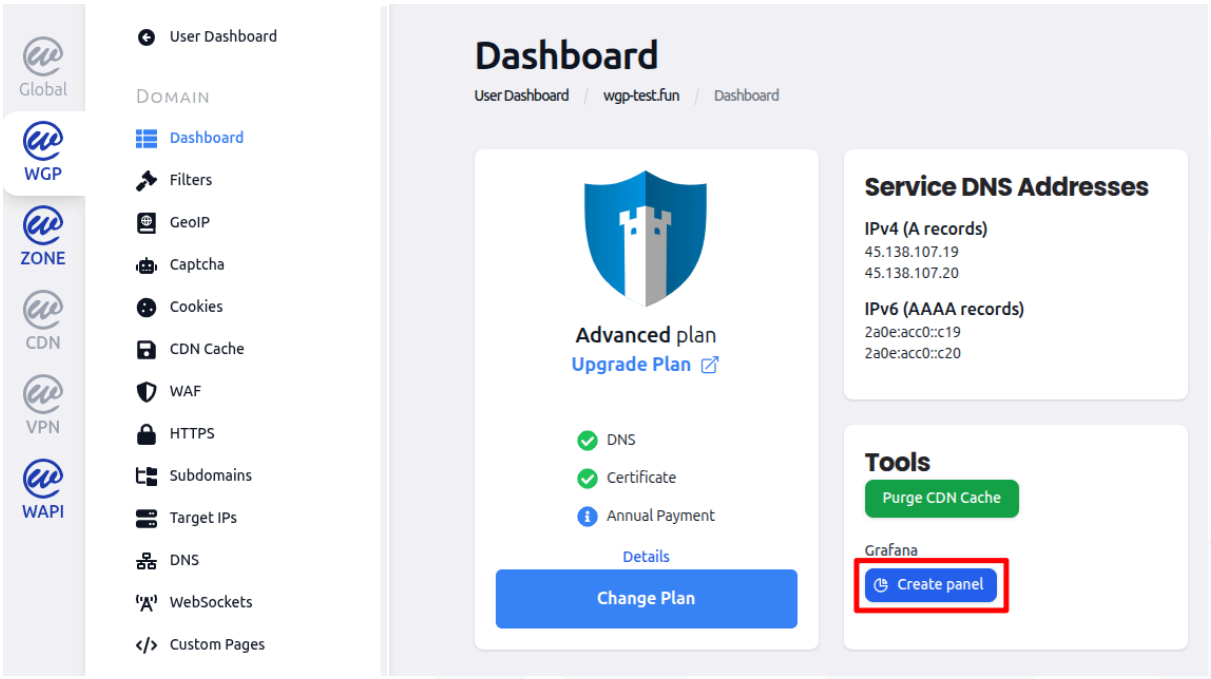
How to Access and Use Grafana

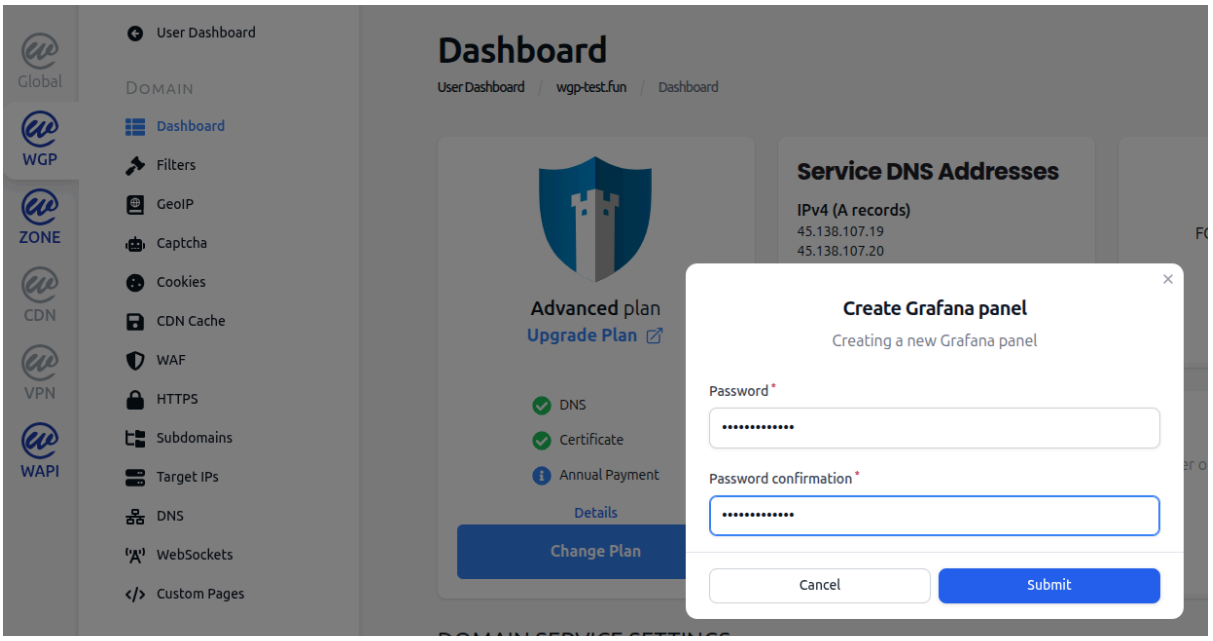
Grafana is a powerful visualization tool integrated with WEDOS.protection that provides extensive traffic statistics and logs. It allows you to monitor live traffic, analyze historical data, create detailed reports, and better understand request patterns, client behavior, and potential security events.

To start using Grafana with your WEDOS Protection account:

1. Log in to WGP at https://client.wedos.global.
2. Select any domain protected with WEDOS.protection.
3. In the **Tools** section of the dashboard, click **Create Panel**.

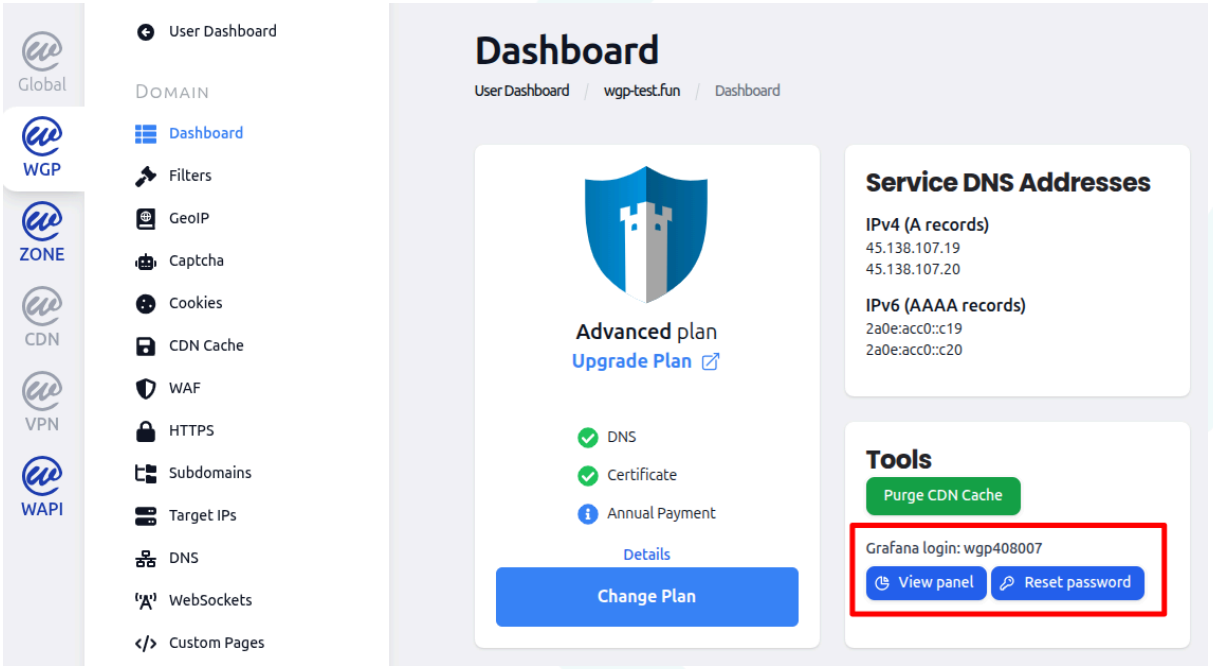


4. Set and confirm a password to secure your panel.
5. Click **Submit**.

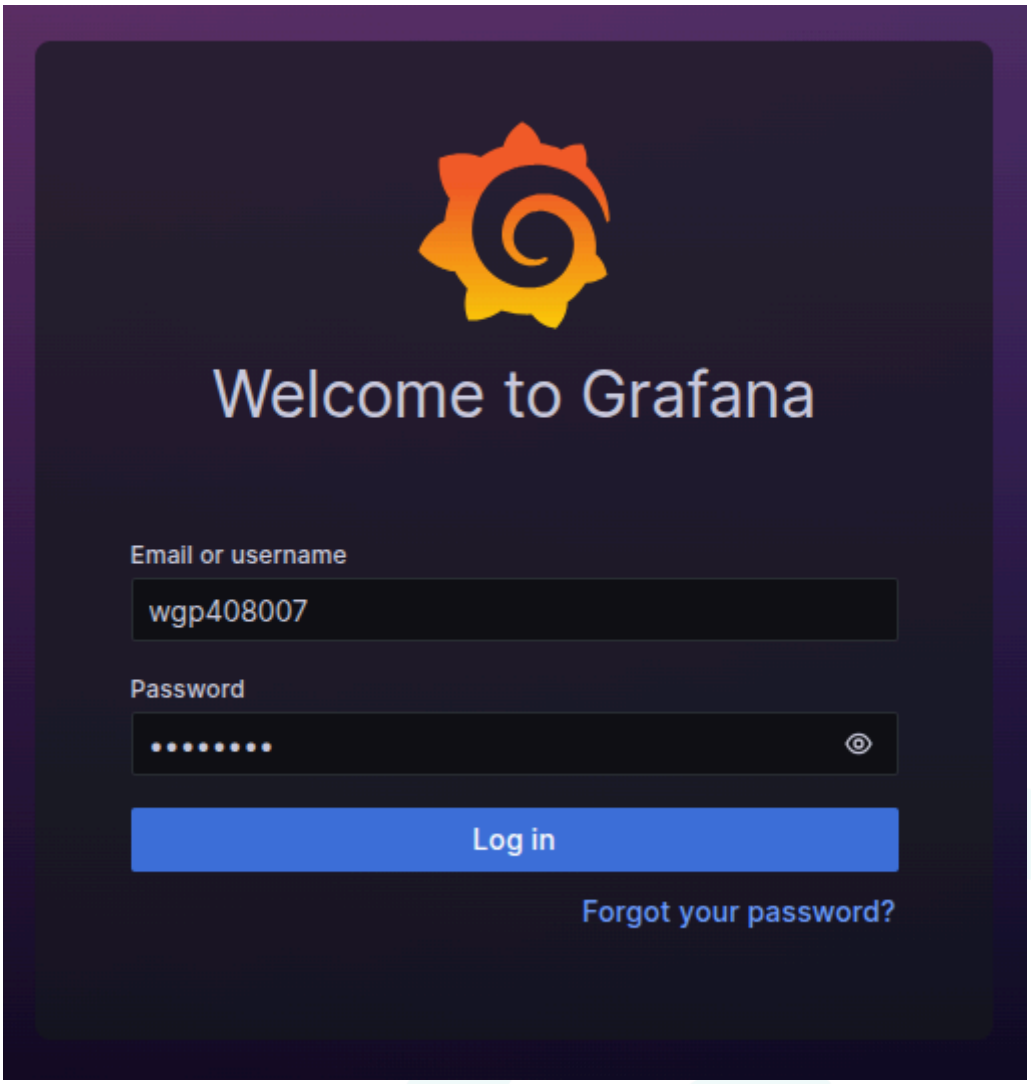


Once created, the Grafana panel uses a shared interface for all domains in your account. Now you can log into Grafana:

1. Return to the **Tools** section in the WGP dashboard.
2. Copy the system-generated username.
3. Click **View panel** to open the Grafana interface.

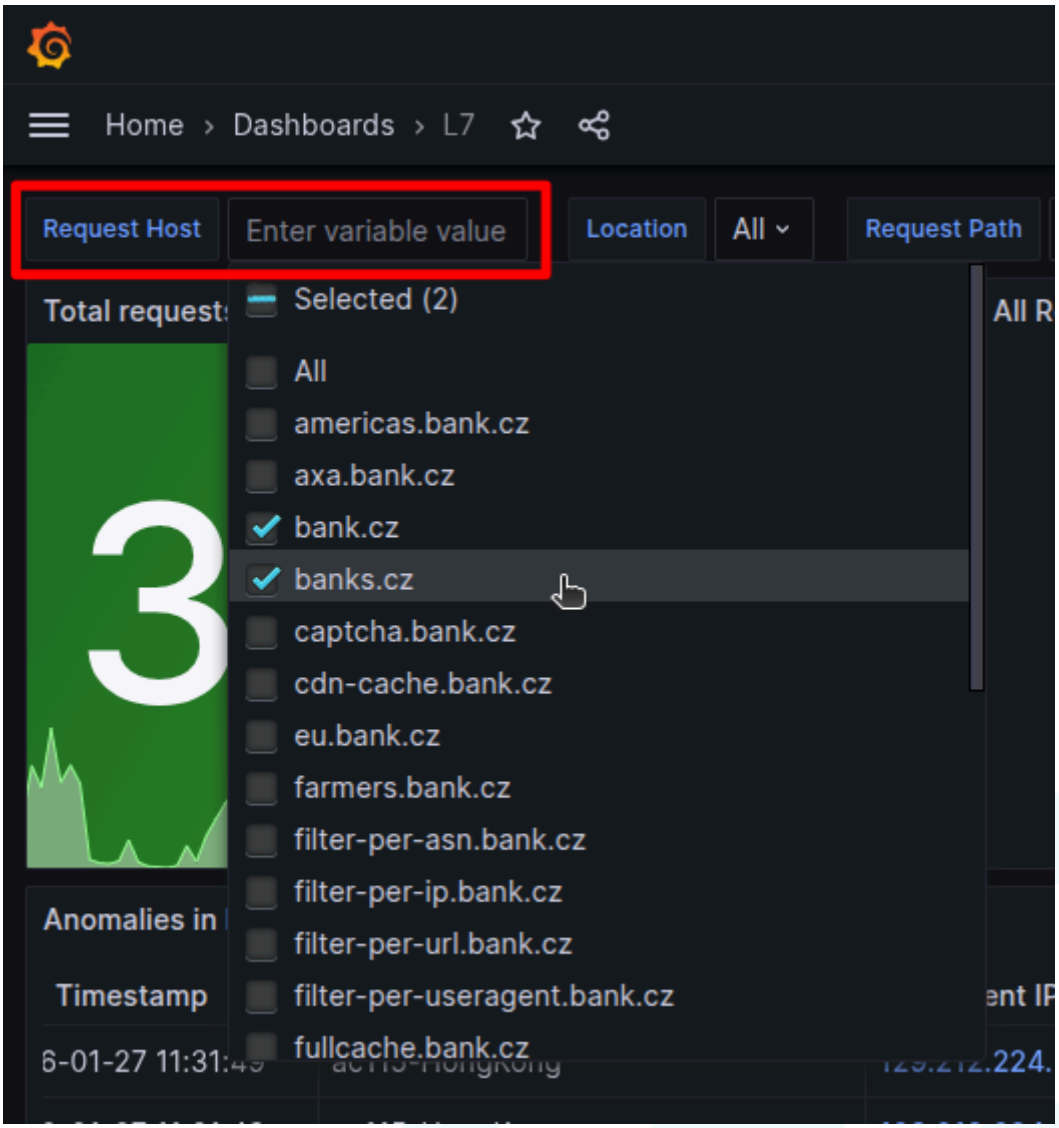


4. Log in to Grafana with the username and your password.



The Grafana panel is shared across all protected domains in your account. To filter by domain:

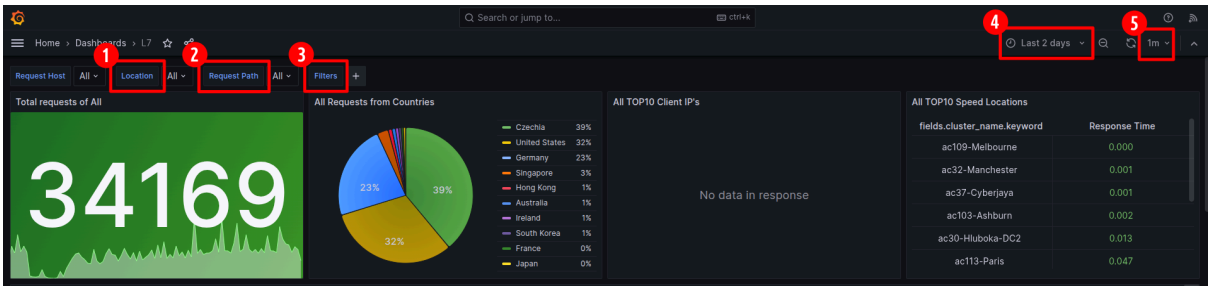
1. Select the domain(s) you want to analyze using the **Request Host** filter.



2. All statistics and logs will update based on your selection.

For even more granular results, filter by:

1. **Edge location.** View data from a specific edge server (Point of Presence).
2. **Request path.** View data from a specific url path (for example, **/wp-login**).
3. **Filters.** Use filters to narrow results by metric and condition (for example, **http_response_code != 200**). You can also filter by clicking the plus magnifying glass next to a valid metric.
4. **Timeframe.** Specify the time range from which the data will be sourced.
5. **Auto refresh interval.** Set how often data is refreshed or disable auto refresh.



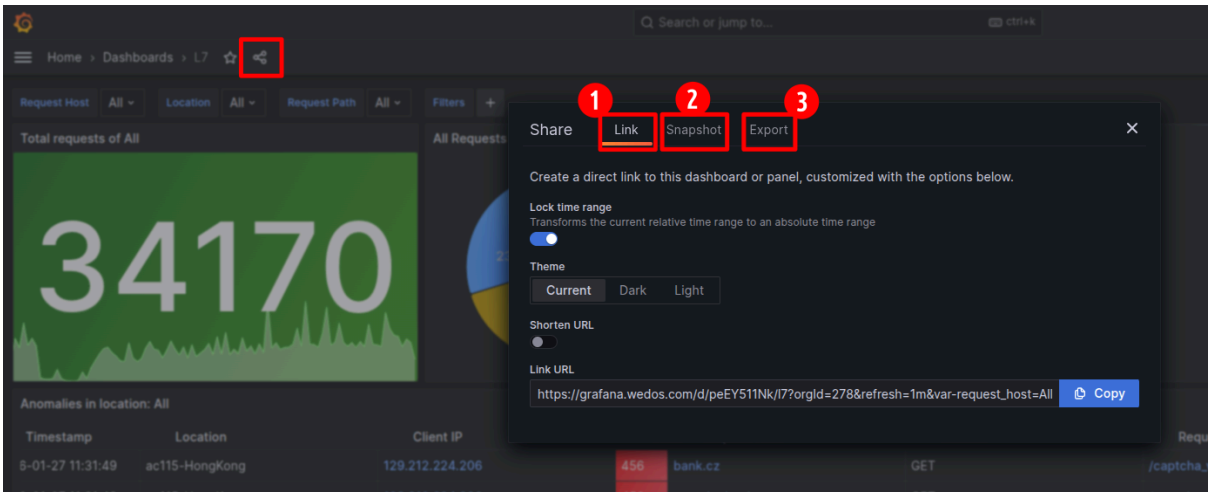
Grafana provides useful metrics to help you identify abnormal behavior, attacks, or traffic spikes.

Useful Metrics and how to use them:

- **Total requests.** Overview of total incoming traffic with a graph to see activity over time.
- **Request distribution by country.** Gain insight into geographic traffic sources. Verify if any unwanted countries are accessing your website.
- **TOP10 IPs.** See which IP addresses generate the most requests. Verify that IPs which are sending too many requests are not malicious by clicking on IP address to view abuseipdb.com entry.
- **Anomalies.** Requests blocked by WGP (HTTP response codes 429 and 456). Gain insight into malicious traffic, request details, and attack patterns.
- **All/Normal traffic.** Successful (unblocked) requests (HTTP response codes 200 and 302). Verify that there is not any malicious traffic that gets through.
- **HTTP response code, methods, and versions.** Gain insight into HTTP request behavior and filter by HTTP response code or version.
- **TOP10 URLs/Request path.** See which URL paths are requested the most. Look for suspicious activity (for example /wp-login or /wp-admin/)
- **TOP10 User Agent.** Identify patterns in User Agents requests that can be filtered out using WGP filters.

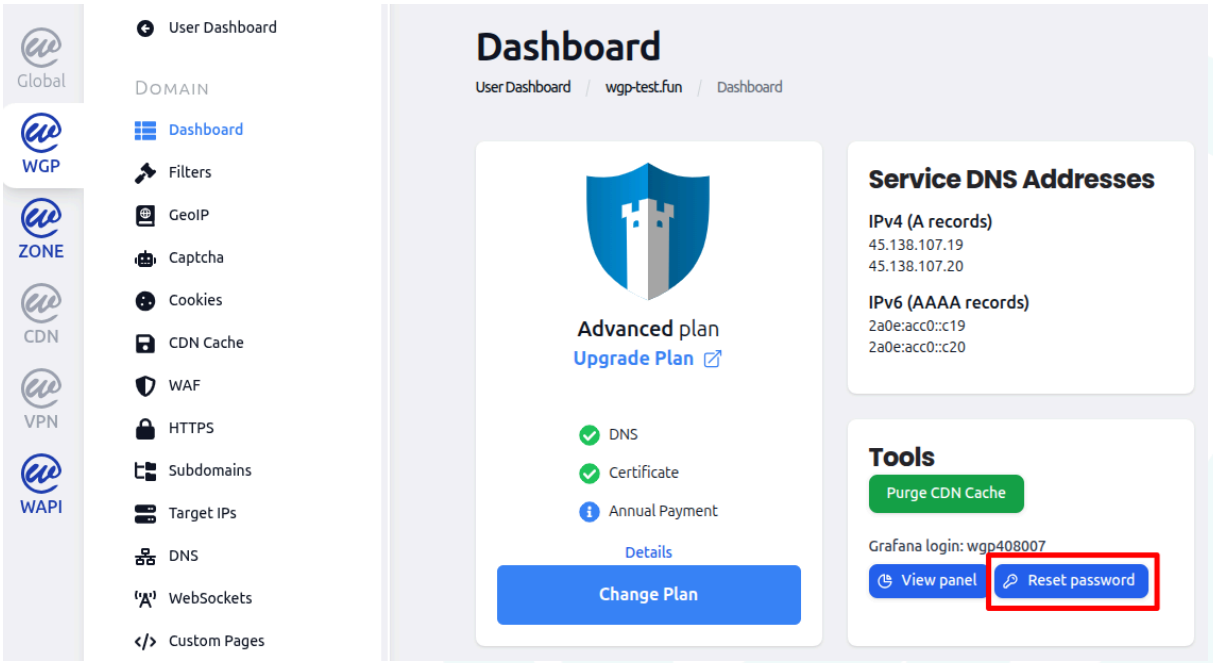
To generate a report click the **share icon** and select the method that fits your needs:

1. **Link.** Create a URL to share with another Grafana user.
2. **Snapshot.** Create a public URL of an interactive dashboard showing the current Grafana dashboard without any sensitive data.
3. **Export.** Copy or download a JSON file with data from the current Grafana dashboard.



You can reset your Grafana password at any time from the WEDOS.global admin panel.

1. Select any domain in WGP.
2. In the **Tools** section click **Reset password**, and set a new password.



To log out of Grafana, use the link https://grafana.wedos.com/logout