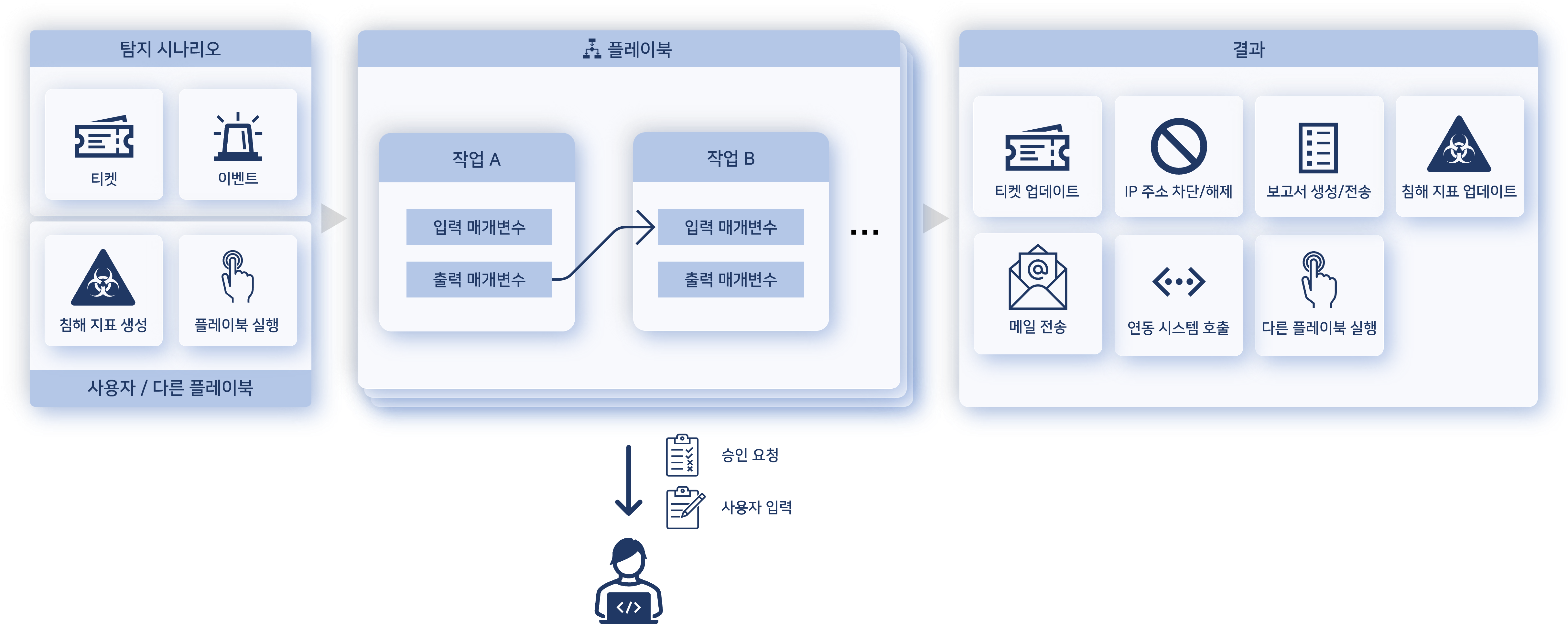
### Playbook

#### Overview

A playbook is a feature that performs automated responses in various situations according to detection scenarios. For instance, it operates when an event is detected, a ticket is issued, a new indicator of compromise (IOC) is registered, or when a user requests execution. The playbook automatically executes a series of tasks according to predefined procedures.

For example, it can automatically block an IP address attempting an attack by integrating with information security systems such as firewalls. Additionally, if abnormal traffic is detected and data leakage is suspected, it can further investigate the data and send alerts via email to the response team.

The following diagram illustrates the concept of a playbook.



Playbooks are executed automatically based on set conditions. They can execute multiple tasks sequentially or in branches, with each task using input data to perform its function and return results. These results are then used as inputs for subsequent tasks, and the playbook concludes once the final task is completed.

Tasks that require user judgment during playbook execution will request approval from the user or prompt them to input necessary data. Tasks requiring user approval can be checked under **Response > Approval Request**.

If the playbook is not visible in the web console, it may be due to a lack of license or an expired license. Please contact Logpresso for a playbook license.

Purpose

The benefits of using a playbook include:

* **Automation of Responses**: Playbooks automate repetitive security response tasks, reducing the burden on security monitoring organizations. For example, when a specific type of security alert occurs, it can automatically isolate related systems or analyze malicious files.
* **Workflow Orchestration**: Playbooks coordinate workflows between various security tools and systems. For instance, when an alert occurs, it can register it in a ticketing system, perform further investigation through log analysis tools, and report the results to other systems.
* **Standardization of Policies and Procedures**: Using playbooks allows for the standardization of security incident response procedures. This ensures that all security monitoring personnel handle security incidents consistently, thereby reducing response times.
* **Real-Time Response and Analysis**: Playbooks enable real-time analysis and response to events, minimizing the impact of security incidents and allowing for quick resolution of issues.
* **Reporting and Audit Capabilities**: Playbooks log their execution history, allowing for the generation of reports on the security incident response process. This enables security monitoring organizations to evaluate the effectiveness of their responses and improve procedures as necessary.

#### Managing Playbooks

Viewing/Search Playbook List

You can view or search the playbook list under **Policy > Playbook**.



* **Start**: Execute the playbook
* **Status**: Toggle button for playbook activation (: Active, : Inactive)
* **Start Type**: The type of start for the playbook (Manual, Ticket Creation, Event Creation, IOC Creation)
* **Name**: The unique name of the playbook
* **Description**: Description of the playbook
* **Modified Date**: The date the playbook was created or last modified

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

Refreshing the List

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

Export/Import

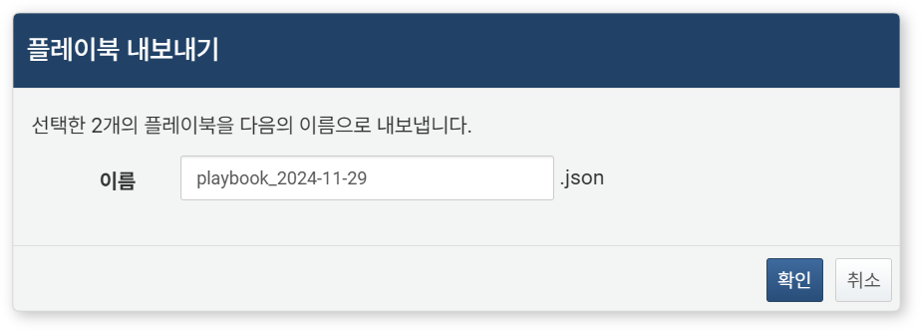
You can export or import playbooks as files. Use this feature to back up or restore playbooks.

To export a playbook:

Select the checkbox for the row of the playbook you want to export from the [Playbook List](https://docs.logpresso.comnull). You can select more than one playbook to export.

Click **Export** in the toolbar.

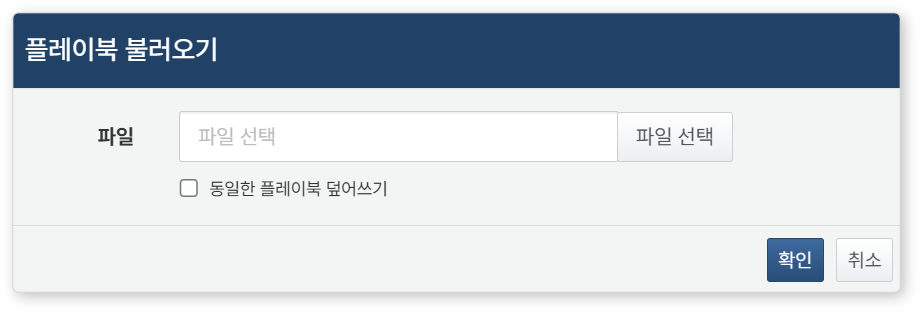
In the **Export Playbook** dialog, set a name and click **OK**.



To import a playbook:

Click **Import** in the toolbar.

In the **Import Playbook** dialog, select the playbook file and click **OK**.



* Selecting **Overwrite Existing Playbook** allows you to ignore duplicates and overwrite them (default: not selected). The criterion for duplication is the GUID. If this option is not selected, playbooks with the same GUID will not be imported.

Adding/Modifying Playbooks

To add or modify a playbook:

Click **Create** in the toolbar from the [Playbook List](https://docs.logpresso.comnull) to add, or click the **Name** of the playbook you want to modify.

Use the [Playbook Editor](https://docs.logpresso.comnull) to create or modify the playbook.

After completing the addition/modification, click **Save** or **Save and Exit** in the playbook editing screen.

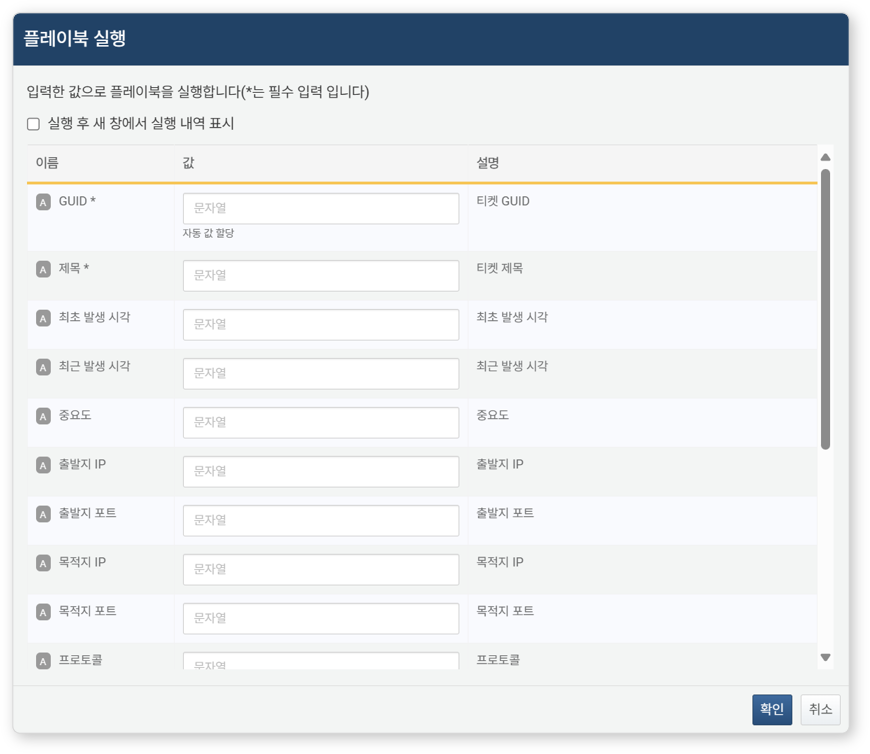
Executing Playbooks

Users can directly execute playbooks. To execute a playbook immediately:

Click **Start** for the playbook you want to execute from the [Playbook List](https://docs.logpresso.comnull).



Enter the input parameters in the **Execute Playbook** window and click **OK**. Playbooks that do not require input parameters will execute immediately.



* **Show Execution History in New Window After Execution**: You can view the execution history of the playbook in a new browser window (default: not selected).
* The list of input parameters varies depending on the playbook's [Start Type](https://docs.logpresso.comnull).

The execution history of the playbook can be checked under **Response > Automated Response History**.

Cloning Playbooks

Instead of creating a playbook from scratch, it is more efficient to clone and modify an existing playbook. To clone a playbook:

Select the checkbox for the row of the playbook you want to clone.

Click **Clone** in the toolbar.

The cloned playbook will be saved with the name '~ Copy'. You can then rename and modify it as needed.

Deleting Playbooks

To delete a playbook:

Select the checkbox for the row of the playbook you want to delete from the playbook list.

Click **Delete** in the toolbar.

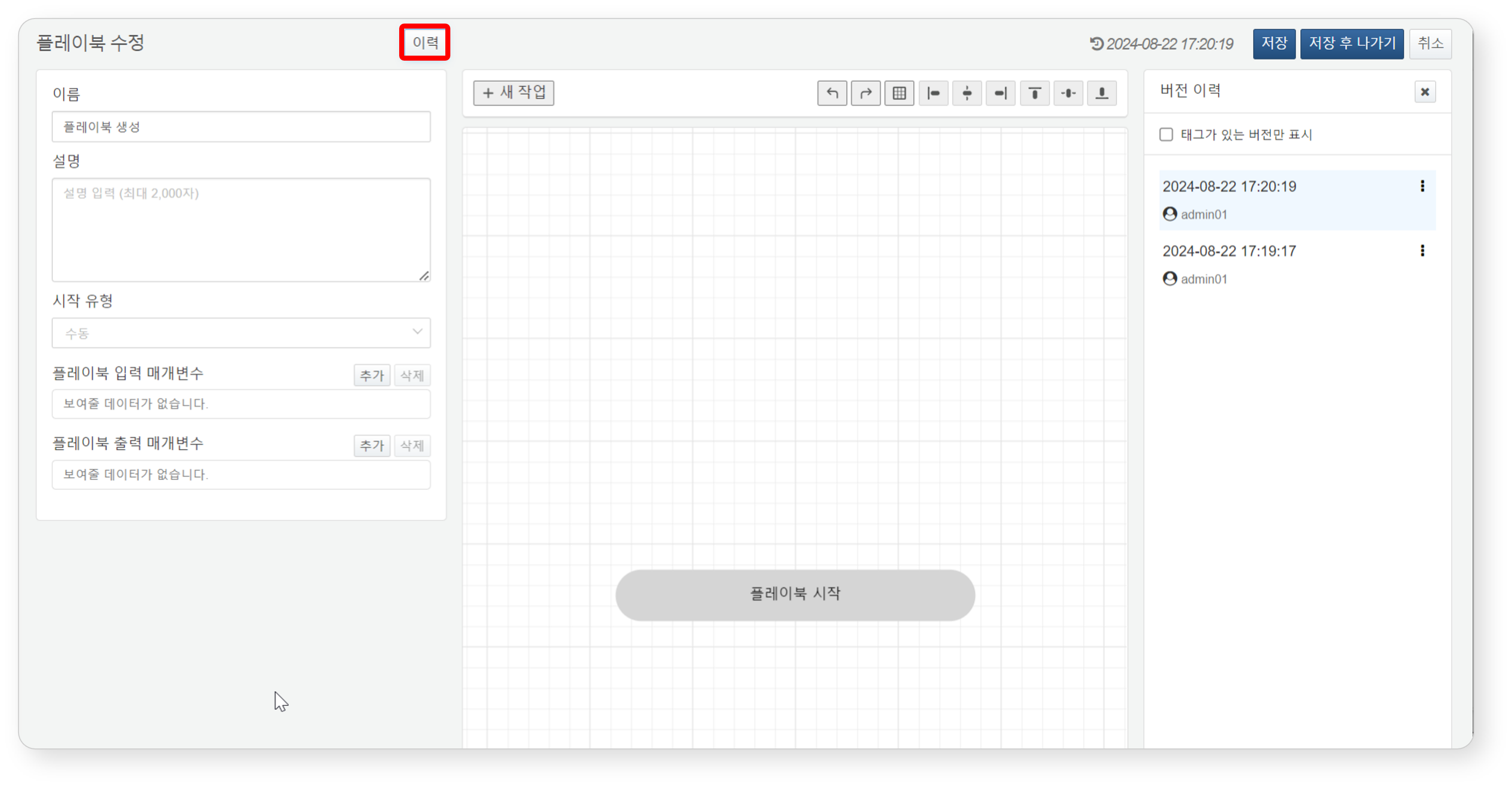
In the **Delete Playbook** dialog, review the list of playbooks to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

Playbook Version Control

When a user edits and saves a playbook in the [Playbook Editor](https://docs.logpresso.comnull), each setting is saved based on the timestamp of when it was saved. This allows for version control by separately saving the modified state of the playbook.

Viewing History

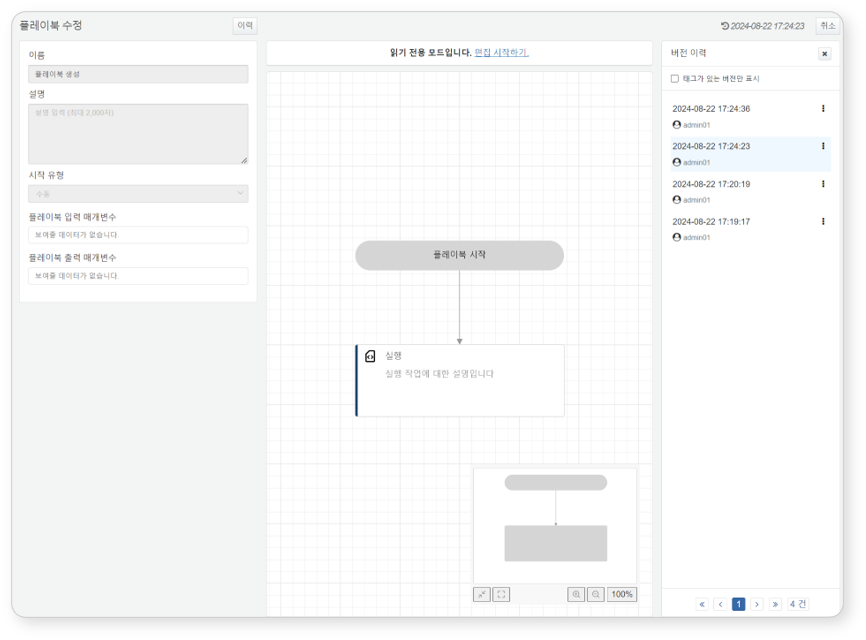
To open or close the version history panel of the playbook, click **History**. Clicking while the panel is closed will open it, and clicking while it is open will close it.



Rollback

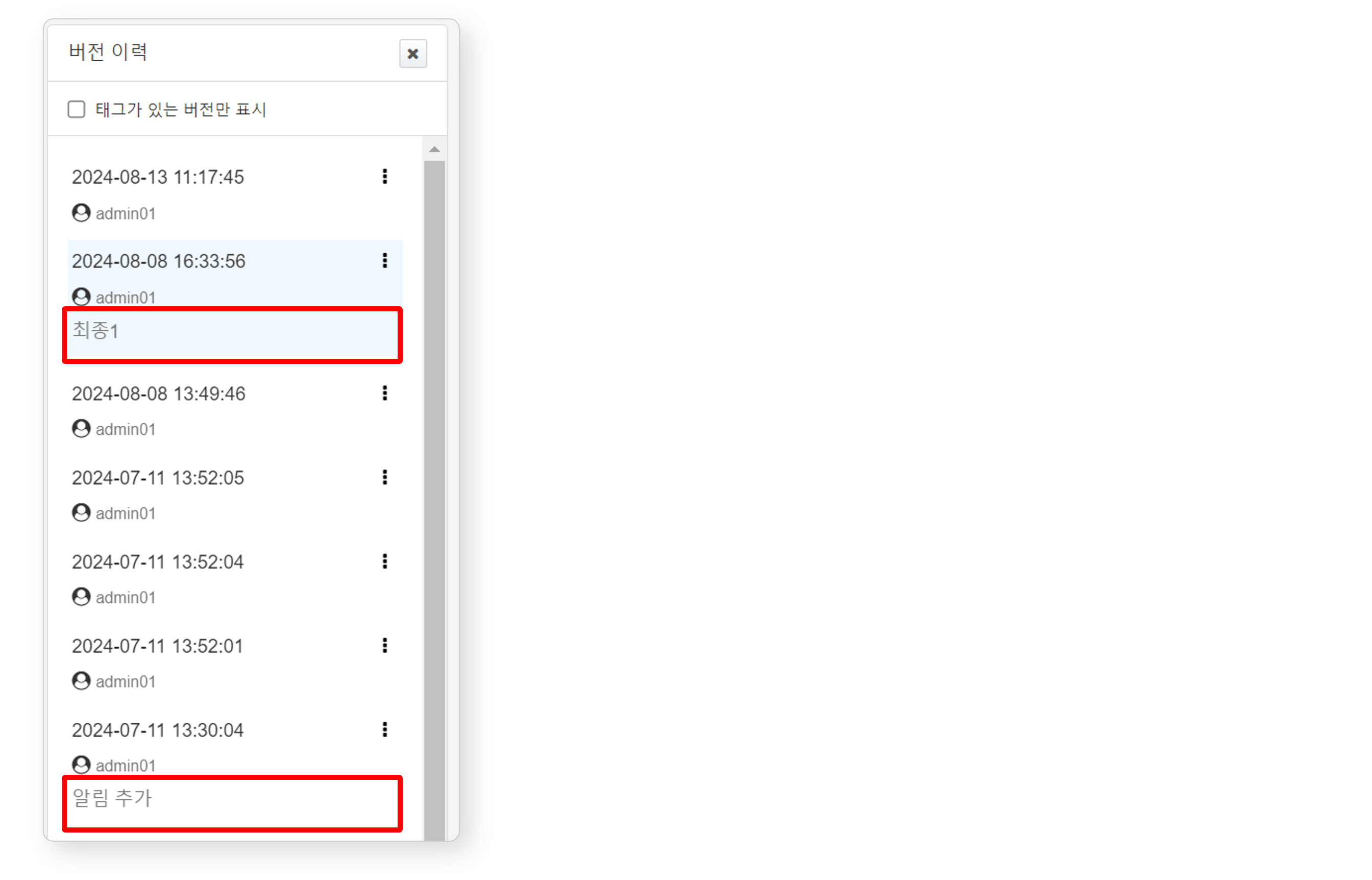
Clicking on a past version history in the version history panel will bring up the settings of that version in read-only mode.

Clicking **Start Editing** allows you to edit that version. If you save the edited version, it will be saved with the timestamp of when it was saved, and the playbook will execute based on the most recently saved version.



Version Tagging

You can tag specific version histories and verify them. By setting **Show Only Versions Without Tags** in the version history, you can separately view only the histories with tags.



To add a tag to a specific version history:

Select the history to which you want to add a tag and click "**⁝**".

Select **Add Tag** from the options menu.

In the **Tag Settings**, enter the tag you want to assign and click **OK**.

To modify a tag assigned to a specific version history:

Select the history to modify the tag and click "**⁝**".

Select **Modify Tag** from the options menu.

In the **Tag Settings**, enter the tag you want to modify and click **OK**.

To remove a tag assigned to a specific version history:

Select the history to delete the tag and click "**⁝**".

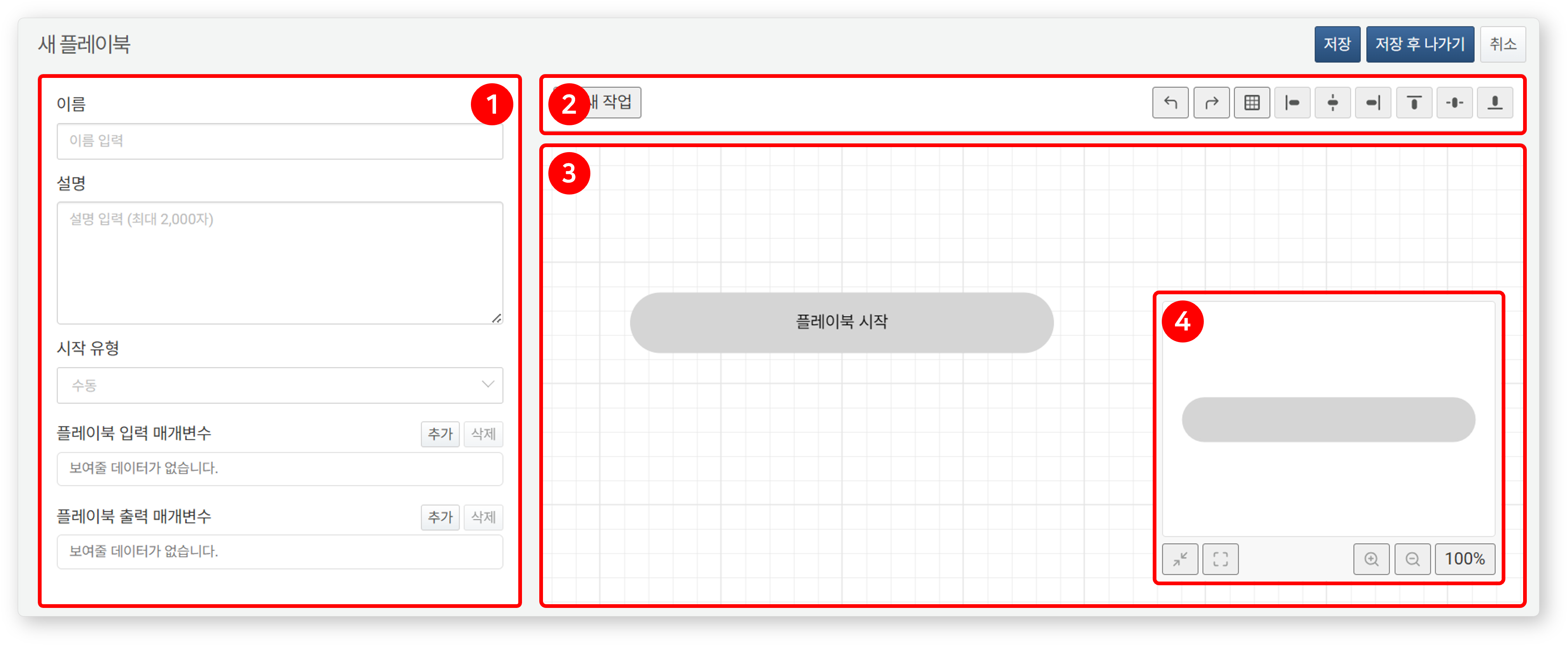
Select **Delete Tag** from the options menu.

#### Playbook Editor

All additions or modifications to playbooks are done through the Playbook Editor.

Screen Composition

When you first add a playbook, the initial screen appears as follows:



(1) **Properties Panel**: The properties panel displays the [Playbook Properties](https://docs.logpresso.comnull) or the [Common Properties](https://docs.logpresso.comnull) and [Type-Specific Properties](https://docs.logpresso.comnull) of tasks. After changing properties, click **Save** at the bottom of the panel to save your edits.

(2) **Toolbar**: Provides options to add new tasks, undo/redo, show/hide gridlines, and alignment tools.

**New Task**: Function to add a new task object

**Undo/Redo**: Undo or redo the most recent actions in reverse order

**Show/Hide Gridlines**: Toggle button to show/hide background gridlines

**Align**: Align or arrange two or more task objects (left, center, right, top, middle, bottom)

(3) **Task Flowchart**: The task flowchart is the screen where task objects that make up the playbook are arranged and connected to form a flow. You can specify the execution order of tasks through [User Interaction](https://docs.logpresso.comnull).

(4) **Map**: The map shows the overall information of the playbook, including the positions and connections of tasks within the task flowchart. Clicking on a specific location in the map will display the task flowchart based on that location.

**Hide/Show Map**: Hides or shows the map.

**Fit to Screen**: Adjusts the size of the task flowchart to view all tasks in one screen.

**Zoom In/Out of Flowchart**: Zooms in or out of the flowchart screen.

**Zoom Ratio**: Displays the ratio of the task flowchart. Clicking this button will change the ratio to actual size (100%). When zooming in or out of the flowchart screen, the current screen ratio will be displayed.

User Interaction

Most tasks are performed in the task flowchart. In the task flowchart, users can perform the following actions:

* **Click**: Move the cursor over an object on the screen and press the left button.
* **Right Click (Secondary Click)**: Move the cursor over an object on the screen and press the right button.
* **Drag and Drop**: Dragging is the action of clicking on a specific object visible on the screen and moving the cursor to another location while holding the click. Dropping is the action of releasing the button while in the drag state. Dragging and dropping are used together.
* **Wheel Scroll**: The action of scrolling the mouse wheel up or down.

Clicking, right-clicking, dragging & dropping perform different actions depending on the target object.

The descriptions are based on a right-handed mouse. The actions may differ based on mouse settings.

**Click/Right Click**: The interactions that can be performed through clicking/right-clicking are as follows:

**Drag and Drop**: The interactions that can be performed through drag and drop are as follows:

**Wheel Scroll**: The interactions that can be performed through wheel scrolling are as follows:

Shortcuts

Shortcuts are actions that quickly execute commands within the program by pressing specific key combinations. The playbook editing screen provides the following shortcuts.

|  |  |  |
| --- | --- | --- |
| Windows/Linux | macOS | Function |
| **ESC** | **ESC** | Deselect, cancel playbook/task property editing |
| **Ctrl+Z** | **Cmd+Z** | Undo |
| **Ctrl+Y** or **Ctrl+Shift+Z** | **Cmd+Shift+Z** | Redo |
| **Ctrl+A** | **Cmd+A** | Select all tasks/connections in the flowchart |
| **+** or **=** | **+** or **=** | Zoom in on the flowchart screen |
| **-** | **-** | Zoom out of the flowchart screen |
| **G** | **G** | Show/hide gridlines in the flowchart |
| **F** | **F** | Fit flowchart to screen |
| **M** | **M** | Show/hide map |
| **Delete** or **Backspace** | **Delete** or **Backspace** | Delete selected tasks/connections |

Task Connection Rules

Playbooks operate by connecting tasks according to defined flows. Task flows can branch into multiple flows or merge together.

**(1) All tasks must be connected.**

All tasks except the first one must be connected to at least one preceding task