1touch.io
Data Aware Security

HOW TO CONNECT TO SALESFORCE

VERSION 4.1.1

October 2024

TABLE OF CONTENTS

SALESFORCE OVERVIEW

The purpose of this document is to explain how to configure Inventa to use the Salesforce CRM application as a source of RDA in two steps:

1. Connect the 1touch.io application to your Salesforce account.

2. Configure the data-at-rest analysis in the Console Manager UI.

3. Configure the root data asset (RDA) analysis in the Root Data Asset Manager.

Inventa is designed for operation with the latest version of Google Chrome. Using other browsers is not recommended and may affect performance and functionality

STEP 1: CONNECTING THE 1TOUCH.IO APPLICATION

To use Salesforce objects as a data source for the Inventa root data asset, you need to connect the 1touch.io application to your Salesforce account by:

- Generating the private key
- Creating the connected app entry
- Approving the created app

HOW TO CREATE A PRIVATE KEY

In the console, generate a private key and X509 certificate and save the private key using the command below. It will be later used as part of credentials for connection to RDA.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout ~/<my_folder>/salesforce_private_
key.pem -out ~/<my_folder>/salesforce_certificate.pem
```

my_folder - a path to a folder you have created for the private key and certificate.

Once you enter the command, you will be asked to fill in a couple of parameters (for example, country code, state, email, etc.) that will be incorporated into the certificate request and could be used to distinguish between the different certificates you have generated.

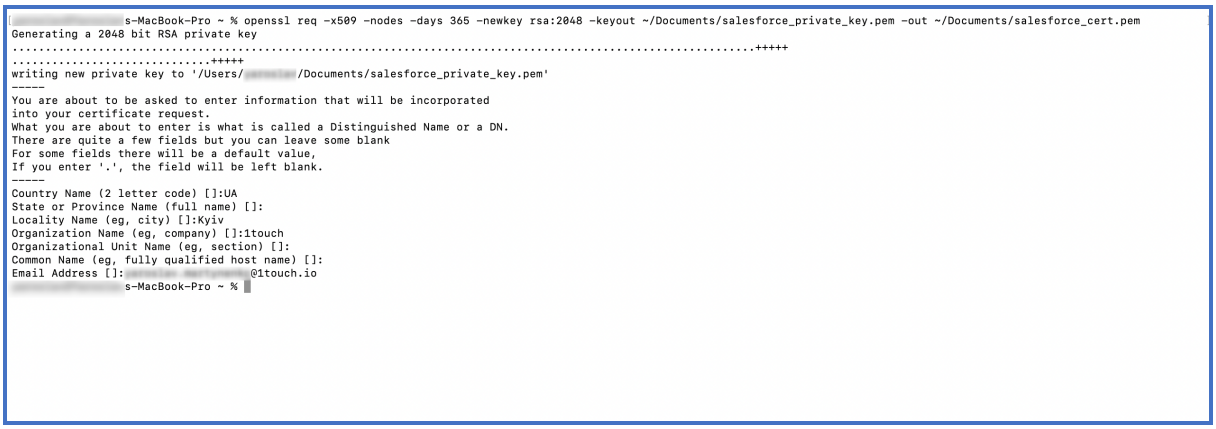


Figure 1: Command prompt

You will need to fill in at least one of the fields in order to successfully execute the command. However, the more fields you fill in the better for distinguishing.

HOW TO CREATE AN APP ENTRY

1. Login to your Salesforce customer account. In the upper right corner, click **Settings wheel** (**1**) > **Setup** (**2**).

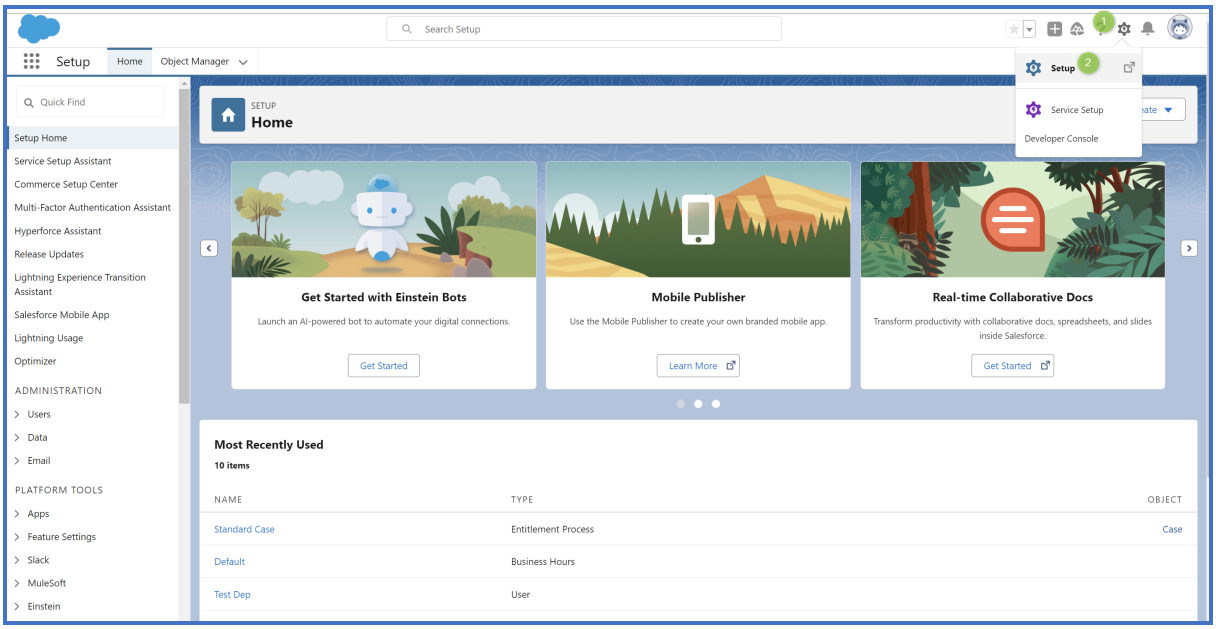


Figure 2: Selecting Setup in the Salesforce customer account

2. In the Sidebar, use the **Quick Find** box (**1**) to find and select the **App Manager** (**2**). Then click the **New Connected App** button (**3**) on the **App Manager** page. You will be redirected to the **New Connected App** page.

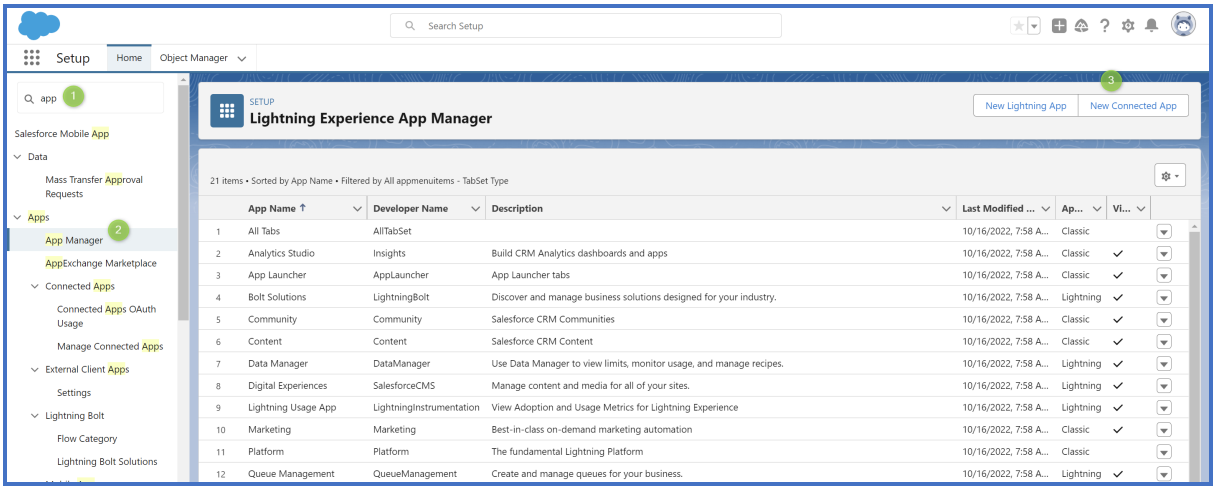


Figure 3: Adding a new connected app in the App Manager

3. In the **Basic Information** pane, fill the required fields: **Connected App Name**, **API Name**, **Contact Email**.

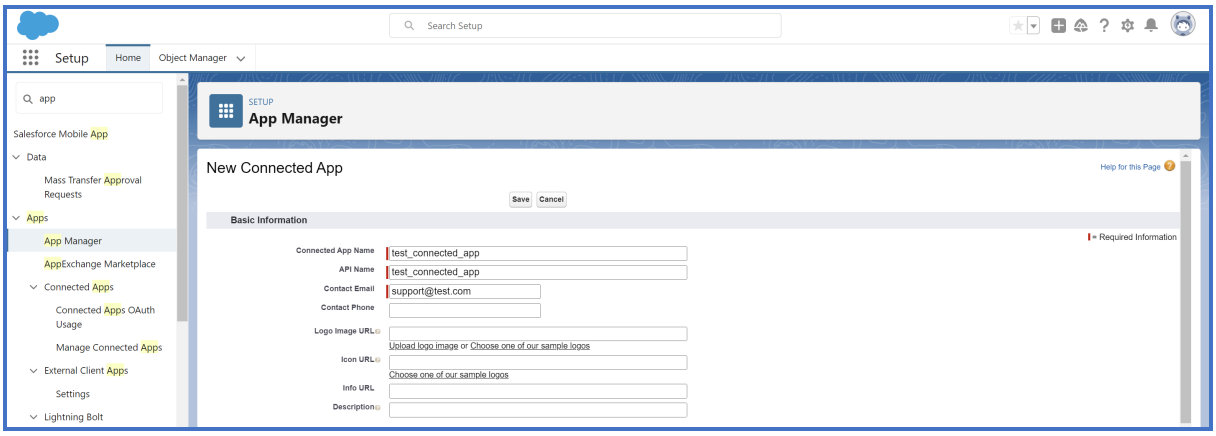


Figure 4: Basic Information pane on the New Connected App page

4. In the **API** pane, perform the following steps:

4.1. Check the **Enable OAuth Settings** (**1**) and **Enable for Device Flow** (**2**) checkboxes.

4.2. Fill in the **Callback URL** text box (**3**). For example, *https://login.salesforce.com/services/oauth2/callback*.

4.3. Check the **Use digital signatures** checkbox (**4**). Then upload the X509 certificate by clicking **Choose File**.

4.4. Grant the following permissions (**5**):

- Manage user data via APIs (**api**)
- Perform requests at any time (**refresh_token**, **offline_access**);
- Access the identity URL service (**id**, **profile**, **email**, **address**, **phone**);
- Allow access to Lightning applications (**lightning**).

Exact permission names may differ depending on the Salesforce version, it may be easier to find the needed permissions by the parenthesis parameters .

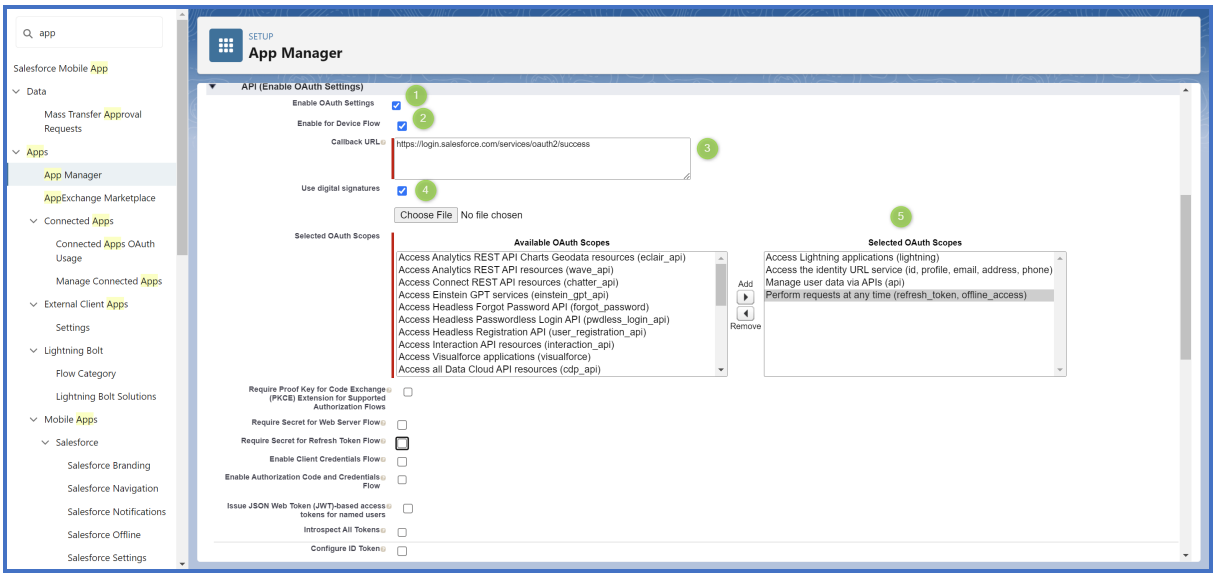


Figure 5: API pane on the New Connected App page

5. Scroll down to the bottom of the page and click **Save**.

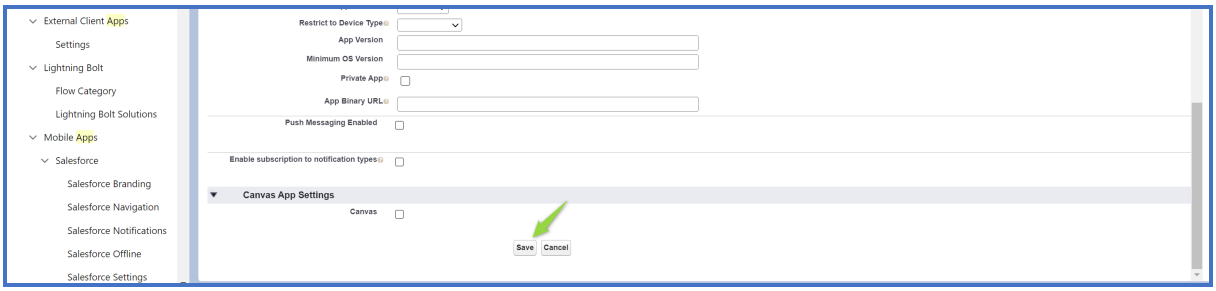
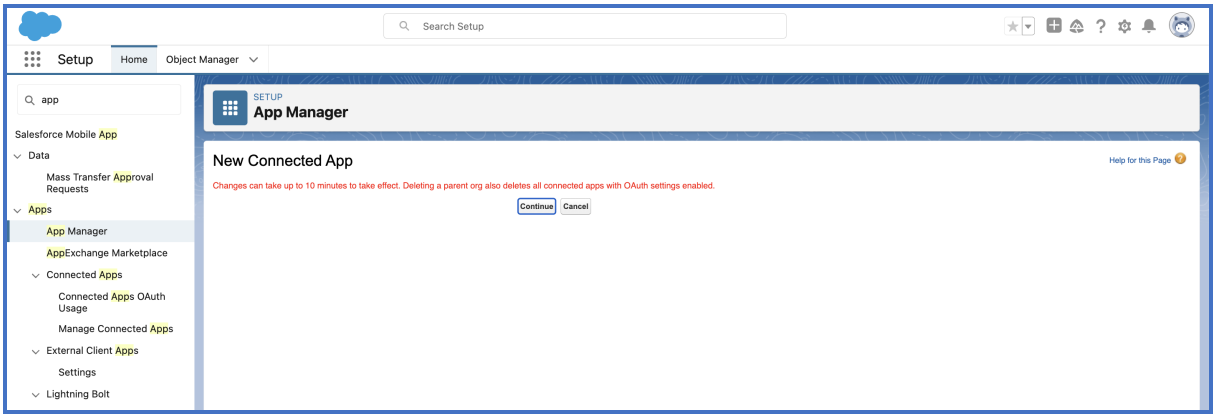


Figure 6: Saving the new connected app

6. If you see the warning message, just click the **Continue** button.



7. Once you click **Save**, continue to the new app page, click the **Manage Consumer Details** button, and copy the consumer key. It will be later used as part of credentials (Client ID) for connection to RDA.

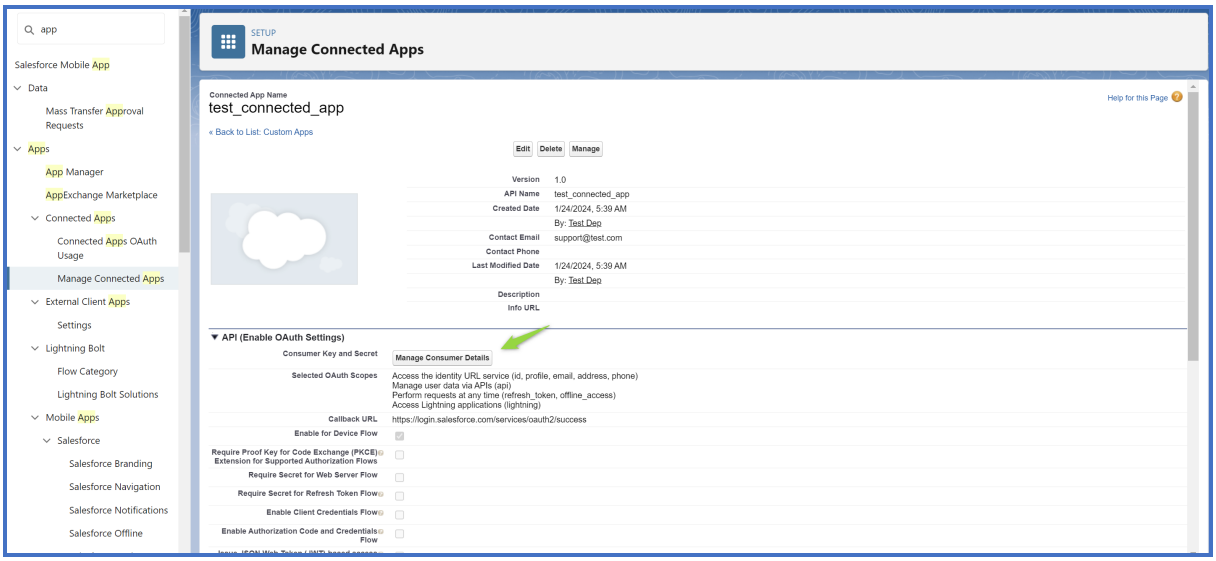


Figure 7: Client ID on the App page

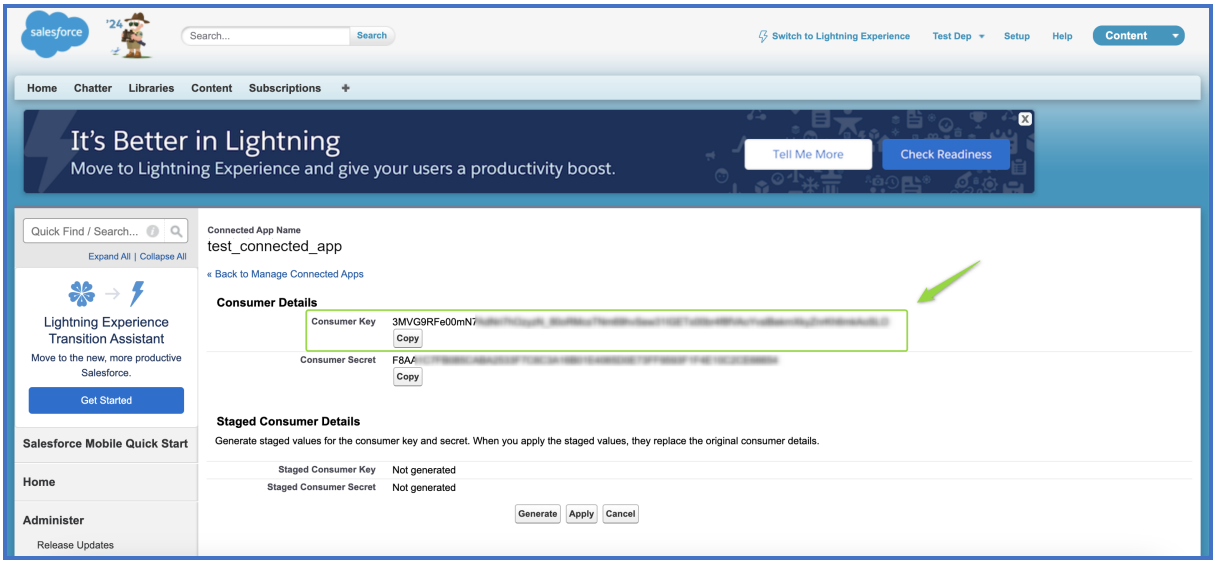
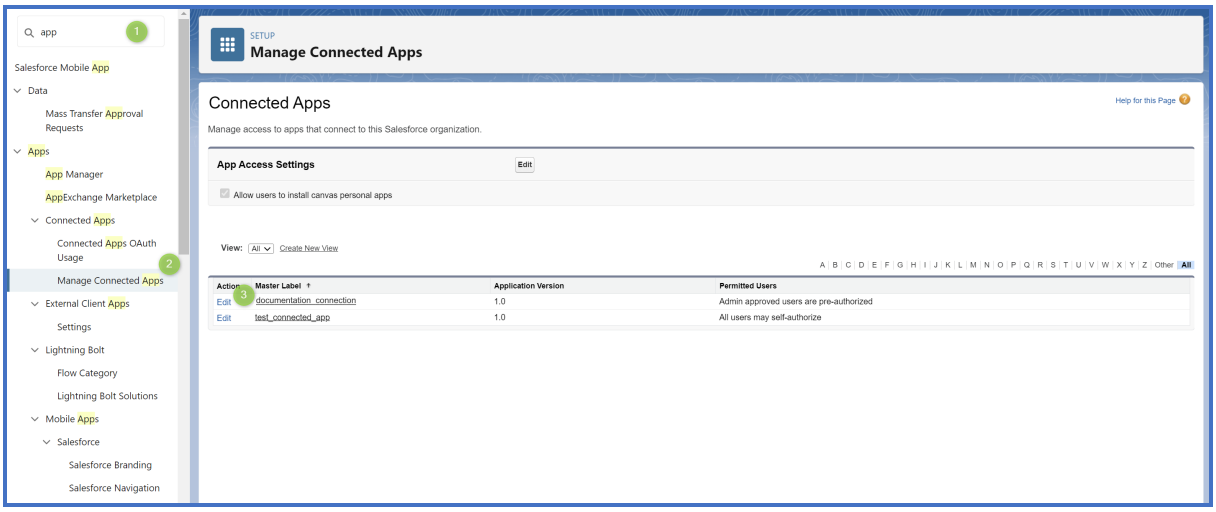


Figure 8: Consumer key

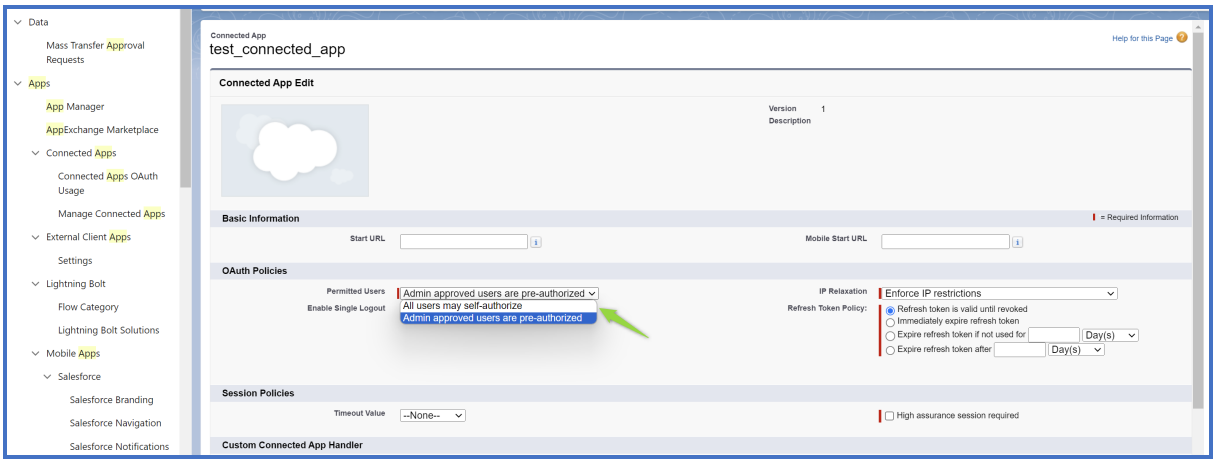
HOW TO APPROVE THE CONNECTED APP

To finish the creation of the application, the app needs to be approved. To approve the application, ensure that you have the Salesforce system administrator permissions and perform the following steps:

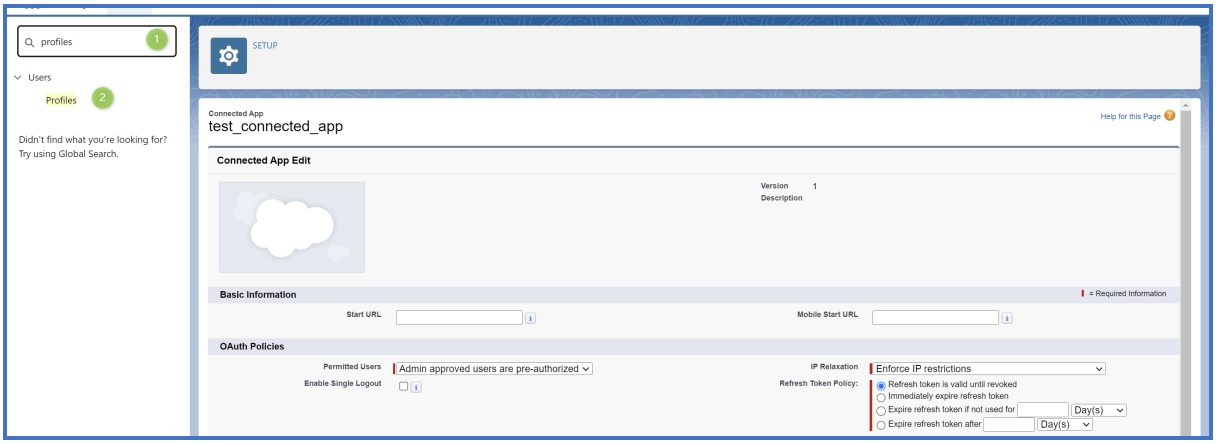
1. In the Sidebar, use the **Quick Find** box (**1**) to find and select the **Manage Connected Apps** or **Connected Apps** options (depending on the Salesforce version) (**2**). Click the **Edit** (**3**) option near the app you have created.



2. In the **OAuth Policies** section, select the **Admin approved users are pre-authorized** option in the **Permitted Users** dropdown menu.



3. In the Sidebar, use the **Quick Find** box (**1**) to find and select the **Profiles** options(**2**).



4. On the **Profiles** page, scroll down to find the **System Administrator** profile and click **Edit**.

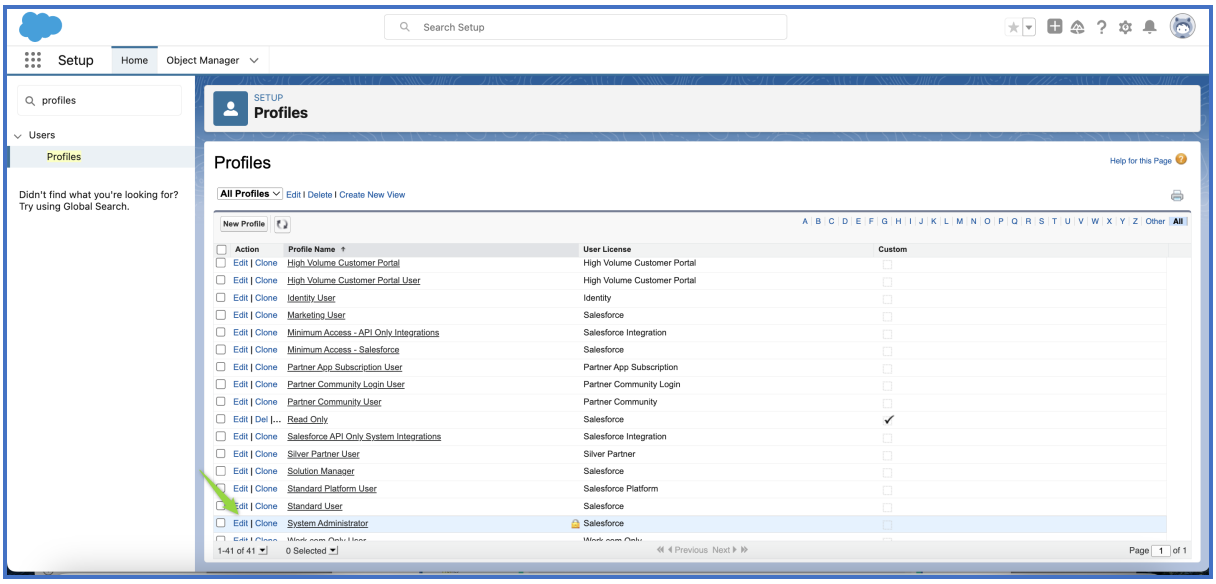


Figure 9: Edit the system administrator profile

5. Scroll down to the **Connected app access pane** and grant access to the newly created app.

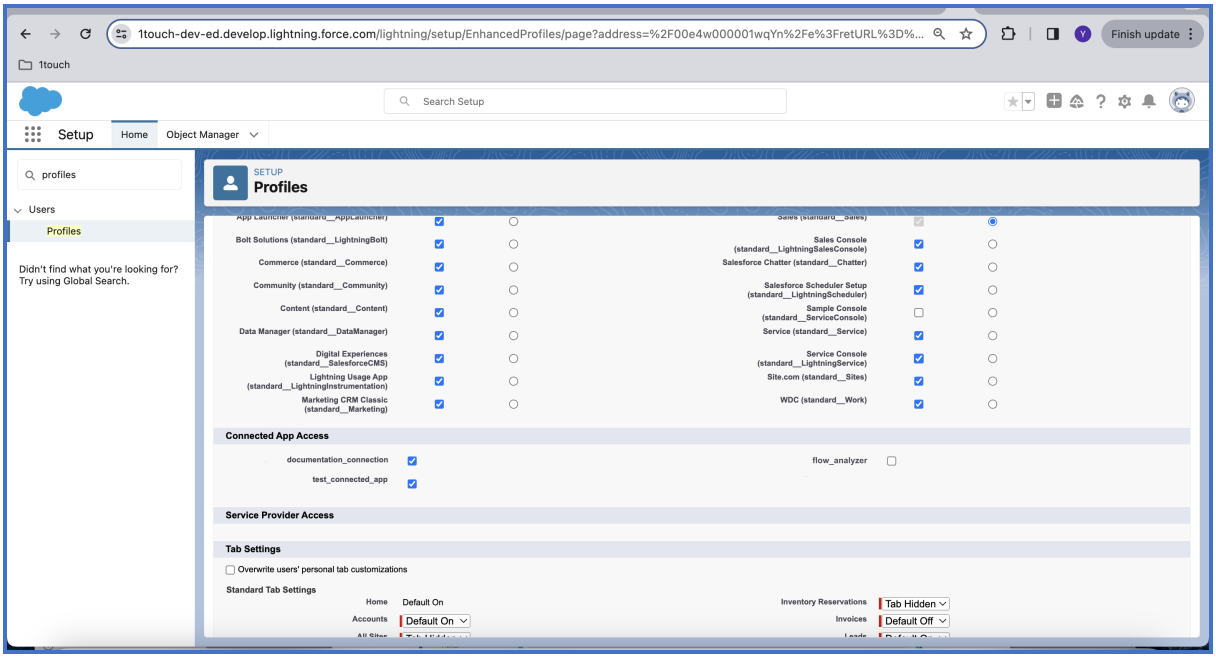


Figure 10: Granting access

STEP 2 CONFIGURING DATA AT REST

HOW TO ADD CREDENTIALS

To enable the filesystem analyzer to connect to the Salesforce account, enter the access credentials in the Console Manager UI.

1. Login into the Console Manager UI as a system administrator. In the **Sidebar**, select **Settings > Data Source Catalog > Credentials** (**1**). On the **Credentials** page, click the **Add** button (**2**).

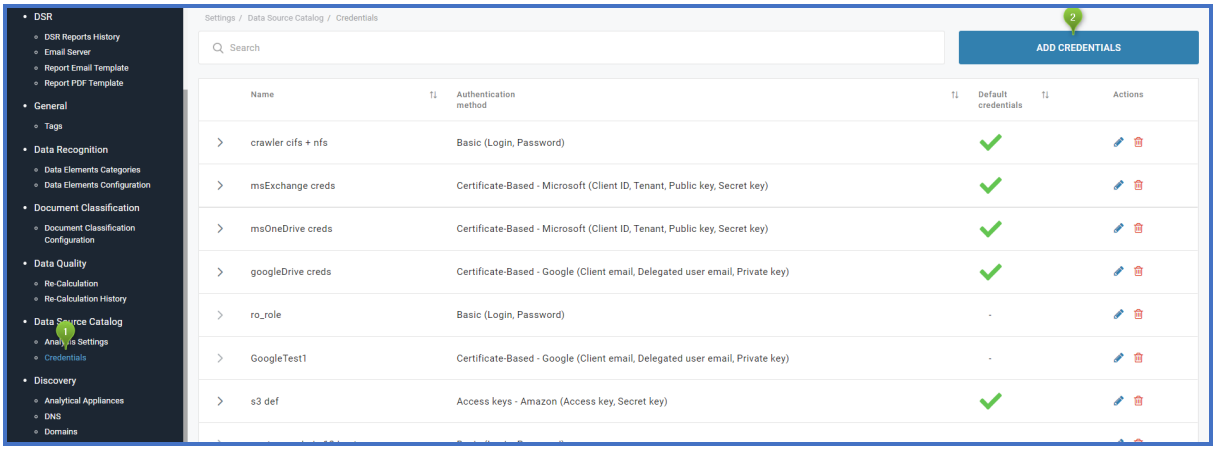


Figure 11: Selecting the Console Management Configuration page

2. In the new credentials form, enter the general information.

Table 12: General form for new credentials

PARAMETER	DESCRIPTION
Name (**1**)	Enter the credentials name to be used within the application. The name will be shown on the **Credentials** page and in the **Credentials** dropdown list while creating or editing a data source. For example, *Salesforce creds.*
Authentication method (**2**)	Select **Certificate-Based – Salesforce (Uservane, Client ID, Private key)**.

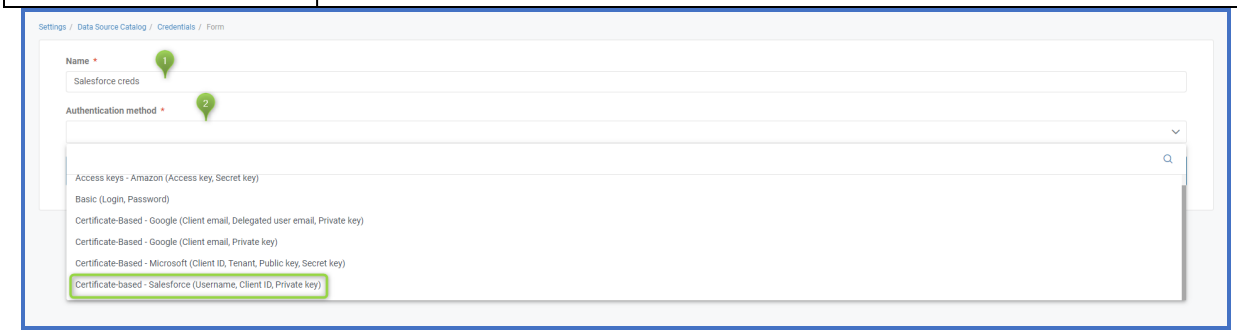


Figure 13: General form for adding a credential entry

3. Fill the credentials form according to the selected authentication method and click the **Save** button.

Inventa supports 2 types of credentials storage:

- **Internal** - credentials are stored in the Inventa application. A user enters and saves the credentials in the appropriate fields. When connecting to a data source, Inventa accesses the internal vault for credentials.
- **External** - in the Conjure CyberArk credentials vault. The user enters the IDs of the credentials from Conjur CyberArk vault appropriate fields. When connecting to a data source, Inventa accesses the Conjur CyberArk vault to get credentials using the IDs provided by the user.

You can select the desired credentials provider in the **Credentials Provider Type** field.

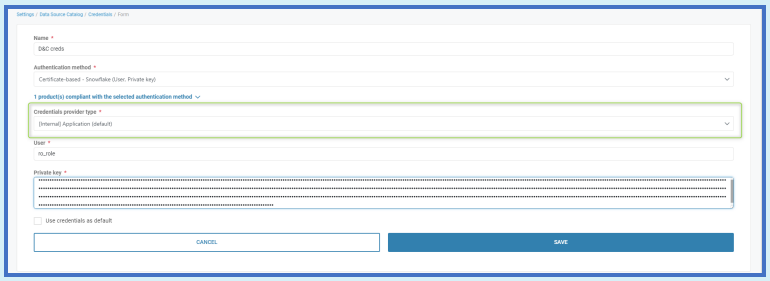


Figure 14: Selecting the credentials provider type

Inventa supports 2 types of credentials storage:

- **Internal** - credentials are stored in the Inventa application. A user enters and saves the credentials in the appropriate fields. When connecting to a data source, Inventa accesses the internal vault for credentials.
- **External** - credentials are stored in an external vault. Options: Conjure CyberArk (all authentication methods), HashiCorp (basic authentic method). When connecting to a data source, Inventa will access the external vault to get credentials using the IDs provided by the user.

  For CyberArk, the user enters the IDs of the credentials from Conjur CyberArk vault appropriate fields. For HashiCorp, the user has to fill in the path, login ID, and password ID.

You can select the desired credentials provider in the **Credentials Provider Type** field.

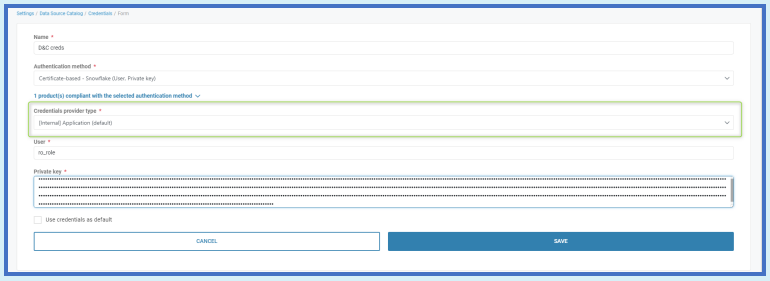


Figure 15: Selecting the credentials provider type

Table 16: One Drive Secret credentials type

PARAMETER	DESCRIPTION
Username field	Salesforce username with granted access to the 1touch.io application **Note:** the username is an email address you use to log in into your Salesforce application, not the contact email you enter during connected app creation.
Client ID field	Consumer key of the connected 1touch.io application.
Private Key field	Private key of the certificate uploaded as a digital signature in the Salesforce account. **Note:** to copy the private key, open the previously generated salesforce_private_key.pem file with a text editor and copy its contents.

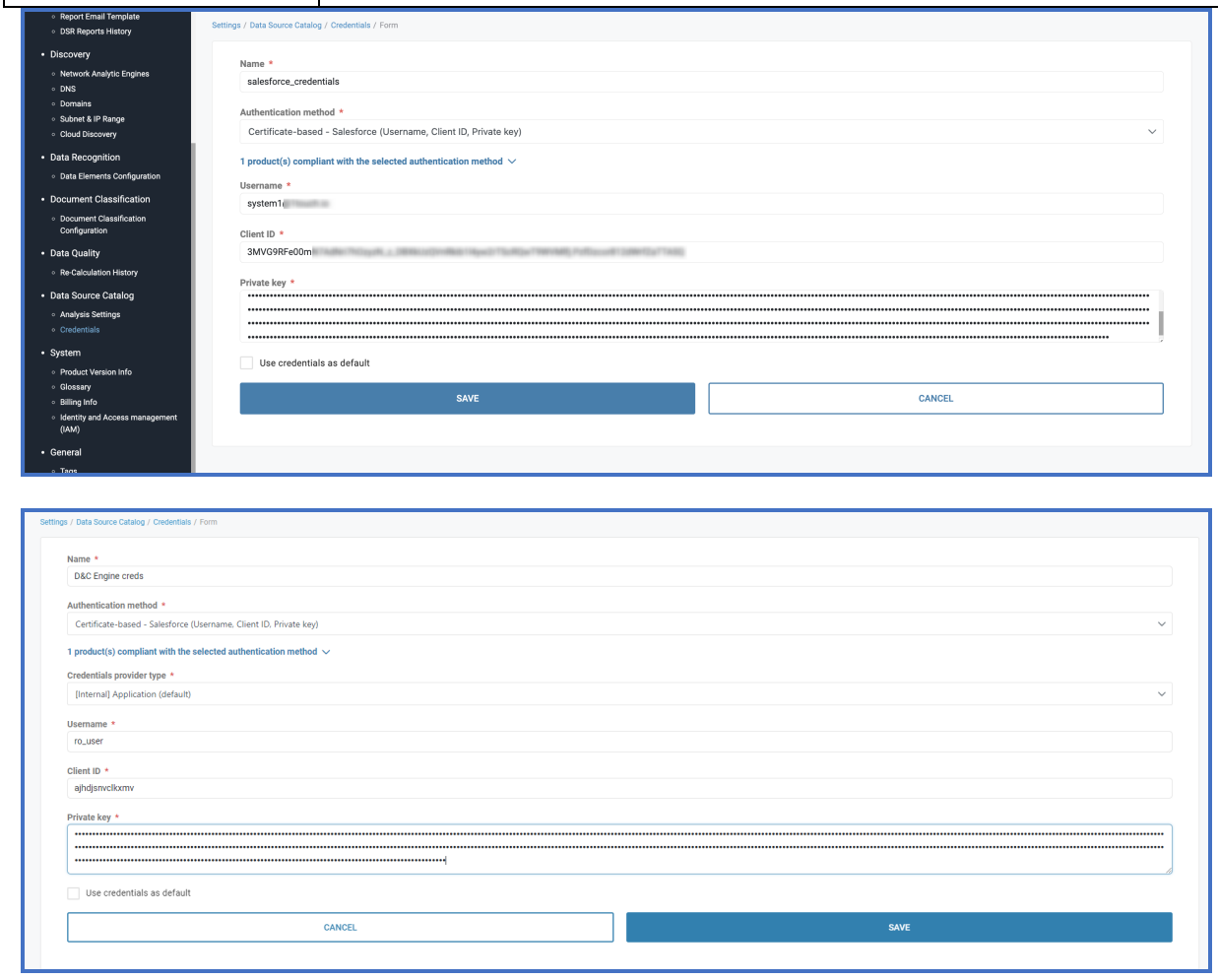


Figure 17: Salesforce credentials type

HOW TO ADD A DATA SOURCE

Data source records are used to define how to connect to your Salesforce data source and when to analyze it to discover sensitive data.

To create a data source entry, take the following steps:

1. To create a data source entry, go to **Sidebar > Inventory > Data Source Catalog**. Then click the **Add Data Source** button. You will be redirected to the **Add Data Source** page.

2. In the **Data Source Type** dropdown list (**1**), select **SaaS Application;** in the **Data Source Product** dropdown list (**2**), select **Salesforce**.

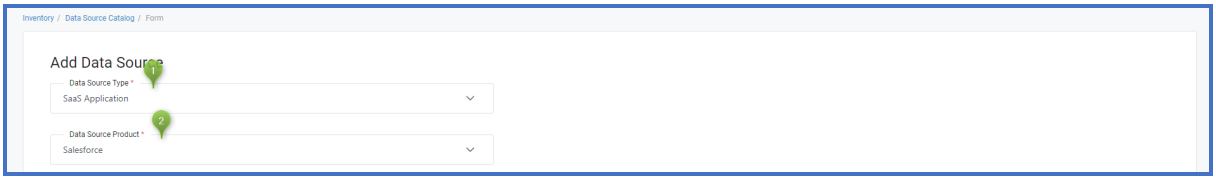
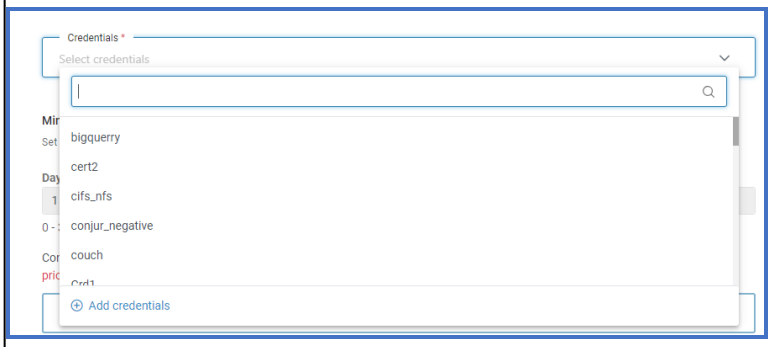


Figure 18: Data Source Type & Product

3. In the **Data Source Details** tab, enter the parameters required to connect to the Salesforce account.

Table 19: Data Source Details Parameters

PARAMETER	DESCRIPTION
Analytic engine (**1**)	Name of the analytic engine (appliance) that will analyze the data source. *(Required)*
URL (**2**)	URL for access to the Salesforce **production** environment (default settings). The URL cannot be edited, but you can switch to the sandbox environment by enabling the **Sandbox** checkbox (**3**). The system will automatically apply the sandbox URL.
Analysis strategy (**4**)	Strategy the plugin will use to analyze the data source. Supported strategies: Baseline.
Credentials (**5**)	Credentials for access to the Salesforce data source. *(Required)* You can check the **Use default credentials** box (**6**) if you defined default credentials for Salesforce account and wish the data source analyzer to use them. If the dropdown list is blank, check if the required credentials are available and correctly configured on the credentials page. **Note**: If the data source's credentials are missing, click **Add Credentials** in the **Credentials** dropdown list . The new credentials form will open in a new tab. 
Min timeout between	Set the interval of time to pass before the system can run data source analysis

PARAMETER	DESCRIPTION
analysis (**7**)	after the previous analysis cycle is completed. *(Optional)* You can check the **Use default timeout** box (**8**) if you defined a default timeout in the **Data Source Catalog > Analysis Settings** form. If there is a conflict between the global timeout on the **Analysis Settings** page and the timeout is configured in this **Data Source Details** tab, the **Data Source Details** tab parameters have priority. See the **Data Source Catalog User Guide** for more information on global data source analysis settings.

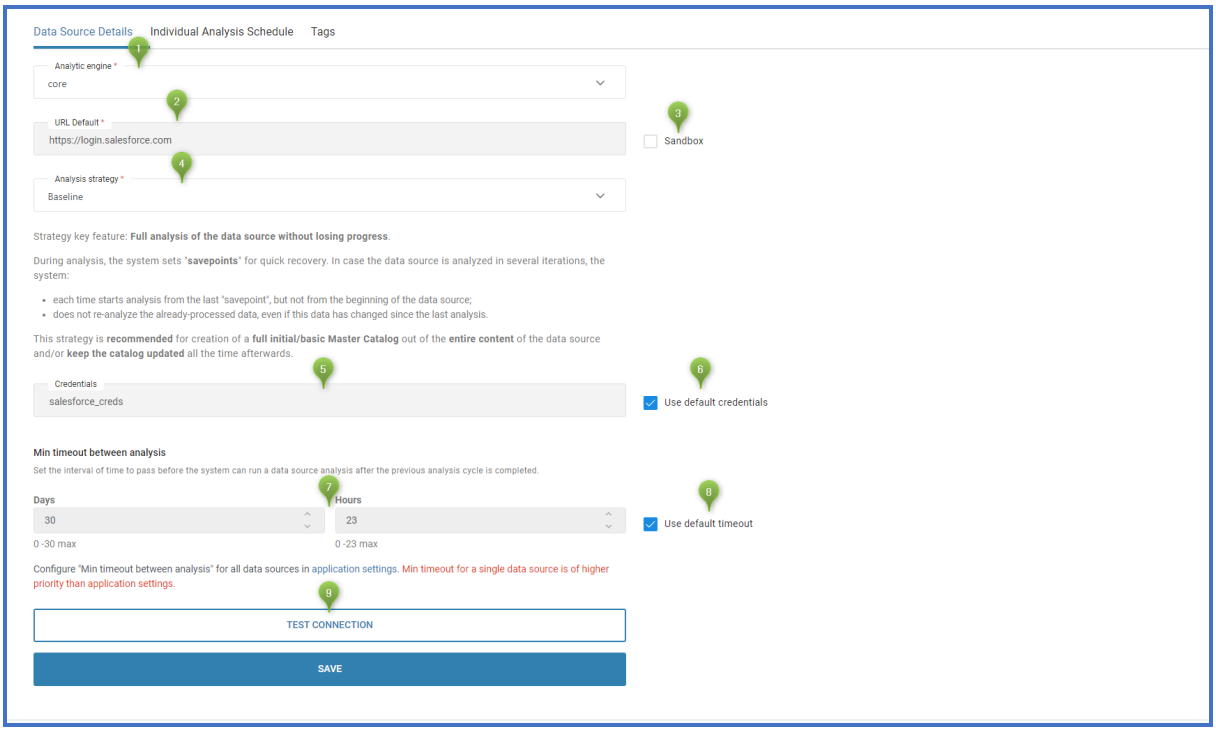


Figure 20: Data Source Details Tab

4. To test the data source connection, click **Test Connection** (**9**). This button will only be enabled once all fields required to establish connection have been filled.

5. To finish the data source record setup process, configure the analysis schedule in the **Individual Analysis Schedule** tab and assign the appropriate tags in the **Tags** tab.

6. To skip schedule confirmation and save the Salesforce data source record, click **Save.** This will add the data source to the list of data sources on the **Data Source Catalog** page with Status=New. However, Inventa will not implement analysis on this data source until you configure the analysis schedule. You can configure the schedule in the data source editing mode in the **Data Source Catalog** page.

See the **Data Source Catalog User Guide** for more information on viewing, editing, and managing data source settings and data.

ADDING TAGS TO THE DATA SOURCE ATTRIBUTES

Tags are attributes used to mark and group data source entries by type, purpose, function, etc. for later use in filtering, reporting, and connecting to 3rd party systems for monitoring, alerts, trigger initiation, etc.

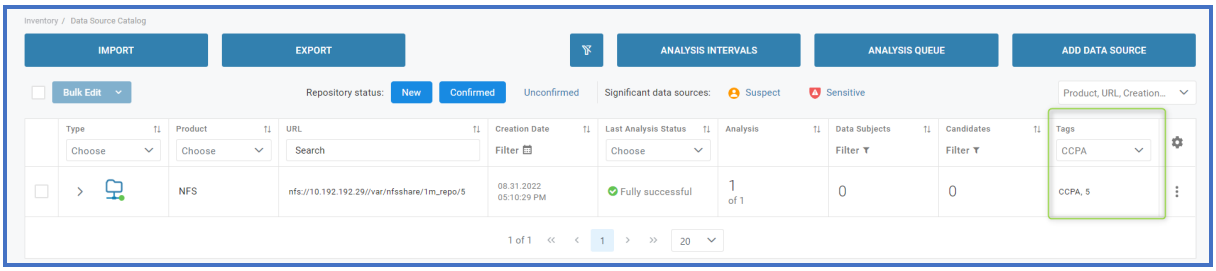


Figure 1: Data Sources with Tag in the Data Source Catalog Page

To configure tags for the data source, take the following steps:

1. In the **Add Data Source** page, click **Tags** (**1**).

2. Check the tags associated with the data source.

3. You can **Search** for a specific tag (**2**), scroll down the list of tag names (**3**). To see the tag description, click the > (**Expand**) icon.

4. New tags can be added in the **Data Source Catalog** module. You can access the tags management page by clicking on the **Data Source Settings** link (**4**).

For detailed information on using and managing tags management, see the **Analytic Engine and Console Manager Administrator Guide** and **Data Source Catalog User Guide**.

5. To save the tags you selected as attributes of the configured data source, click the **Save** button (**5**).

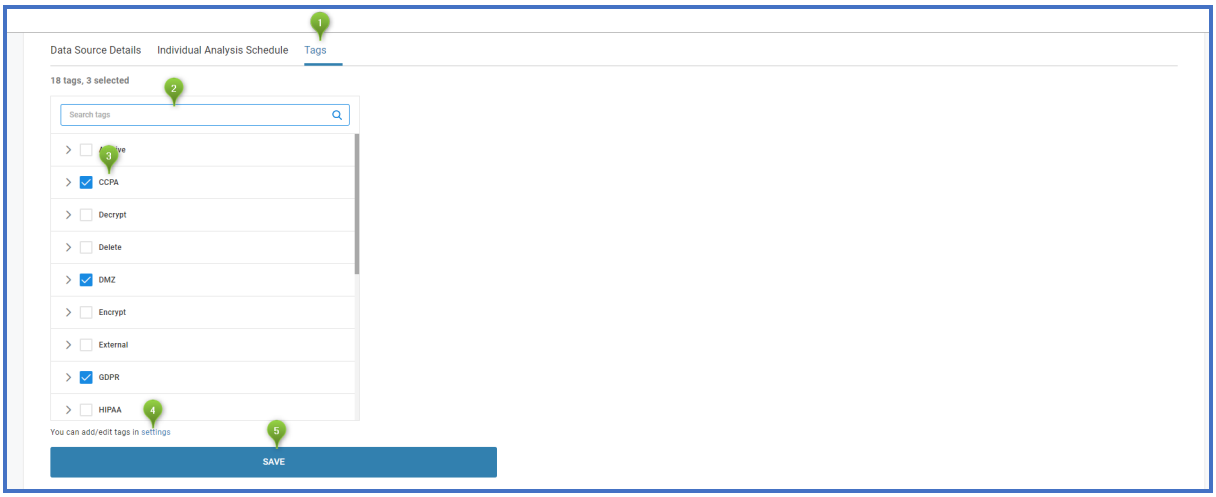


Figure 2: Tags tab

CONFIGURING DATA SOURCE ANALYSIS SCHEDULE

Analysis schedules define when to start and stop analysis of a given data source. The schedule is configured individually for each data source. Inventa will automatically enable and disable the analysis plugin at configured times.

This document explains how to configure an analysis schedule for a specific data source. To configure a default analysis schedule that can be applied to all data sources of a specific product see **Default Schedule** in the **Data Source Catalog User Guide**.

To configure the analysis timeslots for the desired data source, take the following steps:

1. In the **Add Data Source** page, click **Individual Analysis Schedule**:

Figure 1: Individual Analysis Schedule Tab

2. Click the **Add** button (**2**) to open the **Add New Event** popup window.

3. To configure continuous analysis for the current group of data sources, enable the **24/7 analysis** checkbox OR configure a weekly/daily analysis schedule by clicking **Add**.

In the **Add new event** popup window, select a timeslot for the data source group analysis. Enter the analysis event parameters as follows:

The time is configured in UTC (Universal Time Coordinated). Ensure that you take your time zone into account when setting up the schedule.

Table 2: New analysis event parameters

PARAMETER	DESCRIPTION
Event plan (**1**)	The analysis recurrence mode. Options: Weekly or Monthly. All parameters for analysis are identical in the Weekly/Monthly configuration window, except the **Repeat** parameter (**6**).
Timeslot (**2**)	The start and end times of the data source analysis schedule. The timeslot step is 15 minutes. Default: from 12:00 AM to 11:00 PM.
Days Going (**3**)	Rough duration of analysis in days. The total number of hours taking into account the days going, start, and end time is shown in the **Duration** field (**4**).

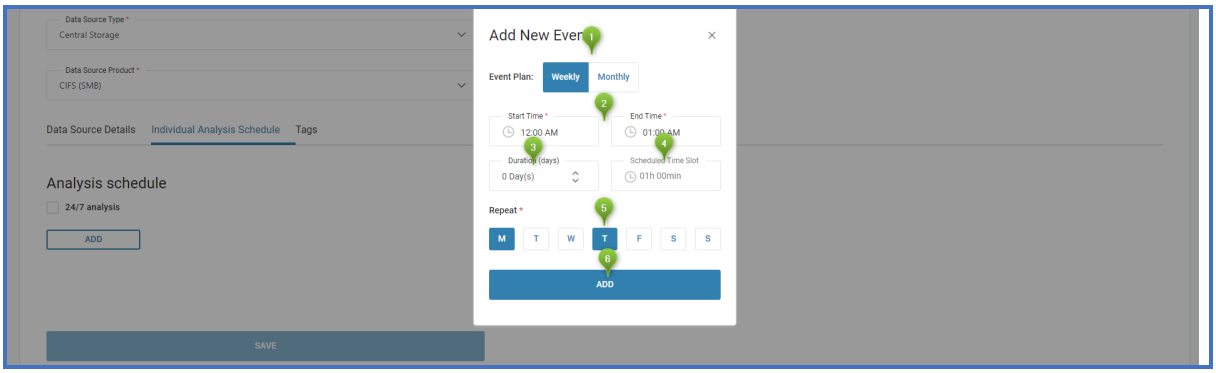
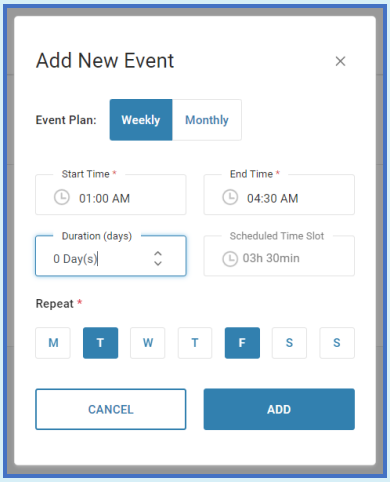


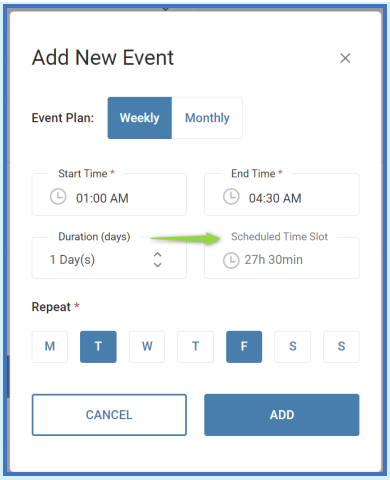
Figure 3: Add New Event popup Window

When you tweak the duration settings, keep in mind that you are not setting an actual data source analysis duration but rather the time slots when the system is allowed to conduct analysis of this data source. For example:

- You set the Start Time at 1:00 AM and End Time at 4:30 AM on Tuesday and Friday. If there are no other data sources to analyze during that time, the system has the capacity, and other configurations allow it to start the process, the analysis will then start at 1:00 AM twice a week with a maximum duration of 3:30 hours.



- If you set the Duration (days) as 1 day, you will add 24 hours to the Scheduled Time Slot. The analysis will still start at 1:00 AM twice a week, however, the maximum duration is now going to be 27:30 hours.



4. Click the **Add** button (**6**) to add the configured analysis time to the schedule.

5. You can edit existing schedules by clicking on the **Edit**/**Delete** icons or add additional schedules by clicking the **Add** button and repeating steps 2-4.

6. Click the **Save** button to save the configured analysis windows.

STEP 3: CONFIGURING ROOT DATA ASSET FOR SALESFORCE

The Root Data Asset (RDA) is a set of structured data applied by 1touch.io as a standard for comparison with the detected personally identifiable information.

For detailed information on how RDAs operate and how to optimize RDA application, see **RDA Management User Guide** and **RDA Optimization Guide**.

HOW TO ADD CREDENTIALS

1. To add Salesforce credentials, login to the Root Data Asset Manager module as an administrator (**https:///[Host]:8443/** or **https:///[Host]/aa**).

2. Go to **Settings > Root Data Asset Settings > Credentials**. On the **RDA Credentials** page, click the **Add** button.

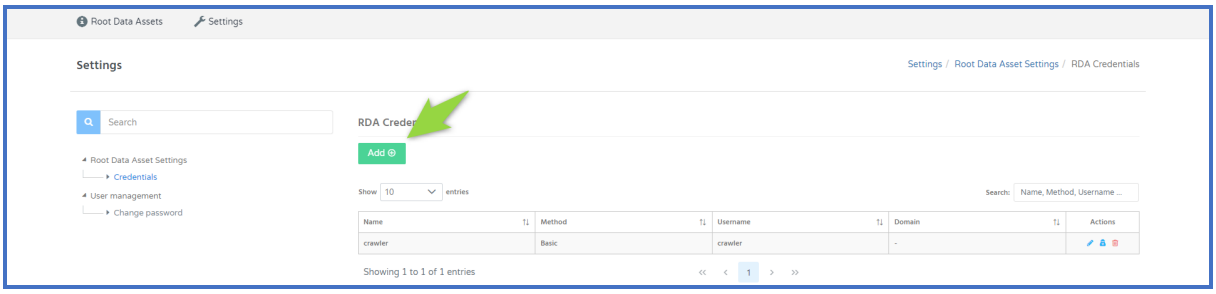


Figure 1: RDA Credentials Page

4. In the **Add RDA Credentials** form, add the Salesforce access credentials. Then click the **Save button (6).**

Table 2: Add RDA credentials popup

PARAMETER	DESCRIPTION
Credentials pane	In the **Name** field (**1**), enter the name of the credentials that will be displayed in the **RDA credential** dropdown list when creating an RDA entry. In the **Authentication Method** dropdown list (**2**), select the **Application secret key (Salesforce)** method.
Application secret key authentication pane	In the **Username** field (**3**), enter the Salesforce username with granted access to the 1touch.io application. In the **Client ID** field (**4**), enter the consumer key of the connected 1touch.io application. Leave the **Private Key** field (**5**), enter the private key of the certificate uploaded as a digital signature in the Salesforce account.

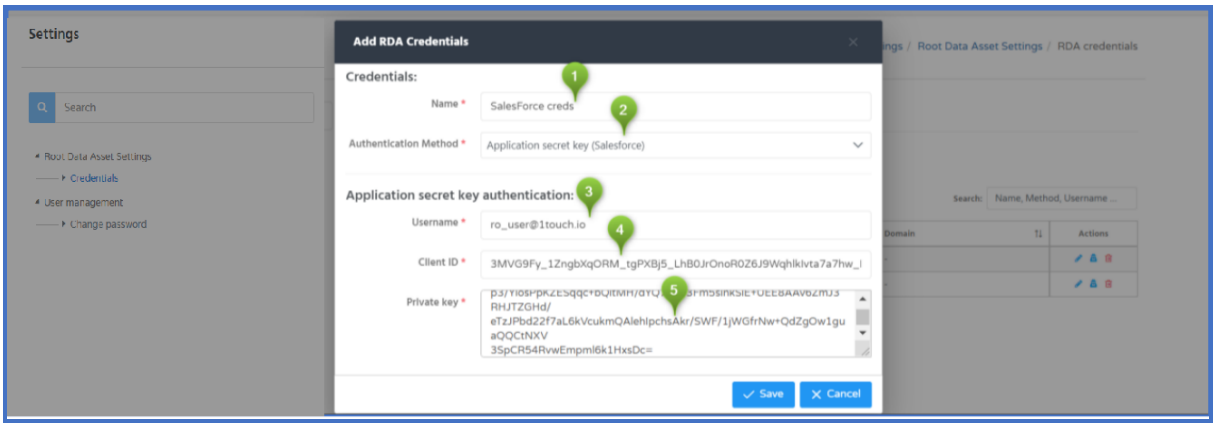
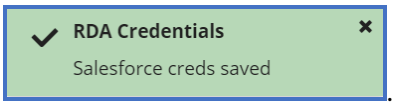


Figure 3: Add RDA Credentials Popup

5. The system will notify you that the credentials are created: 

.

HOW TO CREATE AN RDA ENTRY

1. In the **Header**, click on **Root Data Asset** (**1**) to open the **Root Data Asset Management** page, then click the **Add** button (**2**):

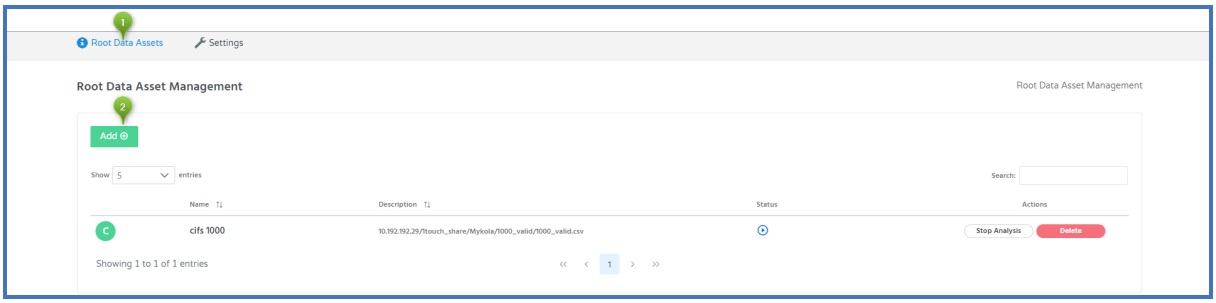


Figure 4: Root Data Asset Management Page

2. In the **Asset Details & Location** tab, fill the RDA details.

Table 5: RDA details in the Asset Details & Location tab

PARAMETER	DESCRIPTION
Name (**1**)	Enter the name of the root data asset shown in the list of RDAs. This name is used only in the application and does not have to match the Salesforce object name. *(Required)*
Description (**2**)	Enter the details with the additional description of the root data asset. For example, *VIP Customers from Salesforce CRM. (Optional)*
Reanalysis (**3**)	Defines the root data asset update analysis rate in seconds. If any If changes are detected during reanalysis, the application downloads and applies them. *(Required)*
Full analysis (**4**)	Defines the root data asset analysis rate in seconds, meaning how often the system must download the file. Full analysis guarantees that the system will apply all the relevant values from the root data asset. *(Required)*

PARAMETER	DESCRIPTION
RDA credentials (5)	Select credentials for access to the Salesforce object. *(Required)*

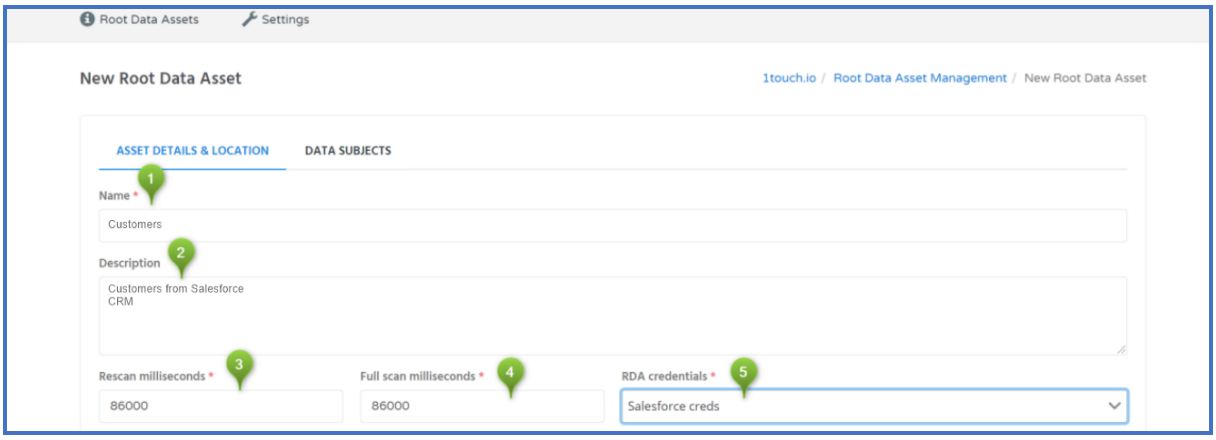


Figure 6: RDA details in the Asset Details & Location tab

3. In the **Asset Details & Location** tab, specify the location of the desired Salesforce object. Then, click the **Validate** button (**5**) to continue.

Table 7: RDA location parameters in the Asset Details & Location tab

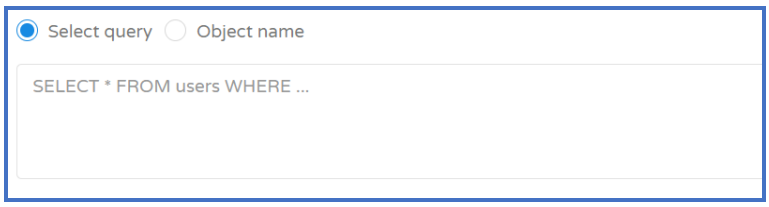
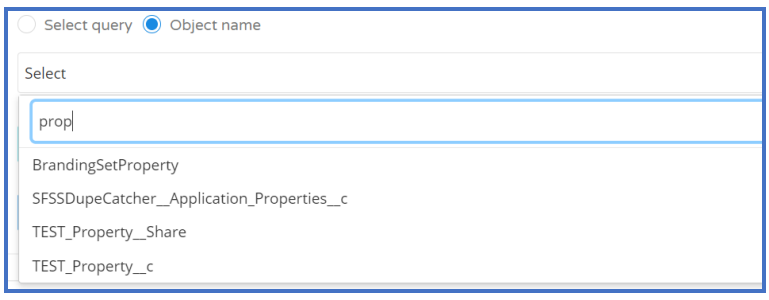
PARAMETER	DESCRIPTION
Type (1)	Select the **SaaS application** option.
Product(2)	Select the **Salesforce** option.
Sandbox (3)	Check **Sandbox** to connect to the Salesforce sandbox environment. Leave **Sandbox** unchecked to connect to the Salesforce production environment.
Connection options (4)	You have two options to connect to the desired object in the Salesforce environment. **Select query**: In the textbox, enter the SQL statement that customizes the RDA list.  **Object name**: In the dropdown list, select the desired Salesforce object. 

Figure 8: RDA location in the Asset Details & Location tab

4. In the **Data Subjects** tab, review and modify the mapping if necessary, then click the **Save** button.

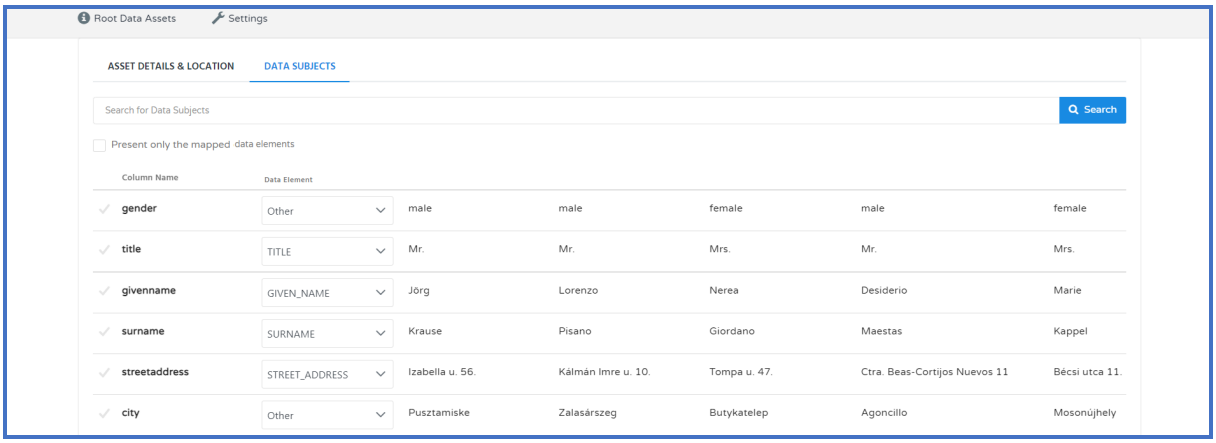


Figure 9: Data Subjects Tab

HOW TO APPLY THE RDA

1. In the **Header**, click on **Root Data Asset** (**1**) to open the **Root Data Asset Management** page.

2. Click **Apply** on the desired entry to enable RDA analysis by the system.

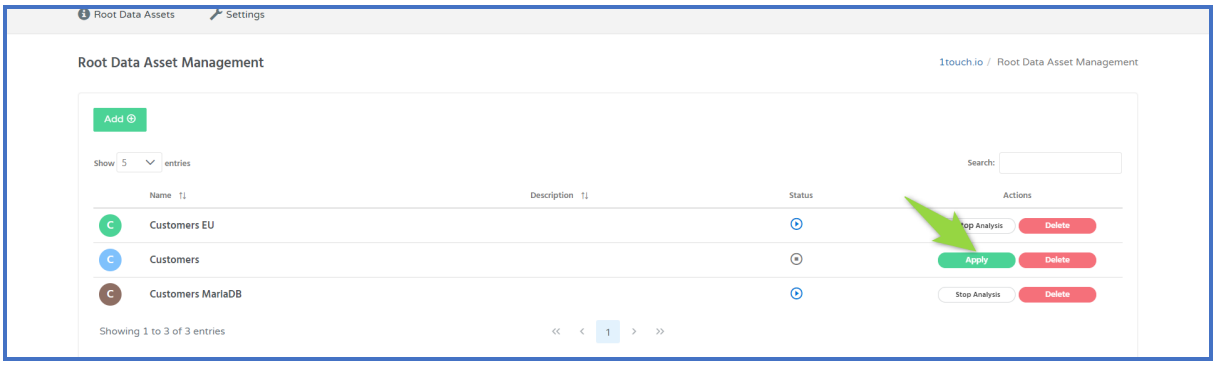


Figure 10: Applying the RDA entry

1touch.io uniquely uses network analytics to help your company discover both sensitive data and its use, even the data you didn't know existed.

1touch.io's Inventa is a data privacy platform with unprecedented data lineage techniques for data discovery and classification. Inventa gives companies complete visibility into their unknown usage of customer data by automating the discovery process and providing them with a comprehensive, accurate, and up-to-date master catalog. This visibility enables you to easily meet regulatory, compliance, and security requirements.