TECHDOCS

WAGO Software

WAGO Device Sphere

Product manual
SW version 1.3.0
3953553547 | 3 | en-US | 2026-05-27 15:52

© 2026 WAGO GmbH & Co. KG
All rights reserved.

WAGO GmbH & Co. KG
Hansastraße 27
D - 32423 Minden
Phone: +49 571/887 – 0
E-Mail: info@wago.com
Internet: www.wago.com

Technical Support
Phone: +49 571/887 – 44555
E-Mail: support@wago.com
Internet: www.wago.com/support

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present documentation are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Provisions

This documentation applies to the WAGO Device Sphere software, software version 1.3.0.

Table 1: Scope of Applicability – Versions

Version WAGO Device Sphere	Documentation Version
1.3.0	3

Note

Note applicable documents!

The complete operating instructions for the software consist of several applicable documents. The software must only be installed and operated in accordance with the complete operating instructions. Knowledge of all applicable documents is required for proper use.

Applicable documents

Technical Information WAGO Device Sphere,
available from: https://downloadcenter.wago.com

WAGO Device Sphere API Documentation Online Help
integrated into the WAGO Device Sphere software and available from:
`https://<HostName>/api-documentation`

WAGO Device Sphere API (Swagger) Online Help
integrated into the WAGO Device Sphere software and available from:
`https://<HostName>/api/doc`

Additional documents

- Product manuals of the configurators used
- Product manuals of used products
- Product Manual of the software used
- Terms of Use
  integrated into the WAGO Device Sphere Software (see Footer Bar [▸ 40])
- Release notes
  integrated into the WAGO Device Sphere software (see Footer Bar [▸ 40])
- Software Bill of Materials (SBOM)
  integrated into the WAGO Device Sphere software and available from:
  C:\Program Files\WAGO Software\WAGO Device Sphere\WDS\Documents

Please find all documents and information at:

www.wago.com/de/wago-device-sphere

1.1 Intended Use

The WAGO Device Sphere software is a central server platform for administration of a large number of different controllers. It can be used to manage both controllers that are directly accessible and controllers that are not directly accessible. The software allows installers to organize all their controllers in a central database and process them in parallel. The software can be used for the following tasks:

- Commissioning:
  Direct commissioning of new controllers without the need for pre-configuration.
- Monitoring:
  Monitoring of existing controllers. The software provides direct information about status changes or error situations.
- Management:
  Structured management of existing controllers.
- Update:
  Central update rollout for all controllers.

Software operation is only permitted if the system requirements and license conditions are met.

Improper Use

Improper use of the software is prohibited.

Improper use occurs in particular in the following cases:
- Non-observance of the intended use
- Implementation of a Known Misuse
- Use of the software in areas with special risk that require continuous fault-free operation and in which failure of or operation of the software can result in an imminent risk to life, limb or health or cause serious damage to property or the environment (such as the operation of nuclear power plants, weapons systems, aircraft and motor vehicles)

Warranty and Liability

The provisions of the latest WAGO General Terms and Conditions of Deliveries and Services (GTC) apply as well as the Software License Terms for Standard Software (SW-License) applicable to software products und software embedded in WAGO hardware products, both available at: **www.wago.com**.

In particular, the warranty is void when:
- The software is improperly used.
- The defect is based on (customer-)specific specifications (hardware and software configurations).
- Modifications of the hardware or software by the user or third parties were made that are not described in this documentation and are at least responsible for the occurrence of the defect.

Individual agreements always take precedence.

Obligations of the installer/operator

The responsibility for the safety of an installation or system assembled with the software lies with the installer/operator.

The installer/operator is responsible for the proper installation and the safety of the system. It must comply with the laws, standards, guidelines, local regulations, the state and the rules of technology applicable at the time of installation and must observe the guidelines and instructions described in the operating instructions. The installation requirements of the approvals must also be met.

In the event of non-compliance, the software may not be operated within the scope of the approval.

1.2 Typographical Conventions

Number Notation

100	Decimals: Normal notation
0x64	Hexadecimals: C-notation
'100'	Binary: In single quotation marks
'0110.0100'	Nibbles separated by a period

Text Markups

italic	Names of paths or files
bold	Menu items, entry or selection fields, emphasis
`Code`	Excerpts from program code
>	Selection of a menu point from a menu
"Value"	Value entries
[F5]	Identification of buttons or keys

Links

	Link to a topic in a document
	Link to a separate document
	Link to a website
	Link to an email address
Glossary	Link to a glossary entry

Sequence of Action

✓ This symbol identifies a precondition.

1. Action step
2. Action step

   ⇨ This symbol identifies an intermediate result.

➡ This symbol identifies the result of an action.

- Individual action step

Lists

- Lists, first level
  - Lists, second level

Figures

Figures in this documentation are for better understanding and may differ from the actual product design.

Warning Messages

⚠ DANGER

Type and source of hazard

Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.

- Action step to reduce risk

⚠ WARNING

Type and source of hazard

Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

- Action step to reduce risk

⚠ CAUTION

Type and source of hazard

Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

- Action step to reduce risk

NOTICE

Type and source of malfunction (property damage only)

Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

- Action step to reduce risk

Information Notices

Note

Information

Indicates information, clarifications, recommendations, referrals, etc.

1.3 Legal Information

Intellectual property

The intellectual property of this document belongs to WAGO GmbH & Co. KG. The reproduction and distribution of its content (in whole or in part) is prohibited, unless otherwise provided by statutory provisions, written agreements or this document. In case of doubt, the written consent of WAGO GmbH & Co. KG must be obtained in advance.

Third-party products are always mentioned without any reference to patent rights. WAGO GmbH & Co. KG, or the manufacturer of third-party products, retains all rights regarding patent, utility model or design registration.

Third-party trademarks are referred to in the product documentation. The "®" and "™" symbols are omitted hereinafter. The trademarks are listed in the Appendix: **Protected Rights [▸ 70]**.

Subject to Change

The instructions, guidelines, standards, etc., in this manual correspond to state of the art at the time the documentation was created and are not subject to updating service. The installer and operator bear sole responsibility to ensure they are complied with in their currently applicable form. WAGO GmbH & Co. KG retains the right to carry out technical changes and improvements of the products and the data, specifications and illustrations of this manual. All claims for change or improvement of products that have already been delivered – excepting change or improvement performed under guarantee agreement – are excluded.

Licenses

The software and related components are protected by license mechanisms. You can find more information at: **Licenses [▸ 14]**.

2 Security

2.1 General Safety Regulations

- This documentation is part of the software. Therefore, keep the documentation for the entire service life of the software. Pass on the documentation to the next user of the software. In addition, ensure that any supplement to this documentation is included, if necessary.
- Any actions related to the use of WAGO software may only be performed by qualified staff with sufficient knowledge to use the respective PC system.
  Steps in which files are created or changed on a PC system may only be performed by qualified employees with sufficient knowledge in the administration of the PC system used in addition to file creation or modification.
  Steps that change the PC system's behavior within a network may only be performed by qualified employees with sufficient knowledge of administration of the responsible network.
- Set up permissions management for authorized persons.
  – Digital access may only be made by authorized persons.
- Comply with the laws, standards, guidelines, local regulations and accepted technology standards and practices applicable at the time of installation.

2.2 Indirect Safety

- If automation solutions are implemented that can lead to personal injury or significant property damage in the event of failure, you must take appropriate measures to ensure that the system remains in a safe operating state even in the event of failure.
- Give all products in a network different IP addresses.
- Never connect a PC on which a DHCP server is installed to a global network. Larger networks usually already have a DHCP server, which can cause collisions that lead to network breakdown.
- Use only the latest security software.
- Uninstall or disable all software components or programs on your PC that are not required for the intended use.

2.3 Cybersecurity Capabilities

Encrypted Communication

The integrated server enables encrypted communication with the products for access to the Web-Based Management.
Note: The encryption capability applies to this interface; the product may have other interfaces that do not support encryption.

Encrypted communication takes place via secure protocols:

- "Transport Layer Security" (TLS 1.2) makes it possible to securely establish communication between the devices used and the software.

Session Locking

Session locking protects against unauthorized access when inactive. A session can be locked after a configurable period of inactivity or by actively logging out. Access is restored once the user has been authenticated.

- The software has an automatic session lockout feature that activates after 10 minutes of inactivity.
- The duration of the inactivity time can be set.

Secure Identification and Authentication

Access to the software is only possible with authentication.

- Integrated authentication method
  - Token-based authentication
- User-defined authentication method

Trusting Devices

- The software rejects configuration for untrusted devices.

Password Strength

A strong password reduces the likelihood of unauthorized access.

- The software checks the password strength (password quality).

3 Overview

The WAGO Device Sphere (WDS) software is a solution for central management of controllers. The software includes a standalone server to communicate with existing controllers.

In addition to the controllers themselves, this software provides a Commissioning Service that can be opened via Web-Based Management. If the service is active, the selected controller automatically searches for the server in the network and logs into it. This controller can then be selected and integrated into the software. After that, the initial controller setup process is performed in the WAGO Device Sphere software.

On the conceptual level, a digital twin is created in the WAGO Device Sphere software to provide a representation of the physical controller. Parameters can be set on either of these and synchronized between the layers.

3.1 Topology

This visually illustrates the interdependencies among the individual components of the program package (see **Overview [▸ 12]**) and the individual functions that they provide.

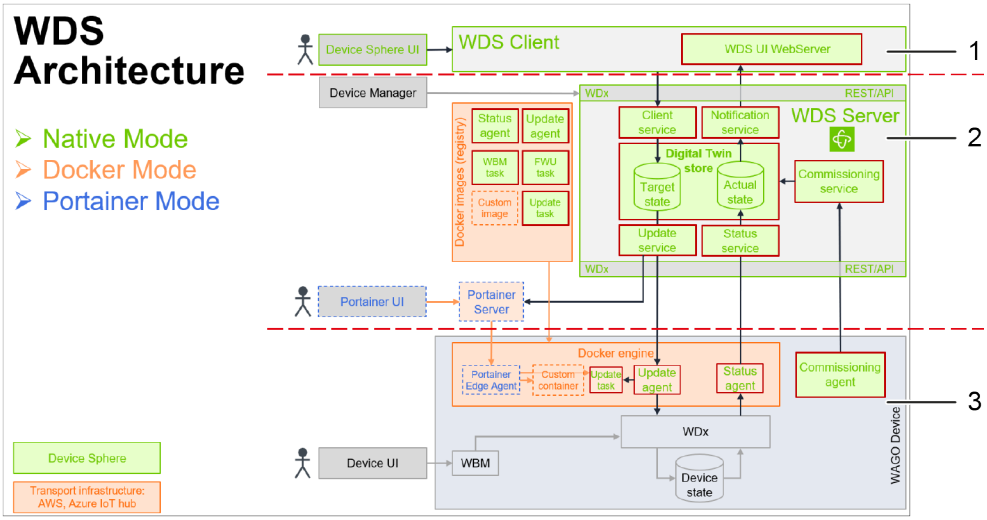


Figure 1: Topology

Position	Area	Description
1	WAGO Device Sphere Client	**Top level:** This level provides a graphical user interface for configuring and parameterizing controllers.
2	WAGO Device Sphere Server	**Middle level:** This level is for configuring and parameterizing connected controllers. The WAGO Device Sphere server receives status messages from controllers and saves them. The WAGO Device Sphere server also provides all tasks and artifacts that can be retrieved by the controllers (the rollout principle).

Position	Area	Description
3	WAGO Device	**Bottom level:** On this level, the controllers connect to the WAGO Device Sphere server autonomously. This procedure enables communication with controllers that cannot establish incoming connections, for example, because they are installed in an isolated environment (but allow an outgoing connection). The first time they connect, the “Update Agent” and “Status Agent” are obtained through the “Commissioning Agent.” Both agents are installed as soon as the controller is actively connected. The agents serve to configure and parameterize the individual controllers via the WAGO Device Sphere server. The request always originates from the controller (request direction: controller → server).

4 Requirements

4.1 System Requirements

The WAGO Device Sphere software is installed on a PC as a local desktop application. The PC must meet at least the following system requirements:

Minimum System Requirements

Table 2: Minimum System Requirements

Component	Requirements
Operating system	Windows 10 Windows 11 Windows Server 2022
Memory	8 GB
Free hard disk space	50 GB
Processor	4 CPU cores
Screen resolution	1366 × 768 pixels

Recommended System Specifications

Table 3: Recommended System Specifications

Component	Requirements
Operating system	Windows 10 Windows 11 Windows Server 2022
Memory	32 GB
Free hard disk space	500 GB
Processor	16 CPU cores
Screen resolution	1920 × 1080 pixels

4.2 Licenses

Using the full scope of the WAGO Device Sphere software with an unlimited number of controllers requires a license.

Software

After registering for the first time in the WAGO Device Sphere software, you can use the software's full scope for 30 days for testing purposes without a license key. During the evaluation period, a banner appears in **Start View [▸ 41]** indicating how much longer the evaluation license remains valid.

Activation

The licenses are valid for one year. This validity period starts when the license is activated.

After activation, the banner in the Start View disappears. A green check mark appears by the **"Licensing" Menu Item [▸ 54]**:

Figure 2: "Licensing" Menu Item: Activated License

In the "Licensing" Menu Item [▸ 54], the "License Repository" tab lists all purchased and activated licenses.

WAGO offers server licenses specifically for the WAGO Device Sphere software. For information, visit the WAGO Download Center: https://downloadcenter.wago.com.

4.3 Hardening Measures

The hardening measures described are not alternatives to one another. To ensure good protection, the various hardening measures must be implemented in addition to each other.

4.3.1 Secure Operating Environment

Operation of the software is only permitted in a secure operating environment.

A secure operating environment helps prevent various attacks. A secure operating environment meets the following requirements at a minimum:
- Protected network segment
- Protected access

Protected Network Segment

The software consists of a server, in addition to other elements. This server contains databases with unencrypted data.

Use of the software is only permitted in a secure operating environment that meets at least the following requirements:
- There is no unprotected connection to the Internet.
- There is no unprotected connection to other network segments.
- Access authorization is performed in accordance with authorization management.
- All network devices are located in a protected network segment.

Protected Access

The software loads firmware onto devices.

Its use is only permitted on a protected engineering device that meets at least the following requirements:
- Access requires authorization and a uniquely identifiable user account.
- The session lock on the engineering device is set up.

4.3.2 Secure Operation

Secure software operation helps prevent various attacks. Secure operation meets at least the following requirements:
- Use of tested and current software/updates

Tested and Current Software (Updates)

- Only use tested and current software (updates).

The following requirement is a property of tested and current software/updates:
- Checksum was successfully verified (integrity check).

WAGO recommends using up-to-date software.

The up-to-date version of a software solution corresponds to the current state of the art and security. Earlier versions of software may have technical and security vulnerabilities.

For current tested WAGO software (and updates) and information on installation, see:

https://downloadcenter.wago.com

WAGO Navigator

For more information, please contact:

Technical Support

5 Installation

Secure installation of the software helps to prevent various attacks. A secure installation meets at least the following requirements:

- Temporary certificates are only used for installation.
- Keys are on the server.
- Certificates are on the server.

The WAGO Device Sphere software is installed as a setup package. By default, this setup package includes the main component, WAGO Device Sphere. The WAGO Device Sphere software consists of three Web services (Server, Auth and UI) and two databases (PostgreSQL database and Mongo database).

The following installation options are available:

- **Full install:**
  Installs all the components in the work environment used. All the components can then be used without limitation and executed in this work environment.
- **Distributed installation:**
  Only installs individual components in the work environment used. All the other components can then be installed and run in other external work environments. For example, individual components could be executed on a local PC and the other components on a higher-level server.

The following components are installed and configured during the installation process according to the installation type selected:

- WAGO Device Sphere Authorization
- WAGO Device Sphere PostgreSQL (database)
- WAGO Device Sphere MongoDB (database)
- WAGO Device Sphere Server
- WAGO Device Sphere UI

5.1 Installing on Windows

Follow the steps below to install the WAGO Device Sphere software on Windows:

✓ You must have the current version of the software downloaded.
You can find the software in the WAGO Download Center at **https://downloadcenter.wago.com**

1. Start the installation process by double-clicking the installation file.
2. Select the installation language.
3. Accept the license agreements.
4. Select the target directory.
5. Select “Full Install” if you want to install all the components in a work environment.
6. Select “Custom Install” if you only want to install subcomponents in a work environment.
7. Select an existing CA certificate, or have the software generate a certificate.
8. If you want to have it generate a new CA certificate:
   Assign a strong password.
   (Minimum length: 16 characters, at least one capital letter, at least one number)
9. Select a username for the initial administrator account.

10. Assign a strong password.
    (Minimum length: 16 characters, at least one capital letter, at least one number)
11. Enter an email address.
12. Enter the data of an outgoing mail server for notifications.

    ⓘ Note **User data is not processed further!**

    All the user data you enter is only saved locally on the installed server. Entering an email address is optional; if you do so, it is not transmitted to WAGO GmbH & Co. KG and/or further processed there.

13. Configure the hostname and communication ports of the selected components.
14. Assign a PostgreSQL password.

    ⓘ Note **PostgreSQL password required!**

    In the "PostgreSQL Password" input field, assign an initial superuser password for the WAGO Device Sphere software database.

    Be sure to remember the assigned password!

15. Specify where shortcuts should be created in the Start menu.
16. Click **[Install]**.

5.2 Install on Linux®

Follow the steps below to install the WAGO Device Sphere software on Linux:

✓ You must have the current version of the software downloaded.
You can find the software in the WAGO Download Center at **https://downloadcenter.wago.com**

✓ You have sufficient permissions to install additional programs.

1. Open the terminal.
2. Navigate to the script:

   ⇨ e.g., *cd Downloads/*

3. Enter *./setup.sh* to run the script and start the installation.

   ⇨ The installation operation starts.

4. Read and accept the license terms.

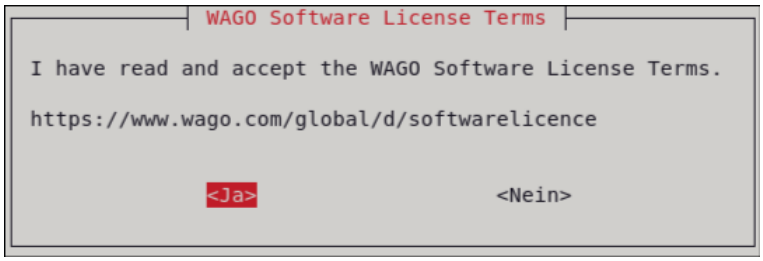


Figure 3: Accept License Terms

5. Configure the hostname.

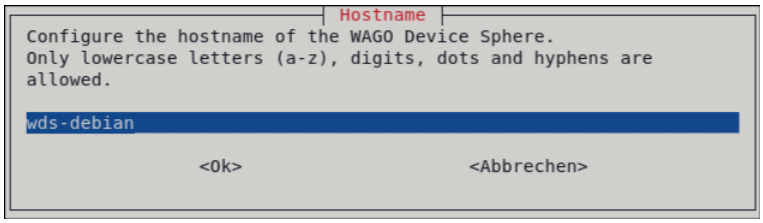


Figure 4: Configure Hostname

6. Import an existing certificate file or create a new directory for certificates.

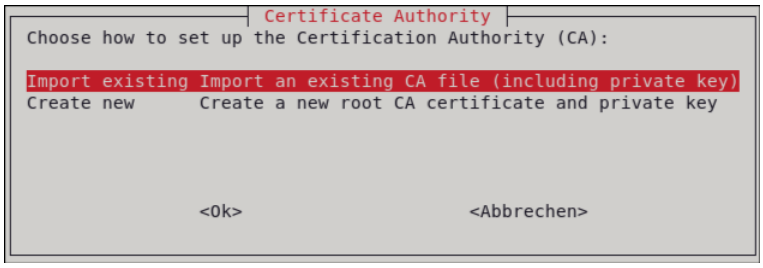


Figure 5: Set Up Certificates

7. Create a password to access the certificates.

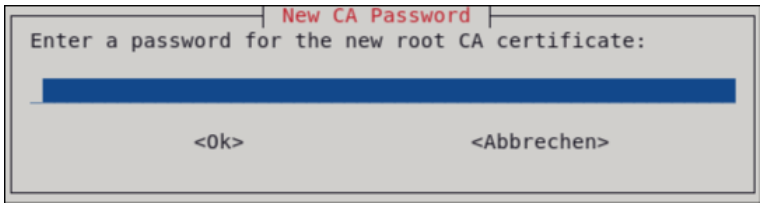


Figure 6: Set Up Password for Access to Certificate Directory

⇨ Reenter the password in the next step.

8. Assign a name for the admin account.

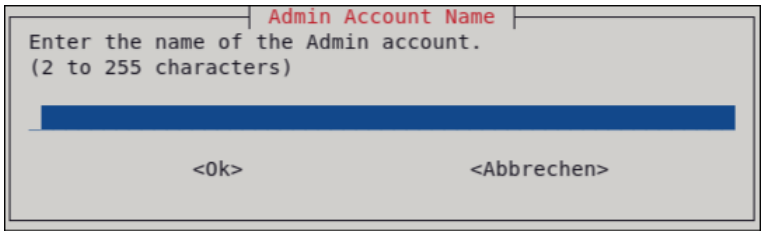


Figure 7: Enter Name for Admin Account

9. Create a password to access the admin account.

⇨ Reenter the password in the next step.

10. Enter an email address to be used for the admin account.
11. Enter the “UI Port” communication port.
12. Enter the “Auth Port” communication port.
13. Enter the “Server Port” communication port.
14. Enter the “MongoDB Port” communication port.
15. Enter the “PostgreSQL Port” communication port.

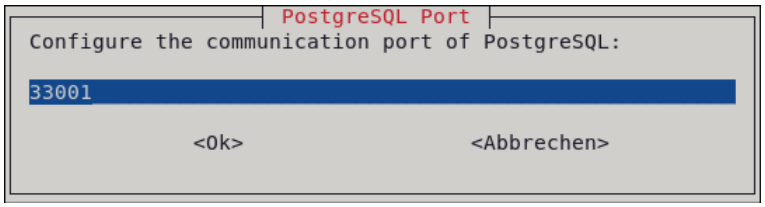


Figure 8: Enter communication ports (for example, the "PostgreSQL Port").

16. Enter the password for the "PostgreSQL Port" communication port.

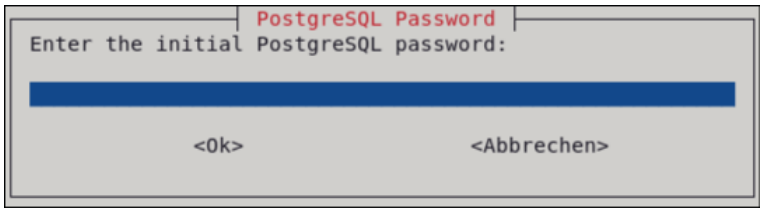


Figure 9: Enter password for "PostgreSQL Port" communication port.

⇨ The installation starts.

➡ The installation has been completed.

➡ Access the software via **https://[servername]:33000/**.

5.3 Backup and Restore

You should back up your data regularly so you can restore the most recent version possible at any time.

5.3.1 Store

All the data for backup is located in the following directory: **%programdata%\WAGO Software\WAGO Device Sphere**

- Back this directory up by copying it to a different location.

5.3.2 Restore

The data can only be restored on an equivalent system, i.e., the hostname and domain name (FQDN) must not change!

✓ The WAGO Device Sphere software must not already be installed on your new PC, or must have been removed!

1. Prepare the new PC.
2. Create the backed up folder **%programdata%\WAGO Software\WAGO Device Sphere** on the new target system.
3. Install the WAGO Device Sphere software.

5.4 Server Configuration

During installation, individual configuration files named **appsettings.json** are stored in the following directories:
C:\Program Files\WAGO Software\WAGO Device Sphere\WDS\Config
C:\Program Files\WAGO Software\WAGO Device Sphere\WDSAuth\Config
C:\Program Files\WAGO Software\WAGO Device Sphere\WDSUI\Config

These files must not be modified, since they will be overwritten with the next installation.

To make custom settings, you can create your own configuration files. For this purpose, you should create a separate configuration file for each specific setting; when settings are made later, this allows better structuring or targeted activation of them.

These configuration files must be stored in the "Config" subfolder of the **WDS**, **WDSAuth** and **WDSUI** modules under the following root directory: **C:\ProgramData\WAGO Software\WAGO Device Sphere**

For the individual configuration files to be included, they must be named **appsettings.json** or follow this naming scheme: **custom{ANY}.json**. The "PostgreSQL" and "MongoDB" components have different subfolders and are not structured according to this schema.

These files must have the same name, **appsettings.json**, and must also be stored in an identical directory structure under **C:\ProgramData\WAGO Software\WAGO Device Sphere**. This contains a "Config" folder for each of the modules **WDS**, **WDSAuth**, **WDSUI** and **MongoDB**. For the **PostgreSQL** module, there is a "Data" folder.

5.4.1 Email Account for Notifications

The WAGO Device Sphere software can send notifications via email. To use this functionality, you need an email account that can send emails.

You have the option of providing the relevant information during the software installation operation, but it can also be added or changed manually later: **C:\ProgramData\WAGO Software\WAGO Device Sphere\WDS\Config\customEmail.json**. Enter the following:

```
"SmtpConfiguration": {
    "Username": "wds-service@e-mail.com",
    "Password": "xxxxxxxxxxxxxxx",
    "FromEmail": "wds-service@e-mail.com",
    "SmtpServer": "mail.e-mail.com",
    "SmtpPort": 25
},
```

5.4.2 Docker Mode

The Device Agent can be deployed to the controller via Docker mode. The agent is then executed as a Docker container.

Before you can begin integration, you need the following information:

1. URL of the Docker registry
2. Port (http or https) for accessing the API

The Docker registry that the devices should use must be configured on the server. For this purpose, a configuration file must be added to the existing folder **C:\ProgramData\WAGO Software\WAGO Device Sphere\WDS\Config**. The filename corresponds to the template **custom<name>.json** (for example: **customDocker.json**).

Table 4: Configuration File

Setting	Description	Example
Location	Hostname and port of the registry	wdsserver:5000
Repository	Repository within the registry	WDS Agents
ConfigureInsecureRegistry	Boolean flag indicating whether the Docker registry on the device should be configured as an "insecure registry." If the flag is set to "true," the specified location is added to the "insecure-registries" array in the "Docker Daemon" configuration file.	true

The exact content of the file depends on whether you want to use the official WAGO registry or your own registry.

Using the WAGO Registry

The required Docker images for the Device Agent are provided in a publicly available Docker registry: **docker.cloudsmith.io/wago/wds-agents**. Add the following configuration options to the **customDocker.json** file to use the public registry:

```
{
    "ContainerRegistry": {
    "Location": "docker.cloudsmith.io",
    "Repository": "wago/wds-agents",
    "ConfigureInsecureRegistry”: false
    }
}
```

Using Your Own Registry

If a private Docker registry is used, the images for the Device Agent must be stored in this private registry. You can find the images in the folder **%ProgramFiles%\WAGO Software\WAGO Device Sphere\WDS\Scripts\Docker**. The command "import-images.ps1" then imports the images into the private registry.

A private registry must use trusted certificates.

```
{
    "ContainerRegistry": {
    "Location": "<<YOUR_REGISTRY_URL>>",
    "Repository": "<<YOUR_REPOSITORY>>",
    "ConfigureInsecureRegistry": true
    }
}
```

5.4.3 Portainer Mode

A Portainer Edge Agent can be automatically configured, started and connected to an instance of the Portainer server during the coupling process.

Before you can begin integration, you need the following information:

1. URL of the Docker registry
2. Port (http or https) for accessing the API

For more information, see **https://docs.portainer.io/**.

Configuration File

If Portainer mode is to be supported, the corresponding portainer installation must be configured on the WDS server.

Add the following configuration option to the custom settings file, or set it as described above:

```
"Portainer": {
    "API": "",
    "User": "admin",
    "Password": "",
    "PortainerAppProxy": "",
    "PortainerTunnelProxy": "",
    "InsecureAgentPoll": ,
    "PullPublicEdgeAgent":
}
```

Table 5: Configuration File

Settings	Description	Example
API	URL of the Portainer API; this must contain the relative path **/api**.	**https://my-portainer:9443/api**
InsecureAgentPoll	Flag indicating whether the Portainer Edge Agent should use the EDGE_INSECURE_POLL option. This allows the use of self-signed certificates.	true or false
PortainerAppProxy	Portainer URL as "seen" from the device. This URL may differ from the API if the installation uses a reverse proxy or other form of deployment.	**https://my-portainer:9443**
PortainerTunnelProxy	API Portainer Web socket URL as seen from the device. The protocol (*http/https*) may or may not be required, depending on the application scenario.	-
PullPublicEdgeAgent	Flag indicating whether the Portainer Edge Agent should be obtained from the Docker Hub instead of the container registry specified in the configuration.	true or false

Example of a **customPortainer.json** file:

```
{
    "ContainerRegistry": {
        "Location": "wdsserver:5000",
        "Repository": "wds-agents",
        "ConfigureInsecureRegistry": true
    },
    "Portainer": {
        "API" : "http://pc-sg-cdr-1:9000/api",
        "User": "admin",
        "Password": "wagowagowago",
        "PortainerAppProxy" : "http://pc-sg-cdr-1:9000",
        "PortainerTunnelProxy": "http://pc-sg-cdr-1:8000",
        "InsecureAgentPoll": true,
        "PullPublicEdgeAgent": true
    }
}
```

5.4.4 Security Configuration

The following WAGO Device Sphere software components can communicate with one another securely, i.e., through encrypted communication, when configured accordingly:

- WAGO Device Sphere UI
- WAGO Device Sphere Server
- WAGO Device Sphere Authorization
- WAGO Device Sphere PostgreSQL (database)
- WAGO Device Sphere Mongo (database)

This requires corresponding certificate files and correct configuration of the individual components. The installation process can optionally generate the initial setup for encrypted communication and the appropriate certificates. These certificates are considered "temporary" and serve to illustrate functional certificate-based encryption.

The following certificates are generated during the installation process:

Table 6: Certificates Generated during the Installation Process

Certificate	Filename	Description
1	**ca.crt**	The root CA certificate is used both as an issuer for the server's TLS certificate and for signing the device certificates during the enrollment process.
2	**ca.pfx**	A file in "PKCS#12" format that combines the root certificate and private key. This file is protected with a password that is entered during setup.
3	**device_sphere_server.crt**	TLS server certificate
4	**device_sphere_server.key**	Private key of a server. This key is required for secure TLS connections.
5	**server.pfx**	A file in "PKCS#12" format that contains the server certificate and the private key. This file is protected with a password that is entered during setup.
6	**signing.pfx**	This file is used by the OAuth server to sign tokens. This file is protected with a password that is entered during setup.
7	**encryption.pfx**	This file is used by the OAuth server to store data in encrypted form. This file is protected with a password that is entered during setup.
8	**postgres_db.crt**	TLS/SSL certificate
9	**postgres_db.key**	Private key of a server. This key is required for secure TLS connections.

The files are stored in the **C:\ProgramData\WAGO Software\WAGO Device Sphere\Certificates** folder and used in the corresponding component configurations. The root CA certificate is automatically imported into Windows "Computer Certificates" as a "trusted certificate." This is necessary so that the server certificates that have been generated will be accepted in the components and the various browsers.

As soon as the WAGO Device Sphere software is put into productive use, public certificates provided by your company's IT department should be used. In this productive environment, the above-mentioned certificates are required and must be present on the server. Ensure that only trusted certificates are used in productive operation! For security reasons, the certificate generated during the installation process should be removed at the end.

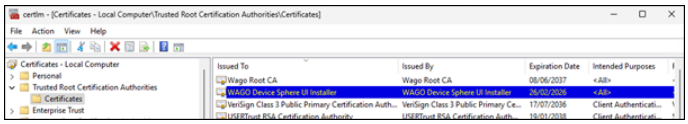


Figure 10: Trusted "Root CA" Certificates in Certificate Manager

5.4.4.1 Using Your Own Certificates

The installer for the WAGO Device Sphere software lets you generate self-signed certificates for initial commissioning. For security reasons, these certificates must be replaced by officially signed certificates before the software is used productively. These certificates must come from a trusted certification authority.

At least two officially signed certificates are required:

1. A server certificate
2. A certificate from the certification authority (CA certificate, root certificate)

Server Certificate

The same server certificate can be used for all servers, or, alternatively, a separate certificate can be used for each server.

Certification Authority Certificate

The Certification Authority certificate (Root CA) should have the following settings:

- `Basic constraints (critical): Type = Certification Authority`
- `"Subject Key Identifier" extension and "Authority Key Identifier" extension: active`
- `Private key: RSA 2048 bit`

The server certificate should have the following settings:

- `Basic constraints: Type = End Entity (CA = false)`
- `Common name: "wdsserver"`
- `Key usage: Digital Signature, Non Repudiation, Key Encipherment, Key Agreement`
- `Extended key usage: TLS Web Server Authentication, TLS Web Client Authentication`
- `Subject alternative name: DNS:wdsserver, DNS:localhost, DNS:[hostname]`

Both certificates are required in the following file formats:

Table 7: File Formats

File Format	Description	CA Certificate (Example)	Server Certificate (Example)
crt	Text with header in PEM format	wdsca.crt	wdsserver.crt
key	Unencrypted private key in PEM format	wdsca.key	wdsserver.key
pfx	Certificate chain and private key as encrypted file in PKCS12 format	wdsca.pfx	wdsserver.pfx

Two options exist for configuring a productive environment:

1. Storing the official certificate files in the certificate folder under the existing names; this does not require any changes to the server configurations.

2. Leaving the official certificate files under the existing names and changing the file paths in the server configurations
   To do this, you must modify the following configuration files:

Table 8: Configuration Files to Modify

Configuration File (in C:\ProgramData\WAGO Software\WAGO Device Sphere)	Section	Setting/Parameter
\WDS\Config\customSecurity.json	CACertificate	Password
		Path
	Endpoints	Password
		Path
\WDSAuth\Config\customSecurity.json	Endpoints	Password
		Path
\WDSAuth\Config\customTokenSecurity.json	Endpoints	TokenEncryptionPassword
		TokenEncryptionPfxPath
		TokenSigningPassword
		TokenSigningPath
\WDSAuth\Config\customDatabase.json	Datatbase	ConnectionString
\WDSUI\Config\customDatabase.json	DatabaseConnectionSettings	Password
		SslCaFile
		SslCertFile
		SslKeyFile
\WDSUI\Config\customSecurity.json	Certificate	Password
		Path
postgres\data\pg_ident.conf	DatabaseConnectionSettings	SYSTEM-USERNAME
postgres\data\postgresql.conf.conf	SSL	SSL_CA_FILE
		SSL_CERT_FILE
		SSL_Key_File
postgres\data\pg_hba.conf (only necessary if you need to change the access type)		Type
		Database
		Address
		Method

Every time a change is made, the corresponding service must be restarted. To do this, open the “Services” program and restart it.

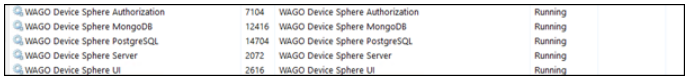


Figure 11: “Services” Program

Trusting a CA Certificate

Each user must perform the following steps individually!

1. Click **[Windows]**.
2. Enter **Manage Computer Certificates** in the input field.
3. Open **Trusted Root Certification Authorities**.
4. Right-click **Certificates** and select **All Tasks** > **Import**.
   ⇨ The “Certificate Import Wizard” opens.

5. Work through all the steps in the wizard.

   ⇨ The certificate is uploaded.

6. Close Explorer.
7. Click **[Windows]** again.
8. Enter **Services** in the input field.
9. Select all specific services of the WAGO Device Sphere software.
10. Right-click on your selection and select **Restart**.

    ⇨ All the services are restarted.

Note **Reconnect devices to the software!**

If communication between the software and connected devices had already been established, it is interrupted when the services are restarted.

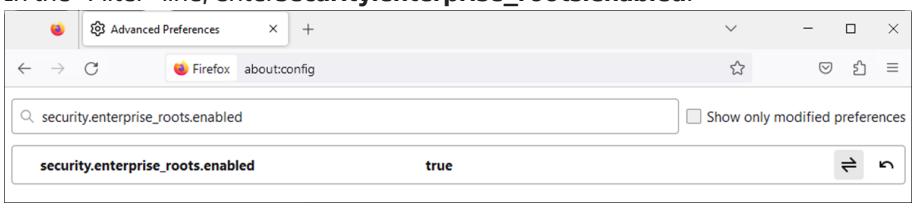
Therefore, you must reconnect the devices to the software. To do this, first disable the Commissioning Service and then re-enable it. For more information, see section **Disabling Commissioning Service and Resetting Coupling State [▸ 62]**.

Information on Secure Browser Access to the WAGO Device Sphere Software

The *Edge* and *Chrome* browsers use Windows Certificate Manager to verify a certificate without any further settings. In the *Firefox* browser, access to Windows Certificate Manager must be explicitly enabled. Every time a new certificate is installed, the *Firefox* browser must be restarted so a new "root CA" can be recognized.

Firefox configuration steps:

1. Enter **about:config** in the address bar.
2. A message appears describing possible risks; click the button to accept.
3. In the "Filter" line, enter**security.enterprise_roots.enabled**.



4. Set the parameter to **true**.
5. Restart the browser.

5.5 Device Configuration

5.5.1 Web-Based Management

The following section explains how to configure an existing device via Web-Based Management before commissioning.

5.5.1.1 "Commissioning Service" Setting

The Web-Based Management provides a "Commissioning Service" setting. This setting ensures that the corresponding device can establish an initial connection to the WAGO Device Sphere software's server.

By default, this setting is enabled in the Web-Based Management. Therefore, the corresponding device is actively available for coupling during commissioning (see **Coupling a Device [▸ 60]**).

For more information on the "Commissioning Service," see **Checking the "Commissioning Service" in the Web-Based Management [▸ 61]**.

5.5.1.2 "Domain Name Server" Setting

The Domain Name Server can be configured in the Web-Based Management. Optionally, a static host entry can be stored for the server. This host entry is required if your own IT department has not provided a DNS entry in a central DNS system.

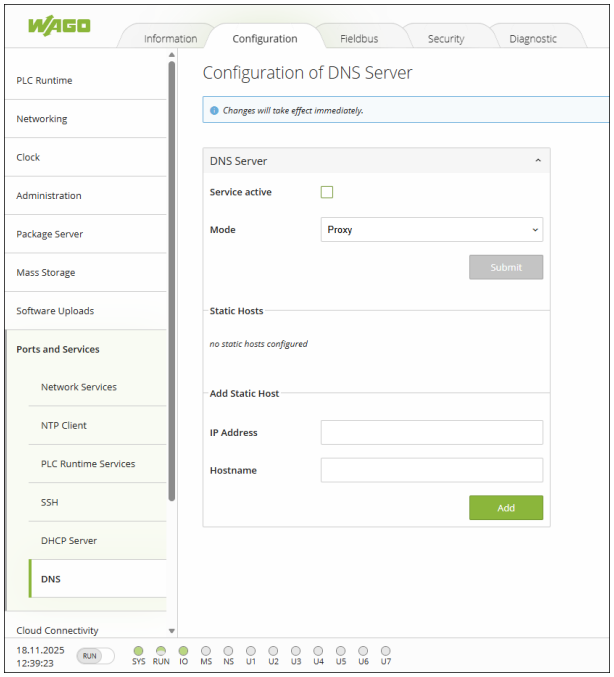


Figure 12: "Domain Name Server" Setting

The following values can be assigned:

Enter the following values in the "Add Static Host" area (example):

Table 9: "Add Static Host" Area

Setting	Description
IP Address	IP address of the server **Example:** 3.3.3.3
Hostname	Hostname under which the server should be reachable **Example:** wdsserver

The host **wdsserver** is then listed in the list of static hosts.

Notes:

- Using static host entries does not require the DNS server to be enabled.
- The **wdsserver** entry allows name resolution even if a central DNS server is not available.

To check whether the DNS server configuration is correct, the following command can be used on the device:

curl -kv https://wdsserver/api/v1

If the server is accessible, it responds with the following analysis outputs:

- IP address
- Server certificate
- *String*, staring with
  `{"name":"wds", …`

5.5.1.3 "Network Time Protocol" Setting

The system time can be configured in the Web-Based Management. A correct system time is crucial for a functioning SSL communication, since certificates are only accepted within their validity period. If the system time is outside this period, SSL communication is refused. To ensure that the time is correct, you can configure an "NTP server" or set the time manually.

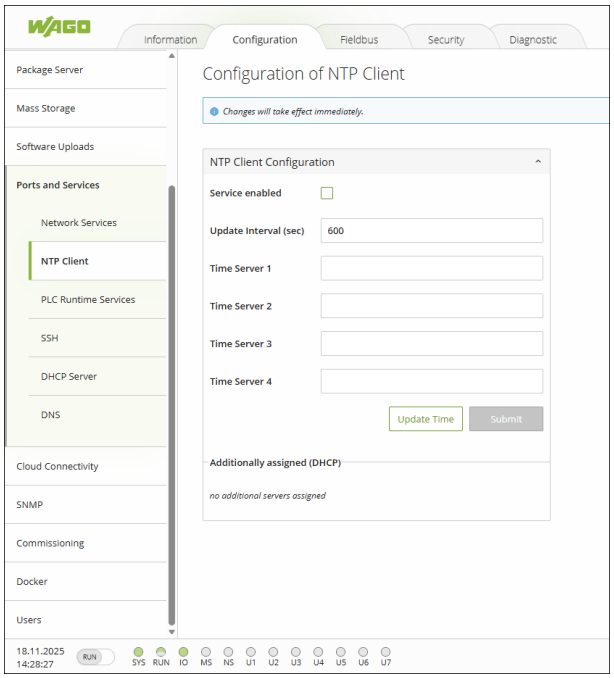


Figure 13: "Network Time Protocol" Setting

Table 10: "NTP Client Configuration" Group

Setting	Description
Service enabled	Activates the NTP service. If the service is enabled, the system automatically synchronizes the local time with the specified NTP servers.
Update Interval (sec)	Update interval (in seconds) at which the time is synchronized with the NTP servers. **Example:** 600 seconds: synchronization every 10 minutes
Time Server 1 … 4	Here you can enter up to four time servers. Entering at least two servers is recommended to ensure redundancy. **Example:** **Time Server 1:** 136.243.177.133 **Time Server 2:** 5.4.3.2
[Update Time]	Synchronizes the time with the first accessible NTP server.
[Submit]	Saves the modified configuration.
Additionally assigned (DHCP)	
Time Server 1 … 4	If the IP address for time synchronization is already provided via DHCP, it is shown here. **Example:** **Time Server 1:** 192.168.3.1 These entries serve as additional sources for the time setting.

Manual Time Setting

If no connection to an NTP server is possible, the system time can be set manually.

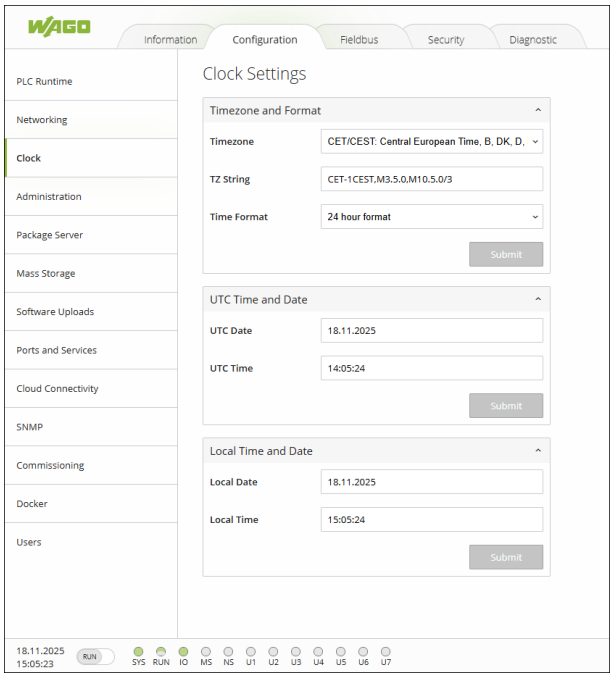


Figure 14: "Clock" setting

Notes:

- If SSL connections fail, verify that the NTP service is active and that the time has been correctly synchronized.
- In closed networks, an internal NTP server provided by your own IT department should be used.

5.5.2 Configuration on the Device

The configuration file **/etc/wds/wds.cfg** is used to configure the Commissioning Agent on a device. The file contains various options that control the behavior of the agent, particularly with regard to server discovery, communication and security parameters. The file can be configured either directly on the device or via an SD card.

General Configuration Options

The commissioning agent attempts to find the WDS server, proceeding in the following order:

1. **servers**: list of specific server addresses
2. **localServers**: list of local server addresses (if no servers are set via the SD card)
3. **Subnet scan**: if **subnet_scan=true** and no servers are set via the SD card
4. **globalServers**: list of global server addresses (if no servers are set via the SD card)

The first server found is used; the search process is then terminated.

Table 11: dw

Option	Description
servers	A comma-separated list of specific server addresses (IP address or hostname)
localServers	A comma-separated list of local server addresses
Subnet Scan	Specifies whether the commissioning agent should scan the subnet for WDS servers

Option	Description
globalServers	A comma-separated list of global server addresses
default_scheme	Specifies the scheme used for the scan if it is not specified in the server address (*http* or *https)* The encrypted variant "https" is the default setting and should not be changed.
polling_rate	Polling rate used by all agents (in seconds)
default_port	Default port; the commissioning agent attempts to contact the addresses in the subnet on this port during the scan. If none is specified, the default port for the scheme is used (**example:** 80 for *http*).
timeout	After a registration request is sent, the commissioning agent waits the specified amount of time (in minutes) for the server to accept the request. A timeout of "0" disables the waiting time.
mode	Specifies the mode that the commissioning agent uses to communicate with the server**Example** **secure:** The commissioning agent only connects to servers that have a valid and trusted certificate. **insecure:** The commissioning agent also accepts self-signed certificates.
tls_cert	This option expects a path to a certificate file. **Relative path:** If a relative path is specified (e.g., **certs/device.crt**), this path automatically references the directory of the SD card, typically **/media/sd/**. **Example: tls_cert = certs/device.crt,** actual storage location: **/media/sd/certs/device.** **crtAbsolute path:** If an absolute path is specified (e.g., **/etc/ssl/device.crt**), the path is applied unchanged and used directly.

Do not store the certificate in the **/etc/wds/** directory, since the contents of this folder are deleted and reset to the default state when the Commissioning Service is disabled. WAGO recommends storing certificates on an SD card or in a separate, persistent directory outside of **/etc/wds**. If the mode is set to "secure," the Commissioning Agent uses this certificate to verify the server. If no certificate is specified, the "Mozilla Trusted CA" list is used.

5.5.3 Configuration via SD Card

By default, the configuration file **/etc/wds/wds.cfg** can be overwritten by a file on an external SD card. The corresponding file should only specify parameters that you want to override.

1. Insert an SD card into the corresponding slot on your PC.
2. Create a file **wds.cfg** in the root directory of the SD card with the custom settings you want.
3. Safely remove the SD card from your PC.
4. Insert the SD card into the slot of your device.
5. Start the device.
6. Carry out commissioning.
7. Remove the SD card.
8. Repeat the steps for all other devices.

6 Starting

The software is a Web-based solution with a server; it does not have to be started as a Windows program. The services start in the background. The services themselves can be accessed by any available browser on any PC.

6.1 Services

The WAGO Device Sphere software consists of five services that are set up during installation (see **Installation [▸ 17]**). The services start automatically as soon as Windows boots up:

- WAGO Device Sphere Authorization
- WAGO Device Sphere PostgreSQL (database)
- WAGO Device Sphere MongoDB (database)
- WAGO Device Sphere Server
- WAGO Device Sphere UI

6.2 Browser

1. Open a browser on your PC.
2. In the address bar, enter the server name and port number used, e.g., *https://wdsserver:33000/*.

   ⇨ The server is accessed.

6.3 Log Files

The log files for all of the services can be found under the following path: *C:\ProgramData\WAGO Software\WAGO Device Sphere\Logs*

Logging

The WAGO Device Sphere software stores log files for various internal components to trace the processes within the software.

Access

The server administrator can access the log files, since access to the file system also automatically provides access to the log files.

Creation

A new log file is created daily for each component. This operation can be set to "Day" via the **rollingInterval** parameter. If the maximum file size is exceeded (*fileSizeLimitBytes: 20971520 bytes ≈ 20 MB*), an additional file with an extension, e.g. "_001", is created for the same day.

- **Specify Maximum Number of Files**
  In the appsettings.json files (WDS, UI, Auth), you can configure the maximum number of files that can be created. When the maximum number of files is reached, the software always overwrites the oldest file with a new one.
  By default, 90 files are preset for each component.

Entry in the file: `retainedFileCountLimit: 90`

- **Specify Maximum File Size**
  In the appsettings.json files (WDS, UI, Auth), you can configure the maximum file size allowed for a file.
  By default, the file size is set to 20 MB per file.
  Entry in the file: `fileSizeLimitBytes: 20971520`

Log Level

By default, only entries from the "Info" level are logged. This can be modified in the corresponding configuration files under *"MinimumLevel" -> "Default"*

Paths

C:\Program Files\WAGO Software\WAGO Device Sphere\WDS\Config\appsettings.json

C:\Program Files\WAGO Software\WAGO Device Sphere\WDSAuth\Config\appsettings.json

C:\Program Files\WAGO Software\WAGO Device Sphere\WDSUI\Config\appsettings.json

Call

Device logs can also be retrieved via the WAGO Device Sphere software. You can find more information in **Opening Log Files from the Device [▸ 63]**.

7 Graphical User Interface

7.1 Main Sections

Note

The figures and descriptions below are an example configuration

The figures and descriptions given in the „Graphical User Interface“ section are based on a sample configuration.

Your configuration and the contents displayed can differ from that shown here.

The graphical user interface can be divided into four main sections, some of which display different content depending on the options selected. The graphical user interface has the following structure:

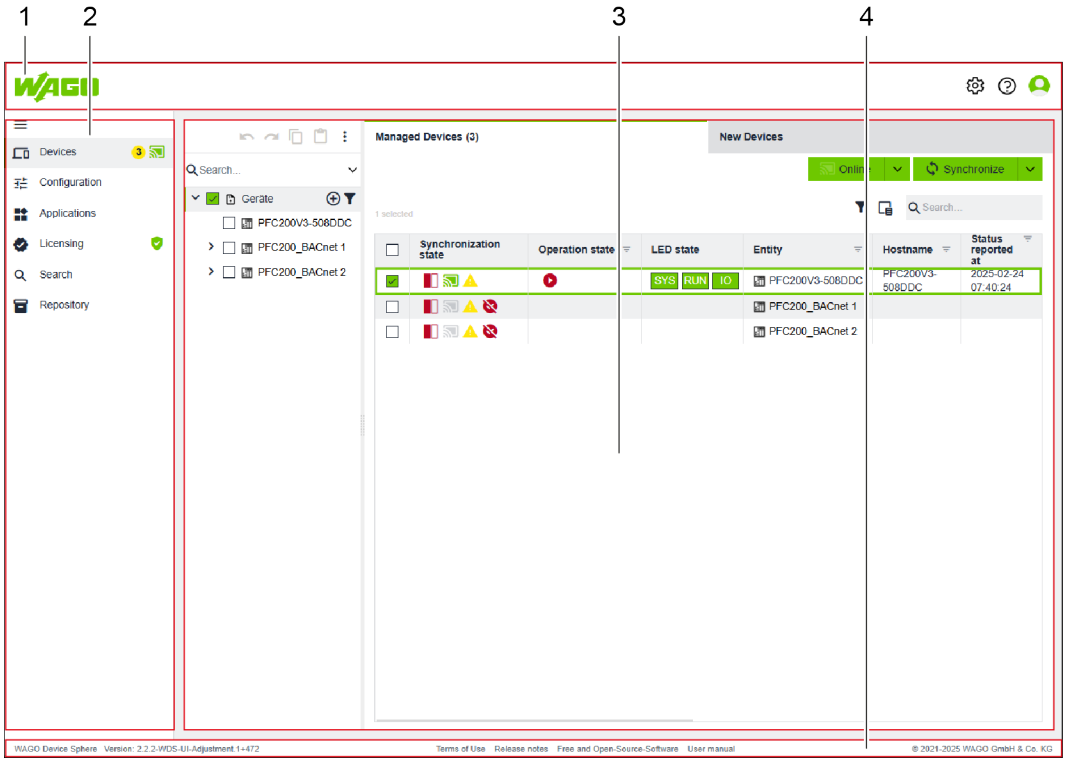


Figure 15: Basic Structure of the Graphical User Interface of the WAGO Device Sphere Software – Main Sections

Table 12: Legend for Figure “Basic Structure of the Graphical User Interface of the WAGO Device Sphere Software – Main Sections”

Position	Designation	Description
1	**Header Bar**	Shows information and interaction options for the user who is logged in and individual shortcuts. You can find further information in Header Bar [▸ 35].
2	**Side Menu**	For navigation through the individual menu items. You can find further information in Side Menu [▸ 38].

Position	Designation	Description
3	**Workspace**	Shows the workspace. The content and representation of the workspace depend on the selection in the side menu. You can find further information in **Workspace [▸ 38]**.
4	**Footer Bar**	Shows general information and version notes. You can find further information in **Footer Bar [▸ 40]**.

7.1.1 Header Bar

The header bar contains information and interaction options for the user who is logged in, as well as shortcuts to the product manual, the online help and the Start screen. The contents of the footer bar are independent of the selection in the side menu and action area.

The header bar has the following structure:

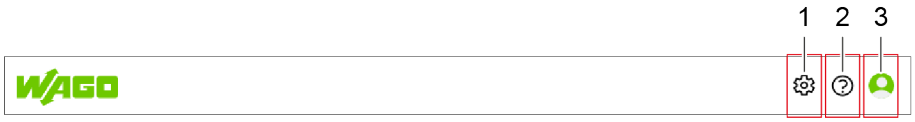


Figure 16: Header Bar

Table 13: Legend for Figure "Header Bar"

Position	Designation	Description	
1	**"Settings" Menu**	⚙	Opens the settings dialog for the Software. You can find further information in **"Settings" Menu [▸ 35]**.
2	**Help/F1**	?	Opens the context-sensitive Help function for the contents shown in the action area. **Note: Context-sensitive Help may differ!** Depending on the connection status (online vs. offline), different versions of the Help may be displayed. If there is an Internet connection, WAGO Solution Builder retrieves the latest available help from an external server. If there is no Internet connection, WAGO Solution Builder retrieves the embedded Help.
3	**User**	👤	Opens the context menu for the user settings.

7.1.1.1 "Settings" Menu

Note

Settings are saved locally in the Web browser in the form of cookies

All settings are saved in the form of cookies in the Web browser used, with the exception of "System Settings," which are saved globally. If the cookies are deleted, these settings are lost.

The **Settings** menu is divided into three areas:

- **"Regional Settings" Area [▸ 36]**
- **"Authentication Settings" Area [▸ 36]**
- **"System Settings" Area [▸ 37]**

7.1.1.1.1 "Regional Settings" Area

In the "Regional Settings" area, you can set the language for the graphical user interface of the Software. You can also customize the date and time format.

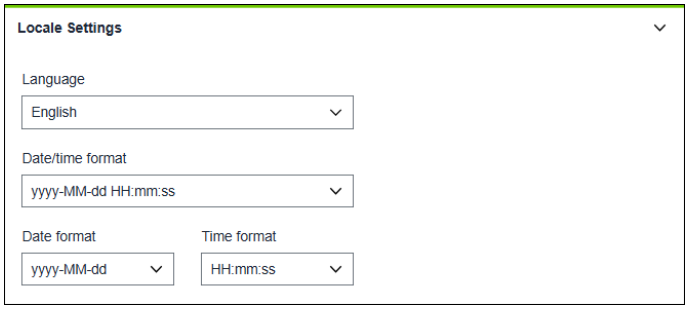


Figure 17: Side Menu > Settings > "Regional Settings" Area

7.1.1.1.2 "Authentication Settings" Area

In the "Authentication Settings" area, you can make login settings and manage WAGO Device Sphere users.

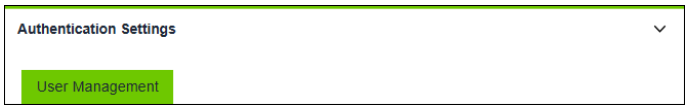


Figure 18: Side Menu > Settings > "Authentication Settings" Area

Table 14: Legend for Figure "Side Menu > Settings > 'Authentication Settings' Area"

Designation	Description
[User Management]	Opens the **"User Management" Dialog [▸ 36]**.

7.1.1.1.2.1 "User Management" Dialog

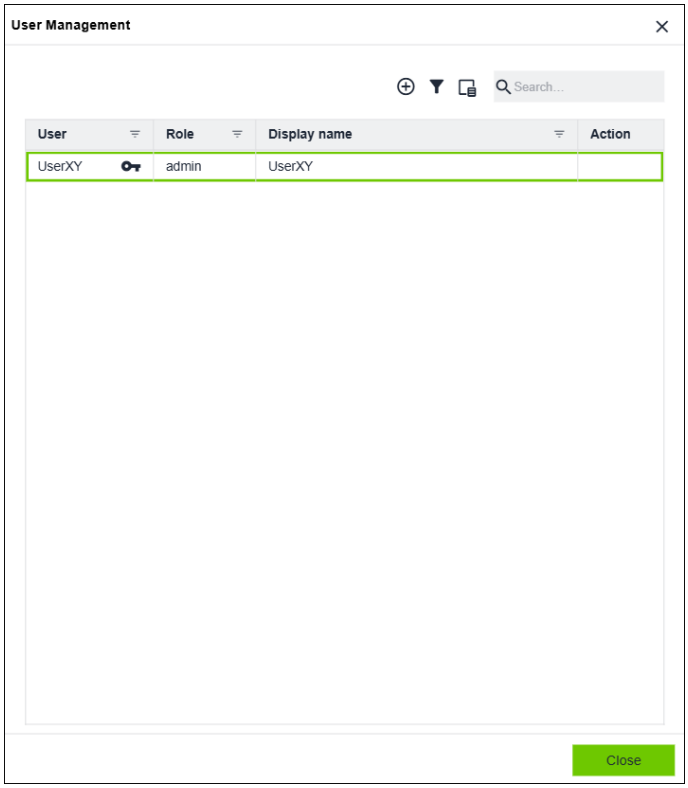


Figure 19: Side Menu > Settings > "Authentication Settings" Area > "User Management" Dialog

Table 15: Legend for Figure “Side Menu > Settings > ‘Authentication Settings’ Area > ‘User Management’ Dialog”

Designation	Description
⊕	Opens the “Add User” Dialog [▸ 37] to create a new user.
User	Shows the user that has been created.
Role	Shows the assigned role.
Display Name	Shows the display name that has been created.
Action	Deletes the user that was created.

7.1.1.1.2.1.1 “Add User” Dialog

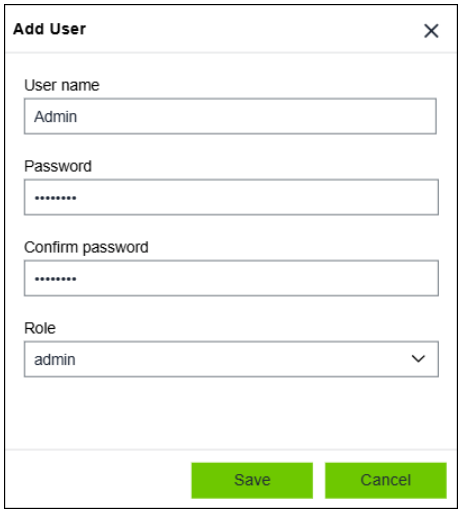


Figure 20: Side Menu > Settings > “Authentication Settings” Area > “User Management” Dialog > “Add User” Dialog

Table 16: Legend for Figure “Side Menu > Settings > ‘Authentication Settings’ Area > ‘User Management’ Dialog > ‘Add User’ Dialog”

Designation	Description	
Username	Enter the username here	
Password	Enter the password here	
Confirm password	Reenter the password here	
Role	Select the role:	
	viewer	Default user who can open and edit projects.
	editor	Identical to the “viewer” role; can also create new projects and manage the repository.
	admin	Identical to the “editor” role; can also make system settings, such as managing users.

7.1.1.1.3 “System Settings” Area

In the “System Settings” area, you can set the addresses for the WAGO Device Sphere software.

The addresses in the “System Settings” area are requested and set during installation. If no changes have been made to the system, you do not have to provide any entries here.

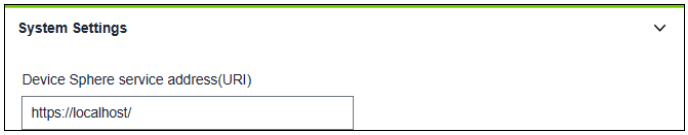


Figure 21: Side Menu > Settings > “System Settings” Area

Table 17: Legend for Figure “Side Menu > Settings > ‘System Settings’ Area

Designation	Description
Device Sphere service address	Address of the WAGO Device Sphere Server.

7.1.2 Side Menu

The side menu is used for navigating through the individual menu items. In addition, it shows various messages that can arise depending on the state.

The side menu has the following structure:

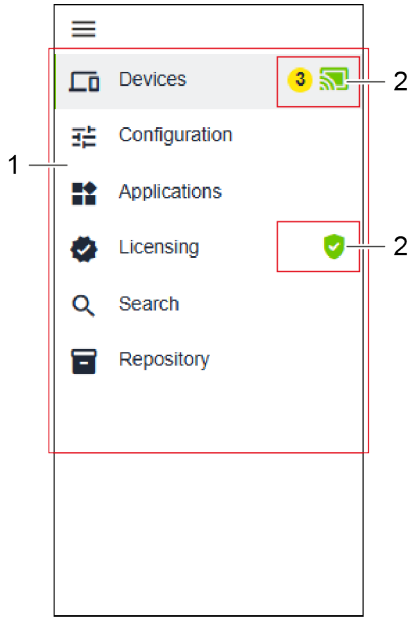


Figure 22: Side Menu

Table 18: Legend for Figure “Side Menu Open”

Position	Designation	Description
1	**Menu Items**	Shows all selectable menu items. Depending on the menu item selected, a specific workspace appears. You can find further information in **Workspace [▸ 38]**.
2	**New Messages**	Shows incoming messages. The corresponding tooltip appears when the mouse hovers over the message. Clicking on it navigates to the corresponding location in the graphical user interface.

7.1.3 Workspace

The content and representation of the workspace depend on the menu item selected in the side menu.

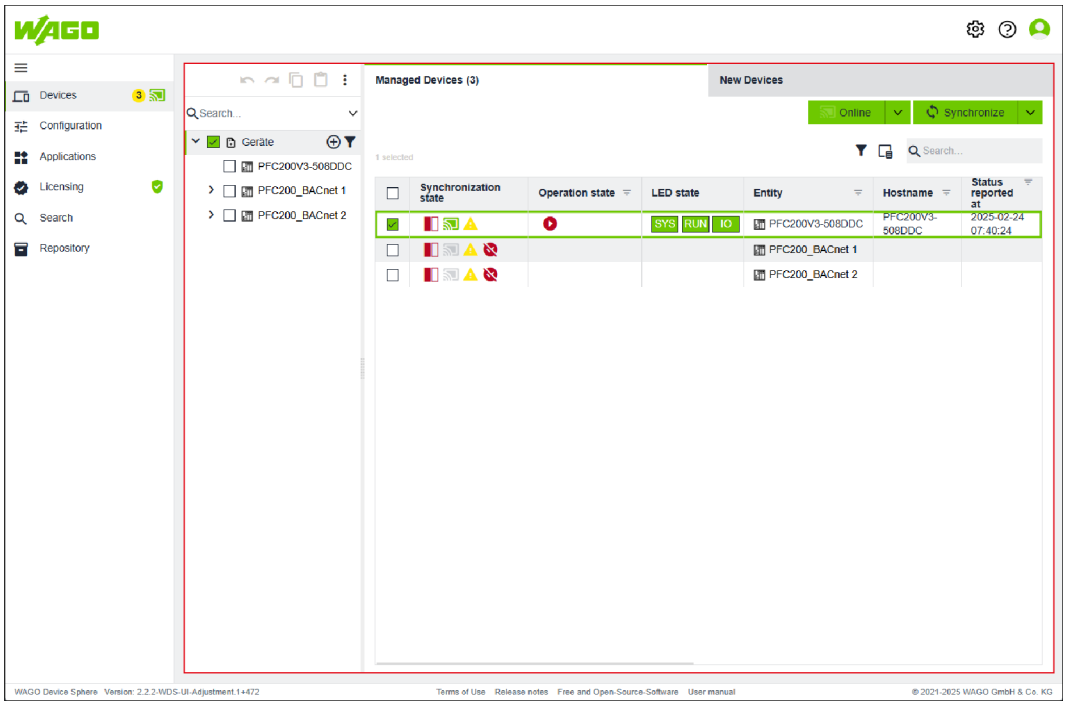


Figure 23: Workspace

The workspace is described individually for each menu item in **Side Menu [▸ 42]**.

7.1.3.1 Entity Tree – Entities with Icons

The following side menu items have a structure tree in the workspace for selecting the entity.

- **"Devices" Menu Item [▸ 42]**
- **"Configuration" Menu Item [▸ 46]**
- **"Applications" Menu Item [▸ 53]**
- **"Search" Menu Item [▸ 57]**

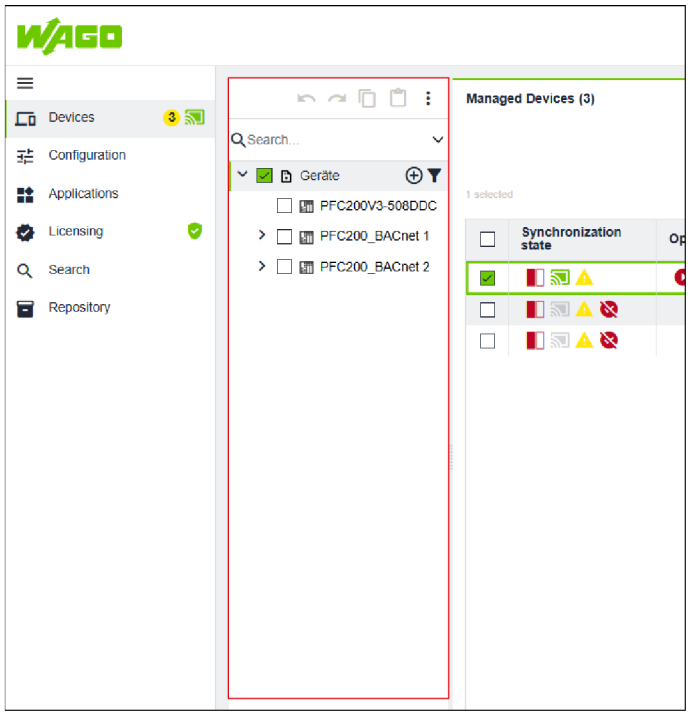


Figure 24: Workspace > Entity Tree

Some possible entities with their associated icons are listed below.

Table 19: Entity Tree – Entities with Icons

Icon	Entity
	Controller
	Third-party controller
	Other device

7.1.4 Footer Bar

The footer bar contains general information about the Software. The contents of the footer bar are independent of the selection in the side menu and action area.

The footer bar has the following structure:

Figure 25: Footer Bar

Table 20: Legend for Figure "Footer Bar"

Position	Designation	Description
1	**Software version**	Shows the Software version currently in use.
2	**Links**	Shows links to additional information.
3	**Publisher**	Shows the publisher of the Software, along with the year of publication.

7.2 General Operating Elements and Icons

The general icons listed below may appear in the graphical user interface.

Besides the descriptions in this product manual, nearly every one of the icons listed here offers a tooltip with a brief description right in the user interface.

Table 21: General Operating Elements and Icons in the Graphical User Interface

Icon	Designation	Description
	"Settings" Menu	Opens the settings dialog for the Software.
	Help/F1	Opens the context-sensitive Help function for the contents shown in the action area.
	User	Opens the context menu for the user settings.
	Function-specific context menu (three-point menu)	Opens a function-specific context menu. Additional settings can be selected from the context menu. The WAGO Device Sphere software provides the context menu for various functions at different points in the graphical user interface.
	Add item	Creates a new item.

7.2.1 Date and Time Input Dialog

The following dialog is used to enter the date and time. The dialog appears in several places within the software. If multiple devices can be selected for the respective operation planning, the selected time applies to all selected devices.

If the selected time is in the past, the respective operation is executed immediately. If the selected time is in the future, the task is executed at that time in the future.

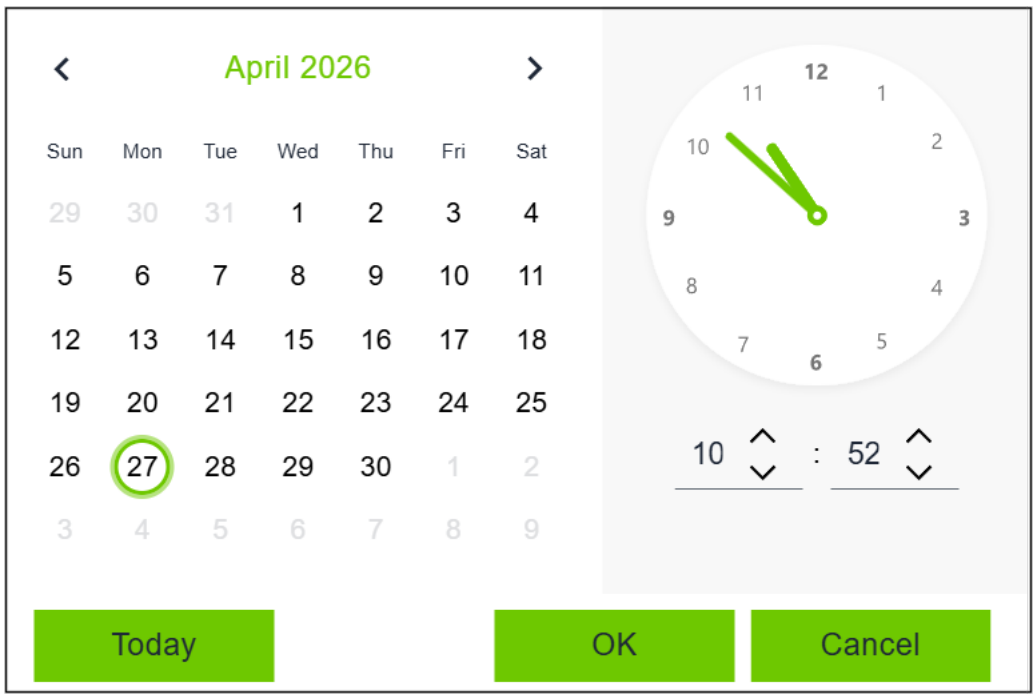


Figure 26: Date and Time Entry Dialog

You can find more information in:

- Backup & Restore Tab [▸ 52]
- "Synchronize Differences" Dialog [▸ 44]

7.3 Start View

The Start view appears immediately after the Software is launched and serves as a starting point for all other activities.

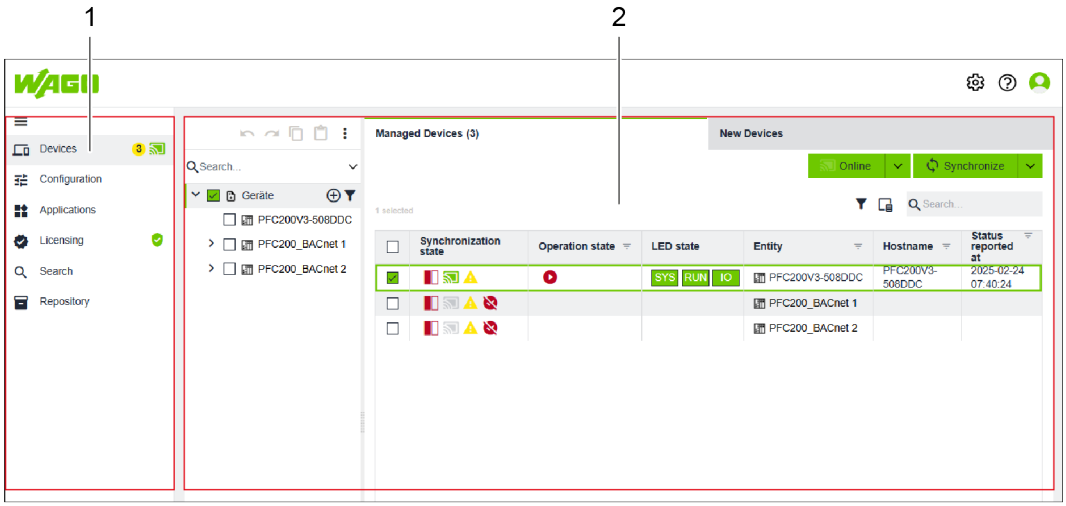


Figure 27: Structure of the User Interface in the "Start View" Area

Position	Designation	Description
1	**Side Menu**	For more information, see Side Menu [▸ 38].
2	**Workspace**	For more information, see Workspace [▸ 38].

7.4 Side Menu

Information about the structure and the icon legend for the side menu can be found under Side Menu [▸ 38].

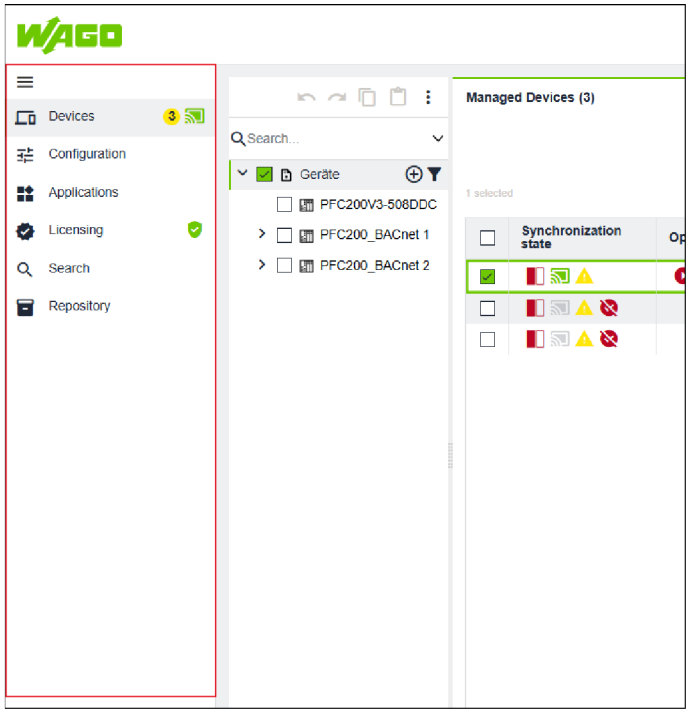


Figure 28: Side Menu

The contents of the side menu and its submenus are described in detail below.

7.4.1 "Devices" Menu Item

This menu item contains the following tabs:

- **“Managed Devices” Tab** (see “Managed Devices” Tab [▸ 43])
  This tab contains all controllers that are logged in and integrated. The other menu items can be used to configure and manage the listed controllers.
- **“New Devices” Tab** (see “New Devices” Tab [▸ 46])
  This tab contains all the controllers that are logged in but not yet integrated. The listed controllers can be preconfigured and added to the “Managed Devices” tab via the context menu.

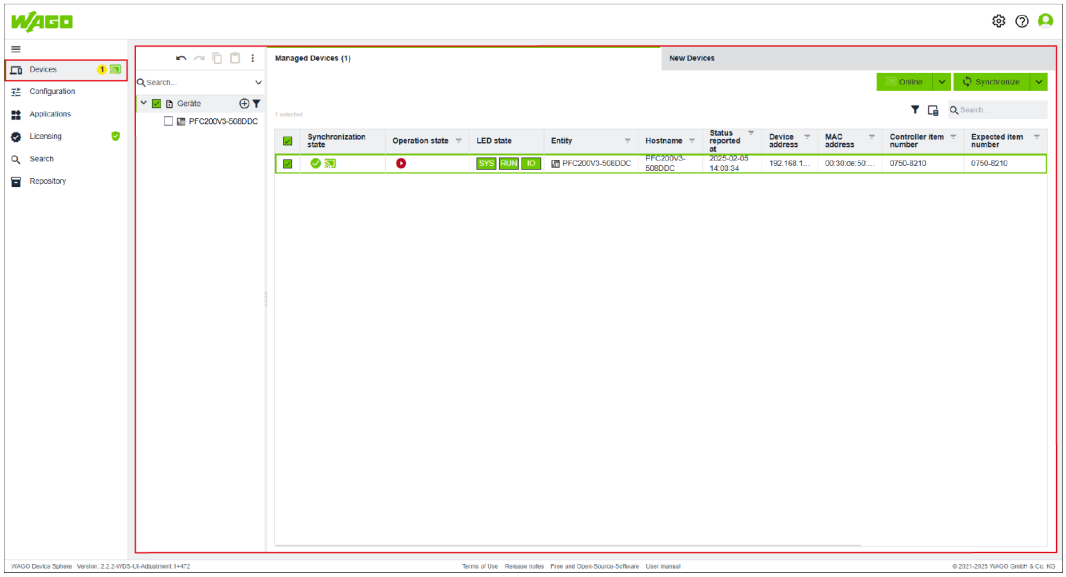


Figure 29: Side Menu > “Devices” Menu Item

7.4.1.1 “Managed Devices” Tab

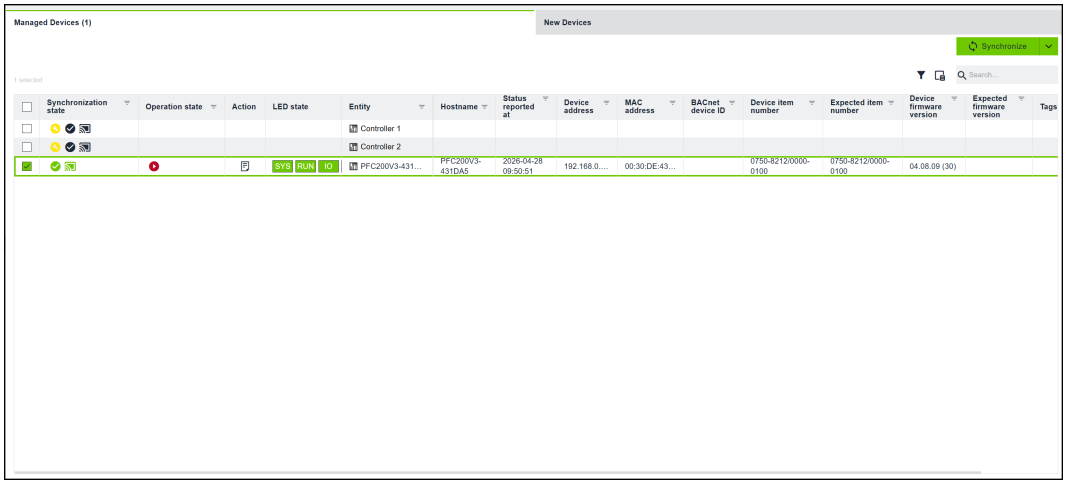


Figure 30: Side Menu > “Devices” Menu Item > “Managed Devices” Tab

Designation	Description
[Online]/ [Offline]	Switches between the “Online“ and “Offline“ mode. The “Online“ mode activates a monitoring job that regularly queries the current status of all the solution’s controllers. These include the “RUN status“ or the current firmware version, for example. The “Offline“ mode is also required in order to start a synchronization job and perform a manual firmware update, as well as for the Backup-and-Restore operation.

Designation		Description
[Sync]	**Merge Manually**	Opens the "Synchronize differences" dialog for performing a manually merged synchronization procedure. For more information, see **"Synchronize Differences" Dialog [▸ 44]**.
	Synchronize All	Synchronizes the modified and non-modified (i.e., all) configuration components for the selected controller.
	Overwrite and Synchronize	Synchronizes only the modified configuration components for the selected controller.
Action		Opens the activity log of the selected controller. For more information, see **"Device Log Messages" Dialog [▸ 45]**.

7.4.1.1.1 "Synchronize Differences" Dialog

In the "Synchronize differences" dialog, you can review in detail which configuration components require synchronization and the direction of the synchronization and specify these before the synchronization operation starts.

When selecting the direction of synchronization, you can transfer an updated application transferred to the controller, for example; in contrast, the current application parameters should be taken from the controller, since changes were made on the controller during operation.

You can also manually mark individual configuration components for synchronization. The checkboxes "Project changes", "Controller changes", and "Synchronized" must be selected. After setting the parameters, you can start the synchronization procedure by clicking the corresponding button.

Figure 31: Side Menu > "Devices" Menu Item > "Managed Devices" Tab > Synchronize > Merge Manually... > "Synchronize Differences" Dialog Graphic

Designation	Description	
Project changes	☐	Does not show entries with the "Project changed" status.
	☑	Displays entries with the "Project changed" status.
Controller changes	☐	Does not display entries with the "Controller changed" status.
	☑	Displays entries with the "Controller changed" status.
Synced	☐	Does not display entries with the "Synchronized" status.
	☑	Displays entries with the "Synchronized" status.
Device	Displays the name of the controller.	
IP address	Displays the controller IP address.	

Designation	Description
Element	Displays the synchronized range.
Status	Displays the synchronization status of the device.
Project version	Displays the timestamp of the project version.
Direction	Indicates the direction for synchronization.
Device version	Displays the configuration's timestamp in the controller.
Synchronized on	Displays the timestamp of the last synchronization between the software and controller. The synchronization relates to the current configuration.
Planned start at	Displays the date and time of the next scheduled synchronization. For more information, see **Date and Time Input Dialog [▸ 41]**.
Reset (cold)	Performs a full resynchronization of the device.

7.4.1.1.1 "Merge 'Device Settings' Configuration Values" Dialog

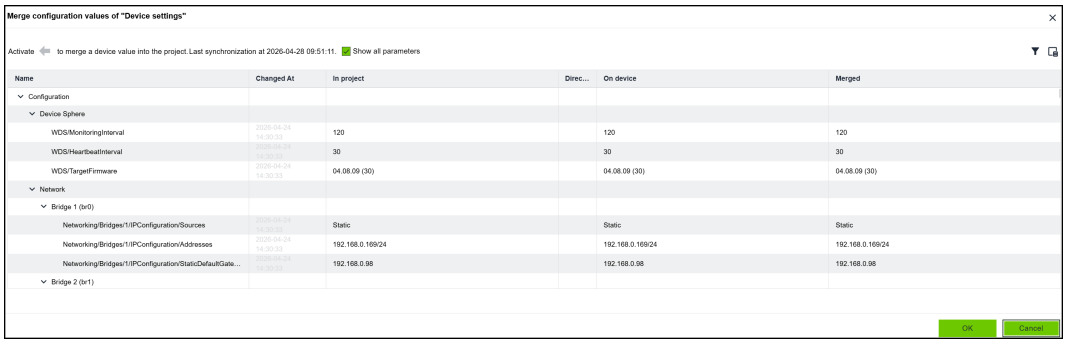


Figure 32: Side Menu > "Devices" Menu Item > "Managed Devices" Tab > Synchronize > Merge Manually > "Merge 'Device Settings' Configuration Values" Dialog

Designation	Description
Name	Displays the device settings.
Changed on	Displays the time stamp for the last change of the setting.
In the project	Displays the setting value in the project.
Direction	Displays the selection option and direction for synchronization.
On the device	Displays the setting value in the controller.
Compiled	Displays the result value after synchronization between the controller and the project.

7.4.1.1.2 "Device Log Messages" Dialog

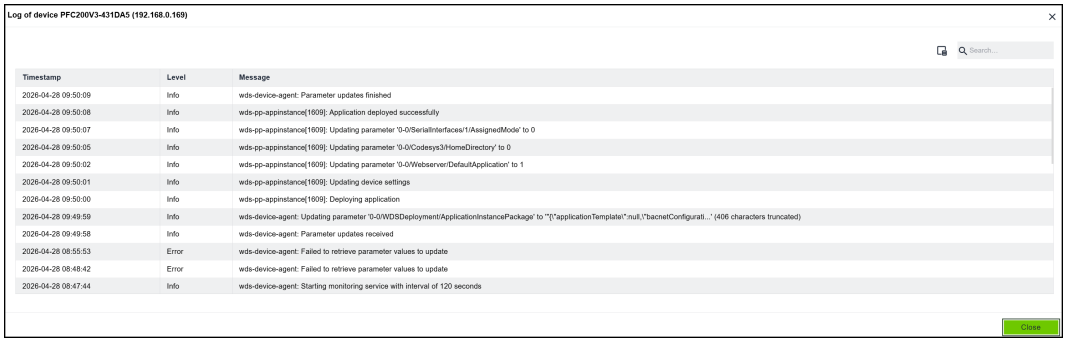


Figure 33: Side Menu > "Devices" Menu Item > "Managed Devices" Tab > "Device Log Messages" Dialog

Designation	Description
Timestamp	Displays the timestamp of the activity.
Level	Displays the message type.
Message	Displays the message content.

7.4.1.2 “New Devices” Tab

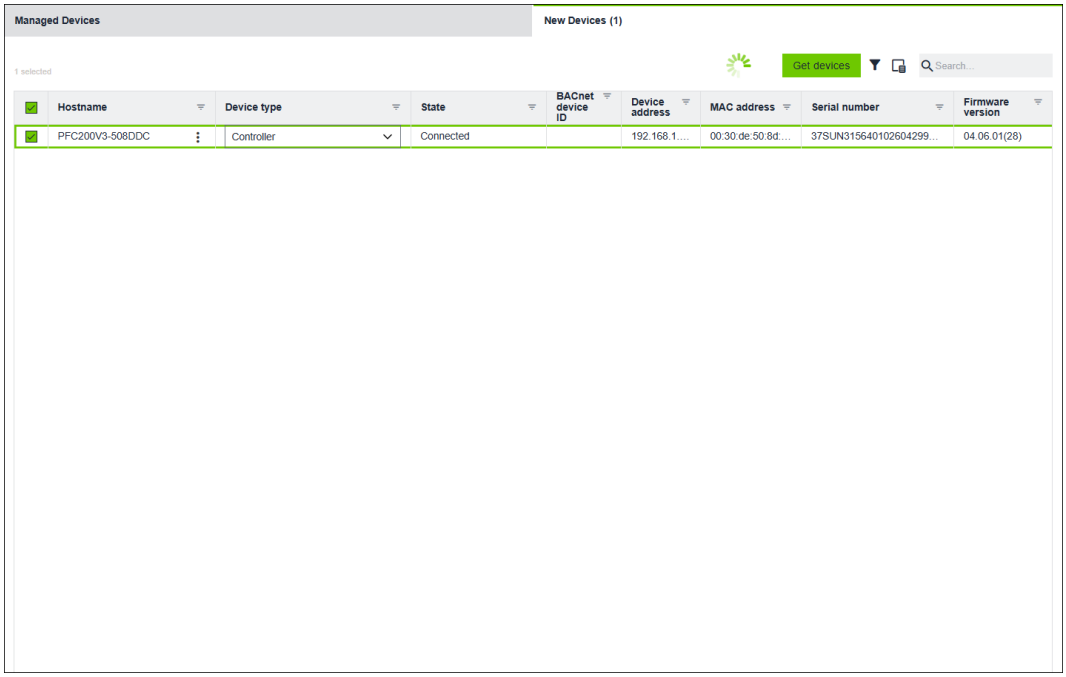


Figure 34: Side Menu > “Devices” Menu Item > “New Devices” Tab

7.4.2 “Configuration” Menu Item

The “Configuration” menu item contains several tabs with different configuration options. In this area, you can set up the selected digital twin and configure it offline. The tabs that are displayed depend on the entity marked in the entity tree.

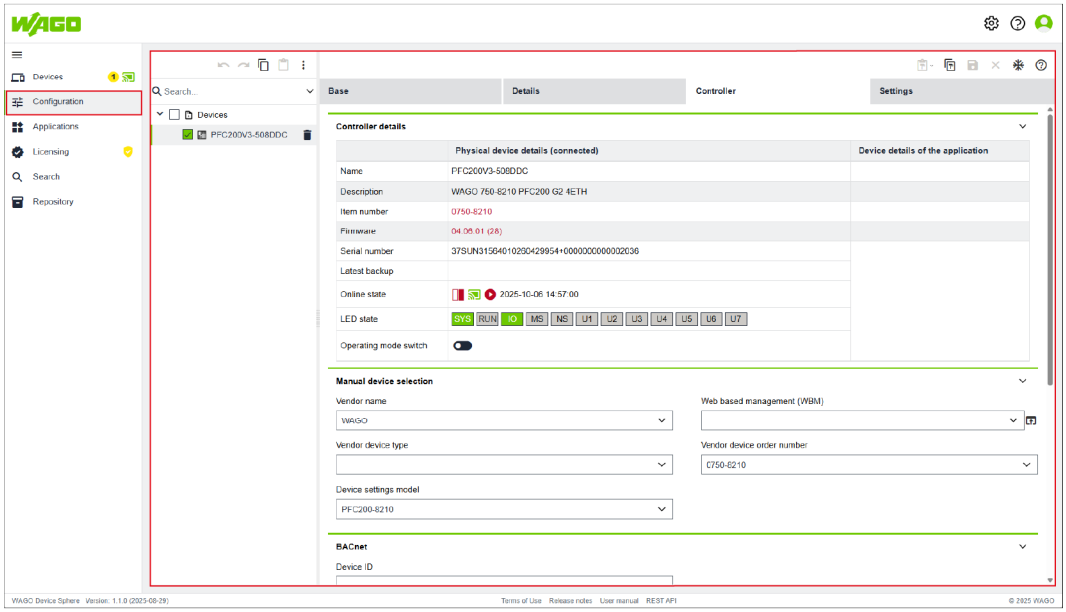


Figure 35: Side Menu > “Configuration” Menu Item

The various tabs are described below.

7.4.2.1 "Basic" Tab

This tab appears with varying contents, depending on the level type when each entity is selected.

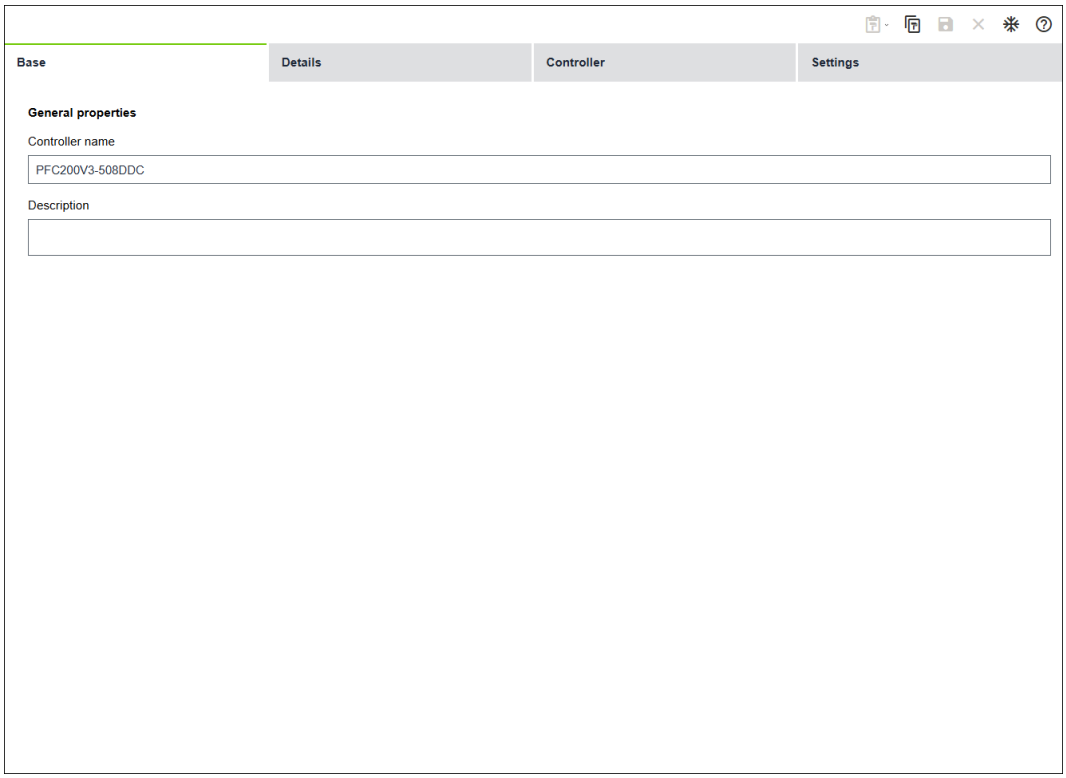


Figure 36: Side Menu > "Configuration" Menu Item > "Basic" Tab

Table 22: Legend for Figure "Side Menu > 'Configuration' Menu Item > 'Basic' Tab"

Designation	Description
General Settings	
Controller name	Name of controller
Description	Description of and information about the controller

7.4.2.2 "Details" Tab

This tab appears with varying contents, depending on the level type when each entity is selected.

This tab contains the following groups:

- **"Tags" group:**
  The "Tags" group allows the entity to be described using one or more tags. Any tag can be entered as free text, which is then offered in all other tag fields as well. Depending on the configuration in the addressing system, default tags are also available for selection to allow for uniform tagging across controllers.
- **"Notes" group:**
  The "Notes" group allows you to create custom notes for the selected entity. Every note is saved with a creation date and time.

- **“Attachments” group:**
  The “Attachments” group allows you to add attachments to the selected controller. You can drag and drop the files you want to attach directly onto the “Attachments” tab or click the **[Select File]** button to use a standard file selection dialog.

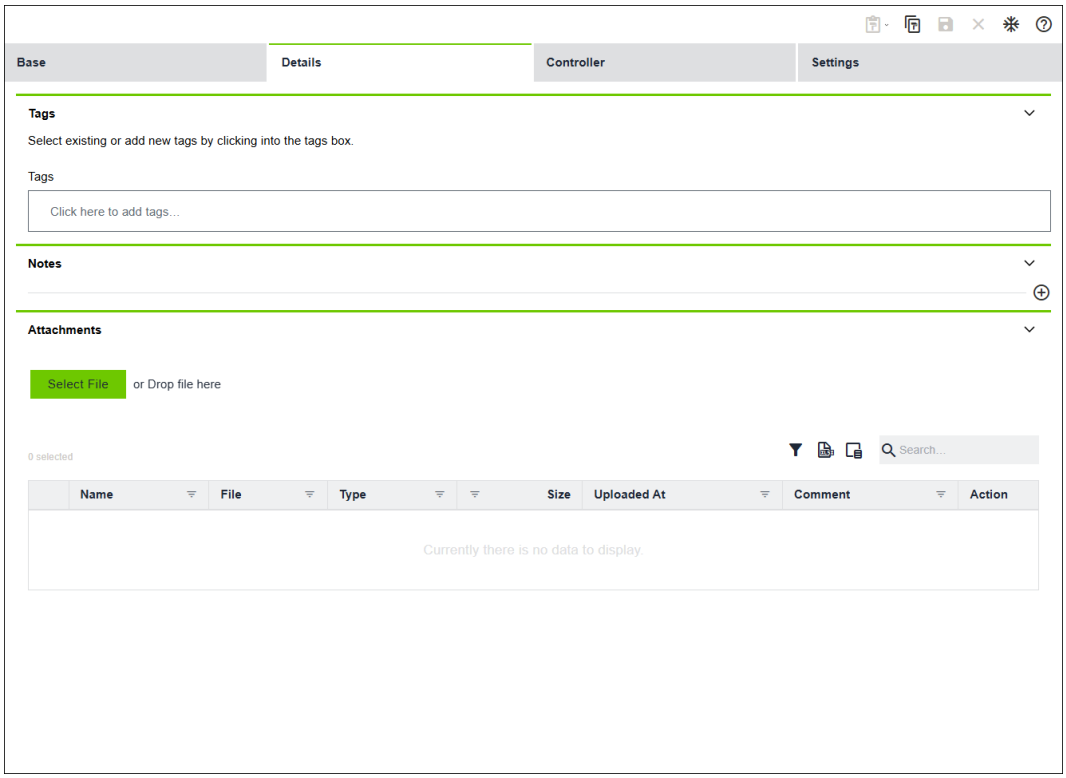


Figure 37: Side Menu > “Configuration” Menu Item > “Details” Tab

Table 23: Legend for Figure “Side Menu > ‘Configuration’ Menu Item > ‘Details’ Tab”

Designation	Description	
Tags		
Tags	Option for selecting one or more tags	
Notes		
Add note	⊕	Adds a new note
Delete note	🗑	Deletes a note
Attachments		
[Select file]	Uploads a file to attach to the entity	

7.4.2.3 “Controller” Tab

The “Controller” tab compares the details of the physical controller to those of the controller required by the application.

This tab appears only when the “Controller” entity is selected.

This tab contains the following groups:

- **“Details” group:**
  The “Details” group displays detailed information about the connected controller.
- **“Manual Device Selection” group:**
  The “Manual Device Selection” group is used for configuring controllers without an assigned application template.

- **“BACnet” group:**
  The “BACnet” group is used for assigning an existing BACnet device ID.
- **“Licenses” group:**
  The “Licenses” group is used for assigning existing licenses.
- **“Packets” group:**
  The “Packets” group is used for adding existing IPK packets.

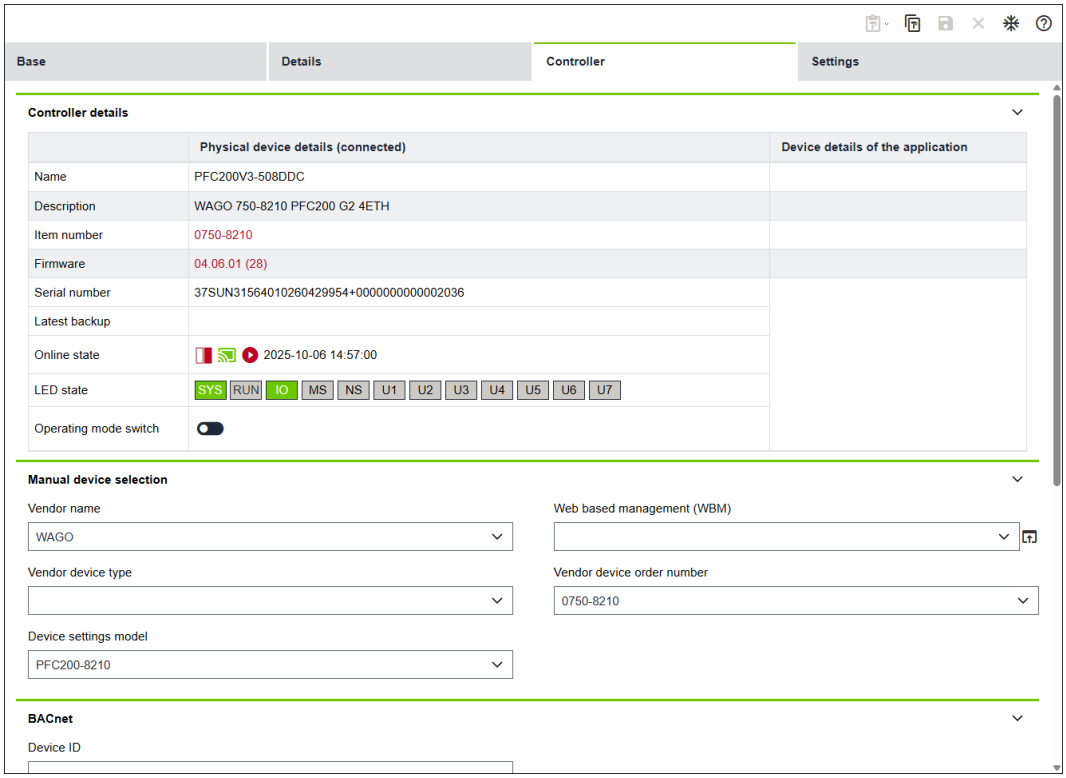
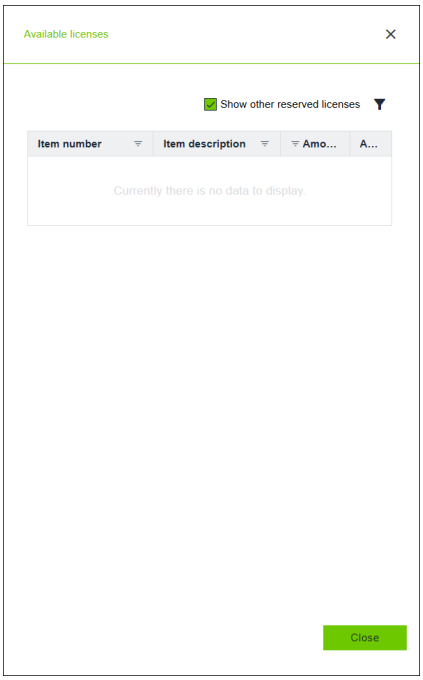


Figure 38: Side Menu > “Configuration” Menu Item > “Controller” Tab

Table 24: Legend for Figure “Side Menu > ‘Configuration’ Menu Item > ‘Controller’ Tab”

Designation	Description
Details	
Physical Details of the Connected Controller	Shows the properties of the physically connected device. **Requirement:** Requires an active monitoring job in “Online” mode and successful connection to the device
Controller Details of the Application	Shows the properties of the controller required by the application
Manual Device Selection	
Manufacturer Name	Entry for manufacturer name
Web-Based Management (WBM)	Entry for WBM address. You can enter the address in the following formats: ▪ **No entry:** Opens the address without *http* or *https* ▪ **URL (short form):** Example: */wbm/index.html* Opens the address in short form ▪ **URL (long form):** Example: *http://{0}:8001/other.html* Opens the address in long form ▪ **URL (fixed):** Example: *http://localhost:8001/controller3.html* Opens a fixed address

Designation	Description
Manufacturer Device Type	Entry for product name
Device Setting Model	Entry for device details/firmware
Manufacturer's Device Order Number	Entry for the item number **Note:** The item number entered must match the item number of the connected controller in order for the settings to be synchronized.
BACnet	
Device ID	For entering the BACnet Device ID
Licenses	
Storage Location	For selecting the storage location
Hardware ID	ID of the selected controller
Open Dialog	 Manually assigns a license to the selected controller. All available licenses are listed. The license can be added to the selected controller. 
Item Number	Item number of the license
Item Name	Item name of the license
Quantity	Number of licenses
Status	Status of the licenses
License Key	License key (in short form)
Serial Number	Serial number of the license
Customer Name	Customer name for which the license was issued
Action	Deletes the license
Packages	
Type	Type of the IPK packet
Name	Name of the IPK package
Version	Version of the IPK package
Action	Deletes the IPK packet

7.4.2.4 "Settings" Tab

On the "Settings" tab, you can make selected controller settings from the Web-Based Management for one or more controllers at the same time.

This tab appears only when the "Controller" entity is selected.

This tab contains the following groups:

- **"WBM" group:**
  The "WBM" group is used for making a wide variety of settings at various levels. This group has specific subsections.

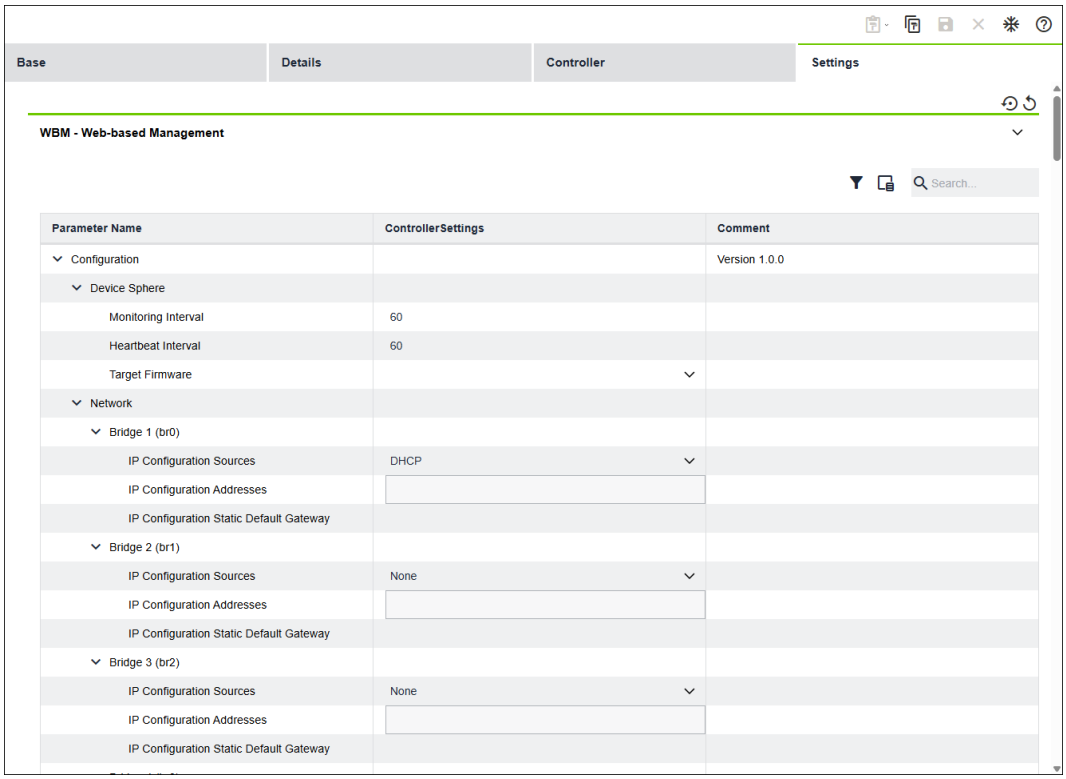


Figure 39: Side Menu > "Configuration" Menu Item > "Settings" Tab

Table 25: Legend for Figure "Side Menu > 'Configuration' Menu Item > 'Settings' Tab"

Designation	Description
Web-Based Management	
Parameter Name	Shows the name of the parameter
Controller Settings	Shows the target value of the parameter **Note:** The WAGO Device Sphere software only transfers modified parameters to the controller! The default values show the firmware's default settings. Since the software does not read these parameters, these values may not match the actual values in the controller!
Comments	Shows added comments
Tags	Shows the tags of parameters

7.4.2.5 "Certificates" Tab

This software version does not support the "Certificates" function yet.

7.4.2.6 Backup & Restore Tab

The “Backup & Restore” tab allows you to restore configurations that were previously backed up on connected controllers. This function is mainly necessary when controllers fail or are configured incorrectly. In the event of an error, all connected controllers can be reset to a normal, fully functional state.

This tab appears only when the “Controller“ entity is selected.

This tab contains the following groups:

- **“Backup” group:**
  The “Backup” group is used to back up existing configurations of connected controllers.
- **“Restore” group:**
  The “Restore” group is used to restore configurations of connected controllers from backup.

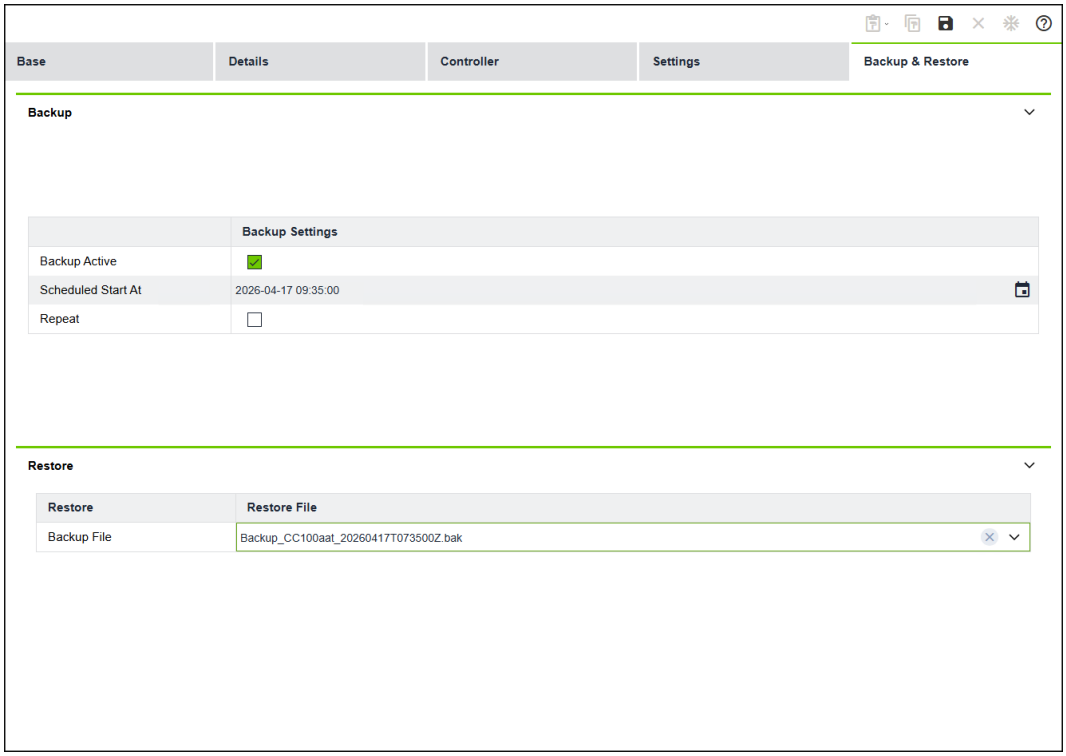


Figure 40: Figure “Side Menu > Menu Item ‘Configuration’ > ‘Backup & Restore’ Tab”

Designation	Description
Backup	
Backup Active	If the checkbox is selected, existing configurations are saved.
Scheduled Start At	Opens a delay start (clock). Using the delay start, you can set when or at what interval an existing configuration should be backed up (see also **Date and Time Input Dialog [▸ 41]**).
Repeat	If this checkbox is selected, additional settings are available.
Repeat Interval (only when “Repeat” is selected)	Repeat interval option: ▪ Hourly: hourly ▪ Daily: daily ▪ Weekly: weekly ▪ Monthly: monthly

Designation	Description
Repeat Every (only when "Repeat" is selected)	Repeat interval option: ▪ Repeat Interval: Hourly Repeat Every: Repeat every x hours – enter the number of hours. ▪ Repeat Interval: Daily Repeat Every: Repeat every x days – enter the number of days. ▪ Repeat Interval: Weekly Repeat Every: Repeat every x weeks – enter the number of weeks. Repeat On: Repeat on the selected weekdays – select the days. ▪ Repeat Interval: Monthly Repeat Every: Repeat every x months – enter the number of months. Repeat on Nth Day: Repeat on the Nth day – enter the day of the month as a number.
Repeat End (only when "Repeat" is selected)	Repeat interval option: ▪ Never: Backup is repeated indefinitely. ▪ On: Backup is no longer repeated after the specified date. ▪ After: No repeats are initiated after x backups.
Restore	
Backup file	You can select a saved configuration to distribute to the connected controllers.

7.4.3 "Applications" Menu Item

The "Applications" menu item manages the all application templates.

New application templates can be uploaded in the **.atpkg* format via the "Import" function.

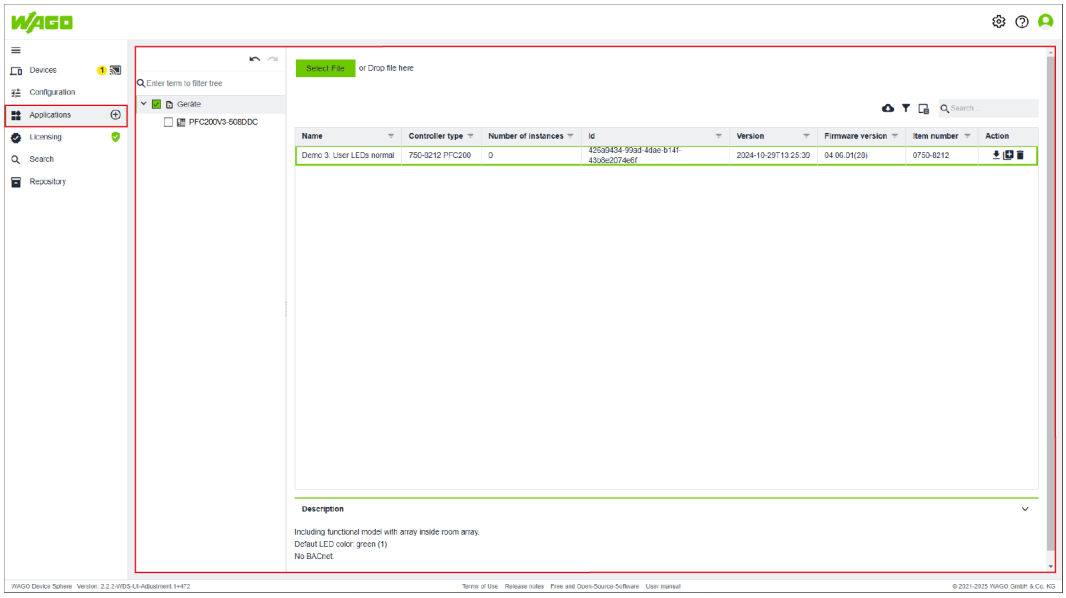
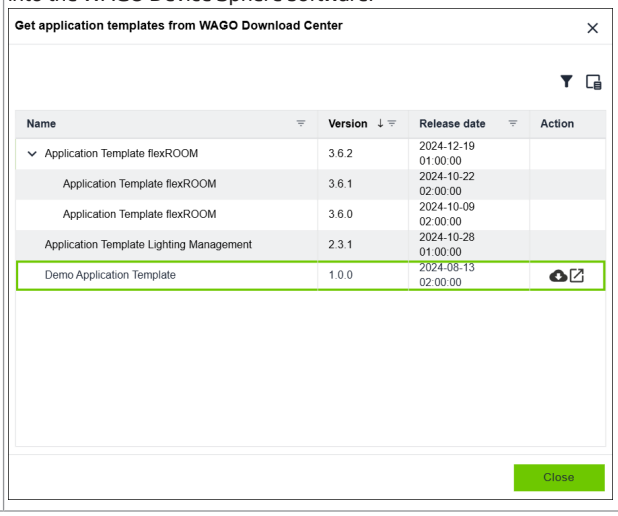


Figure 41: Side Menu > "Applications" Menu Item

Table 26: Legend for Figure "Side Menu > 'Applications' Menu Item"

Designation	Description	
Import application template	⊕	Imports an application template from a file and adds it to the WAGO Device Sphere software.

Designation	Description	
Get application templates from the WAGO Download Center		Opens the "Get Application Templates from the WAGO Download Center" dialog. The dialog lists the latest application templates that are available in the **WAGO Download Center** and can be loaded into the WAGO Device Sphere software. 

7.4.4 "Licensing" Menu Item

The "Licensing" menu item can be used to manage and assign the licenses for all of the implemented controllers. The WAGO Device Sphere software shares the license repository with other WAGO software installed on the same operating system.

This menu item contains the following tabs:

- **"Project Licenses" Tab** (see "Project Licenses" Tab [▸ 56])
  This tab lists all the licenses that are available for the open project.
- **"License Repository" Tab** (see "License Repository" Tab [▸ 56])
  This tab shows all the licenses present in the local license repository for the operating system being used.

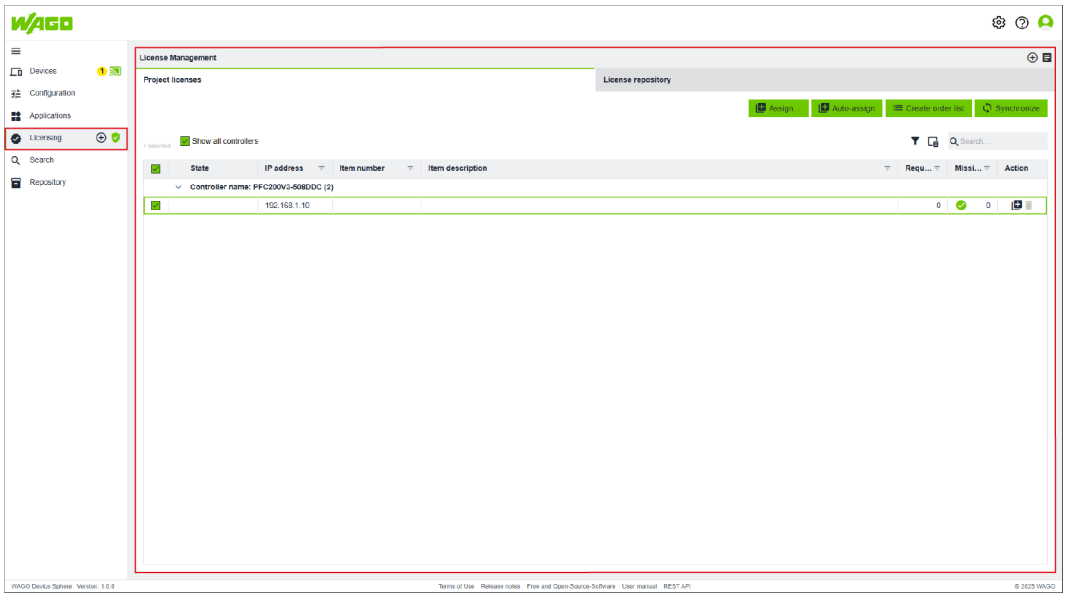
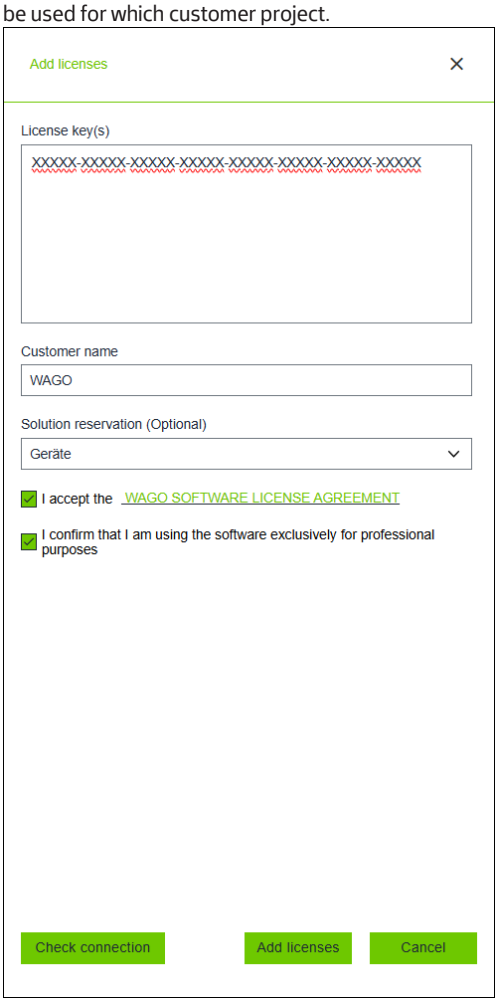


Figure 42: Side Menu > "Licensing" Menu Item

Table 27: Legend for Figure “Side Menu > ‘Licensing’ Menu Item”

Designation	Description	
[Add Licenses]	⊕	Opens the “Add Licenses” dialog. In this dialog, you can enter all the licenses you have purchased from WAGO and add them to the common license repository for the operating system being used. The corresponding license key can be found on your license certificate. You can enter multiple license keys in sequence, separated by spaces. In the dialog itself, you also have to enter the corresponding customer name for the license certificate along with the license key. In addition, licenses that have been entered can be reserved directly for a specific project. This lets you determine which licenses are to be used for which customer project.  **[Check Connection]** checks whether the WAGO license server on the Internet can be reached. This process is necessary for some license keys. **[Add Licenses]** adds the entered licenses to the license repository of the operating system being used, making them then available in WAGO Device Sphere.
View license agreement	🗎	Opens the “WAGO Software License Agreement” (General Terms and Conditions of Use) as a PDF.

7.4.4.1 "Project Licenses" Tab

This tab lists all the licenses that are available for the configured controller. The list is sorted by device and compares the license requirements for a device to the number of licenses actually assigned. The license requirements are determined by the number of assigned application templates.

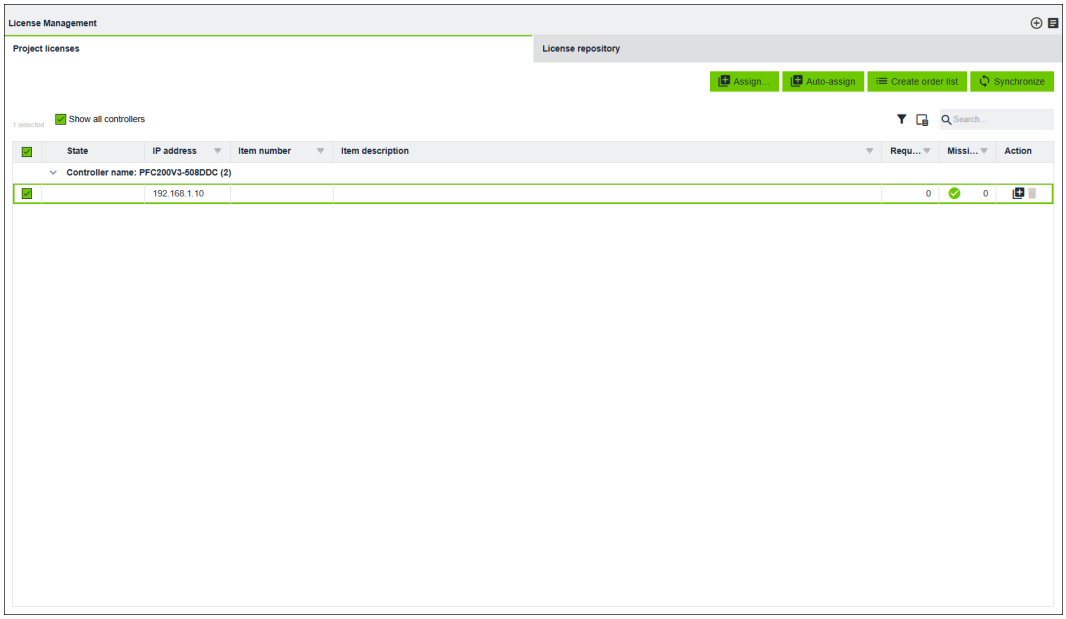


Figure 43: Side Menu > "Licensing" Menu Item > "Project Licenses" Tab

Table 28: Legend for Figure "Side Menu > 'Licensing' Menu Item > 'Project Licenses' Tab"

Designation	Description
Assign	Manually assigns a license to a selected device. All available licenses are listed. The license can be added to the selected device.
Auto-Assign	Automatically assigns available licenses to meet the license requirements that have been identified.
Create Item List	This function is not supported at this time.
Sync	Starts license synchronization between the project and the devices in the network. This transfers the license configuration previously created offline to the devices.

7.4.4.2 "License Repository" Tab

This tab shows all the licenses present in the local license repository for the operating system being used. The corresponding properties are also displayed for each entry.

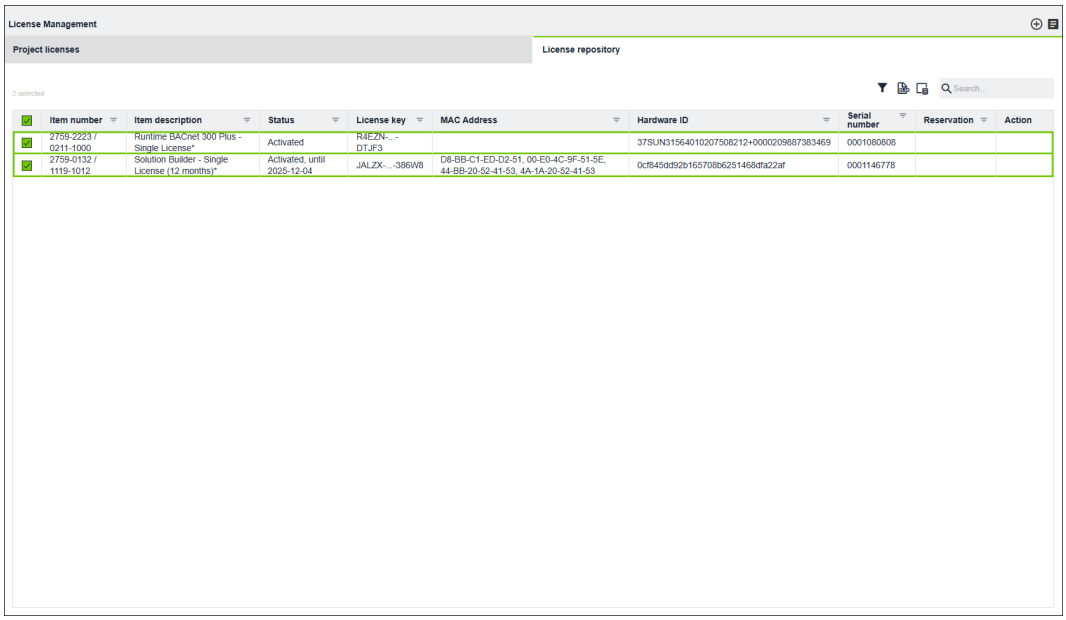


Figure 44: Side Menu > "Licensing" Menu Item > "License Repository" Tab

7.4.5 "Search" Menu Item

You can use the "Search" menu item to search by different criteria and properties and to save filters in search configurations. Saving filters makes them available at all times in the entity tree and for automation assignment of controllers in groups.

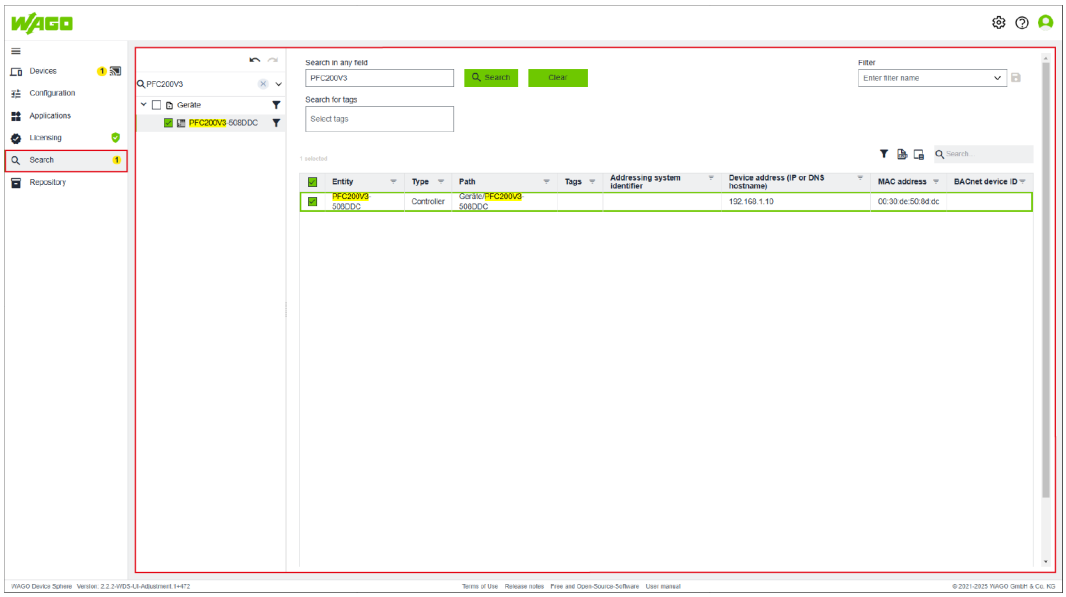


Figure 45: Side Menu > "Search" Menu Item

Table 29: Legend for Figure "Side Menu > 'Search' Menu Item"

Designation	Description
[Search]	Starts the search
[Reset]	Clears the search inputs and results from the search dialog
Full-text search	Full-text search can be used to search all properties of the entities.
Search for tags	Search for one or more tags on entities
Filters	Enter the filter name and save the search configuration using the Save icon. From the drop-down menu, you can open any of the saved search configurations for activation or delete them.

Designation	Description
	Exports the search results as a table in *.xlsx format **Note: The exported table values for controllers can be processed and re-imported. This makes it easier to assign unique values, including target settings for IP addresses, MAC addresses, controller names and BACnet device IDs.**

7.4.6 "Depot" Menu Item

The "Depot" menu item manages all the software versions available for the WAGO Device Sphere software. This includes the controller firmware, for example.

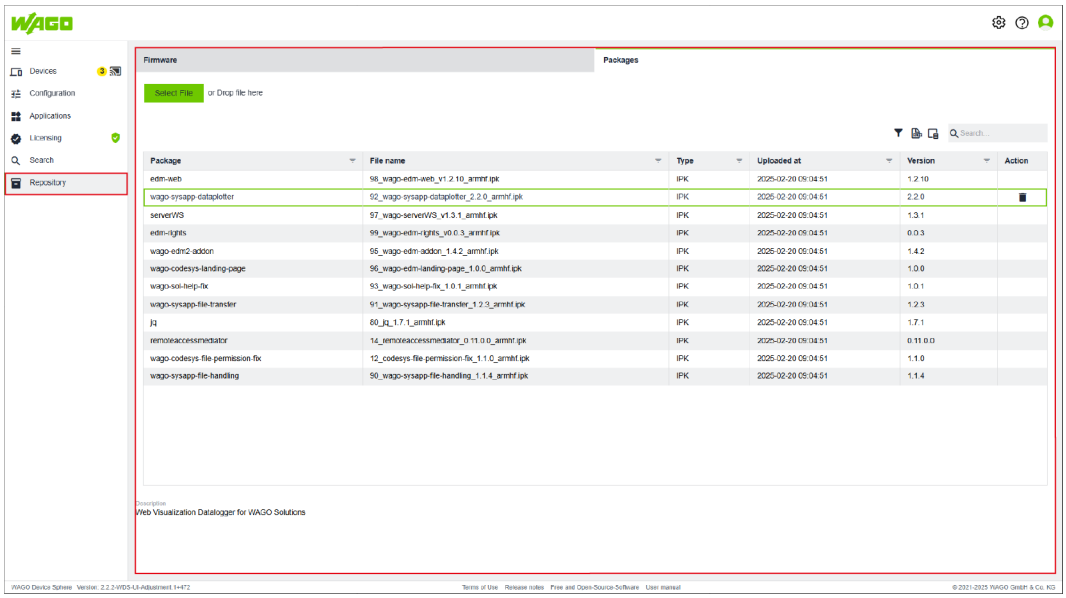


Figure 46: Side Menu > "Depot" Menu Item

7.4.6.1 "Firmware" Tab

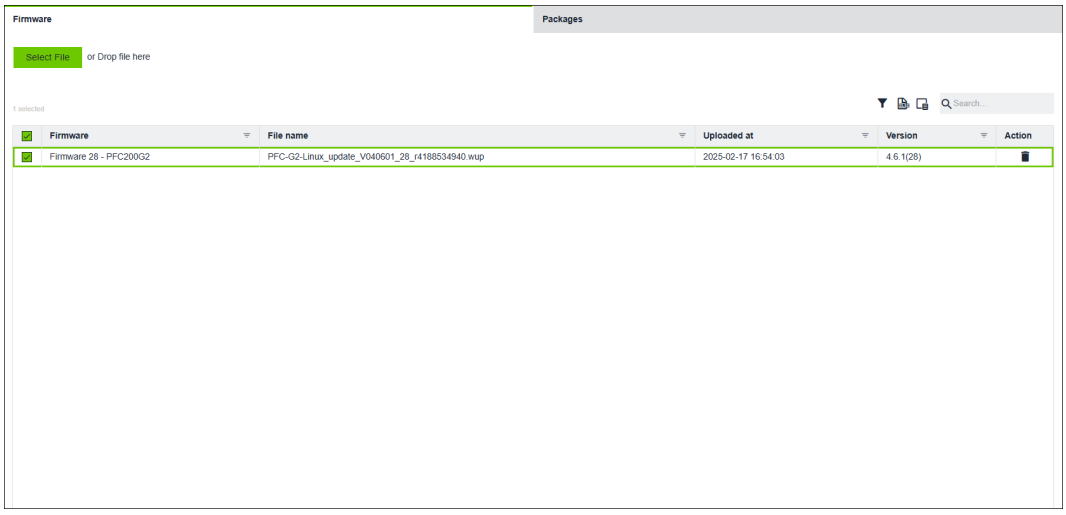


Figure 47: Side Menu > "Depot" Menu Item > "Firmware" Tab

Table 30: Legend for Figure "Side Menu > Depot > 'Firmware' Tab"

Designation	Description
[Select file] or drag here	Allows you to add an export file by using a standard file selection dialog or dragging the export file into the field

Designation	Description
	**This function is only shown when the WAGO Device Sphere software is opened via "localhost"!** Loads the latest firmware version from the **WAGO Download Center**
	Exports the firmware list as an Excel file
Firmware	Shows the firmware name/description
Filename	Shows the firmware filename
Uploaded on	Indicates the date the firmware was uploaded to the WAGO Device Sphere software
Version	Indicates the firmware version
Action	The following actions are available: ▪ Deleting the firmware from the WAGO Device Sphere software

7.4.6.2 "Packages" Tab

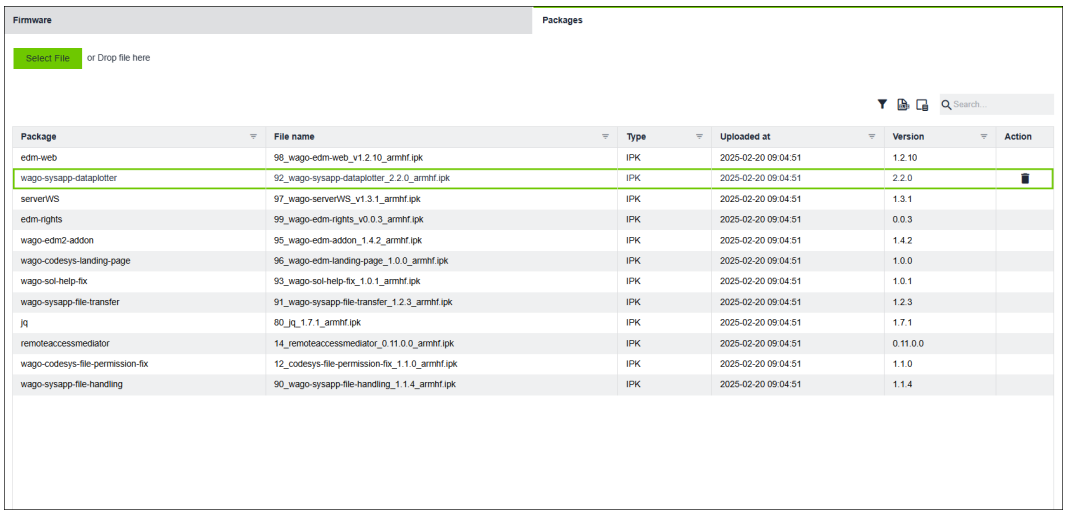


Figure 48: Side Menu > "Depot" Menu Item > "Packages" Tab

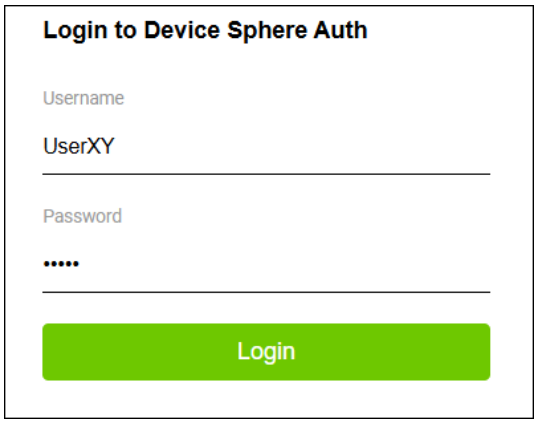
Table 31: Legend for Figure "Side Menu > Depot > 'Packages' Tab"

Designation	Description
[Select file] or drag here	Adds an IPK package file using a standard file selection dialog or by dragging the IPK package file into the box.
	Exports the package list as an Excel file.
Package	Shows the name of the IPK package.
Filename	Shows the filename of the IPK package.
Type	Shows the IPK package type.
Uploaded on	Indicates the date the IPK package was uploaded to the WAGO Device Sphere software.
Version	Shows the IPK package version.
Action	The following actions are available: ▪ Deletes the IPK package from the WAGO Device Sphere software.

8 Operation

8.1 Coupling a Device

1. Open the WAGO Device Sphere software.
2. Log in with the credentials you set up during the installation process (see Installation [▸ 17]).



3. Select the “Devices” menu item.
4. Select the “New Devices” tab.

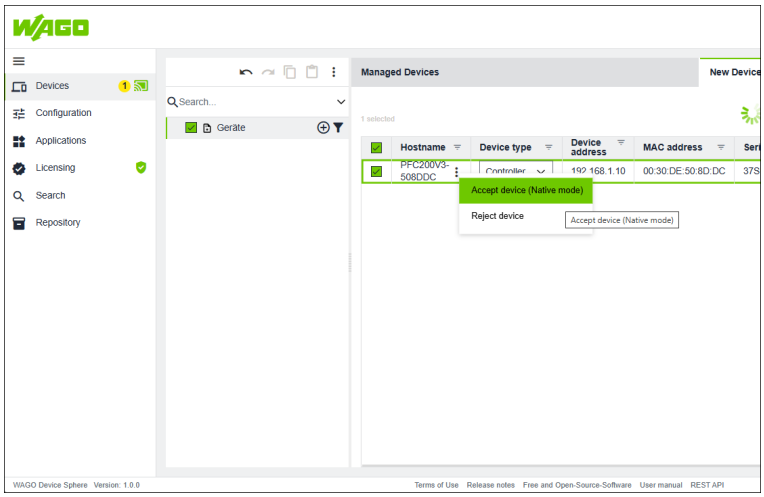
   ⇨ A progress bar appears. The progress bar indicates that the WAGO Device Sphere software server is actively searching for possible controllers.

   ⇨ After a synchronization period, the controller used is displayed.

   ⓘ Note **Synchronization may take some time**

   Depending on your PC’s system and workload, it may take a few minutes for the controller used to appear as a “new device.” During the synchronization process, do not perform other actions on the computer. If no controller is displayed after about two to three minutes, repeat the steps in Web-Based Management.

   ⇨ The controller used is assigned the status “Requested” under “Status.”
5. Click on the context menu under “Hostname.”
6. Select **Integrate Device (Native Mode)**.



⇨ The controller used is assigned the status “Prepared” under “Status.”

⇨ The controller used is initialized.
The required software packages are installed.

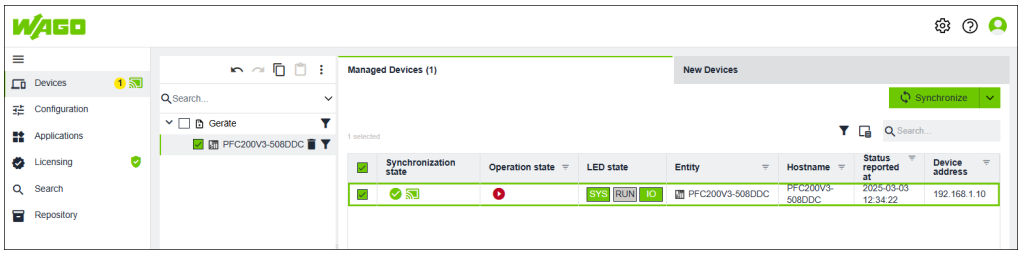
⇨ The controller used is assigned the status “Connected” under “Status.”

7. Drag and drop the controller onto the “Devices” entity.

⇨ The controller is assigned to the “Devices” entity.

⇨ The controller can now be found on the “Managed Devices” tab.

8. Select the “Managed Devices” tab.
9. Select the controller.
10. Click **[Online]**.
11. Click **[Synchronize]**.



⇨ The controller is created and is configurable in the WAGO Device Sphere software as a “managed device.”

8.2 Checking the “Commissioning Service” in the Web-Based Management

The Web-Based Management provides a “Commissioning Service” setting. This setting ensures that the corresponding device can establish an initial connection to the WAGO Device Sphere software’s server.

By default, this setting is enabled in the Web-Based Management. Therefore, the corresponding device is actively available for coupling during commissioning (see **Coupling a Device [▸ 60]**).

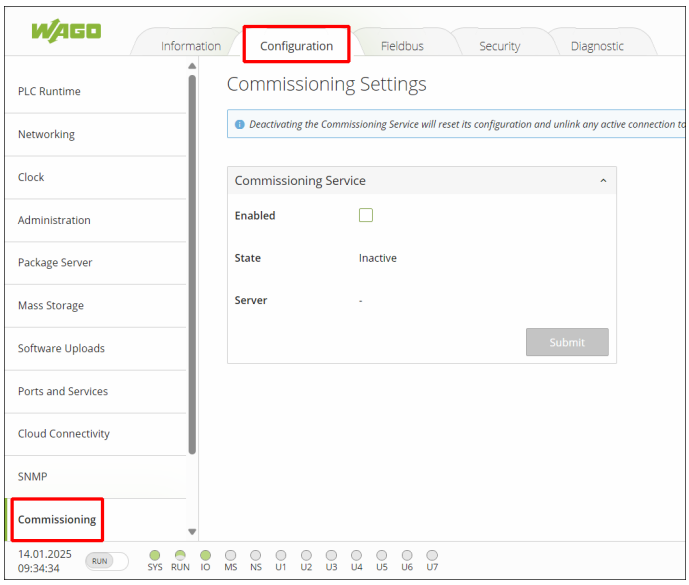
If a connection cannot be established successfully, this setting should be checked.

In certain configuration steps, it is also necessary to restart the Commissioning Service once. That requires disabling the setting and then re-enabling it. This is necessary, for example, if the root CA certificate is switched out and all device connections to the server become invalid.

The following explains how the Commissioning Service can be enabled and disabled in the Web-Based Management.

8.2.1 Enabling Commissioning Service and Establishing Coupling State

1. Enter the IP address of the controller used in a browser.
   ⇨ The Web-Based Management opens.
2. Select the "Configuration" tab.
3. Select the "Commissioning" menu item.



4. In the "Commissioning Service" group, check the "Enabled" box.
5. Click **[Submit]**.
   ⇨ The "Commissioning Service" is enabled.
   ⇨ The controller now attempts to reach the WAGO Device Sphere software server on its own.

8.2.2 Disabling Commissioning Service and Resetting Coupling State

1. Repeat steps 1 … 3 from section **Enabling Commissioning Service and Establishing Coupling State [▸ 62]**.
2. In the "Commissioning Service" group, check the "Disabled" box.
3. Click **[Submit]**.
   ⇨ The Commissioning Service is disabled.
4. In the "Commissioning Service" group, check the "Enabled" box.

5. Click **[Submit]**.
   ⇨ The “Commissioning Service” is re-enabled.
   ⇨ The controller now attempts to reach the WAGO Device Sphere software server on its own.

8.3 Deleting Devices

All connected and coupled devices can be removed manually. There are two different variants:

- **Removing devices from the offline project data**
  Removes all coupled devices from the created project; the devices are still available in the software via the device list and can be used for other projects.
  (See **Removing Devices from the Offline Project Data [▸ 63]**)
- **Completely removing devices from the software**
  Removes all connected devices from the software; the devices are also no longer available in the software via the device list.
  (See **Completely Removing Devices from the Software [▸ 63]**)

8.3.1 Removing Devices from the Offline Project Data

1. In the tree structure, select the device you want to remove.
2. Click **[Delete]**.
   ⇨ The device is removed from the tree structure and no longer assigned to the “Devices” entity.
   ⇨ The “Managed Devices” tab no longer contains the device.
   ⇨ However, the device can be accessed at any time via the “New Devices” tab and is available in the internal device list.
3. Select the “New Devices” tab.
4. Click **[Get Devices]**.
   ⇨ The device is displayed.

8.3.2 Completely Removing Devices from the Software

1. Select the “Managed Devices” tab.
2. Right-click on the corresponding device and select **Delete from WAGO Device Sphere** or **Delete from WAGO Device Sphere and Project**.
   ⇨ The device is completely removed from the WAGO Device Sphere software.
   ⇨ To add the device back to the device list, repeat the steps in section **Coupling a Device [▸ 60]**.

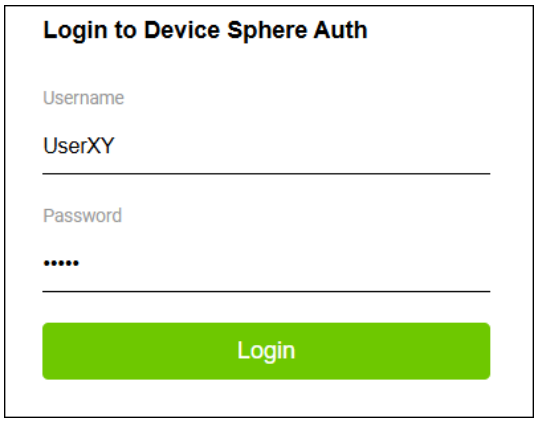
8.4 Opening Log Files from the Device

The WAGO Device Sphere software stores log files for various internal components to trace the processes within the software.

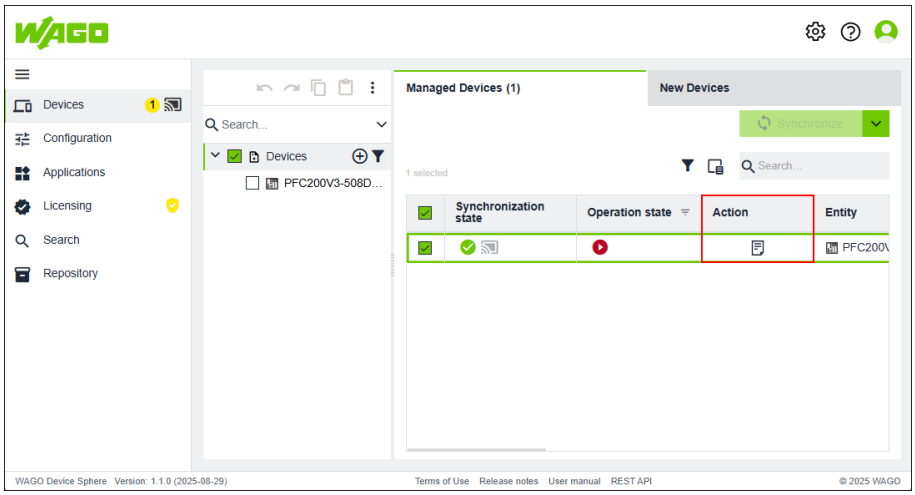
You can open the log files as follows:

1. Open the WAGO Device Sphere software.

2. Log in with the credentials you set up during the installation process (see **Installation [▸ 17]**).



3. Select the "Devices" menu item.
4. Select the "Managed Devices" tab.
5. Under "Action," click the "Display Device Log Messages" icon.



⇨ The log files are retrieved and displayed in a table.

8.5 Update the Controller Firmware

✓ You have opened the WAGO Device Sphere software and are signed in.

1. Select menu item "Configuration".
2. Select the controller whose firmware you want to change.
3. Select the "Settings" tab.
4. In the "WBM – Web-Based Management System" group, under the setting "Configuration > Device Sphere > **Firmware Target**", select the required firmware version.

   ⇨ The screen displays all firmware versions uploaded to the repository are available, and are compatible with the selected controller.
   For more information, see **"Depot" Menu Item [▸ 58]**.

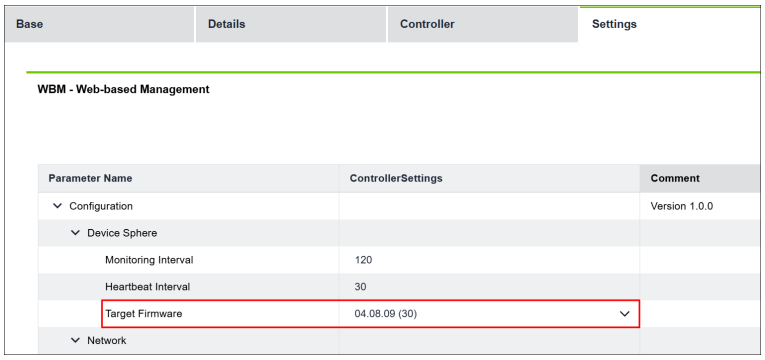


Figure 49: The drop-down menu us used to change the controller firmware version.

➡ The selected firmware version is installed on the controller.

8.6 Create and Configure a Digital Twin

Using a digital twin, you can configure controllers before they are integrated into the WAGO Device Sphere software.

✓ You have opened the WAGO Device Sphere software and are signed in.

1. Select the "Configuration" menu item (also possible via the "Devices" menu item).
   ⇨ A drop-down menu opens.
2. Click the "Add item" icon (⊕).

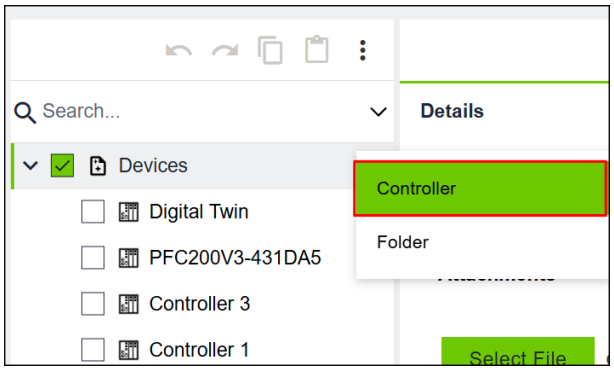


Figure 50: Create a New Digital Twin

3. Select "Controller" from the drop-down menu.
   ⇨ The digital twin has been created.
4. Select the digital twin in the entity tree.
5. In the workspace, select the "Controller" tab.
6. Fill in the controller's property fields.
   ⇨ To use this as a digital twin, you must at least fill in the "Firmware Version" and "Item Number" fields.
7. Save the changes.
   ⇨ The digital twin has been created.
8. In the workspace, select the "Settings" tab to configure the digital twin via the WBM.
9. Save the changes.

➡ The digital twin has been created and configured.

9 Uninstalling

Securely uninstalling the app helps prevent various attacks. A secure uninstallation meets at least the following requirements:

- Software is uninstalled
- Software data is deleted from the environment
  - Deleted certificates
  - Deleted configuration data (active)
  - Deleted log files
  - Deleted database data

9.1 Uninstalling on Windows

1. Uninstall the software using the standard Windows® function for removing programs (e.g., via the **Start menu** or **Settings** > **Apps**).

   ⇨ The software's set-up dialog opens.

2. To remove all saved user settings during uninstallation, the "Remove user settings when uninstalling" option is selected by default.
   By deselecting the checkbox, the following user settings are retained by default:
   - Certificates
   - Configuration files
   - Log files
   - Database data

3. To remove the software, click **[Uninstall]**.

9.1.1 Data Cleanup

If the checkbox for "Remove user settings on uninstall" is not checked, the user settings are retained even after uninstallation.

User settings are saved in the following directory:

```
C:\\ProgramData\\WAGO Software\\WAGO Device Sphere
```

1. Permanently delete the directory.
2. Then delete the files from the Trash.

➡ The software has been completely removed.

9.2 Uninstalling on Linux®

1. Open the terminal.
2. Navigate to the script:

   ⇨ e.g., *cd Downloads/*

3. Enter *sudo ./setup.sh -u --deleteAllData* to run the script and start the uninstallation.

   ⇨ The uninstallation operation starts.

➡ The uninstallation has been completed.

9.2.1 Data Cleanup

Uninstalling the software using the command sudo *./setup.sh -u --deleteAllData* deletes all software files. It is not necessary to manually delete any remaining user files.

10 Appendix

10.1 Managing Controllers and Data via REST API

Note

In-depth IT knowledge in connection with REST API required!

The following content is relevant for the "Software Developers" target group who wish to use the WAGO Device Sphere software outside of the provided graphical user interface. This requires in-depth IT knowledge in connection with the REST API!

In addition to the graphical user interface provided, controllers and data can also be managed via the REST API. The REST API offers the following use cases:
- Scripting, e.g., automatic registration of controllers
- Customer-specific applications

The REST API can execute the following functions:
- Controller management and access to data
- Subscription and workspace management
- Alarm configuration and access to alarm data

This section describes the architecture of the REST API and shows how to register a controller or receive data from a controller, for example.

10.1.1 Supported Endpoints

The following table shows the endpoints supported by the REST API.

Table 32: Supported Endpoints

Supported Endpoint	Description
Root	General endpoint that provides overview information and links to other interfaces.
EnumDefinition	Enums referenced in parameter and method argument definitions are globally defined, reusable types. Therefore, enums are represented as resources in a global collection of resources of type enum-definition. Normally, enum definitions are retrieved through the enum reference of the parameter and method argument definition resources mentioned above. However, an enum definition can also be requested from its primary storage location, as described in the next sections. Regardless of how an enum definition is retrieved, the response body has the same structure.
Features	Each device contains certain functions that are modeled as features. A typical function can consist of several parameters and methods and contain other functions. For example, devices whose firmware can be updated have the feature FirmwareUpdate. The information about which parameters and methods belong to a feature can be retrieved via a feature's reference links. Note that containedParameters and containedMethods only list the parameters and methods that belong directly to a feature. The includedFeatures can also contain parameters and methods that should be understood as indirectly contained.
MonitoringList	Monitoring lists are a mechanism for easily and efficiently managing user-defined monitoring lists for parameters. Creating a monitoring list essentially means defining a temporary container with any parameters. The list then allows easy, efficient read access to the parameters it contains.
Parameter	Using the WDA REST API, you can discover, retrieve and set available parameters on any WDA-capable device. Essentially, the parameter-specific endpoints offer a way to retrieve and set all the available parameters that the WDA-capable device offers.

Supported Endpoint	Description
Service	You can ask the service for basic but important information about itself. The service identity endpoint provides you with relevant information, such as the active REST API and the service version.
WdaDevice	Devices play an important role in the WDA REST API. The endpoints connected to /wda/devices provide read-only information for WDA-enabled devices. The information that can be accessed includes the item number and firmware version.
Apikey	API controller for server Apikey management
Commissioning	API controller for device registration, status queries, approval and confirmation
Configuration	API controller for server configuration
Device	API controller for device endpoints
DeviceTwin	API controllers for managing device twin records, including listing, retrieving, revoking and deleting device twins
Files	API controller for file processing
LicenseCommunication	API controller that handles license communication requests

10.1.2 "Swagger" Tool

Swagger is a tool for managing REST APIs. All the corresponding processes and services of the WAGO Device Sphere software can be used via the Swagger UI. In addition, detailed documentation of the REST API is also part of the Swagger UI.

You can access the WAGO Device Sphere software's REST API through the following link:
`https://<HostName>/api/doc`

Authentication via Swagger

Two authentication methods are available for authorization and interaction with the WAGO Device Sphere software's REST API:

- **Authentication method 1:**
  Authentication via WAGO Device Sphere software login data
- **Authentication method 2:**
  Authentication via API key

ⓘ Note

Use only one authentication method!

Only use one of the two authentication methods. The server does not allow both requests to be used at the same time and cancels both requests if they are. Therefore, log in using only one authentication method!

Authentication Method 1: Authentication via WAGO Device Sphere Software Login Data

1. In the Swagger user interface, click **[Authorize]**.
2. Authenticate yourself with the **Bearer (OAuth2, password)** authentication method.
3. Use your login data to log in from the WAGO Device Sphere software.
4. From the "client_id" drop-down menu, select **wds_generic_client**.
5. Click **[Authorize]**.
   ⇨ Authentication is complete.

Authentication Method 2: Authentication via API Key

1. In the Swagger user interface, click **[Authorize]**.
2. Authentication is performed with the **ApiKey (apiKey)** authentication method.
3. Generate a REST API key by sending a post request to the endpoint **/api/v1/api-key**.
4. Click **[Authorize]**.
5. Enter your API key in the input field.

   ⇨ Authentication is complete.

10.2 Protected Rights

- Adobe® and Acrobat® are registered trademarks of Adobe Systems Inc.
- Android™ is a trademark of Google LLC.
- Apple, the Apple logo, iPhone, iPad and iPod touch are registered trademarks of Apple Inc. registered in the USA and other countries. "App Store" is a service mark of Apple Inc.
- AS-Interface® is a registered trademark of the AS-International Association e.V.
- BACnet® is a registered trademark of the American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc. (ASHRAE).
- *Bluetooth*® is a registered trademark of Bluetooth SIG, Inc.
- CiA® and CANopen® are registered trademarks of CAN in AUTOMATION – International Users and manufacturers Group e.V.
- CODESYS is a registered trademark of CODESYS Development GmbH.
- DeviceNet® is a registered trademark of the Open DeviceNet Vendor Association, Inc (ODVA).
- DALI is a registered trademark of the Digital Illumination Interface Alliance (DiiA).
- Docker® and the Docker® logo are trademarks or registered trademarks of Docker, Inc. in the USA and/or other countries. Docker, Inc. and other parties may also have trademark rights to other terms used herein.
- EtherCAT® is a registered trademark and patented technology licensed by Beckhoff Automation GmbH, Germany.
- ETHERNET/IP™ is a registered trademark of the Open DeviceNet Vendor Association, Inc (ODVA).
- EnOcean® is a registered trademark of EnOcean GmbH.
- ***flex***ROOM® is a registered trademark of WAGO Verwaltungsgesellschaft mbH.
- Google Play™ is a registered trademark of Google Inc.
- IO-Link is a registered trademark of PROFIBUS Nutzerorganisation e.V.
- KNX® is a registered trademark of the KNX Association cvba.
- Linux® is a registered trademark of Linus Torvalds.
- LON® is a registered trademark of the Echelon Corporation.
- Modbus® is a registered trademark of Schneider Electric, licensed for Modbus Organization, Inc.
- OPC UA is a registered trademark of the OPC Foundation.
- PROFIBUS® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- PROFINET® is a registered trademark of the PROFIBUS Nutzerorganisation e.V. (PNO).
- QR Code is a registered trademark of DENSO WAVE INCORPORATED.
- Subversion® is a trademark of the Apache Software Foundation.
- Windows® is a registered trademark of Microsoft Corporation.

List of Figures

List of Tables

Glossary

Application Template

Exported data packet from an IEC development environment (CODESYS or ***e!****COCKPIT).* The data packet contains a boot application, a fieldbus configuration, a description and, optionally, a functional data model. The package can be imported into the WAGO Device Sphere software.

Commissioning Agent

Central software component responsible for initializing devices the first time they are connected to the WAGO Device Sphere software server.

Commissioning Service

This setting in the Web-Based Management ensures that the corresponding device can establish an initial connection to the WAGO Device Sphere software's server.

Device Agent

Central software component that is installed on the devices. This component ensures secure communication, configuration and parameterization of all individual components in the WAGO Device Sphere software. The component is installed on the devices as part of the commissioning process.

Digital Twin

Virtual representation of a physical device. The representation is based on real-time data and simulations so it can represent the behavior, state and performance of its real-world counterpart as precisely as possible.

Docker Daemon

Background process for managing Docker Engine. This process is used to create, execute, manage and delete containers.

IPK Package

An IPK package is a compilation of individual IPK files. IPK files ("Itsy Package File") are small installation files. They are designed for distributing software and other utility programs over low-resource computers such as routers, multimedia receivers, set-top boxes, etc.

Portainer Edge Agent

Central software component that is installed on the devices. This component ensures secure management and orchestration of containers via the Portainer platform. The component is installed on the devices as part of the commissioning process (Portainer Mode).

Vulnerability

A vulnerable spot that is not protected or is insufficiently protected and thus represents a vulnerability.

WAGO Device Sphere

Software for centralized device management of controllers

WAGO GmbH & Co. KG
Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden
info@wago.com
www.wago.com

Headquarters	+49 571/887 – 0
Sales	+49 (0) 571/887 – 44 222
Order Service	+49 (0) 571/887 – 44 333

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.
Copyright – WAGO GmbH & Co. KG – All rights reserved. The content and structure of the WAGO websites, catalogs, videos and other WAGO media are subject to copyright. Distribution or modification of the contents of these pages and videos is prohibited. Furthermore, the content may neither be copied nor made available to third parties for commercial purposes. Also subject to copyright are the images and videos that were made available to WAGO GmbH & Co. KG by third parties.