Splunk <> EasyDMARC Integration Setup Guide

To connect EasyDMARC with Splunk, you need to create an HTTP Event Collector (HEC) endpoint in your Splunk instance and generate an access token. This will allow EasyDMARC to securely push alerts and audit logs directly to your Splunk environment.

Prerequisites:

- Administrative access to your Splunk Enterprise or Splunk Cloud instance.
- Knowledge of the index you want to send EasyDMARC data to.

1. **Navigate to HTTP Event Collector :**
    - Log in to your Splunk Web UI.
    - Navigate to **Settings > Data Inputs**.
    - Under **Local inputs**, select **HTTP Event Collector**.
2. **Enable HEC:**
    - In the Data Inputs settings page, click on **HTTP Event Collect** and then Global Settings in the top right corner.Ensure that **All Tokens** is set to **Enabled**.

- Optionally, specify a **Default Source Type** as Structured → **_json** and a **Default Index**.
- Click **Save**.

3. **Create a New HEC Token:**
   - Return to the HTTP Event Collector page.
   - Click the **New Token** button in the top-right corner.
   - On the **Select Source** step:
     - Enter a **Name** for the token (e.g., `EasyDMARC_Integration`).
     - Optionally, enter a **Source name override**.
     - Click **Next**.
4. **Configure Input Settings:**
   - On the **Input Settings** step select Automatic
   - In the **Index** section, select the index where you want to store EasyDMARC data. It is recommended to have a dedicated index for this purpose.
   - Click **Review**.
5. **Review and Submit:**
   - Review your selections.
   - Click **Submit**.
6. **Copy Your Token:**
   - Splunk will display the **Token Value**. This is the HEC token. **Copy this value immediately**, as you will not be able to see it again.

- You will also need your Splunk instance's HEC URI. This is your Splunk hostname or IP followed by port 8088 (e.g., `https://your-splunk-instance.com:8088`).

Information to Copy to EasyDMARC:

- **HEC URI:** The full URL of your Splunk HEC endpoint, which is as follows
  - **Splunk Cloud Example:** https.://http-inputs.your_stack.splunkcloud.com:443/services/collector
  - **Splunk Enterprise Example:** https.://your-splunk-host.com:8088/services/collector
- **HEC Token:** The token value you just created.