

# Integrate FortiManager with EventTracker EventTracker v9.x and later

Publication Date: October 7, 2019

### Abstract

This guide provides instructions to configure/ retrieve FortiManager events via syslog configuration. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor FortiManager.

### Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and FortiManager 6.2.0 and later.

## Audience

Administrators who are assigned the task to monitor FortiManager events using EventTracker.

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

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



## Table of Contents

1.	Ove	erview	. 3
2.	Pre	erequisites	. 3
3.	Inte 3.1	egrating FortiManager with EventTracker Forwarding FortiManager Logs to EventTracker	. 3 . 3
4.	Eve 4.1	entTracker Knowledge Pack Reports	. 4 . 4
	4.2	Alerts	. 6
	4.3	Saved searches	. 7
	4.4	Dashboards	. 7
5.	۱mµ 5.1	porting knowledge pack into EventTracker Categories	10 11
	5.2	Alerts	12
	5.3	Token Templates	13
	5.4	Flex Reports	15
	5.5	Knowledge Objects	16
	5.6	Dashboards	18
6.	Ver 6.1	rifying knowledge pack in EventTracker Categories	19 19
	6.2	Alerts	20
	6.3	Token Templates	21
	6.4	Flex Reports	21
	6.5	Knowledge Objects	22
	6.6	Dashboards	22



## 1. Overview

FortiManager appliance allows you to centrally manage many Fortinet devices from a few to thousands, including FortiGate, FortiWiFi, FortiCarrier, FortiMail, and FortiAnalyzer appliances and virtual appliances, as well as FortiClient endpoint security agents.

**EventTracker**, when integrated with FortiManager, enables users to view critical information related to activities performed in FortiManager or other Fortinet devices. This information is represented in the form of report, alert and graphical/pictorial representation(dashboard).

In this integration guide, logging is performed by forwarding FortiManager logs to the EventTracker syslog server.

The logs which FortiManager forwards includes,

- 1. System manager (SYSTEM) events.
- 2. FortiGuard service (FGD) events.
- 3. FortiManager web service (FMGWS) events.
- 4. Managed device operations (DEVOPS) events.
- 5. High Availability (HA) events. Etc.

## 2.Prerequisites

- EventTracker agent should be installed in the host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privileges on the host system/ server to run PowerShell.

## 3. Integrating FortiManager with EventTracker

## 3.1 Forwarding FortiManager Logs to EventTracker

EventTracker receives the logs from FortiManager, once the syslog is configured in FortiManager:

- 1. Go to System Settings  $\rightarrow$  Advanced  $\rightarrow$  Syslog Server.
- 2. Select **Create New** to open the **New Syslog Server** window. (The Create New Syslog Server Settings pane opens.)

# Netsurion... EventTracker

Create New Syslog Serv	er Settings		
Name			
IP address (or FQDN)			
Syslog Server Port	514		•
	ОК	Cancel	



- 3. Fill in the Name, for example, "EventTracker".
- 4. Fill in the IP address or FQDN of the EventTracker receiver.
- 5. Enter the Port number. The default is 514.

## 4.EventTracker Knowledge Pack

EventTracker knowledge pack for FortiManager includes:

- 1. Reports.
- 2. Alerts.
- 3. Saved searches.
- 4. Dashboards.

### 4.1 Reports

• FortiManager - Deployment manager operations – This report provides information about the process of deployment. It shows information about the failure or success status of deployment.

A	DOM		Device	Device serial	Event				Policy package	
Log Time 🔄 Computer 💌 N	lame 🔽	Description	name 💌	number 🔤	subty 💌	Log ID 💌	Login user from 💌	Message 🔽	name 🔽	Priority 💌
		cdb event log							<name of="" policy<="" td=""><td></td></name>	
		for object							Package which is	
43195.08735 xxxxxdtpl12 m	ny_adom	changed	FL1000T	FGVM010000102012	2 dm	12021022	David, Miller	<log_id_cfg_sync></log_id_cfg_sync>	installed>	Notice
		cdb event log							<name of="" policy<="" td=""><td></td></name>	
		for object						<log_id_update_n_< td=""><td>Package which is</td><td></td></log_id_update_n_<>	Package which is	
4/6/2018 2:05 xxxxxxdtpl13 m	ny_adom	changed	FL100MK	FGVM010000102023	dm	12021002	Maria, Lou	export_db>	installed>	Error



 FortiManager - Device Manager operations – This report includes events related to FortiManager device activities.



								Policy package				
Log Time	• 💌	Computer 🔽	User 🔻	Action name 🛛 🔽	ADOM r 🔻	Description 💌	Device name	🛛 Device serial num 💌	Log ID 🛛 💌	Message 🗾 💌	name 🗾 💌	Priority 🔽
	cdb event log							<name of="" policy<="" th=""><th></th></name>				
				<action th="" towards<=""><th></th><th>for object</th><th></th><th></th><th></th><th><log_id_dvmlog_< th=""><th>Package which is</th><th></th></log_id_dvmlog_<></th></action>		for object				<log_id_dvmlog_< th=""><th>Package which is</th><th></th></log_id_dvmlog_<>	Package which is	
4/6/2018	8 2:05	xxxxxxdtpl09	Karen	this device>	my_adom	changed	xxxxxxdtpl09	FGVM010000102012	22031004	emerg>	installed>	Emergency
						cdb event log					<name of="" policy<="" th=""><th></th></name>	
				<action th="" towards<=""><th></th><th>for object</th><th></th><th></th><th></th><th><log_id_dvmlog_< th=""><th>Package which is</th><th></th></log_id_dvmlog_<></th></action>		for object				<log_id_dvmlog_< th=""><th>Package which is</th><th></th></log_id_dvmlog_<>	Package which is	
4/7/2018	8 2:05	xxxxxxdtpl10	Peter	this device>	my_adom	changed	xxxxxxdtpl10	FGVM010000102012	220310047	error>	installed>	Error

#### Figure 3

• FortiManager - FGFM protocol operations - This report includes events related to FortiGate-FortiManager protocol operations.

Log Time 🛛 💌	Computer 🔽 L	Log ID 🔄	Device name 💌	User name 💌	Description 🔽	Offline mode 💌	Message 🗾
4/5/2018 2:05	xxxxxxdtpl21	2011003	FL1000T	Mathew	cdb event log for object changed		<log_id_connection_down></log_id_connection_down>
4/6/2018 2:05	xxxxxdtpl12	2011004	FL1000B	John	cdb event log for object changed	<enabled></enabled>	<log_id_offline_mode></log_id_offline_mode>

### Figure 4

• FortiManager - web service (Login Error) – This report provides the summary of events like web UI connection established, login error or login notification.

Log Time 🛛 💌	Computer 💌	ADOM name 💌	Log ID 🛛 💌	User name 💌	Description 💌	Remote host 💌	Message 🗾
4/6/2018 2:05	i xxxxxdtpl09	my_adom	23032003	Karen	cdb event log for object changed	example.com	<log_id_login_error></log_id_login_error>
4/7/2018 2:05	5 xxxxxdtpl10	my_adom	23032004	Brenden	cdb event log for object changed	example.com	<log_id_login_notif>,</log_id_login_notif>

### Figure 5

• FortiManager – Device configuration changes/ operations – Device configuration operation includes events where the new configuration is added of updated on the existing objects.

Log Time 🛛 🔽 Computer 🔽	🛛 Log ID 💌 Event subtype 💌	User name 💌	Description 🔽	Message 🗾	Priority 💌
4/2/2018 14:05 xxxxxdtpl12	3012002 devcfg	Matt, Henry	cdb event log for object changed	LOG_ID_installcmd	notice
4/3/2018 15:05 xxxxxdtpl13	3012002 devcfg	George, Philip	cdb event log for object changed	LOG_ID_installcmd	notice

### Figure 6

 FortiManager - Managed device operations – Managed device operations include events such as unexpected/ unplanned reboot and shut down by Forti devices.

				Event				
Log Time 🛛 💌	Computer 💌	Description 🔤	Device name 💌	subtype 💌	Log ID 💌	Login user from	Message	<ul> <li>Priority</li> </ul>
4/3/2018 15:15	xxxxxdtpl12	cdb event log for object changed	xxxxxxdtpl12	devops	27036002	<login from<="" session="" td="" user=""><td>&gt; LOG_ID_reboot</td><td>critical</td></login>	> LOG_ID_reboot	critical
4/3/2018 16:05	xxxxxdtpl13	cdb event log for object changed	xxxxxxdtpl13	devops	27036003	<login from<="" session="" td="" user=""><td>&gt; LOG_ID_shutdow</td><td>n critical 🔒</td></login>	> LOG_ID_shutdow	n critical 🔒

#### Figure 7

• FortiManager - High Availability events – High availability events are the events considered for a peer/ backup device for primary FortiManager appliance. This report will display the peer devices up/ down status (if any).

l	Log Time	-	Computer 💌	Description	🕶 module 🛛 💌	HA peer serial number 💌	Message 🔽	Interface status 💌	HA down cause 💌
E				cdb event log for	<identifier ha<="" of="" td="" the=""><td><serial ha<="" number="" of="" td=""><td>LOG_ID_status</td><td>;</td><td></td></serial></td></identifier>	<serial ha<="" number="" of="" td=""><td>LOG_ID_status</td><td>;</td><td></td></serial>	LOG_ID_status	;	
L	4/2/2018	14:05	xxxxxxdtpl12	object changed	Sync Module>	peer>	_chg_down	<ha status=""></ha>	<reason causes="" down="" ha="" status="" that=""></reason>
I				cdb event log for	<identifier ha<="" of="" td="" the=""><td><serial ha<="" number="" of="" td=""><td>LOG_ID_status</td><td>;</td><td></td></serial></td></identifier>	<serial ha<="" number="" of="" td=""><td>LOG_ID_status</td><td>;</td><td></td></serial>	LOG_ID_status	;	
L	4/3/2018	14:05	xxxxxxdtpl13	object changed	Sync Module>	peer>	_chg_up	<ha status=""></ha>	<reason causes="" down="" ha="" status="" that=""></reason>

#### Figure 8

• FortiManager - System manager events – System management includes events associated with the devices/ system present in the network or associated with FortiManager.

			Device_					System reboot	System shutdown	
Log Time	🕶 Computer 💌	Log ID 💌	name 💌	IP address 💌	Description 📃 💌	User name 💌	Message 🔽	reason 🔄	reason 💌	Operation result 💌
					cdb event log for		<log_id_logi< td=""><td></td><td></td><td></td></log_id_logi<>			
4/5/2018 14:0	5 xxxxxdtpl12	1010018	FL1000B	30.23.145.221	object changed	John	n_info>			<operation result=""></operation>
							<log_id_ssh_< td=""><td></td><td></td><td></td></log_id_ssh_<>			
					cdb event log for		auth_login_fa			
4/6/2018 14:0	5 xxxxxdtpl13	1010014	FL100CH	30.23.145.222	object changed	Jimmy	ilure>			<operation result=""></operation>
					cdb event log for		<log_id_reb< td=""><td><the for<="" reason="" td=""><td></td><td></td></the></td></log_id_reb<>	<the for<="" reason="" td=""><td></td><td></td></the>		
4/6/2018 14:0	5 xxxxxxdtpl13	1010014	FL100GQ	30.23.145.223	object changed	Karen	oot>	system reboot>		<operation result=""></operation>
					cdb event log for		<log_id_shut< td=""><td></td><td></td><td></td></log_id_shut<>			
4/6/2018 14:0	5 xxxxxxdtpl13	1010014	FL100CA	30.23.145.224	object changed	Bob	down>		<power failure=""></power>	<operation result=""></operation>

Figure 9

### 4.2 Alerts

- FortiManager: Unexpected system reboot
- FortiManager: Log daemon fluctuated
- FortiManager: Unexpected device reboot
- FortiManager: Unexpected device shutdown
- FortiManager: Unexpected system shutdown
- FortiManager: User login failed (SSH auth)
- FortiManager: User login failed (Web service)

# Netsurion... EventTracker

## 4.3 Saved searches

- FortiManager Device configuration operations (DEVCFG)
- FortiManager High Availability status changes
- FortiManager System login events
- FortiManager User login fail (Web service) by user
- FortiManager User login fail (SSH auth) detected
- FortiManager System manager events
- Top 10 FortiManager log types

### 4.4 Dashboards

• FortiManager - User login fail (Web service) by user



Figure 10





• FortiManager - User login fail (SSH auth) by user

Figure 11

### • FortiManager - High Availability status changes

FortiManager - High Availability status changes 🛛 🖉 – 🗙								
application_type	change_info	log_status						
Identifier of the HA Sync Module	Reason that causes HA status down	Operation Result						

### Figure 12

### • FortiManager - FGFM protocol status changes

FortiManager - FGFM protocol status changes							
event_datetime	device_name	log_info					
Sep 27 12:02:05 PM	FL1000B	LOG_ID_connection_down Warning					
Sep 25 12:21:49 PM	FL1000B	LOG_ID_reboot					

Figure 13

# Netsurion... EventTracker



### • FortiManager - System login events



### FortiManager - Managed device operations







• Top 10 FortiManager log types



Figure 16

# 5. Importing knowledge pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.

# Netsurion... EventTracker



Figure 17

🐁 Export Import Utility					
Export Import					
<ol> <li>Provide the path and file name of the Categories file. Use the '' button to 2. Click the Import button.</li> </ol>					
Options					
<ul> <li>Category</li> </ul>					
0.00					



### 3. Click the Import tab.

### 5.1 Categories

- 1. Once you have opened "Export Import Utility" via "EventTracker Control Panel", click the Category option, and then click the browse... button.
- Navigate to the knowledge pack folder and select the file with the extension ".iscat", e.g. "Categories\_FortiManager.iscat" and then click on the "Import" button:



4	Export Import Utility				_		$\times$
E	Export Import						
	1. Provide the path and file nar 2. Click the Import button.	me of the Catego	ies file. Use the '' button to brows	e and locate the import file.			
	Options Category Filters Alerts	Location	Source -				
	<ul> <li>Systems and Groups</li> <li>Token Value</li> <li>Reports</li> <li>Behavior Correlation</li> </ul>		Source : *jscat				
				In	nport	Close	e

Figure 19

EventTracker displays a success message:





## 5.2 Alerts

- 1. Once you have opened "Export Import Utility" via "EventTracker Control Panel", click Alert option, and then click the browse button.
- Navigate to the knowledge pack folder and select the file with the extension ".isalt", e.g. "Alerts\_ FortiManager.isalt" and then click on the "Import" button:



Export Import Utility			×
Export Import			
1. Provide the path and file na 2. Click the Import button.	me of the Alerts file. Use the '' but	on to browse and locate the import file.	
Options	Location		
Category	Import E-mail settings		
	Set Active	T	
<ul> <li>Filters</li> </ul>	<ul> <li>Only if notifications set</li> </ul>	Alert files. For v7, the active status will be set based on	
Alerts	O By default	"Active" key available in the configuration section.	
O Systems and Groups	Watchlist Configuration		
	Import Watchlist configurat	ion	
	This setting is applicable only f	or alerts which have Advanced watchlist configured.	
◯ Reports	on the console where the alert	s are imported.	
O Behavior Correlation			
	Source :		
	*.isalt	· · · · · ·	
			~
		Import	Close



EventTracker displays a success message:





### 5.3 Token Templates

For importing "Token Template", please navigate to EventTracker manager web interface.

1. Click Parsing Rules under the Admin option in the EventTracker manager web interface.







Next, click the "Template" tab and then click the "Import Configuration" button.

Parsing Rules	S		
Parsing Rule	Template		
Groups		<b>(+)</b>	Group :
Default		<b>^</b>	
Azure Intune		0	Templa







Now, click the "Browse" button and navigate to the knowledge packs folder (type C:\Program Files
(x86)\Prism Microsystems\EventTracker\Knowledge Packs" in the navigation bar) where ".ettd", e.g.
"Templates\_FortiManager.ettd" file is located. Wait for a few seconds, as templates will be loaded.
Once you see the templates, click desired templates and click "Import" button:



Import	
Select file Note: Please select	file of type *.ettd (eventtracker template dashlets).



## 5.4 Flex Reports

1. In the EventTracker control panel, select "Export/ Import utility" and select the "Import tab". Then, click Reports option, and choose "New (\*.etcrx)":

Export Import Utility		—		$\times$
Export Import				
1. Provide the path and file nam 2. Click the Import button Note : If report(s) contains templ	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility.			
Options	Location			
Category				
) Filters				
◯ Alerts	O Legacy (*issch)  New (*.etcnx)			
O Systems and Groups	Source :			
🔿 Token Value				
Reports				
O Behavior Correlation				
	Import		Clos	se



Once you have selected "New (\*.etcrx)", a new pop-up window will appear. Click the "Select File" button and navigate to the knowledge pack folder and select file with the extension ".etcrx", e.g. "Reports\_FortiManager.etcrx".

다 Reports Import					
Note : If report(s) contains template, first import temp Select file	ate and proceed with report import proce	SS.			Select file
Title	Frequency Show a		Q Q		
	Sites Groups	Systems	Frequency	Runtime	Туре

### Figure 28

3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click the **Imports** button.

Note: Set run time option is not applicab	le for Defined Reports and Hourly Reports	
Set run time for report(s) from	AM • at interval of _ minutes	Set
Replace	to Replac	e Assign systems
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.



EventTracker displays a success message:

Export Import Utility	×
Selected reports configurations are imported successfu	illy
ОК	



## 5.5 Knowledge Objects

1. Click Knowledge objects under the Admin option in the EventTracker manager web interface.



			🔎 🛛 Admin 🗸	Tools 👻 🌔
	Active Watch Lists	Event Filters	🧭 Parsing Rules	<b>†</b> / Da
	Alerts	Eventvault	Report Settings	
	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
	Behavior Correlation Settings	Group Management	QQ Users	
mi or so	Casebook Configuration	Q IP Lookup Configuration	T Weights	Systems since the last 24 hou
	● Category	· 🔆 Knowledge Objects	Windows Agent Config	
	▲ Diagnostics	Manager		



2. Next, click the "import object" icon:





 A pop-up box will appear, click "Browse" in that and navigate to knowledge packs folder (type "C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs" in the navigation bar) with the extension ".etko", e.g. "KO\_FortiManager.etko" and then click "Upload" button.

Import	
KO_ <product name="">.etko</product>	🗁 Browse Upload

### Figure 33

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the "**Import**" button:





Figure 2

## 5.6 Dashboards

- 1. Login to the EventTracker manager web interface.
- 2. Navigate to **Dashboard**  $\rightarrow$  **My Dashboard**.
- 3. In "My Dashboard", Click Import Button:



Figure 35



### Figure 36

 Select the browse button and navigate to the knowledge pack folder (type "C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs" in the navigation bar) where ".etwd", e.g. "Dashboard\_FortiManager.etwd" is saved and click on "Upload" button.



5. Wait while EventTracker populates all the available dashboards. Now, choose "Select All" and click on "Import" Button.

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with imp <u>orting dashlet.</u>	
🗁 Browse	Upload
Available widgets	
Select All	



	Import



# 6.Verifying knowledge pack in EventTracker

## 6.1 Categories

- 1. Login to the EventTracker manager web interface.
- 2. Click Admin dropdown, and then click Categories.
- 3. In **Category Tree** to view imported categories, scroll down and expand **"FortiManager"** group folder to view the imported categories:



Category
Category Tree Search
All Categories     All error events     All information events     All warning events     Security: All security events
<ul> <li>FortiManager</li> <li>FortiManager - High Availability status</li> <li>FortiManager - system login events</li> <li>FortiManager - System manager event</li> <li>FortiManager - User login fail (Web se</li> <li>FortiManager - Device configuration c</li> <li>FortiManager - User login fail (SSH au</li> <li>Top 10 FortiManager log types</li> </ul>

Figure 39

## 6.2 Alerts

- 1. In the EventTracker manager web interface, click the Admin dropdown, and then click Alerts.
- 2. In the search box enter "FortiManager" and then click the Search button.

EventTracker displays an alert related to FortiManager:

Aler	S All						Search by	Alert name 🔻	<ul> <li>↑ Admin / Alerts</li> <li>FortiiManager</li> <li>Q</li> <li>Q</li> </ul>	
÷	Click 'Activate Now' after making all changes									
	Alert Name ∧	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To	
	ዮਊ FortiManager : unexpected system rebooted triggered	•							FortiManager 6.2.0 and later	
	ዮያ FortiManager: Log daemon fluctuation detected	٠							FortiManager 6.2.0 and later	
	දිරි FortiManager: unexpected device rebooted triggered	٠							FortiManager 6.2.0 and later	
	ዮۇ FortiManager: unexpected device shutdown triggered	٠							FortiManager 6.2.0 and later	
	ዮኞ FortiManager: unexpected system shutdown triggered	•							FortiManager 6.2.0 and later	
	අරි FortiManager: User login fail (SSH auth) detected	•							FortiManager 6.2.0 and later	
	ዮያ FortiManager: User login fail (Web service) detected	٠							FortiManager 6.2.0 and later	

Figure 40



## 6.3 Token Templates

- 1. In the EventTracker web interface, click the Admin dropdown, and then click "Parsing Rules".
- 2. In the "Template" tab, click on the "FortiManager" group folder to view the imported Token.

Parsing Rule	S							
Parsing Rule	Template							
Groups			<b>+</b>	Group : FortiManager		Search	Q	
FortiManager		Ī	Ø ^				_	J
				Template Name	Template D	escription	Added By	Added Date
				FortiManager	FortiManage	r	ETAdmin	Sep 27 03:33:07 PM

Figure 51

### 6.4 Flex Reports

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





- 2. In Reports Configuration pane, select the Defined option.
- 3. Click on the "FortiManager" group folder to view the imported reports.



Report Configuration			
Scheduled OQueued ODefined			
Report Groups	÷		Reports configuration: FortiManager
🔁 FortiManager 🛄	۲	*	
			Title
			FortiManager - Deployment configuration operations
			FortiManager - Test
		i.	FortiManager – Device configuration changes
			FortiManager - Deployment manager operations



## 6.5 Knowledge Objects

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
- 2. In the **Knowledge Object** tree, expand the **"FortiManager"** group folder to view the imported Knowledge objects.

Knowledge Objects			
Search objects	Q Q Activate Now		
Groups 🕀 🧭 🗓	Object name FortiManager		
FortiManager	Applies to Fortimanager 0.0.2 or Later		
FortiManager 🕜 🗓	Rules		

Figure 84

### 6.6 Dashboards

1. In the EventTracker web interface, Click on Home Button and select "My Dashboard".







2. In "FortiManager" dashboard you should be now able to see something like this:



Figure 106

