

Integrate Accellion SFT

EventTracker v9.x and above

Abstract

This guide provides instructions to configure Accellion SFT to send its log to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and **Accellion SFT**

Audience

Administrators who are assigned the task to monitor Accellion SFT events 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview.....	3
2. Prerequisites.....	3
3. Integrating Accellion SFT with EventTracker.....	3
3.1 Integration can be performed via syslog configuration	3
4. EventTracker Knowledge Pack	5
4.1 Category.....	5
4.2 Alert	5
4.3 Report	5
4.4 Dashboards	8
5. Importing Accellion SFT knowledge pack into EventTracker	12
5.1 Category.....	13
5.2 Alert	14
5.3 Token template.....	15
5.4 Knowledge Object.....	16
5.5 Report	18
5.6 Dashboards	19
6. Verifying Accellion SFT knowledge pack in EventTracker	22
6.1 Category.....	22
6.2 Alert	23
6.3 Token templates	24
6.4 Knowledge Object.....	24
6.5 Report	25
6.6 Dashboards	26

1. Overview

Accellion SFT (kiteworks) provides enterprise users, a powerful and secure access to the content. With an integrated environment, users can work seamlessly on different platforms ranging from desktop, tablet to smartphone—an environment where employees are always connected.

EventTracker helps to monitor events from **Accellion SFT**. Its dashboard, alerts and reports will help you to track login activities, login failure, file and folder activities and configuration changes to keep you informed about the systems and its activities. It will trigger alert whenever any login fails, and if any file/folders are deleted.

2. Prerequisites

- Admin privileges for **Accellion SFT** and should be installed.
- **EventTracker agent** should be installed in the system.

3. Integrating Accellion SFT with EventTracker

3.1 Integration can be performed via syslog configuration

Follow the below steps to configure syslog.

1. Login to your Accellion Kiteworks Web UI with an admin account. (<https://<hostname>/admin>)
2. Navigate to System > Locations > Syslog Settings.

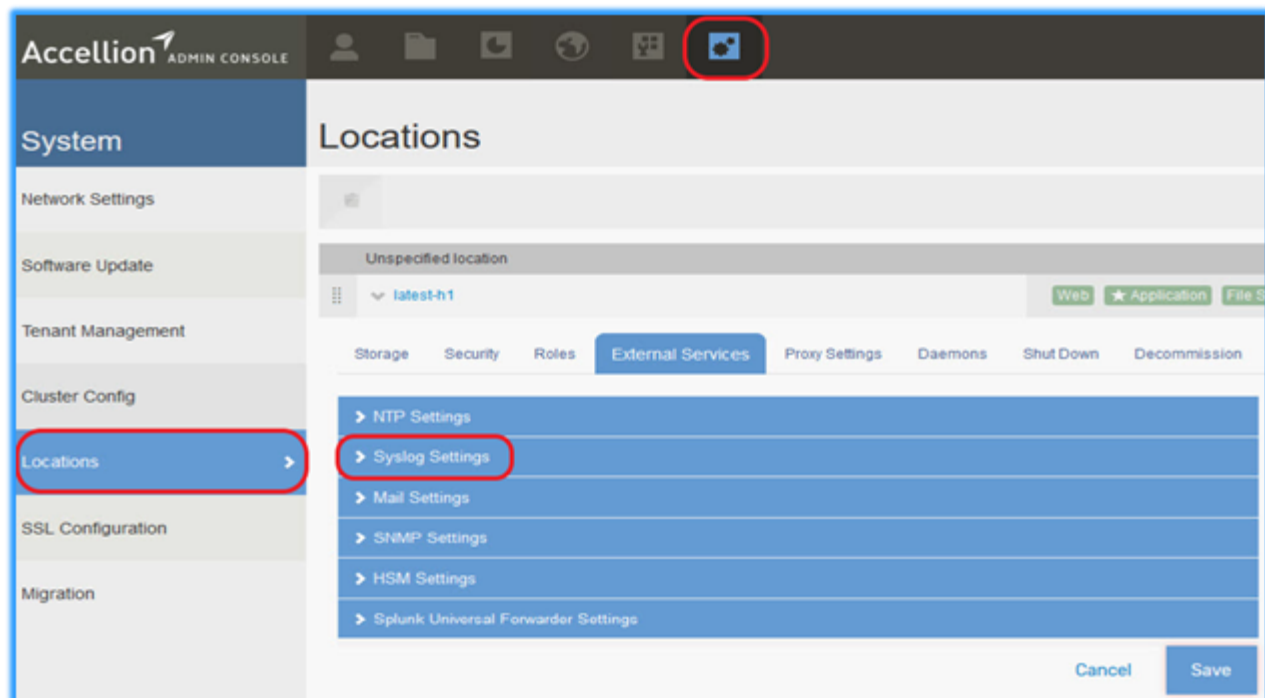


Figure 1

3. Enter the host name or IP Address of the EventTracker Manager.
4. Select the Protocol and Port. (Protocol – UDP & Port - 514)
5. In Format option, choose “Single line with comma separated”.

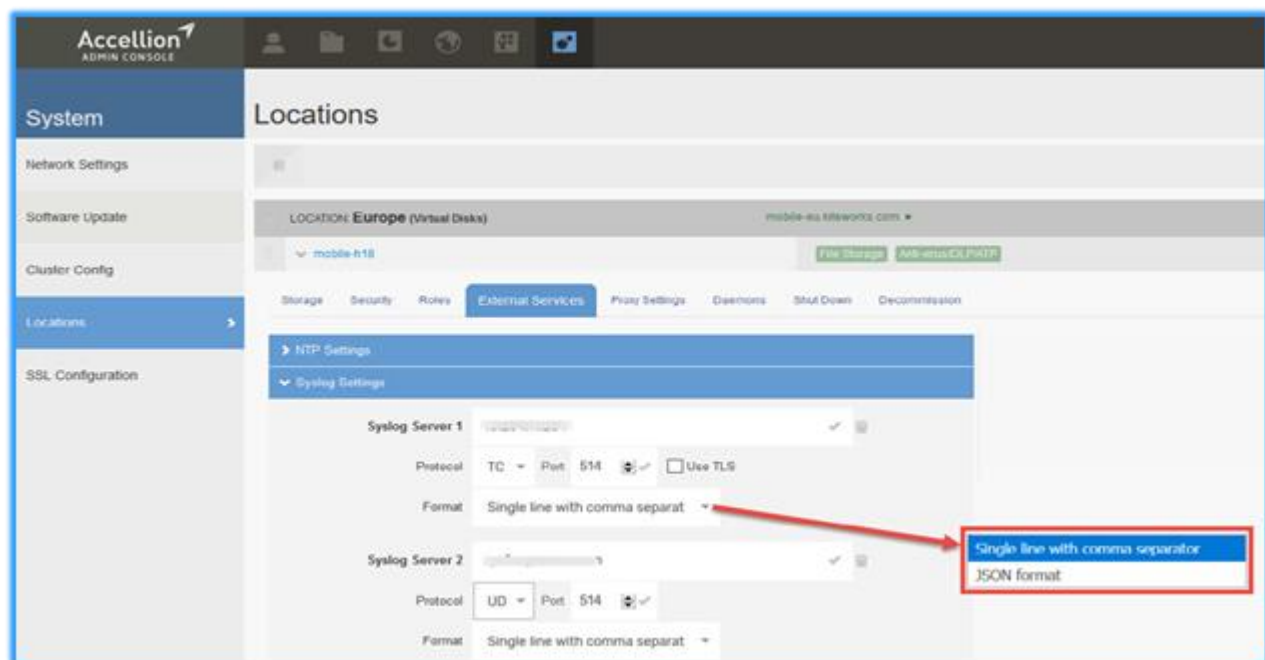


Figure 2

6. Check the Apply the same “Syslog Settings” to all hosts option to apply these settings to the entire cluster before saving.

4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Accellion SFT.

4.1 Category

- **Accellion SFT login failed** - This category provides information related to login failure detected in Accellion SFT.
- **Accellion SFT Login and logout activity** – This category provides information related to all the login and logout activity performed in Accellion SFT.
- **Accellion SFT File management** – This category provides information related to all the file related activity.
- **Accellion SFT Folder management** – This category provides information related to all the folder related activity.
- **Accellion SFT User management** – This category provides information related to all the user management activity.
- **Accellion SFT File/Folder deleted** - This category provides information related to all file/folder delete activity.
- **Accellion SFT DLP flagged/locked a file** - This category provides information related to all DLP flagged/locked file.

4.2 Alert

- **Accellion SFT: Login failed** - This alert is generated when any login failure is detected in Accellion SFT.
- **Accellion SFT: File/Folder deleted** – This alert is generated when any file/folder is deleted.
- **Accellion SFT: DLP flagged/locked a file** – This alert is generated when any file/folder is flagged by DLP or locked.

4.3 Report

- **Accellion SFT – Folder Management**- This report gives information about all the actions performed on folders. Report contains username, source IP, activity type like add, delete, recover, update. Etc. and activity details which can be useful for further analysis.

Activity Type	LogTime	EventId	Computer	EventSource	EventDescription	Activity	ID	Server IP	Username
add_folder	04/24/2020 04:28:43 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 24 16:28:43 172.27.100.13 Apr 14 13:54:28 ec2-34-192-249-174 Apr 14 17:54:28 westonsolutions-h1	My Folder: Created folder FAA WWaves EA	4705 (external)	162.xxx.xxx	will@contoso
add_folder	04/24/2020 04:28:45 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	rest_server nv: brent.ferrv@westonsolutions.com Apr 24 16:28:45 172.27.100.13 Apr 13 15:59:30 ec2-34-192-249-174 Apr 13 19:59:30 westonsolutions-h1	Pitchford Files: Created folder Videos 4-13-20	2613 (internal)	138.xxx.xxx	mark@contoso
add_folder	04/24/2020 04:33:17 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	rest_server nv: mark@westonsolutions.com Apr 24 16:33:17 172.27.100.13 Apr 14 13:54:28 ec2-34-192-249-174 Apr 14 17:54:28 westonsolutions-h1	My Folder: Created folder FAA WWaves EA	4705 (external)	162.xxx.xxx	John@contoso

Figure 3

- **Accellion SFT – File Management** - This report gives information about all the actions performed on files. Report contains username, source IP, activity type like add, modify, delete, recover, quarantine, lock, etc., activity details and other useful information.

LogTime	EventId	Computer	EventSource	Activity	Type	ID	Server IP	Username	File ID	File Size
04/24/2020 04:33:20 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	/: Uploaded file E-WESTON_Voucher 04-L616-613.pdf	add_file	463 (external)	162.xxx.xxx	Mike@contoso	143638	317552261
04/24/2020 04:33:20 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	SVFUDS Deliverables/3706 Fordham Dynamic MPV: Uploaded file Spring_Valley_MOOs_W3.xlsx	add_file	1250 (external)	162.xxx.xxx	Will@contoso	143631	2215080
04/25/2020 02:31:23 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	/: Uploaded file 20200413 GOR 3 Week Look Ahead.xlsx	add_file	382 (external)	162.xxx.xxx	John@contoso	143802	594006

Figure 4

- **Accellion SFT – User Management** – This report gives information about all the user management activities like add user, reactivate user, delete user, user type change, etc. Report contains username, source IP, activity type and activity details along with other useful information.

LogTime	EventId	Computer	EventSource	EventDescription	Activity	Activity Type	ID	Server IP	Username
04/25/2020 02:31:23 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 25 14:31:23 172.27.100.13 Apr 14 14:02:13 ec2-34-192-249-174 Apr 14 18:02:13 westonsolutions-h1	Registered as a new restricted User	add_user	4706 (internal)	162.xxx.xxx	Mike@gmail.com
04/25/2020 02:31:24 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	rest_server nv: samantha.holmes@usarmy.mil Apr 25 14:31:24 172.27.100.13 Apr 14 13:53:49 ec2-34-192-249-174 Apr 14 17:53:49 westonsolutions-h1	Registered as a new restricted User	add_user	4702 (internal)	162.xxx.xxx	John@contoso.com
04/25/2020 02:31:24 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	rest_server nv: brent.ferrv@westonsolutions.com Apr 25 14:31:24 172.27.100.13 Apr 14 13:17:51 ec2-34-192-249-174 Apr 14 17:14:18 westonsolutions-h1	User account unlocked by lockout cooldown	user_login_unlock	1250 (external)	127.xxx.xxx	Mark@contoso.com

Figure 5

- **Accellion SFT – Password Management** – This report gives information about all the password related activities such as password update, reset, etc. Report contains username, source IP, activity type and details along with other useful information.

LogTime	EventId	Computer	EventSource	EventDescription	Activity	Activity Type	ID	Server IP	Username
04/24/2020 04:28:44 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 24 16:28:44 172.27.100.13 Apr 13 20:17:01 ec2-34-192-249-174 Apr 13 21:19:11 westonsolutions-h1	Updated their password	update_password	4149 (internal)	140.xxx.xxx	mike@contoso
04/24/2020 04:28:45 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	rest_server nv: laura.linkeu.finn@usarmy.mil Apr 24 16:28:45 172.27.100.13 Apr 13 15:37:41 ec2-34-192-249-174 Apr 13 19:37:41 westonsolutions-h1	Verification code link sent	add_short_link	4682 (internal)	98.xxx.xxx	John@contoso
04/24/2020 04:28:45 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	rest_server nv: brent.ferrv@westonsolutions.com Apr 24 16:28:45 172.27.100.13 Apr 13 15:59:49 ec2-34-192-249-174 Apr 13 19:59:49 westonsolutions-h1	Updated their password	update_password	4682 (internal)	98.xxx.xxx	Will@Contoso

Figure 6

- **Accellion SFT – User Login Failed** – This report gives information related to all the login failure detected in Accellion SFT. Report contains username, source IP and activity details along with other information for further investigation.

LogTime	EventId	Computer	EventSource	EventDescription	Activity Type	ID	Server IP	Username
04/24/2020 04:28:43 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 24 16:28:43 172.27.100.13 Apr 14 13:30:03 ec2-user_login_failed 34-192-249-174 Apr 14 17:30:03 westonsolutions-	ec2-user_login_failed	4248 (internal)	24.xxx.xxx	john@contoso.com
04/24/2020 04:33:17 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 24 16:33:17 172.27.100.13 Apr 14 13:30:03 ec2-user_login_failed 34-192-249-174 Apr 14 17:30:03 westonsolutions-	ec2-user_login_failed	4248 (internal)	24.xxx.xxx	Mike@contoso.com
04/25/2020 05:57:18 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 25 17:57:18 172.27.100.13 Apr 13 15:42:20 ec2-tfa_login_failed 34-192-249-174 Apr 13 19:42:20 westonsolutions-	ec2-tfa_login_failed	4542 (internal)	24.xxx.xxx	Will@contoso.com

Figure 7

- **Accellion SFT – User Login and Logout** – This report gives information related to all the login and logout activity detected in Accellion SFT. Report contains username, source IP and activity details along with other information.

LogTime	EventId	Computer	EventSource	EventDescription	Activity	Activity Type	ID	Server IP	Username
04/24/2020 04:33:20 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 24 16:33:20 172.27.100.13 Apr 13 15:31:06 ec2-34-192-249-174 Apr 13 19:22:52 westonsolutions-h1 rest_server.py:	Logged out	user_logged_out	463 (external)	162.xxx.xxx	mike@contoso.com
04/25/2020 05:57:15 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 25 17:57:15 172.27.100.13 Apr 14 13:30:10 ec2-34-192-249-174 Apr 14 17:30:10 westonsolutions-h1 rest_server.py:	Logged in	user_logged_in	4248 (internal)	24.xxx.xxx	john@contoso.com
04/25/2020 04:53:36 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	Apr 25 16:53:36 172.27.100.13 Apr 14 13:30:10 ec2-34-192-249-174 Apr 14 17:30:10 westonsolutions-h1 rest_server.py:	Logged in	user_logged_in	4248 (internal)	24.xxx.xxx	will@contoso.com

Figure 8

- **Accellion SFT – Admin Activity** - This report gives information about all the admin activities performed such as system setting switched, add ldap source, application settings changed, edit client, etc. Report contains admin username, source IP, activity type and details and other useful information.

LogTime	EventId	Computer	EventSource	Activity	Activity Type	File ID	File Size	ID	Server IP	Username
04/24/2020 04:28:43 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	View file H-105.pdf from email. Subject: "H-105" To: c.hurt@westonsolutions.com	view_attachment	51fa3f2145b5416fa1539f274aa697ca	534910	1098 (external)	162.xxx.xxx	Will@contoso
04/24/2020 04:28:43 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	View file Seasicks 200945857 Letter Attachments.pdf from email. Subject: "Landowner Letter	view_attachment	8368a0c4999b46eda3411dbcc7db8e17	5061587	2176 (internal)	74.xxx.xxx	Mark@Contoso
04/24/2020 04:28:43 PM	128	172.xxx.xxx-SYSLOG	SYSLOG local0	View file Seasicks 200945857 Letter Attachments.pdf from email. Subject: "Landowner Letter	view_attachment	8368a0c4999b46eda3411dbcc7db8e17	5061587	2176 (internal)	74.xxx.xxx	John@Contoso

Figure 9

- **Logs Considered**

<code>action</code>	+ - Session started
<code>addl_info8</code>	+ - 463 (external)
<code>application_name</code>	+ - rest_server.py
<code>category</code>	+ - session_started
<code>event_category</code>	+ - 0
<code>event_computer</code>	+ - 172.27.100.13-syslog
<code>event_datetime</code>	+ - 4/25/2020 5:57:19 PM
<code>event_datetime_utc</code>	+ - 1587817639
<code>event_description</code>	Apr 25 17:57:19 172.27.100.13 Apr 13 15:31:02 ec2-34-192-24 =463 (external), 172.27.100.13, Activity Type: session_started,
<code>event_group_name</code>	+ - Default
<code>event_id</code>	+ - 128
<code>event_log_type</code>	+ - Application
<code>event_source</code>	+ - SYSLOG local0
<code>event_type</code>	+ - Error
<code>event_user_domain</code>	+ - N/A
<code>event_user_name</code>	+ - N/A
<code>group_name</code>	+ - admin
<code>log_source</code>	+ - Accellion
<code>source_type</code>	+ - Accellion
<code>src_host_name</code>	+ - westonsolutions-h1
<code>src_ip_address</code>	+ - 172.27.100.13
<code>src_ip_address_geoiip.city_name</code>	+ - West Chester
<code>src_ip_address_geoiip.continent_name</code>	+ - North America

Figure 10

4.4 Dashboards

- **Accellion SFT User Login Failed**

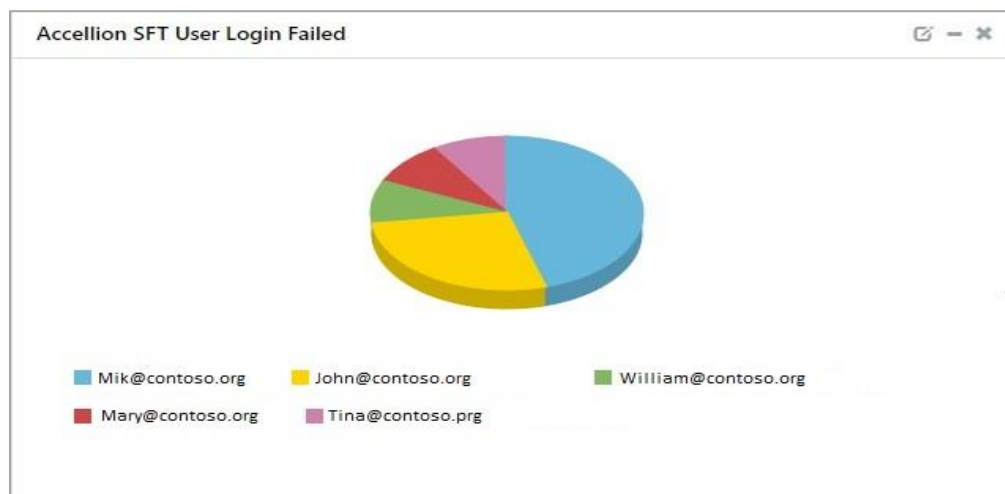


Figure 11

- Accellion SFT User Login and Logout

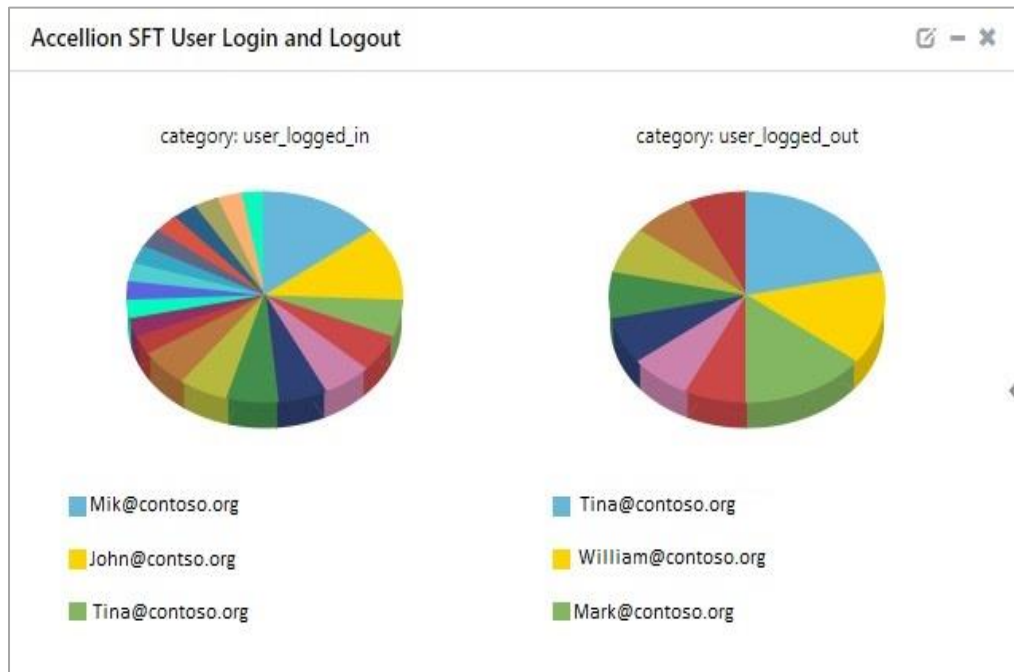


Figure 12

- Accellion SFT User Management

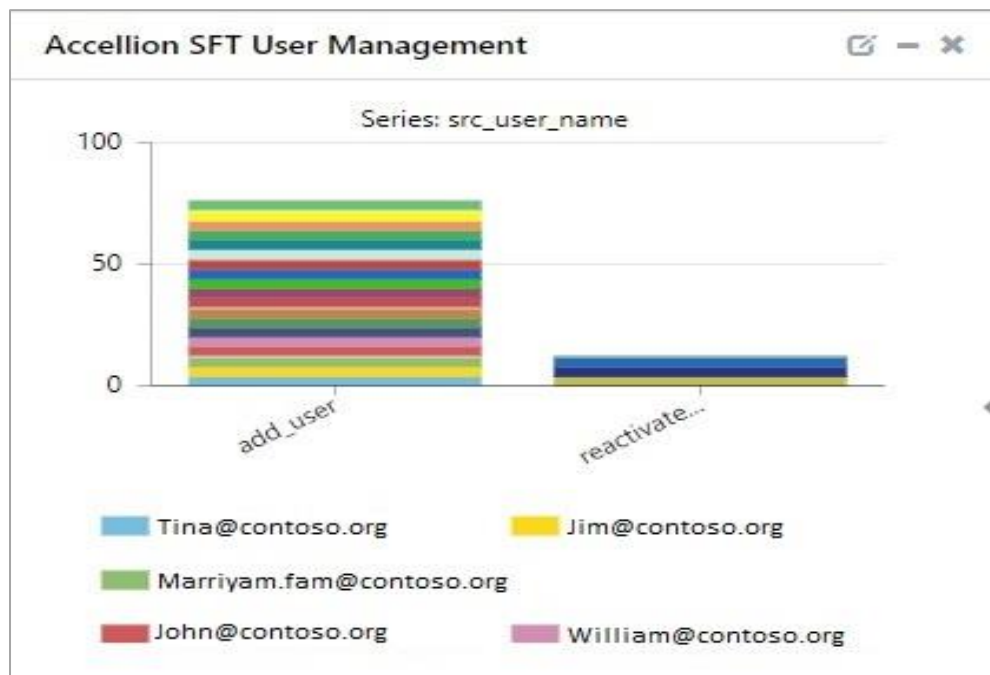


Figure 13

- Accellion File Management

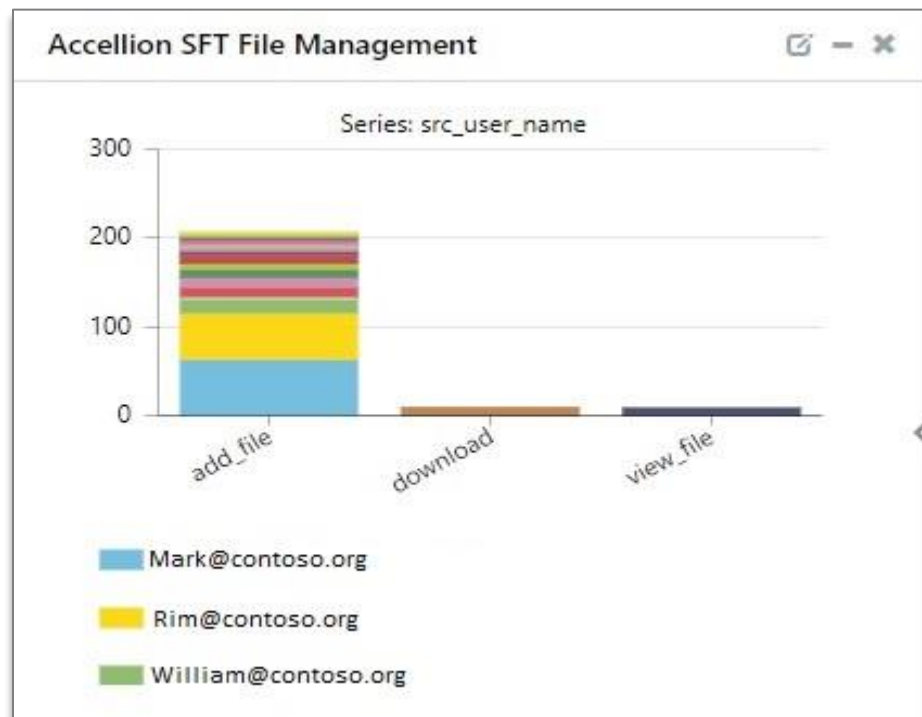


Figure 14

- Accellion SFT Folder Management



Figure 15

- Accellion SFT Activity Performed by Category

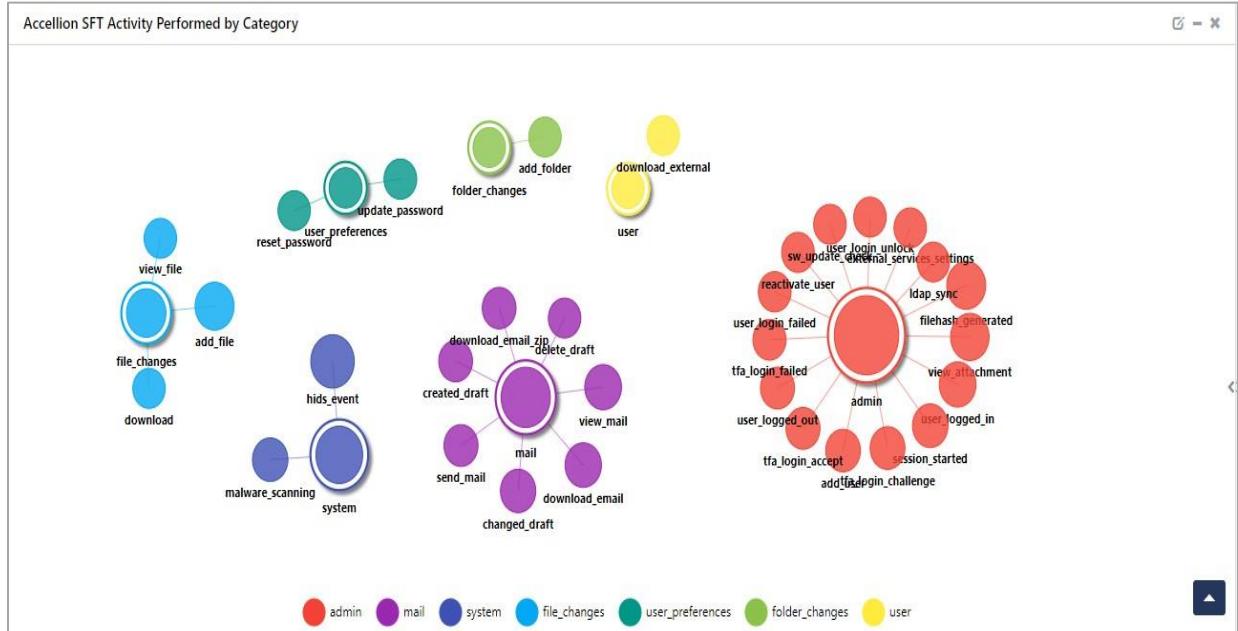


Figure 16

- Accellion SFT Login by Geolocation



Figure 17

- **Accellion SFT Login Failed by Geolocation**



Figure 18

5. Importing Accellion SFT knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Token template
- Knowledge Object
- Report
- Dashboard

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

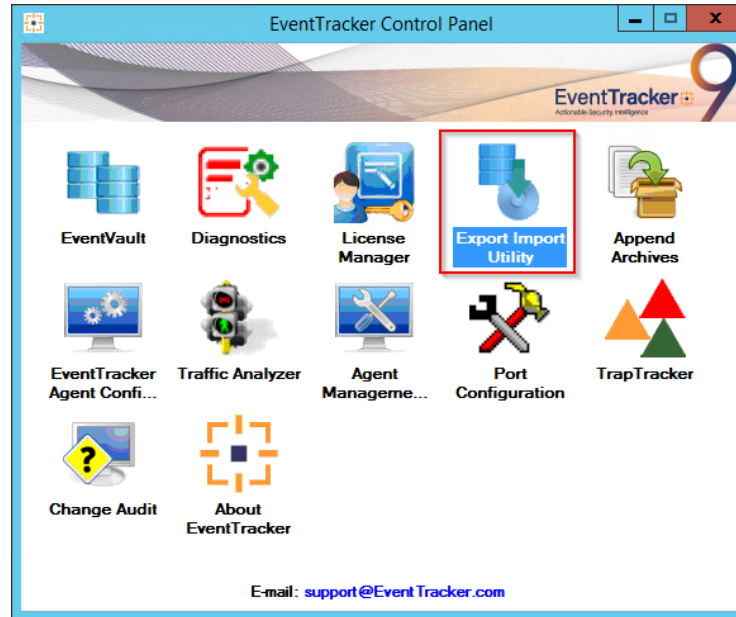


Figure 19

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then click **Browse**

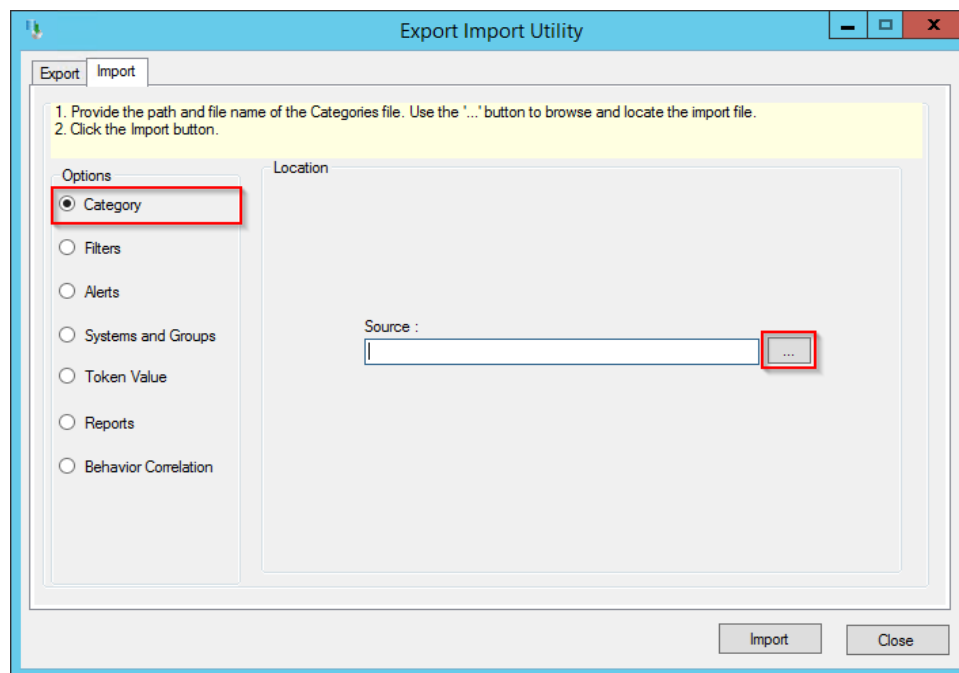


Figure 20

2. Locate **Categories_Accellion SFT.iscat** file, and then click **Open**.
3. To import categories, click **Import**.

EventTracker displays success message.

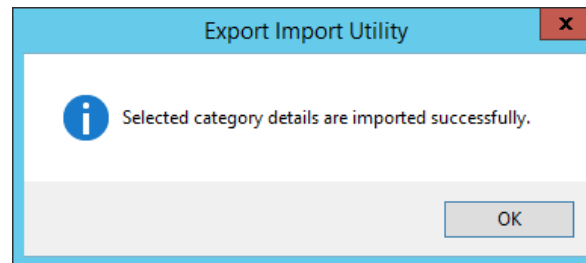



Figure 21

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

5.2 Alert

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

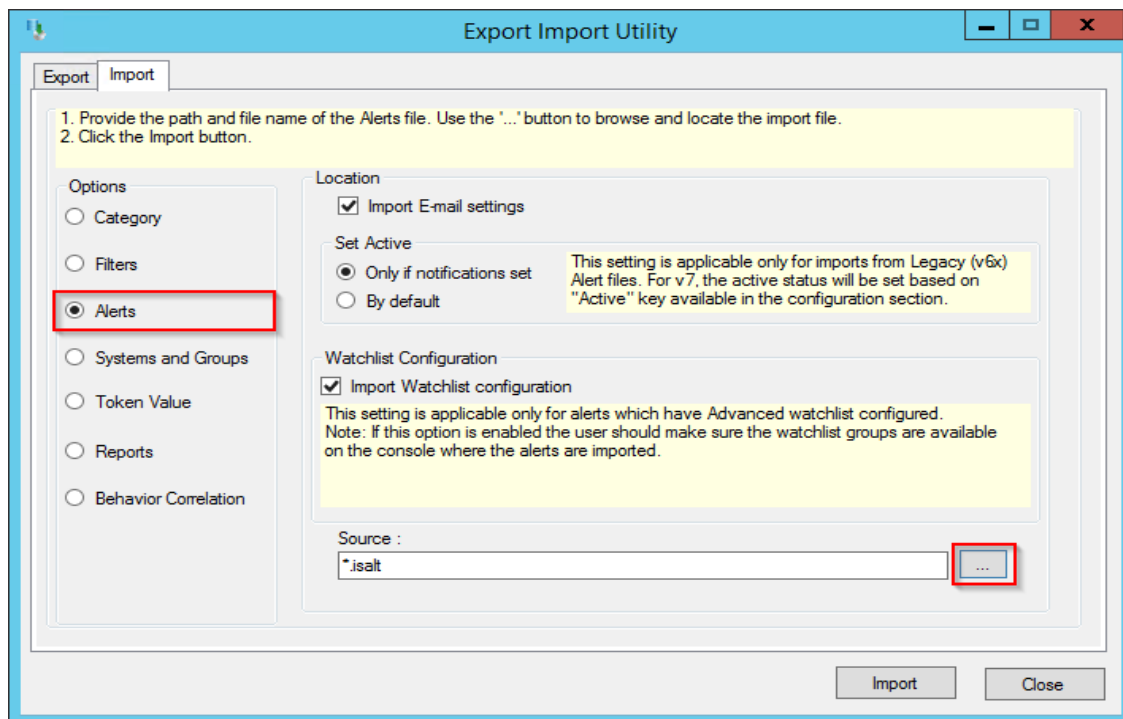


Figure 22

2. Locate **Alerts_Accellion SFT.isalt** file, and then click **Open**.

3. To import alerts, click **Import**.
EventTracker displays success message.

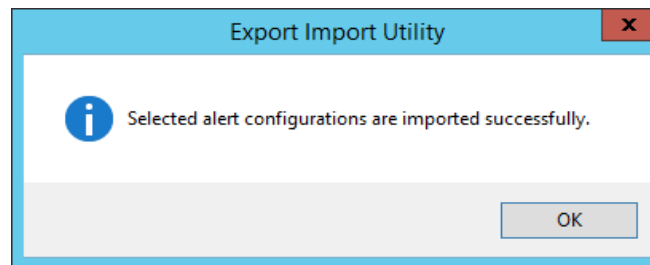


Figure 23

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

5.3 Token template

1. Click **Parsing rule** under **Admin** option in the EventTracker manager page.

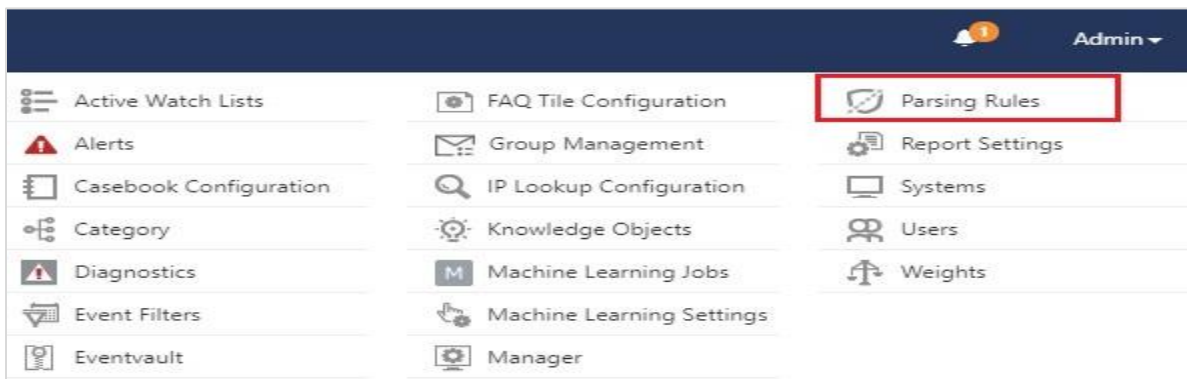


Figure 24

2. Click **Template**.

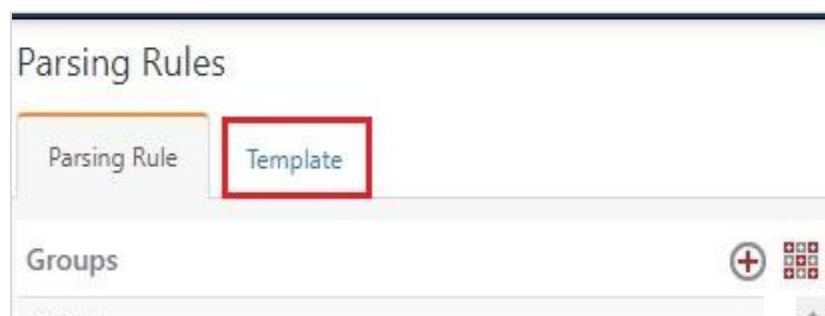


Figure 25

3. To import token template, click **Import**.



Figure 26

4. Locate the **Templates_Accellion SFT.ettd** type file by clicking **Browse** button, enable all the templates and click **import**.



Figure 27

5. Click **OK**.

5.4 Knowledge Object

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

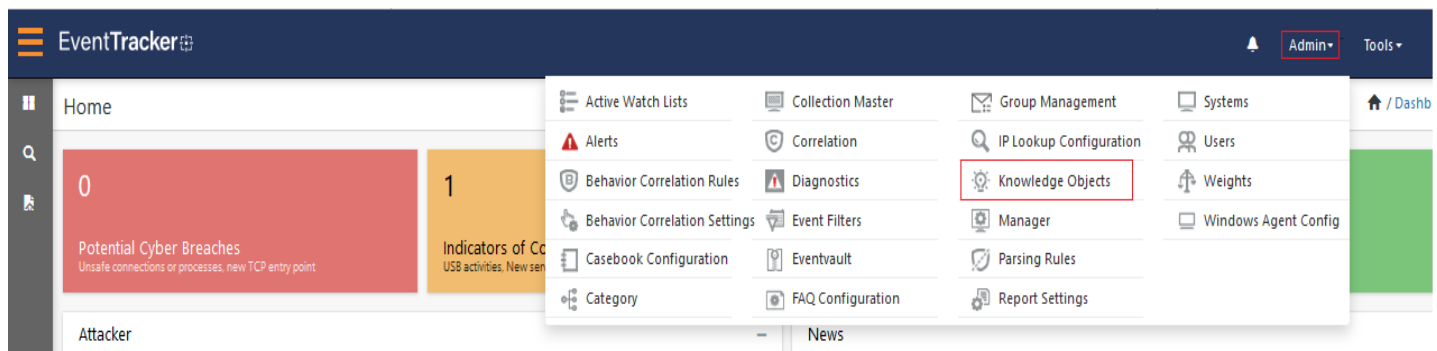


Figure 28

2. Click **Import**  as highlighted in the below image:

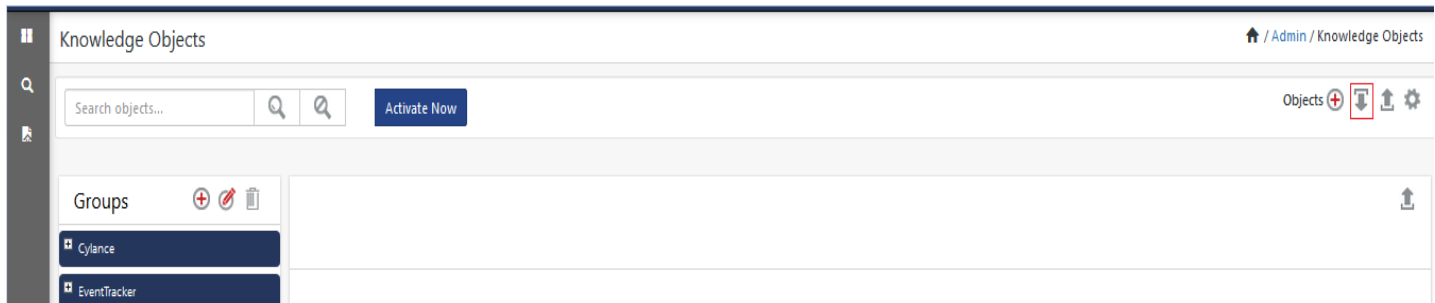


Figure 29

3. Click **Browse**.

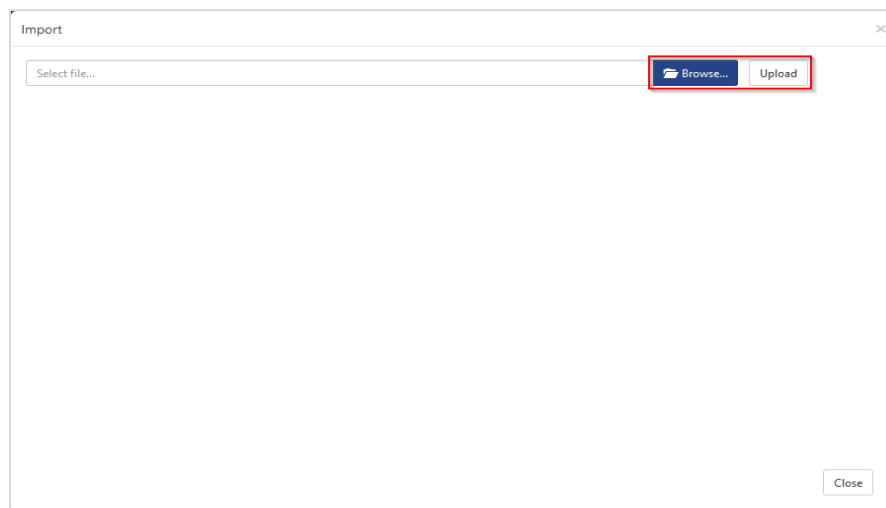



Figure 30

4. Locate the file named **KO_Accellion SFT.etko**.
5. Now select the check box and then click  **Import**.

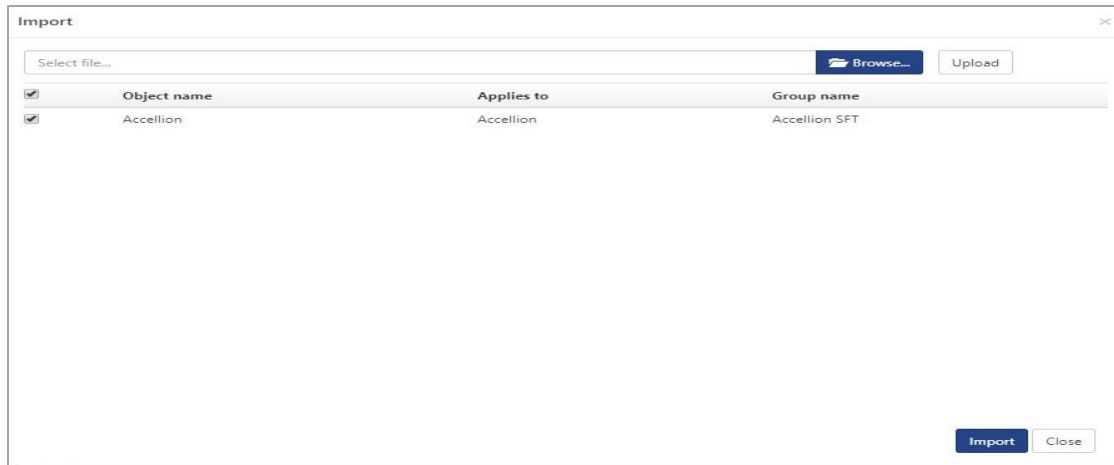


Figure 31

6. Knowledge objects are now imported successfully.

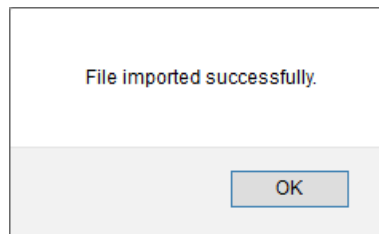


Figure 32

5.5 Report

1. Click **Reports** option and select **New (*.etcrx)** option.

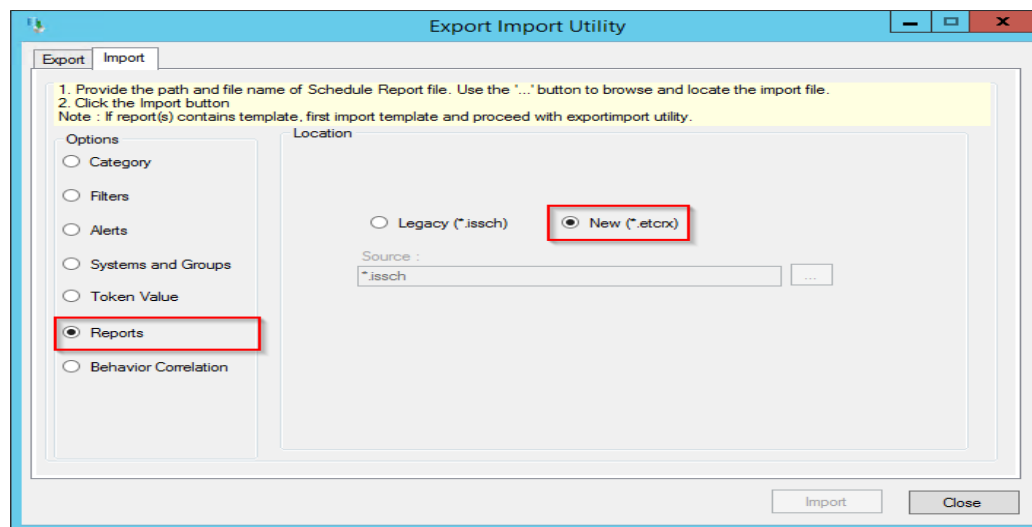


Figure 33

2. Locate the file named **Reports_Accellion SFT.etcrx** and select the check box.

Note : If report(s) contains template, first import template and proceed with report import process.

Select file

Available reports

Title Frequency

<input type="checkbox"/>	Title	Sites	Groups	Systems	Frequency
<input checked="" type="checkbox"/>	EDIT Accellion SFT - Admin Activity	R1S5-VM30			Undefined
<input checked="" type="checkbox"/>	EDIT Accellion SFT - File Management	R1S5-VM30			Undefined
<input checked="" type="checkbox"/>	EDIT Accellion SFT - Folder Management	R1S5-VM30			Undefined
<input checked="" type="checkbox"/>	EDIT Accellion SFT - Password Management	R1S5-VM30			Undefined
<input checked="" type="checkbox"/>	EDIT Accellion SFT - User Login and Logout.	R1S5-VM30			Undefined
<input checked="" type="checkbox"/>	EDIT Accellion SFT - User Login Failed.	R1S5-VM30			Undefined
<input checked="" type="checkbox"/>	EDIT Accellion SFT - User Management.	R1S5-VM30			Undefined


Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from AM minutes

Replace to

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 34

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

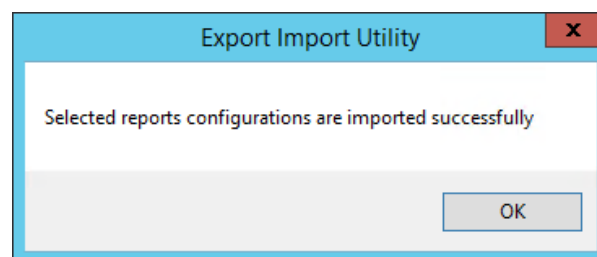


Figure 35

5.6 Dashboards

NOTE- Below steps given are specific to EventTracker 9 and later.

1. Open **EventTracker** in browser and login.

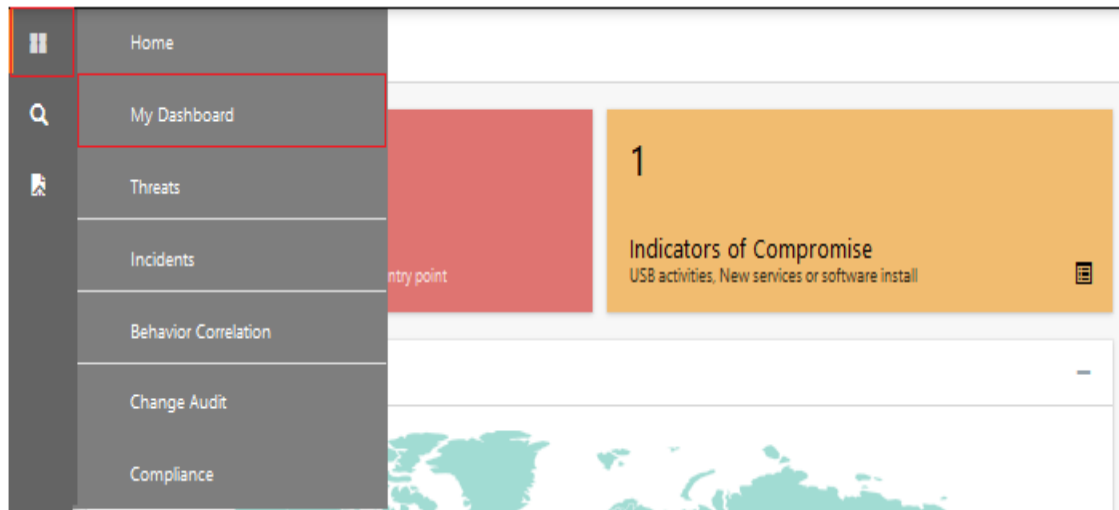


Figure 36


2. Navigate to **My Dashboard** option as shown above.
3. Click **Import**  as show below:



Figure 37

4. Import dashboard file **Dashboard_Accellion SFT.etwd** and select **Select All** checkbox.
5. Click **Import** as shown below:

Figure 38

6. Import is now completed successfully.

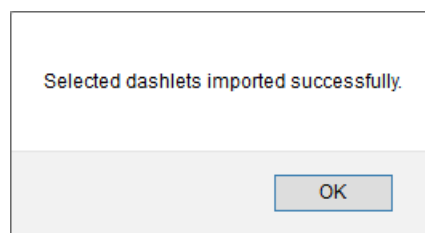



Figure 39

7. In **My Dashboard** page select  to add dashboard.

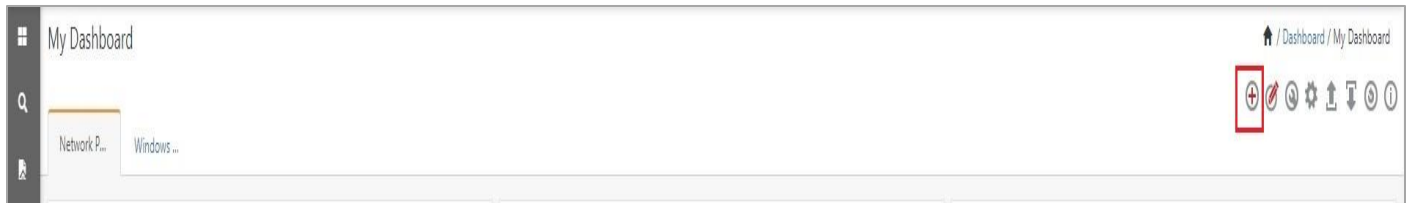



Figure 40

8. Choose appropriate name for **Title** and **Description**. Click **Save**.

Figure 41

9. In **My Dashboard** page select  to add dashlets.

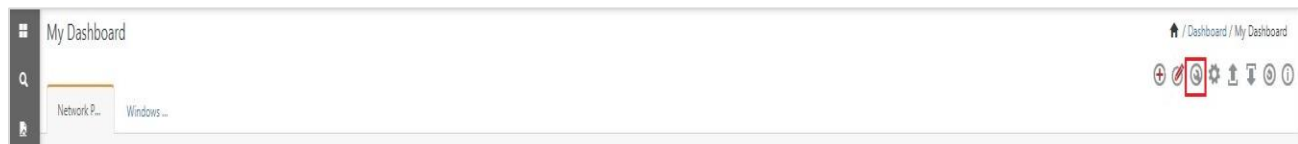


Figure 42

10. Select imported dashlets and click **Add**.

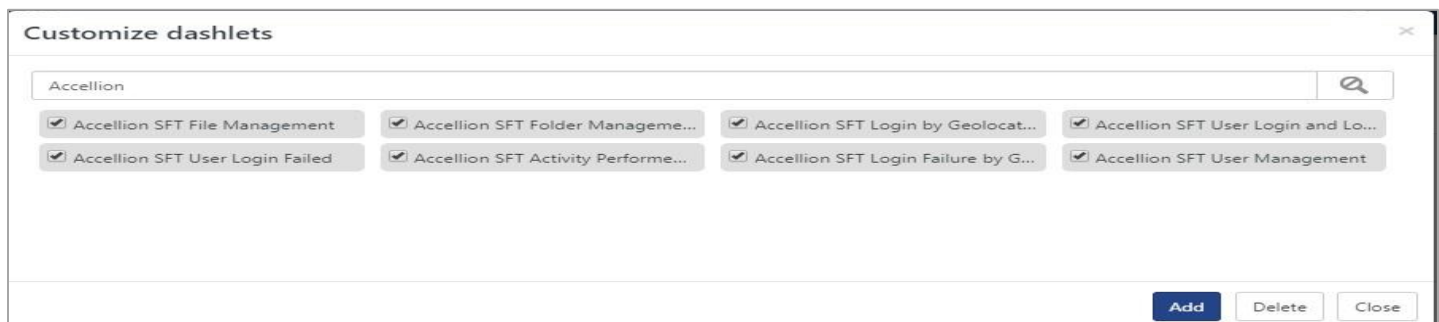


Figure 43

6. Verifying Accellion SFT knowledge pack in EventTracker

6.1 Category

1. Logon to **EventTracker**.
2. Click **Admin** dropdown, and then click **Category**.

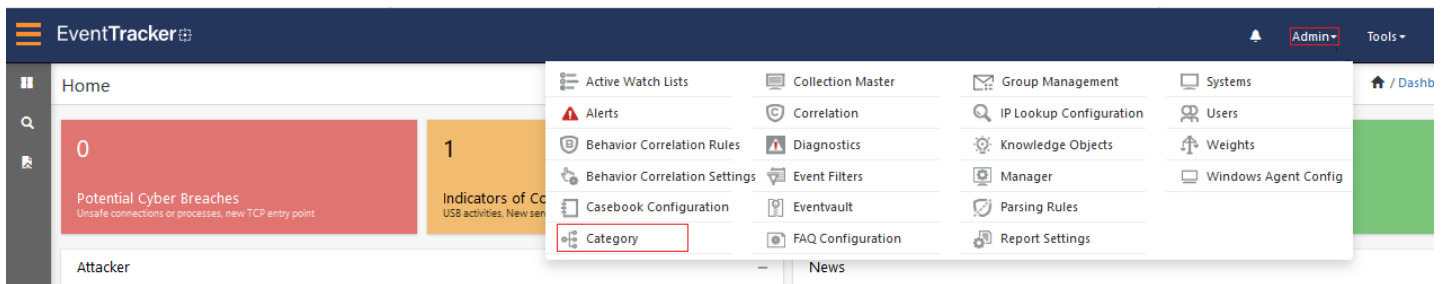


Figure 44

3. In **Category Tree** to view imported category, scroll down and expand **Accellion SFT** group folder to view the imported category.

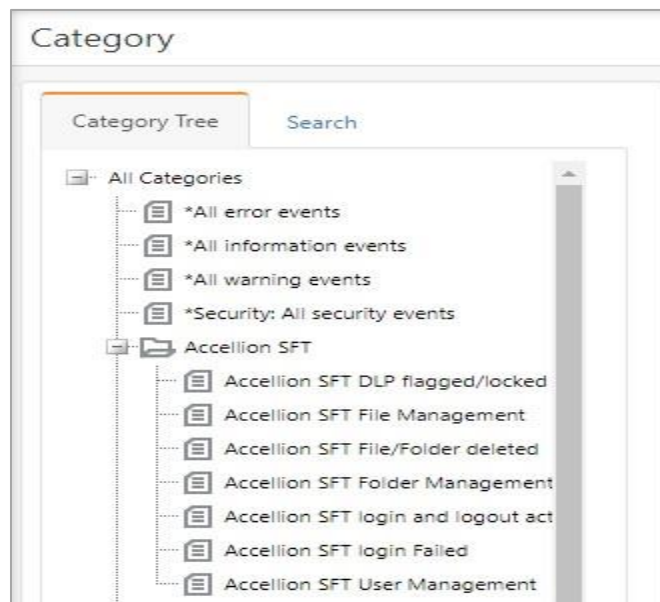


Figure 45

6.2 Alert

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

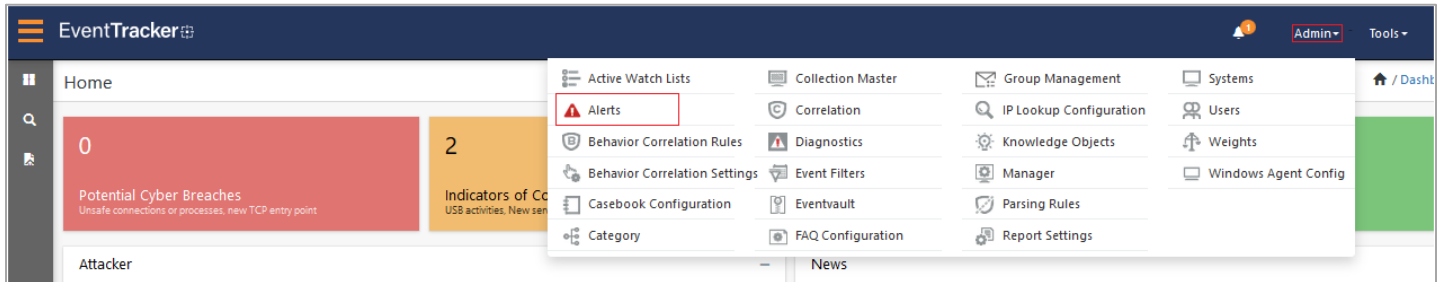


Figure 46

3. In the **Search** box, type '**Accellion SFT**', and then click **Go**.
Alert Management page will display the imported alert.

	Alert Name ^	Threat	Active	Email	Fa
<input type="checkbox"/>	Accellion SFT: DLP flagged/locked a file		<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Accellion SFT: File/Folder deleted		<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Accellion SFT: Login failed		<input type="checkbox"/>	<input type="checkbox"/>	

Figure 47

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.

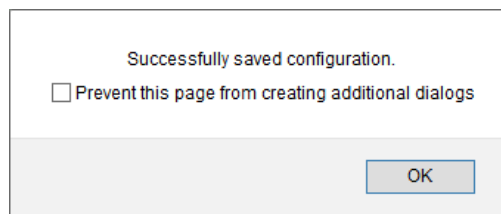


Figure 48

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

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

6.3 Token templates

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing rules**.

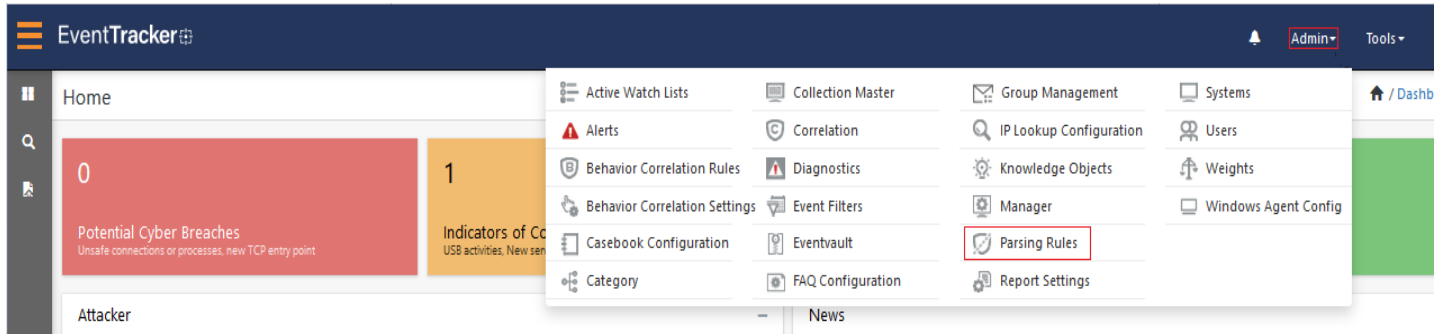


Figure 49

2. On **Template** tab, click on the **Accellion SFT** group folder to view the imported token values.

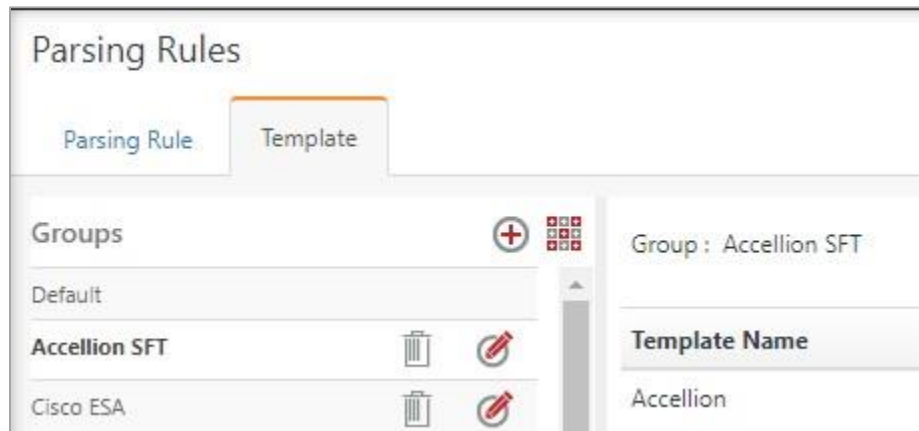


Figure 50

6.4 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects**.

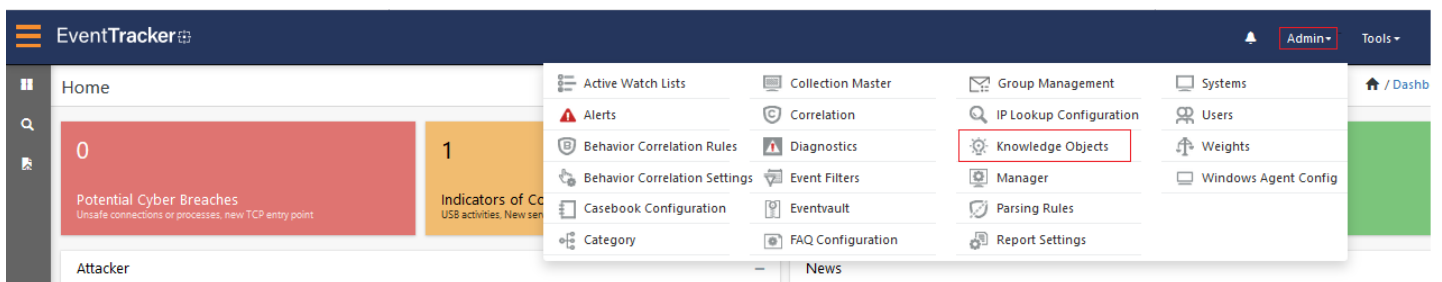


Figure 51

2. In the Knowledge Object tree, expand **Accellion SFT** group folder to view the imported knowledge object.

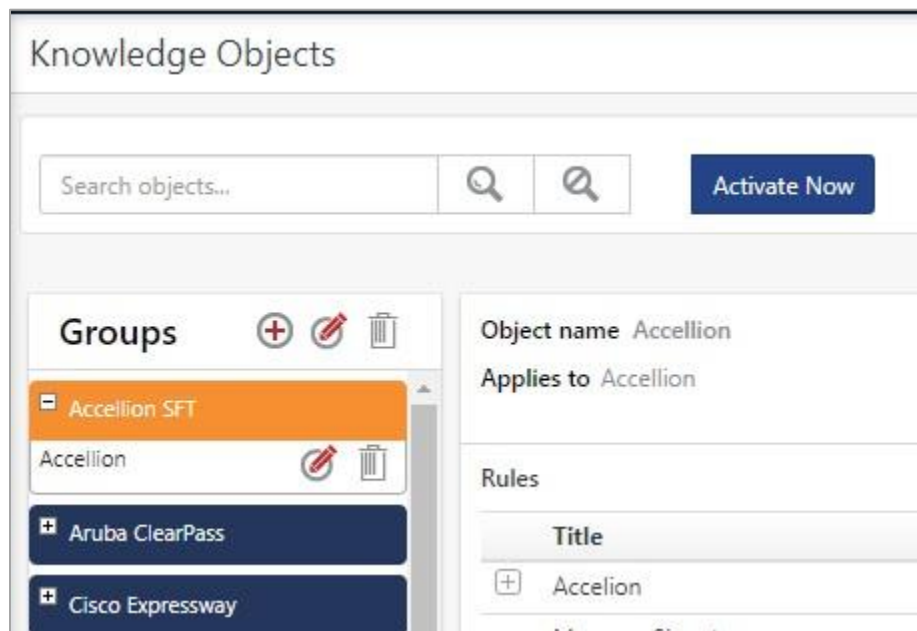


Figure 52

3. Click **Activate Now** to apply imported knowledge objects.

6.5 Report

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

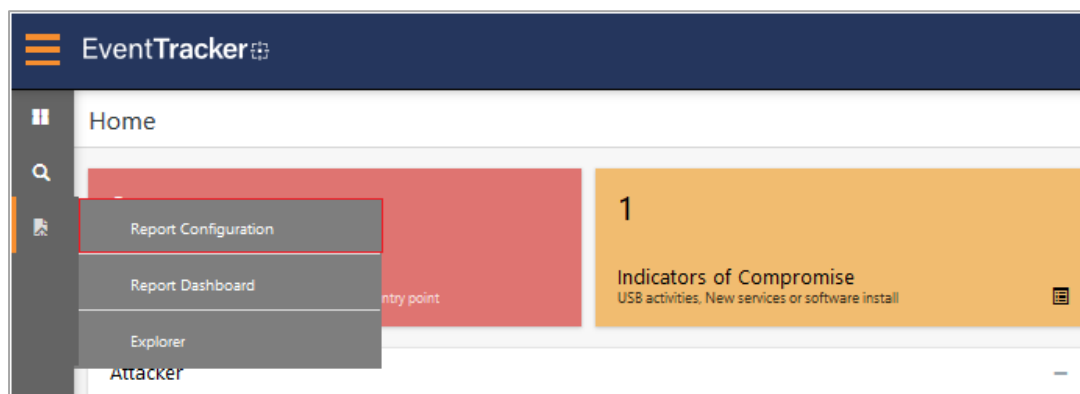


Figure 53

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

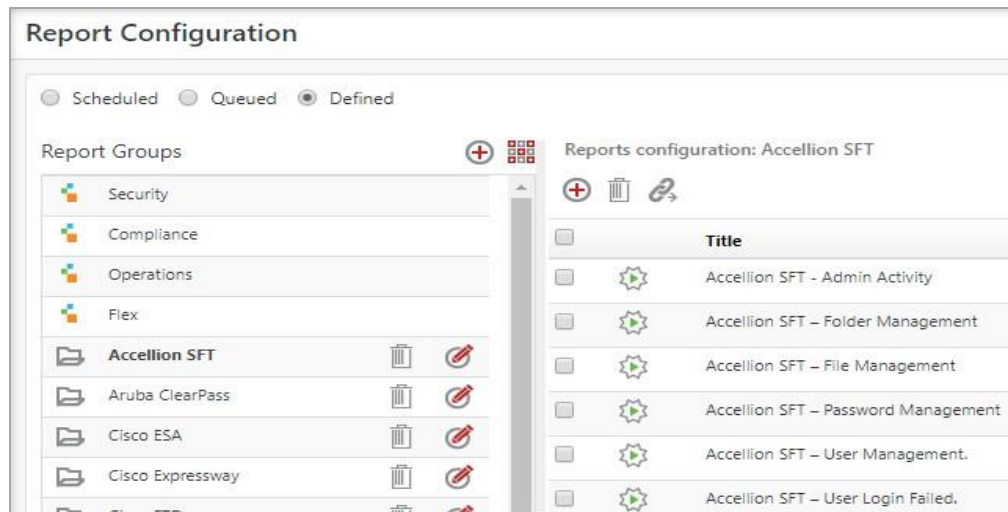


Figure 54

6.6 Dashboards

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

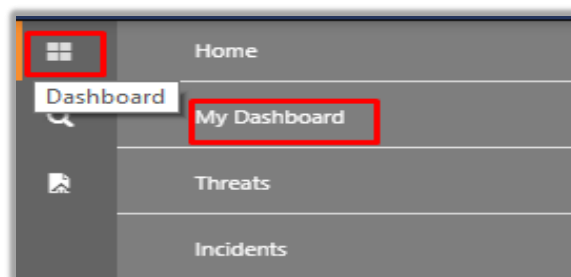


Figure 55

2. In the “**Accellion SFT**” dashboard you should be now able to see something like this.



Figure 56