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, 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 to access the Splunk platform instance.

HEC functionality varies based on Splunk software type

HTTP Event Collector runs on Splunk Cloud Platform and Splunk Enterprise. How it works depends on the type of Splunk platform instance you have.

HEC and Splunk Cloud Platform

You can enable HEC on a Splunk Cloud Platform deployment. The following caveats apply to using HEC on a Splunk Cloud Platform instance:

- If you need to use a configuration file to configure an HEC input, you must do this on a heavy forwarder, then forward the data to Splunk Cloud Platform. This is because Splunk Cloud Platform does not provide access to configuration files locally.
- You must file a ticket with Splunk Support to enable HEC for use with Amazon Web Services (AWS) Kinesis Firehose. Standard HEC is enabled by default on all Splunk Cloud Platform deployments 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 Platform 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 AWS Kinesis Firehose at this time.
- After you create tokens, you can monitor progress of the token as it is deployed across your Splunk Cloud Platform instance.

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

HEC and Splunk Enterprise

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

- 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.

How the Splunk platform uses HTTP Event Collector tokens to get data in

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). Each character can be a number from 0-9 or a letter from a-f, and the token is case insensitive. For example, the following is a valid HEC token: `B5A79AAD-D822-46CC-80D1-819F80D7BFB0`.

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.

Configure HTTP Event Collector on Splunk Cloud Platform

HEC is enabled by default in Splunk Cloud Platform. You can create, modify, delete, enable, and disable HEC tokens.

Enable HTTP Event Collector on Splunk Cloud Platform

HTTP Event Collector is enabled by default on Splunk Cloud Platform.

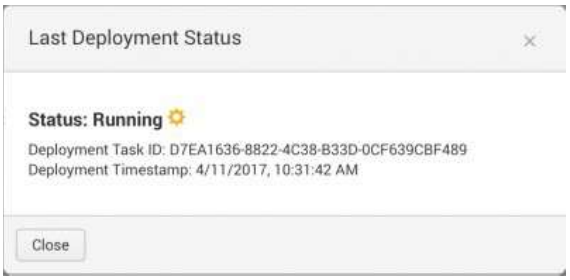
Create an Event Collector token on Splunk Cloud Platform

To use HEC, you must configure at least one token. Splunk Cloud Platform distributes the token 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. (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.
14. (Optional) Click **Track deployment progress** to see progress on how the token has been deployed to the rest of the Splunk Cloud Platform deployment. When you see a status of "Done", you can then use the token to send data to HEC.

Check Event Collector token distribution status on Splunk Cloud Platform

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 on Splunk Cloud Platform

You can make changes to an HEC token after you create 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 list box.
    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 list box.
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 on Splunk Cloud Platform

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 in Splunk Cloud Platform

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.

Configure HTTP Event Collector on Splunk Enterprise

You can enable HEC and create, modify, delete, enable, and disable HEC tokens in Splunk Enterprise.

Enable HTTP Event Collector on Splunk Enterprise

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**.
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 list box before choosing the source type.
6. (Optional) Choose a **Default Index** for all HEC tokens.
7. (Optional) Choose a **Default Output Group** for all HEC tokens.
8. (Optional) To use a deployment server to handle configurations for HEC tokens, click the **Use Deployment Server** check box.
9. (Optional) To have HEC listen and communicate over HTTPS rather than HTTP, click the **Enable SSL** checkbox.
10. (Optional) Enter a number in the **HTTP Port Number** field for HEC to listen on.

    Confirm that no firewall blocks the port number that you specified in the '"HTTP Port Number"' field, either on the clients or the Splunk instance that hosts HEC.
11. Click **Save**.

Create an Event Collector token on Splunk Enterprise

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.

Modify an Event Collector token on Splunk Enterprise

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 list box.
    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 list box.
10. (Optional) Choose whether you want indexer acknowledgment enabled for the token.
11. Click **Save**.

Delete an Event Collector token on Splunk Enterprise

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 on Splunk Enterprise

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.

Use output groups to specify groups of indexers on Splunk Enterprise

To index large amounts of data, you will likely need multiple indexers. On Splunk Enterprise only, you can specify groups of indexers to handle indexing your HTTP Event Collector data. These groups are called *output groups*. You can use output groups to, for example, index only certain kinds of data, or data from certain sources.

You configure output groups in the `outputs.conf` configuration 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.

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 Cloud Platform

You must send data using a specific URI for HEC.

The standard form for the HEC URI in Splunk Cloud Platform free trials is as follows:

```
<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>
```

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

```
<protocol>://http-inputs-<host>.splunkcloud.com:<port>/<endpoint>
```

The standard form for the HEC URI in Splunk Cloud Platform on Google Cloud is as follows:

`<protocol>://http-inputs.<host>.splunkcloud.com:<port>/<endpoint>`
The standard form for the HEC URI in Splunk Cloud Fedramp Moderate on AWS Govcloud is as follows:

`<protocol>://http-inputs.<host>.splunkcloudgc.com:<port>/<endpoint>`

Where:

- <protocol> is either `http` or `https`
- You must add `http-inputs-` before the <host> on AWS.
- You must add `http-inputs.` before the <host> on GCP and AWS Govcloud.
- <host> is the Splunk Cloud Platform instance that runs HEC
- You must add the domain .splunkcloud.com after the <host>
- <port> is the HEC port number
    - 8088 on Splunk Cloud Platform free trials
    - 443 by default on Splunk Cloud Platform instances
- <endpoint> is the HEC endpoint you want to use. In many cases, you use the `/services/collector/event` endpoint for JavaScript Object Notation (JSON)-formatted events or the `services/collector/raw` endpoint for raw events

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

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/event` endpoint for JavaScript Object Notation (JSON)-formatted events or the `services/collector/raw` endpoint for raw events

Example of sending data to HEC with an HTTP request

The following example makes a HTTP POST request to the HEC on port 8088 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 or Splunk Cloud Platform deployment.

The following cURL command uses an example HTTP Event Collector token (`B5A79AAD-D822-46CC-80D1-819F80D7BFB0`), and uses `https://hec.example.com` 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.

The Authorization HTTP header for HEC requires the "Splunk" keyword before the HEC token.

```
curl https://hec.example.com:8088/services/collector/event -H "Authorization: Splunk
B5A79AAD-D822-46CC-80D1-819F80D7BFB0" -d '{"event": "hello world"}'
{"text": "Success", "code": 0}
```

More information on HEC

- 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 acknowledgement, 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.
- For information about using HEC in Splunk Enterprise, see Set up and use HTTP Event Collector in Splunk Web in the Splunk Enterprise *Getting Data In* manual.
- For information about using HEC in Splunk Cloud Platform, see Set up and use HTTP Event Collector in Splunk Web in the Splunk Cloud Platform *Getting Data In* manual.
- For information about using HEC in the Edge Processor service, see Get data into an Edge Processor using HTTP Event Collector in the Splunk Cloud Platform *Use Edge Processors* manual.

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.