

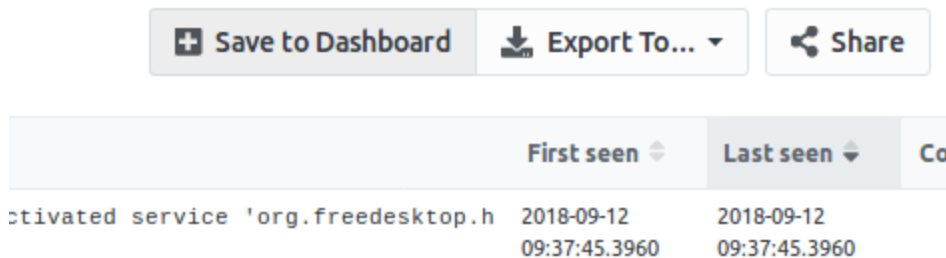
LOGZILLA DOCUMENTATION

Creating your own widgets

Build custom LogZilla widgets from Save to Dashboard or by editing pre-built widget titles, fields, filters, and user tag criteria

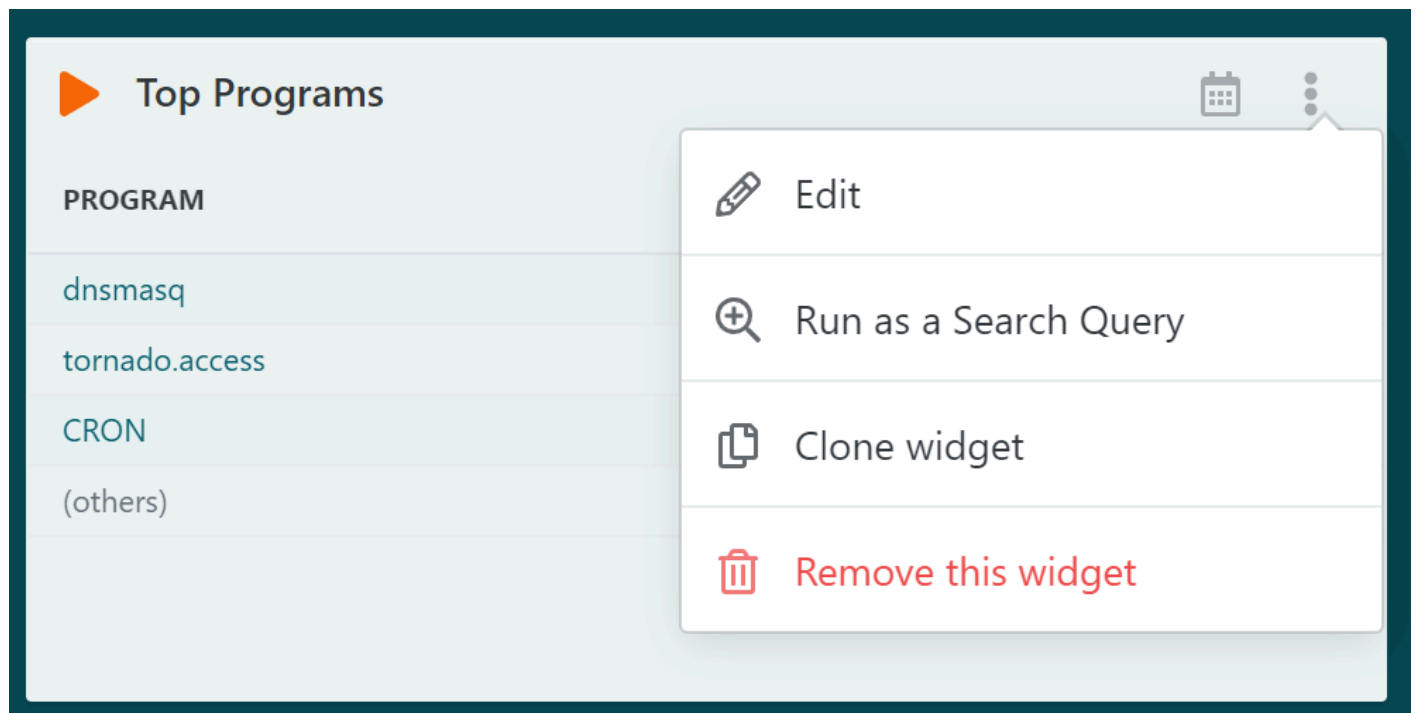
LogZilla Dashboards · Generated June 12, 2026 · logzilla.ai/docs/using-the-dashboard/creating-your-own-widgets

Widgets may be created using either a customizable **pre-built widget** or by performing a search based on the desired filters followed by selecting the **Save to dashboard** button on the search results page.



Customizing Existing Widgets

Widgets may be customized to display only the data users wish to see. The following examples show how to set various options for both a `Top Hosts` (which are `TopN`-type charts) and `Top Programs` widgets.



Access the customization menu by clicking the widget's "options" icon (3 dots). Next, select **edit** from the menu to access the widget settings.

Edit widget ✕

Title
Title of widget

Field
Field to show

Limit
Number of items to present

Filter
Extra filtering
 More ▾ **User Tags** ▾

View type
Type of view

Show other
For 'Top N' params, show also other values aggregated into one value

By changing the Title, Description, and Field, users can easily turn this into a widget for showing top severities.

Users can also monitor top Cisco Mnemonics, or add a search term like 'failed login'. The Title and Description need to be modified by the user to be clear about the information shown in the widget. The Field lets users decide what data to display.

Edit widget ✕

Title
Title of widget

Field
Field to show

Limit
Number of items to present

Filter
Extra filtering **More** **User Tags**

View type
Type of view

Show other
For 'Top N' params, show also other values aggregated into one value

The Filter section lets users narrow results similarly to the main search bar in LogZilla. Users add a search term, such as 'failed login', then select all Windows servers from the Host section. This will give a widget that displays only failed login events generated by Windows hosts. Users can similarly filter results by Severity, Facility, Program, Mnemonic, or Type (Unknown, Actionable, or Non-actionable). So, selecting all 'CONFIG' mnemonics would display configuration changes from routers and switches.

Edit widget ✕

Title
Title of widget

Field
Field to show

Limit
Number of items to present

Filter
Extra filtering **More** 1 **User Tags** 1 **✕ Reset**

View type
Type of view ☰ 📊 📈

For 'Top N' para
other values aggreg

Include **Exclude** **✕ Reset**

✓ PaloAlto Threat

ACK

AasSipMgr

Severity ▾

Host ▾

Facility ▾

Program 1 ▾

Mnemonic ▾

Type ▾

Cancel
Save changes

User tags can be used in the filter. User tags are special key/value pairs associated with each individual event. The LogZilla rules can parse the data in each event message and then set specific named (configurable) tags to values from the event data. For example, some common tags are `DstIP` and `DstPort`, respectively representing the destination IP address and the destination IP port for the given event. User tag `DstIP` could for example have value `192.168.0.2`.

The widget can be filtered based on user tags. If the "User Tag" dropdown is selected, optionally at the top of the dropdown a filter for the desired user tag name can be entered (such as if user tag `DstPort` is desired then "Dst" can be entered in the search field at the top of the dropdown, and each user tag with a name containing "Dst", such as `DstPort` will be listed). At maximum ten user tag names will be shown, so to access the user tags that are not shown the search box at the top of the dropdown should be used to narrow down the selection of available user tags.

Once the desired user tag is shown it can be clicked to open the values dropdown. The values dropdown allows choosing the particular values for the given user tag either to be included or excluded, such that only those events with the chosen values for

the designated user tag will be included in the widget, or those with the chosen values will be specifically excluded from the widget. The top of this dropdown as well contains the search box to find particular values of interest. Multiple user tag values can be chosen by clicking on each and a checkmark will be shown next to those so designated as an indicator, or the checked ones can be clicked once more to deselect them. User tags that have very many values, such as typically IP addresses, will only show an asterisk (*) where the values would be. In this case, the value must be typed directly into the search box.

A special value of * can be typed in, then selected. This value has a special meaning: it selects only those events that have *some* value for the designated user tag. This is useful because not every event may contain every user tag. For example, there may be events that have no SrcPort, and those events are not desired to be included. In order to select only those events that have a value for SrcPort, without distinction of what that value is, the * filter value should be used.

The screenshot shows the 'Edit widget' dialog box. The 'Title' field is 'Top Hosts'. The 'Field' dropdown is set to 'Host'. The 'Limit' field is '5'. The 'Filter' section has a search box with 'Search in messa...', a 'More' dropdown, and a 'User Tags' dropdown. The 'User Tags' dropdown is open, showing a search box with 'nginx' and a list of categories: 'NGINX Destination IPs', 'NGINX Servers', 'NGINX Sites', 'NGINX Sources', 'NGINX Statuses', 'NGINX URI Paths', and 'NGINX User Agents'. Below the 'Filter' section, there is a 'Show other' section with a search box containing '138.68' and a list of values: '138.68' and '138.68.11.35'. At the bottom, there is a 'View type' section with a dropdown menu.

The Limit allows users to control how many results are shown in the widget, while 'Show other' toggles the display of items that don't fit the standard categories of the selected filter. For example, for 'Top N' params, it will also show other values aggregated into one value. The final selection is 'View type', which allows users to select the chart type that best fits the other widget options.

Edit widget ✕

Title
Title of widget

Field
Field to show

Limit
Number of items to present

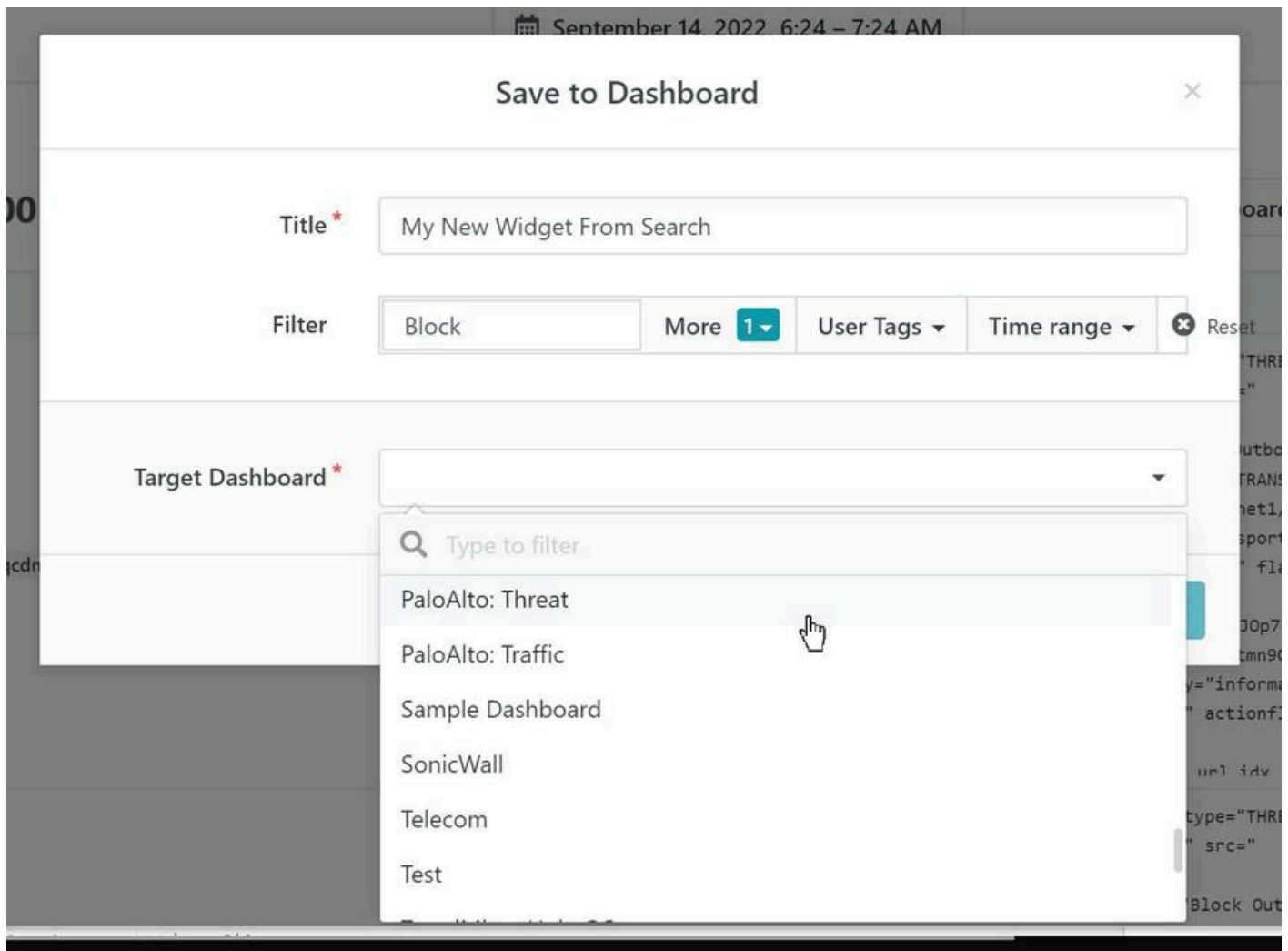
Filter
Extra filtering **More** **User Tags**

View type
Type of view

Show other
For 'Top N' params, show also other values aggregated into one value

Creating Widgets from Search Results

If users find that they run a particular search on a regular basis, they can click the 'Save to dashboard' button. This will prompt them to name the widget and select the dashboard that it should be displayed on. Users can also modify the search parameters or filters further, if needed.



The display will show updated information on a regular basis. This is ideal for keeping up with ongoing network issues, keeping an eye on intrusion attempts, or even knowing when users are locked out after consecutive failed logins.

SEVERITY	HOST	FACILITY	PROGRAM	MESSAGE	FIRST SEEN
INFO	fileshare	SYSLOG	Unknown	MARK -	2018-09-12 09:37:01.208
INFO	fileshare	AUTHPRIV	CRON	pam_unix(cron:session): session closed for user root	2018-09-12 09:17:01.707
INFO	fileshare	CLOCK	CRON	(root) CMD (cd / && run-parts --report /etc/cron.hourly)	2018-09-12 09:17:01.701
				pam_unix(cron:session)	

Using Badge (Counter) Type in Rate and TopN Widgets

- **Rate Type Widgets:** For widgets that show event rates, the badge can display the total count or a summary statistic, like the average rate.

Edit widget ✕

Title
Title of widget
Total Events: China

Filter
Extra filtering
Search in mess... More ▾ User Tags 1 ▾ ✕ Reset

View type
Type of view

Badge source
Type of view
Total events ▾

Cancel Save changes

▶ Total Events: China Last 7 days 📅 ⋮

9.89m

▶ Total Events: Russia Last 7 days 📅 ⋮

2.54m

- **TopN Widgets:** In TopN widgets, the badge can show the count of unique items in the selected field, providing a quick overview of the diversity in the data.

Edit widget



Title
Title of widget

Field
Field to show

Filter
Extra filtering
 More ▾ **User Tags** 1 ▾ **Reset**

View type
Type of view

[Cancel](#) [Save changes](#)



To use a badge in these widgets, select 'badge' in the 'View type' option. Customize the title, field, and filters as needed to reflect the data to showcase.