Netsurion™ | EventTracker

Integrate FortiMail

EventTracker v9.0 and Above

Publication Date: May 24, 2019

Abstract

This guide provides instructions to configure Fortinet FortiMail to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor the emails.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 9.x and later, and FortiMail v6.0 and later.

Audience

IT admins, FortiMail administrators and EventTracker users who wish to forward logs to EventTracker manager and monitor events using EventTracker Enterprise.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2019 EventTracker Security LLC. 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
Configure FortiMail Syslog 3
EventTracker Knowledge Pack (KP) 4
Alert 4
Reports 4
Dashboards 6
Import Knowledge Pack into EventTracker 9
Alerts 9
Knowledge Objects 10
Token Template 12
Flex Reports 13
Category 15
Dashlets 17
Verify Knowledge Pack in EventTracker 20
Category 20
Alerts 21
Knowledge Object 23
Flex Reports 23
Dashlets 24
Token Template 25

Overview

Fortinet FortiMail is an email security gateway product that monitors email messages on behalf of an organization to identify messages that contain malicious content, including spam, malware, and phishing attempts.

FortiMail can be integrated with EventTracker using Syslog. With the help of FortiMail KP items, we can monitor the spam, and virus happening on mail servers and trigger the alert whenever any virus and spam detected. EventTracker dashboard will help you to visualize the malicious activities happening mail servers. It can even create the report which helps to collection malicious activities happening on mail servers on time bases which help you to review the malicious activities. EventTracker CIM will help you to correlate the malicious activities with another log source like a virus, spam events, etc.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **FortiMail v6.0** or the latest version should be installed.

Configure FortiMail Syslog

1. Go to Log and Report → Log Settings → Remote Log Settings.
2. Toggle Enable for your preferred profile.
3. Go to Log and Report → Log Settings → Remote Log Settings.
4. The Remote Log Settings tab is displayed.
5. Select **New** to create a new entry or double-click an existing entry to modify it.
6. Select **Enable** to allow logging to a remote host.
7. Enter a profile name and the IP address of the EventTracker.
8. Enter the **514** in the port section.
9. Select the **severity** level that a log message must equal or exceed to be recorded and stored from the Level dropdown menu.
10. Select the facility identifier that the FortiMail unit uses to identify itself from the Facility dropdown menu.
11. Expand the **Logging Policy Configuration** and enable the types of logs you want to monitor. (recommended: Select all)
12. Select **Create**.

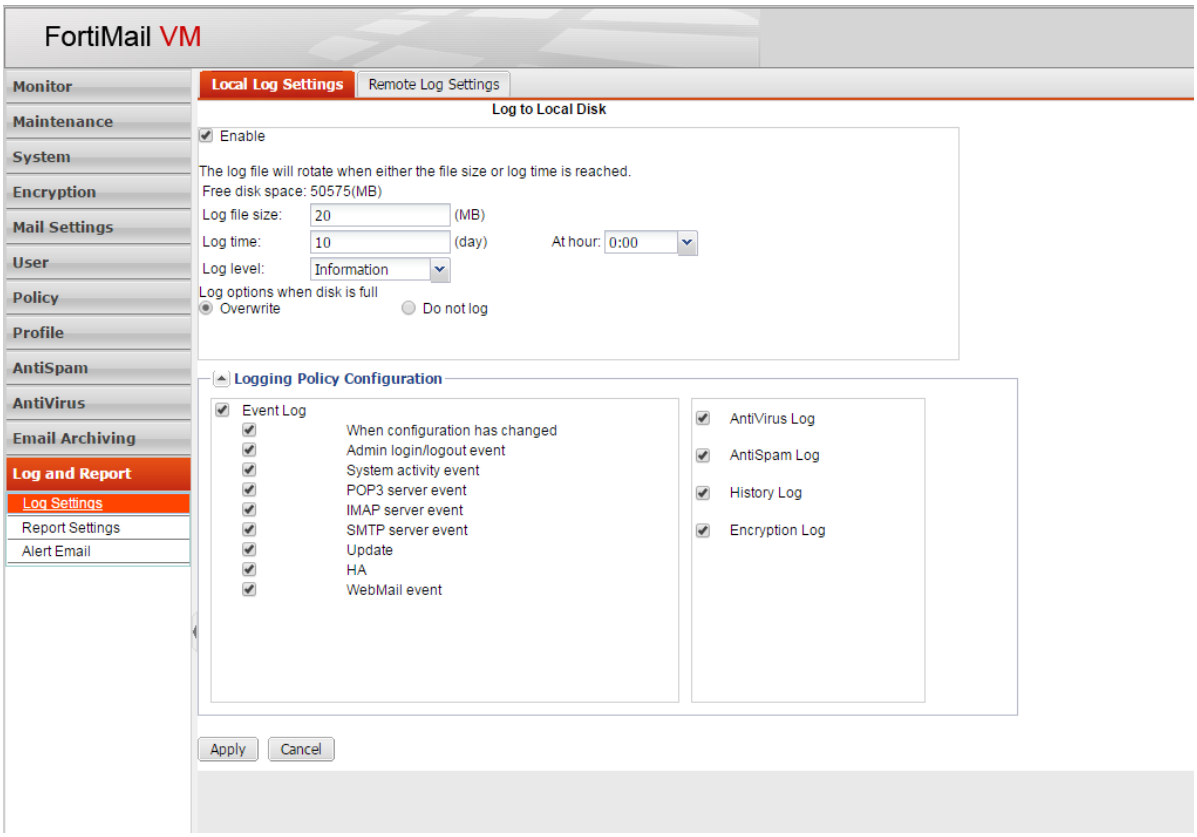

Figure 1

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 v9.x and later to support FortiMail.

Alert

- **FortiMail: Virus detected –** This alert will trigger whenever the virus is detected in the email attachments.
- **FortiMail: Spam detected** – This alert will trigger whenever FortiMail detects spam email.
- **FortiMail: User login failure –** This alert will trigger whenever the user login fails.

Reports

- **FortiMail – Virus detected –** This report provides information related to FortiMail detecting malicious attachments in email.

LogTime	Threat Type	Priority	Device ID	Domain Name	Email From Address	Email To Address	Log ID	Session ID	SubType	Message
05/20/2019 08:19:52 PM	virus	information	FEVM000000000000	"domain.com [2.2.2.2] (may be forged)"	"johndoe3@domain.com"	"johndoe4@domain.com"	0000000000	"u4CFFtJ2019809-u4CFFtJ3019809"	infected	"attachment document doc.zip contains suspicious content"
05/20/2019 08:19:52 PM	virus	information	FEVM000000000000	"domain.com [1.1.1.1] (may be forged)"	"johndoe@domain.com"	"johndoe2@domain.fr"	0000000000	"u4CFFNt4019700-u4CFFNt5019710"	infected	"archive bomb detected in attachment(s)"
05/20/2019 08:19:52 PM	virus	information	FEVM000000000000	"[3.3.3.3]"	"johndoe5@domain.com"	"johndoe5@domain.com"	0000000000	"u4CFnWUE026721-u4CFnWUF026742"	infected	"The file 839.zip is infected with Malicious_Behavior.VEX.99."
05/20/2019 08:21:34 PM	virus	information	FEVM000000000000	"[3.3.3.3]"	"johndoe5@domain.com"	"johndoe5@domain.com"	0000000000	"u4CFnWUE026721-u4CFnWUF026742"	infected	"The file 839.zip is infected with Malicious_Behavior.VEX.99."
05/20/2019 08:21:34 PM	virus	information	FEVM000000000000	"domain.com [2.2.2.2] (may be forged)"	"johndoe3@domain.com"	"johndoe4@domain.com"	0000000000	"u4CFFtJ2019809-u4CFFtJ3019809"	infected	"attachment document doc.zip contains suspicious content"
05/20/2019 08:21:34 PM	virus	information	FEVM000000000000	"domain.com [1.1.1.1] (may be forged)"	"johndoe@domain.com"	"johndoe2@domain.fr"	0000000000	"u4CFFNt4019700-u4CFFNt5019710"	infected	"archive bomb detected in attachment(s)"
05/20/2019 08:21:37 PM	virus	information	FEVM000000000000	"[3.3.3.3]"	"johndoe5@domain.com"	"johndoe5@domain.com"	0000000000	"u4CFnWUE026721-u4CFnWUF026742"	infected	"The file 839.zip is infected with Malicious_Behavior.VEX.99."
05/20/2019 08:21:37 PM	virus	information	FEVM000000000000	"domain.com [1.1.1.1] (may be forged)"	"johndoe@domain.com"	"johndoe2@domain.fr"	0000000000	"u4CFFNt4019700-u4CFFNt5019710"	infected	"archive bomb detected in attachment(s)"
05/20/2019 08:21:37 PM	virus	information	FEVM000000000000	"domain.com [2.2.2.2] (may be forged)"	"johndoe3@domain.com"	"johndoe4@domain.com"	0000000000	"u4CFFtJ2019809-u4CFFtJ3019809"	infected	"attachment document doc.zip contains suspicious content"

Figure 2

- **FortiMail – Spam detected –** This report provides information related to FortiMail detecting malicious URL's in the mail.

LogTime	Log Type	Priority	Client Domain Name	Destination IP Address	Device ID	Email From Address	Email To Address	Log ID	Session ID	Subject Type	Message
05/20/2019 08:19:51 PM	spam	information	"mail.domain.com [1.2.2.1]"	"192.168.4.4"	FEVM000000000000	"johndoe2@business.com"	""	0000000000	"u4CFCo48019219-u4CFCo4A019219"	""	"System White List: 10.11.12. list entry: 10.11.12.14"
05/20/2019 08:19:51 PM	spam	information	"smtp.net [2.1.1.2]"	"192.168.4.4"	FEVM000000000000	"mailreturn@sample.com"	"johndoe3@domain.com"	0000000000	"u4CFCnEU019216-u4CFCnEW019216"	"Weekly Newsletter"	"Detected by ImageSpam che
05/20/2019 08:19:51 PM	spam	information	"smtp.com [4.1.1.4]"	"192.168.4.4"	FEVM000000000000	"johndoe3@domain.com"	""	0000000000	"u4CFCpXn019222-u4CFCpXo019222"	""	"System Black List: johndoe3@domain.com; list er *@*domain.com"
05/20/2019 08:19:51 PM	spam	information	"smtp20.com [1.4.4.1]"	"192.168.4.4"	FEVM000000000000	"bounce@domain.com"	"johndoe4@domain.com"	0000000000	"u4CFCqJV019230-u4CFCqJX019230"	"Offer"	"FortiGuard-AntiSpam identif spam URI: http://domain.com/offer.htm
05/20/2019 08:19:51 PM	spam	information	"mail.domain.com [1.2.3.4]"	"192.168.4.4"	FEVM000000000000	"johndoe@domain.com"	"johndoe@sample.com"	0000000000	"u4CFCkiM019210-u4CFCkiO019210"	"Order"	"johndoe5@domain.com Pers white list: johndoe@domain.c list entry: johndoe@domain.c
05/20/2019 08:21:34 PM	spam	information	"mail.domain.com [1.2.2.1]"	"192.168.4.4"	FEVM000000000000	"johndoe2@business.com"	""	0000000000	"u4CFCo48019219-u4CFCo4A019219"	""	"System White List: 10.11.12. list entry: 10.11.12.14"
05/20/2019 08:21:34 PM	spam	information	"smtp20.com [1.4.4.1]"	"192.168.4.4"	FEVM000000000000	"bounce@domain.com"	"johndoe4@domain.com"	0000000000	"u4CFCqJV019230-u4CFCqJX019230"	"Offer"	"FortiGuard-AntiSpam identif spam URI: http://domain.com/offer.htm
05/20/2019 08:21:34 PM	spam	information	"smtp.net [2.1.1.2]"	"192.168.4.4"	FEVM000000000000	"mailreturn@sample.com"	"johndoe3@domain.com"	0000000000	"u4CFCnEU019216-u4CFCnEW019216"	"Weekly Newsletter"	"Detected by ImageSpam che

Figure 3

- **FortiMail – User login success and login failure -** This report provides information related to the user login success and user login Failure.

LogTime	User Name	User Interface	Log Type	SubType	Priority	Device ID	Action	Log ID	Reason	Status	Message
05/20/2019 08:19:50 PM	webmail	webmail	event	webmail	information	FEVM000000000000	unknown	0000000000		success	"WebMail: User 'user' from 1.2.3.4 logged in"
05/20/2019 08:19:50 PM	admin	GUI(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	none	failure	"User admin login failed from GUI(1.2.3.4)"
05/20/2019 08:19:50 PM	admin	GUI(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	none	success	"User admin login successfully from GUI(1.2.3.4)"
05/20/2019 08:19:50 PM	admin	SSH(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	name_invalid	failure	"User admin login failed from SSH(1.2.3.4)"
05/20/2019 08:19:50 PM	admin	SSH(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	none	success	"User admin login successfully from SSH(1.2.3.4)"
05/20/2019 08:19:50 PM	webmail	webmail	event	webmail	information	FEVM000000000000	unknown	0000000000		failure	"WebMail: Login for 'user' from 1.2.3.4 failed"
05/20/2019 08:21:33 PM	webmail	webmail	event	webmail	information	FEVM000000000000	unknown	0000000000		failure	"WebMail: Login for 'user' from 1.2.3.4 failed"
05/20/2019 08:21:33 PM	admin	SSH(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	none	success	"User admin login successfully from SSH(1.2.3.4)"
05/20/2019 08:21:33 PM	admin	SSH(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	name_invalid	failure	"User admin login failed from SSH(1.2.3.4)"
05/20/2019 08:21:33 PM	admin	GUI(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	none	success	"User admin login successfully from GUI(1.2.3.4)"
05/20/2019 08:21:33 PM	admin	GUI(1.2.3.4)	event	admin	information	FEVM000000000000	login	0000000000	none	failure	"User admin login failed from GUI(1.2.3.4)"

Figure 4

- **FortiMail – Encryption detail -** This report provides information related to the encrypted emails for the secure reading.

LogTime	Log Type	Device ID	Priority	Email From Address	Session ID	Email Subject	Log ID	Message ID	Message
05/20/2019 08:19:51 PM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/20/2019 08:21:34 PM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/20/2019 08:21:36 PM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/20/2019 08:21:38 PM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/21/2019 10:47:34 AM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/21/2019 10:47:41 AM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/21/2019 10:57:54 AM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/21/2019 11:03:21 AM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message
05/21/2019 11:03:24 AM	encrypt	FEVM000000000000	information	'johndoe2@domain.com'	"q79EiV8S007017-q79EiV8T0070170001480"	'ppt file"'	0000000000	'q79EiV8S007017-q79EiV8T0070170001480'	"User johndoe@domain.com read secure message

Figure 5

- **FortiMail – Email filter –** This report provides information related to user-created filters for detecting malicious activities.

LogTime	Log Type	Destination IP Address	Client Domain Name	Device ID	Domain Name	Email From Address	Email To Address	Log ID	Mailer	Policy ID	Priority	Session ID	Spam Classifier
05/20/2019 08:19:50 PM	statistics	"192.168.1.1"	"mail.test.com [1.2.3.4]"	FEVM000000000000	"domain.com"	"johndoe@mail.com"	"johndoe2@domain.com"	0000000000	"mta"	"0:1:4"	information	"u4CFCkiM019219-u4CFCkiO019219"	"User White"
05/20/2019 08:19:51 PM	statistics	"192.168.1.1"	"mail.test.com [1.2.3.4]"	FEVM000000000000	"domain.com"	"johndoe@mail.com"	"johndoe2@domain.com"	0000000000	"mta"	"0:1:4"	information	"u4CFCkiM019219-u4CFCkiO019219"	"User White"
05/20/2019 08:19:51 PM	statistics	"192.168.1.1"	"test.mail.com [4.3.2.1]"	FEVM000000000000	"domain.com"	"johndoe3@mail.com"	"johndoe4@domain.com"	0000000000	"mta"	"0:1:1"	information	"u4CFCkGR019227-u4CFCkGT019227"	"Not Spam"
05/20/2019 08:19:51 PM	statistics	"192.168.100.100"	"smtp.net [14.14.14.14]"	FEVM000000000000	"domain.fr"	"johndoe8@domain.com"	"johndoe9@domain.fr"	0000000000	"mta"	"0:1:4"	information	"u4CFCvPP019240-u4CFCvPQ019240"	"FortiGuard AntiSpam-IP"
05/20/2019 08:19:51 PM	statistics	"192.168.100.100"	"smtp.com [12.12.12.12]"	FEVM000000000000	"domain.fr"	"johndoe4@domain.com"	"johndoe5@domain.fr"	0000000000	"mta"	"0:1:4"	information	"u4CFCqJV019230-u4CFCqJX019230"	"FortiGuard AntiSpam-IP"
05/20/2019 08:19:51 PM	statistics	"192.168.1.1"	"smtp.net [4.4.4.4]"	FEVM000000000000	"domain.fr"	"mailreturn@sample.fr"	"johndoe8@domain.fr"	0000000000	"mta"	"0:1:4"	information	"u4CFCnEU019226-u4CFCnEW019226"	"Image Spam"
05/20/2019 08:19:51 PM	statistics	"192.168.1.1"	"mail.sample.com [2.2.4.4]"	FEVM000000000000	"domain.com"	"johndoe6@business.fr"	"johndoe7@domain.com"	0000000000	"mta"	"0:1:4"	information	"u4CFCo48019319-u4CFCo4A019319"	"System White"
05/20/2019 08:19:51 PM	statistics	"192.168.1.1"	"sample.mail.com [4.4.2.2]"	FEVM000000000000	"domain.fr"	"johndoe4@newsletter.com"	"johndoe5@domain.fr"	0000000000	"mta"	"0:1:4"	information	"u4CFCmMn019223-u4CFCmMp019223"	"Not Spam"
05/20/2019 08:19:51 PM	statistics	"192.168.1.1"	"sample.mail.com [4.4.2.2]"	FEVM000000000000	"domain.fr"	"johndoe4@newsletter.com"	"johndoe5@domain.fr"	0000000000	"mta"	"0:1:4"	information	"u4CFCmMn019223-u4CFCmMp019223"	"Not Spam"
05/20/2019 08:19:51 PM	statistics	"192.168.100.100"	"internet.com [11.11.11.11]"	FEVM000000000000	"domain.com"	"johndoe2@domain.com"	"johndoe3@domain.com"	0000000000	"mta"	"0:1:4"	information	"u4CFCpXn019222-u4CFCpXo019222"	"System Black"
05/20/2019 08:19:51 PM	statistics	"192.168.100.100"	"smtp.net [10.10.10.10]"	FEVM000000000000	"domain.fr"	"mailreturn@sample.com"	"johndoe@domain.fr"	0000000000	"mta"	"0:1:4"	information	"u4CFCnEU019216-u4CFCnEW019216"	"Image Spam"

Figure 6

Dashboards

- **FortiMail Top 10 Email Spam Detected** – This dashboard shows information about the spam detected in the emails.

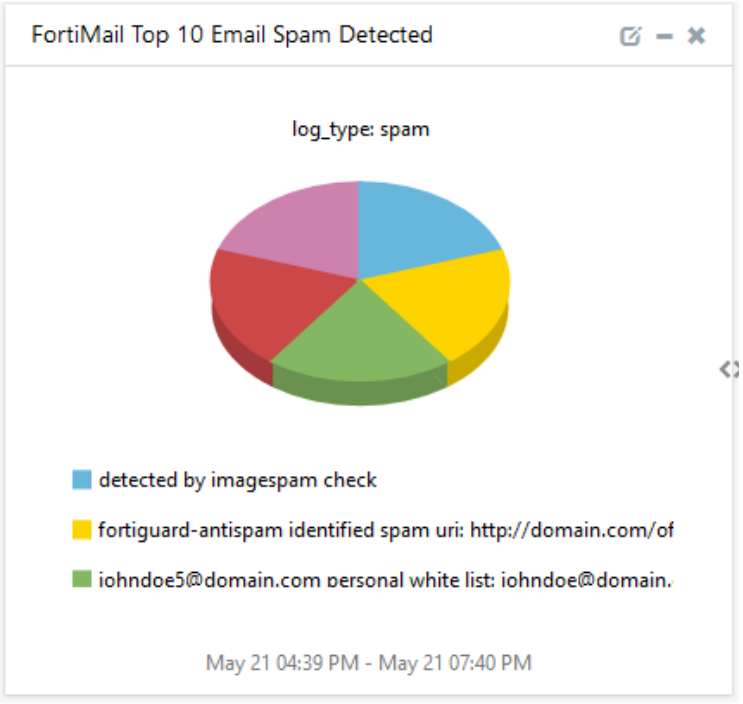

Figure 7

- **FortiMail Top 10 Email Virus Detected** – This dashboard shows information about virus infected in the email attachments.

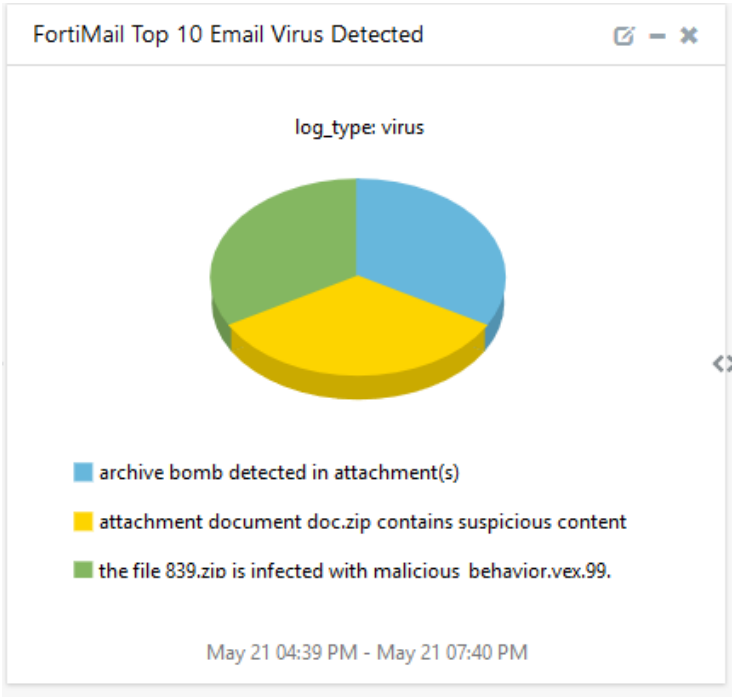

Figure 8

- **FortiMail User Activities** – This dashboard shows information about user login success and user login failure.

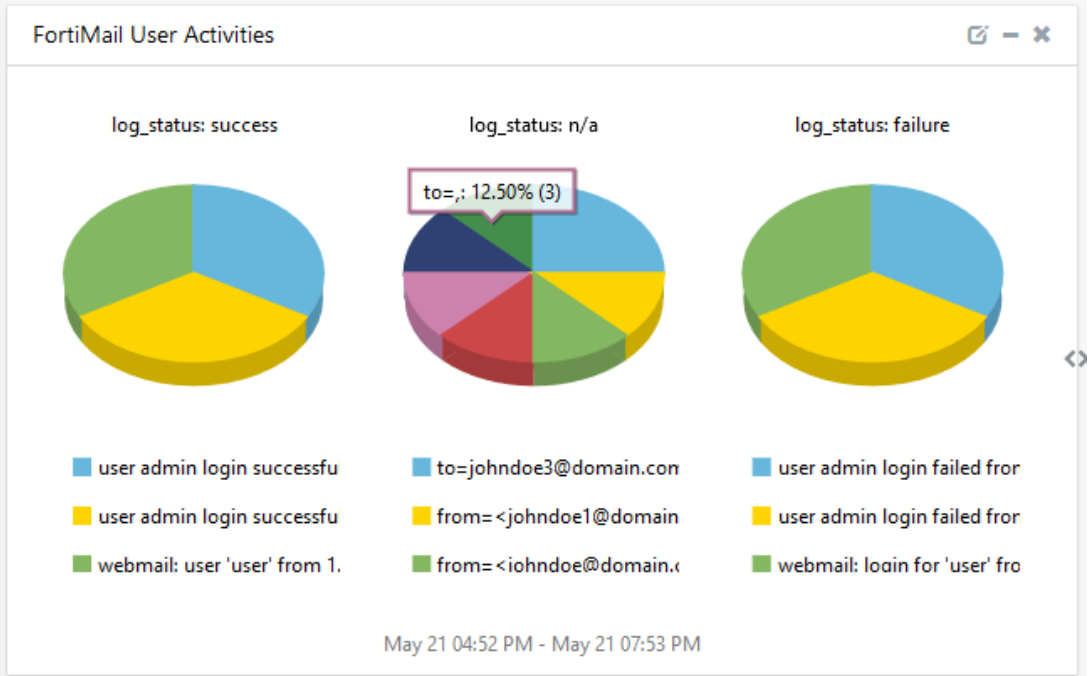

Figure 9

- **FortiMail Email Filters** – This dashboard shows information of user-created email filters for finding malicious activities.

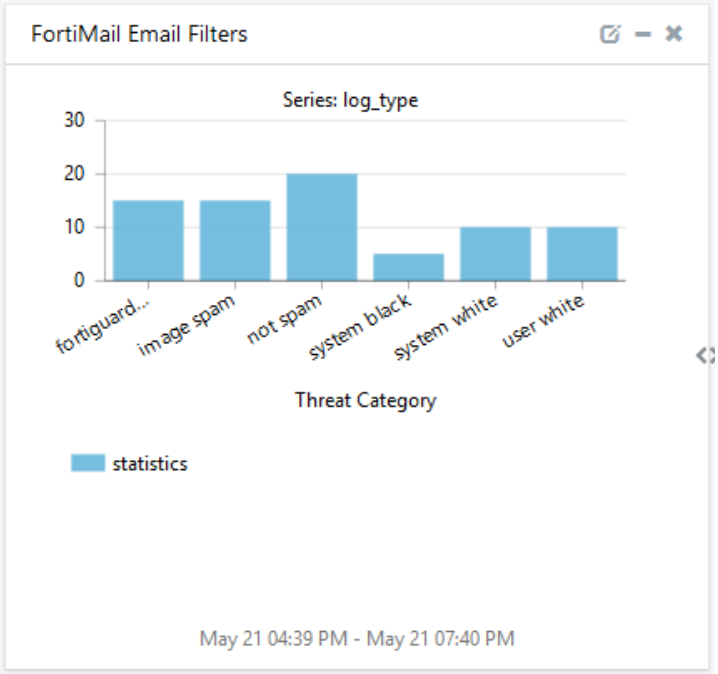

Figure 10

Import Knowledge Pack into EventTracker

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

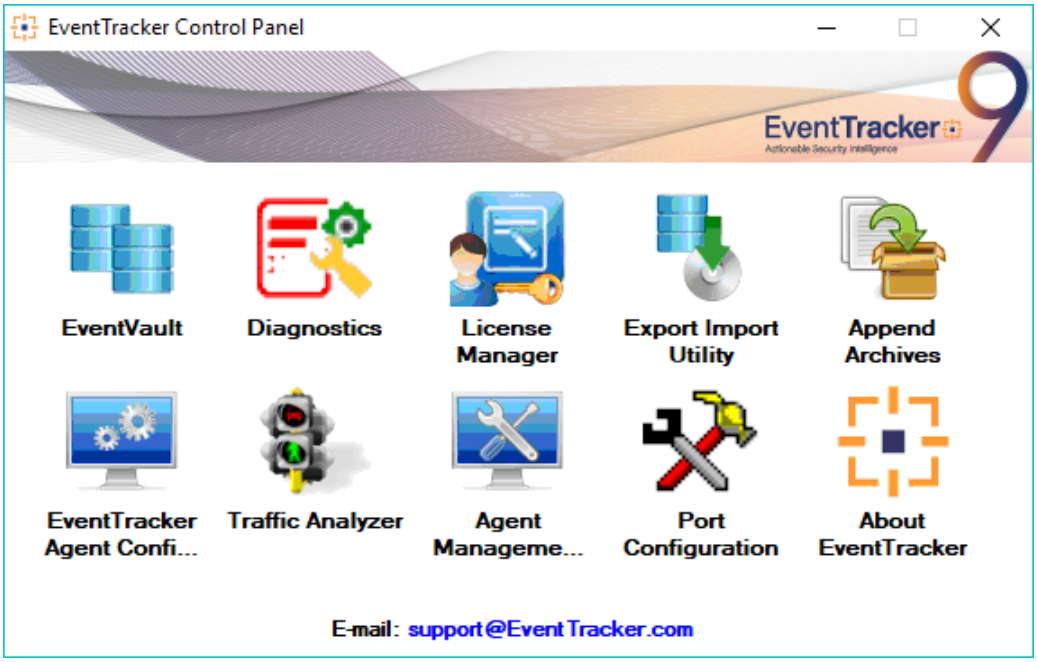

Figure 11

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

Alerts

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

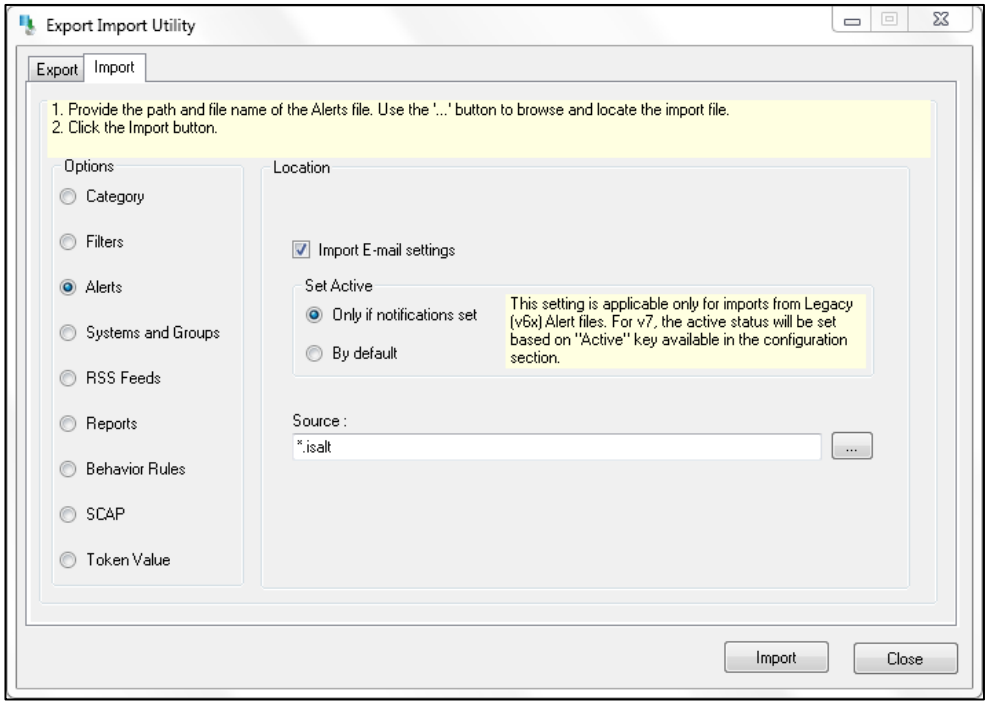

Figure 12

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

Figure 13

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

Knowledge Objects

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

Figure 14

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

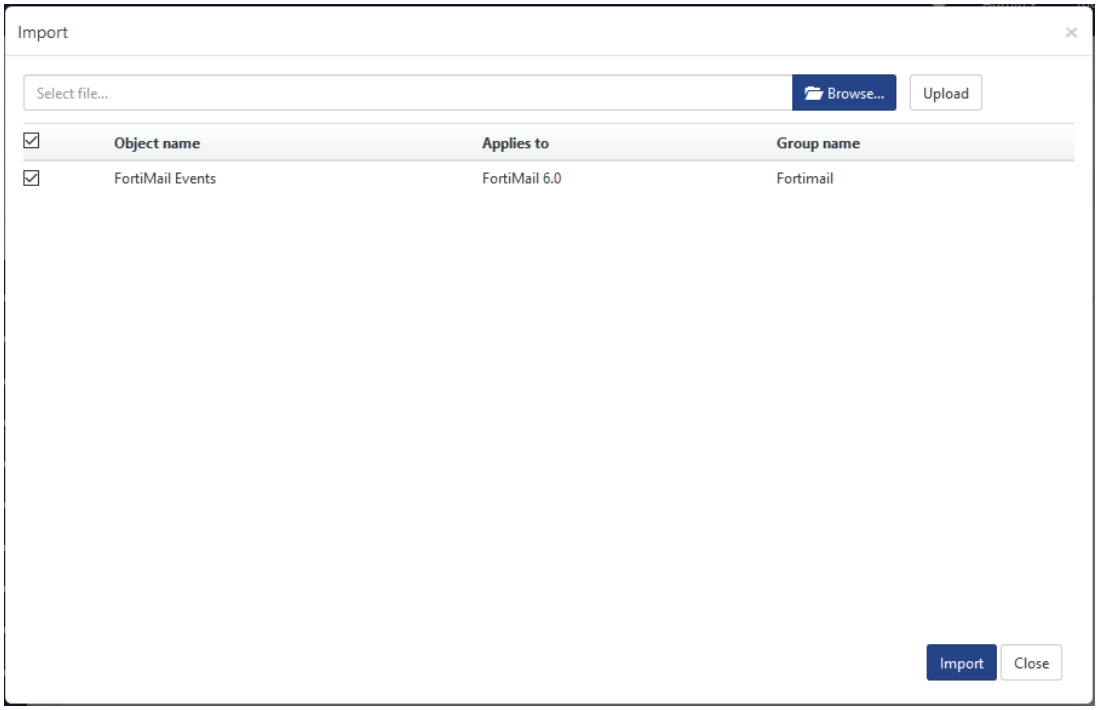

Figure 15

4. Knowledge objects are now imported successfully.

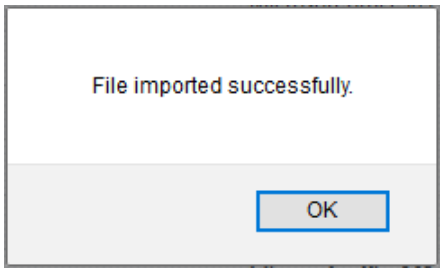

Figure 16

Token Template

1. Login to the **EventTracker Enterprise**.
2. Click on **Admin >> Parsing Rules**.

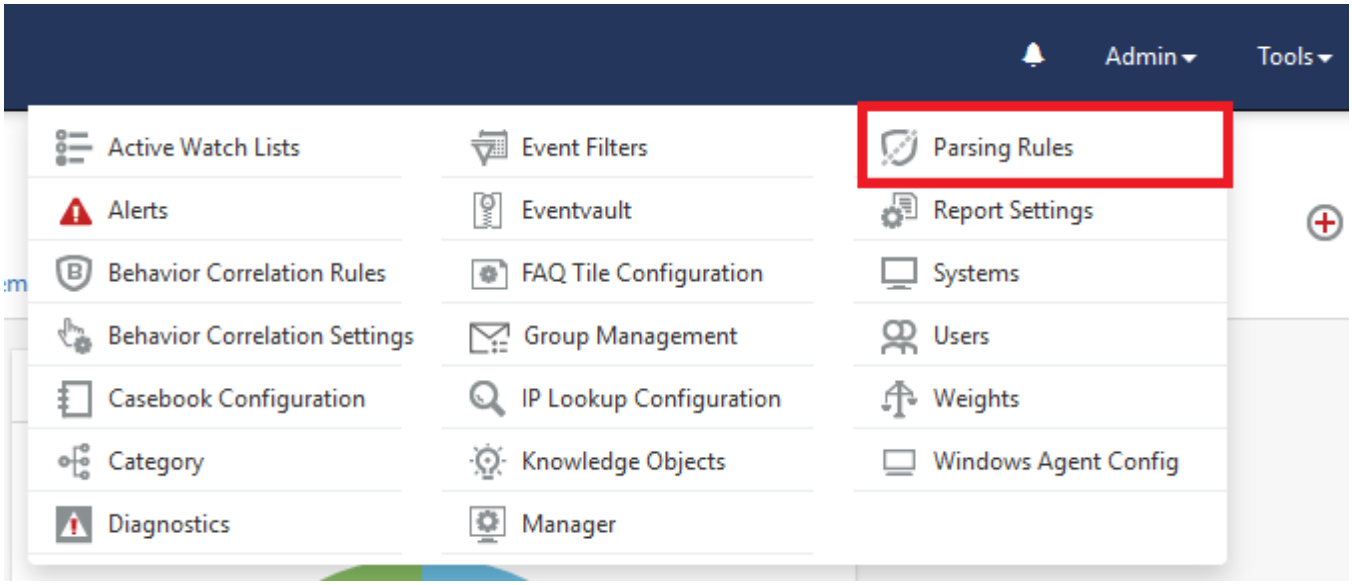

Figure 17

3. Click on **Template** and click **import configuration** Symbol.

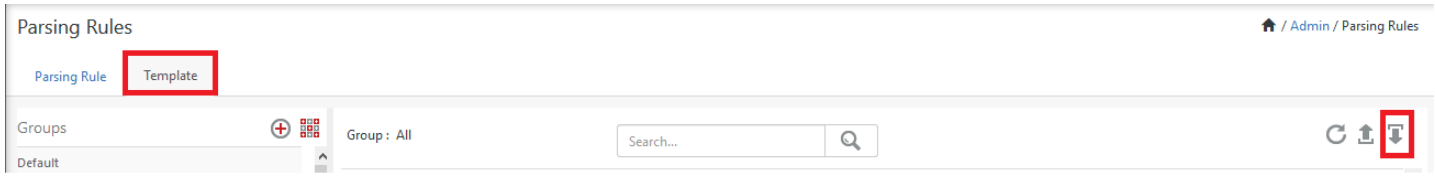

Figure 18

4. Locate the **Template_FortiMail.ettd** file and click on **import**.

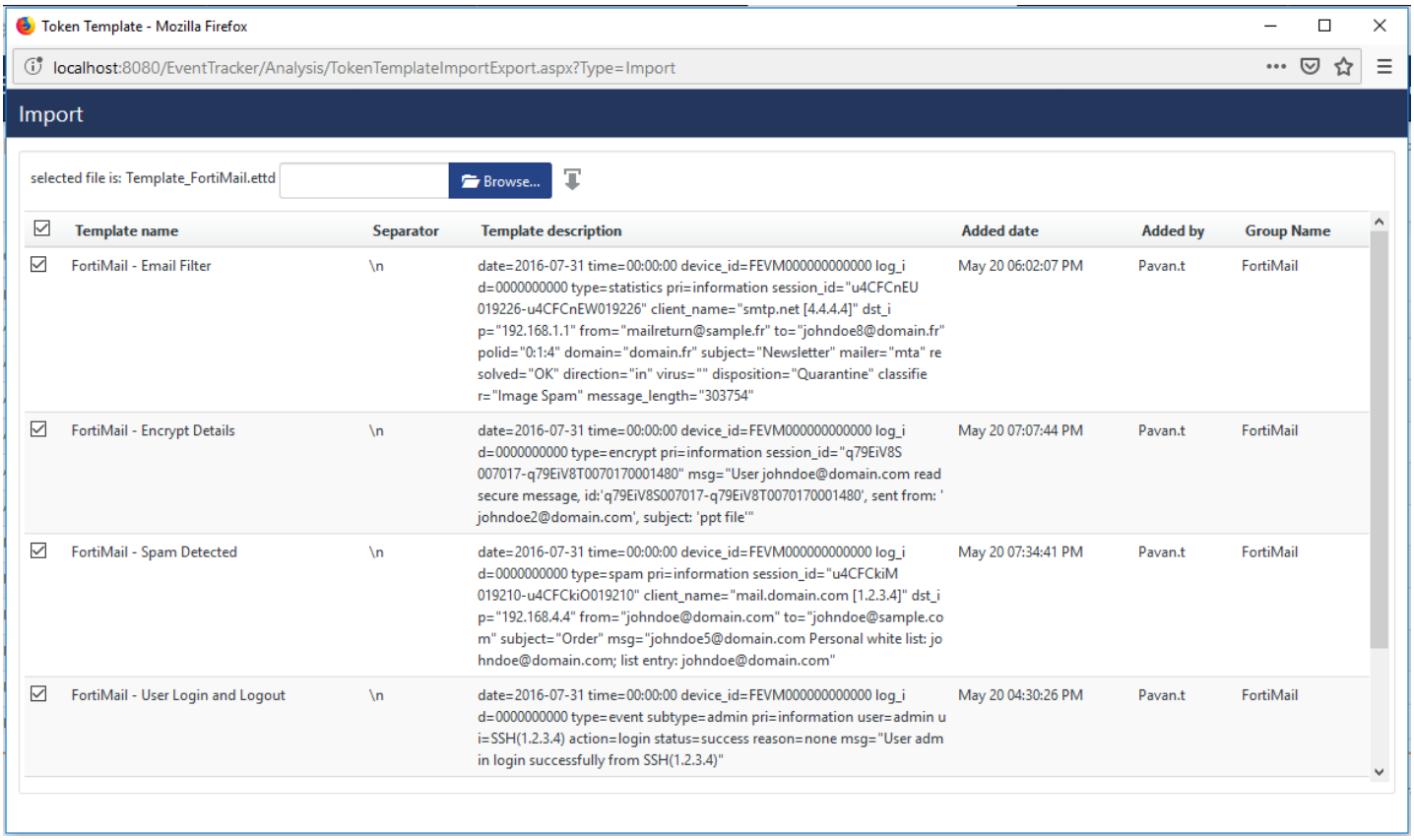

Figure 19

5. Templates are imported now successfully.

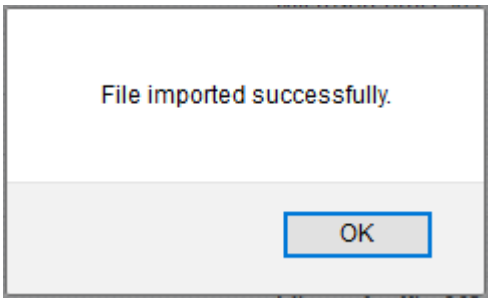

Figure 20

Flex Reports

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

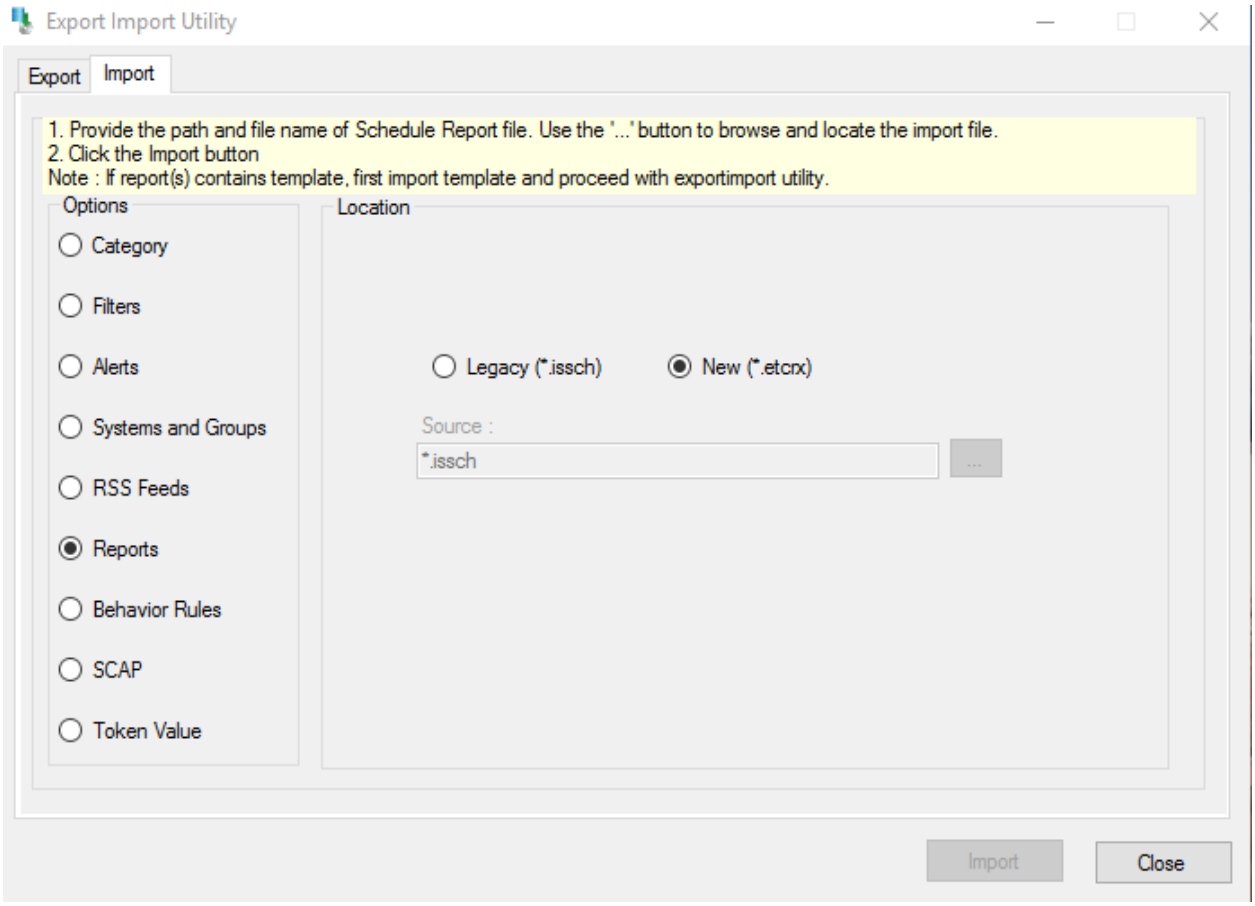

Figure 21

2. Locate the file named **Flex_Reports_FortiMail.etcrx** and select all the checkbox.

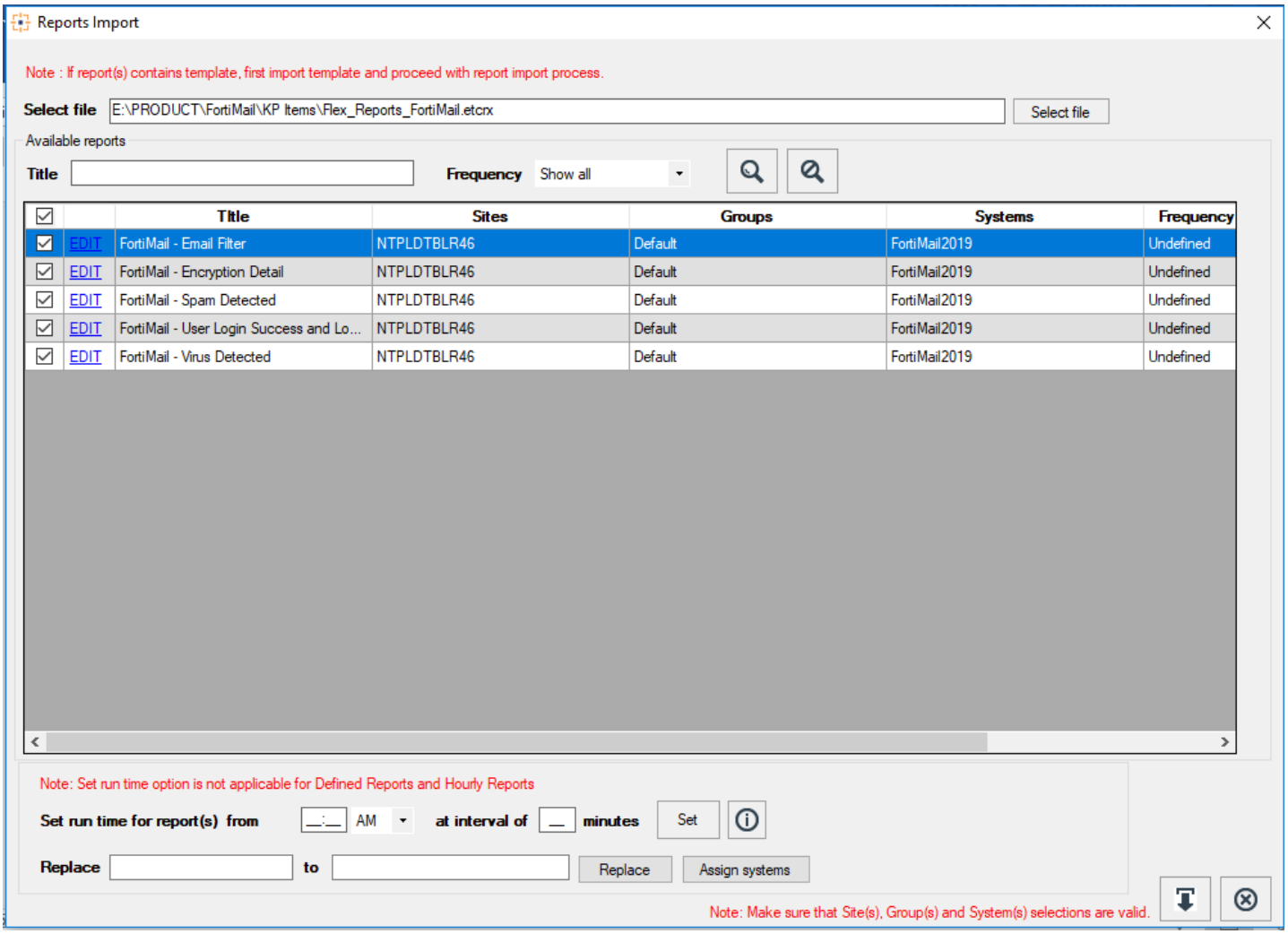

Figure 22

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

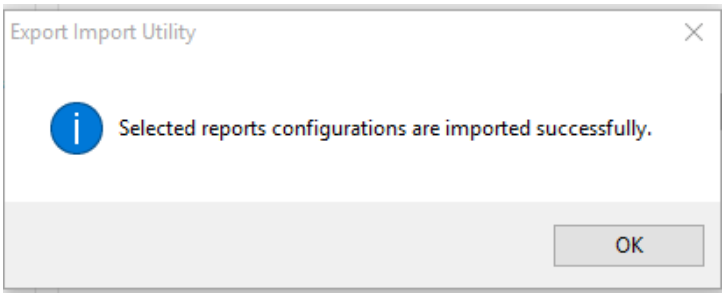

Figure 23

Category

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

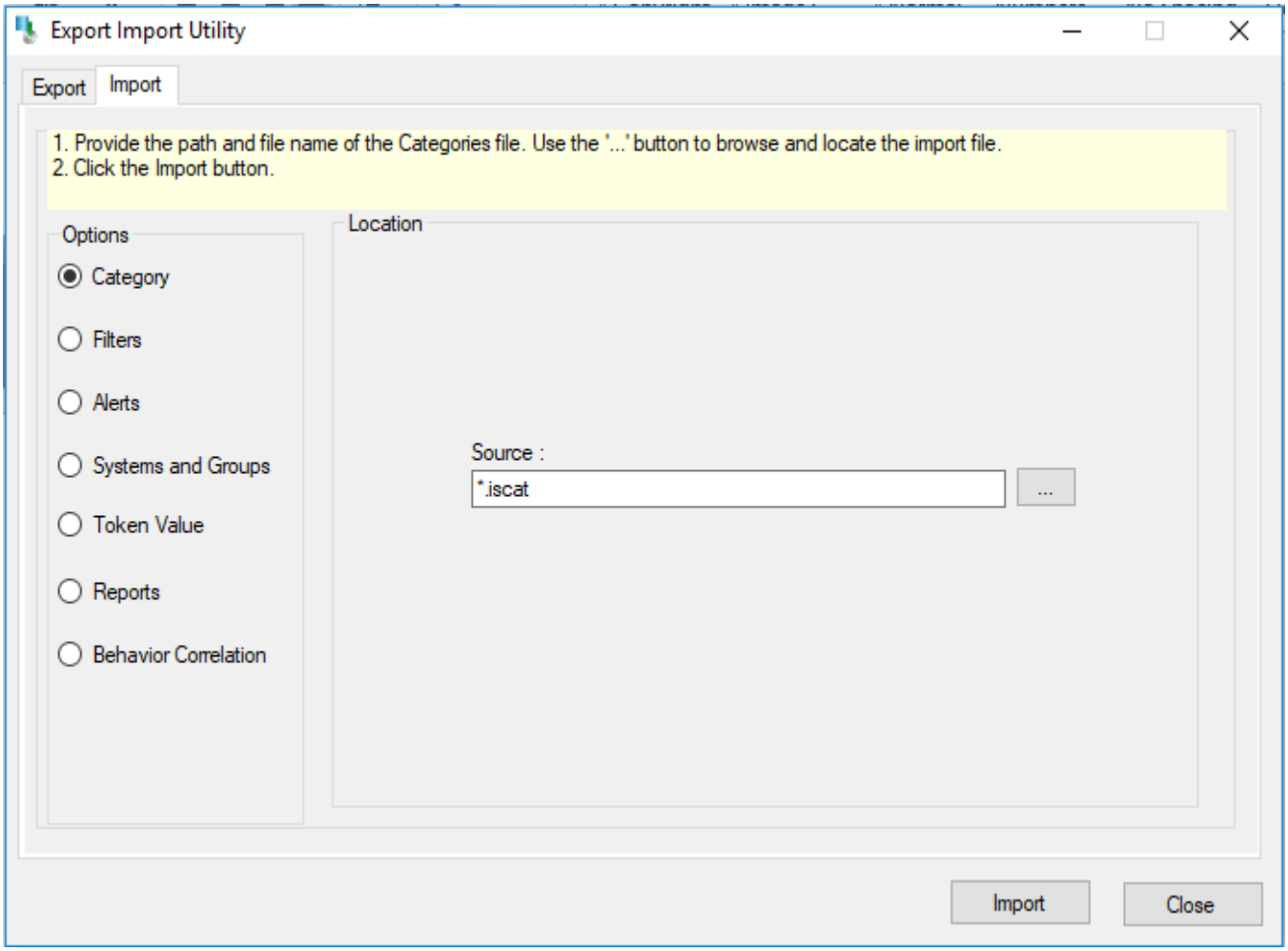

Figure 24

2. Locate **Category_FortiMail.iscat** file, and then click the open button.
3. To import category, click the **Import** button.
   EventTracker displays a success message.

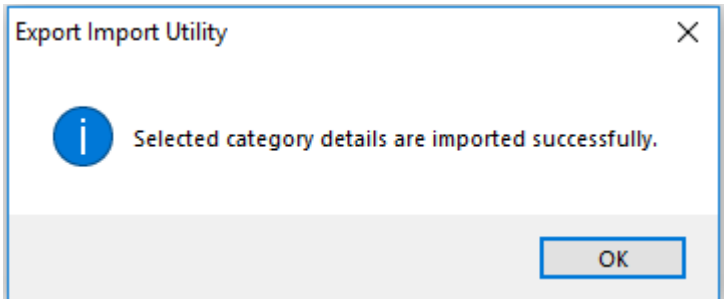

Figure 25

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

Dashlets

In EventTracker 9.0, we have added a new feature that will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker Enterprise Web console.

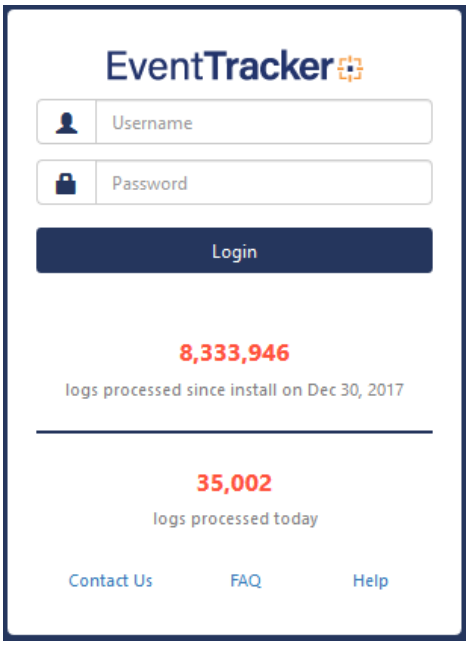

Figure 26

2. Go to **My Dashboard** option.

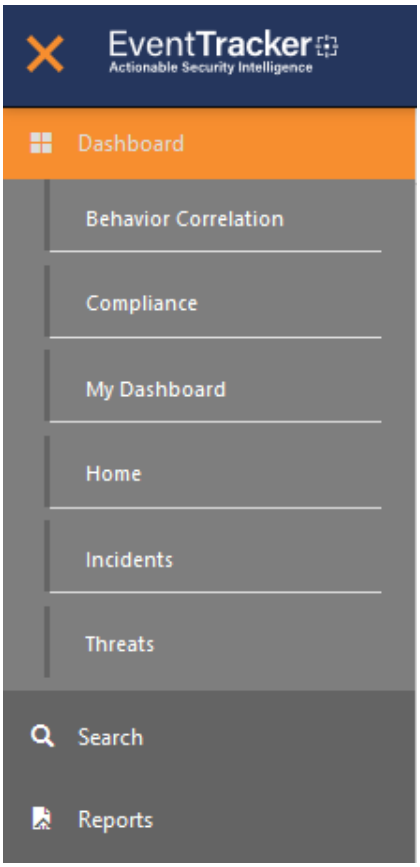

Figure 27

3. Click on the import button and select **.etwd** File.

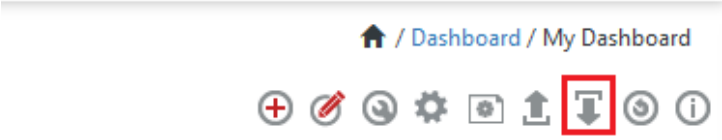

Figure 28

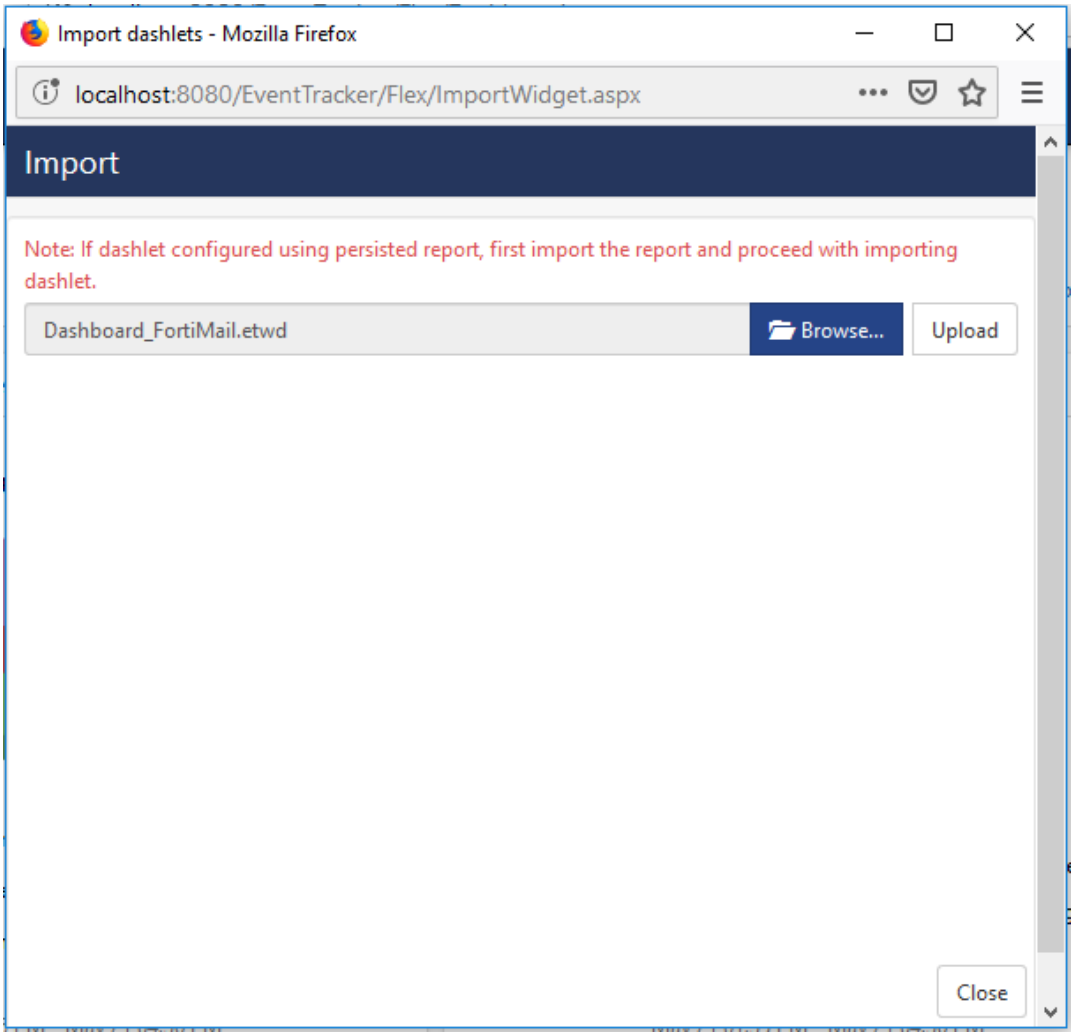

Figure 29

4. Click upload and select Dashboard which you want to import.

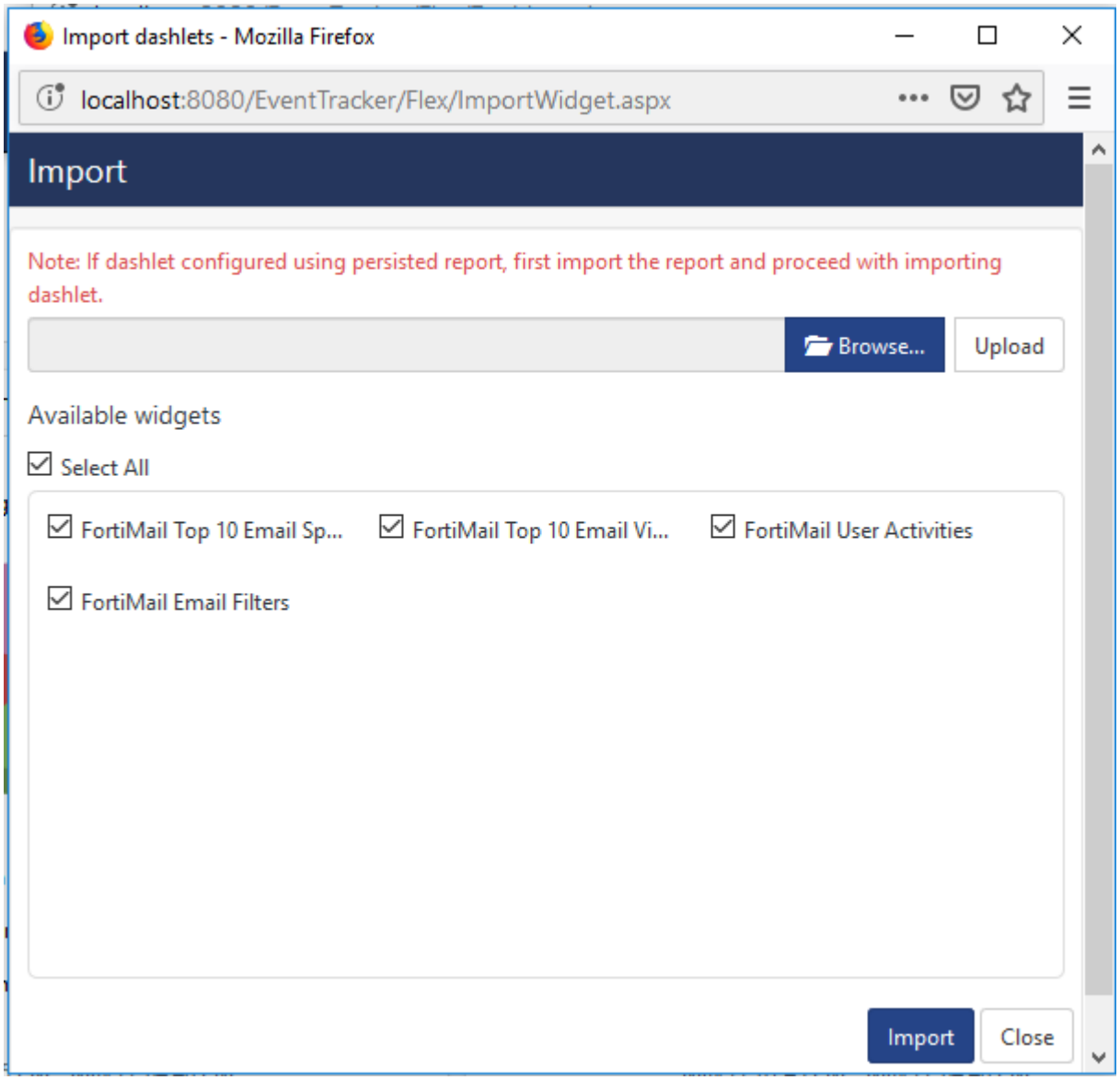

Figure 30

5. Click on the **Import** button. It will upload all selected dashboards.

Verify Knowledge Pack in EventTracker

Category

1. Login to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Category**.

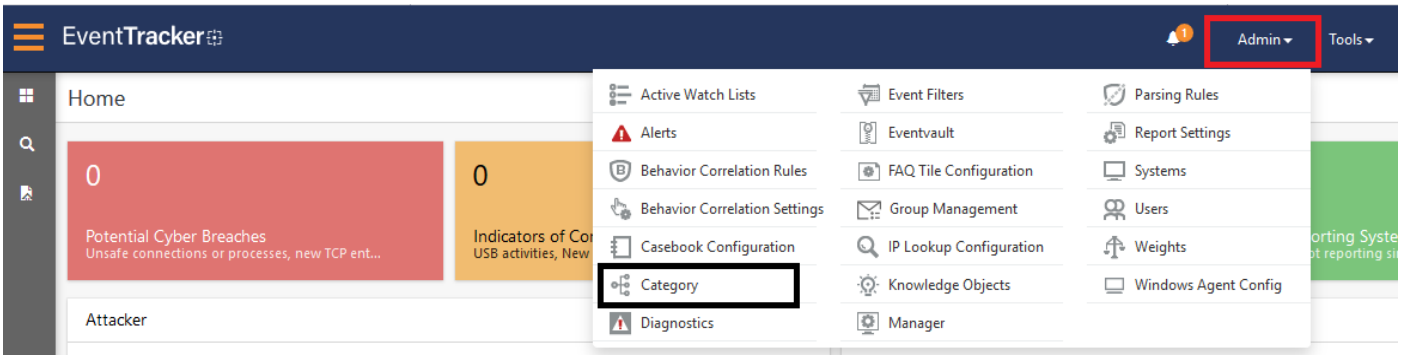

Figure 31

3. Click the **search**, and then **search** with **FortiMail**.

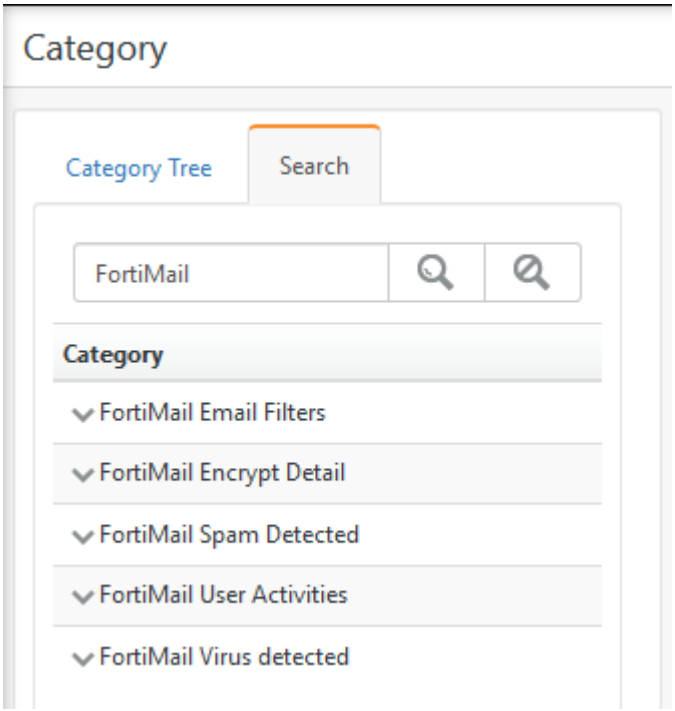

Figure 32

Alerts

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

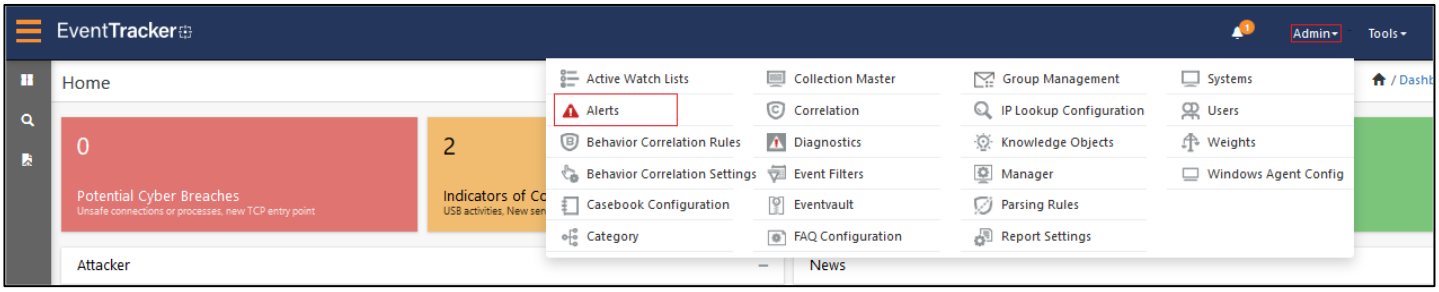

Figure 33

3. In the **Search** box, type **'FortiMail'**, and then click the **Go** button.
   Alert Management page will display all the imported alerts.

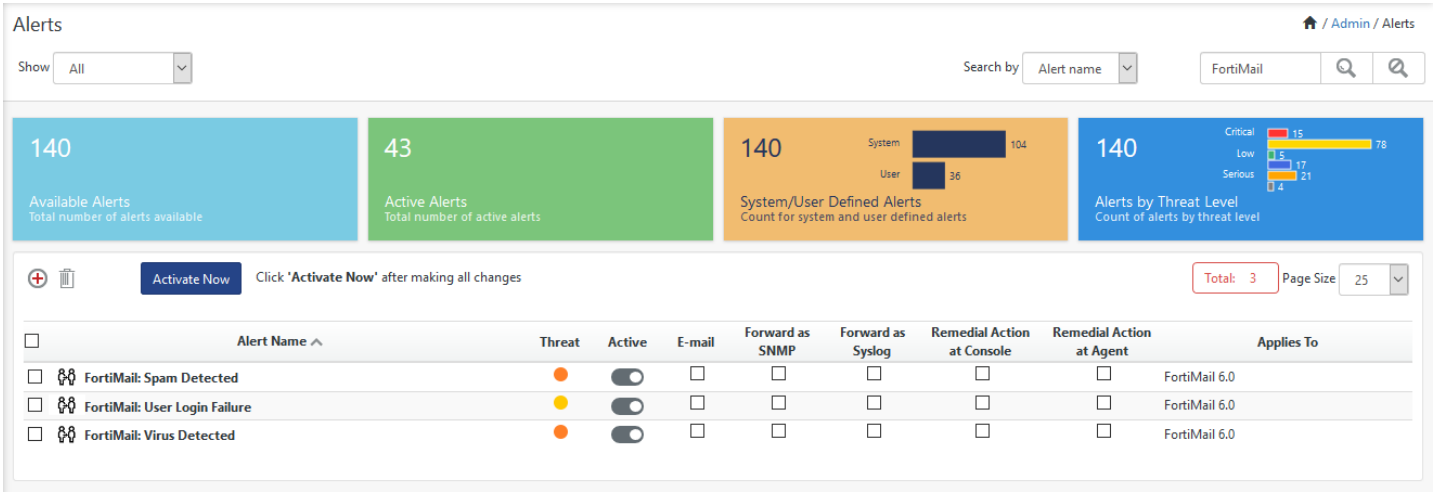

Figure 34

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays a message box.

Figure 35

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

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

Knowledge Object

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

Knowledge Object is displayed in the pane.

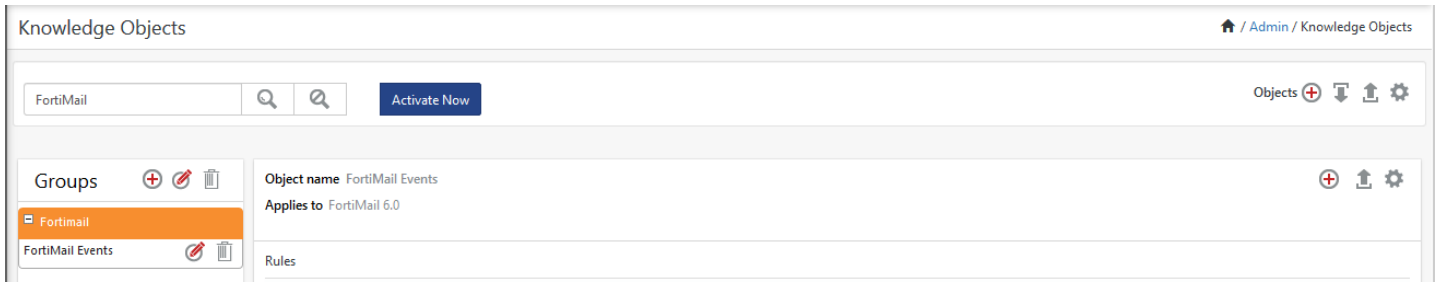

Figure 36

Flex Reports

1. Login 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 **FortiMail** group folder.

   Reports are displayed in the Reports configuration pane.

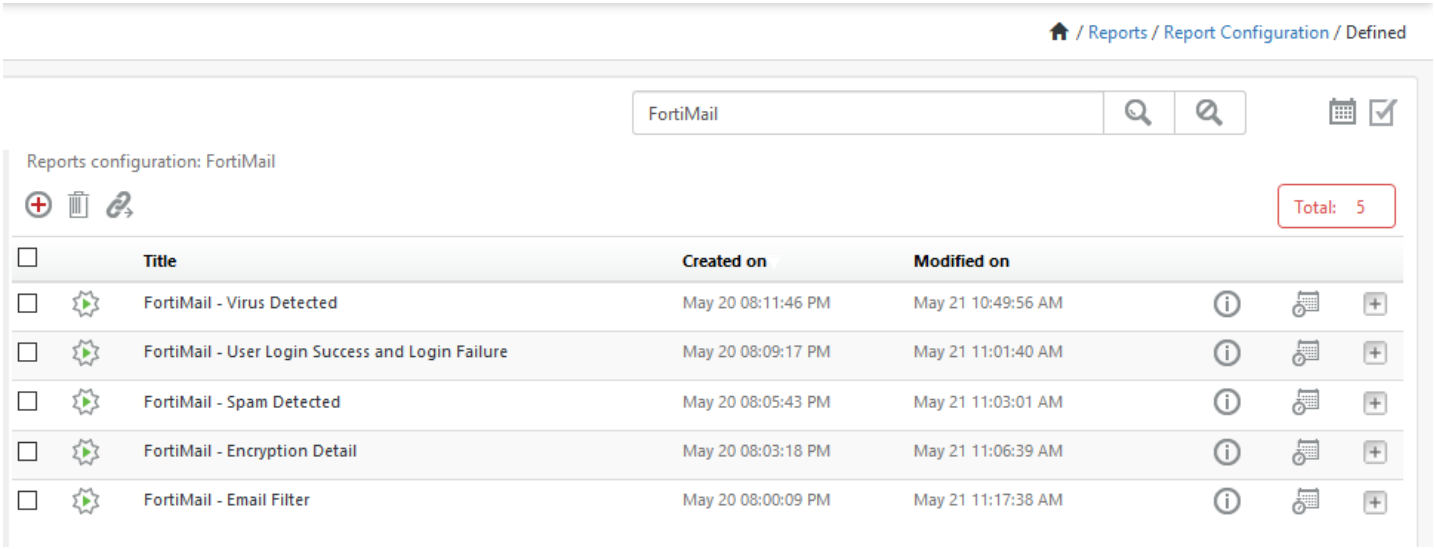

Figure 37

Dashlets

1. Login to **EventTracker Enterprise**.
2. Click the **Dashboard** menu, and then **My Dashboard.**
3. Then click on **Customize Dashlet** button and search for **"FortiMail"**

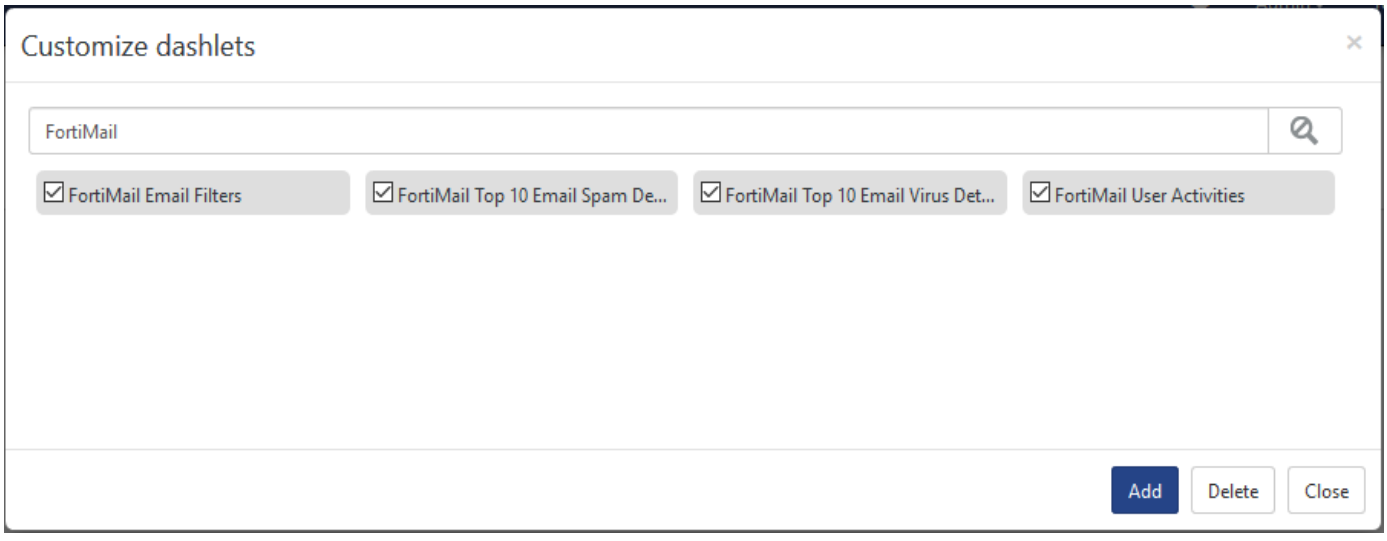

Figure 38

Token Template

1. Login to the **EventTracker Enterprise**.
2. Click on **Admin >> Parsing Rules**.

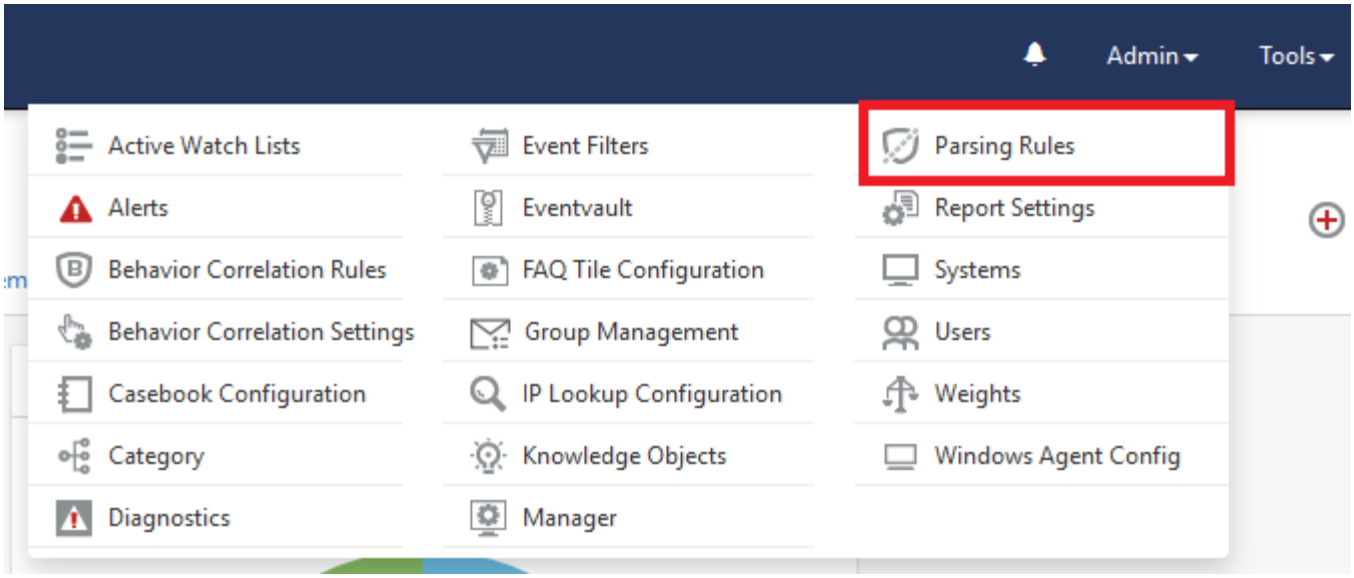

Figure 39

3. Click on **Template** and search for **FortiMail.**

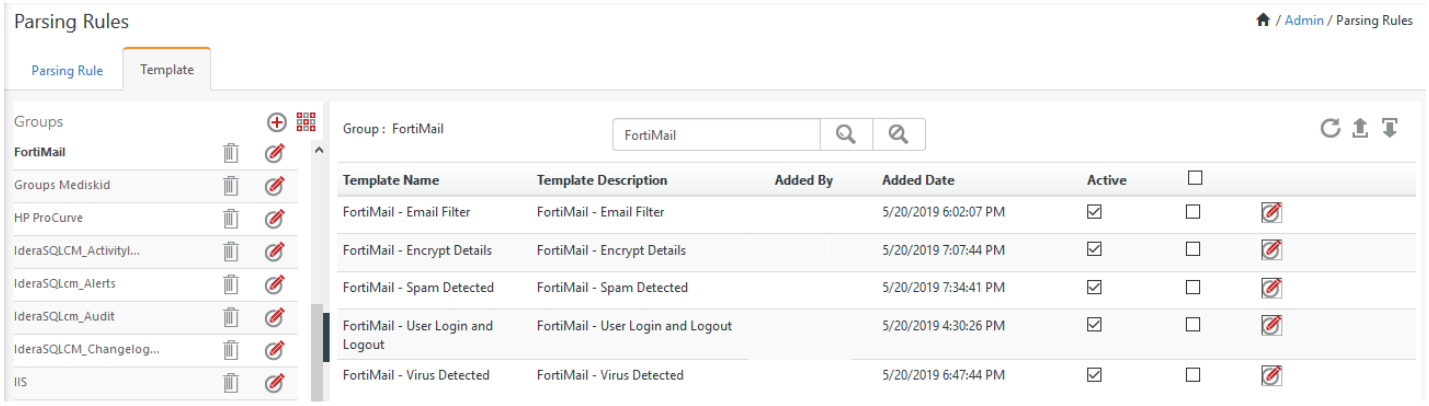

Figure 40