Delete Domain Users’ Emails That Pose Security Risks with GAT+

Email Audit & Management · https://gatlabs.com/knowledge/tech-tips/delete-domain-users-emails-that-pose-security-risks-with-gat/

Embedded media:
https://www.youtube.com/embed/SBoL8MbQ65k?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_l

With the GAT+ tool, Google Workspace Admins can identify and delete emails of any user in your domain. There are several reasons why an admin would want to do that, but the biggest concern is the security risks posed by them. GAT+ has been designed to offer the ability to navigate the emails of your concern and delete them.

Some of the scenarios that may apply are as follows:

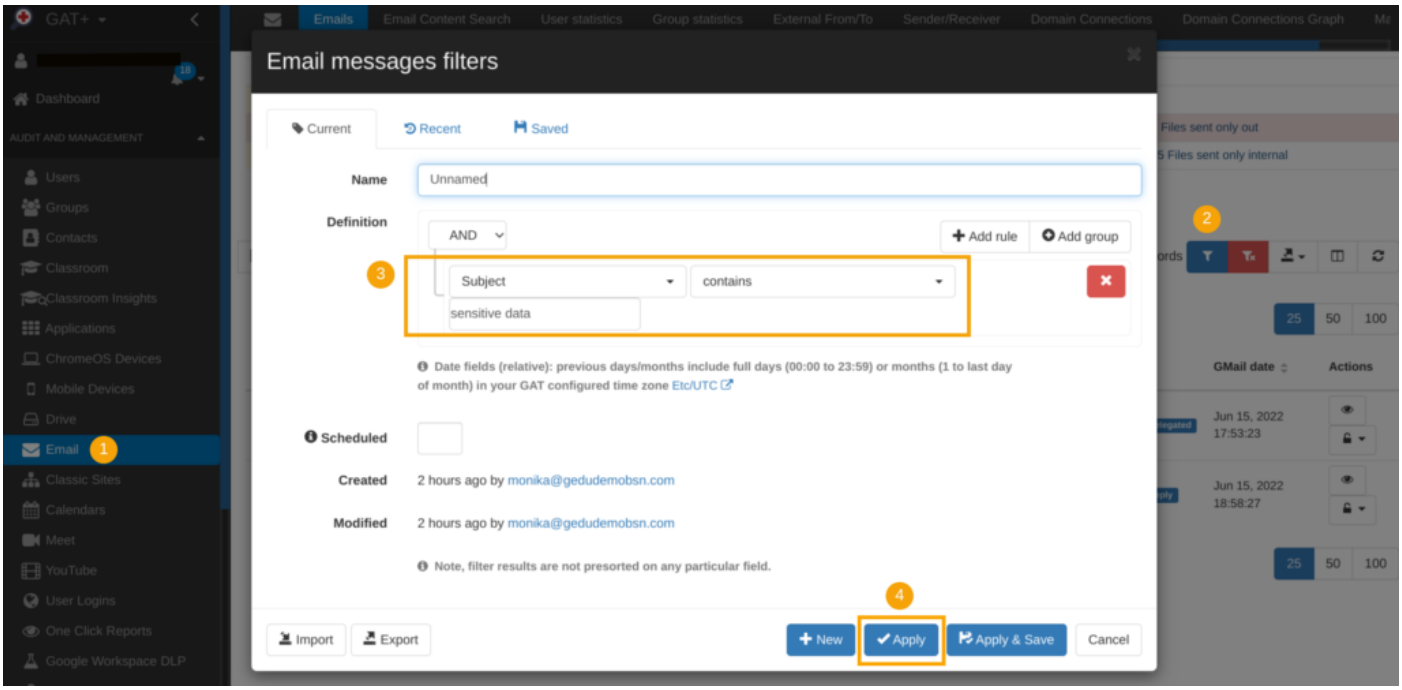
- an email containing sensitive data
- an email wrongly addressed
- phishing or spamming

Identify emails that are a security risks

In order to find the emails of your concerns, navigate to GAT+ and apply a filter that helps to identify them.

There are several filtering options that can be applied depending on your use case. Apply a definition that best suits your search purpose. Once ready, apply the filter.

We show a proposal of the filter below that searches for emails containing specific wording in the title of the email: 'for example 'sensitive data'.

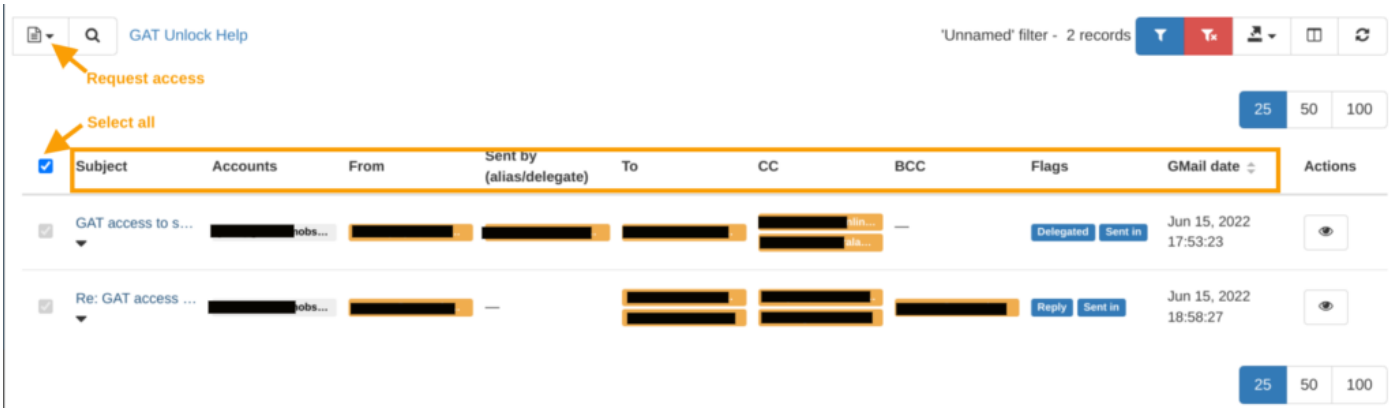


Request access permission to emails for security auditing

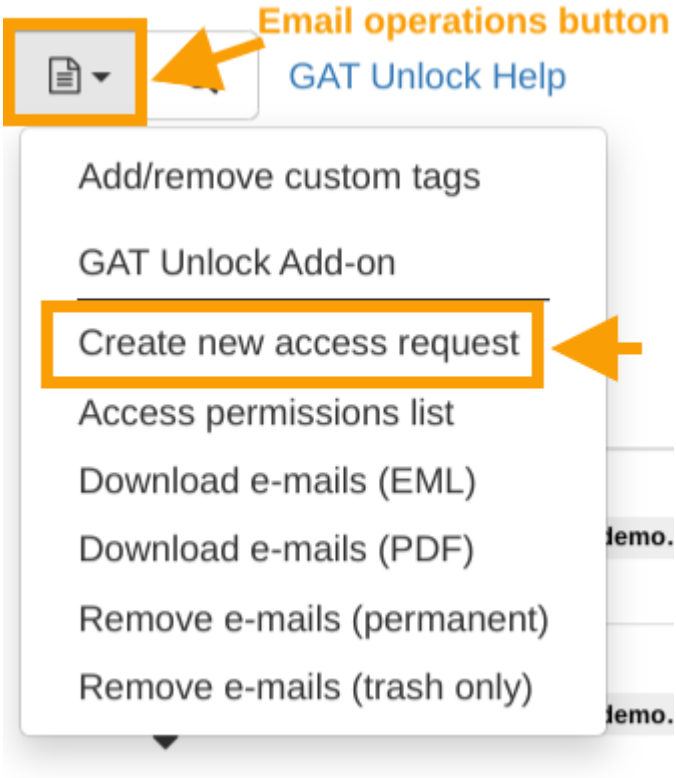
As a result of the above, GAT+ returns the metadata based on the filter applied.

You can have a quick overview of the metadata that is returned and decide on what email you wish to have closer look at by selecting them for further investigation (select All or specific results).

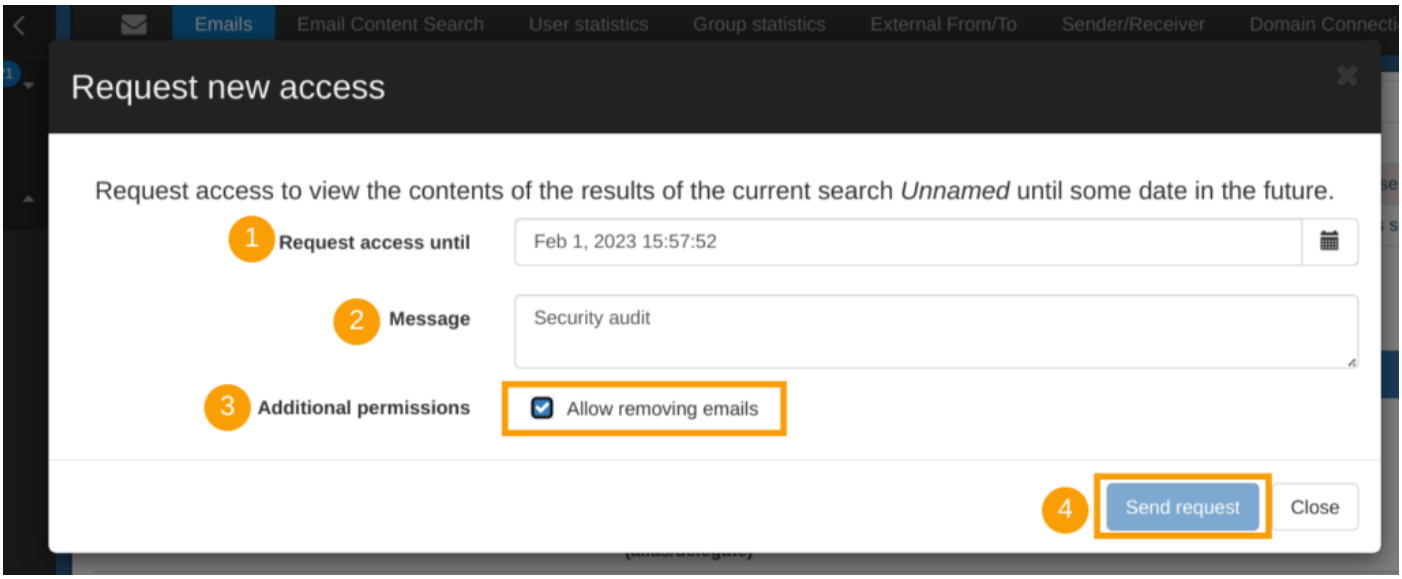
Next, you can request access to view the content of those emails.



To create a request to access the emails' content, click on the '**Email operations**' button. From the drop-down menu select the option '**Create new access request**'.



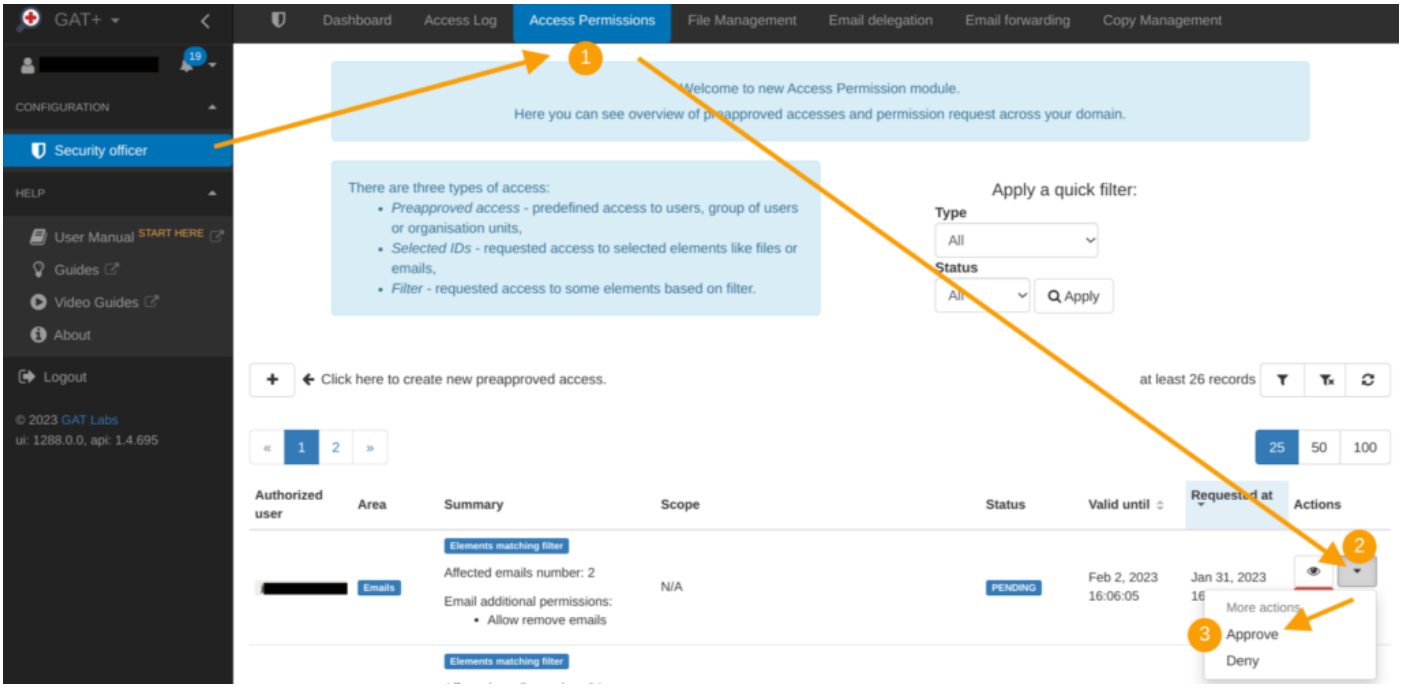
When requesting access, specify the timeframe, add a message for internal communication, and select the option **Allow removing emails**. When ready, send a request for review.



The request can be verified by Security Officer.

Get Security Officer's approval

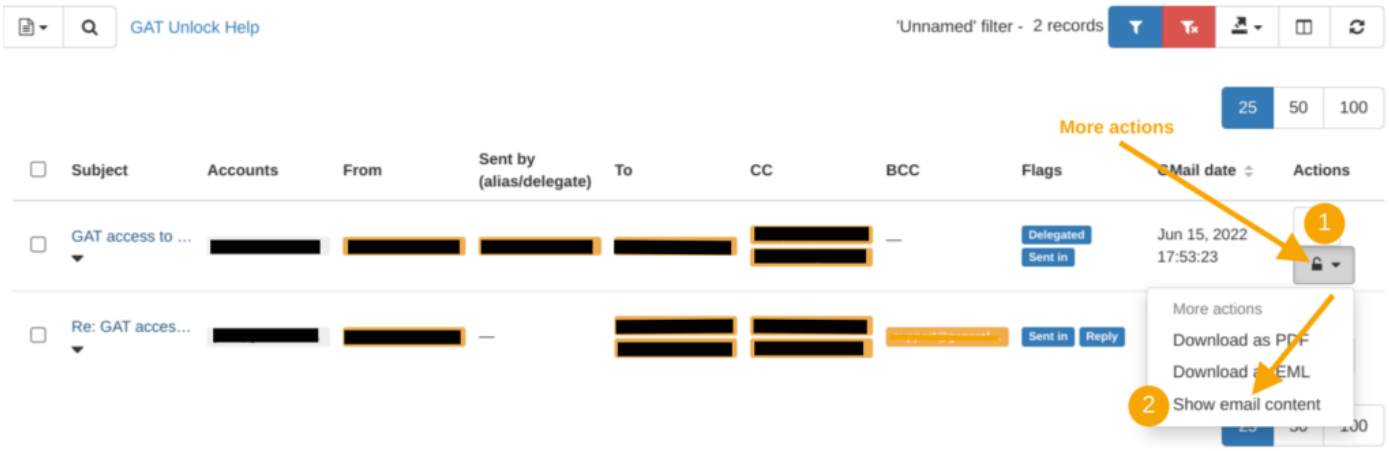
The **Security Officer** can view the request under **Access Permissions** tab once signed in to GAT+ dashboard, and approve it from there.



Review emails' content and delete the ones that pose security risks

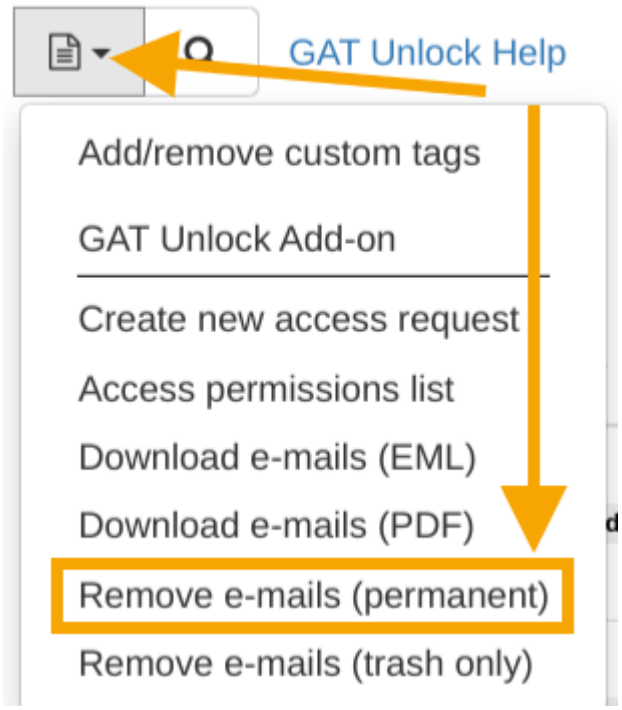
Once the request to access the emails' content is approved, the requestor of the access can now navigate to Email audit in GAT+ and apply the same filter as before.

GAT returns the same results with the additional options enabled under the 'open padlock' icon on the right-hand side.

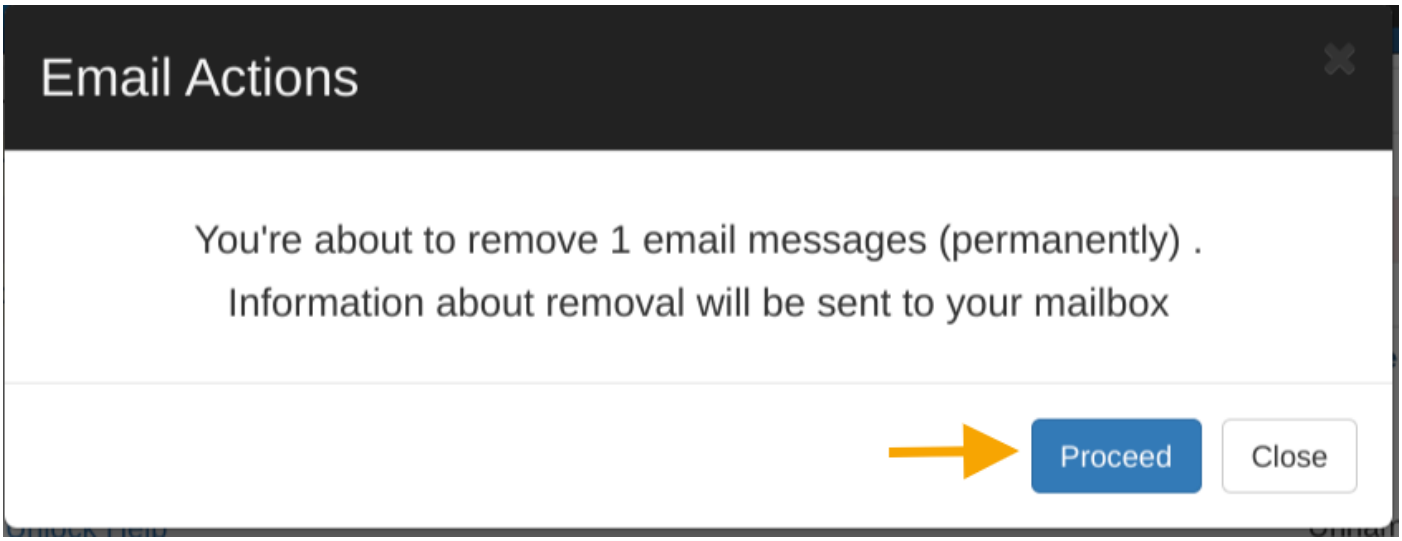


The email content will be displayed in GAT's new window from there the email details can be reviewed. Upon that review, you can decide to move forward and remove the emails.

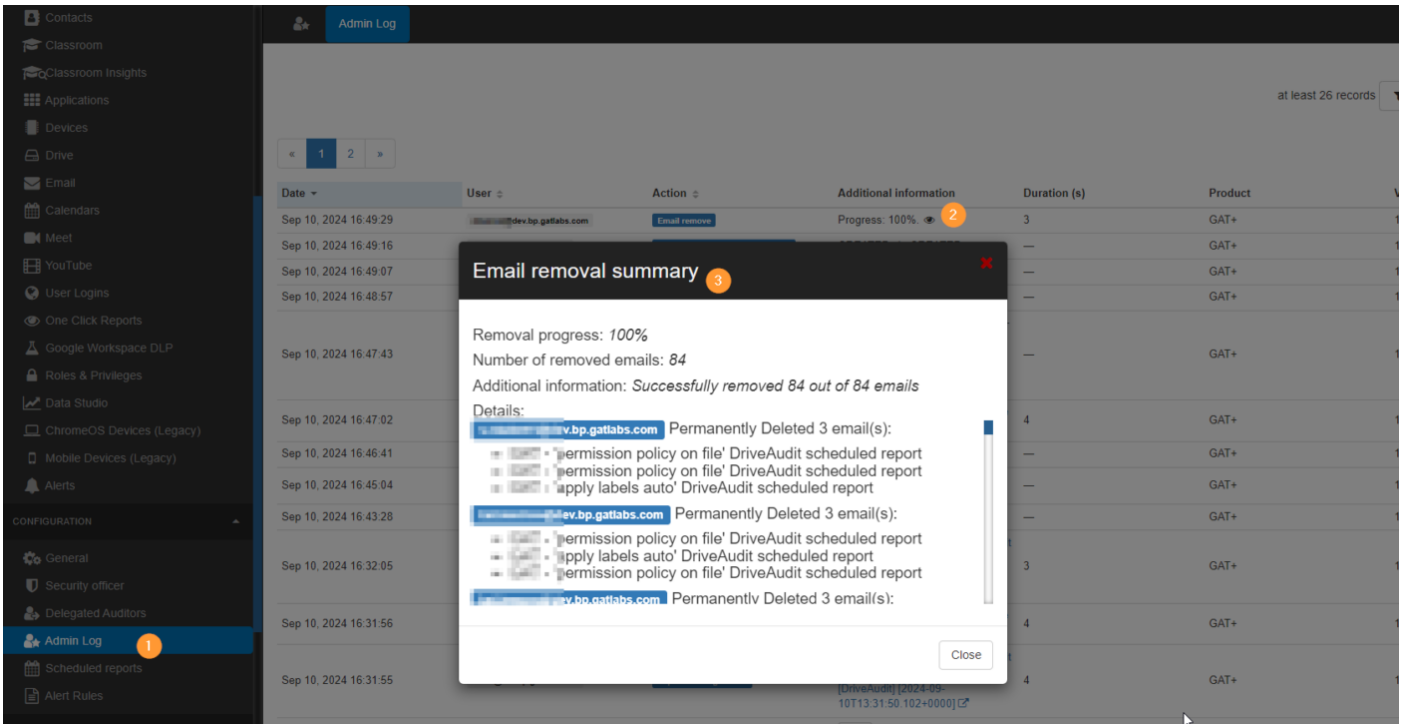
To trigger such an action, select the email you reviewed, navigate again to **Email operations** button, and select the option **Remove e-mails (permanently)**.



Once the option to remove the email is selected, the last verification message comes up. Once confirmed, the email will be removed.



Details can be found in Admin log.



Restore deleted emails

If emails are deleted permanently and done by mistake they can be resoted via the Admin console for 25 days from the day of deletion.

The process is explained in this Google article

Related Posts

- Find and delete Phishing emails
- Delete Spam, Inappropriate or Accidental Emails

- Find Emails Sent and Received by the User with GAT+