



STORMSHIELD



GUIDE

STORMSHIELD LOG SUPERVISOR

SEARCH GUIDE

Version 2

Document last updated: July 4, 2024

Reference: sls-en_search_gde



Table of contents

- Change log 5
- Getting started 6
- Search Bar 7
 - Repo selector 8
 - Time range 9
 - Use Wizard 9
- Search Page 13
 - My Search History 13
 - My Saved Searches 13
 - Search Templates 13
 - Labels 13
 - Vendor Searches 13
 - Search Views 13
- Tools 14
 - Found 14
 - Search Help Text 14
 - Add Search To 15
 - Add Search To Dashboard 15
 - Add Search To Alert Rule 16
 - Add Search To Labelling Rule 16
 - Add Search To Incident 17
 - Add Search To Public URL 17
 - More 17
 - Export Logs 17
 - Permalink 19
 - Save Search 19
 - Report 19
 - Stop/Pause 20
- Drilldown 21
 - Actions in the Field-Value Pairs 22
 - Top 10 Fields 22
 - Time Trend for Fields 22
 - Time Trend for Full Resultset 22
 - Exclude field 22
 - Explore in Search Template 23
 - Request for field 24
 - Add this field to interesting fields 26
 - Hide Fields 26
 - Recover Hidden Fields 26
 - Display maximum 27
- Interesting Fields 28
 - Actions in the Interesting Fields 28
 - Sorting 28
 - View Details 29
 - Adding Interesting Fields 29



- Selecting the fields 29
- Adding the fields 30
- Adding the fields from the search result drop-down 30
- Search Packages 32**
 - Adding a Search Package 32
 - Managing Saved Searches 33
 - Saved Searches 34
 - Cloning Saved Searches 34
 - Registering from a Public API 35
 - Searching a Saved Search 36
 - Deleting a Saved Search 36
 - Exporting Search Packages 38
 - Importing Search Packages 38
 - Editing a Search Package 38
 - Cloning Search Packages 39
 - Deleting Search Packages 40
- Search Views 42**
 - Accessing Search Views 42
 - The Search Views Interface 43
 - Query Bar 43
 - Result Panel 43
 - Top-10 Panel 44
 - Adding a Search View 45
 - Editing a Search View 46
 - Sharing Search Views 47
 - Cloning Search Views 48
 - Deleting Search Views 49
 - Using a Search View 50
 - Using Drill-down in Search Views 52
 - Using Negation in Search Views 53
- Macros 55**
 - Adding Macros 55
 - Searching with Macros 55
 - Updating Macros 56
 - Deleting Macros 56
 - Importing Macros 57
 - Exporting Macros 58
 - Examples of Macros 58
- Search Templates 60**
 - Creating a Search Template 60
 - Exporting Search Templates 61
 - Importing Search Templates 62
 - Editing a Search Template 62
 - Sharing Search Templates 63
 - Deleting a Shared Search Template's Owner 65
 - Cloning Search Templates 66
 - Deleting Search Templates 67
 - Viewing a Search Template 67



Adding a Dashboard	68
Adding a Widget	69
Creating a Report	70
Auto-arrange the Widgets	71
Updating Parameters	71
Stopping widget update	72
Further reading	73



Change log

Date	Description
July 4, 2024	New document

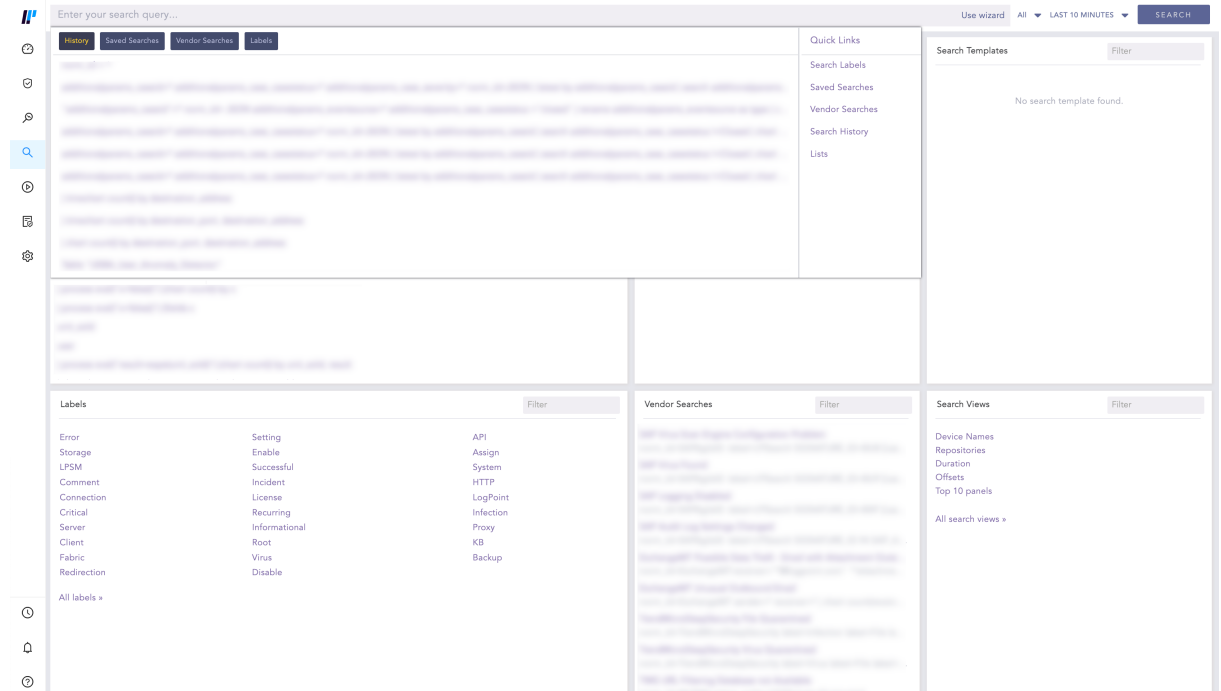


Getting started

Welcome to the SLS version 2 Search Guide.

SLS collects logs using different collectors and fetchers and stores them for a specified period of time. You can search these logs using a query and use the results to create dashboard widgets, generate reports and add alert rules. In addition, you can monitor various compliance requirements, configure different correlation intelligence and respond to critical incidents.

Use the Search bar to perform a search.

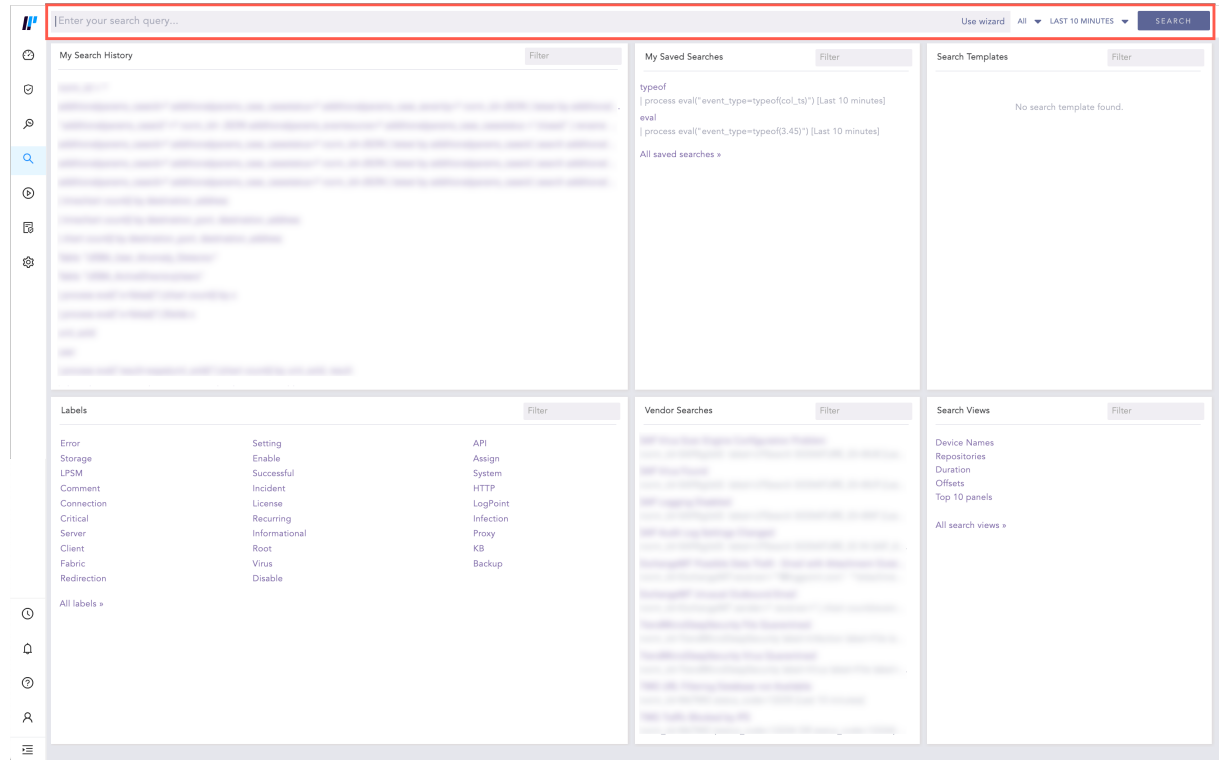


In this document, Stormshield Log Supervisor is referred to in its short form SLS. Images used in this document are from the partner vendor's (Logpoint) software program. In your SLS, the graphics may vary but user experience is exactly the same.

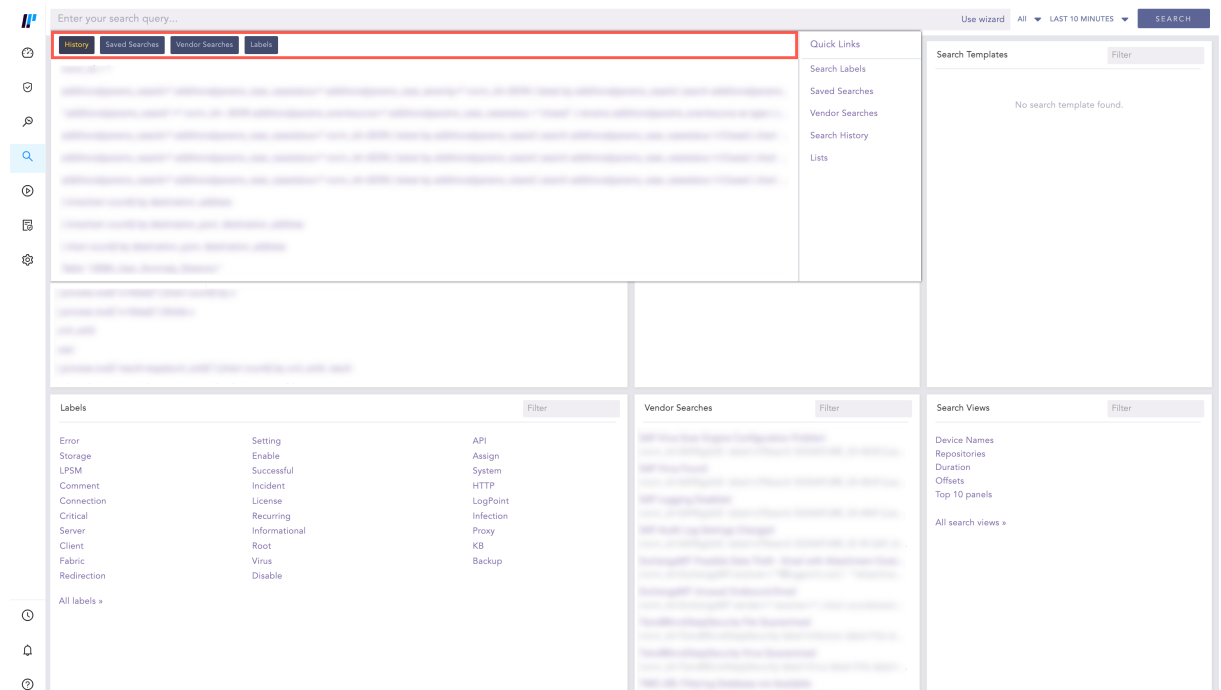


Search Bar

Search Bar lets you search the indexed logs. You can enter the query string in the search space. A **Query String** is a logical combination of words, phrases, or field values. You can either type a query string or build it to aggregate different values in the search result and display the result in a graphical format.

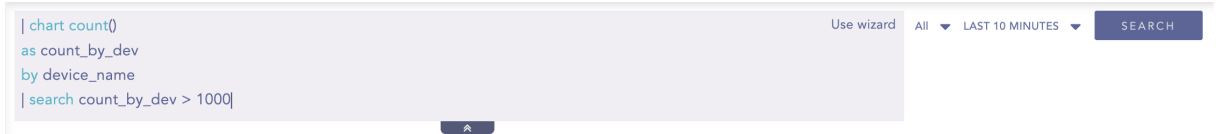


You can view **History**, **Saved Searches**, **Vendor Searches**, and **Labels** once you click on search bar.

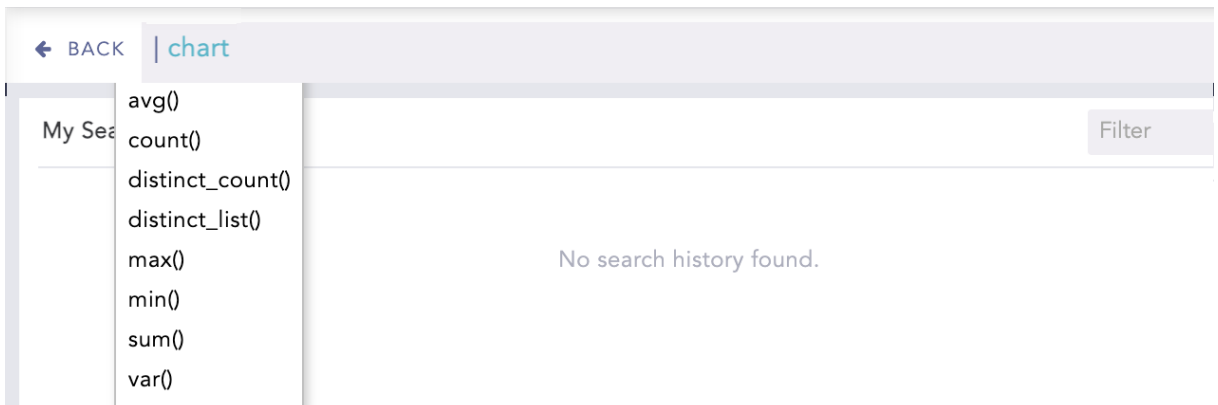
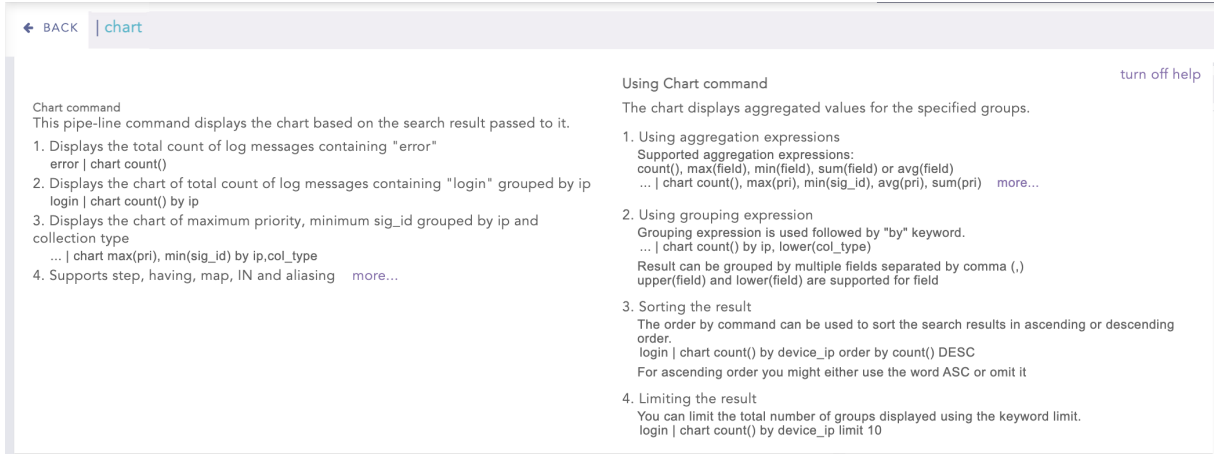




You can write multiple queries using multiple lines. Press **Shift + Enter** to add a new line. The search bar can expand vertically up to 15 lines for your query. After that, a scroll bar appears to the right.

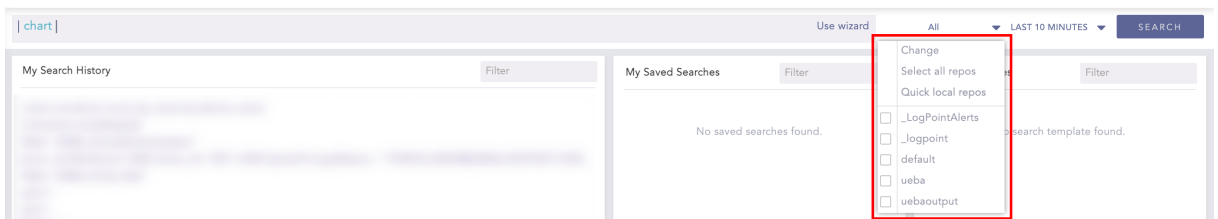


When you type a query, SLS auto-suggests keywords based on your input. SLS can display a detailed and dynamic search guide when you type a query in the search bar.

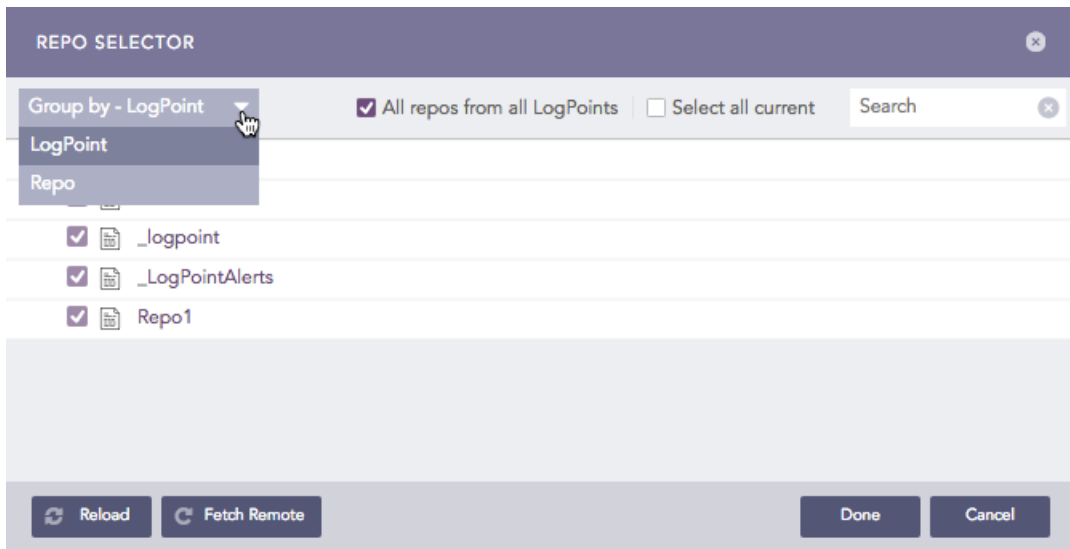


Repo selector

Repo Selector let's you select where to search for logs. Each repository collects the logs and stores them for a pre-defined period. Use the drop-down on the right to select multiple repositories. Choose only the required repos, otherwise performance is affected.

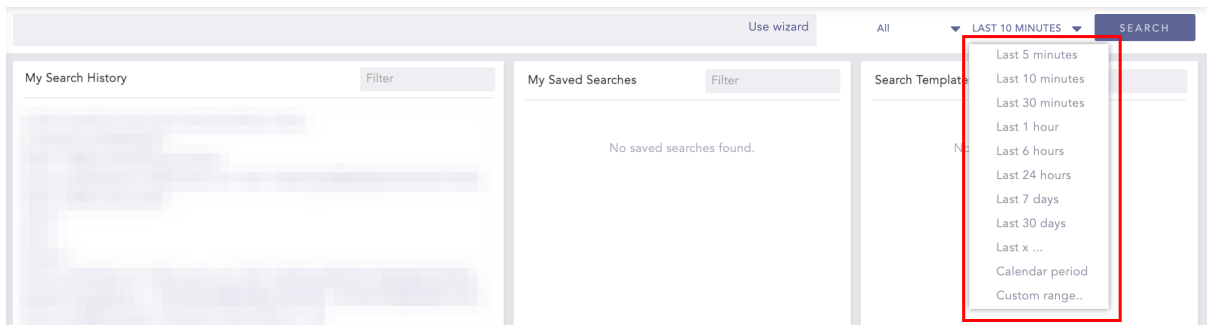


The repos in the **Repo Selector** are grouped either by Distributed SLSs (DLP) or by Repo. From the **Repo Selector**, click **Change** to choose how the repos are grouped.



Time range

You can apply a **Time range** to your search. The default is Last 10 minutes. You can apply a time frame using the "Last x time-range" format, or select a custom time range of **Last 1 hour**, **Last 6 hours**, **Last 7 days** from the drop-down.



Use Wizard

To use **Use Wizard**:

1. In the navigation bar, click **Use Wizard**.



SEARCH WIZARD

Building A Simple Search Query

Enclose a phrase in a double quote
error login "windows machine"

BUILD QUERY

Containing words/phrases:

Not containing words/phrases:

Continue **Search Now** **Cancel**

2. Enter your search terms.
3. Enter the **words/phrases** that you want to exclude from the search.
4. Click **Continue**.

i **NOTE**

You can click **Search Now** at any time while building the search query in this way. It searches for the logs using the query built up to that point in the process.

5. Select **Visualization**.

SEARCH WIZARD

Visualize Result

Select one of the provided option to visualize search result

Chart **Time chart** **Latest**

Previous **Cancel**



- **Chart or Timechart**

1. Select a **Aggregation** function and a **Field**.
2. Click **Add**.

i **NOTE**

You can add multiple aggregation functions and fields. The aggregators are listed under **AGGREGATIONS**.

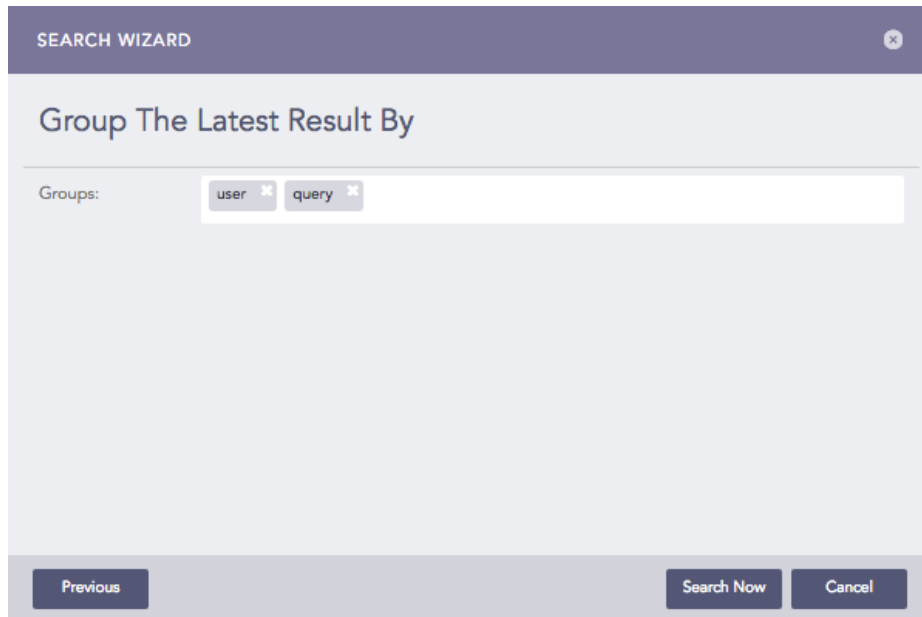
3. Click **Continue**.
4. Choose fields from which to **Group** the results.

5. Click **Search Now** to get your visualization.



- **Latest**

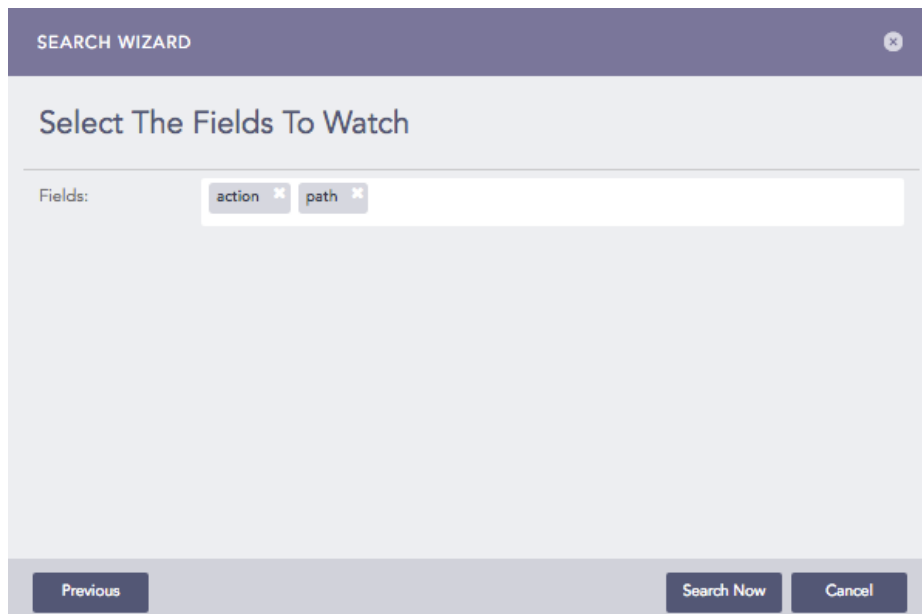
1. Select the fields from dropdown to **Group** the latest results.



2. Click **Search Now** to get your visualization.

- **Selected Fields**

1. Choose the **Fields** from the drop-down.



2. Click **Search Now** to get your visualization.



Search Page

The Search landing page contains six sections. On each section, use the `filter` text-box to search through the respective components. Provide at least one matching search term in the text-box to search the query.

My Search History

Lists the recent search queries executed in the SLS. Click a **Search** to automatically feed it to the search bar and display the results accordingly.

My Saved Searches

Lists the saved search queries in the SLS. Click a **Saved Search** to automatically feed it to the search bar and display the results accordingly.

Search Templates

Lists the search templates created in the SLS. Clicking a template opens the search template page. Enter the desired values in the **Update Parameters** section, select the required **Repos** and click **Update** to refresh the previously created widgets.

Labels

Lists the labels of the system. Labels are assigned while writing signatures for the logs. Click a label to automatically feed it in the search bar and display the results accordingly.

Vendor Searches

Lists the search queries provided by the vendor. Click a vendor search query to automatically feed in the search bar and display the results accordingly.

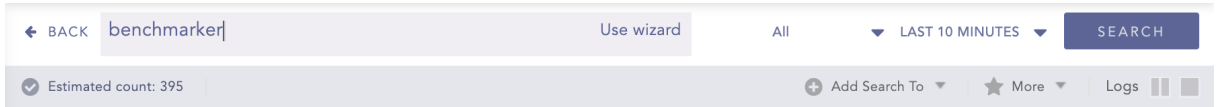
Search Views

Lists a maximum of 20 recently created views. Click any of the added **Search Views** from the list, or, **All search views** to view the search results.



Tools

The search result also has a tool bar that gives you an easy access to the various functions right after search.

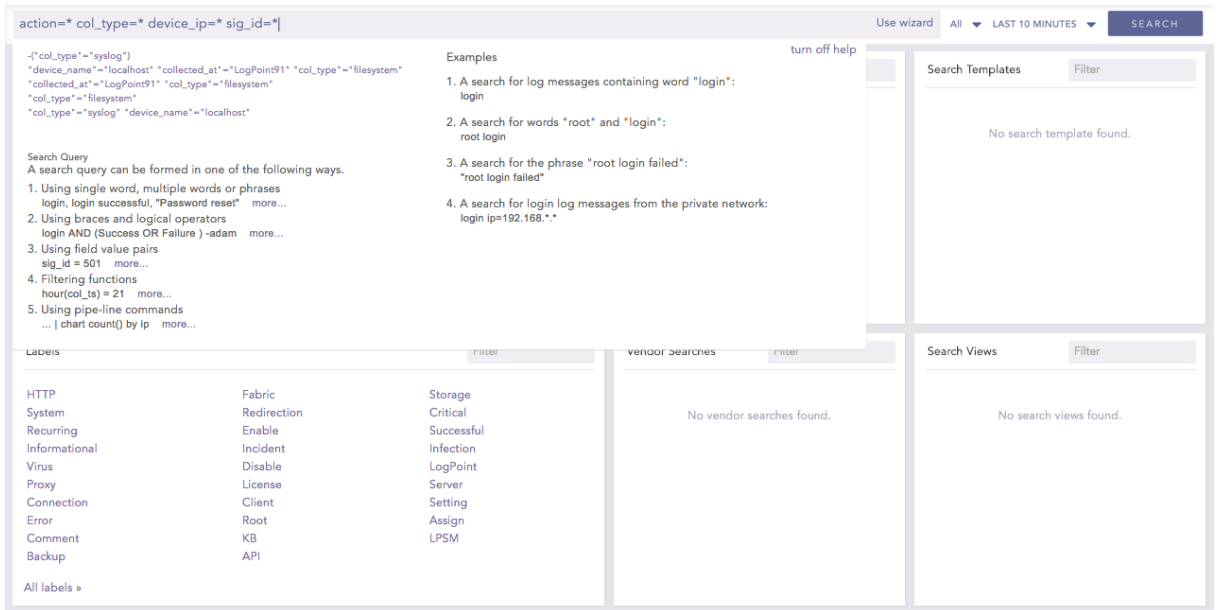


Found

This is the total number of results found for the search query. SLS searches results in an incremental basis, so this number keeps getting updated until all the results have been fetched.

Search Help Text

In the Search Query bar, if you click the down arrow key, a pop-up panel appears. It contains texts to help you write valid search queries. An alternative way to access this feature is to click **CMD + right click** (on a Mac) and **CTRL+ right click** (on a Windows Machine). You can conduct a search query while simultaneously looking at the search help-text window.



NOTE
The search help text is not displayed if you have disabled the **Display search help pop-up** in **My Preferences >> Search**.

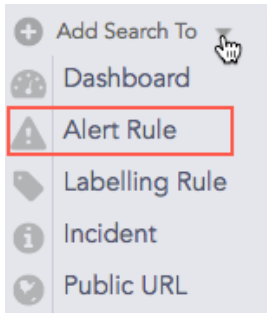


3. Select a **Dashboard**.
4. Click **Finish**.

i NOTE

The display widgets such as bar graphs, donut charts, and tables automatically appear according to the nature of the result of the search query you enter.

Add Search To Alert Rule



1. Click **Alert Rule** to open the **Create Alert** panel.
2. Provide the **Name**, the **Description**, the **Repos**, and the **Time Range** and click **Next**.
3. Select the **Condition**, the **Risk**, and the **Risk Calculation Function** and click **Next**.
4. Choose a medium for the alert notification.
5. Click **Finish**.

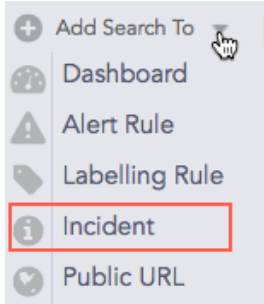
Add Search To Labelling Rule



1. Click **Labelling Rule** to open the **Search Label** panel.
2. Select a **Package** and enter a **List of Labels**.
3. Click **Submit**.



Add Search To Incident



1. Click **Incident** to open the **Create Search Incident** panel.
2. Provide the **Incident Name**, the **Description**, and the **Risk** level.
3. Provide the necessary **Ownership** information.
4. Click **Submit**.

Add Search To Public URL

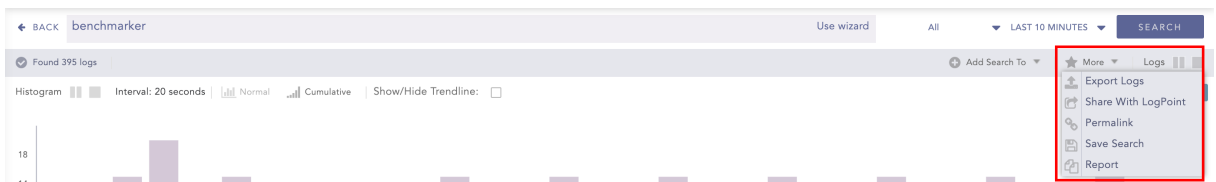
The **Add Search to Public URL** option lets you add and share Dashboard widgets publicly.



1. Click **Public URL** to open the **Register to Public URL** panel.
2. Specify a **Name**, an **Identifier**, and a **Package** to add your search to a public URL.
3. Click **Ok**.

More

The **More** option lists all the functions that can be carried out for the result of a query.



Export Logs

Export Logs lets you export the search results to the specified target on a remote machine. To export the logs of simple search queries, follow these steps:

1. Go to Search from the navigation bar.
2. Enter a **Search Query** in the query bar and click **Search**.
3. Click **Export Logs**.



The screenshot shows the SLS search interface. At the top, there is a navigation bar with 'BACK', 'benchmarker', 'Use wizard', and a search bar. Below this, a histogram displays data over time from January 2, 2022, to January 9, 2022. A menu in the top right corner is open, with 'Export Logs' highlighted. Below the histogram, there is a table of 'Interesting Fields' and a list of log entries. The first log entry is dated 2022/01/09 13:11:02 and contains detailed audit information. The second log entry is dated 2022/01/09 13:10:07. At the bottom, it indicates 'Displaying 1-2 of 2 logs' and 'Display maximum: 25 logs per page'.

4. Specify the Job Name, the Timeout in seconds, the Target and the Max File Size.

The 'EXPORT OPTIONS' dialog box is shown. It contains the following fields and values:

- Job Name: Sample_Export
- Line Separator: \n
- Timeout (seconds): 30
- Target: SCP_Export1
- Max File Size: 128 MB (multiple of 128)

At the bottom of the dialog, there are 'Submit' and 'Cancel' buttons.

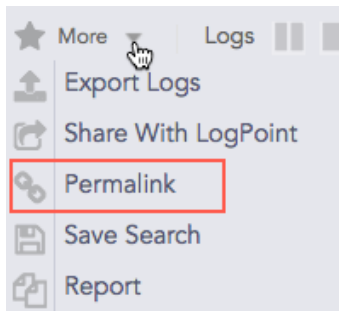
5. Click Submit.

NOTE
The **Export Logs** feature can only be used for simple queries. For aggregated queries, use the **Export as CSV** and **Export as Excel** options.



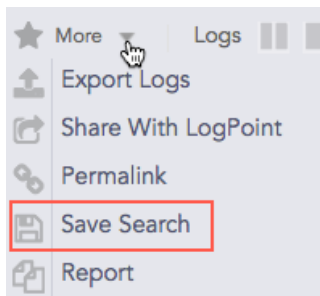
Permalink

Permalink gives you a complete URL required to generate the current search. You can share this link to other users in the system to make exact and similar search.



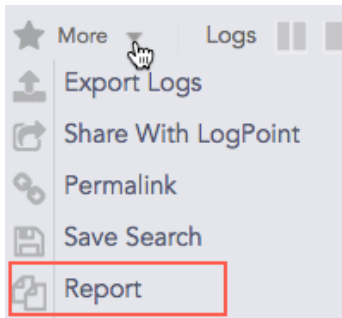
Save Search

Save Search lets you save your current search. You can view the **Saved Searches** on the Search page under the **My Saved Searches** section.



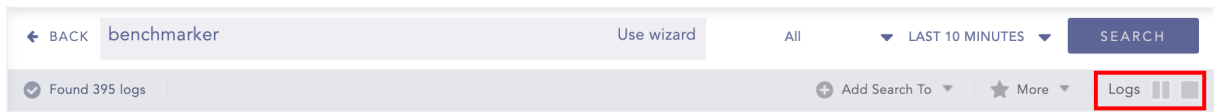
Report

You can click this option to generate the report of the current search result.



Stop/Pause

You can pause or stop the search using the corresponding buttons.

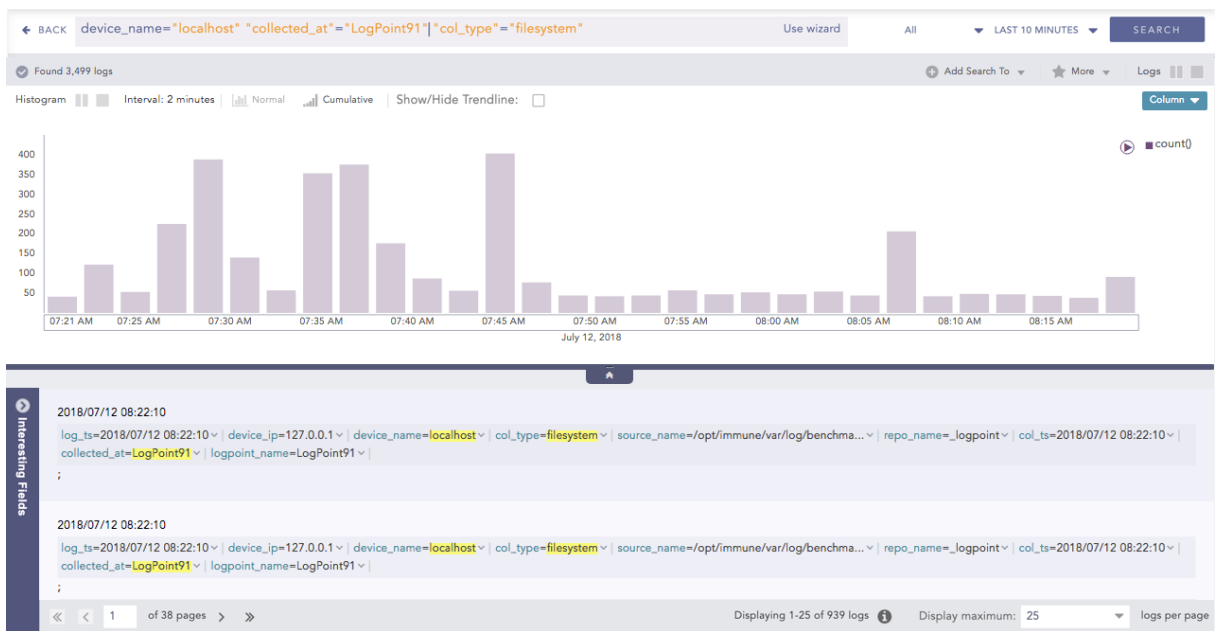




Drilldown

You can refine your search query by clicking the content of the results (key-value pairs or raw log messages) after the search has been done. Clicking on any value in the result adds a filter component to original search query. You can combine any number of filters, thereby making complex drill-down actions. The filter components (key-value pairs or raw log messages) are highlighted in the results as you drill down deeper. If you want to undo the drill-down on any component, click it.

For example, if you want to view successful login events for the user **rst@stormshield.eu** from the IP: **192.168.2.20**, click **successful login** in the action field and click the user **rst@stormshield.eu**. Finally, click IP: **192.168.2.20**. The clicked value is added to the query and is displayed in the query bar.



The example above is for the drill-down search conducted on the **filesystem**, the **SLS** (named **LogPoint**), and the **localhost** respectively. Note that the filter components "**device_name**"="**localhost**", "**collected_at**"="**SLS**" (**LogPoint**), and "**col_type**"="**filesystem**" automatically appear in the search query.

You can also carry out a negative drill-down search in the same manner. However, in this case, you have to use the **Shift** key while selecting the filter components (key-value pair or raw log messages).



The first screenshot shows a search for `"device_name"="William"` with 5 logs found. A histogram shows log counts over time on July 9, 2018. The log results include fields like `log_ts`, `device_ip`, `device_name`, `col_type`, `sig_id`, `repo_name`, `Operation`, `S.No.`, `Task`, and `Value`. The `Value` field in the first log is highlighted as `read2`.

The second screenshot shows the search refined to `!(Value)="read2" device_name="William"` with 4 logs found. The histogram shows a single log entry at 03:00 AM on July 9, 2018. The log results are similar to the first screenshot but exclude the `Value=read2` entry.

The example above describes the **Exclude** operation on the value **read2**.



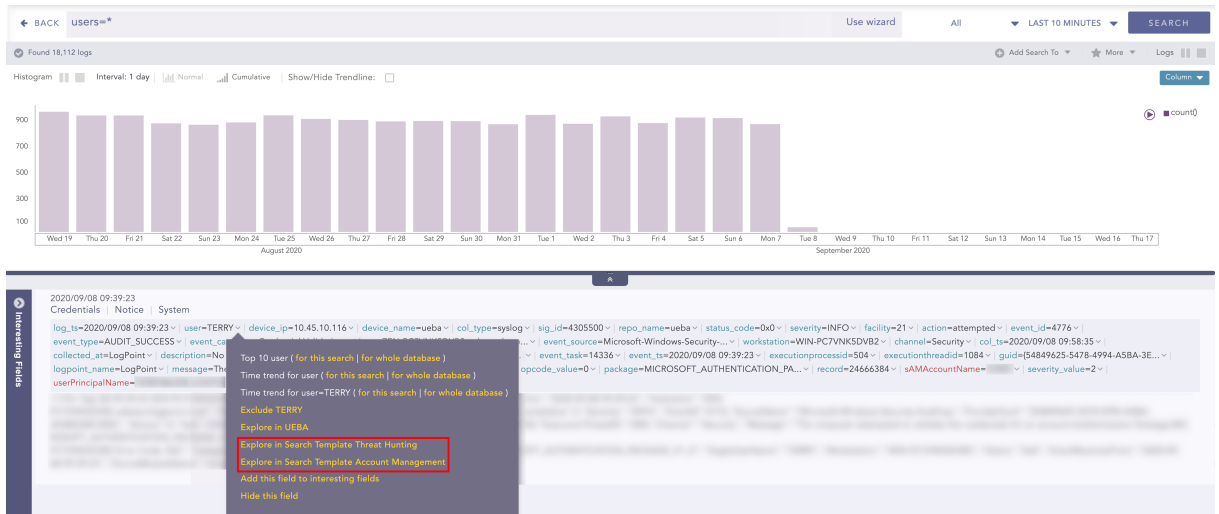
NOTE

The query `!(Value)="read2"` is automatically appended in the search query after clicking **Exclude**.

Explore in Search Template

You can drill-down any value in the search results directly into a search template. Clicking the **Explore in Search Template** option redirects you to the search template with the selected value filled in the corresponding field.

The **Explore in Search Template** option appears only for the search templates that contain the selected field in their respective **Fields** section.

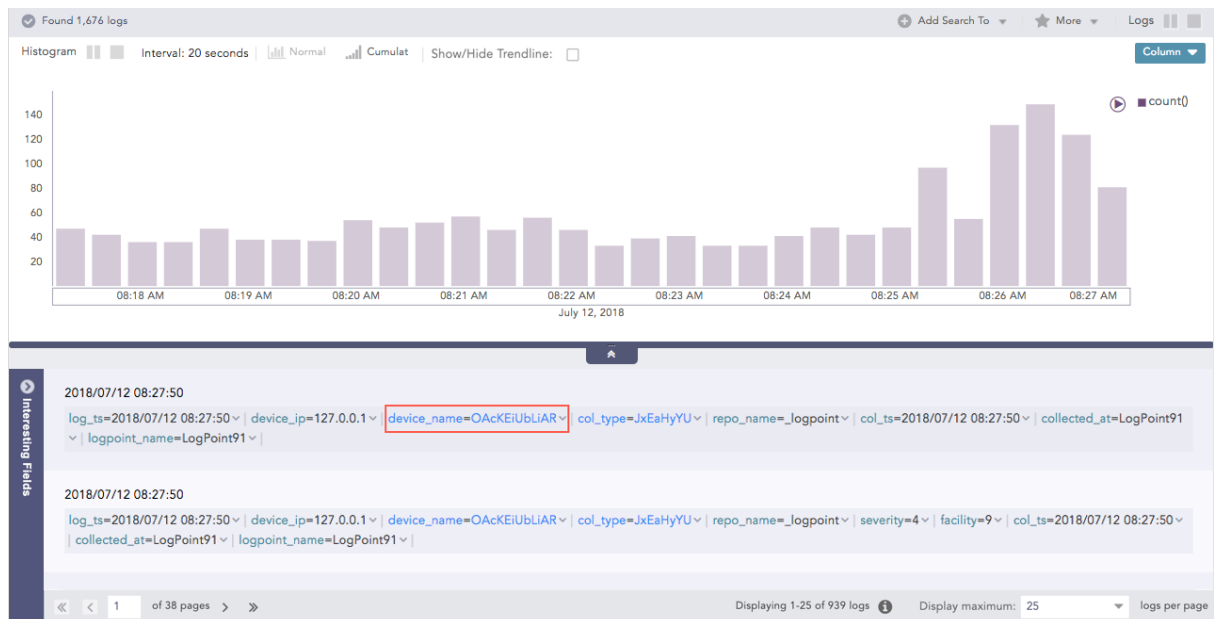


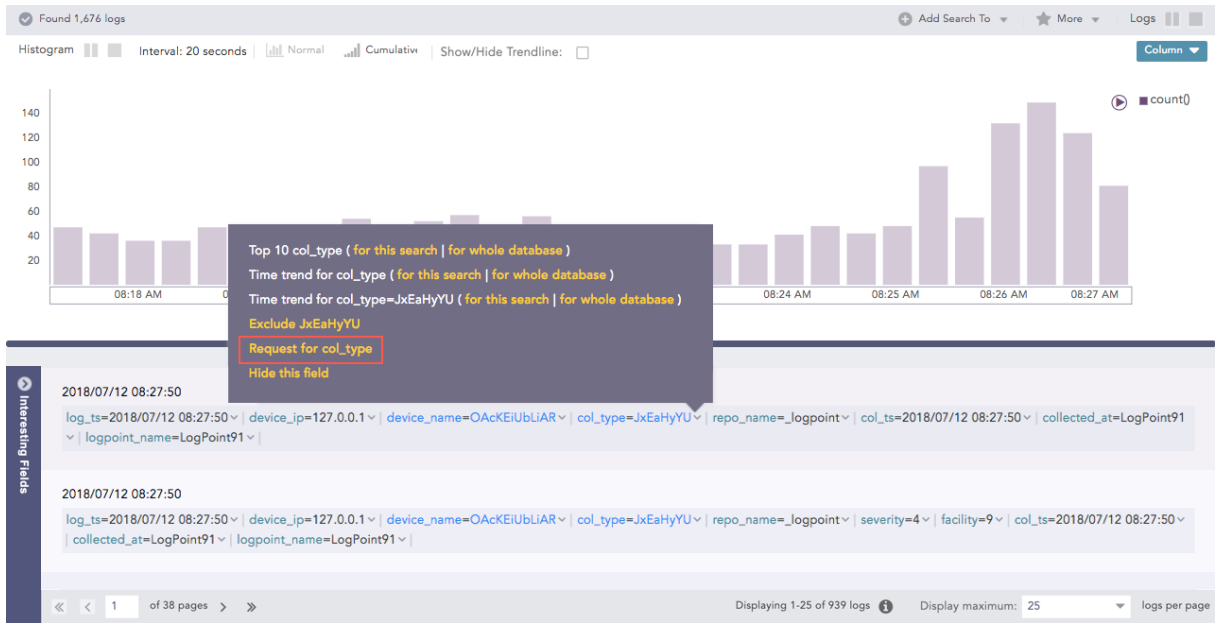
Request for field

This option is applicable for the key-value pairs which are included under the Data Privacy Module. Clicking this option opens the **Data Privacy Request** panel from which you can make a request to view the decrypted values of the encrypted fields. After a request is accepted by a granting user, you can search for the specific field.

To view the decrypted key-value pairs, follow the steps given below:

1. Go to Settings >> Configurations from the navigation bar and click **Data Privacy Module**.
2. Click the **Search** icon for the granted field under the **My Request** tab.
3. SLS redirects you to the **Data Privacy Search** from where you can view the decrypted values.





DATA PRIVACY REQUEST

FIELD VALUE

Field Name:

Value Type

All Value Encrypted Value Plain Value

Value:

All encrypted values will be shown

Add

S.N.	Field	Type	Value	Actions
1	col_type	encrypted	JxEaHyYU	

ACCESS TIME INFORMATION

From: 2018/07/12 08:17:51

To: 2018/07/12 08:27:51

Grant Access for 60 Minutes




Description:

Save Cancel



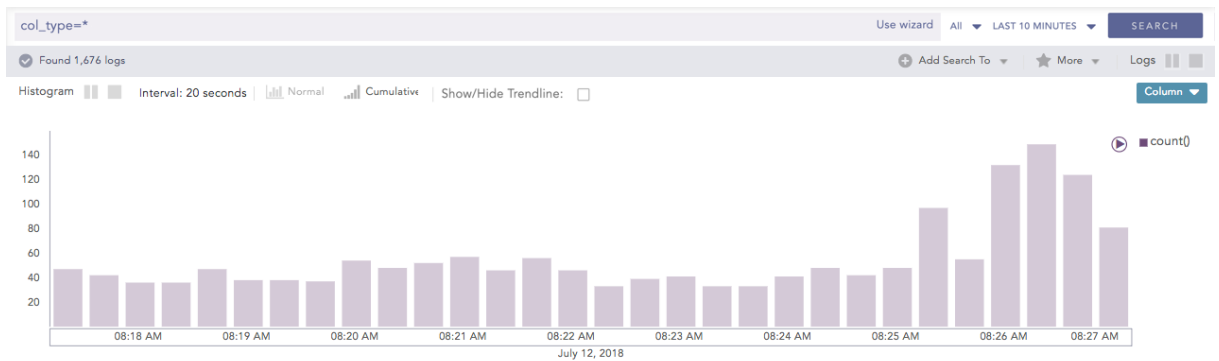
← BACK Data Privacy Module

Data Privacy Module + ADD MORE 0 SELECTED Search

My Request	S.N.	Type	Fields	Start Date	Log Access Dura	Status	Granted/Denied	Actions
Pending Request	1	Search	col_type	2018/07/12 08:17:51	10 minutes	Granted	admin	  
History								

Page 1 of 1 Page size: 25

USER ACCOUNTS CONFIGURATION KNOWLEDGE BASE SYSTEM DATA PRIVACY MODULE



Interesting Fields

2018/07/12 08:27:50
log_ts=2018/07/12 08:27:50 | device_ip=127.0.0.1 | device_name=OAcKEiUblAR | **col_type=syslog** | repo_name=_logpoint | col_ts=2018/07/12 08:27:50 | collected_at=LogPoint91 | logpoint_name=LogPoint91

2018/07/12 08:27:50
log_ts=2018/07/12 08:27:50 | device_ip=127.0.0.1 | device_name=OAcKEiUblAR | col_type=syslog | repo_name=_logpoint | severity=4 | facility=9 | col_ts=2018/07/12 08:27:50 | collected_at=LogPoint91 | logpoint_name=LogPoint91

1 of 38 pages Displaying 1-25 of 939 logs Display maximum: 25 logs per page

Add this field to interesting fields

You can select **Add this field to interesting fields** from the drop-down menu on the key-value pairs to add the required field in the **Interesting Fields** window. The fields added from here can be seen in the **Add Fields** panel of the **Interesting Field** window.

Hide Fields

You can select **Hide this field** from the drop-down menu on the key-value pairs to hide the required field value(s). You can also hide the fields by going through the **My Preferences** >> **Search** >> **Search Log Fields** and entering the field name(s) in **Hide these Fields** text box.

Recover Hidden Fields

- Click the **User** drop-down menu at the top-right corner of the interface and select **My Preferences**.
- Select **Search**.



- Under **Search Log Fields**, deselect the hidden fields from the **Hide these Fields** text-box to unhide the fields.

Display maximum

Select a value from the drop-down menu to view the specified number of logs per page. The default value is 25.



Interesting Fields

The **Interesting Fields** are the relevant fields presented on the basis of the data distribution for the following types of queries:

- **Simple Search** (except the **Table** and **Time Functions** commands)
- **One to One Commands**
- **Filtering Commands** (except the **latest** command and the **search command**)

The **Interesting Fields** window appears at the bottom-left side of the search page after performing a search operation and displays the top 15 fields, sorted according to the occurrence of the fields in the search result.



The parameters used to measure the data distribution are:

- **Percentage [%]** - Displays the percentage of occurrences of a given field.
- **Count [# of values]** - Displays the number of unique values for the given field.
- **Mean Deviation** - Displays the value of the deviation from the average occurrence of the given fields.
- **Median Deviation** - Displays the value of the deviation from the fields with the highest number of similar occurrences.

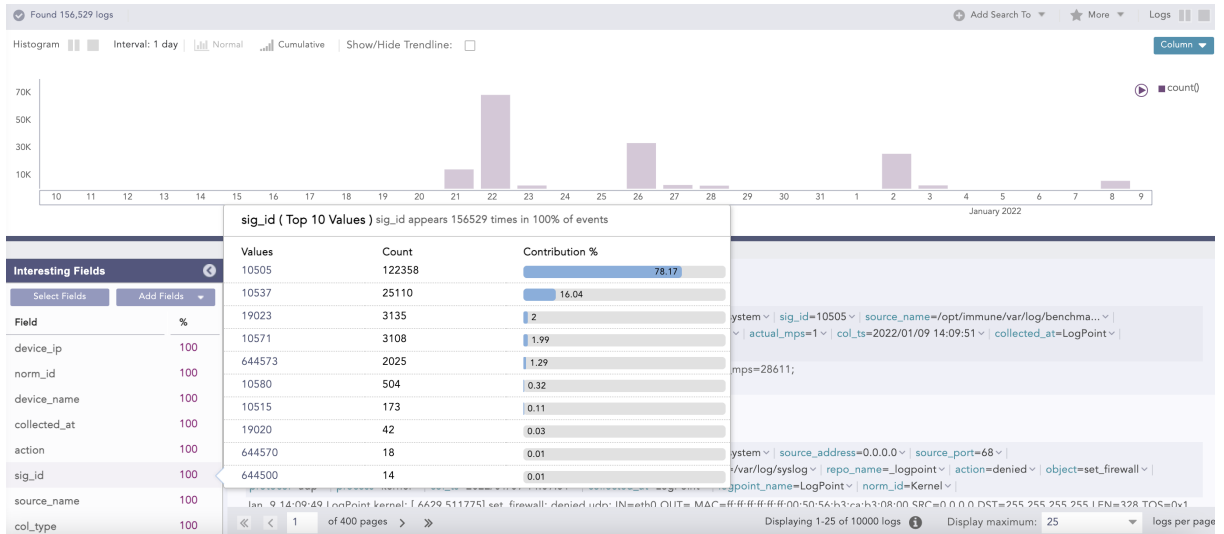
Actions in the Interesting Fields

Sorting

You can sort the Interesting Fields either by clicking on the field header or the parameter header.



View Details



You can view the details of the Interesting Fields by clicking on the desired field from the list. A pop-up panel appears, containing the total number of occurrences of the selected field and its Top 10 values with their distinct counts and percentages.

Adding Interesting Fields

You can add fields to the Interesting Fields window in the following ways:

Selecting the fields

ALL FIELDS

Parameter to display: Percentage

<input type="checkbox"/>	S.N.	Interesting Fields	Percentage ↓
<input checked="" type="checkbox"/>	1	norm_id	100
<input checked="" type="checkbox"/>	2	device_ip	100
<input checked="" type="checkbox"/>	3	sig_id	100
<input checked="" type="checkbox"/>	4	col_type	100
<input checked="" type="checkbox"/>	5	device_name	100
<input checked="" type="checkbox"/>	6	collected_at	100
<input checked="" type="checkbox"/>	7	source_name	100
<input checked="" type="checkbox"/>	8	action	100

Submit



The **All Fields** panel pops up once you click **Select Fields**. The panel lists the top 100 fields from the search results. You can select the desired fields from the list and the relevant parameter from the **Parameter to display** drop-down menu to enlist them in the **Interesting Fields** window.

Adding the fields

Click **Add Fields** to enter the names of the desired fields. These fields are added in the **Interesting Fields** window and in the **All Fields** panel regardless of their occurrence in the search result. You can view these fields in a different colored text in the **Interesting Fields** window.

i NOTE

- You can add a maximum of 20 fields in the **Add Fields** panel.
- You can neither use special characters nor Unicode characters in the **Add Fields** panel.

Adding the fields from the search result drop-down

You can select the **Add this field to interesting fields** option from the drop-down menu on the key-value pairs to add the required field in the **Interesting Fields** window. The fields added from here are appended in the **Add Fields** panel.

i NOTE

- The Percentage [%] parameter is displayed in the **Interesting Fields** window by default. If the percentage of a field is less than **0.005**, it is displayed as **0**.
- The **Interesting Fields** feature is enabled by default. You can disable **Interesting Fields** by selecting the **Disable Interesting Fields in Search Page** option under **My Preferences >> Search**. You can also collapse or expand the **Interesting Fields** window by clicking the window header.
- The **Interesting Fields** window is disabled if:
 - The **Data Privacy Module** is enabled in your system.
 - The queries **Aggregators**, **Pattern Finding**, **Table**, **Time Functions**, **search**, or **latest** are used.
- The values of the parameters in the **Interesting Fields** window are approximated if:
 - The number of fields in the **Interesting Fields** window is more than 100.
 - The distinct count of the given field is more than 100.
- The fields **log_ts**, **col_ts**, **msg**, **sls_name**, **repo_name**, and **label** are not supported in the **Interesting Fields** window.
- The **Loading Interesting Fields** icon appears in the search result tool bar if the system takes time to load the values in the **Interesting Fields** window. The icon disappears once the values are completely loaded.



! IMPORTANT

SLS does not compute the values of the Interesting Fields if you have hidden the **Histogram** and collapsed the **Interesting Fields** window.



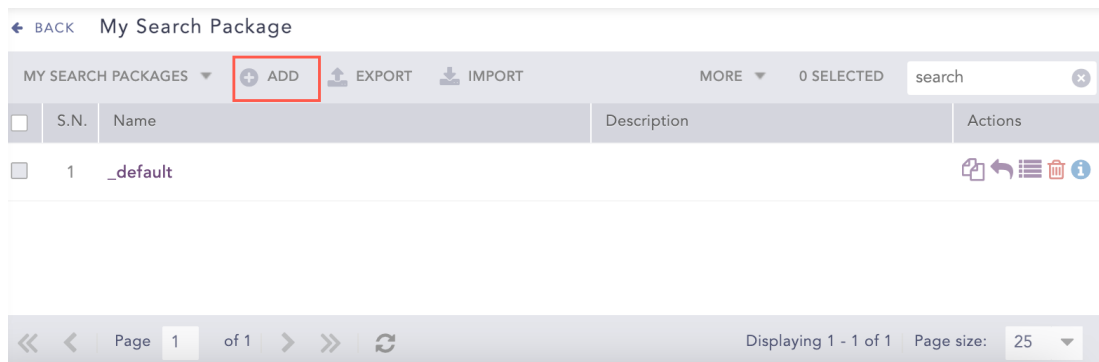
Search Packages

Search Packages are the collection of saved searches. You can **save** a frequently used search query to use it in the future without typing it explicitly.

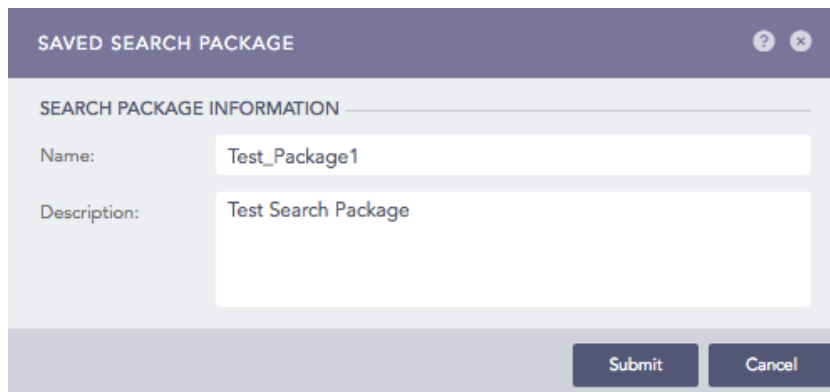
My Packages contains all your **Search Packages**, whereas, the **Search Packages** by vendors are grouped under **Vendor Packages**. Additionally, the search packages that are shared by other users are grouped under **Shared Packages**.

Adding a Search Package

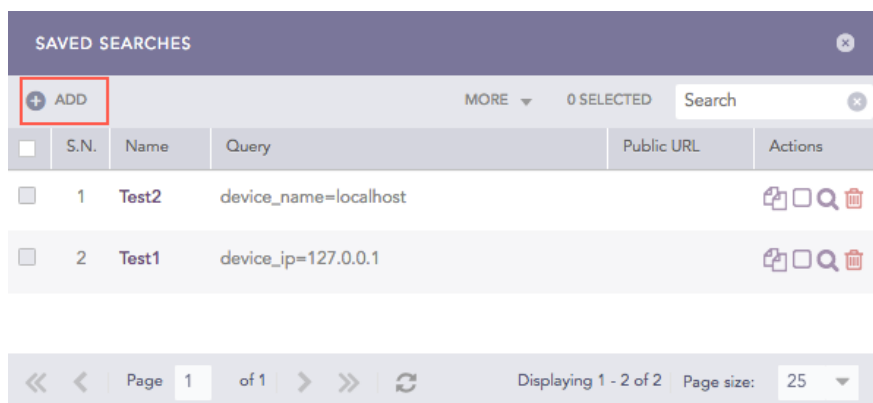
1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.



2. Click **Add** to open the **Saved Search Package** panel.
3. Provide a **Name** and a **Description**.



4. Click **Submit** to open the **Saved Searches** panel.





5. Click **Add** to open the **Saved Search** panel.

SAVED SEARCH

SAVED SEARCH INFORMATION

Name: Test1

Identifier: test

Package: Test_Package1

Query: device_ip=127.0.0.1

Decode

Submit Cancel

- 6. In the **Saved Search Information** section, provide a **Name**, an **Identifier**, and select a **Package**.
- 7. Enter a **Query**.

NOTE
Click **Decode** to convert the URL encoded search string to SLS search query format.

8. Click **Submit**.

NOTE



- Click the **My Packages** drop-down at the top-left corner of the panel and select the **Vendor Packages** to access the **Vendor Search Packages** page.
- Similarly, click the **My Packages** drop-down at the top-right corner of the panel and select the **Shared Packages** to access the **Shared Search Packages** page.

Managing Saved Searches

Click the **Manage Saved Searches** icon under the **Actions** column of a particular package to view or manage the saved searches of that package.

← BACK My Search Package

MY SEARCH PACKAGES + ADD EXPORT IMPORT MORE 1 SELECTED search

<input type="checkbox"/>	S.N.	Name	Description	Actions
<input checked="" type="checkbox"/>	1	Test_Package1		
<input type="checkbox"/>	2	_default		

Page 1 of 1 Displaying 1 - 2 of 2 Page size: 25

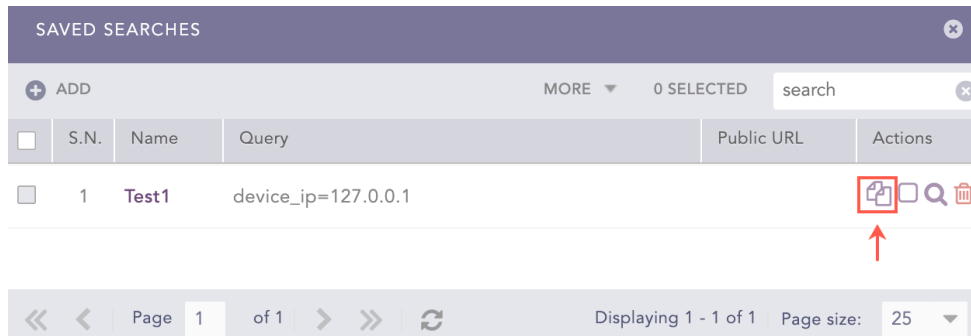


Saved Searches

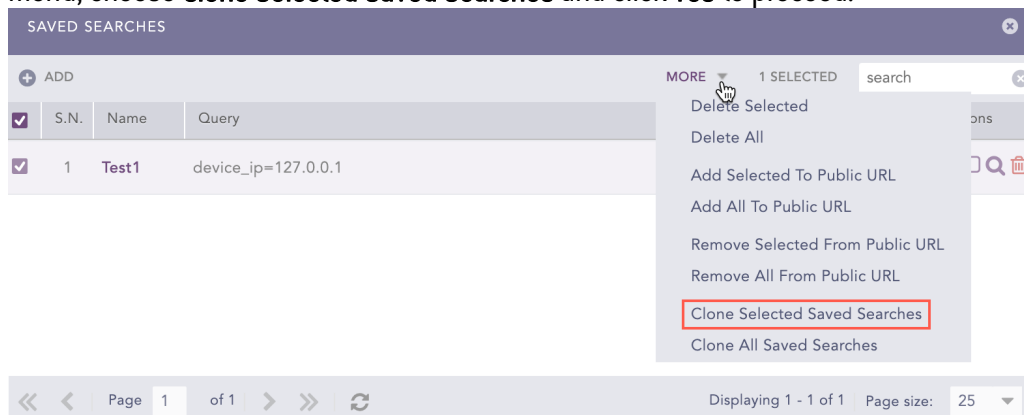
Lists the saved search queries in the SLS. Click a **Saved Search** to automatically feed it to the search bar and display the results accordingly.

Cloning Saved Searches

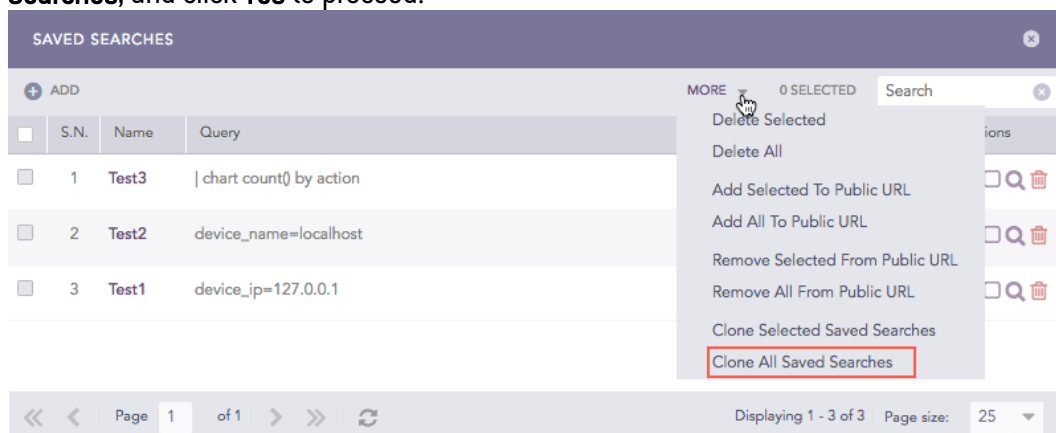
1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.
2. Click the **Manage Saved Searches** icon under the **Actions** column of the concerned search package.
3. Click the **Clone** icon under the **Actions** column for the saved search.



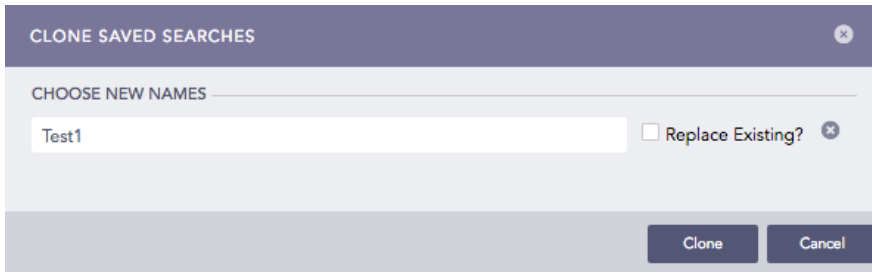
- To clone multiple saved searches, select the respective searches. Click the **More** drop-down menu, choose **Clone Selected Saved Searches** and click **Yes** to proceed.



- To clone all the saved searches, click the **More** drop-down menu, choose **Clone All Saved Searches**, and click **Yes** to proceed.



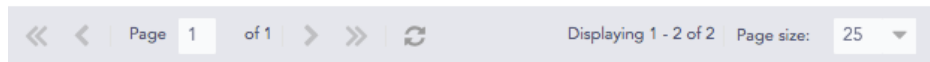
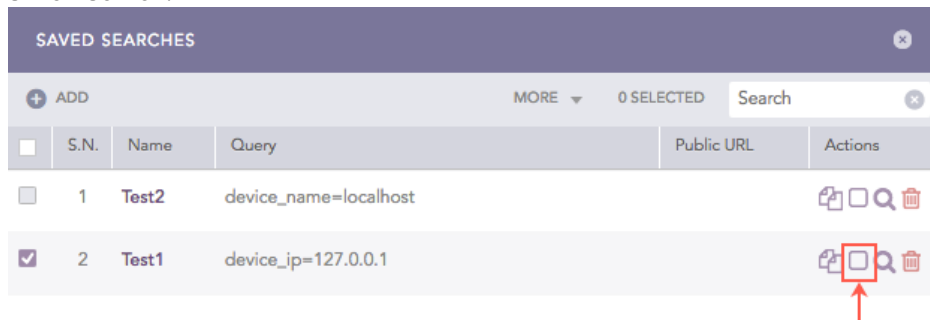
The **Cloning Saved Searches** panel opens.



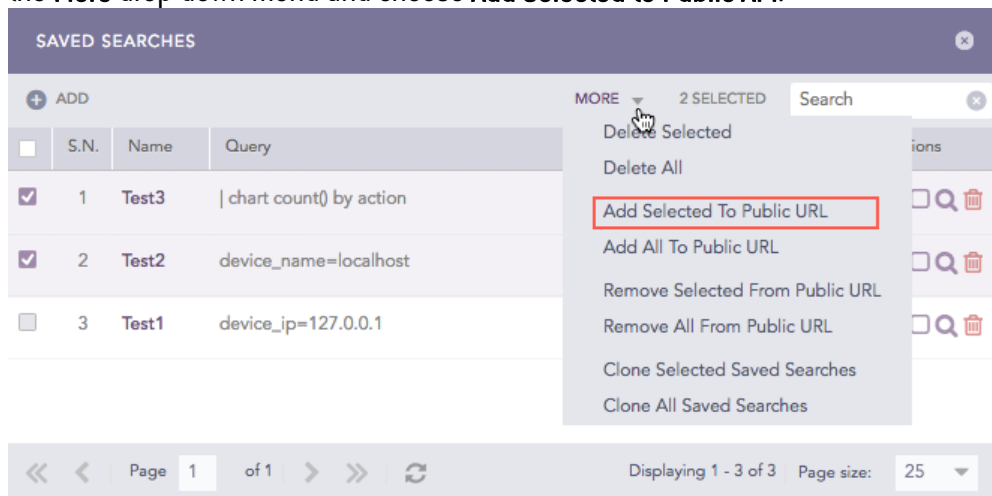
4. Enter new names for the cloned searches.
5. Check the **Replace Existing?** checkbox to replace an existing package with the same name.
6. Click **Clone**.

Registering from a Public API

1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.
2. Click the **Manage Saved Searches** icon under the **Actions** column for the search package.
3. Select the **Click to register from public api** icon under the **Actions** column of the concerned saved search.

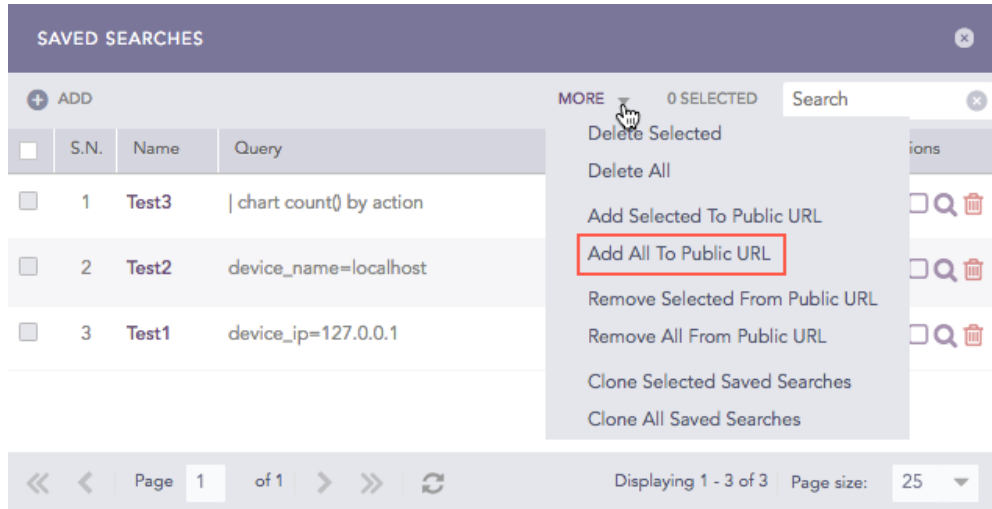


- To register multiple saved searches from a public API, select the concerned searches. Click the **More** drop-down menu and choose **Add Selected to Public API**.





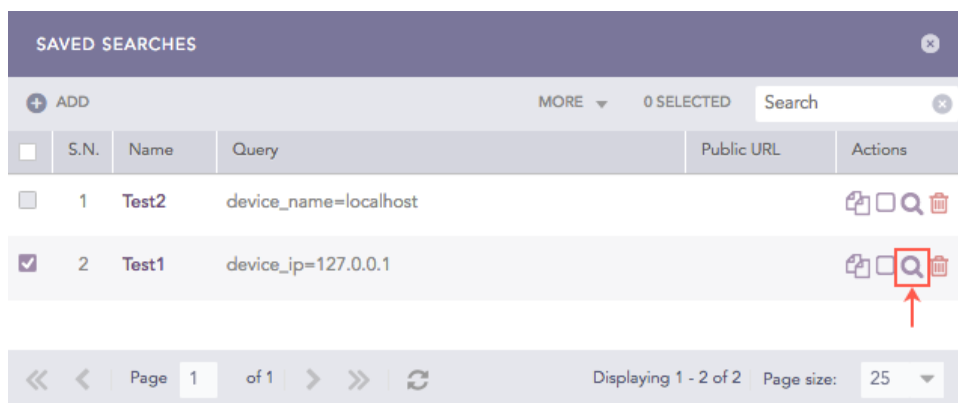
- To clone all the saved searches, click the **More** drop-down menu and choose **Add All to Public API**.



NOTE
You can unregister a saved search from the public API using the same method.

Searching a Saved Search

- Go to **Settings >> Knowledge Base** from the navigation bar and click **Search Packages**.
- Click the **Manage Saved Searches** icon under the **Actions** column of the concerned search package.
- Click the **Search** icon under the **Actions** column of the concerned saved search.

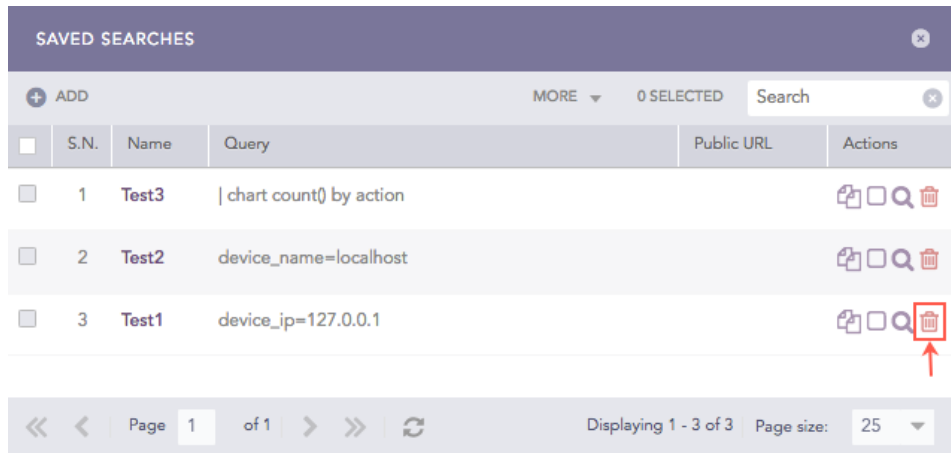


Deleting a Saved Search

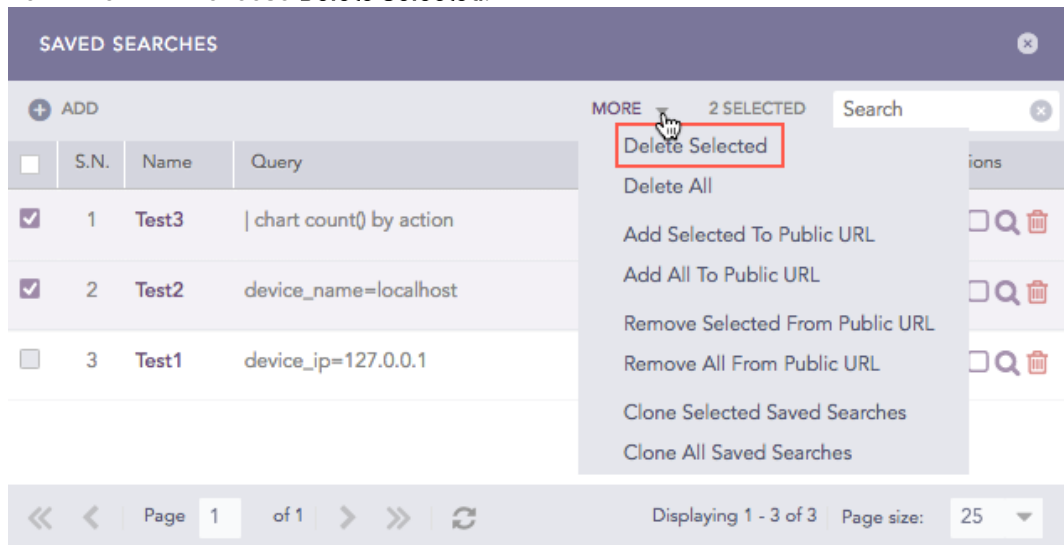
- Go to **Settings >> Knowledge Base** from the navigation bar and click **Search Packages**.
- Click the **Manage Saved Searches** icon under the **Actions** column of the concerned search package.



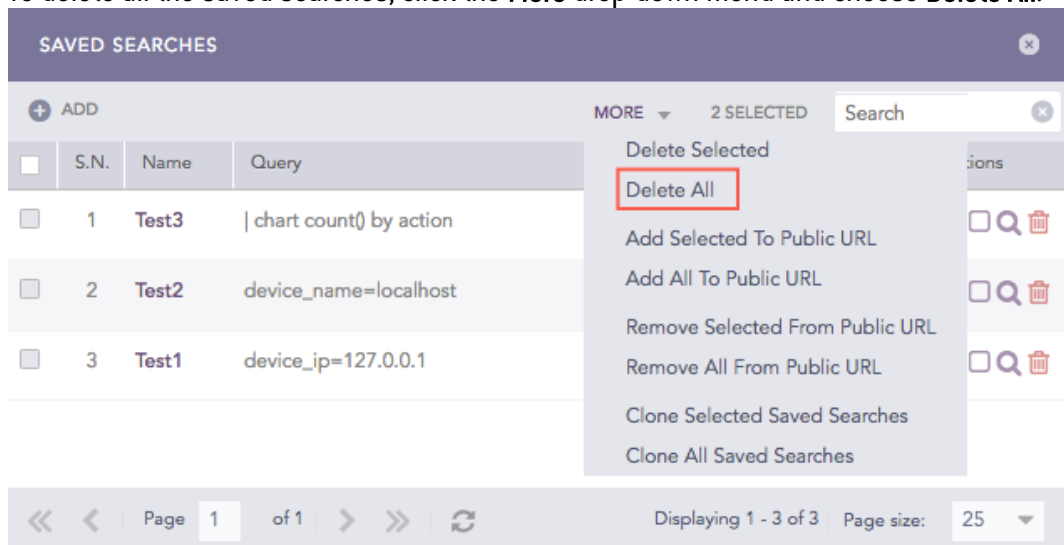
- 3. Click the **Delete** icon under the **Actions** column of the concerned saved search.



- To delete multiple saved searches, select the concerned searches. Click the **More** drop-down menu and choose **Delete Selected**.



- To delete all the saved searches, click the **More** drop-down menu and choose **Delete All**.

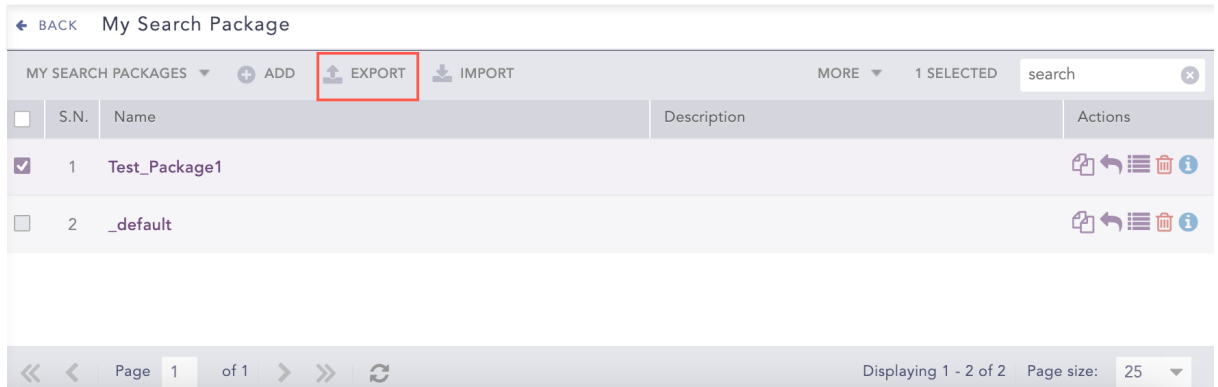


- 4. A delete confirmation dialog box appears on the screen. Click **Yes** to proceed.



Exporting Search Packages

1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.
2. Select the packages to export.



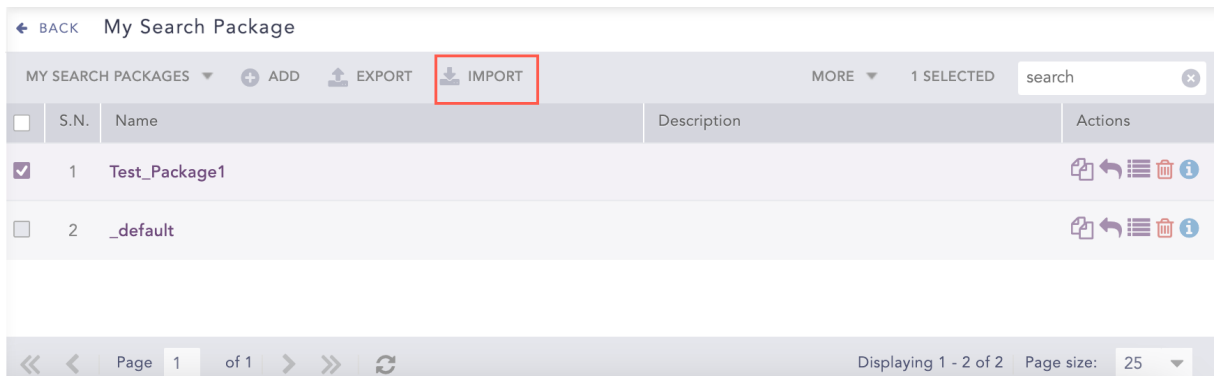
3. Click **Export**.
4. **Save** the exported package.

i NOTE

You can only export the packages in the **My Packages** section.

Importing Search Packages

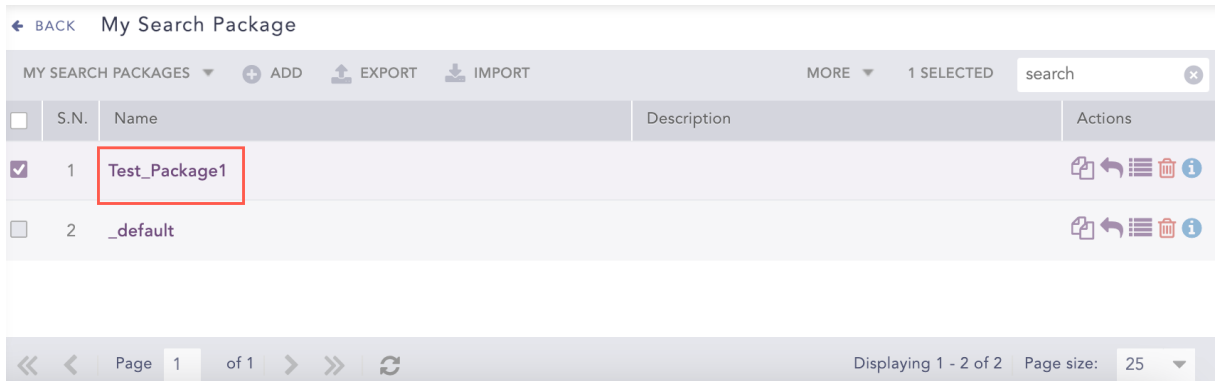
1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.



2. Click **Import**.
3. Browse for the search package file.
4. Click **Upload**.

Editing a Search Package

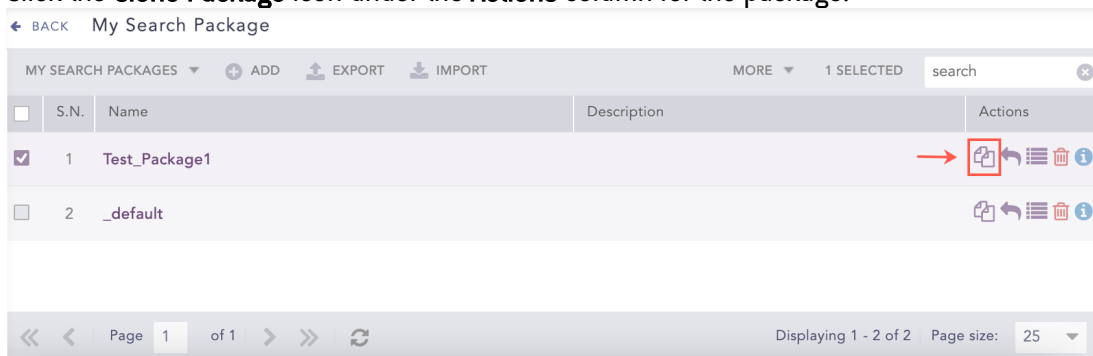
1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.
2. Click the **Name** of the package that you want to edit.



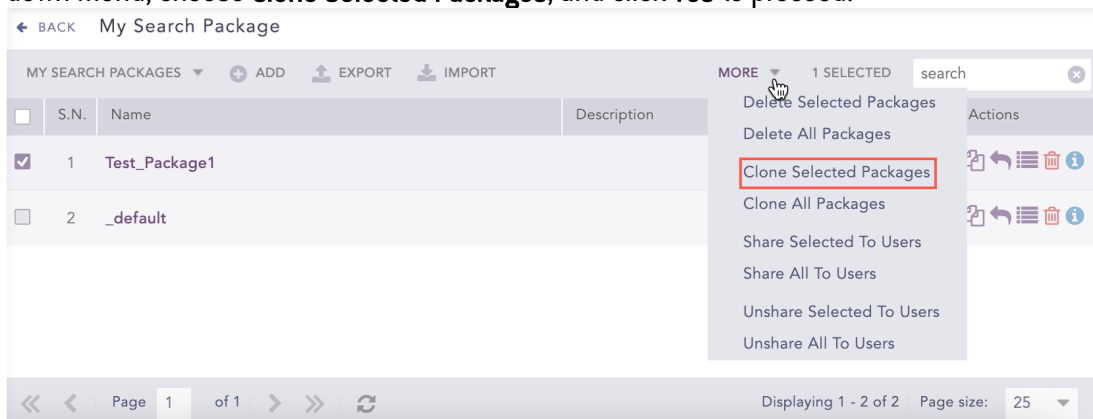
3. Update the information.
4. Click **Submit**.

Cloning Search Packages

1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.
2. Click the **Clone Package** icon under the **Actions** column for the package.

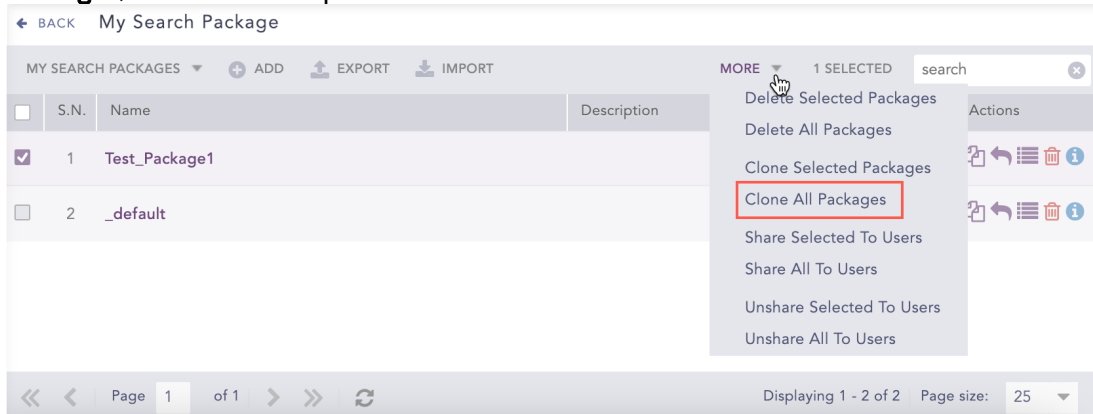


- To clone multiple Search Packages, select the concerned packages. Click the **More** drop-down menu, choose **Clone Selected Packages**, and click **Yes** to proceed.

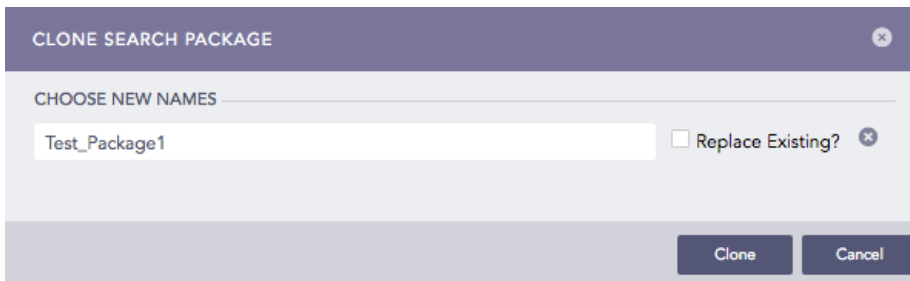




- To clone all the Search Packages, click the **More** drop-down menu, choose **Clone All Packages**, and click **Yes** to proceed.



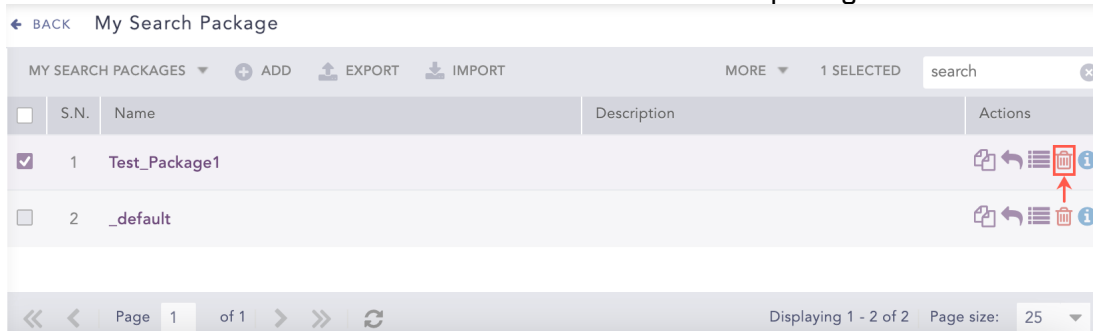
The **Clone Search Package** panel opens.



- Enter a new **Name** for the cloned package.
- Select the **Replace Existing?** checkbox to replace an existing package with the same name.
- Click **Clone**.

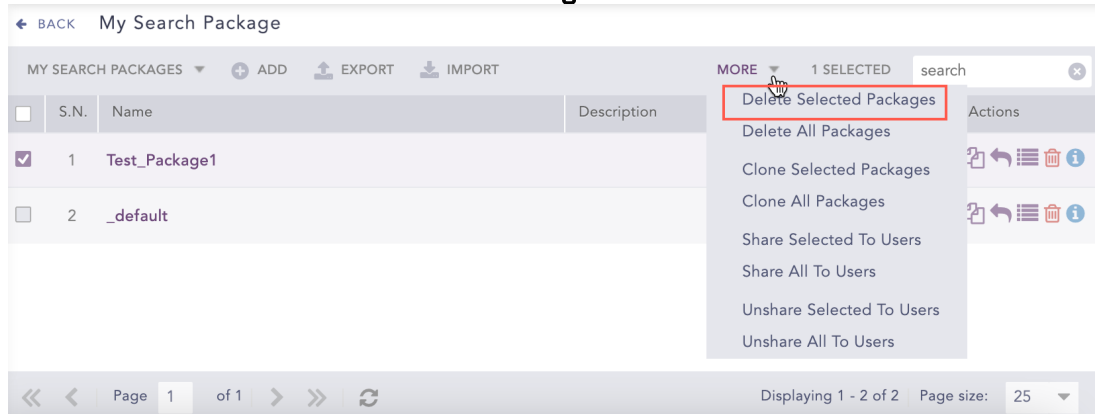
Deleting Search Packages

- Go to Settings >> Knowledge Base from the navigation bar and click **Search Packages**.
- Click the **Delete** icon under the **Actions** column of the concerned package.

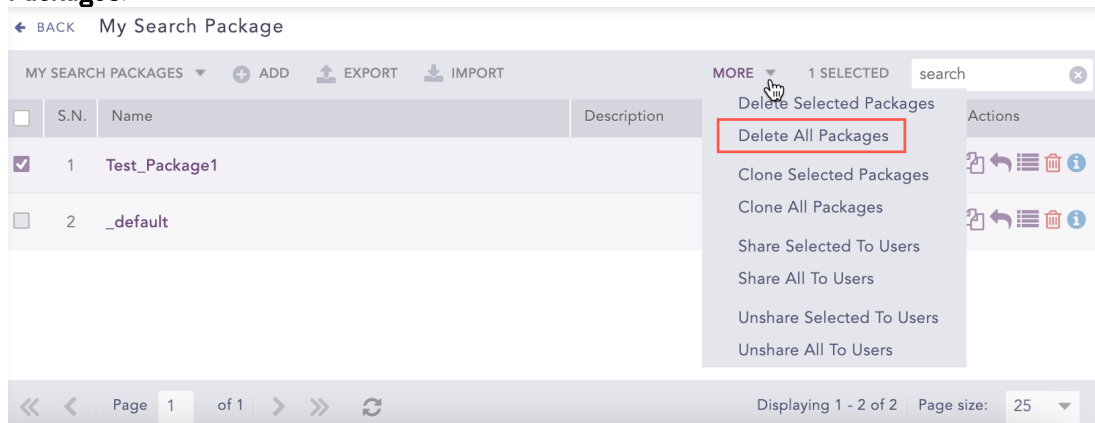




- To delete multiple Search Packages, select the respective packages. Click the **More** drop-down menu and choose **Delete Selected Packages**.



- To delete all the Search Packages, click the **More** drop-down menu and choose **Delete All Packages**.



- A delete confirmation dialog box appears on the screen. Click **Yes** to proceed.

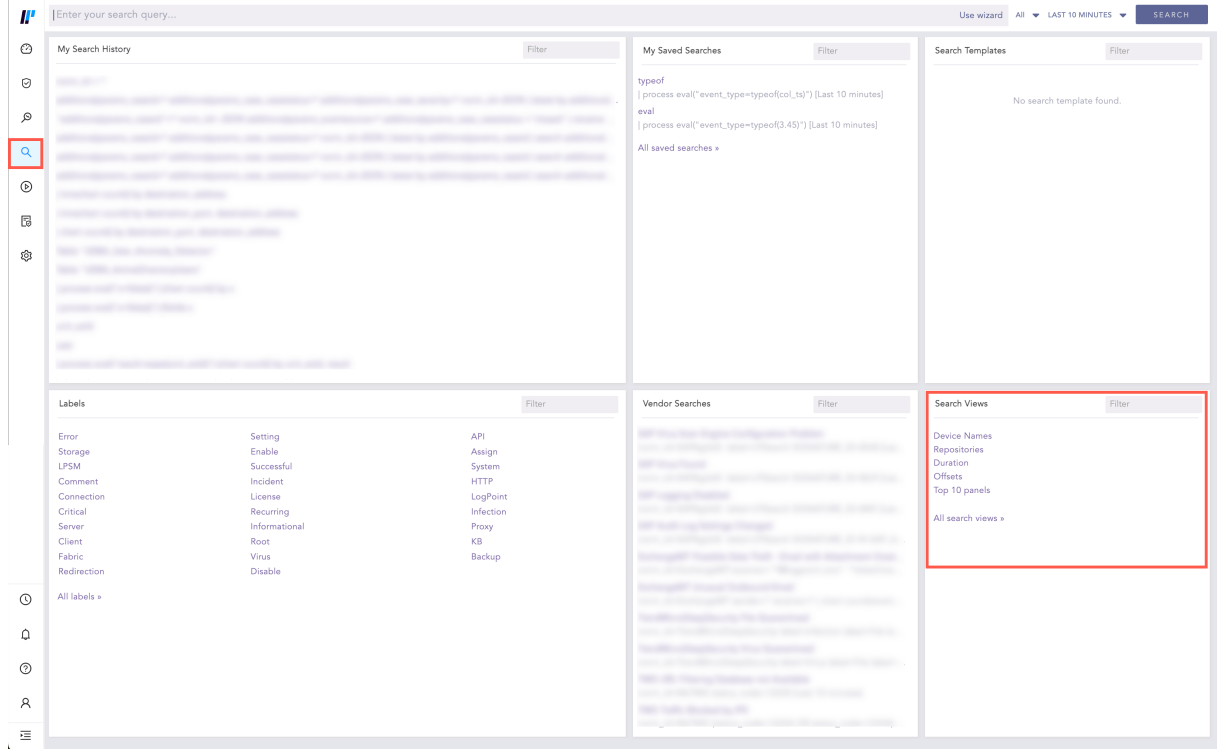


Search Views

The **Search Views** option provides you with the interface that presents the top search views.

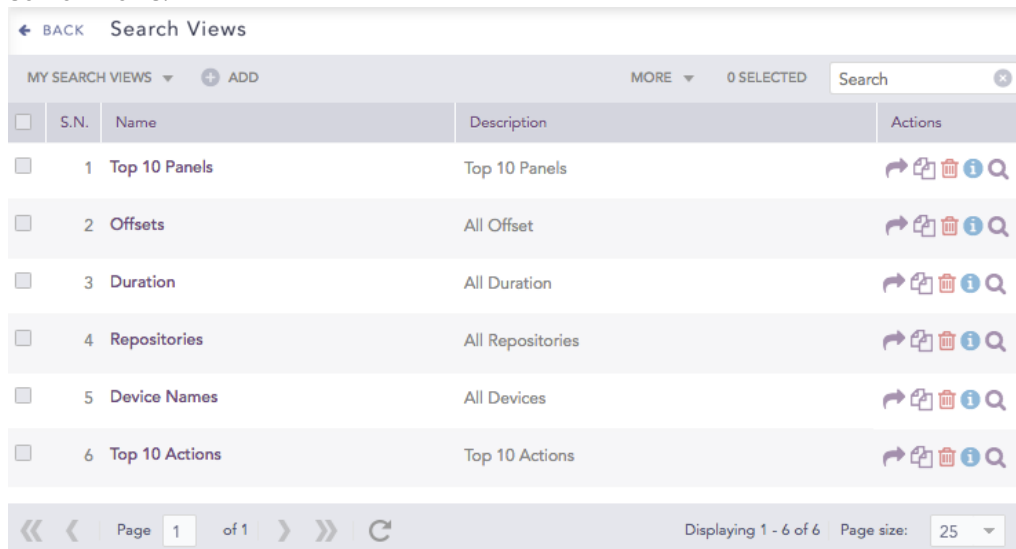
Accessing Search Views

1. Go to Search from the navigation bar.



2. From the **Search Views** section at the bottom-right corner of the page, you can:

- **See all the search views:** Select the **All Search Views** link at the bottom. SLS redirects you to the **Search Views** page. It contains a list of all the recently created search views.



- **See the search results for a single search view:** Click the search view.



SLS redirects you the **Search Views Interface**.

i NOTE

You can also filter your search by entering the desired keyword in the **filter** section.

The Search Views Interface

You can access the **Search Views Interface** page in two different ways.

- By clicking a particular search view from the `Search >> Search Views` panel.
- By clicking a particular search view from the list of **Search Views** from `Settings >> Knowledge Base` from the navigation bar and **Search Views**.

The **Search Views Interface** is divided into three sections, the **Query Bar**, the **Result Panel**, and the **Top-10 Panel**.

Query Bar

The **Query Bar** along with the **Repo selector** and **Time range** appears at the top of **Search Views Interface**.

action	col_type	device_ip	log_ts	sig_id
denied	filesystem	127.0.0.1	2018/06/04 16:51:18	19023
denied	filesystem	127.0.0.1	2018/06/04 16:50:17	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:56	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:16	19023
denied	filesystem	127.0.0.1	2018/06/04 16:48:05	19023
denied	filesystem	127.0.0.1	2018/06/04 16:47:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:44:52	19023
denied	filesystem	127.0.0.1	2018/06/04 16:43:51	19023
denied	filesystem	127.0.0.1	2018/06/04 16:40:29	19023
denied	filesystem	127.0.0.1	2018/06/04 16:39:08	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:07	19023
denied	filesystem	127.0.0.1	2018/06/04 16:36:46	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023

Limit results to: 25
Back to Search Views

Top 10 col_type

filesystem (66)

Top 10 device_ip

127.0.0.1 (66)

Top 10 log_ts

2018/06/04 16:35:35 (2)

2018/06/04 16:46:54 (2)

2018/06/04 15:55:39 (2)

2018/06/04 16:20:45 (2)

2018/06/04 16:22:56 (2)

2018/06/04 16:37:57 (2)

2018/06/04 15:52:27 (1)

Result Panel

The **Result Panel** displays the details of the selected **Search View**.



action	col_type	device_ip	log_ts	sig_id
denied	filesystem	127.0.0.1	2018/06/04 16:51:18	19023
denied	filesystem	127.0.0.1	2018/06/04 16:50:17	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:56	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:16	19023
denied	filesystem	127.0.0.1	2018/06/04 16:48:05	19023
denied	filesystem	127.0.0.1	2018/06/04 16:47:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:44:52	19023
denied	filesystem	127.0.0.1	2018/06/04 16:43:51	19023
denied	filesystem	127.0.0.1	2018/06/04 16:40:29	19023
denied	filesystem	127.0.0.1	2018/06/04 16:39:08	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:07	19023
denied	filesystem	127.0.0.1	2018/06/04 16:36:46	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023

Result Panel

Limit results to: 25

Back to Search Views

Top-10 Panel

The Top-10 Panel displays ten most frequently searched logs for a number of fields.

action	col_type	device_ip	log_ts	sig_id
denied	filesystem	127.0.0.1	2018/06/04 16:51:18	19023
denied	filesystem	127.0.0.1	2018/06/04 16:50:17	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:56	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:16	19023
denied	filesystem	127.0.0.1	2018/06/04 16:48:05	19023
denied	filesystem	127.0.0.1	2018/06/04 16:47:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:44:52	19023
denied	filesystem	127.0.0.1	2018/06/04 16:43:51	19023
denied	filesystem	127.0.0.1	2018/06/04 16:40:29	19023
denied	filesystem	127.0.0.1	2018/06/04 16:39:08	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:07	19023
denied	filesystem	127.0.0.1	2018/06/04 16:36:46	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023

Top 10 Panel

Limit results to: 25

Back to Search Views



NOTE

- You can increase the width of the **Top-10** panel by dragging the pointer towards the **Result Panel**. It gives you a comprehensive view of the **Top-10** search results.

action	col_type	device_ip	log_ts	sig_id
denied	filesystem	127.0.0.1	2018/06/04 16:51:18	19023
denied	filesystem	127.0.0.1	2018/06/04 16:50:17	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:56	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:16	19023
denied	filesystem	127.0.0.1	2018/06/04 16:48:05	19023
denied	filesystem	127.0.0.1	2018/06/04 16:47:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:44:52	19023
denied	filesystem	127.0.0.1	2018/06/04 16:43:51	19023
denied	filesystem	127.0.0.1	2018/06/04 16:40:29	19023
denied	filesystem	127.0.0.1	2018/06/04 16:39:08	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:07	19023
denied	filesystem	127.0.0.1	2018/06/04 16:36:46	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023

Limit results to: 25

Top 10 col_type
filesystem (66)

Top 10 device_ip
127.0.0.1 (66)

Top 10 log_ts
2018/06/04 16:35:35 (2)
2018/06/04 16:46:54 (2)
2018/06/04 15:55:39 (2)
2018/06/04 16:20:45 (2)
2018/06/04 16:22:56 (2)
2018/06/04 16:37:57 (2)
2018/06/04 15:52:27 (1)

Back to Search Views

- Click **Back to Search Views** at the bottom-right corner to redirect to the **Search Views List Page**.

Adding a Search View

- Go to **Settings >> Knowledge Base** from the navigation bar and click **Search Views**.

← BACK Search Views

MY SEARCH VIEWS ▾ **ADD** MORE ▾ 0 SELECTED search

S.N.	Name	Description	Actions
------	------	-------------	---------

Page 0 of 0 No data to display Page size: 25

- Click **Add** to open the **Add Search View** panel.



ADD SEARCH VIEW ✕

SEARCH VIEW INFORMATION

Name:

Description:

FIELDS TO BE USED

Add

S.N.	Field	Show on Top 10 List	Actions
1	sig_id	<input checked="" type="checkbox"/>	^ v 🗑
2	action	<input type="checkbox"/>	^ v 🗑
3	col_type	<input type="checkbox"/>	^ v 🗑

Submit Cancel

3. Provide a **Name** and a **Description**.
4. Select the fields to be used and click **Add**. These fields appear on the **Search Views Interface**.
5. Select the fields to **Show on Top 10 List**.
6. Click **Submit**.

Editing a Search View

1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Views**.
2. Click the **Name** of the view to edit.

← BACK Search Views

MY SEARCH VIEWS + ADD MORE 0 SELECTED

<input type="checkbox"/>	S.N.	Name	Description	Actions
<input type="checkbox"/>	1	Top 10 Panels	Top 10 Panels	↶ ↷ 🗑 ⓘ 🔍

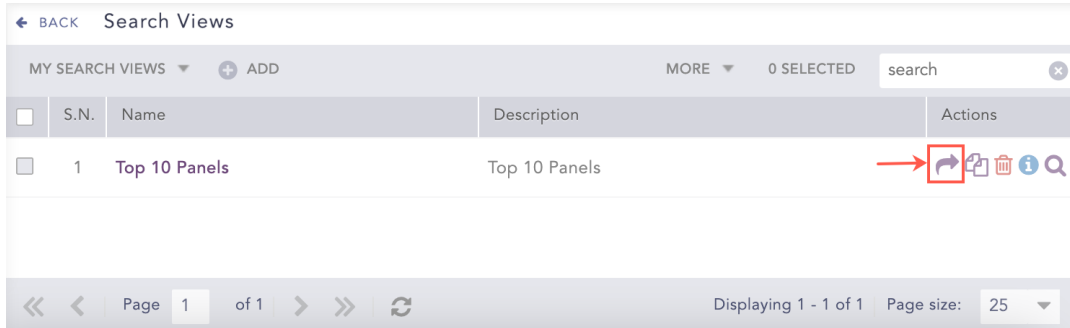
Page 1 of 1 Displaying 1 - 1 of 1 Page size: 25

3. Update the information.
4. Click **Submit**.

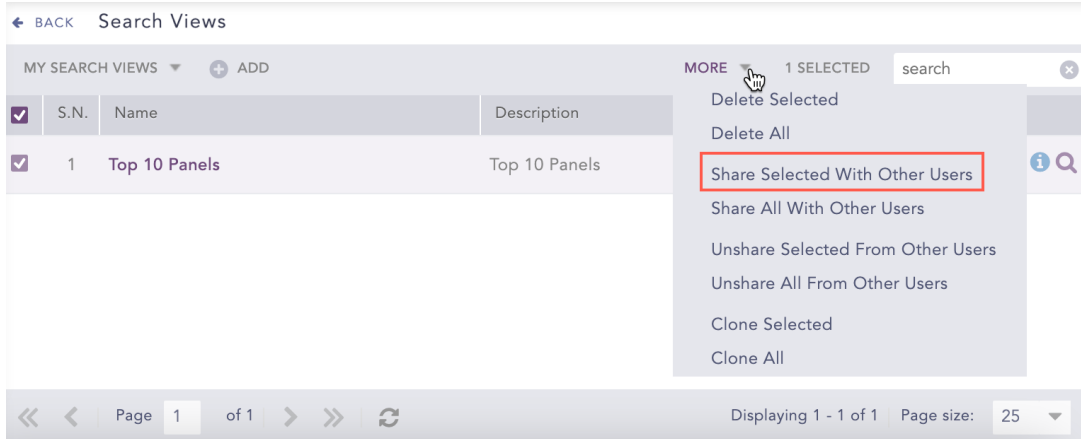


Sharing Search Views

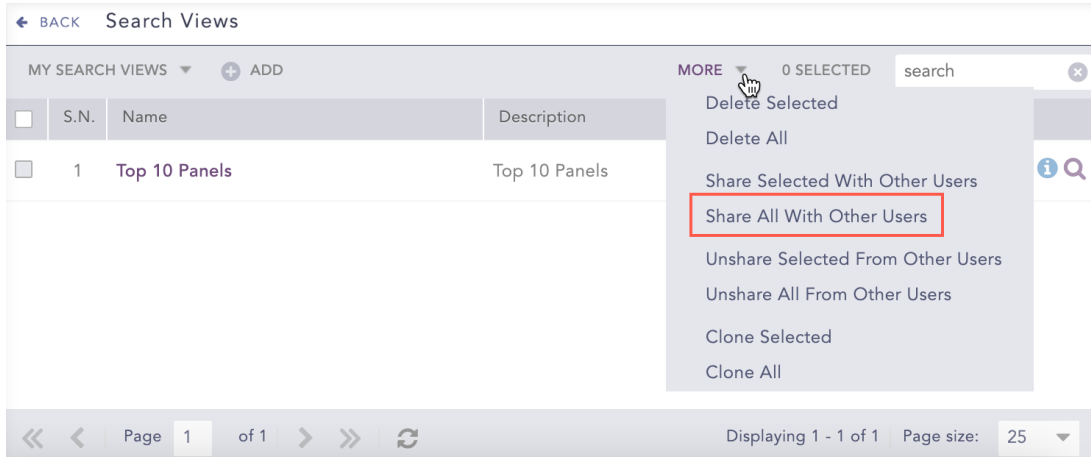
1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Views**.
2. Click the **Click to Share** icon in the **Actions** column for the view.



- To share multiple Search Views, select the concerned views. Click the **More** drop-down menu and choose **Share Selected With Other Users**.



- To share all the Search Views, click the **More** drop-down menu and choose **Share Selected With All Users**.



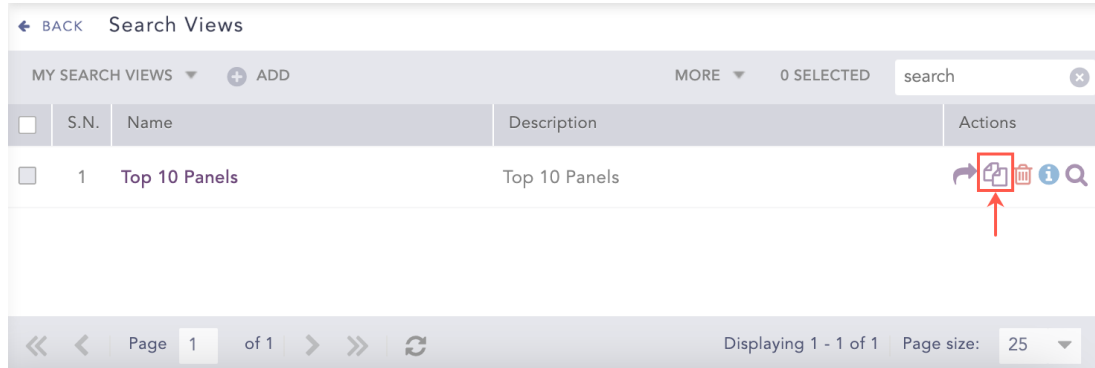
i **NOTE**

Follow the same method to **Unshare** search views.

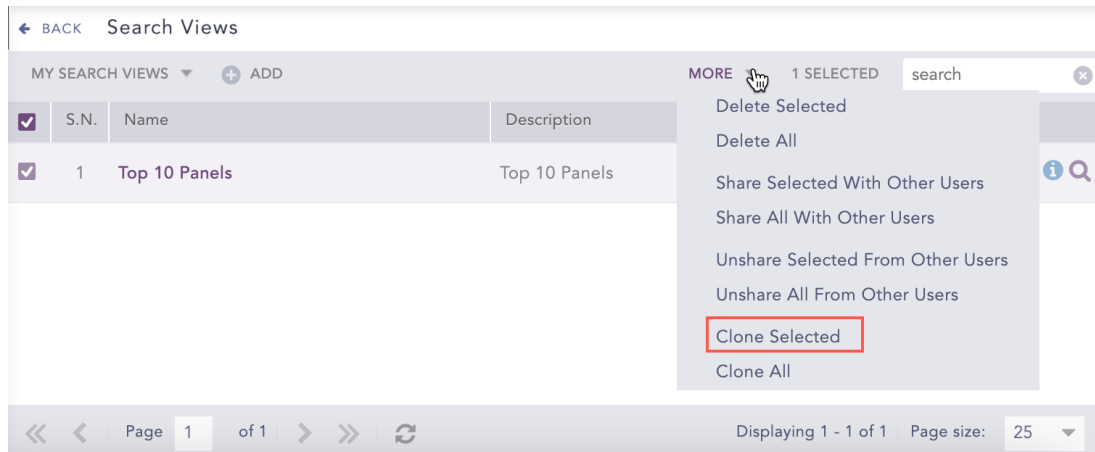


Cloning Search Views

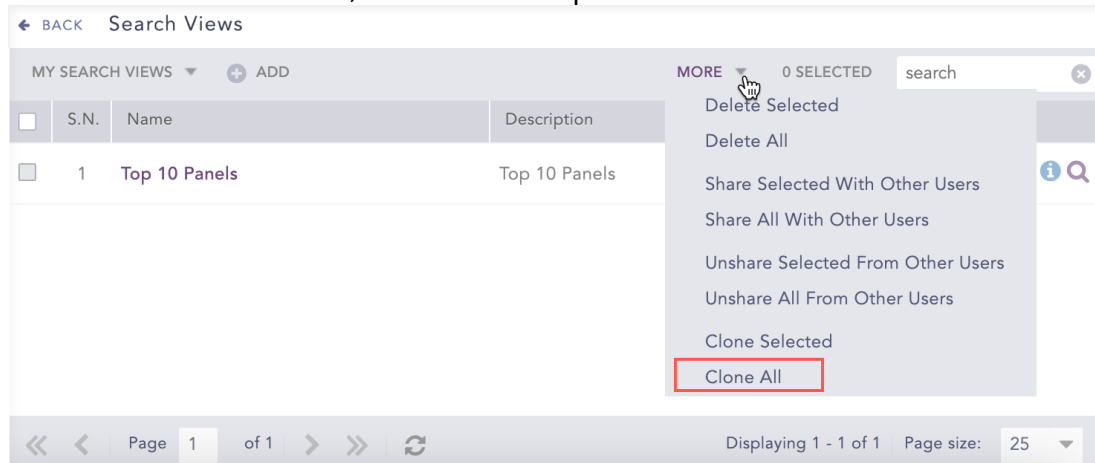
1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Views**.
2. Click the **Clone** icon in the **Actions** column for the view.



- To clone multiple Search Views, select the concerned views. Click the **More** drop-down menu and choose **Clone Selected**.



- To clone all the Search Views, click the **More** drop-down menu and choose **Clone All**.

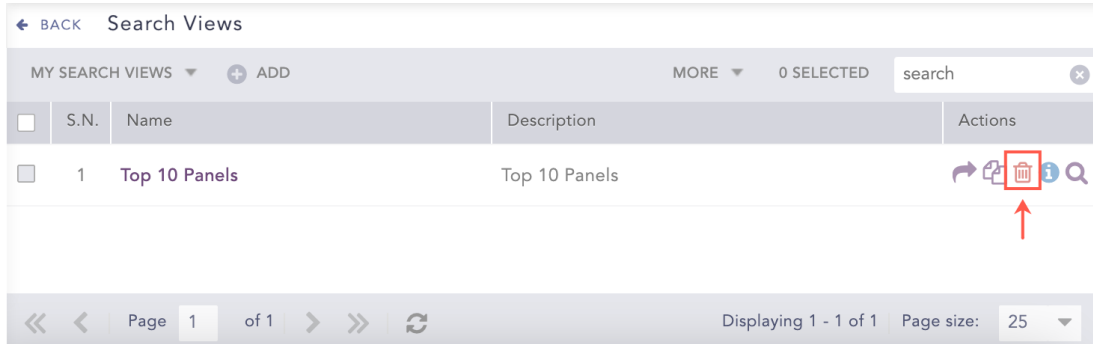


3. Enter a new **Name** for the cloned Search View.
4. Check the **Replace Existing?** checkbox to replace an existing view with the same name.
5. Click **Clone**.

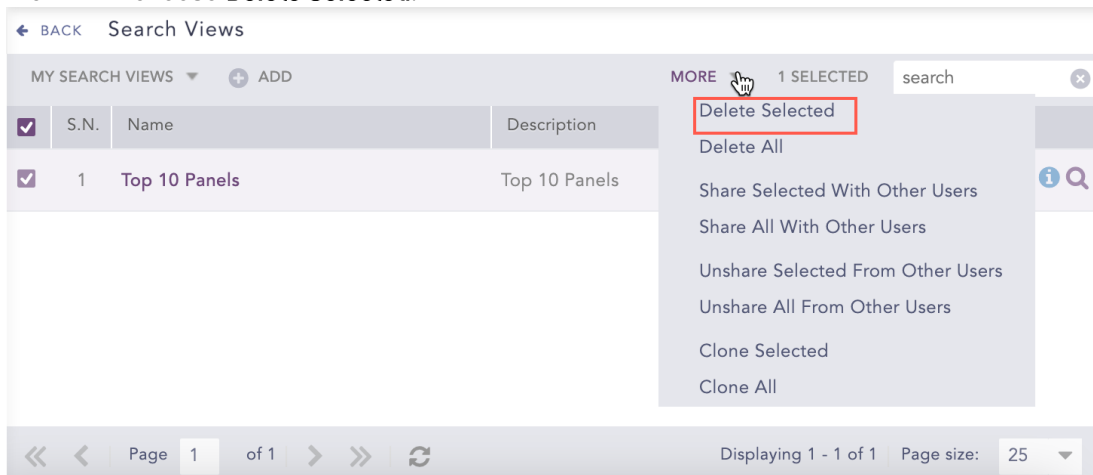


Deleting Search Views

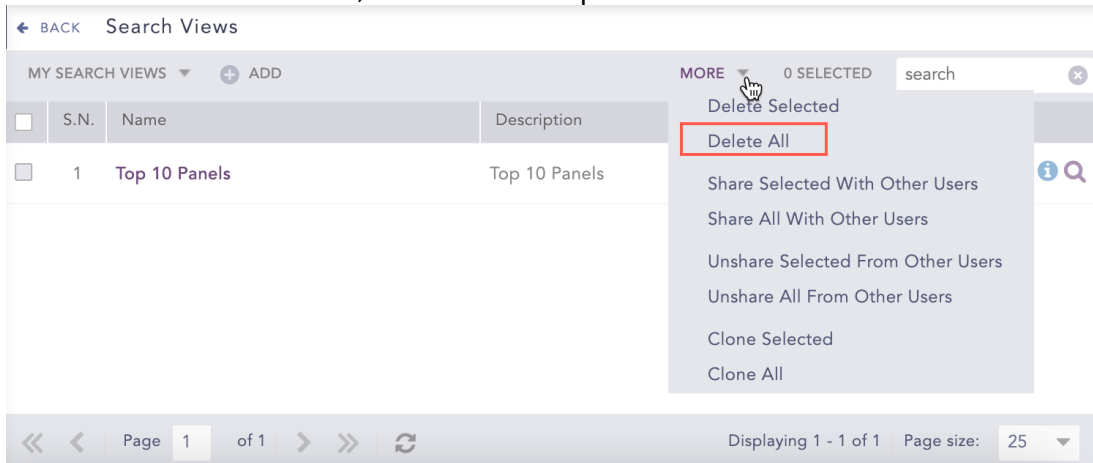
1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Views**.
2. Click the **Delete** icon in the **Actions** column for the view.



- To delete multiple Search Views, select the concerned views. Click the **More** drop-down menu and choose **Delete Selected**.



- To delete all the Search Views, click the **More** drop-down menu and choose **Delete All**.



3. A delete confirmation dialog box appears on the screen. Click **Yes** to proceed.

i NOTE

Clone, Information, and Use are the only actions available for the **Shared Search Views**.



Using a Search View

1. Go to Settings >> Knowledge Base from the navigation bar and click **Search Views**.
2. Click the **Use** icon in the **Actions** column of the concerned view.

← BACK Search Views

MY SEARCH VIEWS + ADD MORE 0 SELECTED search

<input type="checkbox"/>	S.N.	Name	Description	Actions
<input type="checkbox"/>	1	Top 10 Panels	Top 10 Panels	

Page 1 of 1 | Displaying 1 - 1 of 1 | Page size: 25

SLS redirects you to the **Search Views Interface**. Here, you can manage all the information of the selected **Search View**.

action	col_type	device_ip	log_ts	sig_id
denied	filesystem	127.0.0.1	2018/06/04 16:51:18	19023
denied	filesystem	127.0.0.1	2018/06/04 16:50:17	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:56	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:16	19023
denied	filesystem	127.0.0.1	2018/06/04 16:48:05	19023
denied	filesystem	127.0.0.1	2018/06/04 16:47:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:44:52	19023
denied	filesystem	127.0.0.1	2018/06/04 16:43:51	19023
denied	filesystem	127.0.0.1	2018/06/04 16:40:29	19023
denied	filesystem	127.0.0.1	2018/06/04 16:39:08	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:07	19023
denied	filesystem	127.0.0.1	2018/06/04 16:36:46	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023

Limit results to: 25

Top 10 col_type

filesystem (66)

Top 10 device_ip

127.0.0.1 (66)

Top 10 log_ts

2018/06/04 16:35:35 (2)

2018/06/04 16:46:54 (2)

2018/06/04 15:55:39 (2)

2018/06/04 16:20:45 (2)

2018/06/04 16:22:56 (2)

2018/06/04 16:37:57 (2)

2018/06/04 15:52:27 (1)

Back to Search Views

- The **Query Bar** appears at the top of the **Search Views Interface**. By default, the query results in the selection of all the field components.

action	col_type	device_ip	log_ts	sig_id
denied	filesystem	127.0.0.1	2018/06/04 16:51:18	19023
denied	filesystem	127.0.0.1	2018/06/04 16:50:17	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:56	19023
denied	filesystem	127.0.0.1	2018/06/04 16:49:16	19023
denied	filesystem	127.0.0.1	2018/06/04 16:48:05	19023
denied	filesystem	127.0.0.1	2018/06/04 16:47:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:46:54	19023
denied	filesystem	127.0.0.1	2018/06/04 16:44:52	19023
denied	filesystem	127.0.0.1	2018/06/04 16:43:51	19023
denied	filesystem	127.0.0.1	2018/06/04 16:40:29	19023
denied	filesystem	127.0.0.1	2018/06/04 16:39:08	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:57	19023
denied	filesystem	127.0.0.1	2018/06/04 16:37:07	19023
denied	filesystem	127.0.0.1	2018/06/04 16:36:46	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023
denied	filesystem	127.0.0.1	2018/06/04 16:35:35	19023

Limit results to: 25

Top 10 col_type

filesystem (66)

Top 10 device_ip

127.0.0.1 (66)

Top 10 log_ts

2018/06/04 16:35:35 (2)

2018/06/04 16:46:54 (2)

2018/06/04 15:55:39 (2)

2018/06/04 16:20:45 (2)

2018/06/04 16:22:56 (2)

2018/06/04 16:37:57 (2)

2018/06/04 15:52:27 (1)

Back to Search Views

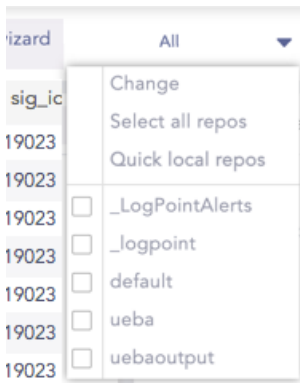
For example:



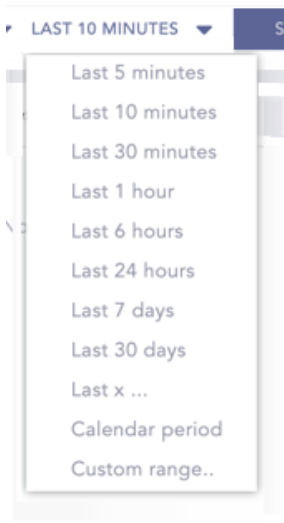
```
action=* col_type=* device_ip=* log_ts=* sig_id=*
```

i NOTE

- SLS suggests some system fields in an auto-suggest box if you type any letter(s) followed by the **space bar**.
- Use only the simple queries. SLS uses query validation to restrict the usage of **aggregators, rex, norm, and rename** commands.
- Use the **Repo selector** to specify the repos to extract the logs. By default, all the repos are selected.



- Specify the **Time range** to fetch the logs. By default, **Last 10 minutes** is selected.



- **Limit Results** to a specific number of logs per page. The default value is set to **25**.



action	col_type	device_ip	log_ts	sig_id	norm_id
indexing speed	filesystem	127.0.0.1	2018/06/05 05:43:03	10537	LogPoint
live search	filesystem	127.0.0.1	2018/06/05 05:43:03	10537	LogPoint
indexing speed	filesystem	127.0.0.1	2018/06/05 05:43:03	10537	LogPoint
live search	filesystem	127.0.0.1	2018/06/05 05:43:03	10537	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:56	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:46	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:46	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:46	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:46	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:46	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:46	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:36	10505	LogPoint
Alert received	filesystem	127.0.0.1	2018/06/05 05:42:36	10510	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:36	10505	LogPoint
reporting speed	filesystem	127.0.0.1	2018/06/05 05:42:35	10505	LogPoint

Top 10 action

- reporting speed (38722)
- indexing speed (5284)
- live search (3160)
- performed (321)
- Alert received (209)
- read (48)
- edited (5)
- Starting (5)
- login (4)
- Login - Successful (4)

Top 10 col_type

- filesystem (47763)

Top 10 norm_id

- LogPoint (47763)

Limit results to: 100 [Back to Search Views](#)

NOTE

- You can administer the **Search Views** for the remote SLSs from the **Distributed SLS** drop-down menu on the **Header Bar** inside the **Settings** menu.
- In the **Data Privacy Module** enabled systems, users with the **Can Request Access** privilege can only view the values in the encrypted form. These encrypted values cannot be requested for decryption.



Macros

A **Macro** lets you save any search query in a single name and re-use it in the system. You can use macros with other search queries in the Search, Dashboards, Reports, Alert Rules, Label Packages, Search Packages and Search Templates. You can also add as many macros as needed or update the same macro several times. This lets you use a macro in different settings but update in one place.

Adding Macros

1. Go to **Settings >> Knowledge Base** from the navigation bar and click **Macros**.
2. Click **Add** to open the **Macros** panel.

The screenshot shows a modal window titled "MACROS" with a close button (X) and a help button (?). Below the title is a section labeled "MACRO INFORMATION". It contains two input fields: "Name:" with the value "admin_log" and "Query:" with the value "user_admin". At the bottom right of the modal are two buttons: "Submit" and "Cancel".

3. Provide a **Name** for the macro. The field supports alpha-numeric and underscore () characters.
4. In the **Query** field, provide a complete and valid query.

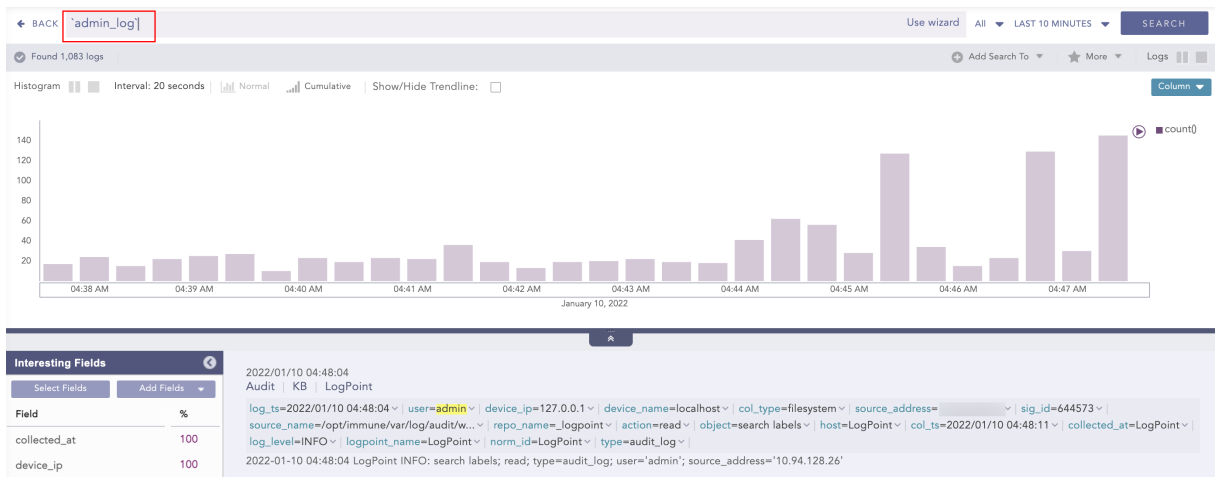
i NOTE

An invalid query results in error. Click the error sign right next to the query bar for details.

5. Click **Submit**.

Searching with Macros

In the **Search** tab of SLS, you can search for various types of logs using macros. When you use macros, put a backtick character (`) before and after the macro name. You can use multiple macros in a single search. You can view the search query defined in the macro from the Macros page under **Settings >> Knowledge Base** from the navigation bar.



Moreover, you can add the macros to the Dashboard, Alert Rule, Labelling Rule, Incident and Public URL by clicking the **Add Search To** option. Refer to the **Add Search To** section for more details.

Updating Macros

1. Go to Settings >> Knowledge Base from the navigation bar and click **Macros**.
2. Click the macro you want to update, and the **Macros** panel opens up.

The screenshot shows the 'Macros' management interface. At the top, there are buttons for 'ADD', 'EXPORT', and 'IMPORT', along with a search bar and a '0 SELECTED' indicator. Below this is a table with the following columns: S.N., Name, Query, and Actions.

S.N.	Name	Query	Actions
1	admin_log	user=admin	

A red arrow points to the 'admin_log' macro name in the table. At the bottom of the interface, there is a pagination bar showing 'Page 1 of 1' and a 'Page size: 25' dropdown.

3. Update the **Name** or **Query**.
4. Click **Submit**.

NOTE

When you update a macro, it is auto-updated in all the settings that use the macro.

Deleting Macros

1. Go to Settings >> Knowledge Base from the navigation bar and click **Macros**.
2. Click the **Delete** icon under the **Actions** column to open the **Confirmation** panel.



<input type="checkbox"/>	S.N.	Name	Query	Actions
<input type="checkbox"/>	1	admin_log	user=admin	

3. Click **Yes**.

NOTE
Before deleting a macro, make sure to remove it from all the Setting items.

ERROR

Unable to delete macro

Hide details ^

1 Error

Macro `admin_log` is being used in Alert Rule "admin_action"

Ok

Importing Macros

1. Go to **Settings >> Knowledge Base** from the navigation bar and click **Macros**.
2. Click **Import** to open the **Import** panel.

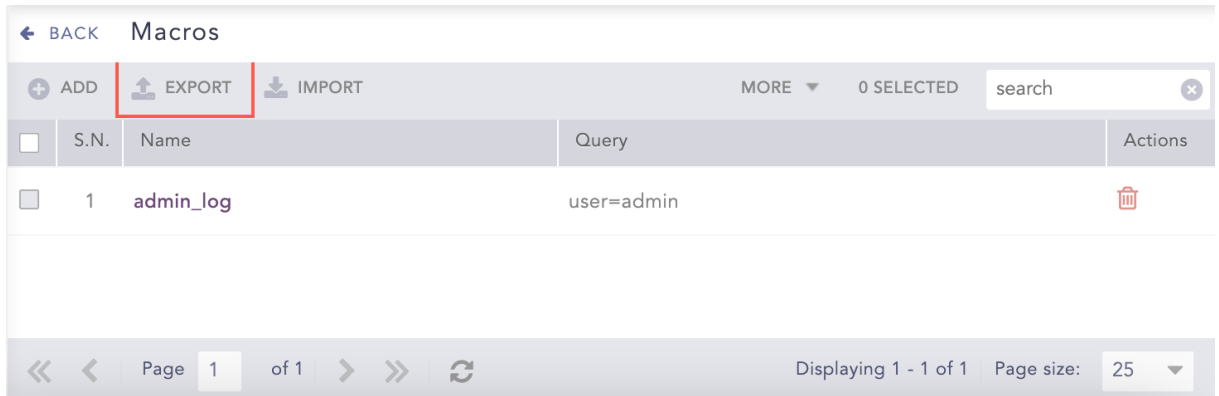
<input type="checkbox"/>	S.N.	Name	Query	Actions
<input type="checkbox"/>	1	admin_log	user=admin	

3. Browse the file to import.
4. Click **Submit**.



Exporting Macros

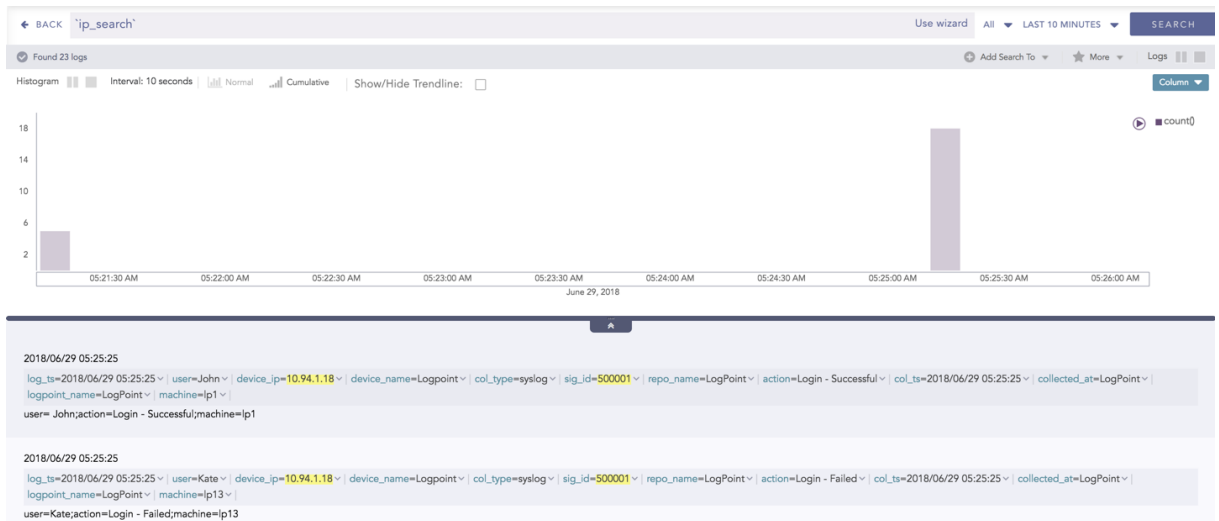
1. Go to Settings >> Knowledge Base from the navigation bar and click **Macros**.
2. Select the macros to export.
3. Click **Export**.



Examples of Macros

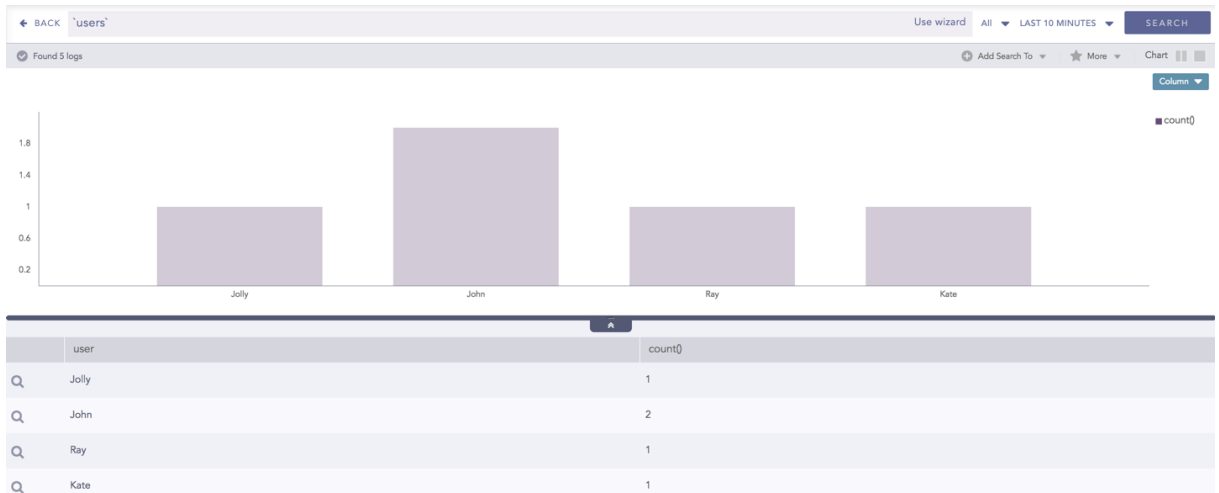
Example 1: Simple search in macros

1. Create a macro named **ip_search** with the following query:
`device_ip=10.94.1.18 sig_id=500001`
2. In the search query bar, type ``ip_search`` and click **Search**.
The above example searches for all the log messages with the **device_ip** as 10.94.1.18 and **sig_id** as 500001.



Example 2: Aggregation function in macros

1. Create a macro named **users** with the following query:
`device_ip=10.94.1.18 | chart count() by user`
2. In the search query bar, type ``users`` and click **Search**.
The above example searches for all the log messages with the **device_ip** as 10.94.1.18, group them by **user**, and displays the count of the log messages for each **user**.



Example 3: Evaluation process command and Aggregation function in macros

1. Create a macro named **eval_revenue** with the following query:

```
| process eval("Revenue=unit_sold*Selling_price") | fields unit_sold, Selling_price, Revenue
```
2. In the search query bar, type ``eval_addition`` and click **Search**.
 The above example calculates the value of **Revenue** by multiplying the values of **unit_sold** and **Selling_price**, and shows the corresponding values of all the three fields in a tabular form.

unit_sold	Selling_price	Revenue
4	1202	4808
6	1205	7230
14	1400	19600
2	1207	2414
20	1508	30160

Example 4: Multiple macros in a single search

In the search query bar, type `user=Jolly `ip_search` `eval_revenue`` and click **Search**.
 The above example first searches for the logs with the **user** as Jolly. It then searches for the logs with **device ip** as 10.94.1.18 and **sig id** as 500001 (as defined in the ip search macro). From these logs, it then calculates the revenue and shows the result in a tabular form (as defined in the eval_revenue macro).

unit_sold	Selling_price	Revenue
2	1207	2414

NOTE

While importing the Setting items that use macros, make sure the macros are present in the system.



Search Templates

A **Search Template** stores search queries with placeholders. The stored queries are called **base queries**.

The placeholders in the base queries are used as variables which you can replace with actual search keywords during runtime. You can save multiple base queries in a search template and use them to run search queries or create dashboard widgets.

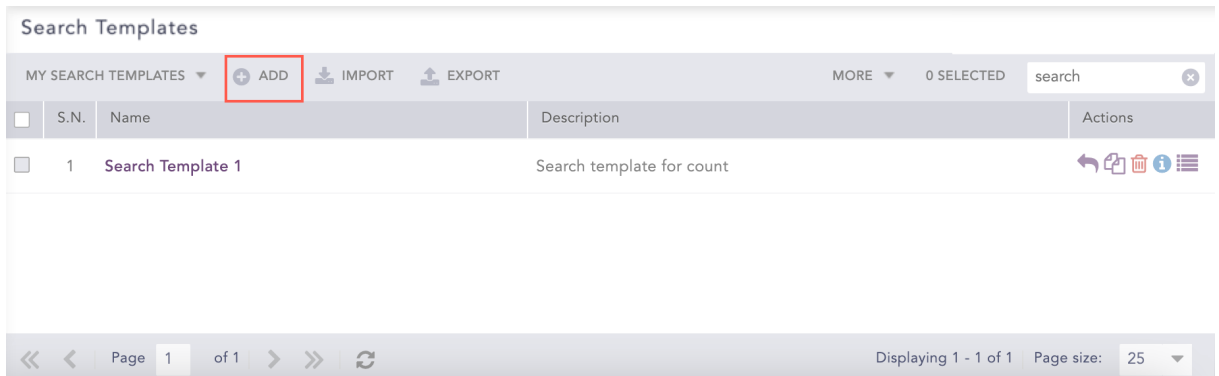
My Search Templates contains all the search templates you have created or cloned. The **Search Templates** by vendors are grouped under **Vendor Search Templates** and those shared by other users are grouped under **Shared Search Templates**.

Creating a Search Template

1. Go to Search Templates from the navigation bar.



2. Click Add.



3. Provide a Name and a Description.



Field	Display Text	Value	Actions
grouper	Group By	source_address	

4. Enter the base queries in the **Basequery list** section. Enter a **name** and a **query** for each base query.

i NOTE

- Use **{{ and }}** to enclose placeholders in the queries.
- Click the **Plus** icon to add new **base query** fields and the **Minus** icon to remove the corresponding field.

5. In the **Fields** section, enter a **Field** used as a placeholder in any of the base queries, a **Display Text** for the field, and a default **Value**.

i NOTE
You can provide multiple values for **Field**, **Display Text**, and **Value**.

6. Click **Submit**.

i NOTE
Click the **?** icon near the top-right corner to get help on the inputs.

Exporting Search Templates

1. Go to **Search Templates** from the navigation bar.
2. Select the templates to export.



The screenshot shows the 'Search Templates' interface. At the top, there is a header with 'MY SEARCH TEMPLATES', '+ ADD', 'IMPORT', and 'EXPORT' buttons. The 'EXPORT' button is highlighted with a red box. Below the header is a table with columns: S.N., Name, Description, and Actions. The table contains one row: S.N. 1, Name 'Search Template 1', Description 'Search template for count', and Actions (edit, delete, info, list). At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 1 of 1'.

3. Click **Export**.
4. **Save** the exported template.

Importing Search Templates

1. Go to **Search Templates** from the navigation bar.

The screenshot shows the 'Search Templates' interface. At the top, there is a header with 'MY SEARCH TEMPLATES', '+ ADD', 'IMPORT', and 'EXPORT' buttons. The 'IMPORT' button is highlighted with a red box. Below the header is a table with columns: S.N., Name, Description, and Actions. The table contains one row: S.N. 1, Name 'Search Template 1', Description 'Search template for count', and Actions (edit, delete, info, list). At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 1 of 1'.

2. Click **Import**.
3. Browse for the template package file.
4. Click **Upload**.

Editing a Search Template

1. Go to **Search Templates** from the navigation bar.
2. Click the **Edit** icon in the **Actions** column of the search template.

The screenshot shows the 'Search Templates' interface. At the top, there is a header with 'MY SEARCH TEMPLATES', '+ ADD', 'IMPORT', and 'EXPORT' buttons. Below the header is a table with columns: S.N., Name, Description, and Actions. The table contains three rows: S.N. 1, Name 'Demo Template 3', Description 'Search Template Demo'; S.N. 2, Name 'Demo Template 2', Description 'Another Search Template Demo'; S.N. 3, Name 'Demo Template 1', Description 'Search Template Demo'. The 'Edit' icon in the Actions column of the first row is highlighted with a red box. At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 3 of 3'.

3. Update the information.
4. Click **Submit**.



Sharing Search Templates

You can share a search template with all the users in the system and give them the read, edit, or full permissions. Any changes made in the search templates are visible to all the shared users.

Each parameter in a shared search template is categorized into three types:

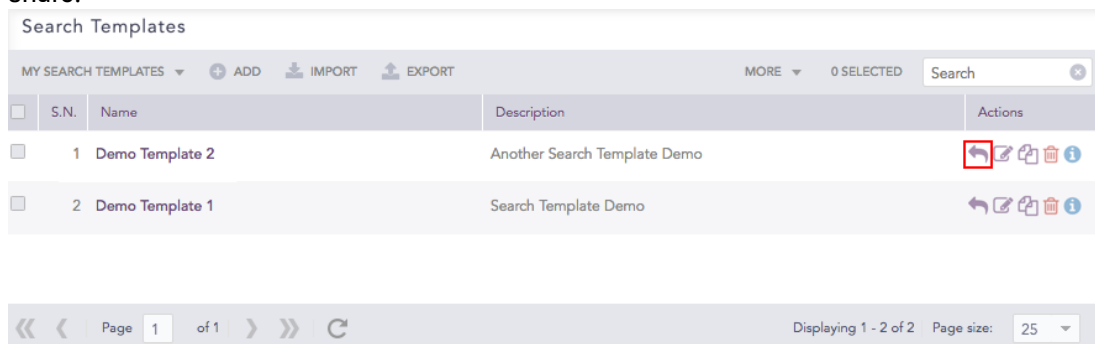
1. **Global parameters** can be changed only by the users with the **Edit** or **Full** permissions. Changes in the global parameters are reflected for all the users using the shared search template. The following parameters are global:
 - The name, description, queries, and field values of the search template.
 - Title and order of tabs, including creation and deletion of tabs.
 - Title, query, dimensions, and positions of widgets, including addition and deletion of widgets.
2. **Personalized parameters** can be changed by all the users. However, the changes in the personalized parameters are reflected only for the users making the change. The following parameters are personalized:
 - The updateable parameters
 - Selected repos
 - Time range
3. **Hybrid parameters** can be changed by all the users. If the user changing the parameters has the **Edit** or **Full** permissions, the changes are reflected for all the users. However, if the user has only the **Read** permission, the changes are reflected only for the user making the change. The following parameters are hybrid:
 - Chart types of widgets
 - Legends and legend labels of widgets
 - Trend state of widgets

NOTE

- If a user with the **Edit** or **Full** permissions changes a hybrid parameter, the changes made by all other users are overridden.
- A user with the **Full** permission can also **Share** and **Delete** a shared search template.

To share a search template:

1. Go to **Search Templates** from the navigation bar.
2. Click the **Share Template** icon under the **Actions** column of the template you would like to share.





- To share multiple Search Templates, select the respective templates. Click the **More** drop-down and choose **Share Selected With Other Users**.

Search Templates

MY SEARCH TEMPLATES + ADD IMPORT EXPORT MORE 2 SELECTED Search

<input type="checkbox"/>	S.N.	Name	Description
<input checked="" type="checkbox"/>	1	Demo Template 3	
<input checked="" type="checkbox"/>	2	Demo Template 2	Another Search Template Demo
<input type="checkbox"/>	3	Demo Template 1	Search Template Demo

Page 1 of 1

More menu options: Delete Selected, Delete All, **Share Selected With Other Users**, Share All With Other Users, Unshare Selected From Other Users, Unshare All From Other Users, Clone Selected, Clone All

- To share all the Search Templates, click the **More** drop-down and choose **Share All With Other Users**.

Search Templates

MY SEARCH TEMPLATES + ADD IMPORT EXPORT MORE 2 SELECTED Search

<input type="checkbox"/>	S.N.	Name	Description
<input type="checkbox"/>	1	Demo Template 3	
<input type="checkbox"/>	2	Demo Template 2	Another Search Template Demo
<input type="checkbox"/>	3	Demo Template 1	Search Template Demo

Page 1 of 1

More menu options: Delete Selected, Delete All, Share Selected With Other Users, **Share All With Other Users**, Unshare Selected From Other Users, Unshare All From Other Users, Clone Selected, Clone All

- Select the users groups for all the users you want to share the search templates.

SHARE SEARCH TEMPLATE

User Group: LogPoint Administrator User Account Administrator

User Groups	Read	Edit	Full
<input type="checkbox"/> LogPoint Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> User Account Administrator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> johndoe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> janedoe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Submit Cancel

- Select the **Read**, **Edit**, or **Full** permissions for the users. Refer to the introduction section of [Sharing Search Templates](#) for details on user permissions.
- Click **Submit**.



i NOTE
You can unshare a search template by removing the permissions for all the user groups from the **Share Search Template** panel.

Deleting a Shared Search Template's Owner

1. Go to **Settings >> User Accounts** from the navigation bar and click **Users**.
2. De-activate the user by clicking the **De-Activate User** icon in the **Actions** column.
3. Click **Manage De-Activated Users**.
4. Click the **Delete** icon in the **Actions** column of the user.
5. Click **Yes**.

i NOTE
While deleting a shared search template's owner, you must delete the shared template or transfer the template's ownership to another user. You can do this from the **Transfer Ownership** panel that appears when you attempt to delete a user whose template is being shared.

6. To transfer the ownership, select a user from the drop-down and click **Submit**.

Username	Shared Item	Name
johndoe	Search Template	Search Template 1

ASSIGN TO USER

admin

Delete Submit Cancel

i NOTE
The transferred template is listed in the **Search Templates** page in the owner's system.

7. To delete the user and user's template without transferring their ownership, click **Delete**.

Username	Shared Item	Name
johndoe	Search Template	Search Template 1

ASSIGN TO USER

admin

Delete Submit Cancel



Cloning Search Templates

1. Go to Search Templates from the navigation bar.
2. Click the **Clone** icon under the **Actions** column of the template.

	S.N.	Name	Description	Actions
<input type="checkbox"/>	1	Demo Template 2	Another Search Template Demo	
<input type="checkbox"/>	2	Demo Template 1	Search Template Demo	

Page 1 of 1 | Displaying 1 - 2 of 2 | Page size: 25

- To clone multiple Search Templates, select the templates. Click the **More** drop-down and choose **Clone Selected Templates**.

	S.N.	Name	Description	Actions
<input checked="" type="checkbox"/>	1	Demo Template 3		
<input checked="" type="checkbox"/>	2	Demo Template 2	Another Search Template Demo	
<input type="checkbox"/>	3	Demo Template 1	Search Template Demo	

MORE 2 SELECTED

- Delete Selected
- Delete All
- Share Selected With Other Users
- Share All With Other Users
- Unshare Selected From Other Users
- Unshare All From Other Users
- Clone Selected**
- Clone All

- To clone all the Search Templates, click the **More** drop-down and choose **Clone All Templates**.

	S.N.	Name	Description	Actions
<input type="checkbox"/>	1	Demo Template 3		
<input type="checkbox"/>	2	Demo Template 2	Another Search Template Demo	
<input type="checkbox"/>	3	Demo Template 1	Search Template Demo	

MORE 2 SELECTED

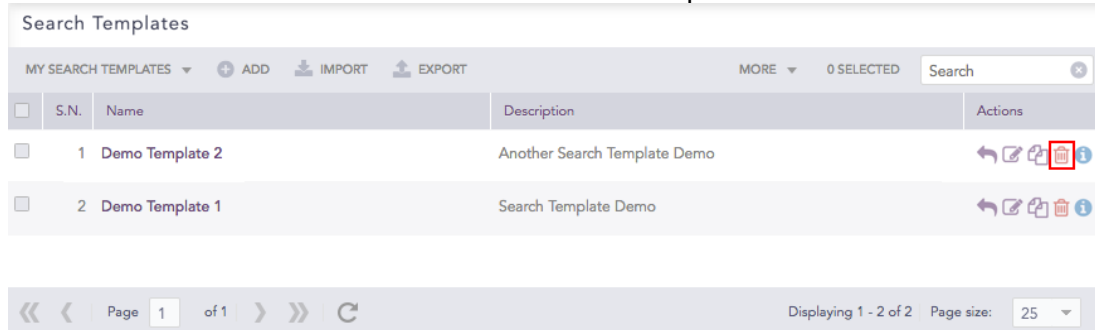
- Delete Selected
- Delete All
- Share Selected With Other Users
- Share All With Other Users
- Unshare Selected From Other Users
- Unshare All From Other Users
- Clone Selected
- Clone All**

3. Enter a new **Name** for the cloned template.
4. Select the **Replace Existing?** checkbox to replace an existing template with the same name.
5. Click **Clone**.

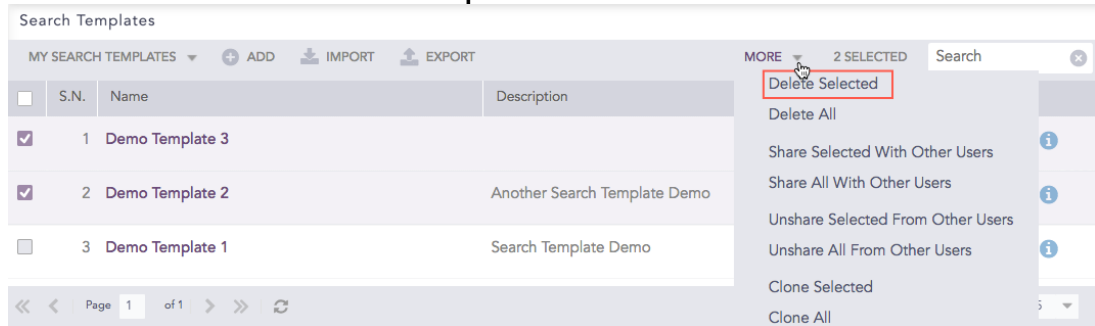


Deleting Search Templates

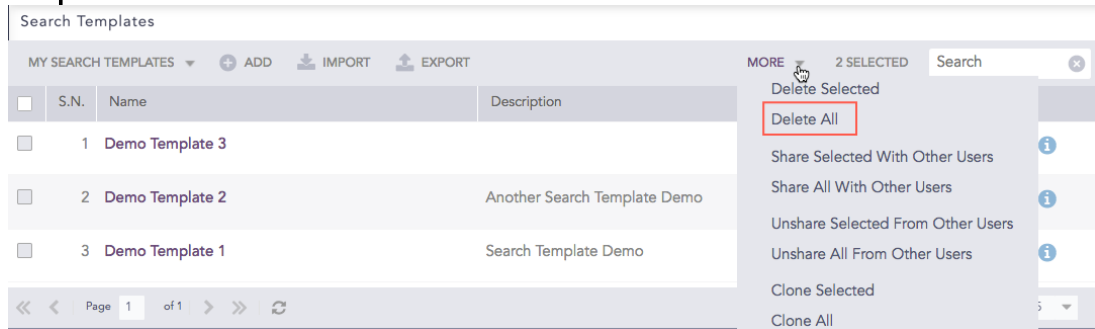
1. Go to *Search Templates* from the navigation bar.
2. Click the **Delete** icon under the **Actions** column of the template.



- To delete multiple Search Templates, select the respective templates. Click the **More** drop-down and choose **Delete Selected Templates**.



- To delete all the Search Templates, click the **More** drop-down and choose **Delete All Templates**.



3. A delete confirmation dialog box appears on the screen. Click **Yes** to proceed.

Viewing a Search Template

1. Go to *Search Templates* from the navigation bar.
2. Click the **Name** of the template.



Search Templates							
MY SEARCH TEMPLATES		+	IMPORT	EXPORT	MORE	0 SELECTED	Search
<input type="checkbox"/>	S.N.	Name	Description	Actions			
<input type="checkbox"/>	1	Demo Template 2	Another Search Template Demo				
<input type="checkbox"/>	2	Demo Template 1	Search Template Demo				

Page 1 of 1 Displaying 1 - 2 of 2 Page size: 25

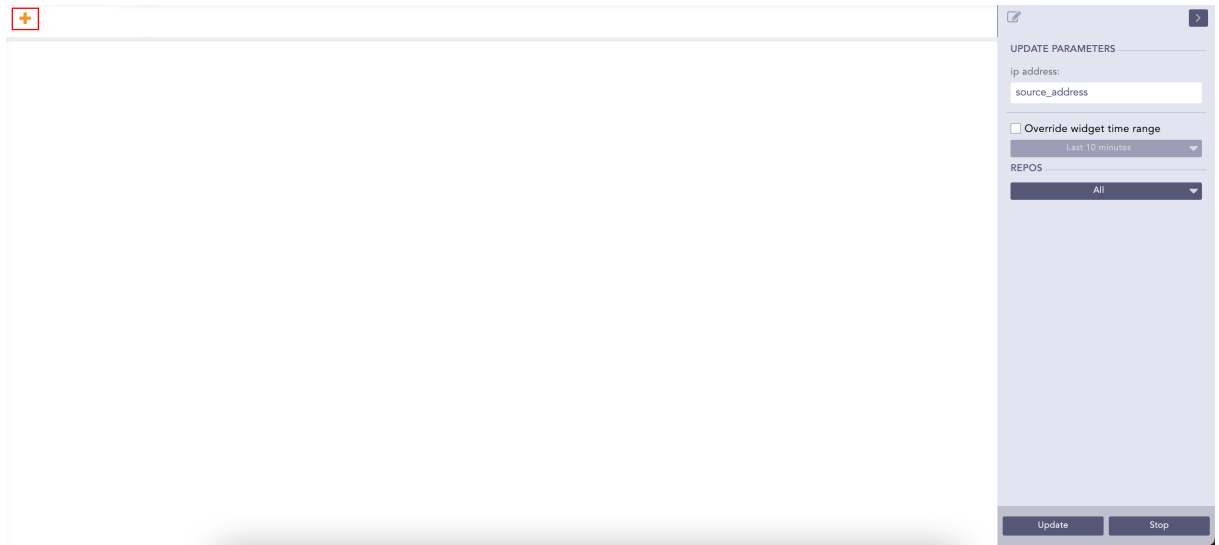
SLS forwards you to the **Search Template View** where you can access the dashboards of the corresponding search template.

NOTE
You can also view a shared search template using the same method.

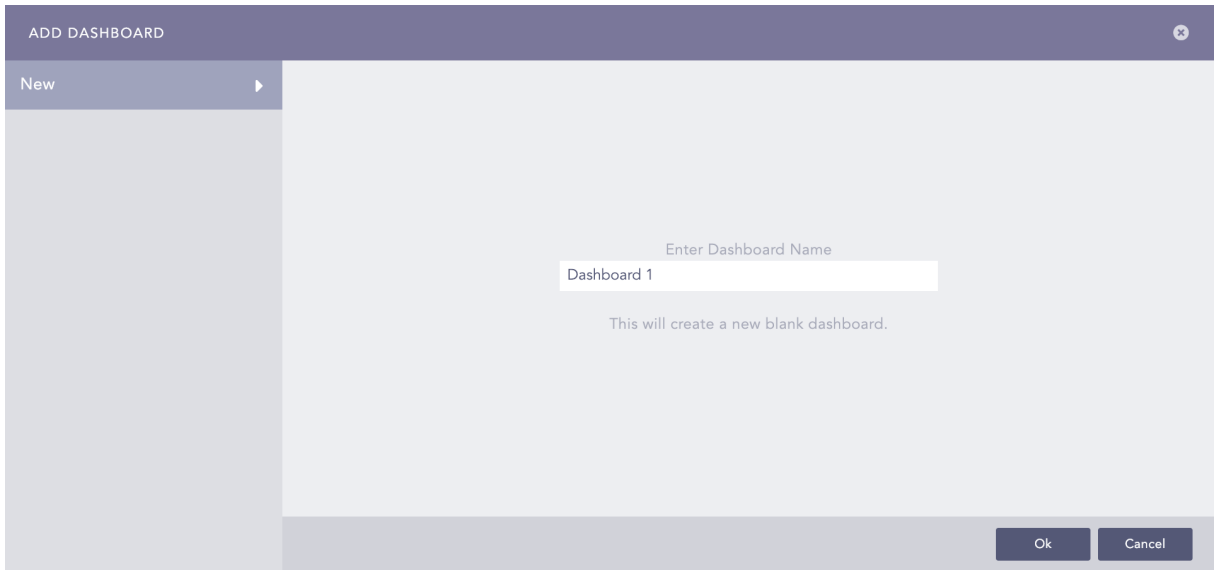
From the search template view, you can perform the following tasks:

Adding a Dashboard

1. Click the **Plus** icon at the top.



2. Enter the **name** of the dashboard.

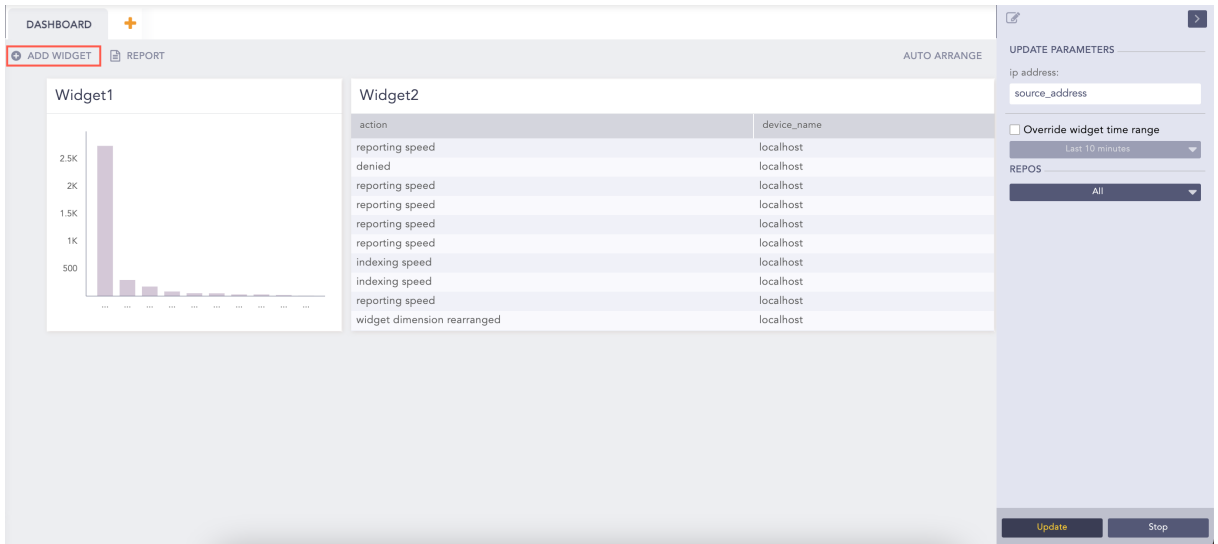


3. Click **Ok**.

i **NOTE**
You must add at least one dashboard to use the features of the **Search Template View**.

Adding a Widget

1. Click **Add Widget**.



2. Enter a **Name** for the widget.



CREATE WIDGET - STEP 1

Create your own custom dashboard widget.

CREATE DASHBOARD WIDGET

Name:

Query: Select

Description:

Time-range: Day: Hour: Minute:

Cancel Previous Finish

3. In the **Query** field, enter the name of a base query within **{{** and **}}**.
4. Enter a **Description** and a **Time-range** for the widget.

Creating a Report

1. Click **Report** at the top of the dashboard.

DASHBOARD +

ADD WIDGET **REPORT** AUTO ARRANGE

UPDATE PARAMETERS

ip address:

source_address

Override widget time range

Last 10 minutes

REPOS:

Update Stop

action	device_name
reporting speed	localhost
denied	localhost
reporting speed	localhost
reporting speed	localhost
reporting speed	localhost
reporting speed	localhost
reporting speed	localhost
indexing speed	localhost
indexing speed	localhost
reporting speed	localhost
widget dimension rearranged	localhost

2. Enter the **Report Name** and an **Email** address.



CREATE REPORT

REPORT OPTIONS

Name:

Email:

3. Click **Submit**.

NOTE
You receive the report in the PDF format.

Auto-arrange the Widgets

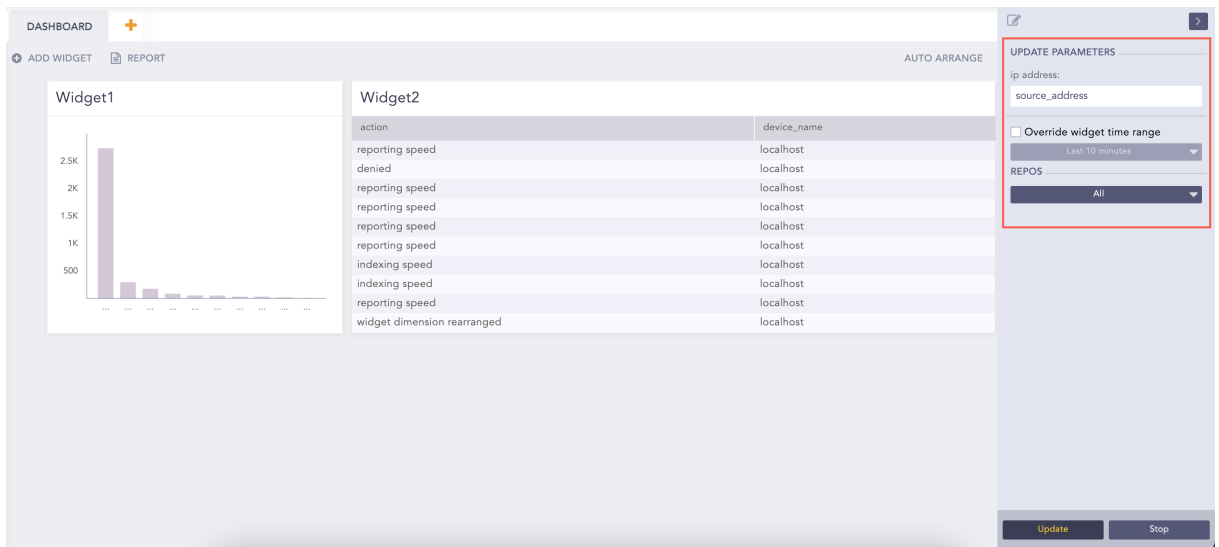
Click **Auto Arrange** to automatically arrange the widgets in a presentable form.

The screenshot shows a dashboard with two widgets: 'Widget1' (a bar chart) and 'Widget2' (a table). A red box highlights the 'AUTO ARRANGE' button. To the right is a 'UPDATE PARAMETERS' panel with fields for 'ip address' and 'source address', a time range selector set to 'Last 10 minutes', and a 'REPOS' dropdown set to 'All'. 'Update' and 'Stop' buttons are at the bottom right.

action	device_name
reporting speed	localhost
denied	localhost
reporting speed	localhost
reporting speed	localhost
reporting speed	localhost
reporting speed	localhost
indexing speed	localhost
indexing speed	localhost
reporting speed	localhost
widget dimension rearranged	localhost

Updating Parameters

1. Enter the new values for the variables in the panel to the right.

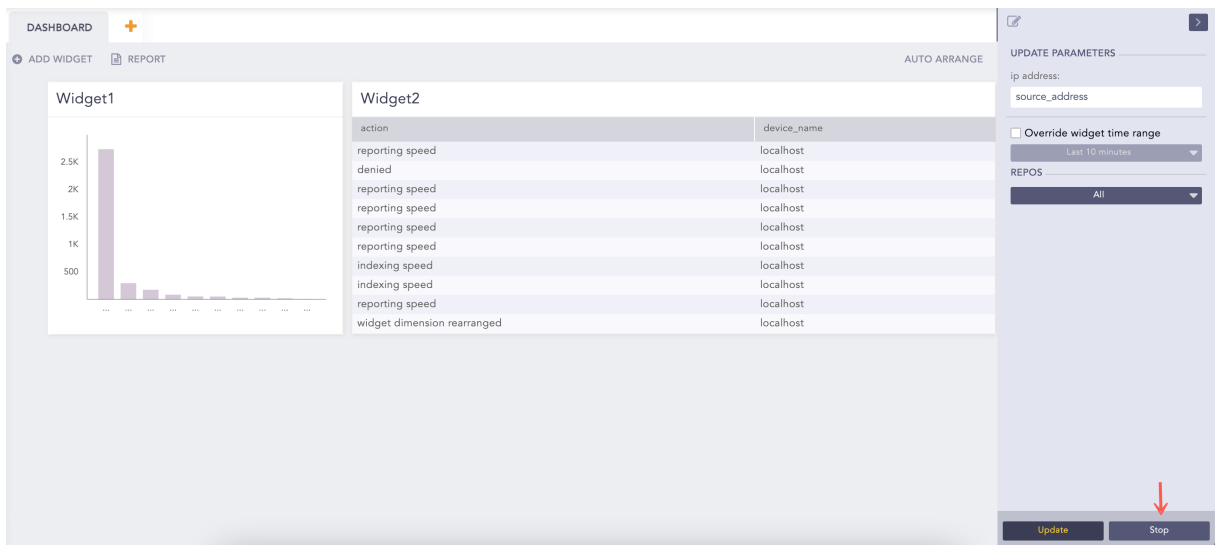


2. Click **Override widget time range** to select a time-range. The time-range you provide in this field takes precedence over the one provided for individual widgets.
3. Select the **Repos** in which to perform the search.
4. Click **Update**.

Stopping widget update

After clicking **Update**, the widgets continuously retrieve their respective logs.

Click the **Stop** button to stop the widgets from retrieving additional logs. Doing this pauses the visualization of all the widgets. You can only see the already received log results.



i NOTE

- The widgets show updated values only after you click the **Update** button.
- Click **Back** to redirect to the list view of the search templates.
- The search templates remember the last visualization used on the widgets.
- You can drill-down on the search results from the non-edit mode of the widget of the search templates.



Further reading

Additional information and answers to questions you may have about SLS are available in the [Stormshield knowledge base](#) (authentication required).



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.