User Guide

Browser on HMI Devices

Installation and Basic Settings

Translation of the original manual

Document 20432551 EN 00

Imprint

KEB Automation KG
Suedstraße 38, D-32683 Barntrup
Germany
Tel: +49 5263 401-0 • Fax: +49 5263 401-116
E-Mail: info@keb.de • URL: https://www.keb-automation.com

ma_mu_browser-hmi_20432551_en.pdf
Version 00 • Edition 10/04/2025

Table of Contents

1 Introduction

1.1 Markings

1.1.1 Warnings

Certain operations can cause hazards during the installation, operation or thereafter. There is safety information in the documentation in front of these operations.

Warnings contain signal words for the severity of the hazard, the type and/or source of the hazard, the consequence of non-compliance and the measures to avoid or reduce the hazard.

⚠ DANGER

Type and/or source of the hazard.

Leads to death or serious bodily injury if not observed.

a) Measures to avoid the hazard.

b) Can be supplemented by an additional danger sign or pictogram.

⚠ WARNING

Type and/or source of the hazard.

May cause death or serious injury if not observed.

a) Measures to avoid the hazard.

b) Can be supplemented by an additional danger sign or pictogram.

⚠ CAUTION

Type and/or source of the hazard.

May cause bodily injury if not observed.

a) Measures to avoid the hazard.

b) Can be supplemented by an additional danger sign or pictogram.

NOTICE

Type and/or source of the hazard.

Can cause damage to property if not observed.

a) Measures to avoid the hazard.

b) Can be supplemented by an additional danger sign or pictogram.

1.1.2 Information notes

Indicates to the user a special condition, prerequisite, scope or simplification.

This is a reference to further documentation. The barcode is for smartphones, the following link is for online users or for typing.

(🌐► https://www.keb-automation.com/search)

Notes on conformity for use in the North American or Canadian market.

1.1.3 Symbols and markers

✓	Condition

a)	Action step
⇨	Result or intermediate result
(≡► Reference [▶ 4])	Reference to a chapter, table or picture with page reference
ru21	Parameter name or parameter index
(🌐►)	Hyperlink
<Strg>	Control code
COMBIVERT	Lexicon entry

1.2 Warranty and liability

The warranty and liability on design, material or workmanship for the acquired device is given in the general conditions of sale.

Here you will find our general sales conditions.
(🌐► https://www.keb-automation.com/terms-conditions)

Further agreements or specifications require a written confirmation.

1.3 Copyright

The customer may use the instructions for use and other documents accompanying the device or parts thereof for internal purposes. Copyrights are with KEB Automation KG and remain valid in its entirety.

This KEB product or parts thereof may contain third-party software, including free and/or open source software. If applicable, the licence terms of this software are contained in the instructions for use. The instructions for use are already available, can be downloaded from the KEB website or can be requested from the respective KEB contact person.

Microsoft®, Win32, Windows®, Windows XP, Windows Vista, Windows 7, Windows 8, Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Google, Google Chrome

Other word and/or figurative marks are trademarks (™) or registered trademarks (®) of their respective owners.

The example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events shown are fictitious. No connection to any real company, organisation, product, domain name, email address, logo, person, place or event is intended or should be inferred.

1.4 Validity of this manual

These instructions for use are valid for the software with the corresponding version specified in the product description. It contains:

- Safety instructions
- Intended use
- Installation
- Description

1.5 Target group

The instructions for use is intended exclusively for persons who have the following qualifications:

- Knowledge and understanding of the safety instructions.

- Knowledge of PCs and the used operating system.
- Installing software.
- Understanding about the function of connected/ simulated devices/ models.
- Detection of hazards and risks of the electrical drive technology.
- Knowledge of automation technology.

2 Product description

Webbrowser is a powerful and efficient HTML5 browser for HMI devices for state-of-the-art industrial applications.

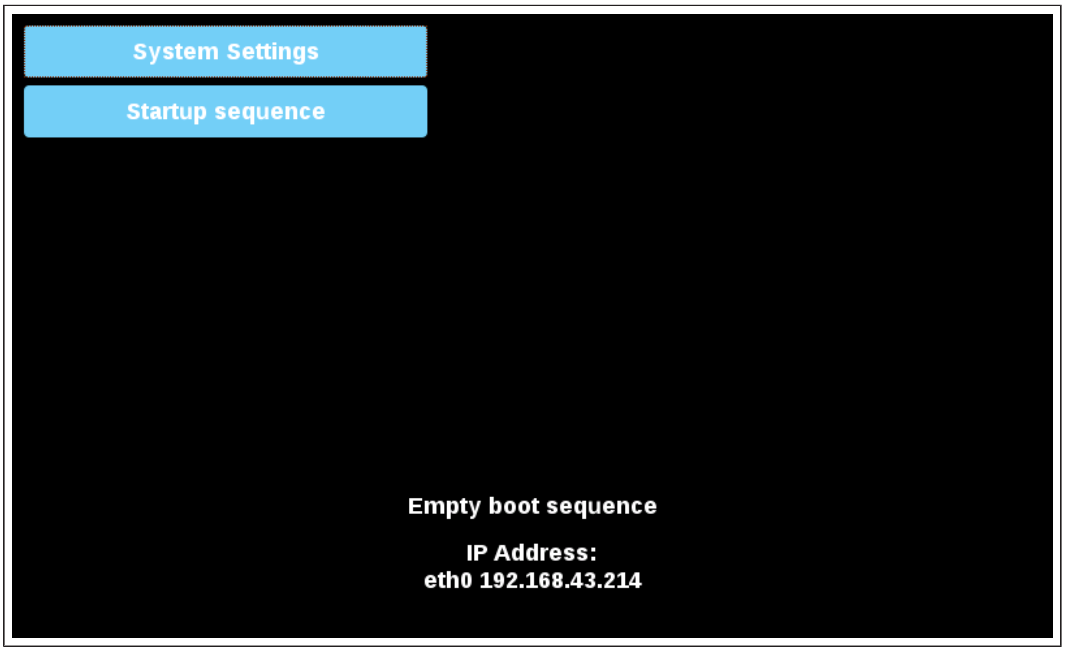
The application was developed for devices based on the embedded Linux platform and ARM processors.

If the web browser is not pre-installed, it can simply be installed on HMI devices with the required platform.

3 Installation

The HMI devices are supplied ex works without runtime. When switching on for the first time, the HMI displays the "Runtime Loader" screen.

If you have already installed an application --- MISSING LINK --- to activate the following page).



Empty boot sequence

IP Address:
eth0 192.168.43.214

Fig. 1: System settings

3.1 USB

Install Chromium application from USB:

1. Copy the application file to an empty USB memory stick.
2. Under "Runtime loader", select "Startup sequence" and then "Install".

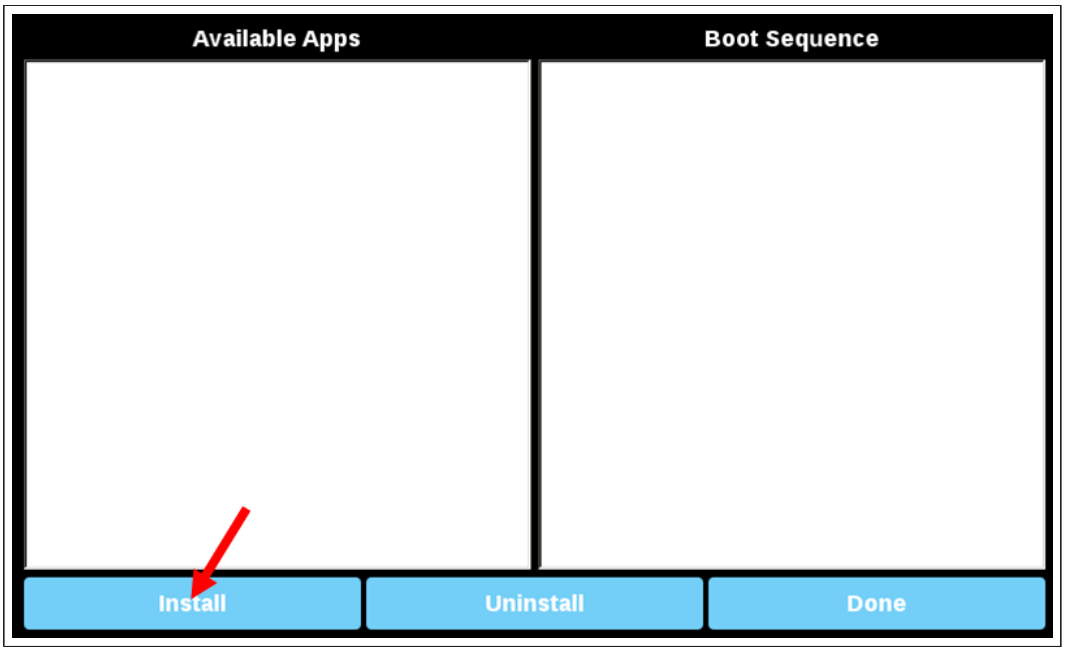


Fig. 2: Install apps

3. Open the "mnt" folder by double-clicking on it.

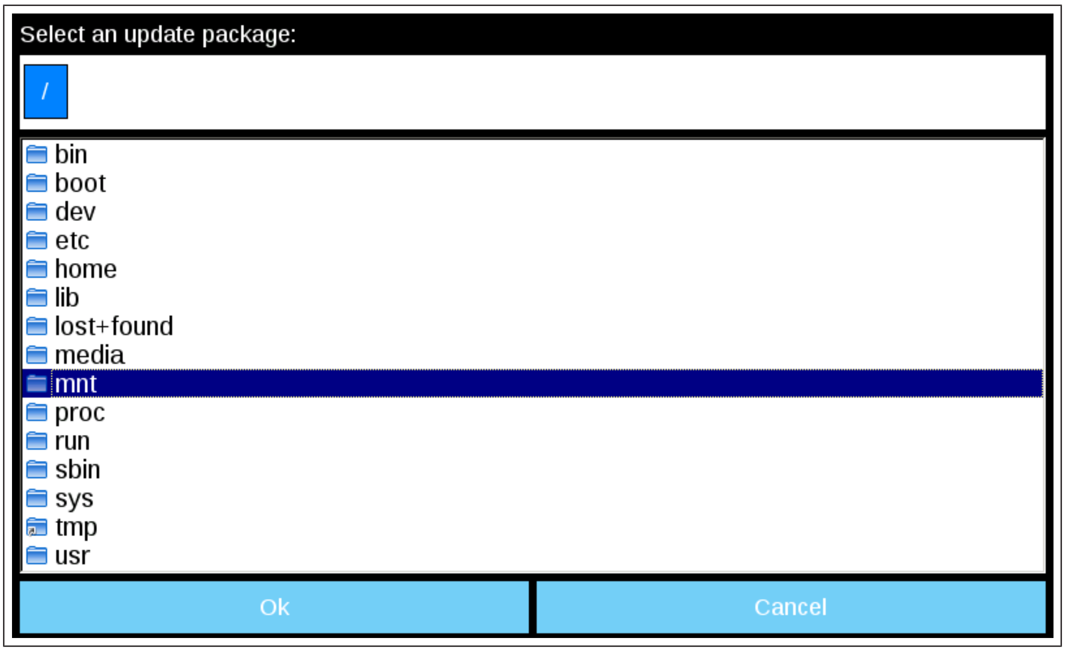


Fig. 3: Select mnt folder

4. Then open the "usbmemory" folder.

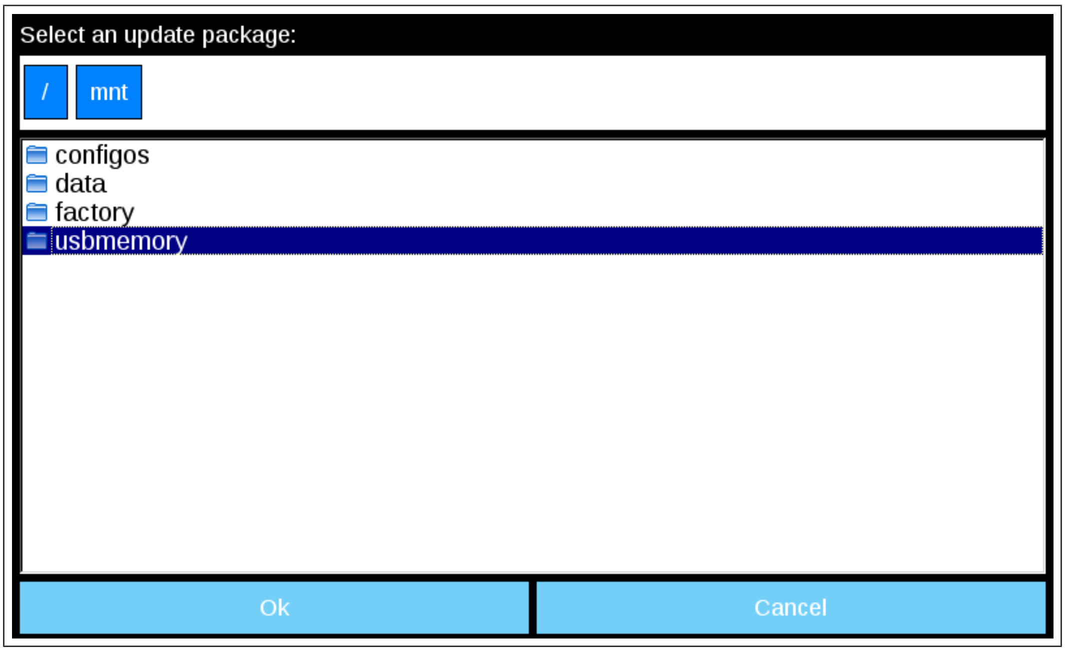
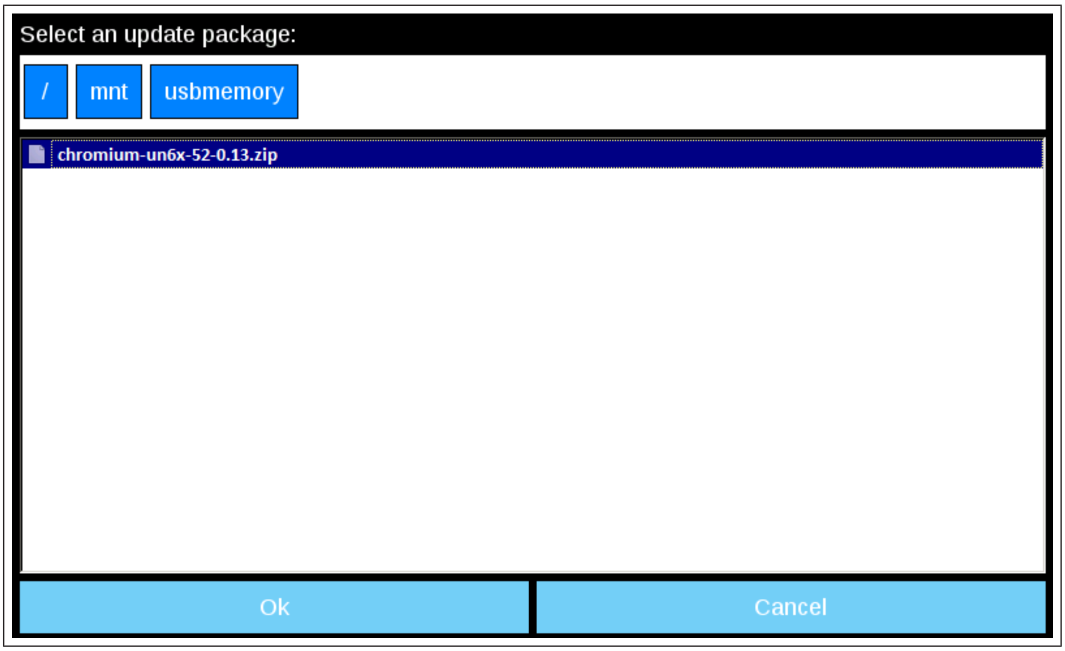


Fig. 4: Open the usbmemory folder

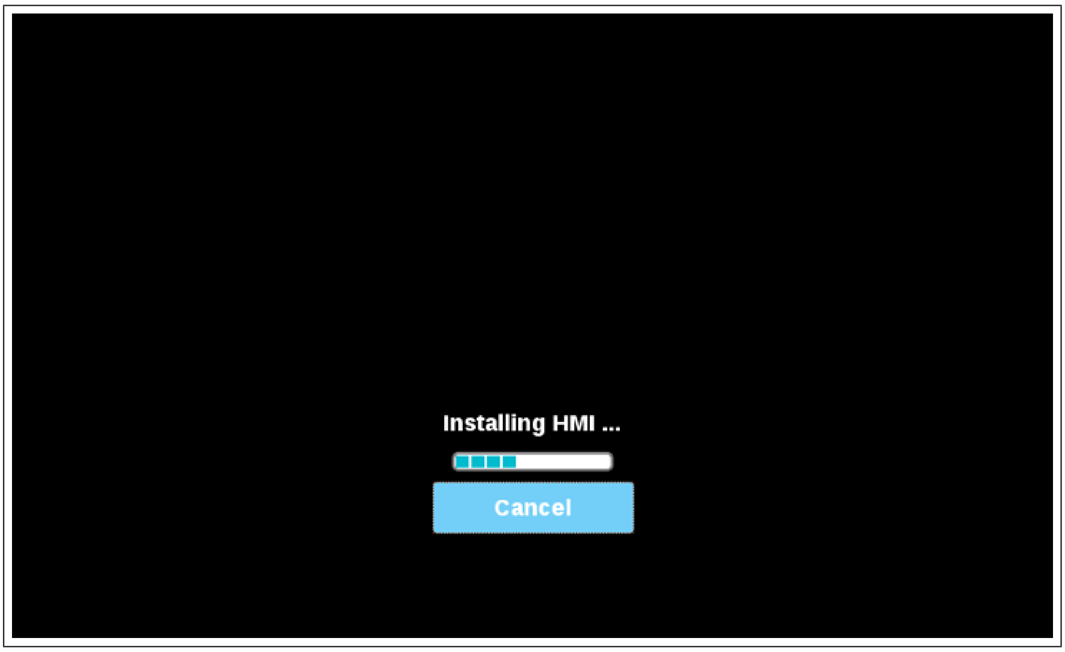
5. Select the Chromium package



Select an update package:

Fig. 5: Select Chrominum package

6. The runtime installation begins.



Installing HMI ...

Fig. 6: Installation running

NOTICE! The file systems FAT16/32 and Linux Ext2, Ext3 and Ext4 are supported.

At the end of the installation process, the HMI device is restarted and the Chromium application is started in full screen mode.

4 Settings

The web browser can be customised with a variety of properties to suit the desired application. The configurable properties are divided into two groups:

- Basic Settings
- Advanced settings

When the browser is started for the first time, the system settings are displayed as the start page.

A login is required to access the system settings. The user name and password are the same as for the HMI device (admin, admin by default). They can be changed in the system settings.

⚠ WARNING ⚠

Protection against unauthorised access to the device.

a) Be sure to change the default password when logging in for the first time.

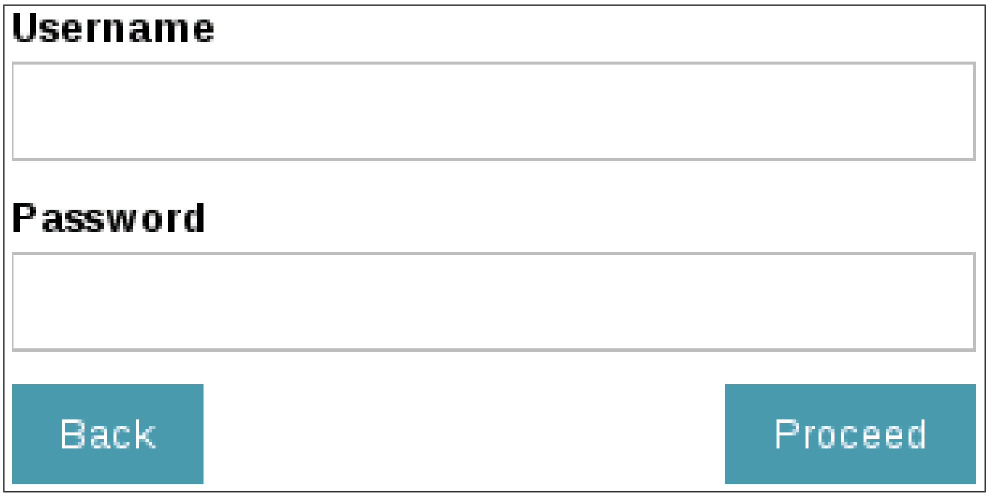


Fig. 7: Registration

4.1 Address bar

If the web browser is configured so that the address bar is not displayed, you can call up the system settings by pressing the top left edge of the display for a few seconds.

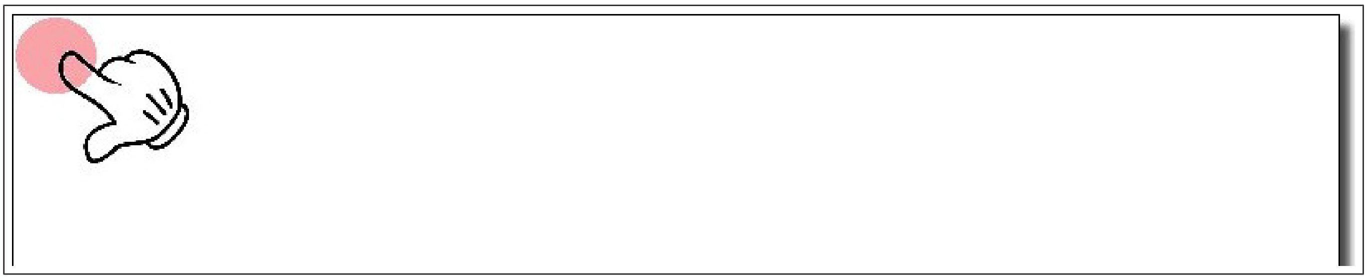


Fig. 8: Show address bar

The system settings can be accessed via the Settings button in the address bar.

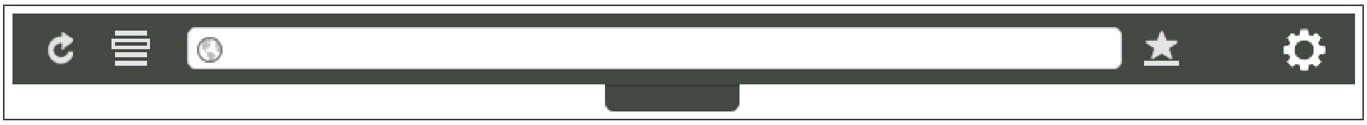


Fig. 9: Address bar

4.2 Toolbar

The toolbar can be opened/closed via the tab in the centre of the address bar.

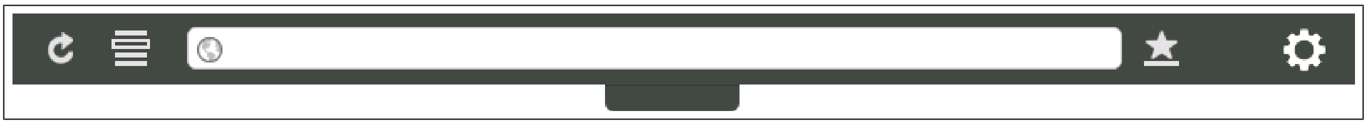


Fig. 10: Open toolbar

The following commands are available:

- Reload page
- History buttons
- Bookmark list
- URL address
- Add bookmark
- Open system settings

4.3 Web browser

Select the "Web browser" tab to access the property settings. Press the "EDIT" button to change the values of the properties

Ownership	**Description**
At the start	Defines the start page.
Homepage	Defines the URL of the start page.
Alternative page	Secondary homepage that is loaded if the primary homepage cannot be loaded. The URL must contain the protocol.
Switch on the toolbar	Show/hide the toolbar.
Allow downloading of files	Activate/deactivate the option to download files. The files are saved in this folder: /mnt/data/storage/chromium/home/Downloads
Activate gesture for history navigation	You can use the swipe gesture to switch back and forth between the pages.
Options Print and hold time (s)	Defines how long the top left edge must be pressed to display the toolbar.
Change UserAgent	Overrides the default browser user agent.
Certificates	Opens the certificate manager of the web browser (only available for local settings).
Certificate settings	Delete all pages in the white list.

Use the system's virtual keyboard	If this function is deactivated, the system's virtual keyboard is not displayed. Keys can be entered via a physical keyboard or via virtual keyboards defined on the active web page.
Activate automatic completion of forms	If this option is activated, the previously entered data is suggested when entering data.
Switch on password management	If this function is activated, the browser prompts you to save the passwords you have entered so that it can suggest them again the next time you try to log in to the same website. **The option is activated the next time the panel is restarted.**

The complete list of available properties can be found at "System options" on page 7

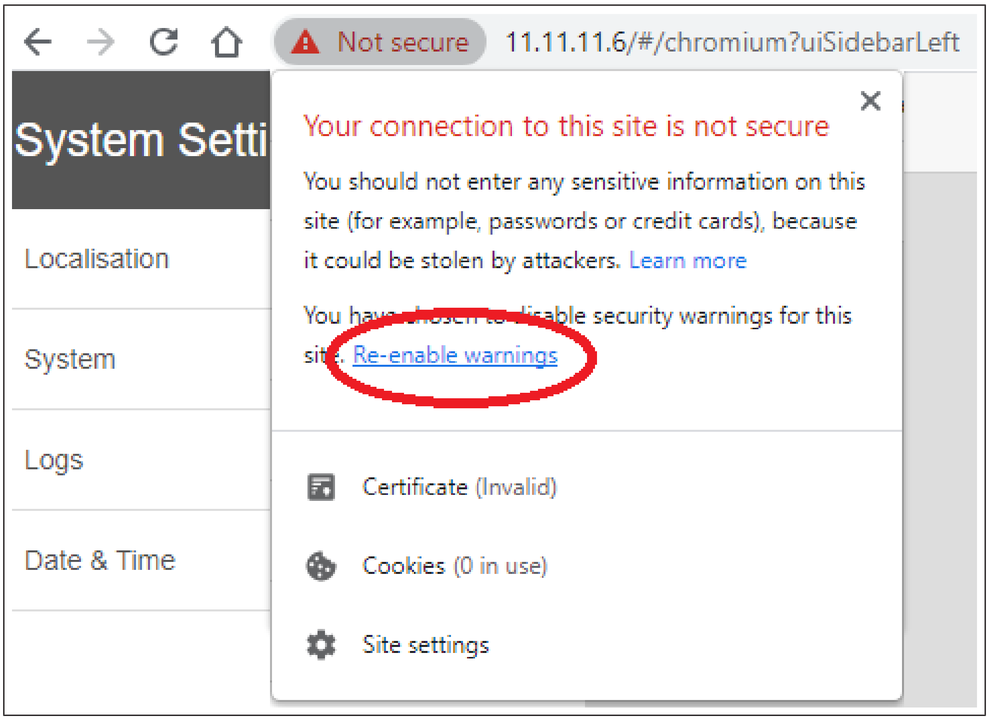
4.4 Switch on warnings

To reactivate the deactivated warning messages (e.g. the certificate warnings), use the following command, which is available in the web browser toolbar.

Remark:

The option is not accessible in kiosk mode.

The settings are only applied after a restart.



Not secure 11.11.11.6/#/chromium?uiSidebarLeft

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

Fig. 11: Switch on warning

The warning message can also be activated on the System settings page:

Path: System settings -> Web browser -> Certificate settings -> Reactivate certificate warnings.

4.5 System options

The system options can be defined at startup using command line arguments or by adding a settings file.

Use of command line arguments

/mnt/data/hmi/chromium/deploy/start.sh <Optionen>

Use settings file

Each command line option can also be set by creating the following file:

/mnt/data/hmi/chromium/deploy/settings

The options can be inserted individually per line in the file.

4.5.1 Available system options

Option	**Description**
--homepage=<uri>	Disable homepage setting.
--enable-exit-button	Activates the "Exit" button on the options page and the "X" icon in the toolbar if it is activated. Closes the web browser.
--enable-restart-button	Activates the "Exit" button on the options page and the "X" icon in the toolbar if it is activated. Restart the web browser.
--enable-window-exit-button	As above, but only the window is closed. In this case, a new window is opened when the web browser is restarted, which is faster. Command line flags that are specified the first time cannot be changed later, as this requires a complete restart. Another URL can be specified instead.
--enable-toolbar	Activates the toolbar. The setting is saved so that it is activated the next time even without this option.
--enable-toolbar-navigation	Display the navigation buttons for the history in the toolbar
--enable-toolbar-on-error	The toolbar is only displayed if an error occurs when loading the page. The setting is saved so that it is activated the next time even without this option.
--fixed-toolbar	The toolbar is fixed and not collapsed.
--disable-toolbar	Deactivates the toolbar. The setting is saved so that it is activated the next time even without this option.
--disable-toolbar-url	Removes the URL text area from the toolbar. When used, the toolbar no longer takes up the entire width of the screen and is centred instead.
--enable-toolbar-bookmarks	Activates the "Bookmark list" and "Add bookmark" buttons in the toolbar if they are activated. The "Add bookmark" button is still hidden if --disable-toolbar- url is used. If it is deactivated, the toolbar is not activated.
--disable-toolbar-options	Removes the radio button from the toolbar. The toolbar is not activated when deactivated.
--disable-options	As above, but in addition the long press is deactivated so that it is no longer possible to open the options page. If a loading error occurs, the browser tries again, and even in this case the options page is never opened.
--disable-toolbar-reload	Removes the "Reload" button from the toolbar.

--loadingPage=<URL>	Displays a custom page that is loaded on boot while the actual page is loading. This also hides the standard error page if the server is not ready. The loading page is displayed until the browser has finished loading the project or the maximum number of loading attempts has been reached. The URL must contain the protocol (i.e. http://, file:// If no URL is specified (only "--loadingPage"), a white page is used. If the web project cannot be loaded, the alternative page is displayed if this is set. Otherwise the login page will be loaded. The toolbar can be activated and displayed in the loadingPage. "--enable-toolbar-on-error" is also supported, in this case the toolbar is only displayed after a second failed attempt to load the web project.
--fallback-url=<uri>	A secondary homepage that is loaded after open-options-after-num-retries has failed attempts to load the primary one. If this is also not available, the options page is loaded. The URL must contain the protocol.
--open-options-after-num-retries=<n>	Specify after how many retries the login page is opened in the event of loading errors (default is 4). A value <1 will deactivate the function.
--repeated-on-error-timeout=<n>	Time in seconds between the repeat attempts. The minimum accepted value is 5 (default is 8).
--disable-fallback-reload	If this option is activated, the browser no longer reloads if the fallback page fails to load and remains on the error page. By default, the options page is opened and reloading continues in the background.
--first-load-repeat	The browser should only attempt to contact the server again during the first loading process. Once a page has been successfully loaded, it should no longer be automatically reloaded.

4.5.2 Loading the homepage

If the web browser is configured so that a homepage is loaded at startup, proceed as follows:

Open a first tab with a local "loading page". This page can be changed with "--loading-page".

Start loading the homepage on a second tab while remaining on the first. Switch to the second one as soon as the page is loaded.

If the homepage was not loaded after "--open-options-after-num-retries", an attempt is made to load the fallback URL if "--fallback-url" is specified.

Open the options page if the fallback URL is not set or cannot be loaded.

"-Homepage" should overwrite the homepage URL and hide the option on the settings page.

4.5.3 Initial configuration

In the "browser.ini" file, you can define the configuration that is only applied once when the web browser is started for the first time. During normal use, users can change the configuration via the "System settings" page or the option flags.

The "browser.ini" file must be copied to the installation folder of the web browser (/mnt/data/hmi/chromium/deploy). The settings are applied at the next restart and at this time the "browser.done" file is created in the same folder to avoid a second reconfiguration.

If the "browser.done" file is removed, a new configuration is forced at the next restart.

Supported buttons

- homepageLink=<url>
  The URL must contain the protocol (i.e. http://, file://)

- customUserAgent=<userAgent>
- showToolbarOnError=<true|false>
- showWiFiStatus=<true|false>
- showHistoryButton=<true|false>
- showLoadingBarAndStopButton=<true|false>
- onStartup=<Settings|Homepage|LastVisistedPage>
- enableToolbar=<true|false>
- holdTimer=<ms>
  Timeout in ms for long press, at least 2000 (2s)
- fallbackToDefaultPageLink=<url>
  The URL must contain the protocol (i.e. http://, file://)
- disableFallbackReload=true

Example of the browser.ini file

```
(🌐► homepageLink=http://google.com)
customUserAgent="Mozilla/5.0 (X11; Linux armv7l) ... "
showToolbarOnError=false
showWiFiStatus=true
showHistoryButton=false
showLoadingBarAndStopButton=false
onStartup=Settings enableToolbar=true
holdTimer=2300
(🌐► fallbackToDefaultPageLink=http://google.)com
```

5 System configuration

The system settings are available in the HMI devices as a tool for configuring the system properties of the device.

5.1 System settings

The user interface for the system settings is based on HTML pages and can be accessed both locally on the screen of the HMI device and remotely via a web browser.

The administrator user name with full access rights is "admin" with the default password "admin". The general user name is "user" with the default password "user".

⚠ **WARNING**

Protection against unauthorised access to the device.

a) Call up System settings => Authentication.

b) Be sure to change the administrator and user passwords.

It is not necessary to enter a password to access the system settings from the HMI device as long as the default password "admin" is not changed.

5.1.1 Input in system settings

There are several ways to access the System settings page:

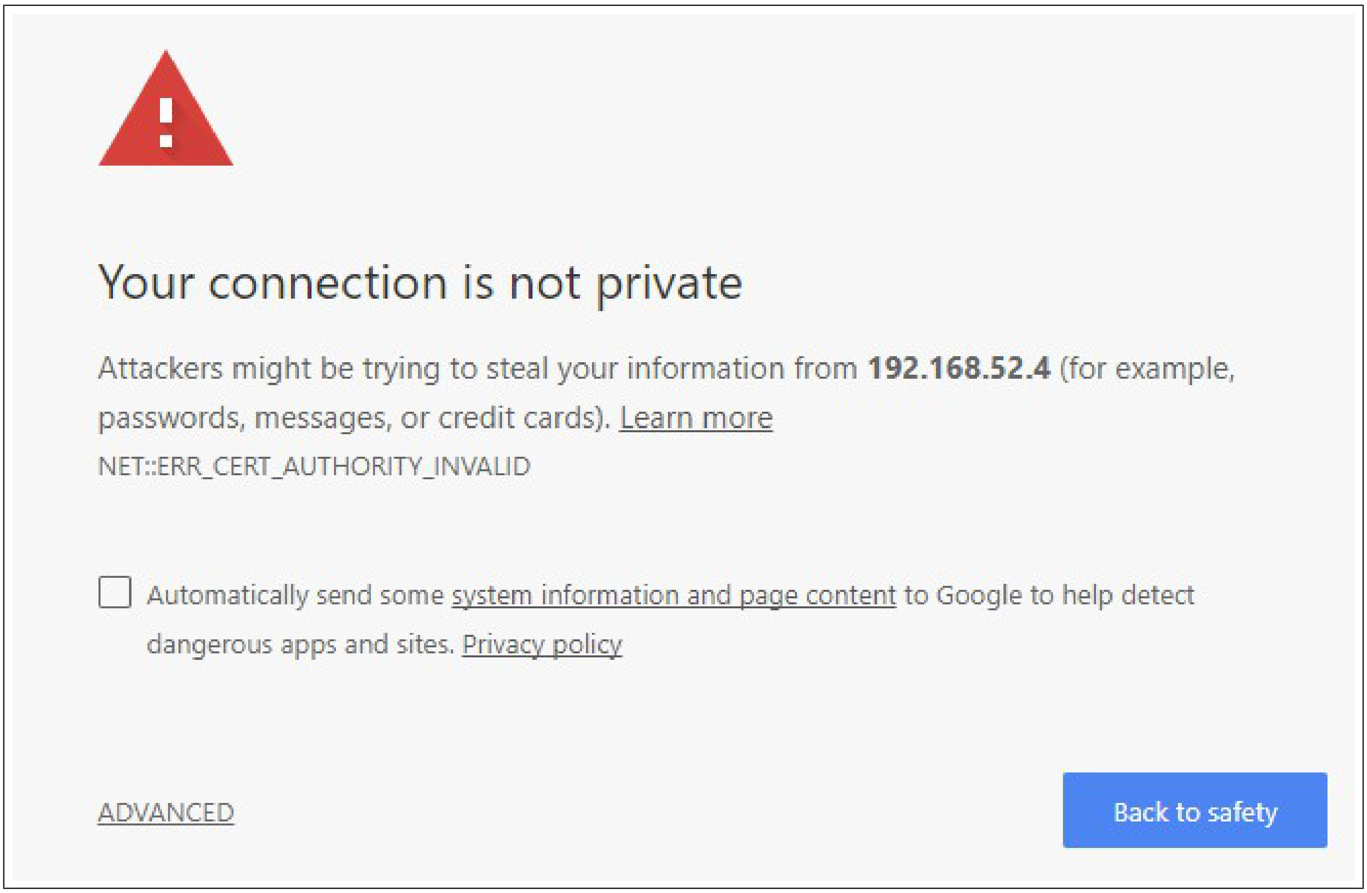
- Via a web browser
- From the HMI device if no runtime is loaded
- From the HMI device using the tap-tap method

5.1.1.1 Access to the system settings via the web browser

To access the system settings via a web browser, enter the IP address of the device in the following format:

https://IP/machine_config

Please note that remote access takes place via the encrypted https protocol on port 443. When the connection is established, the HMI device sends a certificate that is used for encryption. As the certificate is not signed by a certification authority, you will receive a warning message. Please click on the advanced options and select continue.



Your connection is not private

Attackers might be trying to steal your information from **192.168.52.4** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

Fig. 12: Certificate warning message

The standard security protocols suggested by the HTTPS server in the Linux HMI device are:

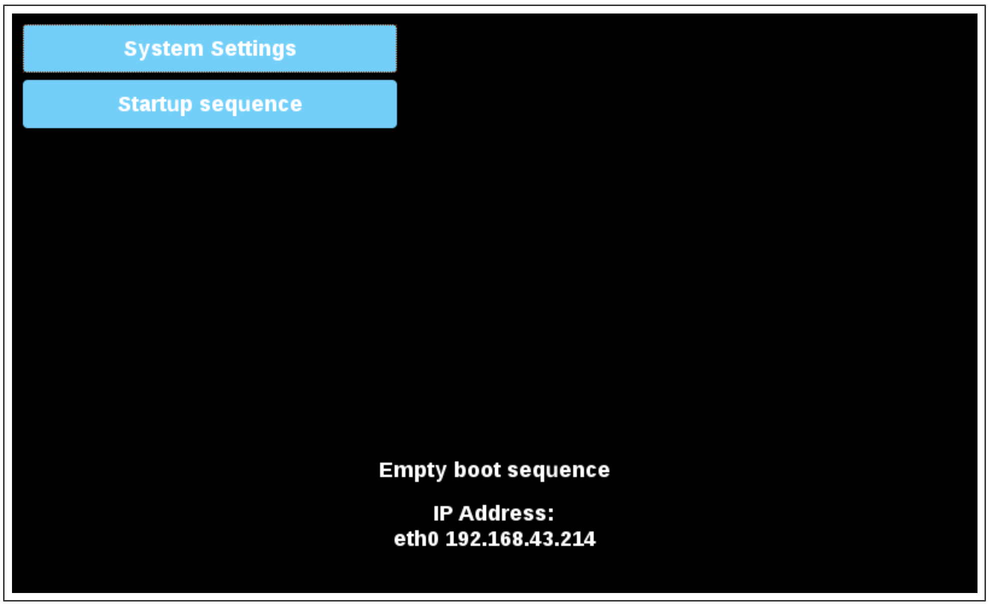
SSLv3 256 bits ECDHE-RSA-AES256-SHA

TLSv1 256 bits ECDHE-RSA-AES256-SHA

WARNING! We do not recommend the use of CBC cyber suites in connection with SSL3 or TLSv1.0 connections, as they may be affected by some vulnerabilities.

5.1.1.2 Access to system settings from the HMI device

If Runtime is not installed, the system settings can be accessed via the Runtime Loader screen.



Empty boot sequence

IP Address:
eth0 192.168.43.214

Fig. 13: Runtime Loader

If the Runtime is installed, you can access the system settings by selecting the "Show system settings " option in the context menu.

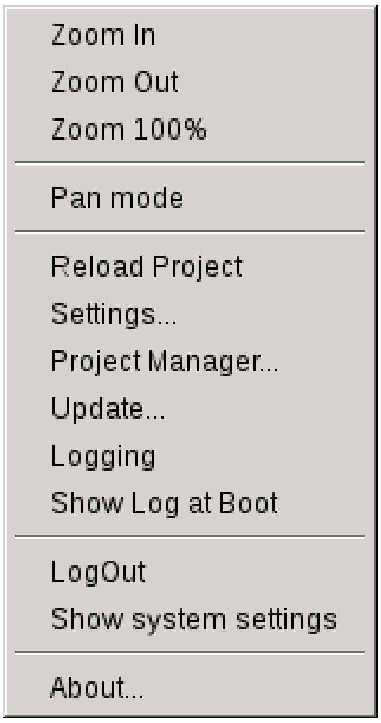


Fig. 14: Show system settings

5.1.1.3 Call up the system settings by tapping (TAP-TAP)

Immediately after switching on the HMI, the tap-tap function is called up by repeatedly tapping the touchscreen with your finger.

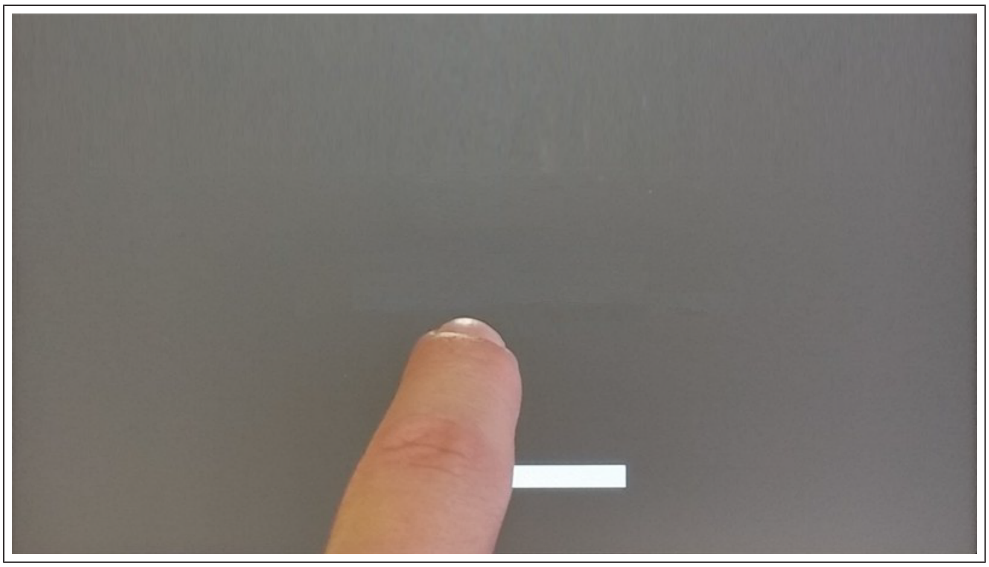
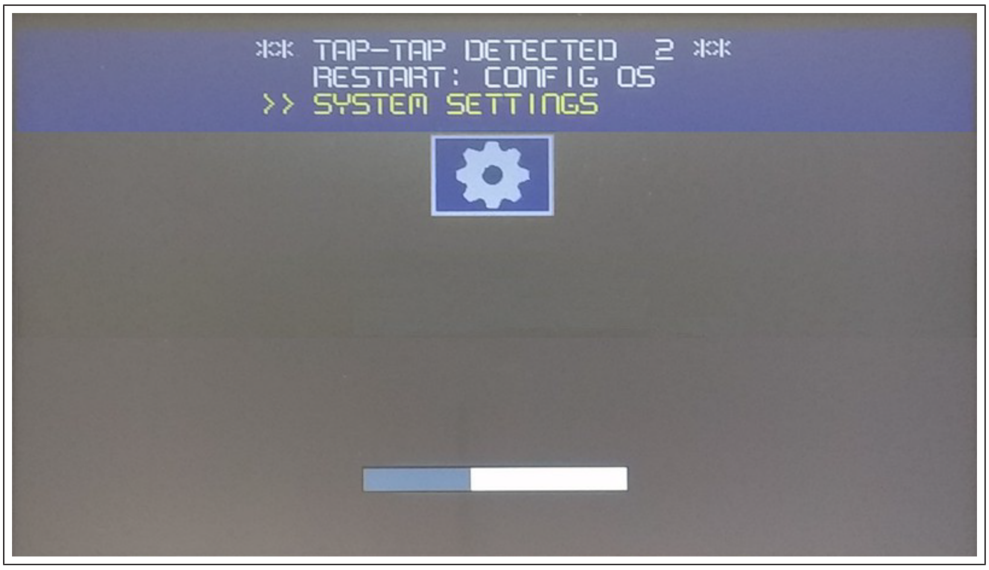


Fig. 15: Start TAP-TAP

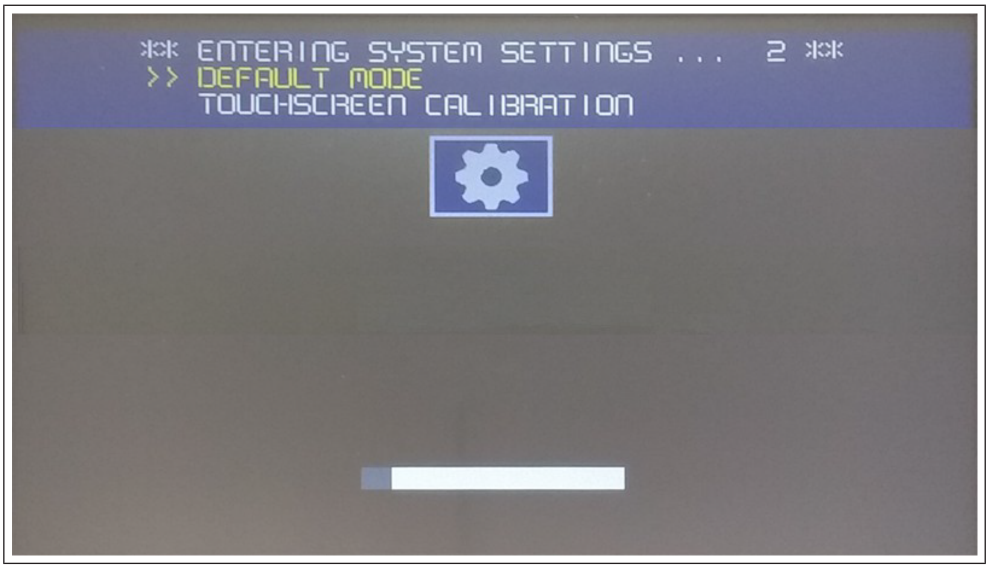
When the message "TAP-TAP DETECTED" appears at the top of the screen. Wait 5 seconds (without touching the screen) to call up the System settings submenu.



** TAP-TAP DETECTED 2 **
RESTART: CONFIG OS
>> SYSTEM SETTINGS

Fig. 16: TAP-TAP recognised

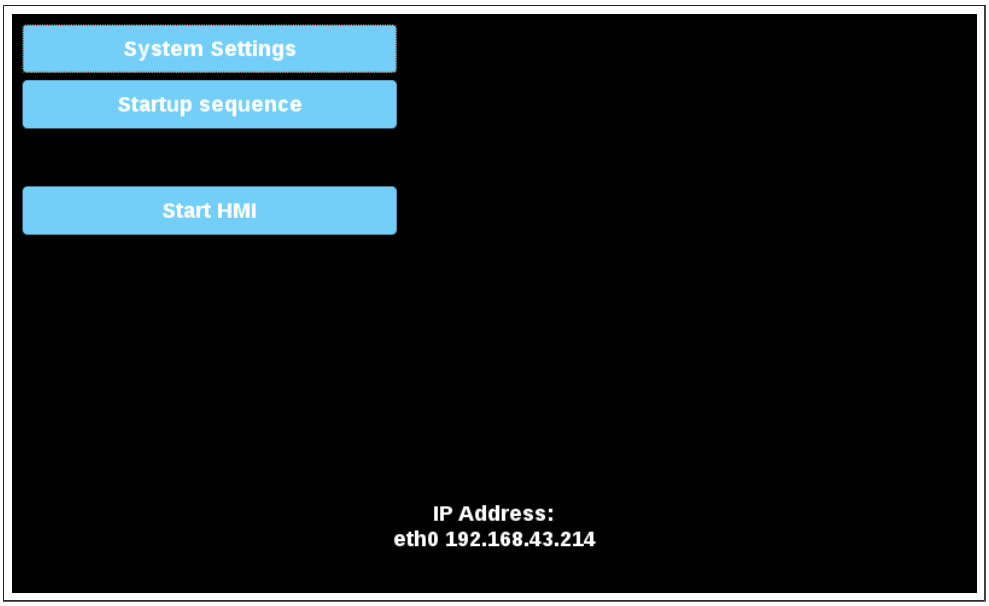
Wait a further 5 seconds (without touching the screen) to switch to default mode.



```
** ENTERING SYSTEM SETTINGS ...   2 **
>> DEFAULT MODE
   TOUCHSCREEN CALIBRATION
```

Fig. 17: Default Mode

The "System settings" and "Start sequence" buttons are now available.



IP Address:
eth0 192.168.43.214

Fig. 18: Start screen

5.1.2 Localisation

Set the following parameters to customise the device to your country.

- Country code (only required for WiFi)
- Language for the system settings interface
- Layout of the virtual keyboard

The country code is required for the Wi-Fi regulation domain and the device will only use the Wi-Fi if this parameter is not set.

The country settings are required for licence-compliant operation. Selecting a country that does not correspond to the country in which the device is operated may be punishable by law. After selecting the country code, the corresponding channels are automatically assigned and the power level is set.

5.1.3 System

Parameter	Description
Info	Information about the device
Status	Device status (free RAM, operating time, CPU load)
Timers	Device timer (system on, backlight on)
PlugIn	Information on hardware plug-ins

5.1.4 Logbook

Activate the "Permanent log files" option if you want the log files to remain saved even after a restart. Use the "Save" button to export a copy of the log files.

The log file manager cyclically fills 3 files of 4Mb each.

5.1.5 Date and time

Date and time of the device.

Parameter	Description
Current time zone	Time zone Region
Current date local time	The date and time can only be set manually if automatic updating is deactivated.
Automatic update (NTP)	Activate the synchronisation of date and time from a remote server **NTP server** Enter the address of the Internet NTP server The HMI device's NTP client is a full implementation of Network Time Protocol (NTP) version 4, but also maintains compatibility with version 3, as defined in RFC-1305, and versions 1 and 2, as defined in RFC-1059 and RFC-1119 respectively. The poll process sends NTP packets at intervals determined by the Clock Discipline algorithm. The process is designed to provide a sufficient update rate to maximise accuracy while minimising network overhead. The process is designed to operate in a variable mode between 8 seconds and 36 hours.
Accept NTP requests	If this function is activated, the device accepts NTP requests from outside. If automatic updating is not activated, the device uses the local RTC time.

5.1.6 Networks

Network parameters. Available parameters in edit mode:

Parameter	Description
General settings	Host name of the device Avahi hostname (see "Avahi Daemon" on page 24)
Network interface	Network parameters of the available interfaces DHCP IP address Net mask Gateway

	By default, the network interface is set so that DHCP is activated and the network parameters are retrieved from the DHCP server. If the DHCP server is not found, the avahi-autoip service is used to set an IP address in the 169.256.x.x range.
DNS	DNS server Is usually provided by the DHCP servers, but can be changed in edit mode. Search domains Optional domains that are used in concatenation with the specified URLs

5.1.7 Security

The services are only available if you are logged in as an administrator.

The security area contains passwords and certificates that are required by applications.

Parameter	**Description**
Range	Identifies a range of secret information that can be used by installed applications that have the corresponding rights. The preconfigured domains are: **General** This area is available for third-party applications. **System** This space is used by the services embedded in the device (e.g. the VNC server). **HMI Runtime** This area is used by the HMI Runtime application.
Secret ID	Name used to identify the individual secret information in the selected domain.
Type	Type of information to be stored. • Text • Password • Certificate • File
Secret Info	Secret information that must be saved. In the case of text or password, enter the text or password to save. In the case of a certificate or a file, use the "Update" button to save the file.
Description	A free text that you can insert as you wish.

Import/Export

Using the Import/Export commands, it is possible to export the saved information and import it into other devices, for example. Note that the export command prompts you to set a password, which is then required to import the exported file.

5.1.8 Applications

The applications loaded on the HMI devices are listed on the Applications page. You can manage the applications from this page.

Parameter	**Description**
Name	Name der Anwendung

Autostart	If this option is selected, the application is started when the control panel is switched on.

App management

Press the "*App Manager*" button to enter application management mode:

- Upload new applications
- Update existing applications
- Remove application
- Set the starting order.

5.1.9 Services

NOTICE! The services are only available if you are logged in as an administrator.

Click on the "Activate" button with the mouse to activate/deactivate the respective service. Click on the name of the service to list the associated parameters.

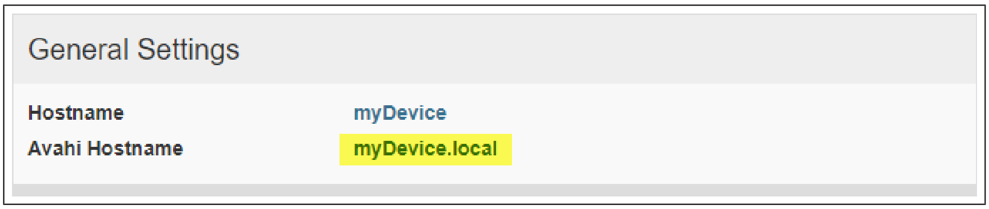
5.1.9.1 Autorun scripts from external memory

Activate/deactivate the option to execute the "autoexec.sh" script file when a USB stick is connected to the device. Deactivate this service if you want to prevent unauthorised access via the USB interface.

NOTICE! Required BSP v1.0.212 or higher

5.1.9.2 Avahi daemon

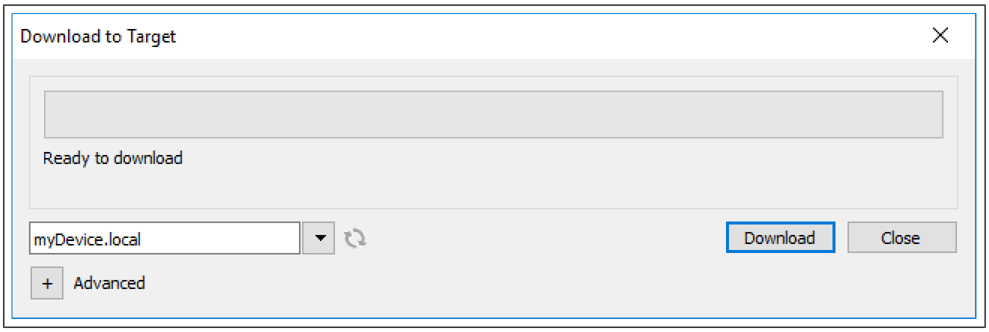
Avahi is a system that enables programmes to find and publish services and hosts running in a local network. If it is activated, the HMI device can also be reached via the host name of the device (instead of the IP address).



General Settings

Hostname	myDevice
Avahi Hostname	myDevice.local

Fig. 19: Avahi - General settings



Download to Target

Ready to download

myDevice.local

Fig. 20: Start the download to the destination folder

Avahi Daemon runs on UDP port 5353

On Linux, the Avahi service is supplied free of charge with the operating system. On Windows PCs, however, you must install an Avahi service to be able to access the panel via its Avahi host name.

5.1.9.3 Bridge/Switch service

With the bridge service, it is possible to connect the WAN network adapter (eth0) to the other network interfaces. When used, the two Ethernet interfaces are bridged and both Ethernet interfaces share the same IP address.

The Bridge service creates a Linux-based Layer 2 network bridge between two or more network interfaces. If both WAN and end devices are connected to such a bridge, the two networks are physically connected and the end points are available as if they were directly connected to the WAN (Note: The router service must still be active for the cloud scenario).

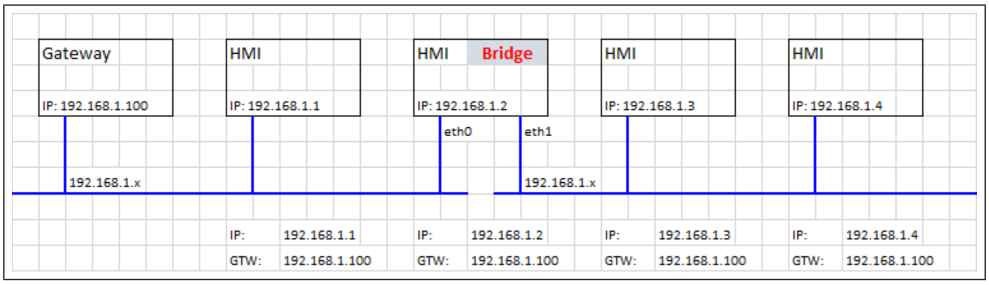


Fig. 21: Bridge service

5.1.9.4 Cloud / VPN service

Enables the management of remote HMI devices that are connected to a central server via gateways. Further information can be found at (≡▶ "Cloud/VPN service" on page 38 [▸ 34]).

5.1.9.5 DHCP server

Provide the DHCP server for the selected interfaces.

Parameter	Description
Enabled	Activates the DHCP server on the selected interface.
Start IP Stop IP	IP addresses distributed by the DHCP server
Gateway	The address of the gateway
Net mask	The specified netmask
DNS server	The address of the DNS server
Lease time (seconds)	Lease time, default is 86400 s (1 day). Permissible values are between 60 s and 864000 s (10 days).

5.1.9.6 Enable device recovery via TAP TAP option

If this function is activated, the control panel can be reset if the administrator password has been forgotten (see: (≡▶ "Forgotten password" on page 1 [▸ 42])).

NOTICE! This option is activated by default. You can deactivate it to increase the security of the device. This excludes the possibility of recovering a forgotten password.

NOTICE! Required BSP v1.0.212 or higher.

5.1.9.7 Restoring the device via USB

If this function is activated, the control panel can be reset if the administrator password has been forgotten (see: (≡▶ "Forgotten password" on page 1 [▸ 42])).

NOTICE! This option is activated by default. You can deactivate it to increase the security of the device. This excludes the possibility of recovering a forgotten password.

NOTICE! Required BSP v1.0.212 or higher

5.1.9.8 Quick start

If quick start is activated, the HMI device starts the HMI application as quickly as possible when it is switched on. In this mode, no diagnostic information is displayed (e.g. the loading bar), but only the minimum required functions are loaded before the user interface is loaded (e.g. system settings, VNC, SSH etc. are only loaded after the HMI application has been loaded).

To achieve optimum performance, it is recommended to make the following settings in addition to the quick start mode:

Deactivate all unnecessary services.

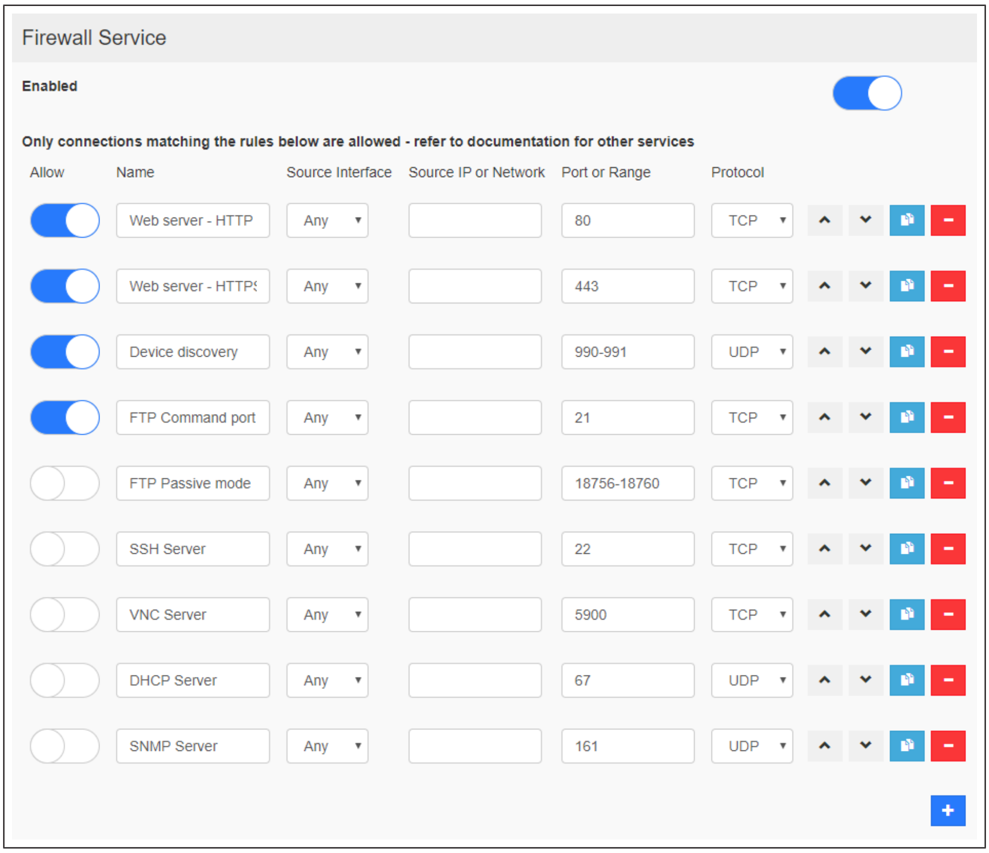
Prevent the persistent protocol from remaining activated.

Use of a static IP address instead of the DHCP service.

NOTICE! Required BSP v1.0.212 or higher

5.1.9.9 Firewall service

If the firewall is activated, only connections that fulfil the defined rules are permitted. Please note that some rules must be activated for the HMI to function correctly.



Firewall Service

Enabled ●

Only connections matching the rules below are allowed - refer to documentation for other services

Allow	Name	Source Interface	Source IP or Network	Port or Range	Protocol
●	Web server - HTTP	Any		80	TCP
●	Web server - HTTPS	Any		443	TCP
●	Device discovery	Any		990-991	UDP
●	FTP Command port	Any		21	TCP
○	FTP Passive mode	Any		18756-18760	TCP
○	SSH Server	Any		22	TCP
○	VNC Server	Any		5900	TCP
○	DHCP Server	Any		67	UDP
○	SNMP Server	Any		161	UDP

Fig. 22: Firewall settings

Notes:

- The firewall is based on IP tables that only work on layer 3 (layer 2 packets are not filtered, e.g. ARP).
- Only INPUT and FORWARD packets are filtered, not OUTPUT.
- PING/ICMP echo response packets are always permitted.
- Internet sharing scenarios (e.g. 3g or WiFi connection to endpoints) are not supported.
- Packets filtered by the firewall are discarded.

Source IP or network

If this field is not specified, access is possible from any source host. Otherwise, access can be restricted to a single IP address (e.g. 192.168.100.123) or a range of IP addresses in CIDR format (e.g. 192.168.100.0/24).

NOTICE! If you want to activate the firewall and use the FTP passive mode with the HMI Runtime older than version 2.10.0.280, you must open the ports 1024-2048/tcp and 16384-17407/tcp. From version 2.10.0.280, HMI Runtime uses the ports 18756-18760/tcp instead, which are suggested by default in the firewall settings.

NOTICE! Firewall is available from BSP v1.0.532. If you are updating from an old BSP version and the default rules are not displayed, you must reset the system settings (see (🌐► "Updating system components" on page 1)**NOTICE!).**

5.1.9.9.1

5.1.9.9.1.1 Router service

This service uses IP forwarding and Network Address Translation to share the connection from the WAN (eth0) to the LAN (eth1 or eth2): Connected endpoints can reach the same networks that are accessible from the gateway (including the Internet, if available). When the cloud service is active, the endpoints can be reached via the LAN port of the gateway (for more information, see (≡▶ "Cloud / [⏵ 34]) (≡▶ VPN Service" on page 38 [⏵ 34]))

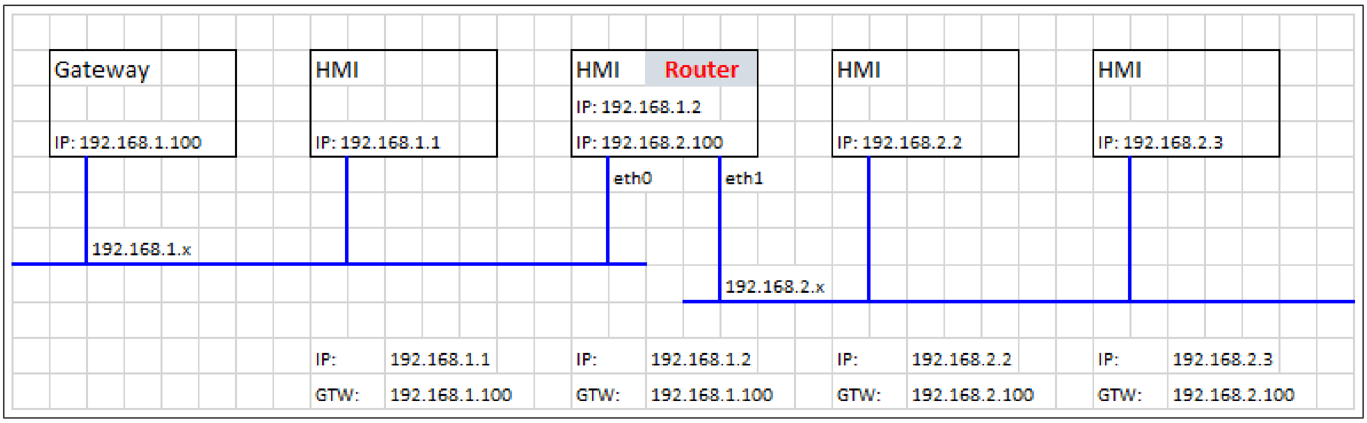
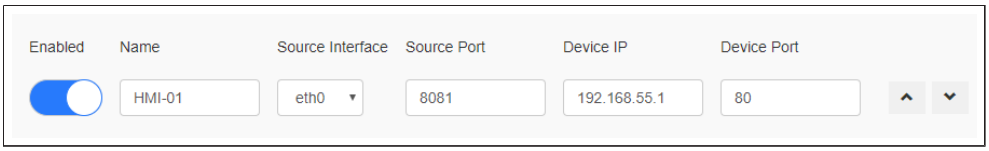


Fig. 23:

5.1.9.10 Router / NAT / Port forwarding

Port forwarding redirects incoming TCP packet requests from the WLAN interface from one address and port number combination to another address and port number combination.

5.1.9.10.1 Rules for port forwarding



Enabled	Name	Source Interface	Source Port	Device IP	Device Port
●	HMI-01	eth0 ▾	8081	192.168.55.1	80

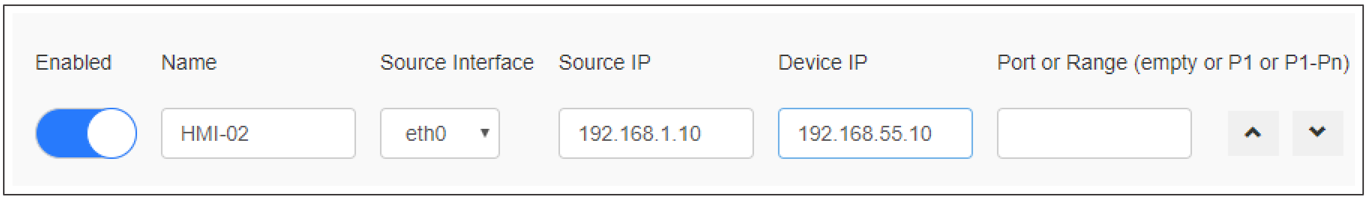
Fig. 24: Port forwarding

NOTICE! Available from BSP v1.0.507

5.1.9.10.2 1:1 NAT rules

1:1 NAT, creation of an alias IP in the WLAN and forwarding of all packets (or a specific port range) with this destination IP to another device connected to a LAN.

NOTICE! Available from BSP v1.0.507



Enabled	Name	Source Interface	Source IP	Device IP	Port or Range (empty or P1 or P1-Pn)
●	HMI-02	eth0 ▾	192.168.1.10	192.168.55.10	

Fig. 25: 1:1 NAT rules

CAUTION! Make sure that the value entered for "Source IP" does not match the real IP address assigned to the physical Ethernet port specified as "Source Interface".

5.1.9.10.3 DNS relay proxy

The DNS relay proxy forwards DNS queries and response packets between the DNS client and DNS server.

If this function is activated, the HMI device forwards DNS queries from other devices (DNS clients) to the DNS server (configured in the network section) and sends the response back to the DNS client that made the query.

NOTICE! Available from BSP v1.0.507

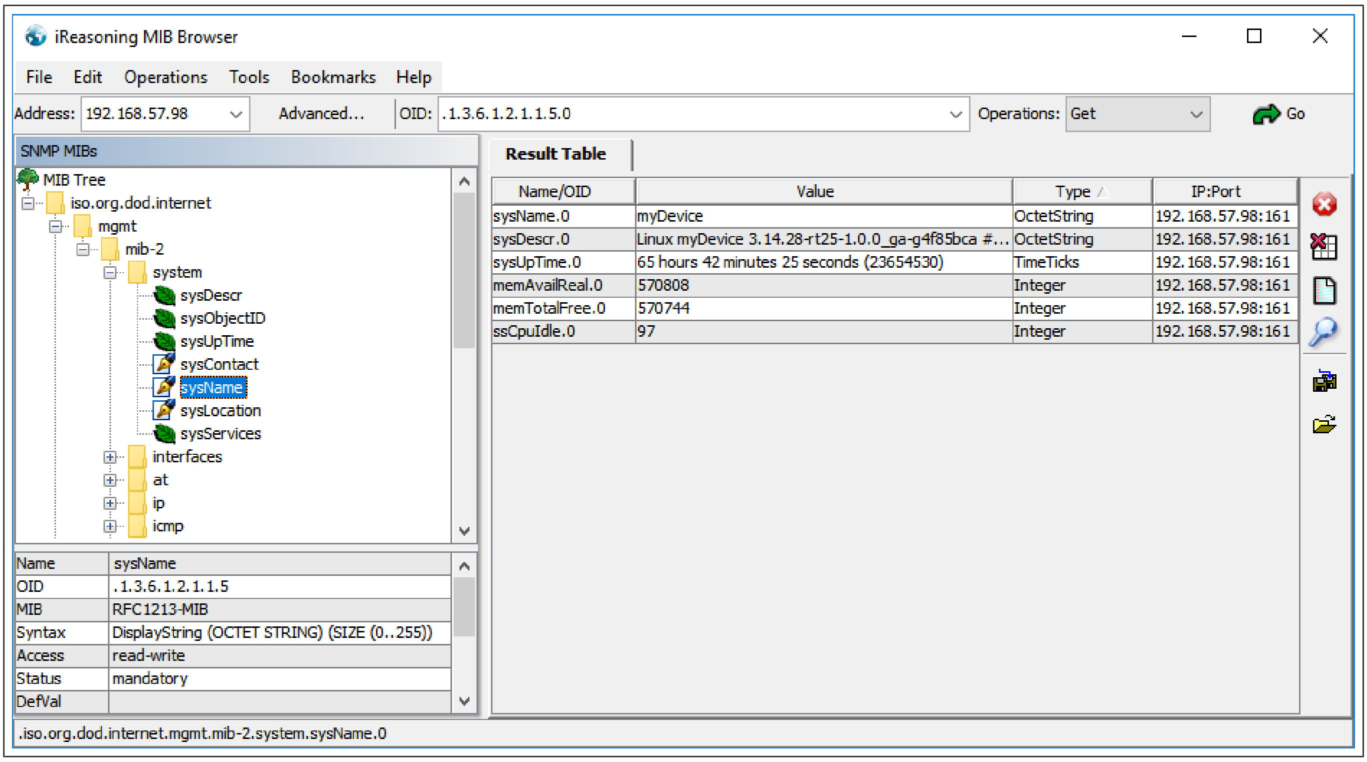
5.1.9.11 Show loading bar on boot

Activate/deactivate the display of the loading bar during the boot phase.

5.1.9.12 SNMP server

SNMP is a network protocol that enables the management of network infrastructures. It is usually used to monitor network devices such as switches, routers, etc. that are connected to a LAN network.

If the SNMP service is activated, an SNMP manager can retrieve information from the HMI device via the SNMP protocol. There are currently no proprietary MIBs available. Only the public standard community MIBs are available in read-only mode.



Address: 192.168.57.98

OID: .1.3.6.1.2.1.1.5.0

Operations: Get

Name/OID	Value	Type	IP:Port
sysName.0	myDevice	OctetString	192.168.57.98:161
sysDescr.0	Linux myDevice 3.14.28-rt25-1.0.0_ga-g4f85bca #...	OctetString	192.168.57.98:161
sysUpTime.0	65 hours 42 minutes 25 seconds (23654530)	TimeTicks	192.168.57.98:161
memAvailReal.0	570808	Integer	192.168.57.98:161
memTotalFree.0	570744	Integer	192.168.57.98:161
ssCpuIdle.0	97	Integer	192.168.57.98:161

Name	sysName
OID	.1.3.6.1.2.1.1.5
MIB	RFC1213-MIB
Syntax	DisplayString (OCTET STRING) (SIZE (0..255))
Access	read-write
Status	mandatory
DefVal	

.iso.org.dod.internet.mgmt.mib-2.system.sysName.0

Fig. 26: MIB Browser

Example

System Name	.1.3.6.1.2.1.1.5.0
System description	.1.3.6.1.2.1.1.1.0
System UpTime	.1.3.6.1.2.1.1.3.0
Total RAM used	.1.3.6.1.4.1.2021.4.6.0
Total free RAM	.1.3.6.1.4.1.2021.4.11.0
Idle CPU time (%)	.1.3.6.1.4.1.2021.11.11.0

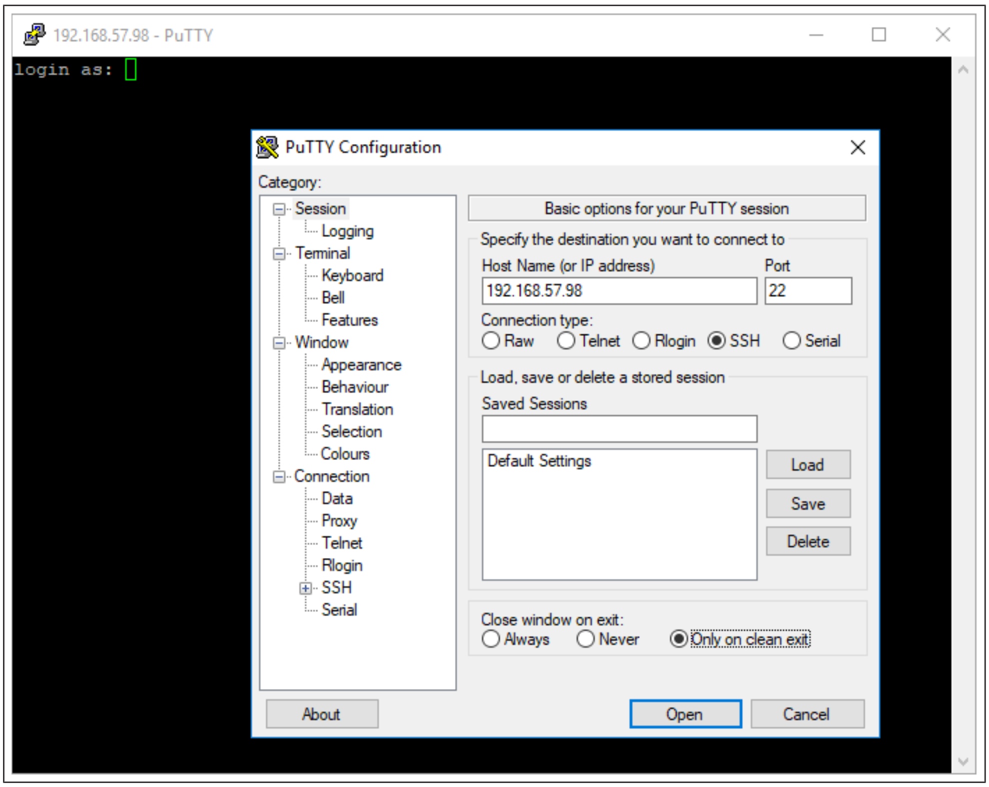
SNMP server runs on UDP port 161

NOTICE! For security reasons, you should not activate the service if you do not need it.

5.1.9.13 SSH server

The SSH service was developed for advanced users only. It enables remote login to the HMI device via the Secure Shell protocol. On the PC, you can run an SSH client such as PuTTY, an open source software distributed under the MIT licence.

The default password for the user name admin is "admin". Further information can be found in the chapter (≡▶ "Authentication" on page 36 [⏵ 33]).



192.168.57.98 - PuTTY

```
login as:
```

PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.57.98

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Fig. 27: PuTTY configuration

SSH server runs on TCP port 22.

CAUTION! This service is intended for use in the development phase. For security reasons, remember to deactivate the service before switching to production.

5.1.9.14 VNC service

VNC is a service that enables remote access to the display of the HMI device. VNC clients can be used for remote control of the HMI device.

CAUTION! VNC should be deactivated after use and an automatic start is not recommended.

Parameter	Description
Enable	Activates the VNC server.
Autostart	Keeps the VNC server activated when the HMI device is started.
Port	VNC server waits for connections on TCP port 5900 (default).
Inactivity timeout (seconds)	An inactivity timeout occurs when no user interaction (via keyboard, mouse, transmissions or other RFB protocol interactions) is detected. The special value 0 indicates that the inactivity timeout is deactivated. The default value is 600 (10 minutes).
Multiple clients	Allow multiple sessions on the same port (if disabled, clients already logged in will be disconnected on a new incoming connection).
View only	Do not allow active user interactions (customers can only watch).
Encryption	Activates SSL encryption of connections. **Customised certificate (security/VNC KeyPair)** The certificate of the HMI device, which is required so that the remote VNC client can check the authenticity of the HMI device. The certificate must contain both the private and the public key and can be in .pem format. **The encryption functions are not generally supported, check the compatibility of your VNC client**
Authentication	Whether users are authenticated during session creation. A user-defined VNC-specific password can be set or system passwords can be used (this option is only available if encryption is also enabled)

Example for the creation of a certificate with the OpenSSL library:

```
@echo off set OpenSSL="C:\Program Files\OpenSSL-
Win64\bin\openssl.exe"
set CertificateName=HMI-Certificate
set DeviceIP=192.168.1.56
rem Erzeugen der ZertifikatsschlÃ¼ssel
%OpenSSL% req -x509 -newkey rsa -days 365 -nodes -keyout
private.pem -out public.pem -subj "/ST=NY/C=US/L=New York/
O=Firmenname/OU=Abteilung/CN=ÎrtificateName%" -addext "sub-
jectAltName=IP:ÞviceIP%"
rem .pem-Datei erstellen
copy private.pem + public.pem hmi- certificate.pem
echo.
echo.
pause
```

5.1.9.15 Web server

The parameters available for configuring the web server are displayed on this page. Please note that it is not possible to deactivate the web server as it is required to access the device's system settings.

- **Only allow secure HTTPS connections**
  Disabled by default to maintain backward compatibility, but it is recommended to enable it to improve the security of the HMI device.
- **CORS domains enabled**
  If this option is disabled (default), access to external domains is not permitted. If activated, access to external domains listed in the "CORS domain filter" is permitted.
- **CORS domain filter**
  You can enter the domain to which access is permitted or use a regular expression to define multiple domains. The regular expression must contain the prefix "re:".

  Leave the filter empty (default) if you want to maintain compatibility with older versions and allow access to all domains (this is not recommended).

  Examples of "CORS domain filters":

  – (🌐► www.test.com)
  – re:(🌐► (www.test1.com|)www.test2.com)
  – re:(www.test.(com|org))
  – re:(www.test[1-9]+.com)

5.1.9.15.1 Plugins

This page displays the parameters that are available for configuring the optional plug-in modules connected to the HMI device. Further information can be found in the description of the individual plug-in modules.

5.1.10 Administration

NOTICE! Administration is only available if you are logged in as an administrator.

From the administration area, it is possible to (🌐► "Update system components") of the HMI device.

CAUTION! Working in the management area is a critical process which, if not carried out correctly, can lead to damage to the product, necessitating maintenance of the appliance. Contact technical support for assistance.

Use the "Clear" command in the "Data" section to remove HMI Runtime from the device.

5.1.11 Display

Parameter	Description
Brightness	Brightness level of the display
Back light timeout	Timeout when the backlight is inactive
Orientation	Alignment of the display

5.1.12 Fonts

Lists the available system fonts and gives you the option of uploading your own fonts.

NOTICE! Please note that a licence may be required for the use of font files.

5.1.13 Authentication

Go to edit mode to change the authentication passwords or personalise the x.509 certificate of the HMI device.

5.1.13.1 Users

There are two user names:

- The administrator user name with full access rights is "**admin**".
- The general user name with basic access rights is "**user**".

5.1.13.2 x.509 certificate

The HMI device uses a self-certificate to encrypt Internet communication via the HTTPS protocol. You can personalise the certificate with your company's details and ask a certification authority to validate it.

The procedure for personalising and confirming your certificate is as follows:

1. Go to edit mode and enter the required parameters. Then press the button <GENERATE> to create a self-signed certificate with your data.
2. Export the "Signed certificate request".
3. Send the "Signed certificate request" to a certification authority to confirm it (this is generally a paid service).
4. Import the signed certificate into the HMI device.

The parameters of the certificate

Parameter	**Description**
Device Name	The name of your device.
Organisation	The legal name of your organisation.
Unit	The department of your organisation that processes the certificate.
State	State/region in which your organisation is based.
Location	The city in which your organisation is based.
Country	The two-digit ISO code for the country in which your organisation is based.
valid (days)	Validity of the certificate.
Key Length	Number of bits of the key used by the cryptographic algorithm.

Managed certificates are base64-encoded.

NOTICE! Required BSP v1.0.212 or higher

5.1.14 Restart

Command to restart the HMI device.

5.1.15 EXIT

Use the EXIT command to exit the system settings.

5.2 Cloud / VPN service

The cloud/VPN service enables devices to connect to remote servers via a secure connection.

NOTICE! BSP v1.0.117 or higher is required.

Prerequisites

This service requires external access to the server for VPN setup (default port UDP/1194) and for self-configuration/other advanced functions on TCP port 443 (only in cloud server mode). Therefore, please check the configuration and make sure that no firewalls are blocking these ports.

Setup

If you need to reach end devices behind your gateway device, make sure that the router service is active and set it up as follows:

- WAN port (eth0), which is connected to the main network with Internet access (the cloud server must be accessible from this network).
- LAN port (eth1) connected to one or more end devices (newly created private network).

NOTICE! This function is automatically supported when using a cloud server, but requires additional manual setup for a simple OpenVPN server.

Configuration

Configuration options are available in the "System settings" menu (see "System settings" on page 12).

NOTICE! In the event of a connection error, the repetition time has a geometric progression from BSP v1.0.348: starting with 5s, the next repetition takes place after 2*(previous time). This means 5s, 10s, 20s, 40s, etc. up to a maximum repetition time of 5 minutes. In earlier BSP versions, the repetition time was set to 5 seconds.

Parameter	Description
Enable	Activates the Cloud / VPN service.
Autostart	If this option is selected, the application is started when the HMI device is switched on.
Server type	Select the server type to be used from the available supported server types.
Server	Select the Corvina Cloud Server to be used (only available if the selected server type is "Cloud Server").
Files	Enables the upload of VPN configuration files (only available if the selected server type is "OpenVPN").
Authentication	Select from the available authentication modes: • User name/password • Activation code (only available if the selected server type is "Cloud Server") • Certificate (only available if the selected server type is "OpenVPN") • Certificate + username/password (only available if the selected server type is "OpenVPN") • None (only available if the selected server type is "OpenVPN")
Username	User name for the account of the remote server.

Password	Password for the remote server account.
Show Password	Displays the characters entered in the password.

5.2.1 Cloud server

Cloud Server is a VPN-based solution that enables a seamless connection of users with gateways and end devices. It offers a complete management infrastructure to make this process effortless.

The configuration is automatically downloaded from the cloud server, so the only parameters required are server (host name or IP address), user name and password.

5.2.2 OpenVPN

In this mode, a standard OpenVPN configuration is used to connect devices.

Case A: Provision of configuration files

In remote environments based on an OpenVPN server, system administrators usually provide a set of OpenVPN configuration files directly to end users.

In this case, the configuration is quite simple as it only requires two simple steps:

1. Browse and upload N files (this should include at least one main OpenVPN configuration file, but may also include server and/or client certificates in .pem, .p12 or other formats). Make sure that you select all required files at once by using the platform-dependent multiple selection.
2. Select a suitable authentication type and add login data if necessary.

Now press Save. After a moment, you should see an updated connection status.

Case B: No configuration files available

If your system administrator has not provided any configuration files, you must create the OpenVPN configuration file yourself.

Example 1: User name/password

This example uses:

- User name/password-based authentication
- LZO compression and TAP device
- Server runs on UDP port 1194

openvpn.conf

```
client
dev tap
proto udp
remote testserver.whatever.com 1194
comp-lzo
ca cacert.pem
auth-user-pass
```

This configuration file only refers to a single external file (*cacert.pem*), that is:

- Upload the 2 files using the "Browse" option
- Insert your assigned username and password - note that the auth-user-pass option can also take a file argument, so you can even insert a newline-separated username and password into a new file and specify their name here (not recommended); In this case, you would also select your external file when browsing files and select the authentication method None (from file).

- Save and wait for the status change

Example 2: Simple certificate

This example uses:

- Simple X509 certificate-based authentication
- LZO compression, TUN device, user-defined MTU and AES-128 CBC encryption
- Server runs on TCP port 1195

openvpn.conf

```
tls-client
dev tun
proto tcp
tun-mtu 1400
remote testserver.whatever.com 1195
pkcs12 mycert.p12
ca cacert.pem
cert client.pem
key client.key
cipher AES-128-CBC
comp-lzo
verb 4
```

This configuration relates to 3 files (*cacert.pem*, *client.pem*, *client.key*), i.e:

- Upload the main file *openvpn.conf* and external files (4 in total) with the "Browse" option.
- As no passwords are required, select *None (from file)* Authentication
- *Save* and wait for the status change.

Example 3: Password-protected PKCS #12 certificate

This example uses:

- Certificate-based authentication (password-protected PKCS #12)
- Other parameters than in example 2

openvpn.conf

```
[..]

pkcs12 mycert.p12
```

The PKCS #12 bundle normally contains both CA certificate client keypairs, so this configuration file only refers to an external file (*mycert.p12*). It follows from this:

- Upload both files using the "Browse" option.
- Select certificate authentication.
- Insert the password with which the PKCS #12 bundle containing your certificate is to be decrypted.
- *Save* and wait for the status change.
-

Example 4 2-factor authentication via password-protected PKCS #12 certificate + user name/password

This example uses:

- Certificate-based authentication (password-protected PKCS #12) and user name/password
- other parameters as in example 2

openvpn.conf

```
[..]
pkcs12 mycert.p12
auth-user-pass
```

- Upload both files using the "Browse" option.
- *Select certificate* + user name/password authentication
- *Insert username* and *password* for PSK authentication
- *PKCS #12 Insert password*
- *Save* and wait for the status change

Links

For further details, please refer to the (🌐► OpenVPN documentation).

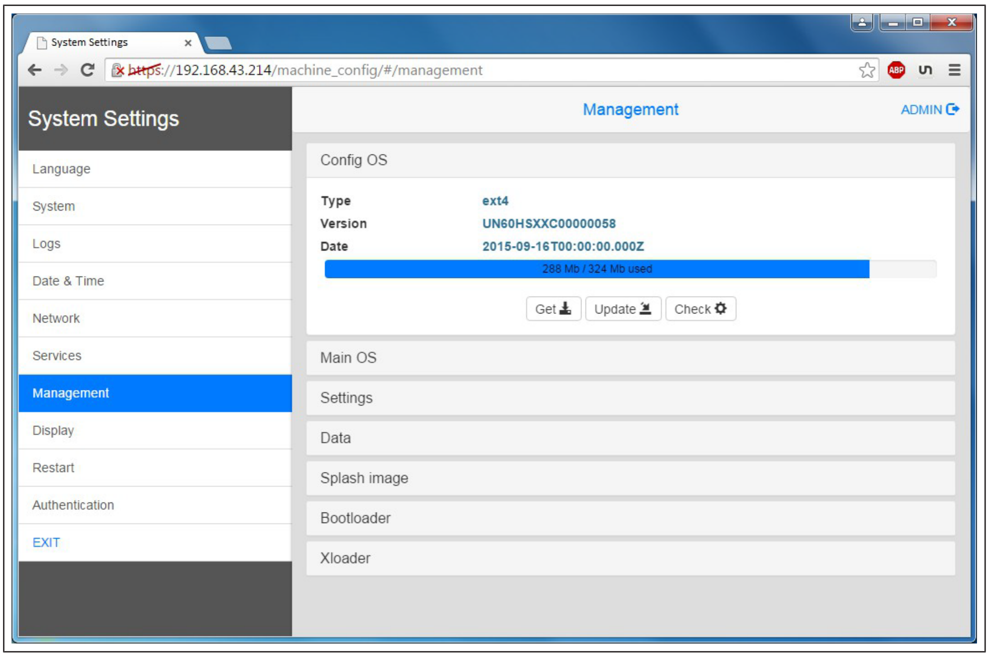
5.3 Update system components

CAUTION! Working in the management area is a critical process which, if not carried out correctly, can lead to damage to the product, necessitating maintenance of the appliance. Contact technical support for assistance (the latest BSP files are provided by technical support).

The system components of the Linux device can be updated locally via a USB memory stick or remotely via a web browser.

To update the system components:

- Call up the system settings in "Config OS" mode by tapping on the HMI.
- Or open the web browser at https://<HMI IP address>/machine_config and select the "Management" section.

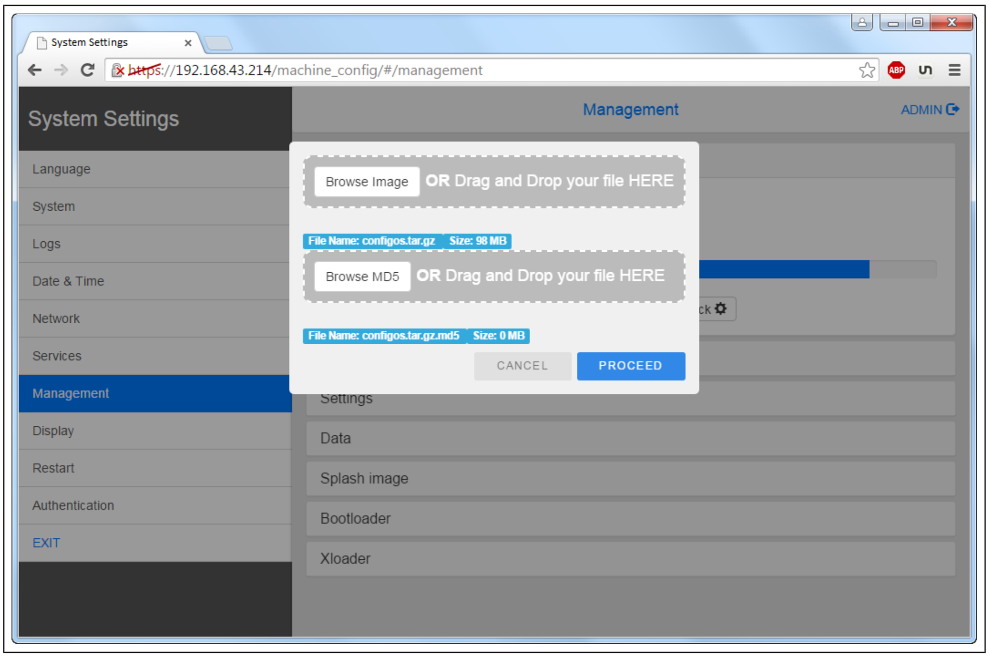


Type ext4
Version UN60HSXXC00000058
Date 2015-09-16T00:00:00.000Z
288 Mb / 324 Mb used

Fig. 28: Management area

Expand the component to be updated and select [Update].

Click on [Browse Image] in the opened dialogue box and select the file "xxx-mainos-xxx.tar.gz". Then click on [Search MD5] and select the file "xxx-mainos-xxx.tar.gz.md5".



File Name: configos.tar.gz Size: 98 MB

File Name: configos.tar.gz.md5 Size: 0 MB

Fig. 29: Select and start image

CAUTION! Do not switch off the device while a system component is being upgraded.

Once the component update is complete, restart the HMI and boot normally.

5.3.1 Call up the system settings in Config OS mode by tapping

The system setting in Config OS mode is available via a tap-tap sequence. This mode can also be accessed if the HMI has a software error.

Immediately after switching on the HMI, the tap-tap function is called up by repeatedly tapping the touchscreen with your finger.

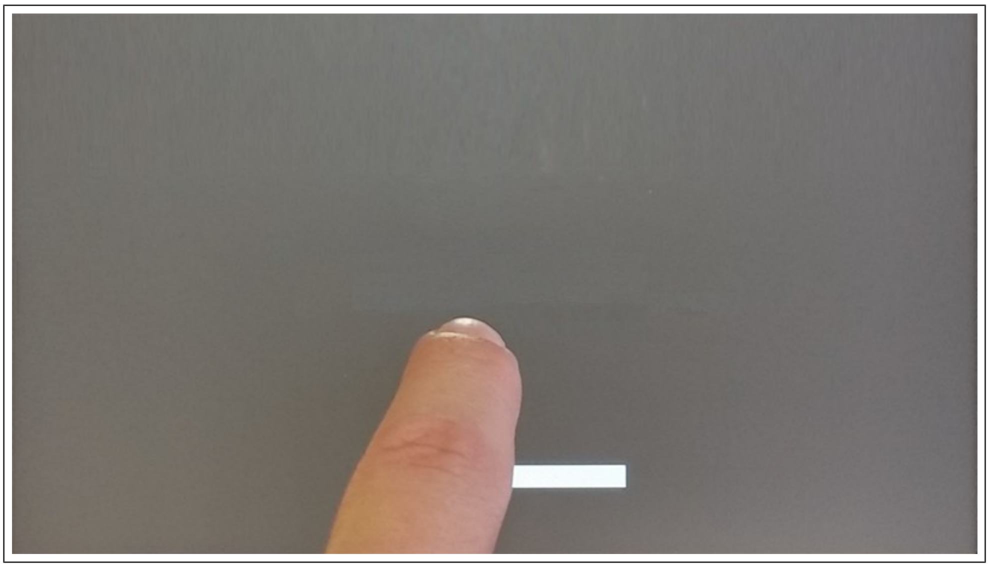
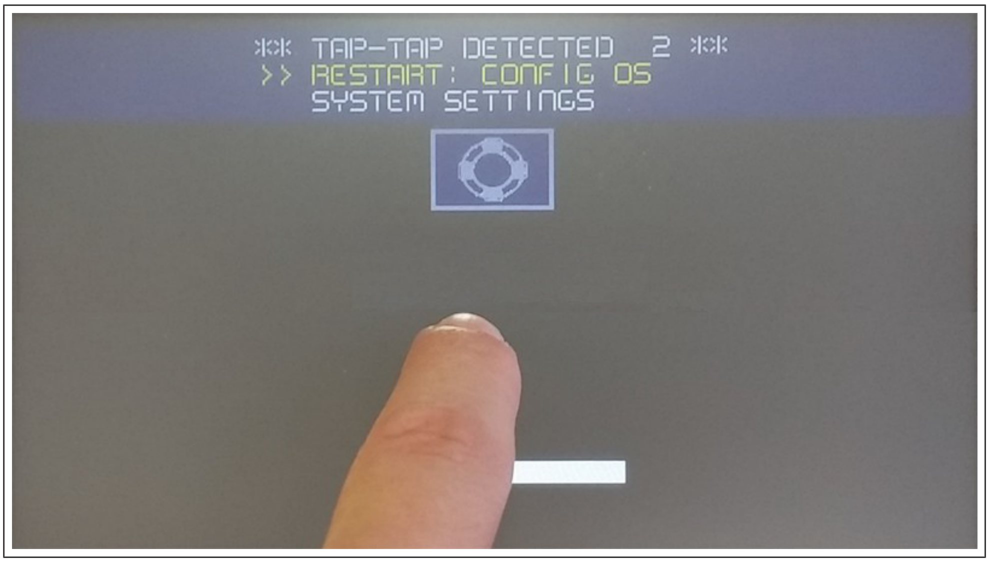


Fig. 30: Start TAP-TAP

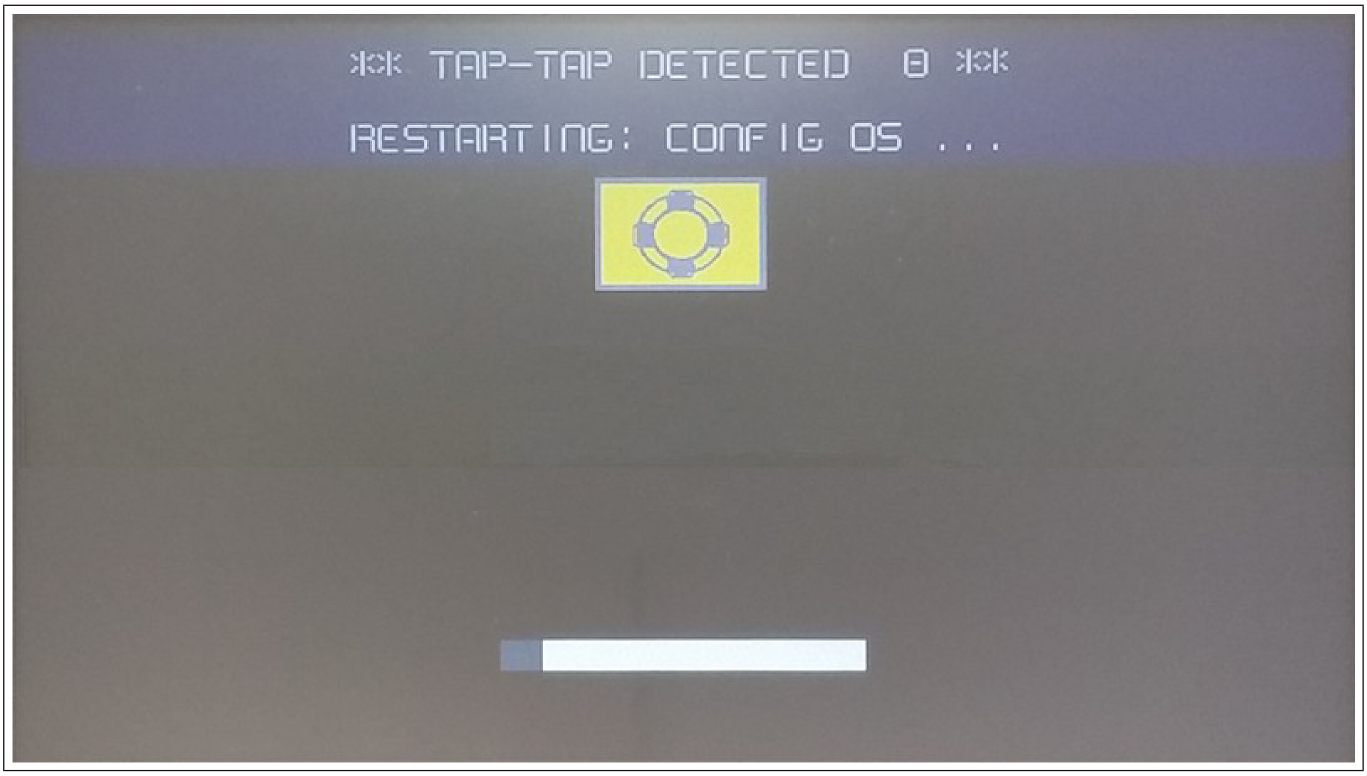
When the message "TAP-TAP DETECTED" appears at the top of the screen, press and hold your finger on the touchscreen to select "Restart": Configure OS".



```
** TAP-TAP DETECTED  2 **
>> RESTART: CONFIG OS
   SYSTEM SETTINGS
```

Fig. 31: Restart: Config OS

The HMI restarts in the system settings in Config OS mode:



** TAP-TAP DETECTED 0 **

RESTARTING: CONFIG OS ...

Fig. 32: Restarting

5.4 Calibration of the touchscreen

The Calibration system setting allows you to calibrate the touchscreen device, which can be accessed by tapping (only available for resistive displays).

Immediately after switching on the HMI, the tap-tap function is called up by repeatedly tapping the touchscreen with your finger.

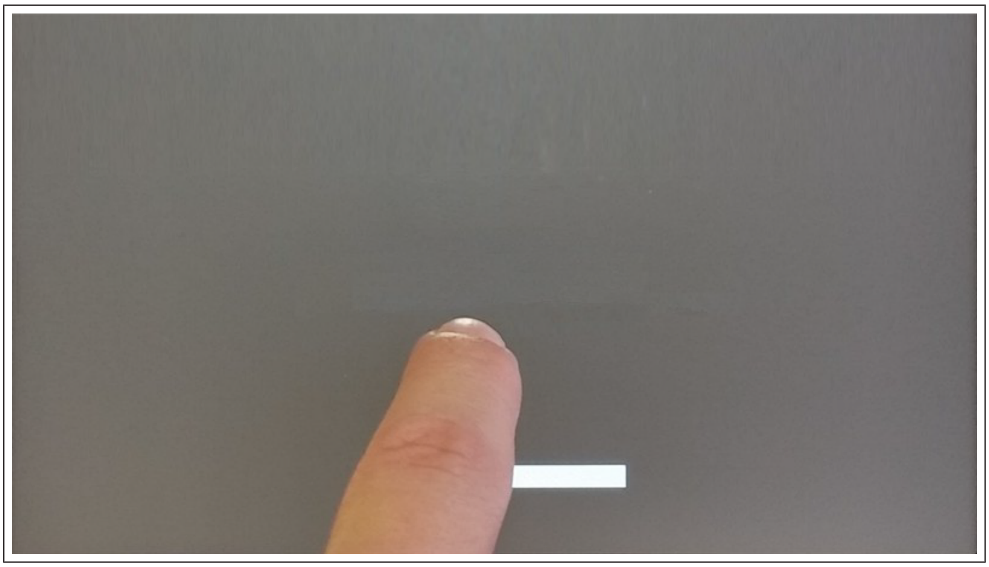
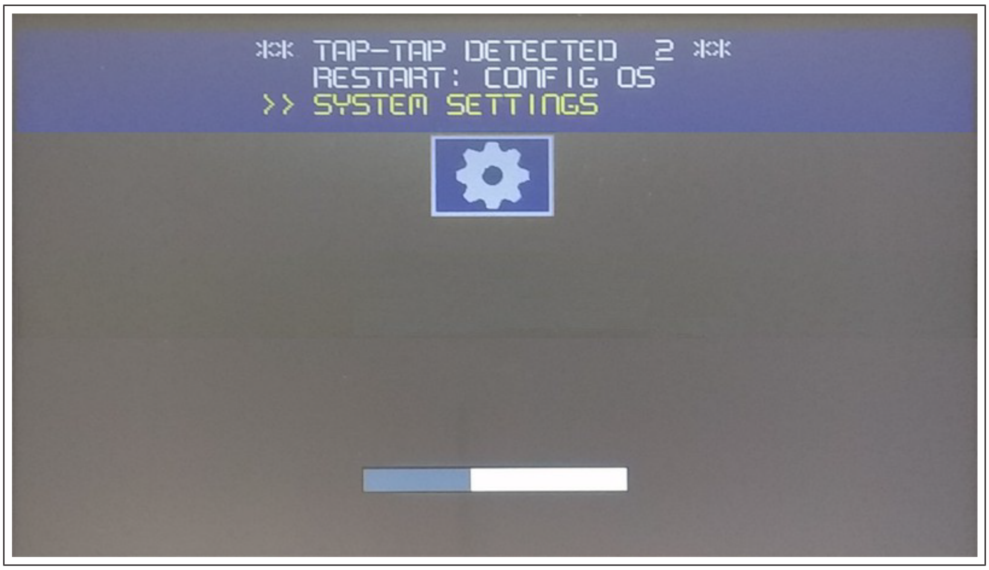


Fig. 33: Start TAP-TAP

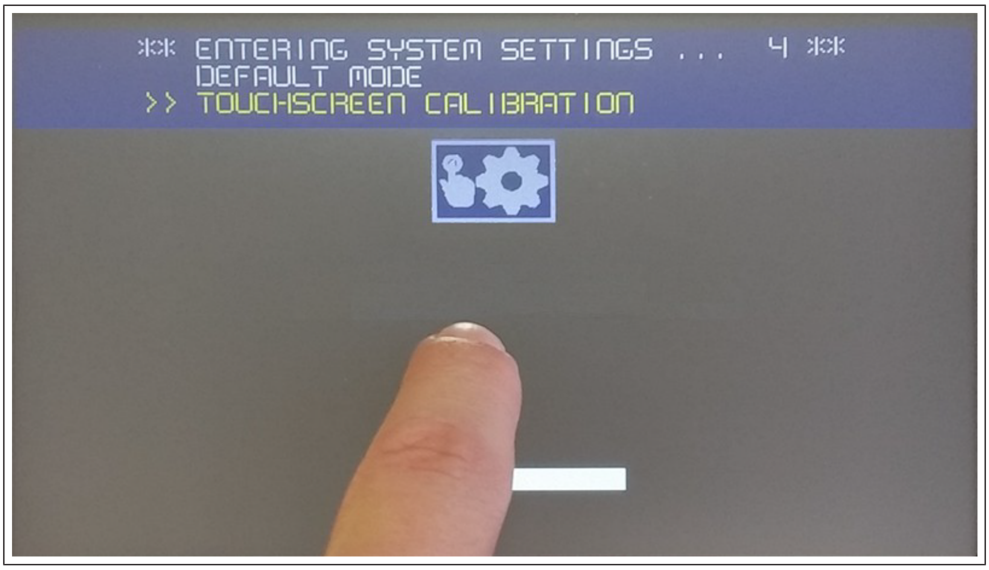
When the message "TAP-TAP DETECTED" appears at the top of the screen. Wait 5 seconds (without touching the screen) to call up the System settings submenu.



```
** TAP-TAP DETECTED  2 **
   RESTART: CONFIG OS
>> SYSTEM SETTINGS
```

Fig. 34: Call up System Settings

Select "Touchscreen calibration". The selection is highlighted in yellow. Press and hold the position for a few seconds until the calibration process for the touchscreen begins.



```
** ENTERING SYSTEM SETTINGS ...   4 **
   DEFAULT MODE
>> TOUCHSCREEN CALIBRATION
```

Fig. 35: Touchscreen calibration

Follow the instructions on the screen to complete the calibration process. The system prompts you to touch certain points to calibrate the touchscreen.

5.5 Password protection

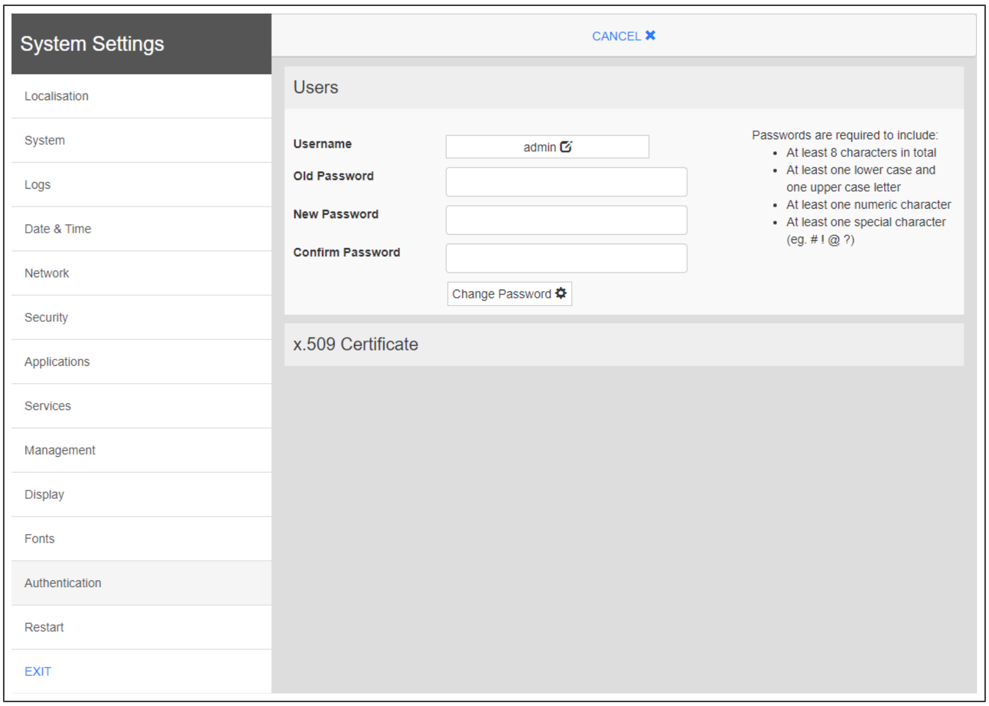
Internal password of the HMI device.

Activate edit mode on the "Authentication" tab in the "System settings" and select the user name to change the associated password.

There are two user names:

The administrator user name with full access rights is "**admin**".

The general user name with basic access rights is "**user**".



Username: admin

Old Password

New Password

Confirm Password

Passwords are required to include:

- At least 8 characters in total
- At least one lower case and one upper case letter
- At least one numeric character
- At least one special character (eg. # ! @ ?)

Fig. 36: Change password

NOTICE! If you have forgotten your password, check the "Forgotten password" option.

NOTICE! When the HMI device is switched on for the first time, you must enter the user "admin" and the password "admin" to set the passwords for both users (admin and user).

Passwords must comply with the following conventions:

At least 8 characters in total.

At least one lowercase and one uppercase letter.

At least one numeric character.

At least one special character (e.g. # ! @ ?).

5.5.1 Forgotten password

If you have forgotten the admin password, you have the option of resetting it to the value "*admin*". Please note that this process deletes the entire memory of the HMI device and all previously downloaded projects are removed.

TAP TAP option

The procedure is only available if it has not been explicitly deactivated via the "Activate device recovery via TAP TAP" option in the device's system settings (see: (≡▶ "Activating device recovery via TAP TAP option" on page 25 [⏵ 25]))

Steps to reset the admin password:

- Switch off the HMI device.
- Switch on the HMI device and start "tapping" the touch panel as soon as the logo appears (see: (≡▶ " [⏵ 41])(≡▶ Password protection" on the previous page [⏵ 41])).

- If "TAP TAP" is recognised, select "System settings" in the first menu, "Standard mode" in the second menu and finally "**Device recovery**" in the third menu.

USB option

The procedure is only available if it has not been explicitly deactivated via the "Activate device recovery via TAP TAP" option in the device's system settings (see: (≡▶ "Activating device recovery via USB" on page 26 [▶ 26])).

Steps to reset the admin password:

- Save the file "*device-factory-restore*" to a USB stick and insert it into the device.
- The device recovery process starts automatically. The buzzer sounds once at the beginning and three times at the end if the process was successful.
- File "*device-factory-restore*" is deleted from the USB stick and the device is rebooted.

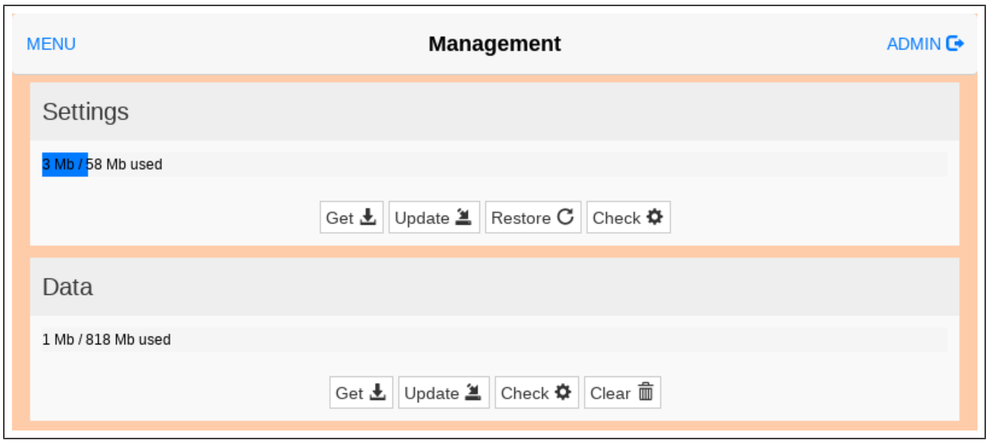
5.6 Backup and restore

To back up or restore all installed applications with their settings, you must open the system settings interface in "Config OS" mode using the tap-tap method.

See "Entering the system settings in Config OS mode by tapping" on page 1

Then log in as an administrator and select the "Administration" option. On this page, you can use the "Retrieve" button to save the contents of the partitions "**Data"** and "**Settings"** to an external storage device (e.g. a USB stick). Instead, use the "Refresh" button to restore the contents of a previous backup.

NOTICE! The Management command is only available if you are logged in as an administrator.



3 Mb / 58 Mb used

1 Mb / 818 Mb used

Fig. 37: Backup and restore management

Data partition

The data partition contains the applications and their settings.

Settings Partition

The settings partition contains the settings of your device (i.e. the configuration parameters that were entered via the system settings interface)

CAUTION! If you update the system settings from a backup, you must be sure that the backup was performed from a device with the same BSP version (Main OS).

The MD5 file

The "Get" command only returns a file with the contents of the partition (e.g. data.tar.gz), but if you want to restore the same file with the "Update" command, you must provide an MD5 checksum file.

The MD5 checksum file must have the same name as the files you want to load, with the extension .md5, e.g:

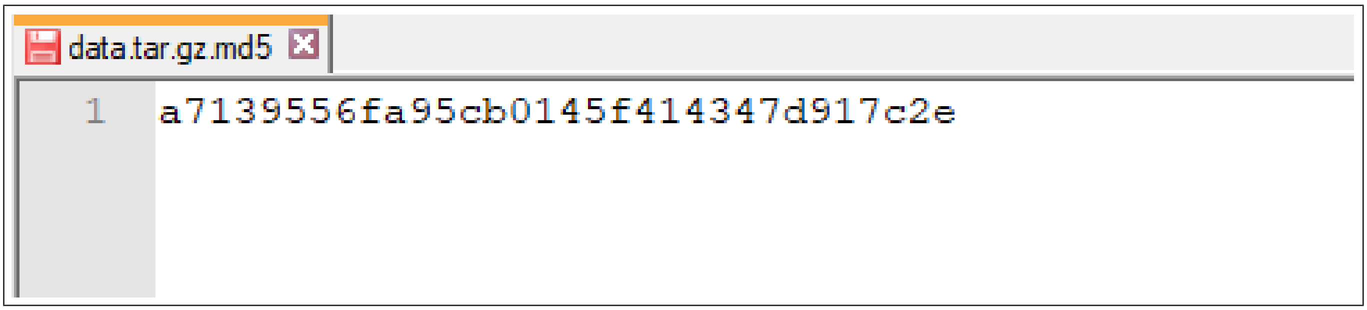
```
data.tar.gz
```

```
data.tar.gz.md5
```

Various tools can be found on the Internet that calculate the MD5 checksum of a file. Under Windows 10, it is also possible to use the "CertUtil" utility on the command line, e.g.

```
CertUtil -hashfile data.tar.gz MD5 > data.tar.gz.md5
```

The MD5 checksum file may only contain one line. If the utility programme that calculates the checksum generates a file with several lines, the additional lines must be deleted.



```
a7139556fa95cb0145f414347d917c2e
```

Fig. 38: MD5 checksum file

KEB

MORE KEB PARTNERS WORLDWIDE:
www.keb-automation.com/contact

Automation **with Drive** **www.keb-automation.com**

KEB Automation KG • Suedstraße 38 • D-32683 Barntrup • Tel: +49 5263 401-0 • E-Mail: info@keb.de