Administration Intelligence AG

AI WEBLAUNCHER

Installation und Betrieb

Version: **1.3.1**
Projekt: **AI WEBLAUNCHER**
Datum: 2. Februar 2024

Inhaltsverzeichnis

0 Release Notes

Die folgende Tabelle listet die Software-Änderungen in den einzelnen Versionen des **AI WEB**LAUNCHER auf.

Version	Release Notes
1.0.3	• Initiale Freigabe
1.0.4	• Neue Code-Signatur zur Vermeidung der Smartscreen Defender Warnmeldung bei der Installation • Erweiterung des Betriebshandbuchs
1.0.5	• Erweiterung des Betriebshandbuchs
1.0.6	• Fehlerbericht kann nun erzeugt werden, wenn der Anwendungsstart fehlschlägt • Wechsel von Verbindung mit Proxy auf eine direkte Verbindung funktioniert jetzt • Englische Sprache ist jetzt Standard, falls Sprache des Betriebssystems nicht unterstützt bzw. erkannt wird
1.1.0	• Anwendungen können im DEBUG Modus gestartet werden • Validierung der Code-Signatur beim Start einer Anwendung
1.1.1	• MacOS Notarisierung hinzugefügt • Serverauthentisierung wurde hinzugefügt • Zentrale Verteilung von SSL-Zertifikaten und Proxy- bzw. Server-Zugangsdaten • Vorherige Java Laufzeitumgebung wird nun bei einem Update korrekt gelöscht
1.1.2	• Fehler bei Installation auf MacOS behoben • Backslashes im Benutzernamen von Proxy-Zugangsdaten nun verwendbar
1.1.3	• Versionsüberprüfung bei Start der Applikation
1.1.4	• Konnektivitätstest und Download finden nun mit HTTP-Methode GET statt • Aufforderung zur Proxy-Konfiguration erscheint nun auch bei Verbindungsabbruch mit ungültigem bzw. unbekanntem HTTP-Status • Beispiele für Konfigurationsdateien
1.1.5	• Zertifikate zur SSL-Client-Authentisierung können bei der Installation importiert werden • Erkennung von vertrauenswürdigen SSL-Zertifikaten auf die Verwendung von Keystores umgestellt • Das Verzeichnis zum Herunterladen von Anwendungen kann jetzt administrativ gewählt werden

Version	Release Notes
1.1.6	• Presources wurden deaktiviert und eine nicht durchführbare Signaturprüfung führt jetzt zum Abbruch des Ladevorgangs • Die Ausführung von Patches wurde generell deaktiviert • Der Start von Anwendungen im versionierten Modus wurde deaktiviert • Kommandozeilenparameter für die Java-VM werden gefiltert • Die ausführbaren Dateien der Java Laufzeitumgebung der Client-Anwendung werden bei Programmstart auf ihre Authentizität geprüft (SHA-256)
1.1.7	• Client-Anwendungen auf Bieterseite starten nun wieder mit Java 11 unter MacOS • Möglichkeit geschaffen, den Verbindungsaufbau nur mit vorher festgelegten SSL-Zertifikaten abgesichert zuzulassen (mandatorycacerts.jks)
1.2.0	• Log4j auf Version 2.17.0 aktualisiert
1.2.2	• Unterstützung der ARM-Technologie unter MacOS (M1 Prozessoren) • Es ist nun nicht mehr möglich, verpflichtende SSL-Zertifikate durch Nutzung des unverschlüsselten HTTP Protokolls zu umgehen. • Bei Angabe von verpflichtenden SSL-Zertifikaten ist es nun nicht mehr möglich, diese Verpflichtung für den Client zu umgehen, indem über System-Properties abweichende Angaben zu Proxies vorgenommen werden. • Der Vergleich der Hashwerte der Bibliotheken findet nun auch dann statt, wenn sie nicht erneut heruntergeladen wurden
1.2.2.1	• Properties zur Server-Kommunikation werden in der Startdatei (*.aiweblaunch) nur noch dann zwingend erwartet, wenn mandatorycacerts hinterlegt sind
1.2.2.2	• Fehler im Installer für macOS M1 (ARM) behoben
1.3.0	• Download der Anwendung von einem schadhaften Fremd-Server wird nun verhindert

1 Überblick

AI WEBLAUNCHER ist eine moderne und auf Open-Source-Komponenten aufbauende Lösung, um die Produkte der Administration Intelligence AG zukünftig starten zu können. **AI WEB**LAUNCHER ersetzt Oracles Java Web Start Technologie, die damit nicht mehr notwendig ist, um Desktop-Anwendungen der Administration Intelligence AG zu starten.

2 Installation

2.1 Installation mit grafischer Oberfläche

Beim Start der Installation mithilfe der Installationsdatei von **AI WEB**LAUNCHER kann eine Hinweismeldung des Smartscreen Defenders von Windows erscheinen. Wenn die **AI WEB**LAUNCHER Installationsdatei aus einer sicheren Quelle bezogen wurde, kann mit einem Klick auf „Weitere Informationen“ und „Trotzdem ausführen“ die Installation gestartet werden.

Bei einem Administratorenkonto wird man durch die Benutzerkontensteuerung aufgefordert das Installationsprogramm mit Administratorenrechten zu starten. Bei einem normalen Benutzerkonto kann **AI WEB**LAUNCHER nur in Verzeichnisse mit Schreibrechten installiert werden. Üblicherweise ist dies das Benutzerverzeichnis.

Abbildung 1: Startbildschirm der **AI WEB**LAUNCHER Installation

Im 2. Schritt der Installation von **AI WEB**LAUNCHER muss der Lizenzvereinbarung zugestimmt werden, um mit der Installation fortfahren zu können.

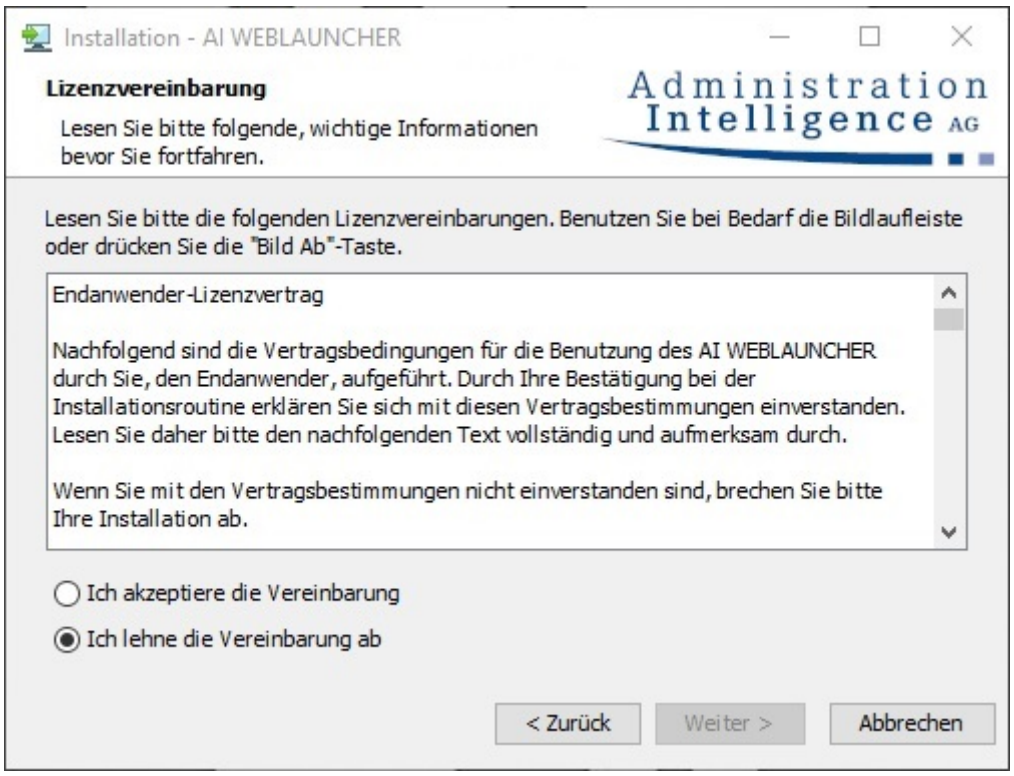

Abbildung 2: Lizenzvereinbarung der **AI WEB**LAUNCHER Installation

Im nächsten Schritt kann das Installationsverzeichnis von **AI WEB**LAUNCHER ausgewählt werden.

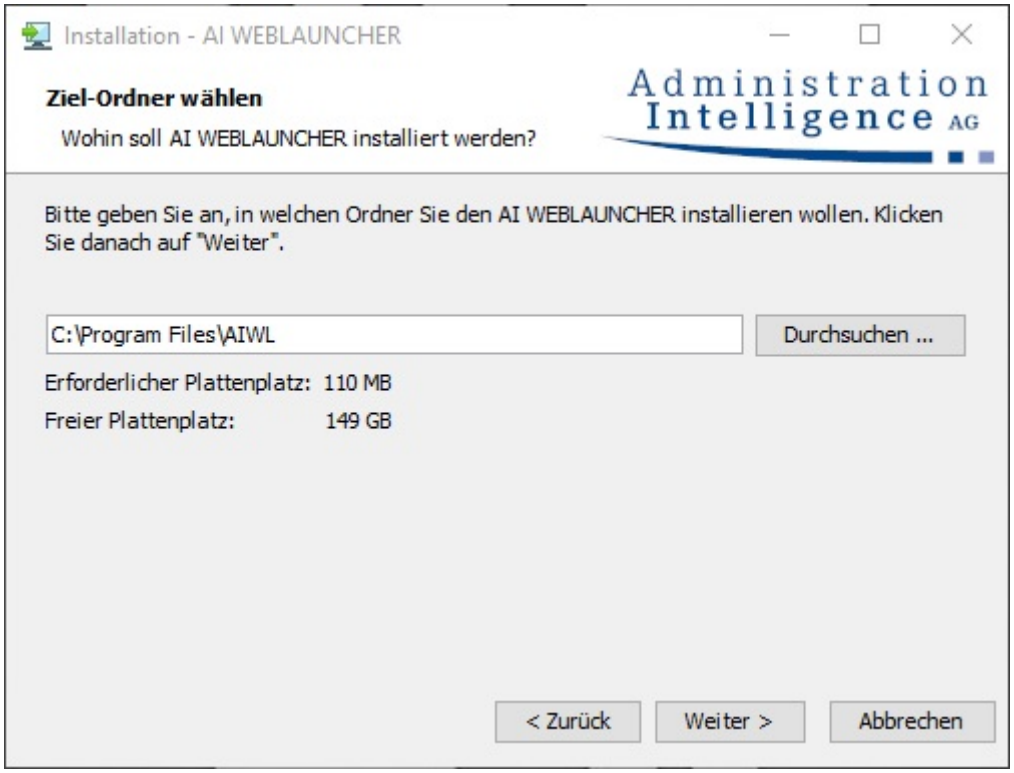

Abbildung 3: Auswahl des **AI WEB**LAUNCHER Installationsverzeichnisses

AI WEBLAUNCHER wird nun in das angegebene Verzeichnis installiert.

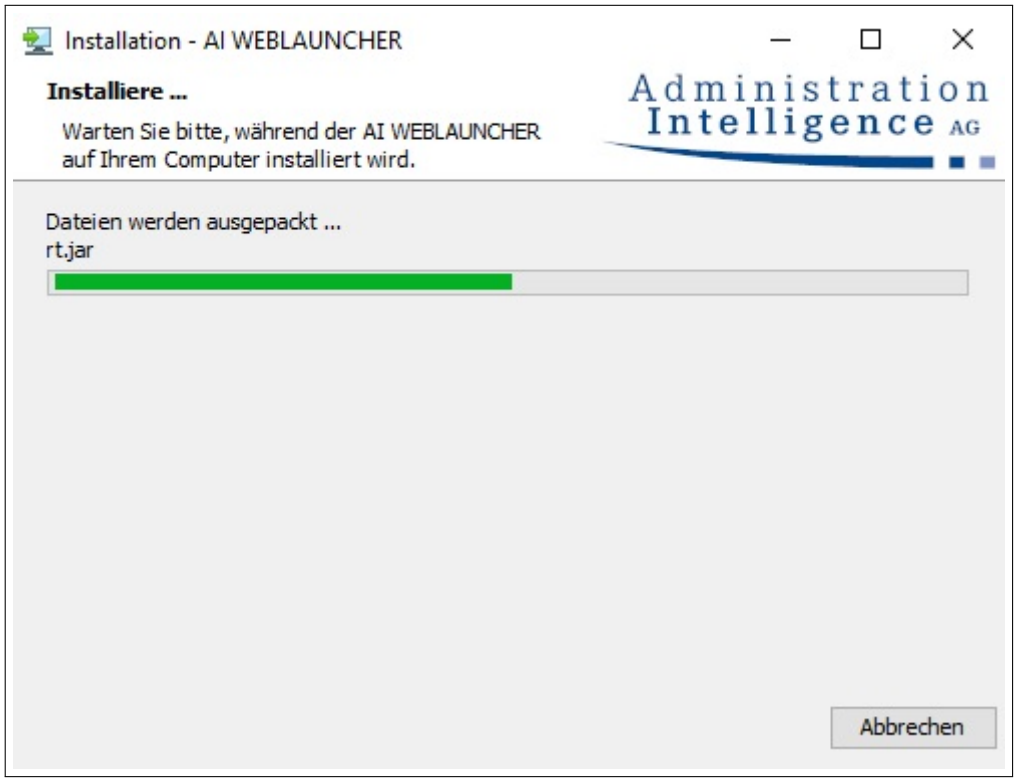

Abbildung 4: **AI WEB**LAUNCHER Installation

Von einigen Servern wird zur Authentisierung des **AI WEB**LAUNCHER ein besonderes, für den Client ausgestelltes Zertifikat benötigt. In den folgenden Schritten haben Sie die Möglichkeit, Client-Zertifikate in den Schlüsselspeicher zu importieren, die dann für die Authentisierung verwendet werden.

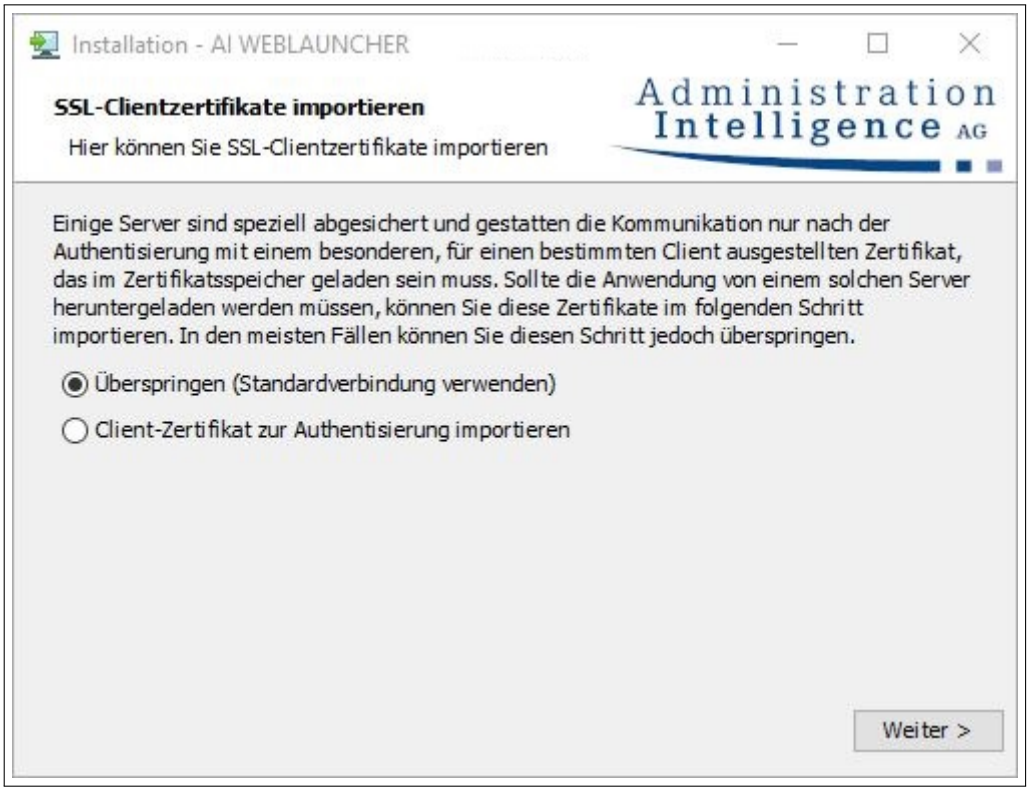

Abbildung 5: Nutzung von für den Client ausgestellten Zertifikaten im **AI WEB**LAUNCHER

Dieser Schritt ist nur bei der Entscheidung zur Nutzung von Client-Zertifikaten aus dem vorhergehenden Schritt relevant. Bei dortigem „Überspringen“ wird dieser Dialog nicht angezeigt und es wird gleich mit dem nächsten Schritt weiter unten fortgefahren.

Ein Klick auf „Durchsuchen“ öffnet einen Dateiauswahldialog zur Wahl von Zertifikatsdateien der Dateitypen **pfx**, **p12** oder **jks**.

Durch Klick auf „Importieren“ wird das genannte Zertifikat dem Zertifikatsspeicher hinzugefügt.

Im unteren Teil des Dialogs ist der Inhalt des Zertifikatsspeichers wiedergegeben. Die genannten Schritte können beliebig oft wiederholt werden, bis der Zertifikatsspeicher alle nötigen Zertifikate enthält. Ebenso ist es über ein wiederholtes Starten der Installation jederzeit möglich, den Zertifikatsspeicher nachträglich zu erweitern.

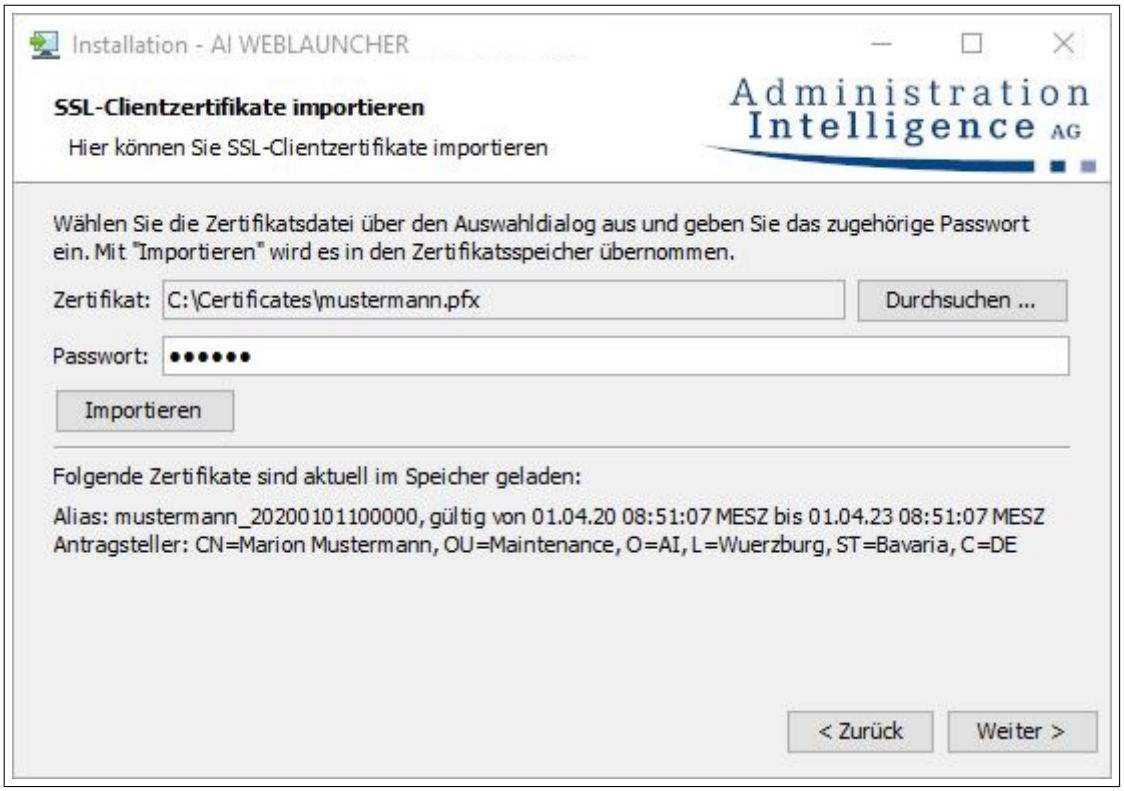

Abbildung 6: Importieren von Client-Zertifikaten im **AI WEB**LAUNCHER

AI WEBLAUNCHER ist nun installiert und die gewünschte Anwendung der Administration Intelligence AG kann gestartet werden.

Abbildung 7: Abschlussbildschirm der **AI WEB**LAUNCHER Installation

2.2 Installation ohne grafische Oberfläche

AI WEBLAUNCHER kann auch ohne grafische Oberfläche mithilfe der Kommandozeile installiert werden. Dabei werden drei verschiedene Möglichkeiten unterstützt. Für die nachfolgenden Beispiele wird exemplarisch eine 64bit Installation für Windows verwendet.

2.2.1 Fragen in der Kommandozeile beantworten

Über den Befehl `start /wait AI_WEBLAUNCHER64bit.exe -c` kann die Installation von **AI WEB**LAUNCHER über die Kommandozeile gestartet werden. Dort müssen, wie in der Installation mit grafischer Oberfläche, alle Fragen beantwortet werden.

2.2.2 Konfiguration als Parameter übergeben

Alternativ kann man das Installationsverzeichnis, in welchem **AI WEB**LAUNCHER installiert werden soll, als Parameter an die Installationsdatei übergeben werden. Der Befehl dafür lautet:
start /wait AI_WEBLAUNCHER64bit.exe -q -dir <Installationsverzeichnis>

2.3 Starten von Anwendungen mittels AI WEBLAUNCHER

Nachdem die Installation von **AI WEB**LAUNCHER abgeschlossen wurde, können die Client-Anwendungen der Administration Intelligence AG erstmalig gestartet werden. Hierzu muss über einen Browser der entsprechende Link angeklickt werden, wodurch die Installation der Client-Anwendung gestartet wird.

2.3.1 Mime-Type-Verknüpfung

Die Installation des **AI WEB**LAUNCHER erzeugt auf dem System eine Verknüpfung mit dem Mime-Type `application/x-aiweblaunch` (Dateiendung aiweblaunch), sodass diese Dateien automatisch durch **AI WEB**LAUNCHER verarbeitet werden.

2.3.2 Speicherort

Wenn die Installation abgeschlossen ist und die benötigten Voreinstellungen vorgenommen wurden, können die Anwendungen gestartet werden. Je nach Betriebssystem werden die notwendigen Komponenten und benutzerspezifischen Einstellungen in den unten genannten Speicherort heruntergeladen:

Betriebssystem	Speicherort
Windows	%LOCALAPPDATA%\AI\PRODUCTNAME\HOSTNAME
Linux	user.home\AI\PRODUCTNAME\HOSTNAME
macOS	user.home\Library\AI\PRODUCTNAME\HOSTNAME

Es handelt sich hier bei PRODUCTNAME und HOSTNAME um Platzhalter. PRODUCTNAME ist z. B. für **AI VERGABE**MANAGER durch **VM** und für **AI BIETER**COCKPIT durch **BCockpit** zu ersetzen. HOSTNAME muss durch die URL des Servers ersetzt werden.
Beispiel für einen Speicherort für den **AI VERGABE**MANAGER:
C:\Users\jdoe\AppData\Local\AI\VM\www.vergabemanager.de\
Beispiel für einen Speicherort für das **AI BIETER**COCKPIT:
C:\Users\jdoe\AppData\Local\AI\BCockpit\www.vergabeplattform.ai-ag.de\

Unter besonderen Umständen kann es erforderlich sein, ein anderes Download-Verzeichnis zu definieren. Legen Sie zu diesem Zweck im Installationspfad des **AI WEB**LAUNCHER die Datei „AI_WEBLAUNCHER.properties“ mit folgendem Inhalt ab:

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

Ein in 2 Prozentzeichen eingefasster Begriff steht für eine Umgebungsvariable. Diese wird entsprechend ersetzt. Es können beliebig viele Umgebungsvariablen verwendet werden.
Wie in der Tabelle angegeben werden durch den **AI WEB**LAUNCHER an den Pfad noch die entsprechenden Unterverzeichnisse „\PRODUCTNAME\HOSTNAME“ angehängt.

Benutzerspezifische Einstellungen, wie zum Beispiel Proxy-Informationen oder persistent gespeicherte, vertrauenswürdige SSL-Zertifikate werden nicht im unter „application_dir“ angegebenen Download-Verzeichnis abgelegt, sondern werden weiterhin in den in der Tabelle „Speicherort“ angegebenen Ordnern gespeichert.

2.3.2.1 Logausgaben

Im Speicherort der Applikation können in der Datei „launcher.log“ die Logausgaben des Programmstarts gefunden werden. Der Speicherort der Logdateien der gestarteten Anwendung ist unverändert.

2.3.2.2 Neuen Download der Applikation erzwingen

Wenn ein erneuter Download der Client-Anwendung erzwungen werden soll, können die Dateien im Speicherort gelöscht werden (Löschen des Cache). **AI WEB**LAUNCHER wird automatisch alle benötigten Dateien erneut vom Applikationsserver herunterladen.

WICHTIG: Sollten Proxyeinstellungen vorgenommen oder SSL-Zertifakten dauerhaft ver-

traut worden sein, dürfen die Dateien „proxy.txt“ (Proxy-Einstellungen) und „usercacerts.jks“ (dauerhaft vertrauenswürdige SSL-Zertifikate) nicht gelöscht werden!

2.3.3 Verwendete Version von AI WEBLAUNCHER auslesen

Wenn innerhalb einer Client-Applikation ein Fehlerbericht erstellt wird, kann in der Datei „SystemInfo.html“ unter dem Punkt „Program information“ die verwendete Version des **AI WEB**LAUNCHER ausgelesen werden.

Außerdem wird die Versionsnummer des installierten **AI WEB**LAUNCHER unter Windows in der Liste der installierten „Programme und Features“ innerhalb der Systemsteuerung angezeigt.

2.3.4 Besonderheiten unter Windows

Benutzerkontensteuerung

UAC beschreibt bewährte Methoden, Standort, Werte, Gruppenrichtlinien-Verwaltungskonsole und Sicherheitsaspekte für die Benutzerkontensteuerung. UAC ist unverzichtbar für alle Umgebungen, in denen mit administrativen Rechten gearbeitet werden muss und erhöht in diesen die Sicherheit. Der entscheidende Punkt ist, dass administrative Rechte immer erst nach einer Zustimmungsabfrage zur Verfügung stehen und nicht automatisch benutzt werden können. Außerdem sind die UAC durchsetzenden Funktionalitäten ideal geeignet, um die Rechte von nicht vertrauenswürdigen Prozessen innerhalb einer Nutzersitzung einzuschränken. Dies gilt vor allem für alle Prozesse, die mit dem Internet kommunizieren.

3 Netzwerkstruktur und Sicherheit

3.1 Proxy-Dialog

Gelingt es nicht, die Verbindung aufzubauen, erscheint ein Dialog zur Eingabe der Proxy-Konfigurationsdaten. Erfassen Sie Hostnamen bzw. IP-Adresse und den Port des Proxy-Servers. Mit der Bestätigung werden diese Informationen für künftige Starts gespeichert.

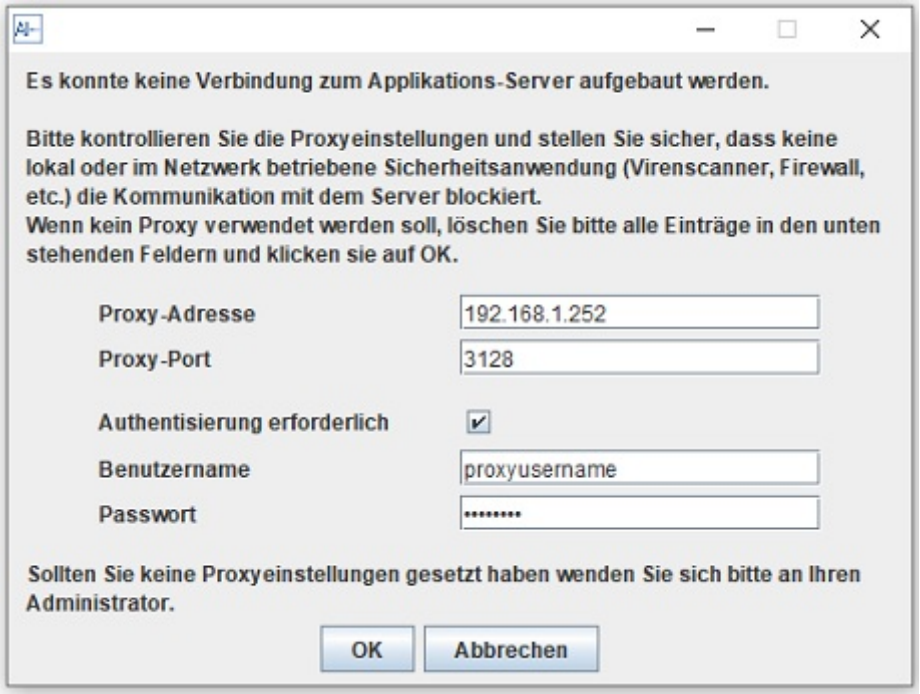

Abbildung 8: Proxy ohne Authentisierung

Falls für den Proxy eine Authentisierung erforderlich ist, muss der entsprechende Haken aktiviert werden, sodass der Benutzername und das Passwort ebenfalls eingetragen werden können.

3.2 Server-Authentisierung-Dialog

Wird während der Datenverbindung durch den **AI WEB**LAUNCHER eine Server-Authentisierungsanfrage erkannt, so wird der Anwender nach den Zugangsdaten gefragt.

Mit der Bestätigung werden diese Informationen für künftige Verbindungen gespeichert.

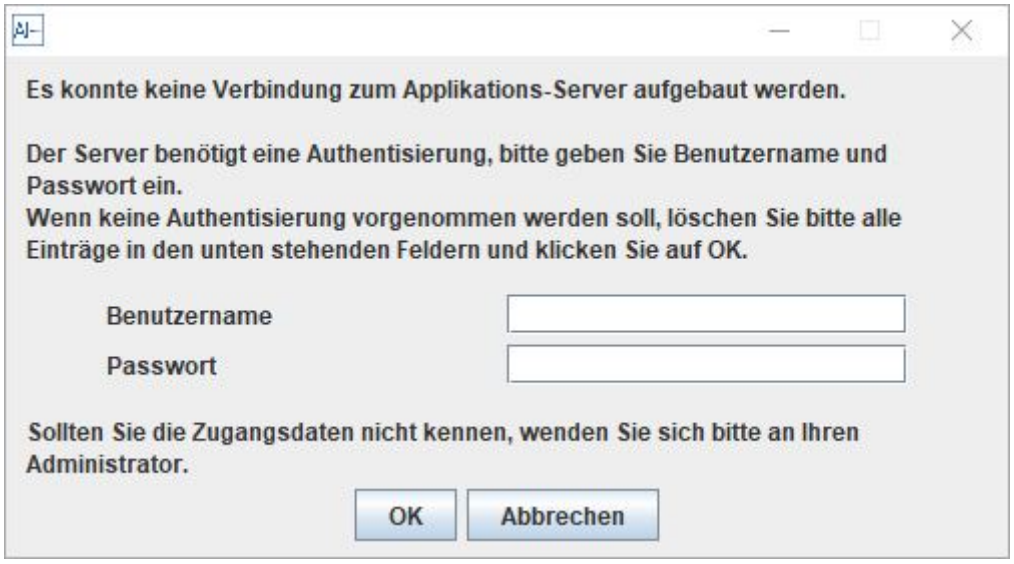

Abbildung 9: Ermittlung der Server-Zugangsdaten für **AI WEB**LAUNCHER

3.3 SSL-Dialog

Ist die Verbindung zu dem Applikationsserver durch ein nicht vertrauenswürdiges SSL-Zertifikat geschützt, wird der Benutzer gefragt ob er diesem trotzdem vertrauen möchte. Dabei werden Informationen wie der Aussteller, die Zertifizierungsstelle und der Gültigkeitszeitraum angezeigt.

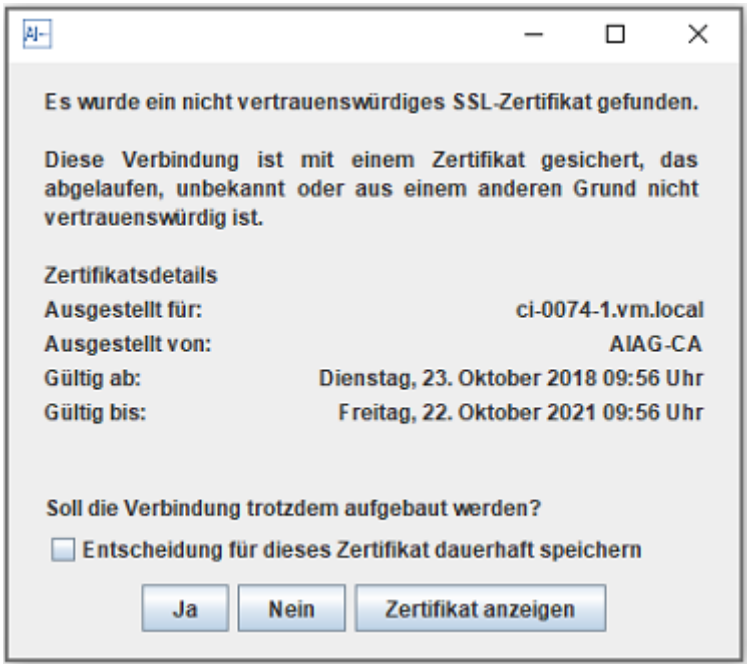

Abbildung 10: SSL Dialog

Durch bestätigen des Dialogs wird dem SSL-Zertifikat temporär vertraut und eine Verbindung

zum Applikationsserver hergestellt. Der Benutzer kann seine Entscheidung dauerhaft speichern, indem er den Haken „Entscheidung für dieses Zertifikat dauerhaft speichern“ setzt und den Dialog bestätigt.

3.4 Zentrale Auslieferung von Konfigurationsdateien

Um die Proxy-, Server- und SSL-Einstellungen (siehe Kapitel 3.1, 3.2 und 3.3) zentral an mehrere Arbeitsplatzrechner zu verteilen, können die Konfigurationsdateien einmalig erstellt und ausgeliefert werden.

3.4.1 Proxy-Einstellungen und Serverauthentisierung

Die Proxy-Einstellungen befinden sich in der Datei proxy.txt.

Beispiele:

proxy.txt

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

Sollte zusätzlich eine Authentisierung am Proxy-Server erforderlich sein (HTTP 407), können die Credentials in der Datei credentials.txt hinterlegt werden.

credentials.txt

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

Credentials für eine Authentisierung am Applikationsserver (HTTP 401) sind in der Datei servercredentials.txt hinterlegt.

servercredentials.txt

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

Die genannten Dateien können manuell in das Arbeitsverzeichnis der Zielanwendung gelegt

werden:

Beispiel für den **AI VERGABE**MANAGER auf Host aivm.intra auf Windows-Clients

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

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

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

Alternativ können diese Einstellungen auch im Installationsverzeichnis des **AI WEB**LAUNCHER hinterlegt werden, falls auf das Arbeitsverzeichnis der Anwendung kein Zugriff besteht. Bitte beachten Sie dabei, dass der Hostname der Zielanwendung Bestandteil des Dateinamens sein muss, um eine Zuordnung zu ermöglichen:

Beispiel für den **AI VERGABE**MANAGER auf Host aivm.intra auf Windows-Clients

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

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

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

3.4.2 Vertrauenswürdige SSL-Zertifikate

Der Schlüsselspeicher usercacerts.jks kann ebenfalls entweder in das Arbeitsverzeichnis der Anwendung oder alternativ in das Installationsverzeichnis des **AI WEB**LAUNCHER gelegt werden.

Beispiele:

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

C:\Programme\AIWL\usercacerts.jks

Falls der Schlüsselspeicher in das Installationsverzeichnis des AI WEBLAUNCHER gelegt wird, gilt er für sämtliche Zielanwendungen.

Um ein SSL-Zertifikat manuell in die Datei „usercacerts.jks“ aufzunehmen, öffnen Sie diese mit einem entsprechenden Editor (z.B. „KeyStore Explorer“) unter Eingabe des Passworts „changeit“ und importieren Sie das entsprechende Zertifikat.

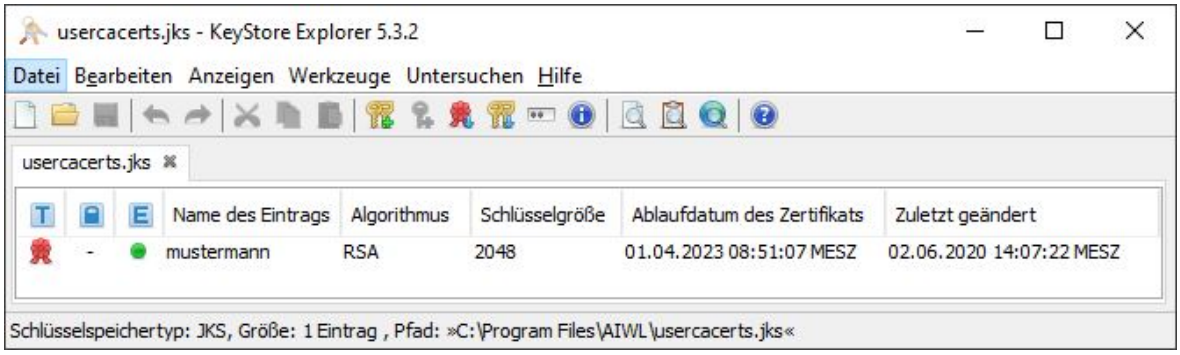

Abbildung 11: SSL Zertifikat im „KeyStore Explorer“

Als Alternative kann das im **AI WEB**LAUNCHER enthaltene Kommandozeilenwerkzeug „keytool“ verwendet werden. Sie finden dieses im Installationspfad des **AI WEB**LAUNCHER im Unterverzeichnis „jre\bin\“.

Erstellen Sie auf diese Weise einen neuen Schlüsselspeicher oder erweitern Sie einen vorhandenen wie folgt:

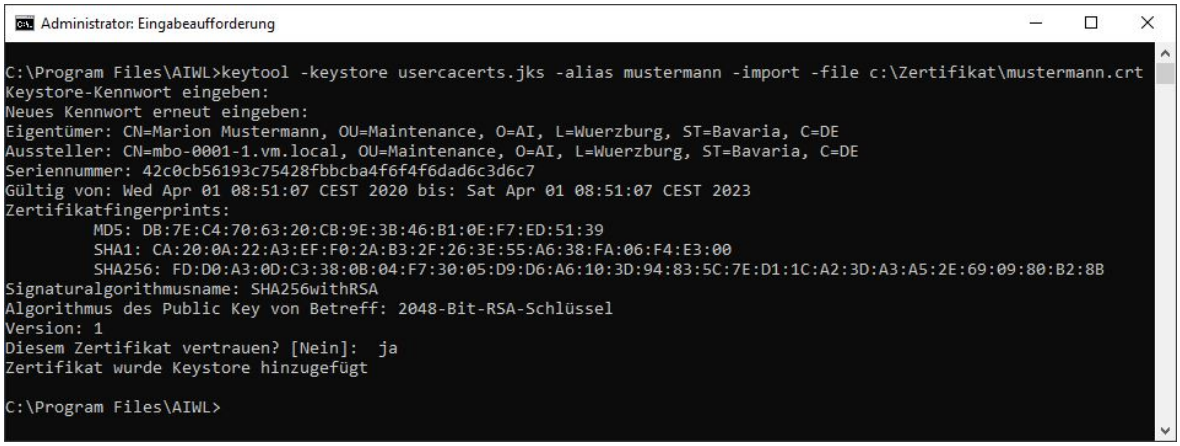

Abbildung 12: SSL Zertifikat mit „keytool“

Das Passwort des Schlüsselspeichers lautet „changeit“. Der Dateiname lautet „usercacerts.jks“. Der Schlüsselspeicher muss vom Typ „jks“ (java key store) sein.

3.4.3 Erforderliche SSL-Zertifikate

Falls ein Schlüsselspeicher mit dem Namen mandatorycacerts.jks existiert, wird eine Verbindung mit dem Server der Zielanwendung (im Beispiel „aivm.intra“) nur dann zugelassen, wenn die Verbindung verschlüsselt und entweder das verwendete SSL-Zertifikat oder sein Ausstellerzertifikat im Schlüsselspeicher mandatorycacerts.jks enthalten ist.

Der Schlüsselspeicher mandatorycacerts.jks kann ebenfalls entweder in das Arbeitsverzeichnis der Anwendung oder alternativ in das Installationsverzeichnis des **AI WEB**LAUNCHER gelegt werden.

Beispiele:

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

C:\Programme\AIWL\mandatorycacerts.jks

Falls der Schlüsselspeicher in das Installationsverzeichnis des **AI WEB**LAUNCHER gelegt wird, gilt er für sämtliche Zielanwendungen.

Um ein SSL-Zertifikat manuell in die Datei „mandatorycacerts.jks“ aufzunehmen, befolgen Sie bitte die Anleitung unter Kapitel 3.4.2 und gehen Sie genauso vor, wie beim manuellen Import eines Zertifikats in den Schlüsselspeicher usercacerts.jks.

Ist eine mandatorycacerts.jks vorhanden, so ist nur noch die Verbindung über SSL möglich. Das Verbinden mit einem Server über HTTP wird dann nicht zugelassen.

3.4.4 SSL-Client-Authentisierung

Falls der Server der Zielanwendung eine SSL-Client-Authentisierung erfordert, kann auch das Client-Zertifikat zentral ausgeliefert werden. Da hierzu jedoch die Eingabe des Zertifikatspasswortes notwendig ist und dieses verschlüsselt gespeichert wird, muss das Client-Zertifikat im Zuge des Installationsvorgangs des **AI WEB**LAUNCHER importiert werden (sh. Kapitel 2.1). Die dabei entstehende Datei sslclientcerts.jks kann dann in das Installationsverzeichnis anderer **AI WEB**LAUNCHER Installationen kopiert werden. Auch hier gilt, dass der Schlüsselspeicher für sämtliche Zielanwendungen verwendet wird

Beispiele:

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

C:\Programme\AIWL\sslclientcerts.jks

3.5 Weitere Sicherheitskonzepte

3.5.1 Validierung von übergebenen Parametern

Die beiden Parameter `jvm.initial-heap-size` und `jvm.max-heap-size` werden vor dem Übergeben an die zu startende Anwendung auf das korrekte Format geprüft, was ein Anhängen von weiteren, unerwünschten Parametern verhindert.

3.5.2 Signieren der übermittelten Hashwerte

Die Integrität der heruntergeladenen Dateien wird durch den Abgleich von Hashwerten sichergestellt. Dabei werden die Dateien, die die Filehashes enthalten (digest.txt und digest2.txt) signiert um auch hier die Echtheit zu prüfen. Sind die Dateien nicht korrekt signiert, startet die Anwendung nicht.