Splunk® Enterprise
Getting Data In 8.0.2

Set up and use HTTP Event Collector in Splunk Web

Generated: 3/31/2020 11:30 pm
Set up and use HTTP Event Collector in Splunk Web

The HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. HEC uses a token-based authentication model. You can generate a token and then configure a logging library or HTTP client with the token to send data to HEC in a specific format. This process eliminates the need for a Splunk forwarder when you send application events.

After you enable HEC, as a developer, you can use HEC tokens in your app to send data to HEC. You do not need to include Splunk credentials in your app or supported files.

**HEC functionality varies based on Splunk software type**

HTTP Event Collector runs on Splunk Enterprise, and self-service and managed Splunk Cloud. How it works depends on the type of Splunk instance you have.

**HEC and Splunk Enterprise**

HEC offers full configurability and functionality on the Splunk Enterprise platform on-premises. It offers the following additional benefits on Splunk Enterprise over the other Splunk types:

- HEC can accept events that you send to it over the HTTP protocol in addition to the HTTPS protocol.
- HEC can forward events to another Splunk indexer with an optional forwarding **output group**.
- You can use the deployment server to distribute HEC tokens across indexers in a distributed deployment.

For instructions on how to enable and manage HEC on Splunk Enterprise, see [Configure HTTP Event Collector on Splunk Enterprise](#).

**HEC and self-service Splunk Cloud**

HEC offers similar functionality on self-service Splunk Cloud instances as it does on Splunk Enterprise. The following exceptions apply:

- You cannot make changes to configuration files, because Splunk Cloud does not provide that access.
- You cannot change the network port that HEC listens on for connections.
- You cannot forward data that HEC receives to another set of Splunk indexers as Splunk Cloud does not support forwarding output groups.

For instructions on how to enable and manage HEC on self-service Splunk Cloud, see [Configure HTTP Event Collector on self-service Splunk Cloud](#).

**HEC and managed Splunk Cloud**

HEC offers an experience on Splunk Cloud deployments that Splunk manages that is similar to the experience on self-service Splunk Cloud. The following exceptions apply:

- You cannot make changes to configuration files, because Splunk Cloud does not provide that access.
- You must file a ticket with Splunk Support to enable HEC for use with Kinesis Firehose. Standard HEC is enabled by default on all Splunk Cloud stacks and does not require a Splunk Support ticket.
- You cannot make changes to global settings. You can only make settings changes to tokens that you create.
• You cannot forward data that HEC receives to another set of Splunk indexers as Splunk Cloud does not support forwarding output groups.
• The index that you choose to store events that HEC receives must already exist. You cannot create a new index during the setup process.
• Indexer acknowledgment is only available for Amazon Kinesis Firehose at this time.
• After you create tokens, you can monitor progress of the token as it is deployed across your managed Splunk Cloud instance.

For instructions on how to enable and manage HEC on managed Splunk Cloud, see Configure HTTP Event Collector on managed Splunk Cloud.

About Event Collector tokens

Tokens are entities that let logging agents and HTTP clients connect to the HEC input. Each token has a unique value, which is a 128-bit number that is represented as a 32-character globally unique identifier (GUID). Agents and clients use a token to authenticate their connections to HEC. When the clients connect, they present this token value. If HEC receives a valid token, it accepts the connection and the client can deliver its payload of application events in either text or JavaScript Object Notation (JSON) format.

HEC receives the events and Splunk Enterprise indexes them based on the configuration of the token. HEC uses the source, source type, and index that was specified in the token. If a forwarding output group configuration exists on a Splunk Enterprise instance, HEC forwards the data to indexers in that output group.

Use output groups to specify groups of indexers

To index large amounts of data, you will likely need multiple indexers. You can specify groups of indexers to handle indexing your HTTP Event Collector data. These are called output groups. You can use output groups to, for example, index only certain kinds of data or data from certain sources. Though using output groups to route data to specific indexers is similar to the routing and filtering capabilities built into Splunk Enterprise, output groups allow you to specify groups of indexers on a token-by-token basis. When you configure output groups with multiple indexers, Splunk Enterprise evenly distributes data among the servers in your output group. You configure output groups in the outputs.conf file. Specifically, for HTTP Event Collector, edit the outputs.conf file at $SPLUNK_HOME/etc/apps/splunk_httpinput/local/ (%SPLUNK_HOME%\etc\apps\splunk_httpinput\local\ on Microsoft Windows hosts). If either the local directory or the outputs.conf file doesn't exist at this location, create it (or both).

HTTP Event Collector is not an app, but it stores its configuration in the $SPLUNK_HOME/etc/apps/splunk_httpinput/ directory (%SPLUNK_HOME%\etc\apps\splunk_httpinput\ on Windows) so that its configuration can be easily deployed using built-in app deployment capabilities.

Configure HTTP Event Collector on Splunk Enterprise

Enable HTTP Event Collector

Before you can use Event Collector to receive events through HTTP, you must enable it. For Splunk Enterprise, enable HEC through the Global Settings dialog box.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
Create an Event Collector token

To use HEC, you must configure at least one token.

1. Click Settings > Add Data.
2. Click monitor.
3. Click HTTP Event Collector.
4. In the Name field, enter a name for the token.
5. (Optional) In the Source name override field, enter a source name for events that this input generates.
6. (Optional) In the Description field, enter a description for the input.
7. (Optional) In the Output Group field, select an existing forwarder output group.
8. (Optional) If you want to enable indexer acknowledgment for this token, click the Enable indexer acknowledgment checkbox.
9. Click Next.
10. (Optional) Confirm the source type and the index for HEC events.
11. Click Review.
12. Confirm that all settings for the endpoint are what you want.
13. If all settings are what you want, click Submit. Otherwise, click < to make changes.
14. (Optional) Copy the token value that Splunk Web displays and paste it into another document for reference later.
For information about HEC tokens, see About Event Collector tokens.

For information about defining forwarding output groups, see Configure forwarders with outputs.conf. You can also set up forwarding in Splunk Web, which generates a default output group called `default-autolb-group`.

For information on indexer acknowledgment, see HTTP Event Collector indexer acknowledgment. Indexer acknowledgment in HTTP Event Collector is not the same indexer acknowledgment capability described in indexer acknowledgment and indexer clusters.

**Modify an Event Collector token**
You can make changes to an HEC token after you have created it.

1. Click **Settings > Data Inputs**.
2. Click **HTTP Event Collector**.
3. Locate the token that you want to change in the list.
4. In the **Actions** column for that token, click **Edit**. You can also click the link to the token name.
5. (Optional) Edit the description of the token by entering updated text in the **Description** field.
6. (Optional) Update the source value of the token by entering text in the **Source** field.
7. (Optional) Choose a different source type by selecting it in the **Source Type** drop-down.
   1. Choose a category.
   2. Select a source type in the pop-up menu that appears.
   3. (Optional) You can also type in the name of the source type in the text box at the top of the drop-down.
8. (Optional) Choose a different index by selecting it in the Available Indexes pane of the Select Allowed Indexes control.
9. (Optional) Choose a different output group from the Output Group drop-down.
10. (Optional) Choose whether you want indexer acknowledgment enabled for the token.
11. Click Save.

**Delete an Event Collector token**

You can delete an HEC token. Deleting an HEC token does not affect other HEC tokens, nor does it disable HEC.

You cannot undo this action. Clients that use this token to send data to your Splunk deployment can no longer authenticate with the token. You must generate a new token and change the client configuration to use the new token.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. Locate the token that you want to delete in the list.
4. In the Actions column for that token, click Delete.
5. In the Delete Token dialog box, click Delete.

**Enable and disable Event Collector tokens**

You can enable or disable a single HEC token from within the HEC management page. Changing the status of one token does not change the status of other tokens. To enable or disable all tokens, use the Global Settings dialog. See Enable the HTTP Event Collector.

To toggle the active status of an HEC token:

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. In the Actions column for that token, click the Enable link, if the token is not active, or the Disable link, if the token is active. The token status toggles immediately and the link changes to Enable or Disable based on the changed token status.

**Configure HTTP Event Collector on self-service Splunk Cloud**

**Enable HTTP Event Collector**

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. Click Global Settings.
4. In the **All Tokens** toggle button, select **Enabled**.
5. (Optional) Choose a **Default Source Type** for all HEC tokens. You can also type in the name of the source type in the text field above the drop-down before choosing the source type.
6. (Optional) Choose a **Default Index** for all HEC tokens.
7. Click **Save**.

**Create an Event Collector token**

To use HEC, you must configure at least one token.

1. Click **Settings > Add Data**.
2. Click **monitor**.
3. Click **HTTP Event Collector**.
4. In the **Name** field, enter a name for the token.
5. (Optional) In the **Source name override** field, enter a name for a source to be assigned to events that this endpoint generates.
6. (Optional) In the **Description** field, enter a description for the input.
7. (Optional) If you want to enable indexer acknowledgment for this token, click the **Enable indexer acknowledgment** checkbox.
8. Click **Next**.
9. (Optional) Make edits to source type and confirm the index where you want HEC events to be stored. See Modify input settings.
10. Click **Review**.
11. Confirm that all settings for the endpoint are what you want.
12. If all settings are what you want, click **Submit**. Otherwise, click < to make changes.
13. (Optional) Copy the token value that Splunk Web displays and paste it into another document for reference later.

For information about HEC tokens, see About Event Collector tokens.

For information on indexer acknowledgement, see HTTP Event Collector indexer acknowledgement. Indexer acknowledgement in HTTP Event Collector is not the same indexer acknowledgement capability described in indexer acknowledgement and indexer clusters.
Modify an Event Collector token

You can make changes to an HEC token after you have created it.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. Locate the token that you want to change in the list.
4. In the Actions column for that token, click Edit. You can also click the link to the token name.
5. (Optional) Edit the description of the token by entering updated text in the Description field.
6. (Optional) Update the source value of the token by entering text in the Source field.
7. (Optional) Choose a different source type by selecting it in the Source Type drop-down.
   1. Choose a category.
   2. Select a source type in the pop-up menu that appears.
   3. (Optional) You can also type in the name of the source type in the text box at the top of the drop-down.
8. (Optional) Choose a different index by selecting it in the Available Indexes pane of the Select Allowed Indexes control.
9. (Optional) Choose whether you want indexer acknowledgment enabled for the token.
10. Click Save.

Delete an Event Collector token

You can delete an HEC token. Deleting an HEC token does not affect other HEC tokens, nor does it disable the HEC endpoint.

You cannot undo this action. Clients that use this token to send data to your Splunk deployment can no longer authenticate with the token. You must generate a new token and change the client configuration to use the token.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. Locate the token that you want to delete in the list.
4. In the Actions column for that token, click Delete.
5. In the Delete Token dialog, click Delete.

Enable and disable Event Collector tokens

You can enable or disable an HEC token from within the HEC management page. Changing the status of one token does not change the status of other tokens. To enable or disable all tokens, use the Global Settings dialog. See Enable the HTTP Event Collector.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. In the Actions column for that token, click the Enable link, if the token is not active, or the Disable link, if the token is active. The token status toggles and the link changes to Enable or Disable based on the changed token.
status.

Configure HTTP Event Collector on managed Splunk Cloud

Enable HTTP Event Collector

Call Splunk Support and open a ticket to enable HEC.

Create an Event Collector token

To use HEC, you must configure at least one token. In managed Splunk Cloud instances, the token is distributed across the deployment. The token is not ready for use until distribution has completed.

1. Click **Settings > Add Data**.
2. Click **monitor**.
3. Click **HTTP Event Collector**.
4. In the **Name** field, enter a name for the token.
5. (Optional) In the **Source name override** field, enter a name for a source to be assigned to events that this endpoint generates.
6. (Optional) In the **Description** field, enter a description for the input.
7. Click **Next**.
8. (Optional) Make edits to source type and confirm the index where you want HEC events to be stored. See **Modify input settings**.
9. Click **Review**.
10. Confirm that all settings for the endpoint are what you want.
11. If all settings are what you want, click **Submit**. Otherwise, click < to make changes.
12. (Optional) Copy the token value that Splunk Web displays and paste it into another document for reference later.
13. (Optional) Click **Track deployment progress** to see progress on how the token has been deployed to the rest of the Splunk Cloud deployment. When you see a status of "Done", you can then use the token to send data to HEC.

For information about HEC tokens, see **About Event Collector tokens**.

For information on indexer acknowledgement, see **Enable indexer acknowledgement**. Indexer acknowledgement in HTTP Event Collector is not the same indexer acknowledgement capability in Splunk Enterprise.

Check Event Collector token distribution status

![Last Deployment Status](image)
You can check the distribution status of an HEC token from the HEC token page. When a distribution is in progress, the page displays "Operation in progress" and a progress bar. Otherwise, the page displays "Last deployment status."

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. Click Operation in progress or Last deployment status.
4. View the status of the token distribution.
5. Click Close.

Modify an Event Collector token

You can make changes to an HEC token after it has been created.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. Locate the token that you want to change in the list.
4. In the Actions column for that token, click Edit. You can also click the link to the token name.
5. (Optional) Edit the description of the token by entering updated text in the Description field.
6. (Optional) Update the source value of the token by entering text in the Source field.
7. (Optional) Choose a different source type by selecting it in the Source Type drop-down.
   1. Choose a category.
   2. Select a source type in the pop-up menu that appears.
   3. (Optional) You can also type in the name of the source type in the text box at the top of the drop-down.
8. (Optional) Choose a different index by selecting it in the Available Indexes pane of the Select Allowed Indexes control.
9. (Optional) Choose whether you want indexer acknowledgment enabled for the token.
10. Click Save.

Delete an Event Collector token

You can delete an HEC token. Deleting an HEC token does not affect other HEC tokens, nor does it disable the HEC endpoint.

You cannot undo this action. Clients that use this token to send data to your Splunk deployment can no longer authenticate with the token. You must generate a new token and change the client configuration to use the new value.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. Locate the token that you want to delete in the list.
4. In the Actions column for that token, click Delete.
5. In the Delete Token dialog, click Delete.

Enable and disable Event Collector tokens

You can enable or disable a token from within the HEC management page. Changing the active status of one token does not change the status of other tokens.

1. Click Settings > Data Inputs.
2. Click HTTP Event Collector.
3. In the Actions column for a token, click the Enable link, if the token is not active, or the Disable link, if the token is active. The token status toggles and the link changes to Enable or Disable based on the changed token status.
Send data to HTTP Event Collector

You must satisfy all of the following conditions when you send data to HEC:

- HEC must be enabled
- You must have at least one active HEC token available
- You must use an active token to authenticate into HEC
- You must format the data that goes to HEC in a certain way. See Format events for HTTP Event Collector

There are several options for sending data to HTTP Event Collector:

- You can make an HTTP request using your favorite HTTP client and send your JSON-encoded events.
- As a developer, you can use the Java, JavaScript (node.js), and .NET logging libraries in your application to send data to HEC. These libraries are compatible with popular logging frameworks. See Java, JavaScript (Node.js), and .NET on the Splunk Dev Portal.

Send data to HTTP Event Collector on Splunk Enterprise

You send data to a specific Uniform Resource Indicator (URI) for HEC.

The standard form for the HEC URI in Splunk Enterprise is as follows:

<protocol>://<host>:<port>/<endpoint>

Where:

- <protocol> is either http or https
- <host> is the Splunk instance that runs HEC
- <port> is the HEC port number, which is 8088 by default, but you can change in the HEC Global Settings
- <endpoint> is the HEC endpoint you want to use. In many cases, you use the /services/collector endpoint for JavaScript Object Notation (JSON)-formatted events or the services/collector/raw endpoint for raw events

Send data to HTTP Event Collector on Splunk Cloud instances

Depending on the type of Splunk Cloud that you use, you must send data using a specific URI for HEC.

The standard form for the HEC URI in self-service Splunk Cloud is as follows:

<protocol>://input-<host>:<port>/<endpoint>

The standard form for the HEC URI in managed Splunk Cloud is as follows:

<protocol>://http-inputs-<host>:<port>/<endpoint>

Where:

- <protocol> is https
- <host> is the Splunk instance that runs HEC
- <port> is the HEC port number
  - 8088 on self-service Splunk Cloud instances
  - 443 on managed Splunk Cloud instances
- <endpoint> is the HEC endpoint you want to use. In many cases, you use the /services/collector endpoint for
JavaScript Object Notation (JSON)-formatted events or the `services/collector/raw` endpoint for raw events

- For self-service Splunk Cloud plans, you must pre-pend the hostname with `input-`
- For managed Splunk Cloud plans, pre-pend the hostname with `http-inputs-`

If you do not include these prefixes before your Splunk Cloud hostname when you send data, the data cannot reach HEC.

**Example of sending data to HEC with an HTTP request**

The following example makes a HTTP POST request to the HEC on the respective port for the deployment and uses HTTPS for transport. This example uses the `curl` command to generate the request, but you can use a command line or other tool that better suits your needs.

You can configure the network port and HTTP protocol settings independently of settings for other instances of HEC in your Splunk Enterprise, managed Splunk Cloud, or self-service Splunk Cloud deployment.

Before running this command in a test environment, disable indexer acknowledgement on the token. This option may have been set when you modified an Event Collector token. When this option is set for the token, the cURL command fails with the following error: 

```
"text": "Data channel is missing","code":10"
```

After you have successfully tested the command, be sure to re-enable indexer acknowledgement for the token.

The following cURL command uses an example HTTP Event Collector token and uses *hec* as the hostname. Replace these values with your own before running this command.

**JSON request and response**

When you make a JSON request to send data to HEC, you must specify the "event" key in the command.

**Managed Splunk Cloud**

```
```

```
{"text": "Success", "code": 0}
```

**Splunk Enterprise and Self-service Splunk Cloud**

```
```

```
{"text": "Success", "code": 0}
```

**More information on HEC for developers**

For developer content on using HTTP Event Collector, see HTTP Event Collector Examples, as well as Introduction to Splunk HTTP Event Collector in the Splunk Developer Portal.