



Accelario

Data Masking Module

User Guide
V20.0

January 2023

Contents

1. Product Overview	3
1.1. Privacy Dashboard	3
1.2. Data Sources	4
1.3. Environments	4
1.4. Sensitive Data Search	4
1.5. Masking Editor	5
1.6. Masking Rules	5
1.7. Privacy Policies	5
1.8. Users	6
1.9. System Setup	6
1.10. Job Monitoring	7
1.11. Event Viewer	7
2. Login to the Data Masking Module	8
3. Getting to Know the GUI	9
4. Privacy Dashboard	10
5. Managing Data Sources	14
6. Managing Environments	20
7. Searching for Sensitive Data	28
8. Masking Editor - Editing Masking Rules and Running Masking Operation	32
9. Job Monitoring	44
10. Managing Masking Rules	45
11. Managing Privacy Policies	54
12. Managing Users and Roles	60
13. System Setup	68
14. Event Viewer	71

1. Product Overview

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

It contains the following components:

- > [Privacy Dashboard](#)
- > [Data Sources](#)
- > [Environments](#)
- > [Sensitive Data Search](#)
- > [Masking Editor](#)
- > [Masking Rules](#)
- > [Privacy Policies](#)
- > [Users](#)
- > [System Setup](#)
- > [Job Monitoring](#)
- > [Event Viewer](#)

1.1. Privacy Dashboard

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

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

For more information, see [Privacy Dashboard](#).

1.2. Data Sources

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

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



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

For more information, see [Managing Data Sources](#).

1.3. Environments

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

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

For more information, see [Managing Environments](#).

1.4. Sensitive Data Search

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

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

For more information, see [Searching for Sensitive Data](#).

1.5. Masking Editor

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

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

For more information, see [Masking Editor - Editing Masking Rules and Running Masking Operation](#).

1.6. Masking Rules

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

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

For more information, see [Managing Masking Rules](#).

1.7. Privacy Policies

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

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

For more information, see [Managing Privacy Policies](#).

1.8. Users

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

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



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

From the Users Management window, you can:

- > Create and modify users
- > Create and modify roles

For more information, see [Managing Users and Roles](#).

1.9. System Setup

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

- > Configure Active Directory Authorization
- > Configure SMTP configuration



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

For more information, see [System Setup](#).

1.10. Job Monitoring

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

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



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

For more information, see [Job Monitoring](#).

1.11. Event Viewer

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

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

For more information, see [Event Viewer](#).

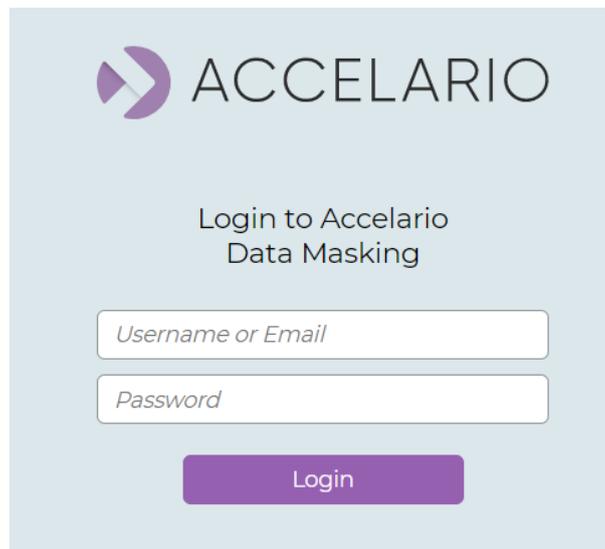
2. Login to the Data Masking Module

To login in to the Data Masking Module:



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

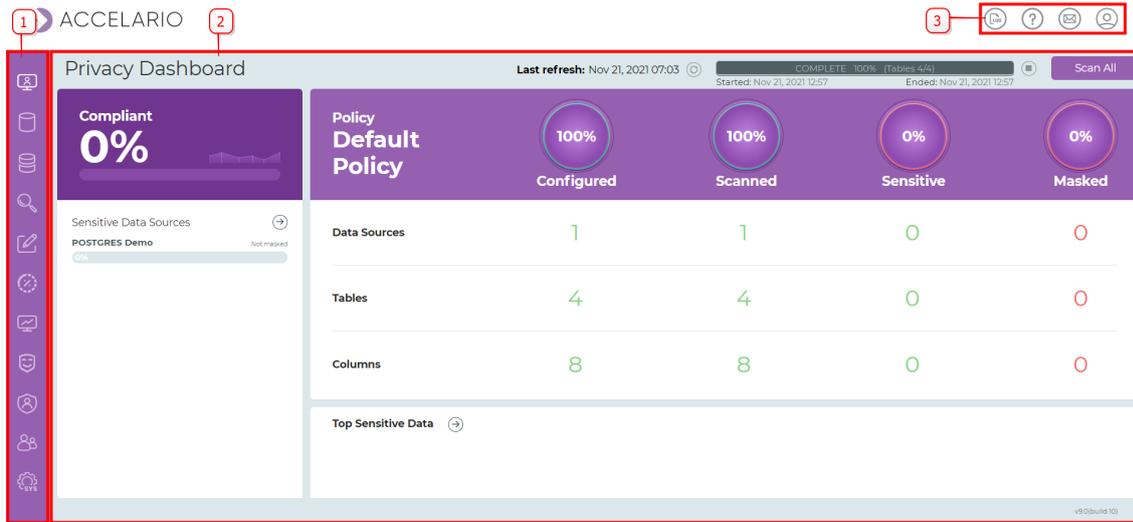
1. Enter your **Username** or **Email**.
2. Enter your **Password**.
3. Click **Login**.



The screenshot shows the Accelario login interface. At the top left is the Accelario logo, which consists of a purple arrow pointing right followed by the word "ACCELARIO" in a sans-serif font. Below the logo, the text "Login to Accelario Data Masking" is centered. There are two input fields: the first is labeled "Username or Email" and the second is labeled "Password". Below these fields is a purple button with the text "Login" in white.

3. Getting to Know the GUI

The following image and table describe the Data Masking Module.

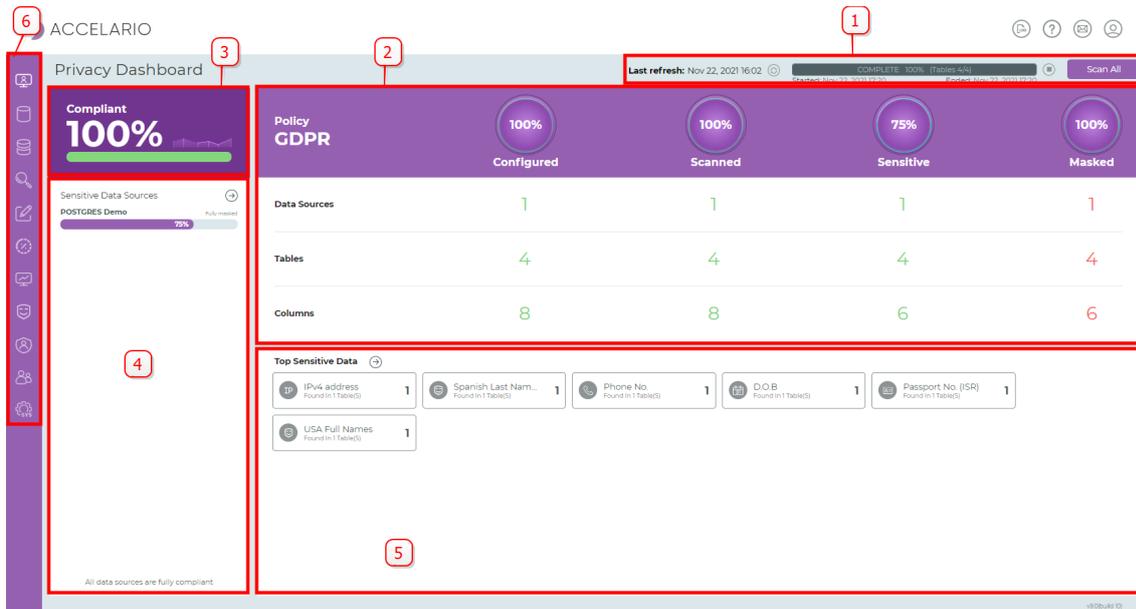


#	Item	Description
1	Navigation bar	Used to put content in the main work area.
2	Main Work Area	Main work area where you perform tasks
3	Task bar	System tasks

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

4. Privacy Dashboard

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



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

To scan for potential sensitive data:

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

Scan Sensitive Data ✕

Environment: All

* Privacy Policy:

* Parallel Processes:

* Number of rows to scan:

Auto Refresh

Incremental



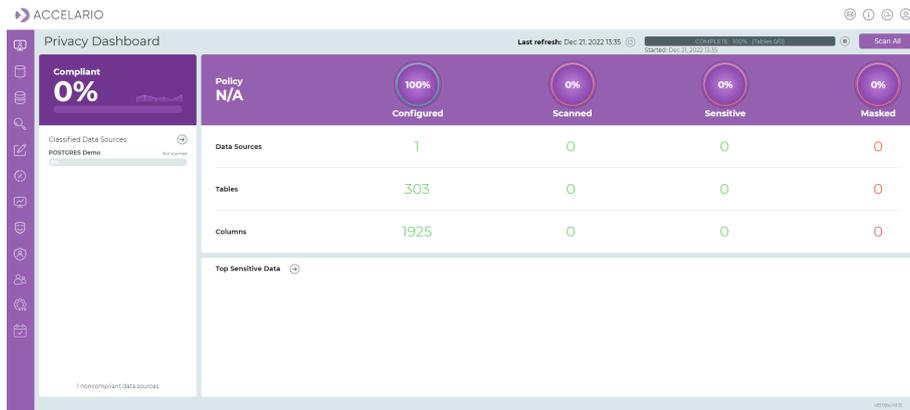
In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

To stop a scan:

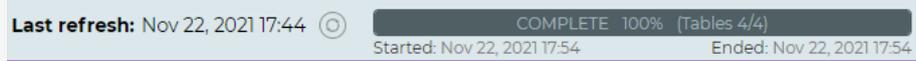
1. Click .

To do a Refresh All:

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

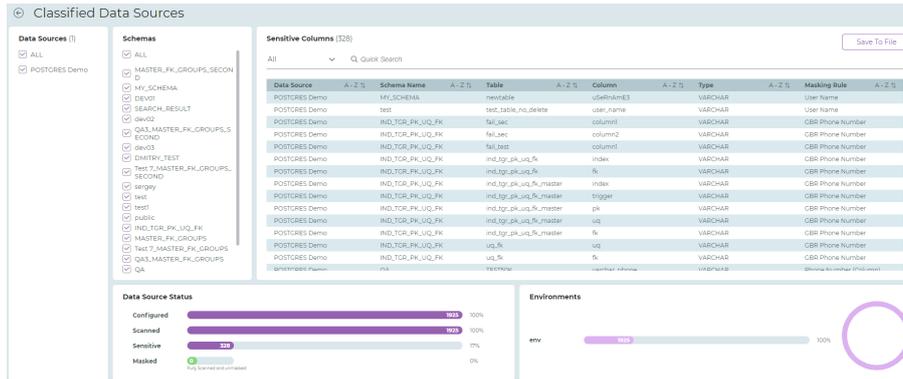


On the scan bar, you can see the following scan information:



To see the potential classified data sources:

1. Click **Classified Data Sources** .



Classified Data Sources

Data Sources (1)

- ALL
- POSTGRES Demo

Schemas

- MASTER_FK_GROUPS,SECON D
- MY_SCHEMA
- EBN01
- SEARCH_RESULT
- jav02
- QAS_MASTER_FK_GROUPS,S ECON0
- jav03
- DMTRIV_TEST
- Test_7_MASTER_FK_GROUPS, SECON0
- serpy
- test
- test1
- test2
- public
- IND_TOR_FK_IJQ_FK
- MASTER_FK_GROUPS
- Test_7_MASTER_FK_GROUPS
- QAS_MASTER_FK_GROUPS
- QA

Sensitive Columns (328)

Data Source	A - Z %	Schema Name	A - Z %	Table	A - Z %	Column	A - Z %	Type	A - Z %	Masking Rule	A - Z %
POSTGRES Demo		MY_SCHEMA		newtable		userIdName3		VARCHAR		User Name	
POSTGRES Demo		test		test_table_no_delete		user_name		VARCHAR		User Name	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		tbl_jac		column1		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		tbl_jac		column2		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		tbl_jac		column1		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		ind_tgr_pk_uq_fk		index		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		ind_tgr_pk_uq_fk		fk		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		ind_tgr_pk_uq_fk_master		index		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		ind_tgr_pk_uq_fk_master		trigger		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		ind_tgr_pk_uq_fk_master		pk		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		ind_tgr_pk_uq_fk_master		uq		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		ind_tgr_pk_uq_fk_master		fk		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		uq_fk		uq		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		uq_fk		fk		VARCHAR		GBR Phone Number	
POSTGRES Demo		IND_TOR_FK_IJQ_FK		uq_fk		fk		VARCHAR		GBR Phone Number	
SPRINTIPET P.../...		QA		TESTENV		userchar_phone		VARCHAR		GBR Phone Number (Phone)	

Data Source Status

- Configured: 100%
- Scanned: 100%
- Sensitive: 77%
- Masked: 0%

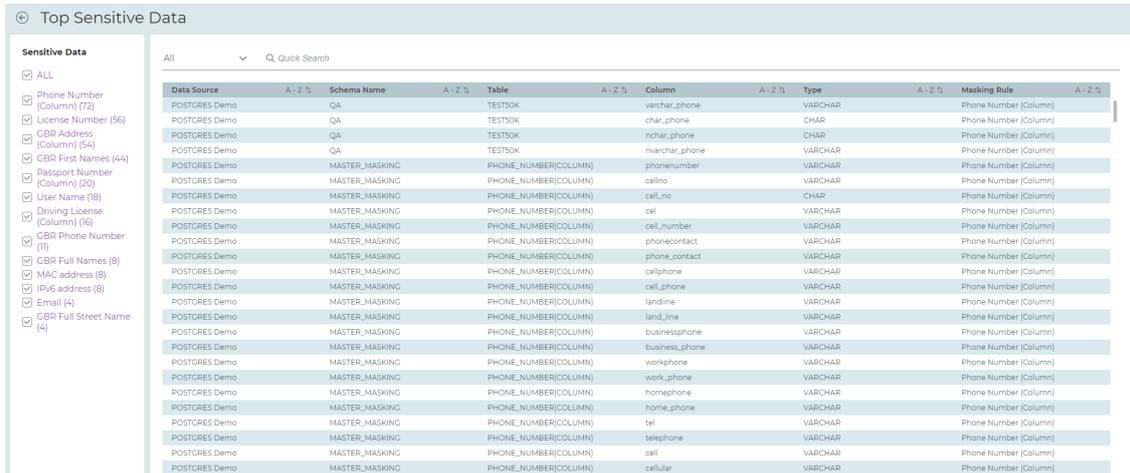
Environments

- env: 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)
- CBR Address (Column) (54)
- CBR First Names (44)
- Passport Number (Column) (20)
- User Name (18)
- Driving License (Column) (16)
- CBR Phone Number (7)
- CBR Full Names (3)
- MAC address (3)
- IPv6 address (8)
- Email (4)
- CBR Full Street Name (4)

Sensitive Columns (328)

Data Source	A - Z %	Schema Name	A - Z %	Table	A - Z %	Column	A - Z %	Type	A - Z %	Masking Rule	A - Z %
POSTGRES Demo		QA		TESTSOK		varchar_phone		VARCHAR		Phone Number (Column)	
POSTGRES Demo		QA		TESTSOK		char_phone		CHAR		Phone Number (Column)	
POSTGRES Demo		QA		TESTSOK		nchar_phone		CHAR		Phone Number (Column)	
POSTGRES Demo		QA		TESTSOK		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)		celno		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. Managing Data Sources

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



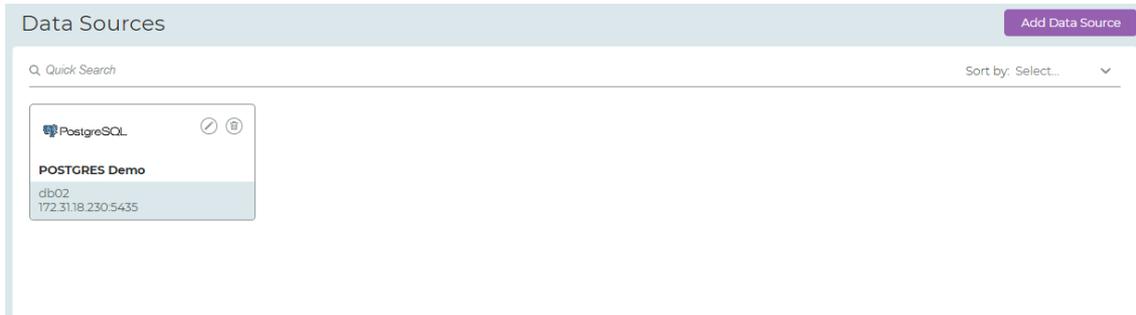
Only a user with **Admin** privileges can see or edit **Data Sources**.

To see available data sources:

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



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



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

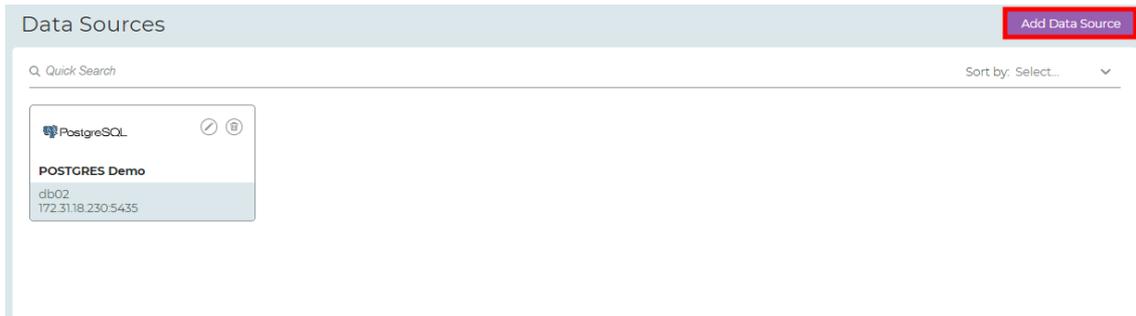


You can display the list in ascending or descending alphabetical order.

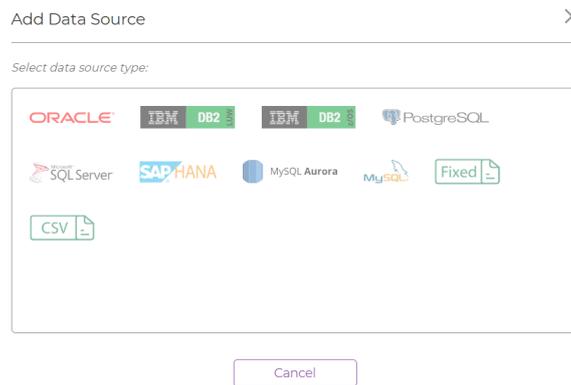


To add a new data source:

1. Click **Add Data Source**.



2. Select source data type.



3. Fill in the data source details.

Add Data Source PostgreSQL X

* Name:

* Host:

* Port:

* DB name:

* User:

* Password:

Wallet:

Create Environment

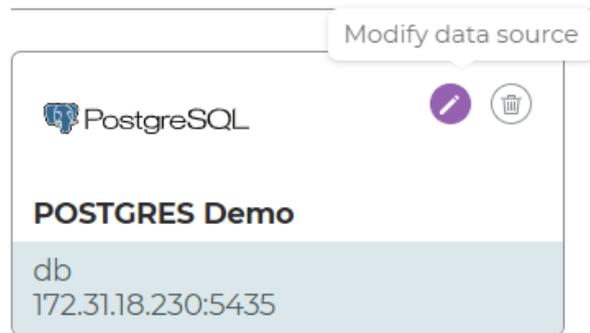


In all dialog boxes, an asterisk * next to a label on the left is used to identify a mandatory user input.

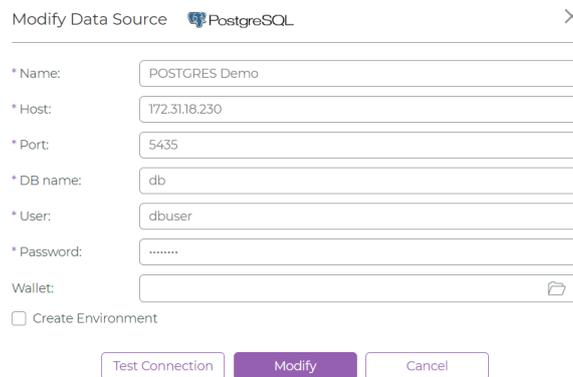
4. Click **Test Connection** to verify that the connection to the new data source is valid.
5. Click **Create Environment** to automatically create an environment that includes all schemes of this data source.
6. Click **Add**.

To modify data source details:

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



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



Modify Data Source PostgreSQL

* Name: POSTGRES Demo

* Host: 172.31.18.230

* Port: 5435

* DB name: db

* User: dbuser

* Password:

Wallet: 

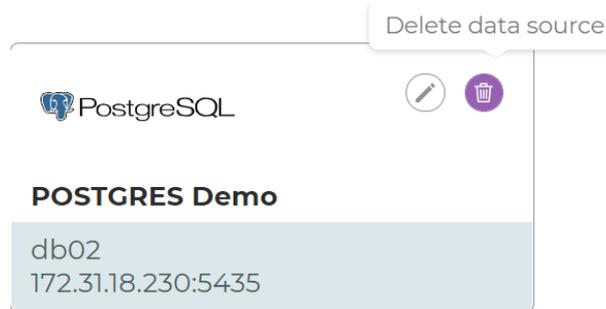
Create Environment

Test Connection Modify Cancel

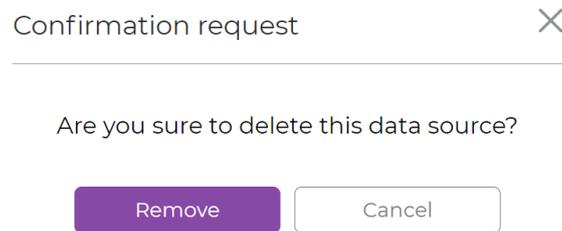
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

To delete a data source:

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



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



6. Managing Environments

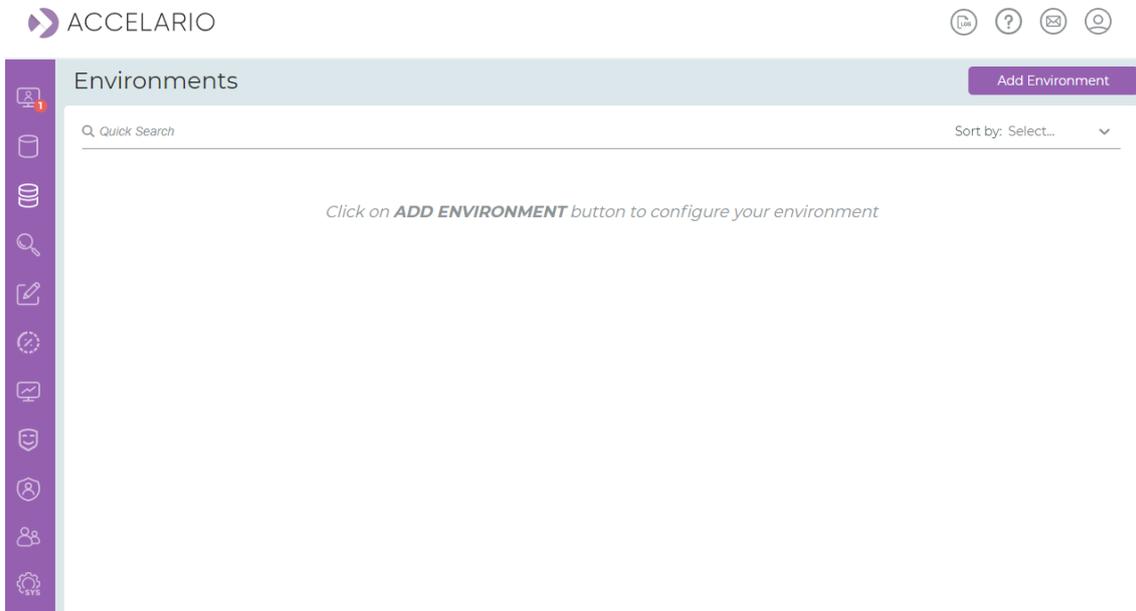
An Environment is an object that groups together database schemas from a data source. An environment object is used for scanning and masking.

To see your environments:

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



2. The **Environments** window appears.



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





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

Sort by: Select... 

- Name (A-Z)
- Name (Z-A)

To add a new environment:

1. Click **Add Environment**.

Environments [Add Environment](#)

Q Quick Search Sort by: Select... 

*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.

Add Environment ✕

Environment name:

Data Sources: A-Z ↓	Schemes:
POSTGRES Demo	<input type="text" value="Quick search"/>

Partial Environment

3. For specific Tables from Schemas:

a. Click **Partial Environment** .

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

Add Environment

Environment name:
env1

Data Sources: A-Z ↓
POSTGRES Demo

Schemes: **Select Tables**

Q. Quick search

- DEV01 Partial
- dev02
- dev03
- DMITRY_TEST
- IND_TGR_PK_UQ_FK
- MASTER_FK_GROUPS
- MASTER_FK_GROUPS_SECOND
- MASTER_MASKING

Add Cancel Partial Environment

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

4. Click **Select Tables**.

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



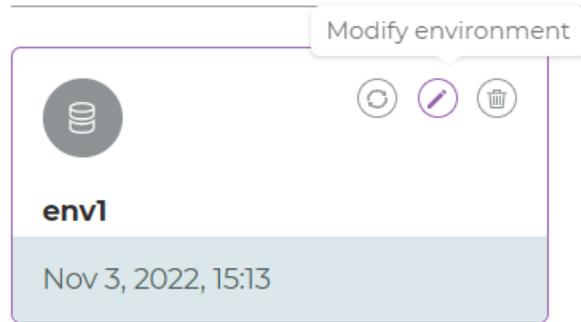
The list shown is the list from the last refresh. To update the list, Click **Refresh**.

6. Click **Submit**.

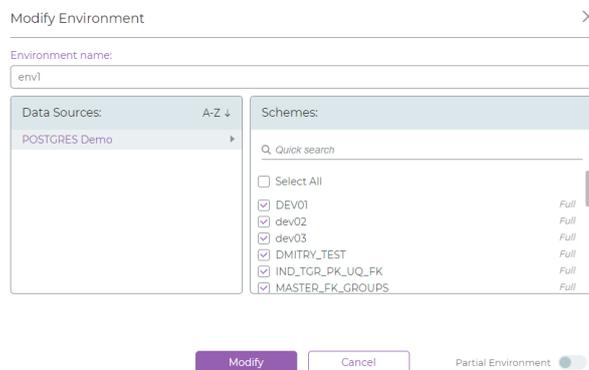
7. Click **Add**.

To modify environment details:

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



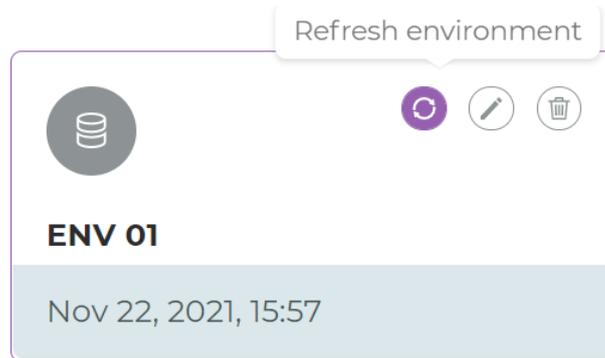
2. The **Modify Environment** window appears. Modify the environment details as required.



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

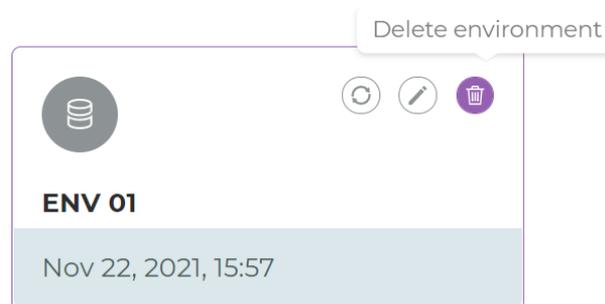
To refresh an environment:

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



To delete an environment:

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



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

Confirmation request ✕

Are you sure to delete this environment?

Remove

Cancel

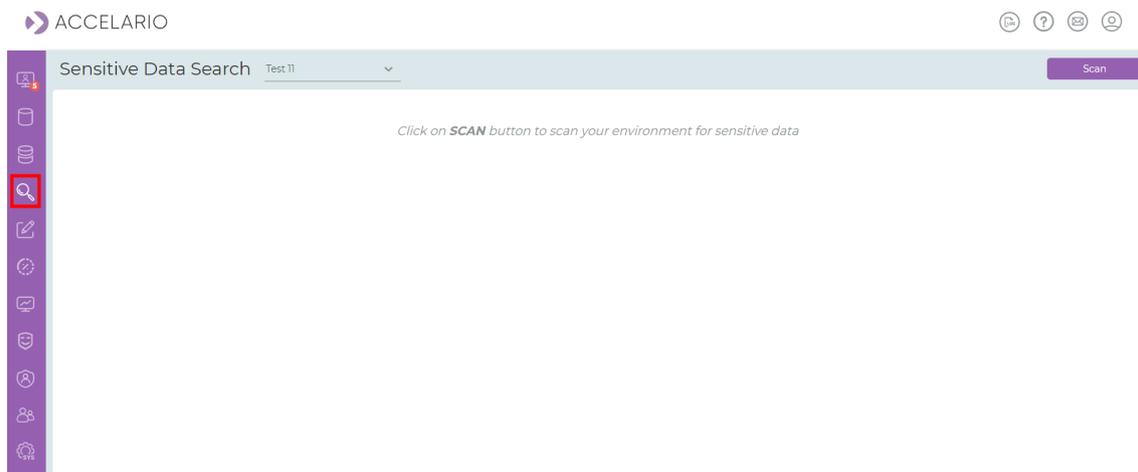
7. Searching for Sensitive Data

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

Once you have setup an environment, you can search the environment for sensitive data that you may want to mask. You can also see results and perform new scans.

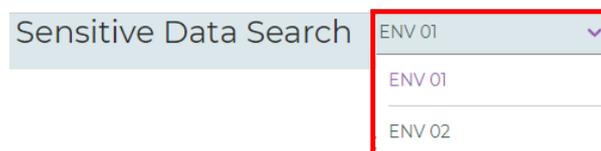
To manage your sensitive data searches:

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

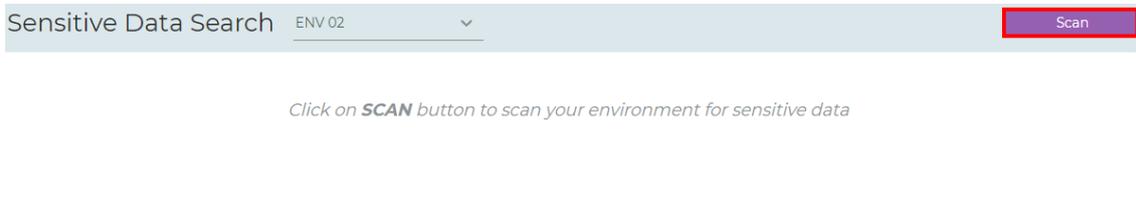


To perform a new sensitive data search:

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



2. Click **Scan**.



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

Search Sensitive Data ✕

Environment: env

* Privacy Policy:

* Parallel Processes:

* Number of unique values to analyze:

* Search Optimization: Search depth:

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**).

After the scan is complete, the scan summary appears.

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

To see detailed scan results:

1. Click **Details**.

Masking Policy: GBR GDPR

Sensitive Data

Passport Number Found in 2 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 7 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

2. In the detailed window you can:

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

Masking Policy: GBR GDPR

All Quick Search

<input type="checkbox"/>	Data Source ¹	Schema ¹	Table ¹	Column ¹	Rule ¹	Probability ¹	FK Group ¹
<input type="checkbox"/>	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
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					
<input checked="" type="checkbox"/>	POSTGRES Demo	MASTER_MASKING	usa_full_address	physicaladdress	GBR Address (Column)	100 %	
<input type="checkbox"/>	POSTGRES Demo	MASTER_MASKING	portuguese_fullnames	column1	GBR First Names	2 %	
<input checked="" type="checkbox"/>	POSTGRES Demo	MASTER_MASKING	spanish_fullnames	column2	GBR Full Names	100 %	
<input checked="" type="checkbox"/>	POSTGRES Demo	MASTER_MASKING	VEHICLE PLATE NUMBER	vehical_plate_no	License Number	100 %	
<input checked="" type="checkbox"/>	POSTGRES Demo	MASTER_MASKING	usa_passport_number	customerpassport	Passport Number (Column)	100 %	

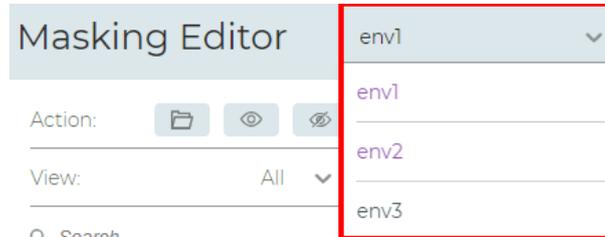
8. Masking Editor – Editing Masking Rules and Running Masking Operation

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

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



2. Select the required environment.



To filter the list of tables:

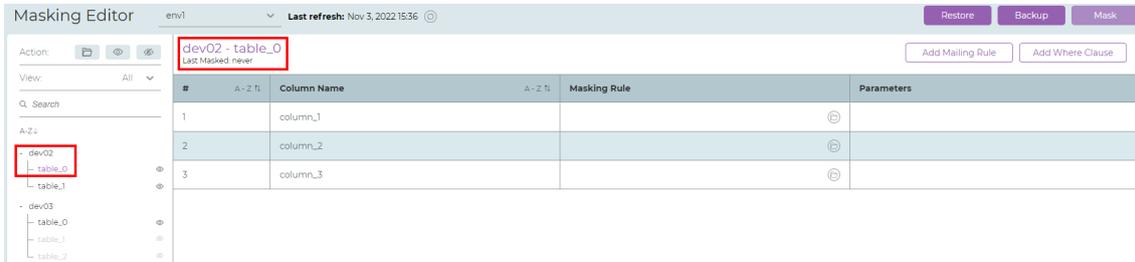
1. Select active or inactive.
2. Select:
 - a. View all tables
 - b. Active tables
 - c. Inactive tables

You can also search for specific tables.

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



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



To select another/new masking rule:

1. For the required column, click .



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

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	IP 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

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

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	  

[+ Add Key](#)

JSON / XML

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

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

To remove a masking rule:

1. On the masking rule, click .

To remove a key:

1. On the key, click .

To see all the masking methods:

1. On the key, click **Show all** .

To add a Where Clause:

1. Click **Add Where Clause**.

dev02 - table_0
Last Masked never

Add Mailing Rule Add Where Clause

#	A - Z Tl	Column Name	A - Z Tl	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»`

VALIDATE CLAUSE ADD CANCEL

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

Add Where Clause ✕

Environment: ENV 2

Table: TABLE1

Where Clause:

To add a Mailing Rule:

1. Click **Add Mailing Rule**.

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

dev02 - table_0
Last Masked: never

The Add Mailing Rule window appears.

Add Mailing Rule

Quick Search

Sort by: Select...

Column Names

Us_State Street json

Zip_Code City

Available Rules

State

City

Address

Zip

Keep State

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

Done Cancel

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

Done Cancel

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.

The screenshot shows the Masking Editor interface for 'dev02 - table_0'. The 'Last refresh' is 'Nov 16, 2022 13:29'. The 'Backup' button is highlighted with a red box. The interface includes a sidebar with a tree view of tables, a search bar, and a main table with columns: #, A-Z fl, Column Name, A-Z fl, Masking Rule, and Parameters. The table contains three rows of data.

#	A-Z fl	Column Name	A-Z fl	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.

The screenshot shows the Masking Editor interface for 'dev02 - table_0'. The 'Last refresh' is 'Nov 16, 2022 13:29'. The 'Restore' button is highlighted with a red box. The interface is identical to the previous screenshot, showing the same table structure and data.

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

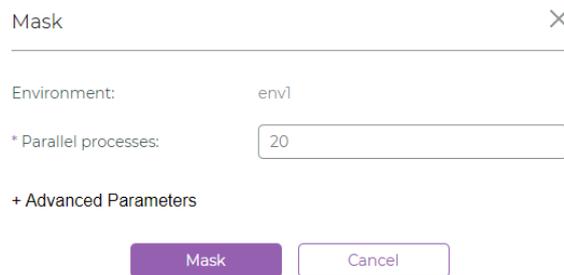
To mask the selected table:

1. Click **Mask**.



The screenshot shows the 'Masking Editor' interface. At the top, there are buttons for 'Restore', 'Backup', and 'Mask'. Below these, the table 'dev02 - table_0' is displayed with columns: '#', 'A - Z T', 'Column Name', 'A - Z T', 'Masking Rule', and 'Parameters'. The table contains three rows with column names 'column_1', 'column_2', and 'column_3'. A 'Mask' button is highlighted in red at the top right.

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



The 'Mask' dialog box is shown with the following fields and buttons:

- Environment: envl
- * Parallel processes: 20
- + Advanced Parameters
- Buttons: Mask, Cancel

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

Mask ✕

Environment: env1

* Parallel processes:

- Advanced Parameters

Fetch size:

Batch size:

Number of masking warning to fail (per table):

Sleep after batch (ms):

Disable database objects:

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

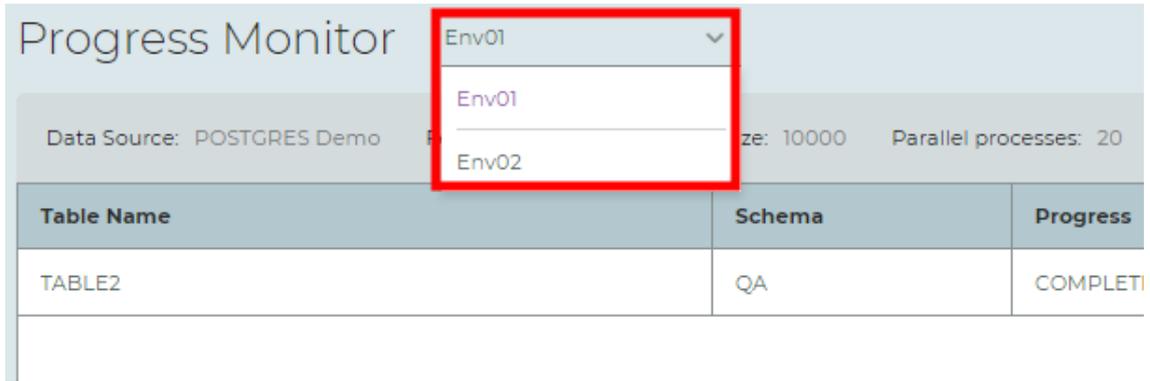
Progress Monitor ENV 01 COMPLETE 100% (Tables: 4/4)
Started: Nov 16, 2023 16:03 Ended: Nov 16, 2023 16:05

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

All Quick Search

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.



The screenshot shows the 'Progress Monitor' interface. At the top, there is a dropdown menu currently set to 'Env01'. Below the dropdown, the 'Data Source' is 'POSTGRES Demo', 'Batch size' is '10000', and 'Parallel processes' is '20'. A table below displays the progress for a table named 'TABLE2' in the 'QA' schema, which is 'COMPLETED'.

Table Name	Schema	Progress
TABLE2	QA	COMPLETED

9. Job Monitoring

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

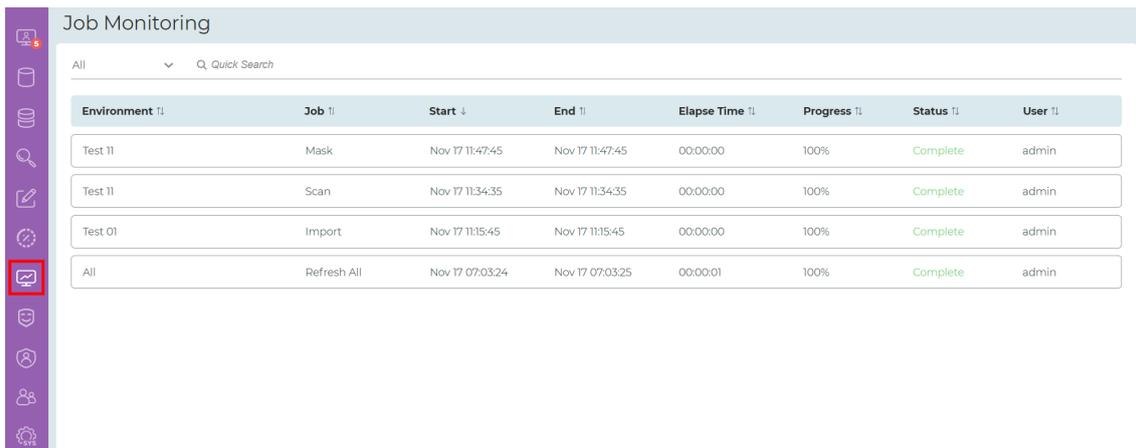
- > See system Jobs: Refresh, Refresh All, Scan, Scan All, and Mask.
- > Drill down and see the detailed status of some of the system jobs.



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

To open the **Job Monitoring** window:

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



The screenshot shows the 'Job Monitoring' window with a table of system jobs. The table has columns for Environment, Job, Start, End, Elapse Time, Progress, Status, and User. The jobs listed are: Test T1 (Mask), Test T1 (Scan), Test O1 (Import), and All (Refresh All). All jobs are in a 'Complete' status.

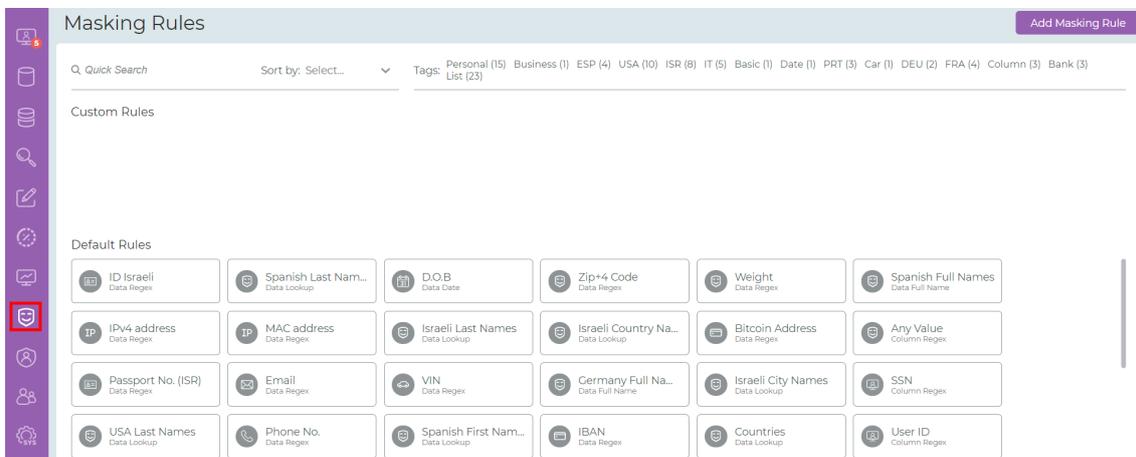
Environment	Job	Start	End	Elapse Time	Progress	Status	User
Test T1	Mask	Nov 17 11:47:45	Nov 17 11:47:45	00:00:00	100%	Complete	admin
Test T1	Scan	Nov 17 11:34:35	Nov 17 11:34:35	00:00:00	100%	Complete	admin
Test O1	Import	Nov 17 11:15:45	Nov 17 11:15:45	00:00:00	100%	Complete	admin
All	Refresh All	Nov 17 07:03:24	Nov 17 07:03:25	00:00:01	100%	Complete	admin

10. Managing Masking Rules

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

To see current masking rules:

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



To see information about the masking rule:

1. On the masking rule, click .

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: dfdf

Masking Definition:
Masking Method: Mask Any Value
Skip first symbols: 0
Skip last symbols: 0
Examples: Custom Column Rule

[Back](#)

To add a new custom masking rule:

1. Click **ADD MASKING RULE**.

Masking Rules [Add Masking Rule](#)

Q Quick Search Sort by: Select... Tags: Personal (33) Business (1) ESP (4) USA (20) ISR (1) IT (5) Basic (3) Date (4) BRA (1) TUR (4) PRT (4) Car (1) DEU (4) FRA (4) ITA (4) Column (24) CBR (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:



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:

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) [X]

Search Definition:

* Search Type: Column - RegExp [v]

* Data Types: Select data types... [v]

Minimum Column Size: 15

* Regular Expressions:

[Text Area]

Next Back Cancel

5. Select a **Data Types**:

- a. **CHAR**
- b. **DATE**
- c. **TIMESTAMP**
- d. **NUMERIC**

Add Masking Rule (Column - RegExp) [X]

Search Definition:

* Search Type: Column - RegExp [v]

* Data Types: Select data types... [v]

Minimum Column Size: CHAR

* Regular Expressions: DATE

[Text Area] TIMESTAMP

NUMERIC

Next Back Cancel

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:

* Data Types:

Minimum Column Size:

* Regular Expressions:

NextBackCancel

- 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:

Don't mask first # of characters:

Don't mask last # of characters:

Masking Example: →

AddBackCancel

- d. Click **ADD**.

The new masking rule appears.

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

The screenshot shows a dialog box titled "Add Masking Rule (Data - RegExp)" with a close button (X) in the top right corner. The "Search Definition" section contains the following fields:

- * Search Type: A dropdown menu with "Data - RegExp" selected.
- * Data Types: A dropdown menu with "CHAR" selected.
- Minimum Column Size: A text input field containing "15".
- * Regular Expressions: A large empty text area.

At the bottom of the dialog, there are three buttons: "Next" (highlighted in purple), "Back" (highlighted in purple), and "Cancel" (white with a grey border).

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

The screenshot shows the same dialog box, but now the "Masking Definition" section is active. It contains the following fields:

- * Masking Method: A dropdown menu with "Mask Any Value" selected.
- Don't mask first # of characters: A text input field containing "0".
- Don't mask last # of characters: A text input field containing "0".
- Masking Example: Two text input fields. The first contains "<string>" and the second contains "<string>", with a right-pointing arrow between them.

At the bottom of the dialog, there are three buttons: "Add" (highlighted in purple), "Back" (highlighted in purple), and "Cancel" (white with a grey border).

- 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) [X]

Search Definition:

* Search Type: Data - Lookup [v]

* Search Lookup File: [file icon]

Next Back Cancel

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

Add Masking Rule (Data - Lookup) [X]

Search Definition:

* Search Type: Data - Lookup [v]

* Search Lookup File: Masking Data Lookup List.docx [file icon]

Next Back Cancel

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) [X]

Masking Definition:

Use same lookup file for search and masking

* Masking Method: Mask Any Value [v]

Don't mask first # of characters: 0

Don't mask last # of characters: 0

Masking Example: <string> → <string>

Add Back Cancel

d. Click **ADD**.

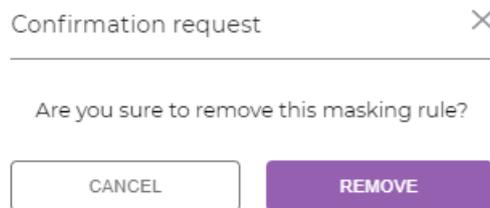
The new masking rule appears.

To delete a custom masking rule:

1. On the masking rule, click .

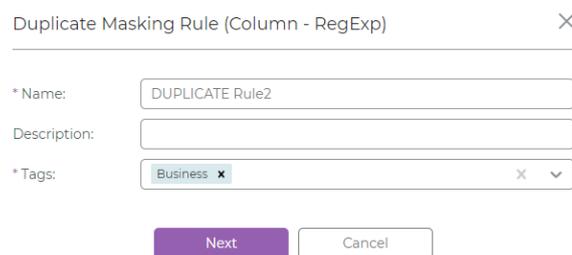


2. Click **REMOVE** to confirm the deletion, or **CANCEL** to exit without deleting the masking rule.



To duplicate a masking rule:

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



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

Duplicate Masking Rule (Column - RegExp) ✕

Search Definition:

* Search Type:

Minimum Column Size:

* Regular Expressions:



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

5. Click **NEXT**.

Duplicate Masking Rule (Column - RegExp) ✕

Masking Definition:

* Masking Method:

Don't mask first # of characters:

Don't mask last # of characters:

Masking Example: →

6. Click **Duplicate**.

11. Managing Privacy Policies

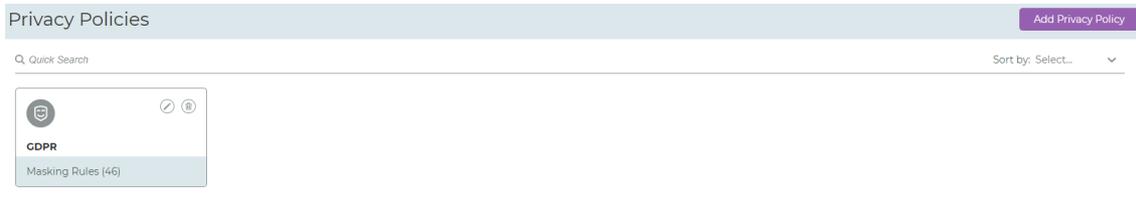
A **Privacy Policy** is a set of masking rules used to scan and mask following a specified privacy regulation such as GDPR, CCPA and HIPAA or to the organization privacy rules. This section describes how to define and manage the privacy policies.

To view available privacy policies:

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



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



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



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



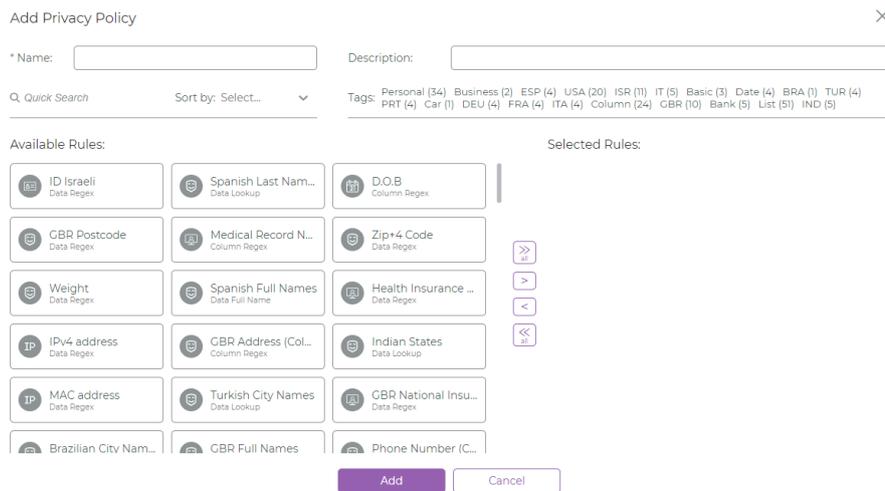
To add a new privacy policy:

1. Click **Add Privacy Policy**.



2. Fill in the policy details:

- a. In **Name**, provide a name.
- b. Under **Available Rules**, select a rule or a number of rules.

A screenshot of the 'Add Privacy Policy' form. At the top right is a close button 'X'. The form has two input fields: '* Name:' and 'Description:'. Below these are search and sort options: 'Quick Search' and 'Sort by: Select...'. A 'Tags' section lists various categories with counts: Personal (34), Business (2), ESP (4), USA (20), ISR (1), 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 (5), IND (5). The main area is divided into 'Available Rules' and 'Selected Rules'. The 'Available Rules' section contains a grid of 15 rule cards, each with an icon and a label like 'ID Israeli Data Regex' or 'Spanish Last Nam... Data Lookup'. The 'Selected Rules' section is currently empty. At the bottom, there are 'Add' and 'Cancel' buttons.

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

Add Privacy Policy X

* Name: Description:

Q 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:

Selected Rules:

--	--

4. Click **Add**.

  To add all the available rules, click  .

 To remove all the available rules, click  .

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

To add a masking rule according to a Tag:

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

* Name: Description:

Q 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: Description:

Q 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: Selected Rules:

IBAN Data Regex SWIFT Data Regex Credit Card Data Regex

>>
>
<
<<

Add Cancel

3. Select a rule.

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

Add Privacy Policy ×

* Name: Description:

Q 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: Selected Rules:

IBAN Data Regex SWIFT Data Regex Credit Card Data Regex

>>
>
<
<<

Add Cancel

5. Click **Add**.



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

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

* Name: Description:

🔍 Quick Search Sort by: Select... ▼ Tags: Personal (15) Business (1) ESP (4) USA (00) ISR (8) IT (5) Basic (1) Date (1) Custom (3) PRT (3)
Car (1) DEU (2) FRA (4) Column (4) **Bank (3)** List (23)

12. Managing Users and Roles



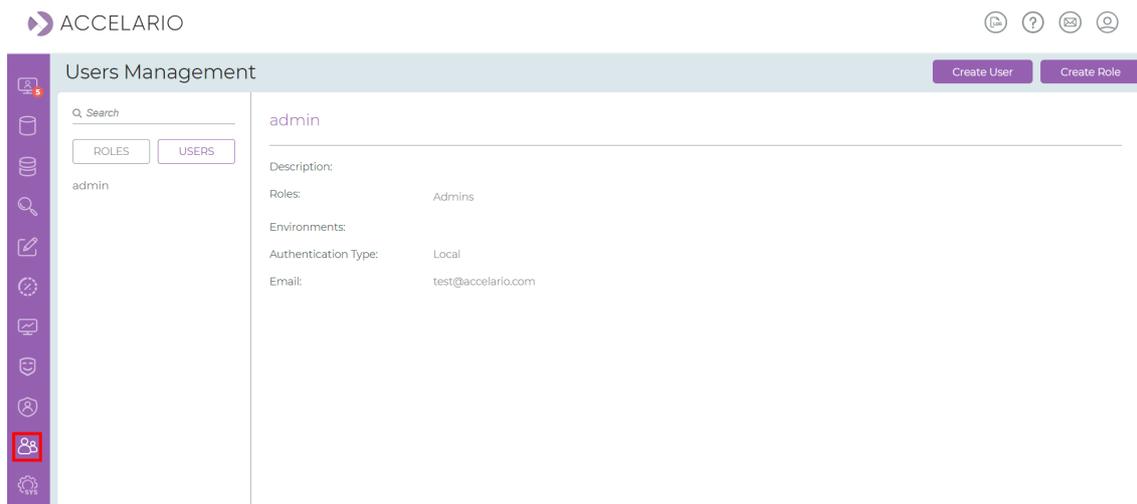
Only a user with **Admin** privileges can create or modify users and roles.



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

To manage users:

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



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



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

Q Search

ROLES

USERS

To create a new role:

1. Click **Create Role**.

Users Management Create User Create Role

Q Search

ROLES USERS

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).

Q Search

Admins

QA 

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

Modify Role ✕

* Role Name:

Description:

* Select Authorized Environments:

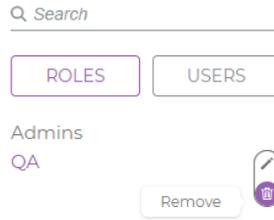
- env2
- env3
- env1

Select Authorized Users:

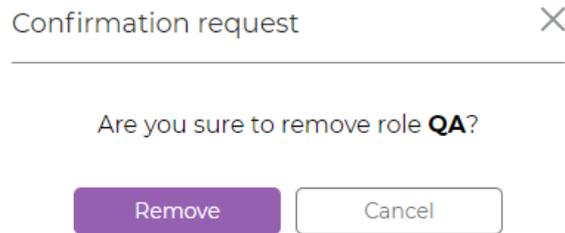
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

To delete a role:

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

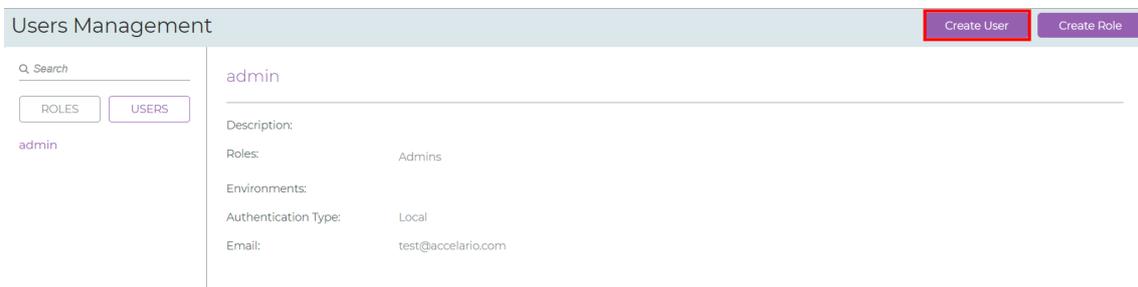


2. Click **Remove** to confirm the deletion, or **Cancel** to exit without deleting the role.



To add a new user:

1. Click **Create User**.



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).

Q Search

ROLES USERS

admin

userA 

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

Modify User ✕

* User Name:

Description:

* Select Roles: QA

Admin

* Authentication Type: Local Active Directory

* Password:

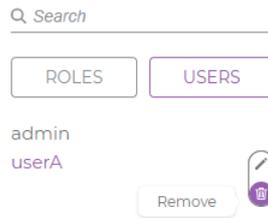
* Confirm Password:

* Email:

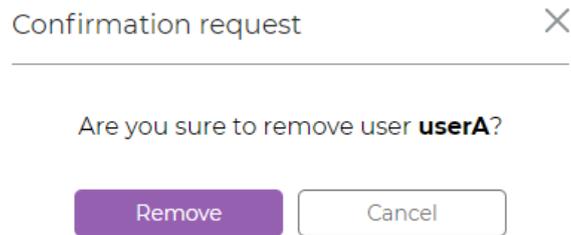
3. To save your changes, click **Modify**. Otherwise, click **Cancel**.

To delete a user:

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



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



13. System Setup

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



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

To setup the active directory:

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

The screenshot shows the 'System Setup' interface with three tabs: 'Users', 'SMTP', and 'Masking Rules'. The 'Users' tab is selected. Below the tabs, there is a section titled 'ACTIVE DIRECTORY SETTING'. It contains a checkbox for 'Use Active Directory Authentication' which is unchecked. Below this are several input fields: '* Server Name/IP' with the value 'smtp~my.company.com', '* Bind Username' (empty), '* Port' with the value '0', '* Authentication Type' with a dropdown menu showing 'Simple', '* Bind Password' (empty), and '* AD Domain Name' (empty). At the bottom of the form are two buttons: 'Test AD' and 'Save'.

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

To setup the SMTP server:

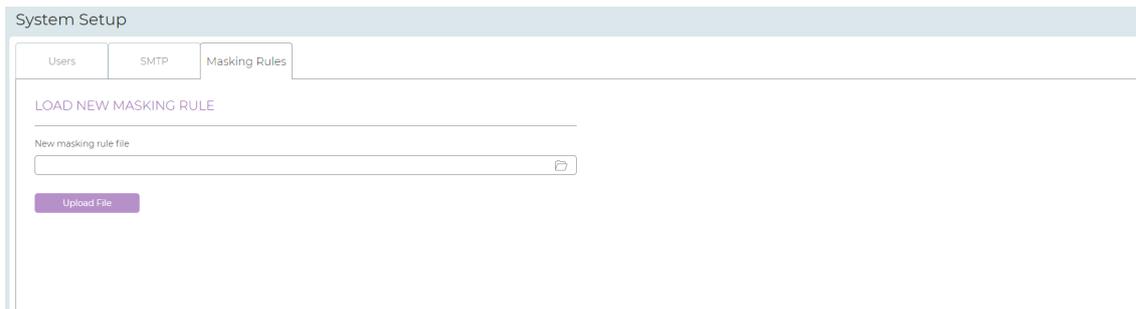
1. Click **SMTP**.
2. Fill in the details to setup the SMTP sever.

The screenshot shows the 'System Setup' interface with the 'SMTP' tab selected. The 'SMTP SERVER' section includes a checkbox for 'Activate SMTP', a 'Server Name/ID' field with the value 'smtp.<my company>.com', 'Bind Username' and 'Bind Password' fields, a 'Port' field with the value '0' and a 'Use SSL' checkbox, and a 'From Email' field with the value 'Accelerario@<my company>.com'. There are 'Test Email' and 'Save' buttons at the bottom. The 'EMAIL NOTIFICATION' section includes an 'Email Recipients' field with the value 'User1@<my company>.com, User2@<my company>.com' and 'Filters' checkboxes for 'Error', 'Warning', and 'Info'.

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

To install new built-in masking rules online:

1. Click **Masking Rules**.



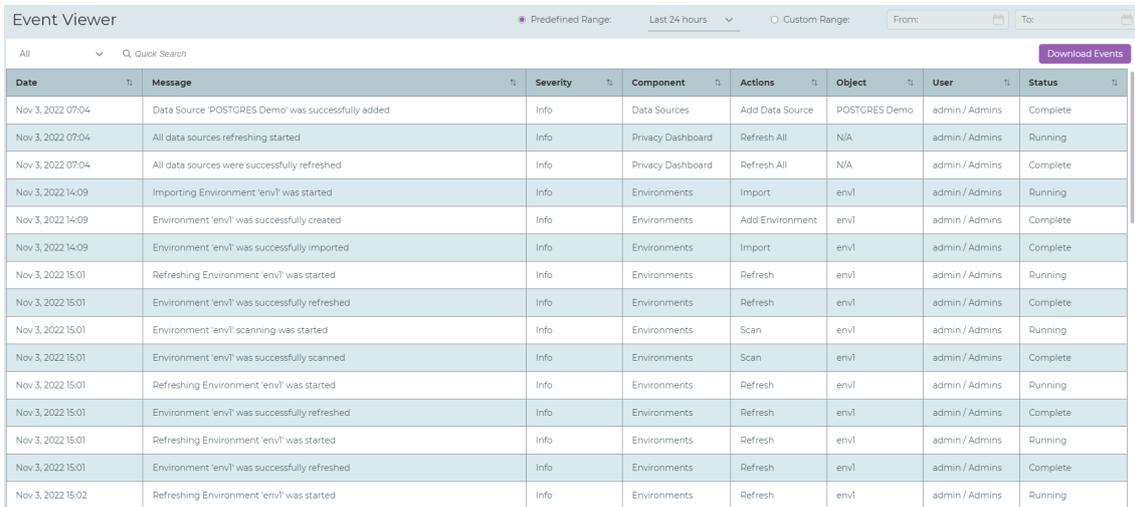
2. Click  .
3. Select file.
4. Click **Upload File** .

14. Event Viewer

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

To open the Event Viewer work area:

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



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

To quick search events with a keyword:

1. Type a keyword in the  Quick Search bar.

To filter events for a specified time period:

1. Select:

a. **Predefined Range.**

Predefined Range: 

or

b. Enter a **Custom Range.**

Custom Range:  

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 .