

Integrate FortiNAC

EventTracker v9.x and above

Publication Date: July 19, 2019

Abstract

This guide provides instructions to retrieve FortiNAC event logs and integrate it with EventTracker. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor FortiNAC.

Audience

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and FortiNAC v8.3 and v8.5.

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

Abstract	1
Audience	1
Overview	3
Prerequisites	3
Configuring FortiNAC to forward the log to EventTracker STEP 1: Enable "External" Logging	3 3
STEP 2: Adding "Log Host" server	4
EventTracker Knowledge Pack Flex Reports	5 5
Alerts	9
Dashboards	9
Saved Searches	11
Importing FortiNAC knowledge pack into EventTracker Categories	16 17
Alerts	18
Token Template	19
Flex Reports	20
Knowledge Object	23
Dashboard	24
Verifying FortiNAC knowledge pack in EventTracker Categories	27 27
Alerts	28
Token Template	28
Flex Reports	29
Knowledge Object	30
Dashboard	31



Overview

Network Access Control (NAC) is an approach to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), the user or system authentication and network security enforcement. FortiNAC provides visibility to all administrators to see everything connected to their network, as well as the ability to control those devices and users, including dynamic, automated responses.

EventTracker collects the event logs delivered from FortiNAC and filters them out to get some critical event types for creating reports, dashboard, and alerts. Among the even types, we are considering: Admin user login success/ failure, rogue MAC address detection, switch interface up/ down and host session login/ logout.

Prerequisites

- EventTracker agents should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on the host system/ server to run PowerShell.
- User must have root-level access to FortiNAC console.

Configuring FortiNAC to forward the log to EventTracker

The logs can be forwarded to EventTracker via configuring "syslog", SNMP trap or API to an external server. In this documentation, we will use syslog "CEF" format.

Integration is divided into 2 steps. STEP 1 for enabling **"External" logging**, and STEP 2 for adding **"Log Host server**".

STEP 1: Enable "External" Logging

- 1. Click Logs>Event Management.
- 2. Use the filters to locate the appropriate event.
- 3. For each event that should be logged externally, select one or more events and click the **Options** button. Select one of the following:
 - External—Logs only to an external host.
 - Internal & External—Logs both to an internal events database and an external host.



Netsurion EventTracker

STEP 2: Adding "Log Host" server

- 1. Click System > Settings.
- 2. In the tree on the left select System **Communication > Log Receivers**.
- 3. Click Add to add a log host.
- 4. Select "Type" field as "Syslog Command Event Format (CEF)"
- 5. Enter the IP address of the EventTracker server.
- 6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered.
- 7. Click **OK**.

4

Add Log H	lost	×
Туре:	Syslog CEF V	ø
IP Address:	192.168.10.100	6
Port:	514	6
Facility	Authorization 🔹	0
	ОК	Cancel



Field	Definition
Туре	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, and Syslog Command Event Format (CEF) .
IP Address	IP Address of the server that will receive event and alarm messages.
Port	Connection port on the server. For syslog CSV and syslog CEF servers, the default=514. For SNMP Trap servers the default=162
Facility	Displays only when syslog is selected as the Type. It allows you to configure the message type. The default is 4. Options include: 0 Kernel messages 1 User-level messages 2 Mail system 3 System daemons 4 Security/authorization messages 5 Messages generated internally by syslog 6 Line printer subsystem 7 Network news subsystem 8 UUCP subsystem 9 Clock daemon 10 Security/authorization messages 11 ETP daemon

Field	Definition
	12 NTP subsystem
	13 Log audit
	14 Log alert
	15 Clock daemon
	16 Local use 0 (local0)
	17 Local use 1 (local1)
	18 Local use 2 (local2)
	19 Local use 3 (local3)
	20 Local use 4 (local4)
	21 Local use 5 (local5)
	22 Local use 6 (local6)
	23 Local use 7 (local7)
Security String	Displays only when SNMP is selected as the type. The security string sent with the
	Event and Alarm message.

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support FortiNAC.

Flex Reports

• FortiNAC - Rogue MAC detected – This report will generate a detailed view on rogue MAC address connecting to an endpoint as detected by FortiNAC.

LogTime	Computer	MAC Address	Port Number	System Name
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	74:86:7A:E1:CD:8E	15	S448DF3X16000158
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	0C:C4:7A:82:AE:7D	6	S224DF3X15000024
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	70:4C:A5:5B:99:5E	Uplink_To_ISFW	Demo-ISFW-FIN wan1
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	00:50:56:A6:7A:26	26	S248EPTF18002331
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	74:86:7A:E1:CD:8C	14	S448DF3X16000158

Figure 2

Netsurion... EventTracker

Sample Logs:

dest_host_name	+- \$448DF3X16000158
event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37>Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Rogue Connected 1 rt=Jul 19 01:48:20 602 EDT cat=Network shost=NAC Director
	msg=Rogue Host 40:8D:5C:5E:BC:55 Connected to S448DF3X16000158:port17.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog

Figure 3

• FortiNAC - Admin user login success and logout – This report will generate a detailed view on login and logout activities users in FortiNAC console.

LogTime	Computer	Log Type	User Name
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Login Success	Bob
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	User Logged Out	root
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Login Success	Brenden
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Login Success	ETAdmin
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Login Success	Gary
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	User Logged Out	Karen
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	User Logged Out	Sophie
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	User Logged Out	Brenden

Figure 4

Sample Logs:

event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Login Success 1 rt=Jul 22 11:26:20 602 EDT cat=Network shost=NAC Director ms
	g=User Karen logged in.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog



• FortiNAC - Admin user login fails – This report will generate a detailed view on failed login activities performed on the FortiNAC admin console.

LogTime	Computer	User Name
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Gary
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Karen
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Philip
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	Brenden
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	root
07/08/2019 06:49:46 PM	NTPLDTBLR48@FORTINAC	qa

Figure 6

Sample Logs:

event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37>Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Login Failure 1 rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director ms
	g=User Bob failed to log in.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog

Figure 7

• FortiNAC - Host session login and logout – This report will generate a detailed view on "Host" (endpoint systems) login and logout activities.

LogTime	Computer	Log Type	System Name	User Name
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	User Logged onto Host	DESKTOP-KKGIBJT	Milton Collier
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	User Logged onto Host	BRADSUPP7-LT	Thomas
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	User Logged off Host	BRADSUPP7-LT	Brenden
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	User Logged onto Host	BRADSUPP7-LT	Maggie
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	User Logged off Host	BRADSUPP7-LT	Karen
07/08/2019 06:49:47 PM	NTPLDTBLR48@FORTINAC	User Logged onto Host	BRADSUPP7-LT	Bob



Sample Logs:

dest_host_name	+- BRADSUPP7-LT
event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37>Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 User Logged onto Host 1 rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Dir
	ector msg=User Thomas logged onto session 1 on host BRADSUPP7-LT.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog

Figure 9

• FortiNAC - Switchport link up-down – This report will generate a detailed view on endpoint network switch port/ interface up/ down status.

LogTime	Computer	Log Type	Interface Number	Port Number	System Name
07/09/2019 12:45:41 PM	NTPLDTBLR48@FORTINAC	Port Link Up	11	16	Demo-ISFW-ENG
07/09/2019 12:45:41 PM	NTPLDTBLR48@FORTINAC	Port Link Up	12		FLINK-AGG
07/09/2019 12:45:41 PM	NTPLDTBLR48@FORTINAC	Port Link Down	11	16	Demo-ISFW-ENG
07/09/2019 12:45:41 PM	NTPLDTBLR48@FORTINAC	Port Link Down	12		FLINK-AGG
07/09/2019 01:07:57 PM	NTPLDTBLR48@FORTINAC	Port Link Down	10	15	Demo-ISFW-ENG

Figure 10

Sample Logs:

device_name	+- Demo-ISFW-ENG	
event_category	+- 0	
event_computer	+- NTPLDTBLR48@FortiNAC	
event_datetime	+- 7/9/2019 1:07:57 PM	
event_datetime_utc	+- 1562657877	
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Port Link Up 1 rt=Jul 19 01:48:20 602 EDT cat=Network shost=NAC Director msg=	
	Link Up: Port Demo-ISFW-ENG port15 on Interface 10.	
event_id	+- 3230	
event_log_type	+- Application	
event_source	+- syslog	



Alerts

- FortiNAC Admin user login fails This alert will be triggered when a new event is detected as login failed while trying to access the FortiNAC admin console.
- FortiNAC Rogue MAC detected This event will be triggered when a new event for rogue/ suspicious MAC address is detected by FortiNAC.

Dashboards

• FortiNAC - Admin user login success (By User name)



FortiNAC - Admin user login success (By User name)

Figure 12



• FortiNAC - Admin user login fail (By User name)



Figure 13



• FortiNAC - Rogue MAC detected

Figure 14

Netsurion. EventTracker

• FortiNAC – Port link up/down

device_name	interface_in	log_type	src_port_no	
Demo-ISFW-ENG	10	Port Link Up	15	
FLINK-AGG	12	Port Link Down		
Demo-ISFW-ENG	11	Port Link Down	16	
Demo-ISFW-ENG	10	Port Link Down	15	
FLINK-AGG	12	Port Link Up		
Demo-ISFW-ENG	11	Port Link Up	16	
Demo-ISFW-ENG	10	Port Link Up	15	
FLINK-AGG	12	Port Link Up		
FLINK-AGG	12	Port Link Down		
Demo-ISFW-ENG	11	Port Link Up	16	

Figure 15

Saved Searches

Along with reports, alerts, and dashboards, EventTracker also provides a feature called "Saved Searches".

This feature allows an individual to retrieve only specific kinds of logs. Below are some saved searches which are included with FortiNAC integration with EventTracker:

• FortiNAC - Port link up/down

Sample logs:

Netsurion... EventTracker

FortiNAC Integration Guide

device_name	+- Demo-ISFW-ENG	
event_category	+- 0	
event_computer	+- NTPLDTBLR48@FortiNAC	
event_datetime	+- 7/9/2019 1:07:57 PM	
event_datetime_utc	+- 1562657877	
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Port Link Down 1 rt=Jul 19 01:48:20 602 EDT cat=Network shost=NAC Director ms	
	g=Link Down: Port Demo-ISFW-ENG port16 on Interface 11.	
event_id	+- 3230	
event_log_type	+- Application	
event_source	+- syslog	
event_type	+- Information	
event_user_domain	+- NA	
event_user_name	+- NA	
interface_in	+- 11	
log_category	+- Network	
log_datetime	+- Jul 19 01:48:20 602 EDT	
log_source	+- FortiNAC Events	
log_status	+- Link Down: Port Demo-ISFW-ENG port16 on Interface 11	
log_type	+- Port Link Down	
src_port_no	+- 16	
src_user_info	+- NAC Director	

Figure 16

• FortiNAC - Rogue MAC detected

Sample Logs:

dest_host_name	+- S224DF3X15000024
event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Rogue Connected 1 rt=Jul 19 01:48:20 602 EDT cat=Network shost=NAC Director
	msg=Rogue Host 90:2B:34:D4:AB:6B Connected to S224DF3X15000024:port4.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- NA
event_user_name	+- NA
log_category	+- Network
log_datetime	+- Jul 19 01:48:20 602 EDT
log_source	+- FortiNAC Events
log_status	+- Rogue Host 90:28:34:D4:AB:6B Connected to S224DF3X15000024:port4
log_type	+- Rogue Connected
src_mac_address	+- 90:2B:34:D4:AB:6B
src_user_info	+- NAC Director



• FortiNAC - Host session logged on

Sample Logs:

dest_host_name	+- BRADSUPP7-LT	
event_category	+- 0	
event_computer	+- NTPLDTBLR48@FortiNAC	
event_datetime	+- 7/9/2019 1:07:57 PM	
event_datetime_utc	+- 1562657877	
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 User Logged onto Host 1 rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Dir	
	ector msg=User Gary logged onto session 1 on host BRADSUPP7-LT.	
event_id	+- 3230	
event_log_type	+- Application	
event_source	+- syslog	
event_type	+- Information	
event_user_domain	+- NA	
event_user_name	+- NA	
log_category	+- Network	
log_datetime	+- Jul 22 11:24:20 602 EDT	
log_source	+- FortiNAC Events	
log_status	+- User Gary logged onto session 1 on host BRADSUPP7-LT	
log_type	+- User Logged onto Host	
src_user_info	+- NAC Director	
src_user_name	+- Gary	

Figure 18

• FortiNAC - Host session logged off

Sample Logs:

dest_host_name	+- BRADSUPP7-LT
event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 User Logged off Host 1 rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Direc
	tor msg=User Gary logged off session 1 on host BRADSUPP7-LT.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- NA
event_user_name	+- NA
log_category	+- Network
log_datetime	+- Jul 22 11:24:20 602 EDT
log_source	+- FortiNAC Events
log_status	+- User Gary logged off session 1 on host BRADSUPP7-LT
log_type	+- User Logged off Host
src_user_info	+- NAC Director
src_user_name	+- Gary



• FortiNAC - Admin user logout

Sample Logs:

event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 User Logged Out 1 rt=Jul 22 11:26:20 602 EDT cat=Network shost=NAC Director
	msg=User Brenden Logged Out.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- NA
event_user_name	+- NA
log_category	+- Network
log_datetime	+- Jul 22 11:26:20 602 EDT
log_source	+- FortiNAC Events
log_status	+- User Brenden Logged Out
log_type	+- User Logged Out
src_user_info	+- NAC Director
src_user_name	+- Brenden

Figure 20

• FortiNAC - Admin user login success

Sample Logs:

event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Login Success 1 rt=Jul 22 11:26:20 602 EDT cat=Network shost=NAC Director ms
	g=User Karen logged in.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- NA
event_user_name	+- NA
log_category	+- Network
log_datetime	+- Jul 22 11:26:20 602 EDT
log_source	+- FortiNAC Events
log_status	+- User Karen logged in
log_type	+- Login Success
src_user_info	+- NAC Director
src_user_name	+• Karen



• FortiNAC - Admin user login fail

Sample Logs:

event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Login Failure 1 rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director ms
	g=User Bob failed to log in.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- NA
event_user_name	+- NA
log_category	+- Network
log_datetime	+- Jul 22 11:24:20 602 EDT
log_source	+- FortiNAC Events
log_status	+- User Bob failed to log in
log_type	+- Login Failure
src_user_info	+- NAC Director
src_user_name	+- Bob

Figure 22

• FortiNAC - SNMP fail

Sample Logs:

dest_host_name	+- FWLC-DEMO
event_category	+- 0
event_computer	+- NTPLDTBLR48@FortiNAC
event_datetime	+- 7/9/2019 1:07:57 PM
event_datetime_utc	+- 1562657877
event_description	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 SNMP Failure 1 rt=Jul 19 01:48:20 602 EDT cat=Network shost=NAC Director ms
	g=SNMP failed for device FWLC-DEMO with message 10.88.51.12 SNMP V1/V2c get failed.
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- NA
event_user_name	+- NA
log_category	+- Network
log_datetime	+- Jul 19 01:48:20 602 EDT
log_source	+- FortiNAC Events
log_status	+- SNMP failed for device FWLC-DEMO with message 10
log_type	+- SNMP Failure
src_user_info	+- NAC Director



Importing FortiNAC knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

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



Figure 24



🐁 Export Import Utility	
Export Import	
1. Provide the path and file na 2. Click the Import button.	ame of the Categories file. Use the '' button to
Options	Location

Figure 25

3. Click the **Import** tab.

Categories

- 1. Click the **Category** option, and then click the **Browse** button.
- 2. Navigate to the location having a file with the extension ".iscat" and then click on the "Import" button:

Export Import Utility						—		\times
Export Import								
1. Provide the path and file na 2. Click the Import button.	me of the Catego	ories file. U	se the '' button to b	prowse and locate the	import file.			
Options Options Category Filters 	Location							
○ Alerts								
Systems and Groups		Source :	ntegration\Configura	ation Items\Category	iscat			
O Token Value								
O Reports								
Behavior Correlation								
					Impo	rt	Close	•

Figure 26

3. EventTracker displays a success message:







Alerts

- 1. Click **Alert** option, and then click the browse button
- 2. Navigate to the location having a file with the extension ".isalt" and then click on the "Import" button:



Figure 28

3. EventTracker displays a success message:





Figure 29

Token Template

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager page.



Figure 30

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

Parsing Rules	5			
Parsing Rule	Template			
Groups			+	Group :
Default				
Azure Intune		1	0	Templa

Figure 31



^	/ Admin / Parsing Rules
	C 1
Active	Import configuration



3. Now, click the "**Browse**" button and navigate to the folder where the ".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:

Impo	rt					
select	ed file is: Template_FortiNAC.ett	d	1 🖙 Browse			Ctrl) -
	Template name	Separator	Template description	Added date	Added by	Group Name
	FortiNAC	\n	<37> Jul 22 11:24:20 : CEF:0 Fortinet NAC Control Server 4.1.1.219.P9 6111 Rogue Connected 1 rt=Jul 19 01:48:20 602 EDT cat=Network shost=NAC D irector msg=Rogue Host 90:28:34:D4:A8:68 Connected to S224DF3X 15000024:port4.	Jul 09 03:51:26 PM	ETAdmin	FortiNAC

Figure 33

Flex Reports

 In 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				
Export Import 1. Provide the path and file na 2. Click the Import button Note : If report(s) contains term Options Octategory Filters Alerts Systems and Groups Token Value Import Behavior Correlation	ame of Schedule Report file. Use the '' button to browse and locate the import f nplate, first import template and proceed with exportimport utility. Location Legacy (*.issch) Image: Source : *.issch	file.		
		Import	Clos	e

- 2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click the "**Select File**" button and navigate to the file path with a file having the extension "**.etcrx**".
- 3. Select all the relevant files and then click the **Import** button.

ş			Select file	
	Frequency Show all	- Q Q		
Title	Sites	Groups	Systems	Frequency
FortiNAC - Admin user login fails	NTPLDTBLR48	Default	NTPLDTBLR48@FortiNAC	Undefined
FortiNAC - Admin user login success a	NTPLDTBLR48	Default	NTPLDTBLR48@FortiNAC	Undefined
FortiNAC - Host session login and logout	NTPLDTBLR48	Default	NTPLDTBLR48@FortiNAC	Undefined
FortiNAC - Rogue MAC detected	NTPLDTBLR48	Default	NTPLDTBLR48@FortiNAC	Undefined
FortiNAC - Switchport link up-down	NTPLDTBLR48	Default	NTPLDTBLR48@FortiNAC	Undefined
				>
	Title FortiNAC - Admin user login fails FortiNAC - Admin user login success a FortiNAC - Host session login and logout FortiNAC - Rogue MAC detected FortiNAC - Switchport link up-down	Title Sites FortiNAC - Admin user login fails NTPLDTBLR48 FortiNAC - Admin user login success a NTPLDTBLR48 FortiNAC - Host session login and logout NTPLDTBLR48 FortiNAC - Rogue MAC detected NTPLDTBLR48 FortiNAC - Switchport link up-down NTPLDTBLR48	Title Sites Groups FortiNAC - Admin user login fails NTPLDTBLR48 Default FortiNAC - Admin user login success a NTPLDTBLR48 Default FortiNAC - Host session login and logout NTPLDTBLR48 Default FortiNAC - Rogue MAC detected NTPLDTBLR48 Default FortiNAC - Switchport link up-down NTPLDTBLR48 Default	Title Sites Groups Systems FortiNAC - Admin user login fails NTPLDTBLR48 Default NTPLDTBLR48@FortiNAC FortiNAC - Admin user login success a NTPLDTBLR48 Default NTPLDTBLR48@FortiNAC FortiNAC - Admin user login and logout NTPLDTBLR48 Default NTPLDTBLR48@FortiNAC FortiNAC - Host session login and logout NTPLDTBLR48 Default NTPLDTBLR48@FortiNAC FortiNAC - Rogue MAC detected NTPLDTBLR48 Default NTPLDTBLR48@FortiNAC FortiNAC - Switchport link up-down NTPLDTBLR48 Default NTPLDTBLR48@FortiNAC

Figure 35

4. EventTracker displays a success message:

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





Knowledge Object

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

		🔎 Admin -	Tools 🕶 (
Active Watch Lists	Event Filters	🧭 Parsing Rules	🔒 / Da
Alerts	Second Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
ns Casebook Configuration	Q IP Lookup Configuration	🕀 Weights	Systems since the last 24 hour
Category	·☆ Knowledge Objects	Windows Agent Config	_
Diagnostics	Manager		

Figure 37

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

Admin / Knowledge Objects
Objects 🕀 丁 🏦 🏟
Import Objects



- 3. A pop-up box will appear, click "**Browse**" in that and navigate to the file path with the extension ".etko" and then click the "upload button".
- 4. A list of available Knowledge objects will appear. Select the relevant files and click the "Import" button.



Import			×
Select file			🗁 Browse
	Object name	Applies to	Group name
	FortiNAC Events	FortiNAC	FortiNAC
			Import Close

Figure 39

Dashboard

- 1. Login to EventTracker.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.
- 3. In "My Dashboard", click Import Button:

Netsurion EventTracker

≡	Event Tracker ⊕
	Home
٩	My Dashboard
R	Threats
	Incidents
	Behavior Correlation
	Change Audit
	Compliance



Figure 41

- 4. Select the **browse** button and navigate to the file path where the Dashboard file is saved and click on the "**Upload**" button.
- 5. Once completed, choose "**Select All**" and click on "**Import**" Button.



S Import dashlets - Google Chrome			×
O localhost:8080/EventTracker/Flex/ImportWidget.aspx			Ð
Import			*
Note: If dashlet configured using persisted report, first import the report and proceed with importing das Brow Available widgets	shlet.	Upload	
 Select All FortiNAC - Admin user log FortiNAC - Admin user log FortiNAC - Rogue MAC dete 			
FortiNAC - Port link up/d			
	Import	Close	

Figure 42

6. Next, click "Customize dashlet" button as shown below:





7. Now, put a text on the **Search bar: "Fortinac"** and then select the FortiNAC Dash-lets and then click the **"Add"** button.

Customize dashlets			×
fortinac			Q
🗹 FortiNAC - Admin user login fail	FortiNAC - Admin user login su	FortiNAC - Port link up/down	FortiNAC - Rogue MAC detected
80			
			Add Delete Close

Figure 44

Verifying FortiNAC knowledge pack in EventTracker

Categories

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

	entTracker
- 🕞 F5	BIG IP
- 🕞 F5	BIG IP LTM
Fo	rtiMail
Fo	rtiNAC
-6	FortiNAC admin user login fail
E	FortiNAC admin user login success
-6	FortiNAC admin user logout
-6	FortiNAC host session logged off
-6	FortiNAC host session logged on
E	FortiNAC port link up/down
-6	FortiNAC rogue MAC detected
G	East NAC SNIMD Fail

Figure 45

Alerts

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Alerts.
- In search box enter "Forti" and then click the Search button.
 EventTracker displays an alert related to "FortiNAC":

Alerts Show All •						Search by Alert n	ame 🔻	fortinac
290 Available Alerts Total number of alerts available	51 Active Alerts Total number of active alerts			290 System/User De Count for system and	System User efined Alerts User defined alerts	152	290 Alerts by Th Count of alerts	Critical 18 144 international Control
Click 'Activate Now' after mak	ing all changes							Total: 2 Page Size 25 ▼
Alert Name A	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
🗷 🖧 FortiNAC - Admin user login fails								FortiNAC v8.3 and v8.5
Ø ₿Ø FortiNAC - Rogue MAC detected								FortiNAC v8.3, and v8.5



Token Template

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



Parsing Rules	5						
Parsing Rule	Template						
Groups			÷		Group : FortiNAC		Search
Default				^			
Amazon AWS		Û	1		Template Name	Templat	e Description
Azure Intune		Û	0		FortiNAC	FortiNAC	:
Cisco		Û	Ø				
EDR		Û	0				
EventTracker		Û	0	l.			
F5 BIG IP		Û	0				
FortiNAC		Û	Ø				
JumpCloud		Ü	0				

Figure 47

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 **FortiNAC** group folder to view the imported reports.

Repor	rt Groups		Ð	000	Repo	orts configu	uration: FortiNAC
0	Operations			^	Ð	∅ ∂,	
0	Flex				0		Title
B	ADManager Plus	Ē	Ø	1000			FortiNAC - Rogue MAC detected
	All Compliance Repor	Ē	Ø				FortiNAC - Admin user login success and logou
٦	All Operations Repor	١ <u>ا</u>	1			(E)	FortiNAC - Admin user login fails
D	All Security Audit R	i i	1			(F)	FortiNAC - Host session login and logout
۵	All Threat Report	Ĩ	1			562	FortiNAC - Switchport link up-down
۵	EventTracker	1	1		Ē	w	
	F5 BIG IP	前	Ø	L.			
	FortiMail	Ē	1	Ш			
	FortiNAC	前	Ø				

Figure 49

Knowledge Object

Report Configuration

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

Knowledge Objects							
Search objects	Q Q Activate Now						
Groups 🕀 🧭 🗓	^						
FortiNAC							



Dashboard

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





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

FortiNAC - Admin user login success (By User name)



Figure 49

