BLOCKLIST

The **IP Blocklist Policy** blocks access to an API's resource based on the IP address of the client. The user must specify the IP address ranges to be excluded from being able to access the API. Any addresses that are not explicitly excluded are able to access the API. It is possible to use wildcard characters to specify the IP addresses to be blocked. It is also possible to define the return error code sent in the response to the client in case a request fails due to the violation of this policy.

> ⚠️ An IP Blocklist policy overrides an IP Allowlist policy.

Configuration Options

Basic Configuration

Option	Description	Possible Values	Default
Failure Response	Select how the gateway should respond to a client if the request fails due to a violation of this policy.	- Authentication Failure (403) - Not Found (404) - Server Error (500)	Server Error (500)
IP Address Rule	The IP address(es), and/or ranges of addresses that will be blocked from accessing the API. IPv4 and IPv6 are supported.	valid IP formats such as: - Literal Addresses: **192.0.2.0** or **2001:db8::1** - CIDR Address Ranges: **192.0.2.0/24** or **2001:db8:1212::/48** - Dashed Address Ranges: **192.0.2.0-192.0.2.10** - Wildcards: **192.0.2.***	-
Click **Add** to create more rows in the table. Click **Delete** to remove selected rows.			

Advanced Configuration

Option	Description	Possible Values	Default
IP Address HTTP Header	Optional. The header can be used to identify the original IP address of the client. ⓘ The PAS gateway runs behind a proxy. There is no need to add the header **X-Real-IP** in the custom header field **IP Address HTTP Header**.	a string	-