# **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.

Home	
Admin Account	
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.

this	page
	How to review a Security
	Possible reasons why the User is on the Security Incidents list
	Compromised
	I hird-party applications User is traveling
	Mobile connection Mark IPs as safe

On

## 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.

	Security Incidents										
(n) Home											
Sub-Admins	Security Incidents										
🗑 Security 🗸 🗸											
Security incidents	These users mish	them their account concerning.	thenne their naneword immediately and instru	et the uner to run en							
- 2fA	arti-vina scan.										
User Trusted Login IPs											
Admin IP Access Lists	Click on the User	o see his last logins.									
👥 Users											
Domains >			Search	Q							
🕐 Compliance											
Aliases	Usemane	domain	Distinct Legin Countries	Emails seet							
() Lista	alce	mydomalin.com	2	909/800							
() Smort Lists	Dec.De	mydomalin.com	2	293/300							
Q Filtering	jana	mydomain.com	2	8/300							
<u>県</u> Zuip			Rows per page: 10 -	1-8 of 8  < < > >							
🛷 Branding											

- 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.

ŵ	Home	cust togins							
\$	Sub-Admina	Last Login							
Ð	security >								
<u>19.</u>	Users								
8	Domains	mydome	n.com	•	1/5/2022			Dis Data	
ŧ¢	Compliance								
0	Alianes								
619	tists	Usem	ame	٠	alice			Negate Condition	•••
619	Smort Lists							_	
Q	filtering >							Se	arch Reset Search
<u>19.</u>	zulp	Usersame	Domain	Researce IP	Location	Password used	Service used	Date	Action
a	tranding	alce	mydomain.com	81.17.18.205	Spain	Main Password	imap	07/01/2023 01:14:58	Mark as Safe
۲	Settings	alce	mydornain.com	214 223 210 18	Spain	Main Password	imap	06/01/2223 21:08:33	0
cá	togs >	alce	mydornein.com	82.199.127.29	Spain	Main Password	imap	06/01/2225 15:15:59	Mark as Safe
		alce	mydomain.com	82,97,174,93	Netherlands	Leptop Mec	smb	06/01/2023 12:03:05	0
Ĩ						Rows per page:	10 +	1-4 of 4	$ \langle \langle \rangle \rangle \rightarrow  $

## 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.

~	Home	Last	Logins							
4	Sub-Admina		ant Lenine							
G	security >		ast cogins							
	Users									
	Domains >	mydomain.com			5141 Date			End Date		
	Compliance									
	Alians									
	tists		Usernar	ne	٠	alice			Negate Condition	•••
	Smort Lists								_	
	filtering >								Sea	rch Reset Search
	zuip		Usenane	Domain	Rostrato IP	Location	Password used	Service used	Dute	Aztian
	Branding		alce	mydomain.com	81.17.18.205	Spain	Main Password	imap	07/01/2023 01:14:58	Mark os Safe
	Settings		alce	mydomain.com	214 223 210 18	Spain	Main Password	Imap	06/01/2023 21:00:33	0 🖬
	Logs >		alce	mydomain.com	82.199.127.29	Spain	Main Password	imap	06/01/2023 15:13:59	Mark as Safe
			alce	mydomain.com	82,97,174,93	Netherlands	Leptop Mec	emtp	06/01/2023 12:03:05	©∎
							Rows per page.	10 -	1-4 of 4	$\langle \cdot \rangle \rightarrow \langle \cdot \rangle$

- In the Last Logins logs, you can click on the Mark as Safe button next to the IP you want to
- In the Last Logins logs, you can click on the **wark as sale** 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

Mark as Safe: 52.97.17	4.93	
Description		
Email-client		
Why do you trust this IP: name of	of the location, or the service.	
Range		
IP: /32	\$	
Choose if you wish to mark as s	afe the IP or the whole network	
	Cancel Mark as	Safe

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