

# Integration Guide for NetMotion Mobility EventTracker v9.x and later

Publication Date: April 16, 2020

### Abstract

This guide provides instructions to retrieve the **NetMotion Mobility** events by syslog configuration. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **NetMotion Mobility**.

### Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **NetMotion Mobility.** 

### Audience

Administrators who are assigned the task to monitor **NetMotion Mobility** 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 Cisco Firepower threat defense (FTD) 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.

© 2020 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	requisites	. 3
3.	Inte 3.1	egrating NetMotion Mobility with EventTracker Configuring a Syslog Server	. 3 . 3
4.	Eve 4.1	ntTracker Knowledge Packs Alerts	. 4 . 4
	4.2	Saved Searches	. 4
	4.3	Reports	. 5
	4.4	Dashboards	. 6
5.	Imp 5.1	orting knowledge pack into EventTracker Saved Searches	. 9 10
	5.2	Alerts	11
	5.3	Parsing Rules1	12
	5.4	Token Template	13
	5.5	Reports1	15
	5.6	Knowledge Objects1	16
	5.7	Dashboards	17
6.	Ver	ifying knowledge pack in EventTracker1	19
	6.1	Saved Searches1	19
	6.2	Alerts	20
	6.3	Token Template	20
	6.4	Reports	21
	6.5	Knowledge Objects	22
	6.6	Dashboards	23



## 1. Overview

NetMotion Mobility is a mobile VPN software, designed specifically for wireless environments. NetMotion Mobility provides IT managers with the security and centralized control to effectively manage a mobile deployment.

EventTracker, when integrated with NetMotion Mobility, collects log from NetMotion Mobility and creates a detailed reports, alerts, dashboards and saved searches. This KP (knowledge Pack) provides detailed information about the User logon failure, in real time. It is helpful to investigate and take responsive actions against Brute-Force Attack.

EventTracker provides a thorough information about policies such as pending policies that must be applied and the policies that have been applied. It also provides information related to Proxy events which contain many important information such as source user, source IP address and session ID. Sessions can be monitored to identify details of user logon and logoff success required for Auditing.

Alerts are provided for critical events such as user logon failure to identify logon attempt. Using the EventTracker's Dashboards we can view and monitor events like user logon events (success, failed), user policy details, user/group management, etc.

## 2. Prerequisites

- EventTracker manager v9.x is required.
- Enable external logging on your NetMotion Mobility appliance.
- Allow Port 514 in the firewall.

## 3. Integrating NetMotion Mobility with EventTracker

NetMotion Mobility can be integrated with EventTracker using syslog forwarding.

### 3.1 Configuring a Syslog Server

The NetMotion Mobility server can send NetMotion Mobility events to EventTracker. NetMotion Mobility support for syslog is only implemented on the NetMotion Mobility server; the NetMotion Mobility client cannot log messages to a syslog server.

#### To log NetMotion Mobility events to EventTracker:

- 1. Go to **Mobility console > Configure > Server Settings**.
  - In the left-hand pane, select the level at which you want to configure logging:
  - To apply the setting to all Mobility servers in a server pool, select **Global Server Settings**.

• To apply the setting to a single server, select the name of the Mobility server you want to configure. Settings applied at the server level take precedence over global settings.

Configure the following settings:

- Select **Syslog On/Off**, and then select the Turn syslog event logging on check box. This enables a Mobility server to log Mobility events to a syslog server. Any information, warning, or error events that are recorded in the Mobility event log are also sent to syslog. However, the Mobility server does not log debug events to syslog. To record debug events, use the Mobility event log.
- Select Syslog Server Host. In the Host box, enter the host name or IP address of the EventTracker.
- 2. By default, the syslog protocol uses UDP **port 514**. To configure the Mobility server to use a different port, select Syslog Server Port in the list of settings. In the Port box, enter the syslog server port.
- 3. In a syslog message, the facility identifies the type of software component that generated the message. Some facilities are reserved for the operating system, or for types of applications (for example, email). Applications that are not assigned a facility can use a "local use" facility, which is not reserved.

## 4. EventTracker Knowledge Packs

### 4.1 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as,

• **NetMotion – Login Failure –** This alert is triggered when the NetMotion Mobility detects a login failure event.

### 4.2 Saved Searches

- **NetMotion Login Failed:** This Saved Search provides information related to a login failure event. It includes information such username, hostname and the reason for login failure.
- **NetMotion Login Logout Events:** This Saved Search provides information related to login and logout events generated by NetMotion Mobility.
- NetMotion Policy Activities This Saved Search provides information related to Policy activities.
- NetMotion Proxy Event: This Saved Search provides information related to Proxy Activities.
- **NetMotion Directory Activity –** This Saved Search provides information related to directory activities such as user added or deleted from group etc.



### 4.3 Reports

NetMotion – Login Failed: This report generates a summary of login failure event. It includes
information such username, hostname and the reason for login failure.

LogTime	Computer	Username	Hostname	Reason
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	AD\James	IFS-HP-REMOTE3	The user name or password is incorrect
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	AD\Adam	IFS-HP-REMOTE2	The user name or password is incorrect
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	AD\Leo	UTL18106L	The user name or password is incorrect
04/09/2020 01:01:44 PM	172.27.100.9-SYSLOG	AD\James	IFS-HP-REMOTE3	The user name or password is incorrect

#### Figure 1

 NetMotion – Login Logout Events: This report generates a summary of login and logout events generated by NetMotion Mobility. It includes username, roles of the user group the user belongs to, and the action performed i.e. login or logout.

LogTime	Computer	Username	Role	Group	Action
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\administrator	Super User		logon
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\Adam	Super User		logon
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\Joey	Client Administration	is_admin	logged on
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\administrator			logged off
04/09/2020 01:01:44 PM	172.27.100.9-SYSLOG	ad\administrator	Super User		logon
04/09/2020 01:01:44 PM	172.27.100.9-SYSLOG	ad\Leo	Client Administration	is_admin	logged on

#### Figure 2

• NetMotion – Policy Activities – This report contains a summary of Policy activities. It includes the username, device on which the policy was applied and the name of the policy along with the message regarding the status.

LogTime	Computer	Username	Device	Policy	Message
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\Joey	01D602C4C6BE193900505697E7B 2020		Client not subscribed to a policy and is already running without policy, no policy download will be attempted
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\Adam	01D5FC688808EEE000505697E7B 200B	Global_Policy	Policy (Global_Test_Policy), NAC (None) on client is current, it will not be downloaded
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\Mike	01D5FC688808EEE000505697E7B 200B	Admin_Policy	Policy (Global_Test_Policy), NAC (None) on client is current, it will not be downloaded

#### Figure 3

• NetMotion – Proxy Event: This report has a summary of Proxy activities. This includes hostname, session ID, Message, source IP address and the username.



LogTime	Computer	Hostname	IMP Session ID	Message	Reason	Source IP Address	Username
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	UTL18061L	0xebeaf4a	Client PID request			
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG			Client PIDGEN RPC session indication			
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebe9f4a	[605] Client XG RPC session indication		10.30.99.30	AD\Martin
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebe944a	[601] Client XG RPC session termination indication	A server session was terminated because the client has established a new connection from the same device	10.30.99.30	
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebeae4a	[604] Client XG RPC session indication		10.30.99.19	AD\Adam
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0x00000000ebe9e4a	Client PID accept			
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebea34a	\[597\] Client XG RPC session indication		10.30.99.35	AD\Joey
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebea14a	\[596\] Client XG RPC session termination indication	The Mobility Client is shutting down or restarting	10.30.99.35	
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebebe4a	\[617\] Client XG RPC session indication	User-initiated disconnect	10.30.99.57	AD\Ross

• **NetMotion** - **Directory Activity** – This report consists summary of Directory activities. It includes username, group on which the action was taken and the status.

LogTime	Computer	Username	Group	Action
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\John	New Users	added
04/12/2020 07:39:15 PM	172.27.100.9-SYSLOG	AD\Adam	New Users	added

Figure 5

### 4.4 Dashboards

• NetMotion: Login Failure



Netsurion. EventTracker\*



• NetMotion: Login Logout Activities

Figure 7

• NetMotion: Policy Details



Figure 8



#### • NetMotion: IMP Authentication by Geo Location



Netmotion - IMP Authentication by Geo location



#### • NetMotion: User added to group



Figure 10





#### • NetMotion: Proxy Login Logout Details by Source IP



## 5. Importing knowledge pack into EventTracker

#### How to get Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

- 1. Press "₩ + R".
- Now, type "%et\_install\_path%\Knowledge Packs" and press "Enter".

(**Note** – If, not able to locate the file path as mentioned above, please contact <u>EventTracker support</u> to get the assistance).

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects

Netsurion... EventTracker\*

- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.



Figure 12





3. Click the Import tab.

#### 5.1 Saved Searches

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



🐁 Export Import Utility					_		$\times$
Export Import							
1. Provide the path and file nar 2. Click the Import button.	me of the Catego	ries file. Use the '' bu	tton to browse and	locate the import f	le.		
Options Category Fiters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location	Source : *iscat					
					Import	Clos	ie

Figure 14

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 browse.
- 2. Navigate to the knowledge pack folder and select the file with extension ".isalt", e.g. "Alerts\_ NetMotion.isalt" and then click "Import":



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	ton to browse and locate the import file.					
Options	Location						
Category	Import E-mail settings						
	Set Active						
○ Filters	<ul> <li>Only if notifications set</li> </ul>	This setting is applicable only for imports from Legacy (v6x) 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	for alerts which have Advanced watchlist configured.					
O Reports	on the console where the alerts are imported.						
O Behavior Correlation							
	Source :						
	*.isalt						
		Import	e				
			_				

EventTracker displays a success message:





### 5.3 Parsing Rules

- 1. Once you have opened "Export Import Utility" via "EventTracker Control Panel", click the "Token Value" option, and then click browse
- 2. Navigate to the knowledge pack folder and select the file with extension ".istoken", e.g. "Parsing Rules\_ NetMotion.istoken" and then click "Import":



Export Import Utility		_		$\times$
Export Import				
1. Provide the path and file na 2. Click the Import button	me of token value file. Use the '' button to browse and locate the import file.			
Options	Location			
◯ Category				
⊖ Filters				
⊖ Alerts	Source -			
O Systems and Groups	*jstoken			
Token Value	_			
Reports				
O Behavior Correlation				
	Im	port	Clos	е

Figure 18

### 5.4 Token Template

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.





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



Parsing Rule	s					
Parsing Rule	Template					
Groups			<b>+</b>	Group :		
Default			-			
Azure Intune		Ŵ	0	Templa		
Figure 20						

<b>†</b>	/ Admin / Parsing Rules
	C 1
Active	Import configuration



3. Now, click "Browse" and navigate to the knowledge packs folder (type "%et\_install\_path%\Knowledge Packs" in navigation bar) where ".ettd", e.g. "Templates\_NetMotion.ettd" file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click "Import":







Netsurion... EventTracker\*

### 5.5 Reports

15

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

Ъ.	Export Import Utility		_		$\times$
Exp	port Import				
	1. Provide the path and file na 2. Click the Import button Note : If report(s) contains tem	ne of Schedule Report file. Use the '' button to browse and locate the import file. plate, first import template and proceed with exportimport utility.			
	Options	Location			
	Category				
	○ Filters				
	◯ Alerts	◯ Legacy (*.issch)			
	Systems and Groups	Source : *issch			
	O Token Value				
[	Reports				
	Behavior Correlation				
_					
		Import		Clos	e

#### Figure 23

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

🔁 Reports Im	iport							
Note : If repo	t(s) contains ter	nplate, first import tem	plate and proceed v	<i>i</i> ith report import proce	SS.			
Select file	*.etcrx							Select file
Available repo	orts							
Title			F	requency Show a	•	Q Q		
		Title	Sites	Groups	Systems	Frequency	Runtime	Туре



Wait while reports are being populated in below tables. Now, select all the relevant reports and then click Import .

Note: Set run time option is not applicat	le for Defined Reports and Hourly Reports	
Set run time for report(s) from	AM • at interval of minutes	Set 🕕
Replace	to Replac	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 successful	ly
ОК	



### 5.6 Knowledge Objects

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

		🔎 🛛 Admin <del>-</del>	Tools 👻 🌔
Active Watch Lists	Event Filters	🧭 Parsing Rules	🏫 / Da
Alerts	Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
r sc Casebook Configuration	🔍 IP Lookup Configuration	T Weights	Systems since the last 24 hour
● 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 "%et\_install\_path%\Knowledge Packs" in navigation bar) with the extension ".etko", e.g. "KO\_ NetMotion.etko" and then click "Upload".

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

#### Figure 29

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



Figure 30

## 5.7 Dashboards

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

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

↑ / Dashboard / My Dashboard
+ 🖉 @ 🌣 1 🏹 @ 🛈



- 4. Select **browse** and navigate to knowledge pack folder (type **"%et\_install\_path%\Knowledge Packs**" in navigation bar) where **".etwd"**, **e.g. "Dashboards\_ NetMotion.etwd**" is saved and click **"Upload**".
- 5. Wait while EventTracker populates all the available dashboards. Now, choose "Select All" and click "Import".

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet	
	Upload
	opioud
Available widgets	
⊠ Select All	

Figure 33







## 6. Verifying knowledge pack in EventTracker

### 6.1 Saved Searches

- 1. Login to EventTracker manager web interface.
- 2. Click Admin dropdown, and then click Categories.
- 3. In **Category Tree** to view imported categories, scroll down and expand "**NetMotion**" 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
🗉 🔁 Change Audit
🛨 🔁 EventTracker
🗉 🔁 Gsuite
Infoblox
Netmotion
···· 🗐 Netmotion - Directory Activities
····· 🗐 Netmotion - Login failed events
🗐 Netmotion - Login Logout Activity
····· 🗐 Netmotion - Policy Activities
🗐 Netmotion - System Audit Activities

Figure 35



### 6.2 Alerts

- 1. In the EventTracker manager web interface, click the Admin dropdown, and then click Alerts.
- In search box enter "<search criteria> e.g. "NetMotion" and then click Search.
   EventTracker displays an alert related to "NetMotion":

Alerts Show All T			
123	26		
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts		
Activate Now Click 'Activate Now' after	r making all changes		
Alert Name A	Threat	t Active	Email
🔲 ይያ Netmotion - Login failure	٠		

#### Figure 36

### 6.3 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 **"NetMotion"** group folder to view the imported Templates.



Parsing Rules			
Parsing Rule Template			
Groups		<b>(+)</b>	Group : Netmotion
Default			
Cisco ESA	Ī	0	Template Name
EventTracker		0	Netmotion - Directory Activities
Gsuite		0	Netmotion - Login Failure
Infoblox DDI		1	Netmotion - Login Logout Details
Netmotion		1	Netmotion - Policy Details
Palo Alto Firewall		1	
Vectra		1	Netmotion - Proxy details
	<b>-</b> :	27	

### 6.4 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 "NetMotion" group folder to view the imported reports.



epoi	rt Groups		$\oplus$	Repo	rts configu	ration: Netmotion
٩.	Security			÷	Ü 0,	
٩.	Compliance					Title
٩.	Operations				₹ <b>€</b> 3	Netmotion - Proxy Activity
٩.	Flex				223	Netmotion - Directory Activity
þ	Cisco ESA		1		£ <b>5</b> 3	Netmotion - Policy Details
þ	EventTracker		1		213	Netmotion - Login Logout Detai
2	Gsuite		1	_	w M	Netmotion - Login failed
7	Infoblox DDI	Ī	1		4.5	Netholion - Login failed
2	Netmotion	Ī	Ø			

#### **Report Configuration**

Figure 39

### 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 "**NetMotion**" group folder to view the imported Knowledge objects.



Know	led	lae	Ob	iects
1010101	i u u	ge.	00	10003

Search objects		0
Search objects		~
Groups	+ 🖉	Ē
Barracuda NG Firewall		
Checkpoint Firewall		
E Cisco ESA		
Cybereason		
■ EventTracker		
■ G suite		
Infoblox DDI		
Juniper JunOS		
Netmotion		
Netmotion All Events	Ø	Û
Palo Alto Firewall		
Sonicwall Firewall		
■ Vectra		
Watchguard XTM Firewa	II	

### 6.6 Dashboards

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





2. Select "Customize daslets".

and type "Cisco" in the search bar.







#### Customize dashlets

Netmotion - IMP Authenticatio     Netmotion - IMP Authenticatio     Netmotion - Login Failed     Netmotion - Login Logout De	Netmotion				Q
	□ Netmotion - IMP Authenticatio	□ Netmotion - IMP Authenticatio	□ Netmotion - Login Failed	Netmotion - Login Logout	Deta
Netmotion - Policy Details	Netmotion - Policy Details	O Netmotion - Proxy Login Logou	□ Netmotion - User added to gro	Netmotion - User deleted f	from

Add Delete Close

 $\times$ 

Figure 43

