

Integrate Solaris

EventTracker v9.0 and above

Abstract

This guide helps you in configuring **Solaris** and **EventTracker** to receive Solaris'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.

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

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

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview.....	3
2. Prerequisites.....	3
3. Configuring Solaris to forward logs to EventTracker	3
4. EventTracker Knowledge Pack	4
4.1 Saved Searches	4
4.2 Reports.....	5
4.3 Alerts.....	5
4.4 Dashboards	5
5. Importing knowledge pack into EventTracker	7
5.1 Categories	8
5.2 Token Template	9
5.3 Flex Reports	10
5.4 Knowledge Objects	11
5.5 Alerts.....	13
5.6 Dashboards	14
6. Verifying knowledge pack in EventTracker	15
6.1 Categories	15
6.2 Token Template	16
6.3 Flex Reports	17
6.4 Knowledge Objects	18
6.5 Dashboards	19

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>.

```
#
# Copyright (c) 1991, 2014, Oracle and/or its affiliates. All rights reserved.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (') names
# that match m4 reserved words. Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice          /dev/sysmsg
*.err;kern.debug;daemon.notice;auth.none;mail.crit /var/adm/messages

# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
*. * @ <EventTracker IP>
audit.* @ <EventTracker IP>
mail.debug                               ifdef('LOGHOST', /var/log/syslog, @loghost)
#*. * /var/adm/auditlog
#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef('LOGHOST', ,
user.err          /dev/sysmsg
user.err          /var/adm/messages
user.alert       `root, operator'
user.emerg       *
)
)
```

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

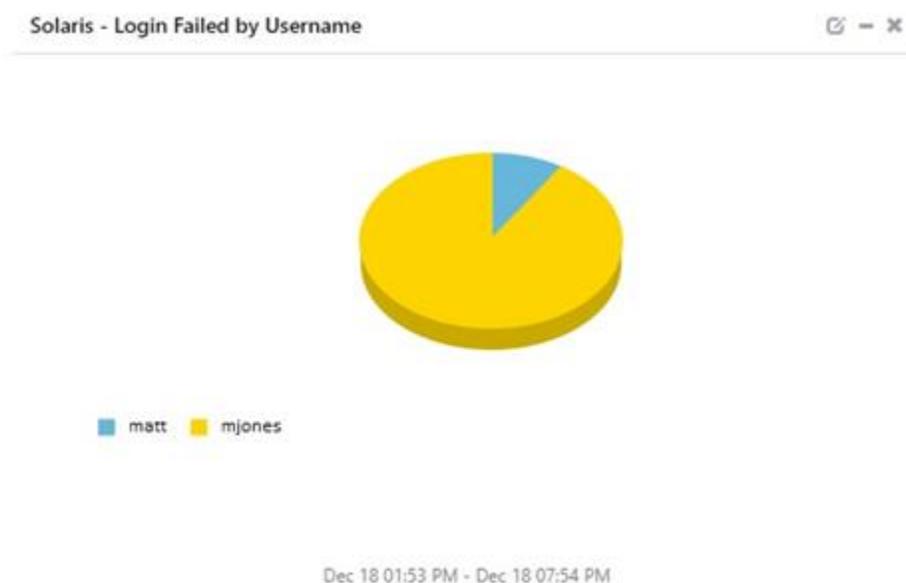


Figure 2

- Solaris – Login and logout by username.

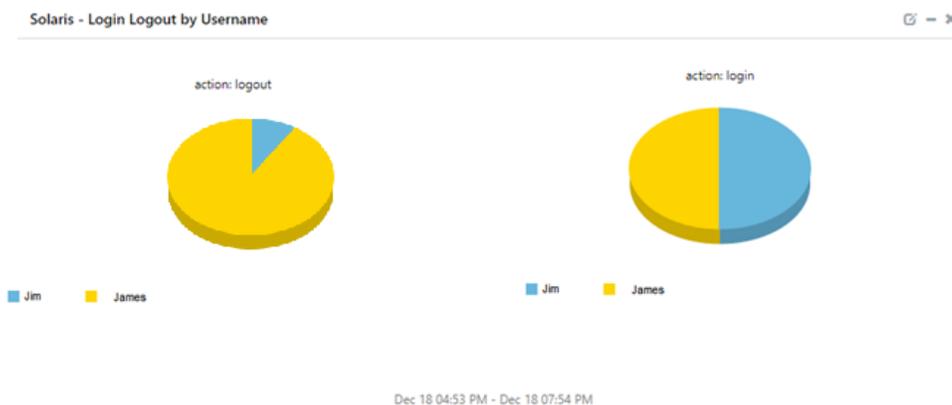


Figure 3

- Solaris – Command executed by username.

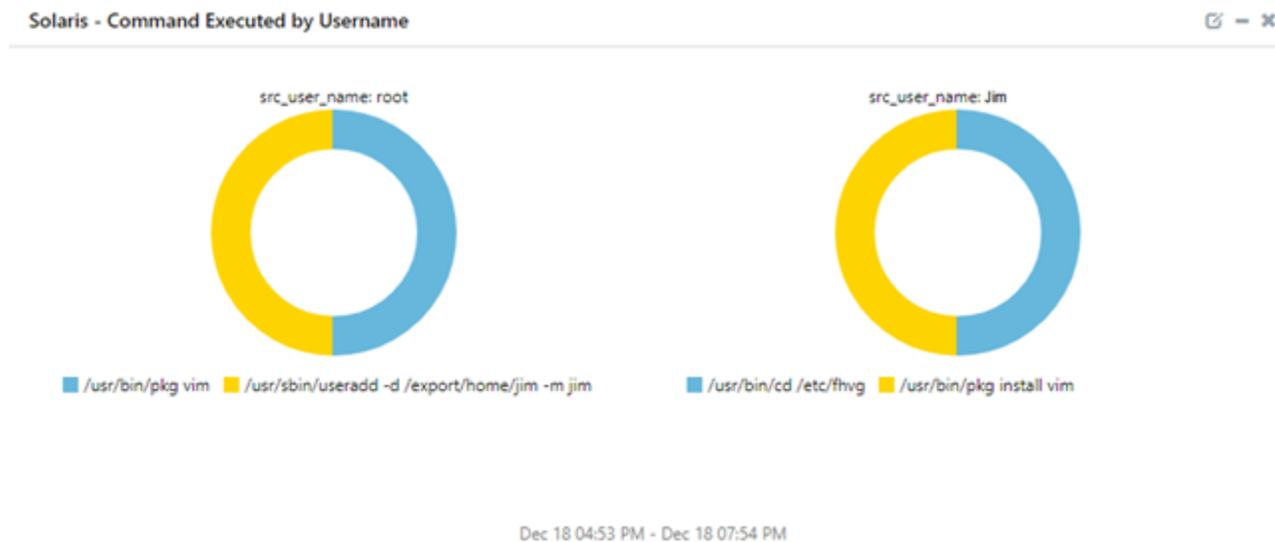


Figure 4

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**.

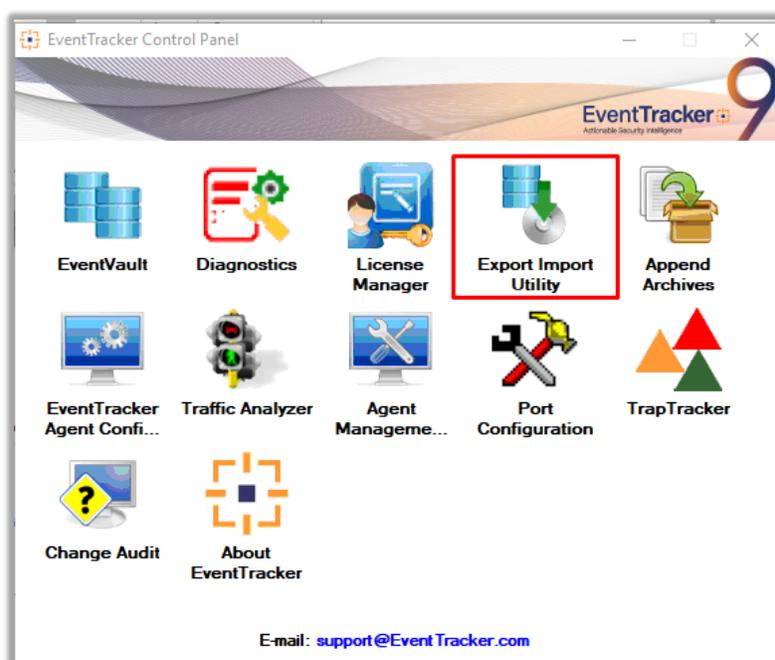


Figure 5

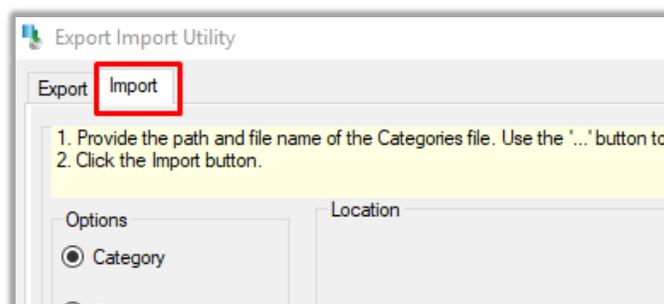


Figure 6

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:

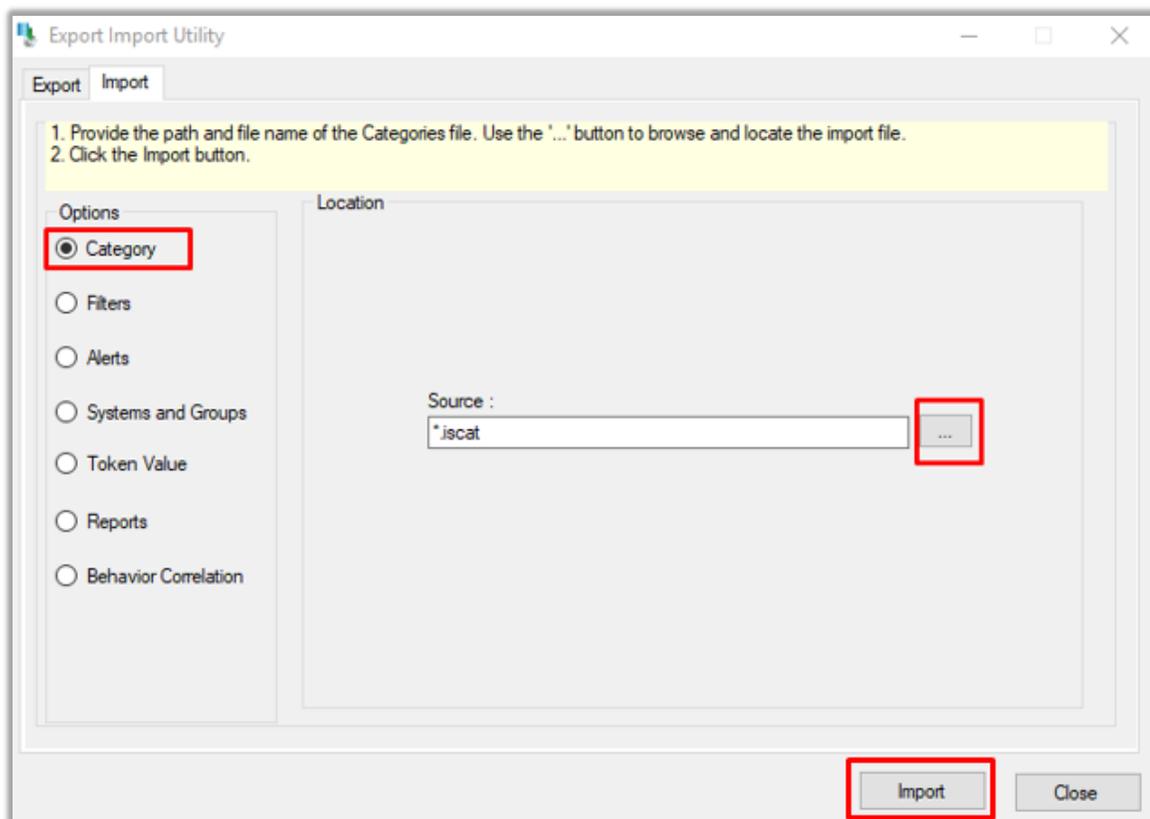


Figure 7

EventTracker displays a success message:

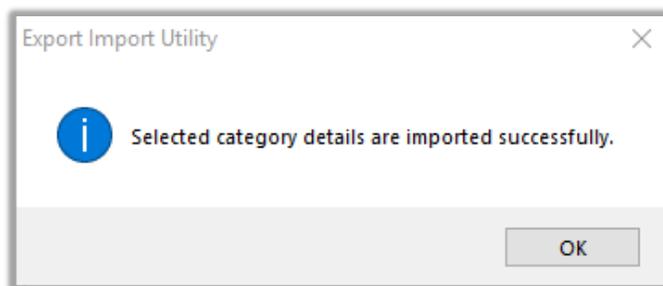


Figure 8

5.2 Token Template

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

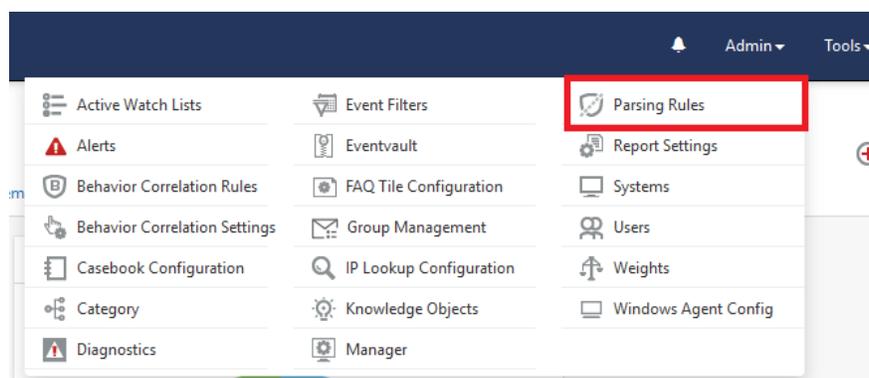


Figure 9

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

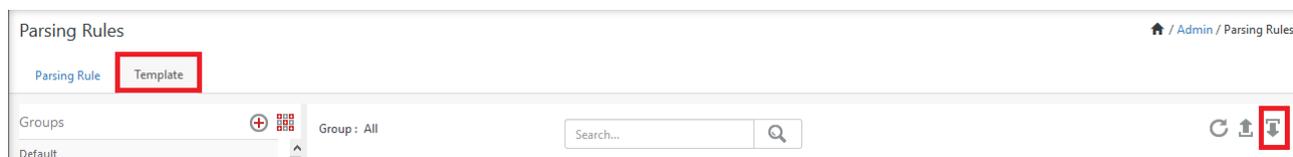


Figure 10

4. Locate the **“.ettd”** file and click on **import**.

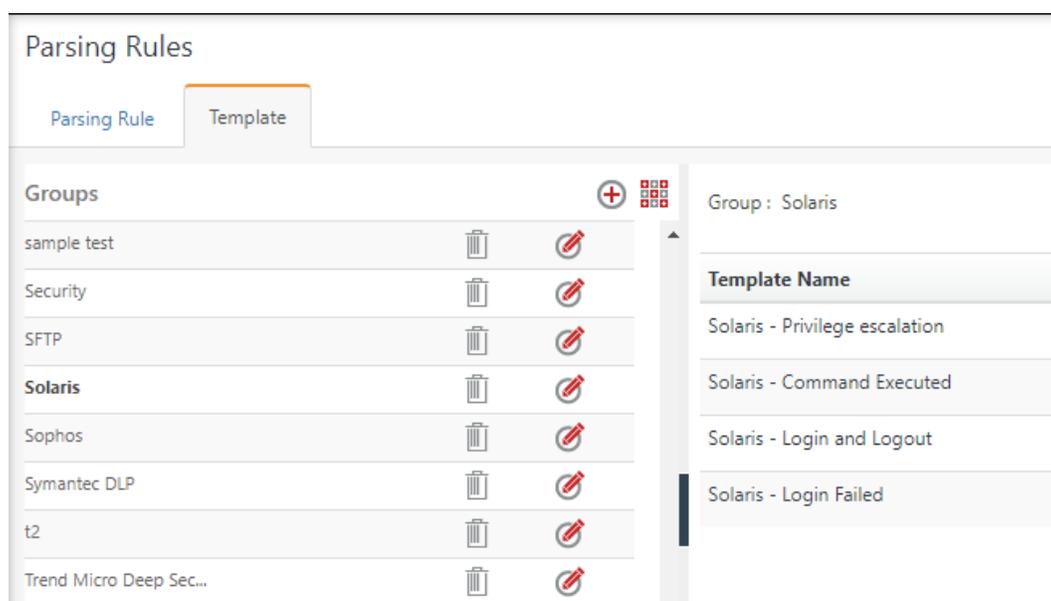


Figure 11

5. Templates are imported now successfully.

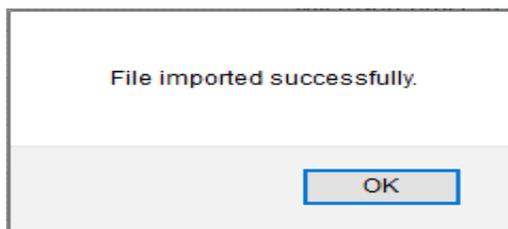


Figure 12

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)**”:

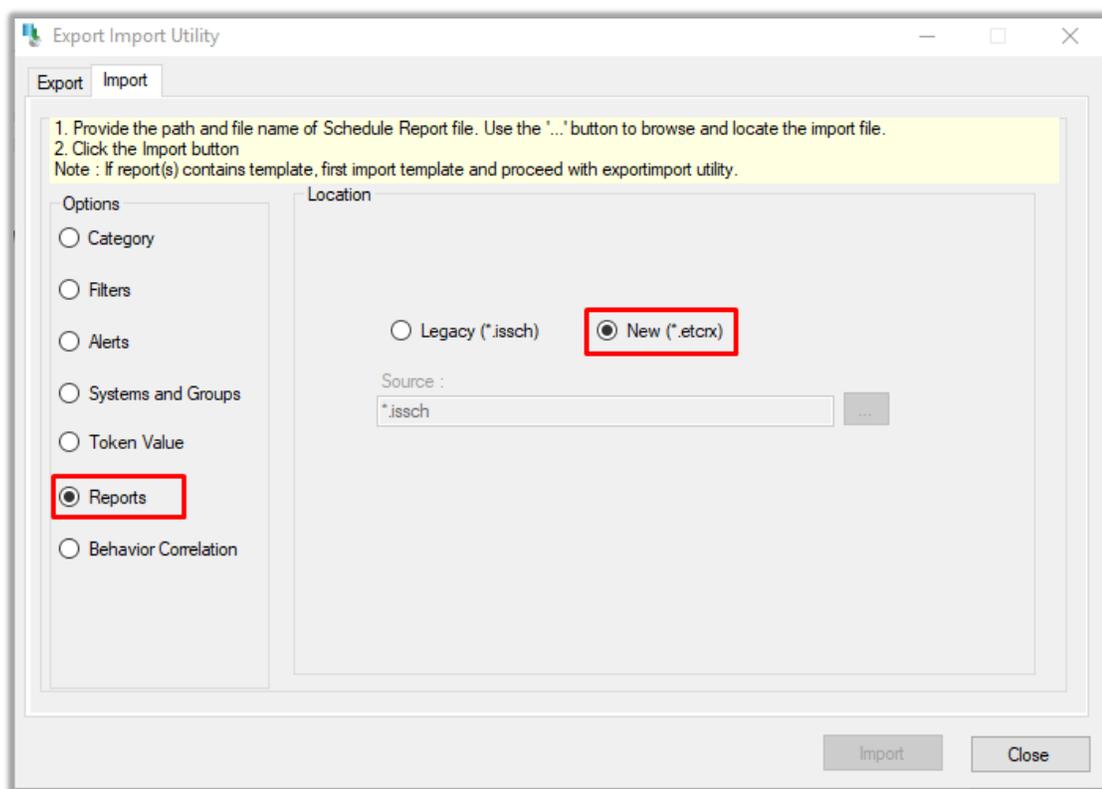


Figure 13

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**”.

Reports Import

Note : If report(s) contains template, first import template and proceed with report import process.

Select file Select file

Available reports

Title Frequency

<input type="checkbox"/>	Title	Sites	Groups	Systems	Frequency	Runtime	Type
--------------------------	-------	-------	--------	---------	-----------	---------	------

Figure 14

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

Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from AM at interval of minutes

Replace to

Note: Make sure that Site(s), Group(s) and System(s) selections are valid. 

Figure 15

EventTracker displays a success message:

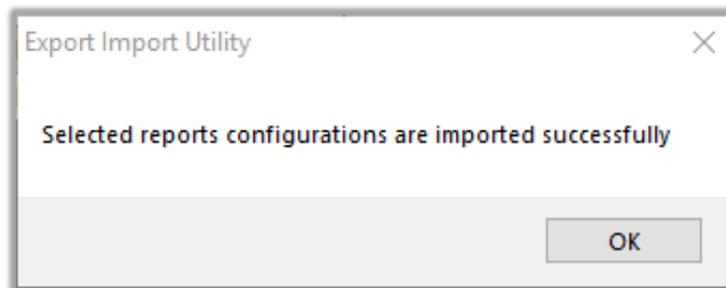


Figure 16

5.4 Knowledge Objects

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

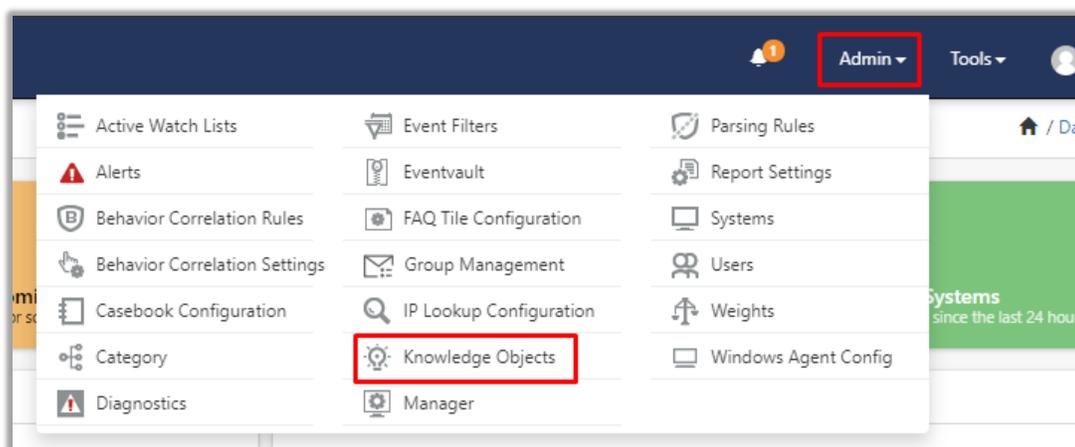


Figure 17

- Next, click the “import object” icon:

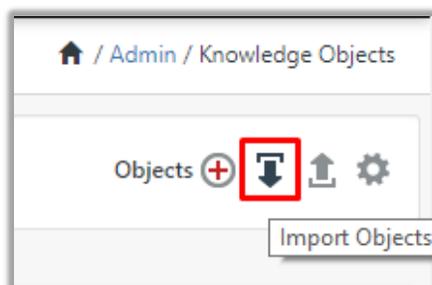


Figure 18

- 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

- 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:

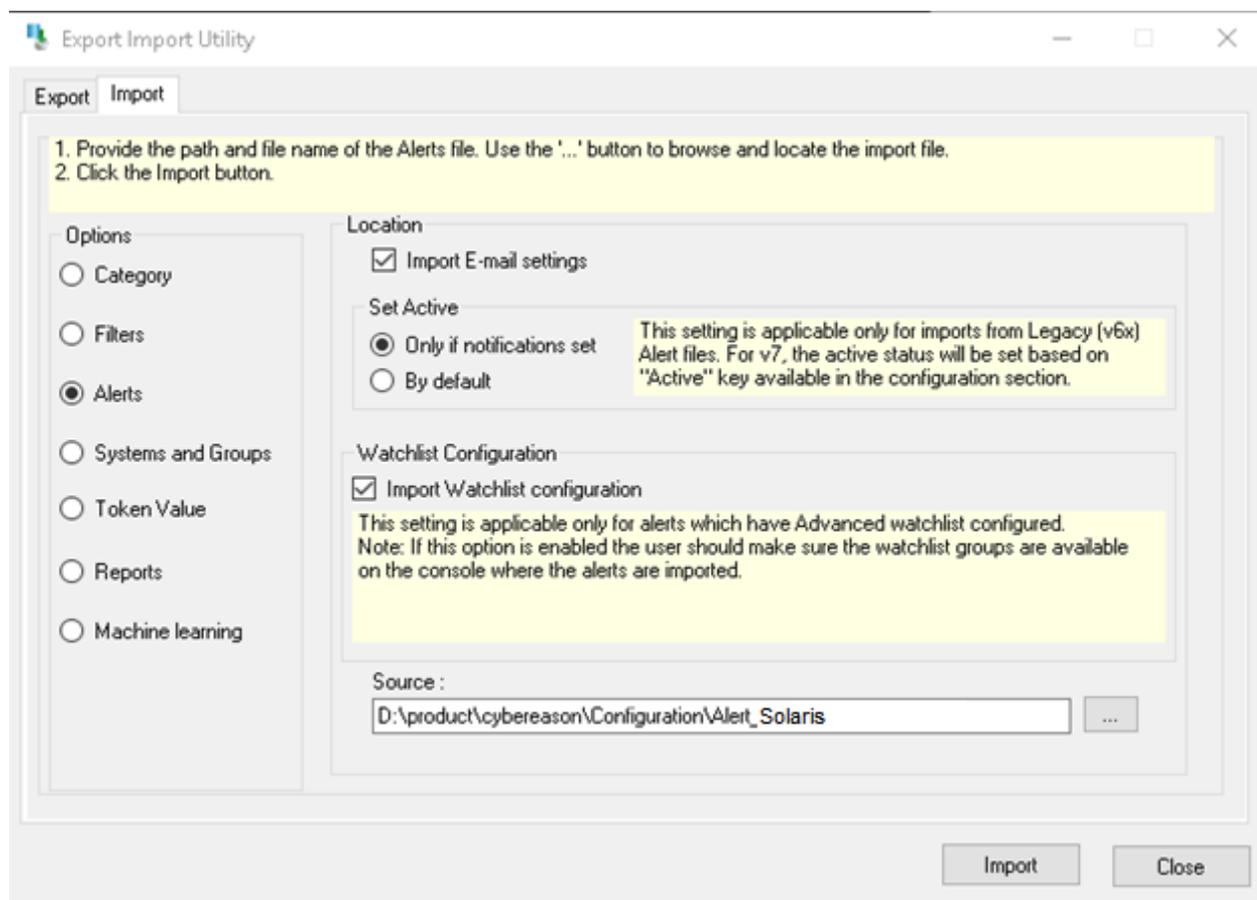


Figure 21

EventTracker displays a success message:

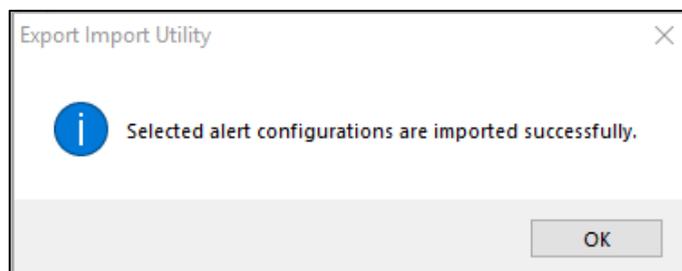


Figure 22

5.6 Dashboards

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

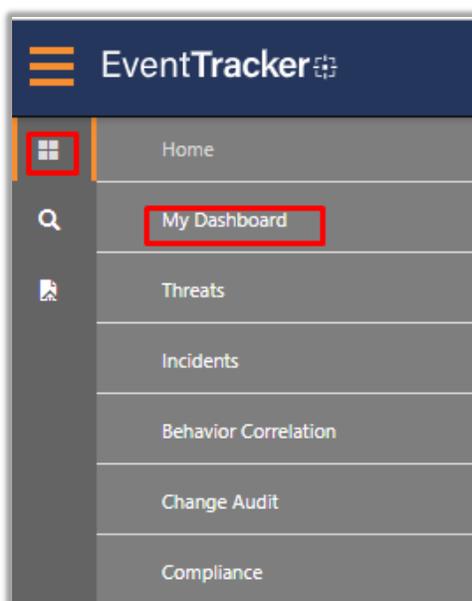


Figure 23

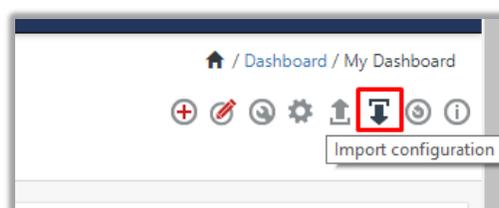


Figure 24

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.

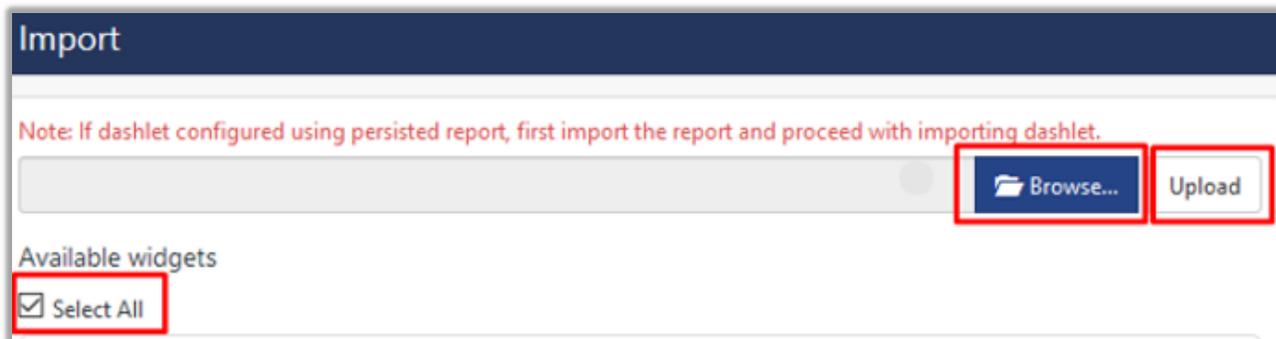


Figure 25



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:

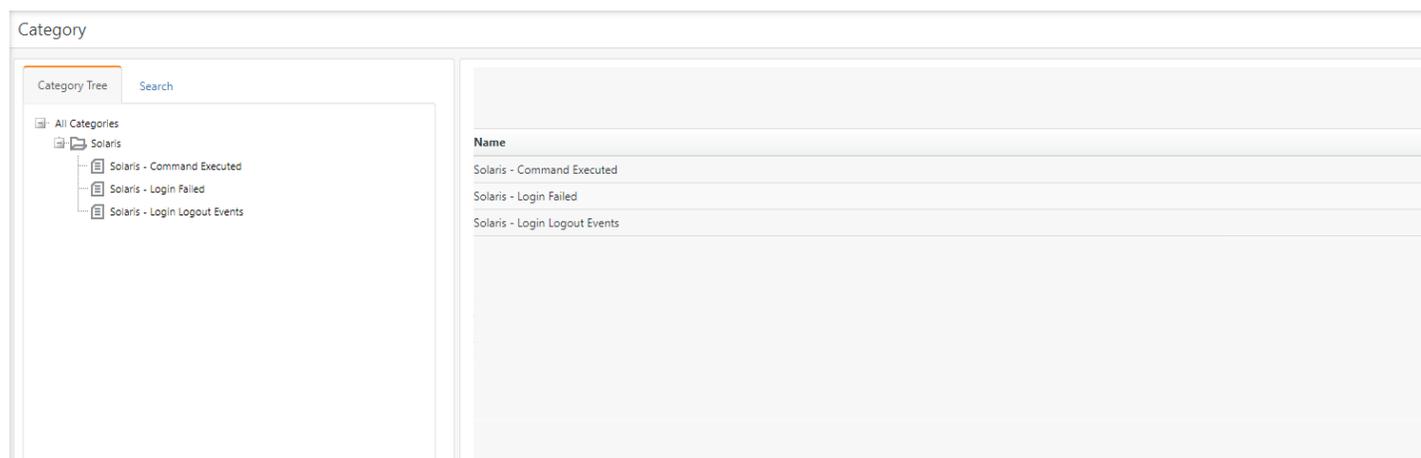


Figure 27

6.2 Token Template

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

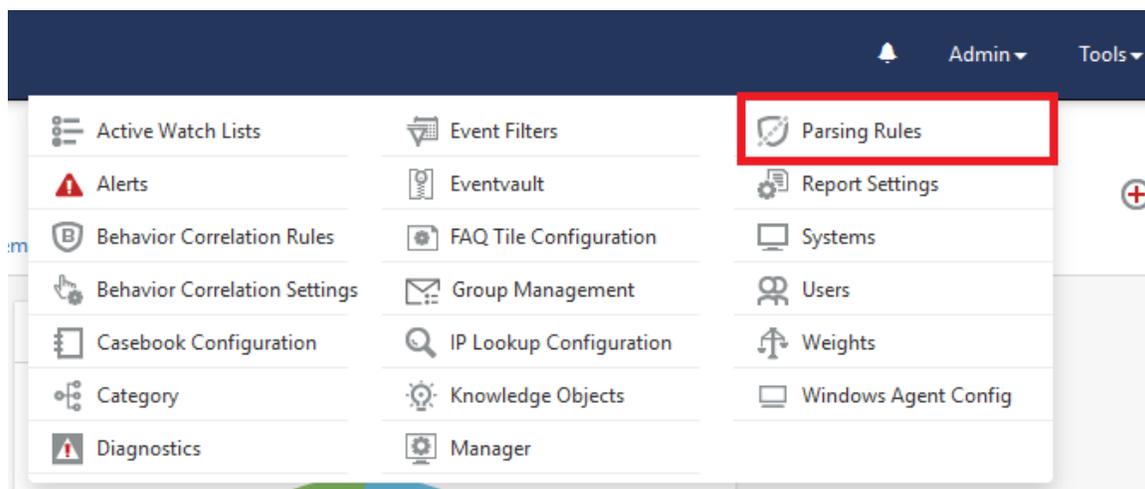


Figure 28

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

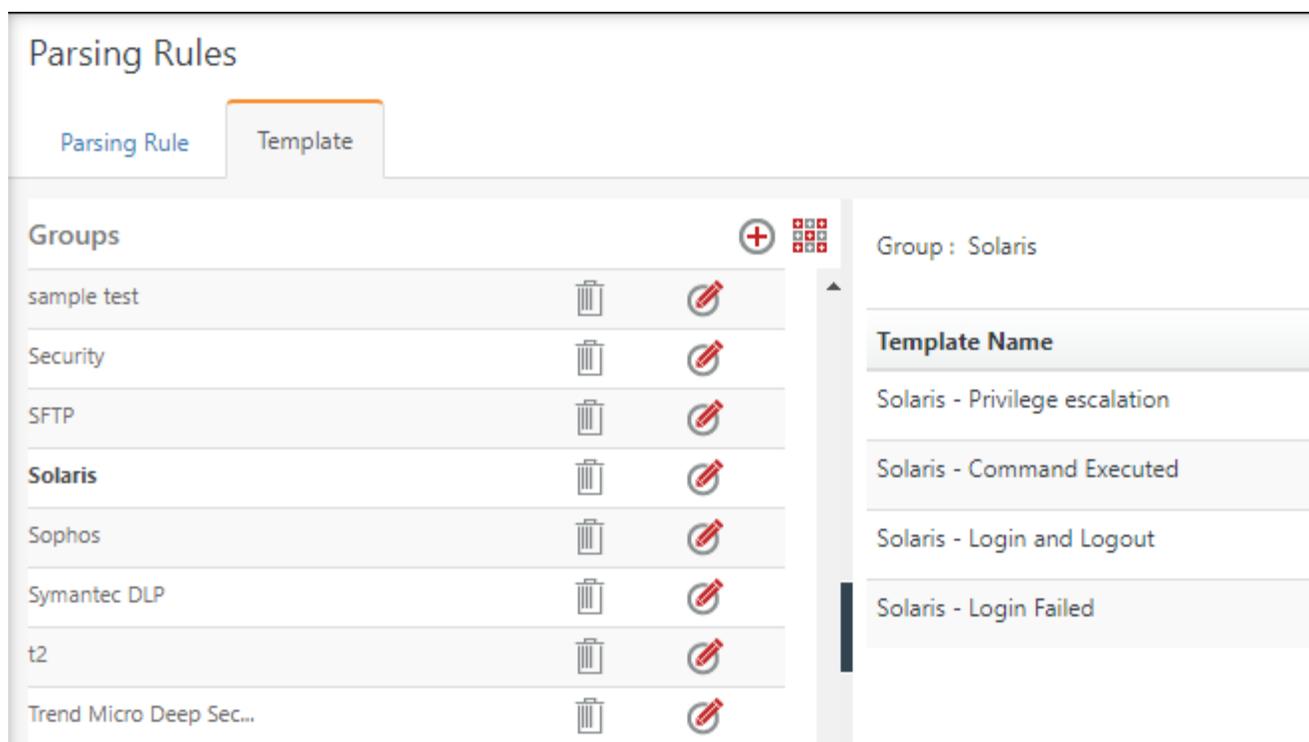


Figure 29

6.3 Flex Reports

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

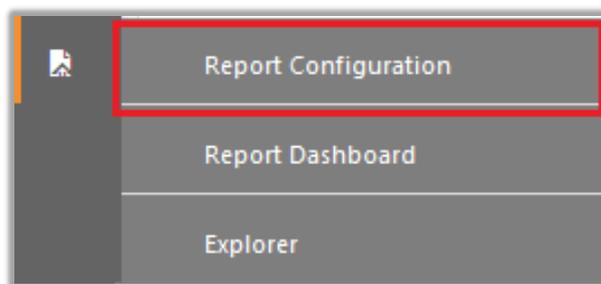


Figure 30

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

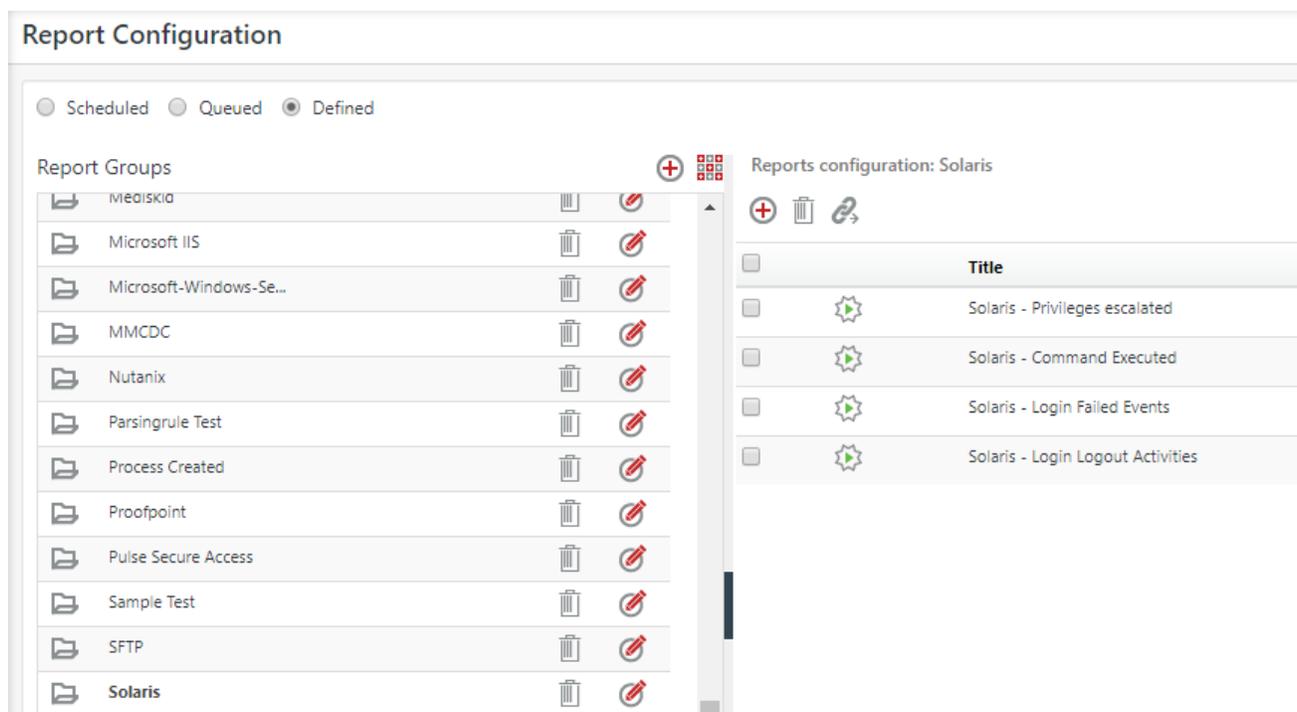


Figure 31

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.

Knowledge Objects

Search objects...

Groups

- MMCDC
- New process created
- Nutanix
- Proofpoint
- Pulse Secure Access
- SFTP
- Solaris**
- Solaris Events
- Sophos
- Sophos UTM Firewall
- Symantec DLP
- Syslog
- Trend Micro Deep Security
- Windows

Object name Solaris Events
Applies to Solaris

Rules

Title	Log type
<input type="button" value="+"/> Login Logout Events	
Message Signature: \w+\s+\[[^\]]+\]\s+(login logout)	
Message Exception:	
Expressions	
Expression type	Expression 1
Regular Expression	(? <Session_ID>(?!<=\\b\\session\\b\\s+\\)d+)
Regular Expression	(? <Privilege>(?!<=\\bas\\b\\)[^:]+)
Regular Expression	(? <Hostname>(?!<=from\\s+)[^\$\\n\\r\\s]+)
Regular Expression	(? <action>\\blogin\\b\\blogout\\b)
Regular Expression	(? <User>(?!<=\\b\\session\\b\\s+\\d+\\s+by\\s+\\)S+)
<input type="button" value="+"/> Login Failed	
Message Signature: login\\s+~\\s+(local ssh)\\s+failed	
Message Exception:	
Expressions	
Expression type	Expression 1

Figure 32

6.5 Dashboards

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

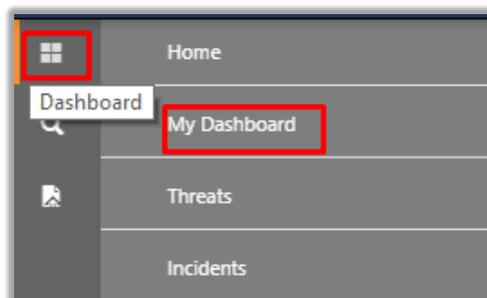


Figure 33

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

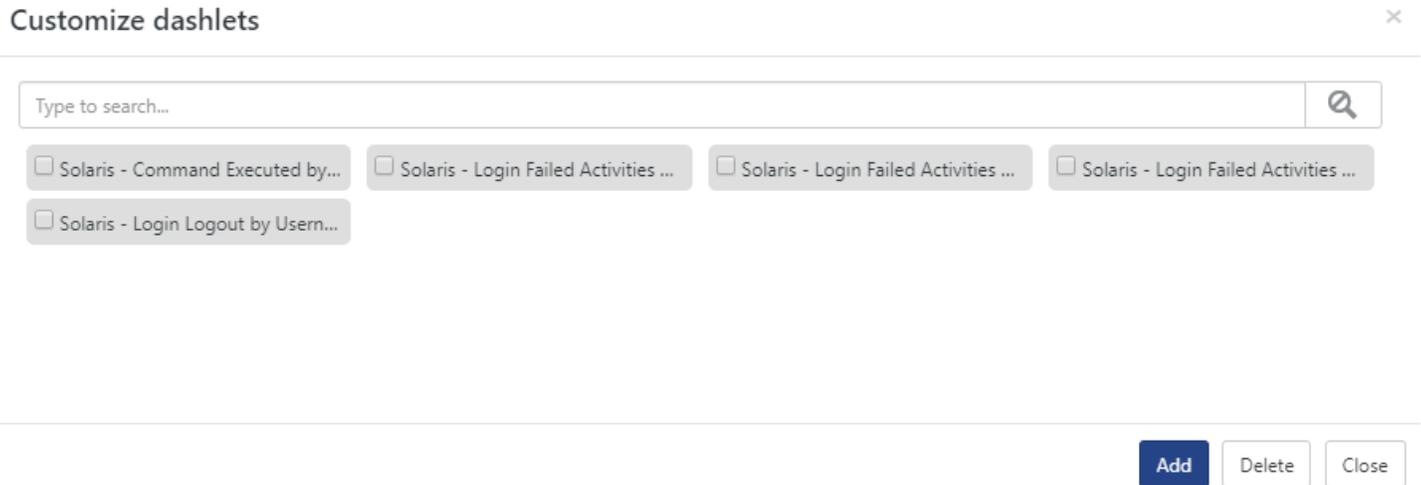


Figure 34