

Security

- [2FA - Two-factor authentication](#)
- [Restrict Login Access: Admin IP Access Lists](#)
- [Security Incidents](#)
- [User Trusted Login IPs](#)

2FA - Two-factor authentication

Two-factor authentication, or **2FA** as it's commonly abbreviated, adds an extra step to your basic login procedure. Without 2FA, the password is your single factor of authentication: you enter your username and password, then you're done.

With 2FA, you log in to the Admin Panel by entering your username and password and the six-digit code provided by an app installed on your smartphone.

After the latest update of the Admin Panel, you will be prompted to enter the 2FA code in a new pop-up window.

Enable 2FA for the Admin Panel

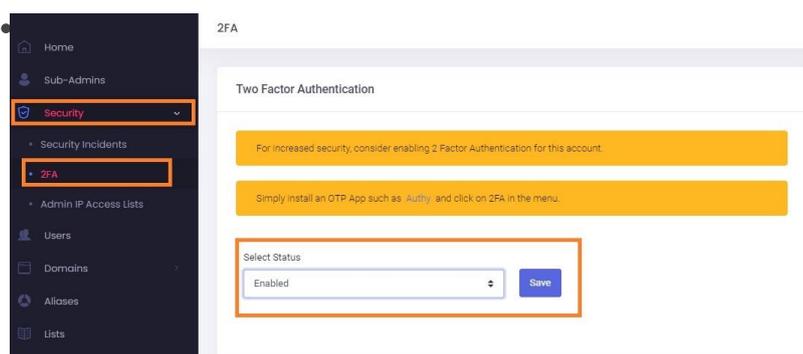
If you're using this Admin account as credentials for the API, the API login will fail after enabling 2FA. To solve this, create a Sub-Admin with special permissions for the API authentication only.

What you need:

- a smartphone with a 2FA App installed (OTP / 2-Step Verification / 2-Factor Authentication), such as [Authy](#) or [Google Authenticator](#).

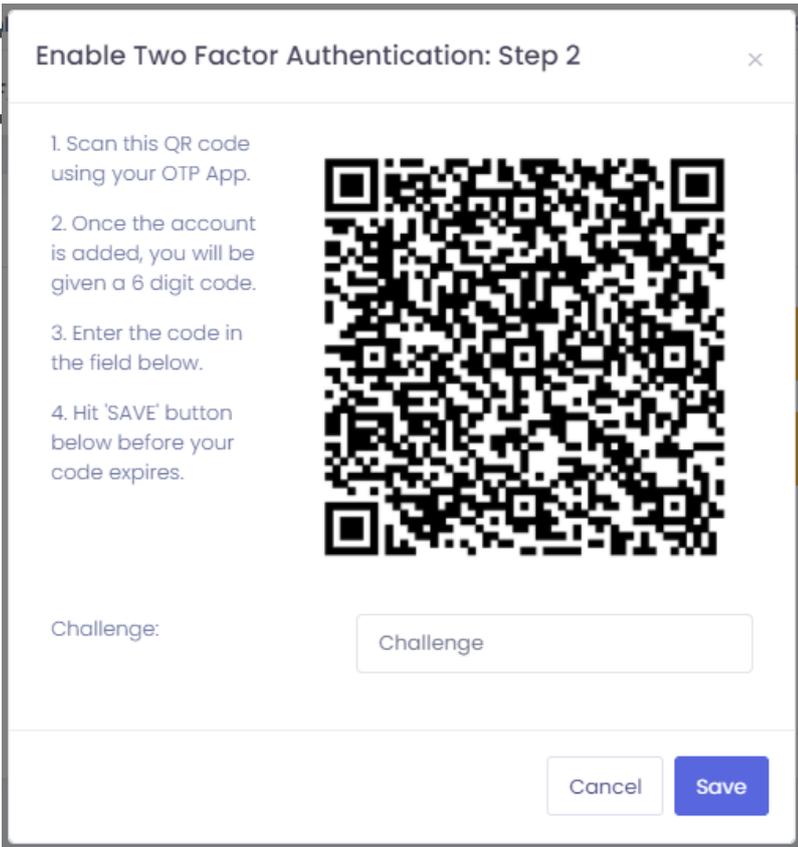
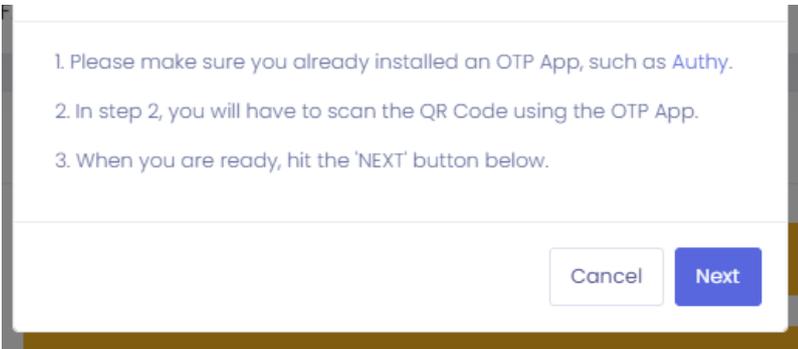
To enable 2FA for your Admin account:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **2FA**



on the **Save** button.

- Recheck the requirements: have a 2FA App installed on your phone.
- When ready, click on the **Next** button.



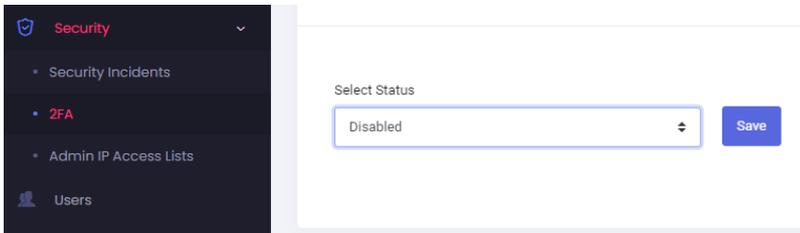
the generated six-digit code in the

es.

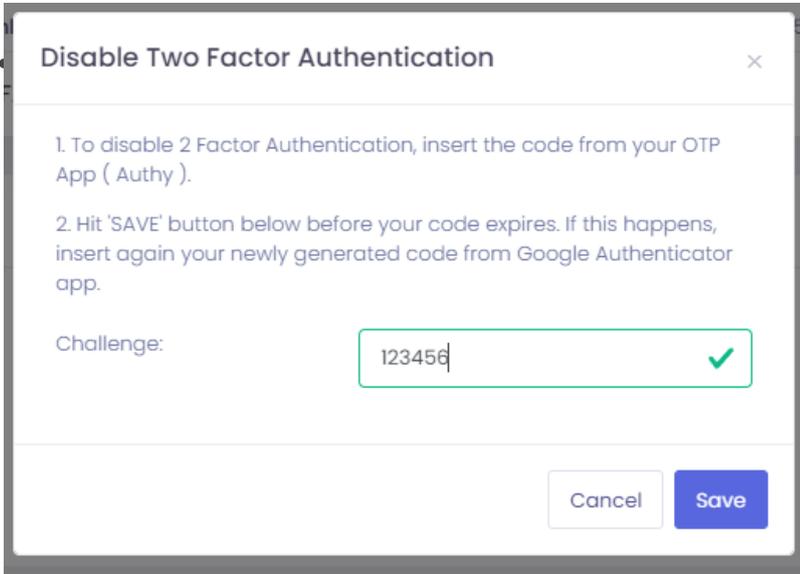
Disable 2FA for the Admin Panel

To disable the 2FA for your Admin account:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **2FA**
- Update the dropdown **Select Status** to **Disabled**. Click on the **Save** button.



- Insert the token from your 2FA App (such as Authy or Google Authenticator) in the



- After you see the confirmation message that the 2FA was disabled, you can delete the entry from your 2FA app.

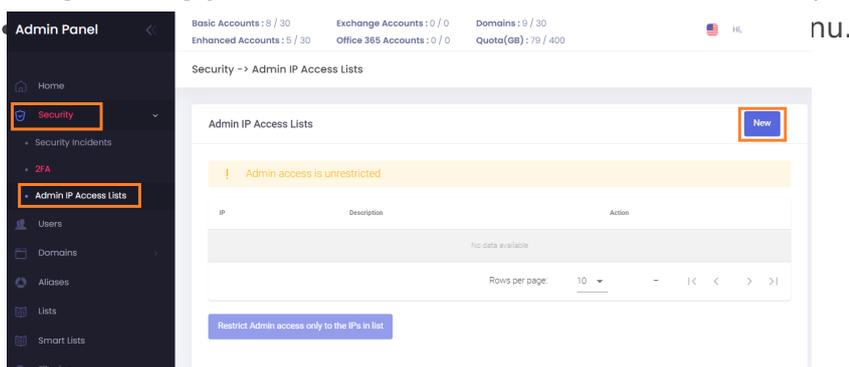
Restrict Login Access: Admin IP Access Lists

You can increase the security of your account by restricting login access for your Admin (or Sub-Admins) account to a list of know IPs, such as your office, your home, and server IPs for API or WHMCS authentication.

This feature works only with static IPs. Make sure your internet provider doesn't use dynamic IP addresses which change over time.

Add a new IP to the Access List

- Go to the [Admin Panel](#).
- Log in using your Admin (or Sub-Admin) username and password.



- Click on the **New** button.
- Fill in the IP and a description.
- Click on the **Add** button to save.

IP

Description

Cancel Add

Restrict Admin Login Access to only the IPs in the Access List

- Go to the [Admin Panel](#).
- Log in using your Admin (or Sub-Admin) username and password.

Security -> Admin IP Access Lists

Admin IP Access Lists

Admin access is unrestricted

IP	Description	Action
1.1.1.1	Office	
2.2.2.2	Server API	
3.3.3.3	Home Office	

Rows per page: 10 1-3 of 3

Restrict Admin access only to the IPs in list

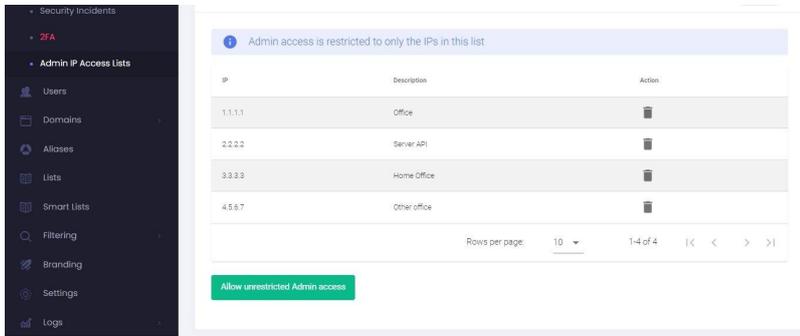
- Click on the **Restrict Admin access only to the IPs in list** button.

Restrict Admin access only to the IPs in list

Warning: make sure your IP is in the Admin IP Access List. Otherwise, you might lock yourself out.

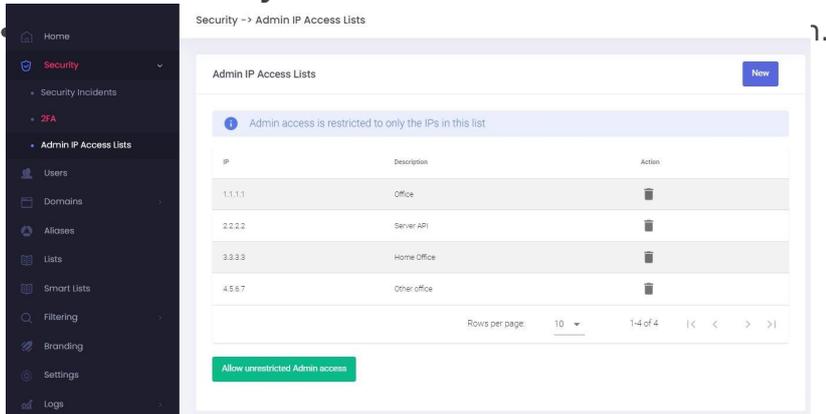
Cancel Restrict

- Access is now restricted to the IPs in your list:



Allow unrestricted access for Admin (or Sub-Admin)

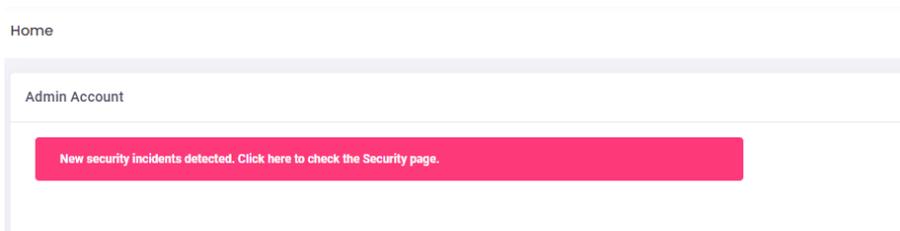
- Go to the [Admin Panel](#).
- Log in using your Admin (or Sub-Admin) username and password.
- Click on **Security** → **Admin IP Access Lists** in the menu.



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.



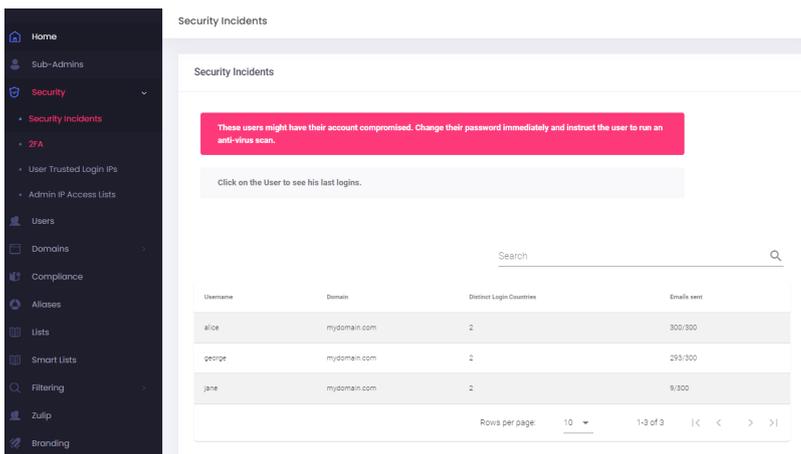
This happens when we detect suspicious logins from more than one location for one of your Users.

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

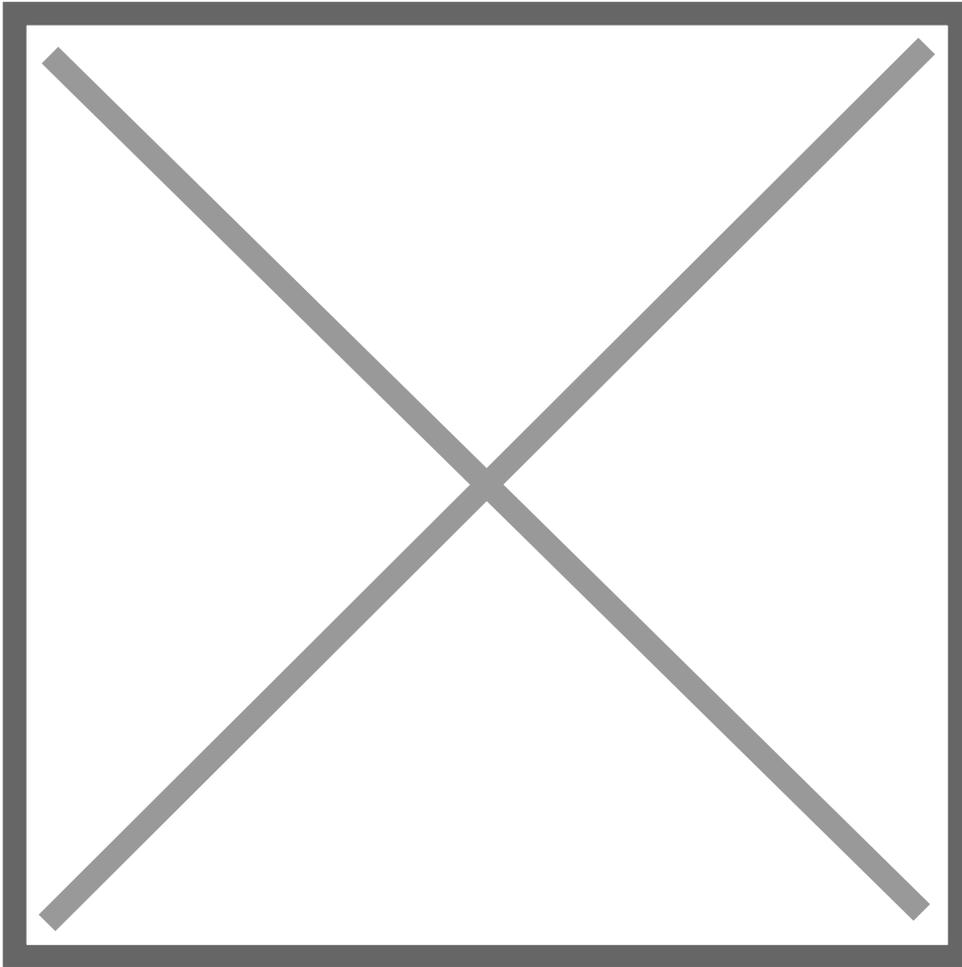
How to review a Security Incident case

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

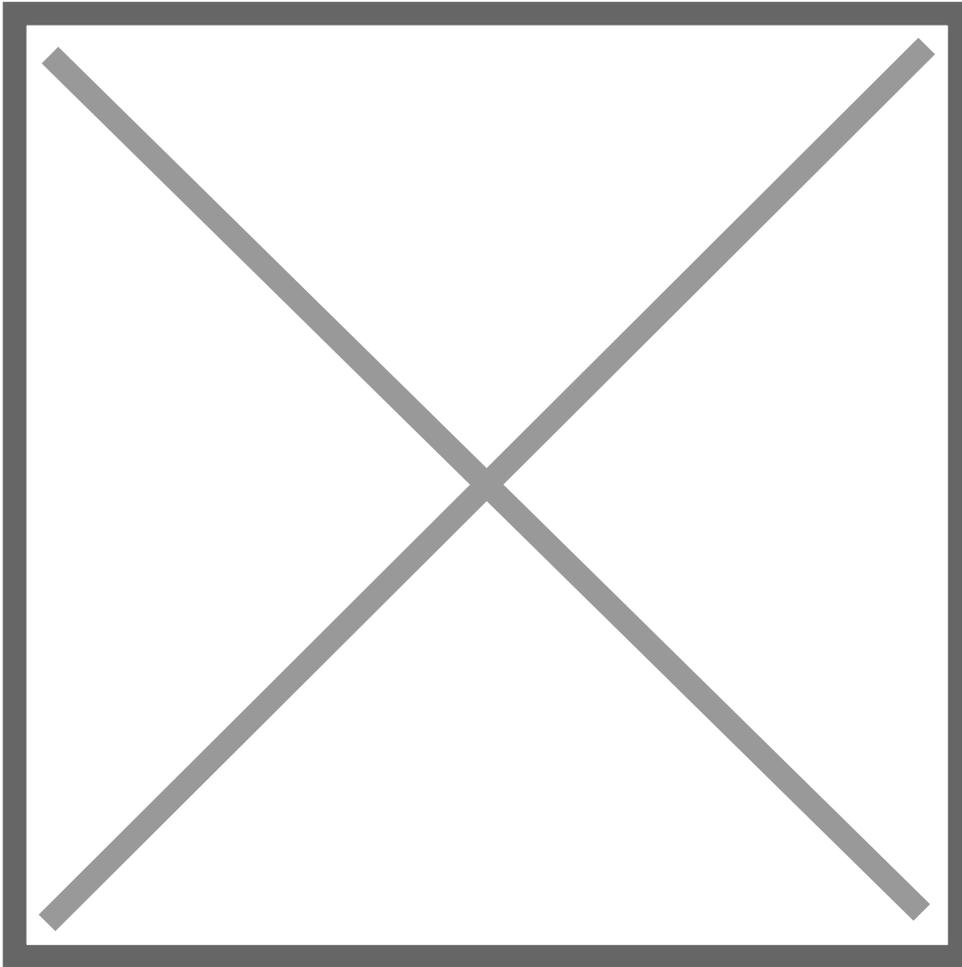
The User is accessing the service using a mobile connection that keeps renewing the IP.

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.

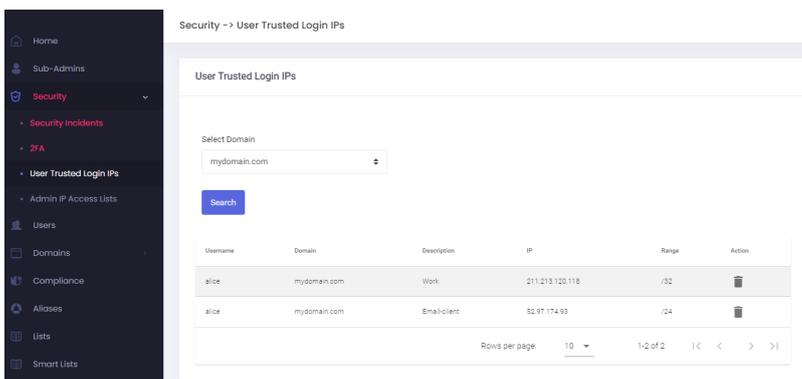
User Trusted Login IPs

You can mark as safe the IPs that your Users log in from. Use the Mark as Safe feature whenever a Security Incident is considered as safe - logins from the safe IP will not trigger Security Incident warning anymore.

Manage User Trusted Login IPs

To manage the User trusted login IPs for an account:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security** → **User Trusted Login IPs**
- Select the domain from the dropdown and click on the **Search** button.
- A list of all trusted IPs that were previously Marked as Safe will show.



- You can delete an entry at anytime
- To add a new trusted IP, [follow these steps](#).