ADOIT Connect for Power BI

Version 3.0

Contents

1. Scenario Overview

The ADOIT Connect for Power BI scenario enables a connection between the data stored in ADOIT and Power BI.

Note: This document focuses on the integration with ADOIT. Integration with ADONIS and ADOGRC is also possible.

The current version of the module supports the following features:

- **Quick start with the predefined template:** Use the predefined dashboard to visualize your key EAM data in Power BI. By inserting your URL, the dashboard will automatically be updated with your data from ADOIT.
- **Reports:** It is possible to embed your Power BI dashboard in MS Teams or MS PowerPoint to keep your colleagues in the loop of the current state of your Enterprise Architecture Portfolio.
- **Real-time Synchronization:** View your ADOIT data in real-time in Power BI by synchronizing your dashboard or configure the dashboard to update itself at certain intervals.
- **Personalize your dashboard:** Change the colors, content and shapes of your graphic presentations quickly and easily by leveraging the data from your ADOIT repository without coding.

The following image shows one page of the predefined template in Power BI containing data retrieved from ADOIT:
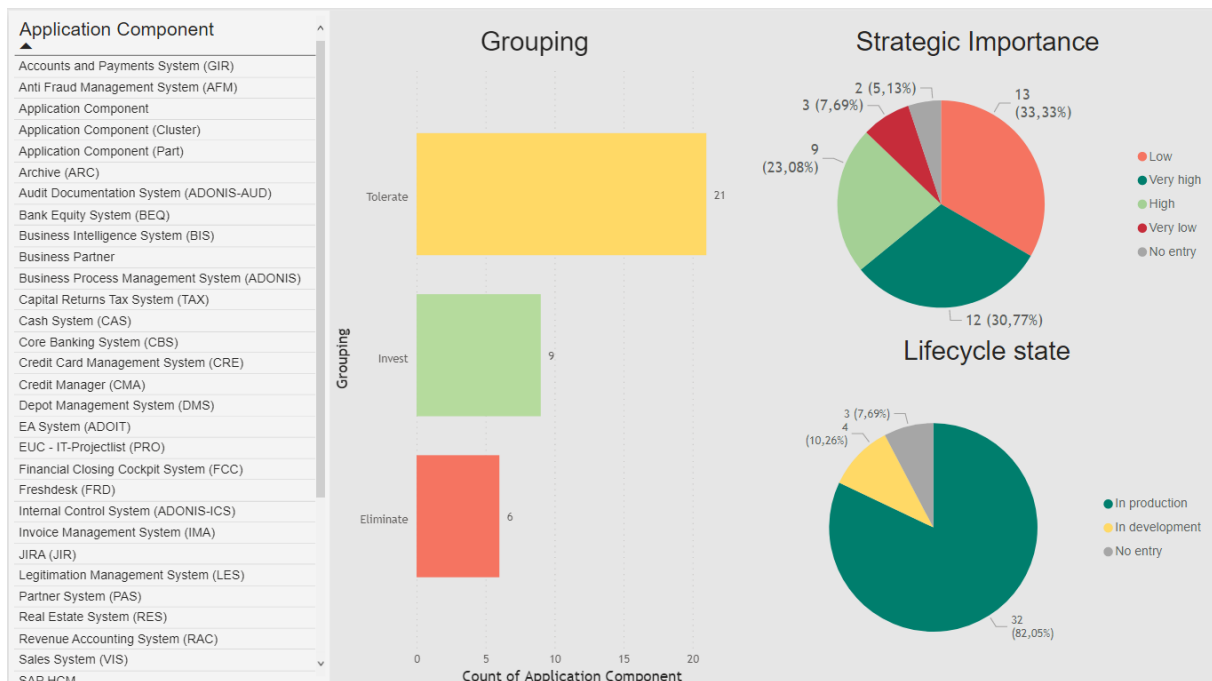

Figure 1: Dashboard in Power BI showing Groupings of Application Components in ADOIT.

2. Architecture

The connection between ADOIT and Power BI is realized through the usage of the ADOIT Standard REST API. Power BI needs the BASE URL of the ADOIT version that the user is currently using. How this is done will be demonstrated in the next chapter.

3. Setup

3.1 Prerequisites

ADOIT 12.0 or higher and Power BI Desktop 2.9 or higher must be installed.

However, the following description is done by using ADOIT 15.0.

Note: If you use an older version than ADOIT 15.0, please go to Chapter 6 after completing step 3 of chapter 3.2.

3.2 Unlock Basic Authentication in Administration Toolkit

1. Library Management

To access the ADOIT data in Power BI, Basic Authentication must first be allowed in the Administration Toolkit. In order to do this, open Administration Toolkit and click on the "Library Management" menu. Then click on "Component Settings" and expand the list of Component Settings by clicking on the plus sign. Further, open "Standard RESTful services" and double-click on "General".
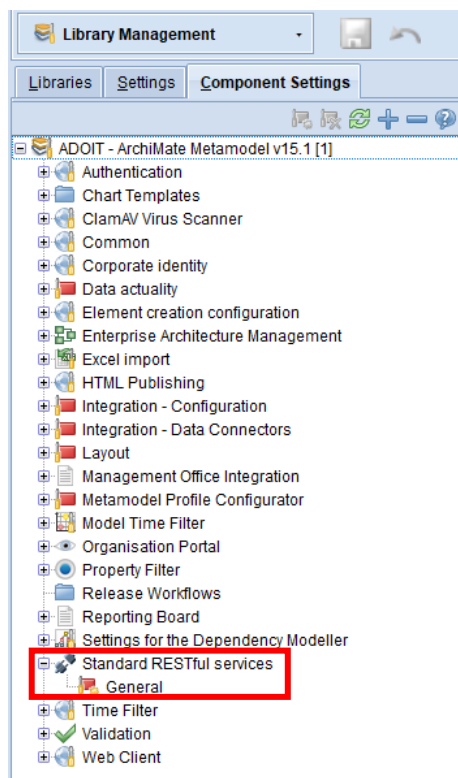

Figure 2: Open Standard RESTful services in ATK.

2. Enable MFB REST globally

Now, you have to enable Standard RESTful Services globally in the "Token" tab to use the authenticated REST API. Nothing else has to be done in the "Token" tab.
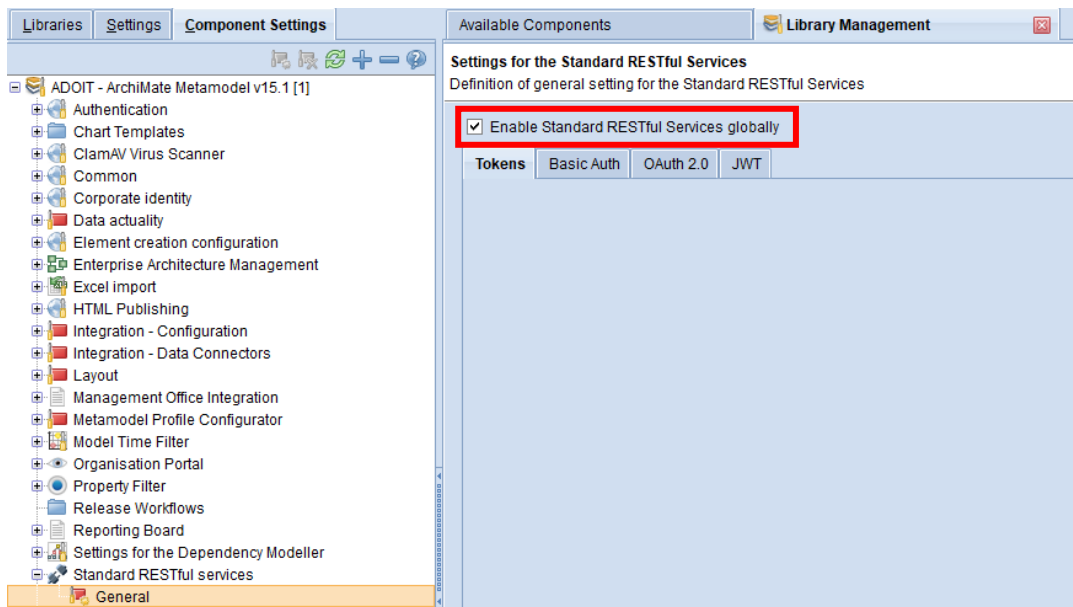

Figure 3: Enable Standard RESTful services.

3. Configure Settings for Basic Authentication

Now switch to the next tab "Basic Auth" and make sure that basic authentication is enabled. Further, enable all repository scenarios as shown in Figure 4. After checking all scenarios click on "OK" to save your changes. Make sure to **restart the Application Server** before you open ADOIT in the Web Client for the next step.
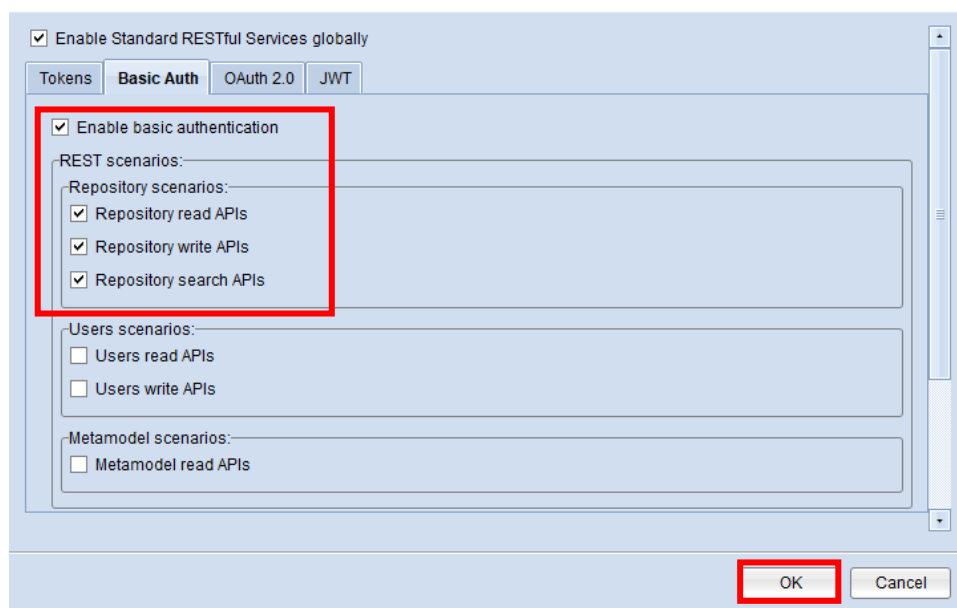

Figure 4: Enable Basic Authentication.

4. Enable Basic Authentication for ADOIT

Basic Authentication is turned off by default in ADOIT. If you want to use the REST API with Basic Authentication, you need to adapt the "Security settings" on the Admin Page. To open the Admin Page open a web browser and navigate to the BASE URL of your respective ADOIT installation, which could look as follows: "http://<SERVER_NAME>:<TOMCAT_PORT>/ADOIT15_0/admin.view".

Note: This example uses ADOIT 15.0, please use your ADOIT version which should be 15.0 or higher for this configuration. Also, to use the Admin Page, the user must have access rights to the Administration Toolkit.

Next, enter your credentials (if needed) and log in. Once you are logged in, click on the three dots (…) on the top left corner and **click on** "Authentication".
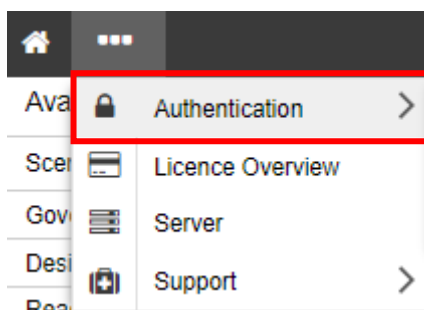

Figure 5: Admin View in ADOIT

You will be lead to a new site, where you can configure your authentication settings. Click on the "Security settings" button.
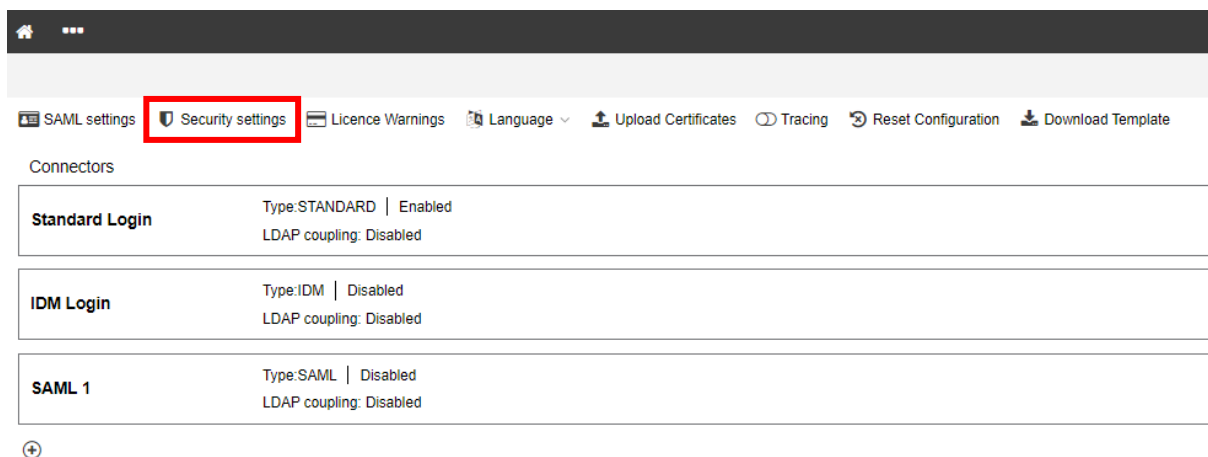

Figure 6: Open Security settings.

A new window will pop up with JSON code. You only have to allow basic authentication for all IP addresses by putting "allow all" between the brackets. Search for the keyword "rest". The code in the security settings should look like this after editing:
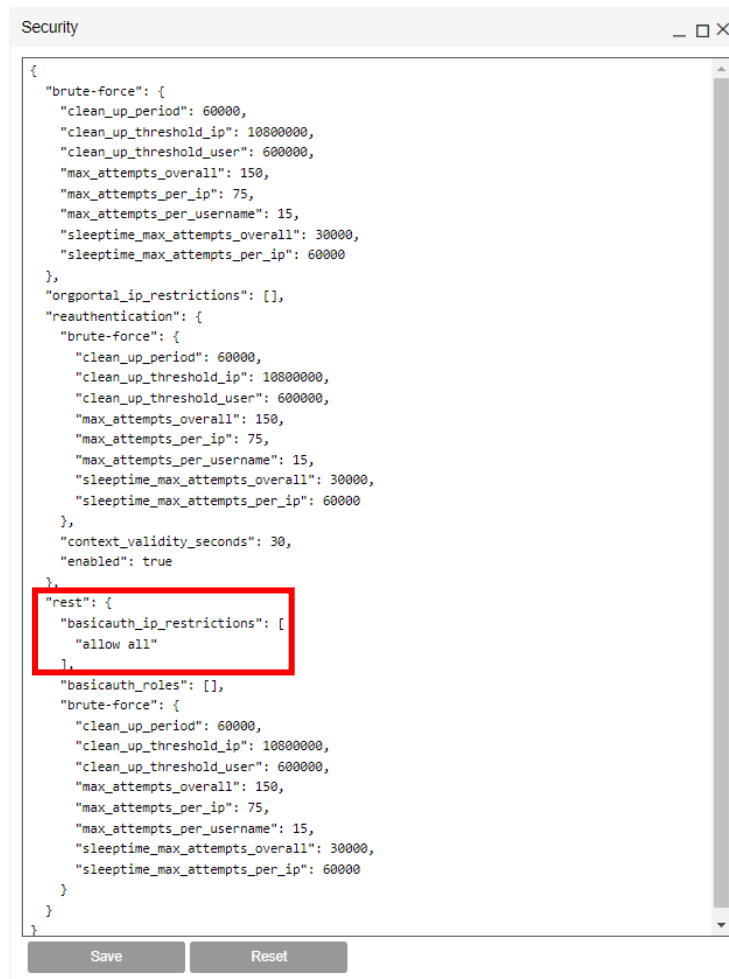
Figure 7: Allow Basic Authentication as Admin.

After saving your changes in the JSON code, make sure to save your changes in the admin view before logging out.
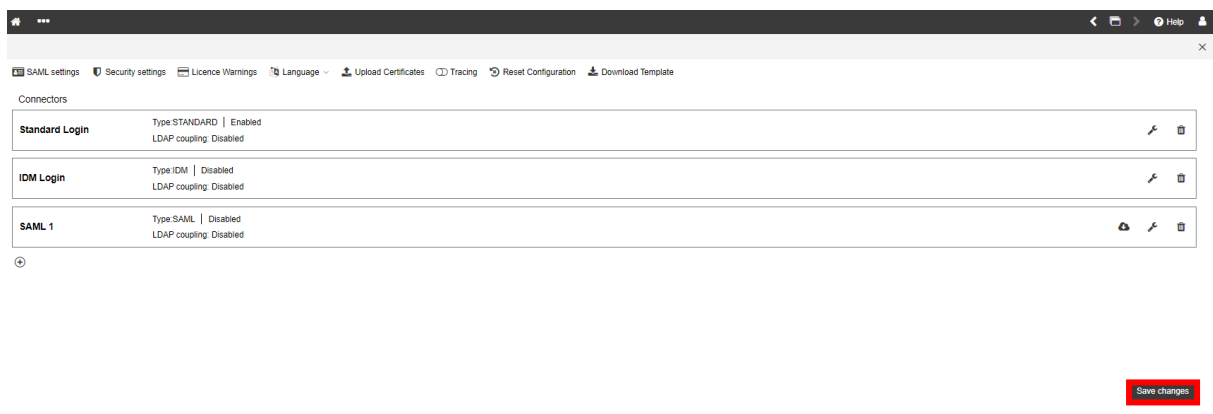

Figure 8: Save changes.

4. Test the ADOIT Connect for Power BI

Perform the following steps to test the ADOIT Connect for Power BI and fill the template with your EAM data.

1. Start the services for ADOIT and open ADOIT in the browser. Then copy the BASE URL of your ADOIT version.
   Example: If you are running the web client locally, the URL should look like this: "http://localhost:8000/ADOIT15_0"

2. Open the predefined template that you have received from us via e-mail. A window should pop up asking you to enter your BASE URL:
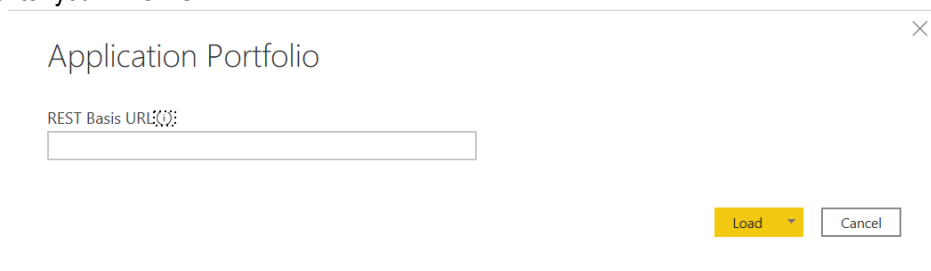

Figure 9: Rest Basis URL.

3. Then enter the URL you copied earlier and add /rest/2.0/ at the end.
   Example: "http://localhost:8000/ADOIT15_0/rest/2.0/".

   Note: Make sure that the ADOIT services are running, as Power BI pulls the ADOIT data directly from the ADOIT web client.

4. The data will not be able to load at first because you have to insert your ADOIT credentials to access the data in Power BI. A window will pop up, in which you have to switch to the "Basic" tab and enter your credentials.
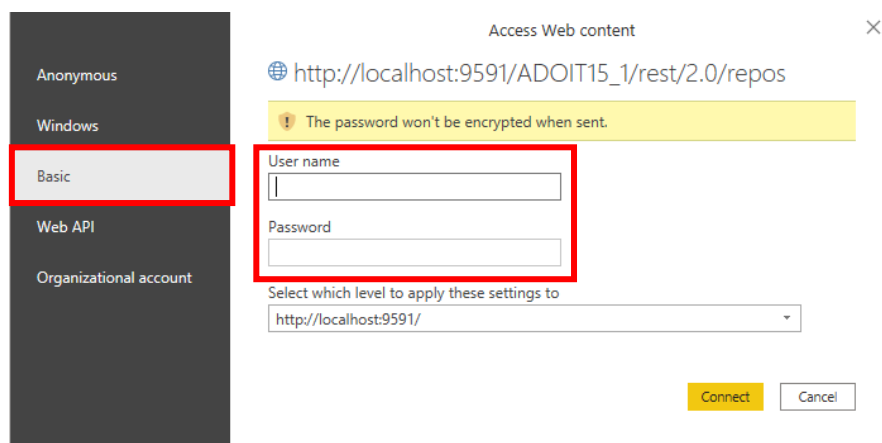

Figure 10: Enter ADOIT credentials in Power BI.

5. Once all these steps have been completed, the template should be filled with your data and your data will be visualized in Power BI.
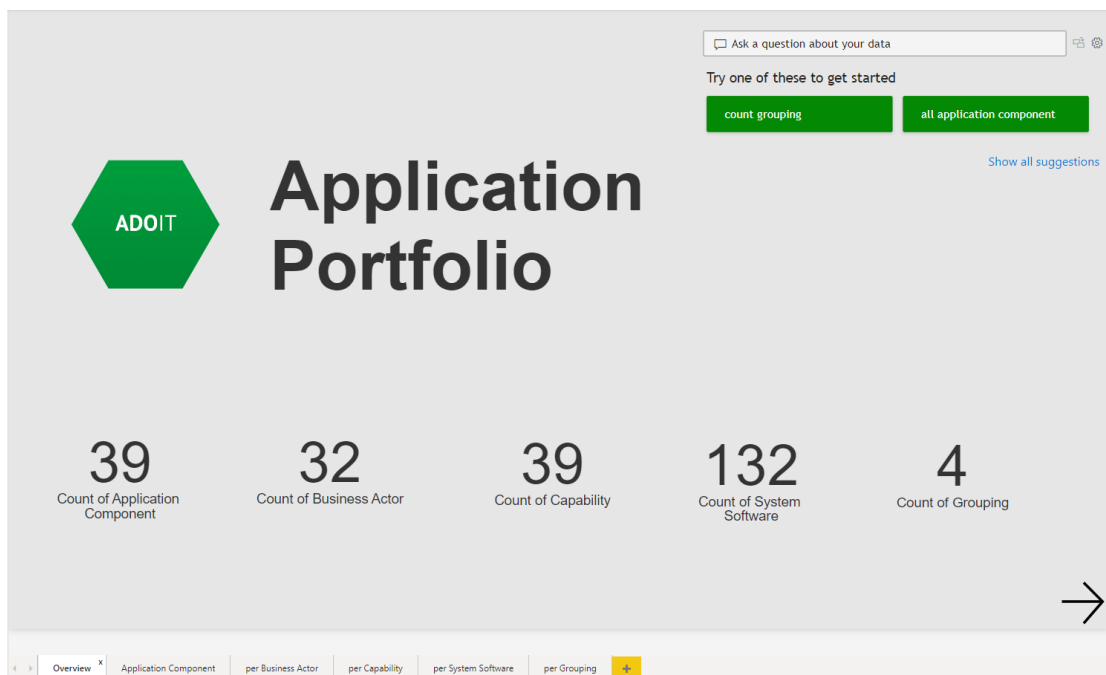
Figure 11: Power BI template with your ADOIT data.

5. Security

The fact that Basic Authentication has to be permitted for Power BI means that it is also generally enabled.

However, this should not cause any security problems, as the user's credentials as well as the repository and query ID are also required to gain access to the data

6. ADOIT 12.0 – 14.0

In ADOIT 12.0 – ADOIT 14.0 it is not possible to allow Basic Authentication in the Admin View of ADOIT. Step 4 in chapter 3.2 is therefore not to be executed. The rest remains the same. Instead of step 4, however, the following must be done:

Under the path webapps/<ADO>/WEB-INF/rest/RESTAuthorization.xml authentication must be allowed in the web application. To do this, one must remove the comments around <entry key="REST_BASIC_AUTHENTICATION">true</entry>. Open the file in a program where you can edit (e.g. Notepad). Then delete the comments as mentioned above.

The code should look this in the end:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Trusted RESTful callers with their secret key</comment>
<!-- True of the rest authentication secret is encrypted, otherwise false -->
<entry key="ENCRYPTED">true</entry>

<!-- The key and its secret.
If the ENCRYPTED flag is set to true then the secret must be encoded via ADOxx API ado.util.encrypt
(recommended). -->
<!--<entry key="%KEY%">%SECRET%</entry>-->

<entry key="REST_BASIC_AUTHENTICATION">true</entry>
</properties>
```

Make sure to restart the Web Server and the Application Server. After completing this step, you can continue by doing the steps described in chapter 4.