+++ title = "Request security" description = "Grafana Enterprise request security" keywords = ["grafana", "security", "enterprise"] weight = 400 +++

Request security

> ***Note:*** *Available in Grafana Enterprise v7.4 and later versions.*

Request security makes it possible to limit requests from the Grafana server, and it targets requests that are generated by users.

For example:

- Data source metric queries
- Alert notifications

This can be used to limit access to internal systems that the server Grafana runs on can access but that users of Grafana should not be able to access. This feature does not affect traffic from the Grafana users browser.

> ***Note:*** *Although request security works with backend plugins, you can create a backend plugin that bypasses this security.*

IP and hostname blocking

You can limit requests based on a hostname, an IP address, or both.

Deny list

Grafana blocks any request to a hostname or IP address on the deny list.

Allow list

If there is at least one entry on the list, then any request to a hostname or IP address not on the list is denied.

For example:

```
[security.egress]
# A list of hostnames or IP addresses separated by spaces for which requests are blocked.
host_deny_list = supersecret.internal 192.168.1.10
# a list of hostnames or IP addresses separated by spaces for which requests will be allowed, all other requests will be blocked
host_allow_list = prometheus.internal
```

Drop headers and cookies

You can set a list of cookies or headers that are to be dropped from outgoing requests.

Example:

```
[security.egress]
# a list of headers that will be stripped from outgoing datasource and alerting requests
header_drop_list = user
```

```
# a list of cookies that will be stripped from outgoing datasource requests (case
sensitive)
cookie_drop_list = session_id
```