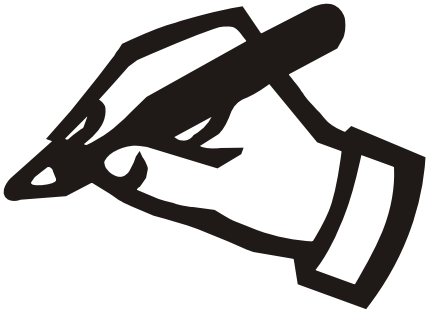
Docker-Manager



Haneke Software

Johannesstraße 41
D-53721 Siegburg

Tel.: +49 (0) 2241-39749-0
Fax: +49 (0) 2241-39749-30
http://www.haneke.de

Stand: 25. Juni 2024

1 Voraussetzungen

Der DockerManager dient dazu, die Serverkomponenten zu unserer Software einfach und ohne Linux-Kenntnisse in einer virtuellen Maschine zu betreiben. Das System ist so eingerichtet, dass es sich automatisch aktualisiert. Die Bedienung erfolgt über eine einfache grafische Oberfläche.
Zum Betrieb brauchen Sie:

- **Eine virtuelle Maschine:** Hier reicht ein kleines System mit AMD64 (bzw. Intel) CPU. Für die meisten Anwendungen sollte ein GB Arbeitsspeicher ausreichen. Die Größe der benötigten Festplatte richtet sich nach dem Umfang der bearbeiteten Datenbanken. Es sollten mindestens 20GB Massenspeicher bereitgestellt werden, wenn viele Dokumente abgelegt werden, kann der Bedarf auch größer ausfallen. Die Speicherbelegung kann bei Bedarf nachträglich mit einer kurzen Unterbrechung des Dienstes vergrößert werden. Das System ist so konfiguriert, dass eine Vergrößerung des virtuellen Datenträgers automatisch in Nutzung genommen wird – Sie müssen keine Anpassung in der Partitionierung vornehmen.
- **Ein Verzeichnis auf Ihrem Fileserver:** Hier wird ein Verzeichnis benötigt, welches über das Protokoll CIFS (Windows-Server, Samba-Linux-Server etc.) bereitgestellt wird. In diesem Verzeichnis werden alle für den Betrieb der Serverkomponenten wichtigen Dateien abgelegt. Lediglich die Datenbankdateien befinden sich in der virtuellen Maschine, da sich diese aus technischen Gründen auf der jeweiligen lokalen Festplatte befinden müssen. Um diese Dateien zu sichern, gibt es entsprechende Programmfunktionen.
  Zusätzlich kann hier ein Programmverzeichnis für die Client-Anwendung bereitgestellt werden.
- **Ein Benutzerkonto am Fileserver:** Bei den Vorplanungen sollten Sie festlegen, über welches Benutzerkonto der Zugriff auf die Dateifreigabe erfolgen soll. Gegebenenfalls müssen Sie hierzu ein neues Benutzerkonto anlegen.

- **Internet-Zugang:** Die virtuelle Maschine muss entweder direkt oder über einen Proxy Dateien aus dem Internet nachladen können.
- **Netzwerk-Konfiguration:** Die virtuelle Maschine bezieht die Netzwerk-Konfiguration normalerweise per DHCP. Sollte dies nicht möglich sein, muss die Konfiguration manuell über die Bedienoberfläche vorgenommen werden (→ 2.2, S. 6).

Die virtuelle Maschine ist so konfiguriert, dass Aktualisierungen der Software automatisch eingespielt werden, es sind somit keine regelmäßigen Eingriffe durch die Administratoren erforderlich.

2 Installation

2.1 Einrichtung der Maschine

Die Auslieferung erfolgt für VM-Ware basierte Server als „Open Virtual Appliance“ im Dateiformat „OVL“, dieses Dateiformat lässt sich bei allen gängigen Virtualisierungslösungen einlesen. Für Hyper-V basierte Systeme verwenden Sie das zweite Archiv mit den entsprechend konvertierten Dateien Die Installationsdatei können Sie unter der folgenden Adresse herunterladen:
https://haneke.de/files/voll/DockerManager_ova.7z
https://haneke.de/files/voll/DockerManager_hv.7z
Nach dem Entpacken und Einlesen der Installationsdatei sollten alle relevanten Einstellungen sinnvoll gesetzt sein, zur Bedienung der Oberfläche wird eine Bildschirmauflösung 1024x768 (XGA) eingestellt. Die Größe der eingerichteten Festplatte ist mit 20 GB vorgegeben, was für die meisten Anwendungen ausreichen sollte, ggf. müssen Sie die Laufwerksgröße später erhöhen.
Falls Sie das System testweise mit dem Desktop-Tool „Virtualbox“ verwenden möchten, lesen Sie dort die OVA-Variante ein. In der Konfiguration müssen Sie anschließend auf dem Reiter „Allgemein“ Das System in „Linux“ und den Typ in „Debian (64Bit)“ und auf dem Reiter Anzeige den Grafikcontroller in „VMSVGA“ ändern.
Wenn die virtuelle Maschine nicht richtig startet, kann es u.U. helfen, die Maschine nach einer kurzen Pause erneut zu starten, da beim Systemstart ggf. Aktualisierungen geholt werden können. Die Benutzeroberfläche fragt normalerweise nicht nach einem Passwort – sollte ausnahmsweise doch ein Login-Dialog erscheinen, können Sie sich mit „dm“ als Benutzernamen und Passwort anmelden.

2.2 Konfiguration der Maschine

Die Benutzeroberfläche besteht aus drei Teilen:

- Im oberen Bereich befinden sich ein Karteireiter-Dialog mit zwei Reitern, der erste („Konfiguration“) dient zur Verbindung mit der Netzwerkfreigabe, auf dem Zweiten („Proxy“) geben Sie die Angaben zu einem eventuell benötigten Proxyserver an.
- Im mittleren Bereich finden Sie die Konfigurations-Bereiche zu den einzelnen Diensten, die aktiviert werden können. Im Titel des jeweiligen Bereiches wird angegeben, ob der Dienst aktiv oder inaktiv ist.
- Ganz unten befindet sich eine Statuszeile, in der Sie Angaben zur Auslastung von Prozessor und Speicher sehen.

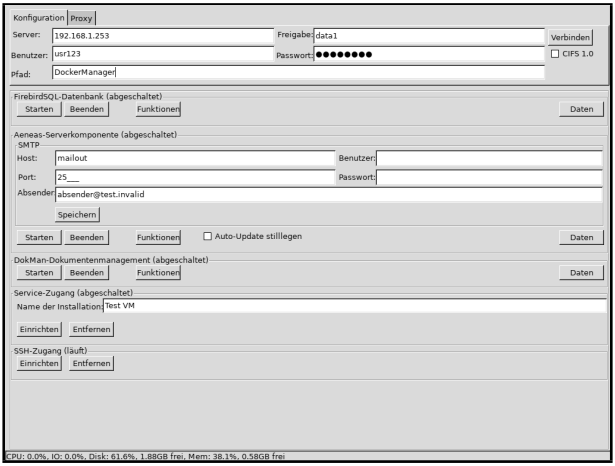


Abbildung 2.1: Startseite des Konfigurationsprogramms

Konfiguration der Netzwerkfreigabe

Auf dem Reiter „Konfiguration“ geben Sie die Daten ein, die zur Verbindung mit dem Fileserver notwendig sind:

1. **Server:** Hier wird der Name oder die IP-Adresse des Servers angegeben.
2. **Freigabe:** Hier wird der Name der Freigabe angegeben, auf die zugegriffen werden soll.

3. **Benutzer:** Hier geben Sie den Benutzernamen ein, mit dem der Zugriff erfolgen soll. Der Name einer Domain kann mit einem „@“ an den Benutzernamen angehängt werden.
4. **Passwort:** Hier wird das Passwort für den Zugriff angegeben.
5. **Pfad:** Hier können Sie einen Pfad angeben, wenn die Dateien in einem Unterverzeichnis auf der Freigabe abgelegt werden sollen. Geben Sie den Pfad ohne Verzeichnistrennzeichen am Anfang und am Ende ein.
6. **CIFS 1.0:** Mit dieser Option können Sie den Zugriff auf sehr alte Server ermöglichen. In der Regel bleibt der Schalter deaktiviert.

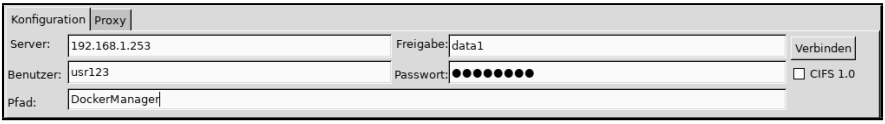


Abbildung 2.2: Karteireiter „Konfiguration“

Wenn alle Angaben eingegeben sind, klicken Sie auf den Button „Verbinden“, um die Verbindung zum Fileserver herzustellen. Falls dort bereits Konfigurationsdaten liegen, werden diese automatisch eingelesen und in die entsprechenden Datenfelder eingetragen.

Konfiguration des Proxy

Auf dem Reiter „Proxy“ geben Sie die Daten ein, die für den Zugriff auf einen HTTP-Proxy erforderlich sind:

- **Host:** Name oder IP-Adresse des Proxy.
- **Port:** Portnummer des Proxy
- **Benutzer:** Falls für den Proxy-Zugriff eine Benutzerkennung erforderlich ist, wird diese hier angegeben.
- **Passwort:** Hier wird das Passwort zu der Benutzerkennung eingegeben.

Wenn alle Eingaben erfolgt sind, klicken Sie auf den Button „Aktivieren“ um die Maschine entsprechend zu konfigurieren.
Wenn für den Internetzugriff kein Proxy verwendet werden soll, lassen sie die Eingabefelder frei.
Falls Ihr Proxy HTTPS-Verbindungen überwacht, muss das Zertifikat der dort verwendeten Zertifizierungsstelle in der virtuellen Maschine als ver-

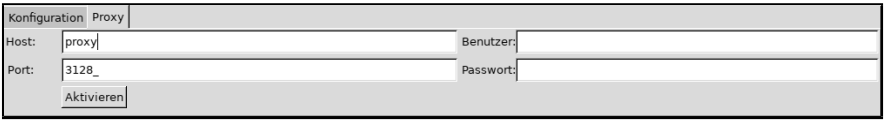


Abbildung 2.3: Karteireiter „Proxy“

trauenswürdig eingetragen werden. Normalerweise erfolgt dieser Eintrag automatisch anhand der beim Seitenabruf mitgelieferten Zertifikate. Sollte die Automatik fehlschlagen, können Sie die entsprechenden CRT-Dateien im Unterordner „cert“ ablegen. Die Angaben müssen in der Codierung „PEM“ gespeichert werden und die Dateiendung „crt“ erhalten. In jeder Datei sollte nur ein Zertifikat enthalten sein. Anschließend muss die Proxy-Konfiguration erneut gespeichert werden, um die Zertifikate zu übernehmen.

Konfiguration des Netzwerkes

Auf dem Reiter „Netzwerk“ können Sie die Netzwerk-Konfiguration der Maschine einstellen. Normalerweise erfolgt die Konfiguration automatisch über einen DHCP-Server. In diesem Fall ist nur der Optionsschalter „DHCP“ angewählt, die Eingabefelder bleiben leer.
Wenn kein DHCP-Server bereit steht, geben Sie in den Eingabefeldern die IP4-Adresse der VM (incl. der Netmaske, z.B. „/24“), die des Gateways und die des DNS-Servers an. Anschließend klicken Sie auf „Aktivieren“, um die Einstellungen zu speichern.

Neustart / Abschalten

Über den Reiter „Boot“ können Sie einen Neustart veranlassen bzw. die Maschine abschalten. Das Betriebssystem wird dabei jeweils ordnungsgemäß heruntergefahren.

Konsolenzugang

Falls Sie für eine manuelle Konfigurationsänderung einen Konsolenzugang zum zugrundeliegenden Linux-System benötigen, erreichen Sie diesen über die Tastenkombination „Strg-Alt-F1“. In dem darauf folgenden Login-Prompt geben Sie als Benutzernamen und Passwort jeweils „root“ ein.
Die Rückkehr zu der grafischen Benutzereoberfläche erfolgt über die Tastenkombination „Strg-Alt-F7“.

Überprüfen der Einstellungen

Nach der Eingabe der Grundeinstellungen sollten Sie den Erfolg der Einrichtung überprüfen:

- Starten Sie die virtuelle Maschine neu.
- Auf der Netzwerk-Freigabe sollte es in dem angegebenen Unterverzeichnis eine Datei `Config.ini` geben. Der Inhalt der Datei ist momentan unwichtig, nach der Grundeinrichtung stehen dort die Angaben zum Proxy-Server drin.
- Ebenfalls sollte es eine Datei `AutoUpdate.log` geben. In dieser Datei wird die automatische Aktualisierung des Management-Programms der VM protokolliert. Am Ende der Datei sollte ein fehlerfreier Update-Lauf protokolliert sein, bei dem nicht unbedingt Dateien aktualisiert worden sind.

Nach dieser kurzen Kontrolle können Sie die benötigten Dienste einschalten.

2.3 Sicherheitsüberlegungen

Ein paar Hinweise zur Sicherheit des Systems:

- Die Bedienungskonsole ist ohne Passwortabfrage offen, dementsprechend muss der Zugang über das Virtualisierungssystem reglementiert werden.
- Die Standard-Passworte der Benutzer „root“ und „dm“ können nur an der Bedinungskonsole genutzt werden und stellen deshalb kein Sicherheitsrisiko da. Wenn Sie möchten können Sie die Passworte über den Konsolenzugang ändern.
- Die eingebundene Netzwerkfreigabe enthält Konfigurationsdaten, die nicht allgemein zugänglich sein dürfen. Die Zugriffsberechtigung sollte sich auf die Systemadministratoren beschränken.
- Wenn Sie auf der Netzwerkfreigabe Programmverzeichnisse für die Client-Rechner bereitstellen lassen (→ 3.6, S. 15), muss für diese Verzeichnisse – und nur für diese – ein lesender Zugriff eingerichtet werden. Ein schreibender Zugriff auf die Programmverzeichnisse ist nicht erforderlich.

3 Konfiguration der Dienste

Für die Benutzung mit unseren Client-Programmen werden die folgenden Dienste angeboten. Die Steuerelemente zur Konfiguration des jeweiligen Dienstes sind zunächst verborgen, klicken Sie auf die entsprechende Eintragung, um den jeweiligen Bereich zu öffnen. In den Titelzeilen wird jeweils angezeigt, ob der jeweilige Dienst aktiv ist.

- **FirebirdSQL-Datenbank:** Dieser Dient enthält den allgemeinen Datenbankserver zur unseren Client-Programme. Dieses Modul kann nicht gleichzeitig mit der Aeneas-Serverkomponente benutzt werden.
- **TLS-Proxy:** Dieser Dienst organisiert die TLS-Verschlüsselung der Web-Zugriffe.
- **Aeneas-Serverkomponente:** Dieser Dienst stellt die Serverkomponente für unsere Flüchtlingsverwaltung Aeneas (bzw. FluV) bereit, der Datenbankserver ist bereits in der Serverkomponente enthalten.
- **DokMan-Dokumentenmanagement:** Dieser Dienst stellt unser System zur Dokumentablage bzw. zur Weiterleitung an CMIS-kompatible Dokumentenmanagementsysteme bereit. Zur Benutzung benötigen Sie eine entsprechende zusätzliche Lizenzkarte.
- **HTTP-Applikation:** Dieser Dienst stellt einige Client-Applikationen zum Zugriff über den Web-Browser bereit.
- **AutoUpdate-Verzeichnisse:** Dieser Dienst erstellt und aktualisiert Programmverzeichnisse für Clients.
- **Service-Zugang:** Über diesen Dienst ermöglichen Sie einen direkten Zugang für unsere Techniker.
- **SSH-Zugang:** Über diesen Dienst können Sie sich einen Zugang zum Linux-System erstellen. Alternativ kann auch der direkte Zugang zur Konsole verwendet werden.

3.1 FirebirdSQL-Datenbank

Die Dateien zu diesem Dienst werden auf der Netzwerkfreigabe im Unterverzeichnis „Firebird“ abgelegt.
Für diesen Dienst muss nichts konfiguriert werden, deshalb gibt es hier keine Eingabefelder.
Dieser Dienst kann nicht gleichzeitig mit der Aeneas-Serverkomponente genutzt werden.

Abbildung 3.1: Bedienungselemente „FirebirdSQL“

Die Schaltflächen haben folgende Funktionen:

- **Starten:** Starten des Dienstes
- **Beenden:** Beenden des Dienstes. Der Dienst steht anschließend für Clienten nicht mehr zur Verfügung, die gespeicherten Daten bleiben jedoch erhalten.
- **Funktionen:** Beim Klicken auf diesen Button öffnet sich ein Menü mit Funktionen, die am laufenden Dienst ausgeführt werden können:
  - **Backup:** Anstoßen eines Sicherungslaufes – normalerweise erfolgt dies täglich zeitgesteuert. Bitte beachten Sie, dass nur die Daten der Anwendungen gesichert werden, bei denen die serverseitige Datensicherung freigeschaltet ist.
  - **Restore:** Anstoßen einer Rücksicherung. Normalerweise erfolgt dies jeweils zur vollen Stunde. In dem entsprechenden Datenverzeichnis müssen zuvor die Dateien zur Rücksicherung abgelegt werden.
  - **Protokoll:** Mit diesem Befehl kopieren Sie das interne Protokoll des Docker-Containers in die Datei „Docker.log“, die im Protokollverzeichnis abgelegt wird.
- **Daten:** Beim Klicken auf diesen Button öffnet sich ein Menü mit Funktionen, die auf den internen Datenbereich des Docker-Contai-

ners wirken. Für die Ausführung wird der Dienst angehalten und anschließend neu gestartet.

  - **Sichern:** Mit diesem Befehl sichern Sie den internen Datenbereich in die Datei „Daten.tar.gz“.
  - **Rücksicherung:** Mit diesem Befehl wird eine zuvor erstellte Sicherung des internen Datenbereiches reaktiviert.
  - **Löschen:** Mit diesem Befehl wird der Dienst beendet und der interne Datenbereich entfernt. Falls die Daten noch gebraucht werden könnten, sollten Sie vorher eine Sicherung anlegen.

3.2 TLS-Proxy

Die Dateien zu diesem Dienst werden auf der Netzwerkfreigabe im Unterverzeichnis „TLSProxy“ abgelegt.
Für diesen Dienst muss nichts konfiguriert werden, deshalb gibt es hier keine Eingabefelder. Die Konfiguration erfolgt über die Angabe der Domainnamen der weiterzuleitenden Dienste. Standardmäßig wird das Server-Zertifikat mittels „certbot“ automatisch generiert. Hierfür müssen sowohl Port 80 als auch Port 443 aus dem Internet erreichbar sein.
Wenn Sie ein eigenes Zertifikat verwenden möchten, tragen Sie dies direkt in der Konfigurationsdatei „lighttp.conf“ ein.
Die Schaltflächen haben folgende Funktionen:

- **Starten:** Starten des Dienstes
- **Beenden:** Beenden des Dienstes. Der Dienst steht anschließend für Clienten nicht mehr zur Verfügung, die gespeicherten Daten bleiben jedoch erhalten.
- **Protokoll:** Mit diesem Befehl kopieren Sie das interne Protokoll des Docker-Containers in die Datei „Docker.log“, die im Protokollverzeichnis abgelegt wird.

3.3 Aeneas-Serverkomponente

Die Dateien zu diesem Dienst werden auf der Netzwerkfreigabe im Unterverzeichnis „Aeneas“ abgelegt.
Dieser Dienst kann nicht gleichzeitig mit der FirebirdSQL-Datenbank genutzt werden.

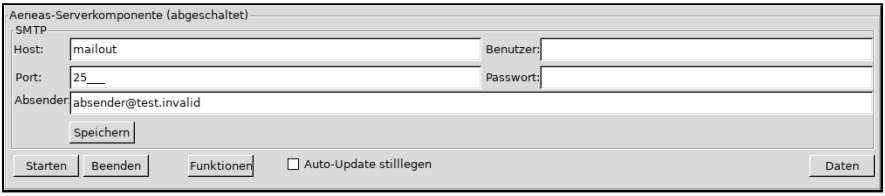


Abbildung 3.2: Bedienungselemente „Aeneas“=Serverkomponente“

Für diesen Dienst kann hier serverseitig die Konfiguration des SMTP-Postausgangs festgelegt werden. Hierzu haben Sie die folgenden Eingabefelder:

- **Host:** Name oder IP-Adresse, des Rechners, über den der Mailversand erfolgen soll.
- **Port:** Nummer des Ports, unter dem die Einlieferung erwartet wird. Normalerweise ist dies „25“, insbesondere bei Exchange-Servern kann aber auch ein anderer Port angegeben werden müssen.
- **Benutzer:** Wenn für den Mailversand eine Anmeldung erforderlich ist, geben Sie hier den Benutzernamen ein.
- **Passwort:** Hier wird das Passwort zu dem zuvor angegebenen Benutzernamen eingetragen.
- **Absender:** Hier können Sie eine Mailadresse eintragen, die als Absender für die automatisch generierten Mails verwendet werden soll.

Über den Button „Speichern“ werden die eingegebenen Daten in die Systemkonfiguration übertragen. Die Konfiguration kann auch am Client in Aeneas erfolgen, die hier angegebenen Werte überschreiben die Angaben aus der Client-Software. Der Mailversand erfolgt direkt aus der Serverkomponente heraus.
Unterhalb der SMTP-Konfiguration finden Sie die folgenden Einstellungen:

- **HTTP extern erreichbar:** Mit diesem Schalter können Sie festlegen, ob der HTTP-Port von AeneasWEB unmittelbar auf der virtuellen Maschine freigegeben werden soll. Da dieser Dienst für externe Mitarbeiter konzipiert ist, muss der Zugriff über einen Reverse-Proxy mit TLS-Verschlüsselung geleitet werden.
- **Domainname für TLS-Proxy:** Wenn Sie hier einen Domainnamen eingeben, wird AeneasWEB mit diesen über den TLS-Proxy freige-

geben. Das Modul „TLS-Proxy“ (→ 3.2, S. 10) muss zusätzlich gestartet werden.

- **Speichern:** Über diesen Button tragen Sie den Domainnamen in die Konfiguration des TLS-Procy ein.
- **Auto-Update stilllegen:** Über diese Option können Sie festlegen, dass in der Serverkomponente keine automatischen Updates eingespielt werden sollen. Wenn diese Option aktiv ist, dürfen am Client ebenfalls keine automatischen Updates eingespielt werden, da beide Programmversionen zueinander kompatibel sein müssen.

Darunter befinden sich einige Schaltflächen, die folgende Funktionen haben:

- **Starten:** Starten des Dienstes
- **Beenden:** Beenden des Dienstes. Der Dienst steht anschließend für Clienten nicht mehr zur Verfügung, die gespeicherten Daten bleiben jedoch erhalten.
- **Funktionen:** Beim Klicken auf diesen Button öffnet sich ein Menü mit Funktionen, die am laufenden Dienst ausgeführt werden können:
  - **Backup:** Anstoßen eines Sicherungslaufes – normalerweise erfolgt dies täglich zeitgesteuert
  - **Restore:** Anstoßen einer Rücksicherung. Normalerweise erfolgt dies jeweils zur vollen Stunde. In dem entsprechenden Datenverzeichnis müssen zuvor die Dateien zur Rücksicherung abgelegt werden.
  - **Update:** Bereitgelegtes Update aktivieren. Normalerweise erfolgt dies jeweils zur vollen Stunde. In dem entsprechenden Datenverzeichnis müssen zuvor die Dateien zur Aktualisierung abgelegt werden.
  - **Hintergrundjobs:** Ausführen der Hintergrund-Jobs, die normalerweise zur vollen Stunde ausgeführt werden. Über diese Funktion können Sie z.B. die Wartezeit auf eine Passwort-Rücksetzung abkürzen.
  - **Restart:** Neustart aller Hilfsprogramme in der Serverkomponente. Der Betrieb der Clients bleibt hiervon unbeeinträchtigt.
  - **Protokoll:** Mit diesem Befehl kopieren Sie das interne Protokoll des Docker-Containers in die Datei „Docker.log“, die im Protokollverzeichnis abgelegt wird.

- **Daten:** Beim Klicken auf diesen Button öffnet sich ein Menü mit Funktionen, die auf den internen Datenbereich des Docker-Containers wirken. Für die Ausführung wird der Dienst angehalten und anschließend neu gestartet.
  - **Sichern:** Mit diesem Befehl sichern Sie den internen Datenbereich in die Datei „Daten.tar.gz“.
  - **Rücksicherung:** Mit diesem Befehl wird eine zuvor erstellte Sicherung des internen Datenbereiches reaktiviert.
  - **Löschen:** Mit diesem Befehl wird der Dienst beendet und der interne Datenbereich entfernt. Falls die Daten noch gebraucht werden könnten, sollten Sie vorher eine Sicherung anlegen.

3.4 DokMan-Dokumentenmanagement

Die Dateien zu diesem Dienst werden auf der Netzwerkfreigabe im Unterverzeichnis „DokMan“ abgelegt.
Für diesen Dienst muss nichts konfiguriert werden, deshalb gibt es hier keine Eingabefelder.

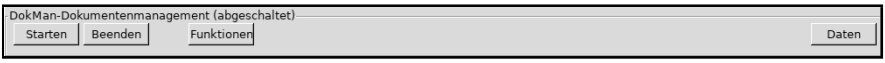


Abbildung 3.3: Bedienungselemente „DokMan-Dokumentenmanagement“

Die Schaltflächen haben folgende Funktionen:

- **Starten:** Starten des Dienstes
- **Beenden:** Beenden des Dienstes. Der Dienst steht anschließend für Clienten nicht mehr zur Verfügung, die gespeicherten Daten bleiben jedoch erhalten.
- **Funktionen:** Beim Klicken auf diesen Button öffnet sich ein Menü mit Funktionen, die am laufenden Dienst ausgeführt werden können:
  - **Backup:** Anstoßen eines Sicherungslaufes – normalerweise erfolgt dies täglich zeitgesteuert
  - **Restore:** Anstoßen einer Rücksicherung. Normalerweise erfolgt dies jeweils zur vollen Stunde. In dem entsprechenden Datenverzeichnis müssen zuvor die Dateien zur Rücksicherung abgelegt werden.

  - **Protokoll:** Mit diesem Befehl kopieren Sie das interne Protokoll des Docker-Containers in die Datei „Docker.log“, die im Protokollverzeichnis abgelegt wird.
- **Daten:** Beim Klicken auf diesen Button öffnet sich ein Menü mit Funktionen, die auf den Internen Datenbereich des Docker-Containers wirken. Für die Ausführung wird der Dienst angehalten und anschließend neu gestartet.
  - **Sichern:** Mit diesem Befehl sichern Sie den internen Datenbereich in die Datei „Daten.tar.gz“.
  - **Rücksicherung:** Mit diesem Befehl wird eine zuvor erstellte Sicherung des internen Datenbereiches reaktiviert.
  - **Löschen:** Mit diesem Befehl wird der Dienst beendet und der interne Datenbereich entfernt. Falls die Daten noch gebraucht werden könnten, sollten Sie vorher eine Sicherung anlegen.

3.5 HTTP-Applikation

Mit diesem Dienst kann ein Client-Programm zum Zugriff über den Webbrowser bereitgestellt werden. Die Bedienung des Programms über den Browser ist weitgehend identisch mit der Bedienung des Programms auf Windows-Rechnern.
Es stehen ihnen die folgenden Einstellungen zur Verfügung:

- **HTTP extern erreichbar:** Mit dieser Einstellung können Sie die den vom Dienst bereitgestellten HTTP-Dienst auf Port 80 der virtuellen Maschine unmittelbar verfügbar machen. Dies ist für rein interne Zugriffe oder für den Fall, dass der Zugang aus dem öffentlichen Internet über einen eigenen Reverse-Proxy erfolgt, sinnvoll. Wenn die Option gewählt wird, kann der TLS-Proxy (→ 3.2, S. 10) nicht verwendet werden, eine direkte Freigabe von AeneasWEB ist damit ebenfalls nicht möglich.
- **Domainname für den TLS-Proxy:** Wenn Sie die Applikation über den TLS-Proxy (→ 3.2, S. 10) freigeben möchten, geben Sie hier den Domainnamen ein, über den die Freigabe erfolgen soll.
- **Anwendung:** Hier wählen Sie die Anwendung, die bereitgestellt werden soll.

- **DB-Server:** Wenn die Datenbank nicht auf der Serverkomponente in der virtuellen Maschine liegen soll, geben Sie hier den Namen des Datenbankservers an.
- **Mandant:** Hier wird das Kürzel des zu verwendenden Mandanten angegeben.
- **Starten:** Starten des Dienstes.
- **Beenden:** Beenden des Dienstes.
- **Protokoll:** Mit diesem Befehl kopieren Sie das interne Protokoll des Docker-Containers in die Datei „Docker.log“, die im Protokollverzeichnis abgelegt wird.

3.6 AutoUpdate-Verzeichnisse

Mit diesem Dienst können Sie auf einfache Weise auf der Konfigurationsfreigabe Programmverzeichnisse für die Client-Programme anlegen und aktuell halten. Das automatische Update wird jeweils nachts ausgeführt.

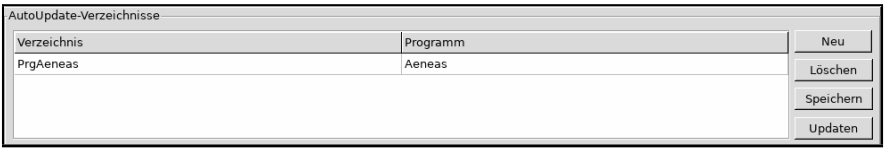


Abbildung 3.4: Bedienungselemente „AutoUpdate-Verzeichnisse“

In der Tabelle geben Sie in der ersten Spalte den Verzeichnisnamen an, in der zweiten Spalte wählen Sie das entsprechende Programm aus.
Die Schaltflächen rechts haben die folgenden Funktionen:

- **Neu:** Anlegen einer neuen, leeren Zeile in der Tabelle.
- **Löschen:** Entfernen der aktuell markierten Zeile.
- **Speichern:** Speichern der Eingaben in der Tabelle.
- **Updaten:** Aktualisierungslauf der Programmverzeichnisse durchführen. Der Aktualisierungslauf erzeugt keine Bildschirmausgabe, Informationen über die aktualisierten Dateien finden Sie jeweils in der Datei „AutoUpdate.log“.

3.7 Service-Zugang

Über den Service-Zugang können Sie es unserer Technik ermöglichen auf die Maschine zuzugreifen. Der Zugriff erfolgt – analog zu dem Kundenservice-Modul am Client über die MeshCentral-Technik. Für die Kommunikation muss Ihr Proxy WebSocket-Verbindungen durchleiten können. In dem Eingabefeld geben Sie einen Namen ein, mit dem unser Techniker Ihr Gerät wiederfinden kann. Der Name sollte den Namen der Stadt und Ihrer Dienststelle enthalten.
Der Service-Zugang wird nur für den Fall der Problembehebung benötigt und kann im Bedarfsfall eingerichtet werden.

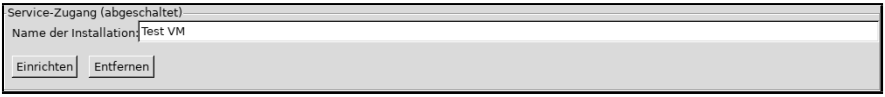


Abbildung 3.5: Bedienungselemente „Service-Zugang“

Über die Schalter „Einrichten“ und „Entfernen“ kann der Dienst aktiviert bzw. deaktiviert werden.

3.8 SSH-Zugang

Über diesen Dienst können Sie einen Zugang zur Maschine über das Protokoll SSH einrichten. Für die Zugangsberechtigung müssen Sie in Ihrem SSH-Programm einen privaten Schlüssel erzeugen und den zugehörigen öffentlichen Schlüssel im Konfigurationsverzeichnis im Unterverzeichnis „ssh“ in der Datei „authorized_keys“ ablegen. Für den Zugang zur virtuellen Maschine wird anschließend der Benutzername „root“ angegeben. Es wird kein Passwort benötigt, da der Zugang über den Besitz des zuvor erstellten privaten Schlüssels abgesichert ist.
Wenn Sie keine Vorstellung haben, was sie mit diesem Zugang machen sollen, werden Sie ihn nicht benötigen. Lassen Sie den Dienst dann inaktiv.
Über die Schalter „Einrichten“ und „Entfernen“ kann der Dienst aktiviert bzw. deaktiviert werden. Bei jeder Einrichtung des Dienstes wird intern ein neuer Identifikationsschlüssel generiert. Da dieser üblicherweise am Client gespeichert wird, erhalten Sie anschließend eine Warnmeldung, dass sich

Abbildung 3.6: Bedienungselemente „SSH-Zugang“

der Schlüssel geändert hat. Nach einer Neuinitialisierung ist das kein Problem, sondern erwartetes Programmverhalten. Der SSH-Client meldet die Änderung, da diese auch dadurch verursacht werden könnte, dass sich jemand in die Netzwerkverbindung eingebunden hat und die Datenübertragung abhören will.