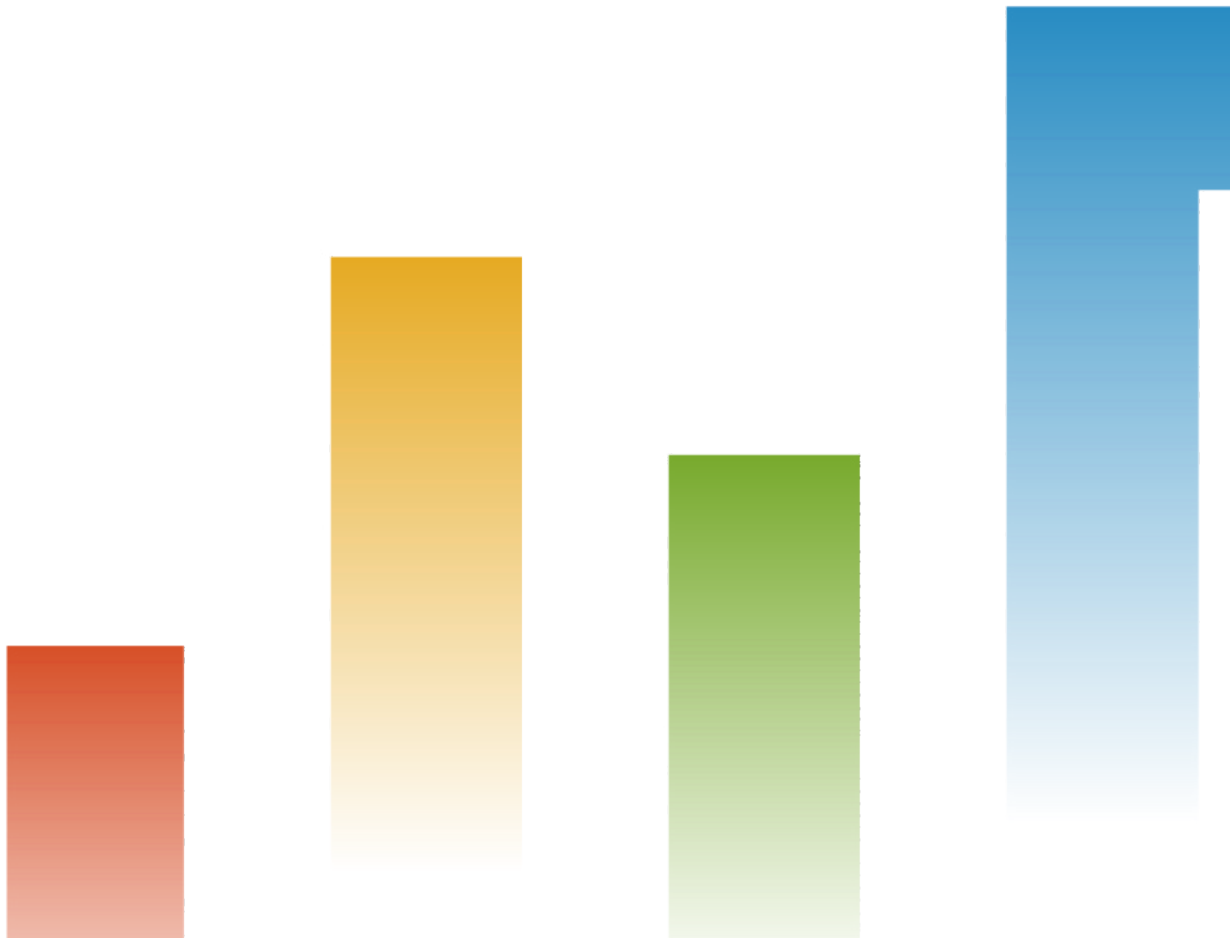


# URL Monitoring

release date. 2026. 09. 11.



# Table Of Contents

|                                      |    |
|--------------------------------------|----|
| • URL Monitoring .....               | 3  |
| ◦ Getting started.....               | 5  |
| ◦ URL List .....                     | 8  |
| ◦ Alert .....                        | 13 |
| ■ Event Configuration .....          | 0  |
| ■ Event Notification Settings.....   | 15 |
| ■ Event Notification Format.....     | 37 |
| ■ Event History and Monitoring ..... | 45 |
| ■ Real-time Notifications.....       | 53 |
| ■ System Events .....                | 56 |
| ◦ HTTP status code types.....        | 59 |
| ◦ Error Type .....                   | 67 |

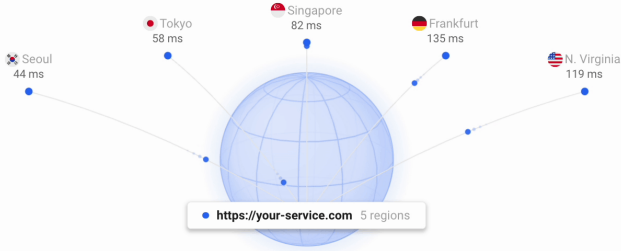
# URL Monitoring

WhaTap URL Monitoring is a service that periodically checks whether your website or service opens normally.

Once you set the address (URL) to monitor and the check interval, WhaTap automatically connects to that address and checks whether the website opens properly. When a problem occurs, such as the website not opening or the response slowing down, you can receive an alert to identify and respond to the incident quickly.

Introduction to URL Monitoring

Explain how to use this screen and its key features.



WELCOME TO URL MONITORING

See your service the way the world sees it.

Create your first project

**Catch downtime first**  
Alerts reach you in seconds — before the first user report does.

**Compare regions**  
Spot the market where your service feels slow to real users.

**Prove reliability**  
Uptime and latency history you can share with your team.

## Key features

- **Checking the global service URL**

You can select and monitor service areas such as North America, Europe, and Asia.

- **Free Service**

All functions in WhaTap URL Monitoring are provided for free.

- **Site availability check**

You can see the site access status by end users in real time through the HTTP status code.

- **Site performance monitoring**

Check the time to access the site from the server in Seoul, Tokyo, etc.

- **Notification settings for each URL**

WhaTap URL Monitoring provides multiple notification channels such as email, mobile push, and 3rd-party.

① URL monitoring service does not provide SMS alerts.

- **Integrated dashboard configuration for WhaTap services**

You can configure the dashboard with combining other WhaTap services such as servers, applications, databases, etc.

# Getting Started

To use the WhaTap monitoring service, after signing up in [Sign up](#), create a project and then add the URL. For more information about registration, see [the following](#).

## Project Creation

Create a project before adding the URL.

1. Go to the [WhaTap monitoring service](#) and log in.
2. To create a project, click **All Projects > + Project** in the side menu on the left of the screen.
3. On the **Select product** screen, click the **URL [ Create > ]** button.

ⓘ When you select the URL monitoring product, the project creation screen starts a three-step onboarding. The progress bar and step indicator at the top of the screen show your current position. When you fill in the required items for each step, the **Continue** button is enabled, and you can return to the previous step with the **Back** button. Clicking the **Back** button on the first step takes you to the product selection screen.

4. In the **Name your project** step, enter a name in the **Project name** field and click the **Continue** button. The name is required.
5. In the **Project settings** step, configure **Time zone**, **Notification language setting**, **Project groups**, and **Project description**, then click the **Continue** button.

| Item                         | Required | Description                                                                                                                                                                               |
|------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time zone</b>             | Required | Reference time for generating alerts and reports<br>- Default value: <b>(GMT +9:00) Seoul, Tokyo, Yakutsk</b><br>- For the available time zones, see <a href="#">the following list</a> . |
| <b>Notification language</b> | Required | Language for sending alerts; select Korean or English                                                                                                                                     |

| Item                       | Required                                               | Description                                                                                                                                                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| setting                    |                                                        |                                                                                                                                                                                                                                                                                                                            |
| <b>Project groups</b>      | Required for organization accounts, optional otherwise | Group that bundles multiple projects<br>- Select the group to which the project belongs.<br>- If there is no group to select, click the <b>Add Group</b> button to create a group first. The values you entered are retained, but the process restarts from the first step when you return from the group creation screen. |
| <b>Project description</b> | Optional                                               | Enter a description of the project.                                                                                                                                                                                                                                                                                        |

#### Available time zones



- (GMT -12:00) Eniwetok, Kwajalein
- (GMT -11:00) Midway Island, Samoa
- (GMT -10:00) Hawaii
- (GMT -9:00) Alaska
- (GMT -8:00) Pacific Time (US & Canada)
- (GMT -7:00) Mountain Time (US & Canada)
- (GMT -6:00) Central Time (US & Canada), Mexico City
- (GMT -5:00) Eastern Time (US & Canada), Bogota, Lima
- (GMT -4:00) Atlantic Time (Canada), Caracas, La Paz
- (GMT -3:00) Brazil, Buenos Aires, Georgetown
- (GMT -2:00) Mid-Atlantic
- (GMT -1:00) Azores, Cape Verde Islands
- (GMT) Western Europe Time, London, Lisbon, Casablanca
- (GMT +1:00) Brussels, Copenhagen, Madrid, Paris



- (GMT +2:00) Kaliningrad, South Africa
- (GMT +3:00) Baghdad, Riyadh, Moscow, St. Petersburg
- (GMT +4:00) Abu Dhabi, Muscat, Baku, Tbilisi
- (GMT +5:00) Ekaterinburg, Islamabad, Karachi, Tashkent
- (GMT +6:00) Almaty, Dhaka, Colombo
- (GMT +7:00) Bangkok, Hanoi, Jakarta
- (GMT +8:00) Beijing, Perth, Singapore, Hong Kong
- (GMT +9:00) Seoul, Tokyo, Yakutsk
- (GMT +10:00) Eastern Australia, Guam, Vladivostok
- (GMT +11:00) Magadan, Solomon Islands, New Caledonia
- (GMT +12:00) Auckland, Wellington, Fiji, Kamchatka

6. In the **Check location** step, click the button for the region to use, then click the enabled **Create project** button.

- The check location selected in the **Check location** step refers to the location of the data center that stores the project data.

7. You can check the new URL project in **Project list**.



For more information about **Project groups**, which bundles multiple projects for management, see [the following](#).



Up to 10 URL projects can be created.

# URL List

On the **URL list** screen, you can check the latest check results of the URLs registered in the project in real time, and add or edit URLs.

## Basic options

- **Search and sorting**

In the search input field on the upper left of the screen, you can search the list by URL or URL name. Clicking the sorting button next to it sorts the list by **Name**, **Status**, or **Agent region name**. The default setting is **Name**.

- **Real-time mode**

The **LIVE** indicator on the upper right of the screen shows the last refresh time. Clicking the pause button stops real-time mode, and clicking the refresh button retrieves the latest data immediately.

- **Project summary card**

The summary card above the list shows the name of the project you are currently viewing and the number of registered URLs. The count badge is based on all URLs registered in the project, so the value does not decrease when you apply a search term or a status filter. If there is no check history yet, a message notifying that data collection is pending appears.

- **Status filter**

Below the summary card, you can check the counts for each final response status and filter the list. The view can be seen based on **Total**, **Success**, **Redirection**, **Client error**, **Internal server error**, and **Unknown**. The default setting is **Total** view.

-  **Import** /  **Export**

Clicking the  **Import** button imports the URL list from an Excel file. Clicking the  **Export** button downloads the current URL list as an Excel file.

## Checking the URL list

You can check the monitoring check results for each registered URL. The columns are as follows.

| Column                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Current status code</b>                                                          | The final check response code (HTTP Status Code). Clicking a status code takes you to the HTTP status code document.                                                                                                                                                                                                                                                        |
| <b>Name/URL</b>                                                                     | The name entered when registering the URL and the URL to check                                                                                                                                                                                                                                                                                                              |
| <b>Location</b>                                                                     | The check location selected when registering the URL                                                                                                                                                                                                                                                                                                                        |
| <b>Elapsed time</b>                                                                 | The check results for the last 20 minutes (response code and response time) and the final response time. Dragging in the chart area retrieves the response codes and response times for that time period.                                                                                                                                                                   |
|    | To change the settings of a registered URL, click the  icon on the right of the row to go to <b>Edit URL</b> .                                                                                                                                                                             |
|  | To register a new URL with the same settings as an existing one, click the  icon to go to <b>Copy URL</b> . The existing values such as the check location, collection cycle, and event settings are retained. Because the name and URL cannot be duplicated, change them before saving. |
|  | To delete a registered URL, click the  icon, and then click the <b>Delete</b> button in the confirmation pop-up window.                                                                                                                                                                  |

 When you delete a URL, all data collected for that URL is deleted and cannot be recovered.

## Adding and editing a URL

1. Click the **+ Add URL** button on the upper right of the screen. The **Add URL** panel opens on the right of the screen.

- Clicking the expand icon on the upper right of the panel displays the panel in a wider view.
- To cancel the addition, click the close (X) icon on the upper left.
- Clicking the **Go To The Guide** link takes you to the URL settings guide document.

2. Enter the basic information. The items marked with an asterisk (\*) are required.

| Item                    | Required | Description                                                                                                                                                                                                                                                    |
|-------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>             | Required | Used as a unique identification for URL settings. Duplicates are not allowed. If you register with the same name when resetting, statistical data with the same name is considered as data from the same URL.                                                  |
| <b>URL</b>              | Required | Enter the full path of the URL to check. It supports the http/https protocol.                                                                                                                                                                                  |
| <b>Check location</b>   | Required | Select the region of the WhaTap agent that performs the check.<br>Available regions: California, Frankfurt, Jakarta, Mumbai, Seoul, Singapore, Tokyo                                                                                                           |
| <b>Region IP</b>        | -        | The IP address of the agent in the selected region appears. Because the connection is attempted from that IP address to check the URL, check your firewall rules and allow access if necessary. For more information, see <a href="#">Selecting a region</a> . |
| <b>Collection cycle</b> | Required | The interval to collect monitoring data.<br>- Default value: <b>1 Minute</b> (60000 ms); you can select up to 5 minutes in 1-minute increments.                                                                                                                |

3. In the **Event configuration** area, set the alert conditions for each URL. Use the toggle for each condition to specify whether to use it.

- You can enter an **alert message** of up to 50 characters. The message you enter is delivered with the alert content.

| Item          | Description                                                                                  |
|---------------|----------------------------------------------------------------------------------------------|
| <b>Status</b> | Sends an alert based on the response status of the check result. Turn on the toggle and then |

| Item                | Description                                                                                                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | select the target statuses.<br>- You can select multiple items among <b>Client error</b> , <b>Internal server error</b> , and <b>Unknown</b> .                                                                                                                                           |
| <b>Elapsed time</b> | Sends an alert based on the check response time. Turn on the toggle and then enter the threshold in seconds. An alert is sent when a response time exceeding the entered value occurs.<br>You can specify a minimum of 5 seconds, and you can adjust the value with the + and - buttons. |

4. After configuration, click the **Save** button.

- It takes about 1 minute for the added/modified/copied URL to be reflected in the list.

! The registered URL also appears as an alert target in the **Classic** area of the **Event Configuration** screen. For more information, see [the following](#).

## Selecting a region

We can provide additional regions for future connectivity testing. For additional regions, contact us at [support@whatap.io](mailto:support@whatap.io).

\* Check location

Seoul
Mumbai
Tokyo
Singapore
Frankfurt
California
Jakarta

▼ Region IP

Singapore 54.169.168.45

\* For URL inspection, we will attempt to connect to that IP address. Check your firewall rules and allow if necessary.

For **access testing to a closed network site**, you may need to open the firewall to allow calls from the agent. The location IP address appears if **Region IP** is selected. **Firewall open target IP addresses** of each agent are as follows:

**Agent IPs by region when using the Seoul region project**

- AWS-Seoul-Agent - 54.180.11.176
- AWS-Mumbai-Agent - 3.6.243.66
- AWS-Tokyo-Agent - 18.179.189.142
- AWS-Singapore-Agent - 54.169.168.45
- AWS-Frankfurt-Agent - 18.197.22.141
- AWS-California-Agent - 54.215.76.203
- AWS-Jakarta-Agent - 16.78.204.227

**Agent IPs by region when using the Tokyo region project**

- Seoul - 54.180.11.176
- Mumbai - 3.6.243.66
- Tokyo - 52.193.204.10
- Singapore - 18.140.134.146
- Frankfurt - 18.158.138.224
- California - 13.52.131.66
- Jakarta - 16.78.204.227

If **cloudflare** is used, you must allow the **region IPs that are compatible with its firewall rules**.

**ⓘ Use of WhaTap URL Monitoring service**

URL Monitoring is provided as a free service until there is any change of payment policy. You do not need to install separate agents and can use the WhaTap agents and server repository.

# Alert Notifications

This feature delivers notifications to users based on predefined conditions when issues occur in monitored systems or applications. Notifications can be sent through various channels such as email, SMS, messengers, and mobile push notifications.

For example, you can configure alert thresholds for key performance indicators such as CPU usage, memory usage, disk I/O, network traffic, transaction count, error occurrences, and response time latency. When these thresholds are exceeded or abnormal behavior is detected, notifications are automatically sent.

With WhaTap's AI-based alerting, you do not need to define complex conditions manually. The AI learns normal application behavior patterns and automatically detects and notifies anomalies. Additionally, by using tag-count alerts, you can define conditions on values aggregated by specific tags, enabling precise detection even in complex scenarios.

## Key Features

- **Event Configuration:** Configure threshold-based alert conditions and notification channels
- **Event Notification Settings:** Configure notification channels and time schedules per user
- **Event History:** View the history of alert occurrences

## Permissions

To add or configure events, the **Alert Configuration** permission is required.

- **View:** To view metrics event configurations, the **View & Analyze** permission is required.
- **Add/Edit/Delete:** To modify configurations, the **Alert Configuration** permission is required.
- **Receive Notifications:** To receive notifications, the **Alert Receive** permission is required.

### Reference

For more details, see [Member Permissions](#).

# Event Settings (Classic)

Home screen > Select a project >  **Alert** > **Event Configuration**

For a URL monitoring project, when you register a URL, the URL item automatically appears in the **Classic** area of **Event configuration**. An alert target is created for each registered URL without adding an event separately, and the alert conditions for each URL are set on the URL add/edit screen.

## URL alert list

The registered URLs appear as a list, and you can search them by name in the **Search alert** input field at the top of the screen. The columns are as follows.

- **Name:** The unique identification specified when registering the URL
- **URL:** The full path of the URL to check
- **Region:** The check location (region) selected when registering the URL and the IP address of that region
- **Status:** The setting status of the response code based alert. If no alert is set, **Inactive** appears.
- **Elapsed time:** The setting status of the response time based alert. If no alert is set, **Inactive** appears.
- : Takes you to editing the event settings of the URL, where you can modify the status, alert message (up to 50 characters), and elapsed time.

### Setting alert conditions

You can set events by clicking the [ + Add URL ] button on the **URL List** menu. For more information, see the **Getting started** document.

# Event Notification Settings

Home > Select Project >  **Alert** > **Notifications**

## Event Notification Settings per User

 Information about other members in **Event notification settings per-user** can only be viewed by members with the **Member Management** permission. For all other members, required information is masked.

- Mobile device management for bulk event notification receipt settings and access control can be managed in **Account Information**.
- For detailed information about member permissions, refer to the [following document](#).

## Notification Methods

Alerts are available via [Email](#), [SMS](#), [WhatsApp](#), and [Mobile](#).

In the **Event notification settings per-user** section, select the checkbox for the desired notification method to receive alerts. If you clear the checkbox for a notification method, alerts will not be sent through that channel.

 All users except the project super administrator can change only their own notification settings.

### Email Alerts

Email alerts are sent to the email address provided during sign-up.

### SMS Alerts

You can receive alerts via SMS.

ⓘ The SMS alert feature is available only for paid projects.

1. Click your **profile icon** at the top right of the screen, then go to **Manage Accounts**.
2. In **Account Information**, click the [ General Mobile Phone ] button in the **User Phone Number** section.
3. Enter the **phone number** that will receive the verification code.
  - Only **Korean mobile phone numbers** can be registered to receive SMS alerts.
4. Click the [ Save ] button.

#### ✔ Change or delete the registered phone number

- To change the phone number, click the [ Change ] button. SMS verification is required.
- To delete the phone number, click the [ Delete ] button. After deletion, you will no longer receive alerts via SMS.

## WhatsApp Alerts

You can receive alerts via WhatsApp.

ⓘ The WhatsApp alert feature is available only for paid projects.

1. Click your **profile icon** at the top right of the screen and go to **Manage Accounts**.
2. In **Account Information**, click the [ WhatsApp ] button in the **User Phone Number** section.
3. Enter the **phone number** that will receive the verification code.
4. Click the [ Send Verification Code ] button.
5. Enter the 6-digit verification code sent to your WhatsApp application.
  - If you do not receive the verification code within 10 minutes, click the [ Resend Verification Code ] button.
6. Click the [ Verify ] button.

## Mobile Alerts

Users who need to receive mobile alerts must install the WhaTap application on their mobile device and log in.

- Download the WhaTap application – [Android](#)
- Download the WhaTap application – [iOS](#)

## Repeated Alerts (Escalation) Settings

If the alert condition is not resolved after an alert is triggered, you can configure repeated alert intervals based on the time of the initial alert. This setting applies only to **Critical** level alerts.

For example, to repeat alerts immediately (0 minutes), 1 hour later, and 1 day later after the initial alert, enter `0,1H,1D` in the **Repeated Alerts (Escalation)** column.

1. Go to **Alert > Notifications** and navigate to the **Event notification settings per-user** section.
2. Configure the settings in the **Repeated Alerts (Escalation)** field.
  - **M**: minutes, **H**: hours, **D**: days. If the unit is omitted, the value is interpreted as minutes.
  - Enter a number or a number with a unit (**M**, **H**, **D**). If the input format is invalid, an error message is displayed.
3. Click the [ Save ] button. The settings will not be applied unless they are saved.

## Event Reception Tags

When configuring events, you can select **event reception tags** to send alerts to project members and 3rd-party plugins associated with those tags. If no event reception tag is set, alert notifications are sent to **all project members**.

### Add / Edit / Delete Event Reception Tags

 Event reception tags that are **currently applied to an event** cannot be deleted.

1. Go to **Alert > Notifications**.

2. In the user list under the **Event notification settings per-user** section, click + **Add Tag** or +.
3. In the **Event reception tag** window, click + **Create New Tag**.
4. In the **Create Tag** dialog, enter a tag name, select a color, and click the [ Create Tag ] button.
5. To edit or delete a created tag, click the  icon in the tag list.
6. Select the desired tag from the **Tag List** in the **Event reception tag** window to apply it.

## Remove Event Reception Tags

1. Go to **Alert > Notifications** and open the **Event notification settings per-user** section.
2. Click + in the **Event reception tag** field for the user whose event reception tag you want to remove.
3. In the **Event reception tag** window, click the **X** on the tag you want to remove. The tag will be removed.

## Receive Alerts Without Reception Tags

When configuring events, you can select event reception tags to send alerts to project members and 3rd-party plugins associated with those tags.

- To receive alerts **without event reception tags**, enable the **Receive alerts without reception tags** option.
- If you want to receive **only alerts that have event reception tags**, disable this option.

 To stop receiving all alerts, disable this option and make sure that no **Event reception tag** is selected.

## Selecting the event reception mode

In the **Event notification settings per-user** section, you can select the event alert reception scope per member or third-party channel from the following three modes. The reception mode is selected in the **Event reception tags** column of each member or channel row.

| Mode                             | Description                                                                      |
|----------------------------------|----------------------------------------------------------------------------------|
| Receive all alerts               | Receive all alerts regardless of the event reception tags                        |
| Receive alerts for selected tags | Receive only alerts that have the selected event reception tags. Select at least |

| Mode              | Description                                                                    |
|-------------------|--------------------------------------------------------------------------------|
| only              | one tag                                                                        |
| Receive no alerts | Receive no event alerts. The selected tags are preserved without being deleted |

- In the **Receive alerts for selected tags only** mode, select at least one tag to receive alerts in the tag selection area.
- To also receive alerts that have no event reception tag specified, select the **Unclassified** virtual tag in the tag selection area. The **Unclassified** tag can be selected or deselected like a normal tag, but the tag itself cannot be edited or deleted.

ⓘ In the **Receive no alerts** mode, the corresponding member or channel receives no event alerts at all. The selected tags are preserved without being deleted, so if you switch back to the **Receive alerts for selected tags only** mode, you can use the previously selected tag settings as is.

## Select Notification Language

You can choose the language in which you receive alert notifications.

1. Go to **Alert > Notifications**.
2. In the user list under the **Event notification settings per-user** section, click the ► button at the far left of the user whose language you want to configure.
3. Select the **Notification Language**.

## Day and Time-based Notification Settings

You can configure whether a user receives notifications by day of the week and time of day.

1. Go to **Alert > Notifications**.
2. In the user list under the **Event notification settings per-user** section, click the ► button at the far left of the user whose day and time settings you want to configure.

### 3. Select the days and/or enter the time ranges during which you want to receive alerts.

- Settings can be configured separately for each notification method.

## 3rd-party Plugins

You can receive alert notifications through external applications.

- **Supported applications:** Slack, Telegram, Teams, Teams Workflows, Jandi, AlertNow, Webhook, Webhook JSON, Opsgenie, PagerDuty, LINE, ilert

ⓘ Internal messengers that are not included in WhaTap Labs' supported scope can be integrated via standard **Webhook** or **Webhook JSON**.

Table | 3rd-party Plugin List

| Item                         | Description                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Plugin Name                  | Name of the plugin                                                                                                            |
| Auth Key                     | Authentication key                                                                                                            |
| Auth Value                   | Authentication value                                                                                                          |
| Receive Level                | Notification level: Warning, All, or Critical                                                                                 |
| Repeated Alerts (Escalation) | Re-notification interval from the initial alert time if the issue is not resolved<br>- Applies only to <b>Critical</b> alerts |
| Smart Message (AI)           | AI-powered notifications available when adding the Telegram plugin<br>- Supported languages: Korean, English, Japanese        |
| Event Reception Tag          | Whether to receive alerts for specific members or teams in the project                                                        |
| Delete                       | Delete the 3rd-party plugin                                                                                                   |

## Add a 3rd-party Plugin

1. Go to **Alert > Notifications**.
2. In the **3rd-party Plugins** section, click **Add**.
3. In the **Add 3rd-party Plugin** window, select the desired service tab.
4. Follow the instructions for the selected service (see [How to add 3rd-party plugin notifications](#)).
5. Click **Test Receive** to verify the configuration.
6. When finished, click **Add** or **Register**.

### How to Add 3rd-party Plugin Notifications

Slack

- ⓘ In the **Add 3rd-party Plugin** window, click the [ **Add To Slack** ] button on the **Slack** tab to register **WhaTapNotiBot** to your Slack team and channel.

Telegram

- ⓘ
1. In **Telegram**, search for **@WhaTapApmNotiBot**.
  2. Select the bot and click the [ **Start** ] button.
  3. In the chat window, enter the `/license` command followed by the access key of the project for which you want to receive alerts.

Telegram

#### ⓘ Available commands

- `/help` : View the list of commands
- `/license` : Enter the access key of the project to receive alerts

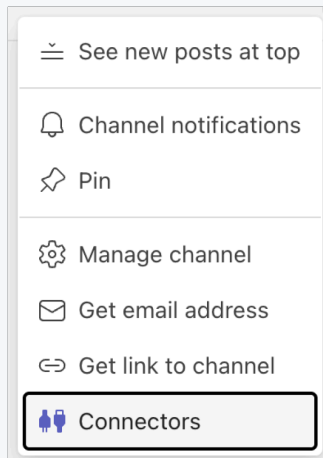


- `/remove` : Enter the project code for which you want to stop receiving alerts
- `/list` : View the list of project codes currently receiving alerts

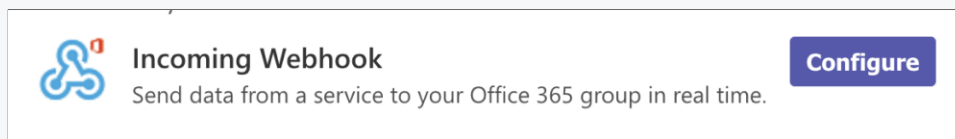
## Teams



1. Go to the **connector** of the channel where you want to receive alerts.



2. Add a **Webhook** and click the [ Configure ] button.



3. Enter a webhook name and click the [ Create ] button.



## Incoming Webhook

[Send feedback](#)

The Incoming Webhook connector enables external services to notify you about activities that you want to track. To use this connector, you'll need to create certain settings on the other service, which needs to support a webhook that's compatible with the [Office 365 connector format](#).

Fields marked with \* are mandatory

To set up an Incoming Webhook, provide a name and select Create. \*

Customize the image to associate with the data from this Incoming Webhook.

Upload Image



Default Image

Create

Cancel

#### 4. Copy the generated **Webhook URL**.

Copy the URL below to save it to the clipboard, then select Save. You'll need this URL when you go to the service that you want to send data to your group.

<https://whatap.webhook.office.com/webhook>



Url is up-to-date.

Done

Remove

#### 5. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams** tab.

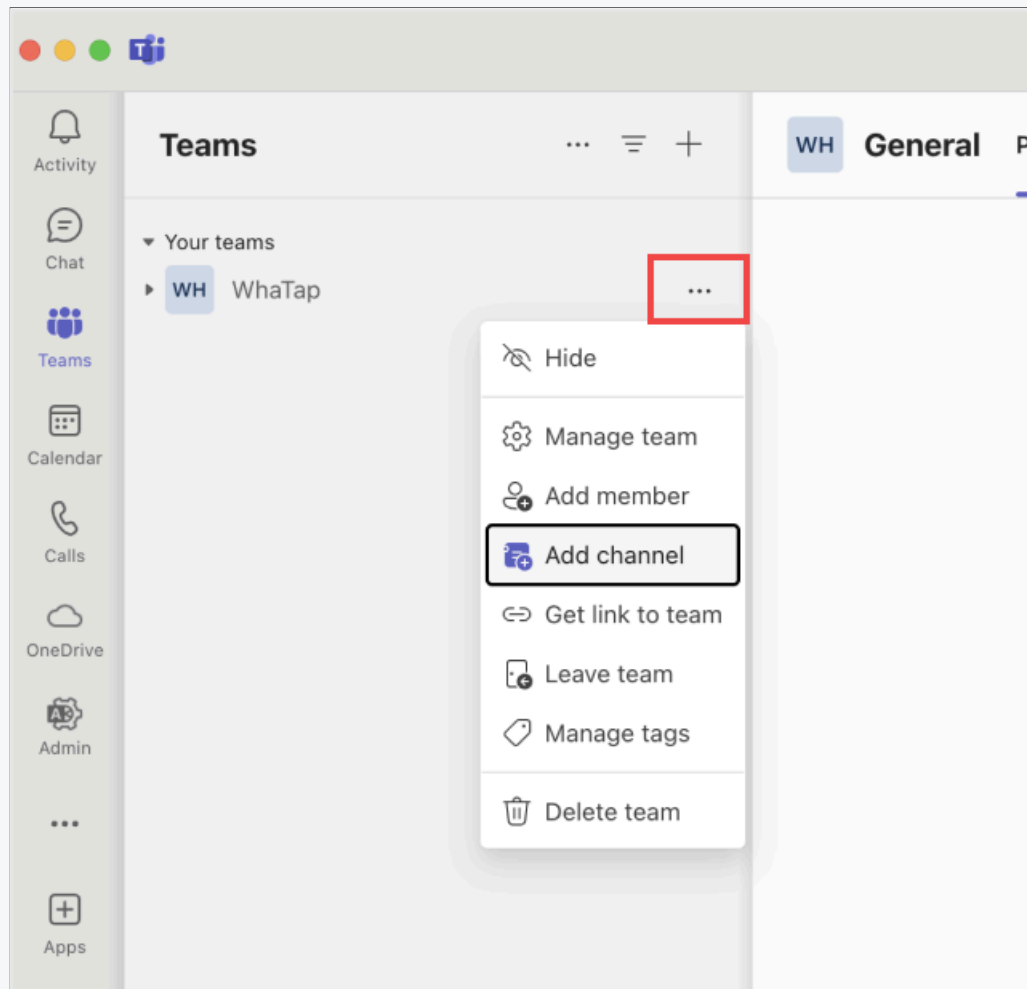
#### 6. Click the [ **Registration** ] button.

Teams Workflows



- ⓘ To use workflows, you need an account that can access **Microsoft Teams** and a **Business plan** subscription.

1. In the **Teams** menu, click **More actions (...)** > **Add channel**.

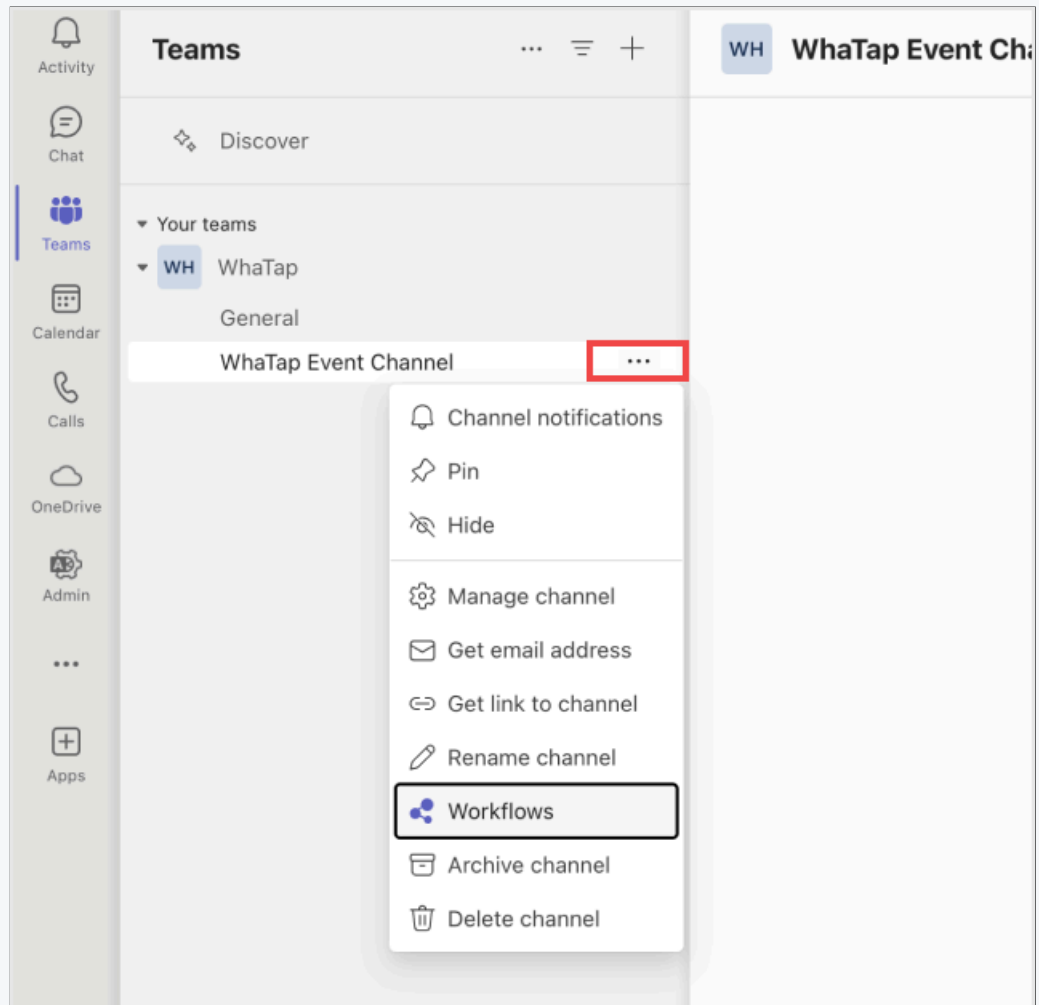


2. In the **Create a channel** window, enter the **Channel name** and **Description**. For **Channel type**, select **Standard**, then click the [ Create ] button.

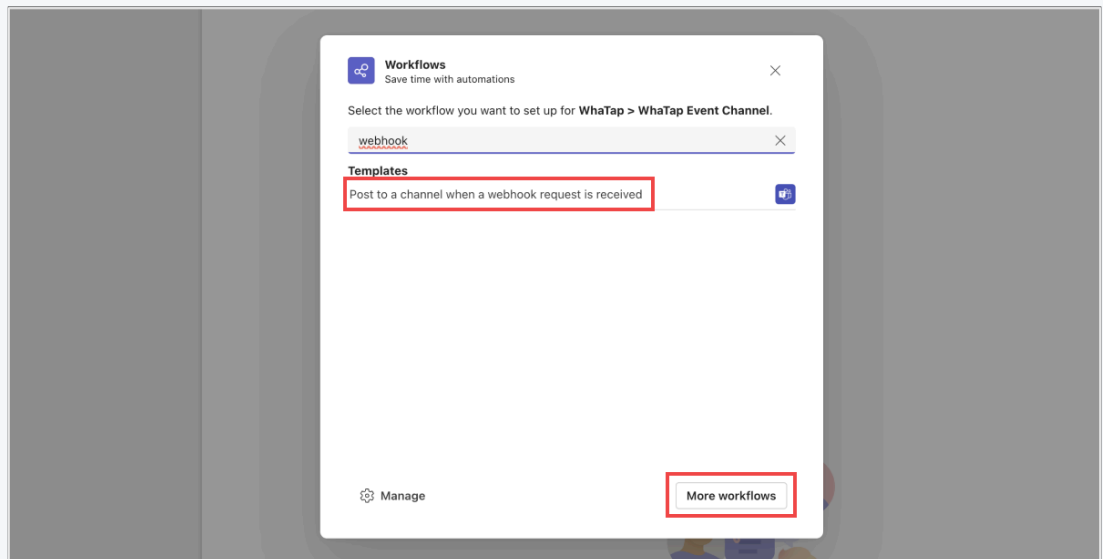


⚠ If you select **Shared** as the channel type, workflows cannot be used. If you select **Private**, workflows can be added but notifications cannot be received.

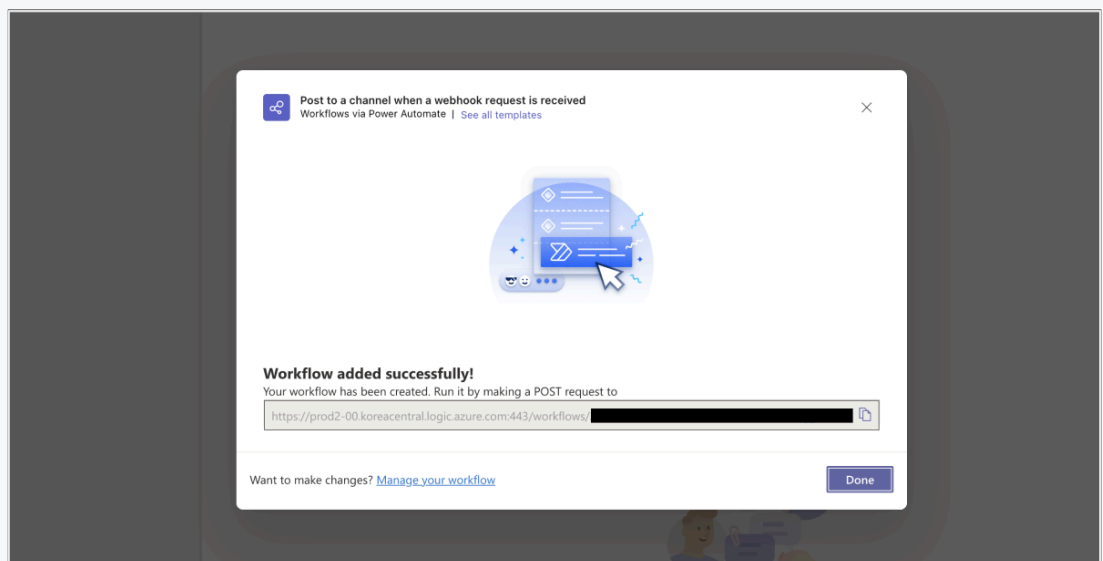
3. Click **More actions (...)** of the created channel, then select **Workflows**.



4. In the **Workflows** dialog, select **Post to a channel when a webhook request is received** from the workflow list, then click the [ Add workflow ] button.



5. Check the **Name** and **Connection** status, then click the [ Next ] button.
6. Review the **Details**, then click the [ Add workflow ] button.
7. The workflow has been added. Copy the generated URL.



8. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Teams Workflows** tab.



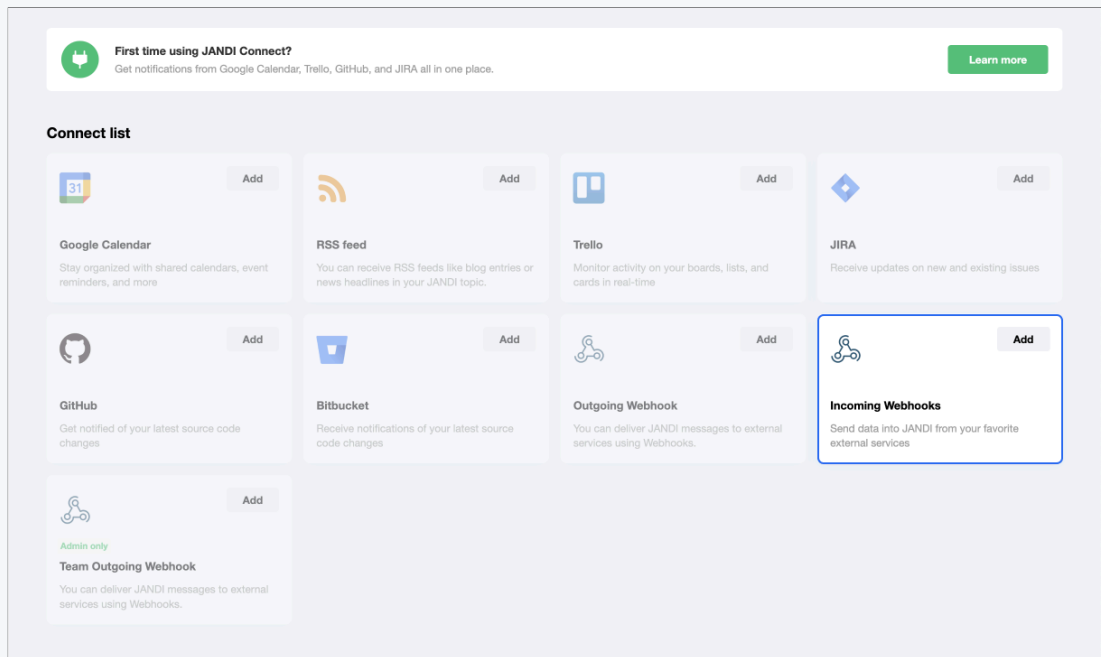
9. Click the [ **Registration** ] button.



Jandi



1. Go to **Jandi Connect settings** in the topic or chat where you want to receive notifications.
2. In the **Connect list**, find **Webhook Receiver (Incoming Webhook)** and click the [ **Connect** ] button.



3. Click the [ **Add Webhook Receiver** ] button.
4. Copy the Webhook URL from the **Register Webhook URL** section.



**Connect settings**

**Profile settings**

Change the name or profile image that appears for messages from this integration



Incoming Webhooks

**Topic / JANDI selection**

Please select a topic or DM to receive integration messages. You change it after saving it.

JANDI

**Webhook URL Registration**

**Webhook URL**

Copy the generated Webhook URL and register with the service.

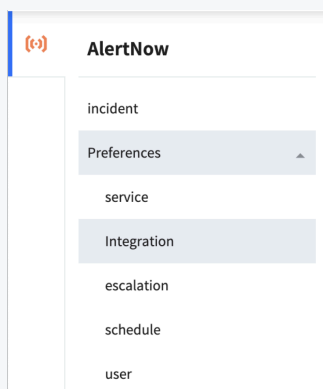
<https://wh.jandi.com/connect-api/webhook/31257583/d3...> Copy

- Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **Jandi** tab.
- Click the [ **Registration** ] button.

## AlertNow



- Access the **AlertNow** service, then go to **Settings > Integration**.



- On the **Integration** screen, click the [ Create Integration ] button.
- From the list of integration types, select **WhaTap**.
- On the **Create Integration** screen, configure the **Name** and **Naming Rules**.

5. Click the [ Confirm ] button to create the integration.
6. Check the list of created integrations and select the newly created integration.

| Integration name | Integration type | Integration key | service name |
|------------------|------------------|-----------------|--------------|
| whatap-test      | WhaTap           |                 | whatap-test  |

7. On the details screen, click the copy icon on the right side of the URL to copy it.

| Basic Information |                                                        |
|-------------------|--------------------------------------------------------|
| Integration type  | WhaTap                                                 |
| Integration key   | fda527a5140                                            |
| URL               | https://alertnowitgr.opsnow.com/integration/whatap/v1/ |
| constructor       | Lisa                                                   |

8. Return to the **Add a third-party plug-in** window in the WhaTap Monitoring service, and enter values for **Channel Name** and **Webhook URL** at the bottom of the **AlertNow** tab.
9. Click the [ **Registration** ] button.

## Webhook



1. Register the Webhook that will receive notifications. The alert `title` and `text` are sent to the registered URL via the **POST** method.

```
{
  "title": "Alert Title",
  "text": "Sample warning message"
}
```

2. Enter values for **Webhook Name** and **Webhook URL**.
3. Click the [ **Registration** ] button.

## Webhook JSON



1. Register the Webhook that will receive notifications. Alert data is sent to the registered URL in **JSON format** via the **POST** method. For substitution variables that can be included in the JSON payload, see **Available Variables**.
  - `${something}` represents a substitution value provided by WhaTap. Refer to **Available Variables** for the full list and descriptions.
  - The event status ( `status` ) is categorized as **event triggered** ( `on` ) or **event recovered** ( `off` ).
  - The `level` is categorized as `None` , `Info` , `Warning` , or `Critical` .

```
{
  "pcode": "${pcode}",
  "projectName": "${projectName}",
  "time": "${time}",
  "oid": "${oid}",
  "oname": "${oname}",
  "title": "${title}",
  "message": "${message}",
  "level": "${level}",
  "status": "${status}",
}
```



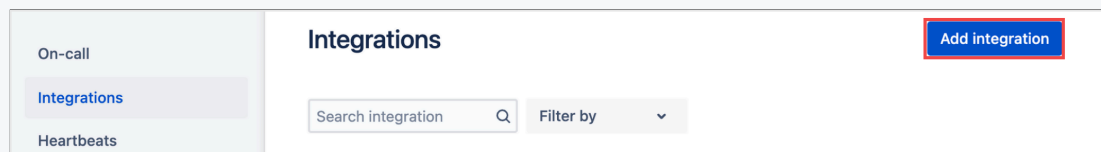
```
"metricName": "${metricName}",
"metricValue": "${metricValue}",
"metricThreshold": "${metricThreshold}",
"uuid": "${uuid}",
"okind": "${okind}",
"onode": "${onode}"
}
```

2. Enter values for the **Webhook Name** and **Webhook URL** fields.
3. To add a header value, click + **Add** in **Add user header value**, then enter the key and value.
4. Click the [ **Registration** ] button.

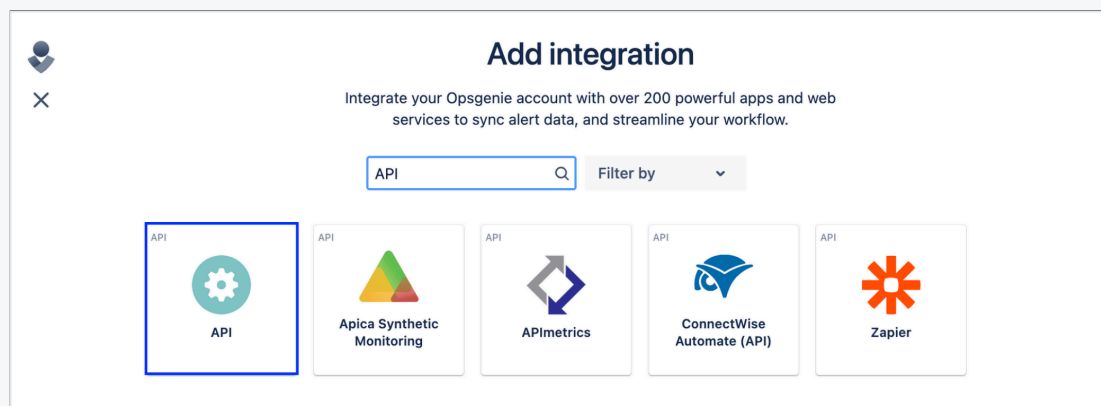
## Opsgenie



1. In the **Teams** menu, select the team that will receive notifications.
2. Go to the **Integration** menu and click the [ Add Integration ] button.



3. In the integration list, search for and select **API**.





4. Set the API name, assign a team, configure the required permissions, and then click the [ Save Integration ] button.

5. Return to the **Add a third-party plug-in** window in the WhaTap monitoring service, and enter values for **Name** and **API Key** at the bottom of the **Opsgenie** tab.
6. Click the [ **Registration** ] button.

## PagerDuty



1. Sign up for a [PagerDuty](#) account and log in.
2. In PagerDuty, go to **Services > Service Directory**, then click the [ + New Service ] button.

PagerDuty

3. Enter the service information (**Name**) and click the [ Next ] button.

PagerDuty

4. Configure the **Escalation Policy**, then click the [ Next ] button.



PagerDuty

5. Configure **Alert Grouping** and **Transient Alerts**, then click the [ Next ] button.

PagerDuty

6. In **Integrations**, select **Event API V2**, then click the [ Create Service ] button.

PagerDuty

7. On the created service page, copy the **Integration Name** and **Integration Key** values.

PagerDuty

8. Return to the **Add a third-party plug-in** screen in the WhaTap monitoring service and enter the **Integration Name** and **Integration Key** values.

9. Click the [ Register ] button.

ⓘ If you do not receive messages or the plugin is not registered, check whether the **Integration Name** or **Integration Key** values are correct.

## LINE



1. Install the LINE app.
2. Scan the QR code below to add the official **WhaTapLabs** channel as a friend.

Add LINE 3rd-party plugin

3. Use the following commands to link your project with LINE and configure notifications.

### Commands

```
/help # Show available commands
/list # View the list of linked projects
/license [ACCESS_KEY] # Add a new project linkage
/remove [PROJECT_CODE] # Remove a linked project
/language [ko|ja|en] # Set notification language (Korean/Japanese/English)
```



- You can find the project access key under **Management > Project Management**.
- Using the `/language` command in LINE applies **only to the current LINE chat room**. It does not change the notification language for other 3rd-party plugins or projects.

#### Examples

```
/license XXXXXXXXXX # Link a project
/language ko # Set language to Korean
/list # Check linked projects
```



- **Project access key:** Available under **Management > Project Management** in the WhaTap project.
- **Language settings:** The `/language` command applies only within the LINE chat room and does not affect other notification channels.

#### ilert



1. In the ilert console, click [+ Create alert source] at the top right of the **Alert sources** page.
2. In the **Integration type** step, enter `WhaTap` in the **Filter integrations** search field at the bottom to search.
3. From the search results, select the **WhaTap** tile and click the [ Next ] button.
4. Enter the alert source name and assign a team, then click the [ Next ] button.
  - You can create a new escalation policy or select an existing one.
5. Select the alert grouping method and click the [ Continue setup ] button.
  - The initially selected **Do not group alerts** option can be changed later.
6. On the next screen, you can configure additional settings such as **alert templates and priorities**. For now, click the [ Finish setup ] button to complete the setup.
7. When the setup is complete, an **API key** or **Webhook URL** will be generated on the completion screen.



8. Copy the generated **Webhook URL** from the **Webhook JSON** tab and paste it into the **Webhook URL** input field below.
9. Click the [ Register ] button.

## Preventing Alert Storms

If a large number of alerts occur within a short period, alert notifications are temporarily paused for a specified duration. For example, if 20 events occur within 5 minutes, alert notifications will be suspended for the next 5 minutes. Once the configured **Pause Duration** has elapsed, the alert-storm prevention feature is automatically released.

1. Go to **Alert > Notifications > the Avoids a large number of alerts** section.
2. Click the toggle button to **Enable** or **Disable** the feature.
  -  **Enabled:** Temporarily pause alerts when an alert storm is detected
  -  **Disabled:** Resume alert notifications
3. Configure the **Detection Time**, **Detection Count**, and **Pause Duration**.
  - If the number of events exceeds the **Detection Count** within the **Detection Time**, alert notifications are paused for the configured **Pause Duration**.



When alerts are blocked due to an alert storm, a notification banner is displayed. To immediately release the alert-storm block, click the **Stop Alert Storm Prevention** button in the banner.

# Event Notification Format

## Common Alert Template

The common template can be applied in most cases. It allows you to receive alerts in a consistent format across various environments.

- Product Type: Application, Database, Kubernetes
- Event Type: Application Alerts, Database Alerts, Metrics Alerts
- Event Channel: SMS, Mobile, 3rd-party plugins, Plugins

## Event Title

Event title format

```
[Level][Platform][ProjectName][ApplicationName][EventTitle]
```

Event title example

```
[Info][JAVA][Application Project][TC-0-1-8081][CRITICAL_HIGH_MEMORY]
```

❗ If ApplicationName is not set, it is omitted from the event title.

- Platform is displayed as one of the following.
  - JAVA
  - NODEJS
  - PYTHON
  - PHP
  - DOTNET
  - GO
  - POSTGRESQL



- ORACLE
- MYSQL
- MSSQL
- BSM\_JAVA
- CLOUDWATCH
- TIBERO
- KUBERNETES
- KUBE\_NS
- URLCHECK
- URLCHECK\_ADMIN
- CUBRID
- ALTIBASE
- CLUSTER
- REDIS
- MONGODB
- VR
- RUM

## Event Message

This section describes the information that can be included in the event message. If `optional` is set to `false`, the item is always included in the message. If `optional` is set to `true`, the item is displayed only when the data is available.

Event message example

```
Project Name : Application Project
Project Code : 3
Agent Name : TC-0-1-8081
Message : RECOVERED: Memory is too high. less than 10%
```

Event Time : 2022-04-12 18:53:24 +0900  
 Event OFF Time : 2022-04-12 18:53:24 +0900  
 Alert Type : APPLICATION\_MEMORY  
 Metric Name : memory  
 Metric Value : 20  
 Metric Threshold : 10  
 Stateful : true

Table | Event Message Components

| En               | Ko                    | Supported Alert Types | Description                                                  |
|------------------|-----------------------|-----------------------|--------------------------------------------------------------|
| Project Name     | Project name          | All                   | -                                                            |
| Project Code     | Project code          | All                   | -                                                            |
| Agent Name       | Agent name            | All (optional)        | oname                                                        |
| Message          | Event message         | All                   | -                                                            |
| Alert Type       | Alert type            | All                   | See the AlertType table below                                |
| Event Time       | Event occurrence time | All                   | In 2022-04-13 10:40:49 +0900, +0900 indicates the GMT offset |
| Event Off Time   | Event recovery time   | All (optional)        | In 2022-04-13 10:40:49 +0900, +0900 indicates the GMT offset |
| Metric Name      | Metric name           | All (optional)        | Name of the metric used to evaluate the event condition      |
| Metric Value     | Metric value          | All (optional)        | Included when the metric value exceeds the threshold         |
| Metric Threshold | Metric threshold      | All                   | Threshold value used to determine the event                  |

| En              | Ko                           | Supported Alert Types    | Description                                                                                               |
|-----------------|------------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------|
|                 |                              | (optional)               | condition                                                                                                 |
| Stateful        | Recovered-event notification | All (optional)           | <code>true</code> if recovered-event notification is enabled; otherwise <code>false</code>                |
| Event Rule      | Event trigger condition      | Metrics alerts           | -                                                                                                         |
| Target Filter   | Event target filter          | Metrics alerts           | Evaluates event conditions only for metrics collected from specific targets                               |
| Repeat Count    | Event repeat count           | Metrics alerts           | The event is triggered when the condition is met the specified number of times within the repeat duration |
| Repeat Duration | Event repeat duration        | Metrics alerts           | Time window used to evaluate the repeat count                                                             |
| Receiver        | Receiver                     | Metrics alerts           | -                                                                                                         |
| Query           | MXQL query                   | Composite metrics alerts | -                                                                                                         |
| Rule            | Event trigger condition      | Composite metrics alerts | -                                                                                                         |
| Query Period    | Query period                 | Composite metrics alerts | -                                                                                                         |
| Query Interval  | Query interval               | Composite                | -                                                                                                         |

| En              | Ko                | Supported Alert Types    | Description                                  |
|-----------------|-------------------|--------------------------|----------------------------------------------|
|                 |                   | metrics alerts           |                                              |
| Silent Time     | Silent time       | Composite metrics alerts | -                                            |
| Query           | URL               | Exception alerts         | URL of the request that caused the exception |
| TXID            | Transaction ID    | Exception alerts         | -                                            |
| Class           | Error class name  | Exception alerts         | -                                            |
| Log Message     | Log message       | Server – file log alerts | -                                            |
| Log File        | Log file path     | Server – file log alerts | -                                            |
| IP              | IP address        | All server alerts        | -                                            |
| CPU             | CPU usage         | All server alerts        | Snapshot at the time the event occurred      |
| CPU_load1       | CPU load (1 min)  | All server alerts        | Snapshot at the time the event occurred      |
| CPU_loadPerCore | CPU load per core | All server               | Snapshot at the time the event occurred      |

| En                                                | Ko                          | Supported Alert Types | Description                             |
|---------------------------------------------------|-----------------------------|-----------------------|-----------------------------------------|
|                                                   |                             | alerts                |                                         |
| Memory                                            | Memory usage                | All server alerts     | Snapshot at the time the event occurred |
| Swap                                              | Swap usage                  | All server alerts     | Snapshot at the time the event occurred |
| Disk Name   Used Percent   Free Size   IO Percent | Disk performance            | All server alerts     | Snapshot at the time the event occurred |
| Name   Bps   Pps                                  | Network traffic performance | All server alerts     | Snapshot at the time the event occurred |
| Message   Time   Name                             | Acknowledgement information | All server alerts     | -                                       |

ⓘ This section displays as much information as possible that can be provided for the event.

- **AlertType** is displayed as one of the following values.

| AlertType                      | Description                          |
|--------------------------------|--------------------------------------|
| APPLICATION_CPU                | Application CPU alert                |
| APPLICATION_MEMORY             | Application memory alert             |
| APPLICATION_DISK               | Application disk alert               |
| APPLICATION_ACTIVE_TRANSACTION | Application active transaction alert |
| APPLICATION_ERROR_TRANSACTION  | Application error transaction alert  |



| AlertType                    | Description                                        |
|------------------------------|----------------------------------------------------|
| APPLICATION_SLOW_TRANSACTION | Application slow transaction (response time) alert |
| METRICS                      | Metrics alert                                      |
| COMPOSITE_METRICS            | Composite metrics alert                            |
| ANOMALY                      | Anomaly detection alert                            |
| LOG_REALTIME                 | Real-time log alert                                |
| COMPOSITE_LOG                | Composite log alert                                |
| SERVER_REBOOT                | Server reboot alert                                |
| SERVER_NO_DATA               | Server no-data alert                               |
| SERVER_PORT                  | Server port alert                                  |
| SERVER_NETWORK_IOPS          | Server network IOPS alert                          |
| SERVER_NETWORK_BPS           | Server network BPS alert                           |
| SERVER_DISK_IO               | Server disk I/O alert                              |
| SERVER_DISK_QUOTA            | Server disk usage alert                            |
| SERVER_DISK_INODE            | Server inode alert                                 |
| SERVER_CPU                   | Server CPU alert                                   |
| SERVER_MEMORY                | Server memory alert                                |
| SERVER_CPU_STEAL             | Server CPU steal alert                             |



| AlertType             | Description                           |
|-----------------------|---------------------------------------|
| SERVER_MEMORY_SWAP    | Server swap memory alert              |
| SERVER_LOG_FILE       | Server log file alert                 |
| SERVER_WINDOW_EVENT   | Server Windows event alert            |
| SERVER_OFF            | Server alert OFF notification         |
| SERVER_ACKNOWLEDGE    | Server acknowledge notification       |
| SERVER_PROCESS_COUNT  | Server process count alert            |
| SERVER_PROCESS_CPU    | Server process CPU alert              |
| SERVER_PROCESS_MEMORY | Server process memory alert           |
| SERVER_PROCESS_OFF    | Server process alert OFF notification |
| AGENT_ACTIVE          | Agent activated alert                 |
| AGENT_INACTIVE        | Agent deactivated alert               |
| AGENT_REACTIVATED     | Agent reactivated alert               |
| URL                   | URL alert                             |
| TOO_MANY_EVENT        | Too many events alert                 |
| CLOUD_WATCH           | CloudWatch alert                      |
| EXCEPTION             | Exception alert                       |

# Event History And Monitoring

Home > Select Project >  **Alert** > **Event History**

**Event History** allows you to view events that have occurred in the project and analyze their detailed information. It supports Elasticsearch DSL queries, enabling you to find events that match specific conditions quickly and accurately.

## Viewing Event History

Click the **event title** in the search results to move to a screen where you can analyze detailed data for the time period when the event occurred. This allows you to comprehensively understand the situation before and after the event.

1. Go to **Alert > Event History**.
2. In the **Event History** screen, use **Time Selection** to set the period for viewing event records.
3. Enter a query in the filter input field and click the [ Magnifying Glass ] button.
  - If no query is entered, all events are displayed.

## Column Settings

You can choose which columns to display or hide.

1. In the **Event History** screen, click the [  Column Settings ] button at the top left.
2. In the **Column Settings** window, select the columns you want to show or hide.
  - You can change the column order in **Displayed Items**.
  - You can search for specific columns using the **Column Name Search** field.

| Column Item | Description            |
|-------------|------------------------|
| Event Name  | The title of the event |

| Column Item         | Description                                                                                                                               |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Message             | The event message or snapshot information                                                                                                 |
| Event Status        | The current status of the event                                                                                                           |
| Agent Name          | The name (Oname) of the agent where the event occurred<br>- Displayed as blank if the event is not associated with a specific agent       |
| Agent Group         | The agent type (OkindName) where the event occurred<br>- Displayed as blank if the event is not associated with a specific agent          |
| Agent Node          | The server (OnodeName) of the agent where the event occurred<br>- Displayed as blank if the event is not associated with a specific agent |
| Event Occurred Time | The time when the event occurred                                                                                                          |
| Event Resolved Time | The time when the event was resolved<br>- Displayed as - for events without a resolved state                                              |

- After completing the settings, click the [ Confirm ] button to apply the column configuration.

## ↓ CSV Download

You can download the query results as a CSV file.

- Go to **Alert > Event History** and click the [ CSV ] button.
- The list of events that match the current filter conditions is saved as a CSV file.

## View Only Events in Progress

You can view only events that are currently in progress.

- Go to **Alert > Event History** and click the [ View Only Events in Progress ] button.
- The following condition is automatically added to the filter query and applied to the search.

Stateful: **true** and Status : **"ON"**

## Event Search

- **Precise Search:** Specify exact conditions to retrieve only the events you need
- **Composite Conditions:** Search across multiple fields at once to handle complex conditions in a single query
- **Flexible Patterns:** Supports various search methods such as wildcards and partial matches
- **High Performance:** Fast searches powered by indexed data

## Searchable Fields

Field names and values are not case sensitive.

- **Field Name Tag:** Event types that support the field
- **Field Type:** The data type of the field
  - **#:** Number
  - **T:** String
  - **🔘:** Boolean
  - **📅:** Date

## Event Information Fields

| Field Name | Type   | Description            | Example Value                            |
|------------|--------|------------------------|------------------------------------------|
| Title      | String | Event title            | "Database Connection Error"              |
| OffTitle   | String | Event recovery title   | "RECOVERED: Database Connection Error"   |
| Message    | String | Event message          | "Connection timeout occurred"            |
| OffMessage | String | Event recovery message | "RECOVERED: Connection timeout occurred" |

| Field Name      | Type   | Description                         | Example Value                                       |
|-----------------|--------|-------------------------------------|-----------------------------------------------------|
| Level           | String | Current event level                 | Critical, Warning, Info                             |
| OriginLevel     | String | Original event level                | Critical, Warning, Info                             |
| Status          | String | Event status                        | ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED |
| ActCount        | Number | Number of occurrences               | 2                                                   |
| MetricName      | String | Metric name                         | "memory"                                            |
| MetricValue     | String | Metric value                        | "85.5"                                              |
| OffValue        | String | Recovery value                      | "72.8"                                              |
| MetricThreshold | String | Threshold value                     | "80"                                                |
| alertType       | String | Event type                          | "BASIC", "METRICS", "TRANSACTION", etc.             |
| alertId         | String | Unique identifier of the event rule | "zf3uojer0fv4v7"                                    |

## Type-specific Supported Fields

ⓘ These fields are supported only for specific event types. If the event type does not match, the value may be empty.

| Field Name | Type   | Event Type     | Description        | Example Value |
|------------|--------|----------------|--------------------|---------------|
| eventRule  | String | Basic, Metrics | Event trigger rule | "memory ≥ 80" |
| field      | String | Real-          | Log search         | "content"     |

| Field Name  | Type   | Event Type    | Description      | Example Value                                                                                                                                                                                              |
|-------------|--------|---------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             |        | time Log      | key              |                                                                                                                                                                                                            |
| keyword     | String | Real-time Log | Log search value | "Error"                                                                                                                                                                                                    |
| logCategory | String | Real-time Log | Log category     | "AppLog"                                                                                                                                                                                                   |
| logContent  | String | Real-time Log | Log content      | "00:00000:00009:2025/04/06 23:03:52.55 server Error: 1601, Severity: 17, State: 3\n00:00000:00009:2025/04/06 23:03:52.55 server There are not enough 'user connections' available to start a new process." |

## Target Fields

| Field Name | Type   | Description                  | Example Value       |
|------------|--------|------------------------------|---------------------|
| Oid        | Number | Agent unique identifier      | -98765432           |
| Oname      | String | Agent name                   | "web-server-01"     |
| Okind      | Number | Agent type unique identifier | 867318026           |
| OkindName  | String | Agent type name              | "web-server"        |
| Onode      | Number | Agent node unique identifier | 334634079           |
| OnodeName  | String | Agent node name              | "production-node-1" |

## Unique Event Fields

| Field Name | Type   | Description                    | Example Value             |
|------------|--------|--------------------------------|---------------------------|
| Id         | Number | Unique identifier of the event | 5768121                   |
| UUID       | String | Unique event identifier        | "550e8400-e29b-41d4-a716" |

## State / Flag Fields

| Field Name  | Type    | Description                      | Example Value |
|-------------|---------|----------------------------------|---------------|
| Stateful    | Boolean | Whether the event is state based | true, false   |
| Disabled    | Boolean | Whether the event is disabled    | true, false   |
| Escalation  | Boolean | Whether escalation is applied    | true, false   |
| SystemEvent | Boolean | Whether it is a system event     | true, false   |

## Query Syntax by Search Type

ⓘ For the basic search syntax, refer to the [WhaTap log search query syntax](#) documentation.

### 1. Keyword Search

Events that contain the string "Database Connection"

```
title: "Database Connection"
```

### 2. Multiple Value Search

Retrieves events that include any one of the specified values.

```
title: Database Connection
```

Events whose current event level is Info or Warning

```
level: info warning
```

### 3. Pattern Search

You can search using patterns with wildcards.

Find events that occurred on specific agents using a name pattern

```
oname: web-*-prod
```

タイトルが Connection で終わるイベントを検索

```
title: *Connection
```

### 4. Complex Condition Search

You can combine multiple conditions to perform precise searches.

Events with a Critical level and a title containing Database

```
level: critical and title: Database
```

Warning or Critical events from a specific agent

```
oname: web-server-01 and level: Warning Critical
```

### 5. OR Condition Search

Retrieves events that satisfy **at least one** of the specified conditions.

Events where the title or message contains a specific keyword

```
title: Connection or message: Connection
```

## 6. Exclusion Conditions

You can exclude specific conditions from the search.

All events except those with an Info level

```
not level: info
```

# Real-time Notifications

The **Alert status** feature displays pop-up notifications when events configured in **Event Configuration** occur. You can receive alerts immediately when an event is triggered, allowing you to quickly recognize issues and respond. You can also review notifications that have already occurred or were missed, helping you understand and resolve situations where real-time response was difficult.

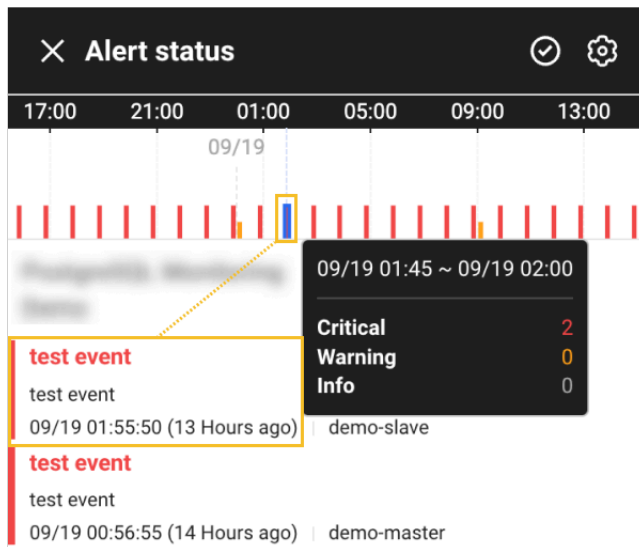
## Viewing Real-time Notifications

Real-time notifications appear as pop-ups in the upper-right corner of the screen. You can check the time, title, and message of each notification.

- To close an individual notification, click the  button in the upper-right corner of the message.
- To close all pop-up notifications displayed on the screen, click **Close All Notifications**.

## Viewing Notification History

1. Click the  icon at the top of the screen after selecting a project.
2. The **Alert status** window appears.
  - You can view up to 100 notifications from the past 24 hours for the current project.
  - Selecting an individual event item navigates you to the related menu.
  - In the time-based chart within the **Alert status** window, selecting a specific time range takes you to the corresponding event items.



- To view the full notification history, click **View All Notification History**. This navigates to **Alert > Event History**.

ⓘ If the **Alert status** list is empty, the **View All Notification History** button is displayed. Disable the **Receive notifications without reception tags** option.

## Resolving Events in Bulk

You can resolve all ongoing events at once from the **Alert status** list. The bulk resolution process may take approximately 30 seconds to 1 minute to complete.

- When using the **Add Acknowledge** feature, a large number of recovery (resolved) notifications may be generated for currently ongoing events.
- Even after using the **Add Acknowledge** feature, events may occur again if the event rules remain enabled and the data still exceeds the threshold.
- Recovery notifications can be disabled by editing the event in **Alert > Event Configuration**. Disable **Send additional notification when the event is resolved** or **Recovered notification**.

**How to use:**

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Real-time Notifications** window appears, click the  icon in the upper-right corner.
3. When the message `Resolve all ongoing events in the real-time notification list.` appears, click the **Resolve** button.

## Configuring Real-time Notifications

1. Click the  icon at the top of the screen after selecting a project.
2. When the **Alert status** window appears, click the  icon in the upper-right corner.
3. Configure each option in the real-time notification settings window.
  - **Popup notifications:** Displays notifications as pop-ups even when the **Alert status** window is closed.
  - **Show resolved events:** Allows resolved events to be displayed in the **Alert status** list.
  - **Preview notification sound:** Lets you preview browser notification sounds. Click the  button next to **Critical** or **Warning**. If you cannot hear the sound, check your browser settings.

# System Events

WhaTap Monitoring provides common system events that are automatically detected and generated across the platform. This document explains the types of events generated by the system, their trigger conditions, and recommended response actions.

## **EVENT\_BLOCKED\_BY\_SYSTEM**

If an excessive number of events occurs within a short period of time in a project, the WhaTap system detects this situation and blocks further events. When events are blocked, the system delivers the following message to the user. If you encounter this event, review and adjust your event configuration settings.

 **Critical**



**Event Message**

**Excessive events detected, event blocked for stability. name: server agent**

|                     |                                |
|---------------------|--------------------------------|
| <b>Project No</b>   | 8                              |
| <b>Project Name</b> | new server                     |
| <b>Target</b>       | server agent                   |
| <b>Event Title</b>  | EVENT_BLOCKED_BY_SYSTEM        |
| <b>Event Time</b>   | (GMT+0900) 2024-11-18 17:58:58 |

**Log In to WhaTap**

Events are blocked as a result of excessive events in the server agent of new server project. If no events occur in server agent for a period of time, it is automatically unblocked.

## Blocking Criteria

Events are blocked based on the following criteria:

- 1. Agent-level blocking**

If **10 events** occur within **1 minute** from a single agent, all subsequent events from that agent are blocked.

- 2. Project-wide blocking triggered by multiple agents**

If **3 or more agents** are blocked within **1 minute** according to condition 1, events from the entire project are blocked.

### 3. Project-level blocking

If **100 events** occur within **1 minute** in a single project, all events from that project are blocked.

## How to Release the Block

When events are blocked by the system, no events must occur from the affected agent or project for **1 minute**.

- Disable all configured events from **Alert > Event Configuration**. **Review your event settings and adjust thresholds to prevent excessive event generation.**
- Before configuring events, use the **Simulation** feature to estimate how many events may occur.

# HTTP Status Code Types

You can check for web service failures through the WhaTap URL monitoring. A warning alert is sent if the status code returned from the web service is 4xx or 5xx. These status codes are called **HTTP Status Code**. A typical example is "404 Not Found."

The status code consists of three digits, with the first digit being 1 through 5. If the first digit is 4 or 5, this is abnormal and the site administrator must be aware of it immediately.

- **1xx (INFO)**: The request has been received and the process is still in progress.
- **2xx (Success)**: The request was successfully received, recognized, and processed.
- **3xx (Redirect)**: Additional actions are required to complete the request.
- **4xx (Client Error)**: The syntax of the request is wrong or the request cannot be processed.
- **5xx (Server Error)**: The server failed to process a valid request.

❗ For more information about **HTTP status codes**, see the following link:

- [W3 RFC 2616 status code summary](#)
- [Mozilla Foundation status code summary](#)
- [IETF's RFC 2616](#)

## 1XX: Information responses

If the status code begins with "1," it indicates that the server has received requests and the clients connected to the server must perform tasks. The code is not supported in HTTP 1.0.

- **100 Continue**

Response code that indicates the processing status. This indicates that it informs that you can ignore the request if there is no issue with the current progress and the clients are still requesting or they have already completed the request.

- **101 Switching Protocol**

The 101 response code is sent in response to the upgrade request header sent by a client. This code indicates that the server is to accept the client's upgrade request and change the protocol. It is mainly used when switching the WebSocket protocol.

- **102 Processing(WebDAV)**

This response code indicates that the server has received the request and is processing it but cannot provide the final response yet.

## 2XX: Successful responses

- **200 OK**

The request has been processed successfully. Information is returned in response to the request.

- **201 Created**

The request was processed successfully and a new resource was created as a result. This response is primarily used after a POST request or some PUT requests.

- **202 Accepted**

The request was received but has not been processed yet. This response does not specify that request processing may occur asynchronously and the results may be delivered via HTTP responses. It is used when another process is processing requests, or when the server is processing the request as a batch process.

- **203 Non-Authoritative Information**

This indicates that the returned meta data does not belong to the origin server and has been collected from local or third-party copies. In this case, a **200 OK** response must come first.

- **204 No Content**

The request was processed successfully but there is no content to return. However, the header may be valid, and the user agent may update the cached headers with the latest information.

- **205 Reset Content**

This indicates that after the request has been completed, the user agent must reset the document view that sent the request.

- **206 Partial Content** It is used when a client requests partial content via the range header. The web server

sends the portion of the data specified in the Range header along with the '206 Partial Content' response code.

- **207 Multi-Status**

Multi-state responses are used in the situation that includes multiple status codes from multiple resources. It is mainly used in WebDAV (Web Distributed Authoring and Visioning).

- **208 Already Reported**

Prostat (a portmanteau of Property and Status) is a response property that is used to avoid repeatedly listing multiple internal members bound to the same collection. It is used in the Web Distributed Authoring and Visioning (WebDAV).

- **226 IM Used (HTTP Delta encoding)**

It indicates that the server has processed a GET request and the response contains the current instance to which one or more instance operations have been applied.

## 3XX: Redirection messages

- **300 Multiple Choice**

This indicates that more than one response is possible to a request. The user agent or user must select one of them. There is no standardized response selection method.

- **301 Moved Permanently**

This indicates that the URI of the requested resource has been permanently changed. A new URI may be provided in the response.

- **302 Found**

This indicates that the URI of the requested resource has been temporarily changed. A new URI may be provided later, and the client must use the same URI in upcoming requests.

- **303 See Other**

The server instructs the client to obtain the requested resources via the GET request from different URIs.

- **304 Not Modified**

It is used for caching purposes. It notifies the client that the response has not been modified, and the client

can continue to use the cached version.

- **305 Use Proxy**

It is defined in the previous HTTP specification, and it indicates that the requested response must be connected through the proxy. Due to security concerns about in-band settings for proxies, its use is gradually decreasing.

- **306 Unused**

Currently, it is not used and reserved for future uses. It is used in the versions prior to HTTP 1.1.

- **307 Temporary Redirect**

This indicates that the resources requested by the client are on a different URI and must be requested using the same method as in the previous request. Similar to **302 Found**, but **307 Temporary Redirect** requires that you must not change the used HTTP method. If the first request is a POST, the second request must also be a POST.

- **308 Permanent Redirect**

This indicates that the resources are permanently at a different URI. Similar to **301 Moved Permanently**, but in **308 Permanent Redirect**, the used HTTP method must not be changed. If the first request is a POST, the second request must also be a POST.

## 4XX: Client error responses

- **400 Bad Request**

This response indicates that the request's syntax is wrong and the server cannot detect it.

- **401 Unauthorized**

Although the HTTP standard clearly specifies "unauthorized," in reality this response indicates "unauthenticated." The client must be authenticated to receive the requested response.

- **402 Payment Required**

This response code is reserved for future uses. It is intended for use in digital payment systems but is not currently in use.

- **403 Forbidden**

The client does not have permission to access the content. The server sends an appropriate response to reject the request. The difference with **401 Unauthorized** is that the server recognizes the client.

- **404 Not Found**

The server could not find the requested resource. In browsers, this indicates an unknown URL. The API may indicate that the endpoint is appropriate but the resource does not exist. The server may send this response instead of 403 to hide resources from unauthenticated clients. This response code is the most widely known on the web.

- **405 Method Not Allowed**

The requested method is known to the server, but its use is prohibited. For example, deleting resources from a specific API may be prohibited. Required methods (GET and HEAD) cannot be removed and cannot return this error code.

- **406 Not Acceptable**

The server sends this response when it cannot find content that meets the specifications specified by the user agent.

- **407 Proxy Authentication Required**

This response is similar to **401 Unauthorized**, but it indicates that proxy authentication is required.

- **408 Request Timeout**

The server sends this response when it attempts to terminate an idle connection. Some browsers such as Chrome, Firefox 27+, and IE 9, can use the HTTP pre-connection mechanism to receive this response. Some servers may be disconnected without sending this message.

- **409 Conflict**

This response is sent when a request conflicts with the current status of the server.

- **410 Gone**

This response is sent when the requested content has been permanently deleted from the server and is no longer available. The client must remove its cache and link to resources.

- **411 Length Required**

The server rejects the requests that do not have the Content-Length header field defined.

- **412 Precondition Failed**

This response is sent when the preconditions in the client's headers do not match those of the server.

- **413 Payload Too Large**

The requested entities exceeded the limit defined by the server. The server can close the connection or respond it with including the Retry-After header field.

- **414 URI Too Long**

The length of the URI requested by the client exceeds the limit that the server can handle.

- **415 Unsupported Media Type**

The format of the requested media is not supported by the server, so the server rejects the request.

- **416 Requested Range Not Satisfiable**

The range requested in the Range header field cannot be satisfied. The requested range might exceed the data size of the target URI.

- **417 Expectation Failed**

This response is sent when the requirements in the Expect request header fields are not met from the server.

- **418 I'm a teapot**

The server refuses to brew coffee in a teapot. It is one of the HTCPCP protocol status codes.

- **421 Misdirected Request**

A request directed to the server cannot generate a response. This is sent when the server is unable to generate a response by configuring the scheme and roles linked to the request URI.

- **422 Unprocessable Entity (WebDAV)**

There is no problem with the request but it cannot comply with the request due to a syntax error.

- **423 Locked (WebDAV)**

The requested resource is locked and cannot be accessed.

- **424 Failed Dependency (WebDAV)**

The current request failed because of the failure of the previous request.

- **426 Upgrade Required**

The server does not use the current protocol to process requests but may process requests if the client is

upgraded to handle a different protocol. The server responds with including the required protocol in the Upgrade header.

- **428 Precondition Required**

In the server, the request must be conditional. This is to prevent the "lost updates" where the status of the server is changed by a third party while the client GETs resources, modifies them, and returns them to the server with PUT.

- **429 Too Many Requests**

It indicates that the user sent too many requests within the specified time period. ("rate limiting")

- **431 Request Header Fields Too Large**

The requested header field is too large for the server to process the request. It needs to shorten the request and retry.

- **451 Unavailable For Legal Reasons**

It indicates that the requested resources are illegal, such as web pages that have been censored by the government.

## 5XX: Server error responses

- **500 Internal Server Error**

This indicates that there is a problem with the server, but the exact problem cannot be clearly identified.

- **501 Not Implemented**

It indicates that the server does not support the functionality for the request.

- **502 Bad Gateway**

It indicates that the server received an invalid response from the gateway. This occurs when the server on the Internet receives an invalid response from another server.

- **503 Service Unavailable**

It indicates that the server is not ready to handle the request. This usually happens when the server is under maintenance or is overloaded. This response must provide a user-friendly page and if possible, it must include an estimated time for service recovery in the Retry-After header.

- **504 Gateway Timeout**

This indicates that the server acting as the gateway did not receive timely responses. It is mainly caused by network issues between servers.

- **505 HTTP Version Not Supported**

It indicates that the client requested an HTTP version that is not supported by the server. It is assumed that most web browsers support the HTTP 1.x. Using the latest version of the protocol is recommended for security and performance reasons.

- **506 Variant Also Negotiates**

It occurs when an internal configuration error occurs in the server, which leads to a circular reference by the transparent content negotiation for a request.

- **507 Insufficient Storage**

This occurs when the server does not have enough space to store requests. It mainly occurs in WebDAV.

- **508 Loop Detected (WebDAV)**

It occurs when the server detects an infinite loop while processing requests.

- **510 Not Extended**

This occurs when the server needs additional expansion to process the request.

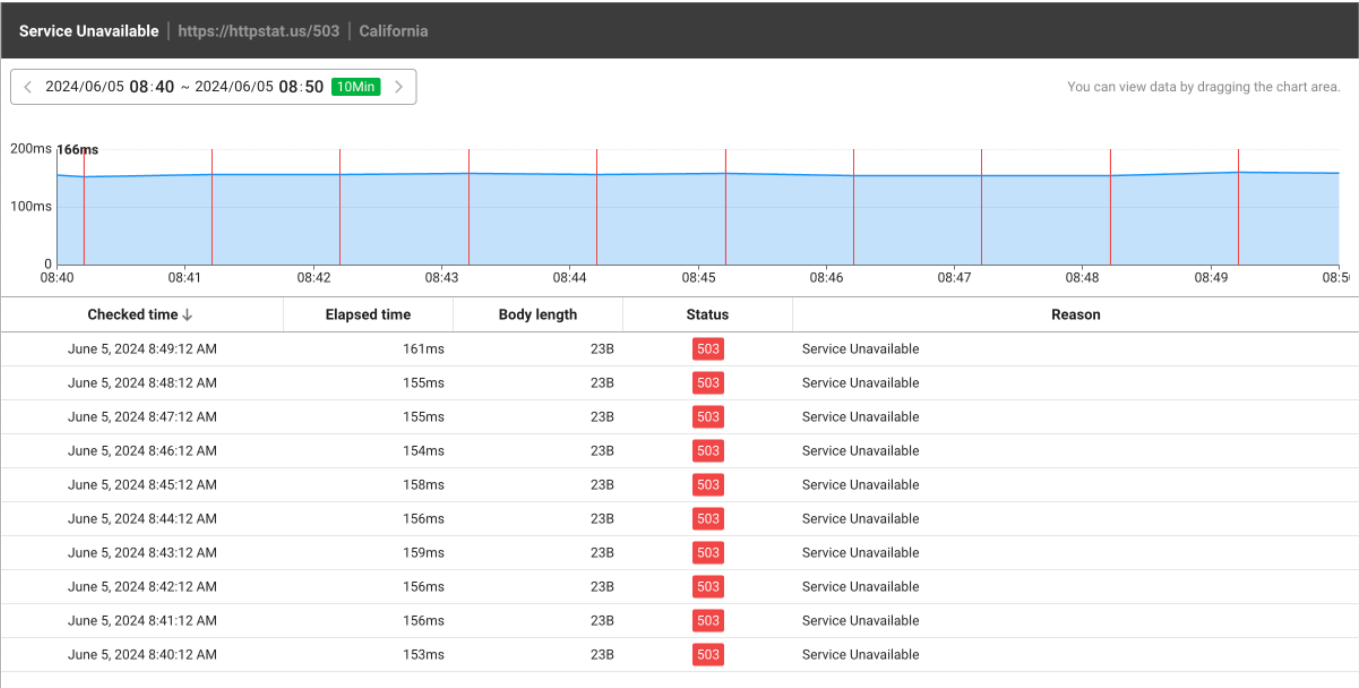
- **511 Network Authentication Required**

This indicates that the client needs authentication to access the network.

# Error Type

It guides you through the types of errors that can occur when applying URL Monitoring and how to set the types.

If you drag the chart area that appears on the URL Monitoring screen, the result data obtained upon calling the URL appears at the bottom of the screen during that time. It guides you on how to take action against the message displayed in the cause details.



## Invalid URL

This message is generated when an incorrect URL is specified.

## Unknown Host or URL

This message is generated when the host or URL cannot be found. Make sure that you entered the protocol

correctly or entered the correct URL format and host address.

## Connect Time Out

This message appears when the time out occurs upon connection to an incorrect URL and connection cannot be made. This message appears when an attempt to connect to the server fails within the maximum time of 5 seconds.

## Read Time Out

This message appears when a read operation is not ended within the specified time. It appears when there is no response within the maximum time of 10 seconds while receiving data from the server.

## Unexpected end of file from server

This message appears when the encoding values of the agent and server are different, or the encoding methods for parameters are different.

## Connection Refused

This message appears when the connection to call the URL is blocked. If calling from the agent is impossible, it is required to check the URL or the server's firewall.

- First check whether access has any problem by entering the URL in the web browser. Errors may occur during data input.
- Check the firewall and IP blocking history against frequent calls and explicitly allow access to the IP of the monitoring agent.

## No route to host

This message appears when there is no path to reach the destination. It appears when the data cannot be found from the DNS and the URL is missing or not updated. Check that you have entered the following items correctly.

- Port assignment
- Protocol of the input URL

e.g. in case of typing 'htts:/' and 'https:/' incorrectly