### 行動プロファイル

#### 概要

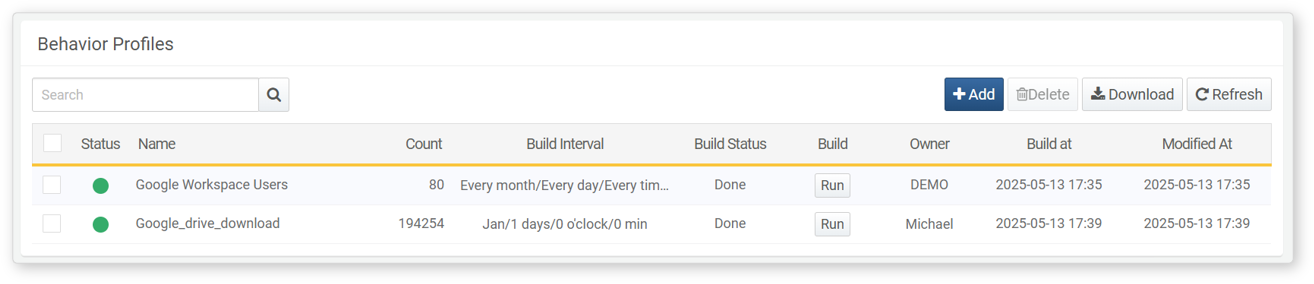
行動プロファイルとは、特定のシステムまたはアプリケーション内でのユーザー、プロセス、または通信の活動を記録・保存するデータセットです。

行動プロファイルは、ユーザーやプロセス、通信の通常パターンから逸脱した異常を特定することで、ストリームルールおよびバッチルールをサポートします。たとえば、過去1年間のVPNアクセスログをもとに行動プロファイルを生成することで、休眠アカウントからのログイン試行や、これまでに見られなかったIPアドレス帯域からのアクセスをリアルタイムで検出できます。不正検出のシナリオでは、過去に取引履歴のない口座への資金移動を検知することも可能です。

行動プロファイルは、設定されたスケジュールに従って定期的に更新（ビルド）されます。更新処理中も、ストリームルールおよびバッチルールは既存の行動プロファイルデータを参照し続け、更新完了後に新しいデータが反映されます。

#### 行動プロファイルの検索

**ポリシー > 行動プロファイル** で、行動プロファイルの一覧表示や検索が可能です。



* **ステータス**: 利用可否の状態（**緑**：利用可能、**グレー**：利用不可）
* **名前**: 行動プロファイル名
* **件数**: プロファイル内のレコード数
* **ビルド間隔**: プロファイルクエリが実行されデータが再生成される頻度
* **ビルド状態**: 行動プロファイルのビルド状態（**待機中**／**ビルド中**／**完了**）
* **ビルド**: ビルドの開始またはキャンセルを行うトグルボタン
* **所有者**: 行動プロファイルを作成したユーザー
* **ビルド日時**: 最終ビルド完了時刻
* **更新日時**: 行動プロファイルの作成日または最終更新日

特定の行動プロファイルを一覧から探す場合は、ツールバーの検索ツールを利用します。検索ツールは、**名前**および**説明**フィールドに含まれるキーワードでプロファイルをフィルタリングします。大文字・小文字は区別されません。

行動プロファイル一覧のダウンロード

行動プロファイル一覧をローカルPCにファイルとしてダウンロードするには、ツールバーの**ダウンロード**をクリックします。

行動プロファイル一覧の更新

最新情報で行動プロファイル一覧を更新するには、ツールバーの**更新**をクリックします。

プロファイルのビルド

行動プロファイルは、ビルドスケジュールに従って自動的に更新されます。プロファイルを即時更新したい場合は、行動プロファイル一覧の**ビルド**列にある**今すぐビルド**をクリックします。

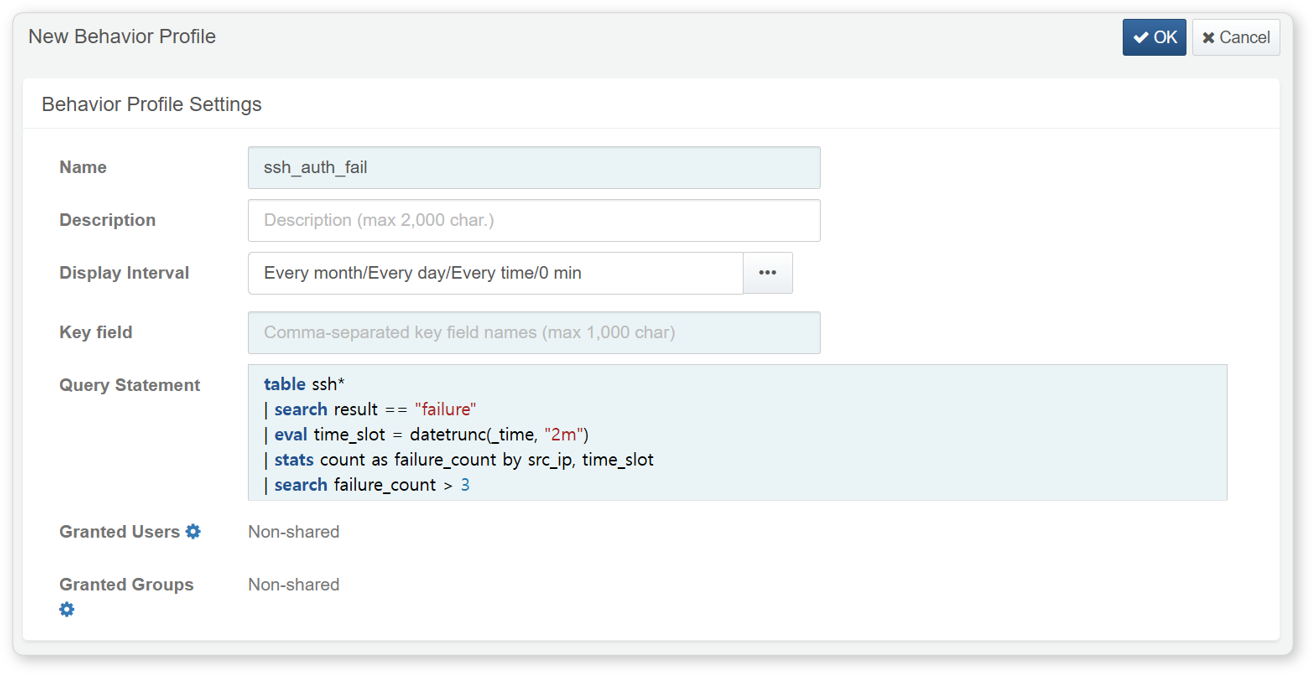
ビルド処理の所要時間はデータ量によって異なります。たとえば、過去1年間のVPNアクセスデータを記録する行動プロファイルの場合、システム負荷を最小限に抑えるため、深夜などのアイドル時間帯に更新をスケジューリングすることを推奨します。

#### 行動プロファイルの追加

行動プロファイルを追加するには、以下の手順に従います。

**ポリシー > 行動プロファイル** に移動し、ツールバーの**追加**をクリックします。

**行動プロファイル追加**画面で必要事項を入力し、**OK**をクリックします。



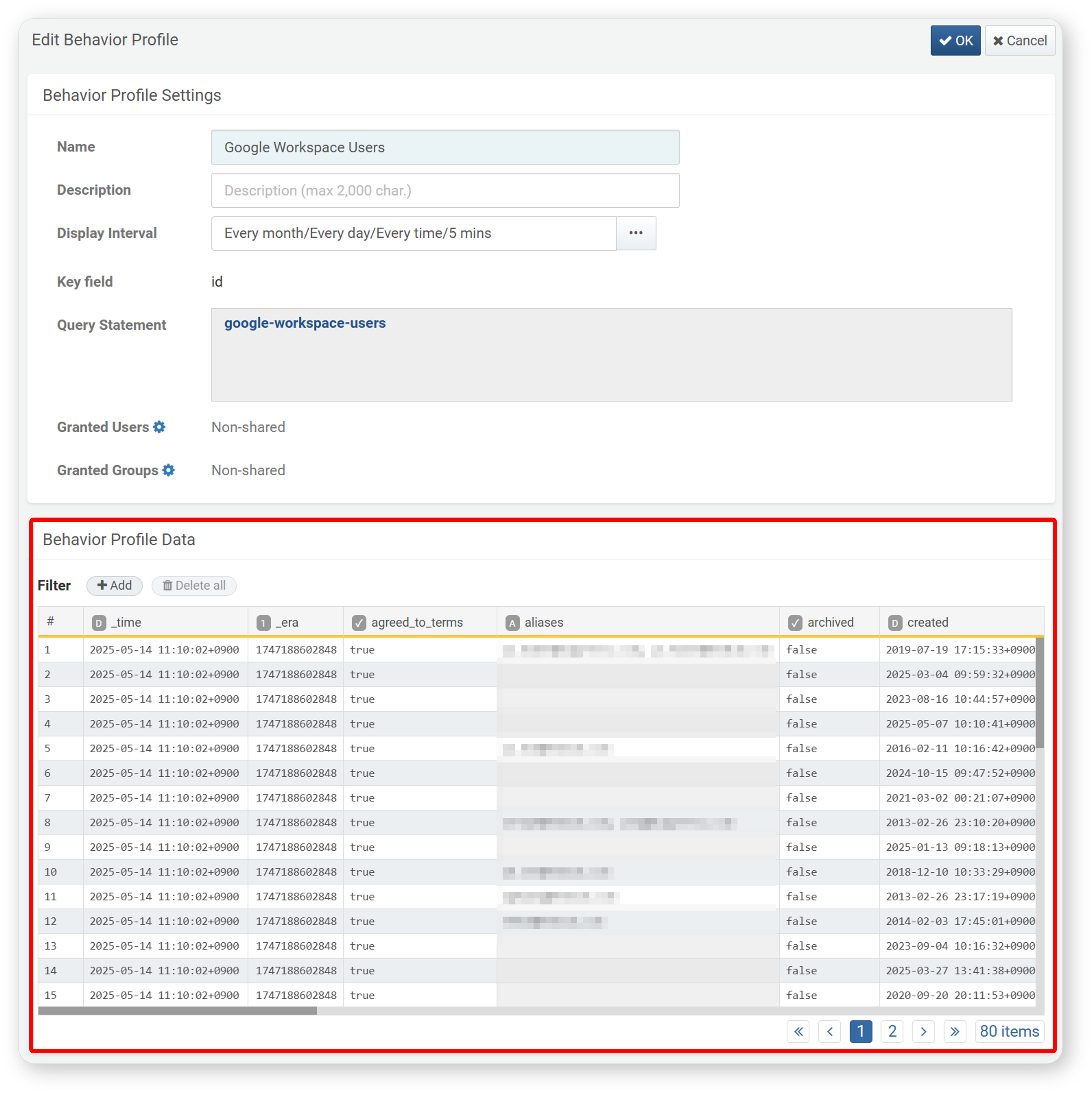
* **名前**: 行動プロファイルの一意な名称（最大50文字）
* **説明**: プロファイルの詳細説明（最大2,000文字）
* **ビルドスケジュール**: CRON形式で指定するプロファイル更新スケジュール（デフォルト：1月1日 00:00）
* **キー項目**: 行動プロファイルで比較キーとして使用するフィールド名（最大1,000文字）。複数指定する場合はカンマ（,）区切りで入力します。例：VPNログイン異常検知シナリオでは、アカウント名フィールド（例：emp\_key）をキー項目に設定します。追加後、キー項目は変更できません。
* **クエリ文**: 行動プロファイルデータを生成するためのクエリ文字列（最大2,000文字）。通常、durationまたはfrom・toオプションを組み合わせて最新データを取り込むようにします。クエリ結果には必ずキー項目が含まれ、その値はプロファイル内で一意でなければなりません。例：VPNアクセス異常検知ルールでは、キー項目emp\_keyに重複レコードが存在しないようにします。追加後、クエリ文は変更できません。
* **許可ユーザー**: 行動プロファイルの閲覧・編集権限を持つユーザーアカウントの一覧
* **許可グループ**: 行動プロファイルの閲覧・編集権限を持つユーザーグループの一覧

クラスター管理者および管理者のみが、行動プロファイルのビルドやクエリ文の修正を行うことができます。グループ共有による権限付与があっても、アカウント単位で適用されます。

**OK**をクリックして設定を完了します。

#### 行動プロファイルデータの閲覧

一覧から行動プロファイル名をクリックすると、その設定内容および該当データを確認できます。



表示データを絞り込むためにフィルターを適用できます。フィルターを追加するには、**フィルター**の横にある**追加**をクリックします。

#### 行動プロファイルの編集

行動プロファイルを編集するには、以下の手順に従います。

一覧から行動プロファイル名をクリックします。

**行動プロファイル編集**画面で情報を更新し、**OK**をクリックします。

* 編集可能な項目の詳細は「**行動プロファイルの追加**」セクションを参照してください。
* **キー項目**および**クエリ文**は変更できません。これらを変更する場合は、行動プロファイルを削除し再作成してください。

#### 行動プロファイルの活用

シナリオビルダー

**ポリシー > ストリームルール**でストリームルールを追加または編集する際、シナリオビルダーで行動プロファイルを活用できます。入力フィールドの型および名称が、行動プロファイルの**キー項目**の型・名称と一致している必要があります。

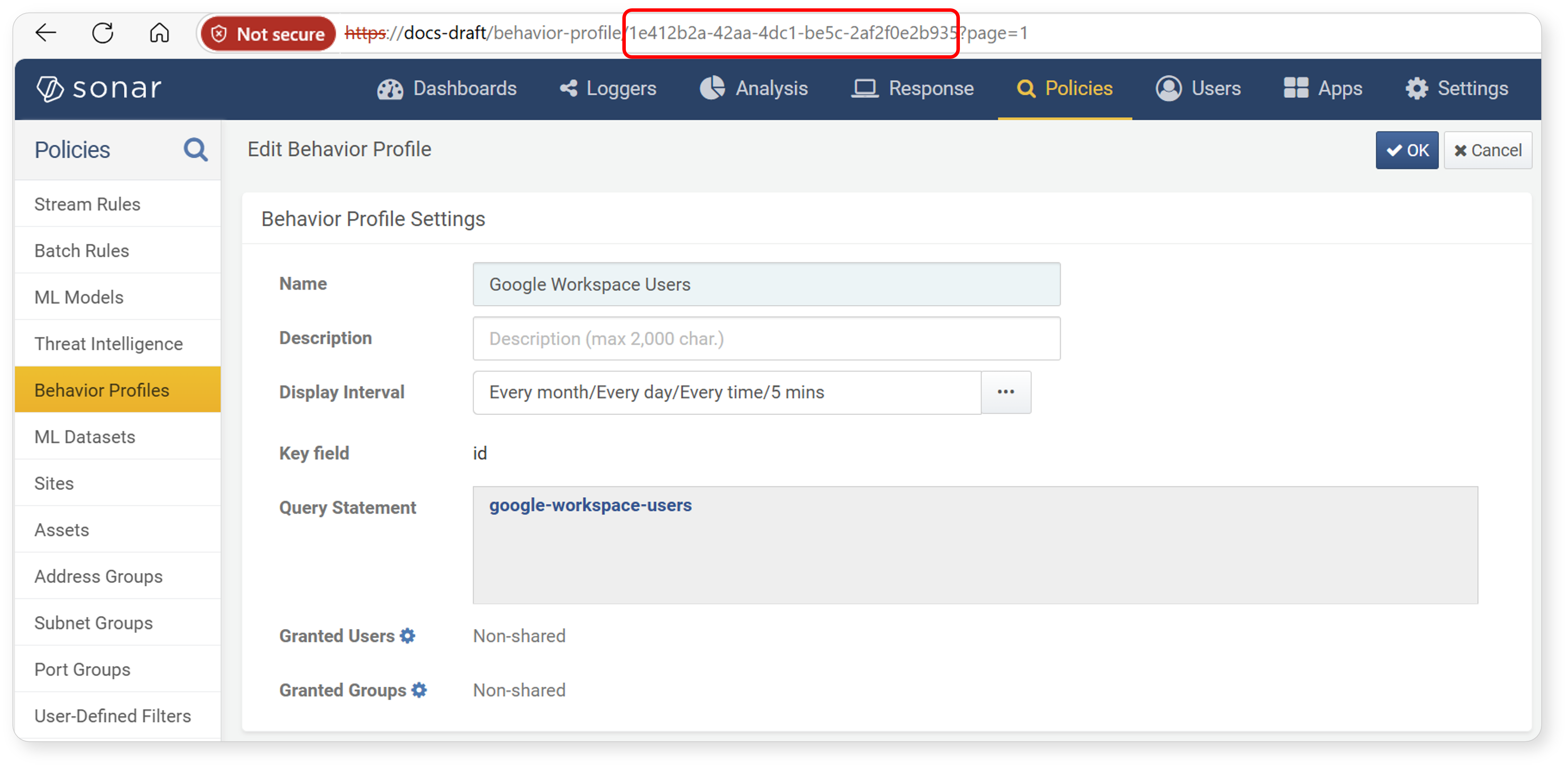
以下の表は、シナリオビルダーで利用可能な行動プロファイル関連関数を示します。詳細は[フィールドタイプ別ルールとパラメータ](https://docs.logpresso.comnull)を参照してください。

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| その他 | 行動プロファイル | 行動プロファイルを選択 | 行動プロファイルのキー項目と一致する値をフィルタリング |

クエリ

**ポリシー > ストリームルール**または**ポリシー > バッチルール**で検出ルールを追加・編集する際、[matchbehavior](https://docs.logpresso.comnull)コマンドや[matchbehavior()](https://docs.logpresso.comnull)関数を利用して行動プロファイルを適用できます。行動プロファイルは、クエリ入力を受け付ける任意の関数でも利用可能です。

[matchbehavior](https://docs.logpresso.comnull)コマンドまたは[matchbehavior()](https://docs.logpresso.comnull)関数を利用するには、行動プロファイルのGUIDが必要です。GUIDはブラウザのアドレスバーで確認できます。



#### 行動プロファイルの削除

行動プロファイルを削除するには、以下の手順に従います。

一覧で削除したい行動プロファイルのチェックボックスを選択します。

ツールバーの**削除**をクリックします。

**行動プロファイル削除**ダイアログで選択内容を確認し、**削除**をクリックします。キャンセルする場合は**キャンセル**をクリックします。

ストリームルールやバッチルールで参照されている行動プロファイルを削除すると、検出ルールが正しく動作しなくなる場合があります。