How to Set Up User Security Alerts with GAT+

Users Audit & Management · https://gatlabs.com/knowledge/tech-tips/how-to-set-up-user-security-alerts-gat-plus/

Stay alert and always up to date with what's happening on your domain. With GAT+ push notification alerts, administrators can increase their vigilance and domain security by configuring multiple alerts simultaniously.

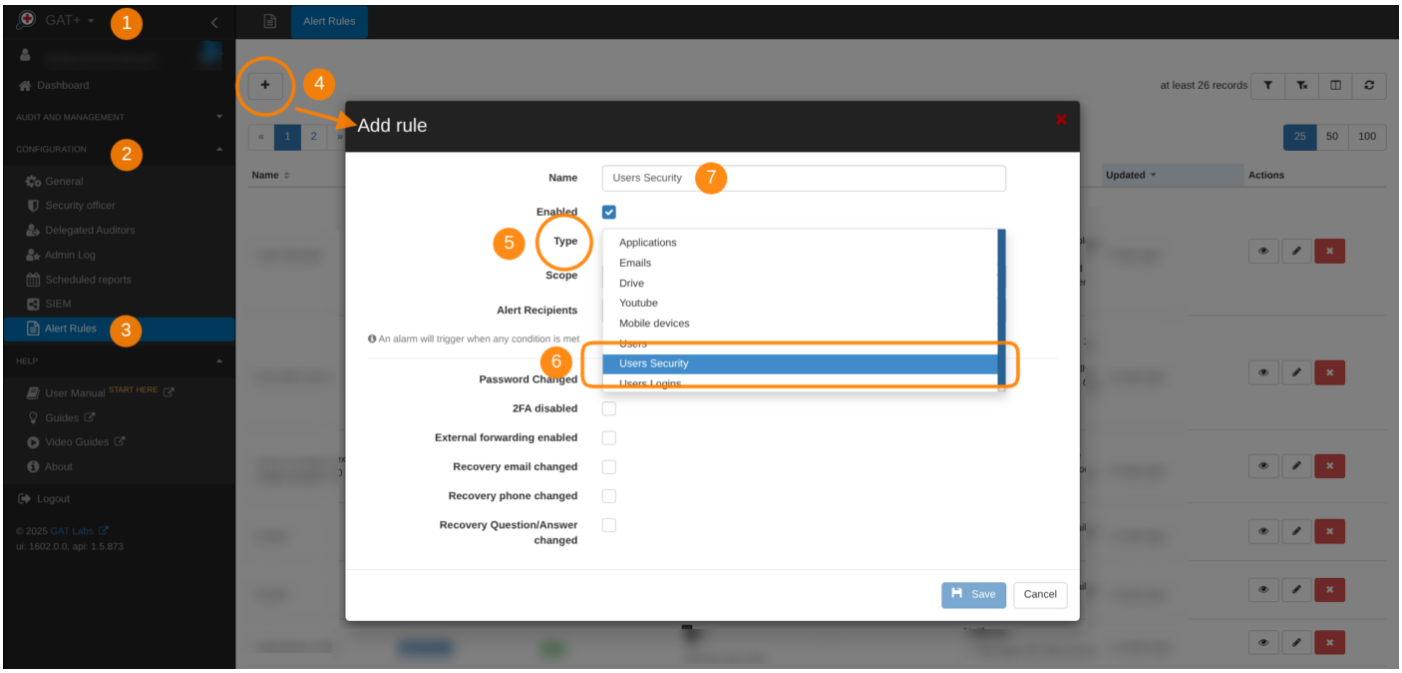
One of the many alerts available in GAT+ is the User Security alert, which can be used to notify you of potential account takeover attempts, especially when multiple changes occur in a short period of time or from unusual locations. This is definitely something to watch out for, and that's why the User Security alert is so helpful.

Below you will find steps explaining how to configure an alert that will suit your needs.

Create Users Security alerts

To create the Users Security alert, navigate to **GAT+ (1) > Configuration (2) > Alert Rules (3) >** click on the "**+**" button **(4)** to add a rule.

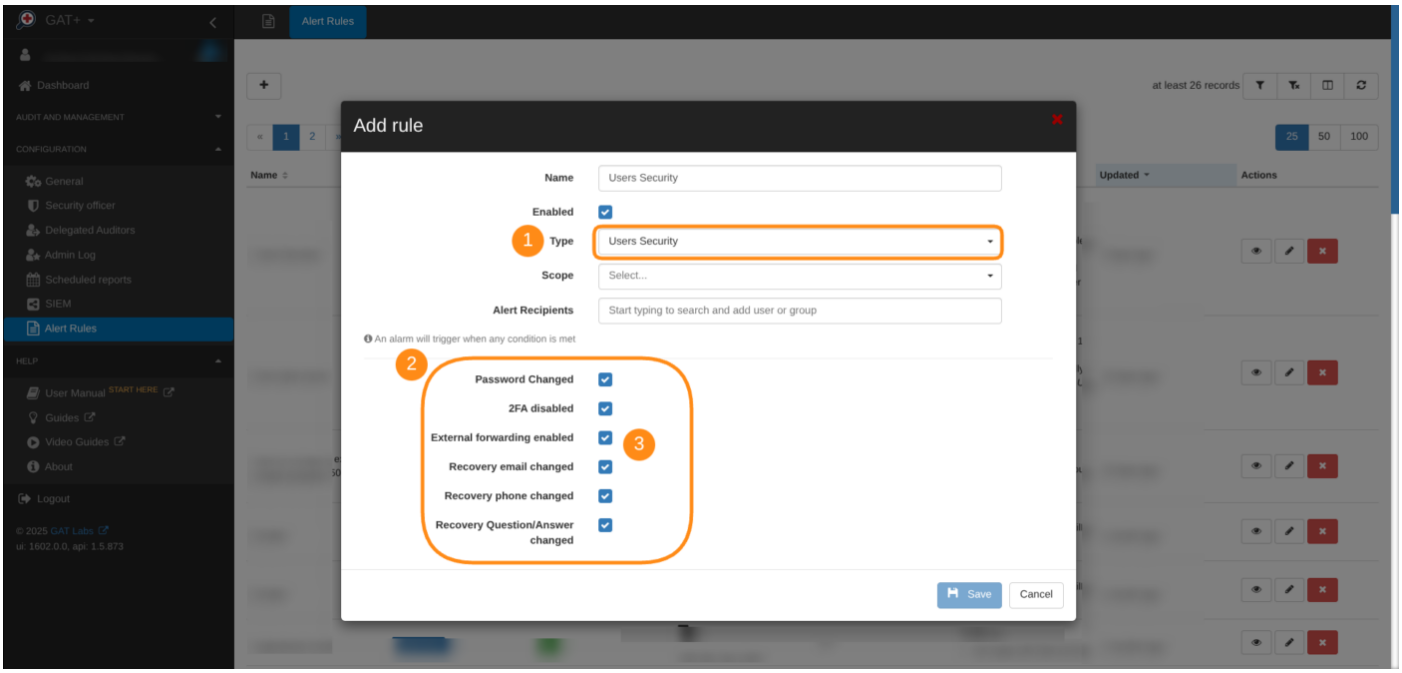
A new wizard window will appear, where you can select the alert **Type (5) : User Security (6)** from the drop-down menu. The alert Name will be automatically filled in and will have the same name as the alert type itself – **Name: User Security (7)**. Note: The alert Name can be customized to differentiate between different alert types.



Select alert event type

Once the **Users Security** type is selected **(1)**, all the available users security events that can be configured and trigger the alert are being displayed **(2)**.

Tick the box(es) next to each alert event type that you wish to trigger the alert **(3)**.



The **Users Security** alert type allows configuring different alert triggering events, and these are as follows:

- **Password Changed** - alert informing about a change of the user account password

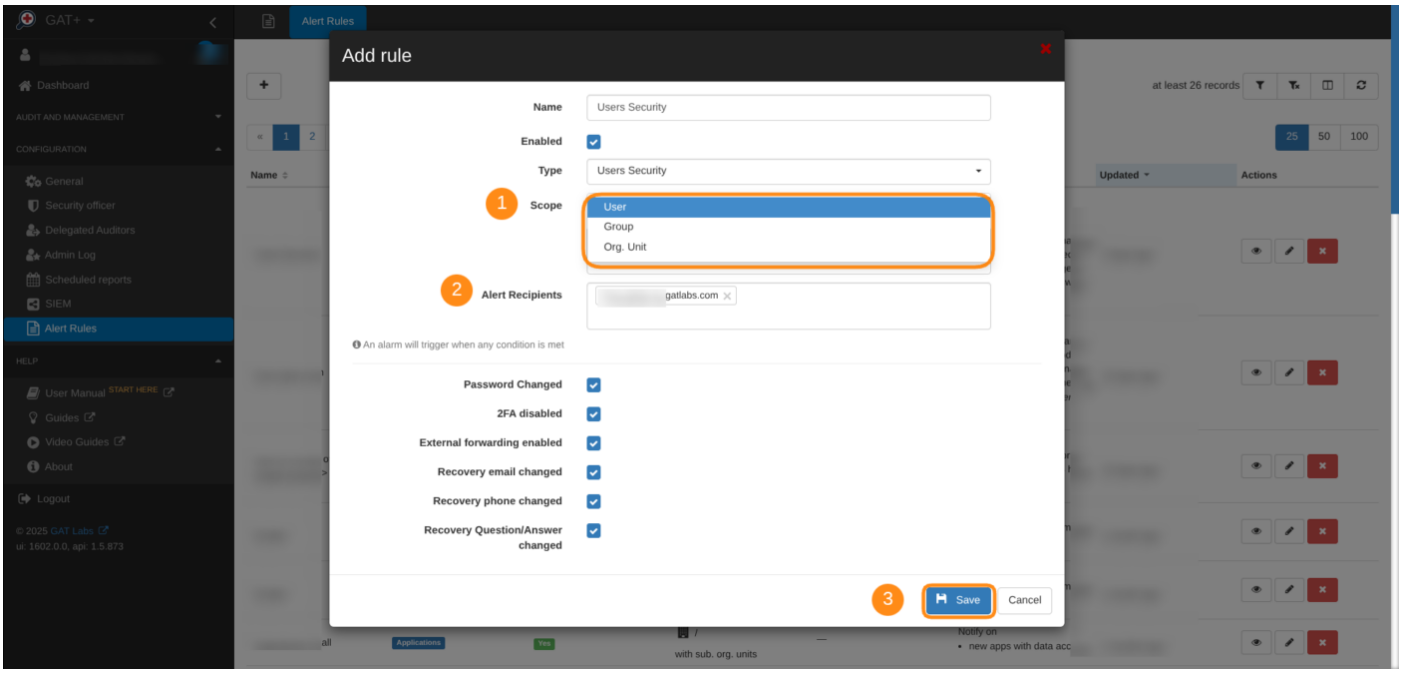
- **2FA disabled** - alert informing 2FA has been disabled on user account
- **External forwarding enabled** - alert notifying if external email forwarding is enabled
- **Recovery email changed** - alert informing about a change of the user account recovery email
- **Recovery phone changed** - alert informing about a change of the user account recovery phone number
- **Recovery Question/Answer changed** - alert informing about a change of the user account recover question/answer

Select the Scope and Alert Recipient

Define the **Scope** of the alert **(1)**, e.g., individual user(s), groups or an entire organizational unit, that will be monitored for this type of behavior. This behavior may be a regular account security measure or a sign of a specific threat. It's important to be aware of these events and monitor them.

Finally, select the alert **Recipient (2)**, this can be an administrator creating this rule for their own awareness, or/and another person responsible for domain security.

Once ready, **Save** the settings **(3)**.

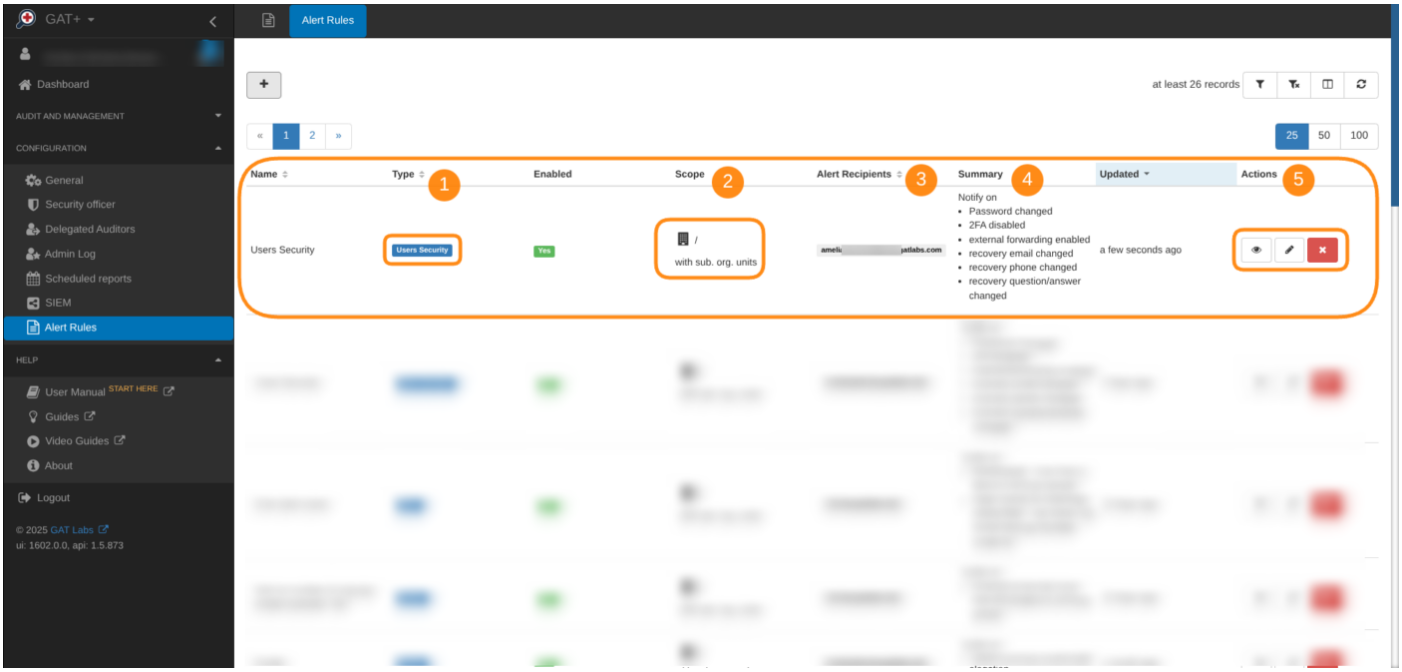


Review alert configuration

After clicking Save, the alert is acitvated and it can serves your needs.

All its details can be reviewed under the Alert Rules section of GAT+, such as:

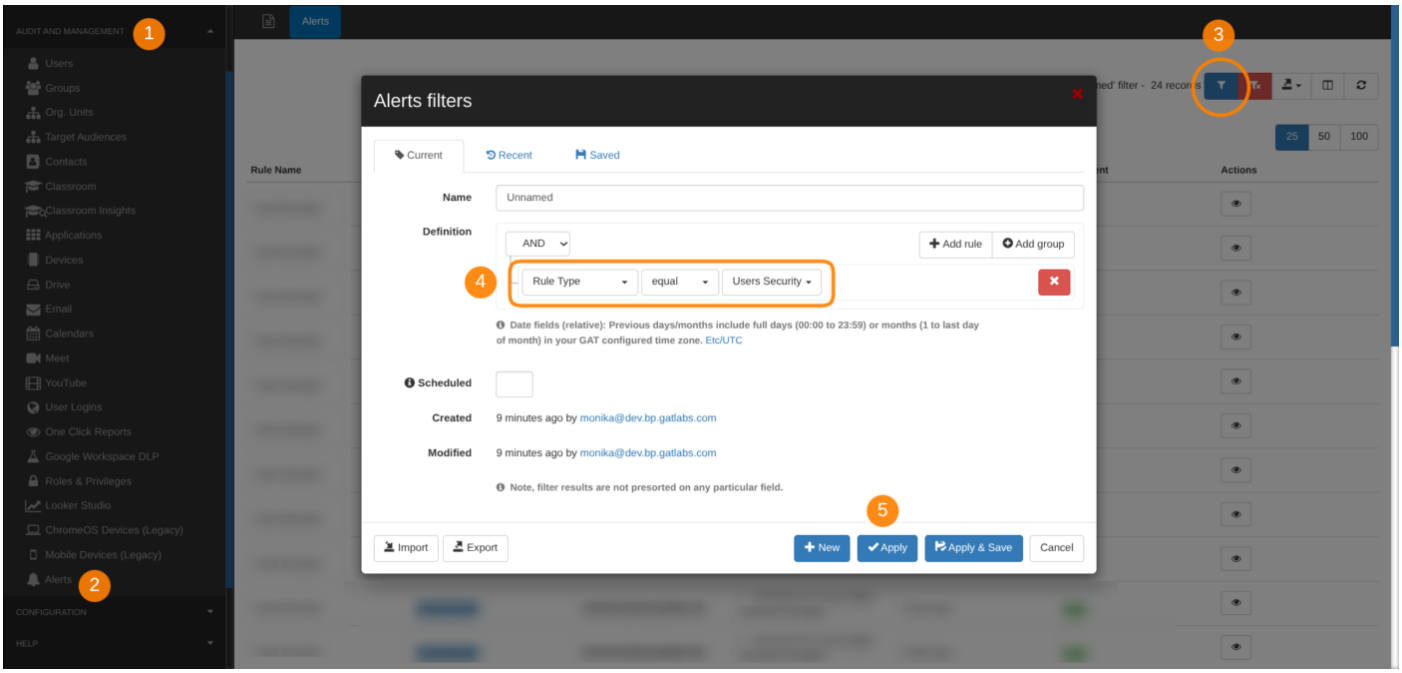
- alert **Type (1)**
- alert **Scope (2)**
- Alert **Recipients (3)**
- alert **Summary (4)**
- alert additional **Actions (5)**, such as the following:
  - "***eye***" icon - review the alert configuration
  - "***pencil***" icon - edit the alert configuration
  - "**x**" icon - delete the alert configuration entirely



Review the alerts logs

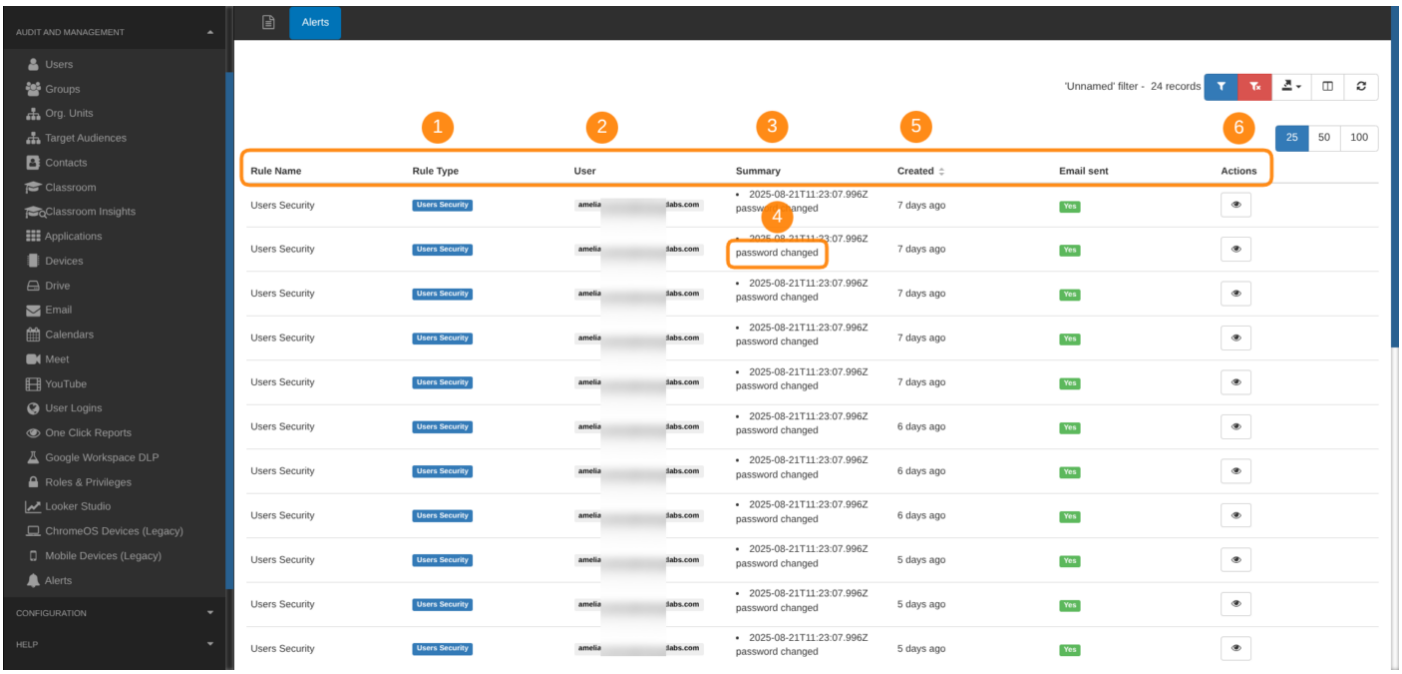
To review if the alert was triggered by any of the configured alert event triggers, navigate to **GAT+ > Audit and Management (1) > Alerts (2) >** and apply a filter **(3)** that returns only the alert events under the specific alert Type **(4)**, e.g. ***Rule Type - equal - Users Security.***

Once ready, hit the **Apply** button **(5).**



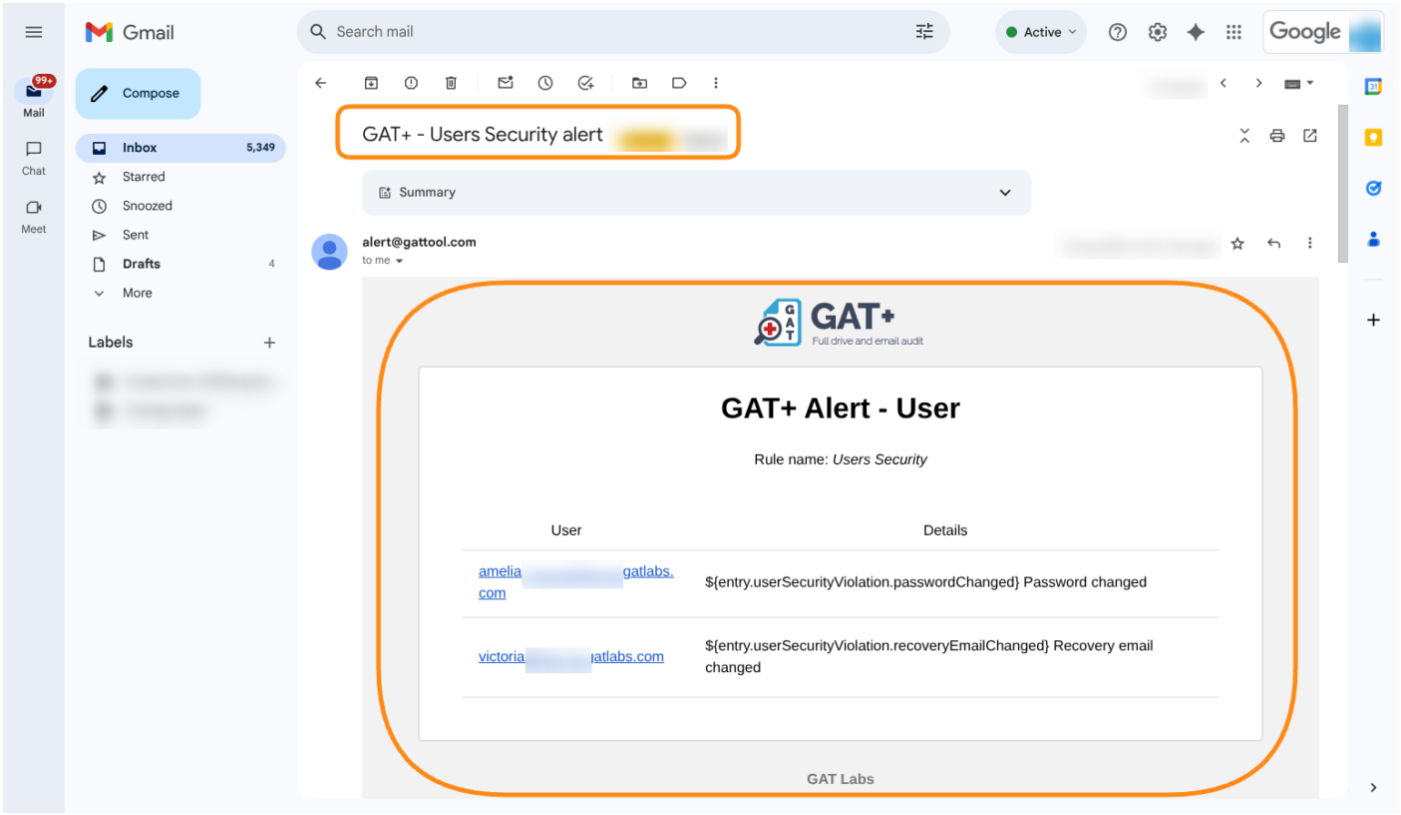
GAT+ returns all the records defined by your filter, and will display them so you can review the following details:

1. **Rule Type (1)**
2. **User (2)** - the person triggered the alert
3. **Summary (3)** - more detailed overview of the alert trigger(s), and underneath also the events that run the alerts **(4)**, e.g. ***password changed*** even, alongside the timestamps of the event
4. **Created (5)** - the time when the alert was logged by the system
5. **Actions (6)** - see Alert details



Review the email notification

Once an alert is triggered, the alert Recipients receive an automated message containing the alert details.



Relevant posts

- Set Up Gmail Alerts for Google Workspace Users with GAT+
- Setting Up User Login Alerts in GAT+
- Alert on Negative Login by Any Google Workspace User
- Alert When 2FA Backup Code is Used by Any User with GAT+
- Alert when 2FA is disabled for any user in your google domain with GAT+

Frequently Asked Questions

Q: What events can trigger a User Security alert?

A: You can configure a User Security alert in GAT+ to notify you of several key events, including a user's password being changed, 2FA being disabled, external email forwarding being enabled, or a recovery email, phone number, or question/answer being changed on their account.

Q: How do I review the log of triggered alerts?

A: To review the logs, navigate to **GAT+ > Audit and Management > Alerts**. From there, you can apply a filter to view all alert events under the specific "Users Security" rule type.

Q: Can I customize the name of an alert rule?

A: Yes. The article states that you can customize the alert's name to differentiate between different alert types, even though it defaults to the alert type itself.

Q: Who receives the notification when an alert is triggered?

A: The alert recipients you select when you configure the rule receive an automated email notification. This can be the administrator who created the rule or any other person responsible for domain security.