ACCELARIO

Accelario Data Masking Module

User Guide V21.0

February 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, CCPAV, PCI, HIPAA.
- 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/collection, and column/key.

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 a data source schema
- 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, CCPA, PCI, HIPAA.
- Masking rules are automatically assigned to the correct sensitive column(s)/key(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/keys that were found.
- Select the sensitive column/key 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/key.
- Add a **Where Clause** to a table for masking.
- Add a **Mailing Rule** to mask an address that is used in more than one columns in one table for a valid address.
- Perform **Backup** / **Restore** of a masking configuration file.
- Execute and monitor a Mask operation in the **Progress Monitor** window.
- 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 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, HIPPA, PCI or a set of organizational specific privacy rules. From the **Privacy Policies** window, you can:

- Add a new privacy policy.
- View, modify, and duplicate a privacy policy.

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
- Install new built-in masking rules online

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

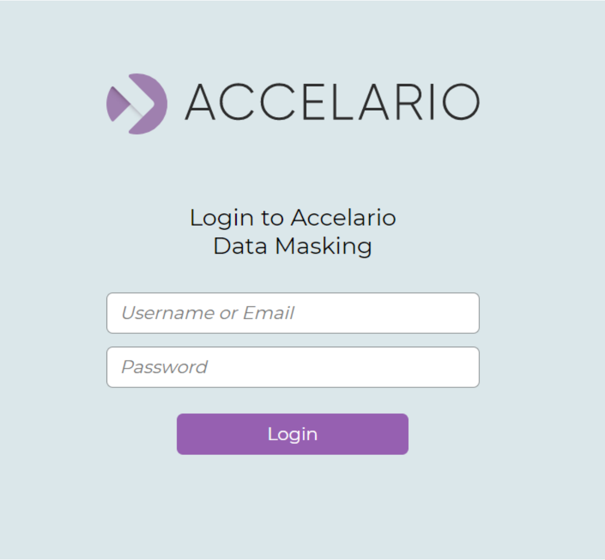
For more information, see Event Viewer.

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.

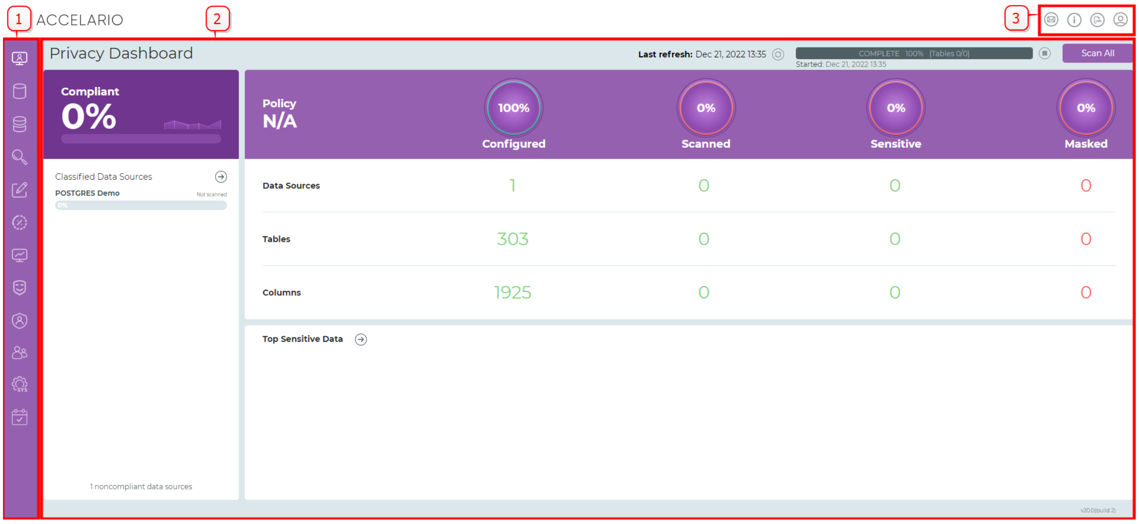
1. Enter your **Username** or **Email**.
2. Enter your **Password**.
3. Click **Login**.



Login to Accelario
Data Masking

3. Getting to Know the GUI

The following image and table describe the Data Masking Module.



Last refresh: Dec 21, 2022 13:35

COMPLETE 100% (Tables 0/0)

Started: Dec 21, 2022 13:35

	Configured	Scanned	Sensitive	Masked
Data Sources	1	0	0	0
Tables	303	0	0	0
Columns	1925	0	0	0

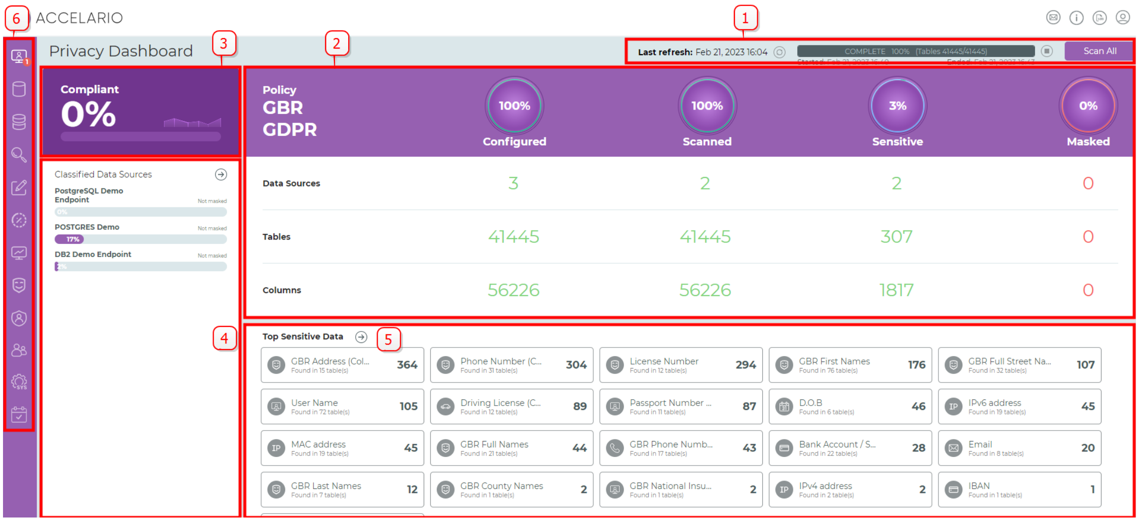
1 noncompliant data sources

#	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**.



Privacy Dashboard

Last refresh: Feb 21, 2023 16:04 COMPLETE 100% (Tables 41445/41445) Scan All

Compliant 0%

Classified Data Sources
- PostgreSQL Demo Endpoint — Not masked — 0%
- POSTGRES Demo — Not masked — 17%
- DB2 Demo Endpoint — Not masked — 2%

Policy GBR GDPR

	100% Configured	100% Scanned	3% Sensitive	0% Masked
Data Sources	3	2	2	0
Tables	41445	41445	307	0
Columns	56226	56226	1817	0

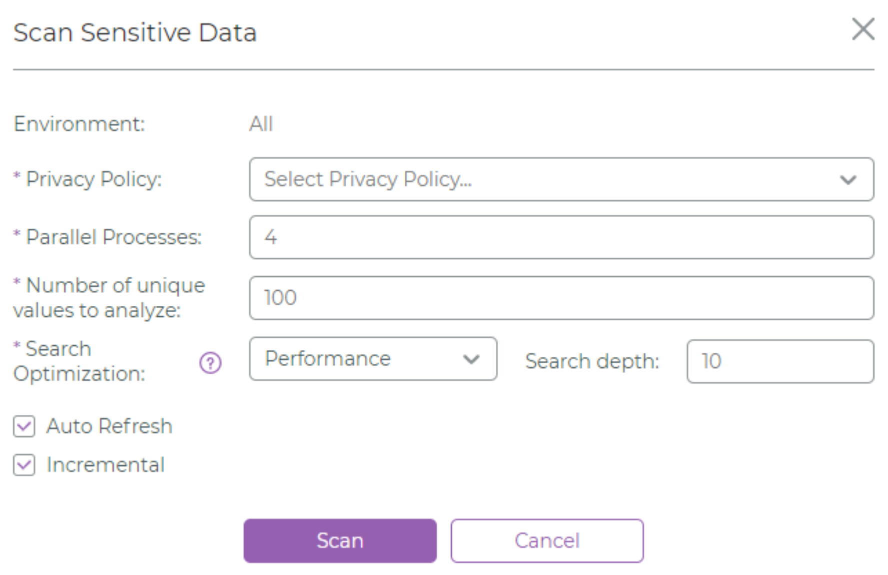
Top Sensitive Data

GBR Address (Col...	Found in 15 table(s)	364
Phone Number (C...	Found in 31 table(s)	304
License Number	Found in 12 table(s)	294
GBR First Names	Found in 76 table(s)	176
GBR Full Street Na...	Found in 32 table(s)	107
User Name	Found in 72 table(s)	105
Driving License (C...	Found in 12 table(s)	89
Passport Number ...	Found in 11 table(s)	87
D.O.B	Found in 6 table(s)	46
IPv6 address	Found in 19 table(s)	45
MAC address	Found in 19 table(s)	45
GBR Full Names	Found in 21 table(s)	44
GBR Phone Numb...	Found in 17 table(s)	43
Bank Account / S...	Found in 22 table(s)	28
Email	Found in 8 table(s)	20
GBR Last Names	Found in 7 table(s)	12
GBR County Names	Found in 1 table(s)	2
GBR National Insu...	Found in 1 table(s)	2
IPv4 address	Found in 2 table(s)	2
IBAN	Found in 1 table(s)	1

#	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**.



Scan Sensitive Data

Environment: All

* Privacy Policy: Select Privacy Policy...

* Parallel Processes: 4

* Number of unique values to analyze: 100

* Search Optimization: Performance Search depth: 10

☑ Auto Refresh

☑ Incremental

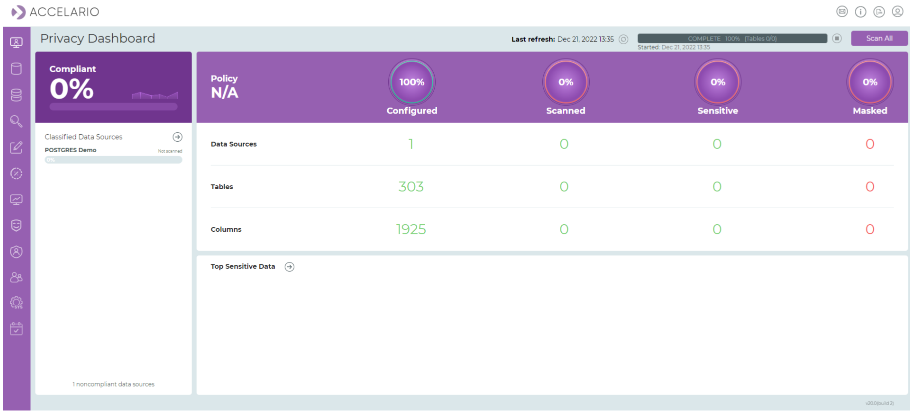
In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

To stop a scan:

1. Click ⏹.

To do a Refresh All:

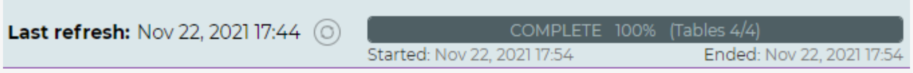
1. Click **Start refresh environments** .
2. All results from the previous scan is removed.



Last refresh: Dec 21, 2022 13:35 COMPLETE 100% (Tables 0/0)
Started: Dec 21, 2022 13:35

Policy N/A	100% Configured	0% Scanned	0% Sensitive	0% Masked
Data Sources	1	0	0	0
Tables	303	0	0	0
Columns	1925	0	0	0

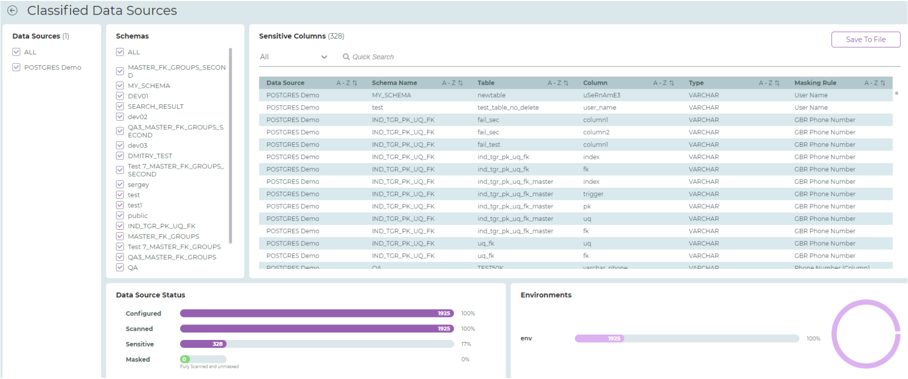
On the scan bar, you can see the following scan information:



Last refresh: Nov 22, 2021 17:44 COMPLETE 100% (Tables 4/4)
Started: Nov 22, 2021 17:54 Ended: Nov 22, 2021 17:54

To see the potential classified data sources:

1. Click Classified Data Sources ➔ .



Classified Data Sources

Data Sources (1)

☑ ALL

☑ POSTGRES Demo

Schemas

☑ ALL
☑ MASTER_FK_GROUPS_SECOND
☑ MY_SCHEMA
☑ DEV01
☑ SEARCH_RESULT
☑ dev02
☑ QA3_MASTER_FK_GROUPS_SECOND
☑ dev03
☑ DMITRY_TEST
☑ Test 7_MASTER_FK_GROUPS_SECOND
☑ sergey
☑ test
☑ test1
☑ public
☑ IND_TGR_PK_UQ_FK
☑ MASTER_FK_GROUPS
☑ Test 7_MASTER_FK_GROUPS
☑ QA3_MASTER_FK_GROUPS
☑ QA

Sensitive Columns (328)

All

Quick Search

Save To File

Data Source	Schema Name	Table	Column	Type	Masking Rule
POSTGRES Demo	MY_SCHEMA	newtable	uSeRnAmE3	VARCHAR	User Name
POSTGRES Demo	test	test_table_no_delete	user_name	VARCHAR	User Name
POSTGRES Demo	IND_TGR_PK_UQ_FK	fail_sec	column1	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	fail_sec	column2	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	fail_test	column1	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk	index	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk	fk	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk_master	index	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk_master	trigger	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk_master	pk	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk_master	uq	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk_master	fk	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	uq_fk	uq	VARCHAR	GBR Phone Number
POSTGRES Demo	IND_TGR_PK_UQ_FK	uq_fk	fk	VARCHAR	GBR Phone Number
POSTGRES Demo	QA	TEST50K	varchar_phone	VARCHAR	Phone Number (Column)

Data Source Status

Configured	1925	100%
Scanned	1925	100%
Sensitive	328	17%
Masked	0 Fully Scanned and unmasked	0%

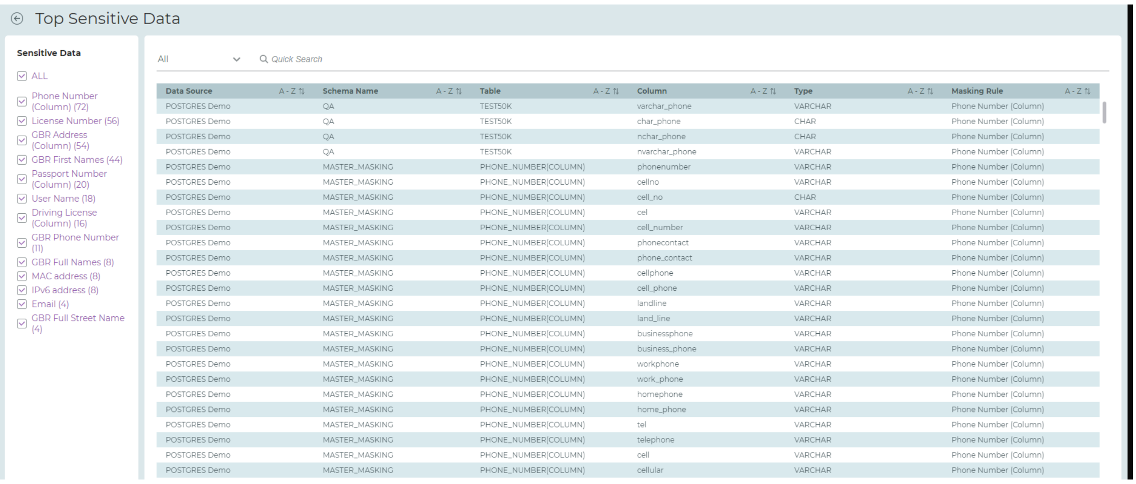
Environments

env	1925	100%

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

To see top sensitive data:

1. Click **Top Sensitive Data** ➔ .



Top Sensitive Data

Sensitive Data

☑ ALL
☑ Phone Number (Column) (72)
☑ License Number (56)
☑ GBR Address (Column) (54)
☑ GBR First Names (44)
☑ Passport Number (Column) (20)
☑ User Name (18)
☑ Driving License (Column) (16)
☑ GBR Phone Number (11)
☑ GBR Full Names (8)
☑ MAC address (8)
☑ IPv6 address (8)
☑ Email (4)
☑ GBR Full Street Name (4)

All

Quick Search

Data Source	Schema Name	Table	Column	Type	Masking Rule
POSTGRES Demo	QA	TEST50K	varchar_phone	VARCHAR	Phone Number (Column)
POSTGRES Demo	QA	TEST50K	char_phone	CHAR	Phone Number (Column)
POSTGRES Demo	QA	TEST50K	nchar_phone	CHAR	Phone Number (Column)
POSTGRES Demo	QA	TEST50K	nvarchar_phone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	phonenumber	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cellno	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cell_no	CHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cel	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cell_number	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	phonecontact	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	phone_contact	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cellphone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cell_phone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	landline	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	land_line	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	businessphone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	business_phone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	workphone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	work_phone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	homephone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	home_phone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	tel	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	telephone	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cell	VARCHAR	Phone Number (Column)
POSTGRES Demo	MASTER_MASKING	PHONE_NUMBER(COLUMN)	cellular	VARCHAR	Phone Number (Column)

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

5. Quick Start for SQL Databases

The following sections from Quick Start to Privacy dashboard are for SQL databases such as:

- ORACLE
- DB2 LUW
- DB2 z/OS
- PostgreSQL
- MS-SQLServer
- SAP HANA
- MySQL
- MySQL Aurora

> The following example shows the procedure to deploy a PostgreSQL. This is a general procedure and is applicable for all the databases listed above.

Return to Privacy Dashboard.

Continue to Managing Data Sources.

Deploying the Data Masking Module

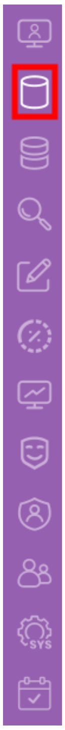
Procedure to deploy the Data Masking Module:

1. Adding a Data Source
2. Creating an Environment
3. Performing a Sensitive Data Search
4. Manual Editing the Masking Configuration
5. Data Masking and Progress Monitoring

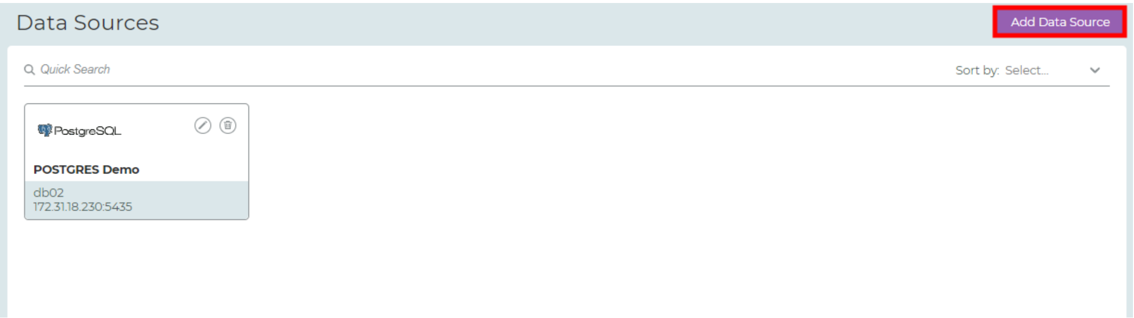
Adding a Data Source

To add a Data Source:

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



2. Click **Add Data Source**.



Data Sources

Add Data Source

Quick Search

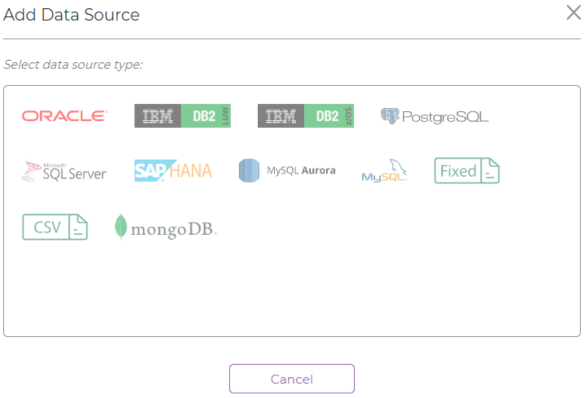
Sort by: Select...

PostgreSQL

POSTGRES Demo

db02
172.31.18.230:5435

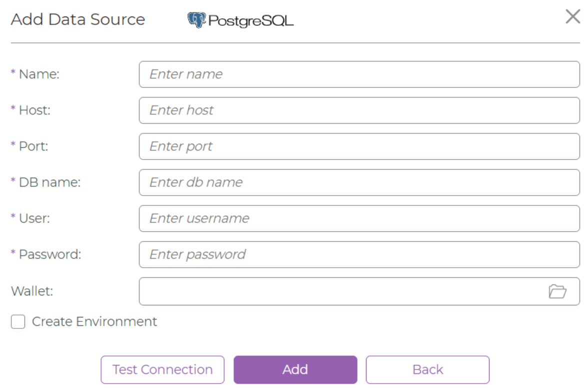
3. Select source data type.



Add Data Source

Select data source type:

4. Fill in the data source details.



Add Data Source PostgreSQL

* Name:	Enter name
* Host:	Enter host
* Port:	Enter port
* DB name:	Enter db name
* User:	Enter username
* Password:	Enter password
Wallet:	

□ Create Environment

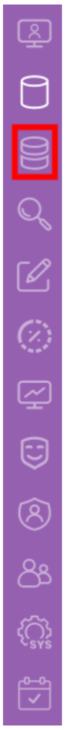
> In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

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

Creating an Environment

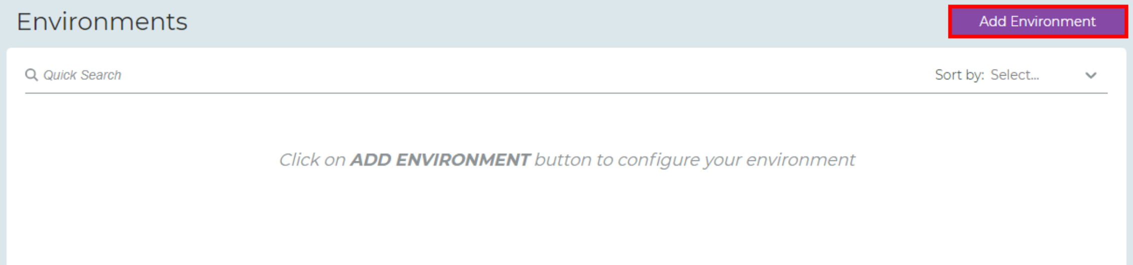
To create an environment:

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



To add a new environment:

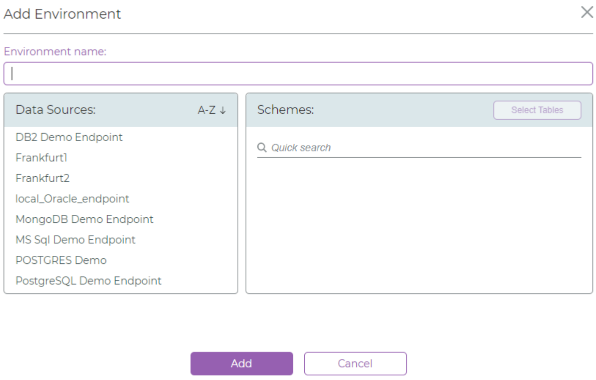
1. Click **Add Environment**.



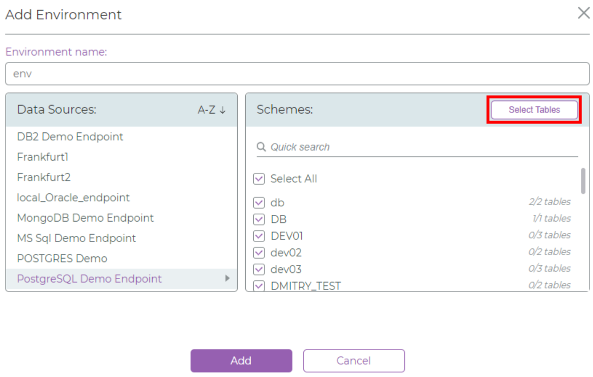
Environments

*Click on **ADD ENVIRONMENT** button to configure your 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. In **Data Sources**, select a data source.
    b. In **Schemes**, click **Select Tables**.



Add Environment

Environment name: env

Data Sources:

- DB2 Demo Endpoint
- Frankfurt1
- Frankfurt2
- local_Oracle_endpoint
- MongoDB Demo Endpoint
- MS Sql Demo Endpoint
- POSTGRES Demo
- PostgreSQL Demo Endpoint

Schemes:

☑ Select All

☑ db	2/2 tables
☑ DB	1/1 tables
☑ DEV01	0/3 tables
☑ dev02	0/2 tables
☑ dev03	0/3 tables
☑ DMITRY_TEST	0/2 tables

    c. Clear the checkbox for a table not to be included.

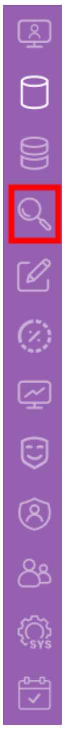
> The list shown is the list from the last refresh. To update the list, click **Refresh**.

4. Click **Submit**.
5. Click **Add**.

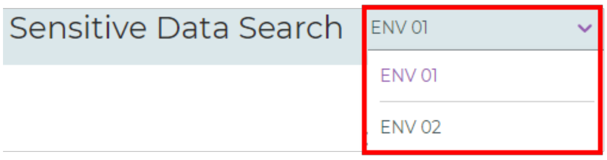
Performing a Sensitive Data Search

To perform a new sensitive data search:

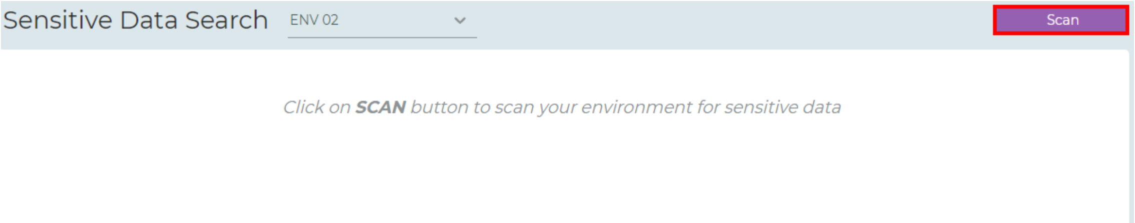
1. On the navigation bar, click 🔍 (**Sensitive Search**).



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

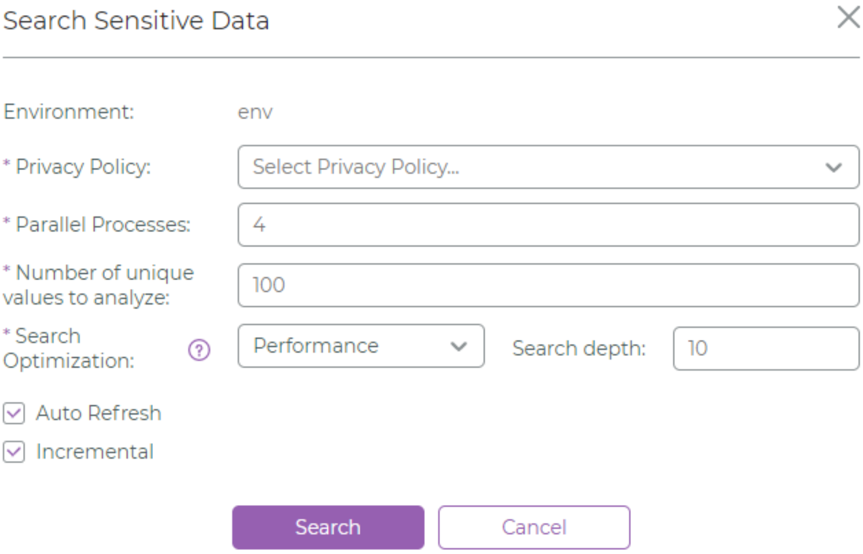


3. Click Scan.


Sensitive Data Search ENV 02

Click on **SCAN** button to scan your environment for sensitive data

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


Search Sensitive Data

Environment:	env
* Privacy Policy:	Select Privacy Policy...
* Parallel Processes:	4
* Number of unique values to analyze:	100
* Search Optimization:	Performance Search depth: 10

☑ Auto Refresh

☑ Incremental

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

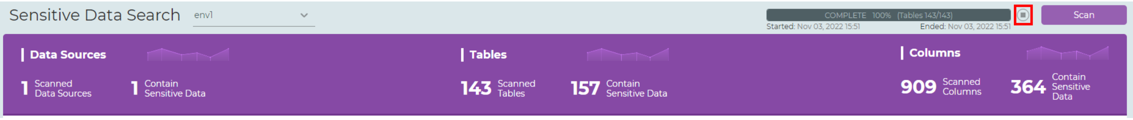
4. Select the **Auto Refresh** checkbox to have the system refresh automatically before doing a scan.
5. Select the **Incremental** checkbox to include columns that were found in a scan done before to be in the search results for this scan.

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

6. Click **Search**.

To stop the search:

1. Click ■ (**Stop**).



Sensitive Data Search env1

COMPLETE 100% (Tables 143/143)
Started: Nov 03, 2022 15:51 Ended: Nov 03, 2022 15:51

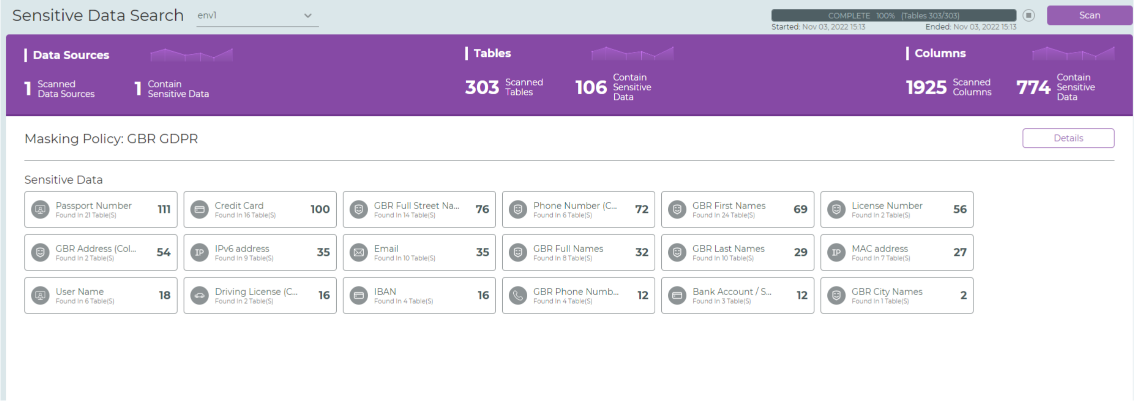
Scan

Data Sources: 1 Scanned Data Sources; 1 Contain Sensitive Data

Tables: 143 Scanned Tables; 157 Contain Sensitive Data

Columns: 909 Scanned Columns; 364 Contain Sensitive Data

After the scan is complete, the scan summary appears.



Sensitive Data Search env1

COMPLETE 100% (Tables 303/303)
Started: Nov 03, 2022 15:13 Ended: Nov 03, 2022 15:13

Scan

Data Sources: 1 Scanned Data Sources; 1 Contain Sensitive Data

Tables: 303 Scanned Tables; 106 Contain Sensitive Data

Columns: 1925 Scanned Columns; 774 Contain Sensitive Data

Masking Policy: GBR GDPR

Details

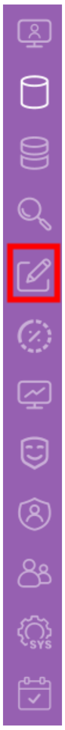
Sensitive Data

Passport Number Found In 21 Table(S) 111	Credit Card Found In 16 Table(S) 100	GBR Full Street Na... Found In 14 Table(S) 76	Phone Number (C... Found In 6 Table(S) 72	GBR First Names Found In 24 Table(S) 69	License Number Found In 2 Table(S) 56
GBR Address (Col... Found In 2 Table(S) 54	IPv6 address Found In 9 Table(S) 35	Email Found In 10 Table(S) 35	GBR Full Names Found In 8 Table(S) 32	GBR Last Names Found In 10 Table(S) 29	MAC address Found In 7 Table(S) 27
User Name Found In 6 Table(S) 18	Driving License (C... Found In 2 Table(S) 16	IBAN Found In 4 Table(S) 16	GBR Phone Numb... Found In 4 Table(S) 12	Bank Account / S... Found In 3 Table(S) 12	GBR City Names Found In 1 Table(S) 2

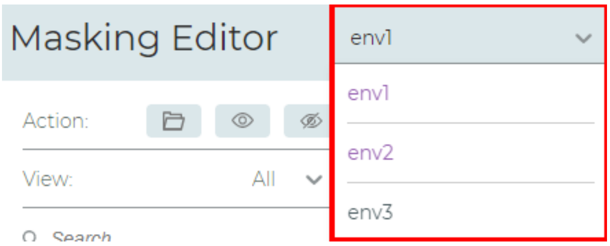
Manual Editing the Masking Configuration

To manually edit the masking configuration:

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



2. Select the required environment.

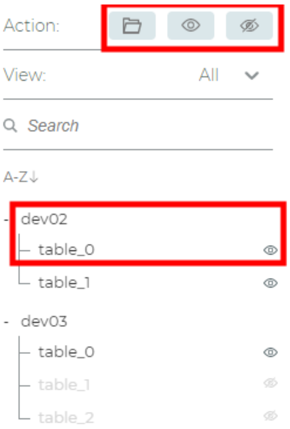


To filter the list of tables:

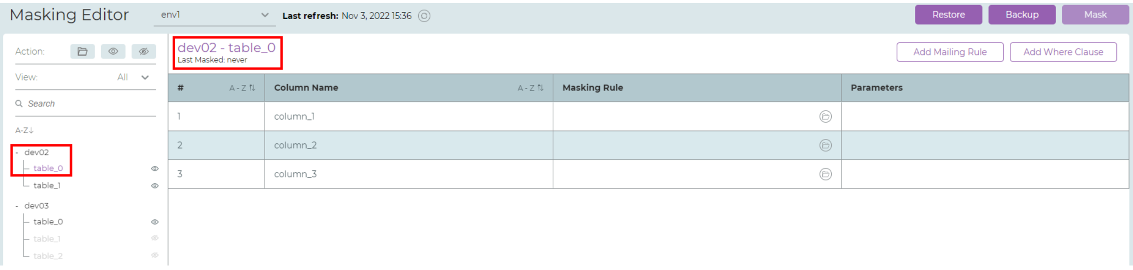
1. Select active or inactive.
2. Select:
   a. View all tables
   b. Active tables
   c. Inactive tables

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.

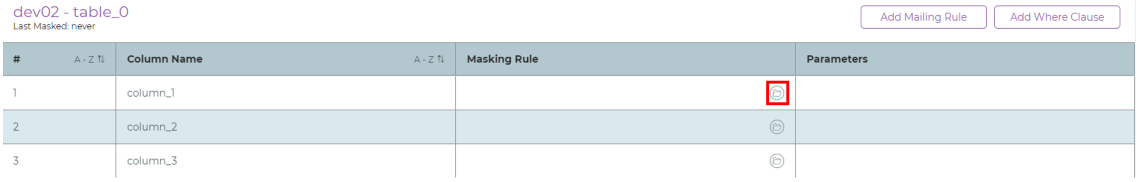


dev02 - table_0
Last Masked: never

# A - Z ⇅	Column Name A - Z ⇅	Masking Rule	Parameters
1	column_1		
2	column_2		
3	column_3		

To select another/new masking rule:

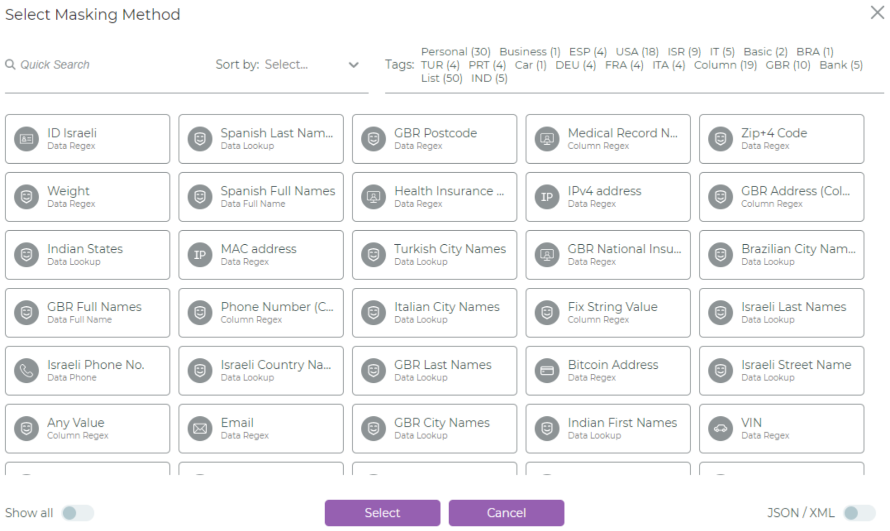
1. For the required column, click 📂.



dev02 - table_0
Last Masked: never

# A - Z ⇅	Column Name A - Z ⇅	Masking Rule	Parameters
1	column_1		
2	column_2		
3	column_3		

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


Select Masking Method
Quick Search
Sort by: Select...
Tags: Personal (30) Business (1) ESP (4) USA (18) ISR (9) IT (5) Basic (2) BRA (1) TUR (4) PRT (4) Car (1) DEU (4) FRA (4) ITA (4) Column (19) GBR (10) Bank (5) List (50) IND (5)
Show all
Select
Cancel
JSON / XML

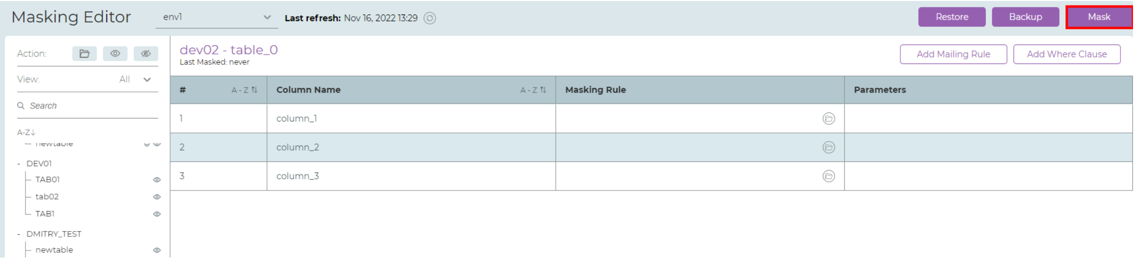
ID Israeli Data Regex	Spanish Last Nam... Data Lookup	GBR Postcode Data Regex	Medical Record N... Column Regex	Zip+4 Code Data Regex
Weight Data Regex	Spanish Full Names Data Full Name	Health Insurance ... Data Regex	IPv4 address Data Regex	GBR Address (Col... Column Regex
Indian States Data Lookup	MAC address Data Regex	Turkish City Names Data Lookup	GBR National Insu... Data Regex	Brazilian City Nam... Data Lookup
GBR Full Names Data Full Name	Phone Number (C... Column Regex	Italian City Names Data Lookup	Fix String Value Column Regex	Israeli Last Names Data Lookup
Israeli Phone No. Data Phone	Israeli Country Na... Data Lookup	GBR Last Names Data Lookup	Bitcoin Address Data Regex	Israeli Street Name Data Lookup
Any Value Column Regex	Email Data Regex	GBR City Names Data Lookup	Indian First Names Data Lookup	VIN Data Regex

ACCELARIO

Data Masking and Progress Monitoring

To mask the selected table:

1. Click **Mask**.

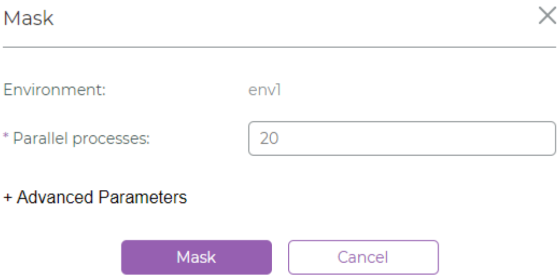


env1 Last refresh: Nov 16, 2022 13:29

dev02 - table_0
Last Masked: never

# A - Z ⇅	Column Name A - Z ⇅	Masking Rule	Parameters
1	column_1		
2	column_2		
3	column_3		

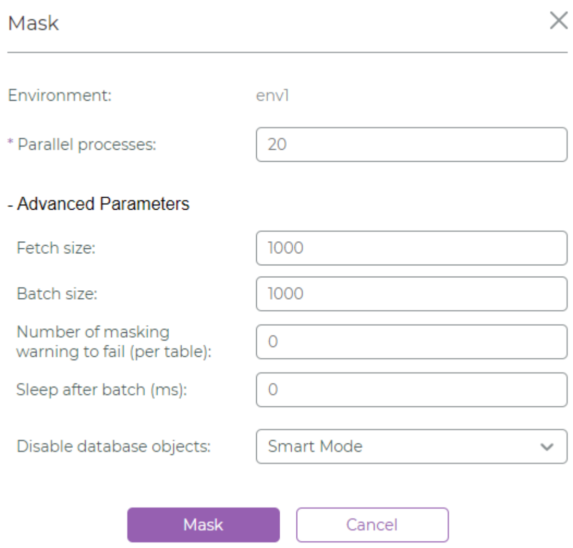
2. Fill in the masking details and click **Mask**.



Environment: env1

* Parallel processes: 20

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



Mask

Environment: env1

* Parallel processes: 20

- Advanced Parameters

Fetch size: 1000

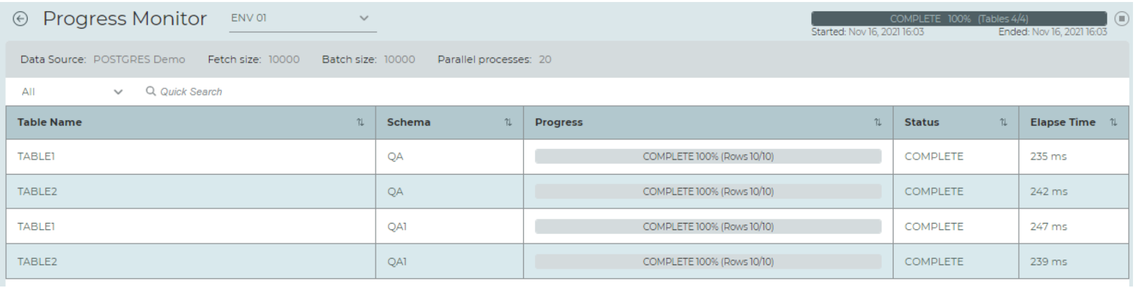
Batch size: 1000

Number of masking warning to fail (per table): 0

Sleep after batch (ms): 0

Disable database objects: Smart Mode

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



Progress Monitor ENV 01

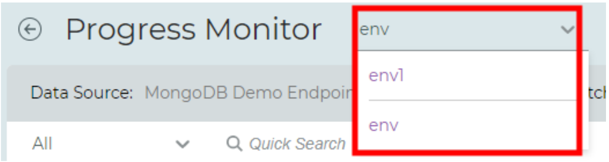
COMPLETE 100% (Tables 4/4)

Started: Nov 16, 2021 16:03 Ended: Nov 16, 2021 16:03

Data Source: POSTGRES Demo Fetch size: 10000 Batch size: 10000 Parallel processes: 20

Table Name	Schema	Progress	Status	Elapse Time
TABLE1	QA	COMPLETE 100% (Rows 10/10)	COMPLETE	235 ms
TABLE2	QA	COMPLETE 100% (Rows 10/10)	COMPLETE	242 ms
TABLE1	QA1	COMPLETE 100% (Rows 10/10)	COMPLETE	247 ms
TABLE2	QA1	COMPLETE 100% (Rows 10/10)	COMPLETE	239 ms

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



Progress Monitor env

Data Source: MongoDB Demo Endpoi

6. Quick Start for NoSQL Databases

The following sections from Quick Start to Privacy dashboard are for a MongoDB.

Return to Privacy Dashboard.

Continue to Managing Data Sources.

Deploying the Data Masking Module

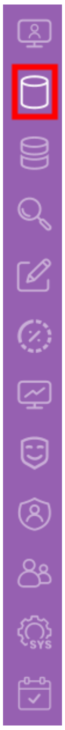
Procedure to deploy the Data Masking Module:

1. Adding a Data Source
2. Creating an Environment
3. Performing a Sensitive Data Search
4. Manual Editing the Masking Configuration
5. Data Masking and Progress Monitoring

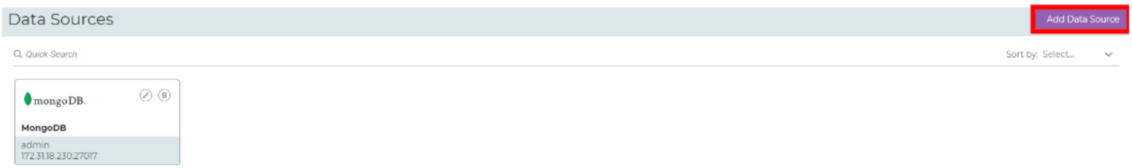
Adding a Data Source

To add a Data Source:

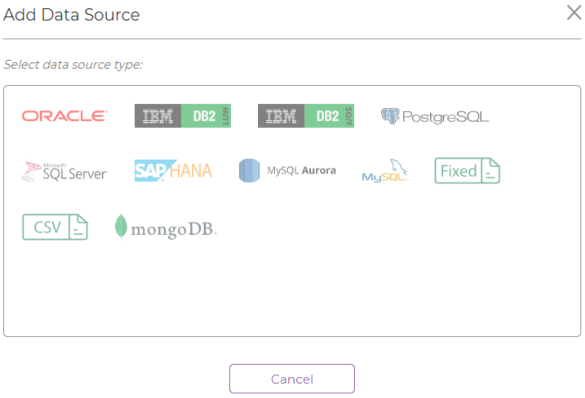
1. On the navigation bar, click 🛢 (**Data Sources**).



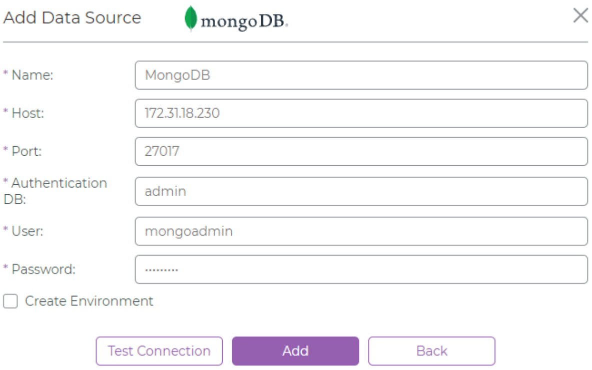
2. Click **Add Data Source**.



3. Select source data type.



4. Fill in the data source details.



Add Data Source mongoDB.

* Name: MongoDB

* Host: 172.31.18.230

* Port: 27017

* Authentication DB: admin

* User: mongoadmin

* Password: ·········

□ Create Environment

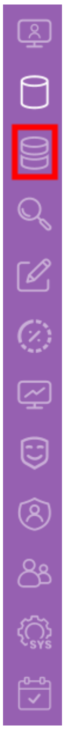
In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

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

Creating an Environment

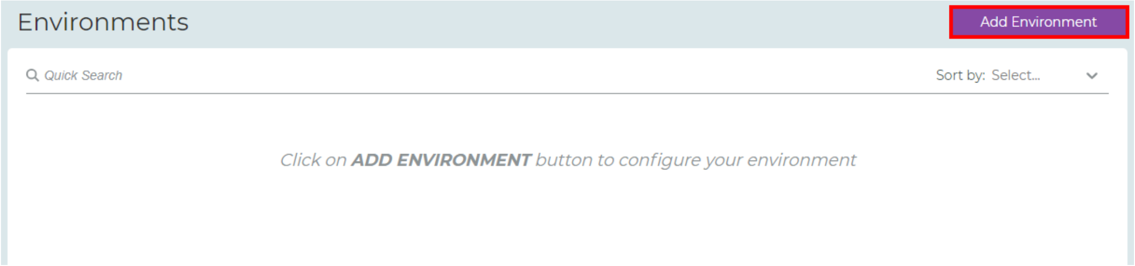
To create an environment:

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



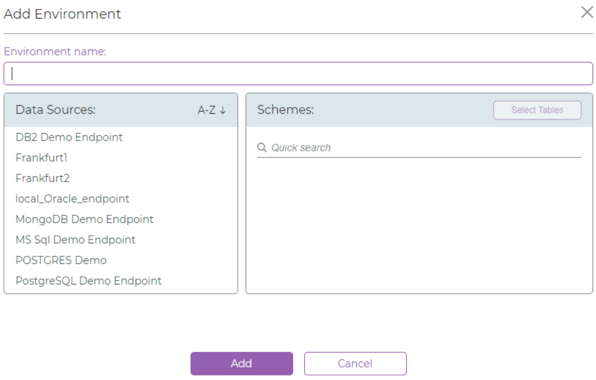
To add a new environment:

1. Click **Add Environment**.

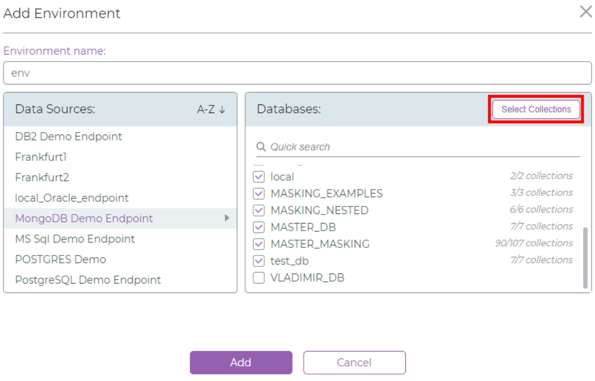


*Click on **ADD ENVIRONMENT** button to configure your environment*

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 **Databases**, select the data source databases that the environment will use, or click **Select All** to include all Databases of the selected data source.



3. For specific collections from databases:
    a. In **Data Sources** select a data source.
    b. In **Databases**, click **Select Collection**.



Add Environment

Environment name: env

Data Sources: A-Z ↓

- DB2 Demo Endpoint
- Frankfurt1
- Frankfurt2
- local_Oracle_endpoint
- MongoDB Demo Endpoint
- MS Sql Demo Endpoint
- POSTGRES Demo
- PostgreSQL Demo Endpoint

Databases:

☑ local	2/2 collections
☑ MASKING_EXAMPLES	3/3 collections
☑ MASKING_NESTED	6/6 collections
☑ MASTER_DB	7/7 collections
☑ MASTER_MASKING	90/107 collections
☑ test_db	7/7 collections
☐ VLADIMIR_DB	

    c. Clear the checkbox for a collection not to be included.

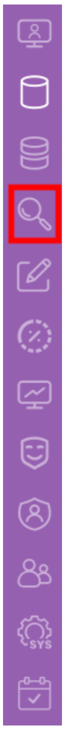
> The list shown is the list from the last refresh. To update the list, Click **Refresh**.

4. Click **Submit**.
5. Click **Add**.

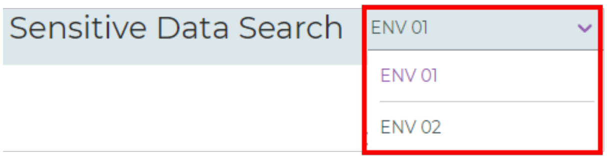
Performing a Sensitive Data Search

To perform a new sensitive data search:

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



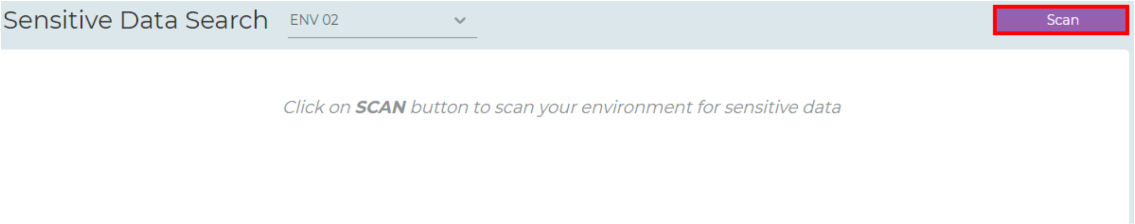
2. Select the required environment for searching for sensitive data.



Sensitive Data Search

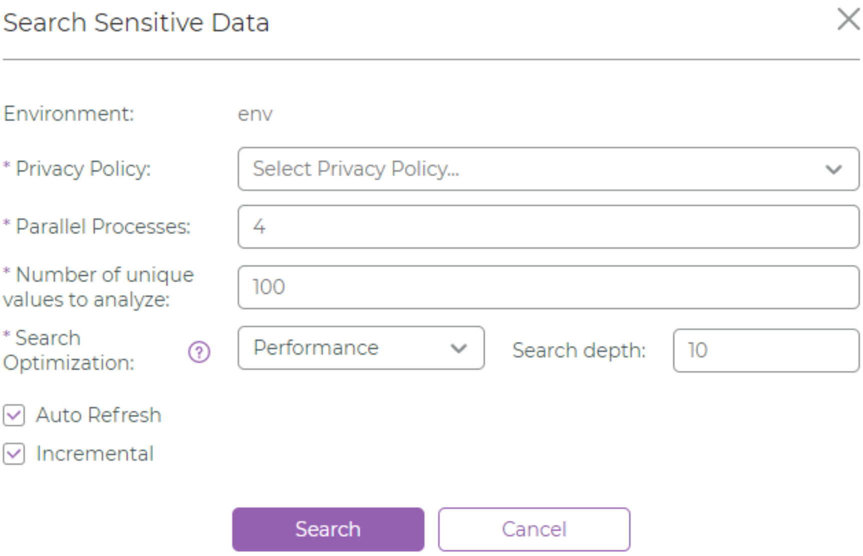
ENV 01

3. Click **Scan**.



*Click on **SCAN** button to scan your environment for sensitive data*

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



Search Sensitive Data

Environment: env

* Privacy Policy: Select Privacy Policy...

* Parallel Processes: 4

* Number of unique values to analyze: 100

* Search Optimization: Performance

Search depth: 10

☑ Auto Refresh

☑ Incremental

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.

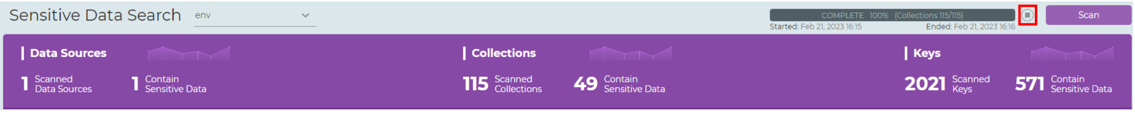
5. Select the **Incremental** checkbox to include columns that were found in a scan done before to be in the search results for this scan.

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

6. Click **Search**.

To stop the search:

1. Click ⏹ (**Stop**).



Sensitive Data Search env

COMPLETE 100% (Collections 115/115)
Started: Feb 21, 2023 16:15 Ended: Feb 21, 2023 16:16

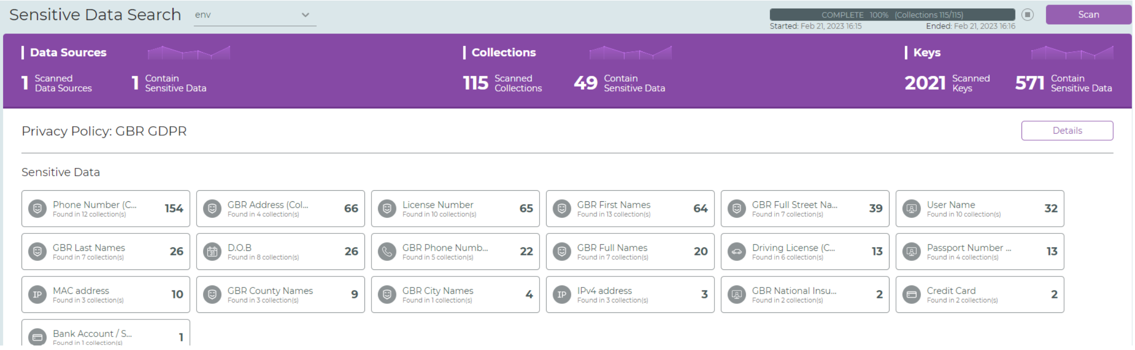
Scan

Data Sources: 1 Scanned Data Sources, 1 Contain Sensitive Data

Collections: 115 Scanned Collections, 49 Contain Sensitive Data

Keys: 2021 Scanned Keys, 571 Contain Sensitive Data

After the scan is complete, the scan summary appears.



Sensitive Data Search env

COMPLETE 100% (Collections 115/115)
Started: Feb 21, 2023 16:15 Ended: Feb 21, 2023 16:16

Scan

Data Sources: 1 Scanned Data Sources, 1 Contain Sensitive Data

Collections: 115 Scanned Collections, 49 Contain Sensitive Data

Keys: 2021 Scanned Keys, 571 Contain Sensitive Data

Privacy Policy: GBR GDPR

Details

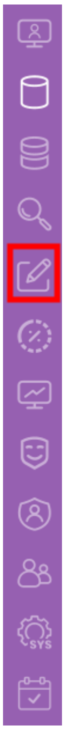
Sensitive Data

Phone Number (C...	Found in 12 collection(s)	154
GBR Address (Col...	Found in 4 collection(s)	66
License Number	Found in 10 collection(s)	65
GBR First Names	Found in 13 collection(s)	64
GBR Full Street Na...	Found in 7 collection(s)	39
User Name	Found in 10 collection(s)	32
GBR Last Names	Found in 7 collection(s)	26
D.O.B	Found in 8 collection(s)	26
GBR Phone Numb...	Found in 5 collection(s)	22
GBR Full Names	Found in 7 collection(s)	20
Driving License (C...	Found in 6 collection(s)	13
Passport Number ...	Found in 4 collection(s)	13
MAC address	Found in 3 collection(s)	10
GBR County Names	Found in 3 collection(s)	9
GBR City Names	Found in 1 collection(s)	4
IPv4 address	Found in 3 collection(s)	3
GBR National Insu...	Found in 2 collection(s)	2
Credit Card	Found in 2 collection(s)	2
Bank Account / S...	Found in 1 collection(s)	1

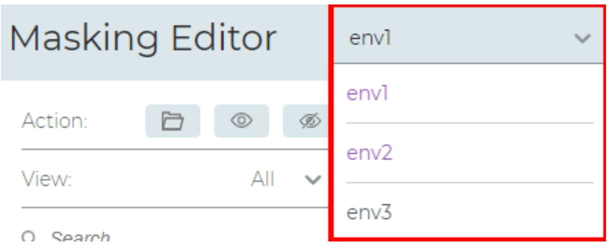
Manual Editing the Masking Configuration

To manually edit the masking configuration:

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



2. Select the required environment.

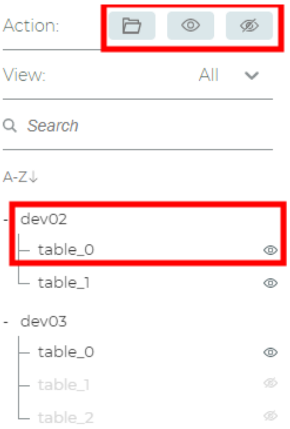


To filter the list of collections:

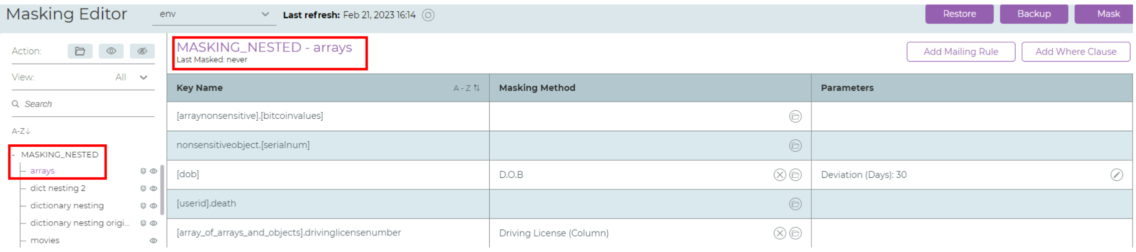
1. Select active or inactive.
2. Select:
   a. View all collections
   b. Active collections
   c. Inactive collections

You can also search for specific collections.

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 keys in the table selected.



Masking Editor env Last refresh: Feb 21, 2023 16:14

Restore Backup Mask

Action: View: All Search A-Z↓

- MASKING_NESTED
  - arrays
  - dict nesting 2
  - dictionary nesting
  - dictionary nesting origi...
  - movies

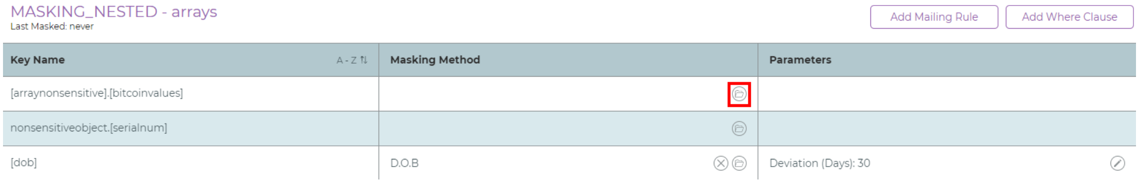
MASKING_NESTED - arrays
Last Masked: never

Add Mailing Rule Add Where Clause

Key Name A - Z ⇅	Masking Method	Parameters
[arraynonsensitive].[bitcoinvalues]		
nonsensitiveobject.[serialnum]		
[dob]	D.O.B	Deviation (Days): 30
[userid].death		
[array_of_arrays_and_objects].drivinglicensenumber	Driving License (Column)	

To select another/new masking rule:

1. For the required column, click .

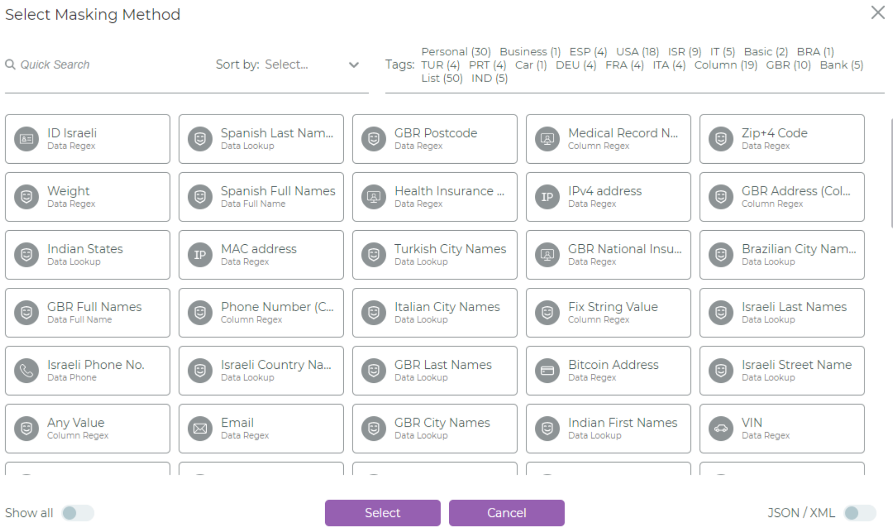


MASKING_NESTED - arrays
Last Masked: never

Add Mailing Rule Add Where Clause

Key Name A - Z ⇅	Masking Method	Parameters
[arraynonsensitive].[bitcoinvalues]		
nonsensitiveobject.[serialnum]		
[dob]	D.O.B	Deviation (Days): 30

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



Select Masking Method

Quick Search Sort by: Select...

Tags: Personal (30) Business (1) ESP (4) USA (18) ISR (9) IT (5) Basic (2) BRA (1) TUR (4) PRT (4) Car (1) DEU (4) FRA (4) ITA (4) Column (19) GBR (10) Bank (5) List (50) IND (5)

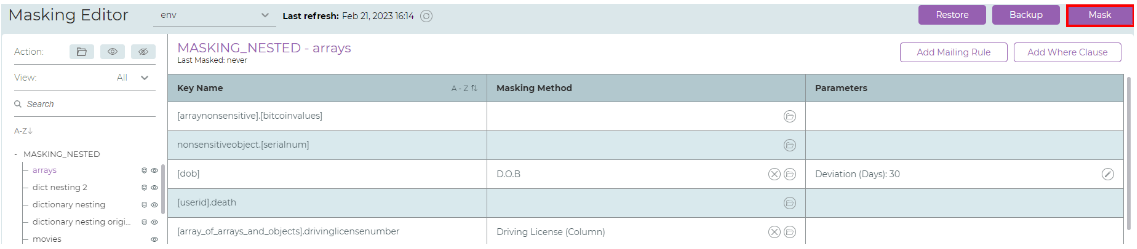
ID Israeli Data Regex	Spanish Last Nam... Data Lookup	GBR Postcode Data Regex	Medical Record N... Column Regex	Zip+4 Code Data Regex
Weight Data Regex	Spanish Full Names Data Full Name	Health Insurance ... Data Regex	IPv4 address Data Regex	GBR Address (Col... Column Regex
Indian States Data Lookup	MAC address Data Regex	Turkish City Names Data Lookup	GBR National Insu... Data Regex	Brazilian City Nam... Data Lookup
GBR Full Names Data Full Name	Phone Number (C... Column Regex	Italian City Names Data Lookup	Fix String Value Column Regex	Israeli Last Names Data Lookup
Israeli Phone No. Data Phone	Israeli Country Na... Data Lookup	GBR Last Names Data Lookup	Bitcoin Address Data Regex	Israeli Street Name Data Lookup
Any Value Column Regex	Email Data Regex	GBR City Names Data Lookup	Indian First Names Data Lookup	VIN Data Regex

Show all Select Cancel JSON / XML

Data Masking and Progress Monitoring

To mask the selected collection:

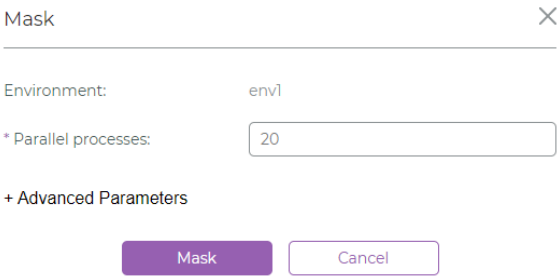
1. Click **Mask**.



MASKING_NESTED - arrays
Last Masked: never

Key Name	Masking Method	Parameters
[arraynonsensitive].[bitcoinvalues]		
nonsensitiveobject.[serialnum]		
[dob]	D.O.B	Deviation (Days): 30
[userid].death		
[array_of_arrays_and_objects].drivinglicensenumber	Driving License (Column)	

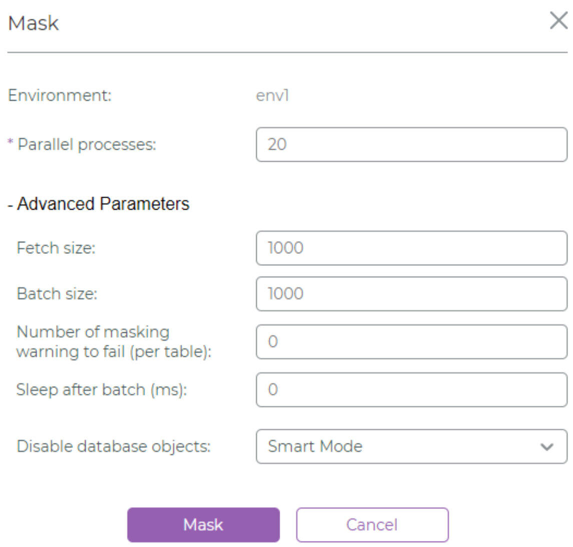
2. Fill in the masking details and click **Mask**.



Environment: env1

* Parallel processes: 20

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



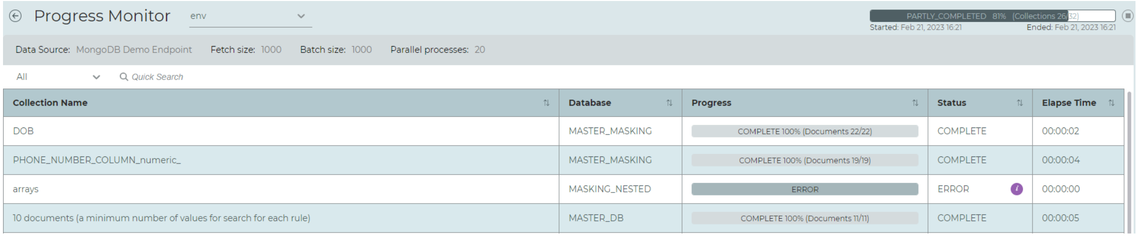
Mask

Environment:	env1
* Parallel processes:	20

- Advanced Parameters

Fetch size:	1000
Batch size:	1000
Number of masking warning to fail (per table):	0
Sleep after batch (ms):	0
Disable database objects:	Smart Mode

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



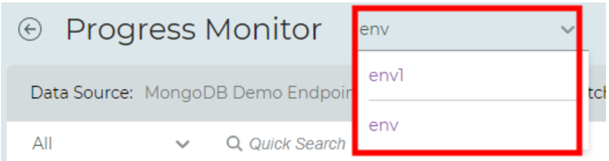
Progress Monitor env

PARTLY_COMPLETED 81% (Collections 26/32)
Started: Feb 21, 2023 16:21
Ended: Feb 21, 2023 16:21

Data Source: MongoDB Demo Endpoint Fetch size: 1000 Batch size: 1000 Parallel processes: 20

Collection Name	Database	Progress	Status	Elapse Time
DOB	MASTER_MASKING	COMPLETE 100% (Documents 22/22)	COMPLETE	00:00:02
PHONE_NUMBER_COLUMN_numeric_	MASTER_MASKING	COMPLETE 100% (Documents 19/19)	COMPLETE	00:00:04
arrays	MASKING_NESTED	ERROR	ERROR	00:00:00
10 documents (a minimum number of values for search for each rule)	MASTER_DB	COMPLETE 100% (Documents 11/11)	COMPLETE	00:00:05

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



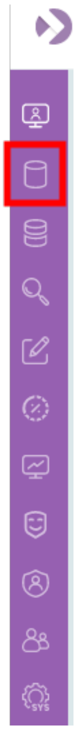
7. Managing Data Sources

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. The following examples show PostgreSQL but are correct for all the databases.

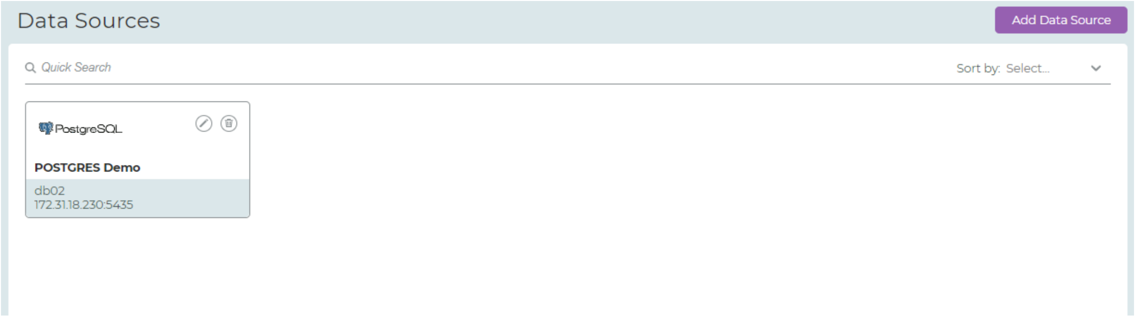
Only a user with **Admin** privileges can see or edit **Data Sources**.

To see available data sources:

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

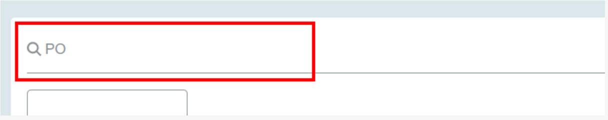


2. The **Data Sources** window appears displaying all data sources that have been added to the system.



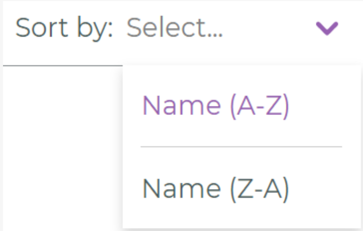
POSTGRES Demo
db02
172.31.18.230:5435

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



PO

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

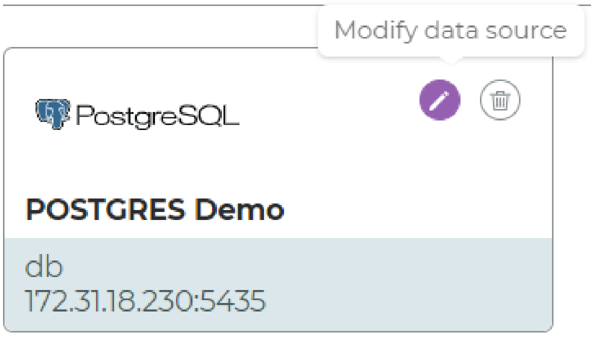


To add a data source for a SQL database, see Adding a Data Source.

To add a data source for a NoSQL database, see Adding a Data Source.

To modify data source details:

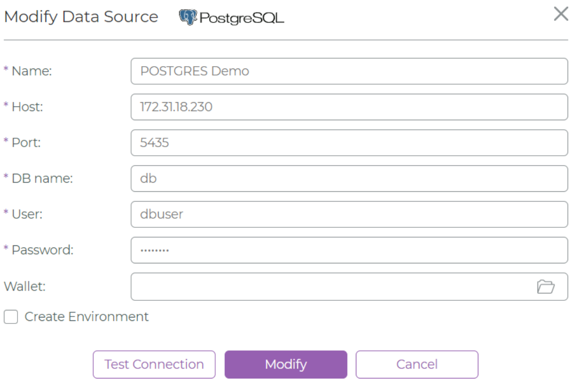
1. On the required data source, click ✎ **(Modify data source)**.



POSTGRES Demo

db
172.31.18.230:5435

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



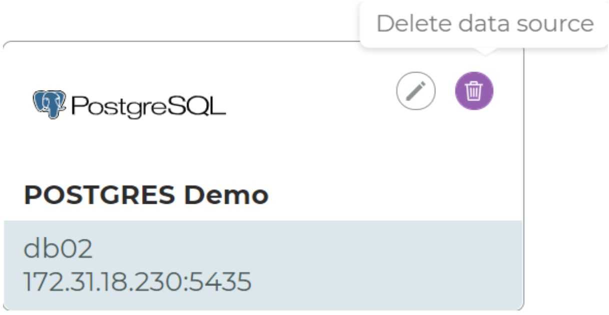
* Name:	POSTGRES Demo
* Host:	172.31.18.230
* Port:	5435
* DB name:	db
* User:	dbuser
* Password:	········
Wallet:	

□ Create Environment

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)** .

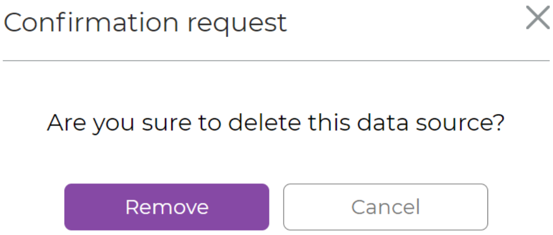


Delete data source

POSTGRES Demo

db02
172.31.18.230:5435

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



Confirmation request

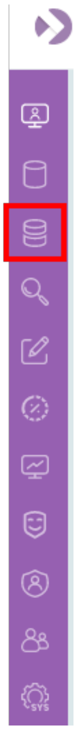
Are you sure to delete this data source?

8. Managing Environments

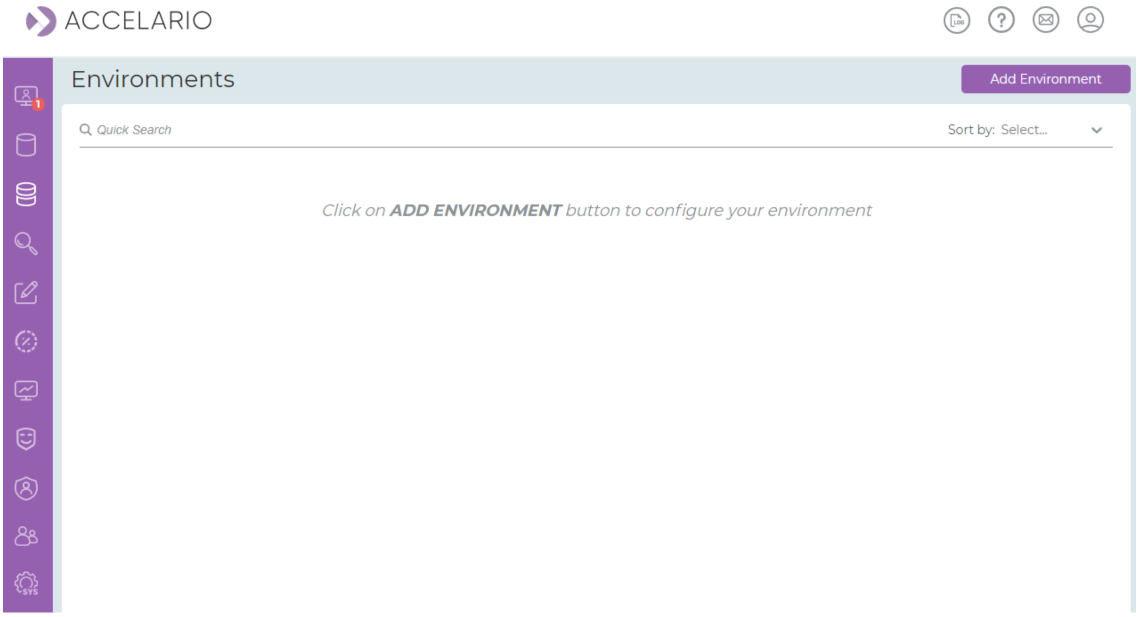
An Environment is an object that groups together database schemas from a data source. An environment object is used for scanning and masking. The following examples show PostgreSQL but are correct for all the databases.

To see your environments:

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

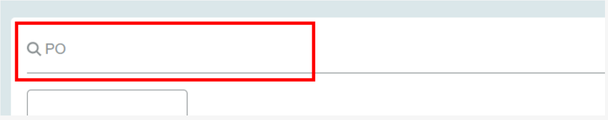


2. The **Environments** window appears.

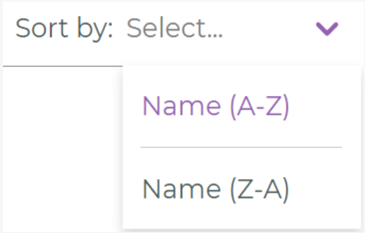


*Click on **ADD ENVIRONMENT** button to configure your environment*

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.



Sort by: Select...

Name (A-Z)

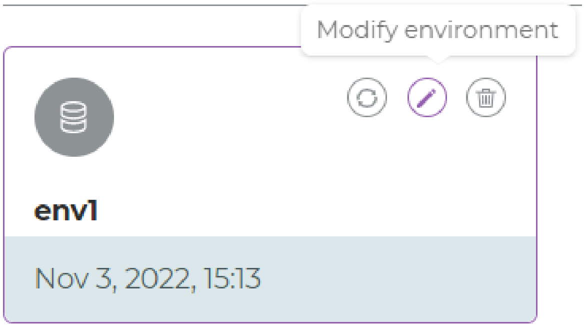
Name (Z-A)

To add an environment for a SQL database, see Creating an Environment.

To add an environment for a NoSQL database, see Creating an Environment.

To modify environment details:

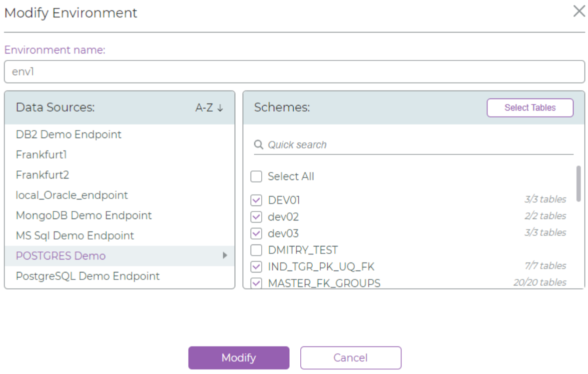
1. On the required environment, click ✎ **(Modify environments)** .



env1

Nov 3, 2022, 15:13

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



Environment name: env1

Data Sources:

- DB2 Demo Endpoint
- Frankfurt1
- Frankfurt2
- local_Oracle_endpoint
- MongoDB Demo Endpoint
- MS Sql Demo Endpoint
- POSTGRES Demo
- PostgreSQL Demo Endpoint

Schemes:

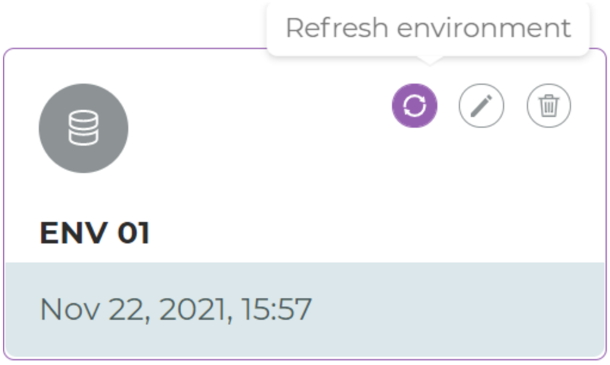
□ Select All

☑ DEV01 3/3 tables
☑ dev02 2/2 tables
☑ dev03 3/3 tables
□ DMITRY_TEST
☑ IND_TGR_PK_UQ_FK 7/7 tables
☑ MASTER_FK_GROUPS 20/20 tables

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

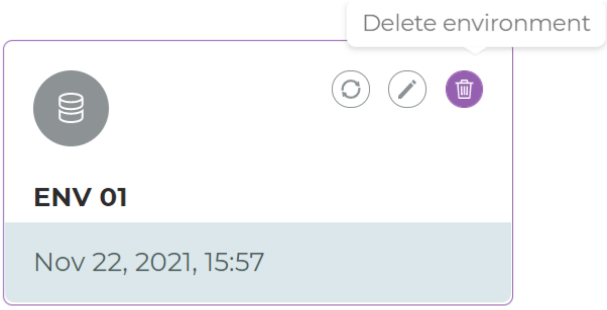
To refresh an environment:

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

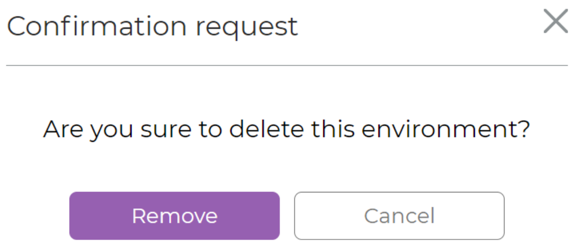


To delete an environment:

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



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



Confirmation request

Are you sure to delete this environment?

9. Searching for Sensitive Data

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

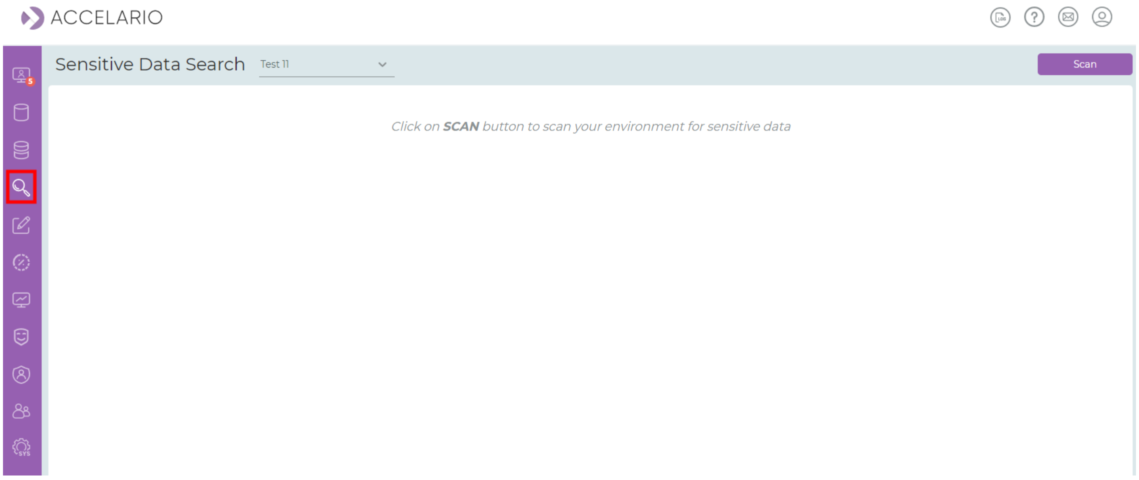
Once you have setup an environment, you can search the environment for sensitive data that you may want to mask.

You can also see results and perform new scans.

The following examples show PostgreSQL but are correct for all the databases.

To manage your sensitive data searches:

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

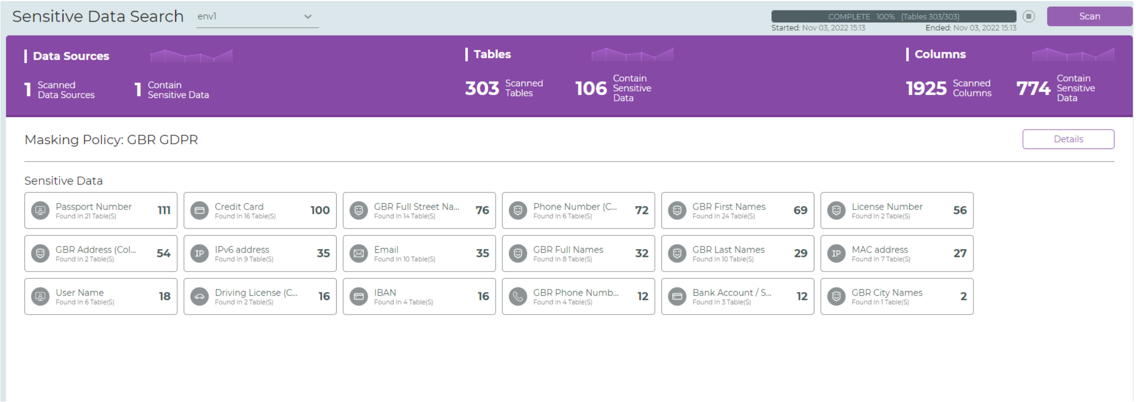


*Click on **SCAN** button to scan your environment for sensitive data*

To do a new sensitive data search for a SQL database, see Performing a Sensitive Data Search.

To do a new sensitive data search for a NoSQL database, see Performing a Sensitive Data Search.

After the scan is complete, the scan summary appears.



Sensitive Data Search env1

COMPLETE 100% (Tables 303/303)
Started: Nov 03, 2022 15:13 Ended: Nov 03, 2022 15:13

Data Sources
1 Scanned Data Sources
1 Contain Sensitive Data

Tables
303 Scanned Tables
106 Contain Sensitive Data

Columns
1925 Scanned Columns
774 Contain Sensitive Data

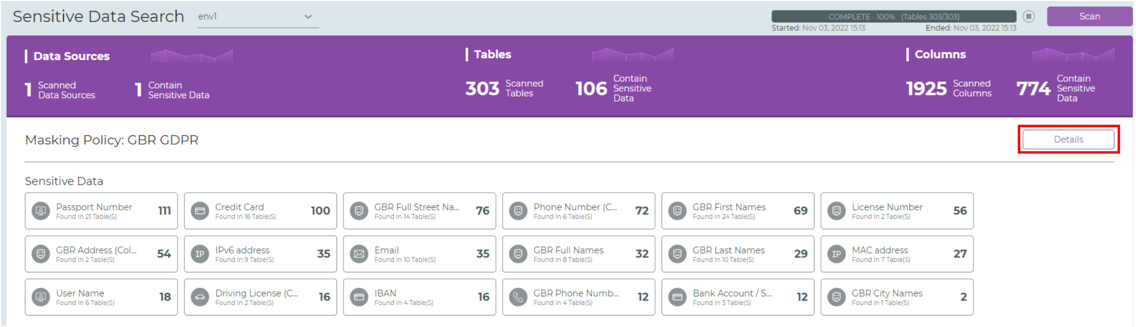
Masking Policy: GBR GDPR

Sensitive Data

Passport Number 111 Found In 21 Table(S)	Credit Card 100 Found In 16 Table(S)	GBR Full Street Na... 76 Found In 14 Table(S)	Phone Number (C... 72 Found In 6 Table(S)	GBR First Names 69 Found In 24 Table(S)	License Number 56 Found In 2 Table(S)
GBR Address (Col... 54 Found In 2 Table(S)	IPv6 address 35 Found In 9 Table(S)	Email 35 Found In 10 Table(S)	GBR Full Names 32 Found In 8 Table(S)	GBR Last Names 29 Found In 10 Table(S)	MAC address 27 Found In 7 Table(S)
User Name 18 Found In 6 Table(S)	Driving License (C... 16 Found In 2 Table(S)	IBAN 16 Found In 4 Table(S)	GBR Phone Numb... 12 Found In 4 Table(S)	Bank Account / S... 12 Found In 3 Table(S)	GBR City Names 2 Found In 1 Table(S)

To see detailed scan results:

1. Click **Details**.



Sensitive Data Search env1

COMPLETE 100% (Tables 303/303)
Started: Nov 03, 2022 15:13 Ended: Nov 03, 2022 15:13

Scan

Data Sources
1 Scanned Data Sources
1 Contain Sensitive Data

Tables
303 Scanned Tables
106 Contain Sensitive Data

Columns
1925 Scanned Columns
774 Contain Sensitive Data

Masking Policy: GBR GDPR

Details

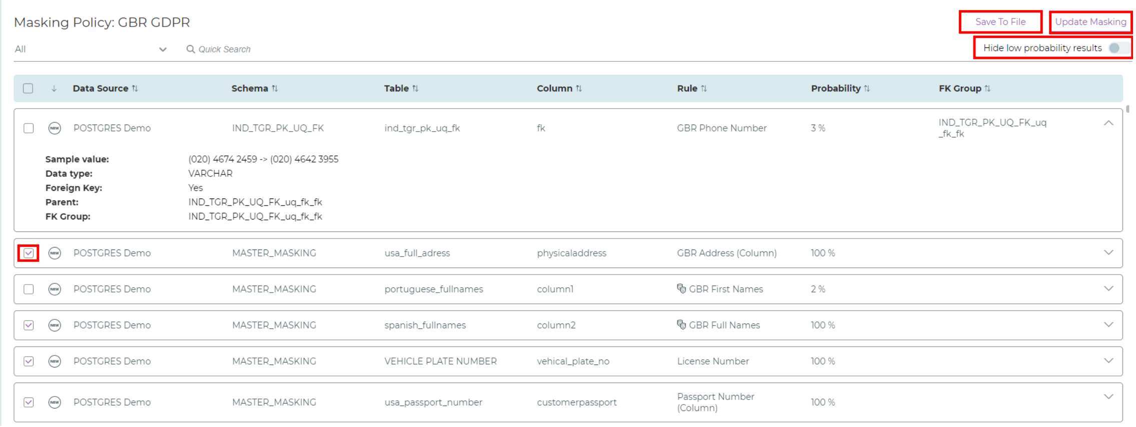
Sensitive Data

Passport Number 111 Found In 21 Table(S) | Credit Card 100 Found In 16 Table(S) | GBR Full Street Na... 76 Found In 14 Table(S) | Phone Number (C... 72 Found In 6 Table(S) | GBR First Names 69 Found In 24 Table(S) | License Number 56 Found In 2 Table(S)
GBR Address (Col... 54 Found In 2 Table(S) | IPv6 address 35 Found In 9 Table(S) | Email 35 Found In 10 Table(S) | GBR Full Names 32 Found In 8 Table(S) | GBR Last Names 29 Found In 10 Table(S) | MAC address 27 Found In 7 Table(S)
User Name 18 Found In 6 Table(S) | Driving License (C... 16 Found In 2 Table(S) | IBAN 16 Found In 4 Table(S) | GBR Phone Numb... 12 Found In 4 Table(S) | Bank Account / S... 12 Found In 3 Table(S) | GBR City Names 2 Found In 1 Table(S)

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

   Example for SQL databases:

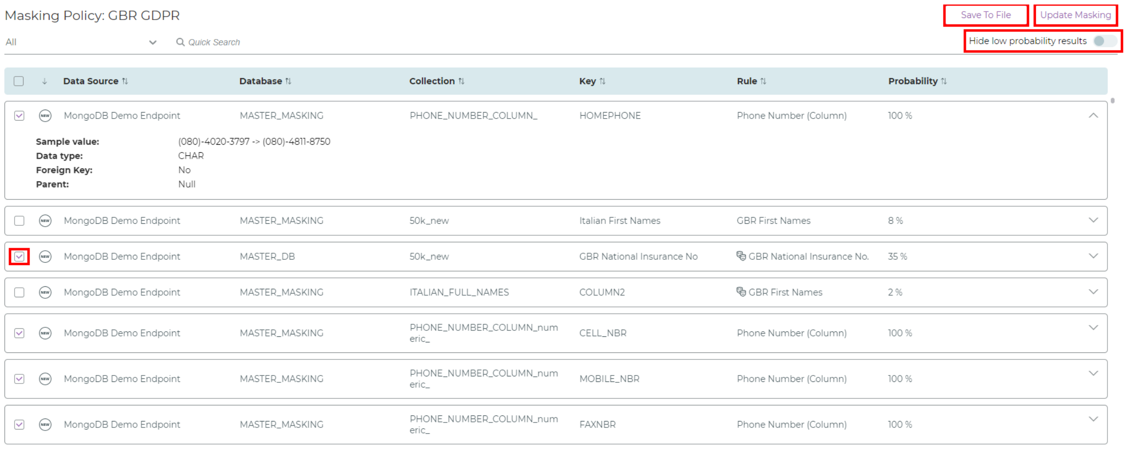


Masking Policy: GBR GDPR

□	Data Source	Schema	Table	Column	Rule	Probability	FK Group
□	POSTGRES Demo	IND_TGR_PK_UQ_FK	ind_tgr_pk_uq_fk	fk	GBR Phone Number	3 %	IND_TGR_PK_UQ_FK_uq_fk_fk
☑	POSTGRES Demo	MASTER_MASKING	usa_full_adress	physicaladdress	GBR Address (Column)	100 %	
□	POSTGRES Demo	MASTER_MASKING	portuguese_fullnames	column1	GBR First Names	2 %	
☑	POSTGRES Demo	MASTER_MASKING	spanish_fullnames	column2	GBR Full Names	100 %	
☑	POSTGRES Demo	MASTER_MASKING	VEHICLE PLATE NUMBER	vehical_plate_no	License Number	100 %	
☑	POSTGRES Demo	MASTER_MASKING	usa_passport_number	customerpassport	Passport Number (Column)	100 %	

Sample value: (020) 4674 2459 -> (020) 4642 3955
Data type: VARCHAR
Foreign Key: Yes
Parent: IND_TGR_PK_UQ_FK_uq_fk_fk
FK Group: IND_TGR_PK_UQ_FK_uq_fk_fk

Example for NoSQL databases:



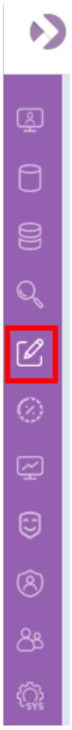
Masking Policy: GBR GDPR

□		Data Source	Database	Collection	Key	Rule	Probability
☑		MongoDB Demo Endpoint	MASTER_MASKING	PHONE_NUMBER_COLUMN_	HOMEPHONE	Phone Number (Column)	100 %
		Sample value:	(080)-4020-3797 -> (080)-4811-8750				
		Data type:	CHAR				
		Foreign Key:	No				
		Parent:	Null				
□		MongoDB Demo Endpoint	MASTER_MASKING	50k_new	Italian First Names	GBR First Names	8 %
☑		MongoDB Demo Endpoint	MASTER_DB	50k_new	GBR National Insurance No	GBR National Insurance No.	35 %
□		MongoDB Demo Endpoint	MASTER_MASKING	ITALIAN_FULL_NAMES	COLUMN2	GBR First Names	2 %
☑		MongoDB Demo Endpoint	MASTER_MASKING	PHONE_NUMBER_COLUMN_numeric_	CELL_NBR	Phone Number (Column)	100 %
☑		MongoDB Demo Endpoint	MASTER_MASKING	PHONE_NUMBER_COLUMN_numeric_	MOBILE_NBR	Phone Number (Column)	100 %
☑		MongoDB Demo Endpoint	MASTER_MASKING	PHONE_NUMBER_COLUMN_numeric_	FAXNBR	Phone Number (Column)	100 %

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

Use the masking editor to apply masking rules to columns in tables that you specify. The following examples show PostgreSQL but are correct for all the databases.

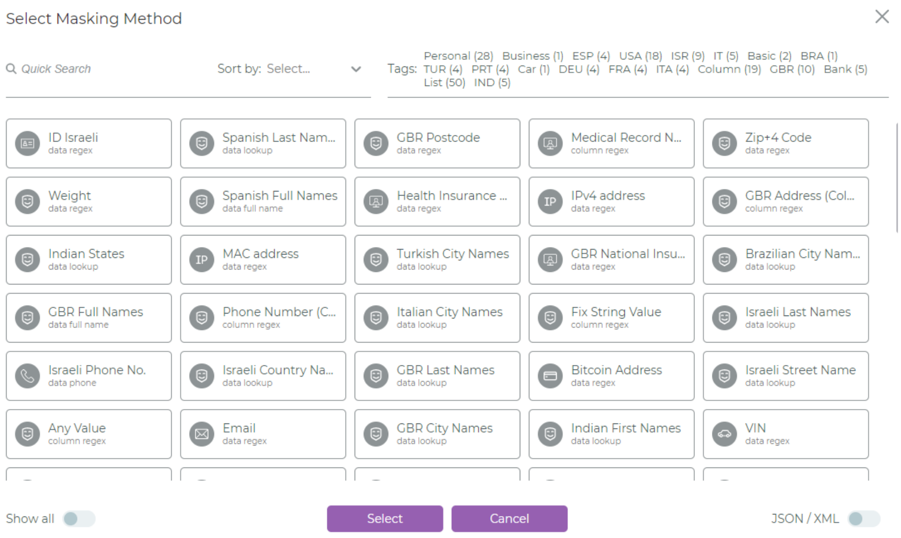
1. On the navigation bar, click ✎ (Masking Editor).



To select another/new masking rule for a SQL database, see Data Masking and Progress Monitoring.

To select another/new masking rule for a NoSQL database, see Data Masking and Progress Monitoring.

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



Select Masking Method

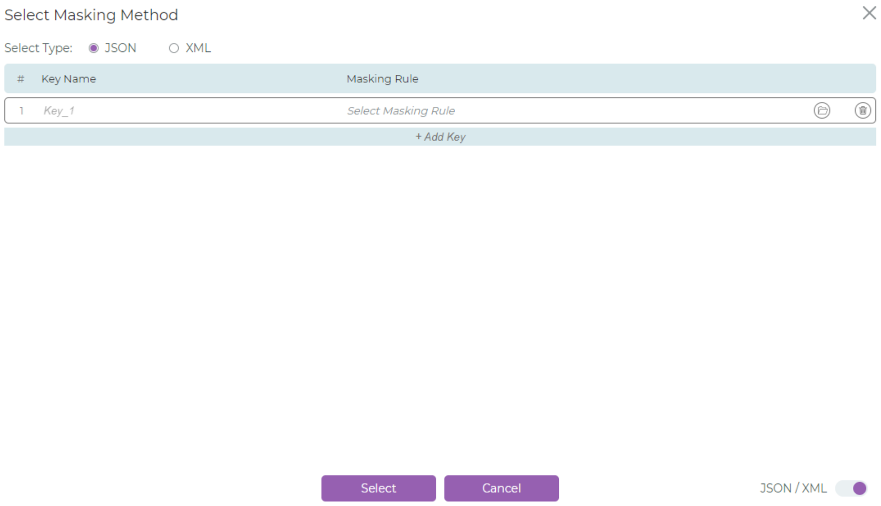
Quick Search   Sort by: Select...

Tags: Personal (28) Business (1) ESP (4) USA (18) ISR (9) IT (5) Basic (2) BRA (1) TUR (4) PRT (4) Car (1) DEU (4) FRA (4) ITA (4) Column (19) GBR (10) Bank (5) List (50) IND (5)

ID Israeli data regex	Spanish Last Nam... data lookup	GBR Postcode data regex	Medical Record N... column regex	Zip+4 Code data regex
Weight data regex	Spanish Full Names data full name	Health Insurance ... data regex	IPv4 address data regex	GBR Address (Col... column regex
Indian States data lookup	MAC address data regex	Turkish City Names data lookup	GBR National Insu... data regex	Brazilian City Nam... data lookup
GBR Full Names data full name	Phone Number (C... column regex	Italian City Names data lookup	Fix String Value column regex	Israeli Last Names data lookup
Israeli Phone No. data phone	Israeli Country Na... data lookup	GBR Last Names data lookup	Bitcoin Address data regex	Israeli Street Name data lookup
Any Value column regex	Email data regex	GBR City Names data lookup	Indian First Names data lookup	VIN data regex

Show all   Select   Cancel   JSON / XML

a. Click JSON / XML ●.



Select Masking Method

Select Type: ● JSON ○ XML

#	Key Name	Masking Rule
1	Key_1	Select Masking Rule

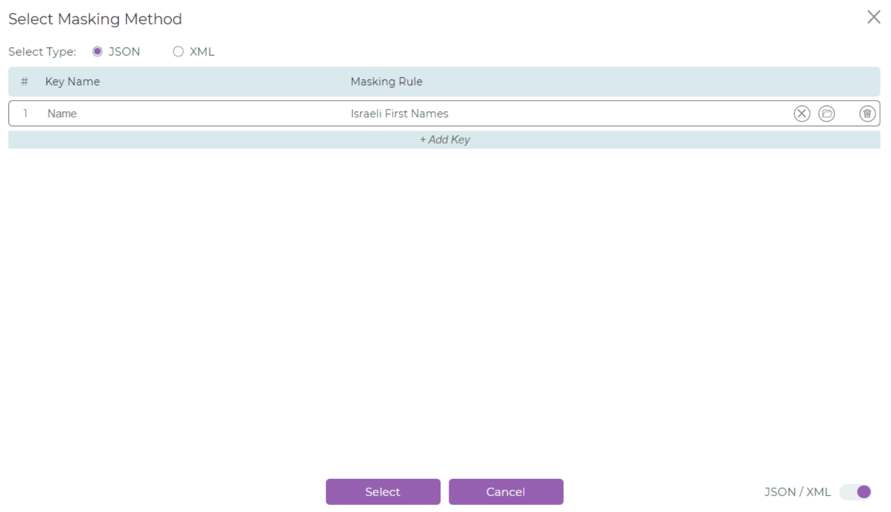
+ Add Key

Select   Cancel   JSON / XML

b. Enter the **Key Name**.

c. Click 🗁.

d. Select a **Masking Method**.



Select Masking Method

Select Type: ● JSON ○ XML

#	Key Name	Masking Rule
1	Name	Israeli First Names

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

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

To remove a masking rule:

1. On the masking rule, click ⊗ .

To remove a key:

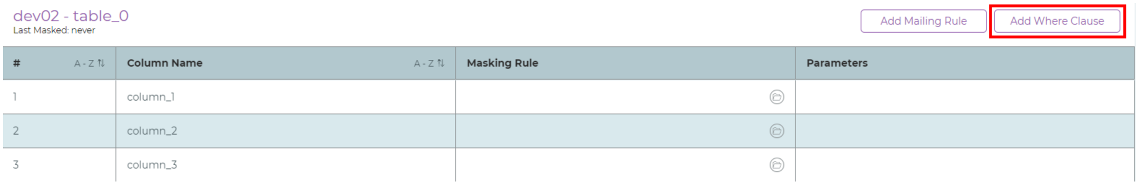
1. On the key, click 🗑 .

To see all the masking methods:

1. On the key, click Show all ● .

To add a Where Clause:

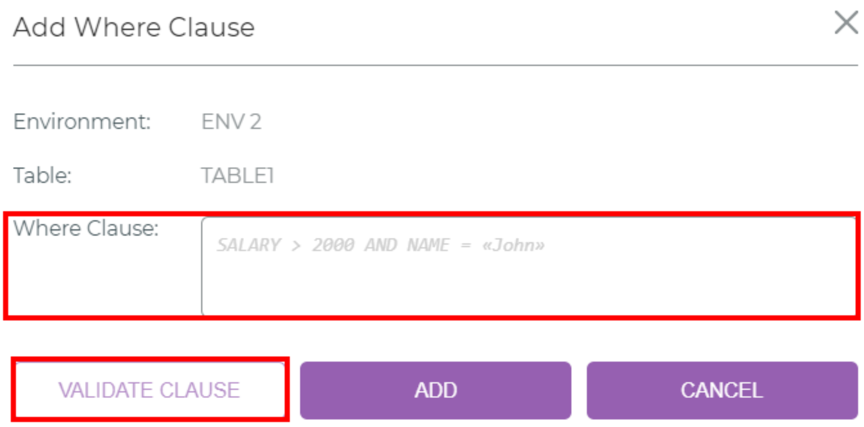
1. Click **Add Where Clause**.



dev02 - table_0
Last Masked: never

# A - Z ⇅	Column Name A - Z ⇅	Masking Rule	Parameters
1	column_1		
2	column_2		
3	column_3		

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



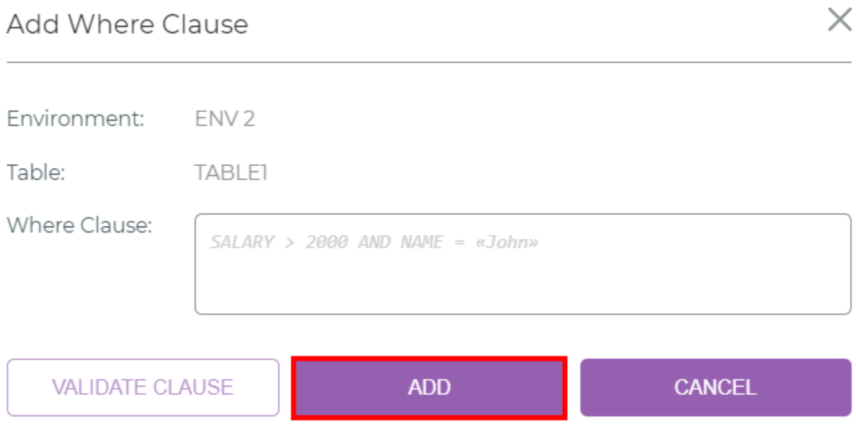
Add Where Clause

Environment: ENV 2

Table: TABLE1

Where Clause: SALARY > 2000 AND NAME = «John»

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


Add Where Clause

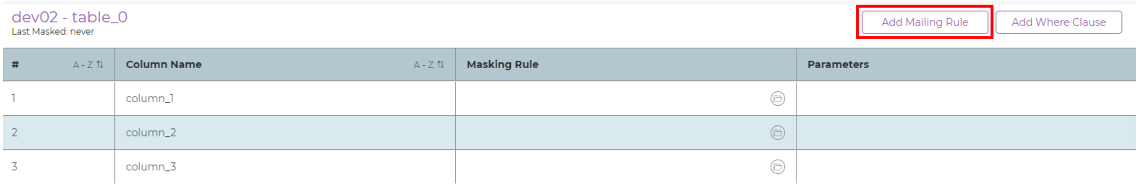
Environment: ENV 2

Table: TABLE1

Where Clause: SALARY > 2000 AND NAME = «John»

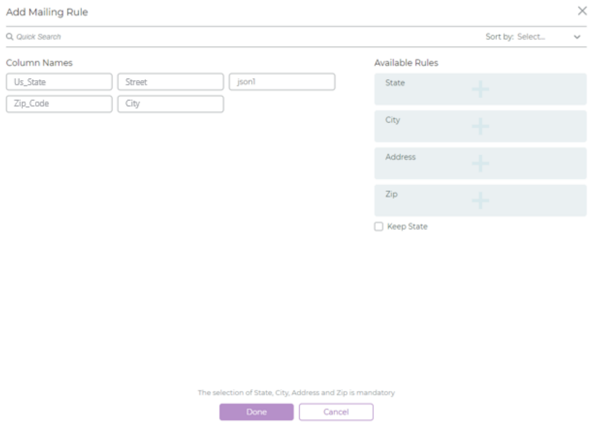
To add a Mailing Rule:

1. Click **Add Mailing Rule**.


dev02 - table_0
Last Masked: never

#	Column Name	Masking Rule	Parameters
1	column_1		
2	column_2		
3	column_3		

The Add Mailing Rule window appears.



Add Mailing Rule

Quick Search

Sort by: Select...

Column Names

Us_State

Street

json1

Zip_Code

City

Available Rules

State

City

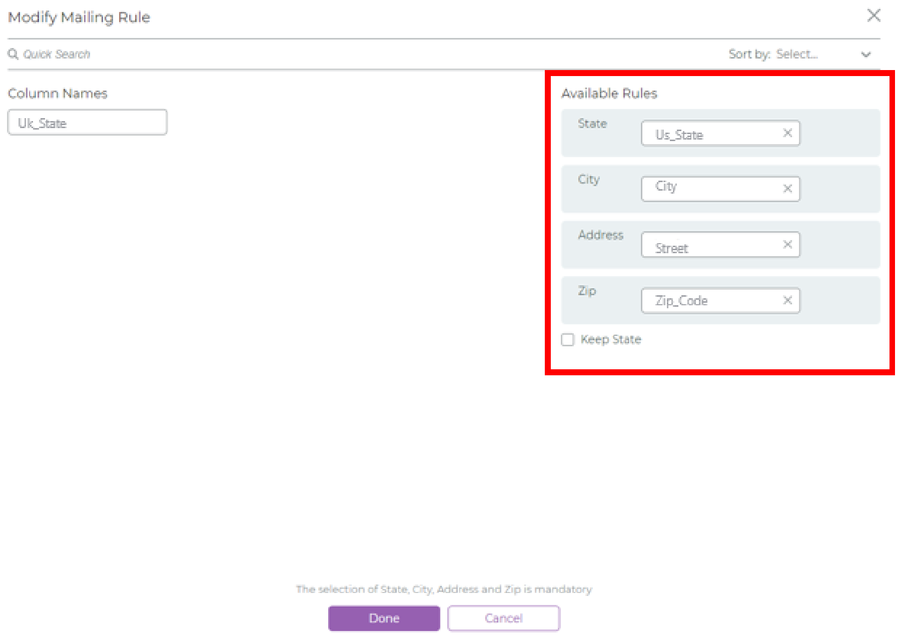
Address

Zip

□ Keep State

The selection of State, City, Address and Zip is mandatory

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



Modify Mailing Rule

Quick Search

Sort by: Select...

Column Names

Uk_State

Available Rules

State: Us_State

City: City

Address: Street

Zip: Zip_Code

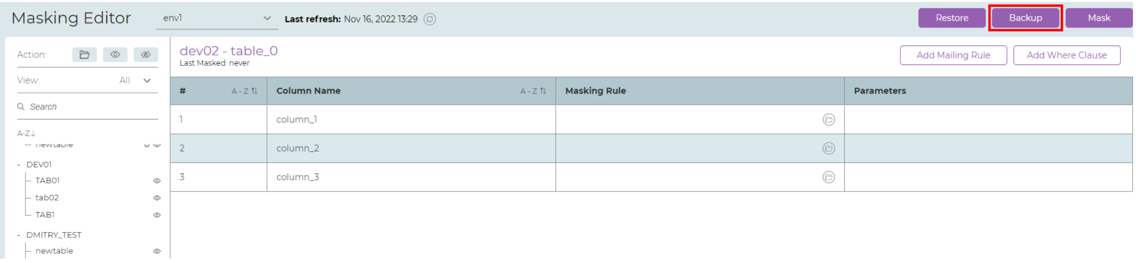
□ Keep State

The selection of State, City, Address and Zip is mandatory

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**.

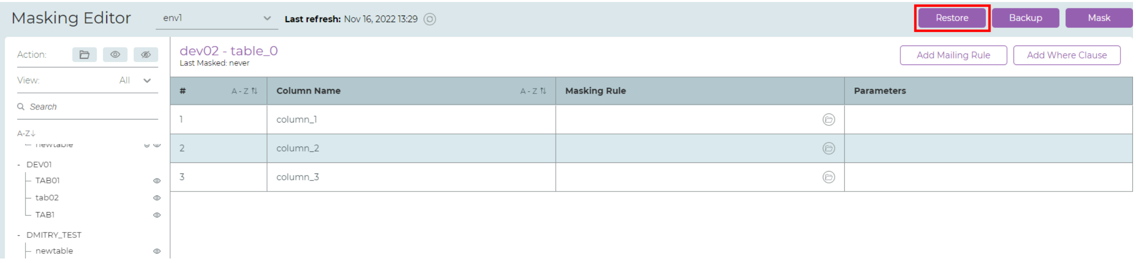
Restore and Backup:

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



#	Column Name	Masking Rule	Parameters
1	column_1		
2	column_2		
3	column_3		

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



#	Column Name	Masking Rule	Parameters
1	column_1		
2	column_2		
3	column_3		

11. Job Monitoring

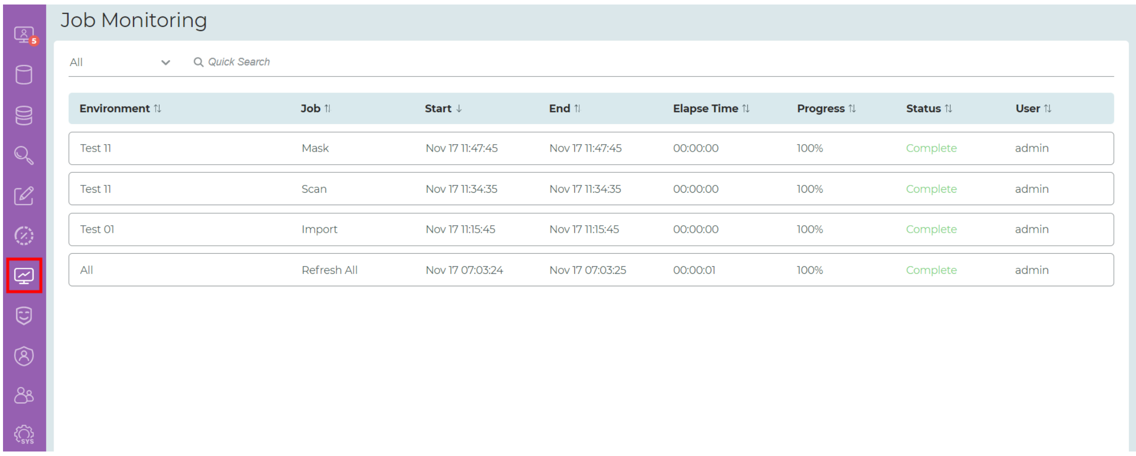
Job Monitoring is used to monitor the status of current system jobs. From the **Job Monitoring** window, you can:

- 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)**.



Job Monitoring

All

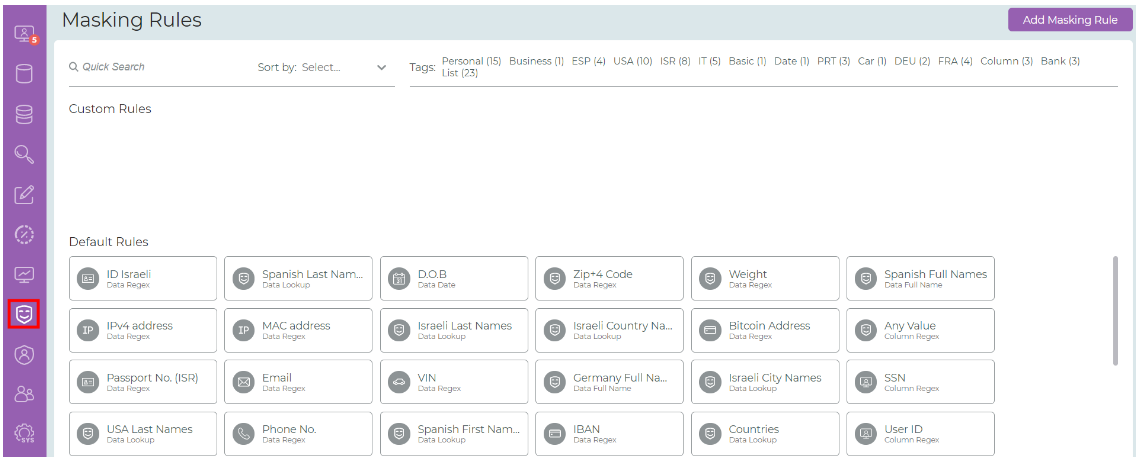
Environment ⇅	Job ⇅	Start ↓	End ⇅	Elapse Time ⇅	Progress ⇅	Status ⇅	User ⇅
Test 11	Mask	Nov 17 11:47:45	Nov 17 11:47:45	00:00:00	100%	Complete	admin
Test 11	Scan	Nov 17 11:34:35	Nov 17 11:34:35	00:00:00	100%	Complete	admin
Test 01	Import	Nov 17 11:15:45	Nov 17 11:15:45	00:00:00	100%	Complete	admin
All	Refresh All	Nov 17 07:03:24	Nov 17 07:03:25	00:00:01	100%	Complete	admin

12. 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:

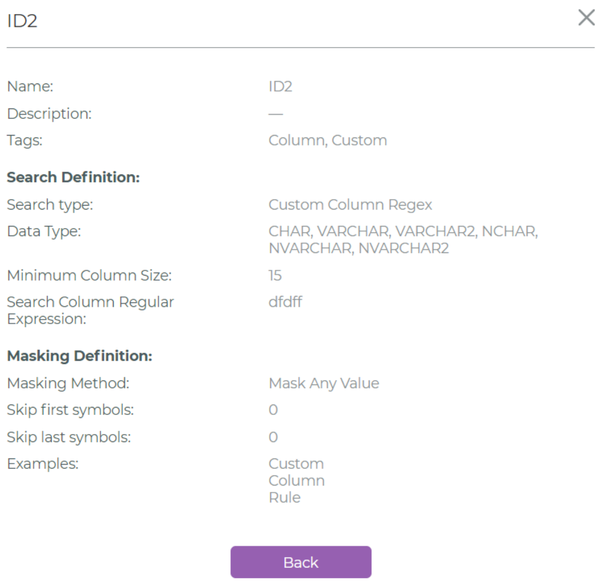
1. On the navigation bar, click **(Masking Rules)**.


Masking Rules
Add Masking Rule
Quick Search
Sort by: Select...
Tags: Personal (15) Business (1) ESP (4) USA (10) ISR (8) IT (5) Basic (1) Date (1) PRT (3) Car (1) DEU (2) FRA (4) Column (3) Bank (3) List (23)
Custom Rules
Default Rules

ID Israeli Data Regex	Spanish Last Nam... Data Lookup	D.O.B Data Date	Zip+4 Code Data Regex	Weight Data Regex	Spanish Full Names Data Full Name
IPv4 address Data Regex	MAC address Data Regex	Israeli Last Names Data Lookup	Israeli Country Na... Data Lookup	Bitcoin Address Data Regex	Any Value Column Regex
Passport No. (ISR) Data Regex	Email Data Regex	VIN Data Regex	Germany Full Na... Data Full Name	Israeli City Names Data Lookup	SSN Column Regex
USA Last Names Data Lookup	Phone No. Data Regex	Spanish First Nam... Data Lookup	IBAN Data Regex	Countries Data Lookup	User ID Column Regex

To see information about the masking rule:

1. On the masking rule, click ⓘ.

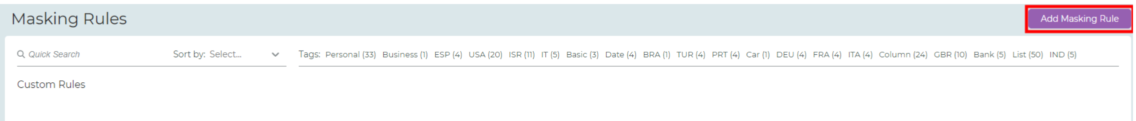


ID2

Name:	ID2
Description:	—
Tags:	Column, Custom
Search Definition:	
Search type:	Custom Column Regex
Data Type:	CHAR, VARCHAR, VARCHAR2, NCHAR, NVARCHAR, NVARCHAR2
Minimum Column Size:	15
Search Column Regular Expression:	dfdff
Masking Definition:	
Masking Method:	Mask Any Value
Skip first symbols:	0
Skip last symbols:	0
Examples:	Custom Column Rule

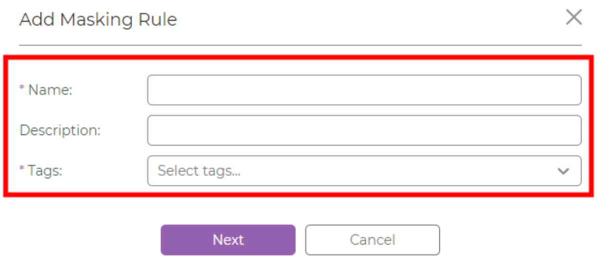
To add a new custom masking rule:

1. Click ADD MASKING RULE.



Masking Rules
Add Masking Rule
Quick Search
Sort by: Select...
Tags: Personal (33) Business (1) ESP (4) USA (20) ISR (11) IT (5) Basic (3) Date (4) BRA (1) TUR (4) PRT (4) Car (1) DEU (4) FRA (4) ITA (4) Column (24) GBR (10) Bank (5) List (50) IND (5)
Custom Rules

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



Add Masking Rule

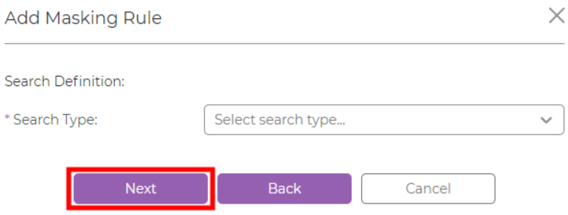
* Name:

Description:

* Tags: Select 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**.

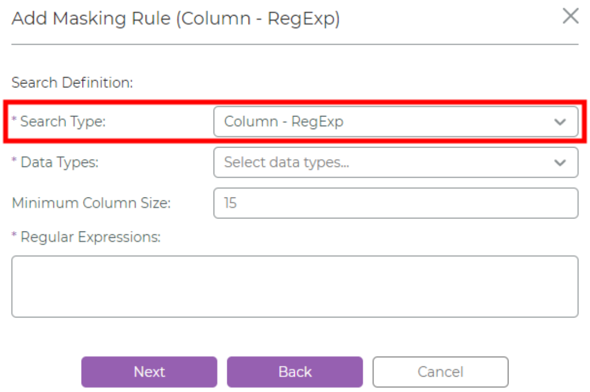


Add Masking Rule

Search Definition:

* Search Type: Select search type...

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.

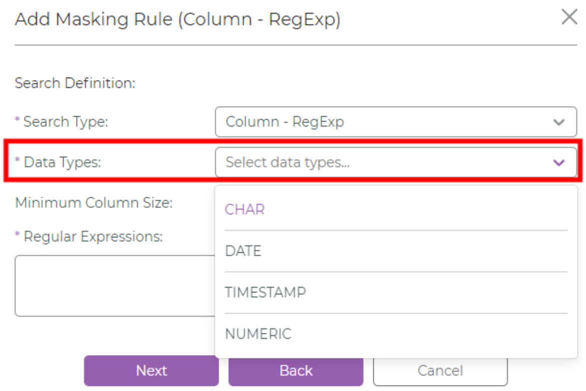


Add Masking Rule (Column - RegExp)

Search Definition:

* Search Type:	Column - RegExp
* Data Types:	Select data types...
Minimum Column Size:	15
* Regular Expressions:	

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



Add Masking Rule (Column - RegExp)

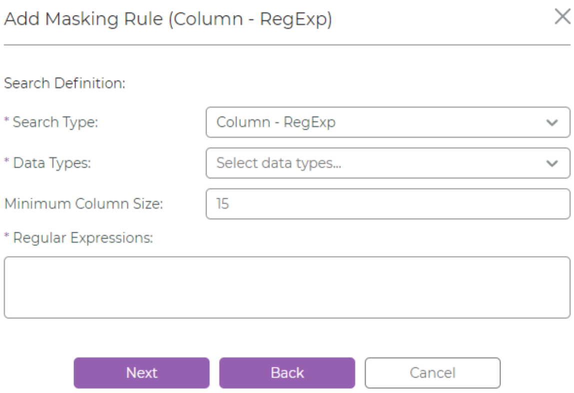
Search Definition:

* Search Type:	Column - RegExp
* Data Types:	Select data types...
Minimum Column Size:	
* Regular Expressions:	

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**.



Add Masking Rule (Column - RegExp)

Search Definition:

* Search Type: Column - RegExp

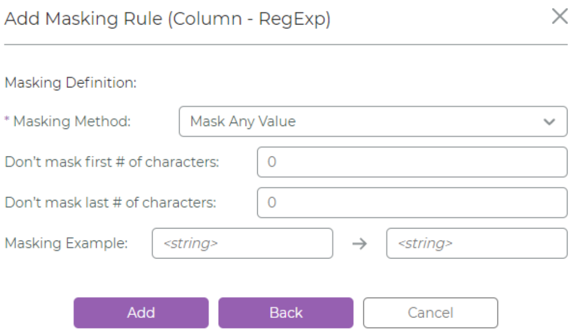
* Data Types: Select data types...

Minimum Column Size: 15

* 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.



Add Masking Rule (Column - RegExp)

Masking Definition:

* Masking Method: Mask Any Value

Don't mask first # of characters: 0

Don't mask last # of characters: 0

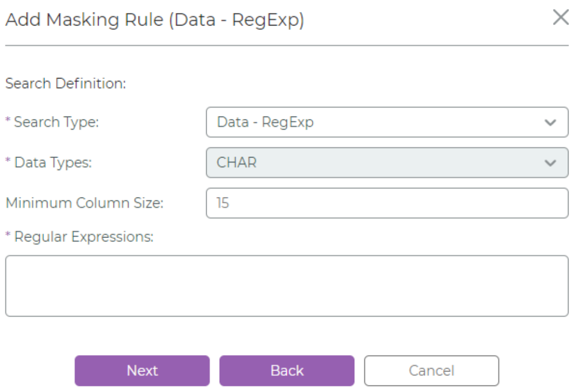
Masking Example: <string> → <string>

   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**.



Add Masking Rule (Data - RegExp)

Search Definition:

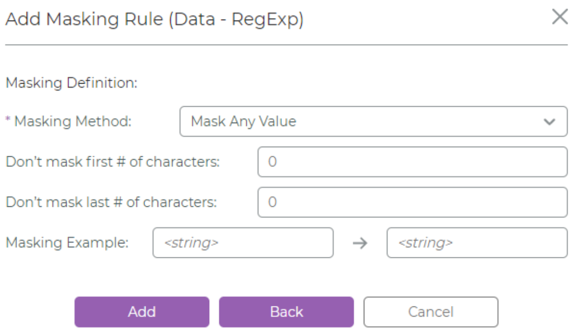
* Search Type: Data - RegExp
* Data Types: CHAR

Minimum Column Size: 15

* 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.



Add Masking Rule (Data - RegExp)

Masking Definition:

* Masking Method: Mask Any Value

Don't mask first # of characters: 0

Don't mask last # of characters: 0

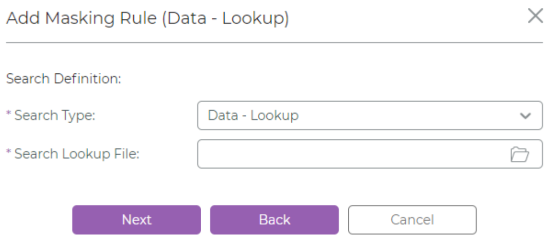
Masking Example: <string> → <string>

   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**.



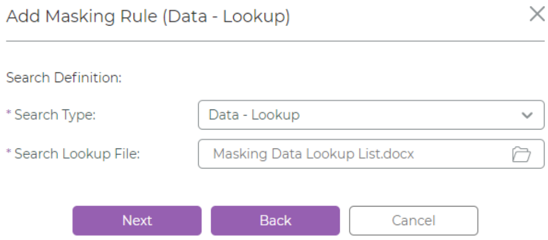
Add Masking Rule (Data - Lookup)

Search Definition:

* Search Type: Data - Lookup

* Search Lookup File:

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



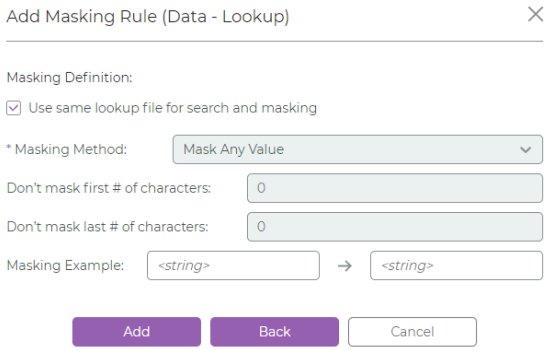
Add Masking Rule (Data - Lookup)

Search Definition:

* Search Type: Data - Lookup

* Search Lookup File: Masking Data Lookup List.docx

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



Add Masking Rule (Data - Lookup)

Masking Definition:

☑ Use same lookup file for search and masking

* Masking Method: Mask Any Value

Don't mask first # of characters: 0

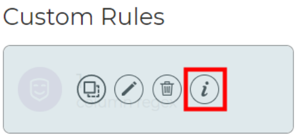
Don't mask last # of characters: 0

Masking Example: <string> → <string>

   d. Click **ADD**.

The new masking rule appears.

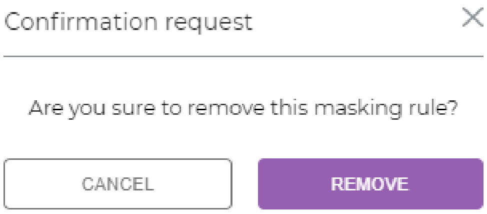
To see information about a custom masking rule:



1. On the masking rule, click ⓘ .

To delete a custom masking rule:

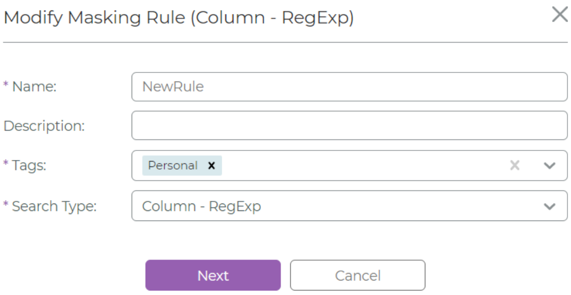
1. On the masking rule, click 🗑 .
2. Click **REMOVE** to confirm the deletion, or **CANCEL** to exit without deleting the masking rule.


Confirmation request

Are you sure to remove this masking rule?

To modify a custom masking rule:

1. On the masking rule, click ✎.
2. The **Modify Masking Rule** window appears. Modify the custom masking rule details as required.



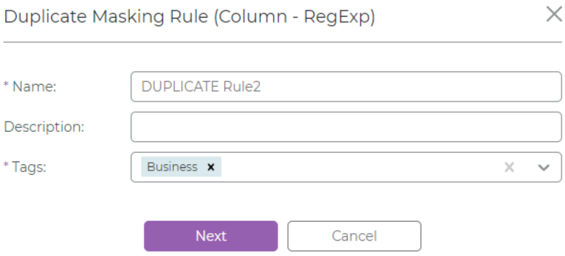
Modify Masking Rule (Column - RegExp)

* Name:	NewRule
Description:	
* Tags:	Personal
* Search Type:	Column - RegExp

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

To duplicate a masking rule:

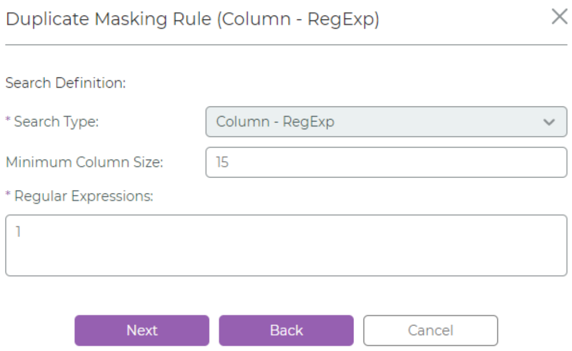
1. On the masking rule, click ⧉.
2. Provide a name.



Duplicate Masking Rule (Column - RegExp)

* Name:	DUPLICATE Rule2
Description:	
* Tags:	Business

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



Duplicate Masking Rule (Column - RegExp)

Search Definition:

* Search Type: Column - RegExp

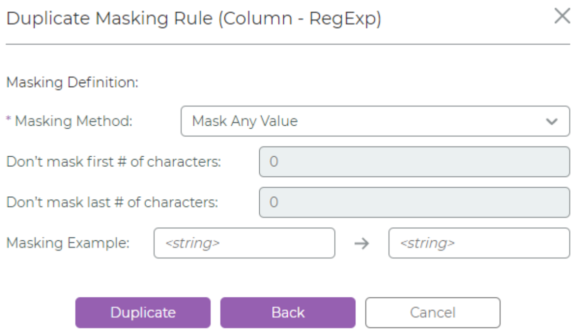
Minimum Column Size: 15

* Regular Expressions:

1

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

5. Click **NEXT**.



Duplicate Masking Rule (Column - RegExp)

Masking Definition:

* Masking Method: Mask Any Value

Don't mask first # of characters: 0

Don't mask last # of characters: 0

Masking Example: <string> → <string>

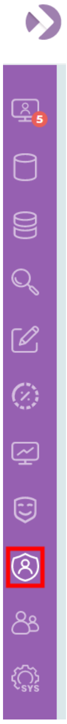
6. Click **Duplicate**.

13. Managing Privacy Policies

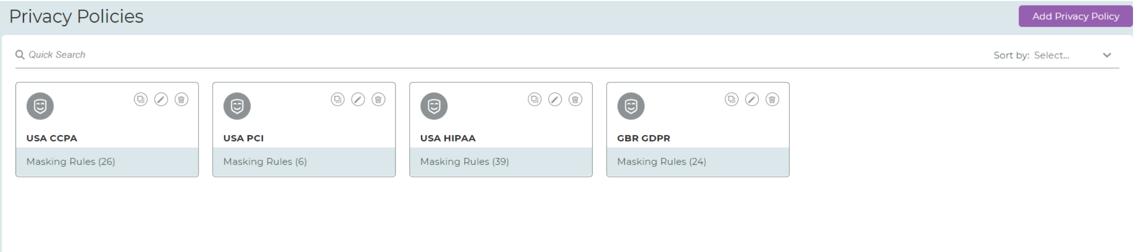
A **Privacy Policy** is a set of masking rules used to scan and mask following a specified privacy regulation such as GDPR, CCPA and HIPAA or to the organization privacy rules. This section describes how to define and manage the privacy policies.

To view available privacy policies:

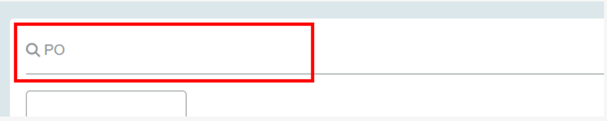
1. On the navigation bar, click 🛡 **(Privacy Policies)**.



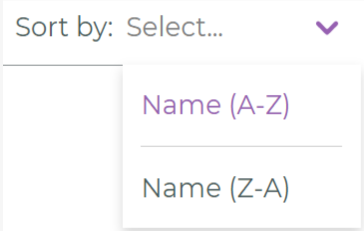
2. The **Privacy Policies** window appears displaying all privacy policies that have been added to the system.



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

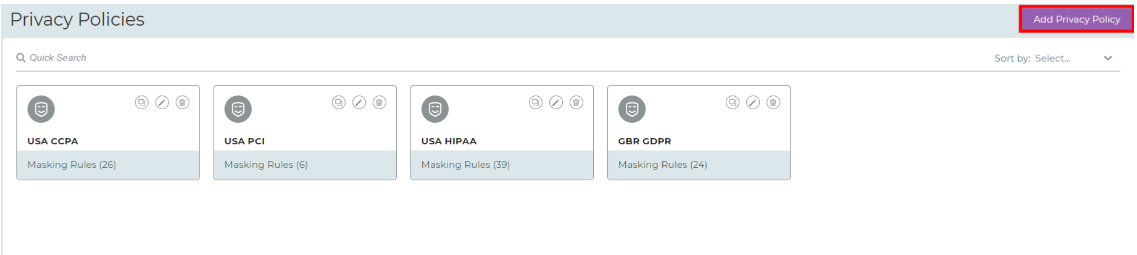


You can display the list in ascending or descending alphabetical order.

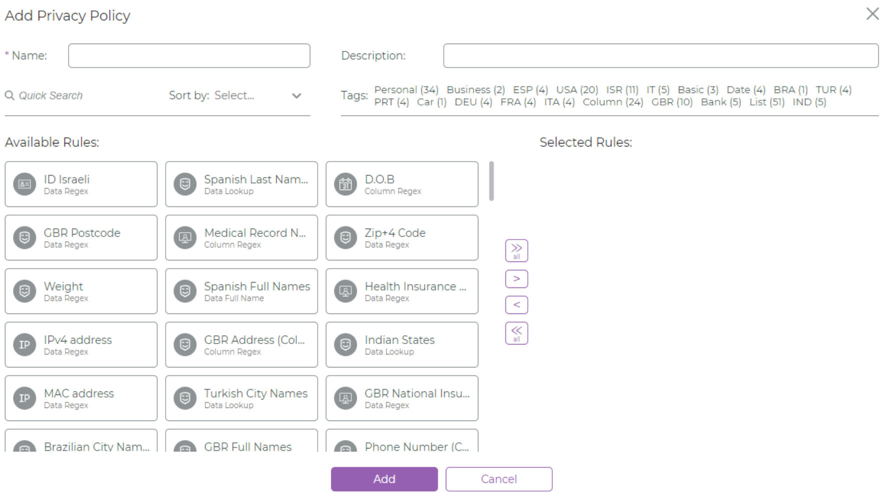


To add a new privacy policy:

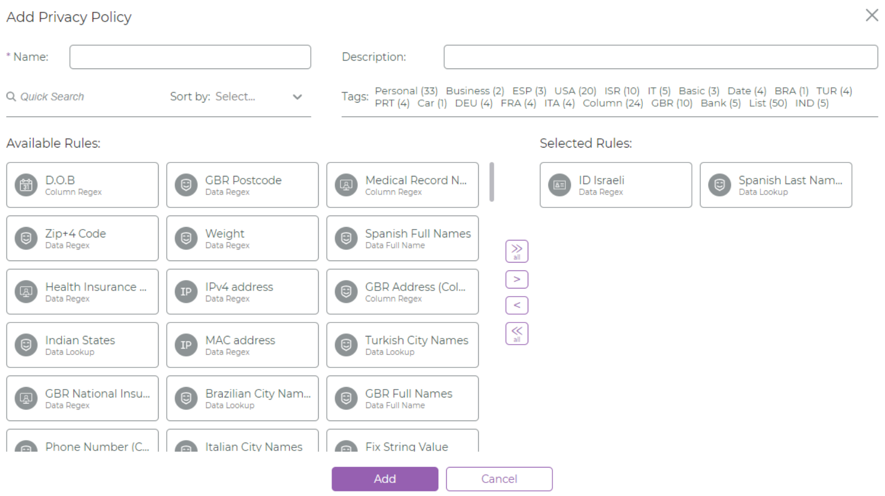
1. Click **Add Privacy Policy**.



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.



Add Privacy Policy

* Name:

Description:

Quick Search Sort by: Select...

Tags: Personal (33) Business (2) ESP (3) USA (20) ISR (10) IT (5) Basic (3) Date (4) BRA (1) TUR (4) PRT (4) Car (1) DEU (4) FRA (4) ITA (4) Column (24) GBR (10) Bank (5) List (50) IND (5)

Available Rules:

D.O.B Column Regex	GBR Postcode Data Regex	Medical Record N... Column Regex
Zip+4 Code Data Regex	Weight Data Regex	Spanish Full Names Data Full Name
Health Insurance ... Data Regex	IPv4 address Data Regex	GBR Address (Col... Column Regex
Indian States Data Lookup	MAC address Data Regex	Turkish City Names Data Lookup
GBR National Insu... Data Regex	Brazilian City Nam... Data Lookup	GBR Full Names Data Full Name
Phone Number (C...	Italian City Names	Fix String Value

Selected Rules:

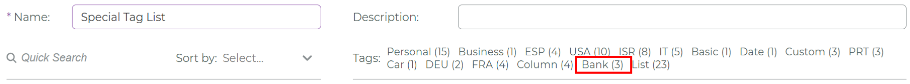
ID Israeli Data Regex	Spanish Last Nam... Data Lookup

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**).



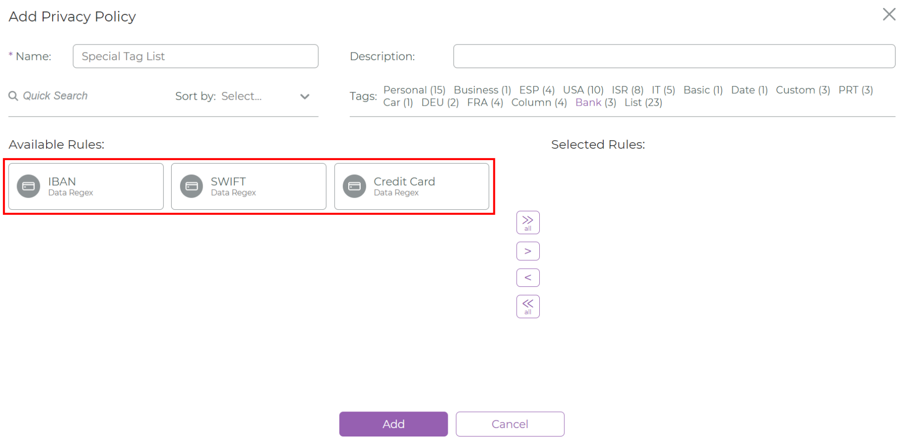
* Name: Special Tag List

Description:

Quick Search Sort by: Select...

Tags: Personal (15) Business (1) ESP (4) USA (10) ISR (8) IT (5) Basic (1) Date (1) Custom (3) PRT (3) Car (1) DEU (2) FRA (4) Column (4) Bank (3) List (23)

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



Add Privacy Policy

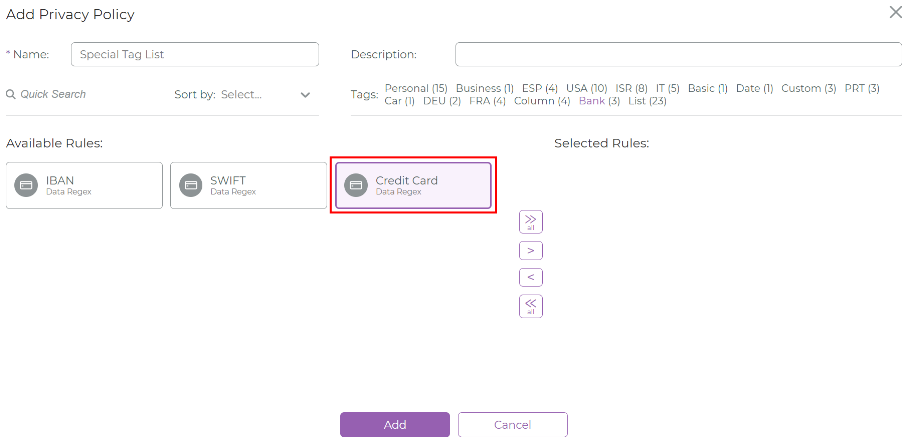
* Name: Special Tag List

Description:

Quick Search
Sort by: Select...
Tags: Personal (15) Business (1) ESP (4) USA (10) ISR (8) IT (5) Basic (1) Date (1) Custom (3) PRT (3) Car (1) DEU (2) FRA (4) Column (4) Bank (3) List (23)
Available Rules:
IBAN
Data Regex
SWIFT
Data Regex
Credit Card
Data Regex
Selected Rules:
all
>
<
all
Add
Cancel

3. Select a rule.

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



Add Privacy Policy

* Name: Special Tag List

Description:

Quick Search
Sort by: Select...
Tags: Personal (15) Business (1) ESP (4) USA (10) ISR (8) IT (5) Basic (1) Date (1) Custom (3) PRT (3) Car (1) DEU (2) FRA (4) Column (4) Bank (3) List (23)
Available Rules:
IBAN
Data Regex
SWIFT
Data Regex
Credit Card
Data Regex
Selected Rules:
all
>
<
all
Add
Cancel

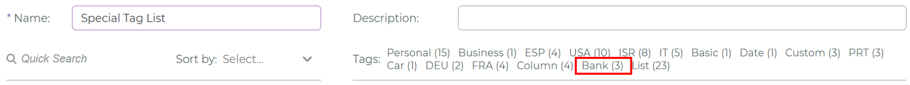
5. Click **Add**.

- 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 < .

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



* Name: Special Tag List

Description:

Quick Search

Sort by: Select...

Tags: Personal (15) Business (1) ESP (4) USA (10) ISR (8) IT (5) Basic (1) Date (1) Custom (3) PRT (3) Car (1) DEU (2) FRA (4) Column (4) Bank (3) List (23)

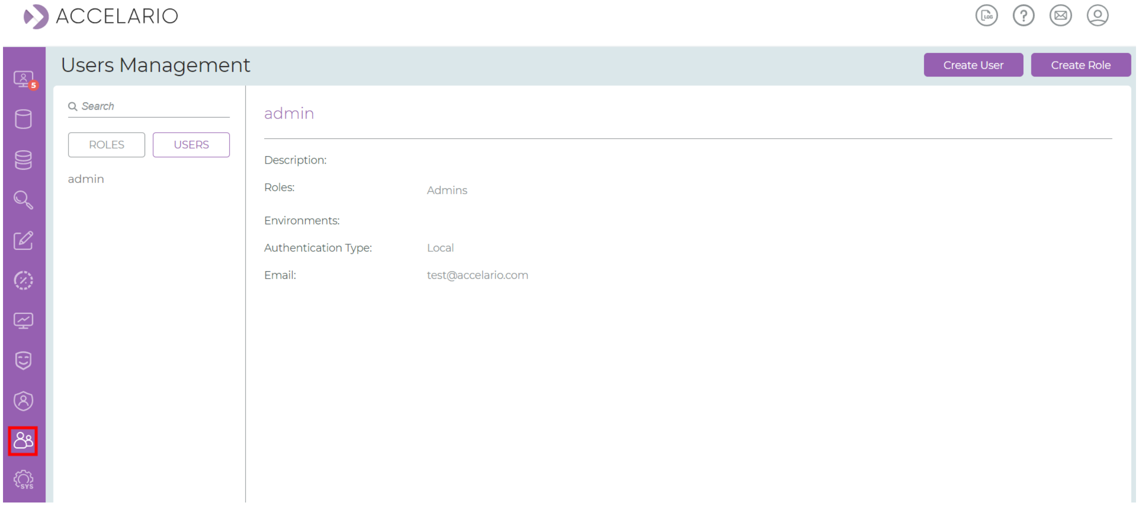
14. Managing Users and Roles

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**).



admin

Description:

Roles: Admins

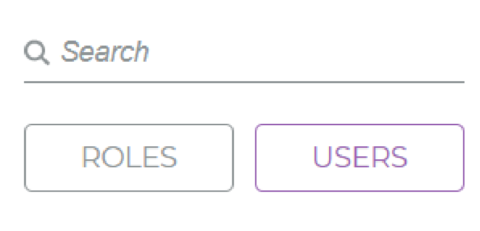
Environments:

Authentication Type: Local

Email: test@accelario.com

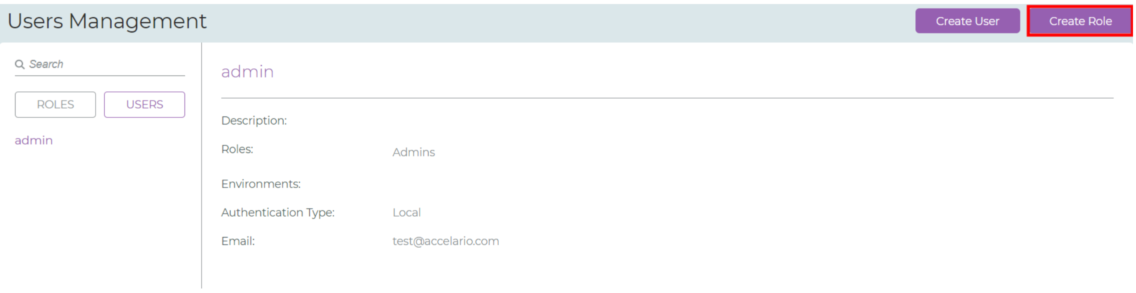
You can quickly locate a user by typing its letters on the **Search** bar. The list updates promptly.

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



To create a new role:

1. Click **Create Role**.



admin

Description:

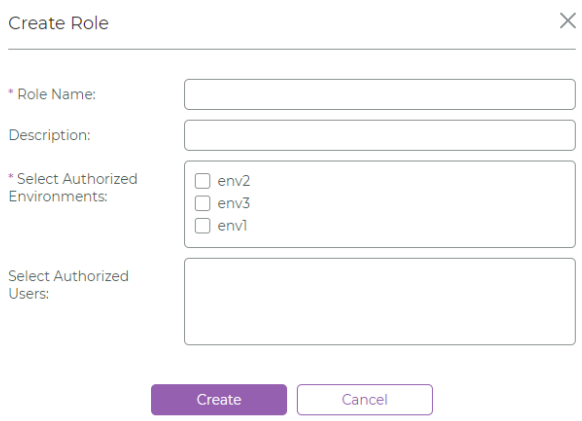
Roles: Admins

Environments:

Authentication Type: Local

Email: test@accelario.com

2. Fill in the details:



Create Role

* Role Name:

Description:

* Select Authorized Environments:

□ env2

□ env3

□ env1

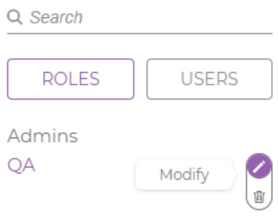
Select Authorized Users:

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

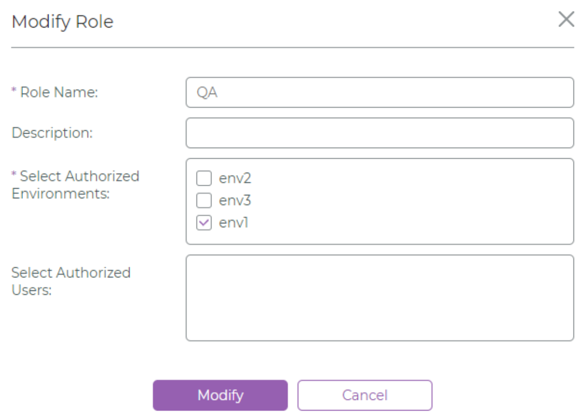
3. Click **Create**.

To edit role details:

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



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



Modify Role

* Role Name: QA

Description:

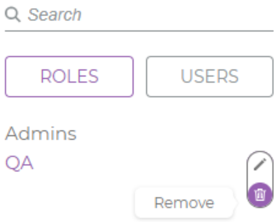
* Select Authorized Environments:
□ env2
□ env3
☑ env1

Select Authorized Users:

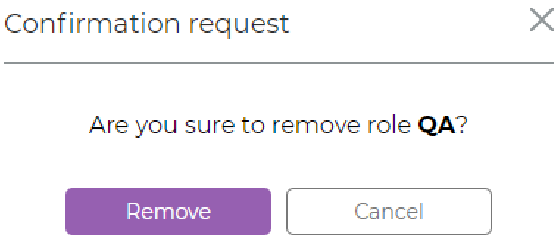
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

To delete a role:

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



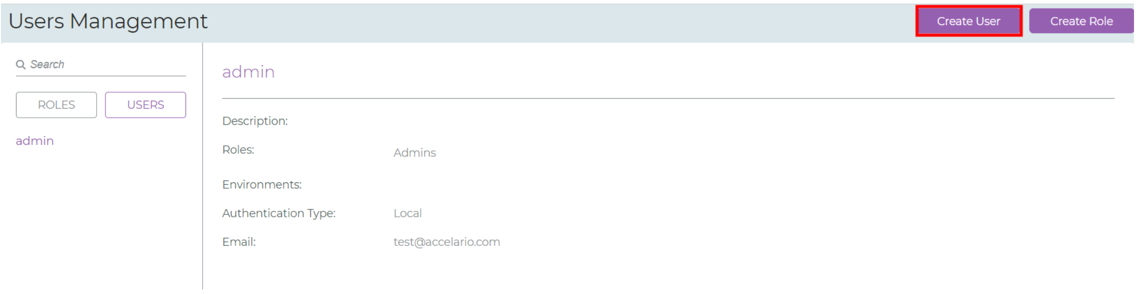
2. Click **Remove** to confirm the deletion, or **Cancel** to exit without deleting the role.


Confirmation request

Are you sure to remove role **QA**?

To add a new user:

1. Click **Create User**.



admin

Description:

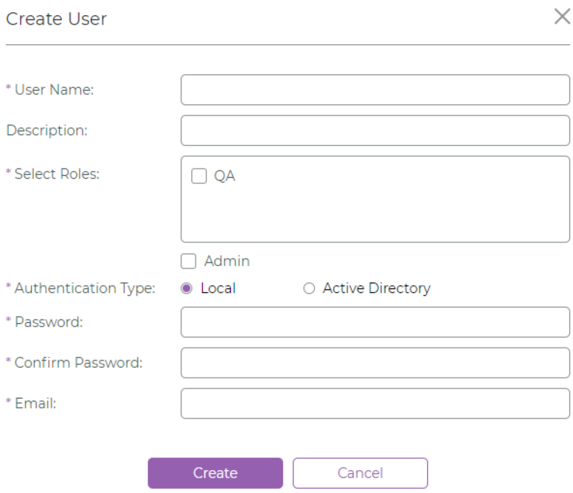
Roles: Admins

Environments:

Authentication Type: Local

Email: test@accelario.com

2. Fill in the details:



Create User

* User Name:

Description:

* Select Roles: □ QA

□ Admin

* Authentication Type: ● Local ○ Active Directory

* Password:

* Confirm Password:

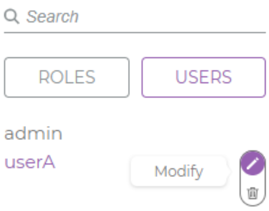
* Email:

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

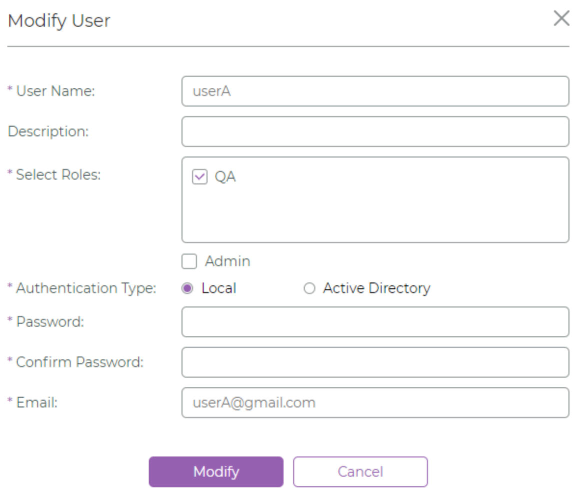
3. Click **Create**.

To edit user details:

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



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



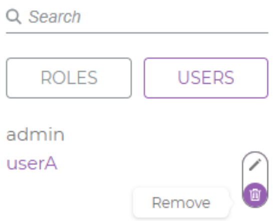
Modify User

* User Name:	userA
Description:	
* Select Roles:	☑ QA
	□ Admin
* Authentication Type:	● Local ○ Active Directory
* Password:	
* Confirm Password:	
* Email:	userA@gmail.com

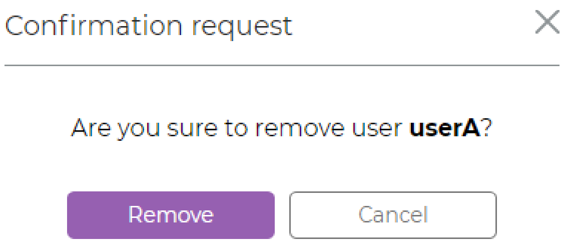
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

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.


Confirmation request

Are you sure to remove user **userA**?

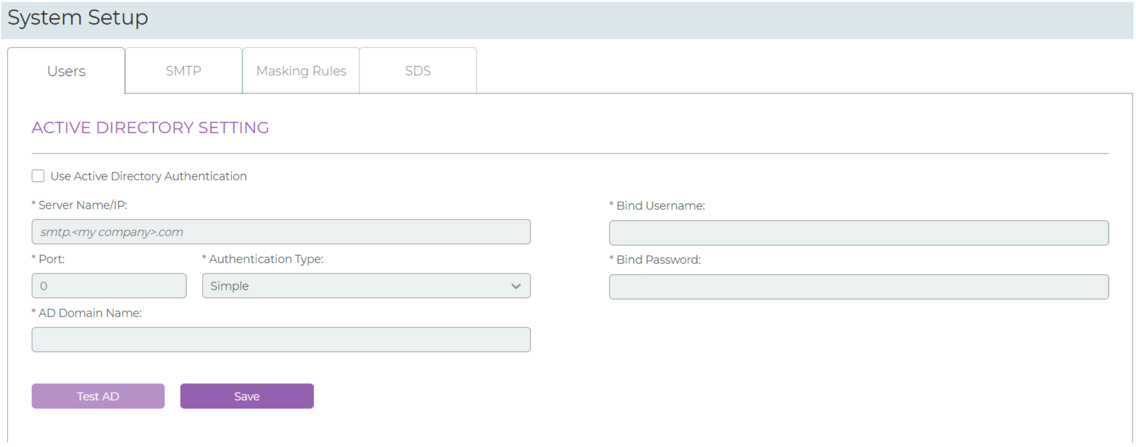
15. System Setup

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.



System Setup

ACTIVE DIRECTORY SETTING

☐ Use Active Directory Authentication

* Server Name/IP: *smtp.<my company>.com*

* Port: 0

* Authentication Type: Simple

* AD Domain Name:

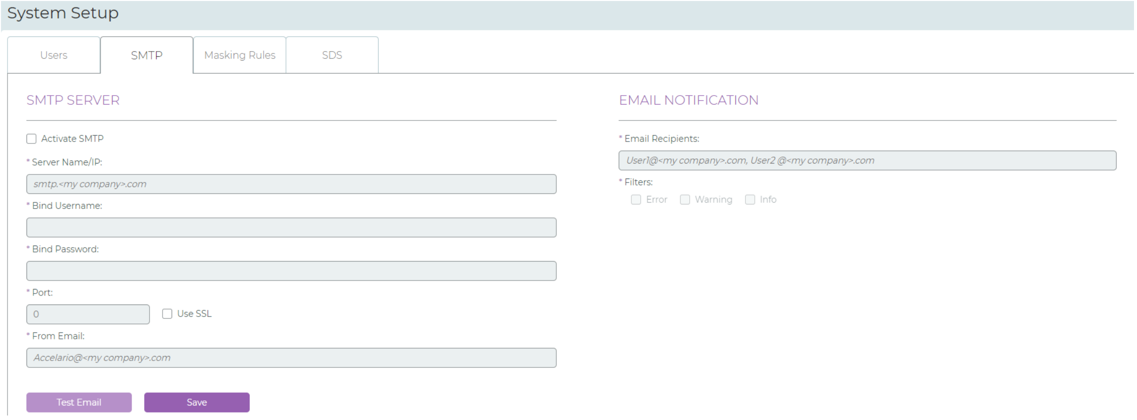
* Bind Username:

* Bind Password:

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.



System Setup

SMTP SERVER

□ Activate SMTP

*Server Name/IP: *smtp.<my company>.com*

*Bind Username:

*Bind Password:

*Port: 0 □ Use SSL

*From Email: *Accelario@<my company>.com*

EMAIL NOTIFICATION

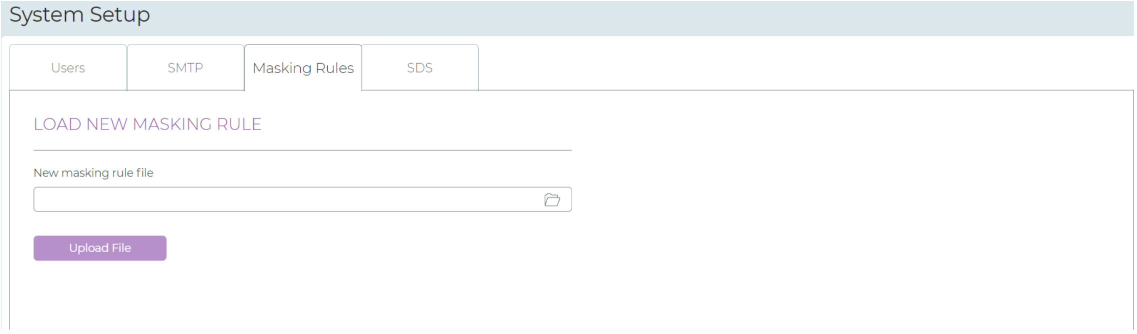
*Email Recipients: *User1@<my company>.com, User2 @<my company>.com*

*Filters: □ Error □ Warning □ Info

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**.



System Setup

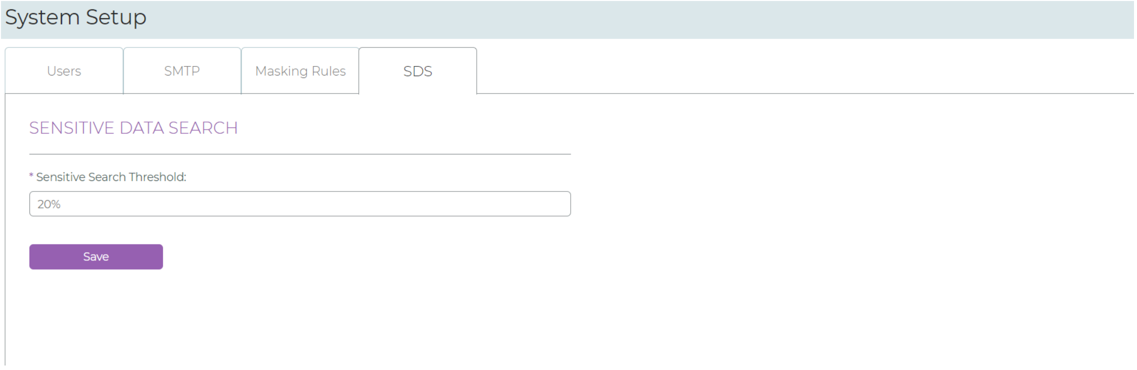
LOAD NEW MASKING RULE

New masking rule file

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

To modify the sensitive search threshold:

1. Click **SDS**.



System Setup

SENSITIVE DATA SEARCH

* Sensitive Search Threshold:

20%

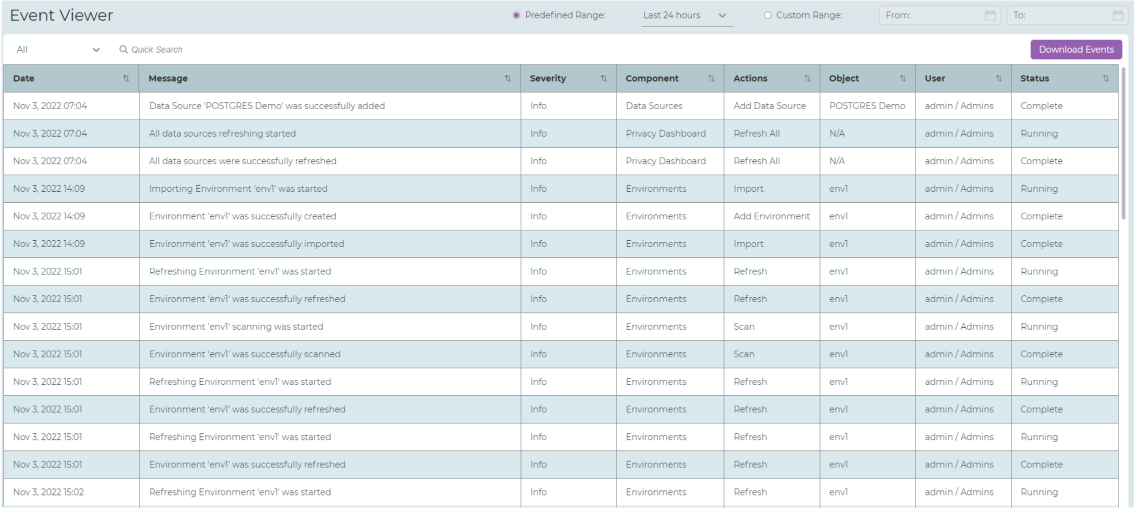
2. Enter the new threshold.
3. Click **Save**.

16. 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).



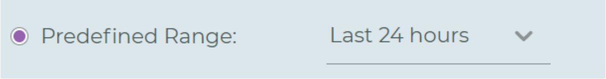
Date	Message	Severity	Component	Actions	Object	User	Status
Nov 3, 2022 07:04	Data Source 'POSTGRES Demo' was successfully added	Info	Data Sources	Add Data Source	POSTGRES Demo	admin / Admins	Complete
Nov 3, 2022 07:04	All data sources refreshing started	Info	Privacy Dashboard	Refresh All	N/A	admin / 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 Quick Search bar.

To filter events for a specified time period:

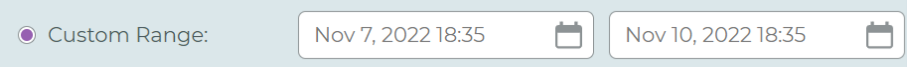
1. Select:
   a. **Predefined Range**.



● Predefined Range: Last 24 hours

   or

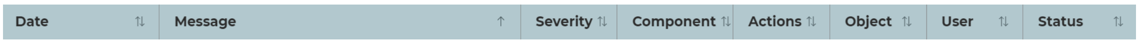
   b. Enter a **Custom Range**.



● Custom Range: Nov 7, 2022 18:35 Nov 10, 2022 18:35

To sort events:

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



Date ⇅	Message ↑	Severity ⇅	Component ⇅	Actions ⇅	Object ⇅	User ⇅	Status ⇅

To download events to a file:

1. Click Download Events.