Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrate McAfee ePolicy Orchestrator

EventTracker v9.2 and later

Publication Date:

June 1, 2021

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

1. Overview

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

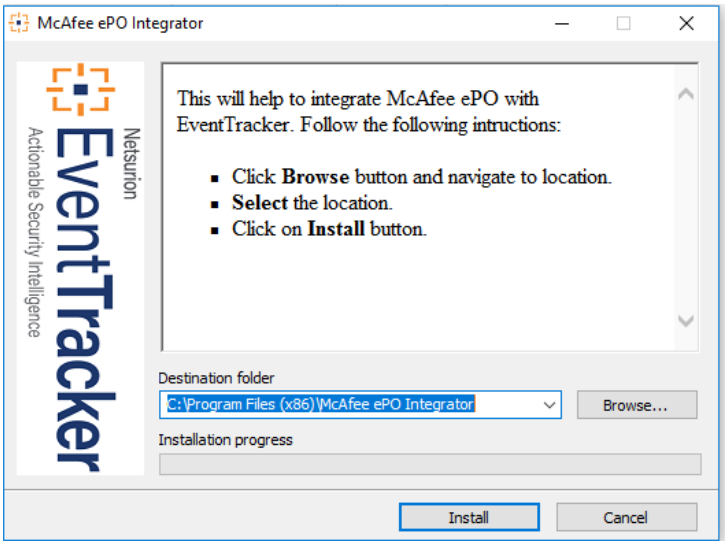
EventTracker helps to monitor events from McAfee ePolicy Orchestrator. Its knowledge object and flex reports help you to analyze critical activities (e.g., Threat Management) and to monitor login/logoff events.

2. Prerequisites

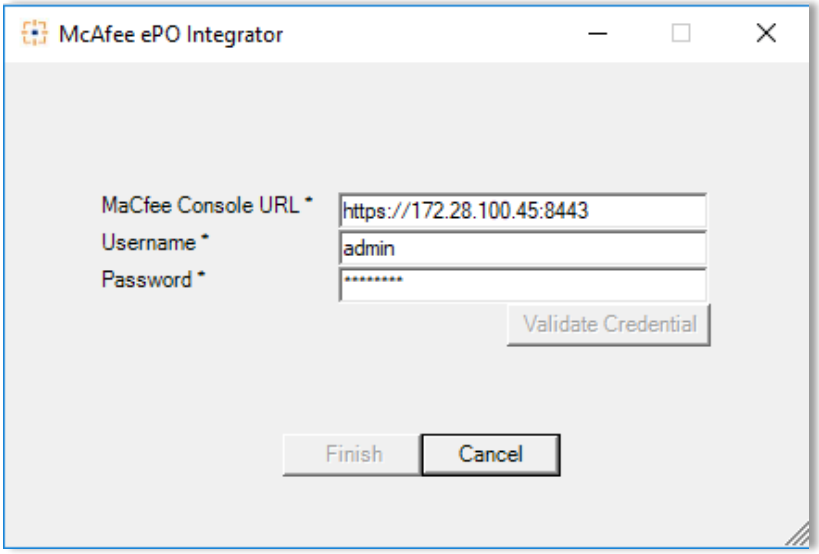
- EventTracker agent should be installed in McAfee ePO Server.
- PowerShell 5.0 and above should be installed on McAfee ePO server.
- User should have **global administrative privilege** on McAfee ePO server.

3. Configuring McAfee ePolicy Orchestrator to forward logs to EventTracker

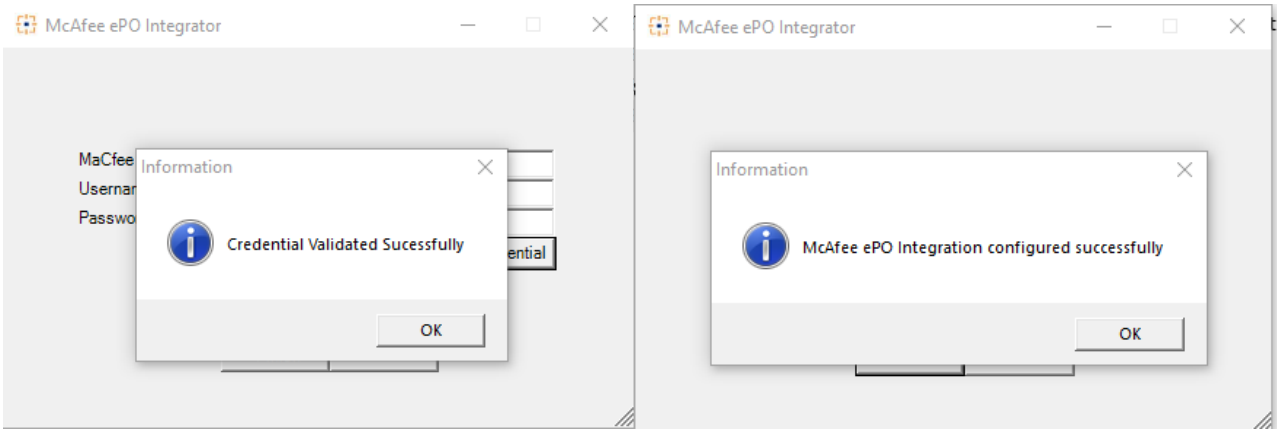
1. Contact EventTracker support for McAfee ePO Integrator.
2. Download and run executable file **McAfeeePOIntegrator.exe**.



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



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



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**.**

Event DateTime	Computer	UserName	Alert Description	Priority	Status	Action Value
2019-02-26T16:00:03+05:30	WIN-0R5VUVO6QVU	admin	Created client task: "Endpoint security, Type: McAfee Agent: Product Deployment"	2	True	Create Client Task
2019-02-26T15:56:38+05:30	WIN-0R5VUVO6QVU	admin	Assign task "Threat Protection" to node "My Organization"	2	True	Save Client Task Assignment
2019-02-26T15:44:24+05:30	WIN-0R5VUVO6QVU	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-0R5VUVO6QVU	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-0R5VUVO6QVU	admin	Successfully sent Run Now task to 1 computers.	3	True	Run Client Task Now
2019-02-26T15:29:49+05:30	WIN-0R5VUVO6QVU	admin	Ran command Deploy McAfee Agent	1	True	Run command as task
2019-02-26T15:28:54+05:30	WIN-0R5VUVO6QVU	admin	Ran command Deploy McAfee Agent	1	True	Run command as task
2019-02-26T15:15:20+05:30	WIN-0R5VUVO6QVU	admin	The attempt to end the task "Deploy McAfee Agent" from Server Task was not successful.	2	False	End Task

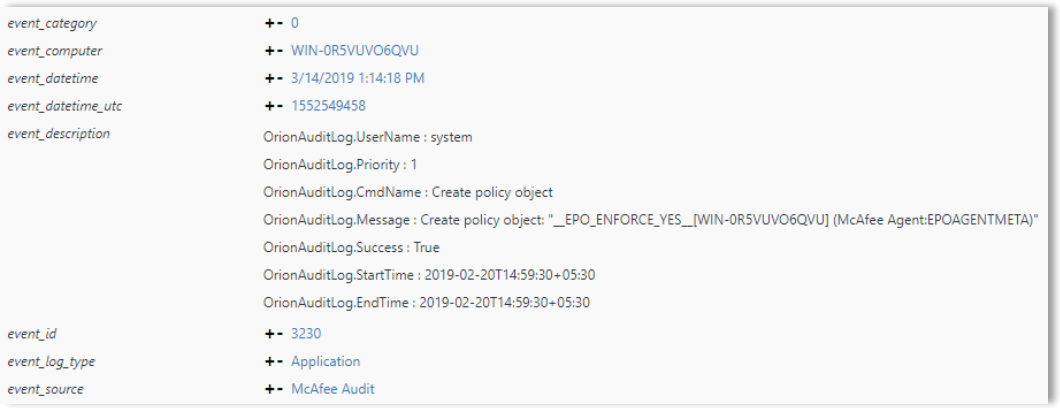
Sample Log:

event_category	+- 0
event_computer	+- WIN-0R5VUVO6QVU
event_datetime	+- 3/14/2019 1:14:19 PM
event_datetime_utc	+- 1552549459
event_description	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
event_id	+- 3230
event_log_type	+- Application
event_source	+- 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-0R5VUVO6QVU	1	admin	Assign policy "My Default" to node "Directory"	Assign policy	True
2019-02-20T14:59:32+05:30	WIN-0R5VUVO6QVU	1	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-0R5VUVO6QVU	1	admin	Assign policy "My Default" to node "Directory"	Assign policy	True
2019-02-20T14:59:32+05:30	WIN-0R5VUVO6QVU	1	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-0R5VUVO6QVU	1	admin	Assign policy "My Default" to node "Directory"	Assign policy	True

Sample Logs:

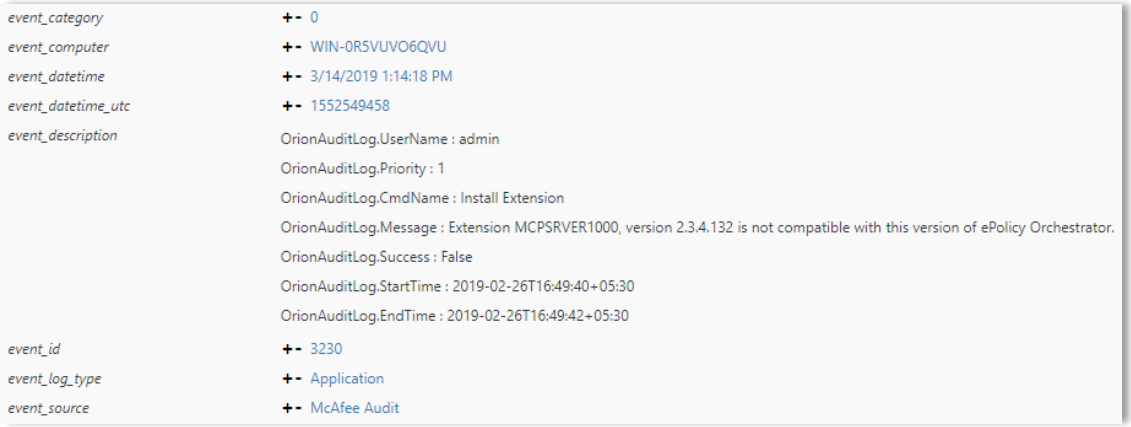


event_category	+- 0
event_computer	+- WIN-0R5VUVO6QVU
event_datetime	+- 3/14/2019 1:14:18 PM
event_datetime_utc	+- 1552549458
event_description	OrionAuditLog.UserName : system OrionAuditLog.Priority : 1 OrionAuditLog.CmdName : Create policy object OrionAuditLog.Message : Create policy object: "__EPO_ENFORCE_YES__[WIN-0R5VUVO6QVU] (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	e	Priority	Action Value	Alert Description	Status
2019-02-20T14:56:22+05:30	WIN-0R5VUVO6QVU	admin	1	Uninstall Extension	No extension named avertalerts was installed.	True
2019-02-20T14:59:39+05:30	WIN-0R5VUVO6QVU	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 Orchestrator.	False
2019-02-20T14:59:46+05:30	WIN-0R5VUVO6QVU	admin	2	List Installed Extensions	List Installed Extensions	True

Sample Log:

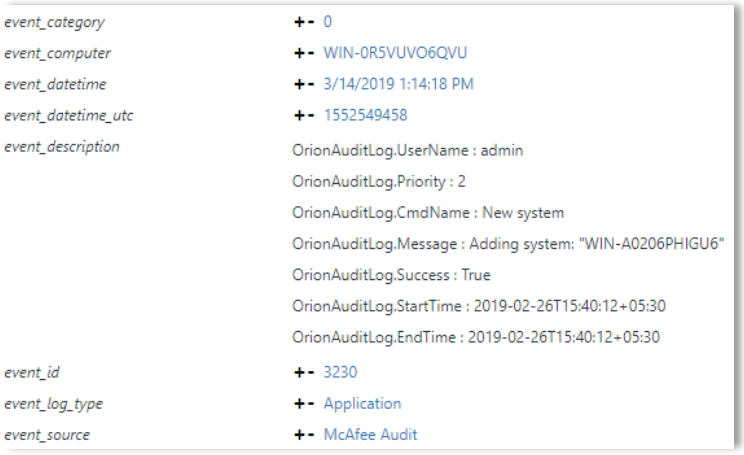


event_category	+- 0
event_computer	+- WIN-0R5VUVO6QVU
event_datetime	+- 3/14/2019 1:14:18 PM
event_datetime_utc	+- 1552549458
event_description	OrionAuditLog.UserName : admin OrionAuditLog.Priority : 1 OrionAuditLog.CmdName : Install Extension OrionAuditLog.Message : Extension MCPSRVER1000, version 2.3.4.132 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-0R5VUVO6QVU	admin	1	Deleting system: "172.32.100.3"	Delete system	True
2019-02-26T15:28:54+05:30	WIN-0R5VUVO6QVU	admin	1	Adding system: "172.32.100.3"	New system	True
2019-02-25T19:23:46+05:30	WIN-0R5VUVO6QVU	admin	2	Adding system: "WIN-0R5VUVO6QVU"	New system	True
2019-02-26T13:26:21+05:30	WIN-0R5VUVO6QVU	admin	2	Adding System Tree group: "My Group 2"	New System Tree group	True

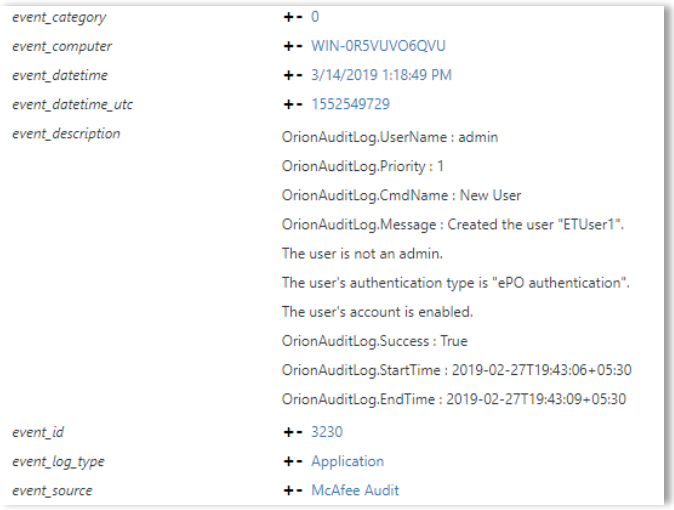
Sample Log:



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

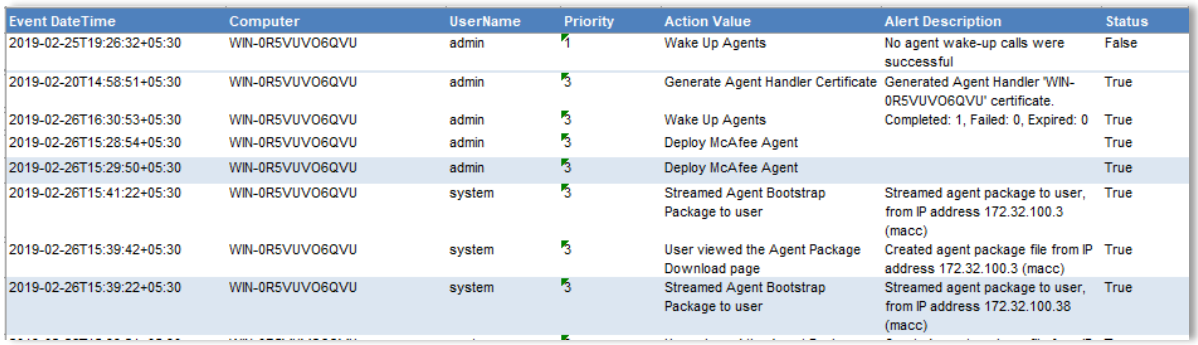
Event DateTime	Computer	UserName	Priority	Action Value	Alert Description	Status
2019-02-28T14:28:14+05:30	WIN-0R5VUVO6QVU	admin	1	Remove User	User removed: ETUser1	True
2019-02-27T19:45:26+05:30	WIN-0R5VUVO6QVU	ETUser1	1	Change Password	Password successfully changed by user: ETUser1 for the user: ETUser1.	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-0R5VUVO6QVU	admin	1	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:



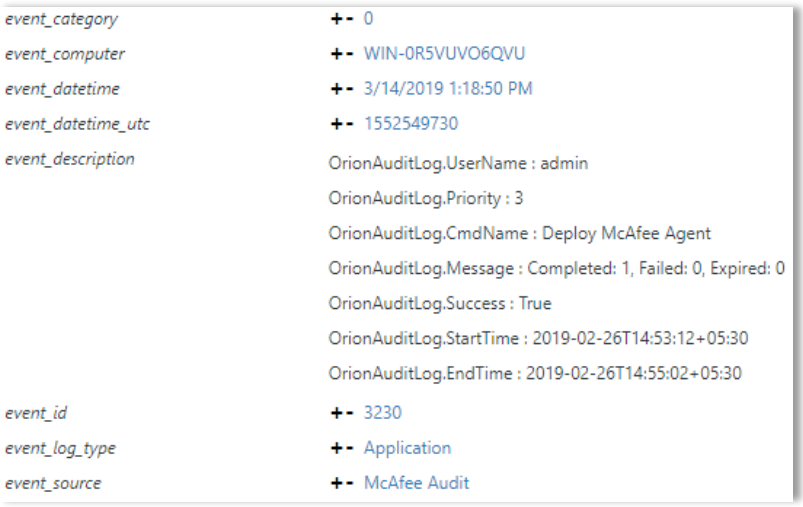
event_category	+ - 0
event_computer	+ - WIN-0R5VUVO6QVU
event_datetime	+ - 3/14/2019 1:18:49 PM
event_datetime_utc	+ - 1552549729
event_description	OrionAuditLog.UserName : admin OrionAuditLog.Priority : 1 OrionAuditLog.CmdName : New User OrionAuditLog.Message : Created the user "ETUser1". The user is 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-0R5VUVO6QVU	admin	3	Generate Agent Handler Certificate	Generated Agent Handler 'WIN-0R5VUVO6QVU' certificate.	True
2019-02-26T16:30:53+05:30	WIN-0R5VUVO6QVU	admin	3	Wake Up Agents	Completed: 1, Failed: 0, Expired: 0	True
2019-02-26T15:28:54+05:30	WIN-0R5VUVO6QVU	admin	3	Deploy McAfee Agent		True
2019-02-26T15:29:50+05:30	WIN-0R5VUVO6QVU	admin	3	Deploy McAfee Agent		True
2019-02-26T15:41:22+05:30	WIN-0R5VUVO6QVU	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-0R5VUVO6QVU	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-0R5VUVO6QVU	system	3	Streamed Agent Bootstrap Package to user	Streamed agent package to user, from IP address 172.32.100.38 (macc)	True

Sample Log:

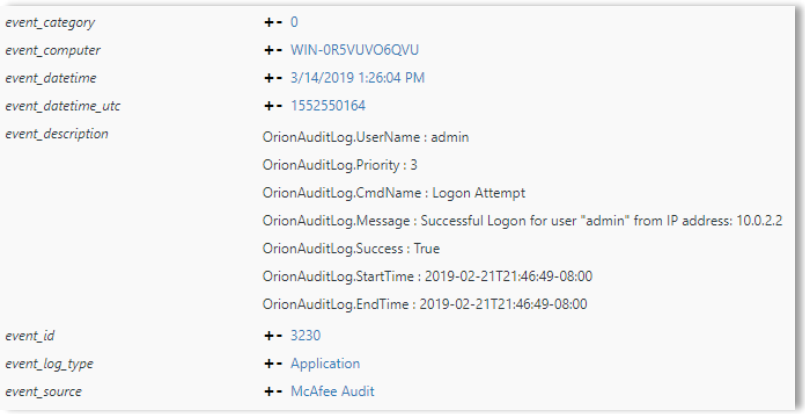


event_category	+ - 0
event_computer	+ - WIN-0R5VUVO6QVU
event_datetime	+ - 3/14/2019 1:18:50 PM
event_datetime_utc	+ - 1552549730
event_description	OrionAuditLog.UserName : admin OrionAuditLog.Priority : 3 OrionAuditLog.CmdName : Deploy McAfee Agent OrionAuditLog.Message : Completed: 1, Failed: 0, Expired: 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:



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

Computer	Event DateTime	Event Priority	Reason	UserName
WIN-0R5VUVO6QVU	2019-02-25T11:01:58+05:30	1	incorrect password	system_WIN-0R5VUVO6QVU
WIN-0R5VUVO6QVU	2019-02-22T12:30:56+05:30	1	user auto-creation failure	Admistrator
WIN-0R5VUVO6QVU	2019-02-22T12:29:20+05:30	1	user auto-creation failure	Admistrator
WIN-0R5VUVO6QVU	2019-02-21T11:27:19+05:30	1	incorrect password	system_WIN-0R5VUVO6QVU
WIN-0R5VUVO6QVU	2019-02-25T18:21:28+05:30	1	incorrect password	admin
WIN-0R5VUVO6QVU	2019-03-04T10:43:20+05:30	1	incorrect password	system_WIN-0R5VUVO6QVU
WIN-0R5VUVO6QVU	2019-02-27T19:00:02+05:30	1	user auto-creation failure	demo123
WIN-0R5VUVO6QVU	2019-02-27T18:59:52+05:30	1	incorrect password	admin
WIN-0R5VUVO6QVU	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	+- 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.

Log DateTime	Analyzer	Analyzer HostName	Analyzer IPAddress	Analyzer Name	Analyzer Version	Threat Severity	Threat Action	Threat Category	Threat EventID	Threat Handled
2019-03-04T18:55:18+05:30	ENDP_GS_1060	WIN-0R5VUVO6QVU	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-0R5VUVO6QVU	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-0R5VUVO6QVU	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-0R5VUVO6QVU	740320293	McAfee Endpoint Security	10.6.0.542	5	none	ops.update.end	1119	True

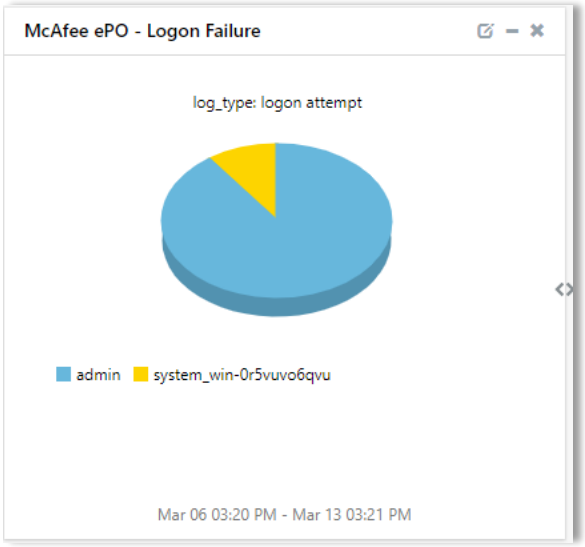
event_log_type	+- Application
event_type	+- Information
event_id	+- 3230
event_source	+- McAfee Threat
event_user_domain	+- N/A
event_computer	+- WIN-0R5VUVO6QVU
event_user_name	+- N/A
event_description	EPOEvents.ServerID : WIN-0R5VUVO6QVU EPOEvents.ReceivedUTC : 2019-03-01T14:58:50+05:30 EPOEvents.DetectedUTC : 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

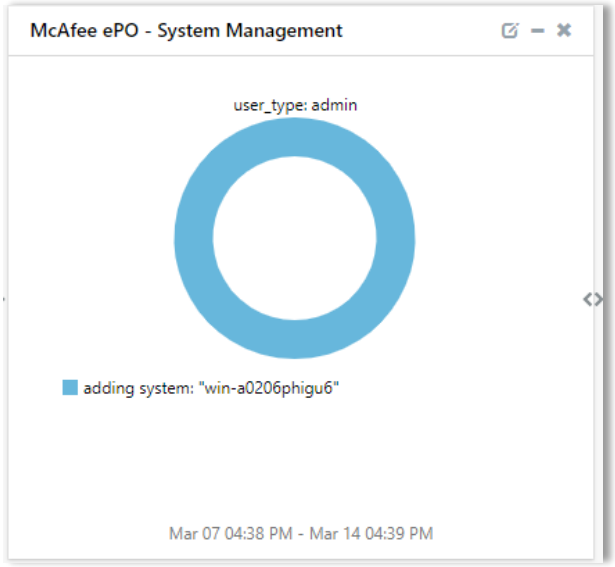
- **McAfee ePO – Log-On Failure -** This alert will generate ,when the user fails to logon attempt.
- **McAfee ePO - Policy Changes -** This alert will generate ,when the policy configuration changes.
- **McAfee ePO – Threat Detected –** This alert will generate ,when the threat is detected on McAfee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

4.3 Dashboards

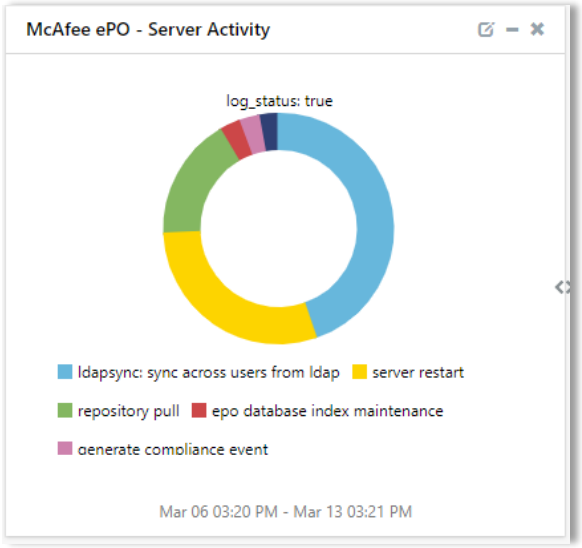
- **McAfee ePO – Logon Failure:**



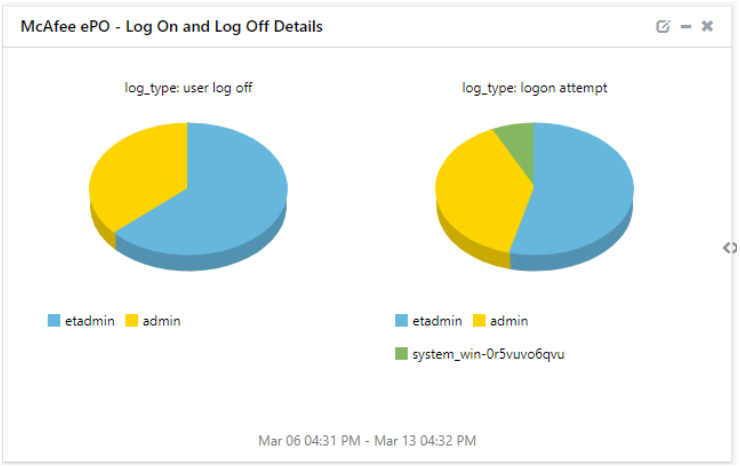
- **McAfee ePO – System Management**



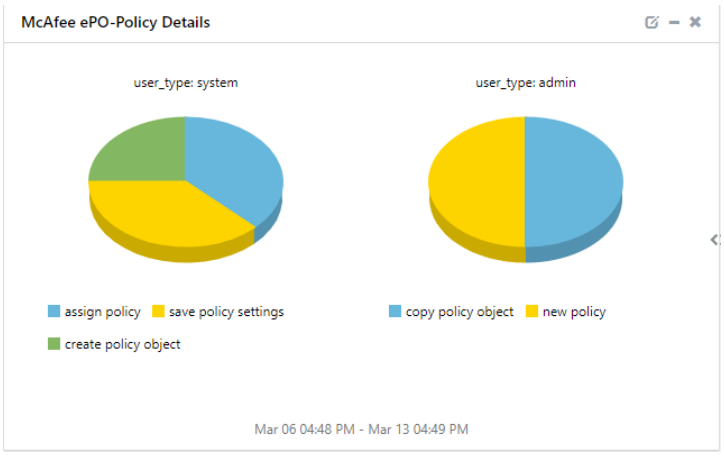
- **McAfee ePO – Server Activity**



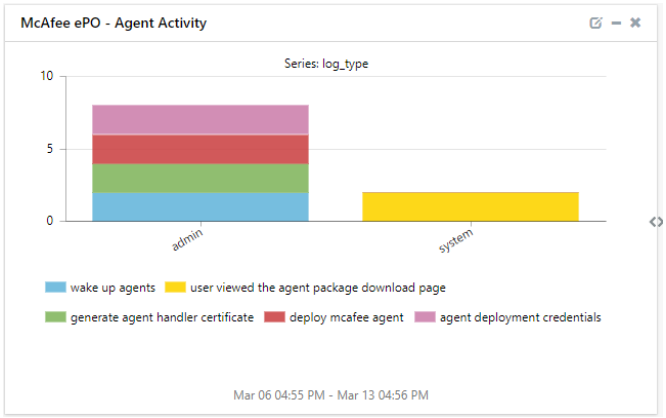
- **McAfee ePO – Log On and Log Off Details**



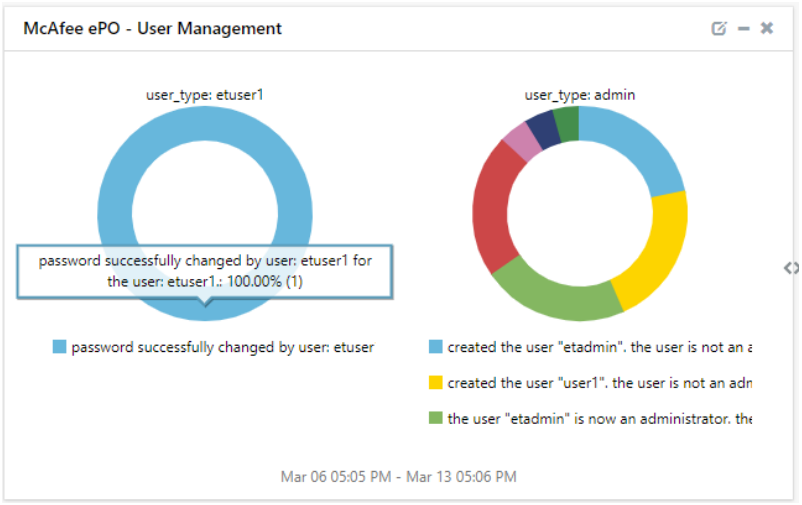
- **McAfee ePO – Policy Details**



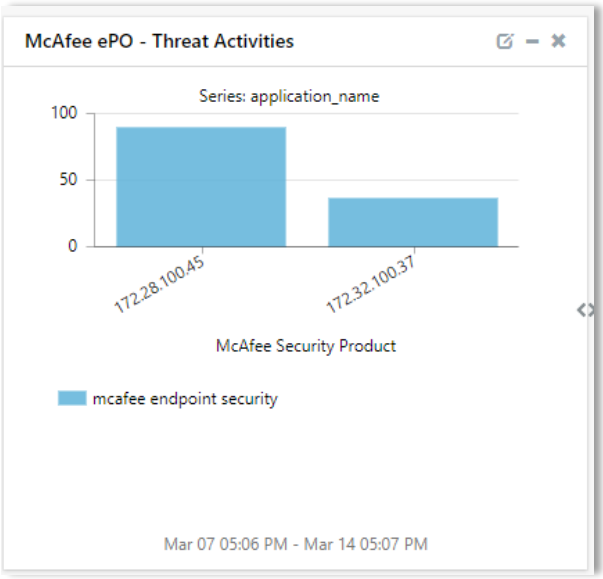
- **McAfee ePO – Agent Activity**



- **McAfee ePO – User Management**



- **McAfee ePO - Threat Activities**

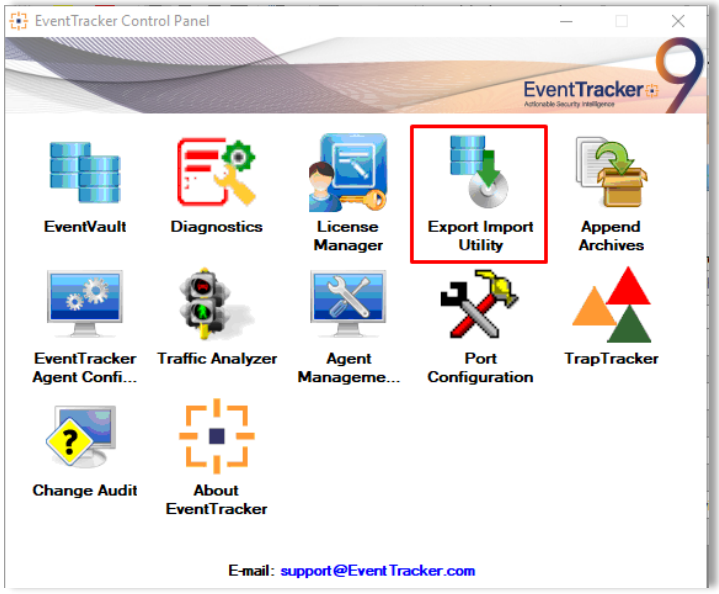


5. Importing McAfee ePolicy Orchestrator Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Values
- Knowledge Objects
- Flex Reports
- Dashboard

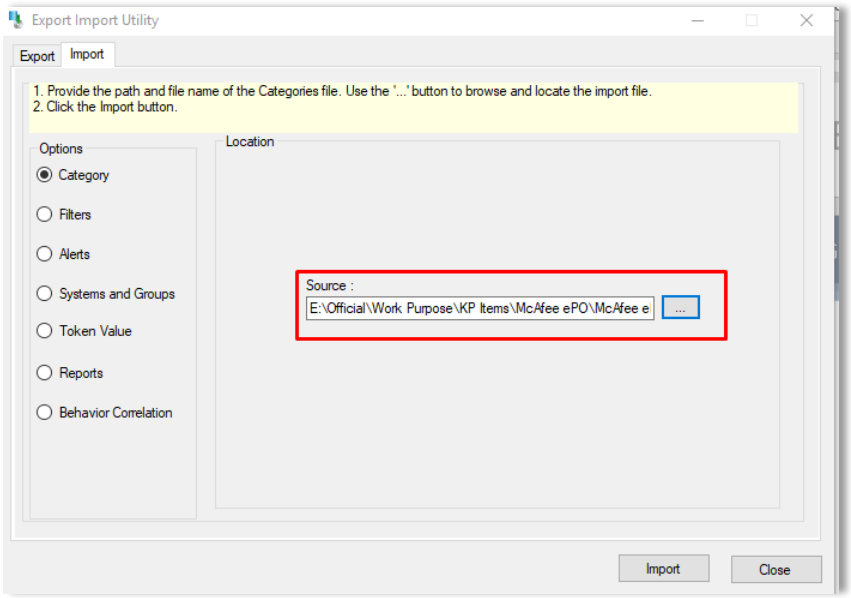
1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



3. Click the **Import** tab.

5.1 Category

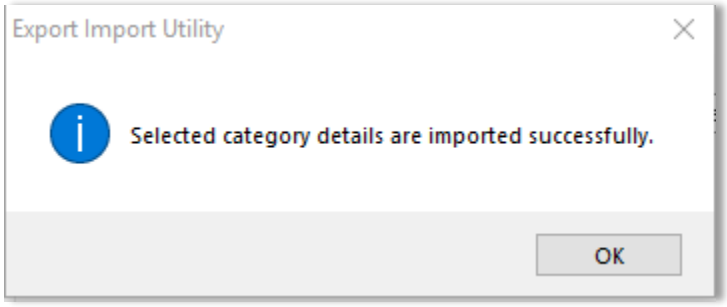
1. Click **Category** option, and then click the browse  button.



2. Locate "**.iscat"** file, and then click **Open**.

3. To import categories, click the **Import** button.

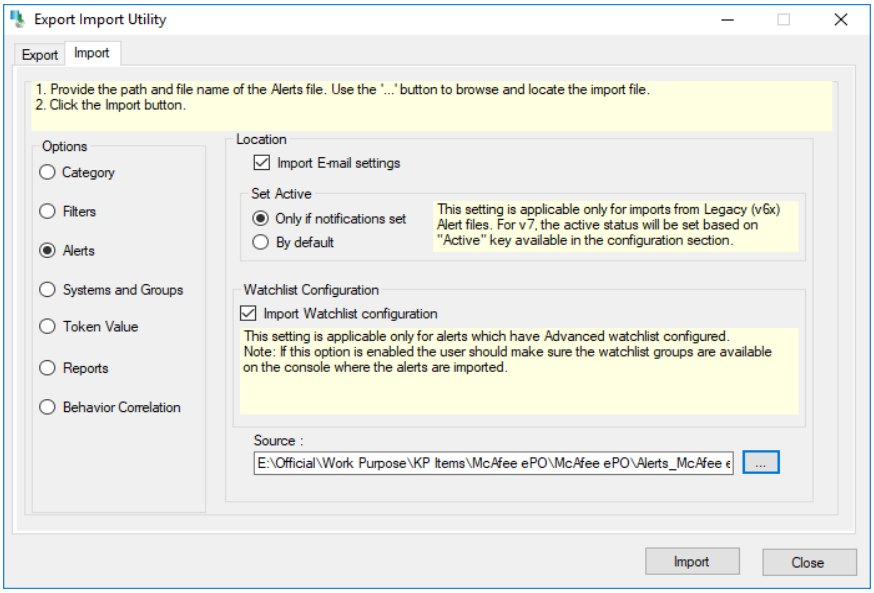
   EventTracker displays success message:



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

5.2 Alerts

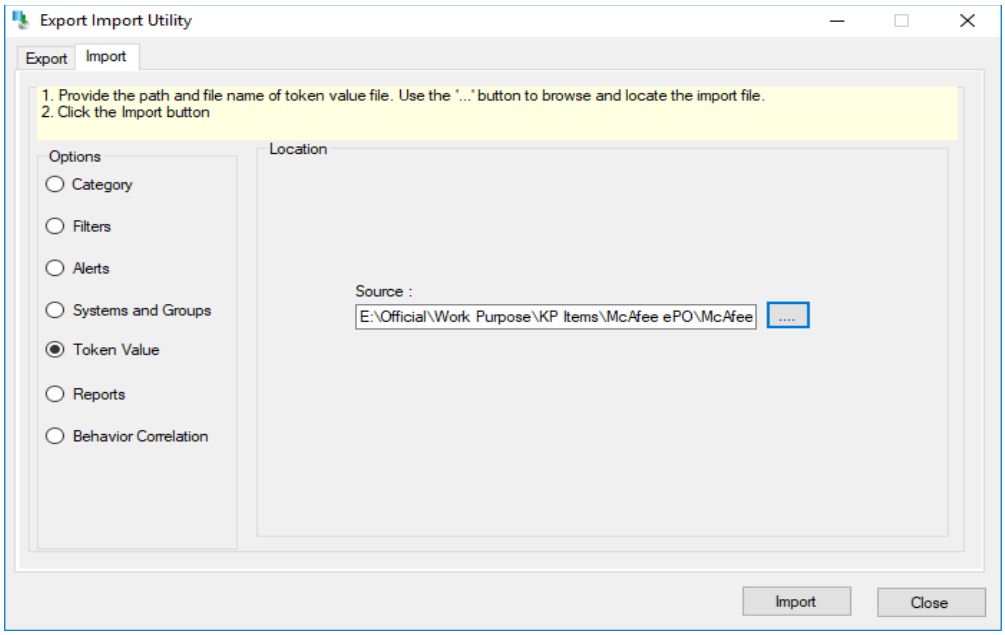
1. Click **Alert** option, and then click the browse  button.



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

5.3 Token Value

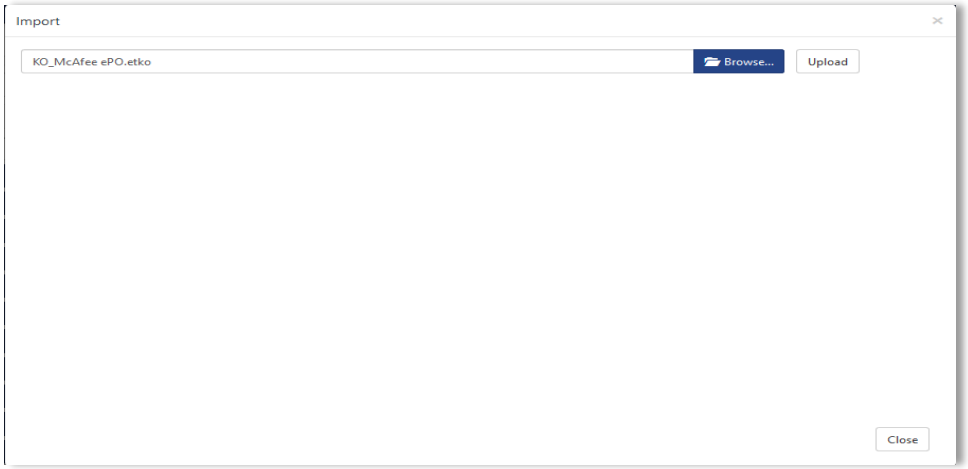
1. Click **Token Value** option, and then click the browse ... button.



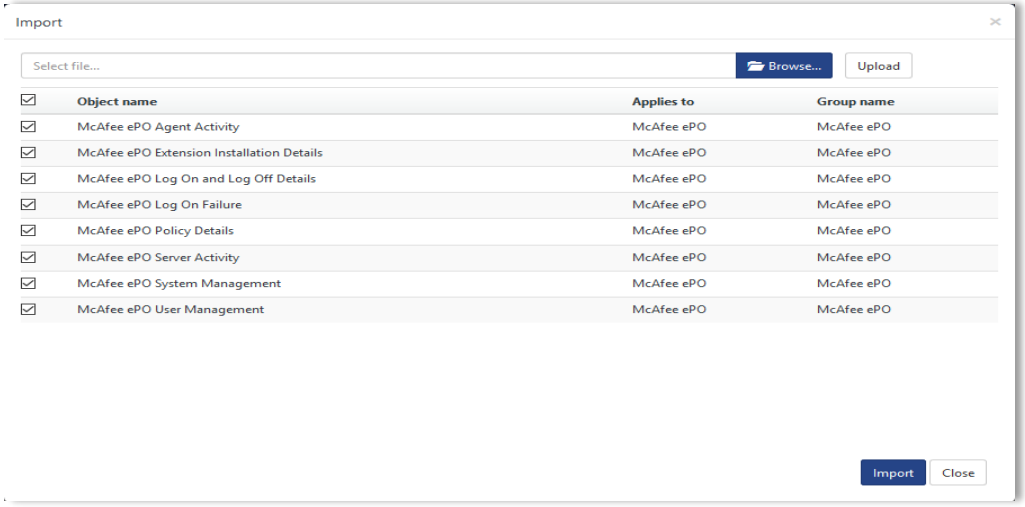
2. Locate "**.istoken"** file, and then click **Open**.
3. To import alerts, click **Import**.

5.4 Knowledge Objects

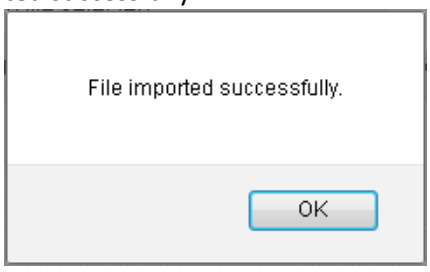
1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the "**.etko"** file.



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



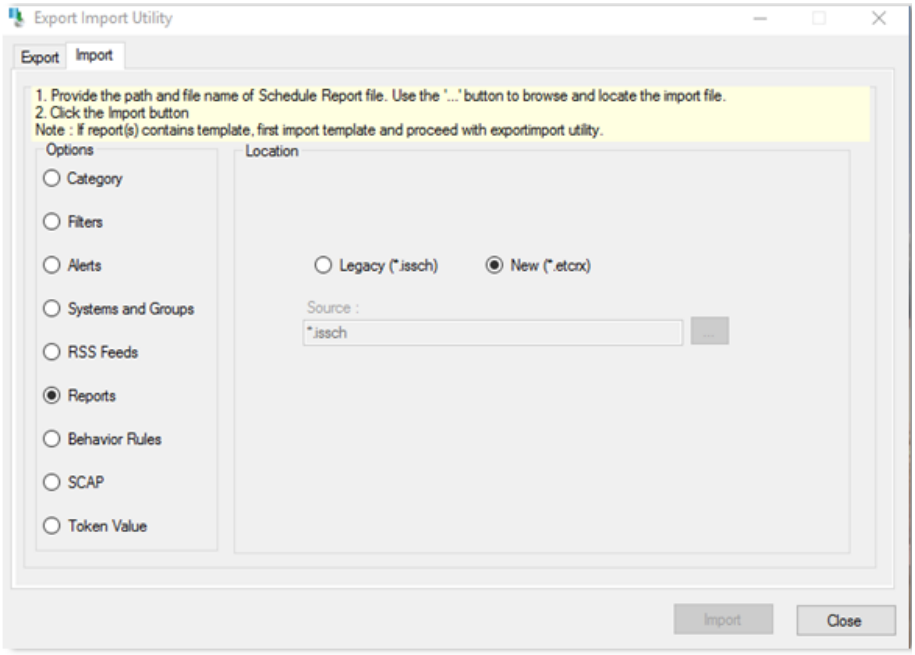
5. Knowledge objects are now imported successfully.



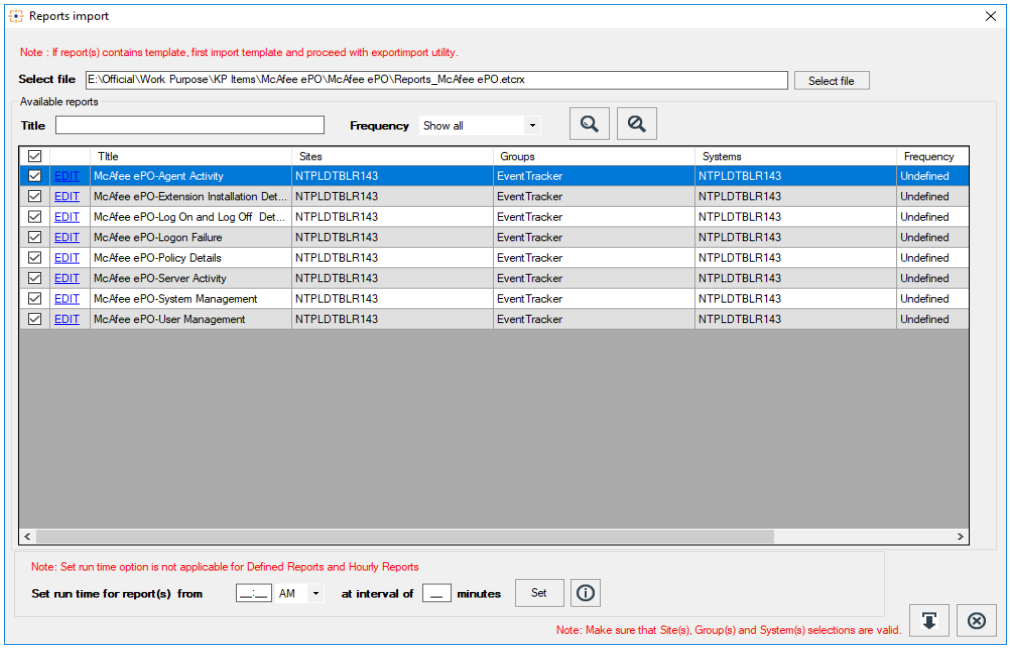
5.5 Flex Reports

On EventTracker Control Panel,

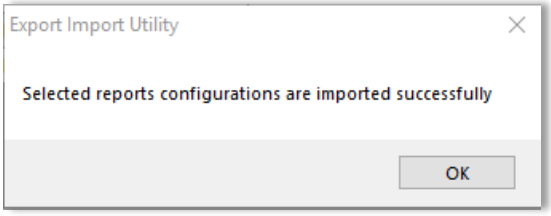
1. Click **Reports** option and select new (*.etcrx) from the option.



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

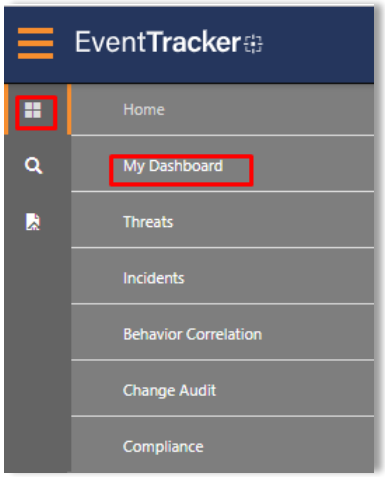


3. Click the **Import** button to import the reports. EventTracker displays success message.

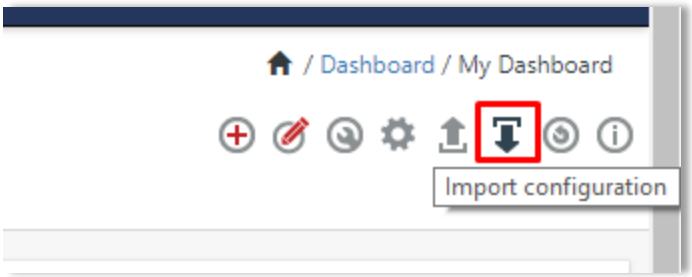


5.6 Dashboard

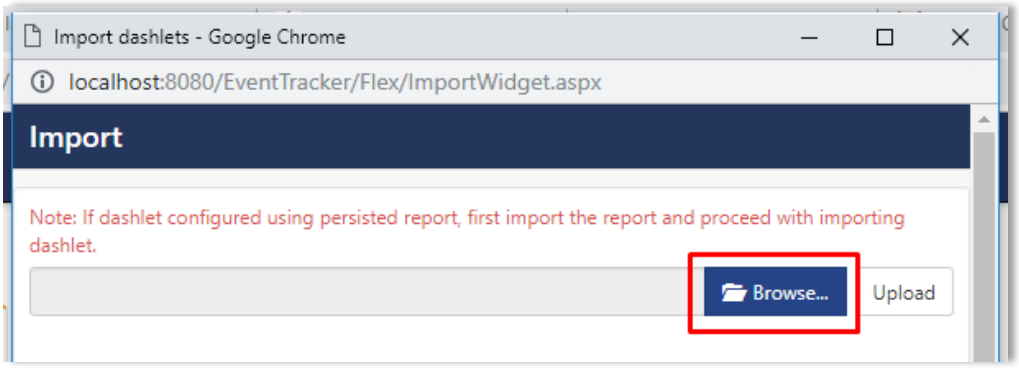
1. Logon to **EventTracker**.
2. Navigate to **Dashboard** → **My Dashboard**.



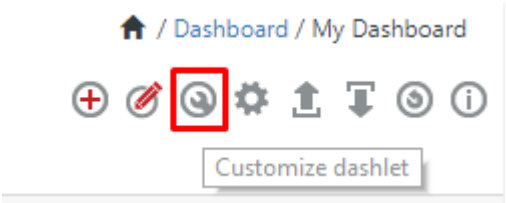
3. In **My Dashboard**, Click **Import Button**.



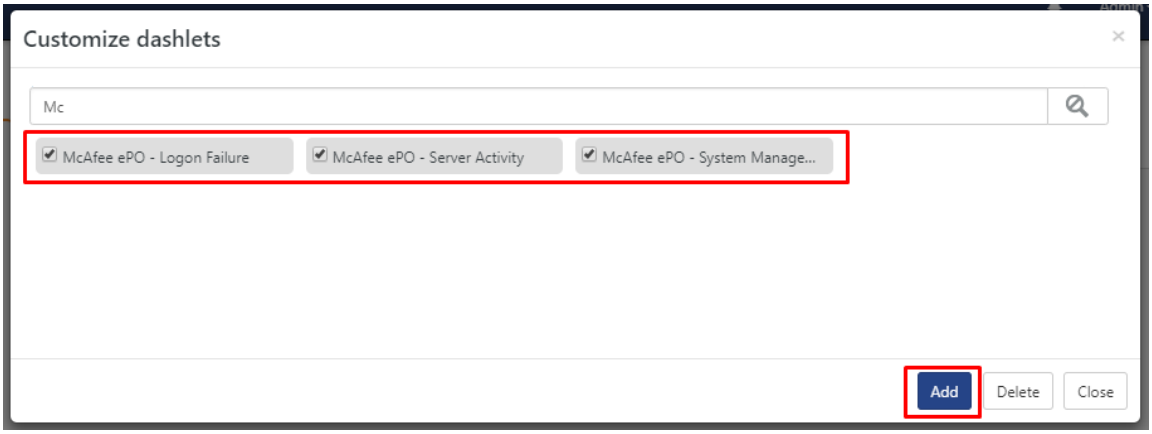
4. Select the **browse** button and navigate to file path where Dashboard file is saved.



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.**

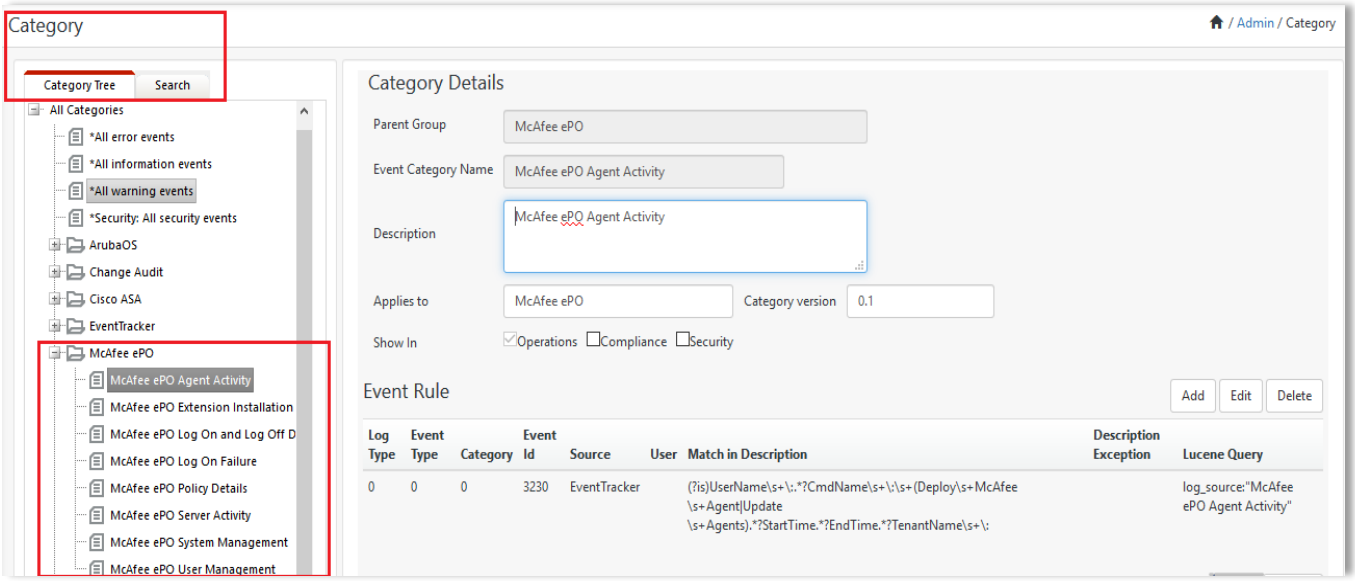


8. Once the **dashlets** gets populating, you see the following screen.

6. Verifying McAfee ePolicy Orchestrator knowledge pack in EventTracker

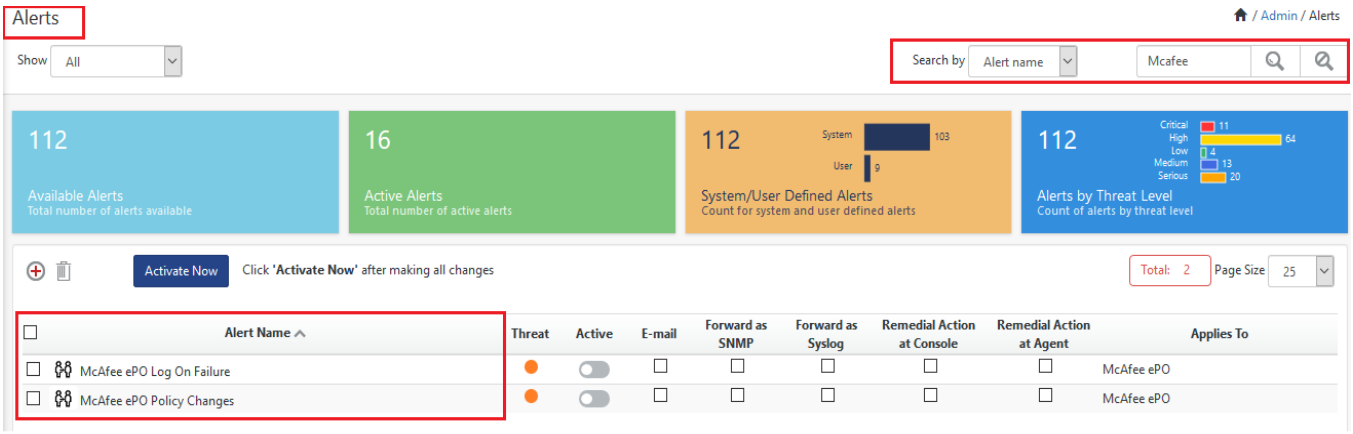
6.1 Categories

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.



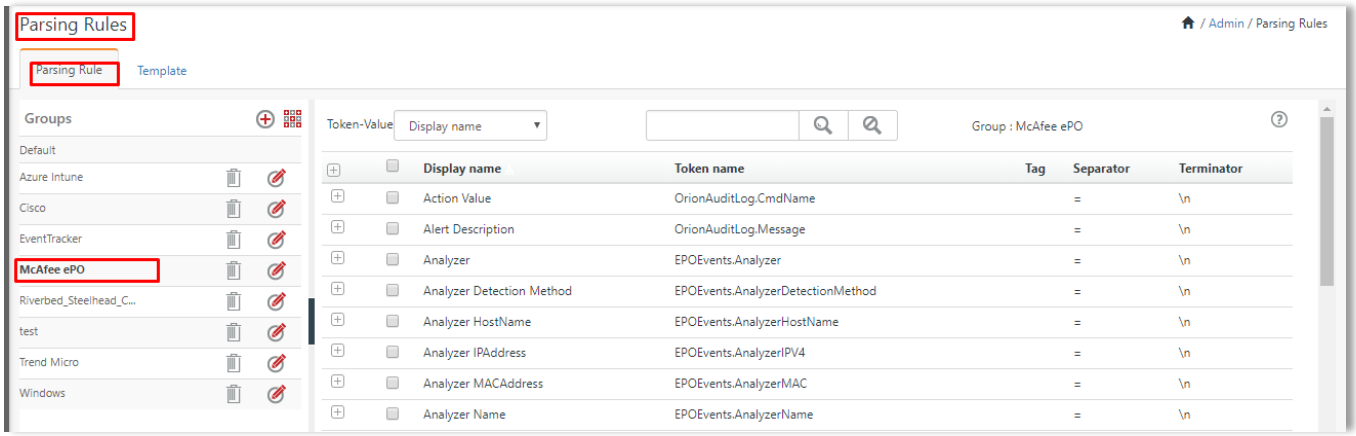
6.2 Alerts

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.**



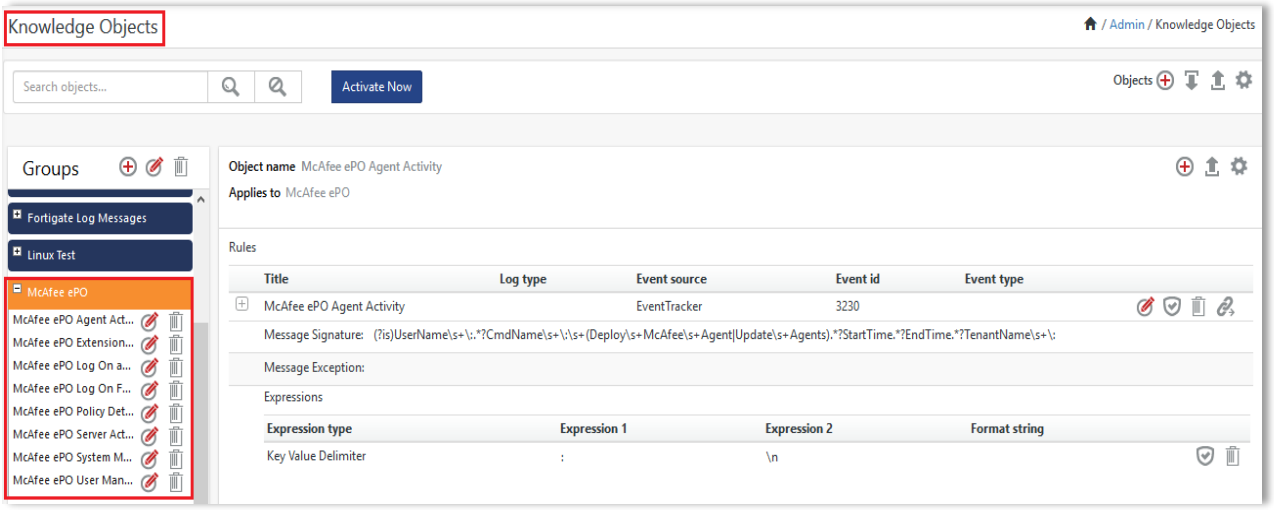
6.3 Token Value

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**.



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.



6.5 Flex Reports

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

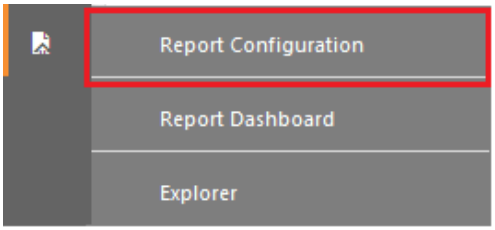
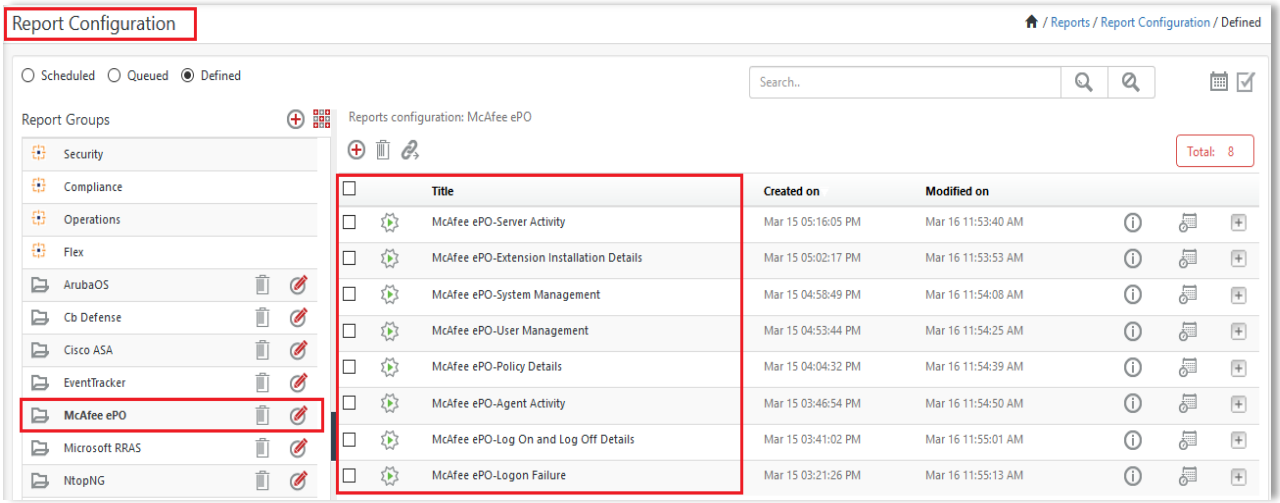


Figure 51

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



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 EventTracker 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 BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location 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 netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

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