Monitoring and Restriction Requests from IP Addresses

> This feature must be switched on for your website by Commerce Vision.

This feature helps to make sure you have real human customers and not bots visiting and browsing your ecommerce store based on their activity in a session. A session is created when a user first comes to your site. Their IP address is logged.

When enabled, you can set up monitoring and restricting of incoming concurrent requests made by a unique IP address in a session. Monitoring is done by setting session maximum limits (threshold values) of:

- page views, and/or
- dynamic service requests.

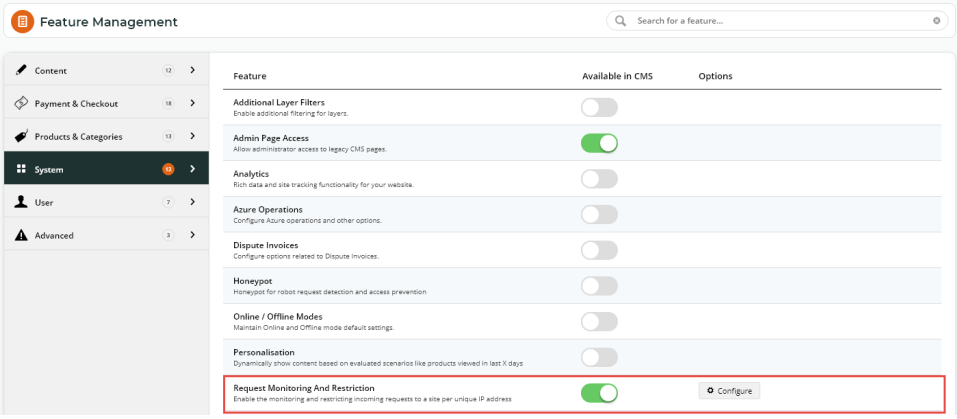
When a maximum threshold value is reached, your site can be set to:

- deny new requests rightaway by showing a '503 server busy' error
- redirect them to a challenge page (a page with Google Capcha on it) they have to pass successfully. (**NOTE -** If using this option, the page must be created first.) Failure to pass this challenge will result in denial of new requests.

When a unique IP address is restricted, they are logged. This data can be collected and viewed. You can also add specific IP addresses to a whitelist so they are excluded from being monitored and restricted.

Configure Settings

1. *In the CMS, go to **Settings Settings Feature Management System Request Monitoring and Restriction**.*



2. *When the **Enable Request Monitoring and Restriction** is enabled. click **Configure**. (If **Configure** is not displayed, contact Commerce Vision to switch on this feature.)*

3. *In **Request Monitoring Dynamic Service Count Threshold**, enter the threshold value for dynamic service request numbers before monitoring the IP address. Default: 0 (off)*

4. *In **Request Monitoring Page View Count Threshold**, enter the threshold value for number of page views before monitoring the IP address. Default: 0 (off)*

5. *In **Total Request Initiate Challenge Threshold**, enter the total number of requests by unique IP addresses before the challenge is initiated. The challenge is a page with captcha, which the user has to pass.*

6. *In **Total Request Terminate Challenge Threshold**, enter the number of failed attempts at the Captcha challenge the user can have. Default: 0 (off)*

7. *In **Total Request Deny New Session Threshold**, enter the threshold value above which will produce the '503 - server too busy' page.*

8. *In **Request Monitoring Excluded IP Address**, enter one or more whitelist IP addresses that can exceed the threshold values set for monitoring. E.g., you might have testing or development IP addresses you might want to exclude.*

9. *In **Challenge Page Content Before**,* (if using Challenge) *enter the HTML code for the page together with the Captcha challenge displayed after the challenge threshold is reached.*

10. *In **Challenge Page Content After**,* (if using Challenge), *enter the HTML code for the page together with the Captcha challenge displayed after the challenge threshold is reached.*

Related help

- User Impersonation
- Update Session Timeouts
- User Password Rules
- Lock a Website User to an IP Address
- Suspicious Activity Report