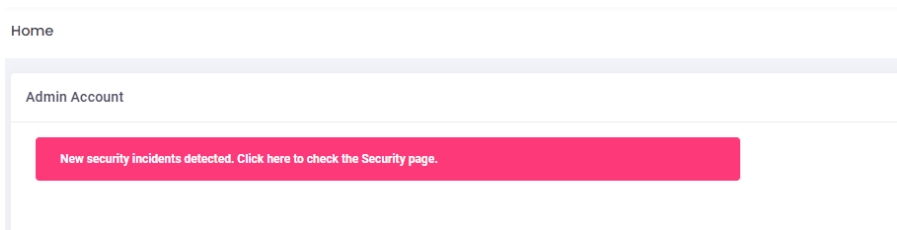


# Security Incidents

When you log in to the Admin Panel, on the Home page, you might see this warning message:

**New security incidents detected. Click here to check the Security page.**



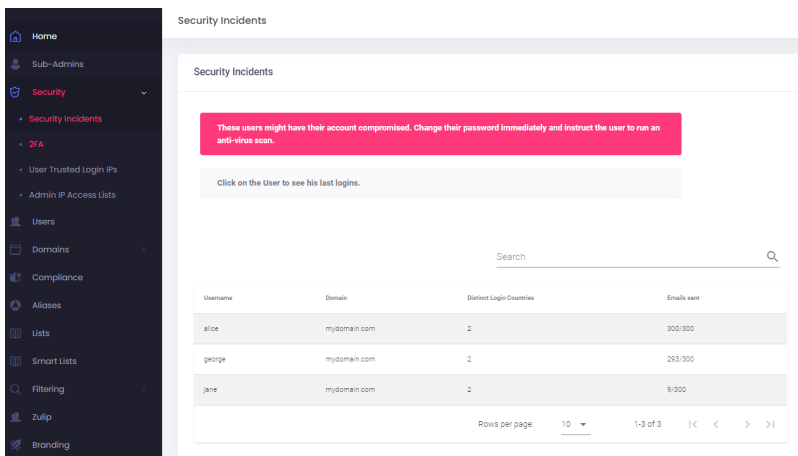
This happens when we detect suspicious logins from more than one location for one of your Users.

Click on the error message to go to the Security Incidents page and review each case.

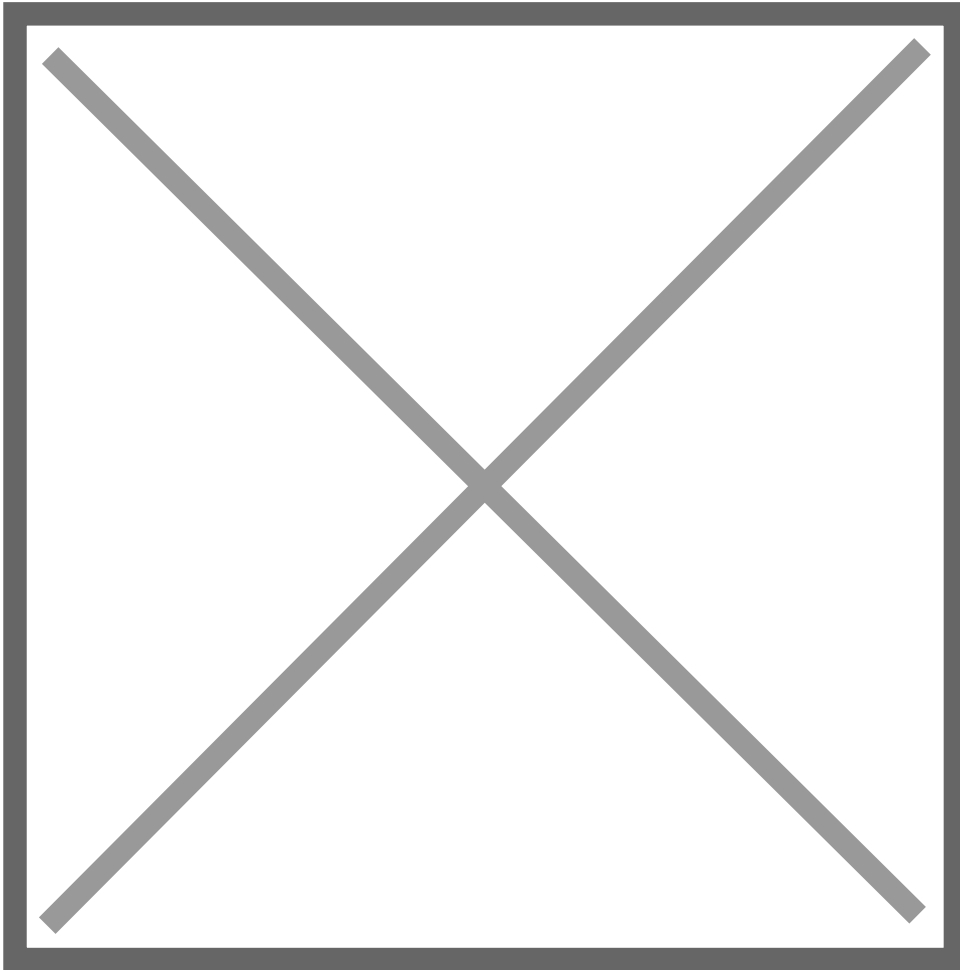
## How to review a Security Incident case

To review the security incidents:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **Security Incidents**; or click on the error message from the Home page.
- You will see a list of Users that have triggered the warning.



- Check how many messages were sent in the last 24 hours and the number of distinct login countries. A higher number might suggest a compromised account.
- Click on each user to see a list of their Last Logins. Contact the customer if you suspect the account was compromised.



## Possible reasons why the User is on the Security Incidents list

### Compromised account

The User's account was compromised and an attacker is sending emails on his behalf or accessing the contents of his emails. This might happen if the User doesn't use a strong password, has malware installed or accessed his account from an insecure location / device and threat actor intercepted their password.

### Third-party applications

Some applications that the User has setup will access the contents of his emails from different servers which will trigger the suspicious login warning. **You should inform the customer that the application has full access to their mailbox and make sure to read their Terms & Conditions about data processing.**

If the User is comfortable with the app having access to their data, you can follow the steps to **Mark IP as Safe.**

Some examples of such applications include:

- CRM applications (such as [Hubspot](#), [Salesforce](#), etc.)
- Sales automation applications
- Email clients (such as [Outlook](#), [MyMail](#), etc.) that read and process all the User's data through their servers. This includes your password in the clear(!) and all e-mail content

## User is traveling

A legitimate case is when the User is traveling and is logging in from new locations.

## Mobile connection

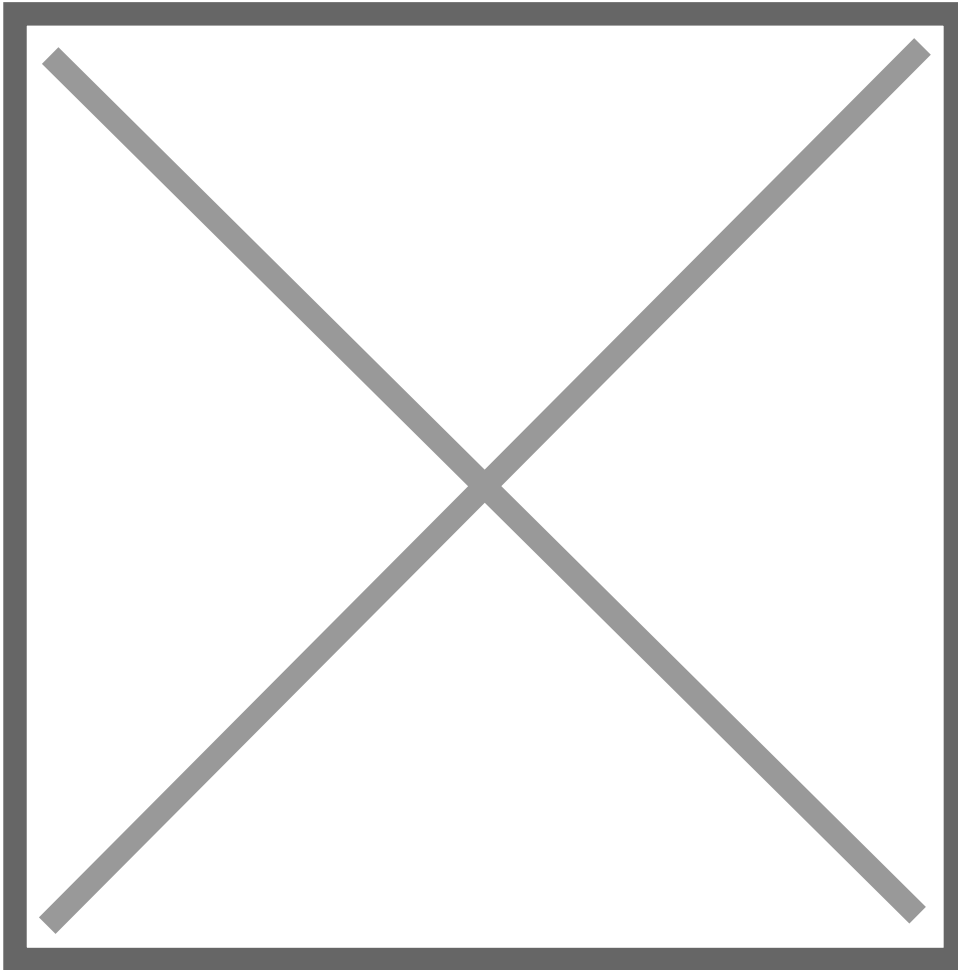
The User is accessing the service using a mobile connection that keeps renewing the IP.

## Mark IPs as safe

In case of legitimate use, the IPs can be marked as safe and will not trigger the Security Incident warning anymore.

To mark an IP as safe:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **Security Incidents**; or click on the error message from the Home page.
- Click on the User for which you want to mark an IP as safe. This will take you to his **Last Logins** logs.



- In the Last Logins logs, you can click on the **Mark as Safe** button next to the IP you want to whitelist.
- In the new pop-up, give a description to the IP (mandatory) and choose whether you want to mark as safe only the IP or the entire network (with options from /31 to /22)
- If you wish to whitelist all of Google's IPs, please set the Range to /17
- If you wish to whitelist all of myMail's IPs, please set the Range to /22



- Click on the **Mark as Safe** button to save the changes.
- You can remove an entry anytime.

---

Revision #1

Created 24 August 2024 14:13:19 by Support

Updated 24 August 2024 15:20:41 by Support