Integrate Microsoft IIS
EventTracker v9.0 and Above

Publication Date: June 21, 2019
Abstract

This guide provides instructions to configure Microsoft IIS to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor the web servers.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and Microsoft IIS.

Audience

IT admins, Microsoft IIS administrators and EventTracker users who wish to forward logs to EventTracker and monitor events using EventTracker.
# Table of Contents

Abstract .................................................................................................................................................. 1
Scope ...................................................................................................................................................... 1
Audience .................................................................................................................................................. 1
Overview .................................................................................................................................................. 3
Prerequisites ............................................................................................................................................. 3
Configuring Microsoft IIS ..................................................................................................................... 3
EventTracker Knowledge Pack (KP) ....................................................................................................... 4
  Reports .................................................................................................................................................. 4
  Dashboards .......................................................................................................................................... 6
Importing Knowledge Pack into EventTracker ..................................................................................... 10
  Knowledge Objects .......................................................................................................................... 11
  Token Template ............................................................................................................................... 12
  Flex Reports ...................................................................................................................................... 14
  Category ............................................................................................................................................. 17
  Dashlets .............................................................................................................................................. 18
Verifying Knowledge Pack in EventTracker .......................................................................................... 22
  Category ............................................................................................................................................. 22
  Knowledge Object ............................................................................................................................ 22
  Flex Reports ...................................................................................................................................... 23
  Dashlets .............................................................................................................................................. 24
  Token Template ............................................................................................................................... 24
Overview

IIS (Internet Information Services), is a web server created by Microsoft. The IIS is designed to deliver high speed and secure information publishing, while also serving as a platform for developers and independent software vendors to extend the Internet’s standard communication capabilities.

EventTracker supports traffic logs from Microsoft IIS. It gives you statistical reports of client requests, URI accessed, HTTP errors and HTTP method used. It also identifies the client browser and operating system used by the clients. From the security point of view, it detects suspicious URI requests run by the client and identifies attacks like SQL injection and cross-site scripting. One can pinpoint the performance bottlenecks by tracking the slow loading pages of the website. Pages visited by a user can be tracked using the user journey data.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **Microsoft IIS v8.5** or latest version should be installed.
- **IIS Logging** should be enabled.

Configuring Microsoft IIS

1. Start Internet Information Services (IIS) Manager.
2. Expand **ServerName**, and then expand **Sites** for Web Sites or FTP Sites.
3. Select the Web Site or FTP Site for which logging is required to be enabled.
4. Click to select the **Logging** option shown in the middle pane once selecting the site.

![Image of IIS Logging settings]

**Figure 2**

5. In the **Log File format** drop-down list, select W3C format.
6. In the **Select Fields** dialog box, select all the fields.
7. Enable the **ETW event only** under **Log Event Description**.
8. Click **Apply** under **Actions** pane at the top right.

### EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; reports and dashboards can be configured in EventTracker.

The following knowledge packs are available in EventTracker v9.x and later to support Microsoft IIS.

#### Reports

- **Microsoft IIS – Directory traversal** – This report provides information related to restricted directories.
- **Microsoft IIS – Backup finder** – This report provides information related to suspicious commands running by a client for data backup.
- **Microsoft IIS – Cross-site scripting** – This report provides information about suspicious cross-site scripting queries run by the client.
• **Microsoft IIS – Malicious SQL injection** - This report provides information about suspicious SQL queries run by the client which we can compare with the MSSQL-Extended error details report for investigating SQL injection.

• **Microsoft IIS – Web traffic details** - This report provides information of all HTTP request and responses send and received by IIS server.

• **Microsoft IIS – Site with errors** - This report provides count and error codes for requested URI’s.
Integrate Microsoft IIS

- **Microsoft IIS – Referral report** – This report provides information about the client accessed URI’s.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Client IP Address</th>
<th>Host</th>
<th>Service Name</th>
<th>URI</th>
<th>HTTP Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/23/2019 03:37:34 PM</td>
<td>::1</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td>/EventTracker/Content/css/tabularData.css</td>
<td>404</td>
</tr>
<tr>
<td>05/23/2019 03:38:19 PM</td>
<td>170.10.72.10</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td>/EventTracker/Content/css/tabularData.css</td>
<td>404</td>
</tr>
<tr>
<td>05/23/2019 03:40:21 PM</td>
<td>::1</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td>/EventTracker/Content/css/tabularData.css</td>
<td>404</td>
</tr>
<tr>
<td>05/23/2019 03:50:59 PM</td>
<td>26.10.43.29</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td>/EventTracker/Content/css/menu/MvSprite.png</td>
<td>404</td>
</tr>
<tr>
<td>05/23/2019 04:46:24 PM</td>
<td>::1</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td>/EventTracker/Content/css/menu/MvSprite.png</td>
<td>404</td>
</tr>
<tr>
<td>05/23/2019 04:46:24 PM</td>
<td>110.17.43.92</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td>/EventTracker/Content/css/menu/MvSprite.png</td>
<td>404</td>
</tr>
<tr>
<td>05/23/2019 04:47:11 PM</td>
<td>::1</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td>/EventTracker/Content/css/menu/MvSprite.png</td>
<td>404</td>
</tr>
</tbody>
</table>

- **Microsoft IIS – Traffic by Error Codes** – This dashboard shows information about the HTTPS error codes.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Client IP Address</th>
<th>Host</th>
<th>Service Name</th>
<th>URI Referer</th>
<th>HTTP Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/19/2019 05:33:06 PM</td>
<td>::1</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td><a href="http://localhost:8080/EventTracker/Analysis/EvtAnalysisWelcome.aspx?QType=134&amp;RptType=100&amp;Chap=&amp;Qid=CHZ4s8ChHsFwF9YgP/A==&amp;amp;gd=">http://localhost:8080/EventTracker/Analysis/EvtAnalysisWelcome.aspx?QType=134&amp;RptType=100&amp;Chap=&amp;Qid=CHZ4s8ChHsFwF9YgP/A==&amp;amp;gd=</a></td>
<td>404</td>
</tr>
<tr>
<td>06/19/2019 05:33:06 PM</td>
<td>::1</td>
<td>localhost:8080</td>
<td>W3SVCS</td>
<td><a href="http://localhost:8080/EventTracker/Analysis/EvtAnalysisWelcome.aspx?QType=134&amp;RptType=100&amp;Chap=&amp;Qid=CHZ4s8ChHsFwF9YgP/A==&amp;amp;gd=">http://localhost:8080/EventTracker/Analysis/EvtAnalysisWelcome.aspx?QType=134&amp;RptType=100&amp;Chap=&amp;Qid=CHZ4s8ChHsFwF9YgP/A==&amp;amp;gd=</a></td>
<td>404</td>
</tr>
</tbody>
</table>

Dashboards
• **Microsoft IIS – Traffic by Server** – This dashboard shows information about how many servers are accessed by the clients.

• **Microsoft IIS – Traffic by Client IP** – This dashboard shows information about the servers accessed by the client IP addresses.
- **Microsoft IIS – Traffic by Non Standard HTTP Methods** – This dashboard shows information about traffic by non-standard HTTP methods.

- **Microsoft IIS – Client Request Per Hour** – This dashboard shows information about how many requests are sent by the client per hour.
• **Microsoft IIS – Client Request Per URI** – This dashboard shows information about how many URI is accessed by the client.

• **Microsoft IIS – Response Time By URL** – This dashboard shows information about what is the URI’s accessed by the client and the response time from the server.
Importing Knowledge Pack into EventTracker

1. Launch the EventTracker Control Panel.
2. Double click Export/Import Utility, and then click the Import tab.
3. Import Tokens/Flex Reports as given below.

Knowledge Objects

1. Login to the EventTracker.
2. Click Knowledge objects under the Admin option in the EventTracker page.
3. Locate the file named KO.Microsoft IIS.etko.

4. Now select all the checkbox and then click on the ‘Import’ option.
5. Knowledge objects are now imported successfully. Click OK and click on the **Activate Now** button.

Token Template
1. Login to the **EventTracker**.
2. Click on **Admin >> Parsing Rules**.
3. Click on Template and click import configuration symbol.

4. Locate the Template_Microsoft IIS.ettd file and click on import.
5. Templates are imported now successfully.

![File imported successfully.](image)

**Flex Reports**

1. Click **Reports** option and select new (.etcrx) from the option.
2. Locate the file named *Flex_Reports_Microsoft IIS.etcrx* and select all the checkbox.
3. Click the **Import** button to import the reports. EventTracker displays a success message.
Category

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

![Figure 26](image)

2. Locate the **Category_Microsoft IIS.iscat** file, and then click the open button.

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

![Figure 27](image)

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

In EventTracker 9.0, we have added a new feature that will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker Web console.

2. Go to **My Dashboard** option.
3. Click on the **import** button and select `.etwd` File.
4. Click upload and select Dashboard which you want to import.
5. Click on the **Import** button. It will upload all selected dashboards.
Verifying Knowledge Pack in EventTracker

Category

1. Login to EventTracker.
2. Click the Admin menu, and then click Category.

3. Click the search, and then search with Microsoft IIS.

Knowledge Object

1. Login to EventTracker.
2. Click the Admin menu, and then click the Knowledge Object.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click the **Microsoft IIS** group folder.

Knowledge Object is displayed in the pane.

![Knowledge Object Group Tree](image)

**Figure 35**

### Flex Reports

1. Login to **EventTracker**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click the **Microsoft IIS** group folder.

5. Reports are displayed in the Reports configuration pane.

![Flex Reports](image)

**Figure 36**
Dashlets

1. Login to EventTracker.
2. Click the Dashboard menu, and then My Dashboard.
3. Then click on Customize Dashlet button and search for “Microsoft IIS”

![Figure 37](image)

Token Template

1. Login to the EventTracker.
2. Click on Admin >> Parsing Rules.

![Figure 38](image)
3. Click on **Template** and search for **Microsoft IIS**.

![Figure 39](image-url)