Für Systembetreuer: Anleitung für die Konfiguration von KIM4charly

ab Version 9.18.0

Stand 22.12.2020

Impressum

solutio GmbH & Co. KG
Zahnärztliche Software und Praxismanagement

Max-Eyth-Straße 42
71088 Holzgerlingen
Fon 07031 4618-700
Fax 07031 4618-99700
info@solutio.de
www.solutio.de

Dokumentversion: 20201222.015433-KIM4charly-9.18.0

Support

Sie erreichen unseren Support jeweils Montag bis Freitag von 7:30 bis 18:00 Uhr.

Produkthotline

Fon 07031 4618-800
Fax 07031 4618-99800
hotline@solutio.de

Technische Hotline

Fon 07031 4618-900
Fax 07031 4618-99900
technik@solutio.de

Inhalt

1	Über diese Anleitung	4
2	Voraussetzungen	5
2.1	Telematikinfrastruktur-Voraussetzungen	5
2.2	Software-Voraussetzungen	5
2.3	Erforderliche Ports für KIM4charly	6
2.4	Erforderliche charly-Rechte	6
3	Konfiguration	7
3.1	[Optional] Ports ändern	7
3.2	In charly: Telematikinfrastruktur (TI) einrichten	8
3.2.1	Konfiguration des Konnektors sowie der Aufrufkontexte testen	8
3.3	KIM-Clientmodul installieren und konfigurieren	11
3.4	In KIM4charly: KIM-Konto erstellen	11
4	Server	15
4.1	charly-Java-Server	15
4.2	Konfigurationsdatei "application.yml"	15
4.3	Service-Registry	16
4.4	Kommandozeilenwerkzeug für Serversteuerung	17

1 Über diese Anleitung

KIM4charly ist die Schnittstelle zwischen charly und dem KIM-Dienst.

> **Hinweis:** Diese Anleitung beschreibt die Konfiguration von KIM4charly. Sie richtet sich an Systembetreuer und setzt Grundkenntnisse zur E-Health-Telematikinfrastruktur voraus. Weitere Informationen zu KIM4charly finden Sie in der integrierten Hilfe.

> **Hinweis:** Diese Anleitung setzt voraus, dass die Telematikinfrastruktur in der Praxis bereits eingerichtet und in charly der Konnektor sowie die Aufrufkontexte konfiguriert sind. Weitere Informationen zur Einrichtung der Telematikinfrastruktur in charly finden Sie in der Anleitung „Für PEDs: E-Health-Anbindung (TI) in charly" im Downloadsbereich unserer Homepage.

> **Tipp:** Alle notwendigen Informationen rund um den prinzipiellen Aufbau sowie die Verwaltung des Servers, haben wir in dem Kapitel „Server" auf Seite15 für Sie zusammengefasst.

2 Voraussetzungen

Für die Verwendung von KIM4charly müssen bestimmte Software- und Betriebsbedingungen erfüllt werden.

2.1 Telematikinfrastruktur-Voraussetzungen

Für die Verwendung des KIM-Dienstes benötigen Sie folgende, von der gematik zugelassene, Komponenten und Dienste:

- Einen E-Health-Konnektor (ab PTV3) – unterstützt neben VSDM auch NFDM, eMP und KIM.
- Einen elektronischen Heilberufsausweis ab der zweiten Generation (eHBA G2) – unterstützt die qualifizierte elektronische Signatur (QES).
- Einen elektronischen Praxisausweis (SMC-B).
- Ein stationäres E-Health-Kartenterminal.
- Einen Vertrag mit einem zugelassenen KIM-Anbieter (auch „KIM-Provider"). Von diesem erhalten Sie eine KIM-Adresse, ähnlich einer E-Mail-Adresse.
- Das KIM-Clientmodul (Software) Ihres KIM-Anbieters.
- Einen Eintrag als identitätsgeprüfter KIM-Teilnehmer im Verzeichnisdienst (VZD) der Telematikinfrastruktur.

> **Tipp:** Das Fachportal der gematik bietet u.a. eine Liste aller zugelassenen Komponenten und Dienste.

2.2 Software-Voraussetzungen

Für KIM4charly benötigen Sie mindestens folgende Software-Versionen:

- charly ab Version 9.18.0
- PostgreSQL-Version ab 8.4

> **Tipp:** Die PostgreSQL-Version prüfen Sie, indem Sie in charly in der Menüleiste auf Hilfe > SQL-Datenbank klicken. Wenn die angegebene PostgreSQL-Version kleiner 8.4 ist, muss zunächst ein Datenbank-Upgrade durchgeführt werden. Wenden Sie sich dazu bitte an die Technische Hotline der solutio GmbH & Co. KG.

2.3 Erforderliche Ports für KIM4charly

Übersicht der Ports, die für die Kommunikation zwischen den Komponenten erforderlich sind:

Port	Beschreibung
10443	Standard für den SSL-Proxy. Wird vom charly-Updater in der Firewall geöffnet. Kann im charly-Updater umkonfiguriert werden. Führen Sie dazu den charly-Updater erneut aus.

Für Änderungen an den Ports, siehe „[Optional] Ports ändern“ auf Seite7.

2.4 Erforderliche charly-Rechte

Für die Konfiguration von KIM4charly benötigt Ihr charly-Benutzer mindestens folgende Zugriffsrechte in charly:

- Für den Zugriff auf die Stammdaten in KIM4charly:
  - Einzelrecht KIM4charly Stammdaten: Lesen, Ändern, Neu, Löschen

Die Zugriffsberechtigungen definieren Sie in charly in den Stammdaten > Praxis > Gruppen > Rechte.

3 Konfiguration

Um über KIM4charly Nachrichten und medizinische Dokumente austauschen zu können, muss die Komponente zunächst konfiguriert werden.

3.1 [Optional] Ports ändern

Falls der erforderliche SSL-Proxy-Port für KIM4charly bereits belegt ist, konfigurieren Sie diesen um.

So ändern Sie mit dem charly-Updater den für den SSL-Proxy

> **Hinweis:** Sofern keine neuere charly-Version vorliegt, aktualisiert der charly-Updater ausschließlich den charly-Java-Server und nimmt dabei die Port-Änderungen vor. Falls eine neuere charly-Version verfügbar ist, aktualisiert der charly-Updater zusätzlich die charly-Version.

Voraussetzungen

- Der charly-Updater liegt auf dem charly-Server (Download Windows bzw. Download macOS).
- Der charly-Server verfügt über eine Internetverbindung.
- Das Ausführen des charly-Updaters ist vorbereitet:
  - Schalten Sie alle charly-Arbeitsplätze (Clients) aus.
  - Schließen Sie auf dem charly-Server alle Programme.
  - Führen Sie auf dem charly-Server eine Datensicherung durch.
  - Starten Sie den charly-Server neu.
  - Melden Sie sich mit Administratorrechten am charly-Server an.
  - Deaktivieren Sie auf dem charly-Server den Virenscanner für den Zeitraum des Updates.

Vorgehensweise

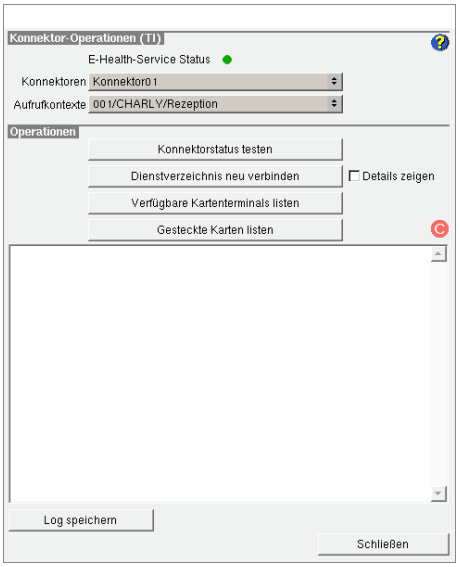
1. Starten Sie den charly-Updater.
2. Folgen Sie den Anweisungen des charly-Updater-Assistenten bis zu der Ansicht für die Konfiguration der Ports für den SSL-Proxy sowie für den Messaging-Service.
3. Ändern Sie den SSL-Proxy-Port.
4. Folgen Sie weiter den Anweisungen des charly-Updater-Assistenten.
   - Der charly-Updater führt die Port-Änderungen im charly-Java-Server durch.

3.2 In charly: Telematikinfrastruktur (TI) einrichten

> **Hinweis:** Diese Anleitung setzt voraus, dass die Telematikinfrastruktur in der Praxis bereits eingerichtet und in charly der Konnektor sowie die Aufrufkontexte konfiguriert sind. Weitere Informationen zur Einrichtung der Telematikinfrastruktur in charly finden Sie in der Anleitung „Für PEDs: E-Health-Anbindung (TI) in charly" im Downloadsbereich unserer Homepage.

3.2.1 Konfiguration des Konnektors sowie der Aufrufkontexte testen

In charly können Sie in dem Fenster Konnektor-Operationen verschiedene Operationen durchführen, um die Konfiguration der Telematikinfrastruktur zu testen.



E-Health-Service Status

Über die Status-Ampel E-Health-Service Status können Sie erkennen, ob der E-Health-Service erreichbar ist.

- Status-Ampel: grün

  Der E-Health-Service ist erreichbar und es können Konnektor-Operationen durchgeführt werden.

- Status-Ampel: rot

  Es erscheint ein Hinweis, dass der E-Health-Service nicht erreichbar ist oder einen Fehler meldet. Es können keine Konnektor-Operationen durchgeführt werden. Im Log-Bereich werden weitere Informationen gelistet.

Konnektorstatus testen

Über den Button Konnektorstatus testen können Sie den TI-Status sowie den SI-Status testen:

TI-Status	Der TI-Status zeigt, ob der Konnektor über den VPN-Zugangsdienst (VPN = Virtual Private Network) eine sichere Verbindung zu der zentralen Telematikinfrastruktur aufbauen kann. Der Weg in die TI wird dabei „getunnelt".
SI-Status	Der SI-Status zeigt an, ob der optionale Dienst „Sicherer Internet Service" (SIS) für den geschützten Zugriff auf das Internet verfügbar ist. Ein Zugriff auf das Praxisnetzwerk über eingehende Verbindungen ist hierbei technologisch ausgeschlossen.

Der TI-Status und der SI-Status kennen jeweils die folgenden Zustände:

Offline	Im Offline-Modus des Konnektors kann keine Verbindung zum VPN-Zugangsdienst aufgebaut werden (z.B. weil die WAN- Schnittstelle nicht angeschlossen oder die Verbindung gestört ist).
Online	Im Online-Modus des Konnektors besteht eine VPN-Verbindung zur zentralen Telematikinfrastruktur oder es wird davon ausgegangen, dass diese Verbindung jederzeit aufgebaut werden kann. Der Online-Modus ist eine wichtige Voraussetzung für die Verwendung von KIM4charly.

Dienstverzeichnis neu verbinden

Über den Button Dienstverzeichnis neu verbinden werden die Fachdienste, die auf dem Konnektor laufen, neu geladen und anschließend mit den Fachdienst-Namen und den Versionen im Log-Bereich gelistet.

Wenn Sie die Checkbox Details zeigen aktivieren, werden neben den Fachdienst-Namen und den Versionen der Fachdienste zusätzliche Informationen angezeigt.

Verfügbare Kartenterminals listen

Über den Button Verfügbare Kartenterminals listen werden die verfügbaren Kartenterminals mit zusätzlichen Informationen im Log-Bereich gelistet.

Gesteckte Karten listen

Über den Button Gesteckte Karten listen werden sämtliche Karten mit zusätzlichen Informationen gelistet, die in den Kartenterminals gesteckt sind.

So führen Sie eine Konnektor-Operation durch

Vorgehensweise

1. Gehen Sie in die Menüleiste unter Hilfe > Konnektor-Operationen (TI).
   - Ein Fenster öffnet sich.
2. Wählen Sie aus der Dropdownliste Konnektoren den Konnektor, für den Sie den Test durchführen möchten.
3. Wählen Sie aus der Dropdownliste Aufrufkontexte den Aufrufkontext, für den Sie den Test durchführen möchten.
4. Klicken Sie auf den gewünschten Button im Bereich Operationen.
   - Der Status wird im Log-Bereich ausgegeben.

3.3 KIM-Clientmodul installieren und konfigurieren

> **Hinweis:** Das KIM-Clientmodul erhalten Sie von Ihrem KIM-Provider. Für die Installation und Konfiguration des KIM-Clientmoduls lesen Sie bitte die Dokumentation Ihres KIM-Providers.

3.4 In KIM4charly: KIM-Konto erstellen

Die KIM-Konten erstellen Sie in KIM4charly in der Ansicht Kontoverwaltung.

So erstellen Sie ein KIM-Konto

Voraussetzungen

- Sie sind als KIM-Nutzer mit Ihren Basisdaten im zentralen Verzeichnisdienst (VZD) eingetragen (wird durch die KZVen gepflegt).

- Sie haben sich bei einem KIM-Provider angemeldet und eine KIM-(E-Mail-)Adresse erhalten. Diese KIM-Adresse wurde von dem KIM-Provider im zentralen VZD eingetragen.
- Sie haben von Ihrem KIM-Provider die POP3- sowie die SMTP-URL erhalten, unter denen die KIM-Kommunikation abgewickelt werden soll.
- Sie kennen die LDAP-, POP3- sowie SMTP-URL des KIM-Clientmoduls.
- Sie verfügen über eine freigeschaltete SMC-B sowie über einen freigeschalteten eHBA.
- Ihr E-Health-Konnektor ist für den Online-Modus konfiguriert.
- Für die KIM-Adresse ist in KIM4charly noch kein KIM-Konto erstellt.

Vorgehensweise

1. Klicken Sie in charly in der Menüleiste auf Bearbeiten > KIM4charly.
   - KIM4charly öffnet sich.
2. Klicken Sie auf den Button für die Kontoverwaltung.
3. Um ein KIM-Konto anzulegen, klicken Sie auf den Erstellen-Button.
   - Die Ansicht zum Erstellen von KIM-Konten öffnet sich.
4. Wählen Sie aus der Dropdownliste Typ die Karte, mit der das KIM-Konto verknüpft werden soll:
   - Wählen Sie SMB für ein Praxiskonto.
   - Wählen Sie HBA für ein Zahnarztkonto.
5. Geben Sie die Daten Ihres KIM-Kontos ein:

Feld	Beschreibung
E-Mail-Adresse	Ihre KIM-Adresse → erhalten Sie von Ihrem KIM-Provider
Passwort	Ihr Passwort für die KIM-Adresse

Feld	Beschreibung
Clientmodul LDAP	URL, unter der das Clientmodul über den LDAP-Proxy des E-Health-Konnektors Daten aus dem Verzeichnisdienst (VZD) abfragen kann
Clientmodul POP3	URL, unter der das Clientmodul die KIM-Nachrichten vom POP3-Server des KIM-Providers abholt
Clientmodul SMTP	URL, unter der das Clientmodul die KIM-Nachrichten an den Mail Transfer Agent des KIM-Providers übermittelt.
Provider POP3	URL, unter der die KIM-Nachrichten vom KIM-Server abgerufen werden → erhalten Sie von Ihrem KIM-Provider
Provider SMTP	URL, unter der die KIM-Nachrichten zum KIM-Server gesendet werden → erhalten Sie von Ihrem KIM-Provider
ICCSN	Kartennummer der Karte, mit der das KIM-Konto verknüpft ist. Sie ist nötig, um KIM-Nachrichten zu senden und zu empfangen. Wird vom Clientmodul für die Transportverschlüsselung verwendet.
Kontobesitzer	Auswahlmöglichkeit des Besitzers. • Voller Zugriff auf die KIM-Nachrichten. • Dürfen das KIM-Konto verwalten (bearbeiten, löschen). Normalerweise der Zahnarzt oder ggf. ein Systembetreuer, der das KIM-Konto im Auftrag des Zahnarztes verwaltet.

Feld	Beschreibung
Kontogäste	Auswahlmöglichkeit weiterer zugriffsberechtigter Personen („Gäste“). • Voller Zugriff auf die KIM-Nachrichten. • Dürfen das KIM-Konto nicht verwalten.
Karteninhaber	Karteninhaber der Karte, mit der das KIM-Konto verknüpft ist. Diese Einstellung dient der automatischen Zuordnung eines Zahnarztes zu einem Signierkonto und der damit verbundenen QES-Funktionalität. • Nur bei eHBA-Konten. • Kann innerhalb eines Mandanten nur einem Konto zugeordnet sein.

6. Klicken Sie auf Speichern.
   ▶ Das KIM-Konto ist angelegt und wird in der Liste der KIM-Konten angezeigt.

4 Server

4.1 charly-Java-Server

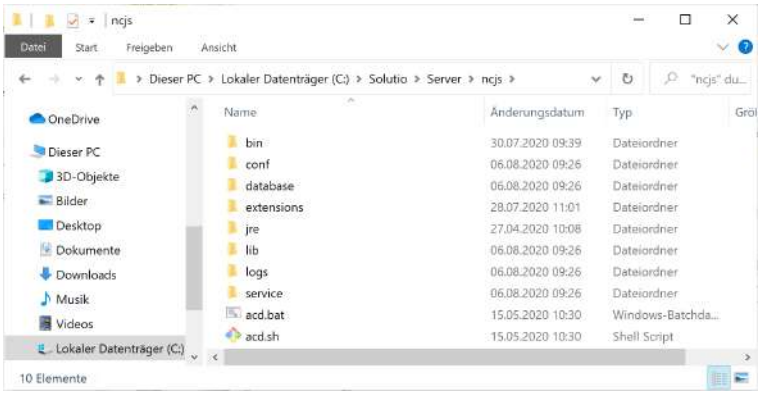
Der charly-Java-Server (ncjs) bezeichnet die Summe aller Microservices und die für deren Betrieb erforderliche Infrastruktur, welche auf dem Server der Zahnarztpraxis betrieben wird.

> Tipp: Der charly-Java-Server ist automatisch in charly enthalten und wird im Rahmen der charly-Updates laufend aktualisiert.

Installationspfad charly-Java-Server (ncjs)

Alle Komponenten des charly-Java-Servers befinden sich auf dem charly-Server unter folgendem Pfad:

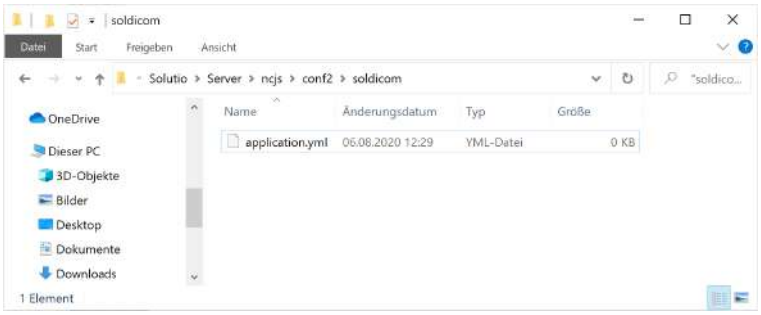
`<charly-Installationspfad>\Solutio\Server\ncjs`



4.2 Konfigurationsdatei "application.yml"

Microservices werden mit Hilfe der Datei „application.yml" konfiguriert. Für jeden Microservice gibt es eine eigene „application.yml"-Datei.

Kundenspezifische Konfigurationen müssen unter „ncjs" in dem **Verzeichnis „conf2"** abgelegt werden, da dieses Verzeichnis durch charly-Updates nicht überschrieben wird. Innerhalb des Verzeichnisses „conf2" muss für jeden Microservice, für den eine kundenspezifische Konfiguration hinterlegt wird, ein weiteres Verzeichnis mit dem Namen des Microservices angelegt werden. Dort wird die kundenspezifische „application.yml"-Datei abgelegt.

> **Beispiel:** Pfad einer kundenspezifischen „application.yml"-Datei mit Konfigurationen für den Soldicom-Service:
>
> `\Solutio\Server\ncjs\conf2\soldicom\application.yml`
>
> 
>

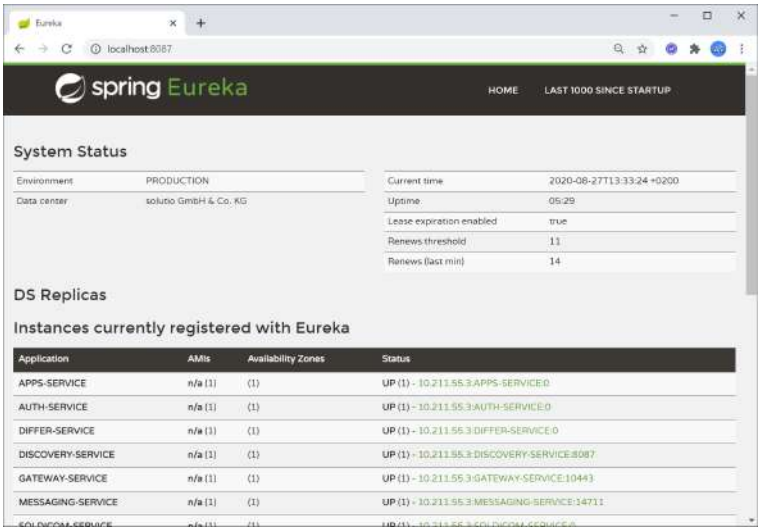
4.3 Service-Registry

Die Service-Registry fasst die Microservices, ihre Instanzen und ihre Lokationen in einer Datenstruktur zusammen. Die Microservices werden unter einem logischen Namen registriert und lassen sich anschließend über diesen Namen ansprechen.

Eine Liste aller registrierter und gestarteter Microservices ist auf der Weboberfläche einsehbar. Diese können Sie wie folgt aufrufen:

1. Öffnen Sie **auf dem Server** ein Browserfenster.
2. Geben Sie folgende URL ein: `http://localhost:8087`

> **Hinweis:** Falls Sie den Port für den Discovery-Service über den charly-Updater geändert haben, geben Sie stattdessen diesen geänderten Port in der URL an.



4.4 Kommandozeilenwerkzeug für Serversteuerung

Alle Microservices werden im Rahmen eines charly-Updates durch den charly-Updater registriert und gestartet. Für den Fall, dass ein Microservice z.B. für eine Konfigurationsänderung manuell gestoppt und wieder gestartet werden muss, gibt es das Tool ACD.

Das ACD-Tool besteht aus jeweils einer Skriptdatei für Windows (`acd.bat`) und macOS (`acd.sh`). Die Skriptdateien sind grundsätzlich in Funktion und Oberfläche identisch. Das Skript muss über die Kommandozeile **im Administratormodus** ausgeführt werden. Dazu muss in der Kommandozeile der Pfad zu dem Verzeichnis geöffnet sein, in dem die Skripdateien (`acd.bat` bzw. `acd.sh`) liegen.

Die Skriptdateien befinden sich unter: `\Solutio\Server\ncjs`.

Aufruf

Der Aufruf beginnt immer mit der Angabe des Skripts gefolgt von dem eigentlichen Befehl. Die Syntax lautet wie folgt:

- **Windows**

```
acd.bat <Befehl> <ggf. Short Name Microservice>
```

- **macOS**

```
sudo ./acd.sh <Befehl> <ggf. Short Name Microservice>
```

Es gibt Befehle, die für alle bekannten Microservices gleichzeitig durchgeführt werden und Befehle, mit denen Sie nur einen bestimmten Microservice ansprechen. Für diese „Einzelbefehle" müssen Sie den Short Name des Microservices angeben. Die Short Names der Microservices finden Sie heraus, indem Sie in der Kommandozeile folgenden Befehl eingeben:

- **Windows**

```
acd.bat list
```

- **macOS**

```
sudo ./acd.sh list
```

Als Ergebnis erhalten Sie eine Liste aller bekannten Microservices.

> **Beispiel:** Im Folgenden ein Beispiel für den Auth-Microservice. Der Short Name ist die Angabe hinter „`Name`". In diesem Fall „`auth`":
>
> ```
>      Name: auth
>    Memory: 32m/256m
>  Filename: auth-service-app-1.3.0-SNAPSHOT.jar
> Full name: NCJS Auth
>     State: RUNNING
> ```

Mit dem Short Name können Sie nun einen „Einzelbefehl" für den Auth-Microservice absetzen.

> **Beispiel:** Der Microservice mit dem Short Name "Auth" soll über ACD gestoppt werden.

- Windows

```
acd.bat stop auth
```

- macOS

```
sudo ./acd.sh stop auth
```

Befehle

Befehl	Beschreibung
`list`	Listet alle bekannten Microservices mit folgenden Informationen: Name (= Short Name), Speicher, Dateiname, voller Name und Status.
`register`	Registriert einen Microservice als Systemdienst. Der Name (= Short Name) des Microservices muss angegeben werden.
`registerall`	Funktioniert wie der Befehl `register`, wird jedoch für alle bekannten Microservices ausgeführt.
`start`	Startet einen Microservice. Der Name (= Short Name) des Microservices muss angegeben werden. Um den Start-Befehl erfolgreich auszuführen, muss der Microservice bereits registriert sein.
`startall`	Funktioniert wie der Befehl `start`, wird jedoch für alle bekannten Microservices ausgeführt. Um den Start-Befehl erfolgreich auszuführen, müssen die Microservices bereits registriert sein.
`stop`	Stoppt einen Microservice als Systemdienst. Der Name (= Short Name) des Microservices muss angegeben werden.

Befehl	Beschreibung
`stopall`	Funktioniert wie der Befehl `stop`, wird jedoch für alle bekannten Microservices ausgeführt.
`unregister`	Meldet einen Microservice als Systemdienst ab. Der Name (= Short Name) des Microservices muss angegeben werden. Falls der Microservice noch läuft, führt diesen Befehl vor dem `unregister` ein `stop` durch.
`unregisterall`	Funktioniert wie der Befehl `unregister`, wird jedoch für alle bekannten Microservices ausgeführt. Für Microservices, die noch laufen, führt diesen Befehl vor dem `unregister` ein `stop` durch.