Splunk® Supported Add-ons
Splunk Add-on for Microsoft IIS released

Generated: 5/30/2022 9:17 pm

Table of Contents

Overview

Splunk Add-on for Microsoft IIS

Version	1.2.0
Vendor Products	Microsoft IIS 7.0, Microsoft IIS 7.5, Microsoft IIS 8.0, Microsoft IIS 8.5, Microsoft IIS 10.0
Visible	No. This add-on does not contain any views.

The Splunk Add-on for Microsoft IIS allows a Splunk software administrator to collect Web site activity data in the W3C log file format from Microsoft IIS servers. It can ingest W3C-compliant log files generated by standard logging as well as advanced logging in IIS.

This add-on provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.

Download the Splunk Add-on for Microsoft IIS from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release Notes for the Splunk Add-on for Microsoft IIS.

For information about installing and configuring the Splunk Add-on for Microsoft IIS, see Installation and configuration overview for the Splunk Add-on for Microsoft IIS.

Search the Splunk Community page for more information about this add-on.

Hardware and software requirements for the Splunk Add-on for Microsoft IIS

Splunk admin requirements

To install and configure the Splunk Add-on for Microsoft IIS, you must be member of the `admin` or `sc_admin` role.

Microsoft IIS setup requirements

You must enable IIS logging for the Web server from which you want to collect data and use the W3C log file format. Refer to the Microsoft IIS documentation for information about configuring logging in IIS. For more information, search for "Configure Logging in IIS" on the Microsoft documentation.

If you use the IIS Advanced Logging Module and you plan to use the the `ms:iis:auto` source type for automatic index-time field extraction, do not include the `EndRequest-UTC` and `BeginRequest-UTC` fields when you configure the logging fields in the IIS Advanced Logging module. These fields are not W3C-compliant. For more information about configuring fields using the Advanced Logging Module, search for "Advanced Logging for IIS - Custom Logging" in the Microsoft documentation.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements, see System Requirements in the Splunk Enterprise *Installation Manual*.
- For Splunk Light system requirements, see System Requirements in the Splunk Light *Installation Manual*.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

For information about installation locations and environments, see Install the Splunk Add-on for Microsoft IIS.

Installation and configuration overview for the Splunk Add-on for Microsoft IIS

Complete the following steps to install and configure this add-on.

1. Install the Splunk Add-on for Microsoft IIS.
2. Determine which source type you want to use. See Source types for the Splunk Add-on for Microsoft IIS.
3. Configure inputs for the Splunk Add-on for Microsoft IIS.
4. (Conditional) If you are using the `ms:iis:default` source type, Configure field transformations for the Splunk Add-on for Microsoft IIS.

Installation

Install the Splunk Add-on for Microsoft IIS

1. Get the Splunk Add-on for Microsoft IIS by downloading it from https://splunkbase.splunk.com/app/3185 or browsing to it using the app browser within Splunk Web.
2. Determine where and how to install this add-on in your deployment, using the tables on this page.
3. Perform any prerequisite steps before installing, if required and specified in the tables below.
4. Complete your installation.

If you need step-by-step instructions on how to install an add-on in your specific deployment environment, see the installation walkthroughs section at the bottom of this page for links to installation instructions specific to a single-instance deployment, distributed deployment, Splunk Cloud, or Splunk Light.

Distributed deployments

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in *Splunk Add-ons* for more information.

This table provides a reference for installing this specific add-on to a distributed deployment of the Splunk platform.

Splunk platform instance type	Supported	Required	Actions required / Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Microsoft IIS knowledge management is required.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to collect data. Required if you use universal forwarders to collect data.
Heavy Forwarders	Yes	See comments	This add-on supports forwarders of any type for data collection. The forwarder needs to be installed directly on the Microsoft IIS server for directory monitoring. As an alternative, the Microsoft IIS log files can be copied or shared to the machine where the forwarder is installed.
Universal Forwarders	Yes	See comments	

Distributed deployment feature compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Actions required / Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality, but configure inputs on forwarders to avoid duplicate data collection.

Distributed deployment feature	Supported	Actions required / Comments
Indexer Clusters	Yes	
Deployment Server	Yes	Supported for deploying the configured add-on to multiple nodes.

Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud
- Splunk Light

Configuration

Configure inputs in the Splunk Add-on for Microsoft IIS

Configure directory monitoring inputs on your data collection node for Microsoft IIS logs. Your forwarders must be installed directly on your Microsoft IIS servers or have the Microsoft IIS log files copied or shared to them from the Microsoft IIS servers. You can configure inputs directly on your forwarders or you can configure inputs on a deployment server and push them to your forwarders.

Configure inputs using Splunk Web

1. Log in to Splunk Web.
2. Click **Settings** > **Data inputs**.
3. Click **Files & directories**.
4. Click **New**.
5. In the **File or Directory** field, specify the path to the Microsoft IIS standard log directory (default: `%SystemDrive%\inetpub\logs\LogFiles`) or advanced log directory (default: `%SystemDrive%\inetpub\logs\AdvancedLogs`), then click **Next**.
6. In the **Sourcetype** field, enter the Microsoft IIS source type that matches the field extraction you plan to use.
    - ♦ `ms:iis:auto` enables automatic index-time field extraction. Supports Splunk recommended MS IIS fields if enabled.
    - ♦ `ms:iis:default` enables search-time field extraction.
    - ♦ `ms:iis:default:85` enables search-time field extraction. Preferable for MS IIS version 8.5 and greater.
    - ♦ `ms:iis:splunk` enables search-time field extraction for Splunk recommended fields MS IIS.
7. Click **Review** and review the information.
8. If all the information is correct, click **Submit**.

Next step
Configure the log format to allow extractions using the `ms:iis:default`, `ms:iis:default:85` or `ms:iis:splunk` sourcetype. See Configure field transformations for the Splunk Add-on for Microsoft IIS.

Configure inputs using the configuration files

1. Create `$SPLUNK_HOME/etc/apps/Splunk_TA_microsoft-iis/local/inputs.conf`.
2. Depending on the IIS source type and field extraction method you want to use, add one of the following stanzas, replacing the default IIS log directory path name with the actual value in your environment and the value for index where you want to collect data into.
   Index-time field extraction:

   ```
   [monitor://C:\inetpub\logs\LogFiles]
   disabled = false
   sourcetype = ms:iis:auto
   index = <preferred index>
   ```
   Search-time field extraction:

   ```
   [monitor://C:\inetpub\logs\LogFiles]
   disabled = false
   sourcetype = [ ms:iis:default | ms:iis:default:85 | ms:iis:splunk ]
   index = <preferred index>
   ```

3. Save the file.
4. Restart the Splunk platform for the new inputs to take effect.

Configure field transformations in the Splunk Add-on for Microsoft IIS

If you are usingÂ the `ms:iis:default`, or `ms:iis:default:85` or `ms:iis:splunk` source type to enable search-time field extraction, perform the following additional steps on your search heads.

> If you are using the ms:iis:auto source type, skip this procedure. The ms:iis:auto source type enables automatic index-time field extraction, so you do not need to configure these field transformations.

You can complete this configuration on Splunk Web or in the configuration files. If you are using this add-on with a search head cluster, perform these configuration steps on one search head node in Splunk Web. The cluster syncs the settings to your other nodes.

Configure field extractions in Splunk Web

1. Use a text editor to open an IIS W3C-standard log file from the directory you configured the Splunk platform to monitor.
2. In the log file, locate the field head line, which begins with `#Fields:`. For example: `#Fields: date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken https`.
3. Copy the field header line to your clipboard, omitting `"#Fields: "`
4. On your search head, click **Settings > Fields**.
5. Click **Field transformations**.
6. In the App drop-down, set the app context to **Splunk Add-on for Microsoft IIS (Splunk_TA_microsoft-iis)**
7. Click on the applicable field transformation and edit for the configured sourcetype:

Field Transformation	Source Type
auto_kv_for_iis_default	ms:iis:default
auto_kv_for_iis_default_85	ms:iis:default:85
auto_kv_for_iis_splunk	ms:iis:splunk

8. In the Fields list field, delete the text that appears and paste the contents of your clipboard.
9. Check to make sure the Fields list field exactly matches the field head line from your log file, with "#Fields:" omitted.
10. Click **Save**.

Configure field extractions using configuration files

1. Use a text editor to open a IIS W3C-standard log file from the directory you configured the Splunk platform to monitor.
2. In the log file, locate the field head line, which begins with `#Fields:` and copy it to your clipboard. For example:
```
#Fields: date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port
cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus
sc-win32-status sc-bytes cs-bytes time-taken https
```

3. Paste the head line from the clipboard at the $SPLUNK_HOME/etc/apps/Splunk_TA_microsoft-iis/local/transforms.conf in the following manner:

Sourcetype	Stanza name in transforms.conf	Example

ms:iis:default	auto_kv_for_iis_default	[auto_kv_for_iis_default]
		DELIMS = " "
		FIELDS = date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status https

ms:iis:default:85	auto_kv_for_iis_default_85	[auto_kv_for_iis_default_85]
		DELIMS = " "
		FIELDS = date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken https

ms:iis:splunk	auto_kv_for_iis_splunk	[auto_kv_for_iis_splunk]
		DELIMS = " "
		FIELDS = date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken X-Forwarded-For Content-Type https

4. Save `transforms.conf`.
5. Restart the search head for the configuration to take effect.

Configure recommended fields in the Splunk Add-on for Microsoft IIS

Splunk recommends you configure these fields for your business needs. There are different configuration instructions for different versions of Microsoft IIS.

For Microsoft IIS versions 8.5 and 10.0

1. Open IIS Manager.
2. On server, site or application level, double click on **Logging**.
3. Click **Select Fields**.
4. In **W3C Logging Fields** window, select all the fields listed under **Standard Fields**.
5. Next, click "**Add Field** under "**Custom Fields** box.

6. In the **Add Custom Field** window, fill out the following fields and click on **OK** after adding each fields in top-down order.

Field Name	Source type	Source
X-Forwarded-For	Request Header	X-Forwarded-For
Content-Type	Request Header	Content-Type
https	Server Variable	HTTPS

7. Click **OK** in the **W3C Logging Fields** window.
8. Click **Apply** in the actions pane.

For Microsoft IIS versions 7, 7.5 and 8.0

1. Open IIS Manager.
2. On server, site or application level, double click **Advanced Logging**.
3. In the action pane on right side, click **Enable Advanced Logging**.
4. In the action pane, click **Edit Logging Fields**.
5. In the new window, click **Add Field**.
6. In **Add Logging Field** window, fill out the following fields and click on **OK** after adding the below fields in top-down order:

Field Name	Source Type	Source
X-Forwarded-For	Request Header	X-Forwarded-For
Content-Type	Request Header	Content-Type
https	Server Variable	HTTPS

7. In the middle pane, select the default log definition `%COMPUTERNAME%-Server`. Click **Edit Log Definition**.
8. Click **Select Logging Fields**.
9. Select **X-Forwarded-For**, **Content-Type** and **https** from the list. Click **OK**.
10. Click **Apply** in the actions pane.

Troubleshooting

Troubleshoot the Splunk Add-on for Microsoft IIS

For troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*.
For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.

When should I use different source types?

- Use `ms:iis:default:85` if you have multiple MS IIS versions or versions 8.5 and greater. This enables you to differentiate the data of multiple MS IIS versions.
- Use `ms:iis:splunk` if you enable the Splunk recommended fields, as that will enrich your IIS log data's CIM mapping to Web data model which you can use to build your dashboards.

The "url" field has "http://" scheme even when the requests are made via HTTPS.

Enable the HTTPS Server variable and update the transform corresponding to the source type for this issue. Name this custom field as "https" ONLY. You'll receive the correct url that you input.

The "url" field mapped to Web data model isn't extracting.

Make sure the fields https, cs-host, s-ip, s-port, cs-uri-stem, cs-uri-query are enabled in MS IIS. If search-time extraction is used, its expected field extraction is mentioned in $SPLUNK_HOME/etc/apps/Splunk_TA_microsoft-iis/local/transforms.conf. If index-time extraction is used, make sure the log file is rolled over with the new headers.

I can't launch the add-on!

This add-on does not have views and is not intended to be visible in Splunk Web. If you are trying to launch or load views for this add-on and you are experiencing results you do not expect, turn off visibility for the add-on.

For more details about add-on visibility and instructions for turning visibility off, see Troubleshoot add-ons in *Splunk Add-ons*.

Reference

Lookups for the Splunk Add-on for Microsoft IIS

The Splunk Add-on for Microsoft IIS has one **lookup**. The lookup file maps fields from Microsoft IIS systems to CIM-compliant values in the Splunk platform. The lookup file is located in `$SPLUNK_HOME/etc/apps/Splunk_TA_microsoft-iis/lookups`.

Filename	Description
`iis_action_lookup.csv`	Maps Microsoft `iis_status` to `action`

Source types for the Splunk Add-on for Microsoft IIS

The Splunk Add-on for Microsoft IIS provides the index-time and search-time knowledge for Microsoft IIS Web site activity data in the following formats.

Determine which source type to use based on the field extraction method you plan to use. Use either search-time field extraction or index-time field extraction, but not both. Using both field extraction methods on the same data source will produce redundant indexed events.

Source type	Description	CIM data models
`ms:iis:splunk`	Microsoft IIS log files in W3C format. Use this source type to enable search-time field extraction. The field list contains Splunk recommended MS IIS fields to enrich CIM mapping.	Web
`ms:iis:default:85`	Microsoft IIS log files in W3C format. Use this source type to enable search-time field extraction. Recommended source type for IIS log files for MS IIS 8.5 and higher.	Web
`ms:iis:default`	Microsoft IIS log files in W3C format. Use this source type to enable search-time field extraction.	Web
`ms:iis:auto`	Microsoft IIS log files in W3C format. Use this source type to enable automatic index-time field extraction.	Web

Index-time field extraction relies on Splunk platform's built-in capability to recognize and process the W3C log format regardless of which fields are logged by IIS and in what order. It requires no additional configuration. Index-time field extraction requires more storage space than search-time field extraction.

Search-time field extraction requires additional configurations in `transforms.conf` to match your log format. For configuration instructions, see Configure field transformations for the Splunk Add-on for Microsoft IIS.

Release Notes

Release notes for the Splunk Add-on for Microsoft IIS

Version 1.2.0 of the Splunk Add-on for Microsoft IIS was released on October 1, 2020.

Compatibility

This release is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.2.x, 7.3.x, 8.0.x
CIM	4.17
Platforms	Platform-independent
Vendor Products	Microsoft IIS 7.0, Microsoft IIS 7.5, Microsoft IIS 8.0, Microsoft IIS 8.5, Microsoft IIS 10.0

> The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New Features

- Supports up to version 10 of Microsoft IIS
- Additional source types for Microsoft IIS W3C-standard log files

Fixed issues

Version 1.2.0 of the Splunk Add-on for Microsoft IIS has the following fixed issues:

Date resolved	Issue number	Description
2020-08-28	ADDON-20997, ADDON-21142	FIELDALIAS is incorrect for host field
2020-08-21	ADDON-28852	File descriptor lines ingested into Splunk when using ms:iis:default sourcetype

If no issues appear, no issues were currently fixed for this release.

Known issues

This version of the Splunk Add-on for Microsoft IIS contains the following known issues.

If no issues appear, no issues have yet been reported.

	Issue number	Description

Date filed		
2020-09-24	ADDON-29718, ADDON-29686	Invalid scheme in URL field for 'ms:iis:auto', 'ms:iis:default', 'ms:iis:default:85' sourcetypes Workaround: Steps to resolve issue for search-time sourcetypes (ms:iis:default, ms:iis:default:85): 1. Enable the HTTPS Server Variable with the field name as "https". (The steps followed for ms:iis:splunk sourcetype.) 2. Update the Field transformation of the respective sourcetype "auto_kv_for_iis_default" (for ms:iis:default) and "auto_kv_for_iis_default_85" (for ms:iis:default:85) with the updated "Field" string from IIS log files. 3. The url field will have the correct scheme for the URL. Steps to resolve issue for index-time sourcetype (ms:iis:auto): 1. Enable the HTTPS Server Variable with the field name as "https". (The steps followed for ms:iis:splunk sourcetype.) 2. Rollover the log file either from IIS manually or wait for IIS to rollover the logfile for writing the logs. 3. The url field will have the correct scheme for the url.

Third-party software attributions

Version 1.2.0 of the Splunk Add-on for Microsoft IIS does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Microsoft IIS

Latest release

The latest version of the Splunk Add-on for Microsoft IIS is version 1.2.0. See Release notes for the Splunk Add-on for Microsoft IIS for the release notes of this latest version.

Release notes for the Splunk Add-on for Microsoft IIS Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Microsoft IIS was released on June 8, 2016.

Compatibility

This release is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3.X and later
CIM	4.4 and later
Platforms	Platform-independent
Vendor Products	Microsoft IIS 7.0 and later

Features

Version 1.0.0 is the first release of the Splunk Add-on for Microsoft IIS, which provides inputs and CIM normalization for Microsoft IIS W3C-standard log files. This release ships with the following prebuilt panels that you can add to your dashboard:

- Microsoft IIS - Actions by Dest IP
- Microsoft IIS - Actions by Src IP
- Microsoft IIS - Actions by HTTP Method

Known issues

This version of the Splunk Add-on for Microsoft IIS contains the following known issues.

Date filed	Issue number	Description
2020-08-19	ADDON-28852	File descriptor lines ingested into Splunk when using ms:iis:default sourcetype
2019-01-17	ADDON-20997, ADDON-21142	FIELDALIAS is incorrect for host field Workaround: Added: [ms:iis:auto] FIELDALIAS-s_computername = host as s_computername
2016-05-20	ADDON-9580	EndRequest-UTC and BeginRequest-UTC make the fields after them fail to extract.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for Microsoft IIS does not incorporate any third-party software or libraries.