

Regular expression filters

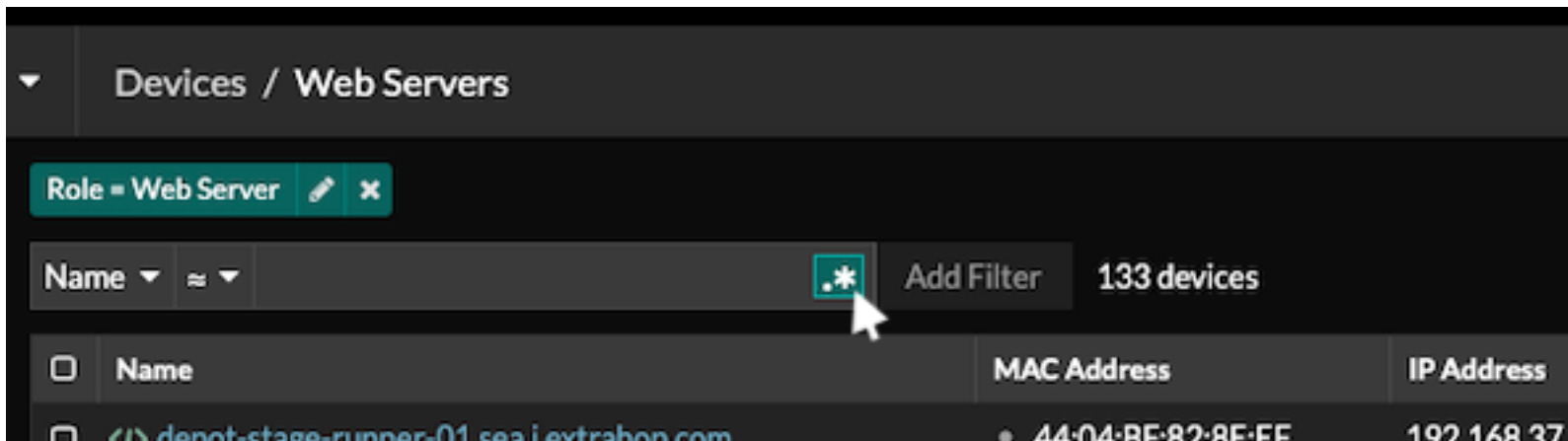
Published: 2020-03-21

Filter your search results by writing regular expression (regex) strings in certain search fields throughout the ExtraHop Web UI. For example, you can filter for parameters in a detail metric key, such as a number within an IP address. You can also filter by excluding specific keys or combination of keys from charts.

Regex-capable search fields have visual indicators throughout the system and accept standard syntax. If you want to configure record relationships for a custom detail metric, the regex syntax has advanced requirements. For more information, see the section on [Additional Filters](#).

Search fields with an asterisk

Click the asterisk in the field to enable regex strings.

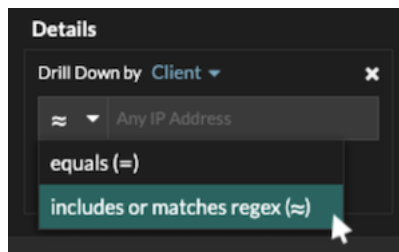


This type of field is available from the following system pages:

- Filtering a table of devices
- Creating filter criteria for a dynamic device group

Certain search fields with a trifold operator

Click the operator drop-down to see the regex option.

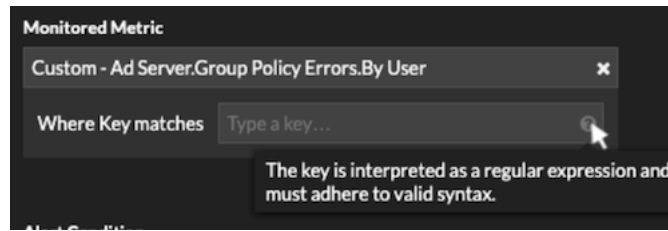


This type of field is available from the following system page:

- Editing a chart in Metric Explorer

Certain search fields with a tooltip

Hover over the tooltip in the field to see the regex option.



This type of field is available from the following system page:

- Creating a threshold alert

The following table includes examples of standard regex syntax.

Chart Scenario	Regex filter	How it works
Compare HTTP status codes 200 to 404 .	<code>(200 404)</code>	Matches 200 and 404 codes where the <code> </code> symbol serves as an OR function.
Display any HTTP status code that contains a 4 .	<code>[4]</code>	Matches any value that contains a 4 . For example, this filter can return 204 and 400 status codes.
Display all 500 -level HTTP status codes.	<code>^[5]</code>	Matches any value that begins with a 5 . For example, this filter can return 500 and 502 status codes.
Display all 400 and 500 -level HTTP status codes.	<code>^[45]</code>	Matches all values that begin with a 4 or 5 . For example, this filter can return 400 , 403 , and 500 status codes.
Display any HTTP status codes except 200 -level status codes.	<code>^(?! 2)</code>	Matches all values except values beginning with a 2 , where <code>^(?!)</code> specifies the range of results to exclude. For example, this filter can return 400 , 500 , and 302 status codes.
Display any IP address with a 187 .	<code>187 .</code>	Matches 1 , 8 , and 7 characters in the IP address.
Review all IP addresses containing 187.18.	<code>187\ .18\ .</code>	Matches 187 and the character <code>.</code> that follows the 187 . For example, this filter returns results for 187.18.0.0.0 , 180.187.0.0.0 , or 187.180.0.0.0/16 .
Display any IP address except 187.18.197.150 .	<code>[^187.18.197.150]</code>	Matches anything except 187.18.197.150 , where <code>[^]</code> specifies the exact value to exclude.
Exclude a list of specific IP addresses	<code>[^187.18.197.150 187.18.197.151 187.18.197.152]</code>	Matches anything except 187.18.197.150 , 187.18.197.151 , and 187.18.197.152 , where the <code> </code> symbol serves as an OR function

Chart Scenario

Regex filter

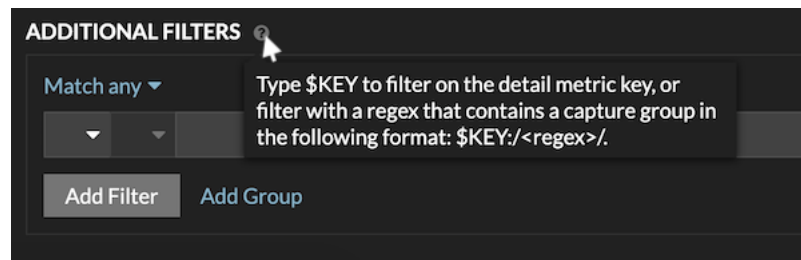
How it works

and [^] specifies the exact values to exclude.

Additional filters

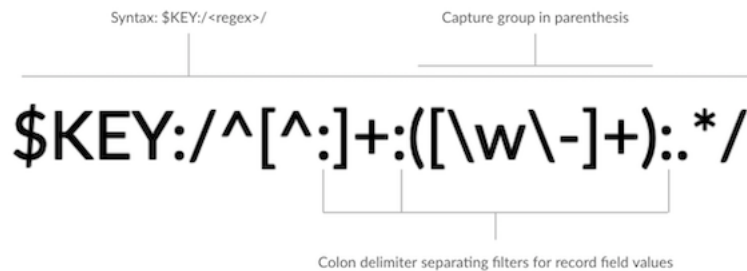
When you [create a custom detail metric](#) from the Metric Catalog, you can add advanced regex syntax to the Additional Filters search field in the Record Relationships section.

The tooltip appears after you select **Detail Metric** and is not available when **Base Metric** is selected.



The regex syntax in this field must meet the following requirements:

- If your key contains multiple values, your regex syntax must include a single capture group. A capture group is designated by parenthesis. Your capture group determines the filter value.



- If you want to return a specific value from a detail metric key that contains multiple record field values, the regex must follow this syntax:

`$KEY: / <regex> /`

For example, if your detail metric key is ipaddr:host:cipher and you only want to return the IP address value, you would type the following:

`$KEY: / ^ ([^ :] +) : . + /`

- If your key contains multiple record field values, the values are separated by a delimiter that is specified in the trigger that is generating the key. The placement of the delimiters in your regex syntax must match the delimiters in the detail key. For example, if you have a key with three values that are separated by a delimiter that is a colon, the three values for the key in your regex syntax must be separated by two colons.

Tip: If you want to return all record field values in a detail metric key, type `$KEY`. For example, if your detail metric key is ipaddr:host:cipher, type `$KEY` in the search field to return all three of those field record values (IP address, hostname, and SSL cipher suite).