Automatically Disable a User’s Device for Inactivity with GAT Flow and GAT+

Chrome Audit & Management · https://gatlabs.com/knowledge/tech-tips/automatically-disable-a-users-device-for-inactivity-with-gat-flow-and-gat/

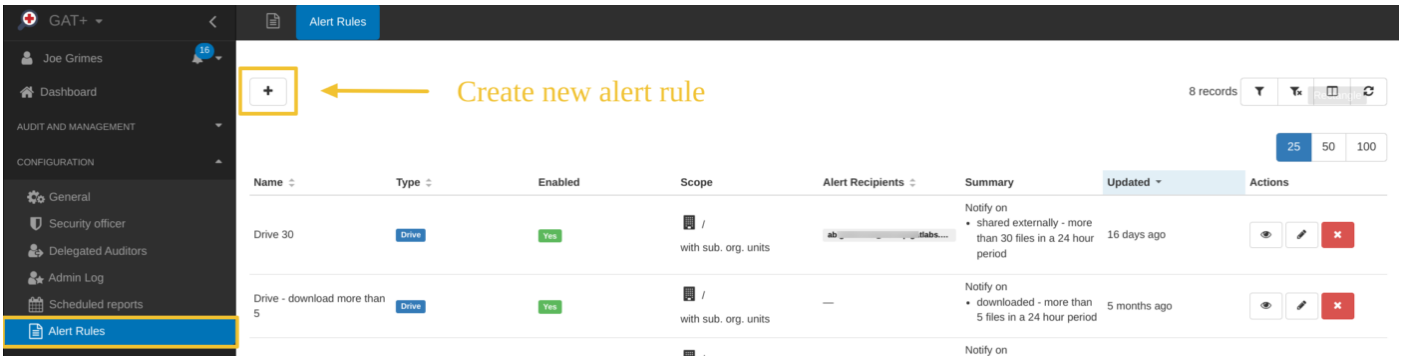
Managing security and user activity is crucial in today's fast-paced digital environment. With GAT Flow and GAT+, it's easier than ever to disable a user’s device for inactivity in Google Workspace.

Utilizing GAT+ to establish an alert rule and GAT Flow to take action, this guide demonstrates how to combine these applications to disable a user's Chromebook or managed device after 28 days of inactivity.

Let's start by setting up the alert rule.

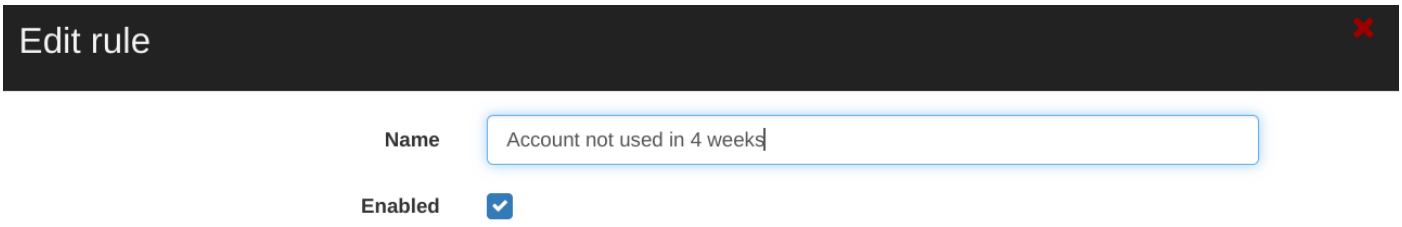
Setting up the Alert Rule

In **GAT+**, go to the **Alert rules** section and click the '**+**' icon in the top left corner to add a new alert rule.



Give it a name, in this example, we'll call it **'Account not used in 4 weeks'.**

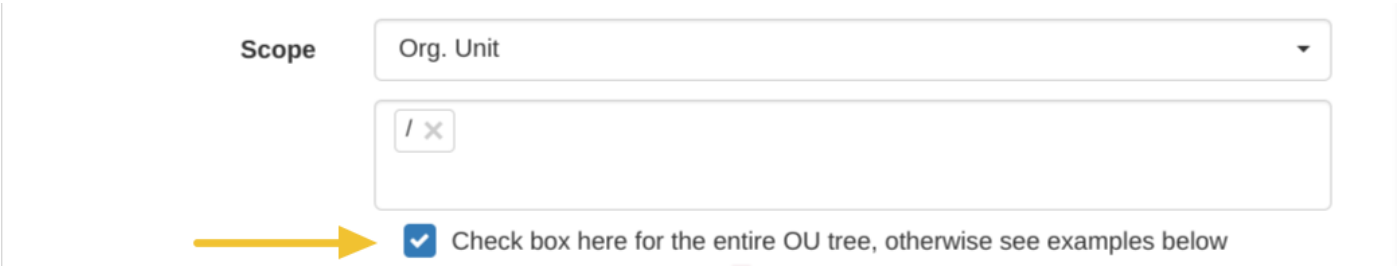
Upon creation, the system sets it to **'enabled'** by default.



Select **Users** as the 'Type' of the alert rule, as the alert rule is running against the user's Google Workspace *account* (not their device specifically).

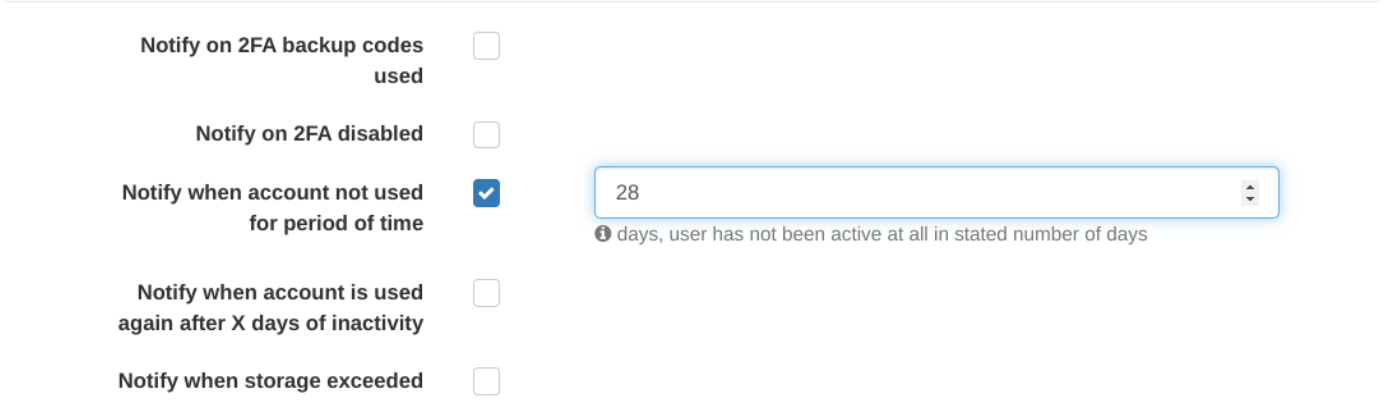


The 'Scope' will allow you to decide which users this alert rule will run on. In this example we will run it on all users, by selecting the root Organisational Unit (OU), denoted by a forward slash (/), and check the box to include all users below the root OU.

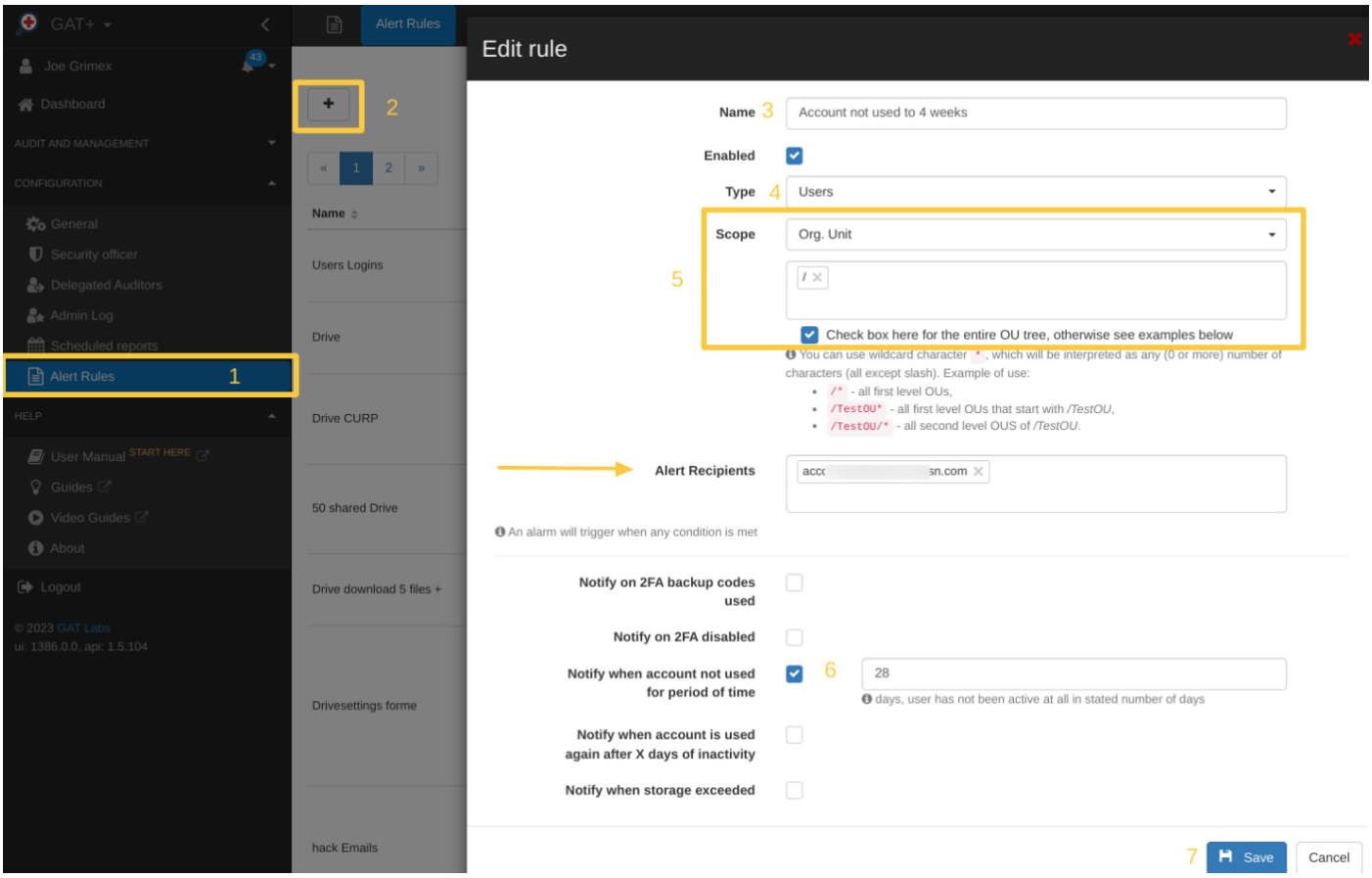


In the 'Alert recipients' field, choose the user(s) that you would like to receive the email. This can be any user's email address, several users, or one or more group email addresses.

Now select the criteria for the rule's alerts. While multiple options are available, for this example, choose **'Notify when the account is not used for a period of time.'** Then, set the time period to 28 days

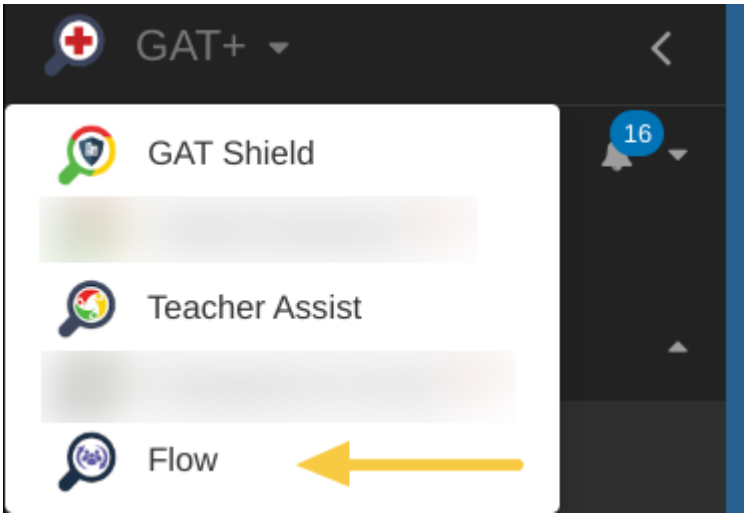


When you have finished, click **'Save'.**

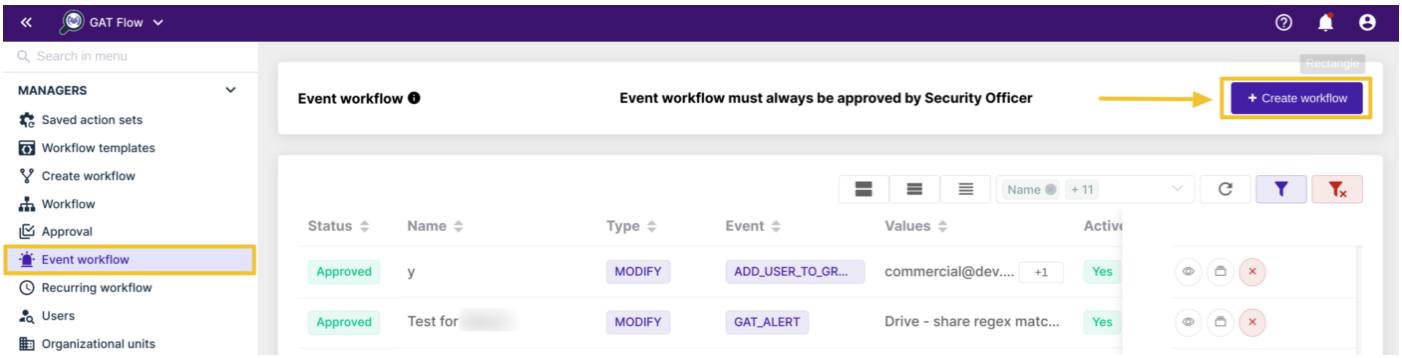


Automatically Disable a User's Device for Inactivity after 28 days

Now click the **GAT+** logo in the top left corner and navigate to GAT Flow.

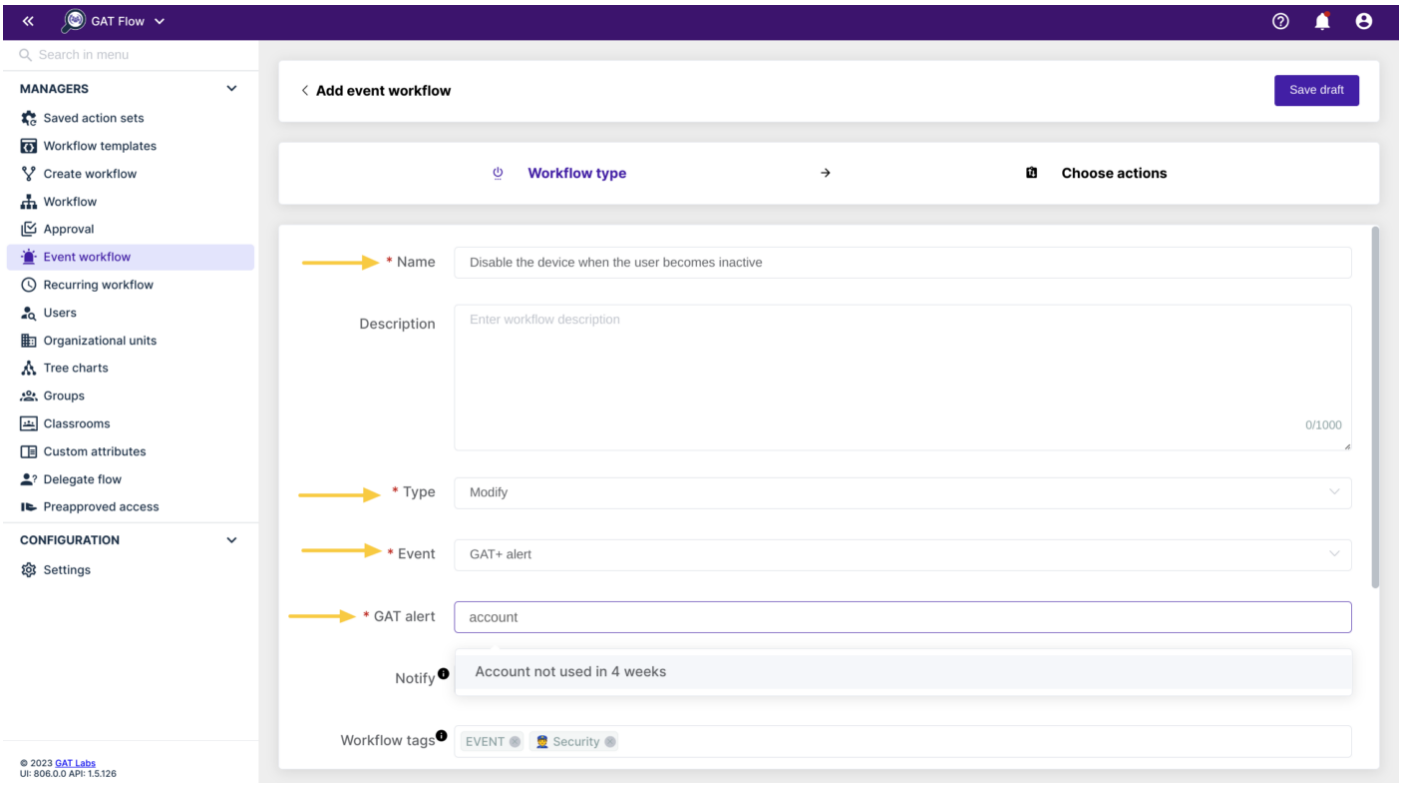


Click the **Event workflow** section and then **Create workflow** in the top right corner.



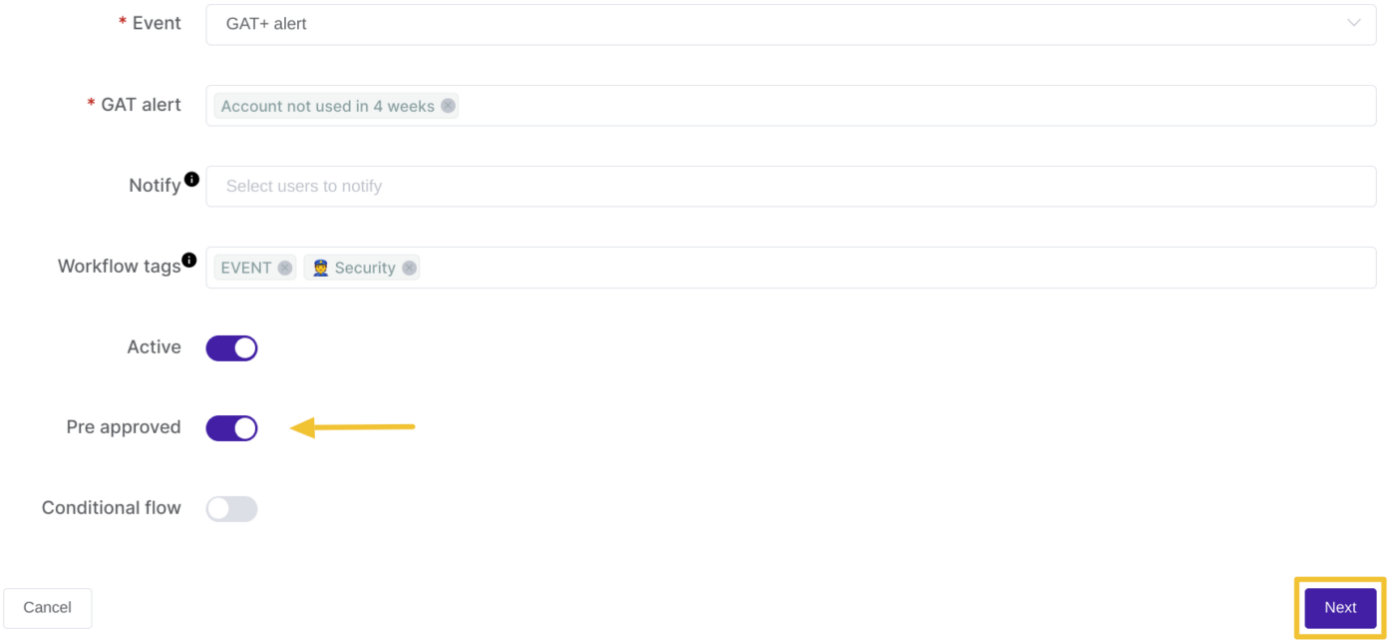
For the type chosen give the workflow a name set the 'Type' to **Modify** and the 'Event' to **GAT+ Alert**.

For 'Alert' you can begin typing the name of your alert and it will appear.



By default, the workflow is set to active. Turn on the **Pre-Approval slider**, and the workflow will automatically run each time the alert is triggered.

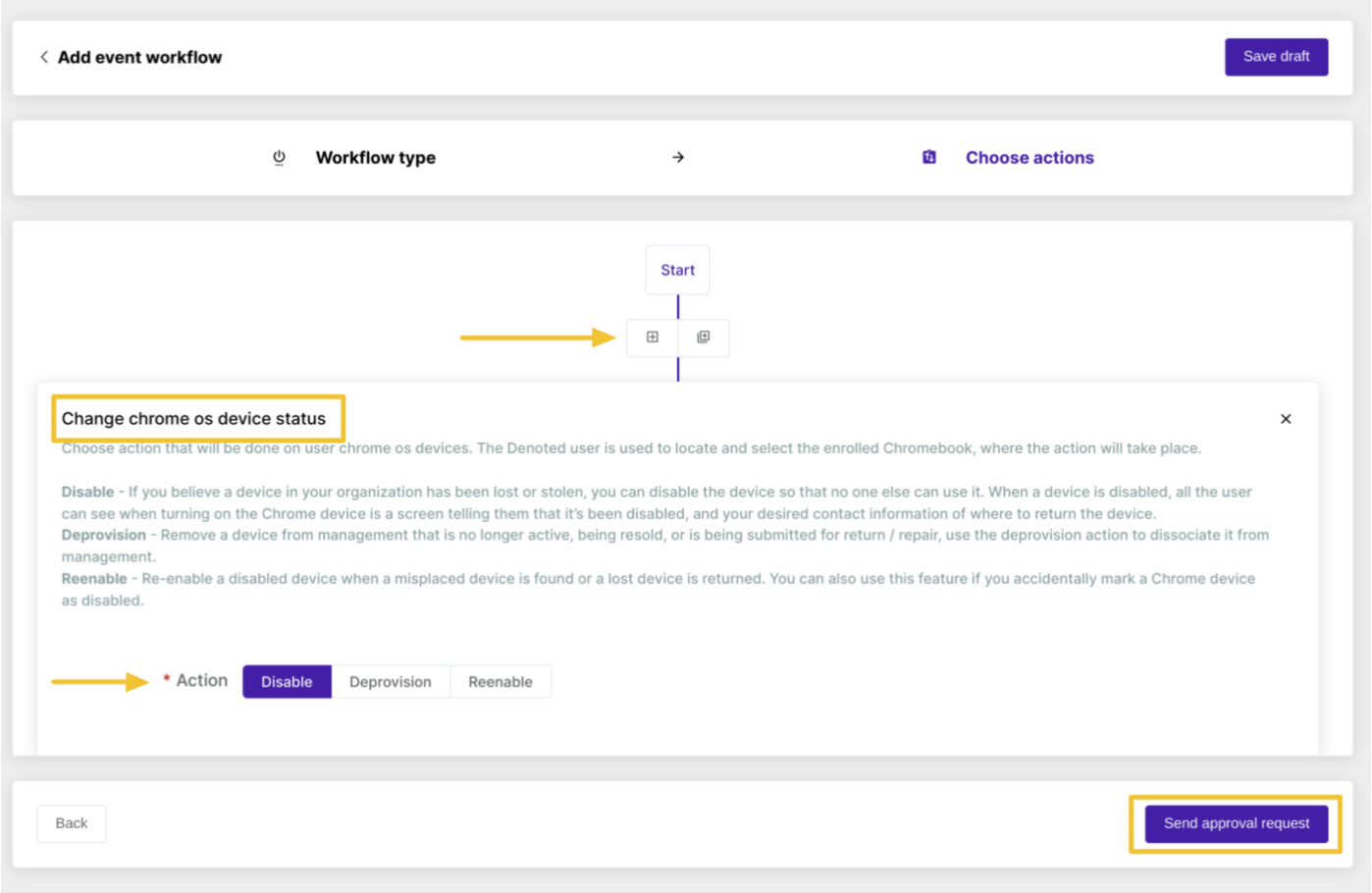
Once you are finished, click **'Next'.**



On the next page, click the **'+'** icon to bring up the list of actions. Find **'Change chrome os device status'** on the list and select it.

On the action itself, click **Disable.**

When you disable a device, the user will see a screen displaying a disabled message and your contact information for returning the device upon turning on the Chrome device. No users can sign into this device until an admin re-enables it, a feature commonly known as 'lost mode'.



It is possible to add other actions you want to happen at this stage if desired by clicking the '+' icon again and selecting those actions.

Lastly, click **'Send approval request'** to submit the workflow to the Security Officer for approval.

Once approved, the workflow automatically runs. If any user in your domain fails to sign into their Google Workspace account for 28 days, the system will automatically disable any managed Chrome device assigned to that user.

Notes

If a user is associated with multiple Chrome OS devices, the system will disable all of them. However, personal devices will remain unaffected.

The alert rule actively checks whether any user has signed into their **Google Workspace** account, rather than monitoring sign-ins on a specific device. Therefore, if a user hasn't signed into a particular device for more than **28 days** but has logged into their Google Workspace account through another device, the rule will not disable the unused device.