Security Settings: Login Restrictions

Last Modified on 09/17/2019 2:15 pm PDT

You have the ability to configure security settings on your account that affect all admins. These settings include requiring sub-admins to set up two-factor authentication and login restrictions. For more information on how to require admins to set up two-factor authentication click here.

Login restrictions allows you to restrict account access depending on the location they are accessing from. This is useful if you want your account to only be accessed in the office, or on a private network IP and dedicated VPN. (Note: if you do not want sub-admins to be able to edit this section, you will need to remove this privilege from their account)

To set this up:

- Click Manage Admins from the side navigations then Security & Notification > Login Restrictions

You have the following options for login restrictions:

Country Restrictions:
- **Standard Security**: allow login access from all countries and receive email notifications when they are outside of your country and whitelisted countries.

- **High Security**: block all logins outside of your country and whitelisted countries.

**State Restrictions:**

- **Standard Security**: allow login access from all states and receive email notifications when they are outside of your state and whitelisted states.

- **High Security**: block all logins outside of your states and whitelisted states.

**IP Restrictions**

- **Standard Security**: allow login access from any IP addresses.

- **High Security**: block all logins from all IP addresses except your whitelisted IPs.
Don't forget to click **Save** after making any changes!