### Batch Detection

#### Overview

Batch detection scenarios analyze the correlation between different data collected from various systems by periodically executing [Logpresso queries](https://docs.logpresso.comnull) according to a schedule. This allows for the analysis and detection of various events, activities, and patterns. The following illustration depicts the operation of a batch detection scenario. Batch detection scenarios are typically applied to data sources stored in tables.

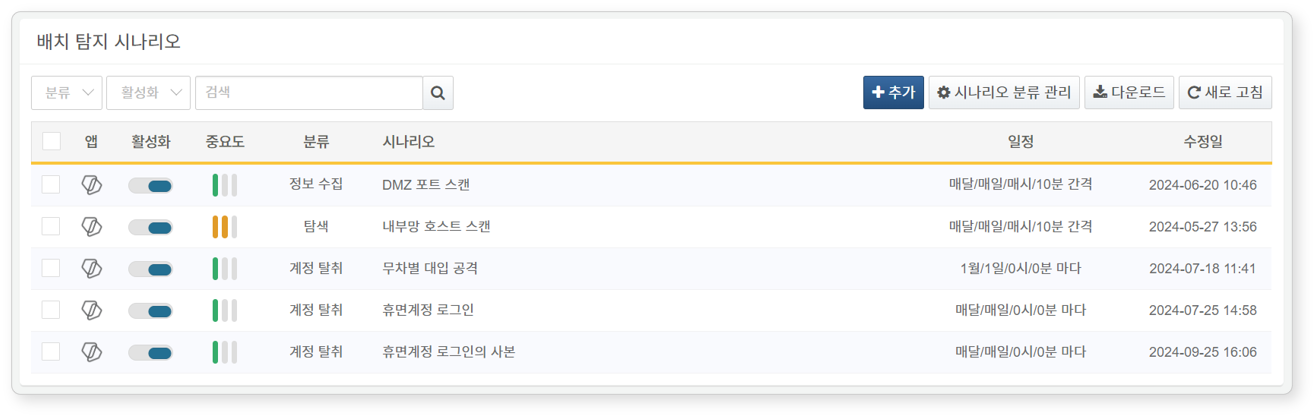


Batch detection scenarios utilize [Logpresso query](https://docs.logpresso.comnull) commands and functions, allowing for flexible scenario creation. For example, it is possible to identify the activity relationships of specific users to predict potential threats and detect suspicious activities.

In most cases, batch detection scenarios issue tickets or request explanations from event actors during event detection. Excessive ticket issuance can increase the workload of malware analysts or security monitoring personnel, necessitating the minimization of duplicate ticket issuance. Logpresso Sonar provides functionality to handle identical events as a single ticket based on alarm messages and ticket titles used during event detection, or based on duplicate criteria fields.

#### Viewing/Search Batch Detection Scenario List

You can view or search the list of batch detection scenarios in **Policy > Batch Detection**.



* **App**: The app icon associated with the detection scenario. Default scenarios or user-added scenarios are represented by the Logpresso icon, while scenarios from installed apps are displayed with the respective app icons.
* **Activation**: Toggle button for activating the detection scenario (: Activated, : Deactivated)
* **Importance**: The importance of the detection scenario (High/Medium/Low)
* **Classification**: Classification information applied to the scenario
* **Scenario**: Name of the detection scenario
* **Schedule**: Execution cycle of the detection scenario
* **Modification Date**: The date the detection scenario was last modified (or created)

To find a specific batch detection scenario in the list, use the search tool in the toolbar. The search tool will display batch detection scenarios that include the entered word in the **Name**, **Description**, or **Stream Query** fields. The search tool is case-insensitive.

Activating/Deactivating Scenarios

To activate or deactivate a batch detection scenario, click the toggle button in the activation column of the detection scenario (: Activated, : Deactivated).

Downloading the List

To save the batch detection scenario list to your local PC, click **Download** in the toolbar.

Refreshing the List

To refresh the batch detection scenario list with the latest information, click **Refresh** in the toolbar.

#### Adding a Batch Detection Scenario

To add a batch detection scenario:

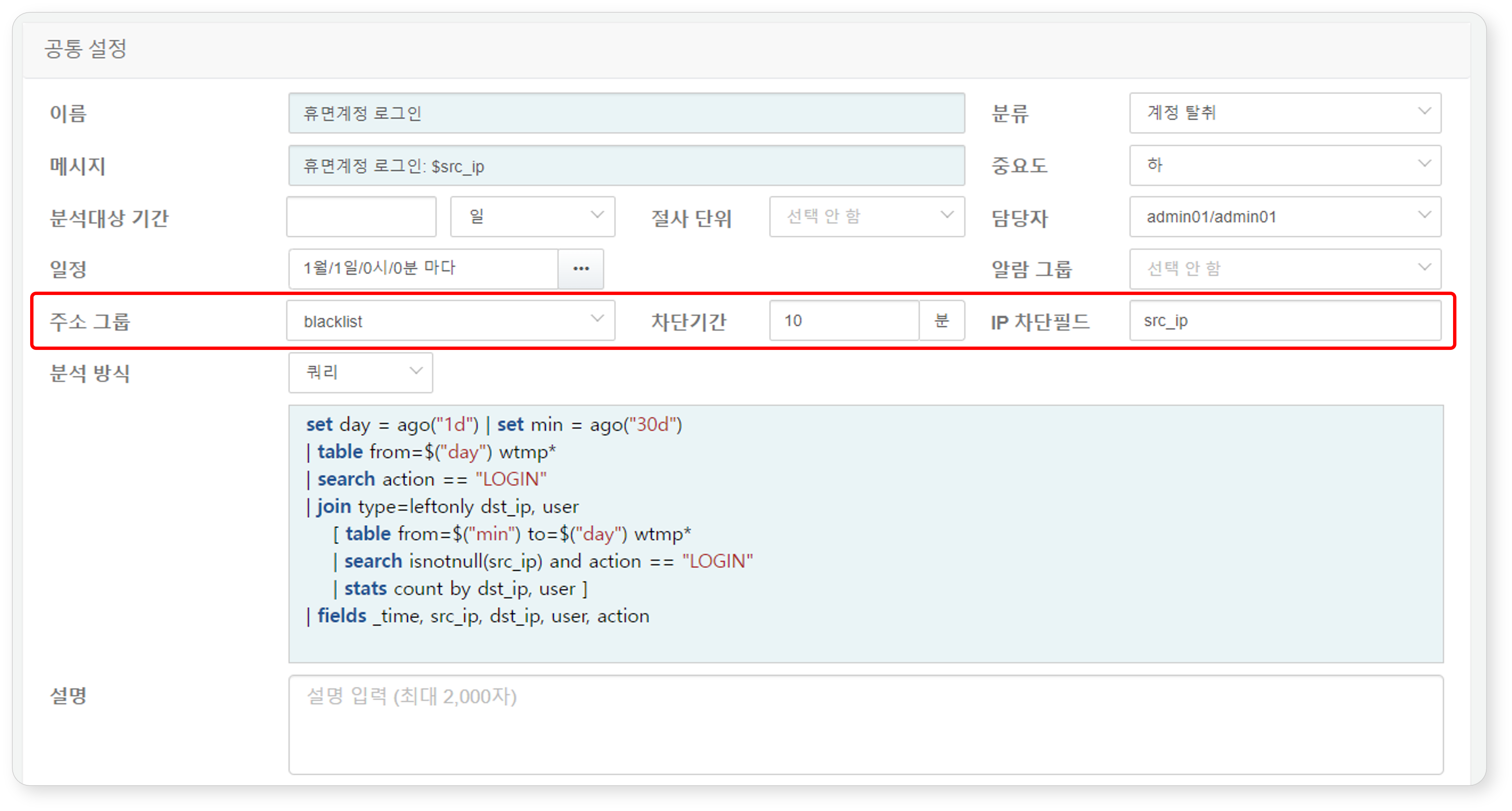
Click **Add** in the toolbar under **Policy > Batch Detection**.

In the **Add Batch Detection Scenario** screen, configure the **Common Settings** section.



* **Name**: Name of the detection scenario (up to 50 characters). The name cannot be duplicated with other scenarios.
* **Classification**: Classification of the detection scenario. The classification will be displayed in the detection status list under **Analysis > Event Summary**. You can add or modify scenario classifications by clicking **Manage Scenario Classifications** in the toolbar. Tickets will not be generated if left unclassified.
* **Message**: Title to be assigned to the ticket upon event detection.
* Enter field names defined in the [Log Schema](https://docs.logpresso.comnull) in the format $FieldName or $FieldName$ to generate messages using field values from the logs that triggered the event detection (e.g., $src\_ip). If the field name contains Korean characters, use the $FieldName$ format.
* If the **Duplicate Criteria Field** is not set in **Advanced Settings**, duplicate tickets will be prevented based on the identical nature of the generated message (maximum range: 2,000 characters).
* **Importance**: Importance of the detected event (High, Medium, Low)
* **Analysis Period**: This feature applies when the **Analysis Method** is set to **Query** and is used to assign values to the parameters from and to that specify the period for data analysis. Enter a number along with a time unit (seconds, minutes, hours, days) (default: not set). To use this feature, the command that retrieves data in the query (e.g., table) must include the options from=$("from") to=$("to").
* For example, if "30 days" is specified for the analysis period, when executing a query (e.g., table from=$("from") to=$("to") FW\_\*), data collected from 30 days prior to the query execution time will be retrieved from the table (with names starting with "**FW\_**") (range: 1 to 3,153,600,000).
* **Truncation Unit**: Time precision to be applied to the retrieved data. Select a time unit (default: not selected, range: not selected, seconds, minutes, hours, days) to display the time precision of the data accordingly.
* For example, if the **Analysis Period** is set to **5 minutes** and the **Truncation Unit** is set to **seconds**, the millisecond values in the time information of the analyzed data will be discarded and changed to seconds.
* **Responsible Person**: Account [Users](https://docs.logpresso.comnull) to whom the issued ticket will be assigned. You can select more than one account. If not specified, the ticket will be created without an assigned responsible person.
* **Schedule**: Execution cycle schedule of the detection scenario. Click the **...** button to specify the execution cycle according to [CRON syntax](https://www.man7.org/linux/man-pages/man5/crontab.5.html).
* **Alarm Group**: [Alarm Group](https://docs.logpresso.comnull) that will receive alarms upon event detection.
* Choose the method of receiving alarms in the alarm group.
* **Analysis Method**: Method of data analysis to be executed according to the schedule (default: Query, range: Dataset, Query)
* When **Dataset**: Select the dataset to be executed from the [Dataset](https://docs.logpresso.comnull) list.
* When **Query**: Enter the query directly (up to 5,000 characters).
* **Description**: Detailed description of the detection scenario (up to 2,000 characters).

If you wish to manage the attacker's IP address or anomalous actor's IP address separately upon event detection, or to relay address group information in conjunction with firewalls, IPS, etc., configure the following items.



* **Address Group**: The address group to which the IP address set in the **IP Block Field** will be added when an event is detected. Additional settings can be made in **Policy > Address Groups** if necessary.
* **Blocking Period**: The duration (in minutes) for which the identified IP address, suspected of being a threat, will be retained in the address group after being added. If the IP address specified in the **IP Block Field** is added to the address group upon event detection, it will be automatically removed from the address group after the set blocking period elapses. If no blocking period is set, it will remain in the address group indefinitely (range: 1 to 100,000,000).
* **IP Block Field**: The field name of the IP address to be managed by adding it to the address group upon event detection. Enter the field names related to IP addresses set in the log schema (e.g., src\_ip, dst\_ip) (up to 50 characters).

For settings related to blocking integration with third-party information security systems, refer to 'System > Blocking Integration'.

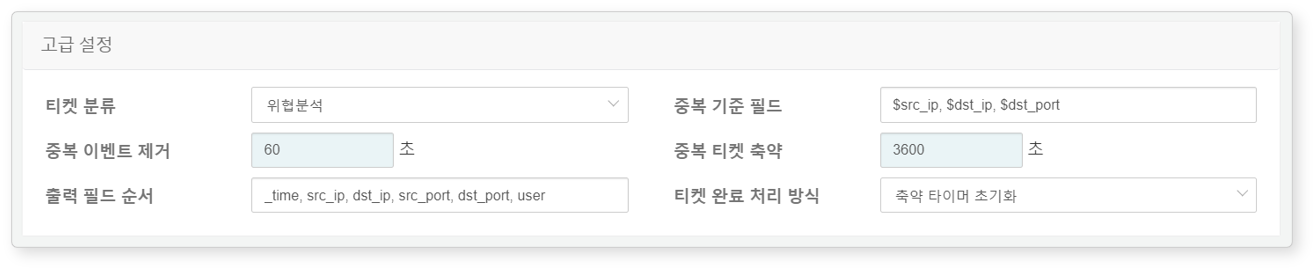
If the detected event is related to the organization's employees, you can request explanations from those employees.



* **Explanation Request**: Whether to use explanation requests (default: disabled)
* **Explanation Target Field**: Field containing the employee number information of the employee to be requested for an explanation.
* When a threat is detected, an automatic explanation request email will be sent to the employee mapped to that employee number. In this case, employee information (employee number, account, email) must be set in **Policy > Employees**.
* **Classification**: Classification of the explanation. If necessary, click **Manage Explanation Classifications** in **Response > Explanations** to add settings.
* **Secondary Reviewer**: Secondary reviewer for the explanation (if not set, defaults to "Department Head"). For information on primary and secondary reviewers, refer to [Explanations](https://docs.logpresso.comnull).
* **Deadline**: Deadline for processing the explanation (default: 7 days). After the deadline, the explanation target cannot submit an explanation.
* **Remarks**: Additional content to be included in the explanation request email. The entered content will be inserted at the location of the text macro $user\_note in the email/SMS template body. You can enter field names defined in the schema in macro format like $FieldName in the remarks, which will be replaced with field values. You can check the remarks in the detailed explanation content in **Response > Explanations** (up to 10,000 characters).

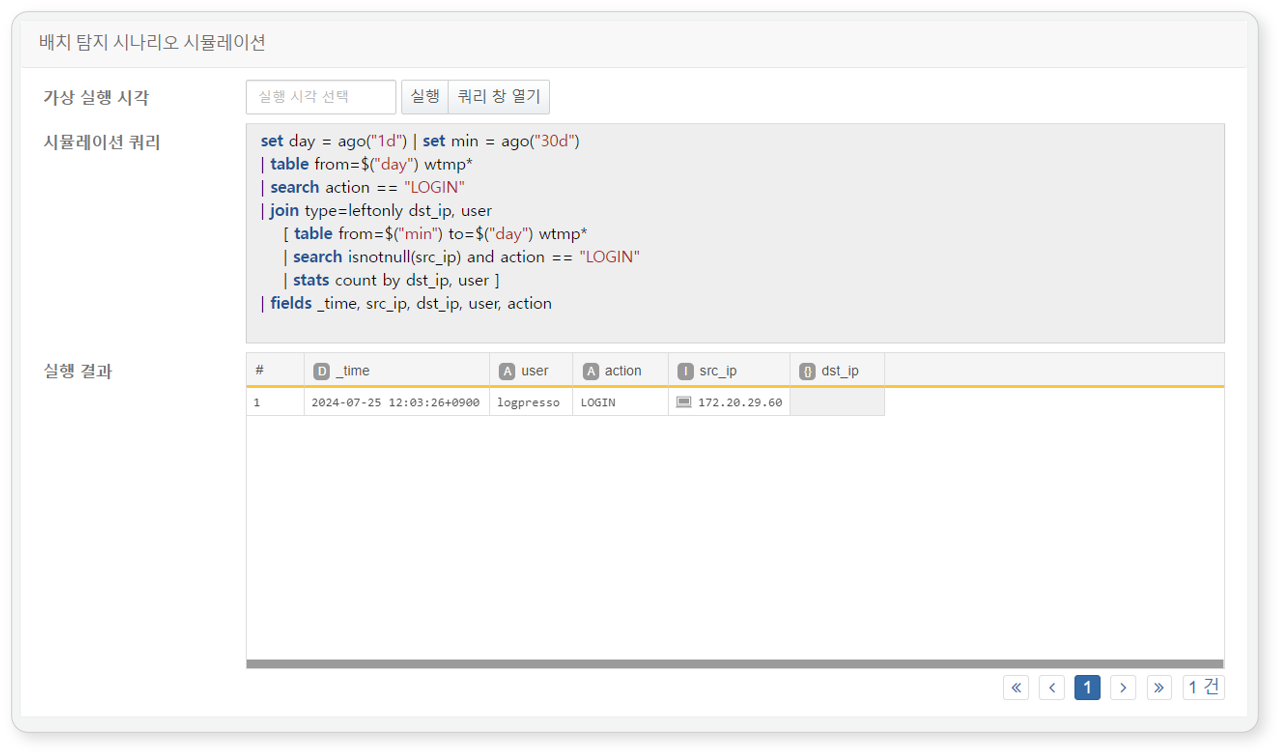
To request an explanation, a field named "emp\_key" is required. If this field is not present, create the emp\_key field when writing the query in step 3, and ensure it can be mapped to user accounts or IP addresses.

To issue tickets upon event detection, configure the **Advanced Settings** section.



* **Ticket Classification**: [Ticket Classification](https://docs.logpresso.comnull) necessary for distinguishing tickets during security monitoring operations (default: not selected).
* To ensure that tickets are automatically generated upon event detection, you must specify a ticket classification. The playbook that operates on the event as a trigger can also determine whether to create a ticket. Do not use this item if you want to determine ticket creation in the playbook.
* **Duplicate Criteria Field**: Enter the name of the field to be used as the basis for duplicate ticket verification in macro format like $FieldName, separated by commas (range: up to 2,000 characters). If not set, the **Message** string will be used as the basis for judgment.
* For example, if the message item is set to "C&C Server Access: $src\_ip -> $dst\_ip", but you want to avoid unnecessary multiple events or tickets for accessing different C&C servers from the same host, set the duplicate criteria key to '$src\_ip'.
* **Remove Duplicate Events**: The period (default: 0, range: 0 to 86,400 seconds) during which duplicate events will be ignored after ticket issuance when the same event occurs consecutively.
* When "0": Operates according to the **Duplicate Ticket Reduction** setting.
* When not "0": Ignores the same event for the specified period and does not use it as supporting material for that ticket.
* **Duplicate Ticket Reduction**: The period (default: 3,600, range: 0 to 86,400 seconds) during which, if the same event occurs after ticket issuance, no new ticket will be issued, and only supporting material and occurrence count will be added to the already issued ticket.
* When "0": A new ticket with the same title is created every time the event occurs.
* When not "0": For the specified period, only supporting material and occurrence count are recorded in the existing ticket.
* **Output Field Order**: The order of log data fields to be displayed in the supporting material of the ticket. Enter field names separated by commas in the order they should be displayed (range: up to 2,000 characters; special characters and pipe symbols excluded).
* **Ticket Completion Handling Method**: The handling method for tickets with **Duplicate Ticket Reduction** set after they are completed (default: reset reduction timer).
* **Maintain Reduction Timer**: Even if the ticket is completed, if the same threat event occurs before the duplicate ticket reduction time expires, supporting material and occurrence count will be recorded in the completed ticket.
* **Reset Reduction Timer**: When the ticket is completed, it is considered that the duplicate ticket reduction time has also expired, and a new ticket will be issued if the same threat event occurs.

You can simulate the execution of the batch detection scenario to match a specific past or future time. Set the **Virtual Execution Time** in **Batch Scenario Simulation** and click **Execute**.



If an invalid query is entered or a non-existent data table is specified when entering the analysis method, the batch detection scenario simulation cannot be executed.

#### Cloning Batch Detection Scenarios

To clone an existing batch detection scenario:

Select the checkbox for the batch detection scenario row you wish to clone in the batch detection scenario list. The toolbar will display the action menu.

Click **Clone** in the toolbar.

In the **Clone Batch Detection Scenario** dialog, review the list of batch detection scenarios to be cloned and click **Clone**. Click **Cancel** if you do not wish to clone.

A new scenario will be added in a disabled state with the name 'Copy of Scenario Name'.

#### Modifying Batch Detection Scenarios

To modify a batch detection scenario:

Click the name of the batch detection scenario you wish to modify in the batch detection scenario list.

In the **Modify Batch Detection Scenario** screen, make the necessary changes and click **OK**. For descriptions of the properties to be modified, refer to [Adding Batch Detection Scenarios](https://docs.logpresso.comnull).

#### Executing Batch Detection Scenarios

To execute a batch detection scenario immediately:

Select the checkbox for the batch detection scenario row you wish to execute in the batch detection scenario list.

The action menu will appear in the toolbar. Click **Execute Now** in the action menu.

Depending on the scenario, if events are detected, you can check the detection results in **Response > Tickets** and **Analysis > Event Summary**.

Executing a disabled batch detection scenario will run it normally, but no tickets will be generated.

#### Deleting Batch Detection Scenarios

To delete a batch detection scenario:

Select the checkbox for the batch detection scenario row you wish to delete in the batch detection scenario list.

The action menu will appear in the toolbar. Click **Delete** in the action menu.

In the **Delete Batch Detection Scenario** dialog, review the list of batch detection scenarios to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.

#### Managing Detection Scenario Classifications

To efficiently manage and classify threats detected by detection scenarios, you can add, modify, or delete scenario classifications. For more details on scenario classification management, refer to [Real-Time Detection - Detection Scenario Classification Management](https://docs.logpresso.comnull).