ACCELARIO

Accelario Data Masking Module

User Guide V20.0

January 2023

Contents

1. Product Overview

The Accelario Data Masking module enables in-place masking using an intelligent, sensitive data search engine to easily locate and mask sensitive data. Data masking is performed in accordance with either customized or predefined masking policies (e.g. GDPR, HIPAA). Masked data is transformed into production quality data which preserves referential integrity with minimal user intervention throughout the masking process.

It contains the following components:

- Privacy Dashboard
- Data Sources
- Environments
- Sensitive Data Search
- Masking Editor
- Masking Rules
- Privacy Policies
- Users
- System Setup
- Job Monitoring
- Event Viewer

1.1. Privacy Dashboard

Accelario **Privacy Dashboard** provides clear indications of your privacy exposures. It can scan all non-production data sources for privacy issues. With just one click you can easily drill-down to see an exposed data source. In the **Privacy Dashboard** window, you can:

- Scan all data sources for sensitive data with one-click, compliant with specific privacy policies such as GDPR or CCPAV.
- Refresh all data sources – metadata DDL is updated from the source. New / altered / deleted tables and columns are automatically updated.
- See a global view of sensitive data for all managed data sources.
- See a detailed view of sensitive data per managed data source.
- Find privacy exposures at any level: data source, environment, database, schema, table, and column.

For more information, see Privacy Dashboard.

1.2. Data Sources

A **Data Source** is database or a file where data that is being used comes from. A **Data Source** is given a name and the location of the server is specified to set up a connection to the database . From the **Data Sources** window, you can:

- Add a new data source
- Modify/remove an existing data source

Only a user with **Admin** privileges can see or edit **Data Sources**.

For more information, see Managing Data Sources.

1.3. Environments

An **Environment** is an object that groups together database schemas from a data source. An environment object is used for scanning and masking. From the **Environments** window, you can:

- Add a new environment from different data source schemas
- Modify/Remove an existing environment
- Refresh an environment – metadata is updated from the data source. new / altered / deleted tables and columns are automatically discovered / discarded. Foreign key relationships are updated to maintain referential integrity.

For more information, see Managing Environments.

1.4. Sensitive Data Search

Accelario **Data Masking** incorporates an intelligent search engine that leverages advanced search algorithms containing lookup lists and AI technology. From the **Sensitive Search** window, you can:

- Scan an environment with one-click, compliant with specific privacy policies such as GDPR or CCPA.
- Masking rules are automatically assigned to the correct sensitive column(s).
- Foreign key groups are assigned with the same masking rules to maintain referential integrity.
- See a high-level view of the scan results including Top Sensitive Data and statistics.
- See a detailed view of all sensitive columns that were found.
- Select the sensitive column to be masked.

For more information, see Searching for Sensitive Data.

1.5. Masking Editor

With the **Masking Editor** you can view / modify selected sensitive columns and manually assign masking rules to columns. From the **Masking Editor** window, you can:

- Assign / modify a masking rule for a specified column.
- Add a **Where Clause** to a table for masking.
- Perform **Backup** / **Restore** of a masking configuration file.
- Execute and monitor a Mask operation in the **Progress Monitor** window.

For more information, see Masking Editor - Editing Masking Rules and Running Masking Operation.

1.6. Masking Rules

A **Masking Rule** contains both the scanning and masking methods used to search for and mask specified sensitive data (e.g. Name, Email, Credit Card, etc.). From the **Masking Rules** window, you can:

- See all supported built-in masking rules
- Add and manage custom masking rules
- Duplicate built-in/custom masking rule to create a new custom masking rule

For more information, see Managing Masking Rules.

1.7. Privacy Policies

A **Privacy Policy** is a set of masking rules that are used to scan and mask following a specified privacy regulation such as GDPR, CCPA, HIPAA, or a set of organizational specific privacy rules. From the **Privacy Policies** window, you can:

- Add, view, modify, and duplicate a privacy policy.
- Add a **Mailing Rule** to mask an address that is spread over several columns in a particular table for a valid address.

For more information, see Managing Privacy Policies.

1.8. Users

Accelario Data Masking uses a **role-based user management system**. All users can access the **Privacy Dashboard**. Users are divided into the following categories:

- Admin – and Admin user can manage data sources, all environments and perform monitoring and troubleshooting
- Regular users – regular users are restricted to scan and mask only the environments that they have authorized access

Only a user with Admin privileges can create or modify users and roles.

From the Users Management window, you can:

- Create and modify users
- Create and modify roles

For more information, see Managing Users and Roles.

1.9. System Setup

The **System Setup** is used to define system parameters, such as SMTP, Active Directory, etc. From the **System Setup** window, you can:

- Configure Active Directory Authorization
- Configure SMTP configuration

Only a user with Admin privileges can access the System Setup.

For more information, see System Setup.

1.10. Job Monitoring

Job Monitoring is used to monitor the status of current system jobs. From the **Job Monitoring** window, you can:

- See all current or just terminated system jobs (the history system jobs can be seen in the Event Viewer window)
- Drill down and see the detailed status of some of the system jobs

Only a user with **Admin** privileges can access **Job Monitoring**.

For more information, see Job Monitoring.

1.11. Event Viewer

The **Event Viewer** is used to view and save all user events. From the **Event Viewer** window, you can:

- View/filter/search all user events
- Save all user events to a file

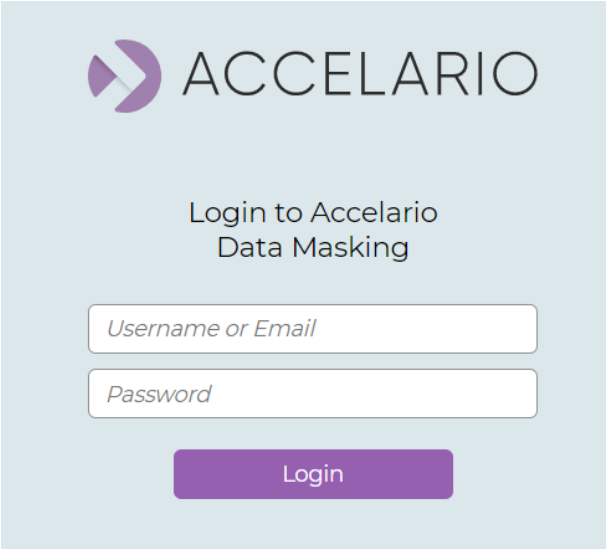
For more information, see Event Viewer.

2. Login to the Data Masking Module

To login in to the Data Masking Module:

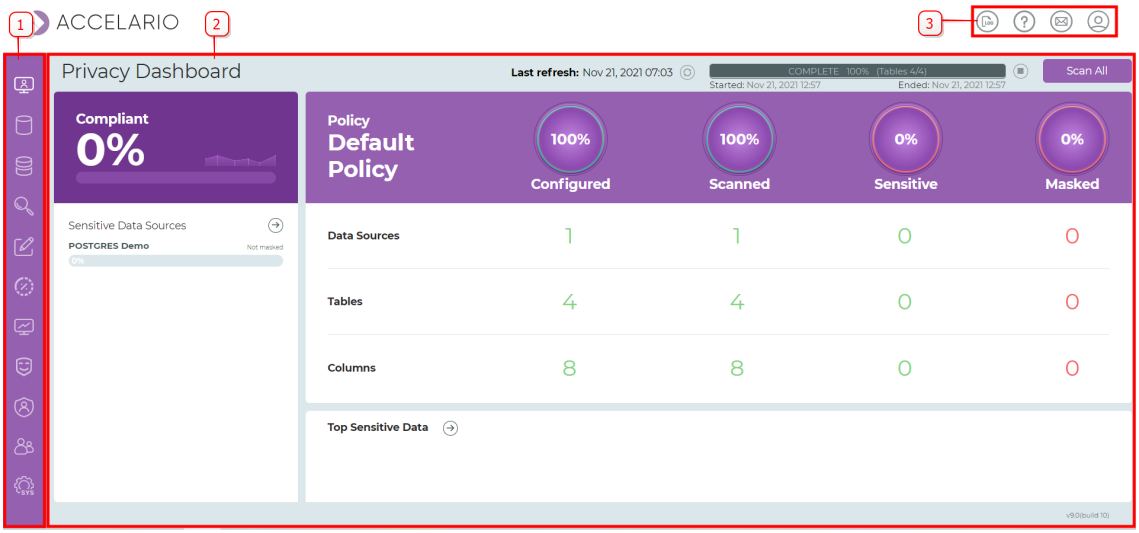
Your username and password are set by the approved person that does the user management process.

1. Enter your **Username** or **Email**.
2. Enter your **Password**.
3. Click **Login**.



3. Getting to Know the GUI

The following image and table describe the Data Masking Module.

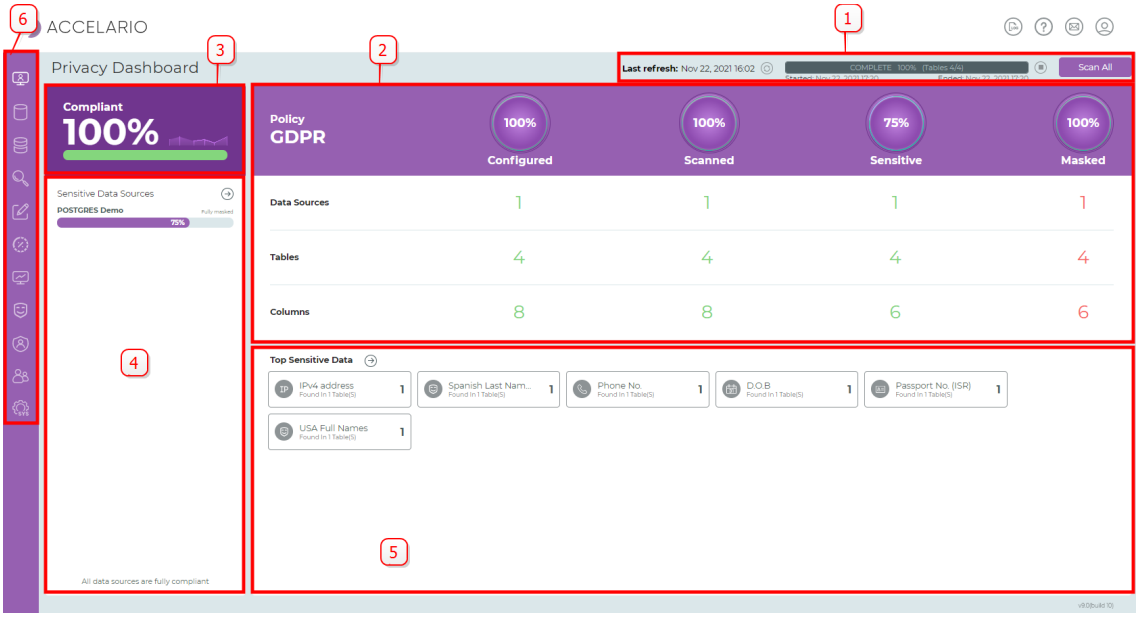


#	Item	Description
1	Navigation bar	Used to put content in the main work area.
2	Main Work Area	Main work area where you perform tasks
3	Task bar	System tasks

The interface is dynamic and changes according to the feature selected.

4. Privacy Dashboard

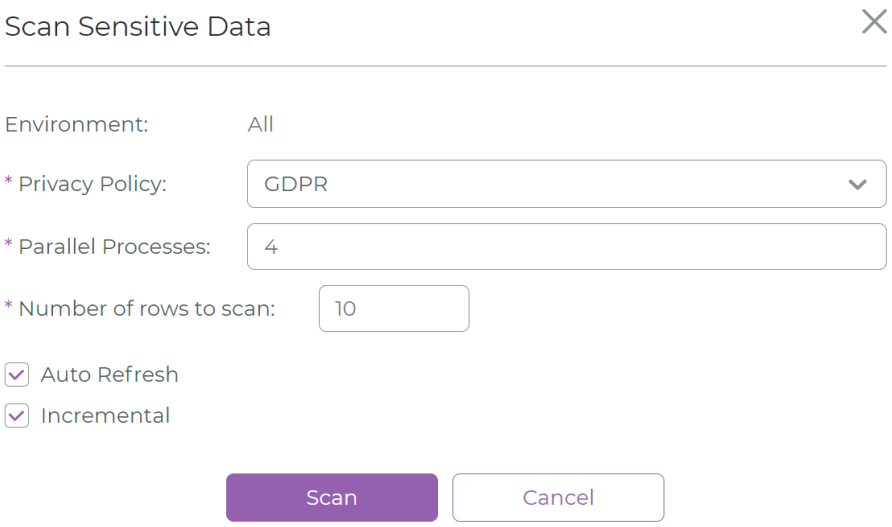
The **Privacy Dashboard** gives clear indications of your privacy exposures. It can refresh and scan all non-production data sources for privacy issues. With just one click you can easily drill-down to see an exposed data source. The following image and table describe the **Privacy Dashboard**.



#	Item	Description
1	Scan bar	Do a refresh and scan for all managed data sources.
2	View Area	Shows the status of a scan and applied masks for a specified privacy policy.
3	Compliant bar	Shows the compliant percentage.
4	Sensitive Data Sources	Shows all managed data sources with their sensitivity level.
5	Top Sensitive Data	Shows the top sensitive data.
6	Navigation Bar	Provides quick access to the main task areas.

To scan for potential sensitive data:

1. Click Scan All (**Scan All**).
2. In the Scan Sensitive Data window, configure the scan parameters and click **Scan**.



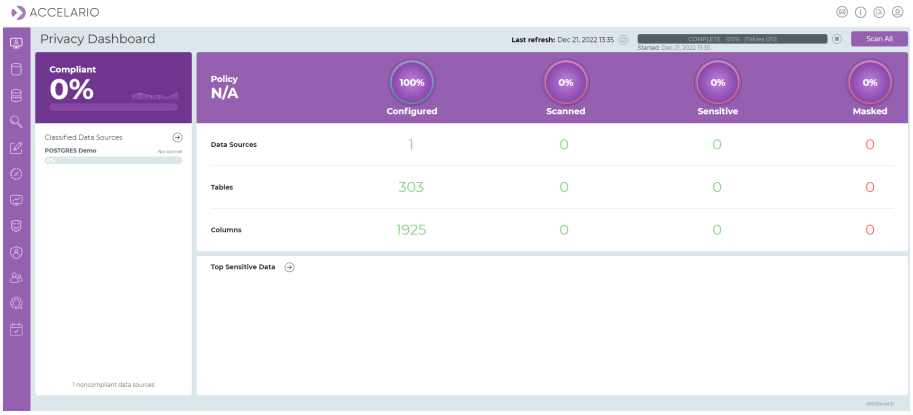
In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

To stop a scan:

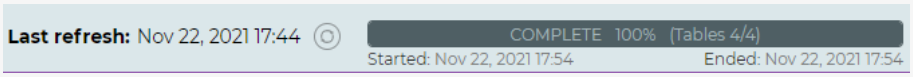
1. Click .

To do a Refresh All:

1. Click **Start refresh environments** .
2. All results from the previous scan is removed.

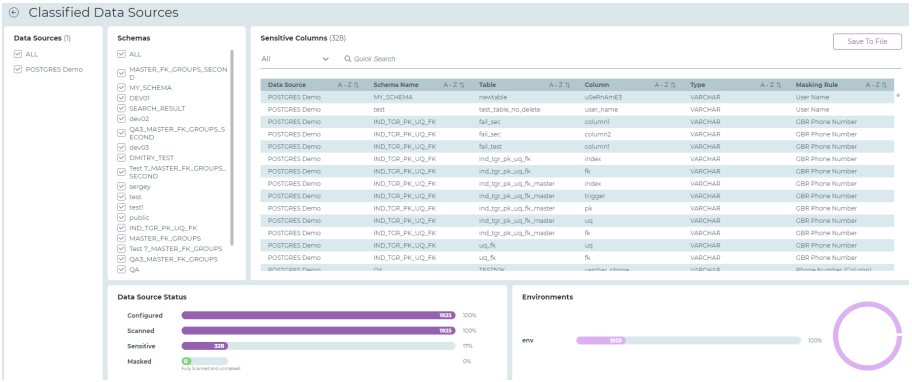


On the scan bar, you can see the following scan information:



To see the potential classified data sources:

1. Click Classified Data Sources .



2. To return to the **Privacy Dashboard**, click Classified Data Sources .

To see top sensitive data:

1. Click **Top Sensitive Data** .

2. To return to the **Privacy Dashboard**, click Top Sensitive Data .

5. Managing Data Sources

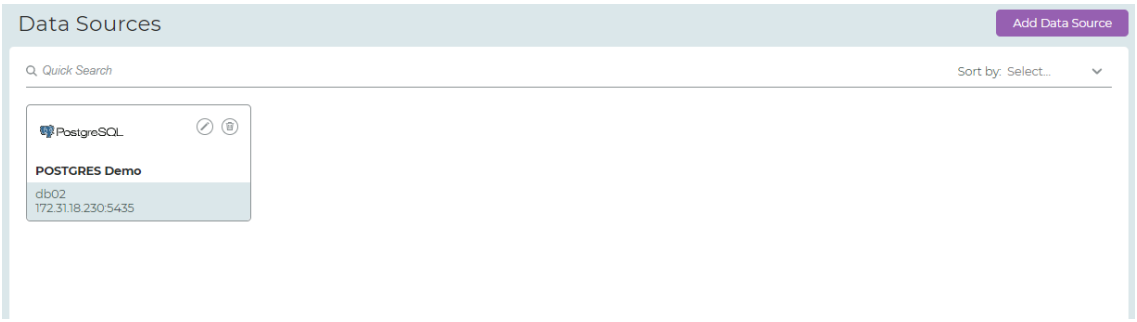
A **Data Source** is database or a file where data that is being used comes from. This section describes how to define and manage the data sources.

Only a user with **Admin** privileges can see or edit **Data Sources**.

To see available data sources:

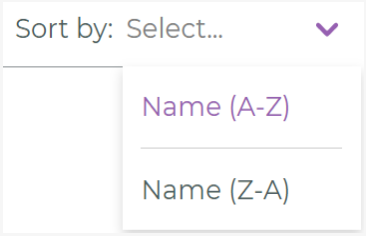
1. On the navigation bar, click **(Data Sources)**.

2. The **Data Sources** window appears displaying all data sources that have been added to the system.



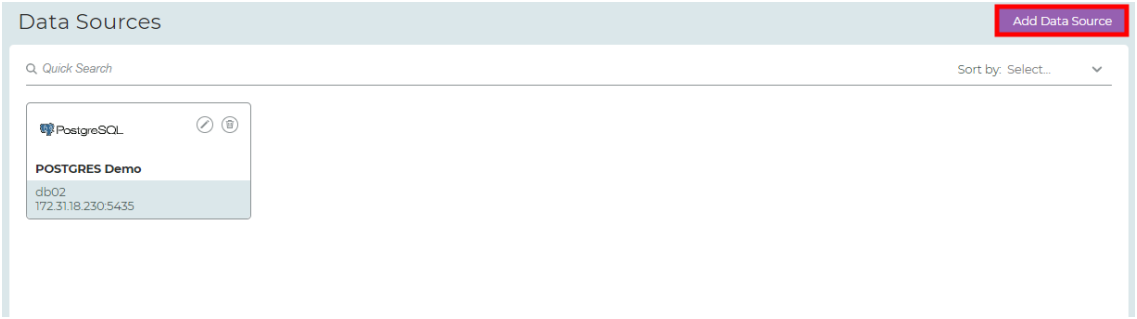
You can quickly locate content by typing its letters on the **Quick Search** bar. The list updates promptly.

You can display the list in ascending or descending alphabetical order.

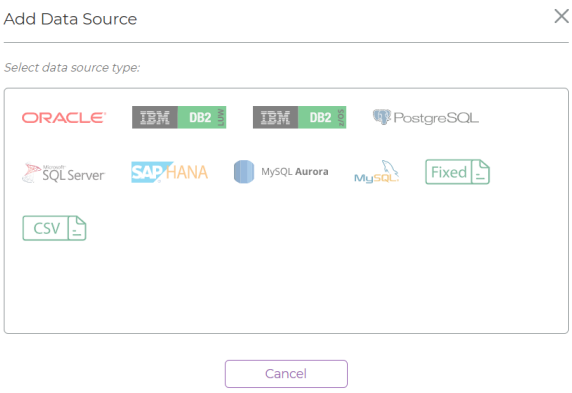


To add a new data source:

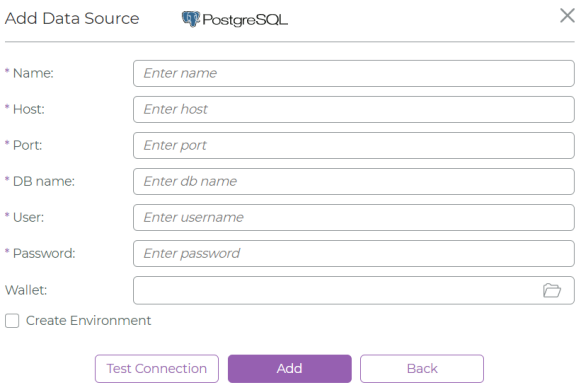
1. Click **Add Data Source**.



2. Select source data type.



3. Fill in the data source details.

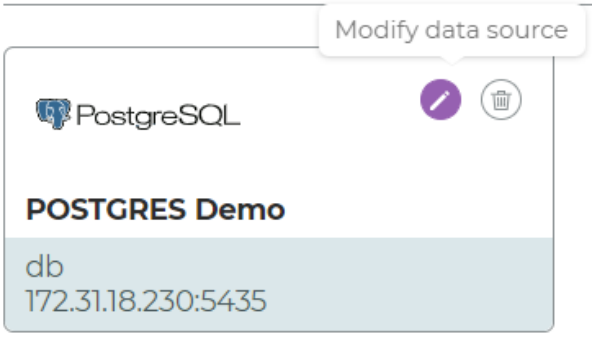


In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

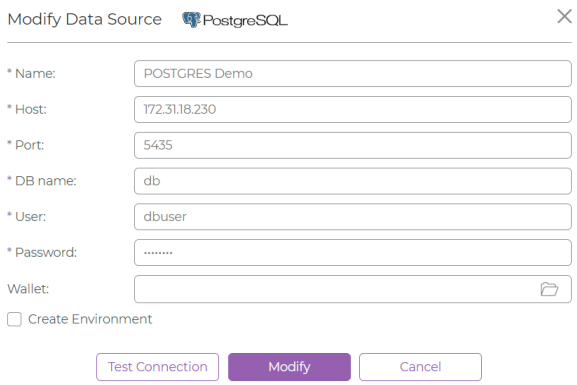
4. Click **Test Connection** to verify that the connection to the new data source is valid.
5. Click **Create Environment** to automatically create an environment that includes all schemes of this data source.
6. Click **Add**.

To modify data source details:

1. On the required data source, click **(Modify data source)**.



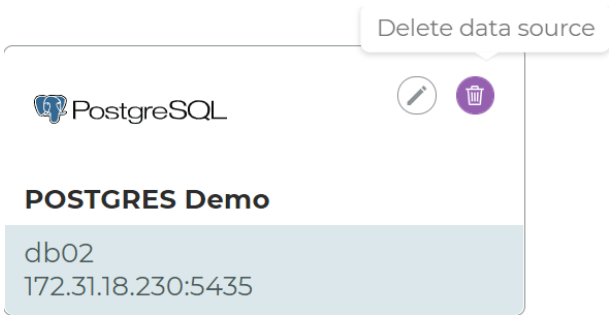
2. The **Modify Data Source** window appears. Modify the data source details as required.



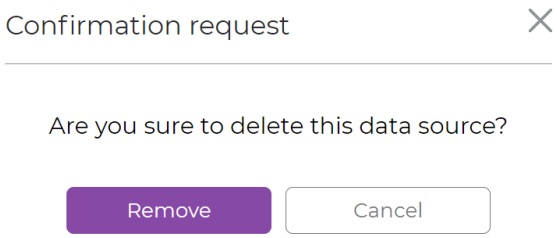
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

To delete a data source:

1. On the required data source, click (Delete data source).



2. Click **Remove** to confirm the deletion, or **Cancel** to exit without deleting the data source.



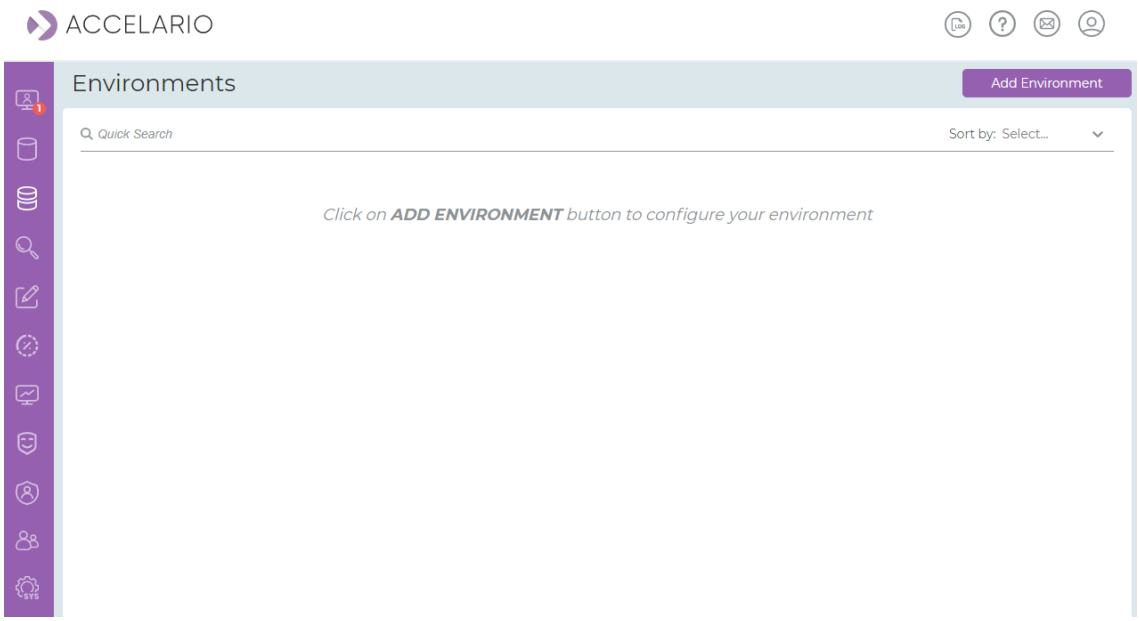
6. Managing Environments

An Environment is an object that groups together database schemas from a data source. An environment object is used for scanning and masking.

To see your environments:

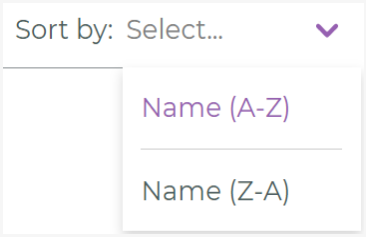
1. On the navigation bar, click  **(Environments)**.

2. The **Environments** window appears.



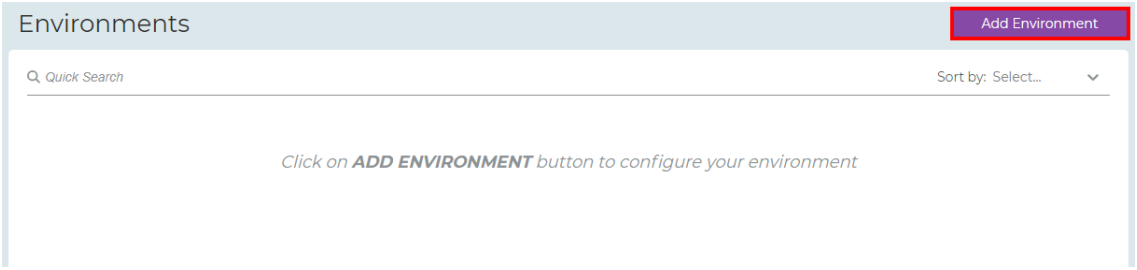
You can quickly locate content by typing its letters on the **Quick Search** bar. The list updates promptly.

You can display the list in ascending or descending alphabetical order.

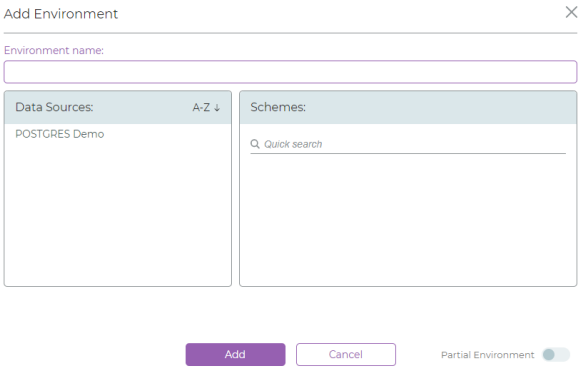


To add a new environment:

1. Click **Add Environment**.



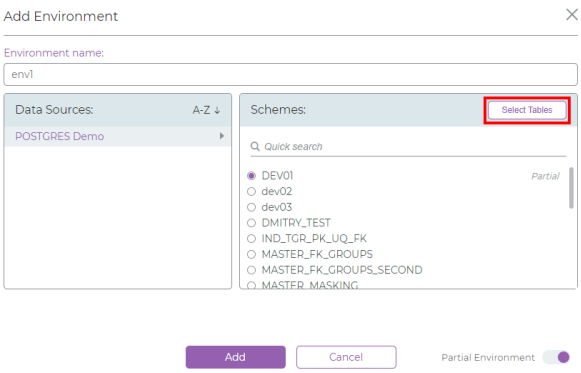
2. Fill in the environment details:
   a. In **Environment name**, provide a name.
   b. Under **Data Sources**, select the data source for the new environment.
   c. Under **Schemes**, select the data source schemes that the environment will use, or click **Select All** to include all schemes of the selected data source.



3. For specific Tables from Schemas:

   a. Click Partial Environment  .

   b. In **Data Sources** select a data source.



   c. In **Schemes**, select the scheme to be used.

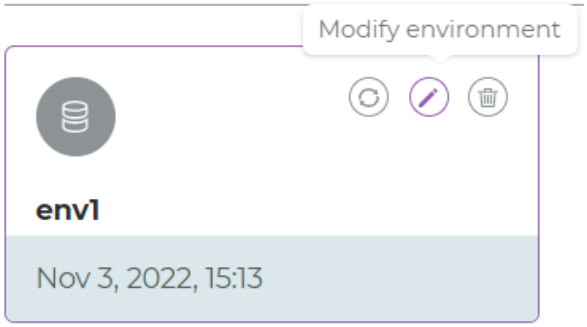
4. Click **Select Tables**.
5. Select the **Table(s)** to be used.

> The list shown is the list from the last refresh. To update the list, Click **Refresh**.

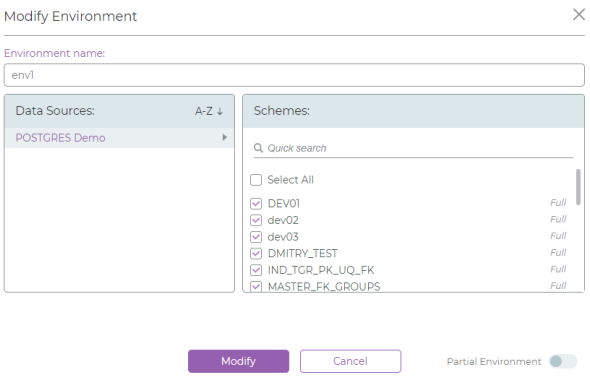
6. Click **Submit**.
7. Click **Add**.

To modify environment details:

1. On the required environment, click **(Modify environments)** .



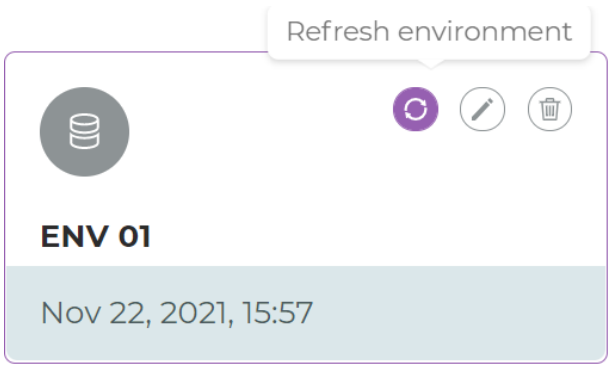
2. The **Modify Environment** window appears. Modify the environment details as required.



3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

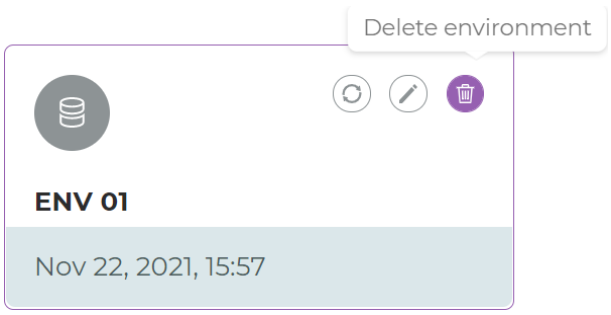
To refresh an environment:

1. On the environment , click (Refresh environment).

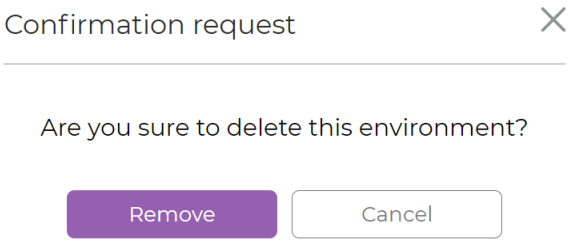


To delete an environment:

1. On the environment , click (Delete environment).



2. Click **Remove** to confirm the deletion, or **Cancel** to exit without deleting the environment.



7. Searching for Sensitive Data

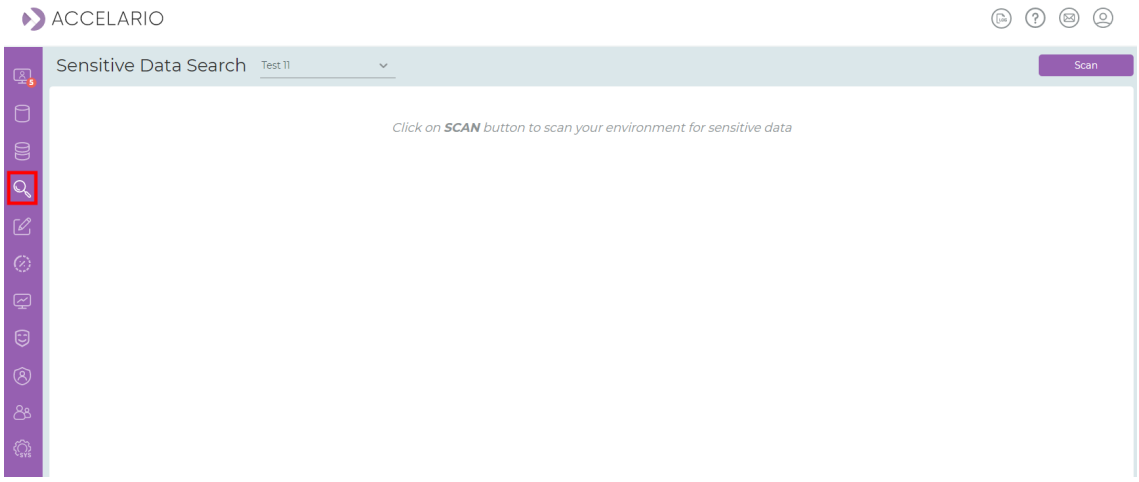
Accelario Data Masking includes an intelligent search engine that leverages advanced search algorithms that contain lookup lists and AI-technology.

Once you have setup an environment, you can search the environment for sensitive data that you may want to mask.

You can also see results and perform new scans.

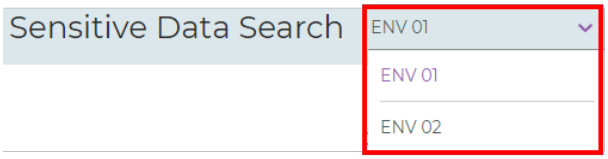
To manage your sensitive data searches:

1. On the navigation bar, click  (**Sensitive Search**).

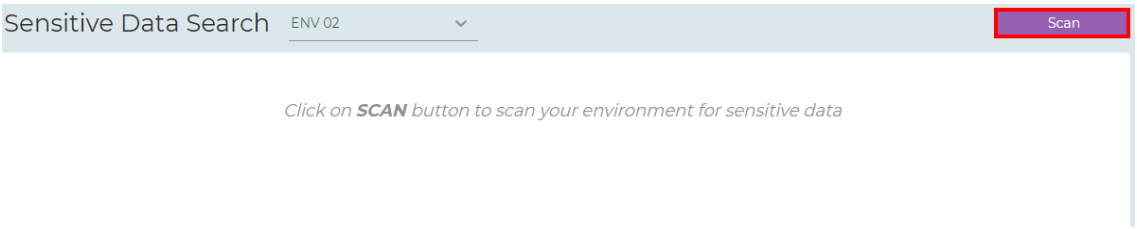


To perform a new sensitive data search:

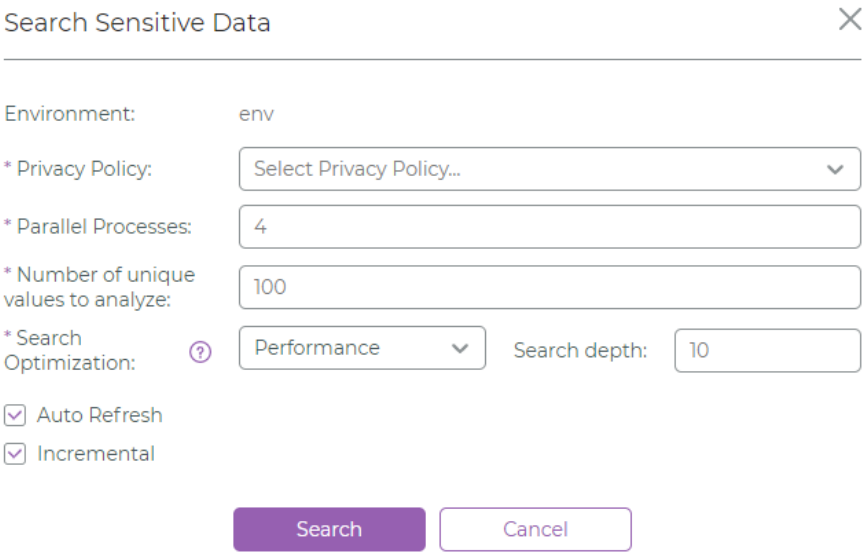
1. Select the required environment for searching for sensitive data.



2. Click **Scan**.



3. In the **Search Sensitive Data** window, configure the search parameters.



In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

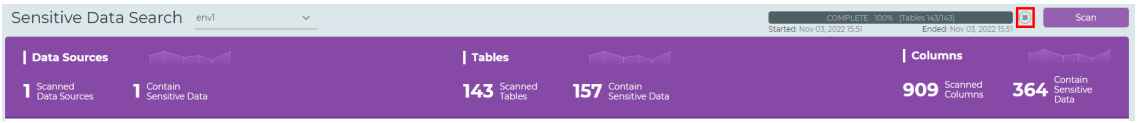
4. Select the **Auto Refresh** checkbox to have the system refresh automatically before doing a scan.
5. Select the **Incremental** checkbox to include columns that were found in a scan done before to be in the search results for this scan.

Columns that are not sensitive at this time are marked as deleted.

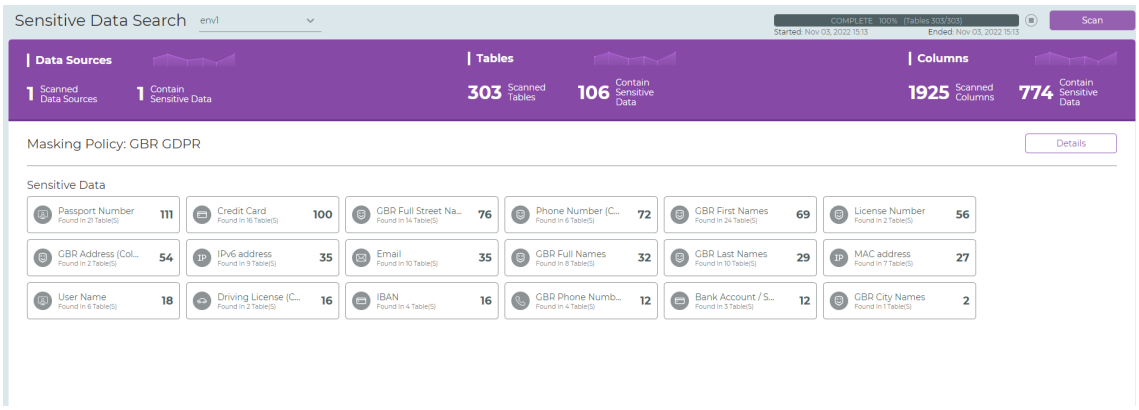
6. Click **Search**.

To stop the search:

1. Click (**Stop**).

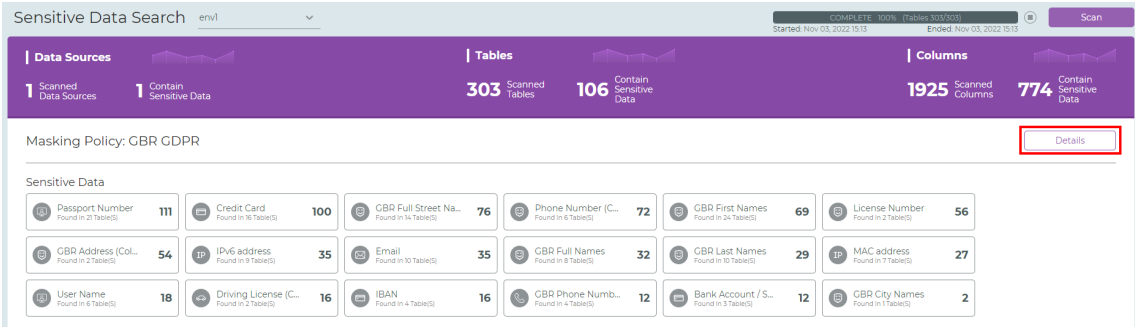


After the scan is complete, the scan summary appears.



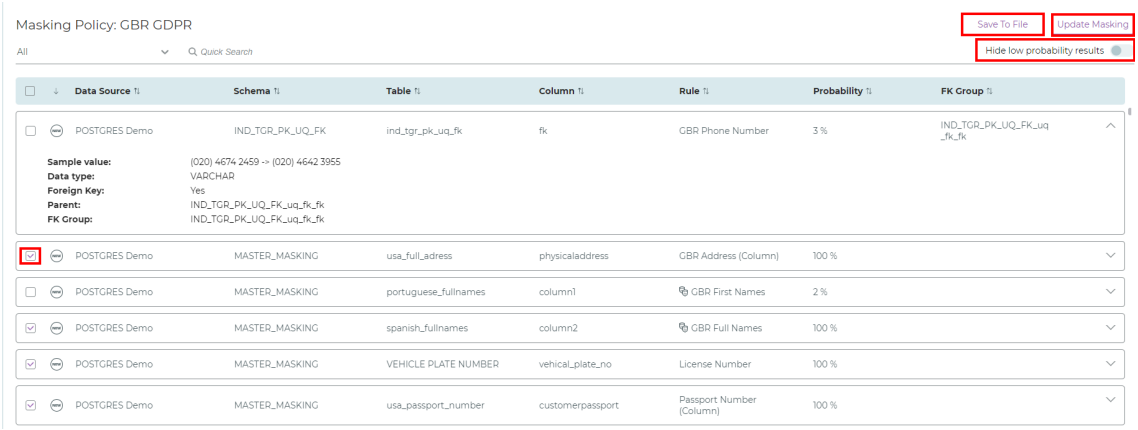
To see detailed scan results:

1. Click **Details**.



2. In the detailed window you can:

   - Click ⌄ to expand details.
   - Select/clear check boxes to update the search result.
   - Click **Save to File** to share the results via file.
   - Click **Hide low probability results** to view only the columns that get Probability higher than the sensitive search threshold.
   - Click **Update Masking** to update the masking configuration with the new search results and to go to the Masking Editor (see Section 8 - Masking Editor - Editing Masking Rules and Running Masking Operation).

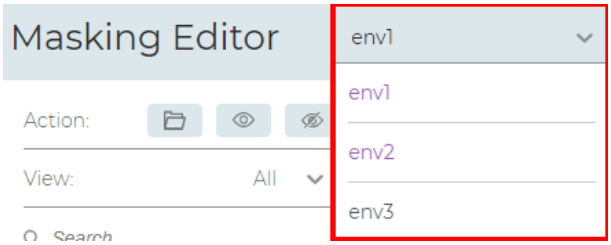


8. Masking Editor - Editing Masking Rules and Running Masking Operation

Use the masking editor to apply masking rules to columns in tables that you specify.

1. On the navigation bar, click  **(Masking Editor)**.

2. Select the required environment.



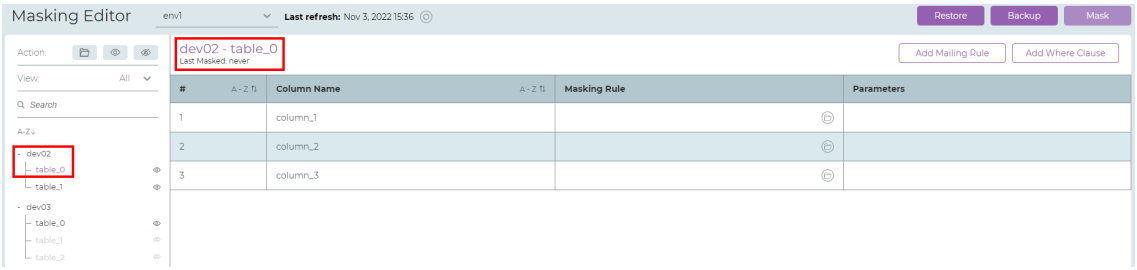
To filter the list of tables:

1. Select active or inactive.
2. Select:
   a. View all tables
   b. Active tables
   c. Inactive tables

You can also search for specific tables.

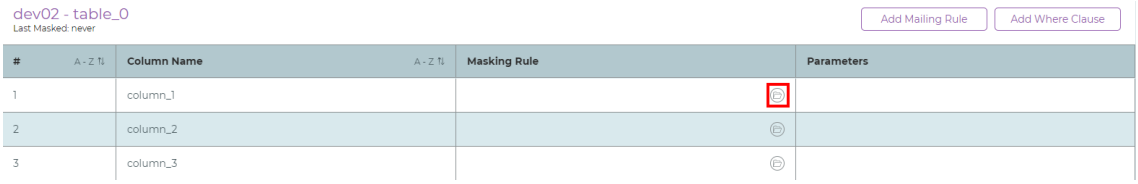
3. Select the required table for which you want to assign a masking rule.

4. The main panel displays the masking rules currently applied to the columns in the table selected.

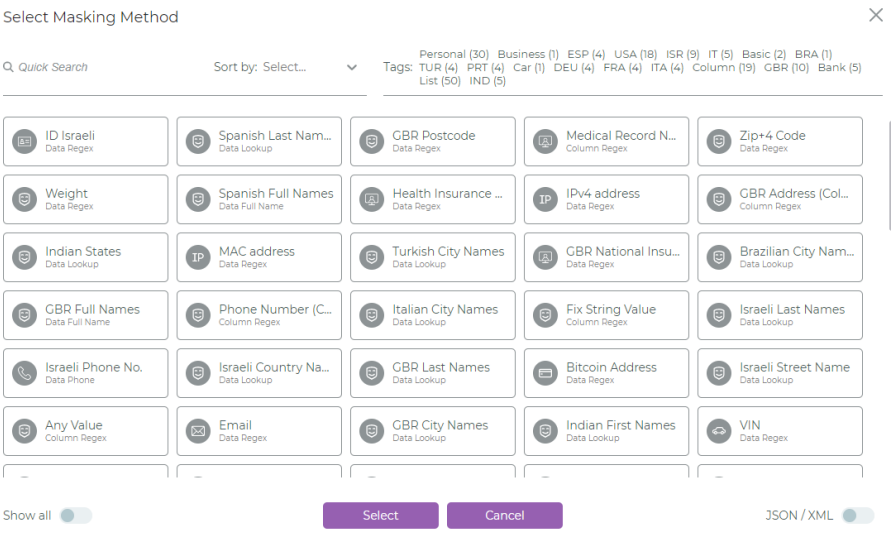


To select another/new masking rule:

1. For the required column, click  .

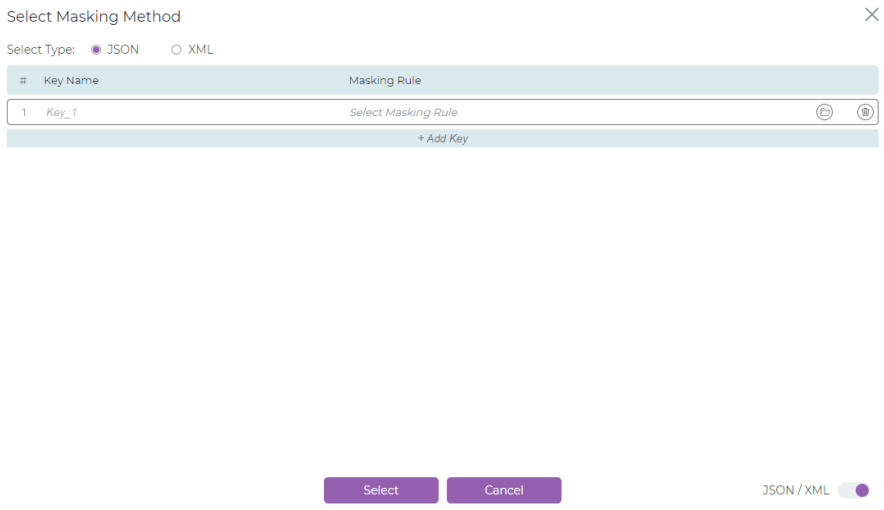


2. Click the required masking rule and click **Select**.



3. To assign a **Masking Rule** to each **Key Name** in the JSON/XML structure:

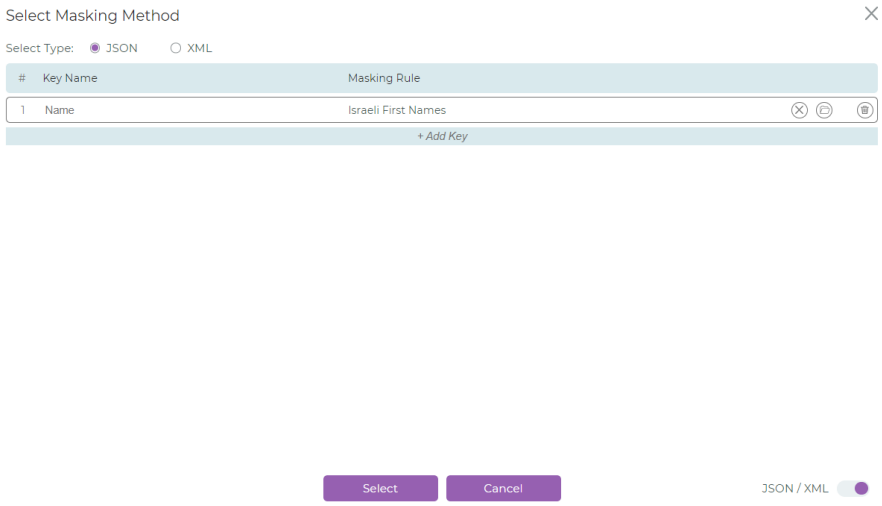
   a. Click JSON / XML .



   b. Enter the **Key Name**.

c. Click .

d. Select a **Masking Method**.



e. To add another key click *+ Add Key*.

4. Click **Select** to save the masking rule(s).

To remove a masking rule:

1. On the masking rule, click .

To remove a key:

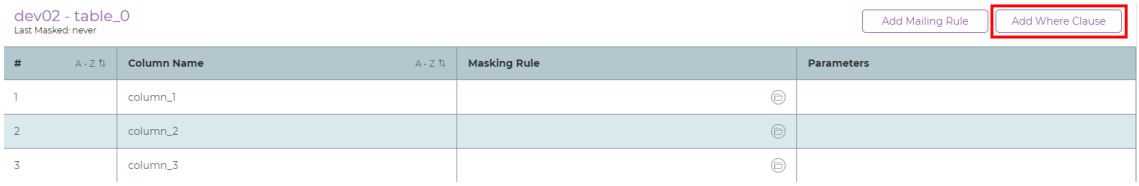
1. On the key, click .

To see all the masking methods:

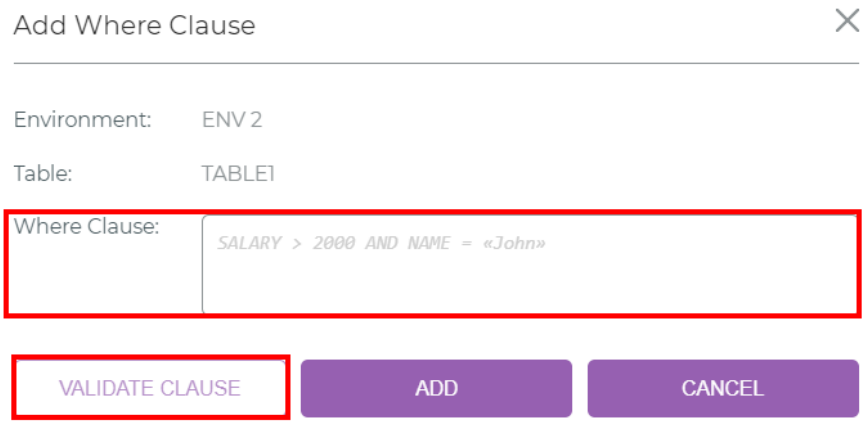
1. On the key, click Show all .

To add a Where Clause:

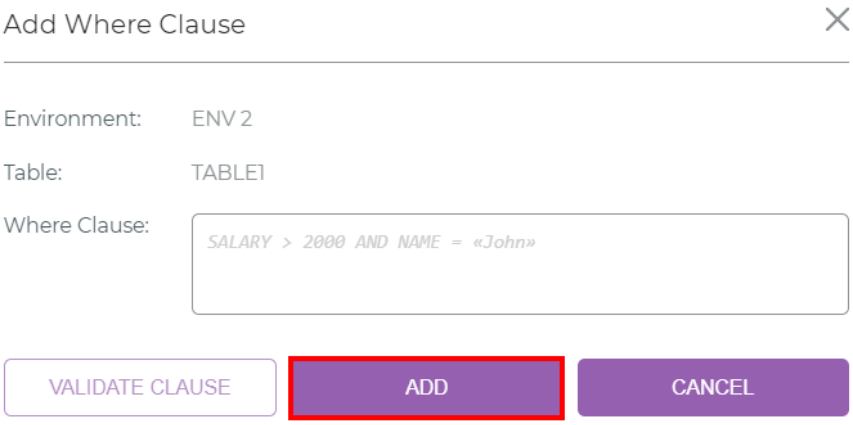
1. Click **Add Where Clause**.



2. Write the clause and click **VALIDATE CLAUSE**.



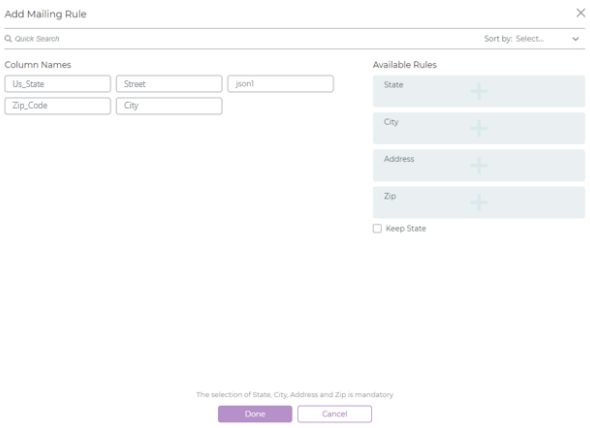
3. If the clause was validated, click **ADD**.



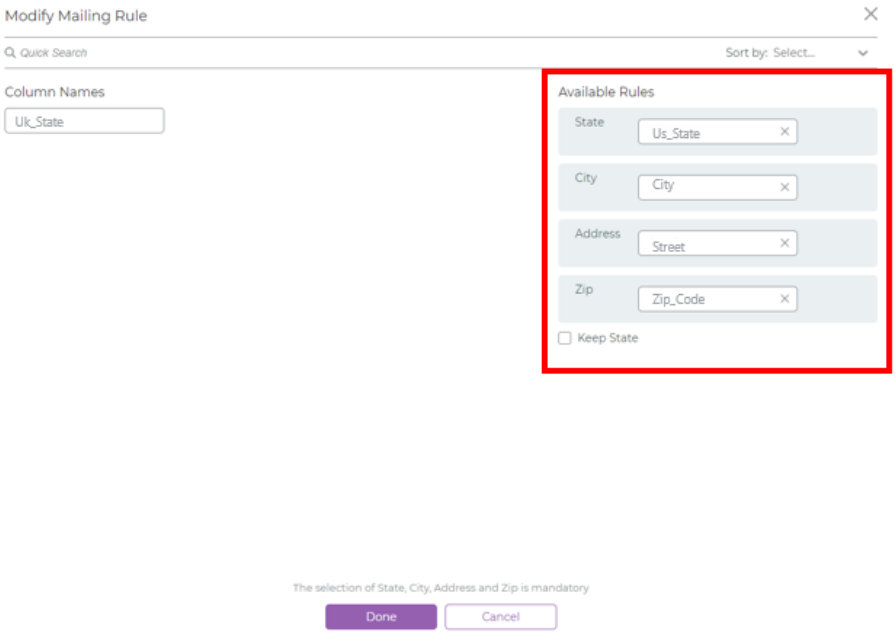
To add a Mailing Rule:

1. Click **Add Mailing Rule**.

The Add Mailing Rule window appears.



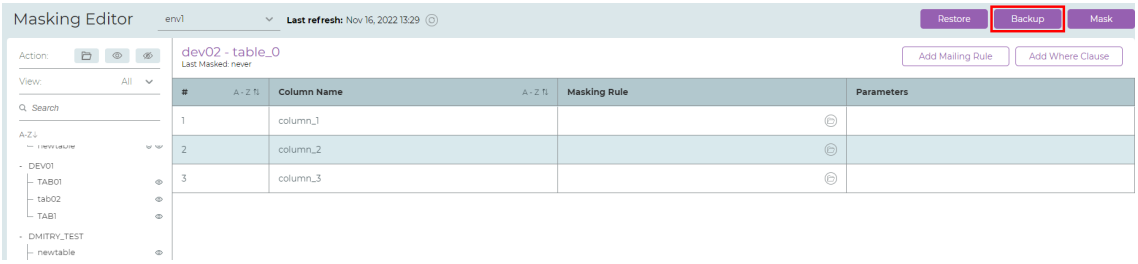
2. Drag the column to the **Available Rules**.



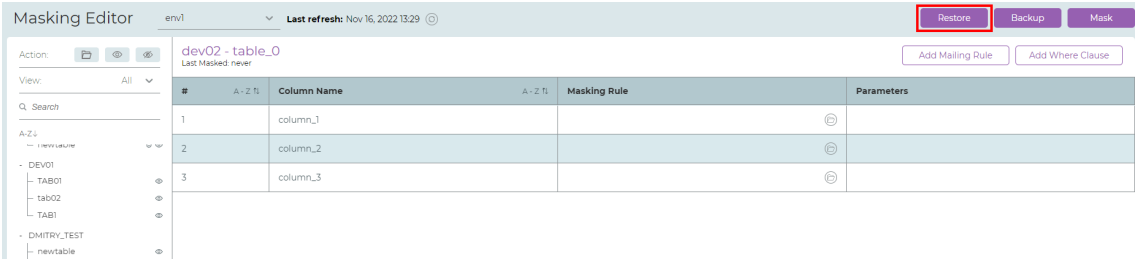
3. Select the Keep State check box to make sure that the state is not masked. and mask the other Available Rules.
4. Mask all the other available rules.
5. Click **Done**.

Restore and Backup:

1. Click **Backup** to save the masking settings to a JSON file.

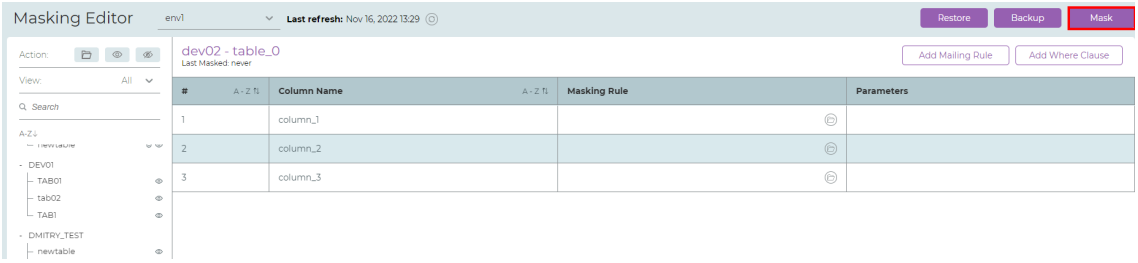


2. Click **Restore** to load masking settings from a backed up JSON file.

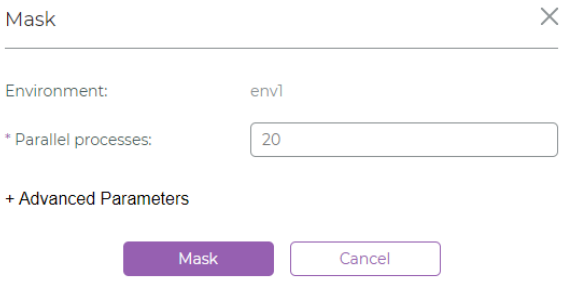


To mask the selected table:

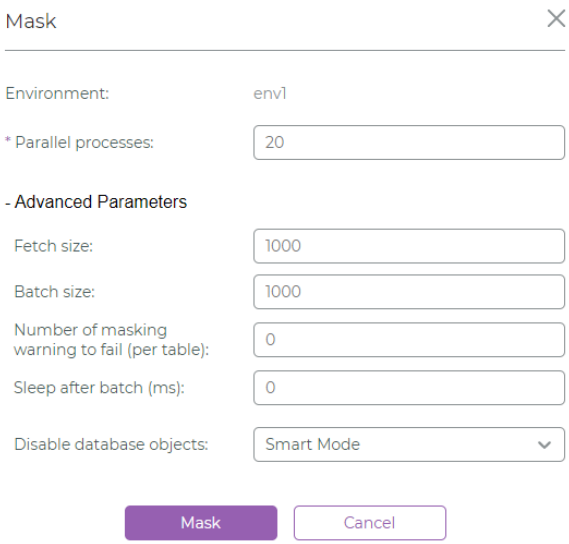
1. Click **Mask**.



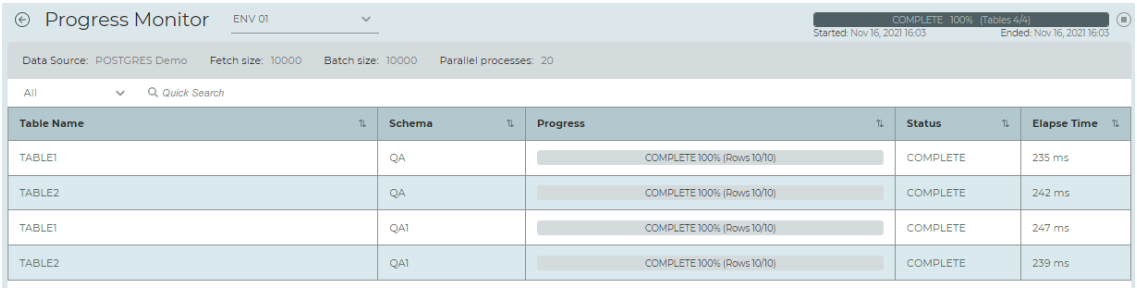
2. Fill in the masking details and click **Mask**.



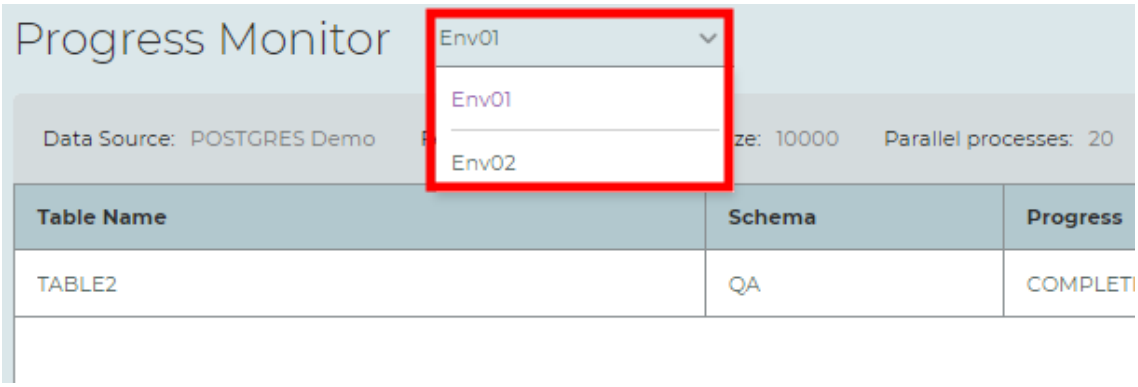
3. Enter **Advanced Parameters** if necessary.



4. Once masking is running, the **Progress Monitor** appears.



5. To see the progress in other environments click ⌄ and click the required environment.



9. Job Monitoring

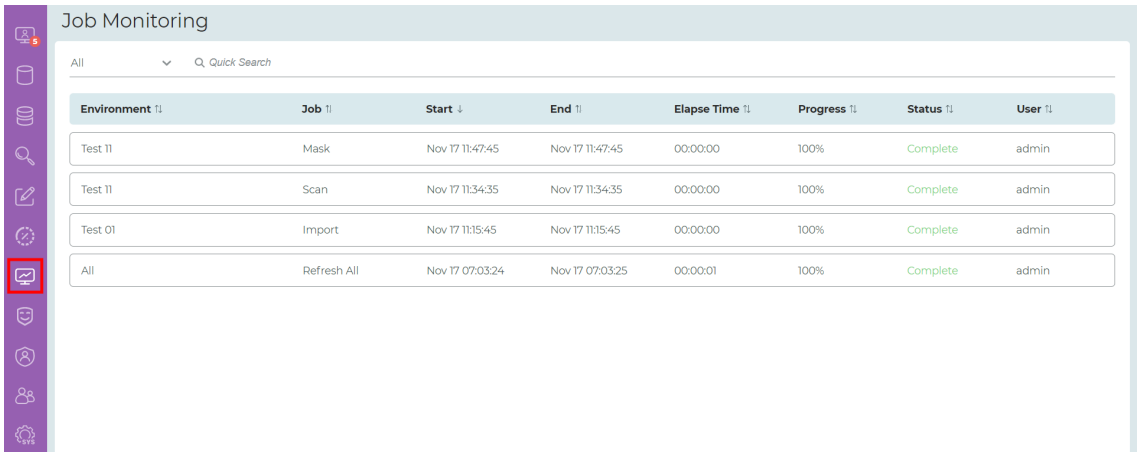
Job Monitoring is used to monitor the status of current system jobs. From the **Job Monitoring** window, you can:

- See system Jobs: Refresh, Refresh All, Scan, Scan All, and Mask.
- Drill down and see the detailed status of some of the system jobs.

Only a user with **Admin** privileges can access **Job Monitoring**.

To open the Job Monitoring window:

1. On the navigation bar, click **(Job Monitoring)**.

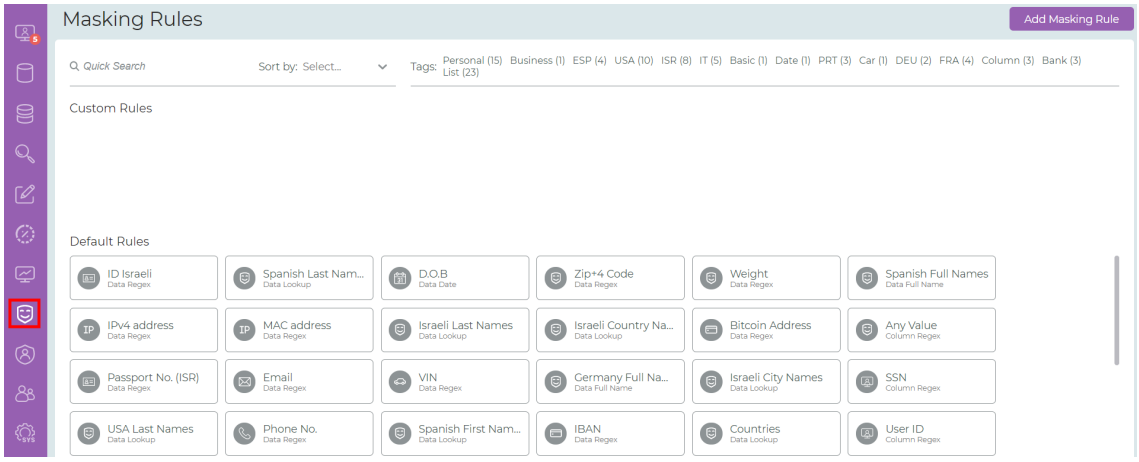


10. Managing Masking Rules

A **Masking Rule** contains both the scanning and masking methods used to search for and mask specific sensitive data (e.g. Name, Email, Credit Card, etc.).

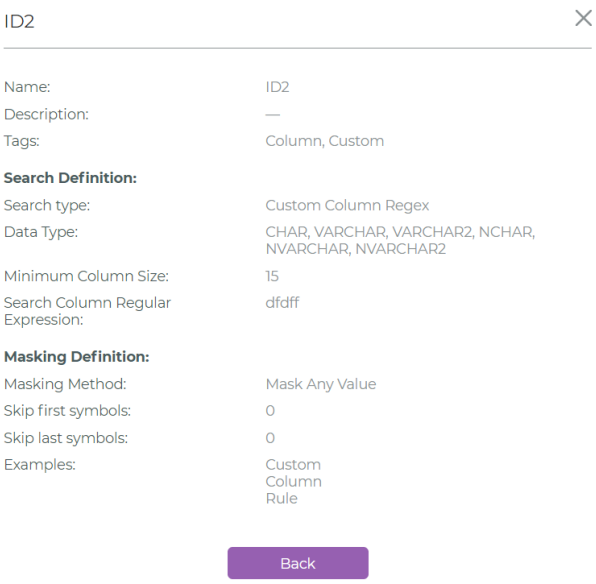
To see current masking rules:

1. On the navigation bar, click **(Masking Rules)**.



To see information about the masking rule:

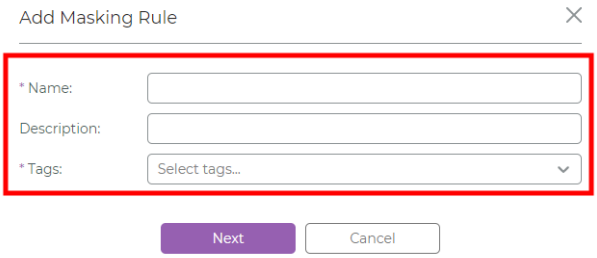
1. On the masking rule, click (i).



To add a new custom masking rule:

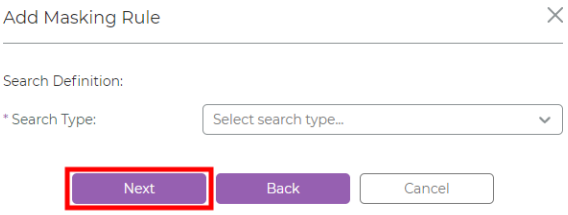
1. Click **ADD MASKING RULE**.

2. Provide a name and description for the new rule and select the required **Tags**.

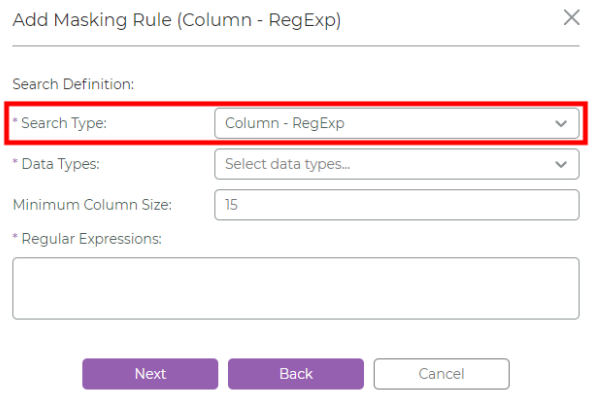


In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

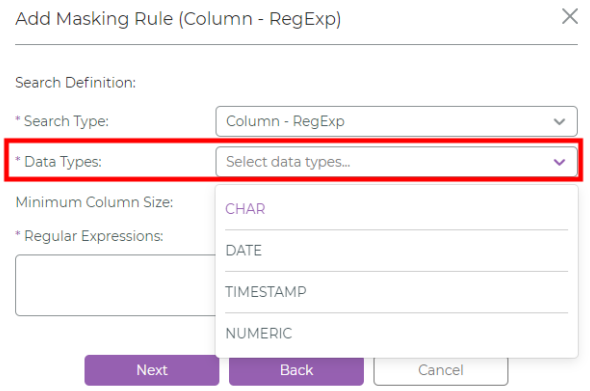
3. Click **NEXT**.



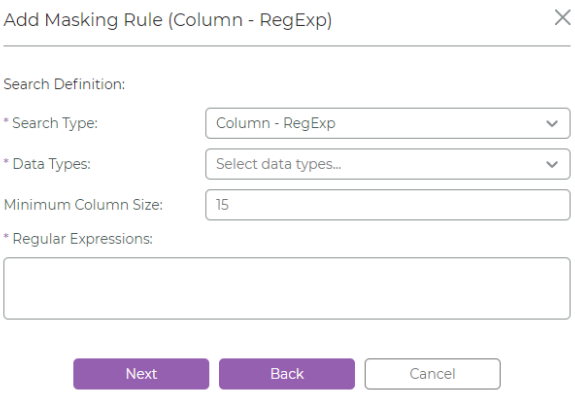
4. Select a **Search Type**:
   a. **Column - RegExp** to search the column name using a regular expression.
   b. **Data - RegExp** to search the column data using a regular expression.
   c. **Data - Lookup** to search the column data using a lookup table.



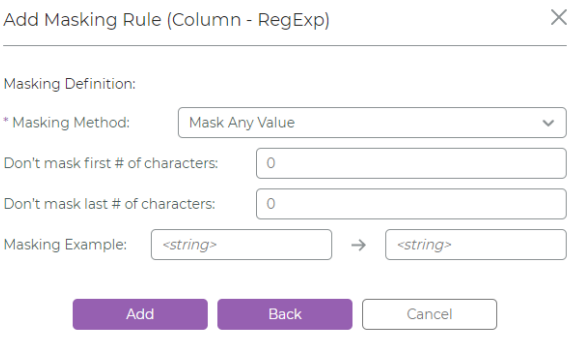
5. Select a **Data Types**:
   a. CHAR
   b. DATE
   c. TIMESTAMP
   d. NUMERIC



6. Click **NEXT**.
7. To configure the masking rule parameters for a **Column - RegExp** search type:
   a. For a **Search Definition**, provide the **Column Regular Expressions**.



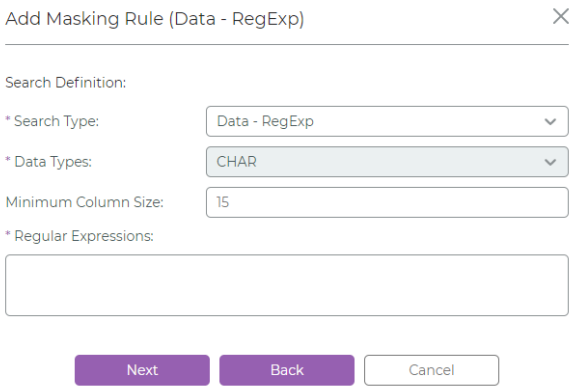
   b. Click **NEXT**.
   c. For a **Masking Definition**, if necessary provide the number of a characters to skip at the start or end.



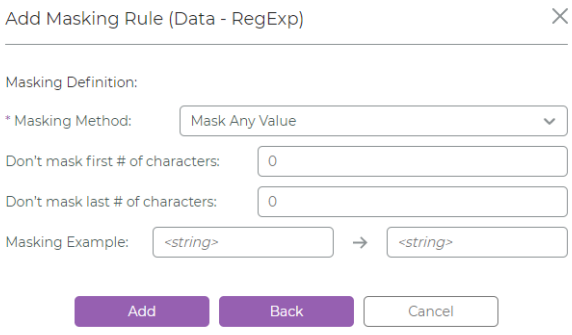
   d. Click **ADD**.

The new masking rule appears.

8. To configure the masking rule parameters for a **Data - RegExp** Search Type:
   a. For a **Search Definition**, provide the **Data Regular Expressions**.



   b. Click **NEXT**.
   c. For a **Masking Definition**, if necessary provide the number of a characters to skip at the start or end.

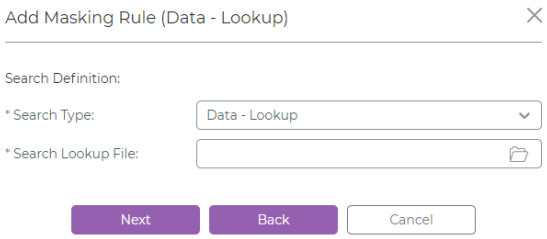


   d. Click **ADD**.

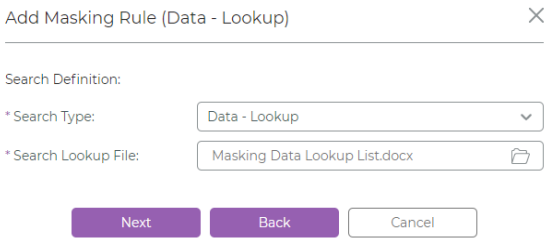
The new masking rule appears.

9. To configure the masking rule parameters for a **Data - Lookup** Search Type:

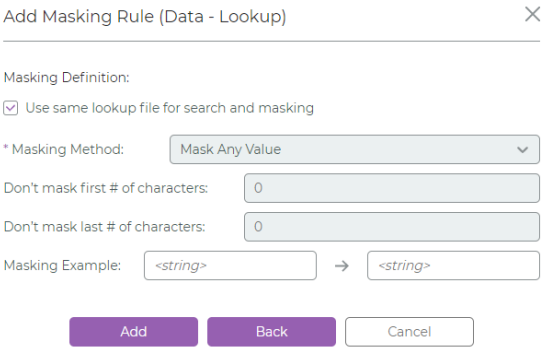
   a. For a **Search Definition**, browse to the location for the **Masking Lookup List** and click **Open**.



   b. After the file is loaded, click **Next**.



   c. For a **Masking Definition**, if necessary provide the number of a characters to skip at the start or end.

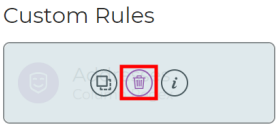


   d. Click **ADD**.

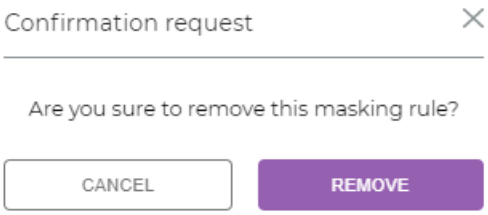
The new masking rule appears.

To delete a custom masking rule:

1. On the masking rule, click  .

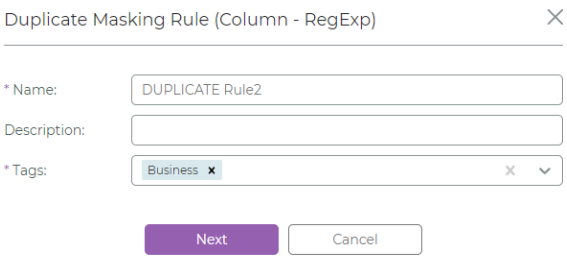


2. Click **REMOVE** to confirm the deletion, or **CANCEL** to exit without deleting the masking rule.

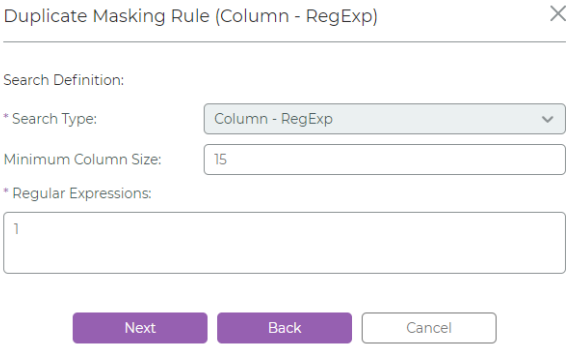


To duplicate a masking rule:

1. On the masking rule, click  .
2. Provide a name.

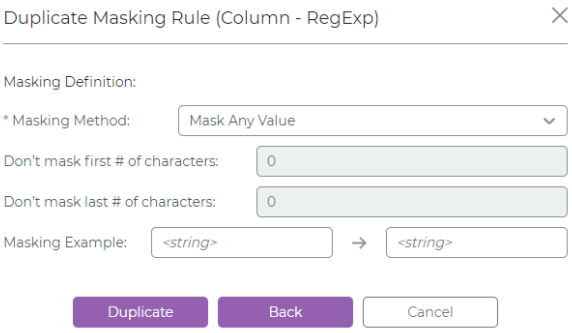


3. Click **NEXT**.
4. Provide **Data Regular Expression(s)**.



You can also modify the **Minimum Column Size**.

5. Click **NEXT**.



6. Click **Duplicate**.

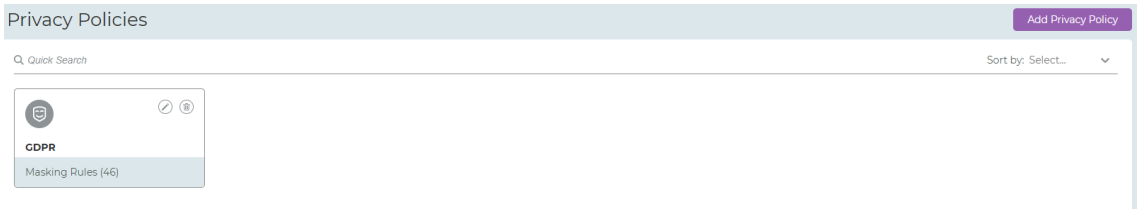
11. Managing Privacy Policies

A **Privacy Policy** is a set of masking rules used to scan and mask following a specified privacy regulation such as GDPR, CCPA and HIPAA or to the organization privacy rules. This section describes how to define and manage the privacy policies.

To view available privacy policies:

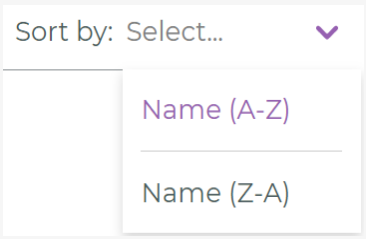
1. On the navigation bar, click  **(Privacy Policies)**.

2. The **Privacy Policies** window appears displaying all privacy policies that have been added to the system.



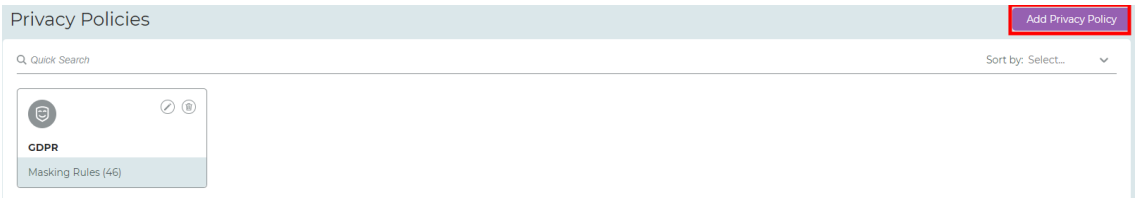
You can quickly locate content by typing its letters on the **Quick Search** bar. The list updates promptly.

You can display the list in ascending or descending alphabetical order.

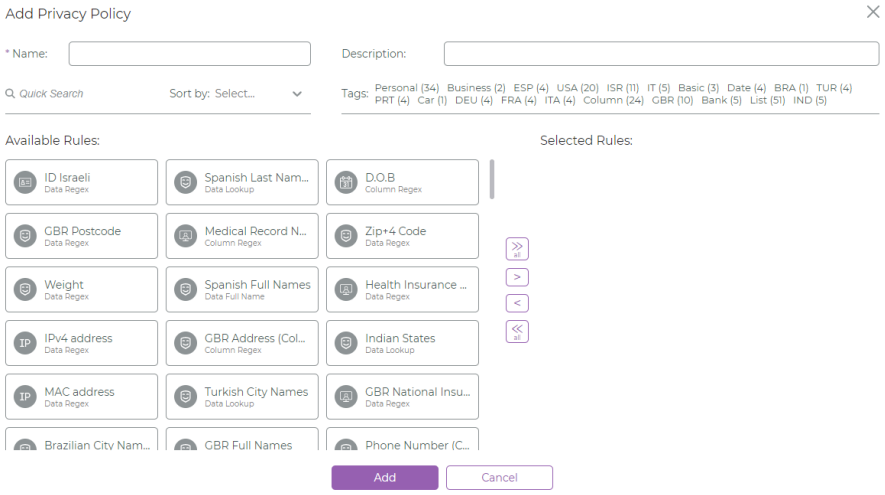


To add a new privacy policy:

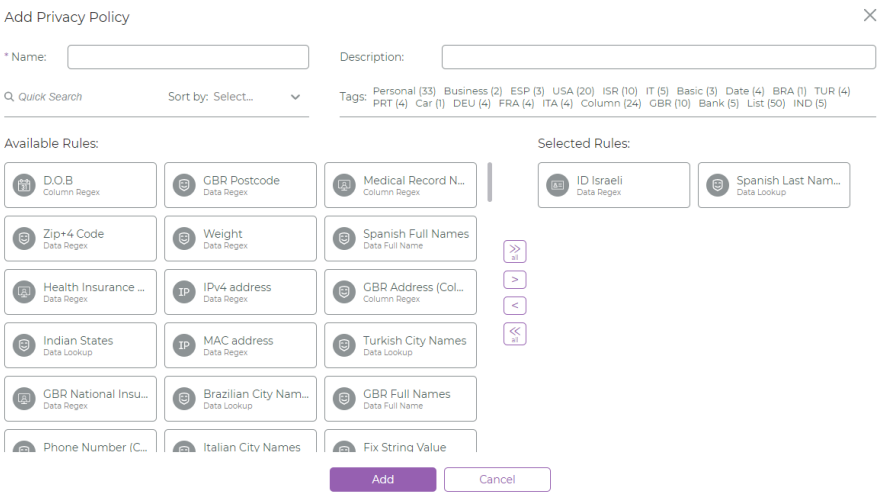
1. Click **Add Privacy Policy**.



2. Fill in the policy details:
   a. In **Name**, provide a name.
   b. Under **Available Rules**, select a rule or a number of rules.



3. Click > to add the rule to the **Selected Rules** list.



4. Click **Add**.

> To add all the available rules, click all.

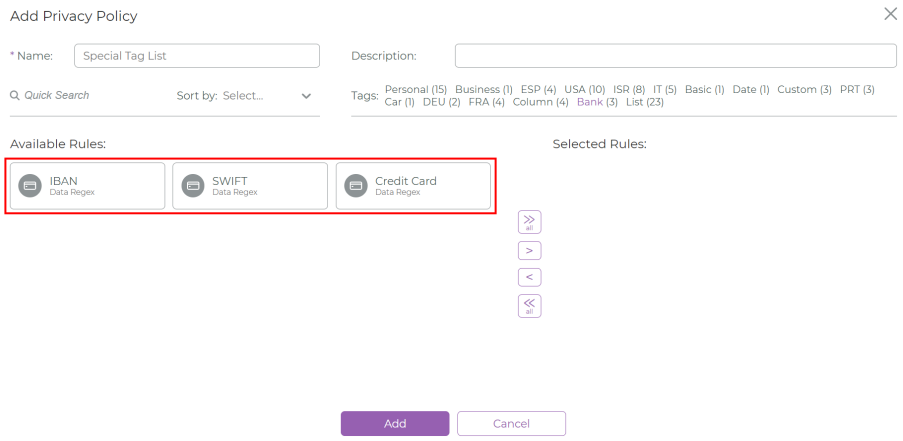
> To remove all the available rules, click all.

> To remove one available rule, select the rule, and click <.

To add a masking rule according to a Tag:

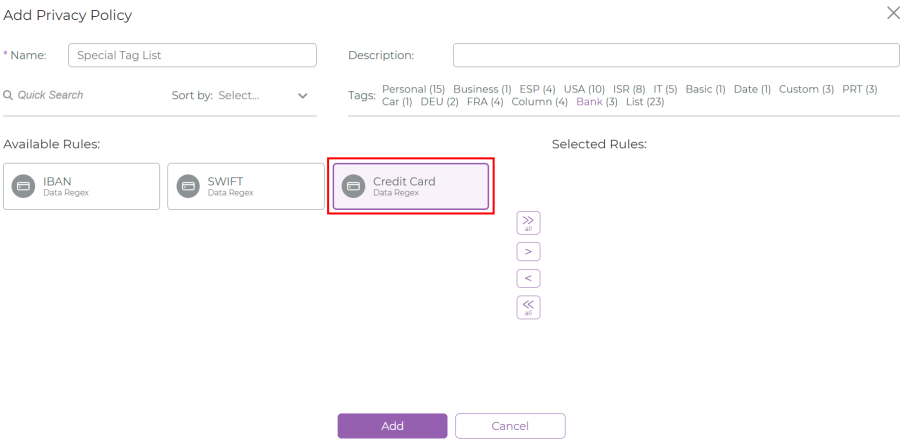
1. Click a Tag (in this example **Bank**).

2. All the masking rules that contain the tag selected are shown in the **Available Rules** list.



3. Select a rule.

4. Click **>** to add the rule to the **Selected Rules** list.



5. Click **Add**.

- To add all the available rules, click .
- To remove all the available rules, click .
- To remove one available rule, select the rule, and click .

1. To remove a Tag from the masking rules in the **Available Rules** list, click on the tag again, (in this example **Bank**).

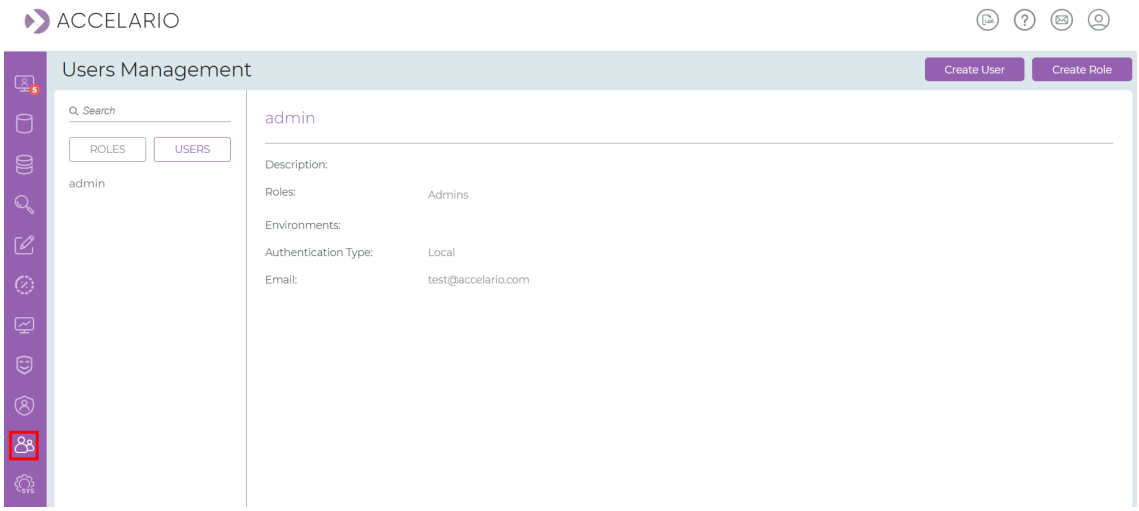
12. Managing Users and Roles

Only a user with **Admin** privileges can create or modify users and roles.

A default user **admin** with the role **Admins** exists when the system is first installed.

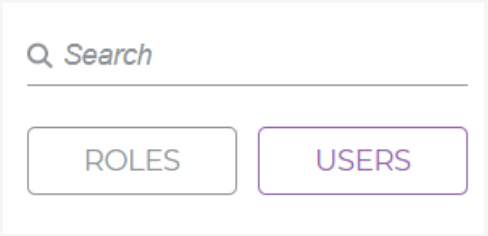
To manage users:

1. On the navigation bar, click (**Users Management**).



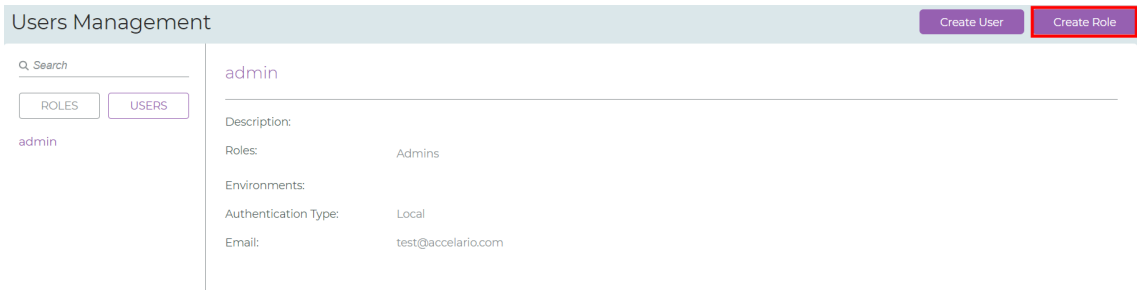
You can quickly locate a user by typing its letters on the **Search** bar. The list updates promptly.

You can display the list based on **ROLES** or **USERS**.

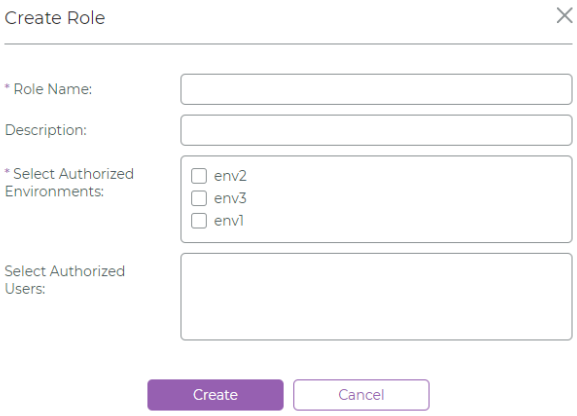


To create a new role:

1. Click **Create Role**.



2. Fill in the details:

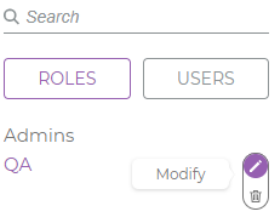


In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

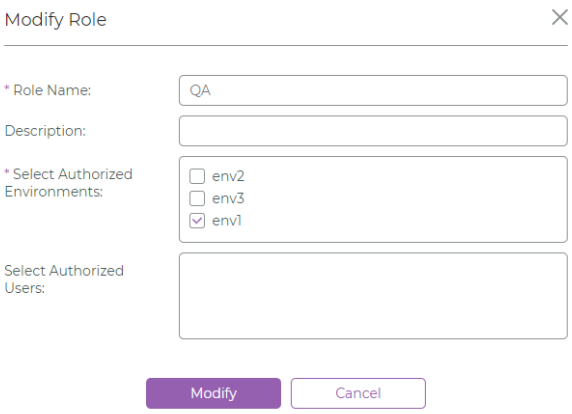
3. Click **Create**.

To edit role details:

1. On the required role, click **(Modify)**.



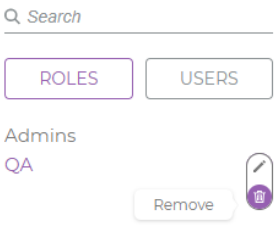
2. The **Modify Role** window appears. Modify the role details as required.



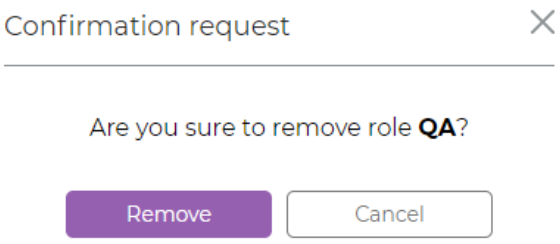
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

To delete a role:

1. On the required role, click (Remove).

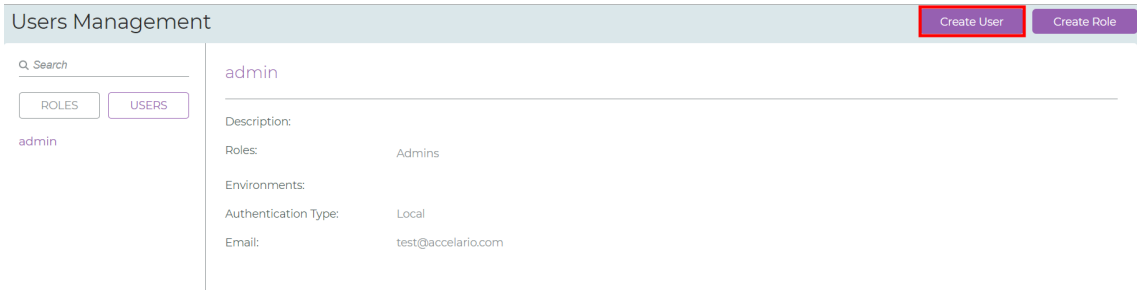


2. Click **Remove** to confirm the deletion, or **Cancel** to exit without deleting the role.

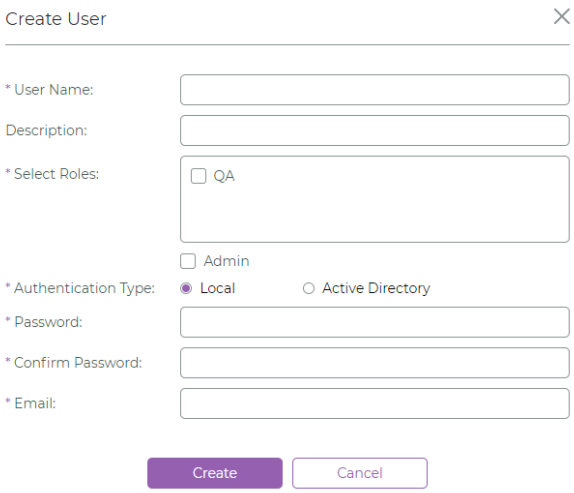


To add a new user:

1. Click **Create User**.



2. Fill in the details:

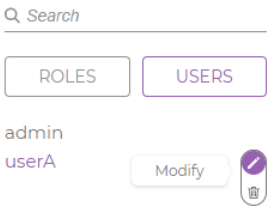


In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

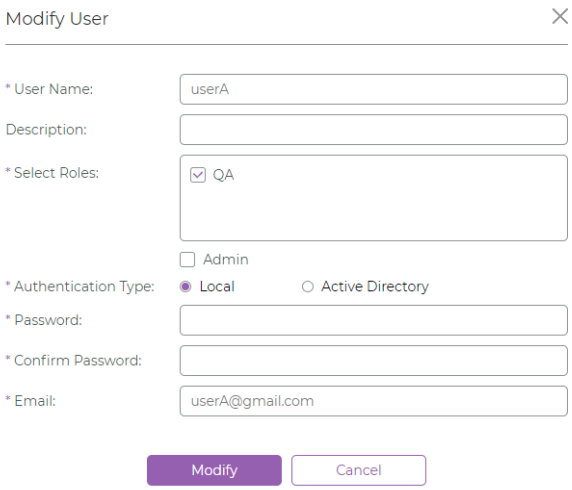
3. Click **Create**.

To edit user details:

1. On the required role, click **(Modify)**.



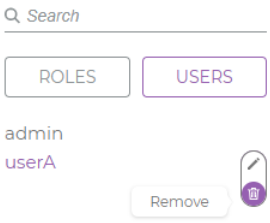
2. The **Modify User** window appears. Modify the user details as required.



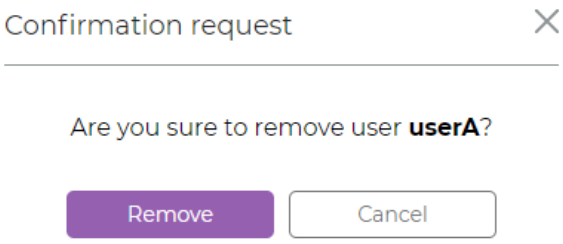
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

To delete a user:

1. On the required role, click (Remove).



2. Click **Remove** to confirm the deletion, or **Cancel** to exit without deleting the role.



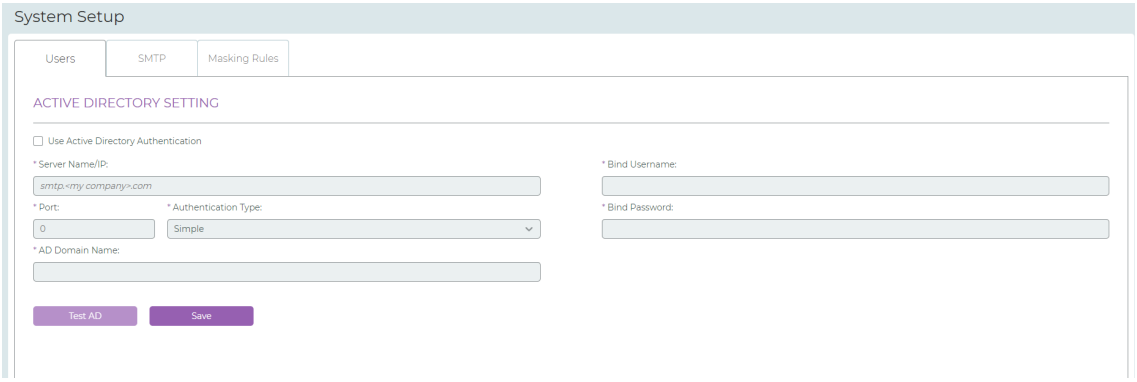
13. System Setup

The **System Setup** is used to define different system setups. In this version it is used to setup the Active Directory, SMTP parameters, and to load new masking rules.

Only a user with **Admin** privileges can access the **System Setup**.

To setup the active directory:

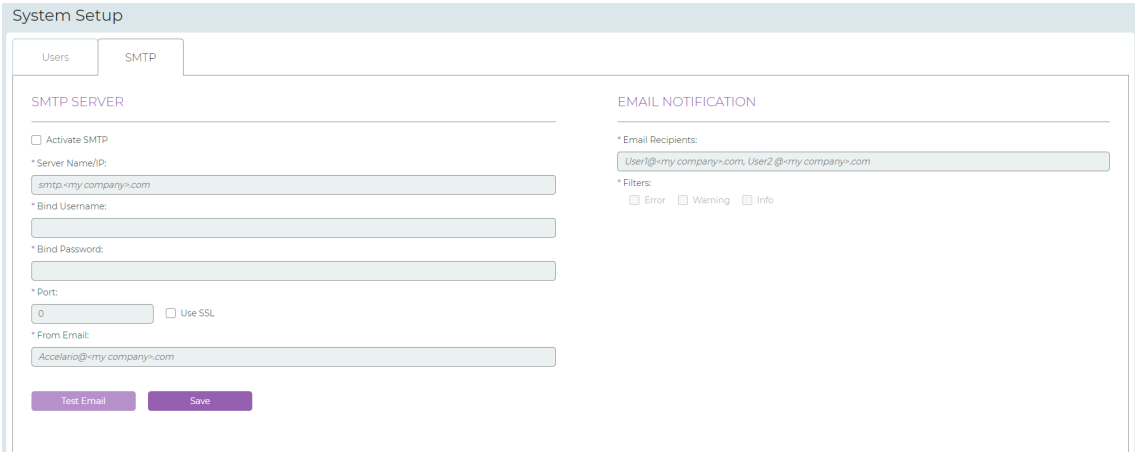
1. Click **Users**.
2. Fill in the details to setup the Active Directory.



3. Click **Test AD** to verify that the active directory settings are correct.
4. Click **Save**.

To setup the SMTP server:

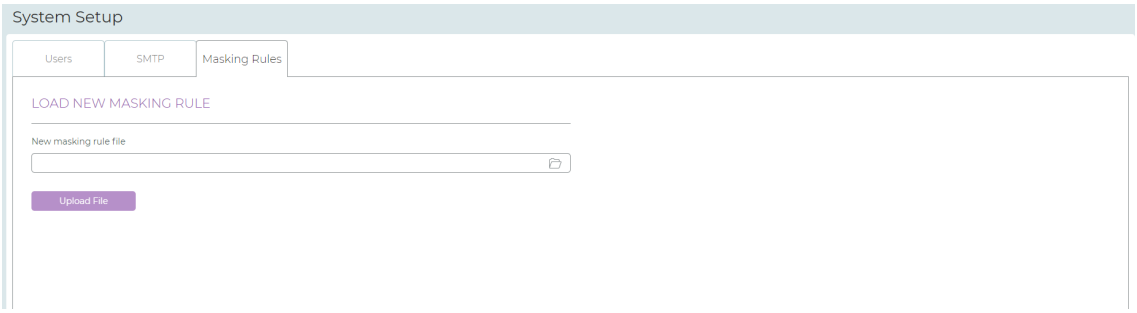
1. Click **STMP**.
2. Fill in the details to setup the STMP sever.



3. Click **Test Email** to verify that the STMP server settings are correct.
4. Click **Save**.

To install new built-in masking rules online:

1. Click **Masking Rules**.



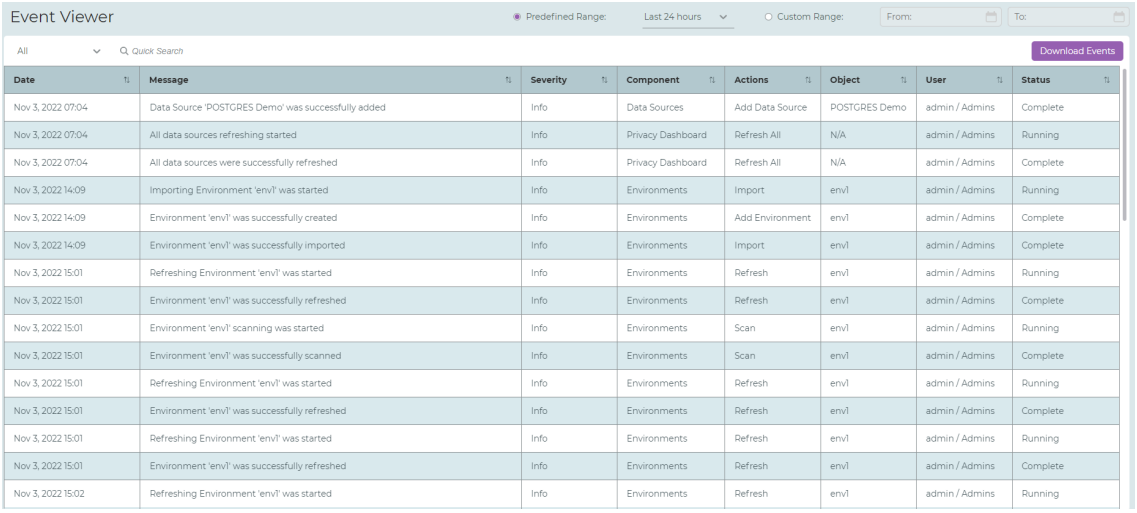
2. Click 🗁 .
3. Select file.
4. Click Upload File.

14. Event Viewer

The Event Viewer is used to see, filter, and search user events. In the Event Viewer you can drill down and see details for events. You can: also save all user events to a file. This section describes how to do these tasks.

To open the Event Viewer work area:

1. On the navigation bar, click  (Event Viewer).



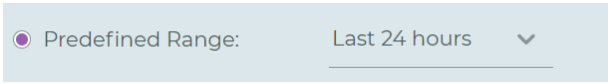
Date	Message	Severity	Component	Actions	Object	User	Status
Nov 3, 2022 07:04	Data Source 'POSTGRES Demo' was successfully added	Info	Data Sources	Add Data Source	POSTGRES Demo	admin / Admins	Complete
Nov 3, 2022 07:04	All data sources refreshing started	Info	Privacy Dashboard	Refresh All	N/A	admin / Admins	Running
Nov 3, 2022 07:04	All data sources were successfully refreshed	Info	Privacy Dashboard	Refresh All	N/A	admin / Admins	Complete
Nov 3, 2022 14:09	Importing Environment 'env1' was started	Info	Environments	Import	env1	admin / Admins	Running
Nov 3, 2022 14:09	Environment 'env1' was successfully created	Info	Environments	Add Environment	env1	admin / Admins	Complete
Nov 3, 2022 14:09	Environment 'env1' was successfully imported	Info	Environments	Import	env1	admin / Admins	Complete
Nov 3, 2022 15:01	Refreshing Environment 'env1' was started	Info	Environments	Refresh	env1	admin / Admins	Running
Nov 3, 2022 15:01	Environment 'env1' was successfully refreshed	Info	Environments	Refresh	env1	admin / Admins	Complete
Nov 3, 2022 15:01	Environment 'env1' scanning was started	Info	Environments	Scan	env1	admin / Admins	Running
Nov 3, 2022 15:01	Environment 'env1' was successfully scanned	Info	Environments	Scan	env1	admin / Admins	Complete
Nov 3, 2022 15:01	Refreshing Environment 'env1' was started	Info	Environments	Refresh	env1	admin / Admins	Running
Nov 3, 2022 15:01	Environment 'env1' was successfully refreshed	Info	Environments	Refresh	env1	admin / Admins	Complete
Nov 3, 2022 15:01	Refreshing Environment 'env1' was started	Info	Environments	Refresh	env1	admin / Admins	Running
Nov 3, 2022 15:01	Environment 'env1' was successfully refreshed	Info	Environments	Refresh	env1	admin / Admins	Complete
Nov 3, 2022 15:02	Refreshing Environment 'env1' was started	Info	Environments	Refresh	env1	admin / Admins	Running

To quick search events with a keyword:

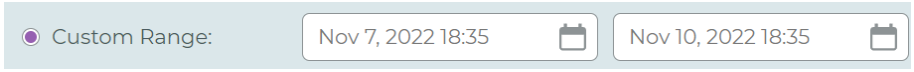
1. Type a keyword in the  bar.

To filter events for a specified time period:

1. Select:
   a. **Predefined Range**.



   or
   b. Enter a **Custom Range**.



To sort events:

1. Select:
   a. A column heading.
   b. Select the sort order ⇅.

To download events to a file:

1. Click Download Events.