**Define a CSV lookup in Splunk Web**

CSV [**lookups**](https://docs.splunk.com/Splexicon:Lookup) are file-based lookups that match field values from your events to field values in the static table represented by a CSV file. They output corresponding field values from the table to your events. They are also referred to as *static lookups*.

CSV lookups are best for small sets of data. The general workflow for creating a CSV lookup in Splunk Web is to upload a file, share the lookup table file, and then create the lookup definition from the lookup table file. CSV inline lookup table files, and inline lookup definitions that use CSV files, are both dataset types. See [Dataset types and usage](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Aboutdatasets).

Your role must have the upload\_lookup\_files capability. Without it you cannot create or edit CSV lookups in Splunk Web.

See [Define roles with capabilities](http://docs.splunk.com/Documentation/Splunk/9.3.1/Security/Rolesandcapabilities) in *Securing Splunk Enterprise*.

**About the CSV files**

There are some restrictions to the files that can be used for CSV lookups.

* The table in the CSV file should have at least two columns. One column represents a field with a set of values that includes values belonging to a field in your events. The column does not have to have the same name as the event field. Any column can have multiple instances of the same value, which is a multivalued field.
* The characters in the CSV file must be plain ASCII text and valid UTF-8 characters. Non-UTF-8 characters are not supported.
* CSV files cannot have "\r" line endings (OSX 9 or earlier)
* CSV files cannot have header rows that exceed 4096 characters.

**Upload the lookup table file**

To use a lookup table file, you must upload the file to your Splunk platform.

**Prerequisites**

* See [lookup](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/LookupexampleinSplunkWeb) for an example of how to define a CSV lookup.
* An available .csv or .gz table file.
* Your role must have the upload\_lookup\_files capability. Without it you cannot upload lookup table files in Splunk Web. See [Define roles with capabilities](http://docs.splunk.com/Documentation/Splunk/9.3.1/Security/Rolesandcapabilities) in *Securing Splunk Enterprise*.

**Steps**

1. Select **Settings > Lookups** to go to the Lookups manager page.
2. Click **Add new** next to **Lookup table files**.
3. Select a **Destination app** from the drop-down list.
4. Click **Choose File** to look for the CSV file to upload.
5. Enter the destination filename. This is the name the lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, enter a filename ending in ".gz". If you are uploading a plaintext CSV file, use a filename ending in ".csv".
6. Click **Save**.

By default, the Splunk software saves your CSV file in your user directory for the **Destination app**: $SPLUNK\_HOME/etc/users/<username>/<app\_name>/lookups/.

**Share a lookup table file with apps**

After you upload the lookup file, tell the Splunk software which applications can use this file. The default app is Launcher.

1. Select **Settings > Lookups**.
2. From the Lookup manager, click **Lookup table files**.
3. Click **Permissions** in the Sharing column of the lookup you want to share.
4. In the Permissions dialog box, under **Object should appear in**, select **All apps** to share globally. If you want the lookup to be specific to this app only, select **This app only**. You can also keep your lookup private by selecting **Keep private**.
5. Click **Save**.

**Create a CSV lookup definition**

You must create a [**lookup definition**](https://docs.splunk.com/Splexicon:Lookupdefinition) from the lookup table file.

**Prerequisites**  
In order to create the lookup definition, share the lookup table file so that Splunk software can see it.

**Review**

* [About lookups](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Aboutlookupsandfieldactions).
* [Configure a time-based lookup](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Configureatime-boundedlookup).
* [Make your lookup automatic](http://docs.splunk.com/Documentation/Splunk/9.3.1/Knowledge/Makeyourlookupautomatic).

**Steps**

1. Select **Settings > Lookups**.
2. Click **Add new** next to **Lookup definitions**.
3. Select a **Destination app** from the drop-down list.  
   Your lookup table file is saved in the directory where the application resides. For example: $SPLUNK\_HOME/etc/users/<username>/<app\_name>/lookups/.
4. Give your lookup definition a unique **Name**.
5. Select **File-based** as the lookup **Type**.
6. Select the **Lookup file** from the drop-down list. For a CSV lookup, the file extension must be .csv.
7. (Optional) If the CSV file contains time fields, make the CSV lookup time-bounded by selecting the **Configure time-based lookup** check box.

|  |  |  |
| --- | --- | --- |
| **Time-based options** | **Description** | **Default** |
| Name of time field | The name of the field in the lookup table that represents the timestamp. | No value (lookups are not time-based by default) |
| Time format | The strptime format of the timestamp field. You can include subseconds but the Splunk platform will ignore them. | **%s.%Q** (seconds from unix epoch in UTC and optional milliseconds) |
| Minimum offset | The minimum time (in seconds) that the event timestamp can be later than the lookup entry timestamp for a match to occur. | **0** seconds |
| Maximum offset | The maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur. | **2000000000** seconds |