Remote-I/O-System u-remote
Web server manual

Weidmüller

Content

Manufacturer

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
www.weidmueller.com

Document No. 2112220000
Revision 08/February 2026

1 About the documentation

The documentation is part of the product. The documentation is intended for the operator of the product and for all persons who interact with the product during its life cycle.

► Read the documentation completely before handling the product.
► Keep the documentation after reading.
► Ensure that all persons who handle the product have access to the documentation.
► If you forward the product to third parties, please also forward the documentation and all applicable documents.

1.1 Graduated warnings

The warnings are graduated according to the severity of the hazard.

⚠ WARNING

A note with the signal word **WARNING** warns of a hazard that can result in serious injury or death if not avoided.

ATTENTION

A note with the signal word **ATTENTION** warns of a hazard that can result in damage or malfunction to the product if not avoided.

1.2 Symbols used

The following symbols may be present in the documentation.

Symbol	Meaning
	Warning of explosion hazard
	Note on documentation or reference to related documentations.
	Information next to this symbol is not safety-relevant, but it supports correct and effective working practice.

1.3 Design elements

– The dash indicates an element within a list that does nocht include any action steps.

◊ The rhombus indicates a prerequisite that must be met before the next action step.

► The black triangle indicates an action step.

☑ The checkbox symbol indicates the result or intermediate result of an action.

1.4 Related documentation

– This manual describes how to use the **Web server** application (Version 3.0.0 or higher).
– Please also observe the manual **u-remote I/O-System**.
– When using safe I/O modules, please also observe the manual **Modules for functional safety**.

You can find all documents in the Weidmüller Support Center.

2 Safety

This section includes general safety instructions for handling the web server. Specific warning notices for specific tasks and situations are given at the appropriate places in the documentation. Failure to observe the safety and warning notices can result in damage to persons and material.

Use in a potentially explosive atmosphere

Access to the web server requires the connection of a computer to the u-remote station. Connecting and disconnecting **must not** be done in a potentially explosive atmosphere!

Earthing

Before connecting to a computer, a proper grounding of the u-remote station must be ensured.

Force mode

In force mode, the system may be manipulated to such an extent that can result in life-threatening personal injury and damage to materials. The force mode may therefore only be used by persons who are fully aware of the connected equipment and the consequences of forcing.

2.1 Intended use

The web server application is designed to display a u-remote station in a browser in order to show the settings of the individual devices and change them as required. In addition, the firmware of the devices in the station can be updated. The web server can also be used to intervene in the live operation of a system (force mode).

2.2 Cybersercurity

In order to achieve an effective protection against cyberattacks, every operator of industrial plants must develop a comprehensive security strategy and implement a cybersecurity concept in practice. It is also the operator's responsibility to continuously adapt the implemented cybersecurity measures to technological developments. Weidmüller products and solutions are designed to be part of such a security strategy and help ensure a secure infrastructure.
Devices, systems, machines and networks must be protected against unauthorised access. Components should only be connected to a company network or the internet if necessary and only if appropriate security measures such as firewalls and network segmentation have been implemented.
Further information about the topic of cybersecurity can be found on the Weidmüller industrial security website. Please observe the following documents:
– Industrial Product Security Guideline
– Security Data Sheets
For information on known vulnerabilities and current security advisories related to Weidmüller products, please visit the Weidmüller Security Advisory Board.
If you have identified a potential security vulnerability related to a Weidmüller product, please report it via the Coordinated Vulnerability Disclosure process.

- Install updates immediately to ensure that you are always using the latest supported version. Using outdated or unsupported versions can increase the risk of cyber attacks. You can download the latest software and firmware files from the product catalog.
- Ensure that the PC operating the Webserver application has the latest Windows update installed, that up-to-date virus protection is active, and that the PC is connected to a secure network. Please note that the data exchanged between the u-remote station and the Webserver is neither signed nor encrypted.
- Administrator rights are required to configure the Webserver application. It is the operator's responsibility to revoke these rights after installation. Using the software with administrator rights poses significant cyberrisks.
- The password strength must be defined for each role created in user management. Please note the requirements for secure passwords in the Industrial Security Product Guide.
- Every user must keep his login credentials confidential. Never share your login credentials.
- The Webserver application is locked after 15 minutes of inactivity. You can log in again with your password.
- Lock the PC on which the Webserver application is installed when leaving your workplace.
- The operator is responsible for preventing unauthorised access to the USB port on the u-remote station.

3 Product description and requirements

3.1 Product description

With the web server, the u-remote station is displayed in a browser on a connected PC. In the web server, you can directly influence the settings of the u-remote station, e.g. for testing purposes, during commissioning or in the event of servicing. The following manipulations are possible:

- Simulate the operation of the u-remote station
- Query the status of each coupler and module
- Display the parameters of couplers and modules, and change them for testing purposes
- Access diagnostic information
- Save and load the configuration file
- Operate the station in force mode for testing purposes
- Update the firmware

The software includes integrated user management, in which users with different permissions can be set up.

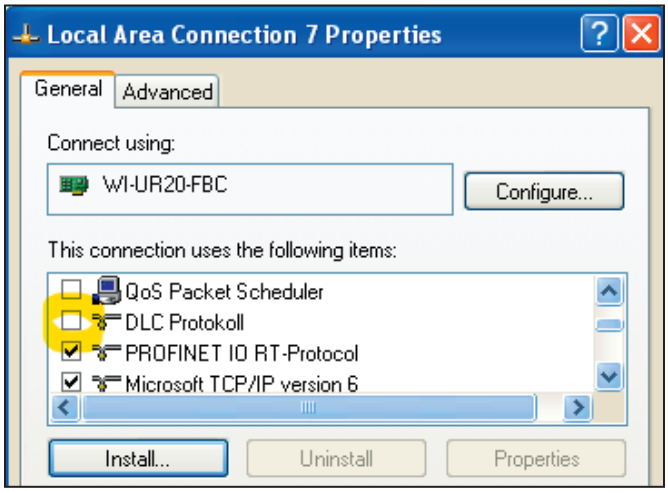
3.2 Requirements

Operating system

The u-remote web server can be used with the following operating systems:

- Windows XP®
- Windows 7®
- Windows Vista®
- Windows 10®
- Windows 11®

For operation with Windows XP: if you installed the Siemens Primary Setup Tool, the DLC (data link control) protocol was also installed. To access the web server, you must deactivate the DLC protocol on the USB interface (LAN connection with WI-UR20-FBC).



Deactivating the DLC protocol (only Windows XP®)

Webbrowser

The u-remote web server can be used with the following browsers:

- Mozilla Firefox 20.0 or higher
- Google Chrome 20.0 or higher
- Opera 10.61 or higher
- Microsoft Internet Explorer 10 or higher
- Microsoft Edge

Screen resolution

When using the web server we recommend a screen resolution 1280 x 800 or higher, at least 1024 x 768. The user interface is displayed optimally with the browser window maximised.

4 Connecting and starting the web server

4.1 Installing the web server via USB

⚠ WARNING

Explosion risk!
Prior to starting work, make sure that there is not a potentially explosive atmosphere!

ATTENTION

Risk of severe damage!
Prior to connecting a PC, make sure that the u-remote station has been earthed properly!

First access to the web server has to be via the USB interface of the coupler, see Chapter 4.2. With couplers designed for the use with ethernet based bus systems – recognisable by the RJ45 sockets – the web server can be accessed alternatively via Ethernet, see Chapter 7.4.

The USB port acts as an virtual DHCP Server. Please do not assign any IP addresses to other devices within the same subnet of the USB port (default 192.168.1.202, UR20-FBC-EIP: 192.168.5.202), otherwise network failure might occur.

The USB cable can be a maximum of 2 m in length (Type USB-A to USB Micro-B e.g. Weidmüller Order No. 1487980000). Extension cables must not be used.

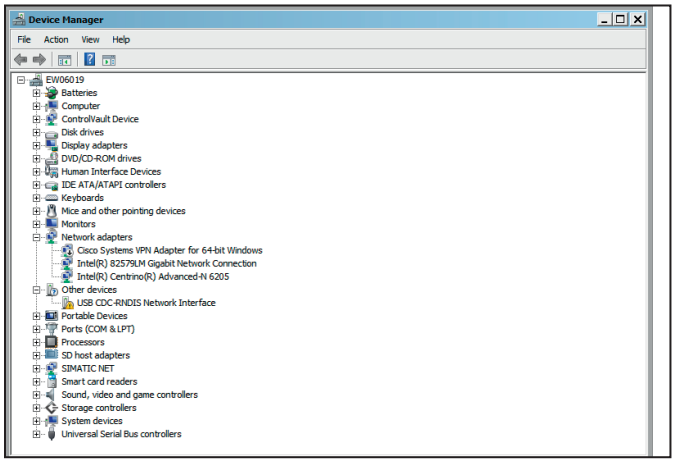
Installing USB device drivers

You can find the driver file is available on the Weidmüller Support Center.

► Download the USB driver for the web server.
► Unpack the ZIP file.

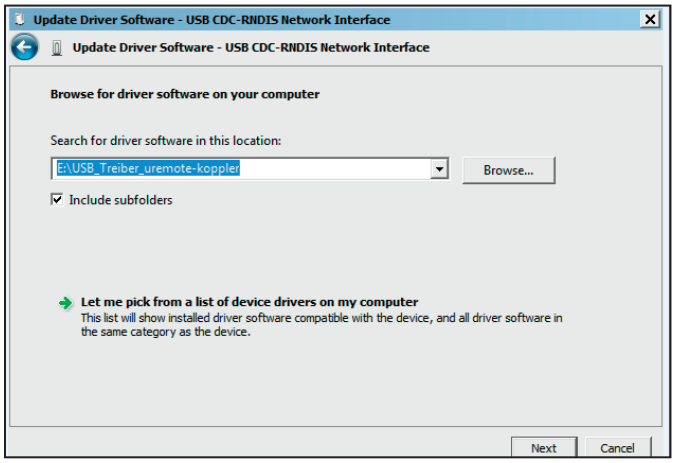
Windows 10® or higher
► Right-click on the **usb8023.inf** file and select **Install**.
► Confirm the dialogue with **Yes**.
► Right-click on the **rndis.inf** file and select **Install**.
► Confirm the dialogue with **Yes**.
☑ The driver is being installed.
☑ After successful installation, a **WI-UR20-FBC** network adapter is displayed in the Device Manager.

Windows 7® or older
► To install the driver manually, open the Device Manager.
Under **Other devices** the **USB CDC-RNDIS Network Interface** interface is displayed.



New USB interface in the Device Manager

► Right-click on the interface and select **Update driver software**.
☑ You will be asked how you would like to search for the driver software.
► Select the option **Search for driver software on this computer**.



Searching for installation files on the computer

► Click **Browse** and navigate to the folder in which you have stored both .inf files.
There could possibly be a security enquiry because the driver software does not have a signature. Nonetheless, continue with the installation.
► Follow the rest of the steps in the installation routine until the successful installation is confirmed.
☑ The driver is displayed in the Device Manager under **Network adapters**.
► Close the Device Manager.

4.2 Making the web server operational

◊ The USB driver must be installed.
◊ The u-remote station must be completely assembled and supplied with voltage.

► Connect the PC to the coupler using a USB cable. The USB socket at the coupler can be found behind the service flap on the front side.
► Open an appropriate browser, see Chapter 3.2.
► In the address line, enter the IP address of the coupler (default: 192.168.1.202, UR20-FBC-EIP: 192.168.5.202).
☑ The web server is started. The connected station is displayed with all of its active modules.

Starting page upon first login after delivery

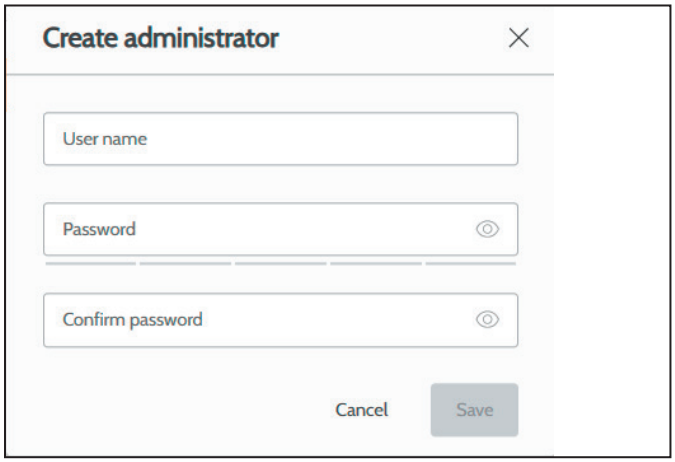
In the event that the web server will not start, please check the IP address, see Chapter 13.2.

The first access to the web server must always be via HTTPS. You can change the access to HTTP later in the coupler parameters, but we do not recommend this for security reasons.

4.3 First commissioning

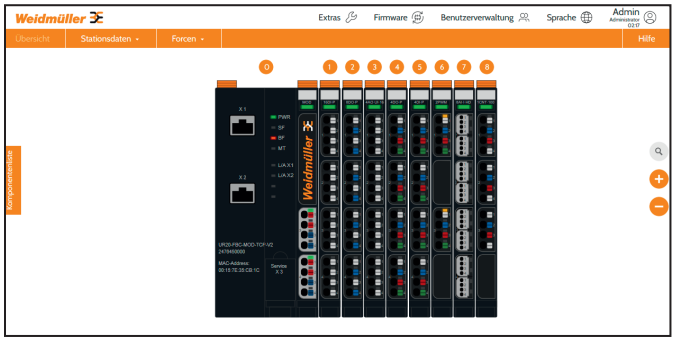
After delivery, a person who can work as an administrator must start up the web server. This person must first create a user for themselves and can then create additional roles and users. When creating a user, a password is assigned to them, which the user must change when they log in for the first time.

► Click **Create administrator**.
☑ A dialogue is opened.



Dialogue box creating an administrator

► Enter a user name.
► Enter a password.
► Confirm the password.
► Click **Save**.
☑ The web server overview is opened.



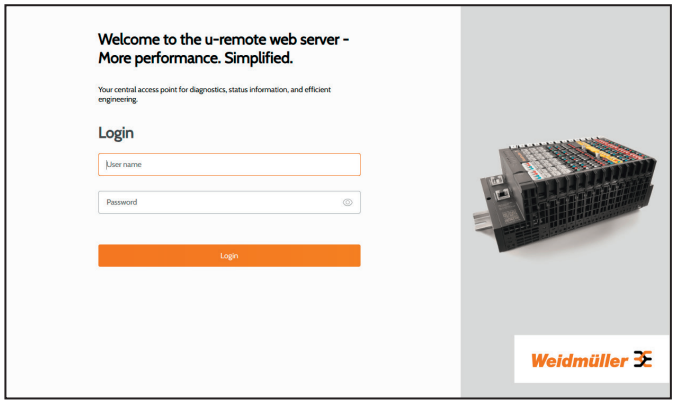
Overview of the u-remote station

5 Getting to know the web server

5.1 Starting the web server

◊ The u-remote station must be completely assembled and supplied with voltage.
◊ At least one user must have been created in the user management.

► Connect the PC to the coupler using a USB cable. The USB socket at the coupler can be found behind the service flap on the front side.
► Open an appropriate browser, see Chapter 3.2.
► In the address line, enter the IP address of the coupler (default: 192.168.1.202, UR20-FBC-EIP: 192.168.5.202).
☑ The web server is started. The starting page is displayed.



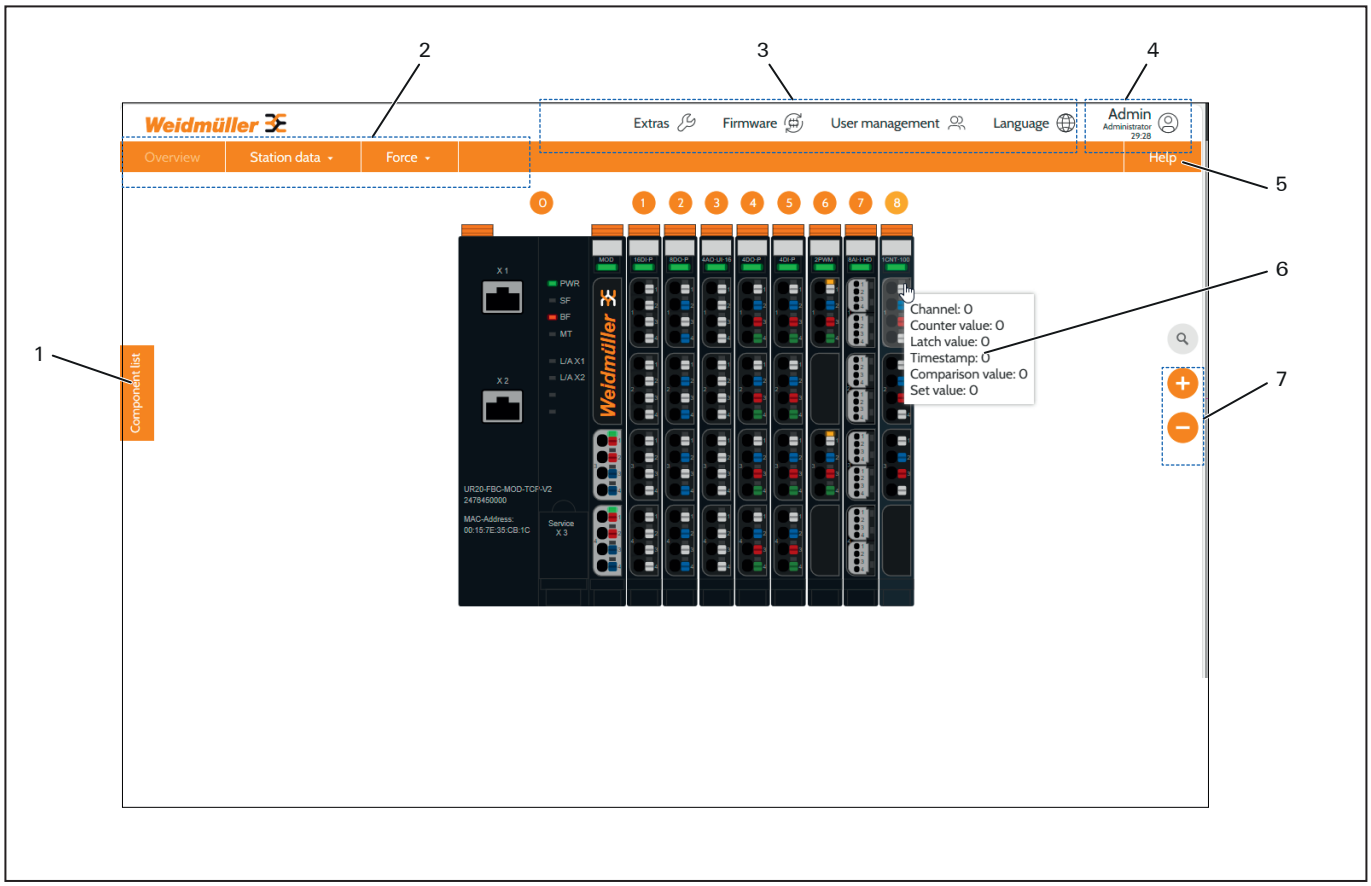
Starting page

► Enter your user name.
► Enter your password.
► Click **Login**.
☑ The station view is opened.

Overview of the u-remote station

5.2 Station view

The station view is displayed on every start up of the web server.



Station view

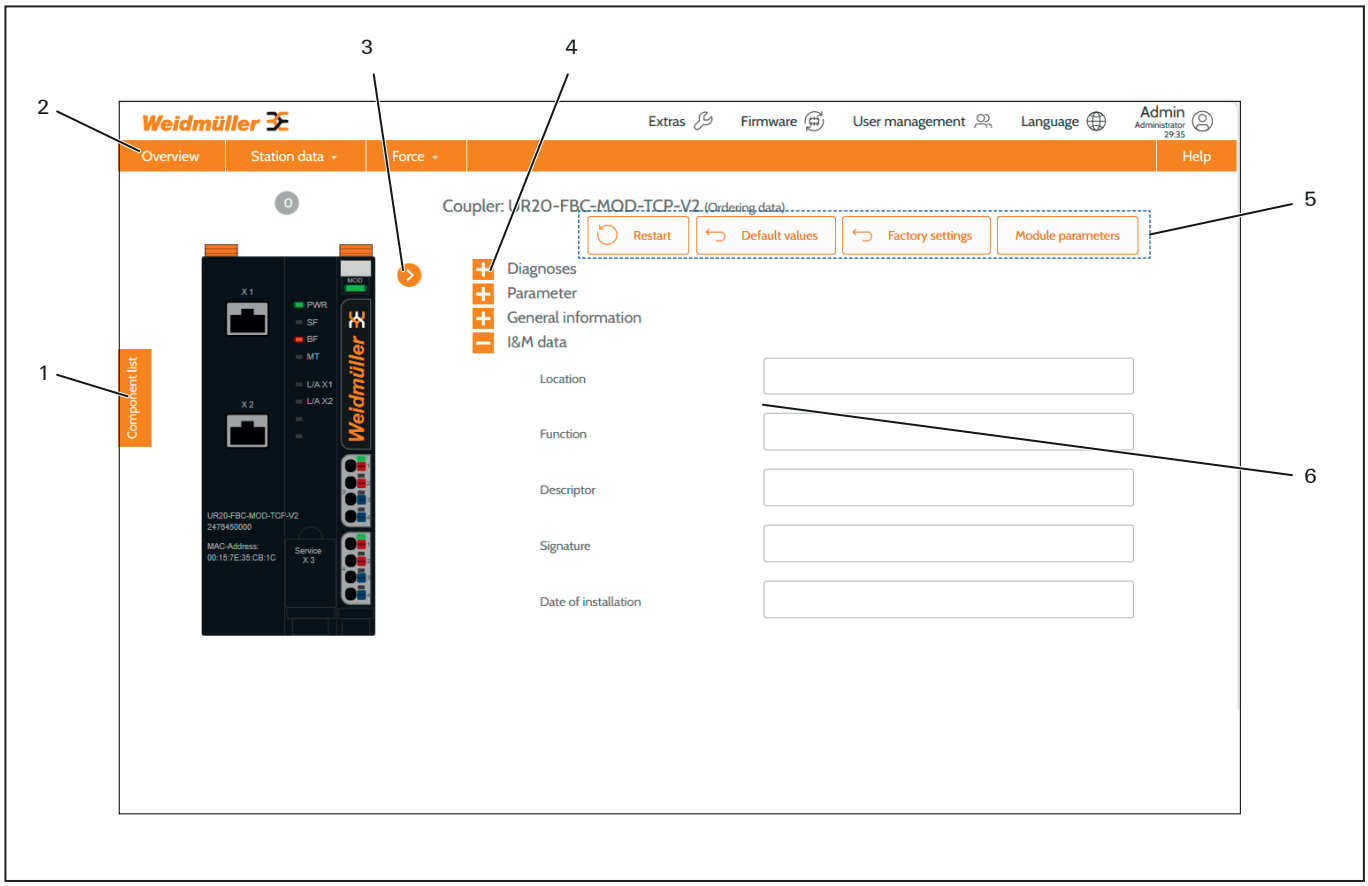
1 Fading in the component list (by mouseover)
2 Access to the web server functions
3 Menu bar
4 Current user and remaining session time
5 Open the help
6 Detail view of module/channel (by mouseover)
Switch over to the component view (by mouse click)
7 Scaling the view up or down

Component list faded in

The web server only registers modules that can communicate on the system bus. Empty slot modules and other passive modules (e.g. AUX modules) are not registered by the web server and thus are not displayed in the screen view. The numbering of the modules in the web server view may therefore deviate from the count in the actual station!

5.3 Coupler componentent view

The component view is opened after clicking on a component or the component list.



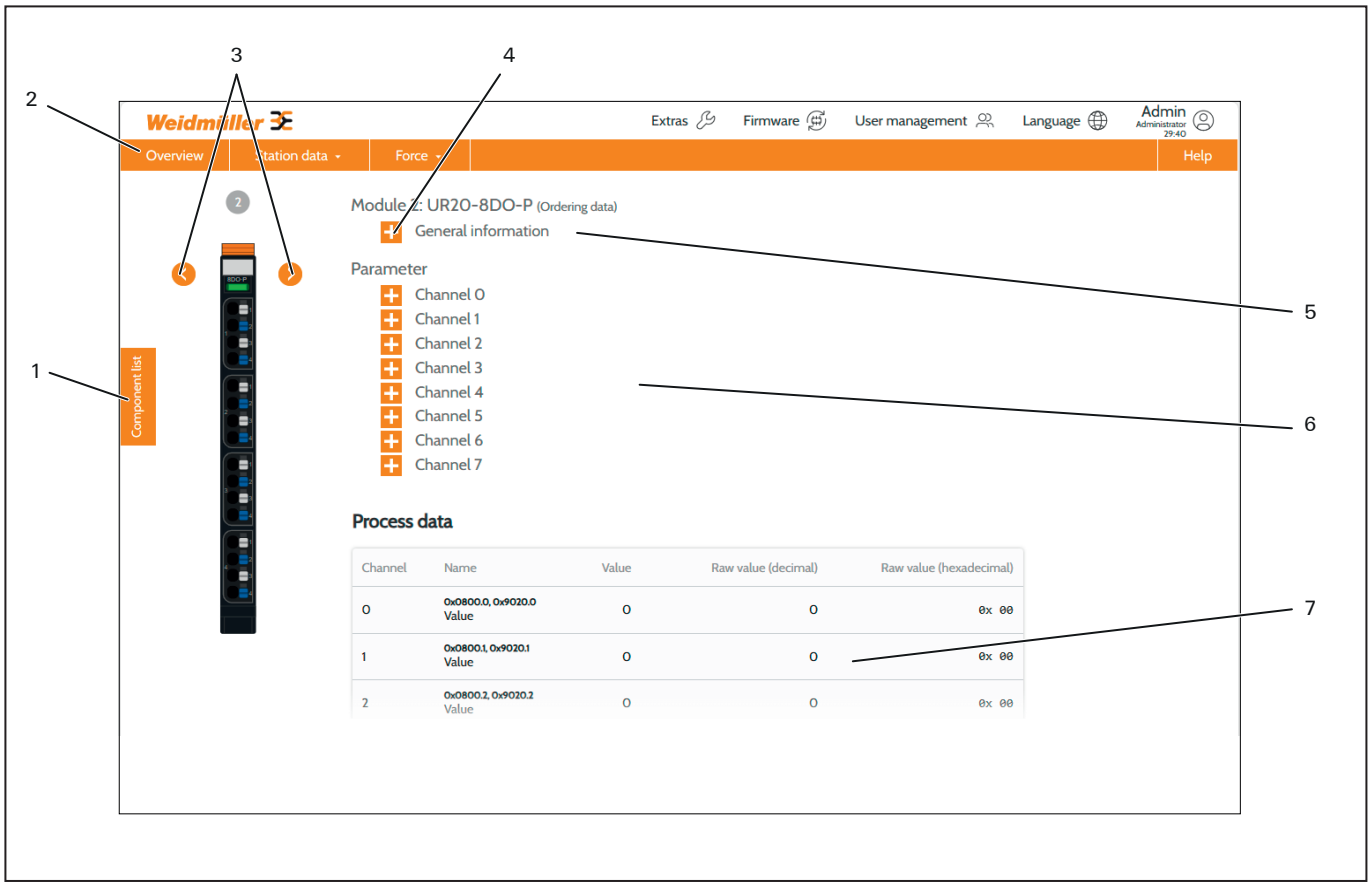
Coupler component view for users with administrator rights

1 Fading in the component list (by mouseover)
2 Switch over to the station view
3 Select the next component right (by mouse click)
4 Show or hide details (by mouse click)
5 Coupler functions, only visible with administrator rights
6 Coupler-related information

Coupler component view for users without administrator rights

5.4 Module component view

The component view is opened after clicking on a component or the component list.



Module component view

1 Fading in the component list (by mouseover)
2 Switch over to the station view
3 Select the next component left or right (by mouse click)
4 Show or hide details (by mouse click)
5 Module-related information
6 Module parameters
7 Process data

5.5 Navigation

There are several options how to display the station or certain components (coupler or modules):

Overview

This view shows all components and you can display details via mouseover. You can open the station view with a click on **Overview**.

Component view

This view shows a single component (coupler or module) with its information and parameter settings. Using the arrow keys you can navigate to the subsequent components in the station. You can open the component view by clicking on the component – either in the station view or the component list.

Station data

This view shows the current process data or diagnostic data of the entire station. Both views are accessible at any time.

5.6 Operation notes

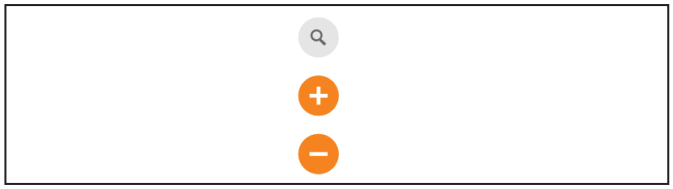
Single mouse clicks (left mouse key) are sufficient when using the web server. Some areas of the user interface are mouse sensitive, which means, they will change whenever you move the cursor in this area without clicking (mouseover).

A mouse click is expected whenever the cursor changes to this shape.

You can move the suface while pressing the left mouse key whenever the cursor changes to this shape

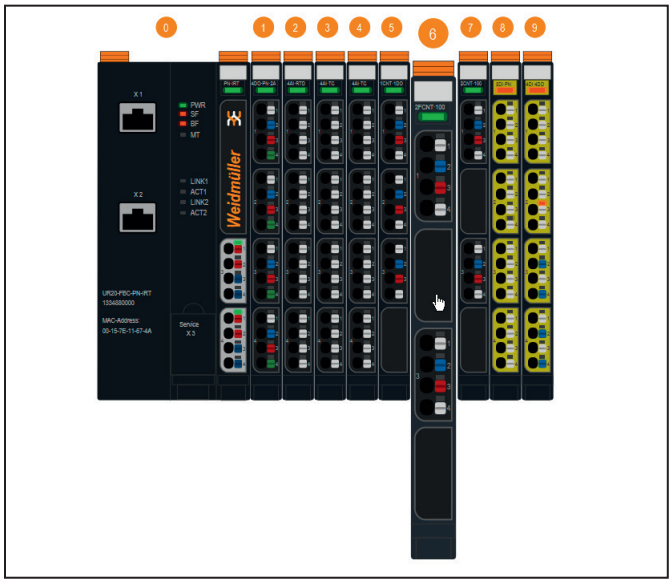
Scaling the station view up and down

- ► To reduce the size of the station view, click on the minus symbol to the right of the station overview.
- ► To enlarge the station view, click on the plus symbol to the right of the station overview.



Scaling the view

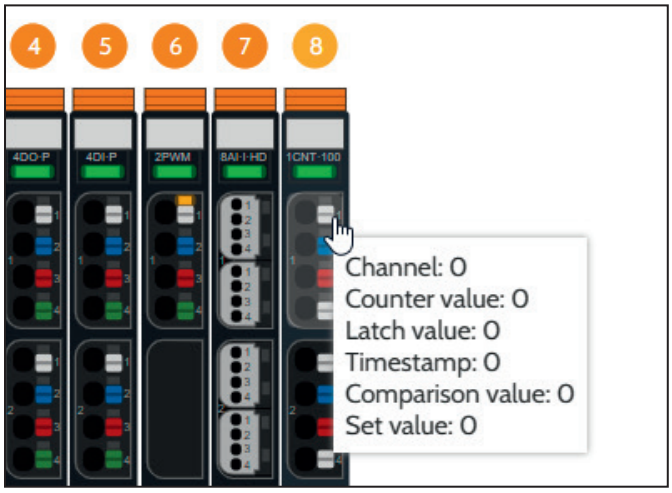
When using a smaller view you can scale up single components by a mouseover.



Scaling up details

Displaying channel values

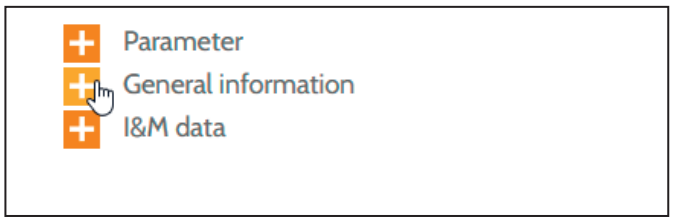
► Move the cursor slowly over the station without clicking.
All values of the channel above which the cursor is presently situated are displayed.



Displaying channel values

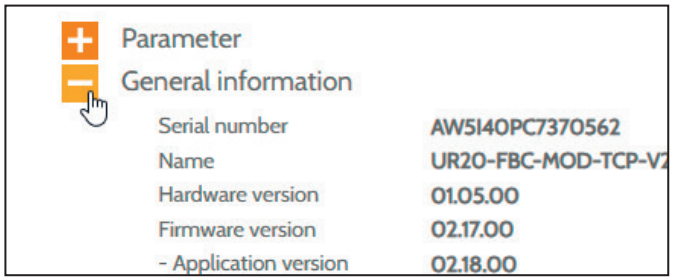
Showing or hiding contents

► To display the contents of an entry, click on the plus symbol.



Showing content

► To hide the contents again, click on the minus symbol.



Hiding content

Applying or resetting changes

When you change settings, they are marked with a green symbol.

Changes marked

In this state you can reset every single change.

► To reset all changes at a time, click **Restore**.

► To apply all changes at a time, click **Apply changes**.

☑ The markings will be eliminated as soon as you apply or reset the changes.

6 User management

Access to the web server is only possible with user login. Every person who is to work with the web server must be created as a user, and each user must be assigned a role. Up to 20 users and up to 5 roles can be created and managed in user administration. Permissions are defined in the roles.

Upon delivery, one administrator role with all available permissions is set up on the web server. After delivery, a person who is able to work as an administrator must put the web server into operation, see Chapter 4.3.

Permission can be given for the following options:
- Read
- Write
  - Change parameters and settings
  - Edit channel names
- Force
  - Force process values
- Logging
  - Read service file
  - Read audit log
- Firmware update
  - Upload and exchange certificates
  - Update firmware
  - Replace language
- Configuration
  - Edit start text
  - Trigger restart
  - Reset to delivery status
- User management
  - Manage users and roles
  - Edit session settings

We recommend developing up a role and rights concept so that you can set up the necessary roles on this basis and then assign them to the intended users.
Please observe the data protection regulations applicable at your location.

6.1 Timeout for incorrect login details

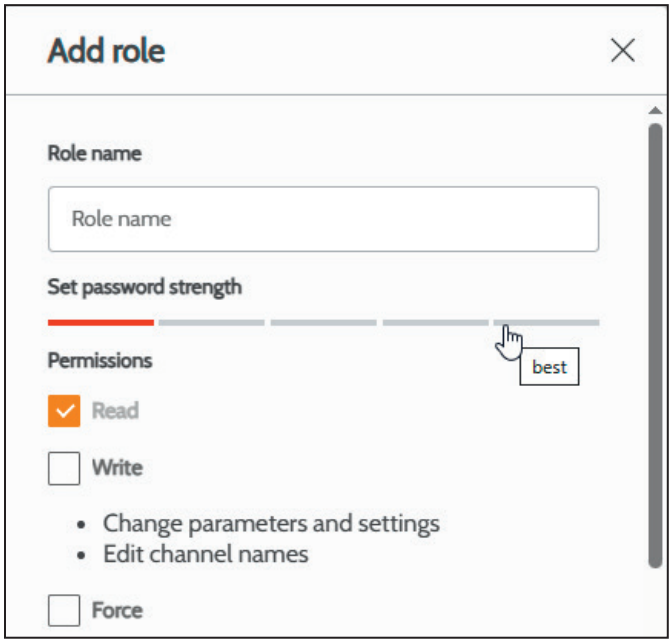
If the login details are entered incorrectly, the login screen will be disabled for a certain period of time, preventing any further entries. The duration of the timeout increases with each failed attempt, up to a maximum of 60 seconds. Once the login is successful, the timeout duration is reset.

The timeout cannot be bypassed by restarting the web server. Do not even try.

6.2 Creating a role

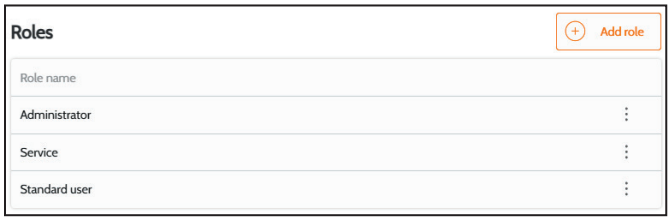
◊ This function requires the necessary permission.

► Clicken **User management**
► Click **Add role**.
☑ A dialogue box is opened.



Creating a role

► Enter a name for the new role.
► Define the required passwort strength with level 1 to 5. All users assigned to this role must choose a suitable strong password.
► Mark the permissions for the new role
► Click **Save**.
☑ The new role is displayed in the role list.

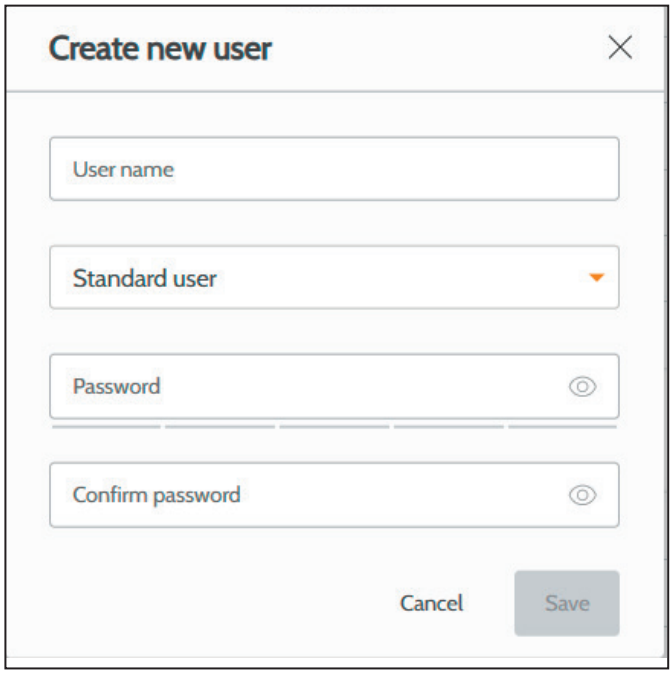


List of created roles

6.3 Creating a user

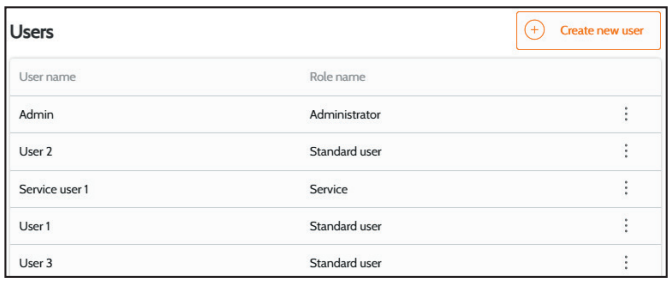
◊ This function requires the necessary permission.

► Click **User management**
► Click **Add user**.
☑ A dialogue box is opened.



Creating a user

► Enter a name for the new user.
Each unser name can only be used once.
► Assign a role to the new user.
► Create a password for the new user.
► Click **Save**.
☑ The new user is displayed in the user list.

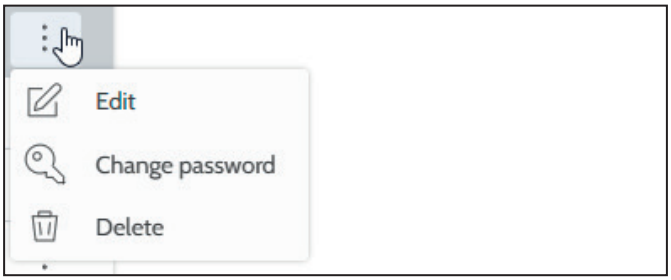


List of created users

Once a new user logs in, he must change the password.

6.4 Editing or deleting users or roles

◊ This function requires the necessary permission.

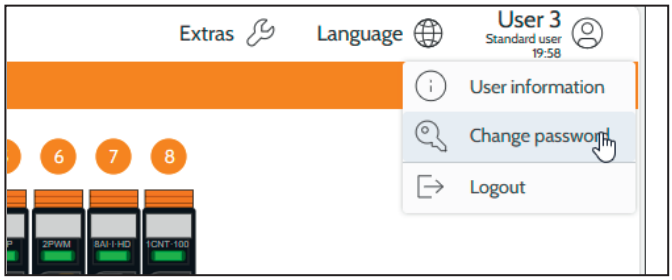


Editing a user or role

► Click the ⋮ beside the entry to be changed.
Depending on the permissions, the options are displayed or grayed out.
► To edit the entry, click **Edit**.
► To delete the entry, click **Delete**.

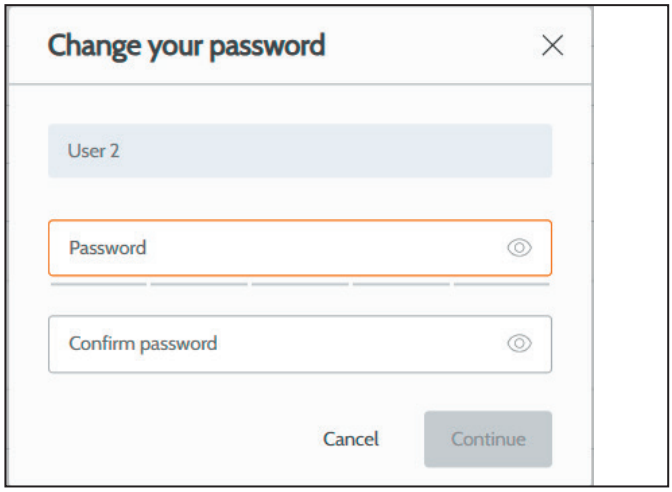
6.5 Changing the own password

Each user can change the own password.



Changing the own password

► Click the user display and then **Change password**.



Entering a new password

► Choose a neuw password that meets the rewuired strength. This is indicated by the display scale turning green.
► Confirm the password.
► Click **Continue**.
☑ The new password is saved.

6.6 Changing another person's password

◊ Permission for the user management (Administrator) is required to change the passwort of another person.

► Open the user management.

Changing a password

► Click the ⋮ beside the entry of which you want to change the password.
► To change the password, click **Change password**.
► Enter the new password.
► Confirm the new password.
► Click **Continue**.
☑ The new password is adopted, the dialogue box is closed.
☑ The affected user will be asked to change the password the next time he logs in.

7 Setting up the web server

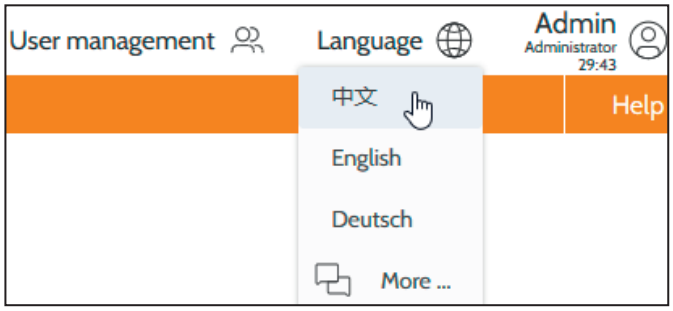
7.1 Setting the language

The web server starts with the language setting of your browser. If this language is not supported, it starts with the setting **English**.

On delivery, the three language files German, English and Chinese for the web server are included in each UR20 fieldbus coupler. You can switch between these languages during operation without restarting the web server.
Each supplied language can be replaced by another language file. You can find all available language files in the Weidmüller Support Center.

Changing the language

► To change the language, click **Language** and then the desired setting.
☑ The language of the software interface changes immediately.



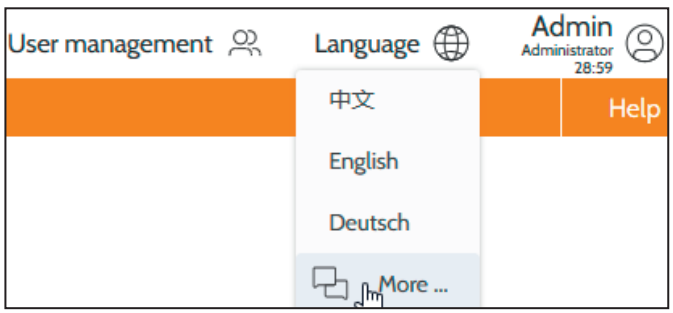
Changing the language

Replacing a language

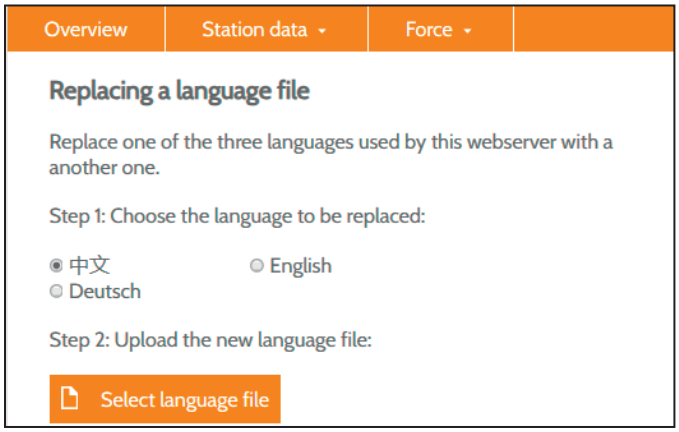
◊ This function requires the necessary permission.

After loading a new language, the web server is automatically restarted.
The three active languages loaded in the web server are identical for all users.

► Download the language files **Language Pack UR20 FBC**.
► Unpack the ZIP file on your PC.
► In the wenbserver, click **Language** and then **More ...**.

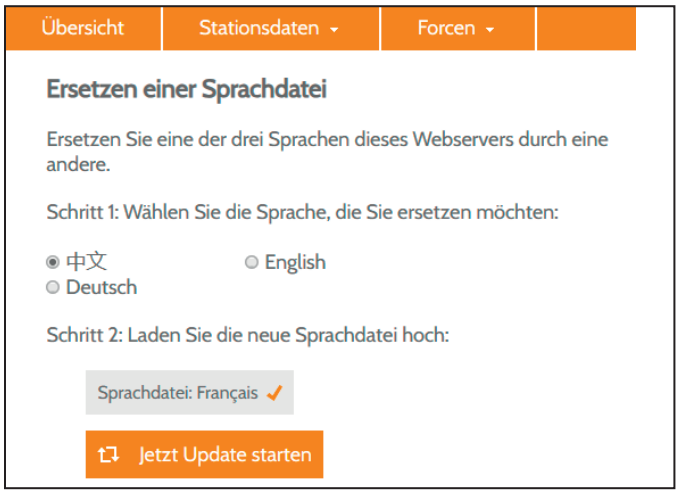


Replacing a language



Choosing the language to be replaced

► Select the language you want to replace.
► Click **Select language file**.
► Navigate to the desired language file on your PC and click **Open**.
► Click **Update now**.



Starting the update of the new language

☑ The new language is uploaded to the coupler.
After a restart of the coupler, you can select the new language in the **Language** menu.

If you want to cancel the process, click on any other menu.

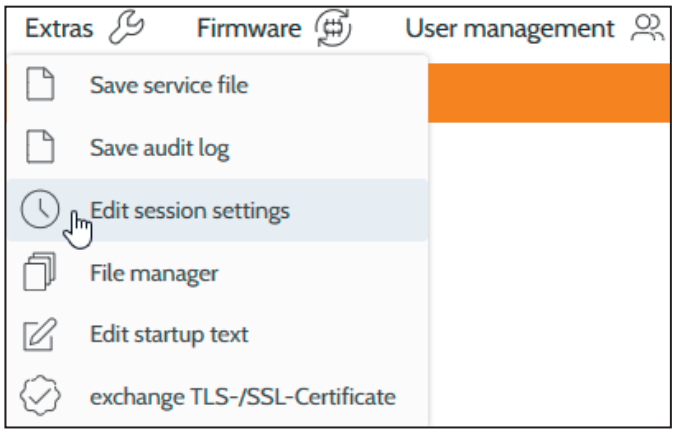
7.2 Editing the session settings

◊ This function requires the necessary permission.

Each session on the web server is time-limited; after this time, you will need to log in again. The maximum session duration is set to 15 minutes on delivery, but can be set between 5 and 120 minutes.

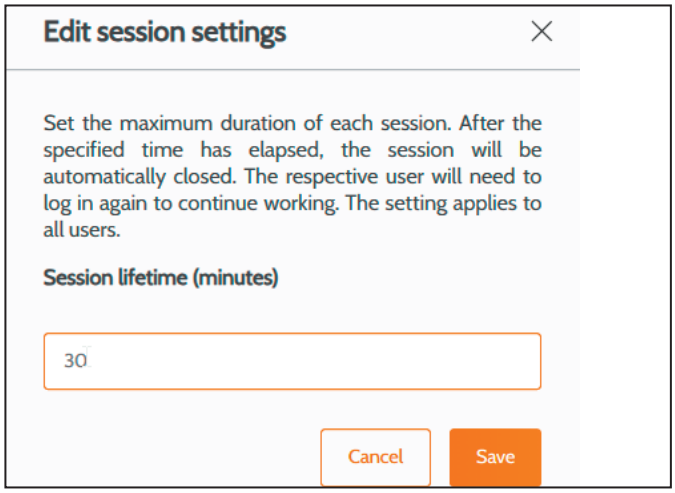
The session duration set is valid for all users.

► Click **Extras** and then **Edit session settings**.



Opeing the session settings

☑ A dialog box is opened.



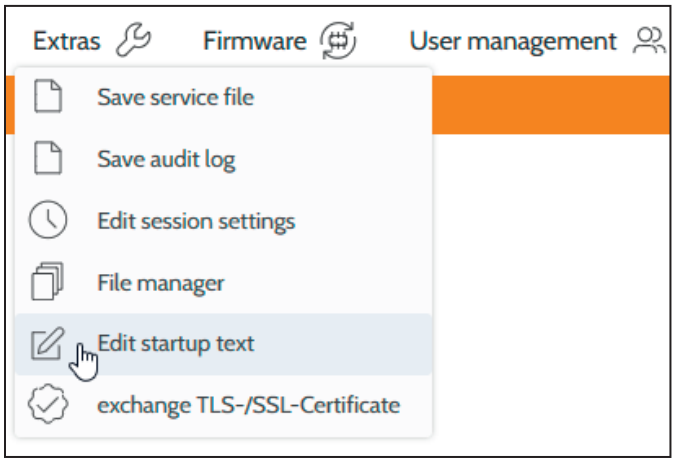
Editing the session duration

► Enter the maximum session duration in minutes.
► Click **Save**.
☑ The setting is adopted and the new remaining session time is displayed.

7.3 Editing the startup text

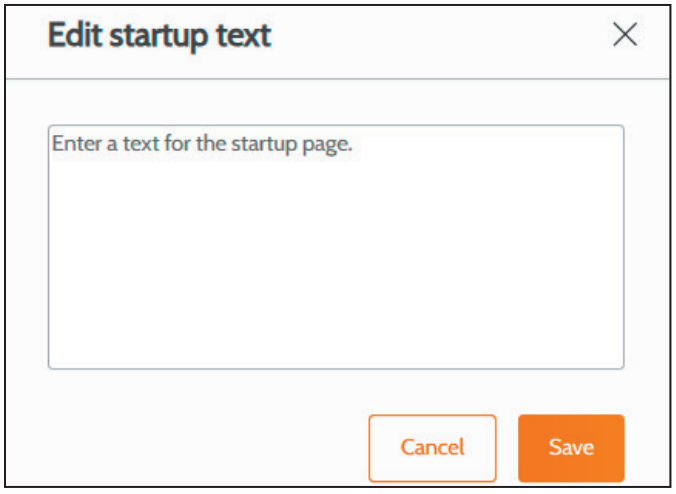
You can specify a text that will be displayed on the starting page each time the web server is started. This text should describe the intended use of the software.

► Click **Extras** and then **Edit start text**.



Opening edit startup text

☑ A dialogue box is opened.



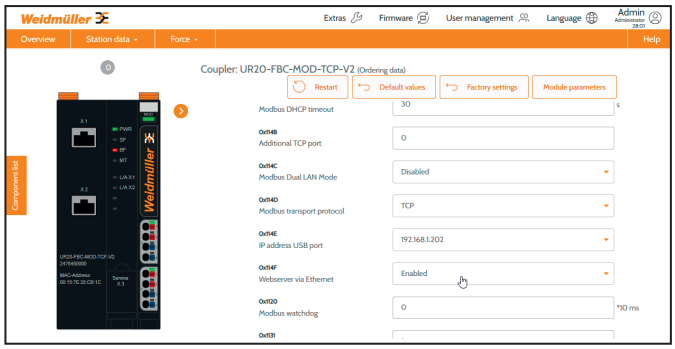
Editing a startup text

► Enter the desired text. Maximum number of characters: 256 characters (UTF-8).
► Cick **Save**.
☑ From now on, the text will be displayed with each web server startup.

7.4 Setting up the Ethernet port

Couplers for ethernet based bus systems are equipped with RJ45 sockets. With this, the web server can alternatively be controlled via Ethernet.
If you want to use the web server via Ethernet you have to set up the ethernet connection first.

► Connect the PC with the coupler (or a switch within the network) using a LAN cable.
► Click on the coupler in the station view and then on **Parameter**.
► Enter the desired IP address, subnet mask and gateway.
► Make sure, that the parameter **Webserver over Ethernet** is enabled.



Setting up the ethernet port

► Click **Apply changes**.
► Remove the USB cable between coupler and PC.
► Restart the coupler.

Any change of IP settings of USB or Ethernet port will only take effect after restarting the coupler.

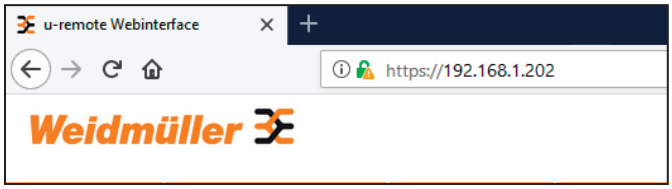
7.5 HTTPS

With the introduction of the user management, the web server can initially only be accessed via HTTPS.
With HTTPS, the web server and client communicate encrypted on the transport layer. This ensures the authenticity of the web server as well as the integrity and confidentiality of the data transmitted.

Opening the web server via HTTPS

◊ The computer must be connected with the u-remote station.
◊ The u-remote station must be assembled in full and powered up.

► Open one of the browsers listed in section 3.2.
► In the address line, enter https:// and the IP address of the coupler (default: 192.168.1.202, UR20-FBC-EIP: 192.168.5.202).



Call up the web server via HTTPS

As your browser does not know the self-signed u-remote standard certificate, it warns you that the connection is not trustworthy.

This warning also appears with the following events:
– After changing the IP address of the coupler.
– After changing the certificate.

► Add an exception rule for this IP address in order to start the web server application.

Only add the exception rule once you are sure that you are connected with the right coupler. Also observe the local data security regulations.
We recommend addressing the coupler via the USB port if you add the exception rule.

You can avoid this warning by using a user-defined certificate that has been signed by a trusted certificate authority.

Exchanging the TLS/SSL certificate

◊ This function requires the necessary permission.

You can replace the u-remote standard certificate with your own certificate. Optionally, you can have your certificate signed by a trusted certificate authority (CA) and also load the CA certificate to the coupler.

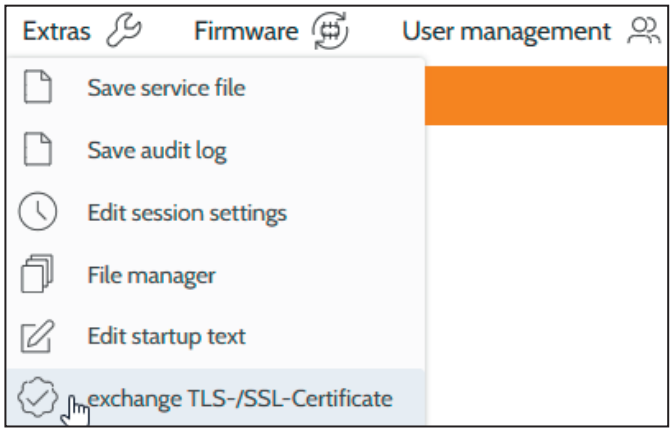
Only transmit certificates and private keys via trusted connections.
We recommend transmitting certificates and private keys via the USB port of the coupler.

The web server supports the following options:
– Encryption with TLS 1.1 and TLS 1.2.
– Key lengths up to 2048 bit.
– PEM-coded keys and certificates (.pem).

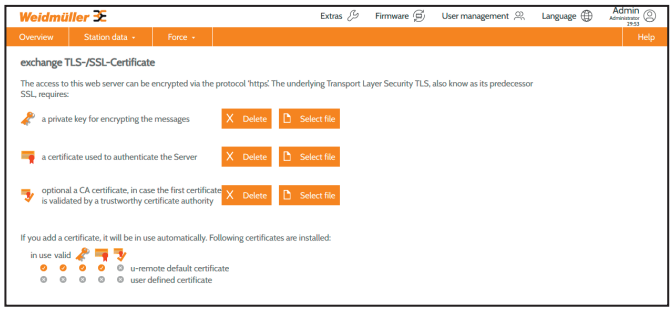
► Generate a private key and an appropriate certificate for it, e.g. with OpenSSL.

Do not encrypt the private key with a pass phrase. The web server cannot read the key in this case and identifies it as invalid.

► Click **Extras** and then **exchange TLS/SSL certificate**.



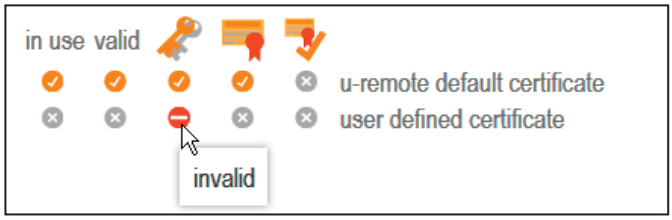
Opening Extras/Exchange TLS-/SSL-Certifcate



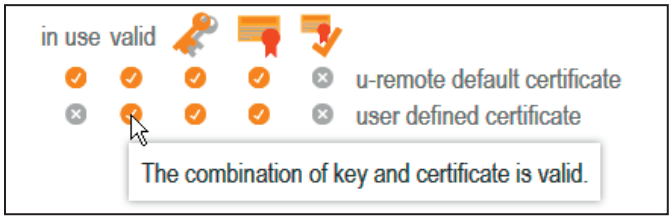
Exchange TLS/SSL certificate

► To delete any old keys and certificates, click **Delete**.
► To load the key and the certificates onto the coupler, click **Select file** and navigate to the desired file on your computer.
☑ Keys and certificates are automatically checked. The result is displayed in the web server.

► Move the mouse over the icons to display the results as text.



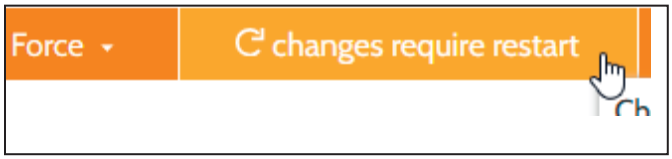
Automatic check: Key invalid



Automatic checking successful

After successful checking, the web server has to be restarted to activate the user-defined certificate.

► Click **Changes require restart**.



Restart the web server

☑ The web server is restarted. After the restart, the user-defined certificate is activated.

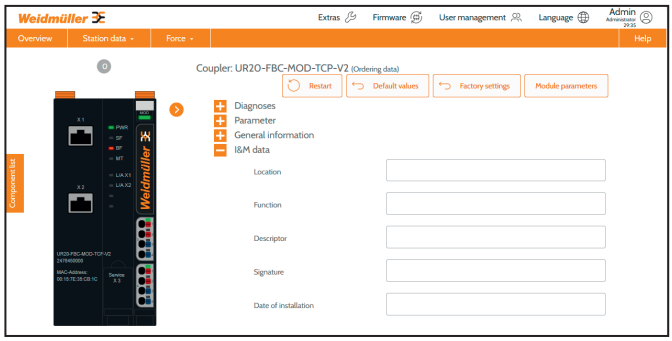
After changing certificates, the restart takes a little longer than usual because each certificate must be read and checked by the browser. You may need to repeat the restart.
Depending on the certificate, it may be necessary to confirm the uploaded certificate in the browser first.

8 Coupler settings and functions

The coupler settings are only accessible when force mode is not active.

The status data can be displayed at all time, regardless of the state of the field bus connection. Setup changes can only be stored while the field bus is not active.

► Open the coupler component view.



Coupler component view

Depending on the individual permissions, the options are editable or read only oder they are not displayed.

The following options are available in the **Coupler component view**:
- Access the datasheet of the coupler (**Ordering data**)
- Query diagnoses
- Access and change the coupler parameters
- Query general information about the coupler
- Type in I&M data (Identification & Maintenance)

The following options are available in the **coupler functions**:
- Reset: Restart the coupler and reset any changes that have not been saved
- Standard values: Reset the coupler to the standard values
- Factory settings: Reset the coupler to factory settings
- Module parameter: Save the module parameters or reset them to standard values

8.1 Displaying the data sheet

► To display the data sheet, click the **Ordering data** link next to the module designation.
☑ A connection to the Weidmüller website is established in a new browser window and the data sheet is displayed as a PDF file.

8.2 Displaying and changing coupler parameters

◊ Changing parameters requires the necessary permission. Without permission, all parameters are diplayed in read-only mode but they are not editable.

► Open the coupler component view.
► Click **Parameter**.
☑ The parameters are displayed.

Displaying and changing the coupler settings

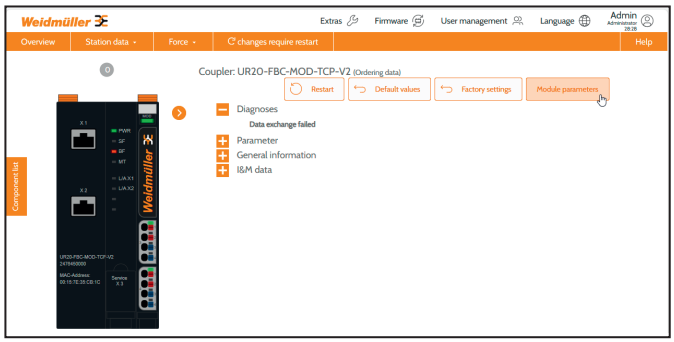
For parameters that can be edited, you can enter the changes in the entry fields or choose alternative settings from a drop-down list.

► Enter the desired changes.
► If you want to cancel the process, click **Restore.**
► To save all changes click **Apply changes**.
☑ The changes are adopted.

8.3 Saving or restoring module parameters in the coupler

◊ This function requires the necessary permission.

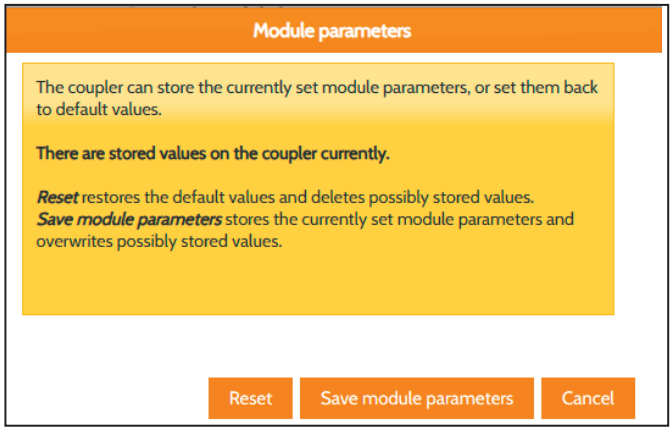
You can save the parameters of the connected modules in the coupler or restore them to the default values.



Module parameters

► Click **Module parameters**.

If no modules are connected to the coupler, the button is inactive.

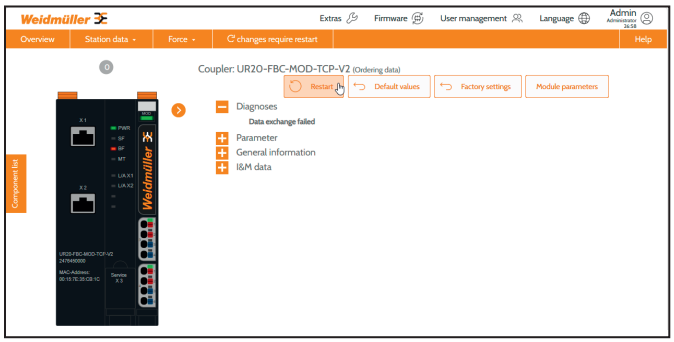


Saving module parameters or restoring default values

► To save the currently set module parameters, click **Save module parameters**.
☑ The module parameters are saved on the coupler, overwriting the old module parameters.
☑ The saved module parameters are sent to the modules again when the coupler is restarted.
► To restore all module parameters to their default values, click **Restore default values**.
☑ Previously saved module parameters are deleted.
☑ Subsequent changes to the module parameters are possible, but will be lost again when the coupler is restarted.

8.4 Restarting the web server

◊ This function requires the necessary permission.

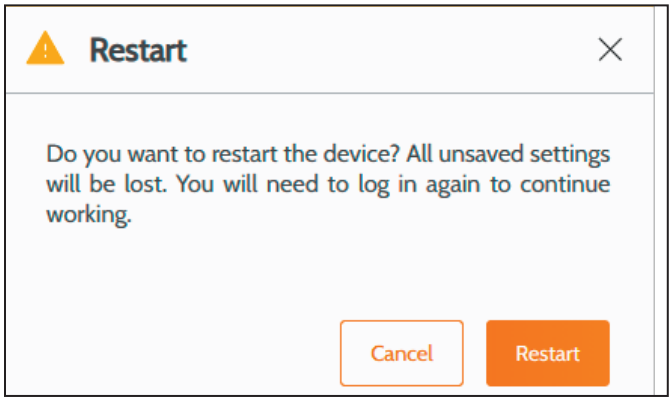


Restart

With a coupler restart the webserver is restarted as well. By proceeding a restart, you can undo all the changes that have been made since the last time that the web server was started.

With a restart, all data which is not protected against power failure is reset.

► Open the coupler component view.
► Click **Restart** and then **Restart**.



Restarting coupler and web server

☑ The coupler as well as the web server are restarted.

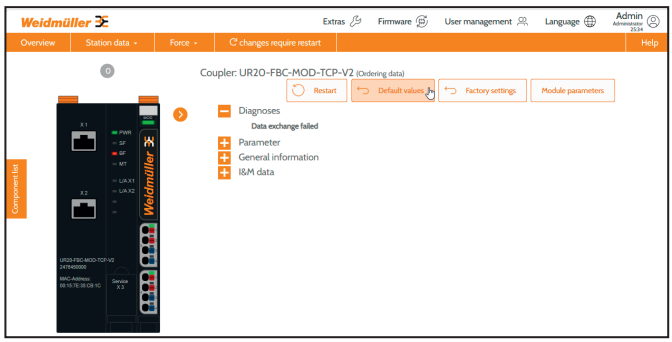
8.5 Resetting the coupler to default values

◊ This function requires the necessary permission.

This function allows you to reset the coupler to its default values. This will reset all settings and delete the coupler's operating information. the user management will remain unchanged.

With a reset, the coupler is automatically restarted.

► Open the coupler component view.
► Click **Default values**.



Resetting the coupler to default values

☑ A dialogue box is opened.
► Click **Reset**.
☑ The device is reset to devault values. All changes get lost, only the user management remains unchanged.
☑ The coupler as well as the web server are restarted.

8.6 Resetting the coupler to factory settings

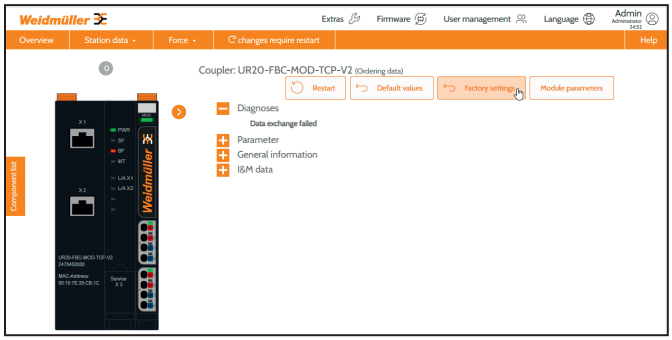
◊ This function requires the necessary permission.

This function allows you to set up the coupler in its original state as at delivery. This will reset all settings, delete the coupler's operating information and the user management. This function is recommended for decommissioning a station.

Resetting to factory settings affects the following functions:
– All coupler parameters
– Login data and password protection
– I&M data
– Modified module parameters that are safed in the coupler
– Channel names

With a factory reset, the coupler is automatically restarted.

► Open the coupler component view.
► Click **Factory settings**
☑ A dialog box is opened.

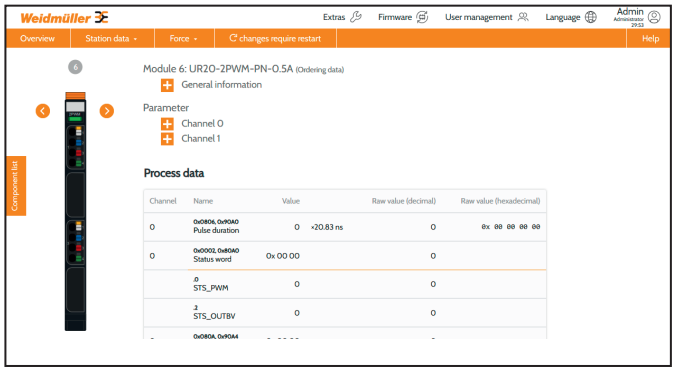


Resetting the coupler to factory settings

► Click **Reset**.
☑ The device is reset to its delivery state. All changes get lost, the user management is deleted.
☑ The coupler as well as the web server are restarted.

9 Module settings

► Open the module component view.



Module component view

Here you can:
- Display general information about the module
- Access and change the module parameters
- Display information about certain channels
- Access the data sheet of the module (link Ordering data)

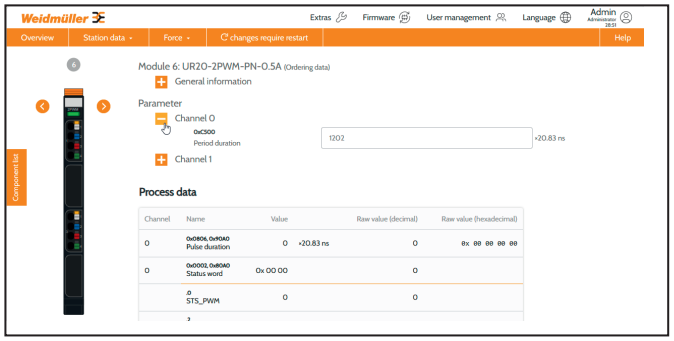
The module settings are only accessible when force mode is not active.

Parameters can only be written when the field bus is not active.

9.1 Displaying and editing parameters

◊ Changing parameters requires the necessary permission. Without permission, all parameters are diplayed in read-only mode but they are not editable.

► Open the module component view.
► Open the Parameters you want to change.
☑ The parameters are displayed.



Displaying and editing module parameters

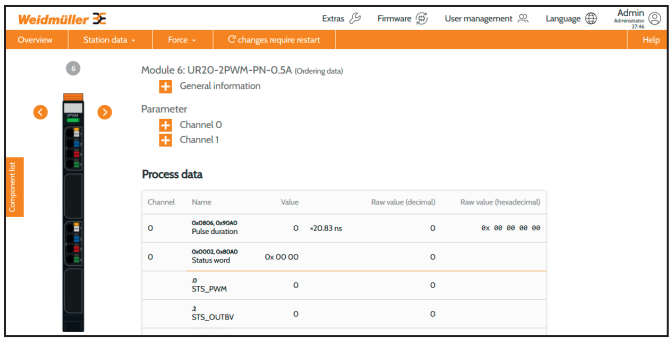
For parameters that can be edited, you can enter the changes in the entry fields or choose alternative settings from a drop-down list.

► Enter the desired changes.
► If you want to cancel the process, click **Restore.**
► To save all changes click **Apply changes**.
☑ The changes are adopted.

9.2 Displaying register settings

For modules with registers (e.g. counter modules and PWM modules), the register settings can be displayed in the process data overview.

► Open the module component view.
► If needed, close the parameters display to see the process data and the register settings.



Displaying the register settings

9.3 Displaying the data sheet

► To display the data sheet, click the **Ordering data** link next to the module designation.

A connection to the Weidmüller website is established in a new browser window and the data sheet is displayed as a PDF file.

10 Configuration and station data

10.1 File manager

◊ This function requires the necessary permission.

In the file manager, you can import and upload individual files and ZIP archives or export files.

Import files

You can import the following files:
- Parameters file
- Channelnames file
- Coupler firmware

When importing several files in a ZIP file, you can choose whether the files are uploaded individually or together into the coupler.

Export files

You can export the following files:
- Service file
- Audit log
- Parameters file
- Channelnames file
- Register description
- For Ethernet-IP couplers: Hardware config file (.l5x)

A channelnames file can only be exported after channels have been renamed, see Chapter 10.3

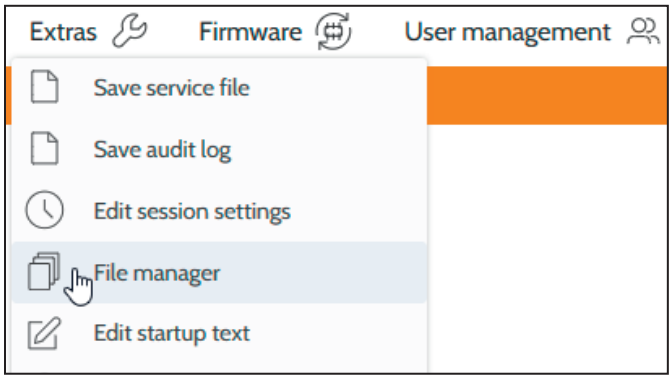
If you select several files, the files are automatically packed into a ZIP file during the export.

Channelnames

Here you can export a template for the channelnames file. After you have renamed channels, you can also restore the channel names to factory settings.

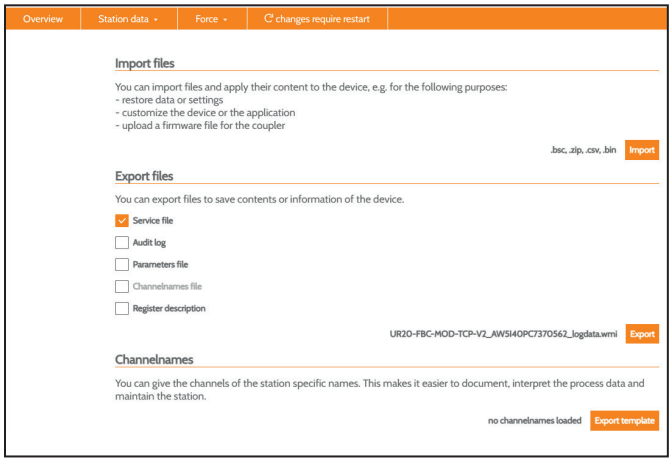
Opening the file manager

► Click **Extras** and then **File manager.**



Opening the file manager

☑ The file manager is opened.



File manager

10.2 Exporting or importing station parameters

◊ This function requires the necessary permission.

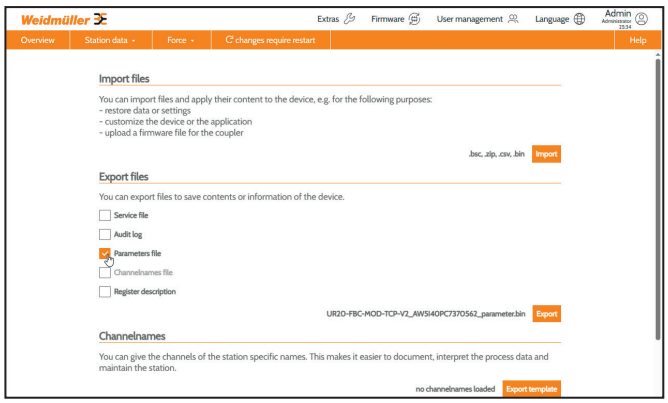
In a parameters file, you can export the current configuration of the u-remote station or import and upload an existing configuration into the coupler. This makes arranging several stations of identical setup very easy.

A saved configuration can only be loaded into the coupler, if the u-remote stations are physically identical (number, sequence and type of modules that are registered by the web server, see Chapter 5.2)

The following information will **not** be saved by the **stations parameters** function:
- IP address
- Gateway
- Subnet mask

For Modbus-TCP coupler only: The IP address will be set to 0.0.0.0 when loading a configuration into the coupler.

► Open the **File manager**.



Exporting or importing station parameters

► To export the configuration, select **Parameters file**.
► Click **Export**.
☑ The file **UR20-FBC...parameter.bin** is downloaded and saved to your download folder.

► To import a configuration, click **Import**.
☑ A file dialogue is opened.
► On you PC, choose the desired configuration file and click **Open**.
☑ A dialogue box is opened.

Uploading a parameters file

► Click **Upload**.

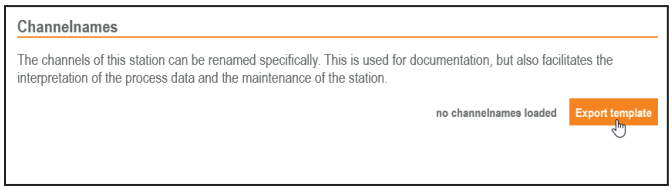
When using PROFINET or PROFIBUS you can continue working.
► With all other fieldbus protocols you have to restart the coupler.

10.3 Renaming channels

◊ This function requires the necessary permission.

In a channelnames file, you can define individual names for the channels of each module. You can transfer the channelnames file to other stations of identical structure to use the same channelnames on all stations. The user-defined channelnames can be reset to default at any time.

► Open the **File manager**.
First you need to export a template file which represents the entire station with all modules and channels.

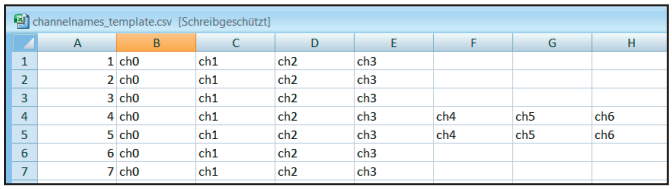


Exporting a template

► Click **Export template**.
☑ The file channelnames_template.csv is downloaded and saved to your download folder.

Observe the following notes when editing the template:
- The structure of modules and channels may not be changed in this file, otherwise it will no longer be compatible with the station.
- Do not use commas or semicolons for channel names, since these are interpreted as seperators in a CSV file.
- If you use mutated vowels or special characters, make sure to safe the CSV file UTF-8-encoded.

Editing the CSV-file using Microsoft® Office Excel®


channelnames_template.csv [Schreibgeschützt]

	A	B	C	D	E	F	G	H
1	1	ch0	ch1	ch2	ch3			
2	2	ch0	ch1	ch2	ch3			
3	3	ch0	ch1	ch2	ch3			
4	4	ch0	ch1	ch2	ch3	ch4	ch5	ch6
5	5	ch0	ch1	ch2	ch3	ch4	ch5	ch6
6	6	ch0	ch1	ch2	ch3			
7	7	ch0	ch1	ch2	ch3			

Template file with placeholders for tag names (view in Excel)

The structure of columns and rows must not be changed.

Editing the CSV-file using a text editor

```
1;ch0;ch1;ch2;ch3;;;;;;;;;;;;
2;ch0;ch1;ch2;ch3;;;;;;;;;;;;
3;ch0;ch1;ch2;ch3;;;;;;;;;;;;
4;ch0;ch1;ch2;ch3;ch4;ch5;ch6;ch7;ch8;ch9;ch10;ch11;ch12;ch13;
ch14;ch15
5;ch0;ch1;ch2;ch3;ch4;ch5;ch6;ch7;ch8;ch9;ch10;ch11;ch12;ch13;
ch14;ch15
6;ch0;ch1;ch2;ch3;;;;;;;;;;;;
7;ch0;ch1;ch2;ch3;;;;;;;;;;;;
```

Template file with placeholders for tag names (view in a text editor)

The separating characters (semicolons) must not be changed or deleted.

► Overwrite the place holders with the desired channel names.
► If you want no tag name for a certain channel, delete the respective place holder.
► After you have changed all names as desired, save the file on the computer using a proper file name.

The new channel names will be displayed in the webserver after the file has been imported and uploaded to the coupler.

Importing and uploading a channelnames file

◊ This function requires the necessary permission.

► Open the **File manager**.
► Click **Import**.
► On your PC, choose the desired file and click **Open**.
☑ A file dialogue is opened.

Uploading a channelnames file

► Click **Upload**.
☑ The file is loaded into the coupler.
☑ The current channel names are now displayed in the web server. The **Restore default** button is displayed.

Exporting a channelnames file

◊ This function requires the necessary permission.

If you have renamed the channels of a station or saved the channel names, you can export the channel names to a file.

► Open the **File manager**.
► Click **Channelnames file**.
► Click **Export**.
☑ The file **channelnames_template.csv** is downloaded and saved to your download folder.

In the file, the station is recorded with all channels and their names.

Deleting user defined channel names

◊ This function requires the necessary permission.

► Open the **File manager**.
► To delete all user-defined channel names, click **Restore default**.
☑ All channel names are reset to factory settings.

10.4 Saving a L5X file

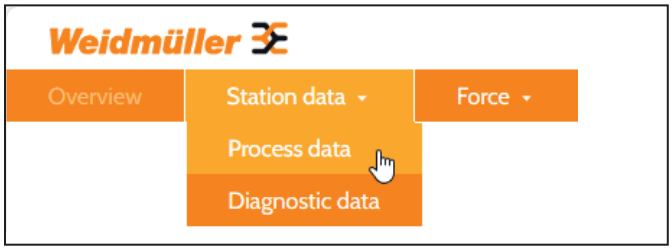
This function is only available for the UR20-FBC-EIP coupler.

You can export the module configuration of the u-remote station to a device configuration file (.l5x). You can then import the file as a routine into the **Studio 5000** Rockwell software.

► Open the **File manager**.
► Select **Hardware config file (.l5x)**.
► Click **Export**.
☑ The file is downloaded and saved to your download folder.

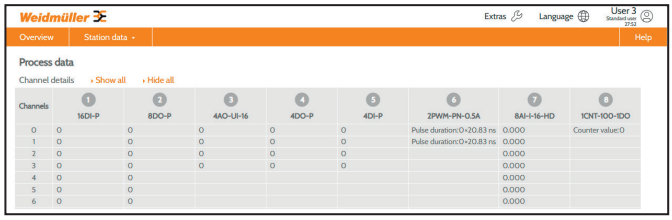
10.5 Displaying process data

► Click **Station data/Process data**.



Menu Station data/Process data

☑ The overview displays the channels of all modules each with its first value.

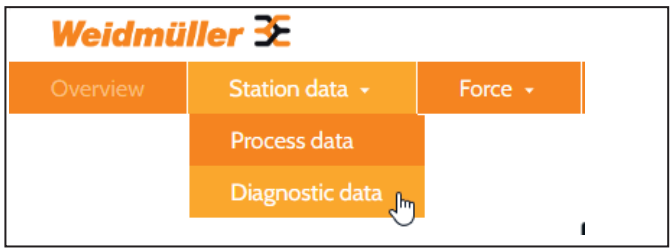


Display of process data

► Click **Show all** to see the entire overview with all values. The values are continuously updated.

10.6 Displaying diagnostic data

► Click **Station data** and then **Diagnostic data**.



Menu Station data/Diagnostic data

The overview displays all current diagnostic messages. Components without diagnostic message are not displayed.

Display of diagnostic data

11 Web server in force mode

11.1 Activating the force mode

⚠ WARNING

Manipulation of the control unit!
In force mode, the system may be manipulated to such an extent that can result in life-threatening personal injury and damage to materials.

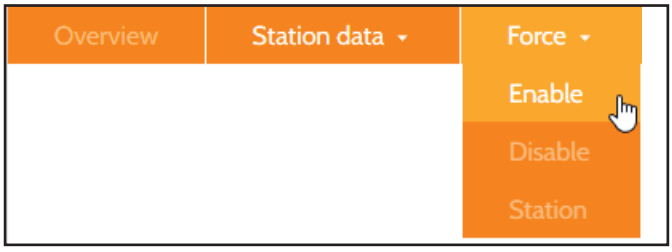
Only use force if you are very familiar with the connected system and know at all times the consequences that your actions will have!

If the force mode is activated during an established field bus connection a diagnose alarm is generated. Depending on parametrised alarm behaviour the PLC can continue to transmit output process data and the u-remote station will process them for all unforced output channels. However, forced output channels will ignore any process data and behave according to forced values.
Input process data are transferred all the time, independently whether they are simulated by forcing or read via the physical inputs.

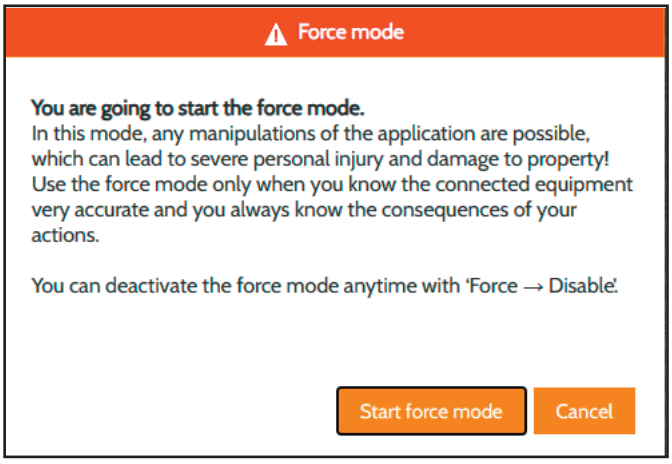
If the force mode is activated without an established field bus connection the fieldbus interface will be deactivated for the duration of forcing. Another fieldbus connection can only be established after the force mode has been deactivated.

Safety related modules (safe I/O modules and safe power-feed modules) can not be forced.

The force mode allows you to carry out functional tests or preconfigure the station prior to commissioning, even if sensors have not yet been connected. To do so, you must change the operating mode of the web server.
► Click **Force/Enable**.



Menu Force/Enable



Starting the force mode

► Click **Start force mode**.

The web server is now in force mode, recognisable by the signal red bar above the station view. Forced channels are marked with a red border line.

Display of the station in force mode

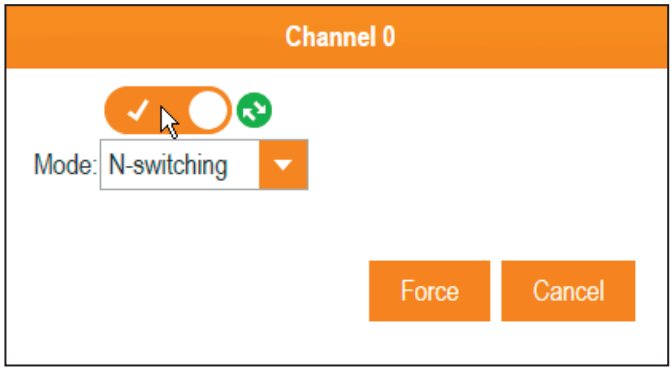
If the connection between web server and coupler is interrupted, the force mode is stopped immediately.

11.2 Forcing via the station view

► Click on the channel to be forced.

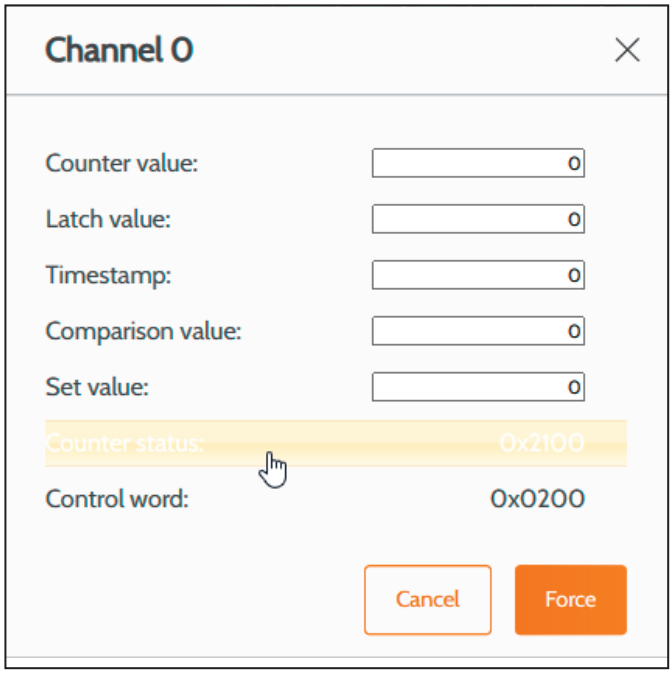
Dependent on the module type there are different options:

► To switch an output, click the switch and then **Force**.



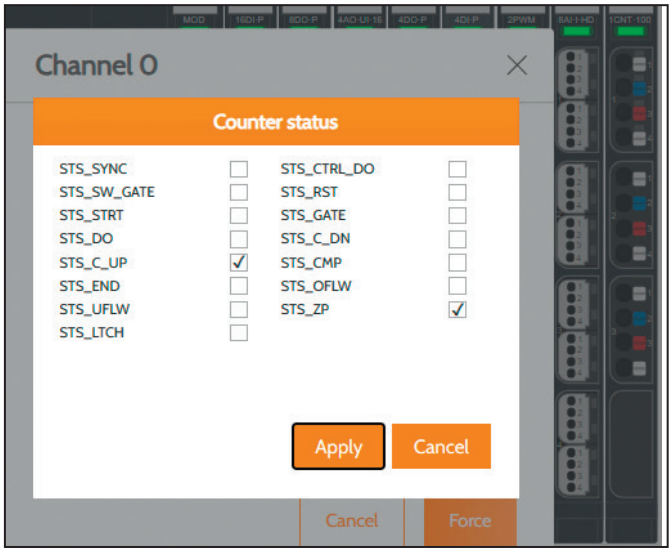
Forcing an output

► To force counter readings, type in the force values and click **Force**.



Forcing of modules with registers

► To force status or control registers (e.g. with counter modules or PWM modules), click on the corresponding entry.



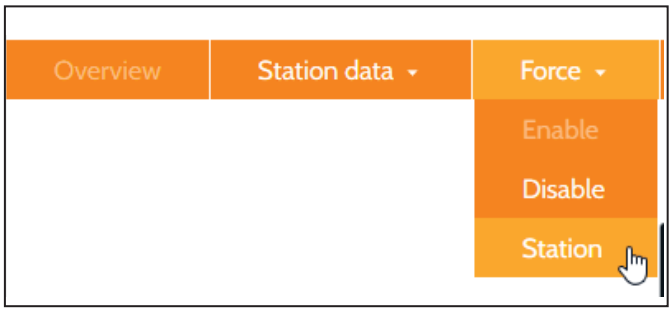
Forcing registers

► Set or remove the check mark for each register to be forced and click **Apply changes**.
► Click **Force**.
☑ The changes are transferred to the coupler.

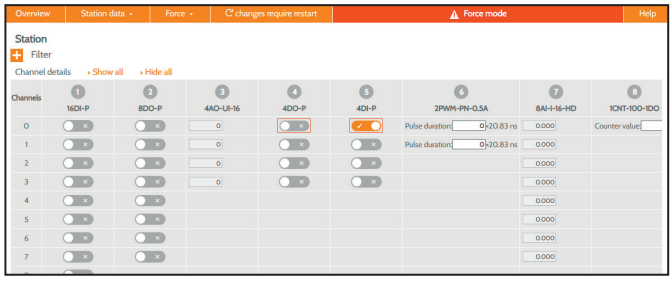
11.3 Forcing via the detail view

For a better survey change to the detail view. In this view modules can be shown and hidden, which is helpful, especially when working with larger stations.

► Click **Force/Station**.



Switching to detail view in force mode



Detail view of the station in force mode

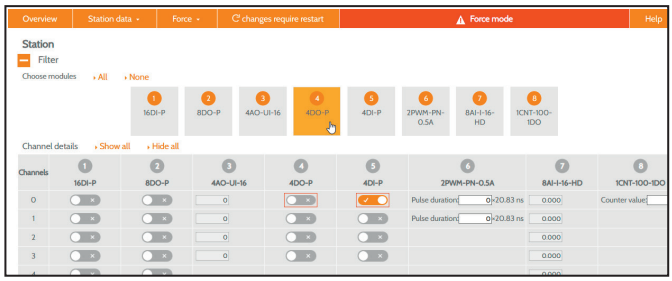
All active modules are displayed in the detail view. The switchable channels are provided with a switch.

- ► To see all channel details, click **Show all**.
- ► To see only the first value of each channel, click **Hide all**.

Filtering the module view

If you only want to see the modules that you would like to force, use the filter function.

- ► Click **Filter**.
- ► To show or hide a module in the overview, click the respective module in the filter bar.



Filtering the displayed modules

Displayed modules are highlighted grey in the filter bar, while hidden modules are displayed in white.

Resetting filters

- ► To display all modules again, click **All**.
- ► To hide all modules, click **None**.

Forcing channels

Depending on the module type you can force channels directly either by clicking on the switch or typing in a value.

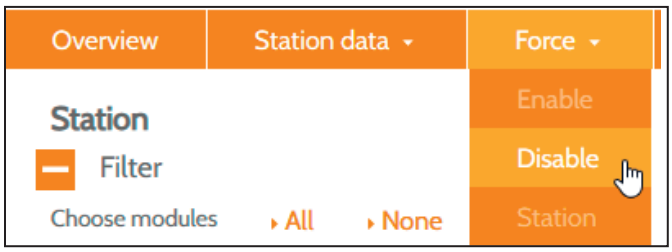
- ► Enter the desired changes.

Each change is marked with a green symbol until it is applied. All changes will only be saved after you click **Apply changes**. All changes will be undone after you click **Restore**.

- ► After entering your changes, click **Apply changes** to start forcing.
- ☑ Changes are transferred to the coupler, the green markings are removed.

11.4 Deactivating the force mode

- ► To deactivate the force mode, click **Force/Disable**.



Deactivating force mode

- ☑ The station is reset to the state it had before the force mode was started.

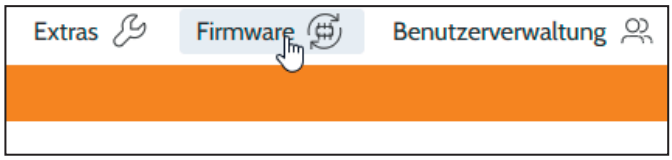
12 Updating the firmware

► Download the latest firmware for each component you want to update from the Weidmüller Support Center.

Firmware files for fieldbus couplers have the extension **.bsc**. For PROFINET couplers, for instance, the file might be named FBC-PN-IRT-00XX.bsc. The compatibility is checked during uploading the coupler firmware. Thus it is not possible to load an incompatible coupler firmware.

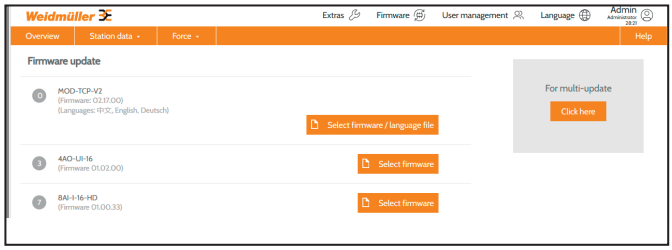
Firmware files for modules have the extension **.bsm**. You can determine for each individual module of a station whether an update is to be carried out.

- A firmware update cannot be undone. The old firmware in the coupler or module is overwritten.
- While uploading the firmware files you cannot access the station via the web server.
- While uploading the firmware files, ensure the following:
  - The power supply must not be interrupted.
  - No modifications must be carried out on the u-remote station.



Menu firmware update

► To carry out a firmware update, click **Firmware**.
☑ All components with a firmware are displayed with their version status.



Overview of the existing firmware

Single update

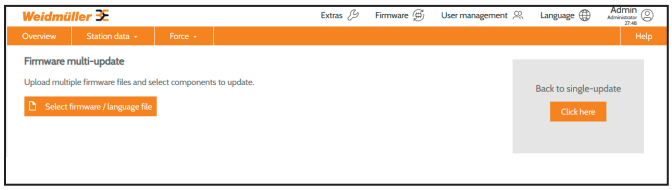
► If you want to update the firmware of a single component (e.g. only the coupler), click **Select firmware** beside this component.
► Select the firmware file from the storage location on your PC and click **Open**.
► Click **Update now**.

The firmware is updated. As long as the update is running, the **BF** LED on the coupler flashes red. Once the data has been transferred, you are asked to restart the coupler.
► Click **Reset**.
► Wait until the coupler has been restarted and the station view is displayed in the web server.

Multiple update

If you want to update several components, use the multiple update.
► Click **Click here** below **For multi-update** and then **Select firmware/language file**.
► Select the firmware files from the storage location on your PC and click **Open**.
☑ The firmware files are displayed in the **Firmware multi-update** dialogue.

► Checkmark all files you want to update.



Checkmarking firmware files for multiple update

► You can deselect single components by clicking on the checkmark. These components will not be updated.
► You can delete each single file in the overview by clicking on the red and white cross.
► After selecting all desired files and the components, click **Update now**.
☑ The firmware is updated.

As long as the update is running, the **BF** LED on the coupler flashes red. Once the data has been transferred, you are asked to restart the coupler.
► Click **Reset**.
► Wait until the coupler has been restarted and the station view is displayed in the web server.

In case the web server does not restart, please act as follows:
► Clear the temporary browser data (cache). Deleting the browser protocol is not sufficient.
► Start the web server again.

13 FAQ, help and documentation

13.1 The web server cannot be loaded

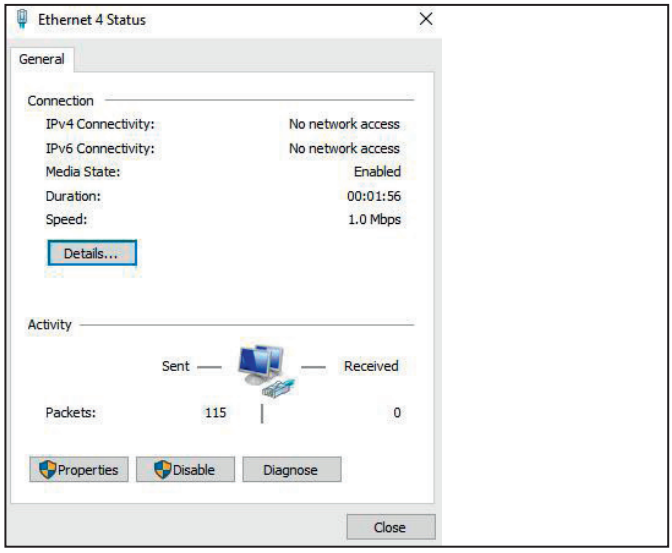
- Are coupler and PC properly connected via an USB cable?
- Is the IP address for the USB port set correctly (see Chapter 13.2)
- Clear the temporary browser data (empty cache, deleting the browser protocol is not sufficient) and reload the web server.
- If you call up the web server via HTTP, try calling up the web server via HTTPS.
- Check whether your IT security guidelines allow access via HTTPS, if the server certificate has not been signed by a trusted certificate authority.

13.2 Identifying the IP address of the USB port

The following addresses can be used for the USB port: 192.168.1.202 (default), 192.168.2.202, 192.168.3.202, 192.168.4.202, 192.168.5.202 (default with UR20-FBC-EIP).
You can identify the IP address in the Network and Sharing Center via the Windows control panel.

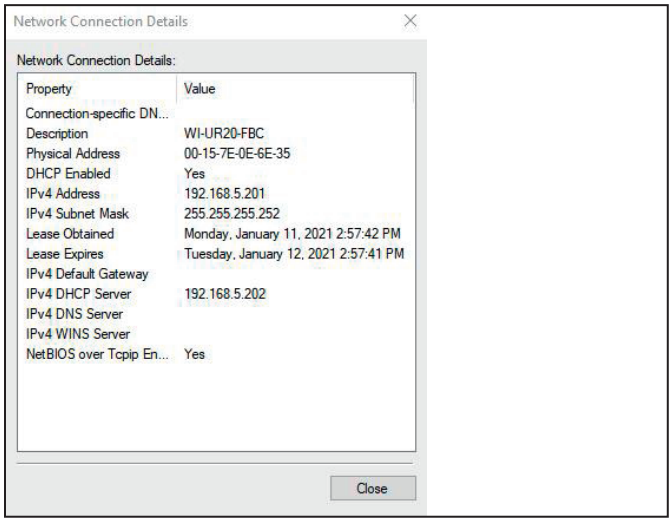
► Click the name of the connection that is displayed as **Unidentified network** (in the following example **Ethernet 4**).

The **Ethernet 4 Status** window is opened.



Ethernet 4 Status

► Click **Details...**.
The **Network Connection Details** window is opened.



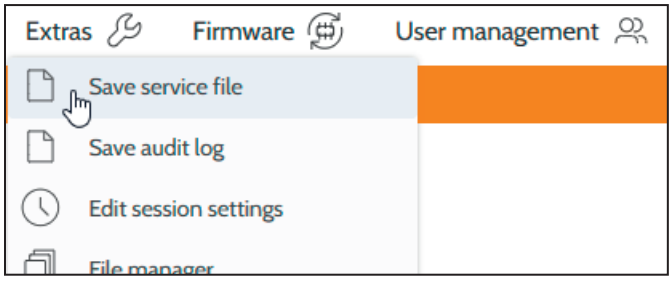
Network Connection Details

The IP address of the virtual LAN port (USB connection) is displayed next to **IPv4 DHCP server**. The standard IP address of the fieldbus coupler is: 192.168.1.202.

13.3 Saving a service file

In the event of problems and service cases, it may be helpful to save the current log data for the u-remote station. This data can provide service technicians with important information in the event of malfunctions.

► Click **Extras** and then **Save service file**.



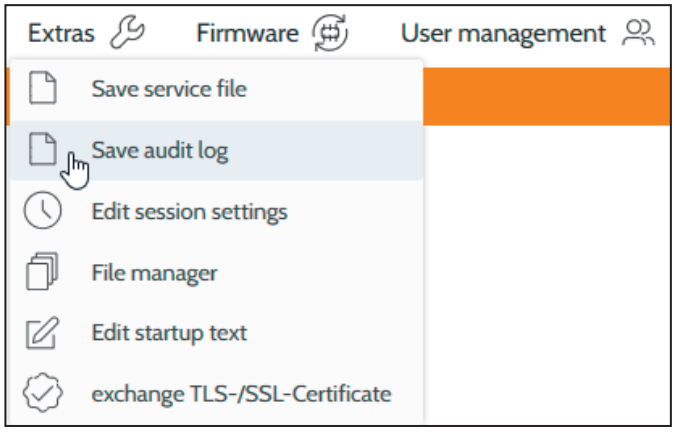
Menu Extras/Save service file

► Select a storage location on your PC for the service file (**logdata.wmi**) and click **Save**.
☑ The service file **UR20-FBC..._logdata.wmi** is downloaded and saved to your download folder.

13.4 Saving a audit log

The following events are logged in the audit log:
- Access (login, logout)
- User management (creating and deleting users)
- Change of security settings

► Click **Extras** and then **Save audit log**.

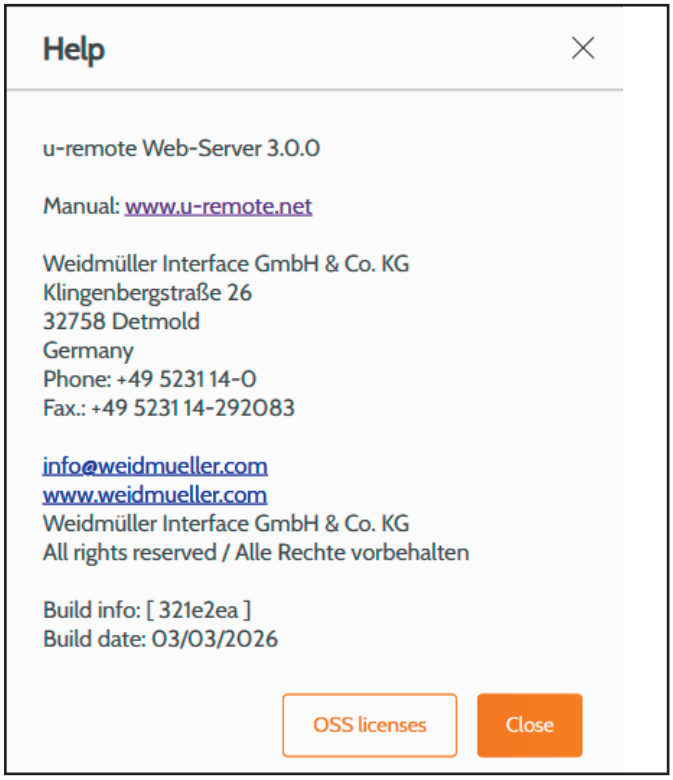


Opening Save audit log

☑ The log file **UR20-FBC..._auditlog.cvs** is downloaded and saved to your download folder.

13.5 Help and documentation

► Click **Help**.
☑ A dialogue box is opened.



Help dialogue

► To open the manuals for the webserver and the u-remote station, click the link.
☑ A connection to the Weidmüller website is established in a new browser window.

► To display the licenses of the used open source software, click **OSS licenses**.
☑ The lincence informatioan are displayed in a new window.

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
www.weidmueller.de

Personal support can
be found on our website:
www.weidmueller.com/contact

Order number: 2112220000/08/02.2026