

# 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) Alert	4 4
Reports	4
Dashboards	6
Import Knowledge Pack into EventTracker Alerts	9 9
Knowledge Objects	
Token Template	12
Flex Reports	13
Category	15
Dashlets	17
Verify Knowledge Pack in EventTracker Category	20 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  $\rightarrow$  Log Settings  $\rightarrow$  Remote Log Settings.
- 2. Toggle Enable for your preferred profile.
- 3. Go to Log and Report  $\rightarrow$  Log Settings  $\rightarrow$  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.



FortiMail V	M
Monitor	Local Log Settings Remote Log Settings
Maintenance	Log to Local Disk
System Encryption	The log file will rotate when either the file size or log time is reached. Free disk space: 50575(MB) Log file size: 20 (MB)
User Policy	Log time: 10 (day) At hour: 0:00 V Log level: Information V Log options when disk is full Do not log
Profile AntiSpam AntiVirus	Logging Policy Configuration     Event Log
Email Archiving Log and Report Log Settings Report Settings Alert Email	Image: Construction with the construction of the constr
	Apply Cancel

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	FEVM0000000000000	"[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	FEVM0000000000000	"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	FEVM0000000000000	"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"

• 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"	FEVM0000000000000	"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 Perse white list: johndoe@domain.c list entry: johndoe@domain.ce
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"	FEVM0000000000000	"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	FEVM00000000000000	in formation	'iohndoe2@domain.com'	"q79EiV8S007017-	'opt file'''	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
	onoryp:			Jonnacozi@doniain.com	q79EiV8T0070170001480"	pp:///o		q79EiV8T0070170001480'	secure message
05/20/2010 08:21:34 PM	encount	FEV/M0000000000000	information	'iohndoe2@domain.com'	"q79EiV8S007017-	'oot file'''	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/20/2013 00.21.34 PM	enerypt		intornation	jonnaoez@aomain.com	q79EiV8T0070170001480"	pprine	0000000000	q79EiV8T0070170001480'	secure message
05/20/2010 09:21:26 DM	encovert	EEV/M00000000000000	in formation	liohadaa2@damain.com	"q79EiV8S007017-	'oot filo"	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/20/2019 00.21.30 PM	encrypt		intormation	junnuuez@uunnain.com	q79EiV8T0070170001480"	pprille	0000000000	q79EiV8T0070170001480'	secure message
05/20/2010 09:21:29 DM	encovert	EEV/M000000000000000	in formation	liohadaa2@damain.com	"q79EiV8S007017-	'oot filo"	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/20/2019 00.21.30 PM	encrypt		intormation	junnuuez@uunnain.com	q79EiV8T0070170001480"	pprilie	0000000000	q79EiV8T0070170001480'	secure message
05/21/2010 10:47:34 AM	encovet	EEV/M000000000000000	in formation	liohadae2@damain.com	"q79EiV8S007017-	'ont file"	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/21/2019 10.4/.34 AM	encrypt	1 L VM000000000000000	intornation	junnuuez@uumain.com	q79EiV8T0070170001480"	pprilie	0000000000	q79EiV8T0070170001480'	secure message
05/21/2010 10:47:41 AM	encovet	EEV/M000000000000000	in formation	liohadae2@damain.com	"q79EiV8S007017-	loot filo"	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/21/2019 10.4/.41 AM	encrypt	1 L V M000000000000000	intornation	junnuuez@uumain.com	q79EiV8T0070170001480"	pprilie	0000000000	q79EiV8T0070170001480'	secure message
05/21/2010 10:57:54 AM	encovet	EEV/M00000000000000	in formation	'iobadoe2@domain.com'	"q79EiV8S007017-	'ont file"	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/21/2019 10.37.34 AM	encrypt	1 E VM000000000000000	intornation	junnuuez@uumain.com	q79EiV8T0070170001480"	pprille	0000000000	q79EiV8T0070170001480'	secure message
05/21/2010 11:03:21 AM	encovet	EEV/M00000000000000	in formation	'iobadoe2@domain.com'	"q79EiV8S007017-	'ont file"	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/21/2019 11:03:21 AM	encrypt	1 E V M000000000000000	intornation	junnuuez@uumain.com	q79EiV8T0070170001480"	pprille	000000000	q79EiV8T0070170001480'	secure message
05/21/2010 11:03:24 AM	encount	EEV/M0000000000000	in formation	liohadae2@damain.com	"q79EiV8S007017-	'ont file"	0000000000	'q79EiV8S007017-	"User johndoe@domain.com read
03/21/2013 11.03.24 AM	encrypt	1 2 4 1000000000000000000000000000000000	intornation	jonnuoez@domain.com	g79EiV8T0070170001480"	hhr me	000000000000	a79EiV8T0070170001480	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	"192.168.100.10 0"	"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	"192.168.100.10 0"	"smtp.com [12.12.12.12]"	FEVM0000000000000	"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]"	FEVM0000000000000	"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.c om"	"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.c om"	"johndoe5@domain.fr"	0000000000	"mta"	"0:1:4"	information	"u4CFCmMn019223- u4CFCmMp019223"	"Not Spam"
05/20/2019 08:19:51 PM	statistics	"192.168.100.10 0"	"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	"192.168.100.10 0"	"smtp.net	FEVM000000000000	"domain.fr"	"mailreturn@sample.com	"johndoe@domain.fr"	0000000000	"mta"	"0:1:4"	in formation	"u4CFCnEU019216-	"Image Spam"

Figure 6

### Dashboards

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





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



Figure 8

7

Netsurion EventTracker

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



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



Figure 10

**Netsurion** EventTracker

# 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.



🐁 Export Import Utility					23
Export Import					
1. Provide the path and file na 2. Click the Import button.	me of the Alerts file. Use the '' button	to browse and locate the import file.			
Options	Location				
Category					
Filters	Import E-mail settings				
Alerts	Set Active				
Systems and Groups	<ul> <li>Only if notifications set</li> <li>By default</li> </ul>	<ul> <li>This setting is applicable only for imports from Leg (v6x) Alert files. For v7, the active status will be subased on "Active" key available in the configural section.</li> </ul>	gacy et tion		
RSS Feeds		securit h			
Reports	Source :				
Dahauira Dulaa	*.isalt				
Benavior Hules					
SCAP					
🔘 Token Value					
		Import		Close	•

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.





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.

Import		×
KO_FortiMail.etko	Browse Upload	
		Class
		Close

3. Now select all the checkbox and then click on the  $\mathbb{T}$  '**Import**' option.

Import				×
Select file			🗁 Browse Upload	
	Object name	Applies to	Group name	
	FortiMail Events	FortiMail 6.0	Fortimail	
			Import Close	

Figure 15



4. Knowledge objects are now imported successfully.





### Token Template

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

		🐥 Admin <del>-</del>	Tools <del>-</del>
Active Watch Lists	Event Filters	🧭 Parsing Rules	
Alerts	Sector Eventvault	🗐 Report Settings	÷
m Behavior Correlation Rules	FAQ Tile Configuration	Systems	
Behavior Correlation Settings	Group Management	Q Users	
Casebook Configuration	Q IP Lookup Configuration	r Weights	
• Category	·O- Knowledge Objects	Windows Agent Config	
Diagnostics	Manager		

Figure 17

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

Parsing Rules							
Parsing Rule	Template						
Groups	<b>(+)     </b>	Group : All	Search	Q	CİŢ		
Default	^						



4. Locate the Template\_FortiMail.ettd file and click on import.

Netsurion... EventTracker

Tok	en Template - Mozilla Firefox					- 0	×
Iocalhost:8080/EventTracker/Analysis/TokenTemplateImportExport.aspx?Type=Import							≡
ιpo	ort						
elect	ted file is: Template_FortiMail.ettd		🖆 Browse				
~	Template name	Separator	Template description	Added date	Added by	Group Name	^
2	FortiMail - Email Filter	\n	date=2016-07-31 time=00:00:00 device_id=FEVM00000000000 log_i d=0000000000 type=statistics pri=information session_id="u4CFCnEU 019226-u4CFCnEW019226" client_name="smtp.net[4.4.4.4]" dst_i p="192.168.1.1" from="mailreturn@sample.fr" to="johndoe8@domain.fr" polid="0:1:4" domain="domain.fr" subject="Newsletter" mailer="mta" re solved="OK" direction="in" virus=" disposition="Quarantine" classifie r="Image Spam" message_length="303754"	May 20 06:02:07 PM	Pavan.t	FortiMail	
2	FortiMail - Encrypt Details	\n	date=2016-07-31 time=00:00:00 device_id=FEVM00000000000 log_i d=0000000000 type=encrypt pri=information session_id="q79EiV8S 007017-q79EiV8T0070170001480" msg="User johndoe@domain.com read secure message, id:'q79EiV8S007017-q79EiV8T0070170001480', sent from: ' johndoe2@domain.com', subject: 'ppt file'"	May 20 07:07:44 PM	Pavan.t	FortiMail	
2	FortiMail - Spam Detected	\n	date=2016-07-31 time=00:00:00 device_id=FEVM00000000000 log_i d=0000000000 type=spam pri=information session_id="u4CFCkiM 019210-u4CFCki0019210" client_name="mail.domain.com [1.2.3.4]" dst_i p="192.168.4.4" from="johndoe@domain.com" to="johndoe@sample.co m" subject="Order" msg="johndoe5@domain.com Personal white list: jo hndoe@domain.com; list entry: johndoe@domain.com"	May 20 07:34:41 PM	Pavan.t	FortiMail	
2	FortiMail - User Login and Logout	\n	date=2016-07-31 time=00:00:00 device_id=FEVM00000000000 log_i d=0000000000 type=event subtype=admin pri=information user=admin u i=SSH(1.2.3.4) action=login status=success reason=none msg="User adm in login successfully from SSH(1.2.3.4)"	May 20 04:30:26 PM	Pavan.t	FortiMail	2
		Token Template - Mozilla Firefox   Iocalhost:8080/EventTracker/Analysis/  port elected file is: Template_FortiMail.ettd  Template name FortiMail - Email Filter  FortiMail - Encrypt Details FortiMail - Spam Detected FortiMail - User Login and Logout	Token Template - Mozilla Firefox         Iocalhost:8080/EventTracker/Analysis/TokenTemplateIm         pport         elected file is: Template_FortiMail.ettd         Image: Template name       Separator         FortiMail - Email Filter       \n         FortiMail - Encrypt Details       \n         FortiMail - Spam Detected       \n         FortiMail - User Login and Logout       \n	Token Template - Mozilla Firefox         Inocalhost:8080/EventTracker/Analysis/TokenTemplateImportExport.aspx?Type=Import         Inocalhost:8080/EventTracker/Analysis/TokenTemplateImportExport.aspx?Type=Import         Import         Import       Separator       Template description         Import       Import	Import         Import		Toten Template - Mozilla Firefox       —       □         I localhost-8080//EventTracker/Analysis/Token TemplateImportExport.aspx?Type=Import       ••• ♥ ↓         aport       ••• ♥       ••• ♥         alected file is: Template_FortiMail.ettd       ••• ♥       ●

5. Templates are imported now successfully.



Figure 20

### **Flex Reports**

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

Netsurion... EventTracker

Detions	coation	my.
) Filters		
Alerts	O Legacy (*.issch)      New (*.etcn	x)
Systems and Groups	Source :	
RSS Feeds	".issch	
Reports		
) Behavior Rules		
) SCAP		
) Token Value		



2. Locate the file named Flex\_Reports\_FortiMail.etcrx and select all the checkbox.



[] Re	ports In	nport				×
Note	· If repo	rt(e) contains template, first import template a	and proceed with report import process			
Colo	at file	E:\PPODUCT\EartiMail\KP.home\Pov_Pov	voarta. EastiMail star:			
- Avail	able rep	E: \FRODUCT\Fottimali\KFTtettis\Flex_Ke	eports_FortiMail.etcrx		Select file	
Title		013	Fraguency Show all			
			Hequency Show an			
		Title	Sites	Groups	Systems	Frequency
	EDIT	FortiMail - Email Filter	NTPLDTBLR46	Default	FortiMail2019	Undefined
	EDIT	FortiMail - Encryption Detail	NTPLDTBLR46	Default	FortiMail2019	Undefined
	EDIT	FortiMail - Spam Detected	NTPLDTBLR46	Default	FortiMail2019	Undefined
	EDIT	FortiMail - User Login Success and Lo	NTPLDTBLR46	Default	FortiMail2019	Undefined
	EDIT	FortiMail - Virus Detected	NTPLDTBLR46	Default	FortiMail2019	Undefined
٢						>
No	te: Set r	un time option is not applicable for Defined I	Reports and Hourly Reports			
Se	t run ti	ime for report(s) from	M ▼ at interval of minut	tes Set		
Re	eplace	to	Rej	place Assign systems		
-				Note: Make sure that Site	(s), Group(s) and System(s) selections are	ralid.



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

Export Import Utility	$\times$
Selected reports configurations are imported successfully.	
ОК	



### Category

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

🐁 Export Import Utility		_		$\times$
Export Import				
1. Provide the path and file nan 2. Click the Import button.	ne of the Categories file. Use the '' button to browse and locate the import file.			
Options	Location			
<ul> <li>Category</li> </ul>				
<ul> <li>Filters</li> </ul>				
◯ Alerts				
O Systems and Groups	Source :			
O Token Value				
⊖ Reports				
O Behavior Correlation				
	Imp	oort	Clos	e



- 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.

Export Impo	ort Utility	×
	Selected category details are imported successfully.	
	ОК	



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.

EventTracker 🕀						
1	Username					
	Password					
	Login					
<b>8,333,946</b> logs processed since install on Dec 30, 2017						
<b>35,002</b> logs processed today						
	35,002 logs processed today					

Figure 26

2. Go to My Dashboard option.

X EventTracker 답
Dashboard
Behavior Correlation
Compliance
My Dashboard
Home
Incidents
Threats
<b>Q</b> Search
Reports
Figure 27

Figure 27

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







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



😉 Import dashlets - Mozilla Firefox	_		]	$\times$
Iocalhost:8080/EventTracker/Flex/ImportWidget.aspx	•••	${\times}$	☆	≣
Import				^
Note: If dashlet configured using persisted report, first import the report and proceed wi dashlet.	th imp	orting	9	
🚍 Brov	vse	U	pload	J
Available widgets				
Select All				
🗹 FortiMail Top 10 Email Sp 🗹 FortiMail Top 10 Email Vi 🗹 FortiMail User	Activi	ties		
☑ FortiMail Email Filters				
	Impo	rt	Close	•

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.

Netsurion... EventTracker

	Admin 🗸	Tools 🕶
Event Filters	🧭 Parsing Rules	
Eventvault	Report Settings	
FAQ Tile Configuration	Systems	
Group Management	Q Users	
Q IP Lookup Configuration	reights	orting Syste ot reporting si
·	Windows Agent Config	
D Manager		
	<ul> <li>₩ Event Filters</li> <li>₩ Eventvault</li> <li>FAQ Tile Configuration</li> <li>₩ Group Management</li> <li>₩ IP Lookup Configuration</li> <li>₩ Knowledge Objects</li> <li>₩ Manager</li> </ul>	Image: Second



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

Category						
Category Tree	Search					
FortiMail		Q	Q			
Category						
❤ FortiMail Emai	il Filters					
✓ FortiMail Encry	ypt Detail					
✓ FortiMail Span	✓ FortiMail Spam Detected					
✓ FortiMail User	✓ FortiMail User Activities					
✓ FortiMail Virus	detected					

Figure 32

### Alerts

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



	Event <b>Tracker</b> ⊕					🔎 🗚 Admin-	Tools <del>+</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	2	Behavior Correlation Rules	Diagnostics	Knowledge Objects	∯ Weights	
			🇞 Behavior Correlation Settings	Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			

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

Alerts									🕈 / Admin / Alerts	
Show All			Search by	Alert name 🗸	FortiMail	ର୍ ବ୍				
140     43       Available Alerts Total number of alerts available     Active Alerts Total number of active alerts					140 System 104 User 36 System/User Defined Alerts Count for system and user defined alerts			140 Critical 15 78 Low 5erious 72 Alerts by Threat Level Count of alerts by threat level		
Activate Now     Click 'Activate No	w' after making all changes							Total: 3	Page Size 25 🗸	
Alert Name A	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Appl	ies To	
ြ မိုမို FortiMail: Spam Detected	•							FortiMail 6.0		
🔲 🖗 FortiMail: User Login Failure	•							FortiMail 6.0		
다 않아 FortiMail: Virus Detected	•							FortiMail 6.0		

#### Figure 34

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

EventTracker displays a message box.

Successfully saved configuration.	
ОК	



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.
- 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.

Knowledge Objects							
FortiMail	Q Q Activate Now	Objects 🕂 Ҭ 🏌 🌣					
Groups 🕀 🤅	Object name FortiMail Events	🕀 🏦 🌩					
Fortimail	Applies to Politimal do						
FortiMail Events	Rules						

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.



A / Reports / Report Configuration / Defined

			FortiMail				<b>i</b>	
Rep	orts confi	guration: FortiMail						
Ð	Ü 2,						Total:	5
		Title	Created on	Modified on				
	£ <b>3</b> 3	FortiMail - Virus Detected	May 20 08:11:46 PM	May 21 10:49:56 AM		i	8	+
	2	FortiMail - User Login Success and Login Failure	May 20 08:09:17 PM	May 21 11:01:40 AM		i	2	+
	£ <b>3</b> 3	FortiMail - Spam Detected	May 20 08:05:43 PM	May 21 11:03:01 AM		(i)	8	+
	£ <b>3</b> 3	FortiMail - Encryption Detail	May 20 08:03:18 PM	May 21 11:06:39 AM		(j)	5	+
	£	FortiMail - Email Filter	May 20 08:00:09 PM	May 21 11:17:38 AM		i	5	+

Figure 37

### Dashlets

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

0	Customize dashlets					×
	FortiMail				Q	
	FortiMail Email Filters	FortiMail Top 10 Email Spam De	FortiMail Top 10 Email Virus Det	FortiMail User Activities		
				Add Delete	Clo	se

Figure 38

Netsurion EventTracker

### Token Template

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

		🐥 Admin <del>-</del>	Tools <del>-</del>
Active Watch Lists	Event Filters	🧭 Parsing Rules	
Alerts	Eventvault	Report Settings	÷
m 📵 Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	QQ Users	
Casebook Configuration	Q IP Lookup Configuration	r Weights	
● Category	· O- Knowledge Objects	Windows Agent Config	
Diagnostics	Manager		

Figure 39

3. Click on Template and search for FortiMail.

Parsing Rules								🕈 / Adm	in / Parsing Rules
Parsing Rule Template									
Groups		<b>+</b> ##	Group : FortiMail	FortiMail	Q	Q			CIT
FortiMail	Ü	Ø ^	·						
Groups Mediskid	Û	0	Template Name	Template Description	Added By	Added Date	Active		
HP ProCurve	Ű	1	FortiMail - Email Filter	FortiMail - Email Filter		5/20/2019 6:02:07 PM	$\checkmark$	0	
IderaSQLCM_ActivityI	Ü	0	FortiMail - Encrypt Details	FortiMail - Encrypt Details		5/20/2019 7:07:44 PM	$\checkmark$	Ø	
IderaSQLcm_Alerts	Ü	1	FortiMail - Spam Detected	FortiMail - Spam Detected		5/20/2019 7:34:41 PM		Ø	
IderaSQLcm_Audit	Ű	1	FortiMail - User Login and	FortiMail - User Login and Logout		5/20/2019 4:30:26 PM		1	
IderaSQLCM_Changelog	Ű	1	Logout	, , ,				Char.	
IIS	Ē	0	FortiMail - Virus Detected	FortiMail - Virus Detected		5/20/2019 6:47:44 PM	$\checkmark$	Ø	

Figure 40

