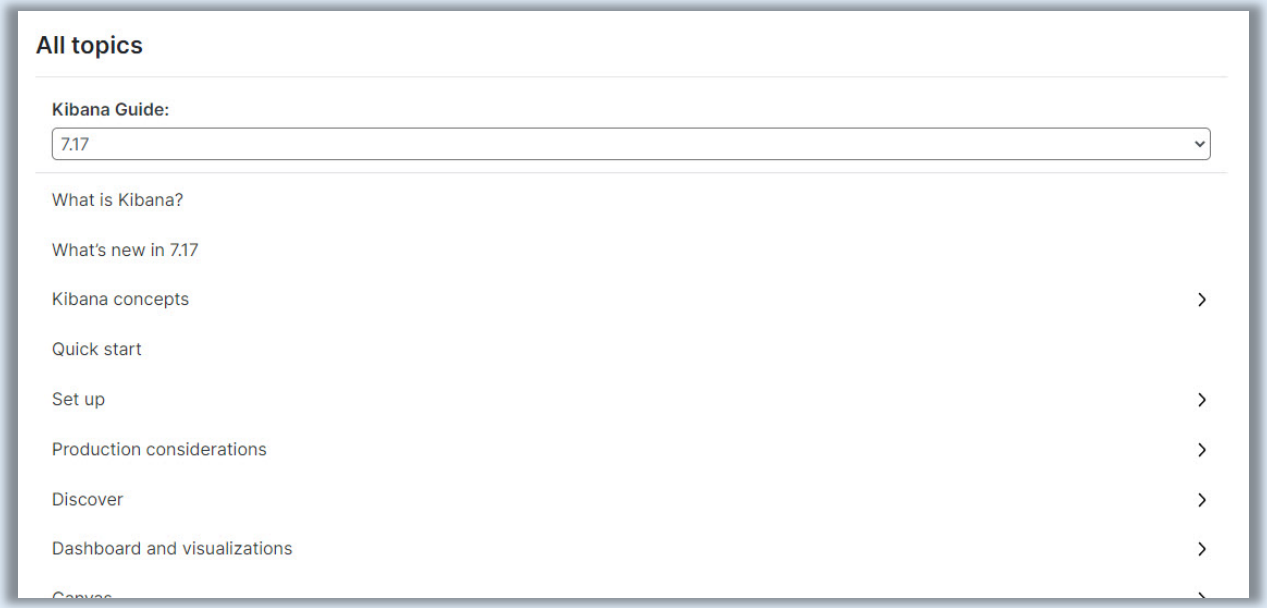
Kibana

Reference Guide

This user reference guide includes instructions for the use of Kibana within the PIEE environment. For further instructions on the use of Kibana, please visit https://www.elastic.co/guide/en/kibana/7.17/index.html.

Table of Contents

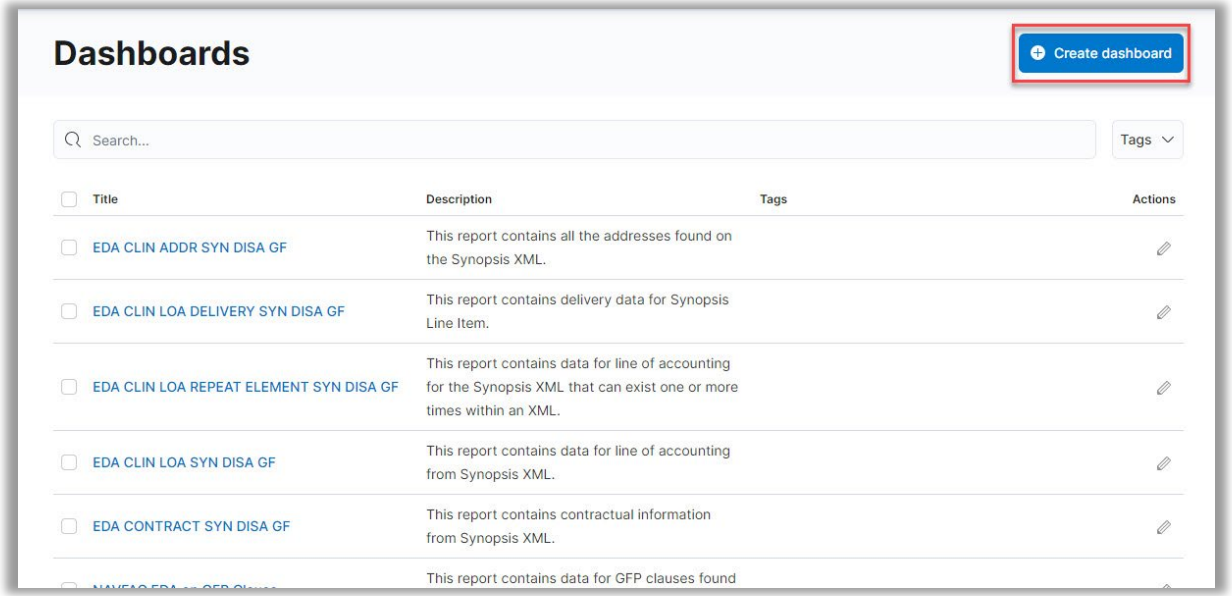
Elastic User Guide



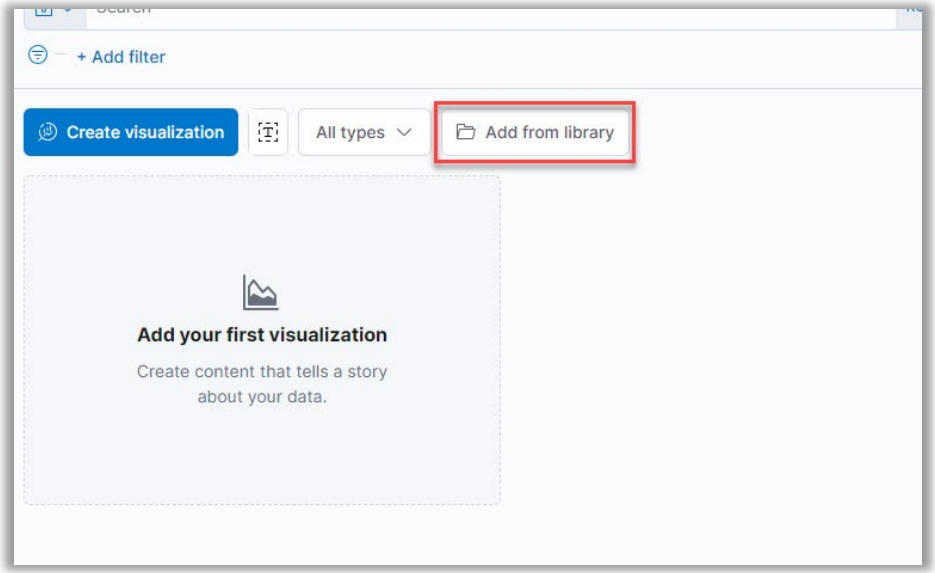
To view Elastic's Kibana user guide, navigate to https://www.elastic.co/guide/en/kibana/7.17/index.html. Navigate to the bottom of the page and utilize the navigational menu to access training materials relevant to 7.17.1.

Dashboards

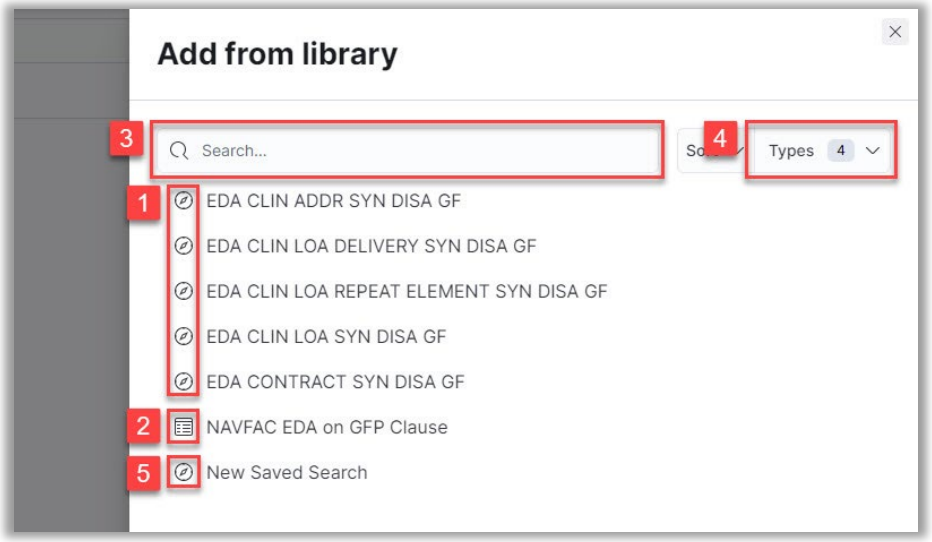
The user may customize the Kibana dashboard to display a collection of searches and visualizations.



Select the **Create dashboard** button to customize the dashboard view.

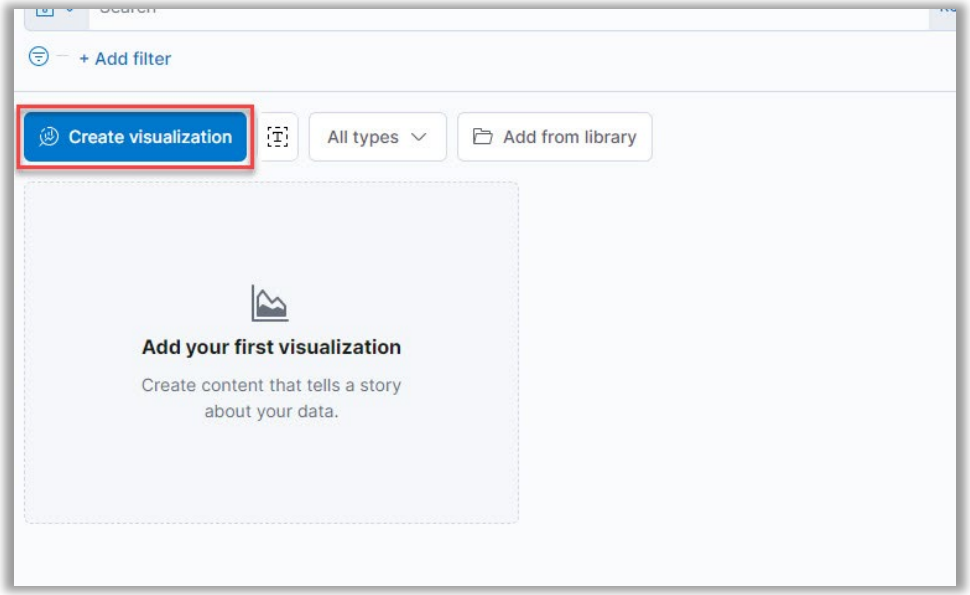


To add a saved visualization to the dashboard, select the **Add from library** button.



All available saved visualizations and searches are displayed by default.

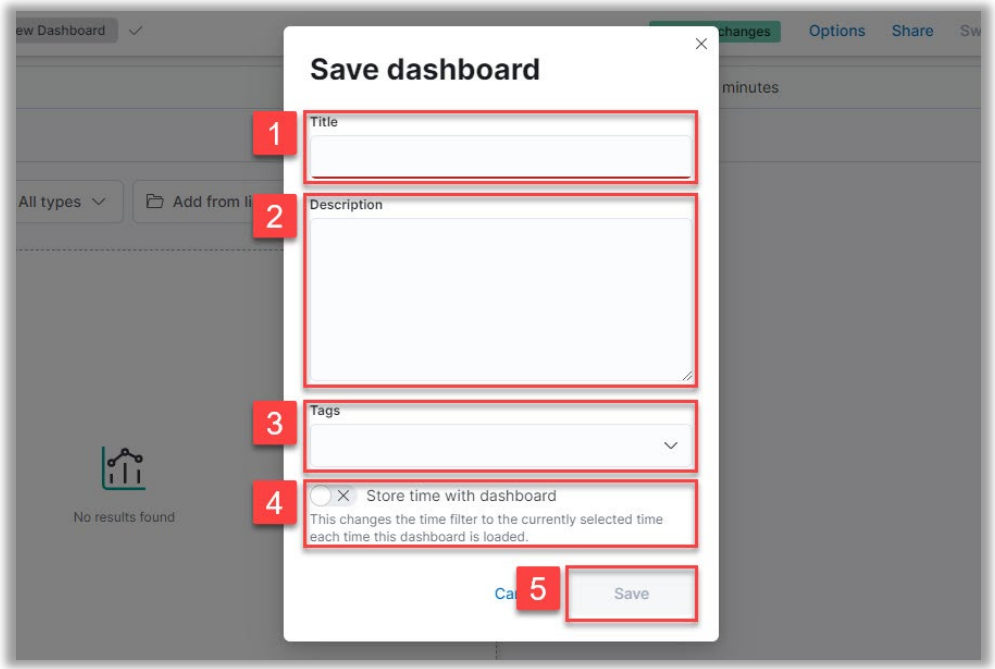
1. Saved visualizations may be selected to add to the dashboard.
2. Saved searches may be selected to add to the dashboard.
3. Visualizations and searches may be located using the **Search** field.
4. Available items may be filtered using the **Types** dropdown menu.
5. A new search may be created using the **New Saved Search** option.



To create a new visualization, select the **Create visualization** button.

Select the desired visualization type from the **Visualization Type** dropdown menu. For more information on creating a visualization, please visit https://www.elastic.co/guide/en/kibana/7.17/dashboard.html.

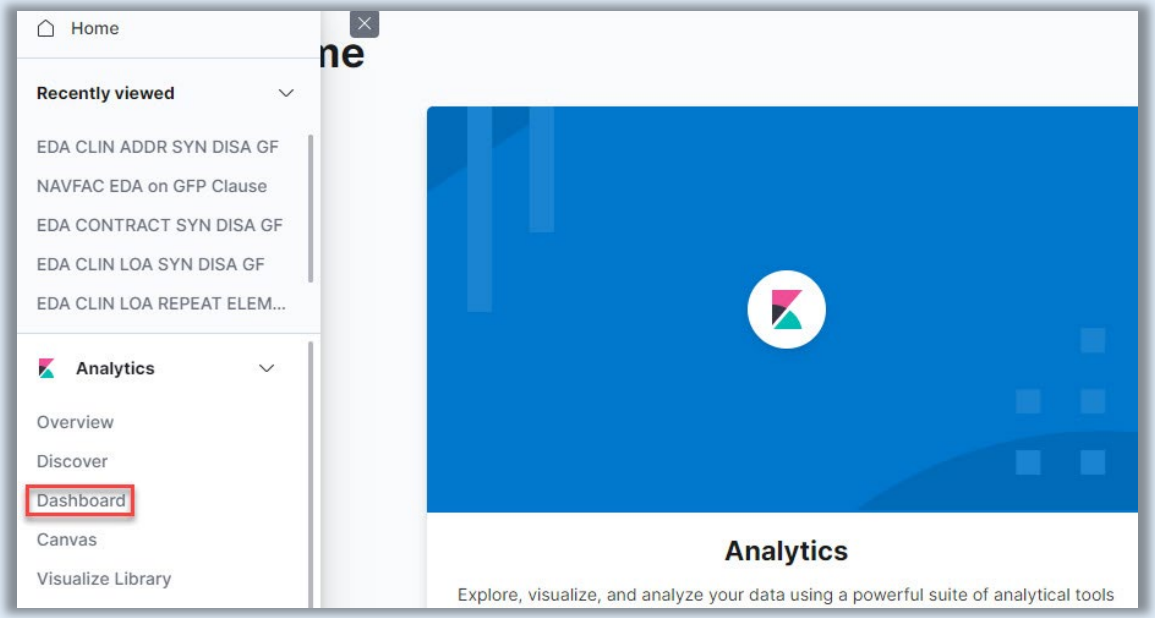
Select **Save** from the Kibana toolbar to save the new dashboard.



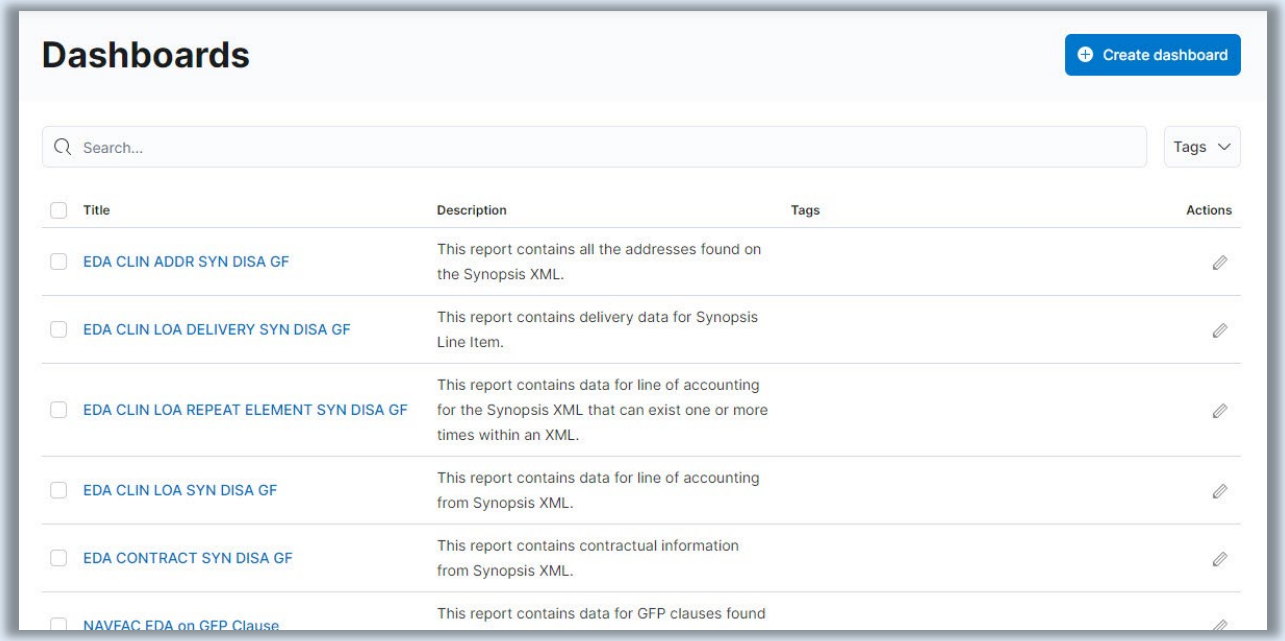
1. Enter the dashboard name in the Title field.
2. Add a description in the Description field, if desired.
3. Add any desired metadata from the Tags dropdown menu.
4. To store the time period specified in the time filter, enable Store time with dashboard.
5. Select **Save** to save the dashboard.

Viewing Report Data

Navigation

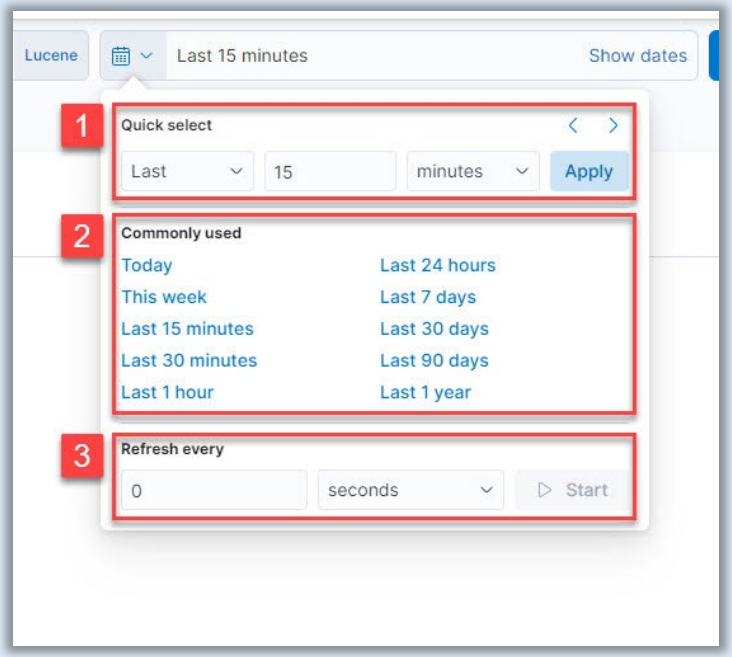


Navigate to the **Dashboard** tab in the navigation pane.



Select the desired report from the Dashboards menu.

View Report Data



The time filter restricts the search results to a specific time period. The time filter can be specified if the index contains time-based events, and a time field is configured for the selected index pattern. The time filter defaults to the last 15 minutes.

1. In the Quick Select menu, arrows or fields may be used to select the desired time filter. Select the Apply button to save changes.
2. Commonly used settings may be selected to apply the time filter.
3. A refresh interval may be specified.

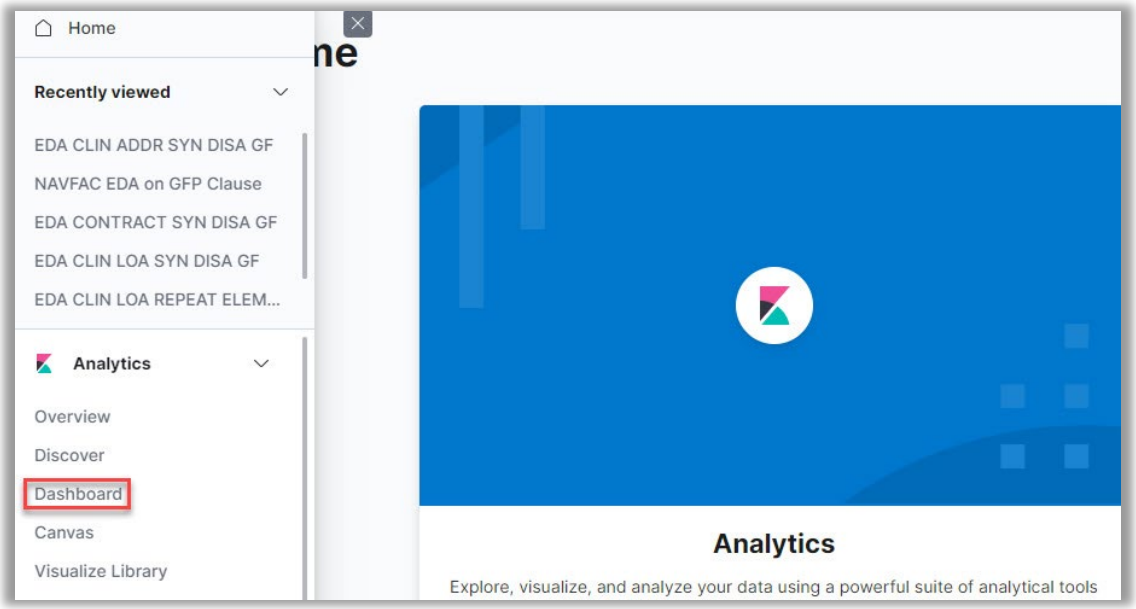
Kibana Reports are displayed on the Kibana Dashboard. Select the **menu expander** to the left of a document to view detailed data for that item.

Select the **Table** tab to view data in table format. In table view, the user will be able to view all the data within the index record. This includes more data than is displayed on the report.

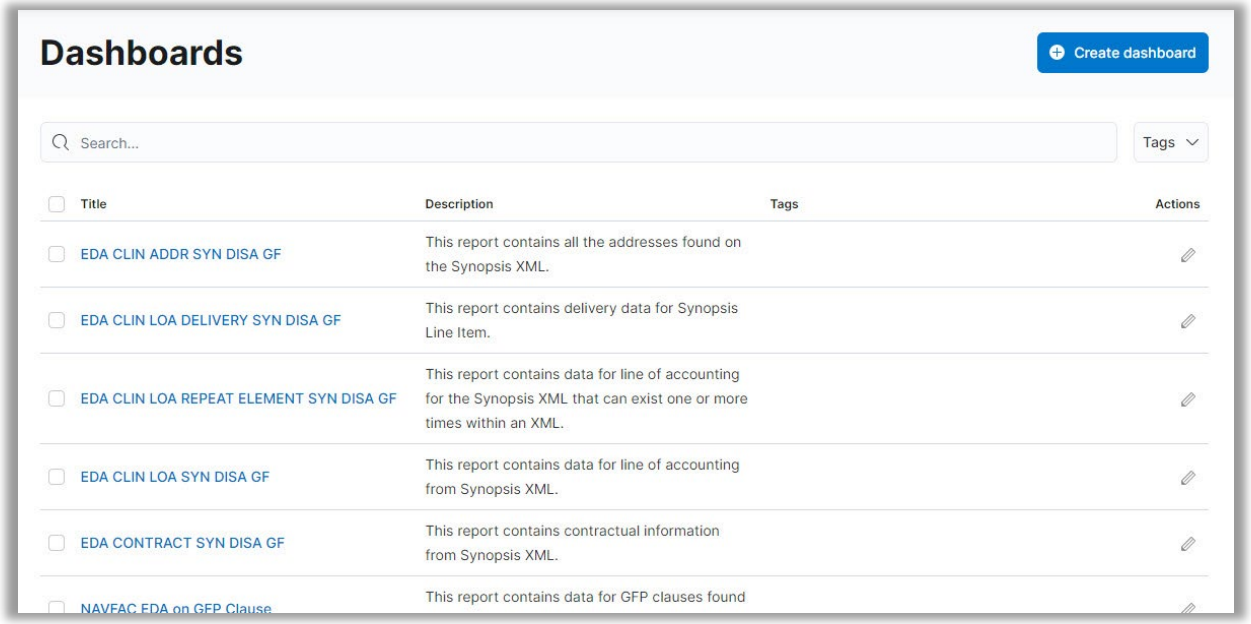
Select the **JSON** tab to view data in JSON format.

Filtering Report Data

Navigation



Navigate to the **Dashboard** tab in the navigation pane.



Select the desired report from the Dashboard menu.

Filter Report Data

Users may utilize filters to return specific data in the report.

Option 1: Lucene Queries

1. Manually enter one or more filter queries in the free text **Search** field. The query must be in the format of field:data (no spaces). As data is entered, matching fields may be displayed in the dropdown menu. The user's search history will also populate in the dropdown menu.

   Examples:
   clin:0001
   parent_record_key:12345 AND clin:0001

   For information regarding building Lucene queries, please visit https://www.elastic.co/guide/en/elasticsearch/reference/7.2/query-dsl-query-string-query.html#query-string-syntax.

2. Select the **Refresh** button to apply the filter.

Option 2: Guided Filtering

1. To select filters from the Add a Filter menu, select the **Add Filter** button below the Search field.

2. The Edit filter modal will be displayed. The user may select the desired field from the **Field** dropdown menu or enter the field name manually. As data is entered into the field, the dropdown menu will display only matching items.

3. The Operator field will now be displayed. Select a search modifier from the **Operator** dropdown menu to apply to the search criteria entered in the Fields field.

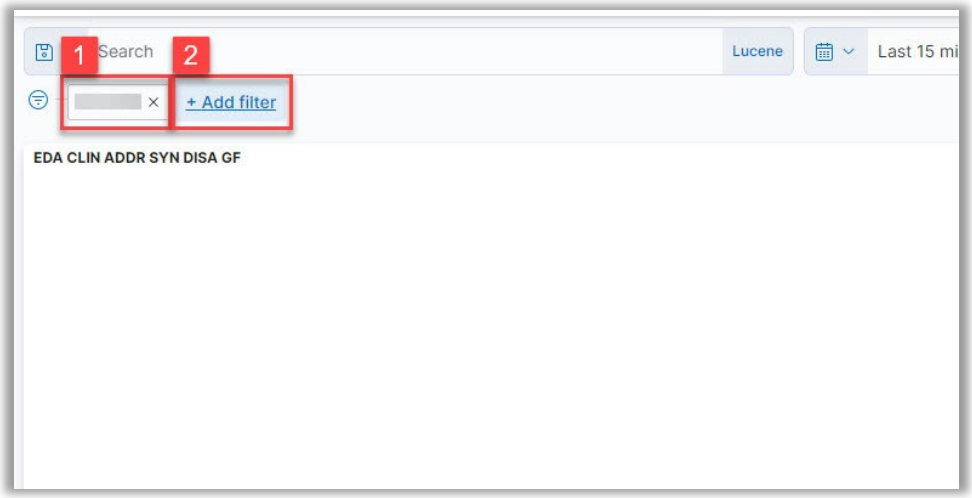
   The operators are defined as follows:
   - Is: Filter where the value for the field matches the given value.
   - Is not: Filter where the value for the field does not match the given value.

- Is one of: Filter where the value for the field matches one of the specified values.
- Is not one of: Filter where the value for the field does not match any of the specified values.
- Exists: Filter where any value is present for the field.
- Does not exist: Filter where no value is present for the field.

4. The Value field will now be displayed. The user may select an item from the **Value** dropdown menu or enter a value manually. As data is entered into the field, the dropdown menu will display only matching items.

   Note: To search for a NULL value for a string field, select the 'Is' operator and enter 'ZZZULL' in the Values field. For non-string fields, such as dates and numbers, use the 'Exists'/'Does not exist' operators.

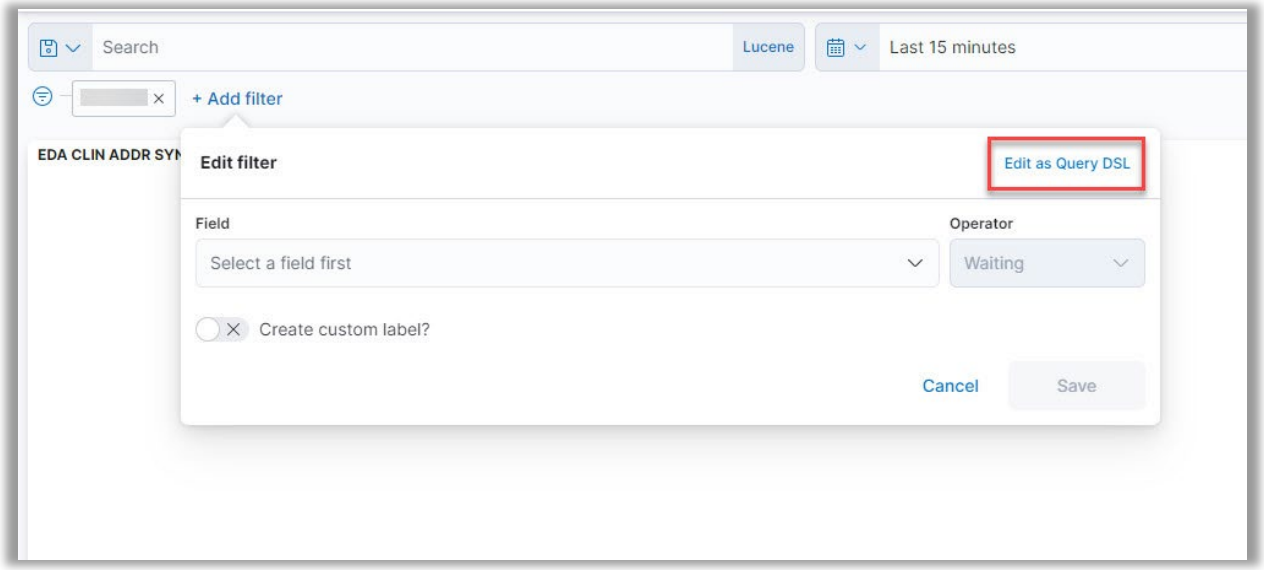
5. Select the **Save** button on the Edit filter modal.



1. The report results are filtered by the user's requested criteria.
2. Multiple filters may be applied simultaneously by selecting the **Add Filter** button and repeating the previous steps.

For more information regarding filtering in Kibana, please visit https://www.elastic.co/guide/en/kibana/7.17/discover.html.

Option 3: Query DSL



1. To use advanced queries, select the **Edit as Query DSL** link on the Add a Filter menu.

Example: Starts With and Wildcard queries

--- Starts with query ----

```
{
  "query": {
    "prefix": {
      "contract_number": "S0"
    }
  }
}
```

--- Wildcard query ----

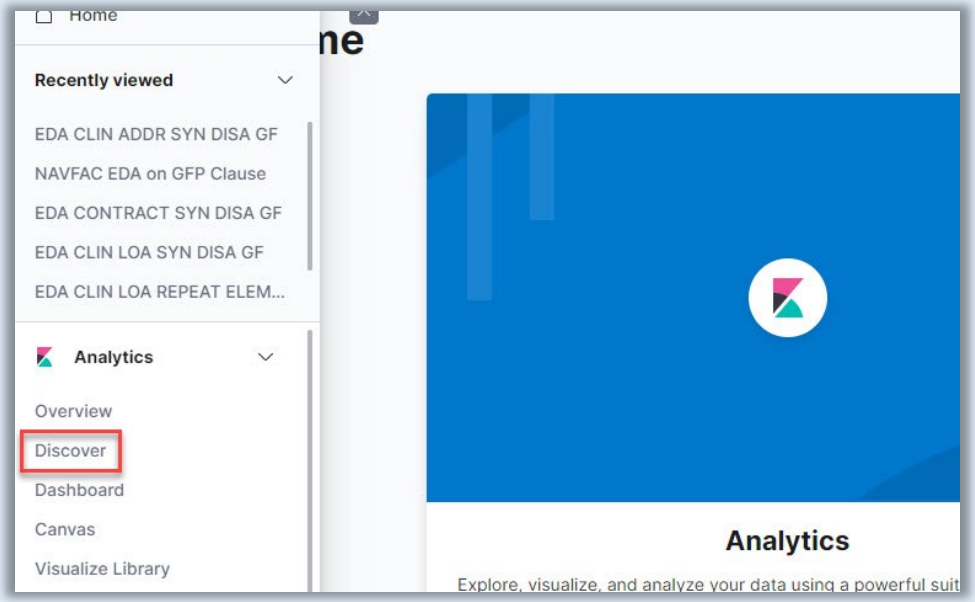
```
{
  "query": {
    "wildcard": {
      "contract_number": "S*"
    }
  }
}
```

Additional filters may be added using the **Edit as Query DSL** link. All entered queries will be chained together to return the desired results.

For more information regarding querying of DSL, please visit https://www.elastic.co/guide/en/elasticsearch/reference/7.17/query-dsl.html.

Exporting Report Data

Users may export report data from Kibana in CSV format.

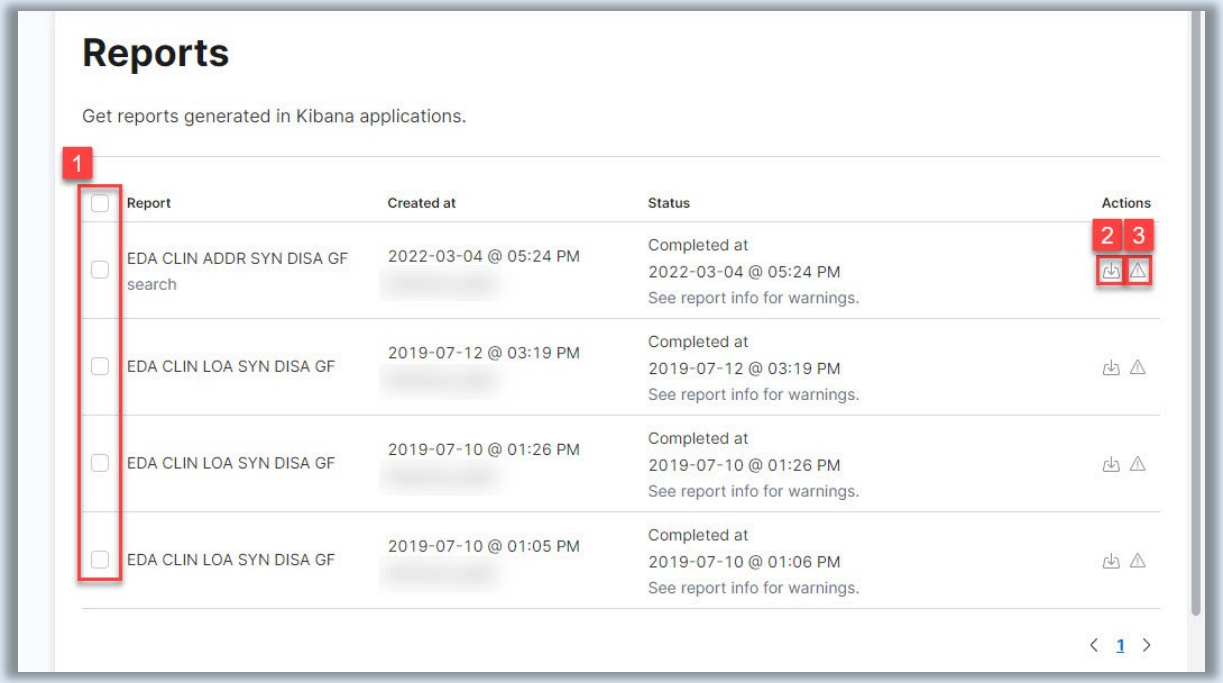


1. Navigate to the **Discover** tab in the navigation pane.
2. Select the **Open** link in the menu bar.
3. In the Open search modal, select a **Search** from the list of reports.
4. Select the **Share** link in the menu bar.
5. Select **CSV Reports** from the Share This Search dropdown menu.

6. Select the **Generate CSV** button to queue the CSV file for download. The user may select the download link in the popup that will display on the screen, or on the Reports page.

7. To download the CSV file from the Reports page, navigate to the **Stack Management** tab in the Management section of the navigation pane.

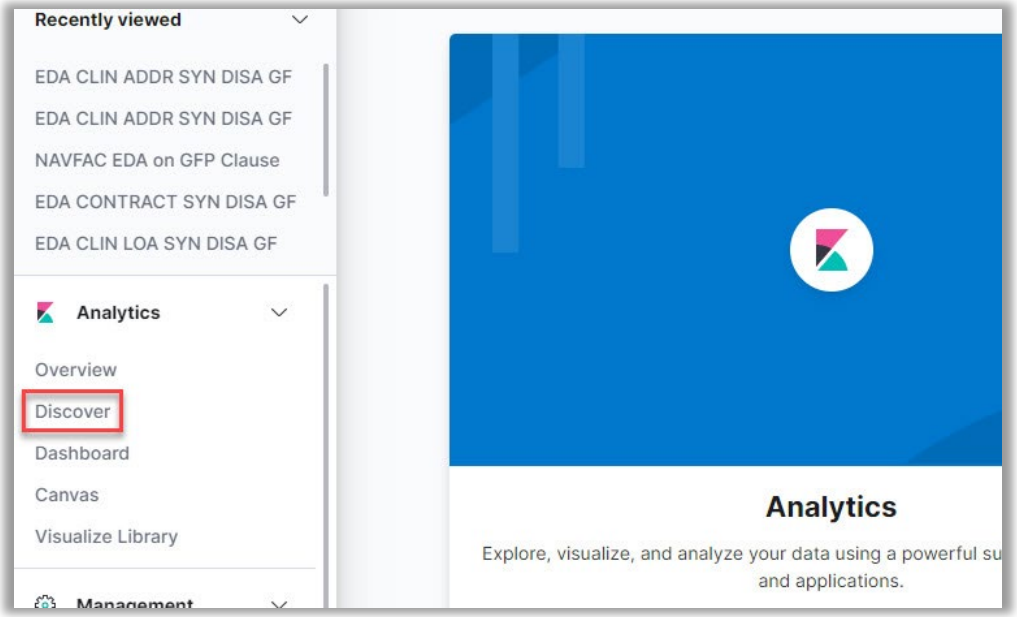
8. Select the **Reporting** link under Alerts and Insights in the navigation pane.



1. Select the **checkbox** of the report to be downloaded.
2. The **Download** button will allow the user to download the report with any warnings.
3. The **Warnings** button will display report info and any warnings.

Searches

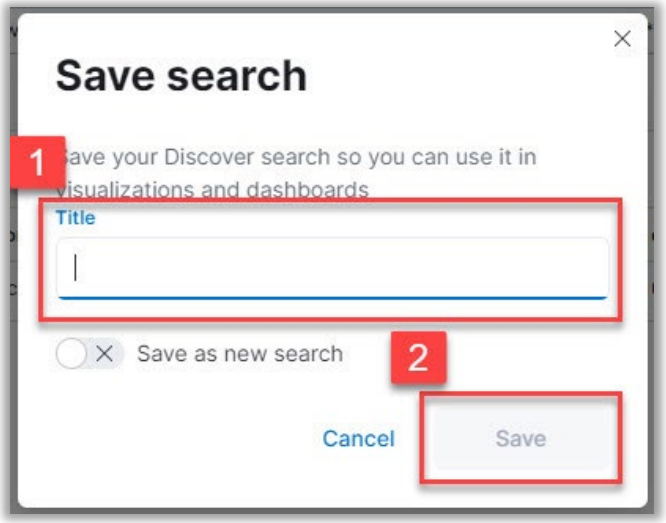
Navigation



Navigate to the **Discover** tab in the navigation pane.

Save Search

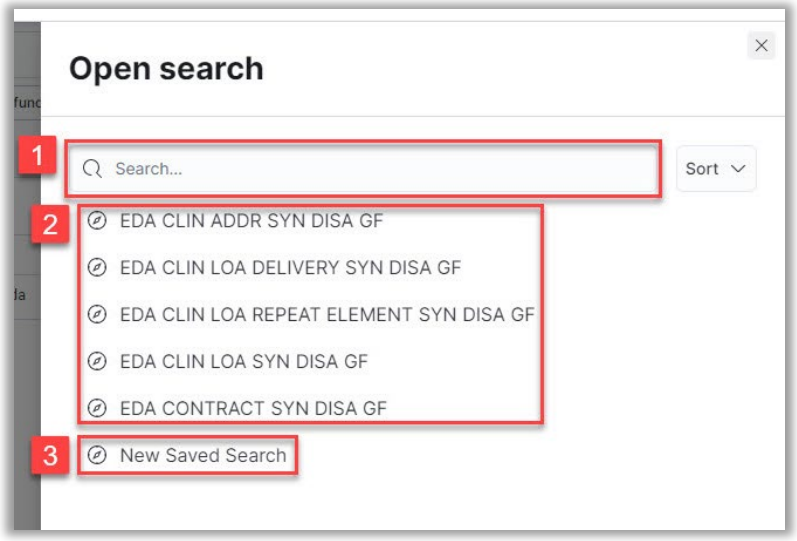
To save a new search, select **Save** in the Kibana toolbar.



1. Enter the Saved Search title in the **Title** field.
2. Select the **Save** button.

Open Saved Search

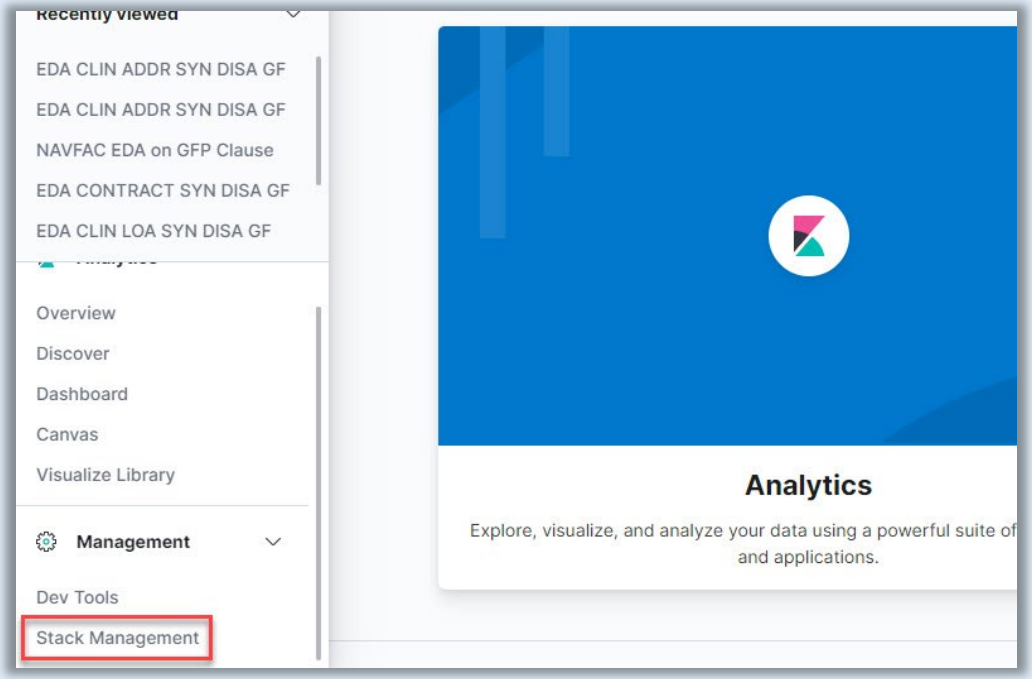
To load a saved search, select **Open** in the Kibana toolbar.



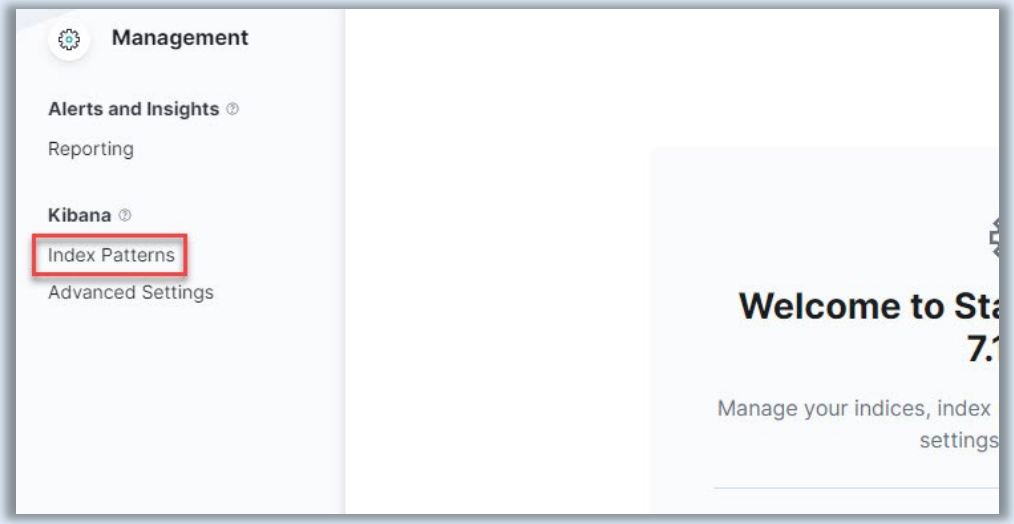
1. The list may be filtered using the **Search** field.
2. Saved searches will be populated in the Open Search menu. Select the desired **search**.
3. A new search may be created using the **New Saved Search** option.

Index Patterns

Navigation

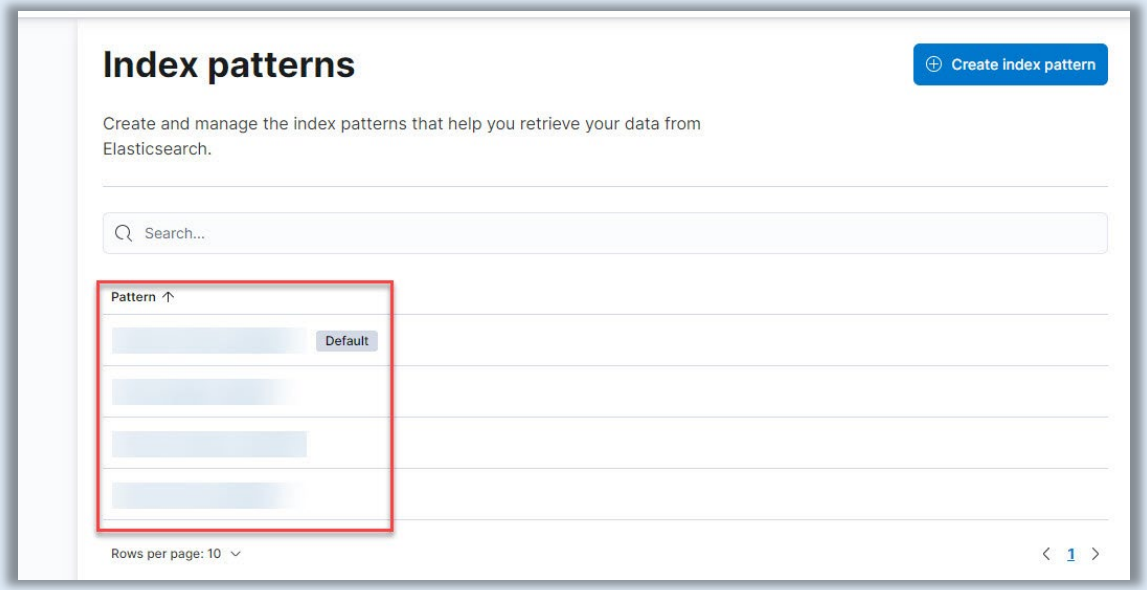


Navigate to the **Stack Management** tab in the navigation pane.



Navigate to the **Index Patterns** link on the Management page.

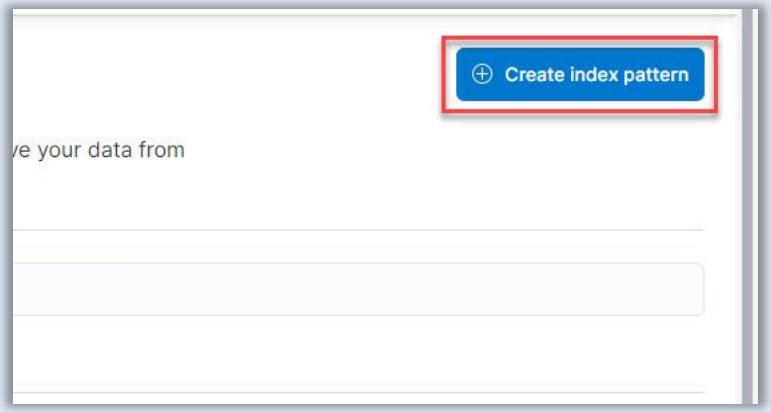
Viewing Index Patterns



Existing index patterns are listed. Select the desired pattern to view.

Creating An Index Pattern

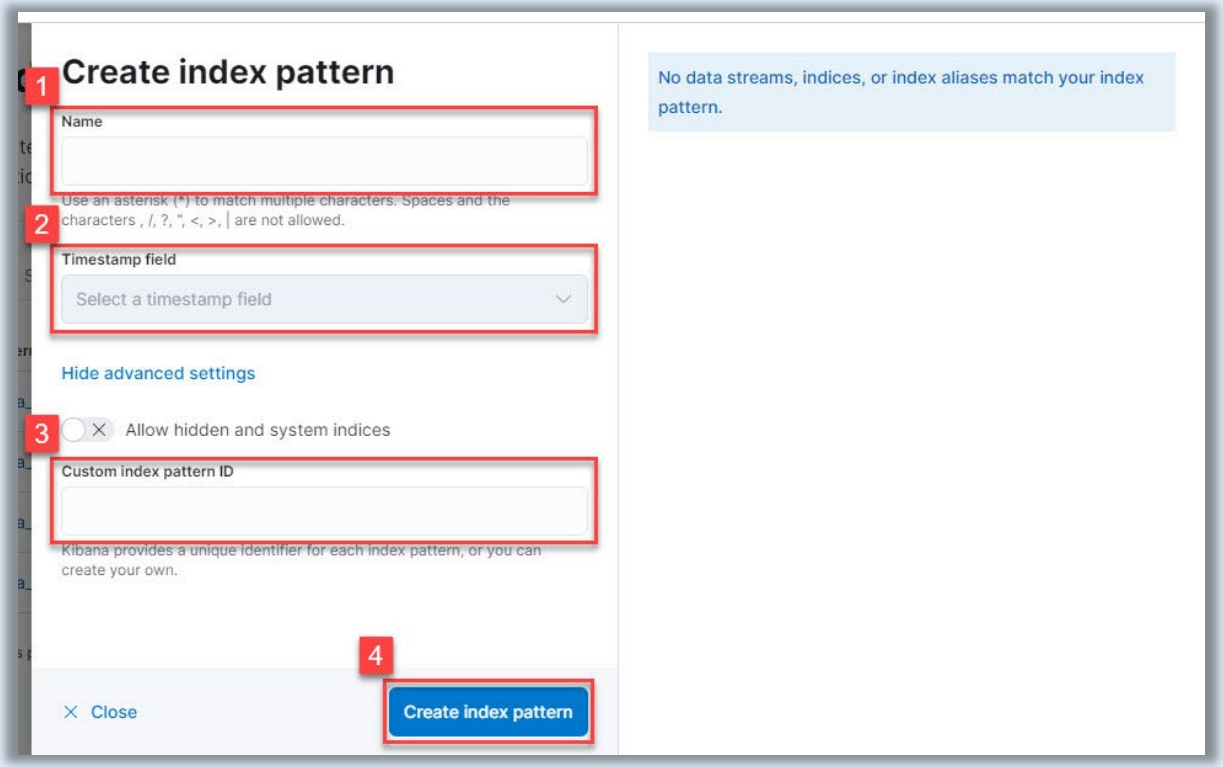
Users may create index patterns to specify which Elasticsearch indices to explore in Kibana. For more information on creating index patterns, please visit https://www.elastic.co/guide/en/kibana/7.17/index-patterns.html.



Select the **Create index pattern** button to begin creating a new index pattern.

In the Change Index Pattern dropdown, enter the index name in the **Filter options** field. An index pattern can match the name of a single index or include a wildcard (*) to match multiple indices. The following characters are prohibited: \, /, ?, “, <, >, |.

If no existing index patterns are available, the Create Index Pattern page will be displayed upon selecting the Create Index Pattern button.



1. Enter a name for the index pattern in the **Name** field. The name must match one or more data streams, indices, or index aliases.
2. A timestamp may be selected from the **Timestamp field** dropdown menu.
3. A unique identifier will be populated in the **Custom index pattern ID** field. This field may be edited to create a custom index pattern ID.
4. Select the **Create index pattern** button.