

**Integration Guide** 

## **Integrate McAfee ePolicy Orchestrator**

EventTracker v9.2 and later

**Publication Date:** 

June 1, 2021

© Copyright Netsurion. All Rights Reserved.



## Abstract

This guide provides instructions to configure McAfee ePolicy Orchestrator to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor McAfee ePolicy Orchestrator.

## Scope

The configuration details in this guide are consistent with EventTracker version v8.x or above and McAfee ePolicy Orchestrator.

## Audience

Administrators who are assigned the task to monitor McAfee ePolicy Orchestrator events using EventTracker.



## Table of Contents

Tab	ble	of Contents	3				
1.	С	verview	4				
2.	. Prerequisites						
3.	. Configuring McAfee ePolicy Orchestrator to forward logs to EventTracker						
4.	E	ventTracker Knowledge Pack	5				
4	1.1	Flex Reports	6				
4	1.2	Alerts	11				
4	1.3	Dashboards	12				
5.	Ir	nporting McAfee ePolicy Orchestrator Knowledge Pack into EventTracker	15				
[	5.1	Category	15				
[	5.2	Alerts	16				
[	5.3	Token Value	17				
ŗ	5.4	Knowledge Objects	18				
ŗ	5.5	Flex Reports	19				
[	5.6	Dashboard	20				
6.	V	erifying McAfee ePolicy Orchestrator knowledge pack in EventTracker	22				
(	5.1	Categories	22				
(	5.2	Alerts	22				
(	5.3	Token Value	23				
(	5.4	Knowledge Objects	23				
(	5.5	Flex Reports	24				
/	٩þс	out Netsurion	25				
(	Con	tact Us	25				

## 1. Overview

The McAfee ePolicy Orchestrator (McAfee ePO) platform enables centralized policy management and enforcement for your endpoints and enterprise security products.

EventTracker helps to monitor events from McAfee ePolicy Orchestrator. Its knowledge object and flex reports help you to analyze critical activities (e.g., Threat Management) and to monitor login/logoff events.

## 2. Prerequisites

- EventTracker agent should be installed in McAfee ePO Server.
- PowerShell 5.0 and above should be installed on McAfee ePO server.
- User should have global administrative privilege on McAfee ePO server.

## 3. Configuring McAfee ePolicy Orchestrator to forward logs to EventTracker

- 1. Contact <u>EventTracker support</u> for McAfee ePO Integrator.
- 2. Download and run executable file McAfeeePOIntegrator.exe.

[] McAfee ePO Int	egrator — 🗌	×
Actionable Security Intelligence	<ul> <li>This will help to integrate McAfee ePO with EventTracker. Follow the following intructions:</li> <li>Click Browse button and navigate to location.</li> <li>Select the location.</li> <li>Click on Install button.</li> </ul>	~
Icker	Destination folder  C:\Program Files (x86)\McAfee ePO Integrator Browse Installation progress	
	Install Cancel	

- 3. Select the path to install Integrator and then click **Install** to proceed.
- 4. Enter McAfee console URL, global admin username and password.



🚼 McAfee ePO Integrator		_		$\times$
MaCfee Console URL*	https://172.28.10	0.45:8443		
Username *	admin			
Password *				
		Validate Crea	lential	
F	inish Cano	cel		

- 5. Click Validate Credential to confirm if the entered credentials are correct.
- 6. Click **Finish** to complete the process.

CT McAfee ePO Integrator	—		$\times$	G McAfee ePO Integrator -		×
MaCfee Information Usernar Passwo Credential Validated Sucess	×	ential		Information  McAfee ePO Integration configured successful	×	
	к		//			

**Note**: MacAfee ePO integration user should have **global admin privileges**. So, that it will work without any issues.

### 4. 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 McAfee ePolicy Orchestrator 5.10.

### 4.1 Flex Reports

• McAfee ePO - Server Activity - This report gives the information about server activities.

	1		-	1	1	
Event DateTime	Computer	UserName	Alert Description	Priority	Status	Action Value
2019-02-26T16:00:03+05:30	WIN-0R5VUV06QVU	admin	Created client task: "Endpoint security, Type: McAfee Agent: Product Deployment"	2	True	Create Client Task
2019-02-26T15:56:38+05:30	WIN-0R5VUV06QVU	admin	Assign task "Threat Protection" to node "My Organization"	2	True	Save Client Task Assignment
2019-02-26T15:44:24+05:30	WIN-0R5VUV06QVU	admin	The attempt to end the task "Deploy McAfee Agent" from Server Task was not successful.	2	False	End Task
2019-02-26T15:44:07+05:30	WIN-0R5VUV06QVU	admin	The attempt to end the task "Deploy McAfee Agent" from Server Task was not successful.	2	False	End Task
2019-02-26T15:42:24+05:30	WIN-0R5VUV06QVU	admin	Successfully sent Run Now task to 1 computers.	3	True	Run Client Task Now
2019-02-26T15:29:49+05:30	WIN-0R5VUV06QVU	admin	Ran command Deploy McAfee Agent	1	True	Run command as task
2019-02-26T15:28:54+05:30	WIN-0R5VUV06QVU	admin	Ran command Deploy McAfee Agent	1	True	Run command as task
2019-02-26T15:15:20+05:30	WIN-0R5VUV06QVU	admin	The attempt to end the task "Deploy McAfee Agent" from Server Task was not successful	2	False	End Task

#### Sample Log:

+- 0			
+- WIN-0R5VUVO6QVU			
+- 3/14/2019 1:14:19 PM			
<b>+-</b> 1552549459			
OrionAuditLog.UserName : admin			
OrionAuditLog.Priority : 2			
OrionAuditLog.CmdName : New Server Task			
OrionAuditLog.Message : Added task: Roll up Data (Local McAfee ePO server)			
OrionAuditLog.Success : True			
OrionAuditLog.StartTime : 2019-02-20T14:59:14+05:30			
OrionAuditLog.EndTime : 2019-02-20T14:59:15+05:30			
+- 3230			
+- Application			
+- McAfee Audit			

• McAfee ePO-Policy Details - This report gives information about policy configuration changes details.

Event DateTime	Computer	Priority	UserName	Alert Description	Action Value	Status
2019-02-20T14:59:32+05:30	WIN-0R5VUV06QVU	1	admin	Assign policy "My Default" to node "Directory"	Assign policy	True
2019-02-20T14:59:32+05:30	WIN-0R5VUVO6QVU	5	admin	Copy policy object: source="McAfee DefaultWIN- 0R5VUVO6QVU (McAfee Agent:McAfee Agent)", target="My DefaultWIN-0R5VUVO6QVU (McAfee Agent:McAfee Agent)"	Copy policy object	True
2019-02-20T14:59:32+05:30	WIN-0R5VUV06QVU	1	admin	Assign policy "My Default" to node "Directory"	Assign policy	True
2019-02-20T14:59:32+05:30	WIN-0R5VUVO6QVU	٩	admin	Copy policy object: source="McAfee DefaultWIN- 0RSVUV06QVU (McAfee Agent:McAfee Agent)", target="My DefaultWIN-0RSVUV06QVU (McAfee Agent:McAfee Agent)"	Copy policy object	True
2019-02-20T14:59:32+05:30	WIN-0R5VUV06QVU	1	admin	Assign policy "My Default" to node "Directory"	Assign policy	True

#### Sample Logs:

event_category	+- 0					
event_computer	+- WIN-0R5VUVO6QVU					
event_datetime	+- 3/14/2019 1:14:18 PM					
event_datetime_utc	<b>+</b> - 1552549458					
event_description	OrionAuditLog.UserName : system					
	OrionAuditLog.Priority : 1					
	OrionAuditLog.CmdName : Create policy object					
	OrionAuditLog.Message : Create policy object: "_EPO_ENFORCE_YES_[WIN-0R5VUVO6QVU] (McAfee Agent:EPOAGENTMETA)"					
	OrionAuditLog.Success : True					
	OrionAuditLog.StartTime : 2019-02-20T14:59:30+05:30					
	OrionAuditLog.EndTime : 2019-02-20T14:59:30+05:30					
event_id	+- 3230					
event_log_type	+- Application					
event_source	+- McAfee Audit					

• **McAfee ePO - Extension Installation Details -** This report gives the information about extension installation and un-installation details.

Event DateTime	Computer		Priority	Action Value	Alert Description	Status
2019-02-20T14:56:22+05:30	WIN-0R5VUV06QVU	admin	1	Uninstall Extension	No extension named avertalerts was installed.	True
2019-02-20T14:59:39+05:30	WIN-0R5VUV06QVU	admin	1	Migrate Extension	The extension "Endpoint Upgrade Assistant" was successfully migrated to version 2.1.0.39.	True
2019-02-26T16:00:59+05:30	WIN-0R5VUVO6QVU	admin	1	Install Extension	Extension MCPSRVER1000, version 2.3.4.132 is not compatible with this version of ePolicy	False
2019-02-20T14:59:46+05:30	WIN-0R5VUVO6QVU	admin	2	List Installed Extensions	Orchestrator. List Installed Extensions	True

#### Sample Log:

event_category	+- 0		
event_computer +• WIN-0R5VUVO6QVU			
event_datetime	+- 3/14/2019 1:14:18 PM		
event_datetime_utc	+- 1552549458		
event_description	OrionAuditLog.UserName : admin		
	OrionAuditLog.Priority : 1		
	OrionAuditLog.CmdName : Install Extension		
	OrionAuditLog.Message : Extension MCPSRVER1000, version 2.3.4.132 is not compatible with this version of ePolicy Orchestrator.		
	OrionAuditLog.Success : False		
	OrionAuditLog.StartTime : 2019-02-26T16:49:40+05:30		
	OrionAuditLog.EndTime : 2019-02-26T16:49:42+05:30		
event_id	+- 3230		
event_log_type	+- Application		
event_source	+- McAfee Audit		

• McAfee ePO - System Management - This report gives information about system details which were added or removed.

Event DateTime	Computer	UserName	Priority	Alert Description	Action Value	Status
2019-02-26T15:35:45+05:30	WIN-0R5VUV06QVU	admin	1	Deleting system: "172.32.100.3"	Delete system	True
2019-02-26T15:28:54+05:30	WIN-0R5VUV06QVU	admin	1	Adding system: "172.32.100.3"	New system	True
2019-02-25T19:23:46+05:30	WIN-0R5VUV06QVU	admin	2	Adding system: "WIN- 0R5VUV06QVU"	New system	True
2019-02-26T13:26:21+05:30	WIN-0R5VUV06QVU	admin	2	Adding System Tree group: "My Group 2"	New System Tree group	True

#### Sample Log:

event_category	+- 0			
event_computer	+- WIN-0R5VUVO6QVU			
event_datetime	+- 3/14/2019 1:14:18 PM			
event_datetime_utc	<b>+ -</b> 1552549458			
event_description	OrionAuditLog.UserName : admin			
	OrionAuditLog.Priority : 2			
	OrionAuditLog.CmdName : New system			
	OrionAuditLog.Message : Adding system: "WIN-A0206PHIGU6"			
	OrionAuditLog.Success : True			
	OrionAuditLog.StartTime : 2019-02-26T15:40:12+05:30			
	OrionAuditLog.EndTime : 2019-02-26T15:40:12+05:30			
event_id	+- 3230			
event_log_type	+- Application			
event_source	+- McAfee Audit			

• McAfee ePO - User Management - This report gives information about user details which were added or removed, and permission changed.

Event DateTime	Computer	UserName	Priority	Action Value	Alert Description	Status
2019-02-28T14:28:14+05:30	WIN-0R5VUV06QVU	admin	1	Remove User	User removed: ETUser1	True
2019-02-27T19:45:26+05:30	WIN-0R5VUVO6QVU	ETUser1	1	Change Password	Password successfully changed by user: ETUser1 for the user: ETUser1.	True
2019-02-27T19:43:09+05:30	WIN-0R5VUVO6QVU	admin	1	Change Permission Sets for User	The user "ETUser1" was added to the following Permission Sets: Executive Reviewer, Group Reviewer.	True
2019-02-27T19:43:06+05:30	WIN-0R5VUV06QVU	admin	5	New User	Created the user "ETUser1". The user is not an admin. The user's authentication type is "ePO authentication". The user's account is enabled.	True

#### Sample Log:

event_category	+- 0
event_computer	+- WIN-0R5VUVO6QVU
event_datetime	+ - 3/14/2019 1:18:49 PM
event_datetime_utc	<b>+</b> - 1552549729
event_description	OrionAuditLog.UserName : admin
	OrionAuditLog.Priority : 1
	OrionAuditLog.CmdName : New User
	OrionAuditLog.Message : Created the user "ETUser1".
	The user is not an admin.
	The user's authentication type is "ePO authentication".
	The user's account is enabled.
	OrionAuditLog.Success : True
	OrionAuditLog.StartTime : 2019-02-27T19:43:06+05:30
	OrionAuditLog.EndTime : 2019-02-27T19:43:09+05:30
event_id	+- 3230
event_log_type	+- Application
event_source	+ - McAfee Audit

• McAfee ePO - Agent Activity - This report gives information about details of agent activities.

Event DateTime	Computer	UserName	Priority	Action Value	Alert Description	Status
2019-02-25T19:26:32+05:30	WIN-0R5VUVO6QVU	admin	1	Wake Up Agents	No agent wake-up calls were successful	False
2019-02-20T14:58:51+05:30	WIN-0R5VUV06QVU	admin	3	Generate Agent Handler Certificate	Generated Agent Handler "WIN- 0R5VUV06QVU' certificate.	True
2019-02-26T16:30:53+05:30	WIN-0R5VUV06QVU	admin	3	Wake Up Agents	Completed: 1, Failed: 0, Expired: 0	True
2019-02-26T15:28:54+05:30	WIN-0R5VUV06QVU	admin	3	Deploy McAfee Agent		True
2019-02-26T15:29:50+05:30	WIN-0R5VUV06QVU	admin	5	Deploy McAfee Agent		True
2019-02-26T15:41:22+05:30	WIN-0R5VUV06QVU	system	3	Streamed Agent Bootstrap Package to user	Streamed agent package to user, from IP address 172.32.100.3 (macc)	True
2019-02-26T15:39:42+05:30	WIN-0R5VUV06QVU	system	3	User viewed the Agent Package Download page	Created agent package file from IP address 172.32.100.3 (macc)	True
2019-02-26T15:39:22+05:30	WIN-0R5VUV06QVU	system	3	Streamed Agent Bootstrap Package to user	Streamed agent package to user, from IP address 172.32.100.38 (macc)	True

#### Sample Log:

event_category	+- 0
event_computer	+- WIN-0R5VUVO6QVU
event_datetime	+- 3/14/2019 1:18:50 PM
event_datetime_utc	<b>+-</b> 1552549730
event_description	OrionAuditLog.UserName : admin
	OrionAuditLog.Priority : 3
	OrionAuditLog.CmdName : Deploy McAfee Agent
	OrionAuditLog.Message : Completed: 1, Failed: 0, Expired: 0
	OrionAuditLog.Success : True
	OrionAuditLog.StartTime : 2019-02-26T14:53:12+05:30
	OrionAuditLog.EndTime : 2019-02-26T14:55:02+05:30
event_id	+- 3230
event_log_type	+- Application
event_source	+ - McAfee Audit

• McAfee ePO - LogOn and Log Off Details - This report gives information about details of user log on and log off.

LogTime	Computer	Category	Log Message	Log Priority	Log Value	User IP address	User Name
03/12/2019 12:26:50 AM	WIN-0R5VUVO6Q	Logon Attempt	Successful Logon for user "admin" from IP address: 172.28.100.17	3	True	172.28.100.17	admin
03/08/2019 01:40:04 AM	WIN-0R5VUVO6Q	Logon Attempt	Successful Logon for user "ETAdmin (ETAdmin)" from IP address: 172.32.100.38	3	True	172.32.100.38	ETAdmin
02/26/2019 12:41:28 AM	WIN-0R5VUVO6Q	Logon Attempt	Successful Logon for user "admin" from IP address: 10.0.2.2	3	True	10.0.2.2	admin
02/20/2019 08:31:47 PM	WIN-0R5VUVO6Q	Logon Attempt	Successful Logon for user "admin" from IP address: 10.0.2.15	3	True	10.0.2.15	admin
03/08/2019 02:06:42 AM	WIN-0R5VUVO6Q	User Log Off	User "ETAdmin (ETAdmin)" has logged out	3	True		ETAdmin

#### Sample Log:

event_category	+- 0
event_computer	+- WIN-0R5VUVO6QVU
event_datetime	+- 3/14/2019 1:26:04 PM
event_datetime_utc	<b>+-</b> 1552550164
event_description	OrionAuditLog.UserName : admin
	OrionAuditLog.Priority : 3
	OrionAuditLog.CmdName : Logon Attempt
	OrionAuditLog.Message : Successful Logon for user "admin" from IP address: 10.0.2.2
	OrionAuditLog.Success : True
	OrionAuditLog.StartTime : 2019-02-21T21:46:49-08:00
	OrionAuditLog.EndTime : 2019-02-21T21:46:49-08:00
event_id	+- 3230
event_log_type	+- Application
event_source	+- McAfee Audit

• McAfee ePO - Logon Failure - This report gives information about details of user log on failure.

Computer	Event DateTime	Event Priority	Reason	UserName
WIN-0R5VUV06QVU	2019-02-25T11:01:58+05:30	1	incorrect password	system_WIN-0R5VUV06QVU
WIN-0R5VUV06QVU	2019-02-22T12:30:56+05:30	1	user auto-creation failure	Admistrator
WIN-0R5VUV06QVU	2019-02-22T12:29:20+05:30	1	user auto-creation failure	Admistrator
WIN-0R5VUV06QVU	2019-02-21T11:27:19+05:30	1	incorrect password	system_WIN-0R5VUV06QVU
WIN-0R5VUV06QVU	2019-02-25T18:21:28+05:30	1	incorrect password	admin
WIN-0R5VUV06QVU	2019-03-04T10:43:20+05:30	1	incorrect password	system_WIN-0R5VUV06QVU
WIN-0R5VUV06QVU	2019-02-27T19:00:02+05:30	1	user auto-creation failure	demo123
WIN-0R5VUV06QVU	2019-02-27T18:59:52+05:30	1	incorrect password	admin
WIN-0R5VUV06QVU	2019-02-27T18:59:45+05:30	1	incorrect password	admin

#### Sample Log:

event_category	+- 0
event_computer	+- WIN-0R5VUVO6QVU
event_datetime	+- 3/14/2019 1:26:04 PM
event_datetime_utc	<b>+-</b> 1552550164
event_description	OrionAuditLog.UserName : demo123
	OrionAuditLog.Priority : 1
	OrionAuditLog.CmdName : Logon Attempt
	OrionAuditLog.Message : Failed Logon for user "demo123" from IP address: 172.32.100.17 due to user auto-creation failure
	OrionAuditLog.Success : False
	OrionAuditLog.StartTime : 2019-02-27T19:00:02+05:30
	OrionAuditLog.EndTime : 2019-02-27T19:00:02+05:30
event_id	+- 3230
event_log_type	+- Application
event_source	+- McAfee Audit

#### • Malware Log Alerts - This report gives information on all the malware events captured by McAfee ePO.

			Analyzer		Analyzer	Threat	Threat			
Log DateTime	Analyzer	Analyzer HostName	IPAddress	Analyzer Name	Version	Severity	Action	Threat Category	Threat EventID	Threat Handled
2019-03-04T18:55:18+05:30	ENDP_GS_1060	WIN-0R5VUV06QVU	740320293	McAfee Endpoint Security	10.6.0.542	5	none	ops.update.end	1119	True
2019-03-04T18:55:18+05:30	ENDP_GS_1060	WIN-0R5VUV06QVU	740320293	McAfee Endpoint Security	10.6.0.542	5	none	ops.update.end	1119	True
2019-03-04T18:55:18+05:30	ENDP_GS_1060	WIN-0R5VUV06QVU	740320293	McAfee Endpoint Security	10.6.0.542	5	none	ops.update.end	1119	True
2019-03-04T14:55:19+05:30	ENDP_GS_1060	WIN-0R5VUV06QVU	740320293	McAfee Endpoint Security	10.6.0.542	5	none	ops.update.end	1119	True

event_log_type	+- Application
event_type	+- Information
event_id	+- 3230
event_source	+- McAfee Threat
event_user_domain	+- N/A
event_computer	+- WIN-0R5VUVO6QVU
event_user_name	+- N/A
event_description	EPOEvents.ServerID : WIN-0R5VUVO6QVU
	EPOEvents.ReceivedUTC : 2019-03-01T14:58:50+05:30
	EPOEvents.DetectedUTC : 2019-03-01T14:56:33+05:30
	EPOEvents.EventTimeLocal : 2019-03-01T14:56:33+05:30
	EPOEvents.AgentGUID : 8819C083-ACFE-467A-997C-D0128085B194
	EPOEvents.Analyzer : ENDP_GS_1060
	EPOEvents.AnalyzerName : McAfee Endpoint Security
	EPOEvents.AnalyzerVersion : 10.6.0.542
	EPOEvents.AnalyzerHostName : WIN-0R5VUVO6QVU

#### 4.2 Alerts

- McAfee ePO Log-On Failure This alert will generate ,when the user fails to logon attempt.
- McAfee ePO Policy Changes This alert will generate ,when the policy configuration changes.
- McAfee ePO Threat Detected This alert will generate ,when the threat is detected on McAfee Agent systems.



### 4.3 Dashboards

• McAfee ePO – Logon Failure:



• McAfee ePO – System Management



• McAfee ePO – Server Activity



• McAfee ePO – Log On and Log Off Details



• McAfee ePO – Policy Details





• McAfee ePO – Agent Activity



• McAfee ePO – User Management



• McAfee ePO - Threat Activities





## 5. Importing McAfee ePolicy Orchestrator Knowledge Pack into EventTracker

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

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



3. Click the **Import** tab.

#### 5.1 Category

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

Options Category	Location				
Alerts  Systems and Groups Token Value Reports Behavior Correlation	s Ē	urce : :∖Official\Work Purpose∖	KP Items\McAfee ePO\Mc	Afee e	

- 2. Locate ".iscat" file, and then click **Open**.
- 3. To import categories, click the **Import** button.

EventTracker displays success message:

Export Im	port Utility	$\times$
1	Selected category details are imported successfully.	
	ОК	

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

#### 5.2 Alerts

1. Click **Alert** option, and then click the browse **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 '' butt	on to browse and locate the import file.	
Options	Location		
Category	Import E-mail settings		
Filters     Alerte	Set Active Only if notifications set D By default	This setting is applicable only for imports from Legacy (v6 Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.	K)
<ul> <li>Systems and Groups</li> </ul>	Watchlist Configuration	-	
O Token Value	This setting is applicable only f Note: If this option is enabled t	on or alerts which have Advanced watchlist configured. he user should make sure the watchlist groups are available	
<ul> <li>Reports</li> </ul>	on the console where the alert	s are imported.	
O Behavior Correlation			
	Source : E:\Official\Work Purpose\K	P Items\McAfee ePO\McAfee ePO\Alerts_McAfee e	]
		Import	Close
		inport	0030

- 2. Locate ".isalt" file, and then click Open.
- 3. To import alerts, click **Import**.

#### 5.3 Token Value

1. Click **Token Value** option, and then click the browse **—** button.

<ol> <li>Provide the path and file nanolisi</li> <li>Click the Import button</li> </ol>	e of token value file. Use the '' button to browse and locate the import file.	
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location Source : E:\Official\Work Purpose\KP Items\McAfee ePO\McAfee	

- 2. Locate ".istoken" file, and then click Open.
- 3. To import alerts, click Import.



### 5.4 Knowledge Objects

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



- 3. Click the **Upload** option.
- 4. Select all the check box and then click **Import** option.

Select	t file	<b>=</b>	Browse Upload
	Object name	Applies to	Group name
	McAfee ePO Agent Activity	McAfee ePO	McAfee ePO
$\square$	McAfee ePO Extension Installation Details	McAfee ePO	McAfee ePO
$\checkmark$	McAfee ePO Log On and Log Off Details	McAfee ePO	McAfee ePO
	McAfee ePO Log On Failure	McAfee ePO	McAfee ePO
$\checkmark$	McAfee ePO Policy Details	McAfee ePO	McAfee ePO
	McAfee ePO Server Activity	McAfee ePO	McAfee ePO
	McAfee ePO System Management	McAfee ePO	McAfee ePO
	McAfee ePO User Management	McAfee ePO	McAfee ePO

5. Knowledge objects are now imported successfully.



Import Close

### 5.5 Flex Reports

On EventTracker Control Panel,

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

🐁 Exp	ort Import Utility		-		$\times$
Export	Import				
1. P 2. C Note	rovide the path and file na lick the Import button e : If report(s) contains tem	me of Schedule Report file. Use the '' button to browse and locate the import file. plate, first import template and proceed with exportimport utility.			
Or	otions	Location			
0	Category				
0	Filters				
0	Alerts	O Legacy ("issch)			
0	Systems and Groups	Source :			
0	RSS Feeds	JSSCH			
۲	Reports				
0	Behavior Rules				
0	SCAP				
0	Token Value				
		hoom		Clos	e
				0.00	~

2. Locate the ".etcrx" file and select all the check box.

ailable rep	orts	Frequency Show all	- Q Q		
2	Title	Sites	Groups	Systems	Frequency
EDIT	McAfee ePO-Agent Activity	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined
EDIT	McAfee ePO-Extension Installation Det	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined
EDIT	McAfee ePO-Log On and Log Off Det	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined
EDIT	McAfee ePO-Logon Failure	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined
EDIT	McAfee ePO-Policy Details	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined
EDIT	McAfee ePO-Server Activity	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined
EDIT	McAfee ePO-System Management	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined
EDIT	McAfee ePO-User Management	NTPLDTBLR143	EventTracker	NTPLDTBLR143	Undefined

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



Export Import Utility	$\times$
Selected reports configurations are imp	orted successfully
	ОК

### 5.6 Dashboard

- 1. Logon to **EventTracker**.
- 2. Navigate to **Dashboard**  $\rightarrow$  **My Dashboard**.



3. In My Dashboard, Click Import Button.



4. Select the **browse** button and navigate to file path where Dashboard file is saved.

ŀ	🗅 Import dashlets - Google Chrome	_		х				
1	O localhost:8080/EventTracker/Flex/ImportWidget.aspx							
	Import			<b>^</b>				
	Note: If dashlet configured using persisted report, first import the report and proceed v dashlet.	vith imp wse	orting Upload					

- 5. Once completed, click **Upload** Button.
- 6. Click **Customize dashlet** button as shown below:



7. Type in a text in Search bar: "McAfee" and then select the McAfee dashlets and then click Add.

Customize dashlets	×
Mc	Q
McAfee ePO - Logon Failure McAfee ePO - Server Activity McAfee ePO - System Manage	
	dd Delete Close

8. Once the **dashlets** gets populating, you see the following screen.



My Dashboard	
Windows McAfee ePO Azure Intune	
McAfee ePO - Logon Failure	McAfee ePO - Server Activity
log_type: logon attempt	log_status: true

## 6. Verifying McAfee ePolicy Orchestrator knowledge pack in EventTracker

#### 6.1 Categories

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

Category			📌 / Admin / Catego
Category Tree Search	Category Details		
All Categories	Parent Group	McAfee ePO	
All information events	Event Category Name	McAfee ePO Agent Activity	
Security: All security events     ArubaOS	Description	McAfee et Agent Activity	
Change Audit     Cisco ASA	Applies to	McAfee ePO Category version 0.1	
EventTracker	Show In	Operations Compliance Security	
🗐 McAfee ePO Agent Activity 🗐 McAfee ePO Extension Installation	Event Rule		Add Edit Delete
(王) McAfee ePO Log On and Log Off D (王) McAfee ePO Log On Failure	Log Event Type Type Catego	Event ry Id Source User Match in Description	Description Exception Lucene Query
	0 0 0	3230 EventTracker (?is)UserName\s+\:,*?CmdName\s+\:\s+(Deploy\s+McAfee \s+Agent]Update \s+Agents).*?StartTime.*?EndTime.*?TenantName\s+\:	log_source:"McAfee ePO Agent Activity"

#### 6.2 Alerts

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Alerts.
- 2. In search box enter McAfee ePolicy Orchestrator and then click Search. EventTracker displays alert of McAfee ePolicy Orchestrator.

Alerts								🔒 / Admin / Alerts	
Show All						Search by	Alert name 🗸 🗸	Mcafee Q Q	
112	16				112	System	103	112	Critical 11 High 64 Low 14
Available Alerts Total number of alerts available	Active Alerts Total number of active aler				System/User Count for syste	User Defined Alerts em and user defin	9 5 ied alerts	Alerts by Count of a	Serious 20 Threat Level lerts by threat level
Activate Now Click 'Activate No	w' after making 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
CAfee ePO Log On Failure		•							McAfee ePO
Konstant And Argenting And Argenting And Argenting And Argenting And Argenting Ar		•							McAfee ePO

#### 6.3 Token Value

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing rules.
- 2. On **Parsing Rule** tab, click the **McAfee ePolicy Orchestrator** group folder to view the imported **Token Values**.

Parsing Rules Parsing Rule Template									🛧 / Admin /	Parsing R	lules
Groups	(	<b>⊕ </b> Ⅲ	Token-V	alue	Display name	Q, Q,	Group : McAfee	ePO		?	^
Default			-		Display pame	Takan nama	Tag	Constator	Terminator		
Azure Intune	Ē	1	±		Display hame	Token name	Tag	Separator	Terminator		
Cisco	Î	Ø	+		Action Value	OrionAuditLog.CmdName		=	\n		
EventTracker	Ê		+		Alert Description	OrionAuditLog.Message		=	\n		
McAfee ePO	<u>ت</u>		+		Analyzer	EPOEvents.Analyzer		=	\n		
Riverhed Steelhead C	<u>ت</u>		+		Analyzer Detection Method	EPOEvents.AnalyzerDetectionMethod		=	\n		
tert	<u>ال</u>		+		Analyzer HostName	EPOEvents.AnalyzerHostName		-	\n		
		۲	+		Analyzer IPAddress	EPOEvents.AnalyzerIPV4		=	\n		
Trend Micro		۷		_		5005					
Windows	Ē	1			Analyzer MACAddress	EPOEvents.AnalyzerMAC		=	\n		
			+		Analyzer Name	EPOEvents.AnalyzerName		=	\n		

### 6.4 Knowledge Objects

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

Knowledge Objects											
Search objects	Q	Q Activate Now					Objects 🕂 Ҭ	1¢			
Groups 🕒 🏈 🗓	Obje	ct name McAfee ePO Agent Activity					÷ :	t ¢			
Fortigate Log Messages	Pulor										
Linux Test	Kules	-									
McAfee ePO		litle	Log type	Event source	Event id	Event type		-			
McAfee ePO Agent Act 🧭 🏢		McAfee ePO Agent Activity		EventTracker	3230		0 0	C/>			
McAfee ePO Extension 🧭 🏢		Message Signature: (?is)UserName\s+\:??CmdName\s+\:\s=(Deploy\s+McAfee\s+Agent]Update\s+Agents).??StartTime.??EnantTime.??EnantName\s+\:									
McAfee ePO Log On a 🧭 🏢		Message Exception:									
McAfee ePO Log On F 🧭 🏢		Expressions									
McAfee ePO Policy Det 🧭 🏢		Expression type	Evore	sion 1	Evoression 2	Format string					
McAfee ePO Server Act 🧭 🏢		Kaultaka Dalimitan	Expre.		Expression 2	Tormac string	0	5 前			
McAfee ePO User Man		Key value Delimiter	:		\n		e	/ 🗉			

### 6.5 Flex Reports

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



- 2. In **Reports Configuration** pane, select **Defined** option.
- 3. Click the McAfee ePolicy Orchestrator group folder to view the imported McAfee ePolicy Orchestrator reports.

Report Configuration A / Reports / Report Configuration / Defined										
○ Scheduled ○ Queued						Search	Search			
Report Groups		<b>⊕</b> #	Repo	orts config	uration: McAfee ePO					
Security			÷	İ <i>0</i> ,					Tota	l: 8
Compliance					Title	Created on	Modified on			
Operations					McAfee ePO-Server Activity	Mar 15 05:16:05 PM	Mar 16 11:53:40 AM	()	5	+
🔁 Flex					McAfee ePO-Extension Installation Details	Mar 15 05:02:17 PM	Mar 16 11:53:53 AM	i	5	+
ArubaOS	Ĩ	Ø			McAfee ePO-System Management	Mar 15 04:58:49 PM	Mar 16 11:54:08 AM	()	5	+
Cb Defense	Ĩ	Ø		213	McAfee ePO-User Management	Mar 15 04:53:44 PM	Mar 16 11:54:25 AM	(i)	2	+
Cisco ASA	Ū.	0		233	McAfee ePO-Policy Details	Mar 15 04:04:32 PM	Mar 16 11:54:39 AM	()	2	+
EventTracker	Û	٢		1	McAfee ePO-Agent Activity	Mar 15 03:46:54 PM	Mar 16 11:54:50 AM	0	5	F
McAfee ePO	<u> </u>	Ø		SM2	McAfee ePO-Log On and Log Off Details	Mar 15 03:41:02 PM	Mar 16 11:55:01 AM	0	5	
Microsoft RRAS		0		527 -25	Malifer and Langer Failure	Mar 15 03/41/02 PM	May 10 11/50/12 AM	0		
NtopNG	Ē	۲		245	MCATEE EPO-Logon Failure	Mar 15 03:21:26 PM	Mar 16 11:55:13 AM	0	Ŏ.	+



#### **About Netsurion**

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's <u>EventTracker</u> cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

#### **Contact Us**

#### **Corporate Headquarters**

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

#### **Contact Numbers**

713-929-0200

#### https://www.netsurion.com/company/contact-us