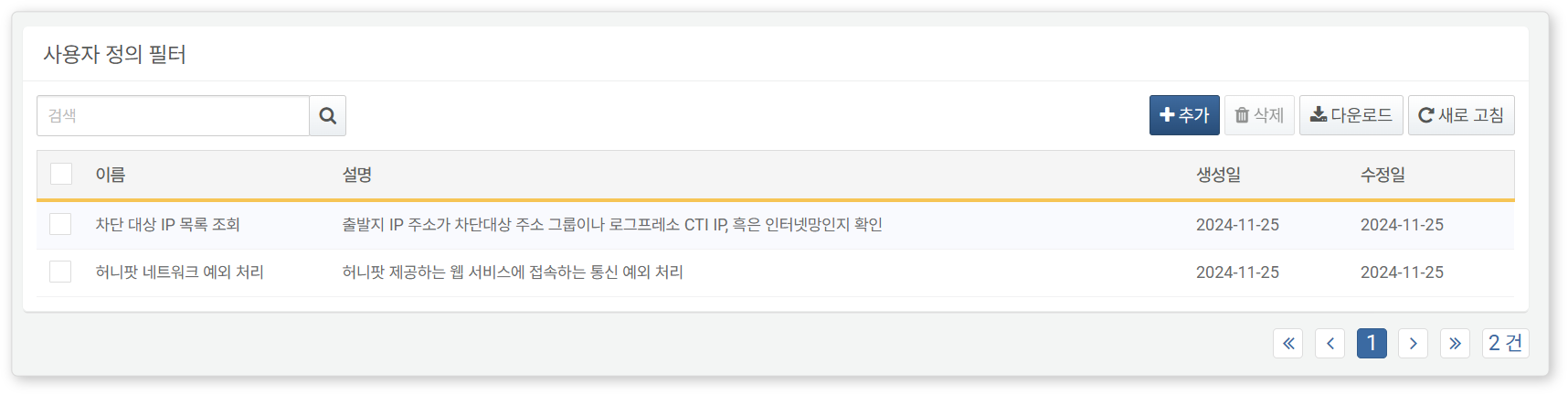
### User-Defined Filters

#### Overview

User-Defined Filters allow for the application of specific filtering conditions to detection scenario policies, enabling data analysis and detection. These filters modularize complex conditions that are used repeatedly, making it easy to apply the same conditions across multiple detection scenarios. This facilitates efficient execution of necessary filters in both real-time and batch detection scenarios. By using User-Defined Filters, accurate data filtering and analysis based on specific conditions can be achieved.

#### Viewing/Search User-Defined Filter List

You can view or search the list of User-Defined Filters under **Policies > User-Defined Filters**.



* **Name**: The unique name of the User-Defined Filter
* **Description**: A description of the User-Defined Filter
* **Creation Date**: The date the User-Defined Filter was created
* **Modification Date**: The date the User-Defined Filter was last modified

To find a specific User-Defined Filter in the list, use the search tool in the toolbar. The search tool will display User-Defined Filters that contain the entered words in the **Name** or **Description** fields. The search tool is case-insensitive.

Downloading the List

To download the User-Defined Filter list as a file to your local PC, click **Download** in the toolbar.

Refreshing the List

To refresh the User-Defined Filter list with the latest information, click **Refresh** in the toolbar.

#### Adding a User-Defined Filter

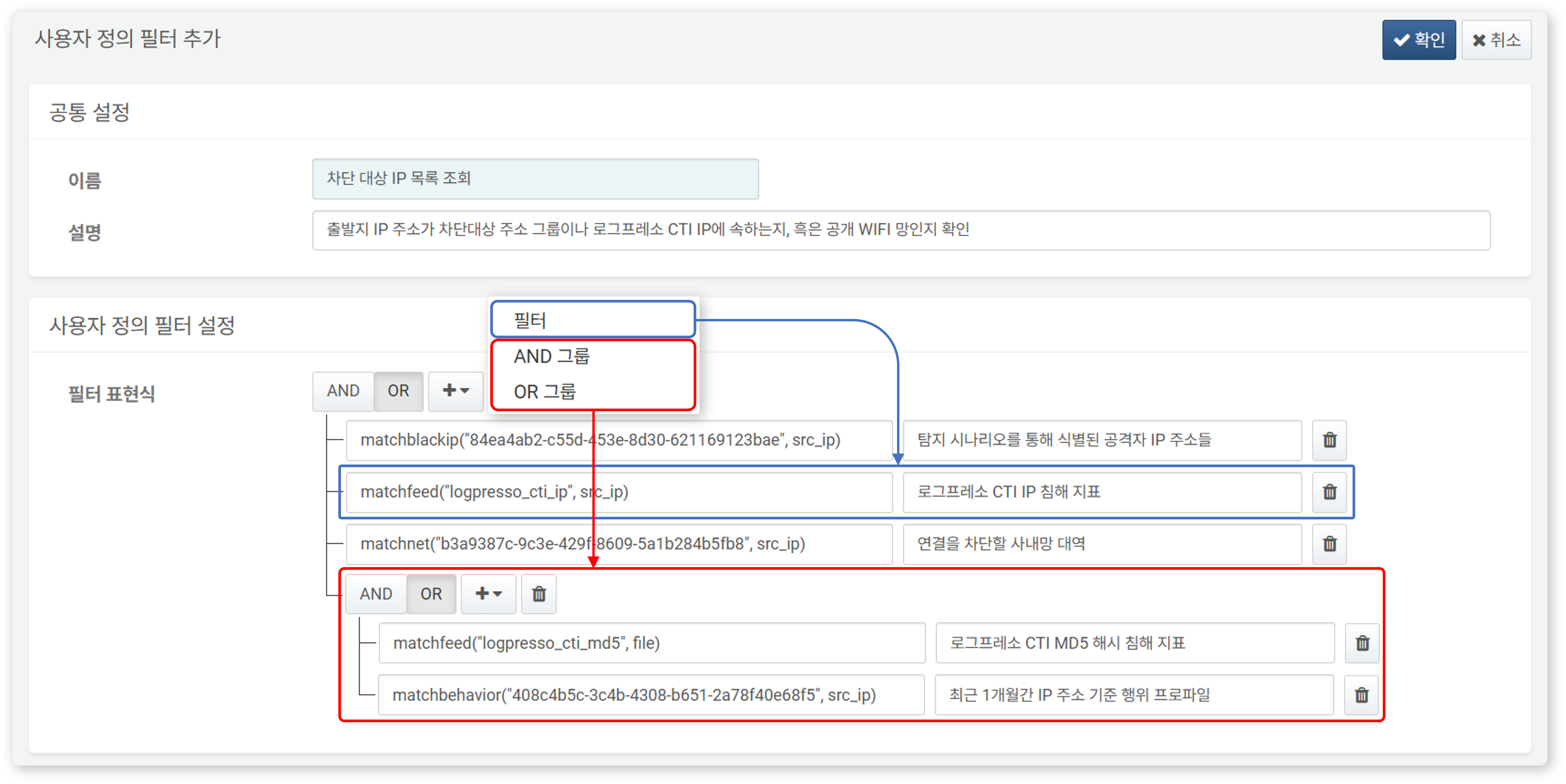
To add a User-Defined Filter:

Click **Add** in the toolbar under **Policies > User-Defined Filters**.

In the **Add User-Defined Filter** screen, enter the **Common Settings** properties.

* **Name**: The unique name of the User-Defined Filter (up to 50 characters). The name cannot be modified after the filter is added.
* **Description**: A description of the User-Defined Filter (up to 2,000 characters).

In the **User-Defined Filter Settings**, enter the **Filter Expression**, then click **OK**.



* Initially, only one **Filter Expression** input field is provided. Enter a boolean expression and description written in Logpresso query here (both the filter expression and description can be up to 1,000 characters).
* Click "**+**" to add a single filter expression or a group of sub-filter expressions. Groups can be added up to 3 levels deep.
* If logical conjunction (AND, returns true only if all conditions are true) or logical disjunction (OR, returns true if at least one of the conditions is true) is needed in the filter expression, click **AND** or **OR**.
* To delete a filter expression or a group of filter expressions, click the trash can icon on the right.

#### Modifying a User-Defined Filter

To modify a User-Defined Filter:

Click the name of the User-Defined Filter you wish to modify in the [User-Defined Filter List](https://docs.logpresso.comnull).

In the **Modify User-Defined Filter** screen, make the necessary changes and click **Save**.

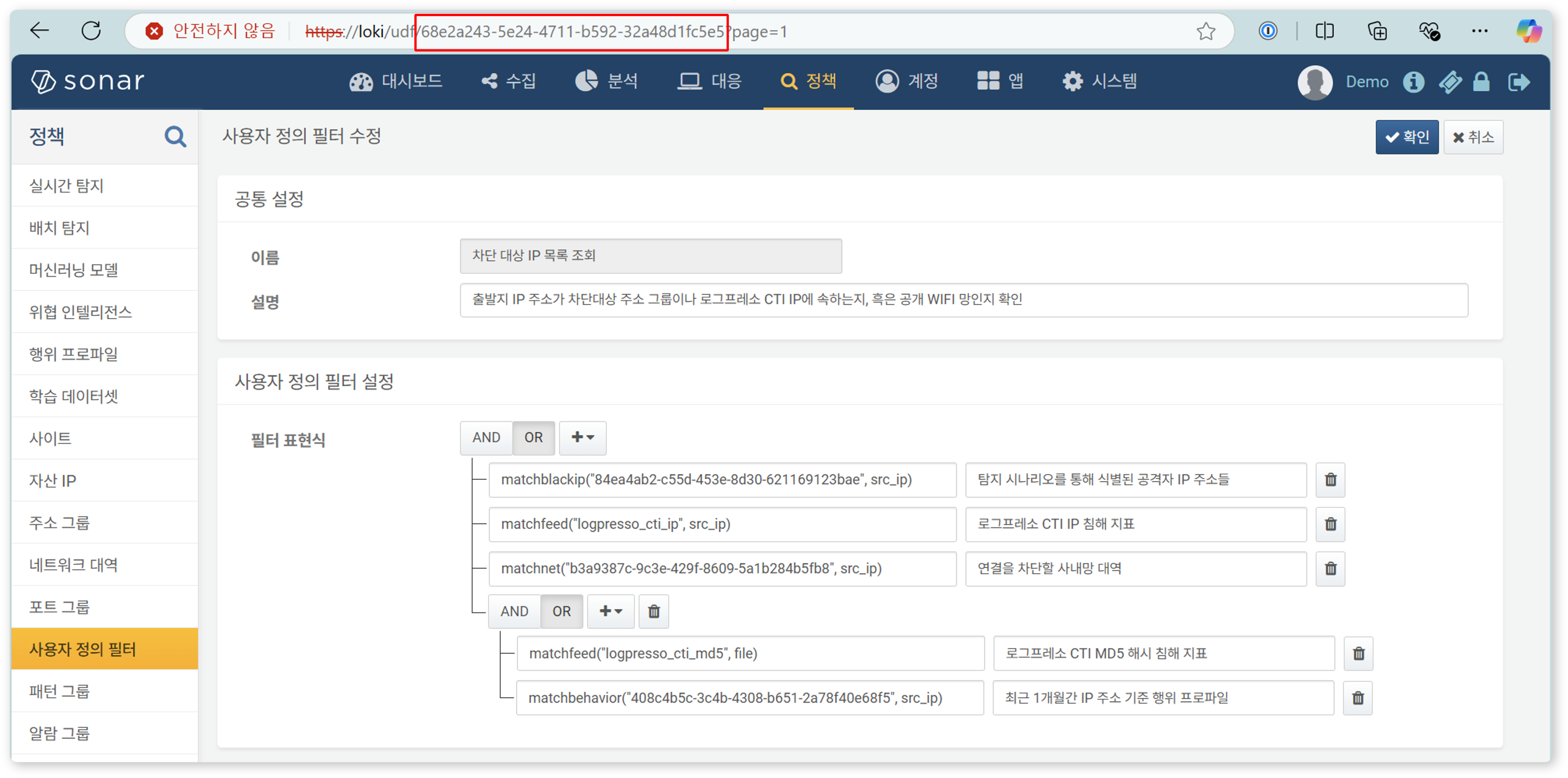
#### Utilizing User-Defined Filters

User-Defined Filters can be set and used in the following ways:

Query

User-Defined Filters can be utilized by calling the [matchfilter()](https://docs.logpresso.comnull) function when writing query statements. For example, if you want to filter a specific IP address using a User-Defined Filter, write the query in the format search matchfilter("User-Defined Filter GUID").

To use the matchfilter() function, you need to know the GUID of the User-Defined Filter. The GUID can be found in the address bar of your web browser.



#### Deleting a User-Defined Filter

To delete a User-Defined Filter:

Select the checkbox for the row of the User-Defined Filter you wish to delete in the User-Defined Filter list.

Click **Delete** in the toolbar.

In the **Delete User-Defined Filter** dialog, review the list of User-Defined Filters to be deleted, then click **Delete**. Click **Cancel** if you do not wish to delete.

Be cautious when deleting User-Defined Filters referenced in real-time or batch detection scenarios, as this may cause the detection scenarios to not function as intended.