Integrate Malwarebytes
EventTracker Enterprise
Abstract

This guide provides instructions to configure Malwarebytes to send the logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise, and Malwarebytes 1.6.1.2997 and 1.7.0.3208.

Target Audience

Malwarebytes users, who wish to forward logs to EventTracker Manager.
# Table of Contents

Abstract ........................................................................................................................................................................ 1  
Scope ........................................................................................................................................................................ 1  
Target Audience ....................................................................................................................................................... 1  
Overview ....................................................................................................................................................................... 3  
Pre-requisite ................................................................................................................................................................ 3  
Configuration for sending logs to EventTracker ........................................................................................................ 3  
  Creating Task Scheduler .......................................................................................................................................... 3  
  Configure log file monitor (LFM) for monitoring Malwarebytes .......................................................................... 9  
  Enable Syslog to forward Malwarebytes Antimalware and Anti-Exploit logs to EventTracker manager .... 14  
EventTracker Knowledge Pack (KP) .......................................................................................................................... 16  
  Category ................................................................................................................................................................. 16  
  Reports ................................................................................................................................................................... 17  
  Alerts ...................................................................................................................................................................... 23  
Import Malwarebytes Knowledge Pack into EventTracker .................................................................................... 23  
  Category ................................................................................................................................................................. 24  
  Alerts ...................................................................................................................................................................... 25  
  Parsing Rules ......................................................................................................................................................... 26  
  Templates ............................................................................................................................................................... 27  
  Reports ................................................................................................................................................................... 28  
Verify Knowledge Pack in EventTracker................................................................................................................... 29  
  Categories .............................................................................................................................................................. 29  
  Alerts ...................................................................................................................................................................... 30  
  Template .............................................................................................................................................................. 31  
  Parsing Rules ......................................................................................................................................................... 31  
  Reports ................................................................................................................................................................... 32  
Create Dashboards in EventTracker ........................................................................................................................... 33  
  Schedule Reports ................................................................................................................................................... 33  
  Create Dashlets ..................................................................................................................................................... 35  
Sample Dashboards ................................................................................................................................................... 40
Overview

Malwarebytes Endpoint Security integrates all of our industry-leading protection and remediation technology into one powerful solution. This solution combines advanced malware detection and remediation, malicious website blocking, and exploit protection in a centrally-managed platform scalable up to thousands of endpoints.

EventTracker collects and analyses events and enlightens an administrator about threat detection, scan details, changes in admin, client and policy modules.

Pre-requisite

- EventTracker Enterprise v7.x for report and alert should be installed.
- Malwarebytes Management Console should be installed.
- EventTracker agent should be installed on Malwarebytes Management Console system.
- Firewall between EventTracker manager and Malwarebytes Management Console system should be off or made exception for port 14505.

Configuration for sending logs to EventTracker

**NOTE:** To fetch logs from the database, PowerShell script is created to query the database and scheduled to extract the specific database tables to folder.

1. **Adminlogs** and **Clientsecuritylogs** are on the database and to forward these logs to EventTracker Enterprise, requires Log File Monitoring (LFM).

2. **Syslog** configuration is required to receive logs from the client machine when threat has been detected.

Creating Task Scheduler

Download the Malwarebytes Knowledge Pack zip file, extract and copy the files to Malwarebytes manager machine. Use the **Malwarebytes.ps1** script to schedule as below mentioned:

1. Create scheduled task to run script automatically.
2. In the **Task Scheduler**, select the **Create Task** option under **Actions** heading on the right-hand side.
3. In **General** tab, enter name of the task and specify the description. Under **security options** specify the user account and change the settings to "**Run with highest privileges**" as the script runs with admin privileges and select **'Run whether user is logged on or not'**.
4. Next, select **Triggers** tab and click **New** to add a new trigger for the scheduled task.
5. Select **On a Schedule** option, the start date can be set to a desired time, and the frequency and duration of the task can be set. Click **OK** when desired settings are entered.
EventTracker: Integrating Malwarebytes

Figure 4
6. Next, go to the **Actions** tab and click **New** to set the action for this task to run. Set the Action to **Start a program**.

7. In the **Program/script** box enter "**PowerShell.exe**"

   In the **Add arguments (optional)** box enter the **Set Execution Policy** value example:

   ```ps
   -ExecutionPolicy Bypass –File
   C:\Users\Administrator\Malwarebytes\Malwarebytes.ps1
   ```
8. Once all the desired actions are made (or added), click OK. The task will be immediately set, and is ready to run.

Configure log file monitor (LFM) for monitoring Malwarebytes

**NOTE:** Once scheduled task writes the logs to the defined folder, configure LFM.

To perform LFM configuration, deploy the EventTracker agent on Malwarebytes management console manager machine. Please refer [EventTracker Agent installation guide](#). After installation of the ET agent, check the steps to configure LFM.

1. Select the **Start** button, select **Prism Microsystems**, and then select **EventTracker Control Panel**.
2. Double-click **EventTracker Agent Configuration**.
3. Select **Logfile Monitor** tab
4. Click the button **Add File Name** and select the **.csv file** which has been generated and then click **OK**.
5. Select **Get All Existing Log Files** option.
6. In **Select Log File Type** drop down, select the **CSV** option.
7. Enter the path of the Malwarebytes logs.

8. Click the **OK** button.
9. Now, click the **Search String** button.
10. Select **Add String**.

11. Select the string that needs to be searched in the selected logs. If any of the string matches, then a log gets generated.
12. Click **Save**

Logs will be sent to the EventTracker Enterprise.
Enable Syslog to forward Malwarebytes Antimalware and Anti-Exploit logs to EventTracker manager.

1. Log into Malwarebytes Management Console.

2. Select **Admin** module from the console.
3. Select tab -> **Syslog Settings** and select **Enable Syslog** checkbox.

4. Enter the IP Address: **192.168.1.78** i.e. IP address of EventTracker Manager.

5. Port **514** (Syslog port).

6. Protocol: **UDP**.

7. Message settings → Select Facility: **23**, Severity: **0** and Payload to **CEF**.

8. Click **OK** to save the settings.
NOTE: Only when the threat is detected by the Antimalware and Anti-Exploit client machines then logs are forwarded to EventTracker Manager Machine.

EventTracker Knowledge Pack (KP)

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

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

**Category**

- **Malwarebytes: Management console user logon and logoff**
  This category provides information when user logs on to or logs off from the managed console.

- **Malwarebytes: User management**
  This category provides information related to user management where user accounts are created, removed, enabled or disabled by the administrator.

- **Malwarebytes: User password changed**
  This category provides information related to user password changes where user’s password has been changed by the administrator.

- **Malwarebytes: Policy management**
  This category provides information related to policy management where policies are created, removed, modified, enabled or disabled by the administrator.

- **Malwarebytes: Threat detection**
  This category provides information related to threats detected on the client machine.

- **Malwarebytes: Group management**
  This category provides information related to group management where groups are created, modified, and removed by the administrator on the console.

- **Malwarebytes: Client management activity**
  This category provides information related to client management activity where installation, uninstallation and simulate of client software is pushed from the managed console to the respective clients.
• **Malwarebytes: Scan status**  
  This category provides the information related to scan status i.e. when the last scan was performed and also the last scan result of the client machine.

**Reports**

• **Malwarebytes-Management console user logon and logoff**  
  This report provides the information related to user logged on and logged off from the Malwarebytes management console.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Admin User Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/19/2016 5:59:29 PM</td>
<td>WIN-1LRC038CCP</td>
<td>Admin</td>
<td>logon</td>
</tr>
<tr>
<td>7/19/2016 6:48:44 PM</td>
<td>WIN-1LRC038CCP</td>
<td>Admin</td>
<td>logoff</td>
</tr>
</tbody>
</table>

**Logs Considered:**

- **Figure 17**

- **Figure 18**

• **Malwarebytes: User management**  
  This report provides the information related to user management where administrator create, remove, import, enable or disable the users from management console.
Logs Considered:

Malwarebytes: User password changed
This report provides the information related to user password changes by the administrator on management console.
• **Malwarebytes-Policy management**
  This report provides information related to policy management where administrator create, edit, remove, deploy, switch clients, enable or disable the policy.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Admin User Name</th>
<th>Action</th>
<th>Client IP or Host Name</th>
<th>Policy Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/22/2016 5:13:32 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Edit</td>
<td></td>
<td>Default Policy</td>
</tr>
<tr>
<td>7/22/2016 5:29:25 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Create</td>
<td></td>
<td>Computing</td>
</tr>
<tr>
<td>7/22/2016 5:29:32 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Deploy</td>
<td></td>
<td>Computing</td>
</tr>
<tr>
<td>7/22/2016 5:29:46 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Switch client</td>
<td>ESXWIN7VM4</td>
<td>Computing</td>
</tr>
<tr>
<td>7/22/2016 2:19:49 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Disable</td>
<td></td>
<td>Finance</td>
</tr>
<tr>
<td>7/22/2016 2:19:53 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Enable</td>
<td></td>
<td>Computing</td>
</tr>
<tr>
<td>7/22/2016 3:08:06 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Edit</td>
<td></td>
<td>HR</td>
</tr>
<tr>
<td>7/22/2016 3:08:06 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Edit</td>
<td></td>
<td>Networking</td>
</tr>
<tr>
<td>7/22/2016 4:54:52 PM</td>
<td>WIN-1LRG03833CP</td>
<td>Admin</td>
<td>Remove</td>
<td></td>
<td>Computing</td>
</tr>
</tbody>
</table>

**Figure 23**

**Logs Considered:**

- **Event Type:** Information
  - Log Type: System
  - Category Id: 2

**Event 1:**
- Description: Entry: ID: 198
  - Time: 7/22/2016 5:29:25 PM
  - Admin User: Admin
  - ConsoleIP: 127.0.0.1
  - EventCategory: Policy
  - EventID: 2000
  - Description: Create policy (Computing)
  - ServerName: WIN-1LRG03833CP
  - Data: FILE:C:\Program Files (x86)\Prism\Management\EventTracker\Malwarebytes\Malwarebytes.csv
  - TYPE:CSV

**Event 2:**
- Description: Entry: ID: 249
  - Time: 7/22/2016 5:29:32 PM
  - Admin User: Admin
  - ConsoleIP: 127.0.0.1
  - EventCategory: Policy
  - EventID: 2001
  - Description: Edit policy (Computing)
  - ServerName: WIN-1LRG03833CP
  - Data: FILE:C:\Program Files (x86)\Prism\Management\EventTracker\Malwarebytes\Malwarebytes.csv
  - TYPE:CSV

**Figure 24**

• **Malwarebytes-Group management**
  This report provides the information related to group management where administrator create, modify, remove the groups and move the clients to different group from management console.
Malwarebytes-Client management activity
This report provides information related to client management activity when administrator performs the client push install activity from the management console.
EventTracker: Integrating Malwarebytes

Figure 27

Logs Considered:

- **Malwarebytes-Scan status**
  This report provides information related to scan details about last scan time, policy used, database updated time, database version, client version updated to and threat detected on the client machine.

Figure 28

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Admin User Name</th>
<th>Client IP or Host Name</th>
<th>Action</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/19/2016 7:34:11 PM</td>
<td>WIN-1LRCG038CCCP</td>
<td>Admin</td>
<td>10.10.1.70</td>
<td>Installation failed</td>
<td>Access is denied</td>
</tr>
<tr>
<td>7/20/2016 3:22:44 PM</td>
<td>WIN-1LRCG038CCCP</td>
<td>Admin</td>
<td>10.10.1.76</td>
<td>Detection failed</td>
<td>The specified network password is not correct</td>
</tr>
<tr>
<td>7/22/2016 4:37:09 PM</td>
<td>WIN-1LRCG038CCCP</td>
<td>Admin</td>
<td>ESXWIN7VM4</td>
<td>Install client software remotely</td>
<td></td>
</tr>
<tr>
<td>7/22/2016 4:37:13 PM</td>
<td>WIN-1LRCG038CCCP</td>
<td>Admin</td>
<td>10.10.1.64</td>
<td>Installation failed</td>
<td>The specified network password is not correct</td>
</tr>
<tr>
<td>7/25/2016 11:52:08 AM</td>
<td>WIN-1LRCG038CCCP</td>
<td>Admin</td>
<td>ESXWIN2K12R2VM</td>
<td>Uninstall client software remotely</td>
<td></td>
</tr>
<tr>
<td>7/19/2016 6:02:12 PM</td>
<td>WIN-1LRCG038CCCP</td>
<td>Admin</td>
<td>10.10.1.27</td>
<td>Detection failed</td>
<td>Failed to ping IP address</td>
</tr>
</tbody>
</table>

Figure 29
EventTracker: Integrating Malwarebytes

Logs Considered:

- **Malwarebytes-Threat detection**
  This report provides information related to threat detection about threat detected time, threat name, threat type, threat scanned path, action taken, outcome and service name on client machine.

---

**Figure 30**

---

**Figure 31**
Logs Considered:

![Log Example](image)

**Alerts**

- **Malwarebytes: Threat detected** - This alert is generated when a malicious virus has been detected on host.

**Import Malwarebytes Knowledge Pack into EventTracker**

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

   **NOTE**: Import the following KP items in the specified sequence.
   - Category
   - Alerts
   - Parsing Rules
   - Templates
   - Reports

### Category

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

2. Locate the **All Malwarebytes group of categories.iscat** file, and then click the **Open** button.

3. Click the **Import** button to import the categories.

   EventTracker displays success message.
4. Click the **OK** button and then click the **Close** button.

### Alerts

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

2. Locate the **All Malwarebytes group of alerts.isalt** file, and then click the **Open** button.

3. Click the **Import** button to import the alerts.

   EventTracker displays success message.

4. Click the **OK** button and then click the **Close** button.
Parsing Rules

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

2. Locate the **All Malwarebytes group of parsing rules.istoken** file, and then click the **Open** button.

3. To import tokens, click the **Import** button. EventTracker displays success message.

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

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on 'Import' option.

3. Browse the All Malwarebytes group of templates.ettd file, and then click the Open button.

4. To import tokens, click the Import button.
5. To import tokens, click the **Import** button.

EventTracker displays success message.

![Message from webpage](image)

Template(s) imported successfully

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

Reports

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

2. Locate All Malwarebytes group of reports.issch file, and then click the **Open** button.

3. Click the **Import** button to import the reports.

EventTracker displays success message.
4. Click the **OK** button, and then click the **Close** button.

**Verify Knowledge Pack in EventTracker Categories**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and select **Category**.
3. In the **Category Tree**, expand **Malwarebytes** group folder to see the imported categories.
Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Alerts.
3. In the Search field, enter ‘Malwarebytes’, and then click the Go button.
   Alert Management page will display all the imported Malwarebytes alerts.

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

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.
Template

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.

Parsing Rules

1. In the EventTracker Enterprise web interface, click the Admin menu, and then click Parsing Rules.
2. Select Malwarebytes.
Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then select Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click Malwarebytes group folder.

Reports are displayed in the Reports configuration pane.
Create Dashboards in EventTracker

Schedule Reports

**NOTE:** To configure the flex dashboards, schedule and then generate the reports. Flex dashboard feature is available from EventTracker Enterprise V8.0.

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **Malwarebytes** in report groups. Check **defined** option.

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in Eventvault explorer** box.

![REPORT WIZARD](image)

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait till the reports get generated.

**Create Dashlets**

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.
3. Navigate to Dashboard>Flex.
Flex Dashboard pane is shown.

4. Click to add a new dashboard.
Flex Dashboard configuration pane is shown.
5. Fill suitable title and description and click Save button.
6. Click to configure a new flex dashlet. Widget configuration pane is shown.

7. Locate earlier scheduled report in Data Source dropdown.
8. Select Chart Type from dropdown.
9. Select extent of data to be displayed in Duration dropdown.
10. Select computation type in Value Field Setting dropdown.
11. Select evaluation duration in As Of dropdown.
12. Select comparable values in X Axis with suitable label.
13. Select numeric values in Y Axis with suitable label.
14. Select comparable sequence in Legend.
15. Click Test button to evaluate. Evaluated chart is shown.
16. If satisfied, click **Configure** button.

17. Click ‘customize’ to locate and choose created dashlet.
EventTracker: Integrating Malwarebytes

**Figure 59**

The chart shows a comparison of policy management actions between computing and default policy settings. The x-axis represents the policy names, and the y-axis represents the count of actions. The policies are categorized by action types: Create, Deploy, Disable, Edit, Enable, Remove, and Switch client. The data range is from 07/26 12:46 to 08/02 12:46.
Sample Dashboards

1. Malwarebytes-Policy management
   - **Widget Title:** Policy management
   - **Data Source:** Malwarebytes-Policy management
   - **Chart Type:** Column
   - **Axis Label [X-axis]:** Policy Name
   - **Label Text:** Policy Name
   - **Legend Series:** Action

![Policy Management Chart](image)

*Figure 60*
2. **Malwarebytes-Threat detected**  
   **Widget Title:** Threat detected  
   **Data Source:** Malwarebytes-Threat detection  
   **Chart Type:** Donut  
   **Axis Label [X-axis]:** Threat Type  
   **Label Text:** Threat Type  
   **Legend Series:** Action Taken

![Figure 61](image-url)