Integrate McAfee ePolicy Orchestrator
EventTracker v8.x and above
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 configurations detailed in this guide are consistent with EventTracker Enterprise 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

Abstract .................................................................................................................. 1
Scope ......................................................................................................................... 1
Audience .................................................................................................................... 1
Overview ................................................................................................................... 3
Prerequisites ............................................................................................................. 3
Configure McAfee ePolicy Orchestrator to forward logs to EventTracker .............. 3
EventTracker Knowledge Pack ................................................................................ 4
  Flex Reports .......................................................................................................... 5
  Alerts ..................................................................................................................... 11
  Dashboards .......................................................................................................... 11
Import McAfee ePolicy Orchestrator knowledge pack into EventTracker ............... 14
  Category .............................................................................................................. 15
  Alerts .................................................................................................................... 16
  Token Value ........................................................................................................ 17
  Knowledge Objects .............................................................................................. 18
  Flex Reports ........................................................................................................ 19
  Dashboard ............................................................................................................ 20
Verify McAfee ePolicy Orchestrator knowledge pack in EventTracker .................... 23
  Categories .......................................................................................................... 23
  Alerts .................................................................................................................... 23
  Token Value ........................................................................................................ 24
  Knowledge Objects .............................................................................................. 24
  Flex Reports ........................................................................................................ 25
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. It’s knowledge object and flex reports that will help you to analyze critical activities (e.g. Threat Management) and to monitor login/logoff events.

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 administrative privilege on McAfee ePO server.

Configure McAfee ePolicy Orchestrator to forward logs to EventTracker

1. Contact EventTracker support for McAfee ePO Integrator.
2. Download and Run executable file “McAfeePOIntegrator.exe”.

![Figure 1](image)

3. Select the path to install Integrator and then click ‘Install’ button to proceed.
4. Enter McAfee console URL, Username and Password.
5. After entering the necessary details, click **Validate Credential** to confirm if the entered credentials are correct.

6. Click “**Finish**” button to complete the process.

---

**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 Enterprise to support McAfee ePolicy Orchestrator 5.10.
Flex Reports

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

![Table showing server activity data]

**Figure 4**

- **McAfee ePO - Policy Details** - This report gives information about details of Policy configuration changes.

![Sample log example]

**Figure 5**
Sample Logs:

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

Sample Log:

Figure 9

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

Sample Log:

Figure 10

Sample Log:

Figure 11
• **McAfee ePO - User Management** - This report gives information about user details which were added or removed, and permission changed.

<table>
<thead>
<tr>
<th>Event Date/Time</th>
<th>Computer</th>
<th>UserName</th>
<th>Priority</th>
<th>Action Value</th>
<th>Alert Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-02-28T14:28:14+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>admin</td>
<td>1</td>
<td>Remove User</td>
<td>User removed: ETUser1</td>
<td>False</td>
</tr>
<tr>
<td>2019-02-27T19:45:26+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>ETUser1</td>
<td>1</td>
<td>Change Password</td>
<td>Password successfully changed by user: ETUser1 for the user: ETUser1</td>
<td>True</td>
</tr>
<tr>
<td>2019-02-27T19:43:09+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>admin</td>
<td>1</td>
<td>Change Permission Sets for User</td>
<td>The user “ETUser1” was added to the following Permission Sets: Executive Reviewer, Group Reviewer.</td>
<td>True</td>
</tr>
</tbody>
</table>
| 2019-02-27T19:43:06+05:30 | WIN-0RSVUV0624VU | 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   |

**Figure 12**

**Sample Log:**

```plaintext
++ 0
++ WIN-0RSVUV0624VU
++ 3/14/2019 1:18:49 PM
++ 1592349729
OrionAuditLogUserName: admin
OrionAuditLogPriority: 1
OrionAuditLogEventName: New User
OrionAuditLogMessage: Created the user “ETUser1”.
The user is not an admin.
The user’s authentication type is “ePO authentication”.
The user’s account is enabled.
OrionAuditLogSuccess: True
OrionAuditLogStartTime: 2019-02-27T19:43:06+05:30
OrionAuditLogEndTime: 2019-02-27T19:43:06+05:30
++ 3230
++ Application
++ McAfee Audit
```

**Figure 13**

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

<table>
<thead>
<tr>
<th>Event Date/Time</th>
<th>Computer</th>
<th>UserName</th>
<th>Priority</th>
<th>Action Value</th>
<th>Alert Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-02-25T19:20:32+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>admin</td>
<td>1</td>
<td>Wake Up Agents</td>
<td>No agent wake-up calls were successful</td>
<td>False</td>
</tr>
<tr>
<td>2019-02-20T14:58:51+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>admin</td>
<td>5</td>
<td>Generate Agent Handler Certificate</td>
<td>Generated Agent Handler: WIN-0RSVUV0624VU certificate. Completed: 1, Failed: 0, Expired: 0</td>
<td>True</td>
</tr>
<tr>
<td>2019-02-28T16:30:53+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>admin</td>
<td>5</td>
<td>Wake Up Agents</td>
<td></td>
<td>True</td>
</tr>
<tr>
<td>2019-02-28T16:28:54+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>admin</td>
<td>5</td>
<td>Display McAfee Agent</td>
<td></td>
<td>True</td>
</tr>
<tr>
<td>2019-02-28T16:29:34+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>admin</td>
<td>5</td>
<td>Deploy McAfee Agent</td>
<td></td>
<td>True</td>
</tr>
<tr>
<td>2019-02-28T16:41:22+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>system</td>
<td>5</td>
<td>Streamed Agent Bootstrap Package to user</td>
<td>Streamed agent package to user, from IP address 172.32.100.3 (macsec)</td>
<td>True</td>
</tr>
<tr>
<td>2019-02-28T16:39:42+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>system</td>
<td>5</td>
<td>User viewed the Agent Package Download page</td>
<td>Created agent package file from IP address 172.32.100.3 (macsec)</td>
<td>True</td>
</tr>
<tr>
<td>2019-02-28T16:38:22+05:30</td>
<td>WIN-0RSVUV0624VU</td>
<td>system</td>
<td>5</td>
<td>Streamed Agent Bootstrap Package to user</td>
<td>Streamed agent package to user, from IP address 172.32.100.3 (macsec)</td>
<td>True</td>
</tr>
</tbody>
</table>

**Figure 14**
Sample Log:

```
event_category   ++  0
event_computer   ++  WIN-0RSVUVQ6QVU
event_datetime   ++  3/14/2019 1:18:50 PM
event_datetime_utc ++  1552548730
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
```

Figure 15

- **McAfee ePO - Log On and Log Off Details** - This report gives information about details of User log on and log off.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Category</th>
<th>Log Message</th>
<th>Log Priority</th>
<th>Log Value</th>
<th>User IP address</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/12/2019 12:26:59 AM</td>
<td>WIN-0RSVUVQ6QVU</td>
<td>Logon Attempt</td>
<td>Successful Login for user &quot;admin&quot; from IP address: 172.32.100.17</td>
<td>5</td>
<td>True</td>
<td>172.32.100.17</td>
<td>admin</td>
</tr>
<tr>
<td>03/09/2019 01:40:04 AM</td>
<td>WIN-0RSVUVQ6QVU</td>
<td>Logon Attempt</td>
<td>Successful Login for user &quot;ETAdmin (ETAdmin)&quot; from IP address: 172.32.100.30</td>
<td>5</td>
<td>True</td>
<td>172.32.100.30</td>
<td>ETAdmin</td>
</tr>
<tr>
<td>02/20/2019 12:41:29 AM</td>
<td>WIN-0RSVUVQ6QVU</td>
<td>Logon Attempt</td>
<td>Successful Login for user &quot;admin&quot; from IP address: 10.0.2.2</td>
<td>5</td>
<td>True</td>
<td>10.0.2.2</td>
<td>admin</td>
</tr>
<tr>
<td>02/20/2019 08:31:47 PM</td>
<td>WIN-0RSVUVQ6QVU</td>
<td>Logon Attempt</td>
<td>Successful Login for user &quot;admin&quot; from IP address: 10.0.2.15</td>
<td>5</td>
<td>True</td>
<td>10.0.2.15</td>
<td>admin</td>
</tr>
<tr>
<td>03/09/2019 02:06:42 AM</td>
<td>WIN-0RSVUVQ6QVU</td>
<td>User Log Off</td>
<td>User &quot;ETAdmin (ETAdmin)&quot; has logged out</td>
<td>5</td>
<td>True</td>
<td>10.0.2.2</td>
<td>ETAdmin</td>
</tr>
</tbody>
</table>

Sample Log:

```
event_category   ++  0
event_computer   ++  WIN-0RSVUVQ6QVU
event_datetime   ++  3/14/2019 1:26:04 PM
event_datetime_utc ++  1552500104
event_description
OrionAuditLog UserName : admin
OrionAuditLog Priority : 3
OrionAuditLog CmdName : Logon Attempt
OrionAuditLog Message : Successful Login for user "admin" from IP address: 10.0.2.2
OrionAuditLog Success : True
OrionAuditLog StartTime : 2019-02-26T14:46:49-08:00
OrionAuditLog EndTime : 2019-02-26T14:46:49-08:00
```

Figure 17
- **McAfee ePO - Logon Failure** - This report gives information about details of User log on failure.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Event DateTime</th>
<th>Event Priority</th>
<th>Reason</th>
<th>UserName</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-02-25T11:01:56+05:30</td>
<td>3</td>
<td>incorrect password</td>
<td>system_WIN-0RSVUV0SQVU</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-02-22T12:30:56+05:30</td>
<td>3</td>
<td>user auto-creation failure</td>
<td>Administrator</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-02-22T12:29:20+05:30</td>
<td>3</td>
<td>user auto-creation failure</td>
<td>Administrator</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-02-22T12:27:19+05:30</td>
<td>3</td>
<td>incorrect password</td>
<td>system_WIN-0RSVUV0SQVU</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-02-22T12:21:26+05:30</td>
<td>3</td>
<td>incorrect password</td>
<td>admin</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-03-04T16:43:20+05:30</td>
<td>3</td>
<td>incorrect password</td>
<td>system_WIN-0RSVUV0SQVU</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-03-04T16:42:00+05:30</td>
<td>3</td>
<td>user auto-creation failure</td>
<td>demo123</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-02-27T18:59:52+05:30</td>
<td>3</td>
<td>incorrect password</td>
<td>admin</td>
</tr>
<tr>
<td>WIN-0RSVUV0SQVU</td>
<td>2019-02-27T16:59:45+05:30</td>
<td>3</td>
<td>incorrect password</td>
<td>admin</td>
</tr>
</tbody>
</table>

**Figure 18**

**Sample Log:**

```plaintext
event_category  + 0
event_computer  + WIN-0RSVUV0SQVU
event_date_time + 3/14/2019 12:04 PM
event_date_time_utc + 1552530164
event_description
OnionAuditLog:UserName: demo123
OnionAuditLog:Priority : 1
OnionAuditLog:CmdName: Logon Attempt
OnionAuditLog:Message: Failed Logon for user "demo123" from IP address 172.32.100.17 due to user auto-creation failure
OnionAuditLog:Success : False
OnionAuditLog:StartTime: 2019-02-27T18:00:00+05:30
OnionAuditLog:EndTime: 2019-02-27T19:00:00+05:30

event_id + 3230
event_log_type + Application
event_source + McAfee Audit
```

**Figure 19**

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

<table>
<thead>
<tr>
<th>Log DateTime</th>
<th>Analyzer</th>
<th>Analyzer HostName</th>
<th>Analyzer IPAddress</th>
<th>Analyzer Name</th>
<th>Analyzer Version</th>
<th>Threat Severity</th>
<th>Threat Action</th>
<th>Threat Category</th>
<th>Threat EventID</th>
<th>Threat Handled</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-03-04T16:55:18+05:30</td>
<td>ENEP_0S_1068</td>
<td>WIN-0RSVUV0SQVU</td>
<td>749320293</td>
<td>McAfee Endpoint Security</td>
<td>10.6.0.542</td>
<td>5</td>
<td>none</td>
<td>ops.update.end</td>
<td>119</td>
<td>True</td>
</tr>
<tr>
<td>2019-03-04T16:55:18+05:30</td>
<td>ENEP_0S_1068</td>
<td>WIN-0RSVUV0SQVU</td>
<td>749320293</td>
<td>McAfee Endpoint Security</td>
<td>10.6.0.542</td>
<td>5</td>
<td>none</td>
<td>ops.update.end</td>
<td>119</td>
<td>True</td>
</tr>
<tr>
<td>2019-03-04T16:55:18+05:30</td>
<td>ENEP_0S_1068</td>
<td>WIN-0RSVUV0SQVU</td>
<td>749320293</td>
<td>McAfee Endpoint Security</td>
<td>10.6.0.542</td>
<td>5</td>
<td>none</td>
<td>ops.update.end</td>
<td>119</td>
<td>True</td>
</tr>
<tr>
<td>2019-03-04T14:55:18+05:30</td>
<td>ENEP_0S_1068</td>
<td>WIN-0RSVUV0SQVU</td>
<td>749320293</td>
<td>McAfee Endpoint Security</td>
<td>10.6.0.542</td>
<td>5</td>
<td>none</td>
<td>ops.update.end</td>
<td>119</td>
<td>True</td>
</tr>
</tbody>
</table>

**Figure 20**
Integrate McAfee ePolicy Orchestrator

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.

Dashboards

- **McAfee ePO – Logon Failure:**
- McAfee ePO – System Management

![McAfee ePO - System Management](image)

Figure 23

- McAfee ePO – Server Activity

![McAfee ePO - Server Activity](image)

Figure 24
• McAfee ePO – Log On and Log Off Details:

![Figure 25](image)

• McAfee ePO – Policy Details:

![Figure 26](image)

• McAfee ePO – Agent Activity:

![Figure 27](image)
- McAfee ePO – User Management:

![Figure 28](image1)

- McAfee ePO - Threat Activities:

![Figure 29](image2)

Import 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.

### Category

1. Click **Category** option, and then click the browse “...” button.
2. Locate “.iscat” file, and then click the **Open** button.

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

   EventTracker displays success message:

   ![Success message](image)

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

**Alerts**

1. Click **Alert** option, and then click the browse button.
2. Locate “.isalt” file, and then click the Open button.
3. To import alerts, click the Import button.

Token Value

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

2. Locate “.istoken” file, and then click the Open button.
3. To import alerts, click the Import button.
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. Now select all the check box and then click ‘Import’ option.
5. Knowledge objects are now imported successfully.

![File imported successfully](image)

**Figure 37**

**Flex Reports**

On EventTracker Control Panel,

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

![Export Import Utility](image)

**Figure 38**

2. Locate the **.etcrx** file, and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

![Figure 39](image1)

![Figure 40](image2)

**Dashboard**

1. Logon to **EventTracker Enterprise**.
2. Navigate to **Dashboard ➔ My Dashboard**.
3. In “My Dashboard”, Click Import Button:

   ![Figure 41]

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

   ![Figure 42]

5. Once completed, click “Upload” Button.

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

   ![Figure 43]
7. Now, put a text on **Search bar: “McAfee”** and then select the McAfee dashlets and then click “Add” button.

8. Once the **dashlets** gets populating, it will look like the below figure:
Verify McAfee ePolicy Orchestrator knowledge pack in EventTracker

Categories

1. Logon to EventTracker Enterprise.
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 Tree](image)

Figure 47

Alerts

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

Token Value

1. In the EventTracker Enterprise 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.

Knowledge Objects

1. In the EventTracker Enterprise 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.
Flex Reports

1. In the EventTracker Enterprise 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.
Figure 52