PLAYBOOKS HOW-TO

Incident Resolution

Whether you're part of a team managing SaaS products or a high-security digital workspace, sometimes Things Go Wrong and must be addressed with extreme care, professionalism, and predictability. For outages, data breaches, vulnerabilities and more, you and your team are juggling a variety of tools, processes, and rigid incident management systems. When the on-call pager goes off at 3 am almost no one has the ability to remember every step needed to kick off all the response workflows.

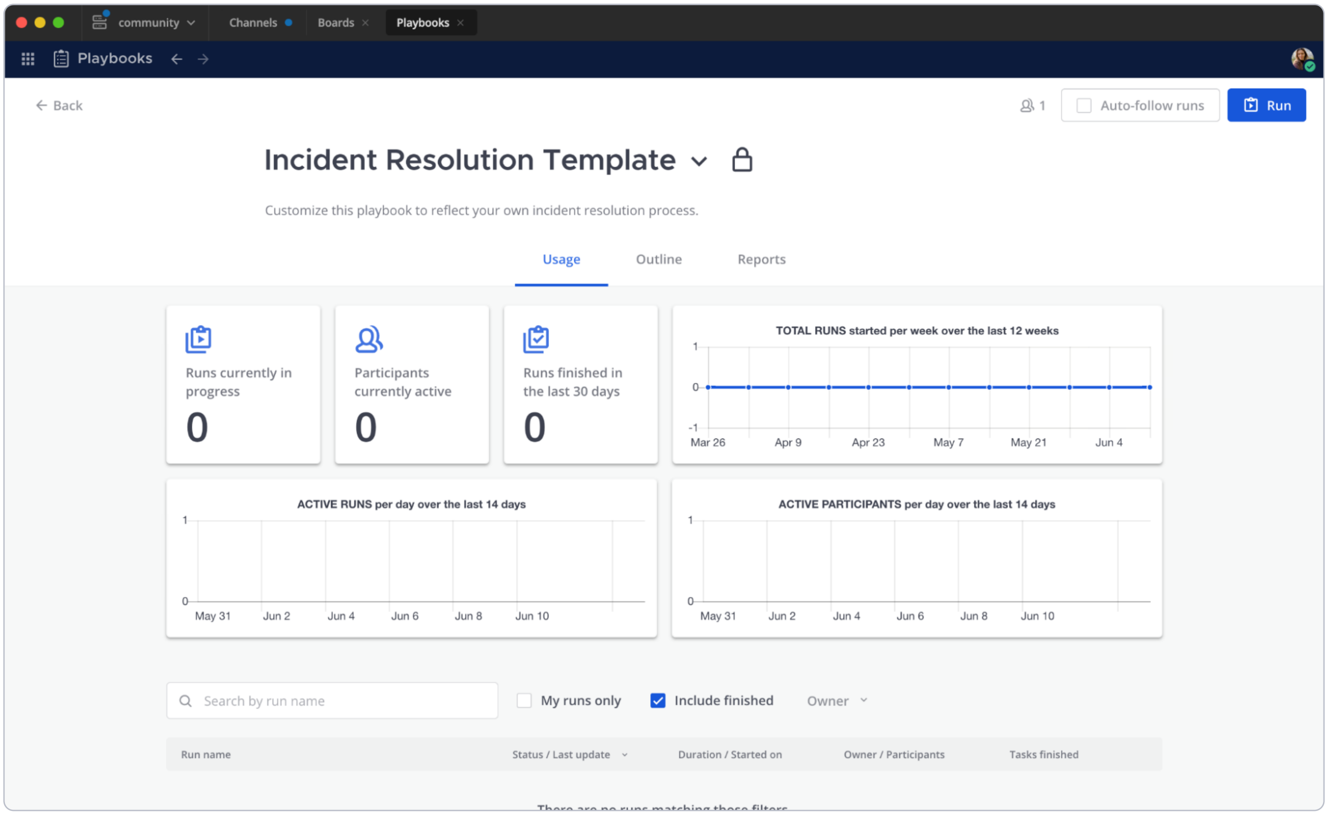
By offering reusable runbooks and standardized templates in the same platform as messaging channels, Mattermost gives teams a shared space to coordinate responses, get full context view of the situation, and ensure that all critical processes are followed for every incident.

In this guide, we'll show you how to customize a pre-built Mattermost Playbooks template to create your own reusable process playbook. Then, any time an incident occurs, you'll click `run` on your playbook to kick off that process and have all the steps, links, and tools on hand right alongside team conversations. Every incident is a learning experience from which you'll collect insights, metrics, and retrospectives, building solid documentation and a collaborative culture to support the entire team.

What you'll need

- ✓ An understanding of your current incident resolution or response process. You may have an established and well-documented process, no process at all, or something in between. Wherever you are, we'll show you some options and structures you can build on.
- ✓ A Mattermost server. You can test this out on our open source community server, your own server, or start a free cloud trial.
- ✓ The "Incident Resolution" Playbooks template from Mattermost, which can be found inside Mattermost at the bottom of this screen `https://{hostname}.mattermost.com/playbooks/playbooks` or in the marketplace as an importable json file.

About the Incident Resolution template



Incident Resolution Template

Customize this playbook to reflect your own incident resolution process.

Runs currently in progress 0

Participants currently active 0

Runs finished in the last 30 days 0

□ My runs only ☑ Include finished

Run name | Status / Last update | Duration / Started on | Owner / Participants | Tasks finished

There are no runs matching those filters

All Playbooks in Mattermost have the same set of features, but how you fill out the details varies depending on the process you are building a playbook for. For Incident Resolution, the playbook template includes a robust retrospective template as well as some small automations and checklist suggestions.

Your team will especially want to modify tasks, templates, automations, and metrics in order to use this *template* to create a custom *playbook* from which you will create regular *runs*:

Template: a simple and generic starting point

↳ **Playbook**: the source copy of your repeatable process

↳ **Run**: a single instance of your repeatable process

The Incident Resolution template is designed to help a team follow the same set of steps any time a particular kind of incident occurs. You might have several playbooks, such as “Cloud incident response,” “Community incident response,” or “Support incident.” The checklists include these sections:

Set up for Triage – Kick off a secure bridge call in Mattermost with a one click slash command, fill out the run summary, and line up the response team.

Investigate cause – Make a list of possible causes and eliminate them.

Resolution – Ensure that all teams have the same language to communicate about the situation with customers, the public, and stakeholders.

Retrospective – Add context from Channels messages to the run timeline, plan follow up actions, and export response data for compliance review.

How to use and modify the Incident Resolution template

In Mattermost, navigate to Playbooks using the global menu in the upper left corner. Select the Playbooks button next to Runs. Scroll down if needed to bring a section titled “Do more with Playbooks” into view. Select the “Incident Resolution” template.

OR, to download and install any PB template from github.com/mattermost/mattermost-product-templates (or a friend) you may copy, export and import playbooks as .json files.

Once you are looking at the template in Mattermost, you’ll be able to start modifying it to match your own process. Start with the title! Here are some other areas you might consider making changes:

Update the playbook description so teams know when to use the playbook and who should use the playbook.

Update the run summary template to give the team a framework to fill in with incident information. This may develop and be updated further during the run so that anyone can glance at the playbook to see what’s happening.

Set a cadence, destinations, and template for regular status updates. You may want to send updates to other channels in Mattermost, or to outgoing webhooks. These can be changed during a run, in case the situation evolves.

Update the checklists. Add and rename sections, add checklist items, and especially add links and slash commands to really speed response times. You may have custom commands for your favorite integrations, such as Opsgenie, PagerDuty, Jira service desk, or Servicenow.

Define your key metrics in the retrospective section – Incidents can have a lot of associated costs and considerations. This is where you can measure things like "mean time to repair/resolve," "cost to customer," or "customers affected" and observe how that metric changes over the course of multiple runs.

Set up a retrospective template. This should be a standardized set of questions for the team to fill in after a run, so that anyone can skim all retros over time and see trends. Our internal template includes sections such as:

`Impact` This section describes what was the impact of the incident

`Root Causes` This section describes the root cause of the incident

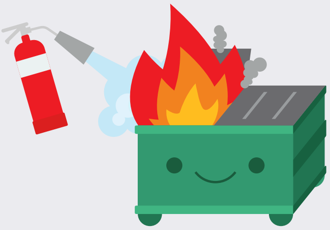
`Trigger` This section describes the trigger point of the incident eg. alert or other etc.

`Resolution` This section describes the way we resolved the incident

`Detection` This section describes how we detected the root cause

`Action Items` This section describes the action items, the type of it, the owner, the state, bug ticket if it exists

Set actions to automatically add the same people or teams for every run of your playbook, send an outgoing webhook when a run starts, or automatically assign the on-call SRE as run owner. Additionally, admins can set Channel Actions to trigger a playbook run in a specific channel using keywords and even create incoming webhooks to automatically trigger a playbook run based on an external monitoring system, for instance.



How to Make Your Incident Response Plan with Mattermost

To go deeper and use a local Docker environment to test out more features and integrations, check out this post from Mattermost developer advocate Andrew Zigler.

Learn more about using Playbooks

As you use your incident response playbook for more and more runs over time you'll start to gather a lot of useful data such as how often you run the playbook, how much of the process is followed, and any other metrics you've configured. With every run your team has an opportunity to learn and improve the process to increase velocity, accuracy, and effectiveness. Read more and find other ways to customize your playbooks in our docs.