## **IP Blocklist**

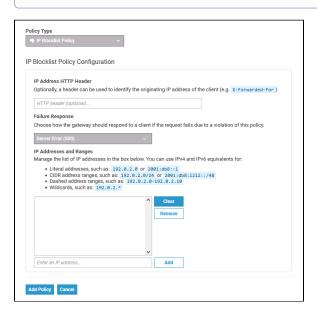
The **IP Blocklist Policy** blocks access to the resource of an API based on the IP address of the client. Users are able to use wildcard characters in specifying the IP addresses to be blocked. In addition, you have the option of specifying the return error code sent in the response to the client if a request is denied.



An IP Blocklist policy overrides an IP Allowlist policy.



Before PAS 22.1.1 the name of this policy was **IP Blacklist**. Existing policy configuration will be shown with the old name.



## On this Page:

Configuration Options

## **Related Pages:**

- Policies
  - Assigning Policies
    - Policy Configuration

## **Configuration Options**

Option	Туре	Description	Possible Values	Default
IP Address HTTP Header	String	Optional. Tells the API Management to use the IP address found in the given HTTP request header <b>instead</b> of the one associated with the incoming TCP socket.  In the default setup the gateway runs behind a proxy. In the default scenario there is no need to add the header X-Real-IP in the custom header field IP Address HTTP Header.	-	-
Failure Respons e	Enum	The server response code.	Authenticatio n Failure (403) Not Found (404) Server Error (500)	None

Enter an IP   [ <iplist [<iplist="" address="" array="" th=""  =""  <=""><th>Literal addres ses CIDR addres s ranges (netma sks) Dashed addres s ranges Wildcar ds</th><th></th></iplist>	Literal addres ses CIDR addres s ranges (netma sks) Dashed addres s ranges Wildcar ds	
---	---	--