Netsurion | EventTracker®

Integrate Solaris

EventTracker v9.0 and above

Publication Date: December 30, 2019

Abstract

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

Scope

The configurations detailed in this guide are consistent with **EventTracker v9.x** and later, **Solaris.**

Audience

Solaris users, who wish to forward events to EventTracker and monitor events using EventTracker.

Table of Contents

1. Overview

Solaris is an operating system based on Unix developed in 1992 by Sun Microsystems. EventTracker integrates with Solaris via syslog. It monitors events to provides insight on security and compliance events such as login, logout, login-failed events, command executed and privilege escalation.

2. Prerequisites

- EventTracker v9.x or above should be installed.
- Allow port 514 in the firewall.

3. Configuring Solaris to forward logs to EventTracker

1. Log into the solaris system you want to monitor.
2. Launch the terminal and run the below command.

   sudo vi /etc/syslog.conf

3. Enter the EventTracker Agent IP in place of **<Eventtracker IP>**.

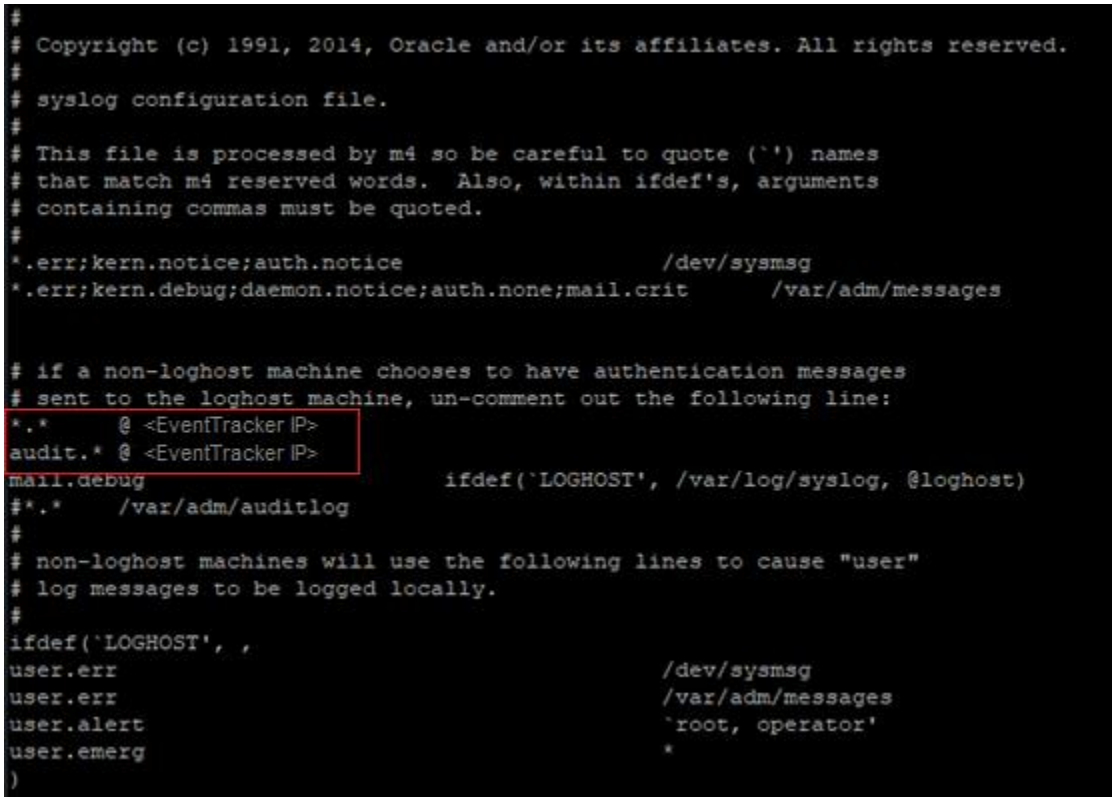

Figure 1

4. Save and quit.
5. Run the following command.

```
sudo /usr/sbin/auditconfig -setflags fd,fc,fm,lo,ex
```

6. Use the below command to restart the syslog service

```
svcadm restart system/system-log:default
```

7. In addition to this, audit logs should also be enabled, which can be done by following the below steps.
   - Assume the Primary Administrator role, or become superuser.
   - Save a backup copy of the `audit_control` file.
     - cp /etc/security/audit_control /etc/security/audit_control.save
   - Add an audit_syslog.so plugin entry in `audit_control`.
     - audit_control file

       flags:lo,ss

       naflags:lo,na

       plugin:name=audit_binfile.so;p_dir=/var/audit; p_minfree=20;
8. Add an audit.notice entry to the syslog.conf file, it should look as shown below

```
cat /etc/syslog.conf

audit.notice        /var/adm/auditlog
```

9. Create a log file.

```
touch /var/adm/auditlog
```

10. Refresh the configuration information for the `syslog` service.

```
svcadm restart system/system-log:default
```

Note: Enabling the audit logs results in a huge amount of log, which can impact the performance.

4. EventTracker Knowledge Pack

Once logs are received into EventTracker, Alerts, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Windows.

4.1 Saved Searches

- **Solaris – Login Logout :** This saved search provides information related to login-logout activities along with the username and IP address from where the login occurred.
- **Solaris – Login Failed :** This saved search provides information related to login failed activities along with the username and IP address from where the login was attempted.

- **Solaris – Command Executed :** This saved search provides information related to the command that were executed.

4.2 Reports

- **Solaris – Login Logout :** This report provides information related to login-logout activities along with the username and IP address from where the login occurred.
- **Solaris – Login Failed :** This report provides information related to login failed activities along with the username and IP Address from where the login was attempted.
- **Solaris – Command Executed :** This report provides information related to the command that were executed.
- **Solaris – Privilege Escalation :** This report provides information related to the privilege escalation and provides information about the user requesting the privilege escalation and status of the request.

4.3 Alerts

- **Solaris – Login Failed :** This alert is generated when a login failed occurs. The alert is generated when both local and ssh login failure events occur and provide information about the user who tried to login.

4.4 Dashboards

- Solaris – Login failed by username

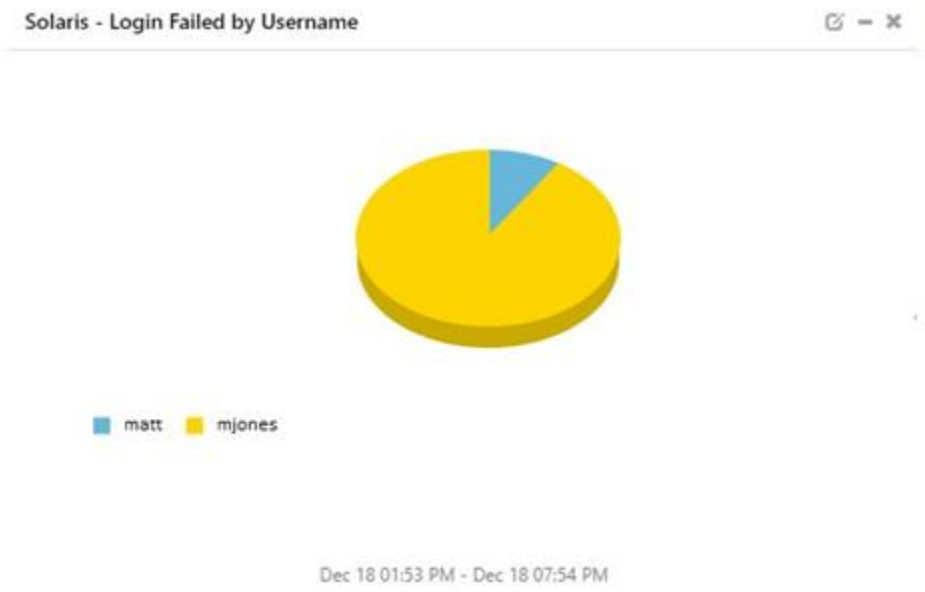

Figure 2

- Solaris – Login and logout by username.

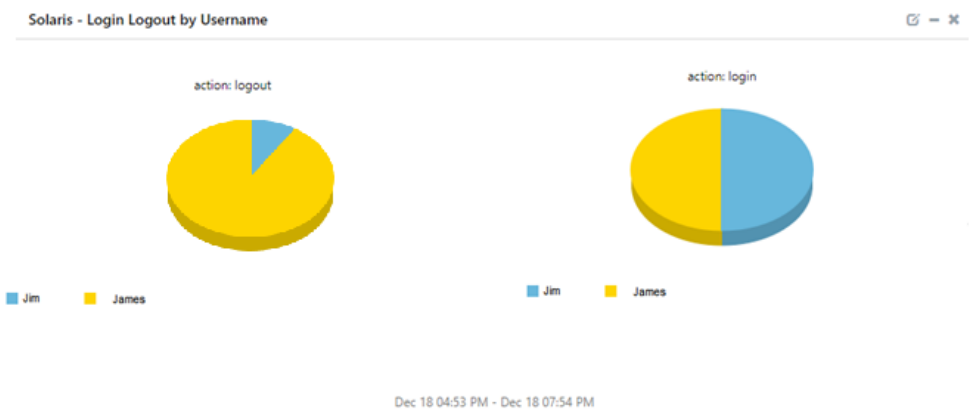

Figure 3

- Solaris – Command executed by username.

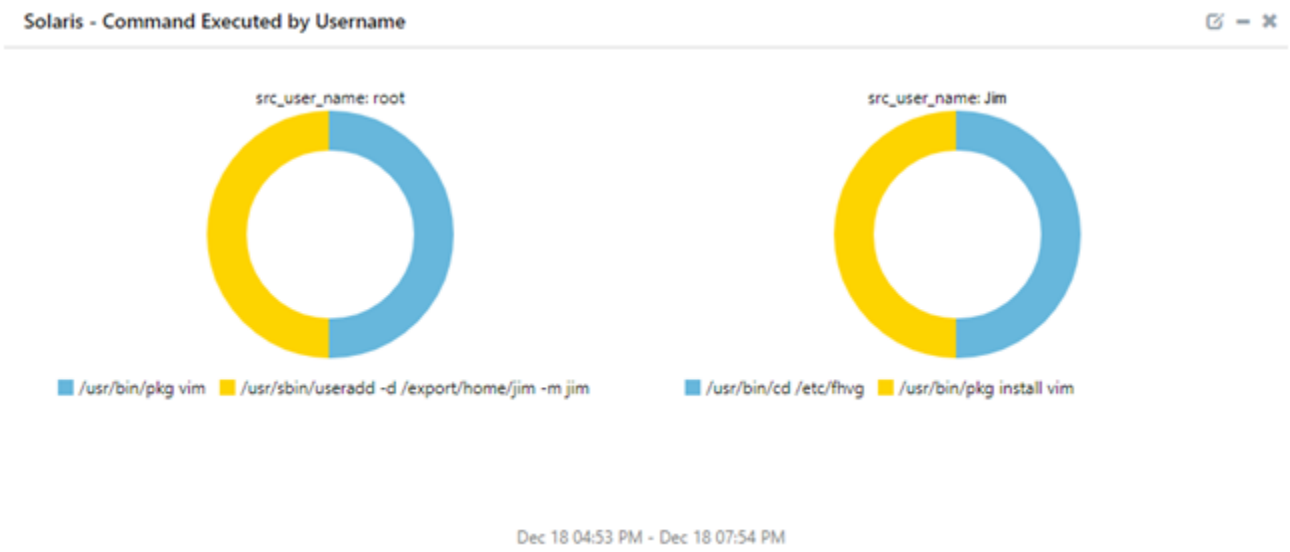

Figure 4

5. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards
- Alerts

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.

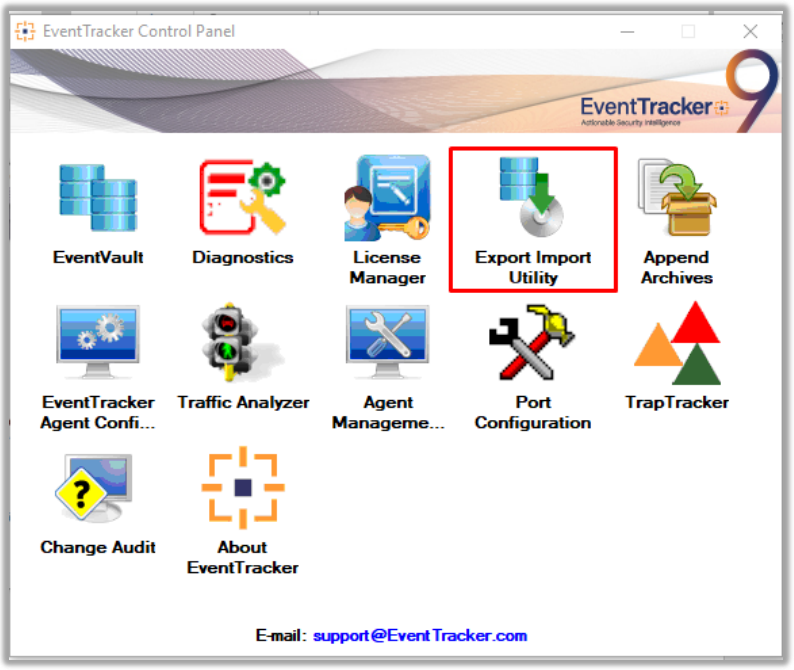

Figure 5

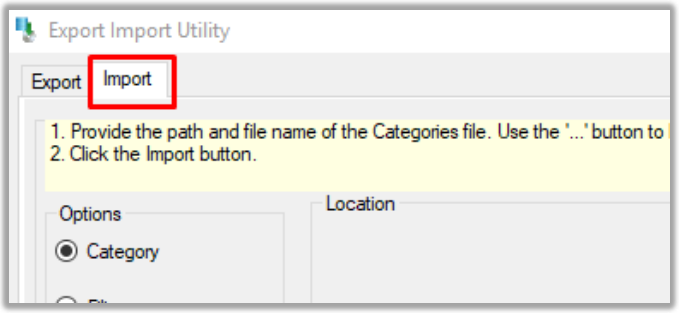

Figure 6

3. Click the **Import** tab.

5.1 Categories

1. Once you have opened "**Export-Import Utility**" via "**EventTracker Control Panel**", click the **Category** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with extension **".iscat", like "Categories_Solaris.iscat"** and then click on the "**Import**" button:

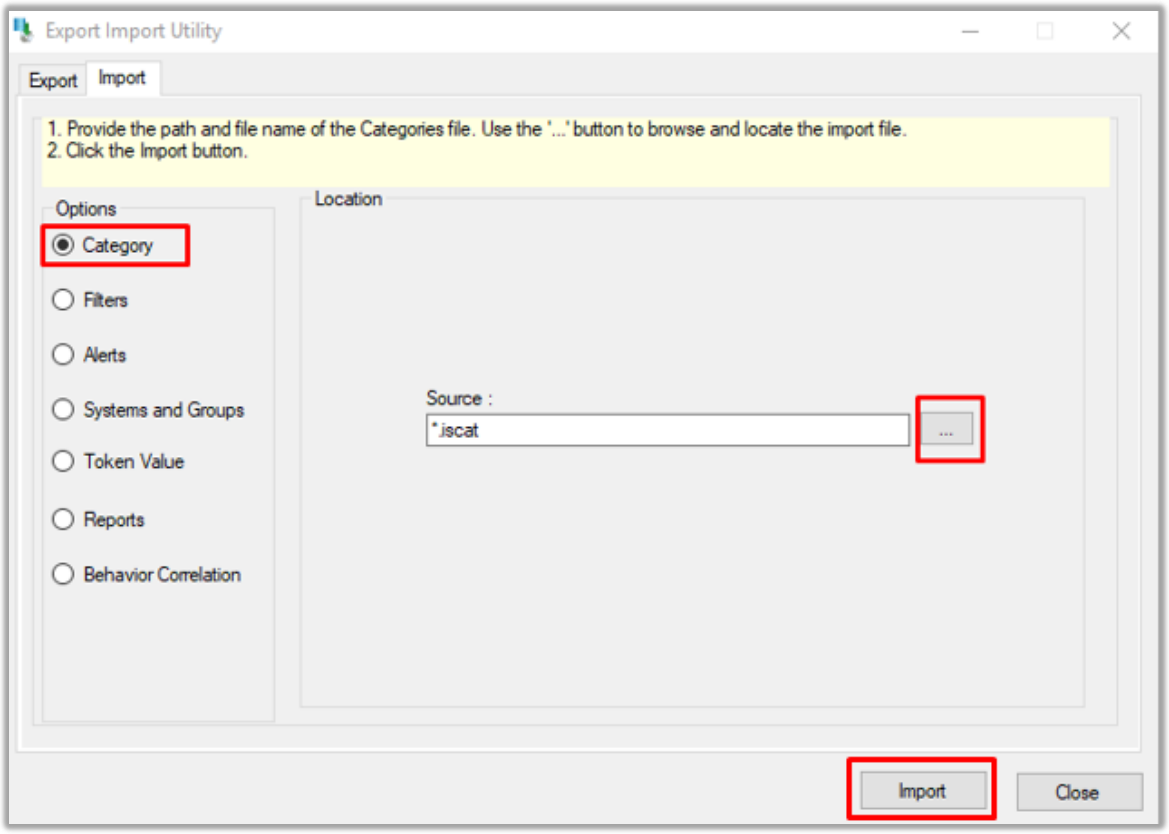

Figure 7

EventTracker displays a success message:

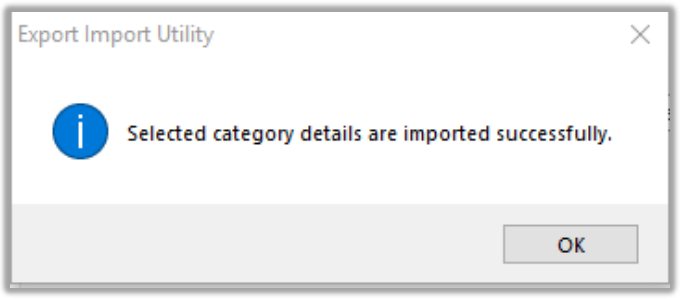

Figure 8

5.2 Token Template

1. Login to the **EventTracker Console**.
2. Click on **Admin >> Parsing Rules**.

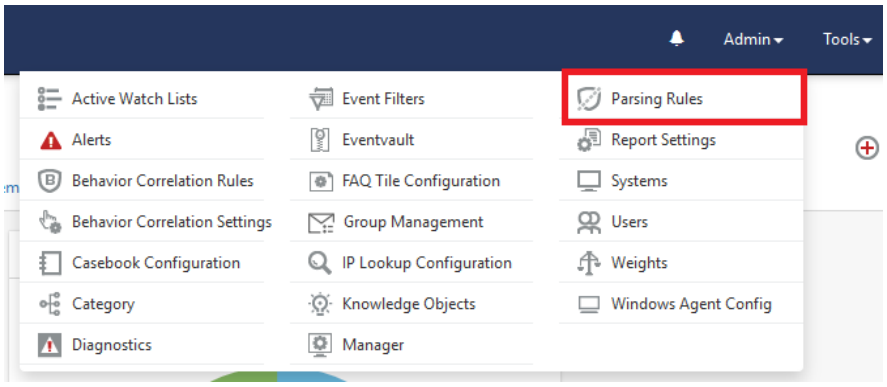

Figure 9

3. Click on **Template** and click **import configuration** Symbol.

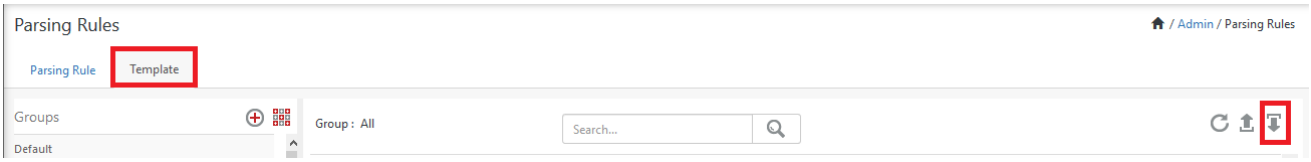

Figure 10

4. Locate the **".ettd"** file and click on **import**.

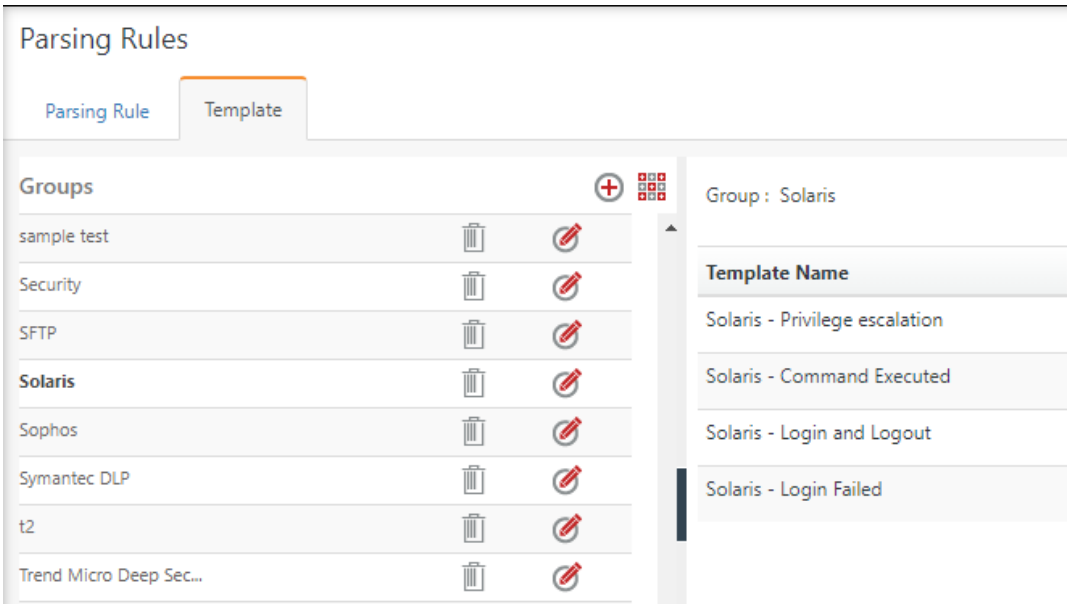

Figure 11

5. Templates are imported now successfully.

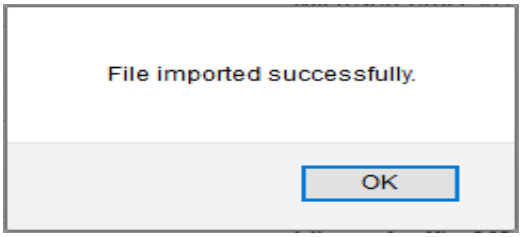

Figure 12

5.3 Flex Reports

1. In the EventTracker control panel, select "**Export/ Import utility**" and select the "**Import tab**". Then click **Reports** option, and choose "**New (*.etcrx)**":

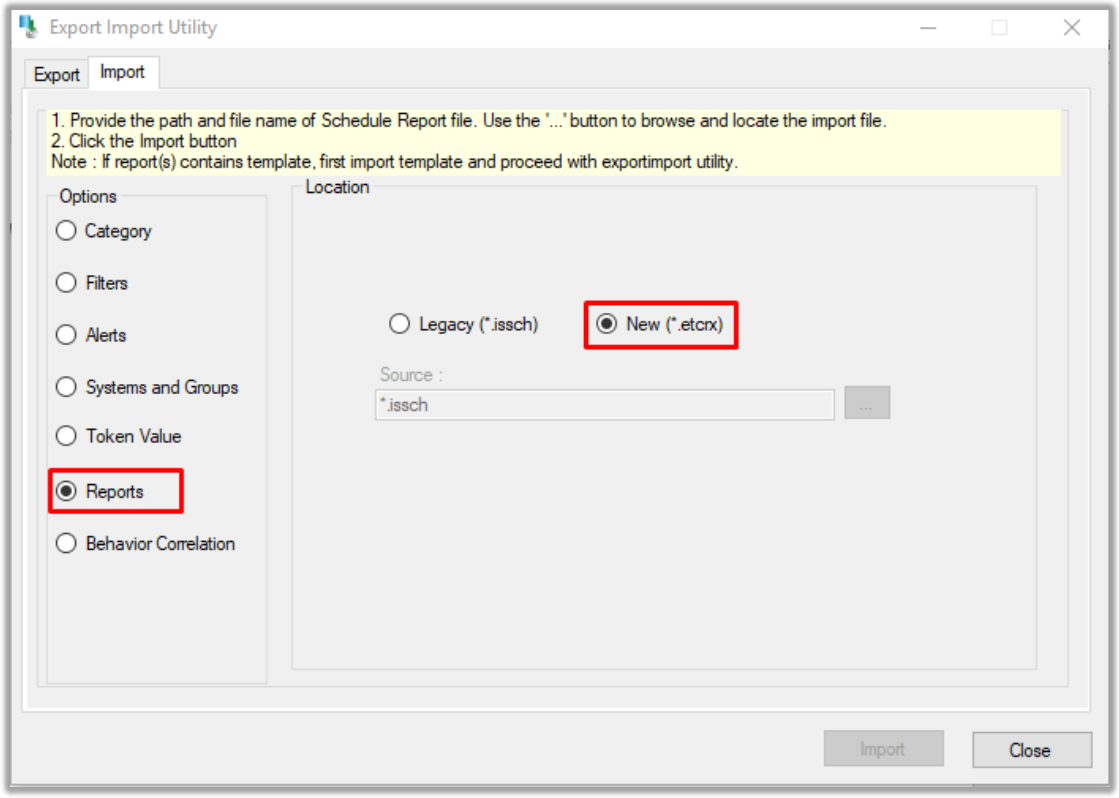

Figure 13

2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click the "**Select File**" button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g. "Reports_Solaris.etcrx".**

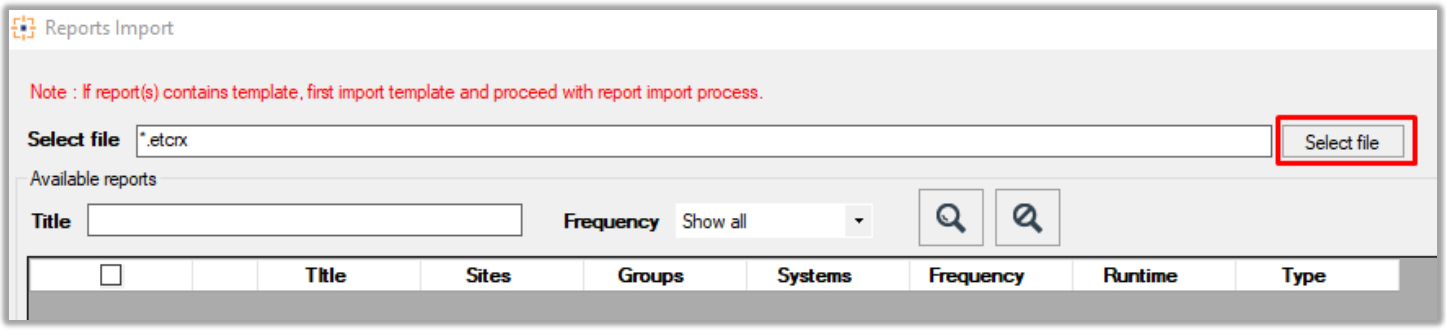

Figure 14

3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click the **Import** button.

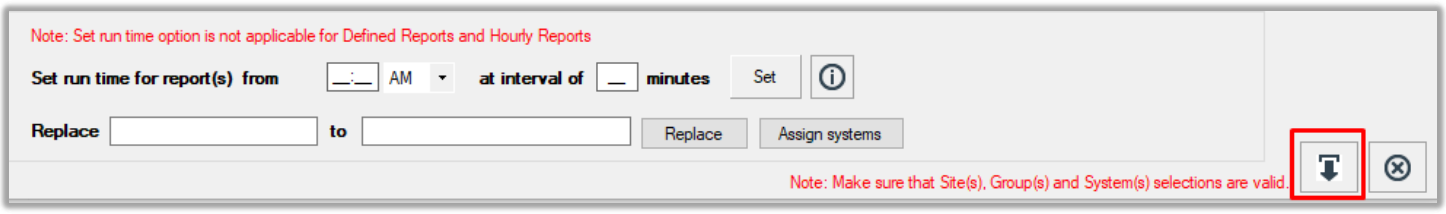

Figure 15

EventTracker displays a success message:

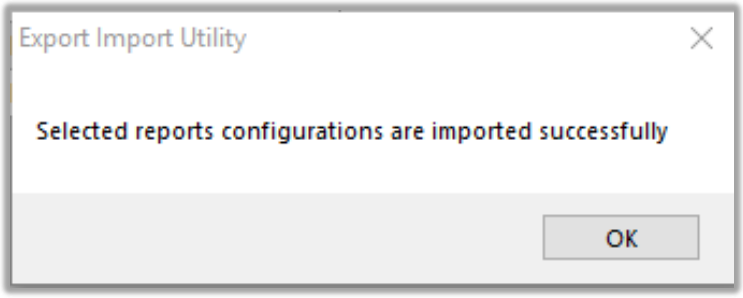

Figure 16

5.4 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

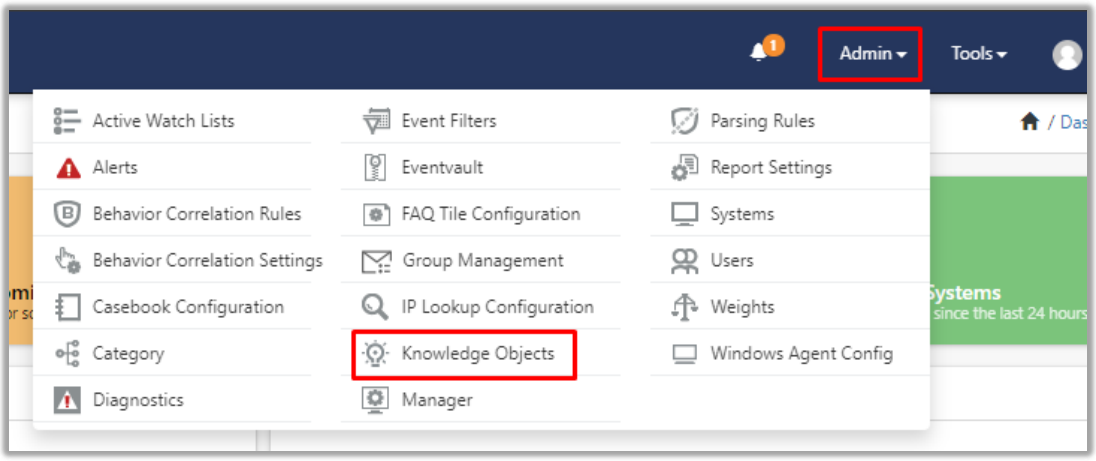

Figure 17

2. Next, click the **"import object"** icon:

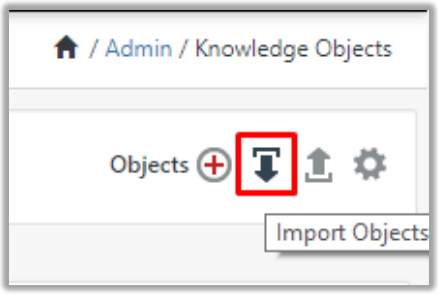

Figure 18

3. A pop-up Solaris will appear, click "**Browse**" in that and navigate to the knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g. "KO_Solaris.etko"** and then click "**Upload**" button.

Figure 19

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the "**Import**" button:

Figure 20

5.5 Alerts

1. Click **Alert** option, and then click the browse  button
2. Navigate to the location having a file with the extension **".isalt**" and then click on the "**Import**" button:

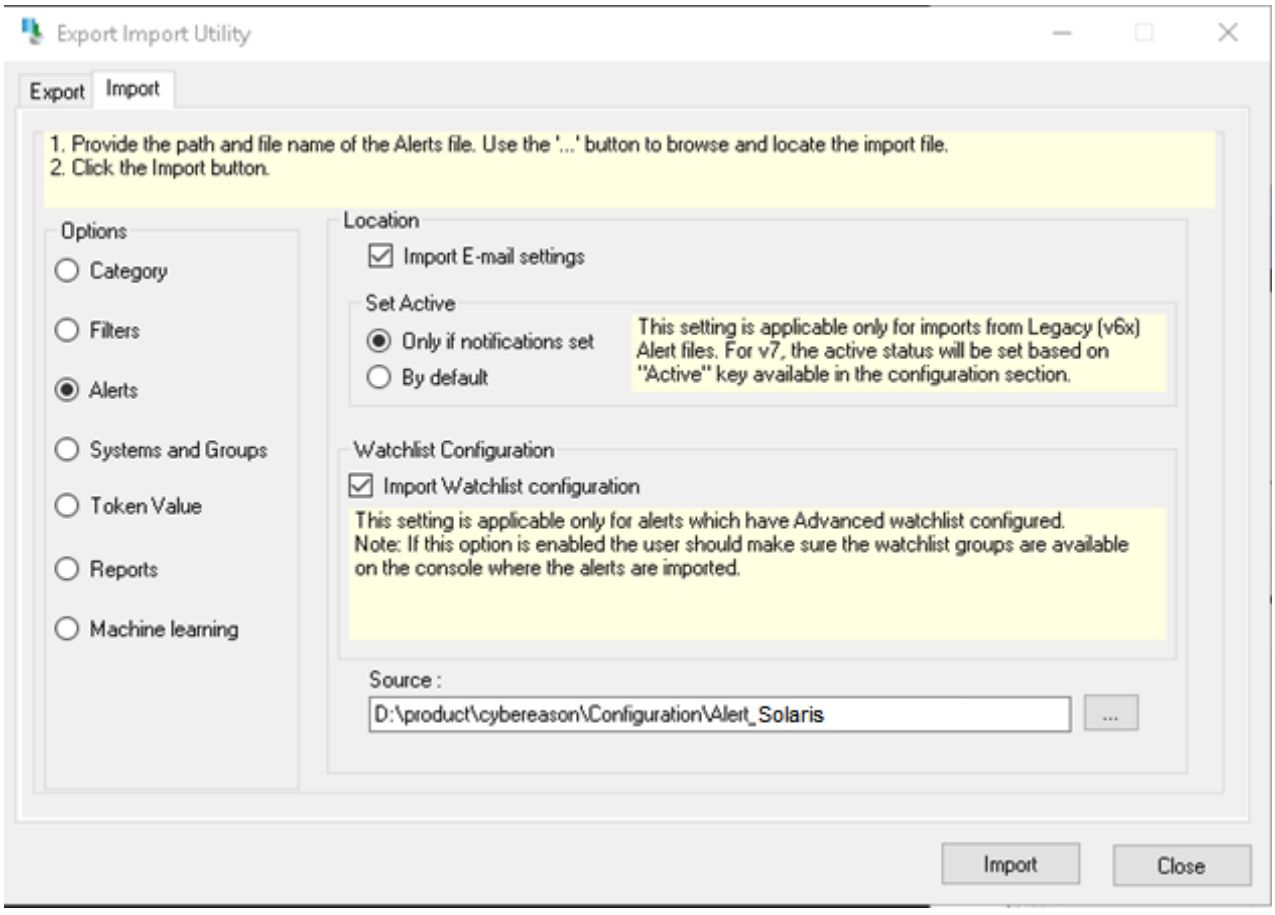

Figure 21

EventTracker displays a success message:

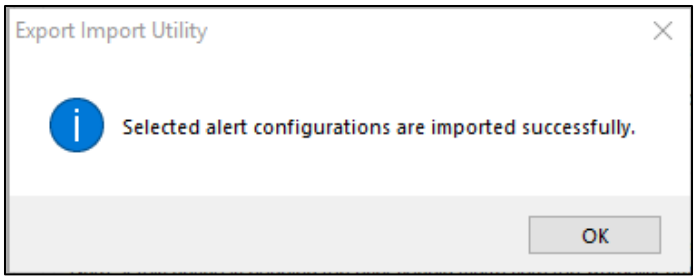

Figure 22

5.6 Dashboards

1. Login to the **EventTracker web interface**.
2. Navigate to **Dashboard → My Dashboard**.
3. In "My Dashboard", Click **Import Button**:

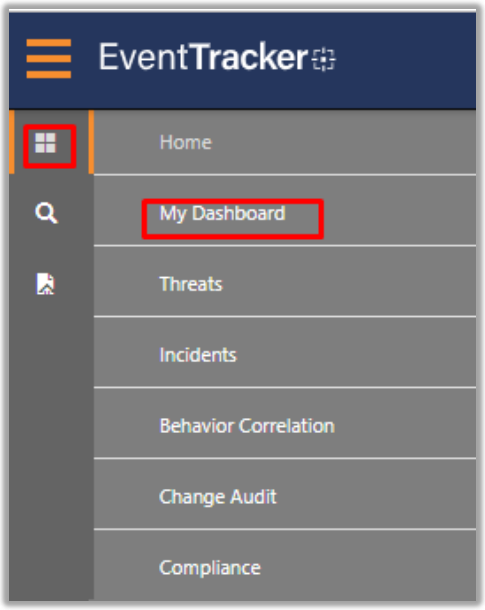

Figure 23

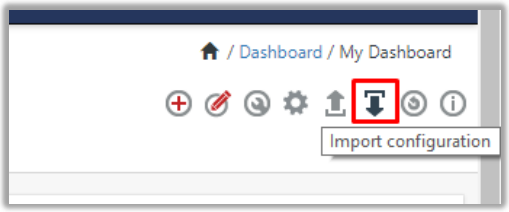

Figure 24

4. Select the **browse** button and navigate to the knowledge pack folder (type **"C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs"** in the navigation bar) where "**.etwd**", **e.g.** "**Dashboard_Solaris.etwd**" is saved and click on "**Upload**" button.

5. Wait while EventTracker populates all the available dashboards. Now, choose "**Select All**" and click on **"Import"** Button.

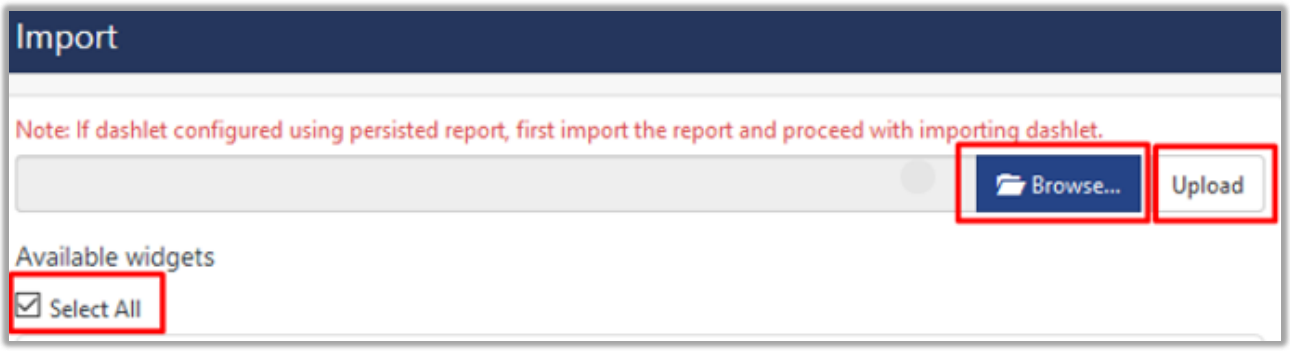

Figure 25

Figure 26

6. Verifying knowledge pack in EventTracker

6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **"Solaris"** group folder to view the imported categories:

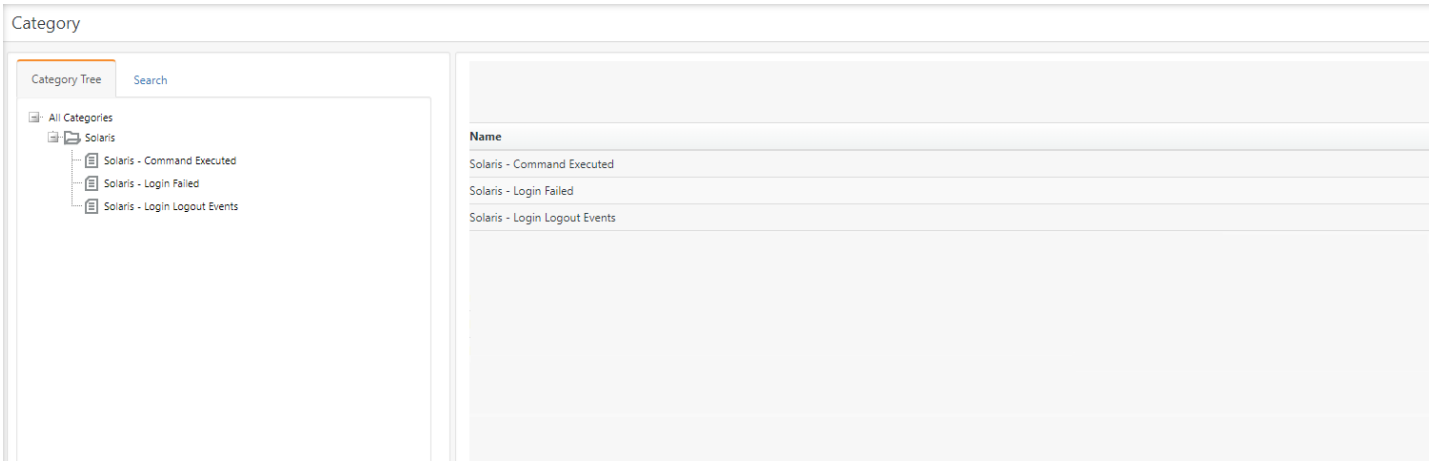

Figure 27

6.2 Token Template

1. Login to the **EventTracker.**
2. Click on **Admin >> Parsing Rules**.

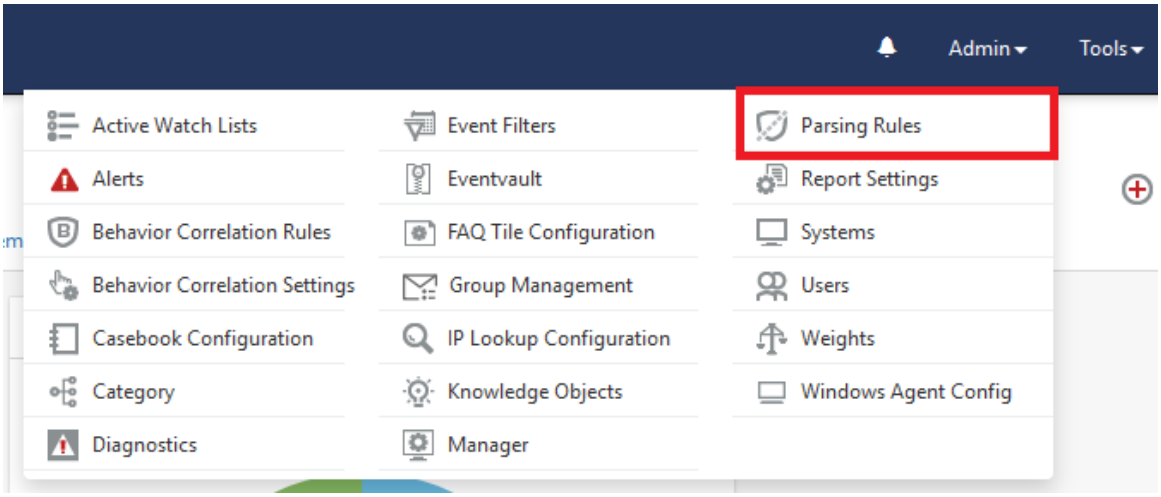

Figure 28

3. Click on **Template** and search for **Solaris.**

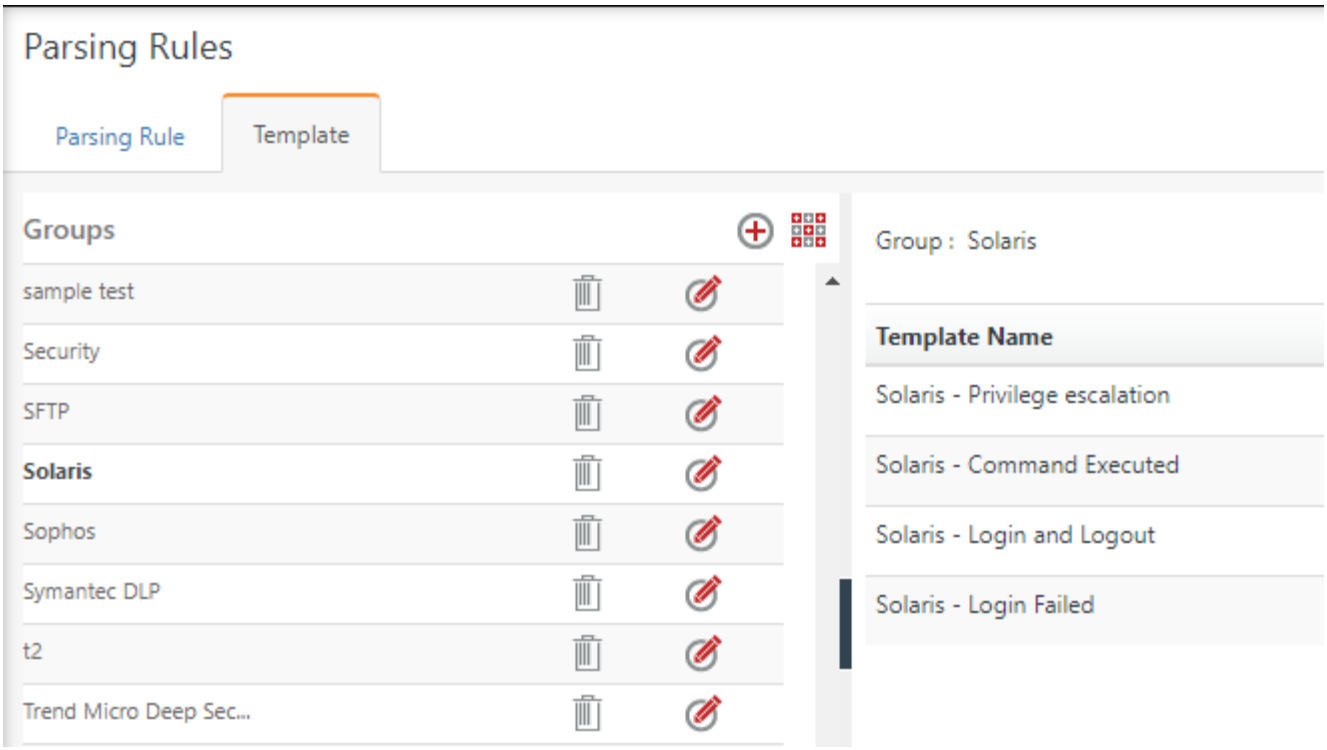

Figure 29

6.3 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.

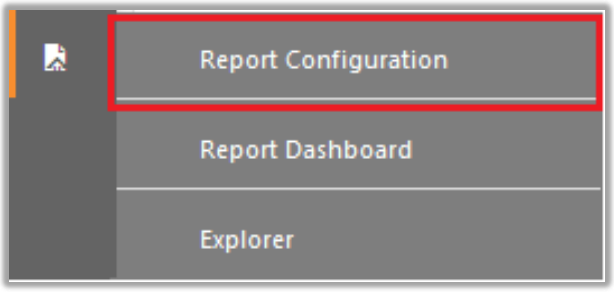

Figure 30

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **"Solaris"** group folder to view the imported reports.

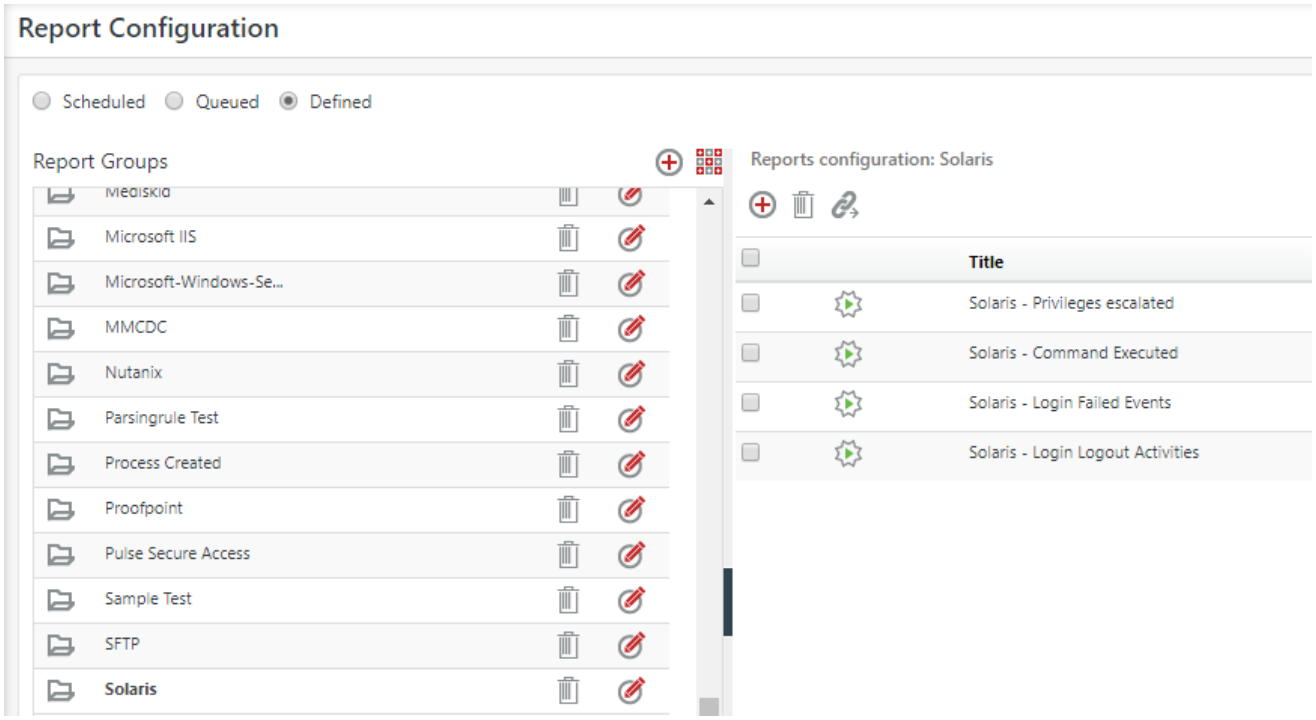

Figure 31

6.4 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **"Solaris"** group folder to view the imported Knowledge objects.

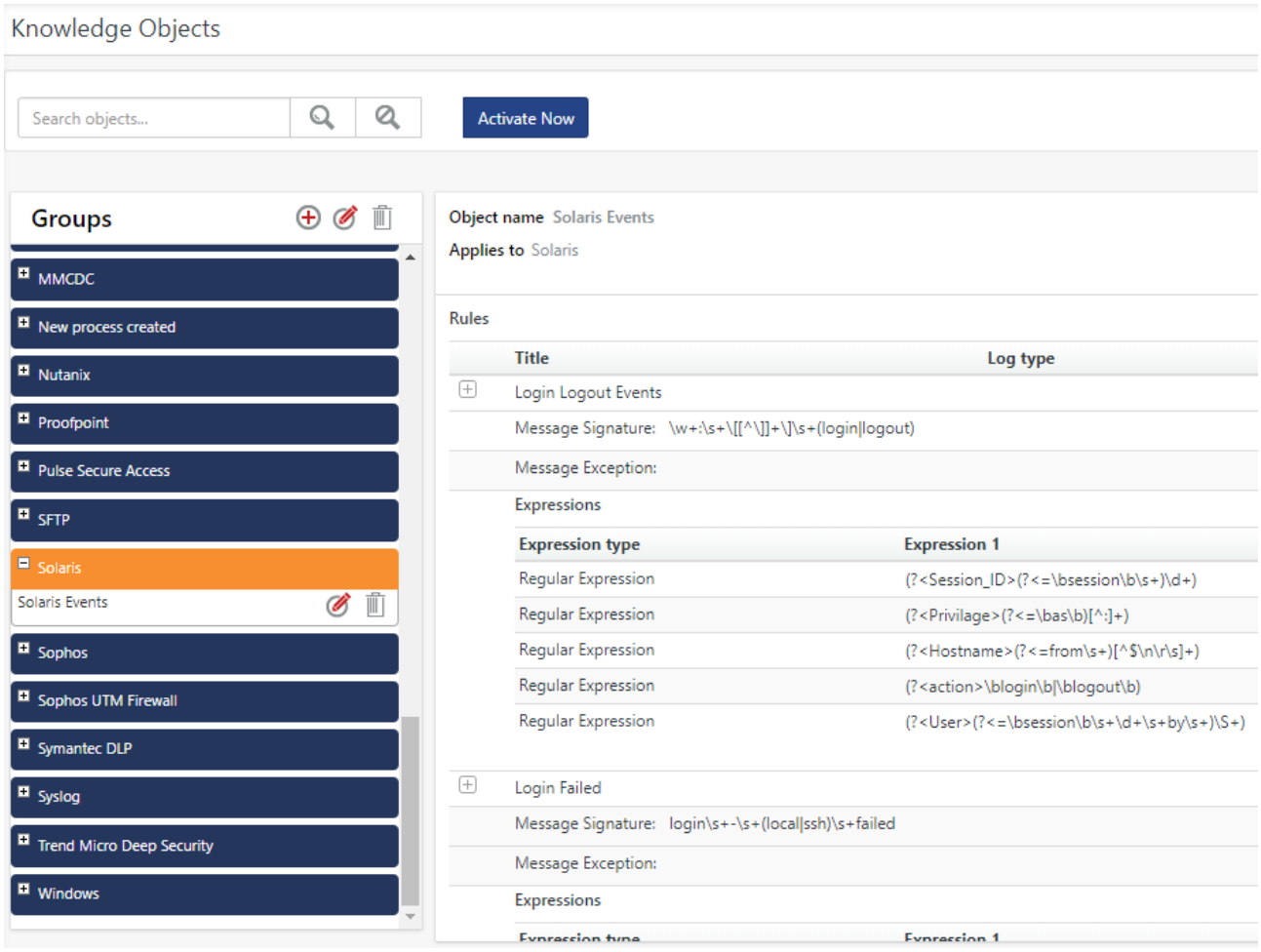

Figure 32

6.5 Dashboards

1. In the EventTracker web interface, Click on Home Button and select "**My Dashboard**".

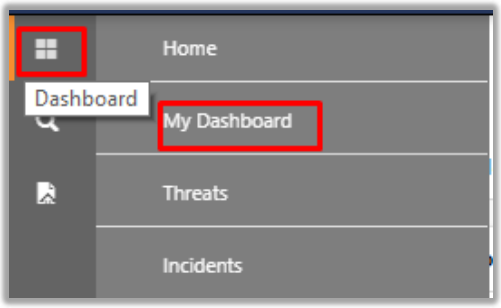

Figure 33

2. In "**Solaris"** dashboard you should be now able to see something like this:

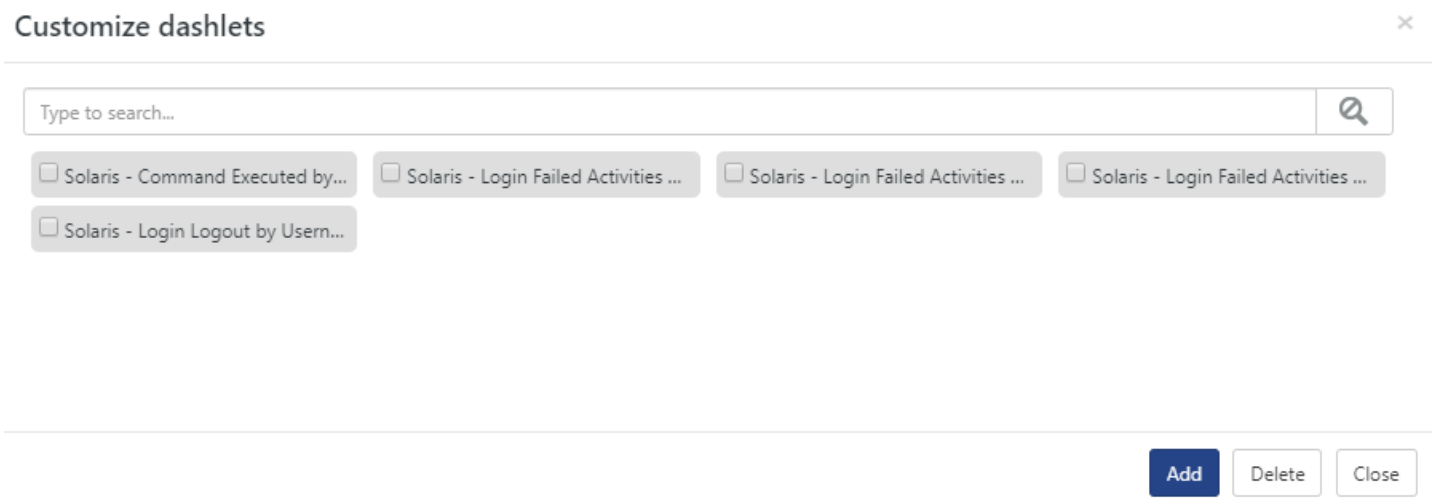

Figure 34