Installation instructions

CENTRUM
Fronius Central User Management

EN-US | Installation instructions

42,0426,0338,EA 003-08062022

Table of contents

General 4
- General 4
- License Agreement 4
- Safety Requirements 4

System requirements 5
- System requirements – server 5
- System requirements – firewall and network 6
- Recommended web browsers 7

Installing and activating CENTRUM 8
- Installing and starting the Docker engine 8
- Starting the server 8

Initial Steps 10
- Logging in for the first time 10
- Adding an administrator 10

Connecting welding systems to the CENTRUM server 12
- Before connecting to the CENTRUM server 12
- Connecting welding systems to the CENTRUM server via SmartManager 12
- Connecting welding systems to the CENTRUM server via the control panel of the power source 15

Connecting WeldCube Premium to the CENTRUM server 16
- Connecting WeldCube Premium to the CENTRUM server 16

Creating a Backup 18
- Overview of backup options 18
- Creating a backup while the server is stopped 18
- Creating a backup while the server is running 18
- Loading the backup 19

Installing the Update 20
- Performing the update 20

Using Specific Versions 21
- Using specific versions 21

General

General

CENTRUM = Fronius Central User Management

CENTRUM is a server-based application that centrally manages the user settings of several connected welding systems in a database.
The hardware or VM configuration required for this depends on the number of devices to be managed.
The user is responsible for the operation of the hardware or VM, and for the configuration, licensing, and maintenance of the recommended operating system.

It is not intended for CENTRUM to be installed and operated on a single desktop computer or system PC, for example in a production hall.

To ensure smooth operation, the setup of the server (hardware or VM), the design of the network infrastructure, and administration should only be performed by the user's IT department.

License Agreement

The license agreement must always be observed.

The license agreement can be found at:
https://www.fronius.com/en/welding-technology/terms-conditions-centrum

Safety Requirements

The confidentiality and integrity of the data must be ensured at all times. To do this, proceed as follows:

1 Protect the host system and the data backups against unauthorized access

2 Use HTTPS

System requirements

System requirements – server

Physical hardware:

Processor (CPU)	Quad Core 1.2 GHz
Memory (RAM)	At least 4 GB (depending on the operating system and the connected welding systems)
Graphics	Integrated graphics unit
Network	Gigabit Ethernet
Storage	At least 50 GB SSD

Virtual Machine (VM)

Processor (CPU)	4 cores
Memory (RAM)	At least 4 GB (depending on the operating system and the connected welding systems)
Graphics	Standard graphics card
Network	Gigabit Ethernet
Storage	At least 100 GB SCSI (see table below)

Storage:
The required memory size depends on the number of connected welding systems and the number of users. The table shows the respective recommended memory size for standard installations.

Welding systems used / users	Memory size
5 / 10	50 GB
50 / 50	55 GB
100 / 100	60 GB
300 / 300	80 GB
500 / 500	100 GB

Supported operating systems:
Central User Management is distributed as a Docker image. The Docker image can be used with one of the following operating systems.

Linux servers
Distributions like: Debian, Ubuntu, Alpine Linux, Container Linux, RancherOS, Atomic Host, Boot2Docker, Ubuntu Core

In addition to the distributions listed above, other Linux distributions can be used if they meet the Docker requirements.

Microsoft Windows Server 2019
With Docker environment enabled to run the Docker container.

For more information, see:

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

Microsoft Windows Server 2022
With Docker environment enabled to run the Docker container.

For more information, see:

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

System requirements – firewall and network

The following Ports and services are used by the respective welding systems for:
- the connection to Central User Management
- the configuration and management of the welding systems

Ensure proper firewall and network configuration for incoming and outgoing data traffic.

Connection from the welding systems to CENTRUM:

Target server	TCP
Central User Management	4711

Connection from the user PC to CENTRUM:

Service	TCP
HTTP	80
HTTPS (recommended)	443

Recommended web browsers

Web browser	Version
Google Chrome	80.0.3987.149
Mozilla Firefox	74.0
Microsoft Edge	101.0.1210.53

IMPORTANT! For functional and security reasons, use the latest versions of the recommended browsers.

Installing and activating CENTRUM

Installing and starting the Docker engine

1 Download and install the Docker engine

Link to the Docker engine Installation Instructions:
https://docs.docker.com/engine/install/

The following instructions are recommended for installing the Docker engine on a Windows server:

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

Starting the server

To start the Central User Management server, you must first create a container for Central User Management.

The container uses a defined Docker volume. The Docker volume is required in order to save the database independently of the container and thus enable server updates to be carried out without any loss of data.

The container uses a HTTPS connection in order to ensure the highest possible level of security during communication between the server and user.

In order to use HTTPS, copy the PFX or P12 certificate into the container as described below:

Run all of the following commands in the Shell of the operating system.

1 Run the following command to log into the Registry of Central User Management:

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

2 Run the following command in order to create the container:

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

Explanation of the command:

<https-port>
The Port via which the Website of Central User Management can be accessed - always select Port 443, as this Port is stored on the welding systems and cannot be changed from there

-p 4711:4711
Port mapping that is required for connecting to the welding systems

-v centrum-data:<Container-Data-Folder-Path>
The Docker volume where the data are stored.

<Container-Data-Folder-Path> is the path for the storage data folder of the Central User Management server.

Linux container: /data
Windows container: C:\data

In this example, the Docker volume is named "centrum-data".

If a Windows container is used, in addition to the volume specification, the user must be specified as the ContainerAdministrator in the "create" command:
--user ContainerAdministrator

<Certificate-Password>
The password for the PFX or P12 certificate

<Certificate-Path-In-Container>
The path for the certificate in the container

Windows does not store certificates in a folder, which is why the path can be freely selected in Windows. For example:
C:\publish\Certificate.pfx

For Linux the following path is recommended:
/etc/ssl/private/Certificate.pfx

---

3 Run the following command to copy the certificate to the container

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

Example of the path on a Windows system:
docker cp C:/Certificate.pfx centrum:/C:\publish\Certificate.pfx

Example of the path on a Linux system:
docker cp /Certificate.pfx centrum:/etc/ssl/private/Certificate.pfx

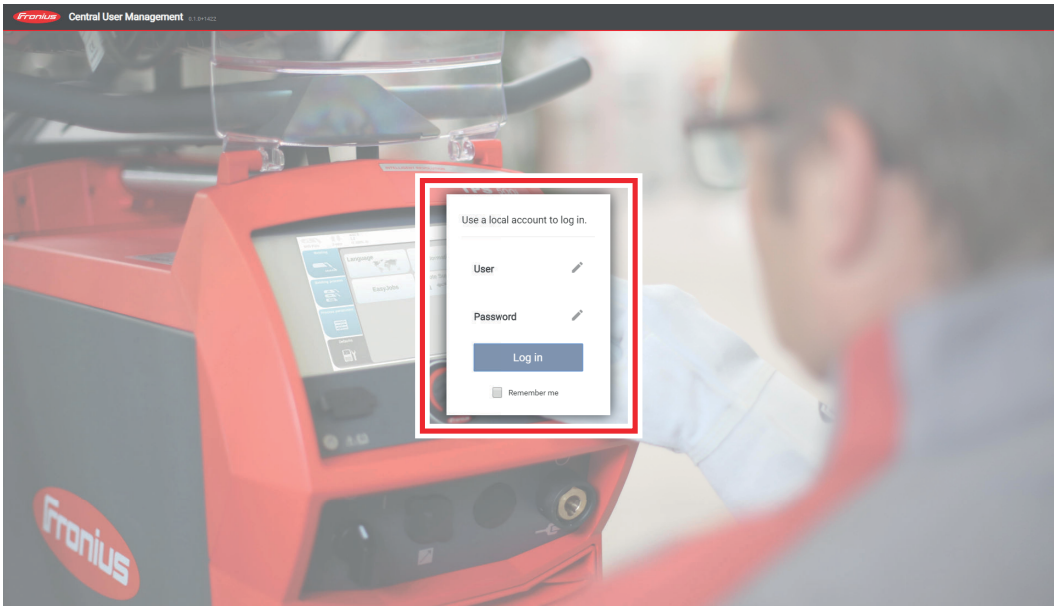
4 Run the following command in order to start the server

docker start centrum

The browser can now be used to access Central User Management.

Initial Steps

Logging in for the first time

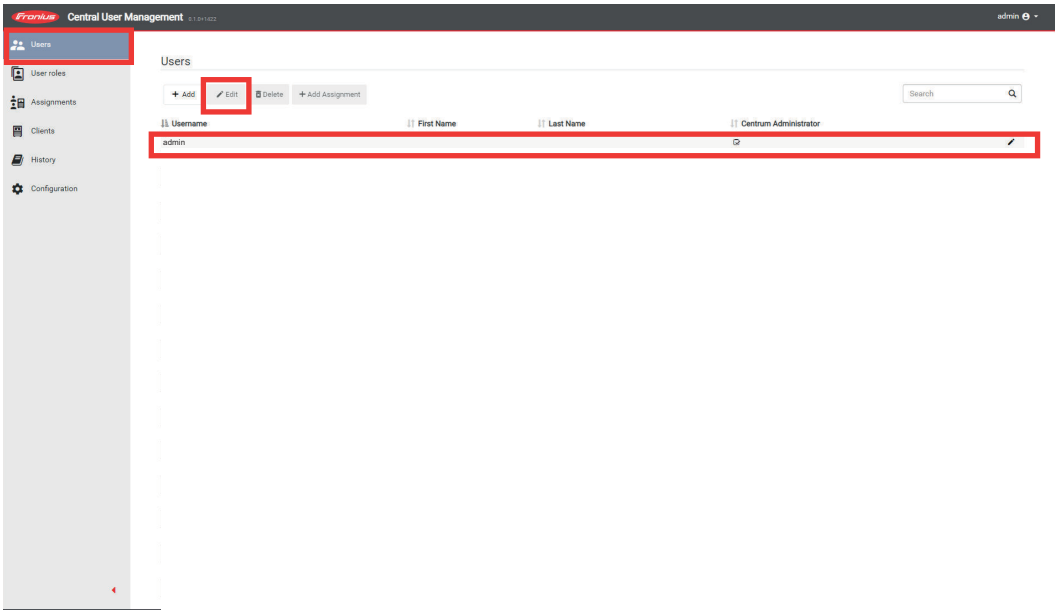


1 Enter the IP address and the port of the Central User Management server into the browser

Central User Management is opened

2 Log in using the standard login details:
User: admin
Password: Admin123!!

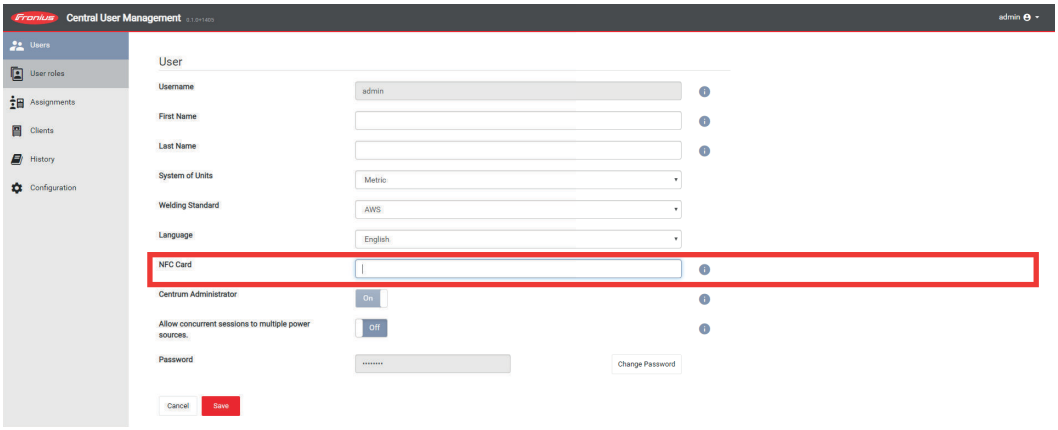
Adding an administrator



1 Select the "Users" tab in Central User Management

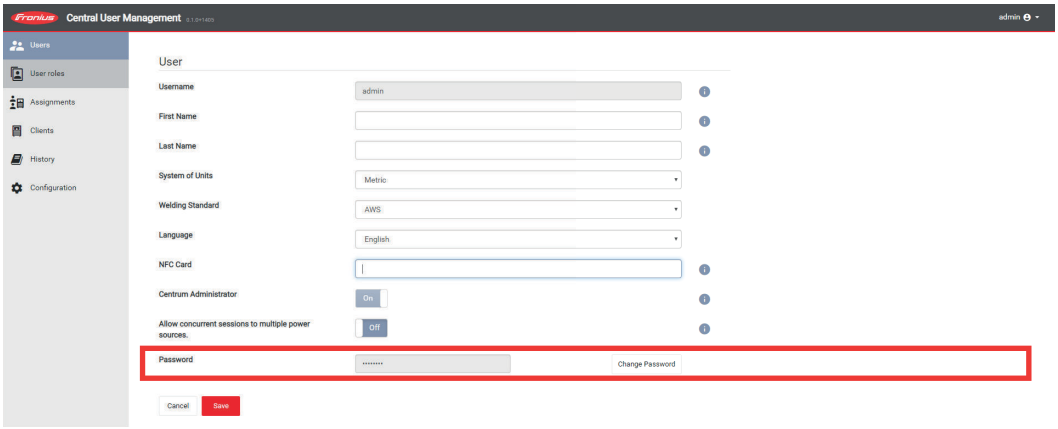
2 Select the admin user (automatically created during installation)

3 Edit the admin user



4 In the "NFC Card" field, enter the number of the appropriate NFC-Key (NFC card, NFC key fob, etc.) and save this information

IMPORTANT! Protect this NFC-Key against unauthorized access as this NFC-Key can be used to access all of the power sources.



5 Enter a new password in the "Password" field

6 Save the settings

Connecting welding systems to the CENTRUM server

Before connecting to the CENTRUM server

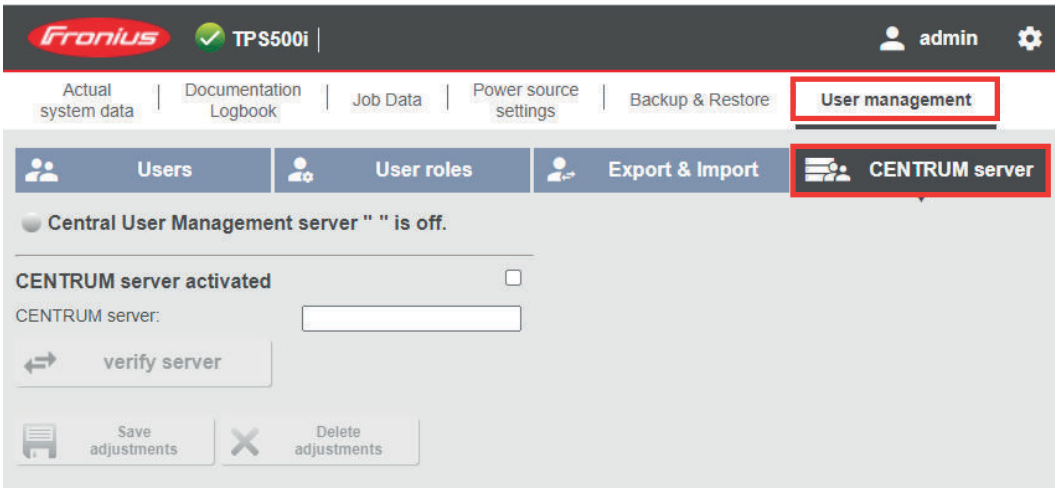
NOTE!

Before connecting welding systems or WeldCube Premium to the CENTRUM server, first configure all users, user roles, client groups, and references to these client groups in CENTRUM!
Otherwise, the systems are locked via the "admin user" until configuration in CENTRUM is completed.

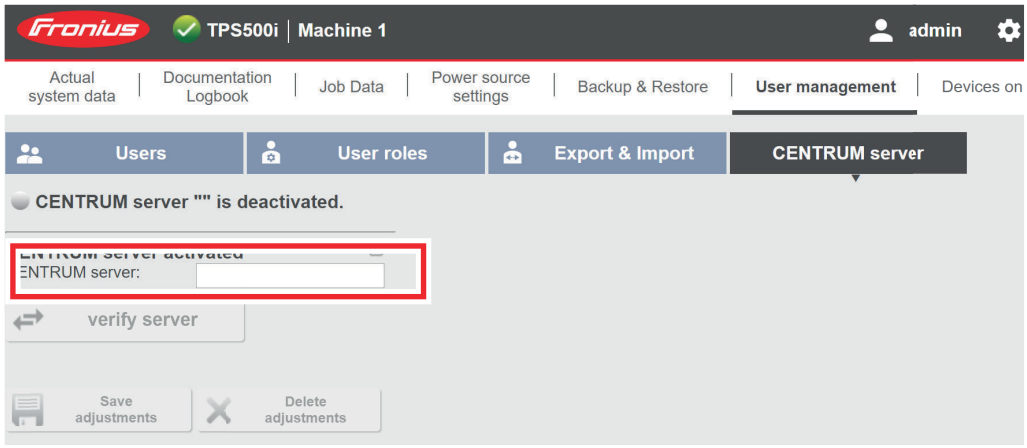
Correct sequence:
- ▶ Install CENTRUM
- ▶ Configure, set up users
- ▶ Connect system to CENTRUM

Connecting welding systems to the CENTRUM server via SmartManager

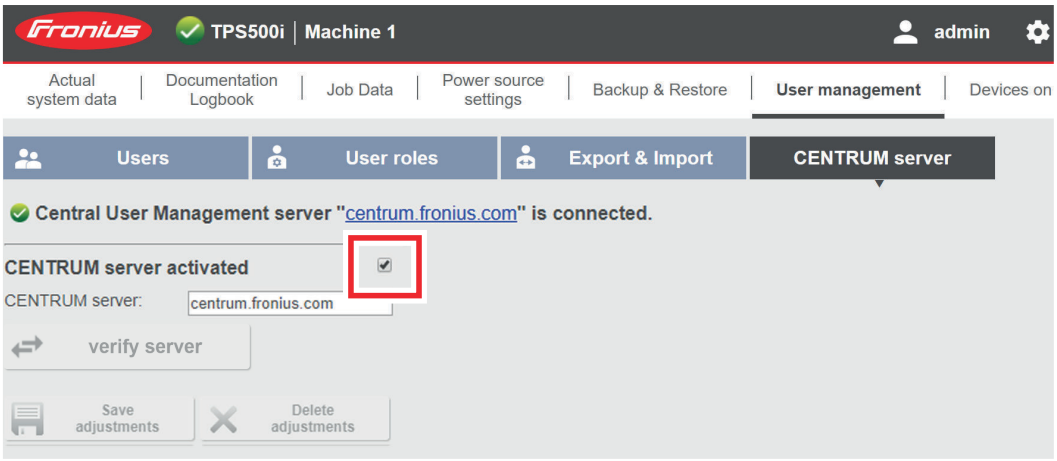
Prerequisite:
The power source of the welding system must be connected to a computer via network cable or integrated in a network.



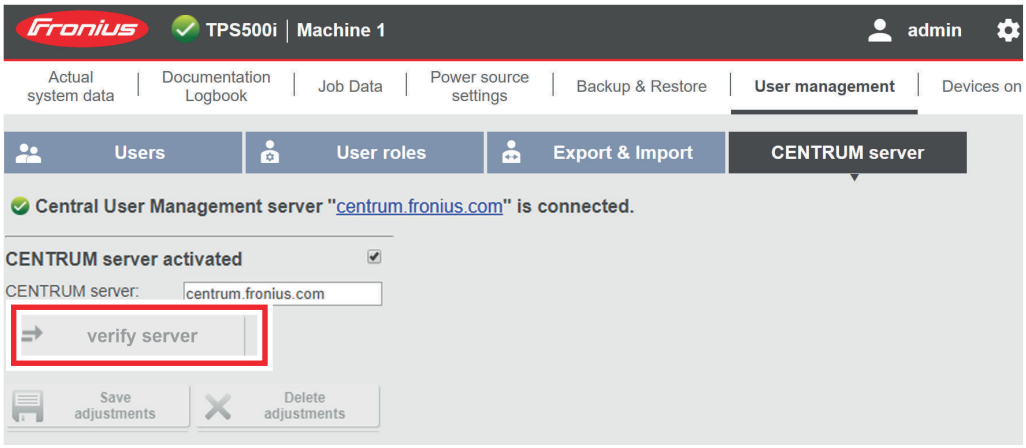
1. Enter the IP address of the desired power source into the browser, open SmartManager and log in
2. Select the User Management tab
3. Select the CENTRUM server tab



4 In the input field highlighted, enter the domain name or the IP address of the server on which Central User Management has been installed (if using a domain name, a valid DNS server must be configured in the network settings of the power source)



5 Check the box highlighted



6 Click on the highlighted button

The availability of the specified server is checked.
If the specified server is available, "Server verified" appears.

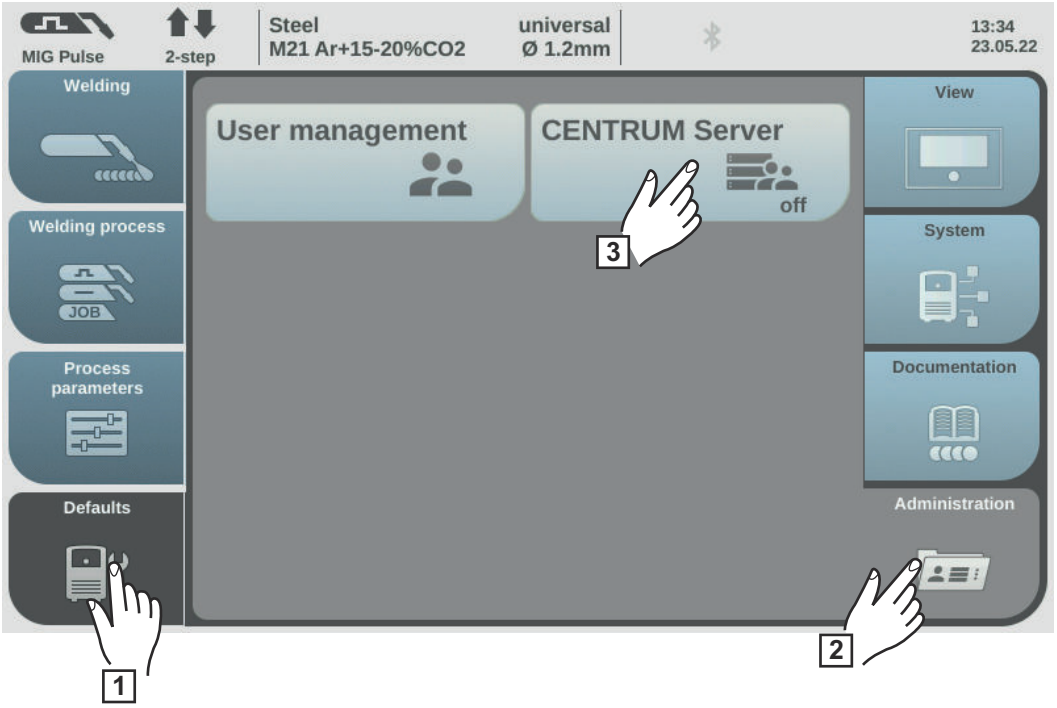
7 Save the changes

The power source is displayed in Central User Management.

8 Integrate all subsequent power sources into Central User Management in the same way

Connecting welding systems to the CENTRUM server via the control panel of the power source

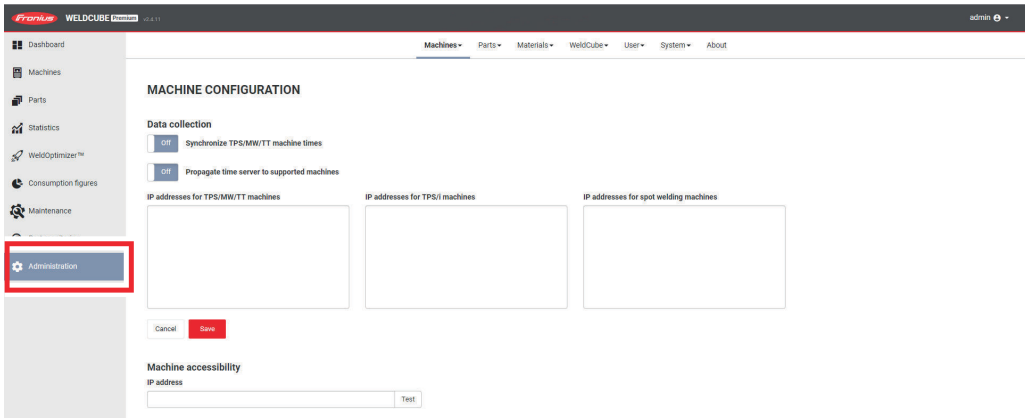
A power source can also be connected to the CENTRUM server via the control panel.



1 Select "Defaults"
2 Select "Administration"
3 Select CENTRUM Server
4 Activate CENTRUM Server
5 Enter the CENTRUM Server
6 Verify CENTRUM
7 Save

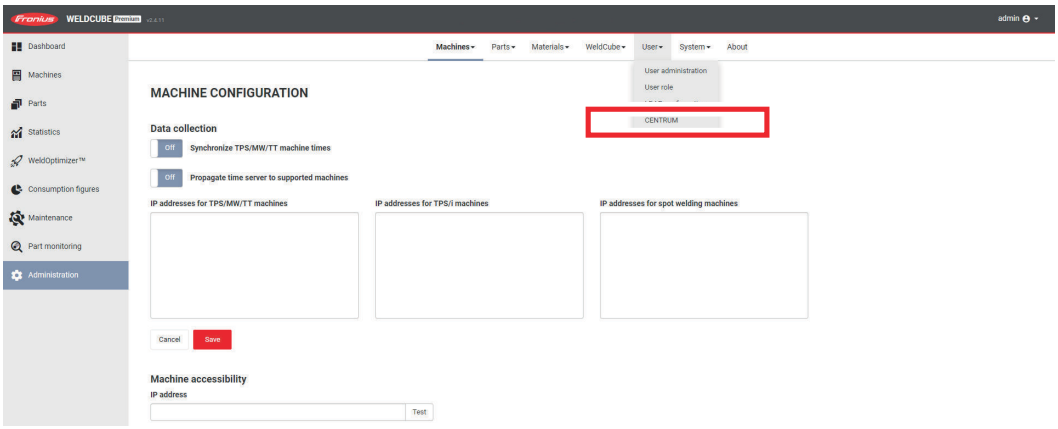
Connecting WeldCube Premium to the CENTRUM server

Connecting WeldCube Premium to the CENTRUM server

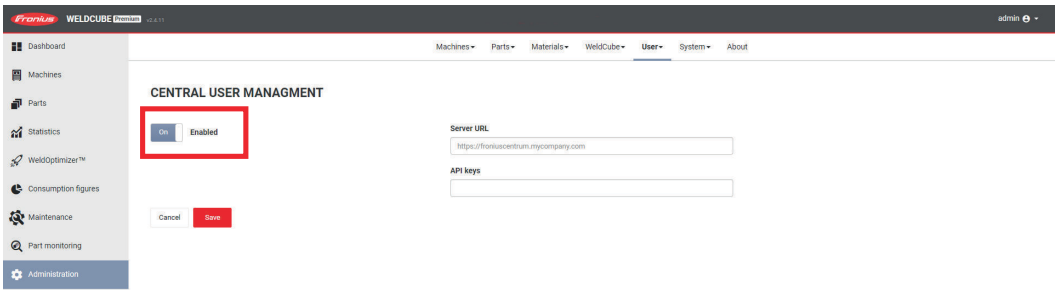


1 Open WeldCube Premium in the browser

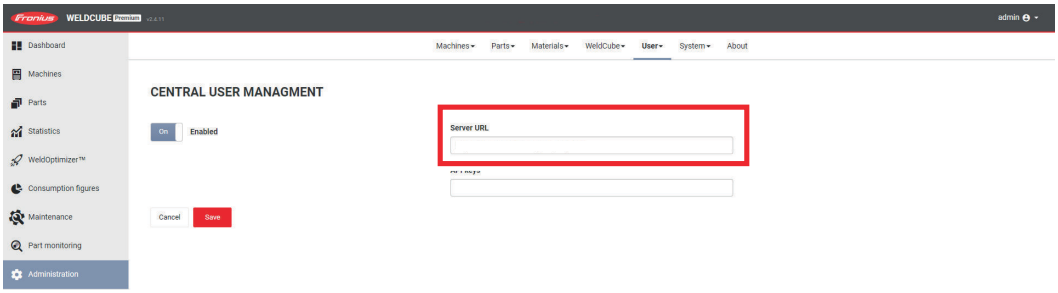
2 Select the "Administration" tab



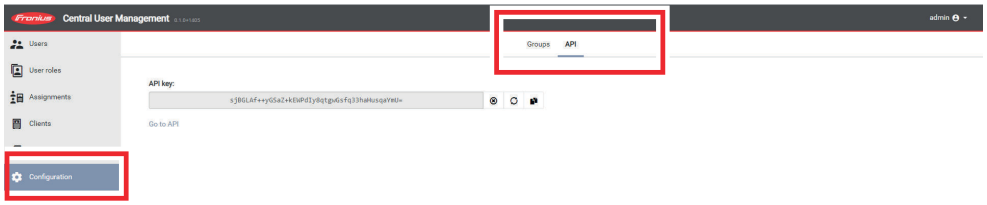
3 Expand the "User" menu and select CENTRUM



4 Enable Central User Management



5 Enter the URL of Central User Management

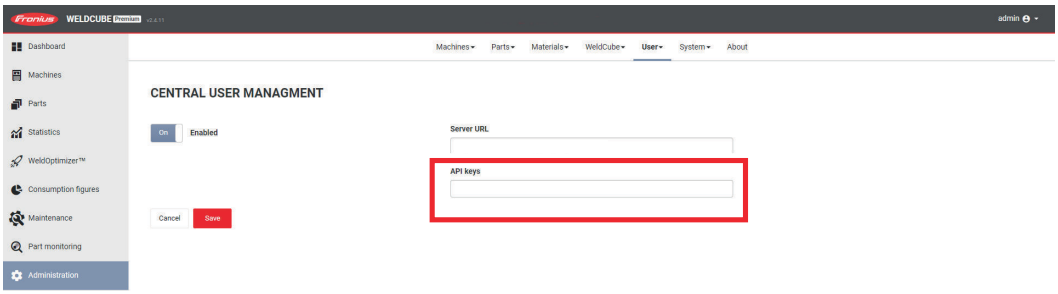


6 Open Central User Management in a separate browser window

7 Select the "Configuration" tab

8 Select API

9 Copy the API key from Central User Management



10 Reopen WeldCube Premium in the current browser window

11 Enter the API key from Central User Management

12 Save the entries

The WeldCube Premium is displayed in Central User Management.

13 Add all subsequent WeldCube Premium accounts to Central User Management in the same way

Creating a Backup

Overview of backup options

There are two available options for creating a server backup
- Option 1 = Stop the server and copy the data (available for Windows and Linux)
- Option 2 = Copy data during operation (available for Linux)

The precise procedure is described below.

Creating a backup while the server is stopped

The procedure described below applies to Windows and Linux.

Run the following commands in the Shell of the server.

1 Stop the server:
docker stop centrum

2 Copy data from the server to the host system:
docker cp centrum:/<Container-Data-Folder-Path> <Destination-on-host-system>

The <Destination-on-host-system> string leads to the storage location for the backup.
For example, C:\backup\centrum\

Creating a backup while the server is running

The procedure described below only applies to Linux.

1 Install SQLite CLI

Run all of the following commands in Shell.

2 Get the path to the Docker volume:
docker volume inspect centrum-data

Upon entering Mountpoint, the path for the Docker volume is displayed, for example: /var/lib/docker/volumes/centrum-data/_data/

3 Copy the database (the command does not copy all data, but only the database):
sqlite3 <docker-volume-path>/centrum.db ".backup <Destination-on-host-system>/centrum.db"
- Instead of <docker-volume-path>, enter the path for the Docker volume
- The <Destination-on-host-system> string leads to the storage location for the backup.
  For example, /var/backups/centrum/

4 List all of the data that appear in the same directory as the database:
ls <docker-volume-path>
- centrum.db is displayed
- speednet.cert is displayed
- ...

5 Copy the speednet.cert file:
cp <docker-volume-path>/speednet.cert <path-of-backup>/speednet.cert
- This command can be used to copy all of the data in the directory
- In order to copy additional data, replace the file name (in this example, instead of speednet.cert , insert the new file name)

Loading the backup

1 Stop the server:
docker stop centrum

2 Copy the backup data to the desired directory:
docker cp <Destination-on-host-system> centrum:<Container-Data-Folder-Path>

3 Restart the server:
docker start centrum

Installing the Update

Performing the update

1. Create a Central User Management server backup - see **Overview of backup options** on page **18**
2. Using the Shell of the operating system, run the following command in order to delete the existing container for Central User Management:
   docker rm -f <container-name>
3. Using the Shell of the operating system, run the following command in order to update the existing CENTRUM server image:
   docker pull registry.pw.fronius.com/centrum
4. Restart the Central User Management server - see **Starting the server** from page **8**

   Use the Docker volume to start the Central User Management server.

Using Specific Versions

Using specific versions

Depending on the user's requirements, Central User Management can be started in any available version. In order to do this, adapt the command used to create the Central User Management container as described below.

Command used to create the Central User Management container:

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

Adapt the command as follows in order to use a specific version:

1 Replace the registry.pw.fronius.com/centrum string with: registry.pw.fronius.com/centrum:<version-number>

   Instead of <version-number>, enter the desired Central User Management version (for example 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.