On-Call Playbook

- Introduction Training
- Before your shift starts
- During your shift
  - Getting help during an incident
    - Triggering a new incident in PagerDuty
    - Engaging your communication manager
    - Navigating environment access restrictions
    - Engaging another on-call rotation
    - Security and Privacy Incident Escalation
  - Things to look at
    - Specific bug
    - Widespread issue
  - De-escalate
    - Internal False Alert
    - External False Alert
    - Lower priority
- After your shift
  - Reporting your on-call shift
    - For Employees
    - For Contractors
  - Reporting other on-call or incident support situations
  - Booking recovery time

Introduction Training

For training on Incident Management, refer to https://league.continu.co/#/view/tracks/633450ad1f6f3200135d8cdc.

For training on PagerDuty, here is a good video that covers the basics:

https://www.youtube.com/watch?v=pNzVLyPrrjs

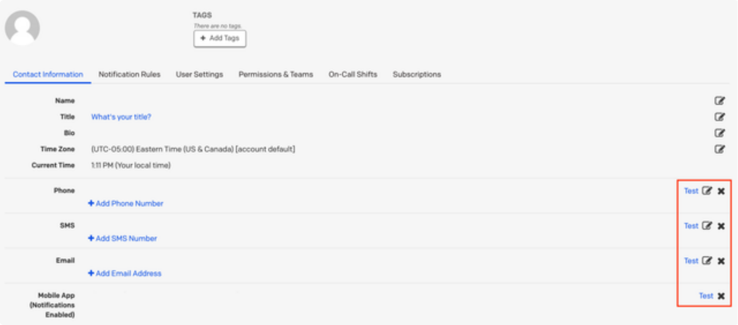
You can skip the sections that are about managing the platform and go straight to specific topics:

- 10:49 - Manage your profile and test notifications via SMS, phone call or mobile app
- 18:26 - Configure notification rules
- 41:15 - Schedule an override (i.e. swap on-call with someone else)
- 58:37 - Responding to an incident (acknowledge, reassign, add responder)

Before your shift starts

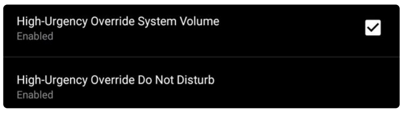
- Get familiar with Incident Response Automation
- Setup your PagerDuty access, see How to access PagerDuty
- Check your on-call schedule in PagerDuty.
- Go to your PagerDuty profile:
  - Check your contact information
  - Configure your notification rules according to your preference (push notification, SMS, phone call), keeping in mind that you want to see the alert in the **first 10 minutes** before it may get escalated.
- Install the PagerDuty mobile app.
- Test the notifications (**including in do-not-disturb, sleep, or any other focus mode**)! At the moment this can only be done from the PagerDuty web app on your profile (look for the Test link next to your phone number config).

  - Enable all do-not-disturb options in the app settings. Give PagerDuty all permissions to override system preferences both for notifications and calls. May also require to manually add the app to the exceptions list for focus modes in system settings.
  - Pro-tip: PagerDuty app also has a feature to install a vCard containing their phone numbers, which you can add to the list of contacts that can override do-not-disturb mode on your phone.



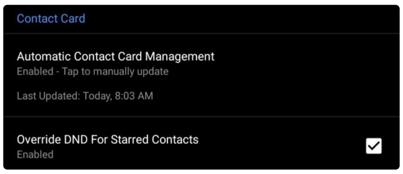
TAGS
There are no tags.

Name
Title: What's your title?
Bio
Time Zone: (UTC-05:00) Eastern Time (US & Canada) [account default]
Current Time: 1:11 PM (Your local time)
Phone: + Add Phone Number — Test
SMS: + Add SMS Number — Test
Email: + Add Email Address — Test
Mobile App (Notifications Enabled) — Test



High-Urgency Override System Volume ☑
Enabled

High-Urgency Override Do Not Disturb
Enabled



Contact Card

Automatic Contact Card Management
Enabled - Tap to manually update

Last Updated: Today, 8:03 AM

Override DND For Starred Contacts ☑
Enabled

- If you are planning some extended period of unavailability during your shift, with inability to check your phone for 15 minutes or longer, find a replacement in your on-call team. Once your replacement is identified, schedule an override in PagerDuty.

During your shift

ℹ For more details on how to handle alerts, refer to How to Handle Alerts .

You just got paged for production incident, what do you do?

1. Acknowledge the PagerDuty alert within 10 minutes
   a. An alert will be escalated to manager on rotation if missed
   b. Acknowledged alerts will auto-unacknowledge (aka retrigger) after 4 hours. This is to ensure that acknowledged alerts are not forgotten completely.
2. Get online within 30 minutes and spend a couple of minutes understanding the problem
3. Once you have assessed the situation:
   a. If the issue appears to be a critical or high priority (as per Priority Guidelines), you are the **Incident Coordinator**. Follow the instructions in Incident Response Automation to kick off **incident response** and engage your communication manager.
   b. If this appears to be a false alarm or low priority issue, see the de-escalate section
   c. If you are not sure, treat the issue as an incident and get some help.
4. Once the issue is resolved or mitigated, resolve the incident in PagerDuty.
   a. If the source of the alert was Prometheus, once the alert recovers on its side the PagerDuty incident will be automatically resolved.
5. Initiate the Post Incident process when appropriate.

If you're a visual learner, the steps above are also described in On-call Process Flowchart ARCHIVED .

Getting help during an incident

Triggering a new incident in PagerDuty

If an issue came to you via slack or other channel, and you need to engage people on-call for help, you will need to create a new incident in PagerDuty, see Escalating an incident to Engineering on-call for more details.

Engaging your communication manager

As per Incident Response Automation , the first step of the automated workflow will page a Communication Manager on-call.

Navigating environment access restrictions

Access to production data and logs is subject to geographic restrictions. For the most part, you should lean on the escalation path defined in Mitigation of access restrictions for on-call when you require data access.

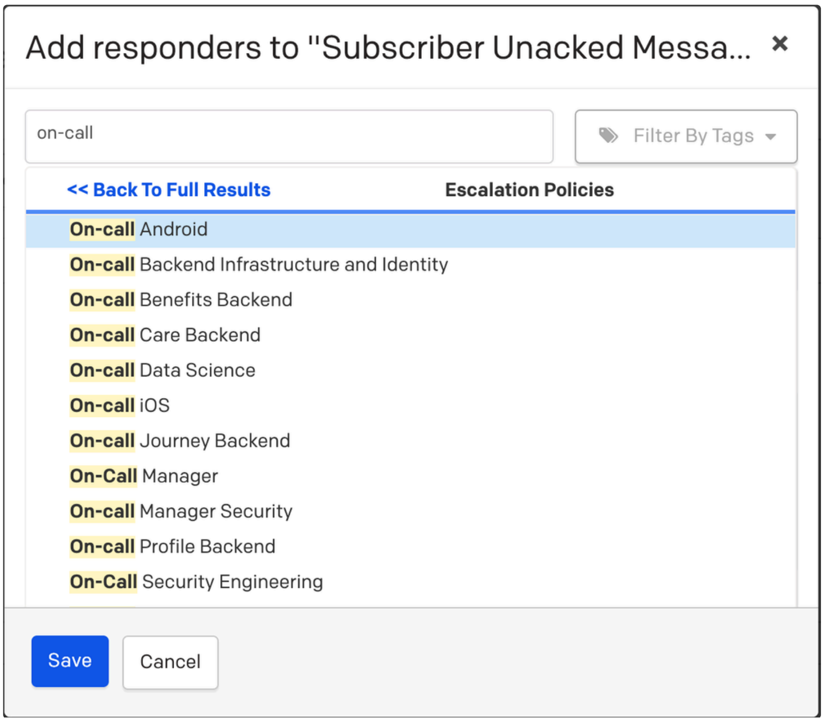
If you know you're going to need access during your on-call shift, and are eligible for it, here are some pointers for requesting this access:

- MongoDB Requesting Production Access
- CHAPI Data Permission or Infra Request

Engaging another on-call rotation

> ⚠ As the first responder of an incident, DO NOT blindly Reassign the incident to another person or escalation policy in PagerDuty. Instead, keep the incident assigned to you and engage others by using "Add Responders". Once others join the zoom call and appear better suited to drive the resolution, you can reassign the incident to them.

You may need to pull Engineers from other teams. In PagerDuty, click "Add Responders" start typing "On-call…" and select the appropriate rotation that you wish to engage.



Add responders to "Subscriber Unacked Messa...

on-call

On-call Android
On-call Backend Infrastructure and Identity
On-call Benefits Backend
On-call Care Backend
On-call Data Science
On-call iOS
On-call Journey Backend
On-Call Manager
On-call Manager Security
On-call Profile Backend
On-Call Security Engineering

Security and Privacy Incident Escalation

If you have reason to believe or suspect that an issue may have critical Security or Privacy impact on League or our members you are encouraged to reach out to the Security On-call individual. The best way to escalate an issue is to create a New Incident Directly in Pagerduty.

What kinds of events should be escalated to the Security Team:

- Customer escalations of potential security or privacy-related incidents (examples include unauthorized access by a terminated HR admin, suspected compromised accounts)
- Failed controls or unauthorized access to data (HR Admins have access to items they should not, PII/PHI available to unauthenticated individuals)
- Suspiciously high failure rates that do not seem to be related to system changes and may be linked to a handful of users (high failure rate against marketplace payment gateway, high failures against promo code remediation endpoints, obvious brute force attacks enumerating numbers)
- Backend related failures in our authentication system including sign-in failures, 2FA failures (Authy), socket authentication failures, HTTP Authentication failures

For Instructions see this document: How to Report a Security Event?

Things to look at

Specific bug

If the problem is affecting a specific part of the product.

- You don't need to fix the bug to resolve the problem. Start by checking #deploy-prod to see if any recent change correlates with the beginning of the problem and consider reverting if this can be done safely.
- Apply typical debugging skills to try and narrow down the root cause:
  - Try to identify "markers" to figure out which job/api is failing.
  - Look at logs using Cloud Logging/ [Logging] Google Cloud Logging, Log-based metrics and Dashboards to find the issue wrt to a specific api that is failing.
  - Reproduce the problem in the prod or testprod environment
  - Formulate hypotheses and run experiments to validate them
  - Try to narrow down the problem to a particular piece of code
  - Check the recent git history of any suspicious code using Git - git-log Documentation or your favorite IDE's git plugin
  - If you need to dig further, try and reproduce the problem in your local environment (See Deploying your PR to Test2/3/4 or Testprod to know how to deploy your app to a test env)
  - If necessary, consider shipping additional logging
- If you need more context on a feature, try to identify the team who owns the functionality and dig into their confluence space or Jira history. A good starting point is Feature Ownership Per Team.

Widespread issue

Note: if any link below appears broken, please also check Devlinks.

Any widespread issue has a very specific root cause that is not directly visible. So you first need to investigate the symptoms to narrow down the problem to a specific one that can be debugged.

Be careful of red herrings! It's very common for a low level issue to trigger side effects upstream.

Check out the following resources:

- Grafana: look for patterns over time across different graphs.
  - The Services Overview dashboard may be useful to narrow down a generalized performance problem to a particular service.
  - System Overview, API, MongoDB, Health App, Salesforce API can be useful to narrow down some performance anomalies compared to a typical healthy state from the past.
  - Pro-tip: You can compare against yesterday/last week in Grafana. Log in (lower left corner, door icon) if you're not already, duplicate the panel, edit the duplicate and set Time Shift to something like "1d" or "1w", back out to the dashboard. You'll be able to see both the current and previous period's graphs. Don't save your changes.
- Sentry can detect new errors on services, frontend-web or league-web
- Google Analytics can be used to compare current traffic levels against normal times.

De-escalate

Internal False Alert

If an automated alert appears to be a false alarm or a temporary glitch that went away. This is not an incident and you can deescalate the issue.

- First, make sure that things are stable and you can't reproduce the problem after multiple attempts.
- Resolve the incident in PagerDuty
- Close the Jira ticket as False Positive (if there is one)

- Archive the incident Slack channel (if there is one)

External False Alert

- If an issue was raised by a client and we believe that the system is working as expected. The Communication Manager works with the Customer Team to provide our feedback to the client and ask them to close the ticket.
- Once confirmed, close the INC Jira ticket as “False Positive” and archive the incident slack channel.

Lower priority

- If an issue was raised by a client and we believe that the priority should be lower. The Communication Manager works with the Customer Team to provide our recommendation to the client and get alignment.
    - Once the issue is downgraded to Medium, close the INC Jira ticket as “No Report Needed” and archive the incident slack channel.
- If the issue is only internal, the Incident Coordinator and Communication Manager can decide to lower the priority to Medium and provide some justification in the incident channel.
    - Create a follow-up ticket for the appropriate team to handle the lower priority issue and let them know in their team channel (see Teams, Mandates & Feature Ownership)
    - Close the INC Jira ticket as “No Report Needed” and archive the incident slack channel.

After your shift

⚠ **Important!** In order to receive the recovery time or monetary compensation that you are eligible for, you need to follow the instructions below.

Reporting your on-call shift

For Employees

- After your on-call shift, submit this google form to report the details of your shift: https://forms.gle/Yafqa9KB4C2MF1qP7
- Each Wednesday, the People Team will process the form entries submitted within the prior week, reflecting as recovery time added in BambooHR or monetary compensation via the next Payroll, according to the rules specified in Engineering On-Call Policy for employees | [inlineExtension]On call compensation.
- If you submit your google form later than Tuesday EOD, there is a chance it will not be processed until the following Wednesday.

For Contractors

- After your on-call shift, submit this google form to report the details of your shift: https://forms.gle/Yafqa9KB4C2MF1qP7
- Add the on-call compensation line item(s) to your next invoice, according to Engineering On-Call services by Contractor Plus | [inlineExtension]On call compensation.

Reporting other on-call or incident support situations

Use the same method if one of these situations apply to you.

- You were NOT on-call for that whole week but you covered a holiday. You are eligible for the recovery time or amount corresponding to that holiday.
- You were NOT on-call for that week but worked 4h or more outside of your normal working hours to assist with the resolution of an incident. You are eligible for the corresponding recovery time or amount.

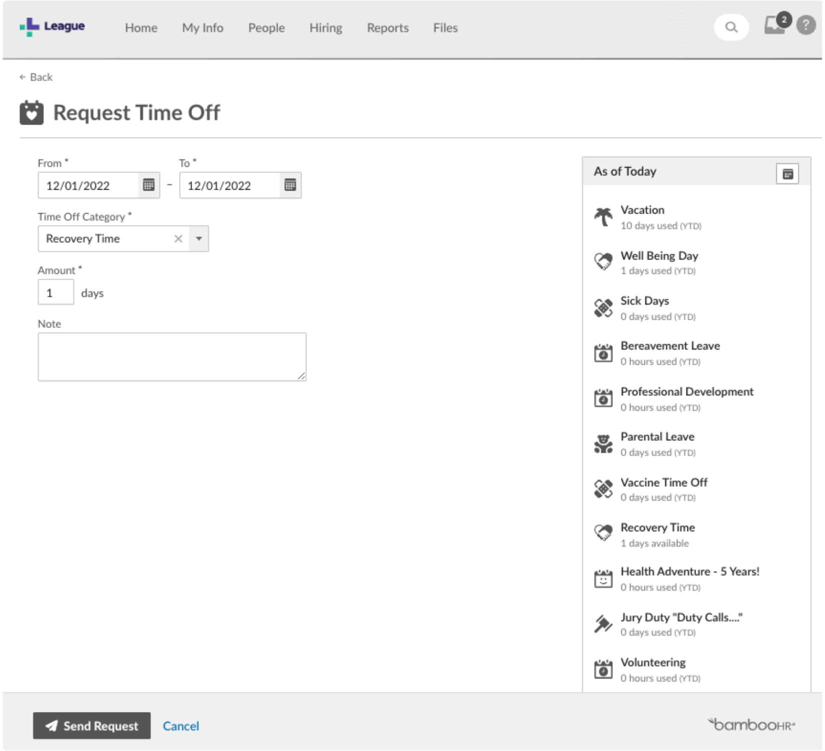
Booking recovery time

If you opted for some recovery time, here is how to book it.

- Similar to booking another type of day off, go to BambooHR and click **Request Time Off** on the homepage.

- Select Time Off Category = Recovery Time and input the date(s) you wish to take as time off
    - You will be able to see the # of recovery days you have available on the Request Time Off screen
- Click **Submit Request**, and the request will be routed to your manager for approval

Note: To promote health & wellness, recovery time should be taken within 2 weeks after the scheduled on-call shift.



Request Time Off

From * 12/01/2022 – To * 12/01/2022

Time Off Category * Recovery Time

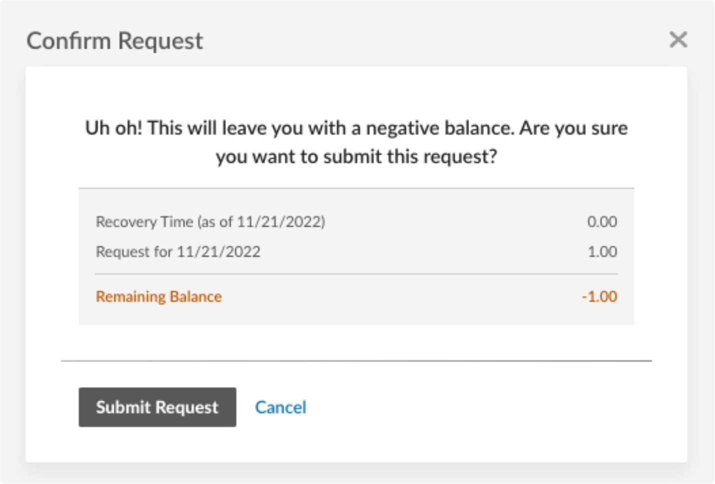
Amount * 1 days

Note

As of Today

Vacation	10 days used (YTD)
Well Being Day	1 days used (YTD)
Sick Days	0 days used (YTD)
Bereavement Leave	0 hours used (YTD)
Professional Development	0 hours used (YTD)
Parental Leave	0 days used (YTD)
Vaccine Time Off	0 days used (YTD)
Recovery Time	1 days available
Health Adventure - 5 Years!	0 hours used (YTD)
Jury Duty "Duty Calls...."	0 days used (YTD)
Volunteering	0 hours used (YTD)

Note: if you are booking a recovery day prior to it being added into BambooHR by the People Team (ie. booking on the Monday immediately after your on call shift, prior to your google form submission being processed on Wednesday), you will receive the following warning. You can still submit your request and the (-1) balance will be corrected to (0) after your recovery time is added.



Confirm Request

Uh oh! This will leave you with a negative balance. Are you sure you want to submit this request?

Recovery Time (as of 11/21/2022)	0.00
Request for 11/21/2022	1.00
Remaining Balance	-1.00