EventTracker

Actionable Security Intelligence

SECURE FILE TRANSFER PROTOCOL

EventTracker v8.x and above

Publication Date: January 02, 2019

Abstract

This guide provides instructions to configure SFTP logs for User Activities and File Operations. Once EventTracker receive logs, dashboard and reports can be configured to monitor SFTP.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and Secure File Transfer Protocol.

Audience

IT Admins and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using EventTracker Enterprise.

Table of Contents

Overview

A "**Secure FTP**" server needs an SSH client for communication. A secure FTP server supports many actions on files such as file transfers comprised of multiple files, remote file management activities, creations of directories and deletions related to directories and directory listings. A secure FTP server also makes use of protocols to provide security features such as authentication, encryption or data integrity, password management and access control mechanisms.

EventTracker helps you to monitor User authenticated, user request open session, user request close session, user request remove session; file opened, file upload started, and successfully stored file.

Prerequisites

- **EventTracker v8.x or above** should be installed.
- Allow 514 port from firewall, if there is in between SFTP and EventTracker manager.

Configure RSyslog to forward SFTP logs to EventTracker

SFTP can send logs to EventTracker using rsyslog. Please follow the following steps to configure it.

1. Open /etc/rsyslog.conf using **vi.**

Figure 1

2. Configure EventTracker Manager IP and syslog port number as per the below specified snap, so that we can get SFTP logs.

   ***.* @EventTracker Manager IP:514**

```
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514

*. *  @192.168.10.254:514

# ### end of the forwarding rule ###
```

Figure 2

Once completed “rsyslog.conf” and the logs will start logging into the specified IP host location.

EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are available in EventTracker v8.x and later to support SFTP:

Reports

- **SFTP-User Activities:** This category provides information related to the User password authentication, user open, close and remove sessions.

Computer	Interface	User Name	Source IP Address	Destination IP Address	Session ID	Status
SFTP	8		10.119.1.242	172.16.28.106	9244	Incoming connection request
SFTP		osiftpuser			9243	authenticated
SFTP	8		10.119.1.242	172.16.28.106	9243	Incoming connection request
SFTP					9242	close
SFTP					9242	
SFTP					9242	Open
SFTP		osiftpuser			9242	authenticated
SFTP					9242	removed
SFTP	8		10.119.1.242	172.16.28.106	9242	Incoming connection request
SFTP					9241	close
SFTP					9241	removed
SFTP					9240	Open
SFTP					9241	Open
SFTP					9240	close
SFTP	8		10.119.1.242	172.16.28.106	9240	Incoming connection request
SFTP					9241	
SFTP					9240	
SFTP					9240	removed
SFTP		osiftpuser			9241	authenticated

Figure 3

- **SFTP- File Operations:** This category provides information related to file opened, upload started, successfully stored.

Computer	User Name	File Name	Session ID	File Operations
SFTP	osiftpuser	FASRPTS\DeprProcesslog_12-14-2018-1.txt	9246	Upload started
SFTP	osiftpuser	FASRPTS\DeprProcesslog_12-14-2018-1.txt	9246	Successfully stored
SFTP			9245	
SFTP	osiftpuser		9245	File open
SFTP	osiftpuser	IPS_EXCP.147	9244	Successfully stored
SFTP		DeprProcesslog_12-14-2018-1.txt	9246	
SFTP	osiftpuser	DeprProcesslog_12-14-2018-1.txt	9246	File open
SFTP	osiftpuser	IPS_EXCP.148	9245	Upload started
SFTP	osiftpuser	IPS_EXCP.148	9245	Successfully stored
SFTP	osiftpuser	AH_CTX.020	9243	Successfully stored
SFTP	osiftpuser	IPS_EXCP.147	9244	Upload started
SFTP	osiftpuser	AH_CTX.020	9243	Upload started
SFTP	osiftpuser		9244	File open
SFTP			9244	
SFTP	osiftpuser		9243	File open
SFTP			9243	
SFTP			9242	
SFTP	osiftpuser		9242	File open
SFTP	osiftpuser	AH_EXCPT.020	9242	Successfully stored

Figure 4

Import Knowledge Pack into EventTracker

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

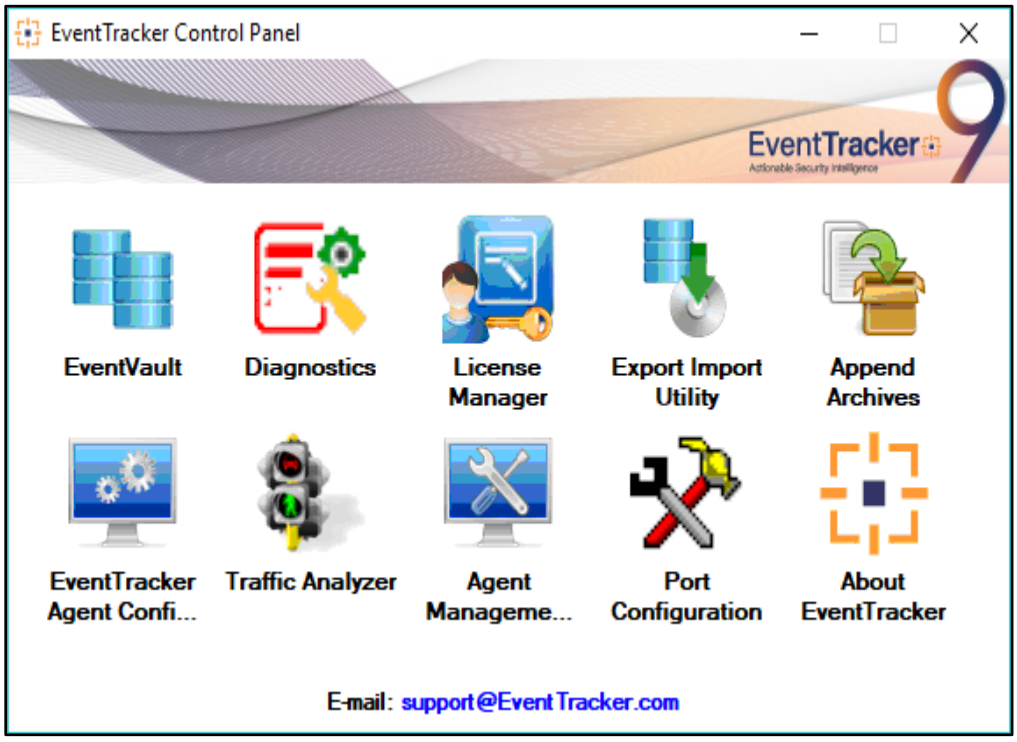

Figure 5

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

Knowledge Objects

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

Figure 6

3. Now select all the check box and then click on ‘**Import**’ option.

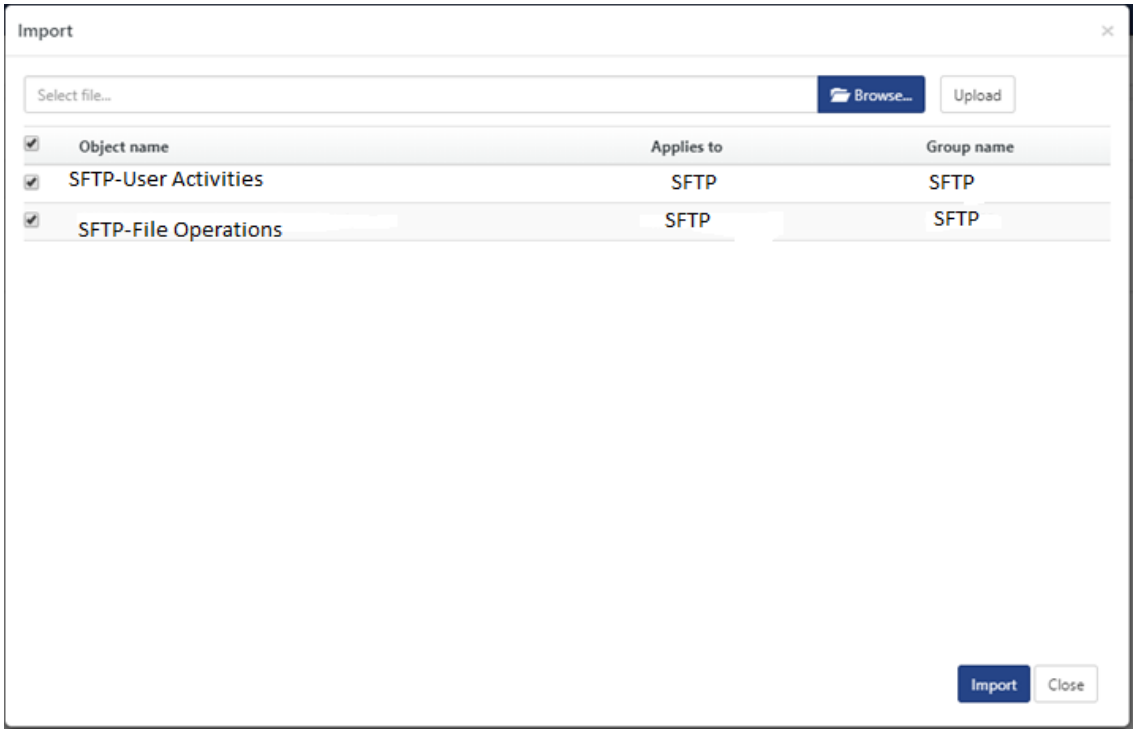

Figure 7

4. Knowledge objects are now imported successfully.

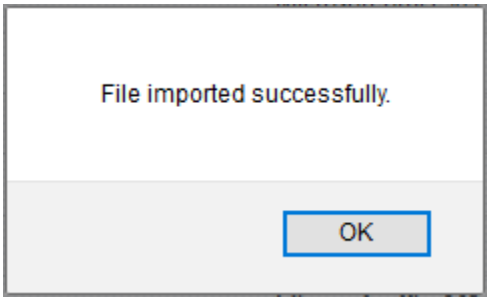

Figure 8

Templates

1. Click parsing rules option, create group and click Import.
2. Locate the file name **KO_SFTP.ettd**.

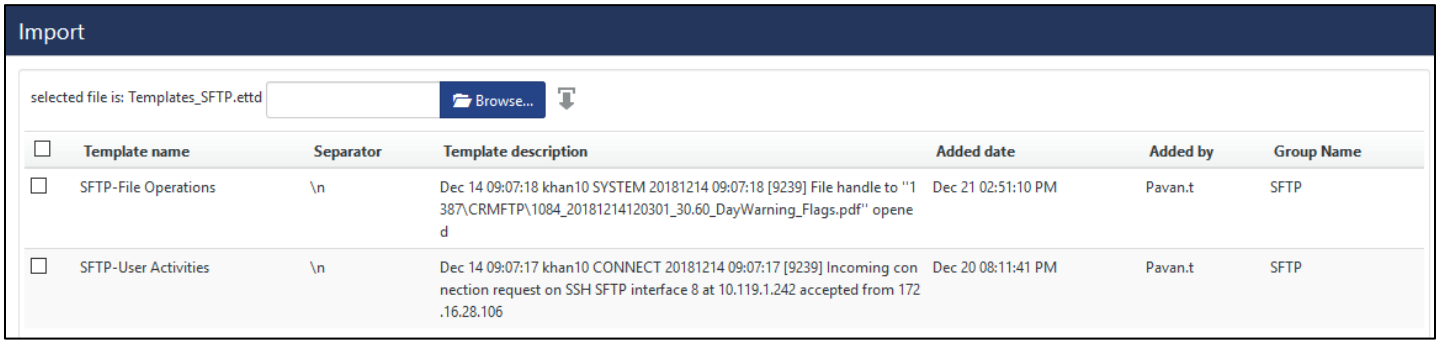

Figure 9

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

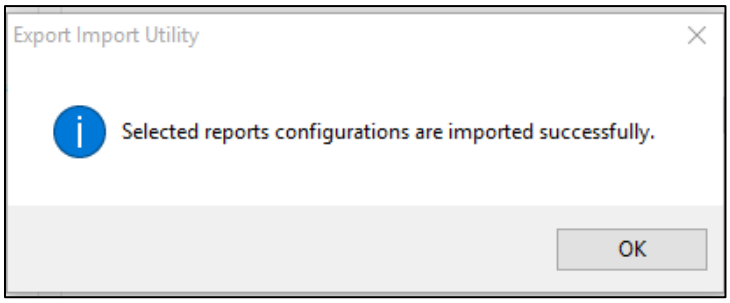

Figure 10

Flex Reports

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

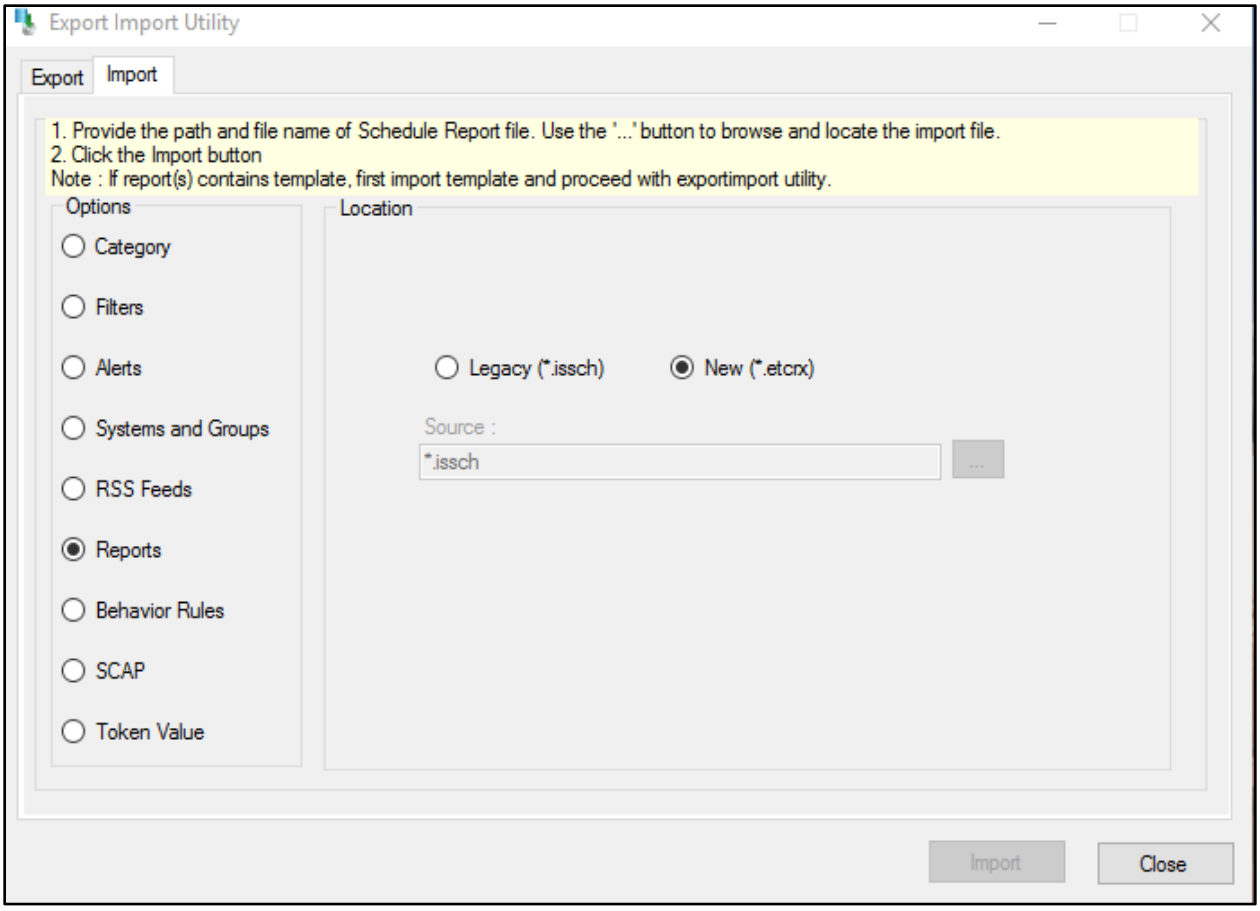

Figure 11

2. Locate the file named **Flex Reports_SFTP.etcrx** and select all the check box.

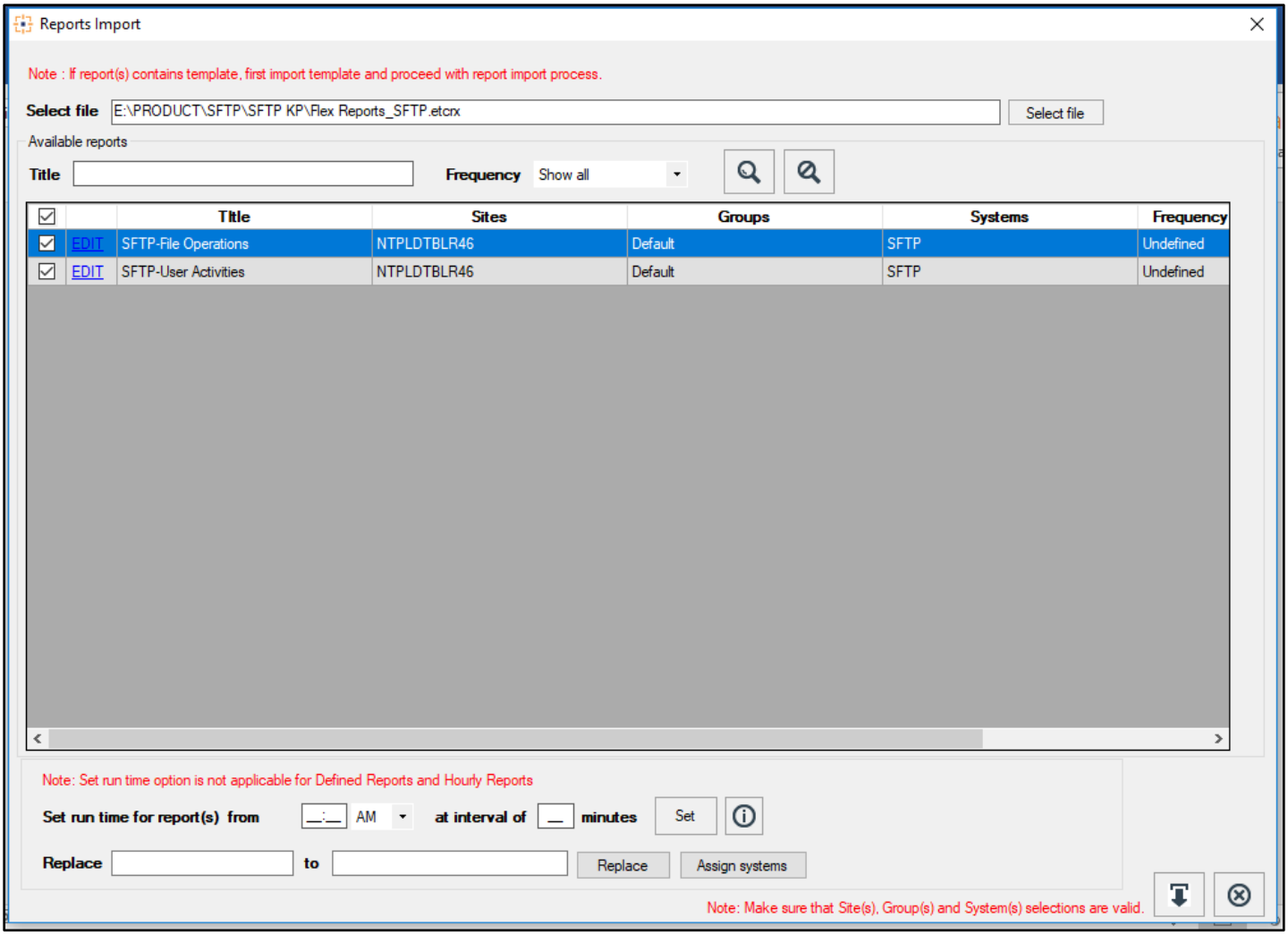

Figure 12

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

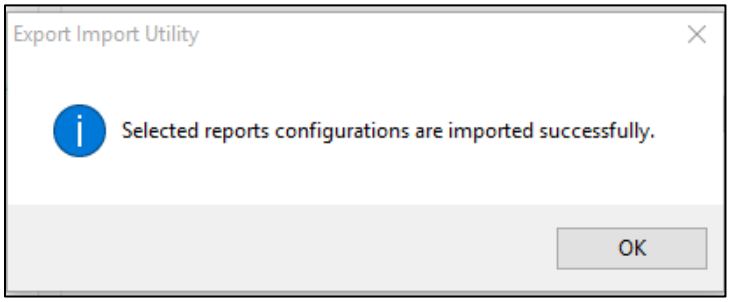

Figure 13

Verify Knowledge Pack in EventTracker

Knowledge Object

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

Knowledge Object are displayed in the pane.

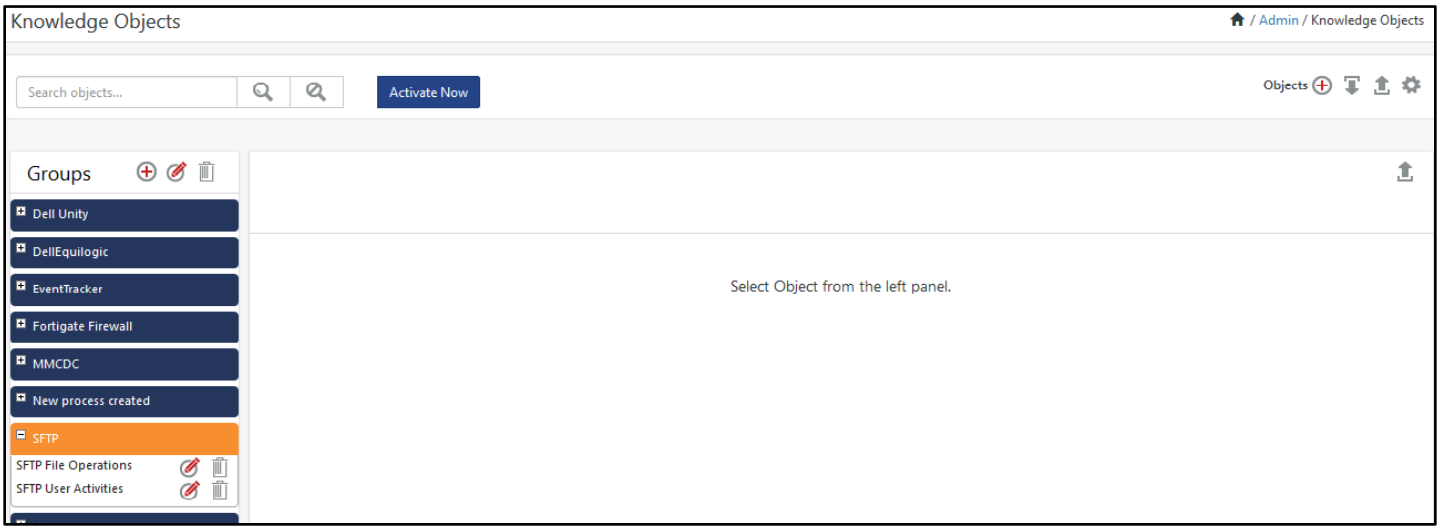

Figure 14

Flex Reports

1. Logon to **EventTracker Enterprise**.
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 **SFTP** group folder.

   Reports are displayed in the Reports configuration pane.

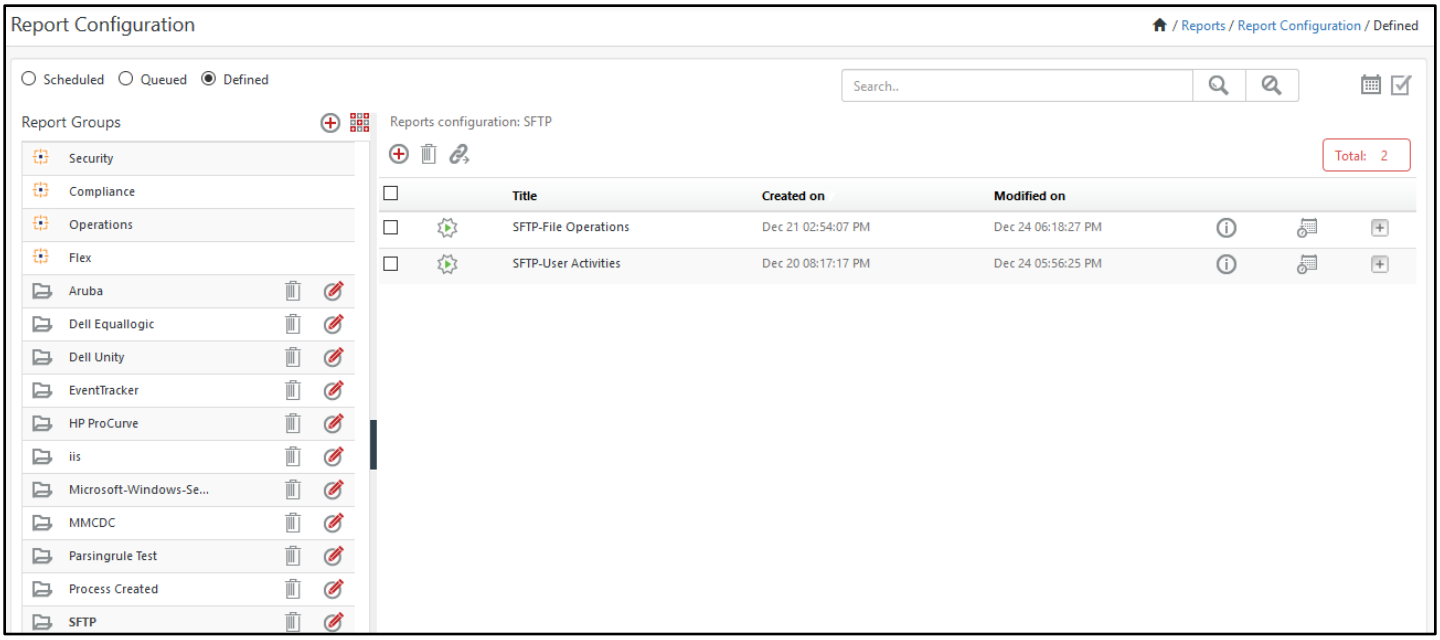

Figure 15

Templates

1. Logon to **EventTracker Enterprise**.
2. Click the **Parsing rules** menu
3. Select **Template** and choose Group name.
4. In **Template** to view imported Templates, scroll down and click **SFTP** group folder.

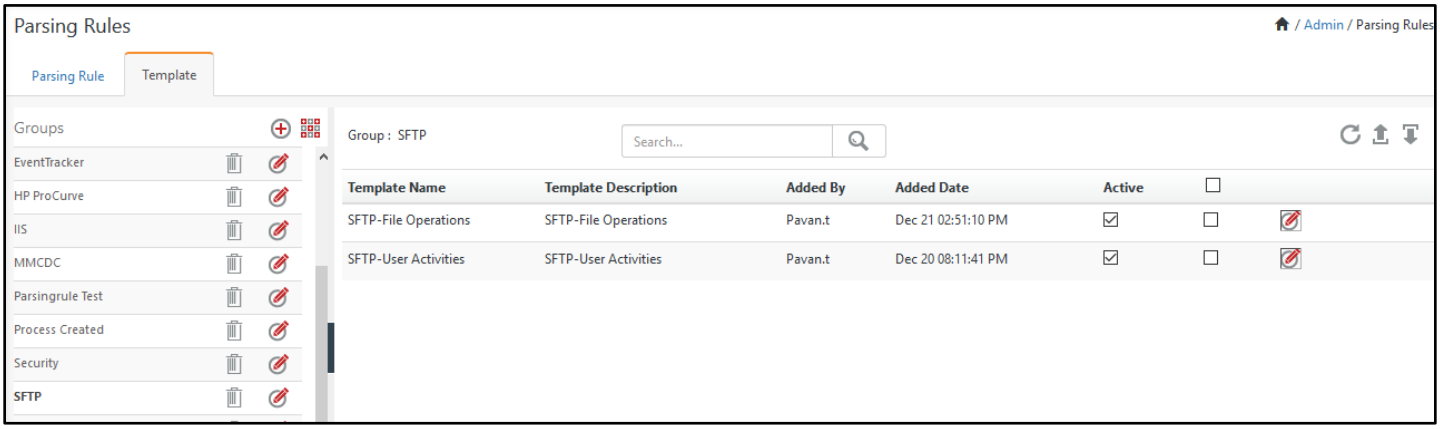

Figure 16