

Installation and Operating Manual

openXEdge

Industrial PC for process data acquisition at the machine



Brinkhaus GmbH

Version 2026.10.21

Date: 10.2026

Subject to technical changes without notice!



Contents

1 Getting started	3
1.1 Introduction	3
1.2 First Boot Walkthrough	3
2 How-to guides	9
2.1 Update firmware	9
2.2 Install firmware offline via USB	10
2.3 Change password	11
2.4 Access from another computer (HTTPS)	13
2.5 Choose the interface language	17
2.6 Configure the network	19
2.7 Configure the firewall	21
2.8 Manage users	23
2.9 Read diagnosis	26
2.10 Configure an IDEA-4S device	28
2.11 Configure the IO-Link master	34
2.12 Export measurement data to Excel	36
3 Reference	38
3.1 Diagnosis codes	38
3.2 IDEA-4S – signal names in the DataStore	41
4 Background	43
4.1 The device	43
4.2 Edge wiring	45
4.3 How updates work	46
4.4 Grafana dashboards	48
4.5 Resource monitoring	52
4.6 Fleet onboarding	53
4.7 Security and support	56
5 Notes	61



1 Getting started

1.1 Introduction

The openXEdge is an industrial PC that works right at the machine. It collects measurement data, stores it on the device and shows it in the browser — on every network port of the edge, without a connection to the internet. It runs unattended: if someone pulls a network cable or a peer goes down, the services reconnect on their own as soon as it is reachable again. It installs firmware updates by itself and returns to the previous state if an update fails.

1.1.1 How this handbook is organised

The page list on the left leads through the whole handbook, top to bottom:

- **Tutorial** — first commissioning step by step. If you are unpacking a new device, start with First Boot Walkthrough (Ch. 1.2).
- **How-to guides** — single tasks in operation: updating the firmware, setting up network and firewall, managing users, reading the diagnosis.
- **Reference** — lists to look things up, such as all diagnosis codes (Ch. 3.1).
- **Explanation** — background: how updates work, how the edge is wired, what it does for security and support.

The language switch at the top right keeps you on the same page.

1.2 First Boot Walkthrough

This walkthrough takes you from the unpacked device to a successful first login. You will need a laptop with a LAN port, or a display and a keyboard connected to the openXEdge, and about 10 minutes.

1.2.1 Prerequisites

- openXEdge is mounted and powered
- The device's label or delivery note with its **serial number** (e.g. SN00100) and **initial password** is at hand
- A laptop with a LAN port and a browser, and a LAN cable — or a display (HDMI) and a USB keyboard connected straight to the edge

1.2.2 Step 1: Get access to the edge

Before you sign in, the edge shows its IP addresses nowhere — neither on its display nor in the browser. For the first sign-in, use a port with a fixed factory address or sign in at the device itself. Which socket is which port is shown in Edge wiring (Ch. 4.2).



1.2.2.1 Recommended: through the service port

Port 3 (Eth3) has the fixed factory address 172.16.10.250/24 and is there for exactly this purpose.

1. Connect your laptop straight to Port 3 with a LAN cable.
2. Give the laptop a fixed address in the same network, e.g. 172.16.10.10/24, without a gateway.
3. The edge is now reachable at 172.16.10.250. Continue with step 2.

Port 1 (Eth1, 172.16.9.112/24) belongs to the IO-Link master; do not connect the laptop there.

1.2.2.2 At the device: display and keyboard

Connect a display to an HDMI port and a keyboard to a USB port of the edge. After start-up the display shows the sign-in page; sign in there as described in step 2.

Keyboard layout: As delivered, the keyboard types in the layout of the language set on the edge — German from the factory. Choosing another language with the globe on the sign-in page changes only the display, not the keyboard layout. The layout can be changed only after signing in (see Choose the interface language (Ch. 2.5)). On a keyboard that is not labelled German, y, z and the hyphen of the initial password therefore sit on other keys.

1.2.2.3 Through the office network

Port 2 (Eth2) gets its address from your office network via DHCP. Which address it got is known to your DHCP server or your IT department; the edge itself shows it only after you have signed in.

Once signed in, you find the current addresses of all ports under **Settings** → **Network** — including the one Port 2 got via DHCP.

1.2.3 Step 2: Sign in with the password from the label

Open <http://<edge-ip>:5000/> in your browser — through the service port, <http://172.16.10.250:5000/>. At the edge's own display there is nothing to open. A device with a serial number needs no activation: on its first start it takes over its serial number, customer assignment and initial password by itself, even without an internet connection. The browser therefore shows the sign-in page straight away:

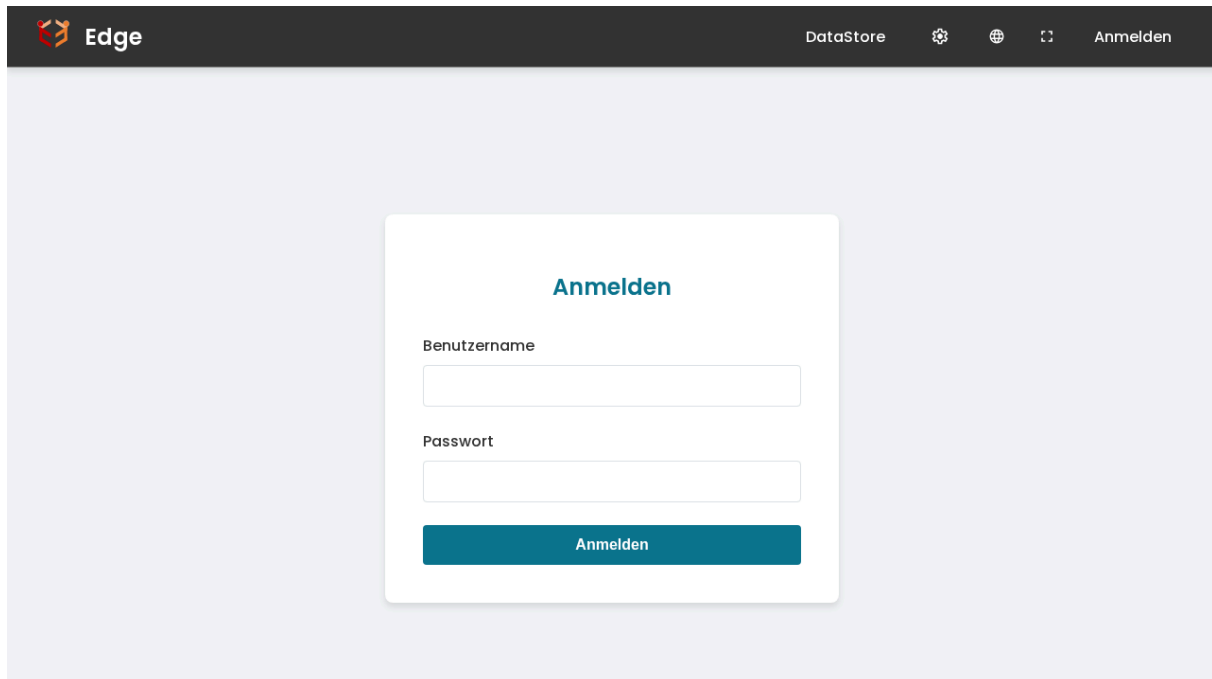


Figure 1: Brinkhaus GmbH openXEdge login page

Sign in with the username `admin` and the **initial password from the label or delivery note**. Type it exactly as printed there, hyphens included: three groups of four lowercase letters and digits. It contains only the digits 2 to 7: what looks like a 1 is a lowercase **l**, what looks like a 0 a lowercase **o**.

⚠ **Important:** the initial password cannot be worked out from the serial number — it is printed only on the label and the delivery note. Keep both as you would a key. After the first sign-in with the initial password, the device takes you straight to changing it; only with a password of your own do you get any further. The password from the label is not accepted again (see also Change password (Ch. 2.3)).

If the browser shows an activation screen instead of the sign-in page, your device was shipped without a serial number. Activate it once yourself as described under Devices without a serial number: activation (Ch. 1.2.5), then come back to step 3.

1.2.4 Step 3: The main view

After signing in you land on the **Main Functions** home page:

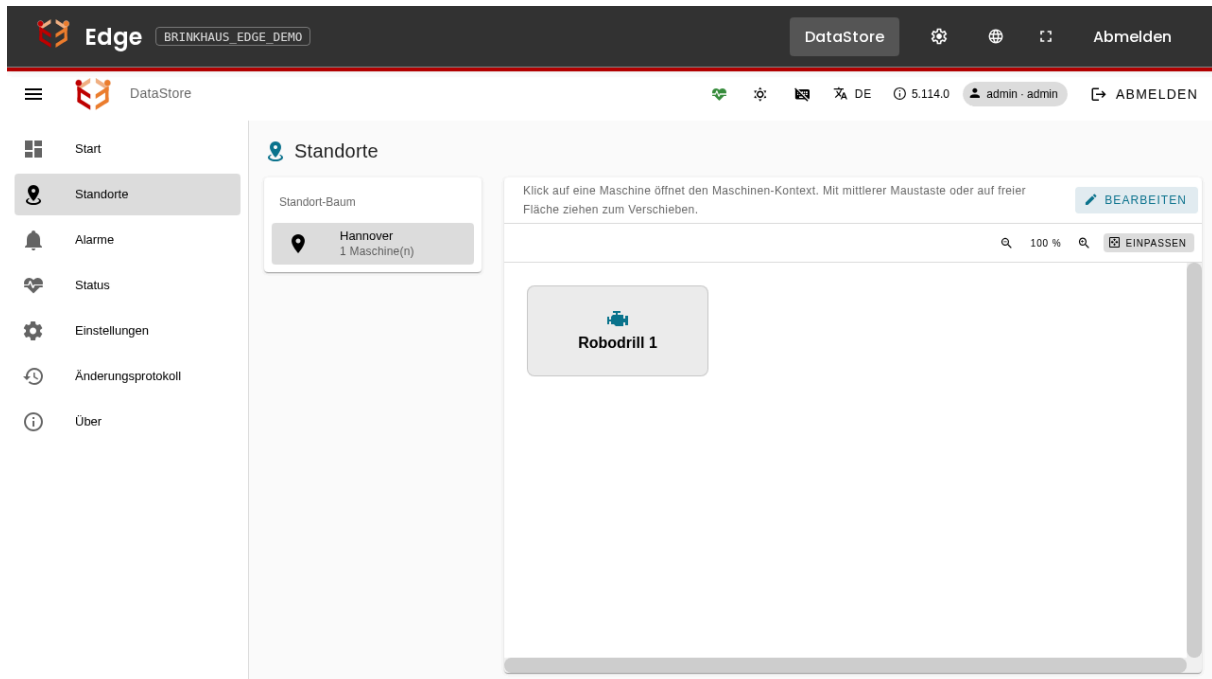


Figure 2: Main Functions home page with the five primary application tiles

The five tiles map to the five embedded applications:

- **Grafana** — dashboards and charts of collected measurements
- **IDEA4SBridge** — overview and configuration of attached IDEA-4S sensors
- **IOLink Master Configuration** — IFM IO-Link master configuration
- **DataStore** — internal database
- **AppStore** — installable extensions via FLECS

The cog icon top-right opens the settings panel.

1.2.5 Devices without a serial number: activation

Devices that were shipped without a serial number and have never been activated ask once for a machine ID the first time you open `http://<edge-ip>:5000/`. Devices that are already activated are not affected: they keep their machine ID and their password, also across firmware updates.



Geräteaktivierung

Geben Sie die Maschinen-ID dieses Geräts ein, um das Erstpasswort für alle Benutzer zu erzeugen und zu setzen.

Maschinen-ID

Gerät aktivieren

Figure 3: Brinkhaus GmbH openXEdge device-activation screen

Enter the **Machine ID** (e.g. PLANT1_M01_GMN, unique across your fleet) and click **Activate Device**. This ID identifies the device in fleet management and is also used to derive the initial password.

The initial password is then shown only once:

Aktivierung abgeschlossen

Das Gerät ist aktiviert. Ihr Erstpasswort steht unten.

Bewahren Sie dieses Passwort sicher auf – es wird nicht noch einmal angezeigt.

Benutzername: **admin**

Das Passwort wird aus der Maschinen-ID abgeleitet und kann von berechtigtem Personal bei Bedarf erneut abgeleitet werden. Sie können Ihr Passwort nach der Anmeldung jederzeit in den Einstellungen ändern.

Weiter zur Anmeldung

Figure 4: Activation Complete — one-time initial password display



△ **Important:** copy the password now. It is not shown again. The default username is `admin`.

Authorised personnel can re-derive the password from the machine ID at any time — so change it right after the first login (see Change password (Ch. 2.3)).

Click **Proceed to Login**, sign in with `admin` and the password just shown, and continue with step 3 (Ch. 1.2.4).

1.2.6 Which page the edge opens first

Out of the box the first thing you see is the overview with the tiles — unless your device was set to a particular application at the factory. On GMN devices that is **Grafana**: both the screen at the device and the browser open the dashboards first, because in day-to-day operation that is the most common reason to look at the device at all.

You can change this yourself at any time: **Settings** → **Pages** → **Start Page**. You can choose the overview or any application this device has. The setting covers both ways in at once — the screen at the device and the browser. Left on **Automatic**, the device behaves as it did before this setting existed: the screen opens the first main application, the browser the overview.

You can always get back to the overview by clicking the logo at the top left, or the device name beside it. And anyone who is not permitted to open an application still lands on the overview rather than on a refusal.

1.2.7 Next steps

- Change password (Ch. 2.3)
- Configure the network (Ch. 2.6)
- Update firmware (Ch. 2.1)
- For background: How updates work (Ch. 4.3)



2 How-to guides

2.1 Update firmware

You want to install a new firmware version on a single openXEdge.

2.1.1 Prerequisites

- You are logged in as `admin` (or any user with the settings permission)
- The edge has a working internet or at least VPN connection to `update.brinkhaus-gmbh.de`

2.1.2 Steps

1. Click the cog icon in the top-right → you land on the settings page.
2. Pick **Update** in the left sidebar.
3. You see the currently installed version on top, the versions of all running Docker services in the middle, and the available-versions list from the update server at the bottom.

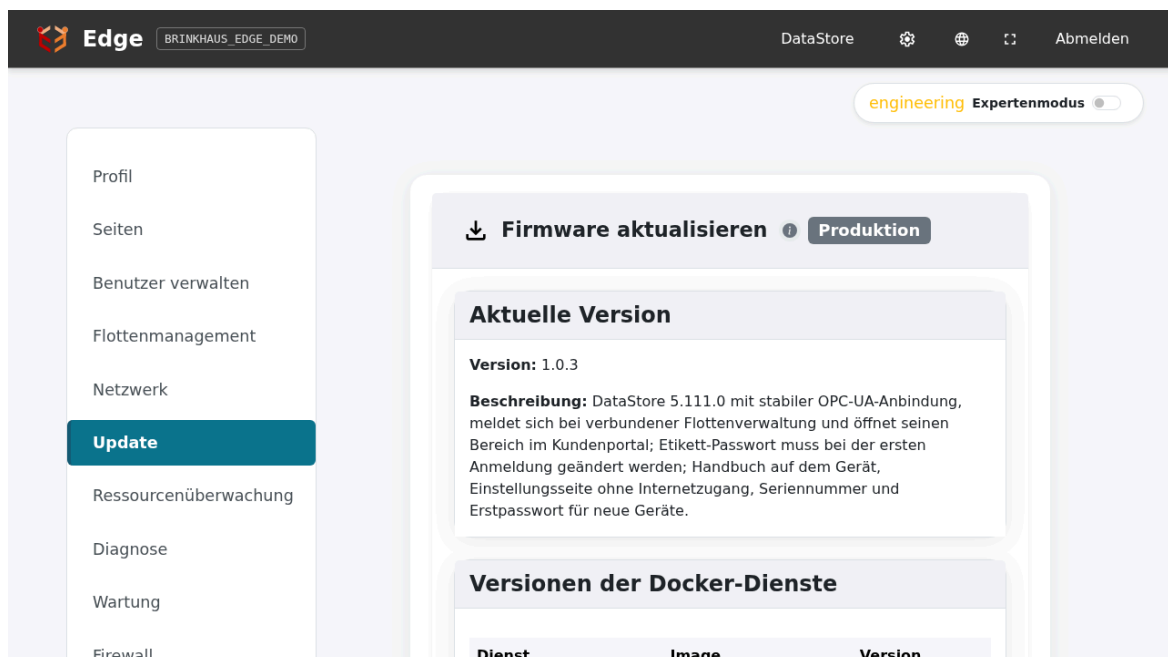


Figure 5: Settings → Update — current version, service table, available versions

4. Find the target version (typically the latest). By default the list only shows versions of the **same major version** as the installed firmware (a 2.x edge only sees 2.x versions). The “**Show all versions**” toggle in the header of the version list also reveals other major versions — however, jumps across a major-version boundary require an explicit bridge version and should only be done after consulting Brinkhaus.
5. The **Release Notes** button shows the changes of all versions of the stream; notes for versions newer than the installed firmware are visually set apart.



6. Click **Upgrade** (or **Downgrade** for older versions).
7. The edge downloads the signed compose file from the update server, verifies the Ed25519 signature, stages the files for the UpdateService, and starts the update process automatically.
8. During the update a progress screen shows the current phase (validation, signature check, stopping services, pulling images, ...). The UI is **briefly unreachable** during this. After a successful health check (typically 1–2 minutes) you are logged back in; on failure the edge automatically rolls back to the previous version — the outcome of the rollback (succeeded / failed) is also shown on the progress screen.

2.1.3 Without an internet connection (USB)

If no connection to the update server is available, a firmware version can also be installed from a USB stick (Ch. 2.2) — with the same signature verification and the same rollback behavior.

2.1.4 Remotely (FleetManager)

Firmware updates can also be triggered centrally from the FleetManager (“Install firmware version” command). The edge then downloads the selected version itself, signed, from the update server and installs it via the normal update mechanism including rollback protection.

2.1.5 Troubleshooting

- **Update stuck on “downloading”** → check the internet connection, reboot the edge if needed and retry.
- **A service stays in “rollback” after the update** → check **Settings** → **Diagnosis** for the offending service; codes are explained on Diagnosis codes (Ch. 3.1).
- **No versions are listed** → enable “Expert Mode” top-right and check that the update-server URL is correct; usually `https://update.brinkhaus-gmbh.de`.

2.1.6 Related

- How updates work (Ch. 4.3) — background on the 7-phase flow and the rollback logic
- Diagnosis codes (Ch. 3.1) — what every code in the Diagnosis panel means

2.2 Install firmware offline via USB

The openXEdge can also install firmware updates **without an internet connection** from a USB stick (available as of firmware 2.10.0). Signature verification, the progress screen, and automatic rollback behave exactly as they do for an online update.

2.2.1 What belongs on the stick

The **root directory** of the USB stick must contain:



File	Purpose
docker-compose.yml	The firmware definition of the target version
a *.sig file	Ed25519 signature of the compose file (any name with the .sig extension)
a *.pem file	Public key for the signature verification (any name with the .pem extension)
description.json	optional — version description

You receive this package from Brinkhaus or from the customer portal.

2.2.2 Steps

1. Log in on the edge and open **Settings** → **Update**.
2. Expand the “**Offline update**” section at the bottom of the page.
3. Insert the USB stick. The stick is **mounted automatically** during the scan — no manual mounting required. Detected sticks with a valid firmware package appear in the list; if multiple packages are found, the one with the highest version is preselected.
4. Start the installation. The edge verifies the Ed25519 signature **locally**; the package is only staged for the UpdateService if the signature is valid.
5. The remainder of the process is identical to an online update: progress screen with phase display, health check, and automatic rollback to the previous version on failure.

2.2.3 Troubleshooting

- **Stick is not detected** → Remove the stick, re-insert it, and open the offline-update section again; try a different stick (FAT32/exFAT) if needed.
- **“Signature invalid”** → The package was modified or belongs to a different stream. Do not install; obtain the package again. See Diagnosis codes (Ch. 3.1) (code 2008).

2.2.4 Related

- Update firmware (Ch. 2.1) — the normal online path
- How updates work (Ch. 4.3)

2.3 Change password

You want to change your own password — typically right after first-boot.

We recommend **replacing the initial password at the first login**. It is printed on the label and the delivery note (on older devices: shown at activation); anyone who gets hold of either can otherwise sign in. Devices with a serial number take you straight to the change after the first sign-in with the label password; older devices do not force it.

2.3.1 Steps

1. Click the cog icon top-right → you are in the settings.



2. Pick **Profile** in the left sidebar.
3. In the **Change Profile Details** form enter a new password and confirm it in the second field. The line under the field states what the password policy requires, by default at least 10 characters and not the username.

The screenshot shows the 'Edge' web interface. The top bar includes the 'Edge' logo, a 'BRINKHAUS_EDGE_DEMO' label, and links for 'DataStore', settings, a globe icon, a refresh icon, and 'Abmelden'. A toggle for 'engineering' and 'Expertenmodus' is visible. The left sidebar lists various settings: 'Profil' (selected), 'Seiten', 'Benutzer verwalten', 'Flottenmanagement', 'Netzwerk', 'Update', 'Ressourcenüberwachung', 'Diagnose', 'Wartung', and 'Firewall'. The main content area is titled 'Profil ändern' and contains three input fields: 'Neuer Benutzername' (placeholder: 'Neuen Benutzernamen eingeben'), 'Neues Passwort' (placeholder: 'Neues Passwort eingeben', with a note 'Mindestens 10 Zeichen, ohne den Benutzernamen.'), and 'Neues Passwort bestätigen' (placeholder: 'Neues Passwort bestätigen'). A 'Profil speichern' button is at the bottom.

Figure 6: Settings → Profile → Change Profile Details

4. Optional: also change the username.
5. Click **Save Profile Changes**.

On the next login use the (possibly new) username and the new password.

2.3.2 Notes

- If the new password does not meet the policy, the old one stays valid and the reason appears at the top. An admin sets the policy under Manage users (Ch. 2.8).
- Once you set a password of your own, the initial password no longer works for your account — neither the one from the label nor the one derived from the machine ID. You alone are responsible for it from then on.
- **What fleet management learns:** only *whether* the initial password was changed — never the password itself, neither the old nor the new one. It counts as changed only once **no** account on the device still uses the initial password from the label; if one operator changes theirs but `admin` does not, it stays “unchanged”. The fleet does not learn of the change immediately, at the latest after the next restart of the device. On devices activated with a machine ID (even with a serial number assigned later) the edge cannot tell and does not report it.
- If you lose your password, a user with `network-configuration` (or other admin) permission can set a new one in **Settings → Manage Users**.



- If access is fully lost, Brinkhaus personnel can re-derive the initial password: on devices with a serial number from the serial number and a key that is never stored on the device, on older devices from the machine ID. That only helps while some account still uses the initial password.
- If the initial password has been changed as well, the Brinkhaus service sets a **one-time password** for your account through fleet management. The device must be connected to fleet management for that. The password travels encrypted, only your device can read it. Whoever signs in with it is first asked to choose a password of their own, as with the label password; the one-time password itself is refused there.
- **From gmn-2.34.0 the machine ID is shown in the header**, next to the plant name, so you can see which system you are on. On narrow screens it is hidden. It appears only **after** you sign in, deliberately: on devices activated with a machine ID, the initial password is derived from it. On a system whose password has not been changed since commissioning, putting it on the login page would offer it to anyone who can reach the device over the network. On devices shipped with a serial number the header shows the serial number in lowercase (e.g. `sn00100`); the password cannot be derived from it alone. Devices activated with a machine ID keep showing their machine ID, even if they received a serial number later.

2.4 Access from another computer (HTTPS)

Directly on the device (kiosk screen), the user interface runs on `http://localhost:5000`. From **other computers on the network**, you can additionally reach the same interface over an encrypted connection:

```
https://<edge-ip>:5443
```

Both access paths show the same application with the same users and permissions.

2.4.1 Why HTTPS on a separate port?

Some embedded applications require what browsers call a *secure context*. That is given for `http://localhost` on the device itself, but for access via a LAN IP it is only available over HTTPS. The edge therefore provides **both** access paths (in the GMN stream as of firmware 2.1.1): HTTP on port 5000 (local/kiosk) and HTTPS on port 5443 (remote access).

2.4.2 The edge's certificate

Edges rarely have internet access, so a certificate from a public certificate authority is not an option. Instead, the edge brings its **own certificate authority**, the *edge CA*. It is created on first startup, stays the same for the life of the device, and issues the certificate for port 5443. That certificate covers all of the edge's private IP addresses; it is valid for a little over a year and the edge renews it in good time by itself, and also on its next start after an IP address has been added.



As long as your computer does not trust the edge CA, the browser shows a warning (“Your connection is not private”). You have three options:

1. **Confirm the warning** (“Advanced” → “Proceed to ...”) — enough for occasional access.
2. **Trust the edge CA once** — no more warnings after that, not even after a renewal or an IP change. See below.
3. **Install a certificate from your company CA** — if your IT runs its own certificate authority that your computers already trust. See Your company CA's certificate (Ch. 2.4.3).

2.4.2.1 Trusting the edge CA

The edge CA can **only vouch for private addresses and local names** (10.x, 172.16–31.x, 192.168.x, names ending in .local, .lan, .internal, .intranet, .intern, .corp, .home.arpa). This is written into the certificate itself and checked by the browser. Even someone who got hold of its key could not use it to impersonate a website on the internet.

1. Sign in as an administrator and open **Settings** → **HTTPS certificate**.
2. Note the **Fingerprint (SHA-256)** and click **Download edge CA**. You get the file `edge-ca.crt`.
3. Install the file on the computer as a trusted root certification authority:
 - **Windows** (applies to Edge and Chrome): double-click `edge-ca.crt` → **Install Certificate** → **Local Machine** → **Place all certificates in the following store** → **Trusted Root Certification Authorities**. Before finishing, Windows shows the fingerprint — compare it.
 - **Many computers at once**: your IT can distribute the file by group policy (*Computer Configuration* → *Policies* → *Windows Settings* → *Security Settings* → *Public Key Policies* → *Trusted Root Certification Authorities*).
 - **macOS**: open the file → keychain **System** → in the certificate under **Trust**, set “SSL” to **Always Trust**.
 - **Firefox** (its own certificate store): **Settings** → **Privacy & Security** → **View Certificates** → **Authorities** → **Import** and tick “Trust this CA to identify websites”.
4. Restart the browser and open `https://<edge-ip>:5443` — no warning.

Every edge has its own CA. With several edges, trust each one — or use a certificate from your company CA for all of them.

2.4.2.2 Host names

If you reach the edge by a name instead of its IP (such as `edge01.local` or an entry in your company's DNS), enter it under **Settings** → **HTTPS certificate** → **Host names**. Names with the local endings listed above go into the edge's certificate right away. The edge CA may not vouch for other names such as `edge01.company.com`; they only go into signing requests — for such names you need a certificate from your company CA.



2.4.3 Your company CA's certificate

If your IT runs its own certificate authority (for example Active Directory Certificate Services), you can use a certificate from it. The edge offers two ways.

2.4.3.1 Way 1: signing request (recommended)

The private key is created on the edge and never leaves it.

1. **Settings** → **HTTPS certificate** → **Your own certificate**: enter the host names (separated by commas), tick **Include the IP addresses of this edge** if needed, and enter the organization.
2. **Create signing request**, then **Download request** (edge.csr) or **Copy to clipboard**.
3. Your IT issues a **web server certificate** from it. With a Windows CA, for example:

```
certreq -submit -attrib "CertificateTemplate:WebServer" edge.csr edge.cer
```

4. On the same page, choose the file you received (.cer, .crt, .pem, or the chain as .p7b) and click **Check and install**. The edge matches the certificate to the waiting key.

While a request is open, the page shows it. **Discard request** deletes the waiting key; a certificate issued for it can then no longer be installed.

2.4.3.2 Way 2: import certificate and key

If your IT has already created certificate and key, upload both:

- **PKCS#12** (.pfx, .p12) — enter the password in the field next to it.
- **PEM** — certificate, intermediate certificates and private key, in one or several files; an encrypted key needs its password.

2.4.3.3 What the edge checks before activating

A certificate is only activated if it can work. It is **refused** if

- the private key is missing or does not belong to the certificate,
- it has expired or is not yet valid (then also check the edge's date and time),
- it is a CA certificate, names no host (*subject alternative name*), or is not meant for servers,
- the key is too weak (RSA below 2048 bits) or it is signed with SHA-1,
- the chain supplied with it does not fit together.

A **warning** — the certificate is installed nevertheless — appears if it covers neither an address nor a configured host name of the edge, an intermediate CA seems to be missing, it is valid for more than 825 days or does not state its use (Apple devices refuse the last two), or it expires in less than 30 days.

After **Check and install**, the certificate applies from the next connection; no restart is needed. Reload the page.



2.4.3.4 Which computer gets which certificate

The edge decides per connection:

- Access by a **name** your certificate lists (also via a wildcard such as *.company.com) → your certificate.
- Access by an **IP address** → your certificate only if it contains **all** IP addresses of the edge; otherwise the edge certificate. When opened by IP, the browser does not tell which address it dialled; a certificate with only one of them would cause a warning on every other port.
- anything else → the edge certificate.

If your certificate should also apply when the edge is opened by IP, tick **Include the IP addresses of this edge** in the request — or open the edge by a name the certificate lists.

2.4.3.5 Expiry and renewal

30 days before expiry, the diagnosis reports code **1012**; with fleet management connected, the message appears there too. Renew the same way as the first time (new request or import). The edge keeps serving an expired certificate: the browser warns, but you still get into the interface to install a new one.

If your certificate ever cannot be loaded, the edge automatically falls back to its own and reports **1013**. **Use the edge certificate again** removes your certificate permanently. The same code appears if the edge could not store or renew its own certificate; it then carries on with a temporary certificate and retries by itself.

2.4.4 Closing the unencrypted access

Port 5000 (HTTP) is open out of the box. To allow only encrypted access over the network, close it under **Settings** → **Firewall** — see Configure the firewall (Ch. 2.7). The kiosk screen accesses the interface locally and is not affected.

2.4.5 Multiple network ports

An openXEdge has up to three LAN ports with their own IP addresses (typically: office network, machine subnet, service port). The interface — including all embedded applications — is reachable via **every** one of these addresses; simply use the IP of the port your computer is connected to. The port assignment is described in Wiring and connections (Ch. 4.2).

2.4.6 Troubleshooting

- **Page does not load** → Are you on the right subnet? The IP addresses of all ports are shown under **Settings** → **Network** once signed in, also on the edge's own display.
- **Embedded view stays empty (only with HTTP via LAN IP)** → Use the HTTPS access path `https://<edge-ip>:5443`.



- **Warning although the edge CA is installed** → Restart the browser completely. If you reach the edge via a public IP or a name without a local ending, the edge CA cannot vouch for it; the **HTTPS certificate** page lists such addresses. Firefox manages certificates separately from Windows.
- **Warning after a firmware update from a version before the edge CA** → One time only: the edge has replaced its old self-signed certificate with one from the edge CA. Trust the edge CA as described above.

2.5 Choose the interface language

You want to see the edge's user interface in another language, or set the language it shows at the machine.

The user interface speaks 33 languages, the same as the DataStore. Out of the box it is **German**. Older firmware shows it in English only.

Two settings work together:

- **Your browser's language** is chosen in the header. It applies only to the browser you chose it in and stays there, also after you sign out.
- **The machine's default** is set by an administrator in the settings. It applies to every browser that has not chosen a language of its own, including the screen at the device.

2.5.1 Choose the language for your browser

1. In the header, click the **globe icon** at the top right. This works on the sign-in page as well.
2. Pick the language from the list. Each language is listed in its own spelling, such as *Deutsch*, *Français* or *Polski*.

The page reloads in the chosen language.

If the window is narrow and the header has collapsed into a menu (☰), the globe sits in that menu, together with the code of the current language, such as **EN**.

Other browsers and other computers are not affected: a colleague in the office can see the interface in English while the screen at the machine stays German.

2.5.2 Set the machine's default

Administrators only.

1. Click the gear icon at the top right → you are in **Settings**.
2. Choose **Pages** on the left.
3. In the **Language** card, select the language.
4. Click **Save Pages** at the bottom.



From the next page load on, the default applies to every browser that has not chosen a language of its own in the header: to the screen at the device as well as to screens signed in with a kiosk link (Ch. 2.8). Those show no globe. A browser in which a language has already been chosen keeps it, including the screen at the device if someone used the globe there.

2.5.3 Keyboard layout at the device

A keyboard plugged directly into the edge types in the layout of the machine's default language: German layout for German, US layout for English. Languages in a non-Latin script, such as Russian or Greek, get the US layout so the password can still be typed. The language of your browser in the header does not change the layout.

If the keyboard does not match the language, for example a Spanish keyboard with an English interface, set the layout explicitly. Administrators only:

1. **Settings** → **Pages** on the left.
2. In the **Language** card, choose the layout under **Keyboard layout**. Out of the box it is **Automatic (follows the language)**.
3. Click **Save Pages** at the bottom.

The change reaches the keyboard within a minute. The screen at the device goes dark for a few seconds and then shows the user interface again. If the layout cannot be set, the edge reports diagnosis 6006 and retries every minute.

2.5.4 What follows the language and what does not

All pages of the user interface switch with the language: sign-in, header, overview, settings and the notices on screen. Hebrew is shown right to left.

The DataStore follows the interface language from DataStore 5.115.0; with an older version, choose the language inside the DataStore itself. A language you choose inside the DataStore holds until the next time you open the DataStore from the user interface. It then shows the interface language again.

Grafana follows as well — its menus, buttons and time picker — in the languages Grafana knows: German, English, French, Spanish, Portuguese, Italian, Dutch, Swedish, Polish, Czech, Hungarian, Russian, Turkish, Japanese and Chinese. For every other language Grafana shows English. Dashboard contents such as panel titles and axes stay as they were made. Grafana remembers the language for your user account: open Grafana with the same account in a browser set to another language and it switches there.

These keep their own language:

- the **AppStore** and the applications installed through it,



- the **IDEA-4S bridge**,
- the configuration page of the **IO-Link master**, which the device serves itself.

The user interface does not translate **diagnosis messages and logs**: the edge's own messages stay in English in every language.

2.5.5 Notes

- If a text is still missing in a language, it appears in a related language or in English, Norwegian for example in Danish first. German is complete.
- Your browser remembers the choice for the address you opened the edge under. If you reach the same edge through another of its IP addresses, such as the service port, choose the language there again. If you clear the browser data, the machine's default applies again.

2.6 Configure the network

You want to adapt an openXEdge to your plant topology. The edge has up to three LAN ports, each independently configurable as static or DHCP.

2.6.1 Prerequisites

- You are logged in as a user with the `network-configuration` permission.
- You have the planned IPs, gateway and optionally DNS servers at hand.
- **Important:** the edge reboots after saving — plan for a brief maintenance window.

2.6.2 Steps

1. Top-right cog → Settings → **Network** in the sidebar.
2. The **Netplan Configurator** shows one block per interface (e.g. `enp1s0`, `enp2s0`) with method (DHCP / Static), address (CIDR), gateway and nameservers.

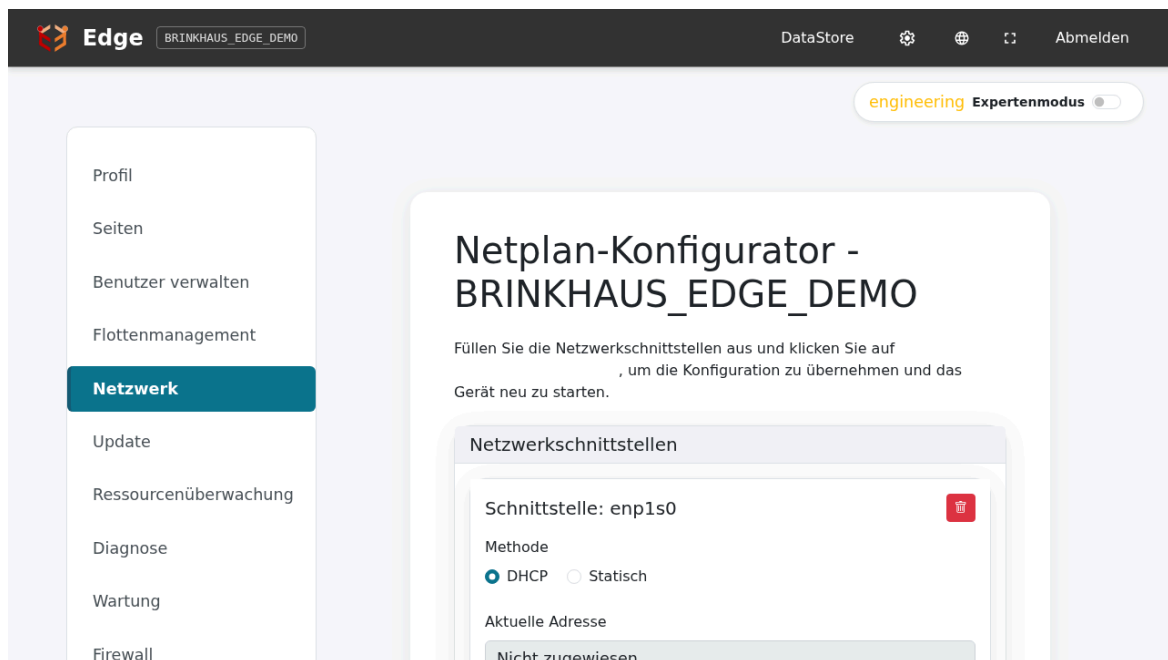


Figure 7: Settings → Network → Netplan Configurator

3. Adjust the fields:

- **DHCP:** no further fields needed.
- **Static:** address as CIDR (e.g. 192.168.10.20/24); optional gateway and nameservers.

4. Click **Save Network Configuration** — the edge applies the new config and reboots automatically.

5. After the reboot the UI is reachable on the new address.

2.6.3 Background

The openXEdge supports up to three concurrent network interfaces because it typically lives at the intersection of the plant network, a machine or sensor subnet, and an optional third network. MainUI is reachable from **every** of these IPs; the HTTPS certificate carries all of them as SANs. A dedicated explanation page on the multi-IP architecture is coming — until then contact Brinkhaus support for edge cases.

2.6.4 What if I lock myself out?

- Reconnect via another LAN port if still reachable.
- If all addresses are unknown: connect a display and a keyboard to the edge, sign in there and look under **Settings** → **Network**. Before sign-in the edge shows no addresses.
- For emergencies a Brinkhaus service technician can reset netplan via VPN or on-site.



2.7 Configure the firewall

The openXEdge accepts connections from the network only on ports that are on its allow-list. Everything else is dropped — including services that run on the device but have no business being reachable from outside: the AppStore's own interface, the ports opened by AppStore applications, the IDEA-4S bridge, the IO-Link relay and the print service that comes along with the kiosk browser. On the device itself and between its services the firewall changes nothing.

You need this page when you want to close one of the system ports from the network, or when one of your systems has to reach a port that is not open anyway — the web interface of an application from the AppStore, for instance, or the IO-Link relay for a DataStore outside the edge.

2.7.1 System ports

These are the ports the edge offers on purpose. In the delivered state they are all open; **Settings** → **Firewall** lists them under *System ports* with their purpose.

Port	Purpose	Closing
22/tcp	Maintenance access for the Brinkhaus service	with confirmation only
5000/tcp	Operator interface, unencrypted	without prompt
5443/tcp	Operator interface, encrypted	with confirmation only
1883/tcp	MQTT broker	with confirmation only

2.7.2 Close a system port

1. Sign in as an administrator and open **Settings** → **Firewall**.
2. Switch *Open from network* off in the port's row. For ports whose loss costs something, the edge names the consequence and asks you to confirm — without 22 the Brinkhaus service can no longer reach the device remotely, without 5443 there is no encrypted operation from the network, without 1883 no MQTT subscribers.
3. Click **Save and apply**.

One of the two operator-interface ports 5000 and 5443 always stays open; the edge refuses to close both at once, because it could then only be operated at its own screen. Opening never needs a prompt.

If you locked yourself out: fleet management offers the action *Firewall: reopen system ports*. It reopens every closed system port and leaves your own rules untouched; talk to your contact.

2.7.3 Open a port or a port range

1. Sign in as an administrator and open **Settings** → **Firewall**.
2. Under *Opened by you*, click **Add rule**.



3. Choose the protocol (TCP or UDP) and enter the first and the last port of the range. For a single port, leave *To port* empty.
4. Optional: restrict the rule with *Source network* to one network in CIDR notation, for example 192.168.0.0/24. Empty means: from anywhere.
5. A comment helps you recognise the rule later.
6. Click **Save and apply**. The rule takes effect immediately and survives a reboot.

To remove a rule, click the ☐ in its row and **Save and apply**.

Example: a DataStore on another machine at 192.168.0.50 is to read the IO-Link master through the edge's relay. That takes two things: the address in the relay's allow list (see Configure the IO-Link master (Ch. 2.11)) and, here, a rule TCP, port 8082, source network 192.168.0.50/32.

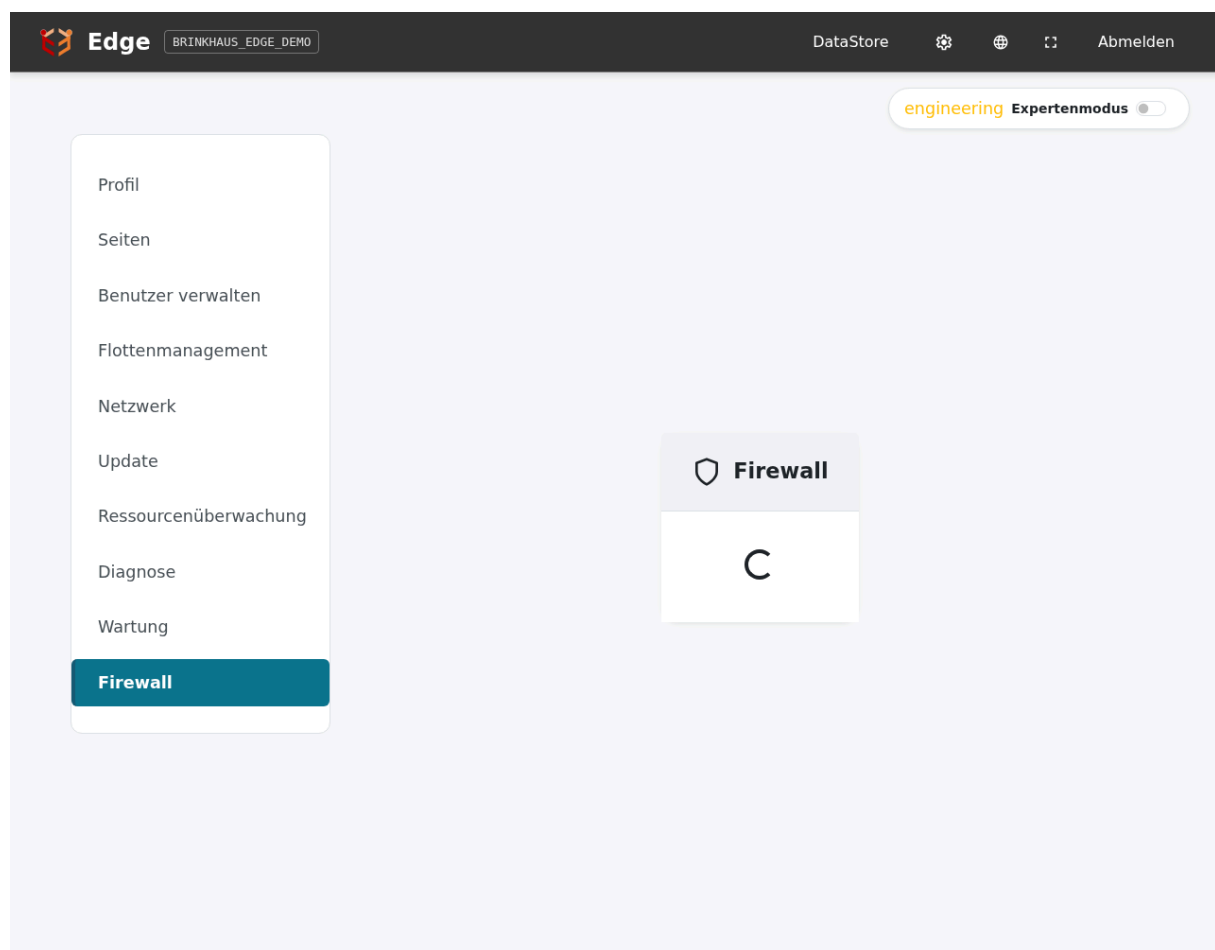


Figure 8: Settings → Firewall

2.7.4 If a rule is rejected

The edge checks every rule before it changes anything: ports have to be between 1 and 65535, the first port must not exceed the last, the source network has to be a valid CIDR expression. On an error the current allow-list stays as it is, and the message names the rule concerned.



2.7.5 Switching the firewall off

The **Firewall active** switch plus **Save and apply** turns the firewall off entirely. The edge then answers on every port again, as it did before the firewall was introduced. That is meant for troubleshooting, not for everyday operation.

2.7.6 Good to know

- The firewall's state (active, last applied, last error) is shown at the top right of the page. If applying fails, the edge also reports it in the diagnosis (code 6005) and retries on its next start.
- AppStore applications you want to reach directly on their port need a rule from this firmware on. Through the edge's operator interface they remain reachable without one, and among themselves and with the IDEA-4S bridge they keep talking without an allowance.
- If the page says the maintenance service is too old, the edge does not yet run the firmware with the firewall — and nothing is blocked yet either.

2.8 Manage users

You want to give additional people access to the openXEdge UI — typically a maintenance and a shop-floor operator account on top of the existing `admin`.

2.8.1 Prerequisites

- You are signed in as a user with the `settings` permission (the factory `admin`).
- You have decided **which areas** the new user should be allowed to see.

2.8.2 See existing accounts

1. Top-right cog → Settings → **Manage Users** in the sidebar.
2. The accounts table appears with permission columns:

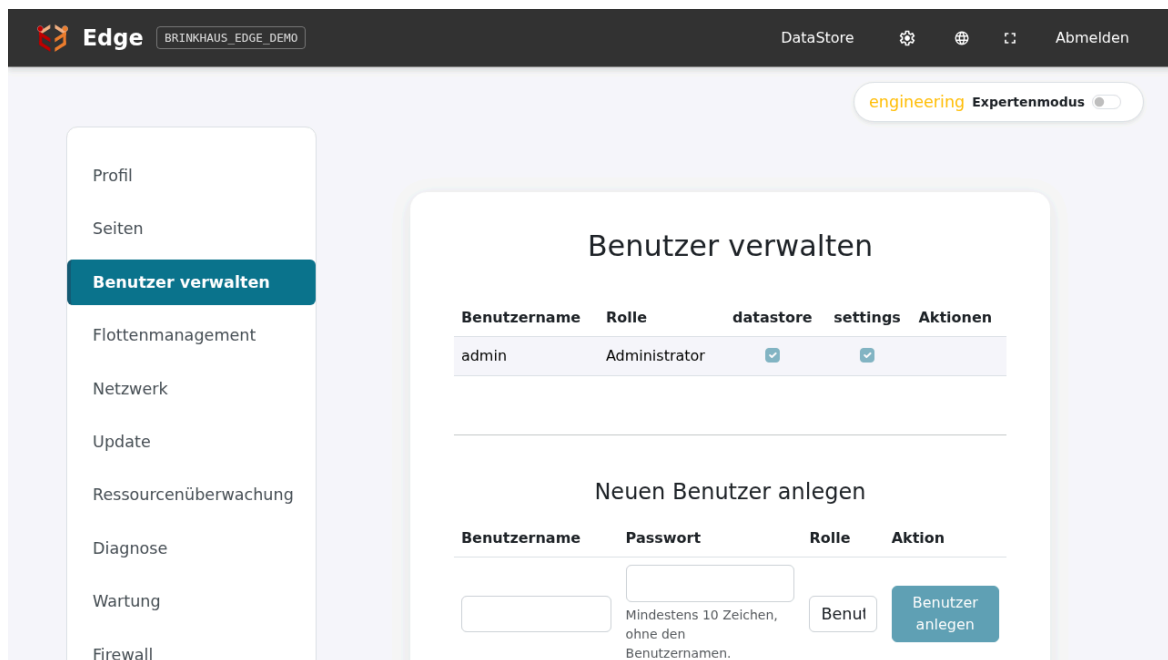


Figure 9: Settings → Manage Users with the permission table and create form

Column	Meaning
network-configuration	May change netplan (in Settings → Network) — the edge reboots on save.
grafana	Sees the Grafana tile on the home page and can open the dashboard.
idea4s-bridge	May view and modify the IDEA-4S sensor and its parameters.
datastore	Sees the DataStore tile and reaches the internal-database UI.
settings	Sees the entire settings area, including other accounts and Update.

admin has every permission by definition.

2.8.3 Create a new user

In the **Create New User** block at the bottom:

1. **Username** — free-form, unique.
2. **Password** — set initial password. The line under the field states what the password policy requires, by default at least 10 characters and not the username.
3. **Role** — User for restricted accounts, admin for full rights.
4. Click **Create User**.

The new row appears immediately. Tick the permission boxes so the person sees exactly the areas they need — e.g. a shop-floor account gets `grafana` and `idea4s-bridge` only, never `settings`.

If the password does not meet the policy, no account is created and the reason appears at the top.



2.8.4 Set the password policy

The **Password policy** block sets what a new password must meet:

Field	Meaning	Default
Minimum length	Minimum number of characters, 8 to 64	10
Character types required	How many of the four character types must appear: lower case, upper case, digits, other characters	any
Must not contain the username	The password may not contain the username	on

Save password policy applies it at once. It applies to new accounts and to every password changed from now on. Existing passwords stay valid, so nobody is locked out. The password from first commissioning and a reset by Brinkhaus staff are exempt.

Length protects better than required character types. A long phrase of several words is safer and easier to remember than a short password with special characters.

2.8.5 Change permissions

Tick or untick the boxes directly in the table — the change takes effect on the user's next page load.

2.8.6 Delete an account

Actions column → trash button. **Note:** the last remaining admin cannot be deleted — otherwise nobody could log in.

2.8.7 Kiosk link: show one app on a shop-floor monitor without a login

A wall-mounted screen should show an app such as the DataStore all day, without somebody typing a password after every restart. The **Kiosk links** block below **Create New User** is for that.

1. Click **Create link** next to the app.
2. Copy the link (**Copy**) and set it as the start page of the monitor's browser.

Whoever opens the link is signed in automatically as a **viewer** and sees **that one app only** — no navigation bar, no settings, no way to change or acknowledge anything. The DataStore opens straight in its kiosk display; its log records such sessions as user `kiosk`.

Button	Effect
Create link / New link	Creates a (new) link. The old one stops working; screens still using it land on the login page the next time they load.
Revoke	Withdraws the link.
Copy	Copies the link to the clipboard.

Notes



- The link is an access: anyone who has it sees that app's data. Hand it only to people who may see it, and create a new one if it may have leaked.
- The link shown carries the address you are signed in through right now. Every other address of the edge works the same; only the part from `/share/` on matters.
- Only apps whose service has a read-only role of its own are offered (DataStore, Grafana). The IDEA-4S bridge and the IO-Link master cannot be shared.

2.8.8 How long a login lasts

A login lasts **72 hours after the last request** and is extended by every use. A screen that runs all the time, such as a shop-floor monitor, therefore stays signed in. A forgotten browser tab signs itself out three days after it was last used. The login also survives a browser restart. Kiosk links do not expire. They stay valid until you revoke or renew them.

2.8.9 After several wrong passwords

After **five wrong passwords within five minutes**, the openXEdge accepts **no sign-in from that network address, usually that computer, for one minute**, not even with the right password. The sign-in page then shows "Too many failed attempts" and the wait. Wait that long, then sign in as usual. If five more wrong passwords follow within five minutes after the wait, it doubles each time, up to 15 minutes. A successful sign-in resets the count.

Only the network address the wrong passwords came from is blocked, never the account. Computers that reach the openXEdge through the same remote-support connection or the same router share one block. You can sign in at once on the openXEdge's own screen or from a computer with an address of its own. Restarting the openXEdge also ends the wait.

2.8.10 If you lock yourself out

- Another user with `settings` permission can reset the password in the Manage-Users table.
- Failing that, Brinkhaus personnel can re-derive the initial password (on devices with a serial number it is also printed on the label and the delivery note) — see First boot walkthrough (Ch. 1.2). It only still works for accounts whose password was never changed.

2.9 Read diagnosis

You see a symptom (no new measurement data, an update keeps failing) and want to know **which service** of the edge is responsible.

2.9.1 Steps

1. Top-right cog → Settings → **Diagnosis** in the sidebar.



- The list shows every edge service of your device (such as main-ui, datastore, postgres, update-service and — depending on the equipment — grafana, idea4sbridge, iolink-proxy, mosquito, usb-service, flecs) — each with a status dot and an **N messages** drawer:

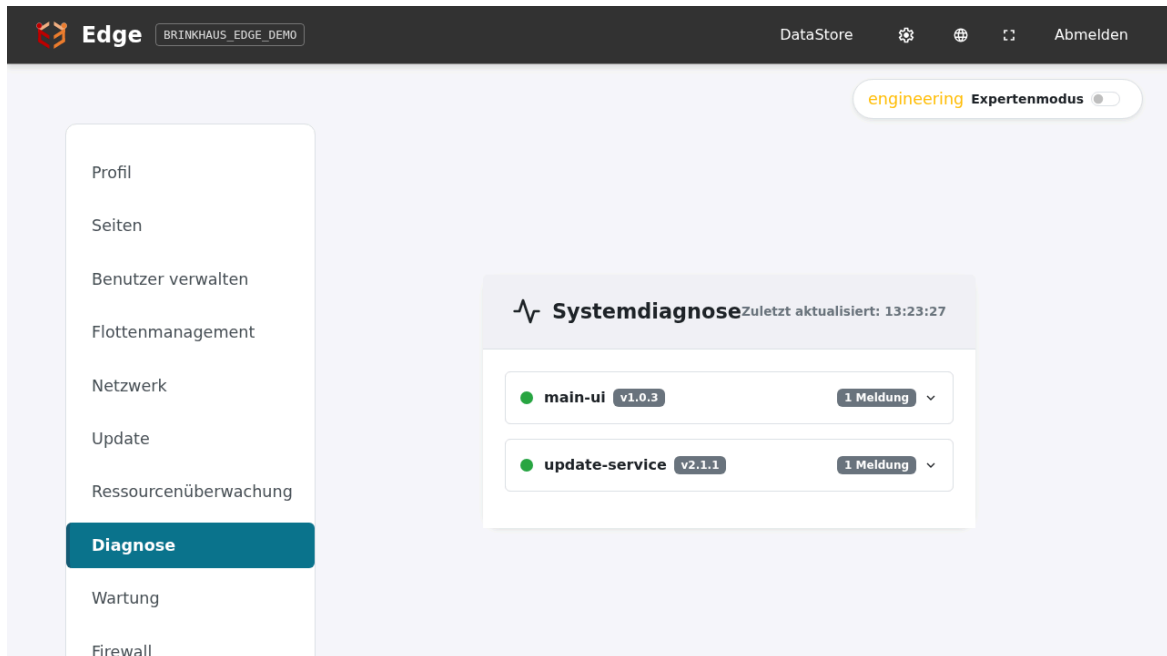


Figure 10: Settings → Diagnosis with green status dots

- Read the status:**
 - ● green → no open messages, the service considers itself healthy.
 - ● yellow → at least one warning. Service still runs, but something is off.
 - □ red → at least one error. Service may be degraded or failed.
- For any non-green dot** expand the **N messages** drawer — individual messages appear with their **code** and an explanation.
- Look the code up in the Diagnosis codes (Ch. 3.1) table — it explains the meaning and the typical action.

2.9.2 Common patterns

- **All green but Grafana has no data:** usually a data-pipeline issue below the diagnosis threshold. Check the IO-Link master (see Configure IO-Link master (Ch. 2.11)) and the MQTT subscriptions.
- **update-service red shortly after an update:** the update was rolled back — the previous state is running again; see Diagnosis codes 2xxx (Ch. 3.1).
- **datastore reports code 7002 (FleetManager not reachable):** a notice, not a fault — the DataStore keeps working. Typical for a device without internet access, or right after first install before the device is known in the fleet — see Fleet onboarding (Ch. 4.6).



2.9.3 If you're stuck

Brinkhaus personnel can read the edge's diagnosis centrally once it is connected to the FleetManager (see Fleet onboarding (Ch. 4.6)). Send the hotline the serial number (the machine ID on older devices) and the symptom; they read the codes in parallel.

2.10 Configure an IDEA-4S device

You want to inspect or maintain the IDEA-4S sensor on Port 1 of the IO-Link master — without IFM-specific tooling, directly from the openXEdge UI.

2.10.1 Prerequisites

- You are signed in as a user with the `idea4s-bridge` permission.
- The IDEA-4S is physically wired (see Edge wiring (Ch. 4.2)) and appears in the device list.

2.10.2 Steps

1. Top-right cog → Settings → **IDEA-4S Devices** in the sidebar.
2. There is one entry per attached device (e.g. **IDEA-4S 0**). Pick the matching one.
3. The value list loads all parameters from the sensor ("Loading values: x/y", with the section being read named in front of it on larger devices). Depending on the device this takes half a minute to a minute — longer while something else is talking to the sensor. Below that a five-tab carousel:

Figure 11: Settings → IDEA-4S Devices → IDEA-4S 0 → Identification

Tab	Content	Editable?
Identification	Vendor, product name, serial number, IDTA Nameplate fields.	Read-only but for one field. Application Specific Tag is the freely chosen device name and is writable



Tab	Content	Editable?
		from gmn-2.30.0 on (32 characters, from gmn-2.33.0 as an administrator only); the remaining fields mirror the sensor's factory data set and only the electro-mounting station can change them.
Parameter	Measurement, threshold and configuration values — the main area for adjustments.	Yes , per field — from gmn-2.33.0 as an administrator only.
Diagnosis	Lifetime, error counters, temperature windows, technical properties.	Read-only.
Other	Reserved for future IODD extensions.	Empty on current firmware.
Factory settings	The sensor's factory data set — what it returns to when factory settings are restored. It mirrors nearly every operating parameter under the same name; up to gmn-2.27.2 these fields were scattered across the other tabs and read as duplicates there.	From gmn-2.33.0 for administrators , see below. Before that, for nobody.

Which value sits in which tab is decided by the sensor, not by the edge: its device description declares the three areas *Identification*, *Parameter* and *Diagnosis* itself, and from gmn-2.32.0 on the view follows that declaration. Before then the edge inferred it from the field names — on the test device that put 347 of 920 rows in the wrong tab and scattered coherent areas such as *Temperature Bearing 1* across all three. **If you find values somewhere other than you are used to, this is why.** The layout now follows the same source as the analysis tool ifm moneo, which GMN supplied as the reference: the device description itself.

2.10.2.1 The columns

Column	Meaning
Status	Traffic light: read, changed (not yet written), or not read.
Name	Name from the device description; the indentation shows the structure.
Value	The value in the sensor. Editable fields are input boxes, with ↓ to re-read and ↑ to write. Commands appear here as buttons (see below).
Range	Permitted range in the same unit as the value, e.g. 0.00 - 19.60 mm/s. For text fields, the number of characters. From gmn-2.32.0.
Description	Explanation from the device description. From gmn-2.32.0.



On narrow screens **Description** is hidden and then appears in the row tooltip, together with the default value from the device description, the path, the identifier and the address. **Up to gmn-2.32.0** the table had two further columns, *Default* and *Type*; the default value is now only in the tooltip.

2.10.2.2 Commands are buttons

From gmn-2.33.0, visible to administrators. Some rows carry no input box but a row of buttons — *Store Factory Settings*, *Service Reset*, *Reset Error Memory* in the **Factory settings** tab, or *Application Reset*, *Restore Factory Settings* and *Back-to-Box* in **Diagnosis**. These are not values but commands: a click fires the named action in the sensor, without a confirmation. What a button does is in its tooltip. Which rows are drawn this way is decided by the device description.

Back-to-Box inhibits the sensor's communication until the next power cycle. It is only reachable again once it has been without power — at the machine, not remotely.

Whether the command arrived is shown on its row (from gmn-2.34.0): the traffic light turns green when the device accepted the command and red when it refused. A few words below the buttons say which — *"Refused by the device (code 531)"* — and the full sentence, including what to do about it, appears when you hover that short text or the traffic light. The banner in the top right clears itself after a few seconds; what is on the row stays. The usual reason for code 531 is a factory password that is unset or wrong.

2.10.2.3 Operator role

Above the tabs you can choose the IO-Link operator role — *Observer*, *Maintenance* or *Specialist*, as far as the device description declares them. Each role opens a different set of fields; *Observer* shows the fewest. *Maintenance* is preselected: the set this page has always shown, so anyone who changes nothing keeps the list they know.

The selector exists from gmn-2.39.0. Before that it was never visible — the page asked for the available roles at an address that did not exist and hid the box in response. The earlier note that the selection takes effect from gmn-2.31.0 was about passing the role on to the device, not about the box.

From gmn-2.39.0 the values shown belong to the selected role as well. Each role numbers its rows for itself, and until then every value was read in the *Maintenance* numbering. Under *Observer* about half the rows would therefore have carried another parameter's value — with no error, because such a value looks exactly like the right one.

2.10.3 When the load has finished

A result line closes the run, for example **"All 760 values read. 13 of them are empty — the device answered and holds no value there."** or, when something really is missing, **"x of y values read — z could not be read."** How large y is depends on the sensor; the test rig carries 760 rows.

Three states have to be told apart, and from gmn-2.31.0 the interface shows them apart:



What you see	What it means
A value, green light	Read.
An empty field , green light	Read — the sensor holds nothing at that address. This covers fields that were never filled at commissioning: manufacturer name, country of origin, company, installation site, machine number, install and de-install date. Not a fault.
not read , red light	Not read. The sensor did not answer for that address.

Up to gmn-2.30.0 the second row also read **not read** with a red light, and the result line counted those fields as losses — 13 of 760 on a typical device. Anyone who went looking for a fault after that was looking for something that was not there.

If fields stay red, press “**Read missing values again**” — only the missing ones are asked for. If the same fields stay red, this device does not deliver them.

2.10.4 Which fields can I change?

From gmn-2.33.0 only an administrator changes values — the whole view, not single tabs. Anyone else sees a note above the list, every field read-only and no command buttons. The commands are the reason: *Back-to-Box* takes the sensor out of service until the machine is next powered off, and the sensor asks nothing first.

Not every field is active for an administrator either. The badge next to the name says what the sensor states about it:

Badge	Meaning
Read-only	The sensor does not offer this field for writing — a property of the sensor, not of the edge.
Write-only	The field accepts a value but never hands it back. It therefore stays empty, and its traffic light is grey.

Editable fields show an active input and a save/write arrow on the right.

2.10.4.1 Changing the factory data set

From gmn-2.33.0, administrators only. The **Factory settings** tab holds what the sensor returns to when factory settings are restored. Up to gmn-2.32.0 it was locked.

Values in this tab are accepted straight away — the sensor asks for no password. Measured on the test device (ADVANCED 1.0.1.5): writing a factory value is confirmed at once.

Commands in this tab are another matter. *Store Factory Settings*, *Service Reset* and *Reset Error Memory* are refused while the sensor’s factory password is unset — the message then names device code 531. Enter the password in the **FactoryPassword** field of the same tab and write it with ↑; the



sensor then carries the commands out. The Brinkhaus service supplies it; it is deliberately not printed here.

What stands here is the sensor's fallback state. A change survives every "restore factory settings" and every restore — a backup **cannot** undo it, because a restore deliberately leaves this area alone.

- If you're unsure whether a change is safe, take a **Backup** (see below) before changing — you can restore at any time.

2.10.5 Backup and restore

Top-right of the IDEA-4S page two buttons:

- **Backup** — reads every parameter from the sensor once more and downloads them as a JSON file. Filename e.g. `idea4s_device_0_backup.json`. This takes about a minute; you may start it while the value list above is still loading — both talk to the same device and then take longer.
- **Restore** (*administrators only*) — writes a previously-downloaded JSON file back to the device. It writes the operating settings; the factory data set is left alone. The values survive a power cycle of the sensor: it stores what is written to it by itself, so no extra saving step is needed. The sensor's factory data set is left alone — a later "restore factory settings" still returns it to its delivery state (up to gmn-2.27.1 that was not the case, see the release notes for 2.27.2).

The factory data set stays out of backup and restore, and gmn-2.33.0 does not change that. It can only be changed field by field (see above), and so it can only be put back field by field.

A backup is either complete or there is no file. If a parameter could not be read even after a retry, the interface says so with numbers and downloads nothing — try again in that case. The success message names what is in the file, e.g. "700 values read, 62 not delivered by the device": the second number are parameters this device never delivers. They are listed by name in the file, so two backups of the same sensor can be compared.

△ Restore overwrites **every** field in the backup with the value it carried at the time. Always reuse a backup taken from the **same** sensor type and firmware.

△ Backup files from firmware older than gmn-2.26.0 may contain gaps that were not visible at the time. Restore refuses them and names how many parameters are missing. You can still write the rest — the prompt says exactly how many parameters would keep their current value. A fresh backup is the better answer.

2.10.6 Loading a new IODD

The whole parameter list — which fields exist, what they are called, their unit and their limits — comes from the **IODD**, the sensor's device description file. The edge ships with the IODDs that were known



when it was built. A sensor on a newer firmware level is not described there: it does not appear in the device list at all, and its measurements are missing from the DataStore.

From gmn-2.31.0 you load the matching IODD yourself, without a firmware update:

1. Gear icon → Settings → **IDEA-4S Devices** → the device in question.
2. Top right, **Upload IODD**.
3. Pick the file. Either works: the single `...-IODD1.1.xml`, or **GMN's complete ZIP package** — only the device descriptions are taken from it, not the images or firmware files.
4. Confirm. The file goes to the IDEA-4S bridge **and** to the DataStore; the bridge then restarts and the parameter list reloads.

Uploaded IODDs shows what is loaded and lets you remove it again — the built-in description then applies once more.

⚠ Do not start an upload while a backup is running: the bridge restart cuts it off.

An uploaded IODD **displaces** the built-in one for the same device and firmware level. A wrong file therefore makes the parameter list unusable — but **Remove** undoes it at any time.

If everything ends up in the **Parameter** tab after an upload and *Identification* and *Diagnosis* are empty, the uploaded file does not declare the three areas (`RoleMenuSet`). Every description GMN ships does; a file from elsewhere need not. The values are all there and in the right order, just not spread across the tabs.

Administrators only.

2.10.7 The start page: which sensors are shown

Under **IDEA4SBridge** the edge shows one card per sensor with the current value, the observed range, the alarm and fault thresholds and the exceedance counters. **Which cards exist is decided by the sensor's device description (IODD)**: every channel it gives statistics or thresholds for gets one. On the IDEA-4S ADVANCED that adds displacement and displacement temperature, on the ADVANCED ENC the encoder channels (air gap, vRMS, aPeak, encoder temperature, vibration and speed).

The **Sensors** button in the bar at the top picks which cards appear; **Save** stores the choice. It applies **to this edge**: the kiosk screen and every office browser show the same cards. Until something is chosen, every card is shown except channels switched off in the sensor. How many cards are hidden is shown below the cards and on the button.

2.10.8 If a field is missing

The split into **Identification / Parameter / Diagnosis** is derived automatically from the sensor's IODD. If a field is missing or in the "wrong" tab, the built-in IODD does not match the sensor's firmware level



— load the IODD that belongs to the device (see above). If that does not help, contact Brinkhaus support with the device type and FW level (visible on the Identification tab).

2.11 Configure the IO-Link master

You want to choose **which** sensor values the IO-Link master actively publishes via MQTT (or delete existing subscriptions). The openXEdge embeds the IFM device's configuration UI directly — no cable swap, no second tool.

2.11.1 What is embedded here?

Click the **IOLink Master Configuration** tile on the home page and the openXEdge loads `/web/subscribe` from the **ifm IoT Core** firmware of your IO-Link master (example device: AL1304, FW 2.6.x). That is the IFM device's standard **Notification** page:

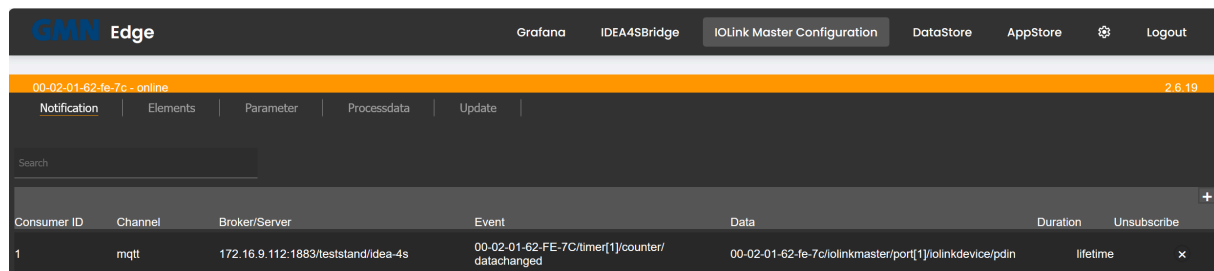


Figure 12: ifm IoT Core — Notification page with an MQTT subscription

The tabs above (Notification, Elements, Parameter, Processdata, Update) are native ifm-IoT-Core tabs — the openXEdge shows them 1:1; every action affects the IO-Link master directly.

2.11.2 Create an MQTT subscription

On the **Notification** page click the **+** in the top-right to add a new row, then per subscription:

Field	Meaning
Channel	Transport — typically <code>mqtt</code> .
Broker/Server	Address + port + topic prefix of the MQTT broker. The openXEdge itself runs Mosquitto on port 1883 with no auth. Example: <code>172.16.9.112:1883/teststand/idea-4s</code> .
Event	The event on the master or device that triggers a publish — e.g. <code>00-02-01-62-FE-7C/timer[1]/counter/datachanged</code> for every tick of an internal timer.
Data	Which data points are included — e.g. <code>00-02-01-62-fe-7c/iolinkmaster/port[1]/iolinkdevice/pdin</code> for process-data-in of the sensor on Port 1.
Duration	<code>lifetime</code> (stays until deleted) or a time limit.

The configuration is stored **inside the IFM device**, not on the openXEdge. The device keeps the subscriptions across openXEdge reboots; they are part of the “ports in the device” and survive a power cycle.



2.11.3 Delete a subscription

Unsubscribe column → click the ✕. The row disappears and the IFM device stops publishing.

2.11.4 Let a system outside the edge read the master

A DataStore that does not run on this edge needs two things to show the sensor as a machine: the live values from the edge's MQTT broker, and the master itself over HTTP JSON-RPC. The second one is closed by default — the edge relays the master on host port **8082**, but only lets through its own UI and the addresses you name.

Add them on the edge, in the settings volume, as `/home/gmn-service/docker/data/web-ui/settings/ioLink_master.json`:

```
{
  "host": "172.16.9.110",
  "port": 80,
  "allow_from": ["172.16.0.229"]
}
```

`host/port` are the master's address (they may be omitted if it sits at the factory default `172.16.9.110:80`); `allow_from` takes single addresses or whole ranges in CIDR form. Then restart the relay: `sudo docker restart docker-iolink-proxy-1`. The file survives firmware updates.

The reader is then pointed at `<edge address>:8082` instead of the master's own address.

The reader also needs the IODD. The edge carries any supplied IODD files for its own acquisition; a DataStore elsewhere gets nothing from that. Without the one matching the sensor's DeviceID it decodes **no** measurement at all, even though the data visibly flows — for an IDEA-4S *Basic* that is the normal case, because no Basic revision ships with DataStore. Load the same IODD there. Everything not on the list is refused with 403 and reported as diagnosis code **3004**, which names the address that was turned away — so a missing entry does not look like a dead cable.

One reader at a time. The IO-Link master answers exactly one viewer; an outside reader shares that with this configuration page, the backup and the edge's own DataStore.

Testing from the edge itself does not work through this port — a request from the edge's own shell reaches the relay wearing an internal address and is refused, exactly like any other host that is not on the list. That is deliberate. Test from the machine that is meant to read, or use this page.

2.11.5 When do you need this?

- First time you set up an edge: create the subscription for the IDEA-4S sensor once, so data reaches DataStore and Grafana.



- When the **Grafana dashboard is empty**: check whether the subscription still exists (some IFM firmware updates clear the list). If yes, check the state; if no, recreate it.
- When you want to forward additional signals — e.g. diagnostic values of the IO-Link master itself.

2.11.6 Notes

- The ifm IoT Core UI is served by the master directly. If it doesn't appear, the master's LAN or power is usually faulty. The openXEdge reports that in **Settings** → **Diagnosis** under `iolink-proxy` with code 3001 (see Diagnosis codes (Ch. 3.1)).
- For exhaustive documentation of the individual IFM fields refer to the **ifm IoT Core** manual for your master model — the openXEdge docs focus on the parts that concern the edge.

2.12 Export measurement data to Excel

You want to work through a stretch of measurements in Excel — to check a run-up, or to hand a recording to someone else. **Every** Grafana panel hands out its data as CSV; the work is in the Excel import afterwards.

2.12.1 1. Pick the time range first

Set the time range top-right **before** you export. What you get is exactly what the panel currently shows.

Keep it short. The IDEA-4S signals add up to tens of thousands of values per hour — the database delivers that in a fraction of a second, but rendering the table in the browser costs the edge noticeable time. For a whole day, export several hours one after another.

2.12.2 2. Download the CSV

1. Click the three dots at the top right of the panel.
2. Choose **Inspect** → **Data**.
3. Under **Data options**, turn on **Download for Excel**.
4. Click **Download CSV**.

That switch is what makes the file open cleanly: Grafana then writes a separator hint into the first line, which Excel reads when opening the file.

2.12.3 3. Import into Excel

Open Excel with an **empty** worksheet and pull the file in via **Data** → **From Text/CSV** — not by double-clicking the file.

In the *Transform Data* window, watch two things:

- **Delimiter** must be comma.



- The **Changed Type** step on the right under *Applied Steps* guesses column types from the locale. Grafana writes numbers with a decimal **point**; an Excel set to a decimal comma therefore guesses wrong and turns 12.5 into a date or into 125. Delete that step with the cross; every column then arrives as text and you set the types yourself.

2.12.4 4. The time axis

Which columns you get depends on the panel you exported. The time-series panels of the delivered dashboard give you a **time** column with date and time plus one column per curve (e.g. `value_temperature_bearing_1`). Those you can use directly: type the column as date/time and you are done.

Some hand-built table panels hand out the time as a **number** instead — seconds since 1 Jan 1970. Turn it into a date axis in a new column (time column in B here):

```
=B2/86400 + DATE(1970,1,1)
```

Or into a **relative axis** in seconds from the start of the recording — usually the better choice for a run-up:

```
=B2-$B$2
```

2.12.5 5. The chart

Use a **scatter (XY) chart with lines**, not a line chart: a line chart treats the timestamps as evenly spaced labels and distorts every gap in the recording. Then right-click the X axis → **Format Axis** → **Number**, clear *Linked to source*, and enter the format you want.

2.12.6 Why some cells stay empty

When a panel folds several signals into one table, gaps show up. The signals do not arrive at the same rate — the sensor reports **on change**, not on a fixed cycle. Measured on an edge over two hours (gap between consecutive values, median): vibration velocity 0.1 s, bearing and coolant temperatures 0.2 s, rotational speed 30 s with the spindle idle. In the rows in between, the slower column stays empty. That is not a gap in the recording. For a continuous curve, filter in Excel on the rows where the column is populated.



3 Reference

3.1 Diagnosis codes

All edge services emit structured diagnosis messages into a central panel (**Settings** → **Diagnosis**). Each message carries a four-digit code.

Range	Service	Codes
1xxx	MainUI	1001–1099
2xxx	UpdateService	2001–2099
3xxx	IOLinkMasterProxy	3001–3099
4xxx	USBService	4001–4099
7xxx	Fleet connection — reported from any service that uses it	7000–7999
—	DataStore	1000–2504, see below

The number alone is not enough. The DataStore brings some 150 codes of its own, and their numbers **overlap** with those of MainUI and the UpdateService. What settles it is the **service name** the message appears under in the diagnosis panel, not the digits.

3.1.1 MainUI (1xxx)

Code	Meaning	Typical action
1001	Update server unreachable	Check the edge's internet / VPN.
1002	IDEA4S interface unreachable	Check the IDEA4S-Bridge service (diagnosis detail); restart the edge if needed.
1003	Netplan apply failed	Re-check the IP config you entered, re-boot.
1004	Config file corrupt	Call a service technician — edge falls back to defaults.
1005	Docker socket unreachable	Reboot; if it persists, service technician.
1006	Service URL unreachable	Which URL is shown in the diagnosis detail.
1007	Container unhealthy	Check that service's diagnosis tab.
1008	Docker command failed	Service technician.
1009	Update signature invalid	Do not install — contact Brinkhaus support.
1010	Update server key does not match the pinned one	The update server delivered a different signing key from the one the edge knows, without valid proof of a key change. The update was not downloaded; the running



Code	Meaning	Typical action
		version is unchanged. Do not retry — contact Brinkhaus support.
1011	UpdateService update refused: image from a source that is not allowed	The new version of the UpdateService named a container image from a source this edge does not accept; it was not installed and the current UpdateService keeps running. Contact Brinkhaus support.
1012	Own HTTPS certificate expires soon or has expired	Install a renewed certificate — see Remote access (HTTPS) (Ch. 2.4.3.5).
1013	HTTPS certificate not usable	If the message names your own certificate : the edge uses its edge certificate instead; reinstall or remove yours under Settings → HTTPS certificate . If it names a temporary certificate , a failed renewal or the HTTPS start: the edge retries by itself; if the message stays, call a service technician.

3.1.2 UpdateService (2xxx)

Code	Meaning	Typical action
2001	Update directory missing	Service technician.
2002	Pre-update backup failed	Check disk space, retry.
2003	<code>docker compose up</code> failed	Check diagnosis detail, possibly perform roll-back.
2004	Post-update health check failed	Update is rolled back automatically — check logs.
2005	Rollback initiated	Informational — no action needed.
2006	Rollback succeeded	Informational — edge is back up.
2007	Rollback failed	Service technician immediately.
2008	Update signature verification failed	Do not install — contact support.
2009	Signature check skipped (legacy 1.x update)	Informational — only occurs while migrating 1.x edges; from 2.x on, signature verification is always enforced.
2010	Update images missing on the device	The message names them: they could not be pulled and are not on the device either, so the update was not started; an edge already running a version returns to it (see 2005–2007). Check the edge's access to the registry and trigger the update again.
2011	Update rejected: image from an unaccepted source	The update named a container image from a repository this edge does not accept; nothing was installed and the running version is un-



Code	Meaning	Typical action
		touched. Do not retry with the same package — contact support: either the release is wrong or someone tampered with it.

3.1.3 IOLinkMasterProxy (3xxx)

Code	Meaning	Typical action
3001	IO-Link master unreachable	Check the LAN cable to the IFM master, reboot the IFM device.
3002	High error rate while proxying	IFM master or network has issues — check logs.
3003	HTTP error from IO-Link master	Check the IFM configuration.
3004	Connection to the IO-Link master relay refused	A host tried to read the IO-Link master and is not permitted to. Intended, unless it is a reader you set up — then add its address to <code>allow_from</code> in the master configuration file on the edge.

3.1.4 USBService (4xxx)

Code	Meaning	Typical action
4001	USB mount failed	Re-insert the stick; try a different stick.
4002	File transfer failed	Re-insert the stick.
4003	MainUI unreachable	The edge itself has a problem — see codes 1xxx.
4004	USB detected but no device	Re-insert the stick.
4005	CSV files pending transfer	Insert a USB stick.
4006	Container restarting	Informational.
4007	No USB with files to copy	Informational.
4008	Last copy succeeded	Informational.

3.1.5 DataStore

If your edge runs a **DataStore**, its own codes come on top. The full list is in the DataStore's own handbook, available from Brinkhaus service; the three that turn up in everyday use are listed here. All three concern **retention** — how long the edge keeps its measurements. The message text in the diagnosis panel names the data set concerned.

Code	Meaning	Usual action
1513	The automatic clean-up cannot keep up — more arrives than it clears.	Check the retention limits (DataStore → Settings → Behavior parameters → <i>Retention</i>); if it persists, inform Brinkhaus service.



Code	Meaning	Usual action
1517	Note (not a fault): after an update, the existing data is classified once.	None. On large edges this takes hours; until then the clean-up only clears measurements it has already classified.
1522	Emergency stop: the edge has halted data recording because a data set reached its emergency level — usually after a size limit was set too low.	Adjust the limit in the DataStore, or wait until the clean-up is done. The message then stays up until a “ small restart ” in the DataStore interface acknowledges it.

3.1.6 Where can I see the codes?

In **Settings** → **Diagnosis** expand the panel per service to see individual messages with their codes and descriptions:

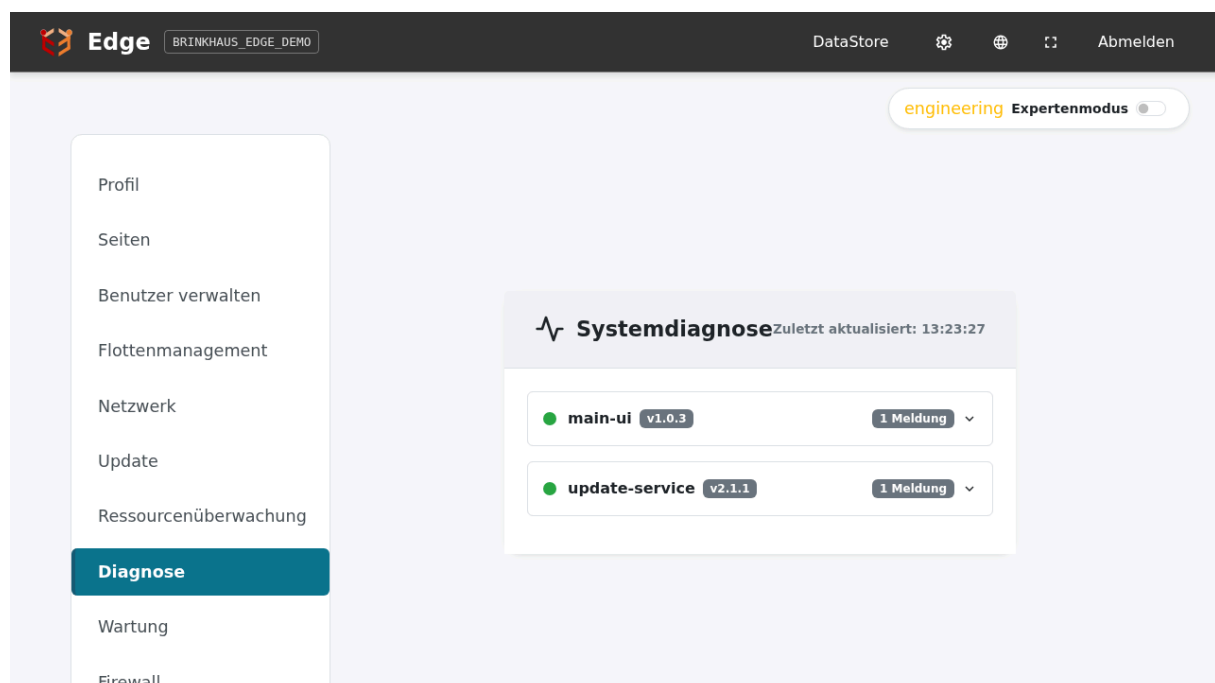


Figure 13: System-Diagnosis panel with green status dots and version badges

Via the fleet integration the same codes are also visible centrally in the FleetManager — a dedicated explanation page is coming.

3.2 IDEA-4S – signal names in the DataStore

When you build your own Grafana panel, you query the `historicValues` table for a `signal_name`. If the name does not match, the panel stays **empty** — **with no error**. This page lists the names as they actually appear in the database on a GMN edge.

3.2.1 Measured values

These ten signals hold a number:



Signal name	Quantity
VibVeloXDirection	Effective vibration velocity, X axis
VibVeloYDirection	Effective vibration velocity, Y axis
VibVeloZDirection	Effective vibration velocity, Z axis
TempBearing1 ... TempBearing4	Bearing temperatures 1 to 4
TempCoolantInlet	Coolant inlet temperature
RotSpeed	Rotational speed
operatingHours	Operating time as a raw counter , not in hours

Two names cause most of the trouble:

- Rotational speed is **RotSpeed**, not **Speed**. A query for **Speed** returns nothing and looks exactly like a machine without a speed signal.
- **operatingHours** counts in steps of roughly a tenth of a second. The DataStore tile converts it to hours using the device constant from the IODD; in your own query you have to do that yourself.

3.2.2 Status signals

Most measured values have a companion signal with a Status Suffix (RotSpeedStatus, TempBearing1Status, ...), plus DeviceStatus, ClampingStatus, DisplacementStatus, DisplacementTempStatus, DrawbarPositionStatus, HydraulicPiston and ReleaseStroke.

These hold **an object, not a number**. That is why every query of your own needs the line

```
AND jsonb_typeof(hv.value) = 'number'
```

Without it the query aborts as soon as one such value falls into the selection — invalid input syntax for type double precision.

3.2.3 Histogram classes

The remaining 51 signals (wearEdge..., wearTime...) are the classes of the dwell-time histograms, numbered per axis. The histogram tiles evaluate them; they are not meant for time-series panels of your own.

3.2.4 Matching the machine

Every signal hangs off the imported IDEA-4S machine, whose id is not fixed — it changes when the machine is created again. Query it rather than writing a number:

```
WHERE hv.machine_id = (SELECT id FROM "machines"
                       WHERE import_type = 'idea4s' ORDER BY id LIMIT 1)
```

ORDER BY id LIMIT 1 is not decoration: with more than one IDEA-4S machine in the DataStore — after a re-import, say — the query fails without it.



4 Background

4.1 The device

The openXEdge consists of two parts: a fanless industrial PC for the control cabinet and the firmware running on it. The firmware keeps itself up to date (see How updates work (Ch. 4.3)); the PC stays the same.

4.1.1 What the openXEdge is for

The openXEdge is the platform for applications at the machine: it brings the user interface, the updates, the diagnosis and the link to fleet management. Which applications run on an edge depends on its edition; the handbooks of the individual editions describe them.

4.1.2 The industrial PC

The openXEdge ships on the **NET-III 2I640DW** embedded computer by LEX COMPUTECH, in the version with an Intel Atom processor (-E13).

4.1.2.1 Technical data

Manufacturer, model, processor, memory and storage as delivered, the other values from the manufacturer's data sheet.

Property	Value
Manufacturer	LEX COMPUTECH Co., Ltd. (Taiwan)
Model	NET-III 2I640DW-E13, fanless embedded computer
Processor	Intel Atom x6413E (Elkhart Lake), four cores, 2.7 GHz
Memory	8 GB DDR4 (one SODIMM slot, up to 32 GB)
Storage	128 GB, M.2
Security chip	TPM 2.0
Network	3 × 2.5 Gbit/s Ethernet (Intel I225 or I226, depending on the batch)
USB	2 × USB 3.0
Display	2 × HDMI
Serial	2 × RS-232/422/485 (COM)
Power supply	9–24 V DC through a two-pole terminal, alternatively an external 100–240 V AC adapter
Dimensions	135 × 110 × 35 mm, with the DIN-rail bracket 142.45 mm high and 40 mm wide
Weight	0.75 kg
Mounting	DIN rail (bracket with 3 × M4) or flat through 4 × M4 on a 75 × 75 mm pattern
Operating temperature	–20 to +60 °C at full processor load (manufacturer's figure) ¹



Property	Value
Storage temperature	–20 to +70 °C
Humidity	up to 95 % at 40 °C, non-condensing

¹ According to the manufacturer with memory and storage for the extended temperature range.

4.1.2.2 Connectors on the housing

- **Front**, top to bottom: power switch, Nano SIM slot, three LAN sockets (top Eth3, middle Eth2, bottom Eth1), two USB sockets next to them, two HDMI sockets below.
- **Top**: two COM ports (9-pin).
- **Bottom**: power supply terminal.

From the factory, the LAN ports are set as follows:

Port	Factory setting
Eth1	fixed 172.16.9.112/24
Eth2	DHCP
Eth3	fixed 172.16.10.250/24 (service port)

What each port is meant for is described in Edge wiring (Ch. 4.2).

4.1.2.3 Dimension drawing

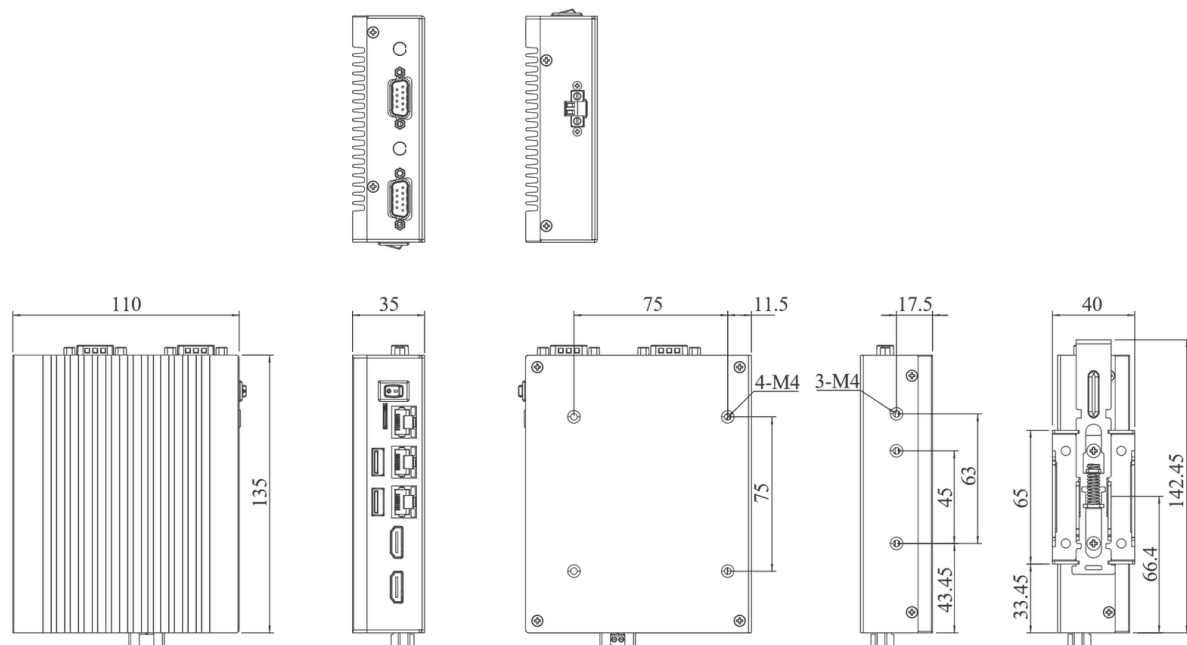


Figure 14: Dimension drawing of the LEX NET-III 2I640DW with housing dimensions, connectors and DIN-rail bracket (dimensions in mm)

4.2 Edge wiring

The openXEdge has three LAN ports on the front. Out of the box they are **fixed** to three distinct roles — once you've internalised that, you also know where service personnel plug in and where the sensor bus must terminate.

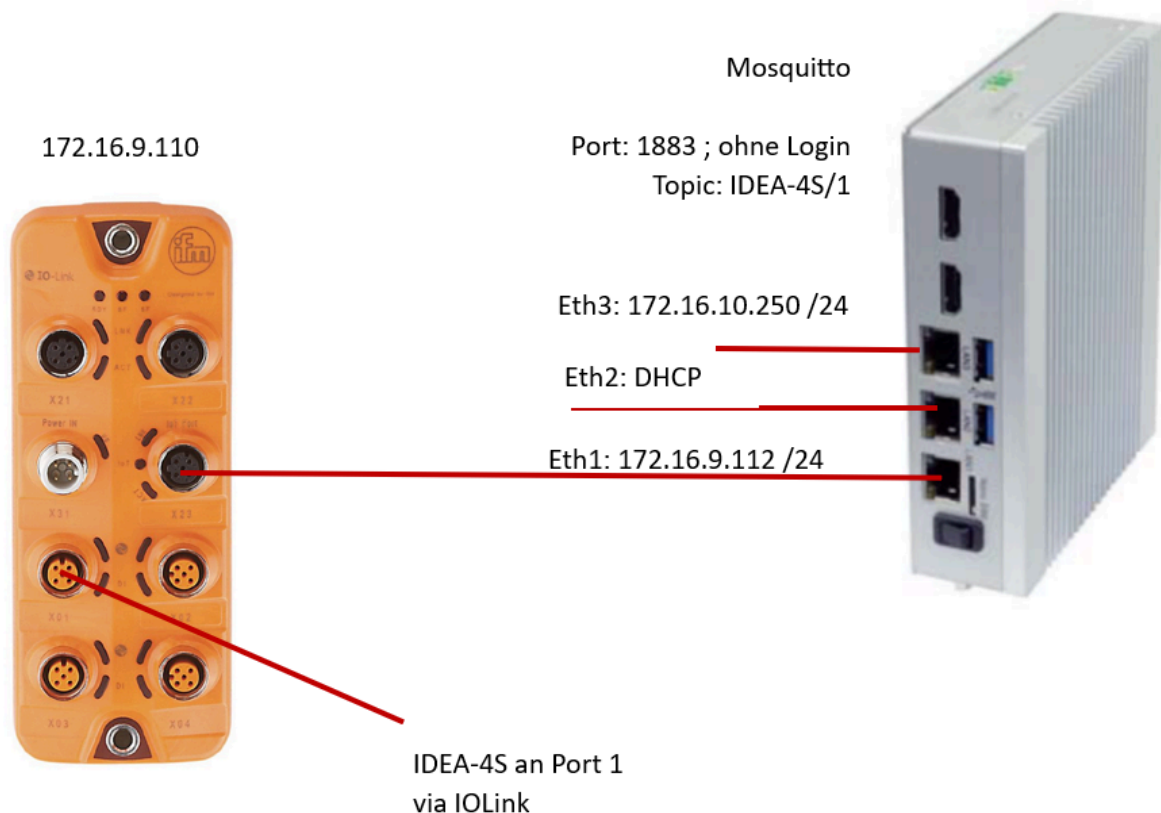


Figure 15: Wiring overview: IO-Link master, edge ports, Mosquitto

4.2.1 The three ports

Top to bottom on the device:

Port	Role	Factory IP
Eth3 (top)	Service port for Brinkhaus service / IT support. Static, isolated from the office network.	172.16.10.250/24
Eth2 (middle)	Office network — DHCP client. The edge gets its company IP here, reaches the internet, talks to the FleetManager.	DHCP
Eth1 (bottom)	IO-Link master uplink. Static in the master subnet.	172.16.9.112/24



Eth1 is therefore permanently pointed at the IFM IO-Link master — factory default 172.16.9.110. The **IDEA-4S** sensor sits on **Port 1** of that master via IO-Link and emits its values over the IO-Link protocol.

4.2.2 Why three separate networks?

The separation does two things at once:

1. **Machine bus stays clean** — the IO-Link master and its sensor strand live in their own small subnet (172.16.9.0/24). Traffic there is in the low-kbit range and is not affected by office load.
2. **Office network stays clean** — anything that needs the outside world (firmware updates, FleetManager onboarding, browser access from a shop-floor PC) goes exclusively through Eth2.

4.2.3 Data path in short



More on visualisation in Grafana dashboards (Ch. 4.4), more on the MQTT subscription in Configure IO-Link master (Ch. 2.11).

4.2.4 Practical consequences

- **Bringing a system online:** Eth1 to the IO-Link master, Eth2 into the office network with DHCP, Eth3 only when a service technician is on site.
- **On-site IDEA-4S work:** a service laptop reaches the device through Eth3 (service subnet) or through Eth2 (office side).
- **Changing the edge's IP:** only via the UI (see Configure the network (Ch. 2.6)) — never via the OS directly, you would break the next update.

4.3 How updates work

When you click **Upgrade** or **Downgrade** in **Settings** → **Update**, a multi-stage process kicks off. This page explains what happens in the background — useful when something doesn't go as expected.

4.3.1 Components involved

- **MainUI** — the UI that catches the click and downloads the update files.



- **BOS Update Server** (<https://update.brinkhaus-gmbh.de>) — the central source of all firmware versions, signed with an Ed25519 key.
- **UpdateService** — a separate background container on the edge that orchestrates the swap. It lives in **its own compose stack**, not the main stack, because it must restart the main stack without tearing itself down.

4.3.2 Phase 1: selection + download (MainUI)

1. MainUI fetches the available-versions list from the update server.
2. You click a version → MainUI downloads three files **in this exact order**:
 1. `public-key.pem` — the public signing key
 2. `docker-compose.yml.sig` — the signature over the new compose file
 3. `docker-compose.yml` — the compose file itself (last!)
3. MainUI verifies the Ed25519 signature. On failure → diagnosis code 1009, update aborted.
4. The three files now sit under `/home/gmn-service/docker/updates/data/`. Writing the compose file is the trigger event for the UpdateService.

4.3.3 Phase 2: 7-phase deploy (UpdateService)

The UpdateService polls the staging directory every 10 seconds. As soon as it finds a new `docker-compose.yml`, the following sequence runs:

Phase	Action
1	Validation — staged compose file exists and is syntactically valid?
2	Backup — copy the current compose file and <code>description.json</code> to the backup directory.
3	Stop — <code>docker compose stop</code> + <code>docker compose rm -f</code> for the main stack (not down, so the shared <code>bos-internal</code> network survives).
4	Deploy — atomic copy of the new files to the live location. <code>config.json</code> is not overwritten (MainUI merges new defaults at startup).
5	Start — regenerate <code>.env</code> (for the current multi-IP list), <code>docker compose pull</code> , <code>docker compose up -d</code> .
6	Health check — container stability (≥ 10 s uptime, no restart loops) and HTTP probe against <code>http://localhost:5000/api/version</code> <i>inside the container</i> .
7	Cleanup (on success) or rollback (on failure).

The UI is **unreachable for the duration**.

4.3.4 Phase 3: rollback (only on failure)

If the health check is not green within 90 seconds, the UpdateService rolls back automatically:

1. Stop the stack with the new version.
2. Copy the backup compose + description to the live location.
3. Bring up the stack with the old version.



4. Emit diagnosis codes 2005 (rollback initiated), then 2006 (succeeded) or 2007 (failed).

❑ **One-cycle backwards-compatibility:** the **previous** UpdateService runs the health check during an upgrade — so the new MainUI must keep answering `http://localhost:5000/api/version` exactly as the old UpdateService expects, for at least one upgrade cycle. This rule was violated in 2.1.0 — every upgrade from 2.0.x rolled back; 2.1.1 fixed it.

4.3.5 What do the versions in the service table mean?

Settings → **Update** shows not just the firmware version (e.g. 2.2.1) but also individual versions of each Docker container:

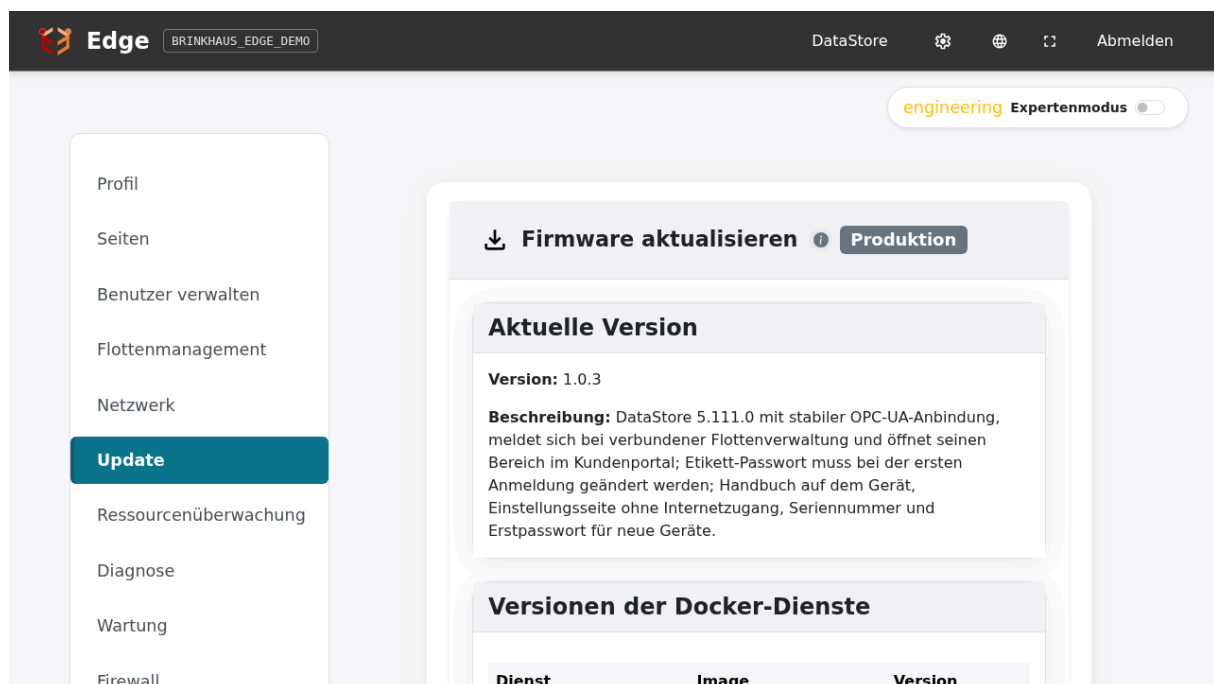


Figure 16: Service versions table in the Update view

A firmware version is a **bundle** of compatible service versions, fixed in the shipped `docker-compose.yml`. An update therefore doesn't just replace one image — it deploys a tested combination of all the stream's containers.

4.3.6 Related

- Update firmware (Ch. 2.1) — the on-screen steps
- Diagnosis codes (Ch. 3.1) — what every update-error code means (range 2xxx)

4.4 Grafana dashboards

Clicking the **Grafana** tile on the home page lands you on a pre-configured dashboard. It shows the most important values from the attached IDEA-4S sensor at a glance.

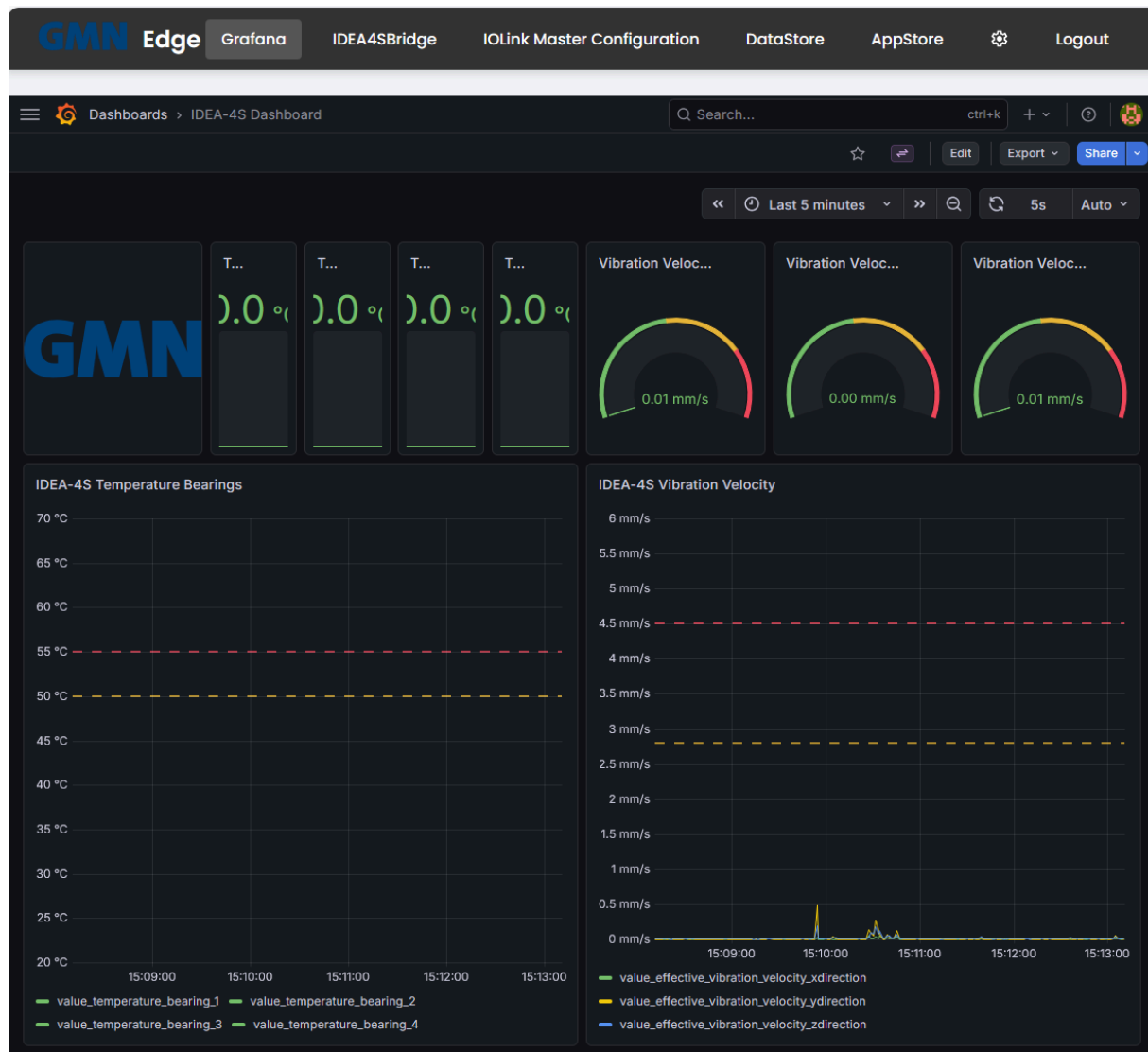


Figure 17: IDEA-4S dashboard in Grafana with bearing temperatures, vibrations, and time-series panels

4.4.1 Dashboard layout

- **Four bearing-temperature stat tiles** top-left: Bearing 1 through Bearing 4, in °C. With live data the tiles colour according to the configured thresholds.
- **Three vibration-velocity gauges** top-right: X, Y, Z axes, in mm/s. The scale runs green → yellow → red as values approach the IODD-defined thresholds.
- **Time-series panel “IDEA-4S Temperature Bearings”** bottom-left: all four bearings over the selected time range. The red dashed line is the alarm threshold; the yellow one the fault threshold.
- **Time-series panel “IDEA-4S Vibration Velocity”** bottom-right: the three axes over the selected time range.

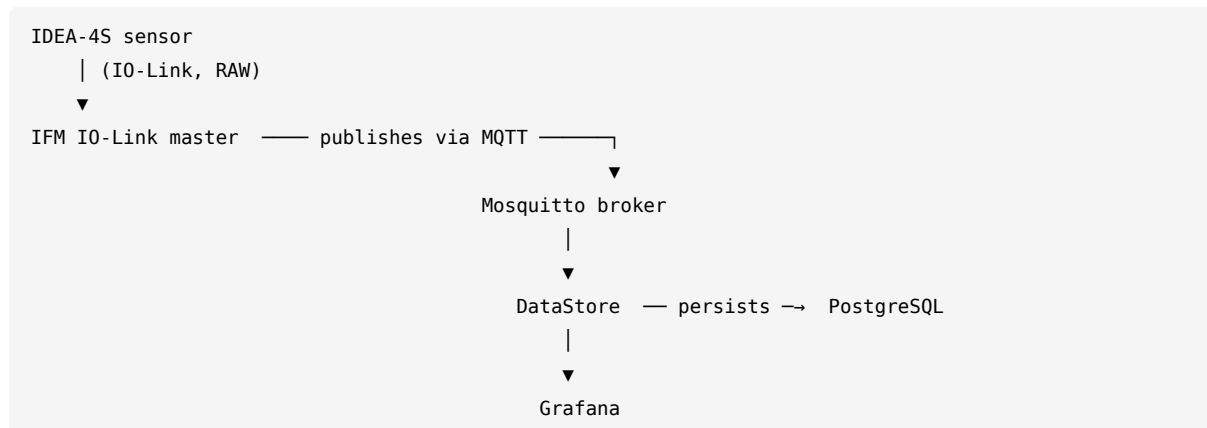
Both time-series panels draw a continuous line even where a bearing reported nothing in a bucket of the selected range (from **gm-n-2.34.1**). The four bearings do not report in the same instant; a bearing's



line used to break at every such point and leave scattered dots behind. Only a straight connection is drawn between two measured values — no value is invented. A genuine sensor dropout therefore does **not** show as a gap in the curve; it shows on the tiles above and on the diagnosis page.

Use the time-range picker top-right (here: “Last 5 minutes”) to switch between live and historical views.

4.4.2 Where does the data come from?



- The IO-Link master polls the IDEA-4S cyclically and sends each change as an MQTT message. The configured topics are visible in **IOLink Master Configuration** → **Notification**.
- **DataStore** subscribes to these topics, validates them against the schema, and writes the values into the local **PostgreSQL** on the edge.
- **Grafana** reads from the PostgreSQL and visualises it. The dashboard ships with the edge; you can clone and customise it.

4.4.3 Signing in: you already are

Grafana has no password of its own. The edge’s control interface signs you in there under **your own user name** — your name appears top right, and whatever you change is recorded under it. Signing out of the control interface ends your Grafana access with it.

What you may do there follows your role in the control interface:

Your role	In Grafana
Administrator	View, edit and save dashboards
User	View dashboards

If an administrator changes your role, Grafana follows immediately — from your next page load.



4.4.4 Custom dashboards

As an **administrator**, click **Dashboards** → **New** in Grafana's left sidebar, or duplicate the shipped dashboard, to build your own views. Custom dashboards survive firmware updates — they are not overwritten by the repo seed.

If the save button is missing, you are not signed in to the control interface as an administrator.

4.4.5 Your own dashboard as the start page

Which dashboard the **Grafana** tab opens is set under **Settings** → **Default Pages**. Pick it from the **list** there — it holds exactly the dashboards that exist on this edge.

If you type the address by hand instead, mind **which part** you are copying:

```
/grafana-proxy/d/c10732a9-2e02-47cd-a033-059fb6f34344/idea-4s-dashboard-vwbaunatal
```

└─────────── UID ───────────┐ └────────── name ─────────┘

Grafana finds a dashboard **by its UID alone** and rewrites the name behind it on every request. An address carrying your dashboard's name and another dashboard's UID therefore opens the other one — it saves, it works, it just shows something else. Copies often carry very similar UIDs that differ only in the last few characters.

The control interface checks the address against the dashboards that exist when you save, and tells you when the UID and the name belong to two different dashboards.

4.4.6 How often the display refreshes

The refresh interval sits next to the time range at the top right of Grafana. The shortest setting the edge allows is **half a second**; 500 ms and 1 s are offered only by dashboards that carry those values in their own interval list — the delivered ones do.

It will not make the display faster than the values arrive. Measured on an edge over two hours, as the gap between consecutive values (median): vibration velocity 0.1 s, bearing and coolant temperatures 0.2 s — a one-second refresh is worth having there. Rotational speed came every 30 s because the spindle was idle: the sensor reports on change, and in operation its values are 0.1 s apart too.

For a smoother picture of a value that is not changing right now, the **Refresh live dashboards** switch (in the dashboard settings) is the better lever — it keeps the time axis moving without querying more often.

4.4.7 When the dashboard stays empty

If you see axes but no data, the data pipeline is usually broken somewhere:

1. Open **Settings** → **Diagnosis** and check that `datastore`, `postgres`, and `mosquitto` are green.



2. Open **IOLink Master Configuration** → **Notification** and confirm there is at least one MQTT subscription to 172.16.9.112:1883/teststand/idea-4s (example topic).
3. If both are OK but Grafana is still empty: this can be a known “memory-loss” case — refer to internal documentation or contact Brinkhaus support.

4.5 Resource monitoring

Settings → **Resource Monitoring** shows the edge hardware load at a glance. Values come from the operating system directly (psutil); the Refresh button fetches a fresh sample.

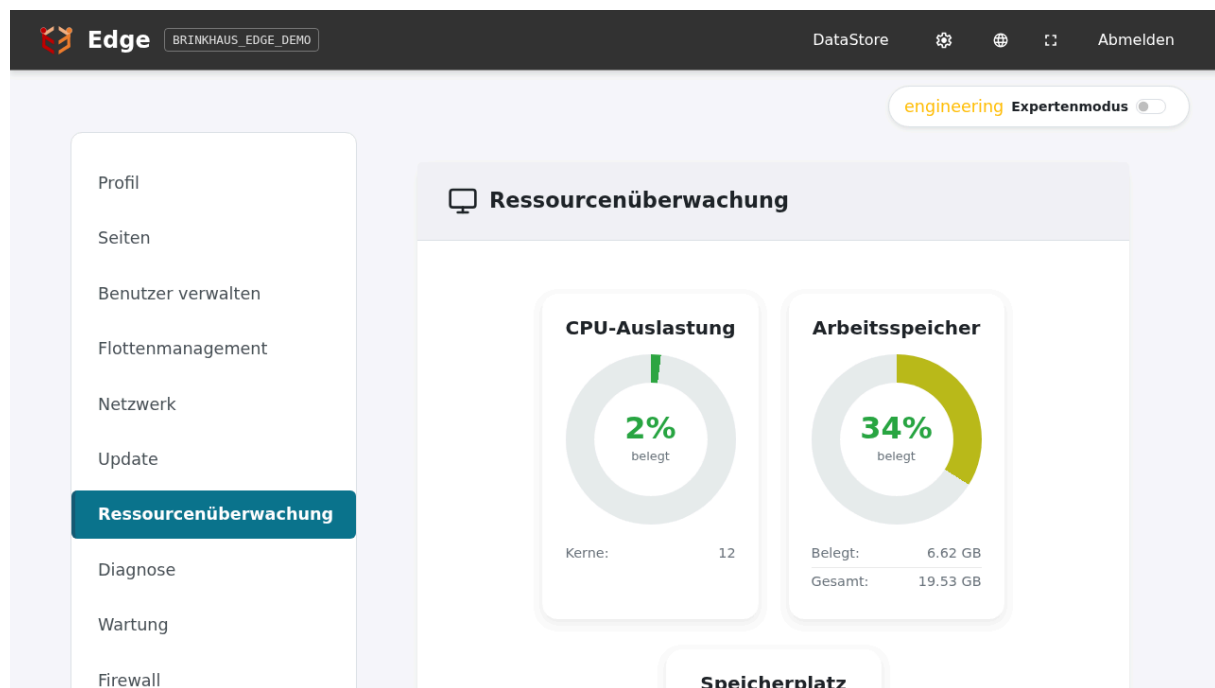


Figure 18: Resource Monitoring with three donut charts

4.5.1 What the three charts mean

Chart	Meaning
CPU Usage	Current load across all CPU cores (snapshot). “Cores” tells you how many cores the edge has.
Memory Usage	RAM in use vs total available. “Used” and “Total” are shown in MB / GB.
Disk Usage	Internal SSD/eMMC fill level. Firmware writes mostly logs and sensor data — fast growth usually means a misconfigured application.

4.5.2 What are “normal” values?

At idle with measurement data being recorded:

- **CPU:** typically 1–5%. Spikes during boot or an update are normal.
- **Memory:** 15–25%. Drifts up slowly as container caches fill — up to ~70% is fine.



- **Disk:** 5–15% depending on uptime and data volume. Postgres data grows by a few hundred MB per month.

4.5.3 When to react

- **CPU sustained > 80%:** usually a runaway loop in a FLECS app or a custom dashboard. Check AppStore, stop the offending app.
- **Memory > 85%:** an app is leaking — the edge won't crash itself, but new containers start more slowly. Reboot or call Brinkhaus support.
- **Disk > 90%:** prune logs or old Postgres tables — contact Brinkhaus support; never delete files on the edge by hand.

4.5.4 Where do the numbers come from?

Values are read from the edge's host OS, not from individual containers. A single misbehaving app drives the chart up here without revealing **which** app — for that, look at **Settings** → **Diagnosis**, where every service reports individually.

4.6 Fleet onboarding

4.6.1 What it is

Every openXEdge is preconfigured to phone home to the **FleetManager** as soon as it can reach the internet. That is the foundation for everything you might want to be remotely supported on — remote diagnosis, update recommendations, emergency repair.

4.6.2 Prerequisites

Three conditions need to hold at the same time:

1. **24 V power** at the edge.
2. Eth2 (middle port) is connected to a **DHCP server** that hands out an office IP and allows internet access — typically an office switch behind your company router.
3. The edge has its **identifier**: devices with a serial number bring it from the factory; older devices get their machine ID at activation (Ch. 1.2.5).

When all conditions hold, the edge sends a **heartbeat** to the FleetManager every few minutes with versions, IPs, and self-diagnosis. Brinkhaus personnel then see your edge in the central overview:



FleetManager

1 machine(s)

GMN
12 machine(s)

- e000002**
6 software instance(s)
- e000003**
6 software instance(s)
- e000005**
6 software instance(s)
 - bos-iolinkmasterproxy** v1.0.3
Status: running | Heartbeat: 4/29/2026, 11:07:55 PM | IP: 10.10.20.202, 172.16.9.112
[Info] 0: All self tests passed
 - bos-mainui** v1.2.11
Status: running | Heartbeat: 4/29/2026, 11:07:55 PM | IP: 10.10.20.202, 172.16.9.112
[Info] 0: All self tests passed
 - bos-updateservice** v1.2.11
Status: running | Heartbeat: 4/29/2026, 11:07:55 PM | IP: 172.19.0.7, 172.20.0.2
[Info] 0: All self tests passed
 - bos-usb-service** v1.1.1
Status: running | Heartbeat: 4/29/2026, 11:07:55 PM | IP: 10.10.20.202, 172.16.9.112
[Info] 0: All self tests passed
 - datastore** v4.3.10
Status: running | Heartbeat: 4/29/2026, 11:07:55 PM | IP: 10.10.20.202, 172.16.9.112
[Info] 510: Error inserting low frequency data into historicValues
 - idea4sbridge** v1.2.14
Status: running | Heartbeat: 4/29/2026, 11:07:55 PM | IP: 10.10.20.202, 172.16.9.112
[Info] 0: All self tests passed
- e000006**
6 software instance(s)

Figure 19: FleetManager with the Brinkhaus GmbH node and one expanded edge

4.6.3 Serial number, device name and inventory number

Every newly shipped edge carries a **serial number** (e.g. SN00100), printed on the label and the delivery note. Fleet management keys the device by this number. It is assigned at first provisioning and cannot be changed on the edge — so a device stays the same device in the fleet, even when you rename it or move it elsewhere.

What you call the device is up to you, with two free fields (the settings page labels them in German):

- **Gerätename** (device name) — the name fleet management shows for the device (e.g. “Lathe 1”). Renaming only changes the label; no second device appears.



- **Inventarnummer** (inventory number) — your own inventory or machine number, so you can find the device in your records.

Both fields are optional.

Older devices without a serial number stay keyed by the machine ID from their activation and keep it. As long as they are connected to fleet management, support can assign them a serial number there later. The machine ID, the password and the history are kept; on the edge the serial number then appears in place of the **Machine** field.

4.6.4 What Brinkhaus personnel can see

Per edge in the central view:

- **Status dot** (green/yellow/red) — at a glance, is the edge still online and does it report problems.
- **Version levels** of every running container (bos-mainui, bos-updateservice, datastore, idea4sbridge, ...).
- **Last heartbeat time** — anything older than a few minutes means the edge is offline or has lost internet.
- **All current IPs** — useful when the office DHCP rotates the lease.
- **Self-diagnosis messages** — the same codes you see under Read diagnosis (Ch. 2.9).

4.6.5 What the edge actually transmits

Deliberately minimal:

- Version levels, IPs, heartbeat time, self-diagnosis codes.
- Serial number, device name and inventory number.
- Whether the initial password has been changed — **never** the password itself (see Change password (Ch. 2.3)).
- **No** sensor measurements, **no** process data, **no** personal data.

That is: the FleetManager is a maintenance plane for the edge itself, **not** an archive of your production data. Your measurements stay on the edge (and wherever you actively export them).

4.6.6 Edge-side control

On the edge you see your part under **Settings** → **Fleetmanagement**:

- **Customer Name** — read-only, the customer this edge belongs to in the fleet.
- **Seriennummer** (serial number) — read-only, only on devices with a serial number. It identifies this edge in the fleet.
- **Machine** — only on devices without a serial number: the machine ID from activation (Ch. 1.2.5) that identifies this edge in the fleet.



- **Gerätename** (device name), **Inventarnummer** (inventory number) and **Aufstellungsort** (location) — free to choose.

Apply changes with **Save Fleetmanagement Settings**. Device name, inventory number and location appear in fleet management only after the next restart of the device.

4.6.7 When an edge goes offline

In the central view (image above) edges whose last heartbeat is too old appear with a **red** status dot (in the example `e0000002` and `e0000003`). Brinkhaus personnel see this immediately and reach out proactively — provided the edge is connected to fleet management. Typical causes are failed switches, forgotten power, or an office DHCP that rotated its pool.

4.6.8 Asking for help

Send the hotline:

1. the **serial number** (on the label and the delivery note, on the edge under **Settings** → **Fleetmanagement**) or, on older devices without a serial number, the **machine ID** (same place),
2. a brief symptom (“Grafana empty”, “update keeps failing”),
3. the last action you tried.

If the edge is connected to fleet management, the hotline reads the diagnosis in the FleetManager in parallel — usually that’s enough to locate the problem without anyone going on-site.

4.7 Security and support

This page collects what you need in order to run the openXEdge safely: where to report a security problem, how long you get updates, what to do at commissioning and decommissioning, which network ports are open, and what data the device processes.

4.7.1 Reporting a vulnerability

If something about the openXEdge looks like a security problem, please report it to:

security@brinkhaus-gmbh.de

Anything that helps us reproduce it is useful: the firmware version (Settings → *Update*), the serial number (the machine ID on older devices), what you did and what happened.

Our commitment. Anyone who reports a vulnerability to us in good faith has no legal action to fear from us. We confirm receipt, keep you posted, and credit you when we close the gap if you want us to. Please give us time to fix the problem before you publish the details.

You can hold us to this:

- You receive an **acknowledgement within 5 working days**.



- Within **15 working days** we tell you whether the openXEdge is affected, how severe we rate the vulnerability and how we intend to proceed.
- Please publish details **no earlier than 90 days after your report or once the fix has shipped**, whichever comes first.

If you suspect a vulnerability is already being exploited, say so explicitly — shorter deadlines apply to those.

4.7.2 How long you get security updates

Brinkhaus provides security updates for the openXEdge firmware and the container stack shipped with it through the signed update channel for **five years** from the delivery of the individual device.

In detail:

- The period starts when **your device is delivered**, not when the product was launched. Two devices can therefore have different end dates.
- If a device is **replaced**, the replacement starts a period of its own.
- It covers the firmware and the services shipped with it. It does **not** cover applications you install yourself from the AppStore — those are covered by whatever their own vendor promises.
- The commitment applies to firmware from version 2 onwards. Devices still on the old 1.1 line are excluded and should be migrated; talk to us.

4.7.3 How security updates reach the device

Security updates arrive the same way as any firmware update: you pick a version in the settings, the edge downloads it from the update server and verifies its **digital signature** before installing. If the signature does not match, nothing is installed. If the installation fails, the edge returns to the previous state by itself.

How updates work (Ch. 4.3) describes the sequence in detail. If your edge cannot reach the update server, there is also the USB route (Ch. 2.2) — with the same signature check.

We mark security-relevant changes in the release notes, which you can read before installing.

4.7.4 Secure commissioning

Two things are worth doing right away:

1. **Change the initial password.** Every edge gets its own initial password. On devices with a serial number it is on the label or delivery note and cannot be worked out from the serial number alone. On older devices the activation shows it once; it is derived from the machine ID and therefore not a secret: anyone who knows the method and the machine ID can work it out. Either way, change it when you first sign in. Devices with a serial number require it after the first sign-in with the label password; older devices do **not** force it. → Change password (Ch. 2.3)



2. **Create individual user accounts** instead of sharing one. Only then does the audit trail tell you afterwards who changed what. Every password someone sets must meet the password policy (in the GMN stream from gmn-2.45.2), by default at least 10 characters. An admin can tighten it there.
→ Manage users (Ch. 2.8)

Beyond that, safe operation assumes the edge sits **in a protected company or plant network** and is **not reachable from the internet**. Do not set up port forwarding to the device. For remote access, use the encrypted route (Ch. 2.4).

4.7.5 Secure decommissioning

When a device is retired, returned or passed on:

1. **Erase the data.** All recorded measurements, settings and credentials live on the built-in disk. Reinstalling from a USB stick writes a complete image to that disk and overwrites it in the process. If the medium has to be erased **verifiably and without residue** — when returning it to a third party, for instance — that is not enough; plan for a full overwrite or physical destruction of the medium. We will help you with that.
2. **Request removal from fleet management.** The device cannot deregister itself. Write to **security@brinkhaus-gmbh.de** or to your contact, and we will remove the record and its log data.
3. **Check your own integrations.** If you wired the edge into your own systems (an MQTT feed on port 1883, for example), remove those entries.

4.7.6 Open network ports

These ports are reachable from outside in the delivered state. Every other service — database, Grafana, DataStore, update service — is reachable **only inside the device** and cannot be addressed from outside. From the software state with maintenance service 1.22 on (GMN: firmware 2.45), a **firewall on the device** enforces this: it drops every connection to a port that is not on the allow-list. You may close the system ports 22, 5000, 5443 and 1883 yourself and open further ports yourself — see Configure the firewall (Ch. 2.7).

4.7.6.1 Your product functions

Port	Purpose	Note
5000/ tcp	Operator interface, unencrypted	The kiosk screen uses it too
5443/ tcp	Operator interface, encrypted	The recommended route; certificate from the device's own edge CA or your company CA, see Remote access (HTTPS) (Ch. 2.4).
8050/ tcp	IDEA-4S bridge	Blocked from the network by the firewall; meant for the applications on the device. The service additionally decides who may read and who may write, by source address.



Port	Purpose	Note
8082/ tcp	IO-Link relay	Blocked from the network by the firewall until you open it by rule for a DataStore outside the edge; the relay additionally checks the source address against its allow list.
1883/ tcp	MQTT broker	No authentication, no encryption. Anyone who reaches this port can read every measurement and inject their own. The interface is deliberately open so your own systems can subscribe — which is exactly why it belongs in a protected network.

4.7.6.2 Base system services

Port	Purpose
22/tcp	Maintenance access for the Brinkhaus service, key-based login only

These base-system services run on the device but are **blocked from outside by the firewall**; they are needed only inside the device:

Port	Purpose
80, 443/tcp	The AppStore's distributor to the installed applications — the operator interface embeds the AppStore through its own port.
8951/tcp	AppStore service.
8085/tcp	Self-diagnosis of the security agent, read by the operator interface.
631/tcp	Print service. It comes along as a dependency of the kiosk browser and is not needed to run the edge

Applications from the AppStore open ports of their own. Those are blocked from outside too until you open them in the firewall; through the edge's operator interface you reach the applications without an allowance. Before maintenance service 1.22 (GMN: firmware 2.45) there was no firewall — on such devices the ports listed here as blocked are open.

4.7.7 What data the edge processes

On the device are the measurements from your sensors and machines, the settings, and the user accounts of the operator interface. You decide yourself how long measurements are kept.

To fleet management go operating data only: version levels, IP addresses, the time of the last heartbeat, self-diagnosis codes, serial number, device name and inventory number, and whether the initial password has been changed (never the password itself). **No** sensor measurements, **no** process data, **no** personal data. The connection always runs outbound from the edge; no port is opened from outside.

More on this: Fleet onboarding (Ch. 4.6).



4.7.8 What the product is, and what it is protected against

The openXEdge is a device for **condition monitoring** of production machines: it records sensor and process values, stores them and displays them. It does **not control the machine** and is not part of a safety chain.

We protect four things, in this order of precedence:

1. **Recording keeps running** — even when the network fails, a plug is pulled or a service crashes.
2. **Only our software reaches the device** — every update is signed and verified before installation.
3. **Credentials stay on the device.**
4. **Interventions are traceable** — sign-ins, sign-outs and changes are logged.

Where availability and hardening conflict, availability wins: a device that stops measuring is of no use on a shop floor. Those trade-offs are written down and justified.

Software bill of materials (SBOM). For every released version we keep a complete list of the software components it contains, in CycloneDX format. You can have it on request to security@brinkhaus-gmbh.de within ten working days; please quote your device's firmware version.

Declaration of conformity. The supplier declaration for your device is a separate, printable page in this documentation.

We provide the full EU declaration of conformity and the technical documentation on request.

Version 2026.10.21

Date: 10.2026

© 2026 Brinkhaus GmbH, Isernhagen



5 Notes



Brinkhaus GmbH

Schneekoppenweg 6
30916 Isernhagen

Support

E-mail: edge-support@brinkhaus-gmbh.de