

The following content is part of the Graylog 6.3 documentation. If you are using another version of Graylog, please switch to your version.

Select Version ▼

We strongly recommend all users currently running Graylog versions 6.2.0–6.2.3 upgrade immediately to the latest secure version to resolve [a high-severity privilege escalation vulnerability](#). See [Upgrade Graylog](#) for detailed instructions on upgrading your Graylog instance.

Install Sidecar on Linux



Warning: This article covers installation steps for **Linux operating systems only**. If you are setting up Sidecar on Windows, please refer to our guide on [Windows Sidecar Installation](#).

In order to install Graylog Sidecar, there are a few preparatory steps that should be taken both in Graylog and on the host machine. Please note the following guide describes a self-managed Graylog Sidecar configuration. For information on using Sidecar in Graylog Cloud, please see [Sidecar in the Cloud](#).

Installation Steps in Graylog

Prerequisites

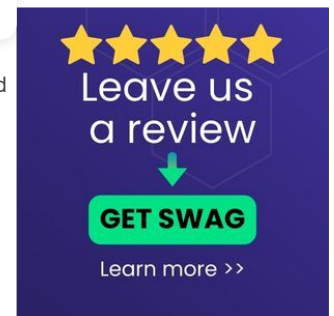
Before installing Sidecar, make sure that you have a [Beats](#) input in order to receive data from the Beats collector, and configure your input to receive Sidecar logs on [port 5044](#).

1. Navigate to *System > Inputs*.
2. Select *Beats* as the input.
3. Click *Launch new input* to prompt a new form.
4. Check the *Global* box if you would like to receive the data set among other nodes.
5. Make sure that the port field is set to [5044](#).

Resource Videos

[Log Wrangling: Make Your Logs Work For You](#)

[What to Feed Your First SIEM](#)



Launch new *Beats* input

☒ Global

Should this input start on all nodes

Title

Beats

Select a name of your new input that describes it.

Bind address

0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port

5044

Port to listen on.

Receive Buffer Size (optional)

1048576

The size in bytes of the `recvBufferSize` for network connections to this input.

No. of worker threads (optional)

2

Number of worker threads processing network connections for this input.

TLS cert file (optional)

Path to the TLS certificate file

Create an API Token

1. Navigate to *System > Sidecars*.
2. Click on *Create or reuse a token for the graylog-Sidecar user*.
3. Enter a name into the *Token Name* field.
4. Click on *Create Token*.



Hint: Save the API server token in a safe yet accessible location in case you need to retrieve it.

Download Sidecar

You can find [.deb](#) and [.rpm](#) packages in our package repository. Please follow the version matrix to select the correct package and download it from our [GitHub page](#).

Sidecar Version	Graylog Server Version
1.5.x	5.2.x or higher
1.4.x	5.0.x or higher
1.3.x	5.0.x
1.2.x	3.2.5 or higher
1.1.x	3.2.5 or higher

Installation Steps on the Host Machine

Select your method of installation based upon your chosen operating system.



Hint: All of the following commands in this section should be executed in the remote machine from where you want to collect log data.

Ubuntu and Debian Installation

1. Install the Graylog Sidecar repository configuration and Graylog Sidecar itself with the following commands:

```
wget https://packages.graylog2.org/repo/packages/graylog-sidecar-repository_1-5_all.deb
sudo dpkg -i graylog-sidecar-repository_1-5_all.deb
sudo apt-get update
sudo apt-get install graylog-sidecar
```

[Copy](#)

2. Edit the configuration file and activate Sidecar as a system service. Please note that most configuration parameters come with built-in defaults. The only parameters whose values need to be configured manually are `server_url` and `server_api_token`.

```
sudo vi /etc/graylog/sidecar/sidecar.yml
sudo graylog-sidecar -service install

# Ubuntu 14.04 with Upstart
sudo start graylog-sidecar

# Ubuntu 16.04 and later with systemd
sudo systemctl enable graylog-sidecar
sudo systemctl start graylog-sidecar
```

[Copy](#)

CentOS and RedHat Installation

1. Install the Graylog Sidecar repository configuration and Graylog Sidecar itself with the following commands:

```
sudo rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-sidecar-repository-1-5.noarch.rpm
sudo yum install graylog-sidecar
```

[Copy](#)

2. Edit the configuration and activate sidecar as a system service. Please note that most configuration parameters come with built-in defaults. The only parameters whose values need to be configured manually are `server_url` and `server_api_token`.

```
vi /etc/graylog/sidecar/sidecar.yml
sudo graylog-sidecar -service install
sudo systemctl enable graylog-sidecar
sudo systemctl start graylog-sidecar
```

[Copy](#)

SUSE Installation

Now that your Sidecar installation is complete, we recommend you proceed to [Install Sidecar Collectors](#).

sidecar.yml Configuration Reference

Below is a list of parameters used in the `sidecar.yml` configuration file for your reference:

Parameter	Description
<code>server_url</code>	URL to the Graylog API, e.g.: <code>https://192.168.1.1:9000/api/</code>
<code>server_api_token</code>	The API token to use to authenticate against the Graylog server API. e.g. <code>1jq26cssvc6rj4qac4bt9oeeh0p4vt5u5ka19joc11g9mdi4og3n</code> The token is mandatory and needs to be configured.

Parameter	Description
<code>node_id</code>	<p>The node ID of the sidecar. This can be a path to a file or an ID string.</p> <p>Example file path: <code>file:/etc/graylog/sidecar/node-id</code></p> <p>Example ID string: <code>6033137e-d56b-47fc-9762-cd699c11a5a9</code></p> <p>Every sidecar instance needs a unique ID!</p> <p>Default: <code>file:/etc/graylog/sidecar/node-id</code></p>
<code>node_name</code>	<p>Name of the Sidecar instance, will also show up in the web interface.</p> <p>The host name will be used if not set.</p>
<code>update_interval</code>	<p>The interval where the sidecar will fetch new configurations from the Graylog server in seconds</p> <p>Default: <code>10</code></p> <p>The Graylog server considers all sidecars that frequently perform these updates "active". In order to globally configure a threshold which determines when a sidecar should be considered "inactive," please navigate to "Sidecars System" under the System/Configuration menu.</p>
<code>tls_skip_verify</code>	<p>This configures if the sidecar should skip the verification of TLS connections. Default: <code>false</code></p>
<code>send_status</code>	<p>This controls the transmission of detailed sidecar information like collector status, metrics and log file lists. It can be disabled to reduce load on the Graylog server if needed.</p> <p>Default: <code>true</code></p>
<code>list_log_files</code>	<p>Send a directory listing to Graylog and display it on the host status page, e.g. <code>/var/log</code>. This can also be a list of directories. Default: <code>[]</code></p>
<code>cache_path</code>	<p>The directory where the sidecar stores internal data. Default: <code>/var/cache/graylog-sidecar</code></p>
<code>collector_configuration_directory</code>	<p>The directory where the sidecar generates configurations for collectors.</p> <p>Default: <code>/var/lib/graylog-sidecar/generated</code></p>
<code>log_path</code>	<p>The directory where the sidecar stores its logs. Default: <code>/var/log/graylog-sidecar</code></p>
<code>log_rotate_max_file_size</code>	<p>The maximum size of the log file before it gets rotated. Default: <code>10MiB</code></p>
<code>log_rotate_keep_files</code>	<p>The maximum number of old log files to retain.</p>
<code>collector_binaries_accesslist</code>	<p>A list of binaries that are allowed to be executed by the Sidecar.</p> <p>An empty list disables the access list feature.</p> <p>Default: <code>/usr/bin/filebeat,/usr/bin/packetbeat,/usr/bin/metricbeat,/usr/bin/heartbeat,/usr/bin/auditbeat,/usr/bin/journalbeat,/usr/share/filebeat/bin/filebeat,/usr/share/packetbeat/bin/packetbeat,/usr/share/metricbeat/bin/metricbeat,/usr/share/heartbeat/bin/heartbeat,/usr/share/auditbeat/bin/auditbeat,/usr/share/journalbeat/bin/journalbeat,/usr/bin/nxlog,/opt/nxlog/bin/nxlog</code></p>
<code>tags</code>	<p>List of configuration tags. All configurations on the server side that match the tag list will be fetched and merged by this instance.</p>



[Graylog Home](#)

[Resources](#)

[Community](#)

[Blog](#)

[Videos](#)

[Webinars](#)

[Events](#)

[Graylog Academy](#)

[Release Notes](#)

[Customer Support](#)

© 2025 Graylog, Inc. | All rights reserved

[Privacy Policy](#) | [Legal](#)