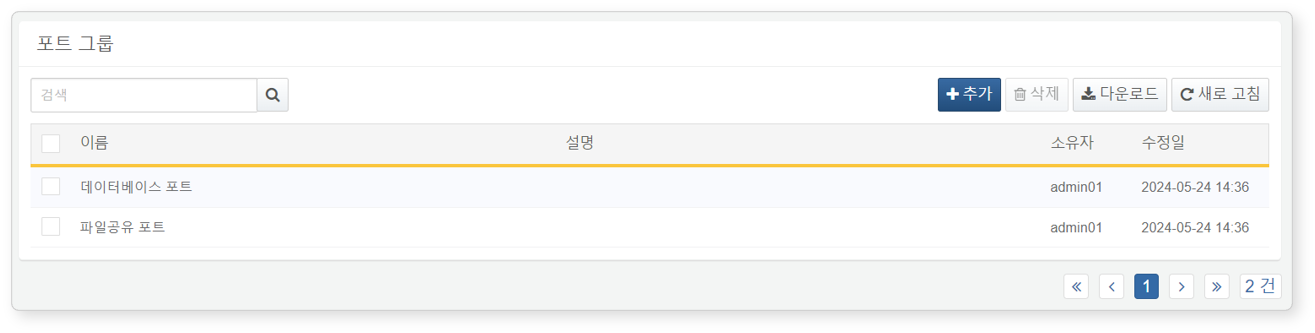
### Port Groups

#### Overview

Port Groups support the grouping of port numbers used in TCP and UDP communications by topic, allowing for their incorporation into detection policies. They are utilized when analyzing access detection and anomalous behavior related to specific ports.

#### Viewing/Search Port Group List

You can view or search the list of Port Groups under **Policies > Port Groups**.



* **Name**: The unique name of the Port Group
* **Description**: Information about the Port Group
* **Owner**: The user account that added the Port Group
* **Modification Date**: The date the Port Group was created or last modified

To find a specific Port Group in the list, use the search tool in the toolbar. The search tool will display Port Groups that contain the entered term in the **Name** or **Description** fields. The search tool is case-insensitive.

Downloading the List

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

Refreshing the List

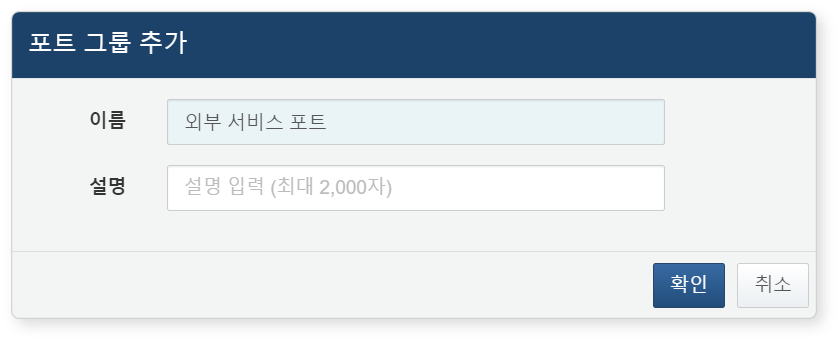
To refresh the Port Group list with the latest information, click **Refresh** in the toolbar.

#### Adding a Port Group

To add a Port Group:

Click **Add** in the toolbar under **Policies > Port Groups**.

In the **Add Port Group** dialog, enter the required values and click **OK**.



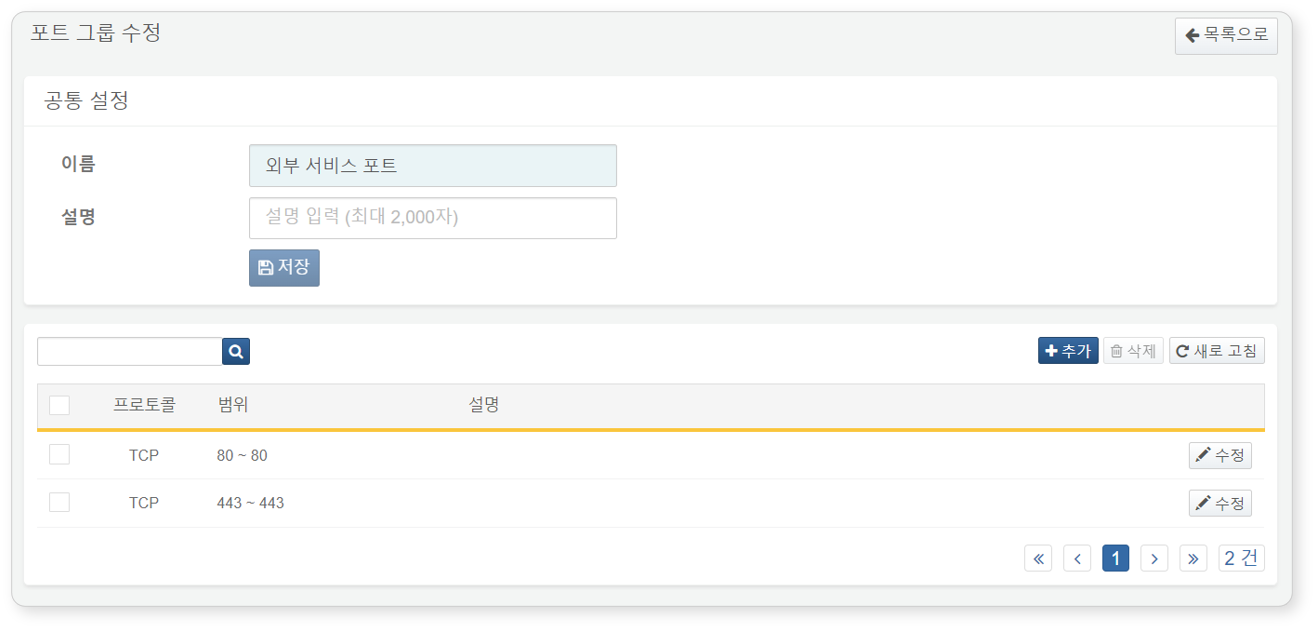
* **Name**: The name of the Port Group (up to 50 characters)
* **Description**: A detailed description of the Port Group (up to 2,000 characters)

#### Modifying a Port Group

To modify a Port Group:

Click the name of the Port Group you wish to modify in the [Port Group List](https://docs.logpresso.comnull).

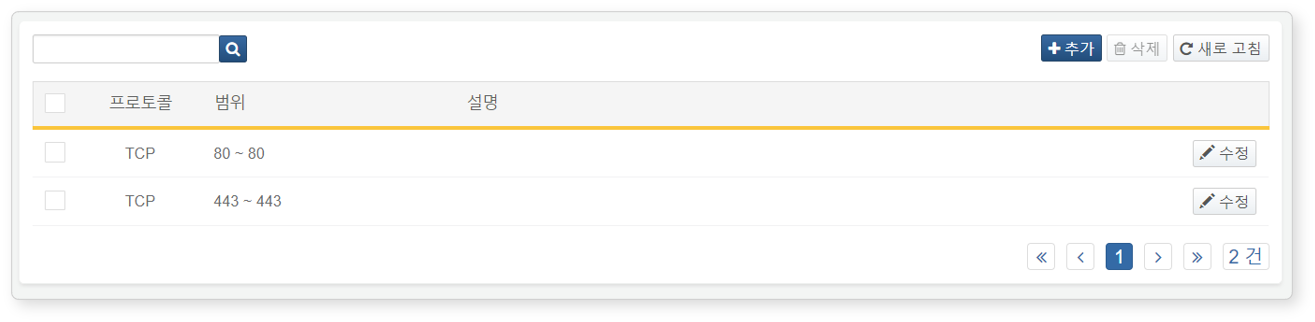
In the **Modify Port Group** screen, update the information and click **Save**.



Viewing/Search Ports

To view or search for ports registered in the Port Group object:

You can check the registered ports in the [Modify Port Group](https://docs.logpresso.comnull) screen.



* **Protocol**: Transport layer protocol (TCP, UDP)
* **Range**: Range of port numbers
* **Description**: Description of the port

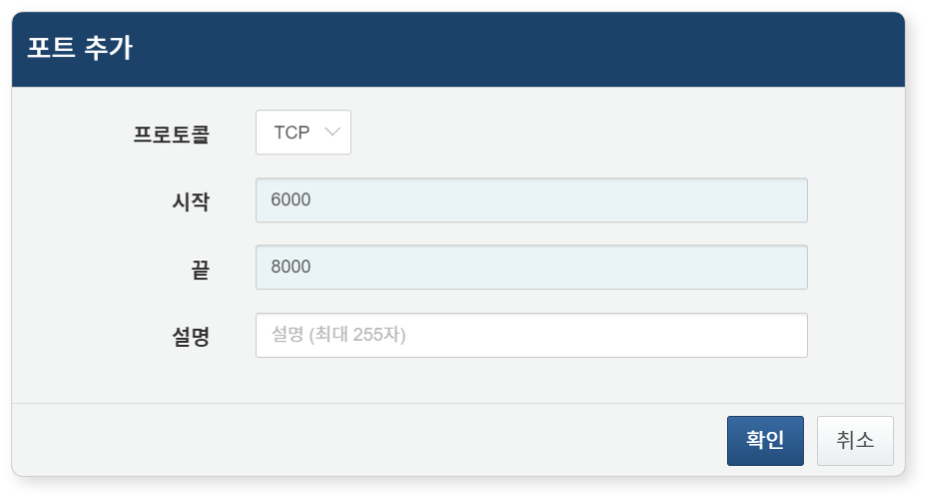
The **Modify Port Group** screen also supports searching. The search tool will display ports that contain the entered term in the **Range** or **Description** fields. The search tool is case-insensitive.

Adding a Port

To add a port to a Port Group:

Click **Add** in the toolbar on the [Modify Port Group](https://docs.logpresso.comnull) screen.

In the **Add Port** dialog, enter the port to be registered and click **OK**.



* **Protocol**: The protocol of the port to be registered (Range: TCP, UDP, Default: TCP)
* **Start**: The starting number of the port range (0-65535)
* **End**: The ending number of the port range (0-65535). When registering a single port number, enter the same port number for both start and end.
* **Description**: A detailed description of the port item (up to 255 characters)

Modifying a Port

To modify a registered port in a Port Group:

Click **Modify** on the row of the port you wish to change in the [Modify Port Group](https://docs.logpresso.comnull) screen.

In the **Modify Port** dialog, update the port information and click **OK**.

Deleting a Port

To delete a registered port from a Port Group:

Select the checkbox for the port row you wish to delete in the [Modify Port Group](https://docs.logpresso.comnull) screen.

Click **Delete** in the toolbar.

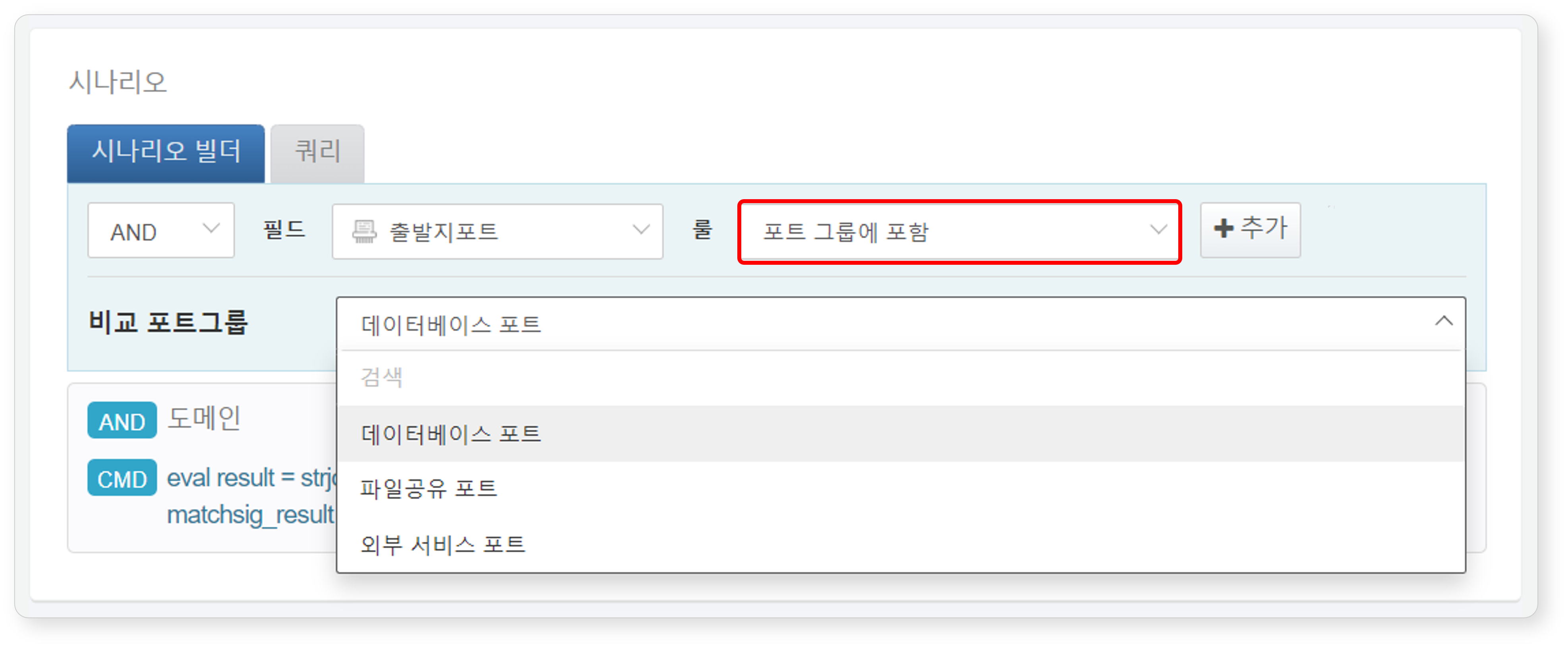
In the **Delete Port** dialog, confirm the port to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

#### Utilizing Port Groups

Port Groups can be used in the following ways:

Scenario Builder

In **Policies > Real-Time Detection**, you can configure scenarios using the Scenario Builder to check if the port number in the input field is included in the Port Group.



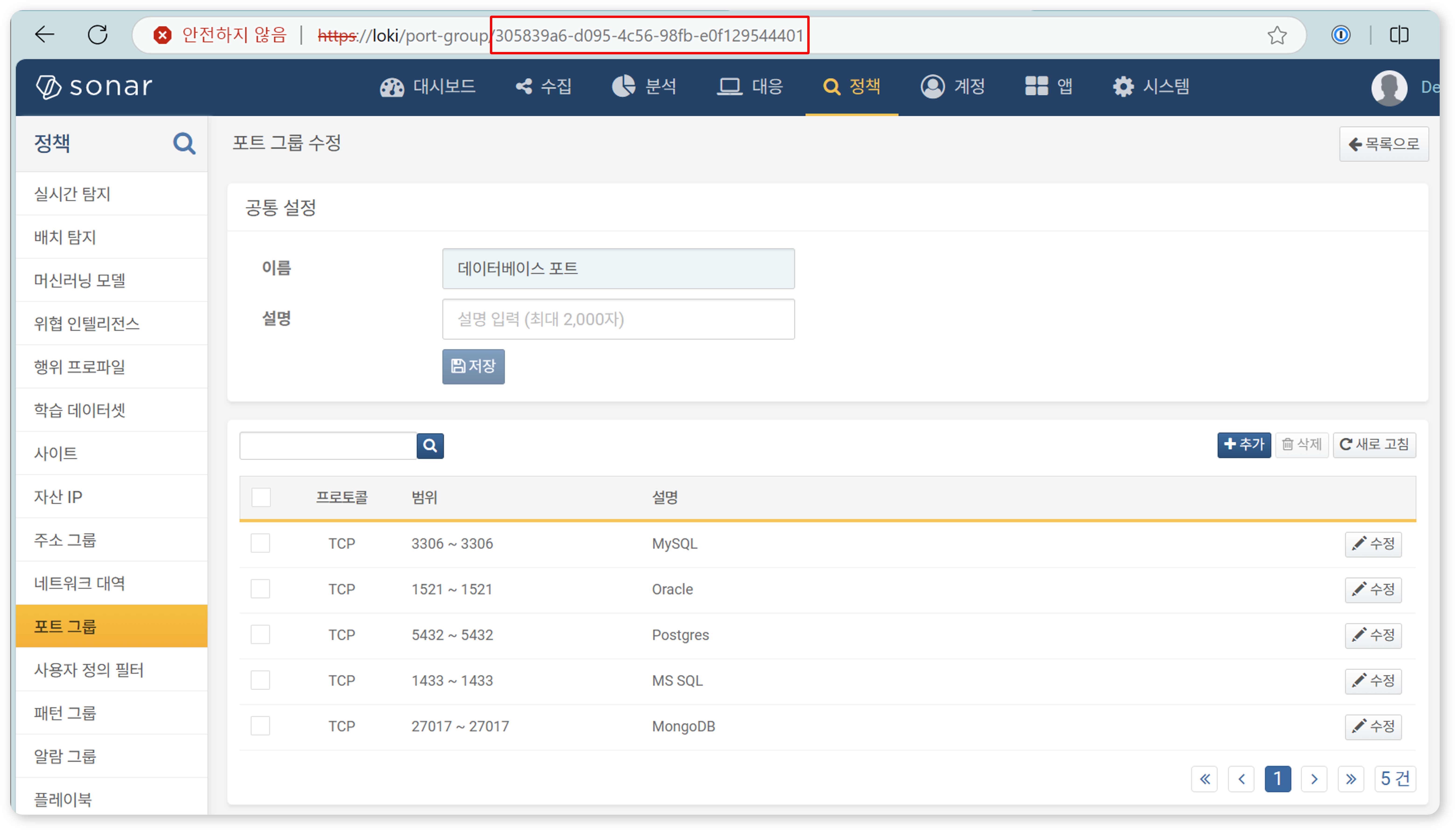
The following summarizes the Port Group-related content that can be used when the input field type is **PORT** in the Scenario Builder. For more details, refer to [Rules and Parameters by Field Type](https://docs.logpresso.comnull).

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Parameter | Input Range | Description |
| Included in Port Group | Compare Port Group | Select Port Group | Filters field values included in the Port Group |

Query

In **Policies > Real-Time Detection** or **Policies > Batch Detection**, when adding or modifying detection scenarios, you can utilize the [matchport](https://docs.logpresso.comnull) command or [matchport()](https://docs.logpresso.comnull) function to leverage Port Groups. Remember that you can use Port Groups anywhere a query input feature is available.

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



#### Deleting a Port Group

To delete a Port Group:

Select the checkbox for the row of the Port Group you wish to delete in the Port Group list.

Click **Delete** in the toolbar.

In the **Delete Port Group** dialog, confirm the list of Port Groups to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

Be cautious when deleting a Port Group referenced in real-time detection or batch detection scenarios, as it may cause the detection scenarios to not function as intended.