



WEB CONTROLS

Web Controls enable site administrators to use predefined and pre-tested security rulesets based on the e-commerce application, alleviating the need to discover, define, and maintain the rules themselves.

With Web Controls, customers can create the equivalent of firewall rules, without actually having to know how to build them. Web Controls are very easy to create, and have been designed specifically to allow users of all technical, and non-technical backgrounds, to quickly take actions to ensure the ongoing high performance, availability, and security of their websites.

Examples: Web controls empower application owners to block requests for a specified duration, or rate limit resource-intensive user sessions to mitigate their impact on the overall application. Web controls can also allow you to block all traffic from a specific country, if you don't do business with potential customers from that country. These are just some of the things you can accomplish with Web Controls.

Web Controls Edit Web Controls Refresh hits

Expand all

> Region based traffic block Block Checkout traffic from venezuela, Columbia and Czech Republic	<input checked="" type="radio"/> Stops when true Enabled Hits: 0 (5 min)
> PageSpeed Filters - DO NOT EDIT Disable additional PageSpeed Image filters	<input type="radio"/> Enabled Hits: 23918 (5 min)
> Whitelist Admin-ajax & Utility Allow /wp-admin/admin-ajax.php /utilityComment.php /customer.php	<input checked="" type="radio"/> Stops when true Enabled Hits: 68 (5 min)
> Block Admin Block non-whitelisted admin access	<input checked="" type="radio"/> Stops when true Enabled Hits: 0 (5 min)
> Cache Domain block Cache domain block, this domain should be open only for Whitelisted IP	<input checked="" type="radio"/> Stops when true Enabled Hits: 0 (5 min)
> PHPMyAdmin pagespeed bypass. Bypass pagespeed so it works.	<input type="radio"/> Enabled Hits: 0 (5 min)

UNDERSTANDING CONDITIONS AND ACTIONS

Conditions are the triggers that activate a web control. Conditions are followed by actions. The list of conditions is as shown below:

Create Condition

What condition do you want match?

You can limit what requests have the actions applied by providing a condition.

- ✓ Select a Condition...
- Cookie is set
- Cookie is not set
- Cookie value matches
- Cookie value does not match
- Country of origin is
- Country of origin is not
- IP address is set
- IP address not in set
- IP address is whitelisted
- IP address is not whitelisted
- User agent matches
- User agent does not match
- Referrer is
- Referrer is not
- Referrer is defined
- Referrer is not defined
- Random
- Rate limit
- URL matches
- URL does not match

Condition invalid. Done Cancel

Actions are completed when conditions in a Web Control are met. List of actions that can be applied is as shown below

Create Action

What action do you want take?

When a condition is met then all actions will be applied to the request. You can only choose one final action. Final actions will be run last; the order of execution of other actions is unspecified and not necessarily in the order displayed.

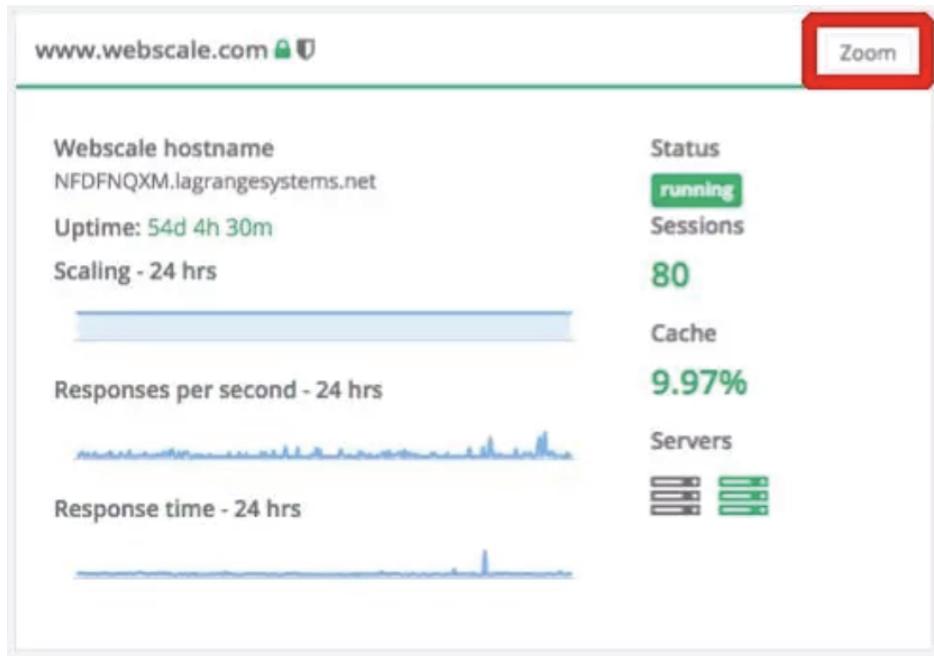
Choose an action type

- ✓ Select an action...
- Add Address To Set
- Cache Override
- Challenge User
- Defer Script
- Disable Session Tracking
- Make Script Asynchronous
- Serve
- Set Cookie
- Set Pagespeed Options
- Set Request Header
- Set Request Timeout
- Set Response Header
- Terminate HTTPS
- Final actions
- Continue
- Deny Request
- Discontinue
- Drop Request
- Redirect Request
- Use Alternate Backend

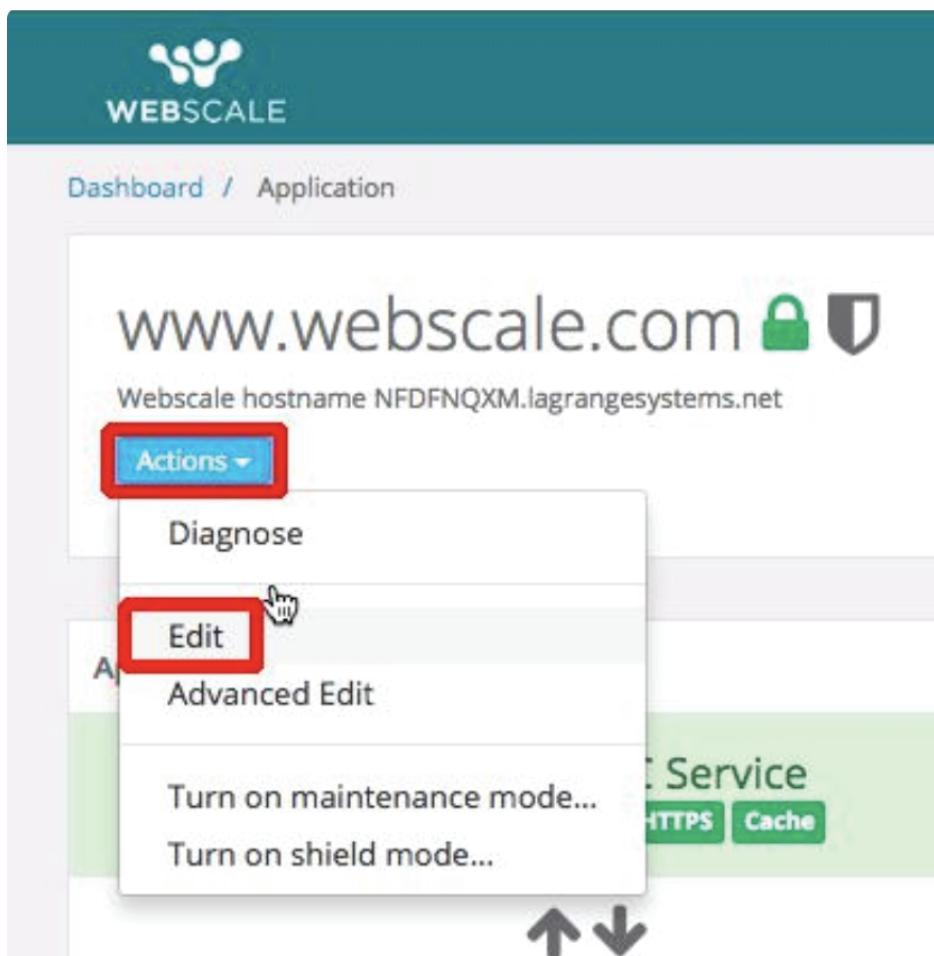
Action invalid. Done Cancel

Example - How to Set up a Web Control for Rate Limiting Traff

Step 1: Login to the Webscale portal and select the appropriate domain by clicking on Zoom.



Step 2: Click on Actions --> Edit.



Step 3: Select Web Controls tab, then click on the "Add A Web Control" button.

The screenshot shows the 'Web Controls' section of a web interface. At the top, there are tabs: General, Servers, Web Controls (which is highlighted with a blue border), HTTPS, Blacklist, and Whitelist. Below the tabs, the 'Web Controls' section has a title 'Control wp-login access'. It contains two rows of configuration. The first row has a 'Condition' of 'IP address is not whitelisted' and a 'Details' note that actions will be applied to all IP addresses not included in the whitelist. The 'Url' condition lists several specific URLs. To the right is a toggle switch which is turned on. The second row has an 'Action' of 'Deny Request' and a 'Details' note that the request will be denied with status code 403 and response Forbidden. The second rule is titled 'Paths /wp-admin /blog' and also has a turned-on toggle switch. At the bottom left, there is a green button labeled 'Add A Web Control' with a blue border.

Step 4: From the "Add a Web Control" window:

1. Enter a name to describe your control. You may also add a description to further clarify the control purpose.
2. Select a Condition for the control. In this case, select "Rate Limit" from the selection list.
3. Add a limit to the number of requests in a time interval.
4. Click on Save.
5. Select an Action to take. In this case, select "Add Address to Set" from the selection list.
6. Click on Save Action.
7. Click on the Save Web Control button.

The screenshot shows the 'Add a Web Control' configuration window. It includes fields for 'Name' (set to 'Rate limit'), 'Description' (set to 'Rate limit traffic based on number of requests'), and a 'Conditions' section. The 'Conditions' section contains two items: 'IP address is not whitelisted' and 'Rate limit'. Under 'Actions', there is one item: 'Add Address To Set'. At the bottom, there are '+ Add condition' and '+ Add action' buttons.

Name	Rate limit
Description	Rate limit traffic based on number of requests
Conditions ①	Details
IP address is not whitelisted	Actions will be applied to all IP addresses not included in the whitelist.
Rate limit	Actions will be applied if the number of requests from a given request address in the last 1 minutes is greater than 100.
Actions ①	
Add Address To Set	Request address will be added to the set Rate limit address set with TTL as 300 seconds.

Step 5: From the "Add a Web Control" window:

1. Select Web Controls tab, then click on the "Address in set" button.
2. Set Action as "Deny Request".

Name	Rate limit	
Description	Description	
Conditions ⓘ	Details	
IP address is not whitelisted	Actions will be applied to all IP addresses not included in the whitelist. <input checked="" type="checkbox"/> <input type="button" value="x"/>	
Rate limit	Actions will be applied if the number of requests from a given request address in the last 1 minutes is greater than 100 . <input checked="" type="checkbox"/> <input type="button" value="x"/>	
⊕ Add condition		
Actions ⓘ	Details	
Add Address To Set	Request address will be added to the set Rate limit address set with TTL as 300 seconds. <input checked="" type="checkbox"/> <input type="button" value="x"/>	
⊕ Add action		

Step 6: Your new Web Control is now created but is disabled by default. To enable the Web Control, click on the "Enable" switch to the right of the Web Control details.

Your Web Control is now enabled and all traffic exceeding the limit of the number of requests will receive a Forbidden error message.

Name	Block Rate limited traffic	
Description	Description	
Conditions ⓘ	Details	
Address in set	Actions will be applied when address is in the address set Rate limit address set . <input checked="" type="checkbox"/> <input type="button" value="x"/>	
⊕ Add condition		
Actions ⓘ	Details	
Deny Request (final)	Request will be denied with status code 403 and response Forbidden <input checked="" type="checkbox"/> <input type="button" value="x"/>	
⊕ Add action		

Another example to set up a Web Control to block specific countries from accessing your site can be found here:

<https://www.webscale.com/knowledgebase/user-guide/web-controls-how-to-block-countries-from-accessing-my-site>

