Ambience 2021 Installation Guide on Windows

Contents

1   Pre-Requisites

1.1   Java (JVM)

Elixir Ambience Server requires Java 11 LTS (Long Term Support) - The Java Platform, standard edition 11 development kit. If you do not have Java installed, you may obtain a copy from OpenJDK or Oracle.

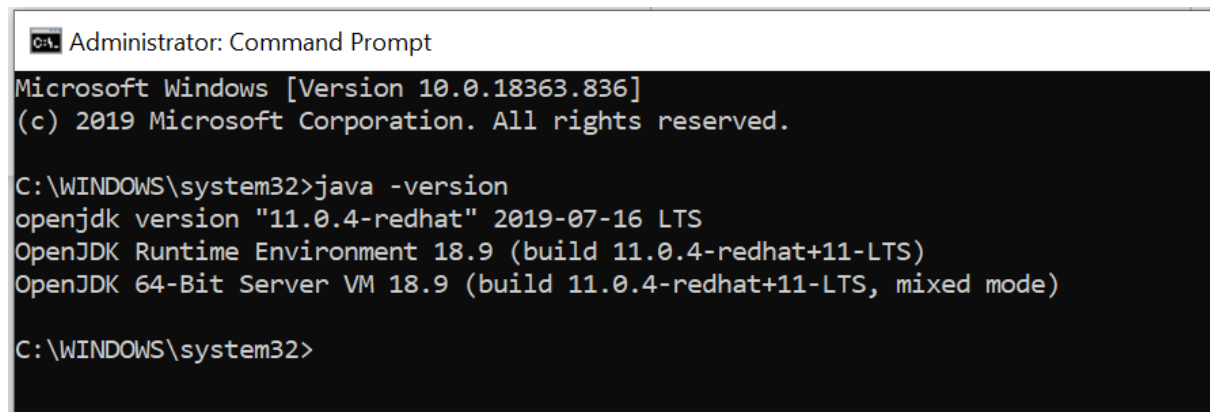You may follow installation instructions from your chosen vendor:

   a)   OpenJDK:

https://adoptopenjdk.net/installation.html?variant=openjdk11&jvmVariant=hotspot

   b)   Oracle Java:

https://docs.oracle.com/en/java/javase/11/install/installation-jdk-microsoft-windows-platforms.html#GUID-DAF345BA-B3E7-4CF2-B87A-B6662D691840

To check if the Java version is installed correctly, run the following commands using a Windows Command Line tool, with the following output observed.

2   Installation

2.1   Mongo DB

2.1.1   Download MongoDB for Windows

Download the release 4.2.7 of MongoDB (MongoDB.msi) from
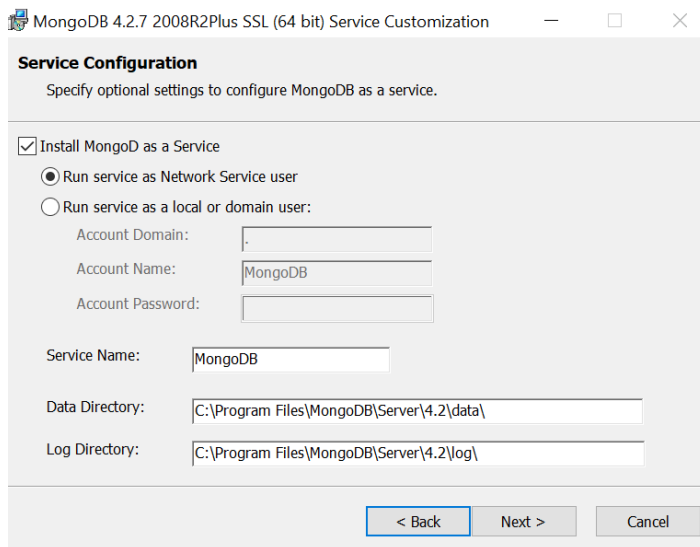
https://www.mongodb.com/download-center/community

2.1.2   Installation of MongoDB

Double-click the MongoDB.msi file. A set of the screens will appear to guide you through the installation process.

Please install MongoDB as a service and fill up your data directory and log directory accordingly.

You may proceed with the default option.

You will receive a success message upon completing of installation.

Alternatively, you can follow the full installation guide here:

https://docs.mongodb.com/manual/installation/#mongodb-community-edition-installation-tutorials

2.2 Elixir Ambience Server

2.2.1 Installing Elixir Ambience As A Service

1. Login to Windows Server as an administrator.
2. Unzip the elx-ambience-windows-4.4.0.zip file into C:\. An *ElixirAmbience* folder would be created under the C drive. Or to your selected file path.
3. Navigate to *C:\ElixirAmbience\bin* using Windows Explorer and open the **elx-ambience-service.xml** file with Notepad. Change the **name** value to *Elixir Ambience.* Edit the **description** value as desired and save the file.
4. Navigate to *C:\ElixirAmbience\bin* using Windows Explorer. Hold Shift key and right click in the folder to select *Open command window here.* The command window would be opened.
5. Type command *install-service.bat* in the command line tool and ElixirAmbience Service would be installed:

Open the System services panel and the *Elixir Ambience* Service would appear:

Name	Description	Status	Startup Type	Log On As
Elixir Ambience Service	This service ...	Running	Automatic	Local System
Embedded Mode	The Embed...		Manual (Trig...	Local System
Encrypting File System (EFS)	Provides th...		Manual (Trig...	Local System
Enterprise App Managemen...	Enables ent...		Manual	Local System

Double click on the *Elixir Ambience* Service to open its properties, under the *General* screen, change the *Startup type* to *Automatic* and click *Apply* to set the service auto start while system restarts.

2.3   Configure Ambience Server

2.3.1   Accounts and Permissions

You have to use administrator account for Ambience installation. You may use service account for daily operations.

The service account must have the following file path permission and access:

Permission and access	Reason
Java installation read access	For daily operation of the application
Ambience installation path read access	For daily operation of the application
Ambience installation path root /log folder write access	For writing logs into a file path.
Ambience installation path root /data/out write access	All export/download file will be write into /data/out. You may define another location in application.conf

2.3.2   Encryption

All plain text passwords can be encoded by using {enc}XXX style logic. This is intended to obfuscate the text to prevent casual/accidental viewing. The config file (and indeed the whole of Ambience) itself should only be readable by the Ambience user, so nobody else should be able to see the contents in the first place.

Any time a password changes, the server needs to be restarted.

Ambience (all versions) supports encrypting sensitive data like passwords by using the prefix {enc} in the configuration. You can then use an encryption mechanism we supply to generate the encrypted string.

```
Administrator: Command Prompt

C:\Users\He Xi\Desktop\Ambience-5.3.0-SNAPSHOT\bin>ambience-cli encrypt hello
hello = {enc}2Y8qleTKJ2PKmJ/UEFRByw==
C:\Users\He Xi\Desktop\Ambience-5.3.0-SNAPSHOT\bin>
```

You need to replace the encrypted string *into /etc/application.conf.*

2.3.3   MongoDB Connection

You may configurate the connection between MongoDB and Elixir Ambience by modifying the following section under */etc/application.conf*:

```
elixir.data.mongodb {
  default {
    connectionString = "mongodb://"${mongodb}":27017"
    database {
      eno = "eno"
    }
  }
}
```

Edit default (you can change the name) to match your MongoDB server connection.

The connection string can be encrypted using {enc} syntax.

Add a new key like "default" to add multiple MongoDB servers - the name is purely descriptive. database **key=value,** keys must be unique throughout all MongoDB connections, value is an actual (mongodb) database name.

Lookup is by key (unique) which is an alias to the physical database name, allowing you to easily switch to point to a different physical database (perhaps on a different server) without changing every caller.

2.3.4 HTTPS Configuration

To enable HTTPS connection, insert the certificate into Java Keystore.

1. Go to your java_home\jre\lib\security.

2. Open admin command line there using cmd and CTRL+SHIFT+ENTER.

3. Place the keystore file (in this example its *cacerts*) in the Ambience folder /etc/https/keystore.

4. Run keytool to import certificate:
(replace *yourAliasName* and *path\to\certificate.cer* respectively.)

```
..\..\bin\keytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias
yourAliasName -file path\to\certificate.cer
```

5. Enable HTTPS connection in the /etc/application.conf file.

```
ambience {
  bindAddress: "0.0.0.0"
  bindPort: ${port}
  https {
    enabled = true
    keystore = "https/keystore"
    keystore-type = "JKS"
    keystore-password = ""
  }
}
```

6. Change *enabled to true* and fill up *keystore-password*. *keystore-password* should be encrypted using {enc} syntax.

```
ambience.web {
  url = "https://"${host}":"${port}
  response-headers {
    # any of these can be overridden either by supplying an alternate string, or else "" to turn the
header off
    X-XSS-Protection = "1; mode=block"
    X-Frame-Options = "SAMEORIGIN"
    X-Content-Type-Options = "nosniff"
    # ONLY enable this if all present and future subdomains will be HTTPS!
    #Strict-Transport-Security = "max-age=31536000; includeSubDomains"
  }
}
```

7. If the SSO service is chosen as the preferred service, change the ***requiresPKCE = true*** into the SSO client section in the /etc/application.conf file. Otherwise, leave it as the default (false).

```
elixir.sso.client (
  …
  service-definition {
   exlsso {
     …
     logout = ${sso-server-baseurl}"/simple-sso/logout "
     requiresPKCE = true
     debug = true
     …
   }
  }
)
```

8. Change ***url*** from ***http*** to ***https***.