

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.

Revision #3

Created 29 October 2026 14:59:00 by Admin

Updated 29 October 2026 15:27:52 by Admin