Integrate VIPRE Business Antivirus

EventTracker v9.x and above

Publication Date: September 26, 2018
Abstract

This guide provides instructions to configure an VIPRE business antivirus to send its syslog to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v9.x or above and VIPRE business antivirus 9.3.

Audience

Administrators who are assigned the task to monitor VIPRE business antivirus events using EventTracker.
## Table of Contents

Abstract ............................................................................................................................................................. 1  
Scope ................................................................................................................................................................. 1  
Audience ............................................................................................................................................................ 1  
Overview ........................................................................................................................................................... 3  
Prerequisites .......................................................................................................................................................... 3  
Integrate VIPRE Business Anti-Virus to EventTracker ........................................................................................... 3  
Verify VIPRE Business Anti-Virus Integration in EventTracker .............................................................................. 6  
EventTracker Knowledge Pack ..................................................................................................................................... 9  
  Alerts ............................................................................................................................................................... 10  
  Categories ........................................................................................................................................................ 10  
  Flex Reports ..................................................................................................................................................... 10  
Import Vipre Business Anti-Virus knowledge pack into EventTracker ................................................................. 15  
  Alerts ............................................................................................................................................................... 16  
  Categories ........................................................................................................................................................ 17  
  Flex Reports ..................................................................................................................................................... 18  
Verify Vipre Business Anti-Virus knowledge pack in EventTracker ...................................................................... 20  
  Alerts ............................................................................................................................................................... 20  
  Categories ........................................................................................................................................................ 20  
  Flex Reports ..................................................................................................................................................... 21
Overview

VIPRE is a scalable Endpoint Solution that protects your networked machines from all types of malware and viruses and includes a firewall (Premium only). It’s Bad URL blocking feature under web filtering prevents end users from accidentally opening known bad websites (Premium only). VIPRE Business can be installed at more than one physical location and still be centrally managed. Its policy-based architecture allows administrators to create multiple policies based on user and machine types.

EventTracker collects and analyses events and enlightens an administrator about threat detection, changes happening in policy and protected system.

Prerequisites

- EventTracker Enterprise v8.x or above for configuring report, alert and flex dashboard should be installed.
- VIPRE business antivirus 9.3 should be installed.

Integrate VIPRE Business Anti-Virus to EventTracker

Following are the steps to integrate VIPRE antivirus and send the logs to EventTracker manager.

As, there is no direct way to send the logs of VIPRE antivirus to remote logging server, we must configure following script for setting it up in VIPRE Antivirus manager machine:

Get the Vipre AV integrator from EventTracker support.

1. Extract the Vipre integration pack.zip and run the Vipre Integrator.exe with Admin privilege.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>query</td>
<td>09/11/2018 11:39</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>sqlite</td>
<td>09/11/2018 11:39</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>vipre integrator.exe</td>
<td>09/11/2018 11:01</td>
<td>Application</td>
<td>62 KB</td>
</tr>
<tr>
<td>vpreinbuilt_report.exe</td>
<td>09/11/2018 11:36</td>
<td>Application</td>
<td>38 KB</td>
</tr>
<tr>
<td>vipgresql_report.exe</td>
<td>09/11/2018 11:28</td>
<td>Application</td>
<td>53 KB</td>
</tr>
</tbody>
</table>

Figure 1
2. A pop-up window will appear as shown below, select the **database type** which is configured on Vipre Anti-Virus.

![Figure 2](image)

3. If the option selected is **"Inbuilt SQLite Database"** then follow **Step 8**.
4. If the option selected is **"MSSQL Database"** then enter the **SQL Server Name** and **Database Name** in the respected fields as shown in the below image.

![Figure 3](image)
For Database Authentication,

5. Select the **SQL Authentication** option if the database has SQL user authentication.
6. Enter **SQL User name** and **Password** as shown in the below image.

![Image of SQL Authentication options](image)

7. If the database is configured with windows authentication, then select the **“Windows Authentication”**.
8. Click **OK** button to continue.
9. If the **“SQL authentication”** was selected in the previous option, then enter the local admin credentials to schedule task.
10. If the **“Windows Authentication”** was selected in the previous option enter the SQL database admin windows authentication credentials to configure the scheduled task.
11. Click **OK** button to continue.
12. If the configuration was successful it will display a message “**Configured successfully**”
13. Click **OK**.

**Verify VIPRE Business Anti-Virus Integration in EventTracker**

1. Go to **EventTracker Control Panel**.
2. Select the **EventTracker Agent configuration** option from the **EventTracker control panel**.
3. Select the **Logfile Monitor** tab.
4. Make sure the **checkbox** beside **Logfile Monitor** is checked.
5. Verify if the path added below is the correct one where the csv is present by clicking on **View File details**.
6. Click **save** to close the window.

7. Press the **Windows key + R** to open the Run box. Type **taskschd.msc** and press Enter, to open Task scheduler.
8. Verify the “Vipre_logger” task is created and enabled as shown below:

![Task Scheduler](image)

Figure 9

9. This completes VIPRE integration with EventTracker.

**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 Vipre Business Anti-Virus.
Alerts

- **VIPRE AV: Threat detection** - This alert is generated when any threat such as virus, malicious content, spyware etc. has been detected.
- **VIPRE AV: Policy management** - This alert is generated when any policy is created and updated in a system along with their hostname.

Categories

- **VIPRE AV-Policy management** - This category provides information related to policy management, i.e. when a policy is created and updated in that system along with their hostname.
- **VIPRE AV-Protected systems** - This category provides information related to protection of the system by the agents for the applied policy.
- **VIPRE AV-Quarantined details** - This category provides information related to quarantined details where a threat has been detected and categorized based on the threat level.
- **VIPRE AV-Scan details** - This category provides information related to scan details, i.e. when a system scans for the following: “Scanned Archives, Scanned Cookie, Scanned Files, Scanned Memory, Scanned Registry, Scanned Rootkit, Found Archives, Found Cookies, Found Files, Found Memory, Found Registry, Found Rootkit, Found Threats, Deleted, Ignored and Quarantined”.
- **VIPRE AV-Threat detection** - This category provides information about all the threats such as virus, malicious content, spyware etc. has been detected.

Flex Reports

- **VIPRE AV-Policy management** - This report provides information about policy management, i.e. when the policy is created and updated in a system along with their hostname.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>SiteName</th>
<th>Hostname</th>
<th>Policy Name</th>
<th>Created Date</th>
<th>Updated Date</th>
</tr>
</thead>
</table>

Figure 11
Sample Logs:

- VIPRE AV-Protected systems: This report provides information related to protection of the system by the agents for the applied policy.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>LogName</th>
<th>Agent Name</th>
<th>AgentIP</th>
<th>AgentOS</th>
<th>Mar-Address</th>
<th>Agent Port</th>
<th>PolicyName</th>
<th>AgentVersion</th>
<th>AgentVersionCheckAt</th>
<th>ThreatDefinitionVersion</th>
<th>ThreatDefinitionCheckAt</th>
</tr>
</thead>
</table>
Sample Logs:

VIPRE AV-Quarantined details: This report provides information about threat quarantined details where a threat has been detected and categorized based on the threat level.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Scan At</th>
<th>Hostname</th>
<th>Threat Name</th>
<th>Threat Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/19/2018 05:59:50 PM</td>
<td>09/22/2018 12:07:10 PM</td>
<td>Toons/PerkintS</td>
<td>VB: Trojan.Valnya.1946</td>
<td>Virus.generic</td>
</tr>
<tr>
<td>09/19/2018 05:59:51 PM</td>
<td>09/22/2018 12:06:38 AM</td>
<td>Toons/PerkintS</td>
<td>VB: Trojan.Valnya.1946</td>
<td>Virus.generic</td>
</tr>
<tr>
<td>09/19/2018 05:59:52 PM</td>
<td>09/22/2018 12:15:03 PM</td>
<td>Toons/PerkintS</td>
<td>W32.M.Ethan.CG</td>
<td>W32.M.Ethan.CG</td>
</tr>
<tr>
<td>09/19/2018 05:59:52 PM</td>
<td>09/22/2018 12:14:50 PM</td>
<td>Toons/PerkintS</td>
<td>W32.M.Ethan.CG</td>
<td>W32.M.Ethan.CG</td>
</tr>
</tbody>
</table>
Sample Logs:

- Sep 19 05:59:05 PM | ENTRY: RowNumber : 175 | scannet : 8/14/2018 1:49:43 PM | threatname : W97M.Ethan.CG | username : \BFLPLP\pedm1 | agentdomain : BFLPLP | agentnameorip :

  event_log_type | ++ Application
  event_type | ++ Information
  event_id | ++ 8220
  event_source | ++ EventTracker
  event_user_domain | ++ N/A
  event_computer | ++ VIPRE
  event_user_name | ++ N/A
  event_destination

ENTRY:

RowNumber : 175
scannet : 8/14/2018 1:49:43 PM
threatname : W97M.Ethan.CG
threatfamily : Virus-generic

FILEC:\Users\forderec\Desktop\knowledge\logs\Quarantined details.csv

Figure 16

- VIPRE AV-Scan details: This report provides information about group scan details, i.e. when a system scans for the following: “Scanned Archives, Scanned Cookie, Scanned Files, Scanned Memory, Scanned Registry, Scanned Rootkit, Found Archives, Found Cookies, Found Files, Found Memory, Found Registry, Found Rootkit, Found Threats, Deleted, Ignored and Quarantined”.

Figure 17
VIPRE AV-Threat detection: This report provides information about all the threats such as virus, malicious content, spyware etc. has been detected.
Sample Logs:

| 15 | Sep 19 05:59:05 PM | ENTRY: RowNumber: 175 | scanet: 8/14/2018 1:49:43 PM | threatname: \WSFM\Ethn\CG | user: \BFLP\flpadm1 | agentdomain: BFLP | agentnamecorp: DESKTOP-MIKE | policyname: Default | accloadev_em: Blocked | FILE:C:\Users\flpadm1\desktop\knowledge\logs\threatdetails.csv | TYPE:CVY | FIELD: * |

1. Launch the EventTracker Control Panel.

2. Double click Export-Import Utility.

---

**Import Vipre Business Anti-Virus knowledge pack into EventTracker**

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

- Alerts
- Categories
- Flex Reports
3. Click the **Import** tab.

### Alerts

1. Click **Alert** option, and then click the browse button.
1. Locate All Vipre AV alerts.isalt file, and then click the **Open** button.
2. To import alerts, click the **Import** button.

![Image](image.png)

Figure 23

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

**Categories**

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

![Image](image.png)

Figure 24
2. Locate All Vipre AV category.iscat file, and then click the Open button.

3. To import categories, click the Import button.

   EventTracker displays a success message.

   ![Selected category details are imported successfully.](image)

   Figure 25

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

**Flex Reports**

On the EventTracker Control Panel,

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

2. Locate the file named Vipre_Reports.etcnx and select all the checkbox.
3. Click the **Import** button to import the reports. EventTracker displays a success message.
Verify Vipre Business Anti-Virus knowledge pack in EventTracker

Alerts

1. In the EventTracker Enterprise web interface, click the Admin drop-down, and then click Alerts.
2. In the search box, enter Vipre Business Anti-Virus and then click the Search button.
3. EventTracker displays alert of Vipre Business Anti-Virus.

Categories

1. Login to EventTracker Enterprise.
2. Click the Admin drop-down, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand the Vipre Business Anti-Virus group folder to view the imported categories.
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports icon, and then select Report Configuration.

2. In Reports Configuration pane, select a Defined option.
3. Click on the Vipre Business Anti-Virus group folder to view the imported Vipre Business Anti-Virus reports.
Integrate VIPRE Business Antivirus

Figure 32