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 **2**

Dashboards **3**

Collaborative Spaces **6**

Creating and Editing a Collaborative Space 6

Sharing from a Personal Space to a Collaborative Space 13

Sharing Saved Objects from User to User **17**

How to share Saved Objects from one User to another User 18

User One (Exporting) *18*

User Two (Importing) *20*

Viewing Report Data **24**

Navigation 24

View Report Data 25

Filtering Report Data **26**

Navigation 26

Filter Report Data 28

Option 1: Lucene Queries *28*

Option 2: Guided Filtering *28*

Option 3: Query DSL *29*

Adding Filters to Dashboards **31**

Managing Added Filters 32

Adding Controls to Dashboards **33**

Types of Controls 33

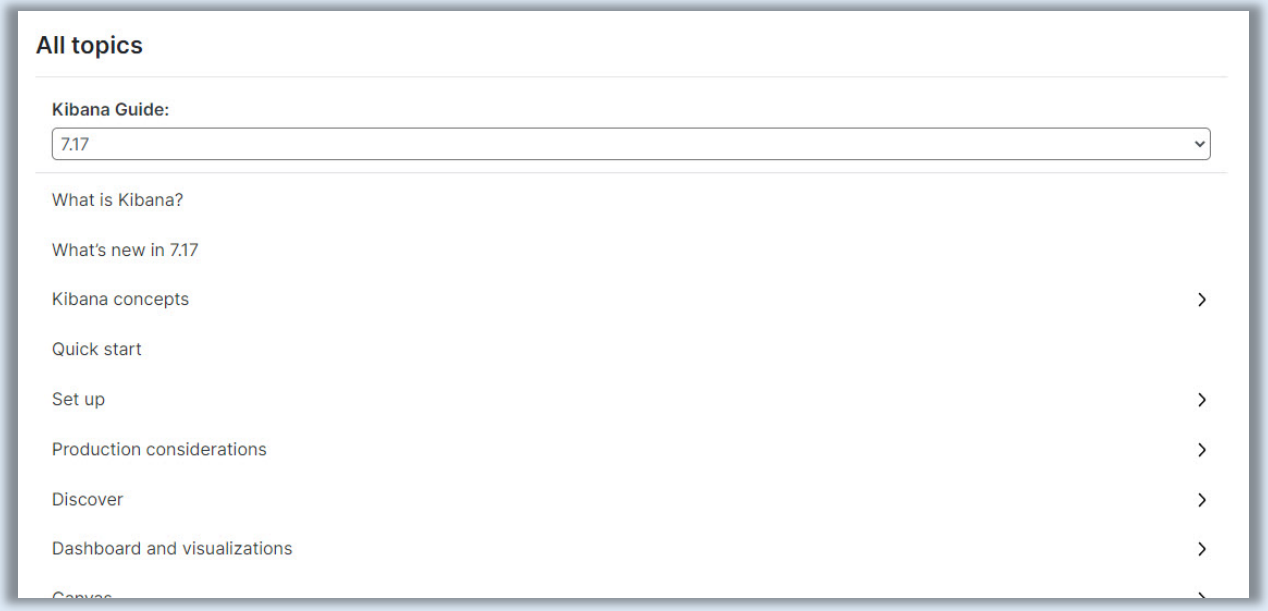
Creating Options List and Range Slider Controls 33

Adding Options List Controls 35

Adding Range Slider Controls 36

Creating Time Slider Controls 37
Adding Time Slider Controls 37
Exporting Report Data 38
Searches 40
Navigation 40
Save Search 40
Open Saved Search 41
Index Patterns 42
Navigation 42
Viewing Index Patterns 43
Creating An Index Pattern 44

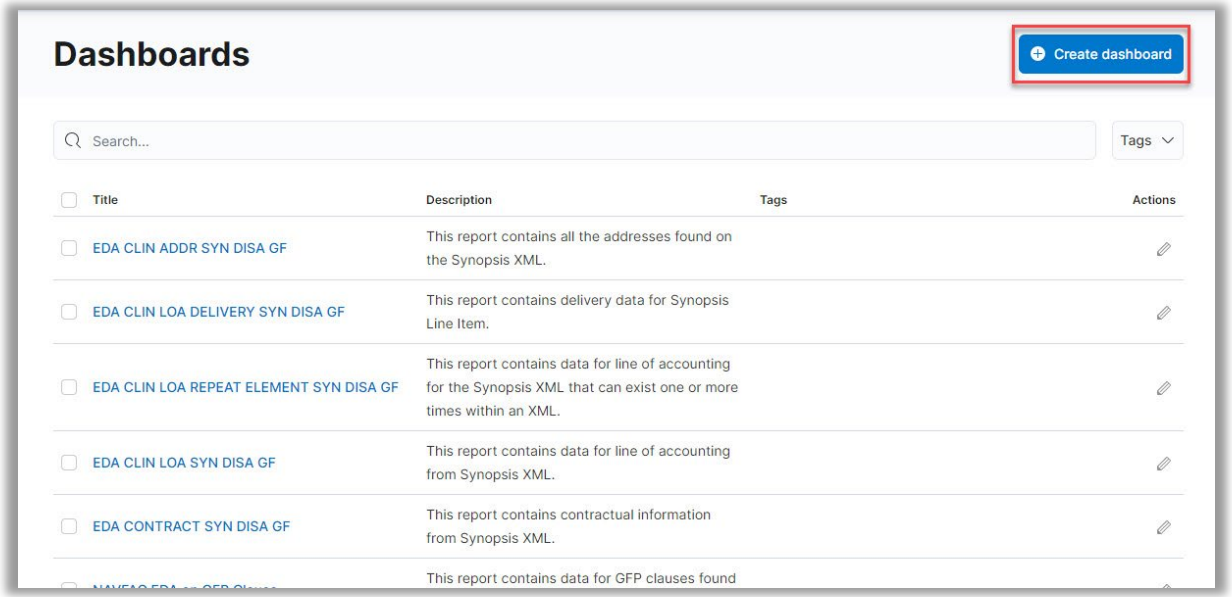
Elastic User Guide



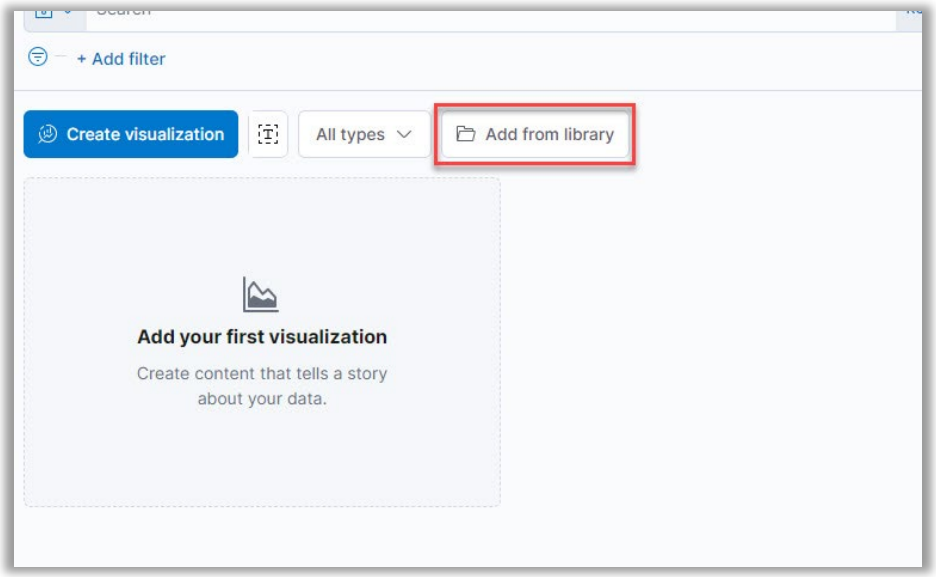
To view Elastic's Kibana user guide, navigate to https://www.elastic.co/guide/en/kibana/7.17/index.html. Navigate to the bottom of the page and utilize the navigational menu to access training materials relevant to 7.17.1.

Dashboards

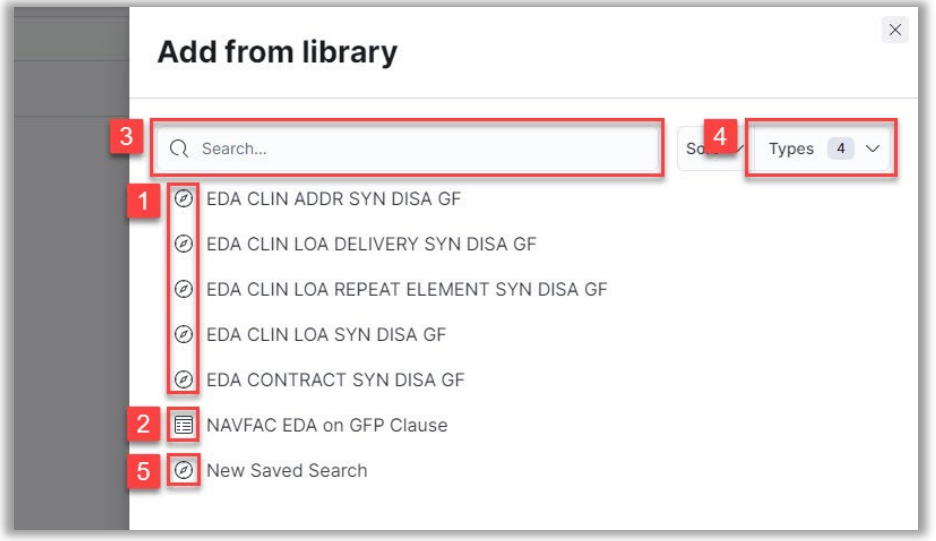
The user may customize the Kibana dashboard to display a collection of searches and visualizations.



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



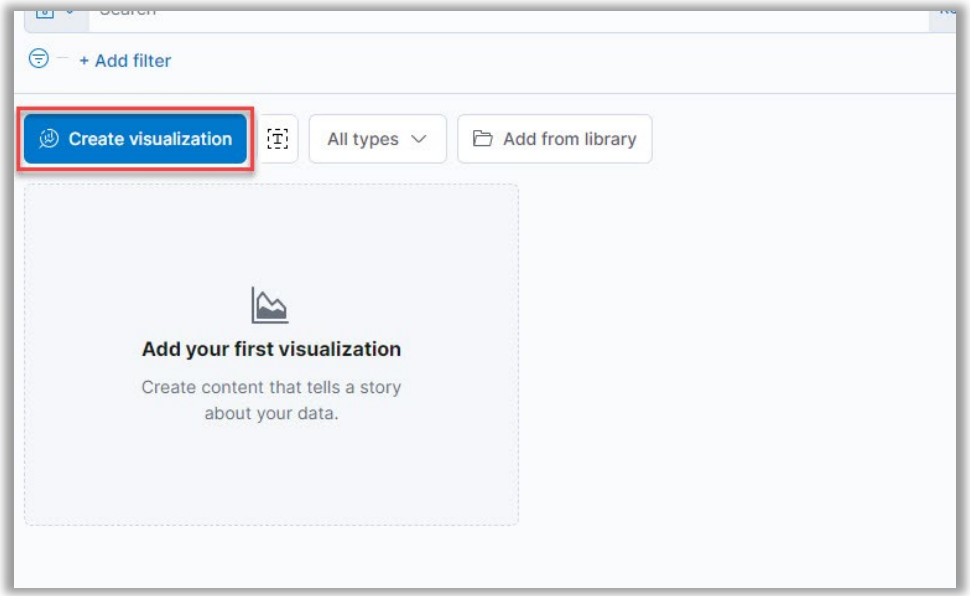
To add a saved visualization to the dashboard, select the **Add from library** button.



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** drop-down menu.

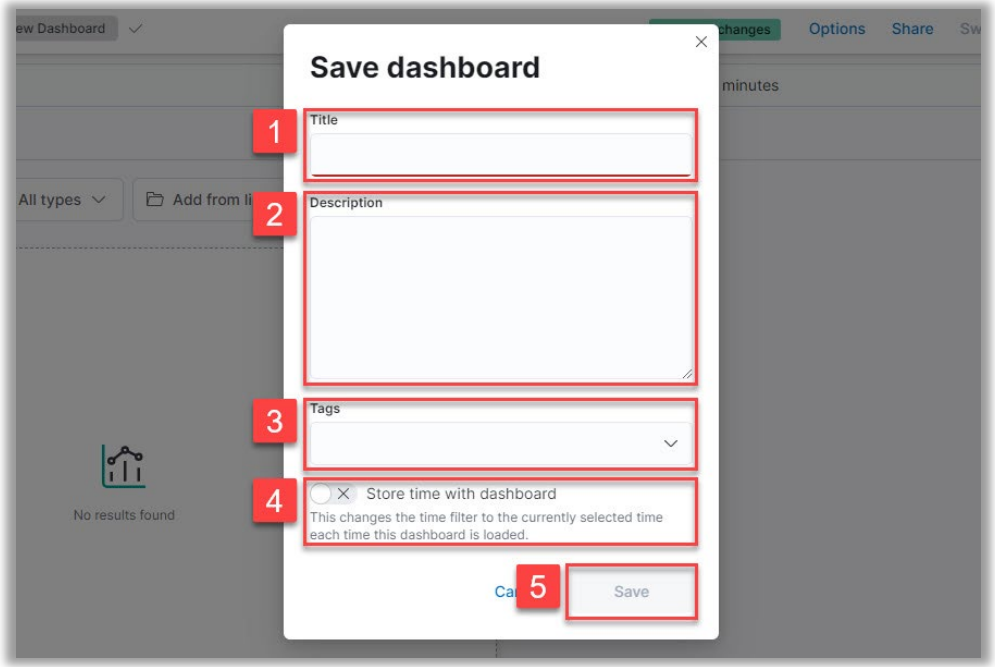
5. A new search may be created using the **New Saved Search** option.



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

Select the desired visualization type from the **Visualization Type** drop-down 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.

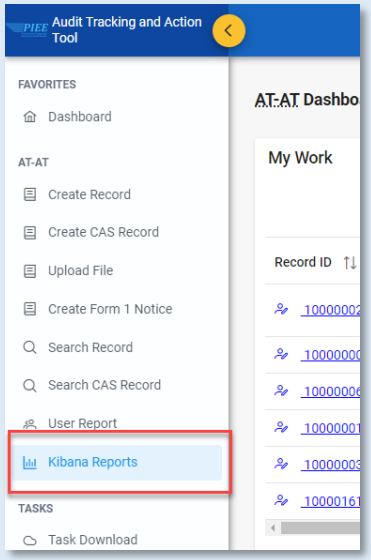


1. Enter the dashboard name in the Title field.
2. Add a description in the Description field, if desired.
3. Add any desired metadata from the Tags drop-down menu.
4. To store the time period specified in the time filter, enable Store time with dashboard.
5. Select **Save** to save the dashboard.

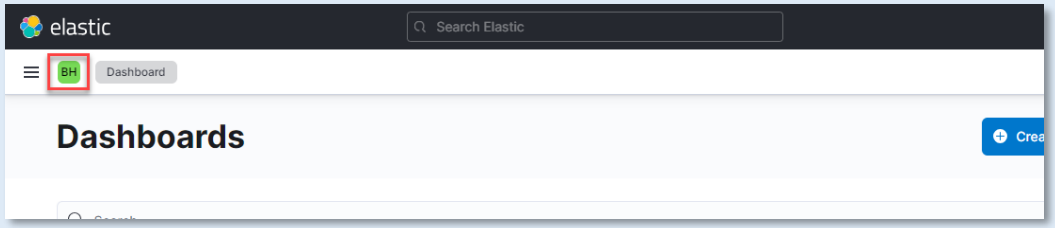
Collaborative Spaces

Creating and Editing a Collaborative Space

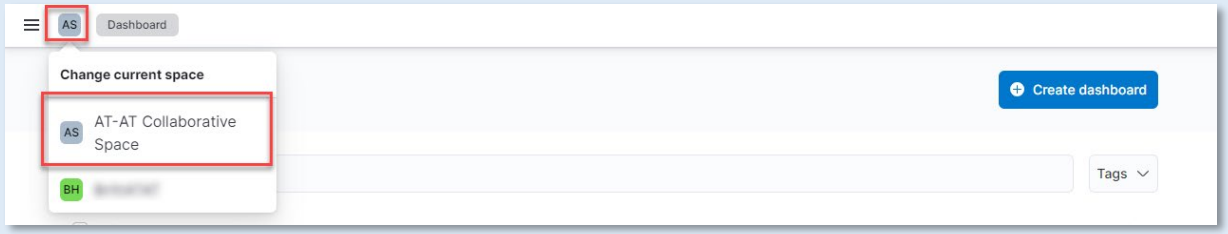
1. Access Kibana (e.g., via AT-AT)



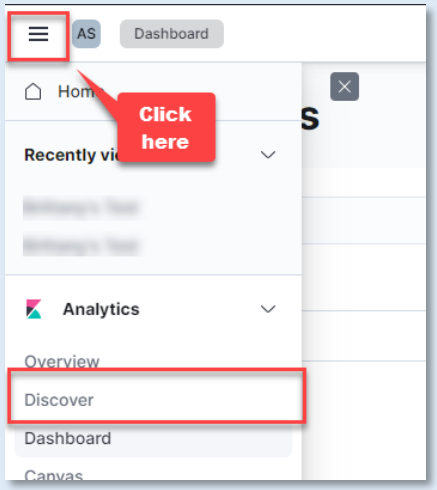
2. Click the small green square with initials in the top left of the page.



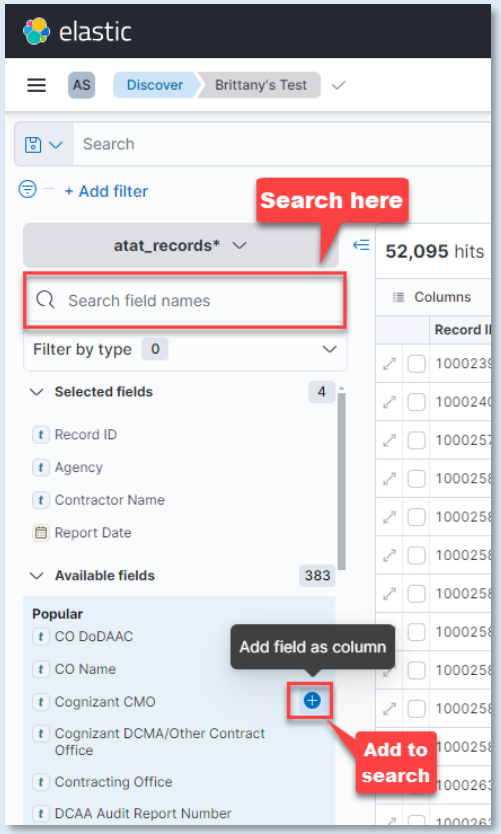
3. Click “’Module’ Collaborative Space” (e.g., AT-AT Collaborative Space).



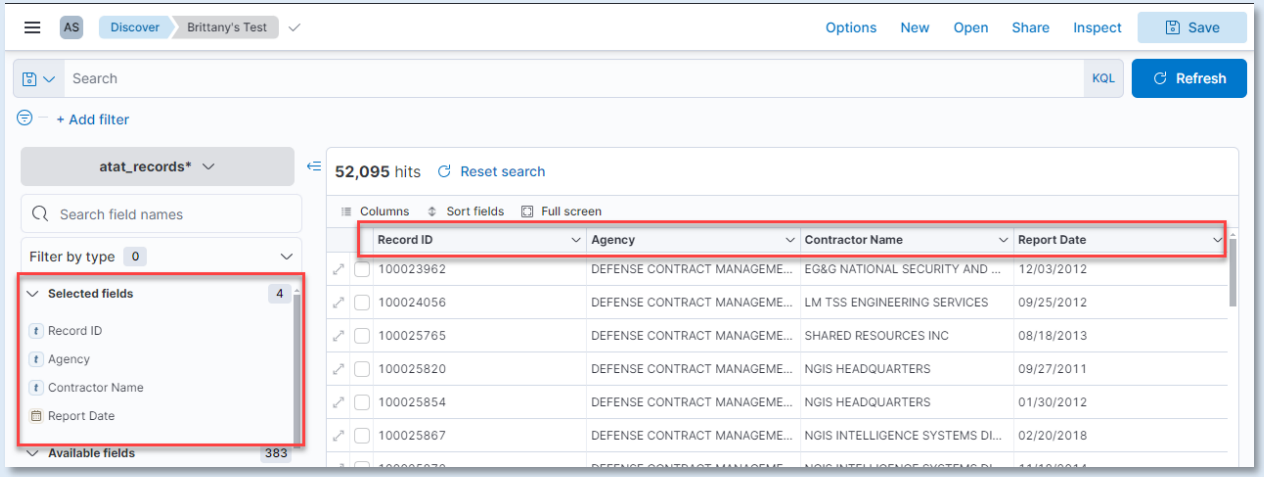
4. The “Dashboards” page displays (if it is blank the user is prompted to create a Dashboard). Rather than clicking “Create Dashboard”, click the 3 lines in the top left of the page and navigate to “Discover”.



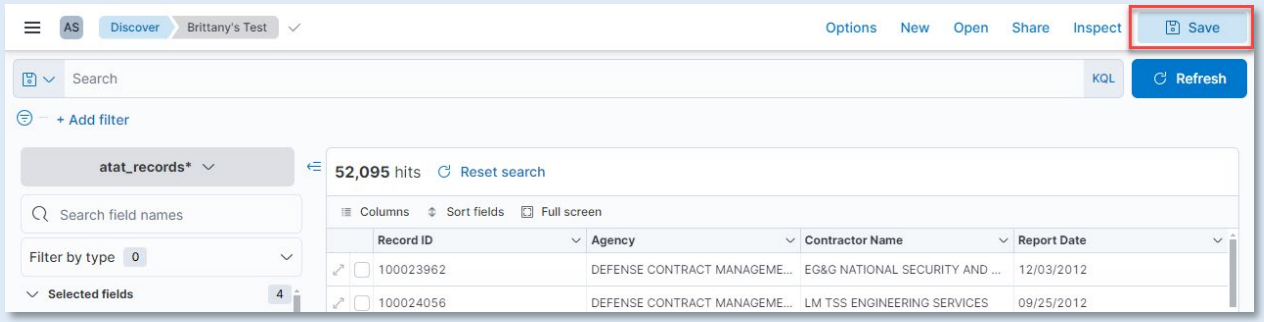
5. Search for fields in the “Search field names” bar. Add fields by clicking the “+” button.



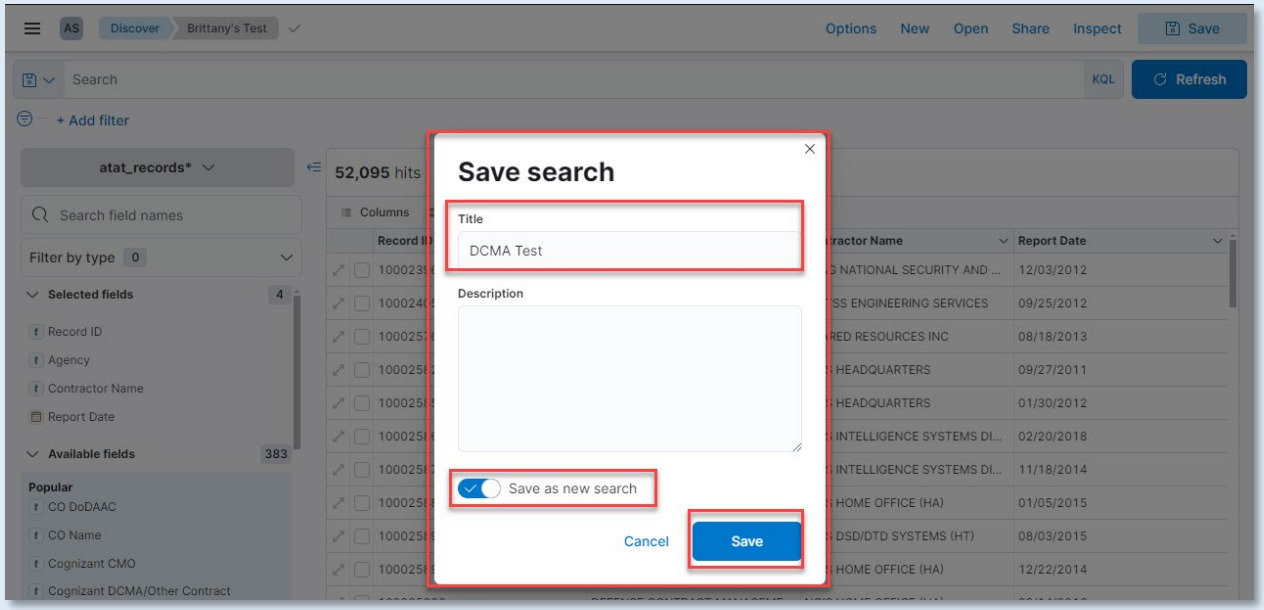
6. A table on the right side of the page is populated with the columns and data correlated to the fields added.



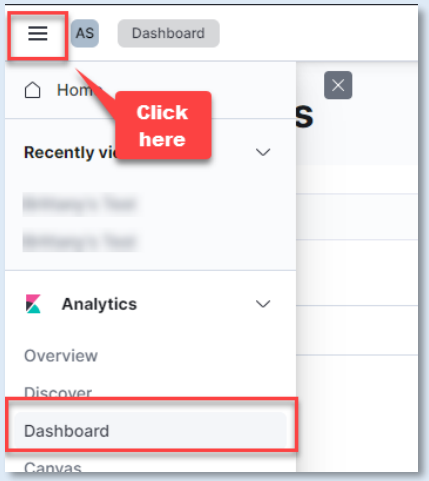
7. After all fields have been added, click the “Save” button in the top right of the page.



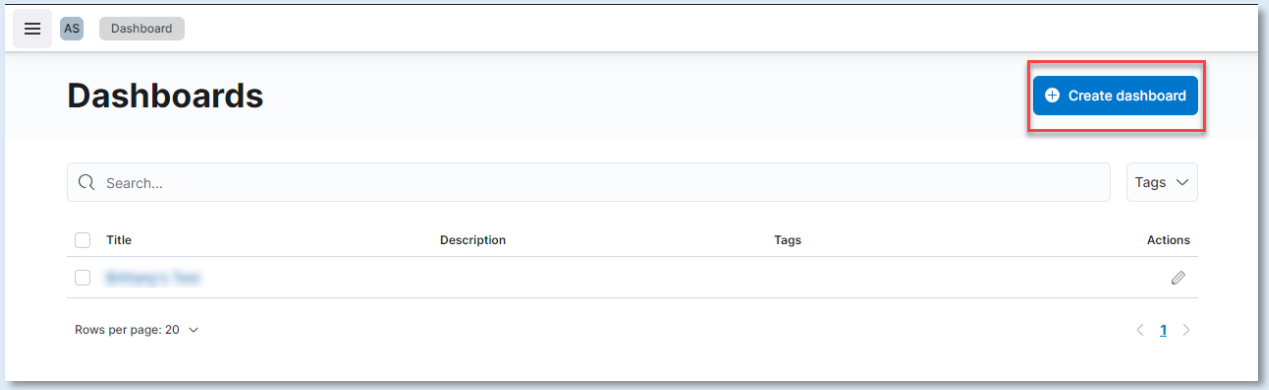
8. A ‘Save search’ pop-up displays. The “Title” field is required. Toggle ON the “Save as new search” switch. Click the “Save” button, the window closes.



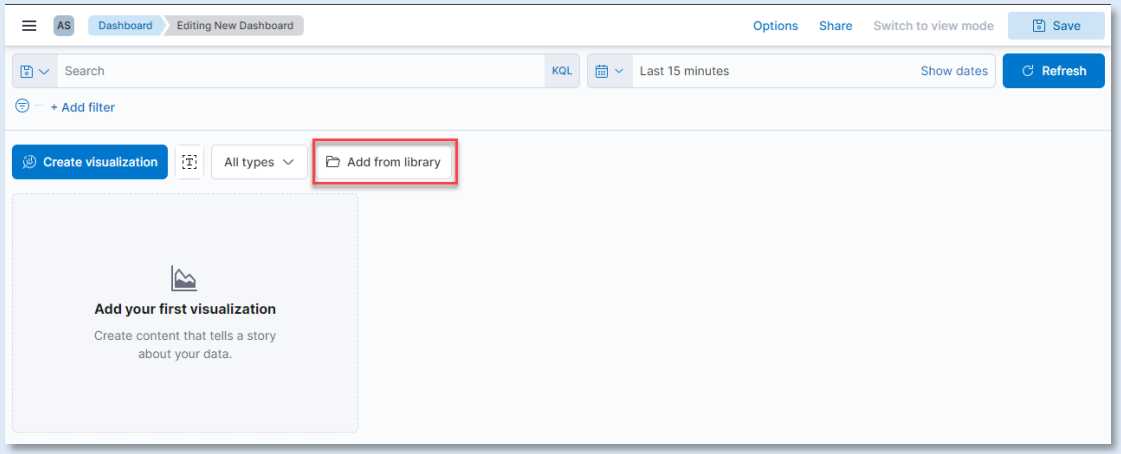
9. Click the 3 lines in the top left of the page and navigate to “Dashboard”.



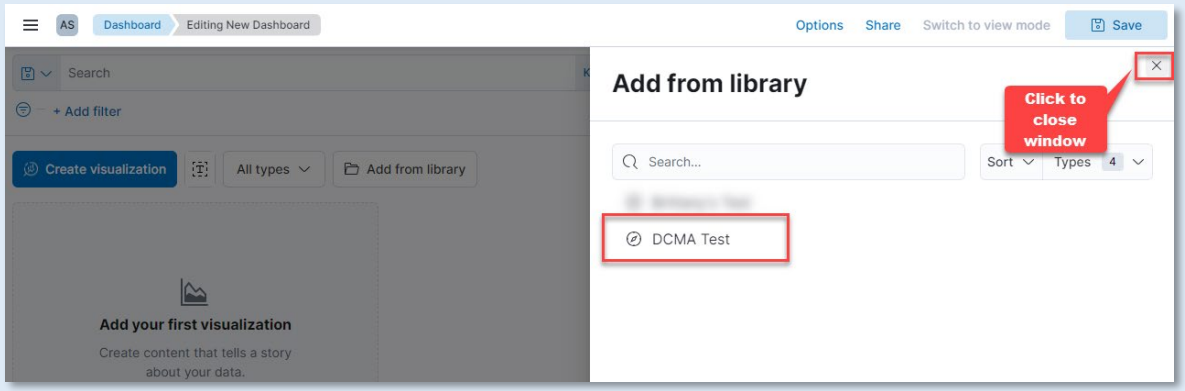
10. The ‘Dashboards’ page displays, click the “Create Dashboard” button in the top right (if the ‘Dashboards’ page is empty, the create button may be in the center of the page).



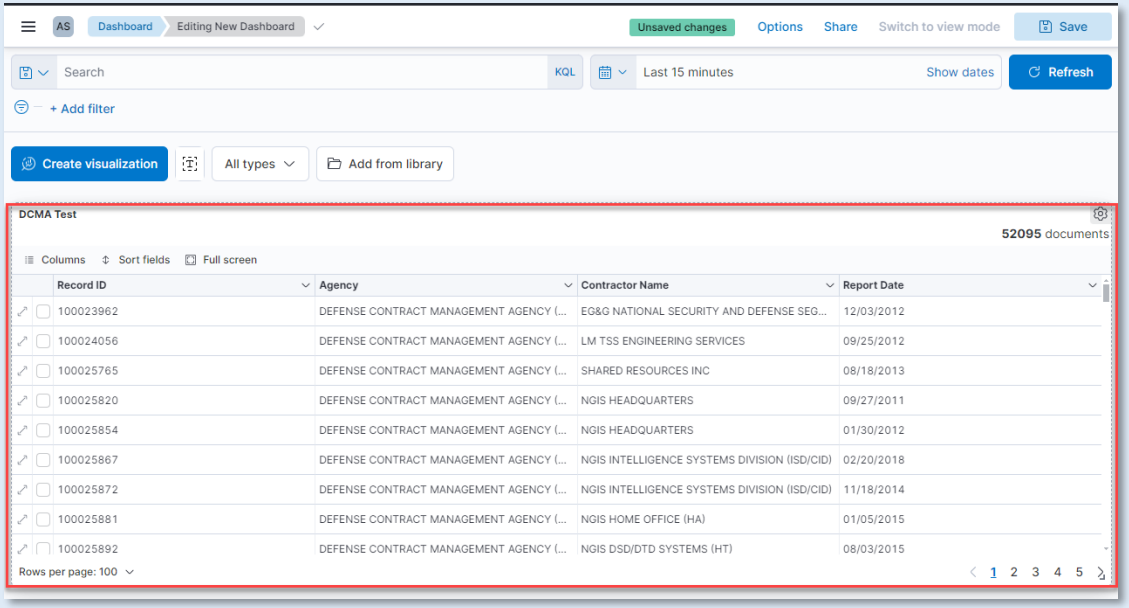
11. An ‘Editing New Dashboard’ page displays, click the “Add from library” button to add saved search to the Dashboard.



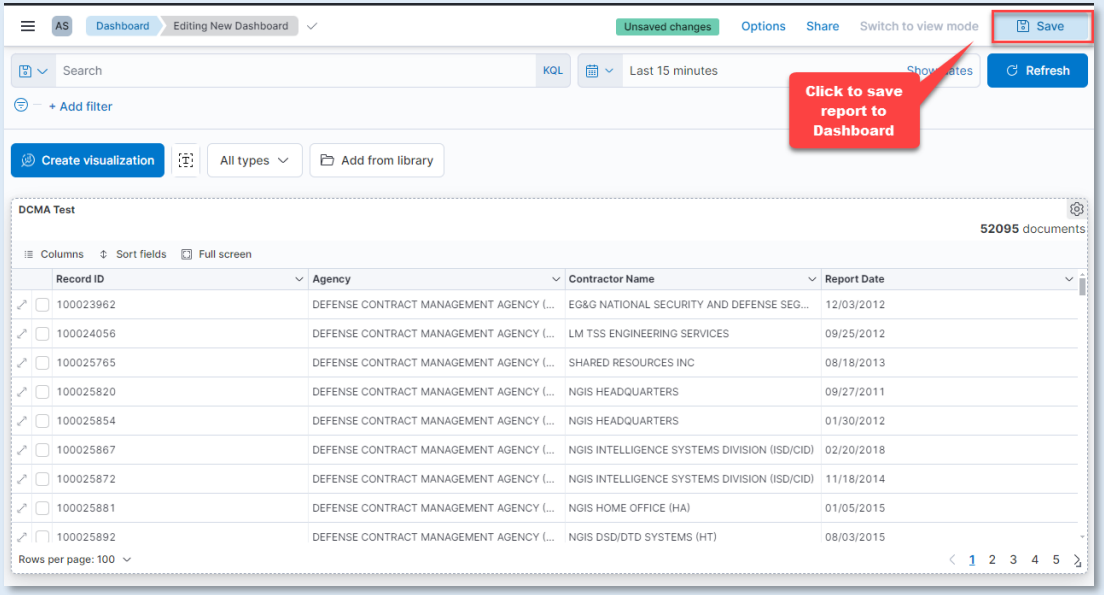
12. An “Add from Library” sidebar displays, click the search saved earlier in these steps (e.g., search titled “DCMA Test”). The Dashboard will reload in the background. Click the “x” in the top right of the sidebar to close it.



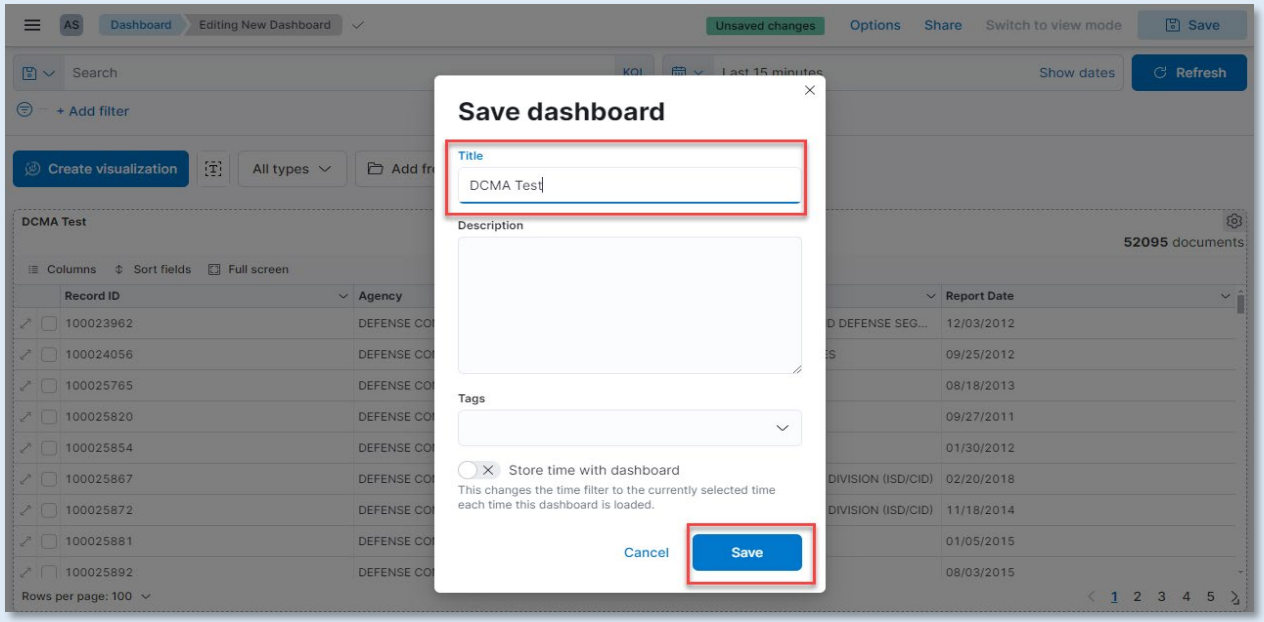
13. The ‘Editing New Dashboard’ page displays a table with the results from the saved search. At this point, if visualizations are desired, those can be added by clicking the “Create visualization” button.



14. Click the “Save” button in the top right corner to save to the ‘Module’ Collaborative Space dashboard.

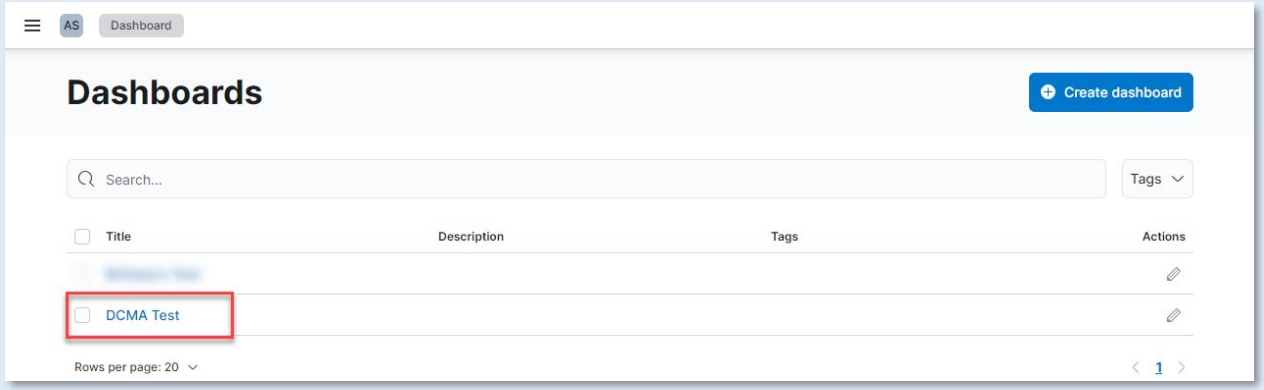


15. The ‘Save Dashboard’ pop-up displays. The “Title” field is required (“Description” is optional). Click the “Save” button.



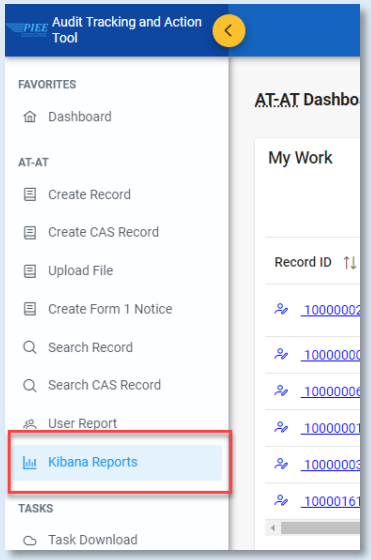
NOTE: The “Title” entered displays on the ‘Module’ Collaborative Space dashboard and will be visible to other ‘Module’ users.

16. The new report now displays in the list on the ‘Dashboards’ page. Any changes to this report will reflect for all *‘Module’* users – and all *‘Module’* users can make changes to the report. This is what makes the collaborative space different than each individual user’s personal dashboard.

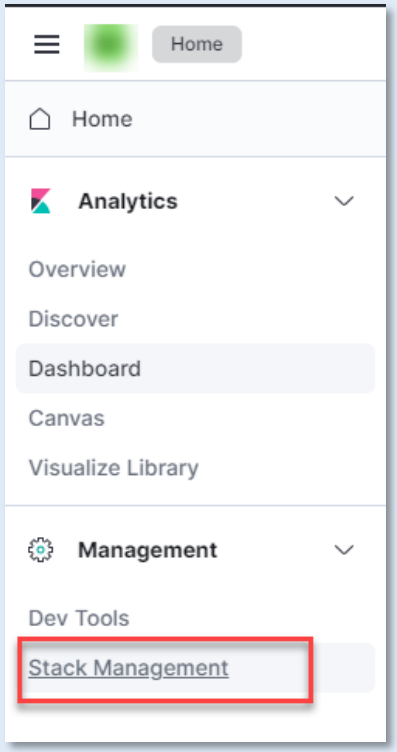


Sharing from a Personal Space to a Collaborative Space

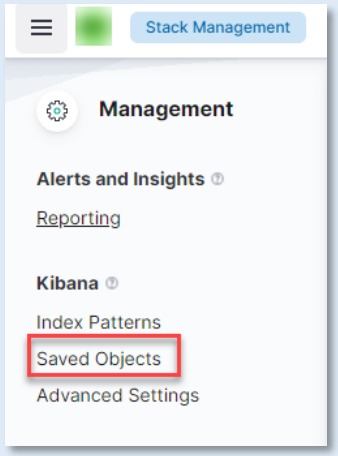
1. Access Kibana (e.g., via AT-AT)



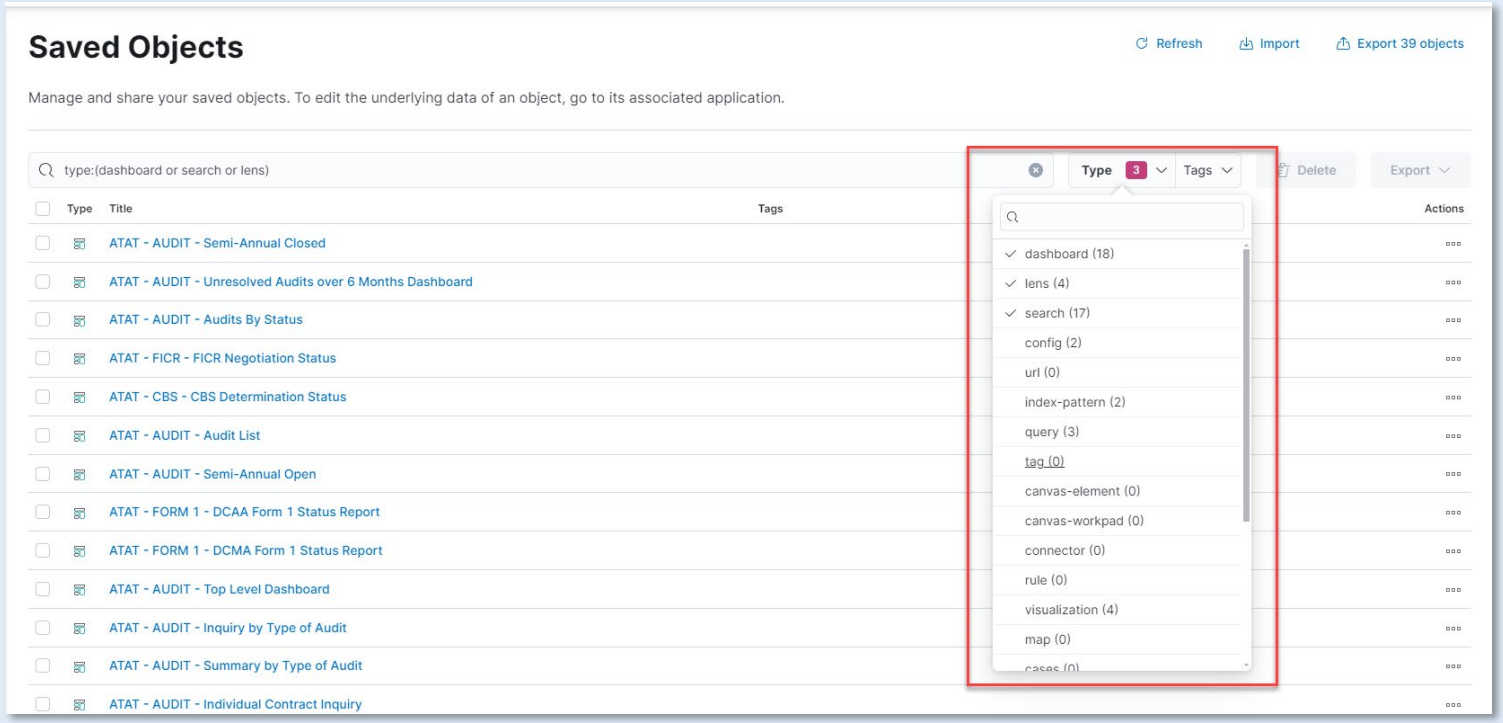
2. Click the 3 lines in the top left of the page and navigate to “Stack Management”.



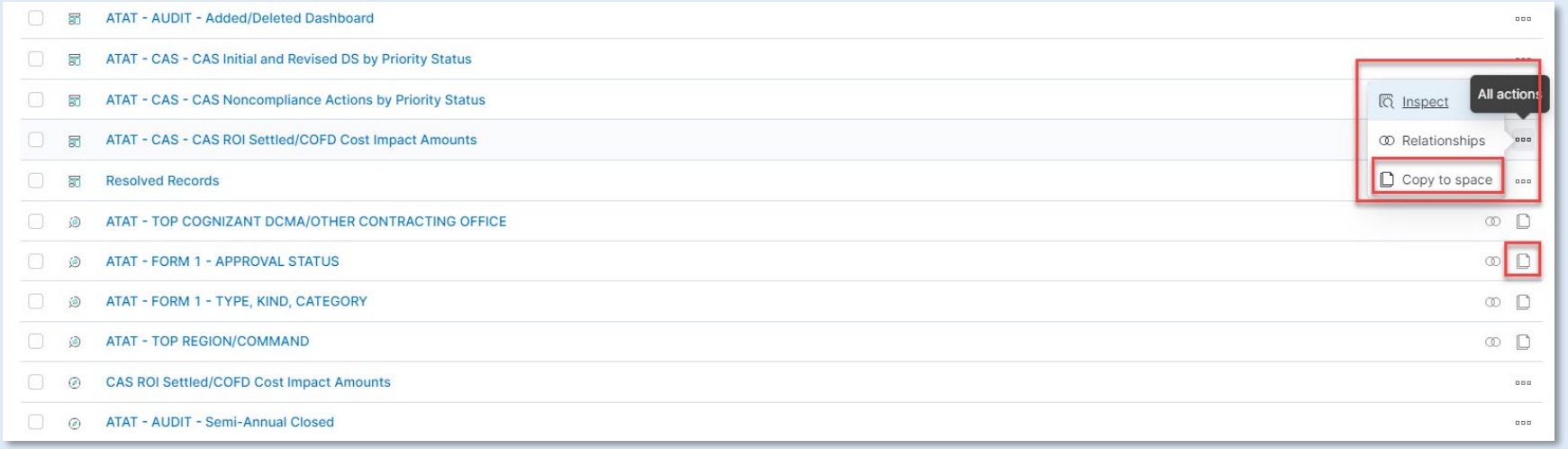
3. The Stack Management page displays. Click the “Saved Objects” link.



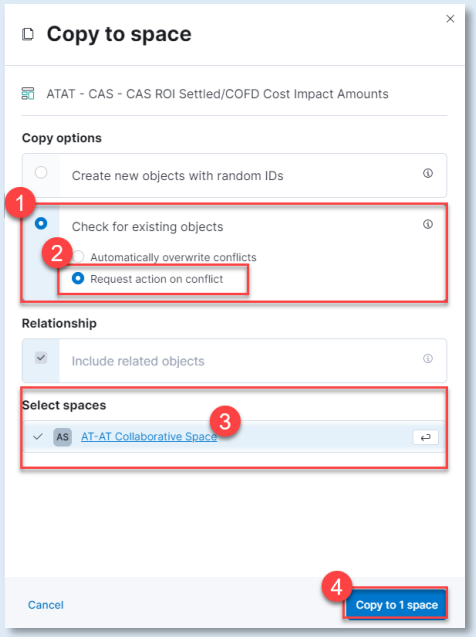
4. The Saved Objects page displays. Select “Types” to filter the list of available saved objects (e.g., Dashboard, Search, Lens).



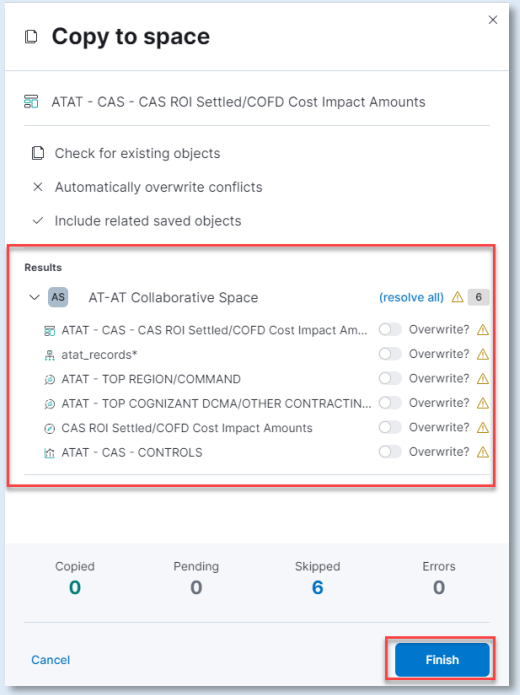
5. Click the 3 dots for All Actions and select “Copy to Space” or the “Copy” icon for the saved object to be shared to the Collaborative Space.



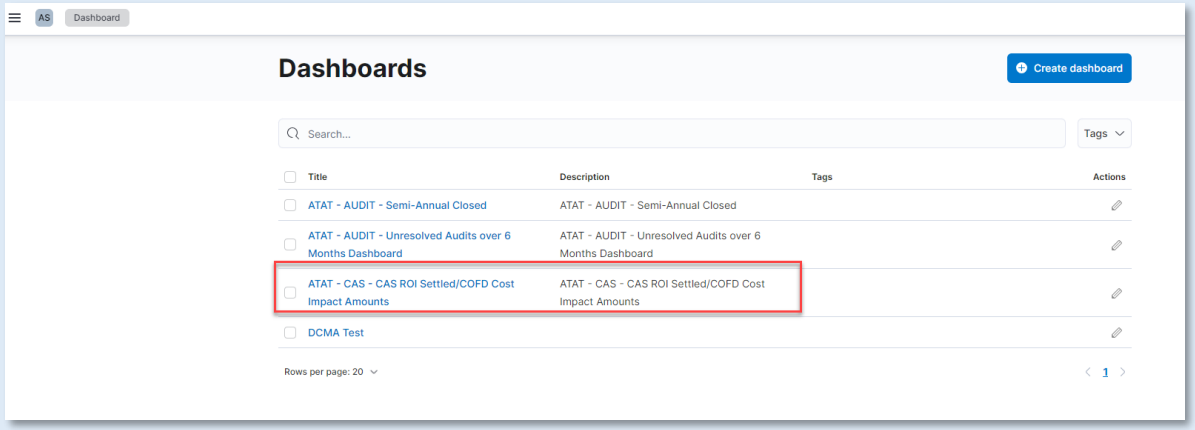
6. The Copy to space sidebar displays.
    1. Click the “Check for existing objects” radio button.
    2. Click the “Request action on conflict” sub-radio button.
    3. Select the Space to be shared to.
    4. Click the “Copy to 1 Space” button.



7. The Results of the copy display, expand the section and review and resolve any conflicts. Click the “Finish” button.



8. The Saved Objects are now available in the Collaborative Space.

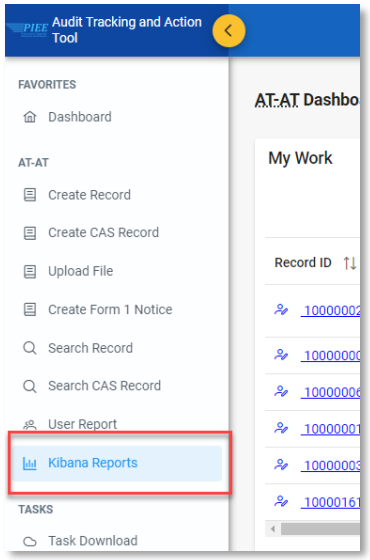


Sharing Saved Objects from User to User

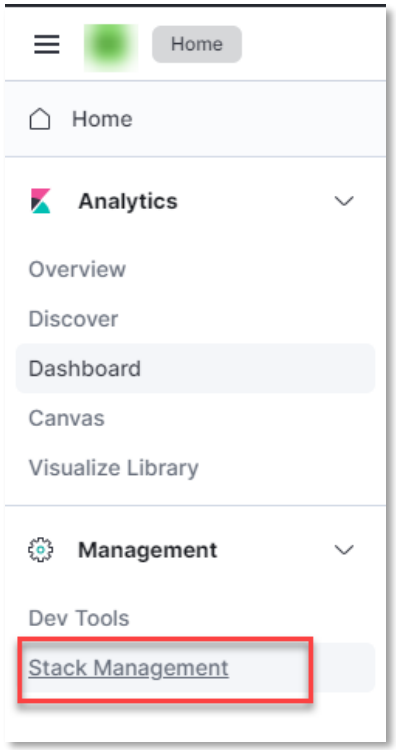
How to share Saved Objects from one User to another User

User One (Exporting)

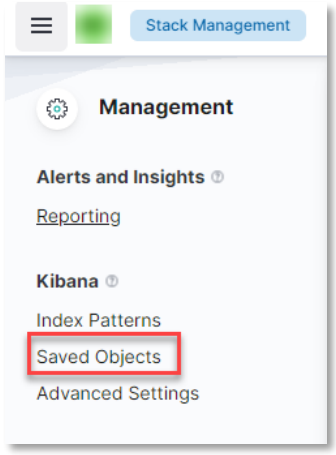
1. Access Kibana (e.g., via AT-AT)



2. Click the 3 lines in the top left of the page and navigate to “Stack Management”.

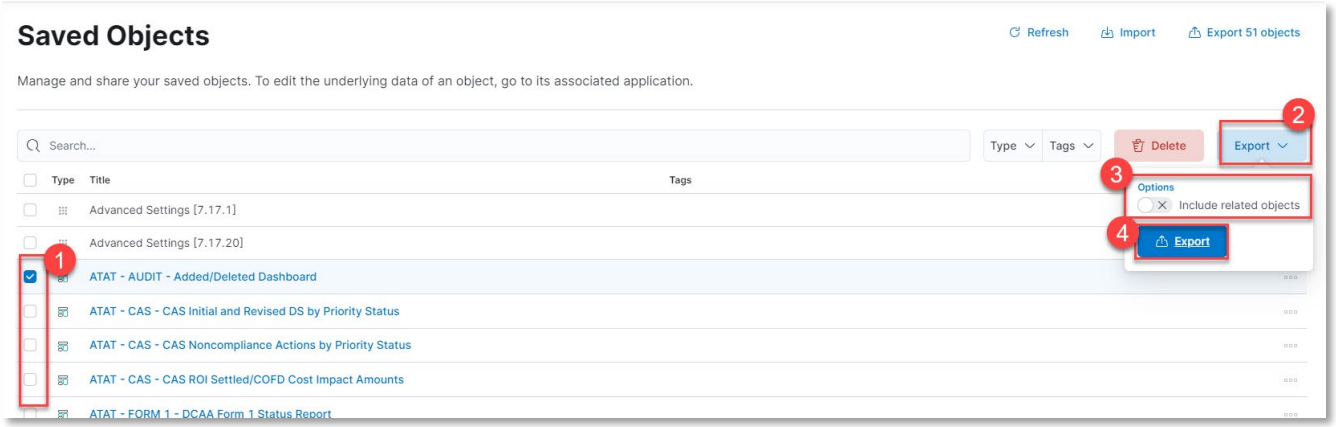


3. The Stack Management page displays. Click the “Saved Objects” link.

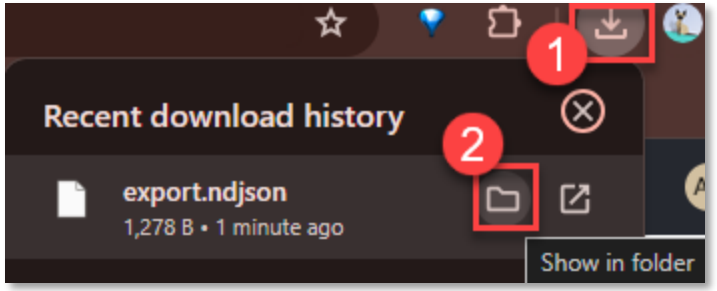


4. The Saved Objects page displays.
    1. Select one to many saved objects for export.
    2. Click the Export drop-down.
    3. Unselect the “Include related objects” unless otherwise directed.

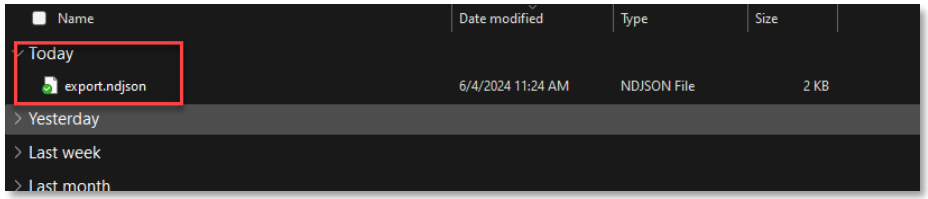
4. Click the “Export” button.



5. An .ndjson file is downloaded to the local machine. Open the folder containing the downloaded export file.

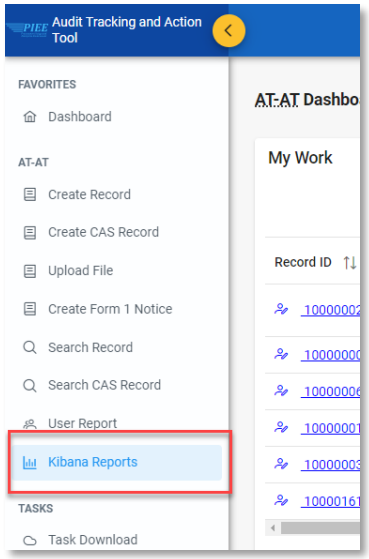


6. Forward the downloaded file to the requesting User (e.g., via email).

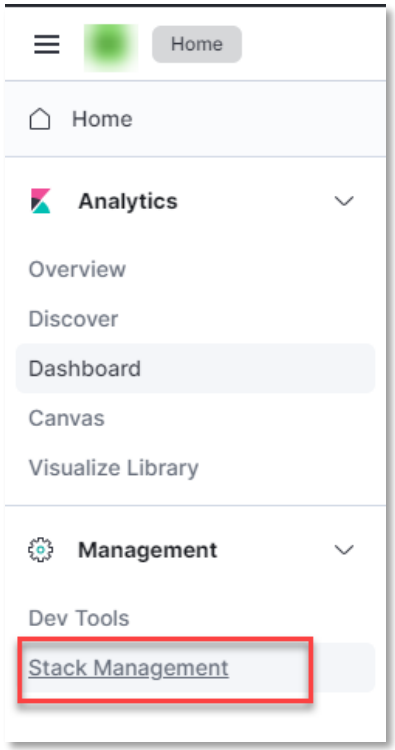


User Two (Importing)

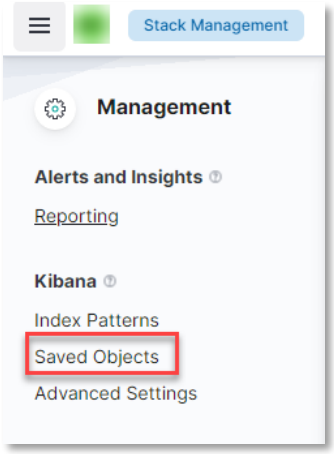
1. After receiving the exported .ndjson file from the sending User, download the file to the local machine.
2. Access Kibana (e.g., via AT-AT)



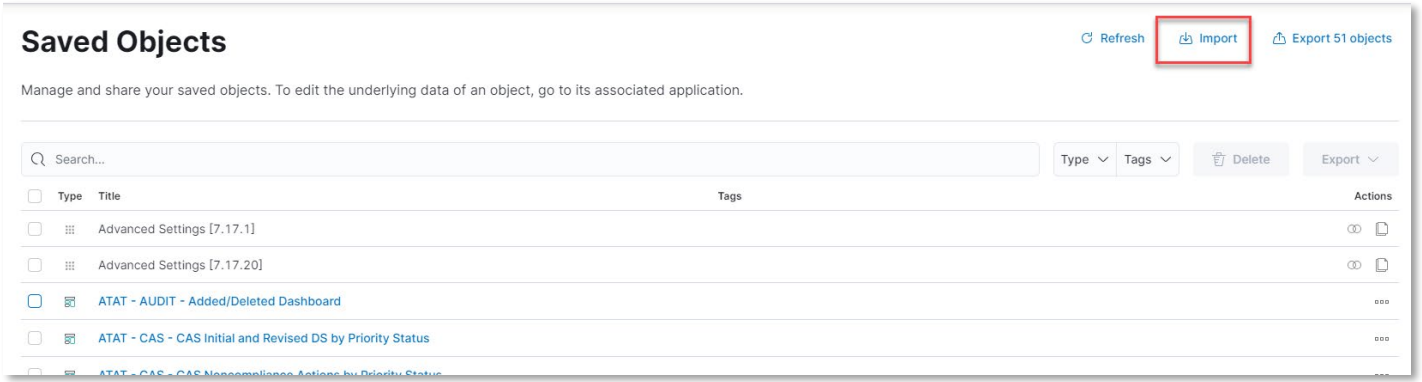
3. Click the 3 lines in the top left of the page and navigate to “Stack Management”.



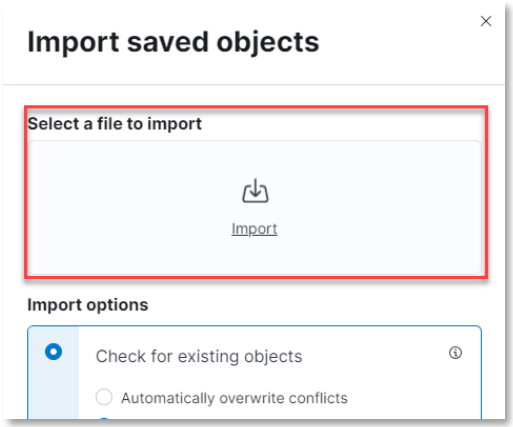
4. The Stack Management page displays. Click the “Saved Objects” link.



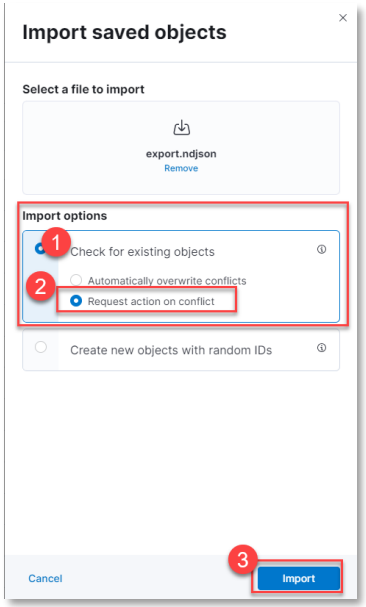
5. The Saved Objects page displays. Click the “Import” button.



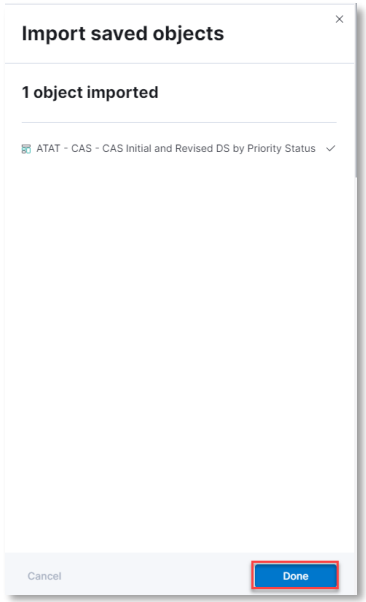
6. The Import save objects sidebar displays. Click the “Import” button or drag and drop the file on top of the sidebar.



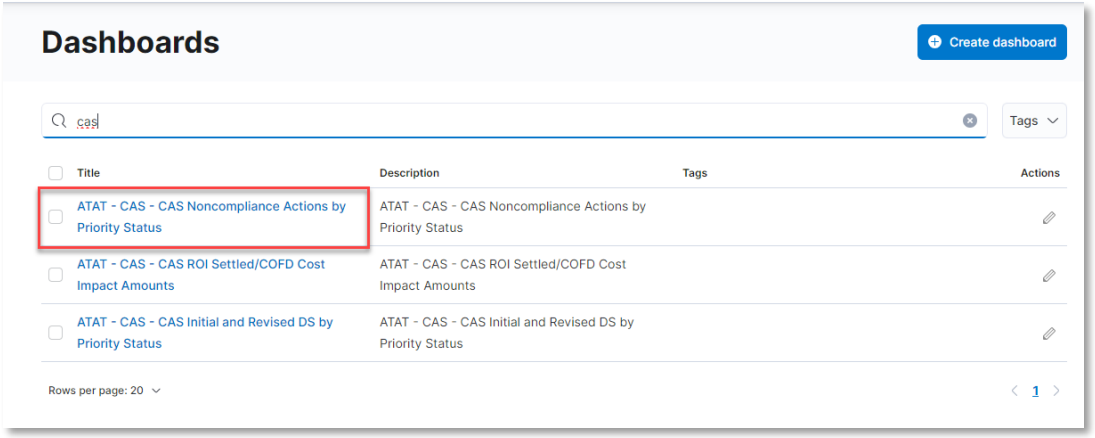
7. The imported file displays in the Select a file to import section.
    1. Select “Check for existing objects” under Import options.
    2. Select the sub-option “Request action on conflict” under “Check for existing objects”.
    3. Click the “Import” button.



8. A success screen displays the number of objects imported. Click the “Done” button.

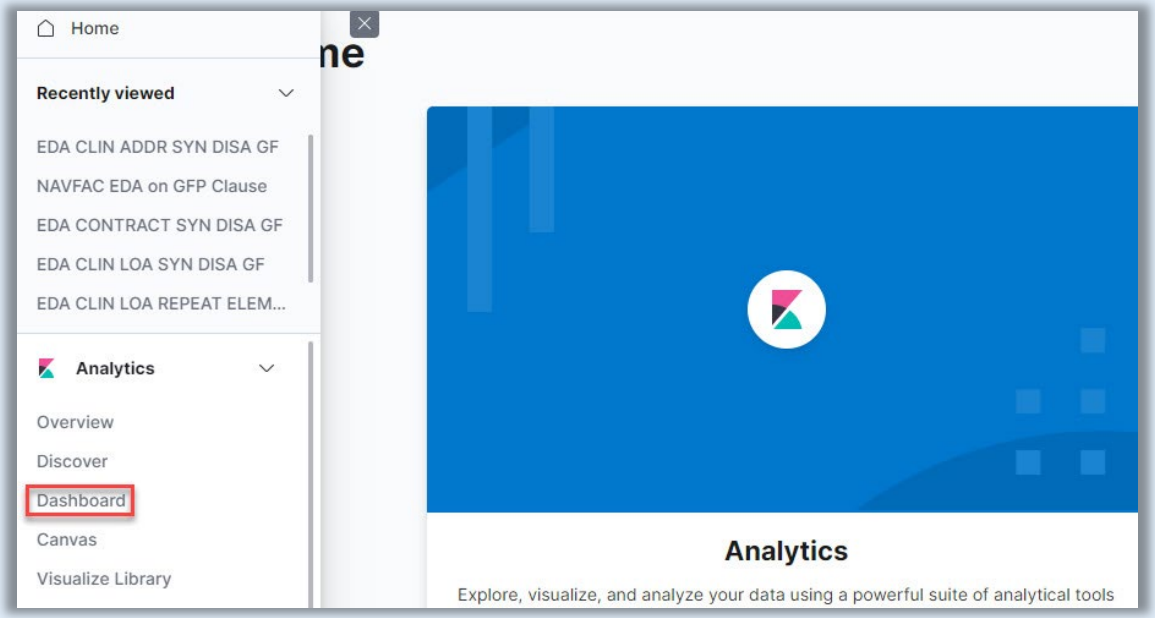


9. The imported objects display in the Saved Objects page (e.g., dashboard objects are displayed on the users Dashboard).

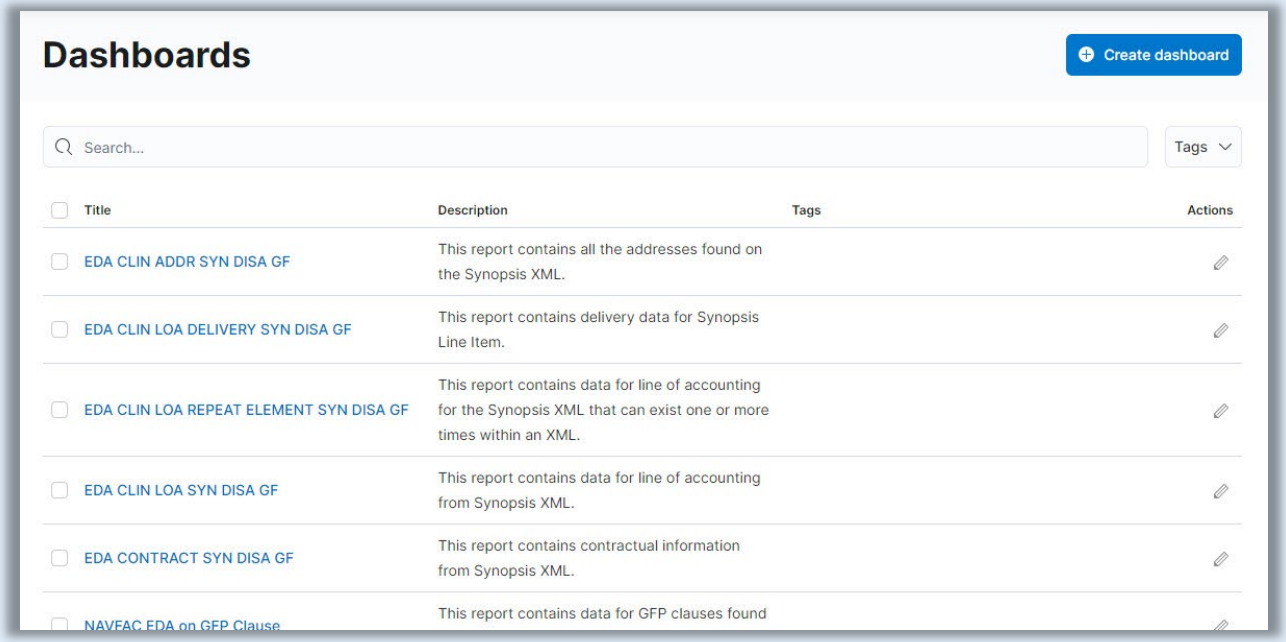


Viewing Report Data

Navigation

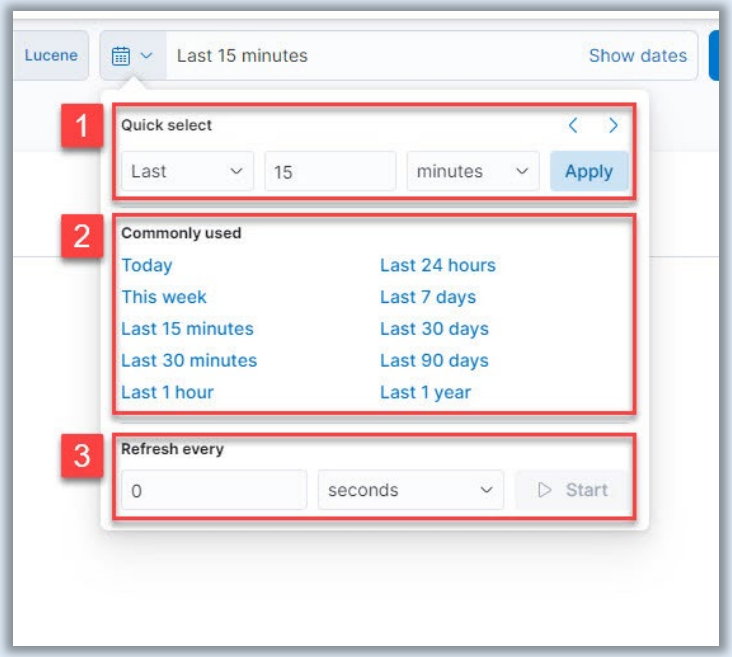


Navigate to the **Dashboard** tab in the navigation pane.



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.

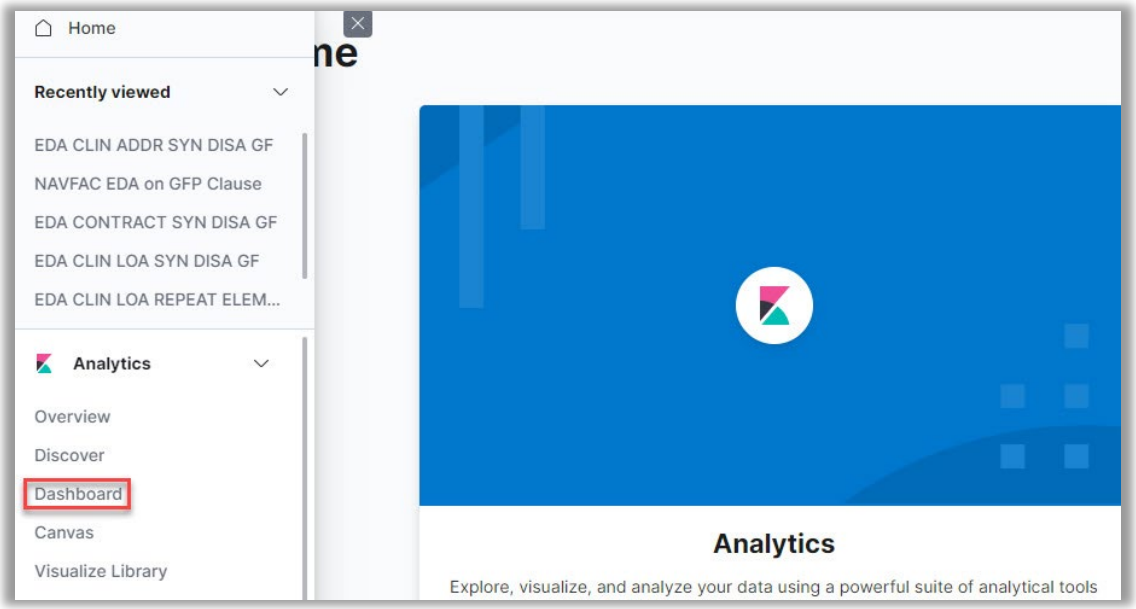
Kibana Reports are displayed on the Kibana Dashboard. Select the **menu expander** to the left of a document to view detailed data for that item.

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.

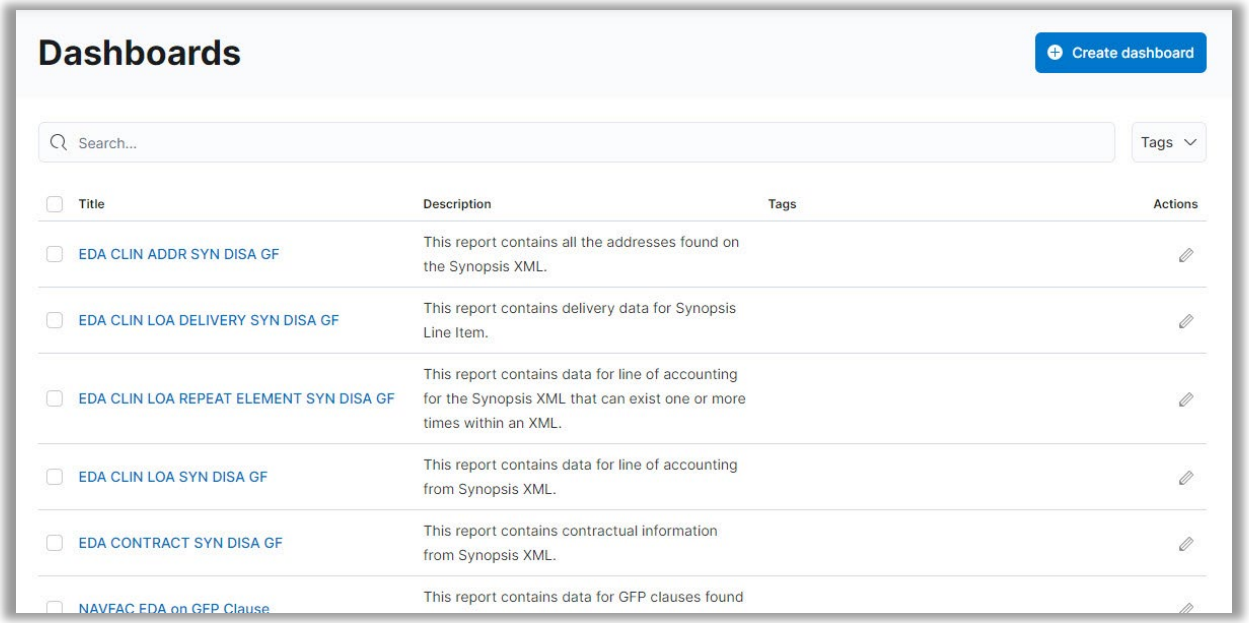
Select the **JSON** tab to view data in JSON format.

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 drop-down menu. The user's search history will also populate in the drop-down 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** drop-down menu or enter the field name manually. As data is entered into the field, the drop-down menu will display only matching items.

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

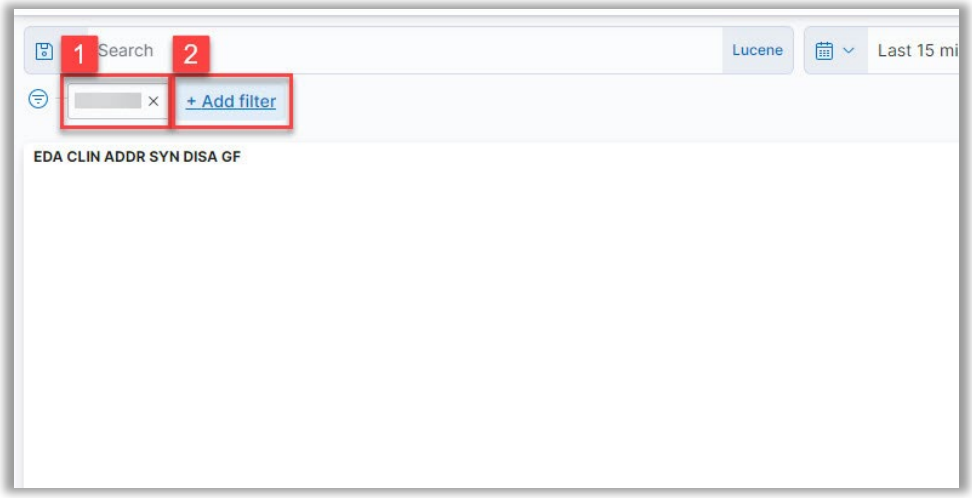
   The operators are defined as follows:
   - Is: Filter where the value for the field matches the given value.
   - Is not: Filter where the value for the field does not match the given value.
   - Is one of: Filter where the value for the field matches one of the specified values.

- 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** drop-down menu or enter a value manually. As data is entered into the field, the drop-down 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.

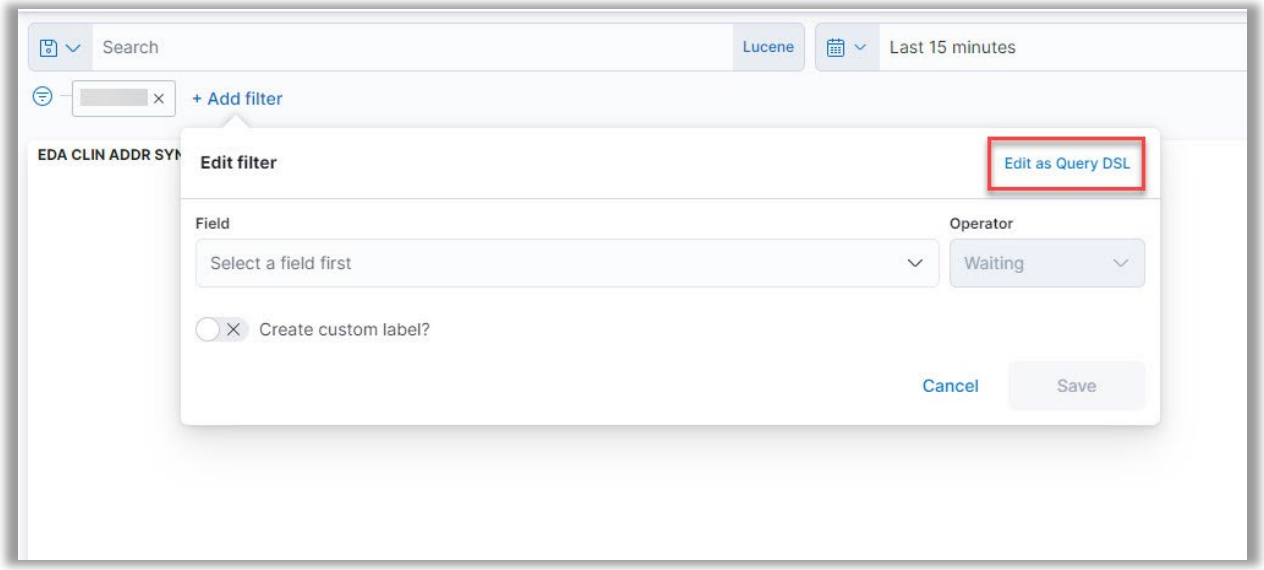
5. Select the **Save** button on the Edit filter modal.



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*"
    }
  }
}
```

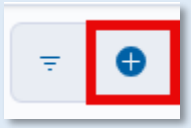
Additional filters may be added using the **Edit as Query DSL** link. All entered queries will be chained together to return the desired results.

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

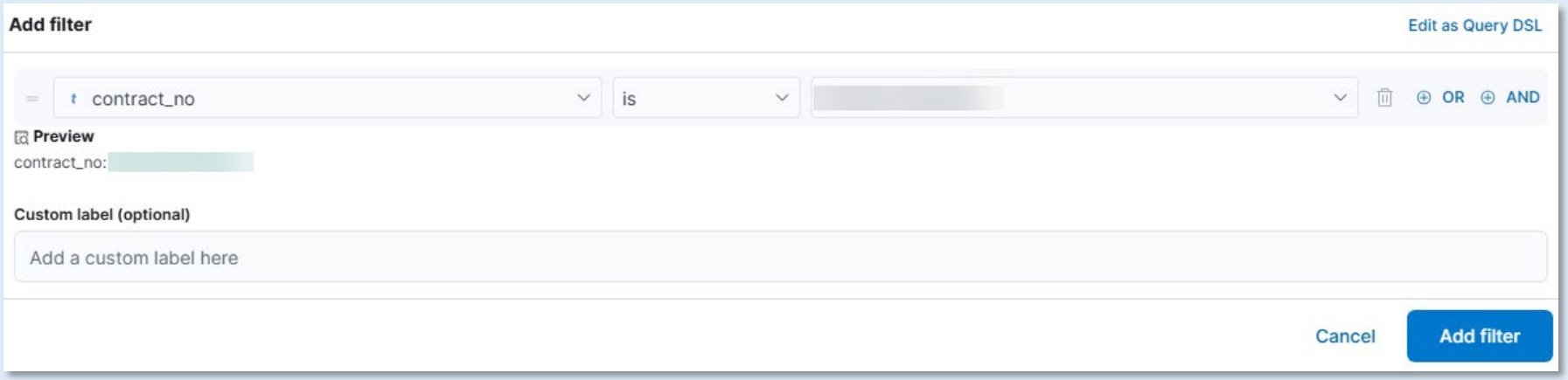
Adding Filters to Dashboards

To refine and focus analysis on specific subsets of data, filters can be added to the dashboard. This allows for dynamic adjustment of the data displayed in visualizations and reports, making it easier to identify trends, outliers, and relevant information.

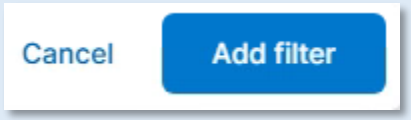
1. Navigate to the Dashboard:
    - Open Kibana and go to the Dashboard tab in the navigation pane.
    - Select the dashboard to edit.
2. Add a Filter:
    - Click on the **Add filter** button located on the left side.
    - This will open the **Add filter** modal where the filter can be configured.



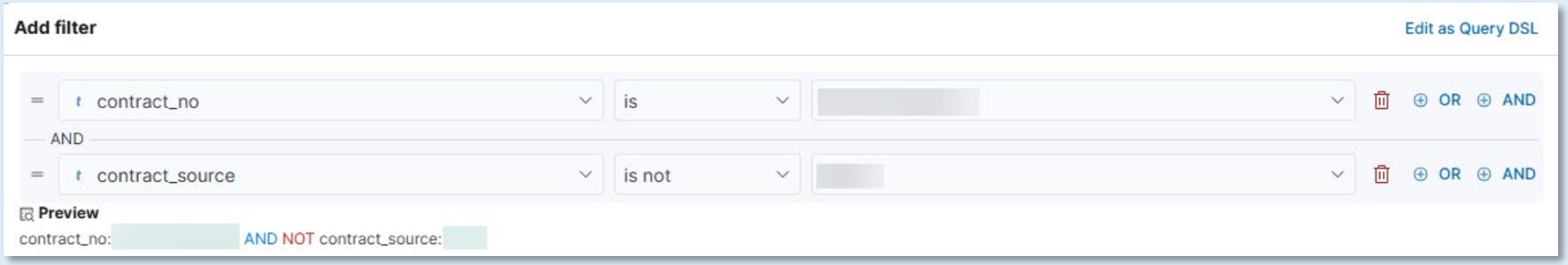
3. Configure the Filter:
    - **Select a field:** Select the field to filter from the drop-down menu or enter the field name manually.
    - **Select operator:** Choose a search modifier from the Operator drop-down menu (e.g., "Is", "Is not", "Is one of", etc.).
    - **Enter/Select a value:** Enter the value or select an item from the Value drop-down menu (if available).
    - **Add a Custom label (optional)**



4. Add the Filter:
    - Click the **Add Filter** button on the Add filter modal.
    - Click the **Cancel** button to cancel filter configuration.
    - The report results are filtered by the criteria specified.



5. Add Multiple Filters:
    - Apply multiple filters by selecting the **Add Filter** button and repeating the previous steps.



6. Use Advanced Queries (Optional):
    - For more complex filtering, select the **Edit as Query DSL** link on the Add a Filter menu.
    - Enter the advanced query in the Query DSL format.

Managing Added Filters

After adding a filter to the dashboard, manage it further by clicking on the filter. This action displays a pop-up menu with several options:

1. **Pin across all apps**: This option allows for the filter to be pinned so that it applies across all applications.
2. **Edit Filter**: Use this to modify the existing filter criteria.
3. **Exclude results**: This option excludes the results that match the filter criteria.
4. **Temporarily disable**: Temporarily disable the filter without removing it.
5. **Delete**: This option allows to permanently remove the filter from the dashboard.

For more information regarding adding filter to the dashboard, please visit: https://www.elastic.co/docs/explore-analyze/query-filter/filtering

Adding Controls to Dashboards

Controls are interactive panels that can be added to dashboards to help users filter and display only the data they want to explore more efficiently. Controls apply filters to relevant panels to focus on specific data segments without writing filtering queries.

Types of Controls

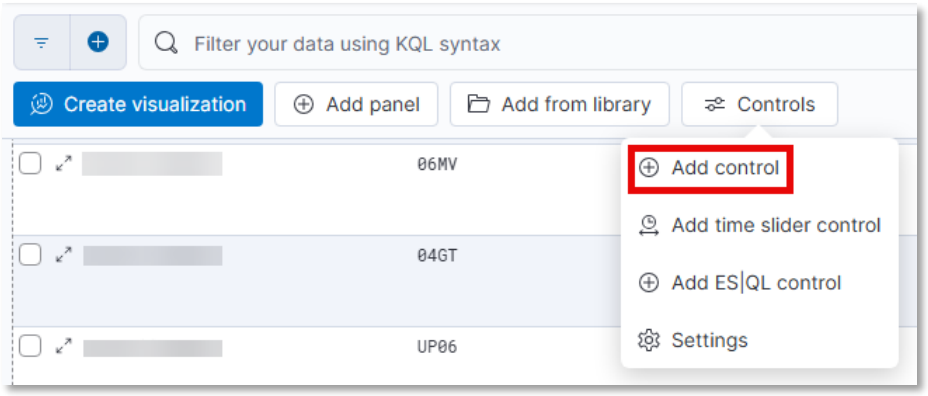
Options list: Adds a drop-down that allows users to filter data by selecting one or more values.
Range slider: Adds a slider that allows users to filter the data within a specified range of values. This type of control only works with numeric fields.
Time slider: Adds a time range slider that allows users to filter the data within a specified range of time, advance the time range backward and forward by a defined unit, and animate changes in data over the specified time range.

Creating Options List and Range Slider Controls

1. Navigate to the Dashboard:
    - Open Kibana and go to the Dashboard tab in the navigation pane.
    - Select the dashboard to edit.
2. Select the **Controls** button. A pop-up menu displays with several options:
    - **Add control:** Creates standard controls such as Options Lists and Range Sliders that allow users to filter dashboard data by selecting values or ranges from configured fields.
    - **Add time slider control:** Adds a time-based control that allows users to filter data within a specified time range, navigate through time periods, and animate changes in data over time.
    - **Add ES|QL control:** Creates variable controls (also called ES|QL controls in versions 9.0 and 9.1) that can be bound to ES|QL visualizations. These controls act as variables in ES|QL queries, enabling dynamic filtering and configuration options for advanced users working with ES|QL-based visualizations. For more information regarding adding variable controls, please visit: https://www.elastic.co/docs/explore-analyze/dashboards/add-controls#add-variable-control

- **Settings:** Opens the control settings panel where global control configurations can be managed, such as enabling or disabling the "Auto apply filters" option that determines whether dashboard updates occur immediately when control selections are made or only after clicking the Apply button.

3. Select **Add control**.



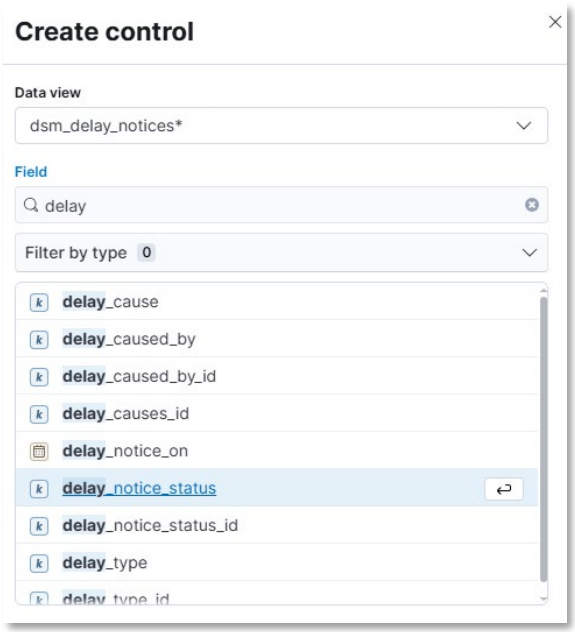
4. On the **Create control** flyout, from the **Data view** drop-down:
   - **Data view:** Select the **Data view** that contains the field to be used for the Control.
   - **Field:** Select the field to filter on.
   - **Control type:** Select whether the control should be an **Options list** or a **Range slider**. *NOTE: Range sliders are for Number type fields only.*
5. Define how the control should appear.

   For Options lists:
   - **Label:** Overwrite the default field name.
   - **Medium width:** Define the amount of horizontal space the control should take up.
   - **Selections:** Choose to filter by multiple values or just one using the control.
   - **Search:** For Options list controls on string and IP address fields, the embedded search behavior can be configured:
     i. **Prefix:** Display options that start with the entered value.
     ii. **Contains:** Show options that include the entered value. This option is only available for string fields and may take longer to display results.
     iii. **Exact:** Show options that exactly match the entered value.
   - Additional settings:
     i. **Use global filters:** A setting at the panel level that applies to each individual control. This setting is enabled by default.
     ii. **Validate user selections:** Highlight selections that do not return any data.
     iii. **Ignore timeout for results:** Delay displaying results until the full list is loaded.

   For Range sliders:
   - **Label:** Overwrite the default field name.
   - **Step size:** Determine the slider's number of steps. The smaller a slider's step size, the more steps it has.
   - **Additional settings:**

i. **Use global filters:** A setting at the panel level that applies to each individual control. This setting is enabled by default.
ii. **Validate user selections:** Highlight selections that do not return any data.

6. Select the **Save** button to save the control or **Cancel** the configuration.

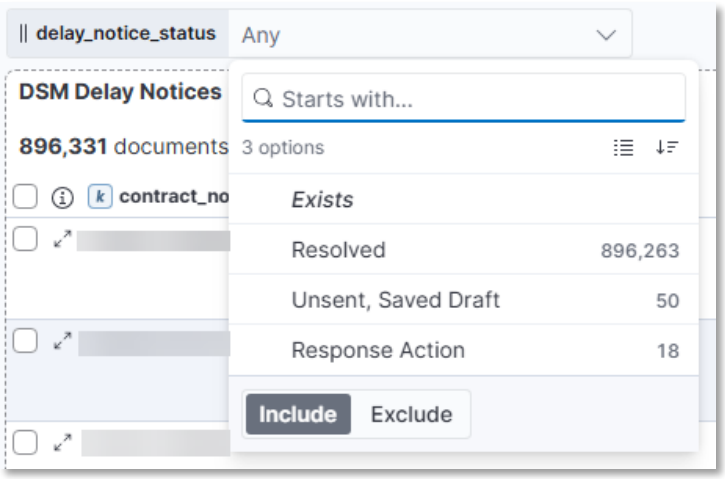


7. After the control is configured and saved, the control becomes active on the dashboard and is available for use.

Adding Options List Controls

After configuring a control as an Options List, a drop-down displays that allows for filtering data by selecting one or more values to focus on specific subsets.

1. **Options:** Select an option from the drop-down. The options displayed in the Options List drop-down depend on available values for that field based on the data in the system.
2. **Include/Exclude buttons:** Select the **Include** button to display only data that matches the selected values or select **Exclude** to filter out data that matches the selected values.
3. **Manage Options control:** Hover over the added control to manage the control:
    - **Clear:** Select to clear the selected options.
    - **Edit:** Select to edit the added options.
    - **Delete:** Select to delete the control.

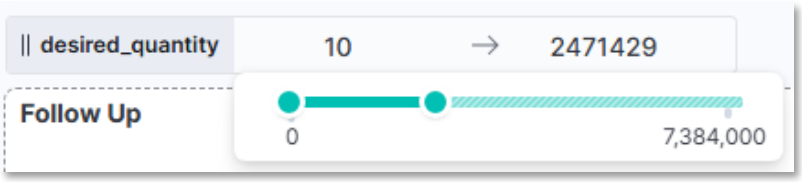


4. Save the dashboard.

Adding Range Slider Controls

After configuring a control as a Range Slider, a slider displays that allows for filtering data within a specified range of numeric values to focus on specific subsets.

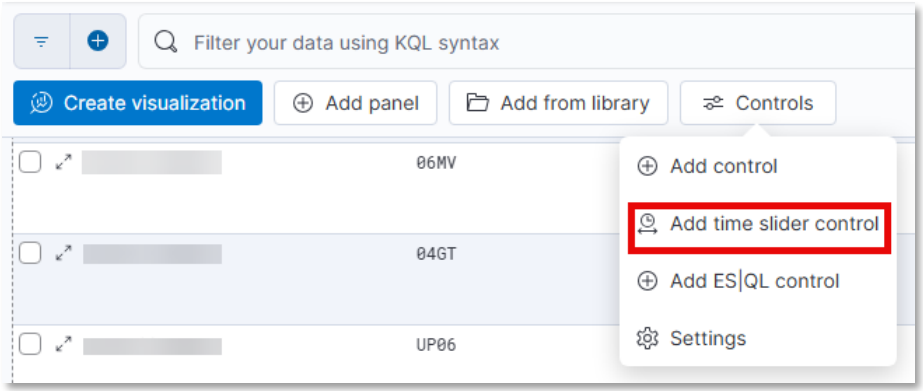
1. **Slider:** Drag the slider handles to select the minimum and maximum values for the range. The range slider only works with numeric fields and displays the available range based on the data in the system.
2. **Value inputs:** Alternatively, enter specific numeric values in the minimum and maximum input fields to define the exact range.
3. **Include/Exclude buttons:** Select the **Include** button to display only data that falls within the selected range or select **Exclude** to filter out data within the selected range.
4. **Manage Range Slider control:** Hover over the added control to manage the control:
    - **Clear:** Select to reset the slider to its default range.
    - **Edit:** Select to edit the control configuration including step size and label.
    - **Delete:** Select to remove the control from the dashboard.



5. Save the dashboard.

Creating Time Slider Controls

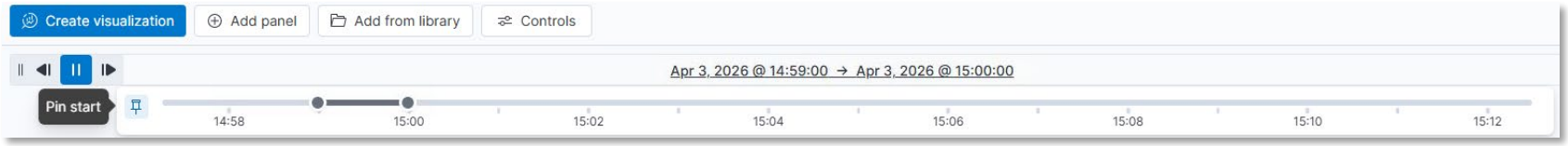
1. **Navigate to the Dashboard:**
    - Open Kibana and go to the Dashboard tab in the navigation pane.
    - Select the dashboard to edit.
2. **Select the Controls button.** A pop-up menu displays with several options:
    - Add control
    - **Add time slider control**
    - Add ES|QL control
    - Settings
3. Select **Add time slider control**.



Adding Time Slider Controls

After adding a time slider control to the dashboard, a slider displays that allows for filtering data within a specified range of time based on the global time filter settings. To change the time range in the time slider control, modify the global time filter settings. *NOTE: Only one time slider control can be added per dashboard.*

1. **Time range slider:** Drag the slider handles to adjust the start and end times within the overall time range. The dashboard updates to show only data within the selected time period.
2. **Navigation buttons:** Use the previous and next buttons to advance the time range backward or forward by the defined time unit.
3. **Play button:** Select the play button to animate the time range changes and watch how the data evolves over the specified time period.
4. **Manage Time Slider control:** Hover over the added control to manage the control:
    - **Edit:** Select to edit the control configuration.
    - **Delete:** Select to remove the control from the dashboard.



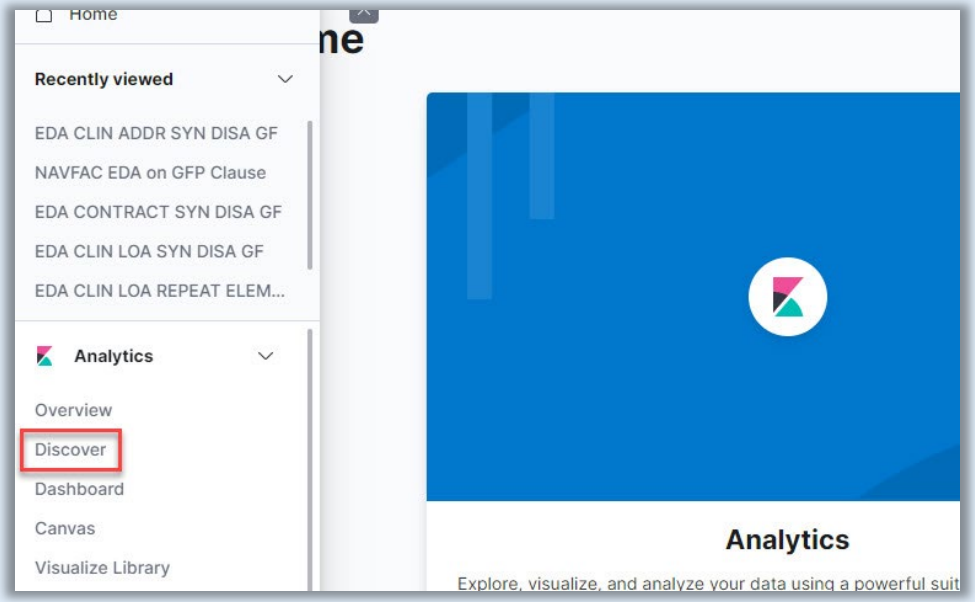
5. Save the dashboard.

NOTE: The time slider control is always pinned to the dashboard header and applies globally to all panels on the dashboard. Changes to the global time filter will affect the time slider's available range.

For more information regarding adding controls to the dashboard, please visit: https://www.elastic.co/docs/explore-analyze/dashboards/add-controls

Exporting Report Data

Users may export report data from Kibana in CSV format.



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

11. Select the **Open** link in the menu bar.

12. In the Open search modal, select a **Search** from the list of reports.

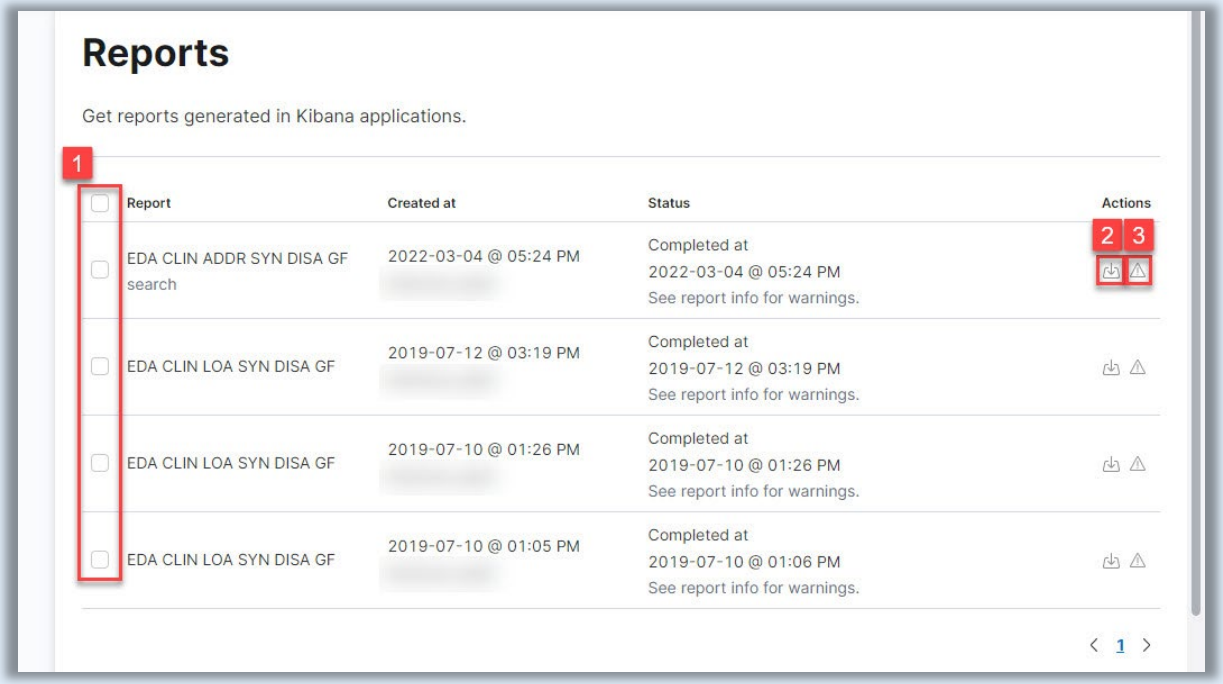
13. Select the **Share** link in the menu bar.

14. Select **CSV Reports** from the Share This Search drop-down menu.

15. 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.

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

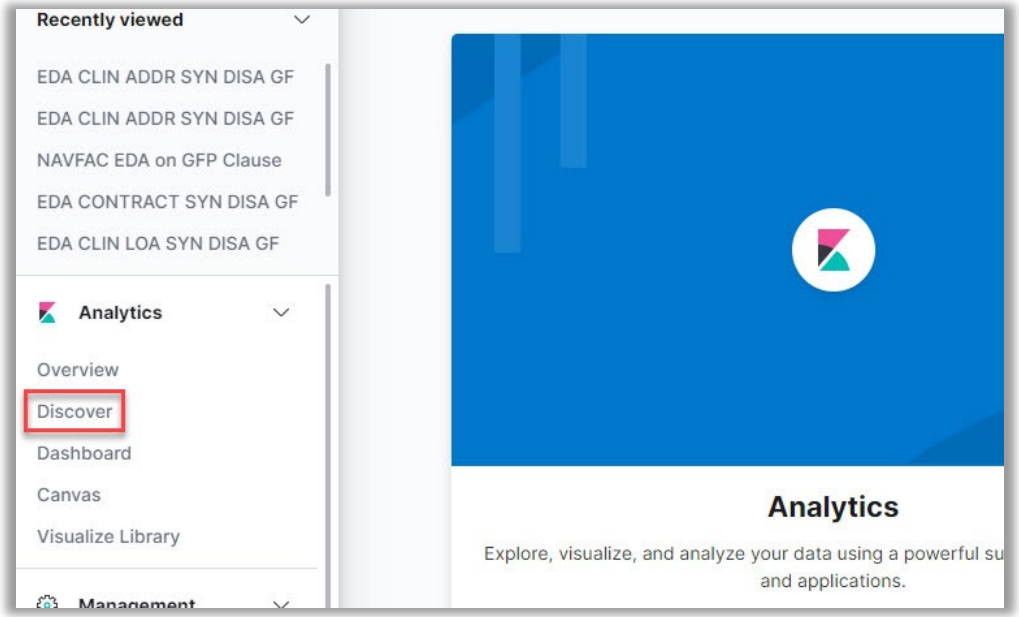
17. Select the **Reporting** link under Alerts and Insights in the navigation pane.



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

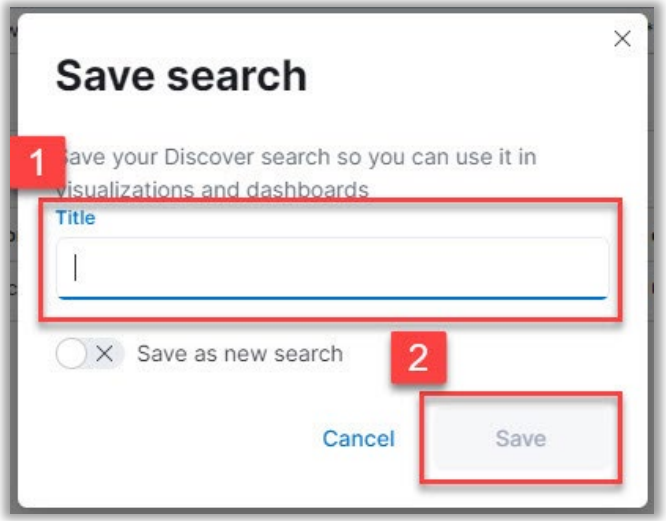
Navigation



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

Save Search

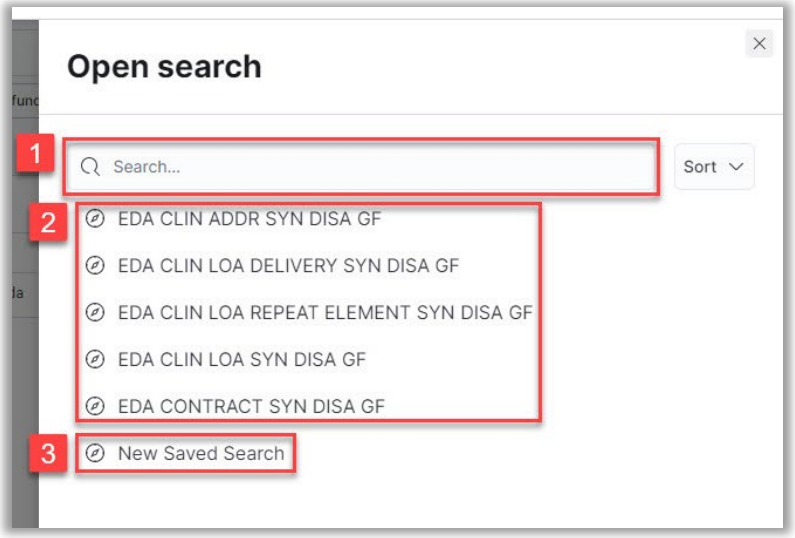
To save a new search, select **Save** in the Kibana toolbar.



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.

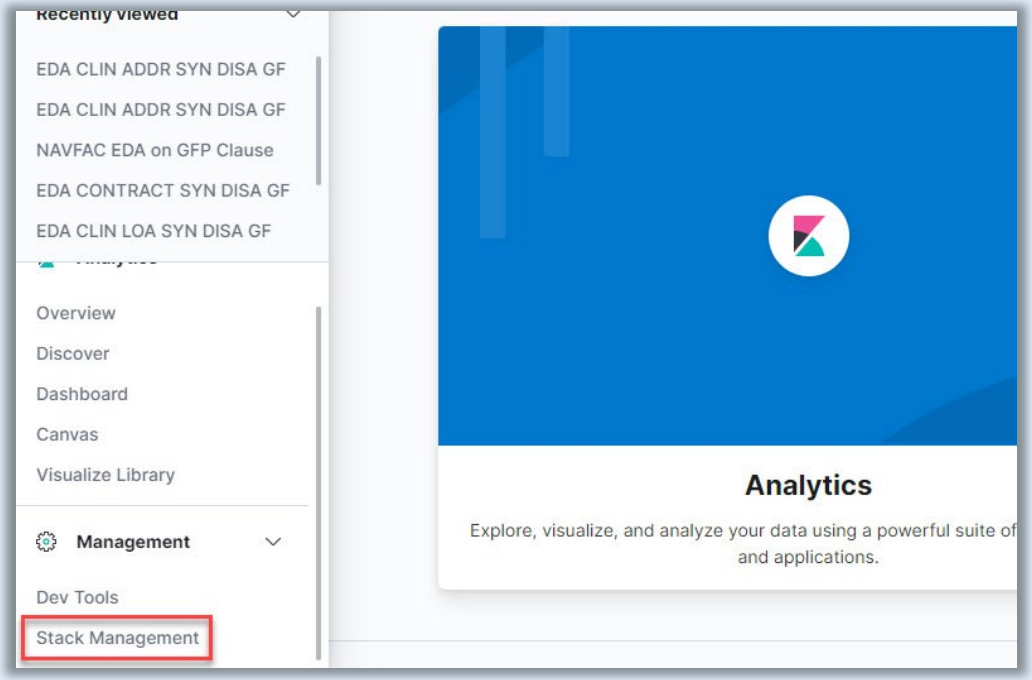


1. The list may be filtered using the **Search** field.

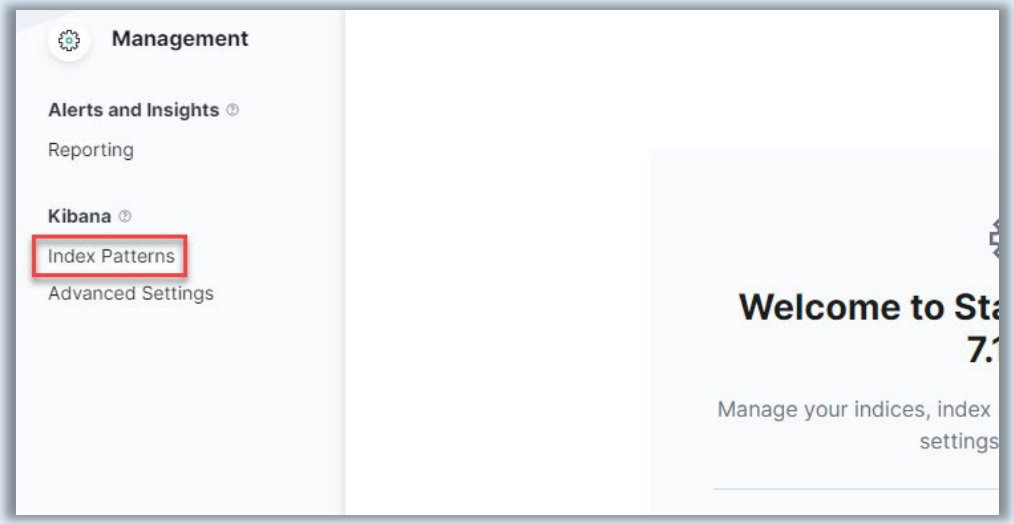
2. Saved searches will be populated in the Open Search menu. Select the desired **search**.
3. A new search may be created using the **New Saved Search** option.

Index Patterns

Navigation

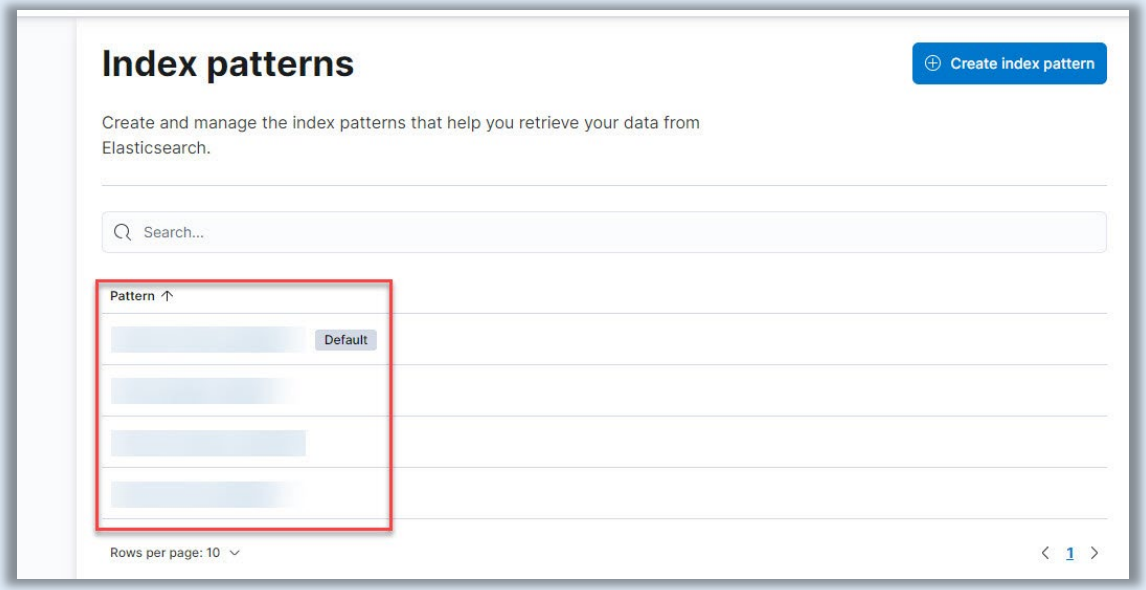


Navigate to the **Stack Management** tab in the navigation pane.



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

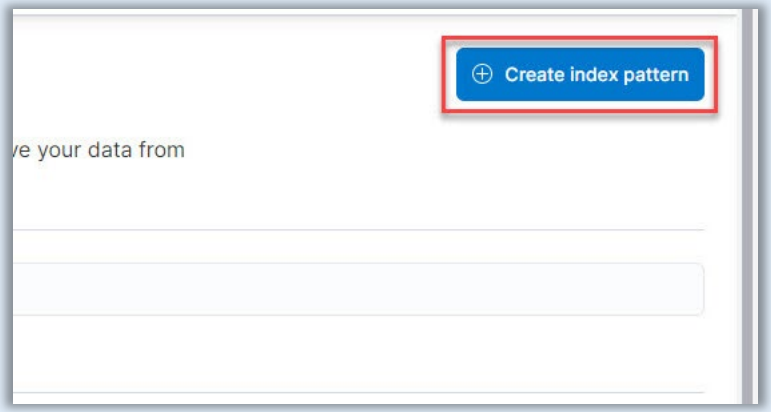
Viewing Index Patterns



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

Creating An Index Pattern

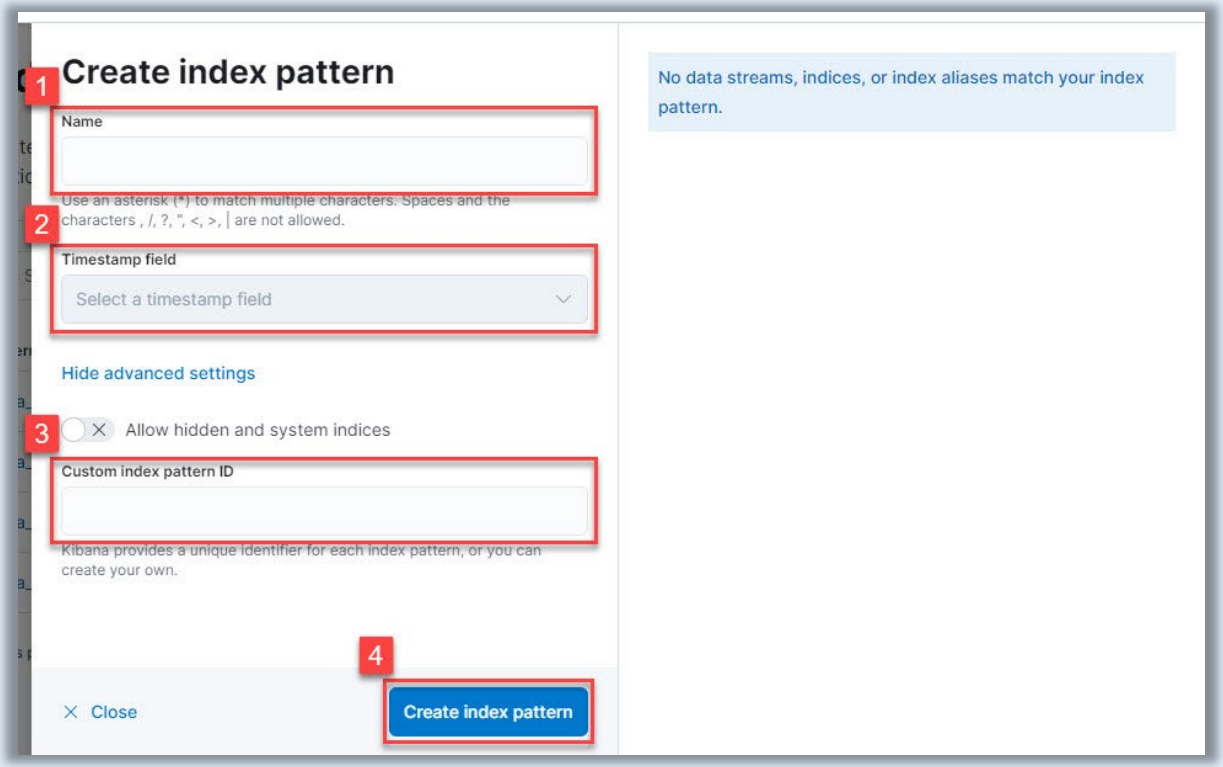
Users may create index patterns to specify which Elasticsearch indices to explore in Kibana. For more information on creating index patterns, please visit https://www.elastic.co/guide/en/kibana/7.17/index-patterns.html.



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

In the Change Index Pattern drop-down, 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** drop-down 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.