

Allow List

<https://campus.barracuda.com/doc/98225903/>

The **DDoS > Allow List** enables you to add the IP address(es) or IP address ranges for which you want to exempt DDoS policy validation.

The IP address(es) configured under DDoS policy are exempted *ONLY* from DDoS validation. Other security validations such as protection from SQL injection and parameter limits, etc are enforced on the request. If you want to bypass all validations, use the **Trusted Hosts** component.

To Add an IP Address to the Allow List

1. On the WAF-as-a-Service web interface, go to the **APPLICATIONS** page and click on the application to which you want to add an IP address.
2. On your application page, click **DDoS** in the left panel and then click **Allow List**.
3. On the **Allow List** page, click **ADD IP ADDRESS**.
4. On the **Add to Allow List** window:
 1. **IP Address** – Enter the IP address or network range for which you want to exempt DDoS policy validations.
 2. **Netmask** – Enter the associated netmask for the IP address or network range.
 3. Click **Add**.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.