

Integrate Juniper JunOS

EventTracker V9.x or above

Abstract

This guide provides instructions to configure Juniper JunOS to send the syslog to EventTracker. Once syslog is being configured to send to EventTracker, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, Juniper JunOS 11.4 and later.

Audience

Administrators who are responsible for monitoring Juniper JunOS which are running 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

Abstract	1
Scope	1
Audience	1
Juniper JunOS	3
Prerequisites.....	3
Verifying Software Version on Juniper device	3
Configuring Juniper JunOS to send syslog Messages from Juniper device Using J-Web to EventTracker	4
Juniper JunOS Knowledge Pack.....	5
Alerts	5
Flex Reports	5
Dashboards.....	7
Importing Juniper JunOS knowledge pack into EventTracker.....	9
Alerts	9
Template(s).....	11
Flex Reports	13
Knowledge Objects.....	15
Dashboards.....	16
Verifying Juniper JunOS knowledge pack in EventTracker.....	19
Knowledge Object	19
Template(s).....	19
Flex Reports	20
Alerts	21

Juniper JunOS

Juniper JunOS is a free BSD-based operating system used in Juniper networks hardware routers. It is an operating system that is used in Juniper's routing, switching and security devices. EventTracker supports Juniper JunOS, it forwards the syslog messages to EventTracker. EventTracker generates the alert and report for critical events.

Prerequisites

- EventTracker v9.x should be installed.
- Juniper JunOS 11.4 and later should be installed.
- To enable logging in some features advanced licenses are required.

Verifying Software Version on Juniper device

1. Using CLI:

- a. **Login as root.**
- b. Enter the following command.
root> show version

2. Using J-Web:

- a. **Login JunOS device using J-Web.**
- b. Enter valid username and password when prompted.
- c. **J-Web Dashboard appears**, your **Software Version** is listed in the **System Identification** section below Hostname.



Figure 1

Configuring Juniper JunOS to send syslog Messages from Juniper device Using J-Web to EventTracker

Configuring Syslog logging:

Syslog is a standard for forwarding log messages in an IP network. Syslog captures the log information provided by the network devices.

1. **Log in** to the **Juniper device**.
2. Click **Configure > CLI Tools > Point** and click CLI in the Juniper device.
3. Expand **System** and click **Syslog**.
4. In the **Syslog** page, click **Add New Entry** placed next to 'Host'.
5. Enter the source **IP address** of the **EventTracker**.
6. Click **Apply** to save the configuration.

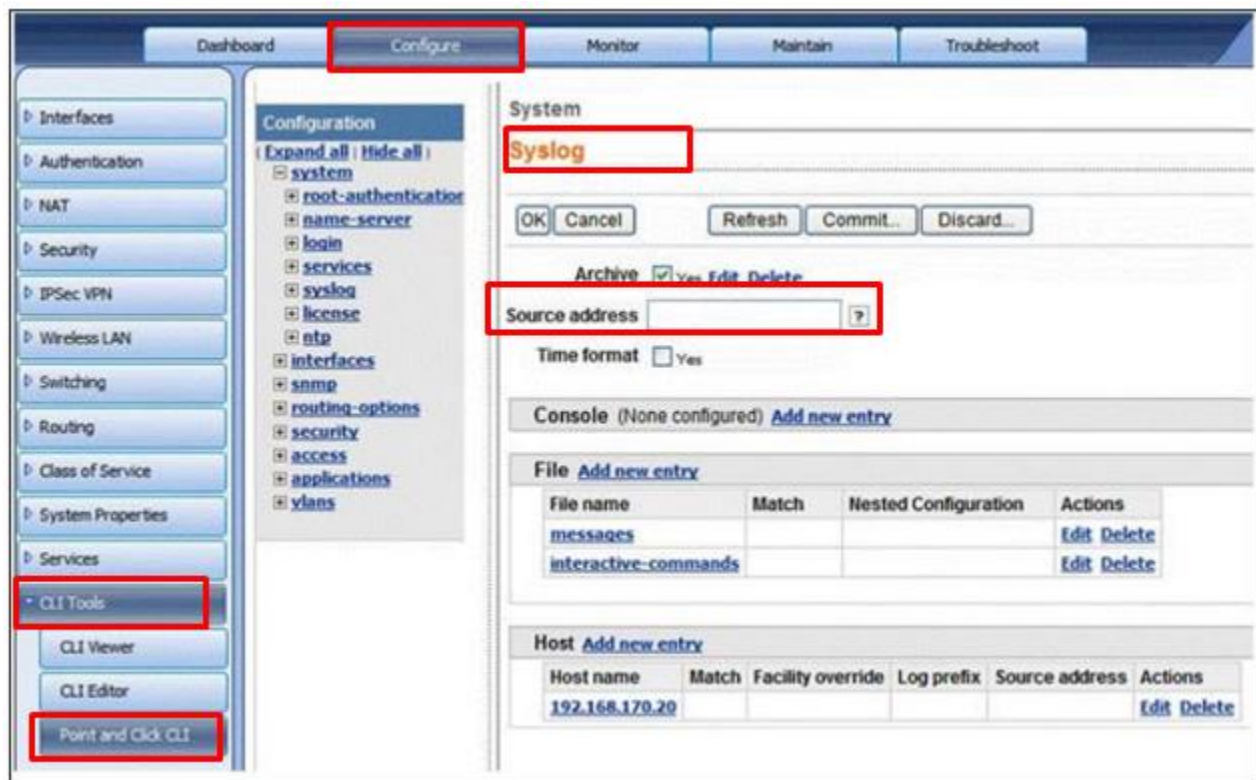


Figure 2

Juniper JunOS Knowledge Pack

Find the specified knowledge pack in the following sequences-

- Alerts
- Flex Reports
- Dashboard

Alerts

1. Juniper JunOS: Authentication failed - This alert is generated when authentication fails in JunOS.
2. Juniper JunOS: Link flap - This alert is generated when link flaps.
3. Juniper JunOS: Login failure - This alert is generated when logon fails.

Flex Reports

- **Juniper JunOS Login Activities by User** - This report provides information related to login and logon activities by a user.

LogTime	Computer	User Name	Source	Logon type
05/28/2019 05:02:51 PM	JUN	test5	192.168.3.1	
05/28/2019 05:02:51 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:56 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:56 PM	JUN	test5	192.168.3.1	
05/28/2019 05:02:58 PM	JUN	test5	192.168.3.1	
05/28/2019 05:02:58 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:59 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:59 PM	JUN	test5	192.168.3.1	
05/28/2019 05:03:00 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:03:00 PM	JUN	test5	192.168.3.1	
05/28/2019 05:03:10 PM	JUN	test5	192.168.3.1	
05/28/2019 05:03:10 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:04:47 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:04:47 PM	JUN	test5	192.168.3.1	
05/28/2019 05:04:50 PM	JUN	test5	192.168.3.1	
05/28/2019 05:04:50 PM	JUN	root8	43.229.53.79	SSHD

Figure 3

Sample Log:

```
sshd[2952]: Accepted password for root from 192.168.1.2 port 1430 ssh2 <<< Successful login
login: Login attempt for user abc from host 192.168.1.2
```


- **Juniper JunOS Web Filter details-** This report provides information related to web-filter activities (URL Filter status).

LogTime	Computer	Source Address	Source Port	Destination Address	Destination Port	Destination URL	URL Status
05/29/2019 02:50:13 PM	JUN	10.252.2.03	50227	74.125.239.155	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.02	50222	77.67.126.10	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.04	50222	77.67.126.11	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.05	50227	74.125.239.150	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.06	50222	77.67.126.12	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.07	50227	74.125.239.145	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.09	50227	74.125.239.140	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.10	50222	77.67.126.15	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.11	50227	74.125.239.166	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.12	50222	77.67.126.19	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.08	50222	77.67.126.13	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.01	50227	74.125.239.160	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:24 PM	JUN	10.252.2.02	50222	77.67.126.10	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:24 PM	JUN	10.252.2.01	50227	74.125.239.160	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:25 PM	JUN	10.252.2.12	50222	77.67.126.19	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:25 PM	JUN	10.252.2.03	50227	74.125.239.155	80	ad.doubleclick.net	BLOCKED

Figure 4

Sample Log:

```
Oct 25 16:08:54 rng-aa RT_UTM: WEBFILTER_URL_BLOCKED: WebFilter: ACTION="URL Blocked"
10.252.2.01(50227)->74.125.239.160(80) CATEGORY="Enhanced_Advertisements" REASON="BY_PRE_DEFINED"
PROFILE="junos-wf-enhanced-default" URL=ad.doubleclick.net
OBJ=/adj/espn.us.com.espn/espnfrontpage;pgtyp=espnfrontpage;sp=espn;ref=other;mnr=f;pos=incontent;swid=20
b69aac-7584-4e46-b1a6-880a71f319ab;dcopt=ist;sz=300x600,300x250,1x1;tile=3;ord=3800646760
USERNAME=Test1 ROLES=N/A)
```

- **Juniper JunOS Attack Detection Details-** This report provides information related to JunOS Screen attack details activities.

LogTime	Computer	Source Address	Source Port	Address	ion Port	Protocol Type	Attack Type
05/29/2019 02:50:13 PM	JUN	10.252.2.03	50227	74.125.239.155	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:13 PM	JUN	10.252.2.02	50222	77.67.126.11	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.04	50222	74.125.239.150	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:13 PM	JUN	10.252.2.05	50227	74.125.239.145	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.06	50222	74.125.239.140	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.07	50227	74.125.239.166	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.09	50227	77.67.126.12	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:14 PM	JUN	10.252.2.10	50222	77.67.126.15	80	SESSION_LIMIT	Dst IP session limit
05/29/2019 02:50:14 PM	JUN	10.252.2.11	50227	77.67.126.13	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:14 PM	JUN	10.252.2.12	50222	74.125.239.150	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:14 PM	JUN	10.252.2.08	50222	77.67.126.19	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:14 PM	JUN	10.252.2.01	50227	74.125.239.160	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:25 PM	JUN	10.252.2.02	50222	77.67.126.10	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:25 PM	JUN	10.252.2.01	50227	74.125.239.155	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:25 PM	JUN	10.252.2.12	50222	77.67.126.11	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:25 PM	JUN	10.252.2.03	50227	77.67.126.12	80	SESSION_LIMIT	Dst IP session limit
05/29/2019 02:50:25 PM	JUN	10.252.2.04	50222	74.125.239.145	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:25 PM	JUN	10.252.2.05	50227	77.67.126.13	80	SESSION_LIMIT	Dst IP session limit
05/29/2019 02:50:25 PM	JUN	10.252.2.07	50227	74.125.239.140	80	SESSION_LIMIT	Dst IP session limit

Figure 5

Sample Log:

Apr 20 16:21:03 SRX-2 RT_IDS: RT_SCREEN_SESSION_LIMIT: Dst IP session limit! destination: 206.25.34.12, action: drop

Dashboards

- Juniper JunOS Login Activities by User:



Figure 6

- **Juniper JunOS Events Commands:**

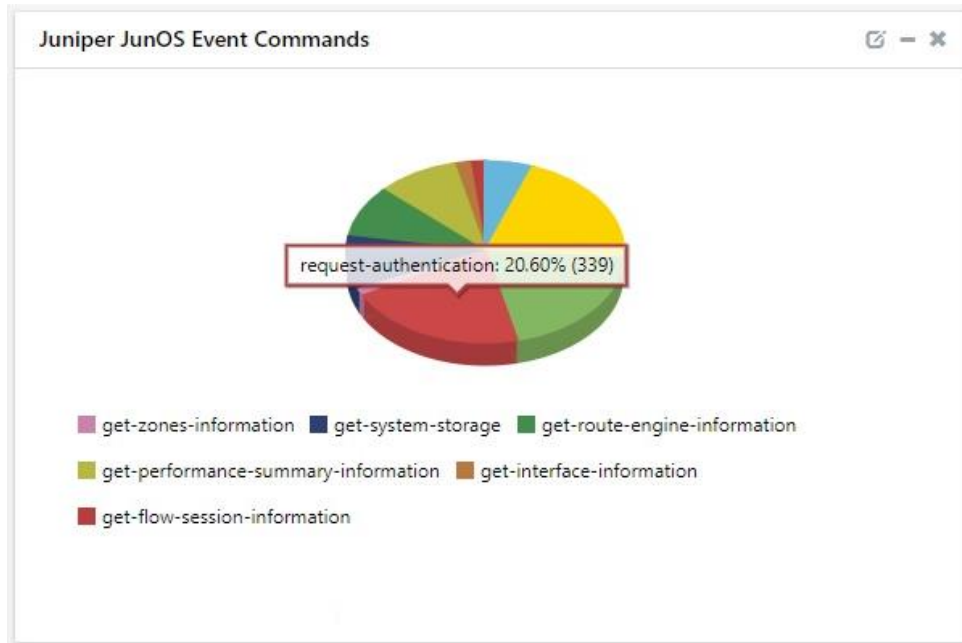


Figure 7

- **Juniper JunOS Login Failure by Users:**

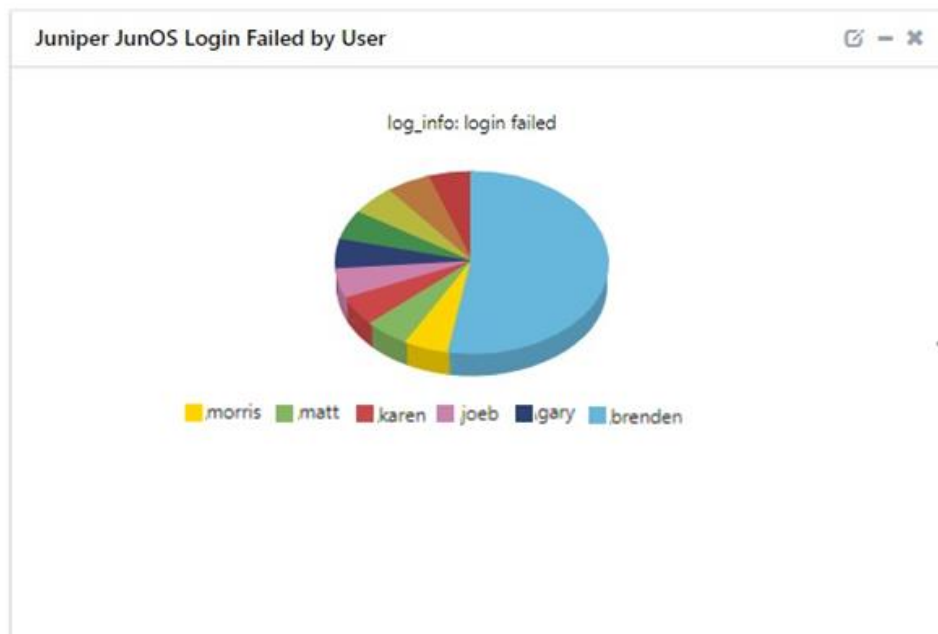


Figure 8

- **Juniper JunOS Web-filter Status:**

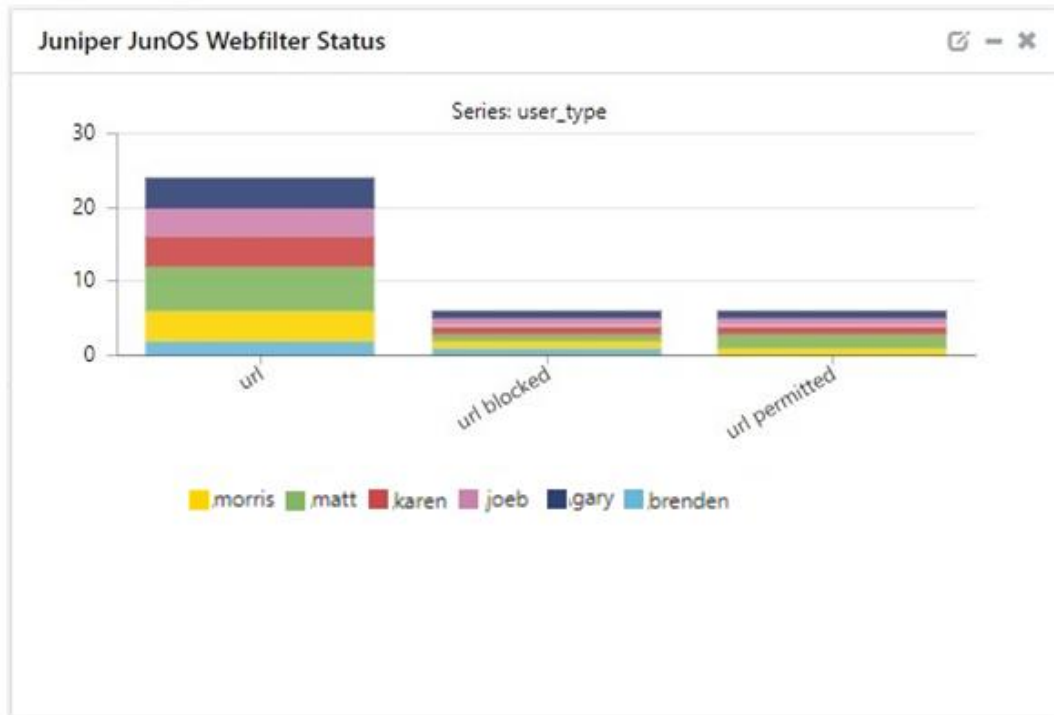


Figure 9

Importing Juniper JunOS knowledge pack into EventTracker

Find the specified knowledge pack in the following sequences-

- Alerts
- Template(s)
- Flex Reports
- Knowledge Objects
- Dashlets

Alerts

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

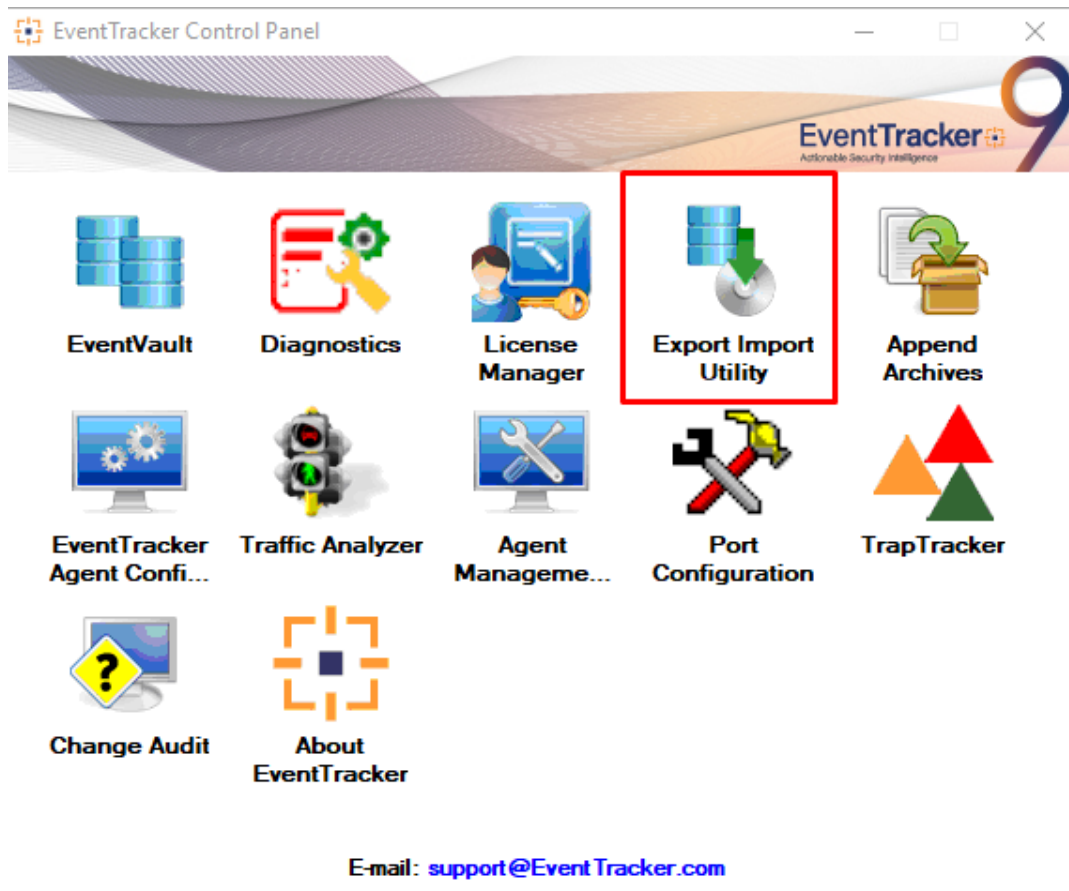


Figure 10

3. Click the **Import** tab.
4. Select the **Alert** option.
5. Click on **Browse** button and select the **file path**.
6. Click on **Import**.

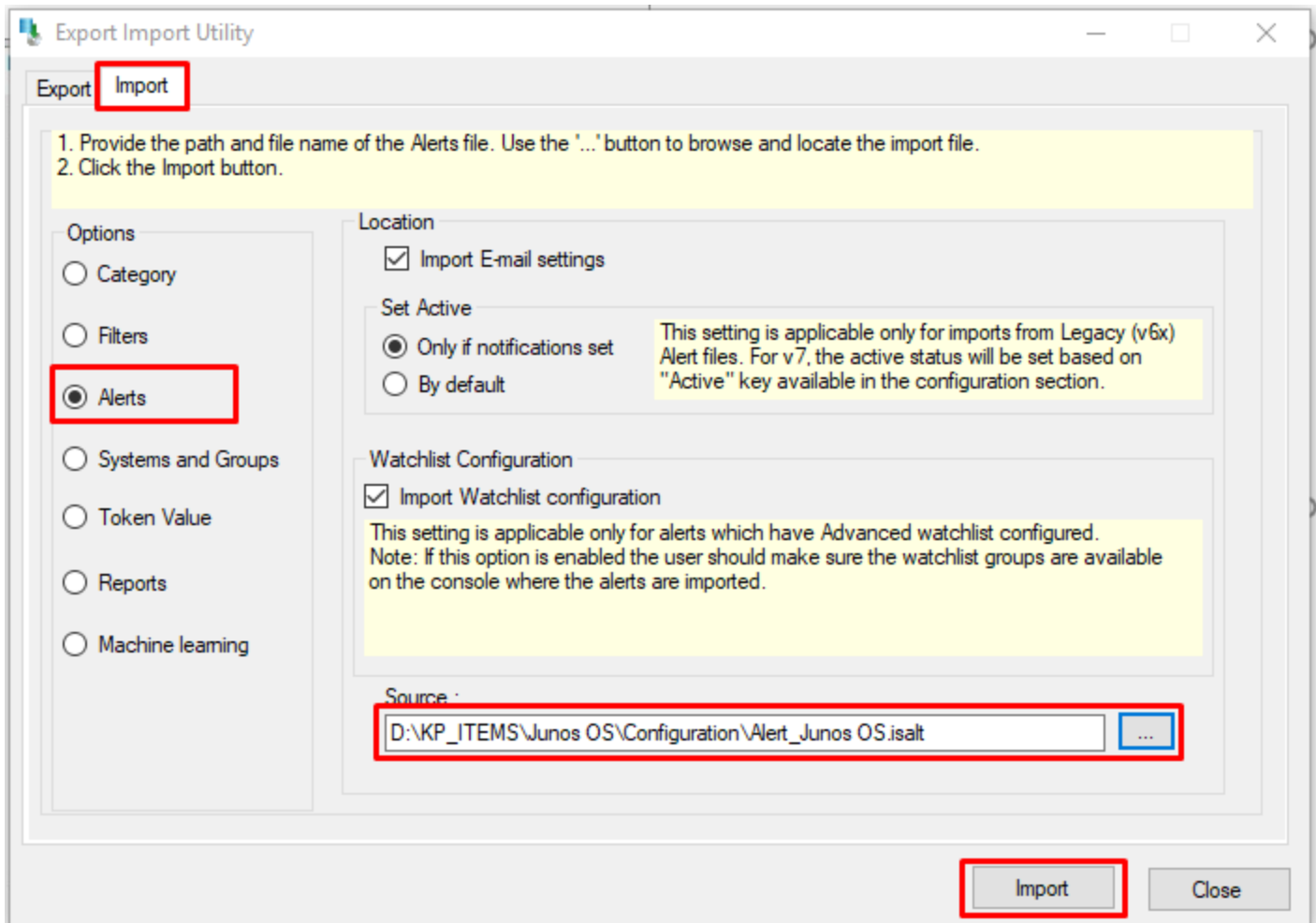


Figure 11

7. Alerts are now imported successfully.

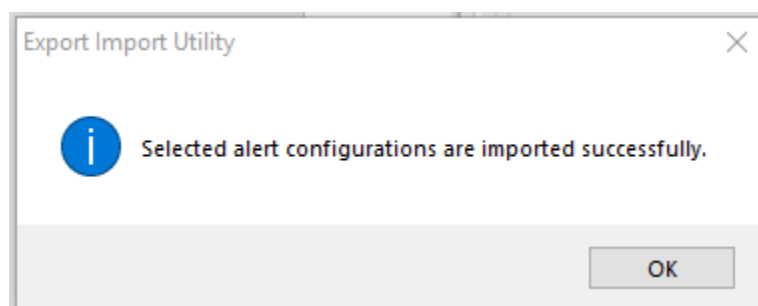


Figure 12

Template(s)

1. Login to EventTracker console.
2. Click on the **Admin** option in the **EventTracker** page and select **Parsing Rules**.

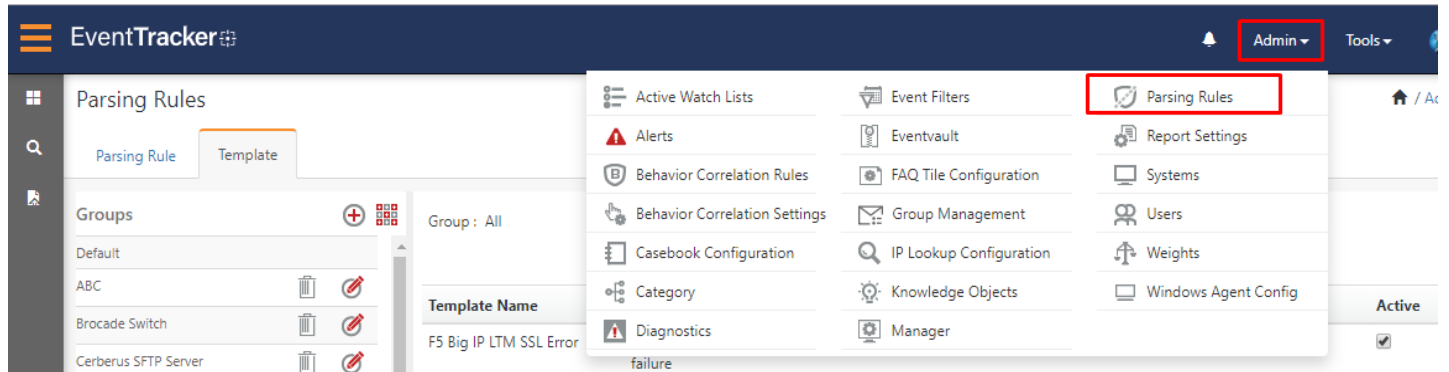


Figure 13

3. Select **Templet** and click on the **import** icon.

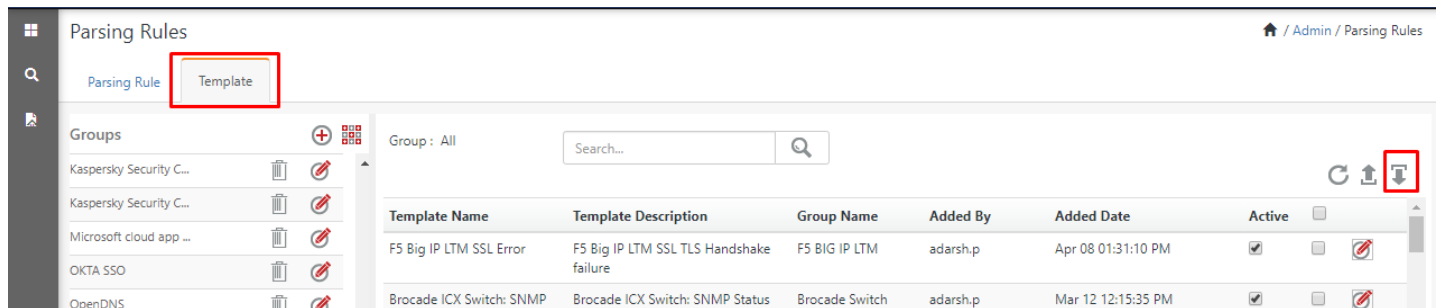


Figure 14

4. Browse Juniper JunOS templet files.

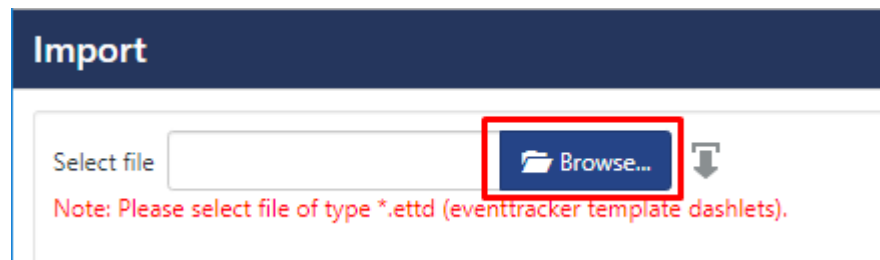


Figure 15

5. Select all **Juniper JunOS** template names.

6. Click on the **Import** button.

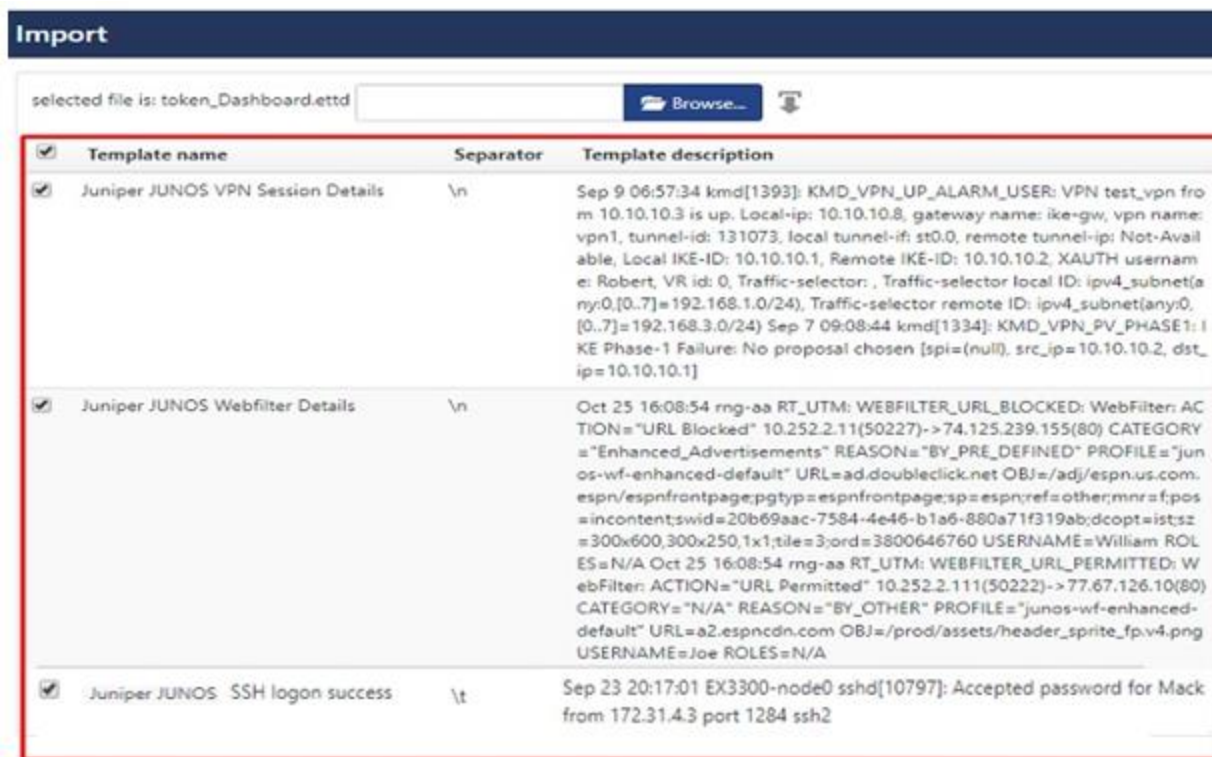


Figure 16

7. Template(s) imported successfully.

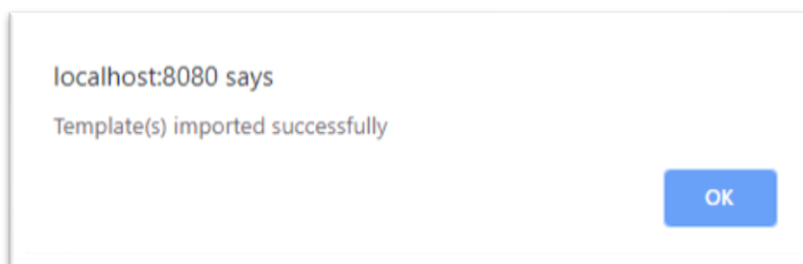


Figure 17

Flex Reports

On EventTracker **Control Panel**,

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

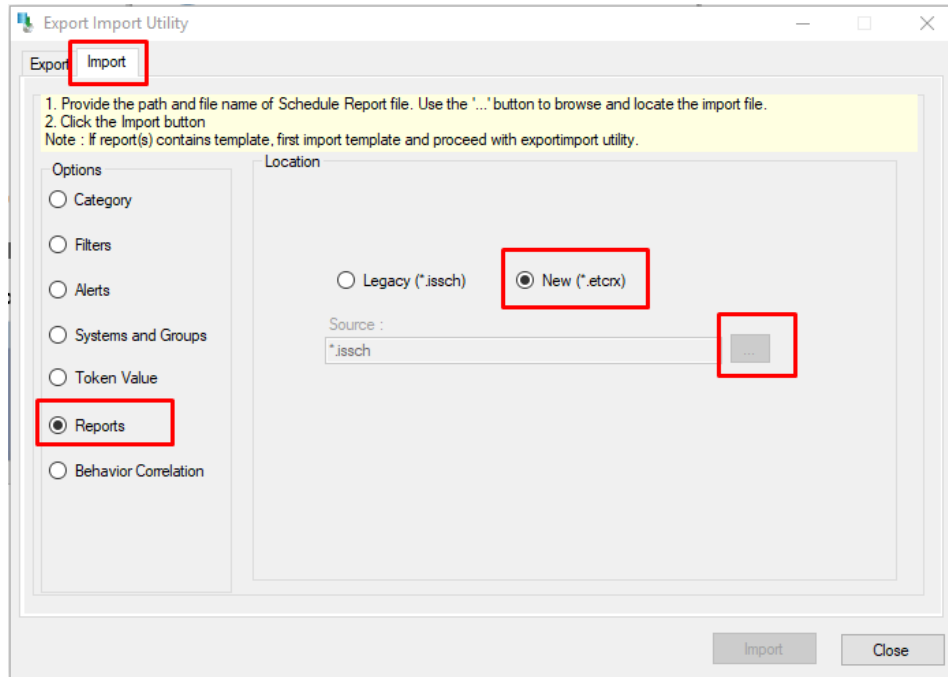


Figure 18

2. Locate the file named **Reports_Juniper JunOS.etcrx** and select all the checkbox.

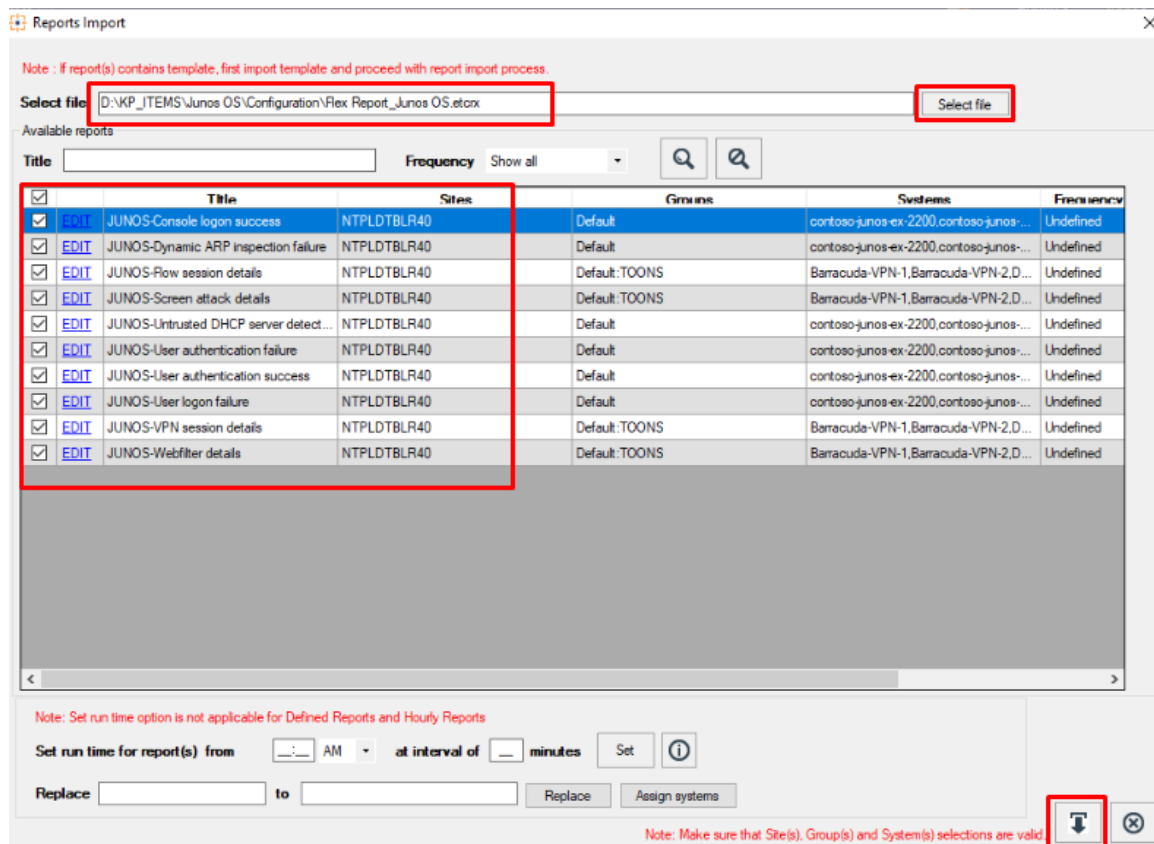


Figure 19

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

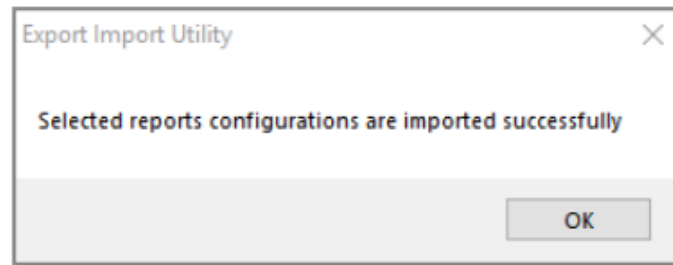


Figure 20

Knowledge Objects

1. Login to EventTracker console
2. Click on **Knowledge objects** under the Admin option in the **EventTracker** page.

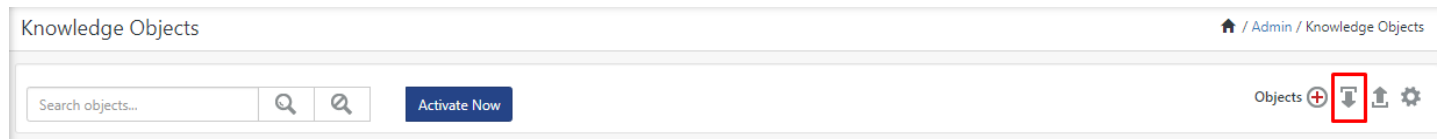


Figure 21

3. Locate the file named **KO_Juniper JunOS.etko**

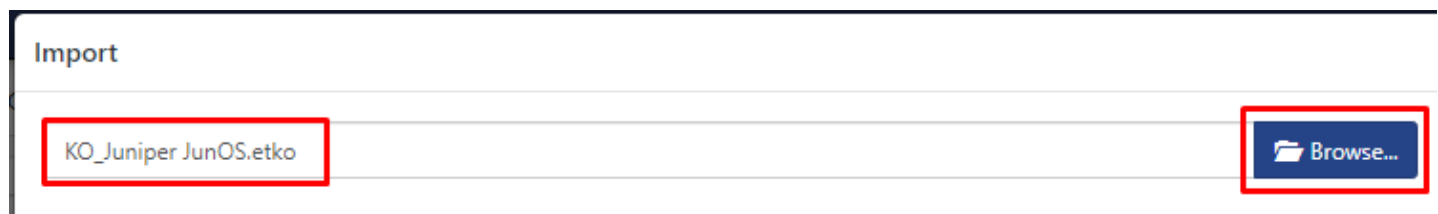


Figure 22

4. Now select all the checkbox and then click on the '**Upload**' option.

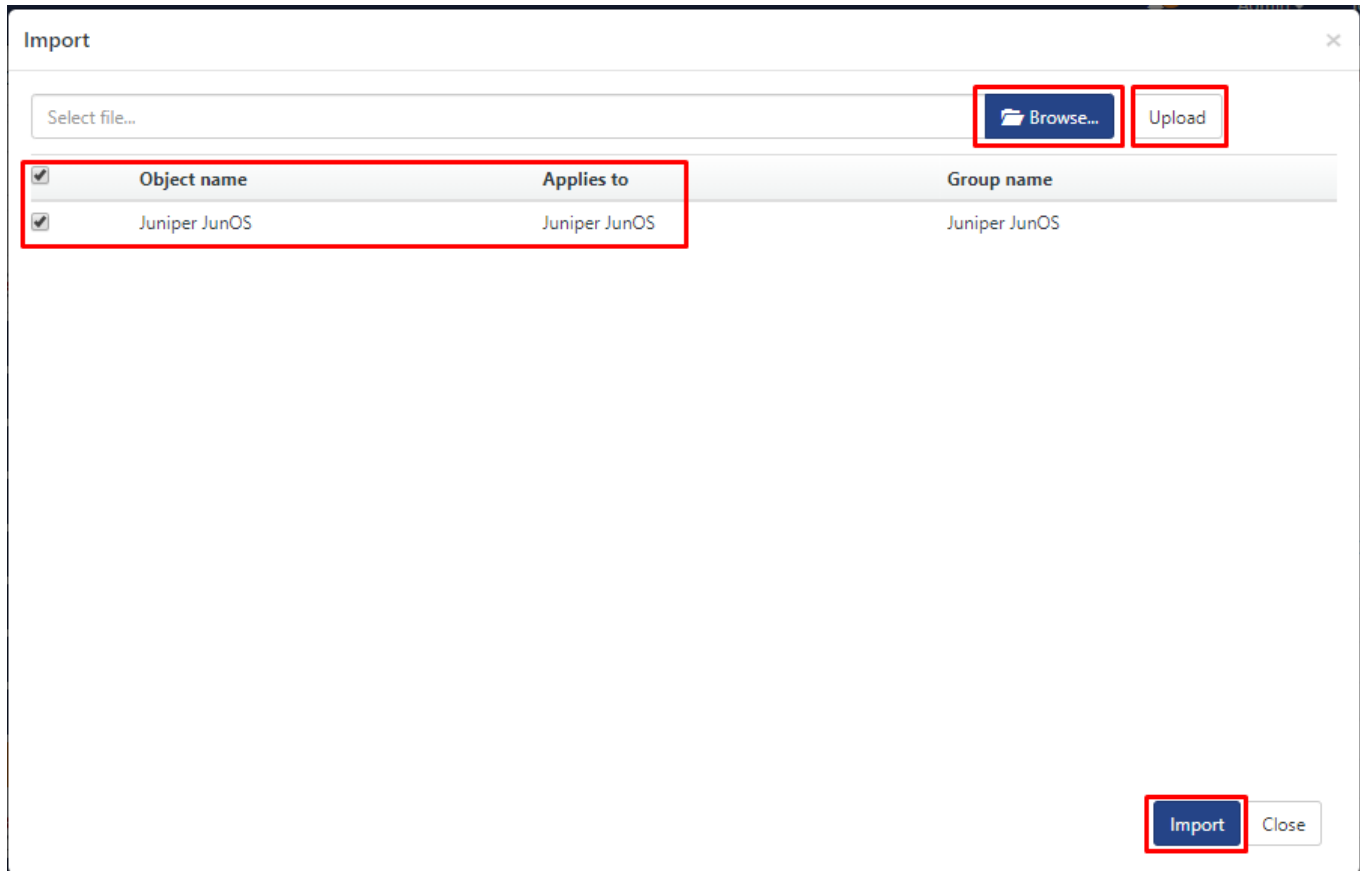


Figure 23

- Knowledge objects are now imported successfully.

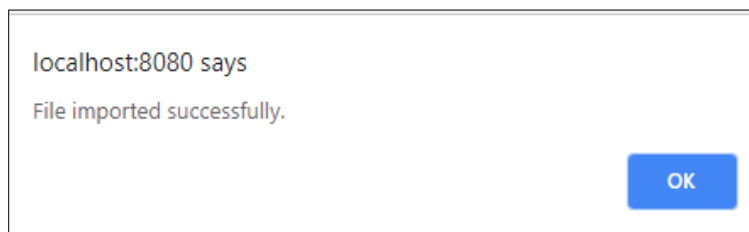


Figure 24

Dashboards

- Open **EventTracker** in the browser and log in.

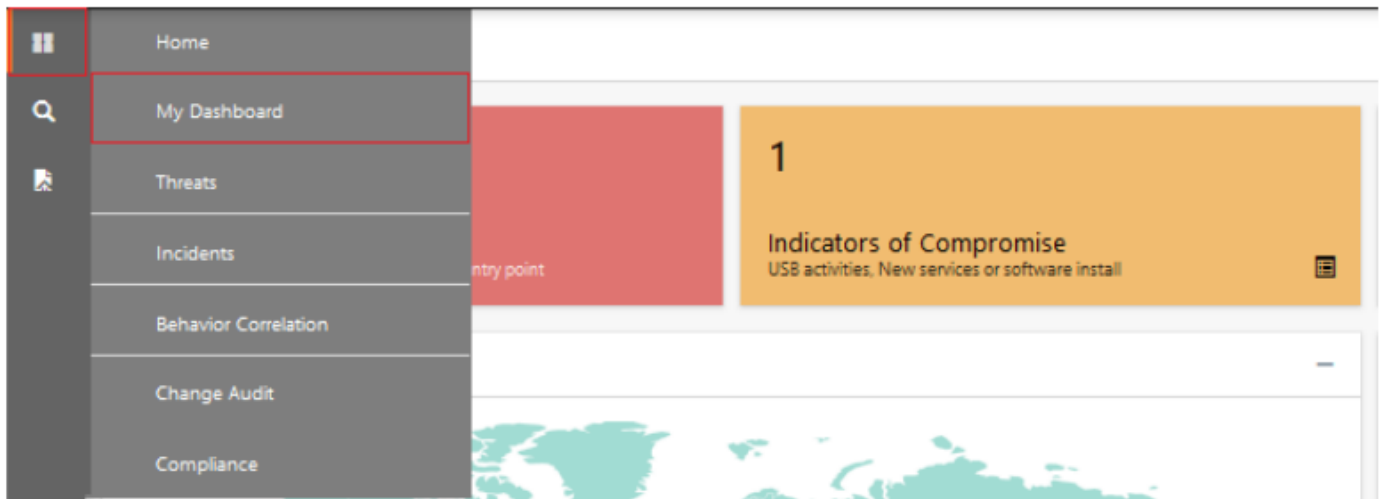



Figure 25

2. Navigate to **My Dashboard**.
3. Click on the **Import configuration**  icon on the top right corner.
4. In the popup window browse the file named **Dashboard_Juniper JunOS.etwd**.

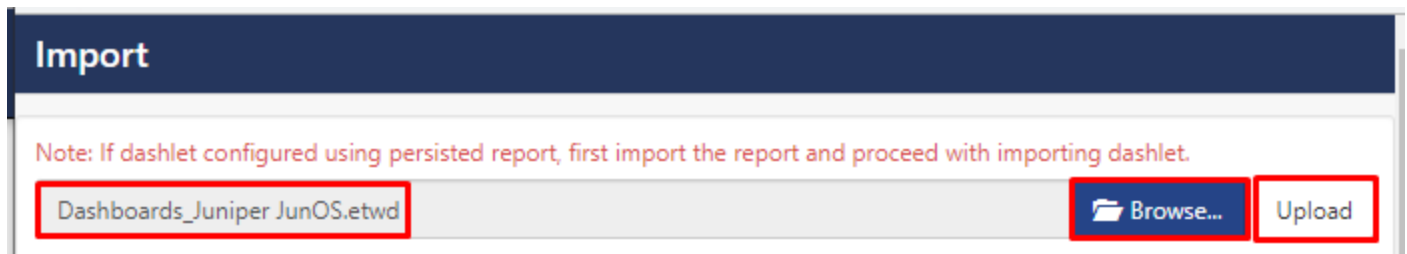


Figure 26

5. Now **select all the checkbox** and then click on the **Import** option.

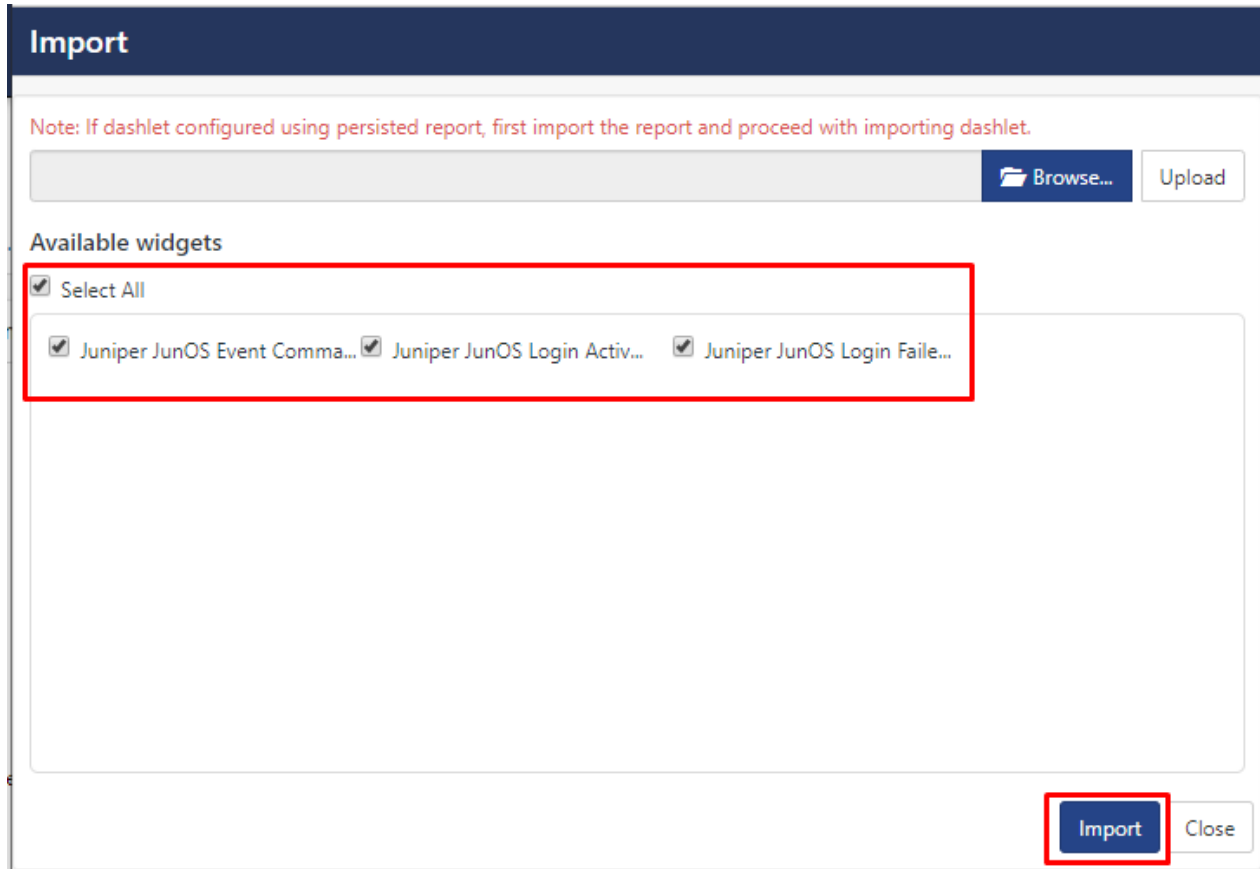



Figure 27

6. Click '**customize**'  locate and choose created Dashlets.
7. Click **Add** to add Dashlets to the dashboard.

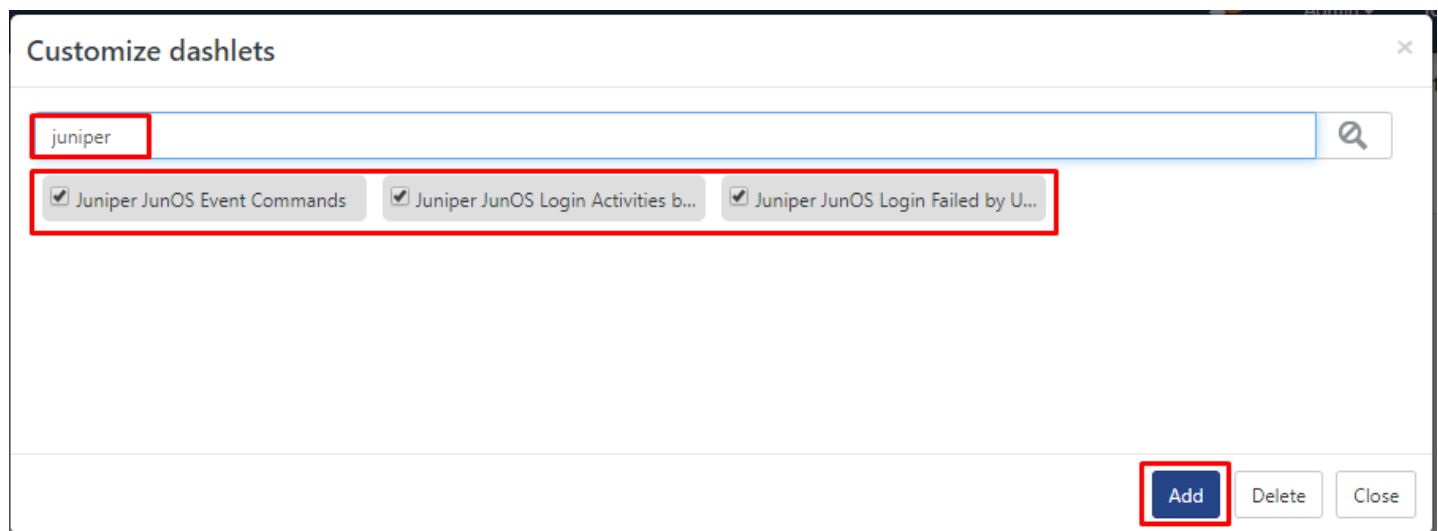


Figure 28

Verifying Juniper JunOS knowledge pack in EventTracker

Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** drop-down, and then click **Knowledge Objects**.
2. In the **Knowledge Object tree**, expand the **Juniper JunOS** group folder to view the imported Knowledge objects.

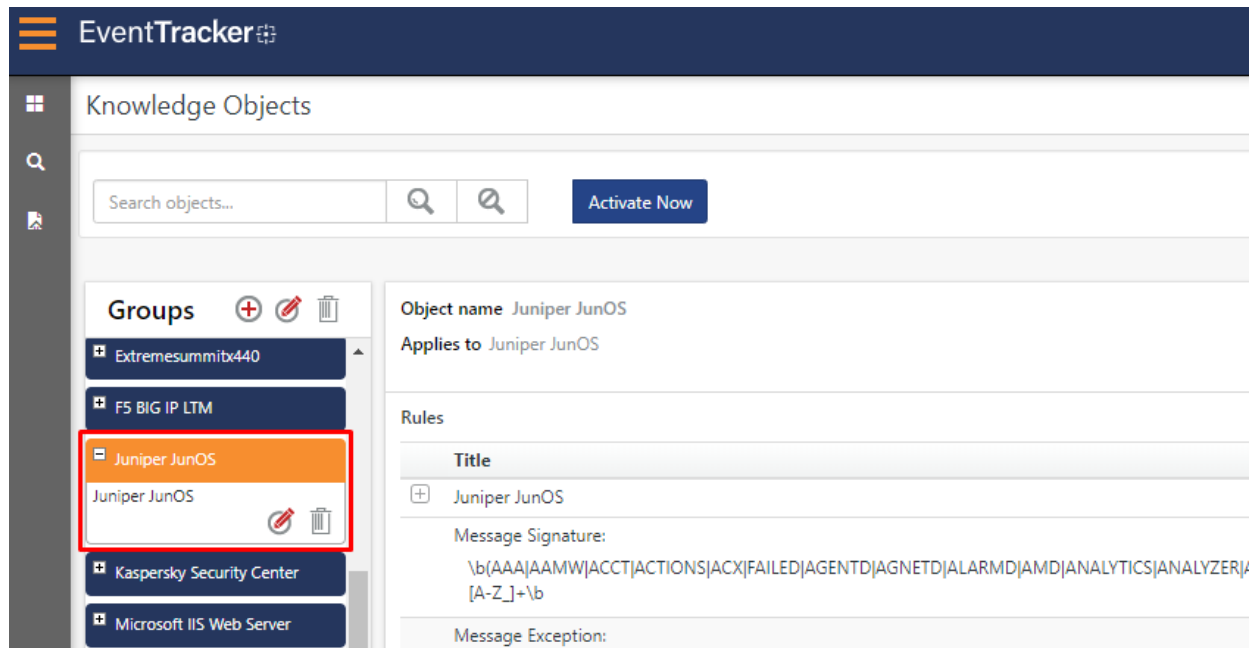


Figure 29

Template(s)

1. In the **EventTracker** web interface, click the **Admin** drop-down, and then click **Parsing Rules**.

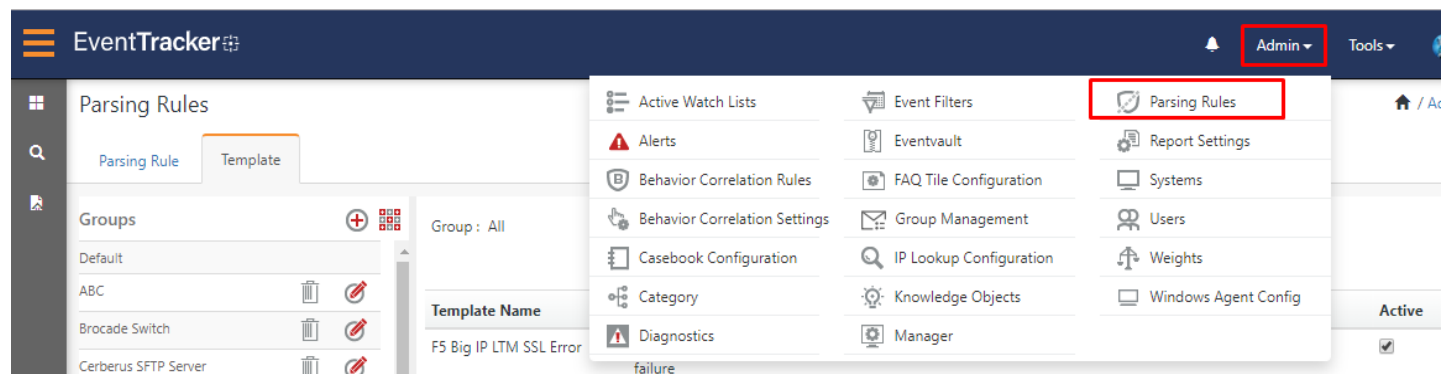


Figure 30

2. Select Templet and find the **Juniper JunOS** Group.
3. Click on Juniper JunOS Group to see the All Template(s).

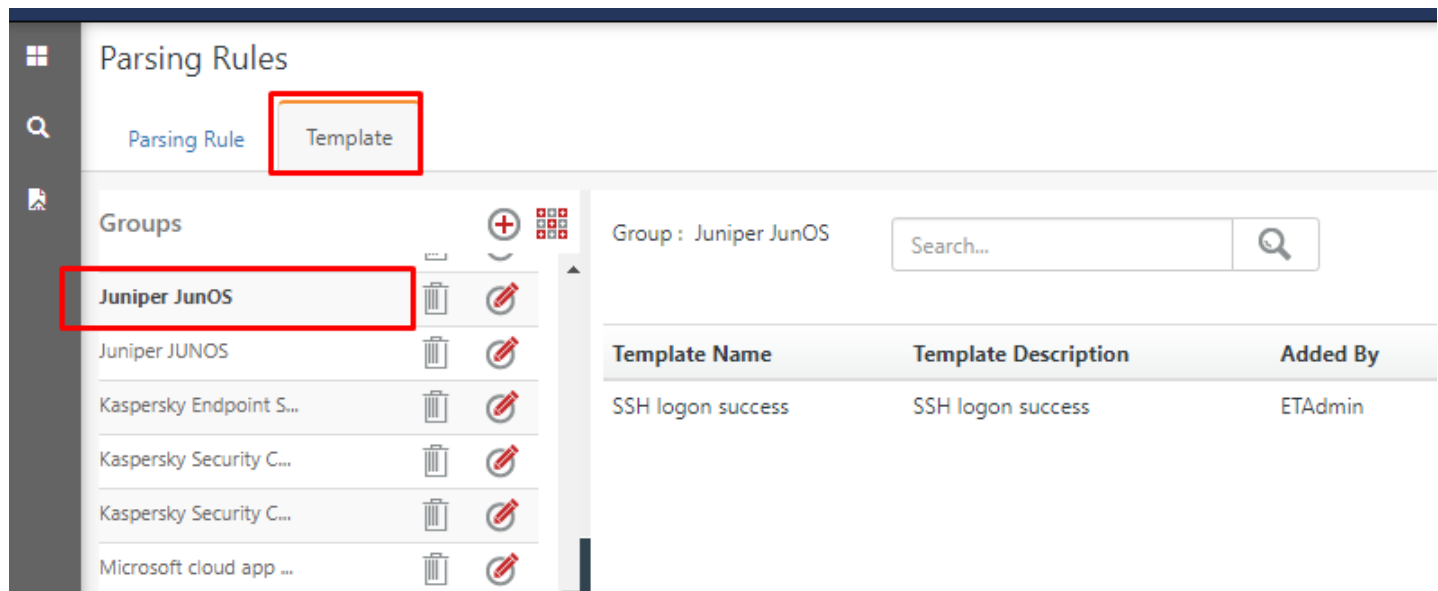


Figure 31

Flex Reports

In the **EventTracker** web interface,

1. Click the **Reports** icon, and then select the **Report Configuration**.

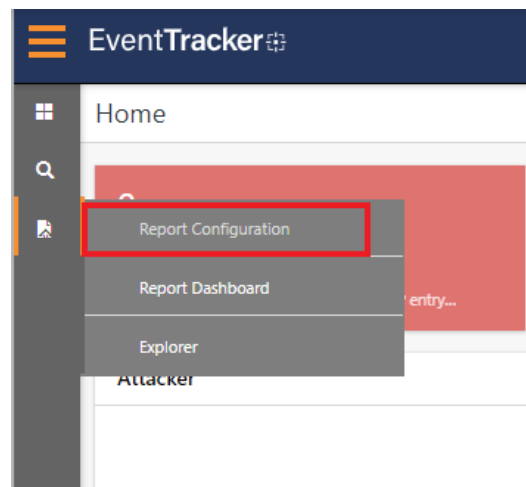


Figure 32

2. In **Reports Configuration** pane, select a **Defined** option.
3. Click on the **Juniper JunOS** group folder to view the imported **Juniper JunOS**.

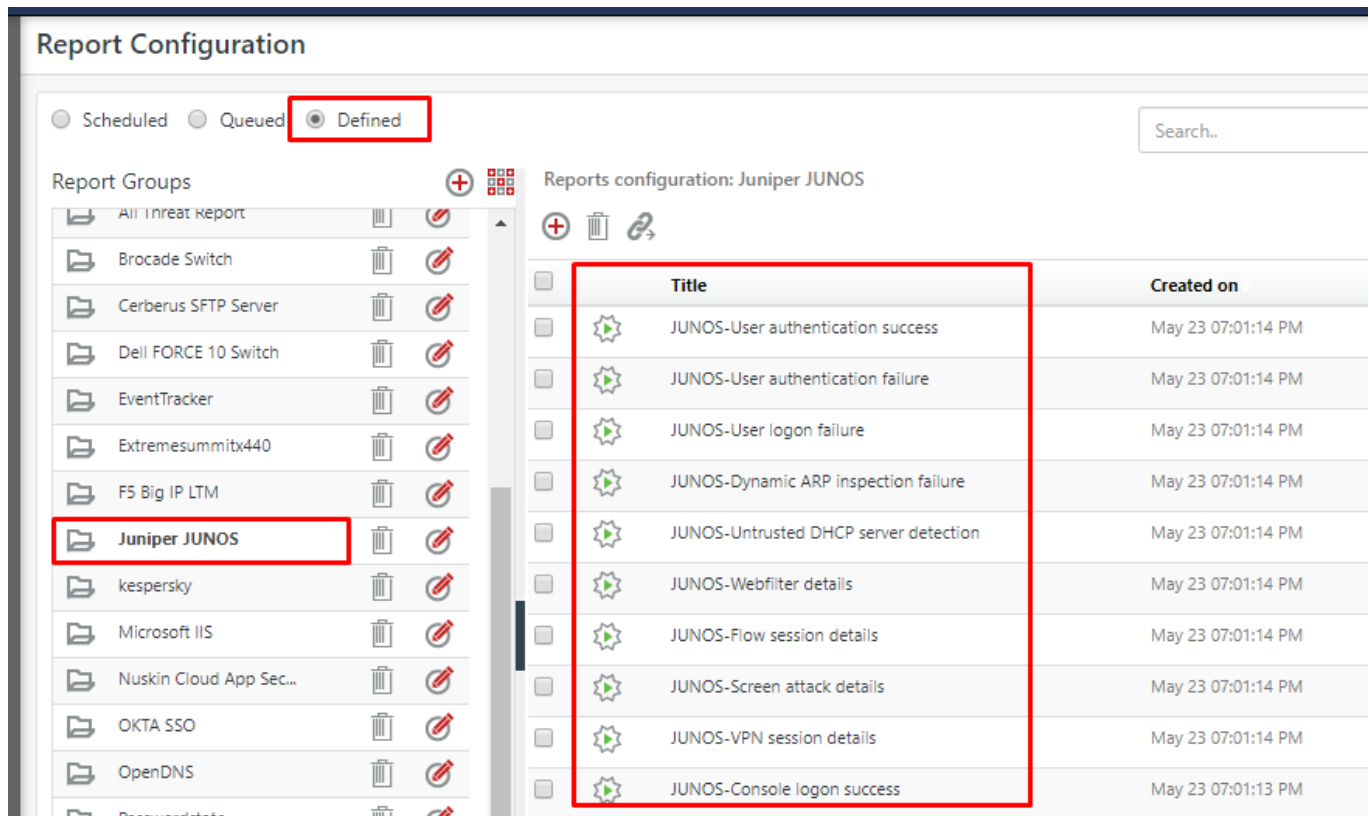


Figure 33

Alerts

1. In the **EventTracker** web interface, click the **Admin** icon, and then select **Alerts**.

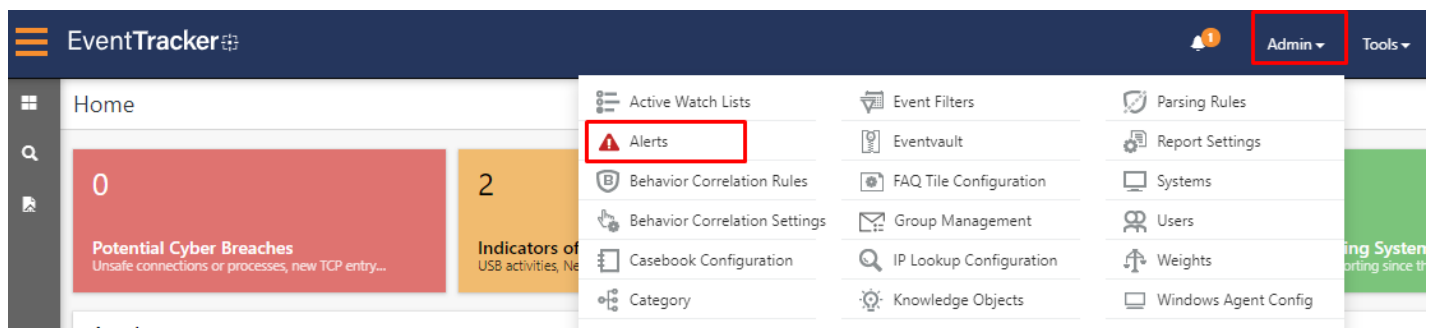


Figure 34

2. In the Alert search bar, we can search the alert name and view the imported **Juniper JunOS**.

EventTracker

Alerts

Show All

190
Available Alerts
Total number of alerts available

26
Active Alerts
Total number of active alerts

Activate Now Click 'Activate Now' after making all changes

<input checked="" type="checkbox"/>	Alert Name ^	Threat	Active	E-mai
<input checked="" type="checkbox"/>	JUNOS: Authentication failed	●	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	JUNOS: Link flap	●	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	JUNOS: Login failure	●	<input type="checkbox"/>	<input type="checkbox"/>

Figure 35