Administration Intelligence AG

AI WEBLAUNCHER

Installation and Operation

Version: **1.3.1**
Project: **AI WEBLAUNCHER**
Date: February 21, 2024

Contents

0 Release Notes

The following table lists the software changes in relation to the individual versions of **AI WEB**LAUNCHER.

Version	Release Notes
1.0.3	• Initial release
1.0.4	• New code signature to avoid the Smartscreen defender warning message during the installation • Extension of operations manual
1.0.5	• Extension of operations manual
1.0.6	• An error report can be created if the application start fails • It is possible to change from connection with proxy to a direct connection to the application server • English is the default language if the language of the operating system is not supported or recognized
1.1.0	• Applications can be executed in DEBUG mode • Validation of code signature at application start
1.1.1	• Added MacOS notarization • Added server authentication • Added centralised distribution of ssl-certificates and proxy configurations • Previous java installation will be deleted properly at update
1.1.2	• Fixed a bug during installation on macOS • Backslashes can now be used properly inside usernames of the proxy configuration
1.1.3	• Validation of version at application start
1.1.4	• Connectivity check and download are using HTTP method GET • Proxy configuration prompt is now shown even on invalid or unknown HTTP status • Configuration file examples
1.1.5	• Certificates for SSL client authentication can be imported during installation • Identification of trusted SSL certificates changed to usage of key stores • The directory to download applications can now be defined administratively
1.1.6	• Presources have been deactivated and a signature check that cannot be carried out now aborts the loading process • The execution of patches was generally deactivated • The launch of applications in versioned mode has been disabled • Command line parameters for the Java VM are filtered • The executable files of the Java runtime environment of the client application are checked for authenticity at program start (SHA-256)

Version	Release Notes
1.1.7	• Client-Applications for the AI BIDDINGCOCKPIT are running again with Java 11 on MacOS • Possibility to only establich connection with predefined SSL-Certificates(mandatorycacerts.jks)
1.2.0	• Log4j update to Version 2.17.0
1.2.2	• Support for ARM technology under MacOS (M1 processors) • It is now no longer possible to circumvent mandatory SSL certificates by using the unencrypted HTTP protocol. When specifying mandatory SSL certificates, it is no longer possible for the client to circumvent this obligation by using system properties to provide different proxy settings. • The comparison of the Library hashing now occurs even if they are not downloaded again
1.2.2.1	• Properties for server communication are only mandatory in the start file (*.aiweblaunch) if mandatorycacerts exists
1.2.2.2	• Fixed a bug in the installer for macOS M1 (ARM)
1.3.0	• Download of the application from a third-party server is now prevented
1.3.1	• Switching from Zulu to OpenJDK and removing a separate M1 installer for macOS

1 Overview

AI WEBLAUNCHER is a modern solution based on open-source-components to start the products from Administration Intelligence AG in future. **AI WEB**LAUNCHER replaces Oracle's Java Webstart technology which will be thereby unnecessary to start the desktop applications from Administration Intelligence AG.

2 Installation

2.1 Installation with graphical user interface

An information message of Windows SmartScreen Defender may appear when starting the installation via the installation file. In case that the **AI WEB**LAUNCHER installation file is obtained from a secure source, the installation can be started by clicking at „Further Informations“ and „Continue to Execute“.

When using an administrator account you will be asked to start the installation program with administrator rights by the User Account Control. With a normal user account, the **AI WEB**LAUNCHER can only be installed into a directory with write permissions. This is normally the user home directory.

Figure 1: Start Screen of **AI WEB**LAUNCHER installation

In the second step of the **AI WEB**LAUNCHER installation, the license contract should be accepted to continue the installation.

Figure 2: License contract of **AI WEB**LAUNCHER installation

The next step consists in selecting the **AI WEB**LAUNCHER installation directory.

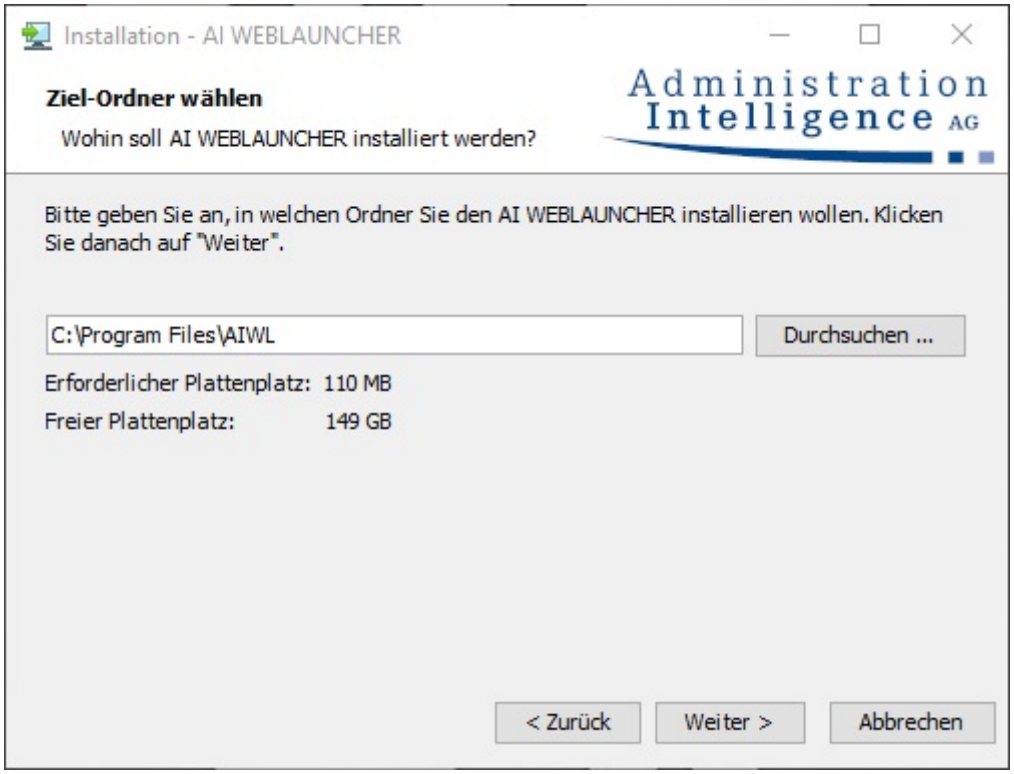

Figure 3: Selecting the **AI WEB**LAUNCHER installation directory.

AI WEBLAUNCHER will be installed into the indicated directory.

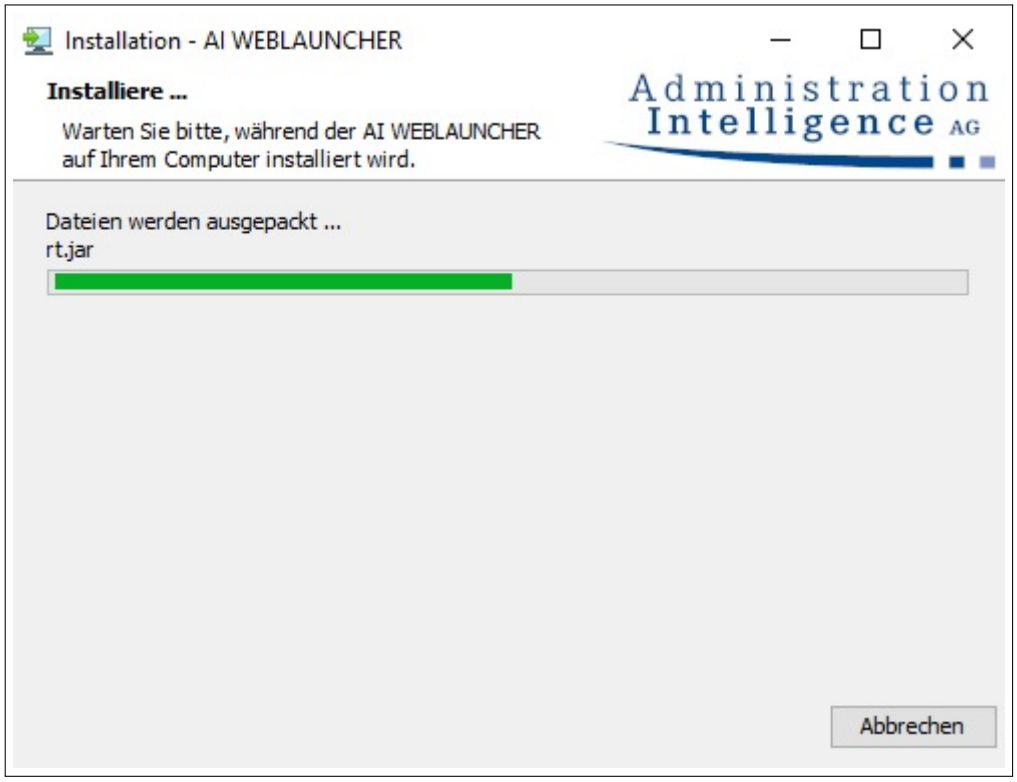

Figure 4: **AI WEB**LAUNCHER installation

Some servers demand a special certificate issued for the client to authenticate the **AI WEB**LAUNCHER. In the following steps, such client certificates can be imported into the key store to be used for authentication.

Figure 5: Usage of certificates issued for the client in **AI WEB**LAUNCHER

This step is only relevant when it was decided to use client certificates from the last step. On „skipping“ certificates back there this dialog will not be shown and the installation will omit this step.

On clicking „Search“ a file chooser dialog is opened to select the certificate for the file types **pfx**, **p12** or **jks**.

On clicking „Import“, the certificate is added to the certificate store.

In the lower part of the dialog, the content of the certificate store is shown. The presented steps can be done multiple times until the certificate store holds all certificates needed. Doing subsequent restarts of the installation, the certificate store can be extended anytime.

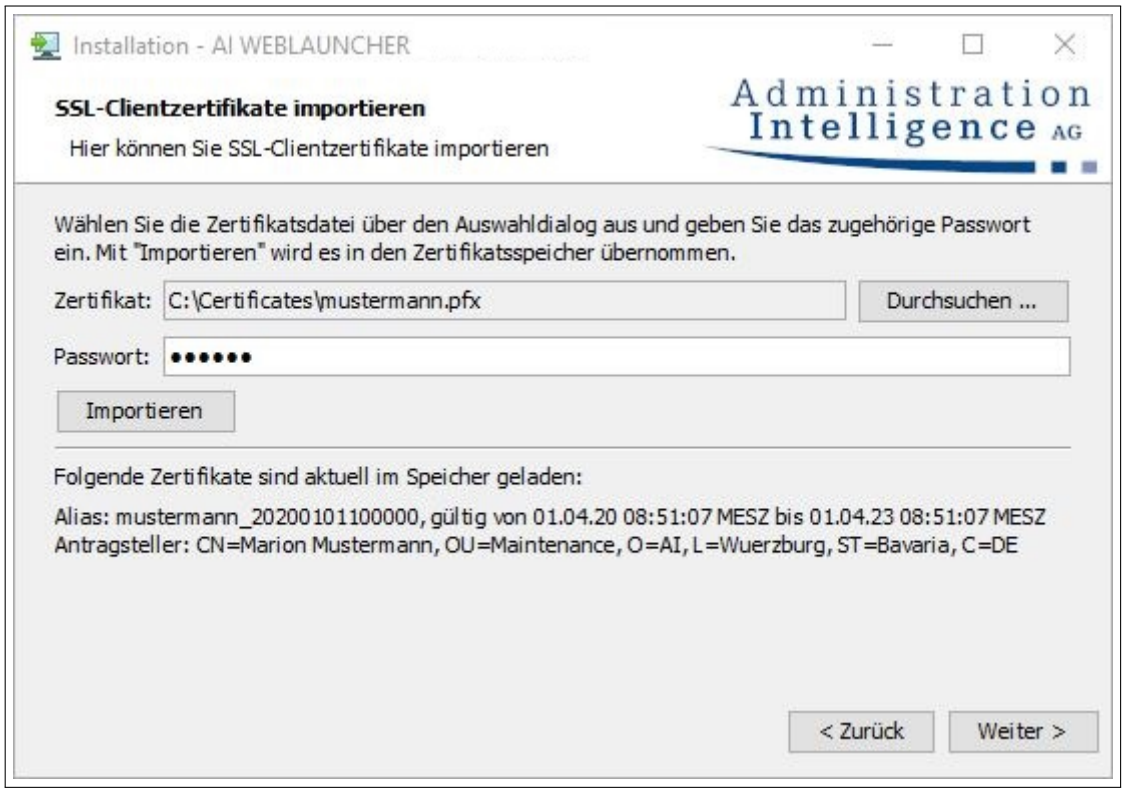

Figure 6: Import of client certificates in **AI WEB**LAUNCHER

The **AI WEB**LAUNCHER is now installed and you can start the required application.

Figure 7: Final Screen of **AI WEB**LAUNCHER installation

2.2 Installation without graphical user interface

AI WEBLAUNCHER can also be installed via command line without graphical user interface. Three different possibilities are supported. For the following examples a 64bit Windows installation is used.

2.2.1 Answering questions in the command line

Using the command `start /wait AI_WEBLAUNCHER64bit.exe -c` the **AI WEB**LAUNCHER installation can be started via the command line. Similar to the installation with graphical user interface, the entire questions have to be answered.

2.2.2 Configuration passed as parameter

Alternatively, the installation directory in which **AI WEB**LAUNCHER should be installed can be passed as a parameter to the installation file. The command for this is: *start /wait AI_WEBLAUNCHER64bit.exe -q -dir <Installationsverzeichnis>*

2.3 Starting the applications via AI WEBLAUNCHER

When the **AI WEB**LAUNCHER installation is completed, the client applications from Administration Intelligence AG can be started once. Therefore, the particular link must be clicked via web browser and then, the installation of the client application will be launched.

2.3.1 Mime-Type File Association

The **AI WEB**LAUNCHER installation generates a link to the Mime-Type `application/x-aiweblaunch` (file extension aiweblaunch), so that the files are automatically processed by **AI WEB**LAUNCHER.

2.3.2 File location

When the installation is completed and all pre-settings are confirmed, the application can be started. Depending on your operating system the components and user-specific settings will be downloaded to the specified location below.

Operating system	File location
Windows	%LOCALAPPDATA%\AI\PRODUCTNAME\HOSTNAME
Linux	user.home\AI\PRODUCTNAME\HOSTNAME
macOS	user.home\Library\AI\PRODUCTNAME\HOSTNAME

PRODUCTNAME and HOSTNAME are designed to be placeholders. PRODUCTNAME is to be replaced by e.g. **VM** for **AI TENDERING**MANAGER and **BCockpit** for **AI BIDDING**COCKPIT. HOSTNAME must be replaced by the server's URL.
Example for file location for **AI TENDERING**MANAGER:
C:\Users\jdoe\AppData\Local\AI\VM\www.vergabemanager.de\
Example for file location for **AI BIDDING**COCKPIT:
C:\Users\jdoe\AppData\Local\AI\BCockpit\www.vergabeplattform.ai-ag.de\

In special circumstances it may be necessary to define a different download directory. To do this, put the file „AI_WEBLAUNCHER.properties“ in the installation path of the **AI WEB**LAUNCHER using the following content:

```
application_dir=s:\download\%ENV_VARIABLE%\AI
```

A term enclosed in 2 percent signs stands for an environment variable. This will be replaced accordingly. Any number of environment variables can be used.
As indicated in the table, the corresponding subdirectories „\PRODUCTNAME\HOSTNAME“ are added by the **AI WEB**LAUNCHER.

User-specific settings, such as proxy information or persistently stored, trusted SSL certificates are not stored in the download directory specified under „application_dir“, but are still saved in the folders specified in the „File location“ table.

2.3.2.1 Log outputs

The log outputs of the program start can be found in the file „launcher.log“ in the application's file location. The location of the log outputs of the started client application remains unchanged.

2.3.2.2 Forcing a new download of the application

To force a re-download of the client application the files can be deleted in the file location (clearing the cache). **AI WEB**LAUNCHER will download automatically the required files from the application server again.

IMPORTANT: If proxy settings were made or SSL-certificates were permanently trusted, the files „proxy.txt“ (proxy settings) and „usercacerts.jks“ (permanently trusted SSL-certificates) must not be deleted!

2.3.3 Reading out the used version of AI WEBLAUNCHER

The used version of **AI WEB**LAUNCHER can be read out in the file „Systeminfo.html“ under „Program information“. This file is contained in the error report which can be generated in the client application.

In addition, the version number of the installed **AI WEB**LAUNCHER under Windows is displayed in the list of installed "Programs and Features" in the Control Panel.

2.3.4 Special circumstances under Windows

User Account Control

UAC describes best practices, location, values, Group Policy Management Console and security aspects for user account control. UAC increases the security in environments and is essential when working with administrative rights. It is crucial that administrative rights are only available after confirmation and cannot be used automatically. Furthermore, the UAC is ideally suited to limit rights for non-trusted processes within a user session. This applies especially to all processes that are communicating via the internet.

3 Network Structure and Security

3.1 Proxy Dialog

If it is not successful to set up an internet connection, a dialog window appears to enter the proxy configuration data. Please record the hostname or rather the IP address and the port of the proxy server. Along with the confirmation, these information will be remembered for subsequent starts.

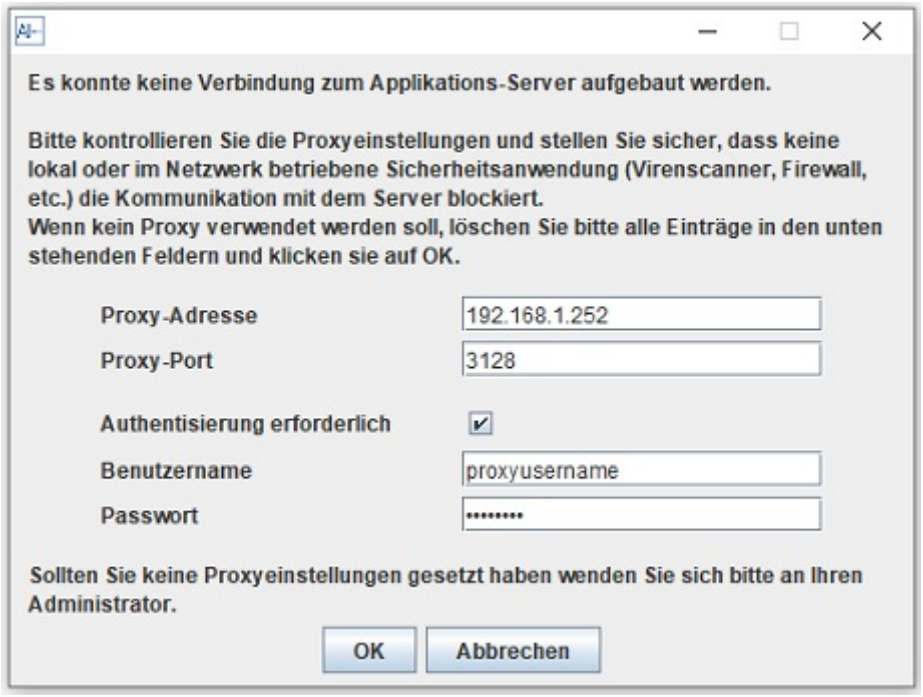

Figure 8: Proxy without authentication

If an authentication for the proxy is necessary, the corresponding check must be activated so that the user name and the password can be entered.

3.2 Server authentication dialog

If **AI WEB**LAUNCHER detects a server authentication request while communicating, the user will be asked for credentials.

This information will be persisted for future communications.

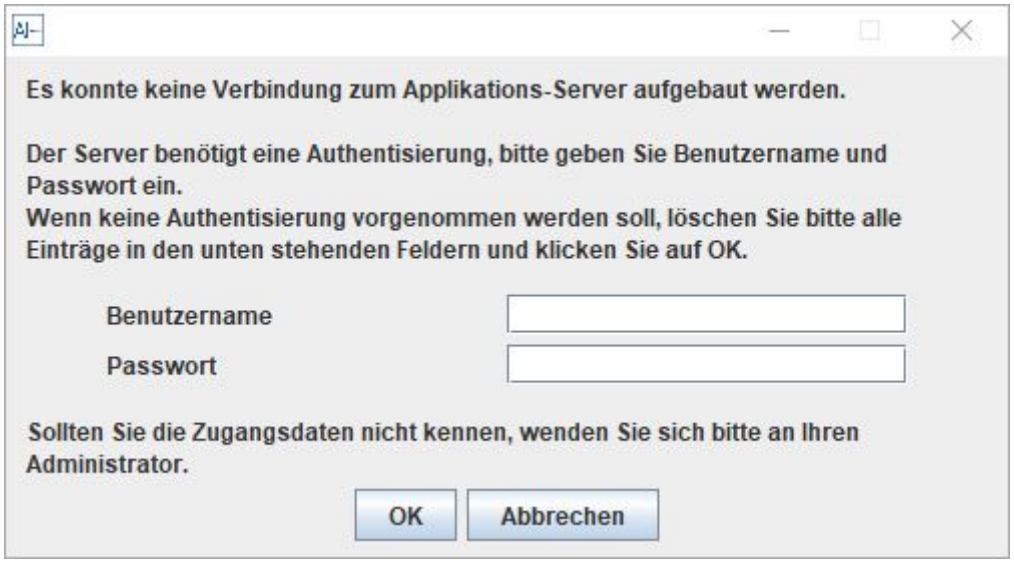

Figure 9: Requesting server credentials for **AI WEB**LAUNCHER

3.3 SSL Dialog

In case that the connection to the application server is not protected by a trusted SSL certificate, the user will be asked whether to trust it. Information regarding the issuer, certification authority and validity period will be displayed.

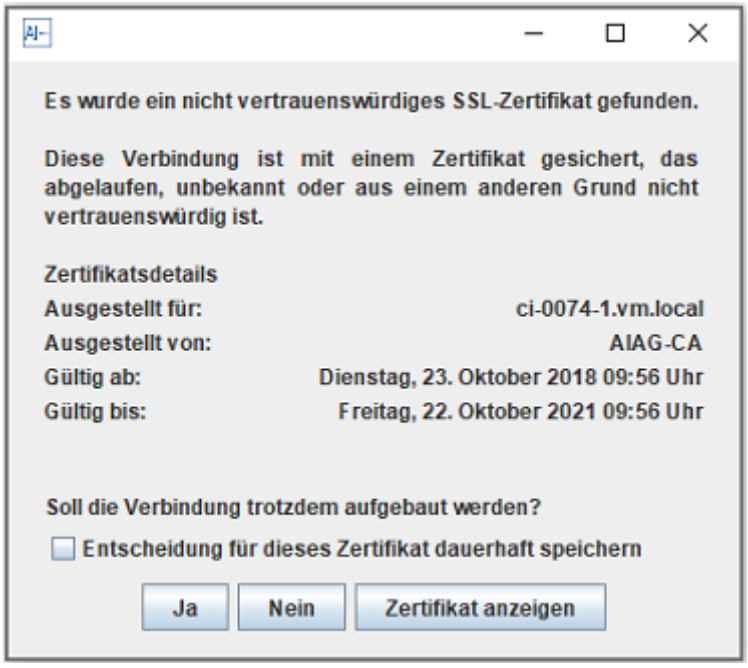

Figure 10: SSL dialog

By confirming the dialog the SSL certificate is trusted temporarily and the connection to the application server will be established. The user's decision can be remembered permanently

by enabling the option at the bottom left.

3.4 Central delivery of configuration files

In order to centrally distribute the proxy, server and SSL settings (see chapter 3.1, 3.2 and 3.3) to several workstation computers, the configuration files can be created once and be delivered.

3.4.1 Proxy Settings and Server Authentication

The proxy settings are in the proxy.txt file.

Examples:

proxy.txt

```
host = 192.168.1.252
port = 3128
active = true
hasCredentials = false
```

If authentication on the proxy server is also required (HTTP 407), the credentials can be stored in the credentials.txt file.

credentials.txt

```
username=testproxyuser1
password=XeQXkFJLW6bLhWoMF9NVJw\=\=
```

Credentials for authentication on the application server (HTTP 401) are stored in the server-credentials.txt file.

servercredentials.txt

```
username=testproxyuser1
password=XeQXkFJLW6bLhWoMF9NVJw\=\=
```

The files mentioned can be placed manually in the working directory of the target application:

Example of **AI TENDERING**MANAGER on host aivm.intra on Windows clients

%LOCALAPPDATA%\AI\VM\aivm.intra\proxy.txt

%LOCALAPPDATA%\AI\VM\aivm.intra\credentials.txt

%LOCALAPPDATA%\AI\VM\aivm.intra\servercredentials.txt

Alternatively, these settings can also be stored in the **AI WEB**LAUNCHER installation directory if there is no access to the working directory of the application. Please note that the host name of the target application must be part of the file name to enable assignment:

Example of **AI TENDERING**MANAGER on host aivm.intra on Windows clients

C:\Programs\AIWL\proxy_aivm.intra.txt

C:\Programs\AIWL\credentials_aivm.intra.txt

C:\Programs\AIWL\servercredentials_aivm.intra.txt

3.4.2 Trusted SSL Certificates

The keystore usercacerts.jks can also be placed either in the working directory of the application or alternatively in the **AI WEB**LAUNCHER installation directory.

Examples:

%LOCALAPPDATA%\AI\VM\aivm.intra\security\usercacerts.jks

C:\Programs\AIWL\usercacerts.jks

If the keystore is placed in the **AI WEB**LAUNCHER installation directory, it applies to all target applications.

To manually add an SSL certificate to the „usercacerts.jks“ file, open it with an appropriate editor (e.g. „KeyStore Explorer“) and enter the password „changeit“ and import the appropriate certificate.

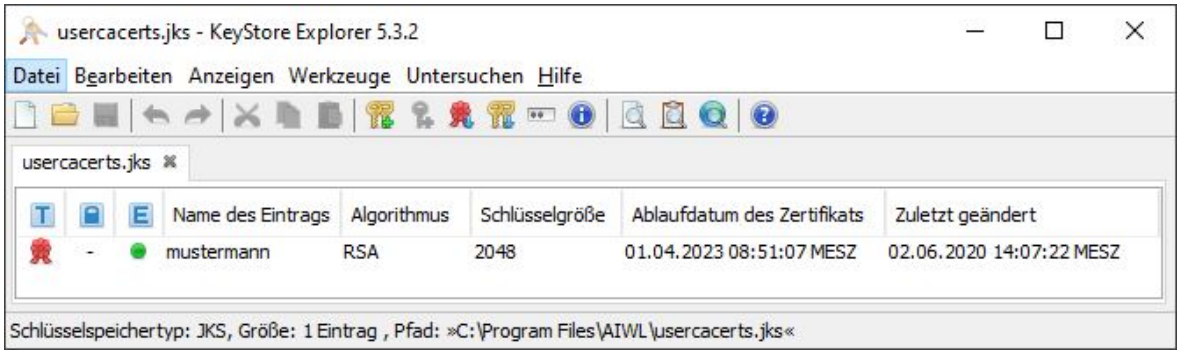

Figure 11: SSL certificate in „KeyStore Explorer“

As an alternative, the command line tool „keytool“ contained in **AI WEB**LAUNCHER can be used. You will find this in the **AI WEB**LAUNCHER installation path in the „jre\bin\“ subdirectory.

Create a new keystore this way or expand an existing one as follows:

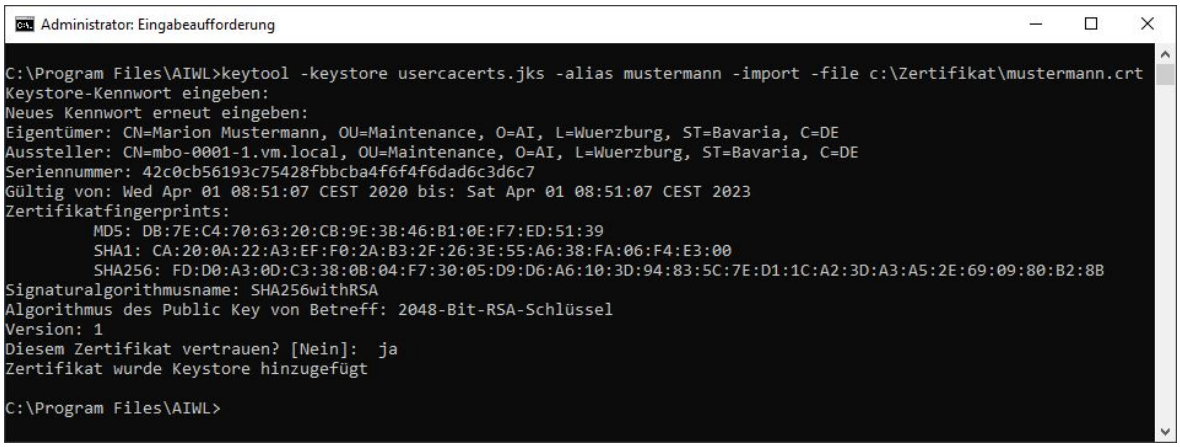

Figure 12: SSL certificate with „keytool“

The keystore password is „changeit“. The filename is „usercacerts.jks“. The key store must be of type „jks“ (java key store).

3.4.3 Required SSL Certificates

If a keystore with the name mandatorycacerts.jks exists, a connection to the server of the target application (in the example "aivm.intra") is only allowed if the connection is encrypted and either the SSL certificate used or its issuer certificate is in the mandatorycacerts keystore. jks is included.

The key store mandatorycacerts.jks can also be placed either in the working directory of the application or alternatively in the installation directory of **AI WEB**LAUNCHER.

Examples:

%LOCALAPPDATA%\AI\VM\aivm.intra\security\mandatorycacerts.jks

C:\Programs\AIWL\mandatorycacerts.jks

If the keystore is placed in the **AI WEB**LAUNCHER installation directory, it applies to all target applications.

To add an SSL certificate manually to the "mandatorycacerts.jks" file, please follow the instructions in Chapter 3.4.2 and proceed in exactly the same way as in

If a mandatorycacerts.jks is available, only connections via SSL are possible. Connecting to a server via HTTP is then not allowed.

3.5 Further Security Concepts

3.5.1 Validation of passed parameters

The two parameters `jvm.initial-heap-size` and `jvm.max-heap-size` are checked for the correct format before they are passed to the application to be started, which prevents additional, unwanted parameters from being appended .

3.5.2 Signing the transmitted hash values

The integrity of the downloaded files is ensured by comparing hash values. The files containing the file hashes (digest.txt and digest2.txt) are signed in order to check their authenticity. If the files are not signed correctly, the application will not start.