

Integrate FortiAnalyzer

EventTracker Enterprise

Publication Date: Feb. 26, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This guide provides instructions to configure FortiAnalyzer to send the event logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and FortiAnalyzer 4.0, 5.0 and later.

Audience

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

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract	1
Scope	1
Audience.....	1
Overview	3
Prerequisites.....	3
Enable Syslog forwarding on FortiAnalyzer	3
Configure Operation Mode.....	3
Configure Syslog Server	4
EventTracker Knowledge Pack (KP).....	5
Categories	5
Alerts	6
Reports.....	7
Dashboard.....	12
Import Knowledge Pack into EventTracker.....	13
Import Category.....	14
Import Alerts.....	15
Import Flex Reports.....	16
Import Parsing Rules.....	17
Import Token Templates.....	18
Import Knowledge Object	19
Verify Knowledge Pack in EventTracker.....	22
Verify Categories.....	22
Verify Alerts.....	22
Verify Parsing Rules.....	23
Verify Token Templates	24
Verify Knowledge Object.....	25
Verify Flex Reports.....	25
Create Dashboards in EventTracker.....	26
Schedule Reports.....	26
Create Dashlets.....	29

Overview

FortiAnalyzer logs and analyzes aggregated log data from Fortinet devices and other syslog-compatible devices. EventTracker examines this collection of logs and leverages machine learning to identify critical events, suspicious network traffic, configuration changes and user behavior analytics.

Prerequisites

- EventTracker v7.x and later should be installed.
- FortiAnalyzer 4.0, 5.0 and 5.2 should be installed.

Enable Syslog forwarding on FortiAnalyzer

Configure Operation Mode

1. Go to **System Settings** > **Dashboard**.
2. In the **System Information** widget, in the **Operation Mode** field, select **[Change]**.
3. In the **Change Operation Mode** dialog box, select **Collector**, and then select **OK**.

▼ System Information	
Host Name	FAZVM64 [Change]
Serial Number	FAZ-VM0000000001
Platform Type	FAZVM64
System Time	Wed Jun 25 09:48:11 PDT 2014 [Change]
Firmware Version	5.2.0 (5.2.0) [Update]
System Configuration	Last Backup:N/A [Backup] [Restore]
Current Administrators	admin [Change Password] /1 in Total [Detail]
Up Time	0 day 0 hour 11 minutes 45 seconds
Administrative Domain	Enabled [Disable]
Operation Mode	Collector [Change]

Figure 1

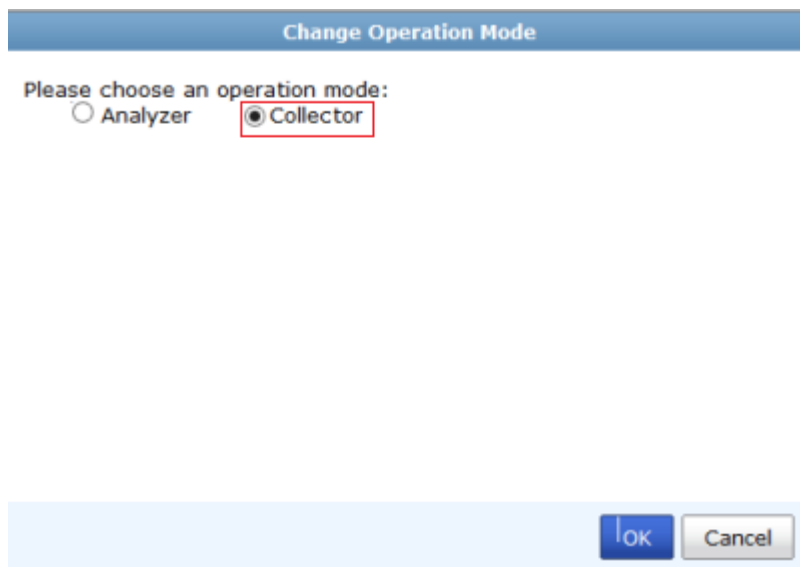


Figure 2

The Web-based Manager will refresh and the Device Manager, Log View, and System Settings tabs will be available.

Configure Syslog Server

1. Go to **System settings > Advanced > Syslog Server > Create new.**

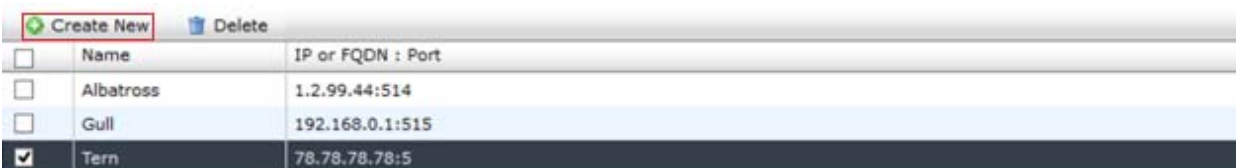


Figure 3

2. Configure the following settings and then select **OK**
Name: Enter a name for the syslog server.
IP address (or FQDN): Enter the IP address or FQDN of the syslog server.
Port: Enter the syslog server port number. The default port is 514.

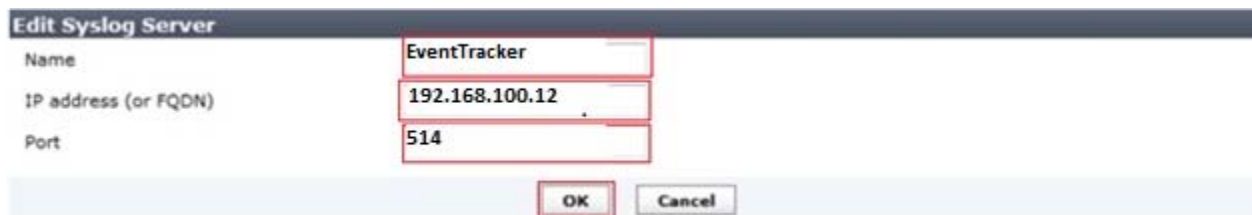


Figure 4

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker categories, alerts, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7 and later to support FortiAnalyzer monitoring:

Categories

- **FortiAnalyzer: Anomalies attack** - This category based report provides information related to attacks detected.
- **FortiAnalyzer: Certificates imported attack** - This category based report provides information related to certificate imported by unknown user.
- **FortiAnalyzer: Configuration back up failed** - This category based report provides information related to configuration backup failure.
- **FortiAnalyzer: Configuration changes** - This category based report provides information related to change in device configuration.
- **FortiAnalyzer: Configuration restored** - This category based report provides information related to external configuration restoration.
- **FortiAnalyzer: Critical error events** - This category based report provides information related to occurrence of critical errors.
- **FortiAnalyzer: Firmware updated** - This category based report provides information related to firmware update.
- **FortiAnalyzer: Added report language** - This category based report provides information related to addition of language report.
- **FortiAnalyzer: Deleted report language** - This category based report provides information related to deletion of language report.
- **FortiAnalyzer: Log backup failed** - This category based report provides information related to failure of log backup.
- **FortiAnalyzer: Log files imported** - This category based report provides information related to log file import.
- **FortiAnalyzer: Migration successfully** - This category based report provides information related to successful migration.
- **FortiAnalyzer: Reports restored** - This category based report provides information related to restoration of reports.
- **FortiAnalyzer: System configuration restored** - This category based report provides information related to restoration of system configuration.
- **FortiAnalyzer: System restarted** - This category based report provides information related to system restarts.

- **FortiAnalyzer: User access profile changed** - This category based report provides information related to change in access profile.
- **FortiAnalyzer: User logged out** - This category based report provides information related to user log off.
- **FortiAnalyzer: User login failed** - This category based report provides information related to user logon failure.
- **FortiAnalyzer: User login successfully** - This category based report provides information related to user logon success.
- **FortiAnalyzer: VPN subsystems** - This category based report provides information related to VPN sessions.
- **FortiAnalyzer: Firmware update failed** - This category based report provides information related to failure of firmware update.

Alerts

- **FortiAnalyzer: User logon failed** – This alert is generated when administrator attempt to log in to the web-based manager using GUI or CLI was failed.

Log Considered:

```
date=2009-12-21 time=15:55:00 log_id=0104000001 type=event subtype=admin pri=alert  
device_id=FLG8002704000076 user=amdin ui=GUI(172.20.110.44) action=login status=failure  
reason=name_invalid msg="User 'amdin'login failed from GUI(172.20.110.44)"
```

- **FortiAnalyzer: Administrator deleted a device** – This alert is generated when administrator deleted the device.

Log Considered:

```
date=2009-12-15 time=14:32:41 log_id=0100000045 type=event subtype=config  
pri= warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10)  
action=config msg="User deleted device 'FG200A3907550170'"
```

- **FortiAnalyzer: Removed a disk from RAID array** – This alert is generated when admin removes the disk from the RAID array.

Log Considered:

```
date=2009-06-24 time=10:31:26 log_id=0100000086 type=event subtype=config pri=warning  
device_id=FLG8002704000076 user=admin ui=console action=config msg="user admin  
delete  
disk md1 from RAID array"
```

Reports

- **FortiAnalyzer – Administrator logon activity** – This report provides information related to user logon behavior which includes User Name, User Interface, Action, Status and Reason fields.

LogTime	Computer	User Name	User Interface	Source IP	Action	Status	Reason
01/27/2016 02:59:41 PM	FORTIANALYZER22	admin	GUI	172.16.1.20	login	success	none
01/27/2016 03:29:54 PM	FORTIANALYZER22	admin	GUI	172.16.1.20	logout	success	none
01/27/2016 03:30:22 PM	FORTIANALYZER22	admin	console		login	success	none
01/27/2016 03:42:54 PM	FORTIANALYZER22	admin	SSH	172.16.1.20	login	success	none
01/27/2016 03:45:55 PM	FORTIANALYZER22	admin	jsconsole		logout	success	user_exit
1/27/2016 03:49:58PM	FORTIANALYZER22	admin	telnet	172.16.1.20	logout	success	user_exit
01/27/2016 03:52:12 PM	FORTIANALYZER22	admin	ssh	172.16.1.20	logout	success	user_exit

Figure 5

Log Considered:

```
date=2009-12-22 time=17:01:57 log_id=0104000001 type=event subtype=admin pri=information
device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=login status=success
reason=none msg="User admin login successfully from GUI(172.16.1.20)"
```

- **FortiAnalyzer – Administrator logon failed** – This report provides information related to login failure which includes column such as User Name, User Interface, Source IP, Action, Status and Reason.

LogTime	Computer	User Name	User Interface	Source IP	Action	Status	Reason
01/27/2016 03:29:54 PM	FORTIANALYZER22	amdin	GUI	172.20.110.44	login	failure	name_invalid
01/27/2016 03:39:55 PM	FORTIANALYZER22	amdin	GUI	172.20.110.45	login	failure	name_invalid
01/27/2016 03:42:54 PM	FORTIANALYZER22	amdin	GUI	172.20.110.48	login	failure	name_invalid
01/27/2016 03:45:55 PM	FORTIANALYZER22	amdin	GUI	172.20.110.41	login	failure	name_invalid

Figure 6

Log Considered:

```
date=2009-12-21 time=15:55:00 log_id=0104000001 type=event subtype=admin pri=alert
device_id=FLG8002704000076 user=amdin ui=GUI(172.20.110.44) action=login status=failure
reason=name_invalid msg="User 'amdin' login failed from GUI(172.20.110.44)"
```

- **FortiAnalyzer – Backup and restore activity** – This reports provides information related to backup, restore, reboot and upload which includes columns such as User Name, User Interface, Source IP, Action, Status and Message details.

LogTime	Computer	User Name	User Interface	Source IP	Action	Status	Message Details
01/28/2016 06:47:41 PM	FORTIANALYZER2	admin	ssh	172.16.1.20	restore_config	success	User admin changed the configuration from ssh(172.16.1.20) by starting migration.
01/28/2016 06:50:12 PM	FORTIANALYZER2	admin	ssh	172.16.1.20	restore_reports	success	User admin restored reports from ssh(172.16.1.20)(ftp) successfully.
01/28/2016 06:52:25 PM	FORTIANALYZER2	admin	GUI	172.16.1.21	factory_reset	success	System has been reset to factory default by user 'admin' via GUI(172.16.1.20)
01/28/2016 06:55:32 PM	FORTIANALYZER2	admin	GUI	172.16.1.21	upload	success	System config file has been backed up by user 'admin' via GUI(172.16.1.20)
01/28/2016 06:58:40 PM	FORTIANALYZER2	system	system		upload	failure	Too many failed attempts(core file or crash log fortilogd.dbg.tgz), deleting upload request for host 172.16.1.20.
01/28/2016 07:10:40 PM	FORTIANALYZER2	unknown	unknown		backup_config	success	User unknown backed up the configuration from unknown successfully.
01/28/2016 07:20:45 PM	FORTIANALYZER2	admin	GUI	172.20.120.104	restore	success	System configuration file has been restored by user 'admin' via GUI(172.16.1.20)

Figure 7

Log Considered:

```
date=2010-01-15 time=16:31:52 log_id=0104000008 type=event subtype=admin pri=information
device_id=FLG8002704000076 user=admin ui=ssh(172.16.1.20) action=restore_reports
status=success reason=none msg="User admin restored reports from ssh(172.16.1.20)(ftp)
successfully."
```

- **FortiAnalyzer – Configuration changes activity** – This report provides information related to change in authentication server which includes columns such as User Name, User Interface, Source IP, Status and Message details.

Log considered:

```
date=2010-01-06 time=12:02:17 log_id=0100032133 type=event subtype=config pri=notice
device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User admin
changed a radius server radius3 setting from GUI(172.16.1.20).name=radius3 old
server=192.168.1.10 new server=192.168.1.20 secret=my secret"
```

LogTime	Computer	User Name	User Interface	Source IP	Status	Message Details
02/24/2016 10:38:33 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	changed	a radius server radius3 setting from GUI(172.16.1.20).name=radius3 old_server=192.168.1.10 new_server=192.168.1.20 secret=mysecret
02/24/2016 10:40:12 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	deleted	A ldap server
02/24/2016 10:43:25 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	deleted	radius server radius3 from GUI(172.16.1.20)
02/24/2016 10:47:33 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	changed	the NTP server sync interval to 61
02/24/2016 10:50:40 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	changed	the system global language to 'English'
02/24/2016 10:52:45 AM	FORTIANALYZER16	admin	GUI	172.16.1.10	changed	the system timeout from 5 to 480 minutes
02/24/2016 10:55:33 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	changed	sync NTP server from " to 'pool.ntp.org'
02/24/2016 10:58:47 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	changed	the system global hostname from 'FortiAnalyzer-800B' to 'FortiAnalyzer-800B-1'
02/24/2016 11:10:23 AM	FORTIANALYZER16	admin	jsconsole		changed	the console baudrate from '57600' to '9600'
02/24/2016 11:25:33 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	changed	DNS server from 'prim=0.0.0.0, sec=0.0.0.0' to 'prim=192.168.1.10, sec=172.16.1.1'
02/24/2016 11:30:40 AM	FORTIANALYZER16	admin	GUI	172.16.1.20	deleted	alias 'alias1' ip_range '192.168.1.20'

Figure 8

- FortiAnalyzer- Network share management** – This report provides information related to network area storage and network file sharing which includes columns such as User Name, User Interface, Source IP, Status and Message Details.

LogTime	Computer	User Name	User Interface	Source IP	Status	Message Details
01/28/2016 05:03:02 PM	FORTIANALYZER9	admin	GUI	172.16.1.10	changed	the NAS group 'grp'
01/28/2016 05:13:02 PM	FORTIANALYZER9	admin	GUI	172.16.1.20	deleted	NAS user 'share-user2'
01/28/2016 05:20:02 PM	FORTIANALYZER9	admin	GUI	172.16.1.10	added	new NFS sharing 'report-share'
01/28/2016 05:25:18 PM	FORTIANALYZER9	system	GUI	172.16.1.10	changed	the NAS user 'share-user3' settings
01/28/2016 05:30:02 PM	FORTIANALYZER9	admin	GUI	172.16.1.10	added	new NAS user 'share-user1'
01/28/2016 05:36:48 PM	FORTIANALYZER9	admin	GUI	172.16.1.20	deleted	NAS user 'share-user2'
01/28/2016 05:40:22 PM	FORTIANALYZER9	system	GUI	172.16.1.10	changed	the NAS user 'share-user3' settings
01/28/2016 05:42:26 PM	FORTIANALYZER9	admin	GUI	172.16.1.10	added	new NAS group 'grp'
01/28/2016 05:45:32 PM	FORTIANALYZER9	system	GUI	172.16.1.20	deleted	NAS group 'share-group2'
01/28/2016 05:48:39 PM	FORTIANALYZER9	admin	GUI	172.16.1.10	added	new NAS share 'report-share'

Figure 9

Log Considered:

```
date=2016-01-25 time=12:55:10 log_id=0100000031 type=event subtype=config pri=information
device_id=FL800B3908000420 user=system-built-in ui=GUI(172.16.1.10) action=config msg=\"User
'systembuilt-in' changed the NAS user 'share-user3' settings
```

- **FortiAnalyzer – IPsec activity** – This report provides information related to IPsec VPN connections which includes columns such as Local IP, Local Port, Remote IP, Remote Port, Outbound Interface, Action, Initiated, Mode, Direction, and Status.

LogTime	Computer	Local IP	Local Port	Remote IP	Remote Port	Outbound Interface	Action	Initiated	Mode	Direction	Status
01/27/2016 03:52:48 PM	FORTIANALYZER5	172.16.1.20	500	172.16.1.30	500	vpn_tunnel=Gateway_Firewall	negotiate	remote	quick	outbound	success
01/27/2016 03:55:48 PM	FORTIANALYZER5	172.16.1.20	500	172.16.1.30	500	vpn_tunnel=Gateway_Firewall	negotiate	remote	aggressive	Inbound	success
01/29/2016 12:11:30 PM	FORTIANALYZER5	172.16.1.20	500	172.16.1.30	500	vpn_tunnel=Gateway_Firewall	install_sa				
01/27/2016 03:10:12 PM	FORTIANALYZER5	172.16.1.20	500	172.16.1.30	500	vpn_tunnel=Gateway_Firewall	negotiate	remote	quick	outbound	success
01/27/2016 03:30:20 PM	FORTIANALYZER5	172.16.1.20	500	172.16.1.30	500	vpn_tunnel=Gateway_Firewall	negotiate	remote	aggressive	Inbound	success
01/29/2016 12:40:22 PM	FORTIANALYZER5	172.16.1.20	500	172.16.1.30	500	vpn_tunnel=Gateway_Firewall	install_sa				

Figure 10

Log Considered:

```
date=2009-12-23 time=05:41:56 log_id=0101000000 type=event subtype=ipsec pri=notice
device_id=FL800B3908000420 loc_ip=172.16.1.20 loc_port=500 rem_ip=172.16.1.30 rem_port=500
out_if=vpn_tunnel=Gateway_Firewall action=negotiate init=remote mode=aggressive stage=1
dir=outbound status=success msg="Responder: sent 172.16.1.30 aggressive mode message #1
(OK)"
```

- **FortiAnalyzer – Resource Monitoring** – This report provides information related to resource usage which includes columns such as Status and Message Details.

LogTime	Computer	Status	Message Details
01/28/2016 04:42:35 PM	FORTIANALYZER6	success	Network Interface (port 1) is up
01/28/2016 04:50:35 PM	FORTIANALYZER6	failure	Killing process httpsd due to high memory usage [RSS:271044 KB, VM:730440 KB].

Figure 11

Log Considered:

```
date=2009-11-27 time=09:15:57 log_id=0106000037 type=event subtype=system pri=warning
device_id=FLG8002704000076 user=system ui=system action=monitor status=success
msg="Network Interfac(port 1) is up"
```

- **FortiAnalyzer – User management** – This report provides information related to user profile accessed, deleted, changed which includes columns such as User Name, User Interface, Source IP, Status and Message Details.

LogTime	Computer	User Name	User Interface	Source IP	Status	Message Details
02/23/2016 10:43:09 AM	FORTIANALYZER29	admin	GUI	172.16.1.20	deleted	access profile reports_only2
02/23/2016 10:45:29 AM	FORTIANALYZER29	admin1	GUI	172.16.21	changed	password of admin user admin4
02/23/2016 10:47:32 AM	FORTIANALYZER29	admin	GUI	172.16.1.20	deleted	an admin user admin4
02/23/2016 10:49:40 AM	FORTIANALYZER29	admin	GUI	172.16.1.20	added	an admin user admin3
02/23/2016 10:51:09 AM	FORTIANALYZER29	admin	jsconsole		changed	the system max concurrent users

Figure 12

Log Considered:

```
date=2010-02-17 time=12:01:19 log_id=0100000000 type=event subtype=config pri=notice
device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin'
deleted access profile reports_only2 from GUI(172.16.1.20)"
```

- **FortiAnalyzer – Device management** – This report provides information related to device added, deleted, rename, changed, registered and unregistered details which includes columns such as User Name, User Interface, Source IP, Action, Status and Message Details.

LogTime	Computer	User Name	User Interface	Source IP	Action	Status	Message Details
01/29/2016 06:47:11 PM	FORTIANALYZER40	admin	console		config		User 'admin' changed device 'FGT- 400-Floor2' settings
01/29/2016 06:47:11 PM	FORTIANALYZER400	admin	GUI	172.16.1.20	config		Device FortiWeb-1000B added
01/29/2016 06:47:11 PM	FORTIANALYZER40	system	system		config		The FortiAnalyzer added new device 'FG200A3907550170' automatically.
01/29/2016 06:47:11 PM	FORTIANALYZER40	system	oftp		config		User 'system' renamed device 'FG36002804033057' to 'FortiGate-3600-Floor2'
01/29/2016 06:47:11 PM	FORTIANALYZER40	system	fortilogd		config		A higher end FortiAnalyzer is recommended for this model of FortiGate(FG36002804033057)
01/29/2016 06:47:12 PM	FORTIANALYZER40	system	system		add_device	success	Log device FMG3KB3F09000109 is registered automatically.

Figure 13

Log Considered:

```
date=2010-01-05 time=14:24:39 log_id=0106000028 type=event subtype=system
pri=warning device_id=FL800B3908000420 user=system ui=system action=add_device
status=success msg="Log device FMG3KB3F09000109 is registered automatically."
```

- **FortiAnalyzer – System management** – This report provides information related to bootup, downgraded, migration, delete log and delete archive which includes columns such as User Name, User Interface, Source IP, Action, Status and Message details.

LogTime	Computer	User Name	User Interface	Source IP	Action	Status	Message Details
02/09/2016 12:04:42 PM	FORTIANALYZER	system	system		RAID	success	md: md0: raid array is not clean -- starting background reconstruction
02/09/2016 12:20:30 PM	FORTIANALYZER	system	system		bootup	success	The configured secondary DNS server is not reachable. A valid DNS server is required for resolving IP addresses to hostnames in reports.
02/09/2016 12:25:42 PM	FORTIANALYZER	admin	console		downgrade	success	Firmware has been downgraded.
02/09/2016 12:40:20 PM	FORTIANALYZER	admin	ssh	172.16.1.20	unknown	success	'admin' is shutting down the system from 'ssh(172.16.1.20)'

Figure 14

Log Considered:

```
date=2009-05-28 time=07:51:36 log_id=0106000001 type=event subtype=system pri=alert
device_id=FLG8002704000076 user=system ui=system action=bootup status=success
msg="The configured secondary DNS server is not reachable. A valid DNS server is required for
resolving IP addresses to hostnames in reports."
```

Dashboard

FortiAnalyzer- Administrator logon activity: This dashboard gives the information about user login, user logout and user exit from the specific user interface and source IP.

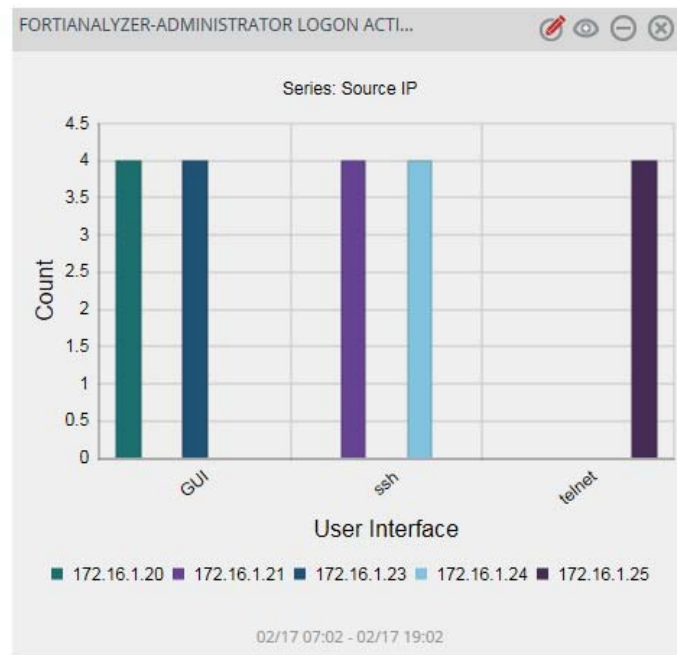


Figure 15

Import Knowledge Pack into EventTracker


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



Figure 16

Import **Categories, Alerts, and Reports** as given below.

Import Category

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

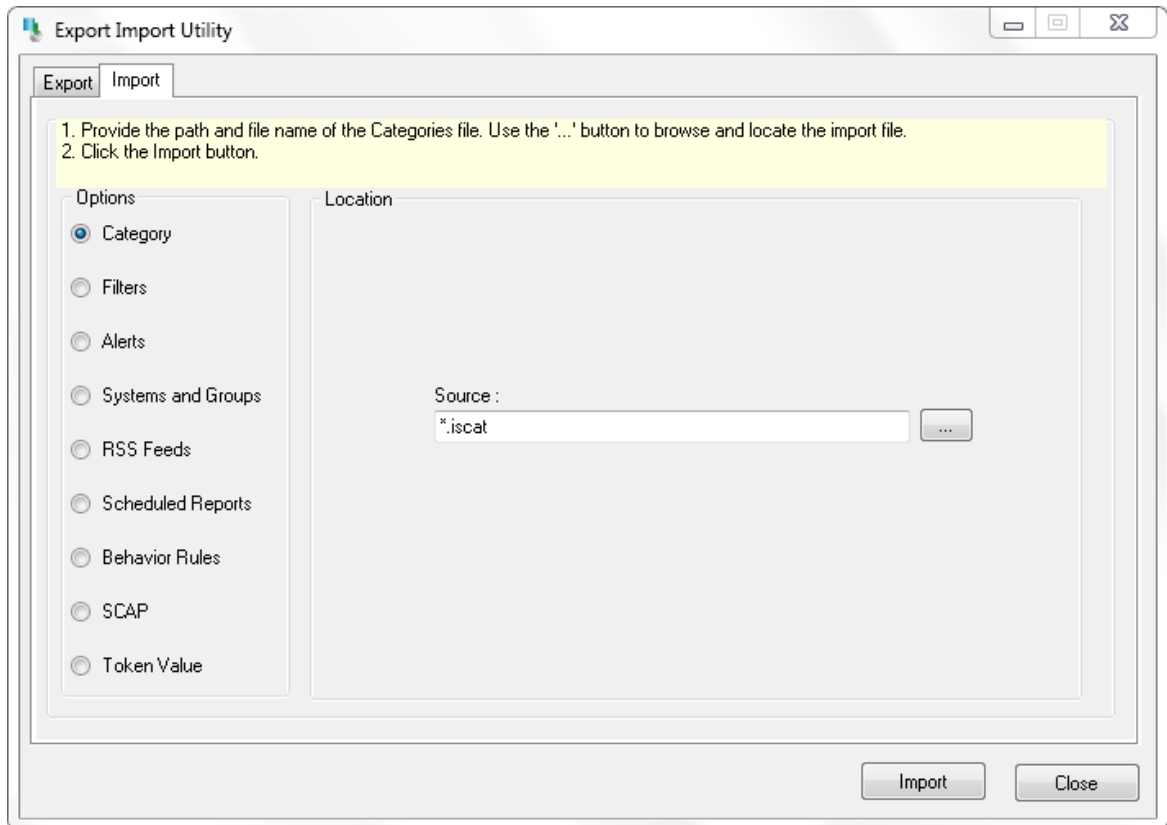


Figure 17

2. Locate **All FortiAnalyzer group categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

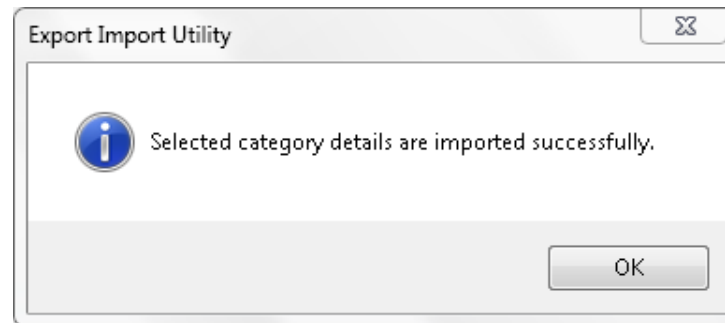



Figure 18

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

Import Alerts

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

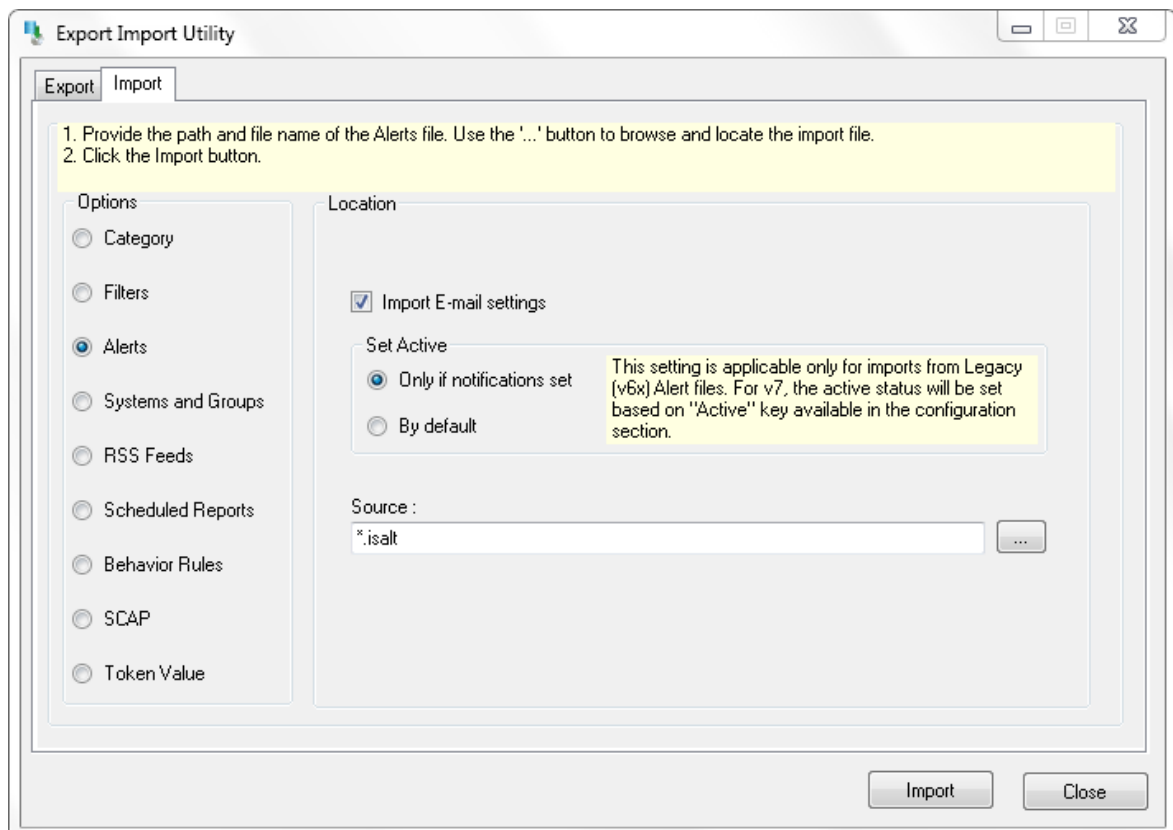


Figure 19

2. Locate **All FortiAnalyzer group alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

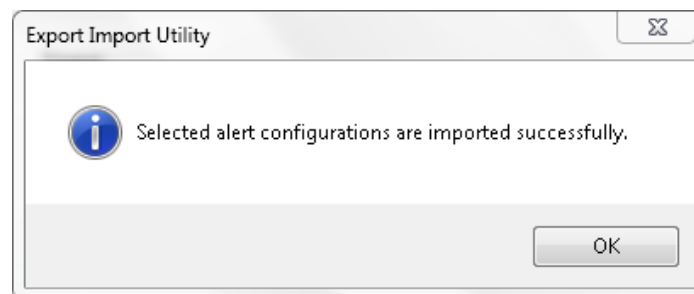



Figure 20

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

Import Flex Reports

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

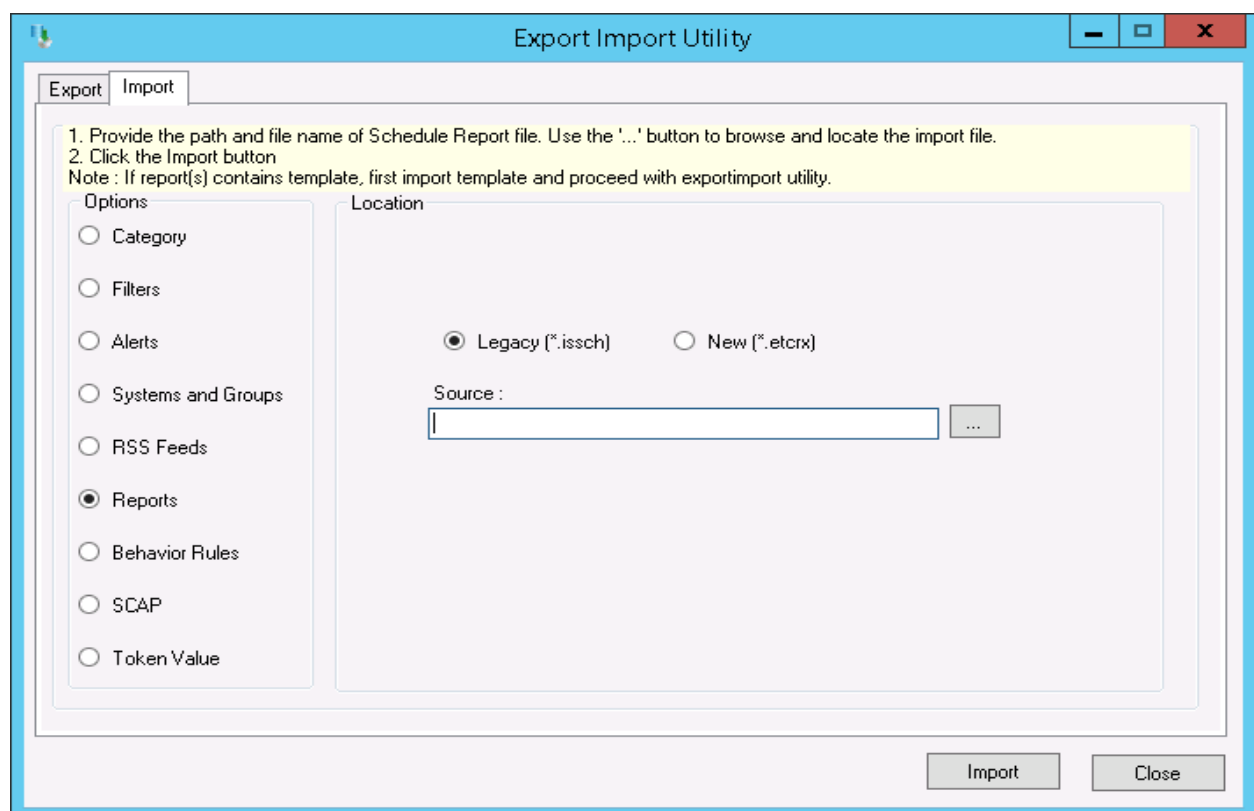


Figure 21

2. Locate the FortiAnalyzer.issch file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports.

EventTracker displays success message.

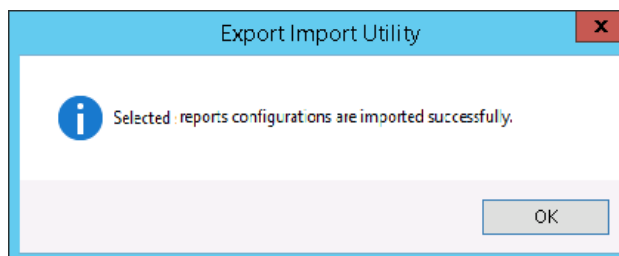



Figure 22

Import Parsing Rules

1. Click **Token Value** option, and then click the browse  button.
2. Locate **All FortiAnalyzer group of tokens.istoken** file, and then click the **Open** button.

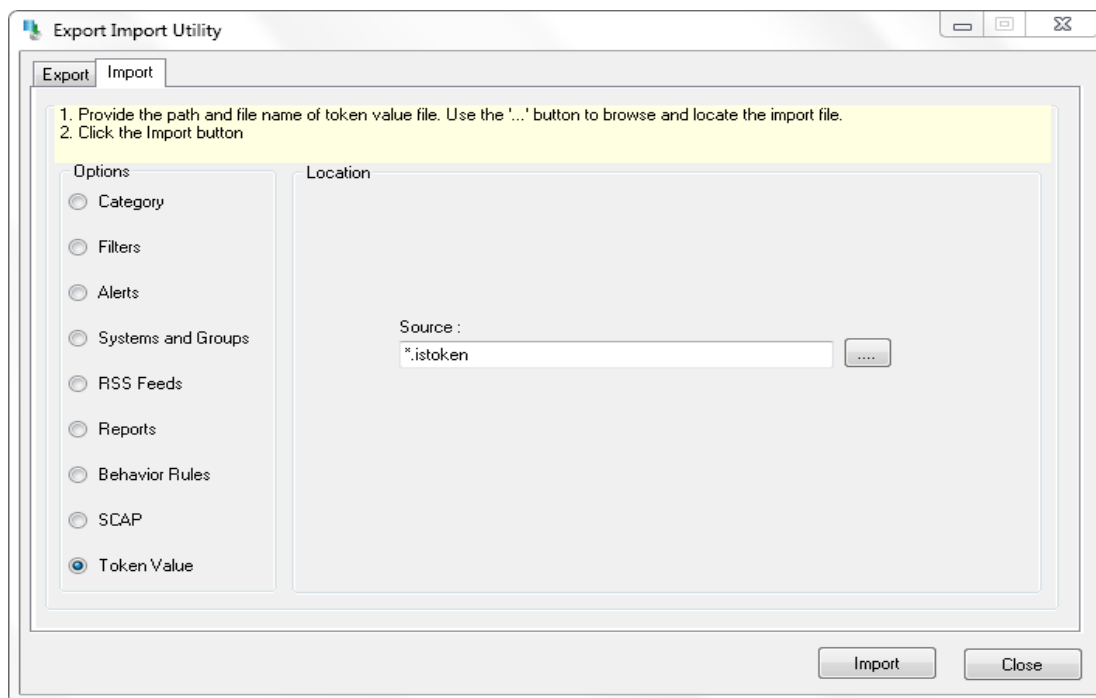


Figure 23

3. To import token value, click the **Import** button.

EventTracker displays success message.

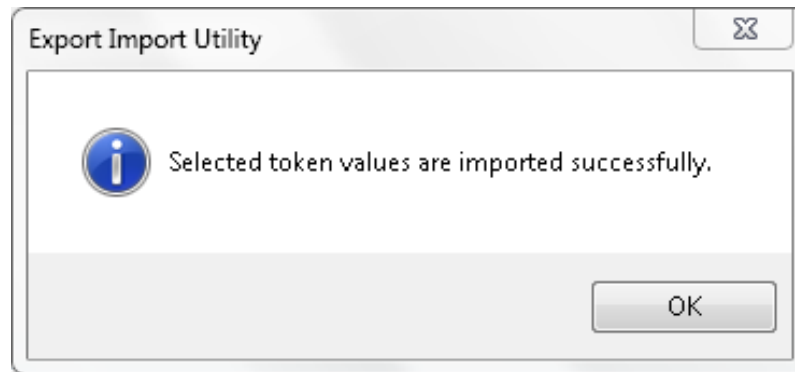



Figure 24

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

Import Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  'Import' option.

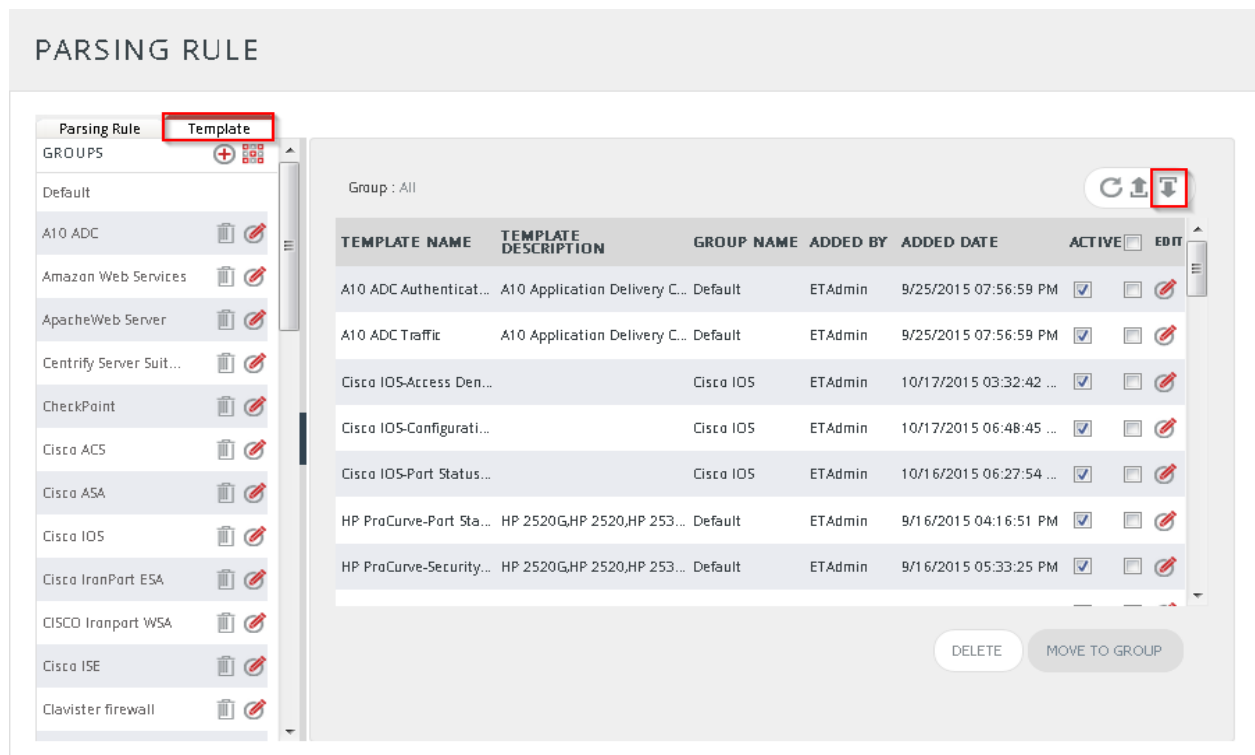


Figure 25

3. Click on **Browse** button.

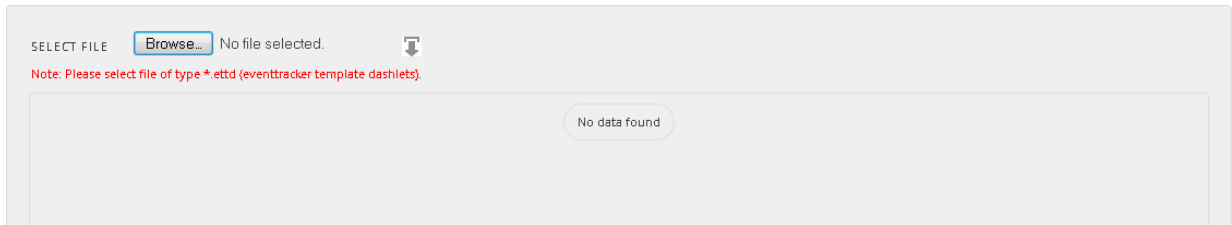


Figure 26

4. Locate All **FortiAnalyzer** token **template.ettd** file, and then click the **Open** button.



Figure 27

5. Now select the check box and then click on **Import** option. EventTracker displays success message.

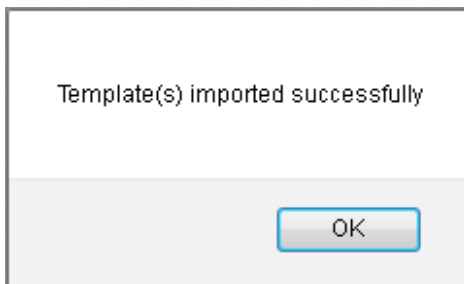


Figure 28

6. Click on **OK** button.

Import Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on **Import** option.

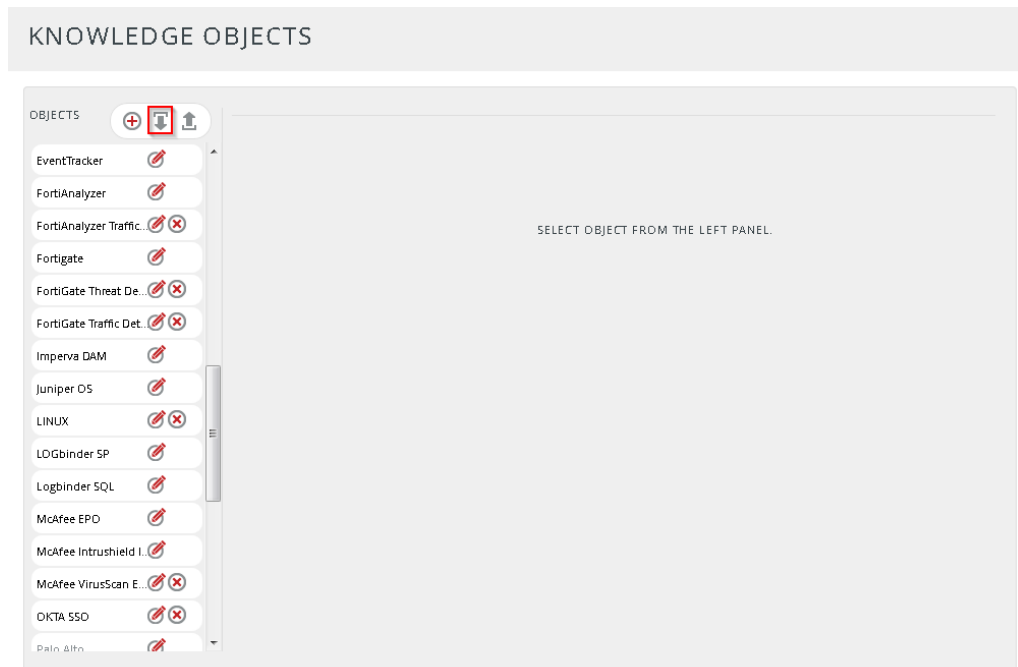


Figure 29

3. In **IMPORT** pane click on **Browse** button.

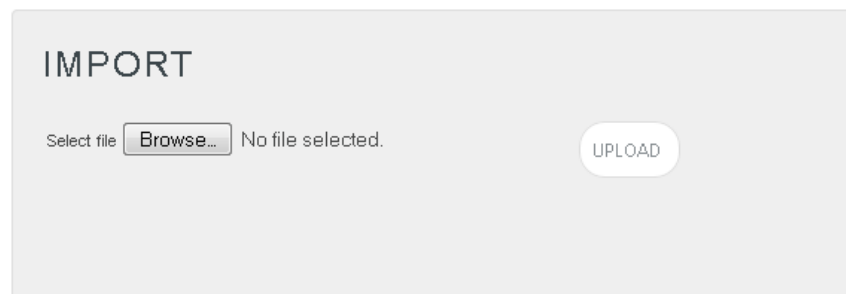


Figure 30

4. Locate **FortiAnalyzer KO.etko** file, and then click the **UPLOAD** button.

IMPORT

Select file No file selected.

<input type="checkbox"/>	OBJECT NAME	APPLIES TO
<input checked="" type="checkbox"/>	FortiAnalyzer Traffic Details	FortiAnalyzer 5.0.0 & later

Figure 31

- Now select the check box and then click on '**MERGE**' option.

EventTracker displays success message.

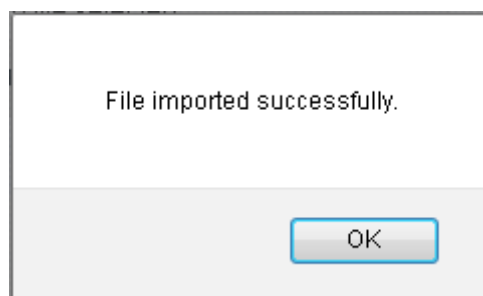


Figure 32

- Click on **OK** button.

Verify Knowledge Pack in EventTracker

Verify Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. To view the imported categories, in the **Category Tree**, expand **FortiAnalyzer** group folder.

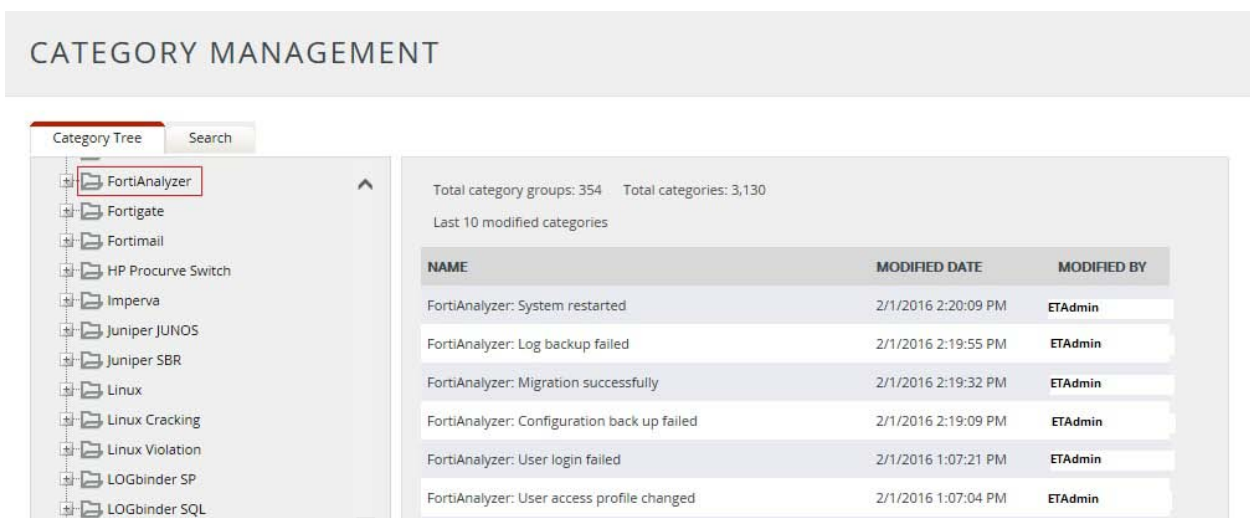



Figure 33

Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type '**FortiAnalyzer**', and then click the  **'search'** button.

Alert Management page will display all the imported alerts.

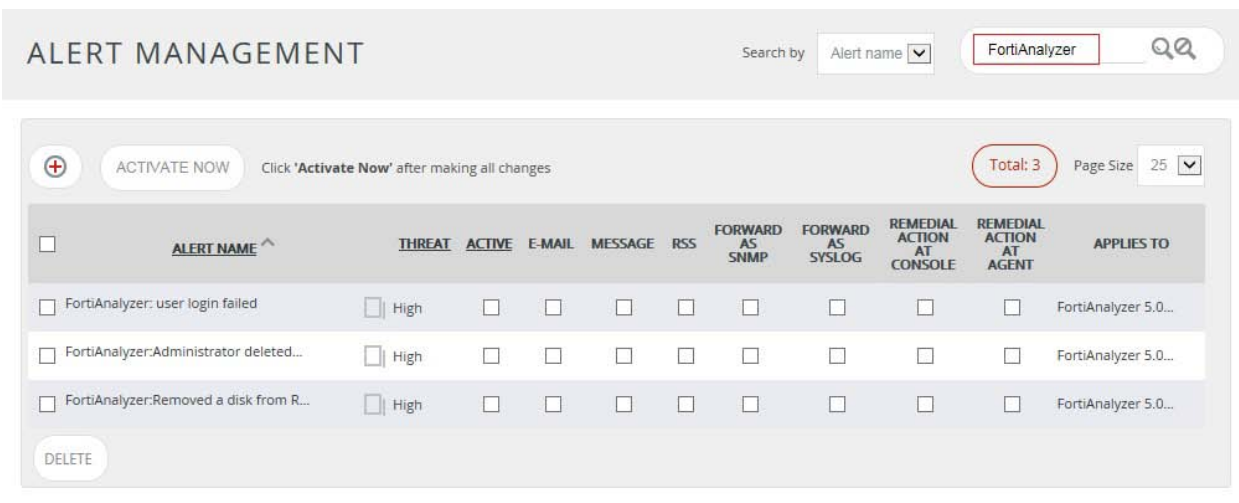


Figure 34

- To activate the imported alerts, select the respective checkbox in the **Active** column and then click the **Activate Now** button.

EventTracker displays message box.

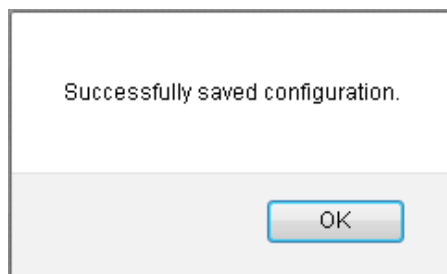


Figure 35

- Click **OK**.

Verify Parsing Rules

- Logon to **EventTracker Enterprise**.
- Click the **Admin** menu, and then click **Parsing Rules** from the dropdown options.
- In **Token Value Group Tree** to view imported token values, scroll down and click **FortiAnalyzer group** folder.

Token values are displayed in the token value pane.

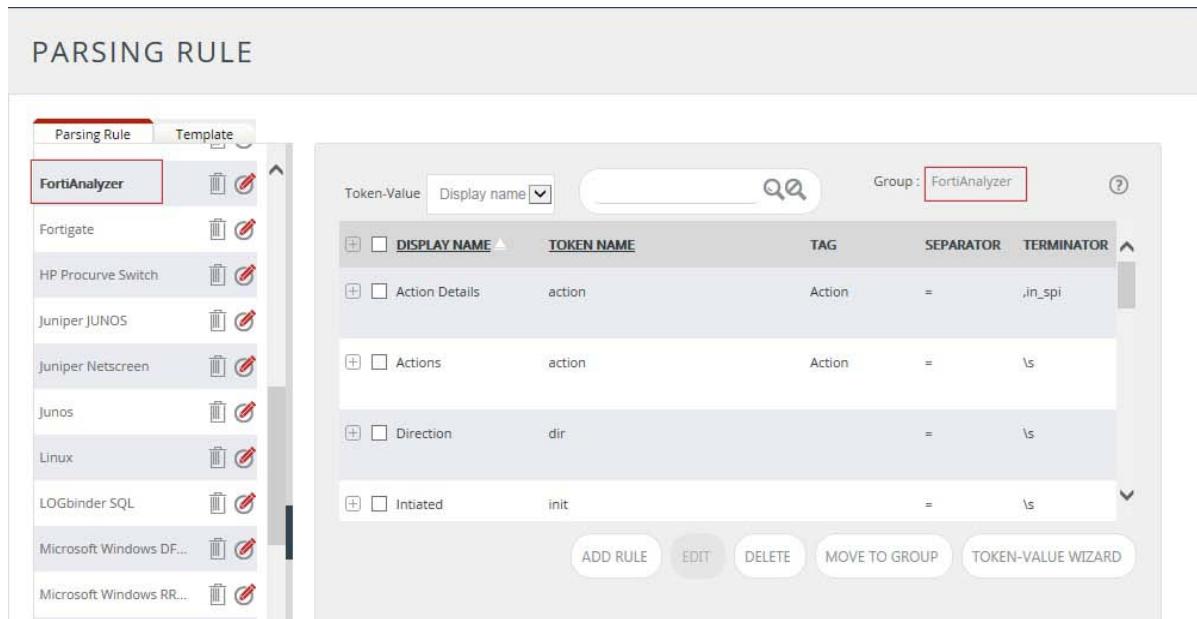


Figure 36

Verify Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab.
3. In **Token Value Group Tree** to view imported token values, scroll down and click **FortiAnalyzer** group folder.

Imported token template is displayed in the template pane.

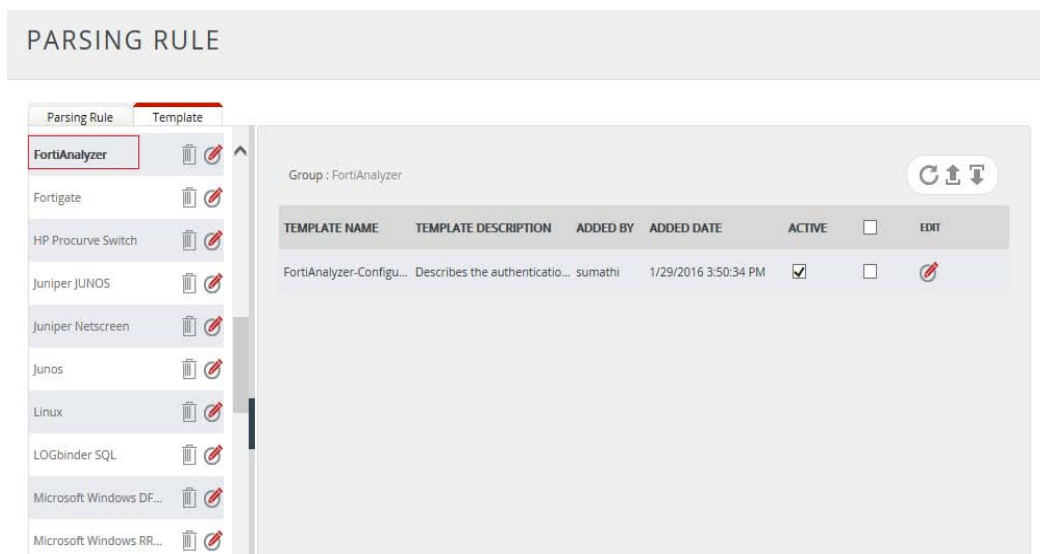


Figure 37

Verify Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Scroll down and select **FortiAnalyzer** in **Objects** pane.

Imported FortiAnalyzer object details are shown.

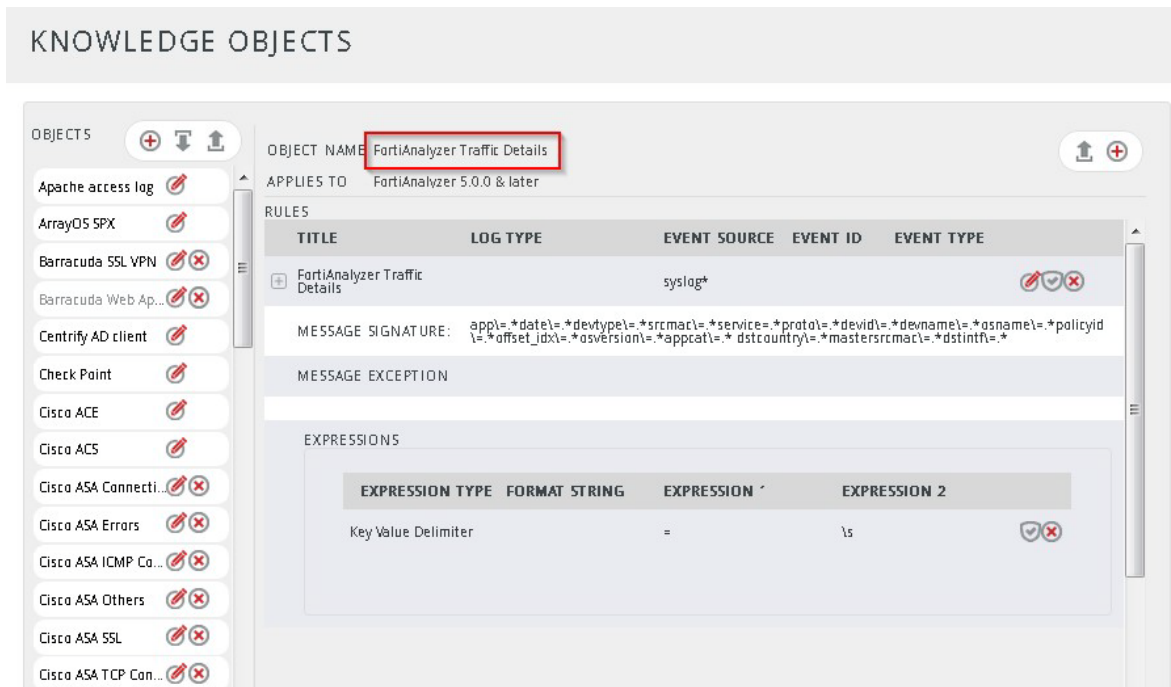


Figure 38

Verify 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 flex reports, scroll down and click FortiAnalyzer group folder.

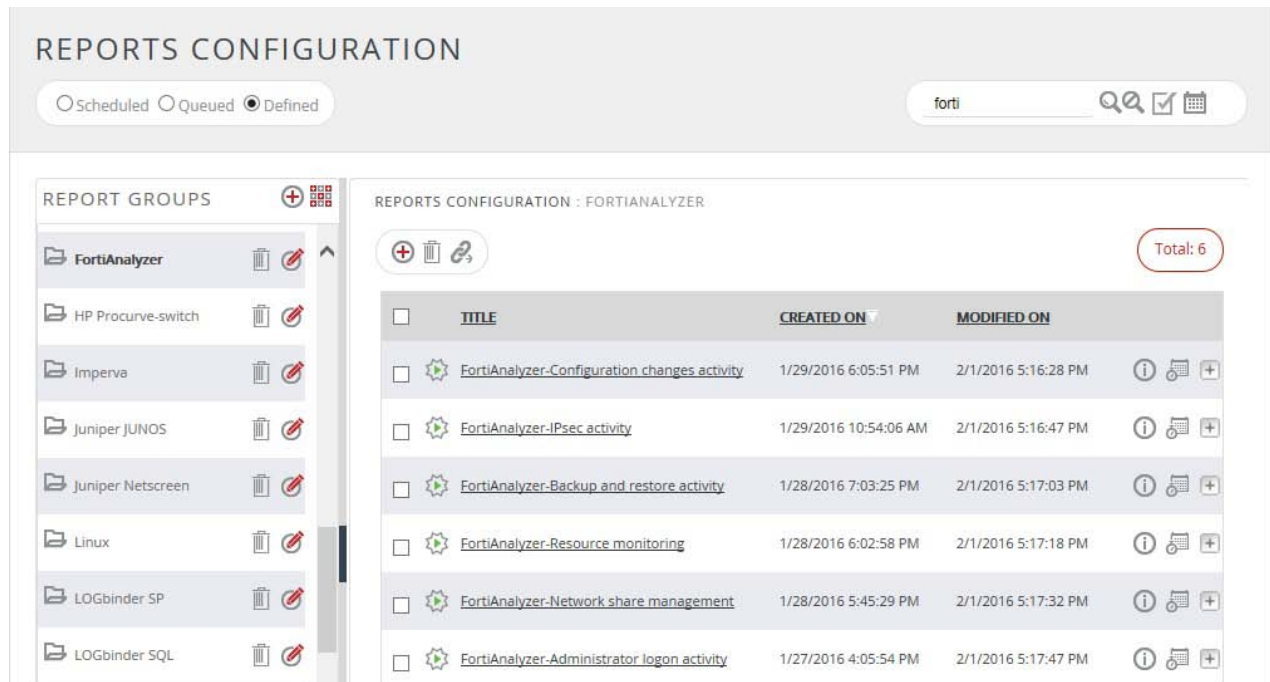


Figure 39

Create Dashboards in EventTracker

Schedule Reports

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

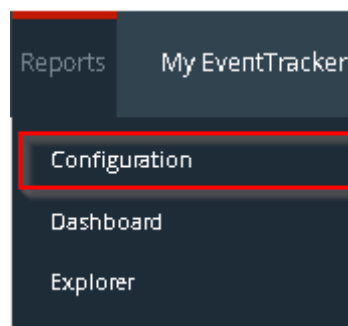



Figure 40

1. Navigate to **Reports>Configuration**.

The screenshot shows the 'REPORTS CONFIGURATION' page in EventTracker. On the left, under 'REPORT GROUPS', 'FortiAnalyzer' is selected and highlighted with a red box. The main area, titled 'REPORTS CONFIGURATION : FORTIANALYZER', shows a table of configured reports. The table has columns for 'TITLE', 'CREATED ON', and 'MODIFIED ON'. There are 6 reports listed, each with a checkbox, a gear icon, and a plus icon. A 'Total: 6' badge is in the top right of the table area. At the top of the page, there are radio buttons for 'Scheduled', 'Queued', and 'Defined' (which is selected), and a search bar with the text 'forti'.

	TITLE	CREATED ON	MODIFIED ON
<input type="checkbox"/>	FortiAnalyzer-Configuration changes activity	1/29/2016 6:05:51 PM	2/1/2016 5:16:28 PM
<input type="checkbox"/>	FortiAnalyzer-IPsec activity	1/29/2016 10:54:06 AM	2/1/2016 5:16:47 PM
<input type="checkbox"/>	FortiAnalyzer-Backup and restore activity	1/28/2016 7:03:25 PM	2/1/2016 5:17:03 PM
<input type="checkbox"/>	FortiAnalyzer-Resource monitoring	1/28/2016 6:02:58 PM	2/1/2016 5:17:18 PM
<input type="checkbox"/>	FortiAnalyzer-Network share management	1/28/2016 5:45:29 PM	2/1/2016 5:17:32 PM
<input type="checkbox"/>	FortiAnalyzer-Administrator logon activity	1/27/2016 4:05:54 PM	2/1/2016 5:17:47 PM

Figure 41

3. Select **FortiAnalyzer** in report groups. Check **defined** dialog box.
4. Click on 'schedule'  icon to plan a report for later execution.

REPORT WIZARD
TITLE: FORTIANALYZER-ADMINISTRATOR LOGON ACTIVITY
LOGS

CANCEL < BACK NEXT >

Review cost details and configure the publishing options. Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:01:32(HH:MM:SS)
Number of cab(s) to be processed: 31
Available disk space: 260 GB
Required disk space: 50 MB

☐ Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
☒ Deliver results via E-mail
☐ Notify results via E-mail

To E-mail: [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:

Show in:

☒ Persist data in Eventvault Explorer

Figure 42

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault Explorer** box.

REPORT WIZARD
TITLE: FORTIANALYZER-ADMINISTRATOR LOGON ACTIVITY
DATA PERSIST DETAIL

CANCEL < BACK NEXT >

Select columns to persist Step 9 of 10

RETENTION SETTING

Retention period: days ⓘ

☐ Persist in database only [Reports will not be published and will only be stored in the respective database]

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Computer	<input checked="" type="checkbox"/>
Event Description	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
User Interface	<input checked="" type="checkbox"/>
Action	<input checked="" type="checkbox"/>
Status	<input checked="" type="checkbox"/>

Figure 43

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

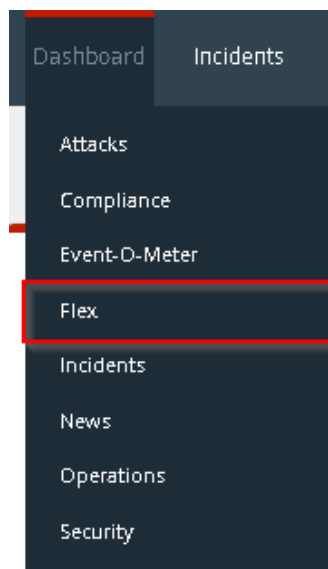


Figure 44

3. Navigate to **Dashboard>Flex**.

Flex Dashboard pane is shown.

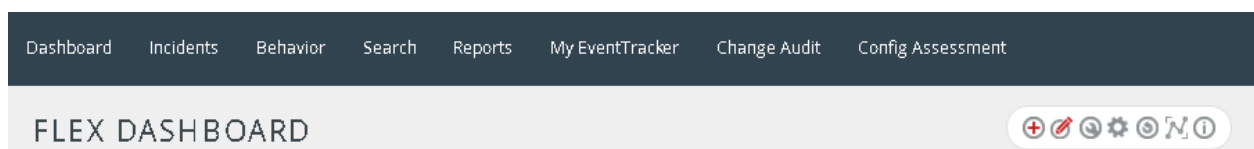

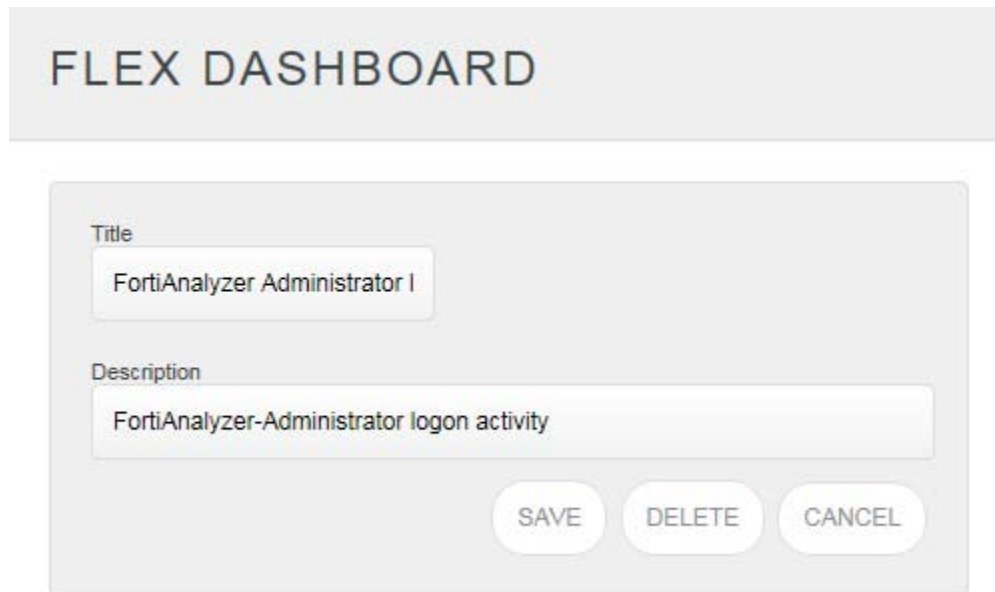


Figure 45

4. Click  to add a new dashboard.

Flex Dashboard configuration pane is shown.



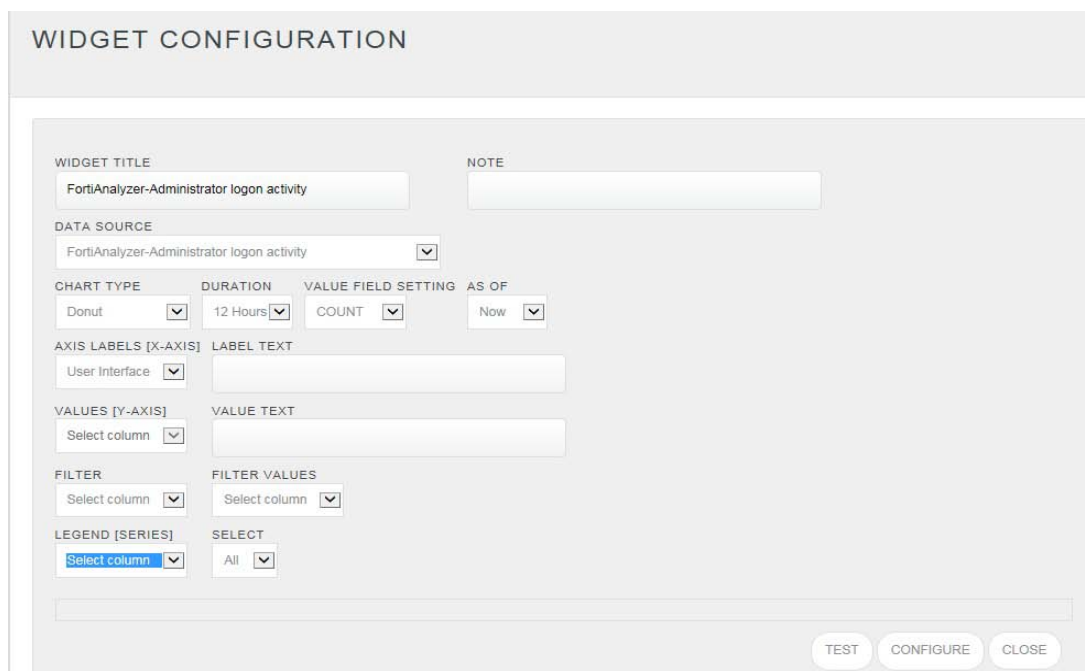
The image shows a configuration pane titled "FLEX DASHBOARD". It contains two text input fields: "Title" with the value "FortiAnalyzer Administrator I" and "Description" with the value "FortiAnalyzer-Administrator logon activity". At the bottom right, there are three buttons: "SAVE", "DELETE", and "CANCEL".

Figure 46

5. Fill fitting title and description and click **Save** button.

6. Click the icon  to configure a new Flex dashlet.

Widget configuration pane is shown.



The image shows a "WIDGET CONFIGURATION" pane. It contains several sections with dropdown menus and text input fields:

- WIDGET TITLE:** FortiAnalyzer-Administrator logon activity
- NOTE:** (empty text input field)
- DATA SOURCE:** FortiAnalyzer-Administrator logon activity
- CHART TYPE:** Donut
- DURATION:** 12 Hours
- VALUE FIELD SETTING:** COUNT
- AS OF:** Now
- AXIS LABELS [X-AXIS]:** User Interface
- LABEL TEXT:** (empty text input field)
- VALUES [Y-AXIS]:** Select column
- VALUE TEXT:** (empty text input field)
- FILTER:** Select column
- FILTER VALUES:** Select column
- LEGEND [SERIES]:** Select column
- SELECT:** All

At the bottom right, there are three buttons: "TEST", "CONFIGURE", and "CLOSE".

Figure 47

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.

Evaluated chart is shown.

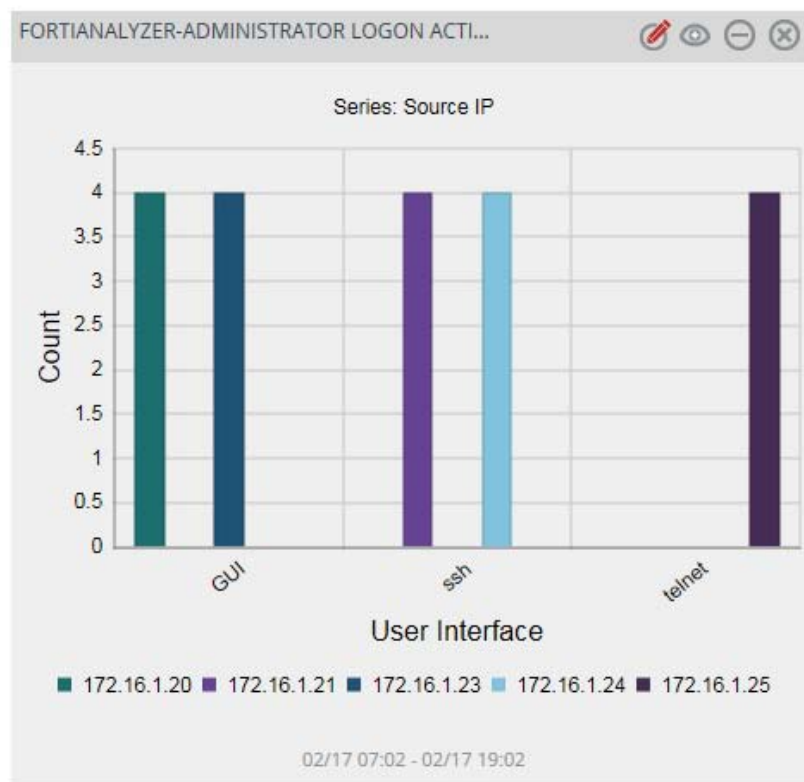


Figure 48

16. If satisfied, click **Configure** button.

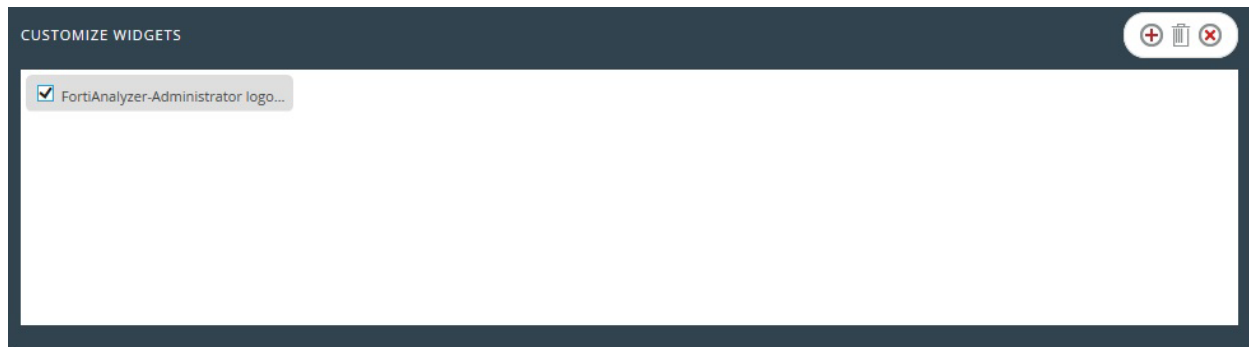



Figure 49

17. Click 'customize'  to locate and choose created dashlet.

18. Click  to add dashlet to earlier created dashboard.

NOTE: For Version 4.0 log field Priority is pri for Version 5.0 pri is replaced with level. For more information please go through the link: <http://docs.fortinet.com/d/log-message-reference>