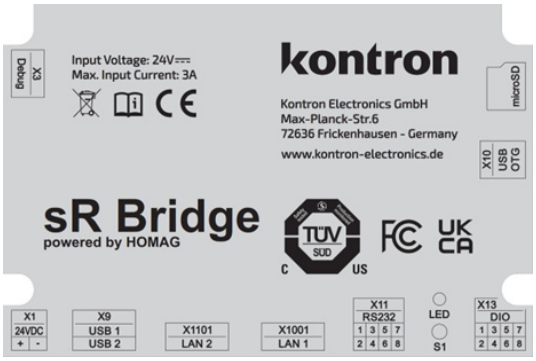
1 Intended use

The *sR Bridge* and its accessories are intended exclusively for the purposes of remote diagnostics. Use of the equipment for any other purpose beyond that described is considered improper use.

Note
Only use the accessories supplied.

Note
The manufacturer and dealer accept no liability for damage caused by improper use. Furthermore, damage caused by improper use is not covered by the warranty.



Contents

1	**Intended use**	**1**
2	**Information and specifications**	**4**
2.1	Safety information	5
2.1.1	Symbols	5
2.1.2	Information on cybersecurity	6
2.2	Functions	7
2.3	Features	8
2.4	Connections	9
2.5	Technical specifications	11
2.6	Mechanical specifications	12
2.7	Electrical specifications	13
2.8	Features	14
2.9	GDPR compliance	15
2.10	Use of open source components	16
3	**Components**	**17**
3.1	Items supplied	17
4	**Assembly**	**19**
4.1	Tools required	20
4.2	Relevant device information	21
4.3	Installation variants	22
4.3.1	Hall network variant — TSN and ISN connections	22
4.3.2	Hall network variant — Linux and older operating systems	22
4.3.3	Machine network variant — TSN router	23
4.4	Connecting accessories	25
4.5	Mounting in the holder	27
4.6	Mounting on the wall	28
4.7	Mounting on the machine protection cover	30
4.8	Mounting in the TSN junction box in the switch cabinet	32
4.9	Mounting without holder	33
5	**Set up network**	**34**
5.1	Change device password	34
5.2	Settings on the customer network/firewall	35
5.3	Settings for the internal network	36
5.4	Required URLs	37
5.5	Network settings for the sR Bridge	38
5.6	Call up the diagnostic page of the sR Bridge	39
5.7	Settings on the diagnostic page of the sR Bridge	40
5.8	sR Bridge firmware update	43
5.8.1	Disabling automatic firmware updates	43
5.8.2	Manually perform the firmware update via the diagnostic page	44
6	**"sR Connect" machine update**	**45**
6.1	Functions of serviceRemote Starter Premium	46
6.2	Install update	47
6.3	serviceRemote Starter Premium	48
6.3.1	Pairing mode (Starter Premium)	48

6.4	serviceRemote Starter Classic	50
6.4.1	Pairing mode (Starter Classic)	50
6.5	Linux	52
6.6	Setting up two-factor authentication (2FA)	53
7	**Button and LED**	**56**
7.1	Internal button and LED color	57
7.2	External button and LED color	58
7.3	LED status displays	59
8	**Creating machine groups**	**60**
9	**Start remote diagnostics**	**61**
9.1	Starter Premium	61
9.2	Starter Classic	63
9.3	Sensing device	64
9.4	Function test	65
10	**Log**	**66**
10.1	sR Bridge logs	67
11	**Maintenance and care**	**68**
11.1	Cleaning	69
12	**Troubleshooting**	**70**
12.1	sR Starter — "Troubleshoot" function	70
12.2	sR Bridge does not have an IP address. How can it be accessed?	71
12.3	sR Bridge — Diagnostic page cannot be opened	72
12.4	Resetting sR Bridge to factory settings	73
12.5	Enter NTP time server	74
12.6	If there are network problems, perform network diagnostics	75
12.7	Available functions in different countries	76
13	**Interfaces**	**78**
13.1	External button/LED — pin assignment and power supply	78
13.2	Wiring diagram (example)	80

2 Information and specifications

The document contains up-to-date information at the time of its creation.

Important changes or new features compared to this status can be found here until the document is updated:

https://docs.homag.cloud/

2.1 Safety information

Note
Observe the safety regulations for production equipment manufactured by HOMAG!

Attention

Components may be damaged or damaged.
Equipment damage

- Visually inspect the device and accessories for damage before each use.
- In the event of damage to the device, disconnect the device from the mains immediately.
- Only use the device on correctly connected shockproof sockets.
- Do not expose the device to moisture or excessive dust.

Danger



danger of explosion! Switching operations can cause sparks.
Risk of fatal injury!

- Do not operate the device in an environment with explosive vapors.

2.1.1 Symbols

- IP20 is a protection class, which protects against contact with your finger >12.5 mm.
  - No protection against water guaranteed

IP20

- Through the CE mark, the manufacturer declares that the device has tested and meets all European requirements for safety, health and environmental protection.

CE

- Through the UKCA mark, the manufacturer declares that the device has tested and complies with all UK requirements for safety, health and environmental protection.

UK
CA

- The Federal Communications Commission (FCC) grants FCC certification for electronic products sold or manufactured in the United States.

FCC

- The NR TL TÜV SÜD mark seal, by recognizing private organizations, signals their qualification to test technical products in accordance with the regulations of the U.S. Federal Office of Health and Safety at Work. The addition U.S. indicates compliance with the requirements of the U.S. authorities, the addition C indicates compliance with the Canadian requirements.



- Do not dispose of the device or accessories in normal household waste. Disposal must be carried out by an approved disposal company or a local disposal facility. Observe current regulations.



- Before commissioning the device, read and observe the production instructions.



2.1.2 Information on cybersecurity

The device comes with a secure configuration and has hardened firmware settings that prevent unauthorized access to the system.

The device may only be used in an environment suitable for production machines with appropriately secured physical access and within a suitably secured network (e.g. ISO 27001 or equivalent).



Note

Change the device password immediately when setting up the device (see chapter "Changing the device password").

Check for new firmware updates when setting up the device.

Also note that the device must be restarted after installing a firmware update.



Note

If you disable automatic firmware updates, the device will no longer receive security updates automatically.
Available updates are displayed on the local diagnostic page, but must be installed manually in this case (see chapter "Firmware update of the sR Bridge").

2.2 Functions

The *sR Bridge* enables a connection for remote diagnostics between machines/cells and the HOMAG Group.

Remote diagnostics start or end via the diagnostic page of the *sR Bridge*.

On older machines, remote diagnostics are started by a button on the *sR Bridge*.

- The button can also be mounted externally.

The LEDs on the *sR Bridge* and on the external button indicate different statuses of the remote diagnostics.

Software and updates:

- If *sR Bridge Support* additional support is active, updates are downloaded and installed automatically.

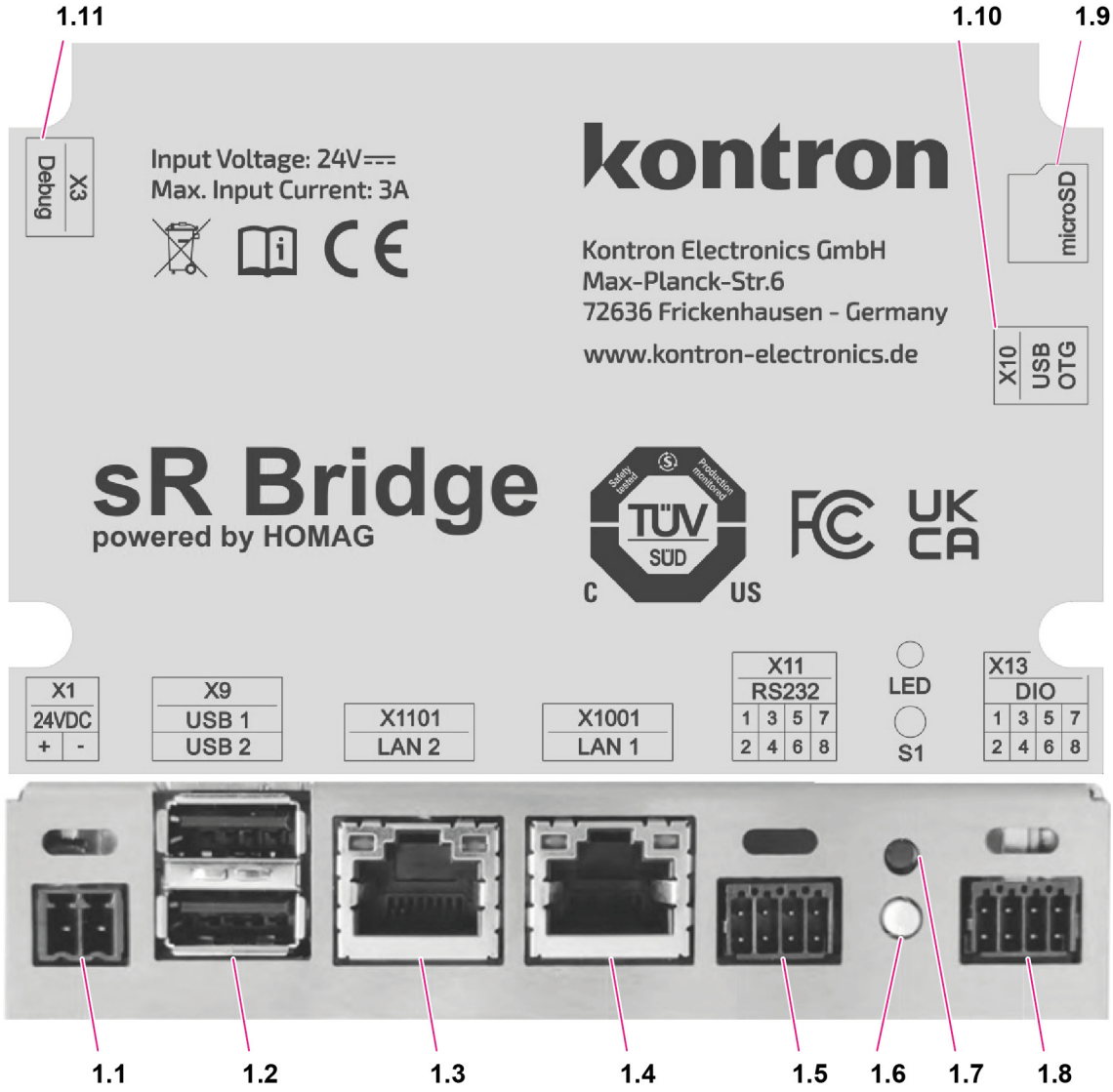
Machines/cells must be linked to the device once by means of a machine update and pairing.

2.3 Features

- External interfaces, 2x Ethernet (1x Gbit/s, 1x 10/100 Mbit/s), 2x USB 2.0, 1x USB OTG, 1x RS232
- 4X DIO 24 V/0.8 A
- Fanless passive cooling

The *AL i.MX8M Mini* is designed for 24/7 continuous operation and long-term industrial applications. All components are selected to ensure a long service life.

2.4 Connections



No.	Connection	Function	Used
1.1	X1	Power supply 24 V DC	Yes
1.2	X9	USB1 USB2	No
1.3	X1101	LAN 2 100 M/Bit	No
1.4	X1001	LAN 1 1000 M/Bit Connection to customer/machine	Yes
1.5	X11	RS232 interface	No
1.6	S1	Internal button	Yes
1.7	LED	Signal display	Yes

No.	Connection	Function	Used
1.8	X13	DIO connection for external button	Yes
1.9	microSD	Memory card slot	No
1.10	X10	USB OTG	No
1.11	X3	Debug	No



2.5 Technical specifications

Interfaces:

- 2X USB 2.0, USB A
- 1x USB OTG, micro USB
- 1x 1 Gbit/s, 1x 10/100 Mbit/s Ethernet
- 1x RS232

Voltage:

- 24 V DC ±20% input voltage

2.6 Mechanical specifications

Dimensions:

- 111x76x25 mm

Dimensions of the holder:

- 145x145x50 mm

2.7 Electrical specifications

Nominal input voltage:

- 24V DC

Input voltage range

- 24V DC ±20%

Max. input current:

- 8A (plug current)

Output current:

- 1 A at 3.3 V
  2 A at 5 V

Output current DOUT

- 2.5 A

Input Power Mating Connector 2-pin Phoenix
Contact 180° MC1.5/2-ST-3.5

2.8 Features

- GDPR-compliant remote diagnostics for individual machines and cells
- Automatic firmware updates
- Reporting
- Configuration on separate diagnostic page
- Pairing mode to connect machines
- Creation of different machine groups for remote diagnostics
- Hardware designed for 24/7 operation
- Can be retrofitted for almost all Homag machines with current remote diagnostics (TSN/TSN-Soft/ISN)
- Two-factor authentication when initiating the approval

2.9 GDPR compliance

The GDPR-compliant remote service connection ensures that all data is transmitted securely and in encrypted form.

This ensures the protection of personal information against unauthorized access. This complies with the legal data protection requirements.

Note

Homag must have explicit consent for data collection and processing.

In addition, appropriate security measures must be taken to prevent misuse or unauthorized access.

2.10 Use of open source components

The operating system of the *sR Bridge* is based on open source components.

The comprehensive license information can be viewed via the local diagnostic page on the device.

The source code used for the open source components can be requested from HOMAG.

3 Components

3.1 Items supplied

- *sR Bridge* incl. plugin power supply unit
  HOMAG-Nr: 2-083-01-0448



sR Bridge

- Plug-in power supply unit
  HOMAG-Nr: 4-086-03-0139



Power supply unit with adapters

- External button
  HOMAG-Nr: 2-082-65-9330



External button

- Holder
  HOMAG-Nr: 2-082-65-9340



Mounting

- Network cable
  HOMAG-Nr: 4-086-06-3005

Manual and Quick Installation Guide



Network cable

4 Assembly



Note
The device has protection class IP20.

➔ Install the device so that it is protected.

4.1 Tools required

Tools:

- Drill machine
- 6 mm drill
- Phillips screwdriver

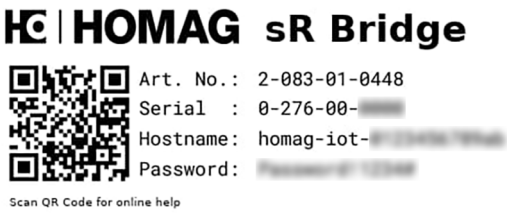
4.2 Relevant device information

Note

Before installation, take a photo of the sticker on the back or make a note of the data.
The sticker contains the necessary information that is important for commissioning.

Term	Explanation
Item no.	Homag item number
Serial	Serial number
Host name	Address for entry in default browser*
Password	Password for the diagnostic page

*This is made up of the "HOMAG IoT" and the MAC address of the device.



4.3 Installation variants

The *sR Bridge* is designed for various installation variants.

The *sR Bridge* can be operated:

- In the hall network
- For one or more individual machines
- In a HOMAG machine network

4.3.1 Hall network variant — TSN and ISN connections

sR Bridge with HOMAG individual machines with TSN Soft or ISN remote diagnostics.

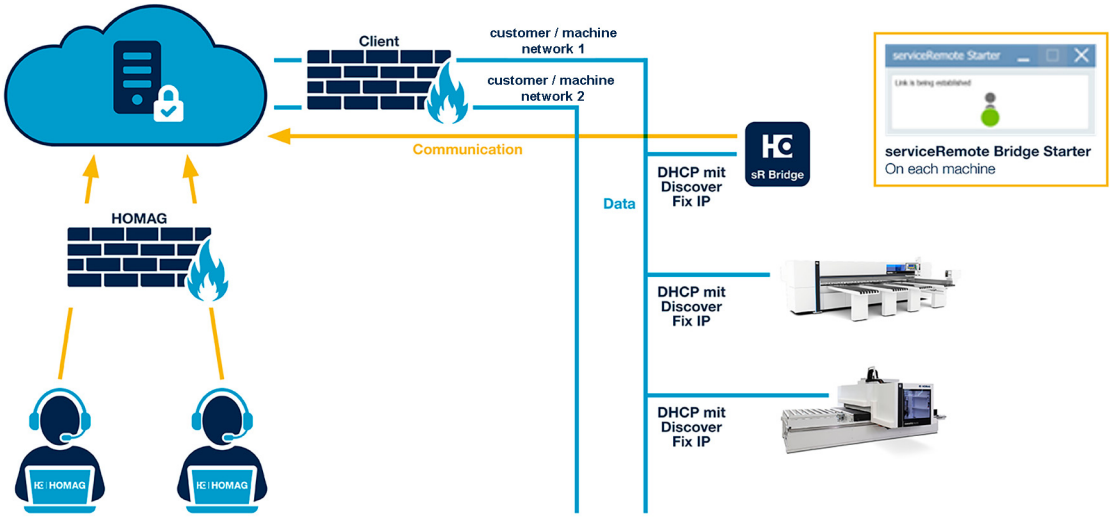
The machines to be connected and the *sR Bridge* are located in the same customer network.

The remote diagnostics can be started on the machines after the *serviceRemote Starter Update* with the previous link.

➔ The external button is not required.

Operating systems:

- *Windows 10*
- *Windows 7*
- *Windows XP* (except *Windows XP* with *Peregrine* remote diagnostics)



4.3.2 Hall network variant — Linux and older operating systems

sR Bridge with HOMAG individual machines with *Linux* and operating systems older than *Windows XP*.

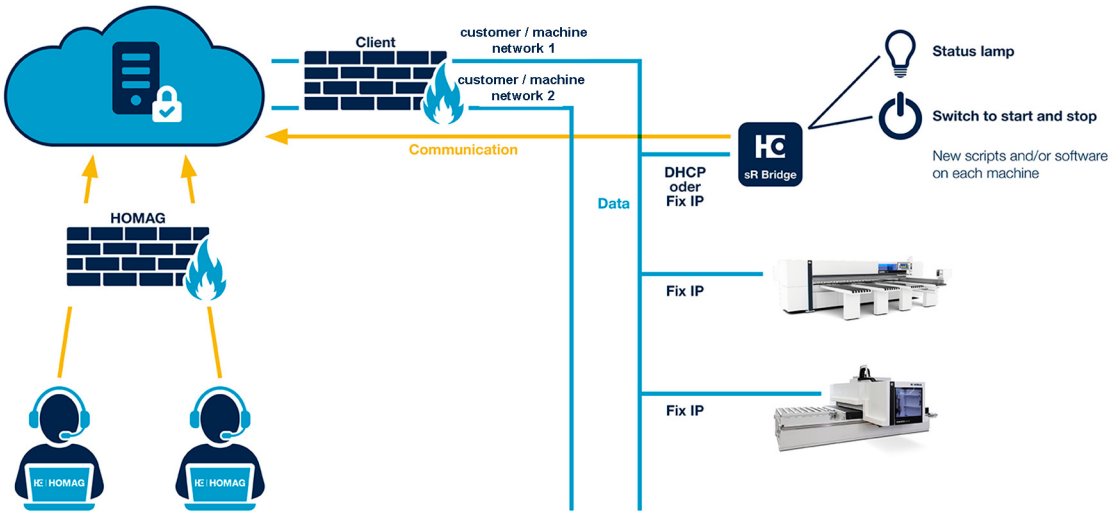
The machines to be connected and the *sR Bridge* are located in the same customer network.

After the update, the previous link to start remote diagnostics no longer works on the machines. The operating system is too old.

➔ To start remote diagnostics, the external button must be used.

Operating systems:

- *Linux*
- *Windows 98*
- *Windows 95*
- *Windows 3.11* and earlier.



4.3.3 Machine network variant — TSN router

sR Bridge within the HOMAG machine network with Internet router and/or NAT router.

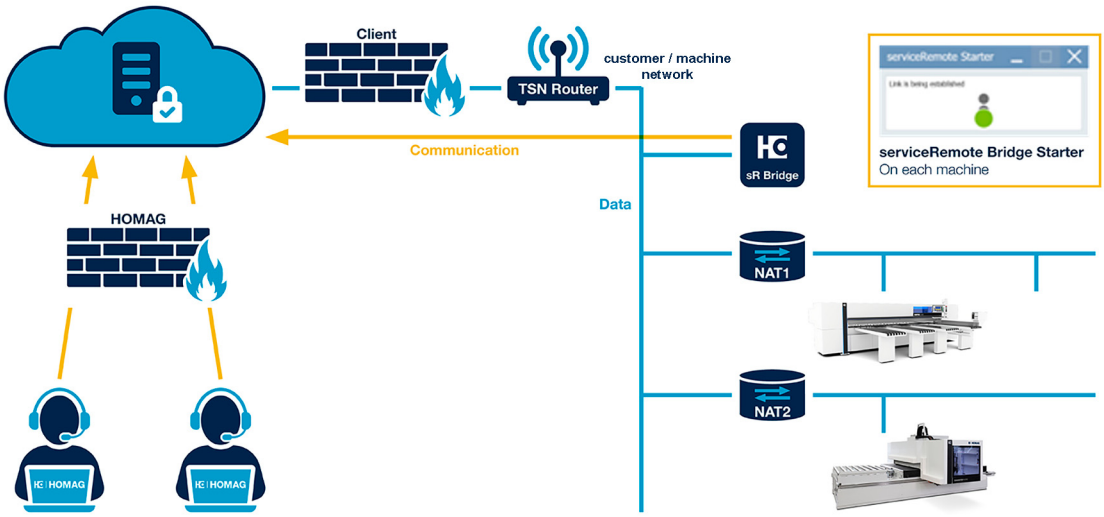
The *sR Bridge* is preferably connected to the Internet router or to a NAT router.

The remote diagnostics can be started on the machines after the *serviceRemote Starter Update* with the previous link.

➔ The external button is not required.

Operating systems:

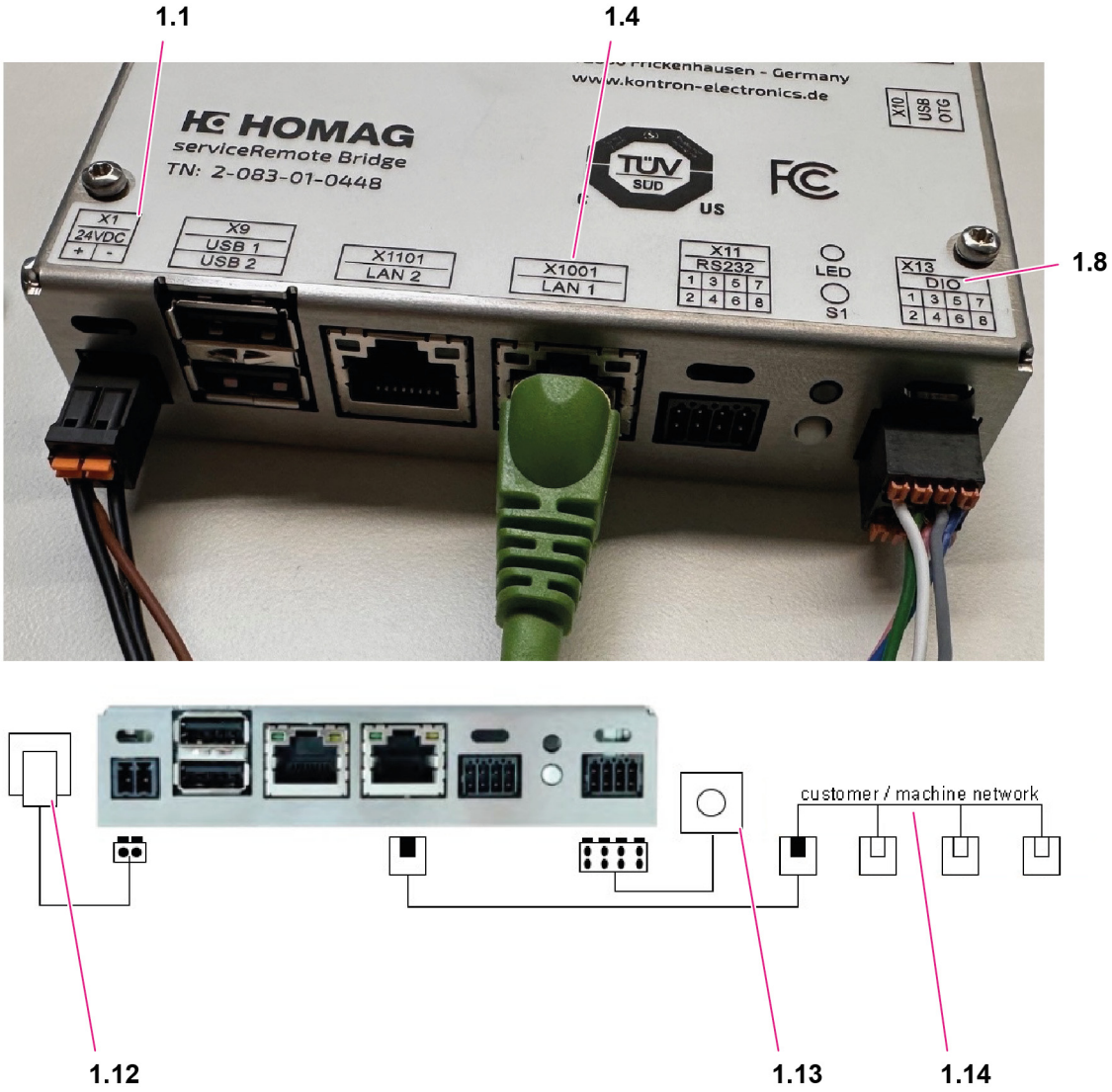
- *Windows 10*
- *Windows 7*
- *Windows XP*


Client
TSN Router
customer / machine network
Communication
sR Bridge
Data
NAT1
NAT2
HOMAG
serviceRemote Starter
serviceRemote Bridge Starter
On each machine

4.4 Connecting accessories

Connect the lines according to the instructions.

The *sR Bridge* starts automatically when connected to the socket via the supplied power supply.



1.1	Connection X1, 24 V power supply
1.4	X1001, LAN1 connection
1.8	Connection X13, DIO connection for external button
1.12	Power supply unit in socket
1.13	External button
1.14	Network

➢ Connect the external button **1.13** at the connection for the external button **X13** (**1.8**).

The external button **1.13** can be moved as required. Cable length: 25 m

The cable can be extended to a maximum of 400 m with the same cross-section.

- Connect the *sR Bridge* via connection **X1001**/**LAN 1** (**1.4**) to the hall network **1.14** or, for HOMAG cells, connect to a free machine LAN connection on the HOMAG Internet router.

  There must be a connection to the Homag Cloud.
- Connect the supplied power supply unit to the power supply connection **1.1** on the *sR Bridge*.
- Close unused connections with dummy plugs.
- Plug the supplied power supply unit into the socket **1.12** using the correct adapter.

  ⇨ The *sR Bridge* starts automatically.

4.5 Mounting in the holder



- Engage in the DIN rail.

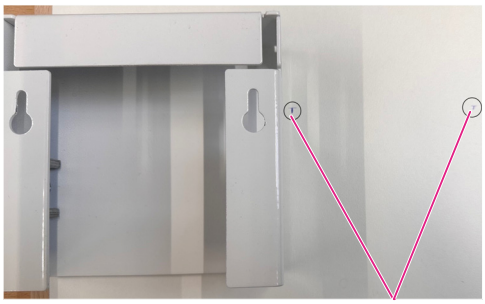
  The joint bar for unhooking must point downward.

- The accessories can be inserted before or after assembly.

4.6 Mounting on the wall

- Mark the positions of the bore holes **3.1**.
- Drill holes.

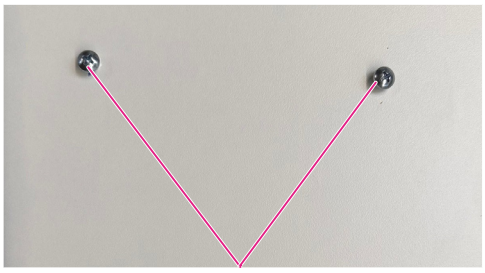
  Drill: 6 mm
- Insert the dowels.



3.1

- Tighten screws **3.2** with a screwdriver.

  Approx. 3 mm from the wall



3.2

- Hang the holder on screws **3.3**.
- Remove the protective film from the Homag logo.



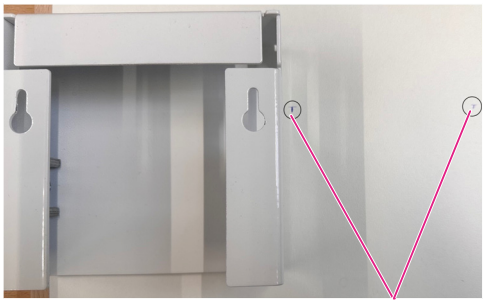
3.3

4.7 Mounting on the machine protection cover

Note

Check the rear side of the machine protection cover before marking the positions of the self-tapping screws. There must be no parts on the rear side.

➢ Mark the positions **3.1** of the self-tapping screws.

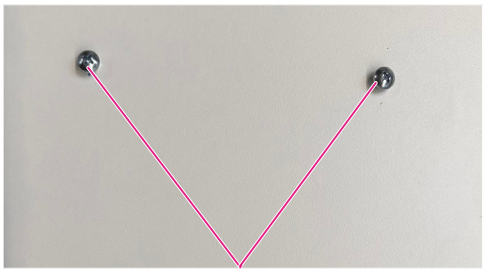


3.1

➢ Screw in self-tapping screws **3.2**.

Self-tapping screws are self-tapping. Holes are not necessary.

Approx. 3 mm from the wall



3.2

- Hang the holder on screws **3.3**.
- Remove the protective film from the Homag logo.



4.8 Mounting in the TSN junction box in the switch cabinet



Pic Installation in the switch cabinet (example)

Note
When the machine is switched off, the *sR Bridge* is no longer powered. Other connected machines can no longer be reached.

Attention

Device may heat up and overheat.
Equipment damage

- Maintain a distance of 15 mm at the side.

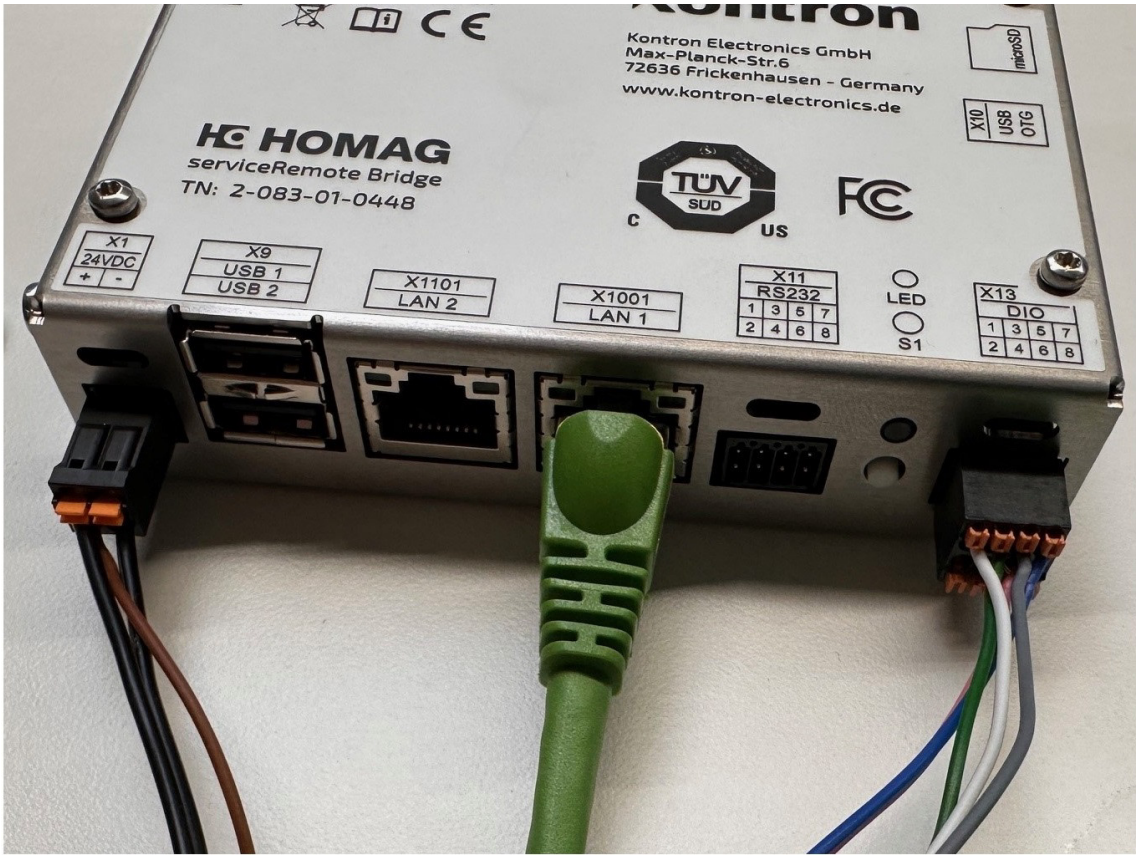
Danger

Danger from electrical current.
Risk of fatal injury!

- Refer to the safety regulations for production equipment manufactured by HOMAG.
- The following operations may only be carried out by qualified electricians or trained service personnel.

➢ Mount the *sR Bridge* on a DIN rail.

4.9 Mounting without holder



Pic Mounting without holder (example)

The *sR Bridge* can be deposited without a holder.

Attention

Device may heat up and overheat.
Equipment damage

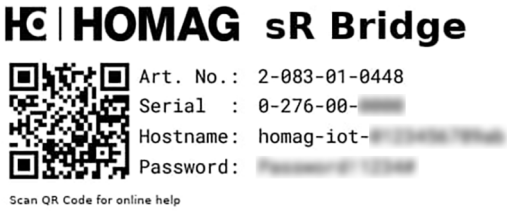
- Leave the ventilation slots on the rear side open. Do not cover!

5 Set up network

5.1 Change device password

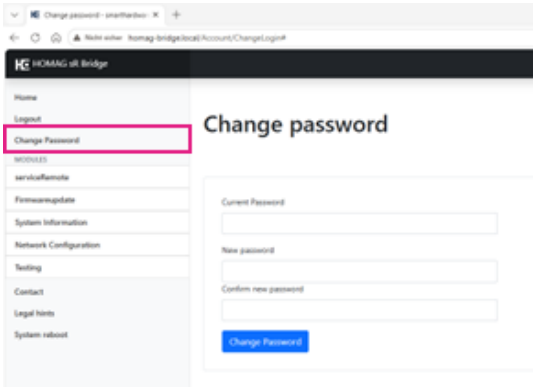
The device is supplied with an individual device password.

The device password can be found on the type plate.



➢ Change the device password after successful login via the local diagnostic page.

See also chapter "Accessing the sR Bridge diagnostic page."



5.2 Settings on the customer network/firewall

Internet settings

Priority	Port	Log	Log Name	Description
Required	123	UDP	NTP	Access to the time server provided by the DHCP server. No secure connections can be established without NTP because certificates cannot be validated.
Required	53	UDP	DNS	Domain Name Service – name resolution on the Internet. This log is used to specify Internet addresses (e.g. https://homag.com or http://serviceremote.net) in IP addresses.
Required	443	TCP	HTTPS	Encrypted connection to the Internet. Required for connecting the HOMAG Cloud services.
Optional*	13	ICMP	ICMP	Outgoing pings are required to check the connection to the Homag Cloud services.

*These ports are not required to operate the *sR Bridge* and are used for diagnostics and analysis in support cases.

5.3 Settings for the internal network

The *sR Bridge* has various diagnostic services that should be accessible in the local network. We recommend making these services available only on the internal network.

Priority	Port	Log	Log name	Description
Required	80 (45001)	TCP	HTTP	Local diagnostic page of the *sR Bridge*
Required	37001	TCP/UDP		Discovery Service for the device pairing process. Communication between the machines and the *sR Bridge*
Optional*	5353	UDP	mDNS	Multicast DNS service to provide the *sR Bridge* name on the local network
Optional*	5355	UDP	LLMNR	Link Local Multicast Name Resolution; allows hosts to perform name resolution for devices on the same LAN
Optional*	13	ICMP	ICMP	Incoming pings to check if the *sR Bridge* is online. Attention: Only one ping is allowed per second!
Optional*	22	TCP/UDP	SSH	The SSH service is disabled by default and must be manually enabled through the diagnostic page. In the case of local maintenance or remote maintenance, the service employee can activate the function manually. When the SSH service is enabled, the status is displayed on the diagnostic pages and via the status light

* Optional: These ports are not required to operate the *sR Bridge*. The ports are active for support cases or analyzes.



5.4 Required URLs

Used for	URL	Description/information
HOMAG serviceRemote	https://api.serviceremote.net https://dispatcherde01.servicere-mote.net https://dispatcherus01.servicere-mote.net https://dispatchersea01.servicere-mote.net	API for serviceRemote Data connection for serviceRemote
HOMAG sh-core API	https://smarthard-ware-core.homag.cloud	API for the firmware update
HOMAG Storage	https://dfshcoreprdeu01sa.blob.core.windows.net/* https://osu-cdn.homag.cloud https://smarthard-ware-storage.homag.cloud	Data storage of firmware updates
Time synchronization (fallback)	time.windos.com time1.google.com time2.google.com time3.google.com time4.google.com	The URLs serve as a backup function if no valid NTP server has been configured via DHCP or via the local configu-ration page.

5.5 Network settings for the sR Bridge

The network settings for the *sR Bridge* can be adjusted via the local diagnostic page under **Modules** in **Network Configuration**.

If special IP settings are required, manual adjustment is necessary.

The standard IP assignment is performed using the Internet router via DHCP.

DHCP = automatic assignment of the IP address.



Note

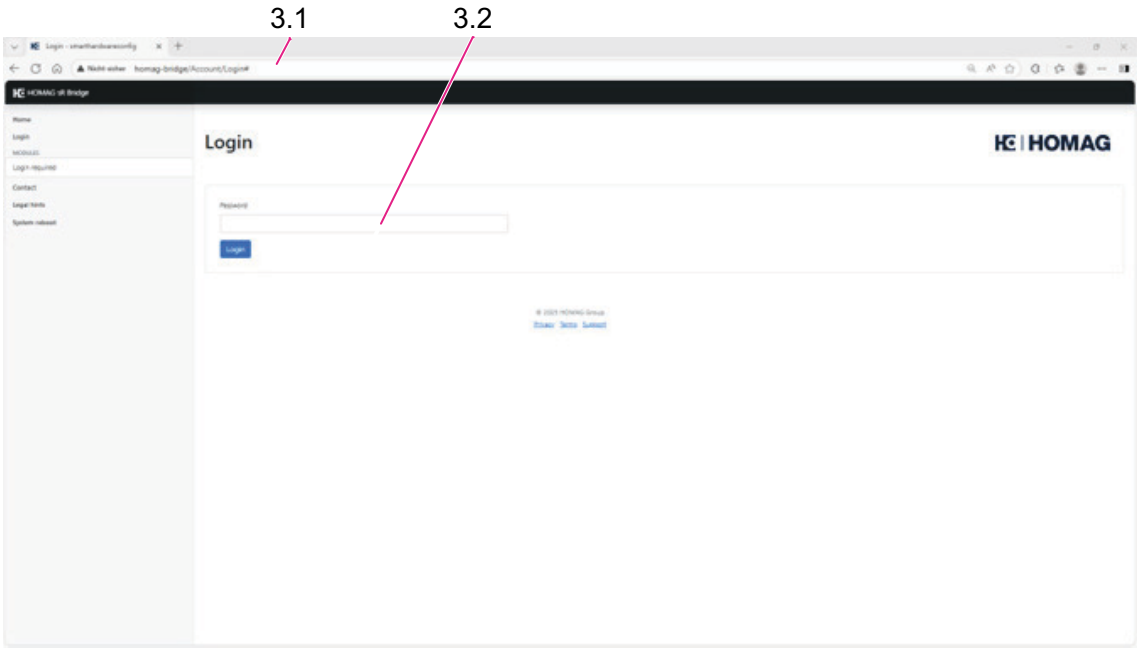
If DHCP is disabled on the network, access to the diagnostic page is restricted. DHCP activation during commissioning is recommended. If the configuration is incorrect, the function of the *sR Bridge* is not guaranteed.

- Activation is described in chapter "Troubleshooting."

For more information, see:

- https://docs.homag.cloud/sr-bridge/faq

5.6 Call up the diagnostic page of the sR Bridge



3.1	Address line
3.2	Password

- In the default browser, enter the host ID or IP address in the address bar **3.1**.

  The host ID is located on the rear side of the device or on the label that came with it.
- Press the *Enter* key.
- Enter the password **3.2**.

  The password can be found on the rear side of the device or on the label provided.
- Press the *Enter* key.

5.7 Settings on the diagnostic page of the sR Bridge

The network settings can be found under **Network Configuration 3.5**.

Hostname: Change host name of sR Bridge

- The host name of the *sR Bridge* is made up as follows in the delivery condition:

  Homag-iot<mac address>

- The host name of the *sR Bridge* is sufficient to call up the local diagnostic page. Knowledge of the IP address is not necessary.



Note
If you have Internet or network problems, you may want to use the host name to access it.



Note
If domains are configured on the network, the following pattern is used:

- <hostname>.<domain>

DNS: Adapt the name server for the sR Bridge

- The name server translates the host names on the network into an IP address. In small networks, this is the Internet router. For larger networks, a separate DNS server is often operated.

Default gateway

- The default gateway is a node in the network. The default gateway enables the *sR Bridge* to access the Internet. The Internet router is the gateway by default.

NTP server: Time server

- If a time server exists in your own network, it can be configured. Some DHCP servers provide this automatically, so no configuration is necessary. If an NTP server is present in the network, it must be ensured that the following NTP protocols are enabled in the firewall:

  - time.windows.com
  - time1.google.com

- time2.google.com
- time3.google.com
- time4.google.com

Network domain

- The domain is a network area in which the user receives the security guidelines or user rights according to the organizational structure.

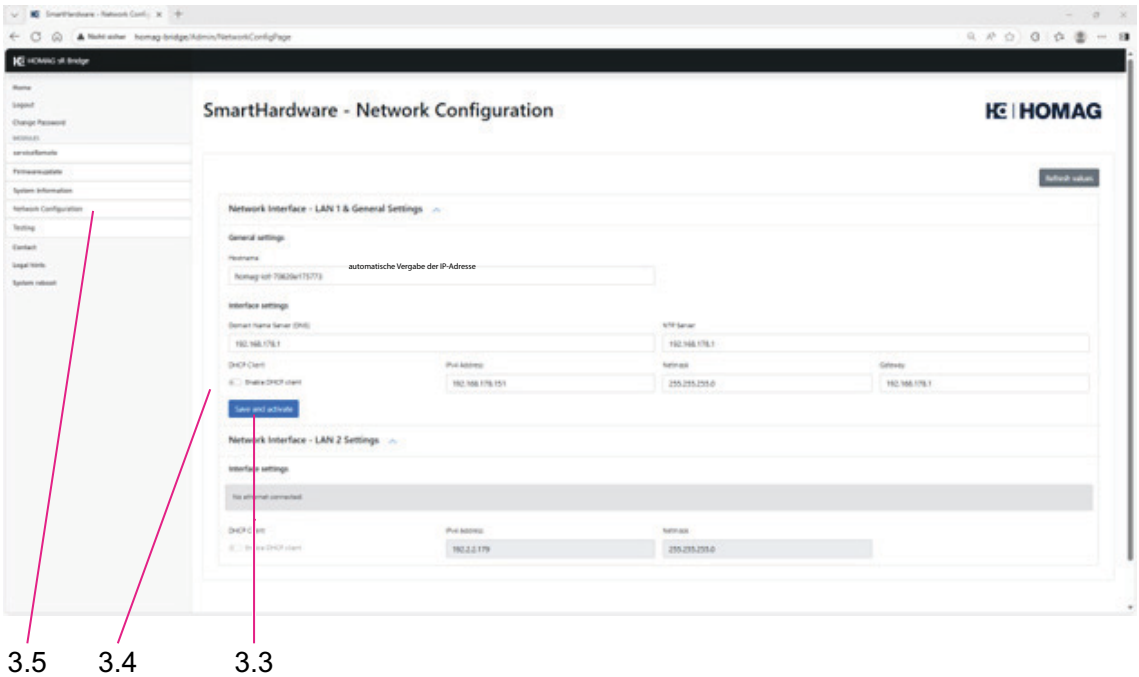
  If a domain exists in the network, this can be configured via the setting options.

  Depending on the configuration, the name resolution of the *sR Bridge* must contain the domain. The following template must be observed:

  - <hostname>.<domain>

DHCP/static network settings

Note
The settings for the **LAN 2** network adapter must not be changed!



3.3	Save and activate
3.4	Enable DHCP client
3.5	Network Configuration

The network configuration can be carried out automatically via DHCP. A static network configuration must be created manually.



Note

If DHCP is disabled on the network, access to the diagnostic page is restricted.
DHCP activation during commissioning is recommended. If the configuration is incorrect, the function of the *sR Bridge* is not guaranteed.

- With **Enable DHCP client 3.4**, DHCP can be enabled (or disabled).
- Only after saving and activating with **Save and activate 3.3** are the network settings applied.



Note

The factory settings can be used to reset to the standard configuration (see chapter "sR Bridge — Resetting to factory settings").



Note

As soon as the *sR Bridge* has a connection to the Internet, it connects to the HOMAG server immediately and automatically installs the latest firmware, if available.
This can be seen by the signal LED (see chapter "Buttons and LEDs").
If the device signals that the update has been performed, disconnect the *sR Bridge* from the power once (unplug the power supply unit) and switch it on again (plug the power supply unit back in).

5.8 sR Bridge firmware update

HOMAG regularly provides security updates for the *sR Bridge* as required by law.

These are installed automatically in the default configuration. The device checks an update server at regular intervals and installs available updates independently. After installation, the device must be restarted.

The local diagnostic page can be used to disable automatic firmware updates.

In this case, firmware updates must be installed manually via the local diagnostic page after successful login.

5.8.1 Disabling automatic firmware updates

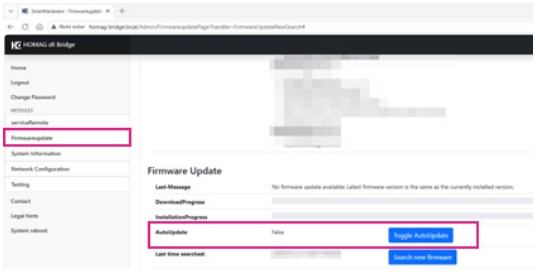
In most application cases, it is not necessary to disable the automatic firmware update. Instead, disabling increases the risk that security gaps will not be closed or will only be closed late.

However, it is possible to disable automatic firmware updates.

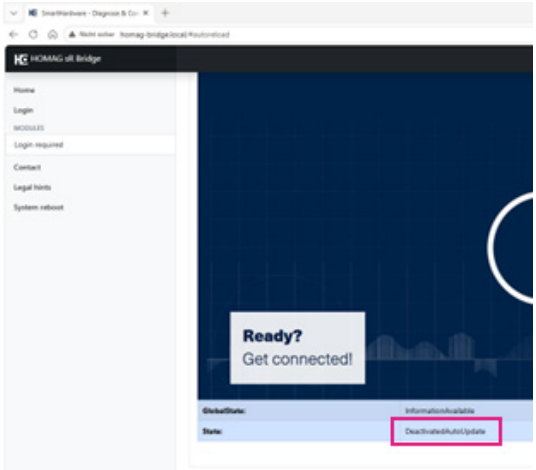
- ➢ Log in to the diagnostic page via **Login** to be able to deactivate automatic firmware updates.
- ➢ Select **Firmware update**.
- ➢ For **AutoUpdate**, select the **Toggle AutoUpdate** button and confirm the dialog.

  The status changes back and forth between **True** (enabled) and **False** (disabled) with each actuation.

  - ⇨ The status of **AutoUpdate** changes to **False** (disabled).
  - ⇨ The **DeactivatedAutoUpdate** status is displayed on the home page of the local diagnostic page even without logging into **State**.



Pic Disabling automatic firmware updates



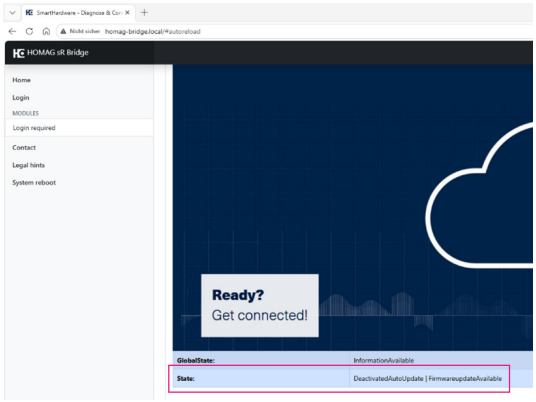
Pic Automatic firmware updates disabled (home page)

5.8.2 Manually perform the firmware update via the diagnostic page

The *sR Bridge* periodically checks whether a firmware update is available, regardless of whether automatic firmware updates are enabled or not.

If an update is available, this is already displayed on the home page in **State** as the status **Firmware update available** without logging in and under **Firmware update** after successfully logging in.

If automatic firmware updates are disabled, they are only not automatically installed. In this case, the update must be started manually.



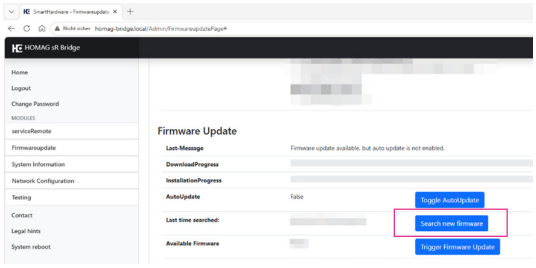
Pic Firmware update available (home page)

The check for new firmware updates can also be carried out manually via the local diagnostic page at any time after successful login.

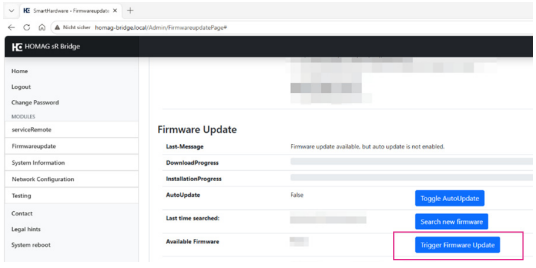
- ➢ Log in to the diagnostic page via **Login** to search for firmware updates and start them.
- ➢ Select **Firmware update**.
- ➢ To search for firmware updates, under **Last time searched**, select the **Search new firmware** button.

  Not necessary if an available update is already displayed.

  ⇨ If available, a firmware update is displayed.
- ➢ To start an available update, select **Trigger Firmware Update**.



Pic Manually search for a firmware update



Pic Starting the firmware update



6 "sR Connect" machine update

The following chapter describes the *sR Connect* machine update. The update must be performed and installs the latest *serviceRemote Starter* software version.

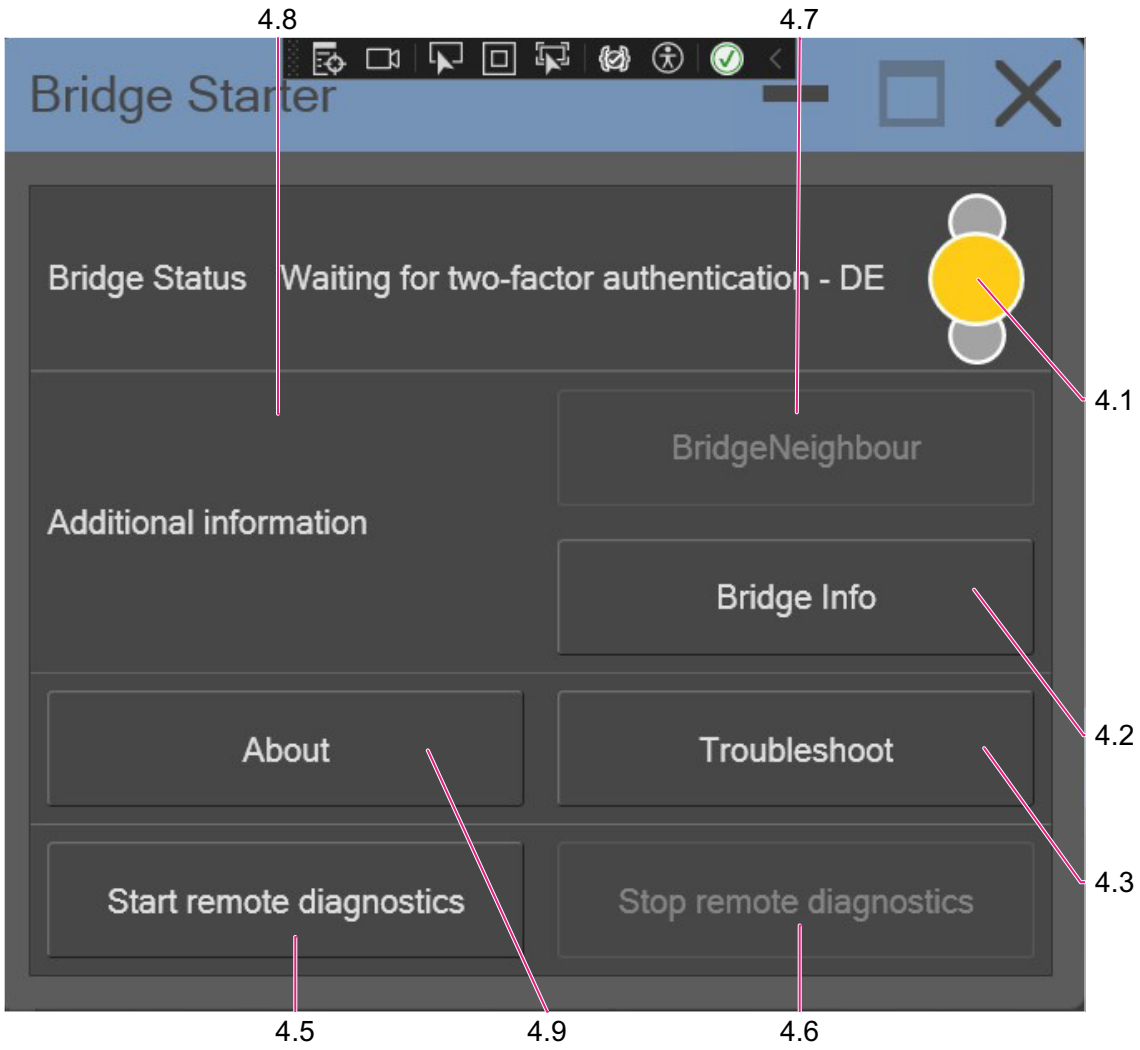
➢ Download the *sR Connect* update and save it on the machine.

The link will be sent by email as soon as the *sR Bridge* is ordered.

Info: *HOMAG Update Agent* is free software for downloading and then installing software updates for machines from Homag.

https://docs.homag.cloud/datenaustausch/homag-update-agent/ueberblick

6.1 Functions of serviceRemote Starter Premium

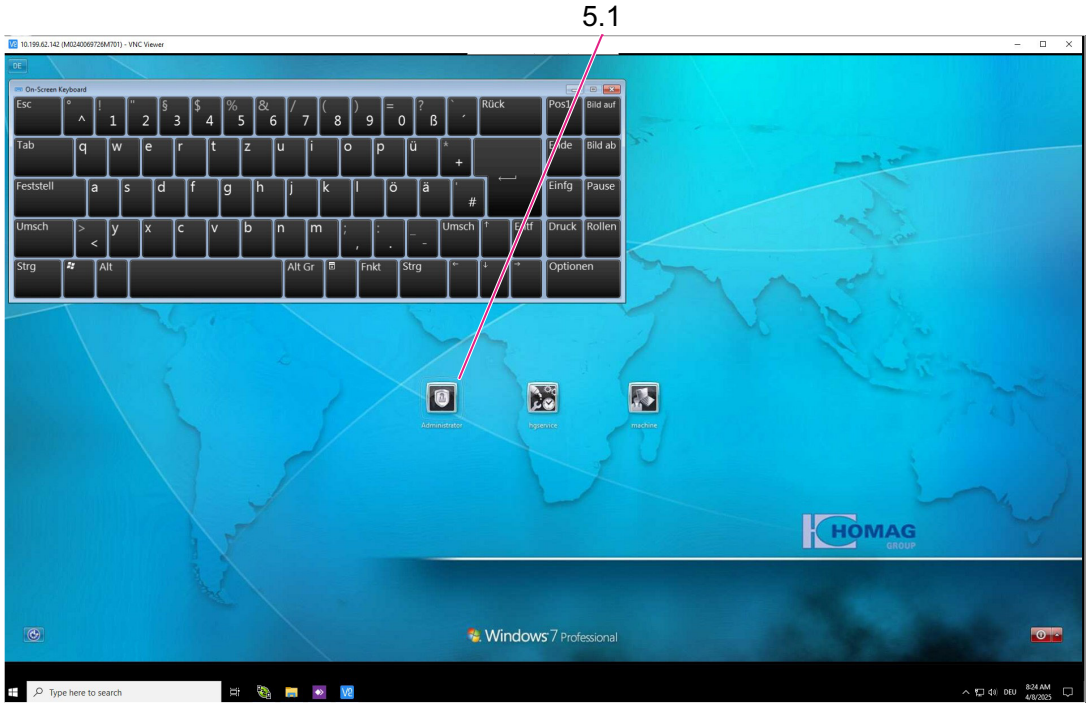


Button	Function
Bridge Status green **4.1**	Connection status OK
Bridge Status yellow **4.1**	2-factor authentication pending
Bridge Status red **4.1**	Connection status not OK
Bridge Neighbour **4.7**	To link the machine to the *sR Bridge*, run **Bridge Neighbour** once.
Bridge Info **4.2**	
Additional information **4.8**	Additional information
About **4.9**	Device information
Troubleshooting **4.3**	Debugging
Start remote diagnostics **4.5**	Starts remote diagnostics
Stop remote diagnostics **4.6**	Stops remote diagnostics

6.2 Install update

Administrator rights are required for the update.

On the machine, switch to the *Admin* user.



5.1 Logging in as Administrator

Note

After changing the user, transfer the update to the machine and execute it.

6.3 serviceRemote Starter Premium

Suitable for operating system:

- *Windows 10*

Note
Functionality with *Windows 7* is not guaranteed due to dotNet issue.

- ➢ Start login as administrator.
- ➢ Open the Update folder.
- ➢ Install update.
- ➢ After installation, log in as a machine user.
- ➢ Open and start the menu for remote diagnostics via *powerTouch*.
  - ➢ Select **powerTouch**.
  - ➢ Select **Other apps**.
  - ➢ Select **Remote diagnostics**.
  - ➢ Start **Remote diagnostics**.

  ⇨ Confirm the message.

6.3.1 Pairing mode (Starter Premium)

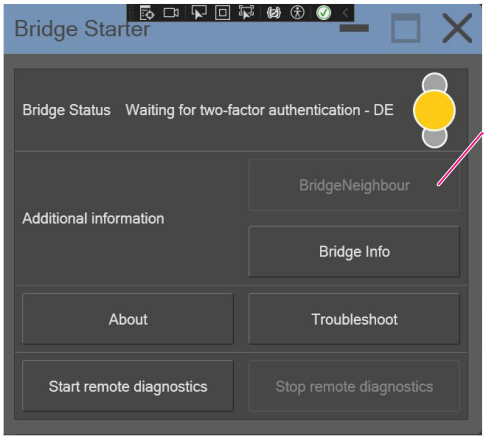
Note
The following steps must be carried out for each machine.

- ➢ Put the *sR Bridge* into pairing mode.
  - ➢ Press and hold the internal button on the *sR Bridge* for 15 seconds.

  ⇨ LED flashes magenta.

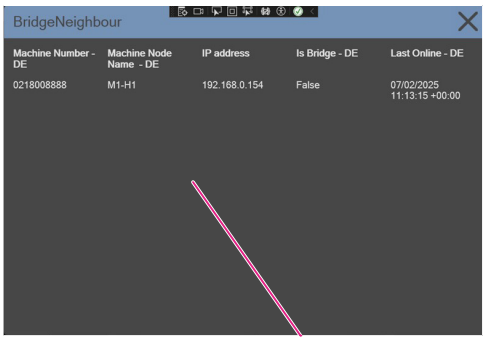
  ⇨ New machines can be integrated for 15 minutes.
- ➢ Start remote diagnostics on the machine.

Note
When the machine is first paired with the *sR Bridge*, a configuration file is exchanged between the machine and the *sR Bridge*. In addition, the machine is automatically created on the HOMAG server. It may be necessary to pair the machine a second time so that this process can be completed on both sides.



6.1	BridgeNeighbour

- Select **BridgeNeighbour 6.1**.
  - ⇨ Machine searches for *sR Bridge* in the network.
  - ⇨ This may take a few minutes.
- When the machine and the *sR Bridge* have found each other, a popup window **6.2** is displayed.
- Select **"OK"** to confirm.



6.2

6.2 Window with connected devices

6.4 serviceRemote Starter Classic

The *serviceRemote Starter Classic* update is suitable for older operating systems.

Operating systems include:

- *Windows 7*
- *Windows XP*
- *Windows NT*

The update replaces existing scripts in the background. The remote diagnostics starts and stops with the softkeys.

➢ Download the *sR Connect* machine update.

The link can be found in the sent email.

Further information:

- https://docs.homag.cloud/datenaustausch/homag-update-agent/ueberblick

➢ If it is not possible to download the update on the machine, a USB stick or the internal network can be used.

6.4.1 Pairing mode (Starter Classic)

Note
The following steps must be carried out for each machine.

➢ Put the *sR Bridge* into pairing mode.

➢ Press and hold the internal button on the *sR Bridge* for 15 seconds.

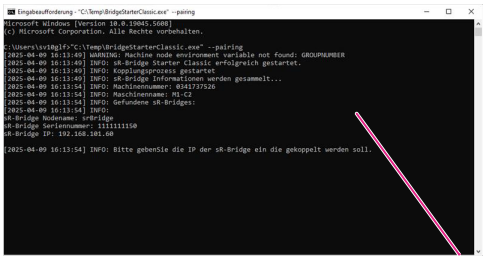
⇨ LED flashes magenta.

⇨ New machines can be integrated for 15 minutes.

➢ Start remote diagnostics on the machine.

⇨ *Command Box*. **6.3** is displayed.

⇨ Available *sR Bridge*s in the network are listed.



6.3

6.3 Command box

- Enter the IP address of the *sR Bridge* to be connected.
  - Press the *Enter* key.



Note

When the machine is first paired with the *sR Bridge*, a configuration file is exchanged between the machine and the *sR Bridge*. In addition, the machine is automatically created on the HOMAG server. It may be necessary to pair the machine a second time so that this process can be completed on both sides.

6.5 Linux

Connecting machines with a *Linux* operating system is a bit more complicated.

The IP address of the machine must be static. It must not be set to DHCP.



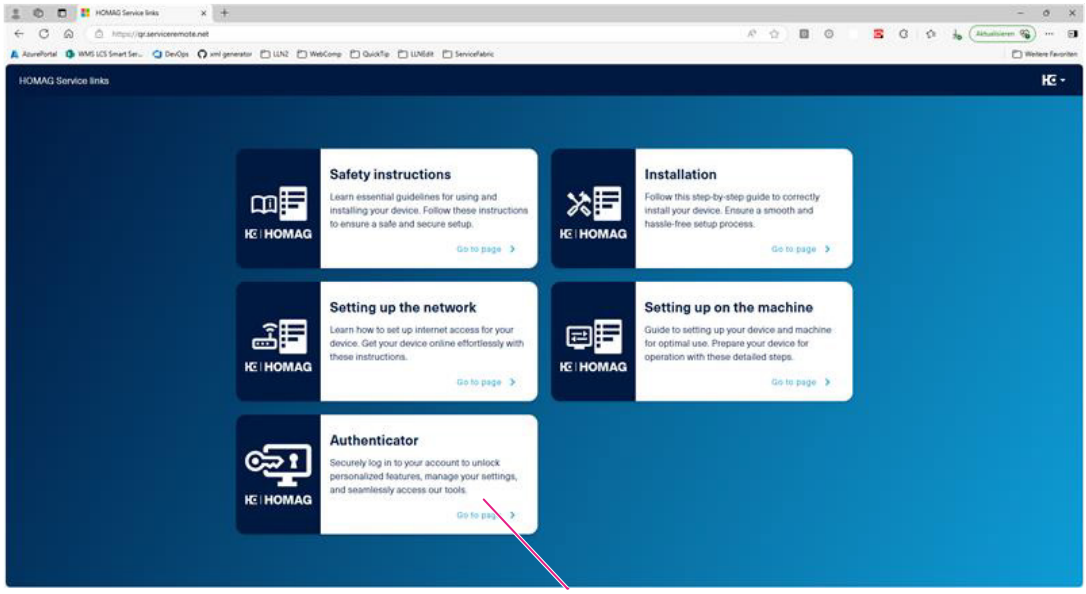
Note

The static IP address must be communicated to HOMAG. This is stored with the machine. Only then are remote diagnostics possible.

Remote diagnostics are then activated using the *sR Bridge* button.

There is currently no machine update for *Linux* in order to retain the old remote diagnostics functionality.

6.6 Setting up two-factor authentication (2FA)



7.1	Authenticator

➢ Scan the QR code on one of the enclosed labels.

⇨ The default browser starts.

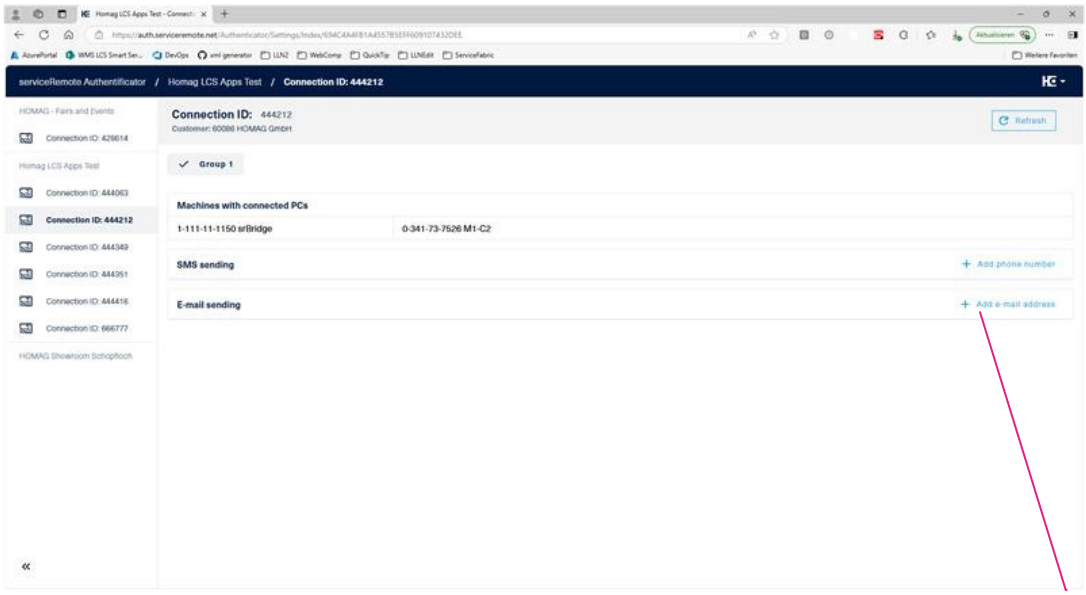
Note

Two-factor authentication can be selected in the countries in which tapio registration is available. Countries can be viewed at the following link:

⇨ https://docs.homag.cloud/sr-bridge/kurz-erklaert/regionale-verfuegbarkeit

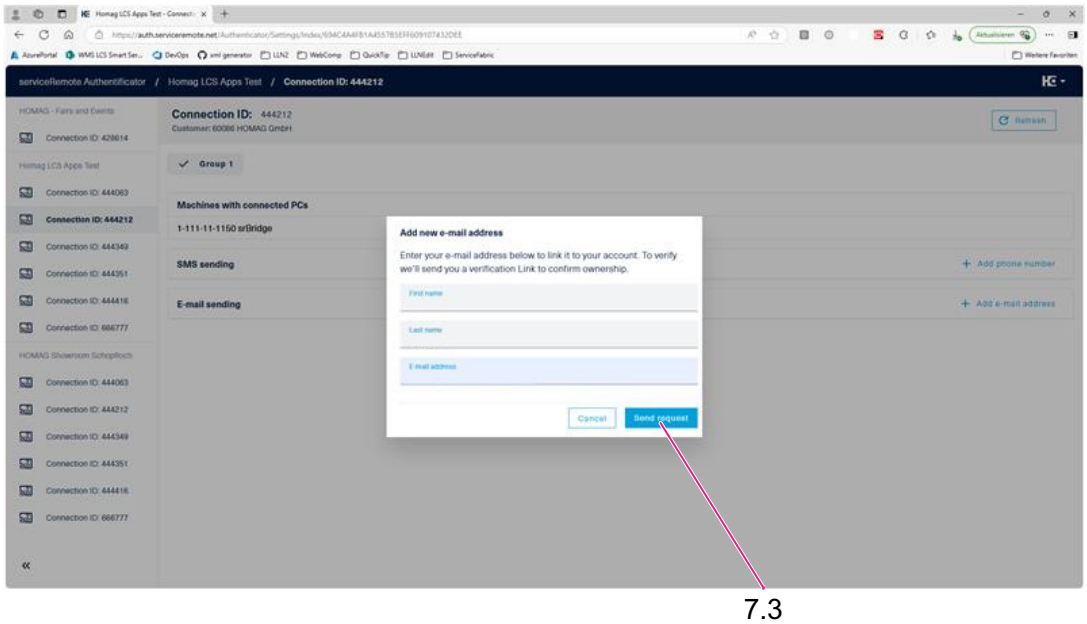
Phone numbers cannot be added yet.

➢ Navigate to the **Authenticator 7.1** home page.



7.2 Enter email address.

- Log in with tapio account.
  - ⇨ Existing *sR Bridge* devices are displayed.
- Select the desired device and select **Add email address 7.2**.



7.3 Send Request

- Enter first and last name and email address.

➢ Select **Send Request 7.3**.

⇨ An email will be sent to the specified address requesting confirmation.



Note

Only after confirmation will emails for two-factor authentication be sent in future.

7 Button and LED

To avoid operating errors as much as possible, the functions of the buttons and the displays of the LEDs have been adapted.

During the desired function, the respective button must be pressed continuously.

If the button is released, the function will stop.

7.1 Internal button and LED color

Function	Actuation Duration	LED Color	LED Code	Explanation
Start /Stop Remote Diagnostics	> 3 seconds	Blue	Flashing	Starts or stops the Remote diagnostics.
Device restart	> 10 seconds	Turquoise	Flashing	The device restarts.
Pairing mode	> 15 seconds	Magenta	Flashing	The device goes into setup mode. Machines can be connected to the device.
Reset	> 25 seconds	Red	Flashing	The device is Factory Settings .
Exit	> 30 seconds	White	Permanent	No function order.

Function	LED Color	LED Code	Explanation
Feedback "successful"	Green	Short, fast flashing	Activation of a function was successful.
Feedback "unsuccessful"	Red	Short, fast flashing	Activation of a function failed.

7.2 External button and LED color

Function	Actuation Duration	LED Color	LED Code	Explanation
Start /Stop Remote Diagnostics	> 3 seconds	Green	Flashing	Starts or stops the Remote diagnostics.
Exit	> 10 seconds	None	None	No function order.

7.3 LED status displays

Status	Internal ID Color, code	External LED Color, code	Explanation
System start	Turquoise, Flash	Turquoise, Flash	Device starts
Errors: • System not ready • Network error. No local diagnostic page available if flashing fast • For more information, see local diagnostic page. If flashing normally	Yellow, fast flashing Yellow, Flash	Yellow, fast flashing Yellow, Flash	• No network cable connected • No connection to the network • No IP address • Internet error • NTP error
Remote Diagnostics ready to connect	Blue, fast flashing Green fast flashing	Green, fast flashing Green fast flashing	• Waiting for connection to be established • Wait for Establishing a connection group 1
Remote diagnostics connected	Blue Green	Green Green	• Active remote shooting • Active remote shooting Group 1
Error: system not ready	Yellow	Yellow	• Error • Error with tapio Cloud connector
Ready	Magenta	Magenta	Pairing mode activated
Ready: • Operator intervention necessary • Firmware update running • Restart required	White, Flash	White, Flash	Operator intervention necessary
Ready	White	White	Ready

8 Creating machine groups

Machines can be assigned to machine groups.

The group function allows certain functions to be sent to all machines in a group.

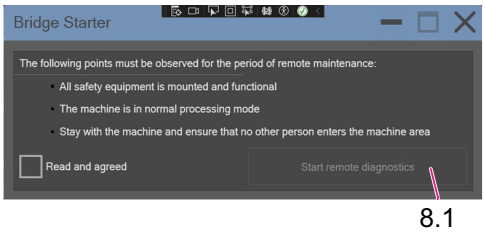


Note

On delivery, each machine is assigned to machine group 1.

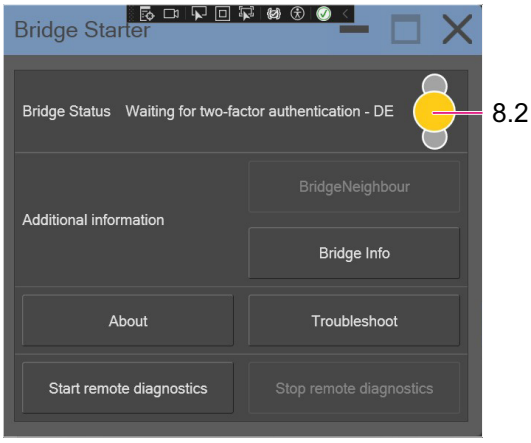
9 Start remote diagnostics

9.1 Starter Premium



8.1	Start remote diagnostics

- ➢ Open and start the menu for remote diagnostics via *powerTouch*.
  - ➢ Select **powerTouch**.
  - ➢ Select **Other apps**.
  - ➢ Select **Remote diagnostics**.
  - ➢ Start **Remote diagnostics**.
- ➢ Confirm the message.
- ➢ Select **Start remote diagnostics 8.1**.
  - ⇨ Two-factor authentication pop-up window **8.2** is displayed.



8.2	Waiting for two-factor authentication confirmation

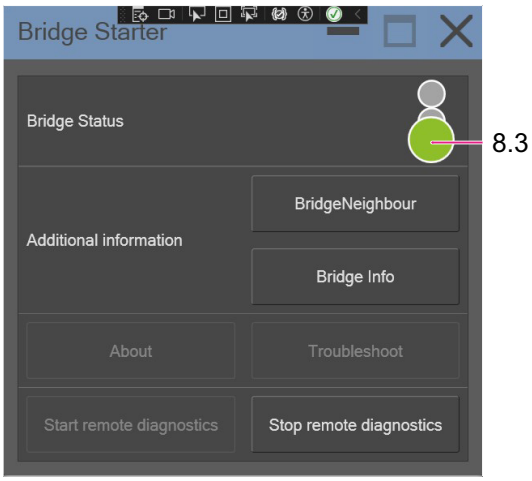
➢ Confirm two-factor authentication.

⇨ Display **8.3** turns green.



Note

For operating systems from *Windows 10* or later, a colored frame is displayed around the screen.



8.3	Two-factor authentication is confirmed

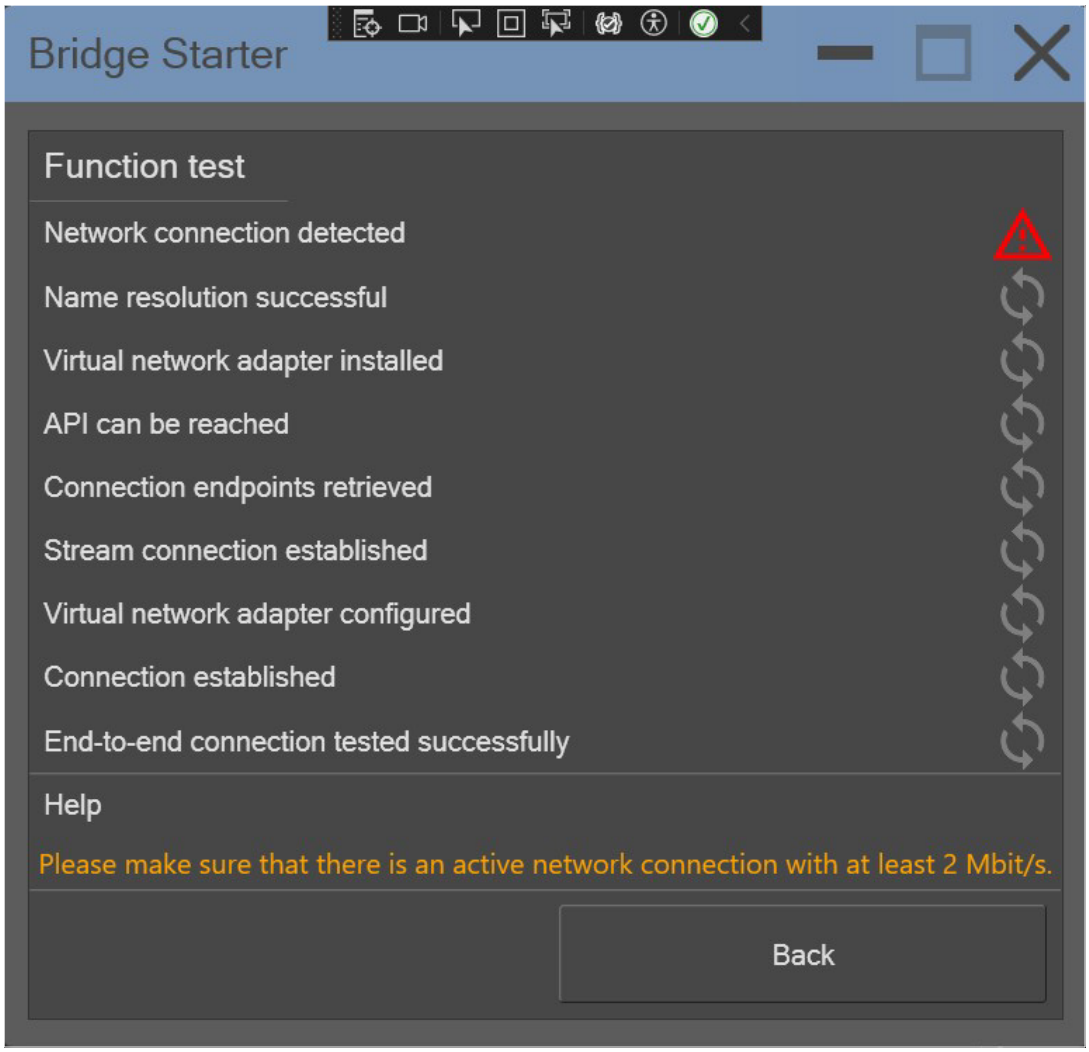
9.2 Starter Classic

With *serviceRemote Starter Classic*, remote diagnostics are started and stopped via the existing links.

9.3 Sensing device

- Press the internal button or external button for at least 3 seconds.
  - ⇨ Remote diagnostic is started.
  - ⇨ The LED shows the status of the remote diagnostics.

9.4 Function test



➢ Select the **Troubleshoot** function on the *Bridge Starter*.

⇨ Function test starts. Various functions are queried and the results are displayed as status.



10 Log

The log can be viewed in *service Assist*.

More information on *serviceAssist*:

- https://docs.homag.cloud/serviceassist/tutorial/erste-schritte

10.1 sR Bridge logs

There are system events that require continuous logging.

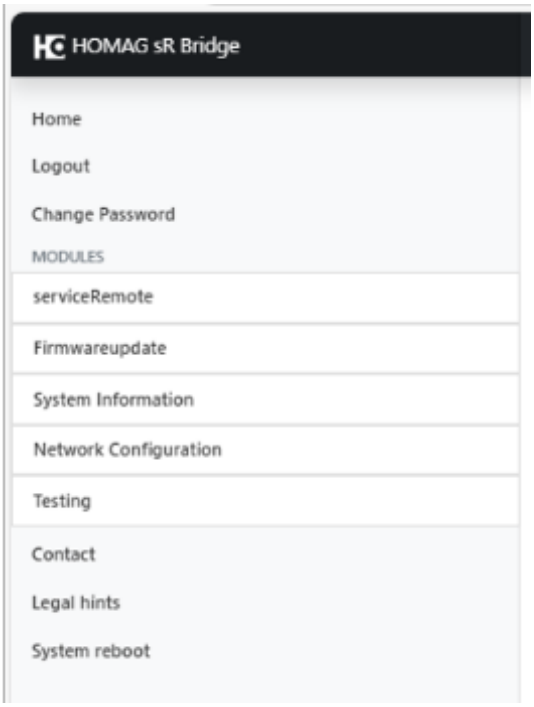
Note
These log entries are not deleted when the system is restarted.

Note
Log entries of system events older than six months are automatically deleted.

Note
Resetting to factory settings deletes all log entries.
In this case, the system reset is recorded as a new, first event in the log.

The log can be accessed via the local diagnostic page under **System Information**.

Examples of system events are:



Pic Local diagnostic page menu

Component	System event	Trigger
Firmware Update	Performing firmware updates	Local diagnostic page, auto-update
	Enabling/disabling automatic updates	Local diagnostic page
	Resetting the firmware	Local diagnostic page
Configuration update	Retrieving new configurations from the cloud	Local diagnostic page, auto-update (initial customer commissioning)
System service	Performing network settings	Local diagnostic page
	Change password	Local diagnostic page
	Enabling SSH connection	Local diagnostic page, HOMAG Service USB stick
	Enabling/disabling *Cloud Connector*	Local diagnostic page
	Resetting to factory settings (after deleting the log)	Local diagnostic page

11 Maintenance and care



Note

The device must be switched off. To do this, simply unplug the power supply unit.

11.1 Cleaning

- Clean the device with a clean, dry cloth if it is slightly dirty.
- Carefully remove dust from the surface of the housing and cooling fins with a soft brush.
- Remove stubborn dirt with mild cleaning agents and a soft cloth.

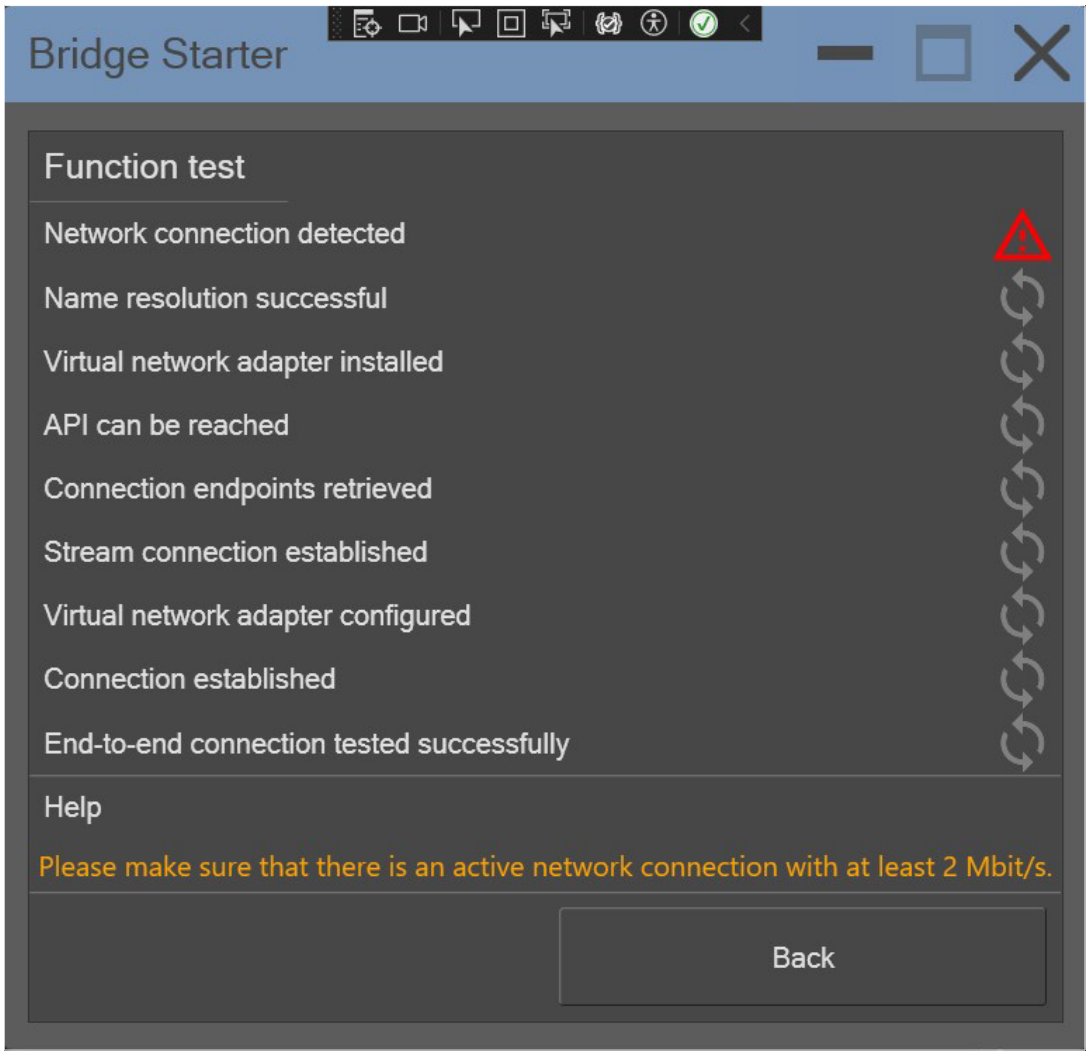
12 Troubleshooting

12.1 sR Starter — "Troubleshoot" function

Troubleshoot tests various functionalities and statuses.

The icons show the corresponding results.

Information about this is displayed under **Help**.



➢ Select **Troubleshooting**.

⇨ The function test starts.

12.2 sR Bridge does not have an IP address. How can it be accessed?

If the customer's DHCP server is disabled and cannot be enabled for initial startup, the following steps are possible:

- Access the *sR Bridge* via the LAN2 connection.

  LAN2 has an IP address of 192.2.2.179.

  This connection is permanently configured and cannot be changed.

  - LAN2 can be connected to the network.

    If you assign a machine a temporary IP address in the range 192.2.2.xxx, the *sR Bridge* can be accessed.

- Make the necessary network settings.
- After completing the settings, reconnect the *sR Bridge* to LAN1.

  If necessary, restore the original IP address of the machine.

12.3 sR Bridge — Diagnostic page cannot be opened

Depending on where the *sR Bridge* is installed in the network, the diagnostic page cannot be opened via the host name. This is due to network settings or network routes that do not support name resolution.

➢ Use the IP address of the *sR Bridge* instead of the host name.

The local diagnostic page can also be accessed via the second LAN connection. This has the static IP address: 192.2.2.179.

12.4 Resetting sR Bridge to factory settings

If the access data is lost, the device can be reset to the factory settings.



Note
Caution: All settings and logs will be lost.

- ➢ Press and hold the internal button for 25 seconds.
  - ⇨ The LED on the device flashes red.
  - ⇨ The device is reset to the factory settings (delivery condition).
- ➢ Set up the device again with access data on the rear side.

12.5 Enter NTP time server

There must be connection to a time server. The *sR Bridge* has various time servers stored.

As long as the time servers are accessible, a connection to the HOMAG Group server can be established.

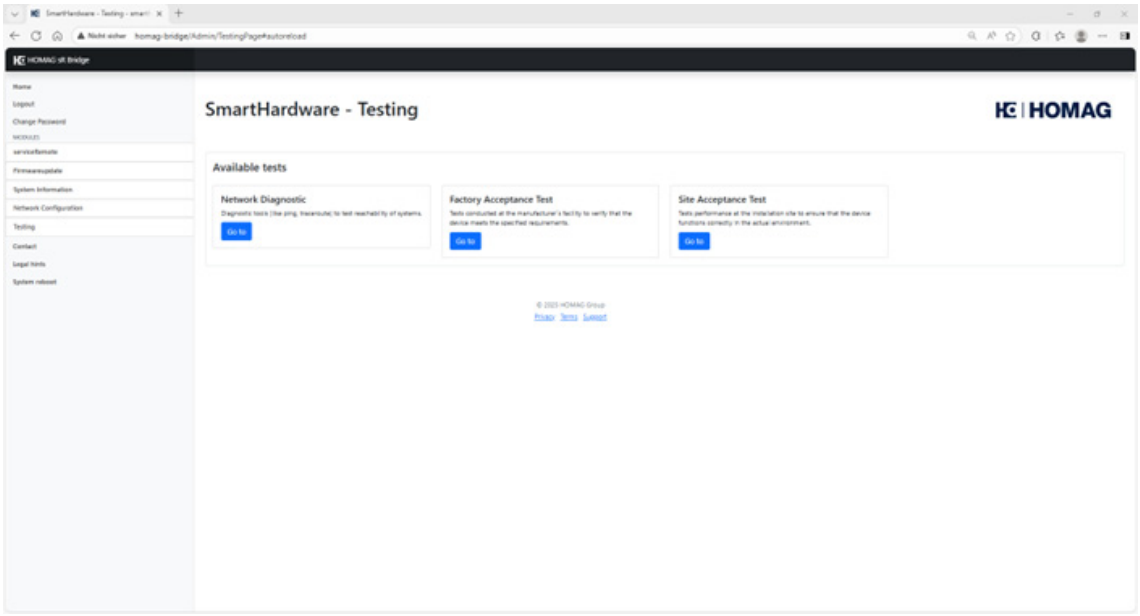
The diagnostic page allows you to enter your own time servers (see chapter "Settings on the diagnostic page of the *sR Bridge*").

The time server functions as a security module and cannot be deactivated.

12.6 If there are network problems, perform network diagnostics

In the event of network problems, the local diagnostic page can help diagnose the problem using various tools.

The available tools can be accessed from the local diagnostic page in **Testing**.



Pic	Local diagnostic page, testing

Note
Other helpful tips:
https://docs.homag.cloud/sr-bridge/faq

12.7 Available functions in different countries

Variant A

The customer can log in to *tapio* and use the apps provided by Homag. The customer does not have access to the *tapio* shop and cannot buy apps there either.

Version B:

The customer can log in to *tapio* and use the apps provided by Homag. In addition, the customer has access to the *tapio* shop and can buy apps there.

Only version A is required for *serviceRemote (ISN)* and the *sR Bridge*. Version B also works.

The distinction was introduced with *serviceRemote (soft)* with the aim of ensuring that it can be used across the board as far as possible.



Note

If the *tapio* connections are disabled via the fire-wall settings, or if the *sR Bridge* and/or the machines are not registered with *tapio*, this can lead to loss of functionality.
This applies to *serviceRemote (ISN)* and *sR Bridge*.
Functions such as two-factor authentication, history, log files, etc. are affected with the *sR Bridge*.

Supported countries

African Federation:

- Algeria, Angola, Congo, Ivory Coast, Egypt, Ethiopia, the Gambia, Libya, Mauritius, Morocco, Namibia, Nigeria, Rwanda, South Africa, Tunisia

Asia:

- Armenia, Azerbaijan, Bahrain, Bangladesh, Georgia, India, Indonesia, Israel, Japan, Jordan, Kenya, Korea, Kuwait, Malaysia, Mongolia, Myanmar, Oman, Philippines, Qatar, Saudi Arabia, Singapore, Sri Lanka, Taiwan, Thailand, United Arab Emirates, Vietnam

Europe:

- Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, French Polynesia, Germany, Greece, Hungary,

Iceland, Ireland, Italy, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom

Persia:

- Iraq, Iran, Kyrgyzstan, Kazakhstan, Lebanon, Pakistan, Syria, Tajikistan, Uzbekistan

North America:

- Canada, Cayman Islands, Dominican Republic, Jamaica, Mexico, Panama, St. Lucia, United States

Oceania:

- Australia, New Zealand, Papua New Guinea

South America:

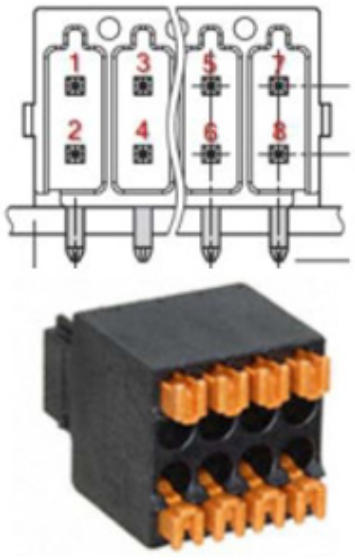
- Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, Suriname, Venezuela

13 Interfaces

13.1 External button/LED — pin assignment and power supply

DIO name	Pin	Designation
X13-DIO1	1	Output +24 V LED red
X13-DIO2	3	Output +24 V LED green
X13-DIO3	5	Output +24 V LED blue
X13-DIO1, 2.3	2, 4, 6 or 8	Ground for LED
X13-DIO4	7	Input +24 V signal button
X1	1	+24 V from power supply unit +24 V from button
X1	2	Ground of power supply unit

Pin	Signal Name	Pin	Signal Name
1	DOUT1/ DIN1 DOUT Imax= 800 mA	2	GND
3	DOUT2/ DIN2 DOUT Imax= 800 mA	4	GND
5	DOUT3/ DIN3 DOUT Imax= 800 mA	6	GND
7	DOUT4/ DIN4 DOUT Imax= 800 mA	8	GND



Pin	Signal name
1	VCC
2	GND

2-Pin Power

Mating Connector



1 (+) 2 (-)

13.2 Wiring diagram (example)

