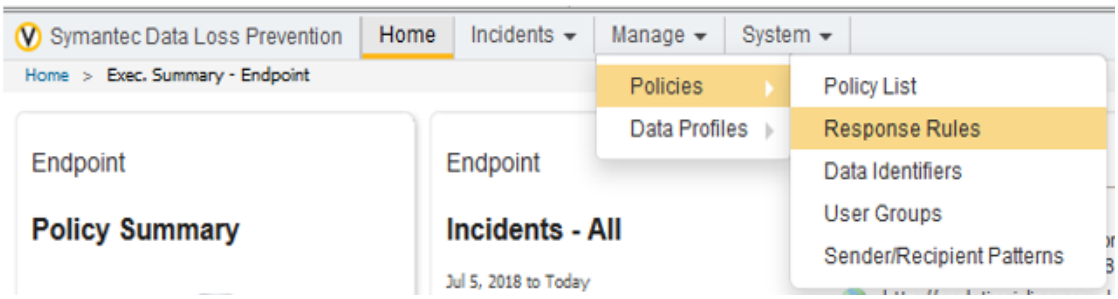

Figure 1

3. Creating new response rule by clicking Add **Response Rule**.

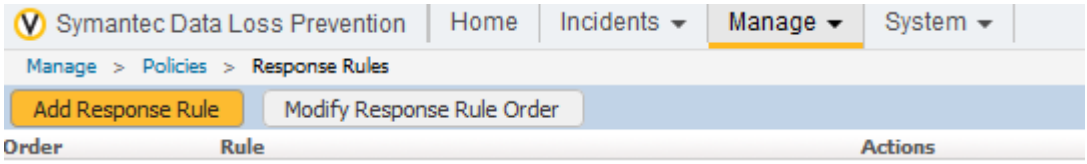

Figure 2

4. Check **Automated Response** and click next.

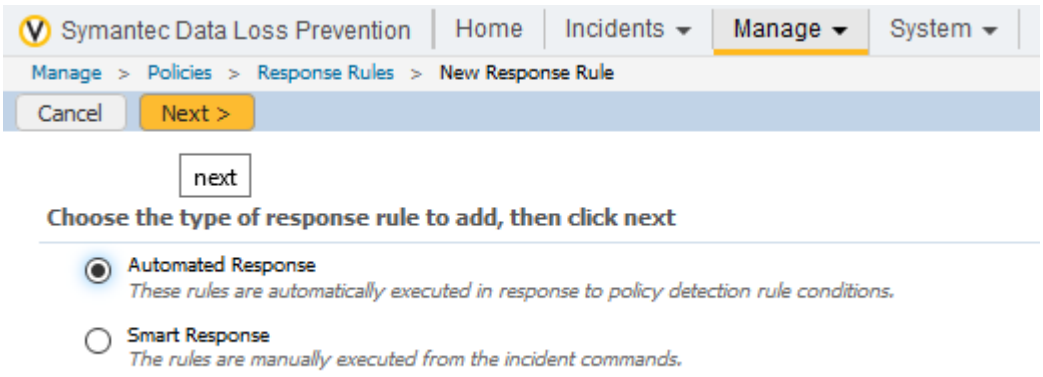

Figure 3

5. Fill details for **Configure Response Rule**.
   - **i) Rule Name:** we can give the **Response Rule** name as per **Policies Names.**
   - **ii) Description:** Description should give overview about **Rule Name.**
   - **iii) Actions: Add Condition** as **Log to a Syslog Server** for Actions.
   - **iv) Host:** Mention EventTracker installed host IP Address.
   - **v) Port:** Mention EventTracker syslog port (514) number.
   - **vi) Message:** Follow below message for logging syslogs.
   - **vii) Level:** Select 7 debugging form level.

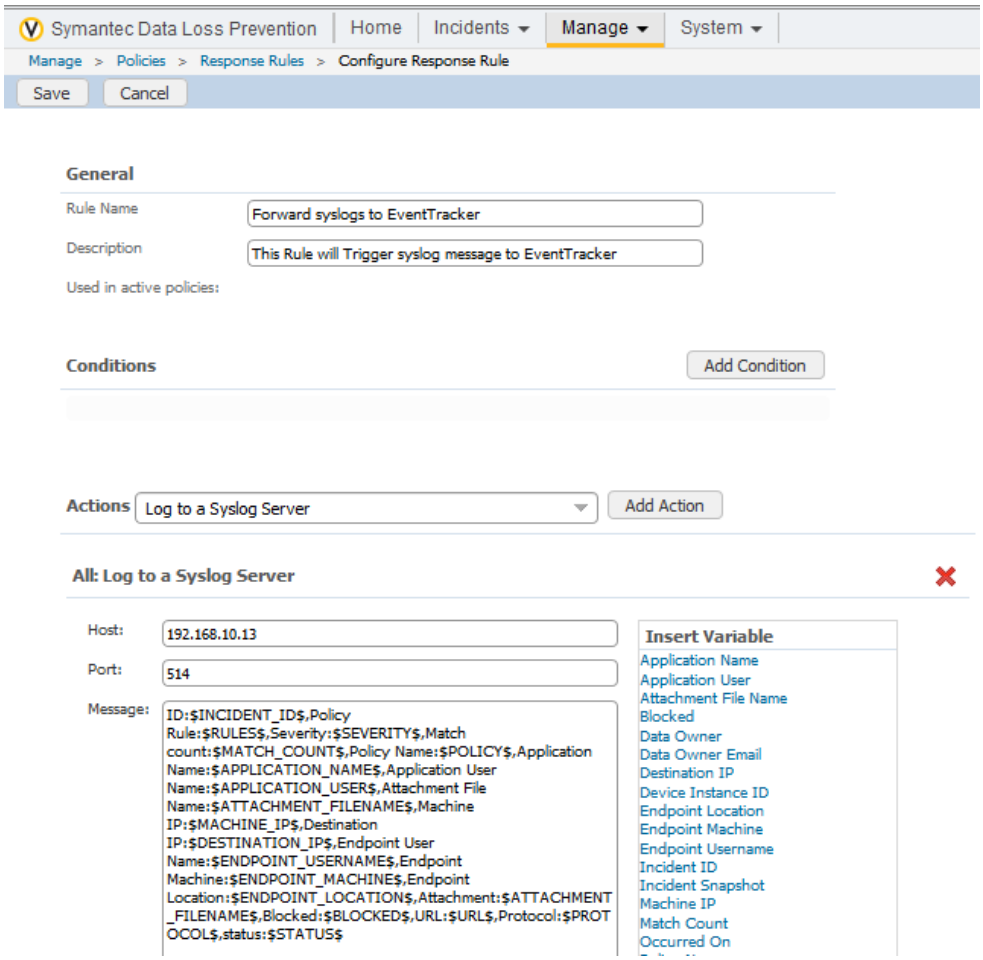

Figure 4

Use below log format.

Log Format:

ID:$INCIDENT_ID$,Policy Rule:$RULES$,Severity:$SEVERITY$,Match count:$MATCH_COUNT$,Policy Name:$POLICY$,Application Name:$APPLICATION_NAME$,Application User Name:$APPLICATION_USER$,Attachment File Name:$ATTACHMENT_FILENAME$,Machine IP:$MACHINE_IP$,Destination IP:$DESTINATION_IP$,Endpoint User Name:$ENDPOINT_USERNAME$,Endpoint Machine:$ENDPOINT_MACHINE$,Endpoint Location:$ENDPOINT_LOCATION$,Attachment:$ATTACHMENT_FILENAME$,Blocked:$BLOCKED$,URL:URL,Protocol:$PROTOCOL$,status:$STATUS$

6. After configuring response rule click **Save**.
7. **Response Rule** must map with **Policy Rule**. Whenever user violated the **Policy Rule** it will trigger **Response Rule** and **Response Rule** send syslog to EventTracker.

Follow the process given below for mapping **Response Rule** to **Policy Rule**.

Same process needs to be followed for other **Policy rules**.

i) Click **Manage** go to **Policies** and go to **Policy List.**

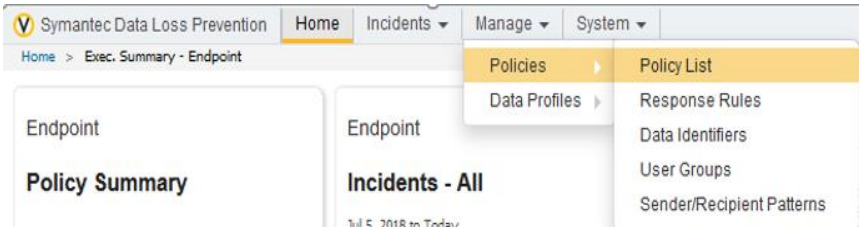

Figure 5

ii) Click any one Policy Rule for mapping Response Rule.

Figure 6

iii) After clicking **Policy Rule** go to **Response** and **choose response rule** and select Response Rule.

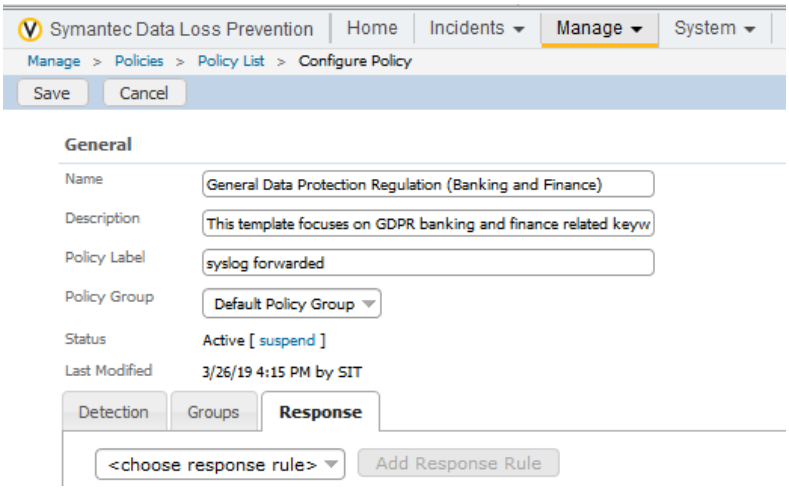

Figure 7

iv) Click save.

Note: Repeat same process for mapping **Response Rule** to all **Policy Rules**.

EventTracker Agent LFM Configuration

1. Logon to Symantec DLP enforce server host.

2. Navigate to **<%EventTracker install directory%>\Prism Microsystems\EventTracker\Agent**.

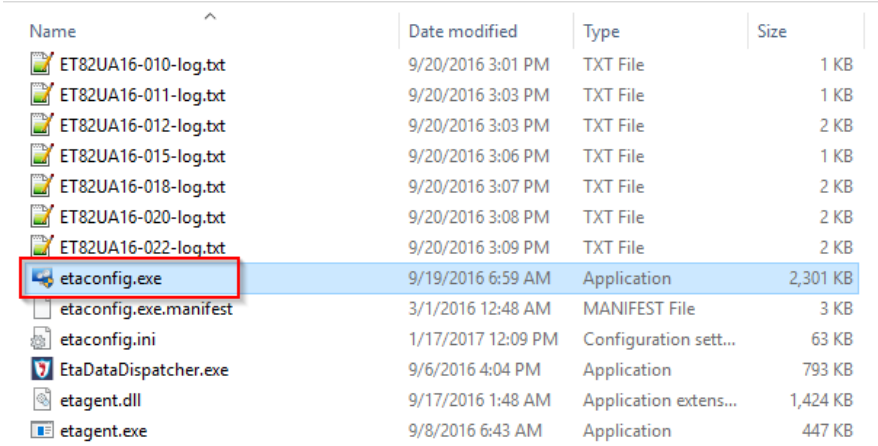

Figure 8

3. Right-click **etaconfig.exe** and select **Run as administrator**.

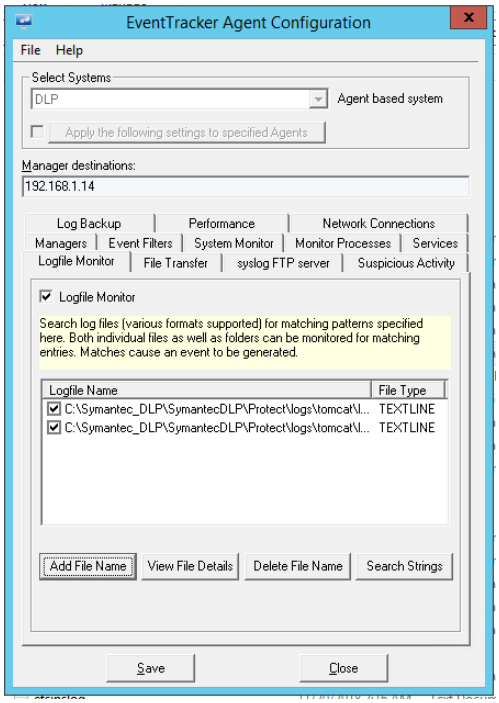

Figure 9

Symantec DLP audit logs has (.txt) and (.log) file extensions.

Below process is for (.txt) audit logs.

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

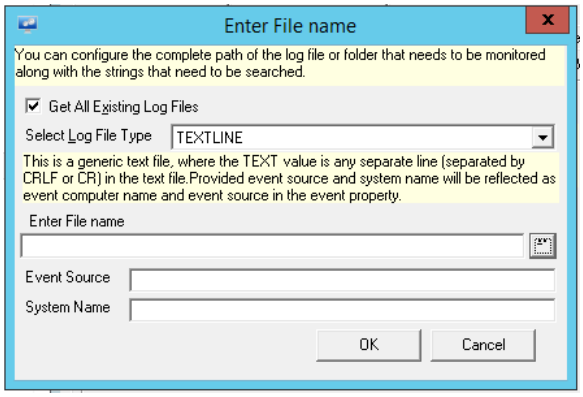

Figure 10

2. Select **Get All Existing Log Files Checkbox**.
3. Select **Text line** from **Select Log File Type drop-down**.
4. Click browse and browse to the earlier selected log file path.
5. Click **OK** to continue.

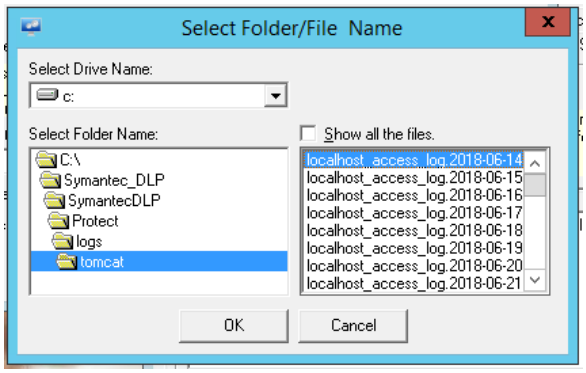

Figure 11

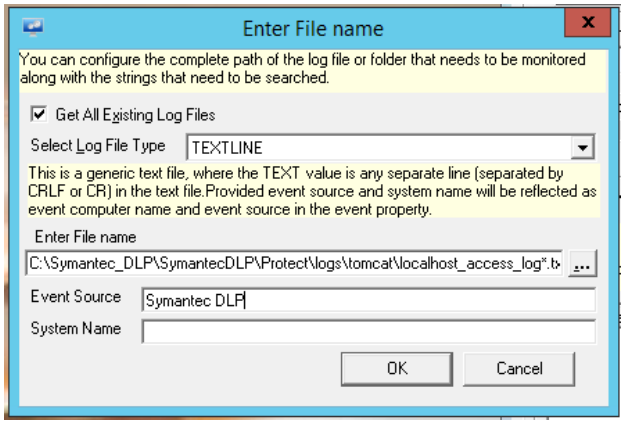

Figure 12

6. Click **Add String** for adding the **Search String.**

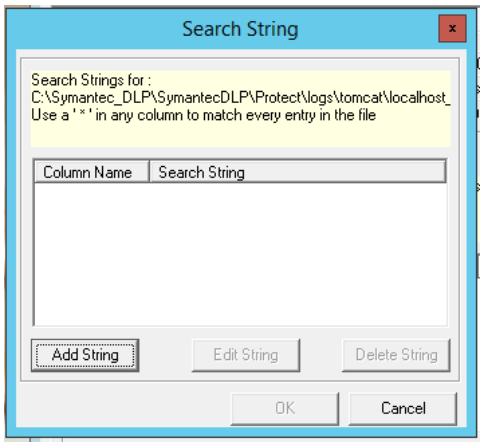

Figure 13

7. Select **text** from **Select Field Name**.
8. Mention ***** for **Enter Search String**.
9. Check **Current Date Time**.
10. Click **Ok** to Continue.

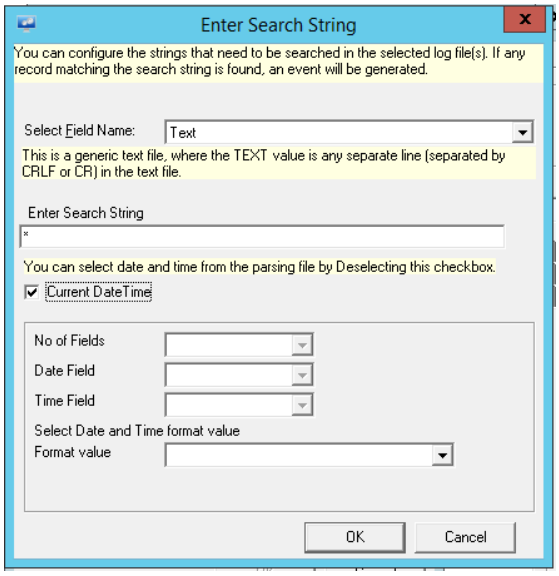

Figure 14

11. Click **Ok** to Accepting **Search String**.

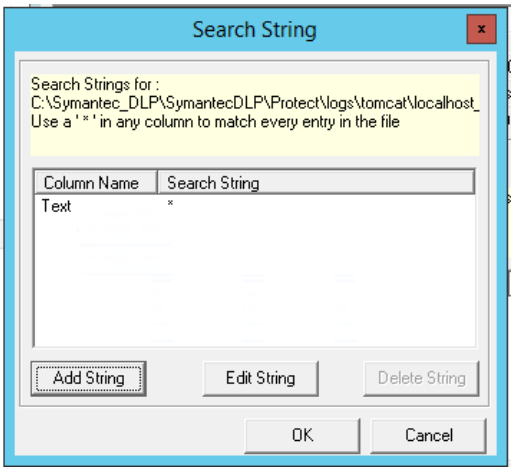

Figure 15

12. Click **Save** from **EventTracker Agent Configuration** for completing LFM configuration for **(.txt)** audit logs.

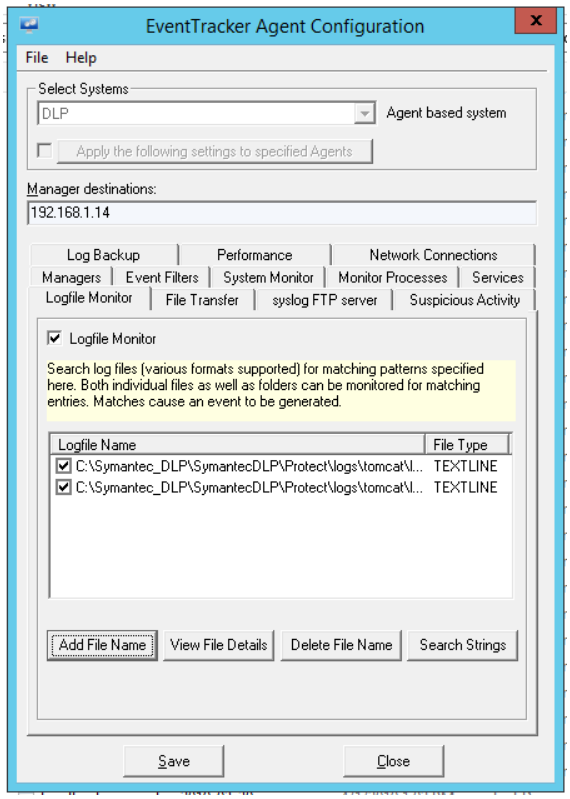

Figure 16

Below Process is for (.log) audit logs.

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

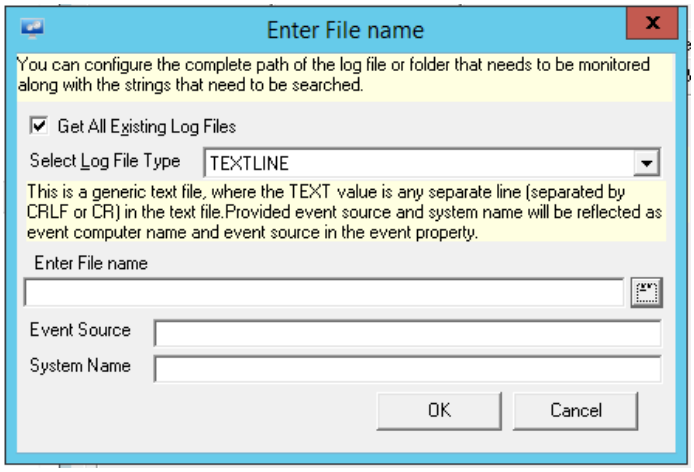

Figure 17

2. Select **Get All Existing Log Files Checkbox.**
3. Select **Text line** from Select **Log File Type drop-down**.
4. Click browse and browse to the earlier selected log file path.
5. Click **OK** to continue.

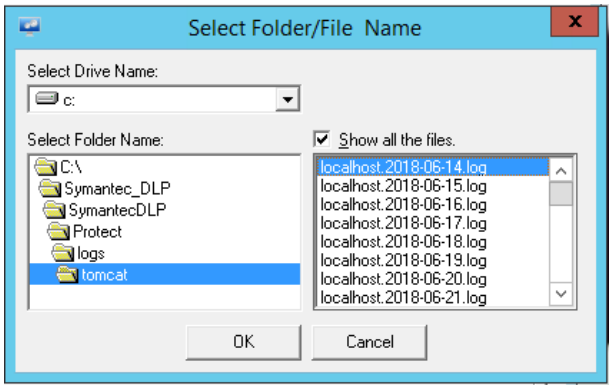

Figure 18

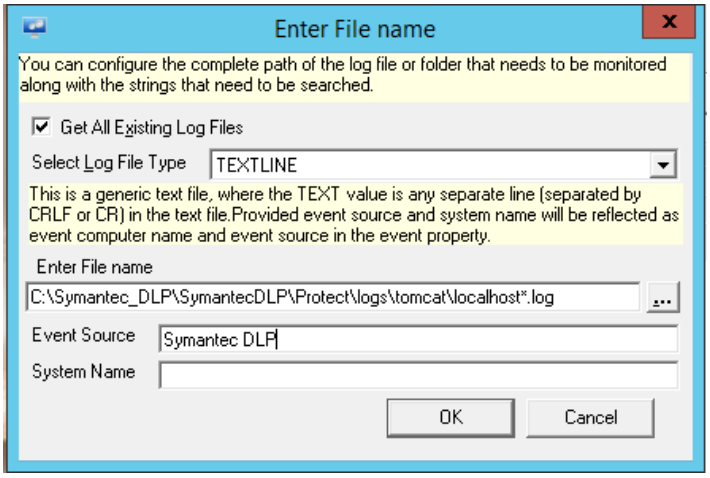

Figure 19

6. Click **Add String** for adding the **Search String**.

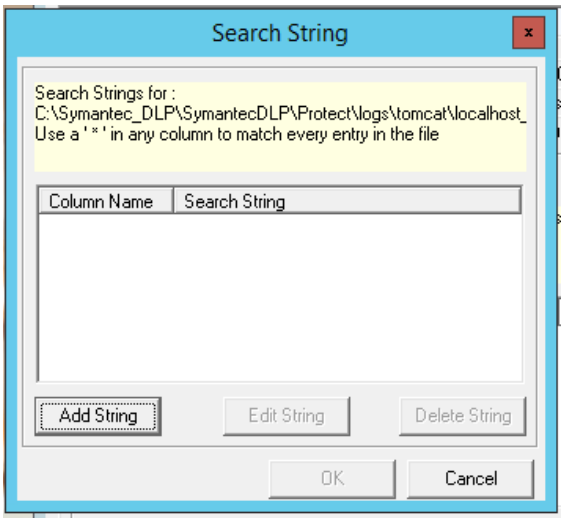

Figure 20

7. Select **text** from **Select Field Name**.
8. Mention ***** for **Enter Search String**.
9. Check **Current Date Time**.
10. Click **OK** to Continue.

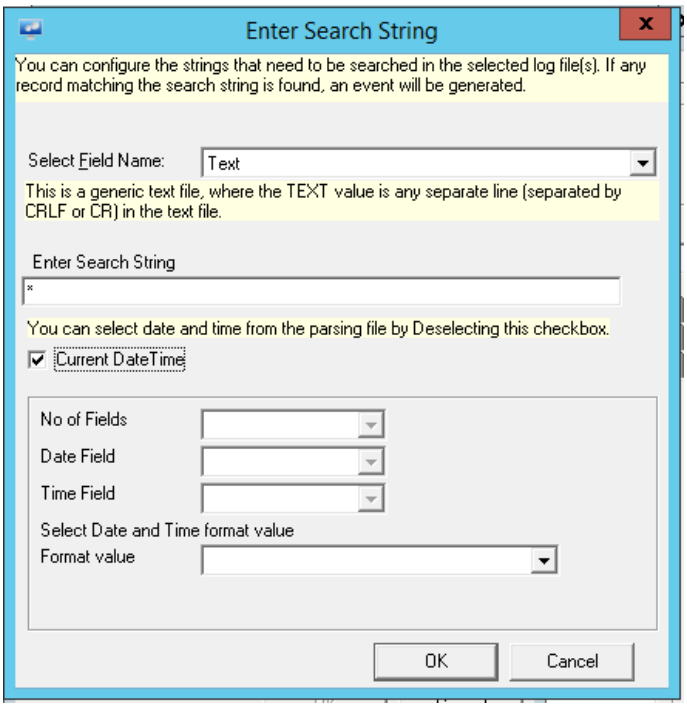

Figure 21

11. Click **OK** to Accepting **Search String**.

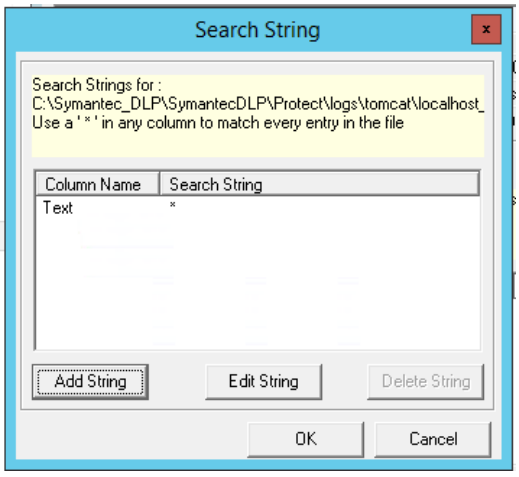

Figure 22

12. Click **Save** from **EventTracker Agent Configuration** for completing LFM configuration for **(.log)** audit logs.

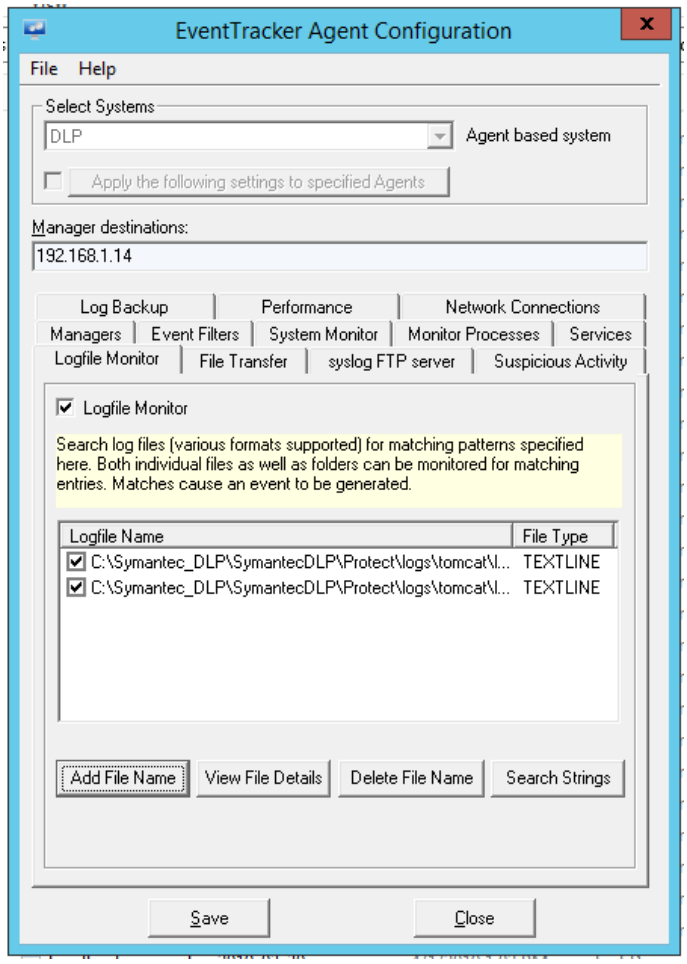

Figure 23

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; alert, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v9.x and later to support Symantec DLP.

Alert

- **Symantec DLP: Audit Changes –** This alert will trigger whenever policy rule is updated, Policy rule is changed.
- **Symantec DLP: Authentication Failed -** This alert will trigger whenever Symantec DLP enforce server user authentication failed, and user not found.
- **Symantec DLP: Policy Violations –** This alert will trigger whenever response rule match with severity is high or severe or critical.

Reports

- **Symantec DLP Policy Violation –** This report provides information related to what are the user and system violated in the mentioned policy.

LogTime	ID	Policy Name	Policy Rule	Match count	Endpoint User Name	Sender IP Address	Destination IP Address	Application Name	Endpoint Name	Endpoint Location
04/02/2019 04:45:33 PM	86813	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.11	null	Mozilla Firefox	CONTOSO12	Off the Corporate Network
04/02/2019 04:45:33 PM	86789	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONTO\Jack	192.168.200.122	null	Mozilla Firefox	CONTOSO221	Off the Corporate Network
04/02/2019 04:45:33 PM	86790	General Data Protection Regulation (Banking and Finance)	Hungarian Social Security Number	13	CONT\CLARKK	192.168.200.142	null	Microsoft Internet Explorer	CONTOSO43	Off the Corporate Network
04/02/2019 04:45:33 PM	86804	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\spinch	172.200.90.110	null	Mozilla Firefox	CONTOSO32	Off the Corporate Network
04/02/2019 04:45:33 PM	86806	General Data Protection Regulation (Banking and Finance)	Netherlands Tax Identification Number	12	CONT\MARYJ	172.40.80.110	127.0.0.1	NVIDIA GeForce Experience	CONTOSO10	Off the Corporate Network
04/02/2019 04:45:33 PM	86814	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.21	null	Mozilla Firefox	CONTOSO42	Off the Corporate Network
04/02/2019 04:45:35 PM	86813	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.11	null	Mozilla Firefox	CONTOSO12	Off the Corporate Network
04/02/2019 04:45:35 PM	86814	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.21	null	Mozilla Firefox	CONTOSO42	Off the Corporate Network
04/02/2019 04:45:35 PM	86806	General Data Protection Regulation (Banking and Finance)	Netherlands Tax Identification Number	12	CONT\MARYJ	172.40.80.110	127.0.0.1	NVIDIA GeForce Experience	CONTOSO10	Off the Corporate Network
04/02/2019 04:45:35 PM	86804	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\spinch	172.200.90.110	null	Mozilla Firefox	CONTOSO32	Off the Corporate Network

Figure 24

- **Symantec DLP User Login and Logout -** This report provides information related to the user login, logout and user authenticated.

LogTime	User Name	Thread ID	Authentication Type	Severity	Status
04/02/2019 04:45:33 PM	clarkk	8145	com.vontu.manager.ui.LogToServerController	SEVERE	loggedIn
04/02/2019 04:45:33 PM	maryj	8145	com.vontu.manager.ui.LogToServerController	SEVERE	loggedout
04/02/2019 04:45:35 PM	clarkk	8145	com.vontu.manager.ui.LogToServerController	SEVERE	loggedIn
04/02/2019 04:45:35 PM	maryj	8145	com.vontu.manager.ui.LogToServerController	SEVERE	loggedIn

Figure 25

- **Symantec DLP Authentication Failed -** This report provides information related to the authentication failed for user and could not find the user.

LogTime	User Name	Thread ID	Authentication Type	Severity	Status
04/02/2019 04:45:33 PM	123	6974	com.vontu.login.spring.VontuFormAuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	maryj	8148	com.vontu.login.spring.VontuFormAuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	clarkk	8148	com.vontu.login.AuthenticationServiceBase	SEVERE	Could not find a user with the name
04/02/2019 04:45:33 PM	maryj	8145	com.vontu.login.spring.VontuFormAuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	clarkk	7565	com.vontu.login.spring.VontuFormAuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	maryj	6960	com.vontu.login.AuthenticationServiceBase	SEVERE	Could not find a user with the name

Figure 26

- **Symantec DLP Web Activities -** This report provides information related to the accessing (access log) Symantec DLP detail IP address, web request method, and browser details.

LogTime	User IP Address	Web Request Method	Accessed URL	Status Code	Web Browser Details
04/02/2019 04:45:33 PM	172.80.200.110	GET	https://192.168.100.122/ProtectManager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:33 PM	172.80.200.110	GET	https://192.168.100.122/ProtectManager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:34 PM	172.80.200.110	GET	https://192.168.100.122/ProtectManager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:34 PM	172.80.200.110	GET	https://192.168.100.122/ProtectManager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:34 PM	172.80.200.110	GET	https://192.168.100.122/ProtectManager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0

Figure 27

- **Symantec DLP Audit Activities –** This report provides information related to policy changed, policy updated.

LogTime	User Name	Thread ID	Authentication Type	Severity	Policy Name	Activity
04/02/2019 04:45:33 PM	clarkk	4604	com.vontu.manager	INFO		POLICY_UPDATE
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.mail.ReportMailer	INFO		Scheduled report sent
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.report.saved.schedule.job.ScheduledReportJob	INFO		Running scheduled report
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.mail.ReportMailer	INFO		Scheduled report sent
04/02/2019 04:45:33 PM	Maryj	80	com.vontu.manager.report.saved.schedule.job.ScheduledReportJob	INFO		Running scheduled report
04/02/2019 04:45:33 PM	clarkk	4604	com.vontu.manager	INFO		POLICY_UPDATE
04/02/2019 04:45:33 PM	clarkk	4604	com.vontu.manager	INFO	Network Security policy	Policy changed
04/02/2019 04:45:33 PM	maryj	80	com.vontu.manager.mail.ReportMailer	INFO		Scheduled report sent
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.report.saved.schedule.job.ScheduledReportJob	INFO		Running scheduled report
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.mail.ReportMailer	INFO		Scheduled report sent

Figure 28

Dashboards

- **Symantec DLP Audit Activity** – This dashboard shows information about policy updated, policy changed, and Schedule report sent by the user.

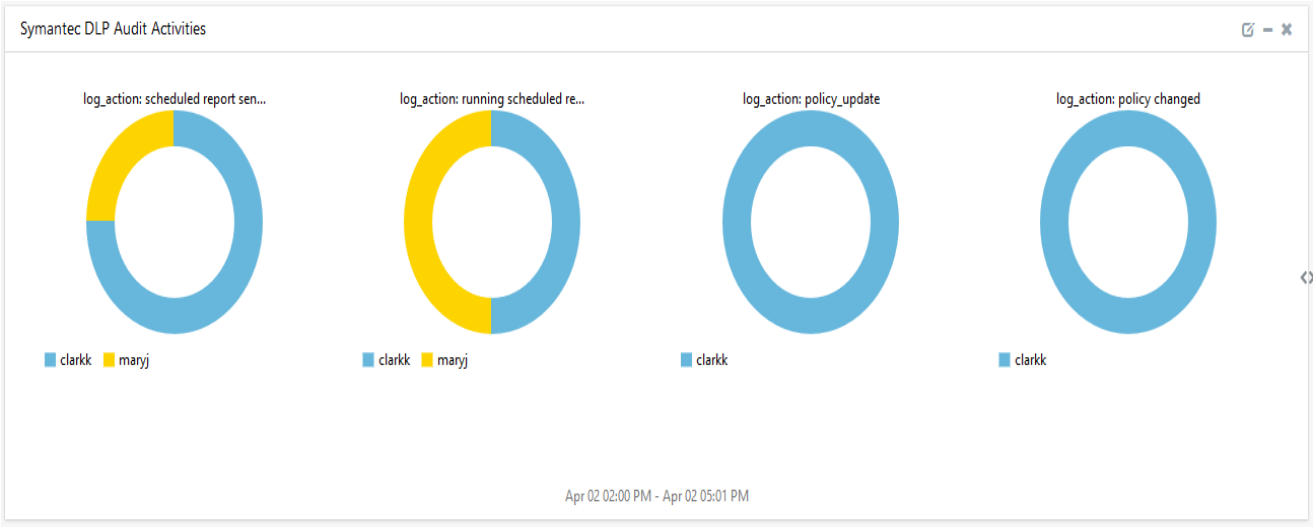

Figure 29

- **Top System Violated DLP Policies** – This dashboard shows information about which host, or user violated DLP policies.

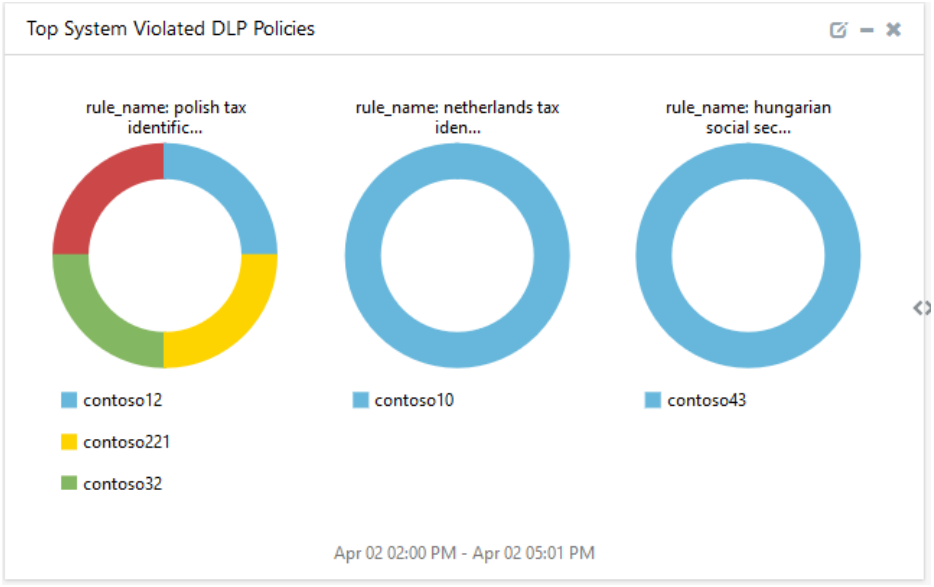

Figure 30

- **Symantec DLP Web Activities** – This dashboard shows information about what are the IP Address accessed by Symantec DLP portal, web request methods, URL and web browser detail.

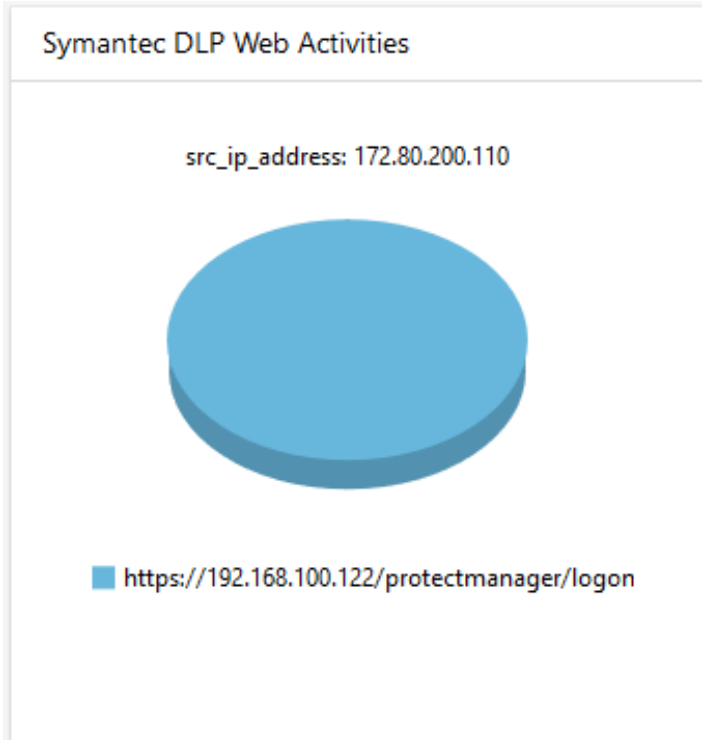

Figure 31

- **Symantec DLP User Login and Logout** – This dashboard shows information about which user is authenticated, login and logout.

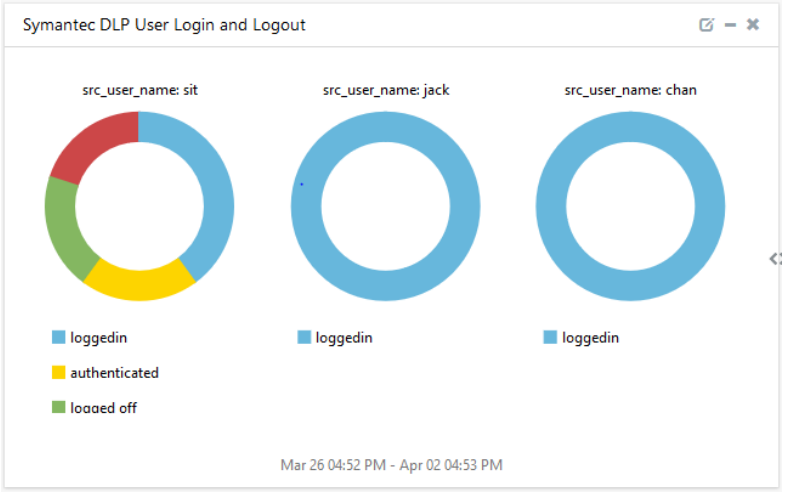

Figure 32

- **Symantec DLP Authentication Failed** – This dashboard shows information for which user authentication failed and user could not find.

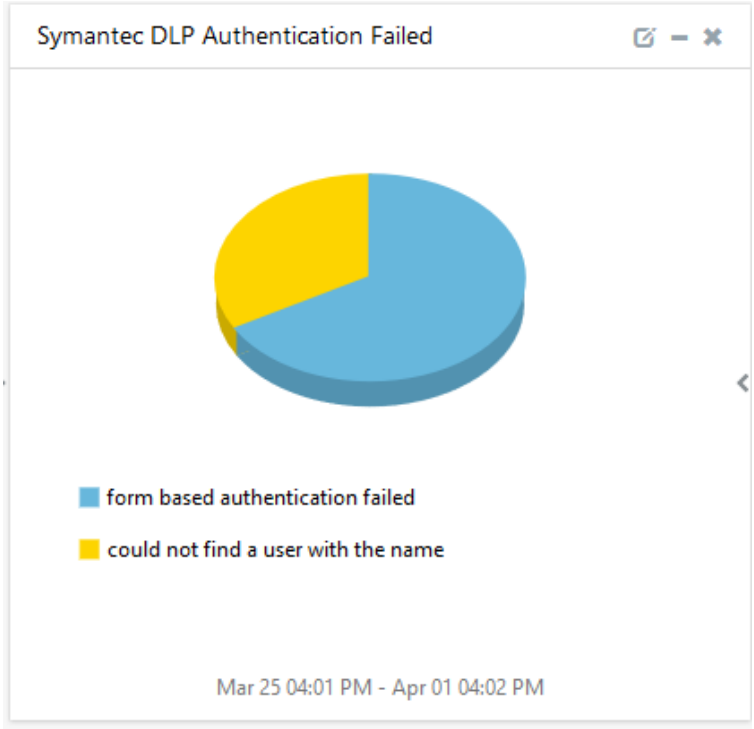

Figure 33

Import Knowledge Pack into EventTracker

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

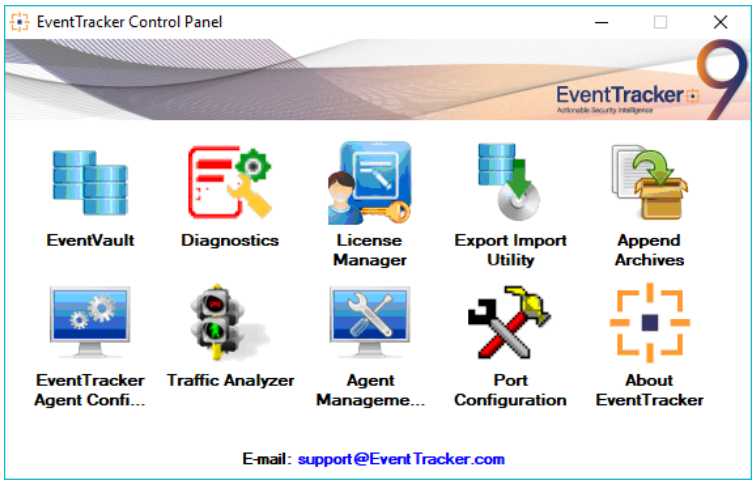

Figure 34

3. Import **Tokens/Flex Reports** as given below.

Category

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

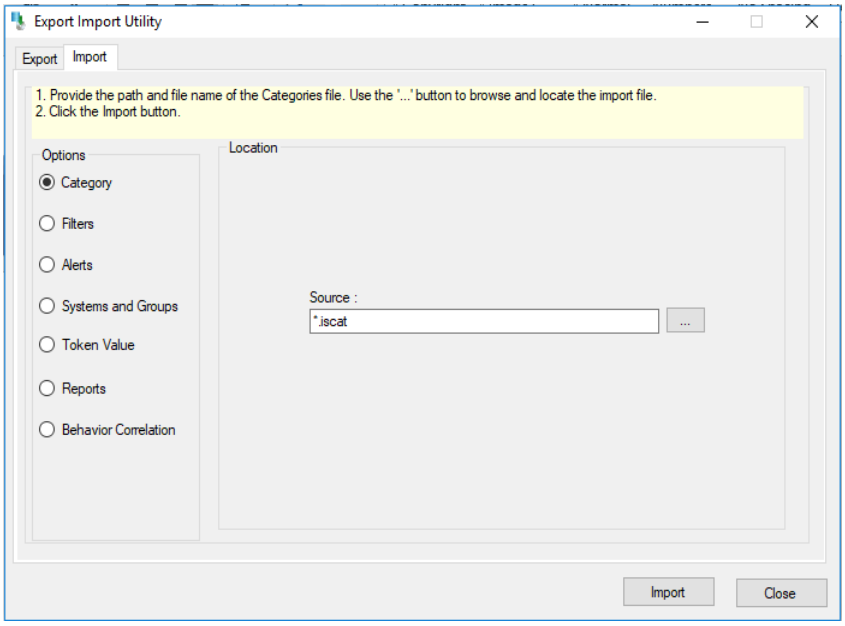

Figure 35

2. Locate **Category_Symantec DLP.iscat** file, and then click the open button.
3. To import category, click the **Import** button.
   EventTracker displays success message.

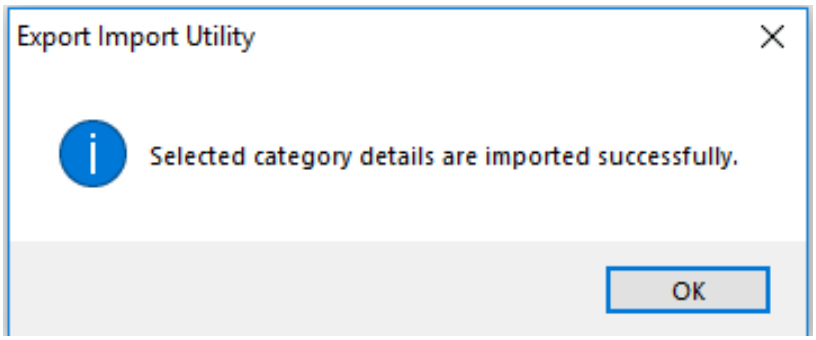

Figure 36

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

Alerts

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

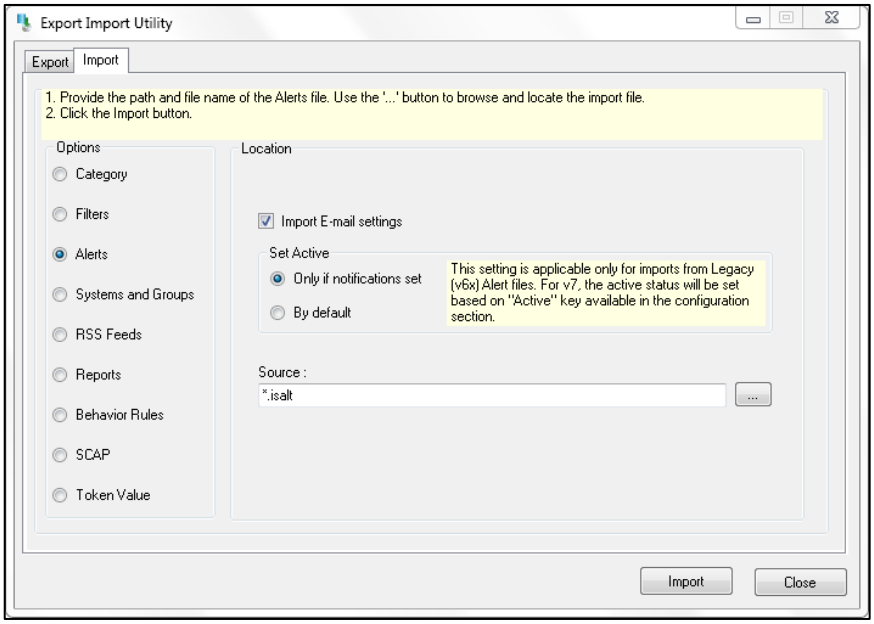

Figure 37

2. Locate **Alerts_Symantec DLP.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.

Figure 38

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

Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.
2. Locate the file named **KO_Symantec DLP.etko**.

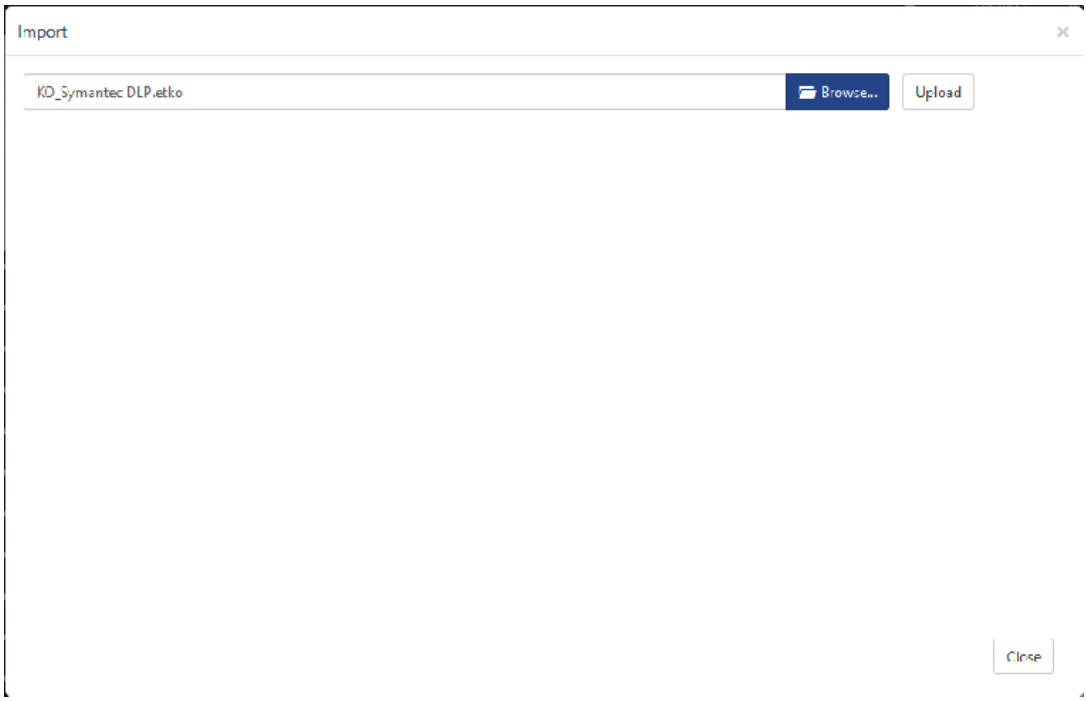

Figure 39

3. Now select all the check box and then click ‘**Import**’ option.

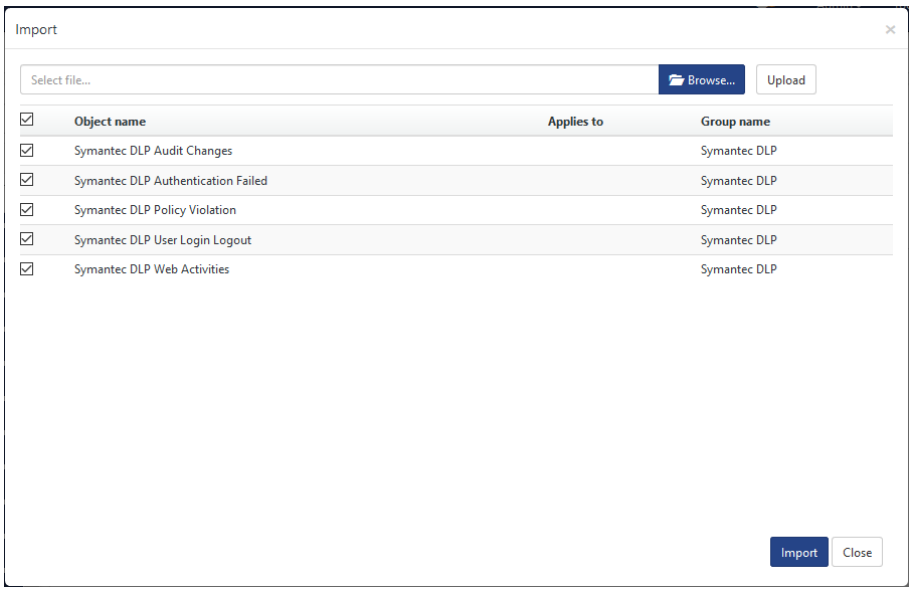

Figure 40

4. Knowledge objects are now imported successfully.

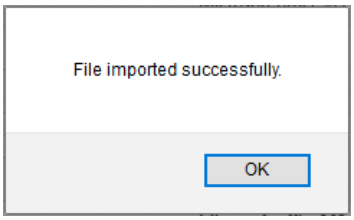

Figure 41

Flex Reports

1. Click **Reports** option and select new (.etcrx) from the option.

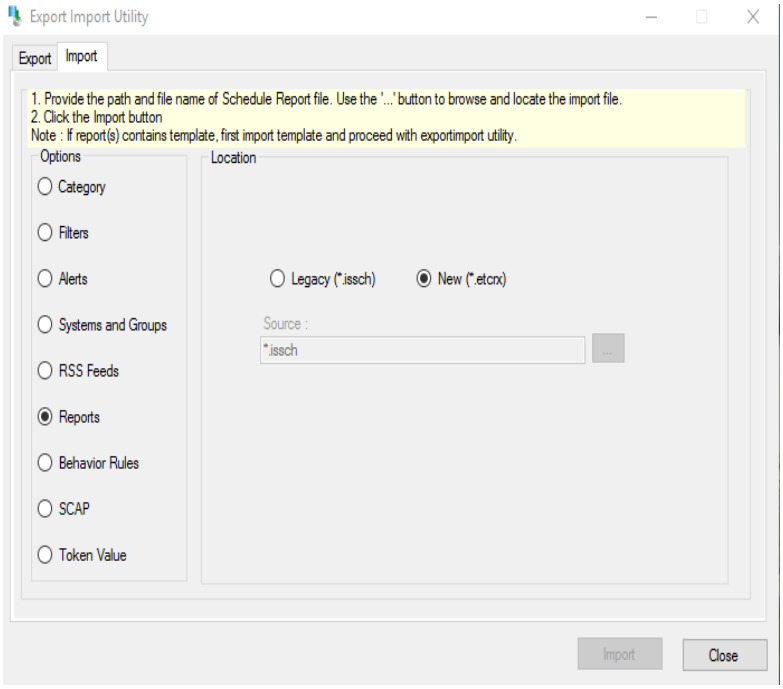

Figure 42

2. Locate the file named **Reports_Symantec DLP.etcrx** and select all the check box.

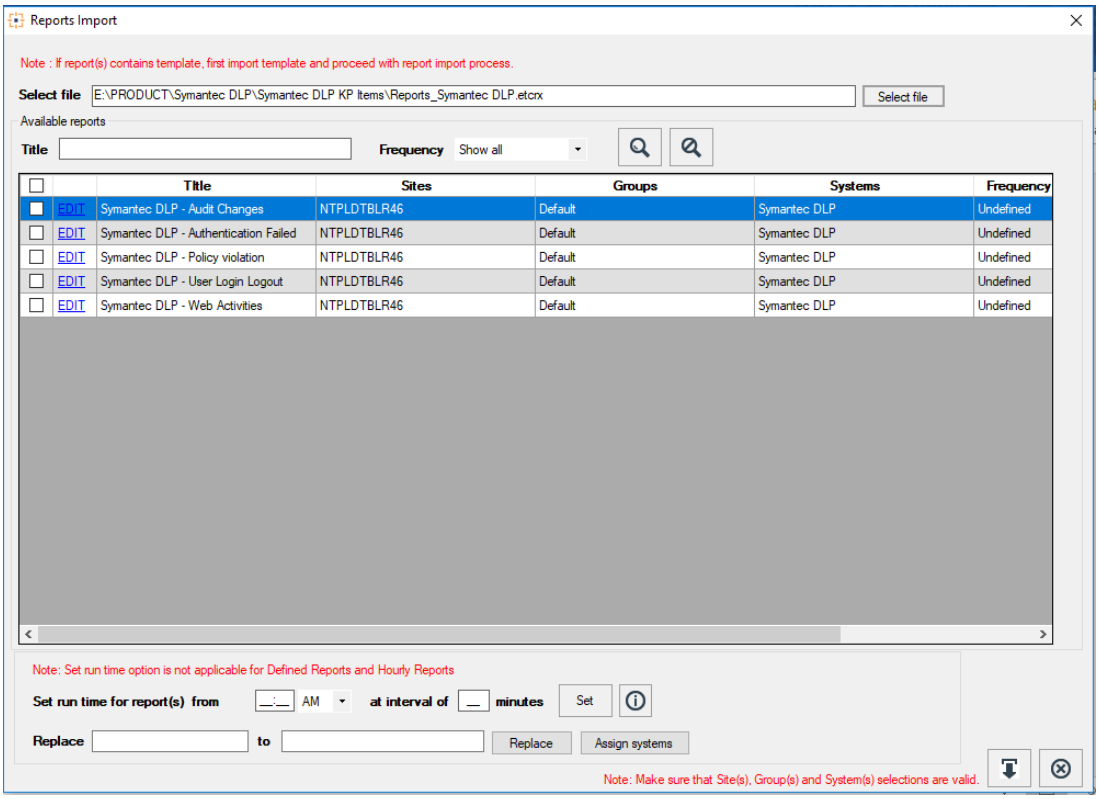

Figure 43

3. Click the **Import** button to import the reports. EventTracker displays success message.

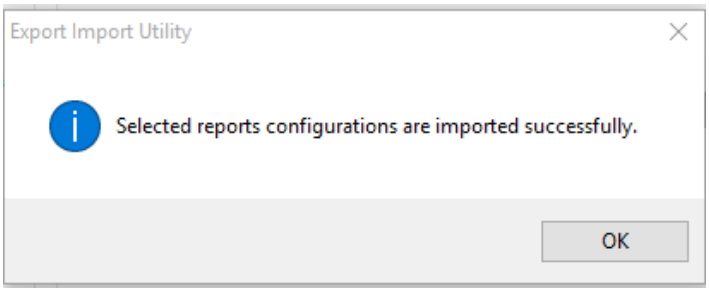

Figure 44

Dashlets

In EventTracker 9.0, we have added new feature which will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker Enterprise Web console.

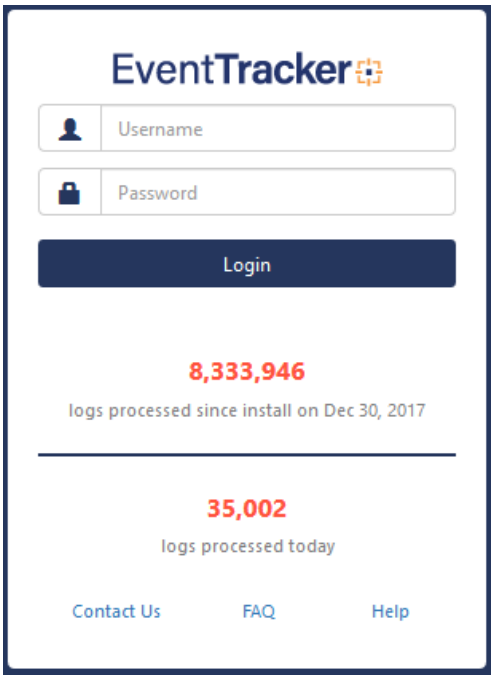

Figure 45

2. Go to **My Dashboard** option.

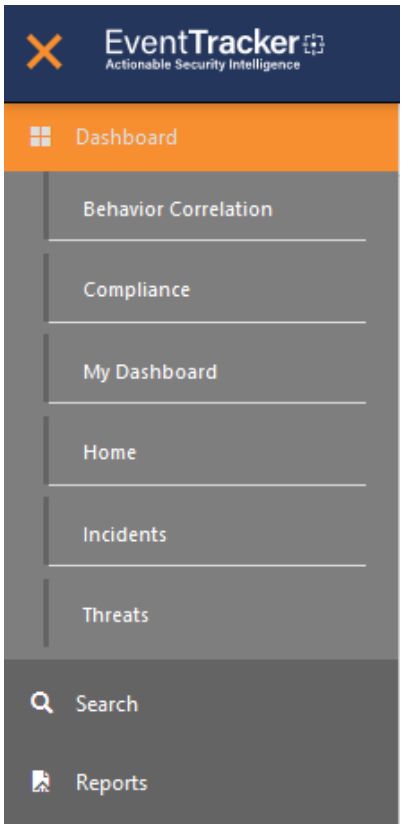

Figure 46

3. Click import button and select **.etwd** File.

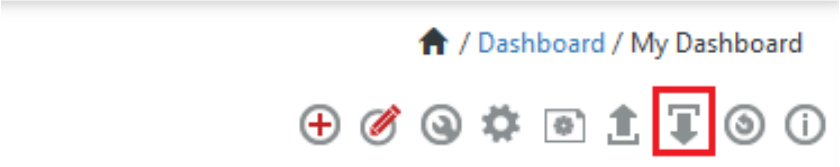

Figure 47

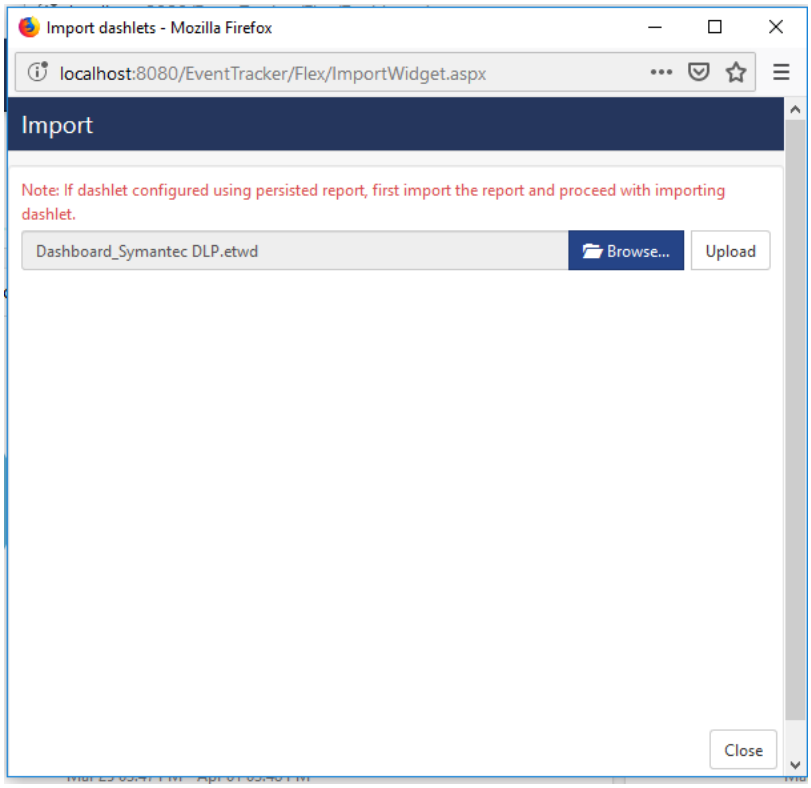

Figure 48

4. Click upload and select Dashboard which you want to import.

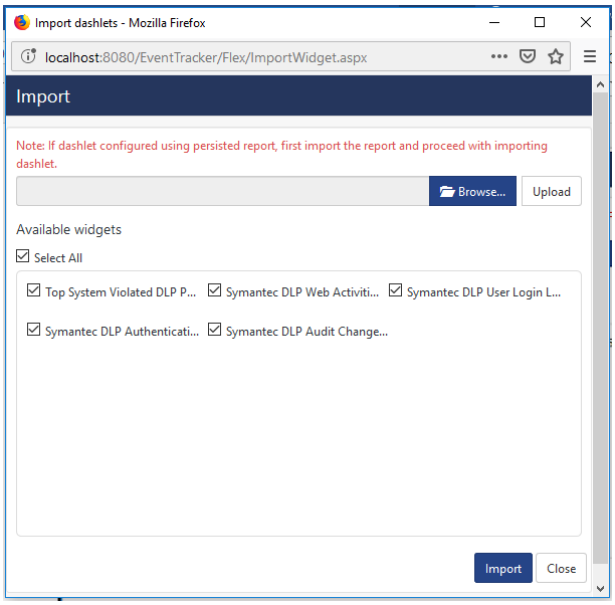

Figure 49

5. Click **Import** button. It will upload all selected dashboards.

Verify Knowledge Pack in EventTracker

Category

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Category**.

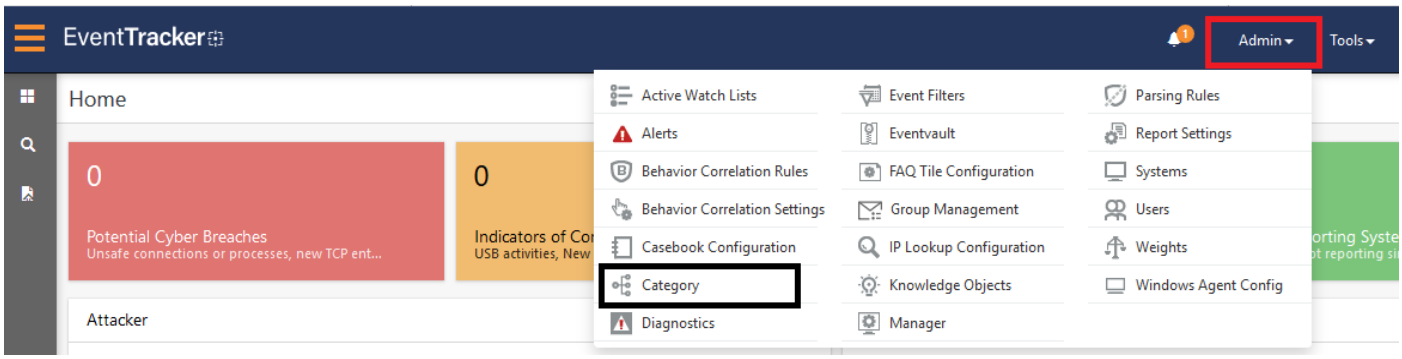

Figure 50

3. Click the **search**, and then **search** with **Symantec DLP**.

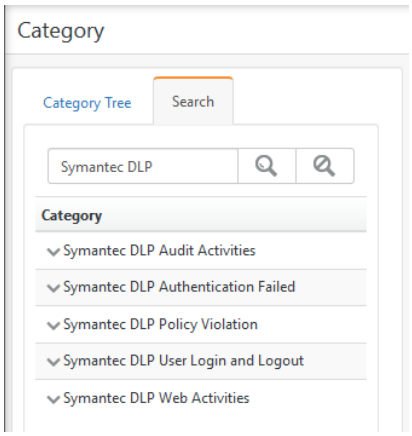

Figure 51

Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.

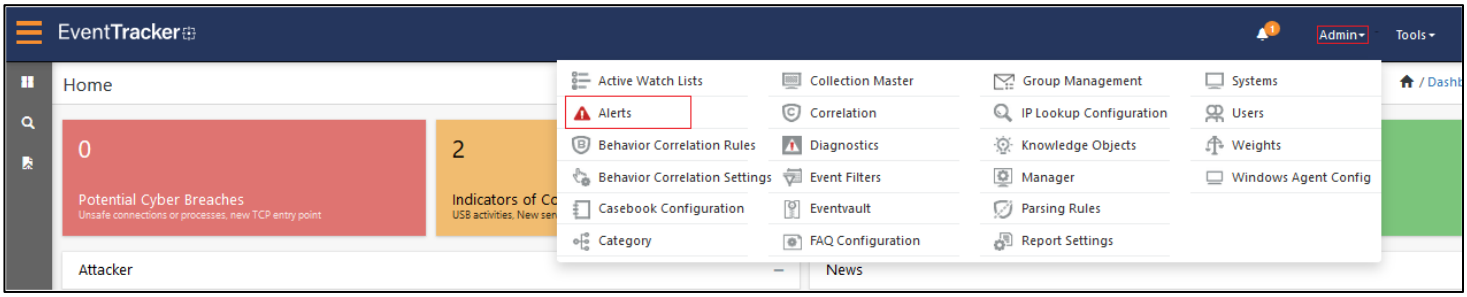

Figure 52

3. In the **Search** box, type **'Symantec DLP'**, and then click the **Go** button.
   Alert Management page will display all the imported alerts.

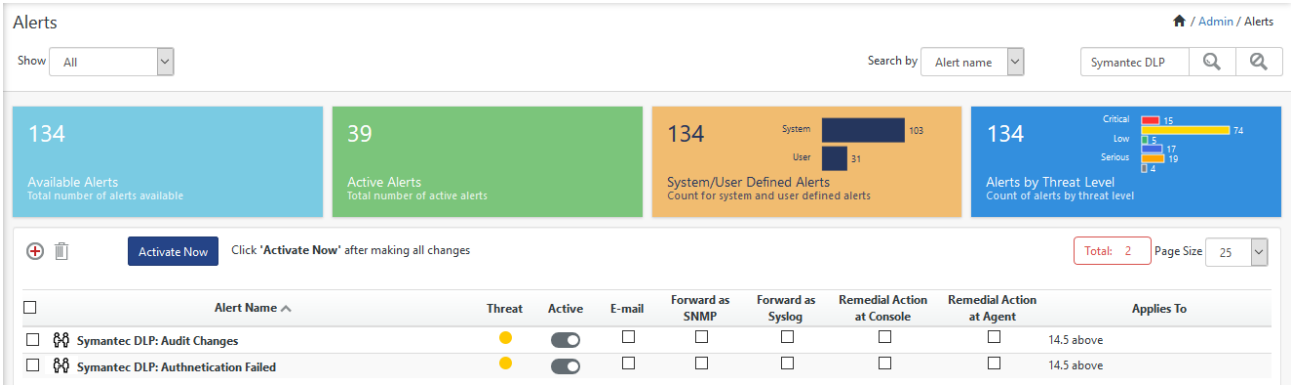

Figure 53

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

EventTracker displays message box.

Figure 54

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

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

Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Symantec DLP** group folder.

Knowledge Object are displayed in the pane.

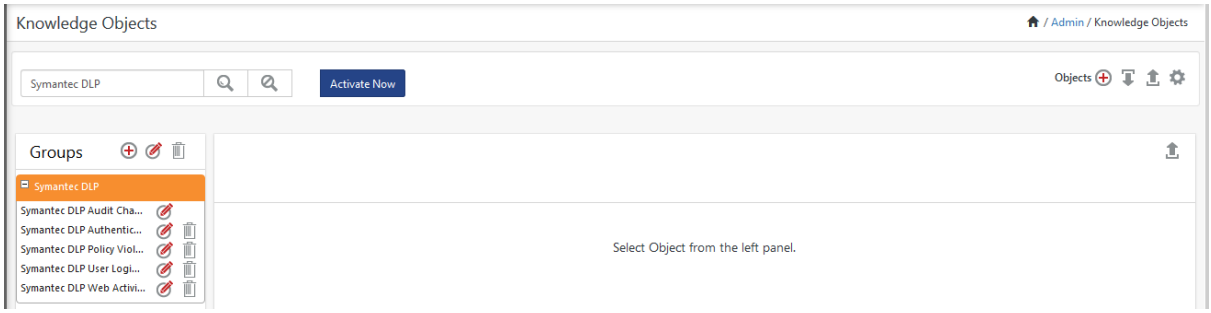

Figure 55

Flex Reports

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

Reports are displayed in the Reports configuration pane.

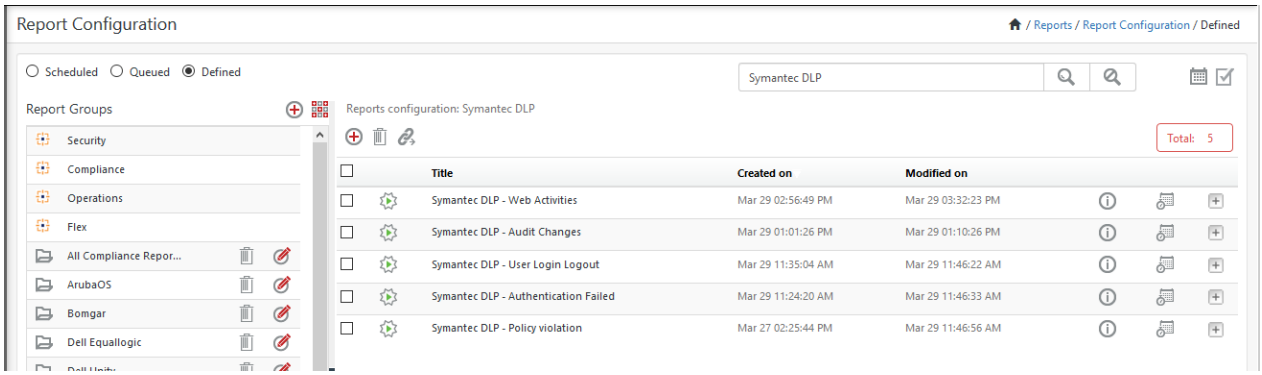

Figure 56

Dashlets

1. Logon to **EventTracker Enterprise**.
2. Click the **Dashboard** menu, and then **My Dashboard.**
3. Then click **Customize Dashlet** button and search for **"Symantec DLP"**

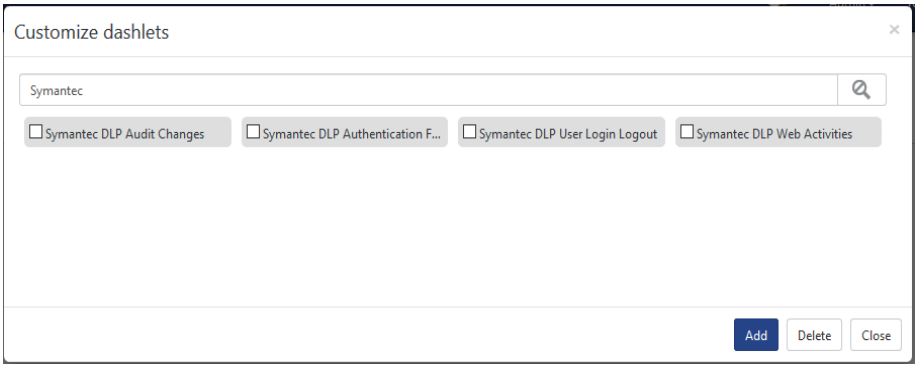

Figure 57