Principal Toolbox installation

Autor: Shadi Saghir
Version: 1.0

Table of contents

1 Document information

Version	Date	Author	Remarks
0.1	09-08-2016	Shadi Saghir	Concept version
0.2	09-08-2016	Shadi Saghir	Software and hardware recommendation 1
0.3	09-08-2016	Shadi Saghir	Software and hardware recommendation 2
0.4	09-08-2016	Shadi Saghir	Software and hardware recommendation 3
0.5	09-08-2016	Shadi Saghir	Installation Principal Toolbox
0.6	09-08-2016	Shadi Saghir	IE security settings
0.7	09-08-2016	Shadi Saghir	Update Principal Toolbox
1.0	09-08-2016	Shadi Saghir	Finalizing document

2 Software and hardware recommendation

Database server:	**Application server:**
Windows Server 2008 with SQL 2008+	Windows Server 2008+
100GB+ HDD	100GB+ HDD
8 GB memory	8 GB memory
Dual core CPU 2 x 3 GHz core, 64-bit	Dual core CPU 2 x 3 GHz core, 64-bit

*More is always better, but the configuration listed above should provide enough performance for users between ~ 5000 and ~ 2000 projects.

Software that are needed for the installation:

Software:
Windows server 2008+
SQL server 2008+
Java version 8
Tomcat version 8
Principal Toolbox

3 Installation of the Principal Toolbox

3.1 JAVA Runtime Environment 1.8 - Installation

Source: https://java.com/en/download/help/windows_manual_download.xml

Download and Install

Before you proceed with online installation you may want to disable your Internet firewall. In some cases, the default firewall settings are set to reject all automatic or online installations such as the Java online installation. If the firewall is not configured appropriately it may stall the download/install operation of Java under certain conditions. Refer to your specific Internet firewall manual for instructions on how to disable your Internet Firewall.

- Go to the Manual download page
- Click on Windows Online
- The File Download dialog box appears prompting you to run or save the download file
    - To run the installer, click Run.
    - To save the file for later installation, click Save.
      Choose the folder location and save the file to your local system.
      Tip: Save the file to a known location on your computer, for example, to your desktop.
      Double-click on the saved file to start the installation process.

- The installation process starts. Click the Install button to accept the license terms and to continue with the installation.

- Oracle has partnered with companies that offer various products. The installer may present you with option to install these programs when you install Java. After ensuring that the desired programs are selected, click the Next button to continue the installation.
- A few brief dialogs confirm the last steps of the installation process; click Close on the last dialog. This will complete Java installation process.

Detect older versions (8u20 and later versions). Starting with Java 8 Update 20 (8u20), on Windows systems, the Java Uninstall Tool is integrated with the installer to provide an option to remove older versions of Java from the system. The change is applicable to 32 bit and 64 bit Windows platforms.

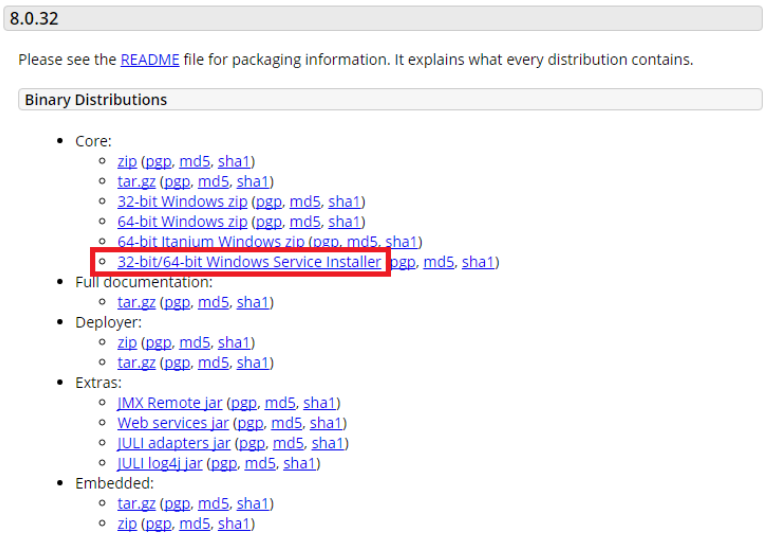
4 Notifications about disabled Java and restoring prompts

The installer notifies you if Java content is disabled in web browsers, and provides instructions for enabling it. If you previously chose to hide some of the security prompts for applets and Java Web Start applications, the installer provides an option for restoring the prompts. The installer may ask you to reboot your computer if you chose not to restart an internet browser when it prompted you to do so.

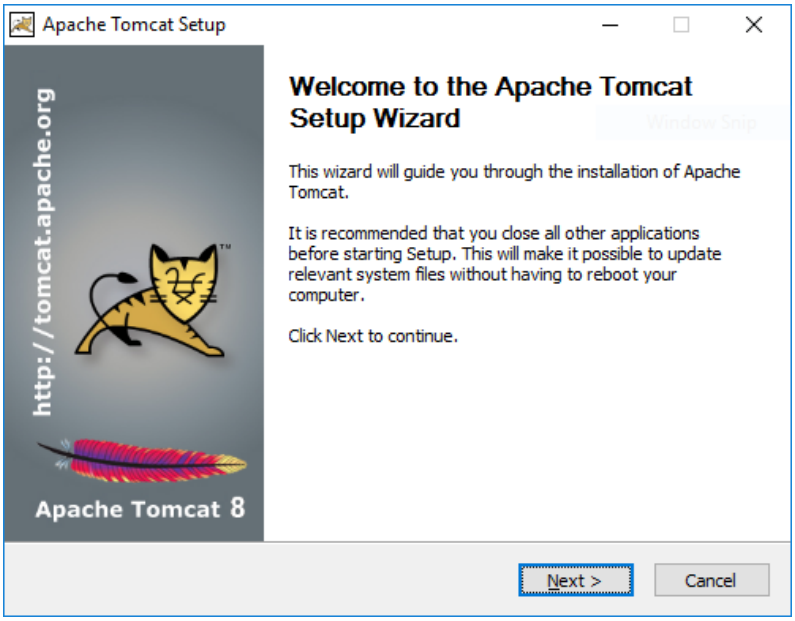
5 Test Installation

To test that Java is installed and working properly on your computer, run this test applet.
NOTE: **You may need to restart (close and re-open) your browser to enable the Java installation in your browser.**

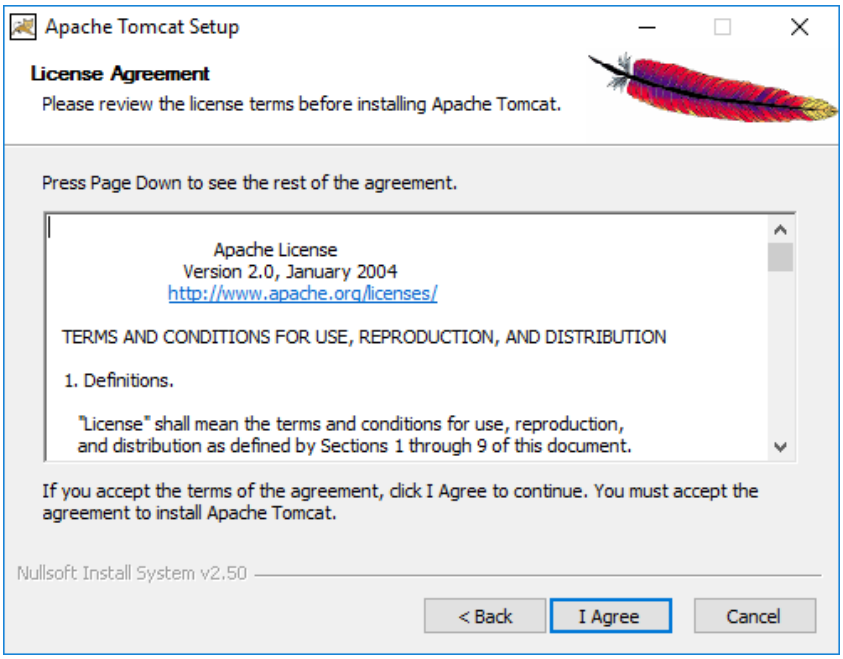
5.1 Tomcat 8.0 – Installation



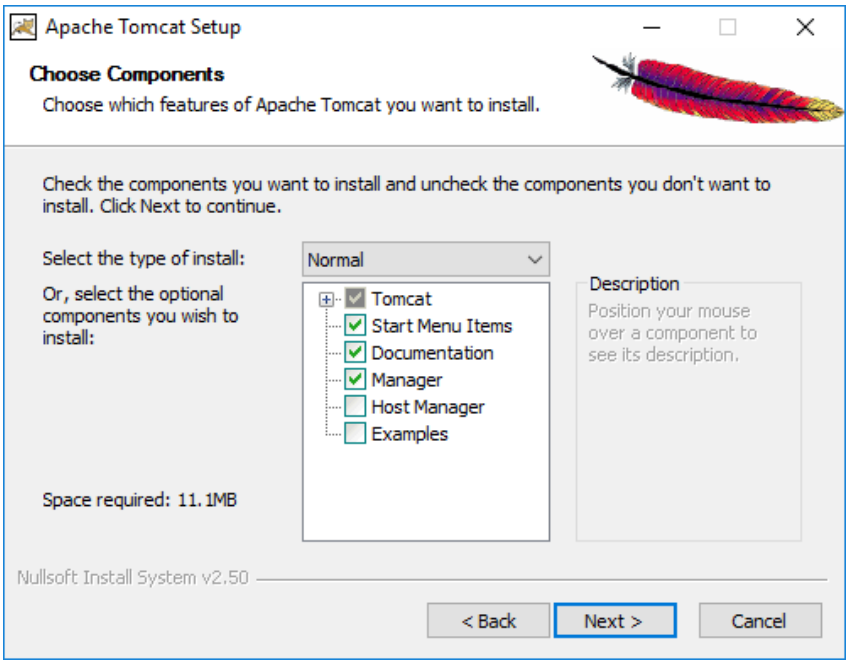
Go to http://tomcat.apache.org/download-80.cgi and download the "32-bit/64-bit Windows Service Installer" file.



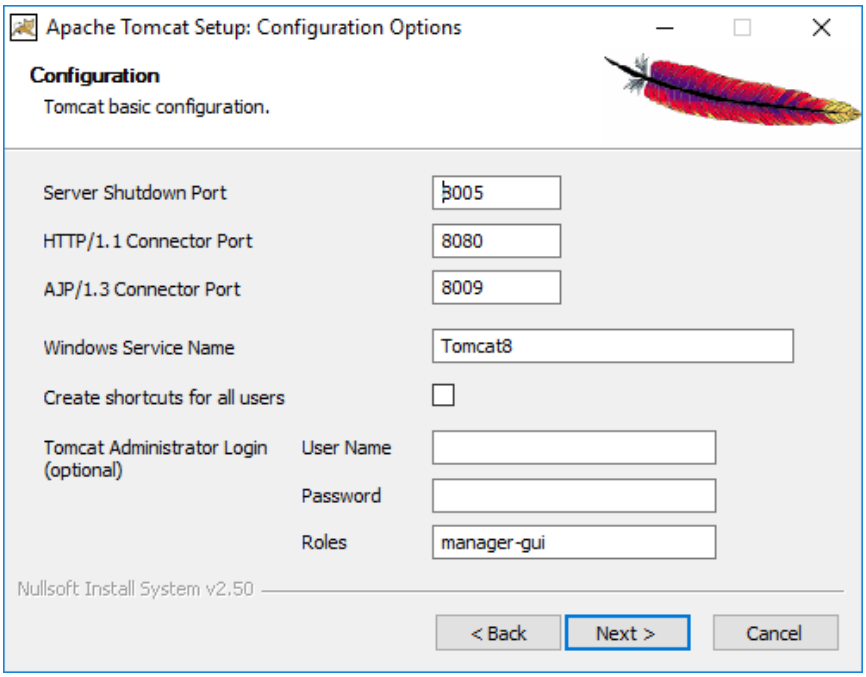
Launch the installer



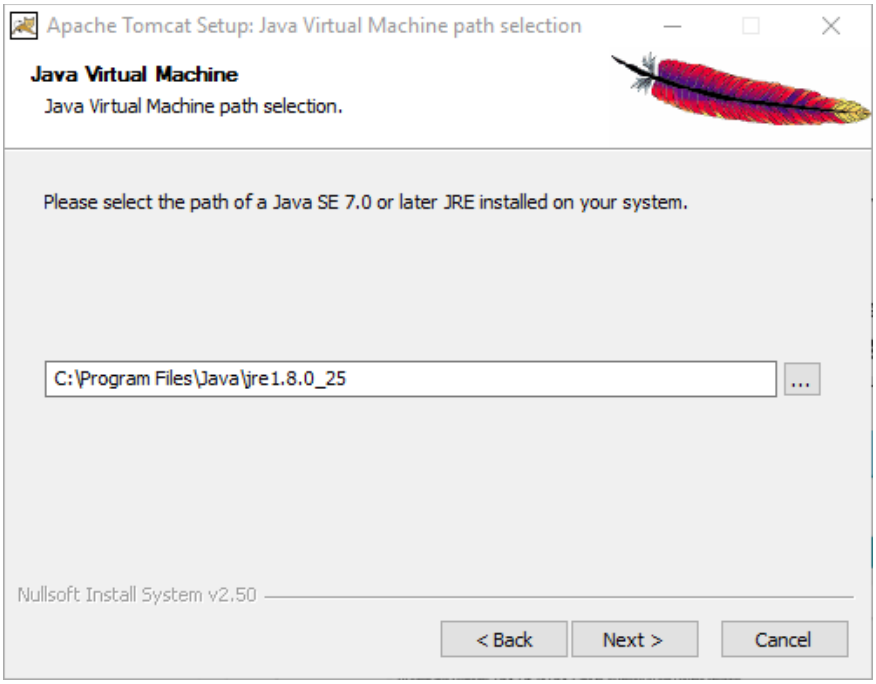
Agree to the terms and conditions.



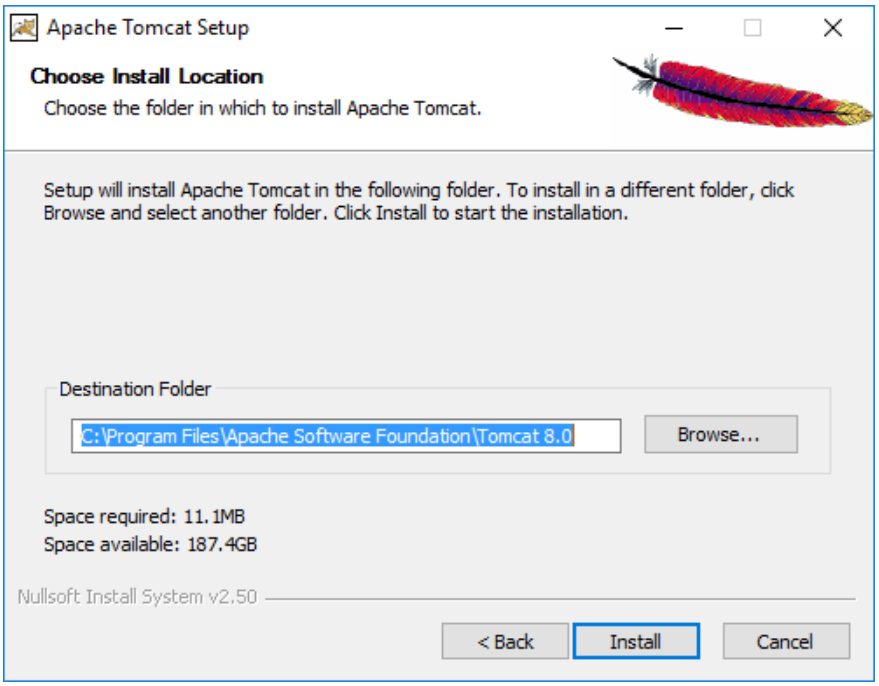
Only the normal installation is required but you may install more.



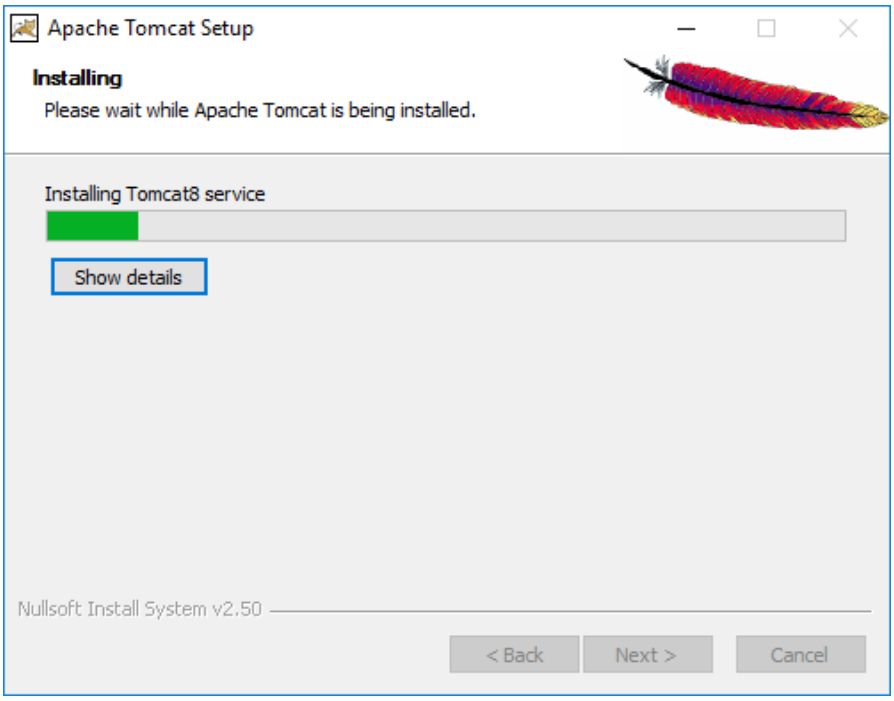
Default values should be fine.



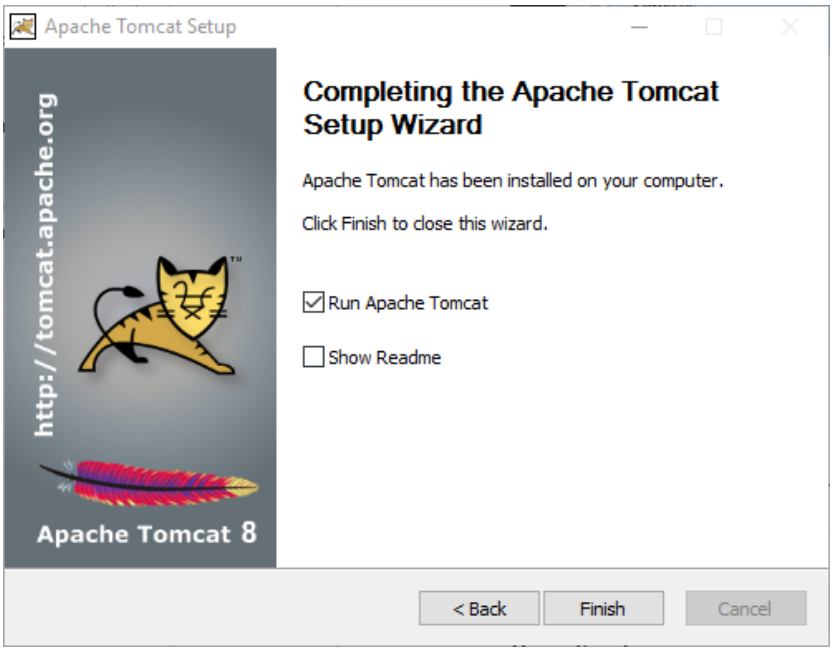
Tomcat automatically looks up the most recent JRE on your system. This is



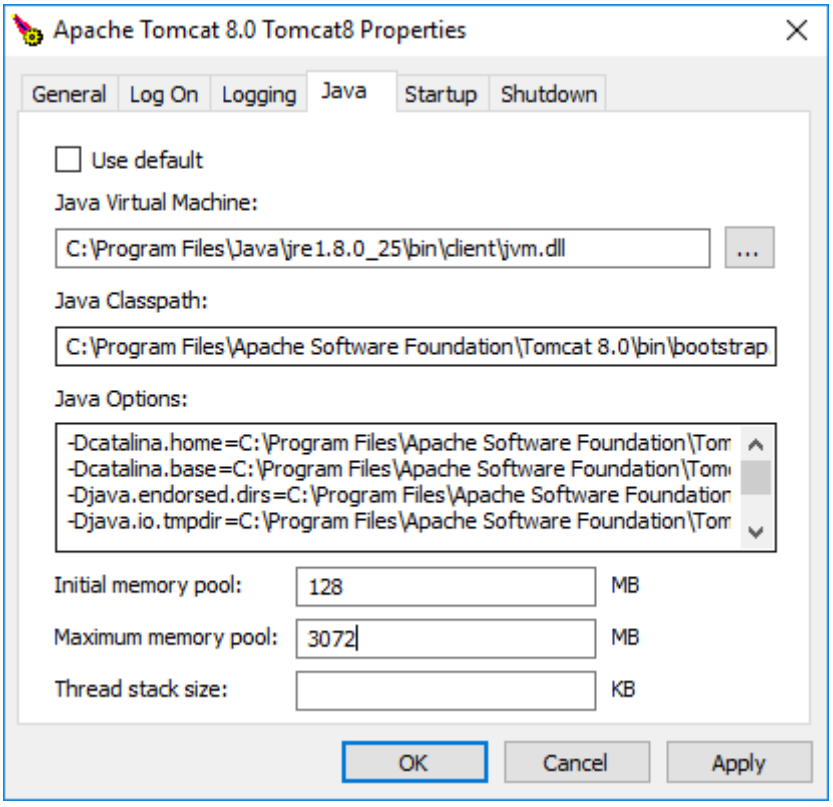
Default installation directory is fine.



Please wait for the service to install.



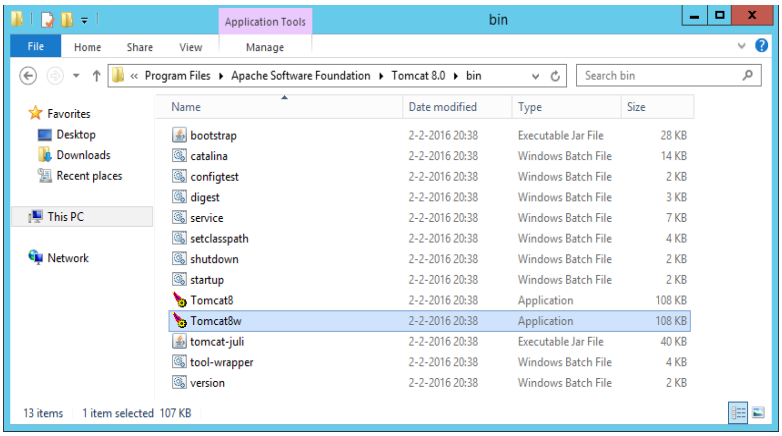
Run Tomcat and Finish the installation.



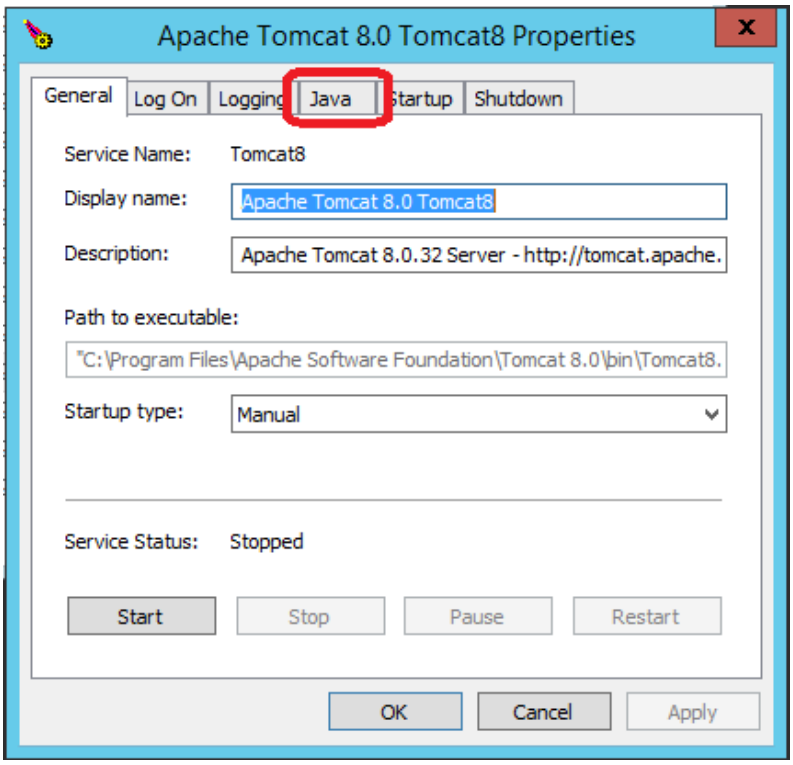
Open “C:\Program Files\Apache Software Foundation\Tomcat 8.0\bin\Tomcat8w.exe” and go to the java tab. Set the Maximum memory pool to at least 2048 MB. Remember to reboot the Tomcat service after changing Tomcat settings.

Special characters support for the Principal Toolbox:

On Windows-server installations (common for on-premise installations) it is needed to add two JVM parameters on starting the application. These parameters are mandatory to work with special characters.



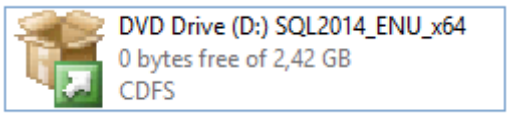
Start the Tomcat8w monitor application, which can be found in the Tomcat bin directory on the application server. The default location of this application is in C:\Program Files\Apache Software Foundation\Tomcat 8.0\bin.



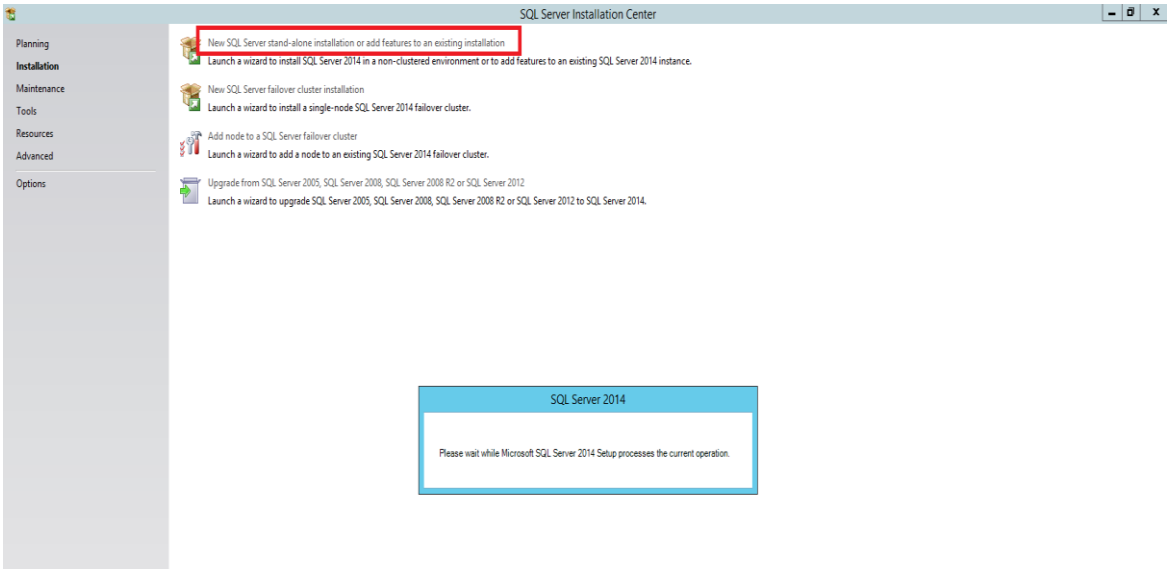
Go to the Java tab. Add the options "-Djavax.servlet.request.encoding=UTF-8" and "-Dfile.encoding=UTF-8" on a new row at the "Java Options" section. Click OK to save the changes

-Djavax.servlet.request.encoding=UTF-8
-Dfile.encoding=UTF-8

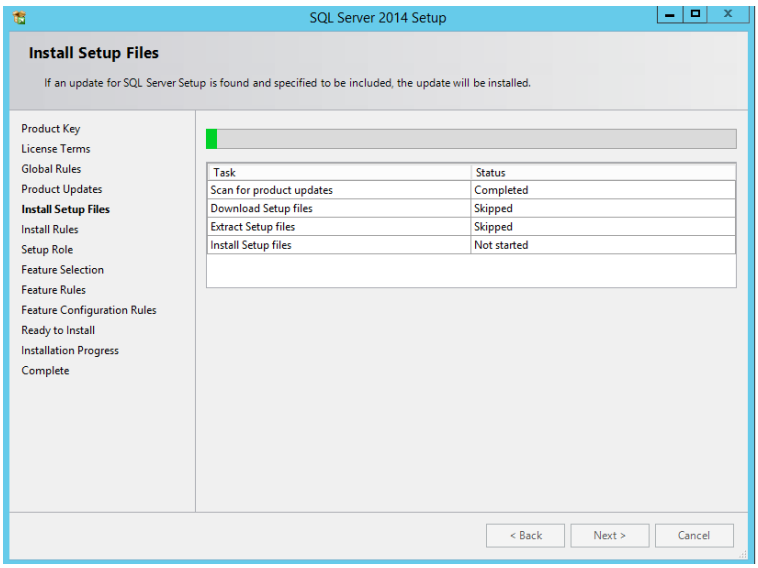
5.2 Microsoft SQL server – Installation



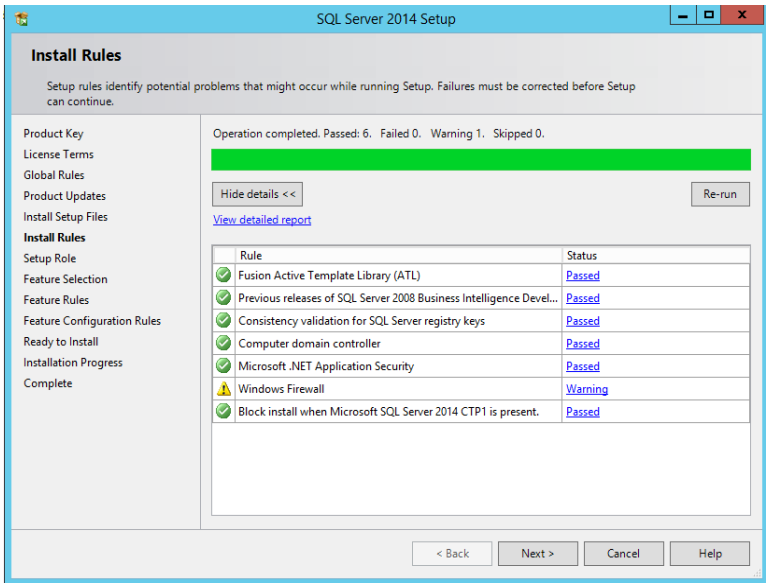
Mount the MSSQL server image and run the installation



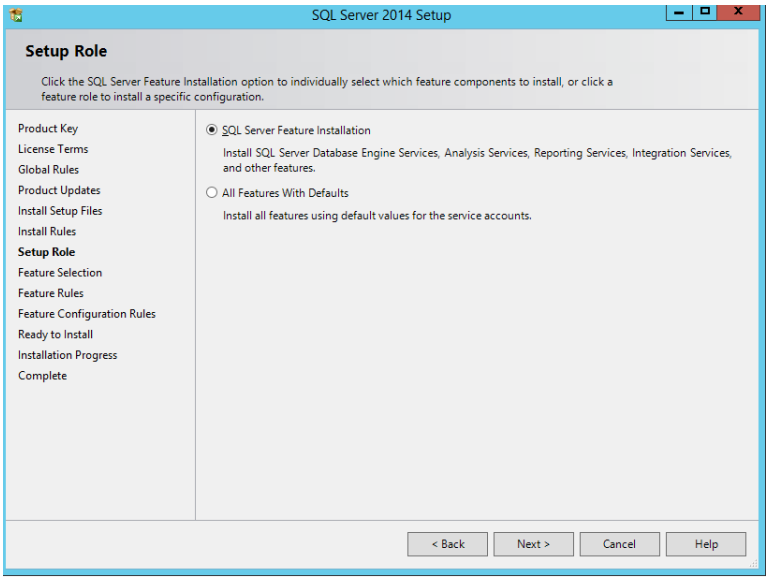
Go to the installation pane and install as a stand-alone installation



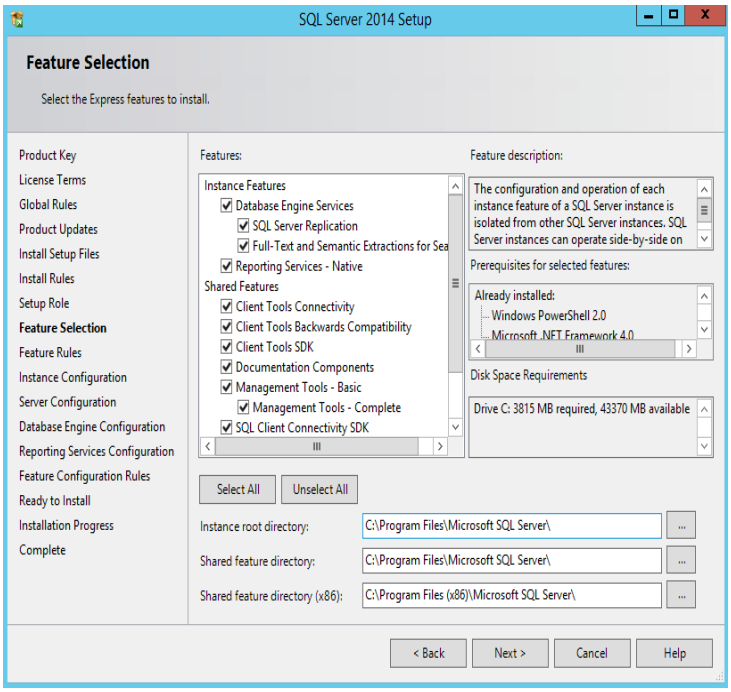
Please wait while the installation prepares the necessary files.



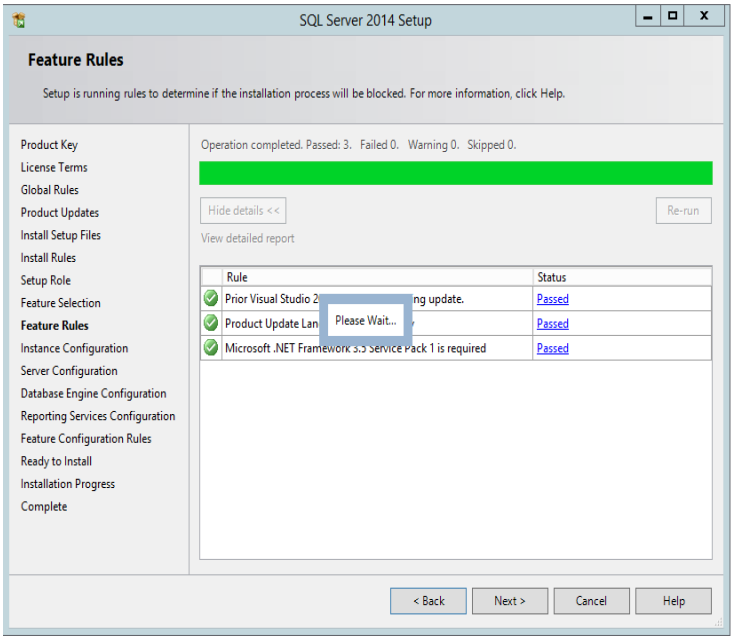
If there are no conflicts this pane is skipped. Fix the mentioned problems if necessary.



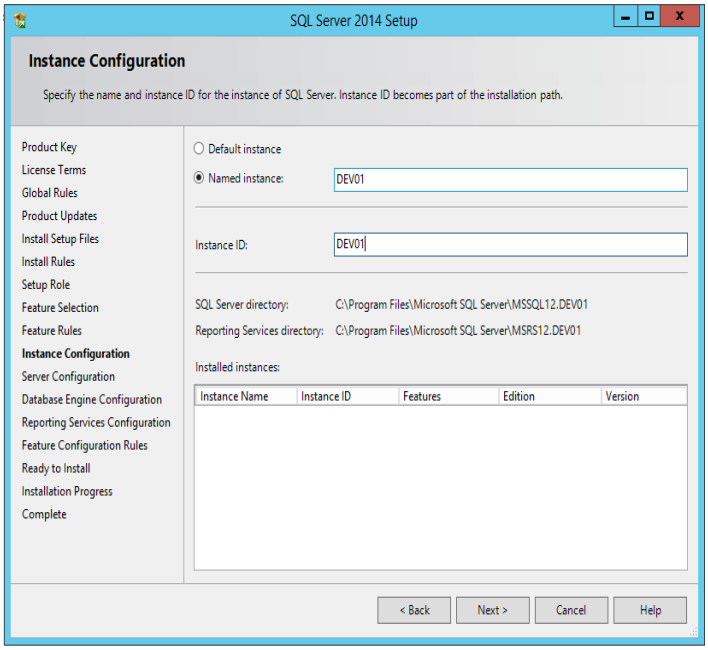
Select the Server Feature Installation.



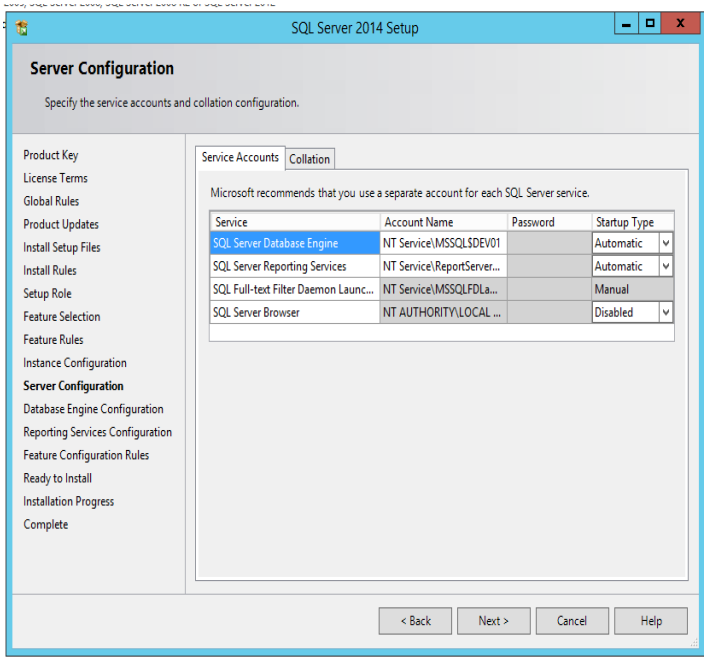
The “Database Engine Services” and “Management Tools - Complete” are necessary. You may install extra features if desired.



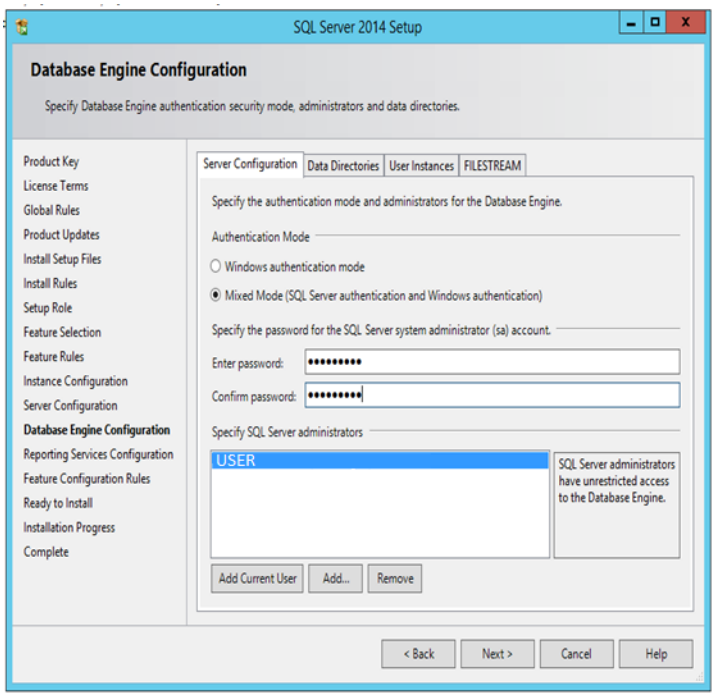
Please make sure that all dependencies are present.



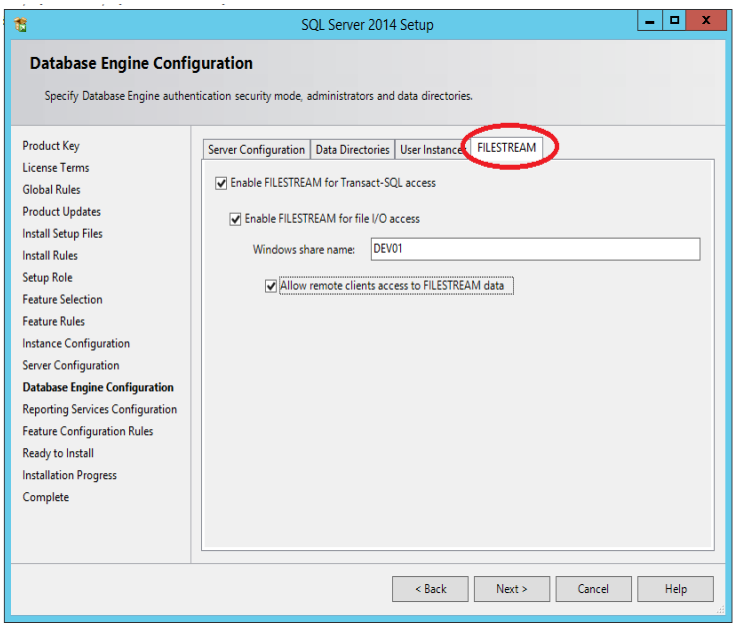
Give your database instance a name, for this tutorial we'll use "DEV01".



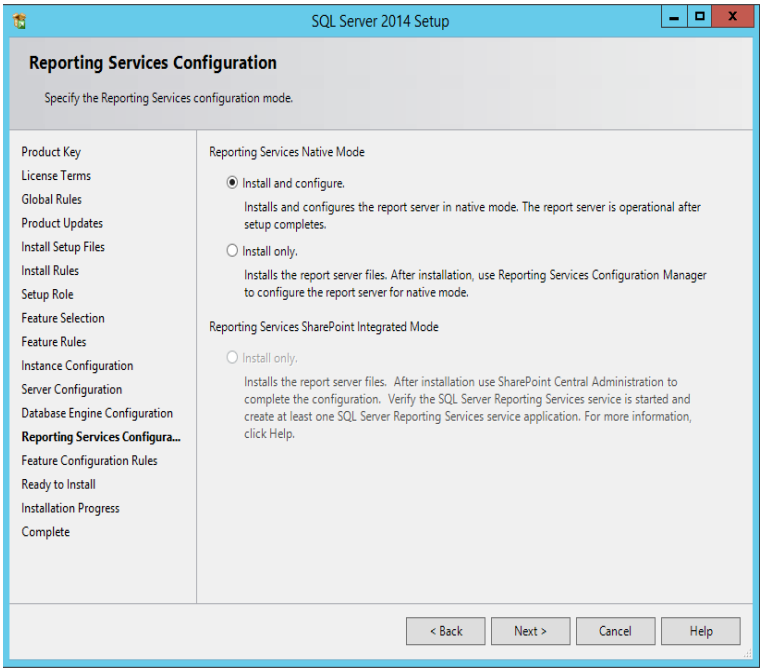
Make sure the "SQL Server Database Engine" starts automatically.
De number of options here may vary based on the earlier chosen features.



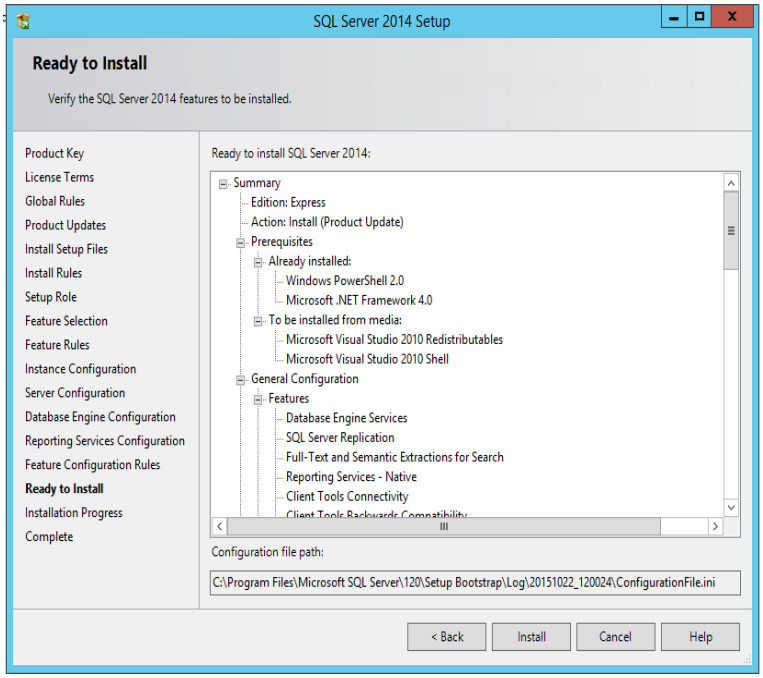
Choose a SQL Server administrator password and make sure that the windows account is an Administrator by pressing the “Add Current User”.
Do not press next yet!!



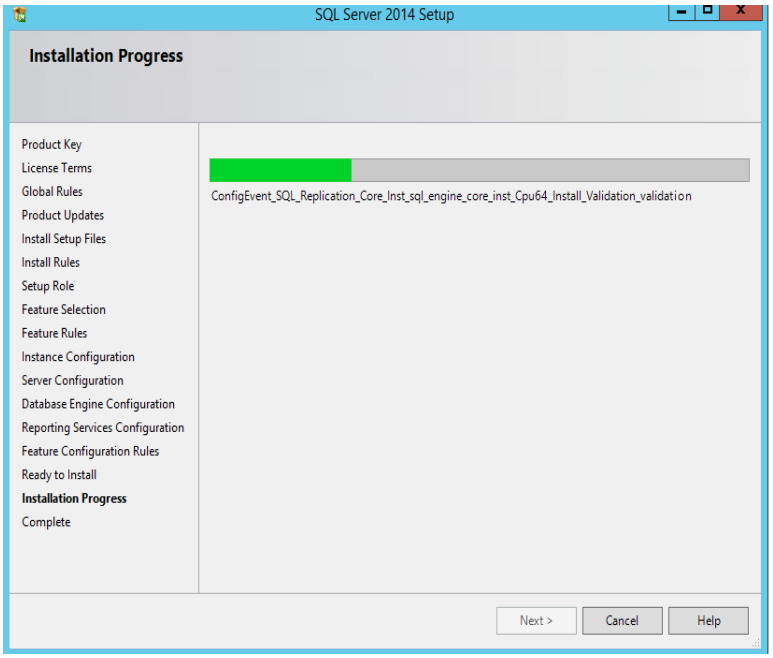
Go to the FILESTREAM tab and enable remote access.



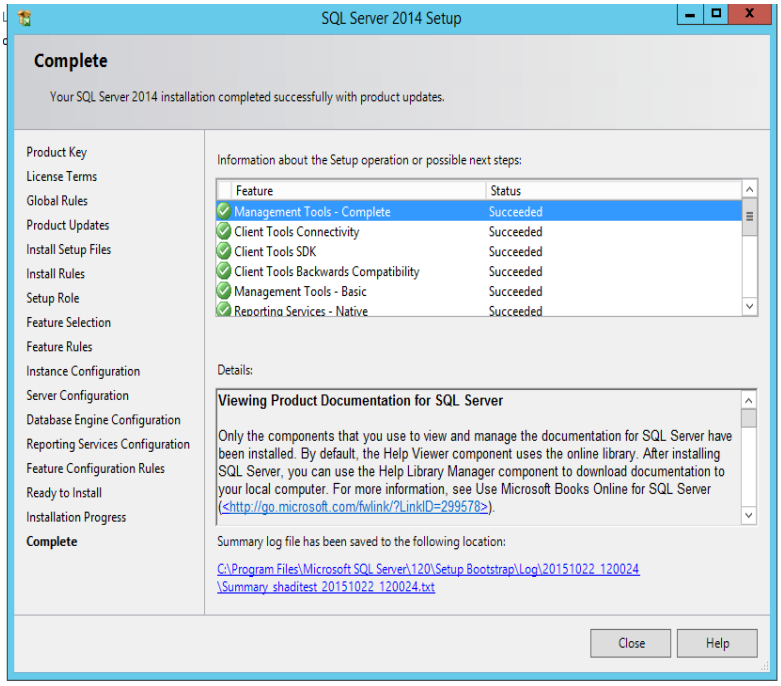
Install and configure.



Check your configuration and if correct “Install”



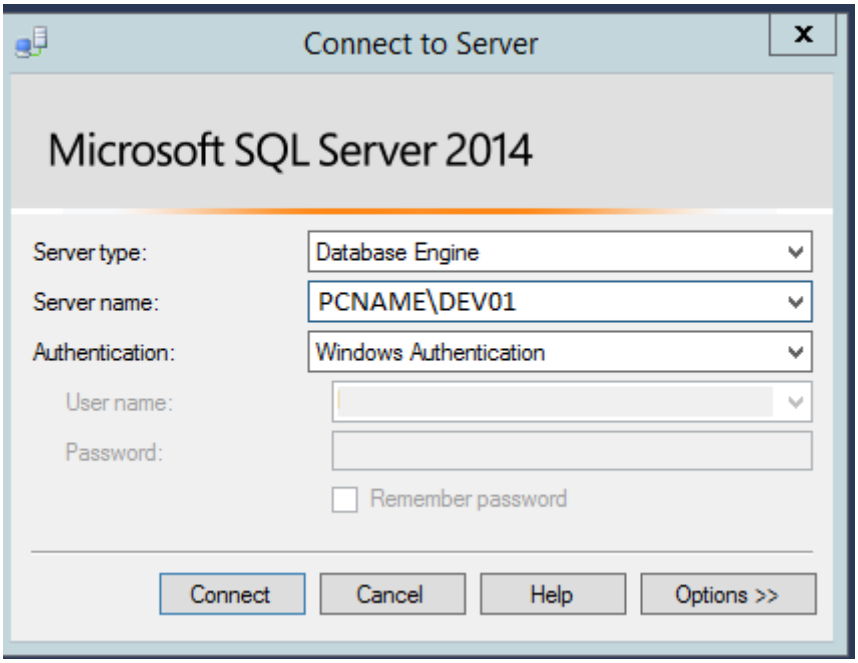
Please wait for this process to complete.



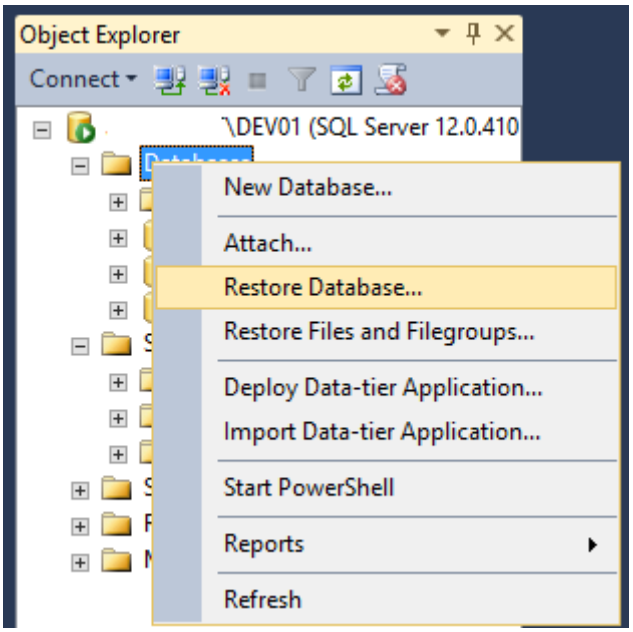
Check if everything is installed correctly.

5.3 Principal Toolbox database

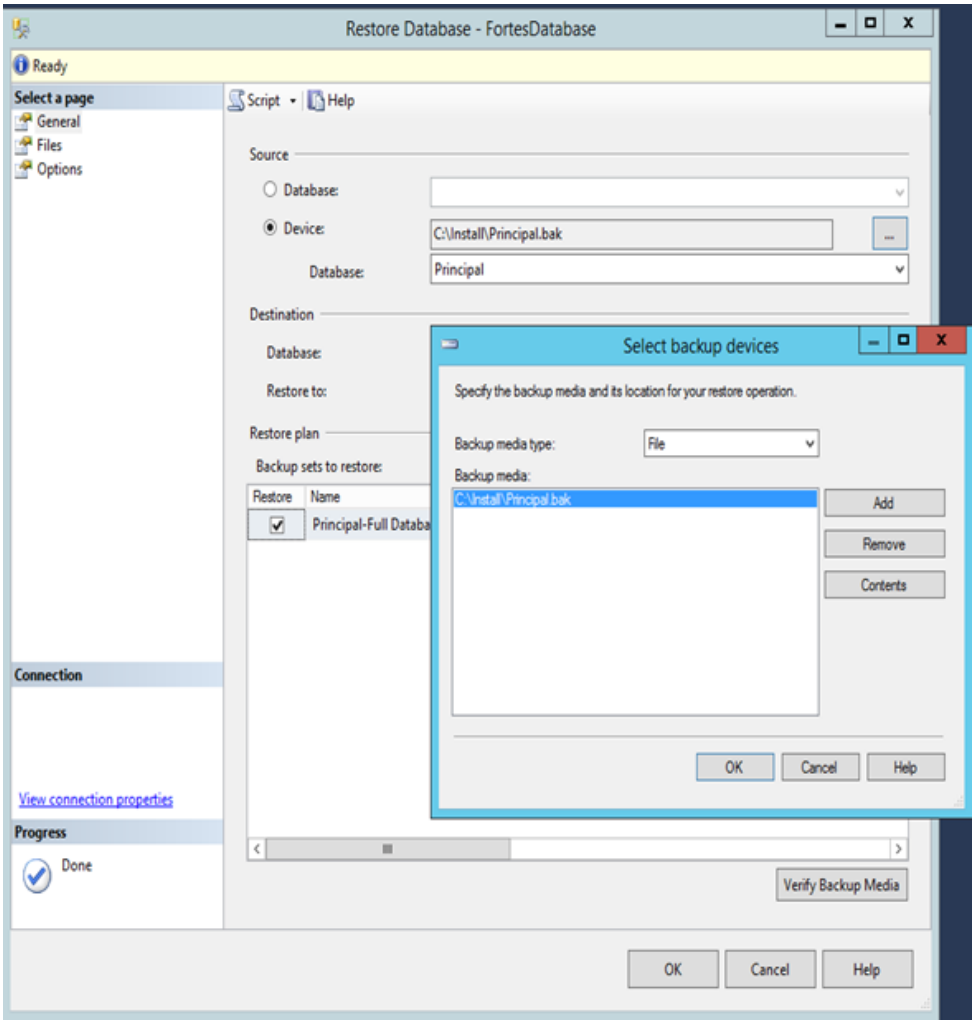
Open “SQL Server 2014 Management Studio”



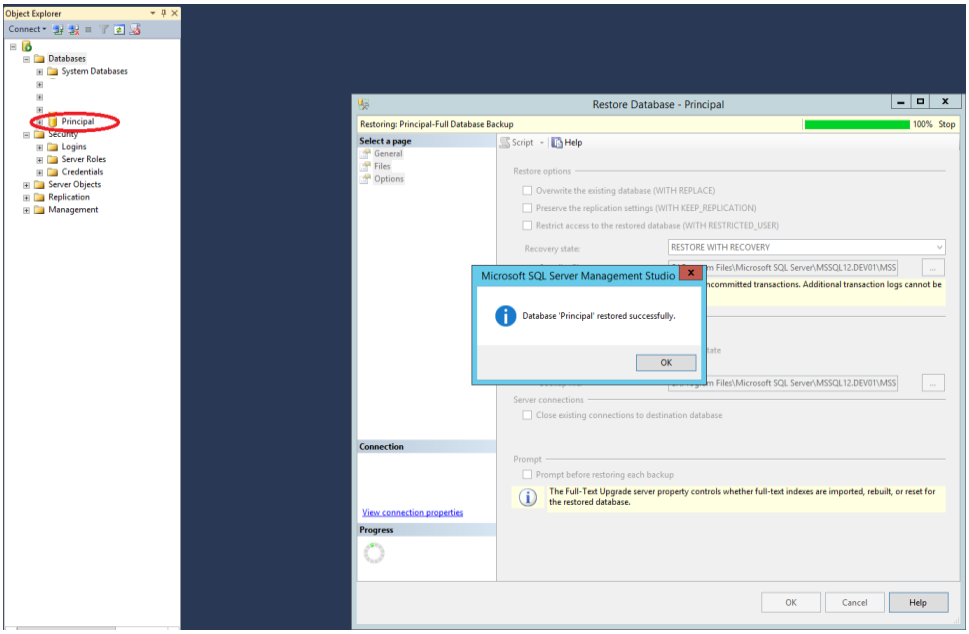
Login to the database instance created before with the account you entered during installation.
The current user is automatically used when using Windows Authentication on the local server.



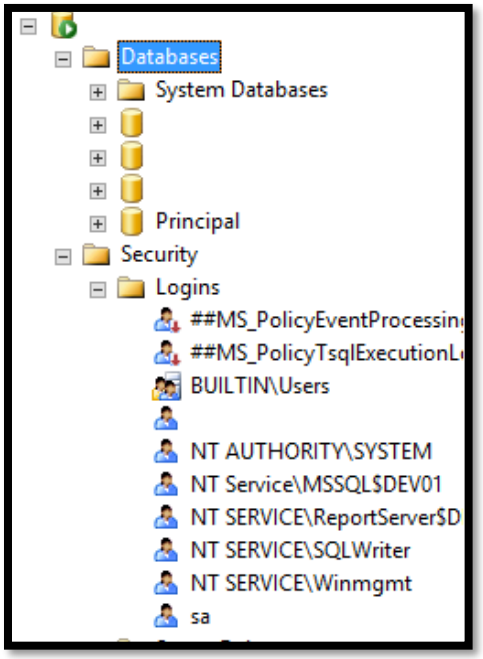
The toolkit database needs to be inserted into the database. This can be done by pressing the "Restore Database…" option in the Right-click menu.

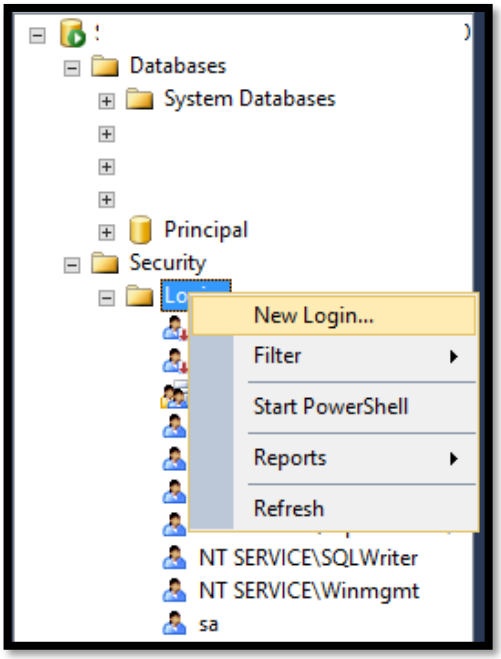


Select "Device" as Source and press the "…" button. Press the add button and locate the provided .bak file.

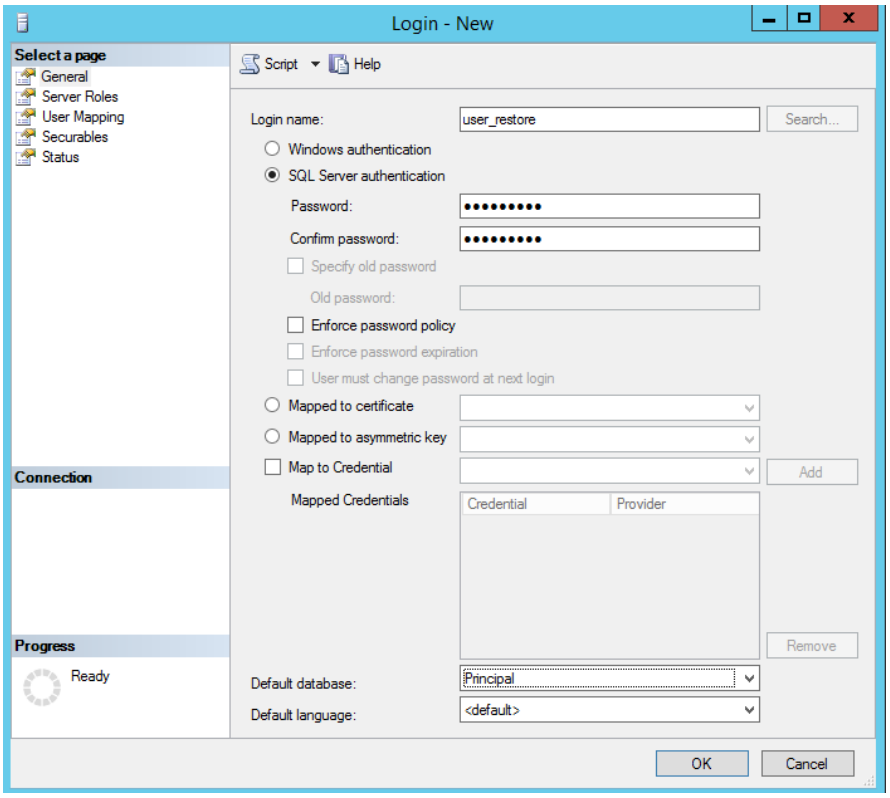


Wait for the restoration to be finished.



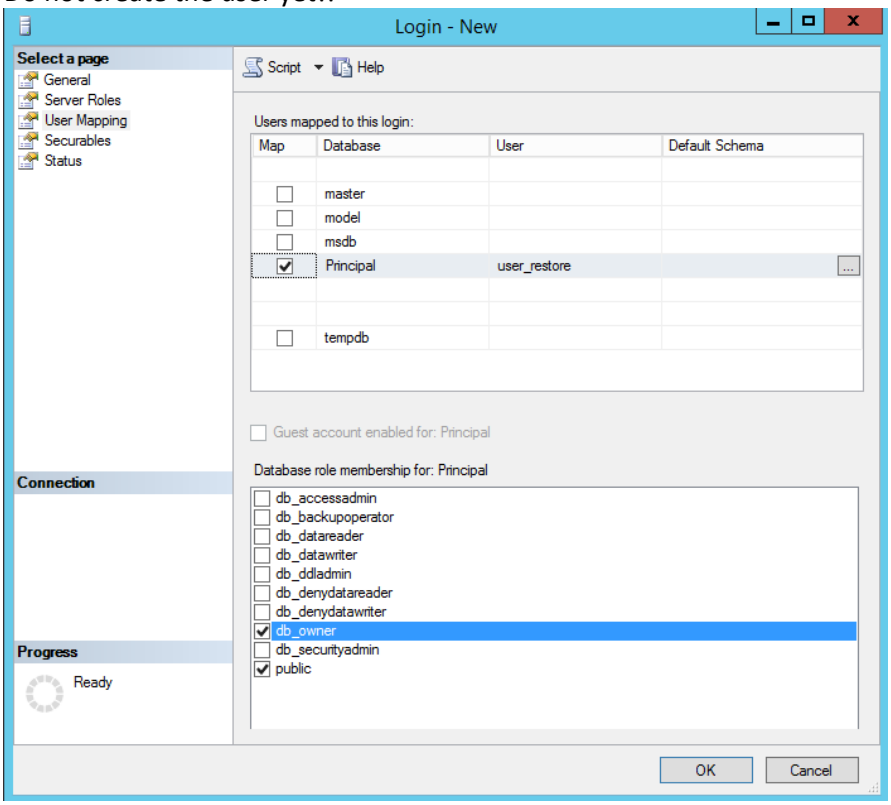


Look for the logins directory and create a new login.

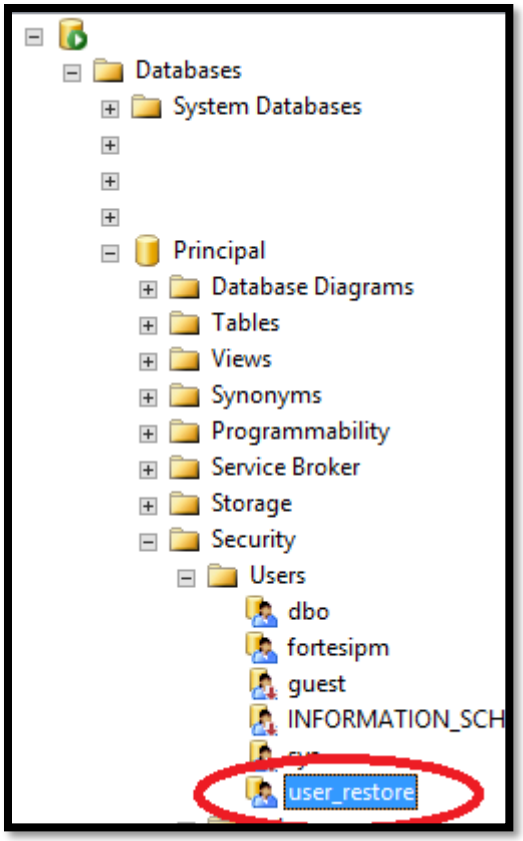


Make a SQL Server account named “user_restore” and select the Principal database as default database.

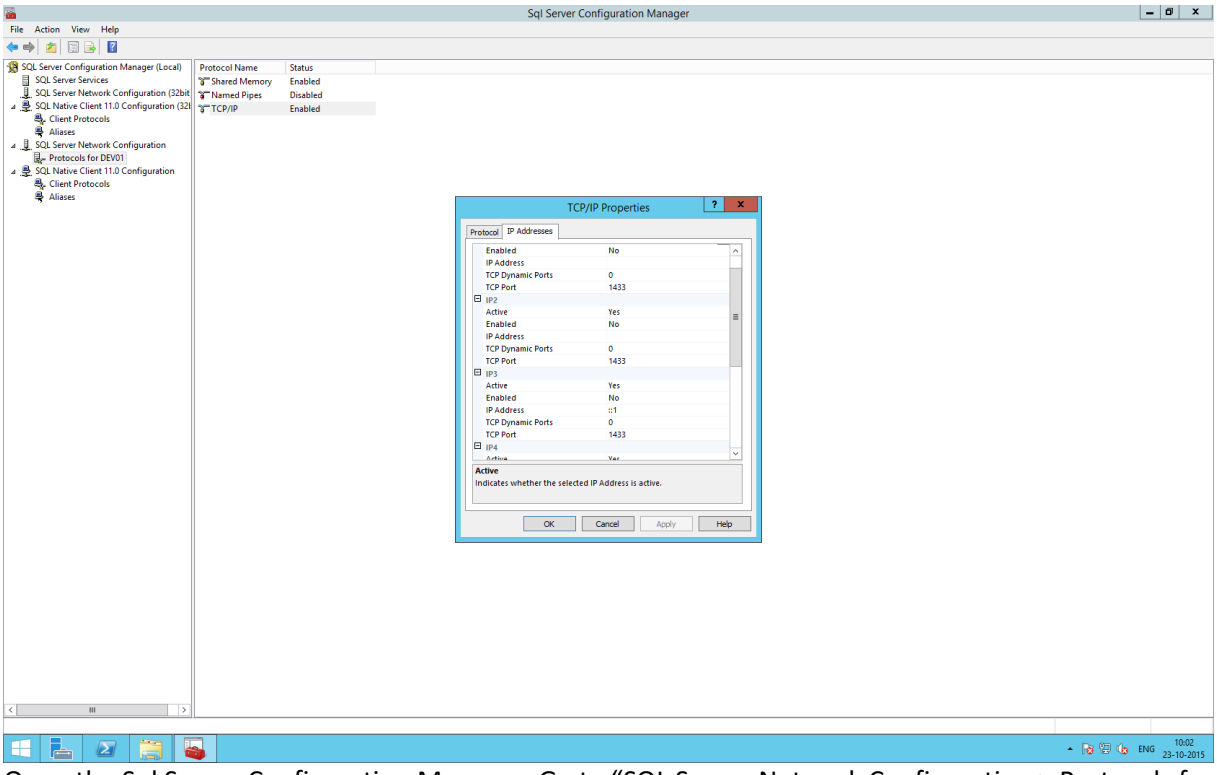
Do not create the user yet!!



Go to the User Mapping pane and select the Principal database. Make the new user the owner of the database by selecting “db_owner”



Check if the new user is created correctly.

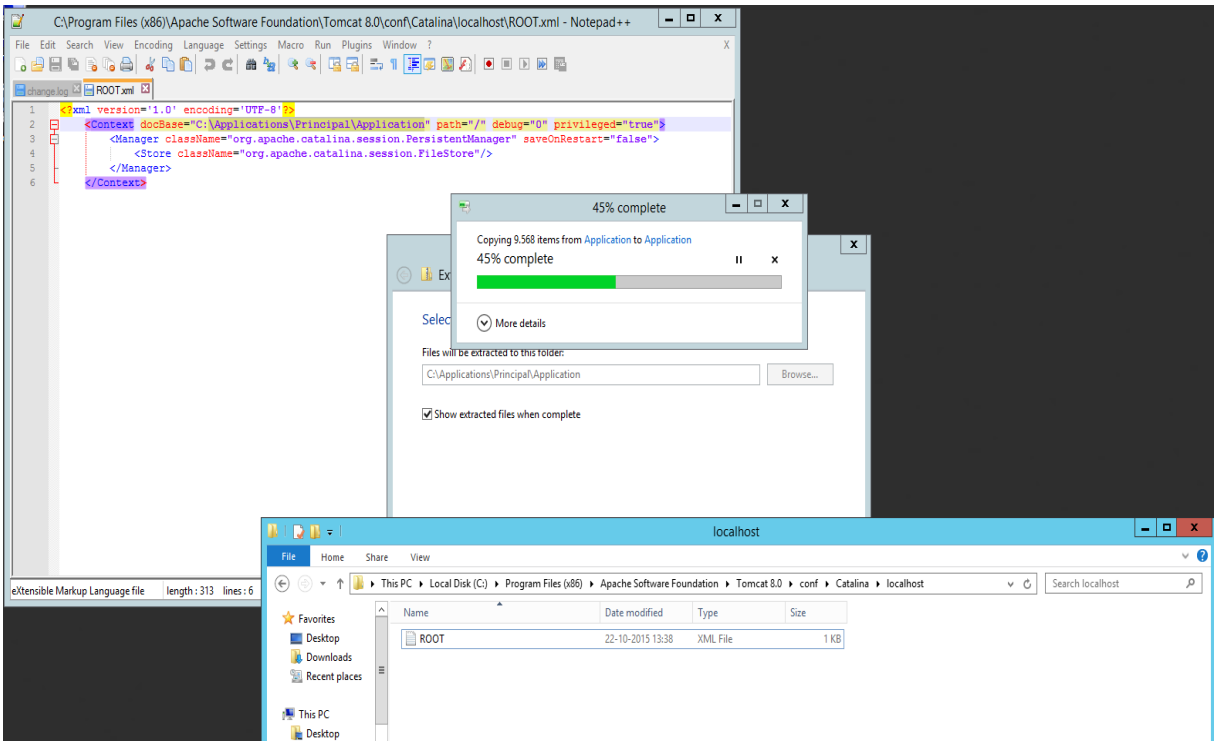


Open the Sql Server Configuration Manager. Go to “SQL Server Network Configuration > Protocols for DEV01” and open the properties of “TCP/IP”. Make sure that the database can be reached on the relevant host on port 1433, you can also allow all hosts by entering the port number in every field.

5.4 Principal Toolbox application

The Principal Toolbox comes with two installation files. The application folder and the database. In this section we will discuss the first installation file (application folder).

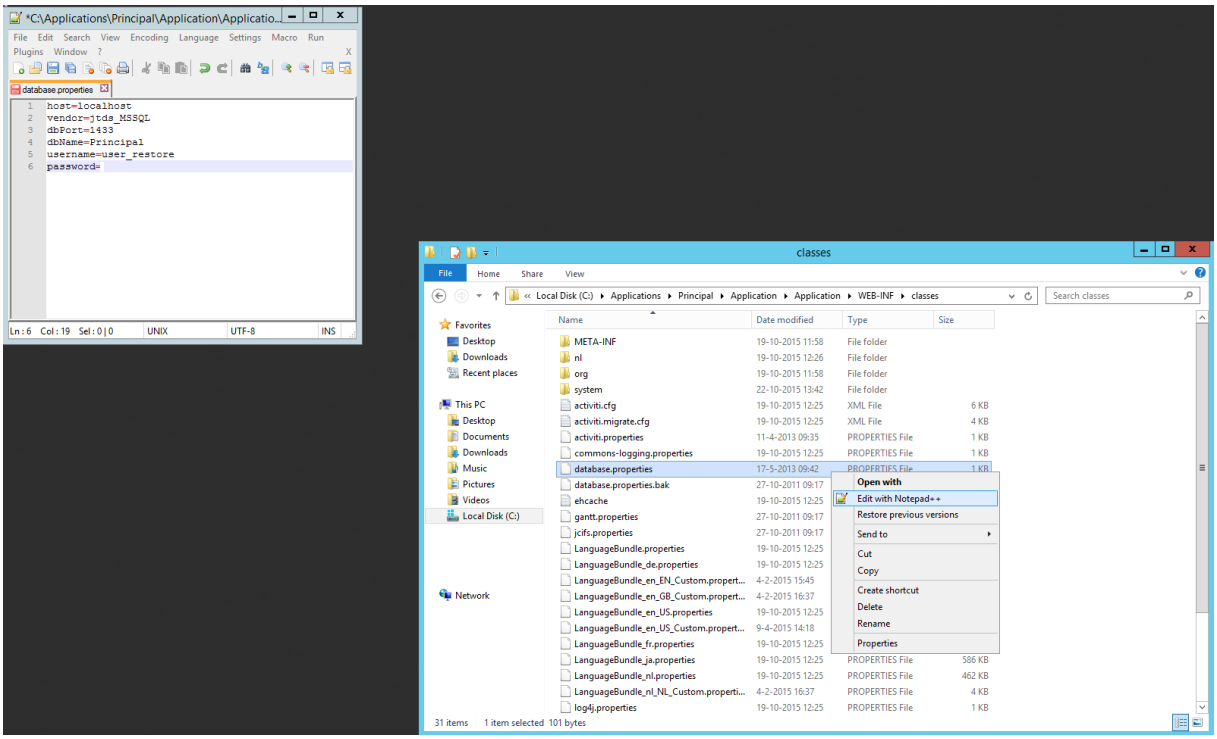
Extract the Toolbox to a logical location. Default is “C:\Applications\Principal\Application”



Copy the ROOT.xml from the “App\Integration\” directory to “C:\Program Files\Apache Software Foundation\Tomcat 8.0\conf\Catalina\localhost\” (It’s possible that this directory does not exist yet). And make sure that the docBase matches the location that you extracted the toolbox to.

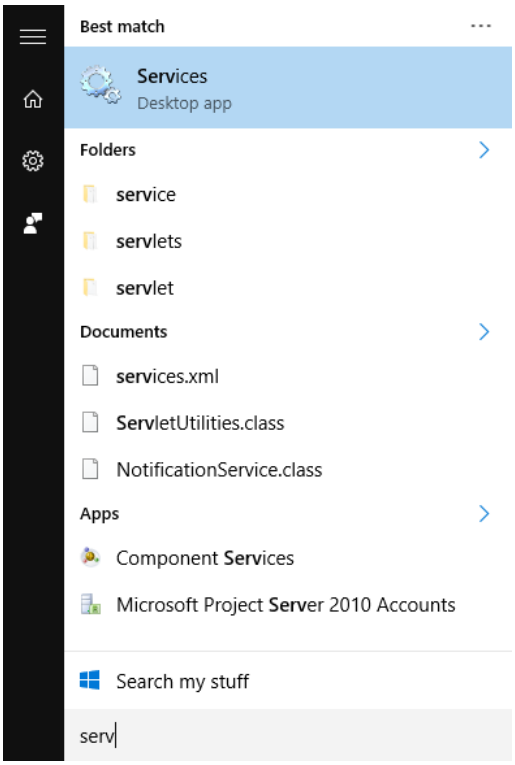
```
<?xml version='1.0' encoding='UTF-8'?>
    <Context docBase="C:\Applications\Principal\Application" path="/" debug="0" privileged="true">
        <Manager className="org.apache.catalina.session.PersistentManager" saveOnRestart="false">
            <Store className="org.apache.catalina.session.FileStore"/>
        </Manager>
    </Context>
```

ROOT.xml

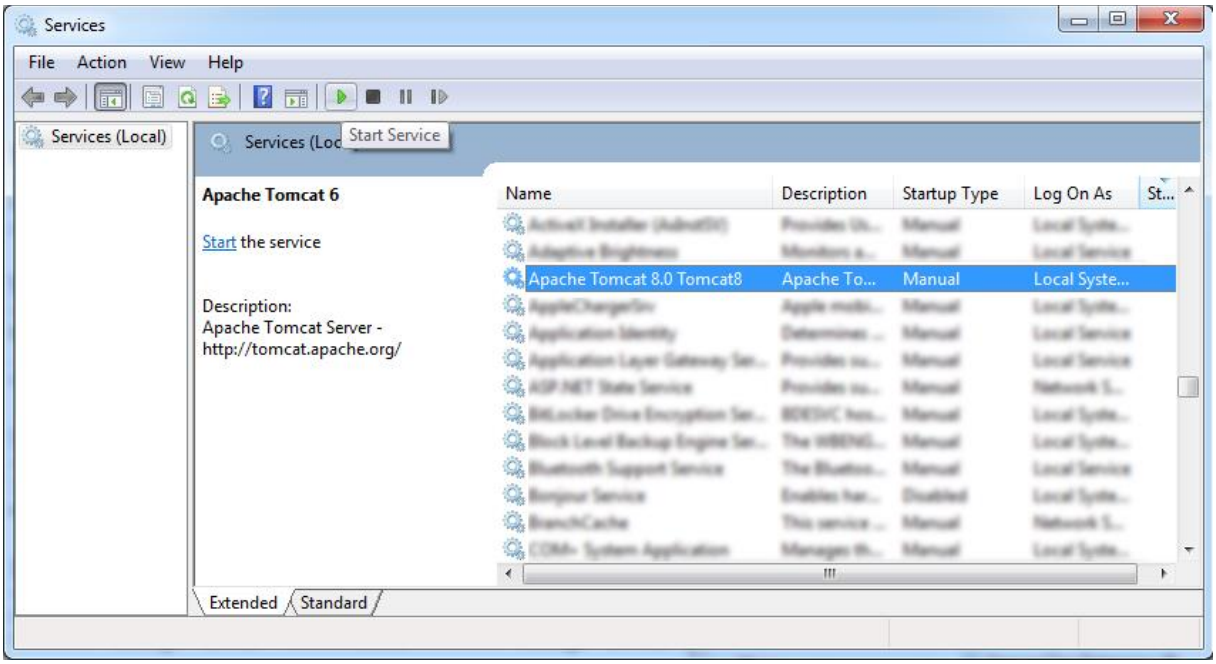


Edit the “database.properties” which can be found in “App\Application\WEB-INF\classes” and make it match:

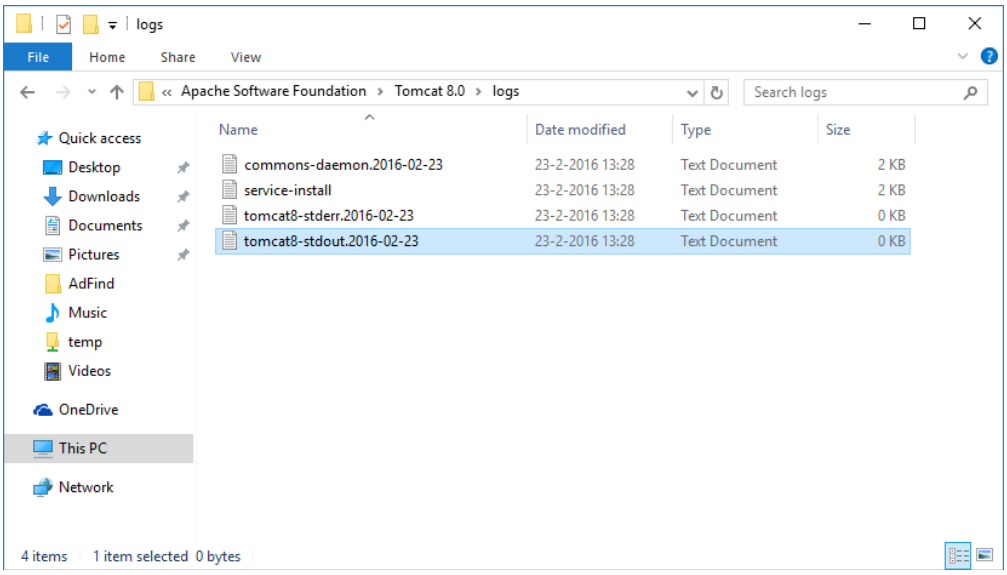
host=localhost	# The host of the used database. Probably localhost.
vendor=jtds_MSSQL	# Which type of database you use. Jtds is the recommended driver.
dbPort=1433	# Port on which the database can be reached
dbName=Principal	# Name of the database. This should match the name given in the # “Installation - Microsoft SQL server” chapter.
username=user_restore	# Name of the user. This should match the name given in the # “Installation - Microsoft SQL server” chapter.
password=*****	# Password for the user. This should match the name given in the # “Installation - Microsoft SQL server” chapter.



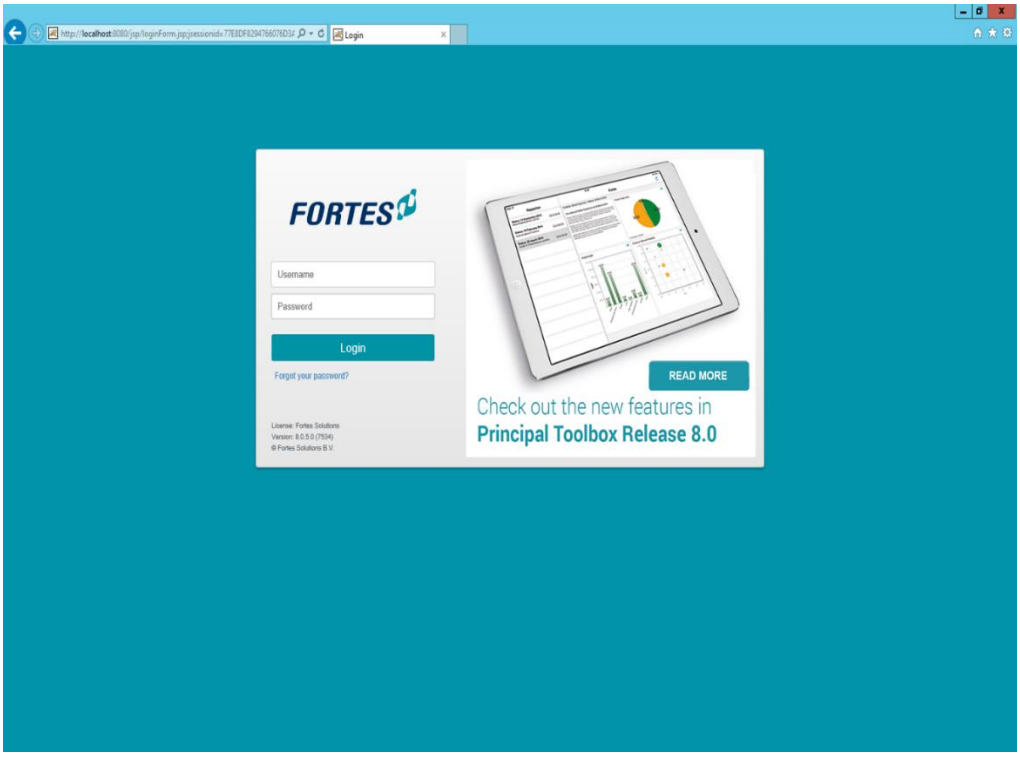
Open Services as Administrator



Look for “Apache Tomcat 8.0”. Notice that Tomcat8 is the name that we used in the installation, this is used to run multiple tomcat services on one system.
By pressing the right mouse button, you can restart the service or like shown in the picture you can use the buttons in the top.



You can find the Tomcat logs in “C:\Program Files\Apache Software Foundation\Tomcat 8.0\logs\”
To check if the server started correctly you can check the “Standard Out”-log. This can be found in the “tomcat8-stdout.<current_date>” like the one selected in the above picture.
TIP: Sort on “Date modified” to easily find the current date.

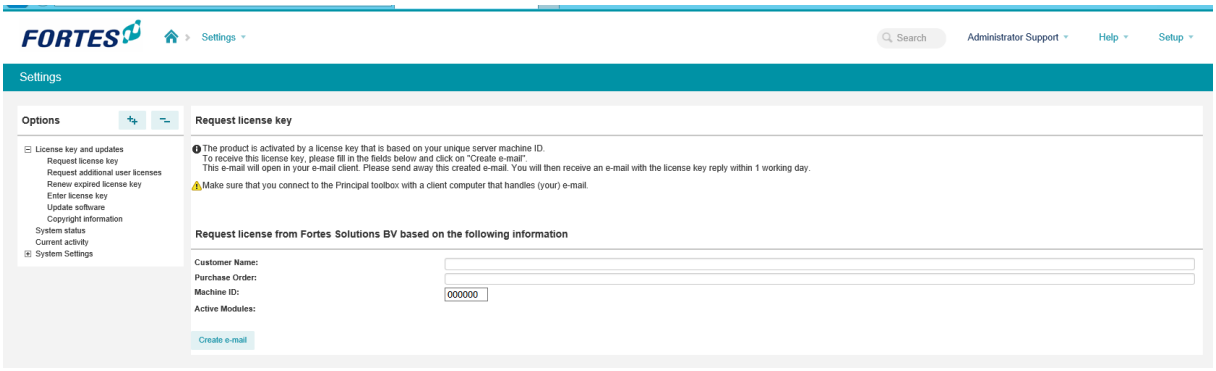


Open a browser with http://localhost:8080/ and check if the Toolbox is running.

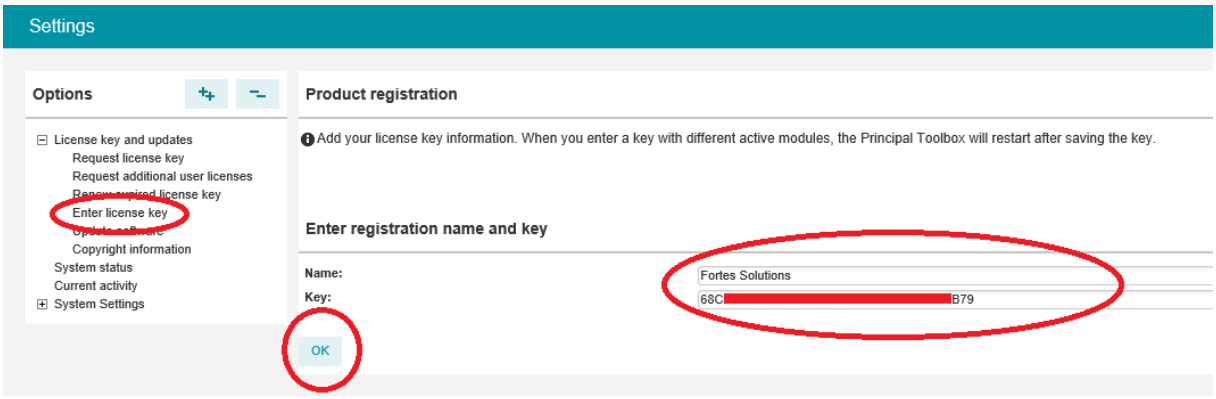
5.5 Principal Toolbox license

The Toolbox will recognize that it is installed on a new server. Any hardware changes forces the application to have a new machine ID. Therefore a new license needs to be added.

Login to the Principal Toolbox with an Administrator account.
Go to “Options > License key and updates > Request license key”

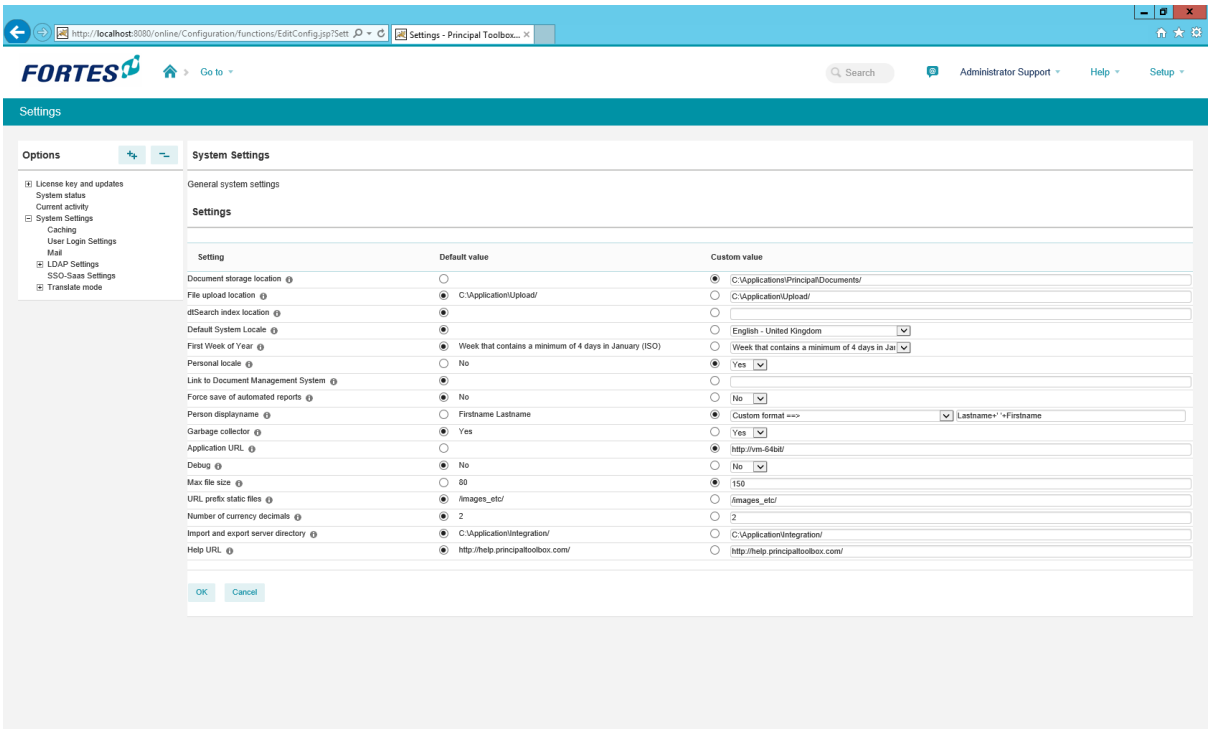


Please fill in the fields and click on “create email”. Please note that the Machine ID will be automaticly filled. The support of Fortes will receive a email after you clicked on the “create email button”. Support will then give you a license key back which you can fill in the “Enter license key” section.

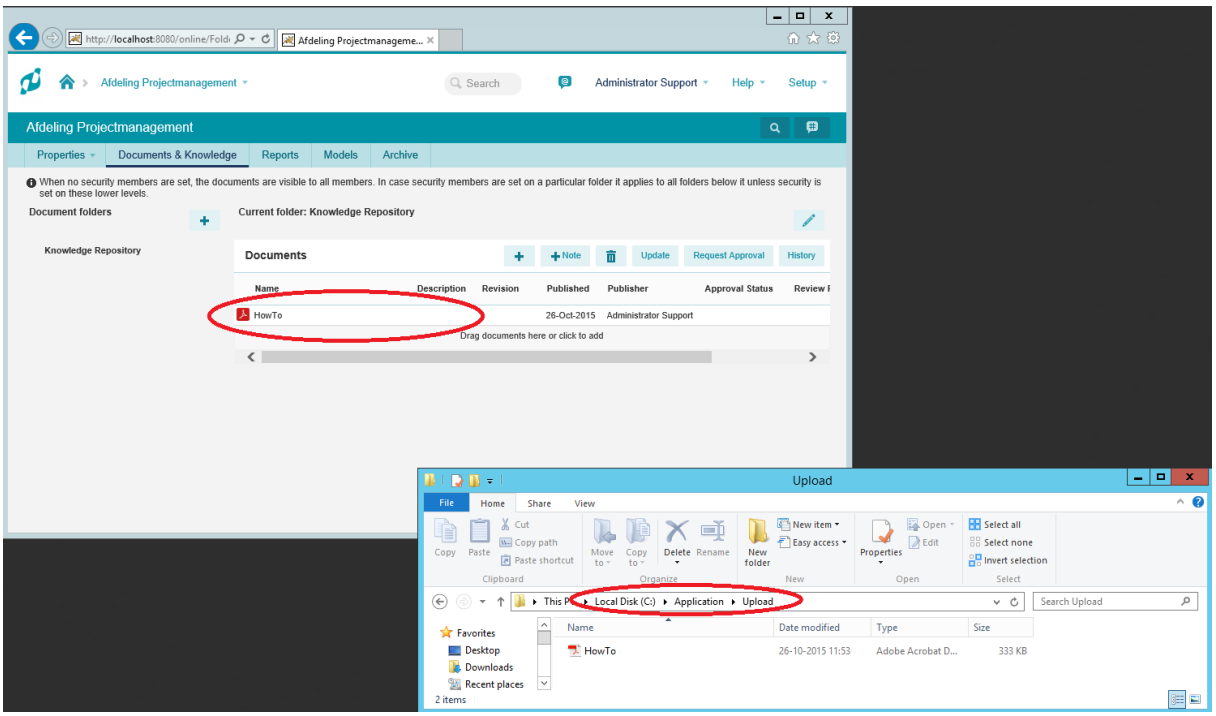


After you receive the licence key go to “Options > License key and updates > Enter license key” to enter the Name and Key you received.
After the license has been entered, restart the Tomcat server again to configure your Principal Toolbox.

5.6 Principal Toolbox configuration



In “Options > System Settings” you can change the storage location of documents. Change these settings to to your situation. Notice that you can also change a lot of other settings, file locations and directories.



Upload a file and check if it’s created in the correct location.

5.7 Securing the web interface

The web interface works just fine right now, but if you want to use Principal Toolbox outside of your intranet you will have to encrypt your web interface.
Setting up SSL for Tomcat can be pided into two main tasks: creating a functional keystore, and configuring the Tomcat connectors and applications. Let's tackle them one at a time.

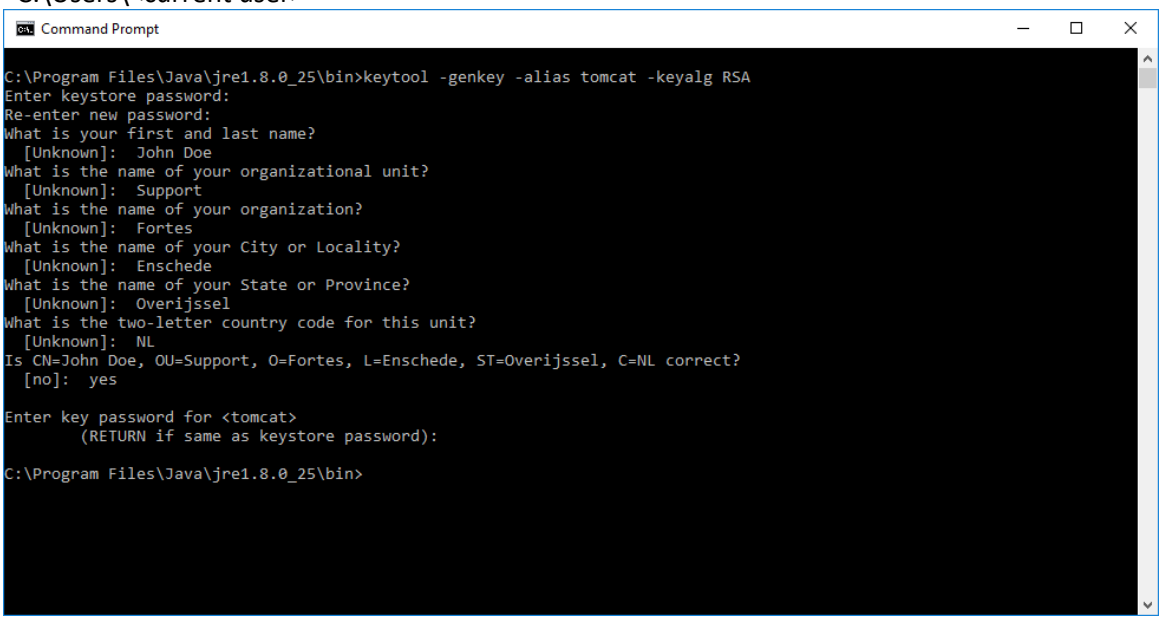
PART I - The Keystore

Step 1 - Creating the Keystore

The keys Tomcat will use for SSL transactions are stored in a password-protected file called, creatively, the "keystore." The first step to enabling SSL on your server is to create and edit this file. You can create this file in one of two ways - by importing an existing key into the keystore, or by creating an entirely new key.

In the interest of simplicity, this guide will only cover the latter (but you can find instructions for importing keys on Apache's Tomcat Documentation site).
A program called keytool, which is included with your JDK, will do the actual work of creating your new keystore. To create a new keystore using this program, enter the following command at the command-line, substituting syntax appropriate for your OS:

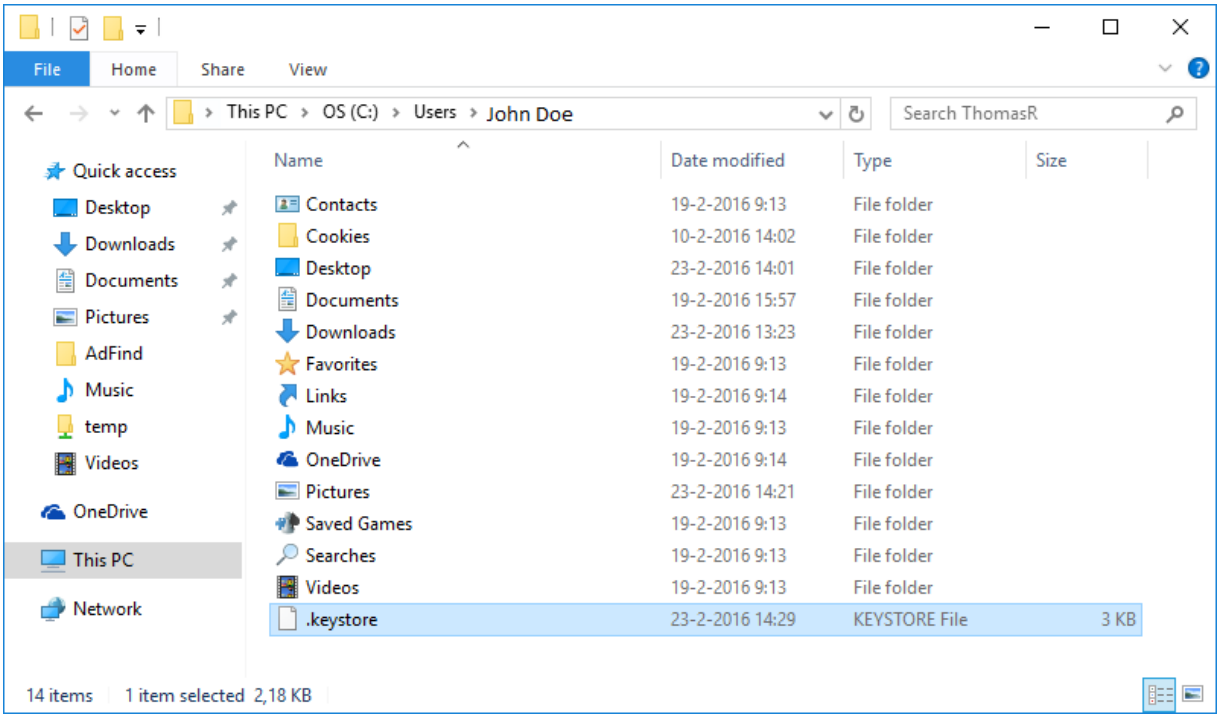
$JAVA_HOME/bin/keytool -genkey -alias [youralias] -keyalg RSA -keystore [/preferred/keystore/path]
Use an [alias] and [path] of your choice.
For example:
"C:\Program Files\Java\jre1.8.0_25\bin\keytool" -genkey -alias tomcat -keyalg RSA
By not defining the keystore location the default is used, namely your home directory "C:\Users\<current user>"



Next, keytool will ask you to enter the password you want to use for the keystore. Again, choose whatever you like (but don't forget it).
After you choose the keystore password, you will enter the information required for the Certificate, such as your company and your name. Make sure this information is accurate, as you will have to submit this file to the Certificate Authority of your choice to obtain a certificate. Also, the users will see this information to verify if the website is not compromised.

The last thing keytool will ask you to specify is the key password, which is the password specific to this specific certificate. Rather than enter anything at this prompt, just press ENTER to use the previously chosen keystore password.

This will cause keytool to set the key password to a value equivalent to the keystore password. Matching passwords are REQUIRED for Tomcat to access the certificate. If you choose two different passwords, any attempts to access the keystore will result in a crash (so don't do it).
Congratulations - if you followed the directions correctly, you should now have a usable keystore file named [youralias], located in the directory you choose.



Step 2 - Creating the Certificate Signing Request (optional)

Now that you've created your keystore, it's time to create a file called the Certificate Signing Request, or CSR, which will be used by the Certificate Authority of your choice to generate the Certificate SSL will present to other parties during the handshake.

You can use the keytool to create this file, as well. To do so, enter the following at the command line:
$JAVA_HOME/bin/keytool -certreq -keyalg RSA -alias [youralias] -file [yourcertificatname].csr -keystore [path/to/your/keystore]

Substitute the values you chose earlier for the [placeholders].
If you follow the instructions correctly, keytool will create a file called yourcertificatename.csr, which you can submit to the CA you've chosen via the process they provide on their website. Using this file, they will generate a custom certificate for your server, which you can download according to the instructions they provide on their website.

Step 3 - Installing Your New Certificate (optional)

SSL verifies the authenticity of a site's certificate by using something called a "chain of trust," which basically means that during the handshake, SSL initiates an additional handshake with the Certificate Authority specified in your site's certificate, to verify that you haven't simply made up your own CA. In order to "anchor" your certificate's chain of trust, you have to download an additional certificate, called a "Root Certificate," from your CA, and then import both this certificate and your site's new certificate into your keystore. Your CA should provide information about obtaining a Root Certificate on their website.

Once you've downloaded both your own Certificate and the Root certificate provided by your CA, import them into your keystore with the following commands, replacing the [placeholders]:

To import the Root Certificate -
keytool -import -alias root -keystore [path/to/your/keystore] -trustcacerts -file [path/to/the/root_certificate]

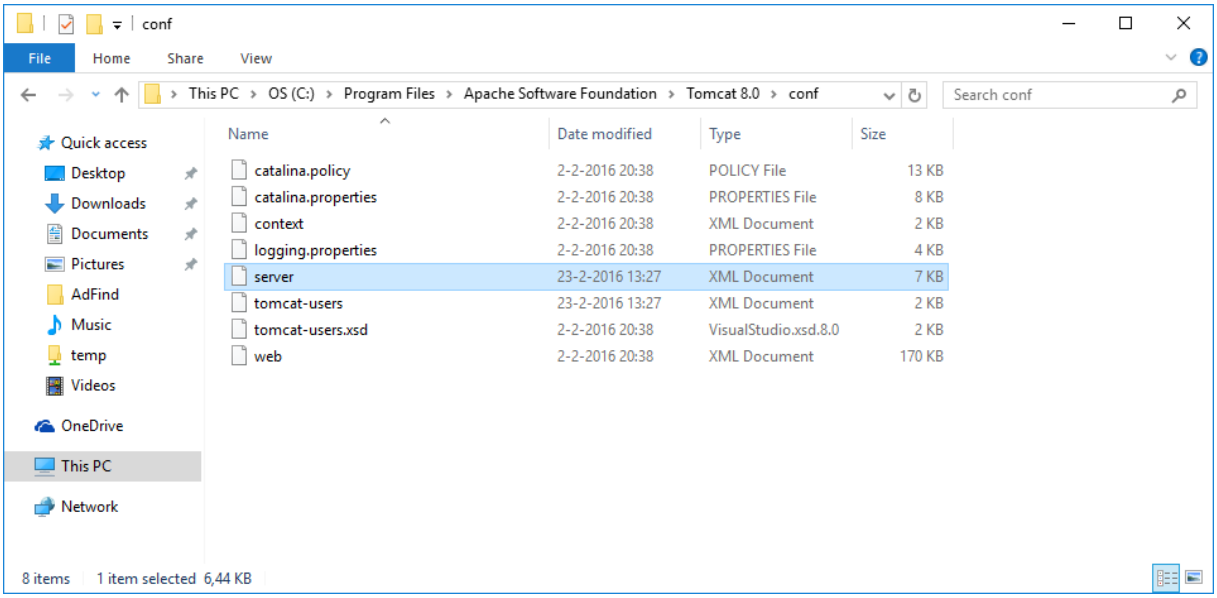
To import your new Certificate -
keytool -import -alias [youralias] -keystore [path/to/your/keystore] -file [path/to/your_keystore]
Do everything right? Then pat yourself on the back - you are now the proud owner of a functional, certified keystore.

PART II - Configuring Tomcat to use SSL

Now that we have a functional keystore populated with valid certificates, it's time to configure Tomcat to use SSL. First, we'll configure Tomcat's SSL connectors, and then we'll specify which webapps we want to use SSL by default.

Configuring Tomcat's SSL Connectors

Tomcat's global Connector options are configured in Tomcat's main configuration file, "$CATALINA_BASE/conf/server.xml", so you should open this file now.



The Connectors we are looking for connect on port 8443 by default, so search for this port, until you come across an entry that looks like this:

```
79      <!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
80           This connector uses the NIO implementation that requires the JSSE
81           style configuration. When using the APR/native implementation, the
82           OpenSSL style configuration is required as described in the APR/native
83           documentation -->
84      <!--
85      <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
86                 maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
87                 clientAuth="false" sslProtocol="TLS" />
88      -->
```

You'll notice that the comment enclosing this connector talks about a choice between APR and JSSE configurations. This refers to the implementation of SSL you are intending to use. JSSE, which is Tomcat's default configuration, is supported by default, and included in all JDKs after version 1.4. So if you don't even know what APR is, you only need to uncomment this entry by removing the “<!--” and “-->”, and add some additional information to allow Tomcat to find your keystore:

keystoreFile="path/to/your/keystore" keystorePass="YourKeystorePassword" keyAlias="yourAlias"

```
79      <!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
80           This connector uses the NIO implementation that requires the JSSE
81           style configuration. When using the APR/native implementation, the
82           OpenSSL style configuration is required as described in the APR/native
83           documentation -->
84
85      <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
86                 maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
87                 clientAuth="false" sslProtocol="TLS"
88                 keystoreFile="path/to/your/keystore" keystorePass="YourKeystorePassword" keyAlias="yourAlias" />
89
```

Restart Tomcat. Once you're up and running again, test your configuration by connecting to a secure page, using a URL such as https://[yourhost]:8443. If you followed the directions correctly, you should be able to view the page over a secure HTTPS connection!

6 Required Internet Explorer Security Settings

Below you will find a table with the required security settings of the appropriate Internet Explorer security zone used by the Principal Toolbox.

	Setting	Value	Remarks
ActiveX controls and plug-ins			
	Initialize and script ActiveX controls not marked as safe for scripting	Enable	Script errors on different pages occurs when disabled.
	Script ActiveX controls marked safe for scripting (*)	Enable	The Edit Project Plan window hangs while message "Processing please wait" is displayed.
Downloads			
	Automatic prompting for file downloads	Enable	Function to pack project offline can't offer to download the offline project.
	File download	Enable	When disabled, automated reports and documents can't be downloaded.
Miscellaneous			
	Allow META REFRESH	Enable	Internet Explorer window stays blanc after login when disabled
	Allow websites to open windows without address or status bars	Enable	Internet Explorer will display a grey address bar in all pop-ups when disabled
	Launching applications and unsafe files	Enable	Required for installing the MS Project Client add-in.
	Submit non-encrypted form data	Enable	When disabled, Internet Explorer can't update changes in text fields.
	Use Pop-up Blocker	Disabled	Internet Explorer blocks the "Edit name for new item" dialog after adding the first product on the Edit project plan page when enabled
Scripting			
	Active scripting	Enable	Login button on login screen doesn't react. Drag and drop in Edit Project Plan window won't work when disabled
	Allow paste operations via script (*)	Enable (or Prompt)	Keywords for automatic reports won't be copied to the clipboard when disabled.
	Allow Programmatic clipboard access (**)	Enable (or Prompt)	Keywords for automatic reports won't be copied to the clipboard when disabled.
User Authentication			
	Logon	Automatic for logon only in Intranet zone	When Single Sign On is enabled, this setting allows to sent username and password over the intranet

(*) Only required or available for Microsoft Internet Explorer version 6.

(**) Only required or available for Microsoft Internet Explorer version 7+.

7 How to update the Principal Toolbox

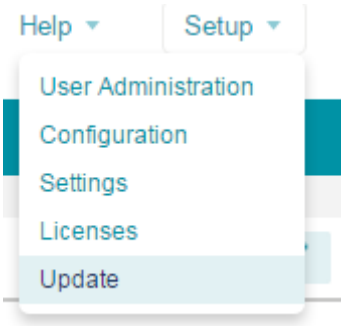
Best practice: make a copy down to test the new version first before updating the production application!

Implementing updates and the installation of new releases of the Principal Toolbox is done via the Settings within the Principal Toolbox application. You will receive a file in the form of a .jar file from Fortes Solutions in order to implement an update or to be able to install a new release. Please ask support for the latest stable version!

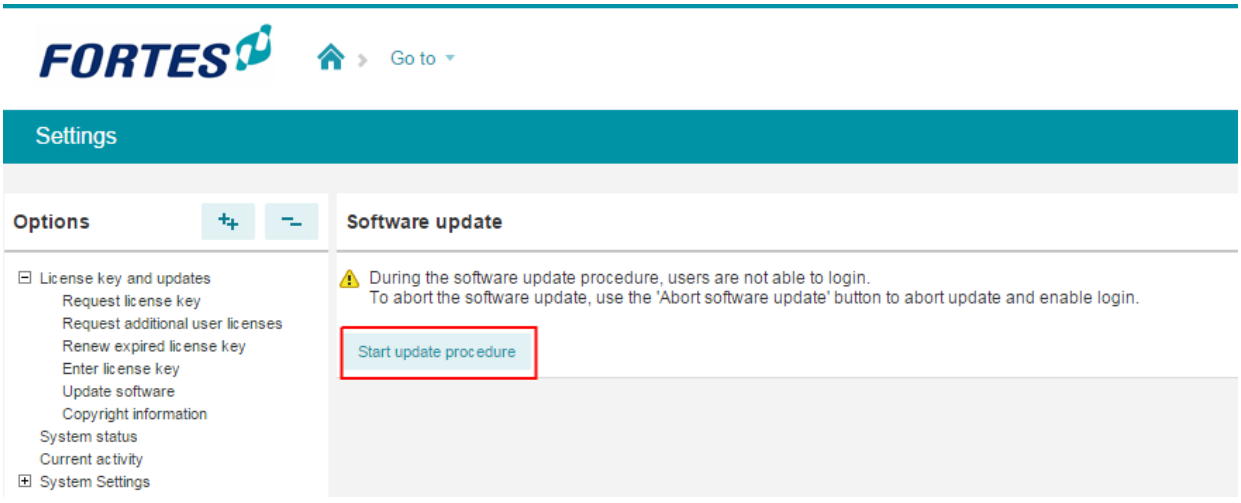
Remember: before starting the update we recommend to back up the database and application. Users should be informed of the update and should not be working on the system during the update.

Important: During the update, leave your browser open!

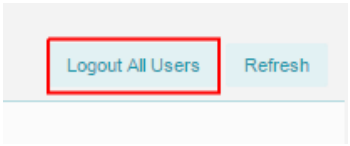
Steps to update the Principal Toolbox:



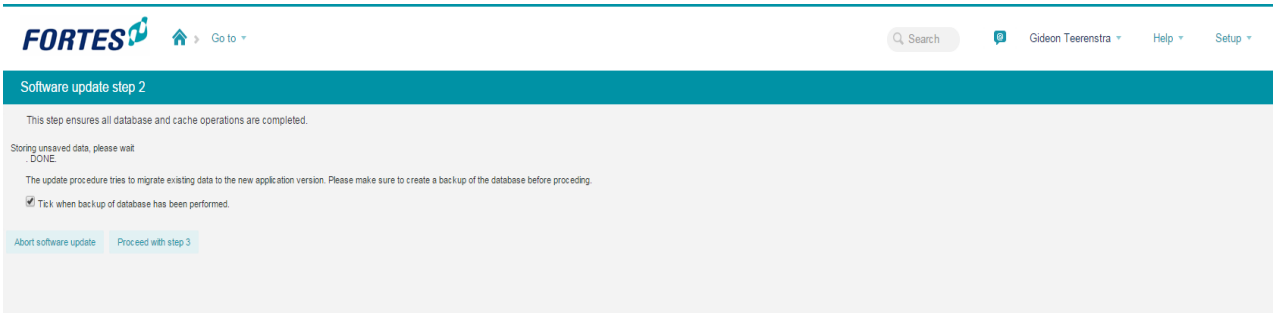
Click Update in the dropdown setup menu



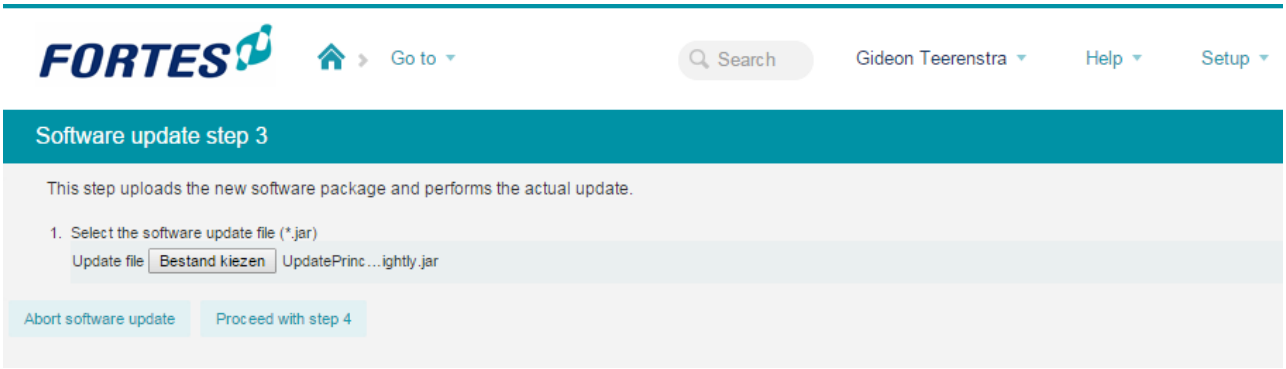
Start the update procedure by clicking the Start update procedure button.



Logout all active users by clicking the button Logout behind the users. Click on the button Proceed with step 2 to proceed with the update procedure when there is no current activity yet.
Tip: All users can be logged out once, by clicking the button Logout All Users.



The Principal Toolbox stored all unsaved data from cache to the database. Tick the checkbox when you are sure there is an database backup. Now click the button Proceed with step 2 to proceed.



Locate the appropriate file (.jar file) using the Browse key. Click the Proceed with step 4 key in order to carry out the update.

After the restart, log in as administrator and wait for eventual update processes and the sanity check to finish. This can take time depending on the update and the size of the database. The system is ready for use after completion of the update processes and the sanity check.

By possible problems or fault announcements you will need to contact Fortes Solutions: support@fortes.nl.