Lastline web API guide

Ymon Oy • Äyritie 8 D • 01510 Vantaa • www.ymon.fi
info@ymon.fi • +358 (0)20 778 0590

Version history

Change date	Author(s)	Subject of change	Approver(s)	Approval date	Version
4.5.2015	Sonia Holopainen	Initial version			1.0

Table of contents

Accessing the service

Logging in

The login screen can be accessed at https://<serveraddress>, where <serveraddress> is replaced with the address of the server the API front has been installed to. You will need to accept the self-signed certificate before you can login, consult your IT support how this is done in your browser.

To login, enter your username and password in the text fields and click the login button below.

The API web interface

The basic interface for a blacklist consists of the following elements.

1. The subject of the blacklist being displayed
2. Text fields for filtering entries
3. Display section for entries retrieved from Lastline (Currently none)
4. Page navigation (Forward, backward, entries to display per page, page quick navigation)
5. Text fields for data entry
6. Button to commit any changes

This is how the API interface will look like once logging on the first time, given no custom intelligence entries have yet been added to Lastline through other means.

Adding entries

To add an entry to a blacklist, navigate to section 5 of the interface, 'Text fields for data entry'. Each field will be pre-filled with a description of what kind of data they accept. In our example we are adding an IP address to the IP blacklist.

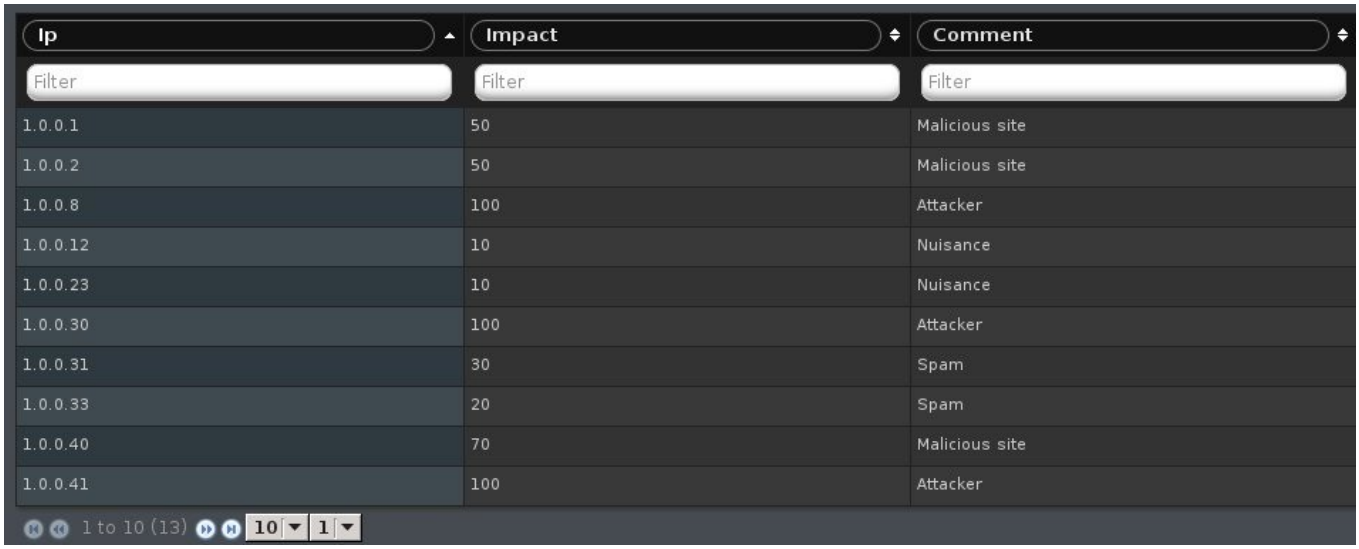
1. First field from the left will accept a correctly formatted IPv4 or IPv6 address to be added. Due to the Lastline API the entry can contain only a single IP address, and not for example a mask.
2. The second field will define the initial value for impact, or seriousness of traffic relating to this address. Impact can be a number between 10 and 100, with increments of 10. For example: 10, 50 or 100. It is not possible to use a number that is not divisible by ten, such as 85.
3. In the the third field you can enter a free-form description for this entry, the field has a maximum length of 255 characters.
4. The fourth field contains a free-form description of what source the blacklist entry is from. This could be for example the name of an internet blacklist, a reference to an IDS system or alike. The maximum length of this field is 45 characters.
5. After all information has been entered correctly, click the 'Update' button to enter it to the system.

Adding domain entries functions the same way, only with the first field replaced by a domain name.

Modifying existing entries

Refer to the section 'Adding entries'. Modifying entries functions the same way as adding them does, but supports overwriting the information relating to the blacklist entry without deleting it first. All fields will need to be filled as with adding the entries.

Browsing entries



Ip	Impact	Comment
Filter	Filter	Filter
1.0.0.1	50	Malicious site
1.0.0.2	50	Malicious site
1.0.0.8	100	Attacker
1.0.0.12	10	Nuisance
1.0.0.23	10	Nuisance
1.0.0.30	100	Attacker
1.0.0.31	30	Spam
1.0.0.33	20	Spam
1.0.0.40	70	Malicious site
1.0.0.41	100	Attacker

1 to 10 (13) 10 1

Once logged into the service, it will automatically retrieve the custom blacklist entries from Lastline through the API. If the display section remains black, there either are no custom entries yet or the API cannot be reached. In the latter case an error message will also be displayed to the user. By default the blacklists are sorted either by IP address or the domain in question.

Navigating pages

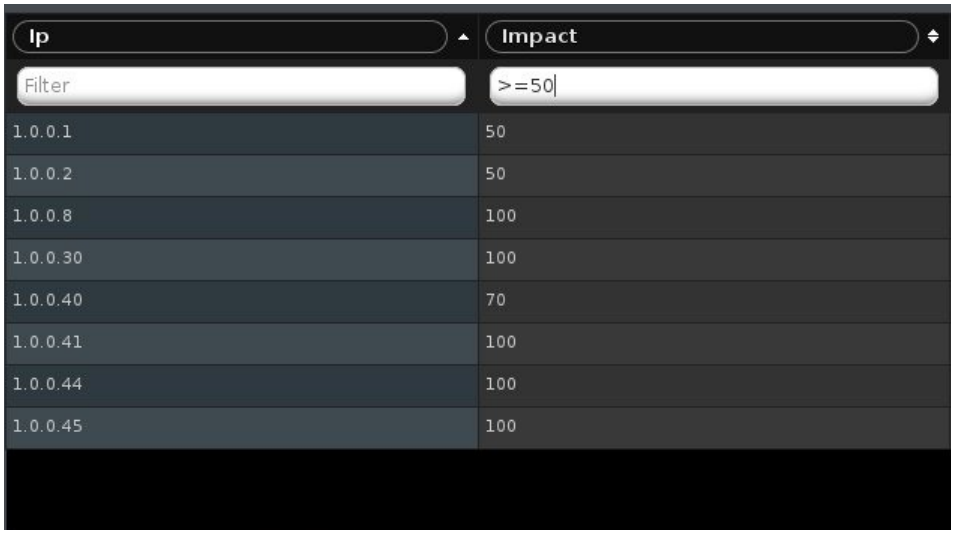
Page navigation described from left to right.

Only 10 entries are shown by default to keep the display of the entries compact, and the rest of the entries are paginated such as is the case here. The '1 of 10 (13)' text at the bottom left states that we are currently displaying the ten first entries, and that three more entries are hidden on other pages of the table. Controls with << and >> arrow symbols are provided to navigate between the pages. The |< and >| symbols will take you to the beginning and ending pages respectively.

If you should like to display more than 10 entries per page, you can also do so by clicking on the dropdown with the number '10' on it to select the desired amount.

Finally a quick navigation dropdown is provided for selecting a page to navigate to directly.

Sorting and filtering entries



Sorting

To sort the blacklist entries by a column of your choosing, you can click on the title describing the contents of the column. The title is located at the top of the table, in this example containing 'Ip' and 'Impact'. To swap between ascending and descending sort order, simply click on the title again.

Should you like to sort the columns based on multiple categories, you can do so by holding down shift while clicking on the titles of the columns you desire to sort. A column chosen for sorting is highlighted in blue in contrast to the other columns.

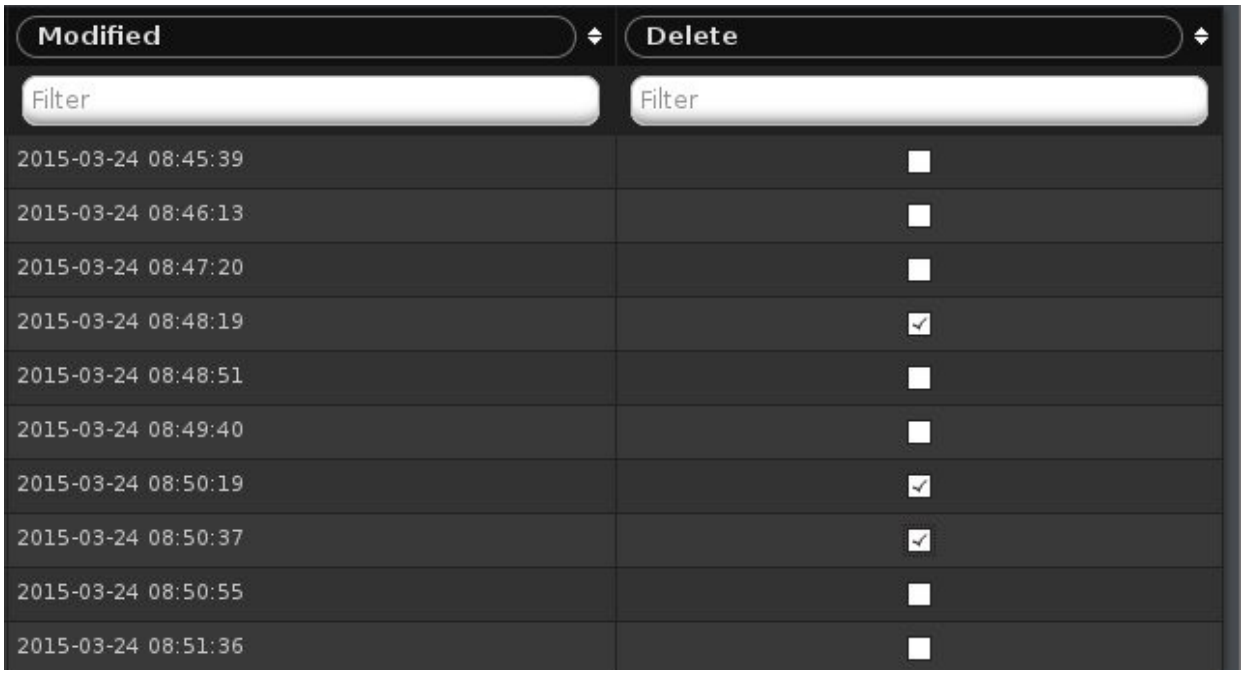
Filtering

The interface also allows filtering all displayed entries based on multiple conditionals. Each column has a text field labeled 'Filter' underneath its title. To begin filtering you can enter a condition based upon you wish to filter by. Note that adding a condition will filter out any entries from all rows that do not match.

In the example above we are filtering to any entries that have either 50 or higher impact value. You can simply enter what you want the filter to match in a given column, or you can prefix number fields with mathematical operators such as: >, <, >=, <=. This is allowed in date columns as well (>2015-03-01).

To filter text based fields you can enter a search to be matched against.
For example, this will return all entries matching it: 1.0.0.
This will return everything else but what is matched: !1.0.0.1

Deleting entries



Each entry displayed from the API is also accompanied by a 'Delete' column. The column contains a checkbox that can be ticked to mark an entry for deletion. No deletion will take place until the 'Update' button is pressed.

To delete entries:

1. Tick the checkboxes of the entries to be deleted
2. Click on the button labeled 'Update'
3. The entries will be deleted and the remaining entries refreshed to update the changes

Logging out

Once logged in, the top left corner of the page will display the username you have logged in with. To the right of your username is a link that will allow you to log out of the service by clicking it. You will then be redirected back to the login screen.