Benutzerhandbuch

Browser auf HMI-Geräten

Installation und Grundeinstellung

Originalanleitung

Dokument 20432551 DE 00

Impressum

KEB Automation KG
Südstraße 38, D-32683 Barntrup
Deutschland
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_de.pdf
Version 00 • Ausgabe 10.04.2025

Inhaltsverzeichnis

1 Einleitung

1.1 Auszeichnungen

1.1.1 Warnhinweise

Bestimmte Tätigkeiten können während der Installation, des Betriebs oder danach Gefahren verursachen. Vor Anweisungen zu diesen Tätigkeiten stehen in der Dokumentation Warnhinweise.

Warnhinweise enthalten Signalwörter für die Schwere der Gefahr, die Art und/oder Quelle der Gefahr, die Konsequenz bei Nichtbeachtung und die Maßnahmen zur Vermeidung oder Reduzierung der Gefahr.

⚠ GEFAHR

Art und/oder Quelle der Gefahr.

Führt bei Nichtbeachtung zum Tod oder schwerer Körperverletzung.

a) Maßnahmen zur Vermeidung der Gefahr.

b) Kann durch ein zusätzliches Gefahrenzeichen oder Piktogramm ergänzt werden.

⚠ WARNUNG

Art und/oder Quelle der Gefahr.

Kann bei Nichtbeachtung zum Tod oder schwerer Körperverletzung führen.

a) Maßnahmen zur Vermeidung der Gefahr.

b) Kann durch ein zusätzliches Gefahrenzeichen oder Piktogramm ergänzt werden.

⚠ VORSICHT

Art und/oder Quelle der Gefahr.

Kann bei Nichtbeachtung zu Körperverletzung führen.

a) Maßnahmen zur Vermeidung der Gefahr.

b) Kann durch ein zusätzliches Gefahrenzeichen oder Piktogramm ergänzt werden.

ACHTUNG

Art und/oder Quelle der Gefahr.

Kann bei Nichtbeachtung zu Sachbeschädigungen führen.

a) Maßnahmen zur Vermeidung der Gefahr.

b) Kann durch ein zusätzliches Gefahrenzeichen oder Piktogramm ergänzt werden.

1.1.2 Informationshinweise

Weist den Anwender auf eine besondere Bedingung, Voraussetzung, Geltungsbereich oder Vereinfachung hin.

Dies ist ein Verweis auf weiterführende Dokumentation. Der Barcode ist für Smartphones, der folgende Link für Online-User oder zum Abtippen.

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

Hinweise zur Konformität für einen Einsatz auf dem nordamerikanischen oder kanadischen Markt.

1.1.3 Symbole und Auszeichnungen

✓	Voraussetzung
a)	Handlungsschritt
⇨	Resultat oder Zwischenergebnis
(≡► Verweis [▸ 5])	Verweis auf ein Kapitel, Tabelle oder Bild mit Seitenangabe
ru21	Parametername oder Parameterindex
(🌐►)	Hyperlink
<Strg>	Steuercode
COMBIVERT	Lexikoneintrag

1.2 Gewährleistung und Haftung

Die Gewährleistung und Haftung über Design-, Material- oder Verarbeitungsmängel für das erworbene Gerät ist den allgemeinen Verkaufsbedingungen zu entnehmen.

Hier finden Sie unsere allgemeinen Verkaufsbedingungen.

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

Alle weiteren Absprachen oder Festlegungen bedürfen einer schriftlichen Bestätigung.

1.3 Urheberrecht

1.4 Gültigkeit der vorliegenden Anleitung

Die vorliegende Gebrauchsanleitung ist für die in der Produktbeschreibung angegebene Software mit der entsprechenden Version gültig. Sie beinhaltet:

- Sicherheitshinweise
- Verwendungszweck
- Installation
- Beschreibung

1.5 Zielgruppe

Die Gebrauchsanleitung ist ausschließlich für Personen bestimmt, die über folgende Qualifikationen verfügen:

- Kenntnis und Verständnis der Sicherheitshinweise.
- Kenntnisse über PCs und das verwendete Betriebssystem.
- Installation von Software.
- Verständnis über die Funktion angeschlossener/ simulierter Geräte/ Modelle.
- Erkennen von Gefahren und Risiken der elektrischen Antriebstechnik.
- Kenntnisse der Automatisierungstechnik.

2 Produktbeschreibung

Webbrowser ist ein leistungsstarker und effizienter HTML5-Browser für HMI-Geräte für modernste Industrieanwendungen.

Die Anwendung wurde für Geräte entwickelt, die auf der Embedded Linux-Plattform und ARM-Prozessoren basieren.

Sofern der Webbrowser nicht vorinstalliert ist, kann einfach auf HMI-Geräten mit der erforderlichen Plattform installiert werden.

3 Installation

Die HMI-Geräte werden ab Werk ohne Runtime ausgeliefert. Beim ersten Einschalten zeigt das HMI den Bildschirm "Runtime Loader" an.

Wenn Sie bereits eine Anwendung installiert haben --- FEHLENDER LINK ---, um die folgende Seite zu aktivieren).

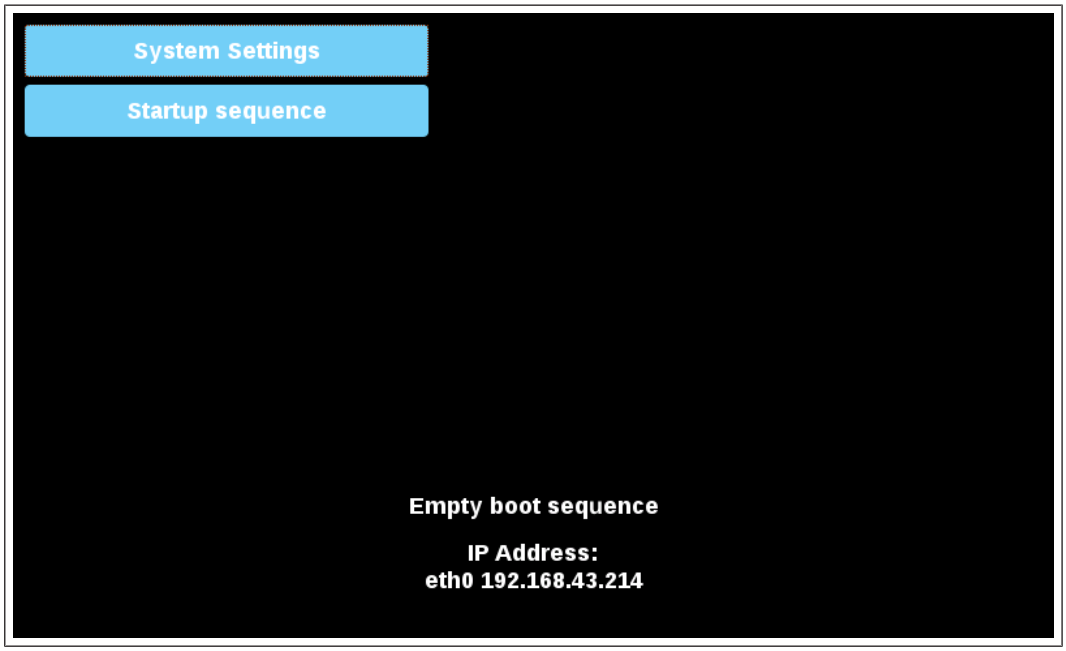

Abb. 1: Systemeinstellungen

3.1 USB

Chromium-Anwendung von USB installieren:

1. Kopieren Sie die Anwendungsdatei auf einen leeren USB-Speicherstick.
2. Wählen Sie beim „Runtime loader“ „Startup sequence“ und dann „Install“.

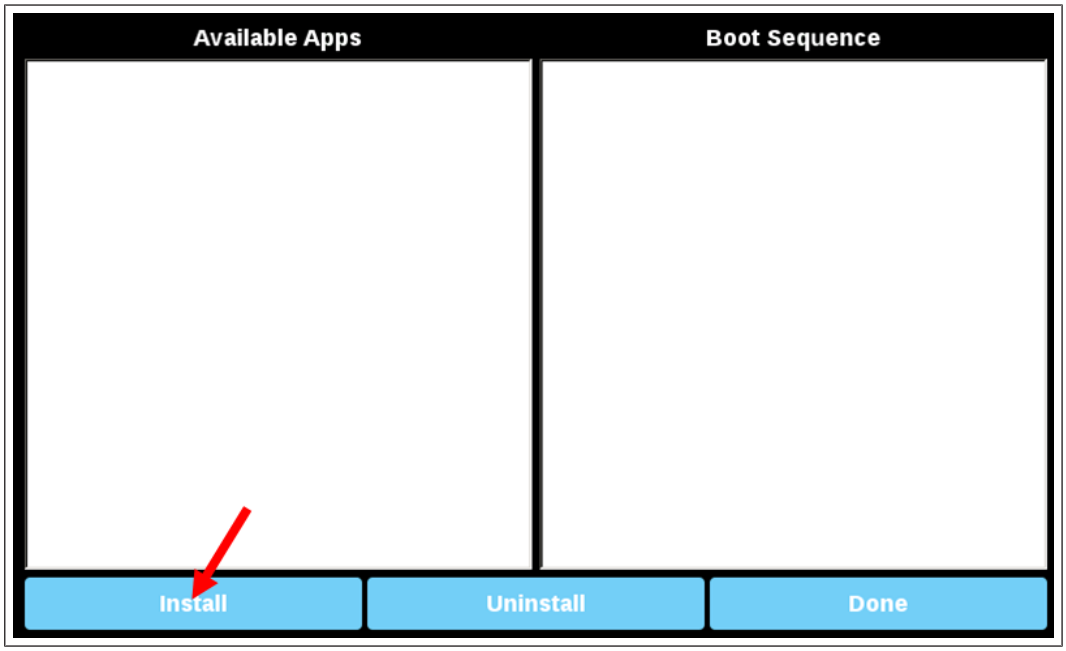

Abb. 2: Apps installieren

3. Öffnen Sie den Ordner "mnt" durch einen Doppelklick.

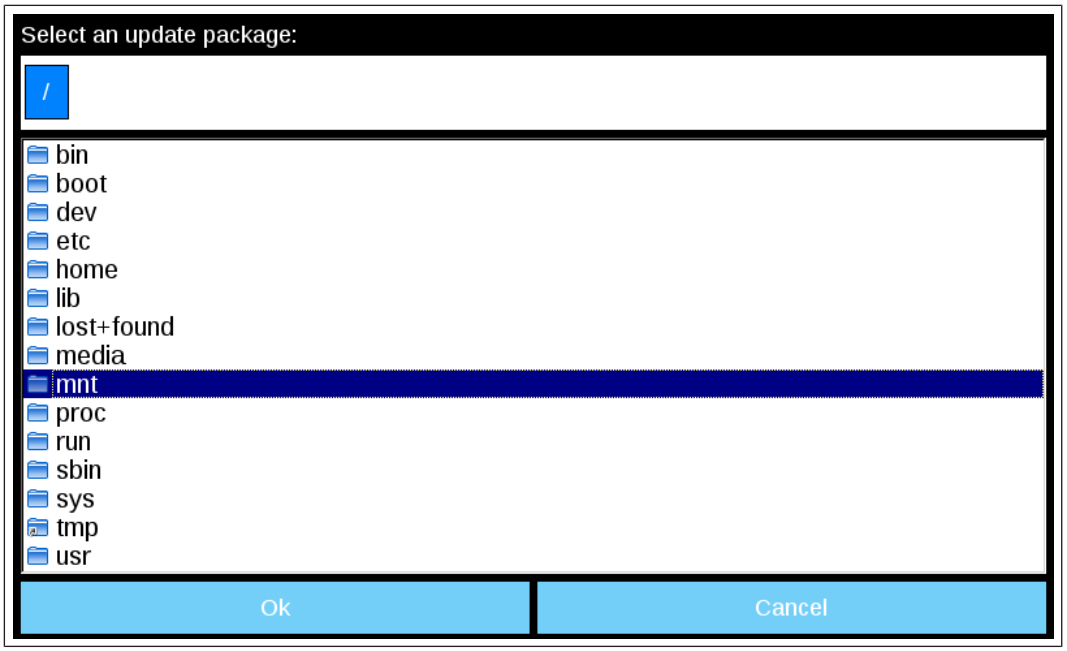

Abb. 3: Ordner mnt auswählen

4. Danach den Ordner „usbmemory“ öffnen.

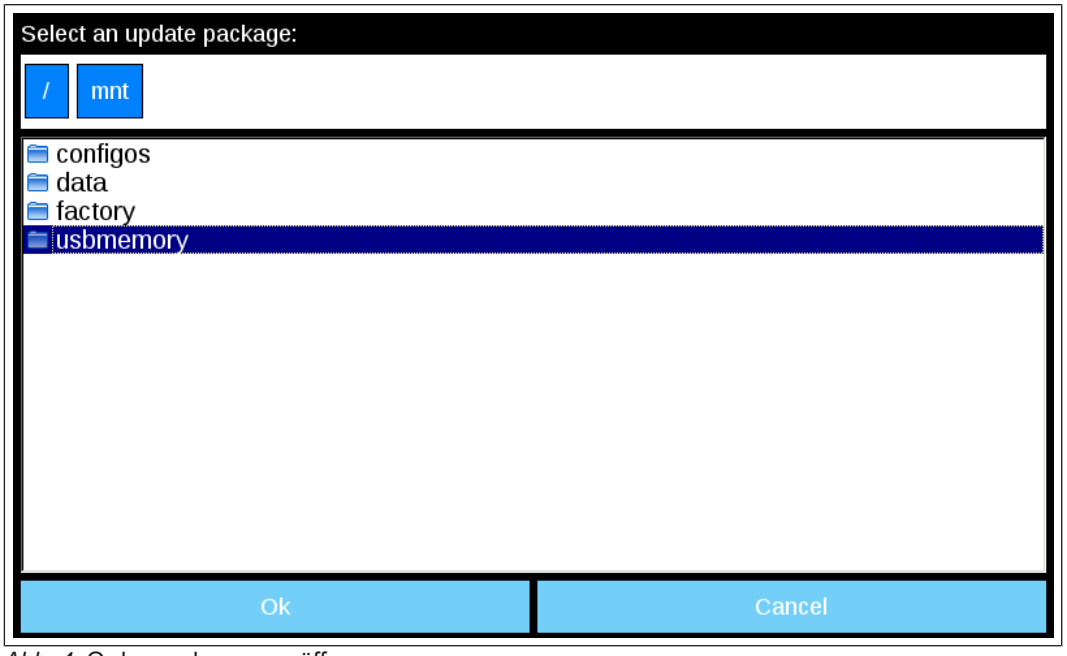

Abb. 4: Ordner usbmemory öffnen

5. Wählen Sie das Chromium-Paket

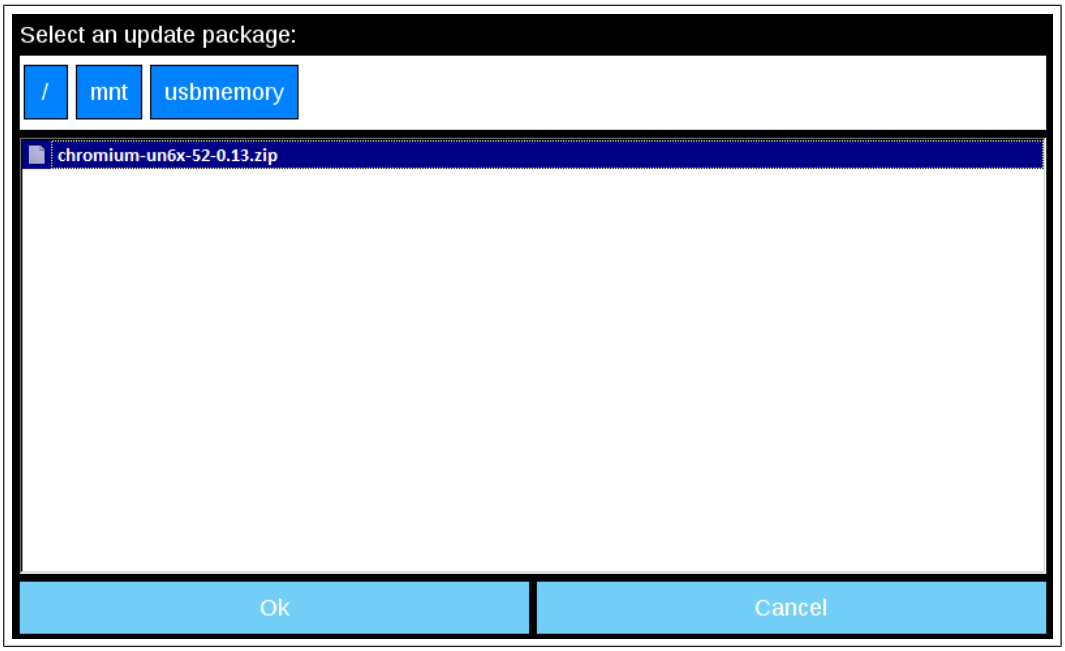

Abb. 5: Chrominum Paket auswählen

6. Die Laufzeitinstallation beginnt.

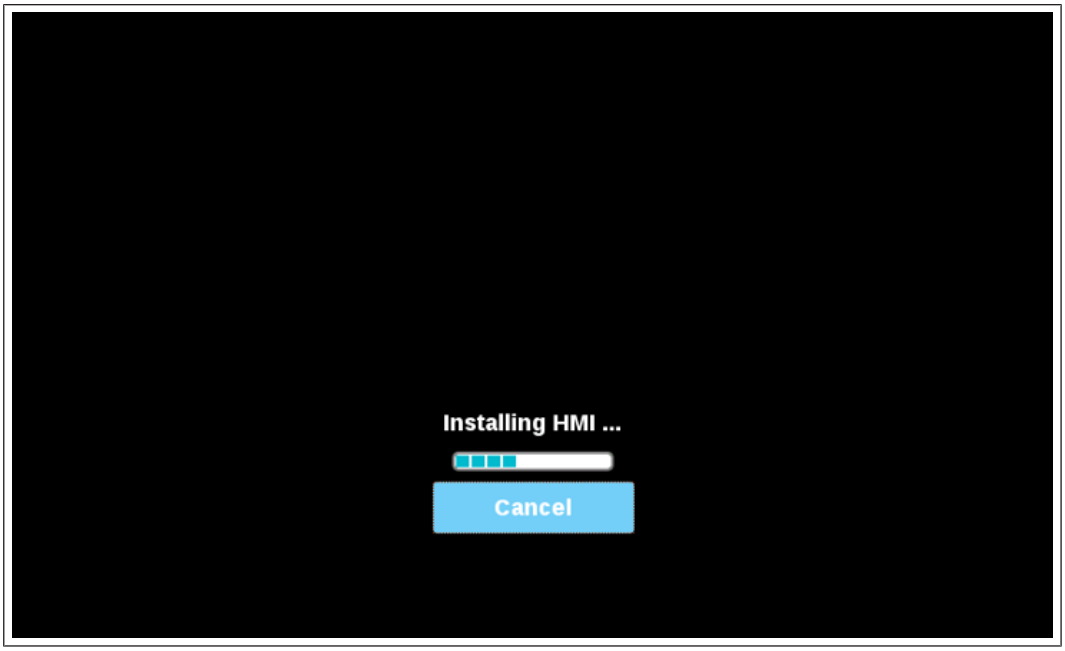

Abb. 6: Installation läuft

ACHTUNG! Unterstützt werden die Dateisysteme FAT16/32 und Linux Ext2, Ext3 und Ext4.

Am Ende des Installationsvorgangs wird das HMI-Gerät neu gestartet und die Chromium-Anwendung wird im Vollbildmodus gestartet.

4 Einstellungen

Der Webbrowser kann mit einer Vielzahl von Eigenschaften an die gewünschte Anwendung angepasst werden. Die konfigurierbaren Eigenschaften sind in zwei Gruppen unterteilt:

- Grundeinstellungen
- erweiterte Einstellungen

Beim ersten Start des Browsers werden die Systemeinstellungen als Startseite angezeigt.

Für den Zugriff auf die Systemeinstellungen ist eine Anmeldung erforderlich. Benutzername und Passwort sind die gleichen wie für das HMI-Gerät (standardmäßig admin, admin). Sie können in den Systemeinstellungen geändert werden.

⚠ WARNUNG

Schutz gegen unberechtigten Zugriff auf das Gerät.

a) Standardpasswort bei Erstanmeldung unbedingt ändern.

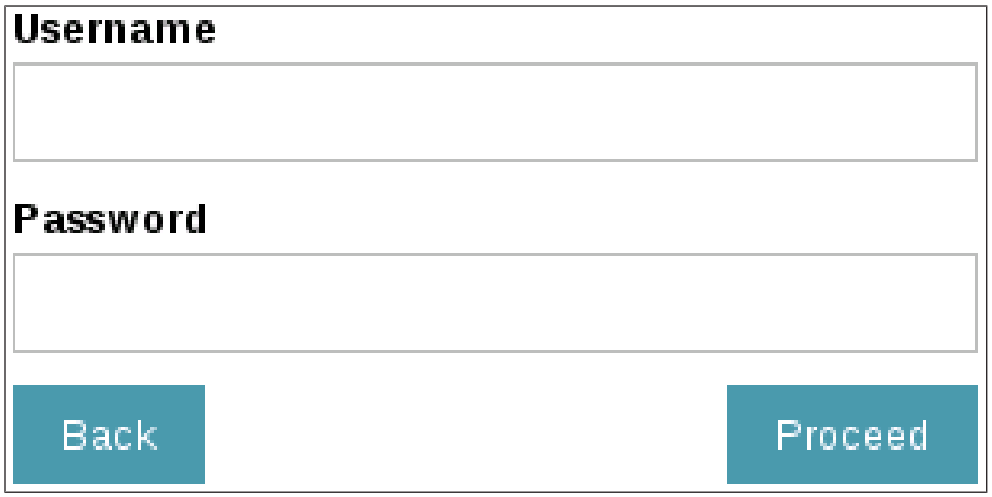

Abb. 7: Anmeldung

4.1 Adressleiste

Wenn der Webbrowser so konfiguriert ist, dass die Adressleiste nicht angezeigt wird, können Sie die Systemeinstellungen aufrufen, indem Sie einige Sekunden lang auf den oberen linken Rand des Displays drücken.

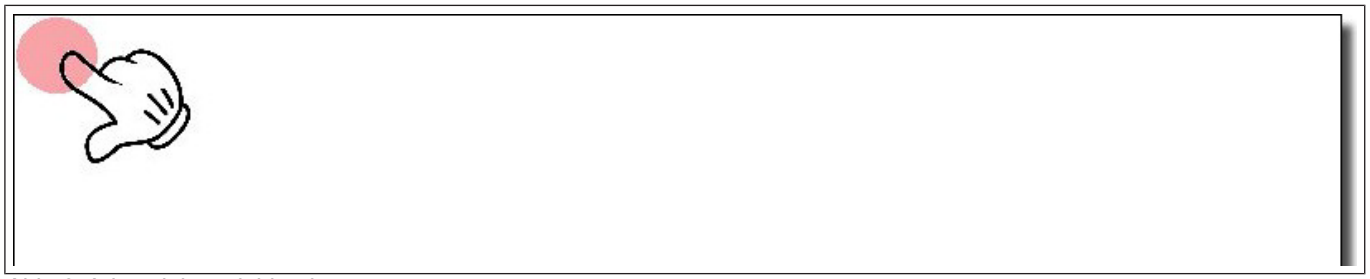

Abb. 8: Adressleiste einblende

Die Systemeinstellungen können über die Schaltfläche Einstellungen in der Adressleiste aufgerufen werden.

Abb. 9: Adressleiste

4.2 Werkzeugleiste

Die Werkzeugleiste kann über den Tab in der Mitte der Adressleiste geöffnet/geschlossen werden.

Abb. 10: Werkzeugleiste öffnen

Folgende Befehle sind verfügbar:

- Seite neu laden
- Verlauf-Schaltflächen
- Lesezeichenliste
- URL-Adresse
- Lesezeichen hinzufügen
- Systemeinstellungen öffnen

4.3 Web-Browser

Wählen Sie die Registerkarte "Webbrowser", um auf die Eigenschaftseinstellungen zuzugreifen. Drücken Sie die Taste "EDIT", um die Werte der Eigenschaften zu ändern

Eigentum	Beschreibung
Beim Start	Legt die Startseite fest.
Homepage	Legt die URL der Startseite fest.
Ausweichseite	Sekundäre Homepage, die geladen wird, wenn die primäre Homepage nicht geladen werden kann. Die URL muss das Protokoll enthalten.
Symbolleiste einschalten	Die Symbolleiste ein-/ausblenden.
Herunterladen von Dateien zulassen	Aktivieren/deaktivieren Sie die Möglichkeit, Dateien herunterzuladen. Die Dateien werden in diesem Ordner gespeichert: /mnt/data/storage/chromium/home/Downloads
Geste für die Verlaufsnavigation aktivieren	Mit der Wischgeste können Sie zwischen den Seiten hin- und herwechseln.
Optionen Druck- und Haltezeit (s)	Legt fest, wie lange auf die linke obere Kante gedrückt werden muss, um die Symbolleiste anzuzeigen.
UserAgent ändern	Setzt den Standardbrowser- Useragent außer Kraft.
Bescheinigungen	Öffnet den Zertifikatsmanager des Webbrowsers (nur bei lokalen Einstellungen verfügbar).
Zertifikat-Einstellungen	Alle in der weißen Liste aufgeführten Seiten löschen.

Virtuelle Tastatur des Systems verwenden	Wenn diese Funktion deaktiviert ist, wird die virtuelle Tastatur des Systems nicht angezeigt. Tasten können über eine physische Tastatur oder über virtuelle Tastaturen, die auf der aktiven Webseite definiert sind, eingegeben werden.
Automatisches Ausfüllen von Formularen aktivieren	Wenn diese Option aktiviert ist, werden bei der Dateneingabe die zuvor eingegebenen Daten vorgeschlagen.
Passwortverwaltung einschalten	Wenn diese Funktion aktiviert ist, fordert der Browser Sie auf, die eingegebenen Passwörter zu speichern, um sie beim nächsten Versuch, sich auf derselben Website anzumelden, erneut vorzuschlagen. **Die Option wird beim nächsten Neustart des Panels aktiviert.**

Die vollständige Liste der verfügbaren Eigenschaften finden Sie unter "Systemoptionen" auf Seite 7

4.4 Warnungen einschalten

Um die deaktivierten Warnmeldungen (z. B. die Zertifikatswarnungen) wieder zu aktivieren, verwenden Sie den folgenden Befehl, der in der Symbolleiste des Webbrowsers verfügbar ist.

Anmerkung:

Im Kioskmodus ist die Option nicht zugänglich.

Die Einstellungen werden erst nach Neustart übernommen.

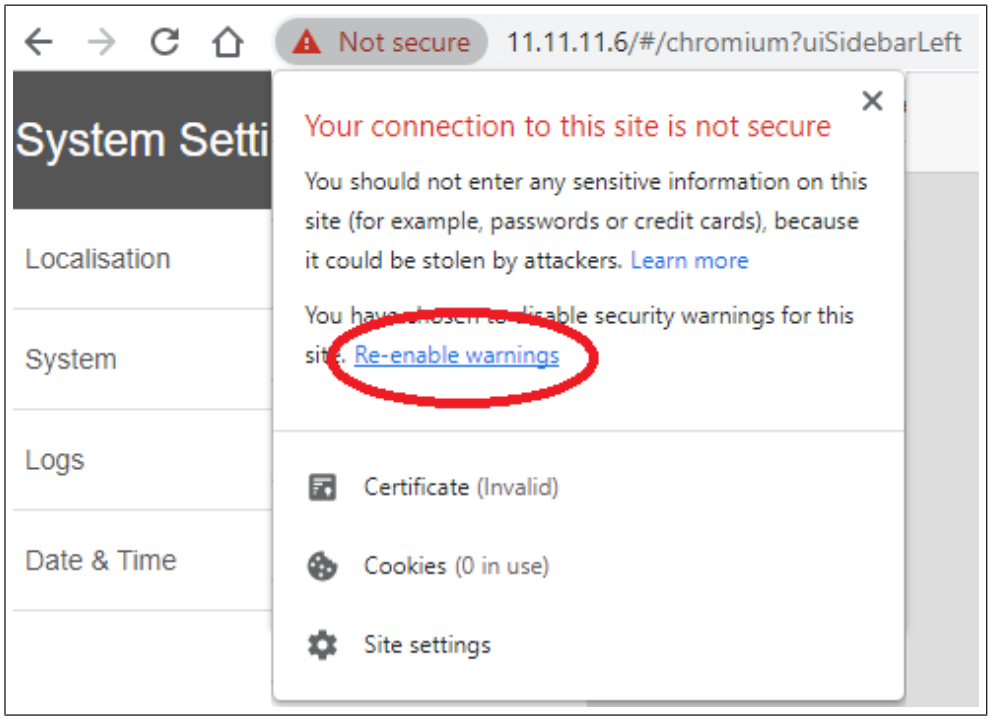

Abb. 11: Warnung einschalten

Die Warnmeldung kann auch auf der Seite Systemeinstellungen aktiviert werden:

Pfad: Systemeinstellungen -> Webbrowser -> Zertifikatsvorgaben -> Zertifikatswarnungen wieder aktivieren.

4.5 Systemoptionen

Die Systemoptionen können beim Start mit Hilfe von Befehlszeilenargumenten oder durch Hinzufügen einer Einstellungsdatei definiert werden.

Verwendung von Befehlszeilenargumenten

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

Einstellungsdatei verwenden

Jede Kommandozeilenoption kann auch durch Erstellen der folgenden Datei festgelegt werden:

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

Die Optionen können jeweils einzeln pro Zeile in die Datei eingefügt werden.

4.5.1 Verfügbare Systemoptionen

Option	Beschreibung
--homepage=<uri>	Homepage-Einstellung außer Kraft setzen.
--enable-exit-button	Aktiviert die Schaltfläche "Beenden" auf der Optionsseite und das Symbol "X" in der Symbolleiste, wenn es aktiviert ist. Schließt den Webbrowser.
--enable-restart-button	Aktiviert die Schaltfläche "Beenden" auf der Optionsseite und das Symbol "X" in der Symbolleiste, wenn es aktiviert ist. Starten Sie den Webbrowser neu.
--enable-window-exit-button	Wie oben, aber es wird nur das Fenster geschlossen. In diesem Fall wird beim Neustart des Webbrowsers ein neues Fenster geöffnet, was schneller ist. Befehlszeilenflags, die beim ersten Mal angegeben werden, können später nicht mehr geändert werden, da hierfür ein vollständiger Neustart erforderlich ist. Stattdessen kann eine andere URL angegeben werden.
--enable-toolbar	Aktiviert die Symbolleiste. Die Einstellung wird gespeichert, so dass sie beim nächsten Mal auch ohne diese Option aktiviert ist.
--enable-toolbar-navigation	Anzeigen der Navigationsschaltflächen für den Verlauf in der Symbolleiste
--enable-toolbar-on-error	Die Symbolleiste wird nur angezeigt, wenn beim Laden der Seite ein Fehler auftritt. Die Einstellung wird gespeichert, so dass sie beim nächsten Mal auch ohne diese Option aktiviert wird.
--fixed-toolbar	Die Symbolleiste wird fixiert und nicht eingeklappt.
--disable-toolbar	Deaktiviert die Symbolleiste. Die Einstellung wird gespeichert, so dass sie beim nächsten Mal auch ohne diese Option aktiviert ist.
--disable-toolbar-url	Entfernt den URL-Textbereich aus der Symbolleiste. Bei Verwendung nimmt die Symbolleiste nicht mehr die gesamte Breite des Bildschirms ein und wird stattdessen zentriert.
--enable-toolbar-bookmarks	Aktiviert die Schaltflächen "Lesezeichenliste" und "Lesezeichen hinzufügen" in der Symbolleiste, wenn sie aktiviert sind. Die Schaltfläche "Lesezeichen hinzufügen" wird weiterhin ausgeblendet, wenn --disable-toolbar-url verwendet wird. Wenn sie deaktiviert ist, wird die Symbolleiste nicht aktiviert.

--disable-toolbar-options	Entfernt die Optionsschaltfläche aus der Symbolleiste. Die Symbolleiste wird nicht aktiviert, wenn deaktiviert.
--disable-options	Wie oben, aber zusätzlich wird das lange Drücken deaktiviert, so dass es nicht mehr möglich ist, die Optionsseite zu öffnen. Bei einem Ladefehler versucht es der Browser erneut, und auch in diesem Fall wird die Optionsseite nie geöffnet.
--disable-toolbar-reload	Entfernt die Schaltfläche "Neu laden" aus der Symbolleiste.
--loadingPage=<URL>	Zeigt eine benutzerdefinierte Seite an, die beim Booten geladen wird, während die eigentliche Seite geladen wird. Dadurch wird auch die Standardfehlerseite ausgeblendet, wenn der Server nicht bereit ist. Die Ladeseite wird so lange angezeigt, bis der Browser das Laden des Projekts abgeschlossen hat oder die maximale Anzahl von Ladeversuchen erreicht wurde. Die URL muss das Protokoll enthalten (d.h. http://, file://). Wenn keine URL angegeben wird (nur "--loadingPage"), wird eine weiße Seite verwendet. Wenn das Webprojekt nicht geladen werden kann, wird die Ausweichseite angezeigt, sofern diese eingestellt ist. Ansonsten wird die Login-Seite geladen. Die Symbolleiste kann aktiviert werden und in der loadingPage angezeigt werden. "--enable-toolbar-on-error" wird ebenfalls unterstützt, in diesem Fall wird die Symbolleiste erst nach einem zweiten fehlgeschlagenen Versuch, das Webprojekt zu laden, angezeigt.
--fallback-url=<uri>	Eine sekundäre Homepage, die geladen wird, nachdem open-options-after-num-retries fehlgeschlagen ist, versucht, die primäre zu laden. Wenn auch diese nicht verfügbar ist, wird die Optionsseite geladen. Die URL muss das Protokoll enthalten.
--open-options-after-num-retries=<n>	Legen Sie fest, nach wie vielen Wiederholungsversuchen bei Ladefehlern die Anmeldeseite geöffnet wird (Standard ist 4). Ein Wert <1 wird die Funktion deaktivieren.
--wiederholte-auf-Fehler-Zeitüberschreitung=<n>	Zeit in Sekunden zwischen den Wiederholungsversuchen. Der akzeptierte Mindestwert ist 5 (Standard ist 8).
--disable-fallback-reload	Wenn diese Option aktiviert ist, lädt der Browser nicht mehr neu, wenn das Laden der Fallback-Seite fehlschlägt, und bleibt auf der Fehlerseite. Standardmäßig wird die Optionsseite geöffnet und das Neuladen im Hintergrund fortgesetzt.
--Erster-Lade-Wiederholung	Der Browser sollte nur während des ersten Ladevorgangs versuchen, den Server erneut zu kontaktieren. Nach dem erfolgreichen Laden einer Seite sollten keine automatischen Neuladungen mehr durchgeführt werden.

4.5.2 Laden der Homepage

Wenn der Webbrowser so konfiguriert ist, dass beim Start eine Homepage geladen wird, gehen Sie wie folgt vor:

Öffnen Sie eine erste Registerkarte mit einer lokalen "Ladeseite". Diese Seite kann mit „--loading-page“ geändert werden.

Starten Sie das Laden der Homepage auf einer zweiten Registerkarte, während Sie auf der ersten bleiben. Wechseln Sie zur zweiten, sobald die Seite geladen ist.

Wenn die Homepage nach „--open-options-after-num-retries“ nicht geladen wurde, wird bei Angabe von „--fallback-url“ versucht, die Fallback-URL zu laden.

Optionsseite öffnen, wenn die Fallback-URL nicht festgelegt ist oder nicht geladen werden kann.

„—Homepage“ sollte die Homepage-URL überschreiben und die Option auf der Einstellungsseite ausblenden.

4.5.3 Initiale Konfiguration

In der Datei "browser.ini" können Sie die Konfiguration festlegen, die nur einmal beim ersten Start des Webbrowsers angewendet wird. Während der normalen Nutzung können die Benutzer die Konfiguration über die Seite "Systemeinstellungen" oder die Optionsflags ändern.

Die Datei "browser.ini" muss in den Installationsordner des Webbrowsers (/mnt/data/hmi/chromium/deploy) kopiert werden. Die Einstellungen werden beim nächsten Neustart übernommen und zu diesem Zeitpunkt wird die Datei "browser.done" im selben Ordner erstellt, um eine zweite Neukonfiguration zu vermeiden.

Wenn die Datei "browser.done" entfernt wird, wird beim nächsten Neustart eine Neukonfiguration erzwungen.

Unterstützte Tasten

- homepageLink=<url>
  Die URL muss das Protokoll enthalten (d.h. http://, file://)
- customUserAgent=<userAgent>
- showToolbarOnError=<true|false>
- showWiFiStatus=<true|false>
- showHistoryButton=<true|false>
- showLoadingBarAndStopButton=<true|false>
- onStartup=<Einstellungen|Homepage|LastVisistedPage>
- enableToolbar=<true|false>
- holdTimer=<ms>
  Timeout in ms für langes Drücken, mindestens 2000 (2s)
- fallbackToDefaultPageLink=<url>
  Die URL muss das Protokoll enthalten (d.h. http://, file://)
- disableFallbackReload=true

Beispiel für die Datei browser.ini

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

5 System-Konfiguration

Die Systemeinstellungen sind in den HMI-Geräten als Werkzeug für die Konfiguration der Systemeigenschaften des Geräts verfügbar.

5.1 Systemeinstellungen

Die Benutzeroberfläche der Systemeinstellungen basiert auf HTML-Seiten und kann sowohl lokal auf dem Bildschirm des HMI-Geräts als auch per Remote über einen Webbrowser aufgerufen werden.

Der Administrator-Benutzername mit vollem Zugriffsrecht ist "admin" mit dem Standardpasswort "admin". Allgemeiner Benutzername ist "user" mit dem Standardpasswort "user".

⚠ WARNUNG

Schutz gegen unberechtigten Zugriff auf das Gerät.

a) Systemeinstellungen => Authentifizierung aufrufen.

b) Administrator- und Benutzerpasswort unbedingt ändern.

Für den Zugriff auf die Systemeinstellungen vom HMI-Gerät aus ist die Eingabe eines Passworts nicht erforderlich, solange das Standardpasswort "admin" nicht geändert wird.

5.1.1 Eingabe in Systemeinstellungen

Es gibt mehrere Möglichkeiten, die Seite Systemeinstellungen aufzurufen:

- Über einen Webbrowser
- Vom HMI-Gerät, wenn keine Laufzeit geladen ist
- Vom HMI-Gerät aus über das Tap-Tap-Verfahren

5.1.1.1 Zugriff auf die Systemeinstellungen über den Webbrowser

Um über einen Webbrowser auf die Systemeinstellungen zuzugreifen, geben Sie die IP-Adresse des Geräts in folgendem Format ein:

https://IP/machine_config

Beachten Sie, dass der Fernzugriff über das verschlüsselte https-Protokoll an Port 443 erfolgt. Wenn die Verbindung hergestellt ist, sendet das HMI-Gerät ein Zertifikat, das für die Verschlüsselung verwendet wird. Da das Zertifikat nicht von einer Zertifizierungsstelle signiert ist, erhalten Sie eine Warnmeldung. Bitte klicken Sie auf die erweiterten Optionen und wählen Sie weiter.

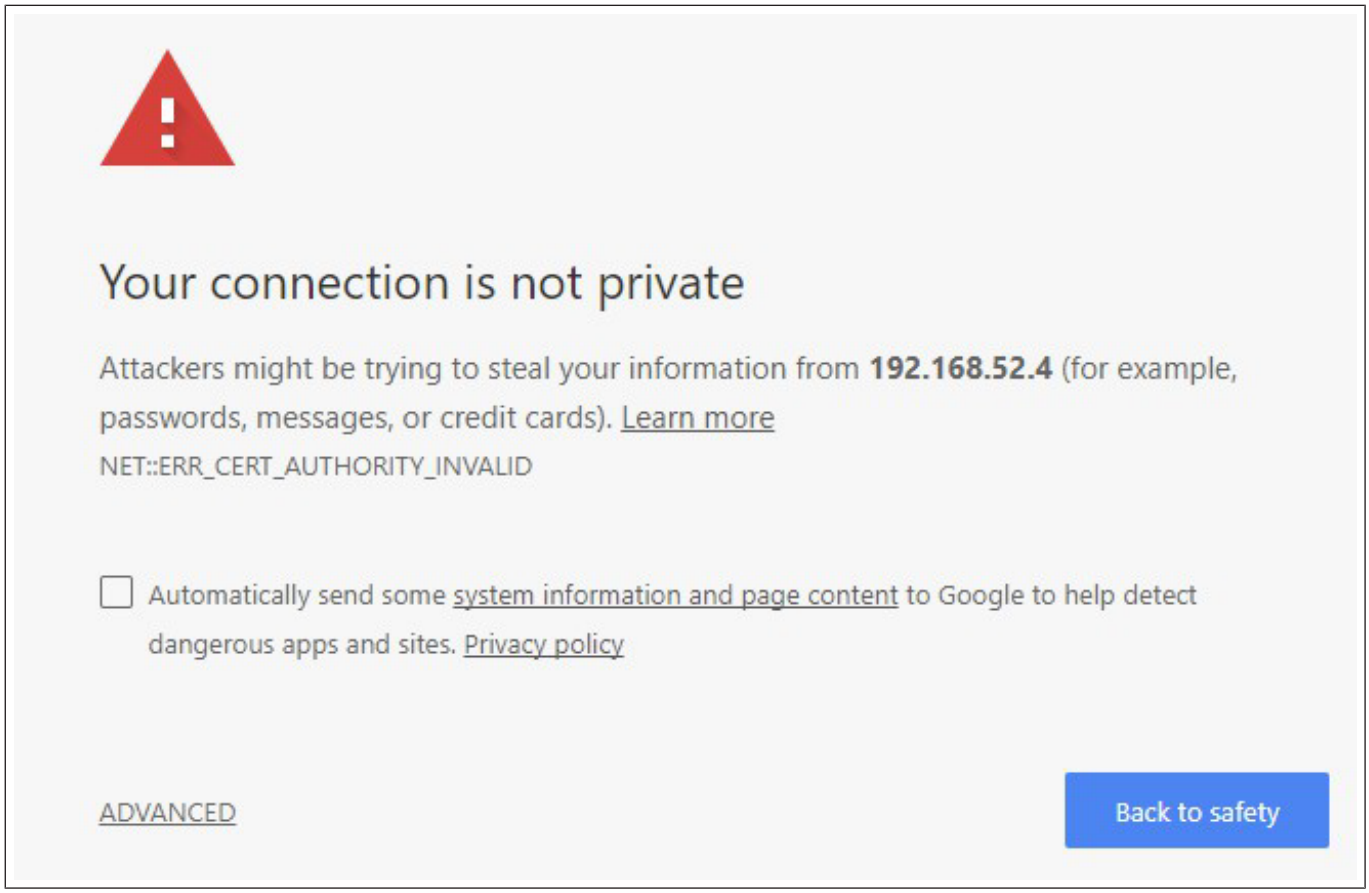

Abb. 12: Warnmeldung Zertifikat

Die vom HTTPS-Server im Linux-HMI-Gerät vorgeschlagenen Standardsicherheitsprotokolle sind:

SSLv3 256 Bits ECDHE-RSA-AES256-SHA

TLSv1 256 Bits ECDHE-RSA-AES256-SHA

WARNUNG! Wir raten von der Verwendung von CBC-Cyber-Suites im Zusammenhang mit SSL3- oder TLSv1.0-Verbindungen ab, da sie von einigen Schwachstellen betroffen sein könnten.

5.1.1.2 Zugriff auf Systemeinstellungen vom HMI-Gerät

Wenn Runtime nicht installiert ist, sind die Systemeinstellungen über den Bildschirm Runtime Loader zugänglich.

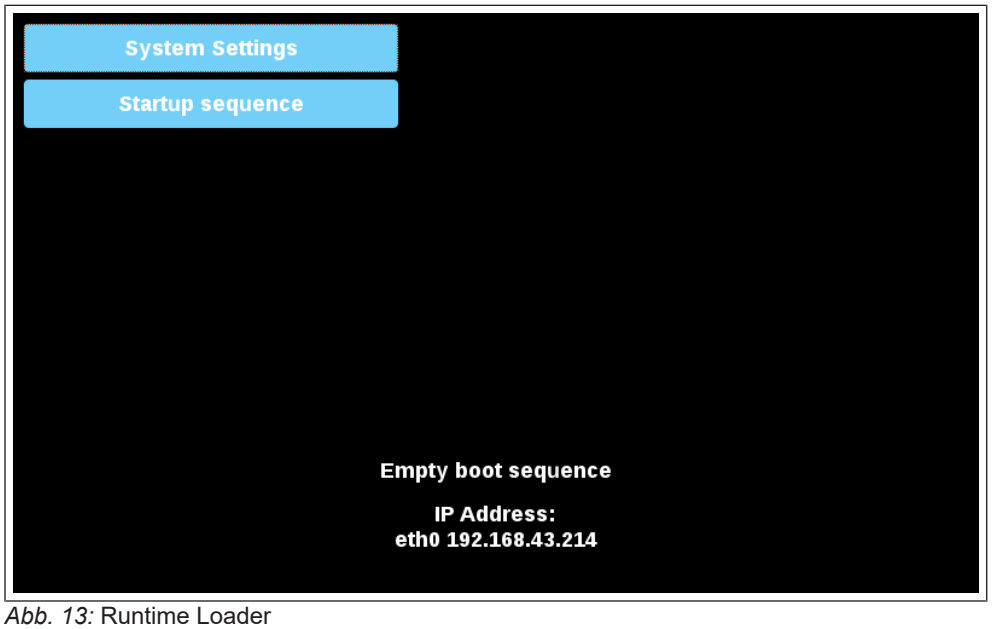

Abb. 13: Runtime Loader

Wenn die Runtime installiert ist, können Sie auf die Systemeinstellungen zugreifen, indem Sie im Kontextmenü die Option "Show system settings " auswählen.

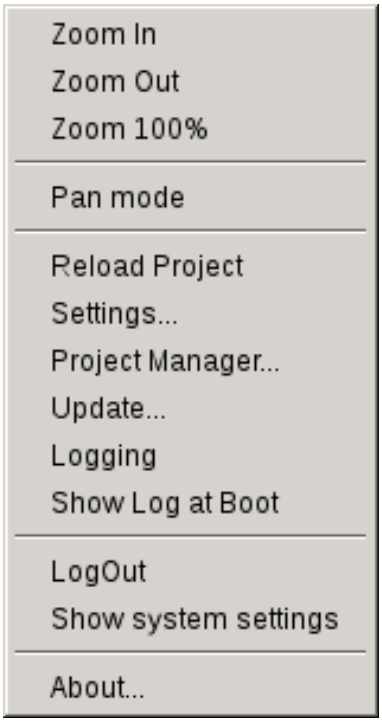

Abb. 14: Systemeinstellungen anzeigen

5.1.1.3 Aufrufen der Systemeinstellungen durch Antippen (TAP-TAP)

Unmittelbar nach dem Einschalten der HMI wird durch wiederholtes Antippen des Touchscreens mit dem Finger die Tap-Tap-Funktion ausgerufen.

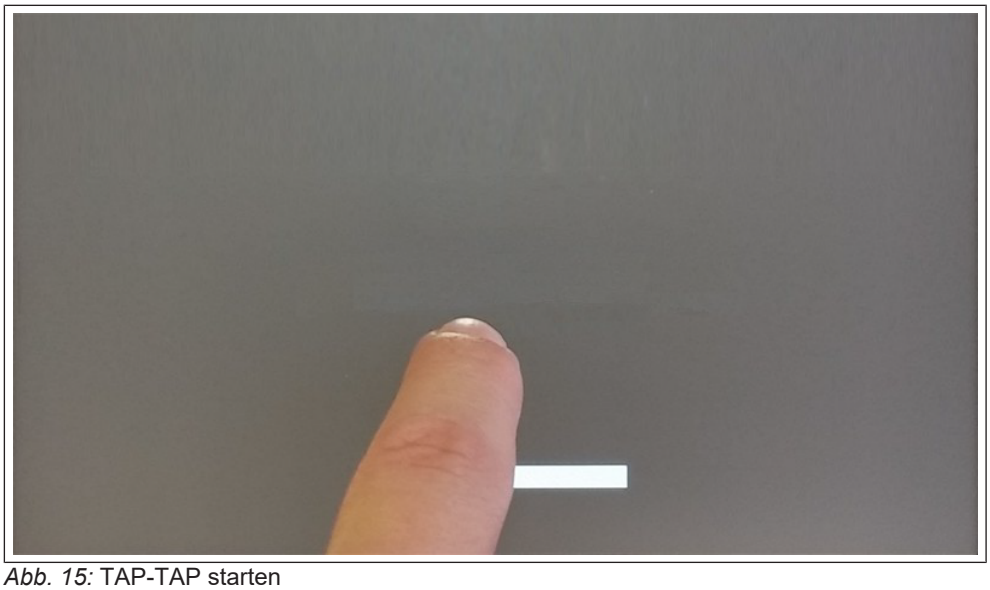

Abb. 15: TAP-TAP starten

Wenn die Meldung "TAP-TAP DETECTED" (Tap-Tap erkannt) oben auf dem Bildschirm erscheint. Warten Sie 5 Sekunden (ohne den Bildschirm zu berühren), um das Untermenü Systemeinstellungen aufzurufen.

Abb. 16: TAP-TAP erkannt

Warten Sie weitere 5 Sekunden (ohne den Bildschirm zu berühren), um in den Default Mode (Standardmodus) zu gelangen.

Abb. 17: Default Mode

Die Schaltflächen "Systemeinstellung" und "Startsequenz" sind nun verfügbar.

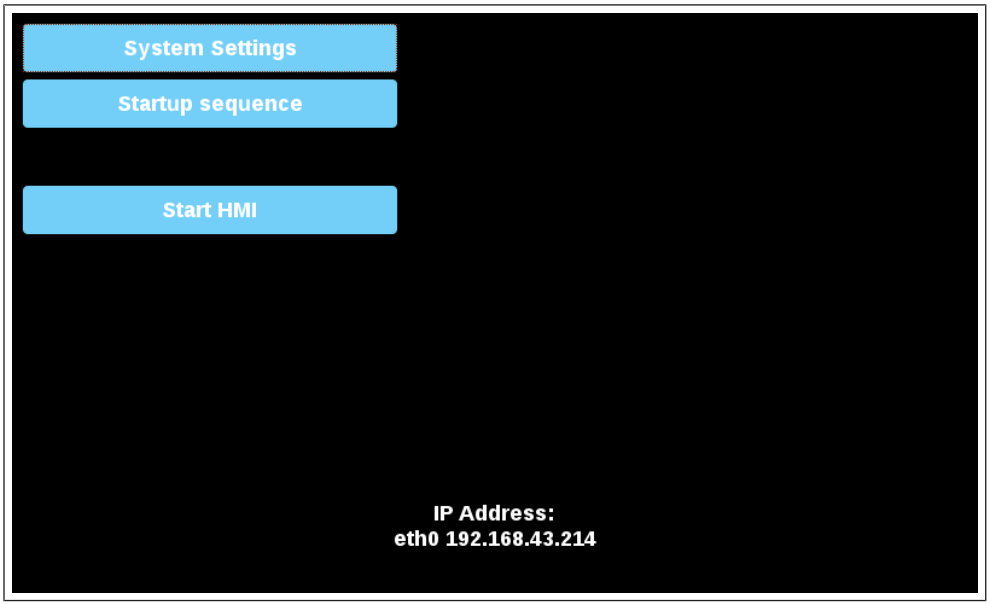

Abb. 18: Startbildschirm

5.1.2 Lokalisierung

Stellen Sie die folgenden Parameter ein, um das Gerät an Ihr Land anzupassen.

- Ländercode (nur bei WiFi erforderlich)
- Sprache für die Oberfläche der Systemeinstellungen
- Layout der virtuellen Tastatur

Der Ländercode ist für die WLAN-Regulierungsdomäne erforderlich, und das Gerät wird das WiFi erst nutzen, wenn dieser Parameter nicht eingestellt ist.

Die Ländereinstellungen sind für den zulassungskonformen Betrieb erforderlich. Die Auswahl eines Landes, das nicht mit dem Land übereinstimmt, in dem das Gerät betrieben wird, kann strafbar sein. Nach der Auswahl des Ländercodes werden die entsprechenden Kanäle automatisch zugewiesen und die Leistungsstufe eingestellt.

5.1.3 System

Parameter	Beschreibung
Infos	Informationen zum Gerät
Status	Gerätestatus (Freies RAM, Betriebszeit, CPU-Last)
Zeitschaltuhren	Geräte-Timer (System ein, Hintergrundbeleuchtung ein)
PlugIn	Informationen zu Hardware-Plugins

5.1.4 Logbuch

Aktivieren Sie die Option "Permanente Logdateien", wenn Sie möchten, dass die Logdateien auch nach einem Neustart gespeichert bleiben. Verwenden Sie die Schaltfläche „Speichern“, um eine Kopie der Logdateien zu exportieren.

Der Logdateimanager füllt zyklisch 3 Dateien von jeweils 4Mb.

5.1.5 Datum und Uhrzeit

Datum und Uhrzeit des Geräts.

Parameter	Beschreibung
Aktuelle Zeitzone	Zeitzone Region
Aktuelles Datum Ortszeit	Datum und Uhrzeit können nur dann manuell eingestellt werden, wenn die automatische Aktualisierung deaktiviert ist.
Automatische Aktualisierung (NTP)	Aktivieren Sie die Synchronisierung von Datum und Uhrzeit von einem entfernten Server **NTP-Server** Geben Sie die Adresse des Internet-NTP-Servers an Der NTP-Client des HMI-Geräts ist eine vollständige Implementierung des Network Time Protocol (NTP) Version 4, behält aber auch die Kompatibilität mit Version 3, wie in RFC-1305 definiert, und Version 1 und 2, wie in RFC-1059 bzw. RFC-1119 definiert, bei. Der Poll-Prozess sendet NTP-Pakete in Intervallen, die durch den Clock Discipline Algorithmus bestimmt werden. Der Prozess ist so konzipiert, dass er eine ausreichende Aktualisierungsrate bietet, um die Genauigkeit zu maximieren und gleichzeitig den Netzwerk-Overhead zu minimieren. Der Prozess ist so konzipiert, dass er in einem veränderlichen Modus zwischen 8 Sekunden und 36 Stunden arbeitet.
NTP-Anfragen akzeptieren	Wenn diese Funktion aktiviert ist, akzeptiert das Gerät NTP-Anfragen von außen. Wenn die automatische Aktualisierung nicht aktiviert ist, verwendet das Gerät die lokale RTC-Uhrzeit.

5.1.6 Netzwerke

Netzwerk-Parameter. Verfügbare Parameter im Bearbeitungsmodus:

Parameter	Beschreibung
Allgemeine Einstellungen	Hostname des Geräts Avahi Hostname (siehe "Avahi Daemon" auf Seite 24)
Netzwerk-Schnittstelle	Netzwerkparameter der verfügbaren Schnittstellen

	DHCP IP-Adresse Netzmaske Gateway Standardmäßig ist die Netzwerkschnittstelle so eingestellt, dass DHCP aktiviert ist und die Netzwerkparameter vom DHCP-Server abgerufen werden. Wenn der DHCP-Server nicht gefunden wird, wird der avahi-autoip-Dienst verwendet, um eine IP-Adresse im Bereich 169.256.x.x festzulegen.
DNS	DNS-Server Wird in der Regel von den DHCP-Servern bereitgestellt, kann aber im Bearbeitungsmodus geändert werden. Domains suchen Optionale Domains, die in Verkettung mit den angegebenen URLs verwendet werden

5.1.7 Sicherheit

Die Dienste sind nur verfügbar, wenn Sie als Administrator angemeldet sind.

Der Sicherheitsbereich enthält Passwörter und Zertifikate, die von Anwendungen benötigt werden.

Parameter	Beschreibung
Bereich	Identifiziert eine Reihe von geheimen Informationen, die von installierten Anwendungen verwendet werden können, die über die entsprechenden Rechte verfügen. Die vorkonfigurierten Domänen sind: **Allgemein** Dieser Bereich ist für Anwendungen von Dritten verfügbar. **System** Dieser Platz wird von den im Gerät eingebetteten Diensten (z. B. dem VNC-Server) genutzt. **HMI Runtime** Dieser Bereich wird von der HMI Runtime-Anwendung verwendet.
Secret ID	Name, der zur Identifizierung der einzelnen geheimen Informationen in der ausgewählten Domäne verwendet wird.
Typ	Art der zu speichernden Informationen. • Text • Passwort • Zertifikat • Datei
Secret Info	Secret Infos, die gespeichert werden müssen. Im Falle von Text oder Kennwort geben Sie den Text oder das Kennwort zum Speichern ein. Im Falle eines Zertifikats oder einer Datei verwenden Sie die Schaltfläche "Aktualisieren", um die Datei zu speichern.
Beschreibung	Ein freier Text, den Sie nach Belieben einfügen können.

Import/Export

Mit den Befehlen Import/Export ist es möglich, die gespeicherten Informationen zu exportieren und z.B. in andere Geräte zu importieren. Beachten Sie, dass der Export-Befehl Sie auffordert, ein Passwort festzulegen, das dann für den Import der exportierten Datei erforderlich ist.

5.1.8 Anwendungen

Auf der Seite Anwendungen werden die auf den HMI-Geräten geladenen Anwendungen aufgelistet. Von dieser Seite aus können Sie die Anwendungen verwalten.

Parameter	Beschreibung
Name	Name der Anwendung
Autostart	Wenn diese Option ausgewählt ist, wird die Anwendung beim Einschalten des Bedienfelds gestartet.

App-Verwaltung

Drücken Sie die Taste "*App Manager*", um in den Modus zur Verwaltung von Anwendungen zu gelangen:

- neue Applikationen hochladen
- bestehende Applikationen aktualisieren
- Applikation entfernen
- Startreihenfolge festlegen.

5.1.9 Services

ACHTUNG! Die Services sind nur verfügbar, wenn Sie als Administrator angemeldet sind.

Klicken Sie mit der Maus auf die Schaltfläche "Aktivieren", um den jeweiligen Dienst zu aktivieren/deaktivieren. Klicken Sie auf den Namen des Dienstes, um die zugehörigen Parameter aufzulisten.

5.1.9.1 Autorun-Skripte von externem Speicher

Aktivieren/Deaktivieren Sie die Möglichkeit, die Skriptdatei "autoexec.sh" auszuführen, wenn ein USB-Stick an das Gerät angeschlossen wird. Deaktivieren Sie diesen Dienst, wenn Sie einen unbefugten Zugriff über die USB-Schnittstelle verhindern möchten.

ACHTUNG! Erforderliches BSP v1.0.212 oder höher

5.1.9.2 Avahi-Daemon

Avahi ist ein System, das es Programmen ermöglicht, Dienste und Hosts, die in einem lokalen Netzwerk laufen, zu finden und zu veröffentlichen. Wenn es aktiviert ist, kann das HMI-Gerät auch über den Host-Namen des Geräts erreicht werden (anstelle der IP-Adresse).

Abb. 19: Avahi - Allgemeine Einstellungen

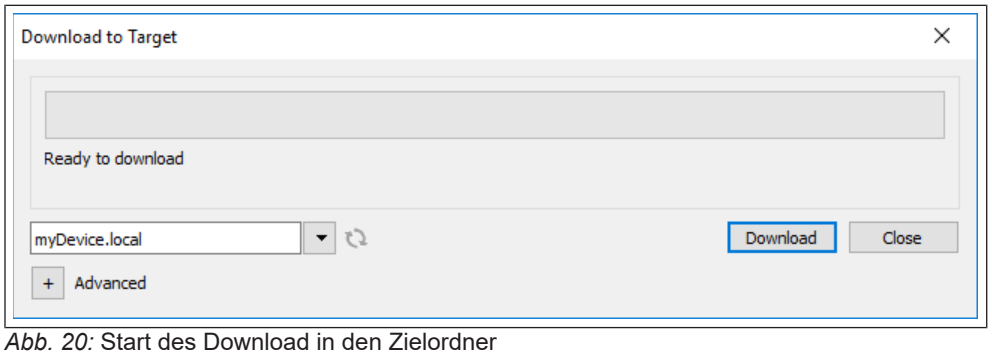

Abb. 20: Start des Download in den Zielordner

Avahi Daemon läuft auf UDP-Port 5353

Auf Linux wird der Avahi-Dienst kostenlos mit dem Betriebssystem geliefert. Auf Windows-PCs hingegen müssen Sie einen Avahi-Dienst installieren, um das Panel über seinen Avahi-Hostnamen erreichen zu können.

5.1.9.3 Bridge/Switch-Dienst

Mit dem Bridge-Dienst ist es möglich, den WAN-Netzwerkadapter (eth0) mit den anderen Netzwerkschnittstellen zu verbinden. Bei der Verwendung werden die beiden Ethernet-Schnittstellen überbrückt und beide Ethernet-Schnittstellen teilen sich die gleiche IP-Adresse.

Der Bridge-Dienst erstellt eine Linux-basierte Layer-2-Netzwerkbrücke zwischen zwei oder mehr Netzwerkschnittstellen. Wenn sowohl WAN- als auch Endgeräte an eine solche Brücke angeschlossen sind, werden die beiden Netzwerke physisch verbunden und die Endpunkte sind so verfügbar, als wären sie direkt mit dem WAN verbunden (Hinweis: Für das Cloud-Szenario muss der Router-Dienst weiterhin aktiv sein).

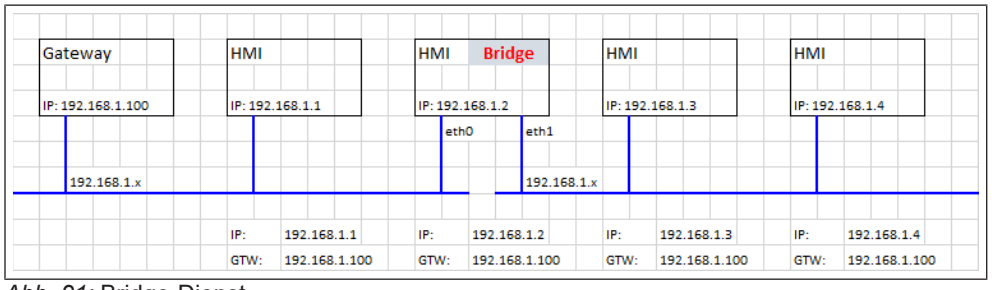

Abb. 21: Bridge-Dienst

5.1.9.4 Cloud / VPN-Dienst

Ermöglicht die Verwaltung entfernter HMI-Geräte, die über Gateways mit einem zentralen Server verbunden sind. Weitere Informationen finden Sie unter (≡► "Cloud-/VPN-Service" auf Seite 38 [▸ 34]).

5.1.9.5 DHCP-Server

Stellen Sie den DHCP-Server für die ausgewählten Schnittstellen bereit.

Parameter	Beschreibung
Enabled	Aktiviert den DHCP-Server auf der ausgewählten Schnittstelle.
Start IP Stop IP	Vom DHCP-Server verteilte IP-Adressen
Gateway	Die Adresse des Gateways
Netzmaske	Die angegebene Netzmaske
DNS-Server	Die Adresse des DNS-Servers
Lease Time (Sekunden)	Lease-Zeit, Standard ist 86400 s (1 Tag). Zulässige Werte liegen zwischen 60 s und 864000 s (10 Tage).

5.1.9.6 Wiederherstellung des Geräts über TAP TAP-Option ermöglichen

Wenn diese Funktion aktiviert ist, kann das Bedienfeld zurückgesetzt werden, wenn das Administrator-Passwort vergessen wurde (siehe: (≡► "Passwort vergessen" auf Seite 1 [▸ 43])).

ACHTUNG! Diese Option ist standardmäßig aktiviert. Sie können sie deaktivieren, um die Sicherheit des Geräts zu erhöhen. Dies schließt die Möglichkeit aus, ein vergessenes Passwort wiederherzustellen.

ACHTUNG! Erforderliches BSP v1.3.491 oder höher.

5.1.9.7 Wiederherstellung des Geräts über USB

Wenn diese Funktion aktiviert ist, kann das Bedienfeld zurückgesetzt werden, wenn das Administrator-Passwort vergessen wurde (siehe: (≡► "Passwort vergessen" auf Seite 1 [▸ 43])).

ACHTUNG! Diese Option ist standardmäßig aktiviert. Sie können sie deaktivieren, um die Sicherheit des Geräts zu erhöhen. Dies schließt die Möglichkeit aus, ein vergessenes Passwort wiederherzustellen.

ACHTUNG! Erforderliches BSP v1.3.564 oder höher

5.1.9.8 Schnellstart

Wenn Schnellstart aktiviert ist, startet das HMI-Gerät beim Einschalten die HMI-Anwendung so schnell wie möglich. In diesem Modus werden keine Diagnoseinformationen angezeigt (z. B. der Ladebalken), sondern es werden nur die minimal erforderlichen Funktionen geladen, bevor die Benutzeroberfläche geladen wird (z. B. werden Systemeinstellungen, VNC, SSH usw. erst nach dem Laden der HMI-Anwendung geladen).

Um eine optimale Leistung zu erzielen, wird empfohlen, zusätzlich zum Schnellstartmodus folgende Einstellungen vorzunehmen:

Alle nicht benötigten Dienste deaktivieren.

Vermeiden, dass das persistente Protokoll aktiviert bleibt.

Verwendung einer statischen IP-Adresse anstelle des DHCP-Dienstes.

ACHTUNG! Erforderliches BSP v1.0.242 oder höher

5.1.9.9 Firewall-Dienst

Wenn die Firewall aktiviert ist, werden nur Verbindungen zugelassen, die den definierten Regeln entsprechen. Beachten Sie, dass einige Regeln aktiviert sein müssen, damit das HMI richtig funktioniert.

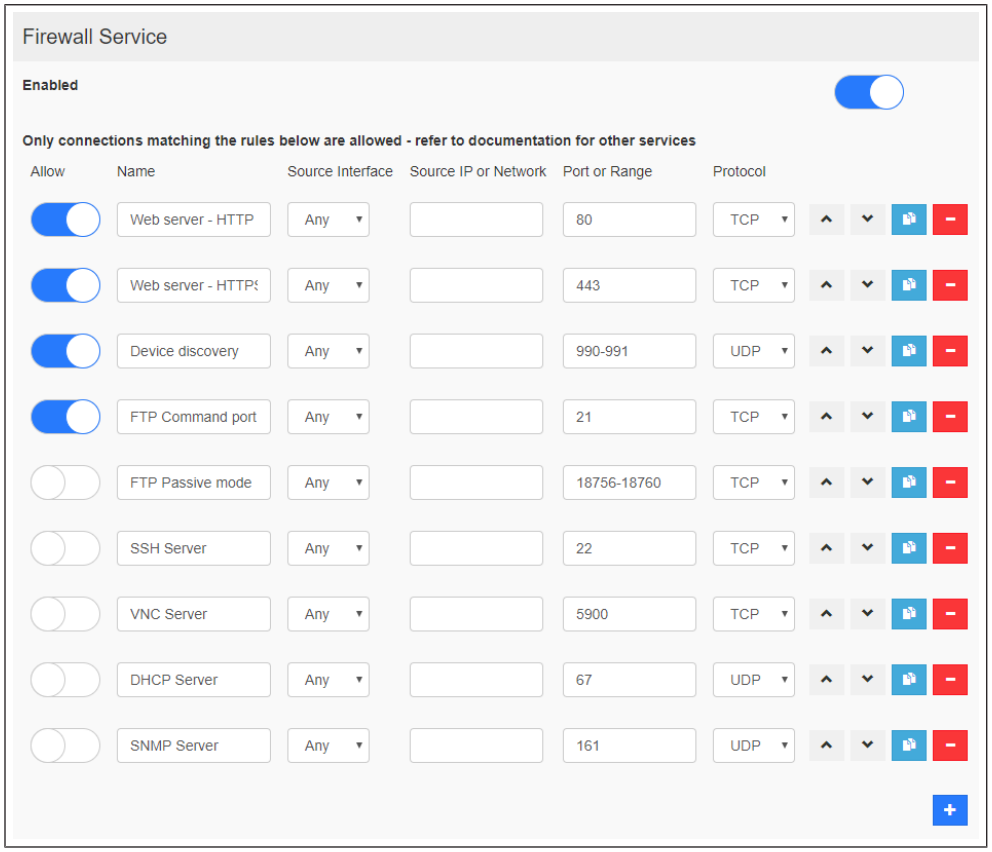

Abb. 22: Firewalleinstellungen

Anmerkungen:

- Die Firewall basiert auf IP-Tabellen, die nur auf Schicht 3 funktionieren (Schicht-2-Pakete werden nicht gefiltert, z. B. ARP).
- Nur INPUT und FORWARD Pakete werden gefiltert, nicht OUTPUT.
- PING/ICMP-Echo-Antwortpakete sind immer erlaubt.
- Internet-Sharing-Szenarien (z. B. 3g- oder WiFi-Verbindung zu Endpunkten) werden nicht unterstützt.
- Von der Firewall gefilterte Pakete werden verworfen.

Quell-IP oder Netzwerk

Wenn dieses Feld nicht angegeben wird, ist der Zugriff von jedem beliebigen Quellhost aus möglich. Andernfalls kann der Zugang auf eine einzelne IP-Adresse (z. B. 192.168.100.123) oder einen Bereich von IP-Adressen im CIDR-Format (z. B. 192.168.100.0/24) beschränkt werden.

ACHTUNG! Wenn Sie die Firewall aktivieren und den FTP-Passivmodus mit der HMI Runtime älter als Version 2.10.0.280 verwenden möchten, müssen Sie die Ports 1024-2048/tcp und 16384-17407/tcp öffnen. Ab Version 2.10.0.280 verwendet HMI Runtime stattdessen die Ports 18756-18760/tcp, die in den Firewall-Einstellungen standardmäßig vorgeschlagen werden.

ACHTUNG! Firewall ist ab BSP v1.0.532 verfügbar. Wenn Sie von einer alten BSP-Version aktualisieren und die Standardregeln nicht angezeigt werden, müssen Sie die Systemeinstellungen zurücksetzen (siehe (🌐► "Systemkomponenten aktualisieren" auf Seite 1)ACHTUNG!).

5.1.9.9.1

5.1.9.9.1.1 Router-Dienst

Dieser Dienst verwendet IP-Weiterleitung und Network Address Translation, um die Verbindung vom WAN (eth0) zum LAN (eth1 oder eth2) gemeinsam zu nutzen: Angeschlossene Endpunkte können dieselben Netzwerke erreichen, die vom Gateway erreichbar sind (einschließlich Internet, falls verfügbar). Bei aktivem Cloud Service können die Endpunkte über den LAN-Port des Gateways erreicht werden (weitere Informationen finden Sie unter (≡► "Cloud / [▸ 34])(≡► VPN Service" auf Seite 38 [▸ 34]))

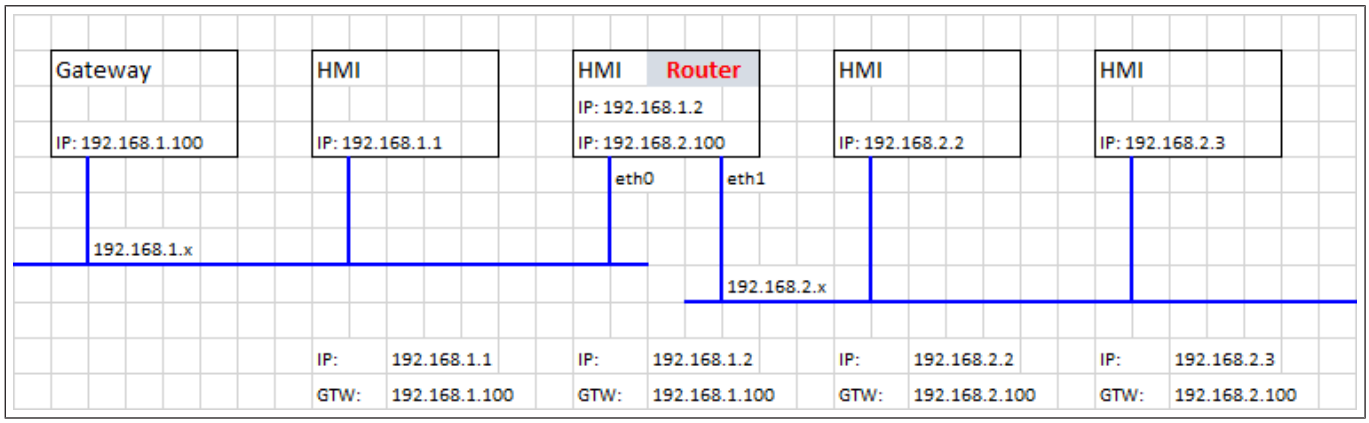

Abb. 23:

5.1.9.10 Router / NAT / Portweiterleitung

Die Portweiterleitung leitet eingehende TCP-Paketanfragen von der WLAN-Schnittstelle von einer Adress- und Portnummernkombination auf eine andere Adress- und Portnummernkombination um.

5.1.9.10.1 Regeln für die Portweiterleitung

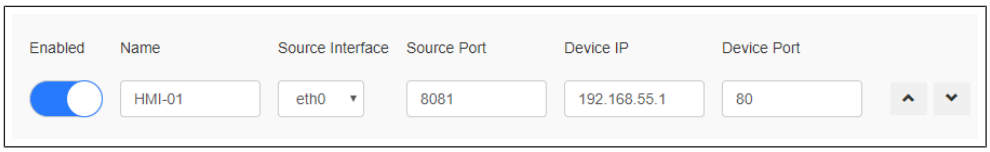

Abb. 24: Portweiterleitung

ACHTUNG! Verfügbar ab BSP v1.0.507

5.1.9.10.2 1:1 NAT-Regeln

1:1 NAT, Erstellung einer Alias-IP im WLAN und Weiterleitung aller Pakete (oder eines bestimmten Portbereichs) mit dieser Ziel-IP an ein anderes Gerät, das an ein LAN angeschlossen ist.

ACHTUNG! Verfügbar ab BSP v1.0.507

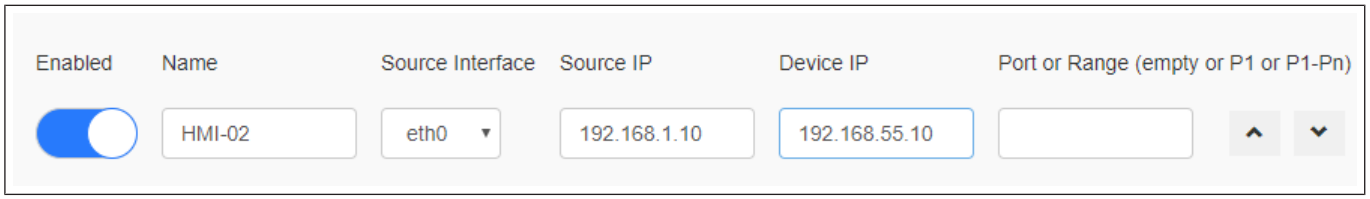

Abb. 25: 1:1 NAT-Regeln

VORSICHT! Stellen Sie sicher, dass der für "Source IP" eingegebene Wert nicht mit der realen IP-Adresse übereinstimmt, die dem als "Source Interface" angegebenen physischen Ethernet-Anschluss zugewiesen ist.

5.1.9.10.3 DNS-Relay-Proxy

Der DNS-Relay-Proxy leitet DNS-Anfragen und Antwortpakete zwischen DNS-Client und DNS-Server weiter.

Wenn diese Funktion aktiviert ist, leitet das HMI-Gerät DNS-Anfragen von anderen Geräten (DNS-Clients) an den DNS-Server weiter (konfiguriert im Netzwerkabschnitt) und sendet die Wiedergabe an den DNS-Client zurück, der die Anfrage gestellt hat.

ACHTUNG! Verfügbar ab BSP v1.3.567

5.1.9.11 Ladebalken beim Booten anzeigen

Aktivieren/Deaktivieren der Anzeige des Ladebalkens während der Boot-Phase.

5.1.9.12 SNMP-Server

SNMP ist ein Netzwerkprotokoll, das die Verwaltung von Netzwerkinfrastrukturen ermöglicht. Es wird üblicherweise zur Überwachung von Netzwerkgeräten wie Switches, Routern usw. verwendet, die an ein LAN-Netzwerk angeschlossen sind.

Wenn der SNMP-Dienst aktiviert ist, kann ein SNMP-Manager über das SNMP-Protokoll Informationen vom HMI-Gerät abrufen. Derzeit sind keine proprietären MIBs verfügbar. Nur die öffentlichen Standard-Community-MIBs sind im Nur-Lese-Modus verfügbar.

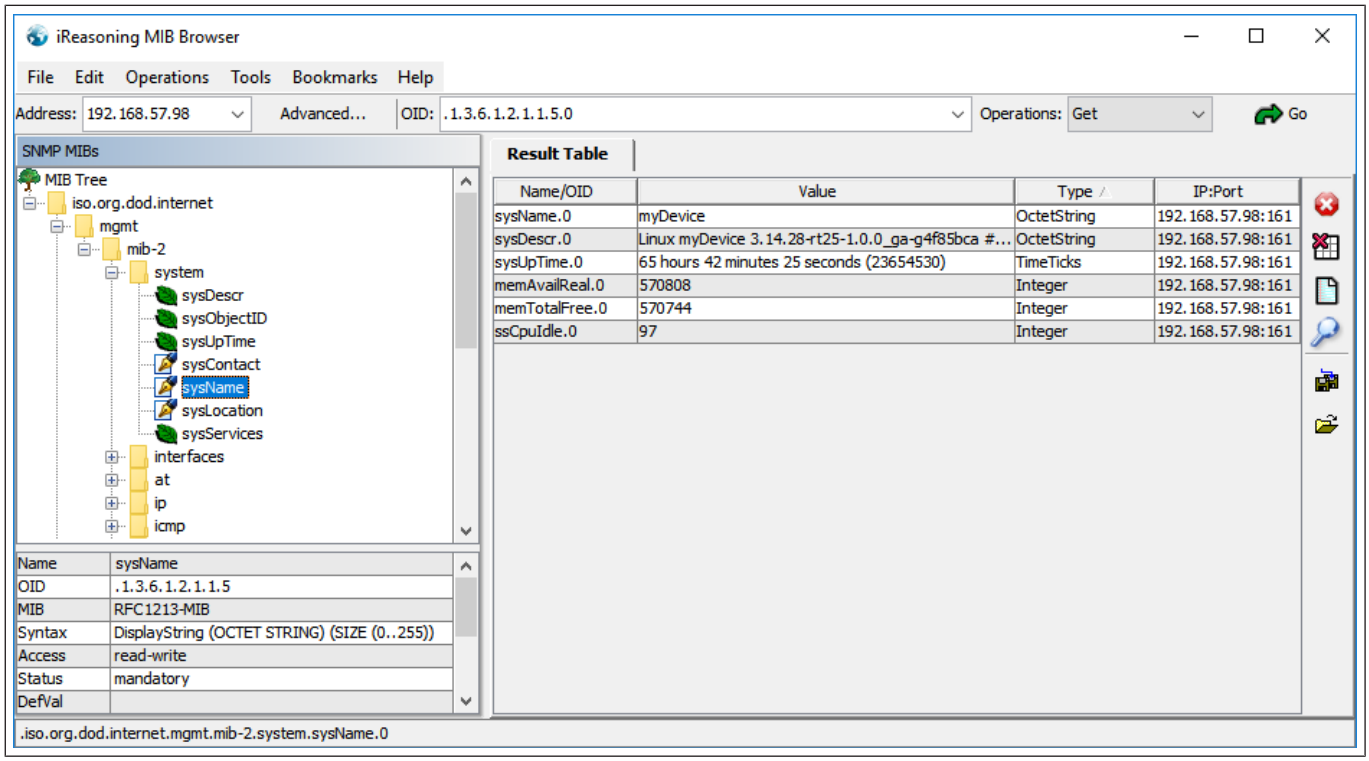

Abb. 26: MIB Browser

Beispiel

System Name	.1.3.6.1.2.1.1.5.0
Systembeschreibung	.1.3.6.1.2.1.1.1.0
System UpTime	.1.3.6.1.2.1.1.3.0
Benutztes RAM insgesamt	.1.3.6.1.4.1.2021.4.6.0
Gesamtes freies RAM	.1.3.6.1.4.1.2021.4.11.0
Idle-CPU-Zeit (%)	.1.3.6.1.4.1.2021.11.11.0

SNMP-Server läuft auf UDP-Port 161

ACHTUNG! Aus Sicherheitsgründen sollten Sie den Dienst nicht aktivieren, wenn Sie ihn nicht benötigen.

5.1.9.13 SSH-Server

Der SSH-Dienst wurde nur für fortgeschrittene Benutzer entwickelt. Er ermöglicht die Fernanmeldung am HMI-Gerät über das Secure Shell-Protokoll. Auf dem PC können Sie einen SSH-Client wie z. B. PuTTY ausführen, eine Open-Source-Software, die unter der MIT-Lizenz vertrieben wird.

Das Standardpasswort für den Benutzernamen admin lautet "admin". Weitere Informationen finden Sie im Kapitel (≡► "Authentifizierung" auf Seite 36 [▸ 33]).

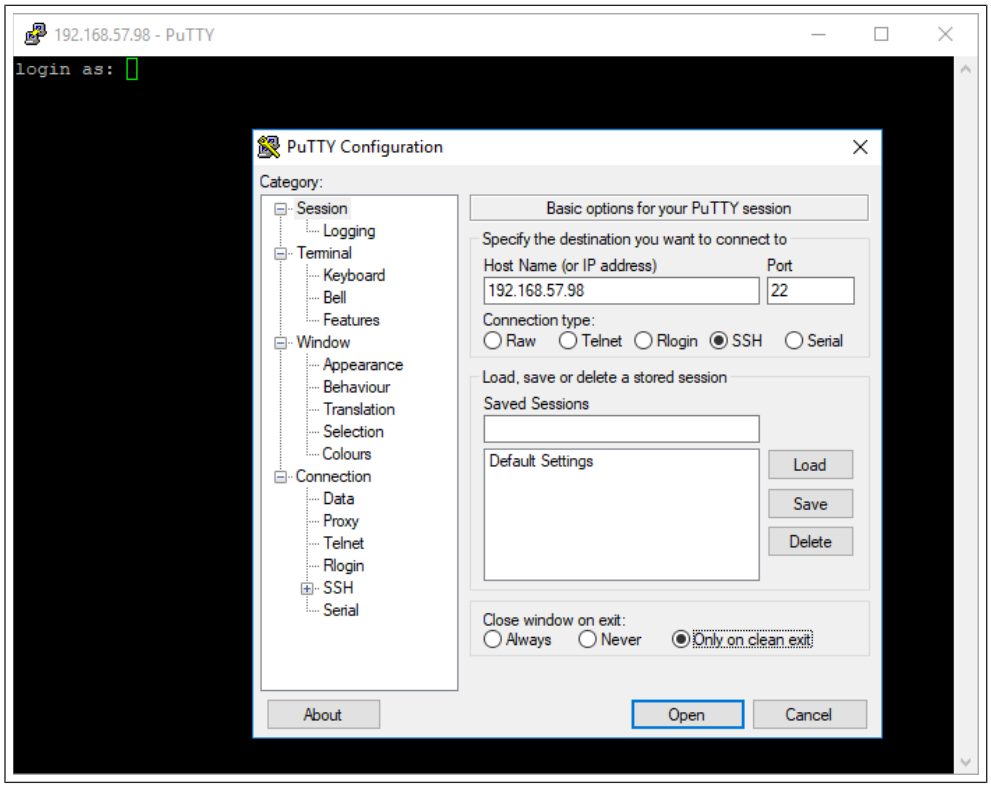

Abb. 27: PuTTY Konfiguration

SSH-Server läuft auf TCP-Port 22.

VORSICHT! Dieser Dienst ist für den Einsatz in der Entwicklungsphase vorgesehen. Denken Sie aus Sicherheitsgründen daran, den Dienst vor der Umstellung auf die Produktion zu deaktivieren.

5.1.9.14 VNC-Dienst

VNC ist ein Dienst, der den Fernzugriff auf die Anzeige des HMI-Geräts ermöglicht. VNC-Clients können für die Fernsteuerung des HMI-Geräts verwendet werden.

VORSICHT! VNC sollte nach der Verwendung deaktiviert werden, und ein automatischer Start wird nicht empfohlen.

Parameter	Beschreibung
Enable	Aktiviert den VNC-Server.
Autostart	Hält den VNC-Server beim Start des HMI-Geräts aktiviert.
Port	VNC-Server wartet auf Verbindungen am TCP-Port 5900 (Standard).
Inactivity timeout (Sekunden)	Eine Zeitüberschreitung bei Inaktivität tritt ein, wenn keine Benutzerinteraktion (über Tastatur, Maus, Übertragungen oder andere RFB-Protokollinteraktionen) festgestellt wird. Der spezielle Wert 0 zeigt an, dass die Inaktivitätszeitüberschreitung deaktiviert ist. Der Standardwert ist 600 (10 Minuten).
Multiple clients	Mehrere Sitzungen auf demselben Port zulassen (wenn deaktiviert, werden bereits angemeldete Clients bei einer neuen eingehenden Verbindung getrennt).
View only	Keine aktiven Benutzerinteraktionen zulassen (Kunden können nur zuschauen).
Encryption	Aktiviert die SSL-Verschlüsselung von Verbindungen.

	Benutzerdefiniertes Zertifikat (Sicherheit/VNC KeyPair) Das Zertifikat des HMI-Geräts, das erforderlich ist, damit der entfernte VNC-Client die Authentizität des HMI-Geräts überprüfen kann. Das Zertifikat muss sowohl den privaten als auch den öffentlichen Schlüssel enthalten und kann im .pem-Format vorliegen. **Die Verschlüsselungsfunktionen werden nicht allgemein unterstützt, überprüfen Sie die Kompatibilität Ihres VNC-Clients**
Authentification	Ob Benutzer bei der Sitzungserstellung authentifiziert werden. Es kann ein benutzerdefiniertes VNC-spezifisches Kennwort festgelegt werden oder es können Systemkennwörter verwendet werden (diese Option ist nur verfügbar, wenn auch die Verschlüsselung aktiviert ist)

Beispiel für die Erstellung eines Zertifikats mit der OpenSSL-Bibliothek:

```
@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 Zertifikatsschlüssel
%OpenSSL% req -x509 -newkey rsa -days 365 -nodes -keyout pri-
vate.pem -out public.pem -subj "/ST=NY/C=US/L=New York/O=Fir-
menname/OU=Abteilung/CN=%CertificateName%" -addext "subjec-
tAltName=IP:%DeviceIP%"
rem .pem-Datei erstellen
copy private.pem + public.pem hmi- certificate.pem
echo.
echo.
pause
```

5.1.9.15 Web-Server

Auf dieser Seite werden die für die Konfiguration des Webservers verfügbaren Parameter angezeigt. Beachten Sie, dass es nicht möglich ist, den Webserver zu deaktivieren, da er für den Zugriff auf die Systemeinstellungen des Geräts erforderlich ist.

- **Nur sichere HTTPS-Verbindungen zulassen**
  Standardmäßig deaktiviert, um die Abwärtskompatibilität aufrechtzuerhalten, aber es wird empfohlen, sie zu aktivieren, um die Sicherheit des HMI-Geräts zu verbessern.
- **CORS-Domänen aktiviert**
  Wenn diese Option deaktiviert ist (Standard), ist der Zugriff auf externe Domänen nicht zulässig. Wenn aktiviert, ist der Zugriff auf externe Domänen, die im "CORS-Domänenfilter" aufgeführt sind, erlaubt.
- **CORS-Domänen-Filter**
  Sie können die Domäne eingeben, auf die der Zugriff erlaubt ist, oder einen regulären Ausdruck verwenden, um mehrere Domänen zu definieren. Der reguläre Ausdruck muss das Präfix "re:" enthalten.

  Lassen Sie den Filter leer (Standard), wenn Sie die Kompatibilität mit älteren Versionen beibehalten und den Zugriff auf alle Domänen erlauben wollen (dies wird nicht empfohlen).

  Beispiele für "CORS-Domänenfilter":

– (🌐► 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

Auf dieser Seite werden die Parameter angezeigt, die für die Konfiguration der an das HMI-Gerät angeschlossenen optionalen Plug-in-Module verfügbar sind. Weitere Informationen finden Sie in der Beschreibung der einzelnen Plug-in-Module.

5.1.10 Verwaltung

ACHTUNG! Die Verwaltung ist nur verfügbar, wenn Sie als Administrator angemeldet sind.

Vom Verwaltungsbereich aus ist es möglich, (🌐► "Systemkomponenten aktualisieren") des HMI-Geräts.

VORSICHT! Die Arbeit im Managementbereich ist ein kritischer Vorgang, der bei unsachgemäßer Ausführung zu Schäden am Produkt führen kann, die eine Wartung des Geräts erforderlich machen. Wenden Sie sich für Hilfe an den technischen Support.

Verwenden Sie den Befehl "Clear" im Abschnitt "Data", um HMI Runtime vom Gerät zu entfernen.

5.1.11 Anzeige

Parameter	Beschreibung
Brightness	Helligkeitsstufe des Displays
Back light timeout	Zeitüberschreitung bei Inaktivität der Hintergrundbeleuchtung
Orientation	Ausrichtung der Anzeige

5.1.12 Schriftarten

Listet die verfügbaren Systemschriften auf und gibt Ihnen die Möglichkeit, eigene Schriften hochzuladen.

ACHTUNG! Beachten Sie, dass für die Verwendung von Schriftdateien eine Lizenz erforderlich sein kann.

5.1.13 Authentifizierung

Gehen Sie in den Bearbeitungsmodus, um die Authentifizierungspasswörter zu ändern oder das x.509-Zertifikat des HMI-Geräts zu personalisieren.

5.1.13.1 Benutzer

Es gibt zwei Benutzernamen:

- Administrator-Benutzername mit vollen Zugriffsrechten ist "**admin**".
- Allgemeiner Benutzername mit grundlegenden Zugriffsrechten ist "**user**".

5.1.13.2 x.509-Zertifikat

Das HMI-Gerät verwendet ein Selbstzertifikat, um die Internetkommunikation über das HTTPS-Protokoll zu verschlüsseln. Sie können das Zertifikat mit den Daten Ihres Unternehmens personalisieren und eine Zertifizierungsstelle bitten, es zu bestätigen.

Das Verfahren zur Personalisierung und Bestätigung Ihres Zertifikats ist wie folgt:

1. Gehen Sie in den Bearbeitungsmodus und geben Sie die erforderlichen Parameter ein. Drücken Sie dann die Schaltfläche <GENERATE>, um ein selbstsigniertes Zertifikat mit Ihren Daten zu erstellen.
2. Exportieren Sie die "Signierte Zertifikatsanforderung".
3. Senden Sie die " Signierte Zertifikatsanforderung" an eine Zertifizierungsstelle, um sie zu bestätigen (im Allgemeinen ist dies ein kostenpflichtiger Dienst).
4. Importieren Sie das signierte Zertifikat in das HMI-Gerät.

Die Parameter des Zertifikats

Parameter	Beschreibung
Device Name	Der Name Ihres Geräts.
Organisation	Der rechtliche Name Ihrer Organisation.
Unit	Die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.
State	Bundesland/Region, in dem/der Ihre Organisation ansässig ist.
Location	Die Stadt, in der Ihre Organisation ansässig ist.
Country	Der zweistellige ISO-Code für das Land, in dem Ihre Organisation ansässig ist.
valid (Tage)	Gültigkeit der Bescheinigung.
Key Length	Anzahl der Bits des vom kryptografischen Algorithmus verwendeten Schlüssels.

Verwaltete Zertifikate sind base64-kodiert.

ACHTUNG! Erforderliches BSP v1.0.239 oder höher

5.1.14 Restart

Befehl zum Neustarten des HMI-Geräts.

5.1.15 EXIT

Mit dem Befehl EXIT werden die Systemeinstellungen verlassen.

5.2 Cloud / VPN-Dienst

Der Cloud-/VPN-Dienst ermöglicht es Geräten, sich über eine sichere Verbindung mit entfernten Servern zu verbinden.

ACHTUNG! BSP v1.0.117 oder höher ist erforderlich.

Voraussetzungen

Dieser Dienst erfordert einen externen Zugriff auf den Server für die VPN-Einrichtung (Standardport UDP/1194) und für die Selbstkonfiguration/andere erweiterte Funktionen auf TCP-Port 443 (nur im Cloud-Server-Modus). Bitte überprüfen Sie daher die Konfiguration und stellen Sie sicher, dass keine Firewalls diese Ports blockieren.

Setup

Wenn Sie Endgeräte hinter Ihrem Gateway-Gerät erreichen müssen, stellen Sie sicher, dass der Routerdienst aktiv ist, und richten Sie ihn wie folgt ein:

- WAN-Port (eth0), der mit dem Hauptnetz mit Internetzugang verbunden ist (der Cloud Server muss von diesem Netz aus erreichbar sein).
- LAN-Anschluss (eth1), der mit einem oder mehreren Endgeräten verbunden ist (neu erstelltes privates Netzwerk).

ACHTUNG! Diese Funktion wird bei der Verwendung eines Cloud-Servers automatisch unterstützt, erfordert aber eine zusätzliche manuelle Einrichtung für einen einfachen OpenVPN-Server.

Konfiguration

Konfigurationsoptionen sind im Menü „System settings“ verfügbar (siehe "Systemeinstellungen" auf Seite 12).

ACHTUNG! Im Falle eines Verbindungsfehlers hat die Wiederholungszeit ab BSP v1.0.348 eine geometrische Progression: beginnend mit 5s, erfolgt die nächste Wiederholung nach 2*(vorherige Zeit). Das bedeutet 5s, 10s, 20s, 40s, usw. bis zu einer maximalen Wiederholungszeit von 5 Minuten. In früheren BSP-Versionen war die Wiederholungszeit auf 5 Sekunden festgelegt.

Parameter	Beschreibung
Enable	Aktiviert den Cloud / VPN-Dienst.
Autostart	Wenn diese Option ausgewählt ist, wird die Anwendung beim Einschalten des HMI-Gerätes gestartet.
Server type	Wählen Sie aus den verfügbaren unterstützten Servertypen den zu verwendenden Servertyp aus.
Server	Wählen Sie den zu verwendenden Corvina Cloud Server aus (nur verfügbar, wenn der ausgewählte Servertyp "Cloud Server" ist).
Files	Ermöglicht das Hochladen von VPN-Konfigurationsdateien (nur verfügbar, wenn der ausgewählte Servertyp "OpenVPN" ist).
Authentication	Wählen Sie aus den verfügbaren Authentifizierungsmodi: • Benutzername/Passwort • Aktivierungscode (nur verfügbar, wenn der ausgewählte Servertyp "Cloud Server" ist) • Zertifikat (nur verfügbar, wenn der ausgewählte Servertyp "OpenVPN" ist) • Zertifikat + Benutzername/Passwort (nur verfügbar, wenn der ausgewählte Servertyp "OpenVPN" ist) • Keine (nur verfügbar, wenn der ausgewählte Servertyp "OpenVPN" ist)
Username	Benutzernamen für das Konto des Remoteservers.
Password	Passwort für das Konto des Remoteservers.
Show Password	Zeigt die eingegebenen Zeichen des Passworts an.

5.2.1 Cloud-Server

Cloud Server ist eine VPN-basierte Lösung, die eine nahtlose Verbindung von Benutzern mit Gateways und Endgeräten ermöglicht. Sie bietet eine vollständige Verwaltungsinfrastruktur, um diesen Prozess mühelos zu gestalten.

Die Konfiguration wird automatisch vom Cloud Server heruntergeladen, so dass die einzigen erforderlichen Parameter Server (Hostname oder IP-Adresse), Benutzername und Passwort sind.

5.2.2 OpenVPN

In diesem Modus wird eine standardmäßige OpenVPN-Konfiguration für die Verbindung von Geräten verwendet.

Fall A: Bereitstellung von Konfigurationsdateien

In Remoteumgebungen, die auf einem OpenVPN-Server basieren, stellen Systemadministratoren den Endbenutzern normalerweise eine Reihe von OpenVPN-Konfigurationsdateien direkt zur Verfügung.

In diesem Fall ist die Konfiguration recht einfach, da sie nur zwei einfache Schritte erfordert:

1. Durchsuchen und Hochladen von N Dateien (dies sollte mindestens eine OpenVPN-Hauptkonfigurationsdatei umfassen, kann aber auch Server- und/oder Client-Zertifikate in den Formaten .pem, .p12 oder anderen Formaten enthalten). Stellen Sie sicher, dass Sie alle erforderlichen Dateien auf einmal auswählen, indem Sie die plattformabhängige Mehrfachauswahl verwenden.
2. Wählen Sie einen geeigneten Authentifizierungstyp aus und fügen Sie ggf. Anmeldedaten ein.

Jetzt auf Speichern drücken. Nach einem Moment sollte ein aktualisierter Verbindungsstatus zu sehen sein.

Fall B: Keine Konfigurationsdateien vorhanden

Wenn Ihr Systemadministrator keine Konfigurationsdateien zur Verfügung gestellt hat, müssen Sie die OpenVPN-Konfigurationsdatei selbst erstellen.

Beispiel 1: Benutzername/Passwort

Dieses Beispiel verwendet:

- Benutzernamen/Passwort-basierte Authentifizierung
- LZO-Komprimierung und TAP-Gerät
- Server läuft auf UDP-Port 1194

openvpn.conf

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

Diese Konfigurationsdatei verweist nur auf eine einzige externe Datei (*cacert.pem*), also:

- Laden Sie die 2 Dateien über die Option „Durchsuchen“ hoch
- Fügen Sie Ihren zugewiesenen Benutzernamen und Ihr Kennwort ein - beachten Sie, dass die Option auth-user-pass auch ein Dateiargument annehmen kann, so dass Sie sogar einen durch neue Zeilen getrennten Benutzernamen und ein Kennwort in eine neue Datei einfügen und ihren Namen hier angeben können (nicht empfohlen); in diesem Fall würden Sie beim Durchsuchen von Dateien auch Ihre externe Datei auswählen und die Authentifizierungsmethode None (from file) wählen.
- Speichern und auf den Statuswechsel warten

Beispiel 2: Einfaches Zertifikat

Dieses Beispiel verwendet:

- Einfache X509-Zertifikat-basierte Authentifizierung
- LZO-Komprimierung, TUN-Gerät, benutzerdefinierte MTU und AES-128-CBC-Verschlüsselung
- Server läuft auf 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
```

Diese Konfiguration bezieht sich auf 3 Dateien (*cacert.pem*, *client.pem*, *client.key*), also:

- Hochladen der Hauptdatei *openvpn.conf* und externer Dateien (insgesamt 4) mit der Option „Durchsuchen“.
- Da keine Kennwörter erforderlich sind, *None auswählen (aus Datei)* Authentifizierung
- *Speichern* und auf den Statuswechsel warten.

Beispiel 3: Passwortgeschütztes PKCS #12-Zertifikat

Dieses Beispiel verwendet:

- Zertifikatsbasierte Authentifizierung (passwortgeschützter PKCS #12)
- Andere Parameter als bei Beispiel 2

openvpn.conf

```
[..]
pkcs12 mycert.p12
```

Das PKCS #12-Bündel enthält normalerweise beide CA-Zertifikat-Client-Keypair, sodass diese Konfigurationsdatei nur auf eine externe Datei (*mycert.p12*) verweist. Daraus folgt:

- Beide Dateien über die Option „Durchsuchen“ hochladen.
- Zertifikat-Authentifizierung auswählen.
- Passwort einfügen, mit dem das PKCS #12-Bündel, das Ihr Zertifikat enthält, entschlüsselt werden soll.
- *Speichern* und auf den Statuswechsel warten.
-

Beispiel 4: 2-Faktor-Authentifizierung über passwortgeschütztes PKCS #12-Zertifikat + Benutzername/Passwort

Dieses Beispiel verwendet:

- Zertifikatsbasierte Authentifizierung (passwortgeschützter PKCS #12) und Benutzername/Passwort
- andere Parameter wie bei Beispiel 2

openvpn.conf

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

- Beide Dateien über die Option „Durchsuchen“ hochladen.
- *Zertifikat* + Benutzername/Passwort-Authentifizierung auswählen
- *Benutzername* und *Passwort* für PSK-Authentifizierung einfügen
- *PKCS #12 Passwort* einfügen
- *Speichern* und auf den Statuswechsel warten

Links

Weitere Einzelheiten entnehmen Sie bitte der (🌐► OpenVPN-Dokumentation).

5.3 Systemkomponenten aktualisieren

VORSICHT! Die Arbeit im Managementbereich ist ein kritischer Vorgang und kann bei unsachgemäßer Ausführung zu Schäden am Produkt führen, die eine Wartung des Produkts erforderlich machen. Wenden Sie sich an den technischen Support um Unterstützung zu erhalten (die neuesten BSP-Dateien werden vom technischen Support bereitgestellt).

Die Systemkomponenten des Linux-Geräts können lokal über einen USB-Speicherstick oder per Remote über einen Webbrowser aktualisiert werden.

Um die Systemkomponenten zu aktualisieren:

- Systemeinstellungen im Modus "Config OS" über das Tippen auf der HMI aufrufen.
- Oder Webbrowser unter https://<HMI-IP-Adresse>/machine_config öffnen und Abschnitt "Management" auswählen.

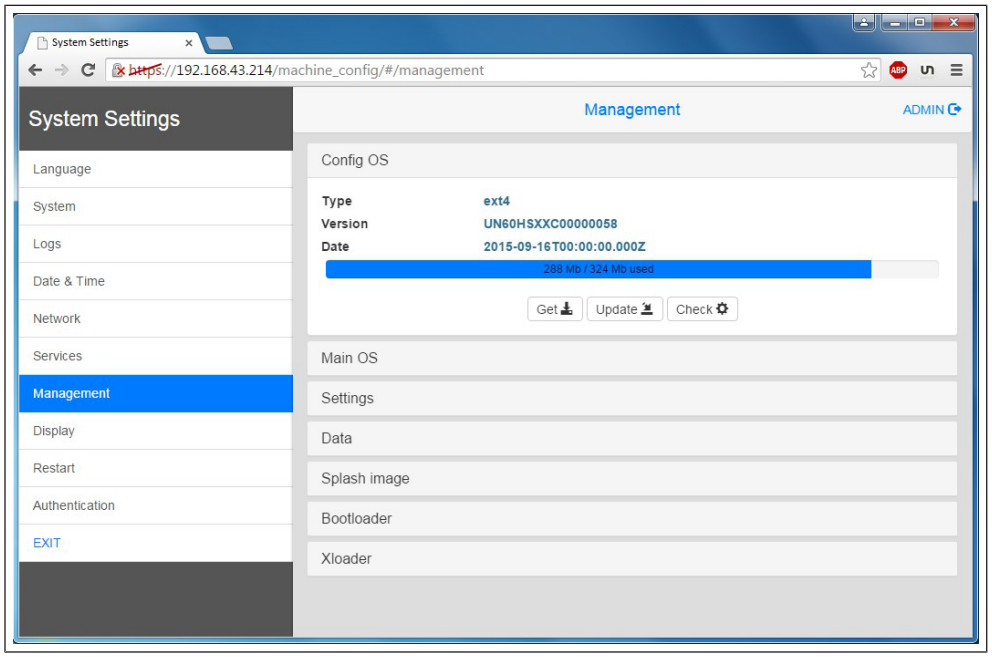

Abb. 28: Managementbereich

Zu aktualisierende Komponente aufklappen und [Aktualisieren] wählen.

Klicken Sie im geöffneten Dialogfeld auf [Browse Image] und wählen Sie die Datei "xxx-mainos-xxx.tar.gz" aus. Klicken Sie dann auf [MD5 durchsuchen] und wählen Sie die Datei "xxx-mainos-xxx.tar.gz.md5".

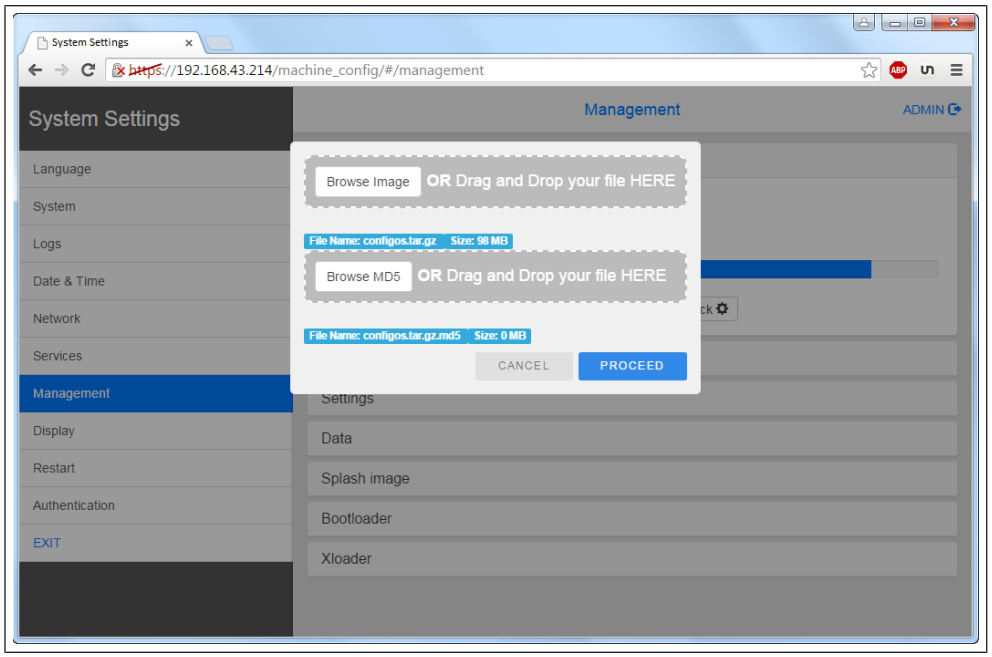

Abb. 29: Image auswählen und starten

VORSICHT! Schalten Sie das Gerät nicht aus, während dem Upgrade einer Systemkomponente läuft.

Nach Abschluss der Komponentenaktualisierung das HMI neu starten und normal booten.

5.3.1 Aufrufen der Systemeinstellungen im Modus Config OS durch Antippen

Die Systemeinstellung im Modus Config OS ist über eine Tap-Tap-Sequenz verfügbar. Auf diesen Modus kann auch zugegriffen werden, wenn die HMI einen Softwarefehler aufweist.

Unmittelbar nach dem Einschalten der HMI wird durch wiederholtes Antippen des Touchscreens mit dem Finger die Tap-Tap-Funktion aufgerufen.

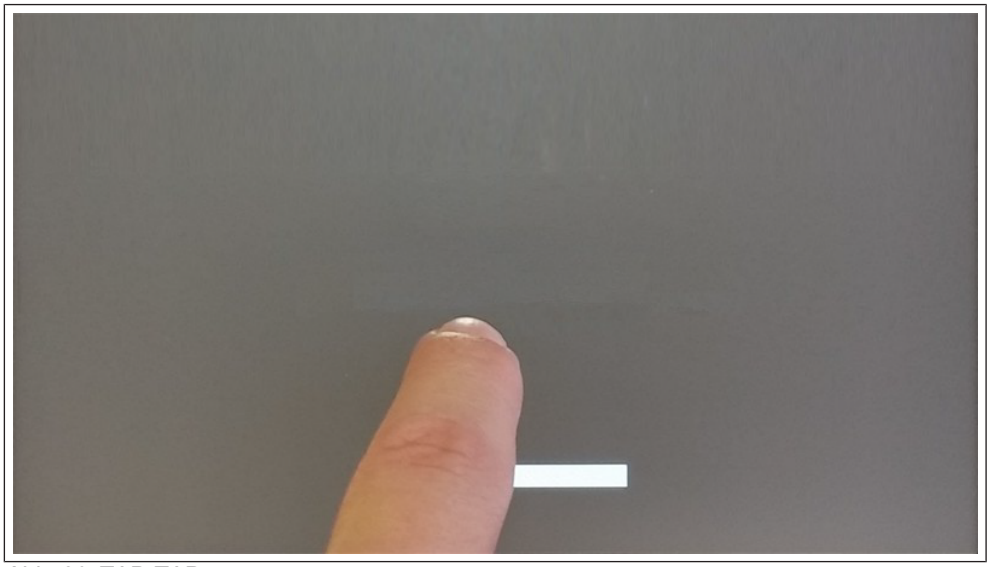

Abb. 30: TAP-TAP starten

Wenn die Meldung "TAP-TAP DETECTED" (Tap-Tap erkannt) oben auf dem Bildschirm erscheint, halten Sie den Finger auf dem Touchscreen gedrückt, um "Neustart" auszuwählen: OS konfigurieren".

Abb. 31: Restart: Config OS

Die HMI startet neu in den Systemeinstellungen im Modus Config OS:

Abb. 32: Restarting

5.4 Kalibrierung des Touchscreens

Die Systemeinstellung Kalibrierung ermöglicht die Kalibrierung des Touchscreen-Geräts, auf die durch Antippen zugegriffen werden kann (nur für resistive Displays verfügbar).

Unmittelbar nach dem Einschalten der HMI wird durch wiederholtes Antippen des Touchscreens mit dem Finger die Tap-Tap-Funktion aufgerufen.

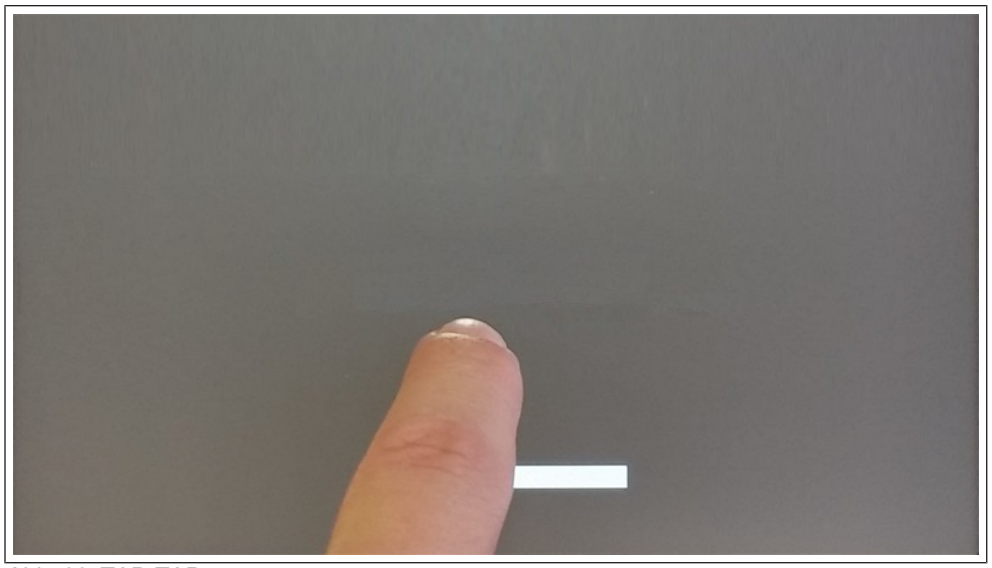

Abb. 33: TAP-TAP starten

Wenn die Meldung "TAP-TAP DETECTED" (Tap-Tap erkannt) oben auf dem Bildschirm erscheint. Warten Sie 5 Sekunden (ohne den Bildschirm zu berühren), um das Untermenü Systemeinstellungen aufzurufen.

Abb. 34: System Settings aufrufen

"Touchscreen-Calibration" auswählen. Die Auswahl wird gelb hervorgehoben. Halten Sie die Position einige Sekunden lang gedrückt, bis der Kalibrierungsvorgang für den Touchscreen beginnt.

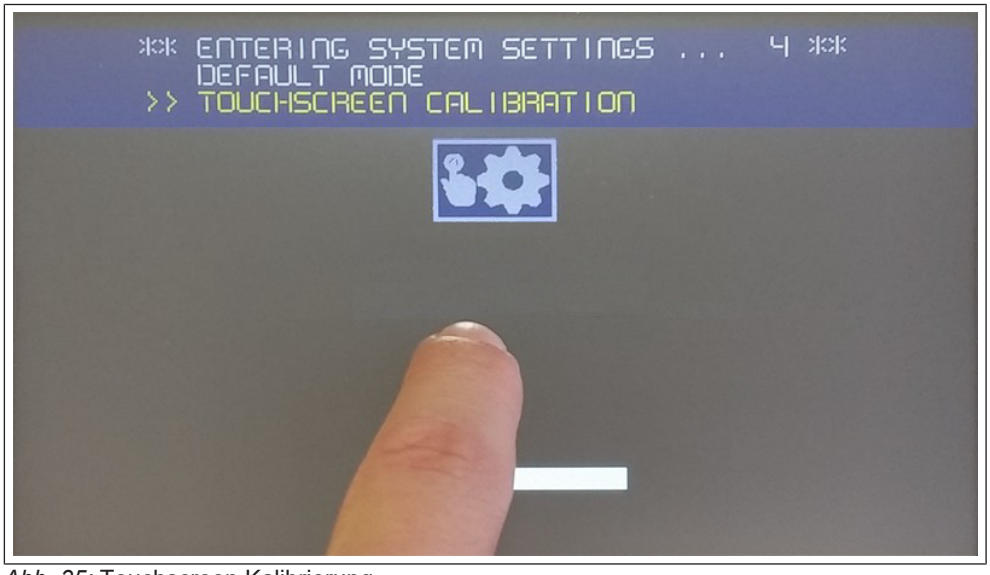

Abb. 35: Touchscreen Kalibrierung

Folgen Sie den Anweisungen auf dem Bildschirm, um den Kalibrierungsvorgang abzuschließen. Das System fordert Sie auf, bestimmte Punkte zu berühren, um den Touchscreen zu kalibrieren.

5.5 Passwortschutz

Internes Passwort des HMI-Gerätes.

Aktivieren Sie auf der Registerkarte "Authentifizierung" in den "Systemeinstellungen" auf den Bearbeitungsmodus und wählen Sie den Benutzernamen aus, um das zugehörige Kennwort zu ändern.

Es gibt zwei Benutzernamen:

Administrator-Benutzername mit vollen Zugriffsrechten ist "**admin**".

Allgemeiner Benutzername mit grundlegenden Zugriffsrechten ist "**user**".

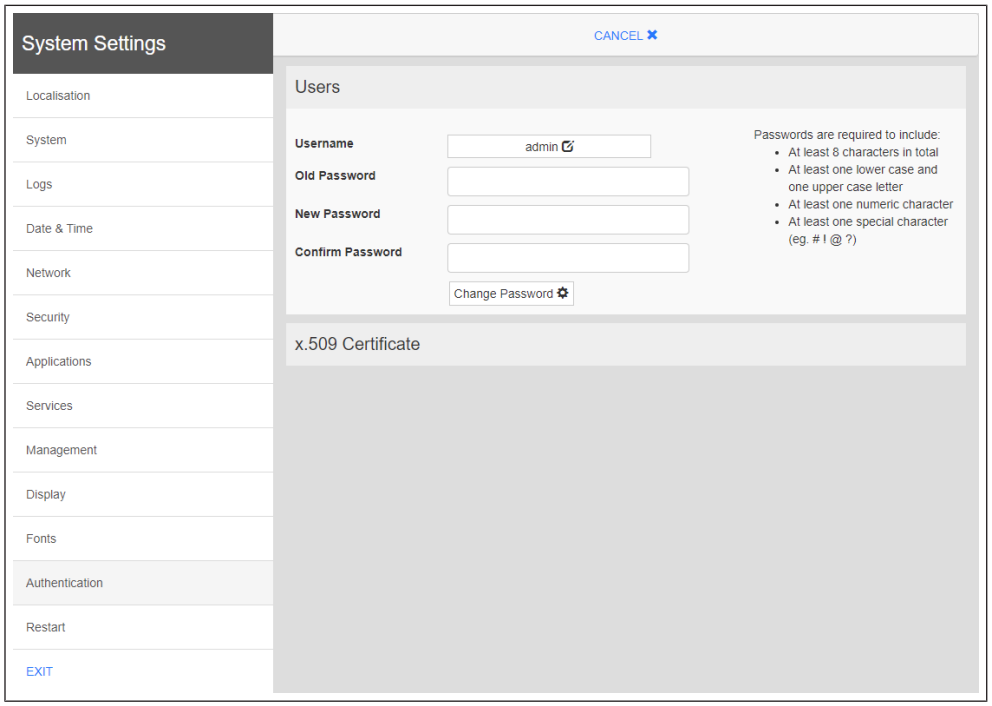

Abb. 36: Passwort ändern

ACHTUNG! Wenn Sie das Passwort vergessen haben, überprüfen Sie die Option "Passwort vergessen".

ACHTUNG! Wenn das HMI-Gerät zum ersten Mal eingeschaltet wird, müssen Sie den Benutzer "admin" und das Passwort "admin" eingeben, um die Passwörter für beide Benutzer (admin und user) festzulegen.

Passwörter müssen folgenden Konventionen entsprechen:

Mindestens 8 Zeichen insgesamt.

Mindestens ein Klein- und ein Großbuchstabe.

Mindestens ein numerisches Zeichen.

Mindestens ein Sonderzeichen (z. B. # ! @ ?).

5.5.1 Passwort vergessen

Wenn Sie das Admin-Passwort vergessen haben, haben Sie die Möglichkeit, es auf den Wert "*admin*" zurückzusetzen. Beachten Sie, dass dieser Vorgang den gesamten Speicher des HMI-Geräts löscht und alle zuvor heruntergeladenen Projekte entfernt werden.

TAP TAP-Option

Das Verfahren ist nur verfügbar, wenn es nicht explizit über die Option "Wiederherstellung des Geräts über TAP TAP aktivieren" in den Systemeinstellungen des Geräts deaktiviert wurde (siehe: (≡► "Wiederherstellung des Geräts über TAP TAP Option aktivieren" auf Seite 25 [▸ 26]))

Schritte zum Zurücksetzen des Admin-Passworts:

- Schalten Sie das HMI-Gerät aus.

- Schalten Sie das HMI-Gerät ein und beginnen Sie, sobald das Logo erscheint, das Touchpanel "anzutippen" (siehe: (≡► " [▸ 42])(≡► Passwortschutz" auf der vorherigen Seite [▸ 42])).
- Wenn "TAP TAP" erkannt wird, wählen Sie im ersten Menü "Systemeinstellungen", im zweiten Menü "Standardmodus" und schließlich im dritten Menü "**Gerätewiederherstellung**".

USB-Option

Das Verfahren ist nur verfügbar, wenn es nicht ausdrücklich über die Option "Wiederherstellung des Geräts über USB aktivieren" in den Systemeinstellungen des Geräts deaktiviert wurde (siehe: (≡► "Wiederherstellung des Geräts über USB aktivieren" auf Seite 26 [▸ 26])).

Schritte zum Zurücksetzen des Admin-Passworts:

- Datei "*device-factory-restore*" auf einem USB-Stick speichern und ins Gerät einstecken.
- Der Wiederherstellungsprozess des Geräts beginnt automatisch. Der Summer ertönt einmal am Anfang und dreimal am Ende, wenn der Vorgang erfolgreich war.
- Datei "*device-factory-restore*" wird vom USB-Stick gelöscht und das Gerät neu gebootet.

5.6 Backup und Restore

Um alle installierten Anwendungen mit ihren Einstellungen zu sichern oder wiederherzustellen, müssen Sie die Schnittstelle für die Systemeinstellungen im Modus "Config OS" mit dem Tap-Tap-Verfahren öffnen.

Siehe "Eingabe der Systemeinstellungen im Modus Config OS durch Antippen" auf Seite 1

Melden Sie sich dann als Administrator an und wählen Sie die Option "Verwaltung". Auf dieser Seite können Sie die Schaltfläche "Abrufen" verwenden, um den Inhalt der Partitionen "**Daten**" und "**Einstellungen**" auf einem externen Speicher (z. B. einem USB-Stick) zu sichern. Verwenden Sie stattdessen die Schaltfläche "Aktualisieren", um den Inhalt einer früheren Sicherung wiederherzustellen.

ACHTUNG! Der Befehl Management ist nur verfügbar, wenn Sie als Administrator angemeldet sind.

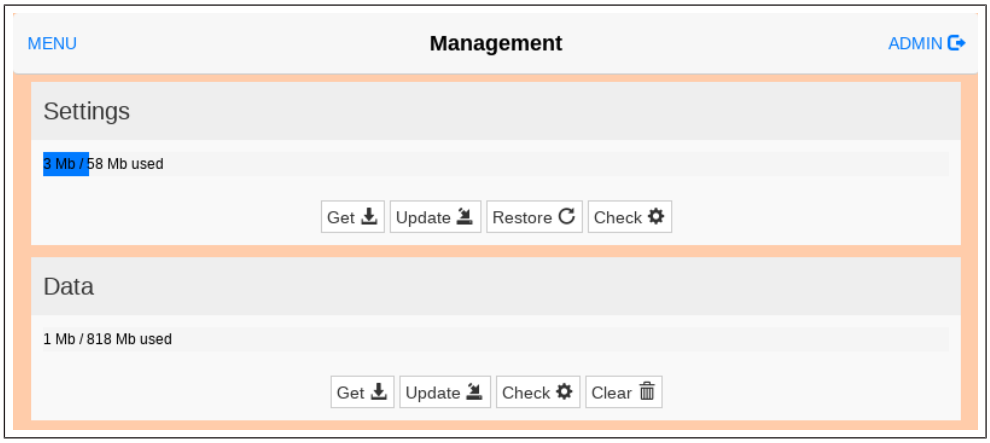

Abb. 37: Backup und Restore Management

Daten Partition

Die Datenpartition enthält die Anwendungen und deren Einstellungen.

Settings Partition

Die Settingspartition enthält die Einstellungen Ihres Geräts (d. h. die Konfigurationsparameter, die über die Systemeinstellungsschnittstelle eingegeben wurden)

VORSICHT! Wenn Sie die Systemeinstellungen von einem Backup aktualisieren, müssen Sie sicher sein, dass das Backup von einem Gerät mit der gleichen BSP-Version (Main OS) ausgeführt wurde.

Die MD5-Datei

Der "Get"-Befehl liefert nur eine Datei mit dem Inhalt der Partition (z.B. data.tar.gz), aber wenn Sie die gleiche Datei mit dem "Update"-Befehl wiederherstellen wollen, müssen Sie eine MD5-Prüfsummendatei bereitstellen.

Die MD5-Prüfsummendatei muss denselben Namen haben wie die Dateien, die Sie laden wollen, mit der Endung .md5, z. B.:

```
daten.tar.gz
```

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

Im Internet lassen sich verschiedene Tools finden, die die MD5-Prüfsumme einer Datei berechnen. Unter Windows 10 ist es auch möglich, das Dienstprogramm "CertUtil" auf der Kommandozeile zu verwenden, z.B.

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

Die MD5-Prüfsummendatei darf nur eine Zeile enthalten. Wenn das Dienstprogramm, das die Prüfsumme berechnet, eine Datei mit mehreren Zeilen erzeugt, müssen die zusätzlichen Zeilen gelöscht werden.

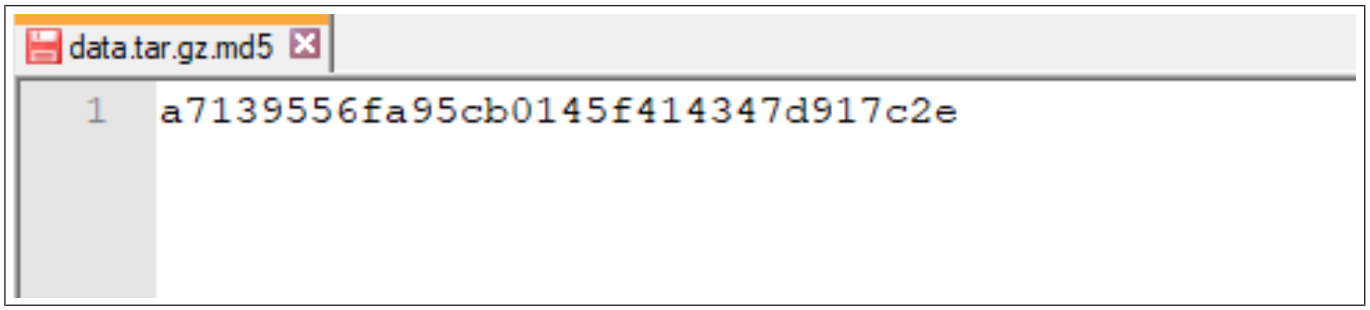

Abb. 38: MD5-Prüfsummendatei

Notizen

WEITERE KEB PARTNER WELTWEIT:
www.keb-automation.com/de/contact

Automation **mit Drive**

www.keb-automation.com

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