

Quick Installation Guide secRT

Content

1 FIRST STEPS 3

2 INSTALLATION 3

3 ADMINCONSOLE 4

3.1 Initial Login 4

 3.1.1 Derby Configuration.....5

 3.1.2 Password Change.....6

3.2 Logout 6

1 First Steps

It is recommended to download the Java JDK package (depending on system 32 bit or 64 bit version). Please make sure that the environment variable (Control Panel > System > Advanced > Environment Variables > System variables) **JAVA_HOME** is set to the correct JDK installation path, e.g. **[PATH]\Java\jdk1.7.0_21**. This should have been done automatically when using the Java JDK installer.

To install and run the secRT, you first need to apply the Java Cryptography Extension. This extension allows Java to use high encryption algorithms. Without the patch, secRT will not operate successfully

You can download the extension from

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

Please make sure to download the correct version. You need to download the extension for the corresponding Java version, e.g. Java 7.

Copy the files from the extension package to the following locations; adapt the installation path to your actual Java JDK installation.

- [Path]\Java\jdk1.7.0_21\jre\lib\security
- [Path]\Java\jre7\lib\security

2 Installation

The deployment of the **secRT** depends on the used servlet engine. In the following example, the deployment for an Apache Tomcat Application Server is described.

If you are using the Apache Tomcat service installer, the CATALINA_HOME environment variable is set automatically. Otherwise, please set the CATALINA_HOME environment variable (Control Panel > System > Advanced > environment Variables > System variables) to your Tomcat installation (example: C :/ apache / tomcat).

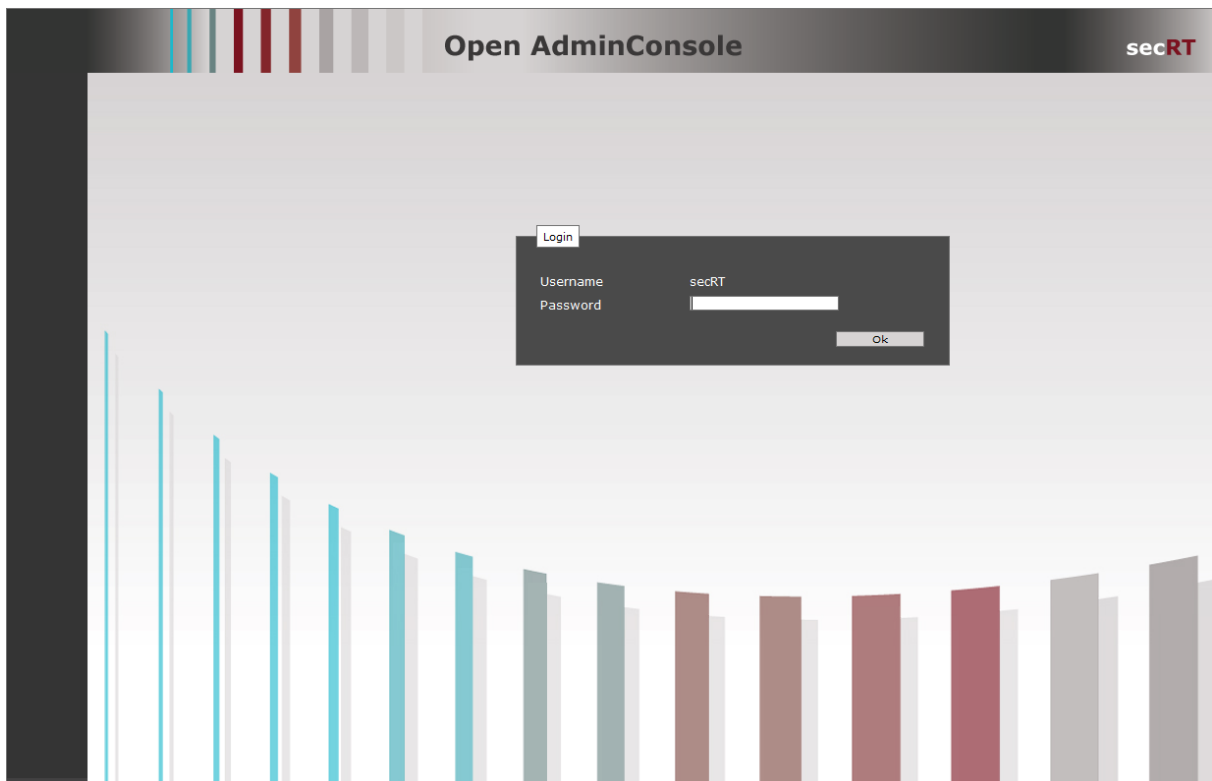
Rename the Web Application Archive (WAR) file, so that the name complies the required context path, e.g. **gateway.war**.

Stop the application server. For further instructions see the documentation of your Apache Tomcat Application Server installation.

Copy the file into the **webapps** directory of the Application Server.

Start the Application Server and wait until the gateway is deployed.

3 AdminConsole



According to the name you choose for the Web Application Archive (in our example **gateway.war**), the secRT will be accessible under the following address in your browser (we recommend Firefox from version 20 or Microsoft Internet Explorer from version 8) available::

[http://\[IP-Address\]:\[Port\]/gateway](http://[IP-Address]:[Port]/gateway)

3.1 Initial Login

To configure the secRT, you will have to login at the AdminConsole. Open the AdminConsole login page in the browser. When initially installed, the username and password are predefined to the following default values:

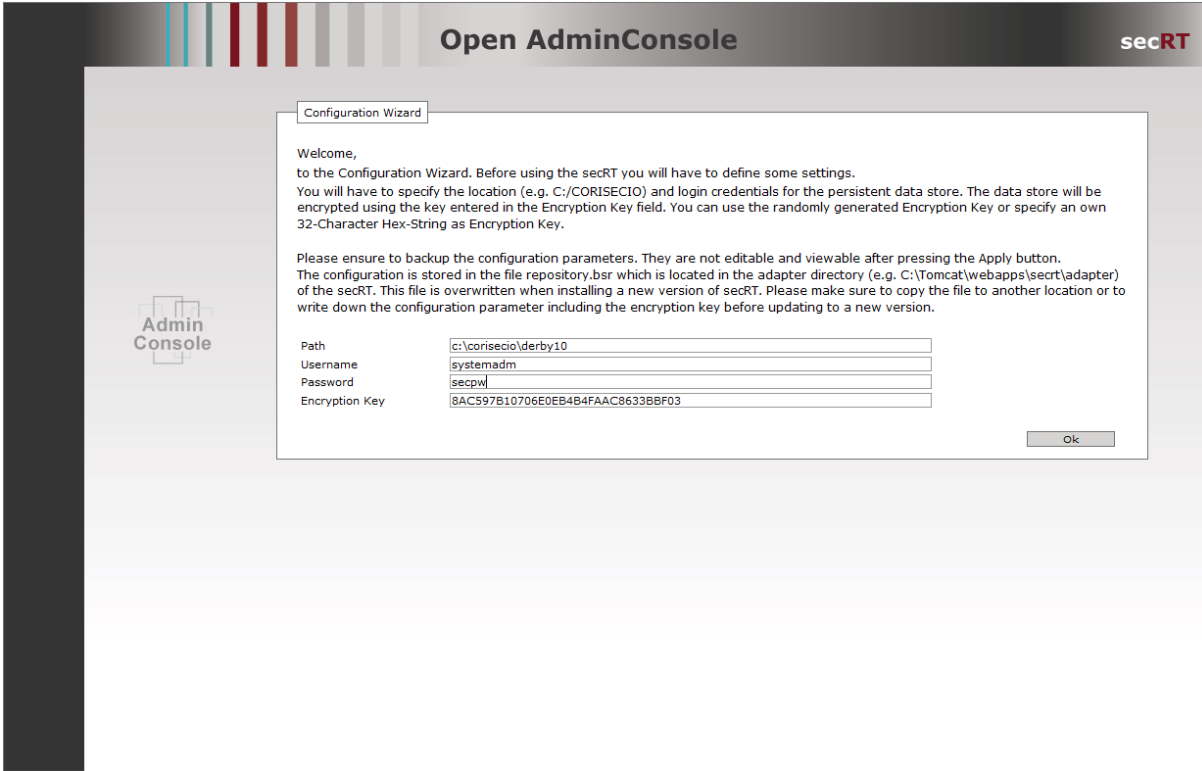
Username: secRT

Password: secRT

After a successful login, you need to configure the derby database.

3.1.1 Derby Configuration

All settings of the secRT are stored in an internal Derby database (the Derby libraries are included in the secRT). After the initial login, you will be prompted to setup the database. Follow the instructions on the screen.



The screenshot shows the 'Open AdminConsole' window with the 'Configuration Wizard' dialog box open. The dialog box contains the following text and fields:

Configuration Wizard

Welcome,
to the Configuration Wizard. Before using the secRT you will have to define some settings.
You will have to specify the location (e.g. C:/CORISECIO) and login credentials for the persistent data store. The data store will be encrypted using the key entered in the Encryption Key field. You can use the randomly generated Encryption Key or specify an own 32-Character Hex-String as Encryption Key.

Please ensure to backup the configuration parameters. They are not editable and viewable after pressing the Apply button.
The configuration is stored in the file repository.bsr which is located in the adapter directory (e.g. C:\Tomcat\webapps\secrt\adapter) of the secRT. This file is overwritten when installing a new version of secRT. Please make sure to copy the file to another location or to write down the configuration parameter including the encryption key before updating to a new version.

Path: c:\corisecio\derby10
Username: systemadm
Password: secpw
Encryption Key: 8AC597B10706E0EB4B4FAAC8633BBF03

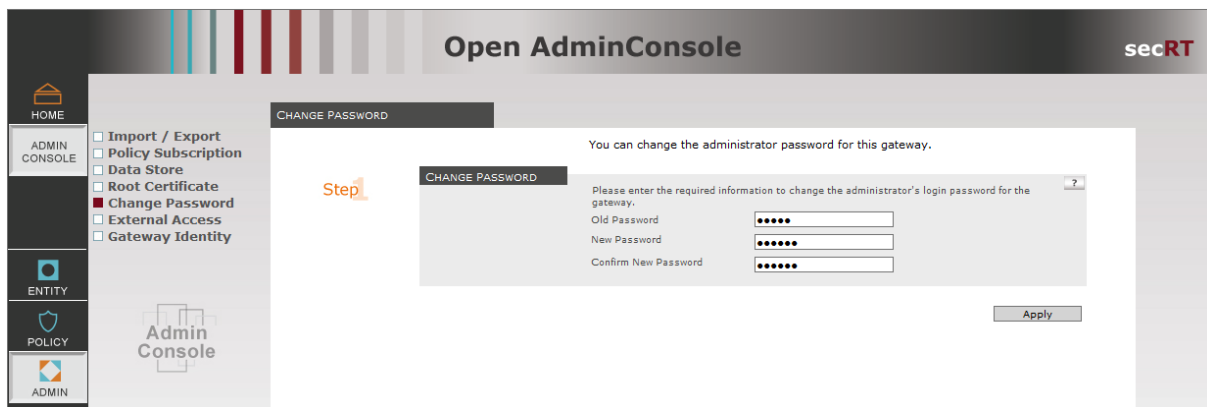
Ok

The **path** of the Derby database can be set absolute or relative. If you define a relative path, the derby database will be created in the execution directory of your Application Server installation. Make sure that you have write access to the Derby destination.

Next, please enter a username and password. The Encryption Key is a randomly generated hex value. You can accept these randomly generated encryption key or enter your own 32-digit hex value.

3.1.2 Password Change

The password can be changed to your choice. It is strongly recommended to change immediately the default password. Please click on **Admin Console / Admin** and select **Change Password**.



Set the new password and click **OK**. After you logged out of the secRT, the new password is active. You will need it to login to the console next time.

3.2 Logout

With Logout you will leave the AdminConsole administration GUI. The web application keeps running. Do not forget to leave the web application via **Logout**, to avoid the AdminConsole usage by unauthorized persons.