Netsurion™ | EventTracker

Integrate FortiManager with EventTracker

EventTracker v9.x and later

Publication Date: October 7, 2019

Abstract

This guide provides instructions to configure/ retrieve FortiManager events via syslog configuration. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor FortiManager.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and FortiManager 6.2.0 and later.

Audience

Administrators who are assigned the task to monitor FortiManager events using EventTracker.

Table of Contents

1.Overview

FortiManager appliance allows you to centrally manage many Fortinet devices from a few to thousands, including FortiGate, FortiWiFi, FortiCarrier, FortiMail, and FortiAnalyzer appliances and virtual appliances, as well as FortiClient endpoint security agents.

EventTracker, when integrated with FortiManager, enables users to view critical information related to activities performed in FortiManager or other Fortinet devices. This information is represented in the form of report, alert and graphical/ pictorial representation(dashboard).

In this integration guide, logging is performed by forwarding FortiManager logs to the EventTracker syslog server.

The logs which FortiManager forwards includes,

1. System manager (SYSTEM) events.
2. FortiGuard service (FGD) events.
3. FortiManager web service (FMGWS) events.
4. Managed device operations (DEVOPS) events.
5. High Availability (HA) events.
   Etc.

2.Prerequisites

- EventTracker agent should be installed in the host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privileges on the host system/ server to run PowerShell.

3.Integrating FortiManager with EventTracker

3.1 Forwarding FortiManager Logs to EventTracker

EventTracker receives the logs from FortiManager, once the syslog is configured in FortiManager:

1. Go to **System Settings** → **Advanced** → **Syslog Server**.
2. Select **Create New** to open the **New Syslog Server** window. (The Create New Syslog Server Settings pane opens.)

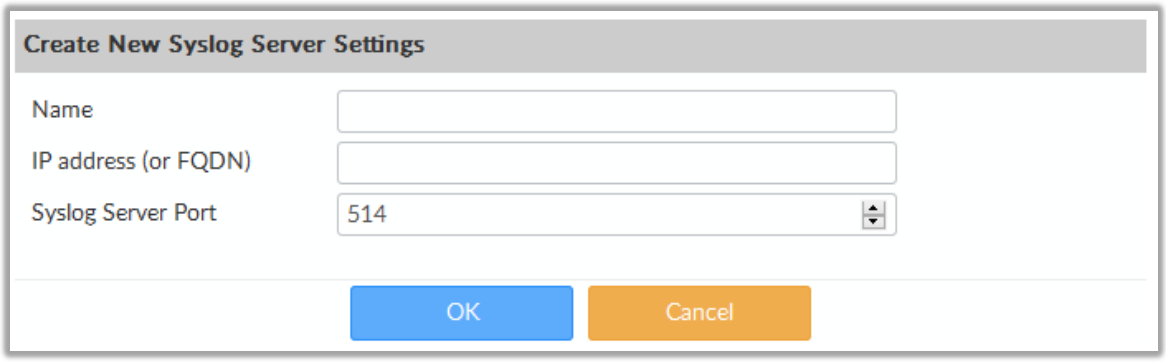

Figure 1

3. Fill in the Name, for example, “EventTracker”.
4. Fill in the IP address or FQDN of the EventTracker receiver.
5. Enter the Port number. The default is 514.

4.EventTracker Knowledge Pack

EventTracker knowledge pack for FortiManager includes:

1. Reports.
2. Alerts.
3. Saved searches.
4. Dashboards.

4.1 Reports

- **FortiManager - Deployment manager operations –** This report provides information about the process of deployment. It shows information about the failure or success status of deployment.

Log Time	Computer	ADOM Name	Description	Device name	Device serial number	Event subtyp	Log ID	Login user from	Message	Policy package name	Priority
43195.08735	xxxxxxdtpl12	my_adom	cdb event log for object changed	FL1000T	FGVM010000102012	dm	12021022	David, Miller	<LOG_ID_cfg_sync>	<Name of Policy Package which is installed>	Notice
4/6/2018 2:05	xxxxxxdtpl13	my_adom	cdb event log for object changed	FL100MK	FGVM010000102023	dm	12021002	Maria, Lou	<LOG_ID_update_n_ export_db>	<Name of Policy Package which is installed>	Error

Figure 2

- **FortiManager - Device Manager operations** – This report includes events related to FortiManager device activities.

Log Time	Computer	User	Action name	ADOM r	Description	Device name	Device serial num	Log ID	Message	Policy package name	Priority
4/6/2018 2:05	xxxxxxdtpl09	Karen	<Action towards this device>	my_adom	cdb event log for object changed	xxxxxxdtpl09	FGVM010000102012	22031004	<LOG_ID_dvmlog_ emerg>	<Name of Policy Package which is installed>	Emergency
4/7/2018 2:05	xxxxxxdtpl10	Peter	<Action towards this device>	my_adom	cdb event log for object changed	xxxxxxdtpl10	FGVM010000102012	220310047	<LOG_ID_dvmlog_ error>	<Name of Policy Package which is installed>	Error

Figure 3

- **FortiManager - FGFM protocol operations** - This report includes events related to FortiGate-FortiManager protocol operations.

Log Time	Computer	Log ID	Device name	User name	Description	Offline mode	Message
4/5/2018 2:05	xxxxxxdtpl21	2011003	FL1000T	Mathew	cdb event log for object changed		<LOG_ID_connection_down>
4/6/2018 2:05	xxxxxxdtpl12	2011004	FL1000B	John	cdb event log for object changed	<Enabled>	<LOG_ID_offline_mode>

Figure 4

- **FortiManager - web service (Login Error**) – This report provides the summary of events like web UI connection established, login error or login notification.

Log Time	Computer	ADOM name	Log ID	User name	Description	Remote host	Message
4/6/2018 2:05	xxxxxxdtpl09	my_adom	23032003	Karen	cdb event log for object changed	example.com	<LOG_ID_login_error>
4/7/2018 2:05	xxxxxxdtpl10	my_adom	23032004	Brenden	cdb event log for object changed	example.com	<LOG_ID_login_notif>

Figure 5

- **FortiManager – Device configuration changes/ operations –** Device configuration operation includes events where the new configuration is added of updated on the existing objects.

Log Time	Computer	Log ID	Event subtype	User name	Description	Message	Priority
4/2/2018 14:05	xxxxxxdtpl12	3012002	devcfg	Matt, Henry	cdb event log for object changed	LOG_ID_installcmd	notice
4/3/2018 15:05	xxxxxxdtpl13	3012002	devcfg	George, Philip	cdb event log for object changed	LOG_ID_installcmd	notice

Figure 6

- **FortiManager - Managed device operations –** Managed device operations include events such as unexpected/ unplanned reboot and shut down by Forti devices.

Log Time	Computer	Description	Device name	Event subtype	Log ID	Login user from	Message	Priority
4/3/2018 15:15	xxxxxxdtpl12	cdb event log for object changed	xxxxxxdtpl12	devops	27036002	<Login Session User From>	LOG_ID_reboot	critical
4/3/2018 16:05	xxxxxxdtpl13	cdb event log for object changed	xxxxxxdtpl13	devops	27036003	<Login Session User From>	LOG_ID_shutdown	critical

Figure 7

- **FortiManager - High Availability events** – High availability events are the events considered for a peer/ backup device for primary FortiManager appliance. This report will display the peer devices up/ down status (if any).

Log Time	Computer	Description	module	HA peer serial number	Message	Interface status	HA down cause
4/2/2018 14:05	xxxxxxdtpl12	cdb event log for object changed	<Identifier of the HA Sync Module>	<Serial Number of HA peer>	LOG_ID_status_chg_down	<HA status>	<Reason that causes HA status down>
4/3/2018 14:05	xxxxxxdtpl13	cdb event log for object changed	<Identifier of the HA Sync Module>	<Serial Number of HA peer>	LOG_ID_status_chg_up	<HA status>	<Reason that causes HA status down>

Figure 8

- **FortiManager - System manager events** – System management includes events associated with the devices/ system present in the network or associated with FortiManager.

Log Time	Computer	Log ID	Device_ name	IP address	Description	User name	Message	System reboot reason	System shutdown reason	Operation result
4/5/2018 14:05	xxxxxxdtpl12	1010018	FL1000B	30.23.145.221	cdb event log for object changed	John	<LOG_ID_login_info>			<Operation Result>
4/6/2018 14:05	xxxxxxdtpl13	1010014	FL100CH	30.23.145.222	cdb event log for object changed	Jimmy	<LOG_ID_ssh_auth_login_failure>			<Operation Result>
4/6/2018 14:05	xxxxxxdtpl13	1010014	FL100GQ	30.23.145.223	cdb event log for object changed	Karen	<LOG_ID_reboot>	<The reason for system reboot>		<Operation Result>
4/6/2018 14:05	xxxxxxdtpl13	1010014	FL100CA	30.23.145.224	cdb event log for object changed	Bob	<LOG_ID_shutdown>		<Power Failure>	<Operation Result>

Figure 9

4.2 Alerts

- **FortiManager: Unexpected system reboot**
- **FortiManager: Log daemon fluctuated**
- **FortiManager: Unexpected device reboot**
- **FortiManager: Unexpected device shutdown**
- **FortiManager: Unexpected system shutdown**
- **FortiManager: User login failed (SSH auth)**
- **FortiManager: User login failed (Web service)**

4.3 Saved searches

- **FortiManager - Device configuration operations (DEVCFG)**
- **FortiManager - High Availability status changes**
- **FortiManager - System login events**
- **FortiManager - User login fail (Web service) by user**
- **FortiManager - User login fail (SSH auth) detected**
- **FortiManager - System manager events**
- **Top 10 FortiManager log types**

4.4 Dashboards

- **FortiManager - User login fail (Web service) by user**

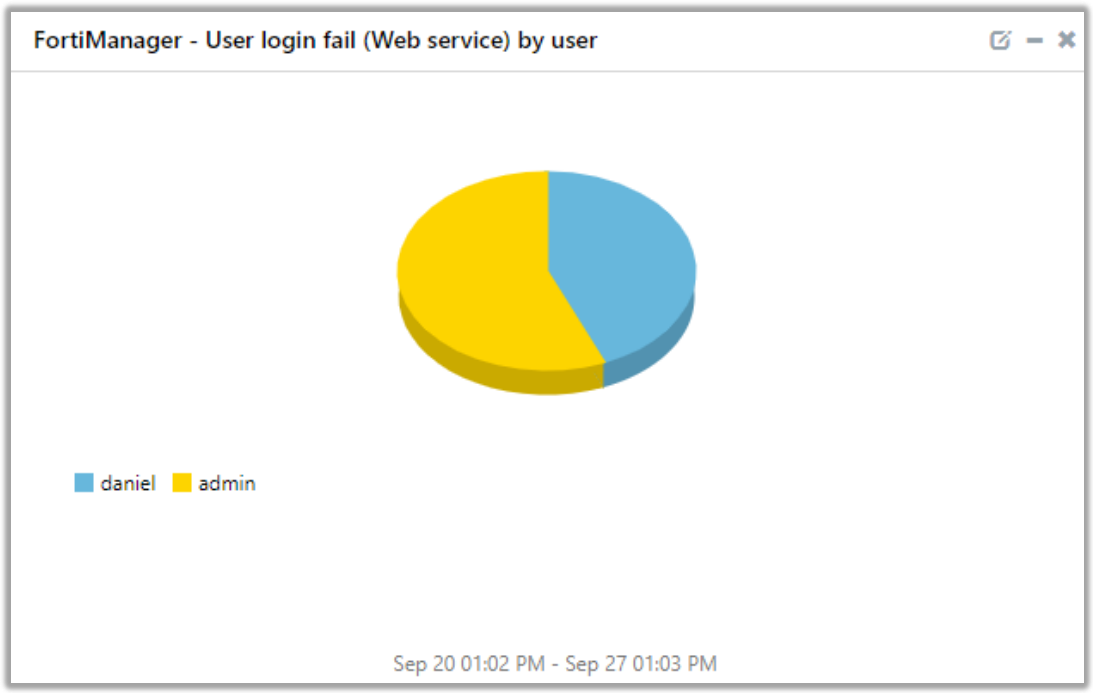

Figure 10

- **FortiManager - User login fail (SSH auth) by user**

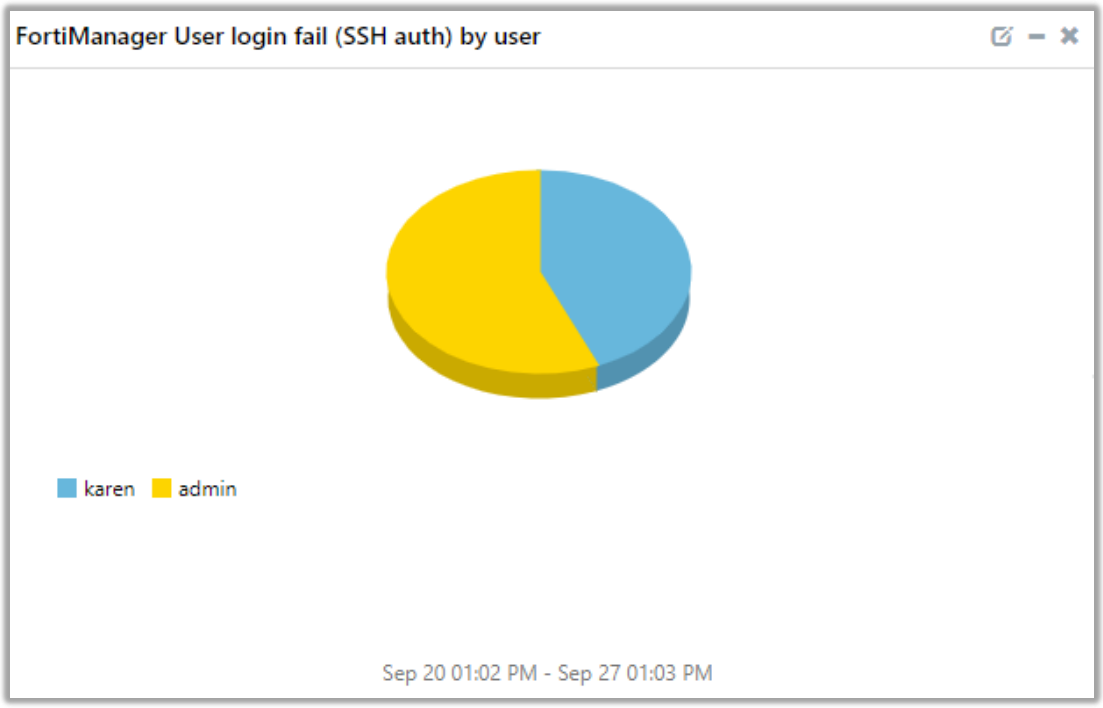

Figure 11

- **FortiManager - High Availability status changes**

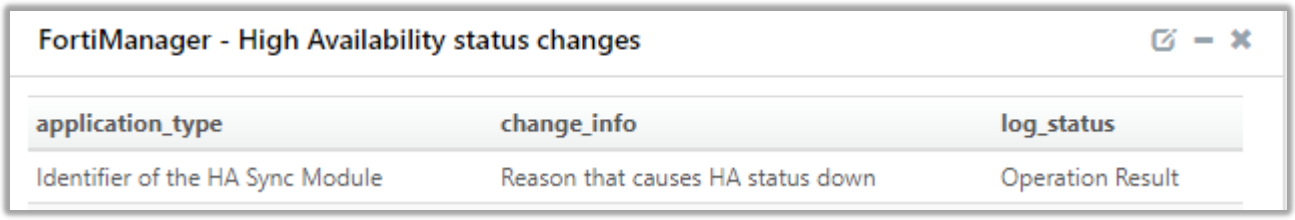

Figure 12

- **FortiManager - FGFM protocol status changes**

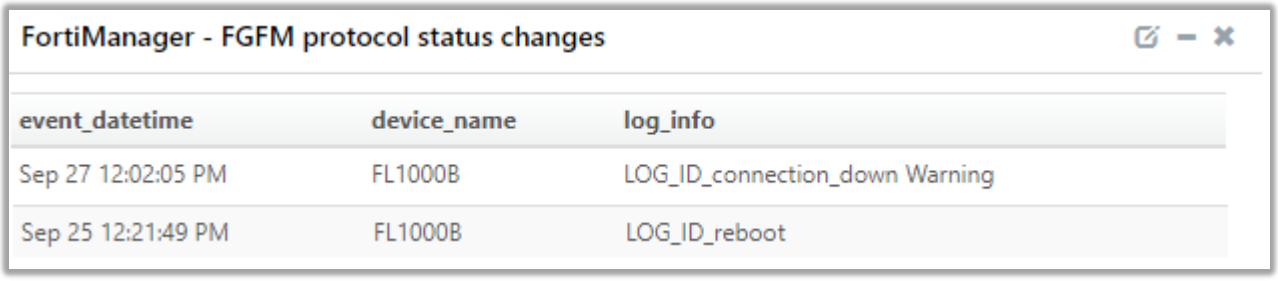

Figure 13

- **FortiManager - System login events**

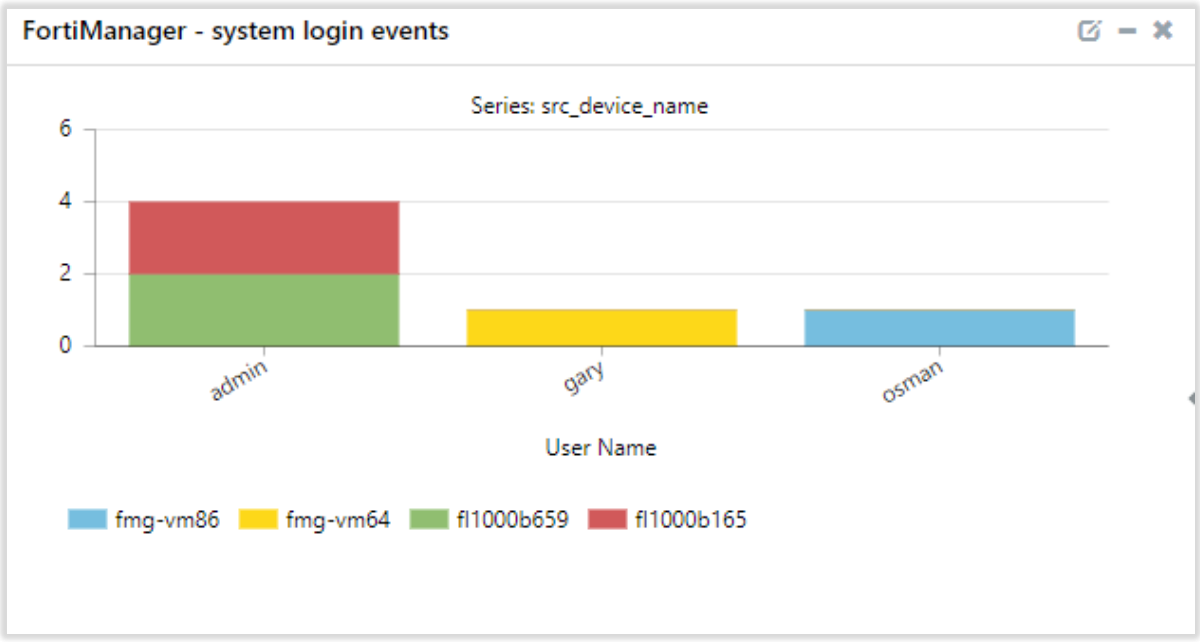

Figure 14

- **FortiManager - Managed device operations**

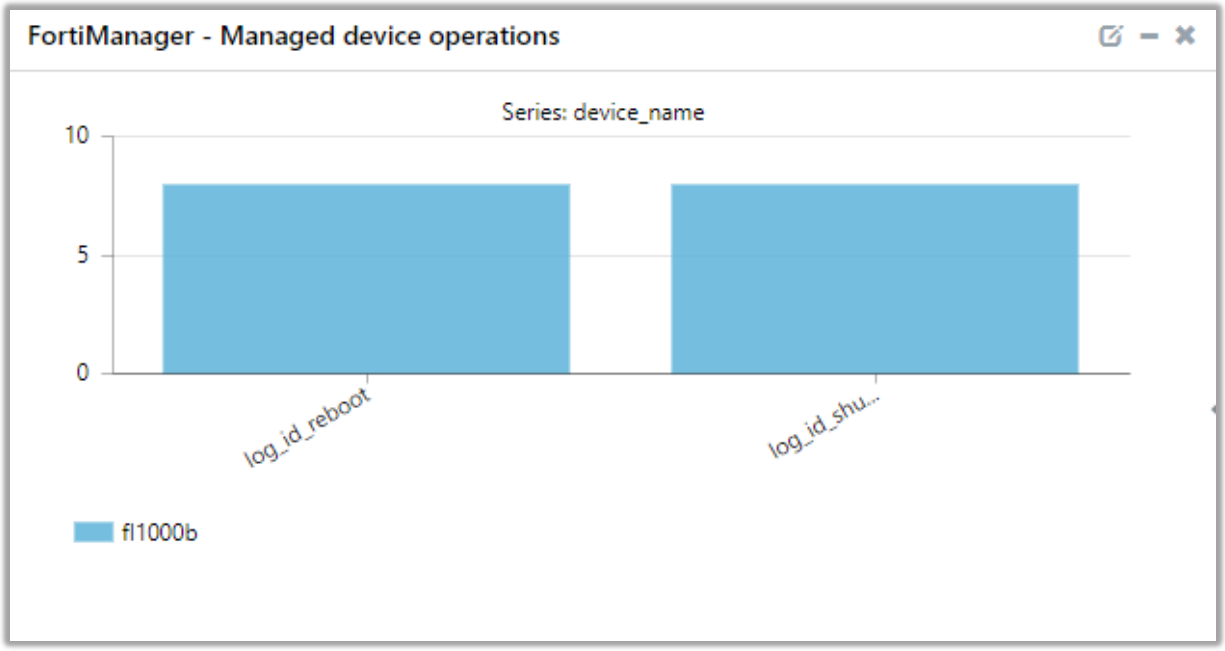

Figure 15

- **Top 10 FortiManager log types**

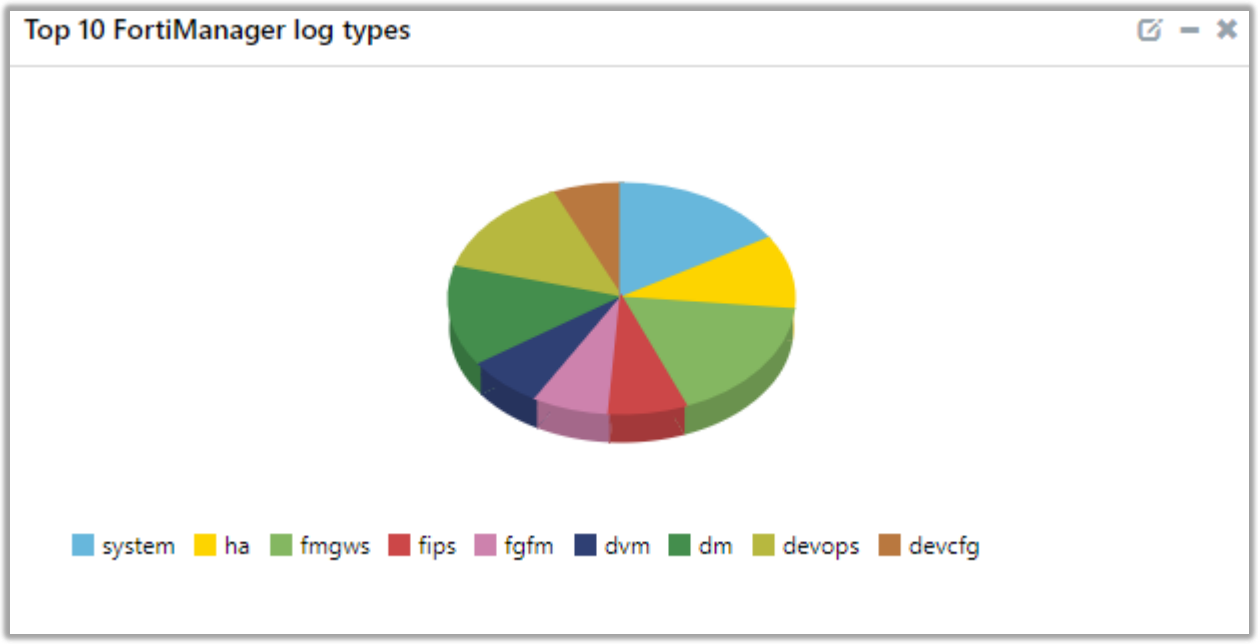

Figure 16

5.Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

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

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

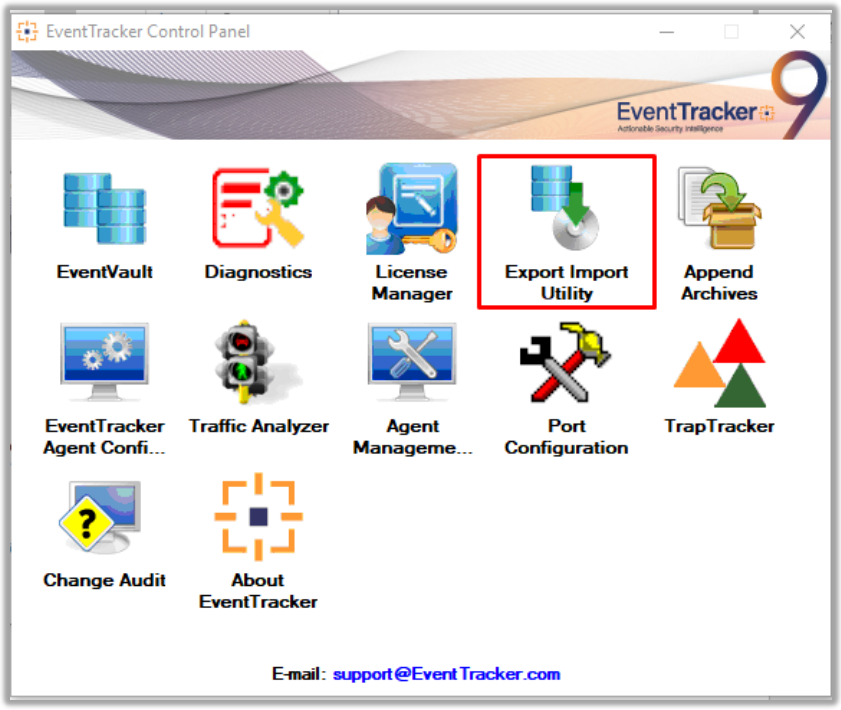

Figure 17

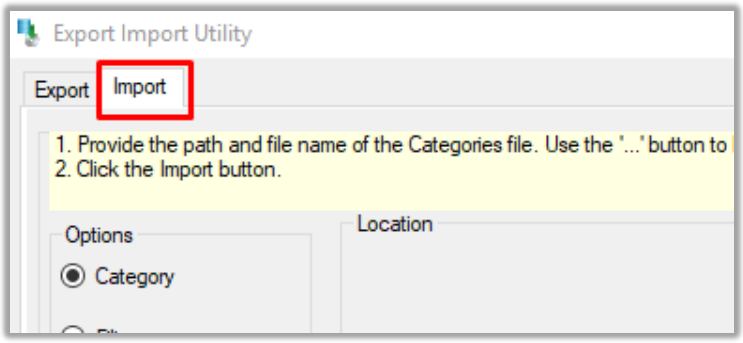

Figure 18

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 the extension **".iscat", e.g. "Categories_FortiManager.iscat"** and then click on the "**Import**" button:

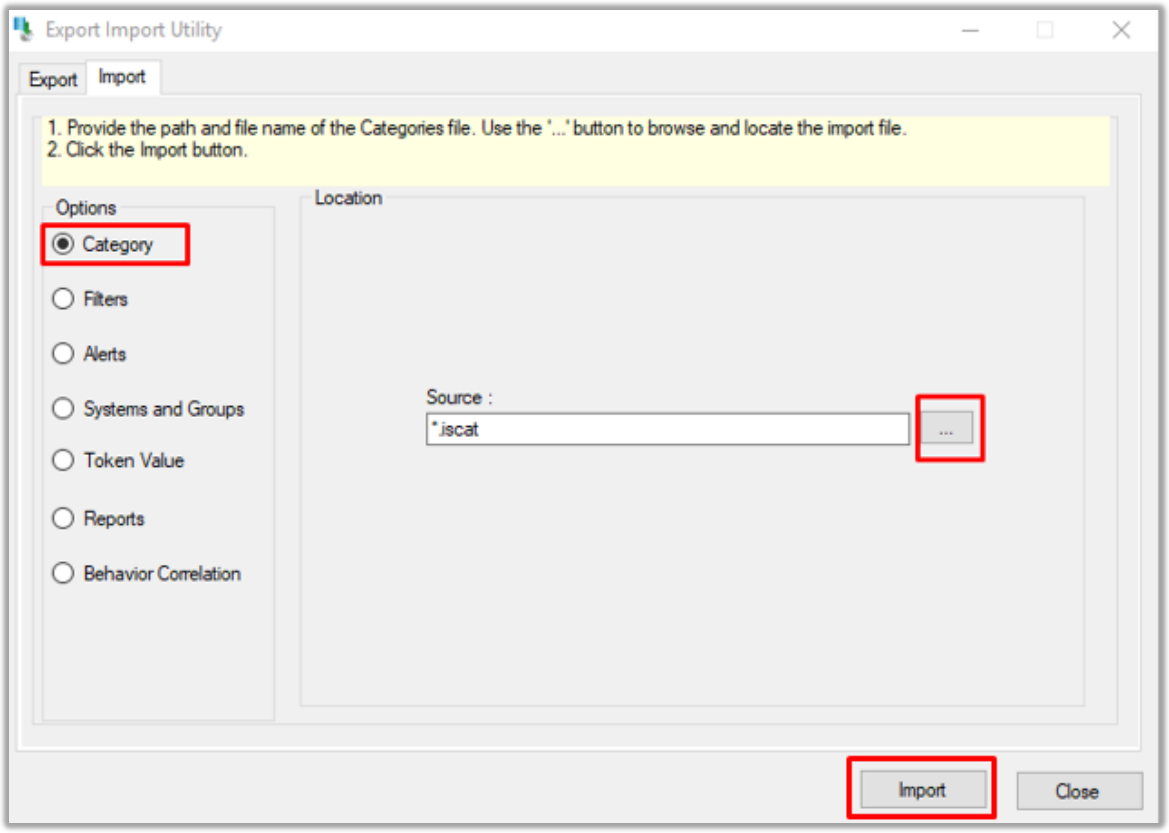

Figure 19

EventTracker displays a success message:

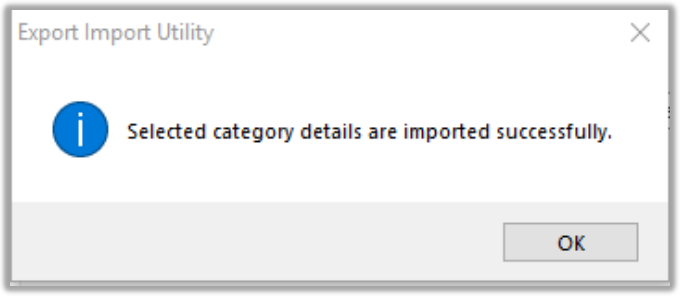

Figure 20

5.2 Alerts

1. Once you have opened "**Export Import Utility**" via "**EventTracker Control Panel**", click **Alert** option, and then click the browse button.
2. Navigate to the knowledge pack folder and select the file with the extension **".isalt"**, **e.g.** "**Alerts_ FortiManager.isalt**" and then click on the "**Import**" button:

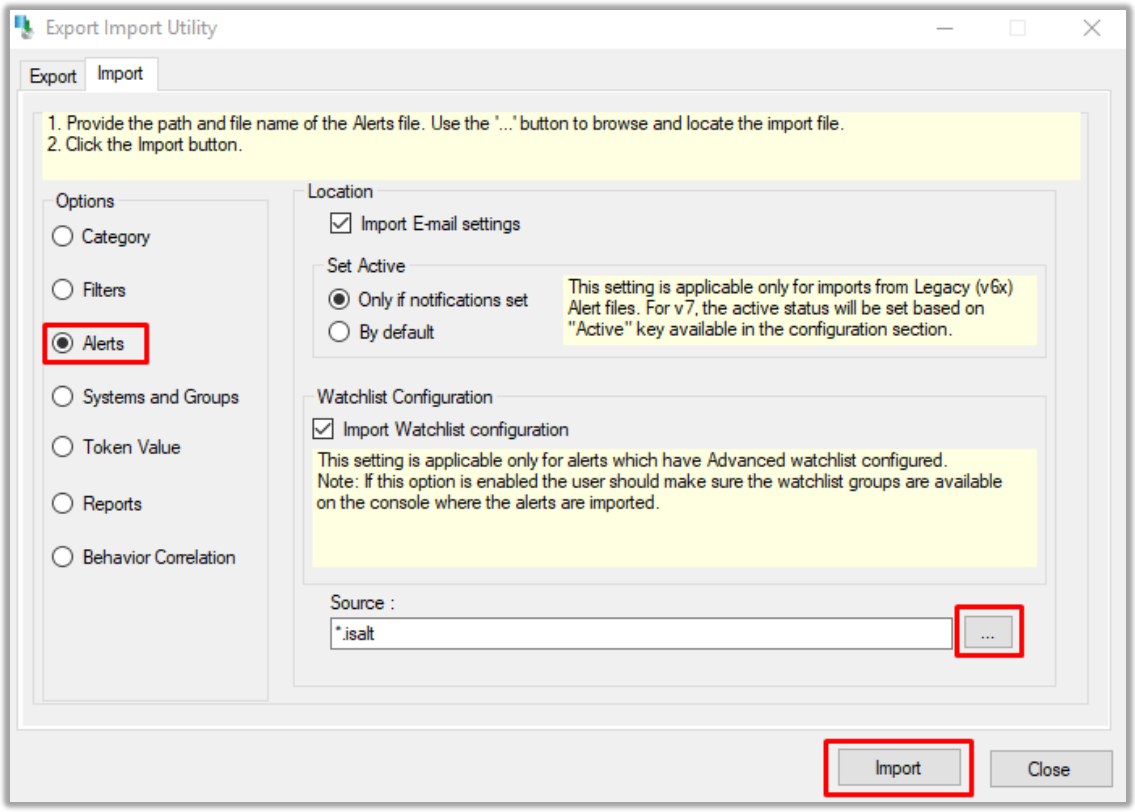

Figure 21

EventTracker displays a success message:

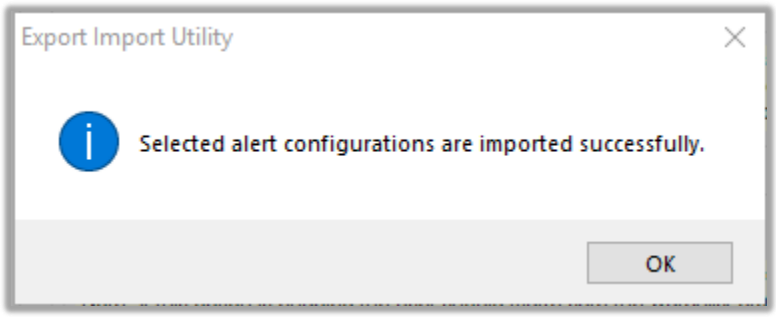

Figure 22

5.3 Token Templates

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

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

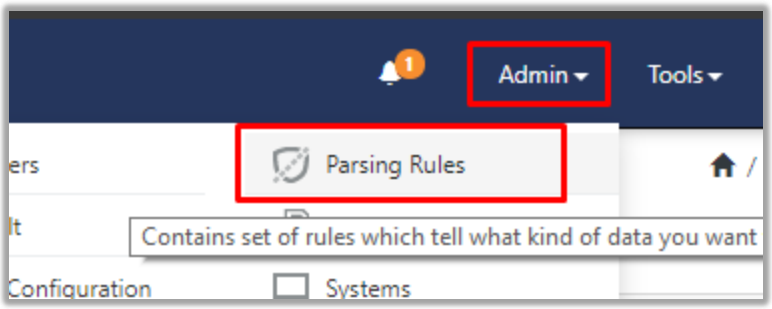

Figure 23

Next, click the "**Template**" tab and then click the "**Import Configuration**" button.

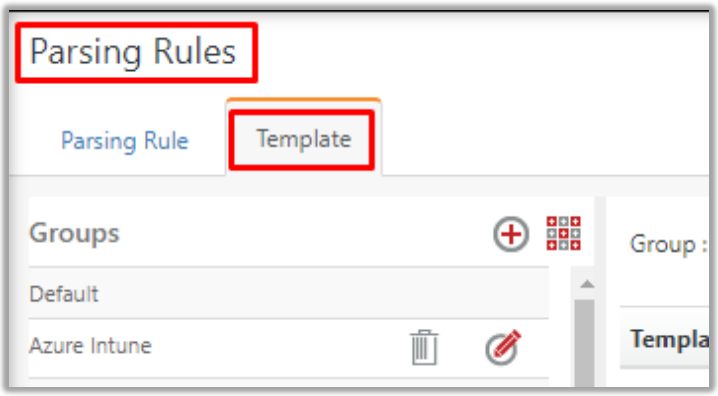

Figure 24

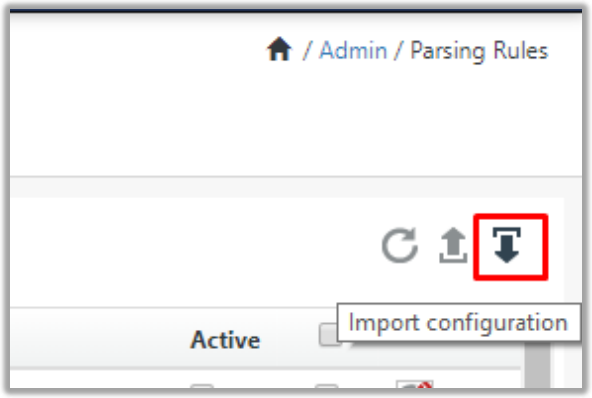

Figure 25

1. Now, 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_FortiManager.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:

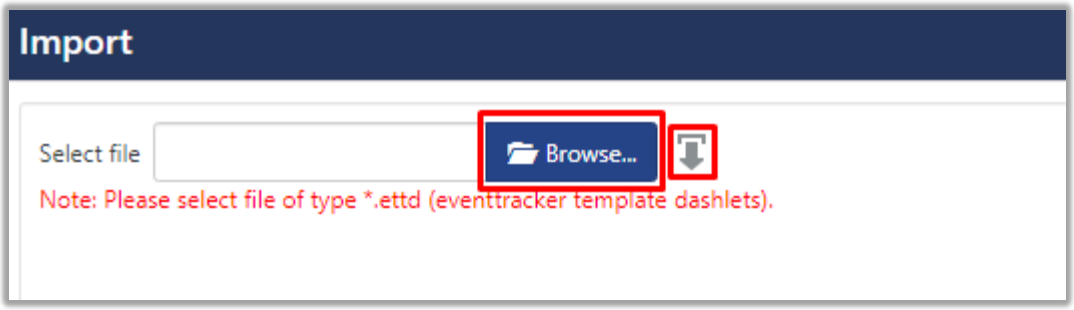

Figure 26

5.4 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)**":

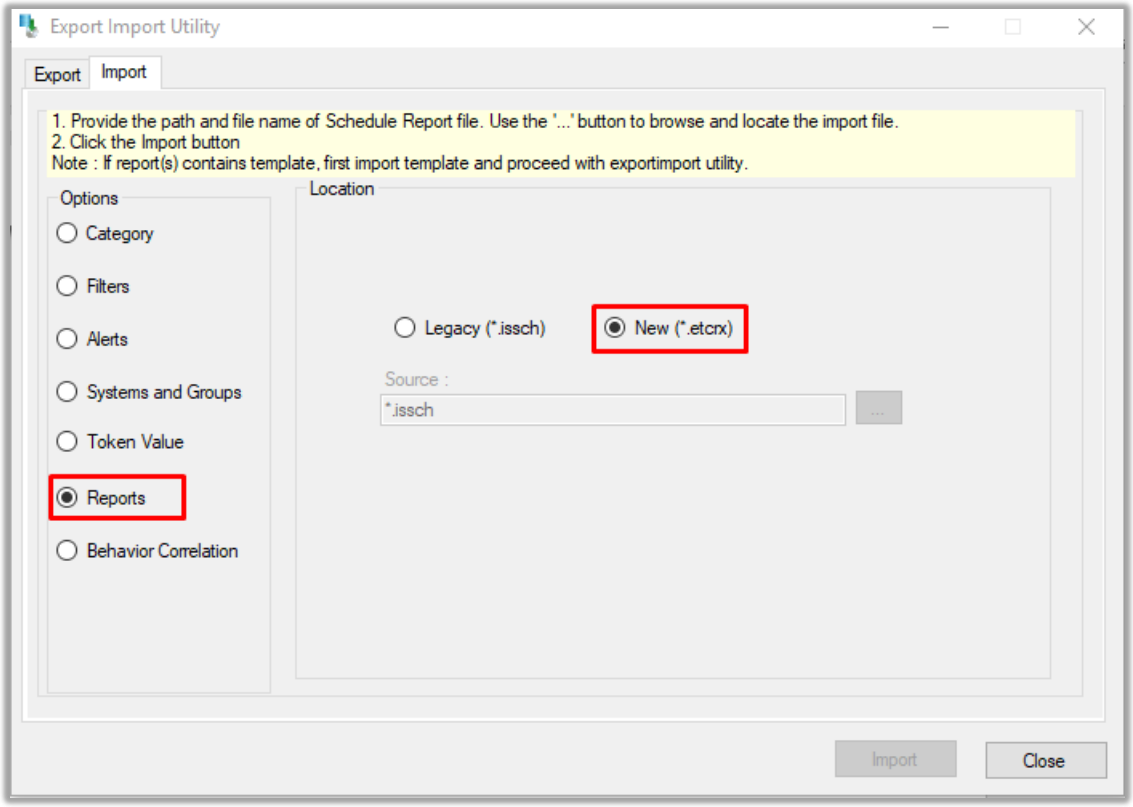

Figure 27

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_FortiManager.etcrx".**

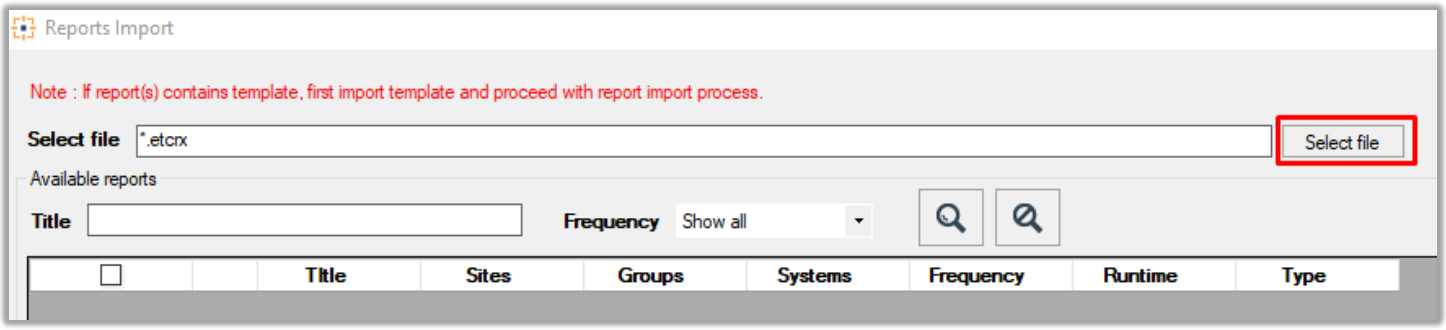

Figure 28

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

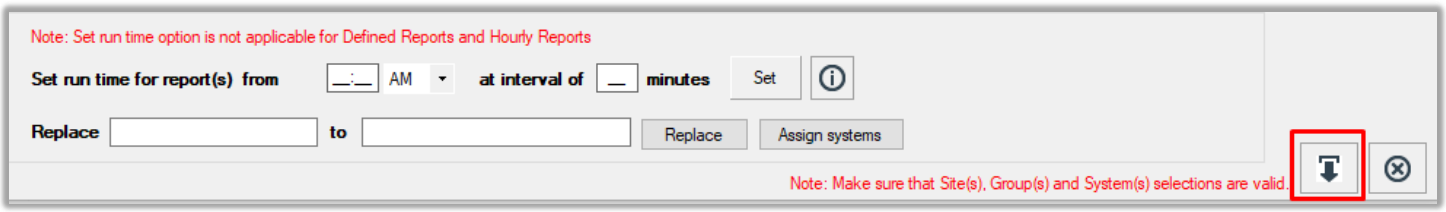

Figure 29

EventTracker displays a success message:

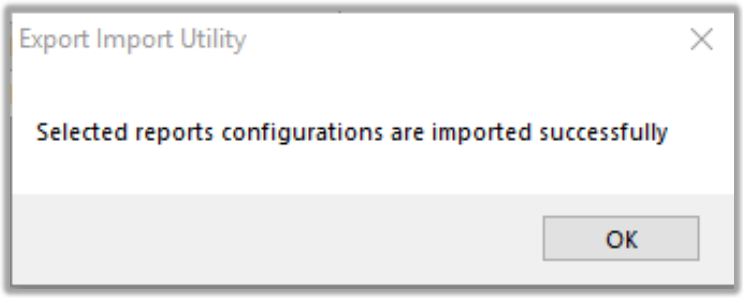

Figure 30

5.5 Knowledge Objects

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

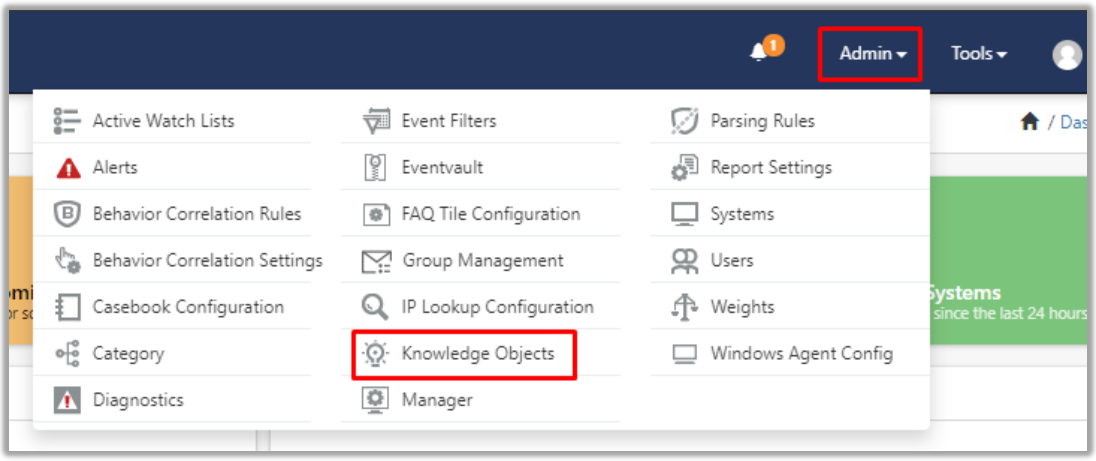

Figure 31

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

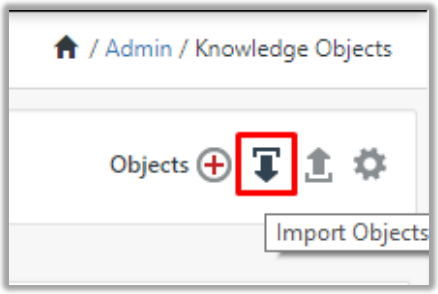

Figure 32

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

Figure 33

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 2

5.6 Dashboards

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

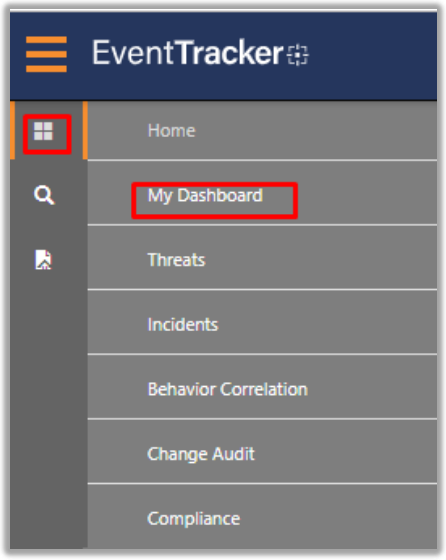

Figure 35

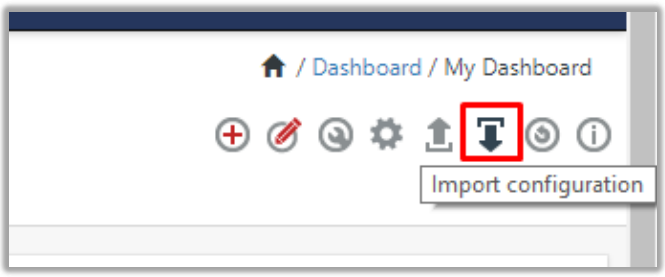

Figure 36

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_FortiManager.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.

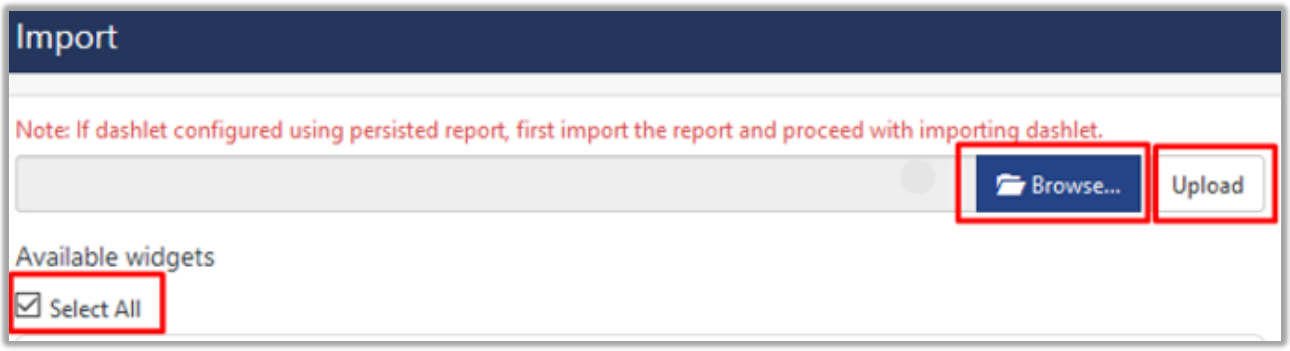

Figure 37

Figure 38

6.Verifying knowledge pack in EventTracker

6.1 Categories

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

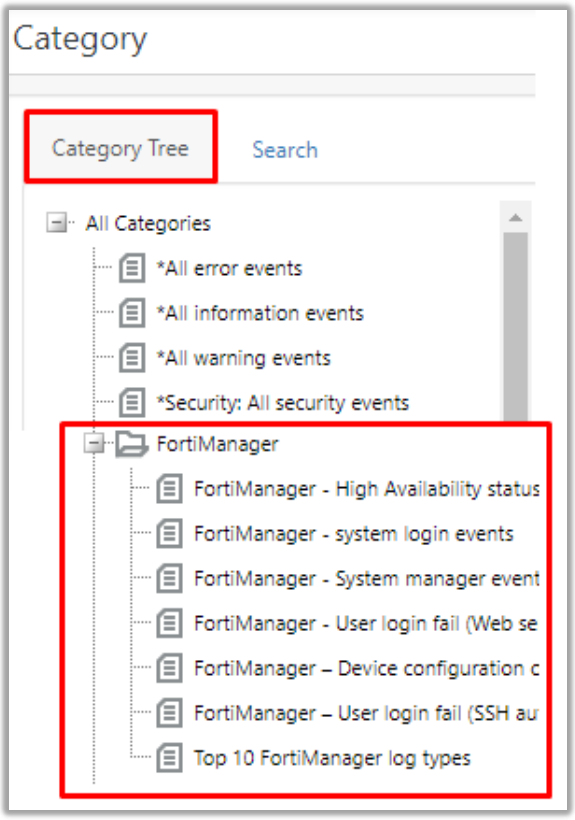

Figure 39

6.2 Alerts

1. In the **EventTracker manager** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In the search box enter **"FortiManager"** and then click the **Search** button.

EventTracker displays an alert related to FortiManager**:**

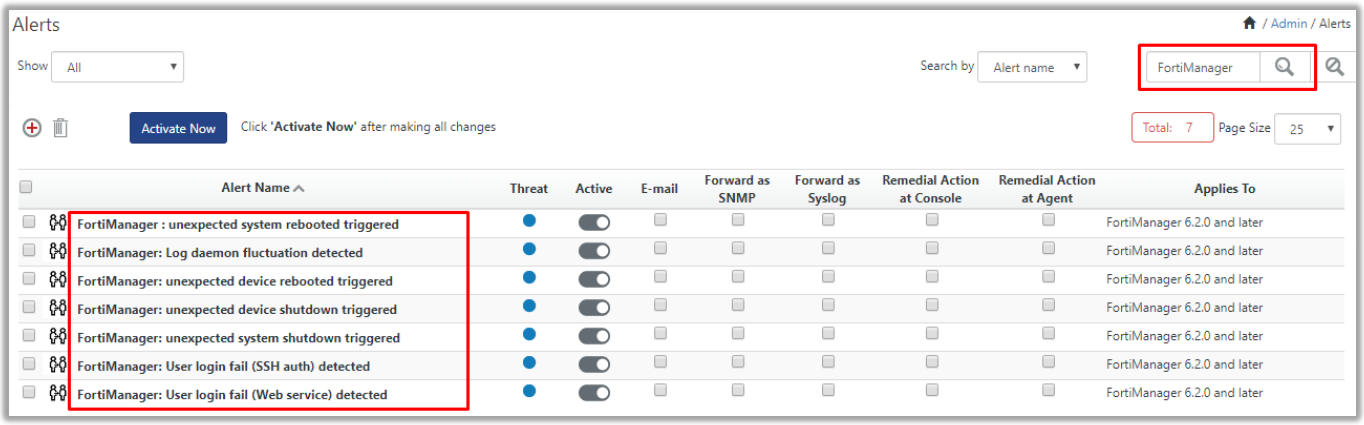

Figure 40

6.3 Token Templates

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

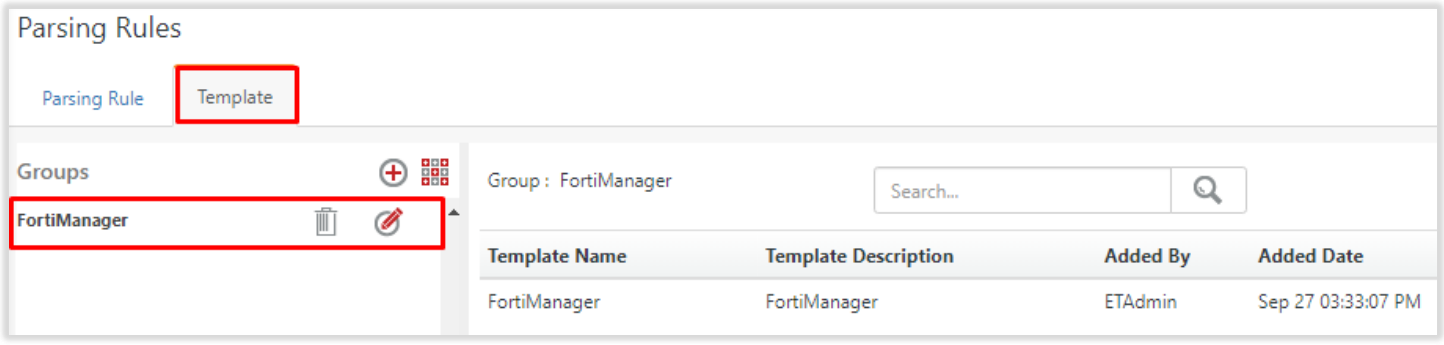

Figure 51

6.4 Flex Reports

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

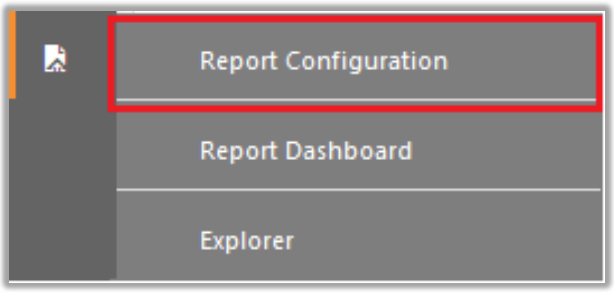

Figure 62

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

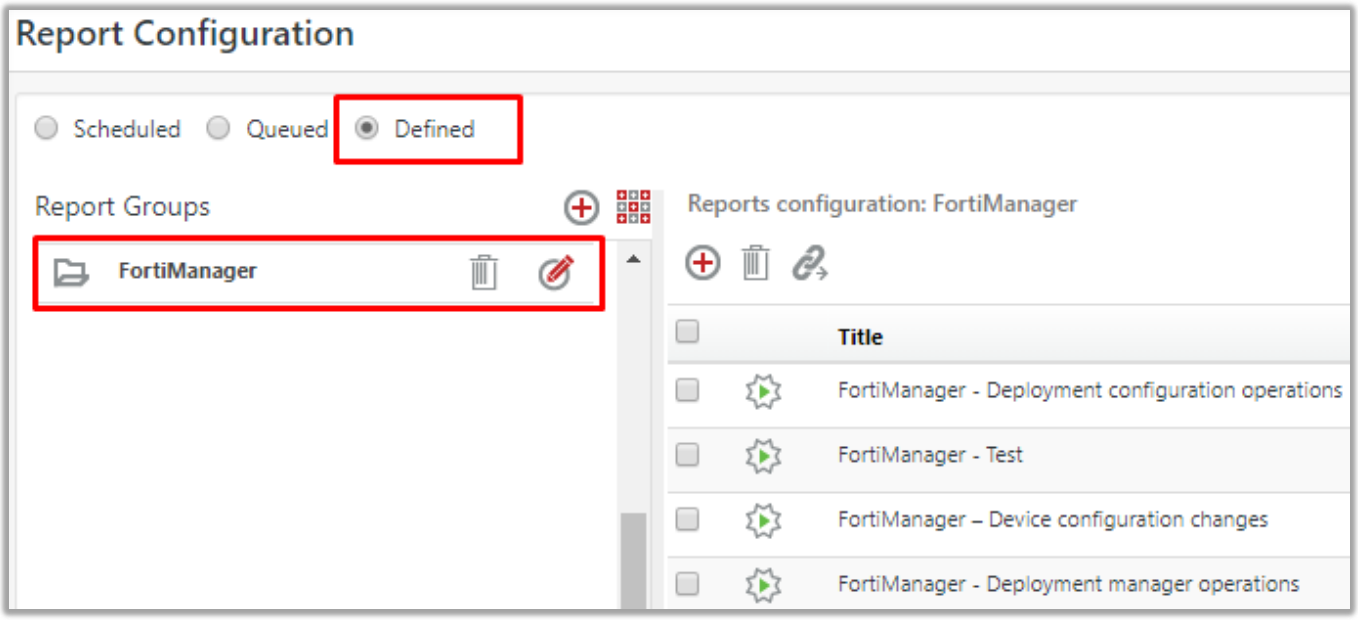

Figure 73

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 **"FortiManager"** group folder to view the imported Knowledge objects.

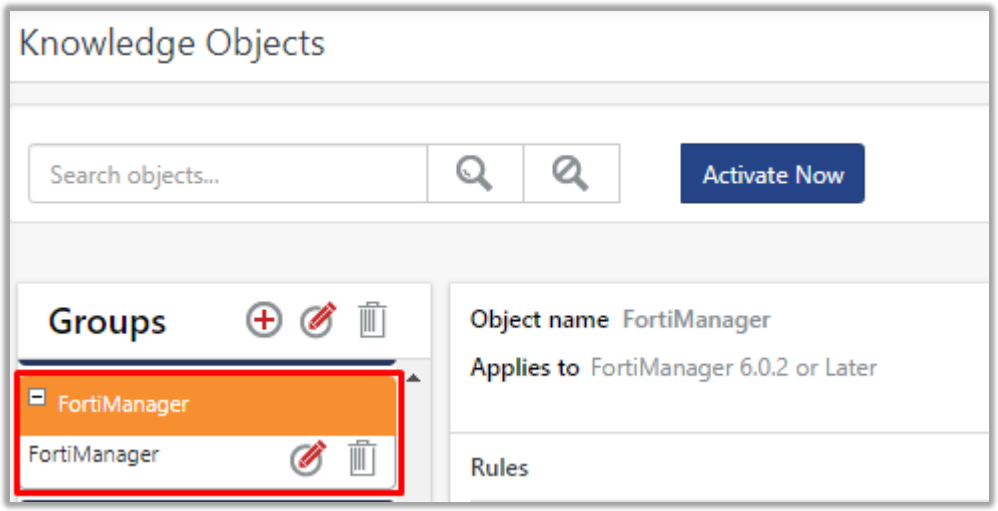

Figure 84

6.6 Dashboards

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

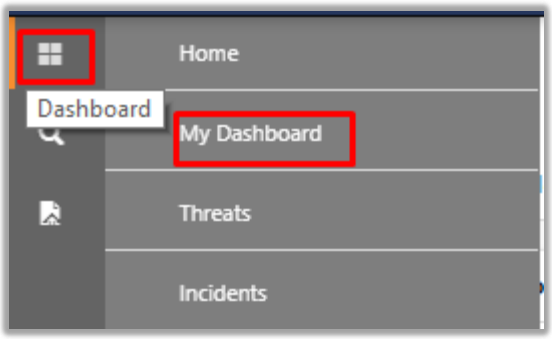

Figure 95

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

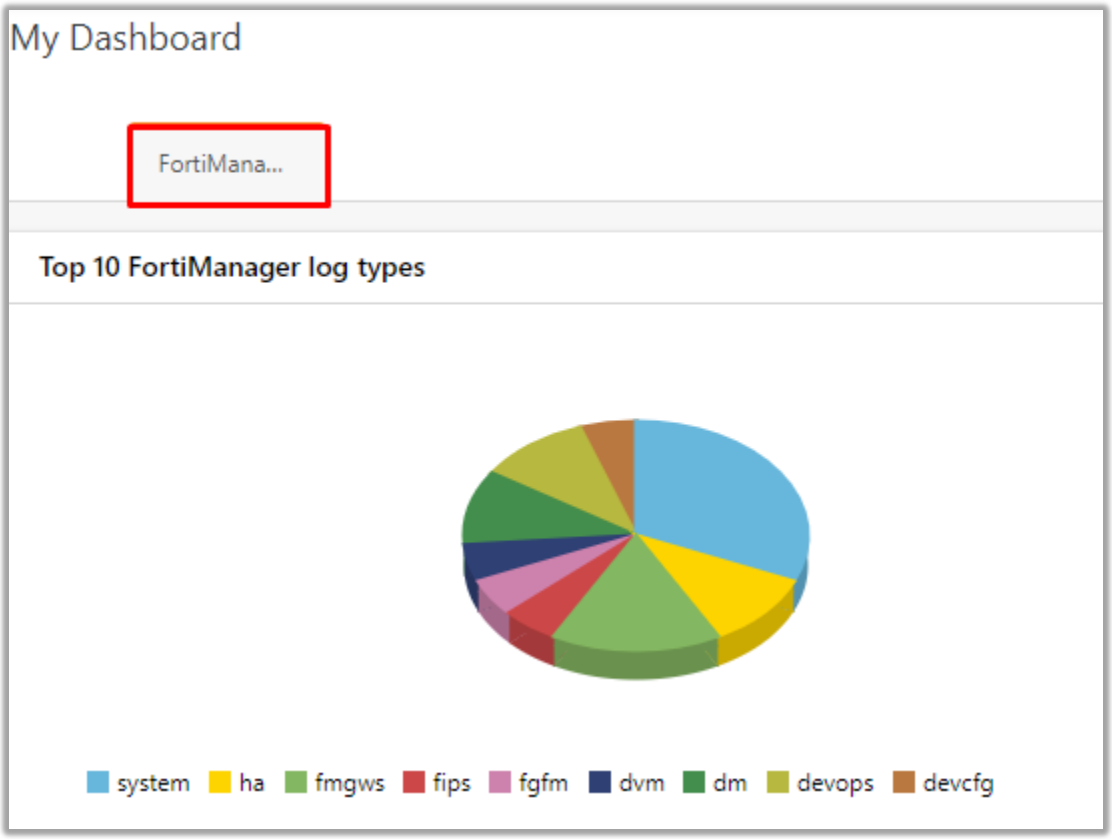

Figure 106