How to Install ELK Stack

## Get Elasticsearch

You know, for search — and logging, and analytics, and more.

After downloading, watch [**Getting Started with Elasticsearch**](https://www.elastic.co/webinars/getting-started-elasticsearch?elektra=startpage).

##### Choose platform:

Linux

Install Elasticsearch with RPM

The RPM for Elasticsearch can be [downloaded from our website](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/rpm.html#install-rpm) or from our [RPM repository](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/rpm.html#rpm-repo). It can be used to install Elasticsearch on any RPM-based system such as OpenSuSE, SLES, Centos, Red Hat, and Oracle Enterprise.

RPM install is not supported on distributions with old versions of RPM, such as SLES 11 and CentOS 5. Please see [Install Elasticsearch from archive on Linux or MacOS](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/targz.html) instead.

This package contains both free and subscription features. [Start a 30-day trial](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/license-settings.html) to try out all of the features.

The latest stable version of Elasticsearch can be found on the [Download Elasticsearch](https://www.elastic.co/downloads/elasticsearch) page. Other versions can be found on the [Past Releases page](https://www.elastic.co/downloads/past-releases).

Elasticsearch includes a bundled version of [OpenJDK](https://openjdk.java.net/) from the JDK maintainers (GPLv2+CE). To use your own version of Java, see the [JVM version requirements](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/setup.html#jvm-version)

**Import the Elasticsearch GPG Key**

We sign all of our packages with the Elasticsearch Signing Key (PGP key [D88E42B4](https://pgp.mit.edu/pks/lookup?op=vindex&search=0xD27D666CD88E42B4), available from [https://pgp.mit.edu](https://pgp.mit.edu/)) with fingerprint:

4609 5ACC 8548 582C 1A26 99A9 D27D 666C D88E 42B4

Download and install the public signing key:

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

**Installing from the RPM repository**

Create a file called elasticsearch.repo in the /etc/yum.repos.d/ directory for RedHat based distributions, or in the /etc/zypp/repos.d/ directory for OpenSuSE based distributions, containing:

[elasticsearch]

name=Elasticsearch repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=0

autorefresh=1

type=rpm-md

And your repository is ready for use. You can now install Elasticsearch with one of the following commands:

sudo yum install --enablerepo=elasticsearch elasticsearch

sudo dnf install --enablerepo=elasticsearch elasticsearch

sudo zypper modifyrepo --enable elasticsearch && \

sudo zypper install elasticsearch; \

sudo zypper modifyrepo --disable elasticsearch

|  |  |
| --- | --- |
|  | Use yum on CentOS and older Red Hat based distributions. |
|  | Use dnf on Fedora and other newer Red Hat distributions. |
|  | Use zypper on OpenSUSE based distributions |

The configured repository is disabled by default. This eliminates the possibility of accidentally upgrading elasticsearch when upgrading the rest of the system. Each install or upgrade command must explicitly enable the repository as indicated in the sample commands above.

**Download and install the RPM manually**

The RPM for Elasticsearch v7.16.3 can be downloaded from the website and installed as follows:

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.16.3-x86\_64.rpm

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.16.3-x86\_64.rpm.sha512

shasum -a 512 -c elasticsearch-7.16.3-x86\_64.rpm.sha512

sudo rpm --install elasticsearch-7.16.3-x86\_64.rpm

|  |  |
| --- | --- |
|  | Compares the SHA of the downloaded RPM and the published checksum, which should output elasticsearch-{version}-x86\_64.rpm: OK. |

On systemd-based distributions, the installation scripts will attempt to set kernel parameters (e.g., vm.max\_map\_count); you can skip this by masking the systemd-sysctl.service unit.

**Enable automatic creation of system indices**

Some commercial features automatically create indices within Elasticsearch. By default, Elasticsearch is configured to allow automatic index creation, and no additional steps are required. However, if you have disabled automatic index creation in Elasticsearch, you must configure [action.auto\_create\_index](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/docs-index_.html" \l "index-creation" \o "Automatically create data streams and indices) in elasticsearch.yml to allow the commercial features to create the following indices:

action.auto\_create\_index: .monitoring\*,.watches,.triggered\_watches,.watcher-history\*,.ml\*

If you are using [Logstash](https://www.elastic.co/products/logstash) or [Beats](https://www.elastic.co/products/beats) then you will most likely require additional index names in your action.auto\_create\_index setting, and the exact value will depend on your local configuration. If you are unsure of the correct value for your environment, you may consider setting the value to \* which will allow automatic creation of all indices.

**SysV init vs systemd**

Elasticsearch is not started automatically after installation. How to start and stop Elasticsearch depends on whether your system uses SysV init or systemd (used by newer distributions). You can tell which is being used by running this command:

ps -p 1

**Running Elasticsearch with SysV init**

Use the chkconfig command to configure Elasticsearch to start automatically when the system boots up:

sudo chkconfig --add elasticsearch

Elasticsearch can be started and stopped using the service command:

sudo -i service elasticsearch start

sudo -i service elasticsearch stop

If Elasticsearch fails to start for any reason, it will print the reason for failure to STDOUT. Log files can be found in /var/log/elasticsearch/.

**Running Elasticsearch with systemd**

To configure Elasticsearch to start automatically when the system boots up, run the following commands:

sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable elasticsearch.service

Elasticsearch can be started and stopped as follows:

sudo systemctl start elasticsearch.service

sudo systemctl stop elasticsearch.service

These commands provide no feedback as to whether Elasticsearch was started successfully or not. Instead, this information will be written in the log files located in /var/log/elasticsearch/.

If you have password-protected your Elasticsearch keystore, you will need to provide systemd with the keystore password using a local file and systemd environment variables. This local file should be protected while it exists and may be safely deleted once Elasticsearch is up and running.

echo "keystore\_password" > /path/to/my\_pwd\_file.tmp

chmod 600 /path/to/my\_pwd\_file.tmp

sudo systemctl set-environment ES\_KEYSTORE\_PASSPHRASE\_FILE=/path/to/my\_pwd\_file.tmp

sudo systemctl start elasticsearch.service

By default the Elasticsearch service doesn’t log information in the systemd journal. To enable journalctl logging, the --quiet option must be removed from the ExecStart command line in the elasticsearch.service file.

When systemd logging is enabled, the logging information are available using the journalctl commands:

To tail the journal:

sudo journalctl -f

To list journal entries for the elasticsearch service:

sudo journalctl --unit elasticsearch

To list journal entries for the elasticsearch service starting from a given time:

sudo journalctl --unit elasticsearch --since "2016-10-30 18:17:16"

Check man journalctl or <https://www.freedesktop.org/software/systemd/man/journalctl.html> for more command line options.

**Checking that Elasticsearch is running**

You can test that your Elasticsearch node is running by sending an HTTP request to port 9200 on localhost:

GET /

Copy as curl[View in Console](http://localhost:5601/app/kibana#/dev_tools/console?load_from=https://www.elastic.co/guide/en/elasticsearch/reference/7.16/snippets/16.console)

which should give you a response something like this:

{

"name" : "Cp8oag6",

"cluster\_name" : "elasticsearch",

"cluster\_uuid" : "AT69\_T\_DTp-1qgIJlatQqA",

"version" : {

"number" : "7.16.3",

"build\_flavor" : "default",

"build\_type" : "tar",

"build\_hash" : "f27399d",

"build\_date" : "2016-03-30T09:51:41.449Z",

"build\_snapshot" : false,

"lucene\_version" : "8.10.1",

"minimum\_wire\_compatibility\_version" : "1.2.3",

"minimum\_index\_compatibility\_version" : "1.2.3"

},

"tagline" : "You Know, for Search"

}

**Configuring Elasticsearch**

The /etc/elasticsearch directory contains the default runtime configuration for Elasticsearch. The ownership of this directory and all contained files are set to root:elasticsearch on package installations.

The setgid flag applies group permissions on the /etc/elasticsearch directory to ensure that Elasticsearch can read any contained files and subdirectories. All files and subdirectories inherit the root:elasticsearch ownership. Running commands from this directory or any subdirectories, such as the [elasticsearch-keystore tool](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/secure-settings.html" \o "Secure settings), requires root:elasticsearch permissions.

Elasticsearch loads its configuration from the /etc/elasticsearch/elasticsearch.yml file by default. The format of this config file is explained in [*Configuring Elasticsearch*](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/settings.html).

The RPM also has a system configuration file (/etc/sysconfig/elasticsearch), which allows you to set the following parameters:

|  |  |
| --- | --- |
| ES\_JAVA\_HOME | Set a custom Java path to be used. |
| MAX\_OPEN\_FILES | Maximum number of open files, defaults to 65535. |
| MAX\_LOCKED\_MEMORY | Maximum locked memory size. Set to unlimited if you use the bootstrap.memory\_lock option in elasticsearch.yml. |
| MAX\_MAP\_COUNT | Maximum number of memory map areas a process may have. If you use mmapfs as index store type, make sure this is set to a high value. For more information, check the [linux kernel documentation](https://github.com/torvalds/linux/blob/master/Documentation/sysctl/vm.txt" \t "_top) about max\_map\_count. This is set via sysctl before starting Elasticsearch. Defaults to 262144. |
| ES\_PATH\_CONF | Configuration file directory (which needs to include elasticsearch.yml, jvm.options, and log4j2.properties files); defaults to /etc/elasticsearch. |
| ES\_JAVA\_OPTS | Any additional JVM system properties you may want to apply. |
| RESTART\_ON\_UPGRADE | Configure restart on package upgrade, defaults to false. This means you will have to restart your Elasticsearch instance after installing a package manually. The reason for this is to ensure, that upgrades in a cluster do not result in a continuous shard reallocation resulting in high network traffic and reducing the response times of your cluster. |

Distributions that use systemd require that system resource limits be configured via systemd rather than via the /etc/sysconfig/elasticsearch file. See [Systemd configuration](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/setting-system-settings.html" \l "systemd" \o "Systemd configuration) for more information.

**Directory layout of RPM**

The RPM places config files, logs, and the data directory in the appropriate locations for an RPM-based system:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Description** | **Default Location** | **Setting** |
| **home** | Elasticsearch home directory or $ES\_HOME | /usr/share/elasticsearch |  |
| **bin** | Binary scripts including elasticsearch to start a node and elasticsearch-plugin to install plugins | /usr/share/elasticsearch/bin |  |
| **conf** | Configuration files including elasticsearch.yml | /etc/elasticsearch | [ES\_PATH\_CONF](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/settings.html#config-files-location) |
| **conf** | Environment variables including heap size, file descriptors. | /etc/sysconfig/elasticsearch |  |
| **data** | The location of the data files of each index / shard allocated on the node. | /var/lib/elasticsearch | path.data |
| **jdk** | The bundled Java Development Kit used to run Elasticsearch. Can be overridden by setting the ES\_JAVA\_HOME environment variable in /etc/sysconfig/elasticsearch. | /usr/share/elasticsearch/jdk |  |
| **logs** | Log files location. | /var/log/elasticsearch | path.logs |
| **plugins** | Plugin files location. Each plugin will be contained in a subdirectory. | /usr/share/elasticsearch/plugins |  |
| **repo** | Shared file system repository locations. Can hold multiple locations. A file system repository can be placed in to any subdirectory of any directory specified here. | Not configured | path.repo |

## Configuring Elasticsearch

Elasticsearch ships with good defaults and requires very little configuration. Most settings can be changed on a running cluster using the [Cluster update settings](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/cluster-update-settings.html) API.

The configuration files should contain settings which are node-specific (such as node.name and paths), or settings which a node requires in order to be able to join a cluster, such as cluster.name and network.host.

### Config files location

Elasticsearch has three configuration files:

* elasticsearch.yml for configuring Elasticsearch
* jvm.options for configuring Elasticsearch JVM settings
* log4j2.properties for configuring Elasticsearch logging

These files are located in the config directory, whose default location depends on whether or not the installation is from an archive distribution (tar.gz or zip) or a package distribution (Debian or RPM packages).

For the archive distributions, the config directory location defaults to $ES\_HOME/config. The location of the config directory can be changed via the ES\_PATH\_CONF environment variable as follows:

ES\_PATH\_CONF=/path/to/my/config ./bin/elasticsearch

Alternatively, you can export the ES\_PATH\_CONF environment variable via the command line or via your shell profile.

For the package distributions, the config directory location defaults to /etc/elasticsearch. The location of the config directory can also be changed via the ES\_PATH\_CONF environment variable, but note that setting this in your shell is not sufficient. Instead, this variable is sourced from /etc/default/elasticsearch (for the Debian package) and /etc/sysconfig/elasticsearch (for the RPM package). You will need to edit the ES\_PATH\_CONF=/etc/elasticsearch entry in one of these files accordingly to change the config directory location.

### Config file format

The configuration format is [YAML](https://yaml.org/). Here is an example of changing the path of the data and logs directories:

path:

data: /var/lib/elasticsearch

logs: /var/log/elasticsearch

Settings can also be flattened as follows:

path.data: /var/lib/elasticsearch

path.logs: /var/log/elasticsearch

In YAML, you can format non-scalar values as sequences:

discovery.seed\_hosts:

- 192.168.1.10:9300

- 192.168.1.11

- seeds.mydomain.com

Though less common, you can also format non-scalar values as arrays:

discovery.seed\_hosts: ["192.168.1.10:9300", "192.168.1.11", "seeds.mydomain.com"]

### Environment variable substitution

Environment variables referenced with the ${...} notation within the configuration file will be replaced with the value of the environment variable. For example:

node.name: ${HOSTNAME}

network.host: ${ES\_NETWORK\_HOST}

Values for environment variables must be simple strings. Use a comma-separated string to provide values that Elasticsearch will parse as a list. For example, Elasticsearch will split the following string into a list of values for the ${HOSTNAME} environment variable:

export HOSTNAME="host1,host2"

### Cluster and node setting types

Cluster and node settings can be categorized based on how they are configured:

**Dynamic**

You can configure and update dynamic settings on a running cluster using the [cluster update settings API](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/cluster-update-settings.html). You can also configure dynamic settings locally on an unstarted or shut down node using elasticsearch.yml.

Updates made using the cluster update settings API can be persistent, which apply across cluster restarts, or transient, which reset after a cluster restart. You can also reset transient or persistent settings by assigning them a null value using the API.

If you configure the same setting using multiple methods, Elasticsearch applies the settings in following order of precedence:

1. Transient setting
2. Persistent setting
3. elasticsearch.yml setting
4. Default setting value

For example, you can apply a transient setting to override a persistent setting or elasticsearch.yml setting. However, a change to an elasticsearch.yml setting will not override a defined transient or persistent setting.

If you use Elasticsearch Service, use the [user settings](https://www.elastic.co/guide/en/cloud/current/ec-add-user-settings.html) feature to configure all cluster settings. This method lets Elasticsearch Service automatically reject unsafe settings that could break your cluster.

If you run Elasticsearch on your own hardware, use the [cluster update settings API](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/cluster-update-settings.html) to configure dynamic cluster settings. Only use elasticsearch.yml for static cluster settings and node settings. The API doesn’t require a restart and ensures a setting’s value is the same on all nodes.

We no longer recommend using transient cluster settings. Use persistent cluster settings instead. If a cluster becomes unstable, transient settings can clear unexpectedly, resulting in a potentially undesired cluster configuration. See the [Transient settings migration guide](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/transient-settings-migration-guide.html).

**Static**

Static settings can only be configured on an unstarted or shut down node using elasticsearch.yml.

Static settings must be set on every relevant node in the cluster.

1. **Get Logstash**

**Installing Logstash**

**Installing from a Downloaded Binary**

The Logstash binaries are available from https://www.elastic.co/downloads. Download the Logstash installation file for your host environment—​TARG.GZ, DEB, ZIP, or RPM.

Unpack the file. Do not install Logstash into a directory path that contains colon (:) characters.

These packages are free to use under the Elastic license. They contain open source and free commercial features and access to paid commercial features. Start a 30-day trial to try out all of the paid commercial features. See the Subscriptions page for information about Elastic license levels.

Alternatively, you can download an oss package, which contains only features that are available under the Apache 2.0 license.

On supported Linux operating systems, you can use a package manager to install Logstash.

Installing from Package Repositoriesedit

We also have repositories available for APT and YUM based distributions. Note that we only provide binary packages, but no source packages, as the packages are created as part of the Logstash build.

We have split the Logstash package repositories by version into separate urls to avoid accidental upgrades across major versions. For all 7.x.y releases use 7.x as version number.

We use the PGP key D88E42B4, Elastic’s Signing Key, with fingerprint

4609 5ACC 8548 582C 1A26 99A9 D27D 666C D88E 42B4

to sign all our packages. It is available from <https://pgp.mit.edu>.

**YUM**

Download and install the public signing key:

sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

Add the following in your /etc/yum.repos.d/ directory in a file with a .repo suffix, for example logstash.repo

[logstash-7.x]

name=Elastic repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

And your repository is ready for use. You can install it with:

sudo yum install logstash

1. **Get Kibana**

Your window into the Elastic Stack. Visualize and manage your data.After downloading, watch Getting Started with Kibana. Choose platform:

Install Kibana with RPM

The RPM for Kibana can be [downloaded from our website](https://www.elastic.co/guide/en/kibana/7.16/rpm.html#install-rpm) or from our [RPM repository](https://www.elastic.co/guide/en/kibana/7.16/rpm.html#rpm-repo). It can be used to install Kibana on any RPM-based system such as OpenSuSE, SLES, Centos, Red Hat, and Oracle Enterprise.

RPM install is not supported on distributions with old versions of RPM, such as SLES 11 and CentOS 5. Please see [Install from archive on Linux or macOS](https://www.elastic.co/guide/en/kibana/7.16/targz.html) instead.

This package contains both free and subscription features. [Start a 30-day trial](https://www.elastic.co/guide/en/kibana/7.16/managing-licenses.html) to try out all of the features.

The latest stable version of Kibana can be found on the [Download Kibana](https://www.elastic.co/downloads/kibana) page. Other versions can be found on the [Past Releases page](https://www.elastic.co/downloads/past-releases).

**Import the Elastic PGP key**

We sign all of our packages with the Elastic Signing Key (PGP key [D88E42B4](https://pgp.mit.edu/pks/lookup?op=vindex&search=0xD27D666CD88E42B4), available from [https://pgp.mit.edu](https://pgp.mit.edu/)) with fingerprint:

4609 5ACC 8548 582C 1A26 99A9 D27D 666C D88E 42B4

Download and install the public signing key:

rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

**Installing from the RPM repository**

Create a file called kibana.repo in the /etc/yum.repos.d/ directory for RedHat based distributions, or in the /etc/zypp/repos.d/ directory for OpenSuSE based distributions, containing:

[kibana-7.x]

name=Kibana repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

type=rpm-md

And your repository is ready for use. You can now install Kibana with one of the following commands:

sudo yum install kibana

sudo dnf install kibana

sudo zypper install kibana

|  |  |
| --- | --- |
|  | Use yum on CentOS and older Red Hat based distributions. |
|  | Use dnf on Fedora and other newer Red Hat distributions. |
|  | Use zypper on OpenSUSE based distributions |

**Download and install the RPM manually**

The RPM for Kibana v7.16.3 can be downloaded from the website and installed as follows:

wget https://artifacts.elastic.co/downloads/kibana/kibana-7.16.3-x86\_64.rpm

shasum -a 512 kibana-7.16.3-x86\_64.rpm

sudo rpm --install kibana-7.16.3-x86\_64.rpm

|  |  |
| --- | --- |
|  | Compare the SHA produced by shasum with the [published SHA](https://artifacts.elastic.co/downloads/kibana/kibana-7.16.3-x86_64.rpm.sha512). |

**SysV init vs systemd**

Kibana is not started automatically after installation. How to start and stop Kibana depends on whether your system uses SysV init or systemd (used by newer distributions). You can tell which is being used by running this command:

ps -p 1

**Run Kibana with SysV init**

Use the chkconfig command to configure Kibana to start automatically when the system boots up:

sudo chkconfig --add kibana

You can start and stop Kibana using the service command:

sudo -i service kibana start

sudo -i service kibana stop

If Kibana fails to start for any reason, it will print the reason for failure to STDOUT. Log files can be found in /var/log/kibana/.

**Run Kibana with systemd**

To configure Kibana to start automatically when the system boots up, run the following commands:

sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable kibana.service

Kibana can be started and stopped as follows:

sudo systemctl start kibana.service

sudo systemctl stop kibana.service

These commands provide no feedback as to whether Kibana was started successfully or not. Log information can be accessed via journalctl -u kibana.service.

**Configure Kibana via the config file**

Kibana loads its configuration from the /etc/kibana/kibana.yml file by default. The format of this config file is explained in [Configuring Kibana](https://www.elastic.co/guide/en/kibana/7.16/settings.html).

**Directory layout of RPM**

The RPM places config files, logs, and the data directory in the appropriate locations for an RPM-based system:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Description** | **Default Location** | **Setting** |
| **home** | Kibana home directory or $KIBANA\_HOME | /usr/share/kibana |  |
| **bin** | Binary scripts including kibana to start the Kibana server and kibana-plugin to install plugins | /usr/share/kibana/bin |  |
| **config** | Configuration files including kibana.yml | /etc/kibana | [KBN\_PATH\_CONF](https://www.elastic.co/guide/en/kibana/7.16/settings.html) |
| **data** | The location of the data files written to disk by Kibana and its plugins | /var/lib/kibana | path.data |
| **logs** | Logs files location | /var/log/kibana | path.logs |
| **plugins** | Plugin files location. Each plugin will be contained in a subdirectory. | /usr/share/kibana/plugins |  |

Configure Kibana

The Kibana server reads properties from the kibana.yml file on startup. The location of this file differs depending on how you installed Kibana. For example, if you installed Kibana from an archive distribution (.tar.gz or .zip), by default it is in $KIBANA\_HOME/config. By default, with package distributions (Debian or RPM), it is in /etc/kibana. The config directory can be changed via the KBN\_PATH\_CONF environment variable:

KBN\_PATH\_CONF=/home/kibana/config ./bin/kibana

The default host and port settings configure Kibana to run on localhost:5601. To change this behavior and allow remote users to connect, you’ll need to update your kibana.yml file. You can also enable SSL and set a variety of other options. Finally, environment variables can be injected into configuration using ${MY\_ENV\_VAR} syntax.

|  |  |
| --- | --- |
| console.ui.enabled: | Toggling this causes the server to regenerate assets on the next startup, which may cause a delay before pages start being served. Set to false to disable Console. **Default: true** |
| console.enabled: | [~~7.16.0~~] Deprecated in 7.16.0. In 8.0 and later, this setting will no longer be supported.Set to false to disable Console. **Default: true** |
| cpu.cgroup.path.override: | [~~7.10.0~~] Deprecated in 7.10.0. In 8.0 and later, this setting will no longer be supported.This setting has been renamed to [ops.cGroupOverrides.cpuPath](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "ops-cGroupOverrides-cpuPath). |
| cpuacct.cgroup.path.override: | [~~7.10.0~~] Deprecated in 7.10.0. In 8.0 and later, this setting will no longer be supported.This setting has been renamed to [ops.cGroupOverrides.cpuAcctPath](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "ops-cGroupOverrides-cpuAcctPath). |
| csp.rules: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.A [Content Security Policy](https://w3c.github.io/webappsec-csp/) template that disables certain unnecessary and potentially insecure capabilities in the browser. It is strongly recommended that you keep the default CSP rules that ship with Kibana. |
| csp.script\_src: | Add sources for the [Content Security Policy script-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/script-src). |
| csp.worker\_src: | Add sources for the [Content Security Policy worker-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/worker-src). |
| csp.style\_src: | Add sources for the [Content Security Policy style-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/style-src). |
| csp.connect\_src: | Add sources for the [Content Security Policy connect-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/connect-src). |
| csp.default\_src: | Add sources for the [Content Security Policy default-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/default-src). |
| csp.font\_src: | Add sources for the [Content Security Policy font-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/font-src). |
| csp.frame\_src: | Add sources for the [Content Security Policy frame-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-src). |
| csp.img\_src: | Add sources for the [Content Security Policy img-src directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/img-src). |
| csp.frame\_ancestors: | Add sources for the [Content Security Policy frame-ancestors directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-ancestors). |

The frame-ancestors directive can also be configured by using [server.securityResponseHeaders.disableEmbedding](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-securityResponseHeaders-disableEmbedding). In that case, that takes precedence and any values in csp.frame\_ancestors are ignored.

|  |  |
| --- | --- |
| csp.report\_uri: | Add sources for the [Content Security Policy report-uri directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/report-uri). |
| csp.report\_to: | Add sources for the [Content Security Policy report-to directive](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/report-to). |
| csp.strict: | Blocks Kibana access to any browser that does not enforce even rudimentary CSP rules. In practice, this disables support for older, less safe browsers like Internet Explorer. For more information, refer to [Content Security Policy](https://www.elastic.co/guide/en/kibana/7.16/Security-production-considerations.html#csp-strict-mode). **Default: true** |
| csp.warnLegacyBrowsers: | Shows a warning message after loading Kibana to any browser that does not enforce even rudimentary CSP rules, though Kibana is still accessible. This configuration is effectively ignored when [csp.strict](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "csp-strict) is enabled. **Default: true** |
| elasticsearch.customHeaders: | Header names and values to send to Elasticsearch. Any custom headers cannot be overwritten by client-side headers, regardless of the [elasticsearch.requestHeadersWhitelist](https://www.elastic.co/guide/en/kibana/7.16/settings.html#elasticsearch-requestHeadersWhitelist) configuration. **Default: {}** |
| elasticsearch.hosts: | The URLs of the Elasticsearch instances to use for all your queries. All nodes listed here must be on the same cluster. **Default: [ "http://localhost:9200" ]**  To enable SSL/TLS for outbound connections to Elasticsearch, use the https protocol in this setting. |
| elasticsearch.logQueries: | [~~7.12.0~~] Deprecated in 7.12.0. This setting is no longer used and will be removed in Kibana 8.0.Instead, configure the elasticsearch.query logger. This is useful for seeing the query DSL generated by applications that currently do not have an inspector, for example Timelion and Monitoring. **Default: false**  The following example shows a valid elasticsearch.query logger configuration: |

logging:

appenders:

console\_appender:

type: console

layout:

type: pattern

highlight: true

root:

appenders: [default, console\_appender]

level: warn

loggers:

- name: elasticsearch.query

level: debug

|  |  |
| --- | --- |
| elasticsearch.pingTimeout: | Time in milliseconds to wait for Elasticsearch to respond to pings. **Default: the value of the**[elasticsearch.requestTimeout](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-requestTimeout)**setting** |
| elasticsearch.requestHeadersWhitelist: | List of Kibana client-side headers to send to Elasticsearch. To send **no** client-side headers, set this value to [] (an empty list). Removing the authorization header from being whitelisted means that you cannot use [basic authentication](https://www.elastic.co/guide/en/kibana/7.16/kibana-authentication.html#basic-authentication) in Kibana. **Default: [ 'authorization' ]** |
| elasticsearch.requestTimeout: | Time in milliseconds to wait for responses from the back end or Elasticsearch. This value must be a positive integer. **Default: 30000** |
| elasticsearch.shardTimeout: | Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable. **Default: 30000** |
| elasticsearch.sniffInterval: | Time in milliseconds between requests to check Elasticsearch for an updated list of nodes. **Default: false** |
| elasticsearch.sniffOnStart: | Attempt to find other Elasticsearch nodes on startup. **Default: false** |
| elasticsearch.sniffOnConnectionFault: | Update the list of Elasticsearch nodes immediately following a connection fault. **Default: false** |
| elasticsearch.ssl.alwaysPresentCertificate: | Controls Kibana behavior in regard to presenting a client certificate when requested by Elasticsearch. This setting applies to all outbound SSL/TLS connections to Elasticsearch, including requests that are proxied for end users. **Default: false** |

When Elasticsearch uses certificates to authenticate end users with a PKI realm and [elasticsearch.ssl.alwaysPresentCertificate](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-ssl-alwaysPresentCertificate) is true, proxied requests may be executed as the identity that is tied to the Kibana server.

|  |  |
| --- | --- |
| elasticsearch.ssl.certificate: and elasticsearch.ssl.key: | Paths to a PEM-encoded X.509 client certificate and its corresponding private key. These are used by Kibana to authenticate itself when making outbound SSL/TLS connections to Elasticsearch. For this setting to take effect, the xpack.security.http.ssl.client\_authentication setting in Elasticsearch must be also be set to "required" or "optional" to request a client certificate from Kibana. |

These settings cannot be used in conjunction with [elasticsearch.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-ssl-keystore-path).

|  |  |
| --- | --- |
| elasticsearch.ssl.certificateAuthorities: | Paths to one or more PEM-encoded X.509 certificate authority (CA) certificates, which make up a trusted certificate chain for Elasticsearch. This chain is used by Kibana to establish trust when making outbound SSL/TLS connections to Elasticsearch.  In addition to this setting, trusted certificates may be specified via [elasticsearch.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html#elasticsearch-ssl-keystore-path) and/or [elasticsearch.ssl.truststore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html#elasticsearch-ssl-truststore-path). |
| elasticsearch.ssl.keyPassphrase: | The password that decrypts the private key that is specified via [elasticsearch.ssl.key](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-ssl-cert-key). This value is optional, as the key may not be encrypted. |
| elasticsearch.ssl.keystore.path: | Path to a PKCS#12 keystore that contains an X.509 client certificate and it’s corresponding private key. These are used by Kibana to authenticate itself when making outbound SSL/TLS connections to Elasticsearch. For this setting, you must also set the xpack.security.http.ssl.client\_authentication setting in Elasticsearch to "required" or "optional" to request a client certificate from Kibana.  If the keystore contains any additional certificates, they are used as a trusted certificate chain for Elasticsearch. This chain is used by Kibana to establish trust when making outbound SSL/TLS connections to Elasticsearch. In addition to this setting, trusted certificates may be specified via [elasticsearch.ssl.certificateAuthorities](https://www.elastic.co/guide/en/kibana/7.16/settings.html#elasticsearch-ssl-certificateAuthorities) and/or [elasticsearch.ssl.truststore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html#elasticsearch-ssl-truststore-path). |

This setting cannot be used in conjunction with [elasticsearch.ssl.certificate](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-ssl-cert-key) or [elasticsearch.ssl.key](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-ssl-cert-key).

|  |  |
| --- | --- |
| elasticsearch.ssl.keystore.password: | The password that decrypts the keystore specified via [elasticsearch.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-ssl-keystore-path). If the keystore has no password, leave this as blank. If the keystore has an empty password, set this to "". |
| elasticsearch.ssl.truststore.path: | Path to a PKCS#12 trust store that contains one or more X.509 certificate authority (CA) certificates, which make up a trusted certificate chain for Elasticsearch. This chain is used by Kibana to establish trust when making outbound SSL/TLS connections to Elasticsearch.  In addition to this setting, trusted certificates may be specified via [elasticsearch.ssl.certificateAuthorities](https://www.elastic.co/guide/en/kibana/7.16/settings.html#elasticsearch-ssl-certificateAuthorities) and/or [elasticsearch.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html#elasticsearch-ssl-keystore-path). |
| elasticsearch.ssl.truststore.password: | The password that decrypts the trust store specified via [elasticsearch.ssl.truststore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "elasticsearch-ssl-truststore-path). If the trust store has no password, leave this as blank. If the trust store has an empty password, set this to "". |
| elasticsearch.ssl.verificationMode: | Controls the verification of the server certificate that Kibana receives when making an outbound SSL/TLS connection to Elasticsearch. Valid values are "full", "certificate", and "none". Using "full" performs hostname verification, using "certificate" skips hostname verification, and using "none" skips verification entirely. **Default: "full"** |
| elasticsearch.username: and elasticsearch.password: | If your Elasticsearch is protected with basic authentication, these settings provide the username and password that the Kibana server uses to perform maintenance on the Kibana index at startup. Kibana users still need to authenticate with Elasticsearch, which is proxied through the Kibana server. |
| elasticsearch.serviceAccountToken: | [beta] This functionality is in beta and is subject to change. The design and code is less mature than official GA features and is being provided as-is with no warranties. Beta features are not subject to the support SLA of official GA features.. If your Elasticsearch is protected with basic authentication, this token provides the credentials that the Kibana server uses to perform maintenance on the Kibana index at startup. This setting is an alternative to elasticsearch.username and elasticsearch.password. |
| enterpriseSearch.host | The http(s) URL of your Enterprise Search instance. For example, in a local self-managed setup, set this to http://localhost:3002. Authentication between Kibana and the Enterprise Search host URL, such as via OAuth, is not supported. You can also [configure Kibana to trust your Enterprise Search TLS certificate authority](https://www.elastic.co/guide/en/enterprise-search/7.16/configure-ssl-tls.html#configure-ssl-tls-in-kibana). |
| interpreter.enableInVisualize | Enables use of interpreter in Visualize. **Default: true** |
| kibana.defaultAppId: | [~~7.9.0~~] Deprecated in 7.9.0. This setting will be removed in Kibana 8.0.Instead, use the [defaultRoute advanced setting](https://www.elastic.co/guide/en/kibana/7.16/advanced-options.html" \l "defaultroute). The default application to load. **Default: "home"** |
| kibana.index: | [~~7.11.0~~] Deprecated in 7.11.0. This setting will be removed in 8.0.Multitenancy by changing kibana.index will not be supported starting in 8.0. See [8.0 Breaking Changes](https://ela.st/kbn-remove-legacy-multitenancy) for more details. Kibana uses an index in Elasticsearch to store saved searches, visualizations, and dashboards. Kibana creates a new index if the index doesn’t already exist. If you configure a custom index, the name must be lowercase, and conform to the Elasticsearch [index name limitations](https://www.elastic.co/guide/en/elasticsearch/reference/7.16/indices-create-index.html). **Default: ".kibana"** |
| data.autocomplete.valueSuggestions.timeout: | Time in milliseconds to wait for autocomplete suggestions from Elasticsearch. This value must be a whole number greater than zero. **Default: "1000"** |
| data.autocomplete.valueSuggestions.terminateAfter: | Maximum number of documents loaded by each shard to generate autocomplete suggestions. This value must be a whole number greater than zero. **Default: "100000"** |

To reload the logging settings, send a SIGHUP signal to Kibana.

|  |  |
| --- | --- |
| logging.root: | The [root logger](https://www.elastic.co/guide/en/kibana/7.16/logging-service.html#logging-service) has a dedicated configuration node since this context name is special and is pre-configured for logging by default. |
| logging.root.appenders: | A list of logging appenders to forward the root level logger instance to. By default root is configured with the default appender that must be included in the list. This is the configuration that all custom loggers will use unless they’re re-configured explicitly. Additional appenders, if configured, can be included in the list. |
| logging.root.level: | Level at which a log record should be logged. Supported levels are: *all*, *fatal*, *error*, *warn*, *info*, *debug*, *trace*, *off*. Levels are ordered from *all* (highest) to *off* and a log record will be logged it its level is higher than or equal to the level of its logger, otherwise the log record is ignored. Use this value to [change the overall log level](https://www.elastic.co/guide/en/kibana/7.16/logging-settings.html#change-overall-log-level). Set to all to log all events, including system usage information and all requests. Set to off to silence all logs. **Default: info**. |
| logging.loggers: | Allows you to [customize a specific logger instance](https://www.elastic.co/guide/en/kibana/7.16/logging-settings.html#customize-specific-log-records). |
| logging.loggers.name: | Specific logger instance. |
| logging.loggers.level: | Level at which a log record should be shown. Supported levels are: *all*, *fatal*, *error*, *warn*, *info*, *debug*, *trace*, *off*. |
| logging.loggers.appenders: | Specific appender format to apply for a particular logger context. |
| logging.appenders: | [Appenders](https://www.elastic.co/guide/en/kibana/7.16/logging-service.html#logging-appenders) define how and where log messages are displayed (eg. **stdout** or console) and stored (eg. file on the disk). |
| logging.appenders.console: | Appender to use for logging records to **stdout**. By default, uses the [%date][%level][%logger] %message **pattern** layout. To use a **json**, set the [layout type to json](https://www.elastic.co/guide/en/kibana/7.16/logging-settings.html#log-in-json-ECS-example). |
| logging.appenders.file: | Allows you to specify a fileName to send log records to on disk. To send [all log records to file](https://www.elastic.co/guide/en/kibana/7.16/logging-settings.html#log-to-file-example), add the file appender to root.appenders. |
| logging.appenders.rolling-file: | Similar to Log4j’s RollingFileAppender, this appender will log into a file and rotate if following a rolling strategy when the configured policy triggers. There are currently two policies supported: size-limit and time-interval.  The size limit policy will perform a rollover when the log file reaches a maximum size. **Default 100mb**  The time interval policy will rotate the log file every given interval of time. **Default 24h** |
| map.includeElasticMapsService: | Set to false to disable connections to Elastic Maps Service. When includeElasticMapsService is turned off, only tile layer configured by [map.tilemap.url](https://www.elastic.co/guide/en/kibana/7.16/settings.html#tilemap-url) is available in [Maps](https://www.elastic.co/guide/en/kibana/7.16/maps.html). **Default: true** |
| map.emsUrl: | Specifies the URL of a self hosted [Elastic Maps Server](https://www.elastic.co/guide/en/kibana/7.16/maps-connect-to-ems.html#elastic-maps-server) |
| map.proxyElasticMapsServiceInMaps: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Set to true to proxy all [Maps application](https://www.elastic.co/guide/en/kibana/7.16/maps.html) Elastic Maps Service requests through the Kibana server. **Default: false** |
| map.regionmap: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Specifies additional vector layers for use in [Maps](https://www.elastic.co/guide/en/kibana/7.16/maps.html) visualizations. Each layer object points to an external vector file that contains a geojson FeatureCollection. The file must use the [WGS84 coordinate reference system (ESPG:4326)](https://en.wikipedia.org/wiki/World_Geodetic_System) and only include polygons. If the file is hosted on a separate domain from Kibana, the server needs to be CORS-enabled so Kibana can download the file. The following example shows a valid region map configuration. |

map.regionmap:

layers:

- name: "Departments of France"

url: "http://my.cors.enabled.server.org/france\_departements.geojson"

attribution: "INRAP"

fields:

- name: "department"

description: "Full department name"

- name: "INSEE"

description: "INSEE numeric identifier"

|  |  |
| --- | --- |
| map.regionmap.layers[].attribution: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Optional. References the originating source of the geojson file. |
| map.regionmap.layers[].fields[]: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Mandatory. Each layer can contain multiple fields to indicate what properties from the geojson features you wish to expose. The following shows how to define multiple properties: |

map.regionmap:

layers:

- name: "Departments of France"

url: "http://my.cors.enabled.server.org/france\_departements.geojson"

attribution: "INRAP"

fields:

- name: "department"

description: "Full department name"

- name: "INSEE"

description: "INSEE numeric identifier"

|  |  |
| --- | --- |
| map.regionmap.layers[].fields[].description: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Mandatory. The human readable text that is shown under the Options tab when building the Region Map visualization. |
| map.regionmap.layers[].fields[].name: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Mandatory. This value is used to do an inner-join between the document stored in Elasticsearch and the geojson file. For example, if the field in the geojson is called Location and has city names, there must be a field in Elasticsearch that holds the same values that Kibana can then use to lookup for the geoshape data. |
| map.regionmap.layers[].name: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Mandatory. A description of the map being provided. |
| map.regionmap.layers[].url: | [~~7.14.0~~] Deprecated in 7.14.0. In 8.0 and later, this setting will no longer be supported.Mandatory. The location of the geojson file as provided by a webserver. |
| map.tilemap.options.attribution: | The map attribution string. **Default: "© [Elastic Maps Service](https://www.elastic.co/elastic-maps-service)"** |
| map.tilemap.options.maxZoom: | The maximum zoom level. **Default: 10** |
| map.tilemap.options.minZoom: | The minimum zoom level. **Default: 1** |
| map.tilemap.options.subdomains: | An array of subdomains used by the tile service. Specify the position of the subdomain the URL with the token {s}. |
| map.tilemap.url: | The URL to the tileservice that Kibana uses to display map tiles in tilemap visualizations. By default, Kibana reads this URL from an external metadata service, but users can override this parameter to use their own Tile Map Service. For example: "https://tiles.elastic.co/v2/default/{z}/{x}/{y}.png?elastic\_tile\_service\_tos=agree&my\_app\_name=kibana" |
| migrations.batchSize: | Defines the number of documents migrated at a time. The higher the value, the faster the Saved Objects migration process performs at the cost of higher memory consumption. If upgrade migrations results in Kibana crashing with an out of memory exception or fails due to an Elasticsearch circuit\_breaking\_exception, use a smaller batchSize value to reduce the memory pressure. **Default: 1000** |
| migrations.maxBatchSizeBytes: | Defines the maximum payload size for indexing batches of upgraded saved objects to avoid migrations failing due to a 413 Request Entity Too Large response from Elasticsearch. This value should be lower than or equal to your Elasticsearch cluster’s http.max\_content\_length configuration option. **Default: 100mb** |
| migrations.retryAttempts: | The number of times migrations retry temporary failures, such as a network timeout, 503 status code, or snapshot\_in\_progress\_exception. When upgrade migrations frequently fail after exhausting all retry attempts with a message such as Unable to complete the [...] step after 15 attempts, terminating., increase the setting value. **Default: 15** |
| newsfeed.enabled: | Controls whether to enable the newsfeed system for the Kibana UI notification center. Set to false to disable the newsfeed system. **Default: true** |
| path.data: | The path where Kibana stores persistent data not saved in Elasticsearch. **Default: data** |
| pid.file: | Specifies the path where Kibana creates the process ID file. |
| ops.interval: | Set the interval in milliseconds to sample system and process performance metrics. The minimum value is 100. **Default: 5000** |
| ops.cGroupOverrides.cpuPath: | Override for cgroup cpu path when mounted in a manner that is inconsistent with /proc/self/cgroup. |
| ops.cGroupOverrides.cpuAcctPath: | Override for cgroup cpuacct path when mounted in a manner that is inconsistent with /proc/self/cgroup. |
| savedObjects.maxImportExportSize: | The maximum count of saved objects that can be imported or exported. This setting exists to prevent the Kibana server from runnning out of memory when handling large numbers of saved objects. It is recommended to only raise this setting if you are confident your server can hold this many objects in memory. **Default: 10000** |
| savedObjects.maxImportPayloadBytes: | The maximum byte size of a saved objects import that the Kibana server will accept. This setting exists to prevent the Kibana server from runnning out of memory when handling a large import payload. Note that this setting overrides the more general [server.maxPayload](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-maxPayload) for saved object imports only. **Default: 26214400** |
| server.basePath: | Enables you to specify a path to mount Kibana at if you are running behind a proxy. Use the [server.rewriteBasePath](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-rewriteBasePath) setting to tell Kibana if it should remove the basePath from requests it receives, and to prevent a deprecation warning at startup. This setting cannot end in a slash (/). |
| server.publicBaseUrl: | The publicly available URL that end-users access Kibana at. Must include the protocol, hostname, port (if different than the defaults for http and https, 80 and 443 respectively), and the [server.basePath](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-basePath) (if configured). This setting cannot end in a slash (/). |
| server.compression.enabled: | Set to false to disable HTTP compression for all responses. **Default: true** |
| server.cors.enabled: | [experimental] This functionality is in technical preview and may be changed or removed in a future release. Elastic will apply best effort to fix any issues, but features in technical preview are not subject to the support SLA of official GA features.Set to true to allow cross-origin API calls. **Default:** false |
| server.cors.allowCredentials: | [experimental] This functionality is in technical preview and may be changed or removed in a future release. Elastic will apply best effort to fix any issues, but features in technical preview are not subject to the support SLA of official GA features.Set to true to allow browser code to access response body whenever request performed with user credentials. **Default:** false |
| server.cors.allowOrigin: | [experimental] This functionality is in technical preview and may be changed or removed in a future release. Elastic will apply best effort to fix any issues, but features in technical preview are not subject to the support SLA of official GA features.List of origins permitted to access resources. You must specify explicit hostnames and not use server.cors.allowOrigin: ["\*"] when server.cors.allowCredentials: true. **Default:** ["\*"] |
| server.compression.referrerWhitelist: | Specifies an array of trusted hostnames, such as the Kibana host, or a reverse proxy sitting in front of it. This determines whether HTTP compression may be used for responses, based on the request Referer header. This setting may not be used when [server.compression.enabled](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-compression) is set to false. **Default: none** |
| server.securityResponseHeaders: strictTransportSecurity: | Controls whether the [Strict-Transport-Security](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) header is used in all responses to the client from the Kibana server, and specifies what value is used. Allowed values are any text value or null. To disable, set to null. **Default:** null |
| server.securityResponseHeaders: xContentTypeOptions: | Controls whether the [X-Content-Type-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) header is used in all responses to the client from the Kibana server, and specifies what value is used. Allowed values are nosniff or null. To disable, set to null. **Default:** "nosniff" |
| server.securityResponseHeaders: referrerPolicy: | Controls whether the [Referrer-Policy](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy) header is used in all responses to the client from the Kibana server, and specifies what value is used. Allowed values are no-referrer, no-referrer-when-downgrade, origin, origin-when-cross-origin, same-origin, strict-origin, strict-origin-when-cross-origin, unsafe-url, or null. To disable, set to null. **Default:** "no-referrer-when-downgrade" |
| server.securityResponseHeaders: permissionsPolicy: | [experimental] This functionality is in technical preview and may be changed or removed in a future release. Elastic will apply best effort to fix any issues, but features in technical preview are not subject to the support SLA of official GA features.Controls whether the [Permissions-Policy](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy) header is used in all responses to the client from the Kibana server, and specifies what value is used. Allowed values are any text value or null. To disable, set to null. **Default:** null |
| server.securityResponseHeaders: disableEmbedding: | Controls whether the [Content-Security-Policy](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy) and [X-Frame-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options) headers are configured to disable embedding Kibana in other webpages using iframes. When set to true, secure headers are used to disable embedding, which adds the frame-ancestors: 'self' directive to the Content-Security-Policy response header (if you are using the default CSP rules), and adds the X-Frame-Options: SAMEORIGIN response header. **Default:** false |
| server.customResponseHeaders: | Header names and values to send on all responses to the client from the Kibana server. **Default: {}** |
| server.shutdownTimeout: | Sets the grace period for Kibana to attempt to resolve any ongoing HTTP requests after receiving a SIGTERM/SIGINT signal, and before shutting down. Any new HTTP requests received during this period are rejected with a 503 response. **Default: 30s** |
| server.host: | This setting specifies the host of the back end server. To allow remote users to connect, set the value to the IP address or DNS name of the Kibana server. **Default: "localhost"** |
| server.keepaliveTimeout: | The number of milliseconds to wait for additional data before restarting the [server.socketTimeout](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-socketTimeout) counter. **Default: "120000"** |
| server.maxPayloadBytes: | [~~7.13.0~~] Deprecated in 7.13.0. In 8.0 and later, this setting will no longer be supported.This setting has been renamed to [server.maxPayload](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-maxPayload). |
| server.maxPayload: | The maximum payload size in bytes for incoming server requests. **Default: 1048576** |
| server.name: | A human-readable display name that identifies this Kibana instance. **Default: "your-hostname"** |
| server.port: | Kibana is served by a back end server. This setting specifies the port to use. **Default: 5601** |
| server.requestId.allowFromAnyIp: | Sets whether or not the X-Opaque-Id header should be trusted from any IP address for identifying requests in logs and forwarded to Elasticsearch. |
| server.requestId.ipAllowlist: | A list of IPv4 and IPv6 address which the X-Opaque-Id header should be trusted from. Normally this would be set to the IP addresses of the load balancers or reverse-proxy that end users use to access Kibana. If any are set, [server.requestId.allowFromAnyIp](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-requestId-allowFromAnyIp) must also be set to false. |
| server.rewriteBasePath: | Specifies whether Kibana should rewrite requests that are prefixed with [server.basePath](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-basePath) or require that they are rewritten by your reverse proxy. In Kibana 6.3 and earlier, the default is false. In Kibana 7.x, the setting is deprecated. In Kibana 8.0 and later, the default is true. **Default: deprecated** |
| server.socketTimeout: | The number of milliseconds to wait before closing an inactive socket. **Default: "120000"** |
| server.ssl.certificate: and server.ssl.key: | Paths to a PEM-encoded X.509 server certificate and its corresponding private key. These are used by Kibana to establish trust when receiving inbound SSL/TLS connections from users. |
| server.uuid: | The unique identifier for this Kibana instance. |

These settings cannot be used in conjunction with [server.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-keystore-path).

|  |  |
| --- | --- |
| server.ssl.certificateAuthorities: | Paths to one or more PEM-encoded X.509 certificate authority (CA) certificates which make up a trusted certificate chain for Kibana. This chain is used by Kibana to establish trust when receiving inbound SSL/TLS connections from end users. If PKI authentication is enabled, this chain is also used by Kibana to verify client certificates from end users.  In addition to this setting, trusted certificates may be specified via [server.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-keystore-path) and/or [server.ssl.truststore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-truststore-path). |
| server.ssl.cipherSuites: | Details on the format, and the valid options, are available via the [OpenSSL cipher list format documentation](https://www.openssl.org/docs/man1.1.1/man1/ciphers.html#CIPHER-LIST-FORMAT). **Default: TLS\_AES\_256\_GCM\_SHA384 TLS\_CHACHA20\_POLY1305\_SHA256 TLS\_AES\_128\_GCM\_SHA256 ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384, DHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, DHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-SHA256, DHE-RSA-AES256-SHA256, HIGH,!aNULL, !eNULL, !EXPORT, !DES, !RC4, !MD5, !PSK, !SRP, !CAMELLIA**. |
| server.ssl.clientAuthentication: | Controls the behavior in Kibana for requesting a certificate from client connections. Valid values are "required", "optional", and "none". Using "required" will refuse to establish the connection unless a client presents a certificate, using "optional" will allow a client to present a certificate if it has one, and using "none" will prevent a client from presenting a certificate. **Default: "none"** |
| server.ssl.enabled: | Enables SSL/TLS for inbound connections to Kibana. When set to true, a certificate and its corresponding private key must be provided. These can be specified via [server.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-keystore-path) or the combination of [server.ssl.certificate](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-cert-key) and [server.ssl.key](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-cert-key). **Default: false** |
| server.ssl.keyPassphrase: | The password that decrypts the private key that is specified via [server.ssl.key](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-cert-key). This value is optional, as the key may not be encrypted. |
| server.ssl.keystore.path: | Path to a PKCS#12 keystore that contains an X.509 server certificate and its corresponding private key. If the keystore contains any additional certificates, those will be used as a trusted certificate chain for Kibana. All of these are used by Kibana to establish trust when receiving inbound SSL/TLS connections from end users. The certificate chain is also used by Kibana to verify client certificates from end users when PKI authentication is enabled.  In addition to this setting, trusted certificates may be specified via [server.ssl.certificateAuthorities](https://www.elastic.co/guide/en/kibana/7.16/settings.html#server-ssl-certificateAuthorities) and/or [server.ssl.truststore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html#server-ssl-truststore-path). |

This setting cannot be used in conjunction with [server.ssl.certificate](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-cert-key) or [server.ssl.key](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-cert-key)

|  |  |
| --- | --- |
| server.ssl.keystore.password: | The password that will be used to decrypt the keystore specified via [server.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-keystore-path). If the keystore has no password, leave this unset. If the keystore has an empty password, set this to "". |
| server.ssl.truststore.path: | Path to a PKCS#12 trust store that contains one or more X.509 certificate authority (CA) certificates which make up a trusted certificate chain for Kibana. This chain is used by Kibana to establish trust when receiving inbound SSL/TLS connections from end users. If PKI authentication is enabled, this chain is also used by Kibana to verify client certificates from end users.  In addition to this setting, trusted certificates may be specified via [server.ssl.certificateAuthorities](https://www.elastic.co/guide/en/kibana/7.16/settings.html#server-ssl-certificateAuthorities) and/or [server.ssl.keystore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html#server-ssl-keystore-path). |
| server.ssl.truststore.password: | The password that will be used to decrypt the trust store specified via [server.ssl.truststore.path](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-ssl-truststore-path). If the trust store has no password, leave this unset. If the trust store has an empty password, set this to "". |
| server.ssl.redirectHttpFromPort: | Kibana binds to this port and redirects all http requests to https over the port configured as [server.port](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "server-port). |
| server.ssl.supportedProtocols: | An array of supported protocols with versions. Valid protocols: TLSv1, TLSv1.1, TLSv1.2, TLSv1.3. **Default: TLSv1.1, TLSv1.2, TLSv1.3** |
| server.xsrf.allowlist: | It is not recommended to disable protections for arbitrary API endpoints. Instead, supply the kbn-xsrf header. The [server.xsrf.allowlist](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "settings-xsrf-allowlist) setting requires the following format: |

\*Default: [ ]\* An array of API endpoints which should be exempt from Cross-Site Request Forgery ("XSRF") protections.

|  |  |
| --- | --- |
| server.xsrf.disableProtection: | Setting this to true will completely disable Cross-site request forgery protection in Kibana. This is not recommended. **Default: false** |
| status.allowAnonymous: | If authentication is enabled, setting this to true enables unauthenticated users to access the Kibana server status API and status page. **Default: false** |
| telemetry.allowChangingOptInStatus | When true, users are able to change the telemetry setting at a later time in [Advanced Settings](https://www.elastic.co/guide/en/kibana/7.16/advanced-options.html). When false, Kibana looks at the value of [telemetry.optIn](https://www.elastic.co/guide/en/kibana/7.16/settings.html" \l "settings-telemetry-optIn) to determine whether to send telemetry data or not. [telemetry.allowChangingOptInStatus](https://www.elastic.co/guide/en/kibana/7.16/settings.html#telemetry-allowChangingOptInStatus) and [telemetry.optIn](https://www.elastic.co/guide/en/kibana/7.16/settings.html#settings-telemetry-optIn) cannot be false at the same time. **Default: true**. |
| telemetry.optIn | When true, telemetry data is sent to Elastic. When false, collection of telemetry data is disabled. To enable telemetry and prevent users from disabling it, set [telemetry.allowChangingOptInStatus](https://www.elastic.co/guide/en/kibana/7.16/settings.html#telemetry-allowChangingOptInStatus) to false and [telemetry.optIn](https://www.elastic.co/guide/en/kibana/7.16/settings.html#settings-telemetry-optIn) to true. **Default: true** |
| telemetry.enabled | Reporting your cluster statistics helps us improve your user experience. Your data is never shared with anyone. Set to false to disable telemetry capabilities entirely. You can alternatively opt out through **Advanced Settings**. **Default: true** |
| vis\_type\_vega.enableExternalUrls: | Set this value to true to allow Vega to use any URL to access external data sources and images. When false, Vega can only get data from Elasticsearch. **Default: false** |
| xpack.ccr.ui.enabled Set this value to false to disable the Cross-Cluster Replication UI. **Default: true** | xpack.discoverEnhanced.actions. exploreDataInContextMenu.enabled |
| Enables the **Explore underlying data** option that allows you to open **Discover** from a dashboard panel and view the panel data. **Default: false** | xpack.discoverEnhanced.actions. exploreDataInChart.enabled |
| Enables you to view the underlying documents in a data series from a dashboard panel. **Default: false** | xpack.ilm.ui.enabled Set this value to false to disable the Index Lifecycle Policies UI. **Default: true** |
| xpack.index\_management.ui.enabled Set this value to false to disable the Index Management UI. **Default: true** | xpack.license\_management.enabled |
| [~~7.16.0~~] Deprecated in 7.16.0. In 8.0 and later, this setting will no longer be supported.Set this value to false to disable the License Management UI. **Default: true** | xpack.license\_management.ui.enabled Set this value to false to disable the License Management UI. **Default: true** |
| xpack.remote\_clusters.ui.enabled Set this value to false to disable the Remote Clusters UI. **Default: true** | xpack.rollup.enabled: |
| [~~7.16.0~~] Deprecated in 7.16.0. In 8.0 and later, this setting will no longer be supported.Set this value to false to disable the Rollup UI. **Default: true** | xpack.rollup.ui.enabled: Set this value to false to disable the Rollup Jobs UI. **Default: true** |
| xpack.snapshot\_restore.ui.enabled: Set this value to false to disable the Snapshot and Restore UI. **Default: true** | xpack.upgrade\_assistant.ui.enabled: Set this value to false to disable the Upgrade Assistant UI. **Default: true** |
| i18n.locale | Set this value to change the Kibana interface language. Valid locales are: en, zh-CN, ja-JP. **Default: en** |