Integrate Microsoft Antimalware

EventTracker v8.x and above

Publication Date: September 6, 2017
Abstract

This guide provides instructions to configure Microsoft Antimalware to send logs to EventTracker Enterprise. Once logs are being configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Microsoft Antimalware.

Audience

Administrators who are responsible for monitoring Microsoft Antimalware which are running using EventTracker Manager.

The information contained in this document represents the current view of EventTracker on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract ........................................................................................................................................................................ 1
Scope ........................................................................................................................................................................ 1
Audience .................................................................................................................................................................. 1

Overview ...................................................................................................................................................................... 3
Prerequisites ............................................................................................................................................................ 3

Integration of MS Antimalware events to EventTracker server ................................................................. 3

EventTracker Knowledge Pack ................................................................................................................................. 5
Alerts ...................................................................................................................................................................... 5
Flex Reports ............................................................................................................................................................. 6

Import MS Antimalware knowledge pack into EventTracker ................................................................. 10
Alerts ...................................................................................................................................................................... 11
Knowledge Objects ................................................................................................................................................ 13
Flex Reports ........................................................................................................................................................... 15
Parsing Rule............................................................................................................................................................ 16

Verify MS Antimalware knowledge pack in EventTracker ................................................................. 18
Alerts ...................................................................................................................................................................... 18
Flex Reports ........................................................................................................................................................... 19
Parsing Rule............................................................................................................................................................ 19

Create Flex Dashboards in EventTracker ........................................................................................................ 20
Schedule Reports ................................................................................................................................................ 20
Create Dashlets ................................................................................................................................................... 23
Sample Flex Dashboards ....................................................................................................................................... 27
Overview

Microsoft Antimalware is an antivirus software (AV) product that fights malware (malicious software), including computer viruses, spyware, Trojan horses and rootkits. The software runs on Windows XP, Windows Vista and Windows 7. Built upon the same virus definitions and scanning engine as other Microsoft antivirus products, Microsoft Antimalware Service provides real-time protection, constantly monitoring activities on the computer and scanning new files as they are downloaded or created and disable detected threats.

EventTracker integrates Microsoft Antimalware and provides reports, knowledge objects and dashboards for all generated events including attacks, configuration changes etc. EventTracker will also monitor antivirus sensors and process execution statuses for all workstations in the network.

Prerequisites

- EventTracker v8.x should be installed.
- You must have a valid and active Azure subscription account to use the Microsoft antimalware for Azure features and deploy antimalware for your cloud services and or virtual machines.
- The Microsoft Antimalware solution is supported on Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 operating system families.
- The VM agent is required to run the Microsoft antimalware extension on the virtual machine. Make sure VM agent is enabled on the VM.

Integration of MS Antimalware events to EventTracker server

Once you deploy the Azure portal, follow the below steps to enable the logging.

1) In the Recommendations blade, select **Enable data collection for subscriptions**. This opens the **Turn on data collection** blade.
2) On the **Turn on data collection** blade, select your subscription. The Security policy blade for that subscription opens.

3) On the **Security policy** blade, select ‘On’ under Data collection to automatically collect logs. Turning on data collection provisions the monitoring extension on all current and new supported VMs in the subscription.

4) Select **Save**.

5) Select **OK**.

6) Also, please ensure that in the VM the security extensions need to be enabled during the creation of a VM as shown below.

7) These are Virtual machine environments, so once enabled the extension, events will be shown in the Event Viewer.
EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Alerts

- **MS Antimalware-Action taken against malware activity**: This alert is generated when an action is taken against the detected malware.
- **MS Antimalware-Detected malware activity**: This alert is generated when any malware activity is detected.
- **MS Antimalware-Quarantined malware restored**: This alert is generated when a quarantined malware is restored.
- **MS Antimalware-Removed history of malware**: This alert is generated when the malware history is removed or deleted.
Flex Reports

- **MS Antimalware-Action taken against malware activity** - This report provides details about all the action taken against malware activities.

Logs Considered:

- **MS Antimalware-Detected malware activity** - This report provides details about all the malwares that are detected by Microsoft Antimalware.
Logs Considered:

- **MS Antimalware-Quarantined malware restored**- This report provides details on all the quarantined malwares that were restored.
Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/11/2017 4:22:33 PM</td>
<td>1013</td>
<td>NTPLDBLR38 / PNPL-1</td>
<td>N/A</td>
<td>N/A</td>
<td>Microsoft Antimalware</td>
</tr>
</tbody>
</table>

Event Type: Information
Log Type: Application
Category Id: 0

**Description:**
Microsoft Antimalware has restored an item from quarantine.
For more information please see the following link:
http://go.microsoft/fwlink/?linkid=370206\&name=HackTool.PowerShell\%2FSa\%2FThreadid-2147722658\&enterprise=1
Name: HackTool\%2FPowerShell\%2FThreadid-2147722658
Severity: Medium
Category: Tool
Path: C:\\Windows\\Temp\\RZWzhlnpYbat
User: CORPDAGNER300
Signature Version: AV: 1.249.20.0, AS: 1.249.20.0
Engine Version: 1.1.14003.0

**MS Antimalware-Removed history of malware** - This report provides details about the malware history that was removed.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/10/2017 06:26:08 PM</td>
<td>PNPL-15-KP</td>
<td>Antimalware has removed history of malware and other potentially unwanted software.</td>
<td>NT AUTHORITY\SYSTEM</td>
</tr>
</tbody>
</table>

Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/11/2017 4:22:33 PM</td>
<td>1013</td>
<td>NTPLDBLR38 / PNPL-1</td>
<td>N/A</td>
<td>N/A</td>
<td>Microsoft Antimalware</td>
</tr>
</tbody>
</table>

Event Type: Information
Log Type: Application
Category Id: 0

**Description:**
Microsoft Antimalware has restored an item from quarantine.
For more information please see the following link:
http://go.microsoftrors://go.microsoft.com/fwlink/?linkid=370206\&name=HackTool\%2FPowerShell\%2FThreadid-2147722658\&enterprise=1
Name: HackTool\%2FPowerShell\%2FThreadid-2147722658
Severity: Medium
Category: Tool
Path: C:\\Windows\\Temp\\RZWzhlnpYbat
User: CORPDAGNER300
Signature Version: AV: 1.249.20.0, AS: 1.249.20.0
Engine Version: 1.1.14003.0

**MS Antimalware-Service stopped** - This report provides details about all the services that are stopped.
Integrate Microsoft Antimalware EventTracker

Logs Considered:

- **MS Antimalware-Configuration changes** - This report provides details about all the configuration changes that are done.
Logs Considered:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site/Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/11/2017 4:22:31 PM</td>
<td>0007</td>
<td>NTPLDTRJ85 / PNR-1</td>
<td>N/A</td>
<td>N/A</td>
<td>Microsoft Antimalware</td>
</tr>
</tbody>
</table>

Event: Type: Information
Log Type: Application
Category ID: 0

Description:
Microsoft Antimalware Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.
Old value: HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x185
New value: HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x186

Import MS Antimalware knowledge pack into EventTracker

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

- Knowledge Objects
- Alerts
- Flex Reports
- Parsing Rule

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

- Knowledge Objects
- Alerts
- Flex Reports
- Parsing rule

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility.
3. Click the **Import** tab.

**Alerts**

1. Click **Alerts** option, and then click the browse button.
2. Locate the **MS Antimalware alerts.isalt** file, and then click the **Open** button.
2. To import alerts, click the **Import** button.

   EventTracker displays success message.

3. Click **OK**, and then click the **Close** button.
Knowledge Objects

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

![Figure 6](image)

2. Locate the **MS Antimalware knowledge objects.etko**, and then click **Import** button.

![Figure 7](image)

3. Choose the Knowledge objects that needs to be imported and click on **upload**.
4. Knowledge objects are now imported successfully.
Flex Reports

1. Click **Reports** option, and then click the browse button.
2. Locate the **MS Antimalware reports.etcxr** file, and then click the **Open** button.

![Export Import Utility](image)

**Figure 10**
3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

**Figure 11**

**Figure 12**

**Parsing Rule**

1. Click **Token Value** option, and then click the browse button.
2. Locate the **MS Antimalware Token Value.istoken** file, and then click the **Open** button.

![Figure 13](image)

4. Click the **Import** button to import the tokens. EventTracker displays success message.

![Figure 14](image)
Verify MS Antimalware knowledge pack in EventTracker

Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In the Search field, type MS Antimalware, and then click Go button.
3. Alert Management page will display the imported MS Antimalware alert.

![Alert Management Page](image)

Figure 15

4. To activate the imported alerts, select the respective checkbox in the Active column. EventTracker displays message box.

![Successfully saved configuration](image)

Figure 16

5. Click the OK button, and then click the Activate now button.

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the Activate Now button.
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.
2. In Reports Configuration pane, select Defined option.
3. In search box enter 'MS Antimalware, and then click the Search button.
   EventTracker displays Flex reports of 'MS Antimalware

![Image of EventTracker interface showing Flex reports of MS Antimalware]

Parsing Rule

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules.
3. Click on MS Antimalware group option.
Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.

3. Select MS Antimalware in report groups. Check Defined dialog box.
4. Click on ‘schedule’ to plan a report for later execution.
5. Click Next button to proceed.
6. In review page, check Persist data in EventVault Explorer option.
7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable Retention period.
8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

**Create Dashlets**

1. Open **EventTracker Enterprise** in browser and logon.
2. Navigate to **Dashboard** > **Flex**. Flex Dashboard pane is shown.

3. Fill suitable title and description and click **Save** button.

4. Click to configure a new flex dashlet. Widget configuration pane is shown.
5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.
Integrate Microsoft Antimalware EventTracker

15. Click ‘customize’ to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.

Sample Flex Dashboards

- REPORT: MS Antimalware-Action taken against malware activity
  WIDGET TITLE: MS Antimalware-Action taken against malware activity
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Threat Name
  LEGEND [SERIES]: Severity
- **REPORT: MS Antimalware-Quarantined malware restored**
  - **WIDGET TITLE:** MS Antimalware-Quarantined malware restored
  - **CHART TYPE:** Stacked Column
  - **AXIS LABELS [X-AXIS]:** Threat Name
  - **LEGEND [SERIES]:** User Name

  ![MS Antimalware-Quarantined malware restored chart](image1)

- **REPORT: MS Antimalware-Removed history of malware**
  - **WIDGET TITLE:** MS Antimalware-Removed history of malware
  - **CHART TYPE:** Donut
  - **AXIS LABELS [X-AXIS]:** User Name
  - **LEGEND [SERIES]:** Message

  ![MS Antimalware-Removed history of malware chart](image2)
- REPORT: MS Antimalware-Service stopped
  WIDGET TITLE: MS Antimalware-Service stopped
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Scan Id
  LEGEND [SERIES]: User Name

- REPORT: MS Antimalware-Configuration changes
  WIDGET TITLE: MS Antimalware-Configuration changes
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Old Value
  LEGEND: New Value