Netsurion™ | EventTracker

Integrate Pulse Secure Access

EventTracker v9.0 and Above

Publication Date: June 6, 2019

Abstract

This guide provides instructions to configure Pulse Secure Access to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor the application and user activities.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and Pulse Secure Access and later.

Audience

IT admins, Pulse Secure Access administrator, and EventTracker users who wish to forward logs to EventTracker and monitor events using EventTracker.

Table of Contents

Overview

Pulse Secure Access's suite offers complete, end-to-end usability, visibility, and protection to enable remote, mobile and cloud access to hybrid IT services and applications from any device.

Pulse Secure Access can be integrated with EventTracker using syslog. With the help of Pulse Secure Access knowledge pack, we can monitor the user URI requests, user login, and logout, user connection status on applications and trigger the alert whenever any user authentication failure is detected. EventTracker dashboard will help you to visualize the web activities on applications. It can even create the report which helps to collect user activities happening in the applications for a time interval. This will help you to review the different user activities. EventTracker CIM will help you to correlate the web requests from users, and user connection status with another log sources like web requests, user activities, user connection status, etc.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **Pulse Secure Access** should be installed.

Configuring Pulse Secure Access syslog

To configure reporting to a syslog server:

1. Login into Pulse Secure Access admin console.
2. Select **System** > **Log/Monitoring**.
3. Click the **Settings** tab to display the configuration page.
4. Specify the maximum log size and select the events to be logged. Specify the server configuration as described in.

Note: Select all in the **Select Events to Log**.

5. Fill details and click **Add**. You can specify multiple syslog servers.

    - **Server name/IP**: Specify the fully qualified domain name or IP address for the syslog server.
    - **Facility**: Select a syslog server facility level (LOCAL0-LOCAL7). Your syslog server must accept messages with the following settings: facility = LOG_USER and level = LOG_INFO.
    - **Type**: Select the connection type to the syslog server. You can select:
        - **UDP** (User Datagram Protocol) -A simple non-secure transport model.
        - **TCP** (Transmission Control Protocol) -A core protocol of the Internet Protocol suite (IP), but lacks strong security.

- **Filter**: Select a filter format. Any custom filter format and the following predefined filter formats are available:
  - **Standard(default)**—This log filter format logs the date, time, node, source IP address, user, realm, event ID, and message.

  Note: Select **Standard**(default) as a **Filter**.

6. Save the configuration.

NOTE: To enable syslog reporting for each local log category, you must perform this procedure on each local log tab: Events, User Access, Admin Access, and Sensors

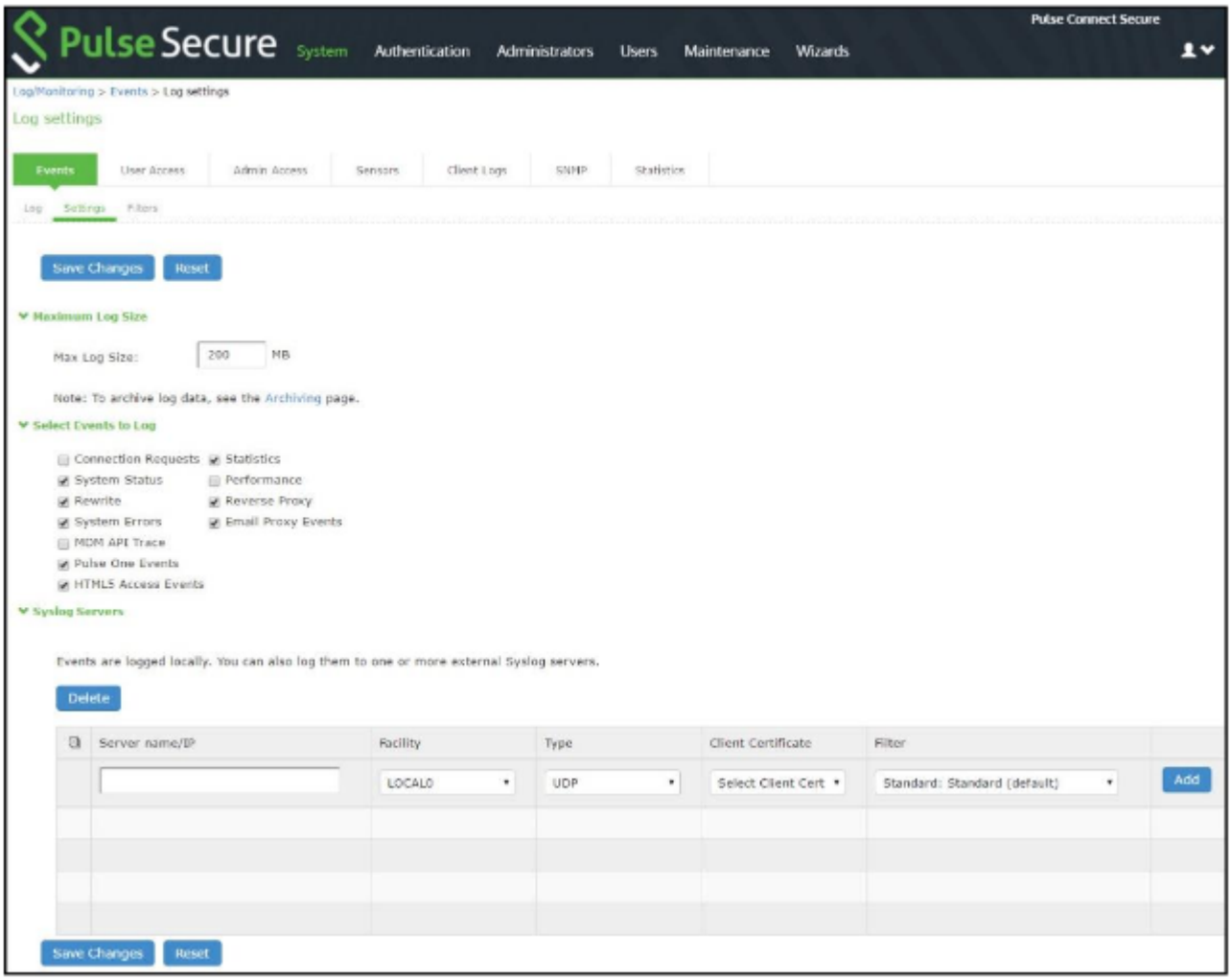

Figure 1

EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are available in the EventTracker v9.x and later to support Pulse Secure Access.

Alert

- **Pulse Secure Access: Authentication failure –** This alert will trigger whenever the user authentication fails.

Reports

- **Pulse Secure Access – Web connection activities –** This report provides information related to the user requesting detail like user IP address, URI, how many bytes are received and sent.

LogTime	User Name	Source IP Address	Requested URI	Total Bytes Expected	Total Bytes Received
03/27/2019 04:49:45 PM	contosowork1\mark	20.10.11.12	/dana-na/hc/hcif.cgi?cmd=getzipfile&f=OPSWAT/UnifiedV4/Windows/dlls/UnifiedSDK		0
03/27/2019 04:52:28 PM	contosowork2\matt	20.10.11.127	/	0	0

Figure 2

- **Pulse Secure Access – User login and logout –** This report provides information related to user login and logout from user agent, IP address.

LogTime	User Name	User Agent	Company Name	Source IP Address	Status
03/27/2019 04:54:46 PM	mathew		CONTOSOAT	10.6.68.4	Logout
03/27/2019 04:54:47 PM	john	PulseSecureiPhone(Compatible with JunosPulseiPhone) Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16D57 PulseSecure(Version-7.1.1.78493)iPhone.	CONTOSOAT	20.11.12.30	Login succeeded
03/27/2019 04:54:49 PM	william		CONTOSOWORK1	31.40.12.23	Logout
03/27/2019 04:54:54 PM	mark		CONTOSOWORK	40.123.110.18	Logout
03/27/2019 04:54:56 PM	jerry		CONTOSOWORK4	50.10.43.10	Logout
03/27/2019 04:55:00 PM	matt	Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/7.0; rv:11.0) like Gecko.	contosowork3	15.10.43.98	Login succeeded

Figure 3

- **Pulse Secure Access – Authentication success -** This report provides information related to the user authentication success.

LogTime	User Name	Authentication Server	Company Name	Destination IP Address
03/27/2019 04:47:52 PM	mat	CONTOSOTWORK/STATION/284/MAT	CONTOSOWORK3	71.20.111.10
03/27/2019 04:47:55 PM	jerry	CONTOSOTWORK/STATION/284/JERRY	CONTOSOWORK2	10.81.95.41
03/27/2019 04:47:57 PM	jack	CONTOSO	CONTOSOTAM	41.20.188.43
03/27/2019 04:47:57 PM	andrew	NEW/CONTOSO/WORKSTATION/AND	NEWWORKSTATION	10.20.10.11

Figure 4

- **Pulse Secure Access – Authentication failure -** This report provides information related to user authentication failed.

LogTime	User Name	Company Name	Authentication Server	Destination IP Address
03/27/2019 04:47:59 PM	jack	CONTOSOTWORK/STATION/284/MAT	CONTOSOWORK3	21.54.98.34
03/27/2019 04:47:59 PM	matt	CONTOSOTWORK/STATION/284/JERRY	CONTOSOWORK2	32.45.65.43
03/27/2019 04:48:40 PM	andy	CONTOSO	CONTOSOTAM	21.56.83.92
03/27/2019 04:48:40 PM	john	NEW/CONTOSO/WORKSTATION/AND	NEWWORKSTATION	10.20.43.28

Figure 5

- **Pulse Secure Access – Access connection detail –** This report provides information related to user details like destination IP address, port number, company name, user name, how many bytes are received and access connection status.

LogTime	User Name	Company Name	Destination IP Address	Port	Bytes Read	Bytes Written	Status
03/27/2019 04:48:01 PM	ven	CONTOSOWORK1	9.57.98.30	3389			Connected
03/27/2019 04:49:00 PM	mat	CONTOSOWORK1	TUN-VPN	443	157	0	Closed connection
03/27/2019 04:49:14 PM	joe	Freelancers	9.39.10.76	3389			Connected
03/27/2019 04:49:17 PM	derek	CONTOSOANL	9.41.98.230	3389	193945306	6566751	Closed connection
03/27/2019 04:49:17 PM	john		9.47.98.56	3389	1203	316	Closed connection
03/27/2019 04:49:17 PM	dany	CONTOSOSTAT	9.45.28.97	3389			Connected

Figure 6

Dashboards

- **Pulse Secure Access Authentication failed** – This dashboard shows information about the top ten user authentication failed.

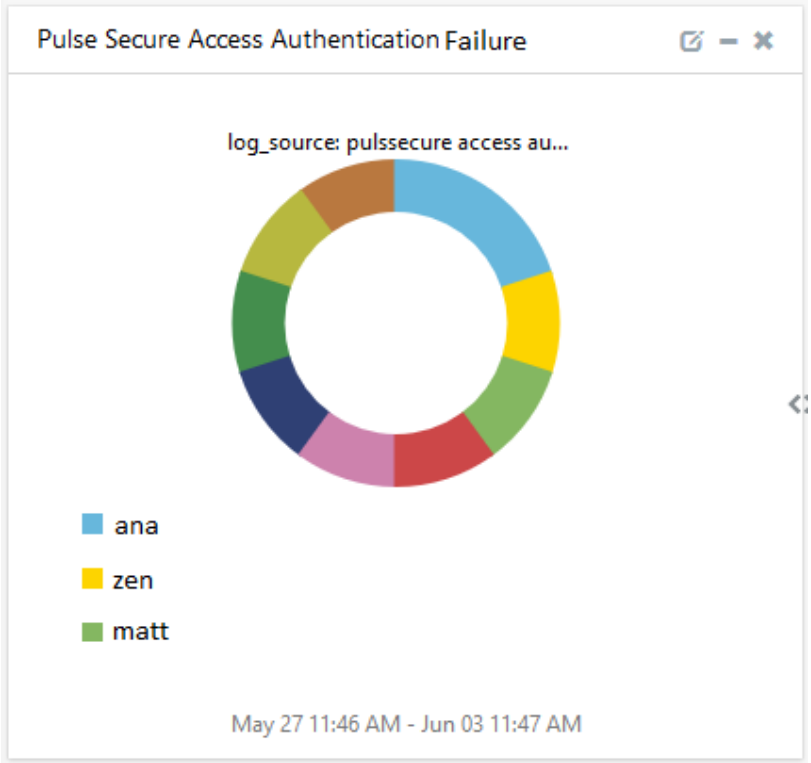

Figure 7

- **Pulse Secure Access Authentication Success** – This dashboard shows information about user authentication success.

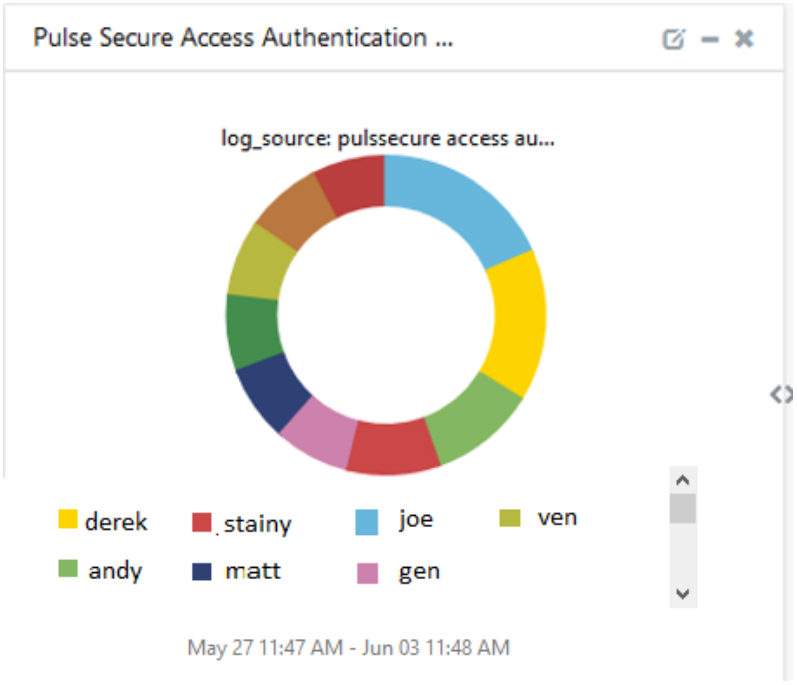

Figure 8

- **Pulse Secure Access Web Connection Details** – This dashboard shows information about user name, client IP address, port, user connectivity status.

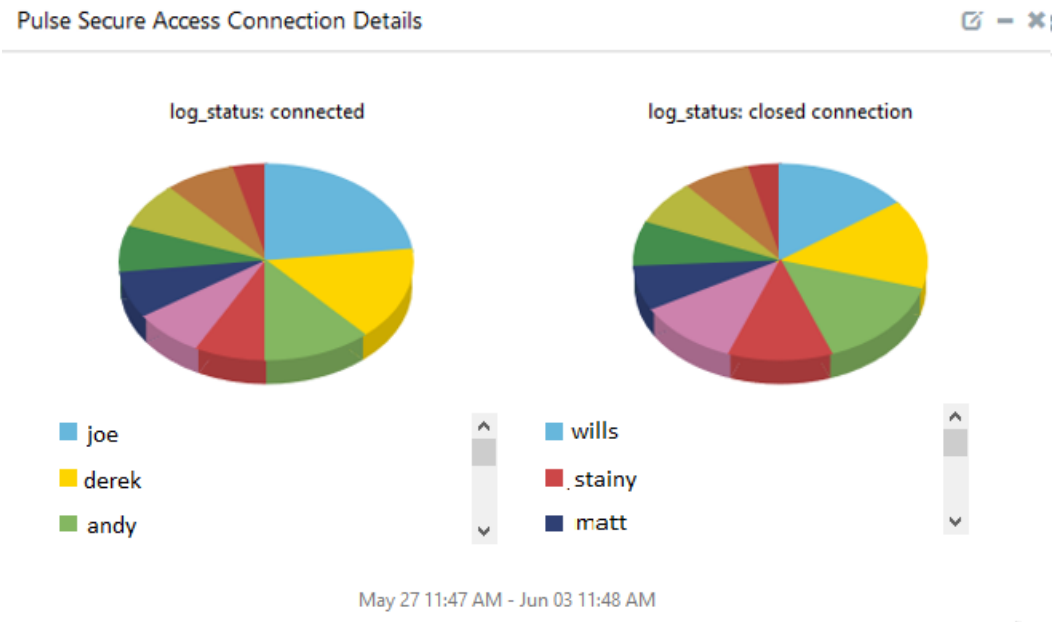

Figure 9

- **Pulse Secure Access User login and logout** – This dashboard shows information about the user login and log out.

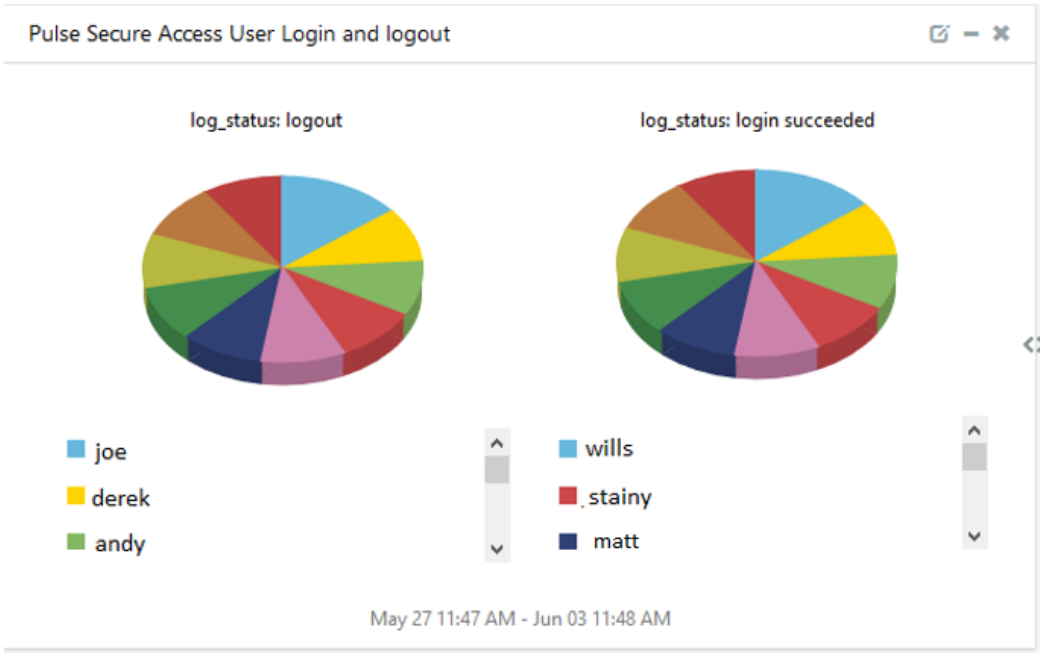

Figure 10

- **Pulse Secure Access Web Request Activities –** This dashboard shows information about web requests from IP address connected, user name, URI, the total count of bytes sent and received.

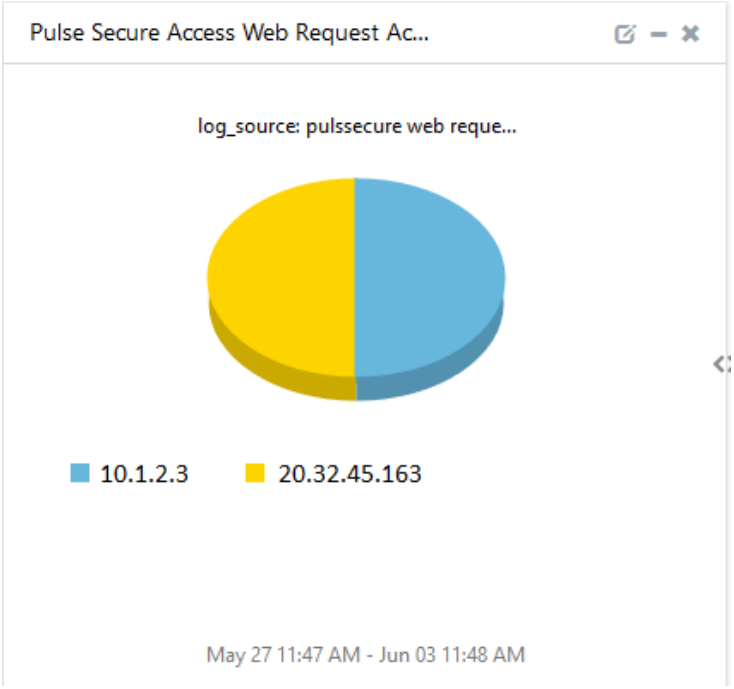

Figure 11

- **Pulse Secure Top 10 Ports Accessed** – This dashboard shows information about the ports frequently accessed by the client.

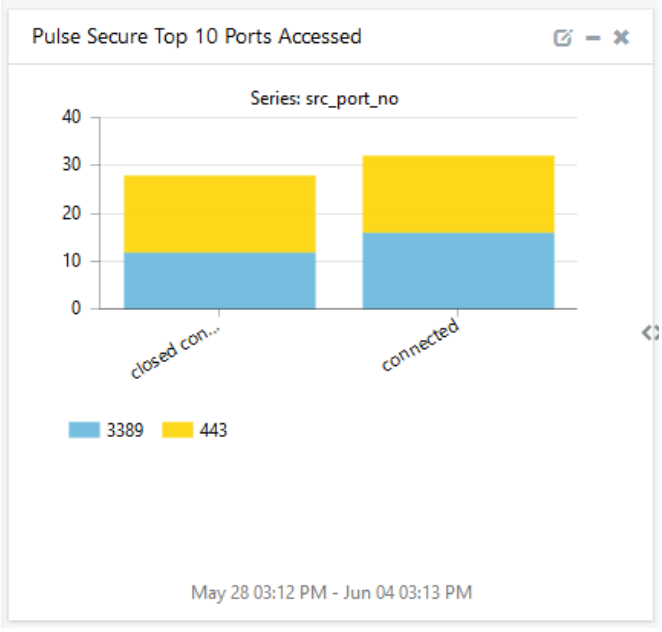

Figure 12

Importing Knowledge Pack into EventTracker

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

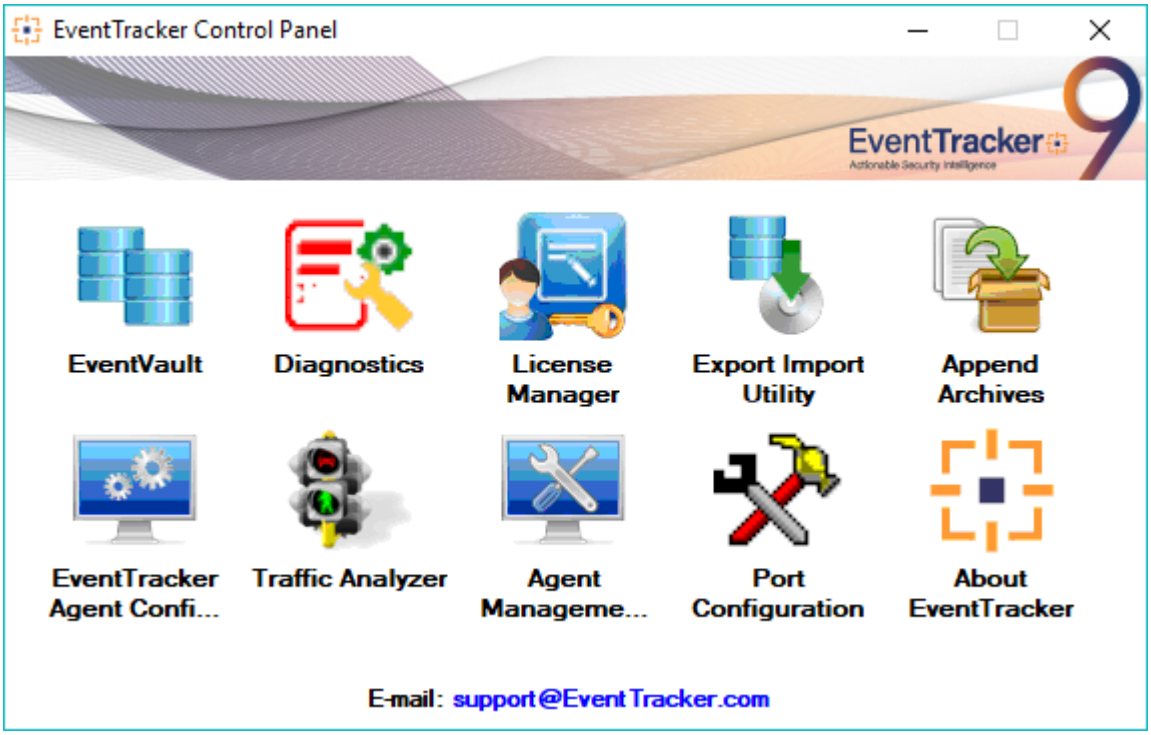

Figure 13

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

Alerts

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

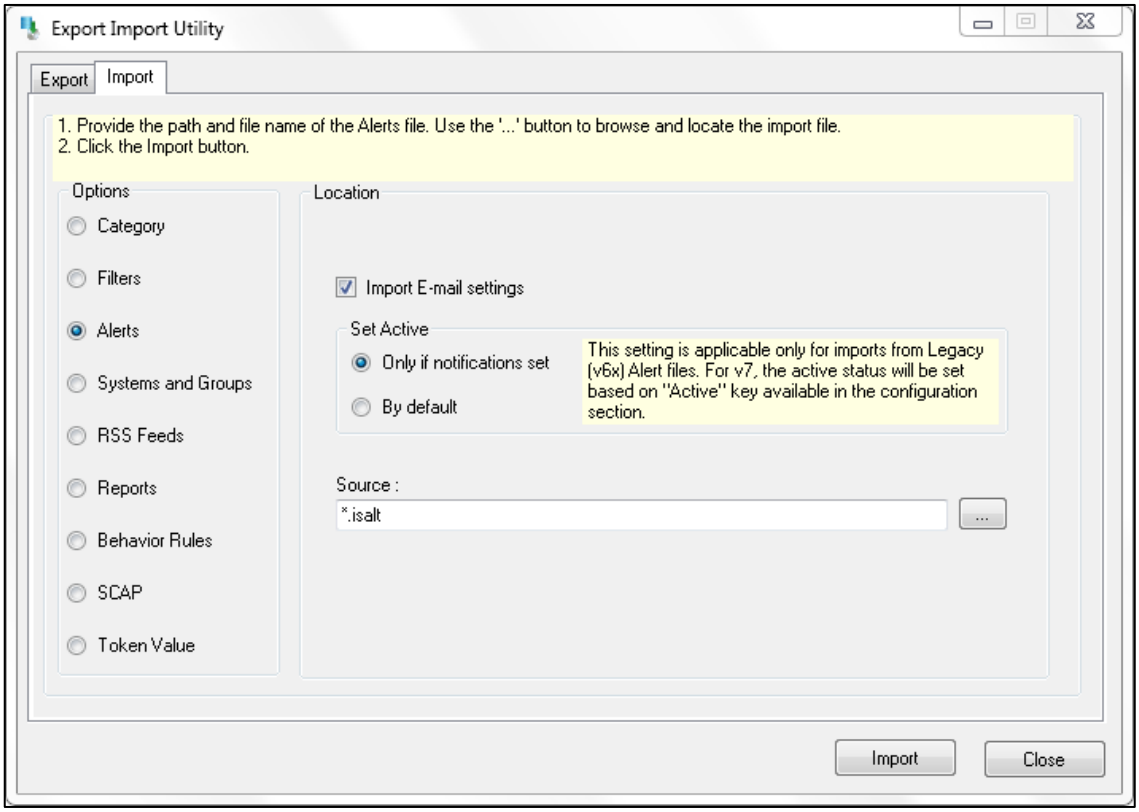

Figure 14

2. Locate **Alerts_Pulse Secure Access.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays a success message.

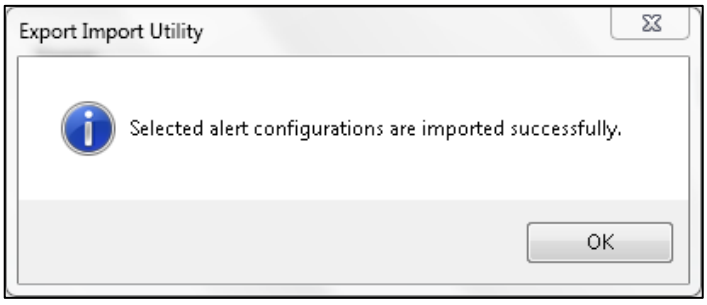

Figure 15

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

Knowledge Objects

1. Click **Knowledge objects** under the Admin option in the EventTracker page.
2. Locate the file named **KO_Pulse Secure Access.etko**.

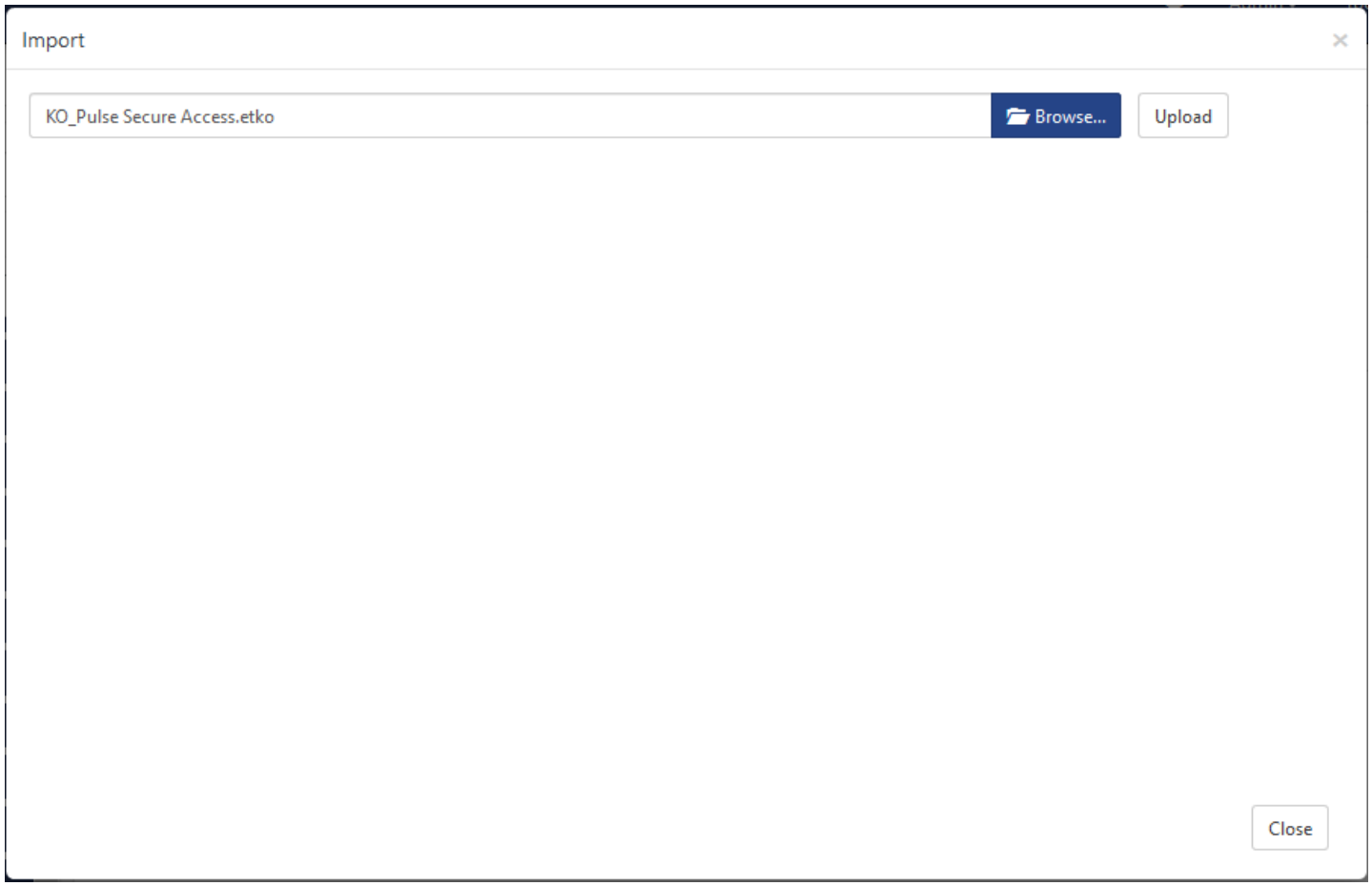

Figure 16

3. Now select all the checkbox and then click on the '**Import**' button option.

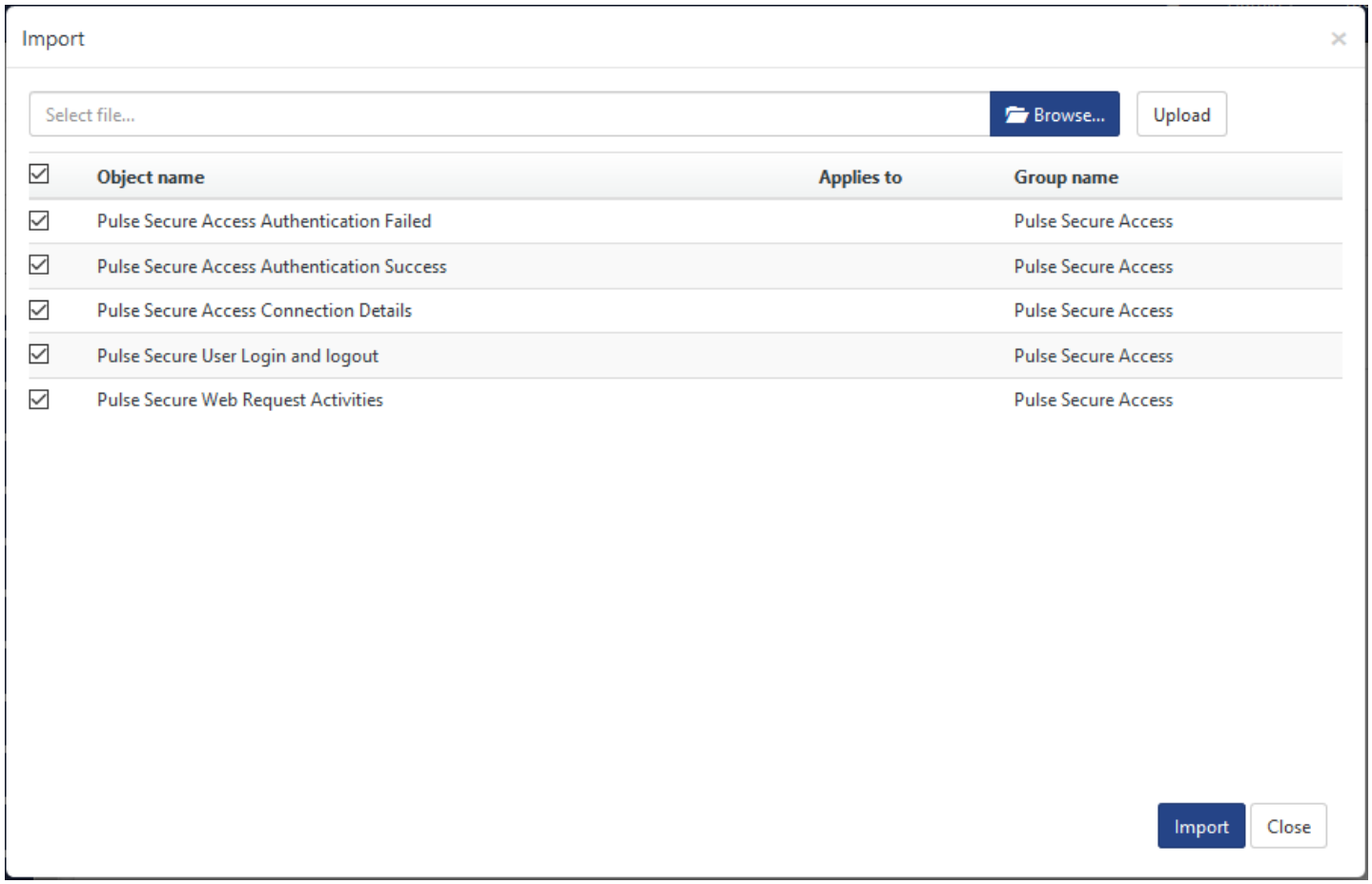

Figure 17

4. Knowledge objects are now imported successfully.

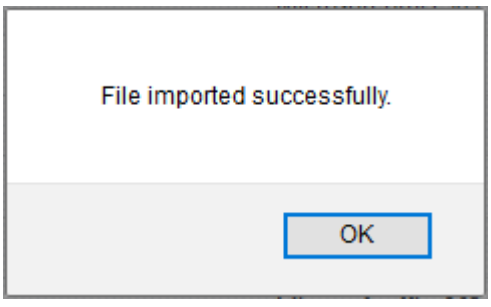

Figure 18

Token Template

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

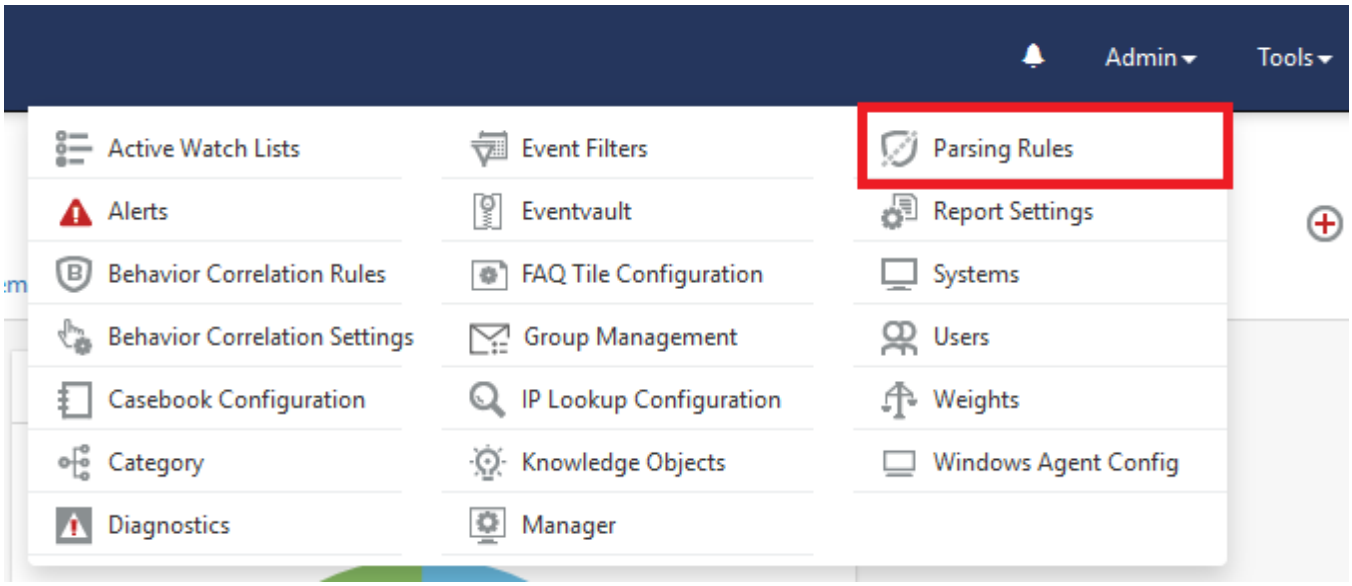

Figure 19

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

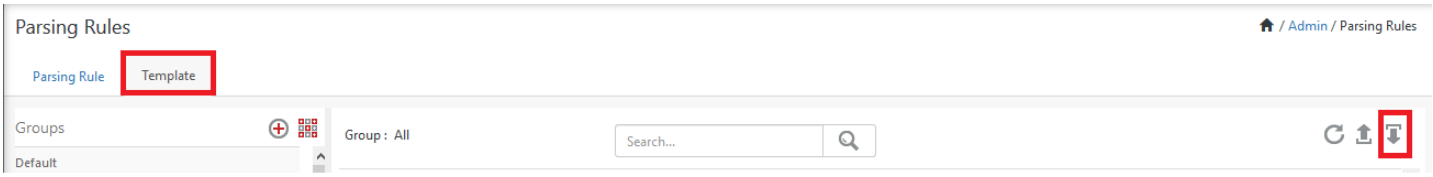

Figure 20

4. Locate the **Template_Pulse secure Access.ettd** file and click on the I**mport**.

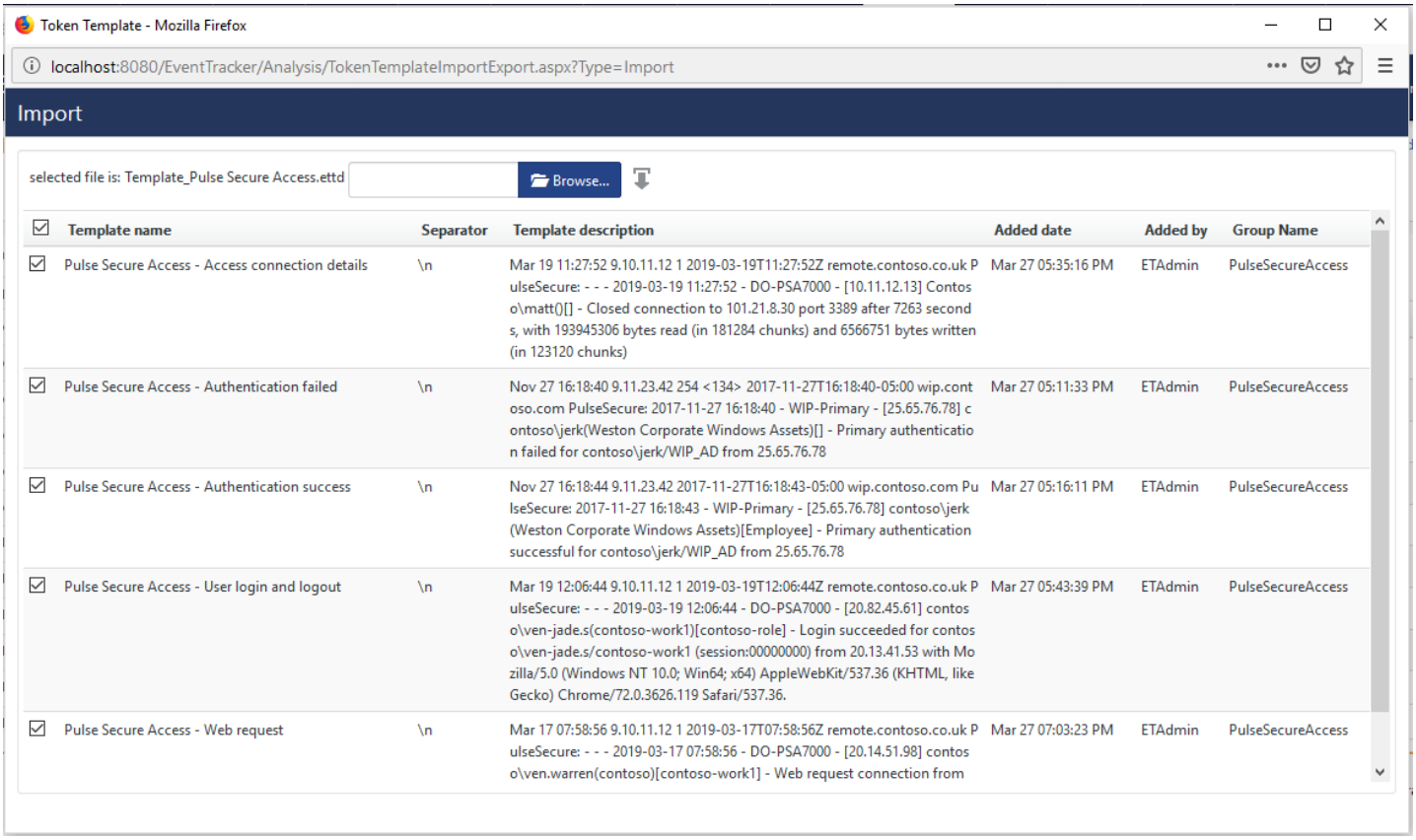

Figure 21

5. Templates are imported now successfully.

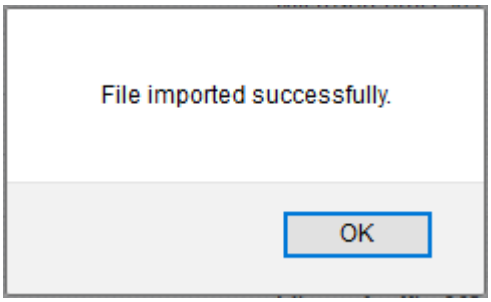

Figure 22

Flex Reports

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

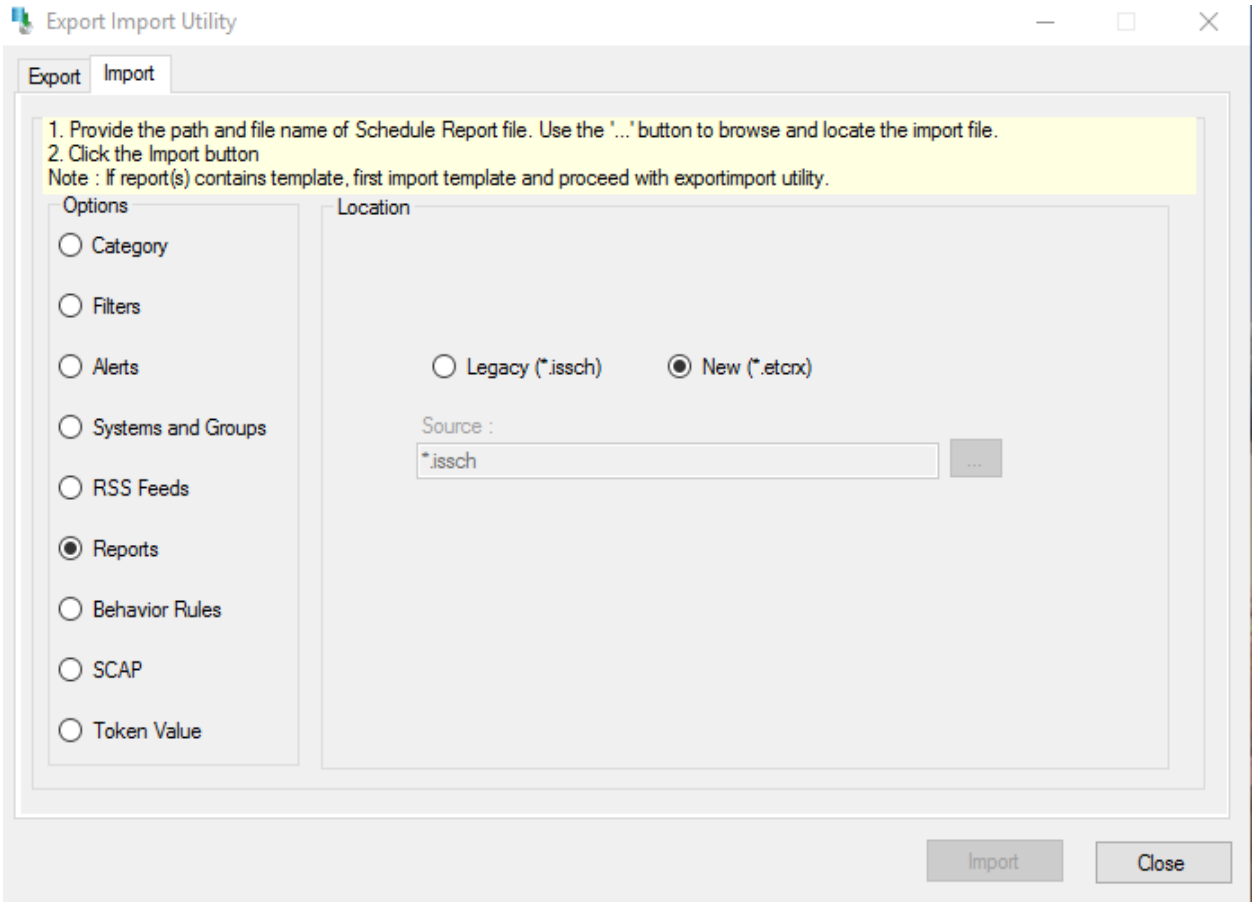

Figure 23

2. Locate the file named **Flex_Reports_Pulse Secure Access.etcrx** and select all the checkbox.

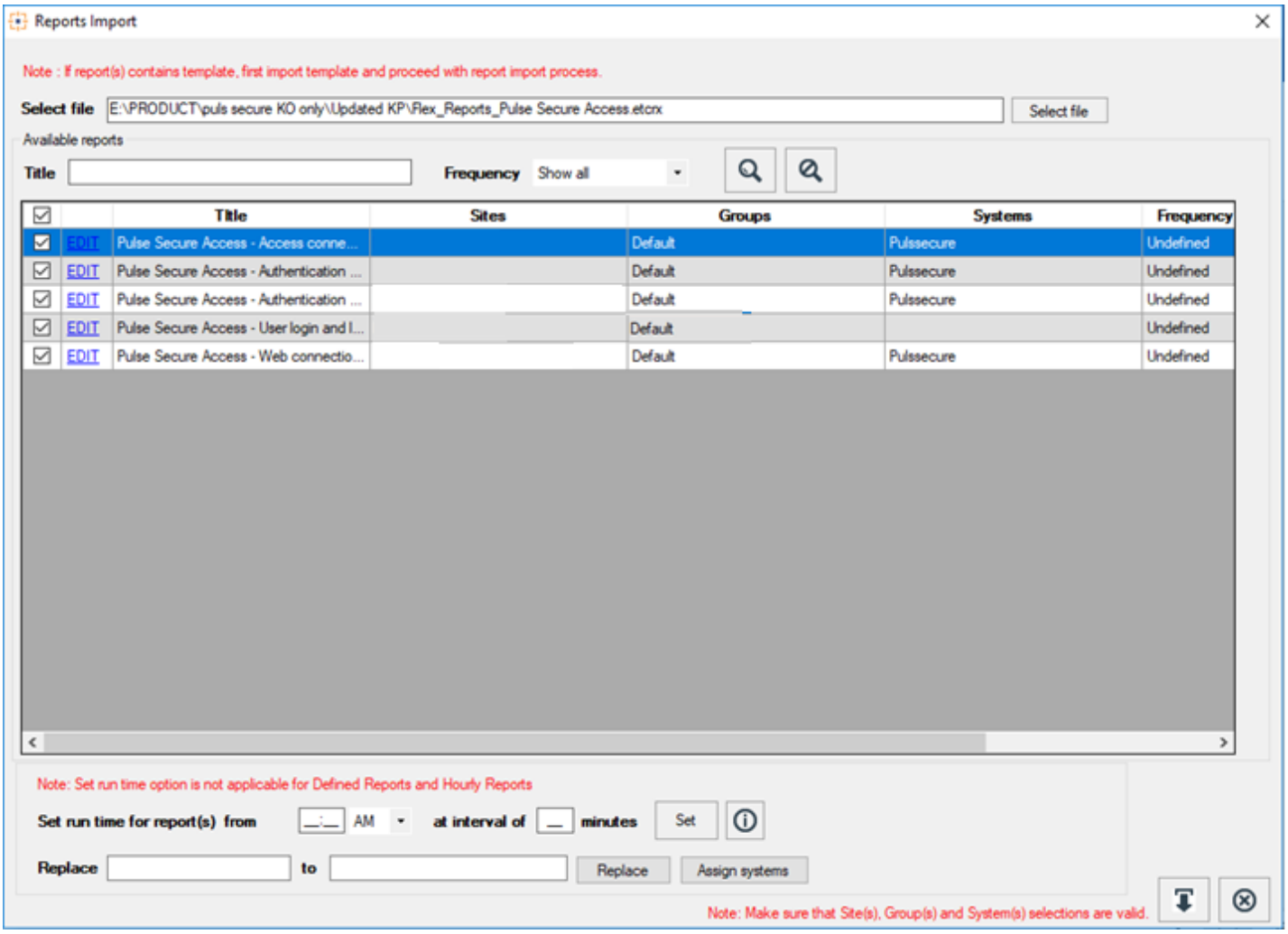

Figure 24

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

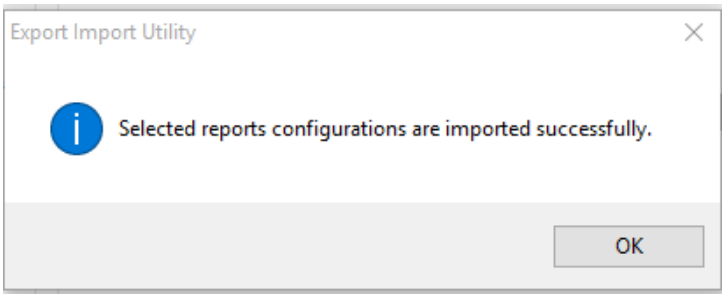

Figure 25

Dashlets

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

1. Login into EventTracker Web console.

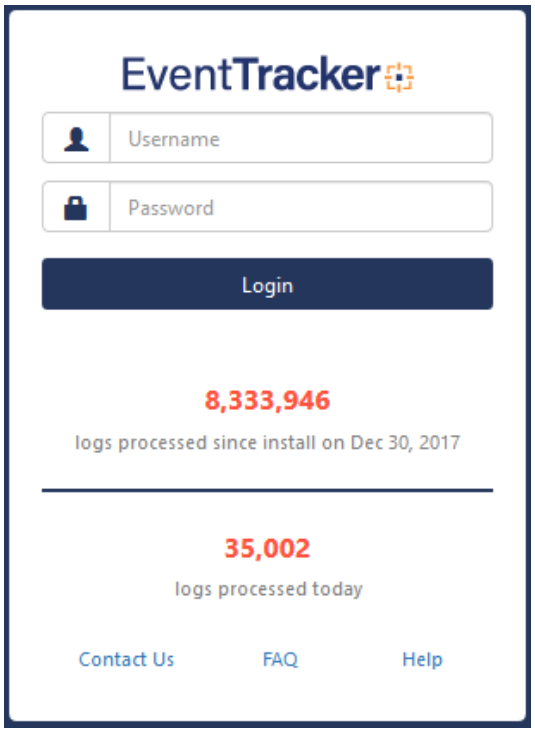

Figure 26

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

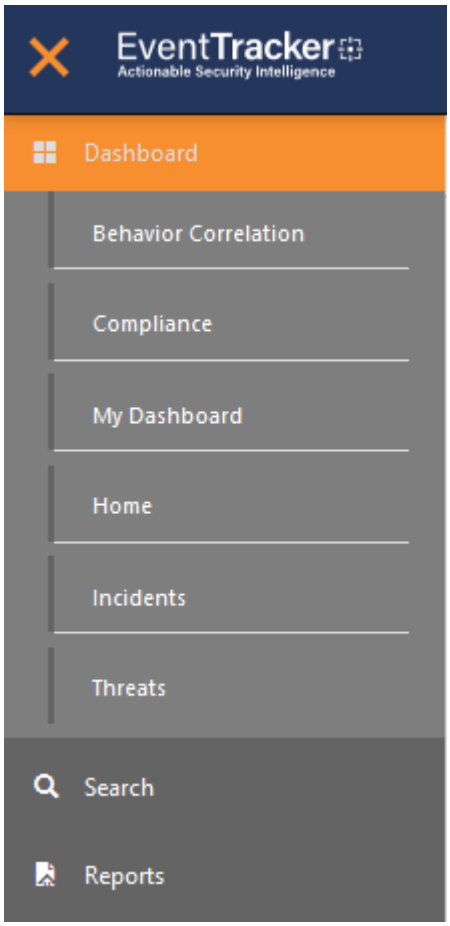

Figure 27

3. Click on the **Import** button and select **.etwd** File.

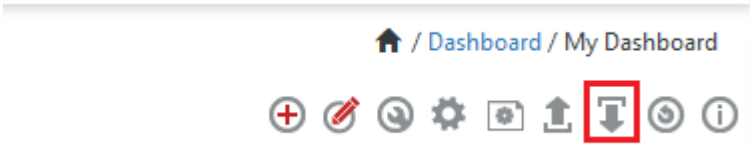

Figure 28

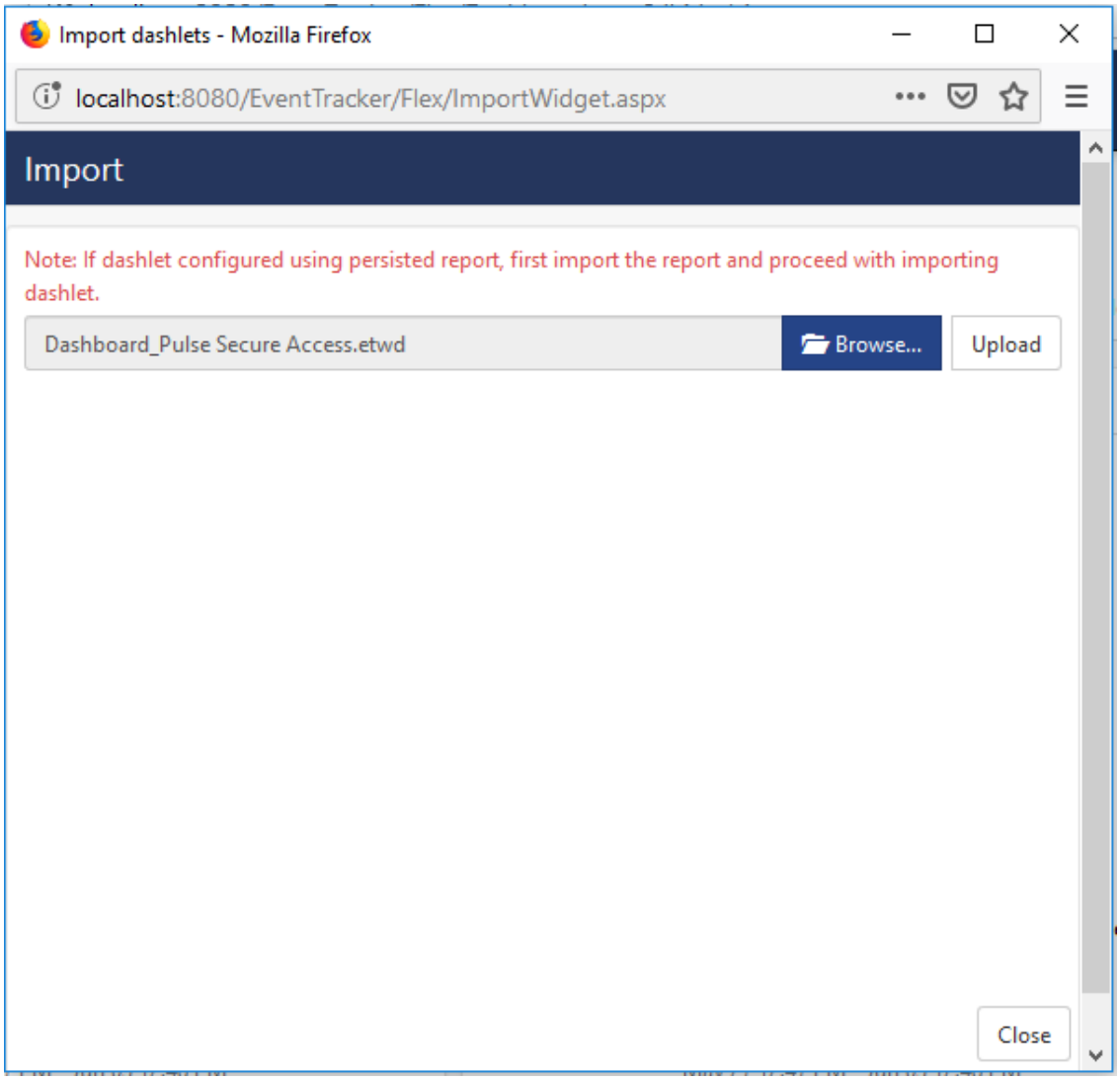

Figure 29

4. Click **Upload** and select Dashboard which you want to import.

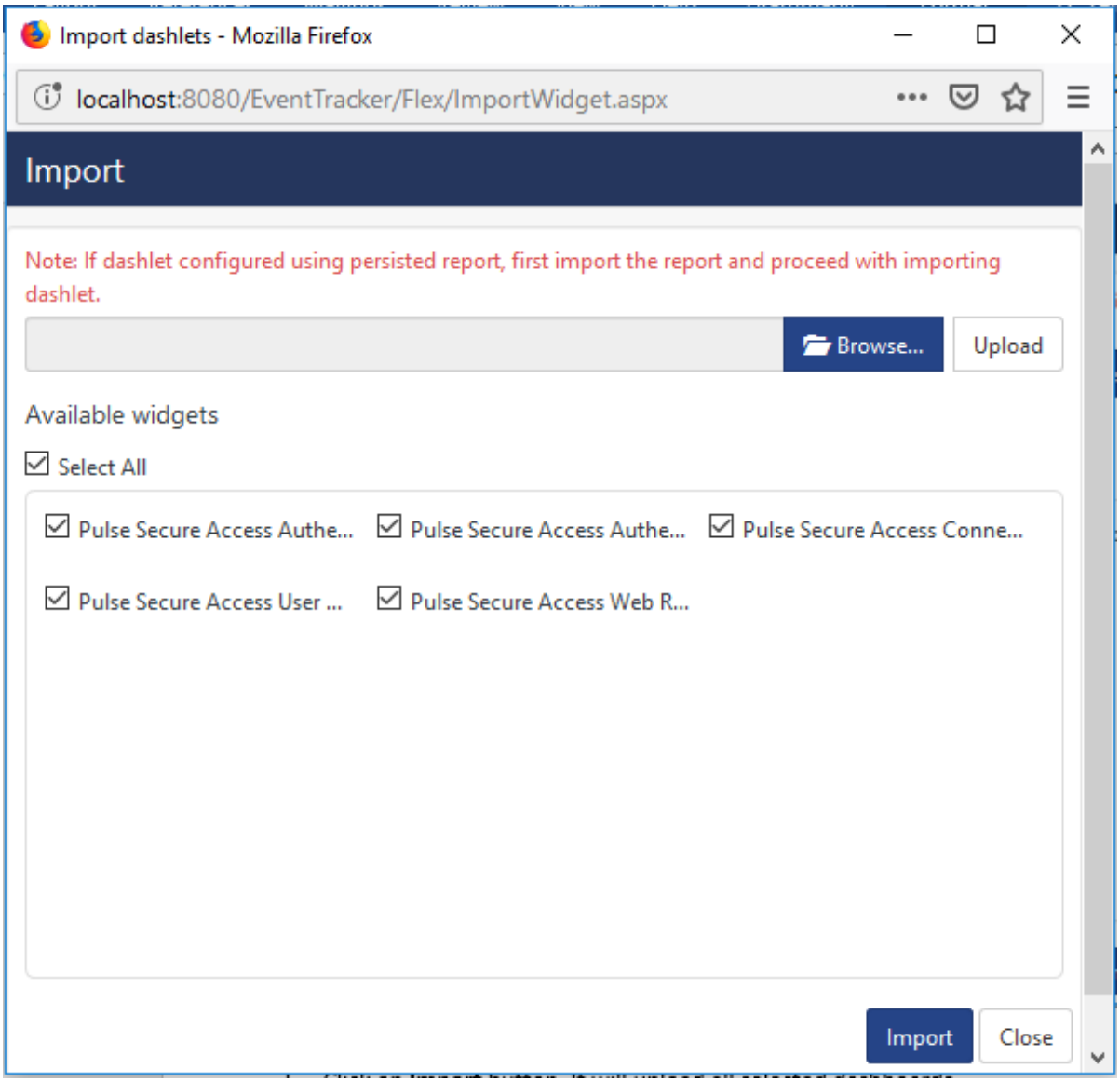

Figure 30

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

Verifying Knowledge Pack in EventTracker

Alerts

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

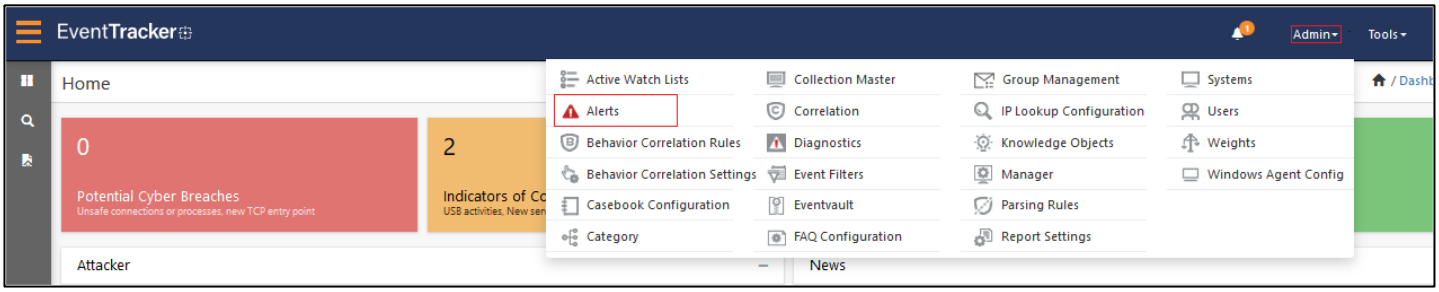

Figure 31

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

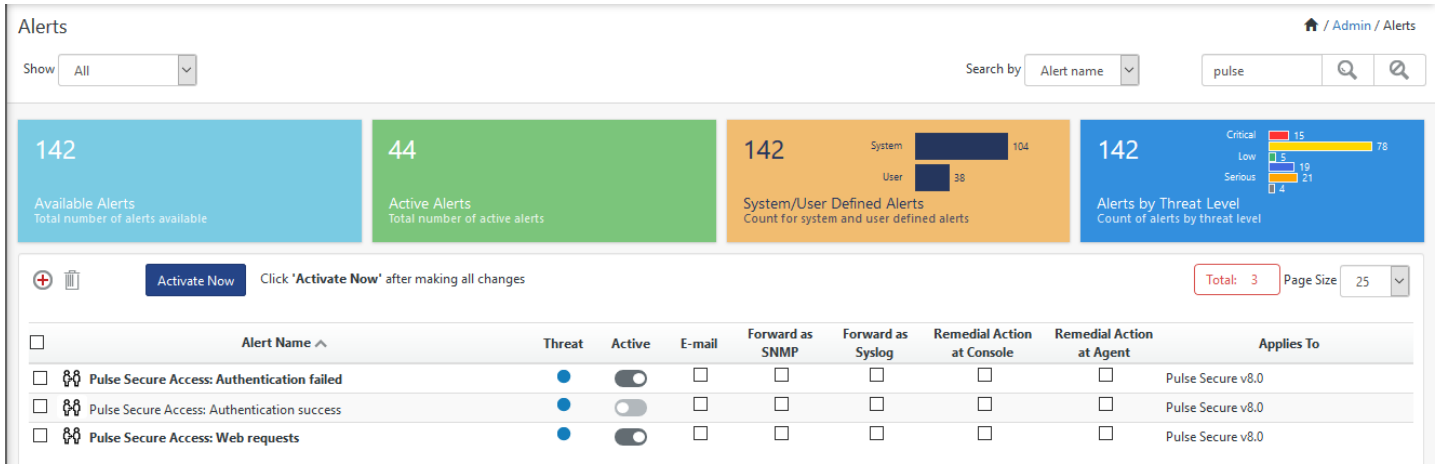

Figure 32

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

   EventTracker displays a message box.

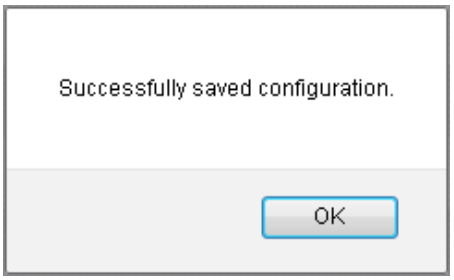

Figure 33

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

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

Knowledge Object

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click the **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Pulse Secure Access** group folder.

Knowledge Object is displayed in the pane.

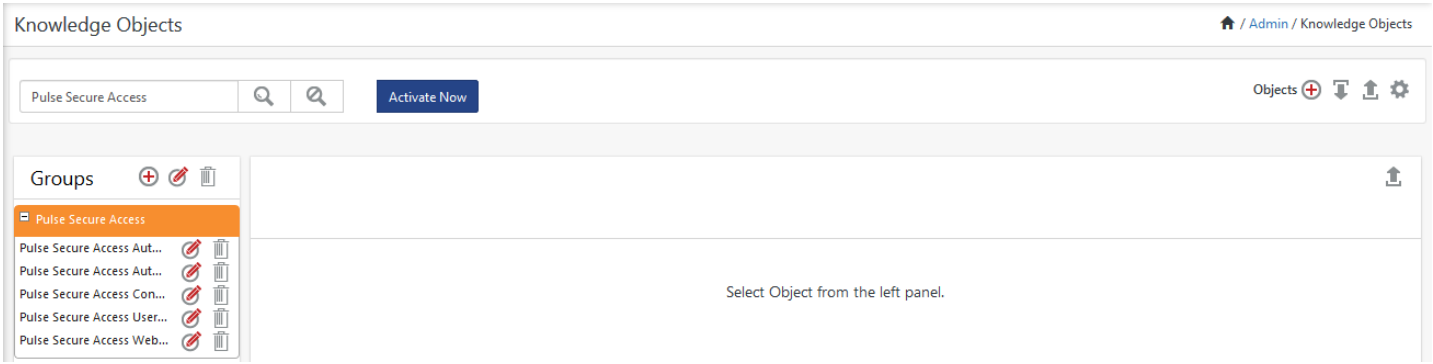

Figure 34

Flex Reports

1. Login to **EventTracker**.
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 **Pulse Secure Access** group folder.

   Reports are displayed in the Reports configuration pane.

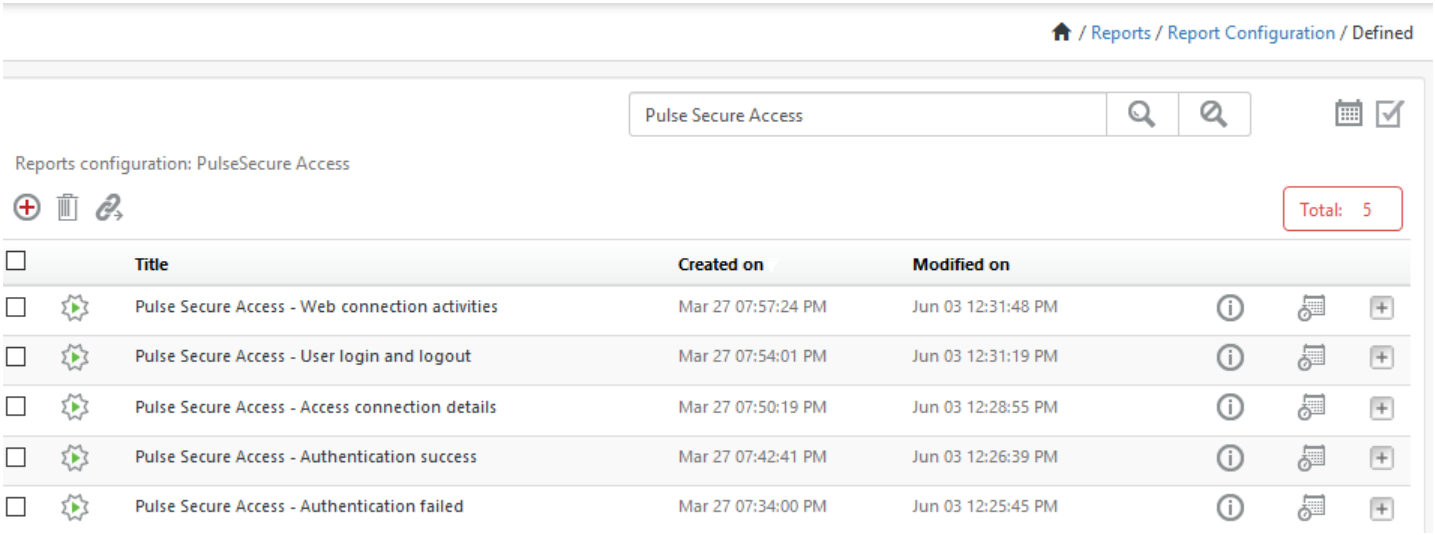

Figure 35

Dashlets

1. Login to **EventTracker**.
2. Click the **Dashboard** menu, and then **My Dashboard.**
3. Then click on **Customize Dashlet** button and search for **"Pulse Secure Access"**

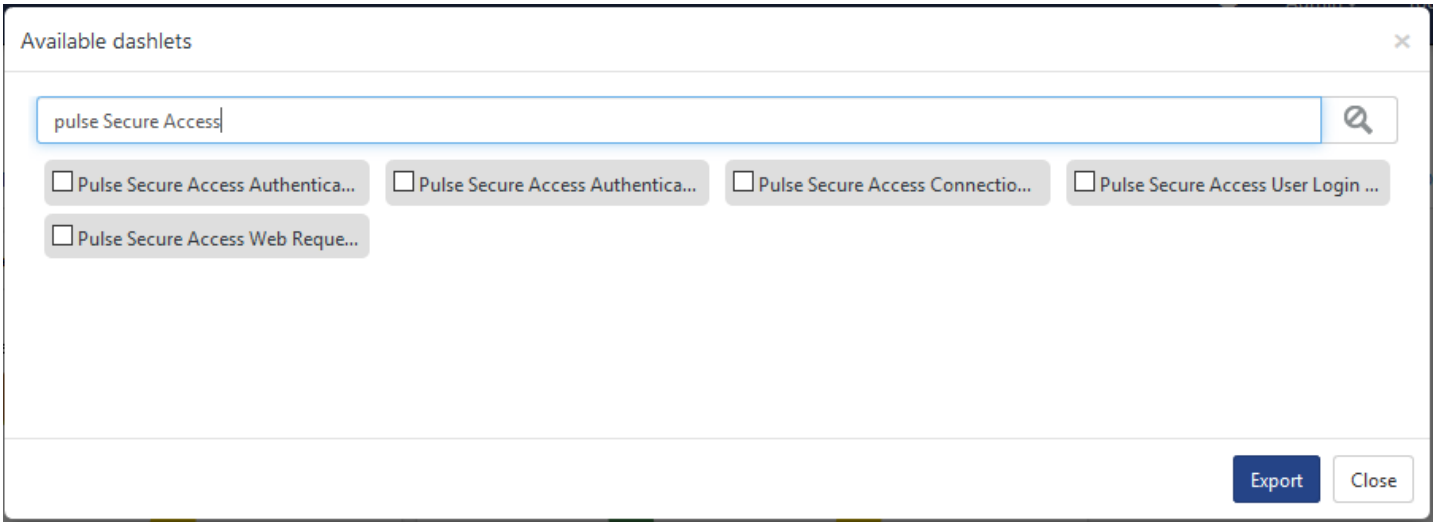

Figure 36

Token Template

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

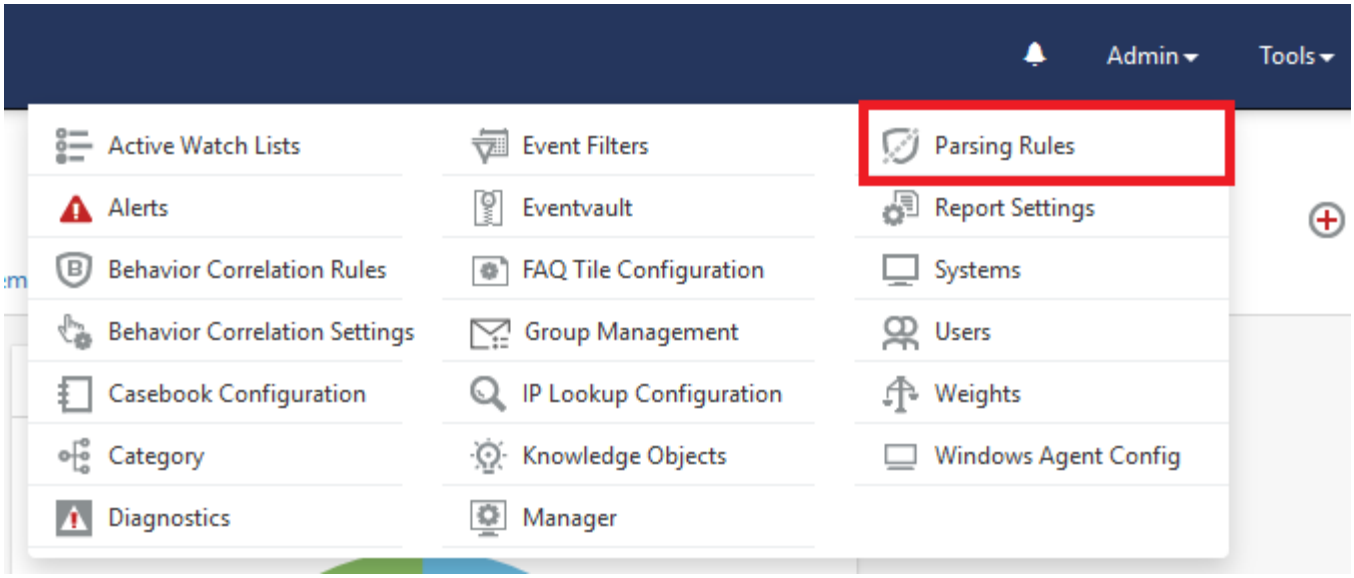

Figure 37

3. Click on **Template** and search for **Pulse Secure Access.**

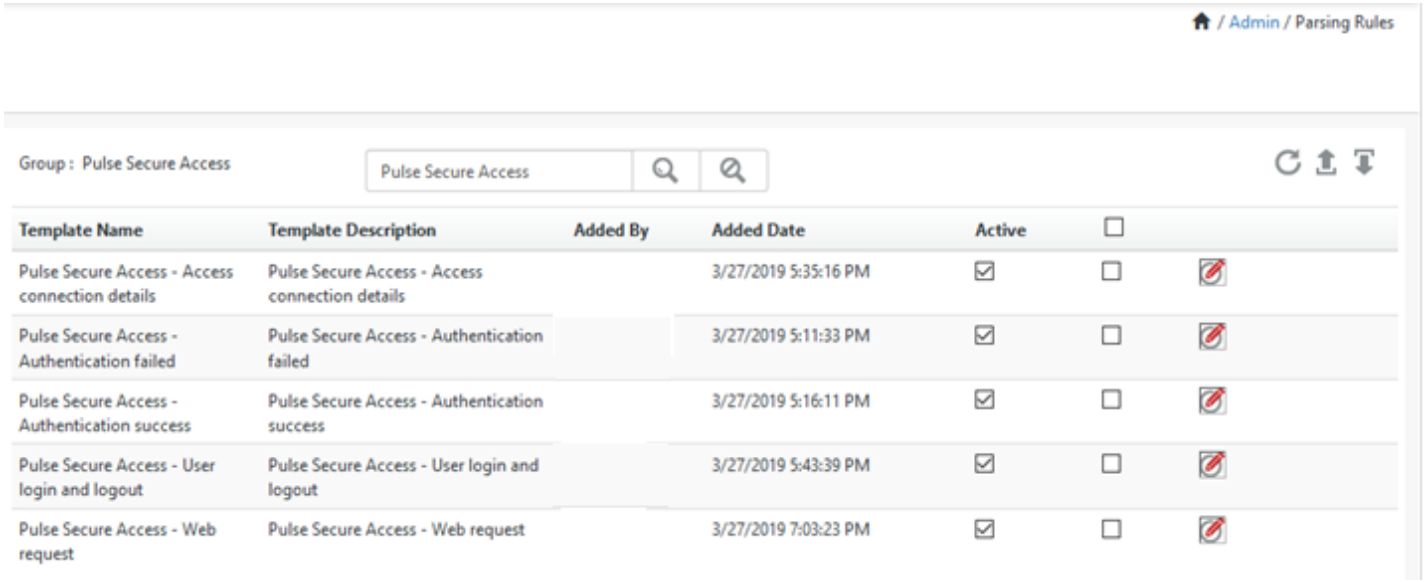

Figure 38