Siren
Powering investigations

EASY START GUIDE
ANALYST

Version 15.2

Table of contents

About this tutorial

This tutorial helps you perform analyst tasks using Siren Investigate version 15.2, which is a part of the Siren platform. The two elements of Siren Platform are:

Siren Investigate, a web application that provides active dashboards and the easy-to-use Siren Search that can act as a starting point for the exploration of data. It includes powerful graphical, analytical, and reporting capabilities.

Siren Federate, a plugin installed in an Elasticsearch cluster that forms the Siren Platform backend system.

For demonstration purposes, this tutorial uses static demo data about companies, investments, and investors. Static data, which does not change or changes only a few times a day, is commonly used in Business Intelligence (BI) or broader knowledge discovery scenarios. You can follow along using your own data or use the demo data.

Objectives and outcomes

In this tutorial you will learn how to search in Siren Investigate, filter dashboards, send results to a graph, analyze relations and connections in the Graph Browser and export your findings.

Important data concepts

The following concepts are important to understand how data is connected:

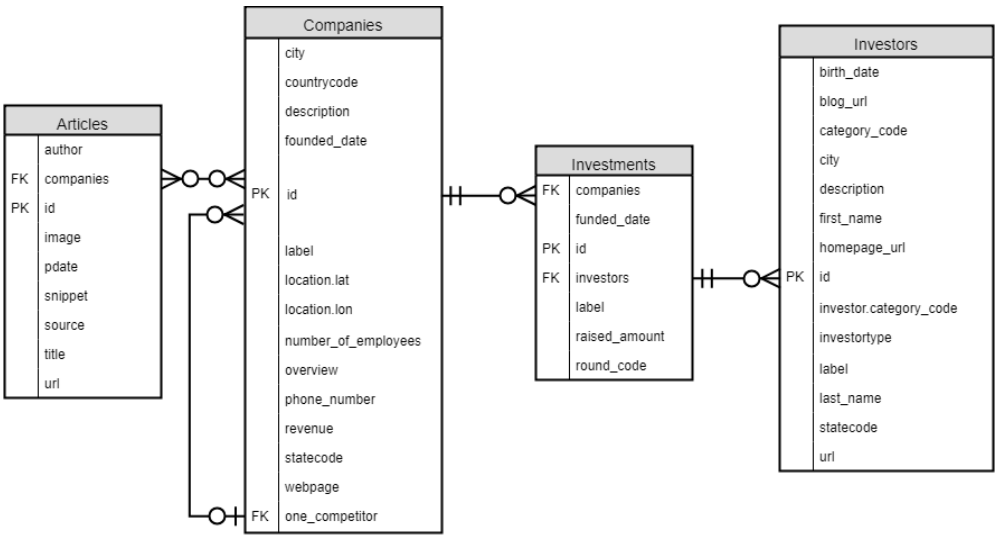
Entity tables
An entity table is a table that contains data about a specific type of entity. An entity table represents the link between Siren Investigate and one or more Elasticsearch indices that you intend to explore. For example, a Companies entity table might contain thousands of records about companies (the entity) and their attributes, such as their location, a description, the date they were founded.

Relations
A relation is the connection between fields of one entity table and another.

Data model
The data model is at the core of Siren Platform's ability to investigate connected data by performing link analysis or associative dashboard navigation. It acts like a blueprint that maps out:

- The entity tables, the data and fields that they contain, and how they map to conceptual *entities*.
- The subsets of entity tables, known as searches.
- The relations between entities.

In the companies demo data the main files are relationally connected. The following entity-relationship diagram shows the connections between the tables. There are also other relationships in the data, for example, city and state names, URLs, and email addresses.



Launching Siren Platform

(Average completion time: 10 mins)

Before you begin, make sure you have the following:

- Siren Investigate installed on your machine.
- User login credentials.
- Google Chrome or Mozilla Firefox.
- A Siren Platform license key.
- Data uploaded to Siren Platform, either Siren demo data or your company data.

Launching on Windows

1. Navigate to the Siren Platform installation.
2. Double-click **start.bat** and wait for both Elasticsearch and Siren Investigate to load.
3. Open a Web browser and go to **http://localhost:5606**.

NOTE Do not close either the Elasticsearch or Siren Investigate command windows until you are finished working with Siren Investigate.

IMPORTANT The first time you run the installation, the Investigate window may appear to be stuck. This is the optimization phase. It continues writing log messages after a few minutes.

Launching on a Mac or Linux machine

1. Go to the location of the Siren Platform installation location and open the **elasticsearch** folder.
2. Open a **Terminal** window at the **bin** folder. For example, right-click the **siren-platform** folder and select **New Terminal at folder**.
3. Execute the following command: `./investigate`
4. When the log prints `[console] Template [template:kibi-html-angular] successfully loaded`, open a Web browser and go to **http://localhost:5606**.

NOTE Do not close either the Elasticsearch or Siren Investigate command windows until you are finished working with Siren Investigate.

Applying your license

- In the app menu, click **Management** → **License**.

Welcome to Siren Investigate

Siren Investigate opens to Siren Search by default. When data is uploaded to Siren Investigate you can immediately search a search term.

NOTE To navigate to Siren Search from anywhere in Siren Investigate, in the app menu, click **Search**. You can also use Siren Search directly from the graph.

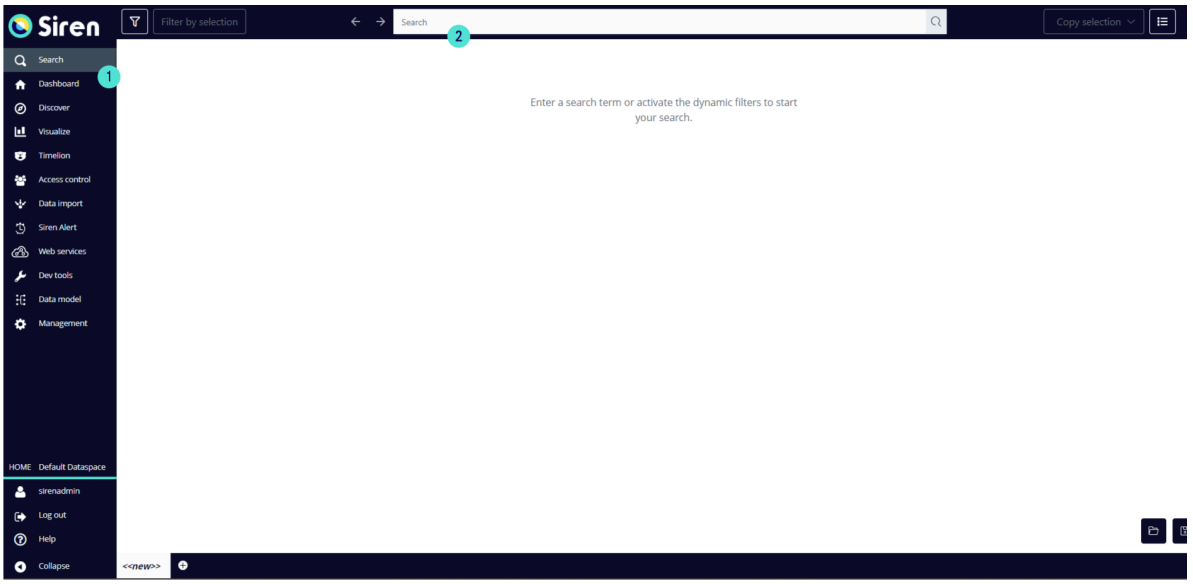


Figure 1: Siren Search

Callout	Description
1	App menu
2	Search bar

Performing a Siren Search

(Average completion time: 10 mins)

In this exercise you perform a search with Siren Search and send the results to a graph. With Siren Search you can search for specific text, date ranges, and field values.

1. In the search bar enter a search term, for this exercise search the company **LinkedIn**. The results appear in a table.
2. Select the company record for LinkedIn.
3. In the upper-right corner, click **Action** > **Copy selection** > **My Records**. Note that records in **My Records** disappear when you log out.

TIP To view more information about a search result, click the record viewer button.

Using dynamic filters

You can use dynamic filters in Siren Search to narrow the results. They connect to multiple entities and dynamically show filter options based on the results of the search. Dynamic filters are created by your system implementer. For more information, refer to the Dynamic filters documentation.
Use the dynamic filters to search for early investments in LinkedIn.

1. Optional: If the dynamic filters panel is not already open, in the upper-left corner of Siren Search, click the filter button.
2. In **Entity tables**, unselect **All tables** and select **Investments**.
3. Click **Apply filters** to see the available dynamic filters.
4. In the **Time** dynamic filter, change the end date to **Dec 31, 2010**.
5. Click **Apply filters**.

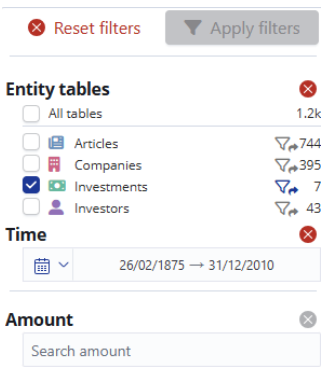


Figure 2: Search term LinkedIn dynamically filtered to show investments before 2011

Sending records to a graph

Spend some time looking at the results. If you look at the **Related data** section, you can see that two of the investments were secured by other companies and are not relevant. You could choose not to send these records to a graph but for the purpose of the exercise include them so that you can see them visualized on the graph.

To send the results to a graph, do the following:

1. From the Siren Search results, select all seven investments.
2. In the upper-right corner, click **Action** > **Copy selection** > **My Records**. Note that you previously sent the LinkedIn company record to **My Records.**
3. In the bottom-right corner, click the Bookmark Search button to save your search.
4. In the Graph list panel, click **Create graph**.
5. Enter a name for your graph and click **Create**.
6. Next to **My Records**, click the copy button and select the graph you created.
7. In the graph list, next to your graph, click the **Open in dashboard** button to open the graph.

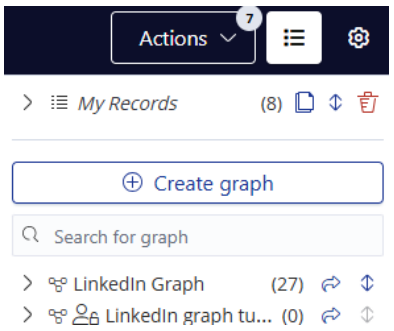


Figure 3: Graph list with My Records (8) and newly created LinkedIn graph

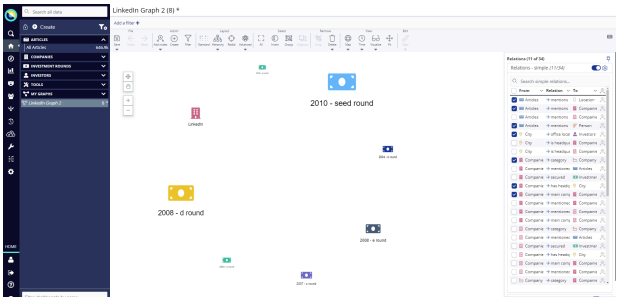


Figure 4: Graph browser with our current investigation

Graph Browser

(Average completion time: 60 mins)

The Graph Browser is the most complex visualization in Siren Investigate. It visualizes graphs, displaying records as nodes with the defined relation between records as links between the nodes.

For example, the following figures show a graph visualizing the LinkedIn investigation at a more advanced stage.

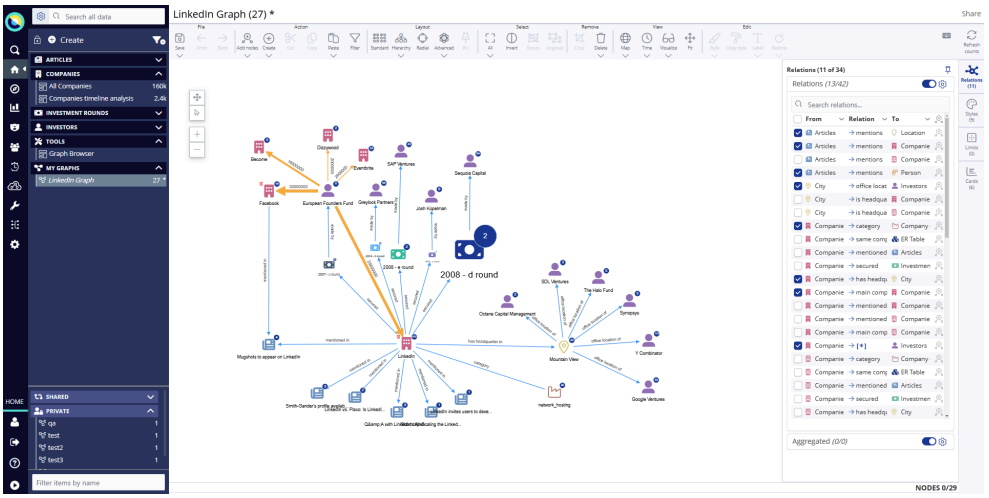


Figure 4: Graph Browser with an advanced investigation

NOTE In the last exercise, you opened your graph from Siren Search. If you need to navigate back to your graph, from the menu, click **Dashboard** and from the sidebar, select your graph.

At this point you have one node representing LinkedIn and seven nodes representing different investments. You can add more nodes to a graph from dashboards or while you are working on the graph, you can add nodes related to a node on the graph. During this exercise, you add nodes to your graph by using these different methods.

Open your saved graph in the Graph Browser visualization:

1. In the Dashboard sidebar, expand **TOOLS** and select **Graph Browser**.
2. On the Graph Browser toolbar, click **Open** and select your graph.
3. Click **Add nodes to current graph** and click **Add nodes.**

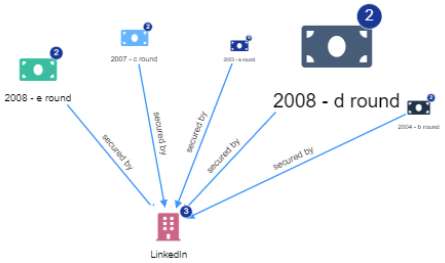
Showing relations between nodes

At this stage you have one node representing LinkedIn and seven nodes representing different investments. However, the relations connecting the nodes are not visible. Turn on the relations for the investments:

1. From the right-most sidebar, click **Relations**.
2. Select the **Investments secured by Companies** checkbox.

You can now see the five investments secured by LinkedIn and the two irrelevant investments visualized separately. If you hadn't noticed these investments in Siren Search, it would be clear on the graph.

Delete the irrelevant investments: select the nodes and, on the toolbar, click **Delete.**

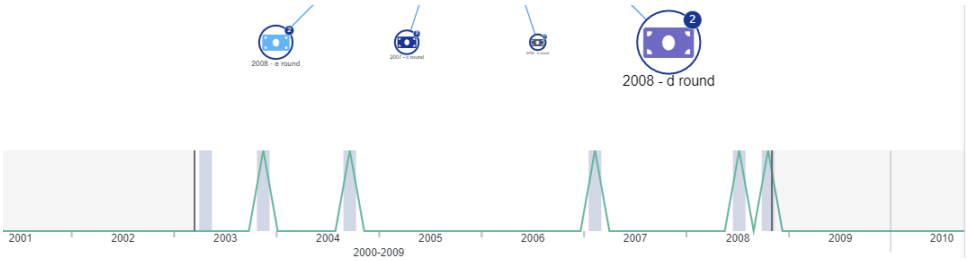


Showing the timeline of nodes

Question: When was the first investment made in LinkedIn?

To discover when investments were made, use the time feature as follows:

1. Right-click on the graph → **Select** → **By Entity Type**.
2. Select **Investments** and click **OK** to select all investment nodes.
3. On the toolbar, click **Time** to open a timeline of the investments.



Answer: The first investment was in 2003.

Working with dashboards

(Average completion time: 15 mins)

Siren Search is just one way to investigate data. You can also use dashboards to filter data and send results to a graph. Dashboards are custom created with different visualizations and can be linked together by their connected data. In this exercise, you filter dashboards to investigate the investors in LinkedIn.

Filtering and navigating dashboards

1. Go to the dashboard sidebar and click the **All Companies** dashboard.
2. In **Search in dashboard**, enter **LinkedIn**. This filters the dashboard to companies that reference LinkedIn.
3. In the **Companies Table** visualization, select the checkbox next to the LinkedIn record and from the right, click **Create Filter** to filter to the LinkedIn company record only.
4. In the **Relational Navigator** visualization, click **secured (All investments).** This brings you to the All Investments dashboard and applies a filter of LinkedIn investments on that dashboard.
5. In the **Relation Navigator** visualization, click **made by (5 All Investors)** to navigate to the **All Investors** dashboard filtered to show investors in LinkedIn only.

Question: What percentage of the investors are organizations?

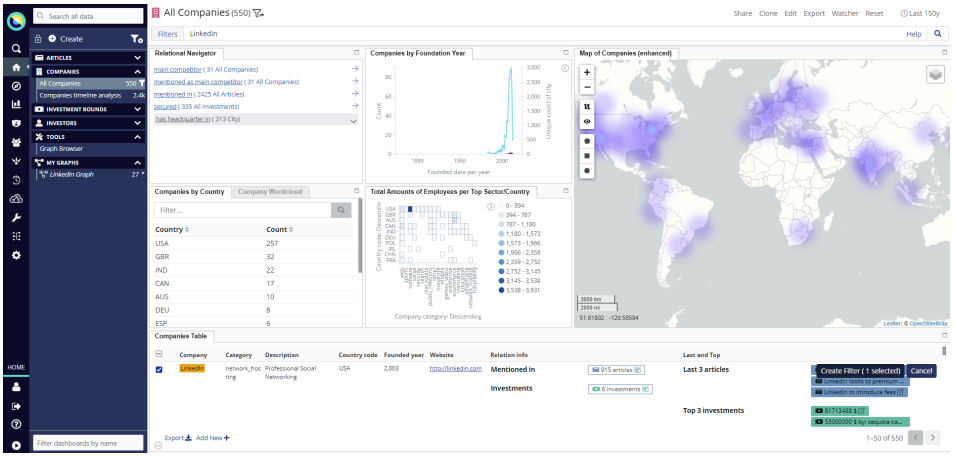


Figure 7: All Companies dashboard

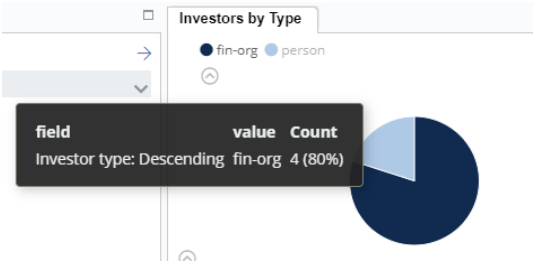


Figure 8: Investors by Type

Answer: You can use the **Investors by Type** visualization to see that 80% of the investors are organizations and 20% are individual people.

Adding nodes from a dashboard to a graph

Add the LinkedIn investors to a new graph and investigate the investments.

1. In the Dashboard sidebar, click **Create** → **Graph**, and name the graph **Investors**.
2. In the Dashboard sidebar, drag the filtered **All Investors** dashboard to the **Investors** graph and click **Add**.
3. Select the **Investors** graph to open it.

Investigating on the graph

(Average completion time: 40 mins)

On the graph investigate one of the investors to discover the other companies it invested in and the locations of those companies.

Add the nodes by their relations as follows:

1. Select the **European Founders Fund** node.
2. On the toolbar, click **Add nodes** → **Expand by relation**.
3. Select **made Investments** and click **Add**.
4. Select all the investments: right-click, click **Select** → **Select By Entity Type** → **Investments** → **OK**.
5. Right-click on an investment and select **Expand by relation.**
6. Select **secured by companies** and click **Add**.

Investigating locations

To view data, including locations, about the companies in the selection table:

1. Click **Map** to close map view.
2. Select all of the company nodes.
3. At the bottom of the graph, click the **Companies** tab to open the selection table.

You can see location data in the **County code** column, alternatively you can see these locations on a map. To view the locations of the companies on a map, from the toolbar, click **Map**.

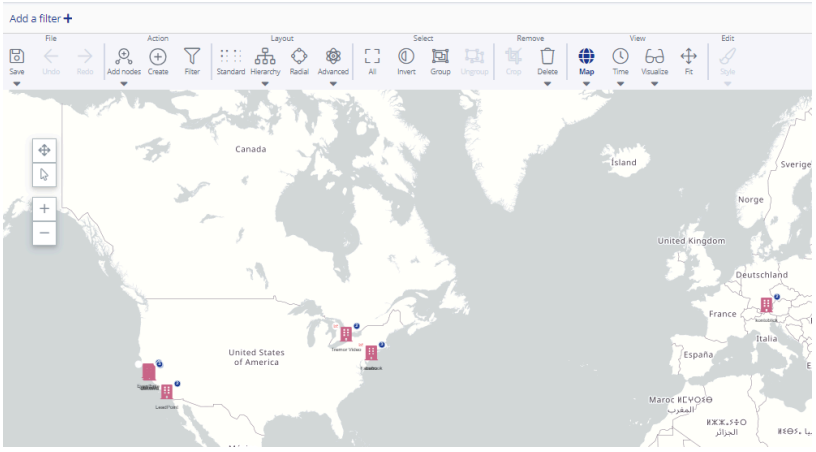


Figure 7: Companies located on the map

Adding nodes from one graph to another

You can now add the nodes from the Investors graph to your LinkedIn graph and show the relation to LinkedIn as follows:

1. In the Dashboard sidebar, drag the **Investors** graph to the **LinkedIn** graph.
2. Open the LinkedIn graph.
3. Select all the investment nodes.
4. From the right-most sidebar, click **Relations** and select **Investors made Investment** to show the relation on the graph.
5. Select all the company nodes, and from **Relations**, select **Companies secured Investment.**

Organizing your layout

At this point the graph has many nodes and relations. Change the layout of the nodes, adjust the styles, and add annotations. Use styles to control how the nodes and relations appear on the graph. Styles can be custom created by your system implementer.

Using styles to streamline the layout

You can select a layout and use styles to organize the graph as follows:

1. In the right-most sidebar, click **Styles**.
2. Select the **Investment to edge** checkbox.
3. Tidy the layout. On the toolbar, click **Select - All** and from **Layout** select **Standard.**
4. On the toolbar, click **Save.**

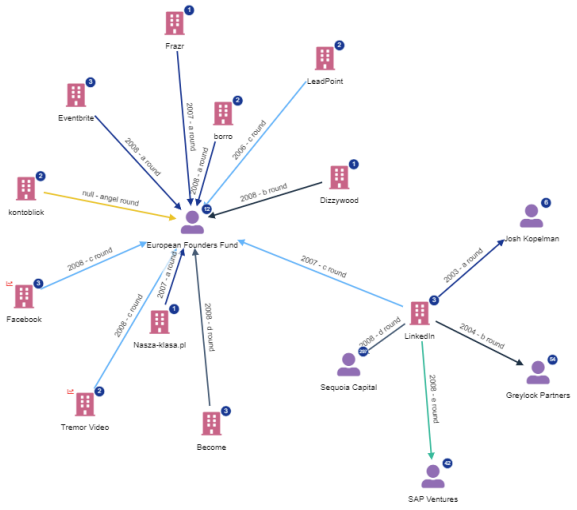


Figure 8: Organized layout

Changing the appearance of individual nodes

You can customize the appearance of individual nodes and edges, modify labels, and show more information next to nodes.

In this exercise change the size and color of the LinkedIn node and the edge that shows the relation to the European Founders Fund. Add field records to European Founders Fund, change its label, and add a text box to annotate the graph.

Modify the appearance of LinkedIn as follows:

1. Select the LinkedIn node.
2. From the toolbar **Edit** section, click **Style** → **Color**, and select a color.
3. Click **Style** → **Size**, and increase the size.
4. Select the edge between the LinkedIn and European Founder Fund nodes.
5. From the toolbar **Edit** section, click **Style** → **Color**, and select a color.
6. Click **Style** → **Width** and increase the size.
7. Optional: Copy the style changes to the **European Founders Fund** node- select the LinkedIn node, click **Copy style**, and then click the European Founder Fund node.

Change the European Founders Fund label to EFF and show field record information on the node as follows:

1. Select the European Founders Fund node.
2. From the toolbar **Edit** section, click **Label** and change the name to EFF.
3. At the bottom of the screen, click the **Investors** tab.
4. In the selection table, next to DEU, click the **Add bullet point** button to add this information to the node.

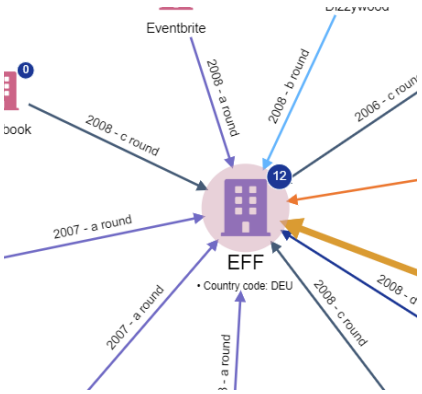


Figure 9: Modified nodes

To add a text box:

1. From the toolbar, click **Create** → **Text box**.
2. Drag the text box to where you would like it to be.
3. From the toolbar **Edit** section, click **Label** and add information to the text box.

Finding the shortest path between nodes

You can use the shortest path script to find the shortest connection between two nodes. You can select the path length and maximum retrieved records. In the Relations menu, you can select what relations you want to find the shortest path with.

Maximum path length controls how many steps along a potential path the calculation can travel. The algorithm identifies increasingly longer paths connecting the selected nodes, up to the specified maximum path length.

Maximum retrieved records per join limits the number of records that are returned by each backend query that extracts entities connecting the selected nodes. This roughly translates to the count of selected nodes returned for each entity table or entity identifier that is encountered while detecting paths.

To calculate the shortest path between two nodes:

1. Select two company nodes.
2. Right-click and select **Shortest Path**.
3. From the **Choose Parameters** window, enter the path length, maximum retrieved records, and join type.
4. Click **OK**.

NOTE If you cannot find the shortest path, you might need to select the relations you want to find the path with. From the right-most sidebar, click **Relations** and select the relation checkboxes.

Sharing and reporting

(Average completion time: 15 mins)

There are different features to help you share your investigation findings, create PNG images of the graph, and generate reports.

Sharing Siren Search results

In an earlier exercise you bookmarked your search. To share bookmarked searches, do the following:

1. From the menu, Select **Search**.
2. In the bottom-right, click the **Open Search** button and select your bookmarked search.
3. In the bottom-right corner, click the **Share Search** button to copy a URL to your clipboard.
4. Paste the URL into an email or messaging system to share it with others.

NOTE

- If the search is private, only the search owner, admins, and dataspace owners can access it.
- You must save any updates to the bookmarked search before you generate the URL.

Exporting an image of the graph

1. Open the graph you want to export and an image.
2. On the toolbar, click **Save** → **To image**.

The graph is downloaded as a PNG.

Optional: Generating a report

If your implementer has integrated the reporting tool through Siren AI, you can quickly generate a report of your graph as follows:

1. Right-click on the graph.
2. Select **Generate a report**.

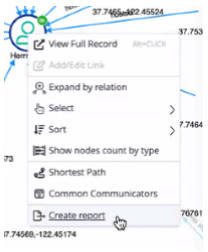


Figure 10: Create report

Creating a new dataspace

(Average completion time: 5 mins)

You can create new dataspaces to work in. This is helpful if you want to start a new investigation separate to others. You can create a new empty dataspace but in this exercise, clone the existing dataspace.

1. In the bottom-right corner of the menu, click the current dataspace to see a list of existing dataspaces.
2. Click **Create** dataspace.
3. In **Title**, enter a name for the dataspace.
4. In **Short code**, enter a shortened name for the dataspace.
5. In **Clone from**, select the current dataspace.
6. Optional: Select the users to give access to and select their access level.
7. Optional: Change the icon, color, and enter a description.

You can now continue investigating the data separately to your previous investigation.

Additional resources:

Easy Start Guide for Implementers
Siren website www.siren.io
Documentation www.docs.siren.io
Siren training platform www.training.siren.io

Legal notices