

Installation instructions

CENTRUM
Fronius Central User Management



DE | Installationsanleitung



42,0426,0338,DE

003-25052022

Inhaltsverzeichnis

Allgemeines	4
Allgemeines	4
Lizenzvereinbarung.....	4
Sicherheitsanforderungen.....	4
Systemanforderungen.....	5
Systemanforderungen - Server.....	5
Systemanforderungen - Firewall und Netzwerk.....	6
Empfohlene Webbrowser.....	7
CENTRUM installieren und aktivieren	8
Docker Engine installieren und starten.....	8
Server starten.....	8
Erste Schritte	10
Erstmalige Anmeldung.....	10
Administrator anlegen.....	10
Schweißsysteme mit dem CENTRUM-Server verbinden	12
Vor dem Verbinden mit dem CENTRUM-Server	12
Schweißsysteme mittels SmartManager mit dem CENTRUM-Server verbinden	12
Schweißsysteme über das Bedienpanel der Stromquelle mit dem CENTRUM-Server verbinden.....	15
WeldCube Premium mit dem CENTRUM-Server verbinden.....	16
WeldCube Premium mit dem CENTRUM-Server verbinden.....	16
Backup erstellen	18
Übersicht Backup-Möglichkeiten.....	18
Backup während Server-Stopp erstellen.....	18
Backup bei laufendem Server erstellen.....	18
Backup einlesen	19
Update durchführen	20
Update durchführen	20
Spezifische Version verwenden.....	21
Spezifische Version verwenden.....	21

Allgemeines

Allgemeines

CENTRUM = Fronius Central User Management

CENTRUM ist eine Server-basierte Anwendung, die zentral die Benutzereinstellungen mehrerer angeschlossener Schweißsysteme in einer Datenbank verwaltet. Die hierfür erforderliche Hardware oder VM-Konfiguration hängt von der Anzahl der zu verwalteten Geräte ab.

Der Anwender ist für den Betrieb der Hardware oder VM, für die Konfiguration, Lizenzierung und Wartung des empfohlenen Betriebssystems verantwortlich.

Es ist nicht vorgesehen, CENTRUM auf einem einzelnen Desktop-Rechner oder System-PC zu installieren und zu betreiben, beispielsweise in der Produktionshalle.

Um einen reibungslosen Betrieb zu gewährleisten, sollte das Einrichten des Servers (Hardware oder VM), die Konzeption der Netzwerk-Infrastruktur und die Administration nur von der IT-Abteilung des Anwenders durchgeführt werden.

Lizenzvereinbarung

Immer die Lizenzvereinbarung beachten.

Die Lizenzvereinbarung ist zu finden unter:

<https://www.fronius.com/en/welding-technology/terms-conditions-centrum>

Sicherheitsanforderungen

Stets die Vertraulichkeit und Integrität der Daten gewährleisten. Hierfür wie folgt vorgehen:

- 1** Das Hostsystem und die Datensicherung (Backups) vor unerlaubtem Zugriff schützen
- 2** HTTPS verwenden

Systemanforderungen

Systemanforderungen - Server

Physische Hardware:

Prozessor (CPU)	Quad Core 1,2 GHz
Arbeitsspeicher (RAM)	mindestens 4 GB (abhängig vom Betriebssystem und den verbundenen Schweißsystemen)
Grafik	Integrierte Grafikeinheit
Netzwerk	Gigabit Ethernet
Speicher	mindestens 50 GB SSD

Virtual Machine (VM)

Prozessor (CPU)	4 Kerne
Arbeitsspeicher (RAM)	mindestens 4 GB (abhängig vom Betriebssystem und den verbundenen Schweißsystemen)
Grafik	Standard-Grafikadapter
Netzwerk	Gigabit Ethernet
Speicher	mindestens 100 GB SCSI (siehe nachfolgende Tabelle)

Speicher:

Die benötigte Speichergröße ist abhängig von der Anzahl angeschlossener Schweißsysteme und der Anzahl der Benutzer. Die Tabelle zeigt die jeweils empfohlene Speichergröße für Standardinstallationen.

Verwendete Schweißsysteme / Benutzer	Speichergröße
5 / 10	50 GB
50 / 50	55 GB
100 / 100	60 GB
300 / 300	80 GB
500 / 500	100 GB

Unterstützte Betriebssysteme:

Das Central User Management wird als Docker-Image verteilt. Das Docker-Image kann mit einem der nachfolgenden Betriebssysteme verwendet werden.

Linux Servers

Distributionen wie: Debian, Ubuntu, Alpine Linux, Container Linux, RancherOS, Atomic Host, Boot2Docker, Ubuntu Core

Zusätzlich zu den oben angeführten Distributionen können auch weitere Linux-Distributionen verwendet werden, wenn diese die Docker-Anforderungen erfüllen.

Microsoft Windows Server 2019

Mit aktivierter Docker-Umgebung um den Docker-Container auszuführen.

Weitere Informationen unter:

<https://docs.microsoft.com/en-us/virtualization/windowscontainers/quick-start/set-up-environment?tabs=Windows-Server>

Microsoft Windows Server 2022

Mit aktivierter Docker-Umgebung um den Docker-Container auszuführen.

Weitere Informationen unter:

<https://docs.microsoft.com/en-us/virtualization/windowscontainers/quick-start/set-up-environment?tabs=Windows-Server>

Systemanforderungen - Firewall und Netzwerk

Die nachfolgenden Ports und Dienste werden von den jeweiligen Schweißsystemen verwendet für:

- die Verbindung zum Central User Management
- die Konfiguration und Verwaltung der Schweißsysteme

Für den ein- und ausgehenden Datenverkehr eine ordnungsgemäße Firewall- und Netzwerk-Konfiguration sicherstellen.

Verbindung von den Schweißsystemen zu CENTRUM:

Ziel-Server	TCP
Central User Management	4711

Verbindung vom Anwender-PC zu CENTRUM:

Dienst	TCP
HTTP	80
HTTPS (empfohlen)	443

**Empfohlene
Webbrowser**

Webbrowser	Version
Google Chrome	80.0.3987.149
Mozilla Firefox	74.0
Microsoft Edge	101.0.1210.53

WICHTIG! Aus Funktions- und Sicherheitsgründen die neuesten Versionen der empfohlenen Browser verwenden.

CENTRUM installieren und aktivieren

Docker Engine installieren und starten

- 1 Docker Engine herunterladen und installieren

Link zu den Docker Engine Installationsanleitungen:

<https://docs.docker.com/engine/install/>

Für die Installation von Docker Engine auf einem Windows Server wird folgende Anleitung empfohlen:

<https://docs.microsoft.com/en-us/virtualization/windowscontainers/quick-start/set-up-environment?tabs=Windows-Server>

Server starten

Um den Central User Management-Server zu starten, muss zuerst ein Container für das Central User Management angelegt werden.

Der Container greift auf ein definiertes Docker-Volume zu. Das Docker-Volume wird benötigt, um die Datenbank unabhängig vom Container zu speichern und dadurch Server-Updates ohne Datenverlust durchführen zu können.

Der Container verwendet eine HTTPS-Verbindung, um die größtmögliche Sicherheit bei der Kommunikation zwischen Server und Anwender zu gewährleisten.

Für die Verwendung von HTTPS das PFX- oder P12-Zertifikat wie nachfolgend beschrieben in den Container kopieren:

Alle nachfolgenden Befehle in der Shell des Betriebssystems ausführen.

- 1 Den nachfolgenden Befehl zur Anmeldung in der Registry des Central User Management ausführen:

```
docker login registry.pw.fronius.com --username 9432fea2-51d0-4450-a255-702bbe79d2be --password 6f7bda41-b0a2-48f3-b6a2-bbbb8ce754f4
```

- 2 Den nachfolgenden Befehl ausführen, um den Container zu erstellen:

```
docker create --name centrum -p <https-port>:443 -p 4711:4711 -v centrum-data:/<Container-Data-Folder-Path> -e ASPNETCORE_URLS="https://+;http://+" -e ASPNETCORE_HTTPS_PORT=<https-port> -e ASPNETCORE_Kestrel__Certificates__Default__Password=<Certificate-Password> -e ASPNETCORE_Kestrel__Certificates__Default__Path=<Certificate-Path-In-Container> --restart=always registry.pw.fronius.com/centrum
```

Erklärung des Befehls:

<https-port>

der Port, über den die Website des Central User Management erreichbar ist - immer den Port 443 auswählen, da dieser Port auch bei den Schweißsystemen hinterlegt ist und dort nicht verändert werden kann

-p 4711:4711

ein Port-Mapping, welches für die Verbindung zu den Schweißsystemen benötigt wird

-v centrum-data:<Container-Data-Folder-Path>
das Docker-Volume, auf dem die Daten gespeichert werden.

<Container-Data-Folder-Path> ist der Pfad zum Speicherdaten-Ordner des Central User Management-Server.

Linux Container: /data

Windows Container: C:\data

In diesem Beispiel wird das Docker-Volume als „centrum-data“ bezeichnet.

Wird ein Windows-Container verwendet, muss zusätzlich zur Volume-Spezifikation der User als ContainerAdministrator im "create"-Befehl angegeben werden:
--user ContainerAdministrator

<Certificate-Password>
das Passwort, für das PFX- oder P12-Zertifikat

<Certificate-Path-In-Container>
der Pfad, zum Zertifikat im Container.

Windows speichert Zertifikate nicht in einem Ordner, weshalb der Pfad bei Windows frei gewählt werden kann. Beispielsweise:
C:\publish\Certificate.pfx

Für Linux wird folgender Pfad empfohlen:
/etc/ssl/private/Certificate.pfx

- 3** Den nachfolgenden Befehl ausführen, um das Zertifikat in den Container zu kopieren

```
docker cp <Certificate-Path-On-Host> centrum:<Certificate-Path-In-Container>
```

Beispiel für den Pfad auf einem Windows-System:
docker cp C:/Certificate.pfx centrum:/C:\publish\Certificate.pfx

Beispiel für den Pfad auf einem Linux-System:
docker cp /Certificate.pfx centrum:/etc/ssl/private/Certificate.pfx

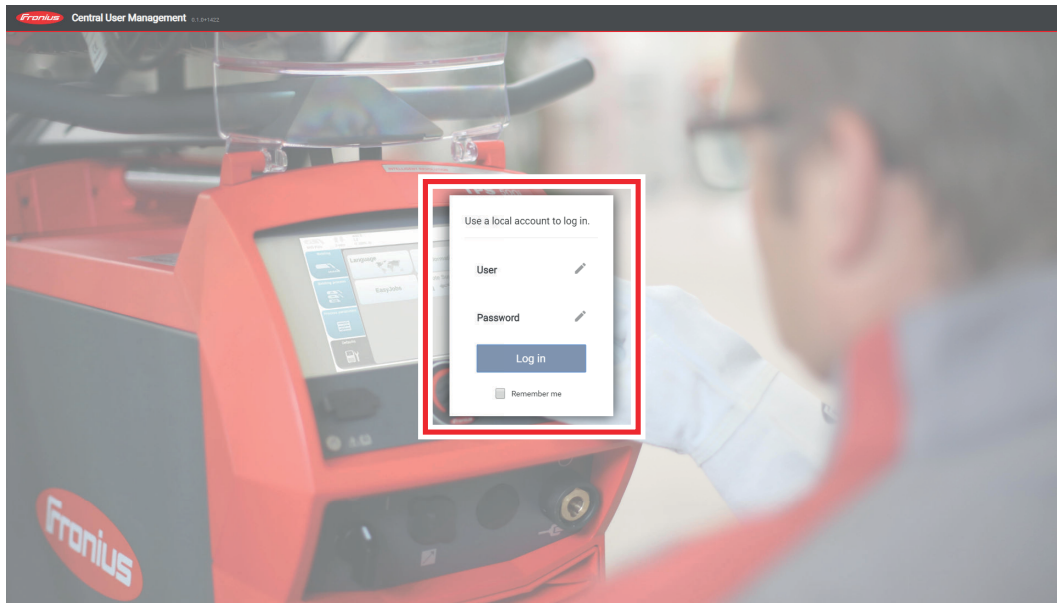
- 4** Den nachfolgenden Befehl ausführen, um den Server zu starten

```
docker start centrum
```

Nun kann über den Browser auf das Central User Management zugegriffen werden.

Erste Schritte

Erstmalige Anmeldung

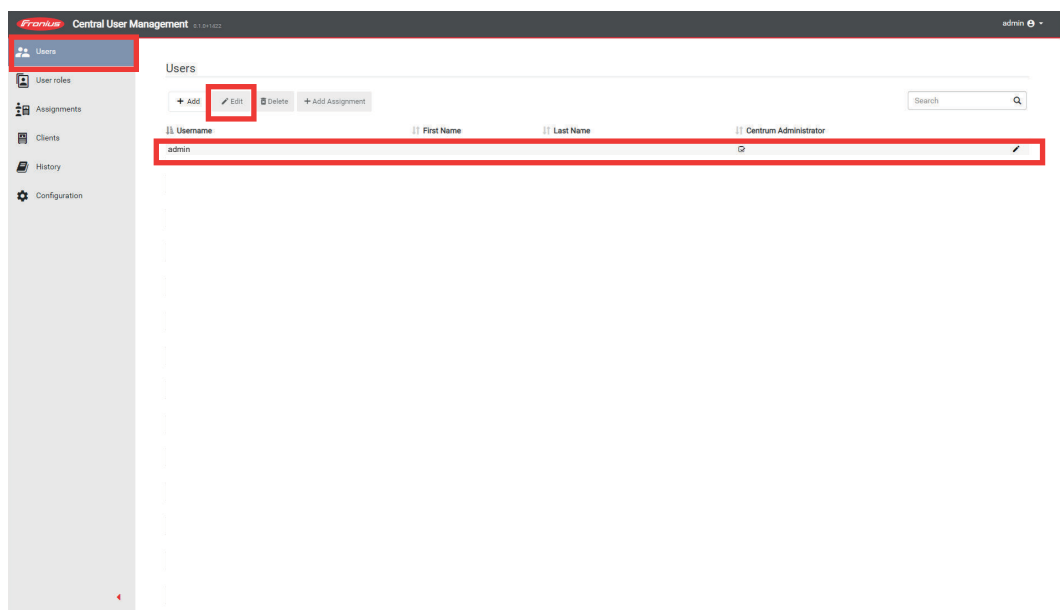


- 1 Die IP-Adresse und den Port des Central User Management-Server im Browser eingeben

das Central User Management wird geöffnet

- 2 Zur Anmeldung die Standard-Login-Daten eingeben:
User: admin
Password: Admin123!!

Administrator anlegen



- 1 Im Central User Management den Reiter „Benutzer“ auswählen
- 2 Den Benutzer admin auswählen (dieser wurde bei der Installation automatisch erstellt)
- 3 Den Benutzer admin bearbeiten

The screenshot shows the 'User' configuration page in the Fronius Central User Management system. The left sidebar contains navigation links: Users, User roles, Assignments, Clients, History, and Configuration. The main area displays the configuration for a user named 'admin'. Fields include Username (admin), First Name, Last Name, System of Units (Metric), Welding Standard (AWS), Language (English), and NFC Card (highlighted with a red rectangle). Below these are toggle switches for 'Centrum Administrator' (On) and 'Allow concurrent sessions to multiple power sources' (Off). A 'Password' field with a masked input and a 'Change Password' button are at the bottom. 'Cancel' and 'Save' buttons are at the very bottom.

- 4 Im Feld „NFC-Karte“ die Nummer des jeweiligen NFC-Key (NFC-Karte, NFC-Schlüsselanhänger, ...) hinterlegen und die Eingabe speichern

WICHTIG! Diesen NFC-Key vor unbefugtem Zugriff schützen, da mit diesem NFC-Key auf alle Stromquellen zugegriffen werden kann.

This screenshot shows the same 'User' configuration page, but now the 'Password' field is highlighted with a red rectangle. The 'NFC Card' field is no longer highlighted. All other elements, including the sidebar, user details, and toggle switches, remain the same as in the previous screenshot.

- 5 Im Feld „Passwort“ ein neues Passwort hinterlegen
- 6 Einstellungen speichern

Schweißsysteme mit dem CENTRUM-Server verbinden

Vor dem Verbinden mit dem CENTRUM-Server

HINWEIS!

Bevor Schweißsysteme oder WeldCube Premium mit dem CENTRUM-Server verbunden werden, zuerst sämtliche Benutzer, Benutzerrollen, Client-Gruppen und Verweise auf diese Client-Gruppen in CENTRUM konfigurieren!

Andernfalls sind die Systeme über den „admin user“ gesperrt bis, die Konfiguration in CENTRUM abgeschlossen ist.

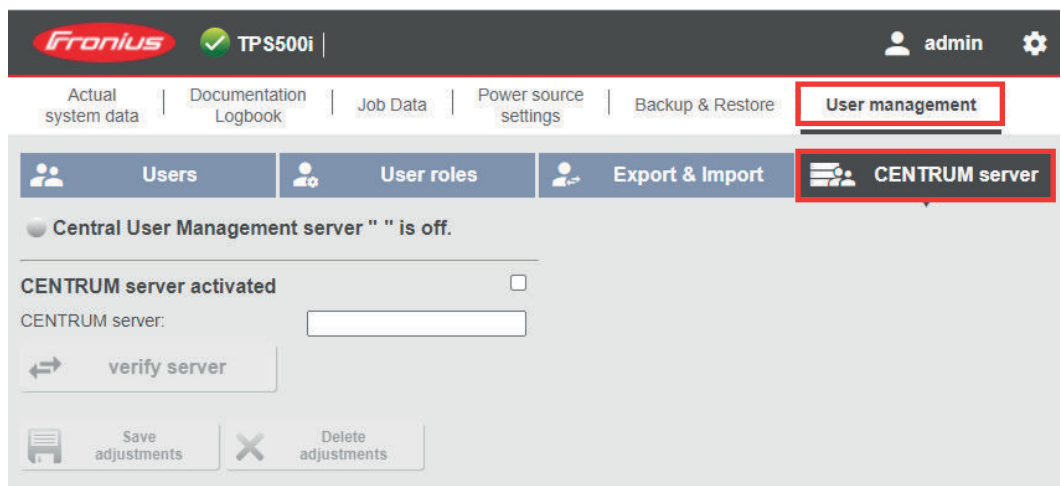
Korrekte Reihenfolge:

- ▶ CENTRUM installieren
- ▶ Konfigurieren, User einrichten
- ▶ System mit CENTRUM verbinden

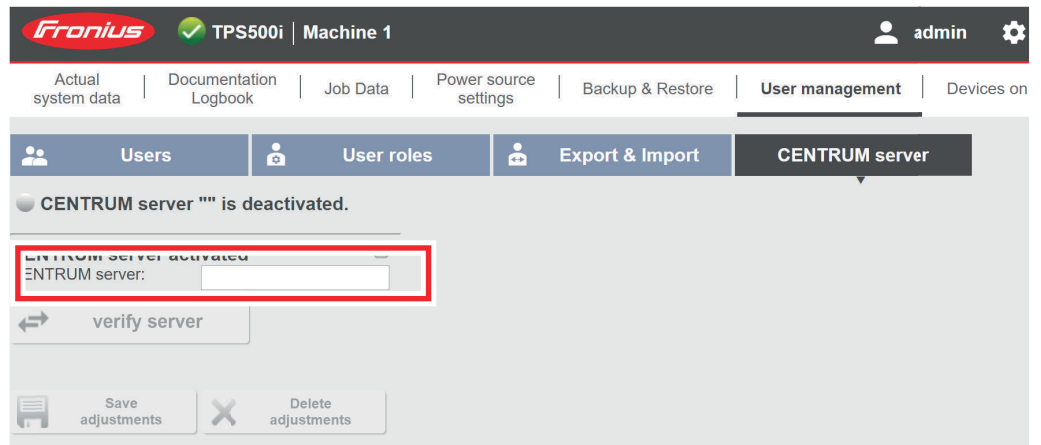
Schweißsysteme mittels Smart-Manager mit dem CENTRUM-Server verbinden

Voraussetzung:

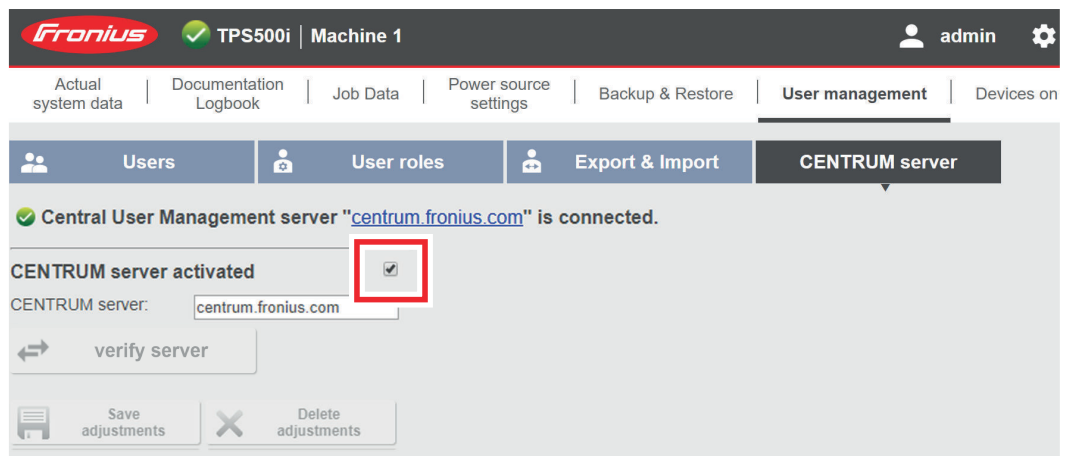
Die Stromquelle des Schweißsystems muss mittels Netzwerk-Kabel mit einem Computer verbunden oder in einem Netzwerk integriert sein.



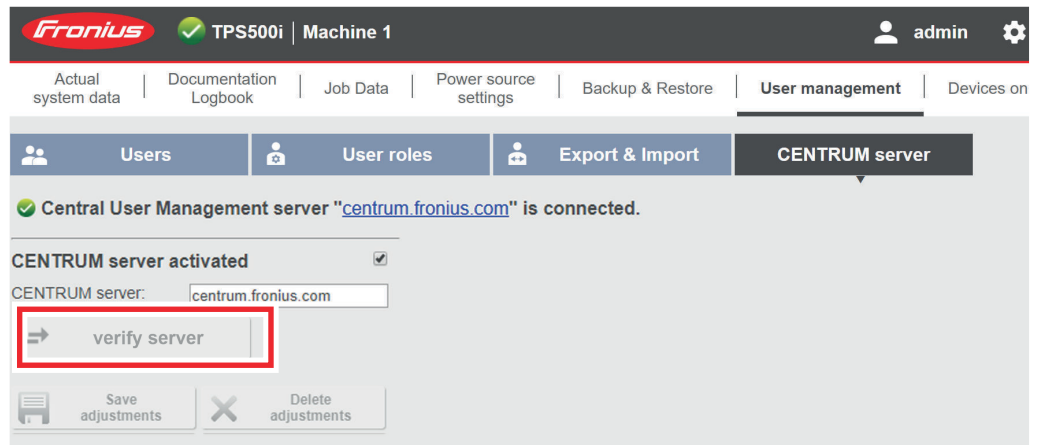
- 1** IP-Adresse der gewünschten Stromquelle im Browser eingeben, den Smart-Manager öffnen und anmelden
- 2** Den Reiter für das User Management auswählen
- 3** Den Reiter für den CENTRUM Server auswählen



- 4 Im markierten Eingabefeld den Domain-Namen oder die IP-Adresse des Servers angeben, auf dem das Central User Management installiert wurde (wenn ein Domain-Name verwendet wird, muss bei den Netzwerkeinstellungen der Stromquelle ein gültiger DNS-Server konfiguriert sein)



- 5 Die markierte Schaltfläche anwählen



6 Die markierte Schaltfläche anklicken

Die Verfügbarkeit des angegebenen Servers wird überprüft.
Ist der angegebene Server erreichbar, erscheint die Anzeige „Server verified“.

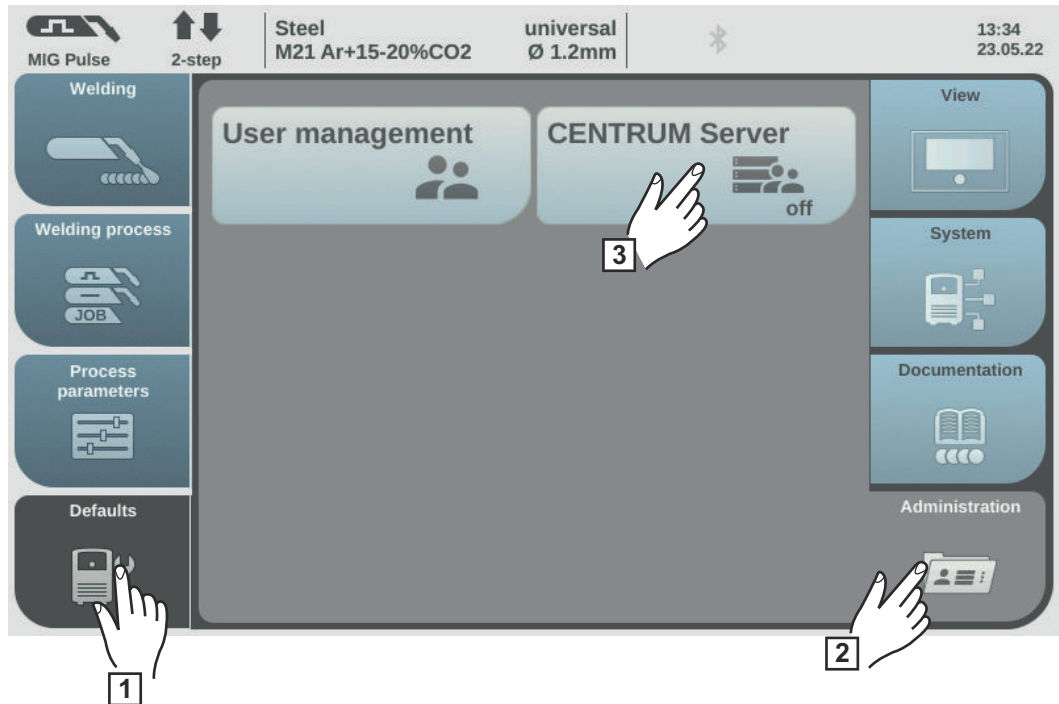
7 Änderungen speichern

Die Stromquelle wird im Central User Management angezeigt.

8 Auf die gleiche Weise alle weiteren Stromquellen in das Central User Management integrieren

Schweißsysteme über das Bedien- panel der Strom- quelle mit dem CENTRUM-Ser- ver verbinden

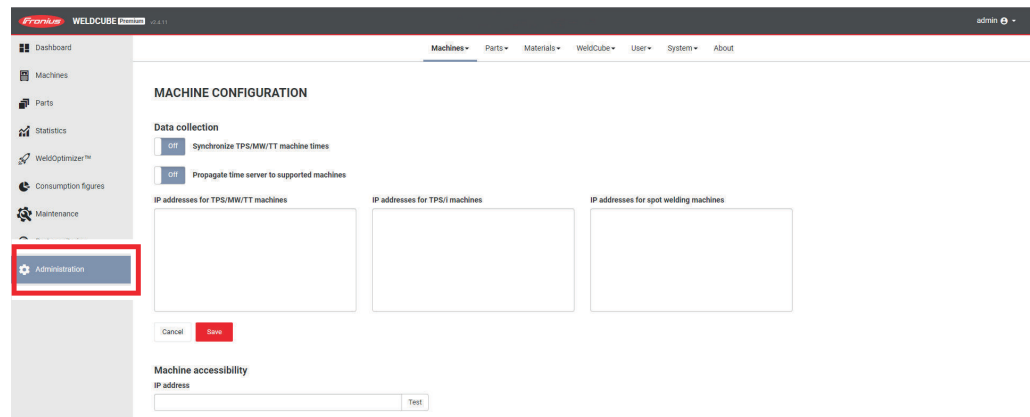
Eine Stromquelle kann auch über das Bedienpanel mit dem CENTRUM-Server verbunden werden.



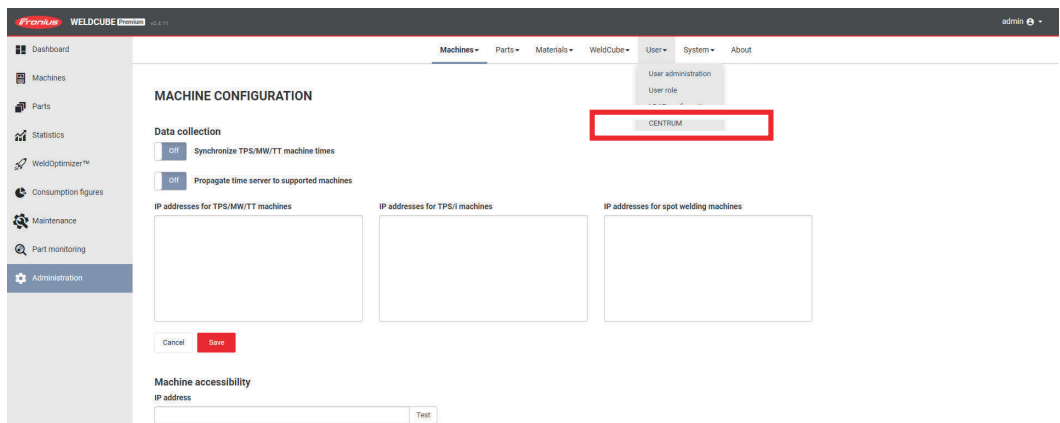
- 1 Voreinstellungen auswählen
- 2 Administration auswählen
- 3 CENTRUM Server auswählen
- 4 CENTRUM Server aktivieren
- 5 CENTRUM Server eintragen
- 6 CENTRUM verifizieren
- 7 Speichern

WeldCube Premium mit dem CENTRUM-Server verbinden

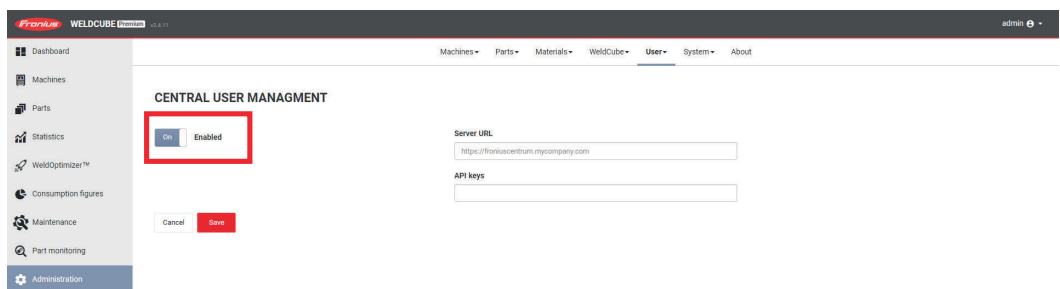
WeldCube Premium mit dem CENTRUM-Server verbinden



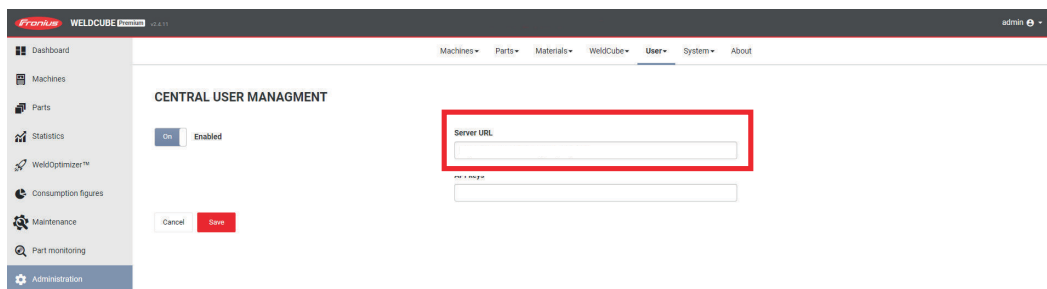
- 1 WeldCube Premium im Browser öffnen
- 2 Den Reiter für die Administration auswählen



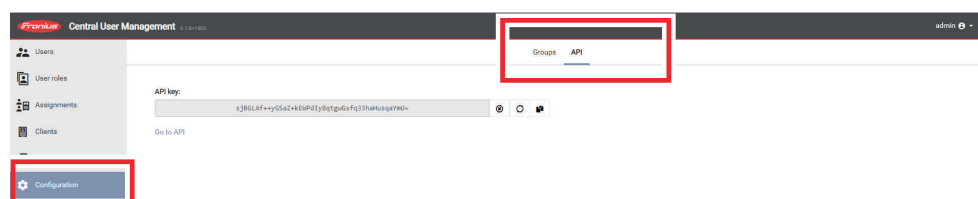
- 3 Das Benutzer-Menü aufklappen und CENTRUM auswählen



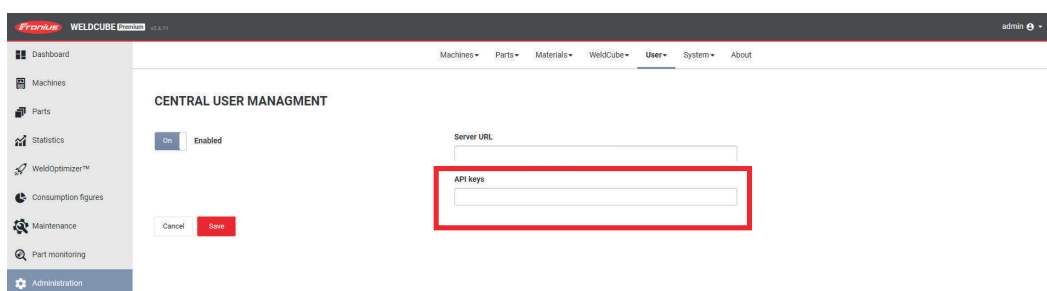
- 4 Central User Management aktivieren



- 5 Die URL des Central User Management eingeben



- 6 Das Central User Management in einem zusätzlichen Browser-Fenster öffnen
- 7 Den Reiter für die Konfiguration auswählen
- 8 API auswählen
- 9 Den API-Schlüssel des Central User Management kopieren



- 10 WeldCube Premium im bestehenden Browser-Fenster wieder öffnen
- 11 Den API-Schlüssel des Central User Management einfügen
- 12 Eingaben speichern

Der WeldCube Premium wird im Central User Management angezeigt.

- 13 Auf die gleiche Weise alle weiteren WeldCube Premium zum Central User Management hinzufügen

Backup erstellen

Übersicht Backup-Möglichkeiten

- Für das Erstellen eines Server-Backups stehen 2 Möglichkeiten zur Verfügung
- Möglichkeit 1 = Server stoppen und Daten kopieren (verfügbar für Windows und Linux)
 - Möglichkeit 2 = Daten im laufenden Betrieb kopieren (verfügbar für Linux)

Die genaue Vorgehensweise wird nachfolgend beschrieben.

Backup während Server-Stopp erstellen

Die nachfolgend beschriebene Vorgehensweise funktioniert bei Windows und Linux.

In der Shell des Servers die nachfolgenden Befehle ausführen.

- 1** Server stoppen:
`docker stop centrum`
- 2** Daten vom Server auf das Host-System kopieren:
`docker cp centrum: /<Container-Data-Folder-Path> <Destination-on-host-system>`

Der String <Destination-on-host-system> führt zum Speicherort für das Backup.

Beispielsweise `C:\backup\centrum\`

Backup bei laufendem Server erstellen

Die nachfolgend beschriebene Vorgehensweise funktioniert nur bei Linux.

- 1** SQLite CLI installieren

Alle nachfolgenden Befehle in Shell ausführen.

- 2** Den Pfad zum Docker-Volume ermitteln:
`docker volume inspect centrum-data`

Beim Eintrag Mountpoint wird der Pfad zum Docker-Volume angezeigt, beispielsweise: `/var/lib/docker/volumes/centrum-data/_data/`

- 3** Die Datenbank kopieren (der Befehl kopiert nicht alle Daten, sondern nur die Datenbank):
`sqlite3 <docker-volume-path>/centrum.db ".backup <Destination-on-host-system>/centrum.db"`
 - statt <docker-volume-path> den Pfad zum Docker-Volume anführen
 - Der String <Destination-on-host-system> führt zum Speicherort für das Backup.
Beispielsweise `/var/backups/centrum/`
- 4** Alle Daten auflisten, welche sich im gleichen Verzeichnis wie die Datenbank befinden:
`ls <docker-volume-path>`
 - `centrum.db` wird angezeigt
 - `speednet.cert` wird angezeigt
 - ...

- 5** Die Datei speednet.cert kopieren:
cp <docker-volume-pfad>/speednet.cert <path-of-backup>/speednet.cert
 - mit diesem Befehl können alle Daten in dem Verzeichnis kopiert werden
 - für das Kopieren weiterer Daten den Dateinamen ersetzen (in diesem Beispiel statt speednet.cert den neuen Dateinamen einsetzen)
-

Backup einlesen

- 1** Server stoppen:
docker stop centrum
- 2** Backup-Daten in das gewünschte Verzeichnis kopieren:
docker cp <Destination-on-host-system> centrum:<Container-Data-Folder-Path>
- 3** Server neu starten:
docker start centrum

Update durchführen

Update durchführen

- 1** Central User Management Server-Backup erstellen - siehe [Übersicht Backup-Möglichkeiten](#) auf Seite **18**
- 2** Mit der Shell des Betriebssystems den nachfolgenden Befehl ausführen, um den bestehenden Container des Central User Management zu löschen:
`docker rm -f <container-name>`
- 3** Mit der Shell des Betriebssystems den nachfolgenden Befehl ausführen, um das bestehende CENTRUM Server-Image zu aktualisieren:
`docker pull registry.pw.fronius.com/centrum`
- 4** Den Central User Management-Server erneut starten - siehe [Server starten](#) ab Seite **8**

Zum Starten des Central User Management-Server das Docker-Volume verwenden.

Spezifische Version verwenden

Spezifische Version verwenden

Je nach Anforderung, kann das Central User Management in jeder verfügbaren Version gestartet werden. Hierfür den Befehl für die Erstellung des Central User Management-Containers wie nachfolgend beschrieben ändern.

Befehl für die Erstellung des Central User Management-Containers:

```
docker create --name centrum -p <https-port>:443 -p 4711:4711 -v
centrum-data:/<Container-Data-Folder-Path> -e ASPNETCORE_
URLS="https://+;http://+" -e ASPNETCORE_HTTPS_PORT=<https-
port> -e ASPNETCORE_Kestrel__Certificates__Default__Password=
<Certificate-Password> -e ASPNETCORE_Kestrel__Certificates__
Default__Path=<Certificate-Path-In-Container> --restart=always
registry.pw.fronius.com/centrum
```

Befehl wie folgt ändern um eine spezifische Version zu verwenden:

- 1 den String registry.pw.fronius.com/centrum ersetzen durch:
registry.pw.fronius.com/centrum:<version-number>

statt <version-number> die gewünschte Central User Management-Version eingeben (beispielsweise 1.0.0)



Fronius International GmbH

Froniusstraße 1
4643 Pettenbach
Austria
contact@fronius.com
www.fronius.com

Under www.fronius.com/contact you will find the addresses
of all Fronius Sales & Service Partners and locations.