Security

- 2FA - Two-factor authentication
- Restrict Login Access: Admin IP Access Lists
- Security Incidents
- User Trusted Login IPs
- Secure API Setup Guide

2FA - Two-factor authentication

> **Two-factor authentication (2FA), also known as multi-factor authentication (MFA) is mandatory for all Admin and Sub-admin accounts that do not have IP-based login restrictions.**

Setting Up Mandatory Two-Factor Authentication (2FA)

Two-factor authentication (2FA), also known as multi-factor authentication (MFA), adds an extra step to your basic login procedure. Without 2FA, the password is your single factor of authentication. 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.

Because this security measure is now mandatory for all accounts without IP restrictions, you will be prompted to enable 2FA for the account upon logging in, if it is not already active.

Enable 2FA for the Admin Panel

> If you're using this Admin account as credentials for the API, WHMCS, or similar integrations, the API login will fail after enabling 2FA. To solve this, create a Sub-Admin with special permissions for the API authentication only.
>
> **Click here for more details on secure API setup.**

Phase 1: Download an Authenticator App

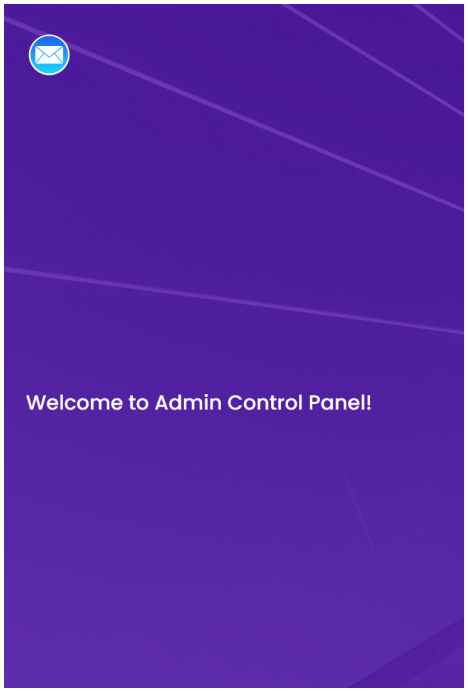
Before you can scan the barcode on your computer screen, you need the correct software on your mobile device. You must have a smartphone with a 2FA App installed, such as Authy or Google Authenticator.

1. Open the app store on your smartphone.
2. Search for and download a free authenticator app like Authy or Google Authenticator.
3. Open the app on your phone and look for an option to add a new account or scan a QR code.

Phase 2: Connect Your Account

Once the app is ready on your phone, return to your computer screen to complete the enrollment.

1. Locate the square barcode, known as a QR code, displayed on your **Admin Panel** setup page.
2. Scan the QR code with the installed 2FA App. Point your smartphone camera at the computer screen.
3. Look at your smartphone screen. The app will generate a six-digit code.
4. Fill in the generated **six-digit code** in the **Your code** input field from the Admin Panel.





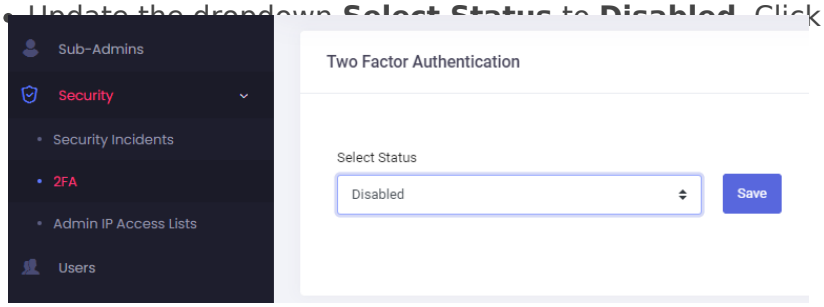
5. Click on the **Verify and continue** button before your token expires. The numbers in your authenticator app refresh automatically every 30 seconds.

Disable 2FA for the Admin Panel

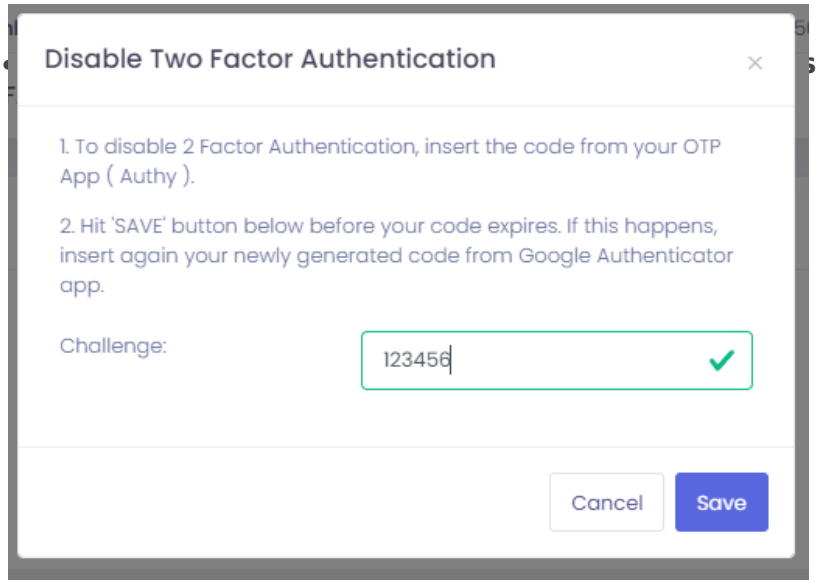
> You can only disable 2FA if your Admin login is restricted to specific IP addresses. If your login access remains unrestricted, 2FA is mandatory and cannot be disabled.
>
> Before proceeding, please ensure you have configured your IP restrictions. You can learn how to do this in our guide on Restricting Login Access via Admin IP Access Lists.

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.

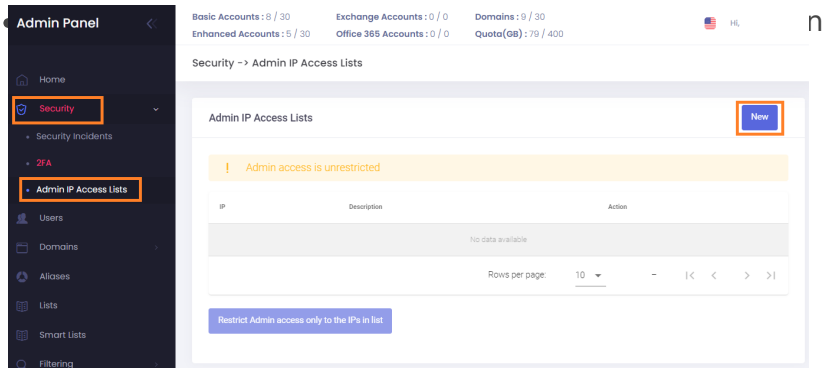
Restrict Login Access: Admin IP Access Lists

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.



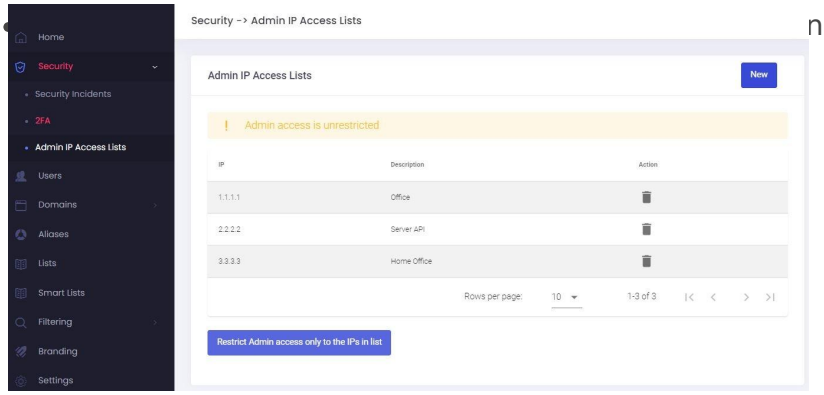
nu.

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

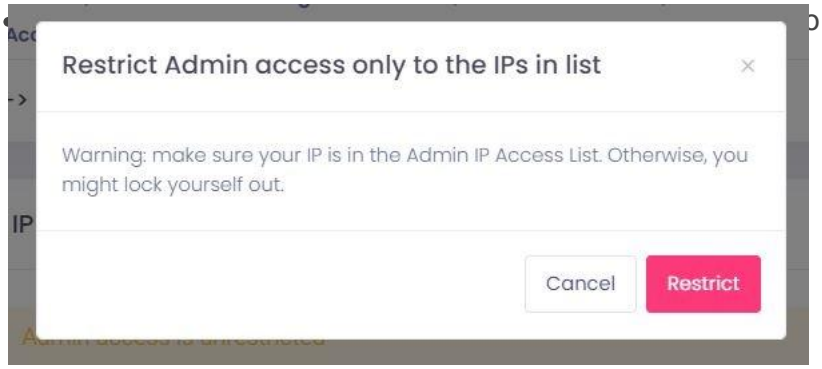


Restrict Admin Login Access to only the IPs in the Access List

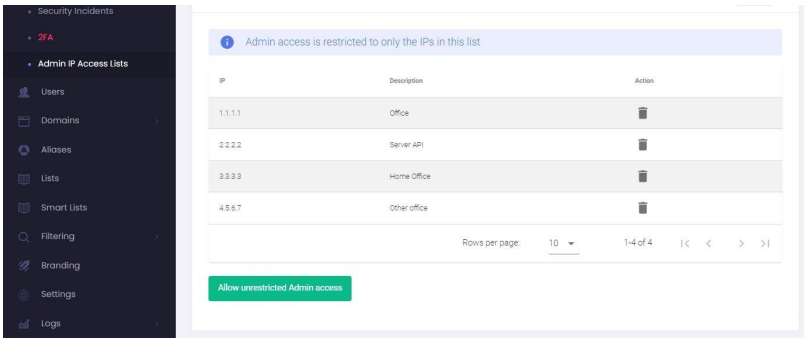
- Go to the Admin Panel.
- Log in using your Admin (or Sub-Admin) username and password.



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

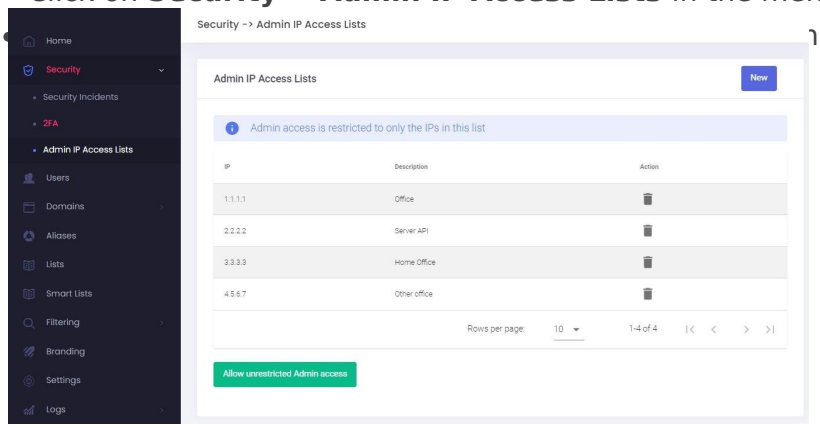


- Access is now restricted to the IPs in your list:



Allow unrestricted access for Admin (or Sub-Admin)

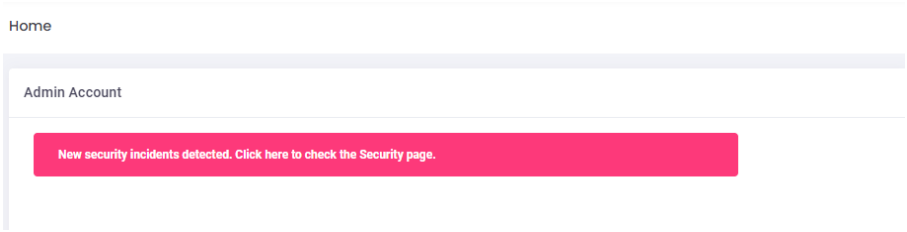
- Go to the Admin Panel.
- Log in using your Admin (or Sub-Admin) username and password.
- Click on **Security → Admin IP Access Lists** in the menu.



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.



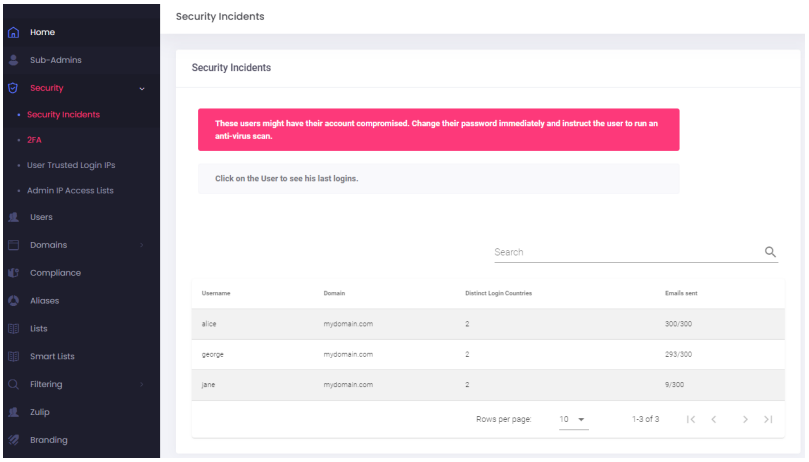
This happens when we detect suspicious logins from more than one location for one of your Users.

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

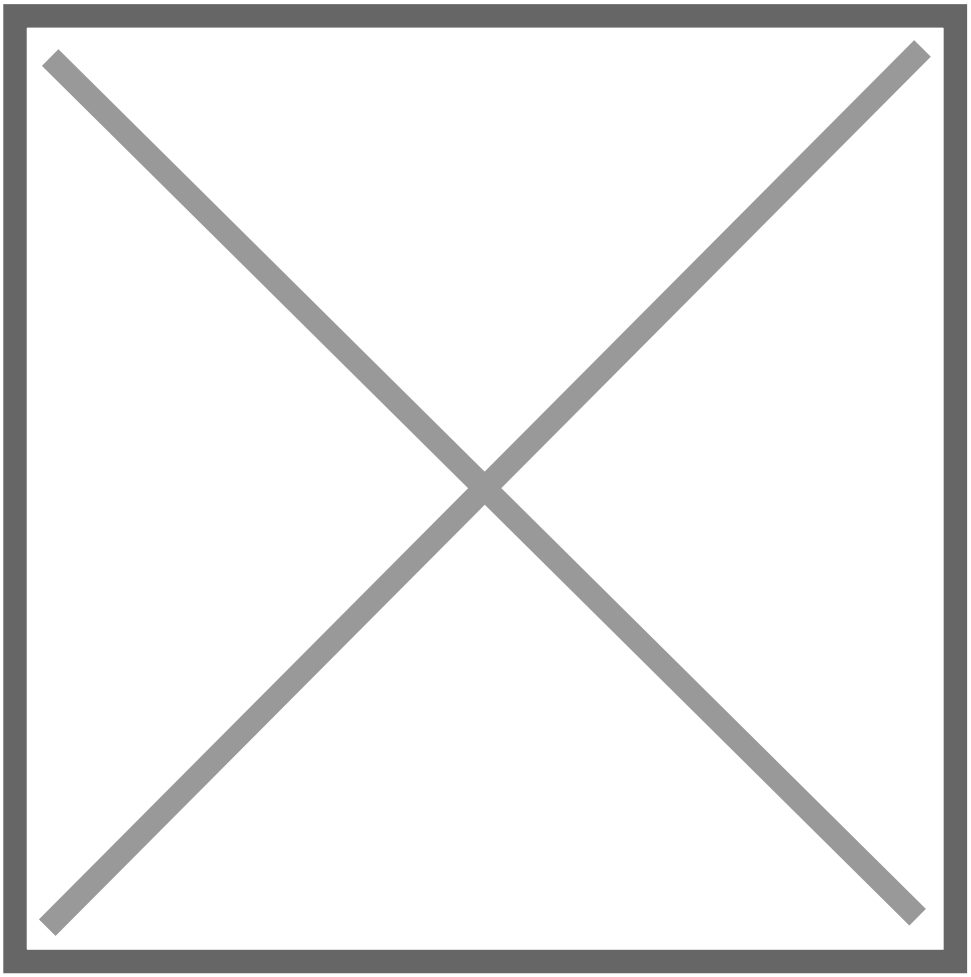
How to review a Security Incident case

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. To prevent the system from triggering security warnings during their trip, you can temporarily enable **Travel Mode**.

To turn on Travel Mode:

1. Go to **Users**.
2. Select the user you want to edit.
3. Click on **More options**.
4. Set **Travel mode** to **Yes**.

For more details, please see the Manage Users guide.

> **Security Warning:** When Travel Mode is active, you will not be notified of foreign access to this account. Disabling this security feature is potentially dangerous, so please ensure you turn it back off as soon as the user returns.

Mobile connection

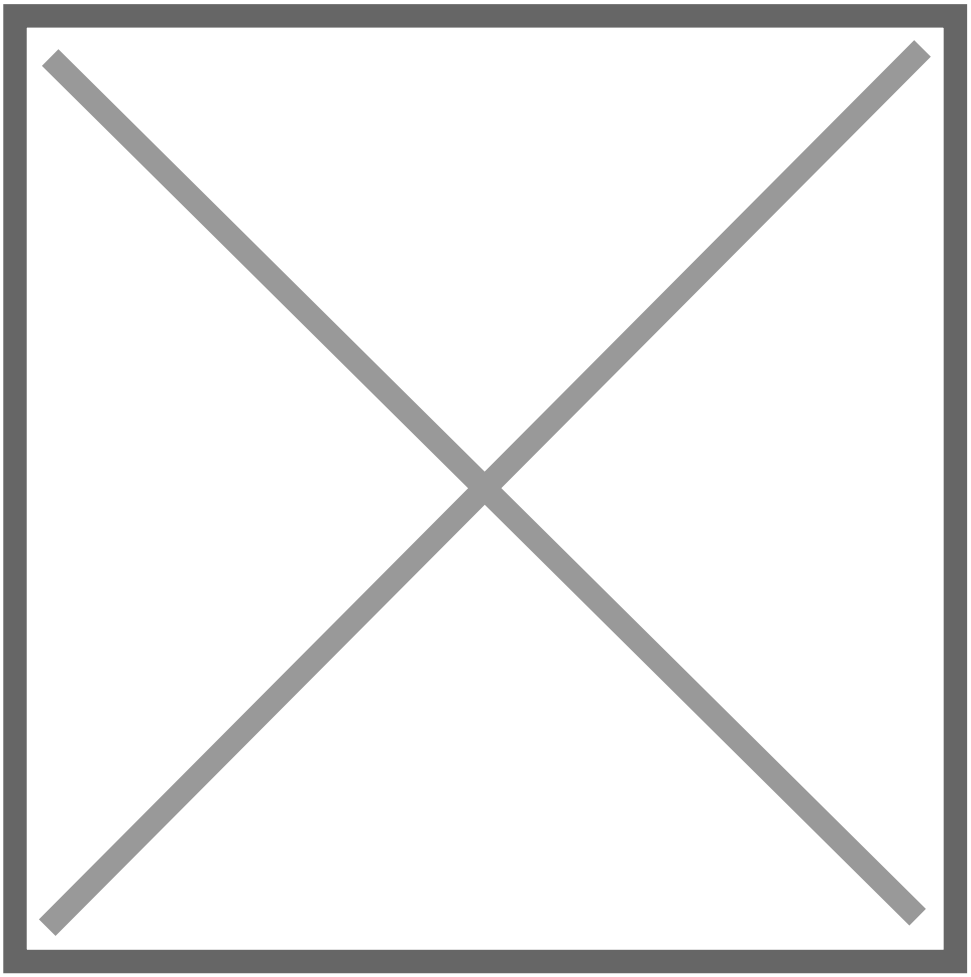
The User is accessing the service using a mobile connection that keeps renewing the IP.

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.

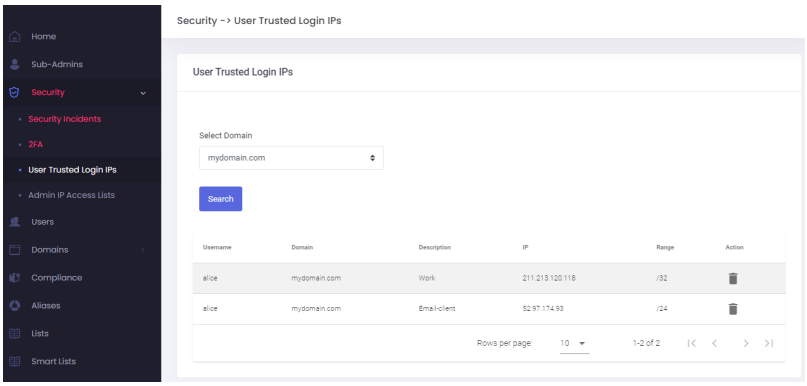
User Trusted Login IPs

Maintain seamless access for your users while keeping your infrastructure secure. The **User Trusted Login IPs** feature allows you to whitelist specific IP addresses used by your team or clients, ensuring that legitimate logins from known locations are never interrupted. By marking an IP as "Safe," you prevent future security incident warnings for that specific source, allowing for a smoother user experience without compromising enterprise-grade protection.

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 to **mark IP as safe**.

Checking and Unblocking IP Addresses

If a user is unable to connect, it may be because their IP address has been temporarily restricted due to security protocols. You can check the status of an IP and mark it as "Safe" directly from the management panel.

How to Check if an IP is Blocked

- Navigate to the **Security → User Trusted Login IPs** section in your panel.

- Enter the specific **IP address** into the search field.
- If the IP is restricted: An option to **Mark as Safe** will appear.

Adding an IP to the Safe List

When you choose to mark an IP as safe, a configuration window will open. To ensure the security of the account, please provide the following details:

- **Domain & Username**: Select the specific domain and user account this rule should apply to.
- **Description (Required)**: Provide a brief note (minimum 2 characters) explaining why this IP is trusted, such as the office location or the specific service name.
- **Range**: Choose whether to whitelist only the specific Remote IP (/32) or the entire network range.
  - **Single IP (/32):** Use this for individual users working from a fixed location, like a home office with a static IP. It is the most secure option because it only whitelists one specific address.
  - **IP Range (Network):** This is ideal for larger corporate offices where many employees share a single network. Mark the whole network as safe to prevent repeated blocks for different users in the same building.

> **Security Note:** Only whitelist an entire range if you are certain the network is private and managed. Whitelisting large public ranges can leave accounts vulnerable to unauthorized access from other users on that same network.

Once submitted, logins from this IP will no longer trigger security warnings or connection blocks for that user.

Secure API Setup Guide

To integrate with our API safely, authentication must be handled through a dedicated Sub-Admin account rather than your primary Admin account. For maximum security, Multi-Factor Authentication (MFA) is mandatory on all Admin and Sub-Admin accounts unless they have an active IP restriction enabled.

Since automated API scripts cannot easily process MFA prompts, you must secure your API Sub-Admin by restricting its login access to the specific IP addresses of your connecting servers.

Follow these steps to create your Sub-Admin, whitelist your server IPs, and lock down the account securely.

Step 1: Create a Dedicated Sub-Admin

A Sub-Admin is a specialized account that allows you to delegate administrative tasks while protecting your primary credentials.

1. Go to the Admin Panel and log in using your main Admin username and password.
2. Click on **Sub-Admins** in the menu, then click the **New** button.
3. Fill in the details for the new account, including the username, password, email address for password recovery, and full name.
4. Select the appropriate permissions for each section. Assign only the level of access required for your specific API integration.
5. Click the **Add Sub-admin** button to save.

Note: Once you have created your API Sub-Admin, please email our Support Team to enable unlimited email account creation for that specific Sub-Admin. Without this step, the Sub-Admin will be limited by the resources of your current subscription.

Step 2: Add Your Server IP to the Access List

Next, you need to tell the system which IP addresses are allowed to log in to this new account. Please ensure your server uses a static IP address, as this feature does not work with dynamic IPs that change over time.

1. Log out of your main account, then log in to the Admin Panel using your new Sub-Admin username and password. After you log in with your Sub-Admin account, the system will prompt you to enable MFA. This is mandatory until you restrict the login to specified IPs.
2. In the menu, click on **Security** and then select **Admin IP Access Lists**.
3. Click the **New** button.
4. Enter your server's IP address and a brief description.

5. Click the **Add** button to save the IP to your list.
6. Note: Be sure to add your office or local IP address to the access list as well. This ensures you can still log in directly to the Admin Panel as the Sub-Admin if you need to manage settings manually.

Step 3: Restrict Login Access

Finally, you must enforce the IP restriction so the Sub-Admin can only be accessed from your approved list.

1. While still logged in as the Sub-Admin, navigate back to **Security** and then **Admin IP Access Lists**.
2. Click the button labeled **Restrict Admin access only to the IPs in list**.
3. Read the warning prompt and click the **Restrict** button to confirm.

Once enabled, login access is restricted strictly to the IPs on your list.

Step 4: Disable Multi-Factor Authentication (MFA)

Once login access is restricted to your approved IP list, you can disable MFA for the Sub-Admin account so your automated API scripts can connect without interruption.

1. While logged in as the Sub-Admin, go to **Security** and select **Two-Factor Authentication** in the menu.
2. Click the option to disable Two-Factor Authentication.
3. Confirm your choice to save the change.

Note: The option to disable MFA is only available after you have restricted login access to your specified IPs. If login access remains unrestricted, MFA is mandatory and cannot be disabled.