Netsurion™ | EventTracker

Integrate FortiAuthenticator with EventTracker

EventTracker v8.x and above

Publication Date: October 9, 2019

Abstract

This document guides the users to integrate FortiAuthenticator with EventTracker to monitor the activities on the FortiAuthenticator such as Channel events, File uploads, User events etc.

Scope

The configurations detailed in this guide are consistent with EventTracker version 8.x and later, and FortiAuthenticator v6.0.0 and above.

Audience

FortiAuthenticator users, who wish to forward logs to EventTracker Manager and monitor events using Event Tracker.

Table of Contents

1.Overview

The FortiAuthenticator device is an identity and access management solution. Identity and access management solutions are an important part of an enterprise network, providing access to protected network assets and tracking user activities to comply with security policies.

EventTracker, when integrated with FortiAuthenticator, enables users to view critical information's related to user logon activities performed in FortiAuthenticator or other Fortinet devices. These information's are represented in the form of report, alert and graphical/ pictorial representation(dashboard).

2.Integrating FortiAuthenticator

FortiAuthenticator logs we can get by using syslog.

1. To add a syslog server
   a. Go to **Logging > Log Config > Syslog Servers**.
   b. From the syslog servers list, select Create New.
   c. Enter the following information.
      - **Name**: Enter a name for the syslog server on FortiAuthenticator.
      - **Server Name/IP**: Enter **EventTracker IP** address.
      - **Port**: Enter the syslog server port number **514**.
      - **Level**: Select a log level as **information** from the dropdown menu.
      - **Facility**: Select a facility from the dropdown menu.

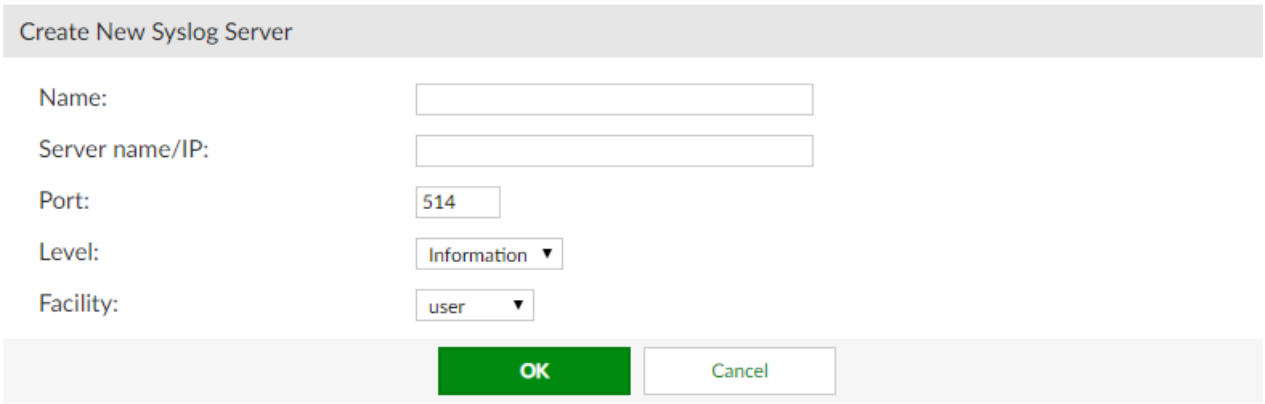

Figure 1

   - Select **OK** to add the syslog server.

2. To configure logging to a remote syslog server
   a. Go to Logging > Log Config > Log Settings.
   b. Under **Remote Syslog**, select **Send logs to remote Syslog servers**.

c. Move the syslog servers to which the logs will be sent from the **Available syslog servers'** box to the **Chosen syslog servers'** box.

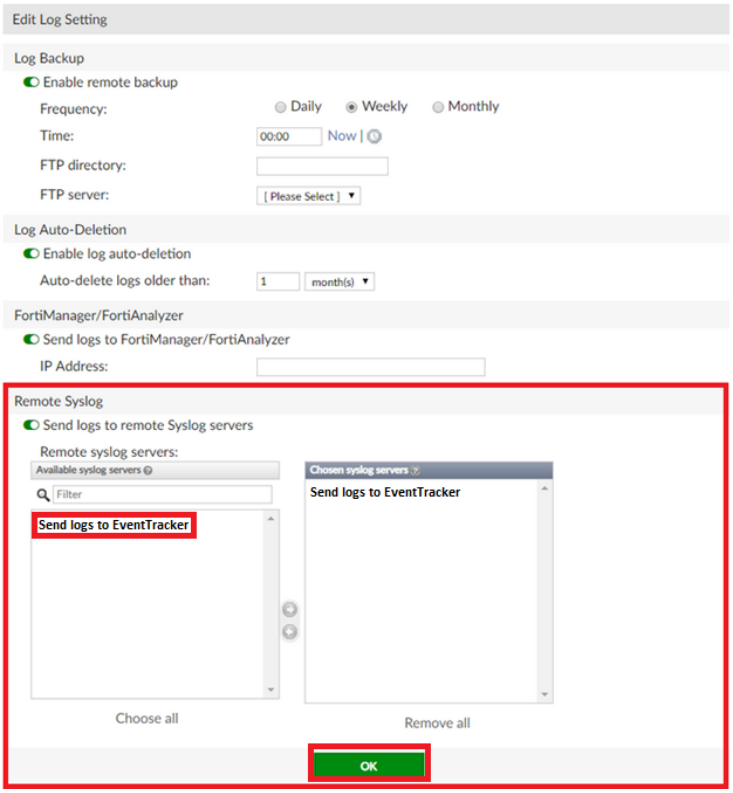

Figure 2

3. Select **OK** to save your settings.

3.EventTracker Knowledge Pack

3.1 Saved Search

- **FortiAuthenticator – Login Failed:** This saved search gives you information about the login failure that occurred.
- **FortiAuthenticator - Login Success:** This saved search gives you information about the successful login events that occurred.

3.2 Reports

- **FortiAuthenticator – Login Failed:** This report gives you information about the login failure that occurred and gives information the username that tried to login, Source IP Address and the reason for failure.

- **FortiAuthenticator - Login Success:** This report gives you information about the successful login events that occurred and gives you information about the user that logged in and source IP address from where the login occurred.

3.3 Alerts

- **FortiAuthenticator – Login Failed:** This alert is generated when the login failure occurs.

3.4 Dashboards

- **FortiAuthenticator – Login Failed**

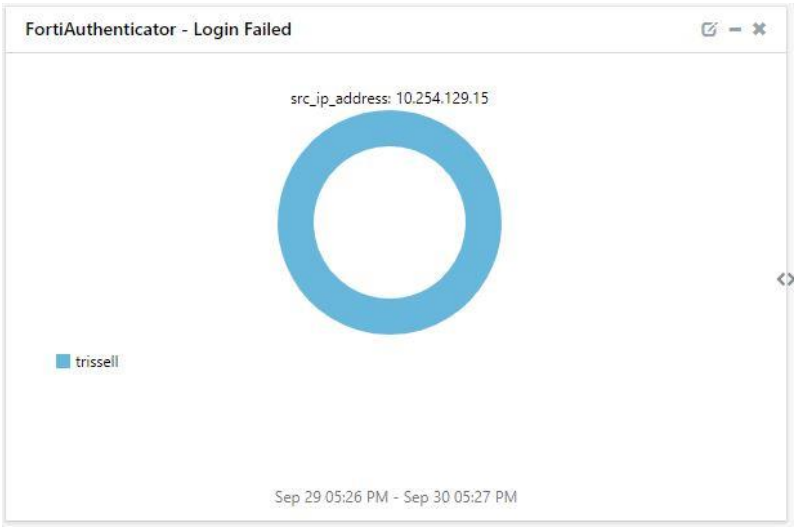

Figure 3

- **FortiAuthenticator – Login Success**

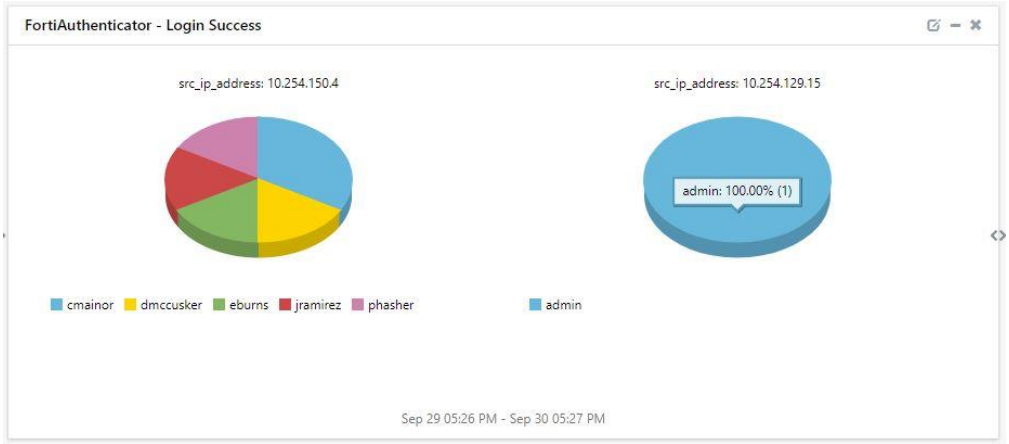

Figure 4

- **FortiAuthenticator – Login Failed Reasons**

Figure 5

4. Importing FortiAuthenticator knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Templates
- Knowledge Objects
- Flex Reports
- Dashboards

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

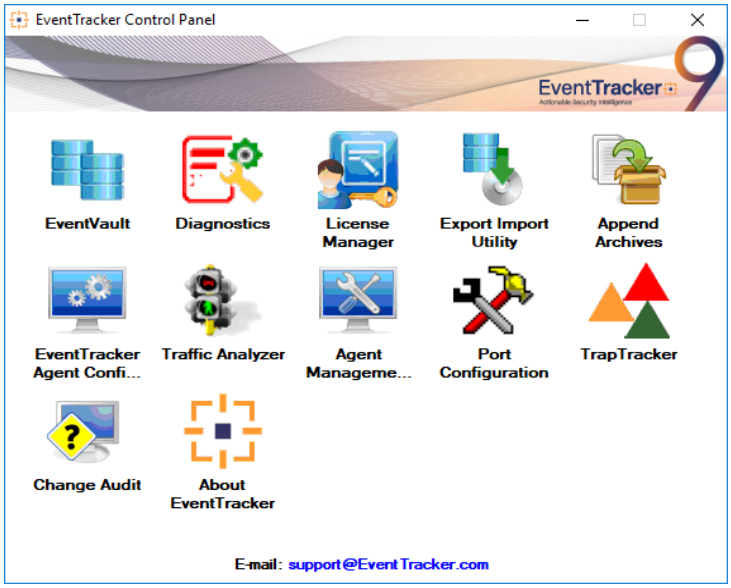

Figure 6

3. Click the **Import** tab**.**

4.1 Alerts

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

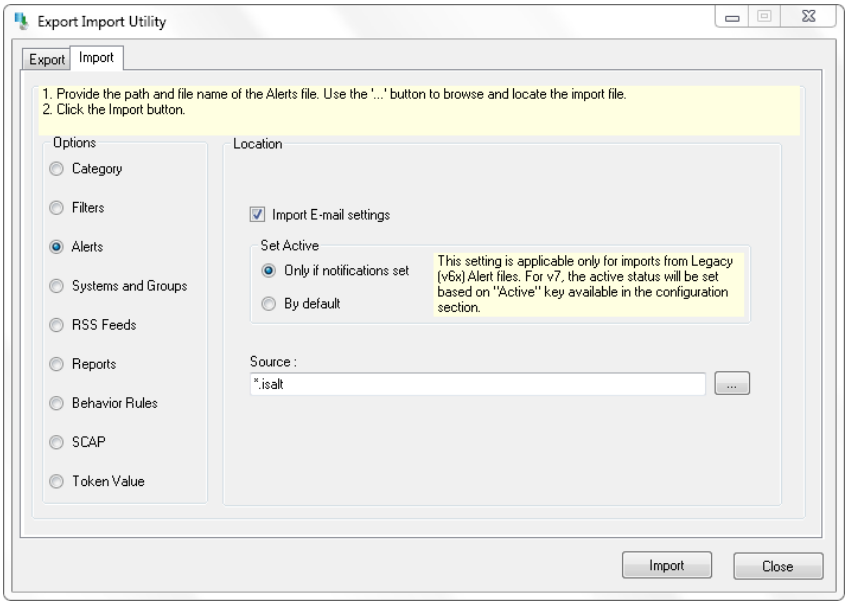

Figure 7

2. Locate **Alerts_FortiAuthenticator.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
4. EventTracker displays success message.

Figure 8

5. Click the OK button, and then click the Close button.

4.2 Category

1. Click **Category** option, and then click the browse  button.

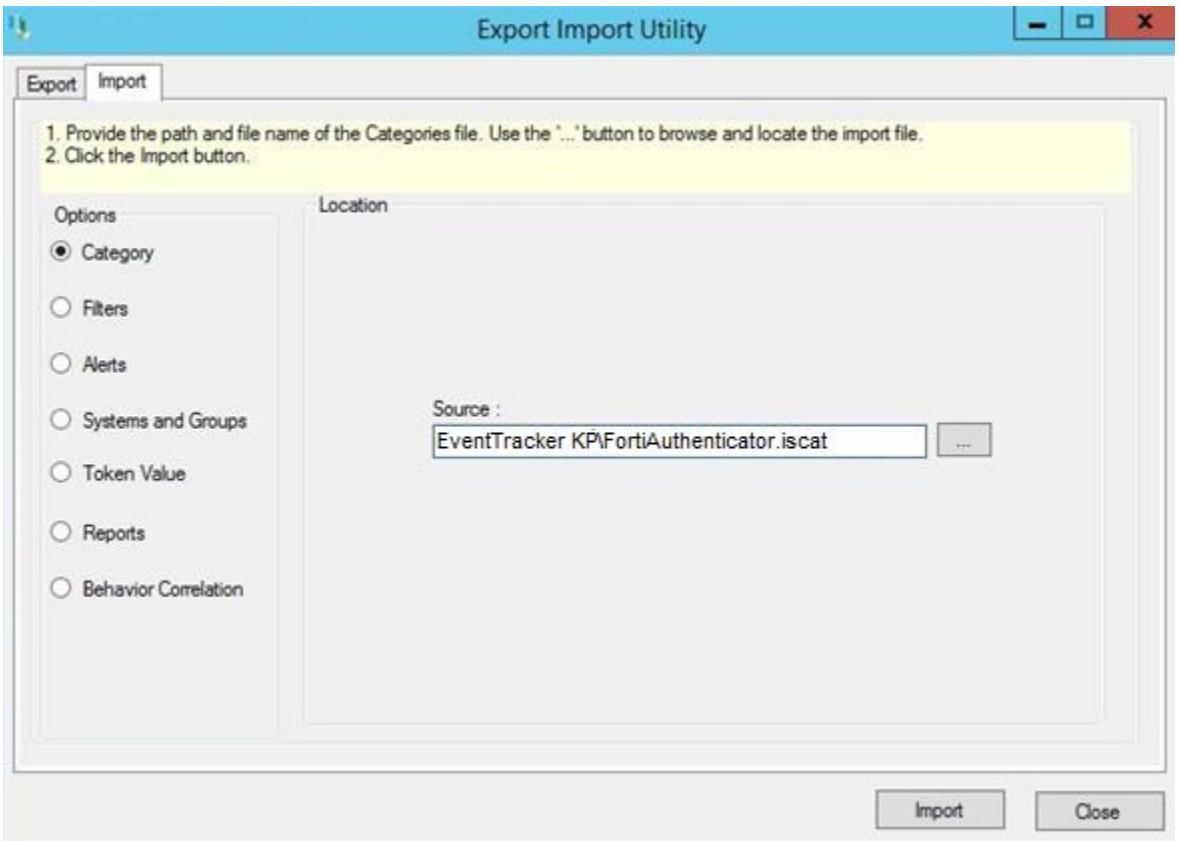

Figure 9

2. Locate **Category_FortiAuthenticator.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

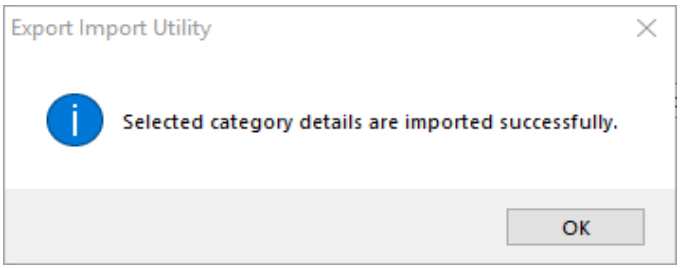

Figure 10

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

4.3 Knowledge object

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **KO_FortiAuthenticator.etko** file.

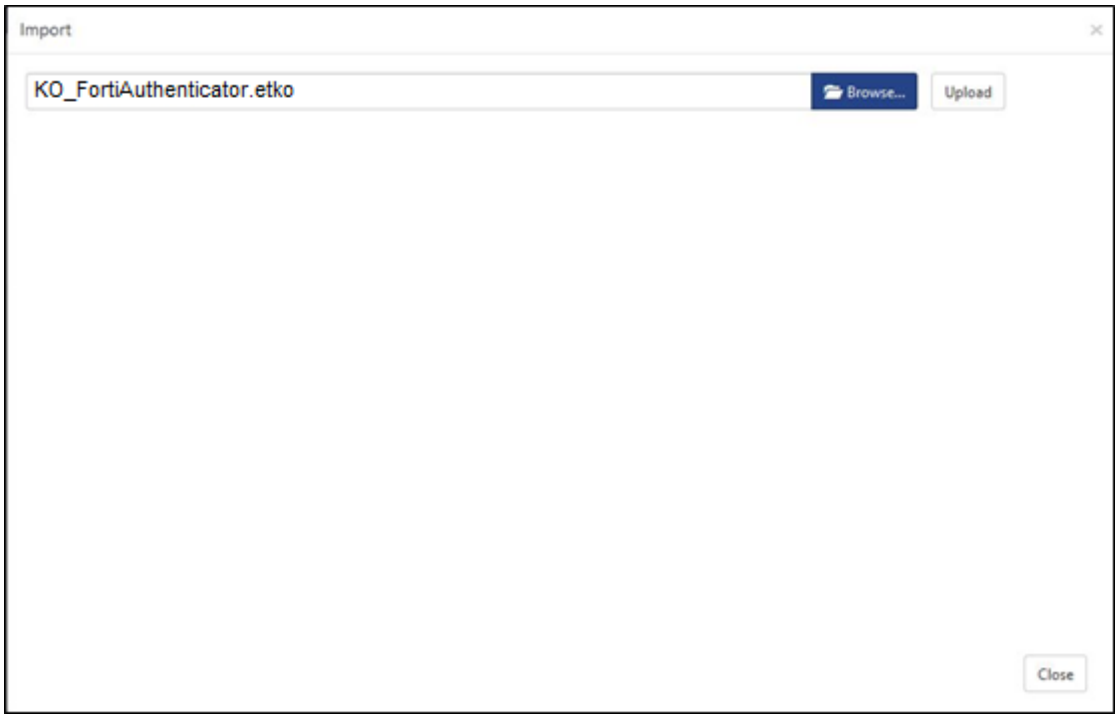

Figure 11

3. Click the '**Upload'** option.
4. Now select all the check box and then click on '**Import**' option.
5. Knowledge objects are now imported successfully.

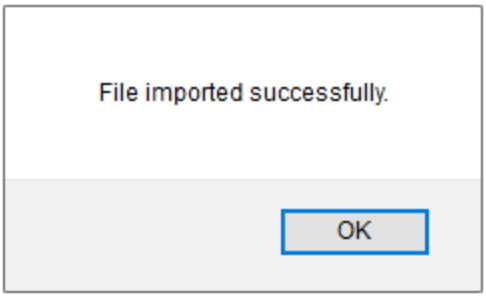

Figure 12

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

4.4 Flex Reports

On EventTracker Control Panel,

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

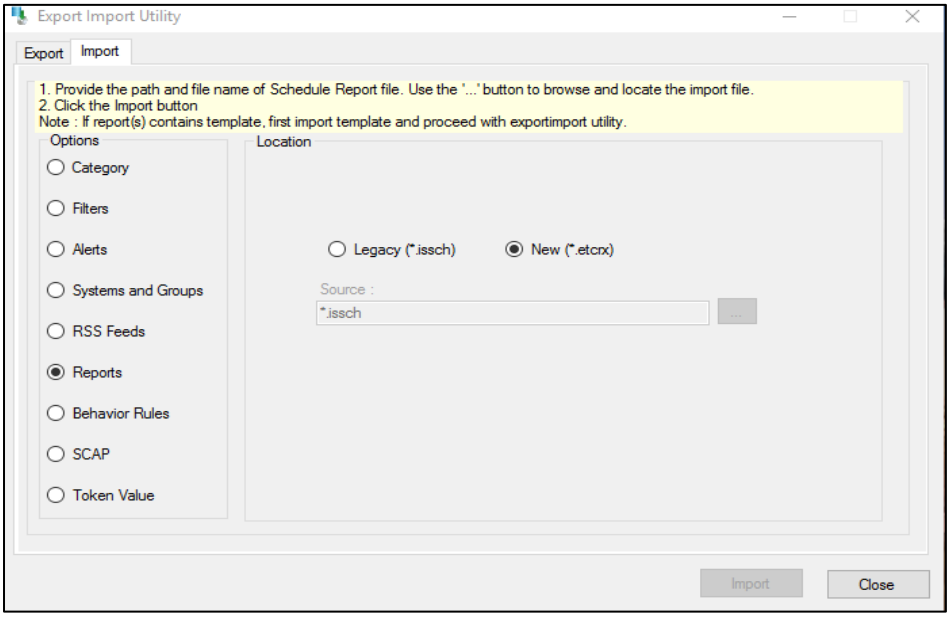

Figure 13

2. Locate the **Reports_FortiAuthenticator.etcrx** file and select all the check box.

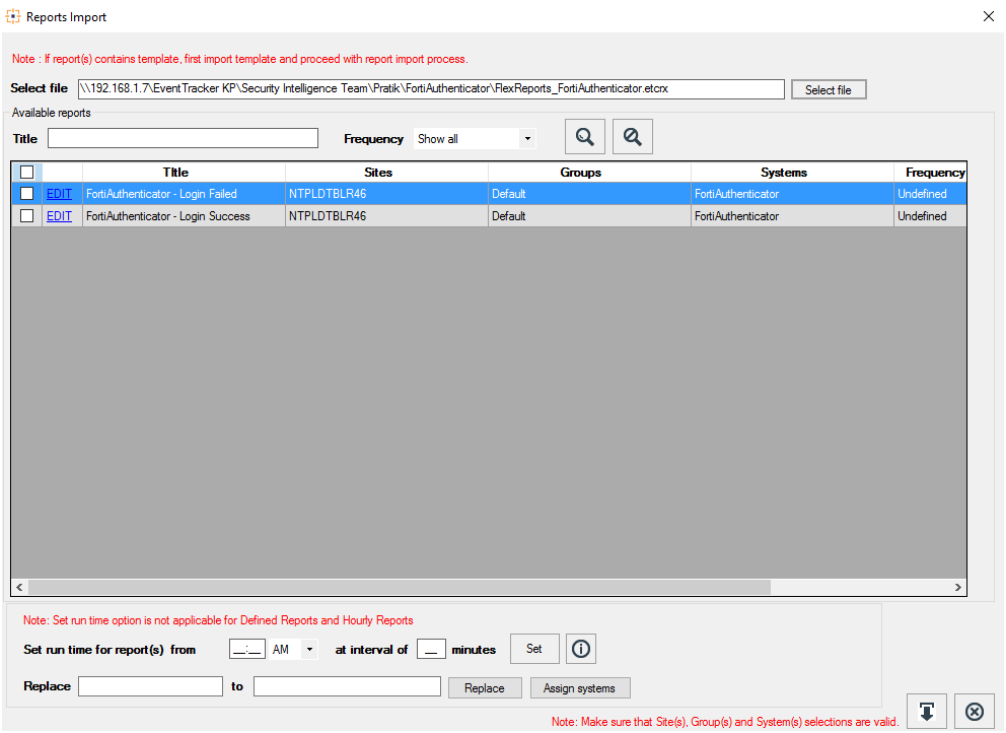

Figure 14

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

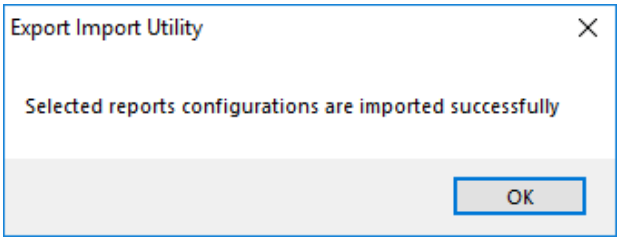

Figure 15

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

5. Verifying FortiAuthenticator Knowledge Pack in EventTracker

5.1 Categories

1. Logon to **EventTracker**.

2. Click **Admin** dropdown, and then click **Categories**.

3. In **Category Tree** to view imported categories, scroll down and expand **FortiAuthenticator** group folder to view the imported categories.

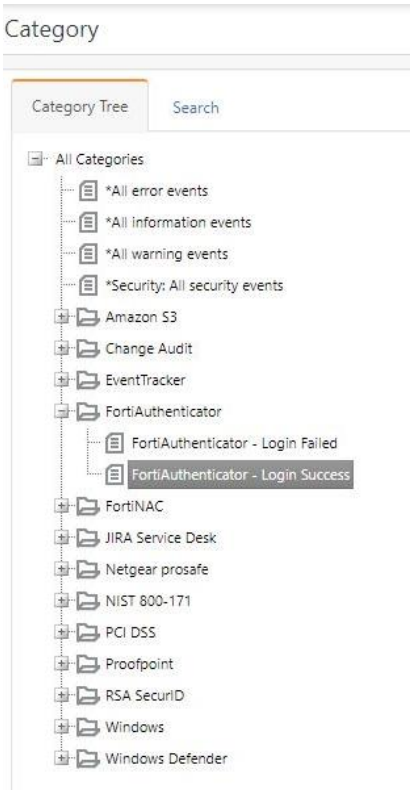

Figure 16

5.2 Knowledge Objects

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

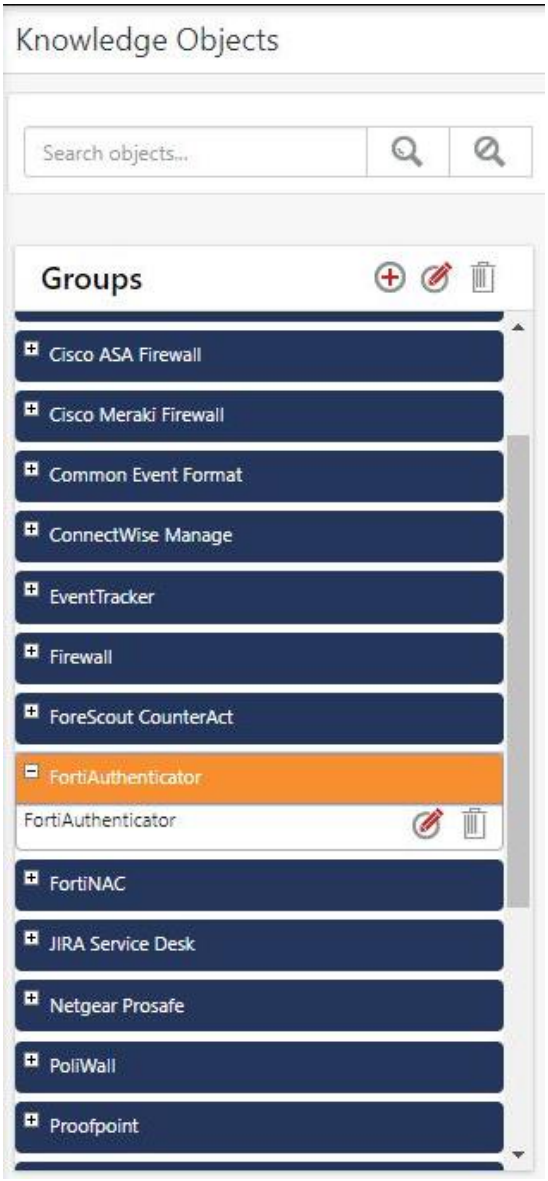

Figure 17

5.3 Alerts

1. Logon to EventTracker.
2. Click Admin dropdown, and then click Alerts.
3. In Alerts Tree to view imported Alerts, search **FortiAuthenticator** to view the imported Alerts.

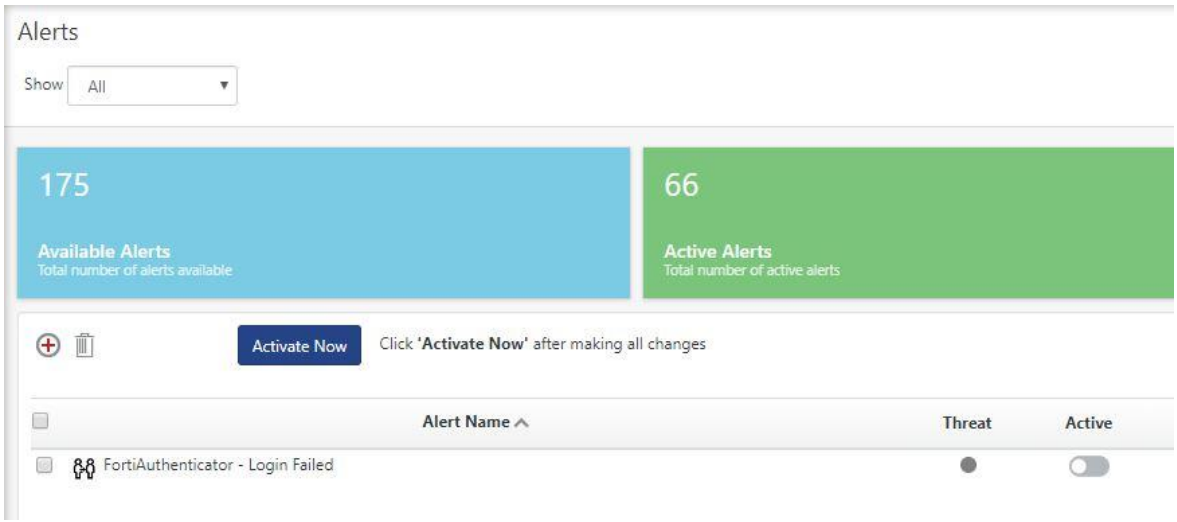

Figure 18

5.4 Flex Reports

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

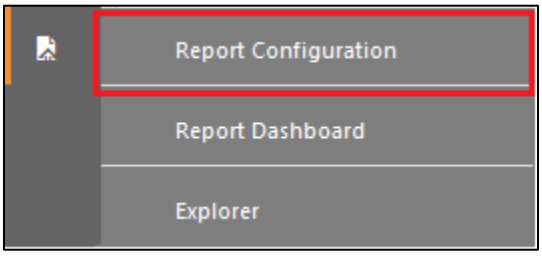

Figure 19

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

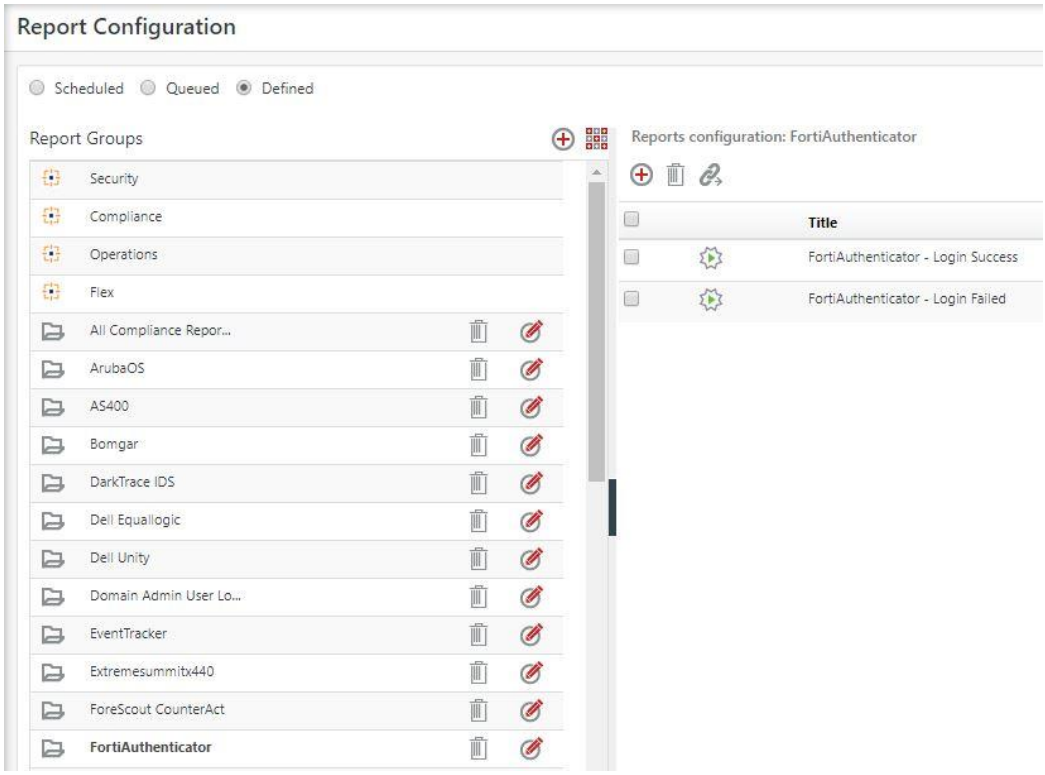

Figure 20

5.5 Dashboard

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
   - In "**FortiAuthenticator**" dashboard you should be now able to see something like this.

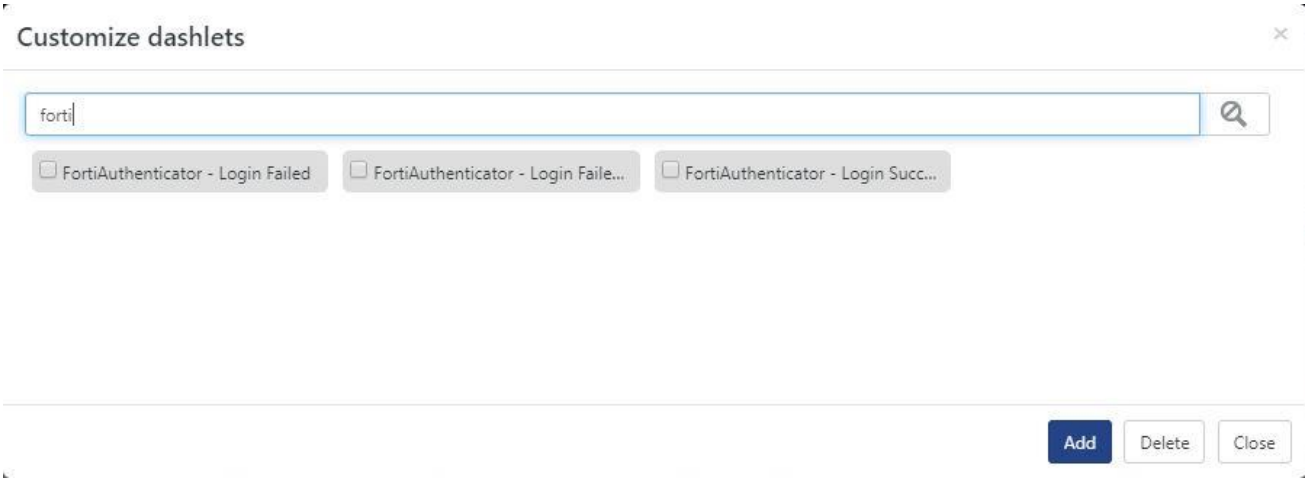

Figure 21