### Behavior Profile

#### Overview

A behavior profile is a dataset that records and stores the behavior or communication history of users/processes occurring in a specific system or application.

Behavior profiles serve as a support feature for real-time and batch detection scenarios, used to detect anomalies that deviate from typical behavior patterns of users, processes, or communications at an early stage. For example, by generating a behavior profile based on VPN access logs from the past year, it is possible to detect login attempts from dormant accounts or access from previously unconnected IP address ranges in real-time. Additionally, when applied to anomaly transaction detection scenarios, it can detect attempts to transfer funds to accounts with no transaction history in real-time.

Behavior profiles periodically update (build) profile data according to a set schedule. During the update of profile data, the behavior profiles referenced by real-time and batch detection scenarios continue to apply based on existing data until the update is complete.

#### Viewing/Search Behavior Profile List

You can view or search the list of behavior profile models in **Policy > Behavior Profile**.



* **Status**: Availability (**Green**: Available, **Gray**: Unavailable)
* **Name**: Name of the behavior profile
* **Count**: Number of data entries included in the current profile
* **Build Cycle**: The frequency at which the profile query is re-executed to generate profile data.
* **Build Status**: Build status of the behavior profile (**Pending**/**Building**/**Build Complete**)
* **Build**: Toggle button to execute or cancel the build
* **Owner**: User account that added the behavior profile
* **Last Build**: Timestamp of the last completed build
* **Modification Date**: Date the behavior profile was created or last modified

To find a specific behavior profile in the list, use the search tool in the toolbar. The search tool will find and display behavior profiles that include the entered term in the **Name** or **Description**. The search tool is case-insensitive.

Downloading the List

To download the behavior profile list as a file to your local PC, click **Download** in the toolbar.

Refreshing the List

To refresh the behavior profile list with the latest information, click **Refresh** in the toolbar.

Building the Profile

Behavior profiles are automatically updated when the build cycle occurs. To immediately refresh a behavior profile, click **Build Now** in the **Build** column of the profile you wish to update.

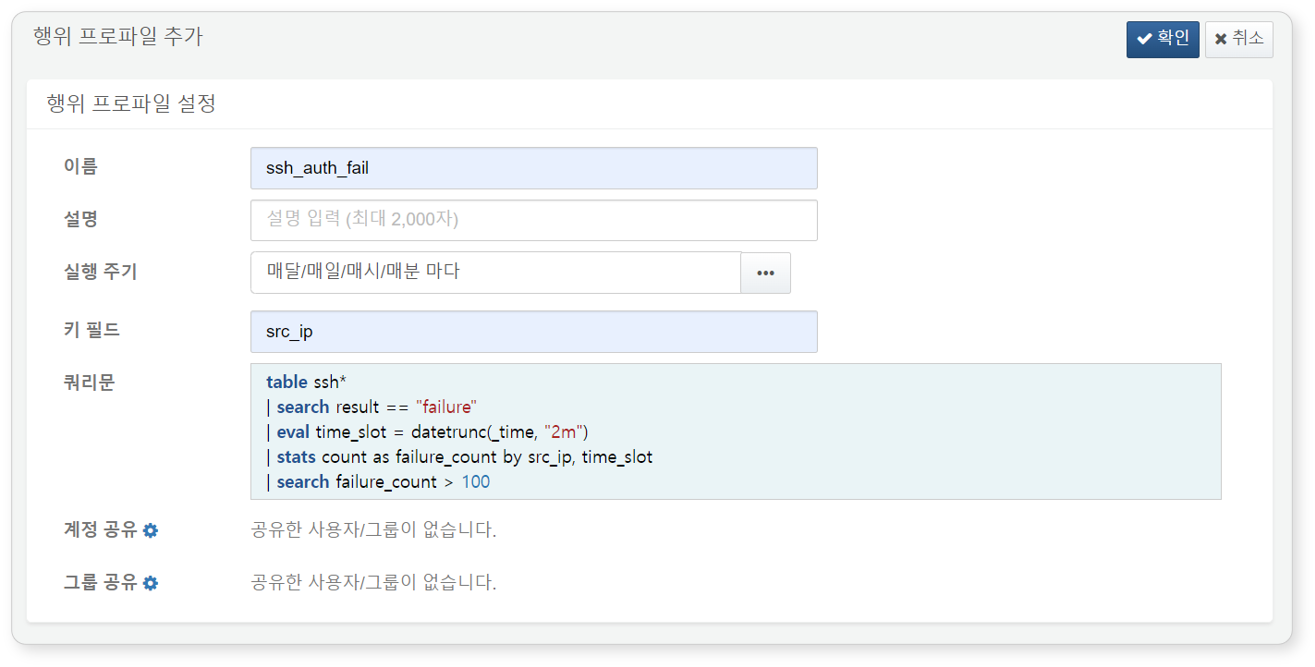
The update of behavior profiles may take a long time depending on the size of the data being processed. For example, if the behavior profile records VPN login information for the past year, it is advisable to schedule the automatic update during off-peak hours, such as early morning.

#### Adding a Behavior Profile

To add a behavior profile:

Click **Add** in the toolbar under **Policy > Behavior Profile**.

In the **Add Behavior Profile** screen, enter or select the required values and then click **OK**.



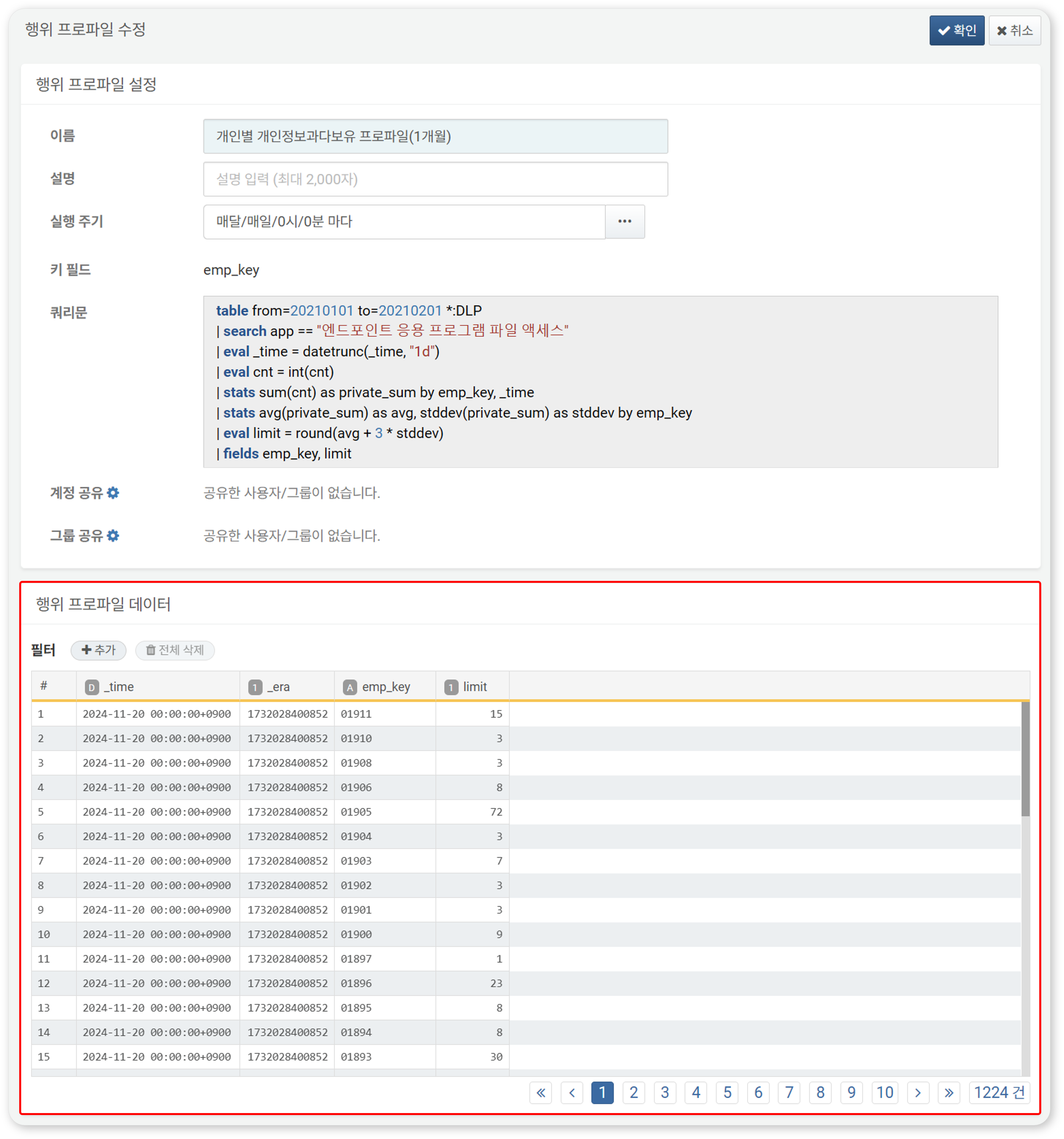
* **Name**: Unique name for the behavior profile (up to 50 characters)
* **Description**: Detailed description of the profile (up to 2,000 characters)
* **Execution Cycle**: Schedule for behavior profile updates specified in CRON syntax (default: January 1st, 00:00)
* **Key Field**: Field name used as a key when comparing behavior profiles. To specify more than one, separate them with commas (,). For example, if the behavior profile is used to detect login attempts from dormant or new accounts during VPN logins, specify the account name field (e.g., emp\_key) as the key field (up to 1,000 characters). The key field cannot be changed after the behavior profile is added.
* **Query String**: Query string used to generate behavior profile data (up to 2,000 characters). The query string for behavior profiles is typically written to reflect recent data using options like duration or combinations of from and to. The query result must include the key field, and the value of the key field must be unique within the behavior profile. For example, in a scenario for detecting anomalies in VPN access, there cannot be multiple records with the same account in the key field emp\_key. The query string cannot be changed after the behavior profile is added.
* **Account Sharing**: List of accounts that will share view and edit permissions for the behavior profile
* **Group Sharing**: List of account groups that will share view and edit permissions for the behavior profile

Only cluster administrators and admin accounts can perform builds and modify query strings for behavior profiles. Even if permissions are granted through group sharing, they are applied at the account level.

After completing the settings in the **Add Behavior Profile** screen, click **OK**.

#### Viewing Behavior Profile Data

Clicking the name of a behavior profile in the built behavior profile list allows you to view the behavior profile data below the behavior profile settings information.



You can apply filters to view only the desired data. To add filtering conditions, click **Add** next to **Filter**.

#### Modifying a Behavior Profile

To modify a behavior profile:

Click the name of the behavior profile you wish to modify in the behavior profile list.

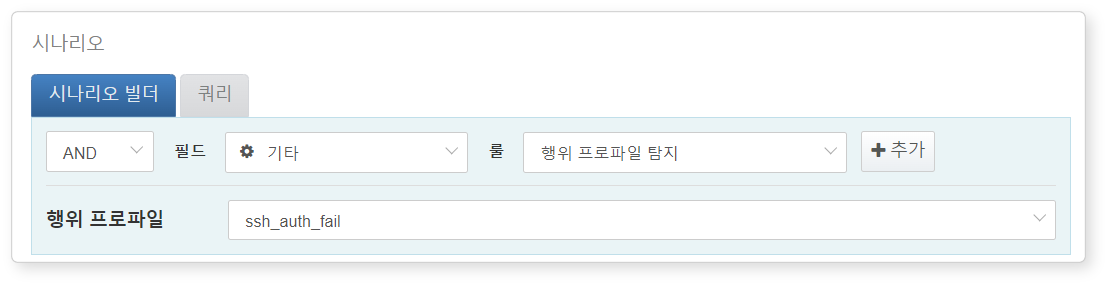
In the **Modify Behavior Profile** screen, edit the information and click **OK**.

* Refer to the behavior profile addition section for descriptions of the properties to be modified.
* The **Key Field** and **Query String** cannot be modified. To change these items, you must delete the behavior profile and recreate it.

#### Utilizing Behavior Profiles

Scenario Builder

In **Policy > Real-Time Detection**, you can utilize behavior profiles when adding or modifying detection scenarios using the scenario builder. At this time, the **input fields** must include fields that **match the key fields, field types, and field names of the behavior profile**.



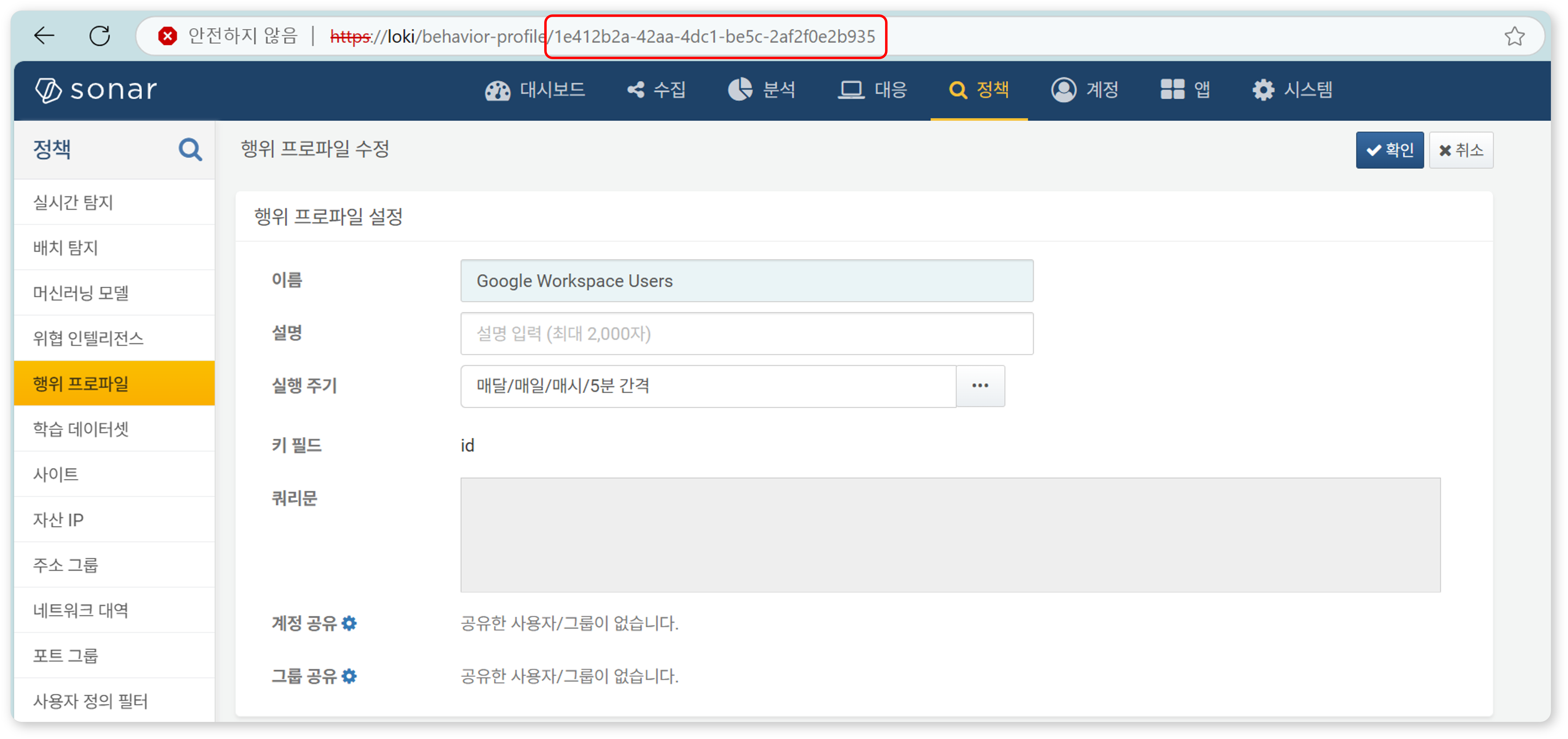
The following summarizes the behavior profile-related content that can be used in the scenario builder. For more details, refer to [Rules and Parameters by Field Type](https://docs.logpresso.comnull).

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| Other | Behavior Profile Detection | Select Behavior Profile | Filters based on field values that match the key fields of the behavior profile |

Query

In **Policy > Real-Time Detection** or **Policy > Batch Detection**, you can utilize behavior profiles with the [matchbehavior](https://docs.logpresso.comnull) command or the [matchbehavior()](https://docs.logpresso.comnull) function when adding or modifying detection scenarios. Remember that you can use behavior profiles anywhere a query string can be entered.

To use the matchbehavior command or matchbehavior() function, you need to know the GUID of the behavior profile. The GUID can be found in the address bar of your web browser.



#### Deleting a Behavior Profile

To delete a behavior profile:

Select the checkbox for the behavior profile row you wish to delete in the behavior profile list.

Click **Delete** in the toolbar.

In the **Delete Behavior Profile** dialog, review the list of behavior profiles to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

Be cautious when deleting behavior profiles referenced in real-time or batch detection, as it may cause detection scenarios to not function as intended.