

HOW TO CONNECT TO SALESFORCE

VERSION 4.1.1

October 2024

TABLE OF CONTENTS

Table of Contents	2
Salesforce Overview	3
Step 1: Connecting the 1touch.io application	4
How to Create a Private Key	4
How to Create an App Entry	4
How to Approve the Connected App	8
Step 2 Configuring Data at Rest	11
How to Add Credentials	11
How to Add a Data Source	13
Adding Tags to the Data Source Attributes	16
Configuring Data Source Analysis Schedule	18
Step 3: Configuring Root Data Asset for Salesforce	21
How to Add Credentials	21
How to Create an RDA Entry	22
How to Apply the RDA	24

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 Inventra 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.

```
s-MacBook-Pro ~ % openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout ~/Documents/salesforce_private_key.pem -out ~/Documents/salesforce_cert.pem
Generating a 2048 bit RSA private key
.....+=====
writing new private key to '/Users/...../Documents/salesforce_private_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:UA
State or Province Name (full name) []:
Locality Name (eg, city) []:Kyiv
Organization Name (eg, company) []:1touch
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:
Email Address []:
          @1touch.io
s-MacBook-Pro ~ %
```

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)**.

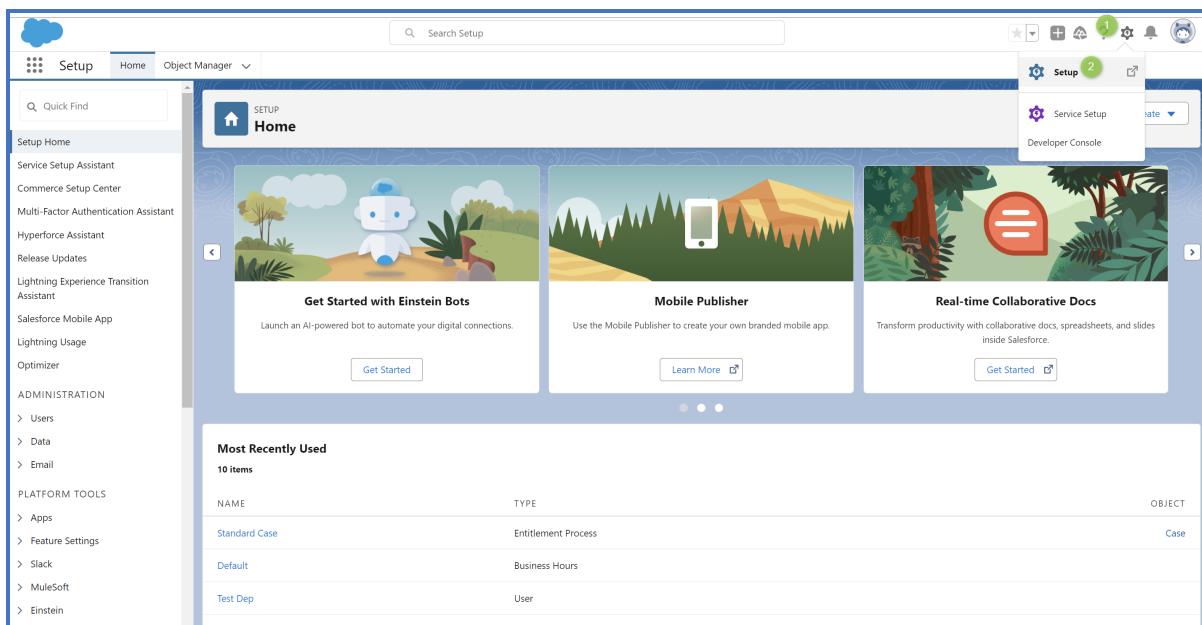


Figure 2: Selecting Setup in the Salesforce customer account

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.

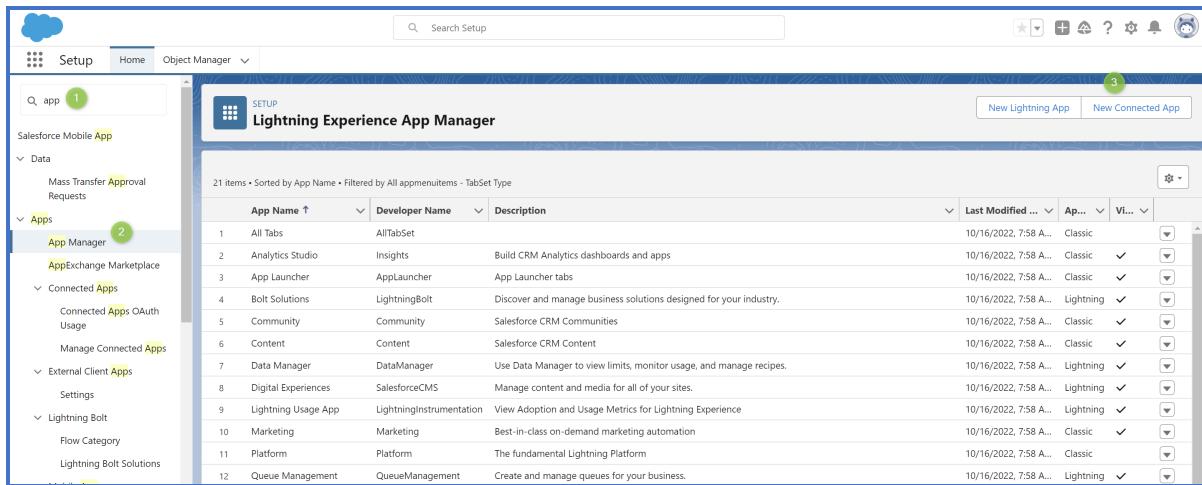


Figure 3: Adding a new connected app in the App Manager

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

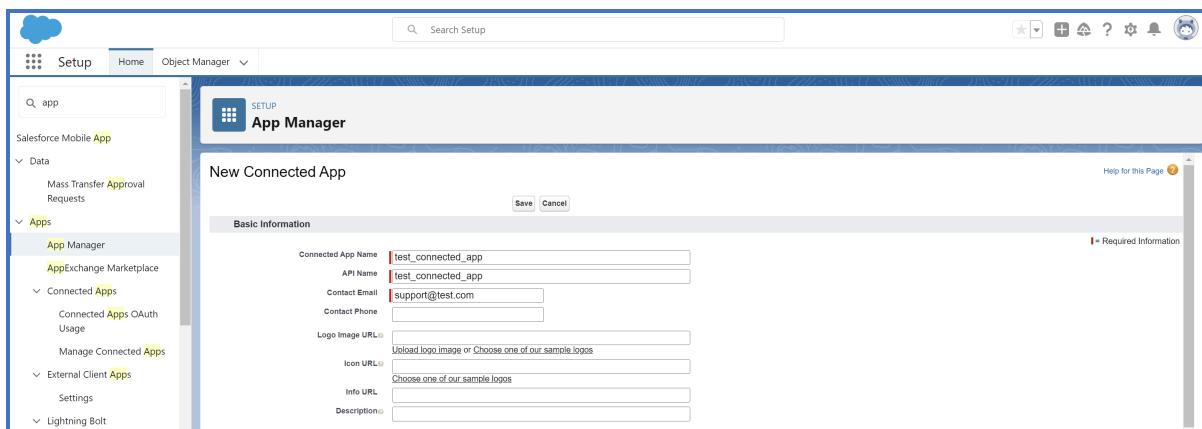


Figure 4: Basic Information pane on the New Connected App page

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 .

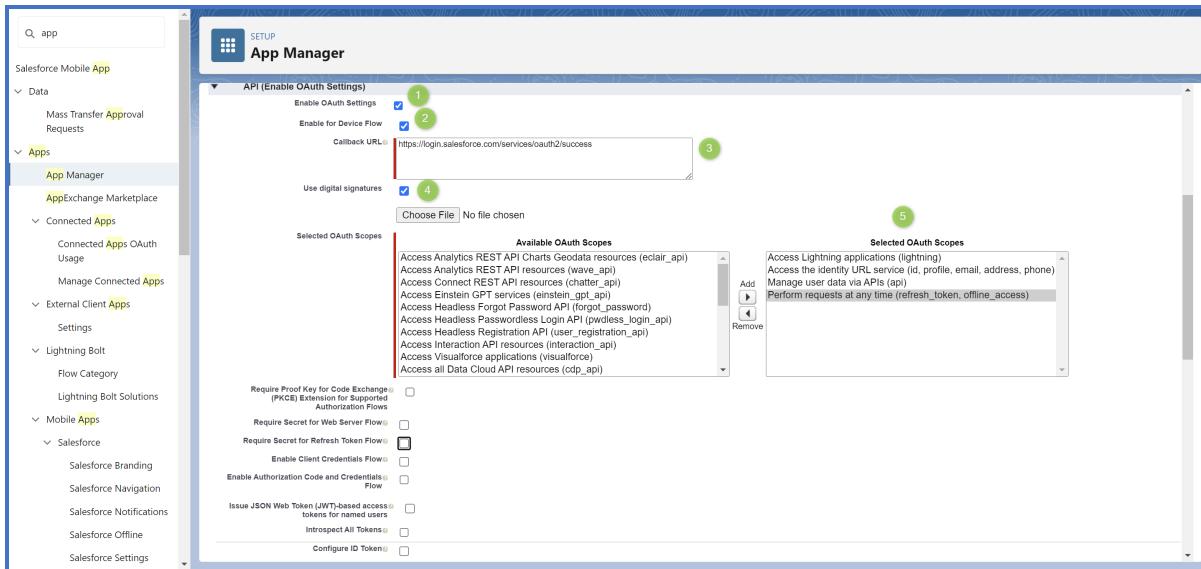


Figure 5: API pane on the New Connected App page

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

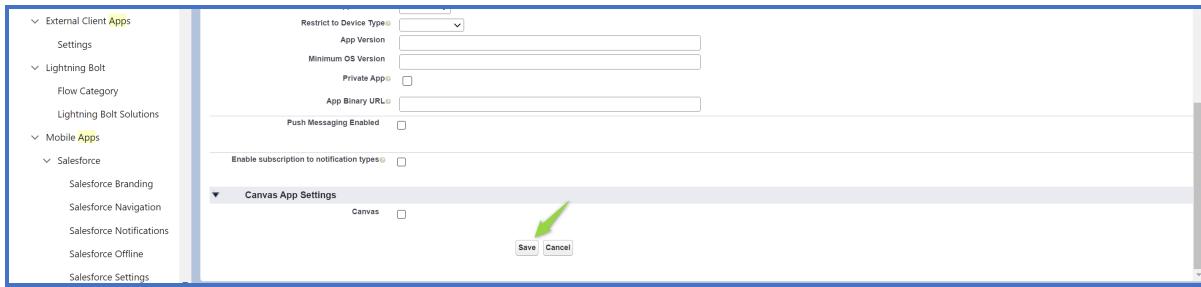
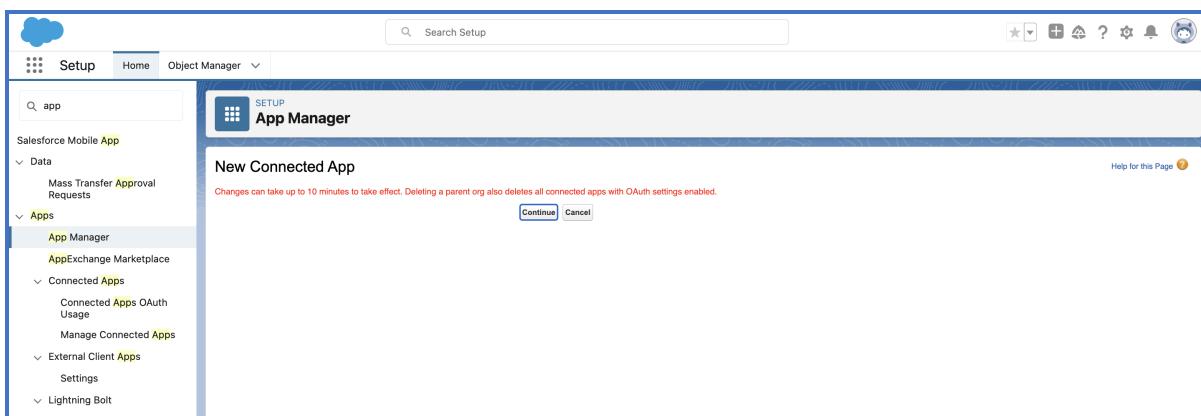


Figure 6: Saving the new connected app

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](#).

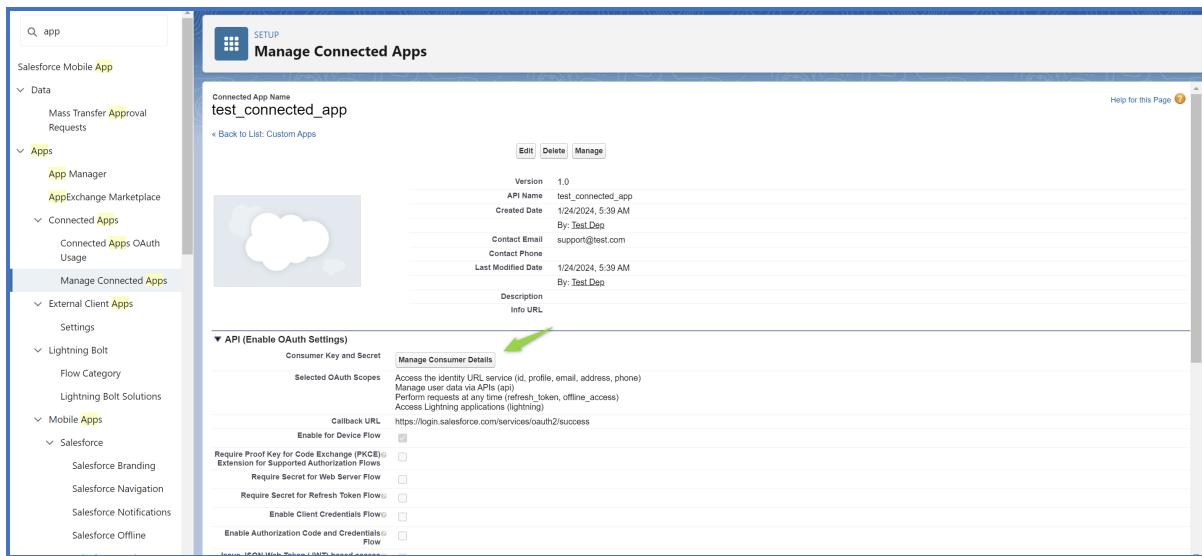


Figure 7: Client ID on the App page

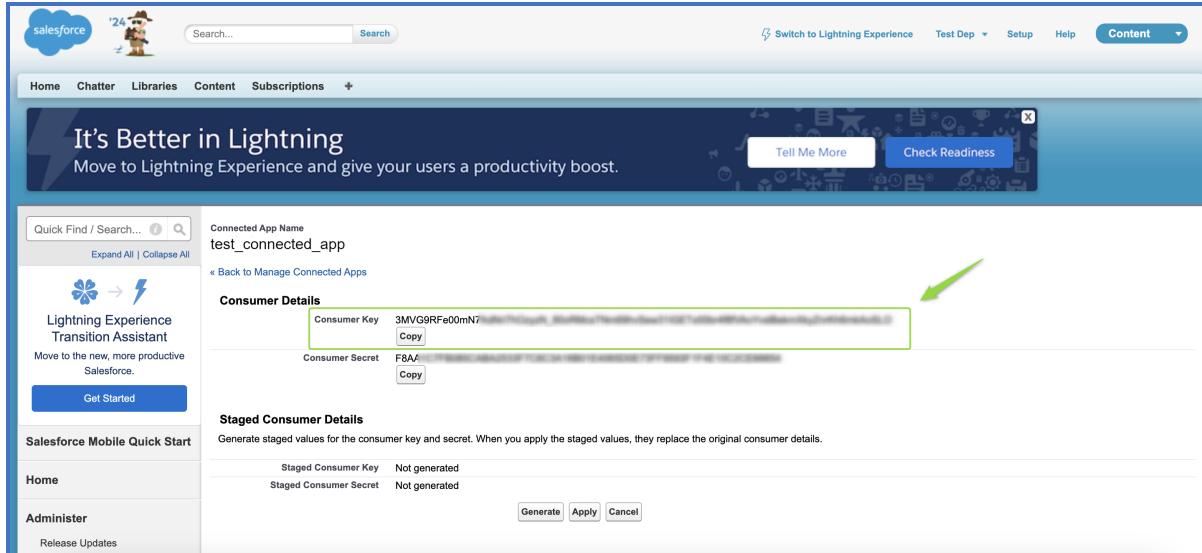


Figure 8: Consumer key

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:

- 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.

The screenshot shows the 'Manage Connected Apps' page. It has a header 'Connected Apps' and a sub-header 'App Access Settings'. Below is a table with two rows:

Action	Master Label	Application Version	Permitted Users
Edit	documentation_connection	1.0	Admin approved users are pre-authorized All users may self-authorize
Edit	test_connected_app	1.0	All users may self-authorize

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**.

The screenshot shows the Salesforce Setup interface under the 'Profiles' section. It lists various profiles such as High Volume Customer Portal, Identity, Salesforce, and System Administrator. The 'System Administrator' profile is selected. The bottom of the list shows a note about 'Work now Only'.

Figure 9: Edit the system administrator profile

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

The screenshot shows the 'Connected App Access' section of the Salesforce Setup interface. It lists several apps and their access status. The 'Connected App Access' section includes checkboxes for 'documentation_connection' (checked) and 'test_connected_app' (checked). Other checkboxes like 'flow_analyzer' and 'Sales Console' are unchecked.

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).

Name	Authentication method	Default credentials	Actions
crawler cifs + nfs	Basic (Login, Password)	✓	edit trash
msExchange creds	Certificate-Based - Microsoft (Client ID, Tenant, Public key, Secret key)	✓	edit trash
msOneDrive creds	Certificate-Based - Microsoft (Client ID, Tenant, Public key, Secret key)	✓	edit trash
googleDrive creds	Certificate-Based - Google (Client email, Delegated user email, Private key)	✓	edit trash
ro_role	Basic (Login, Password)	-	edit trash
GoogleTest1	Certificate-Based - Google (Client email, Delegated user email, Private key)	-	edit trash
s3 def	Access keys - Amazon (Access key, Secret key)	✓	edit trash

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, <i>Salesforce creds</i> .
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.

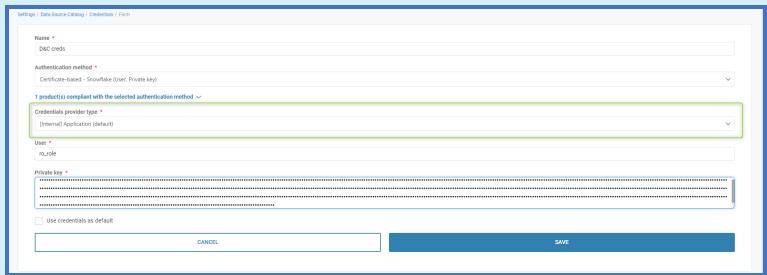


Figure 14: Selecting the credentials provider type

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.

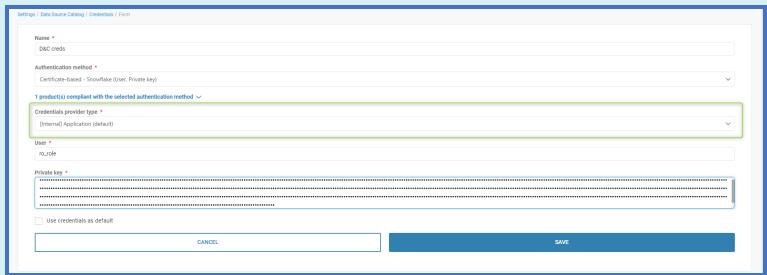


Figure 15: Selecting the credentials provider type

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.

The figure consists of two screenshots of the 1touch.io interface, both titled "Settings / Data Source Catalog / Credentials / Form".

Screenshot 1 (Top): This screenshot shows the "One Drive Secret credentials type" configuration. The "Name" field is set to "salesforce_credentials". The "Authentication method" is selected as "Certificate-based - Salesforce (Username, Client ID, Private key)". The "Username" field contains "system1@...". The "Client ID" field contains "3MVG9RFc00m...". The "Private key" field is filled with a long string of dots, indicating a large private key value. A checkbox for "Use credentials as default" is unchecked. At the bottom are "SAVE" and "CANCEL" buttons.

Screenshot 2 (Bottom): This screenshot shows the "Salesforce credentials type" configuration. The "Name" field is set to "D&C Engine creds". The "Authentication method" is selected as "Certificate-based - Salesforce (Username, Client ID, Private key)". The "Credentials provider type" is set to "[Internal] Application (default)". The "Username" field contains "ro_user". The "Client ID" field contains "ajhdjsncclickxmv...". The "Private key" field is filled with a long string of dots. A checkbox for "Use credentials as default" is unchecked. At the bottom are "CANCEL" and "SAVE" buttons.

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**.

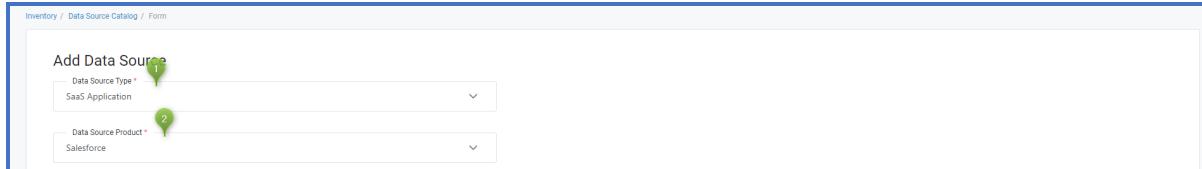


Figure 18: Data Source Type & Product

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. <i>(Required)</i>
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. <i>(Required)</i> 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)	<p>after the previous analysis cycle is completed. (<i>Optional</i>)</p> <p>You can check the Use default timeout box (8) if you defined a default timeout in the Data Source Catalog > Analysis Settings form.</p> <p>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.</p> <p>See the Data Source Catalog User Guide for more information on global data source analysis settings.</p>

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, Inventia 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.

The screenshot shows the 'Data Source Catalog' page. At the top, there are buttons for 'IMPORT' and 'EXPORT'. Below these are filters for 'Repository status' (New, Confirmed, Unconfirmed), 'Significant data sources' (Suspect, Sensitive), and a search bar for 'Product, URL, Creation...'. A 'Bulk Edit' dropdown is also present. The main table lists data sources with columns for Type, Product, URL, Creation Date, Last Analysis Status, Analysis, Data Subjects, Candidates, and Tags. One row is highlighted, showing 'NFS' as the product and 'nfs://10.192.192.29/var/nfsshare/1m_repo/5' as the URL. The 'Tags' column for this row contains 'CCPA'. A green box highlights this 'CCPA' entry.

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).



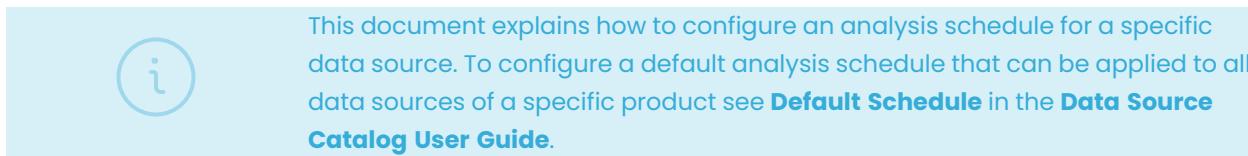
5. To save the tags you selected as attributes of the configured data source, click the **Save** button (5).

The screenshot shows the 'Data Source Details' page with the 'Tags' tab selected. At the top, there are tabs for 'Data Source Details', 'Individual Analysis Schedule', and 'Tags'. Below the tabs, it says '18 tags, 3 selected'. There is a 'Search tags' input field with a magnifying glass icon. A list of tags is shown, with several checked: 'GDPR', 'CCPA', 'DMZ', 'Encrypt', 'External', 'Decrypt', 'Delete', 'Encrypt', 'External', 'GDPR', 'HIPAA', and 'None'. A note at the bottom says 'You can add/edit tags in settings'. A blue button at the bottom right is labeled 'SAVE'.

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. Inventra will automatically enable and disable the analysis plugin at configured times.



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**:

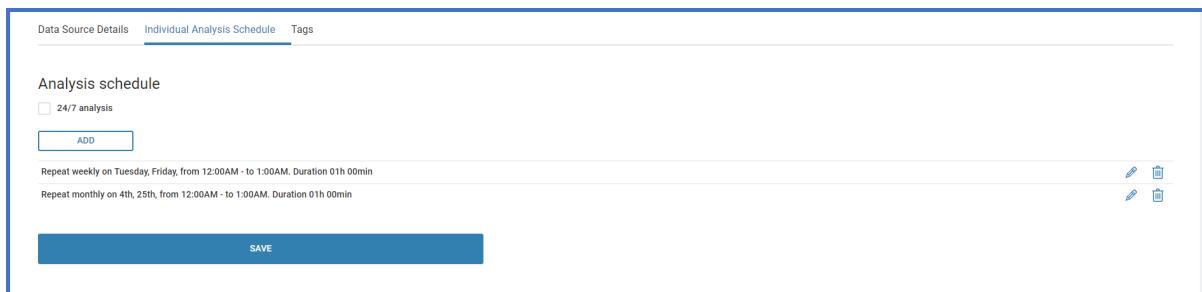


Figure 1: Individual Analysis Schedule Tab

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:



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).

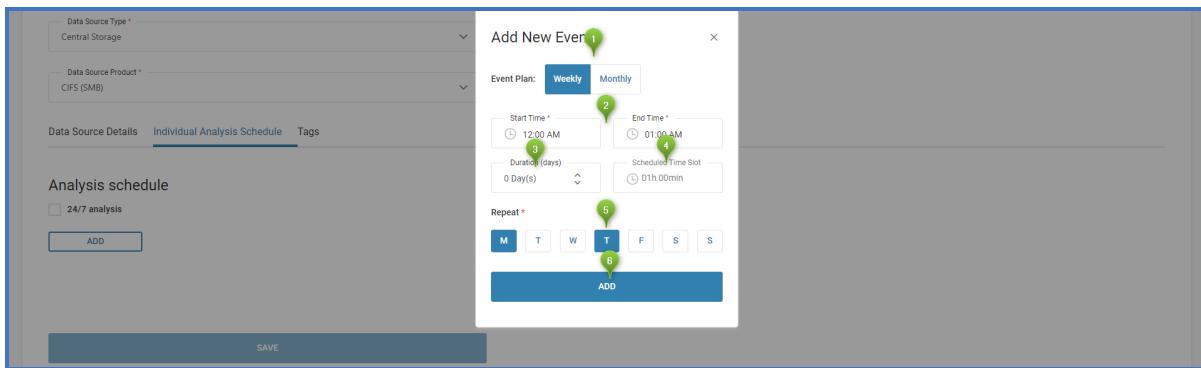


Figure 3: Add New Event popup Window

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.

i

Add New Event

Event Plan: **Weekly**
Monthly

Start Time *

End Time *

Duration (days)

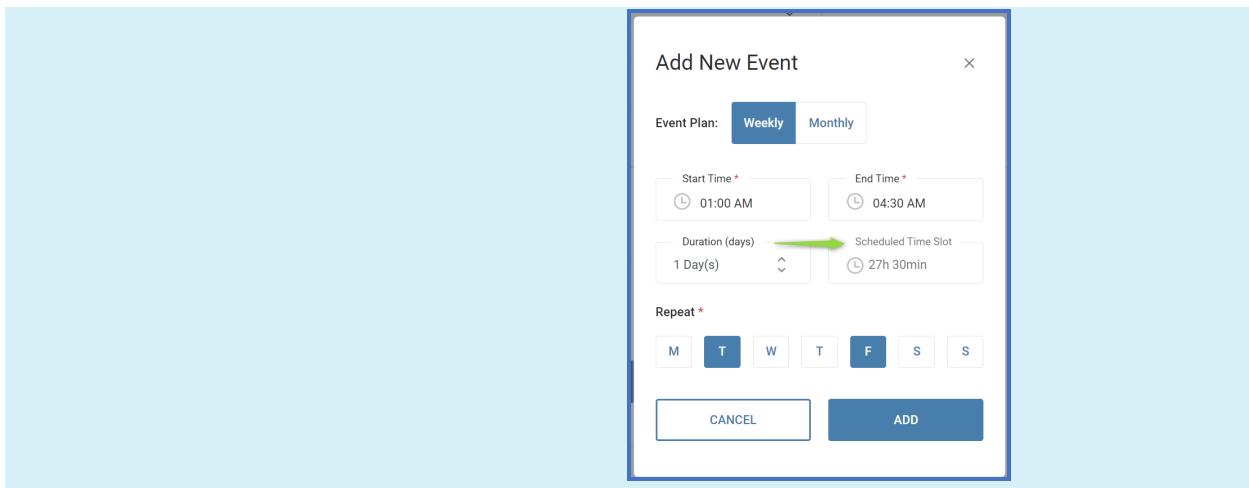
Scheduled Time Slot

Repeat *

M
T
W
T
F
S
S

CANCEL
ADD

- 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/](https://[Host]:8443/) or [https://\[Host\]/aa](https://[Host]/aa)).
2. Go to **Settings > Root Data Asset Settings > Credentials**. On the **RDA Credentials** page, click the **Add** button.

The screenshot shows the 'RDA Credentials' page within the 1touch.io Root Data Asset Manager. At the top, there's a navigation bar with 'Root Data Assets' and 'Settings'. Below it is a search bar and a sidebar with links like 'Root Data Asset Settings', 'Credentials' (which is selected and highlighted in blue), 'User management', and 'Change password'. The main area has a heading 'RDA Credentials' with a green arrow pointing to the 'Add' button. Below the heading is a table with columns: Name, Method, Username, Domain, and Actions. A single row is shown: 'crawler' under Name, 'Basic' under Method, 'crawler' under Username, '-' under Domain, and a set of icons under Actions. At the bottom of the table, it says 'Showing 1 to 1 of 1 entries'.

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.

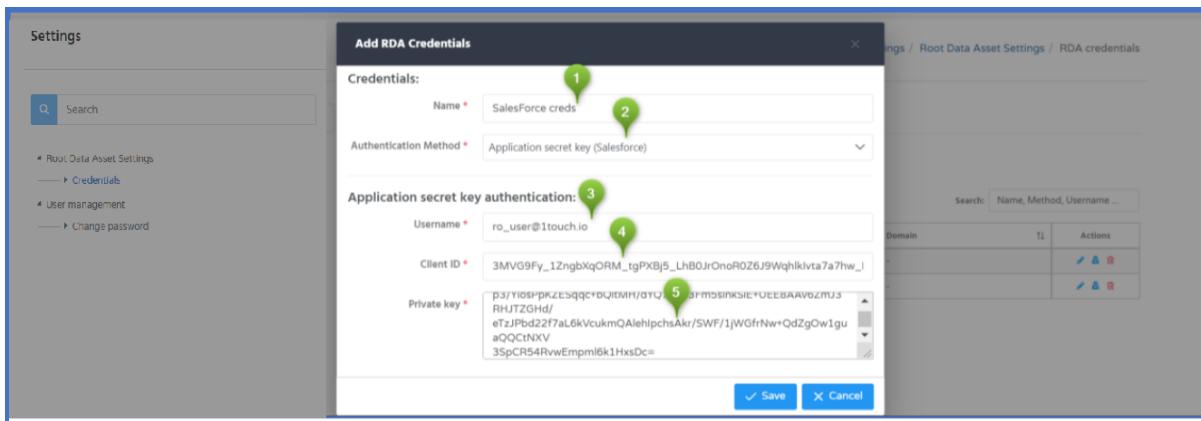


Figure 3: Add RDA Credentials Popup



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):

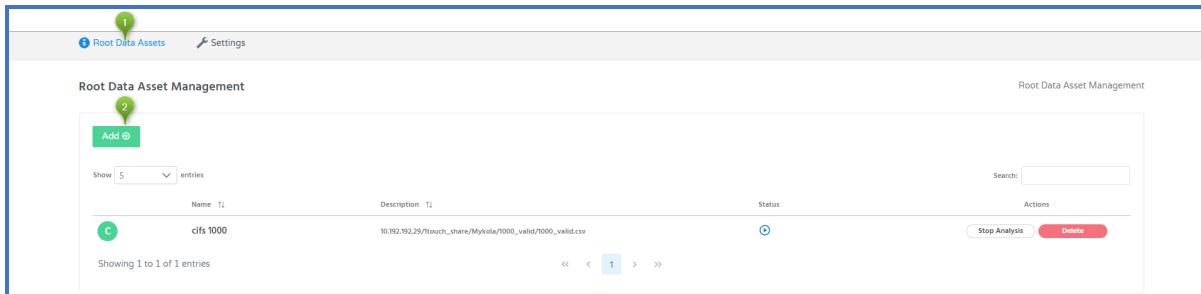


Figure 4: Root Data Asset Management Page

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, <i>VIP Customers from Salesforce CRM</i> . (Optional)
Reanalysis (3)	Defines the root data asset update analysis rate in seconds. If any 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)

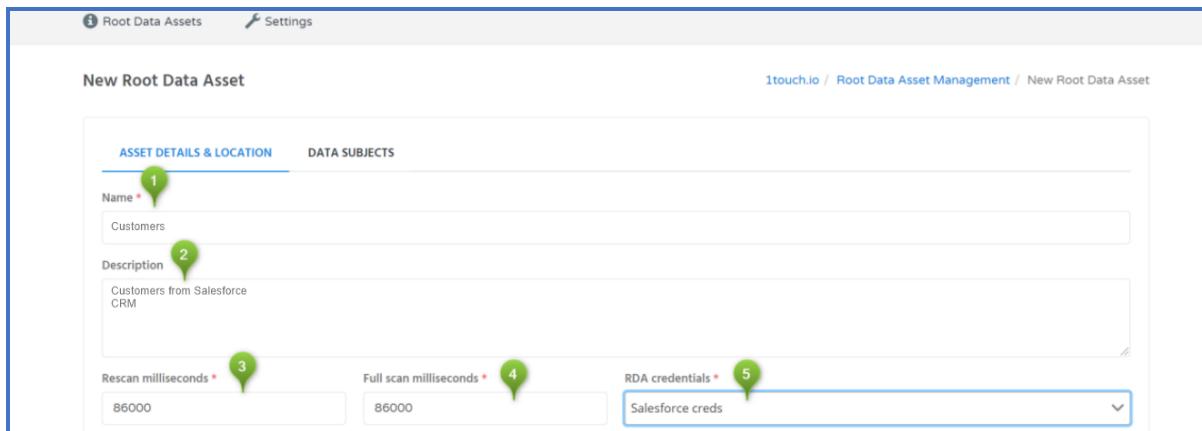
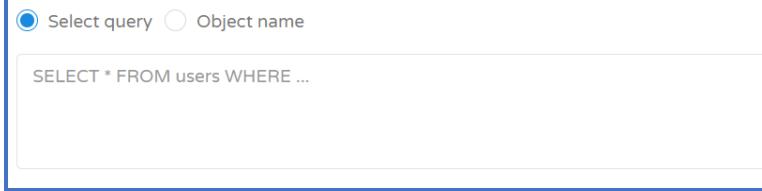
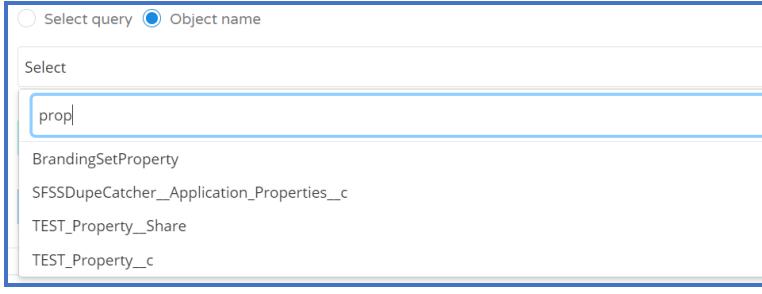


Figure 6: RDA details in the Asset Details & Location tab

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. 

The screenshot shows the 'Asset Details & Location' tab of the 1touch.io interface. It includes fields for 'Reanalysis, ms *' (set to 86000), 'Full analysis, ms *' (set to 86000), and 'RDA credentials *' (set to 'salesforce_documentation_test_creds'). A 'Type' section has 'SaaS application' selected. A 'Product' dropdown is set to 'Salesforce'. Under 'Salesforce', there's a 'Sandbox' checkbox (unchecked) and a dropdown for 'Select query' or 'Object name' (set to 'Object name'). An 'Account' dropdown is present. At the bottom are 'Save' and 'Cancel' buttons.

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

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

The screenshot shows the 'Data Subjects' tab. It lists various columns from a database and maps them to data elements in Salesforce. The columns include gender, title, givenname, surname, streetaddress, and city. The data elements mapped to them are Other, TITLE, GIVEN_NAME, SURNAME, STREET_ADDRESS, and Other respectively. The table also includes male, female, Mr., Mrs., Jörg, Lorenzo, Krause, Pisano, Izabella u. 56., Kálmán Imre 10., Pusztafalu, Zalasárszeg, Butykatelep, Desiderio, Nerea, Giordano, Tompa u. 47., Ctra. Beas-Cortijos Nuevos 11, Agoncillo, and Mosonújhely.

Figure 9: Data Subjects Tab

HOW TO APPLY THE RDA

- In the **Header**, click on **Root Data Asset** (1) to open the **Root Data Asset Management** page.
- Click **Apply** on the desired entry to enable RDA analysis by the system.

The screenshot shows the 'Root Data Asset Management' page. It lists three entries: 'Customers EU' (Status: Enabled), 'Customers' (Status: Enabled), and 'Customers MariaDB' (Status: Enabled). Each entry has an 'Actions' column with buttons for 'Top Analysis', 'Delete', 'Stop Analysis', and 'Apply'. A green arrow points to the 'Apply' button for the 'Customers' entry.

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.

