Export search results

You can export search results from your Splunk deployment, and forward data to third-party systems, as described in this topic.

What are the available export methods?

The Splunk platform provides several export methods:

- Export data using Splunk Web
- Export data using the CLI
- Export data using SDKs
- Export data using REST API
- The `dump` search command
- Data forwarding

Splunk apps

- Deploy and Use Splunk App for CEF
- Deploy and Use Splunk DB Connect
- Hadoop Connect
- Install and Use Splunk ODBC Driver with Microsoft Excel
- Install and Use Splunk ODBC Driver with MicroStrategy
- Install and Use Splunk ODBC Driver with Tableau

Export options

The export method you choose depends on the data volumes involved and your level of interactivity. For example, a single on-demand search export through Splunk Web might be appropriate for a low-volume export. Alternatively, if you want to set up a higher-volume, scheduled export, the SDK and REST options work best.

For large exports, the most stable method of search data retrieval is the Command Line Interface (CLI). From the CLI, you can tailor your search to external applications using the various Splunk SDKs. The REST API works from the CLI as well, but is recommended only for internal use.

In terms of level of expertise, the Splunk Web and CLI methods are significantly more accessible than the SDKs and REST API, which require previous experience working with software development kits or REST API endpoints.
<table>
<thead>
<tr>
<th>Method</th>
<th>Volume</th>
<th>Interactivity</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Web</td>
<td>Low</td>
<td>On-Demand, Interactive</td>
<td>Easy to obtain on-demand exports</td>
</tr>
<tr>
<td>CLI</td>
<td>Medium</td>
<td>On-Demand, Low Interactive</td>
<td>Easy to obtain on-demand exports</td>
</tr>
<tr>
<td>REST</td>
<td>High</td>
<td>Automated, best for computer-to-computer</td>
<td>Works underneath SDK</td>
</tr>
<tr>
<td>SDK</td>
<td>High</td>
<td>Automated, best for computer-to-computer</td>
<td>Best for automation</td>
</tr>
</tbody>
</table>

**Supported export formats**

You can export Splunk data into the following formats:

- Raw Events (for search results that are raw events and not calculated fields)
- CSV
- JSON
- XML
- PDF (for saved searches, using Splunk Web)