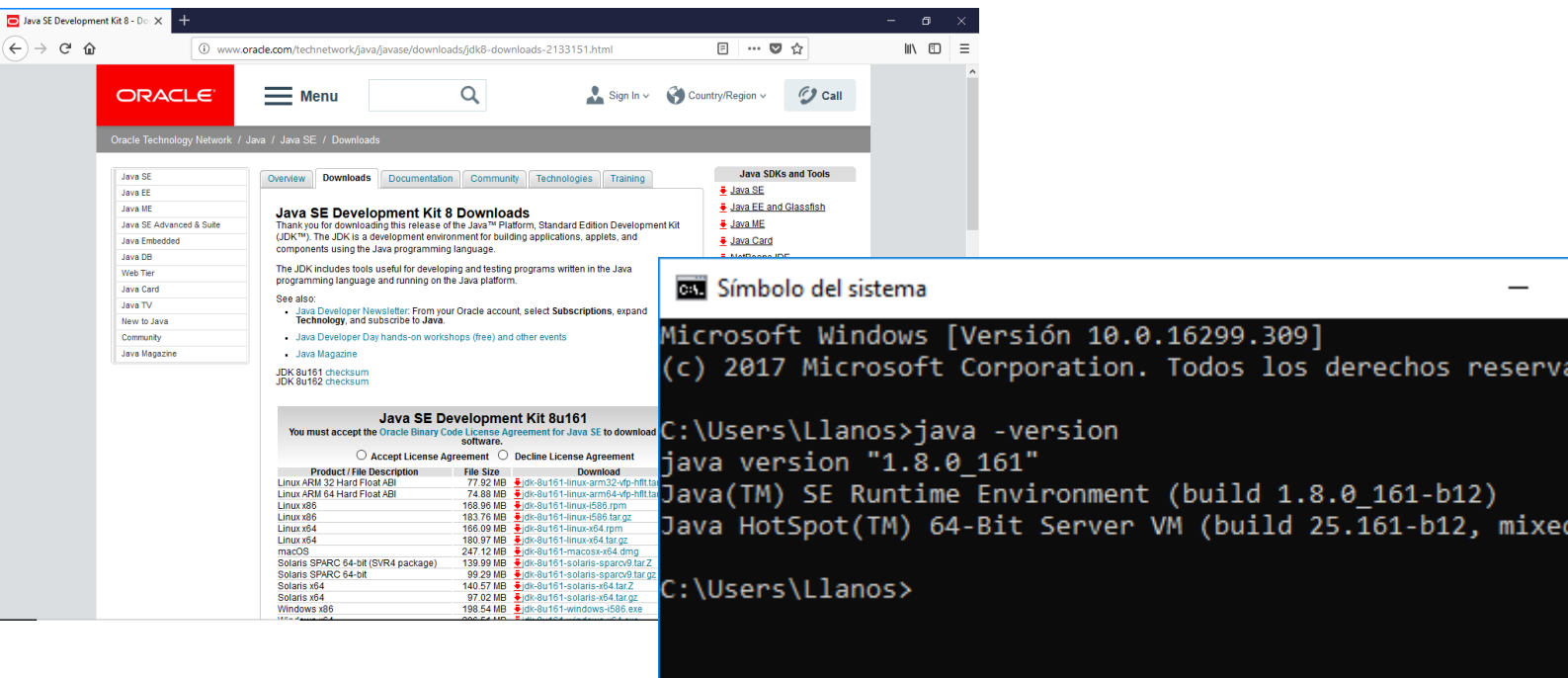


# Setup instructions: Windows Desktops

## Prerequisites

First, we must check that Java Standard Developers Kit (SDK) 7 (or higher version) is installed. In a terminal, we can check it with the order `java -version`. This program can be downloaded from the following link: <http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>



The screenshot shows the Oracle Java SE Development Kit 8 Downloads page. The page title is "Java SE Development Kit 8 Downloads". It includes a sidebar with navigation links for Java SE, Java EE, Java ME, Java SE Advanced & Suite, Java Embedded, Java DB, Web Tier, Java Card, Java TV, New to Java, Community, and Java Magazine. The main content area has tabs for Overview, Downloads, Documentation, Community, Technologies, and Training. The Downloads tab is active, showing the "Java SE Development Kit 8 Downloads" section. It includes a table of download links for various operating systems and architectures. Below the table, there is a section for "Java SE Development Kit 8u161" with a table of download links for various operating systems and architectures. The table has columns for Product / File Description, File Size, and Download. The download links are provided for various operating systems including Linux, macOS, Solaris, and Windows.

```
C:\Users\Llanos>java -version
java version "1.8.0_161"
Java(TM) SE Runtime Environment (build 1.8.0_161-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.161-b12, mixed mode)
C:\Users\Llanos>
```

The version of Java must be a developer kit and not a run time environment. And the path to the Java installation must be added to the system path variable.

## Elasticsearch and Kibana installation

From the URL <https://www.elastic.co/downloads/elasticsearch> we download the ZIP version of Elasticsearch:

# Download Elasticsearch



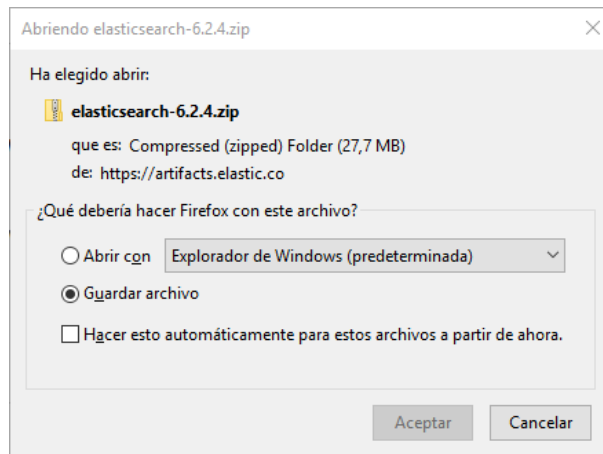
Want to upgrade? We'll give you a hand. [Upgrade Guidance »](#)

Version: 6.2.4

Release date: April 17, 2018

Notes: View the detailed release notes [here](#).  
Not the version you're looking for? View [past releases](#).

Downloads: [ZIP](#) sha [TAR](#) sha [DEB](#) sha  
[RPM](#) sha [MSI \(BETA\)](#) sha



We create a folder called ELK and we unzip the zip file inside.

We can download Kibana from the following link: <https://www.elastic.co/downloads/kibana>.  
As we do with Elasticsearch, we choose the Windows version, that is the zip version. The zip file should be unzipped in the ELK folder.

# Download Kibana



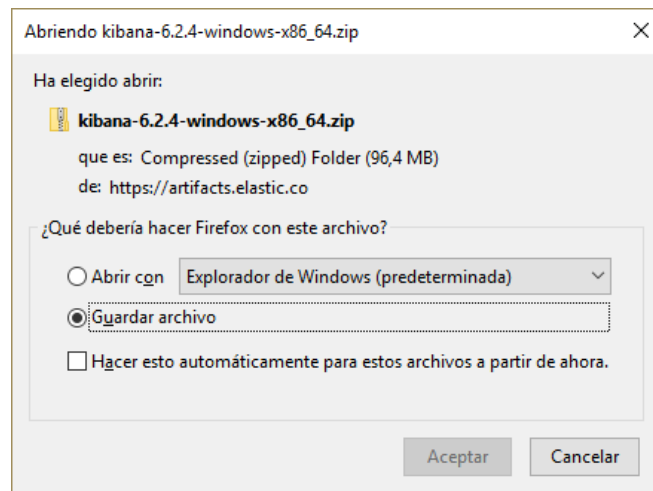
Want to upgrade? We'll give you a hand. [Migration Guide »](#)

Version: 6.2.4

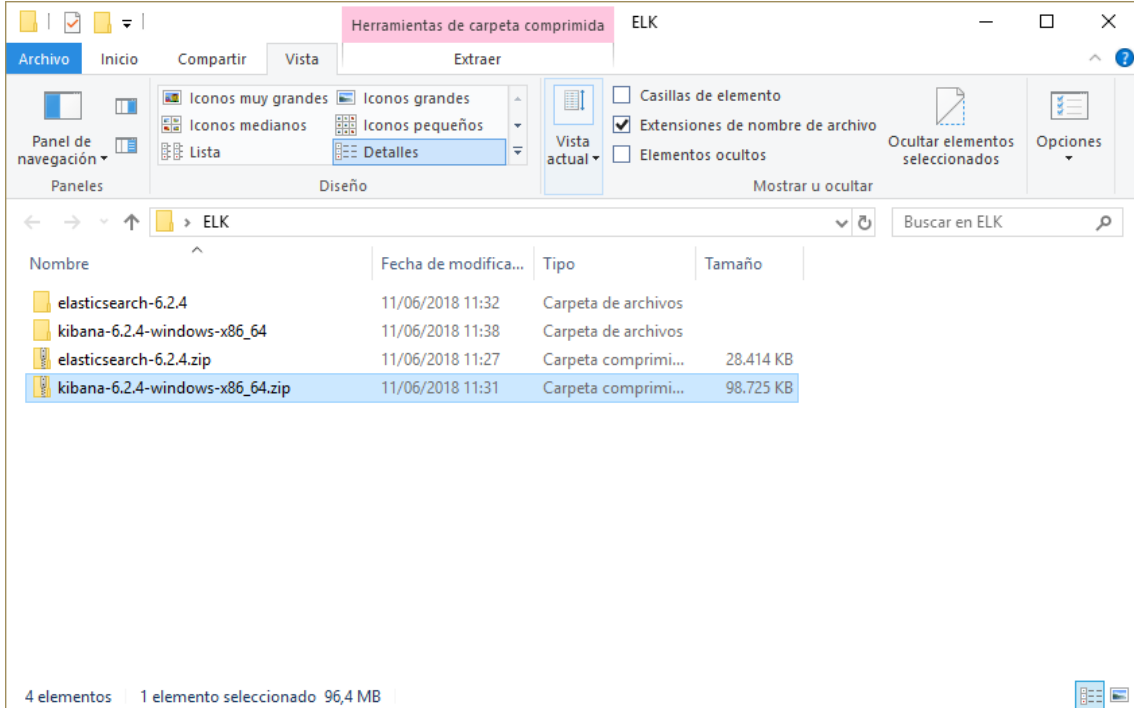
Release date: April 17, 2018

Notes: View the detailed release notes [here](#).  
Not the version you're looking for? View [past releases](#).

Downloads: [📄 WINDOWS sha](#) [📄 MAC sha](#) [📄 LINUX 64-BIT sha](#)  
[📄 RPM 64-BIT sha](#) [📄 DEB 64-BIT sha](#)



In the following image we can see the result:



## X-Pack Installation

X-Pack is an extension that allows us to perform certain machine learning functions. Its installation requires Internet connection. The detailed installation instructions can be found in the following link: <https://www.elastic.co/downloads/x-pack>

First, X-Pack must be installed in Elasticsearch with the command `elasticsearch-plugin install -xpack`

```
c:\Users\Llanos\Desktop\ELK\elasticsearch-6.2.4\bin>elasticsearch-plugin install x-pack  
-> Downloading x-pack from elastic  
[=====] 100%  
@ WARNING: plugin requires additional permissions @  
java.io.FilePermission \\.\\pipe\* read,write  
java.lang.RuntimePermission accessClassInPackage.com.sun.activation.registries  
java.lang.RuntimePermission getClassLoader  
java.lang.RuntimePermission setContextClassLoader  
java.lang.RuntimePermission setFactory  
java.net.SocketPermission * connect,accept,resolve  
java.security.SecurityPermission createPolicy.JavaPolicy  
java.security.SecurityPermission getPolicy  
java.security.SecurityPermission putProviderProperty.BC  
java.security.SecurityPermission setPolicy  
java.util.PropertyPermission * read,write  
See http://docs.oracle.com/javase/8/docs/technotes/guides/security/permissions.html  
for descriptions of what these permissions allow and the associated risks.  
  
Continue with installation? [y/N] y  
@ WARNING: plugin forks a native controller @  
This plugin launches a native controller that is not subject to the Java security manager nor to system call filters.  
  
Continue with installation? [y/N] y  
Elasticsearch keystore is required by plugin [x-pack-security], creating...  
-> Installed x-pack with: x-pack-core,x-pack-deprecation,x-pack-graph,x-pack-logstash,x-pack-ml,x-pack-monitoring,x-pack-security,x-pack-upgrade,x-pack-watcher
```

```
c:\Users\Llanos\Desktop\ELK\elasticsearch-6.2.4\bin>
```

Once it is installed, we can run Elasticsearch with the command `elasticsearch.bat`:

```
C:\Windows\System32\cmd.exe - elasticsearch
C:\Users\Llanos\Desktop\ELK\elasticsearch-6.2.4\bin>elasticsearch
[2018-06-11T12:28:10,818][INFO ][o.e.n.Node               ] [] initializing ...
[2018-06-11T12:28:10,975][INFO ][o.e.e.NodeEnvironment ] [6xt1jfu] using [1] data paths, mounts [(C:)], net usable_
space [212.7gb], net total_space [443.4gb], types [NTFS]
[2018-06-11T12:28:10,975][INFO ][o.e.e.NodeEnvironment ] [6xt1jfu] heap size [990.7mb], compressed ordinary object po
inters [true]
[2018-06-11T12:28:10,975][INFO ][o.e.n.Node               ] node name [6xt1jfu] derived from node ID [6xt1jfuQBwepPLcNp
YMPA]; set [node.name] to override
[2018-06-11T12:28:10,975][INFO ][o.e.n.Node               ] version[6.2.4], pid[8492], build[cccec39f/2018-04-12T20:37:28
.497551Z], OS[Windows 10/10.0/amd64], JVM[Oracle Corporation/Java HotSpot(TM) 64-Bit Server VM/1.8.0_161/25.161-b12]
[2018-06-11T12:28:10,975][INFO ][o.e.n.Node               ] JVM arguments [-Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:
CMSInitiatingOccupancyFraction=75, -XX:+UseCMSInitiatingOccupancyOnly, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=
true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKey
SetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.j
mx=true, -Djava.io.tmpdir=C:\Users\Llanos\AppData\Local\Temp\elasticsearch, -XX:+HeapDumpOnOutOfMemoryError, -XX:+PrintG
CDetails, -XX:+PrintGCDateStamps, -XX:+PrintTenuringDistribution, -XX:+PrintGCApplicationStoppedTime, -Xloggc:logs/gc.lo
g, -XX:+UseGCLogFileRotation, -XX:NumberOfGCLogFiles=32, -XX:GCLogFileSize=64m, -Delasticsearch, -Des.path.home=C:\Users
\Llanos\Desktop\ELK\elasticsearch-6.2.4, -Des.path.conf=C:\Users\Llanos\Desktop\ELK\elasticsearch-6.2.4\config]
[2018-06-11T12:28:15,506][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [aggs-matrix-stats]
[2018-06-11T12:28:15,506][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [analysis-common]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [ingest-common]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [lang-expression]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [lang-mustache]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [lang-painless]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [mapper-extras]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [parent-join]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [percolator]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [rank-eval]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [reindex]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [repository-url]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [transport-netty4]
[2018-06-11T12:28:15,522][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded module [tribe]
[2018-06-11T12:28:15,537][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-core]
[2018-06-11T12:28:15,537][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-deprecation]
[2018-06-11T12:28:15,537][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-graph]
[2018-06-11T12:28:15,537][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-logstash]
[2018-06-11T12:28:15,537][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-ml]
[2018-06-11T12:28:15,537][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-monitoring]
[2018-06-11T12:28:15,537][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-security]
[2018-06-11T12:28:15,553][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-upgrade]
[2018-06-11T12:28:15,553][INFO ][o.e.p.PluginsService     ] [6xt1jfu] loaded plugin [x-pack-watcher]
[2018-06-11T12:28:22,122][INFO ][o.e.x.m.j.p.l.CppLogMessageHandler] [controller/8996] [Main.cc@128] controller (64 bit)
: Version 6.2.4 (Build 524e7fe231abc1) Copyright (c) 2018 Elasticsearch BV
[2018-06-11T12:28:25,653][DEBUG][o.e.a.ActionModule         ] Using REST wrapper from plugin org.elasticsearch.xpack.secur
ity.Security
[2018-06-11T12:28:26,356][INFO ][o.e.d.DiscoveryModule   ] [6xt1jfu] using discovery type [zen]
```

Now, the users and passwords must be created. So, to enable default passwords we move towards x-pack directory and we use the command setup-passwords auto:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versi3n 10.0.16299.431]
(c) 2017 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>cd C:\Users\Llanos\Desktop\ELK\elasticsearch-6.2.4\bin\x-pack

C:\Users\Llanos\Desktop\ELK\elasticsearch-6.2.4\bin\x-pack>setup-passwords auto
Initiating the setup of passwords for reserved users elastic,kibana,logstash_system.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y

Changed password for user kibana
PASSWORD kibana = RIfvLVwliMa8KMg2ldX

Changed password for user logstash_system
PASSWORD logstash_system = 7ZC7gILRuLdPd8ii6FSz

Changed password for user elastic
PASSWORD elastic = Pssmdc3ot1RjjxYlNe23

C:\Users\Llanos\Desktop\ELK\elasticsearch-6.2.4\bin\x-pack>
```

These passwords are generated randomly for each installation of X-Pack.

Once passwords are set, we can test the access to Elasticsearch. In a browser we open the link <http://localhost:9200>. A dialog is prompted asking username and password.

Identificación requerida

?

http://localhost:9200 solicita su nombre de usuario y contraseña. El sitio dice: "security"

Nombre de usuario: elastic

Contraseña:

Aceptar Cancelar

If we use the credentials of elastic user the webpage is showed is the following:

localhost:9200/

localhost:9200

JSON
Datos sin procesar
Cabeceras

Guardar Copiar
Filtrar JSON

```

name: "6xt1jfu"
cluster_name: "elasticsearch"
cluster_uuid: "DwLe4c0LSee4GVzz4ICmrQ"
version:
  number: "6.2.4"
  build_hash: "ccec39f"
  build_date: "2018-04-12T20:37:28.497551Z"
  build_snapshot: false
  lucene_version: "7.2.1"
  minimum_wire_compatibility_version: "5.6.0"
  minimum_index_compatibility_version: "5.0.0"
tagline: "You Know, for Search"

```

Now, X-Pack must be installed into Kibana. So, we change the directory towards kibana-6.2.4-windows-x86\_64/bin directory and execute command kibana-plugin install x-pack:

```
C:\Users\Llanos\Desktop\ELK\kibana-6.2.4-windows-x86_64\bin>kibana-plugin.bat install x-pack
Attempting to transfer from x-pack
Attempting to transfer from https://artifacts.elastic.co/downloads/kibana-plugins/x-pack/x-pack-6.2.4.zip
Transferring 264988487 bytes.....
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Optimizing and caching browser bundles...
Plugin installation complete
```

Before stating Kibana, we must configure Kibana so it finds Elasticsearch installation and it uses its use and password. Thus, we must edit the file kibana-6.2.4-windows-x86\_64\config\kibana.yml as follows:

```

# The URL of the Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://localhost:9200"

# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
#elasticsearch.preserveHost: true

# 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.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# 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. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "kibana"
elasticsearch.password: "RIfVlVwvliMa8KMg2ldX"

```

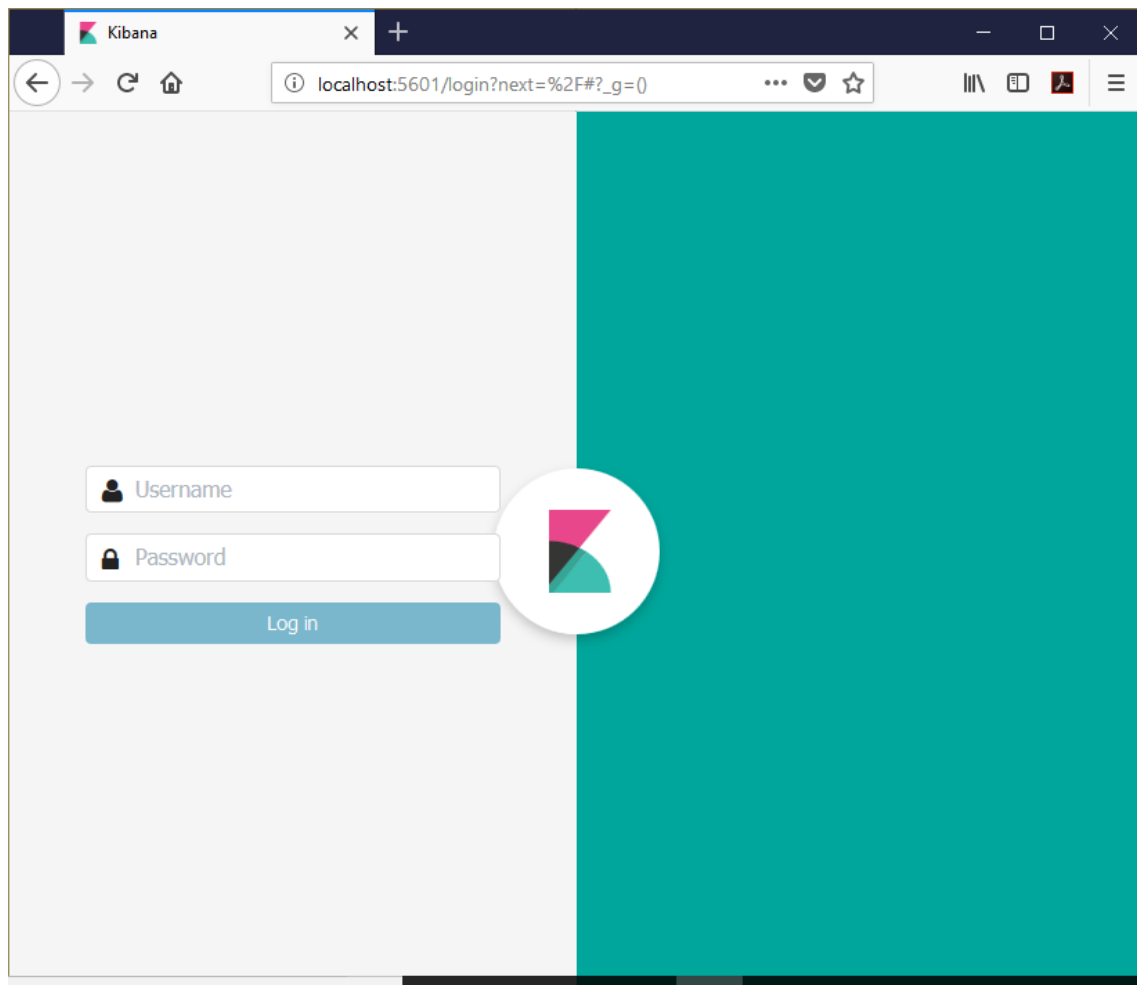
Finally, we can start Kibana:

```

C:\Users\l\lanos\Desktop\ELK\kibana-6.2.4-windows-x86_64\bin>kibana
log [11:12:49.724] [info][status][plugin:kibana@6.2.4] Status changed from uninitialized to green - Ready
log [11:12:50.318] [info][status][plugin:elasticsearch@6.2.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [11:12:50.318] [info][status][plugin:xpack_main@6.2.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [11:12:50.333] [info][status][plugin:searchprofiler@6.2.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [11:12:50.349] [info][status][plugin:ml@6.2.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [11:12:50.443] [info][status][plugin:tilemap@6.2.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [11:12:50.458] [info][status][plugin:watcher@6.2.4] Status changed from uninitialized to yellow - Waiting for Elasticsearch
log [11:12:50.536] [info][status][plugin:license_management@6.2.4] Status changed from uninitialized to green - Ready

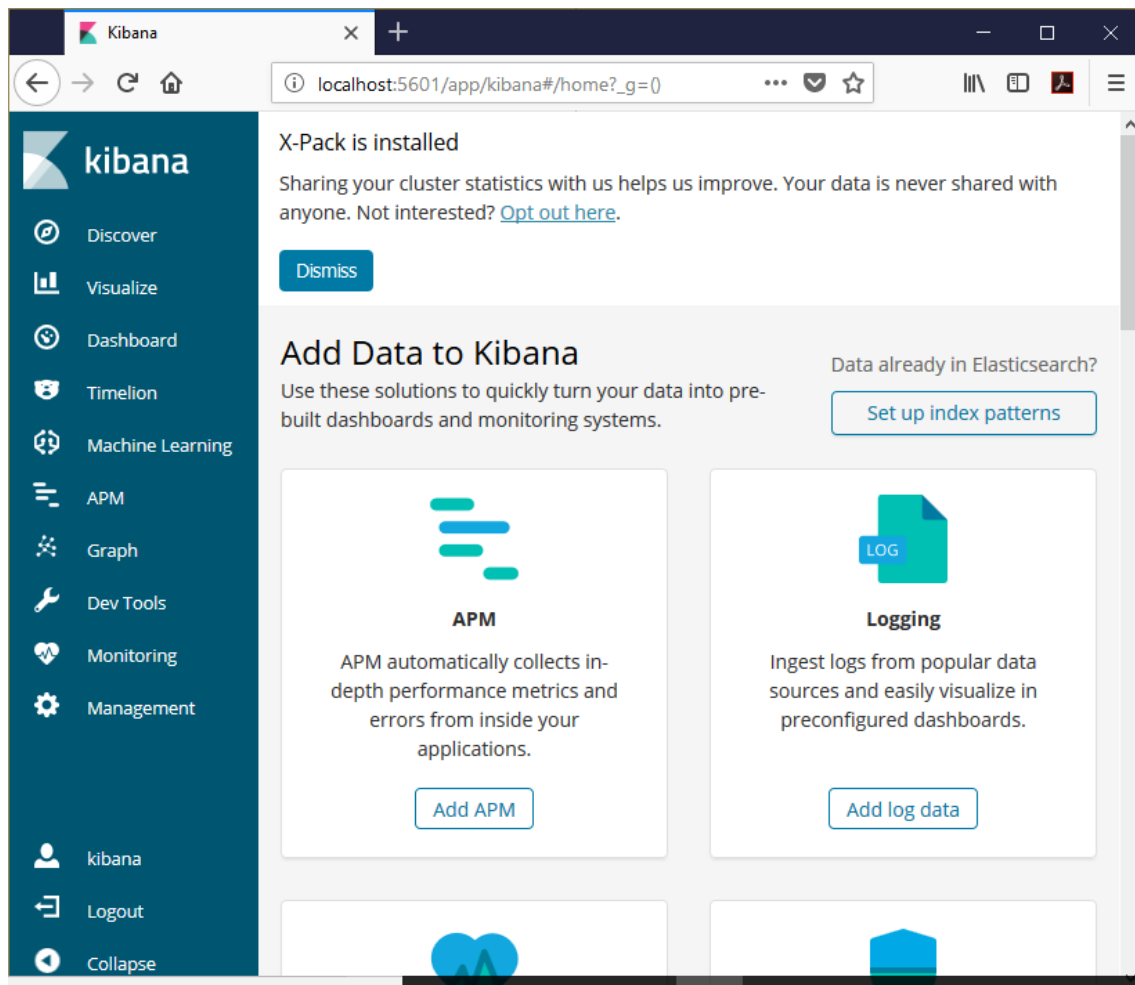
```

In order to check that we have successfully installed Kibana, we can open the following link in a browser: <http://localhost:5601>:



After using the Kibana username and password, the browser should show us the following page:





## Setup instructions: Other Operation Systems

First, Docker must be installed.

A full docker composition for ELK with X-Pack can be found in the following link:

<https://hub.docker.com/r/sebp/elkx/>.

