Installation Guide

This short guide shall enable you to install TIM v7.13 on Windows or Linux OS.

JBOSS = WildFly

Preconditions for Windows or UNIX

Database access preferably db_owner on either MySQL 8, SQL Server 2019, or Oracle 19c according to our latest requirements in the release notes → [Release Notes - Documentation EN - TIM BPM Documentation (atlassian.net)](atlassian.net)

Get additional tools if possible:

- notepad++ [Downloads | Notepad++ (notepad-plus-plus.org)](notepad-plus-plus.org)
- keystore explorer [KeyStore Explorer (keystore-explorer.org)](keystore-explorer.org)
- jxplorer [JXplorer - an open source LDAP browser](#)
- 7z [7-Zip](#) for Windows
- Latest JDK 11 from [Latest Releases | Adoptium](#) or [Downloads for Amazon Corretto 11 - Amazon Corretto](#)
- MSSQL Management Studio or MySQL Workbench
- open Ports for incoming connections, such as 443/8443
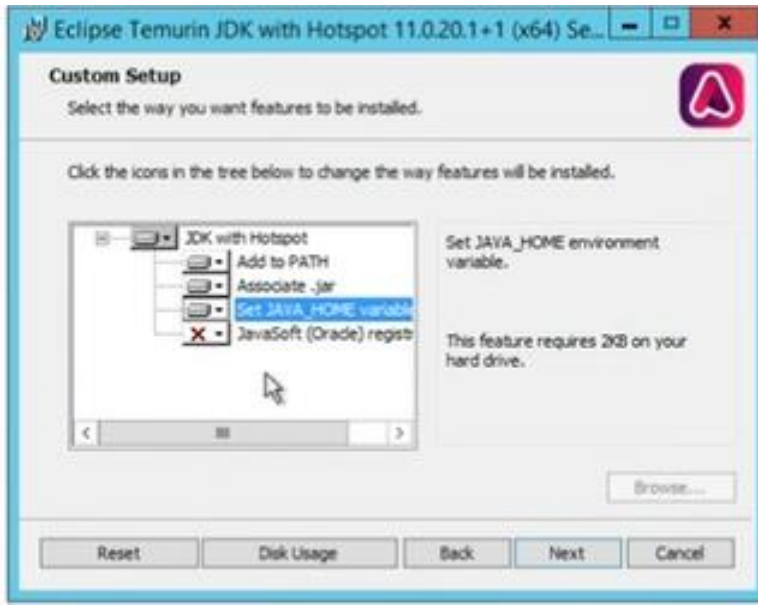
Windows OS

Quick guide for Windows installation with WildFly29 & TIM v7.13

Resources

- https://s3.eu-central-1.amazonaws.com/delivery.aws.tim-bpm.com/setup/wildfly-29.0.1.Final/wildfly-29.0.1.Final.zip
- https://s3.eu-central-1.amazonaws.com/delivery.aws.tim-bpm.com/setup/wildfly-29.0.1.Final/wildfly-29.0.1.Final-JWT-delta.zip
- https://s3.eu-central-1.amazonaws.com/delivery.aws.tim-bpm.com/TIM_7.13.0.zip

Installation

1. Install JDK and set JAVA_HOME for the system. Can be checked via system environmental variables.

2. On Disk create folder tim e.g. C:\tim
3. Unzip wildfly as per request to C:\tim\wildfly-VERSION and rename the folder to wildfly-VERSION-dev, -stage or -prod according to purpose.
4. Copy & replace the content of wildfly-VERSION-JWT-delta.zip into WildFly Home e.g. C:\tim\wildfly-VERSION-dev
5. Copy folder service from C:\tim\wildfly-VERSION-\docs\contrib\scripts to C:\tim\wildfly-VERSION.Final-\bin
6. Edit with notepad++ C:\tim\wildfly-VERSION-dev\bin\service\service.bat and change SHORTNAME and DISPLAYNAME to e.g. TIM24DEV / Timprod-WildFly29

CONTROLLER=localhost:9990 in service.bat needs to match jboss.management.http.port in standalone-tim.xml

important if multiple app server are installed on one host machine

Copy from https://s3.eu-central-1.amazonaws.com/delivery.aws.tim-bpm.com/setup/jbcs-jsvc-1.1.0-win6-x86_64.zip

\jbcs-jsvc-1.1.0-win6-x86_64\jbcs-jsvc-1.1\bin\prunmgr.exe
\jbcs-jsvc-1.1.0-win6-x86_64\jbcs-jsvc-1.1\sbinprunsrv.exe

into the \bin folder when having trouble with shut-down of service

6. Open C:\tim\wildfly-VERSION.Final\standalone\configuration\tim.properties and add

```
keypair-password=changeit
```

7. Run the following keytool command to create a jwt.keystore and adding the key

```
keytool -genkey -alias jwt.key -keyalg RSA -keysize 2048 -keystore
C:\tim\wildfly-VERSION.Final\standalone\configuration\jwt.keystore -
storepass changeit -keypass changeit
```

8. Iterate through the questions

9. Open C:\tim\wildfly-VERSION.Final-dev\bin\standalone.conf.bat to check for XMS and rem all lines from 96 to 104 regarding port offset and the DB connection string
10. `set "JAVA_OPTS=%JAVA_OPTS% -Xms2G -Xmx2G -XX:MetaspaceSize=96M -XX:MaxMetaspaceSize=512m"`
11.
12. `rem TIM Solutions GmbH Configuration part`
13. `rem Feel free to edit this configuration below!`
14. `rem set "JAVA_OPTS=%JAVA_OPTS% -Djboss.socket.binding.port-offset=0"`
15. `rem set "JAVA_OPTS=%JAVA_OPTS% -Djboss.http.port=8080"`
16. `rem set "JAVA_OPTS=%JAVA_OPTS% -Djboss.JDBC_CONNECTION=jdbc:sqlserver://database.fqdn:1433;database=tim;encrypt=true;loginTimeout=30;"`
17. `rem set "JAVA_OPTS=%JAVA_OPTS% -Djboss.JDBC_DRIVER=sqlserver"`
18. `rem set 'JAVA_OPTS=%JAVA_OPTS% -Djboss.CHECK_ALIVE_QUERY="SELECT 1 FROM TIM_DUAL"'`
19. `rem set "JAVA_OPTS=%JAVA_OPTS% -Djboss.DBUSER=tim"`
    `rem set "JAVA_OPTS=%JAVA_OPTS% -Djboss.DBPASSWORD=t1m"`

20. Open under C:\tim\wildfly-VERSION.Final-dev\standalone\configuration\standalone-tim.xml to configure the data source. e.g. connection URL

11. SET 'SELECT 1 FROM TIM_DUAL' only for ORA DB
12. Open under C:\tim\wildfly-VERSION.Final-dev\standalone\configuration\tim.properties to set default client and add initpass for custom passwords (after the initial init of the system credentials can be encrypted via admin panel)
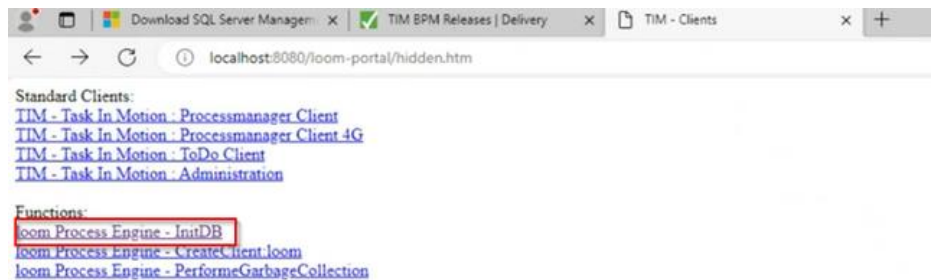13. `default-client=`
14.
15. `#initpass-super-admin=`
16. `#initpass-super-sys.support=`
17. `#initpass-x-admin=`

```
18.  #initpass-x-sys.support=
     #initpass-x-others=
```

19. Encoding via the administration panel of secrets is possible after the initialization of the application.
20. Copy tim.ear and dashboard.war from TIM_x.x.x.zip into C:\tim\wildfly-VERSION.Final-dev\standalone\deployments
21. Open cmd as admin and install the service.

```
22.  cd C:\tim\wildfly-VERSION.Final-dev\bin\service
23.
     service.bat install /config standalone-tim.xml
```

24. Open Windows Services and navigate to e.g. TIM24DEV. Set starttyp to automatic.
25. Start TIM Service and check server.log C:\tim\wildfly-24.0.1.Final-dev\standalone\log for any issues to resolve. 😄Popular issues: closed ports, the network connection to the database, missing permissions, or antivirus tool intervention.
26. Open http://127.0.0.1:8080/loom-portal/hidden.htm to initialize the database. (InitDB)

27. Open Eclipse for licence generation, ID Token, Multi or Single Node, Validity in month, Customer Name, values have to be provided from Ticket except ID and Node copy and paste licence into customer page. Customers can order a license under https://webform.tim-solutions.de/licenserequest/

The difference between single and multi node license depends on the database instance. As soon as a multi node token is displayed, a multi node license should be ordered.

20. Open http://127.0.0.1:8080/loom-portal/license.htm to install the licence as super/admin.
21. Log into super tenant http://localhost:8080/tim/client/ to create a customer tenant. Tenant Creation - Documentation EN - TIM BPM Documentation (atlassian.net)
22. Replace unencrypted Passwords with encrypted ones in C:\tim\wildfly-VERSION.Final-dev\standalone\configuration\tim.properties
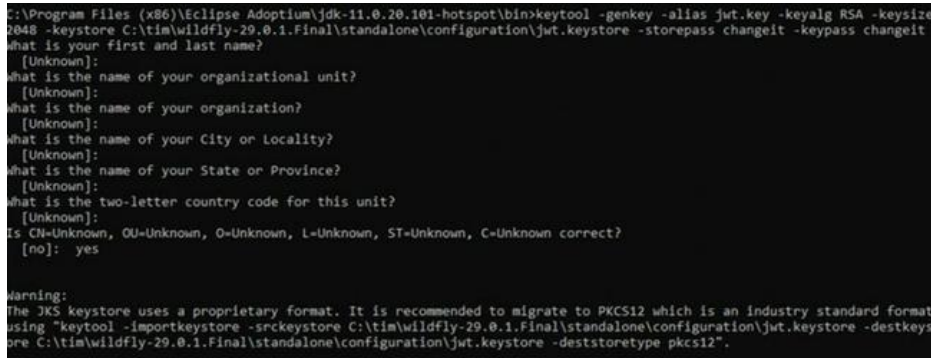
For further configuration check Documentation EN - TIM BPM Documentation (atlassian.net) e.g SMTP, LDAP Auth & Sync or SSO with SAML

UNIX

Resources

- https://s3.eu-central-1.amazonaws.com/delivery.aws.tim-bpm.com/setup/wildfly-29.0.1.Final/wildfly-29.0.1.Final.zip
- https://s3.eu-central-1.amazonaws.com/delivery.aws.tim-bpm.com/setup/wildfly-29.0.1.Final/wildfly-29.0.1.Final-JWT-delta.zip
- https://s3.eu-central-1.amazonaws.com/delivery.aws.tim-bpm.com/TIM_7.13.0.zip
- JDK 11

Installation

1. Similar to the Windows installation, create a folder tim under e.g /usr/local/
2. Create a user and group, e.g. tim that owns folder tim
3. Copy WildFly and WildFly JWT Delta into tim folder
4. Copy docs/contrib/scripts/systemd/launch.sh to bin\
5. Copy docs/contrib/scripts/systemd/wildfly.conf to /etc/default/
6. Copy docs/contrib/scripts/systemd/wildfly.service to /etc/systemd/system/
7. Open bin/standalone.conf to disable
8. `# TIM Solutions GmbH Configuration part`
9. `# Feel free to edit this configuration below!`
10. `#JAVA_OPTS="$JAVA_OPTS -Djboss.socket.binding.port-offset=0"`
11. `#JAVA_OPTS="$JAVA_OPTS -Djboss.http.port=8080"`
12. `#JAVA_OPTS="$JAVA_OPTS -Djboss.JDBC_CONNECTION=jdbc:sqlserver://database.fqdn:1433\;database=tim\;encrypt=true\;loginTimeout=30\;"`
13. `#JAVA_OPTS="$JAVA_OPTS -Djboss.JDBC_DRIVER=sqlserver"`
14. `#JAVA_OPTS="$JAVA_OPTS -Djboss.CHECK_ALIVE_QUERY='SELECT 1 FROM TIM_DUAL'"`
15. `#JAVA_OPTS="$JAVA_OPTS -Djboss.DBUSER=tim"`
    `#JAVA_OPTS="$JAVA_OPTS -Djboss.DBPASSWORD=t1m"`

16. Open standalone/configuration/standalone-tim.xml to set datasources to the desired database.

SET 'SELECT 1 FROM TIM_DUAL' only for ORA DB

17. Check socket-binding for correct port offset
18. Open /usr/local/tim/wildfly-VERSION.Final/standalone/configuration/tim.properties and add

    `keypair-password=changeit`

19. Open /usr/local/tim/wildfly-VERSION.Final/standalone/configuration/tim.properties and add

    `keypair-password=changeit`

20. Run the following keytool command to create a jwt.keystore and adding the key

```
keytool -genkey -alias jwt.key -keyalg RSA -keysize 2048 -keystore
usr/local/tim/wildfly-
VERSION.Final/standalone/configuration/jwt.keystore -storepass changeit
-keypass changeit
```

21. Iterate through the questions

22. Open under /usr/local/tim/wildfly-
VERSION.Final/standalone/configuration/tim.properties to set default client and add
initpass for custom passwords (after the initial init of the system credentials can be
encrypted via admin panel)
23. ```default-client=```
24.
25. ```#initpass-super-admin=```
26. ```#initpass-super-sys.support=```
27. ```#initpass-x-admin=```
28. ```#initpass-x-sys.support=```
     ```#initpass-x-others=```

29. Encoding via the administration panel of secrets is possible after the initialization of the
application.
30. Copy tim.ear and dashboard.war from TIM_x.x.x.zip into /usr/local/tim/wildfly-
VERSION.Final/standalone/deployments
31. Set WILDFLY_CONFIG=standalone-tim.xml in /etc/default/wildfly.conf
32. Set below parameters for /etc/systemd/system/wildfly.service
33. ```[Service]```
34. ```Environment=LAUNCH_JBOSS_IN_BACKGROUND=1```
35. ```EnvironmentFile=-/etc/default/wildfly.conf```
36. ```User=tim```
37. ```LimitNOFILE=102642```
38. ```PIDFile=/run/wildfly/wildfly.pid```
39. ```ExecStart=/usr/local/tim/wildfly-VERSION.Final/bin/launch.sh```
     ```$WILDFLY_MODE $WILDFLY_CONFIG $WILDFLY_BIND```
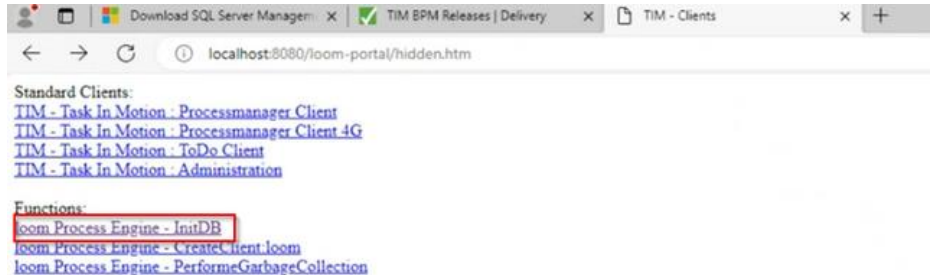   ```StandardOutput=null```

40. Enable service with systemctl enable wildfly.service & systemctl daemon-reload

41. Run systemctl start wildfly.service and check server.log /usr/local/tim/wildfly-VERSION.Final/standalone/log for any issues to resolve. Popular issues: closed ports, the network connection to the database, missing permissions, or antivirus tool intervention.
42. Open http://127.0.0.1:8080/loom-portal/hidden.htm to initialize the database. (InitDB)

43. Open Eclipse for licence generation, ID Token, Multi or Single Node, Validity in month, Customer Name, values have to be provided from Ticket except ID and Node copy and paste licence into customer page. Customers can order a license under https://webform.tim-solutions.de/licenserequest/

The difference between single and multi node license depends on the database instance. As soon as a multi node token is displayed, a multi node license should be ordered.

23. Open http://127.0.0.1:8080/loom-portal/license.htm to install the licence as super/admin.
24. Log into super tenant http://localhost:8080/tim/client/ to create a customer tenant. Tenant Creation - Documentation EN - TIM BPM Documentation (atlassian.net)
25. Replace unencrypted Passwords with encrypted ones in /usr/local/tim/wildfly-VERSION.Final/standalone/configuration/tim.properties

For further configuration check Documentation EN - TIM BPM Documentation (atlassian.net) e.g SMTP, LDAP Auth & Sync or SSO with SAML

Additional Configuration

Configuration Properties
https://tim-doc.atlassian.net/wiki/spaces/eng/pages/228102152/Module+Requirements#Mailserver
https://tim-doc.atlassian.net/wiki/spaces/eng/pages/228102152/Module+Requirements#SAML-2.0
https://tim-doc.atlassian.net/wiki/spaces/eng/pages/228102152/Module+Requirements#LDAP
LDAP
Dashboard

˅ Extended jwt.keystore explanation

KEYSTORE GENERATION

There is a command to create a keystore:

```
keytool -genkey -alias jwt.key -keyalg RSA -keysize 2048 -keystore
jwt.keystore -storepass changeit -keypass changeit
```

The generated keystore must be located under standalone/configuration folder and must have a name **jwt.keystore**

TIM.PROPERTIES CONFIGURATION

Text above highlighted in bold can be changed and must be the same as defined in tim.properties. The tim.properties file has the following properties:

1. Value of keystore-password property must be equal to the *-storepass* value of the aforementioned command
2. Value of *keypair-name* property must be equal to the -alias value of the aforementioned command
3. Value of keypair-password property must be equal to the *-keypass* value of the aforementioned command

STANDALONE XML CONFIGURATION

Additionally, the standalone file must contain the keystore-password in the section of keystores definition:

```
<key-store name="jwt-key-store">
        <credential-reference clear-text="changeit"/>
        <implementation type="JKS"/>
        <file path="jwt2.keystore" relative-to="jboss.server.config.dir"/>
</key-store>
```

Have a look at the **<credential-reference** clear-text="changeit"**/>** . Credential-reference must be equal to the keystore-password.

When defining a certificate parameter for jwt issuer in the standalone config, we must put a value of the certificate name:

```
<token-realm name="tim-jwt-realm" principal-claim="uid">
        <jwt issuer="TimBpmSuite" audience="TimBpmSuiteAudience" key-
store="jwt-key-store" certificate="jwt.key"/>
</token-realm>
```

This value must be equal to *keypair-name* property value in tim.properties and *-alias* of the keystore generation command

Azure SaaS Considerations

1. Azure Application Gateway
2. App Gateway Listener

3. Check Firewall Port
4. Log into the customer tenant to configure SMTP settings or create customer accounts as per ticket.

Installation TIM v7.14 or higher

From v7.14 onwards, TIM requires JDK 17.

- [Preconditions for Windows or UNIX](#)
- [Windows OS](#)
  - o [Resources](#)
  - o [Installation](#)
- [UNIX](#)
  - o [Resources](#)
  - o [Installation](#)
- [Additional Configuration](#)
  - o [KEYSTORE GENERATION](#)
  - o [TIM.PROPERTIES CONFIGURATION](#)
  - o [STANDALONE XML CONFIGURATION](#)
- [Azure SaaS Considerations](#)
- [Installation TIM v7.14 or higher](#)

SSL

Convert pfx to jks with `keytool -importkeystore -srckeystore` *`mypfxfile.pfx`* `-srcstoretype pkcs12 -destkeystore` *`clientcert.jks`* `-deststoretype JKS`

`Change standalone-igrafx for ssl, remember to change basedir to configdir`

`Check /and add if necessary) pagefile on c:`