Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Pure Storage with EventTracker

EventTracker v9.2 and later

Publication Date:

April 20, 2021

Abstract

This guide helps you in configuring Pure Storage with EventTracker to receive Pure Storage events. In this guide, you will find the detailed procedures required for monitoring Pure Storage.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 and later, Pure Storage FlashArray FA-400, Purity v4.8 and later.

Audience

Administrators who are assigned the task to monitor and manage Pure Storage events using EventTracker.

Table of Contents

1. Overview

Pure Storage provides an all-flash enterprise array storage for vendors. They provide the logs which allow administrators to troubleshoot issues and oversee their infrastructure operations from a single, simple -to-use application quickly and easily. Using the Flash Array syslog server, these logs can be forwarded for future analysis.

Pure storage logs can be integrated with EventTracker via syslog. Pure Storage sends events information like volume activities, user activities, cluster activities, audit events, etc. EventTracker generates a detail reports for additional volumes that are attached, created, deleted, user logon activities, etc. Its graphical representation shows user login success, volumes created by device names and actions.

EventTracker triggers alerts in the event when a volume has been removed, flash array replication delayed, etc.

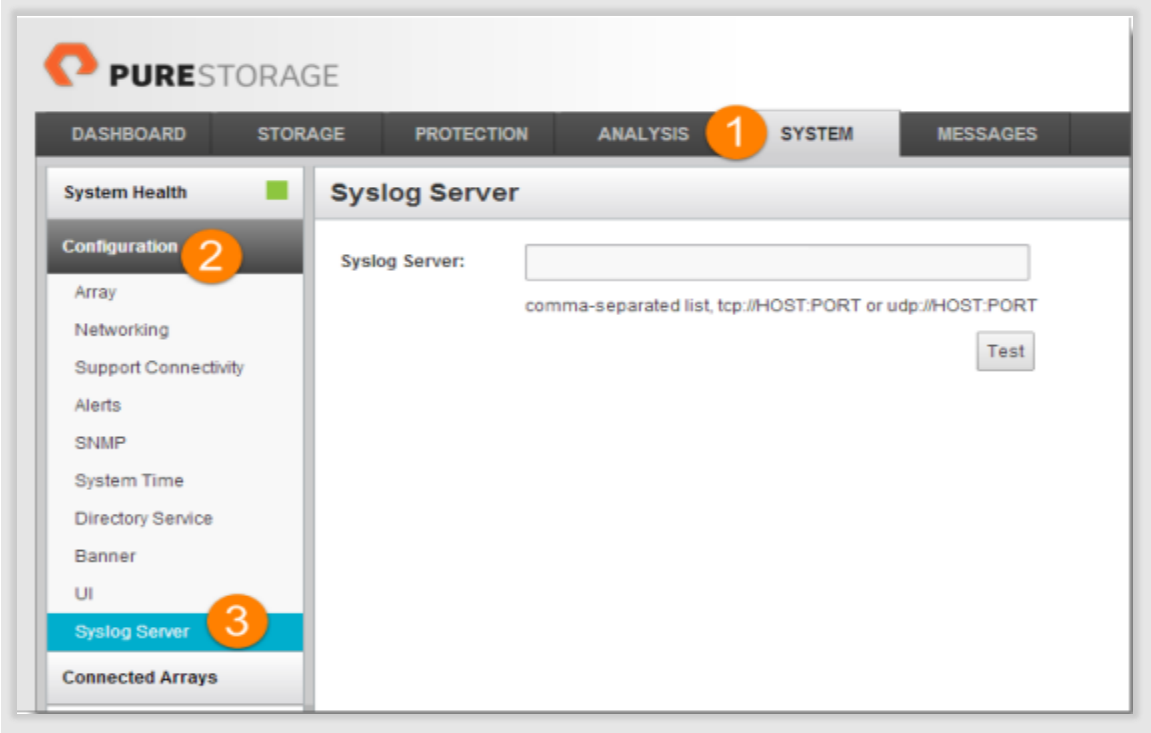
2. Prerequisites

- Admin access to Pure Storage.
- Pure storage Flash Array FA-400 series, Purity v4.8 and later should be installed.
- Collect EventTracker IP address for log integration.
- Allow syslog server port 514 if any firewall exists between Pure Storage and EventTracker.

3. Integrating Pure Storage events to EventTracker server

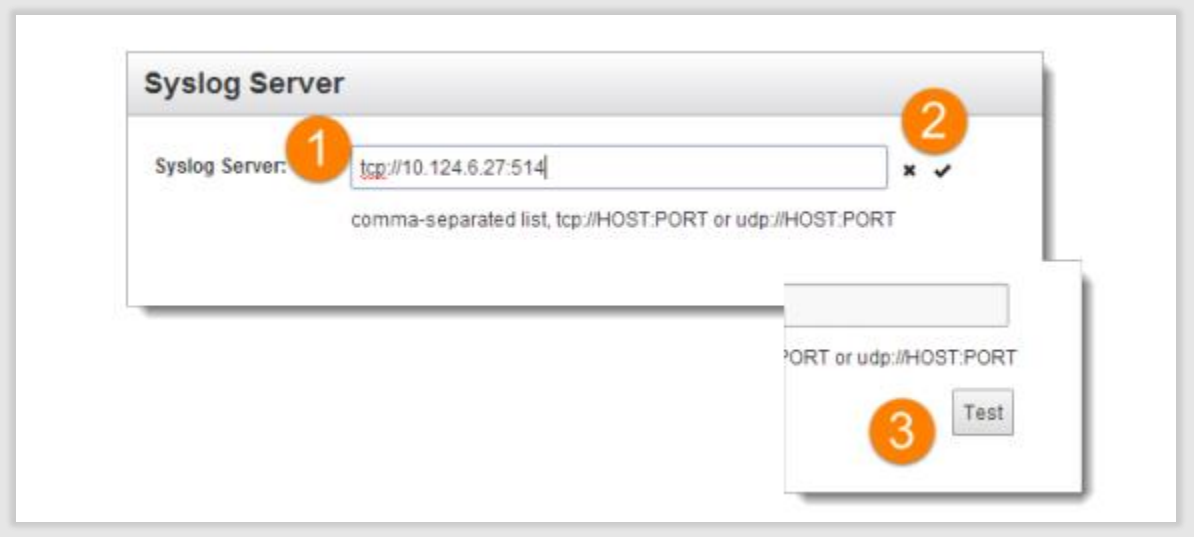
To get FlashArray information, log forwarding can be configured into the FlashArray syslog server. The simplest method for this is to use the Pure Graphical User Interface (GUI).

1. Login to the **Pure GUI** of your FlashArray using the Virtual IP of the array using authorized credentials (using privileges higher than read-only).
2. Navigate to the **System** tab, followed by the **Configuration** page and then the **Syslog Server** sub-entry as seen in the below figure.



3. The FlashArray Syslog Server supports all these combinations so choose the appropriate one for your environment.
    - **TCP Port 514**
    - **UDP Port 514**
    - **TCP Port 1514**

    For this example, TCP Port 514 will be used. Enter the IP or FQDN in the format like below: tcp://EventTracker_IP:514.
4. If there is already a syslog target there, append the address to the list in a comma-separated fashion.
5. After entering the address in the entry box, click the black check mark to save it and then click the test button that appears below the entry box. This will send a test message immediately.
6. If the message does not appear, check the syntax and accuracy of the **address/port/protocol** and **firewall settings**.



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 Categories

Pure Storage: User logon activities – This category provides events information related to user try to log into Pure Storage and is successful.

Pure Storage: Additional volume activities – This category provides information related to additional volumes created, deleted, added, and removed.

Pure Storage: User login failed – This category provides information related to user failed login events.

4.2 Alerts

Pure Storage: Volume has been deleted or disconnected or removed – This alert is generated when additional volume has been removed or deleted or disconnected.

Pure Storage: User login failed – This alert is generated when the user tries to login and fails.

4.3 Reports

Pure Storage - User logon success – This report provides information user login success that are done in Pure Storage.

Log_Sample:

Apr 01 12:15:02 172.21.250.22 Apr 1 12:15:02 WKSTSRE-ct1 purity.audit: (login message ID: 10089041) Array name: 'wkstssrv645' Controller: 1 Interface: 'GUI' Module: '' Session: '9c6360-68c6-4042-8bcf-

81a00f7fc' UTC Time: 2021-04-01T12:13:16Z User: 'joeb' Location '172.21.120.124' Sublocation: 'Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/89.0.4389.90 Safari\/537.36 Edg\/89.0.774.63' Action: 'session end' Method: '' Result: Success Description: ''

Sample_Report:

LogTime	Computer	User Name	Source IP	Host Name	Authentication Method	Login Method	User Agent
04/19/2021 09:41:15 AM	PURE_STORAGE	kenneth	172.221.2.4	WKSTS328		CLI	MozillaV5.0 (Windows NT 10.0; Win64; x64) AppleWebKitV537.36 (KHTML, like Gecko) ChromeV89.0.4389.90 SafariV537.36 EdgV89.0.774.63
04/19/2021 09:41:15 AM	PURE_STORAGE	joeb	172.21.2.6	WKSTSAR54	password	GUI	MozillaV5.0 (Windows NT 10.0; Win64; x64) AppleWebKitV537.36 (KHTML, like Gecko) ChromeV89.0.4389.90 SafariV537.36 EdgV89.0.774.63

Pure Storage - Volume activities – This report provides information of the additional flash array volumes created, added, deleted, removed, volume size, volume name, etc.

Log_Sample:

Apr 01 11:33:51 172.21.250.22 Apr 1 11:33:51 WKSTSRE-32-ct1 purity.audit: [kenneth (local)] purevol setattr Siemn_v2 --size 3T. Message ID: 189038 UTC Time: 2021-04-01T10:33:51Z Array Name: WKSTSRE32

Sample_Report:

LogTime	Computer	Host Name	User Name	Volume Name	Volume	Action
04/19/2021 09:41:15 AM	PURE_STORAGE	WKSTS432	pureuser	SYSDIS_VDI1	4T	setattr
04/19/2021 09:41:15 AM	PURE_STORAGE	WKSTSRE32	pureuser	IVIADT	500G	setattr
04/19/2021 09:41:15 AM	PURE_STORAGE	WKSTSRE32	pureuser	SYSDIS_VDI1	2T	setattr
04/19/2021 09:41:15 AM	PURE_STORAGE	WKSTSRE32	pureuser	SYSDIS_VDI2	2T	setattr
04/19/2021 09:41:15 AM	PURE_STORAGE	WKSTSRE32	pureuser	WKSTS432	2T	disconnect
04/19/2021 09:41:15 AM	PURE_STORAGE	wkstspure01	MAYA	SYSDIS_VDI2	2T	connect
04/19/2021 09:41:15 AM	PURE_STORAGE	WKSTS323	KENNETH	SYSDIS_V11DI2	5T	remove
04/19/2021 09:41:17 AM	PURE_STORAGE	WKSTSRE32	pureuser	SYSDIS_VDI1	2T	setattr
04/19/2021 09:41:17 AM	PURE_STORAGE	WKSTS323	KENNETH	SYSDIS_V11DI2	5T	remove

Pure Storage – User login failed – This report provides information related to user logon failure event i.e., when a user tries to login and fails. It will contain the fields information like username, IP address, login console type, etc.

Log_Sample:

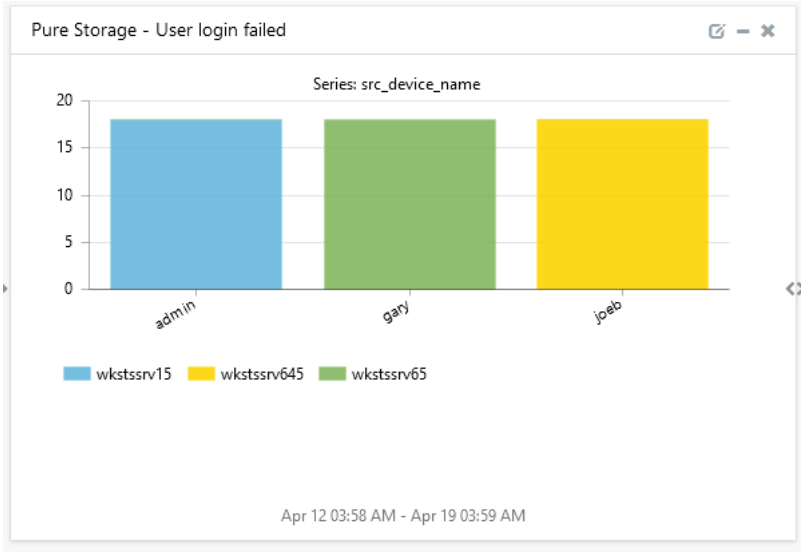
Apr 01 12:15:02 172.21.250.22 Apr 1 12:15:02 WKSTSRE-ct1 purity.audit: (login message ID: 10089041) Array name: 'wkstssrv645' Controller: 1 Interface: 'GUI' Module: '' Session: '9c6ddec60-68c6-4042-8bcf-81a06b00f7fc' UTC Time: 2021-04-01T12:13:16Z User: 'joeb' Location '172.21.2.4' Sublocation: 'Mozilla\/5.0 (Windows NT 10.0; Win64; x64) WebKit\/537.36 (KHTML, like Gecko) Chrome\/89.0.4389.90 Safari\/537.36 Edg\/89.0.774.63' Action: '' Method: '' Result: Fail Description: ''

Sample_Report:

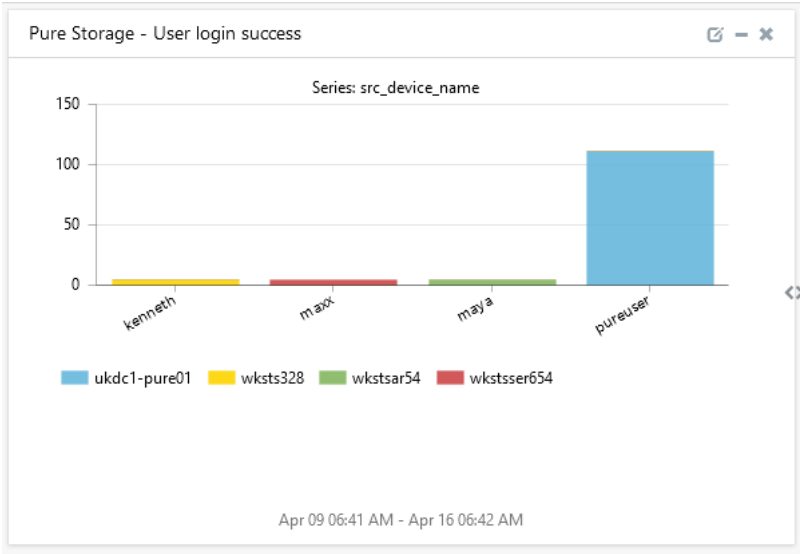
LogTime	Computer	User Name	Source IP	Login Method
04/19/2021 03:41:24 PM	WKSTSRE32	joeb	172.221.20.24	GUI
04/19/2021 03:41:24 PM	WKSTSRE32	gary	172.21.29.24	Rest
04/19/2021 03:41:24 PM	WKSTSRE32	admin	172.21.2.24	Rest
04/19/2021 03:41:26 PM	WKSTSRE32	joeb	172.221.20.24	GUI
04/19/2021 03:41:26 PM	WKSTSRE32	gary	172.21.29.24	Rest
04/19/2021 03:41:26 PM	WKSTSRE32	admin	172.21.2.24	Rest

4.4 Dashboards

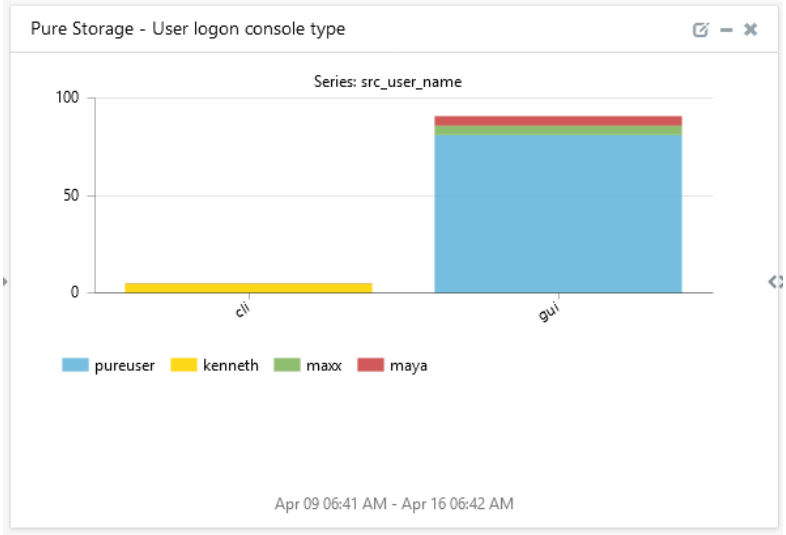
- **Pure Storage – User login failed**



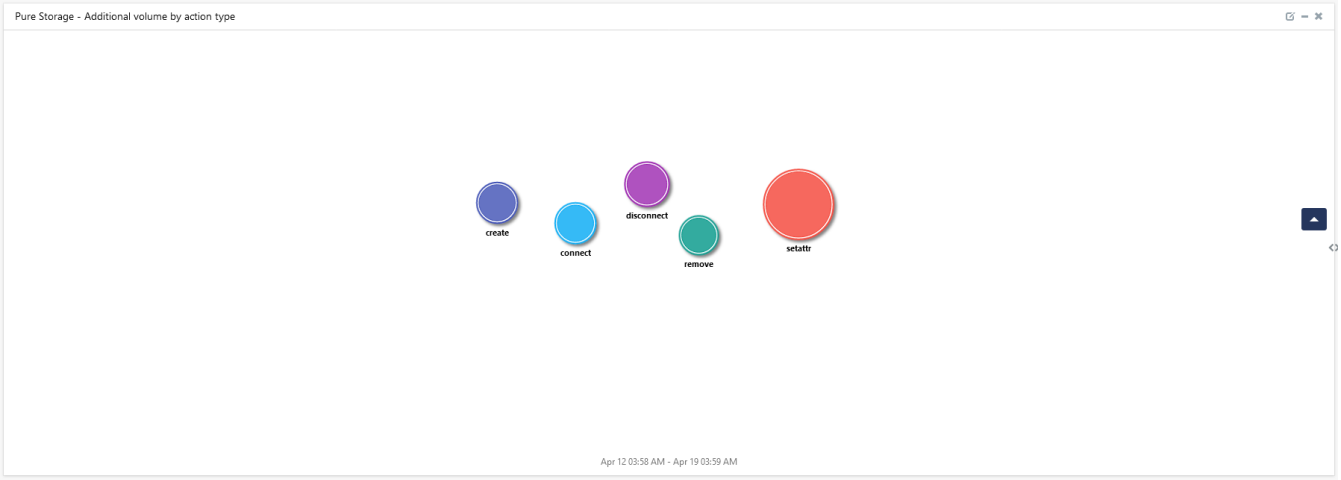
- **Pure Storage - User login success**



- **Pure Storage - User logon console type**



- **Pure Storage - Additional volume by action type**



- **Pure Storage - Additional volumes activities**

Pure Storage - Additional volumes activities

action	addl_info7	device_name	src_user_name	Count
setattr	2t	kindertons_vdi1	pureuser	13
setattr	2t	kindertons_vdi2	pureuser	13
setattr	500g	itvdi	pureuser	13
setattr	3t	kindertons_vdi1	pureuser	8
setattr	3t	kindertons_vdi2	pureuser	8
remove	5t	kindertons_v11di2	kenneth	5
setattr	4t	kindertons_vdi1	pureuser	5

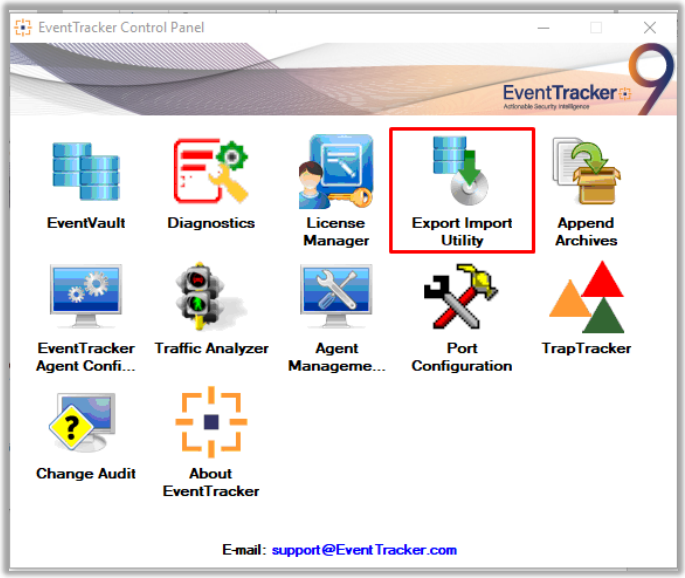
Apr 09 06:41 AM - Apr 16 06:42 AM

5. Importing Knowledge Pack into EventTracker

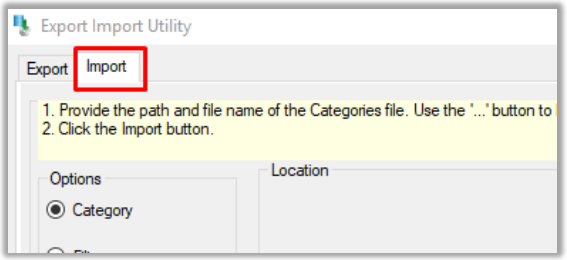
NOTE: Import knowledge pack items in the following sequence:

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

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



Export-Import Utility window opens.

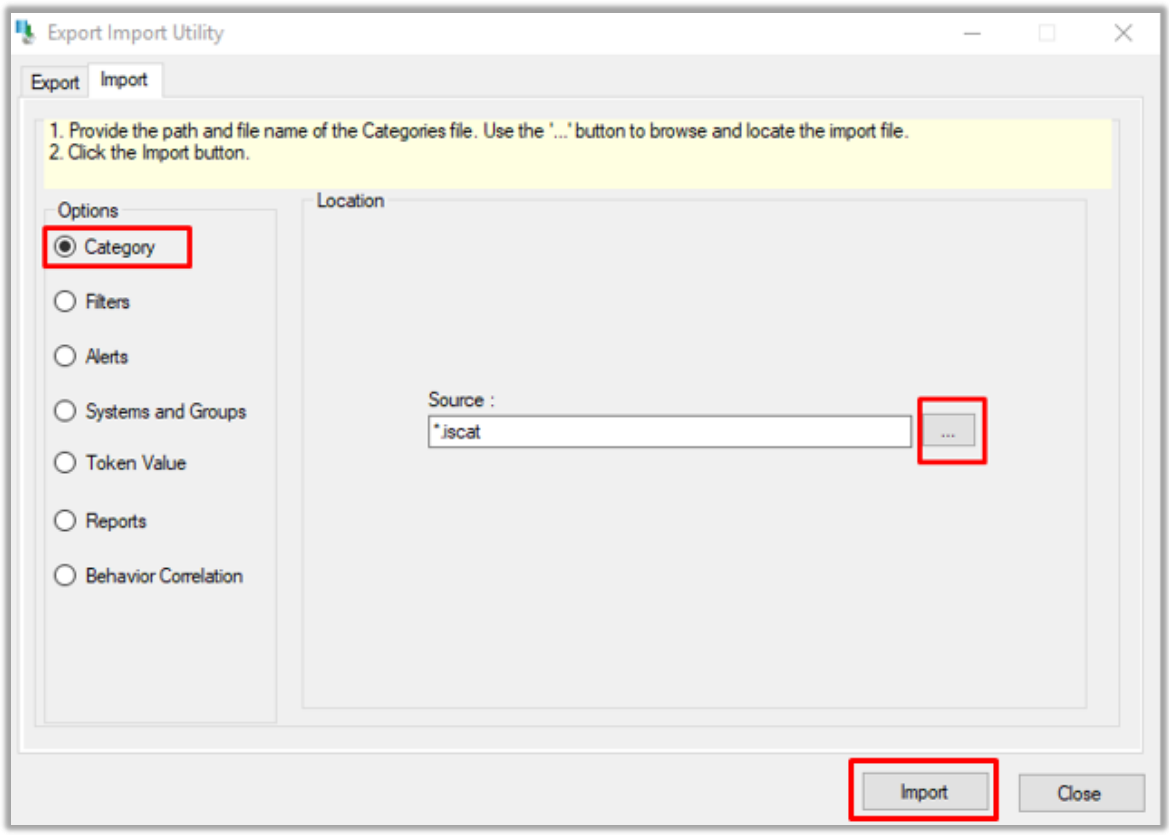


3. Click the **Import** tab.

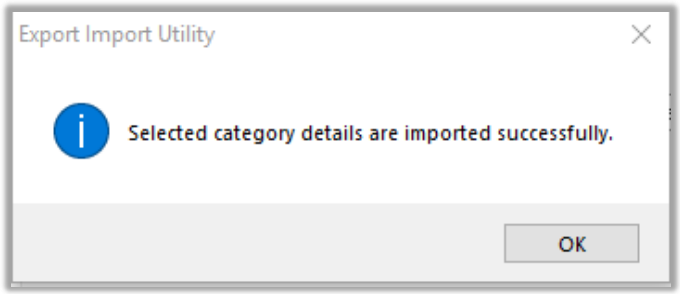
5.1 Categories

1. In **Export-Import Utility** window, select the **Category** option, and click **Browse** ...

2. Navigate to the knowledge pack folder and select the file with the extension **".iscat",** like **Categories_Pure Storage. iscat** and click **Import**.

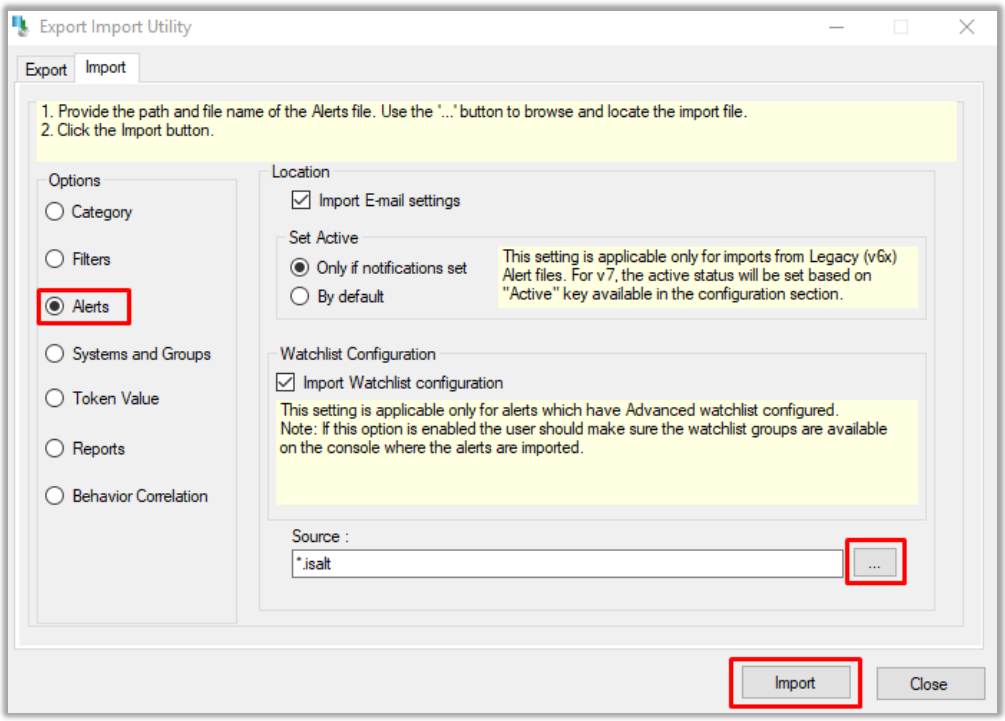


EventTracker displays a success message.

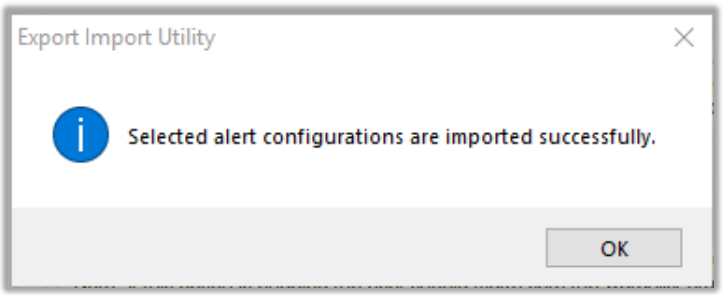


5.2 Alerts

1. In **Export-Import Utility** window , select the **Alert** option and click **Browse**.
2. Navigate to the knowledge pack folder and select the file with the extension **".isalt**", **e.g.**, "**Alerts_ Pure Storage.isalt**" and click **Import**.



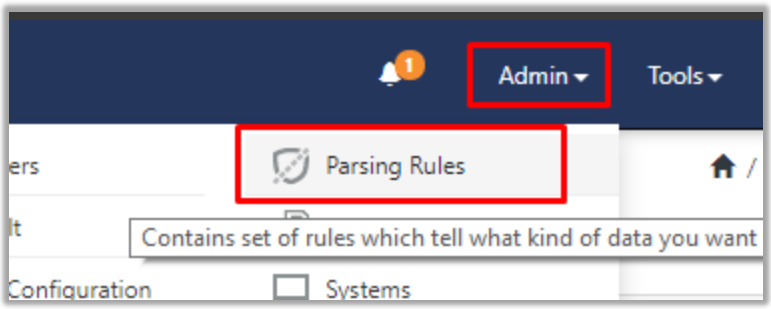
EventTracker displays a success message.



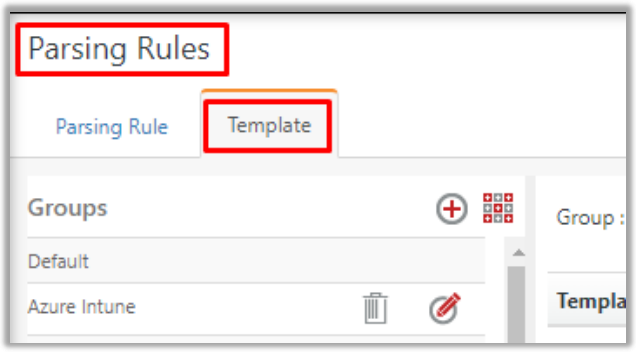
5.3 Token Template

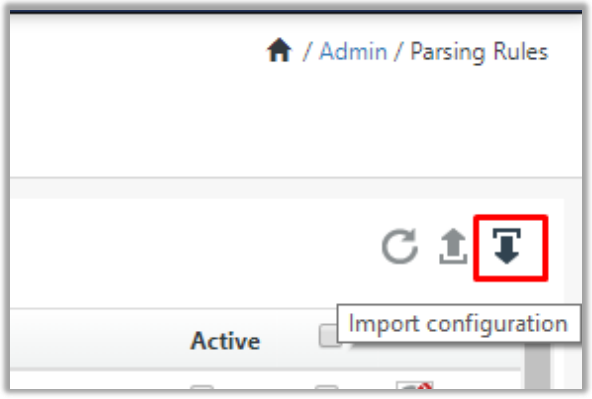
For importing **Token Template**, navigate to the **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.

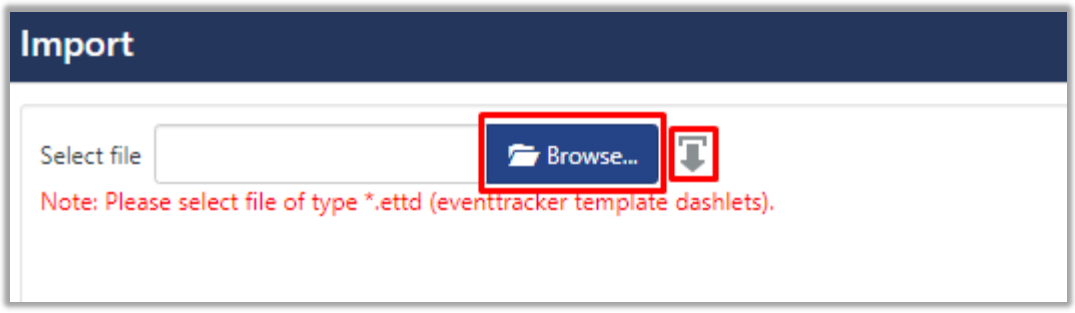


2. Click the **Template** tab and then click the **Import Configuration** button.



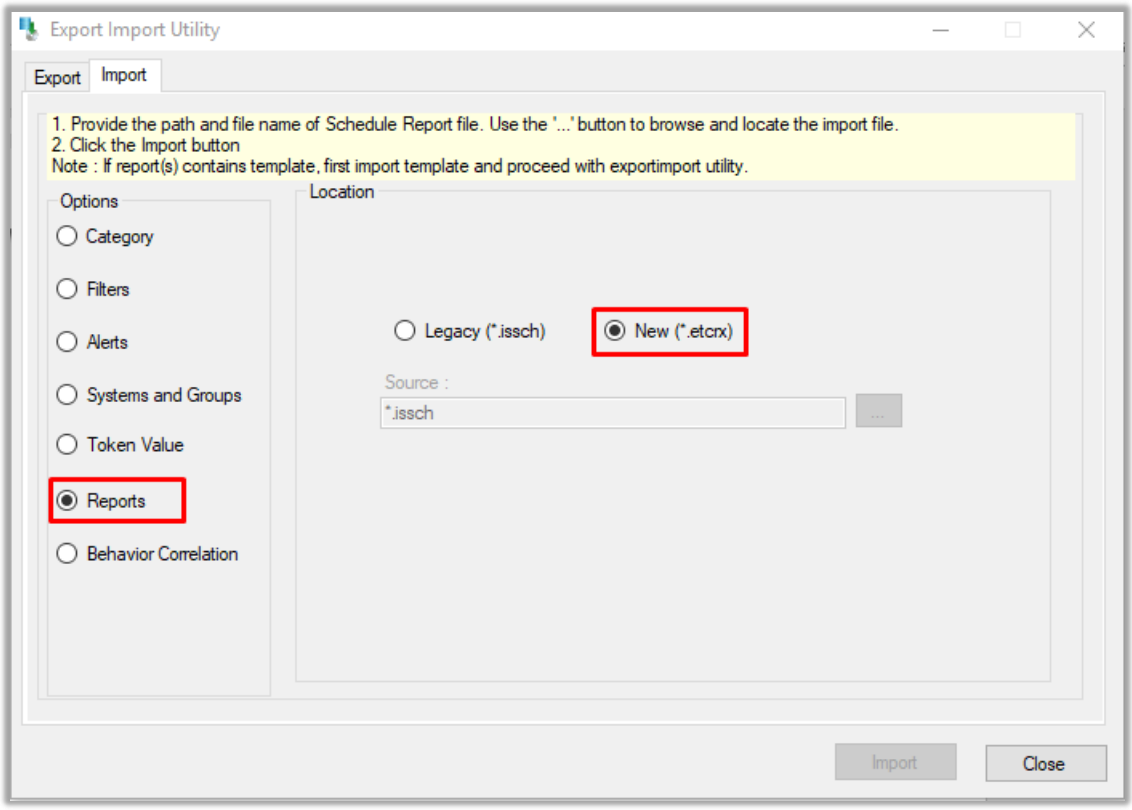


3. Click the **Browse** button and navigate to the knowledge packs folder (type **C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) where **".ettd", e.g., "Templates_Pure Storage.ettd"** file is located. Wait for a few seconds, as templates will be loaded. Once you see the templates, click desired templates and click **Import** button:

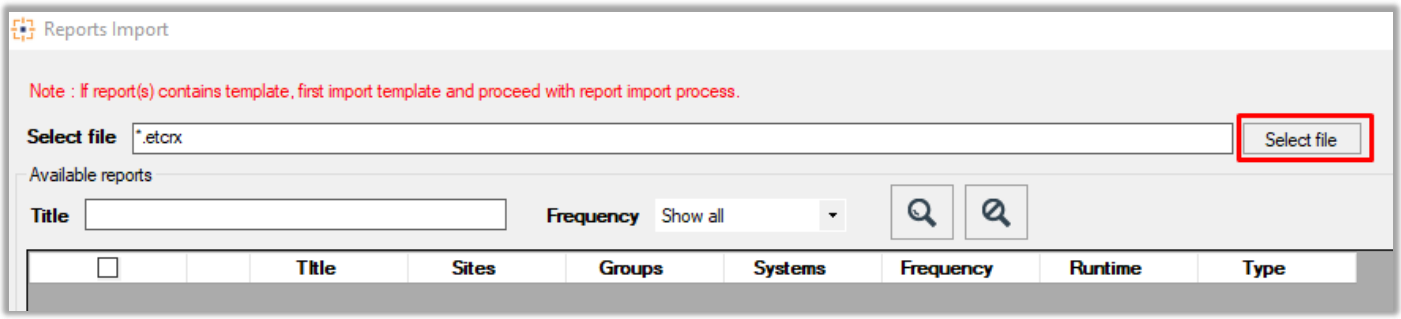


5.4 Flex Reports

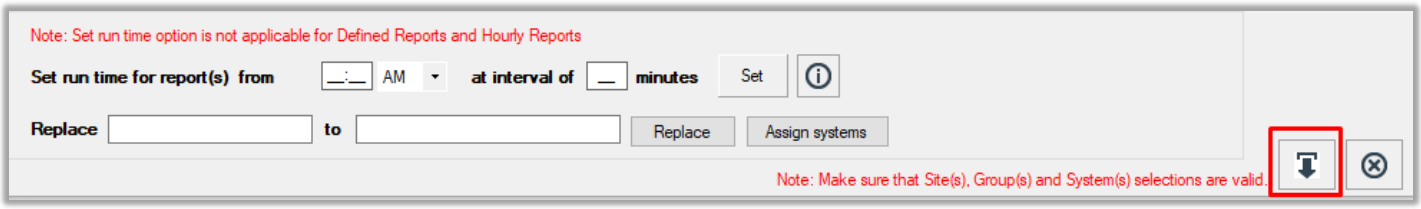
1. In **Export-Import Utility** window, select the **Import tab**. Click the **Reports** option, and choose **New (*.etcrx)**.



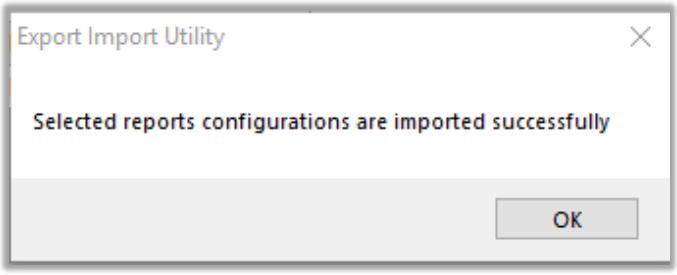
2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g., "Reports_Pure Storage.etcrx".**



3. Wait while reports populate. Select all the relevant reports and click **Import** .

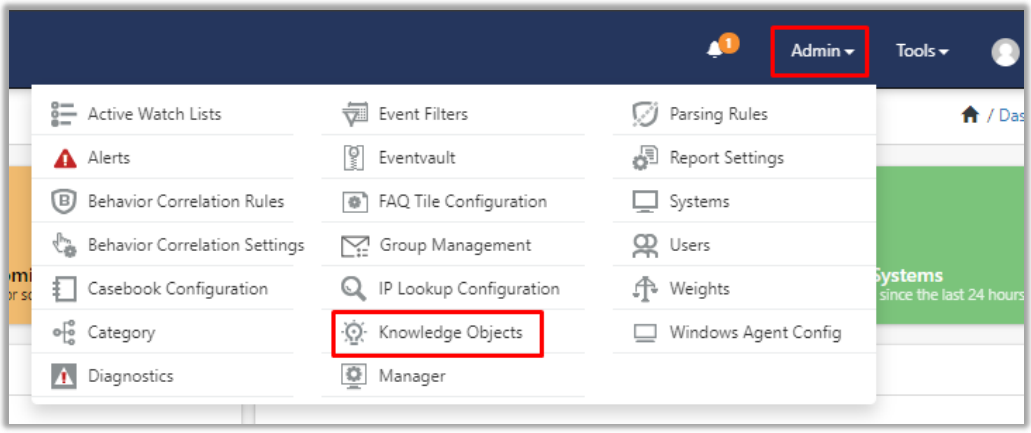


EventTracker displays a success message.

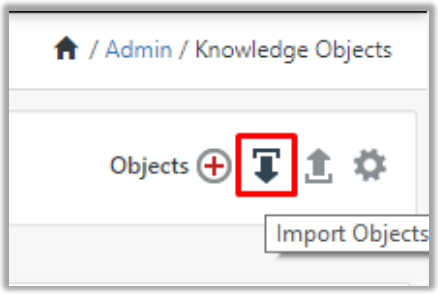


5.5 Knowledge Objects

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



2. Click the **import object** icon.

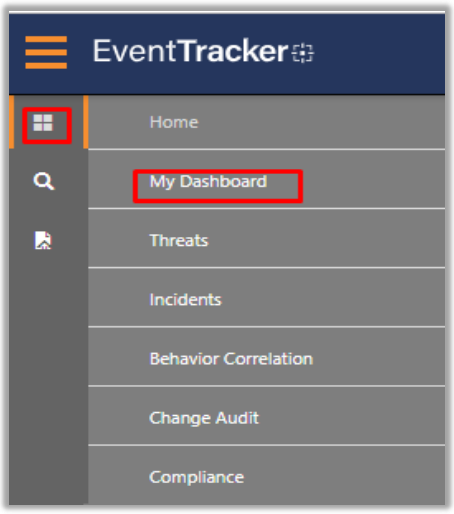


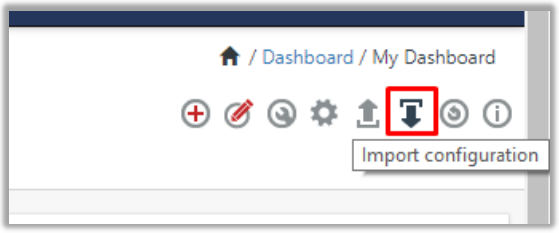
3. A pop-up box appears, click **Browse** and navigate to the knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g., "KO_Pure Storage.etko"** and click **Upload**.

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

5.6 Dashboards

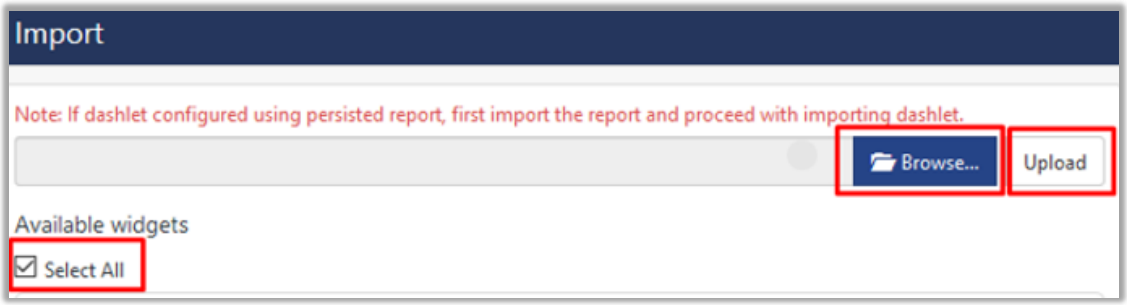
1. Login to the **EventTracker web interface**.
2. Navigate to **Dashboard** → **My Dashboard**.
3. In **My Dashboard**, Click the **Import** button.





4. Click **Browse** 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_Pure Storage.etwd**" is saved and click **Upload**.

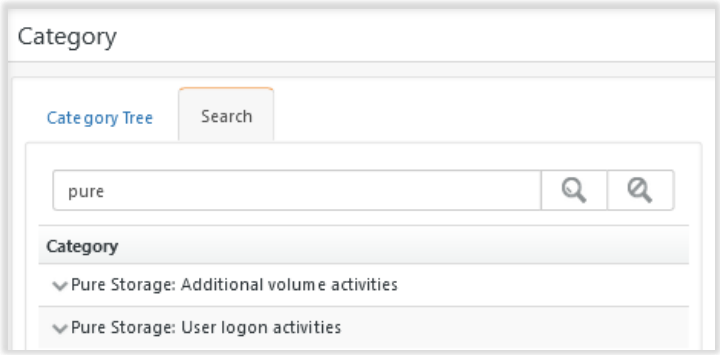
5. Wait while EventTracker populates all the available dashboards. Enable **Select All** and click **Import**.



6. Verifying Knowledge Pack in EventTracker

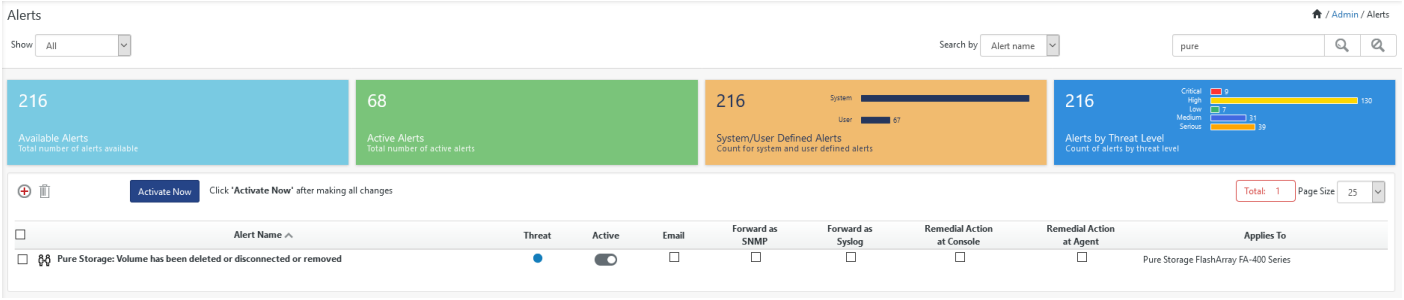
6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown and click **Categories**.
3. In **Category Tree** to view imported categories, click the **Search** tab and enter **Pure Storage** in the search**.**



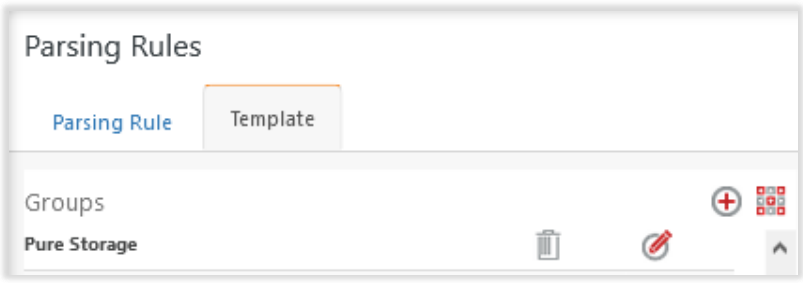
6.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter **Pure Storage** and click **Search**.
   EventTracker displays an alert related to Pure Storage**.**



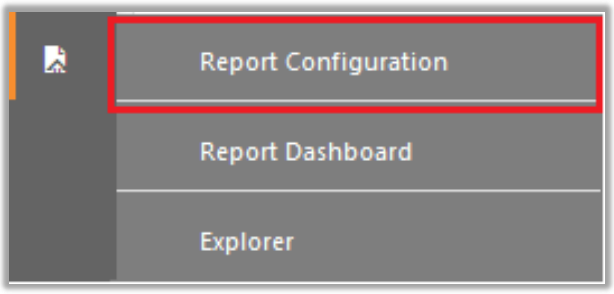
6.3 Token Template

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click **Parsing Rules**.
2. In the "Template" tab, click on the "Pure Storage" group folder to view the imported Token.

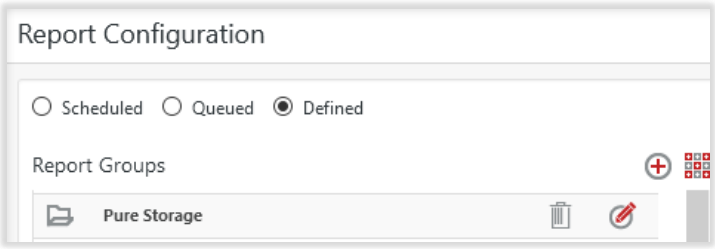


6.4 Flex Reports

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

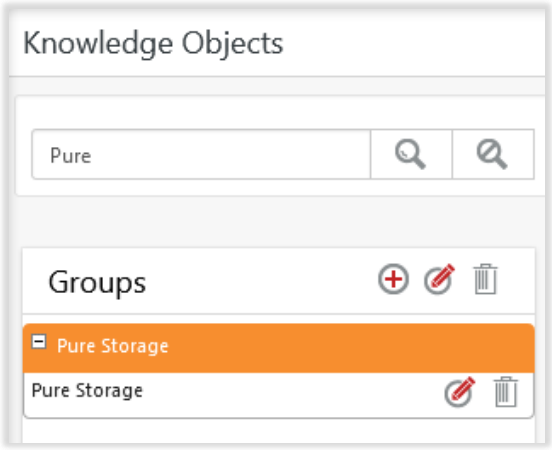


2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Pure Storage** group folder to view the imported reports.



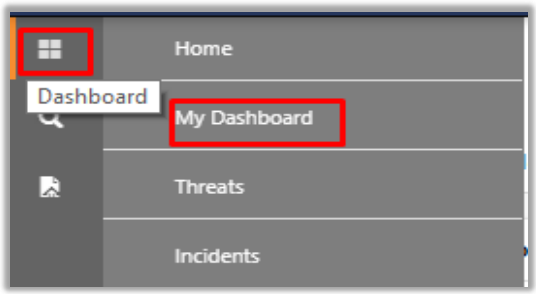
6.5 Knowledge Objects

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

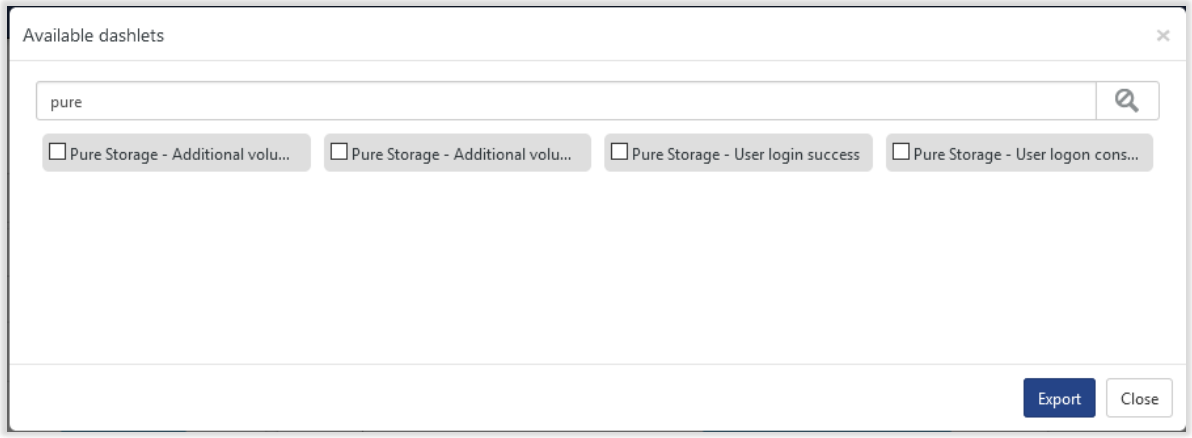


6.6 Dashboards

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



2. In the **Pure Storage** dashboard you see the following screen.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support