Splunk® Light Getting Started Manual 6.6.3

Generated: 9/13/2017 2:25 pm

Table of Contents

Table of Contents

Getting Started

About the Splunk Light Getting Started Manual

Welcome to the Splunk Light Getting Started Manual. This manual will help you to:

- Create and manage user accounts.
- Add data to your Splunk Light instance.
- Start searching your data and generate reports.
- Build dashboards to visually display your data.

For more information, see the Splunk Light product page and watch the Splunk Light Product Tour video.

Splunk Light Overview

Splunk Light features

Splunk Light delivers log search and analysis for individuals, small businesses, and work groups within larger organizations. It provides monitoring and troubleshooting solutions for the system administrators, support analysts, application teams, and developers who work with logs and are responsible for multiple use cases across multiple platforms.

Key features and capabilities

Indexing

Add data from a variety of sources: upload files to Splunk Light, monitor files or directories, receive data from Splunk Forwarders, or enable pre-defined data sources from Splunk Add-ons. You can index logs, clickstream data, configurations, traps and alerts, messages, scripts, performance data and statistics from your applications, servers, mainframes and network devices?physical, virtual and in the cloud. See About adding data to Splunk Light in the *Getting Started Manual*.

Freeform search

Freeform search supports intuitive Boolean, nested, quoted string and wildcard searches familiar to anyone comfortable on the web. Includes real-time search, timerange search, and transaction-level search.

Monitor and alerting

Monitor for specific conditions and correlate events from multiple data sources across your IT infrastructure so you can monitor more meaningful and complex events.

Reporting and analysis

Generate reports on an immense amount of data instantly. Provides access to key data for a specified time window to make business-critical, real time decisions. Easily report on search results and on correlated events.

Custom Dashboards

Create custom dashboards and interactive views for different types of users, technical and non-technical. Integrate reports with search results. Edit dashboards using a simple drag-and-drop interface.

Add-ons

You can extend the capabilities of Splunk Light by installing and enabling additional Splunk Add-ons. Splunk Light includes a set of add-ons that you can install and enable to configure new data inputs. You can also browse Splunkbase for more Splunk Light compatible add-ons to install. See Configure an add-on to add data in Splunk Light in the *Getting Started Manual*.

Splunk Light Free versus Splunk Light

The following table lists the Splunk Light features enabled by the license type.

Features	Splunk Light Free	Splunk Light
Daily Indexing Volume	Up to 500MB	Up to 20GB
Search and Reporting	Yes	Yes
Dashboards	Yes	Yes
Alerting	No	Yes
Accounts	1 Admin	Up to 5, Admin and User
Add-ons	Yes	Yes

See About Splunk Light licensing in the *Installation Manual*.

Differences between Splunk Light and Splunk Enterprise

Features	Splunk Enterprise	Splunk Light
Maximum daily indexing volume	Unlimited	20GB
Maximum users	Unlimited	5
Data collection add-ons	Yes	Yes
Apps	Yes	No
Monitoring and alerting	Yes	Yes

Dashboards and reports	Yes	Yes
Search and analysis	Yes	Yes
Automatic data enrichment	Yes	Yes
Anomaly detection	Yes	Yes
Scalability	Unlimited	Single Server
Access control	Customizable	User and Admin only

See Splunk Light versus Splunk Enterprise Comparison.

Upgrade to Splunk Enterprise

You can upgrade and migrate from Splunk Light to Splunk Enterprise. See About upgrading and migrating Splunk Light in the *Installation Manual*.

Starting Splunk Light

Start Splunk Light and log into Splunk Web

Before you use Splunk Light, you need to do the following.

Start Splunk Light

When you install Splunk Light using the graphical installers for Windows and Mac OSX, you can start Splunk Light from the Windows Start Menu or the Mac OSX Splunk Light application icon, respectively. When you install Splunk Light with the compressed installer files or Linux packages, you can start and stop Splunk Light by using the command line interface.

```
splunk start
splunk stop
```

Launch Splunk Web

Splunk Web is the graphical user interface for Splunk Light. You access Splunk Web using a web browser. After Splunk Light starts, it displays the location URL for accessing Splunk Web.

```
The Splunk web interface is at http://username-local:8000
```

Open the URL for Splunk Web in a supported browser.

Log into Splunk Web

After you navigate to Splunk Web, you need to log in. Unless you or your administrator configured it otherwise, your login credentials are not your Splunk.com username and password.

If this is the first time you log in after a new installation, use the default credentials.

```
username = admin
password = changeme
```

You can change your password when prompted in the next screen. If you are the administrator of this Splunk Light instance, you can change your username and manage your account settings.

About the Splunk Light user interface

This topic explains the different views that make up the Splunk Light user interface, Splunk Web.

Navigation menus

You can navigate the Splunk Light bar and the system or sidebar menu.

There are two menus that you can use to navigate your Splunk Light instance: the Splunk Light bar and the system or sidebar menu.

At the top of every page is the Splunk Light bar.

Use the Splunk Light bar to navigate the different views in Splunk Light. These views include **Search**, **Reports**, **Alerts**, and **Dashboards**. You can click the Splunk Light logo on the top left to return to Home, which is the Splunk Light landing page.

The top right of the bar includes your account menu. You can use this menu to edit your account settings and log out of your instance.

The menu icon to the left of the Splunk Light logo opens a sidebar menu. Use this menu to view and manage system messages and access the different settings pages for your Splunk Light instance.

Tasks you can accomplish from the settings pages include the following.

- To view and manage the data sources you added to Splunk Light, go to **Data** and select **Data inputs**.
- To update or reset your license, go to **System** and select **Licensing**.
- To restart Splunk Light, go to **System** and select **Restart**.

Splunk Light Home

Splunk Light Home is the landing page when you log into Splunk Light and when you click the Splunk Light logo at the top left. Another name for Splunk Light Home is the Search Summary view.

You can use this page to do the following actions.

- Open the **Add Data** view to configure new data inputs.
- View a summary of the existing data inputs that is stored in the main index.
- Run a new search by typing your search string into the search bar.
- View and interact with your search history.

New Search

After you run a search, the **New Search** view opens.

This view consists of the search bar, a time range picker, search job actions and controls, and search results tabs. You can use this view to do the following.

- Interact with the results of a recently completely search.
- Refine the search or run a new search.
- Edit the visualization for your result.

After you run a search, you can save it as a report, configure alerts based on the search, and create dashboards based on the searches and reports.

Reports

View and manage your saved reports from the **Reports** page.

Actions you can do include the following.

- Open the saved report and edit the underlying search or data visualization.
- Edit the report's Permissions to share it with other users.
- Open the report in the Search view to modify the search and save it as another report.
- Clone the report to edit it and save it as another report.
- Toggle the display of the reports to show as tiles or as a list.

Alerts

With a Splunk Light paid license, you can configure alerts. An alert is an action that triggers based on specified results of the search. View and manage your configured and triggered alerts from the **Alerts** page.

See About alerting in Splunk Light in the *Getting Started Manual.*

Dashboards

Use the **Dashboards** page to access your saved dashboards. You can also create new dashboards from inline searches using the dashboard editor on this page.

See About using dashboards in Splunk Light in the *Getting Started Manual*.

Managing accounts

About Splunk Light accounts

Splunk Light supports two pre-defined user roles: Admin and User. The Admin role can add users and manage account settings for users. The User role only has access to its own settings. Neither role can create custom roles or modify access that particular roles have.

Splunk Light uses Splunk Authentication and does not support integration with LDAP or single sign-on.

Admin versus User roles

If you are logged into Splunk Light with a User account, you can only view your own account details and edit your own password.

If you are logged into Splunk Light with an Admin account, you can view and manage all the accounts on the instance. Management tasks include adding new accounts, changing account passwords, changing the account type to have User or Admin permissions, and deleting the account.

If you are logged into Splunk Light Free, you are limited to a single Admin account. You cannot add additional accounts or change your account type.

Splunk Light versus Splunk Light Free

The number of accounts you can have depends on your Splunk Light license.

License	Accounts	Roles
Splunk Light Free	1	Admin
Splunk Light	Up to 5	Admin, User

Create a User account in Splunk Light

The Splunk Light license supports up to five user accounts in your Splunk Light instance. Accounts can have Admin or User roles. You need to log in as an Admin to create and manage user accounts.

The Splunk Light Free license supports a single Admin account. You cannot add additional accounts.

Create a user account

1. Click the sidebar menu in the Splunk bar.
2. Under **System**, click **Manage accounts**.
3. In the **Manage Accounts** view, click **New user**. **Note:** This option is only available when you log in as an **Admin**. The **User** role cannot create new accounts.
4. Next to **Role**, click **User**. This assigns the role of **User** to the new account you create.
5. Enter the **Username** for the account.
6. Select permission to delete data.
7. Enter a valid **Email address**.
8. Enter a **Password** and **Confirm password**.
9. Enter the user's **Full name**. The user's initials are used in the account's icon.
10. Select the user's **Time zone**.
11. Click **Save**.

Manage account settings in Splunk Light

If you log into Splunk Light as a User, you can only view your own account details and edit your own password.

If log into Splunk Light as an Admin, you can view and manage all the accounts on the instance. The following are examples of management tasks.

- Changing the account's password.
- Changing the account type to have User or Admin permissions.
- Enabling or disabling the **Permission to Delete Data** option for other users.
- Deleting the account.

Change the password for an account

1. In the **Manage Accounts** page, select the user's account. This opens the user's account details.
2. Next to **Password**, type a new password.
3. Next to **Confirm password**, type the password again.

4. Click **Save**.

Change a User to an Admin

1. In the **Manage Accounts** page, select the user's account. This opens the user's account details.
2. Next to **Role**, click **Admin**.
3. (Optional) Next to **Permission to Delete Data**, click **Yes**.
4. Click **Save**.

Delete an account

1. In the **Manage Accounts** page, select the user's account. This opens the user's account details.
2. At the bottom of the page, click **Delete**.
3. In the dialog window, click **Delete** to confirm that you want to delete the user.

Getting data in

About adding data to Splunk Light

This section discusses options for getting data into Splunk Light. You can add data inputs from files and directories, network ports, scripted inputs, and from Splunk universal forwarders.

When you add data, the indexer processes it and stores it in an **index**. Indexes reside in flat files on your Splunk Light instance. By default, data you feed to an indexer is stored in the **main** index, but you can create and specify other indexes for different data inputs.

The Add Data page

There are different options for getting data into Splunk Light. Use the **Add Data** page to upload, monitor, or forward data. You can also configure an Add-on to add data to Splunk Light.

Upload

The Upload option lets you upload a file or archive of files for indexing. When you click Upload, Splunk Web goes to a page that starts the upload process. See:

- Upload a file to Splunk Light in the *Getting Started Manual*.
- About source types and input settings for Splunk Light in the *Getting Started Manual*.

Monitor

The Monitor option lets you monitor one or more files, directories, network

streams, scripts, Event Logs (on Windows hosts only), performance metrics, or any other type of machine data that the Splunk Light instance has access to. When you click Monitor, Splunk Web loads a page that starts the monitoring process. See:

- Monitor files and directories using Splunk Light in the *Getting Started Manual*.
- Monitor network ports using Splunk Light in the *Getting Started Manual*.

Note: The Splunk Light cloud service does not support monitoring inputs.

Forward

The Forward option lets you receive data from forwarders into your Splunk Light instance. When you click the "Forward" button, Splunk Web takes you to a page that starts the data collection process from forwarders. The Forward option requires configuration of a universal forwarder before the Forwarder page is populated. See:

- Forward data to Splunk Light using Microsoft Windows in the *Getting Started Manual*.
- Forward data to Splunk Light using Linux in the *Getting Started Manual*.
- Forward data to Splunk Light using Mac OS in the *Getting Started Manual*.

Check the status of configured forwarders:

- Check the status of forwarders in Splunk Light in the *Getting Started Manual*.

Use an Add-on to add data

To use an add-on to add data to Splunk Light, see Configure an Add-On to add data in Splunk Light in the *Getting Started Manual*.

About source types and input settings for Splunk Light

Splunk Light assigns a set of **default fields** to all incoming data as it **indexes** each **event**. These default fields include the **source**, **source type**, **host**, and **index**.

- **source** is the file name, directory path, or network protocol and port where the data originates.
- **source type** is the format of the data, such as syslog, IIS, or access_combined.
- **host** is the machine or device where the data originates.
- **index** is where Splunk Light stores the data after you add it.

When you configure new data inputs, you can override the default field assignments for source type, host, and index. This topic discusses the importance of each input setting and why you might want to change them.

Understanding source and source types

The source identifies where the data originates and assigns it to the field named, `source`. For data monitored from files and directories, the source is the name of the file or the full pathname of the file or directory, such as `errorlog.txt` or `/var/log`. For a network-based input, the source is the the protocol and port, such as `UDP:514`. Data can originate from one source, but have many source types.

The source type indicates the format of the data and assigns it to the field named, `sourcetype`. It is important to assign the correct source type to your data for the **event data** to display with the correct **timestamps** and event breaks.

Any common data format can be a source type. Splunk Light includes predefined source types for most log formats. When you configure new data inputs, Splunk Light attempts to automatically assign the source type based on these predefined settings. You can override the setting by selecting another source type from the list, if one matches. If your data is specialized and does not match one of the predefined source types, you can create new source types and customize your event processing settings. If needed, you can assign source types based on the event, rather than based on the source.

See Why source types matter in the Splunk Enterprise *Getting Data In* manual.

Predefined source types

The following table lists examples of predefined source types that Splunk Light can automatically assign to the `sourcetype` field when it indexes new data.

Source type	Description	Sample Event
access_combined_wcookie		

	NCSA combined format HTTP web server logs with cookie field added at the end. This log can be generated by Apache or other web servers.	`"66.249.66.102.1124471045570513" 59.92.110.121 - - [19/Aug/2005:10:04:07 -0700] "GET /themes/splunk_com/images/logo_splunk.png HTTP/1.1" 200 994 "http://www.splunk.org/index.php/docs" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.8) Gecko/20050524 Fedora/1.0.4-4 Firefox/1.0.4" "61.3.110.148.1124404439914689"`
apache_error	Standard Apache web server error log.	`[Sun Aug 7 12:17:35 2005] [error] [client 10.1.1.015] File does not exist: /home/reba/public_html/images/bullet_image.gif`
cisco_syslog	Standard Cisco syslog produced by all Cisco network devices including PIX firewalls, routers, ACS, and so on, usually via remote syslog to a central log host.	`Sep 14 10:51:11 stage-test.splunk.com Aug 24 2005 00:08:49: %PIX-2-106001: Inbound TCP connection denied from IP_addr/port to IP_addr/port flags TCP_flags on interface int_name Inbound TCP connection denied from 144.1.10.222/9876 to 10.0.253.252/6161 flags SYN on interface outside`
websphere_activity	Websphere activity log, also often referred to as the	`---------- ComponentId: Application Server ProcessId: 2580 ThreadId: 0000001c ThreadName: Non-deferrable Alarm : 3 SourceId: com.ibm.ws.channel.framework.impl. WSChannelFrameworkImpl ClassName: MethodName:`

	service log.	`Manufacturer: IBM Product: WebSphere Version: Platform 6.0 [BASE 6.0.1.0 o0510.18] ServerName: nd6Cell01\was1Node01\TradeServer1 TimeStamp: 2005-07-01 13:04:55.187000000 UnitOfWork: Severity: 3 Category: AUDIT PrimaryMessage: CHFW0020I: The Transport Channel Service has stopped the Chain labeled SOAPAcceptorChain2 ExtendedMessage: ----------`

For the complete list, see List of pretrained source types in the Splunk Enterprise *Getting Data In* manual.

Overriding default host values

An event's `host` field value is the typically the hostname, the IP address, or the fully qualified domain name for the machine or device where the event orginates.

Splunk Light assigns a default host value to all incoming data, if no other host rules exist for the source. When you run Splunk Light on the server generating the events, this host assignment is the server's name and should not need to be modified.

You might need to override the default host assignment for received data inputs from a Splunk Forwarder. You can define a static host value for all incoming data for this input, or you can dynamically assign the host value to a portion of the path or filename of the source. Using the path segment can be helpful when you have a directory structure that segregates each host's log archive into different sub-directories.

See About hosts in the Splunk Enterprise *Getting Data In* manual.

Customizing indexes

The `index` field value specifies where the event data is stored on the Splunk Light instance after the data is added. By default, incoming data is saved to the `main` index. If you want to save new data to a custom index, you first need to create the index.

The following are some reasons why you might want to have multiple indexes:

- **Control user access.** You might want to restrict access to data based on the user's role and permissions.
- **Accommodate different retention policies.** If you have different archive or retention policies for different data sets, your can create indexes to

reflect these policies.
- **Improve search speed.** The index is a searchable field. If you typically search for events from specific inputs, you can create dedicated indexes for each data source. Then, you can specify that index when you search for that specific event.

See About managing indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

Upload a file to Splunk Light

Use **Upload** to get data in when you want to index the data once. The data source can be a static file, such as a CSV file, or an archive of historical data.

1. Go to the Splunk Light Search view.

The **Data** panel is located under the search bar and to the right.

2. Under **Data**, click **Add Data**.

3. In the **Add Data** view, click **Upload**.

4. Click **Select File** to browse for your CSV file, or drag-and-drop the file into the outlined box.

The following screenshot shows the file "all_month.csv", which is a csv file of earthquake data.

5. Click **Next**.

6. (Optional) Review your data in the **Set Sourcetype** view.

7. Click **Next**.

8. Use **Input Settings** to customize the host and index values.

9. Click **Next** to **Review** your input.

10. Click **Submit**.

Monitor files and directories using Splunk Light

Use **Monitor** to get data in when the file or directory updates and you want to continue to index the data as it updates. You can also monitor mounted or shared directories, including network file systems. If the specified directory contains subdirectories, the monitor function recursively examines them for new files.

For Windows data inputs, you can use monitor to add data from Windows event logs, Windows registry, Windows performance monitoring, and Active Directory logs.

Select the data source

1. In the **Add Data** view, click **Monitor**.

2. Select **Files & Directories** to view the configuration options.

3. Next to **File or Directory**, type in or **Browse** for the directory path.

4. Choose how to monitor the data input:

- **Continuously monitor** configures an ongoing data input. This means that Splunk Light monitors the file or directory for updates and indexes the updates.
- **Index once** copies the data into the Splunk Light index.

5. (Optional) For directory inputs, you can specify a whitelist and blacklist to indicate files you want to include and exclude when indexing the data. Use regular expressions to match these files.

6. Click **Next** to continue.

Data preview

For file inputs, after you define the source, you have an additional **Set source type** step. This step lets you preview the data before it is indexed, customize the source type, and adjust the event breaks, timestamp, and other settings.

For directory inputs, you do not have data preview. You can set the source type in **Input Settings**.

Specify input settings

1. Next to **Source Type**, click **Automatic** for Splunk Light to assign the source type, click **Select** to choose from a list of predefined source types, or click **Manual** to type in a custom source type.

2. (Optional) Override the automatic **Host** field value assignment with a custom **Constant value**, **Regular expression on path**, or **Segment in path**.

3. (Optional) Specify a different **Index** to save the data.

You can **Create a new index** and refresh the list of indexes. By default all data saves to the default `main` index.

4. Click **Review** to continue.

Review and Save

1. Review the summary of your data input.

2. (Optional) Go back, to make changes.

3. Click **Submit** to complete the add data process.

Monitor network ports using Splunk Light

You can monitor TCP or UDP ports to add data from the syslog service on one or more machines.

Select the network source

1. In the **Add Data** view, click **Monitor**.

2. Select **TCP**/**UDP** to view the configuration options for network ports.

3. Select either **TCP** or **UDP**.

4. Type in the **Port** number.

For example, the standard port for TCP is 9997 and for UDP is 514.

5. (Optional) Next to **Source name override**, type in a custom source name using the format `host:port`.

6. (Optional) Next to **Only accept connection from**, type in the name, IP address, or fully qualified domain name for each host. You can use wildcards to specify more than one host. This setting restricts the data input to specific machines or devices.

7. Click **Next** to continue.

Specify input settings

Use the **Input Settings** to modify the source type, host, and index assignments for the incoming network data.

1. Select the **Source type** from the list of predefined source types or type it in manually.

2. (Optional) Assign the **Host** field value.

- Select **IP** for IP addresses.
- Select **DNS** for domain name system.
- Select **Custom** to type in a host name.

3. (Optional) Select a different **Index** to store the data.

You can **Create a new index** and refresh the list of indexes. By default all data saves to the default `main` index.

4. Click **Review** to continue.

Review and Save

1. Review the summary of your data input.

2. (Optional) Go back to make changes.

3. Click **Submit** to complete the add data process.

Use HTTP Event Collector in Splunk Light

HTTP Event Collector (HEC) is an endpoint that lets you send application events to your Splunk deployment using the HTTP or Secure HTTP (HTTPS) protocols. HEC uses an authentication model based on tokens that you generate. You then configure a logging library or HTTP client with this token to send data to HEC in a specific format. This process eliminates the need for a forwarder when sending application events.

HEC was created with application developers in mind, so that all it takes is a few lines of code added to an app for the app to send data. Also, HEC is token-based, so you never need to hard-code your Splunk credentials in your app or supporting files.

HEC runs as a separate app called `splunk_httpinput` and stores its input configuration in `$SPLUNK_HOME/etc/apps/splunk_httpinput/local`.

For more information about getting started with HEC on the Splunk platform, see Getting data in with HTTP Event Collector on *Splunk Dev Portal*.

About Event Collector Tokens

Tokens are entities that let logging agents and clients connect to the HTTP Event Collector endpoint. Each token has a token value: a 32-bit number that agents and clients use to authenticate their connections to HEC. When they connect, they present this token value. If HEC has the token value configured and it is active, HEC accepts the connection and the agent can then begin delivering its payload of application events in JavaScript Object Notation (JSON) format.

HEC receives the events and Splunk software indexes them based on the configuration of the token that the agent used to connect, using the source, source type, and index that was specified in the token. If a forwarding output group configuration exists, the application events are forwarded to other indexers as the output group defines them.

Configure HTTP Event Collector in Splunk Web

Enable HTTP Event Collector

Before you can use Event Collector to receive events through HTTP, you must enable it. If your Splunk deployment is a managed Splunk Light cloud service deployment, HEC must be enabled by Splunk Support before you can use it. For

Splunk Light, enable HEC as follows:

1. From the sidebar menu, click **Data > Data Inputs**.

2. On the left side of the page, click **HTTP Event Collector**. The HEC management page loads.

3. In the upper right corner, click **Global Settings**.

4. In the **All Tokens** toggle button, select **Enabled**.

5. To set the source type for all HEC tokens, select a category from the **Default Source Type** drop-down, then select the source type you want. 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. To set the default index for all HEC tokens, choose an index in the **Default Index** drop-down.

7. (Optional) To set the default forwarding output group for all HEC tokens, choose an output group from the **Default Output Group** drop-down.

8. To use a deployment server to handle configurations for HEC tokens, click the **Use Deployment Server** check box.

9. To have HEC listen and communicate over HTTPS rather than HTTP, click the **Enable SSL** checkbox.

10. To specify the port number that HEC listens on, enter a number in the **HTTP Port Number** field.

Note: To ensure that proper communication happens between logging agents and HEC, confirm that no firewall blocks the port number specified in the **HTTP**

Port Number field, either on the agents, the Splunk instance that hosts HEC, or in between.

11. To save your settings, click **Save**. The dialog box disappears and Splunk Web saves the global settings and returns you to the HEC management page.

12. Restart Splunk Light.

Create an Event Collector token

To use the HTTP Event Collector, you must configure at least one token. The token is what clients and agents use when they connect to Event Collector to send data.

1. Go to the HEC management page. From the sidebar menu, click **Data > Data Inputs > HTTP Event Collector**.

2. In the upper right corner, click **New Token**. The right pane populates with fields for HEC end point.

3. In the **Name** field, enter a name for the token that describes its purpose and that you will remember.

4. (Optional) In the **Source name override** field, enter a name for a source to be assigned to events that this endpoint generates.

5. (Optional) In the **Description** field, enter a description for the input.

6. (Optional) In the **Output Group** field, select an existing forwarder output group by picking it in the drop-down list.

> **Note:** Define output groups in `outputs.conf`. See Configure forwarders with outputs.conf in the Splunk Universal Forwarder *Forwarder Manual*. You can also set up forwarding in Splunk Web, which generates a default output group called `default-autolb-group`.

7. (Optional) If you want to enable **indexer acknowledgment** for this token, click the **Enable indexer acknowledgment** checkbox.

> **Note:** Indexer acknowledgement is verification from the indexer that events have been indexed. Indexer acknowledgement in HTTP Event Collector is not the same indexer acknowledgement capability described in Protect against loss of in-flight data in the Splunk Enterprise *Forwarding*

Data manual. For more information about indexer acknowledgement in HTTP Event Collector, see **Enable indexer acknowledgment**.

8. Click **Next**. The **Input Settings** page displays.

9. Make edits to source type and confirm the index where you want HEC events to be stored. See Modify input settings in the Splunk Enterprise *Getting Data In* manual.

10. Click **Review**. Confirm that all settings for the endpoint are what you want. If you need to change settings, click the gray **<** button at the top of the page.

11. If all settings are what you want, click **Next**. The success page loads and displays the token value that Event Collector generated. You can copy this token value from the displayed field and paste it into another document for reference later. See About Event Collector Tokens in the *Getting Started Manual*.

Modify an Event Collector token

You can make changes to an HEC token after you have created it. Visit the HEC management page and edit a token to change any of its characteristics, including its name, description, default source type, default index, and output group.

To change the properties of a token:

1. Go to the HEC management page. From the sidebar menu, click **Data > Data Inputs > HTTP Event Collector**.

2. Locate the token that you want to change in the list.

3. In the **Actions** column for that token, click **Edit**. You can also click the link to the token name.

4. Edit the description of the token by entering updated text in the **Description** field.

5. (Optional) Update the source value of the token by entering text in the **Source** field.

6. (Optional) Choose a different source type by selecting it in the **Source Type** drop-down. First choose a category, then select a source type in the pop-up menu that appears. You can also type in the name of the source type in the text box at the top of the drop-down.

7. (Optional) Choose a different index by selecting it in the **Available Indexes** pane of the **Select Allowed Indexes** control. The index moves to the **Selected Indexes** pane of the control.

8. (Optional) Choose a different output group from the **Output Group** drop-down.

9. (Optional) Choose whether or not you want indexer acknowledgment enabled for the token.

10. Click **Save**.

Delete an Event Collector token

You can also delete an HEC token if you don't plan to use it any more. Deleting an HEC token does not affect other HEC tokens, nor does it disable the HEC endpoint.

> **Caution:** You cannot undo this action. Agents that use this token to send data to your Splunk deployment will no longer be able to authenticate with the token. You must generate a new token and change the agent configuration to use the new token value.

To delete an HEC token:

1. Go to the HEC management page. From the sidebar menu, click **Data > Data Inputs > HTTP Event Collector**.

2. Locate the token that you want to delete in the list.

3. In the **Actions** column for that token, click **Delete**.

4. In the Delete Token dialog, click **Delete**. Splunk Light deletes the token and returns you to the HEC management page.

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 an HEC token:

1. Go to the HEC management page. From the sidebar menu, click **Data > Data Inputs > HTTP Event Collector**.

2. Locate the token whose status you want to toggle.

3. In the **Actions** column for that token, click the **Enable** link (if the token is active) or the **Disable** link (if the token is inactive.) The token status toggles immediately and the link changes to **Enable** or **Disable** based on the changed token status.

Make use of HTTP Event Collector from a developer perspective

You have several options within your developer environment for using HTTP Event Collector. You can use our Java, JavaScript (Node.js) and .NET logging libraries, which are compatible with popular logging frameworks. Or you can make an HTTP request using your favorite HTTP client and send your JSON-encoded events.

Making an HTTP call with the command line using a `curl` command in your operating system is an easy way to test this out.

Example:

> **Note:** This POST request is made to port 8088 and uses HTTPS for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

JSON

The following cURL statement uses an example HTTP Event Collector token (`B5A79AAD-D822-46CC-80D1-819F80D7BFB0`), and uses `https://localhost` as the hostname. Replace these values with your own before executing this statement.

JSON Request

```
curl -k  https://localhost:8088/services/collector/event -H
"Authorization: Splunk B5A79AAD-D822-46CC-80D1-819F80D7BFB0" -d
'{"event": "hello world"}'
```

Note: the key "event" is required.

JSON Response

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

More information

You can find more developer-related content about using HTTP Event Collector in the Splunk Developer Portal. For a complete walkthrough of using HTTP Event Collector, see HTTP Event Collector walkthrough.

Forward data to Splunk Light using Microsoft Windows

The **Splunk Universal Forwarder** is the easiest and preferred way of getting data from remote systems into Splunk Light, also known as forwarding data to Splunk Light. The universal forwarder is a separate Splunk software product that needs to be installed and configured as a prerequisite to collect data from a remote system.

The following steps are for a default configuration of the universal forwarder to get data into Splunk Light. In these steps, you will:

- Configure Splunk Light to receive data from the universal forwarder.
- Download and install the universal forwarder software, which includes:
    - Configure the universal forwarder to act as a deployment client.
    - Configure the universal forwarder to send data to the Splunk Light instance.
- Configure inputs to collect data from the host that the universal forwarder is on.

Log into Splunk Light

Log into Splunk Light, also referred to as your Splunk Light instance.

- If you have Splunk Light installed, log into your instance to access the user interface.
- If you do not have Splunk Light, you must provision an instance first before continuing with these steps. Visit the Splunk Light website to learn how to try or buy Splunk Light.

Step 1: Configure Splunk Light to receive data from the universal forwarder

Configure the Splunk Light instance to *receive* data from the universal forwarder.

1. From the Splunk Light user interface, click the menu at the top left of the screen to open the sidebar menu and select **Data > Data receiving**.

2. Click **Add new**.

3. In the **Listen on this port** field, enter the port number that you want the Splunk Light instance to listen on and click **Save**.

- The TCP port is also known as the receiving port.
- The default port is 9997.

The Splunk Light instance begins listening on the port that you entered.

Step 2: Download the universal forwarder

Download the **Splunk Universal Forwarder for Windows** from Splunk.com using the link below. Choose the installer that matches the platform of the machine that will forward data to your Splunk Light instance.

1. From a web browser, go to:
http://www.splunk.com/en_us/download/universal-forwarder.html

2. Click the **Windows** button and click the installer that is appropriate for your platform.

3. Click **Save File** and click **OK** to download the **splunkforwarder** file. The full download file name is similar to *splunkforwarder-<release>-f44afce176d0-x64-release.msi*.

Note: The **splunkforwarder** file is typically saved to the **Downloads** directory by default (for example, \Users\<username>\Downloads\). If downloaded to a different location, make note of the location.

Step 3: Install the universal forwarder

Install the universal forwarder on the machine that holds, or has access to, the data you want to collect and forward to Splunk Light.

Note: If you want to install the universal forwarder on a different machine, copy the universal forwarder package file to that machine and continue with the steps below.

1. Double-click the **splunkforwarder** file to launch and run the installer.

2. Read the license agreement. If you agree to the terms of the license, select **Check this box to accept the License Agreement** and click **Next**.

3. On the Deployment Server dialog, in the **Hostname or IP** field enter the hostname or IP address of the Splunk Light instance, which is the *deployment server*.

4. Enter the port number **8089**. This is the default management port.

5. Click **Next**.

6. On the Receiving Indexer dialog, in the **Hostname or IP** field enter the hostname or IP address of the Splunk Light instance, which is the *receiving server*.

7. Enter the port number **9997**. This is the default receiving port.

8. Click **Install** for the Setup Wizard to perform the installation.

Note: The **SplunkUniversalForwarder** is typically installed in the **Program Files** directory by default. If installed in another location, make note of the location.

9. Click **Finish**. The universal forwarder installation is successfully installed and started.

You should see the universal forwarder listed in the Splunk Light user interface *Forwarder Management* and *Forwarder Monitoring* views (in the sidebar menu, select System > Forwarder Management or Forwarder Monitoring.) This can take a few minutes to update.

Step 4: Specify data inputs to forward data to Splunk Light

Specify which data inputs the universal forwarder uses to collect data.

1. In the Splunk Light user interface, click **Search** in the top menu bar.

2. In the Search view, under **Data** on the right of the screen, click the **Add Data** button.

3. On the Add Data view, click **Forward**.

4. Next to **Select Server Class**, click **New**.

- **Available host(s)** are listed, which are the hostnames of the universal forwarders (deployment clients) connected to the Splunk Light instance (deployment server).

5. Under **Available host(s)**, click one or more forwarder hosts to add to the **Selected host(s)** box. This allows you to add a new **Server Class**.

6. In the **New Server Class Name** field, enter a name for the new server class.

7. Click **Next** near the top of the screen.

8. Select the type of data for the universal forwarder to collect. Click a source option:

- **Files & Directories** for file uploads and directory monitoring.
- **TCP/UDP** for network port inputs.
- **Scripts** for data from APIs and services. In this example, Files & Directories is selected.

9. Enter a File or Directory name. For example, `c:\Windows\windowsupdate.log`

10. Click **Next** near the top of the screen.

11. In the Input Settings view, next to **Source type** click **Automatic**.

12. Click **Review** near the top of the screen. This view provides a summary of the data input configuration that is being used to collect data from the universal forwarder and forward to the Splunk Light instance.

13. Click **Submit**.

14. The **File input has been created successfully** displays. Click **Start Searching** to see the data in the Search view. This might take a few moments to display on the Search page.

Learn more

To continue adding data and to learn more about searching and reporting, see:

- About adding data to Splunk Light in the *Getting Started Manual*.
- About Splunk Light Search and Reporting Examples and Scenarios in *Search and Reporting Examples*.

Forward data to Splunk Light using Linux

The **Splunk Universal Forwarder** is the easiest and preferred way of getting data from remote systems into Splunk Light, also known as forwarding data to Splunk Light. The universal forwarder is a separate Splunk software product that needs to be installed and configured as a prerequisite to collect data from a remote system.

The following steps are for a default configuration of the universal forwarder to get data into Splunk Light. In these steps, you will:

- Configure Splunk Light to receive data from the universal forwarder.
- Download and install the universal forwarder software.
- Configure the universal forwarder to send data to the Splunk Light instance.
- Configure the universal forwarder to act as a deployment client.
- Configure inputs to collect data from the host that the universal forwarder is on.

Log into Splunk Light

Log into Splunk Light, also referred to as your Splunk Light instance.

- If you have Splunk Light installed, log into your Splunk Light instance to access the user interface.
- If you do not have Splunk Light, you must provision an instance first before continuing with these steps. Visit the Splunk Light website to learn how to try or buy Splunk Light.

Step 1: Configure Splunk Light to receive data from the universal forwarder

Configure the Splunk Light instance to *receive* data from the universal forwarder.

1. Once you are logged into the Splunk Light user interface, click the menu at the top left of the screen to open the sidebar menu and select **Data > Data receiving**.

2. Click **Add new**.

3. In the **Listen on this port** field, enter the port number that you want the Splunk Light instance to listen on and click **Save**.

- The TCP port is also known as the receiving port. The default port is 9997.
- The Splunk Light instance begins listening on the port that you specified.

Step 2: Download the universal forwarder

Download the **Splunk Universal Forwarder for Linux** from Splunk.com using the link below. Choose the installer that matches the platform of the machine that will forward data to your Splunk Light instance.

1. From a web browser, go to:
http://www.splunk.com/en_us/download/universal-forwarder.html

2. Click the **Linux** button and click the installer that is appropriate for your platform. This example uses a tar file.

3. Click **Save File** to download the **splunkforwarder** file. The full download file name is similar to *splunkforwarder-<release>-f44afce176d0-Linux-ppc64.tgz*.

4. Save the tar file and make note of the location for where you save it.

Step 3: Install the universal forwarder

Install the universal forwarder on the machine that holds, or has access to, the data you want to collect and forward to Splunk Light.

Note: If you want to install the universal forwarder on a different machine, copy the universal forwarder package file to that machine and continue with the steps below.

1. Expand the tar file into an appropriate directory using the `tar` command. The default installation location is `splunkforwarder` in the current working directory:

```
tar xvzf splunkforwarder-<?>-Linux-x86_64.tgz
```

To install into `/opt/splunkforwarder`, execute:

```
tar xvzf splunkforwarder-<?>-Linux-x86_64.tgz -C /opt
```

2. Start the universal forwarder, including reading and accepting the license.

```
 splunk start --accept-license
```

Step 4: Configure the universal forwarder to send data to Splunk Light

Configure the universal forwarder to *send* data to the Splunk Light instance.

1. Launch a shell or command prompt.

2. Go to `$SPLUNK_HOME/bin` enter the following command:

```
./splunk add forward-server <host>:<port> -auth <username>:<password>
```

- <host> is the host name or IP address of the Splunk Light instance that will *receive* the data. In this example, the hostname is *mycompany.*
- <port> is the receiving port you set on the Splunk Light instance. The default port is 9997.
- <username>:<password> are the username and password used to log into the universal forwarder. In this example, the username and password are admin:changeme.

For example, `./splunk add forward-server mycompany:9997 -auth admin:changeme`

Step 5: Configure the universal forwarder to be a deployment client

Configure the universal forwarder to be a *deployment client*. This allows you to configure data inputs on the universal forwarder from your Splunk Light instance, which is the *deployment server*.

1. Register the universal forwarder as a deployment client of the Splunk Light instance, the deployment server. From `$SPLUNK_HOME/bin`, enter the following command:

```
./splunk set deploy-poll <host>:<mgmtPort>
```

- <host> is the hostname or IP address of the Splunk Light instance. In this example, the hostname is *mycompany*.
- <mgmtPort> is the management port of the Splunk Light instance. The default is 8089.

For example, `./splunk set deploy-poll mycompany:8089`

2. Restart the universal forwarder. From `$SPLUNK_HOME/bin`, enter the following command:

```
./splunk restart
```

You should see the universal forwarder listed in the Splunk Light user interface *Forwarder Management* view (in the sidebar menu, select System > Forwarder Management.) This can take a few minutes to update.

Step 6: Specify data inputs to forward data to Splunk Light

Specify which data inputs the universal forwarder uses to collect data.

1. In the Splunk Light user interface, click **Search** in the top menu bar.

2. In the Search view, under **Data** on the right of the screen, click the **Add Data** button.

3. On the Add Data view, click **Forward**.

4. Next to **Select Server Class**, click **New**.

- **Available host(s)** are listed, which are the hostnames of the universal forwarders (deployment clients) connected to the Splunk Light instance (deployment server).

5. Under **Available host(s)**, click one or more forwarder hosts to add to the **Selected host(s)** box. This allows you to add a new **Server Class**.

6. In the **New Server Class Name** field, enter a name for the new server class.

7. Click **Next** near the top of the screen.

8. Select the type of data for the universal forwarder to collect. In this example, Files & Directories is selected.

- **Files & Directories** for file uploads and directory monitoring.
- **TCP/UDP** for network port inputs.
- **Scripts** for data from APIs and services.

9. Enter a File or Directory name. For example, `/var/log`

10. Click **Next** near the top of the screen.

11. In the Input Settings view, next to **Source type** click **Automatic**.

12. Click **Review** near the top of the screen. This view provides a summary of the data input configuration that is being used to collect data from the universal forwarder and forward to the Splunk Light instance.

13. Click **Submit**.

14. The **File input has been created successfully** displays. Click **Start Searching** to see the data in the Search view. This might take a few moments to display on the Search page.

Learn more

To continue adding data and to learn more about searching and reporting, see:

- About adding data to Splunk Light in the *Getting Started Manual*.
- About Splunk Light Search and Reporting Examples and Scenarios in *Search and Reporting Examples*.

Forward data to Splunk Light using Mac OS

The **Splunk Universal Forwarder** is the easiest and preferred way of getting data from remote systems into Splunk Light, also known as forwarding data to Splunk Light. The universal forwarder is a separate Splunk software product that needs to be installed and configured as a prerequisite to collect data from a remote system.

The following steps are for a default configuration of the universal forwarder to get data into Splunk Light. In these steps, you will:

- Configure Splunk Light to receive data from the universal forwarder.
- Download and install the universal forwarder software.
- Configure the universal forwarder to send data to the Splunk Light instance.
- Configure the universal forwarder to act as a deployment client.
- Configure inputs to collect data from the host that the universal forwarder is on.

Log into Splunk Light

Log into Splunk Light, also referred to as your Splunk Light instance.

- If you have Splunk Light installed, log into your Splunk Light instance to access the user interface.
- If you do not have Splunk Light, you must provision an instance first before continuing with these steps. Visit the Splunk Light website to learn how to try or buy Splunk Light.

Step 1: Configure Splunk Light to receive data from the universal forwarder

Configure the Splunk Light instance to *receive* data from the universal forwarder.

1. From the Splunk Light user interface, click the menu at the top left of the screen to open the sidebar menu and select **Data > Data receiving**.

2. Click **Add new**.

3. In the **Listen on this port** field, enter the port number that you want the Splunk Light instance to listen on and click **Save**.

- The TCP port is also known as the receiving port. The default port is 9997.
- The Splunk Light instance begins listening on the port that you entered.

Step 2: Download the universal forwarder

Download the **Splunk Universal Forwarder for Mac OS** from Splunk.com using the link below. Choose the installer that matches the platform of the machine that will forward data to your Splunk Light instance.

1. From a web browser, go to:
http://www.splunk.com/en_us/download/universal-forwarder.html

2. Click the **Mac OS** button and click the installer that is appropriate for your platform.

3. Click **Save File** to download the **splunkforwarder** file. The full download file name is similar to *splunkforwarder-<release>-f2c83...8108-macosx-10.9.intel.dmg*.

By default, the **splunkforwarder** file is saved to the **Downloads** (/Users/<username>/Downloads/) directory.

Step 3: Install the universal forwarder

Install the universal forwarder on the machine that holds, or has access to, the data you want to collect and forward to Splunk Light.

Note: If you want to install the universal forwarder on a different machine, copy the universal forwarder package file to that machine and continue with the steps below.

1. Double-click the **splunkforwarder** file to launch the installer.

2. Double-click the **Install Splunk Universal Forwarder** icon.

3. The **Introduction** dialog displays, indicating the version and copyright information. Click **Continue**.

4. Read the **Software License Agreement**. Click **Continue** to agree to the license terms.

5. Click **Agree** to confirm you accept the software license agreement and to continue with the installation.

6. The **Installation Type** dialog displays, showing a pre-installation summary. Click **Install**.

7. Confirm you want to install new software. Enter your **Username** and **Password** for the machine you are installing the universal forwarder on, and click **Install Software**.

8. The **Summary** dialog displays indicating the installation was successful. Click **Close**.

9. A brief initialization performs. Click **OK** to continue. The installation starts and might take a few minutes to complete.

10. Click **Start Splunk**.

11. Click **OK** to acknowledge the universal forwarder is installed and started.

By default, the **SplunkForwarder** is installed in the /**Applications** directory.

Step 4: Configure the universal forwarder to send data to Splunk Light

Configure the universal forwarder to *send* data to the Splunk Light instance.

1. Launch a terminal window. A terminal window can typically be found on your Mac by going to Finder > Applications > Utilities > Terminal.

2. Enter the following command:

```
/Applications/SplunkForwarder/bin/splunk add forward-server
<host>:<port> -auth <username>:<password>
```

- <host> is the hostname or IP address of the Splunk Light instance that will *receive* the data. In this example, the hostname is *mycompany.*
- <port> is the receiving port you set on the Splunk Light instance. The default port is 9997.
- <username>:<password> are the username and password used to log into the universal forwarder. In this example, the username and password are admin:changeme.

For example, `/Applications/SplunkForwarder/bin/splunk add forward-server mycompany:9997 -auth admin:changeme`

Step 5: Configure the universal forwarder to be a deployment client

Configure the universal forwarder to be a *deployment client*. This allows you to configure data inputs on the universal forwarder from your Splunk Light instance, which is the *deployment server*.

1. Register the universal forwarder as a deployment client of the Splunk Light instance, the deployment server. Enter the following command:

```
/Applications/SplunkForwarder/bin/splunk set deploy-poll
<host>:<mgmtPort>
```

- <host> is the hostname or IP address of the Splunk Light instance. In this example, the hostname is *mycompany*.
- <mgmtPort> is the management port of the Splunk Light instance. The default is 8089.

For example, `/Applications/SplunkForwarder/bin/splunk set deploy-poll mycompany:8089`

2. Restart the universal forwarder. Enter the following command:

```
/Applications/SplunkForwarder/bin/splunk restart
```

You should see the universal forwarder listed in the Splunk Light user interface *Forwarder Management* view (in the sidebar menu, select System > Forwarder Management.) This can take a few minutes to update.

Step 6: Specify data inputs to forward data to Splunk Light

Specify which data inputs the universal forwarder uses to collect data.

1. In the Splunk Light user interface, click **Search** in the top menu bar.

2. In the Search view, under **Data** on the right of the screen, click the **Add Data** button.

3. On the Add Data view, click **Forward**.

4. Next to **Select Server Class**, click **New**. **Available host(s)** are listed, which are the hostnames of the universal forwarders (deployment clients) connected to the Splunk Light instance (deployment server).

5. Under **Available host(s)**, click one or more forwarder hosts to add to the **Selected host(s)** box. This allows you to add a new **Server Class**.

6. In the **New Server Class Name** field, enter a name for the new server class.

7. Click **Next** near the top of the screen.

8. Select the type of data for the universal forwarder to collect. In this example, Files & Directories is selected. Click a source option:

- **Files & Directories** for file uploads and directory monitoring.
- **TCP/UDP** for network port inputs.
- **Scripts** for data from APIs and services.

9. Enter a File or Directory name. For example, `/var/log`

10. Click **Next** near the top of the screen.

11. In the Input Settings view, next to **Source type** click **Automatic**.

12. Click **Review** near the top of the screen. This view provides a summary of the data input configuration that is being used to collect data from the universal forwarder and forward to the Splunk Light instance.

13. Click **Submit**.

14. The **File input has been created successfully** displays. Click **Start Searching** to see the data in the Search view. This might take a few moments to display on the Search page.

Learn more

To continue adding data and to learn more about searching and reporting, see:

- About adding data to Splunk Light in the *Getting Started Manual*.
- About Splunk Light Search and Reporting Examples and Scenarios in *Search and Reporting Examples*.

Check the status of forwarders in Splunk Light

You can check the status of the universal forwarders that are configured with your Splunk Light instance using the following views:

The **Forwarder Monitoring** view is a dashboard that lists the total count of forwarders you have configured, including a status of each forwarder. From the sidebar menu, go to **System > Forwarder monitoring**.

The **Forwarder Management** view is a dashboard that lists universal forwarders configured as deployment clients with your Splunk Light instance. From the dashboard, you can view and manage deployed add-ons, server classes, and clients. From the sidebar menu, go to **System > Forwarder management**.

Note: If you have universal forwarder(s) configured, but they are not displaying on the Forwarder Monitoring or Forwarder Management pages, confirm you have installed and configured the universal forwarder(s) according to the installation steps.

- For Splunk Light on-premises installations, the universal forwarder must be configured to forward data to Splunk Light and as a deployment client, and the Splunk Light instance configured to receive data from the universal forwarder and as a deployment server. See Forward Data to Splunk Light in the *Getting Started Manual*.
- For Splunk Light cloud service installations, the universal forwarder must have the credentials installed and configured, and configured as a deployment client. See About forwarding data to a Splunk Light cloud service in the *Splunk Light Cloud Service* manual.

Configure an add-on to add data in Splunk Light

Add-ons extend the capabilities of Splunk Light, usually by providing pre-defined data inputs for a specific technology or vendor. Splunk Light includes a set of add-ons that you can install and enable to configure new data inputs.

To install and enable add-ons available in your Splunk Light instance, use the Add-Ons view. Each add-on includes a summary of its features. Note the following:

- Steps to install or enable an add-on vary depending on the add-on.
- Based on the platform you are running, one or more add-ons are pre-installed.
    - ♦ If an add-on has the **install** option, you install the add-on and it is automatically enabled.
    - ♦ If an add-on has the **enable** option, it is pre-installed.
- Some add-ons need additional configuration or set up after enabling, or you can customize and add-on.
- Use Objects to access data inputs, field extractions, knowledge objects, indexes, and prebuilt panels.
- You can install and enable multiple add-ons available in your Splunk Light instance.

Install an add-on

When installing an add-on, the add-on is automatically enabled after installing.

1. In your Splunk Light instance, in the sidebar menu select **Data > Add-ons**.

2. Select the add-on you want to install and click **Install**.

3. Enter your Splunk **username** and **password**.

4. Read and accept the terms and conditions of the license agreement.

5. Click **Login and Install**. The add-on is downloaded and installed in your Splunk Light instance.

6. To complete the installation:

- Click **Restart Splunk** and **Done**. Splunk Light restarts and the add-on is automatically enabled.
- Click **Go Home** and **Done** to remain in Splunk Light.

7. (Optional) To customize an add-on, go to the **Add-Ons** view and the add-on you enabled:

- Click **Set up** to customize data inputs, including enabling, disabling, and configuring polling intervals. Click **Save** after making your selections. Not all add-ons have the Set up option.
- Click **Objects** to view, use, configure, or edit:
    - Indexes
    - Prebuilt panels, which include reusable dashboard content that you can add to multiple dashboards.
    - All objects, which include data inputs, field extractions, and other knowledge objects that are added to your instance.

8. You must restart Splunk Light for your changes to update. To restart:

- At the top of the Add-Ons view, click **Click here to restart**.
- In the sidebar menu, select **System > Restart**.

Enable an add-on

When enabling an add-on, you are selecting to enable a pre-installed add-on.

1. In your Splunk Light instance, in the sidebar menu select **Data > Add-ons**.

2. Select the add-on you want to enable and check **Enable**.

3. (Optional) To customize an add-on:

- Click **Set up** to customize data inputs, including enabling, disabling, and configuring polling intervals. Click **Save** after making your selections. Not all add-ons have the Set up option.
- Click **Objects** to view, use, configure, or edit:
    - Indexes
    - Prebuilt panels, which include reusable dashboard content that you can add to multiple dashboards.
    - All objects, which include data inputs, field extractions, and other knowledge objects that are added to your instance.

4. You must restart Splunk Light for your changes to update. To restart:

- At the top of the Add-Ons view, click **Click here to restart**.
- In the sidebar menu, select **System > Restart**.

Searching, Reporting, and Alerting

About searching and reporting using Splunk Light

This topic contains and overview of searching and reporting.

Searching

After getting data in, you can run **searches** to:

- Learn more about the data you just added.
- Investigate to find the root cause of an issue.
- Summarize your search results into a report, whether tabular or another visualization format.
- Save and share the report.

Raw event searches are searches that retrieve events from one or multiple indexes and are done when you want to analyze a problem. For example, searches you run to check error codes, correlate events, investigate security issues, and analyze failures do not usually include search commands (except `search`, itself), and the results are a list of raw events.

Transforming searches are searches that perform a statistical calculation against a set of results. These are searches where you first retrieve events from an index and then pass them into one or more search commands. These searches will always require fields and at least one of a set of transforming commands. Some examples include: getting a daily count of error events, counting the number of times a specific user has logged in, or calculating the 95th percentile of field values.

See other search topics in this manual, and About Splunk Light Search and Reporting Examples and Scenarios in *Search and Reporting Examples.*

Reporting

Reports are created when you save a search for later reuse. You can save reports with data visualizations, such as charts and tables.

Once you create a report, you can:

- Add the report to a dashboard panel.
- Share the report with others by changing its permissions.
- Set the report to run on a schedule and trigger an alert action.
- Print or generate a PDF of the report.

See Use dashboards in Splunk Light in this manual, and Data Visualization Library in the Splunk Enterprise *References* manual.

Manage the search experience in Splunk Light

This topic discusses search job actions and search modes you can use to manage your search experience. For example, if your search takes too long to run, you can pause it or stop it.

Select time ranges to apply to your search

Use the **time range picker** to set time boundaries on your searches. You can restrict the search to Preset time ranges, custom Relative time ranges, and custom Real-time time ranges. You can also specify a Date Range, a Date & Time Range, and use more advanced options for specifying the time ranges for a search.

When you start a new search, the default time range is **Last 24 hours**. This range helps to avoid running searches with overly-broad time ranges that waste system resources and produce more results than you really need.

Note: If you are located in a different timezone, time-based searches use the timestamp of the event from the Splunk instance that indexed the data.

Search job actions

The search actions are buttons located under the search bar.

While the search is running, you can use the buttons to **Pause** and **Stop** the search. Also, you can access and manage information about the search's **job** without leaving the Search page.

- **Edit job settings.** Select this option to open the Job Settings dialog box, where you can change the job's read permissions, extend the job's lifespan, and get a URL for the job that you can use to share the job with others or put a link to the job in your browser's bookmark bar.

- **Send job to the background.** Select this option if the search job is slow and you want to run the job in the background while you work on other Splunk Light activities (including running a new search job).
- **Inspect job.** Opens a separate window and displays information and metrics for the search job using the **Search Job Inspector**.
- **Delete job.** Use this option to delete a job that is running, is paused, or which has finalized. After you delete the job, you can save the search as a report.

After the search completes, you can also **Share**, **Export**, or **Print** it.

- The **Share** option shares the search job. This option extends the job's lifetime to seven days and set the read permissions to Everyone.
- The **Export** option exports the results. Select this option to output to CSV, raw events, XML, or JSON and specify the number of results to export.
- The **Print** option sends the results to a printer that has been configured.

Search modes

The search mode selector is at the bottom right-hand corner of the search bar. The available modes are **Smart Mode** (default), **Fast Mode**, and **Verbose Mode**:

The Search mode controls the search experience. You can set it to speed up searches by cutting down on the event data it returns (Fast Mode), or you can set it to return as much event information as possible (Verbose Mode). In Smart Mode (the default setting) it toggles search behavior based on the type of search you're running.

The Fast and Verbose modes represent the two ends of the search mode spectrum. The default Smart mode switches between them depending on the type of search that you are running. Whenever you first run a saved search, it will run in Smart mode.

Help building searches in Splunk Light

The Splunk Search Processing Language (SPL) includes many commands and functions that you can use to build searches.

When you write a search in Splunk Web, there are several built-in features that help you build and parse searches.

- Search assistant modes
- Syntax highlighting
- Auto-format search syntax
- Numbering search lines
- Shortcuts

This topic discusses using the search assistant. See Help reading searches in Splunk Light for information about syntax highlighting and shortcuts. All of the SPL commands and functions are documented in the Splunk Enterprise *Search Reference*.

Use the search assistant to build searches

When you type a few letters or a term into the search bar, the search assistant shows you terms and searches that match what you typed.

The **Matching Terms** are based on the terms that are indexed from your data. The **Matching Searches** are based on your recent searches.

The list continues to update as you type.

To add an item in the list to your search criteria you can click on an item, or use the arrow keys to highlight the item and press **Enter**.

Search assistant mode

The search assistant has two modes: Compact and Full. The default mode is Compact.

Compact mode

The Compact mode displays a list of matching terms and searches when you type. When you type a pipe (|) character, to indicate that you want to use a command, a list of the SPL commands appears. You can type a letter to quickly jump to the section of the list that begins with that letter. For example, if you type the letter **s**, the list displays all of the commands that begin with the letter **s**.

When you type a command, a list appears showing Command History and Matching Searches. Initially, the Command History shows some command examples. As you use a command in your searches, the Command History displays your uses of the command instead of the examples.

Below the list is a brief description for the command and an example. The **Learn More** link opens the Splunk Enterprise *Search Reference* in a new window and displays documentation about the command.

> **Tip:** To access the **Learn More** link, use your keyboard. Arrow down to the command or attribute name to highlight the name. Press **Tab** to highlight the **Learn More** link and then press **Enter** to activate the link.

If you type something after the command, the search assistant shows any command arguments or history that match what you type.

The search assistant can also show you the data type that an argument requires. Type the argument in the Search bar. Include the equal (=) symbol, if that is part of the argument syntax. In the following example, the search assistant shows that a <string> value is required for the `countfield` argument.

Full mode

The Full mode displays a list of matching terms and searches when you type, along with a count of how many times a term appears in your indexed data. This

count tells you how many search results will be returned if you search on that term. If a term or phrase is not in the list, the term is not in your indexed data.

The Full mode also provides suggestions in the How To Search section on ways that you can retrieve events and use the search commands.

When you type a command in the Search bar, the list of matching terms and searches is replaced with the **Command History** list.

To add an item in the Command History list to your search criteria click on an item, or use the arrow keys to highlight the item and press **Enter**.

The search assistant displays a brief description of the command and several examples. There are two links next to the command description: Help and More.

- The **Help** link opens the *References* in a new window, and displays documentation about the command.
- The **More** link expands the information about the command that is displayed on the screen.

When you select the **More** link, several new sections appear. The **Details** section provides a more detailed description of the command. The **Syntax** section shows the basic syntax for the command. The **Related** section lists commands that are related to the command that you typed. If the command has complex syntax, click the **More** link next to the syntax to expand the syntax.

If you type something after the command, the search assistant shows any command arguments or history that match what you type.

The search assistant can show you the data type that an argument requires. Type the argument in the Search bar. Include the equal (=) symbol if that is part of the argument syntax. In the following example, the search assistant shows that a <string> value is required for the `countfield` argument.

Change the search assistant mode

The default search assistant mode is Compact. You can change the search assistant mode or temporarily hide the search assistant while you build your search.

When you change the search assistant mode, the change is only for your user account.

Prerequisite

If the Search bar contains a search that you have not run, run the search before you change the search assistant mode. Otherwise the search is lost when you change modes. Running the search adds the search to the search history, where you can access it after you change the mode.

Steps

1. On the Splunk bar, select **[*User icon*] > Account Settings**.
2. Under the **Search Preferences** section, look for **Search assistant** and select **Compact**, **Full**, or **None**.
3. Click **Save**.

The **None** mode turns the search assistant off.

Hide and display the search assistant

By default, the search assistant opens when you type something into the Search bar.

Hide the search assistant by default

Depending on the mode you are using, you can turn off the search assistant or make the search assistant hidden by default.

Compact mode

With the Compact mode, you cannot permanently hide the search assistant. You can only temporarily hide it, or turn it off by changing the search assistant mode to **None**.

- See Temporarily hide the search assistant
- See Change the search assistant mode

Full mode

With the Full mode, you can set the search assistant to be hidden by default.

- In the search assistant window, select **Auto Open**. This removes the check mark next to **Auto Open**.

When you start a new search, the search assistant is hidden. This setting remains active even when you close Splunk Web. The next time you open Splunk Web, the search assistant is hidden.

Temporarily hide the search assistant

In both the Compact and Full modes, you can temporarily hide the search assistant.

Compact mode

- Press **ESC**.

Full mode

- At the bottom of the search assistant window, click the collapse arrow to hide the window.

Unhide the search assistant window

If the search assistant window is hidden, you can unhide it.

Compact mode

- Use the keyboard shortcut for your operating system to unhide the window.
    - ♦ On Linux or Windows, press **CTRL+space**.
    - ♦ On Mac, press **Control+space**.

Full mode

Whether you have the search assistant hidden by default or temporarily hidden, you can unhide the search assistant window at any time.

- Under the Search bar, click the **expand arrow** to display the search assistant window.

  See Temporarily hide the search assistant for information about the collapse/expand button.

If these steps do not unhide the search assistant window, then either the search assistant is turned off or there is no assistance for what you have typed.

To turn the Search Assistant back on, see Change the search assistant mode.

Help reading searches in Splunk Light

The Search bar contains features to help you read, parse, or interpret the Splunk Search Processing Language (SPL) syntax. The syntax highlighting feature displays parts of SPL in different colors. There are also keyboard shortcuts to help you find information in your searches.

Syntax highlighting

With syntax highlighting, the SPL commands, arguments, functions, and keywords are color-coded to make it easier to read a search.

Consider the following search.

```
sourcetype=access_* | timechart count(eval(action=purchase)) BY
productName usenull=false useother=false
```

With syntax highlighting turned on, the search is easier to read. The following image shows the syntax highlighting **Light theme**.

By default, syntax highlighting is turned on.

Color codes

The color coding that is used for the search syntax depends on the color theme that is implemented. The **Light** theme is the default theme. The color codes for the **Light** theme are described in the following table.

Syntax component	Color	Example
Commands	Blue	...timechart
Command arguments	Green	...timechart usenull=false
Functions	Pink	...timechart count
Keyword modifiers and Boolean operators	Orange	...timechart count BY productName

Syntax validation

If command, argument, function, or boolean operator is not spelled or capitalized correctly the term is not highlighted in color. The lack of color helps you ensure that the search is using the correct syntax.

If you specify incorrect data type for an argument, the value turns red. For example, the `limit` argument for the `top` command expects an integer. If you type `...|top limit=false` the term `false` is highlighted in red because it is not a integer.

Turn off syntax highlighting

You can turn syntax highlighting off.

1. On the Splunk bar, select **[*User icon*] > Account Settings**.
2. In the **Search Preferences** section under **Syntax highlighting**, select **Black on white**.
3. Click **Save**.

Color themes

You can change the appearance of the criteria in the Search bar by specifying a color theme. There are several themes to choose from.

Theme name	Theme colors	Notes

Light theme	White background. Black text. Colors for commands, arguments, clauses, functions, keys (in a key-value pair), values, and comments.	Default theme
Dark theme	Black background. Light grey text. Colors for commands, arguments, clauses, functions, keys (in a key-value pair), values, and comments.	
Black on white	White background. Black text. No other colors.	

Change your theme

1. On the Splunk bar, select **[*User icon*] > Account Settings**.
2. In the **Search Preferences** section under **Syntax highlighting**, select the color theme that you want to use.
3. Click **Save**.

Auto-format search syntax

As you build a search, you can set up the Splunk software to format the search syntax as you type.

Auto-format works on searches that you type

The auto-format feature works on searches that you type into the Search bar. If you paste a search into the Search bar or select a search from **Search History**, the search is not automatically formatted even when the auto-format feature is turned on.

To apply auto-formatting to a search that you paste into the Search bar or select from Search History, use the keyboard shortcut to apply auto-formatting to that specific search.

- On Linux or Windows use **Ctrl +** \
- On Mac OSX use **Command +** \

Characters that trigger auto-format

Character	Automatic formatting
Pipe (|)	The pipe is placed on a new line to separate each new piped section of your search criteria.

Left square bracket ([ )	The left square bracket, which signifies the start of a subsearch, is placed on a new line and indented several spaces.

If the pipe or left bracket is inside a quoted string, the auto-format is not triggered.

Turn on Search auto-format

By default, automatic formatting of search syntax is turned off. You can turn on the automatic formatting of the search syntax in Search Preferences.

1. On the Splunk bar, select **[*User icon*] > Account Settings**.
2. In the **Search Preferences** section under **Search auto-format**, select **On**.
3. Click **Save**.

Changing the options in Search Preferences, changes the setting only for you. It does not impact the setting for other users.

Number search lines

To make reading your searches easier, you can display line numbers in the Search bar.

A row in the Search bar is not a line

The line numbering feature applies numbers only to lines. A row in the Search bar is not necessarily a line. You might have a long line that spans multiple rows in the Search bar, but is still only one line.

For example, if you paste a long search into the Search bar that has not already been formatted with multiple lines, the search has one line number and spans multiple rows.

You can create lines in the Search bar by using the following methods.

- The Search auto-formatting feature is turned on and you type a pipe character or left square bracket.
- You use the keyboard shortcut to auto-format the current search.
    - ♦ On Linux or Windows use **Ctrl +** \
    - ♦ On Mac OSX use **Command +** \
- You press **Shift + Enter** to split the active row at the cursor. Pressing **Enter** does not create a new line in the Search bar.

Turn on line numbering

By default, line numbering is turned off. You turn on line numbering in Search Preferences.

1. On the Splunk bar, select **[*User icon] > Account Settings*.**
2. In the **Search Preferences** section under **Show line numbers**, select **On**.
3. Click **Save**.

Changing the options in Search Preferences changes the setting only for you. It does not impact the setting for other users.

Search bar shortcuts

In the Search bar, you can use keyboard shortcuts to help you develop, read, and parse your search criteria.

Make searches easier to read

Long searches can be difficult to read. For example, the following search uses multiple commands and includes many occurrences of renaming columns in the search results.

```
sourcetype=access_* status=200 | stats count AS views
count(eval(action="addtocart")) AS addtocart
count(eval(action="purchase")) AS purchases by productName | eval
viewsToPurchases=(purchases/views)*100 | eval
cartToPurchases=(purchases/addtocart)*100 | table productName views
addtocart purchases viewsToPurchases cartToPurchases | rename
productName AS "Product Name", views AS "Views", addtocart as "Adds To
Cart", purchases AS "Purchases"
```

The following image shows how this search appears in the Search bar.

You can use a keyboard shortcut to parse each pipe section on a separate line. Any subsearches are indented.

- On Linux or Windows use **Ctrl +** \
- On Mac OSX use **Command +** \

The results of the shortcut are shown in the following image.

You can also use **Shift + Enter** to force a new line. See Line and word shortcuts in the Splunk Enterprise *Search Manual*.

Expand your search

You can see the contents of your search with a keyboard shortcut, **Command-Shift-E (Mac OSX)** or **Control-Shift-E (Linux or Windows)** from the Search bar in the Search page. This opens a preview that displays the expanded search string, including all **search macros** and **saved searches**. If syntax highlighting or line numbering are turned on, those features also appear in the preview.

You can copy parts of the search in the preview. You can also click **Open in Search** to run your search in a new window from the preview.

Highlight search terms

- To highlight all of the occurrences of a word in the search, double-click on that word.

Locate matching parenthesis

- Position your cursor immediately after an open or close parenthesis. The matching parenthesis is highlighted.

Undo and Redo shortcuts

Use these keyboard shortcuts to undo and redo actions in the Search bar.

Action	Linux or Windows	Mac OSX
Undo the previous action.	Ctrl + Z	Command + Z
Redo the previous action.	Ctrl + Y or Ctrl + Shift + Z	Command + Y or Command + Shift + Z

Search assistant window shortcuts

With the Compact mode of the search assistant, you can use keyboard shortcuts to select items in the list, and close and reopen the search assistant window.

Action	Linux or Windows	Mac OSX
Move your cursor into the search assistant window.	Down arrow key	Down arrow key
Close the search assistant window.	ESC	ESC
Reopen the search assistant window.	Ctrl + Space	Control + Space
Select an item in the search assistant window and insert it into the Search bar.	Use the Up arrow and Down arrow keys to highlight the item and press **Enter**.	Use the Up arrow and Down arrow keys to highlight the item and press **Enter**.
Toggle between the list and the **Learn More** link in the search assistant window.	Tab	Tab

Find and replace shortcuts

Use the following keyboard shortcuts to find and replace terms in the Search bar.

Action	Linux or Windows	Mac OSX
Find a term.	Ctrl + F	Command + F
Find and replace a term.	Ctrl + H	Command + Option + F

Line and word shortcuts

The distinction between *rows* and *lines* is important to understand when you use keyboard shortcuts to manipulate rows or lines in your search criteria in the Search bar.

- Long searches appear on multiple *rows* in the Search bar.
- If the search is not parsed, the search is one *line*.
- If the search is parsed, separating each piped section and subsearch into its own line, a row is the same as a line.

Action	Linux or Windows	Mac OSX
Split the active row at the cursor.	Shift + Enter	Shift + Enter

Remove the active line. If the search is one line with multiple rows and not parsed into separate lines, the entire search is removed.	Ctrl + D	Command + D
Copy the active row and place the copy below the active row.	Alt + Shift + Down arrow	Command + Option + Down arrow
Copy the active row and place the copy above the active row.	Alt + Shift + Up arrow	Command + Option + Up arrow
Move the active row down one row.	Alt + Down arrow	Option + Down arrow
Move the active row up one row.	Alt + Up arrow	Option + Up arrow
Remove the search criteria from the cursor to the end of the row.	Alt + Delete	Control + K
Remove the search criteria from the cursor to the start of the row.	Alt + Backspace	Command + Delete
Remove the word or space to the right of the cursor.	Ctrl + Delete	Alt + Delete
Remove the word or space to the left of the cursor.	Ctrl + Backspace	Option + Delete

View search results in Splunk Light

After a search runs, the results appear in tabs located below the search bar. There are four results tabs: Events, Patterns, Statistics, and Visualizations. The results tabs populate depending on the type of search commands used in the search. If your search retrieves events, you can view the results in the Events tab and the Patterns tab, but not in the other tabs. If your search includes transforming commands, you can view the results in the Statistics and Visualization tabs.

Events

The Events tab displays the timeline of events, the fields sidebar, and the events viewer. To change the event view, use the **List** and **Format** options. By default, the events appear as a list that is ordered starting with the most recent event. In each event, the matching search terms are highlighted.

Timeline of events: A visual representation of the number of events that occur at each point in time. As the timeline updates with your search results, you might notice clusters or patterns of bars. The height of each bar indicates the count of events. Peaks or valleys in the timeline can indicate spikes in activity or server downtime. Thus, the timeline highlights patterns of events or investigates peaks and lows in event activity. The timeline options are located above the timeline. You can zoom in, zoom out, and change the scale of the chart.

Fields sidebar: When you run a search, the fields discovered are listed next to your search results. You can select other fields to show in your events. Also, you can hide this sidebar and maximize the results area.

- **Selected fields** are set to be visible in your search results. By default, host, source, and sourcetype appear.

- **Interesting fields** are other fields that Splunk has extracted from your search results.

Patterns

The **Patterns** tab simplifies event pattern detection. It displays a list of the most common patterns among the set of events returned by your search. Each of these patterns represents a number of events that all share a similar structure.

You can click on a pattern to:

- View the approximate number of events in your results that fit the pattern.
- See the search that returns events with this pattern.
- Save the pattern search as an event type, if it qualifies.
- Create an alert based on the pattern.

For more information, see Identify event patterns with the Patterns tab in the Splunk Enterprise *Search Manual*.

Statistics

The **Statistics** tab populates when you run a search with transforming commands such as stats, top, chart, and so on. The results are displayed as a statistics table.

Visualizations

Transforming searches also populate the **Visualization** tab. The results area of the Visualizations tab includes a chart and the statistics table used to generated the chart.

You can change the type and Format of the visualization using the menus above the visualization chart area. You can choose from a variety of chart visualizations, such as column, line, area, scatter, and pie charts. The visualization type menu displays the name of the selected type.

When **Recommended** displays next to a chart type, it indicates the types that Splunk Enterprise suggests based on the transforming search that produced the results.

Use reports in Splunk Light

When you create a search or a pivot that you would like to run again or share with others, you can save it as a report. This means that you can create reports from both the Search and the Pivot sides of the Splunk platform.

Once you create a report you can:

- **View the results that the report returns** on the report viewing page. You can get to the viewing page for a report by clicking the name of the report on the Reports listing page.
- **Open the report and edit it** so that it returns different data or displays its data in a different manner. Your report opens in either Pivot or Search, depending on how it was created.

In addition, if your permissions enable you to do so, you can:

- **Change the report permissions** to share it with other Splunk users. See Set report permissions in the Splunk Enterprise *Reporting Manual*.
- **Schedule the report so that it runs on a regular interval.** Scheduled reports can perform actions each time they run, such as sending report results via email to a set of stakeholders. See Schedule reports in the Splunk Enterprise *Reporting Manual*.
- **Accelerate slow-completing reports** built in Search. See Accelerate reports in the Splunk Enterprise *Reporting Manual*.
- **Embed scheduled reports in external websites.** See Embed scheduled reports in external websites in the Splunk Enterprise *Reporting Manual*.
- **Add the report to a dashboard** as a dashboard panel. see Add a search, report, or pivot to a dashboard in the Splunk Enterprise *Dashboards and Visualizations* manual.

Note: Permissions for reports built via Pivot must match those of the data model that was used to construct them. See Permissions for Pivot-based reports in the Splunk Enterprise *Reporting Manual*.

For more information about reports, see the Splunk Enterprise *Reporting Manual*.

Use lookups in Splunk Light

Lookups enable you to enrich and extend the usefulness of your event data through interactions with external resources. Lookup tables use information in your events to determine how to add other fields from external data sources such as static tables (CSV files).

You can use **field lookups** to add new fields to your events. With field lookups you can reference fields in an external CSV file that match fields in your event data. Using this match, you can enrich your event data by adding more

meaningful information and searchable fields from the CSV file to each event. The external CSV files are referred to as **lookup table files**.

Configure a lookup table file

1. In the sidebar menu, go to **Knowledge > Lookups**. The Lookups manager opens, where you can create new lookups or edit existing lookups.

2. In the Lookups manager, locate **Lookup table files**.

3. In the Actions column click **Add new**. You use the Add new lookup table files view to upload CSV files that you want to use.

4. The **Destination app** field specifies which app you want to upload the lookup table file to. The default value is **search**.

5. Under **Upload a lookup file**, browse to and upload the file you want to use.

6. Under **Destination filename**, type the name the lookup table will have on the Splunk server. This is the name that you will use to refer to the file when you create a lookup definition.

7. Click **Save**. This uploads your lookup file to Search and displays the lookup table files list. The lookup table files listed, that are other than what you have uploaded, are included with the Splunk software.

Note: If the Splunk software does not recognize or cannot upload the file, you can take the following actions.

- Check that the file is uncompressed.
- If an error message indicates that the file does not have line breaks, the file has become corrupted. This can happen if a ZIP file is opened in Microsoft Excel before it is uploaded. You should delete the file, then download the ZIP file again, and uncompress the file.

8. Next, share the lookup table file.

Share a lookup table file

After you have a lookup table file uploaded, you need tell the Splunk software which applications can use this file. You can share the lookup table file with Search.

1. In the **Lookup table files** list, locate the list you want to share.

2. In the **Sharing** column, click **Permissions**.

3. Select if you want to share the lookup table file or keep it private.

4. Select the roles you want to share this lookup table file with, including giving read and write access.

5. Click **Save**.

6. Next, add the field lookup definition.

Add the field lookup definition

You must create a lookup definition from the lookup table file.

1. In the sidebar menu, go to **Knowledge > Lookups**.

2. For **Lookup definitions**, click **Add New**. The Add new lookups definitions page opens, where you define the field lookup.

3. There is no need to change the **Destination app** setting. It is already set to the default of **search**.

4. For **Name**, type the name of the lookup definition.

5. For **Type**, select the type of file. A file-based lookup is typically a static table, such as a CSV file.

6. For **Lookup file**, select your lookup table file.

7. If you want to select **Configure time-based lookup** and **Advanced options**, click the box and complete the additional configuration.

8. Click **Save**. Your lookup table file now has a lookup definition.

9. Next, share the lookup definition.

Share the lookup definition

Now that you have created the lookup definition, specify the roles in which you want to share the definition.

1. In the Lookup definitions list, click **Permissions**.

2. Select the roles you want to share this lookup table file with, including giving read and write access.

3. Click **Save**.

You can use this field lookup to add information from the lookup table file to your events. You use the field lookup by specifying the `lookup` command in a search string. Or, you can set the field lookup to run automatically.

Make the lookup automatic

Instead of using the `lookup` command when you want to apply a field lookup to your events, you can set the lookup to run automatically.

1. In the Lookups manager, for **Automatic lookups**, click **Add New**.

> This takes you to the Add new automatic lookups view, where you configure the lookup to run automatically.

2. The default **Destination app** setting is **search**.

3. For **Name**, enter a name for this automatic lookup.

4. Select the **Lookup table**.

> The other options are lookups that are based on the lookup table files that come with the product.

5. For **Apply to**, the value and enter the name.

6. For **Lookup input fields**, enter the values from the lookup table file with values in your events.

- The first text box specifies the value in the lookup table file.
- The second text box specifies the value in your events.

7. For **Lookup output fields**, specify the names of the fields from the lookup table file that you want to add to your event data. You can specify different names.

- In the first text box, type a name that is descriptive name for each productId.
- In the second text box, after the equal sign, type the name of the field that will appear in your events for the descriptive name of the product.

8. If you want to overwrite field values, check **Overwrite field values**. Typically, this remains unchecked.

9. Click **Save**.

Use search macros in Splunk Light

Search macros are reusable chunks of Search Processing Language (SPL) that you can insert into other searches. Search macros can be any part of a search, such as an eval statement or search term, and do not need to be a complete command. You can also specify whether or not the macro field takes any arguments.

Insert search macros into search strings

To include a search macro in a search string, use the back tick character (` ). On most English-language keyboards, this character is located on the same key as the tilde (~). You can also reference a search macro within other search macros using this same syntax. If you have a search macro named `mymacro` it looks like this when referenced in a search:

```
sourcetype=access_* | `mymacro`
```

Macros inside of quoted values are not expanded. In the following example, the search macro `bar` is not expanded.

```
"foo`bar`baz"
```

Search macros that contain generating commands

Generating commands like `search`, `metadata`, `inputlookup`, `pivot`, and `tstats` always appear at the start of search strings with a leading pipe character. If the definition of your search macro starts with a generating command, the search macro should be inserted into the start of your search string, with a leading pipe character before it. Do not put a leading pipe character in the definition of search macros that begin with generating commands. Here is an example:

```
| `mygeneratingmacro`
```

When search macros take arguments

If your search macro takes arguments, you define those arguments when you insert the macro into the search string. For example, if the search macro `argmacro(2)` includes two arguments that are integers, you might have insert the macro into your search string like this: `` `argmacro(120,300)` ``.

If your search macro argument includes quotes, escape the quotes when you call the macro in your search. For example, if you pass a quoted string as the argument for your macro, you would use: `` `mymacro("He said \"hello!\"")` ``.

Your search macro definition can include a validation expression that determines whether the arguments you have entered are valid, and a validation error message that you see when you provide invalid arguments.

Define search macros

Prerequisites

- Learn how to Insert search macros into search strings.
- Understand how to design a search macro definition.
- If your search macros require the search writer to provide argument variables, you can design validation expressions that tell you when invalid arguments have been submitted. See Validate search macro arguments.

Steps

1. In the sidebar menu, go to **Knowledge > Search macros**.
2. Click **New** to create a new search macro.
3. Change the **Destination App** to the app you want to restrict your search macro to if it has defaulted to the wrong app.
4. Provide a unique **Name** for the search macro.
   If your search macro includes an argument, indicate this by appending the number of arguments to the name. For example, if your search macro `mymacro` includes two arguments, name it `mymacro(2)`.
5. In **Definition**, provide the search string that the macro expands to when you reference it in another search.
6. (Optional) Select **Use eval-based definition?** to indicate that the **Definition** value is an `eval` expression.
7. (Optional) Provide **Arguments** as appropriate for your search macro. This is a comma-delimited string of argument names without repeated

elements. Argument names may only contain alphanumeric characters (a-Z, A-Z, 0-9), underscores, and dashes.
8. (Optional) Provide a **Validation expression** that verifies whether the argument values used to invoke the search macro are acceptable. The validation expression is an `eval` expression that evaluates to a boolean or a string.
9. (Optional) Provide a **Validation error message** if you defined a validation expression. This is the message that returns when the argument values that invoke the search macro fail the validation expression.
10. Click Save to save your search macro.

Design a search macro definition

The fundamental part of a search macro is its definition, which is the SPL chunk that the macro expands to when you reference it in another search. There are a few things that you should know before you design a search macro definition.

If your search macro definition has variables that must be input by the macro user, put them in the definition as tokens that have dollar signs wrapped around them. For example, `$arg1$` could be the first argument in a search macro definition.

Pipe characters and generating commands in macro definitions

When you use **generating commands** such as `search`, `inputlookup`, or `tstats` in searches, you always put them at the start of the search, with a leading pipe character.

However, if you want your search macro to use a generating command, you should remove the leading pipe character from the macro definition, and instead place it at the start of the search string that you are inserting the search macro into, in front of the search macro reference.

For example, say you have a search macro named `mygeneratingmacro` that has the following definition:

```
tstats latest(_time) as latest where index!=filemon by index host
source sourcetype
```

The definition of `mygeneratingmacro` begins with the generating command `tstats`. Instead of preceding `tstats` with a pipe character in the macro definition, you put the pipe character in the search string, ahead of the search macro reference, like this:

```
| `mygeneratingmacro`
```

Eval expressions in macro definitions

To create macro definitions that are `eval` command expressions, select **Use eval-based expression?**. This setting specifies that the search macro definition is an eval expression that returns a string. This string is what the macro ultimately expands to.

Validate search macro arguments

When you define a search macro that includes arguments that must be entered by the user, you can define a **Validation expression** that determines whether the arguments supplied by the user are valid or not. You can also define a **Validation error message** that displays when search macro arguments fail validation.

The validation expression must be an `eval` expression that evaluates to a boolean or a string. If the validation expression is boolean, validation succeeds when the validation expression returns "true". If it returns "false" or is null, validation fails.

If the validation expression is not boolean, validation succeeds when the validation expression returns null. If it returns a string, validation fails.

Check search and scheduler activity in Splunk Light

You can view the status of search and scheduler activity of your Splunk Light instance using the System Activity dashboard. This dashboard displays information about search activity by user or type and scheduled report activity, which includes information about reports being run, counts of scheduler executions, and skipped reports.

In the sidebar menu, go to **Activity > System activity**. The System activity page displays the following panels:

- The **Search Activity** panel displays information about how users are running their searches, including search activity and run time information. The panels are filtered by users (admin or user reports) or types (ad hoc, other, scheduled, and summarization). See Search activity dashboards in the Splunk Enterprise *Monitoring Splunk Enterprise* manual.

- The **Scheduler Activity** panel displays information about how search jobs (reports) are scheduled. View individual reports to see search information, count of scheduler executions over time, and select the group of report data to display. Skipped reports are listed in the count of skipped reports, the report name, and reason for the skip. See Scheduler activity in the Splunk Enterprise *Monitoring Splunk Enterprise* manual.

About alerting in Splunk Light

An alert is an action that triggers based on specified results of the search. When creating an alert, you specify a condition that triggers the alert and configure actions such as sending an email or running a script.

An alert executes its action only when it meets specified conditions. An alert to notify of failed log-ins each hour does not send an email if there are no failed log-ins for a specific hour. To avoid sending out alerts too frequently, you can specify a throttle condition.

Splunk Light lets you configure or enable different types of alerts, including schedule, real time, and platform alerts.

Scheduled alert

Use a scheduled alert to notify when a scheduled search returns results that meet a specific condition. A scheduled alert is useful when immediate response to the alert is not a priority.

Scheduled alert examples include:

- Trigger an alert that runs daily, notifying when the number of items sold that day is less than 500.
- Trigger an alert that runs hourly, notifying when the number of 404 errors in any hour exceeds 100.

Real Time alert

Per result alerting

Use a per result alert to notify when a real-time search returns a result that matches a condition. You can specify a throttle condition so the alert triggers only once for a specified time period.

Per result examples include the following:

- Trigger an alert for every failed login attempt.
- Trigger an alert when a "file system full" error occurs on any host. You can specify field values that suppresses hosts for which you do not want an alert notification.
- Trigger an alert when a CPU on a host sustains 100% utilization for an extended period of time.

Rolling-window alert

Use a rolling window alert to monitor results of a real-time search within a specified time interval, such as every 10 minutes or every four hours.

Rolling-window alert examples include:

- Trigger an alert when there are three consecutive failed logins for a user within a 10 minute period. You can set a throttle condition to suppress an alert to once an hour from any user.
- Trigger an alert when a host is unable to complete an hourly file transfer to another host. Set a throttle condition so the alert fires only once every hour for any specific host.

Platform alerts

Platform alerts are preconfigured alerts that you can optionally enable. After you enable a platform alert, the user interface displays a notification if the alarm triggers.

Enable platform alerts by selecting **System > Platform alerts**. You can optionally edit the platform alerts to set or modify an alert action, such as sending an email. View a list of triggered platform alerts in the Triggered alerts or Resource usage dashboards.

Platform alerts are disabled by default.

Platform alerts included with Splunk Light

Platform alerts that are included with Splunk Light are listed in the table. To start monitoring your deployment with platform alerts, enable the individual alerts.

Alert name	Description	For more information

DMC Alert - Expired and Soon To Expire Licenses	Triggers when you have a license that is expired or will expire within two weeks.	Click **Licensing** in the sidebar menu.
DMC Alert - Missing forwarders	Triggers when one or more forwarders are missing.	Click **Forwarder management** in the sidebar menu.
DMC Alert - Near-Critical Disk Usage	Triggers when you use 80% of your disk capacity.	Click the **Resource Usage** dashboard in the sidebar menu.
DMC Alert - Total License Usage Near Daily Quota	Triggers when you use 90% of your total daily license quota.	Click **Licensing** in the sidebar menu.

Use throttling to limit alerts

An alert can trigger frequently if the search returns many similar results within the scheduled period of the search. Throttling reduces the frequency that an alert notifies you.

To throttle alerts, you can configure the time period in which to suppress results and the field values that the search returns.

For example, assume that when a particular system error occurs, it typically occurs 20 or more times each minute. You can configure throttling so that when one alert of this type triggers, it suppresses all successive alerts of the same type for the next 10 minutes. After each successive 10 minute period passes, the alert can trigger again.

Building dashboards

Use dashboards in Splunk Light

Dashboards contain panels that display data visualizations such as charts, tables, event lists, and maps. Each dashboard panel uses a base search to provide results for the visualizations, or uses searches referenced from reports. When you run a search, you can save it as a report, and add it to a dashboard.

A form is a dashboard with user inputs to the search, such as a drop-down list, buttons, or a text box. A form has the same options for panels and visualizations that are available for dashboards.

You can build and edit dashboards using the Splunk Web dashboard editor, which is the user interface in Splunk Light, and edit dashboards using Simple XML source code.

Dashboard creation workflow

To create a dashboard or form, use the following workflow.

1. Add content. Create searches that power dashboards, save searches as reports, or create panels for reuse.
2. Design the user interface. Create and modify dashboards using panels, forms, and visualizations.
3. Add interactivity (Optional). Add interactivity to dashboards with forms.
4. Customize the dashboard. Add custom features to your dashboard.

Example dashboard

The following is an example of a dashboard in Splunk Light. Six panels with visualizations represent searches or reports that make up the dashboard.

Create dashboards in Splunk Light

There are several ways to create dashboards in Splunk Light.

- Create a dashboard from the Dashboards page, and then add panels or inputs to the dashboard.
- Use prebuilt panels to create a dashboard.
- Clone an existing dashboard.

Create a dashboard

Create a dashboard from the Dashboards page, and then add panels from searches, reports, or prebuilt panels.

1. In your Splunk Light instance, select **Dashboards** in the menu bar.
2. Click **Create New Dashboard.**
3. (Optional) Enter a **Title**.
4. Enter an **ID**.
5. (Optional) Enter a **Description**.
6. Click a **permission level**.
7. Click **Create Dashboard**.
8. On the Edit Dashboard page, add panels or inputs to your dashboard.
9. Click **Save**.
10. (Optional) To confirm that you have saved the dashboard, click **Dashboards** in the menu bar to see the dashboard listed on the Dashboards page.

Create a dashboard from a search

1. On the Search page, run a search.
2. Select **Save As > Dashboard Panel**.
3. Enter the information for the dashboard panel, such as if you are adding this panel to a new or existing dashboard, dashboard permissions, and panel title.
4. Click **Save**.
5. Click **View Dashboard**.
6. (Optional) Click **Edit** to add more panels and inputs to your dashboards.

Create a dashboard from a report

1. From the Reports page, select a report and click **Open**.
2. Click **Add to Dashboard**.
3. In **Save As Dashboard Panel**, enter the information for the dashboard panel, such as if you are adding this panel to a new or existing dashboard, dashboard permissions, and panel title.
4. Click **Save**.
5. (Optional) Click **View Dashboard**.
6. (Optional) Click **Edit** to add more panels and inputs to your dashboards.

Clone a dashboard to create a copy of a dashboard or panel

Create a copy of a dashboard or panel. The panel appears on your dashboard with the same editing permissions as the original panel.

1. On the Dashboards page, select the dashboard you want to clone.
2. In the table view select the Actions menu and select **Clone**, or in the tile view select the gear icon menu and select **Clone**.
3. (Optional) Enter a **Title**.
4. Enter an **ID**.

5. (Optional) Enter a **New Description**.
6. Select **permissions**.
7. Click **Clone Dashboard**.

Use dashboard panels in Splunk Light

Dashboard panels are containers in a dashboard that hold one or more visualizations of your search or report content. The panel visualizations display the data as graphs, tables, or charts, and the panels are arranged in rows on the dashboard. A dashboard panel typically contains one or more searches that drive the data that is displayed in the panel. The search data can be from different sources, such as an inline search that you create and edit using the Panel Editor, or user inputs that modify the search results.

There are different types of panels that you can use in your dashboard, and depending on the panel, you can edit the search and visualization for the panel. Panel types include:

- **Inline panel**: An inline panel contains one or more inline searches to drive the data that appears in a visualization. You can create an inline panel in three ways:
    - Saving a search as a dashboard panel.
    - Creating a dashboard panel that is based on an existing report.
    - Adding a panel to a dashboard and choosing to configure it as an inline panel.
- **Panel from a report**: A panel created from a report is based on both the search and visualization from a report.
- **Prebuilt panel**: A prebuilt panel can be shared among various dashboards. Some add-ons include a set of prebuilt panels that you can add to your dashboard.

The following are different ways to create and add panels to your dashboard.

Add a panel to your dashboard

1. From a dashboard, select **Edit**.
2. Select **Add Panel**.
3. Expand one of the panel categories:
    1. **New**
    2. **New from Report**
    3. **Clone from Dashboard**

4. **Add Prebuilt Panel**
5. (Optional) To search for specific panels, enter text in the **Add Panel > find...** text box.

4. Select a panel and preview the selection.
5. Click **Add to Dashboard**.

Create an inline panel

1. From a dashboard, select **Edit**
2. Select **Add Panel**.
3. Expand the panel category **New** and select a visualization for the data.
4. (Optional) Enter a title for the panel.
5. Enter a search string that returns the data to display in the panel.
6. (Optional) Select **Run Search** to preview the search results.
7. Select a time range for the search and click **Add to Dashboard**.

Create a panel from a search

1. On the Search page, perform a new search.
2. Select **Save As > Dashboard Panel**.
3. Enter the information for the new dashboard panel, such as if you are adding this panel to a new dashboard or an existing dashboard.
4. Click **Save**.
5. Click **View Dashboard**.

Create a panel from a report

1. From a dashboard, select **Edit**.
2. Select **Add Panel**.
3. Expand the panel category **New from Report** to view available reports.
4. (Optional) Use the **find...** option to search for specific reports.
5. Select a report to view a preview of the report.
6. Click **Add to Dashboard**.

Create a prebuilt panel

1. From a dashboard, select **Edit**.
2. Select **Add Panel**.
3. Expand the panel category **Add Prebuilt Panel** to view available panels.
4. Click **Add to Dashboard**.

Clone a panel

1. From a dashboard, select **Edit**.
2. Select **Add Panel**.
3. Expand the panel category **Clone from Dashboard** to view available reports.
4. (Optional) Use the **find...** option to search for specific panels.
5. Select and expand a dashboard. Select a panel to view a preview of the panel.
6. Click **Add to Dashboard**.

Delete a panel

1. From a dashboard, select **Edit**.
2. On the panel you want to delete, click the **X** at the top right of the panel.
3. Click **Delete** to confirm you want to delete the panel.

Use visualizations in Splunk Light

When you create a dashboard panel, you select how the panel displays the results of a search or report with a visualization. Visualizations are graphical representations of your data, such as a graph, table, or chart. You can change your visualization selection with the Dashboard Panel Editor.

For information about visualizations types, see the Visualization Reference in the Splunk Enterprise *Dashboards and Visualizations* manual.

Add a visualization to a search and save as a dashboard panel

When you run a search, the visualization tab on the Search page lists visualizations that represent your data based upon your search results. Select a visualization and save the search and visualization as a dashboard panel.

1. After running a search, select the **Visualization** tab on the Search page.
2. Click the **Visualization Picker**, which is the menu that lists available visualizations.
3. Select a visualization. The Splunk Light software suggests Recommended visualizations that best represent your data, although you can select any visualization listed.
4. Select **Save As > Dashboard Panel** to save your search and visualization as a dashboard panel.

Change a visualization on a dashboard panel

Change a visualization on a dashboard panel by editing the panel.

1. On a dashboard, click **Edit**.
2. On the dashboard panel, click the **Visualization Picker** and select a visualization. The recommended visualizations best represent your data, although you can select any visualization listed.
3. Click **Save**.

Edit visualizations using the Dashboard Editor

Edit a visualization to configure its search, type, appearance, and behavior. You can edit visualizations from the Panel Editor or on the Search page. In either location, you can adjust the following visualization components.

Visualization components	Description
Search string	Use the dashboard search editor or the search bar to change the query driving the visualization.
Type	Use the Visualization Picker to select a visualization type. Ensure that the query generates results in the proper structure for the selected visualization.
Format and behavior	Use the Format menu to adjust appearance, drilldown, and other settings for the visualization's user interface.

Formatting and other options vary by visualization type. To compare visualizations and for details about writing queries for different visualizations, see the Visualization reference and Data structure requirements for visualizations in the Splunk Enterprise *Dashboards and Visualizations* manual.

View, export, inspect or refresh a visualization

In the Panel Editor you can access and view details of the search that drives the data in a panel. These features are available from icons that are visible when you mouse-over the bottom right of a panel.

Panel Editor components	Description
Open the Search	You can open a search for a visualization in Search. This is useful to inspect details of the search and perhaps test modifications to it before updating the search in the panel. In the Panel Editor, click the **Open in Search** icon. A new window opens with the search running in the Search.
Export	You can save the results of the search, or a limited set of results, to a file. In the Panel Editor, click the **Export** icon and specify the format, filename, and number of results to export. Click Export.
Inspect	Use the Search Job Inspector to view details of the search. In the Panel Editor, click the **Inspect** icon. The Search job inspector opens in a new window. In the Panel Editor, click the Inspect icon. The Search Job Inspector opens in a new window.
Refresh	You can refresh the results for a search in a panel. This is useful to verify that you are seeing the latest results. In the Panel Editor, click the **Refresh** icon.

Create forms in Splunk Light

A form is a dashboard that provides user inputs to the search. User inputs include components such as a list, a button, or a text box. A form has all the properties and behaviors of a dashboard.

The image shows a dropdown box, multiselect, and checkbox inputs added to a dashboard panel to make a form.

Convert a dashboard panel to a form

You can create and edit a form with the Dashboard Editor. To create a form, create a dashboard panel and then add a user input component to convert it to a form.

1. Open the dashboard panel that you want to convert for a form.
2. Select **Edit**.
3. From the **Add Input** menu, select one or more inputs.
4. For each input that you add, edit the input behavior.
5. Click the **pencil icon** to open the edit window.
6. Click **Apply** to save.
7. (Optional) Drag the inputs to rearrange them.
8. (Optional) Drag an input into a panel to specify an input applicable only to that panel.

For more information inputs and forms, see Create and edit forms in the Splunk Enterprise *Dashboards and Visualizations* manual.

Use drilldown for dashboard interactivity in Splunk Light

You might want to share additional data insights when users click on data points, table rows, or other visualization elements in a dashboard. Use drilldown to build this interactivity into your dashboards.

How drilldown works

Drilldown is a tool for configuring responses to user clicks on visualizations in a dashboard or form. Drilldown behavior is configured within individual visualizations. You can have separate drilldown configurations for each visualization in a dashboard. Depending on the visualization type, you can also enable drilldown on specific elements in a visualization, such as a table row or cell.

Drilldown actions

The drilldown actions that you configure happen when a user clicks the visualization element where the drilldown is enabled.

Link to a target
Drilldown actions can link a source dashboard or form to an external target that opens on a user click. The target can be a secondary search, another dashboard or form, or a website.

Trigger interactive behavior in the current dashboard
Drilldown action scan also trigger contextual changes in the same dashboard or form. For example, you can show or hide content depending on a clicked value.

Using tokens to customize a drilldown

Tokens are like programming variables. A token name represents a value that can change, such as a user selection in a form input. You can use a token name to access the value that it represents. In drilldown, you can use tokens to capture contextual values from the current dashboard or values from clicked elements. You might also define custom tokens to help implement interactive behavior.

You can pass token values to a target search, dashboard, or URL by configuring a drilldown to set tokens in the target to the captured source values. Setting token values in this way lets you show customized content in the target.

You can also use token values to trigger interactive changes in the current dashboard, such as content display or more specific search results. Configure elements in the current dashboard to listen for and respond to these changes.

Tokens available in drilldown

Several predefined token types representing dashboard events are available within a drilldown context. You can use these tokens to access clicked fields,

search events, and other dynamic values.

See Token usage in dashboards in the Splunk Enterprise *Dashboards and Visualizations* manual for details on working with the following token types.

Form input change events

Form inputs use a token to represent the value that users select in the input. If your drilldown target is a form, you can pass a value from a source dashboard to the input token in the target form so that users see content customized for the selected value.

To determine the token name for a form input, check the Simple XML source code for that input.

Search events

Predefined tokens represent search progress and completion events. Include search event handlers inside the `<search>` element for a visualization to get search job or result properties. You can use tokens to pass these values to the `<drilldown>` element.

Tokens set on page load

You can use an `<init>` element to set token values when a dashboard loads in the browser. You can access token values from the `<init>` element in a `<drilldown>`.

Chart navigation and selection events

You can access token values representing user pan and zoom or selection events in some chart types. See Chart controls in the Splunk Enterprise *Dashboards and Visualizations* manual for more information on working with these tokens.

Predefined click event tokens

Some tokens that you can use for drilldown are predefined in Splunk software. You can use these tokens to capture user actions or other values from a dashboard. For example, you can use the predefined `$click.value2$` token to capture a clicked table cell value.

See Predefined drilldown tokens in the *Simple XML Reference* in the Splunk Enterprise *Dashboards and Visualizations* manual for a list of predefined tokens available for each visualization.

Custom tokens

In addition to predefined tokens, you can create custom tokens to help create dynamic or conditional display behavior. These tokens can represent other values that change, such as search results.

Choose a drilldown action

Choose a drilldown action depending on the type of interactive behavior that you want and the data insights that you are sharing with users.

Action	Type	Behavior and configuration
Link to a search	Link to a target	Open a search page in the browser. A secondary search generates automatically to show results for the clicked value. You can also create a custom search.
Link to a different dashboard or form	Link to a target	Open a target dashboard or form in the browser. Use tokens to pass values to the target and show content customized to the clicked value or other values from the source.
Link to a URL	Link to a target	Open an external website in the browser. Pass token values from the source to the URL as query string parameters.
Manage token values in the current dashboard or form	Trigger interactivity in the current dashboard	Set, unset, or filter token values when a user clicks on an element in a dashboard or form. Instead of linking to a different location, use token value changes to configure interactive behavior in the same dashboard. For example, you can use `depends` or `rejects` attributes in the dashboard to control panel show or hide behavior when a token is set.

Drilldown defaults and customization

Some drilldown components have default settings. Depending on the component, you can use the drilldown editor or Simple XML to customize them.

Drilldown component	Default configuration	Where to customize
Enabled?	If you are building a new visualization or dashboard, drilldown is disabled by default. If you are migrating existing dashboards to software version 6.6, your prior drilldown settings, including drilldown enablement by default, are retained.	Enable or disable drilldown using the drilldown editor or in Simple XML.
Element in the visualization where drilldown is enabled	Varies by visualization. For example, you can enable drilldown on table rows or on single table cells to capture more specific clicked values. Check the Simple XML reference in the Splunk Enterprise *Dashboards and Visualizations* manual for defaults and options.	Use Simple XML to adjust the drilldown location.
Browser tab where linked searches, dashboards, or URLs open	In the drilldown editor, the option to open in a new tab is selected by default. In Simple XML, drilldown opens in the same tab by default.	In the drilldown editor, you can opt out of opening the drilldown target in a new tab. In Simple XML, add the `target="blank"` attribute to a `<link>` to open the target in a new tab.

Default settings and source code synchronization

Drilldown is disabled by default in new dashboard content. To disable drilldown, an `<option name="drilldown">none</option>` Simple XML element is added to visualizations that you save to a dashboard.

To avoid synchronization issues, do not delete this `<option>` from your dashboard source code. You can use the drilldown editor to change drilldown configurations or edit the `<option="drilldown">` element without deleting it.

Access the drilldown editor

You can use the drilldown editor to enable or configure drilldown actions. Some advanced configurations, such as conditional linking, are available only in Simple XML.

Steps

1. In the dashboard where you want to configure drilldown, click **Edit**.
2. Find the panel where you are adding or updating drilldown. Click the additional options icon at the right. Select **Edit Drilldown**.
3. Use the editor to enable and configure drilldown actions.

For details on configuring specific drilldown actions in the drilldown editor and Simple XML, see the options and linked topics in Choose a drilldown action.

Use trellis layout to split visualizations in Splunk Light

Trellis layout lets you split search results by fields or aggregations and visualize each field value separately.

This is a single value visualization with trellis layout applied. It splits customer purchase results by product category values. Users can see how the purchase metric varies for different product types.

Use cases

Use trellis layout to make value differences in a given data dimension more visible.

Highlight outlying values
Trellis layout can help to make outlying field values more noticeable. For example, your dashboard users might want to track status across multiple servers in a network. A single value visualization with trellis layout can show the status of multiple servers at once. Servers with unusual status values stand out.

Compare trends for a specific metric
You can split search results so that it is easier to compare different field values visually. For example, you can apply trellis layout to a bar chart showing recent customer activity for different product types. Splitting on the customer action field lets you scan variations in purchase frequency across different product types.

Monitor multiple resources with one search
Trellis layout can be helpful if you want to monitor multiple resources without creating and running multiple searches or generating multiple visualizations. You can use one search to generate metrics for each resource in a category or group and then split the visualization on the field that you are tracking.

Data formatting for trellis layout

Use trellis layout to split your search results on a field. You can also split the visualization on an aggregation if your search includes two or more aggregations, such as a `count` or `sum`.

Generating split fields
To use trellis layout, make sure that your search results include the field that you want to use for splitting the visualization. The split field is additional to any fields

that you might need to generate the visualization without trellis layout. For example, you can generate a single value visualization using the following search.

```
index=_internal | stats count
```

To use trellis layout, adjust the search to generate an additional field for splitting the visualization.

```
index=_internal | stats count by sourcetype
```

You can split the single value on the `sourcetype` field to show a `count` for each sourcetype in your search results.

Use additional fields to add insight
Depending on your use case, you can generate multiple result fields to add further data dimensions to each visualization segment.

As an example, you can aggregate recent retail website data by customer action and product type. With these fields in your search results, you can use one of them to split the visualization. Users can use the split visualizations to compare customer actions across product types or see how product types relate to customer actions.

For more information on creating searches, see Statistical and charting functions in the Splunk Enterprise *Search Reference*.

Enable and configure trellis layout

Trellis layout lets you split on available result fields or aggregations. When enabling trellis layout, consider the comparisons or trends that you want to provide at a glance. Make sure that your search results include the fields or aggregations that represent these values.

Access the trellis menu from a visualization

If you are building a visualization on the **Search** page, you can access the Trellis configuration menu on the **Visualization** tab.

Trellis layout is not available for table visualizations or cluster maps.

Access the trellis menu from a dashboard

1. From a dashboard, click **Edit** to open the dashboard editor.
2. Find the panel where you want to apply trellis layout.
3. Click the "More actions" icon and select Trellis.

Configure trellis layout

When you enable trellis layout, you can use the "Split by" list to select a split field or aggregation.

Select a split field or aggregation
When you split the visualization by a field or aggregation, a separate visualization segment appears for each value in the selected field.

Result fields generated with the `eval` command appear in the aggregations list.

If you do not see the split field or aggregation that you want to use in this list, adjust the search to make sure that it generates the field in your search results. You might need to adjust your search to return additional fields that are not necessary for generating the visualization without trellis layout.

Adjust segment size
Select one of the segment size options. Segment size affects panel data density. Panels can show more small sized segments at once. Larger segments can help

users make more detailed visual comparisons depending on the number of segments.

Small segments

Large segments

Formatting and appearance

Use the **Format** menu or Simple XML to configure visualization appearance. Format a visualization with trellis layout in the same way that you format a visualization without trellis layout. Each segment gets the format configurations that you apply.

Trellis layout and dashboard display

Segment density

The number of segments that trellis layout generates varies according to the number of split field or aggregation values in your search results. Dashboard panels might include a scroll bar if there are too many visualization segments to show at once.

Use the **Trellis** menu to adjust the segment size and show more segments in the panel. You can also use the dashboard editor to drag the panel size or change the panel `height` option in Simple XML.

To change the order in which segments appear, adjust the search to sort or change search result order.

Panel and row best practice

Separate panels using trellis layout into their own dashboard rows. Displaying additional content in the same row can constrain trellis layout content and make the dashboard difficult to scan.

Avoid	Best practice
Additional panels in the same row constrain display.	Put the panel with trellis layout in its own row.

Drilldown in trellis layout

Use the drilldown editor or Simple XML to enable and configure drilldown. After you apply Trellis layout to a visualization, drilldown is available in each visualization segment.

Drilldown options

Typical drilldown actions, such as linking to a search or an external URL, are available for visualizations using Trellis layout. Depending on the behavior that you want, you can configure drilldown to capture and use details from the element and the visualization segment that a user clicks.

Example

This drilldown links to a search. By default, the secondary search modifies the original search to include field values from the clicked segment.

For example, trellis layout splits a retail activity visualization by customer action. if a user clicks the "ARCADE" category column in the "purchase" customer action segment, a secondary search using these field values opens.

Clicked visualization segment and column

Search generating the visualization

```
...| stats count by action, categoryId | rename categoryId as
"category"
```

Drilldown search

```
...| action=purchase | rename categoryId as "category" | search
category=ARCADE
```

Predefined tokens for trellis split fields

If your trellis layout splits on a search result field, you can use the `trellis.name` and `trellis.value` predefined tokens to access the split field name and value from a clicked visualization segment.

You can pass these values to a drilldown target, such as a form or external URL. This example drilldown links to an external retail website, using the `trellis.value` token to pass in the product field value from the clicked segment.

```
<drilldown>
<link>
  http://buttercupgames.com?product=$trellis.value$
</link>
</drilldown>
```

Aggregations are not available in predefined tokens.

Limitations

- Fields generated with the `eval` command appear as aggregations in the trellis layout configuration menu.
- Trellis layout is not available for table visualizations or cluster maps.
- A predefined token is not available for aggregations used for splitting a visualization.
- Visualizations using trellis layout do not render in dashboard PDFs.

Configure trellis layout in Simple XML

Use the following Simple XML options to configure trellis layout.

Property	Type	Description
`trellis.enabled`	Boolean	Enable or disable trellis layout. Defaults to `false`
`trellis.size`	String	Configure the visualization segment size. Segment size affects panel display density for the split visualization. Defaults to `Medium`.
`trellis.splitBy`	Field name	Indicate the field to use for splitting the visualization. Segments appear for each value in this field.

Example

Research sales trends

An analyst for an online retailer researches customer actions by product category. They use the following search to find recent customer `action` events by product `category`.

```
source=recent_sales_data action != NULL
| rename categoryId as "category"
|  chart count by category, action
```

The search generates the following column chart, showing customer actions across all product categories.

The analyst can use trellis layout to split the visualization into separate column charts for each customer action category. Trellis layout lets the analyst compare trends in the product types associated with each action.

Edit dashboards in Splunk Light

When you edit a dashboard, you can edit the panels, title, description, permissions, or rearrange the panels.

Edit a dashboard

You can access a dashboard to edit from the Dashboards page.

1. On the Dashboard page, click the gear icon of the dashboard you want to edit.
2. Click the area of the dashboard you want to edit.
3. Make changes.
4. Click Save.

Edit the XML of a dashboard

You can edit a dashboard by accessing the simple XML code of the dashboard.

1. In the dashboard you want to edit, click **Edit**.
2. On the Edit Dashboard page, click **Source**.
3. Make changes to the XML code.
4. Click **Save**.

For more information about using simple XML in Splunk Light, see Simple XML Reference in the *Splunk Enterprise Dashboards and Visualizations* manual.

Edit a dashboard panel

The tools available to edit a panel depend on the base search that powers the panel. The Panel Editor displays an icon for each type of base search.

1. From a dashboard, select **Edit**.
2. Each panel displays editing icons for modifying the contents of the panel. The options available to you depend on the type of base search.

Action	Description
Gear icon	You can edit the panel by converting to a prebuilt panel.
Inline search	You can edit an inline search, including the title of the panel, the search, convert it to a report, or delete the panel. The options available to you depend on the type of base search.
Search from report	You can view or edit a report, including open the search in Search, clone to an inline search, select a different report for the panel, select the visualization specified in the report for this panel, select permissions, and more. The options available to you depend on the type of base search.
Panel visualization	Select a visualization to represent the data of search or report. Recommended visualizations are given that will best represent your data, or you can select any of the visualizations listed.
Panel style	Select the format that you want to display.

Edit a panel search

Update the search driving a particular dashboard panel.

When you are working with inline searches, the dashboard search bar has syntax highlighting and auto-complete features that can help you build a search string. To learn more, see Help reading searches in the *Getting Started Manual*.

Search editing options

All search types	Reports	Inline searches
• Edit the title. • Delete the search.	• View and edit the report in a new window. • Open the report search in a new window. • Clone to an inline search. • Select a different report for the panel. • Select the visualization specified in the report for this panel. • Specify an automatic refresh interval delay and indicator option.	• Edit the search, specifying a new inline search. • Convert the inline search to a report. • Specify an automatic refresh interval delay and indicator option.

Steps

1. From the **Dashboards** listing page, open the dashboard that you want to edit.
2. Click **Edit** to open the dashboard editor.
   At the top right of each panel, editing icons appear. The first editing icon represents the search for the panel. The search icon varies to represent the type of search being used.
3. Select the search icon to view configuration options for the search.
4. Select the search configuration that you want to change. Depending on the option you select, additional configuration dialogs or windows might open.
5. After editing the search, click **Save** to save changes to the dashboard.

Rearrange dashboard panels

Drag and drop panels to rearrange their position on a dashboard.

1. From a dashboard, select **Edit**.
2. Click and hold the line above the panel name.
3. When the cursor changes to the drag and drop symbol, drag the panel to the new position on the dashboard.

Delete a dashboard

You can delete a dashboard using the Edit menu of a dashboard. Access the Edit menu directly from the dashboard or from the list of dashboards on the Dashboards page.

1. On the Dashboards page, select the dashboard you want to delete.
2. Click the gear icon and select **Delete**.
3. Confirm that you want to delete the dashboard, and click **Delete**.

Manage dashboard permissions in Splunk Light

This topic discusses managing permissions for creating, viewing, and editing dashboards and dashboard panels.

Manage dashboard permissions by role

Depending on your role, either user or admin, there are different options for managing dashboard permissions as follows.

User role options

If you have the `user` role and its default capabilities, you can do the following.

- Create dashboards that are private to you.
- Provide other users with read and write access to the dashboard.

Admin role options

If you have the `admin` role and its default capabilities, you can do the following.

- Create dashboards that are private or shared.
- Provide other users and roles with read and write access to the dashboard.

Specify permissions for a new dashboard

When you create a new dashboard, you can configure permissions. Choose one of the following options.

Private dashboard

- Only you have permission to view and edit the dashboard.
- The dashboard is not visible to other users.

Shared dashboard

- The dashboard is available to other users.
- Depending on their permissions, other users can edit the dashboard.

Permissions needed for editing a dashboard

Write permission is required for editing dashboard panels. By default, you have write permission for any dashboard that you create. However, you might have read-only access to other dashboards. Admins can change editing permissions.

Permissions needed to access dashboard panel searches

The search that drives a dashboard panel can run using the permissions of the user who created the search (the search owner), or a user who views the dashboard (a search user). Depending on the access that you want to provide, you can adjust the permissions context for the search in the Reports listing page.

1. Locate the search on the Reports page.
2. Click the **gear icon** on the report.
3. Select **Edit Permissions** to change whether the search runs with the owner or user context.

Edit dashboard permissions

After creating a dashboard, you can change the permissions.

1. From the Dashboards page, select the dashboard for which you want to edit permissions.
2. Click the **gear icon** and select **Edit Permissions**.
3. (Optional) Edit Global **read** and **write** permissions.

Generate PDFs and printing dashboards in Splunk Light

You can generate a PDF from a dashboard, or print a dashboard.

Generate a dashboard PDF

1. From the dashboard, select **Export > Export PDF**. The PDF appears in a browser window.
2. View, download, or print the PDF from the browser window.

Print a dashboard

1. From the dashboard, select **Export > Print**.
2. The default print driver for your browser opens with print settings, from which you can select to print the dashboard.

Datasets and Data Models

About datasets in Splunk Light

A **dataset** is a collection of data that you define and maintain for a specific business purpose. It is represented as a table, with fields for columns and field values for cells. You can view and manage datasets with the Datasets listing page.

The Splunk Datasets Add-on is installed by default in Splunk Light, and the Datasets listing page is available from the menu bar.

Dataset types

You can work with three dataset types. Two of these dataset types, lookups and data models, are existing knowledge objects that have been part of the Splunk platform for a long time. Table datasets, or tables, are a new dataset type that you can create and maintain.

Use the Datasets listing page to view and manage your datasets. See View and manage datasets in Splunk Light in this manual.

Lookups

The Datasets listing page displays two categories of lookup datasets: lookup table files and lookup definitions. It lists lookup table files for .csv lookups and lookup definitions for .csv lookups and KV Store lookups. Other types of lookups, such as external lookups and geospatial lookups, are not listed as datasets.

You upload lookup table files and create file-based lookup definitions through the sidebar Lookups page. See Use lookups in Splunk Light in this manual.

Data model datasets

Data models are made up of one or more data model datasets. When a data model is composed of multiple datasets, those datasets are arranged hierarchically, with a root dataset at the top and child datasets beneath it. In data model dataset hierarchies, child datasets inherit fields from their parent dataset but can also have additional fields of their own.

You create and edit data model dataset definitions with the Data Model Editor. See About data models in Splunk Light in this manual.

Note: In previous versions of the Splunk platform, data model datasets were called data model objects.

Table datasets

Table datasets, or tables, are focused, curated collections of event data that you design for a specific business purpose. You can derive their initial data from a simple search, a combination of indexes and source types, or an existing dataset of any type. For example, you could create a new table dataset whose initial data comes from a specific data model dataset. After this new dataset is created, you can modify it by updating field names, adding fields, and more.

You define and maintain datasets with the Table Editor, which translates sophisticated search commands into simple UI editor interactions. It is easy to use, even if you have minimal knowledge of Splunk search processing language (SPL).

Datasets gives you the ability to create and edit table datasets. See About table datasets in Splunk Light in this manual.

View and manage datasets in Splunk Light

The Datasets listing page gives you a high-level view of all of the datasets that you have access to in your Splunk implementation. You can see what types of datasets you have, who owns them, and how they're shared.

This topic covers the default capabilities of the Datasets listing page. By default you can use it to:

- Access dataset Explorer views
- Edit datasets in their native editing environments
- Visualize datasets in Pivot
- Investigate datasets in Search
- Manage dataset permissions
- Delete lookup table files and lookup definitions

View dataset detail information

You can expand a dataset row to see detail information about that dataset, such as the fields contained in the dataset or the date the dataset was last modified.

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Find a dataset you want to explore.
3. Click the **>** symbol to expand the row of the dataset and reveal dataset detail information. You can review a list of the fields contained in the dataset without going to the viewing page.
4. (Optional) Click **Edit** to change the dataset permissions.

See Manage dataset permissions in this topic.

Access the Explorer view of a dataset

Use the Explorer view to see the dataset structure and determine whether it contains information you want to work with. You can also use this view to:

- See what datasets contain for specific time ranges.
- Export dataset contents to a CSV file.
- Save datasets as scheduled reports.
- Carry out other functions that are present in the Datasets listing page, such as managing dataset acceleration, setting dataset permissions, and opening datasets in Search and Pivot.

The Explorer view presents datasets as tables, with fields as columns and values in cells. Data model datasets and table datasets display events as rows. Lookups display their records as rows.

Prerequisites

Learn what you can do with your datasets in the Explorer view. See Explore a dataset in Splunk Light in this manual.

Steps

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Find a dataset you want to explore.
3. (Optional) Click the **>** symbol to expand the row of the dataset and reveal dataset detail information. You can review a list of the fields contained in the dataset without going to the viewing page.
4. Click the dataset name to open it in the Explorer view.

Visualize a dataset with Pivot

Use **Pivot** to create a visualization based on your dataset. When you are satisfied with what you have created, you can save the visualization as a report or dashboard panel. You do not need to know how to use the Splunk Search Processing Language (SPL) to use it.

You can open all dataset types in Pivot.

Prerequisites

See Introduction to Pivot in the Splunk Enterprise *Pivot Manual*.

Steps

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Find a dataset that you want to work with in Pivot.
3. Select Explore > Visualize with Pivot.

You can also access Pivot from the Explorer view. See Explore a dataset in Splunk Light in this manual.

Investigate a dataset in Search

You can investigate the contents of a dataset in the Search view. When you click **Investigate in Search** for a dataset, the Search view opens with a search string that uses the `from` command to reference that dataset. The results returned by this search provide a view into the contents of the dataset.

Apply additional **SPL** to the search string if you want, or leave it as is. At any time, you can save the search as a report, alert, or dashboard panel.

The saved search is considered to be **extended** from the original dataset. An extended dataset is distinct from, but dependent to, the parent dataset that it was extended from. If you change a parent dataset, that change propagates down to all datasets that you have extended from that parent dataset.

Prerequisites

- Get started with Search in the Splunk Enterprise *Search Manual*
- Extend datasets in the Splunk Enterprise *Knowledge Manager Manual*.

Steps

1. In the menu bar, click **Datasets** to open the Datasets listing page..
2. Locate a dataset that you want to explore in Search.
3. Select **Explore > Investigate in Search**.
   The search returns results in event list format by default. Switch the results format from **List** to **Table** to see the table view of the dataset.
4. (Optional) Update the search string with additional SPL. Do not remove the `from` reference.
5. (Optional) Click **Save as** to save your search, and select either **Report**, **Dashboard Panel**, or **Alert**.
6. (Optional) Click **New Table** to create a new table dataset based on the search string.
   This option is only available if you use Splunk Cloud or Splunk Light, or if you use Splunk Enterprise and have installed the Splunk Datasets Add-on.

Edit datasets

From the Datasets listing page you can access the editing options for various dataset types.

Edit lookup table files

Prerequisites

See Use field lookups to add information to your events in the Splunk Enterprise *Knowledge Manager Manual* to learn about managing lookup table files.

Steps

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Locate a lookup table file that you want to edit.
3. (Optional) Click the name of the lookup table file to view it in the dataset viewing page.
4. Select **Manage > Edit Lookup Table File**. This opens a Settings page that lists the lookup table files that are uploaded to your Splunk platform implementation.

5. (Optional) Update the permissions of the file.
6. (Optional) Move lookup table files to a different app context.
7. (Optional) Delete lookup table files.
8. (Optional) Upload new .csv lookup table files.

Edit lookup definitions

The Datasets listing page lists all of the .csv lookup definitions and KV Store lookup definitions in your Splunk implementation.

Prerequisites

See Use field lookups to add information to your events in the Splunk Enterprise *Knowledge Manager Manual* to learn about editing lookup definitions.

Steps

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Locate a lookup definition that you want to edit.
3. (Optional) Click the name of the lookup definition to view it in the dataset viewing page.
4. Select **Manage > Edit Lookup Definition**. This opens the Settings page for the lookup definition.
5. (Optional) Update the lookup definition. You can change the fields it matches, configure it to be time-based, and set up advanced field-matching rules.

Data model datasets

Go to the Data Model Editor to edit a data model dataset.

Prerequisites

See Design data models in Splunk Light in this manual.

Steps

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Locate a data model dataset that you want to edit.
3. (Optional) Click the name data model dataset to view it in the dataset viewing page.
4. Select **Manage > Edit Data Model**. This opens the data model dataset in the Data Model Editor.

5. (Optional) Use the Data Model Editor to update the constraints and fields for the data model dataset.

Manage dataset permissions

Change dataset permissions to widen or restrict their availability to other users. You can set up read and write access by role, and you can determine whether datasets are globally accesible, restricted to a particular app context, or private to a single user.

For an overview of how the Splunk platform permissions features work, see Manage knowledge object permissions in the Splunk Enterprise *Knowledge Manager Manual*.

Lookups and table datasets

You can set permissions for lookups and table datasets directly through the Datasets listing page.

When you set permissions for a lookup table file, its permissions should be scoped in a way that makes it usable by any lookup definitions that you associate with it. For example, if a lookup table file has permissions that are scoped to a specific app, this is fine, as long as any lookup definitions that use that lookup table file also have permissions scoped to that app. If you want to associate that lookup table file with lookup definitions that are scoped to a different app, or that have global permissions, you will want to ensure the lookup table file has permissions scoped to "all apps." If you do not do this, the lookup may not work for some users.

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Locate a lookup or table dataset for which you need to view or update permissions.
3. Select **Manage > Edit Permissions**.
4. (Optional) Change the audience that you want the dataset to **Display for**.

Option	Definition
Owner	The lookup or table dataset is only available to the person who created it.
App	The lookup or table dataset has its permissions scoped to a single app. Users in other app contexts will be unable to see it or use it.
All apps	

	The lookup or table dataset has its permissions scoped to all apps. This means it has global availability to all users of your Splunk implementation.

5. (Optional) If the dataset displays for an **App** or **All apps**, you can change the **Read** and **Write** settings that determine which roles can view or edit the dataset.
6. Click **Save** to save your changes, or **Cancel** if you decide not to make any changes.

Data model datasets

Permissions for data model datasets are set at the data model level. All datasets within a data model have the same permissions settings. There are two ways to set permissions for data models:

- Through the Data Model Editor
- Through the Data Models listing page available from the sidebar menu

Prerequisites

Learn about setting data model permissions in About data model permissions in this manual.

Steps for setting data model dataset permissions with the Data Model Editor

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Identify the data model dataset for which you want to update permissions.
3. Select **Manage > Edit Data Model**.
4. Select **Edit > Edit Permissions** to set permissions for the data model that your selected data model dataset belongs to.
5. (Optional) Change the audience that you want the data model to **Display For**. It can display for users of a specific **App** or users of **All apps**.
6. (Optional) If the data model displays for an **App** or **All apps**, you can change the **Read** and **Write** settings that determine which roles can view or edit the data model.
7. Click **Save** or **Cancel**.

Steps for setting data model dataset permissions with the Data Models listing page in the sidebar menu

1. In the sidebar menu, select **Data models**.
2. Identify the data model for which you would like to change permissions.

3. Select **Edit > Edit Permissions** to set permissions for the data model that your selected data model dataset belongs to.
4. (Optional) Change the audience that you want the data model to **Display For**. It can display for users of a specific **App** or users of **All apps**.
5. (Optional) If the data model displays for an **App** or **All apps**, you can change the **Read** and **Write** settings that determine which roles can view or edit the data model.
6. Click **Save** or **Cancel**.

Delete datasets

You can delete lookups and table datasets through the Datasets listing page. You can delete a data model dataset from the Data Model editor.

Lookups and table datasets

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Locate a lookup or table dataset that you want to delete.
3. Select **Manage > Delete**.
4. On the **Delete Dataset** dialog, click **Delete** again to verify that you want to delete the dataset.

You can also delete lookups and tables from their dataset viewing pages.

Data model datasets

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Locate a data model dataset that you want to delete.
3. Select **Manage > Edit Dataset**.
4. In the Data Model Editor, click **Delete** for the data model dataset.

Explore a dataset in Splunk Light

The Explorer view lets you look at the contents of any **dataset** on the Datasets listing page. It gives you an easy way to inspect the contents of any dataset listed on the page, including data model datasets and lookups.

The Explorer view provides a variety of dataset exploration and management capabilities:

- Use two views for dataset exploration:

    - ♦ **Preview Rows**, which renders the dataset in a standard table format.
    - ♦ **Summarize Fields**, which displays statistical information for each of the fields in your table and their values.
- Set the dataset time range.
- Manage the dataset search job.
- Export the contents of the dataset for a given time range.
- Extend your dataset as a scheduled report.

You can also perform the same dataset management actions that you have access to through the Datasets listings page. See View and manage datasets in Splunk Light and View and manage table datasets in Splunk Light in this manual.

Open the Explorer view for a dataset

Use the Datasets listing page to access the Explorer view for a selected dataset.

1. In the menu bar, click **Datasets** to open the Datasets listing page.
2. Find a dataset you want to explore.
3. Click the dataset name to open it in the Explorer view.

Ways to view datasets

The Explorer view gives you two ways to view your dataset. You can **Preview Rows** or you can **Summarize Fields**.

Preview Rows

Preview Rows is the default for the Explorer view. It displays your table dataset as a table, with fields as columns, values in cells, and sample events in rows.

Summarize Fields

Click **Summarize Fields** to see analytical details about the fields in the table. You can see top value distributions, null value percentages, numeric value statistics, and more.

Set the dataset time range

The time range picker enables you to restrict the data your dataset view contains to events that fall within specific ranges of time. It applies to search-based dataset types like data model datasets and table datasets.

Lookup table files and lookup definitions usually get their data from static CSV files and KV store collections, so the time range picker does not apply to them. They display the same rows of data no matter what time range you select.

The time range picker is set to **Last 24 hours** by default. If your dataset has no results from the last 24 hours, this view will appear to be empty when you first enter it. To fix this, adjust the time range picker to a range where events are present.

The time range picker gives you a variety of time range definition options. You can choose a pre-set time range, or you can define a custom time range. For help with the time range picker, see Select time ranges to apply to your search in the Splunk Enterprise *Search Manual*.

Manage the dataset search job

When you enter the Explorer view, a search **job** runs over the time range set by the time range picker. Its results populate the dataset view.

After you launch a dataset search, a set of controls to the top right of the dataset view let you manage the search job in different ways without leaving the Explorer view. In the middle of this control set you can find pause/start and stop icons that you can use while the dataset search is in progress.

Use the Job menu actions

The **Job** menu helps you access the dataset search job and access information about it.

1. After your search is running, paused, or finalized, click **Job**.

2. Choose from the list options.

Action	Description
Edit Job Settings...	Opens the Job Settings dialog, where you can change the read permissions for the job, extend the job lifespan, and get a URL for the job. You can use the URL to share the job with others or to add a bookmark to the job in your Web browser.
Send Job to Background	Runs the job on the background. Use this option if the search job is slow to complete. This enables you to work on other activities, including running a new search job.
Inspect Job	Opens the Search Job Inspector window and displays information and metrics about the search job. You can select this action while the search is running or after the search completes. For more information, see View search job properties in the Splunk Enterprise *Search Manual*.

For more information, see About jobs and job management in the Splunk Enterprise *Search Manual*.

Share a job

Click the **Share** icon to share the job. When you select this, the job's lifetime is extended to 7 days and read permissions are set to **Everyone**. For more information about jobs, see About jobs and job management in the Splunk Enterprise *Search Manual*.

Export the job results

Click the **Export** icon to export the results of a dataset search job. You can select to output to CSV, XML, or JSON and specify the number of results to export.

If this export method does not meet your needs, see Export search results in the Splunk Enterprise *Search Manual*.

Extend the dataset as a scheduled report

You can **extend** your dataset as a new **scheduled report**. The report uses a `from` in its base search to reference the dataset that you are viewing. This means that the report has a child/parent relationship with the dataset. Changes you make to the dataset in the future are passed down to the report. Changes you make to the report are not passed up to the dataset.

Select **Manage > Schedule Report** to extend the dataset as a scheduled report. This opens the Schedule Report dialog where you can create the report schedule and define actions that are triggered each time the report runs. For example, you can arrange to have the Splunk software add the report results to a specific CSV file each time the report runs. You can also define scheduled report actions that send the results to a set of people in email format or that run scripts.

For more information about using this dialog to create the report schedule and define actions for it, see Schedule reports in the Splunk Enterprise *Reporting Manual*.

Manage your dataset

The Explorer view gives you the same dataset management capabilities as the Dataset listing page. If you review the contents of a dataset and decide you want to work with it, you do not need to return to the Dataset listing page. You can apply management actions to it from this view.

The Explorer view includes management actions for all dataset types:

- Visualize a dataset with Pivot
- Investigate a dataset with Search
- Edit a dataset
- Update dataset permissions
- Delete a dataset
- Extend a dataset as a new table dataset
- Clone a table dataset

- Edit table dataset descriptions
- Accelerate table datasets

See View and manage datasets in Splunk Light and View and manage table datasets in Splunk Light in this manual for details on these tasks.

About table datasets in Splunk Light

Table datasets, or tables, are a type of **dataset** that you can create, shape, and curate for a specific purpose. You begin by defining the initial data for the table, such as an index, source type, search string, or existing dataset. Then you edit and refine that table in the Table Editor until it fits the precise shape that you and your users require for later analysis and reporting work.

After you create your table, you can continue to iterate on it over time, or you can share it with others so they can refine it further. You can also use techniques like dataset cloning and dataset extension to create new datasets that are based on datasets you have already created.

You can manage table datasets alongside other dataset types that are available to all users, like data model datasets and lookups. All of these dataset types appear in the Datasets listing page.

Default datasets functionality for users

This table explains what all users can do with datasets by default.

Dataset activity	Why this is useful
View dataset contents	Check a dataset to determine whether it contains fields and values that you want to work with. For example, you can view lookup table files directly instead of searching their contents in the Search view.
Open datasets in Pivot	With Pivot you can design a visualization-rich analytical report or dashboard panel that is based on your dataset. Pivot can also help you discover data trends and field correlations within a dataset.
Extend datasets in Search	Extend your dataset as a search, modify its search string as necessary, and save the search as a report, alert, or dashboard panel.

Next steps

- Read an overview of the of the dataset types that you can explore, manage, and create. See About datasets in Splunk Light in this manual.
- Learn about the Datasets listing page. See View and manage datasets in Splunk Light in this manual.
- Learn about dataset extension. See Dataset extension in the Splunk Enterprise *Knowledge Manager Manual*.

Additional dataset features

Additional dataset features are listed in the table.

Dataset activity	Why this is useful
Use the Table Editor to create tables	You can design sophisticated and tightly-focused collections of event data that fit specific business needs, even if you have minimal SPL skills.
Share and refine tables over time	After you create a table you can give other users read or write access to it so they can curate and refine it. For example, you can create a simple dataset, and then pass it to another user with deep knowledge of the source data to shape it for a specific use. You can also extend your dataset and let other people refine the extension without affecting the original dataset.
View field analytics	The Table Editor offers a Summarize Fields view that provides analytical information about the fields in your dataset. You can use this knowledge to determine what changes you need to make to the dataset to focus it to your needs.
Extend any dataset as a table	Dataset extension enables you to create tables that use the definition of any dataset type as their foundation. This enables you to create tables that are based on lookups and data model datasets and then modify those tables to fit your specific use cases.
Clone tables	You can make exact copies of table datasets and save the copy with a new name. Only table datasets can be cloned.
Accelerate tables	You can accelerate table datasets in a manner similar to report and data model acceleration. This can be helpful if you are using a very large dataset as the basis for a pivot report or dashboard panel. Once accelerated, the table returns results faster than it would otherwise.

Next steps

- Define initial data for a new table dataset. See Define initial data for a new table dataset in the Splunk Enterprise *Knowledge Manager Manual*.
- Edit a table dataset. See Define initial data for a new table dataset in the Splunk Enterprise *Knowledge Manager Manual*.
- Accelerate a table dataset. See Accelerate tables in the Splunk Enterprise *Knowledge Manager Manual*.

About data models in Splunk Light

Data models drive the Pivot tool. They enable users of Pivot to create compelling reports and dashboards without designing the searches that generate them. Data models can have other uses, especially for Splunk app developers.

Splunk knowledge managers design and maintain data models. These knowledge managers understand the format and semantics of their indexed data and are familiar with the Splunk search language. In building a typical data model, knowledge managers use knowledge object types such as **lookups**, **transactions**, search-time **field extractions**, and **calculated fields**.

What is a data model?

A data model is a type of **knowledge object** that makes raw data easier to use by adding an information structure. Each data model represents a category of event data, such as Web Intelligence or Email Logs. Data models are composed of **datasets**, which are a collection of fields and constraints.

Data models provide the domain knowledge necessary to build a variety of specialized searches of those datasets. The Splunk platform uses data model searches to generate reports for Pivot users and to accelerate key data in searches and dashboards. The Splunk Common Information Model Add-on, which includes a set of data models for common event types, provides a common structure against which you can normalize your data at search time.

To create an effective data model, you must understand your data sources and your data semantics. For example, if your dataset is based on the contents of a table-based data format, such as a .csv file, the resulting data model is flat, with a single top-level root dataset that encapsulates the fields represented by the columns of the table. The root dataset may have child datasets beneath it, but

these child datasets do not contain additional fields beyond the set of fields that the child datasets inherit from the root dataset.

If your data model is derived from a heterogeneous system log, you might have several root datasets (events, searches, and transactions). Each of these root datasets can be the first dataset in a hierarchy of datasets with nested parent and child relationships. Each child dataset in a dataset hierarchy can have new fields in addition to the fields they inherit from ancestor datasets.

Data model datasets can get their fields from custom **field extractions** that you have defined. Data model datasets can get additional fields at search time through regular-expression-based field extractions, **lookups**, and `eval` expressions.

The fields that data models use are divided into the categories described above (auto-extracted, eval expression, regular expression) and more (lookup, geo IP). See Dataset fields in this topic.

Data models are a category of **knowledge object** and are fully permissionable. A data model's permissions cover all of its data model datasets.

See View and manage data models in Splunk Light in this manual.

Data models generate searches

When you consider what data models are and how they work it can also be helpful to think of them as a collection of structured information that generates different kinds of searches. Each dataset within a data model can be used to generate a search that returns a particular dataset.

We go into more detail about this relationship between data models, data model datasets, and searches in the following subsections.

- **Dataset constraints** determine the first part of the search through:
  - Simple search filters (Root event datasets and all child datasets).
  - Complex search strings (Root search datasets).
  - `transaction` definitions (Root transaction datasets).
- When you select a dataset for Pivot, the unhidden fields you define for that dataset comprise the list of fields that you choose from in Pivot when you decide what you want to report on. The fields you select are added to the search that the dataset generates. The fields can include **calculated fields**, user-defined field extractions, and fields added to your data by lookups.

The last parts of the dataset-generated-search are determined by your Pivot Editor selections. They add transforming commands to the search that aggregate the results as a statistical table. This table is then used by Pivot as the basis for charts and other types of visualizations.

For more information about how you use the Pivot Editor to create pivot tables, charts, and visualizations that are based on data model datasets, see Introduction to Pivot in the Splunk Enterprise *Pivot Manual*.

Datasets

Data models are composed of one or more datasets. Here are some basic facts about data model datasets:

- **Each data model dataset corresponds to a set of data in an index.** You can apply data models to different indexes and get different datasets.
- **Datasets break down into four types.** These types are: *Event* datasets, *search* datasets, *transaction* datasets, and *child* datasets.
- **Datasets are hierarchical.** Datasets in data models can be arranged hierarchically in parent/child relationships. The top-level event, search, and transaction datasets in data models are collectively referred to as "root datasets."
- **Child datasets have inheritance.** Data model datasets are defined by characteristics that mostly break down into *constraints* and *fields*. Child datasets inherit constraints and fields from their parent datasets and have additional constraints and fields of their own.

We'll dive into more detail about these and other aspects of data model datasets in the following subsections.

- **Child datasets provide a way of filtering events from parent datasets** - Because a child dataset always provides an additional constraint on top of the constraints it has inherited from its parent dataset, the dataset it represents is always a *subset* of the dataset that its parent represents.

Root datasets and data model dataset types

The top-level datasets in data models are referred to as "root datasets." Data models can contain multiple root datasets of various types, and each of these root datasets can be a parent to more child datasets. This association of base and child datasets is a "dataset tree." The overall set of data represented by a dataset tree is selected first by its root dataset and then refined and extended by

its child datasets.

Root datasets can be defined by a search constraint, a search, or a transaction:

- **Root event datasets** are the most commonly-used type of root data model dataset. Each root event dataset broadly represents a type of event. For example, an *HTTP Access* root event dataset could correspond to access log events, while an *Error* event corresponds to events with error messages.
  Root event datasets are typically defined by a simple constraint. This constraint is what an experienced Splunk user might think of as the first portion of a search, before the pipe character, commands, and arguments are applied. For example, `status > 600` and `sourcetype=access_* OR sourcetype=iis*` are possible event dataset definitions.
  See Dataset Constraints in this topic.
- **Root search datasets** use an arbitrary Splunk search to define the dataset that it represents. If you want to define a base dataset that includes one or more fields that aggregate over the entire dataset, you might need to use a root search dataset that has transforming commands in its search. For example: a system security dataset that has various system intrusion events broken out by category over time.
- **Root transaction datasets** let you create data models that represent **transactions**: groups of related events that span time. Transaction dataset definitions utilize fields that have already been added to the model via event or search dataset, which means that you can't create data models that are composed *only* of transaction datasets and their child datasets. Before you create a transaction dataset you must already have some event or search dataset trees in your model.

Child datasets of all three root dataset types--event, transaction, and search--are defined with simple constraints that narrow down the set of data that they inherit from their ancestor datasets.

Dataset types and data model acceleration

You can optionally use **data model acceleration** to speed up generation of pivot tables and charts. There are restrictions to this functionality that can have some bearing on how you construct your data model, if you think your users would benefit from data model acceleration.

To accelerate a data model, it must contain at least one root event dataset, or one root search dataset that only uses streaming commands. Acceleration only affects these dataset types and datasets that are children of those root datasets.

You cannot accelerate root search datasets that use nonstreaming commands (including transforming commands), root transaction datasets, and children of those datasets. Data models can contain a mixture of accelerated and unacellerated datasets.

See View and manage data models in Splunk Light in this manual.

See Command types in the Splunk Enterprise *Search Reference* for more information about streaming commands and other command types.

Example of data model dataset hierarchies

The following example shows the first several datasets in a "Call Detail Records" data model. Four top-level root datasets are displayed: **All Calls**, **All Switch Records**, **Conversations**, and **Outgoing Calls**.

All Calls and **All Switch Records** are root event datasets that represent all of the calling records and all of the carrier switch records, respectively. Both of these root event datasets have child datasets that deal with subsets of the data owned by their parents. The **All Calls** root event dataset has child datasets that break down into different call classifications: Voice, SMS, Data, and Roaming. If you were a Pivot user who only wanted to report on aspects of cellphone data usage, you'd select the Data dataset. But if you wanted to create reports that compare the four call types, you'd choose the **All Calls** root event dataset instead.

Conversations and **Outgoing Calls** are root transaction datasets. They both represent transactions--groupings of related events that span a range of time. The "Conversations" dataset only contains call records of conversations between two or more people where the maximum pause between conversation call record events is less than two hours and the total length of the conversation is less than one day.

For details about defining different data model dataset types, see Design data models in Splunk Light in this manual.

Dataset constraints

All data model datasets are defined by sets of **constraints**. Dataset constraints filter out events that aren't relevant to the dataset.

- **For a root event dataset or a child dataset of any type**, the constraint looks like a simple search, without additional pipes and search commands. For example, the constraint for `HTTP Request`, one of the root event dataset of the Web Intelligence data model, is `sourcetype=access_*`.
- **For a root search dataset**, the constraint is the dataset search string.
- **For a root transaction dataset**, the constraint is the transaction definition. Transaction dataset definitions must identify *Group Dataset* (either one or more event dataset, a search dataset, or a transaction dataset) and one or more *Group By* fields. They can also optionally include **Max Pause** and **Max Span** values.

Constraints are inherited by child datasets. Constraint inheritance ensures that each child dataset represents a subset of the data represented by its parent datasets. Your Pivot users can then use these child datasets to design reports with datasets that already have extraneous data prefiltered out.

Say you have a data model called Buttercup Games. Its Successful Purchases dataset is a child of the root event dataset `HTTP Requests` and is designed to contain only those events that represent successful customer purchase actions.

Successful Purchases inherits constraints from HTTP Requests and another parent dataset named Purchases.

1. HTTP Requests starts by setting up a search that only finds webserver access events.

   ```
   sourcetype=access_*
   ```
2. The Purchases dataset further narrows the focus down to webserver access events that involve purchase actions.

   ```
   action=purchase
   ```
3. And finally, Successful Purchases adds a constraint that reduces the dataset event set to web access events that represent successful purchase events.

   ```
   status=200
   ```

   When all the constraints are added together, the base search for the Successful Purchases dataset looks like this:

   ```
   sourcetype=access_* action=purchase status=200
   ```

   A Pivot user might use this dataset for reporting if they know that they only want to report on successful purchase actions.

For details about datasets and dataset constraints, see the topic Design data models in Splunk Light in this manual.

Dataset fields

There are five categories of dataset fields:

- **Auto-extracted** - A field derived at **search time**. You can only add auto-extracted fields to root datasets. Child datasets can inherit them, but they cannot add new auto-extracted fields of their own. Auto-extracted fields can be:
  - Fields that are extracted automatically, like `uri` or `version`. This includes fields indexed through structured data inputs, such as fields extracted from the headers of indexed CSV files.
  - **Field extractions**, **lookups**, or **calculated fields** that you have defined in Settings or configured in `props.conf`.
  - Fields that you have manually added because they aren't currently in the dataset, but should be in the future. Can include fields that

are added to the dataset by generating commands such as `inputcsv` or `dbinspect`.

- **Eval Expression** - A field derived from an `eval` expression that you enter in the field definition. Eval expressions often involve one or more extracted fields.
- **Lookup** - A field that is added to the events in the dataset with the help of a **lookup** that you configure in the field definition. Lookups add fields from external data sources such as CSV files and scripts. When you define a lookup field you can use any lookup that you have defined and associate it with any other field that has already been associated with that same dataset.
- **Regular Expression** - This field type is extracted from the dataset event data using a regular expression that you provide in the field definition. A regular expression field definition can use a regular expression that extracts multiple fields; each field will appear in the dataset field list as a separate regular expression field.
- **Geo IP** - A specific type of **lookup** that adds geographical fields, such as latitude, longitude, country, and city to events in the dataset that have valid IP address fields. Useful for map-related visualizations.

See About datasets in Splunk Light in this manual.

Field categories

The Data Model Editor groups fields into three categories:

- **Inherited** - All datasets have at least a few inherited fields. Child fields inherit fields from their parent dataset, and these inherited fields always appear in the Inherited category. Root event, search, and transaction datasets also have default fields that are categorized as inherited.
- **Extracted** - Any auto-extracted field that you add to a dataset is listed in the "Extracted" field category.
- **Calculated** - The Splunk software derives calculated fields through a calculation, lookup definition, or field-matching regular expression. When you add Eval Expression, Regular Expression, Lookup, and Geo IP field types to a dataset, they all appear in this field category.

The Data Model Editor lets you arrange the order of calculated fields. This is useful when you have a set of fields that must be processed in a specific order. For example, you can define an Eval Expression that adds a set of fields to events within the dataset. Then you can create a Lookup with a definition that uses one of the fields calculated by the eval expression. The lookup uses this definition to add another set of fields to the same events.

Fields are inherited

All datasets have inherited fields.

A child dataset will automatically have all of the fields that belong to its parent. All of these inherited fields will appear in the child dataset's "Inherited" category, even if the fields were categorized otherwise in the parent dataset.

You can add additional fields to a child dataset. The Data Model Editor will categorize these datasets either as extracted fields or calculated fields depending on their field type.

You can design a relatively simple data model where all of the necessary fields for a dataset tree are defined in its root dataset, meaning that all of the child datasets in the tree have the exact same set of fields as that root dataset. In such a data model, the child datasets would be differentiated from the root dataset and from each other only by their constraints.

Root event, search, and transaction datasets also have inherited fields. These inherited fields are default fields that are extracted from from every event, such as `_time`, `host`, `source`, and `sourcetype`.

You cannot delete inherited fields, and you cannot edit their definitions. The only way to edit or remove an inherited field belonging to a child dataset is to delete or edit the field from the parent dataset it originates from as an extracted or calculated field. If the field originates in a root dataset as an inherited field, you won't be able to delete it or edit it.

You can hide fields from Pivot users as an alternative to field deletion.

You can also determine whether inherited fields are optional for a dataset or required.

Fields serve several purposes

Their most obvious function is to provide the set of fields that Pivot users use to define and generate a pivot report. The set of fields that a Pivot user has access to is determined by the dataset the user chooses when she enters the Pivot Editor. You might add fields to a child dataset to provide fields to Pivot users that are specific to that dataset.

On the other hand, you can also design calculated fields whose only function is to set up the definition of other fields or constraints. This is why **field listing**

order matters: Fields are processed in the order that they are listed in the Data Model Editor. This is why The Data Model Editor allows you to rearrange the listing order of calculated fields.

For example, you could design a *chained set* of three Eval Expression fields. The first two Eval Expression fields would create what are essentially **calculated fields**. The third Eval Expression field would use those two calculated fields in its eval expression.

Fields can be visible or hidden to Pivot users

When you define a field you can determine whether it is *visible* or *hidden* for Pivot users. This can come in handy if each dataset in your data model has lots of fields but only a few fields per dataset are actually useful for Pivot users.

Note: A field can be visible in some datasets and hidden in others. Hiding a field in a parent dataset does *not* cause it to be hidden in the child datasets that descend from it.

Fields are visible by default. Fields that have been hidden for a dataset are marked as such in the dataset's field list.

The determination of what fields to include in your model and which fields to expose for a particular dataset is something you do to make your datasets easier to use in Pivot. It's often helpful to your Pivot users if each dataset exposes only the data that is relevant to that dataset, to make it easier to build meaningful reports. This means, for example, that you can add fields to a root dataset that are hidden throughout the model except for a specific dataset elsewhere in the hierarchy, where their visibility makes sense in the context of that dataset and its particular dataset.

Consider the example mentioned in the previous subsection, where you have a set of three "chained" Eval Expression fields. You may want to hide the first two Eval Expression fields because they're just there as "inputs" to the third field. You'd leave the third field visible because it's the final "output"--the field that matters for Pivot purposes.

Fields can be required or optional for a dataset

During the field design process you can also determine whether a field is *required* or *optional.* This can act as a filter for the event set represented by the dataset. If you say a field is *required,* you're saying that every event represented by the dataset *must* have that field. If you define a field as *optional,* the dataset

may have events that do not have that field at all.

Note: As with field visibility (see above) a field can be required in some datasets and optional in others. Marking a field as *required* in a parent dataset *will not* automatically make that field *required* in the child datasets that descend from that parent dataset.

Fields are optional by default. Fields that have had their status changed to *required* for a dataset are marked as such in the dataset's field list.

View and manage data models in Splunk Light

The Data Models management page is where you go to create data models and maintain some of their "higher order" aspects such as permissions and acceleration. On this page you can:

- **Create a new data model** - It's as easy as clicking a button.
- **Set permissions** - Data models are knowledge objects and as such are permissionable. You use permissions to determine who can see and update the data model.
- **Enable data model acceleration** - This can speed up Pivot performance for data models that cover large datasets.
- **Clone data models** - Useful for quick creation of new data models that are based on existing data models, or to copy data models into other apps.
- **Upload and download data models** - Download a data model (export it outside of Splunk). Upload an exported data model into a different Splunk implementation.
- **Delete data models** - Remove data models that are no longer useful.

In this topic, we'll discuss these aspects of data model management. When you need to define the dataset hierarchies that make up a data model, you go to the Data Model Editor. See Design data models in Splunk Light in this manual.

Navigating to the Data Models management page

The Data Models management page is essentially a listing page, similar to the Alerts, Reports, and Dashboards listing pages. It enables management of permissions and acceleration and also enables data model cloning and removal. It is different from the Select a Data Model page that you may see when you first enter Pivot (you'll only see it if you have more than one data model), as that page

exists only to enable Pivot users to choose the data model they wish to use for pivot creation.

The Data Models management page lists all of the data models in your system in a paginated table. This table can be filtered by app, owner, and name. It can also display all data models that are visible to users of a selected app or just show those data models that were actually created within the app.

See About datasets in Splunk Light in this manual for more information about datasets.

There are two ways to get to the Data Models management page:

Through the sidebar menu in Splunk Light

In the sidebar menu, navigate to **Knowledge > Data models**.

Through the Datasets listing page

1. In the menu bar, open the **Datasets** listing page.
2. Locate a data model dataset.
3. (Optional) Click the name of the data model dataset to view it in the dataset viewing page.
4. Select **Manage > Edit Data Model** for that dataset.
5. On the Data Model Editor, click **All Data Models** to go to the Data Models management page.

Create a new data model

Prerequisites

You can only create data models if your permissions enable you to do so. Your role must have the ability to write to at least one app. If your role has insufficient permissions the **New Data Model** button will not appear.

See Enable roles to create data models in this topic.

Steps

1. Navigate to the Data Models management page.
2. Click **New Data Model** to create a new data model.
3. Enter the data model **Title**.
   The **Title** field can accept any character except asterisks. It can also

accept blank spaces between characters.
The data model **ID** field fills in as you enter the title. Do not update it. The data model **ID** must be a unique identifier for the data model. It can only contain letters, numbers, and underscores. Spaces between characters are also not allowed. After you click **Create** you cannot change the **ID** value.
4. (Optional) Enter the data model **Description**.
5. (Optional) Change the **App** value if you want the data model to belong to a different app context. **App** displays app context that you are in currently.
6. Click **Create** to open the new data model in the Data Model Editor, where you can begin adding and defining the datasets that make up the data model.

When you first enter the Data Model Editor for a new data model it will not have any datasets. To define the data model's first dataset, click **Add Dataset** and select a dataset type. For more information about dataset definition, see the following sections on adding field, search, transaction, and child datasets.

For all the details on the Data Model Editor and the work of creating data model datasets, see Design data models in Splunk Light in this manual.

Enable roles to create data models

By default, only users with the *admin* or *power* role can create data models. For other users, the ability to create a data model is tied to whether their roles have "write" access to an app. To grant another role write access to an app, follow these steps.

Steps

1. Click the **App** dropdown at the top of the page and select *Manage Apps* to go to the Apps page.

2. On the Apps page, find the app that you want to grant data model creation permissions for and click **Permissions**.
3. On the Permissions page for the app, select **Write** for the roles that should be able to create data models for the app.
4. Click **Save** to save your changes.

Giving roles the ability to create data models can have other implications.

See Disable or delete knowledge objects in the Splunk Enterprise *Knowledge Manager Manual*.

About data model permissions

Data models are knowledge objects, and as such the ability to view and edit them is governed by role-based permissions. When you first create a data model it is private to you, which means that no other user can view it on the Select a Data Model page or Data Models management page or update it in any way.

If you want to accelerate a data model, you need to share it first. You cannot accelerate private data models. See Enable data model acceleration in the Splunk Enterprise *Knowledge Manager Manual*.

Align data model permissions with those of related knowledge objects

When you share a data model the knowledge objects associated with that data model (such as lookups or field extractions) must have the same permissions. Otherwise, people may encounter errors when they use the data model.

For example, if your data model is shared to all users of the Search app but uses a lookup table and lookup definition that is only shared with users that have the Admin role, everything will work fine for Admin role users, but all other users will get errors when they try to use the data model in Pivot. The solution is either to restrict the data model to Admin users or to share the lookup table and lookup definition to all users of the Search app.

Edit the permissions for a data model

Prerequisites

- Manage knowledge object permissions in the Splunk Enterprise *Knowledge Manager Manual*.

Steps

1. Go to the Data Models management page.
2. Locate the data model that you want to edit permissions for. Use one of the following options.

Option	Additional steps for this option
Select **Edit > Edit Permissions**.	None
Expand the row for the dataset.	Click **Edit** for permissions.

3. Edit the dataset permissions and click **Save** to save your changes.

This brings up the **Edit Permissions** dialog, which you can use to share private data models with others, and to determine the access levels that various roles have to the data models.

Design data models in Splunk Light

In Splunk Web, you use the Data Model Editor to design new **data models** and edit existing models. This topic shows you how to use the Data Model Editor to:

- Build out **data model dataset** hierarchies by adding root datasets and child datasets to data models.
- Define datasets (by providing **constraints**, search strings, or transaction definitions).
- Rename datasets.
- Delete datasets.

You can also use the Data Model Editor to create and edit dataset **fields**. For more information, see Define dataset fields in the Splunk Enterprise *Knowledge Manager Manual*.

Note: This topic will not spend much time explaining basic data model concepts. If you have not worked with Splunk data models, you may find it helpful to review the topic About data models in Splunk Light in this manual. It provides a lot of background detail around what data models and data model datasets actually are and how they work.

For information about creating and managing new data models, see View and manage data models in Splunk Light in this manual. Aside from creating new data models via the Data Models management page, this topic will also show you how to manage data model permissions and acceleration.

The Data Model Editor

Data models are collections of data model datasets arranged in hierarchical structures. To design a new data model or redesign an existing data model, you go to the Data Model Editor. In the Data Model Editor, you can create datasets for your data model, define their constraints and **fields**, arrange them in logical dataset hierarchies, and maintain them.

You can only edit a specific data model if your permissions enable you to do so.

Navigate to the Data Model Editor

To open the Data Model Editor for an existing data model, choose one of the following options.

Option	Additional steps for this option
From the **Data Models** page.	Find the data model you want to edit and select **Edit > Edit Datasets**.
From the Datasets listing page	Find a data model dataset that you want to edit and select **Manage > Edit data model**.
From the Pivot Editor	Click **Edit dataset** to edit the data model dataset that the Pivot editor is displaying.

Add a root event dataset to a data model

Data models are composed chiefly of dataset hierarchies built on root event dataset. Each root event dataset represents a set of data that is defined by a **constraint**: a simple search that filters out events that aren't relevant to the dataset. Constraints look like the first part of a search, before pipe characters and additional search commands are added.

Constraints for root event datasets are usually designed to return a fairly wide range of data. A large dataset gives you something to work with when you associate child event datasets with the root event dataset, as each child event dataset adds an additional constraint to the ones it inherits from its ancestor datasets, narrowing down the dataset that it represents.

For more information on how constraints work to narrow down datasets in a dataset hierarchy, see dataset constraints in the Splunk Enterprise *Knowledge Manager Manual*.

To add a root event dataset to your data model, click **Add Dataset** in the Data Model Editor and select *Root Event*. This takes you to the Add Event Dataset page.

Give the root event dataset a **Dataset Name**, **Dataset ID,** and one or more **Constraints.**

The **Dataset Name** field can accept any character except asterisks. It can also accept blank spaces between characters. It's what you'll see on the Choose a Dataset page and other places where data model datasets are listed.

The **Dataset ID** must be a unique identifier for the dataset. It cannot contain spaces or any characters that aren't alphanumeric, underscores, or hyphens (*a-z*, *A-Z*, *0-9*, _, or -). Spaces between characters are also not allowed. Once you save the **Dataset ID** value you can't edit it.

After you provide **Constraints** for the root event dataset you can click *Preview* to test whether the constraints you've supplied return the kinds of events you want.

Add a root search dataset to a data model

Root search datasets enable you to create dataset hierarchies where the base dataset is the result of an arbitrary search. You can use any SPL in the search string that defines a root search dataset.

You cannot accelerate root search datasets that use transforming searches. A transforming search uses transforming commands to define a base dataset where one or more fields aggregate over the entire dataset.

To add a root search dataset to your data model, click **Add Dataset** in the Data Model Editor and select *Root Search*. This takes you to the Add Search Dataset page.

Give the root search dataset a **Dataset Name**, **Dataset ID,** and search string. To preview the results of the search in the section at the bottom of the page, click the magnifying glass icon to run the search, or just hit return on your keyboard while your cursor is in the search bar.

The **Dataset Name** field can accept any character except asterisks. It can also accept blank spaces between characters. It's what you'll see on the Choose a

Dataset page and other places where data model datasets are listed.

The **Dataset ID** must be a unique identifier for the dataset. It cannot contain spaces or any characters that aren't alphanumeric, underscores, or hyphens (*a-z*, *A-Z*, *0-9*, _, or -). Spaces between characters are also not allowed. Once you save the **Dataset ID,** value you can't edit it.

For more information about designing search strings, see the Splunk Enterprise *Search Manual*.

Don't create a root search dataset for your search if he search is a simple `transaction` search. Set it up as a root transaction dataset.

Using transforming searches in a root search dataset

You can create root search datasets for searches that do not map directly to Splunk events, as long as you understand that they cannot be accelerated. In other words, searches that involve input or output that is not in the format of an event. This includes searches that:

- Make use of **transforming commands** such as `stats`, `chart`, and `timechart`. Transforming commands organize the data they return into tables rather than event lists.
- Use other commands that do not return events.
- Pull in data from external non-Splunk sources using a command other than `lookup`. This data cannot be guaranteed to have default fields like `host`, `source`, `sourcetype`, or `_time` and therefore might not be event-mappable. An example would be using the `inputcsv` command to get information from an external .csv file.

Add a root transaction dataset to a data model

Root transaction datasets enable you to create dataset hierarchies that are based on a dataset made up of **transaction** events. A transaction event is actually a collection of conceptually-related events that spans time, such as all website access events related to a single customer hotel reservation session, or all events related to a firewall intrusion incident. When you define a root transaction dataset, you define the transaction that pulls out a set of transaction events.

Read up on transactions and the `transaction` command if you're unfamiliar with how they work. Get started at **About transactions,** in the Splunk Enterprise *Search Manual*. Get detail information on the `transaction` command at its entry

in the Splunk Enterprise *Search Reference*.

Root transaction datasets and their children do not benefit from data model acceleration.

To add a root transaction dataset to your data model, click **Add Dataset** in the Data Model Editor and select *Root Transaction*. This takes you to the Add Transaction Dataset page.

Root transaction dataset definitions require a **Dataset Name** and **Dataset ID** and at least one **Group Dataset**. The **Group by**, **Max Pause**, and **Max Span** fields are optional, but the transaction definition is incomplete until at least one of those three fields is defined.

The **Dataset Name** field can accept any character except asterisks. It can also accept blank spaces between characters. It's what you'll see on the Choose a dataset page and other places where data model datasets are listed.

The **Dataset ID** must be a unique identifier for the dataset. It cannot contain spaces or any characters that aren't alphanumeric, underscores, or hyphens (*a-z*, *A-Z*, *0-9*, _, or -). Spaces between characters are also not allowed. Once you save the **Dataset ID** value you can't edit it.

All root transaction dataset definitions require one or more **Group Dataset** names to define the pool of data from which the transaction dataset will derive its transactions. There are restrictions on what you can add under **Group Dataset**, however. **Group Dataset** can contain one of the following three options:

- One or more event datasets (either root event datasets or child event datasets)
- One transaction dataset (either root or child)
- One search dataset (either root or child)

In addition, you are restricted to datasets that exist within the currently selected data model.

If you're familiar with how the `transaction` command works, you can think of the **Group Datasets** as the way we provide the portion of the search string that appears *before* the transaction command. Take the example presented in the preceding screenshot, where we've added the *Apache Access Search* dataset to the definition of the root transaction dataset Web Session. *Apache Access Search* represents a set of successful webserver access events--its two constraints are `status < 600` and `sourcetype = access_* OR source = *.log`. So the start of the transaction search that this root transaction dataset represents would be:

```
status < 600 sourcetype=access_* OR source=*.log | transaction...
```

Now we only have to define the rest of the `transaction` argument.

Add a child dataset to a data model

You can add child datasets to root datasets and other child datasets. A child dataset inherits all of the constraints and fields that belong to its parent dataset. A single dataset can be associated with multiple child datasets.

When you define a new child dataset, you give it one or more additional constraints, to further focus the dataset that the dataset represents. For example, if your Web Intelligence data model has a root event dataset called HTTP Request that captures all webserver access events, you could give it three child event datasets: HTTP Success, HTTP Error, and HTTP Redirect. Each child event dataset focuses on a specific subset of the HTTP Request dataset:

- The child event dataset *HTTP Success* uses the additional constraint `status = 2*` to focus on successful webserver access events.
- *HTTP Error* uses the additional constraint `status = 4*` to focus on failed webserver access events.
- *HTTP Redirect* uses the additional constraint `status = 3*` to focus on redirected webserver access events.

The addition of fields beyond those that are inherited from the parent dataset is optional.

To add a child dataset to your data model, select the parent dataset in the left-hand dataset hierarchy, click **Add Dataset** in the Data Model Editor, and select *Child*. This takes you to the Add Child Dataset page.

Give the child dataset a **Dataset Name** and **Dataset ID.**

The **Dataset Name** field can accept any character except asterisks. It can also accept blank spaces between characters. It's what you'll see on the Choose a Dataset page and other places where data model datasets are listed.

The **Dataset ID** must be a unique identifier for the dataset. It cannot contain spaces or any characters that aren't alphanumeric, underscores, or hyphens (*a-z*, *A-Z*, *0-9*, _, or -). Spaces between characters are also not allowed. After you save the **Dataset ID** value you can't edit it.

After you define a **Constraint** for the child dataset you can click *Preview* to test whether the constraints you've supplied return the kinds of events you want.

Some best practices for data model design

It can take some trial and error to determine the data model designs that work for you. Here are some tips that can get you off to a running start.

- **Use root event datasets and root search datasets only use streaming commands whenever possible** to take advantage of the benefits of data model acceleration (and to benefit from their ease of optimization).

- **When you define constraints for a root event dataset or define a search for a root search dataset that you will accelerate, include the index or indexes it is selecting from.** Data model acceleration efficiency and accuracy is improved when the data model is directed to search a specific index or set of indexes. If you do not specify indexes, the data model searches over all available indexes.
- **Minimize dataset hierarchy depth whenever possible.** Constraint-based filtering is less efficient deeper down the tree.
- **Use field flags to selectively expose small groups of fields for each dataset.** You can expose and hide different fields for different datasets. A child field can expose an entirely different set of fields than those exposed by its parent. Your Pivot users will benefit from this selection by not having to deal with a bewildering array of fields whenever they set out to make a pivot chart or table. Instead they'll see only those fields that make sense in the context of the dataset they've chosen.
- **Reverse-engineer your existing dashboards and searches into data models.** This can be a way to quickly get started with data models. Dashboards built with pivot-derived panels are easier to maintain.
- **When designing a new data model, first try to understand what your Pivot users hope to be able to do with it.** Work backwards from there. The structure of your model should be determined by your users' needs and expectations.

Use Pivot visualizations in Splunk Light

The Pivot tool lets you report on a specific data set without the Splunk Search Processing Language (SPL™). First, identify a dataset that you want to report on, and then use a drag-and-drop interface to design and generate **pivots** that present different aspects of that data in the form of tables, charts, and other visualizations.

How does Pivot work? It uses **data models** to define the broad category of event data that you're working with, and then uses hierarchically arranged collections of **data model datasets** to further subdivide the original dataset and define the **fields** that you want Pivot to return results on. Data models and their datasets are designed by the knowledge managers in your organization. They do a lot of hard work for you to enable you to quickly focus on a specific subset of event data.

For example, you can have a data model that tracks email server information, with datasets representing emails sent and emails received. If you want to focus on patterns in your sent email, select the "Email Activity" data model and choose

the "Emails Sent" dataset.

For an in-depth conceptual overview of data models and data model datasets, see About data models in Splunk Light in this manual.

Creating a pivot:

There are two ways to navigate to the Pivots view:

- Through the Datasets page
- Through the Data Model listing page

Prerequisites

- Learn about creating a pivot in Create and save a pivot in the Splunk Enterprise *Pivot Manual*.

Steps

From	What to do
Datasets page	1. In the menu bar, open the **Datasets** listing page. 2. Identify the data model dataset for which you want to create a Pivot for. 3. Select **Pivot** 4. Click **Save As...** to save your changes as a report or a dashboard panel.
Knowledge > Data Models	1. In the sidebar menu, select **Knowledge > Data models**. 2. On the Data Models page, choose a data model to identify the dataset that you want to work with. (If there's only one data model in your system you'll be moved directly to the next step, where you select an dataset in that data model.) 3. On the Datasets page, select a dataset within that data model. 4. Click **Pivot**. 5. Click **Save As...** to save your changes as a report or a dashboard panel.

If you view Pivot in smaller browser windows, the navigation bar is hidden. To use the navigation bar, click the menu icon on the upper right. The navigation bar slides down.

After you select an dataset, Splunk Web takes you to the Pivot Editor where you can create a pivot using the fields that are available to you. Your pivot can take the form of a table or chart. Go to the Design pivots with the Pivot Editor topic in the Splunk Enterprise *Pivot Manual* to learn how to use the Pivot Editor to create a table, chart, or other visualization with Pivot.

To learn more about Pivot, see the Splunk Enterprise *Pivot Manual* and the Splunk Enterprise *Data Model and Pivot Tutorial*.