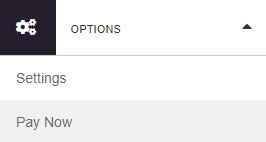
# **IP Restrictions Setup**

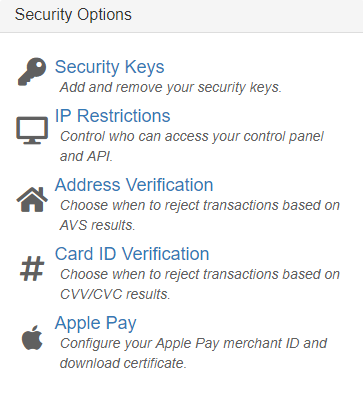
IP Restriction is a tool that is provided within the merchant portal to ensure that a merchant’s account cannot be accessed outside of the desired IP address(es) or IP ranges. It allows you to “White-List” a group of IPs your administration team or applications may communicate from, providing you the ability to add any IP you wish to grant access to (either the control panel or a website).

## **Setup/Functionality Instructions**

To set up an IP Restriction on a merchant account, you will first need to log in, click on Options, and then Settings.



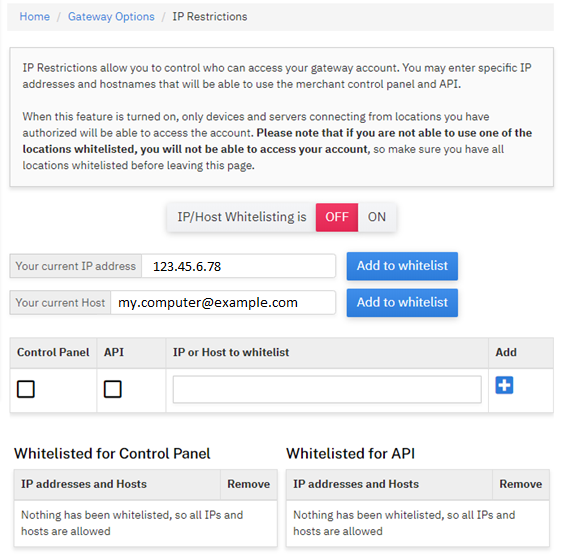
Once you are in settings, under the heading “Security Options”, click on “IP Restrictions”.



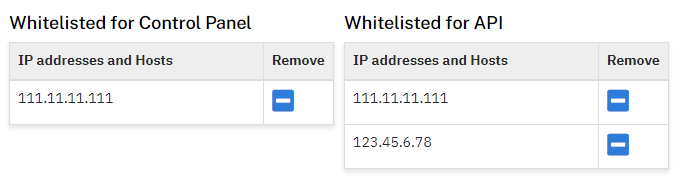
Next, you will want to take the IP address and/or range used to access your account and enter this into the text box under the “IP or Host to whitelist” column. For those who are not sure of what their current public IP Address is, you will notice that it will be shown on the page next to “Your current IP address”. If you click on the “Add to whitelist” button, it will populate your current IP Address into the box under “IP or Host to whitelist”.

There are also two checkboxes shown next to each IP address/range entry to configure which component you wish to restrict access to:

* Control Panel (where you are currently logged in)
* API – Website/Application Access
  + Configuring any “API” restriction will disallow transactions sent from a system whose IP Address has not been explicitly whitelisted. All systems that interact with the API should be configured to be allowed access.



When you have completed these settings, click on the '+' under the “Add” column to add the IP allowance. Based on the settings selected, the IP address/range configured will be populated under the “Whitelisted for Control Panel”, “Whitelisted for API”, or both.



Based on the above example, the IP “111.11.11.111” would be allowed to interact with the Control Panel and API, where the IP “123.45.6.78” would only be allowed to interact with the API.

Once the appropriate IPs/Hosts have been added, click the ‘ON’ button next to “IP/Host Whitelisting is” to toggle the service on.

|  |  |
| --- | --- |
| **Disabled** | **Enabled** |

After IP Restrictions have been enabled, any attempt to log in or send transactions from a server or IP that has not been white-listed will produce an 'Authentication Failed' message, regardless of the accuracy of the credentials.

A merchant can add as many IP addresses or IP ranges as they want.

### **Notes**

Restrictions are activated when at least one IP address has been added for the method of connection. For example, if four IP addresses are added for the Control Panel, but no IP addresses are added for the API, then Control Panel access will be limited but the API access will not.