

How to prevent an IP address from being Blocked/Blacklisted

Luminate Online block an IP Address if there is an unusually high volume of donor activity from the same IP address, especially for a virtual food drive. This is a security measure to help prevent carding runs (fraud). The default setting is 5 declines within a 30-minute period (*it used to be after 3 declines*) will result in a block on that IP address for 4 hours.

Adding an IP address to the Allowlist means you are deliberately accepting traffic to and from a particular IP address. An example of when adding an IP address to the Allow list might be appropriate would be if numerous donations were being accepted on the same workstation during a virtual food drive or eventathon. Each of these donations would be using the same IP address and run the possibility of being found as fraudulent. If the IP address is on the BBPS/BBMS Allowlist, no donations will be declined due to high traffic using that IP address.

For the reasons stated above, it is highly encouraged that you gather as much info as you can from the company who may have high volume and let Cindy Shanks know before their fundraising event to whitelist the IP addresses that will be taking donations. She will work with Blackbaud's server team to ensure the IP address is allowed on the Blackbaud's hosted servers.

Information needed for IP(s) address to be place on the Allow list:

- IP(s) addresses to be placed on the Allow list.
- The source of this IP address (office network, event space, etc.)
- The purpose of the Allow list request.
- Start and End Date for the requested IP(s) address.

Please allow two to seven days prior to the requested Start Date to request the Allowlisting. A minimum of two business days is needed to set up the Allowlisting. The IP addresses will be removed from the Allowlist the day after the conclusion of the event/End Date.

You will need to provide their **public IP address**, and not an internal one. They can determine their public IP address by simply going to Google and searching "What is my IP address." The first result will be their public IP address. Private IP addresses will be in the following ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 – 192.168.255.255. Be sure that IP you are requesting is a static IP, (e.g., their organization's IP) rather than a dynamic IP (e.g., the IP of a donor or an employee using their home network).

Note: Dynamic IP addresses cannot be whitelisted. IP addresses for home/residential internet service are normally dynamic and will not be whitelisted. Dynamically assigned IPs may change or be reassigned without notice or warning. If a dynamic IP address were to be whitelisted and was then reassigned, the organization user (whose IP changed) would no longer be whitelisted and would again be subject to automatic blocking to prevent fraud and this would leave an unknown user with an IP address that could be potentially used for abuse and not subject to normal fraud prevention.