

# **Adabas Manager**

## **Configuration**

Version 8.5

October 2019

This document applies to Adabas Manager Version 8.5 and all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2014-2019 Software AG, Darmstadt, Germany and/or Software AG USA, Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA, Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <http://softwareag.com/licenses/> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third-Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

**Document ID: AMN-CONFIG-85-20210929**

## Table of Contents

1 About this Documentation .....	1
Document Conventions .....	2
Online Information and Support .....	2
Data Protection .....	3
2 Configuration .....	5
Adabas Manager Post-Installation Configuration .....	6
Adabas Manager and REST Server Configuration .....	7
Adabas Environment .....	13
File and Directory Browsing .....	14
Adabas Manager Communicator .....	17
Administering Internal Users in the InternalRepository File for Local Authentication .....	17



# 1

## About this Documentation

---

■ Document Conventions .....	2
■ Online Information and Support .....	2
■ Data Protection .....	3

## Document Conventions

---

Convention	Description
<b>Bold</b>	Identifies elements on a screen.
Monospace font	Identifies service names and locations in the format <i>folder.subfolder.service</i> , APIs, Java classes, methods, properties.
<i>Italic</i>	Identifies:  Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
Monospace font	Identifies:  Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the   symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

## Online Information and Support

---

### Software AG Documentation Website

You can find documentation on the Software AG Documentation website at <https://documentation.softwareag.com>.

### Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to [empower@softwareag.com](mailto:empower@softwareag.com) with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at <https://empower.softwareag.com/>.

You can find product information on the Software AG Empower Product Support website at <https://empower.softwareag.com>.

To submit feature/enhancement requests, get information about product availability, and download products, go to [Products](#).

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the [Knowledge Center](#).

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at [https://empower.softwareag.com/public\\_directory.aspx](https://empower.softwareag.com/public_directory.aspx) and give us a call.

### **Software AG Tech Community**

You can find documentation and other technical information on the Software AG Tech Community website at <https://techcommunity.softwareag.com>. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

## **Data Protection**

---

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.





## 2 Configuration


---

■ Adabas Manager Post-Installation Configuration .....	6
■ Adabas Manager and REST Server Configuration .....	7
■ Adabas Environment .....	13
■ File and Directory Browsing .....	14
■ Adabas Manager Communicator .....	17
■ Administering Internal Users in the InternalRepository File for Local Authentication .....	17

## Adabas Manager Post-Installation Configuration

### ■ Required Post-Installation Configuration for Adabas Manager

#### Required Post-Installation Configuration for Adabas Manager

1. Click on the host configuration icon  on the top right corner of the Adabas Manager screen.
2. Click on the button **Add Host** on the Adabas Host Connections screen.

3.

### Add Host

Connection Name	<input type="text" value="Connection Name"/>
Hostname / IP	<input type="text" value="Hostname"/>
Port	<input type="text" value="Port Number"/>
Authentication Configuration	<p><input checked="" type="radio"/> Use Adabas Manager login credentials</p> <p><input type="radio"/> Use different login credentials, please specify username:</p> <div><input type="text" value="Username"/></div> <p><input checked="" type="checkbox"/> Enabled</p> <p><input type="checkbox"/> Secured Connection (via HTTPS)</p>

Enter the Connection Name, Host Name/IP and Port.

4. Select the Authentication Configuration.
5. Click on the **Add Host** button to add the new host connection to the Adabas REST server.

You can add as many host connections to the Adabas REST Server as you want, and enable only those you want to administer by setting the connection to 'Enabled' (default setting).

## Adabas Manager and REST Server Configuration

---

- [Login to the Adabas Manager](#)
- [Default Configuration of the Adabas REST Server After Installation](#)
- [Default Authentication Mode of the Adabas REST Server After Installation](#)
- [Port Number for Adabas Manager Host Connection to the Adabas REST Server](#)
- [Authentication Configuration for Adabas Manager Host Connection to the Adabas REST Server](#)
- [Configuring the REST Server to use Adabas Manager Login Credentials](#)
- [Configuring the Adabas REST Server to use Different Login Credentials](#)

### Login to the Adabas Manager

Adabas Manager accepts log-ins from the following:

- Operating system (e.g. Windows) local user
- LDAP domain user

If the username of local user and LDAP user are identical, then the local user credentials take precedence.

For further information about Adabas REST Server connection authentication using its default authentication mode, refer to *Adabas Rest Administration, Installation and First Steps* for the Adabas REST Server default login credentials.

### Default Configuration of the Adabas REST Server After Installation

The default configuration of the REST server can be found in *config.default.xml* file.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <!-- This is the standard Adabas Rest Server configuration file.
3  The main entry point is the RestServer tag.
4  Additional restriction of databases are defined by DatabaseAccess entry below. -->
5  <RestServer configWatcher="true" showDbId="true" statisticTimer="false">
6  <!-- Server tag defines various information of Adabas Client for Java Rest Server. -->
7  <Server>
8  <!-- Content attribute directory defines, where the static HTML files are taken from. -->
9  <Content directory="examples" />
10 <!-- Service tags define a service port number and type. Valid types are http, https and ws.
11 http - HTTP server
12 https - SSL/HTTP server
13
14 if the type https is chosen, the KeyStore and KeyPassword tags are needed to define the SSL
15 certificate and corresponding password, if needed.
16 -->
17 <Service port="8190" type="http" />
18 <Service port="8191" type="https">
19 <KeyStore file="keys/keystore.jks" />
20 <KeyPassword password="test123" />
21 </Service>
22 <!-- The LoginService tag describe the chosen authentication method. Valid types are
23 jaas - Java JAAS authentication is chosen.
24 A standard "Adabas" JAAS configuration is provided for authentication.
25 The realm.properties file is needed containing user and password
26 information.
27 If no module is given, standard JAAS local authentication is choosen.
28 saf - The credentials are pass through to Adabas SAF enabled databases.
29 readonly - Only Read-Only access is granted. No modification are possible. Authentication is not checked.
30 -->
31 <LoginService class="" type="jaas" module="Adabas" />
32 <!-- To shutdown the client need a server password initiating the shutdown. -->
33 <Shutdown passCode="test123" />

```

Extensible Markup Language file      length: 2,098   lines: 41      Ln: 1   Col: 1   Sel: 0 | 0      Windows (CR LF)   UTF-8   INS

## Default Authentication Mode of the Adabas REST Server After Installation

Adabas REST Server uses Java JAAS with the standard "Adabas" configuration as its default authentication mode (see the XML tag `<LoginService . . .>` in the `config.xml` file located in the Adabas REST Server installation configuration directory). By default it is `<LoginService class="" module="Adabas" type="jaas" />`. It authenticates the Adabas REST Server login credentials (including the Adabas REST Server post-installation default login credentials) contained in the `realm.properties` file located in the same Adabas REST Server installation configuration directory. The authentication mode can be changed by adapting the server module of the `<LoginService . . .>` in the `config.xml` file. Refer to *Adabas Rest Administration, Authentication* for further information.

```

14      SSL certificate and corresponding password, if needed. -->
15      <Service port="8190" type="http"/>
16      <Service port="8191" type="https">
17          <KeyStore file="keys/keystore.jks"/>
18          <KeyPassword password="test123"/>
19      </Service>
20      <!-- The LoginService tag describe the chosen authentication method. Valid
21          types are jaas - Java JAAS authentication is chosen. A standard "Adabas"
22          JAAS configuration is provided for authentication. The realm.properties file
23          is needed containing user and password information. If no module is given,
24          standard JAAS local authentication is choosen. saf - The credentials are
25          pass through to Adabas SAF enabled databases. readonly - Only Read-Only access
26          is granted. No modification are possible. Authentication is not checked. -->
27      <LoginService class="" module="Adabas" type="jaas"/>
28      <!-- To shutdown the client need a server password initiating the shutdown. -->
29      <Shutdown passCode="test123"/>

```

## Port Number for Adabas Manager Host Connection to the Adabas REST Server

Use the Adabas REST Server default port (assigned during Adabas REST Server installation), which is port 8190 for connection via HTTP, or port 8191 for a secured connection via HTTPS. The port is evaluated in the *config.xml* file located in the Adabas REST Server installation configuration directory.

Select the **Secured Connection (via HTTPS)** check box if you want to use a secured connection via HTTPS to the Adabas REST Server.

### Add Host

Connection Name	<input type="text" value="SecuredHost"/>
Hostname / IP	<input type="text" value="ADAHOST1"/>
Port	<input type="text" value="8191"/>
Authentication Configuration	<input type="radio"/> Use Adabas Manager login credentials <input checked="" type="radio"/> Use different login credentials, please specify username: <input type="text" value="admin"/>
	<input checked="" type="checkbox"/> Enabled <input checked="" type="checkbox"/> Secured Connection (via HTTPS)
<input type="button" value="Add Host"/> <input type="button" value="Cancel"/>	

## Authentication Configuration for Adabas Manager Host Connection to the Adabas REST Server

Select the **Use Adabas Manager login credentials** radio button to connect to the Adabas REST Server using Adabas Manager credentials, otherwise select the **Use different login credentials, please specify user name** radio button and specify the user name to connect, using Adabas REST Server credentials and its default authentication mode.

Prerequisite: Adabas REST Server authentication and credentials configuration.


### Add Host

Connection Name	<input type="text" value="HumanResource"/>
Hostname / IP	<input type="text" value="ADAHOST1"/>
Port	<input type="text" value="8190"/>
Authentication Configuration	<input checked="" type="radio"/> Use Adabas Manager login credentials <input type="radio"/> Use different login credentials, please specify username: <input type="text" value="admin"/>
	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Secured Connection (via HTTPS)

## Configuring the REST Server to use Adabas Manager Login Credentials

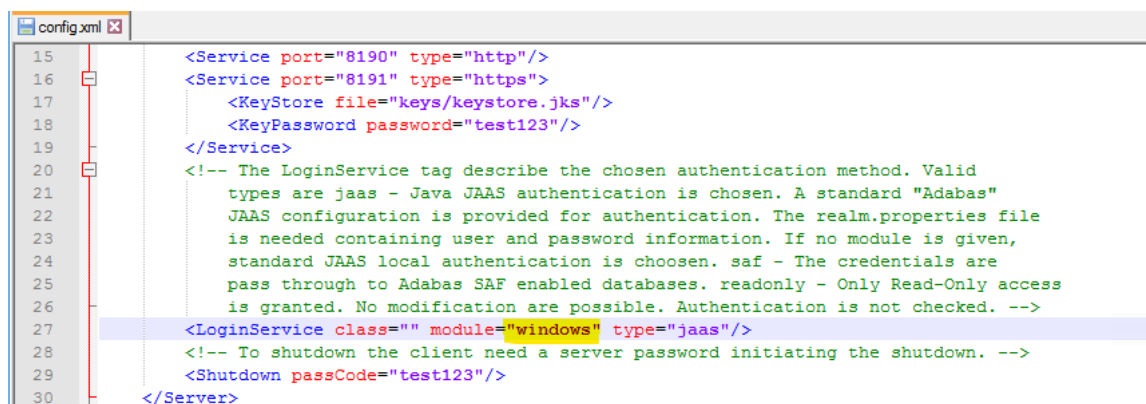
➤ To configure the REST server to use Adabas Manager login credentials:

- Follow the steps below if you select **Use Adabas Manager login credentials** and use LDAP domain user credentials:
  1. Go to the Adabas REST Server installation directory *<installation directory>\AdabasRestAdministration\configuration*.
  2. Open the file *config.xml* and search for the XML tag `<LoginService...>`.
  3. Edit the value of `module` to `module="windows"` (for Windows).



**Note:** The module name is case sensitive and must match the module name defined in the *security.conf* file located in the same directory

  4. Save the edited version of *config.xml*.



```

15 <Service port="8190" type="http"/>
16 <Service port="8191" type="https">
17   <KeyStore file="keys/keystore.jks"/>
18   <KeyPassword password="test123"/>
19 </Service>
20 <!-- The LoginService tag describe the chosen authentication method. Valid
21 types are jaas - Java JAAS authentication is chosen. A standard "Adabas"
22 JAAS configuration is provided for authentication. The realm.properties file
23 is needed containing user and password information. If no module is given,
24 standard JAAS local authentication is choosen. saf - The credentials are
25 pass through to Adabas SAF enabled databases. readonly - Only Read-Only access
26 is granted. No modification are possible. Authentication is not checked. -->
27 <LoginService class="" module="windows" type="jaas"/>
28 <!-- To shutdown the client need a server password initiating the shutdown. -->
29 <Shutdown passCode="test123"/>
30 </Server>

```

If you select **Use Adabas Manager login credentials** and use OS local user credentials, see [Configuring the Adabas REST Server to use Different Login Credentials](#)

If local and domain user names are identical, the local user name authentication takes precedence.

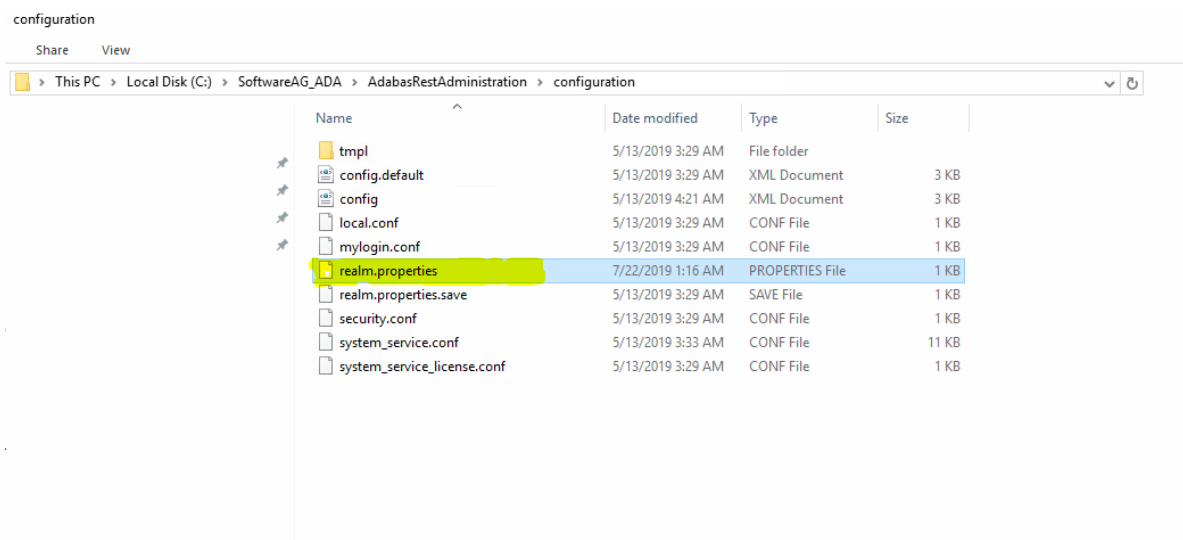
## Configuring the Adabas REST Server to use Different Login Credentials

➤ To configure the Adabas REST server to use different login credentials (other than its default login credentials and LDAP domain user)

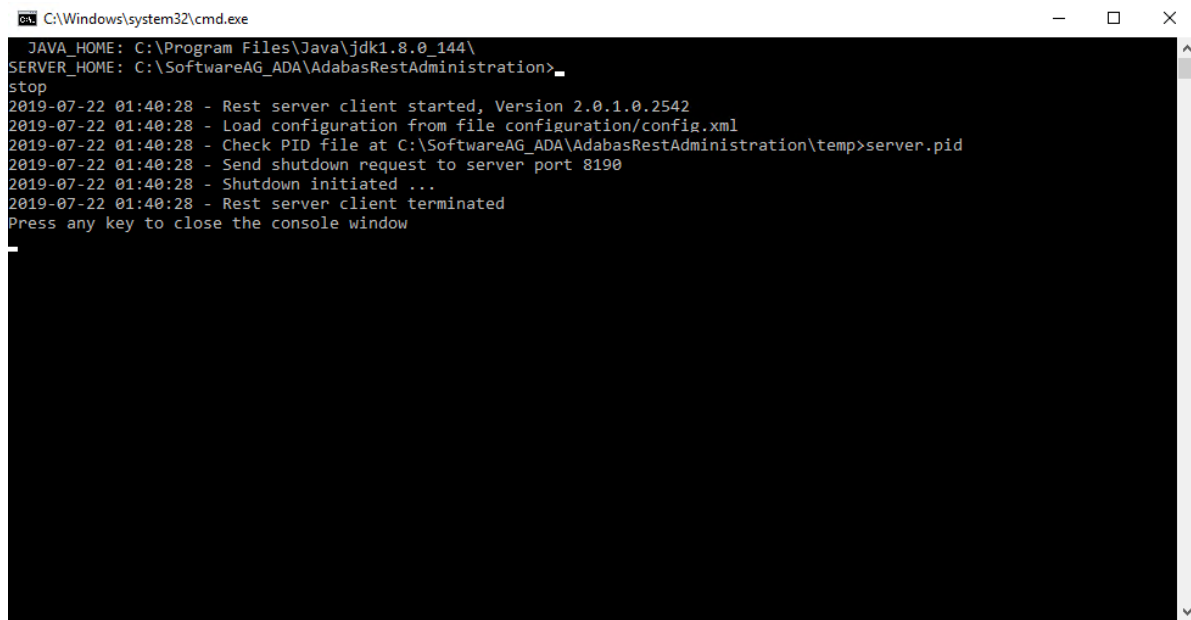
- 1 Go to the Adabas REST Server installation directory (*<installation directory>\AdabasRestAdministration\configuration*) and rename the file *realm.properties* to an arbitrary name.



**Note:** You can ignore this step if you want to keep the default post-installation user name and password. The new user name and password will be added as a new entry to the existing one.

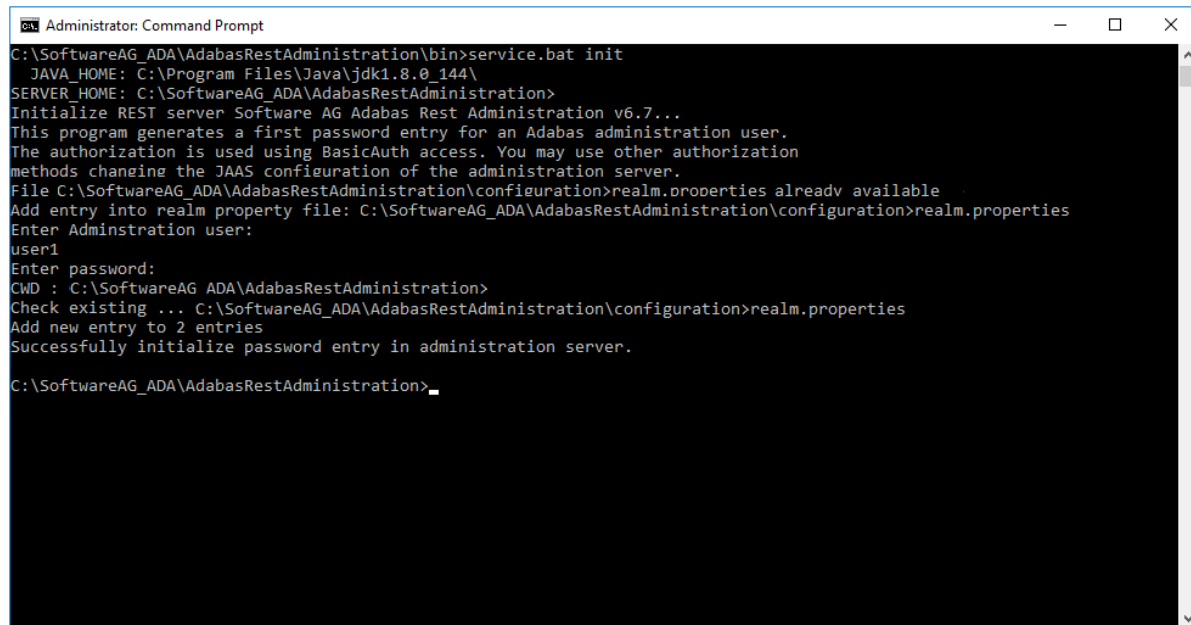


- 2 Stop the Adabas REST Server if it is running.



```
C:\Windows\system32\cmd.exe
JAVA_HOME: C:\Program Files\Java\jdk1.8.0_144\
SERVER_HOME: C:\SoftwareAG_ADA\AdabasRestAdministration>
stop
2019-07-22 01:40:28 - Rest server client started, Version 2.0.1.0.2542
2019-07-22 01:40:28 - Load configuration from file configuration/config.xml
2019-07-22 01:40:28 - Check PID file at C:\SoftwareAG_ADA\AdabasRestAdministration\temp>server.pid
2019-07-22 01:40:28 - Send shutdown request to server port 8190
2019-07-22 01:40:28 - Shutdown initiated ...
2019-07-22 01:40:28 - Rest server client terminated
Press any key to close the console window
```

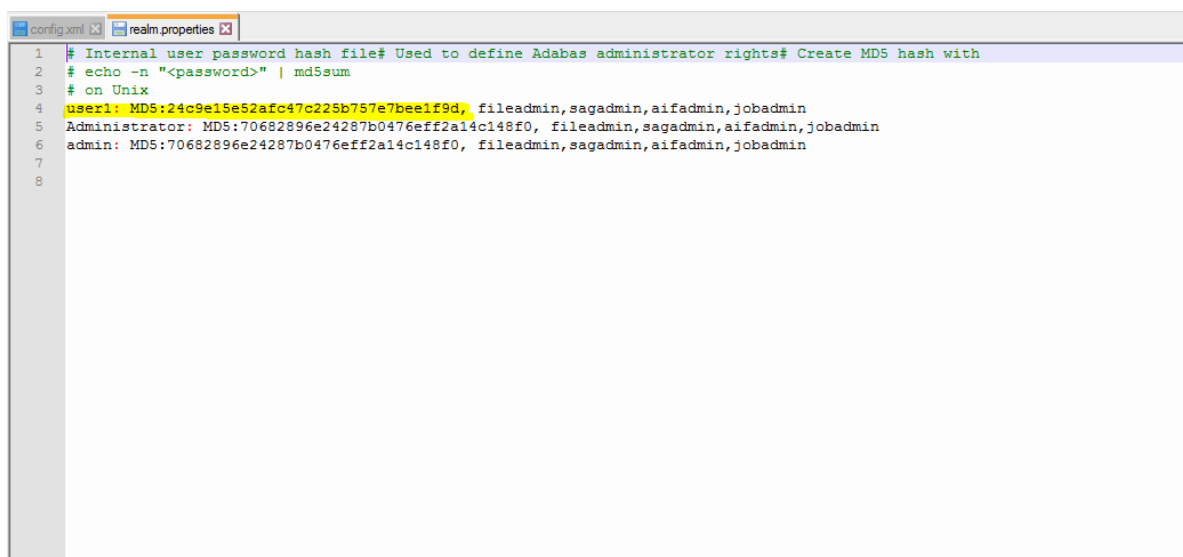
- 3 From the Adabas command prompt, go to the Adabas REST Server installation directory (*<installation directory>\AdabasRestAdministration\bin*) and run the command *service.bat init*. You will be prompted to Enter Administration user: enter the user name and password for that user.



```
Administrator: Command Prompt
C:\SoftwareAG_ADA\AdabasRestAdministration\bin>service.bat init
JAVA_HOME: C:\Program Files\Java\jdk1.8.0_144\
SERVER_HOME: C:\SoftwareAG_ADA\AdabasRestAdministration>
Initialize REST server Software AG Adabas Rest Administration v6.7...
This program generates a first password entry for an Adabas administration user.
The authorization is used using BasicAuth access. You may use other authorization
methods changing the JAAS configuration of the administration server.
File C:\SoftwareAG_ADA\AdabasRestAdministration\configuration>realm.properties already available
Add entry into realm property file: C:\SoftwareAG_ADA\AdabasRestAdministration\configuration>realm.properties
Enter Administration user:
user1
Enter password:
CWD : C:\SoftwareAG_ADA\AdabasRestAdministration>
Check existing ... C:\SoftwareAG_ADA\AdabasRestAdministration\configuration>realm.properties
Add new entry to 2 entries
Successfully initialize password entry in administration server.
C:\SoftwareAG_ADA\AdabasRestAdministration>
```



- 4 The user name and password are now set. Go back to the Adabas REST Server installation directory and check for a new *realm.properties* file. Your new user name should appear in the file.



```

1 # Internal user password hash file# Used to define Adabas administrator rights# Create MD5 hash with
2 # echo -n "<password>" | md5sum
3 # on Unix
4 user1: MDS:24c9e15e52afc47c225b757e7bee1f9d, fileadmin,sagadmin,aifadmin,jobadmin
5 Administrator: MDS:70682896e24287b0476eff2a14c148f0, fileadmin,sagadmin,aifadmin,jobadmin
6 admin: MDS:70682896e24287b0476eff2a14c148f0, fileadmin,sagadmin,aifadmin,jobadmin
7
8

```

- 5 Run the command *service.bat run* to restart the Adabas REST Server.

## Adabas Environment

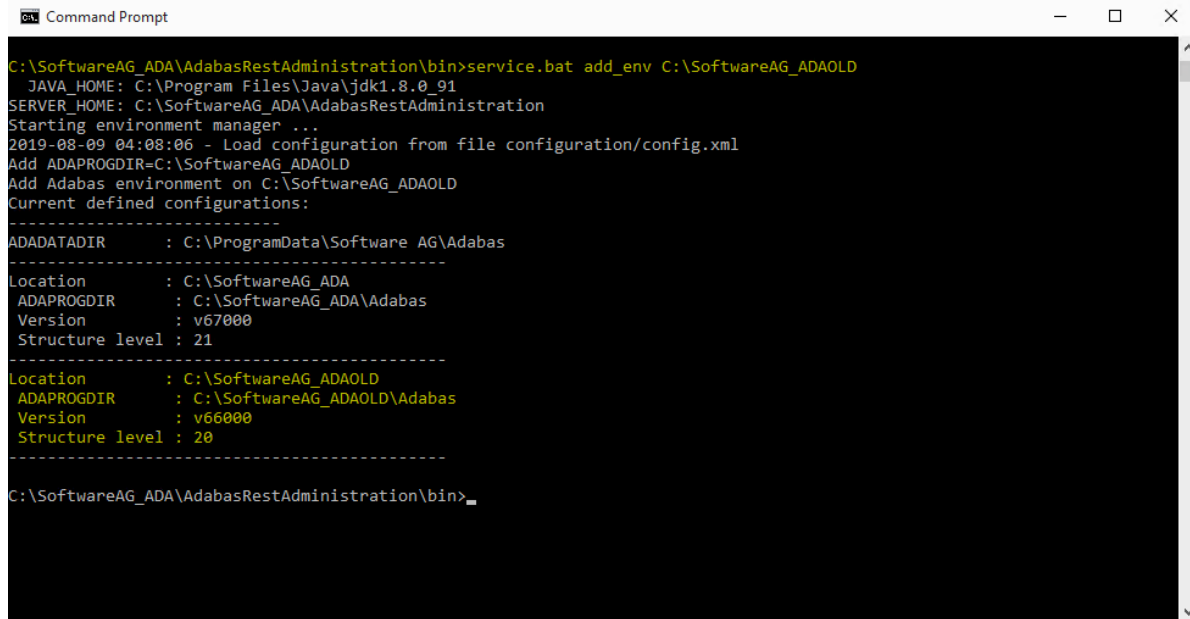
- [Configuring Adabas Manager and the Adabas REST Server to Allow the Administration of a Different Adabas Version in a Different Location](#)

### Configuring Adabas Manager and the Adabas REST Server to Allow the Administration of a Different Adabas Version in a Different Location

In the Adabas REST Server configuration file, the Adabas installation location (ADAPROGDIR) is set by default to the Adabas REST Server installation directory.

➤ To enable administration of a different Adabas version:

- 1 From an Adabas command prompt, set the Adabas environment by executing the command *service.bat add\_env <Adabas installation location>*.



```
Command Prompt
C:\SoftwareAG_ADA\AdabasRestAdministration\bin>service.bat add_env C:\SoftwareAG_ADAOLD
  JAVA_HOME: C:\Program Files\Java\jdk1.8.0_91
SERVER_HOME: C:\SoftwareAG_ADA\AdabasRestAdministration
Starting environment manager ...
2019-08-09 04:08:06 - Load configuration from file configuration/config.xml
Add ADAPROGDIR=C:\SoftwareAG_ADAOLD
Add Adabas environment on C:\SoftwareAG_ADAOLD
Current defined configurations:
-----
ADADATADIR      : C:\ProgramData\Software AG\Adabas
-----
Location        : C:\SoftwareAG_ADA
ADAPROGDIR      : C:\SoftwareAG_ADA\Adabas
Version         : v67000
Structure level : 21
-----
Location        : C:\SoftwareAG_ADAOLD
ADAPROGDIR      : C:\SoftwareAG_ADAOLD\Adabas
Version         : v66000
Structure level : 20
-----
C:\SoftwareAG_ADA\AdabasRestAdministration\bin>
```

- 2 To set the Adabas environment for lower Adabas version, use the latest Adabas REST Server installed for the current Adabas version.



**Note:** If the specified installation location does not have Adabas installed, the error message *EAI00013:Adabas environment path error* will be displayed, e.g. 'Error evaluating environment on C:\SoftwareAG\_ADA:EAI00013:Adabas environment path error for C:\SoftwareAG\_ADA\Adabas'

## File and Directory Browsing

### Browsing in Adabas Manager

By default, the browsing directory is set to `{ADADATADIR}`.

```

11      https - SSL/HTTP server
12
13      if the type https is chosen, the KeyStore and KeyPassword tags are needed to define the SSL
14      certificate and corresponding password, if needed.
15      -->
16      <Service port="8190" type="http"/>
17      <Service port="8191" type="https">
18          <KeyStore file="keys/keystore.jks"/>
19          <KeyPassword password="test123"/>
20      </Service>
21      <!-- The LoginService tag describe the chosen authentication method. Valid types are
22      jaas - Java JAAS authentication is chosen.
23          A standard "Adabas" JAAS configuration is provided for authentication.
24          The realm.properties file is needed containing user and password
25          information.
26          If no module is given, standard JAAS local authentication is choosen.
27      saf - The credentials are pass through to Adabas SAF enabled databases.
28      readonly - Only Read-Only access is granted. No modification are possible. Authentication is not checked.
29      -->
30      <LoginService class="" module="windows" type="jaas"/>
31      <!-- To shutdown the client need a server password initiating the shutdown. -->
32      <Shutdown passCode="test123"/>
33  </Server>
34  <Directories role="fileadmin" use_role="false">
35      <Directory location="{ADADATADIR}" name="adadatadir"/>
36  </Directories>
37  <Admin role="aifadmin" use_role="false">
38      <Installation location="C:\SoftwareAGAMN841"/>
39      <Installation location="C:\softwareagada66"/>
40  </Admin>
41  </RestServer>
42

```

eXtensible Markup Language file      length: 2,218    lines: 42      Ln: 1    Col: 1    Sel: 0 | 0      Windows (CR LF)    UTF-8    INS

If you want to browse files on another location, e.g. local drive or network drive, add its directory location to the Adabas REST Server *config.xml* file.

```

11      https - SSL/HTTP server
12
13      if the type https is chosen, the KeyStore and KeyPassword tags are needed to define the SSL
14      certificate and corresponding password, if needed.
15      -->
16      <Service port="8190" type="http"/>
17      <Service port="8191" type="https">
18          <KeyStore file="keys/keystore.jks"/>
19          <KeyPassword password="test123"/>
20      </Service>
21      <!-- The LoginService tag describe the chosen authentication method. Valid types are
22      jaas - Java JAAS authentication is chosen.
23          A standard "Adabas" JAAS configuration is provided for authentication.
24          The realm.properties file is needed containing user and password
25          information.
26          If no module is given, standard JAAS local authentication is choosen.
27      saf - The credentials are pass through to Adabas SAF enabled databases.
28      readonly - Only Read-Only access is granted. No modification are possible. Authentication is not checked.
29      -->
30      <LoginService class="" module="windows" type="jaas"/>
31      <!-- To shutdown the client need a server password initiating the shutdown. -->
32      <Shutdown passCode="test123"/>
33  </Server>
34  <Directories role="fileadmin" use_role="false">
35      <Directory location="{ADADATADIR}" name="adadatadir"/>
36      <Directory location="C:\" name="C drive"/>
37      <Directory location="S:\" name="Network S drive"/>
38  </Directories>
39  <Admin role="aifadmin" use_role="false">
40      <Installation location="C:\SoftwareAGAMN841"/>
41      <Installation location="C:\softwareagada66"/>
42  </Admin>
43

```

eXtensible Markup Language file      length: 2,320    lines: 44      Ln: 34    Col: 52    Sel: 0 | 0      Windows (CR LF)    UTF-8    INS

Browsing local drive:

Select FDT file ✕

Host

MCIRJAM03 : 8190

Browse

C drive: C:\

Current Directory

C:\

+ Create New Directory

Name	Type	Size	Modified	Created
\$Recycle.Bin	Directory	0 KB	18-Jan-2017 14:04	14-Jul-2009 11:18
0000352254_nat83.xml	File	1 KB	19-Jul-2017 02:16	05-Sep-2018 13:29
304111	Directory	0 KB	23-May-2019 11:23	23-May-2019 11:22
ACI841.BIN	File	43 KB	23-Oct-2017 10:47	30-May-2019 13:07
ada66.xml	File	1 KB	16-Aug-2018 02:04	28-Sep-2018 09:52
ada67.xml	File	1 KB	23-Nov-2017 22:21	02-Jul-2018 11:58
Adabas	Directory	0 KB	11-Jul-2017 13:39	11-Jul-2017 13:39
AdabasDB	Directory	0 KB	10-Jul-2017 15:23	10-Jul-2017 15:23
angular-2-4-child-routes-and-				

File Name:

File Name

Select

## Browsing mapped network drive:

Select FDT file ✕

Host

MCIRJAM03 : 8190

Browse

Network S drive: S:\

Current Directory

S:\

+ Create New Directory

Name	Type	Size	Modified	Created
Apps	Directory	16 KB	08-Jan-2019 14:03	29-Mar-2012 10:59
Dept	Directory	4 KB	10-Nov-2016 13:10	29-Mar-2012 10:58
User	Directory	4 KB	25-Jul-2019 17:03	29-Mar-2012 10:58

File Name:

File Name

Select

## Adabas Manager Communicator

- [Configuring Adabas Manager Communicator to Administer Entire Net-Work](#)

### Configuring Adabas Manager Communicator to Administer Entire Net-Work

Adabas Manager Communicator disables CORS by default. CORS must be enabled in order for Adabas Manager to connect to and administer Entire Net-Work. Open the file *<Software AG Installation Folder>\AdabasManagerCommunicator\config\amc.properties* and change the following line from:

```
ENABLE_CORS=NO
```

to

```
ENABLE_CORS=YES
```

To allow all connections to Adabas Manager Communicator:

```
ALLOW_ORIGIN=*
```

To allow a specific Adabas Manager to connect:

```
ALLOW_ORIGIN=http://<host>:<port> (for example http://amn.com:8083)
```

Restart the Adabas Manager Communicator service after configuring the *amc.properties* file in order for the changes to take effect.

## Administering Internal Users in the InternalRepository File for Local Authentication

Besides logging into Adabas Manager using LDAP authentication, it is possible to create local user IDs and store them into a text file. This is useful for users of Adabas Manager who only want to test out Adabas Manager locally without connecting to the company network (LDAP).

➤ To create a *users.txt* file for local authentication:

- Create the *users.txt* file in *<install-dir>/AdabasManager/config* by executing the following command at *<install-dir>/common/bin*, where *<install-dir>* represents your Adabas Manager installation directory:

```
./internaluserrepo.sh -c -f ../../AdabasManager/config/users.txt -p mypassword ↵  
myusername
```

Or:

In a Windows environment, issue the following command at the Windows command prompt to create the authentication text file (*users.txt*):

```
internaluserrepo.bat -c -f ..\..\AdabasManager\config\users.txt -p mypassword ↵  
myusername
```

➤ **To add internal users to the InternalRepository file for local authentication:**

- To add internal users (e.g. *user1*) to the authentication text file (*users.txt*), issue the following command at the bash shell prompt:

```
sh /<install-dir>/common/bin/internaluserrepo.sh -f ↵  
/<install-dir>/AdabasManager/config/users.txt user1
```

Or:

In a Windows environment, issue the following command at the Windows command prompt to add internal users (e.g. *user1*) to the authentication text file (*users.txt*):

```
<install-dir>\common\bin\internaluserrepo.bat ↵  
-f <install-dir>\AdabasManager\config\users.txt user1
```

➤ **To list internal users in the InternalRepository file for local authentication:**

- To list internal users in the authentication text file, issue the following command at the bash shell prompt:

```
sh /<install-dir>/common/bin/internaluserrepo.sh -f ↵  
/<install-dir>/AdabasManager/config/users.txt -lu
```

Or:

In a Windows environment, issue the following command at the Windows command prompt to list internal users in the authentication text file (*users.txt*):

```
<install-dir>\common\bin\internaluserrepo.bat ↵  
-f <install-dir>\AdabasManager\config\users.txt -lu
```

➤ **To delete internal users from the InternalRepository file for local authentication:**

- To delete internal users (e.g. *user1*) from the authentication text file (*users.txt*), issue the following command at the bash shell prompt:

```
sh /<install-dir>/common/bin/internaluserrepo.sh -f ↵  
/<install-dir>/AdabasManager/config/users.txt -d user1
```

Or:

In a Windows environment, issue the following command at the Windows command prompt to delete internal users (e.g. *user1*) from the authentication text file (*users.txt*):

```
<install-dir>\common\bin\internaluserrepo.bat ↵  
-f <install-dir>\AdabasManager\config\users.txt -d user1
```

