ユーザガイド
[Accelario Data Masking]

株式会社クライム

Climb Inc.
Growing to Meet Your Needs

作成日: 2023/03/06(月)

バージョン: 1.0

目次

はじめに

本ドキュメントは製品を購入されたお客様、評価版をご使用のお客様向けに株式会社クライムが提供しております。

範囲

本ドキュメントは、Accelario Data Masking モジュールの使用方法について記載しております。

対象バージョン

本ドキュメントは、以下の製品に対応しております。

- Accelario Data Masking

プロダクトの概要

Accelario Data Masking(アクセラリオデータマスキング)モジュールでは、インテリジェントな機密データ検索エンジンを使用して機密データを簡単に特定でき、その場でマスキングすることができます。データのマスキングは、カスタマイズされた、または事前に定義されたマスキングポリシー(GDPR、HIPAA などの各種規制に対応)に基づいて実行されます。マスキングプロセスでユーザが手動介入する必要は最小限にとどめられ、なおかつ、参照整合性を維持しながら本番品質のデータに変換することができます。

Accelario Data Masking モジュールは、以下のコンポーネントで構成されます:

- Privacy Dashboard (プライバシーダッシュボード)
- Data Source (データソース)
- Environment (環境)
- Sensitive Search (機密データ検索)
- Masking Editor (マスキングエディタ)
- Masking Rule (マスキングルール)
- Privacy Policy (プライバシーポリシー)
- Users Management (ユーザ管理)
- System Setup (システム設定)
- Job Monitoring (ジョブモニタリング)
- Event Viewer (イベントビューア)

プライバシーダッシュボード

Accelario **Privacy Dashboard**(プライバシーダッシュボード)では、プライバシー侵害の兆候を察知して、明確に示すことができます。本番環境以外のすべてのデータソースをスキャンして、プライバシーの問題を検出します。問題のあるデータソースは、ワンクリックで簡単にドリルダウンでき、詳細を確認することができます。

Privacy Dashboard ウィンドウでは、以下の操作を行うことができます:

- 機密データのデータソースをワンクリックでスキャンでき、GDPR(EU 一般データ保護規則)や CCPA(カリフォルニア州消費者プライバシー法)などのプライバシーポリシーへの準拠を徹底できます。
- すべてのデータソースをリフレッシュして、メタデータを元のデータソースから更新できます。新たに追加された、あるいは削除されたテーブルやカラムは自動的に検出/削除されます。
- 管理対象のすべてのデータソースから機密データを一括表示できます。
- データソースごとに機密データの詳細を表示できます。
- プライバシー侵害のリスクを、データソース、環境、スキーマ、テーブル、カラムなど、あらゆるレベルで確認できます。

プライバシーダッシュボードの画面操作について詳しくは、プライバシーダッシュボードの GUI を参照してください。

データソース

Data Source(データソース)とは、使用中のデータの取得元であるデータベースやファイルを指します。データソースの名前が指定され、サーバの場所が特定されることで、データソースとの接続が成立します。

Data Source ウィンドウでは、以下の操作を行うことができます:

- 新しいデータソースの追加
- 既存のデータソースの変更または削除

注意:
データソースの表示や編集ができるのは、管理者(Admin)権限を持つユーザに限られます。

データソースの画面操作について詳しくは、データソースの管理を参照してください。

Environment(環境)

Environment(環境)は、データソースから取得したデータベーススキーマを一まとめにグループ化したオブジェクトです。このオブジェクトを使用して、スキャニングとマスキングが行われます。

Environment ウィンドウでは、以下の操作を行うことができます:

- 異なるデータソーススキーマからの Environment(環境)の新規追加
- 既存の Environment を変更または削除
- Environment のリフレッシュ — メタデータが元のデータソースから更新され、新たに追加された、あるいは削除されたテーブルやカラムは自動的に検出／削除されます。さらに、外部キーのリレーションシップが更新されて参照整合性が維持されます。

詳しくは、環境の管理を参照してください。

機密データの検索

Accelario Data Masking モジュールにはインテリジェント検索エンジンが搭載されており、ルックアップリストと AI テクノロジーを活用した高度な検索アルゴリズムによってスマートな検索が実行できます。

Accelario Data Masking モジュールの **Sensitive Search** ウィンドウでは、以下の操作を行うことができます:

- ワンクリックで環境をスキャンして、GDPR(EU 一般データ保護規則)や CCPA(カリフォルニア州消費者プライバシー法)などのプライバシーポリシーへの準拠を確認できます。
- 適正な機密データカラムにマスキングルールを自動割り当てできます。
- 外部キーにグループごとに同じマスキングルールを適用して参照整合性を維持できます。
- 特に重要な機密データや統計情報を含むスキャン結果を包括的に表示できます。
- 検出されたすべての機密データカラムの詳細情報を表示できます。
- 機密データカラムを選択してマスキングできます。

詳しくは、機密データの検索プロセスを参照してください。

マスキングエディタ

Masking Editor(マスキングエディタ)を使用すると、選択した機密データカラムを表示したり、変更したり、他のカラムに手動でマスキングルールを適用したりできます。

Accelario Data Masking モジュールの **Masking Editor** ウィンドウでは、以下の操作を行うことができます:

- 特定のカラムにマスキングルールを適用またはルール変更
- マスキングの対象テーブルに Where Clause を追加
- マスキング構成ファイルのバックアップ／リストア
- Mask オペレーションの実行と **Progress Monitor** ウィンドウでの進捗確認

詳しくは、マスキングエディタ - マスキングルールの変更とマスキング処理の実行を参照してください。

マスキングルール

Masking Rule(マスキングルール)には、機密データ検索のスキャニングに関する情報と、指定した機密データ(名前、メールアドレス、クレジットカード番号など)のマスキング方法に関する情報が含まれています。

Accelario Data Masking モジュールの **Masking Rule** ウィンドウでは、以下の操作を行うことができます:

- サポートされているすべてのビルトインマスキングルールを表示確認
- カスタムマスキングルールの追加／修正
- ビルトインまたはカスタムのマスキングルールをコピーしいて、新規マスキングルールを作成

詳しくは、マスキングルールの管理を参照してください。

プライバシーポリシー

Privacy Policy(プライバシーポリシー)とは、GDPR(EU 一般データ保護規則)、CCPA(カリフォルニア州消費者プライバシー法)、HIPPA(医療保険の相互運用性と説明責任に関する法律)などの各種規制や、社内のプライバシールールを遵守するために適用するスキャニングとマスキングのためのマスキングルールのセットを指します。

Accelario Data Masking モジュールの **Privacy Policies** ウィンドウでは、以下の操作を行うことができます:

- プライバシーポリシーの追加、表示、変更
- 有効な住所に対して、特定のテーブルの複数の列にまたがる住所をマスクする **Mailing Rule** を追加

詳しくは、プライバシーポリシーの管理を参照してください。

ユーザ管理

Accelario Data Masking は **Role-based User Management System**(ロールベースのユーザ管理システム)を採用しています。すべてのユーザが Privacy Dashboard(プライバシーダッシュボード)にアクセスできますが、各ユーザはさらに以下のカテゴリに分類されます:

- Admin(管理者ユーザ) — データソースとすべての環境を管理でき、モニタリングとトラブルシューティングを実行できます。
- 一般ユーザ — アクセス権を付与された環境のみを対象として、スキャニングとマスキングを実行できます。

注意:
管理者(**Admin**)権限を持つユーザのみ、ユーザおよびロールの作成または変更を行うことができます。

Accelario Data Masking モジュールの **Users Management** ウィンドウでは、以下の操作を行うことができます:

- ユーザの作成と変更
- ロールの作成と変更

詳しくは、ユーザとロールの管理を参照してください。

システム設定

System Setup(システム設定)では、SMTP、Active Directory などのシステムパラメータを定義します。

Accelario Data Masking モジュールの **System Setup** ウィンドウでは、以下の操作を行うことができます:

- Active Directory 認証情報の構成
- SMTP の構成

注意:
システム設定にアクセスできるのは、管理者(**Admin**)権限を持つユーザに限られます。

詳しくは、システム設定の管理を参照してください。

ジョブのモニタリング

進行中のシステムジョブのステータスは、**Job Monitoring**(ジョブモニタリング)で確認できます。

Accelario Data Masking モジュールの **Job Monitoring** ウィンドウでは、以下の操作を行うことができます:

- 進行中のすべてのシステムジョブや停止済みのシステムジョブを表示確認(システムジョブの履歴は Event Viewer ウィンドウで表示)
- システムジョブの詳細ステータスを掘り下げ

注意:
ジョブモニタリングにアクセスできるのは、管理者(**Admin**)権限を持つユーザに限られます。

詳しくは、ジョブモニタリングの GUI を参照してください。

イベントビューア

Event Viewer(イベントビューア)を使用すると、すべてのユーザイベントを表示確認して、保存することができます。

Accelario Data Masking モジュールの **Event Viewer** ウィンドウでは、以下の操作を行うことができます:

- すべてのユーザイベントの表示／フィルタリング／検索
- すべてのユーザイベントをファイル保存

詳しくはイベントビューアを参照してください。

インストール手順

インストールキットは次のファイルを含む Zip アーカイブです。

- jar ファイル
- conf ディレクトリ内の yaml ファイル

例:

data-masking-1.0-SNAPSHOT.jar

conf/application.yml

前提条件

- Windows または Linux サーバ - 任意のリリース/バージョン。このサーバは、アプリケーションサーバとして機能します。専用のホストまたはデータベースサーバと同じホストのいずれでもかまいません。最小要件: 2 つの CPU コア、2GB RAM、20GB のディスク容量
- Java 8
- 必要なデータベースへのネットワークアクセス
- OS ユーザ:

  Linux - sudo 権限を持つユーザ

  Windows - Java を実行し、“app_home”ディレクトリに読み書きする権限を持つユーザ
- データベースユーザ - アプリが操作するすべてのデータベースで DBA 権限を持つユーザ。各データベースには、異なるユーザとパスワードが設定されている場合があります。

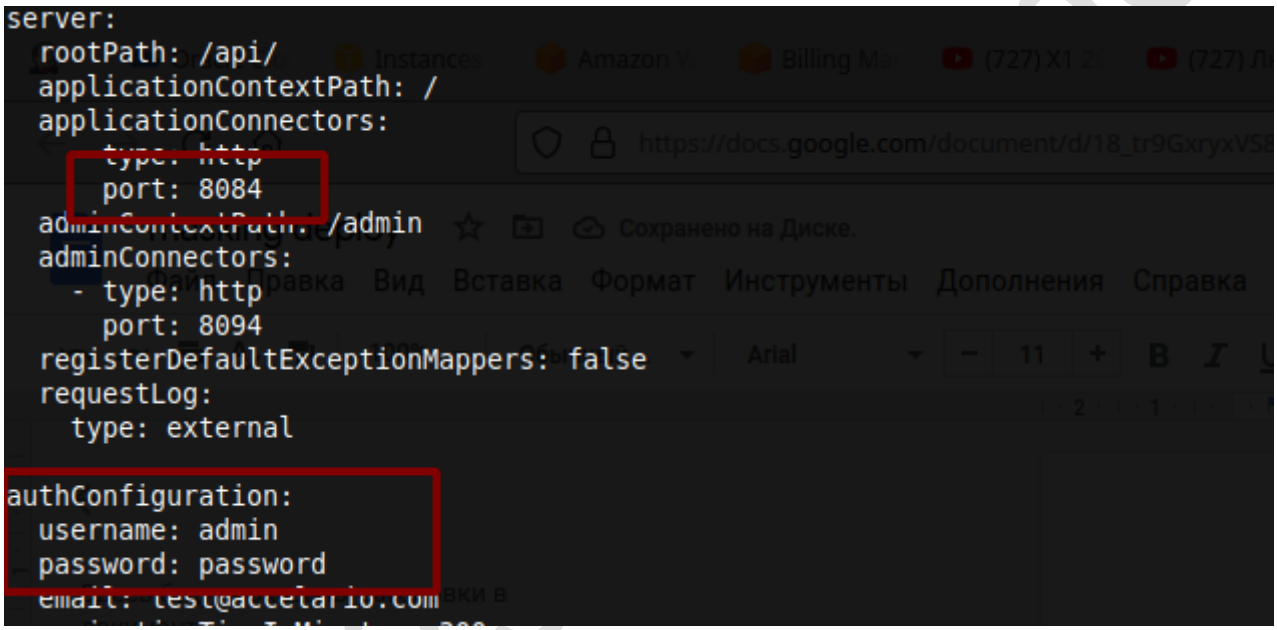
展開

インストールキットをアプリサーバの空のディレクトリに解凍します。このディレクトリはさらに“app_home”と呼ばれます。

構成ファイル“conf/application.yml”には、すべてのパラメータがデフォルト値で既に含まれています。

必要に応じて、このファイルを更新してアプリケーションを再起動することにより、パラメータを変更できます。

たとえば、次の図に示すように、ポートと管理者ログインパスワードを変更します。



Linux

Java 1.8 がインストールされていることを確認してください。

次のコマンドを実行します。

```
cd {app_home}
sudo screen -dmSL masking java -Duser.timezone=GMT -jar data-masking-1.0-SNAPSHOT.jar
```

screen がインストールされていない場合は、nohup を使用することもできます。

```
sudo nohup java -Duser.timezone=GMT -jar data-masking-1.0-SNAPSHOT.jar &
```

シェルの特別なロケールの場合は、次のパラメータを追加します。

```
-Dfile.encoding=UTF-8 -Dconsole.encoding=UTF-8
```

Windows

Java 1.8 の 64 ビットがインストールされていることを確認します。

次のコマンドを実行します。

```
cd {app_home}
java -Duser.timezone=GMT -jar data-masking-1.0-SNAPSHOT.jar
```

シェルの特別なロケールの場合は、次のパラメータを追加します。

```
-Dfile.encoding=UTF-8 -Dconsole.encoding=UTF-8
```

アプリケーションへのアクセス

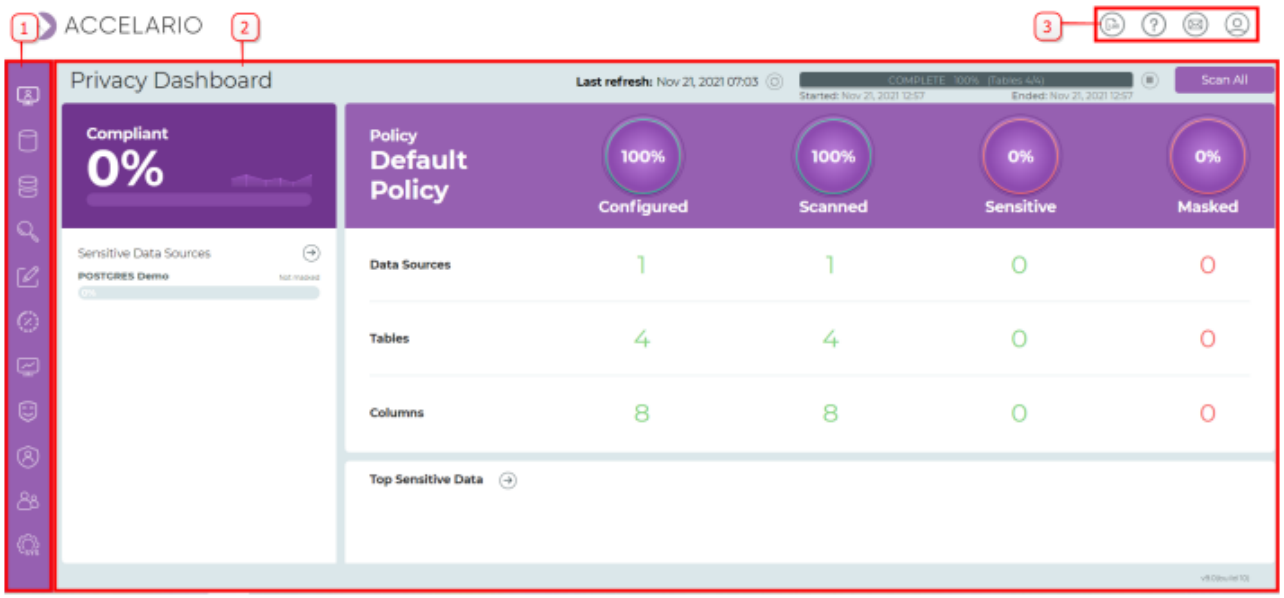
ブラウザーを開き、**http://myserver:8084** に移動します。

“myserver”を jar ファイルが開始されたホスト名に置き換えます

注意: デフォルトのポート(8084)は、「展開」セクションで説明されているように変更できます。

グラフィカルユーザインターフェースの概要

以下の図表は、Accelario Data Masking モジュールのグラフィカルユーザインターフェース(GUI)を表しています。

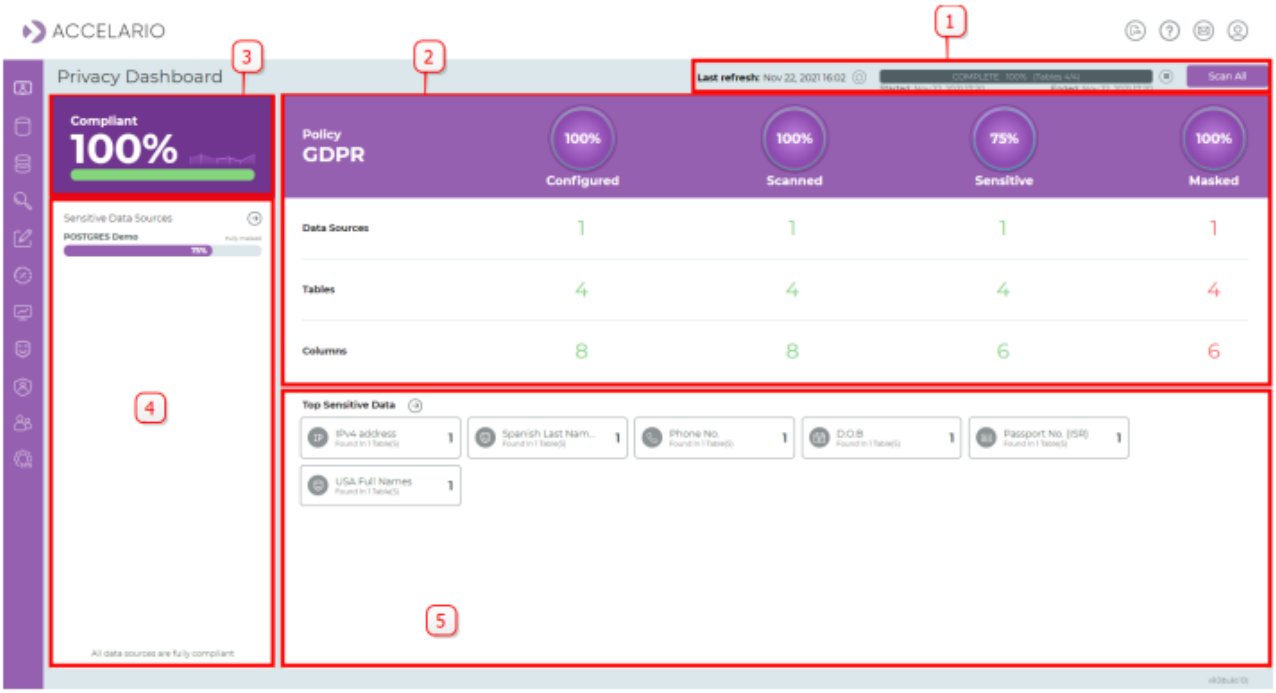


番号	項目	詳細
1	ナビゲーションバー	メインワークエリアに詳細情報を表示するために使用します。
2	メインワークエリア	タスクを実行するための作業スペースです。
3	タスクバー	システムタスクを表します。

インターフェースは選択した機能に応じて動的に切り替わる設計になっています。

プライバシーダッシュボードの GUI

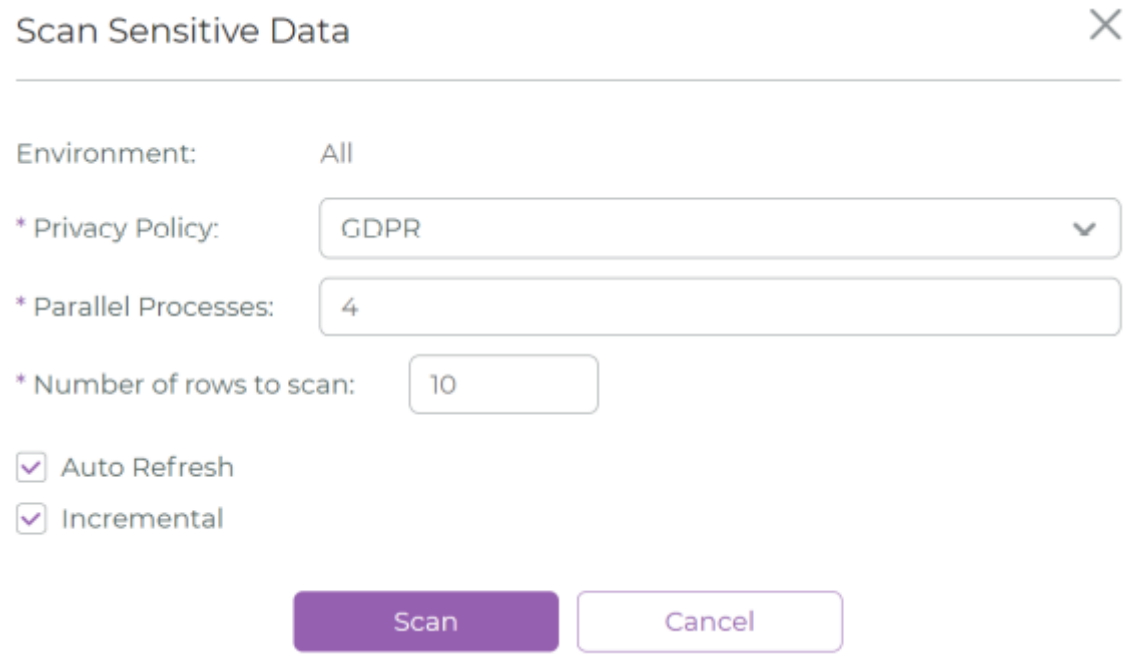
Privacy Dashboard（プライバシーダッシュボード）を使用すると、プライバシー侵害のリスクを明確に確認することができます。本番環境以外のすべてのデータソースをスキャンして、プライバシーの問題を検出します。問題のあるデータソースは、ワンクリックで簡単にドリルダウンでき、詳細を確認することができます。以下の図表は、プライバシーダッシュボードのグラフィカルユーザインターフェース（GUI）を表しています。



番号	項目	詳細
1	スキャンバー	管理対象のすべてのデータソースのリフレッシュとスキャニングを実行します。
2	表示エリア	スキャニングのステータスと、特定の機密データに適用されたマスキングのステータスを表示します。
3	コンプライアンスバー	コンプライアンスの遵守度を%表示します。
4	機密データソース	管理対象のすべてのデータソースを機密レベルとともに表示します。
5	最高機密データ	最高位の機密データを表示します。

機密データの問題リスクをスキャンする手順は次のとおりです:

1. Scan All (すべてをスキャン)をクリックします。
2. **Scan Sensitive Data** ウィンドウでスキャンパラメータを設定し、**Scan** をクリックします。

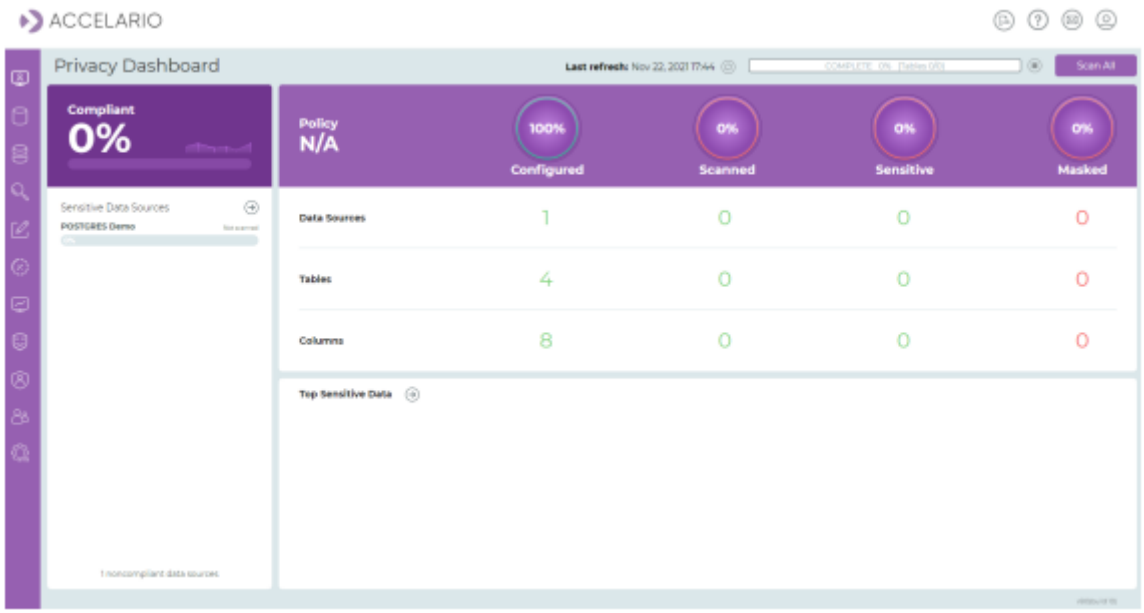


スキャニングを停止する手順は次のとおりです:

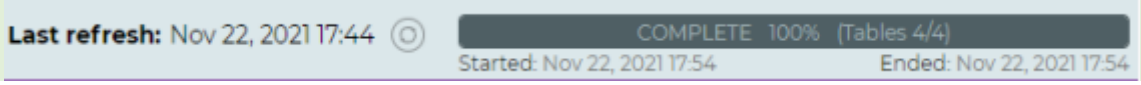
1.  をクリックします。

すべてをリフレッシュする手順は次のとおりです:

1.  をクリックします。
2. 前に行われたスキャニングの結果がすべて削除されます。

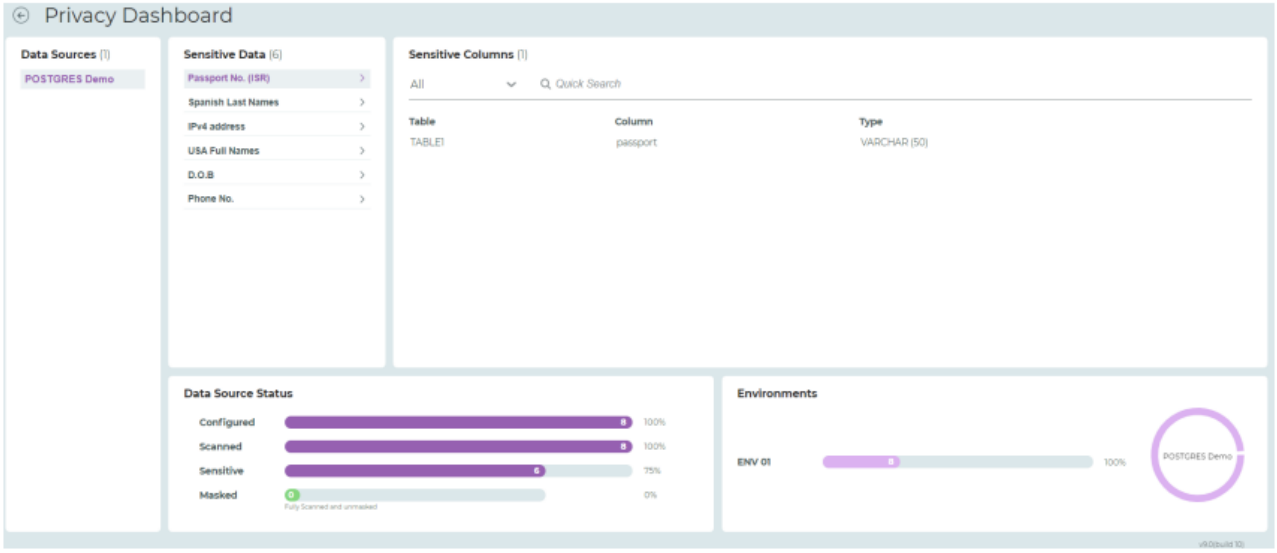


注意:
スキャンバーに以下の情報が表示されます。



機密性が認められるデータの詳細を確認する手順は次のとおりです:

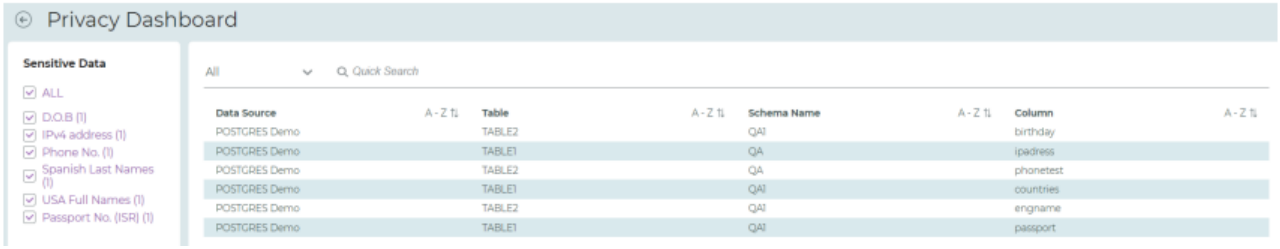
1. 機密データソース→をクリックします。



2. プライバシーダッシュボードに戻るには、Privacy Dashboardをクリックします。

最高位の機密データを確認する手順は次のとおりです:

1. Top Sensitive Data →をクリックします。



2. プライバシーダッシュボードに戻るには、Privacy Dashboardをクリックします。

データソースの管理

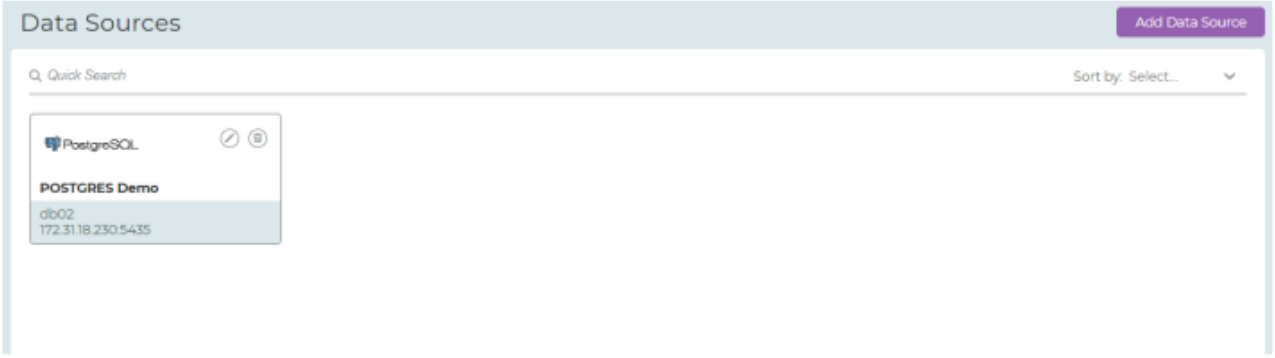
Data Source(データソース)とは、使用するデータの取得元であるデータベースやファイルのことを指します。ここでは、データソースの定義と管理方法について解説します。

注意:
Data Sources を表示、編集できるのは、管理者(Admin)権限を持つユーザに限られます。

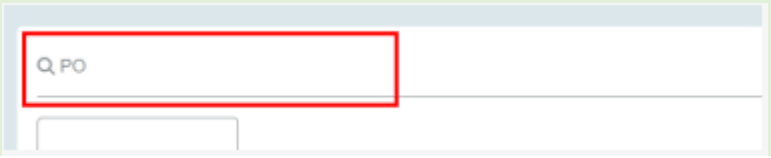
利用可能なデータソースを確認する手順は次のとおりです:

1. ナビゲーションバーで  (Data Sources)をクリックします。

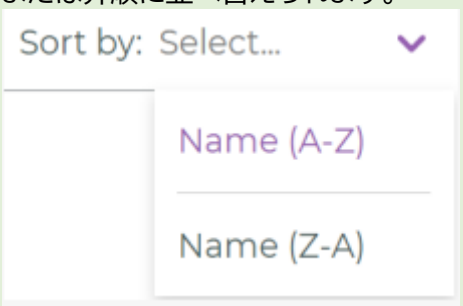
2. Data Sources ウィンドウが開き、システムに追加されているすべてのデータソースが表示されます。



注意:
Quick Search バーから文字列を検索すると、必要なデータソースを迅速に見つけることができます。検索によってリスト表示がすばやく更新されます。

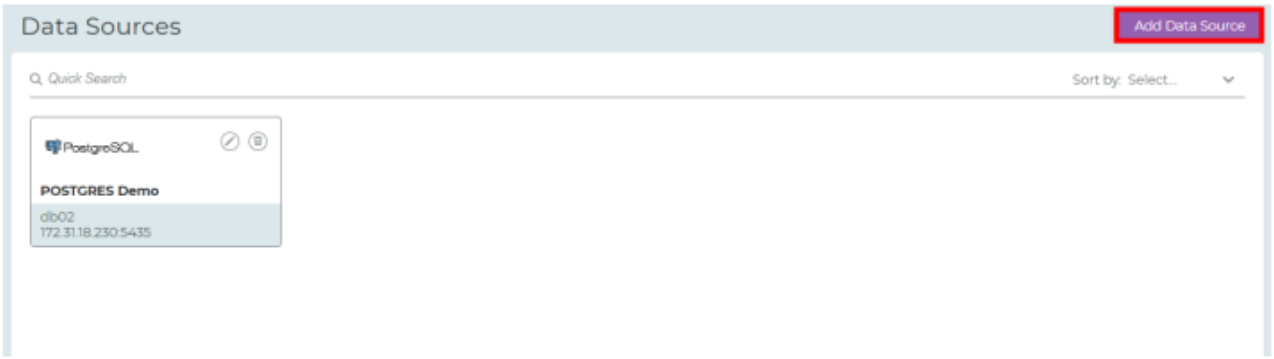


注意:
リスト表示はアルファベットの降順または昇順に並べ替えられます。

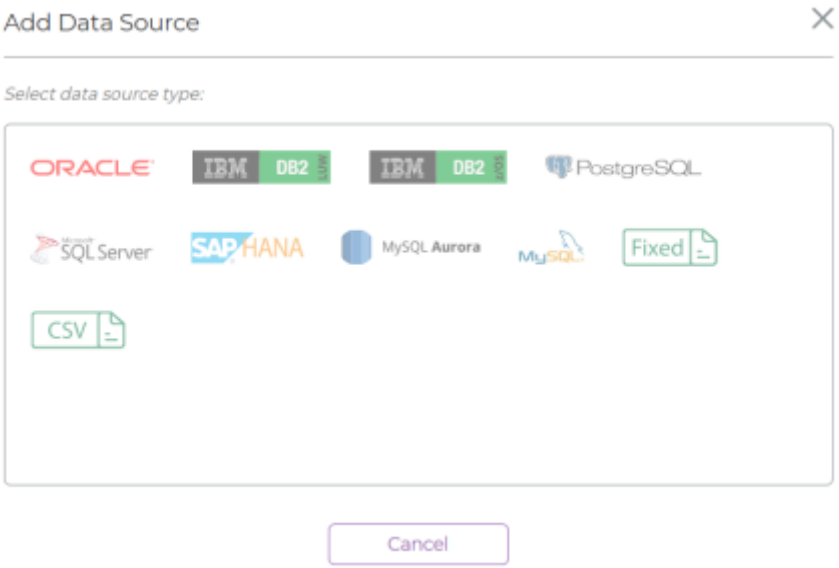


新しいデータソースを追加する手順は次のとおりです:

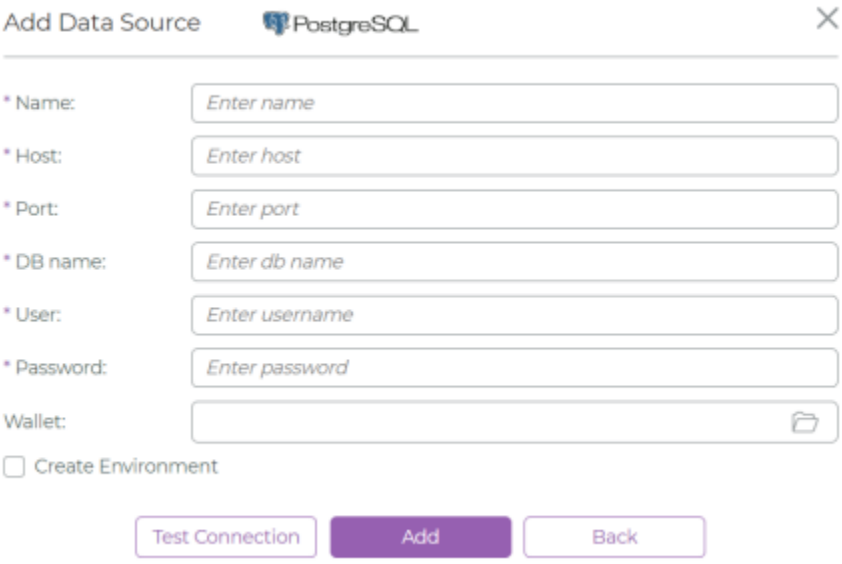
1. **Add Data Source** をクリックします。



2. ソースデータの種類を選択します。



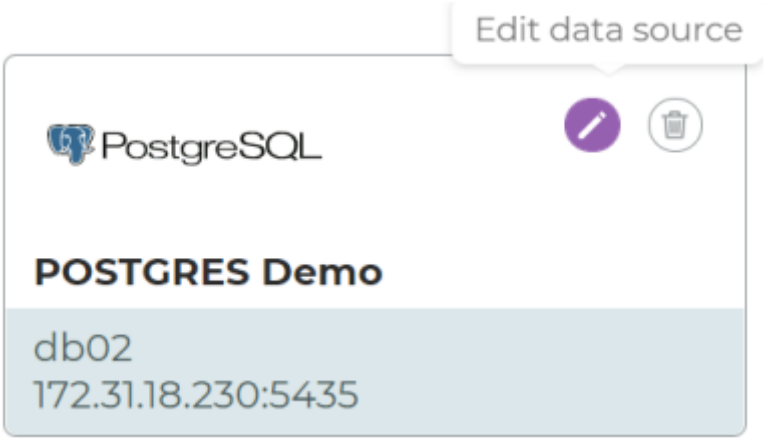
3. データソースの詳細を記入します。



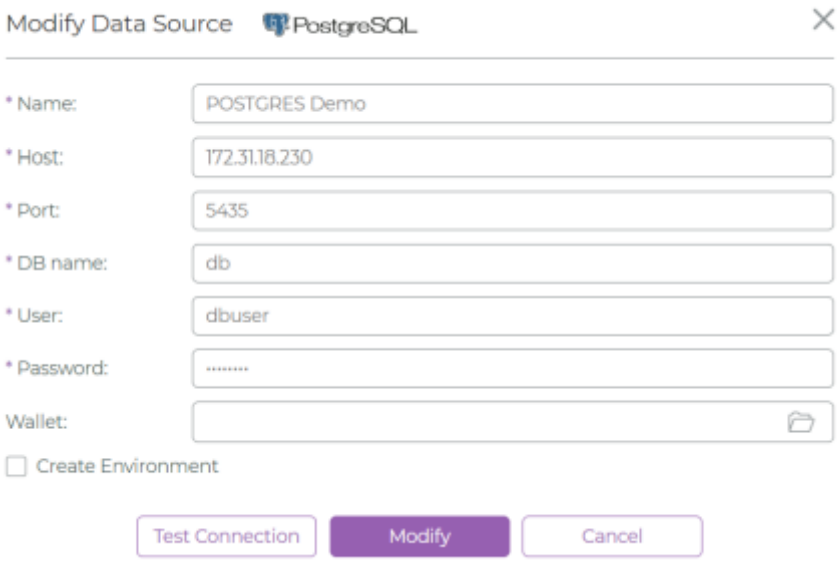
4. **Test Connection** をクリックして、新しいデータソースへの接続が有効かどうかを確認します。
5. **Add** をクリックします。

データソースの詳細を変更する手順は次のとおりです:

1. 目的のデータソースに対して（**Edit Data Source**）をクリックします。



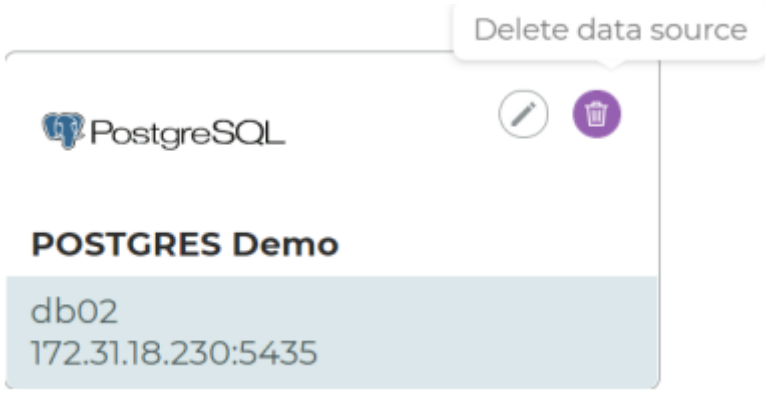
2. **Modify Data Source** ウィンドウが表示されるので、必要に応じて詳細情報を変更します。



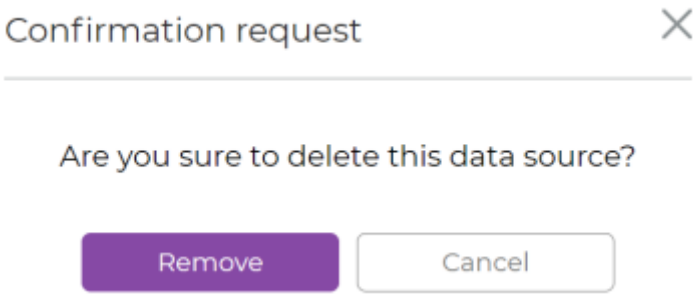
3. 変更を保存するには **Modify** を、保存したくない場合は **Cancel** をクリックします。

データソースを削除する手順は次のとおりです：

1. (**Delete Data Source**)をクリックします。



2. 削除を確定するには **Remove** を、確定しない場合は **Cancel** をクリックします。



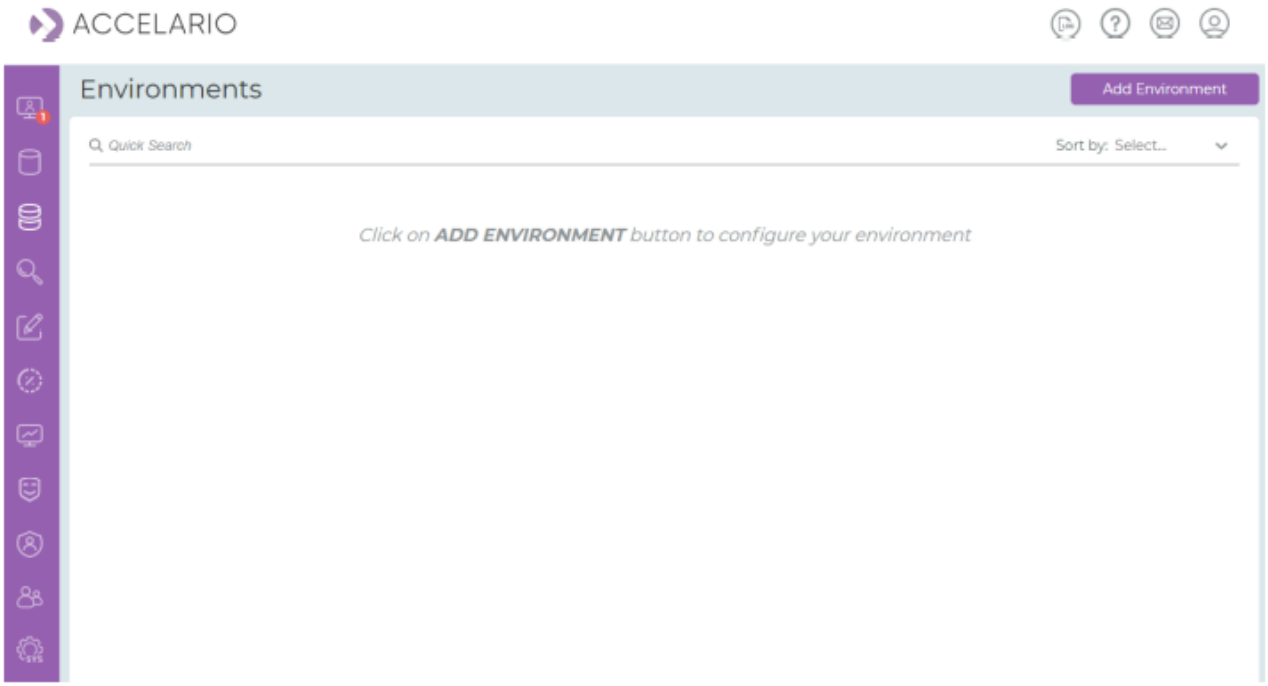
環境の管理

Environment(環境)とは、データソースからのデータベーススキーマを一まとめにグループ分けしたオブジェクトです。この環境オブジェクトを使用して、スキャニングとマスキングが実行されます。

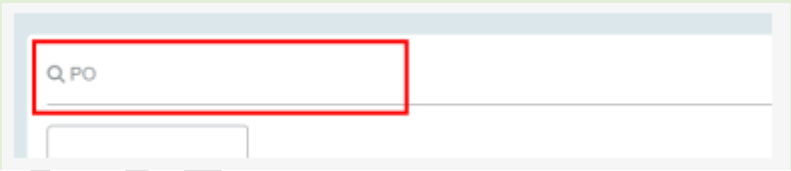
環境を表示する手順は次のとおりです:

1. ナビゲーションバーで(Environments)をクリックします。

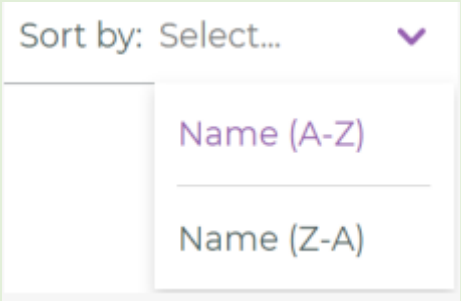
2. **Environments** ウィンドウが開きます。



注意:
Quick Search バーに文字列を入力すると、目的の環境をすぐに見つけることができます。検索によってリスト表示がすばやく更新されます。



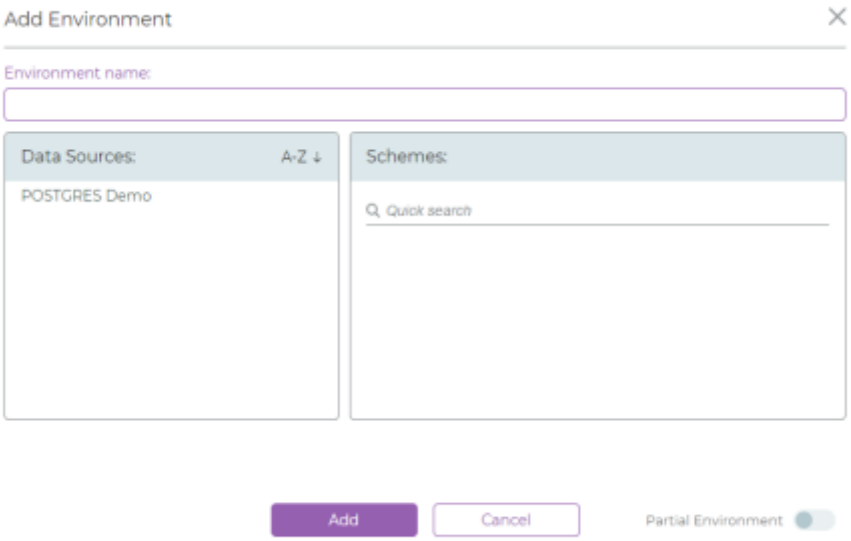
注意:
リスト表示はアルファベットの降順または昇順に並べ替えられます。



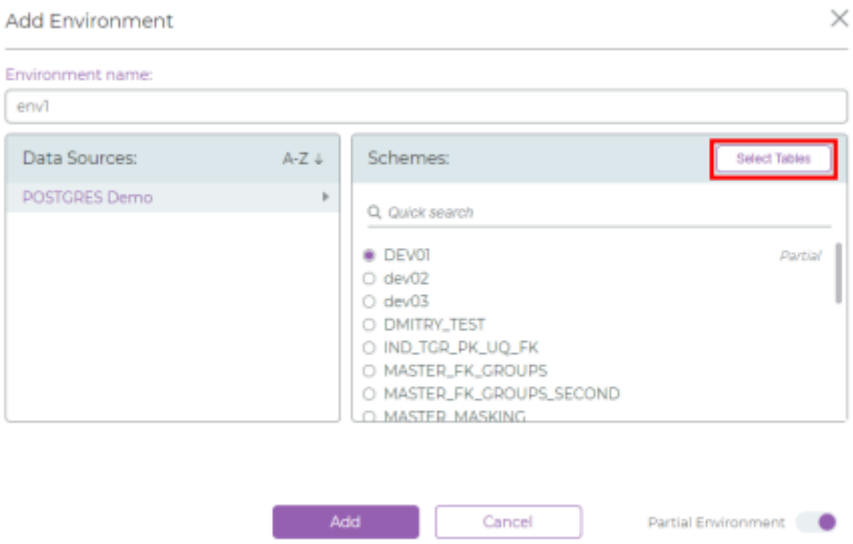
新しい環境を追加する手順は次のとおりです:

1. **Add Environment** をクリックします。

2. 環境の詳細を記入します。
   a. **Environment name** フィールドに環境名を入力します。
   b. **Data Sources** 欄で、追加する環境のデータソースを選択します。
   c. **Schemas** 欄で、環境に使用するデータソーススキーマを選択します。選択したデータソースの全スキーマを追加するには **Select All** をクリックします。



3. スキーマからテーブルを指定する場合は、
   a. Partial Environment をクリックします。
   b. **Select Tables** を開き、



   i. **Schema** を選択します。
   ii. 使用するテーブルを選択します。

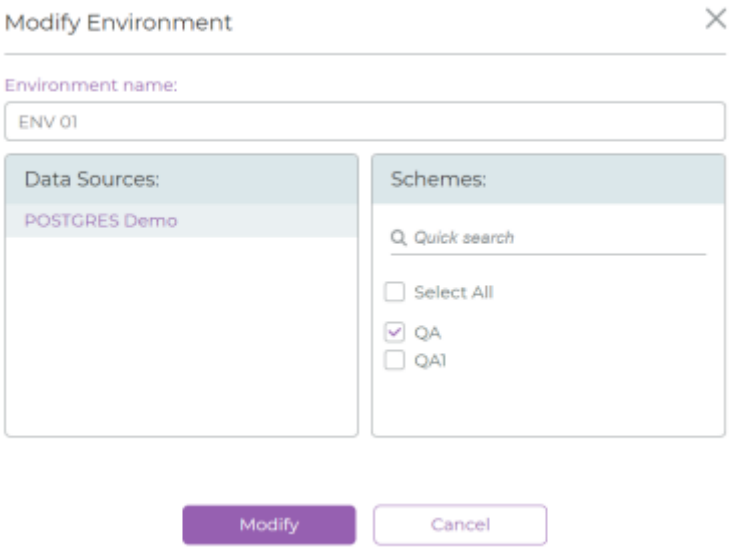
注意:

表示されるリストは、最後に更新されたときのリストです。リストを更新するには、**Refresh** をクリックします。

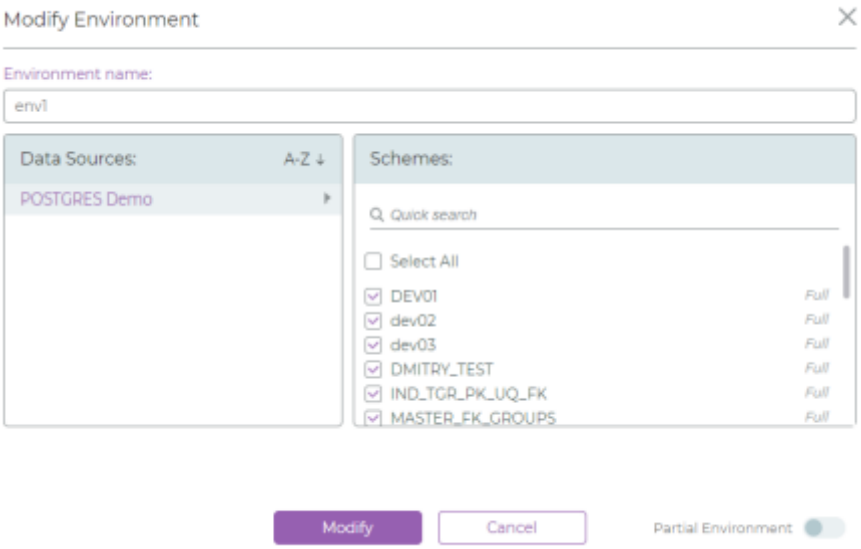
4. **Submit** をクリックします。
5. **Add** をクリックします。

環境の詳細を確認／変更する手順は次のとおりです：

1. 目的の環境に対して（**Edit environments**）をクリックします。



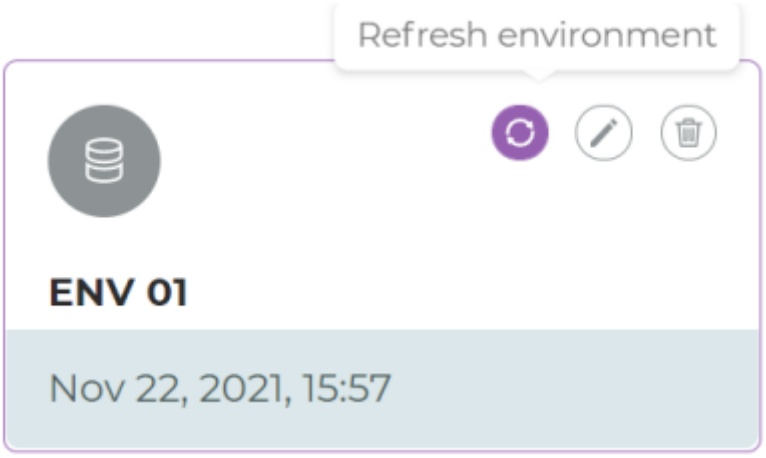
2. **Modify Environment** ウィンドウが表示されるので、必要に応じて詳細情報を変更します。



3. 変更を保存するには、**Modify** をクリックします。保存したくない場合は **Cancel** をクリックします。

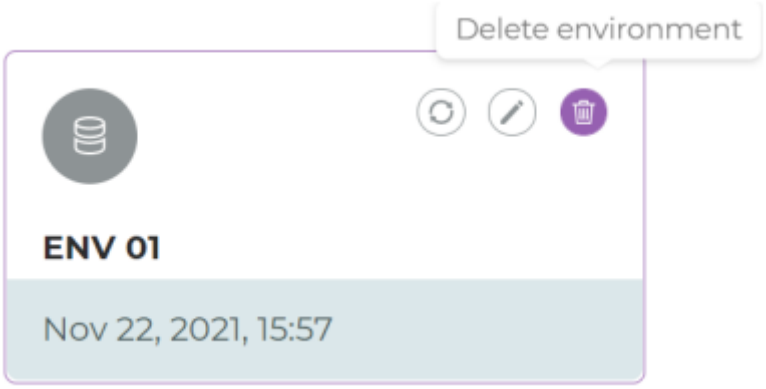
環境をリフレッシュする手順は次のとおりです:

1. 目的の環境に対して(**Refresh environment**)をクリックします。

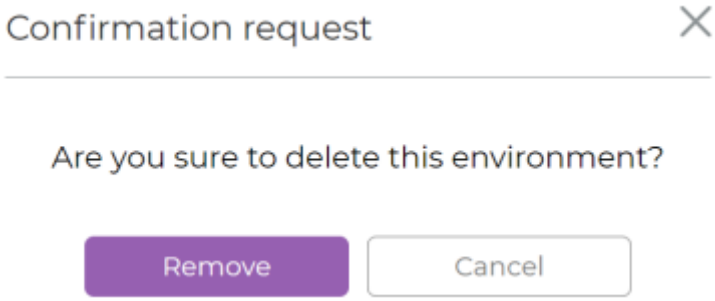


環境を削除する手順は次のとおりです:

1. 目的の環境に対して(**Delete environment**)をクリックします。



2. 削除を確定するには **Remove** を、削除しないで閉じるには **Cancel** をクリックします。



機密データの検索プロセス

Accelario Data Masking モジュールにはインテリジェント検索エンジンが搭載されており、ルックアップリストと AI テクノロジーを活用した高度な検索アルゴリズムによってスマートな検索が実行できます。

環境を設定したら、直ちに機密データを検索でき、その結果に応じてマスキングの適用を決定することができます。

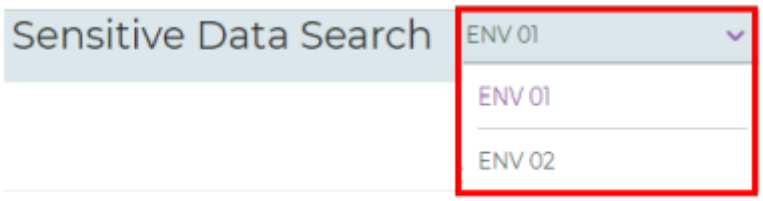
スキャニングの結果確認と新たなスキャニングの実行も簡単に行えます。

機密データの検索を管理する手順は次のとおりです:

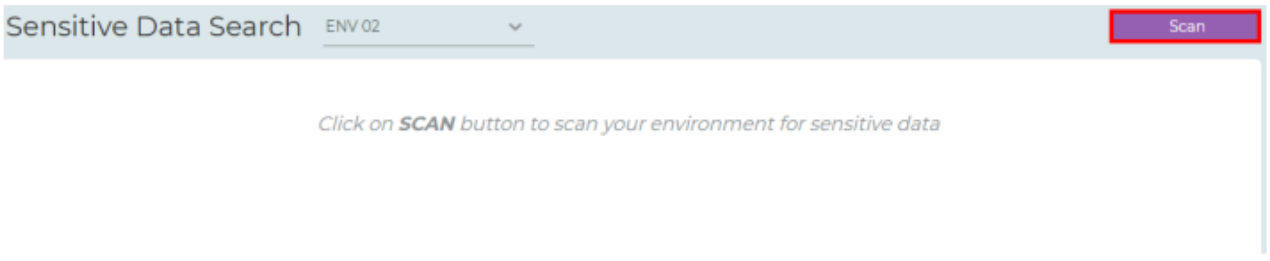
1. ナビゲーションバーで  (**Sensitive Search**)をクリックします。

新規の機密データ検索を実行する手順は次のとおりです:

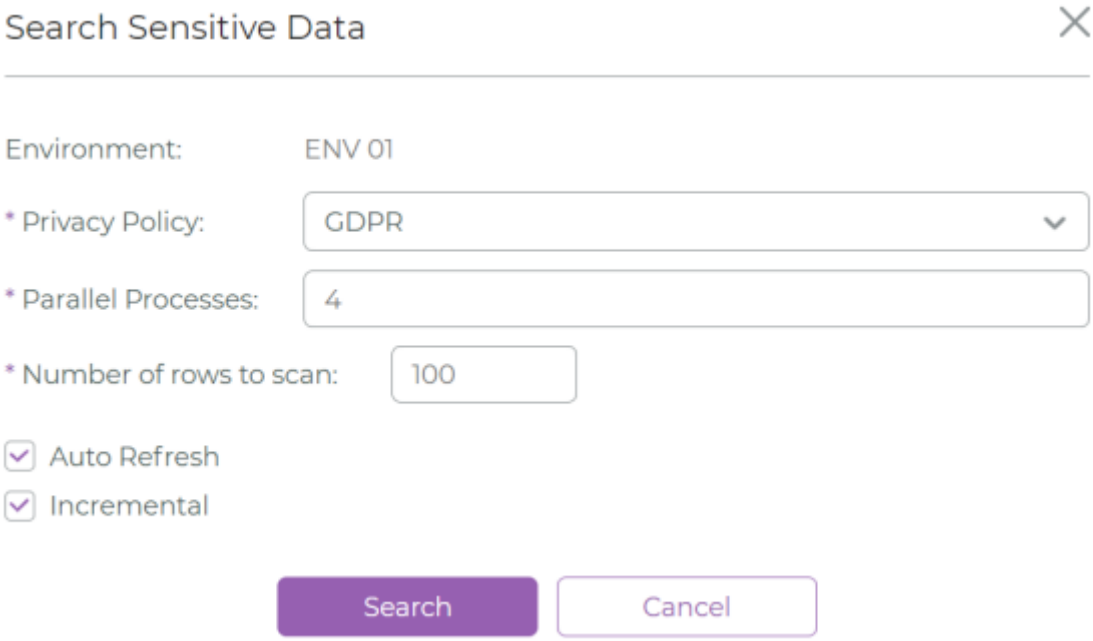
1. 機密データを検索する環境を選択します。



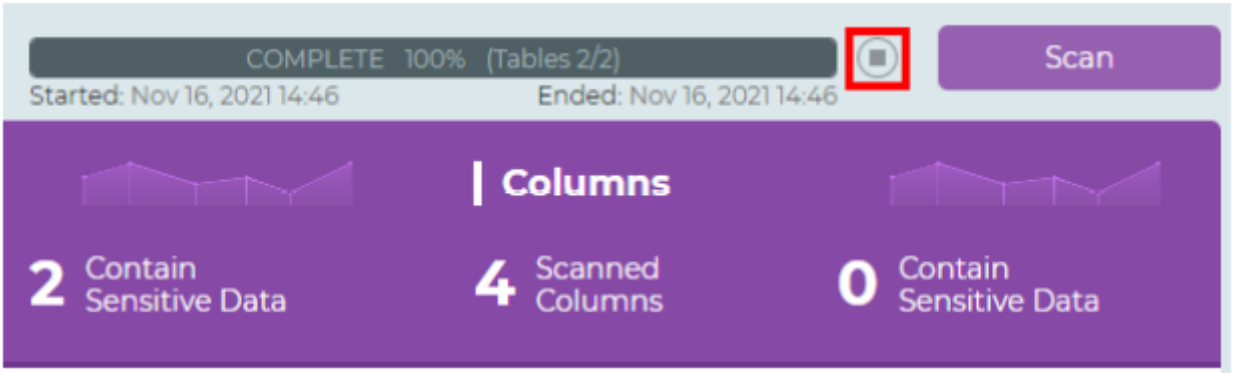
2. **Scan** をクリックします。



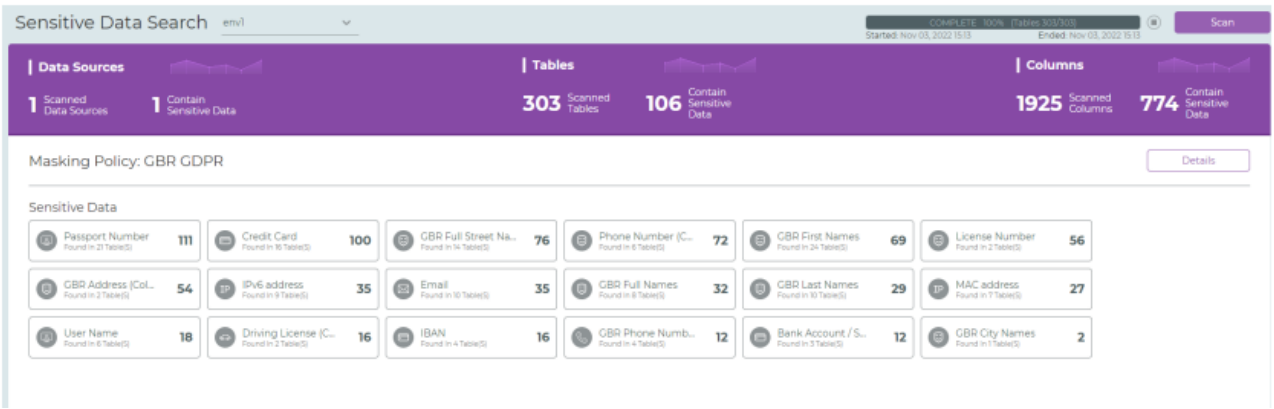
3. **Search Sensitive Data** ウィンドウで検索パラメータを設定してから **Search** をクリックします。



検索を停止するには (**Stop**)をクリックします。

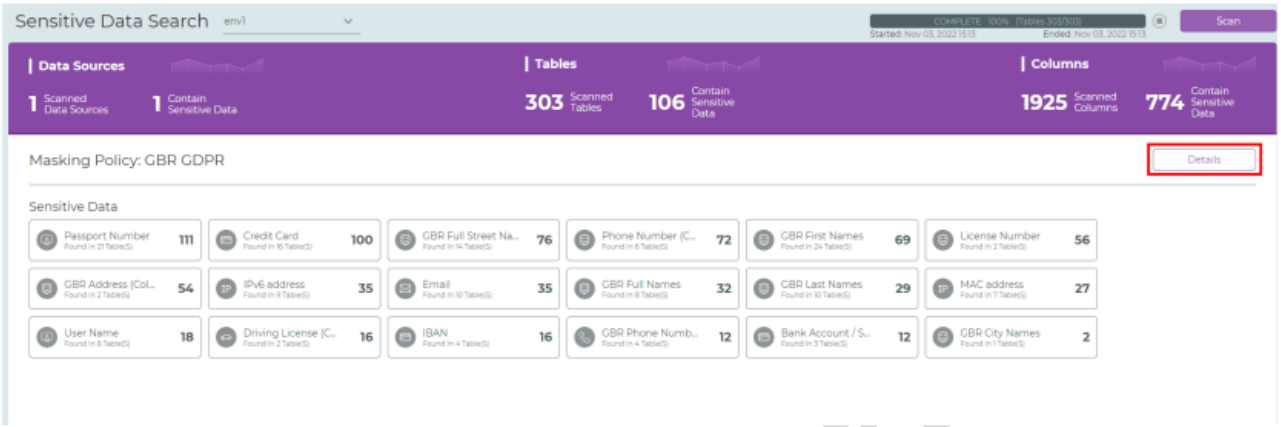


4. スキャニングが完了したら、スキャニング結果の概要が表示されます。



スキャニング結果の詳細を確認する手順は次のとおりです：

1. **Details** をクリックします。



2. 詳細ウィンドウでは以下の操作を行うことができます：

   - ⌄ をクリックして詳細を展開
   - チェックボックスを選択または解除して検索結果を更新
   - ファイル経由で結果を共有するには **Save to File** をクリック
   - テーブルの部分的なリストが表示される環境を作成するには **Hide low probability results** をクリック
   - **Update Masking** をクリックしてマスキングエディタを開く（詳しくは[マスキングエディタ - マスキングルールの変更とマスキング処理の実行]を参照）

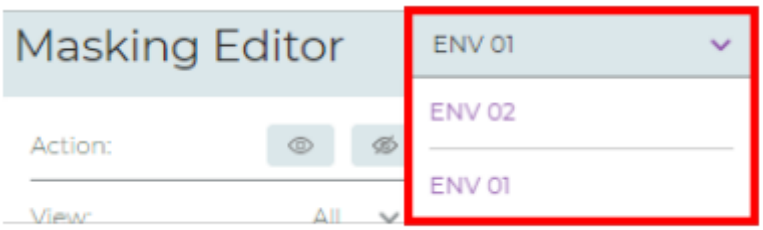
マスキングエディタ - マスキングルールの変更とマスキング処理の実行

マスキングエディタを使用すると、指定のテーブル／カラムにマスキングルールを適用することができます。

手順は次のとおりです：

1. ナビゲーションバーで  (**Masking Editor**)をクリックします。

2. 目的の環境を選択します。



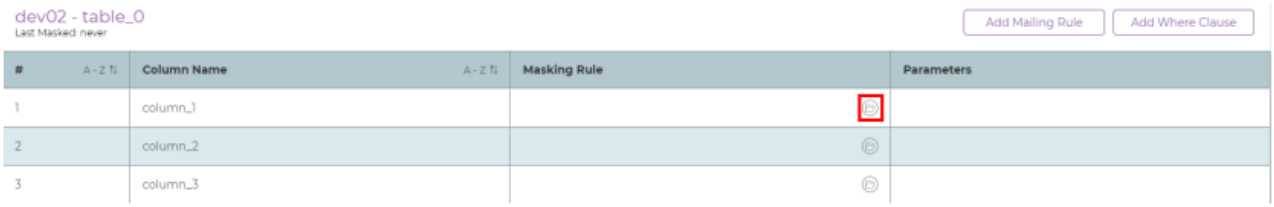
3. マスキングルールを適用したいテーブルを選択します。

注意:
テーブルのリストは各テーブルのステータスを有効または無効に設定することでフィルタリングできます。すべてのテーブルを表示するか、有効なテーブルまたは無効なテーブルのみを表示するように、画面を切り替えることができ、特定のテーブルを検索することもできます。

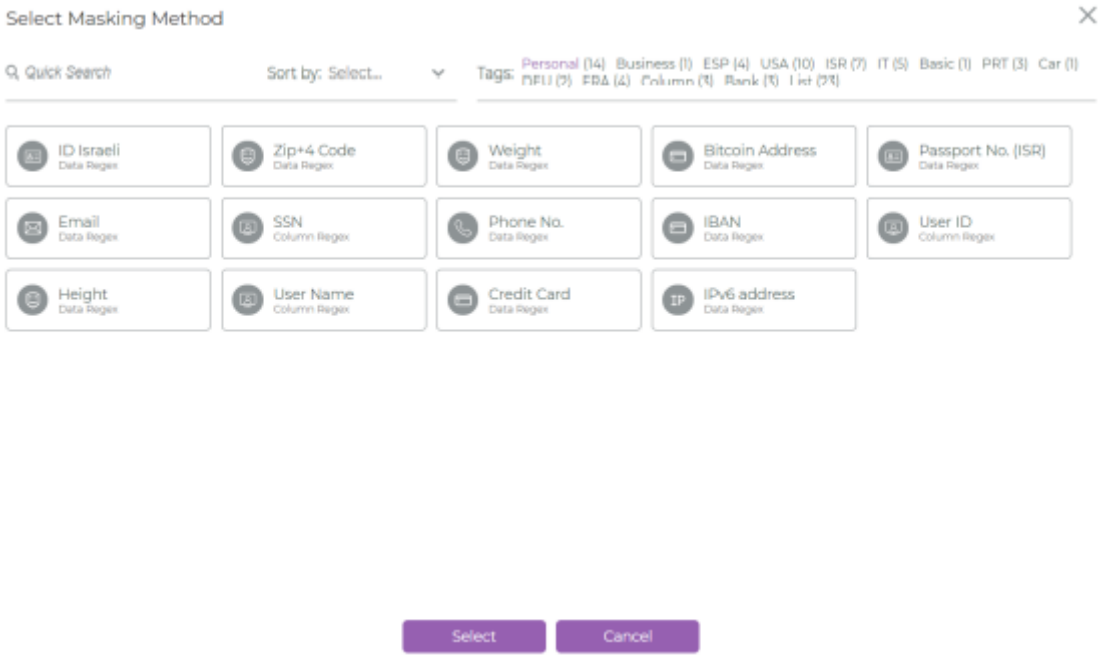
4. メインパネルには、選択したテーブルのカラムに現在適用されているマスキングルールが表示されます。

他のマスキングルールまたは新規のマスキングルールを確認する手順は次のとおりです:

1. 目的のカラムで  をクリックします。



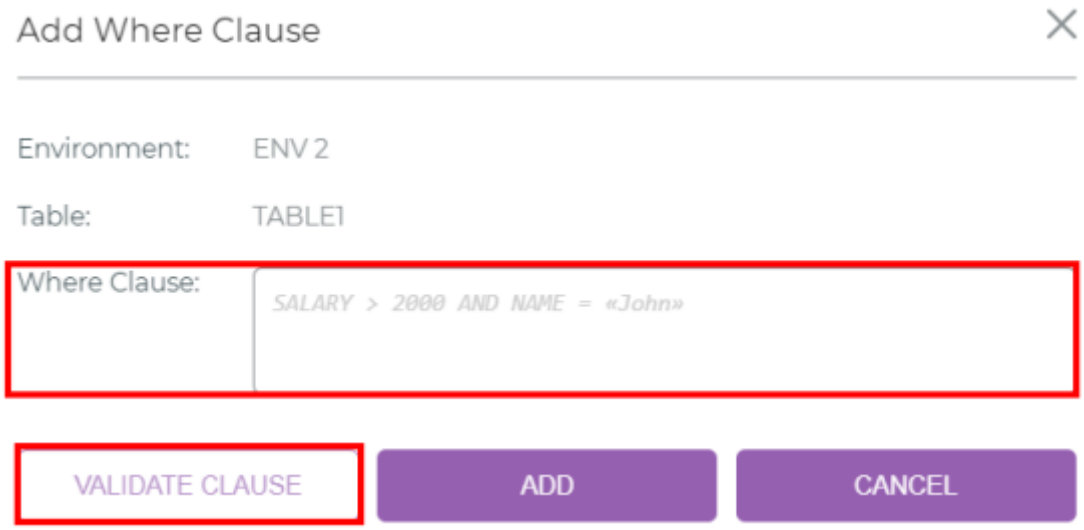
2. 表示したいマスキングルールをクリックしてから **Select** をクリックします。



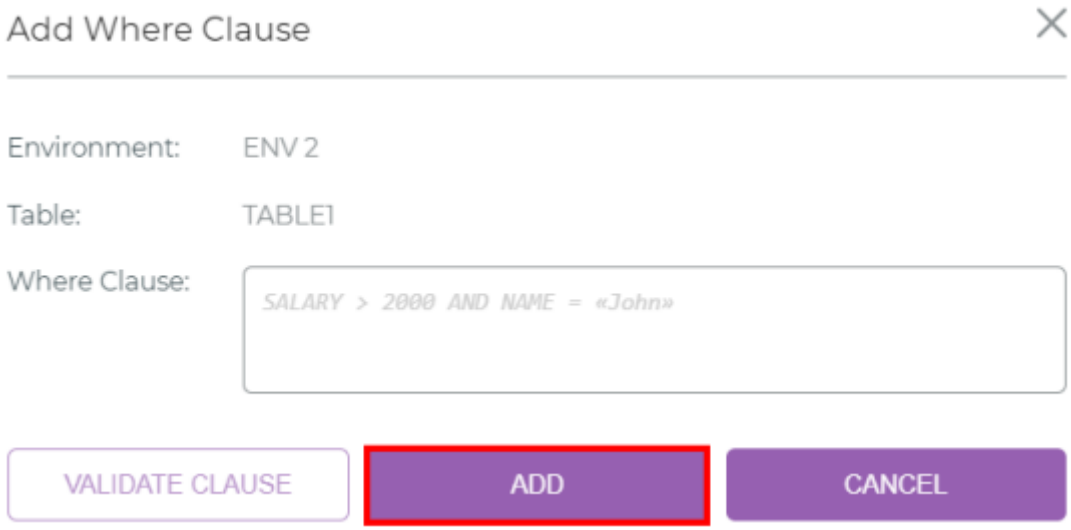
Where 句を追加する手順は次のとおりです:

1. **Add Where Clause** をクリックします。

2. Where 句を記述してから **VALIDATE CLAUSE** をクリックします。



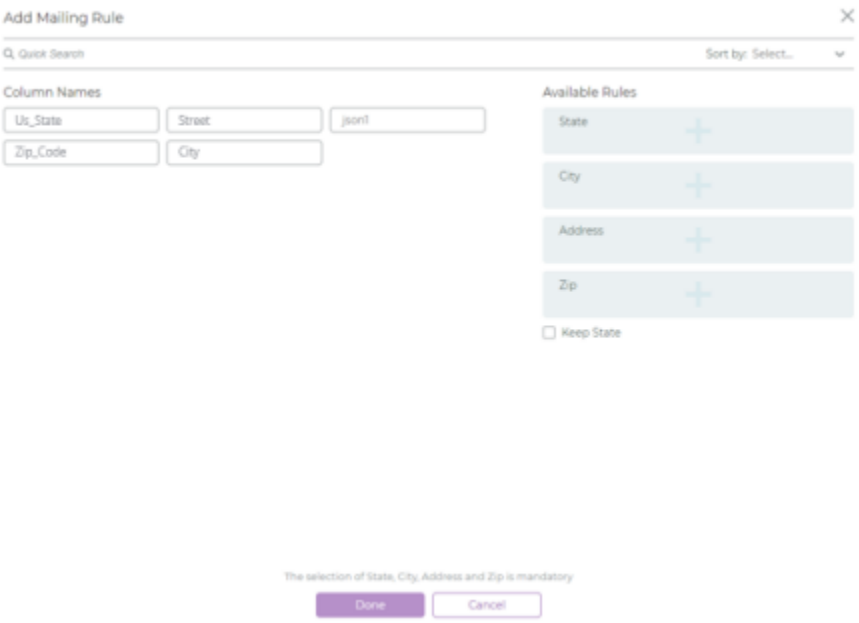
3. 確認が完了したら **ADD** をクリックします。



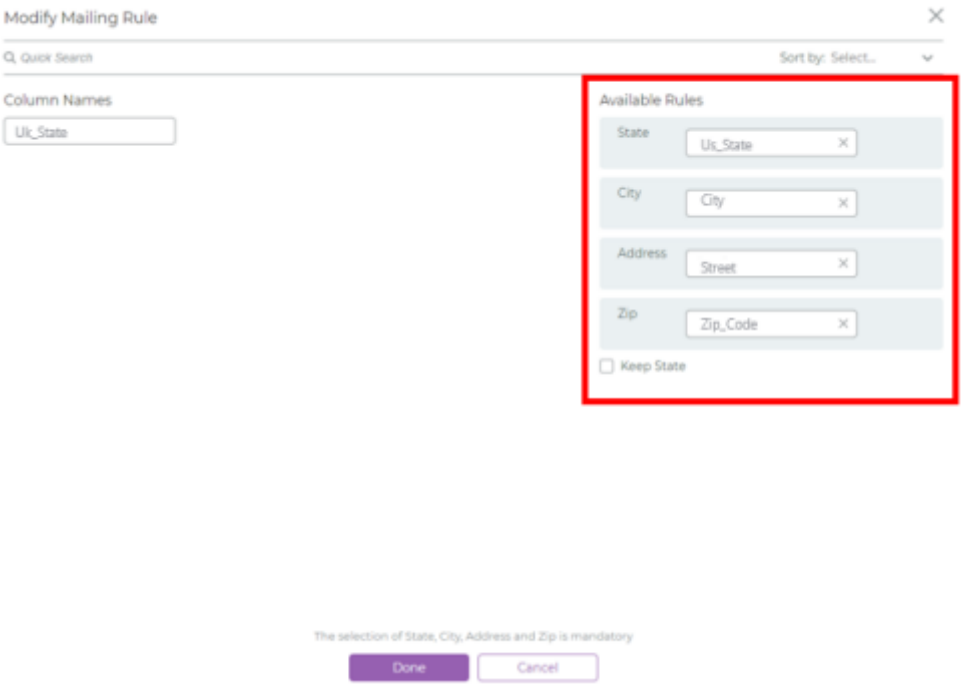
メーリングルールを追加する手順は次のとおりです：

1. **Add Mailing Rule** をクリックします。

Add Mailing Rule ウィンドウが表示されます。



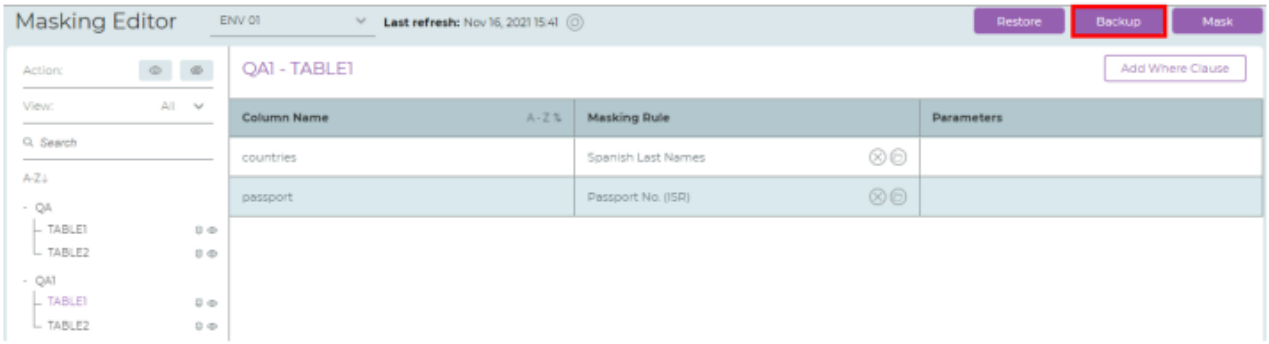
2. **Available Rules** にカラムをドラッグします。



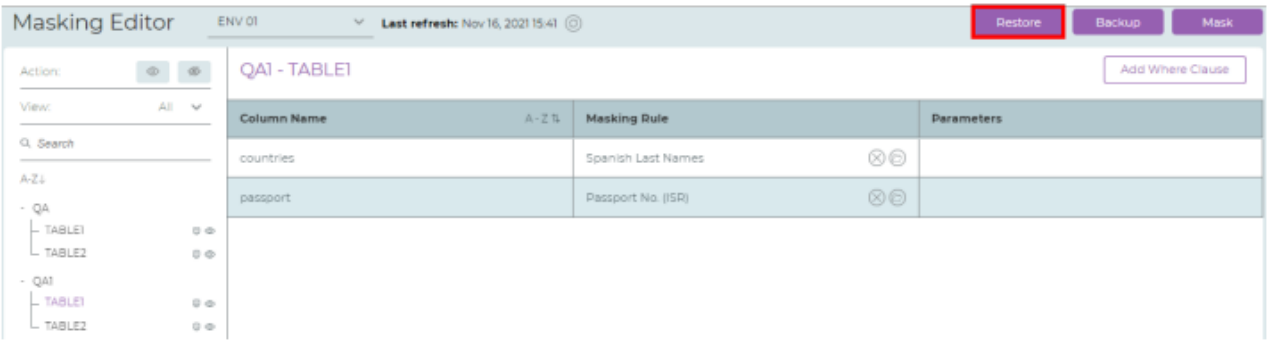
3. Keep State チェックボックスを選択して、State がマスクされていないことを確認し、他の Available Rules をマスクします。
4. **Done** をクリックします。

リストアとバックアップの手順は次のとおりです:

1. **Backup** をクリックすると、マスキング設定が JSON ファイルに保存されます。

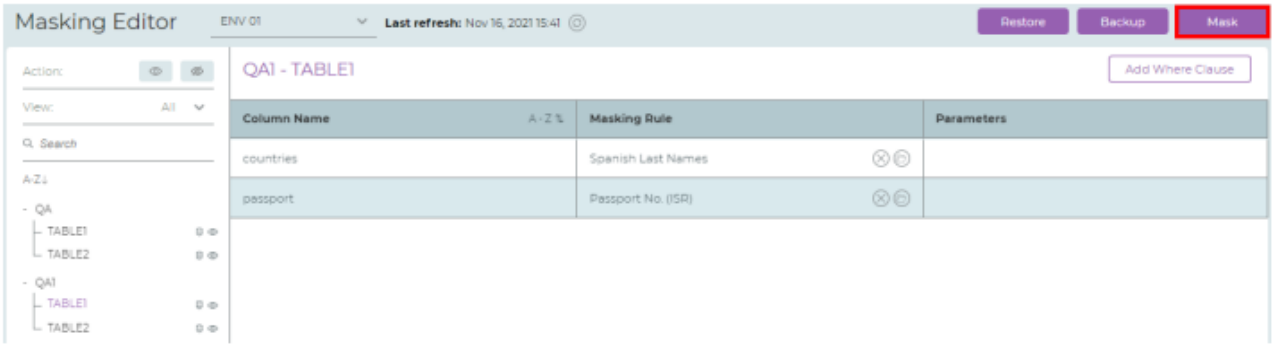


2. バックアップの JSON ファイルからマスキング設定をロードするには、**Restore** をクリックします。

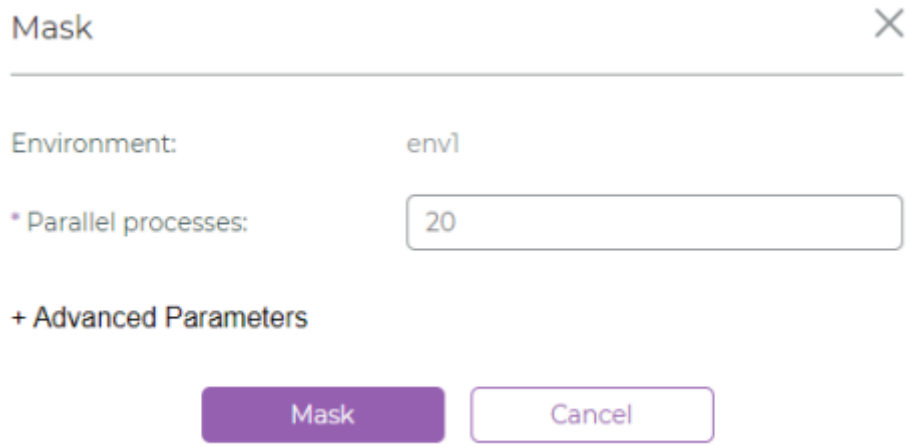


選択したテーブルをマスクする手順は次のとおりです:

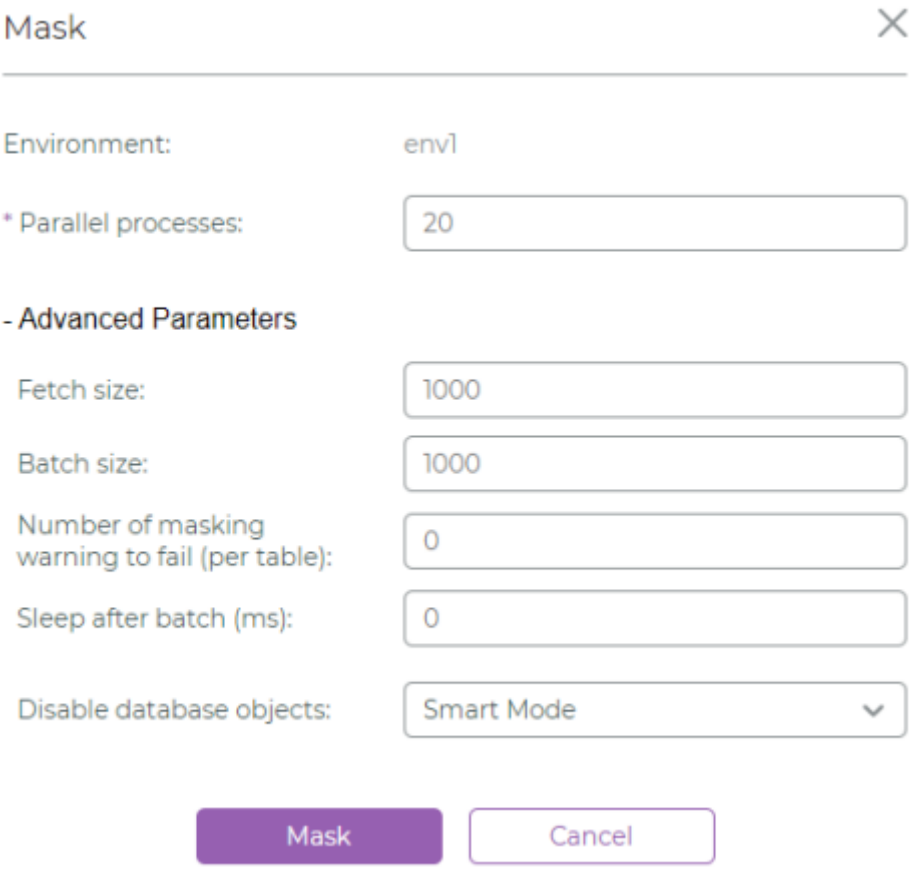
1. **Mask** をクリックします。



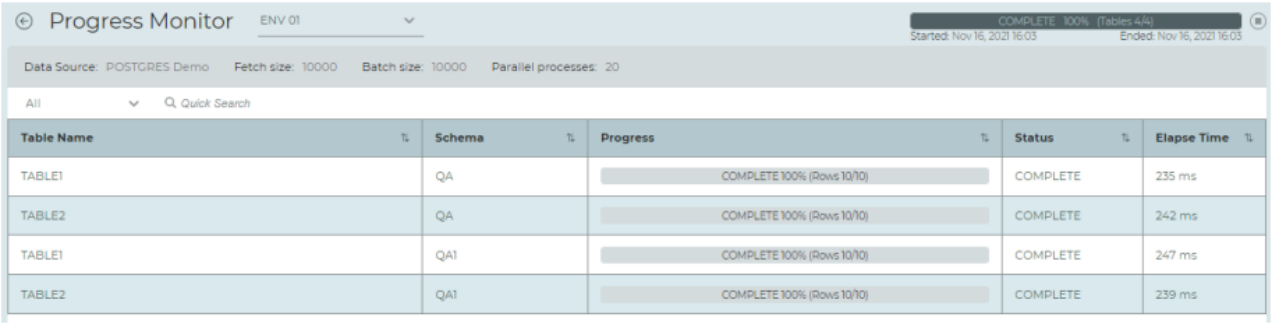
2. マスキングの詳細を記入したら、**Mask** をクリックします。



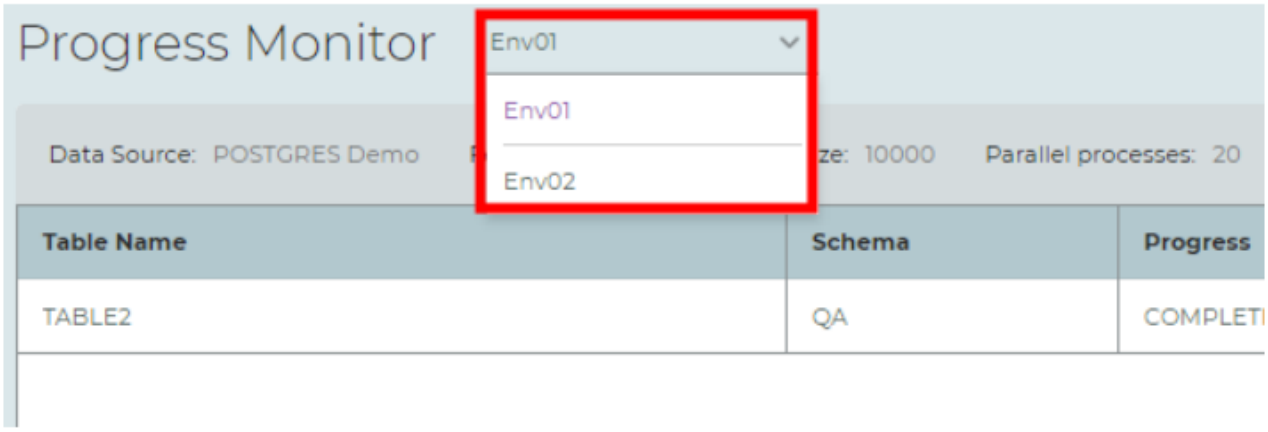
3. 必要に応じて、**Advanced Parameters** を入力します。



4. マスキングが開始されると、**Progress Monitor** が表示されます。



5. 他の環境での進捗状況を確認するには、 をクリックして、目的の環境を選択します。



ジョブモニタリングの GUI

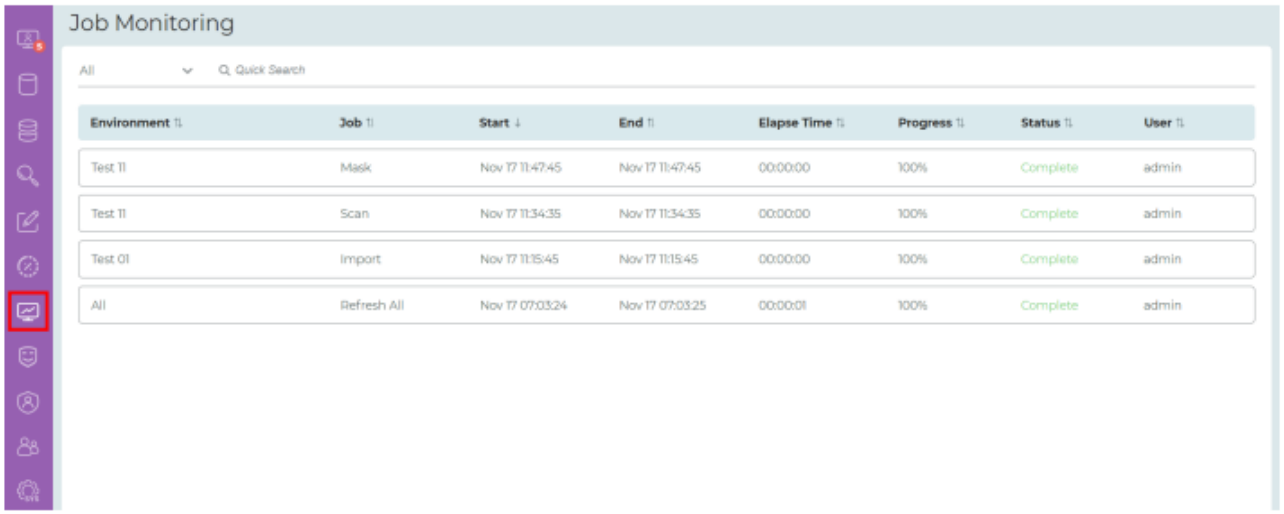
システムジョブの現在のステータスを確認するにはジョブモニタリング(Job Monitoring)を使用します。
Job Monitoring ウィンドウで以下の操作を行うことができます:

- Refresh、Scan、Mask などのシステムジョブの確認
- システムジョブをドリルダウンして詳細ステータスを確認

注意:
Job Monitoring にアクセスできるのは、管理者(**Admin**)権限を持つユーザに限られます。

ジョブモニタリングでステータスを確認する手順は次のとおりです:

1. ナビゲーションバーで  (**Job Monitoring**)をクリックします。

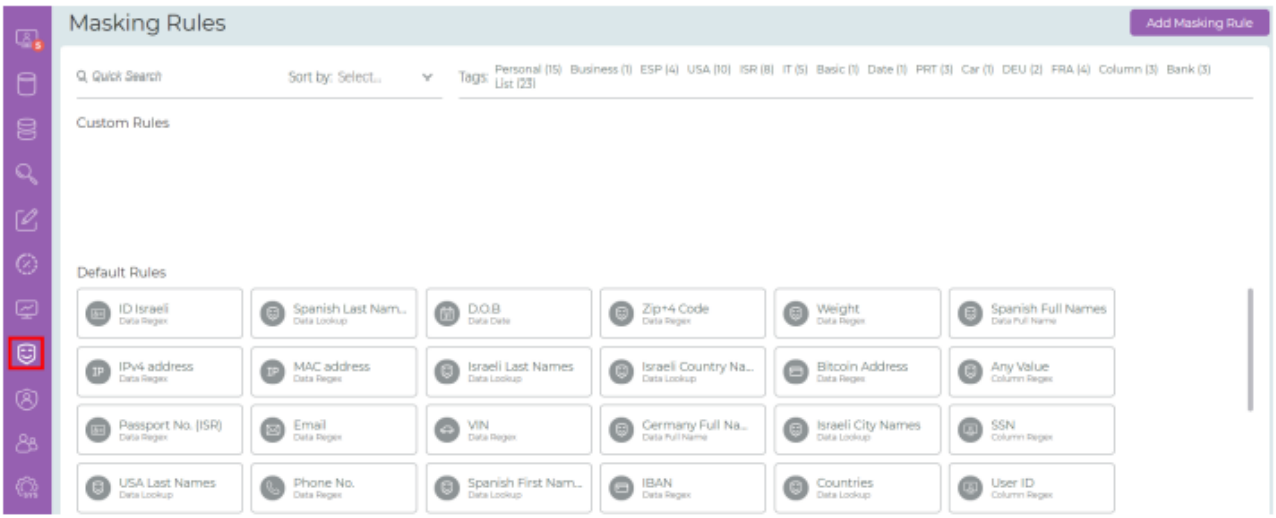


マスキングルールの管理

マスキングルールにはスキャニングやマスキングの方法に関する情報が含まれ、特定の機密データ(氏名、メールアドレス、クレジットカード番号など)の検索とマスキングに使用されます。

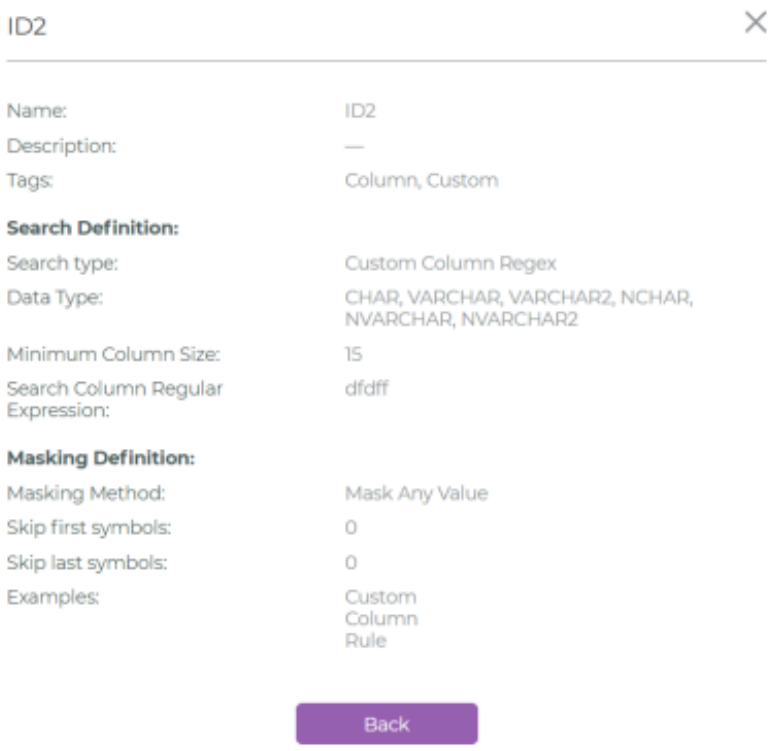
現在使用中のマスキングルールを確認する手順は次のとおりです:

1. ナビゲーションバーで(**Masking Rule**)をクリックします。



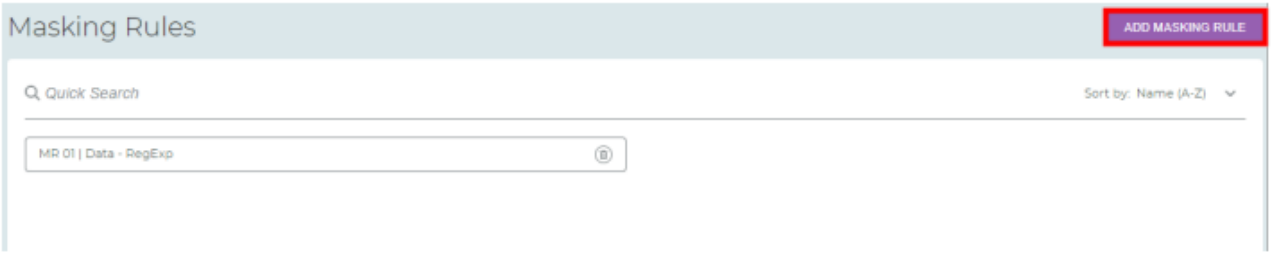
マスキングルールの詳細を確認する手順は次のとおりです:

1. 確認したいマスキングルールに対して をクリックします。

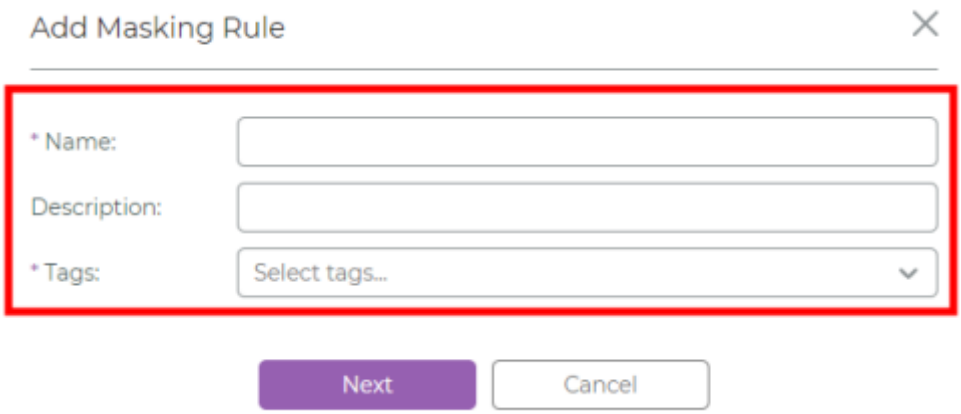


新しいマスキングルールを追加する手順は次のとおりです：

1. **ADD MASKING RULE** をクリックします。

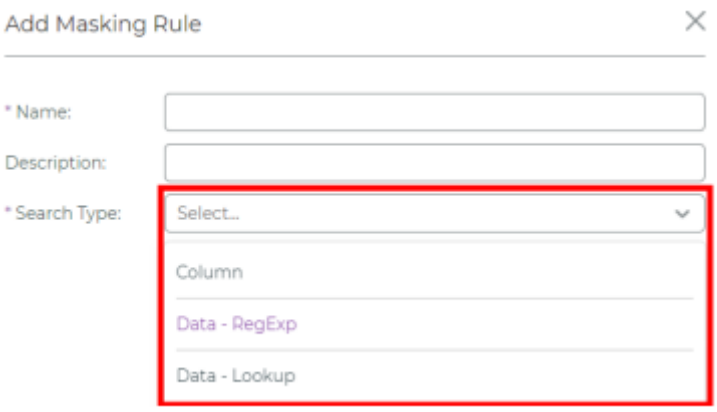


2. 新しいルールの名前と説明を入力し、必要な **Tags** を選択します。

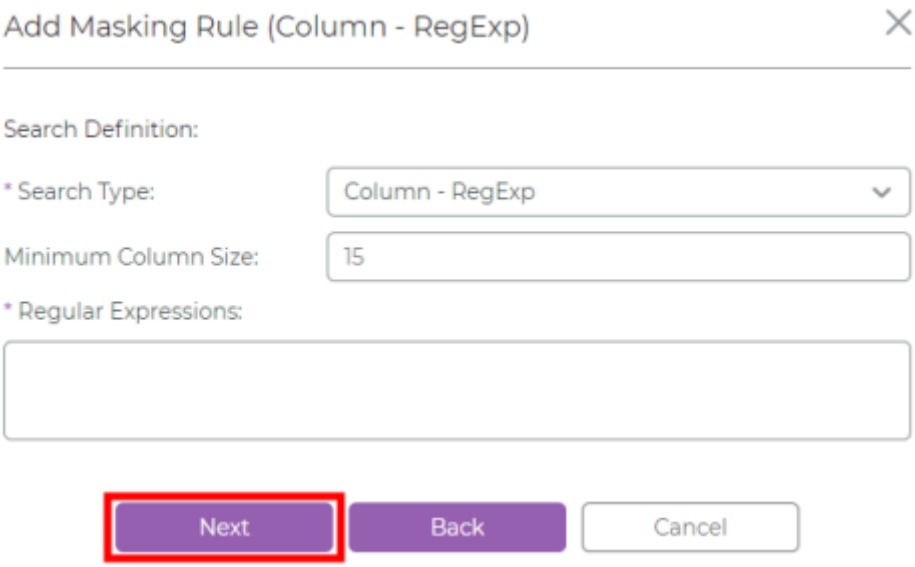


3. **Next** をクリックします。

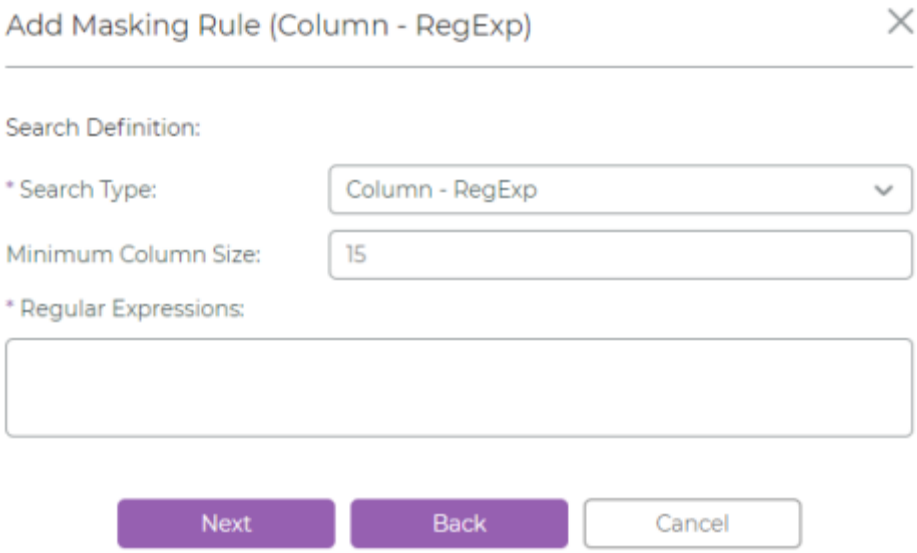
4. **Search Type** を選択します：
   a. **Column - RegExp** — 通常の語句検索でカラム名を検索します。
   b. **Data - RegExp** — 通常の語句検索でカラムデータを検索します。
   c. **Data - Lookup** — ルックアップテーブルを使用してカラムデータを検索します。



5. **Next** をクリックします。

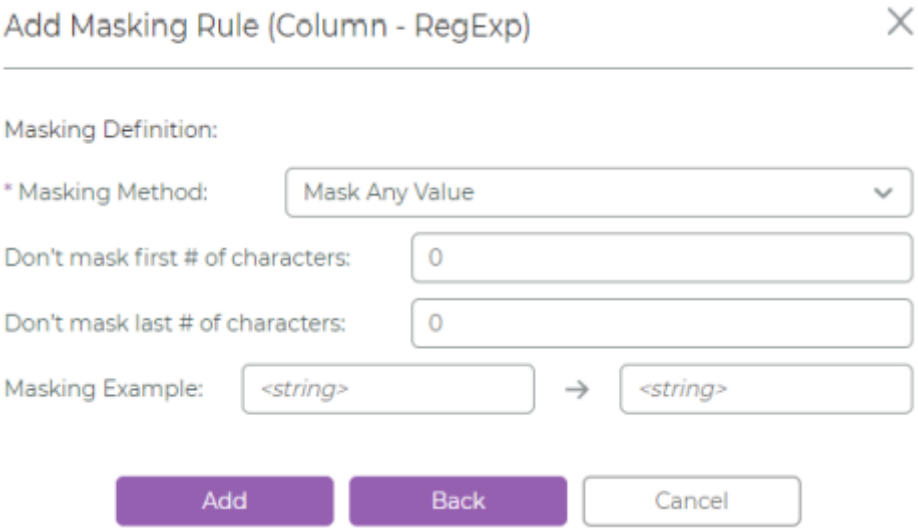


6. **Column - RegExp** 検索タイプを選択した場合は、次の手順でマスキングルールのパラメータを設定します：
   a. **Search Definition** に、**Column Regular Expressions**（通常のカラム検索語句）を記入します。



   b. **Next** をクリックします。

c. **Masking Definition** に、必要に応じてマスクの対象外とする最初の文字数または最後の文字数を記入します。

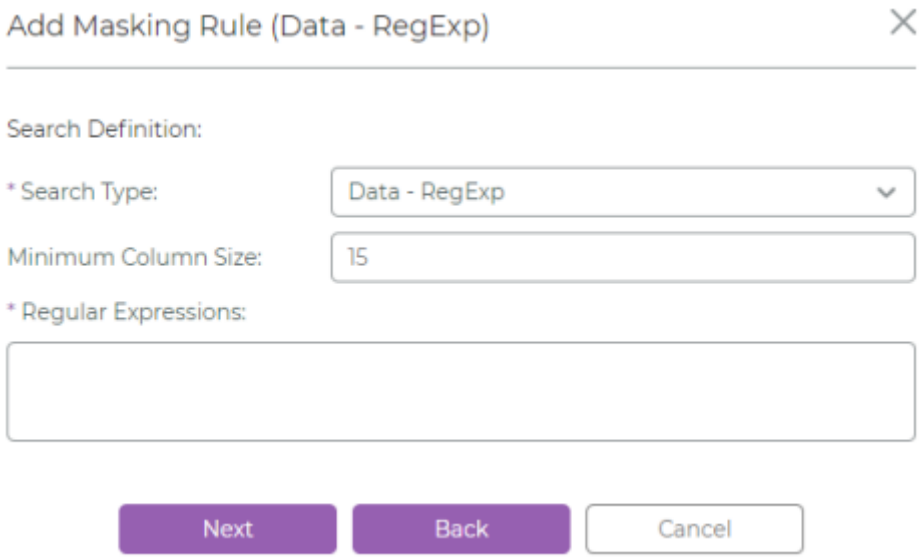


d. **ADD** をクリックします。

以上により、作成された新しいマスキングルールが表示されます。

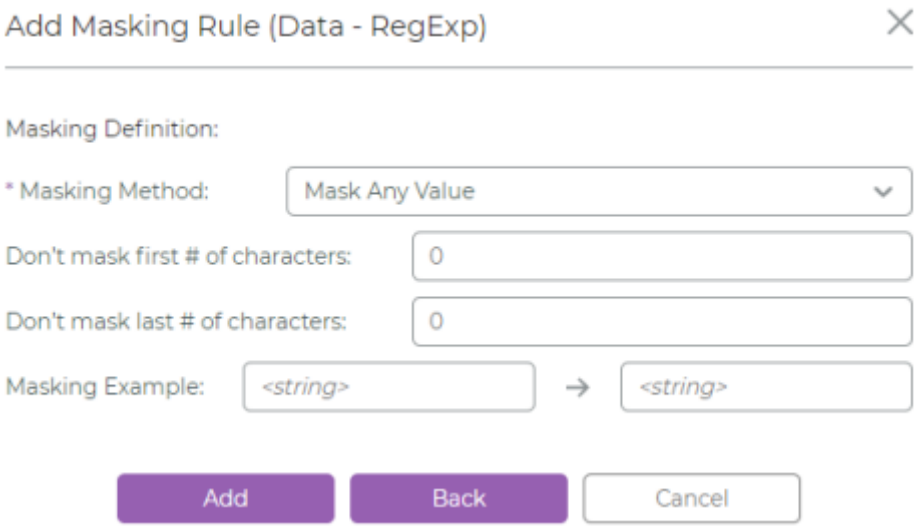
7. **Data - RegExp** 検索タイプを選択した場合は、次の手順でマスキングルールのパラメータを設定します。

a. **Search Definition** に、**Data Regular Expressions**（通常のデータ検索語句）を記入します。



b. **Next** をクリックします。

c. **Masking Definition** に、必要に応じてマスクの対象外とする最初の文字数または最後の文字数を記入します。

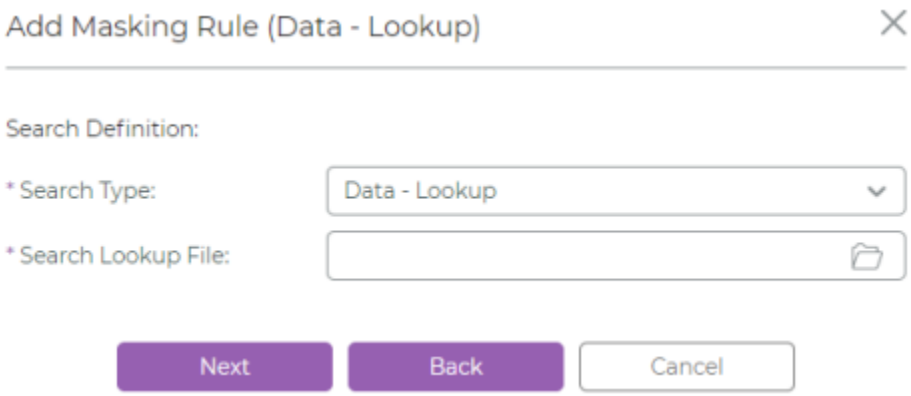


d. **ADD** をクリックします。

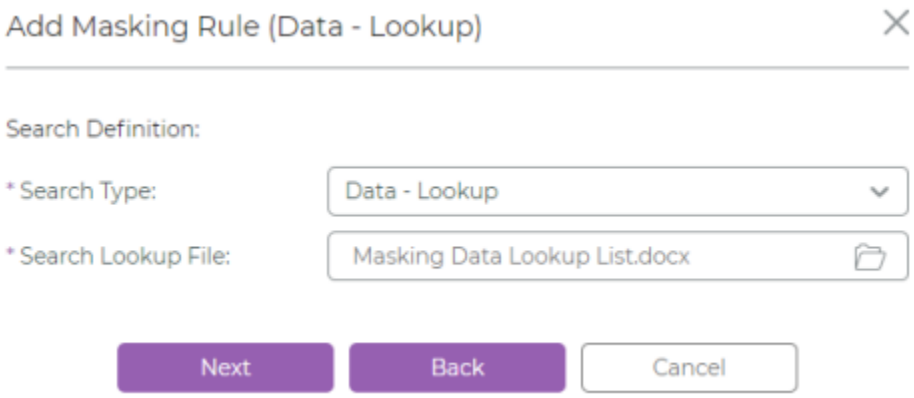
以上により、作成された新しいマスキングルールが表示されます。

8. **Data - Lookup** 検索タイプを選択した場合は、次の手順でマスキングルールのパラメータを設定します。

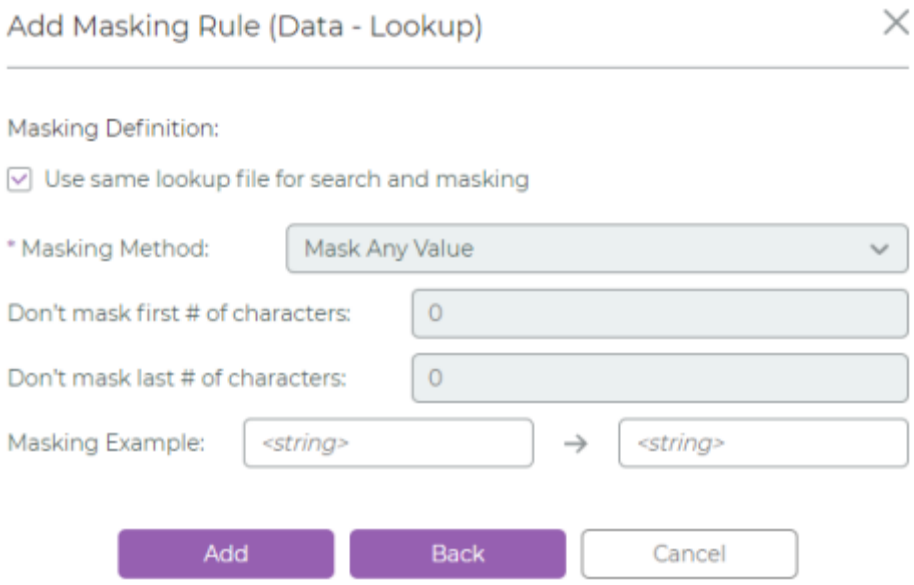
a. **Search Definition** で、**Masking Lookup List** の場所を指定して **Open** をクリックします。



b. ファイルがロードされたら **Next** をクリックします。



c. **Masking Definition** に、必要に応じてマスクの対象外とする最初の文字数または最後の文字数を記入します。

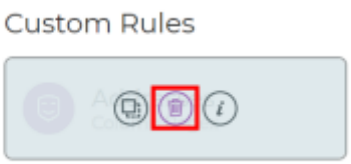


d. **Add** をクリックします。

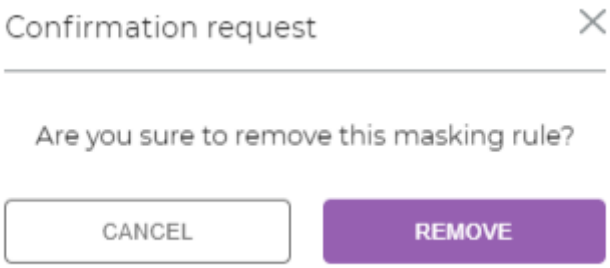
以上により、作成された新しいマスキングルールが表示されます。

カスタムマスキングルールを削除する手順は次のとおりです:

1. 削除したいマスキングルールに対して  をクリックします。

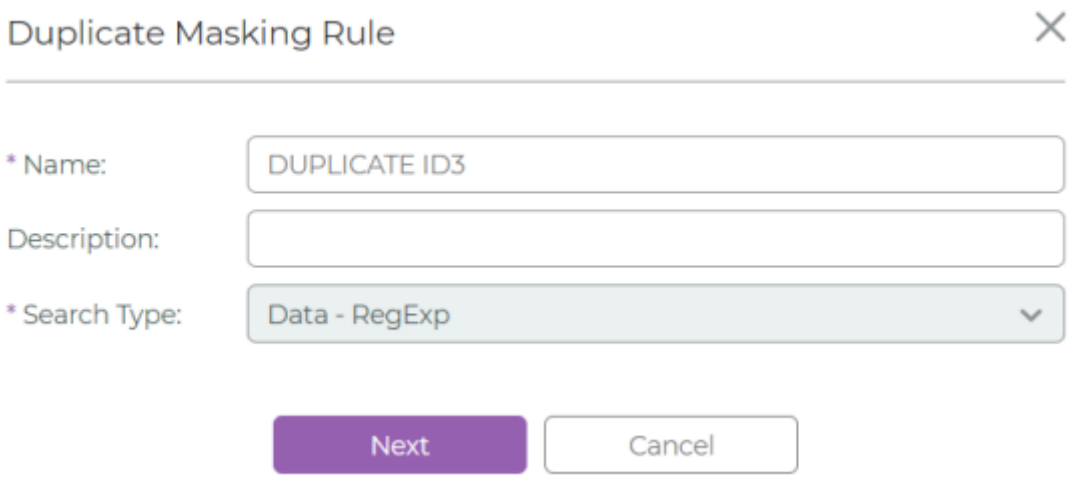


2. 削除を確定するには **REMOVE** を、削除せずに画面を閉じるには **CANCEL** クリックします。



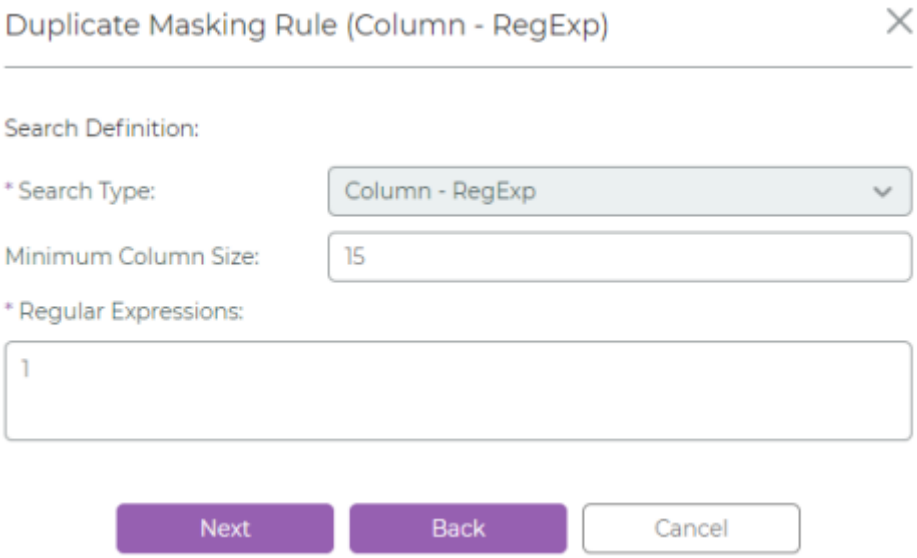
マスキングルールをコピーする手順は次のとおりです:

1. コピーしたいマスキングルールに対して をクリックします。
2. 新しいルール名を記入します。



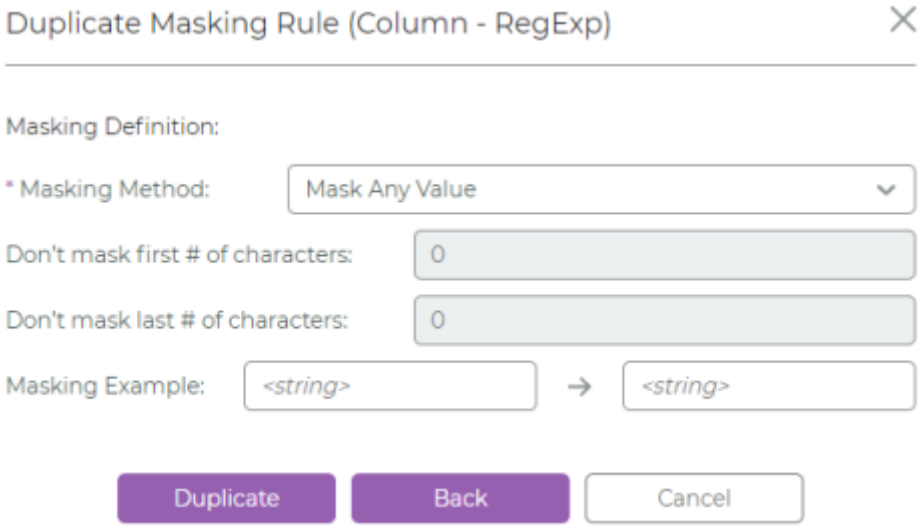
3. **NEXT** をクリックします。

4. **Data Regular Expressions**(通常のデータ検索語句)を記入します。



注意:
Minimum Column Size(最小カラムサイズ)も変更できます。

5. **NEXT** をクリックします。



6. **Duplicate** をクリックします。

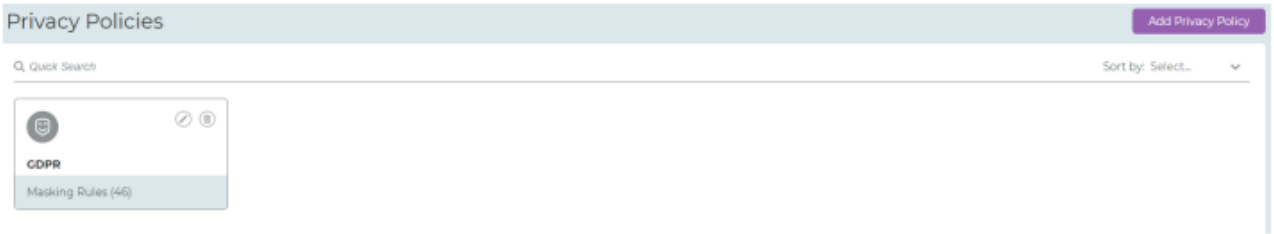
プライバシーポリシーの管理

Privacy Policy(プライバシーポリシー)とは、GDPR(EU 一般データ保護規則)、CCPA(カリフォルニア州消費者プライバシー法)、HIPPA(医療保険の相互運用性と説明責任に関する法律)などの各種規制や、社内のプライバシールールを遵守するために適用するスキャニングとマスキングのためのマスキングルールのセットを指します。このセクションでは、プライバシーポリシーの定義方法と管理方法を説明します。

既存のプライバシーポリシーを確認する手順は次のとおりです:

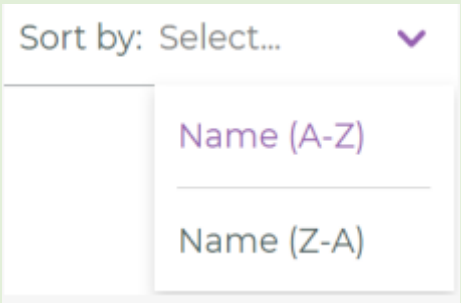
1. ナビゲーションバーで  (**Privacy Policies**)をクリックします。

2. **Privacy Policies** ウィンドウが開いて、システムに追加済みのすべてのプライバシーポリシーが表示されます。



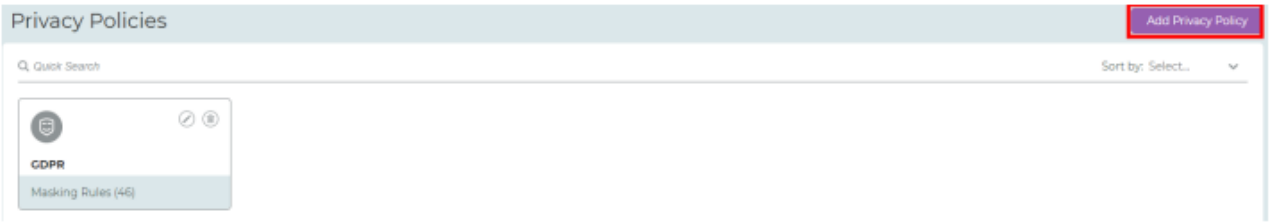
注意:
Quick Search バーに文字入力すると、必要なプライバシーポリシーを迅速に見つけることができます。検索によってリスト表示がすばやく更新されます。

注意:
リスト表示はアルファベットの降順または昇順に並べ替えられます。

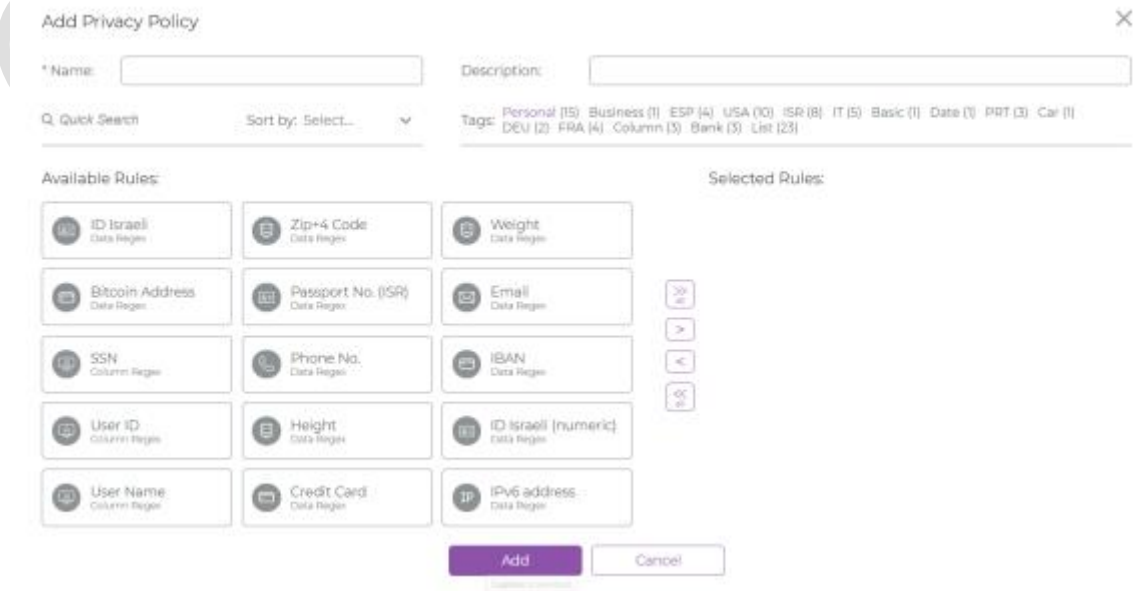


新しいプライバシーポリシーを追加する手順は次のとおりです:

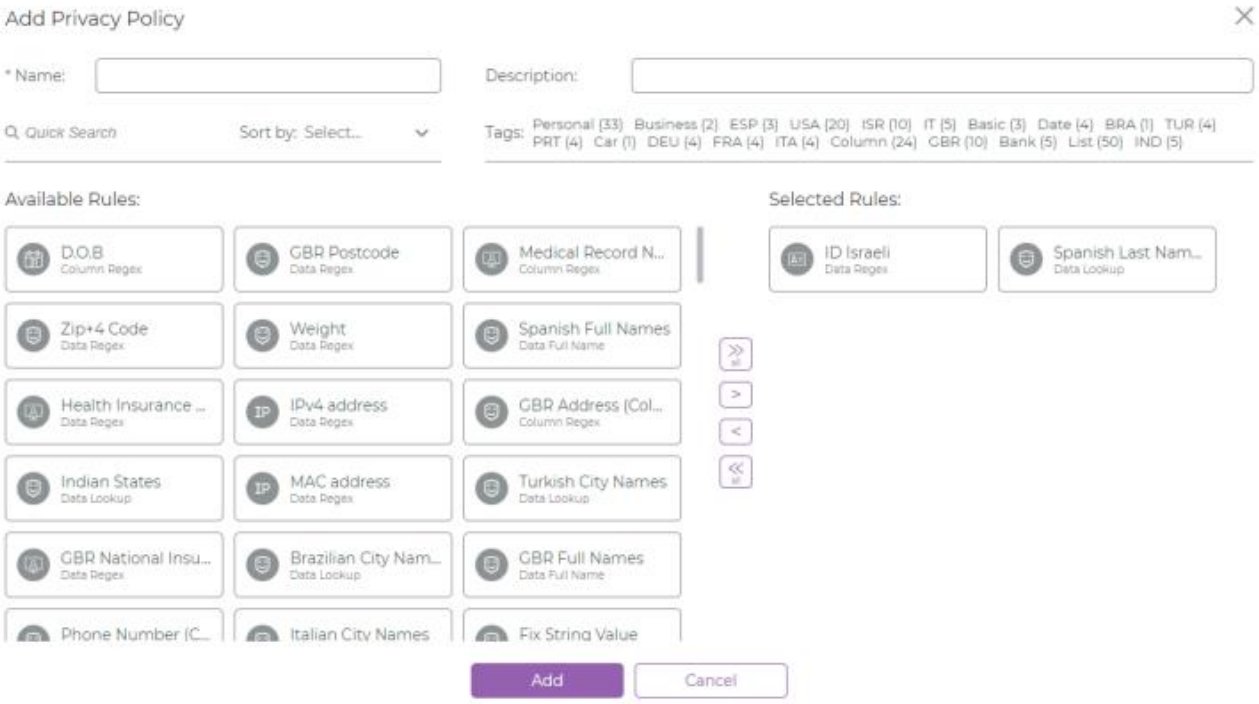
1. **Add Privacy Policy** をクリックします。



2. ポリシーの詳細を記入します:
   a. **Name** にポリシー名を記入します。
   b. **Available Rules** からルールを選択します。
3. 必要に応じて、**Advanced Parameters** を入力します。



4. > をクリックして、**Selected Rules** リストにルールを追加します。**Add** をクリックします。



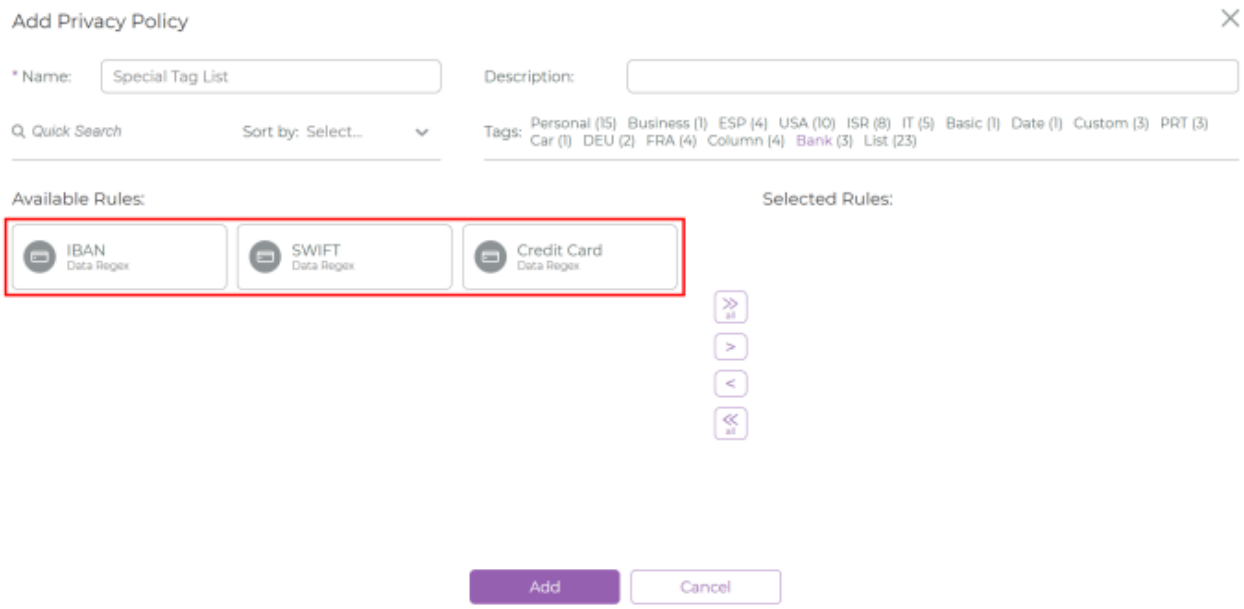
注意:

- 利用可能なすべてのルールを追加するには » をクリックします。
- 既存のすべてのルールを削除するには « をクリックします。
- 1 つのルールだけを削除するには < をクリックします。

タグをもとにマスキングルールをプライバシーポリシーに追加する手順は次のとおりです:

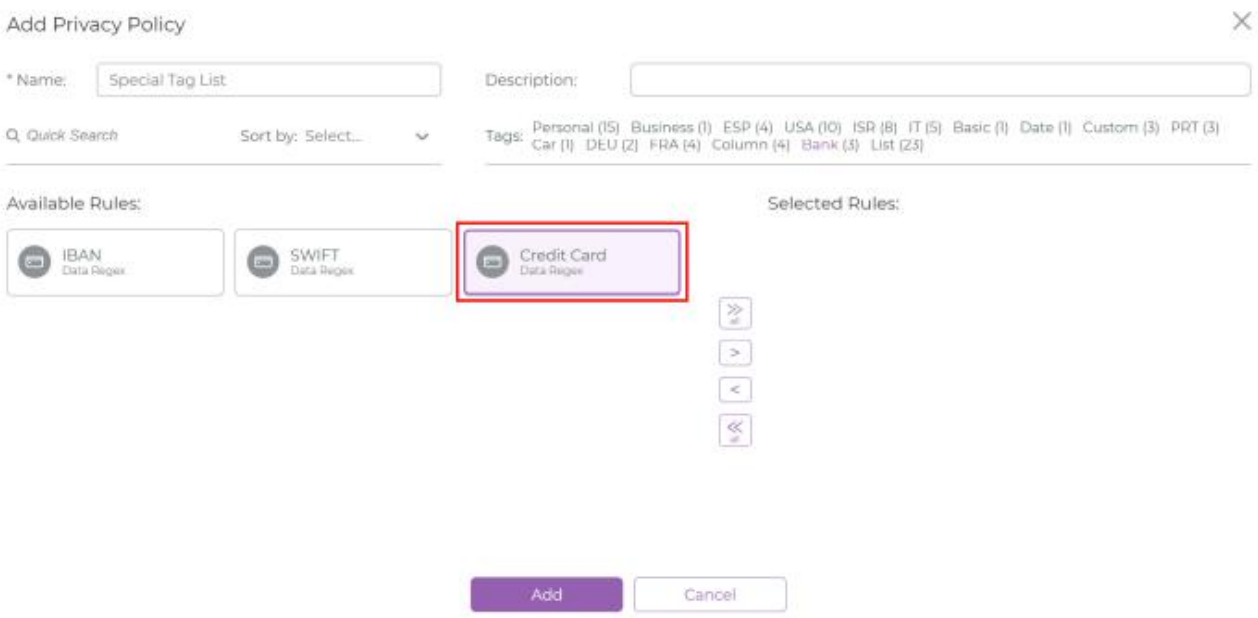
1. 特定のタグをクリックします(この例では **Bank** をクリックします)。

2. 指定のタグを含むすべてのマスキングルールが **Available Rules** リストに表示されます。



3. 追加したいルールを選択します。

4. > をクリックして、選択したルールを **Selected Rules** リストに追加します。



注意:

- 利用可能なすべてのルールを追加するには » all をクリックします。
- 既存のすべてのルールを削除するには « all をクリックします。
- 1 つのルールだけを削除するには < をクリックします。

5. **Add** をクリックします。

マスキングルールからタグを削除する手順は次のとおりです:

1. 削除したいタグを **Available Rules** リストでクリックします(この例では **Bank** をクリックします)。

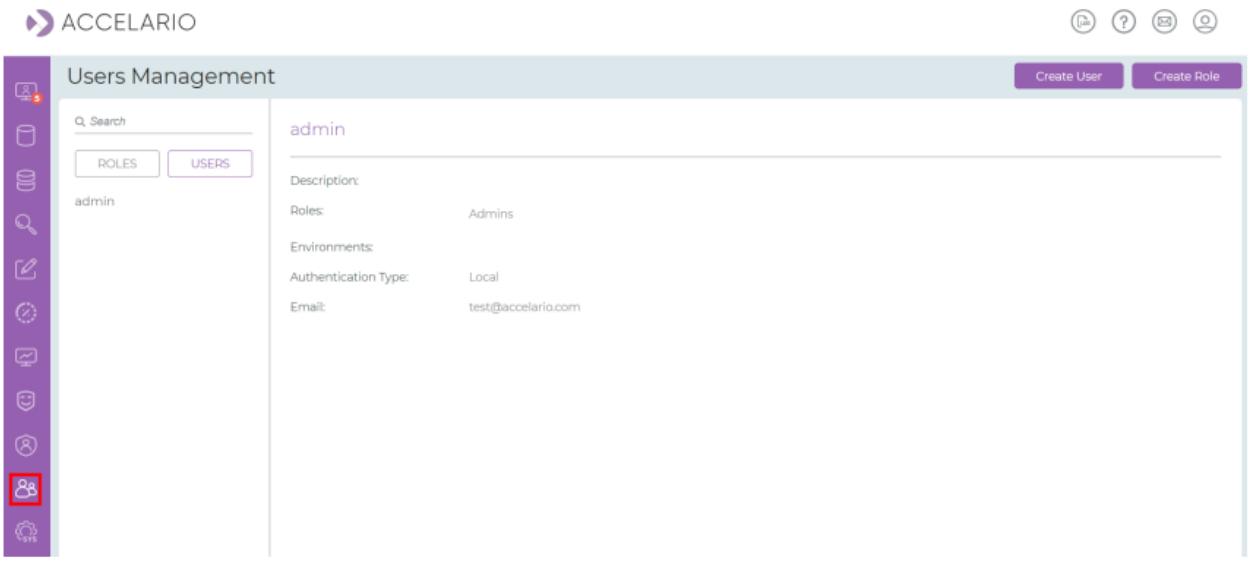
ユーザとロールの管理

このセクションでは、ユーザ管理とロール管理の手順について説明します。

注意:
- ユーザまたはロールを作成、管理できるのは、管理者(**Admin**)権限を持つユーザに限られます。
- システムを最初にインストールした際に、デフォルトの管理者ユーザが管理者(**Admin**)ロールで作成されます。

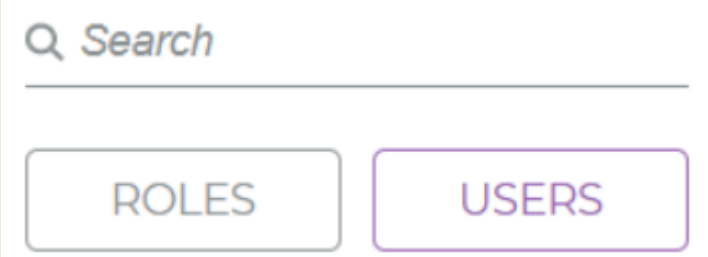
ユーザを管理する手順は次のとおりです:

1. ナビゲーションバーで(**Users Management**)をクリックします。



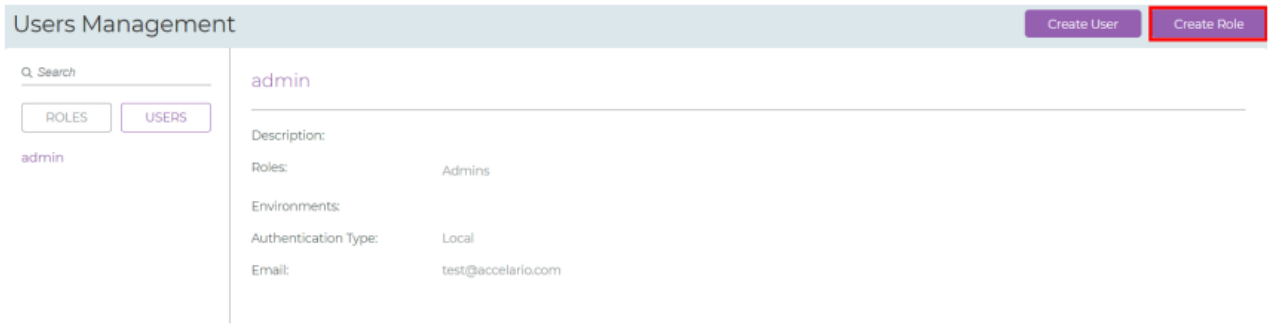
注意:
Quick Search バーに文字入力すると、必要なユーザを迅速に見つけることができます。検索によってリスト表示がすばやく更新されます。

注意:
リストはロール(**ROLES**)またはユーザ(**USERS**)基準の表示に切り替えることができます。

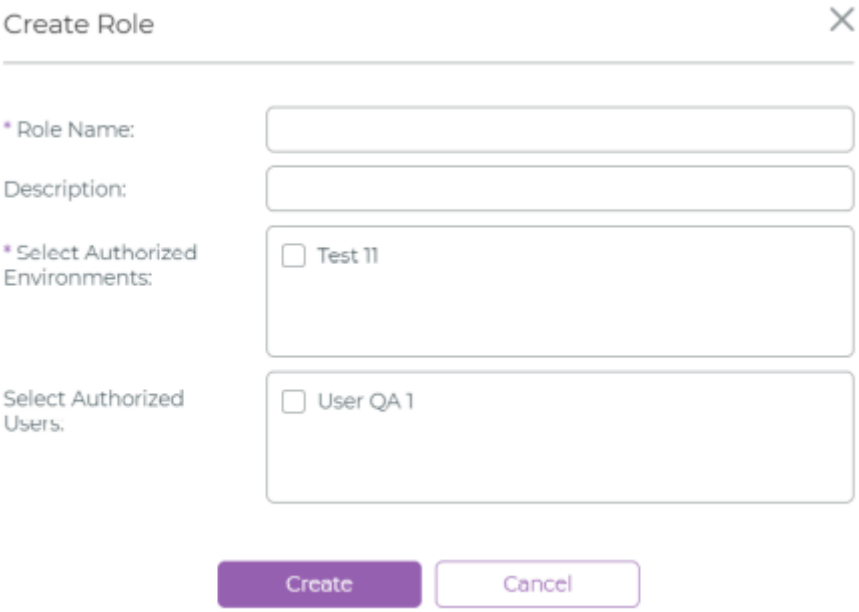


新しいロールを作成する手順は次のとおりです:

1. **Create Role** をクリックします。



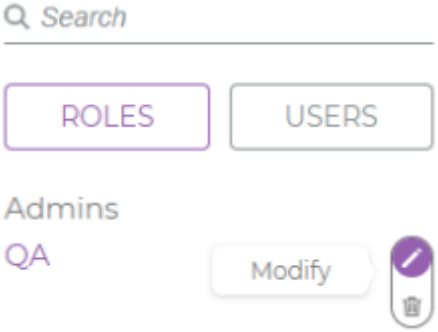
2. 詳細を記入します。



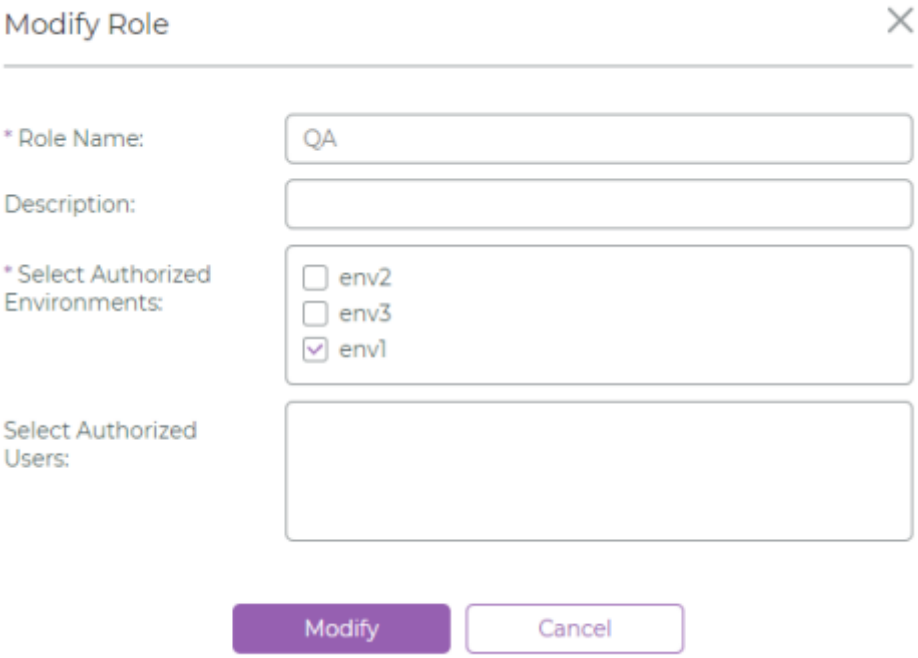
3. **Create** をクリックします。

ロールの詳細を変更する手順は次のとおりです:

1. 詳細を変更したいロールに対して (**Modify**)をクリックします。



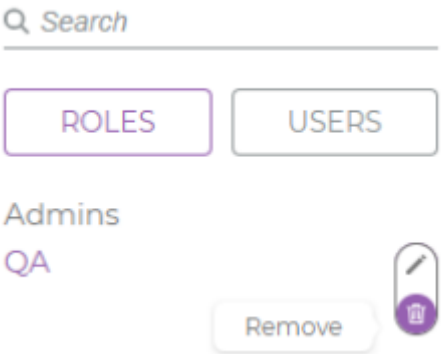
2. **Modify Role** ウィンドウが表示されたら、必要に応じて、ロールの詳細を変更します。



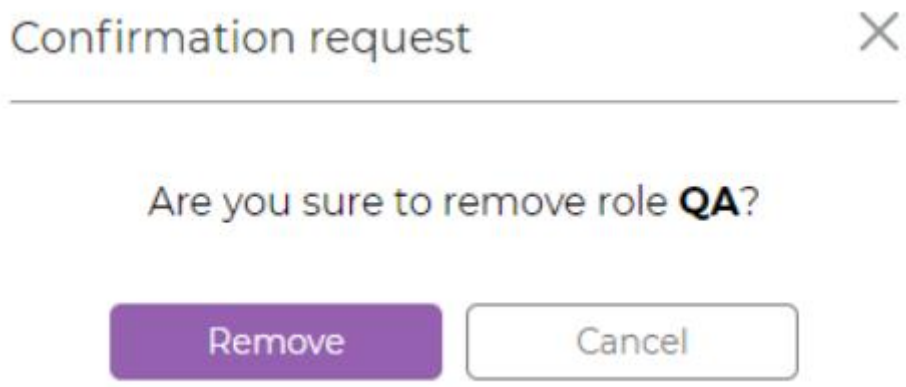
3. 変更を保存するには **Modify** を、保存せずに中止するには **Cancel** をクリックします。

ロールを削除する手順は次のとおりです:

1. 削除したいロールに対して（**Remove**）をクリックします。

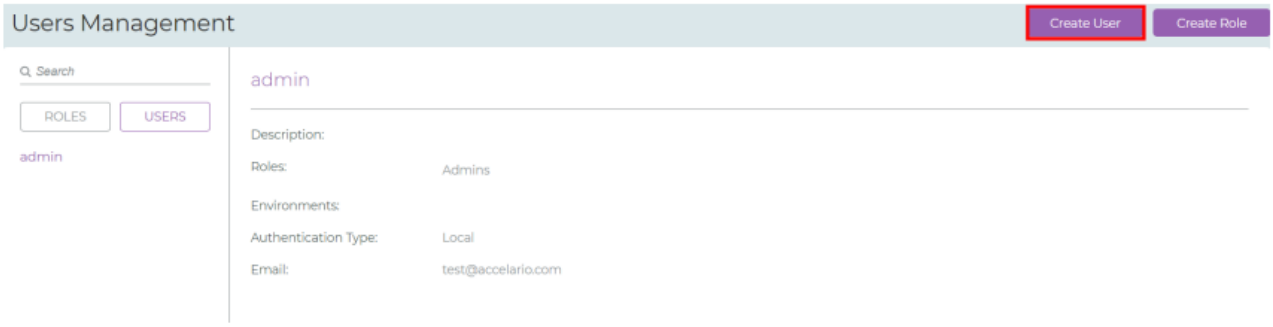


2. 削除を確定するには **Remove** を、削除せずに画面を閉じるには **Cancel** をクリックします。

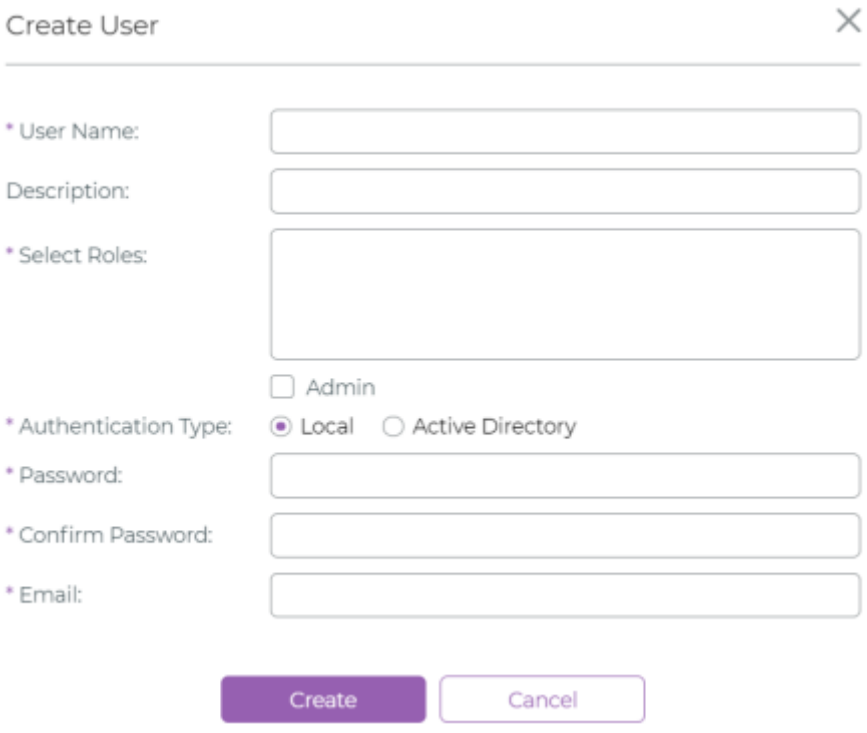


新しいユーザを追加する手順は次のとおりです:

1. **Create User** をクリックします。



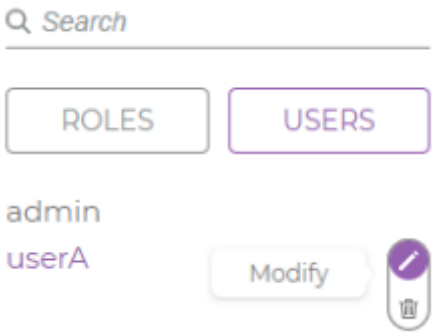
2. 詳細を記入します。



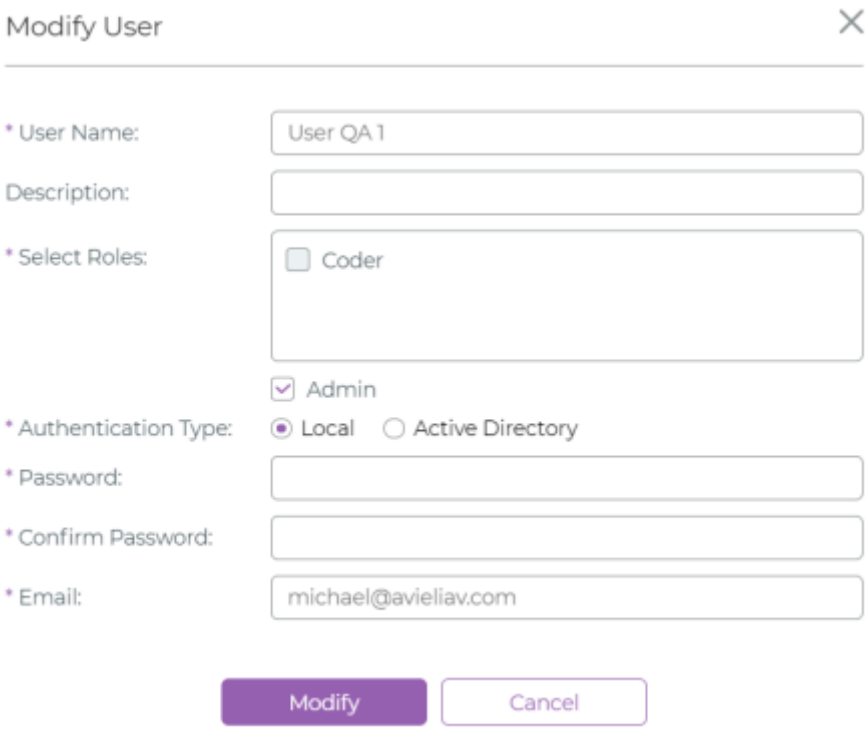
3. **Create** をクリックします。

ユーザの詳細を変更する手順は次のとおりです:

1. 詳細を変更したいロールに対して (**Modify**)をクリックします。



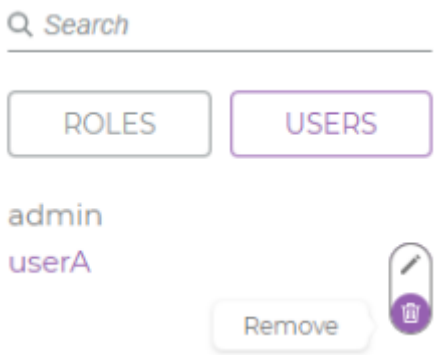
2. **Modify User** ウィンドウが表示されたら、必要に応じて、ユーザの詳細を変更します。



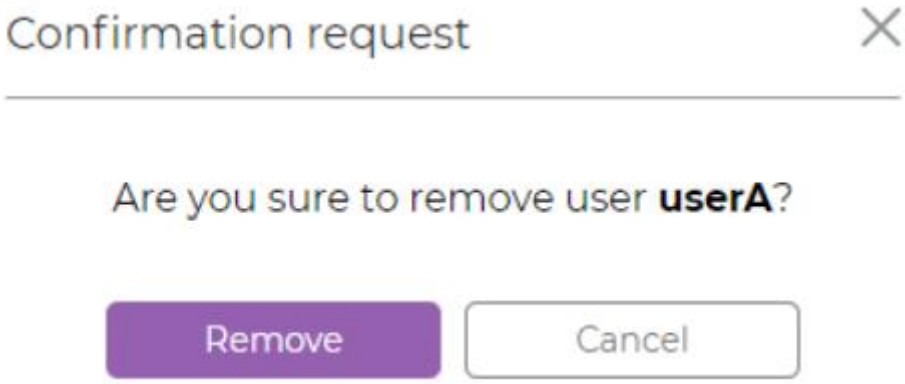
3. 変更を保存するには **Modify** を、保存せずに中止するには **Cancel** をクリックします。

ユーザを削除する手順は次のとおりです:

1. 削除したいユーザに対して(**Remove**)をクリックします。



2. 削除を確定するには **Remove** を、削除せずに画面を閉じるには **Cancel** をクリックします。



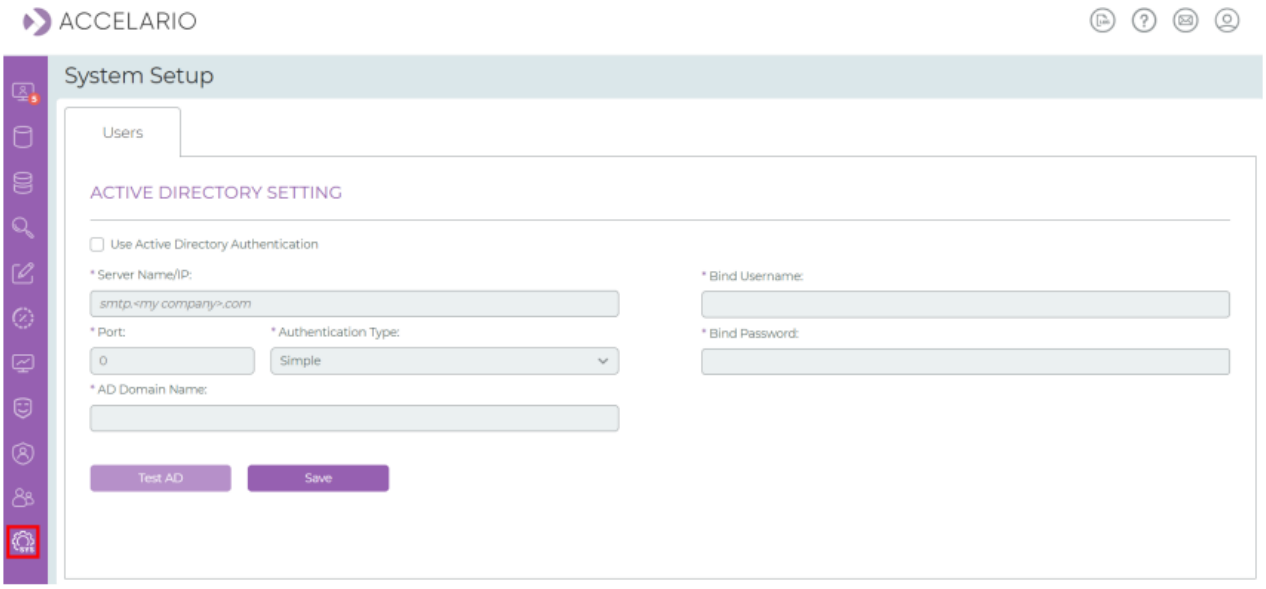
システム設定の管理

システムのさまざまな設定は **System Setup** を使用して行います。本バージョンの Accelario Data Masking モジュールでは、この設定に Active Directory を活用しています。

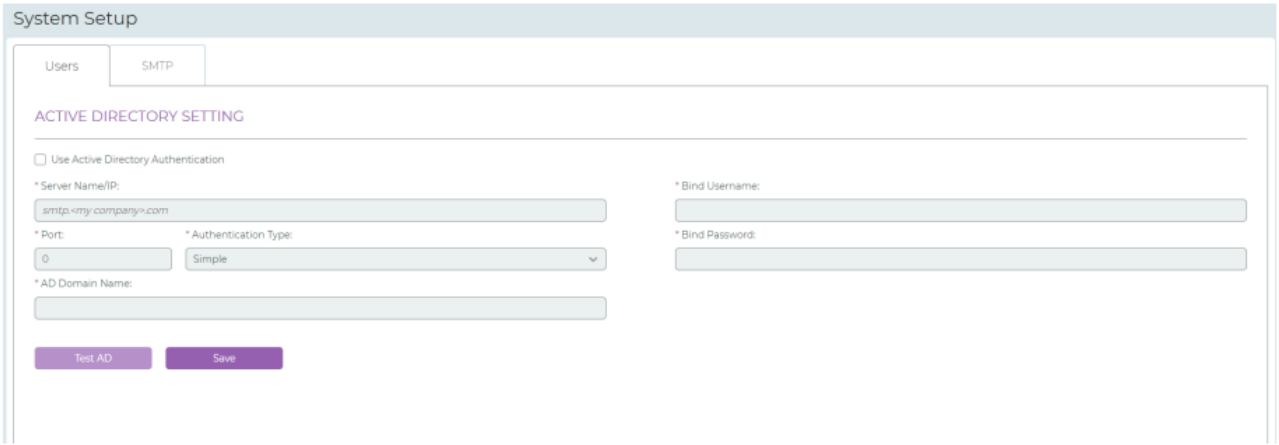
注意:
System Setup にアクセスできるのは、管理者(**Admin**)権限を持つユーザに限られます。

Active Directory をセットアップする手順は次のとおりです:

1. ナビゲーションバーで(**System Setup**)をクリックします。



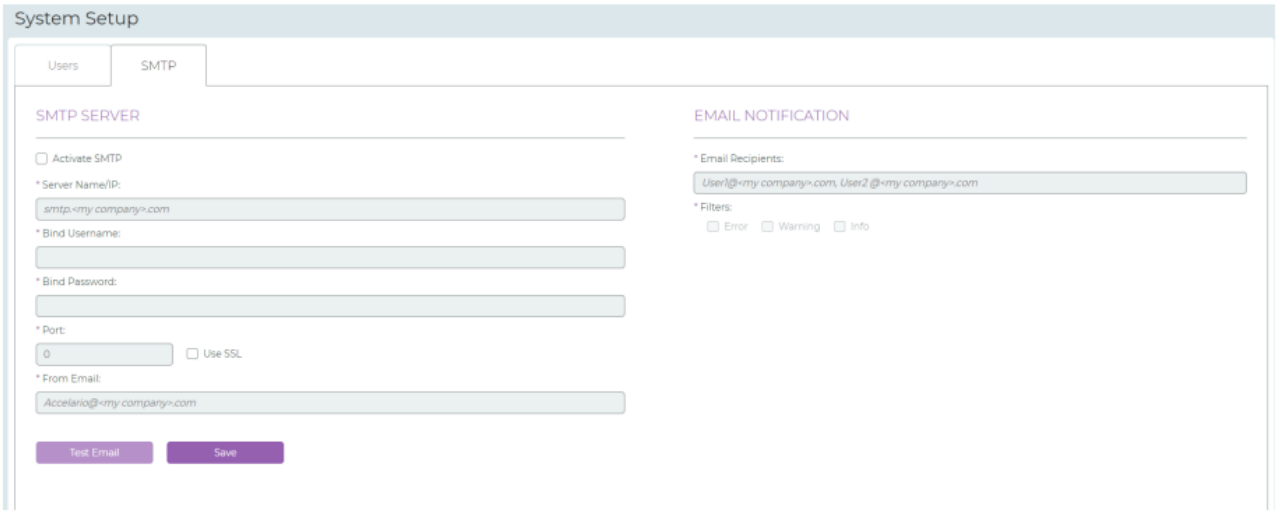
2. **Users** をクリックして、Active Directory の詳細設定を記入します。



3. **Test AD** をクリックして、Active Directory 設定の有効性を確認します。
4. **Save** をクリックします。

SMTP サーバをセットアップする手順は次の通りです:

1. **SMTP** をクリックします。
2. SMTP サーバのセットアップに必要な情報を入力します。



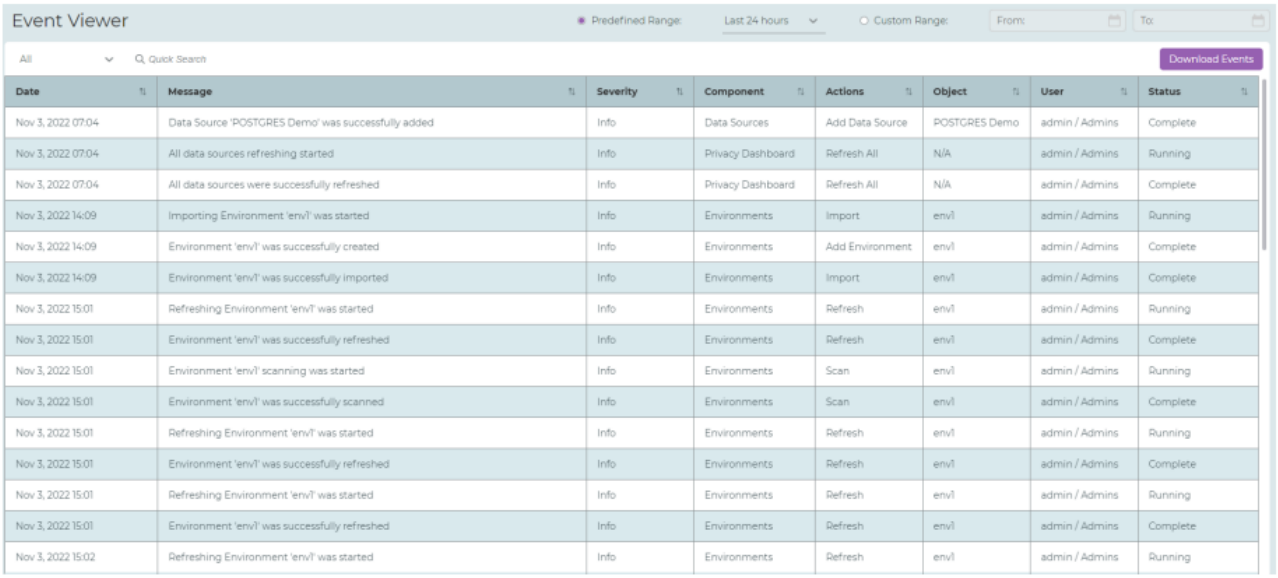
3. **Test Email** をクリックして、SMTP サーバの設定が正しいか確認します。
4. **Save** をクリックします。

イベントビューア

イベントビューアは、ユーザイベントの確認、フィルタリング、検索に使用されます。イベントビューアでは、ドリルダウンしてイベントの詳細を確認することができます。また、すべてのユーザイベントをファイルに保存することもできます。このセクションでは、これらのタスクを実行する方法について説明します。

イベントビューアを開く手順は次のとおりです:

1. ナビゲーションバーの(イベントビューア)をクリックします。



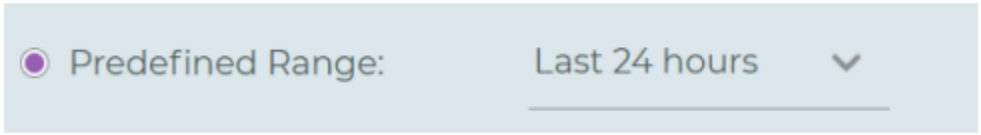
Date	Message	Severity	Component	Actions	Object	User	Status
Nov 3, 2022 07:04	Data Source 'POSTGRES Demo' was successfully added	Info	Data Sources	Add Data Source	POSTGRES Demo	admin / Admins	Complete
Nov 3, 2022 07:04	All data sources refreshing started	Info	Privacy Dashboard	Refresh All	N/A	admin /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

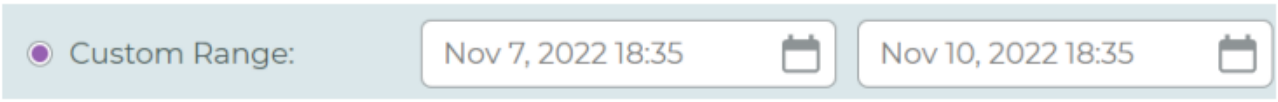
キーワードでイベントを検索する手順は次のとおりです:

1. Quick Search バーにキーワードを入力します。

特定期間のイベントをフィルタリングする手順は次のとおりです:

1. **Predefined Range**(事前に決められた範囲)または **Custom Range**(任意の範囲)を入力します。





イベントをソートする手順は次のとおりです:

1. 列の見出しのソート順序を選択します。

イベントをダウンロードする手順は次のとおりです：

1. Download Events をクリックします。

更新履歴

版	修正日	修正者	内容
1.0	2023/3/6	Y.F	初版