Chromium

Web browser on HMI device

User manual

4189341234-B

Improve Tomorrow



Disclaimer

© 2020-2026 DEIF A/S

Subject to change without notice

The information contained in this document is provided for informational purposes only. While efforts were made to verify the accuracy of the information contained in this documentation, it is provided 'as is' without warranty of any kind.

- The copyright of this manual is owned by DEIF A/S
- Unauthorized reproduction of this manual is strictly prohibited.
- Windows is a registered trademark of Microsoft Corporation in the U.S. and other countries.
- Ethernet is a registered trademark of FUJIFILM Business Innovation Co., Ltd. and Xerox Corporation.
- Other company and product names are trademarks or registered trademarks of their respective companies.

Third-party brands and names are the property of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logo, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

Contents

Disclaimer

Web Browser for HMI Devices

Installation from USB Flash Drives 1

Installation from Remote 3

Settings 4

Web Browser 4

The Toolbar 7

Re-enable warnings 7

System options 7

Initial configuration 9

System Configuration

Board Support Package (BSP) 11

Installation of Certified Software Modules 12

Signed file 12

User's Certificate 13

Signature of USB tools 15

Manufacturer's certificate 15

Guideline 15

Allow installation of unsigned modules (Compatible Mode) 16

System Settings 16

Enter in System Settings 17

Localisation 19

System 20

Logs 20

Date & Time 21

Networks 23

Security 24

Applications 26

Services 27

Management 27

Display 27

Fonts 28

Authentication 28

Restart 28

EXIT 28

Services 28

Autorun scripts from external storage 28

Avahi Daemon 29

Bridge/Switch Service 29

Cloud / VPN Service 30

DHCP Server 30

Enable device restore via TAP TAP option 30

Enable device restore via USB 31

Enable TAP TAP menu via touchscreen or mouse 31

Fast Boot 31

Firewall Service 31

Network Rate Limiter 33

NFC Keyboard emulation 34

Reserved CPU cores for applications 34

Router / NAT / Port Forwarding 34

Show loading bar during boot 35

SNMP Server 35

SSH Server 36

VNC Service 36

Web Server 37

Authentication 38

Users and Roles 38

Session 41

x.509 Certificate 41

Forgot password 42

Cloud / VPN Service 42

Update System Components 47

Touchscreen calibration 49

Backup and Restore 51

Recovery Mode 52

Factory Reset 52

Plugin modules

PLCM09 Plugin Wireless Modem 56

Mobile Network 56

LEDs and Digital I/O 58

PLCM10 Plugin Wireless Modem 61

Wireless Network 62

Mobile Network 62

GNSS 64

LEDs and Digital I/O 65

MicroEdge Plug-In LTE/4G Wi-Fi 68

Wireless Network 68

Mobile Network 69

GNSS 71

LEDs and Digital I/O 72

Cybersecurity Guide

Operational States 74

Unboxing 74

Device security-related parameters 75

Logs 75

Date & Time 75

Network 75

Security 76

Applications 77

Services 77

Management 80

Authentication 81

Safe disposal 81

Security Disclosure Policy 81

Web Browser for HMI Devices

Web Browser is a software module that implements a powerful and efficient HTML5 browser for embedded HMI devices.

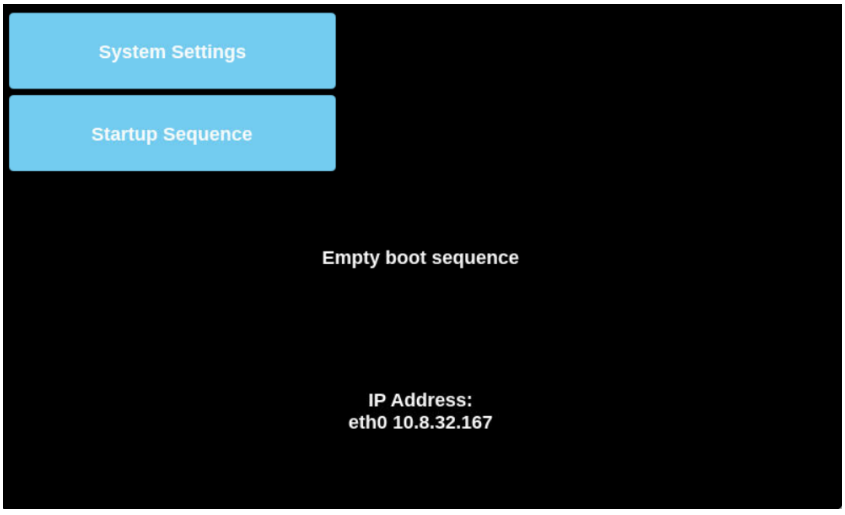
Web Browser is the ideal solution to transform an embedded HMI device in a browser device with HTML5 compatibility for state-of-the-art browsing applications for the industry. With the choice of the appropriate HMI device, the browsing application can be easily installed in the most challenging industrial environments, including hazardous locations, marine installations, outdoor installations and building automation.

The application has been designed for devices based on the embedded Linux platform and ARM processors.

Web Browser can be easily installed on HMI devices with the required platform. Some HMI device models may come with Web Browser already installed..

Installation from USB Flash Drives

Use this procedure for HMI devices that do not have the web browser installed at factory. At first power-up the device shows the “Runtime Loader” screen. If you already have installed applications, you can reach the "Runtime Loader" following the instructions at "Enter System Settings via tap-tap procedure" page 1.



To install the web browser application follow this procedure:

1. Copy the application file to an empty USB stick and insert the key into the operator panel (The supported file systems are FAT16/32 and Linux Ext2, Ext3 and Ext4).

2. On the device select [Startup sequence]

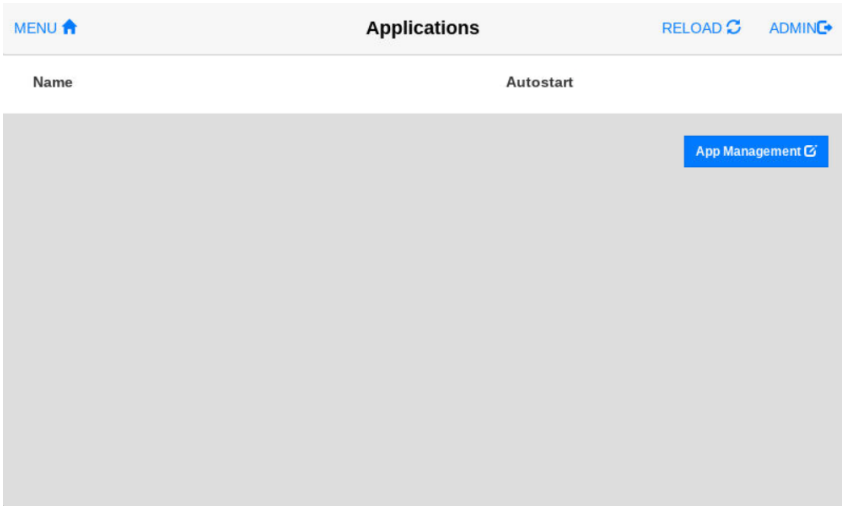
3. Authentication with "admin" credentials is required

4. The System Settings Applications page opens. Click on the [App Management] button.

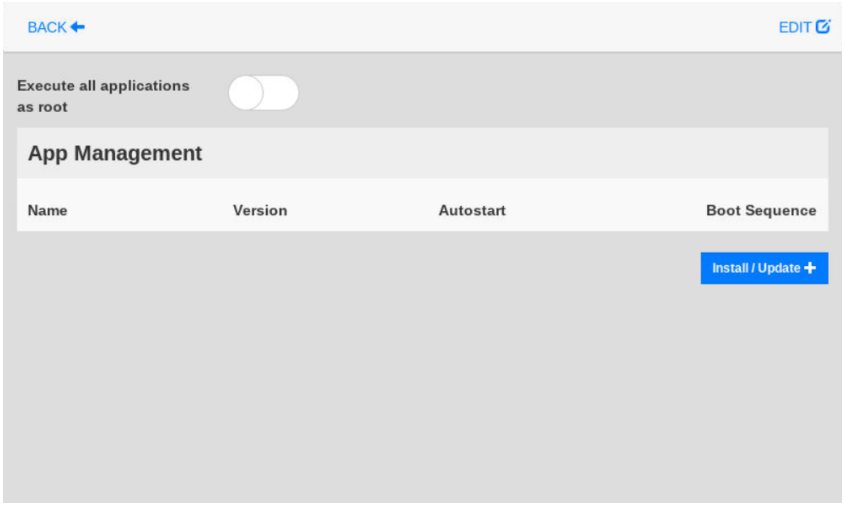


5. In the App Management dialog, click on [Install/Update] button

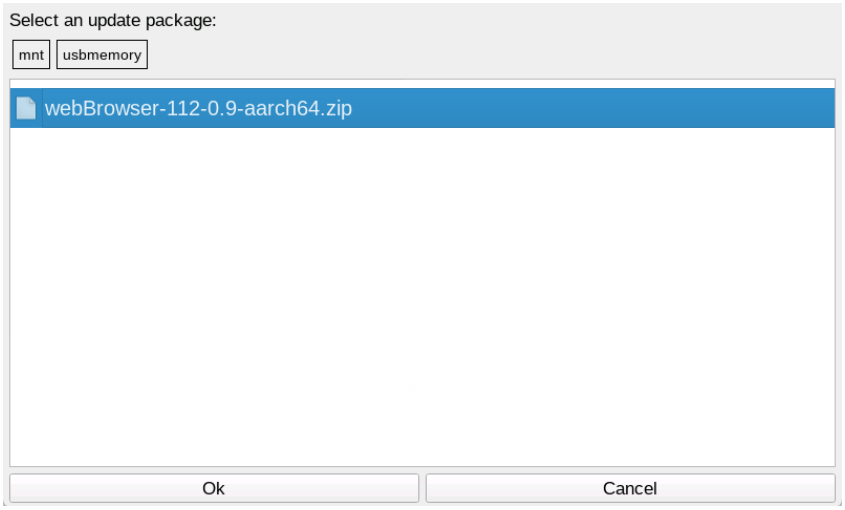
6. Then click [Browser Image] to open the file system dialog where you can select the package to install



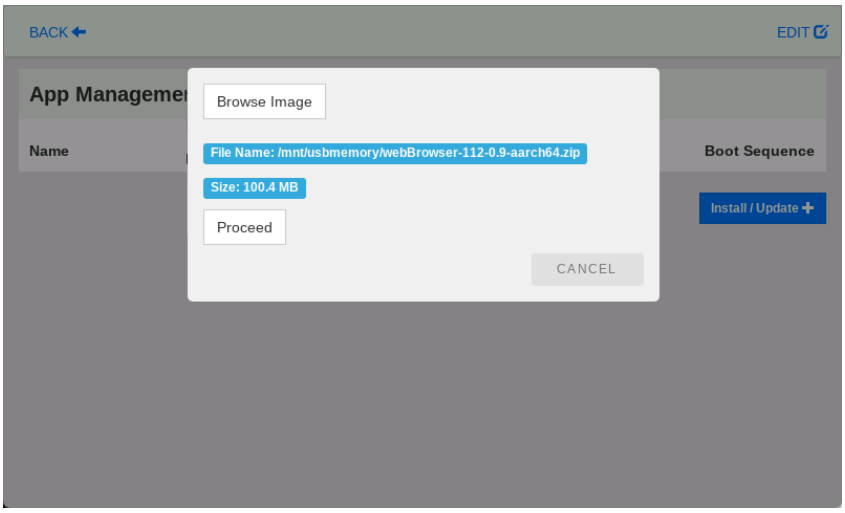
7. Double click on “usbmemory” to open the folder



8. Select the web browser package



9. The runtime installation begins



At the end of the installation, HMI device will restart and the web browser application will start full screen.

Installation from Remote

> This function is not available if the HMI device does not allow remote access.

For remote installation, a PC must be connected to the same network as the operator panel.

1. Enter in your browser the URL of your HMI device: https://<IP-Address>/machine_config
2. Authentication with "admin" credentials is required
3. In the left menu, select "Applications". The System Settings Applications page will open.

Follow the same instructions in the previous chapter and provide the webBrowser package.

Settings

Web Browser software can be fine-tuned for the required application with a rich set of property settings.

Configurable properties are divided in two sets: Basic Settings and Advanced Settings.

At first start up the browser will show System Settings as home page.

To access System Settings you must log in. The user name and password are the same as the operator panel (default admin, admin). At first start up, you will be forced to define a different password (later the password can be changed from System Settings).



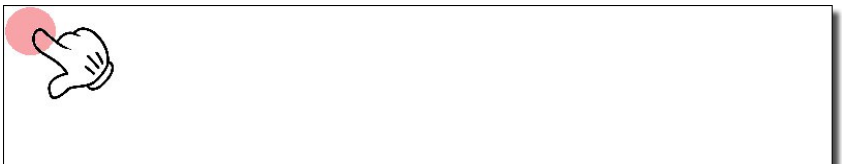
Next, the System Settings page can be opened in several ways:

- From the web browser toolbar (optional, can be disabled) .
- Press and hold the upper left edge of the display for a few seconds .
- Using the Tap Tap procedure on the operating panel, see: "Enter in System Settings" on page 17
- From a remote browser, see: "Enter in System Settings" on page 17 (This feature may be not available)

If enabled, System Settings can be invoked using the Settings button in the address bar



Systems Settings can be recalled keeping pressed the top left edge of the display for few seconds.



Web Browser

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

Property	Description
On Startup	Defines what the device should display when started.
Homepage	URL of the home page to load (must start with https:// or http://)
Alternative homepage	URL of an alternative home page (must start with https:// or http://)
Fallback page	Secondary home page that is loaded when failed to load the primary home page (must start with https:// or http://)
Enable toolbar	Show/hide the toolbar.
- Show toolbar only on error	The toolbar will be displayed only when there is a page loading error.
- Show history buttons	Arrow buttons to navigate through history pages are shown.
- Show bookmarks	Enable the ability to save and use bookmarks.
Allow links to load on a new tab	If the option is enabled new tabs opened by a web page will be managed as follows: • The toolbar, even if enabled, won't be shown. This is done to prevent the user from using a different tab to browse other pages which won't allow to close the tab anymore. • Long press support is enabled. After the system settings login page is loaded, pressing "Back" will make the browser go back to the last opened tab. • From the system settings login page pressing "Load Homepage" will close all tabs except the first one and reload the homepage. • If the page fails to load the tab is automatically closed shortly after (no automatic reloads). • Fallback page and alternative homepage features will only take effect on the main project page loaded on the first tab.
Default page zoom	Only 75, 80, 90, 100, 110, 125 and 150 values can be selected from a drop down menu • This option is global so every page is zoomed in the same way. • The option is not available for devices under 7".
Allow downloading files	Enable the ability to download files. The files will be stored in the folder: /mnt/data/storage/chromium/home/Downloads
Enable history navigation gesture	The swipe gesture can be used to move back and forth between pages.
Options press-and-hold time (s)	How long you have to press the top left edge to view the toolbar.
Change UserAgent	Overrides the default browser user agent.
Restart browser daily	Allows you to set the device to automatically restart at a specific time.

Property	Description
	• No reboot occurs if less than an hour has passed since the last Chromium startup or reboot. • There may be a few minutes delay compared to the configured time
Certificates	Open the web browser certificates manager. (Available only on local settings).
Certificate preferences	Clear all white listed sites . The action can be done in chromium from the toolbar (see: "Re-enable warnings" on the facing page).
Use system virtual keyboard	When disabled, the system virtual keyboard is not shown. Keys can be entered from a physical keyboard or from virtual keyboards define on the active web page.
Enable form autofill	If enabled, the data previously entered are proposed when entering data.
Enable password management	When enabled, the browser will ask to save the entered passwords to repropose them the next time that you will try to log in to the same site. The option will be activated the next time the panel is restarted.

Alternative and fallback homepages

If enabled and an URL is specified the browser will do the following:

At start up if “On start up“ is set to “Open Homepage“:

1. The browser will make 4 attempts to load the main homepage
2. If all 4 attempts fail it will make other 4 attempts to load the alternative homepage
3. If all attempts fail the fallback page (if enabled) or options page is loaded

During runtime:

1. If the browser is pointing to the homepage or alternative homepage domain a HEAD request is sent every 20s to the related full URL specified by the user in the settings.
2. If a HEAD request fails other two attempts are made 5 seconds apart.
3. If 3 consecutive HEAD requests fail the browser will try to load the other homepage.
4. If 4 attempts to load the page fail, the options page is loaded instead. On the other hand if the page is loaded the monitoring process is resumed on the new URL.

For the complete list of available properties, refer to "System options" on the facing page

The Toolbar

When enabled, the Toolbar can be opened/closed using the tab visible at the middle of the top area of the display.



Available commands are:

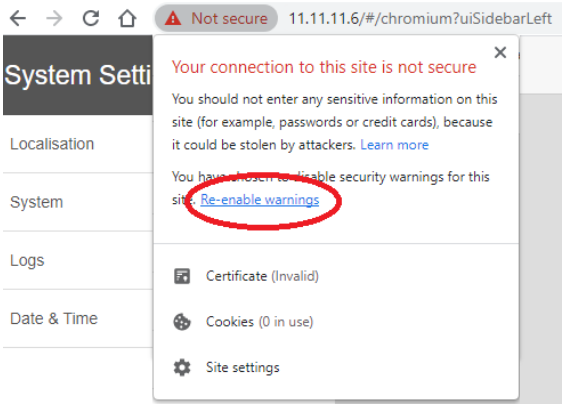
- Page Reload
- Bookmark List
- History Buttons
- URL Address
- Add Bookmark
- Open System Settings

Re-enable warnings

To re-enable the disabled warning messages (e.g., the certificate warning messages) use the below command available from the toolbar of the Web Browser.

Note:

- In kiosk mode, the option is not accessible
- Reboot is needed to apply the settings



The warning message can be re-enabled even from the System Setting page:

Path: System Settings -> Web Browser -> Certificate Preferences -> [Re-enable certificate warnings]

System options

System options can be defined at start-up using command line arguments or adding a settings file .

Using command line arguments

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

Using settings file

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

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

where the options can be added to the file, one per line.

Available System Options

Option	Description
--homepage=<uri>	Override homepage setting.
--enable-exit-button	Enables the "Exit" button in the options page and the "X" icon on the toolbar when enabled. Closes the web browser.
--enable-restart-button	Enables the "Exit" button in the options page and the "X" icon on the toolbar when enabled. Restart the web browser.
--enable-window-exit-button	Like above but only closes the window. In this case when starting again the web browser it will open a new window, which is faster. Command line flags given the first time can not be modified later as it is required a full restart for this. A different URL may be specified instead.
--enable-toolbar	Enables the toolbar. The setting is saved so it will be enabled the next time even without this option.
--enable-toolbar-navigation	Show the history navigation buttons in the toolbar
--enable-toolbar-on-error	Toolbar will be displayed only if there is an error loading the page. The setting is saved so it will be enabled the next time even without this option.
--fixed-toolbar	Toolbar will be fixed and will not be collapsed.
--disable-toolbar	Disables toolbar. The setting is saved so it will be enabled the next time even without this option.
--disable-toolbar-url	Removes URL text area from the toolbar. When used, the toolbar will no longer occupy the whole width of the screen and will be centered instead.
--enable-toolbar-bookmarks	Enables bookmark list and "Add bookmark" buttons on the toolbar when enabled. The "Add bookmark" button will still be hidden if --disable-toolbar-url is used. It won't enable the toolbar if disabled.
--disable-toolbar-options	Removes the options button from the toolbar. It will not enable the toolbar if disabled.
--disable-options	Like above but also disables the long press so that it is no longer possible to access the options page. On loading error the browser will continue to retry and also in this case the options page is never opened.
--disable-toolbar-reload	Removes the reload button from the toolbar
--loadingPage=<URL>	Specified to show a custom page that will load at boot while the actual page is being loaded. This will also hide default error page if the server is not

Option	Description
	ready available. The loading page will remain on until the browser has finished loading the project or the maximum number of load attempts have occurred. The URL must include the protocol (i.e. https://, file://). If no URL is specified (just "--loadingPage") a white page is used. If the web project fails to load the fallback page is shown if set. Otherwise the login page is loaded. The toolbar can be enabled and shown in the loadingPage. "--enable-toolbar-on-error" is also supported, in this case the toolbar has to be shown only 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 failed attempts to load the primary. If this is also not available, the options page is loaded. The URL must include the protocol.
--open-options-after-num-retries=<n>	Modify after how many retries on load error the login page is opened (default is 4). A value <1 will disable the feature.
--retries-on-error-timeout=<n>	Time in seconds between retries. Minimum accepted value is 5 (default is 8).
--disable-fallback-reload	When enabled if the loading of the fallback page fail the browser does not reload anymore and stays on the error page. The default would be to open the options page and continue reloading in background.
--first-load-retry	The browser should retry contacting the server only during the first load. After successfully loading a page no more automatic reloads should be done.

Loading the homepage

If web browser is configured to load a homepage at start-up , these are the steps:

1. Open a first tab with a local "loading page". This page can be modified by using **--loading-page**
2. Start loading the homepage on a second tab while remaining on the first one. Switch to the second as soon the page is loaded
3. If the home page as not loaded after **--open-options-after-num-retries**, if **--fallback-url** is specified try to load fallback URL
4. Open options page if fallback URL is not set or fails to load.
5. **--homepage** should override homepage URL and hide the option from settings page

Initial configuration

Using the file "browser.ini" you can define the configuration that will be applied only once when web browser is started for the first time. So, during normal use, users are free to change the configuration using the System Settings page or the option flags.

The file "browser.ini" must be copied to the web browser installation folder (/mnt/data/hmi/chromium/deploy). Settings are applied at the next restart and at that point the file "browser.done" is created in the same folder to avoid a second reconfiguration. If the file "browser.done" is removed, reconfiguration will be forced at next restart.

Supported keys

- homepageLink=<url>
  URL must include the protocol (i.e. https://, 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, minimum 2000 (2s)
- fallbackToDefaultPageLink=<url>
  URL must include the protocol (i.e. https://, file://)
- disableFallbackReload=true

Example for file browser.ini

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

System Configuration

System Settings is available in the HMI devices as a tool for the configuration of the system properties of the device.

Board Support Package (BSP)

The Board Support Package (BSP) is the software layer containing hardware-specific routines, such as the bootloader, device drivers, and the kernel, that enable the real-time operating system to operate the HMI hardware device.

Currently, in the BSPs, we have two different architectures that we have named "MainOS/ConfigOS" and "A/B, MainOS".

MainOS/ConfigOS

- BSP Version <= 7.x
- Secure Boot is supported when the BSP firmware is labeled with the initials SBxx, whereas firmware labeled UNxx does not support Secure Boot.
- The BSP firmware is distributed in two files, one for the MainOS module and the other for the ConfigOS module (with the extension "*.tar.gz*" for non-secureboot BSPs and "*.img*" for secureboot BSPs), plus two additional files containing the necessary signatures (with the extension "*.tar.gz.sig*" or "*.img.sig*") to ensure their authenticity.
- The BSP can be configured, via the System Settings, to install software modules bypassing the signature authenticity check.
- In BSPs that support Secure Boot (SBxx), the data partition is encrypted and encryption cannot be disabled, whereas in BSPs that do not support Secure Boot (UNxx), the data partition is not encrypted.

A/B, MainOS

- BSP Version >= 8.x
- Secureboot mode.
- The BSP firmware is distributed in a single file (with the "*.img*" extension), plus an additional file containing the signature necessary to ensure its authenticity (with the "*.img.sig*" extension).
- It is not possible to configure the BSP to install software modules bypassing the signature authenticity check. The signature verification is performed again every time the device is powered on. To speed up the boot process, it is possible to disable this additional check.
- The data partition is encrypted, however this feature can be disabled to optimize boot performance.

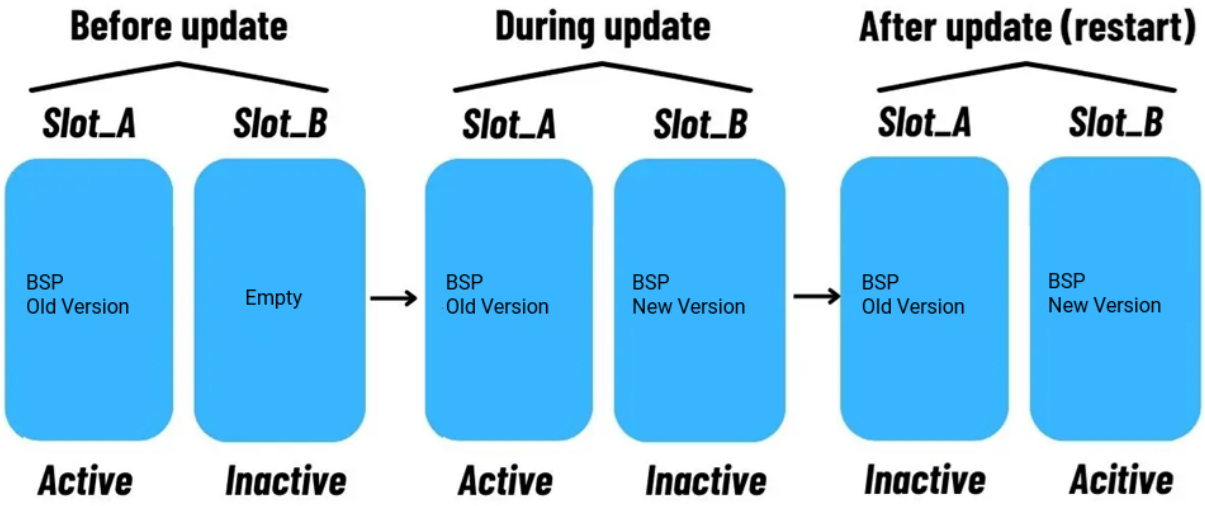
A brief introduction to the 'A/B, MainOS' architecture

Unlike devices with the 'MainOS/ConfigOS' architecture, where the HMI device can operate in the MainOS partition (with all functionalities available) or in the ConfigOS partition (with reduced functionalities), in devices with the 'A/B, MainOS' architecture, the device will always operate in the same partition both in "Default Mode" (with all functionalities available) and in "Recovery Mode" (with reduced functionalities).

This means that with the new "A/B, MainOS" architecture, we do not have two different versions of the BSP for Default and Recovery mode, but it is always the same version that manages both working modes. Consequently, the distributions for BSP firmware updates will occur with a single file (with the "*.img*" extension), plus the signature file (with the "*.img.sig*" extension) for authenticity verification.

BSP Update

To manage the BSP update, a secondary partition, identical to the BSP's working partition, is used. The update occurs in the secondary partition, and only after verifying that it has been successful are the two partitions swapped, thereby disabling the previous primary partition.



> The file system of the active partition is checked at every power on, and if any anomaly is detected, the device is booted in recovery mode using the previous firmware version present in the secondary slot.

Installation of Certified Software Modules

With the introduction of new generation BSPs, system component updates or application installations can only occur if they are certified via a digital signature performed by the manufacturer. Limiting the installation of software modules to signed modules only is a fundamental security practice that offers numerous advantages. In essence, it ensures that the software installed on your system is authentic, integral, and unmodified by unauthorized third parties.

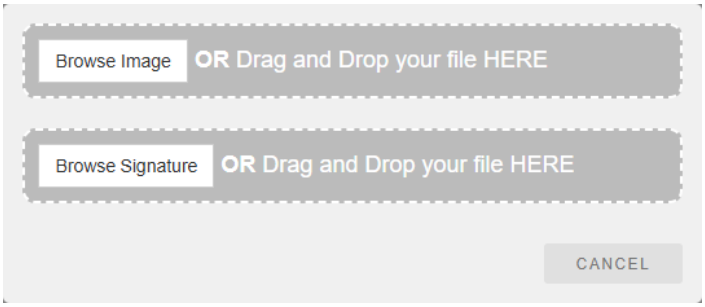
The new generation of BSPs 4.1 and 5.1, starting from build 665, include the ability to control that every module installed on the panel must be signed. To reduce the impact of this new functionality, the new BSPs are distributed with signature control disabled. Anyway, we recommend carefully reading this guide and enabling support for signature control (see: "Allow installation of unsigned modules (Compatible Mode)" on page 16).

> Since European directive **RED-DA-18031** requires verification of software module authenticity for all devices equipped with radio equipment, when WiFi is enabled (for devices that support it), it's recommended to also enable signature control.

When signature control is enabled, the user must obtain their own certificate (**User's Certificate**) to sign and install applications on the HMI device.

Signed file

To install or update a software module, you'll also need to provide the module's signature file.



The file containing the module's signature is a two-line ASCII file. The first line contains the MD5 hash of the file, while the second line holds the module's signature performed by the manufacturer.



User's Certificate

If you don't own a certificate to sign your applications for upload to the device, you can create one using OpenSSL.

Here is an example of how to generate a certificate using a public OpenSSL-Win32 library (https://www.openssl.org).

File: *CreateCertificates.cmd*

```
@echo off
set OpenSSL="C:\Program Files\OpenSSL-Win64\bin\openssl.exe"
set CertificateName=MyCertificate

rem Generate an RSA key
    %OpenSSL% genrsa -out private_key.pem 4096

rem Creating Certificate Signing Requests
    %OpenSSL% req -new -sha256 -key private_key.pem -out certificate.csr -subj
"/ST=NY/C=US/L=New York/O=CompanyName/OU=R&D Team/CN=%CertificateName%"

rem Self Sign the Certificate Signing Requests
    %OpenSSL% x509 -req -days 365 -in certificate.csr -signkey private_key.pem -out
certificate.crt

rem Convert to .pfx file
    %OpenSSL% pkcs12 -export -passout pass:PswOfCertificate -out certificate.pfx -
inkey private_key.pem -in certificate.crt -CSP "Microsoft Enhanced RSA and AES
Cryptographic Provider"

pause
```

The procedure will require creating a password, which will then be necessary to access the certificate's private key (in the example script, the password "*PswOfCertificate*" has been defined).

Two files will be generated:

- **certificate.pfx** is the certificate containing the private key to install on your PC to sign code. You'll need the certificate's password to install it

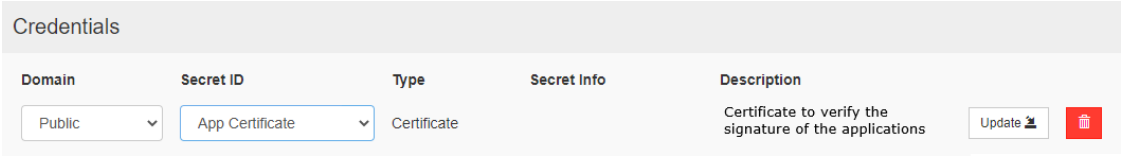
- **certificate.crt** is the certificate containing the public key that must be installed on the HMI device so it can verify the signature
- **private_key.pem** It's the file with the private key associated with the certificate that can be used to sign your applications. It's crucial not to disclose this key to avoid invalidating the encryption process.

How to install the certificate on the HMI device

On the HMI device the *certificate.crt* can be installed from the System Settings of the HMI device in the Security area (Ref. "Security" on page 24).

In the Security area, select:

- Domain = Public
- Secret ID = App Certificate
- Type = Certificate
- Use the "Update" button to load the certificate



Script to sign a file

Here is an example of how to sign the application file to be installed on the HMI device.

File: *Signing.cmd*

```
@echo off
set OpenSSL="C:\Program Files\OpenSSL-Win64\bin\openssl.exe"
set FileName=MyApplication.zip

rem Generate the MD5 file
    certUtil -hashfile %FileName% MD5 | find /v "hash" > md5.tmp

rem Sign the MD5 file
    %OpenSSL% dgst -sha256 -sign private_key.pem -out %FileName%.sig.tmp %FileName%
    CertUtil -encodehex %FileName%.sig.tmp encoded.tmp 12 > nul

rem Merge MD5 and sign
    copy /b md5.tmp+encoded.tmp %FileName%.sig > nul

rem Delete the MD5 file
    del *.tmp

echo Done
pause
```

A new file with a .sig extension will be generated:

- **MyApplication.zip.sig** It's the file with the application's signature to be used for installing the application.

Signature of USB tools

Applications run from a USB drive will also need to be signed. In addition to the tool itself, a file named "**manifest.json**" must be included on the USB drive, containing the signature for each file belonging to the tool. The "manifest.json" file itself must also be signed.

Here is an example of a manifest file.

File: *manifest.json*

```
2b3247e12c7d99d20cd797c2239e50f345f0f6676ea6872b1943be4144ec...
{
   "name": "PrintScreen",
   "version": "1.0",
   "files": [
      {
         "path": "autoexec.sh",
         "signature": "badf27ae987e4c70a45ae20ee2d4545e7e8bd...
      },
      {
         "path": "bin/mylib.so",
         "signature": "d725d491fe911afe39ce4c5380aff2f1a115c...
      }
   ]
}
```

The first line contains the signature of the manifest.json file, while the file itself lists the tool's files with their signatures.

Here's how to prepare a manifest.json file, step by step

1. Create a text file without the first line, meaning the text contained between the two curly braces (here you need to include one or more files).
2. Using the "Signing.cmd" script, generate the signatures for each file.
3. Copy each file's signature (the second line of the file generated by the "Signing.cmd" script) into the "signature" field of its respective file descriptor.
4. Use the "Signing.cmd" script to generate the signature for the "manifest.json" file.
5. Insert the "manifest.json" file's signature (the second line of the generated signature) into the first line of the file.

Manufacturer's certificate

To validate the integrity of the certificate included in the BSP, it is necessary to verify the fingerprint contained in the certificate and displayed in the first line of the management page ("Update System Components" on page 47) by comparing it with the fingerprint published by DEIF A/S.

Date	Fingerprint	Status
18/Jun/2025	11:DF:FE:FD:E5:55:A9:D0:2A:3B:EE:70:BA:29:C9:73:B9:F0:72:41	Valid

Guideline

When signature control is enabled, all software modules, including applications, can only be installed if they are certified (i.e., signed by the developer). Therefore, the application developer must obtain their own certificate to sign the

applications or modules they intend to distribute or install on the device.

The certificate essentially consists of two keys: a **secret key** (which must not be disclosed) that allows the developer to sign the application, certifying it was developed by its owner, and a **public key** to be installed on devices, which allows for verification of the signature's authenticity. After installing the public key on the devices, the developer can generate their application and distribute it along with the file containing its signature to install it on the HMI devices.

System modules as well, e.g., Data Partition, Settings, FRAM, etc., must be signed to be loaded onto the device.

> The user certificate, if installed, allows for the signing of all device modules except for system modules (MainOS, ConfigOS, and Bootloader), which must be signed by the manufacturer.

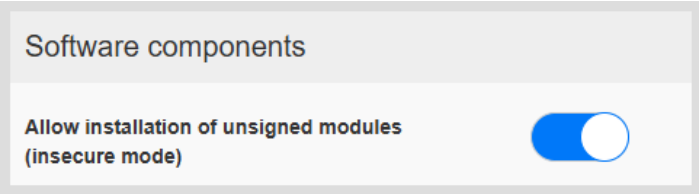
Step by Step Procedure

1. Use the *CreateCertificates.cmd* file to generate a certificate.
2. Use the *Signing.cmd* file to sign the software module you want to install on the panel.
3. Install the **certificate.crt**, which contains the public key, in the "Security" area of the device where you intend to upload your application.
4. Provide the software module and its signature during the installation process.

Allow installation of unsigned modules (Compatible Mode)

Signature verification can be disabled, however, this is an unrecommended operating mode that you shouldn't use unless you're fully aware of what you're doing.

System Settings -> Security -> Software Components



> This option is not available in BSPs with the 'A/B MainOS' architecture.

System Settings

The user interface of System Settings is based on HTML pages and can be accessed both locally on the HMI device screen and remotely using a web browser (remote access may be disabled and may be unavailable).

The administrator username is "admin" with default password "admin", but at first start up, you will be forced to define a different password (later the password can be changed in the “System Settings -> Authentication” page).

> The 'admin' user always has access to all services available on the HMI device, while other users only have access to the services that have been enabled for their role.

Enter in System Settings

There are several ways to access the System Settings page.

You can enter

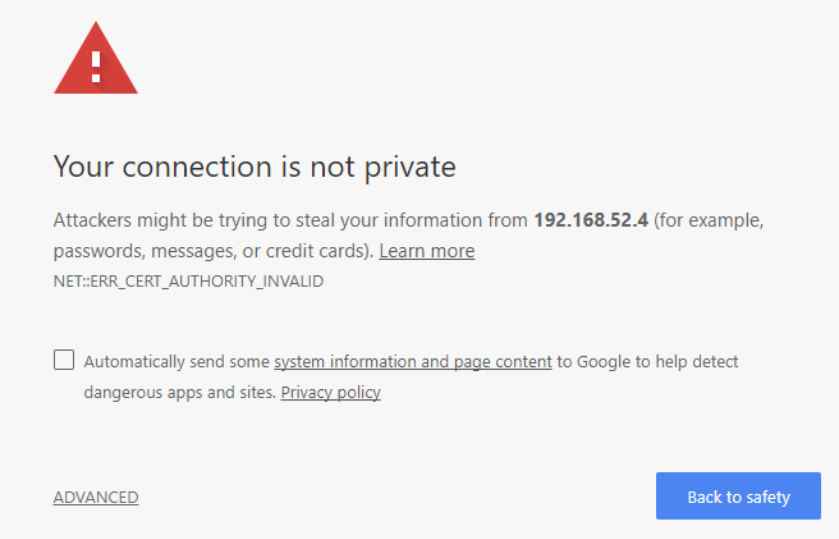
- From a remote web browser (remote access may be disabled and may be unavailable)
- From the HMI device when no runtime is load
- From the HMI device using the tap-tap procedure

System Settings access from Web browser

To access System Settings using a Web browser, enter the IP address of the device, in the following format:

https://IP/machine_config

> Note the remote access use encrypted https protocol on port 443. When the connection is established, the HMI device send a certificate to use for the encryption. Since the certificate is not signed from a Certificate Authority you will get a warning message. Please, click on advanced options and choice to proceeding.



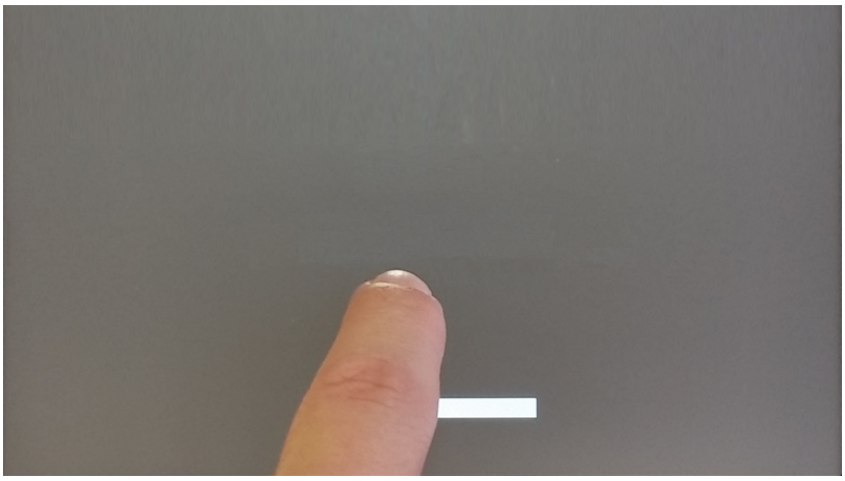
System Settings access from HMI device

When no applications are installed, System Settings are accessible from the buttons displayed on the screen.



System Settings access via TAP TAP procedure

Tap-tap consists in a sequence of several touch activations by simple means of the finger tapping the touch screen performed during the power-up phase and started immediately after the HMI is powered on.



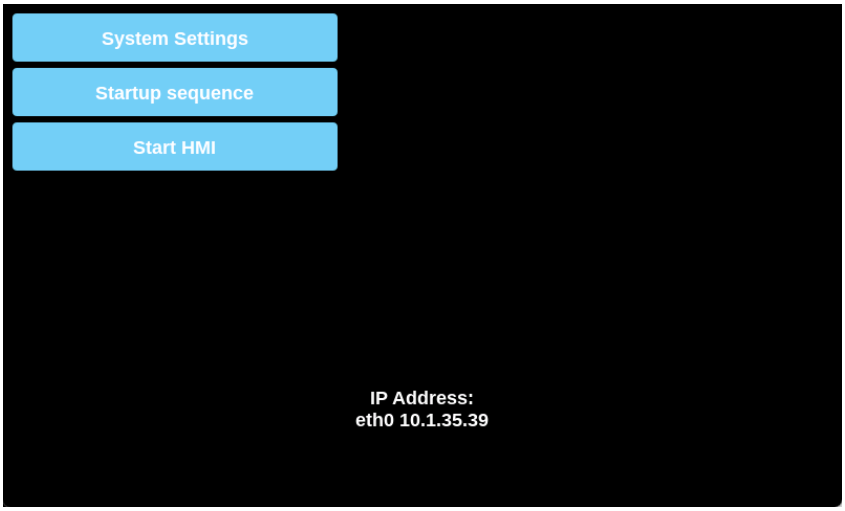
When “tap-tap detected” message appears on the top of the screen. Wait for 5 seconds (without touching the screen) to enter System Settings sub menu



Wait for 5 more seconds (without touching the screen) to enter Default Mode



Select "System Setting" from the HMI Default Mode screen



System Settings Sections

To change system settings values, enter in edit mode by click the edit button on the right top.

> The edit button is available only inside the dialogs that contains modifiable parameters.

Localisation

Set the below parameters to adapt the device to your country.

- Country Code (only needed on 5G devices)
- Language for the system settings interface
- Layout of the virtual keyboard

> Country Code is required for the WLAN Regulatory Domain and the device will not use the WiFi until this parameter will not have been set.

The country settings are required for operation complying with the approvals. Selecting a country that does not match the country in which the device is operated may be punishable by law. After selecting the Country Code, the corresponding channels allocation and setting and for power level will be automatic.

System

Parameter	Description
Info	Device information
Status	Device status (Free RAM, Up time, CPU Load)
Timers	Device timers (System on, Back light on)
Sensor	Values detected by any sensors present in the HMI device (Temperature, Humidity, etc.) Sensors are not available on all models.
RGB Led mode	Some HMI devices have an RGB LED that can be configured to indicate the connection status of the Cloud/VPN service. • Cloud / VPN Service The RGB LED indicates the Cloud/VPN connection status. RED — Internet connection not present RED (Blinking) — Corvina Service not enabled YELLOW — Corvina Servers not reachable YELLOW (Blinking) — License not active BLU — Device connected to Corvina BLU (Blinking) — Device connected but not yet activated on Corvina ORANGE — VPN connection active • User Controlled The RGB LED is controlled by the application loaded on the HMI device
PlugIn	Hardware plugin information
Legal	Legal information regarding components licensed under GPL/LGPL

Logs

OS Logs
refer to all information related to the HMI device's operation, used to verify its correct functioning or to diagnose any malfunctions. This type of log collects information from the moment the equipment is powered on until it is powered off.

Parameter	Description
Persistent	If enabled, log files will not be deleted when the HMI device is powered off.
Size (MB)	Log file size. The system manager cyclically fills 3 files of this size.

Security Logs
refer to the audit information collected to track who accesses the HMI Device and the operations performed. This log is permanent and is not deleted when the device is powered off.

The messages are RFC 5424 compliant.

Parameter	Description
Persistent	If enabled, log files will not be deleted when the HMI device is powered off.
Size (MB)	Log file size. The system manager cyclically fills 3 files of this size.

Remote Logging	If enabled, send the log messages to a remote RSysLog server.
	Useful rule to add to the rsyslog.conf file:
	`# Audit with RFC5424 format`
	`$template RemoteAudit,`
	`"/var/log/remotelogs/%HOSTNAME%@%FROMHOST-IP%/audit.log"`
	`local0.* ?RemoteAudit;RSYSLOG_SyslogProtocol23Format`

- Server	RSysLog server IP address.
- Port	RSysLog server port (usually 514).

GET Button
A collection of text-based log files is compressed into a .gz file. The 'messages' file contains primary system information, and the 'audit' folder holds security-related data.

Date & Time

Device date and time.

Parameter	Description
Current Timezone	Timezone region **Daylight Saving Time (DST) Handling** Some regions use DST, where the system clock is automatically adjusted during specific periods of the year. In installations where automatic time changes are not required, DST adjustments can be avoided by selecting a fixed-offset time zone. **Fixed Time Zone Configuration** Linux systems provide special time zones under the Etc category that represent fixed UTC offsets and do not apply DST changes. For example: For Ex, for Italy, "Etc/GMT-1" it's equivalent to "UTC+1" to have a date/time without any change. Using an Etc/GMT time zone keeps the system time constant throughout the year without automatic daylight-saving adjustments.
Current Date **Local Time**	Date and Time can set manually only when the Automatic Update is disabled.
Automatic Update (NTP)	Enable to keep date and time synchronized from a remote server • NTP Server Specify the Internet NTP Server address The NTP Client of the HMI Device is a complete implementation of the Network Time Protocol (NTP) version 4, but also retains compatibility with version 3, as defined by RFC-1305, and version 1 and 2, as defined by 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 maximize accuracy while minimizing network overhead. The process is designed to operate in a changeable mode between 8 sec and 36 hr.
Slow time adjustment (not more than one minute a day)	Here, you can select whether the NTP can apply a signification correction to correct date & time error. • Disabled The NTP can apply a signification correction to correct date & time error

Parameter	Description
	• Enabled The NTP must correct the drift by using the standard correction rate of 500 ppm . If the latter is the case, it should take quite a long time to align system time to the NTP server time (for example, to correct a difference of 5 minutes would take about 7 days)
Accept NTP requests	When enabled the device will accepts NTP requests from outside. When automatic update is not enabled the device will share the local RTC clock time.

Networks

Network parameters. Available parameter in edit mode:

Parameter	Description
General Settings	Device hostname Avahi Hostname (see "Avahi Daemon" on page 29)
Network Interface	Network parameters of the available interfaces • DHCP • IP Address • Net Mask • Gateway • Metric • 801.2x Protocol **Metric** The 'metric' parameter is a numerical value assigned to a network interface that determines its preference in routing decisions. This means that when a device has multiple network interfaces configured on the same subnet, the operating system will typically choose the interface with the lowest metric as the default route for outgoing traffic.

Parameter	Description
Native Buzzer Event	Offers the option to keep or remove the buzzer feedback when the network cable is plugged in or unplugged. The change will take effect after restarting the device.
DNS	DNS Servers DNS server addresses are generally provided by DHCP servers, but you can manually add the addresses of the DNS server to be used. Manually entered static DNS servers have a higher priority than dynamic addresses provided by the DHCP server. Search Domains Optional domains that will be used in concatenation with the provided URLs

Security

Services are available only when logged as admin.

The security area contains passwords and certificates, required by applications.

Parameter	Description
Domain	Identifies a set of secret information that can be used by installed applications that have the rights to use it. The preconfigured domains are: • General This space is available for third party applications • System This space is used from the services embedded in the device (e.g. the VNC Server) • HMI Runtime This space is used from the HMI Runtime application • Public This space is available for public certificates. Specifically, the certificate used to verify the application's signature (App Certificate) to be uploaded to the device should be placed here.
Secret ID	Name used to identify each secret information included in the selected domain.
Type	Type of information to be stored.

Parameter	Description
	• Text • Password • Certificate • File
Secret Info	The secret information to keep stored.. In case of text or password, type the text or the password to store. In case of certificate or file use the "Update" button to upload the file to store.
Description	A free text that you can insert at will.

Import/Export

Using the Import/Export commands, it is possible to export the stored information and import it, e.g., into other devices. Note that the export command will prompt you to define a password which will then be required in order to import the exported file.

> Data is exported to the file using a proprietary format with AES-256 encryption.

External Devices

- **Disabled external USB device**

  If disabled, unknown USB devices are not accessible. When the "Disable External USB Devices" switch is set to ON, all devices connected to USB devices are added to a white list and will continue to be available.

  > Before disabling external USB devices, be sure to disconnect any connected devices that should not be accessible.

- **Disable SD card automount**

  If disabled, SD cards are not automatically mounted. They can be mounted from the SSH interface or a script file.

  > The bootloader will still allow updates via SD even when automatic mounting is disabled.

System Hardening

- **Enable encryption of user data**

  The data partition can be encrypted (using a cbc-aes cipher) so that the data is illegible in the event that the physical storage medium is exported from the device.

- **Enable application signature verification at startup**

  The authenticity check of the software modules can be repeated at every device power-up (or 'startup') to ensure that no tampering has occurred.

> These options are not available in BSPs with the 'MainOS\ConfigOS' architecture.

Software Components

The option "*Allow installation of unsigned modules (insecure mode)*" allows you to disable the signature verification of modules loaded onto the BSP.

> For security reasons, this is a not recommended operating mode, and you shouldn't use it unless you're fully aware of what you're doing.

> This option is not available in BSPs with the 'A/B MainOS' architecture.

Applications

The applications page is listing the applications loaded on the HMI devices. From this page is possible to manage the applications.

Parameter	Description
Name	Application name
Autostart	If selected, the application will start when the operator panel is turned on

App Management

Press the "*App Manager*" button to enter the application management mode from where you can:

- upload new applications

> If signature verification has been disabled, you can provide an .md5 file for check sum verification (ref.; "Allow installation of unsigned modules (Compatible Mode)" on page 16)

- update existing applications
- remove application
- define the startup sequence.

Execute all applications as root

For security reasons, applications are currently running in a restricted user mode. Setting this flag will escalate their privileges to root mode, allowing them to access system-level resources.

> The "Applications" page is not available when you access the System Settings directly from Chromium. It can be accessed by going to the System Settings page from an external browser or directly on the device using the TAP TAP procedure.

Services

From the Services page, you can enable and configure the various services available on the HMI device. For more details, refer to the "Services" on the next pagechapter.

Management

From the management page, you can update the system components of the HMI device. Please refer to the chapter "Update System Components" on page 47 for more details.



CAUTION: Working in the Management area is a critical operation and, when not performed correctly, may cause product damages requiring service of the product. Contact technical support for assistance.

Display

You can personalize your display by adjusting the following settings:

- Brightness
- Back light timeout
- Orientation
- Display Hue
- Display White Balance
- Display Color Saturation (RGB)
- Enable G2D graphics acceleration (Wayland BSP version)

The available options may vary depending on your device.

Fonts

Lists available system fonts and gives you the option to upload custom fonts.

Note that font files may require a license to use.

Authentication

From this page, you can customize the X.509 certificate of the HMI device and define the users who have access to the configuration parameters. Please refer to the chapter "Authentication" on page 38for more details.

Restart

HMI device restart command

EXIT

Exit from the System Setting tool.

Services

Mouse click on the enable button to enable/disable the service. Click the service name to list the associate parameters.

Autorun scripts from external storage

Enable/Disable the possibility to run the "autoexec.sh" script file when a USB key is plugged into the device. Disable this service if you want to prevent unauthorized access through the USB interface.

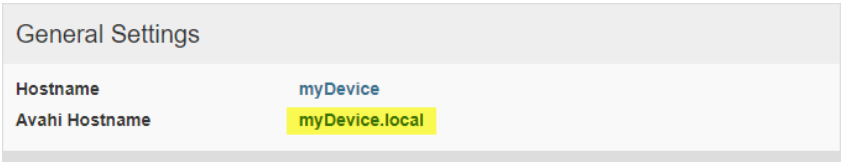
Using next-generation BSPs, these files must be signed in order to be executed (see: "Installation of Certified Software Modules" on page 12)

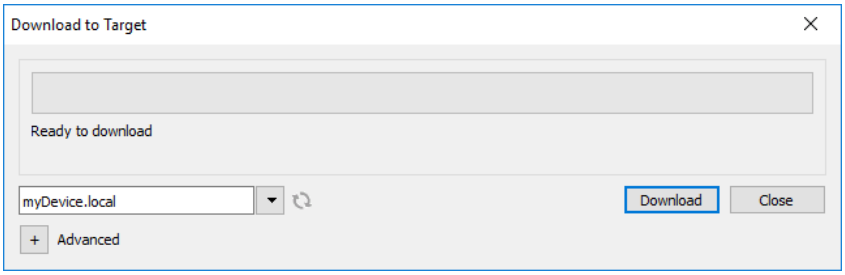
Parameter	Description
Enabled	If enabled, an "autoexec.sh" script file found on a USB drive will execute when the USB drive is inserted into the device.
Allow user-certified scripts only	If enabled, any signed tools from the manufacturer will not run. Only tools signed with the user-installed certificate will be able to execute (ref.: "User's Certificate" on page 13). This way, the administrator can select which USB tools to allow on the device.

Parameter	Description
	Digital signature is not checked when "Allow installation of unsigned modules (insecure mode)" is enabled..

Avahi Daemon

Avahi is a system which enables programs to publish and discover services and hosts running on a local network. When it is enabled, the HMI device can be reached even using the device's host name (in alternative to the IP Address).





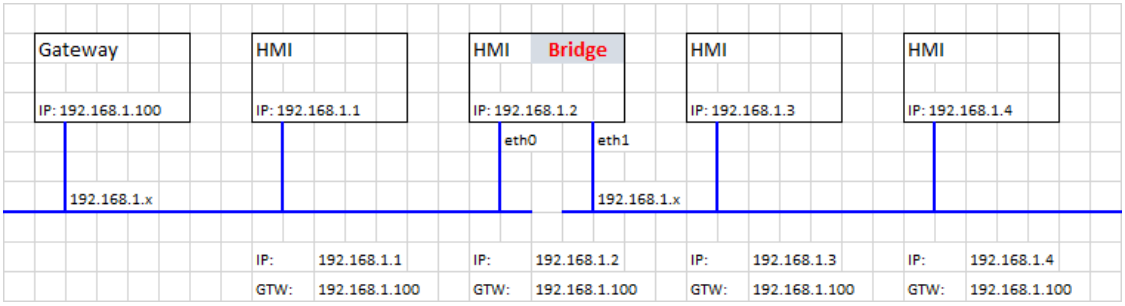
Avahi Daemon runs on UDP port 5353

> On Linux and Apple PCs, the Avahi service comes for free with the OS. On Windows PCs instead, you need to install an Avahi service to be able to reach the panel by his Avahi host name (e.g. you need to install the Apple Bonjour application - Bonjour is a trademark of Apple inc.).

Bridge/Switch Service

Using the bridge service is possible connect together the WAN (eth0) network adapter with the other network interfaces. When used, the two Ethernet interfaces are bridged and both Ethernet interfaces are sharing the same IP address.

Bridge Service creates a Linux-based layer-2 Network Bridge between two or more network interfaces. If both WAN and endpoint devices are attached to such bridge, the two networks will be physically joined and endpoints will be available as if they were directly connected to the WAN (Note: Cloud scenario still requires Router Service to be active)



Cloud / VPN Service

Allow to manage remote HMI devices connected to a centralized server through gateways.

See "Cloud / VPN Service" on page 42 for additional details.

DHCP Server

Provide the DHCP Server on the selected interfaces.

Parameter	Description
Enabled	Enable the DHCP Server on the selected interface
Start IP **Stop IP**	IP addresses distributed from the DHCP Server
Gateway	The gateway address
Netmask	The provided netmask
DNS Server	The DNS server address
Lease Time (seconds)	Lease time, default is 86400s (1 day) Acceptable values are from 60s to 864000s (10 days)

Enable device restore via TAP TAP option

When enabled, it gives the possibility to reset the operator panel in case the administrator password is forgotten. (See.: "Forgot password" on page 42)

This option is enabled by default. You can disable it to increase the security of the device (this could eliminate the possibility of recovering a forgotten password).

Required BSP v1.3.491 or greater

Enable device restore via USB

When enabled, it gives the possibility to reset the operator panel in case the administrator password is forgotten. (See.: "Forgot password" on page 42)

This option is enabled by default. You can disable it to increase the security of the device (this could eliminate the possibility of recovering a forgotten password).

Required BSP v1.3.564 or greater

Enable TAP TAP menu via touchscreen or mouse

Configure whether the taptap menu can be accessed using a mouse or touchscreen.

Keyboard access (via the CANC key on a USB keyboard) will remain unaffected by this setting.

Fast Boot

When fast boot is enabled, at the power up the HMI device will start the HMI application as fast as possible. In this mode, there are not showed diagnostic information (e.g. the loading bar) but only the minimum necessary features are loaded before loading the User Interface (e.g. System Settings, VNC, SSH, etc. will be load after loading the HMI application).

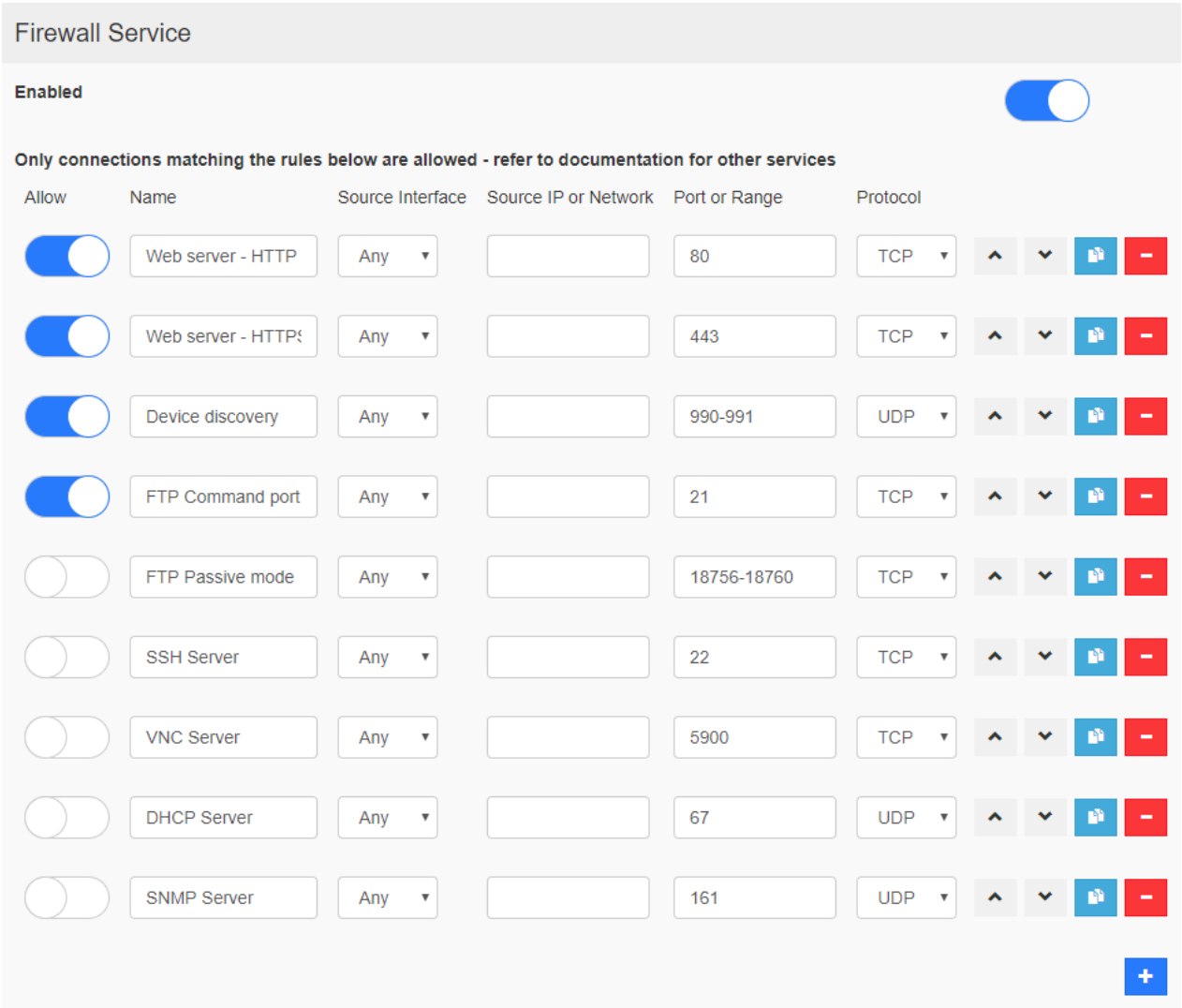
To obtain best performance, in addition of enabling the fast boot mode, it is recommended to:

- disable any service that is not necessary
- avoid keeping enabled the persistent log
- use static IP address instead of DHCP service

Required BSP v1.0.242 or greater

Firewall Service

When the firewall is enabled, only connections matching the defined rules are allowed. Note that some rules must be enabled for the HMI can to work properly.



Notes:

- The firewall is based on IP tables which operates only at layer 3 (layer 2 packets won't be filtered, e.g. ARP)
- Only INPUT and FORWARD packets are filtered, not OUTPUT
- PING/ICMP echo reply packets are always allowed
- Internet sharing scenarios (e.g. 3g or wifi connection to endpoints) are not supported
- Packets filtered by the firewall are dropped

Source IP or Network

If this field is unspecified, access will be allowed 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). For details on valid subnet specifications following such format, please refer to: https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

If you enable the Firewall and you need to use the FTP passive mode with HMI Runtime older than version 2.10.0.280 then you need to open the ports 1024-2048/tcp and 16384-17407/tcp. From version 2.10.0.280

nstead, HMI Runtime uses the ports 18756-18760/tcp that are proposed into Firewall settings by default.

Firewall is available from BSP v1.0.532
If you are updating from an old BSP version and you don't see the default rules, you have to reset the system settings (see "Update System Components" on page 47).

Whitelist & Blacklist

By configuring a DNS whitelist, you can restrict network traffic to a specific set of DNS servers. Conversely, the blacklist feature allows you to prevent devices from resolving names using certain DNS servers.

- Disable
  All DNS server are accessible:
- Whitelist
  List of only accessible DNS servers.
- Blacklist
  List of inaccessible DNS servers.

Network Rate Limiter

Rate limiting is a method employed to control the amount of network traffic. By setting limits on the number of requests that can be made within a specific time frame, it prevents users from overwhelming system resources. This technique acts as a safeguard against malicious attacks like Denial of Service (DoS) where attackers flood a system with excessive requests, rendering it inaccessible to legitimate users.

Using this service, you can create rules to limit the maximum number of packets transmitted on network interfaces.

Parameter	Description
Active	Enable the rule
Name	A label that identifies the rule
Source Interface	The network interface where the rule is applied
Data Type	Choose the network packet type to be subjected to filtering (ETHER, IP, SYN, UNI)
Rate	Data rate over a defined time period
Measure	Select the measurement unit • Packets per second (Pcks/sec) • Packets per minute (Pcks/min) • Megabytes per second (MBps)

Parameter	Description
Port or range	You can assign the filter to a single port (like port "20") or a range of ports (such as "20-40") for TCP or UDP protocols
Protocol	Protocol Type • IPV4 or ARP using Data Type = ETHER • IPV4, TCP, UDP or ICMP using Data Type = IP

NFC Keyboard emulation

When enabled, reading a code via the NFC interface is handled by the BSP, simulating the acquisition of the UID code as if it were coming from a keyboard.

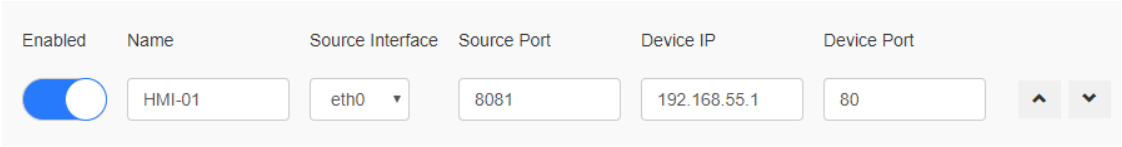
Reserved CPU cores for applications

By default, all CPU cores are used by the BSP. From this section, you can select the CPU cores that should not be used by the BSP to leave them reserved for user applications.

Router / NAT / Port Forwarding

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

Port Forwarding Rules

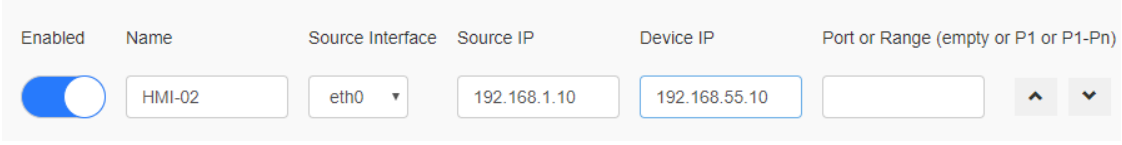


Available from BSP v1.0.507

1:1 NAT Rules

1:1 NAT, create alias IP on WLAN and forward all packets (or given port range) with that destination IP to another device attached to a LAN

Available from BSP v1.0.507



> Warning: make sure the value entered for “Source IP” is not the same as real IP address assigned to the physical Ethernet port specified as “Source Interface”.

DNS Relay Proxy

The DNS Relay Proxy will forward DNS requests and response packets between DNS Client and DNS Server.

When enabled, the HMI device will forward DNS requests received from other devices (DNS clients) to the DNS server (configured within the network section) and return the replay to the DNS client that made the request.

> Available from BSP v1.3.567

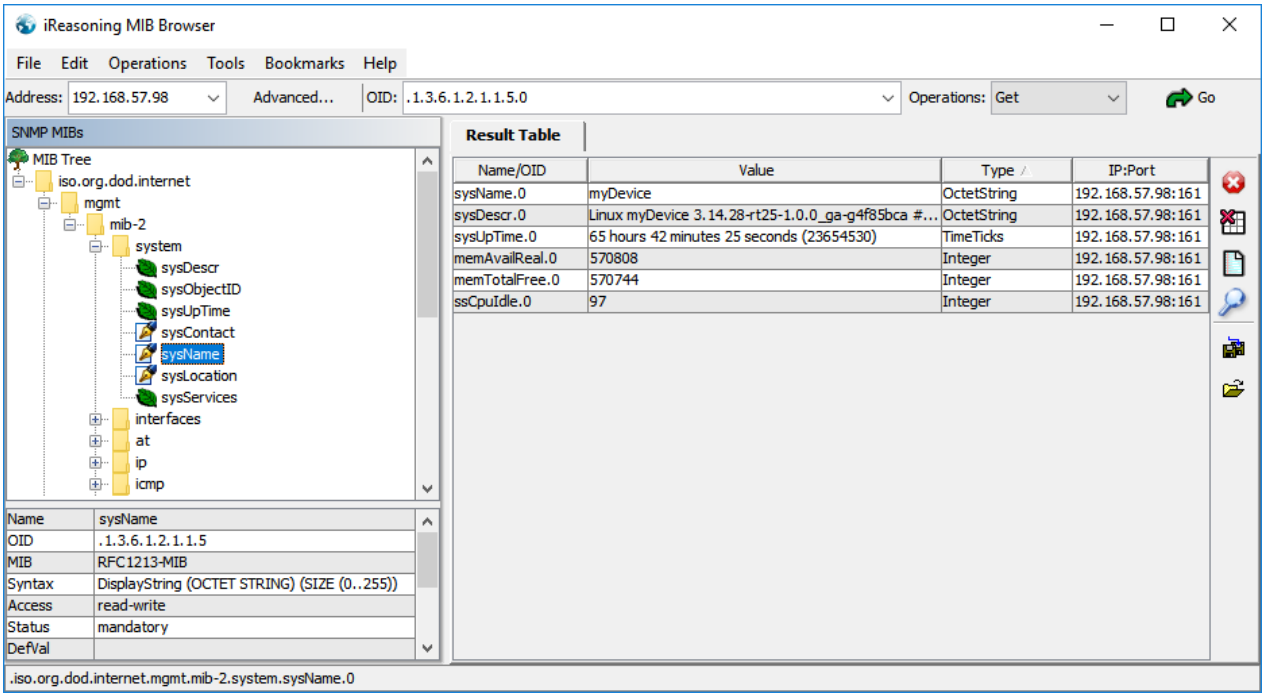
Show loading bar during boot

Enable/Disable the display of the loading bar during the boot phase.

SNMP Server

SNMP is a network protocol that allow to manage network infrastructures. It is commonly used to monitor network devices as switches, routers, etc. connected to a LAN network.

When the SNMP service is enabled, an SNMP Manager can retrieve information from the HMI device using the SNMP protocol. Currently, there are not proprietary MIBs available. Only the standard public community MIBs are available in read only mode.



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 RAM Free:	.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

> For security reasons, do not enable the service if you do not need it.

SSH Server

SSH service provides remote login to HMI device using the secure shell protocol. On PC you can run a SSH Client as, for example, PuTTY that is an open source software distributed under the MIT license.

- SSH server runs on TCP port 22.
- SSH access is restricted to the "admin" user only.

Parameter	Description
Enable	Enable the SSH server
Autostart	Keep the SHH server enabled when HMI device starts
Inactivity Timeout (seconds)	Duration of inactivity before session timeout

> This service is designed to be used during the development phase. For security reasons, remember to disable the service before switch to production.

VNC Service

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

Parameter	Description
Enable	Enable the VNC server
Autostart *	Keep the VNC server enabled when HMI device starts
Port	VNC Server listens for connections on TCP port 5900 (default)
Inactivity timeout (seconds) *	“Inactivity timeout” occurs if no user interaction is detected (via keyboard, mouse, transfers or other RFB protocol interactions). The special value 0 indicates that idle timeout is disabled. Default value is 600 (10 minutes).

Parameter	Description
Multiple clients *	Allow multiple sessions on the same port (if disabled, previously logged clients are disconnected upon a new incoming connection)
View only *	Do not allow active user interactions (clients can only watch)
Encryption *	Activate SSL encryption of connections **Custom certificate (Security/VNC KeyPair)** The HMI device certificate that is necessary to permit the remote VNC client to verify the authenticity of the HMI device. The certificate must contain both the private and the public keys and can be .pem format. The encryption features are not widely supported, check your VNC client compatibility
Authentication	Whether users are authenticated upon session creation. A custom VNC specific password can be set or system passwords can be used (this option is only available if also Encryption is enabled)

* Not available in Wayland BSPs (v2.x, v4.x)

Example of how to generate a certificate using 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 Create the certificate keys
%OpenSSL% req -x509 -newkey rsa -days 365 -nodes -keyout private.pem -out public.pem -
subj "/ST=NY/C=US/L=New York/O=CompanyName/OU=Department/CN=%CertificateName%" -addext
"subjectAltName=IP:%DeviceIP%"

rem Create .pem file
copy private.pem + public.pem hmi-certificate.pem

echo.
echo.
pause
```

This service is designed to be used during the development phase. For security reasons, remember to disable the service before switch to production.

Web Server

This page will show the parameters available to configure the Web Server. Note that it is not possible to disable the Web Server because it is necessary to allow access to the System Settings of the device.

- Allow only Secure HTTPS connections

  Disabled by default to maintain backward compatibility, but it is recommended to enable it to improve the HMI device security.

- CORS domains enabled

  When disabled (default), access from external domains is not allowed. When enabled, access from external domains listed in the "CORS domains filter" is allowed.

- CORS domains filter

  You can enter the domain to which access is allowed or use a regular expression to define multiple domains. The regular expression must have the prefix "re:".

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

  Examples of "CORS domains filter":

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

Authentication

Authentication is required to access system settings and manage HMI device service configuration.

The 'admin' user is a preconfigured account with full administrative privileges on the HMI device. Upon initial login or after a system reset, you will be prompted to set a new password.

> The first time the HMI device is turned on it is necessary to enter with the user "**admin**" and password "**admin**" to proceed with the definition of the passwords.

Password policy

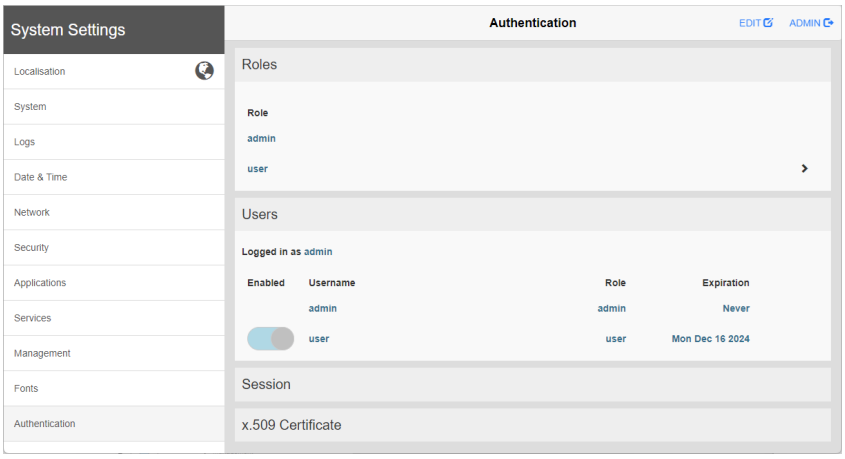
It is possible to define a custom policy for the required password format.

> By default, passwords must be at least 8 characters long and contain at least one lowercase letter, one uppercase letter, one number, and one special character.

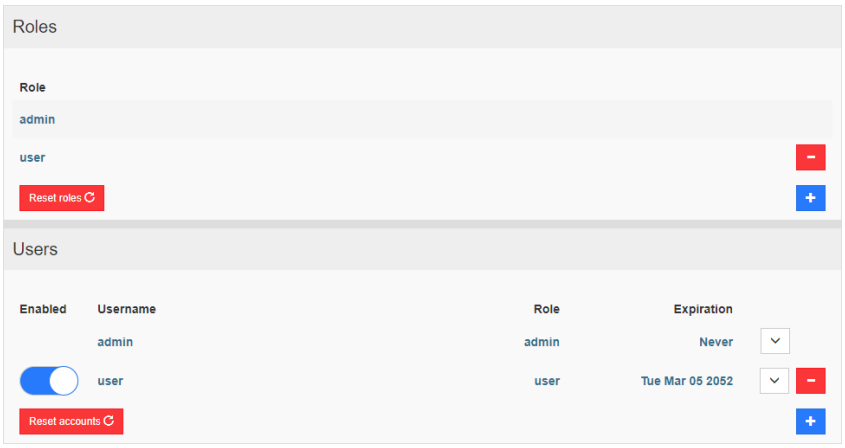
Users and Roles

The 'admin' user can create additional users and define their roles, assigning specific access permissions.

> It is possible to create a maximum of 50 users and 30 roles.



Upon clicking the "EDIT" button, it becomes possible to add or remove roles and accounts.



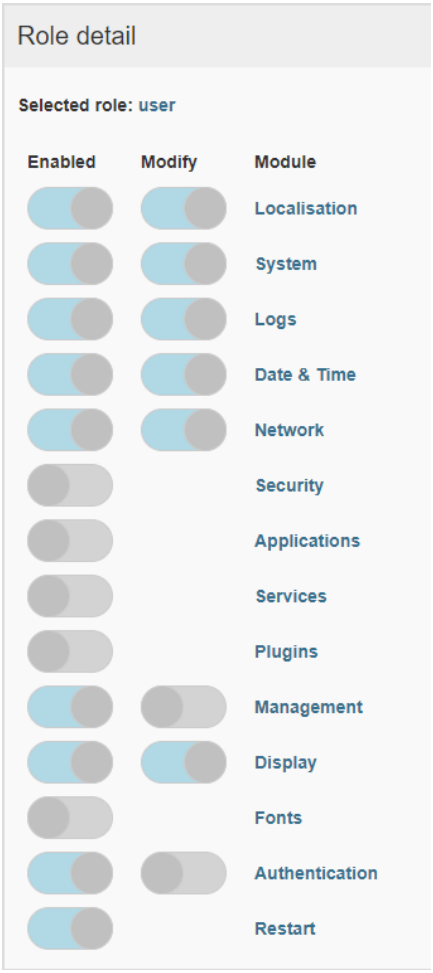
Clicking 'Reset Roles' will delete all existing roles. Please ensure that no roles are currently assigned to any users.

Clicking 'Reset Accounts' will delete all existing accounts.

Roles

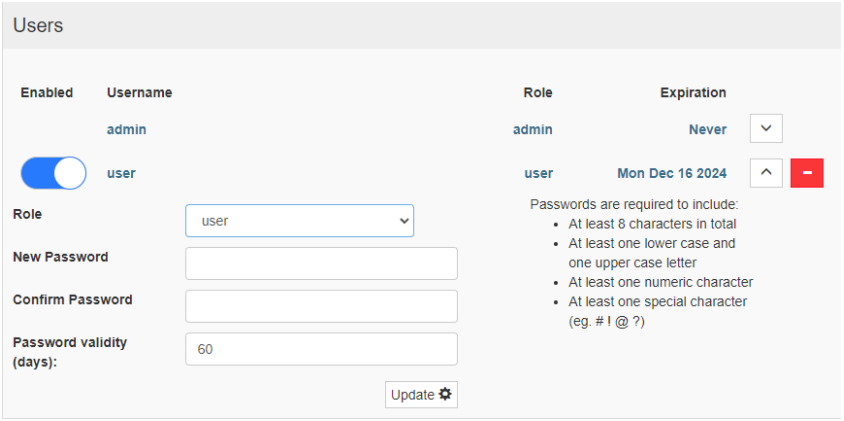
Click the "EDIT" button to add or remove a role, or click the role (">") to open the role definition.

For each feature, it is possible to define whether it is enabled and if it will be modifiable or read-only (disabled features will not be visible).



Users

Click the "EDIT" button to manage users.



Parameter	Description
Enabled	Button to keep user account enabled or disabled.
Role	Specify the user's permissions level.
New Password	Set a temporary password that the user will be forced to change on their first login.
Password validity	Duration in days for which the password remains valid, after which the user is required to change it. Leave empty for no expiration.

In order to make changes to a user's settings, you will need to input the specific values you wish to alter and then click on the "Update" button. A pop-up window will appear, requesting that you verify your identity by entering your password.

Session

The following parameters are useful for strengthening the defense against potential cyber threats, such as brute-force attacks aimed at guessing account passwords.

Parameter	Description
Inactivity Timeout (minutes)	Amount of time a user can be inactive before the session expires and closes.
Session Timeout (minutes)	Maximum allowed duration for a work session, after which the user will be prompted to re-authenticate.
Max user login attempts	The maximum number of failed login attempts from a single user within a one-minute, one-hour, or one-day window. Upon exceeding this limit, the user will be locked out..
Max host login attempts	The maximum number of failed login attempts from multiple users within a one-minute, one-hour, or one-day window. Upon exceeding this limit, the user will be locked out.

A blocked account will be unlocked:

- Upon expiration of the time limit
- Upon device reset

x.509 Certificate

HMI Device use a self-certificate to encrypt the Internet communication trough the HTTPS protocol. You can personalize the certificate with the data of your Company and ask to a Certificate Authority to firm it.

The procedure to personalize and firm your certificate is:

1. Enter in edit mode and fill the necessary parameters, then push GENERATE button to generate a self-signed certificate with your data.
2. Export the “Certificate Signed Request”
3. Sent the “Certificate Signed Request” to a Certificate Authority to firm it (general this is a paid service)
4. Import the signed certificate into the HMI device

Certificate's parameters

Parameter	Description
Device Name	The name of your device
Organization	The legal name of your organization
Unit	The division of your organization handling the certificate
State	The state/region where your organization is located
Location	The city where your organization is located
Country	The two-letter ISO code for the country where your organization is location
Valid (days)	Validity of the certificate
Key Length	Number of bits of the key used from the cryptographic algorithm

Managed certificates are base64 encoding.

Forgot password

If all administrators forget their passwords, access to the device's configuration will be permanently lost. To restore functionality, a factory reset will be required. This process will completely erase all user-stored data, settings, and applications. See: "Factory Reset" on page 52

Cloud / VPN Service

Cloud / VPN Service allows devices to connect to remote servers through a secure connection.

> BSP v1.0.117 or greater is required

Prerequisites

This service requires external access to the server for VPN setup (default port UDP/1194) and for self-configuration/other advanced features on TCP port 443 (Cloud Server mode only), so please check configuration and make sure no firewalls block such ports.

Setup

If you need endpoints behind your gateway device to be reached, make sure Router Service is active and set it up as follows:

- WAN port (eth0) connected to the main network with Internet access (Cloud Server must be reachable from this network)
- LAN port (eth1) connected to one or more endpoint devices (newly-created private network)

This functionality is automatically supported when using a Cloud Server, but will require extra manual setup for plain OpenVPN server.

Configuration

Configuration options are available in the Services Menu of System Settings (see "System Settings" on page 16).

In case of connectivity error, from the BSP v1.0.348 and later the retry timeout has a geometric progression: starting from 5s, the successive retry is after 2*(Previous Time). This means 5s, 10s, 20s, 40s, etc. until a max retry time of 5 minutes. On previous BSP versions, the retry times was fixed to 5 Seconds.

Parameter	Description
Enable	Enable the Cloud / VPN Service
Autostart	If selected, the application will start when the HMI device is turned on
Server type	Select, from the available supported server types, the server type to use
Server	Select the Corvina server to use (available only when the selected server type is "Cloud Server")
Files	Allows you to upload VPN configuration files (available only when the selected server type is "OpenVPN")
Authentication	Select from the available authentication modes • Username/ password • Activation code (available only when the selected server type is "Cloud Server") • Certificate (available only when the selected server type is "OpenVPN") • Certificate + username/ password (available only when the selected server type is "OpenVPN") • None (available only when the selected server type is "OpenVPN")
Username	Enter the username of the remote server account
Password	Enter the password of the remote server account
Show Password	Displays the typed characters on the password

Cloud Server

Cloud Server is a VPN-based solution that allows seamless connection of users with gateways and endpoints. It provides a full management infrastructure to make such process painfree.

Configuration is downloaded automatically from Cloud Server, so the only required parameters are Server (hostname or IP address), Username and Password.

Error list

Error	Note
System Error - please check resource status	Unpacking downloaded configuration package error
Generic Error	Generic Error
Configuration missing	Downloaded configuration package is empty
Please check credentials	Authentication data error, not present, invalid
Request timed out	An API request has not received a response, generic error
Invalid activation code	Error from Corvina
Activation code not registered	Error from Corvina
Local Encloud Service Unreachable	Local service on BSP not active
Server Unreachable	Server not reachable
Failed verifying Server - check CA certificate	Invalid certificate
Generic Server Error	Generic error from Server
Server reported Invalid License	Error from Corvina
Server reported content not found	Error from Corvina
Server Authentication Failure - please check credentials	Invalid credentials
Server Authentication Failure - user already connected	The user is valid but is already connected
Proxy Authentication Failure - please check credentials	The proxy responded with an error to the authentication request
Server Authentication Failure - organization required	The mandatory organization field was not entered
Configuration download failed - Please check that your license is valid and credits assigned	Unable to download the configuration
VPN Client Failure	VPN client generic error
VPN Client Timeout	The VPN client (openVPN) is not responding
Bad Client Configuration	The VPN client (openVPN) does not have a valid configuration

OpenVPN

This mode uses a standard OpenVPN configuration to connect devices.

Case A: Configuration files provided

In remote access environments based on an OpenVPN server, system administrators normally supply a number of OpenVPN configuration files directly to end users.

In such case configuration is quite straight-forward since it requires only two simple steps:

1. browse and upload N files (this should include at least a main OpenVPN configuration file, but may also include server and/or client certificates in .pem, .p12 or other formats); make sure you select all necessary files in one shot by using platform-dependent multiselection;
2. select an appropriate Authentication type and insert credentials if they are required.

You're done! now press Save, wait a little while and you should see an updated connection status.

Case B: No configuration files provided

If no configuration files have been provided by your system administrator, you will need to create the OpenVPN configuration file yourself.

Sample 1: Username/Password

This sample uses:

- username/passsword-based authenticaition
- LZO compression and TAP device
- server running 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 one external file (*cacert.pem*), so:

1. upload the 2 files using the Browse option
2. insert your allocated Username and Password - note that the *auth-user-pass* option can also take a file argument, so you can even insert newline-separated username and password in a new file and specify its name here (not recommended); in such case you would select also your external file when browsing files and choose *None (from file)* Authentication method
3. *Save* and wait for State change

Sample 2: Plain certificate

This sample uses:

- plain X509 certificate-based authentation
- LZO compression, TUN device, custom MTU and AES-128-CBC cipher
- server running 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 refers to 3 files (*cacert.pem*, *client.pem*, *client.key*), so:

1. upload main *openvpn.conf* and external files (total 4), using the Browse option
2. since no passwords are required, choose *None (from file)* Authentication
3. *Save* and wait for State change

Sample 3: Password-protected PKCS #12 certificate

This sample uses:

- certificate-based authentation (password-protected PKCS #12)
- other parameters same as Sample 2

openvpn.conf

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

The PKCS #12 bundle normally contains both CA certificate client keypair, so this configuration file only refers to one external file (*mycert.p12*). Hence:

1. upload the 2 files using the Browse option
2. choose *Certificate* Authentication
3. insert the password which should be used to unencrypt the PKCS #12 bundle containing your certificate
4. *Save* and wait for State change

Sample 4: 2-factor authentication via password-protected PKCS #12 certificate + username/password

This sample uses:

- both certificate-based authentication (password-protected PKCS #12) and username/password
- other parameters same as Sample 2

openvpn.conf

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

upload the 2 files using the Browse option

choose *Certificate + Username/Password* Authentication

insert *Username* and *Password* for PSK authentication

insert the *PKCS #12 Password*

Save and wait for State change

Links

Please refer to openvpn.net for further details.

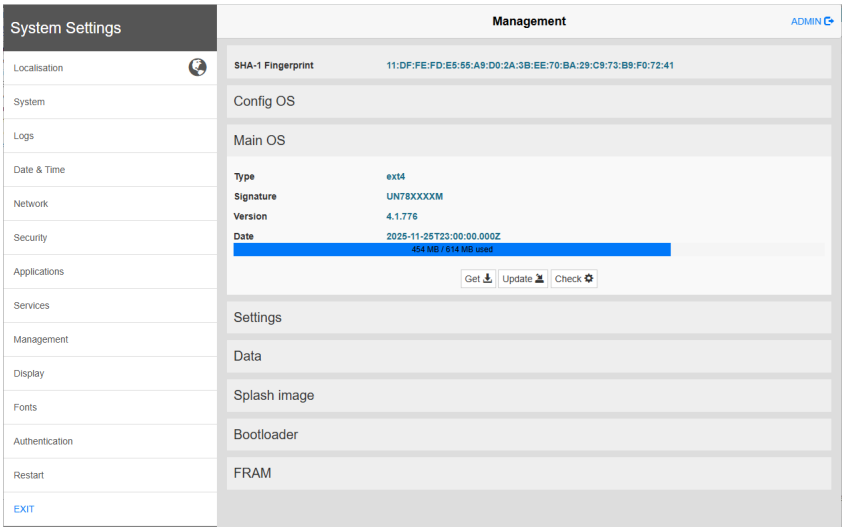
Update System Components

CAUTION: Working in the Management area is a critical operation and, when not performed correctly, may cause product damages requiring service of the product. Contact technical support for assistance (the latest BSP files will provided from tech support).

The system components of the Linux device can update locally using an USB memory key or remotely via web browser.

To update system components enter System Settings in Config OS mode (or Recovery Mode) via tap-tap procedure on HMI or open web browser to https://<HMI-IP-address>/machine_config and select the “Management” section.

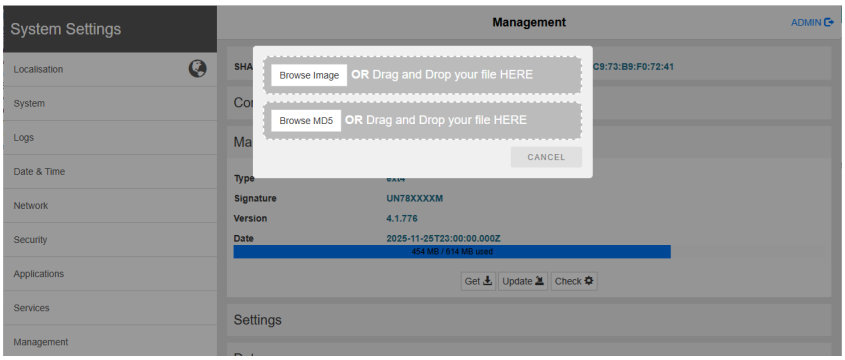
> To validate the integrity of the certificate included in the BSP, it is necessary to verify the fingerprint contained in the certificate and displayed in the first line of the management page by comparing it with the fingerprint published by DEIF A/S (ref.: "Manufacturer's certificate" on page 15).



> The 'Config OS' section is not available in BSPs with the 'A/B MainOS' architecture.

Expand the component to update and select [Update]

In the opened dialog box, click [Browse Image], then select the component file to be updated. Then click on [Browse MD5] and select its md5 file.



Important: Do not turn off the device while a system component is being upgraded.

At the end of the component update, restart HMI and leave it starting normally.

FRAM

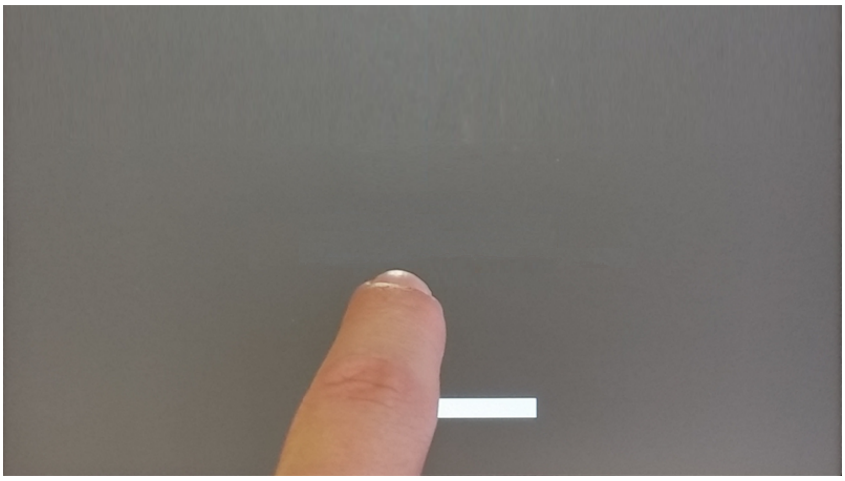
When available on the HMI device, you can "Get" or "Update" the FRAM data. To transfer FRAM data, the HMI device must be in OS Config mode, otherwise, the transfer will not take place.

> BSP v1.3.786 or v2.0.786 or v2.1.67 or v3.1.67 or greater is required to transfer FRAM

Enter System Settings in Config OS mode (or Recovery Mode) via tap-tap procedure

System Setting in Config OS mode (or Recovery Mode) is available via tap-tap sequence, this mode can be accessed also when HMI is facing a software failure.

Tap-tap consist in a sequence of several touch activations by simple means of the finger tapping the touch screen performed during the power-up phase and started immediately after the HMI is powered on.



When “tap-tap detected” message appears on the top of the screen, press and hold the finger on touchscreen, to select “Restart: Config OS” (or "Restart: Recovery Mode")



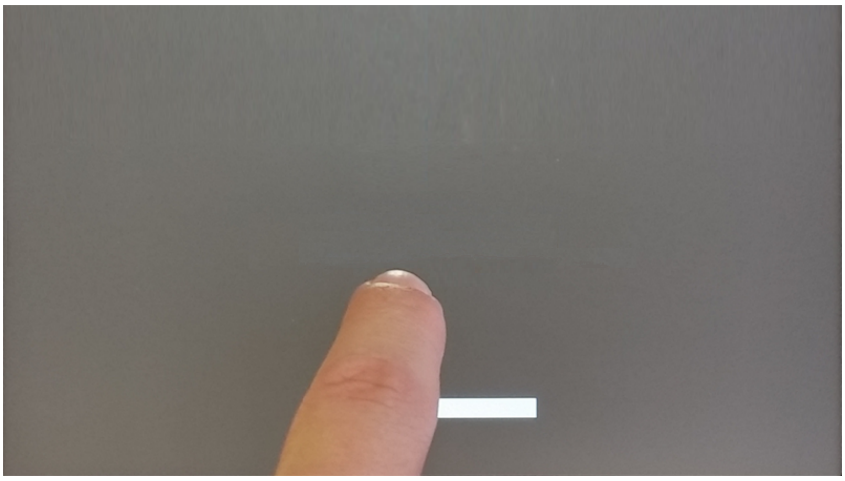
HMI will restart into System Settings in Config OS mode (or Recovery Mode):



Touchscreen calibration

System Setting Calibration allows to calibrate Touchscreen device, can be accessed by tap-tap procedure (available only for resistive type displays).

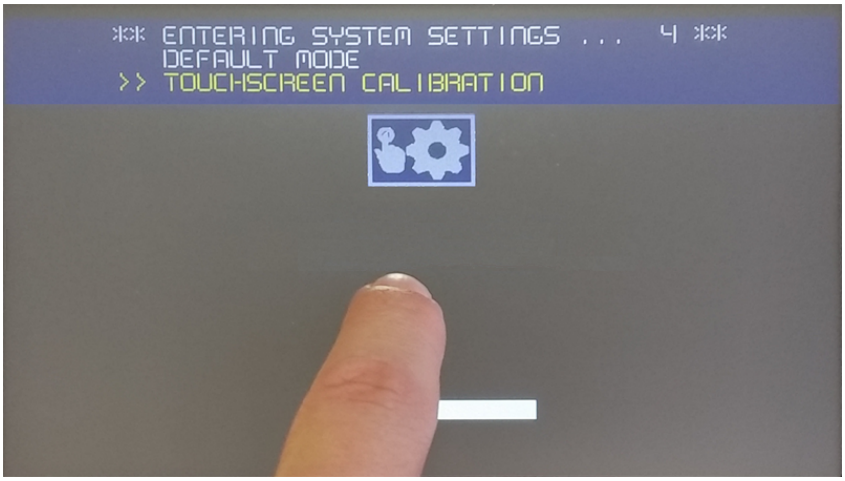
Tap-tap consists in a sequence of several touch activations by simple means of the finger tapping the touch screen performed during the power-up phase and started immediately after the HMI is powered on.



When “tap-tap detected” message appears on the top of the screen, wait for 5 seconds (without touching the screen) to enter System Settings sub menu



Press on touch screen, “Touchscreen calibration” voice will be highlighted in yellow, hold pressed for few seconds until touchscreen calibration procedure starts



Follow the instructions on screen to complete the calibration procedure, system will prompt to touch specific points to calibrate the touchscreen device.

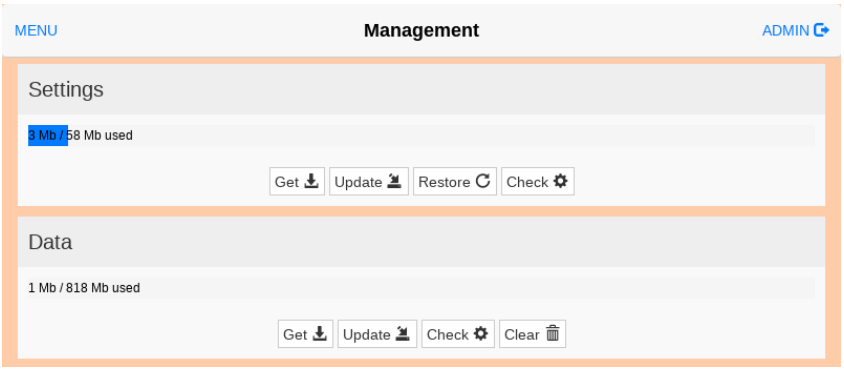
Backup and Restore

To backup or restore all the installed applications with their settings, you must open the System Settings interface in Config OS mode using the TAP TAP procedure.

See "System Settings access via TAP TAP procedure " on page 18

Then log as admin and select the "Management" option. From this page, you can use the "Get" button to backup inside an external memory (e.g. USB key) the contents of the **Data** and the **Settings** partitions. Use instead the "Update" button to restore the contents from a previous backup.

> Management command is available only when logged as admin.



Data Partition

The data partition contains the applications and they settings

Settings Partition

The settings partition contains the settings of your device (this means the configuration parameters entered using the System Settings interface)

> When you update the System Settings from a backup you must be sure that the backup was executed from a device with the same BSP version (Main OS).

The MD5 file

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

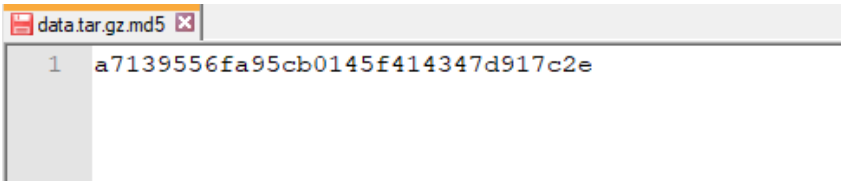
The MD5 checksum file must have the same name as the files that you want to load with the .md5 suffix as e.g.:

- data.tar.gz
- data.tar.gz.md5

On the Internet, it is easy to find various tools that calculate the MD5 checksum of a file. On 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 must have only one line. If the utility that calculates the checkum generates a file with multiple lines, the additional lines must be deleted.



Recovery Mode

If the device fails to boot correctly, a special procedure is available to restore it by entering a recovery mode. From this mode, you can open the device management dialog to delete user data, restore system settings, or update the device's firmware.

To boot the device in recovery mode choice one of the below procedures:

- Power on the device and immediately power off when splash screen appear on the screen (if you cannot see the splash screen, power off the device when you heart the beep-beep). Repeat this procedure for three times then power on again the device and wait the configuration mode appears.
- Create a special file named “$0030D8$.bin” and put it inside an empty SD card. Insert the SD card into the device and power on the device. Device will start in configuration mode.

Factory Reset

Factory reset is a process that restores the HMI device to its original state, as if it were just unboxed. This process will completely erase all user-stored data, settings, and applications. Once the factory reset is complete, the administrator password will automatically be reset to its original default value, "admin".

TAP TAP option

> The procedure is available only if it has not been explicitly disabled through the "Enable device restore via TAP TAP option" available in the device system settings (Ref.: "Enable device restore via TAP TAP option" on page 30)

Steps to reset the admin password:

1. Power off the HMI device.
2. Power on the HMI device and when the logo appears start to "tap tap" the touch panel (Ref.: "System Settings access via TAP TAP procedure " on page 18).
3. When "TAP TAP" is detected select "System Settings" on the first menu, "Default mode" on the second menu, and finally "**Device restore**" on the third menu.

USB option

> The procedure is available only if it has not been explicitly disabled through the "Enable device restore via USB option" available in the device system settings (Ref.: "Enable device restore via USB" on page 31)

Steps to reset the admin password:

1. Placing a file named “*device-factory-restore*“ into a USB stick and plugging it into the device.
2. The device restore process starts automatically. The buzzer is played once at the beginning and 3 times at the end if the operation is successful.
3. The “*device-factory-restore*“ is deleted from the USB stick and the device rebooted.

Plugin modules

Several optional plugin modules are available that can be used to extend the features of the HMI device.

> It's recommended that you check the datasheet for your specific HMI device to see which plugins are supported.

PLCM09 Plugin Wireless Modem

The PLCM09 is an optional module that adds the ability to communicate with all machines and systems worldwide.

> Available only Linux HMI Devices

PLCM09 provide:

- Wireless modem with a Micro-SIM slot
- 4 LED indicators (2 user programmable, Modem Status, Network Status)
- 2 Digital Inputs
- 2 Digital Output

> BSP v1.0.364 or greater is required

Mobile Network

Behavior of the wireless modem can be configured from the HMI device System Setting tool:

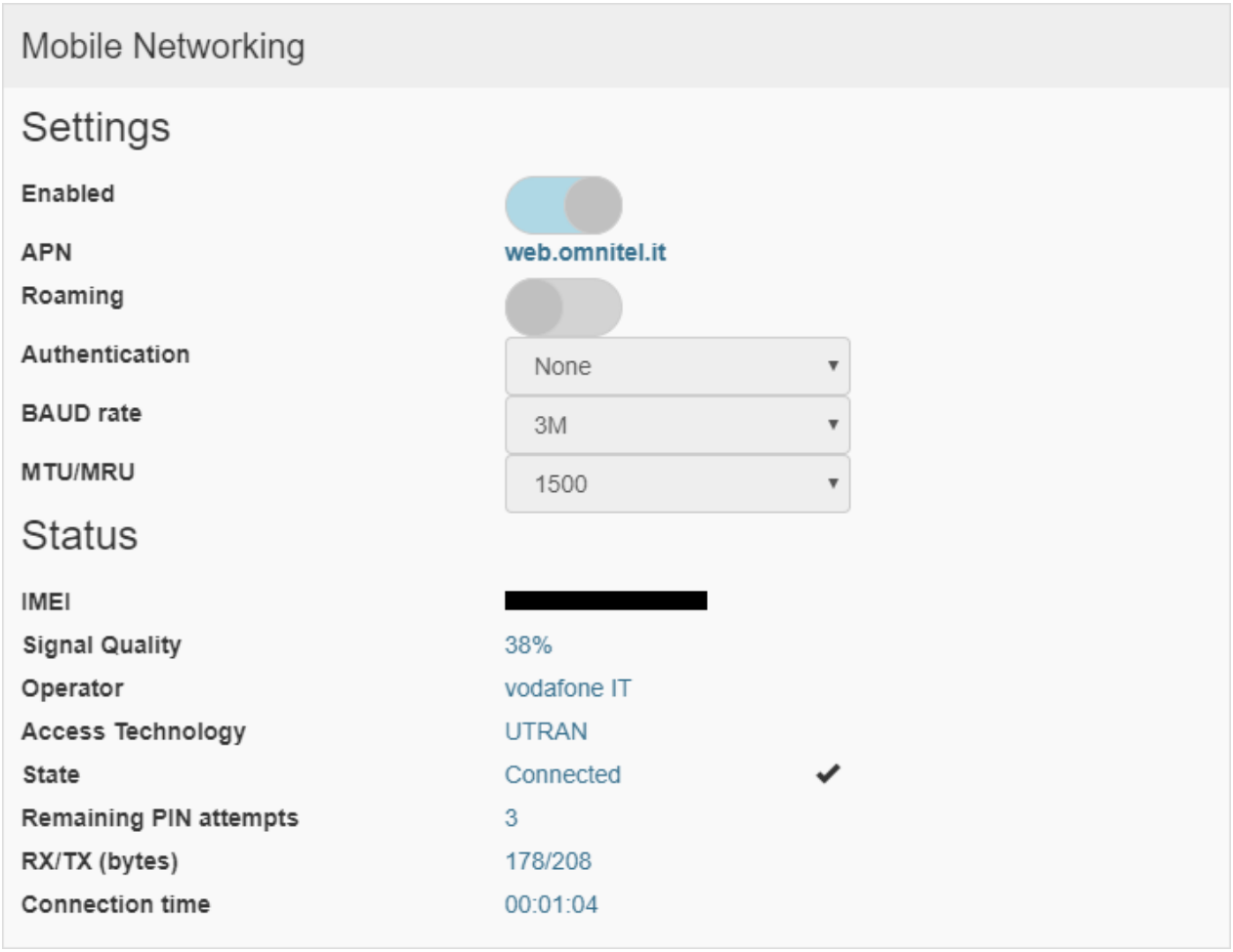
System Settings -> Network -> Mobile Network

> The Mobile Network section is available only when the optional PLCM09 module is plugged to the HMI device

Parameter	Description
Enabled	Enable the Wireless Modem
SIM PIN	SIM Card PIN code if required
APN	APN (Access Port Name) If you do not know this information please contact your mobile services provider.
Roaming	Enable Roaming option if required
Authentication	Authentication mode: • None • PAP (Password Authentication Protocol)
BAUD rate	Baudrate: • 900K

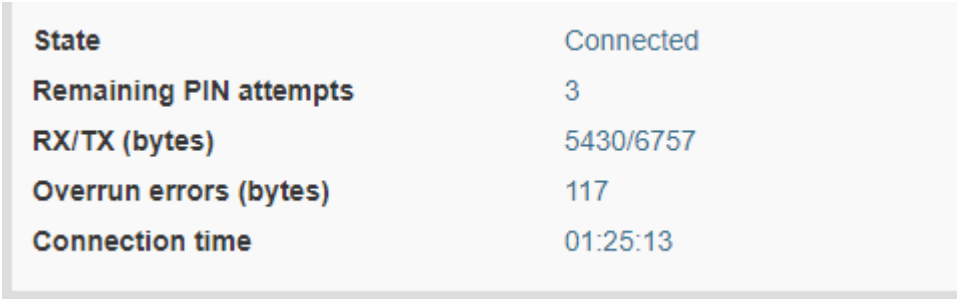
Parameter	Description
	• 3M (default) BSP v1.0.413 or greater is required
MTU/MRU	Max Packets Size: • 1500 • 512 • 256 • 128 BSP v1.0.413 or greater is required
Username **Password**	Username and password to be used when the authentication mode is selected

Once you have confirmed the system setting, you will find detailed information about your SIM card and mobile network connection in the Status area.



Overrun Errors

The "Overrun Errors" is a read-only parameter that is shown inside the status area only in the case of bad communication with the internal modem. In this case is advisable a review of the modem's communication parameters (Baudrate, MTU/MRU)



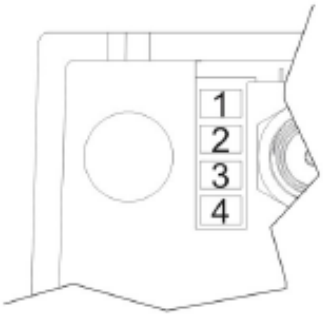
LEDs and Digital I/O

Behavior of the first two available LEDs and of the Digital I/O can be configured from the HMI device System Setting tool:

System Settings -> Plugins -> PLCM09

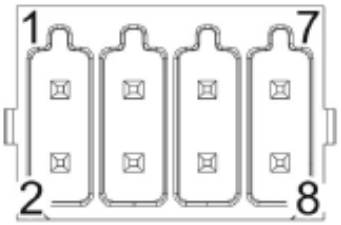
Digital I/O	Description
Input-1 **Input-2**	User configurable: • None • Cloud: 0=down, 1=up When the input signal is on, HMI device will connect to remote cloud. When it is off, the remote cloud will be disconnected. • Mobile: 0=down, 1=up When the input signal is on, HMI device will start the wireless modem. When it is off, the wireless modem will be disconnected. • 1=system reboot When the input signal is detect to be 1, HMI device will force a reboot
Output-1 **Output-2**	User configurable: • None (not used) • User controlled Output signal will be managed by the HMI application • Cloud: down=0, up=1 Output will be set to 1 when cloud connection is active, 0 when not active • Mobile: down=0, up=1 Output will be set to 1 when wireless modem connection is active, 0 when not active

LED	Description
LED #1 **LED #2**	User configurable: • None (not used) • User controlled LED status will be managed by the HMI application • Cloud: down=off, up=on, error=blink Show the cloud connection status • Mobile: down=off, up=on, error=blink Show the mobile connection status
LED #3	Show the wireless modem status: • OFF = Disabled • ON = Enabled
LED #4	Show the network activity (blinking)



LED	Specifications
1	User configurable
2	User configurable
3	Modem status ON/OFF
4	Netlight (network status indication LED)

Pin	Description	Pin	Description
1	OUT 1A	5	IN 1+
2	OUT 1B	6	IN 1-
3	OUT 2A	7	IN 2+
4	OUT 2B	8	IN 2-



PLCM10 Plugin Wireless Modem

The PLCM10 is an optional module that adds the ability to communicate with all machines and systems worldwide.

When the PLCM10 module is plugged and recognized, its properties will become available as “System Settings”

Warning

- Available only on Linux HMI devices that support plug-in modules
- Only one PLCM10 module per device is supported
- PLCM10 module is not supported when a WiFi dongle is already plugin in the HMI device

PLCM10 may be available with different configurations. Make sure what are the functions supported in the device you are using.

PLCM10 provide:

- 4G/LTE wireless modem with Micro-SIM slot
- WiFi connection (only for devices with USB support in plug-in connectors)
- GNSS service (only for devices with USB support in plug-in connectors)
- 4 LED indicators (2 user programmable, Modem Status, Network Status)
- 2 Digital Inputs
- 2 Digital Output

Software requirements:

- On BSP v1.0 the version 1.0.721 or higher is required
- On BSP v1.3 the version 1.3.483 or higher is required

PLCM10B provide:

- 4G/LTE wireless modem with Micro-SIM slot
- 4 LED indicators (2 user programmable, Modem Status, Network Status)
- 2 Digital Inputs
- 2 Digital Output

Software requirements:

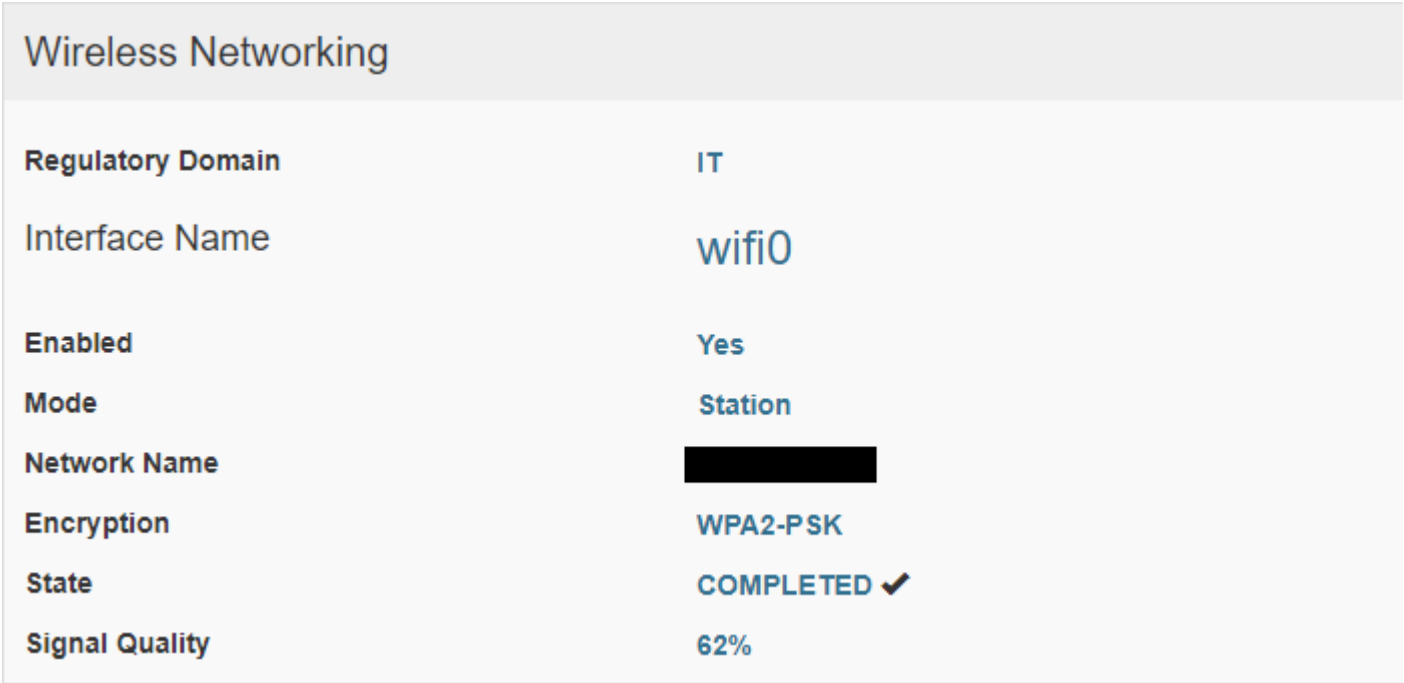
- On BSP v1.0 the version 1.0.821 or higher is required
- On BSP v1.3 the version 1.3.712 or higher is required

Wireless Network

System Settings -> Network -> Wireless Network

Parameter	Description
Regulator Domain	It is read-only information that can be set on the localisation page
Interface Name	Interface name (read-only)
Enable	Enable operation of Wireless Network
Mode	Select: • Station • Access Point
Network Name	This is the network identifier (the SSID) When Mode = Station a "Browser" button will appear, to list the available wifi networks. When Mode = Access Point you have to define the SSID of the network you are creating.
Encryption	The WPS-PSK encryption mode is supported
Password	Available only when the Encryption=WPS-PSK is selected.

Once you have confirmed the system setting, you will find the connection State and the Signal Quality information.

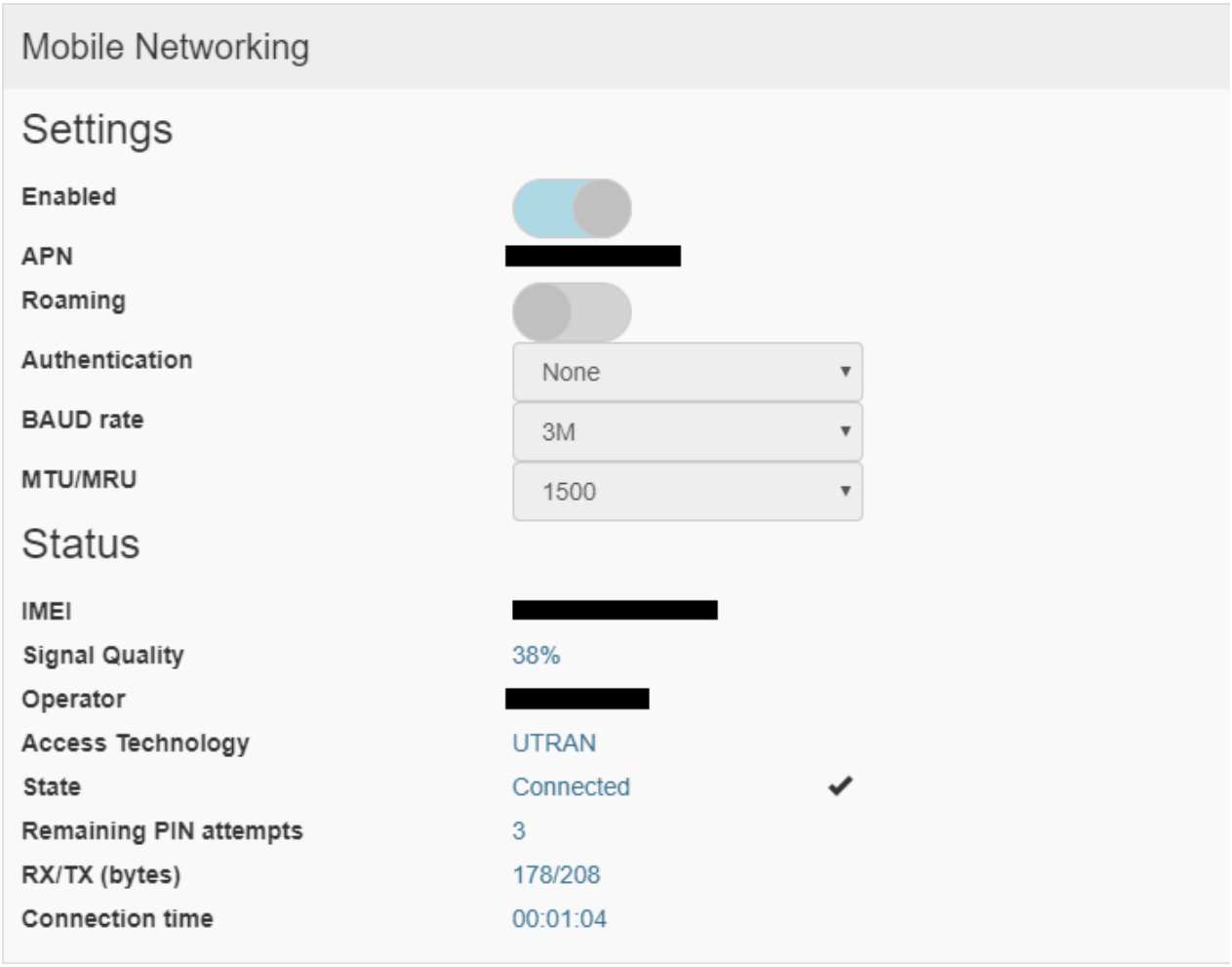


Mobile Network

System Settings -> Network -> Mobile Network

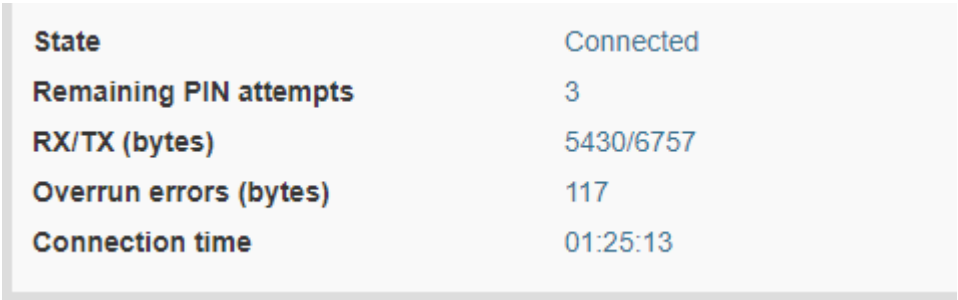
Parameter	Description
Enabled	Enable the Wireless Modem
SIM PIN	SIM Card PIN code if required
APN	APN (Access Port Name) If you do not know this information please contact your mobile services provider.
Roaming	Enable Roaming option if required
Authentication	Authentication mode: • None • PAP (Password Authentication Protocol)
BAUD rate	Baudrate (only for the HMI devices that supports plug-in via serial port): • 900K • 3M (default)
MTU/MRU	Max Packet Size: • 1500 • 512 • 256 • 128
Username **Password**	Username and password to be used when the authentication mode is selected

Once you have confirmed the system setting, you will find detailed information about your SIM card and mobile network connection in the Status area.



Overrun Errors

The "Overrun Errors" is a read-only parameter that is shown inside the status area only in the case of bad communication with the internal modem. In this case is advisable a review of the modem's communication parameters (Baudrate, MTU/MRU)



GNSS

System Settings -> Network -> GNSS

Parameter	Description
Enabled	Enable the GNSS module Mobile Network must be enabled

Once you have confirmed the system setting, you will find detailed information about the GNSS status value



Status Value	Description
NMEA Service	Enabled = the GNSS signal is present
Satellites	Number of locked satellites
State	FIX = last GNSS sentence is valid
Date and Time **Longitude** **Latitude** **Altitude (m)** **Speed (m/s)**	Values received from the GNSS

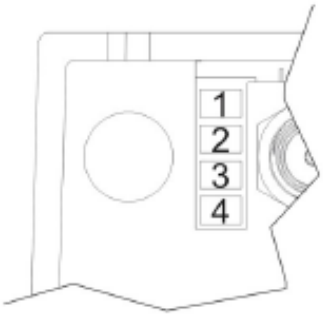
LEDs and Digital I/O

Behavior of the first two available LEDs and of the Digital I/O can be configured from the HMI device System Setting tool:

System Settings -> Plugins -> PLCM10

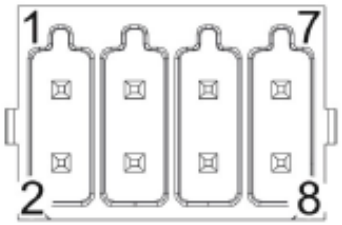
Digital I/O	Description
Input-1 **Input-2**	User configurable: • None • Cloud: 0=down, 1=up When the input signal is on, HMI device will connect to remote cloud. When it is off, the remote cloud will be disconnected. • Mobile: 0=down, 1=up When the input signal is on, HMI device will start the wireless modem. When it is off, the wireless modem will be disconnected. • 1=system reboot When the input signal is detect to be 1, HMI device will force a reboot
Output-1 **Output-2**	User configurable: • None (not used) • User controlled Output signal will be managed by the HMI application • Cloud: down=0, up=1 Output will be set to 1 when cloud connection is active, 0 when not active • Mobile: down=0, up=1 Output will be set to 1 when wireless modem connection is active, 0 when not active

LED	Description
LED #1 **LED #2**	User configurable: • None (not used) • User controlled LED status will be managed by the HMI application • Cloud: down=off, up=on, error=blink Show the cloud connection status • Mobile: down=off, up=on, error=blink Show the mobile connection status
LED #3	Show the wireless modem status: • OFF = Disabled • ON = Enabled
LED #4	Show the network activity (blinking)



LED	Specifications
1	User configurable
2	User configurable
3	Modem status ON/OFF
4	Netlight (network status indication LED)

Pin	Description	Pin	Description
1	OUT 1A	5	IN 1+
2	OUT 1B	6	IN 1-
3	OUT 2A	7	IN 2+
4	OUT 2B	8	IN 2-



MicroEdge Plug-In LTE/4G Wi-Fi

The MicroEdge Plug-In LTE/4G Wi-Fi is an optional module available for the MicroEdge device that adds the ability to communicate with all machines and systems worldwide.

When the MicroEdge Plug-In LTE/4G Wi-Fi module is plugged and recognized, its properties will become available as “System Settings”

Warning

- Only one MicroEdge Plug-In LTE/4G Wi-Fi module per device is supported

MicroEdge Plug-In LTE/4G Wi-Fi provide:

- 4G/LTE wireless modem with Micro-SIM slot
- WiFi connection (not available in all models)
- GNSS service
- 2 LED indicators (Modem Status, Network Status)
- 1 LED RGB
- 2 Digital Inputs
- 2 Digital Output

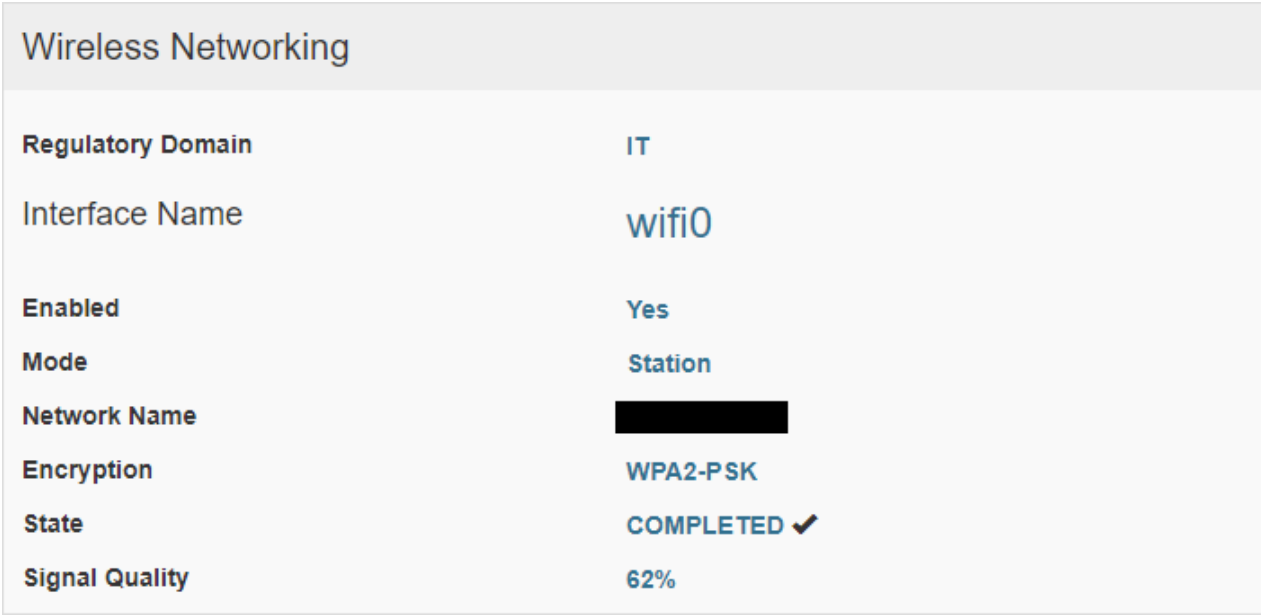
Wireless Network

System Settings -> Network -> Wireless Network

Parameter	Description
Regulator Domain	It is read-only information that can be set on the localisation page (See "Localisation" on page 19)
Interface Name	Interface name (read-only)
Enable	Enable operation of Wireless Network
Mode	Select: • Station • Access Point
Network Name	This is the network identifier (the SSID) When Mode = Station a "Browser" button will appear, to list the available wifi networks. When Mode = Access Point you have to define the SSID of the network you are creating.

Parameter	Description
Encryption	The WPS-PSK encryption mode is supported
Password	Available only when the Encryption=WPS-PSK is selected.

Once you have confirmed the system setting, you will find the connection State and the Signal Quality information.



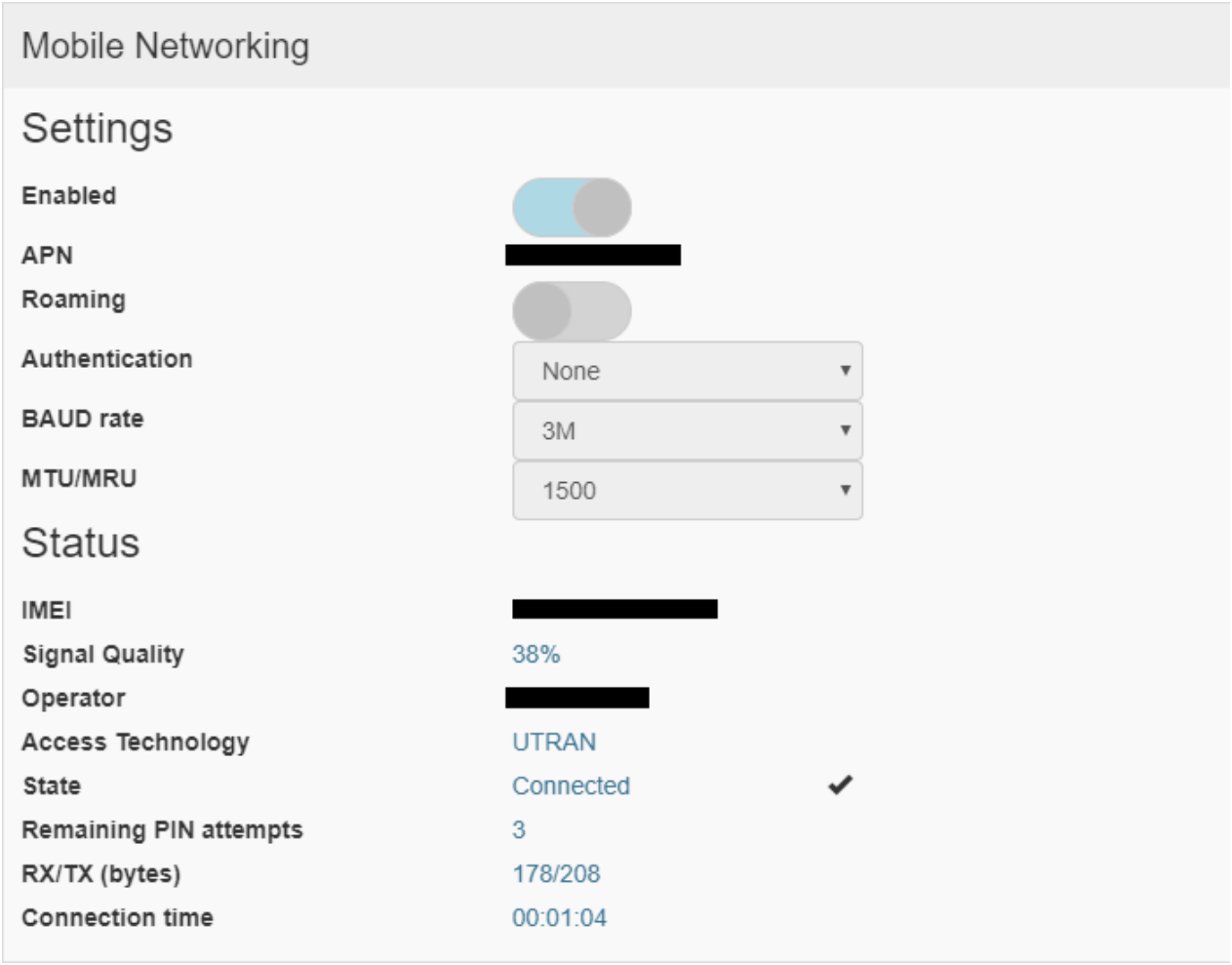
Mobile Network

System Settings -> Network -> Mobile Network

Parameter	Description
Enabled	Enable the Wireless Modem
SIM PIN	SIM Card PIN code if required
APN	APN (Access Port Name) If you do not know this information please contact your mobile services provider.
Roaming	Enable Roaming option if required
Authentication	Authentication mode: • None • PAP (Password Authentication Protocol)
BAUD rate	Baudrate (only for the HMI devices that supports plug-in via serial port): • 900K • 3M (default)

Parameter	Description
MTU/MRU	Max Packet Size: • 1500 • 512 • 256 • 128
Username **Password**	Username and password to be used when the authentication mode is selected

Once you have confirmed the system setting, you will find detailed information about your SIM card and mobile network connection in the Status area.



Overrun Errors

The "Overrun Errors" is a read-only parameter that is shown inside the status area only in the case of bad communication with the internal modem. In this case is advisable a review of the modem's communication parameters (Baudrate, MTU/MRU)

State	Connected
Remaining PIN attempts	3
RX/TX (bytes)	5430/6757
Overrun errors (bytes)	117
Connection time	01:25:13

GNSS

System Settings -> Network -> GNSS

Parameter	Description
Enabled	Enable the GNSS module Mobile Network must be enabled

Once you have confirmed the system setting, you will find detailed information about the GNSS status value



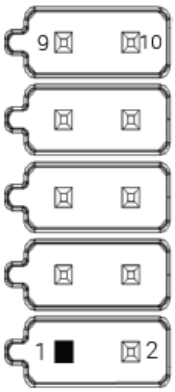
Status Value	Description
NMEA Service	Enabled = the GNSS signal is present
Satellites	Number of locked satellites
State	FIX = last GNSS sentence is valid
Date and Time **Longitude** **Latitude** **Altitude (m)** **Speed (m/s)**	Values received from the GNSS

LEDs and Digital I/O

Behavior of the Digital I/O can be configured from the HMI device System Setting tool:

System Settings -> Plugins -> "*PlugIn-ID*"

Digital I/O	Description
Input-1 **Input-2**	User configurable: • None • Cloud: 0=down, 1=up When the input signal is on, HMI device will connect to remote cloud. When it is off, the remote cloud will be disconnected. • Mobile: 0=down, 1=up When the input signal is on, HMI device will start the wireless modem. When it is off, the wireless modem will be disconnected. • 1=system reboot When the input signal is detect to be 1, HMI device will force a reboot
Output-1 **Output-2**	User configurable: • None (not used) • User controlled Output signal will be managed by the HMI application • Cloud: down=0, up=1 Output will be set to 1 when cloud connection is active, 0 when not active • Mobile: down=0, up=1 Output will be set to 1 when wireless modem connection is active, 0 when not active



Pinout I/O Port	
OUT 2A	OUT 2B
OUT 1A	OUT 1B
IN 2+	IN 2-
IN 1+	IN 1-

LED	Description
LED #1	Show the wireless modem status: • OFF = Disabled • ON = Enabled
LED #2	Show the network activity (blinking)

Cybersecurity Guide

This document provides the guidelines for correctly configuring the HMI device's functionality, making it as secure as possible from external Cyber Attacks.

> It is assumed that the most recent **v4.1** or **v5.1** versions have been installed on the HMI devices and that they are updated whenever a new version is made available on the manufacturer's website.

The **Software Bill of Materials (SBOM)** for the HMI device is accessible from the device System Settings page.

Operational States

The HMI device has three operating states:

- **Boot Mode**

  Upon power-on, essential services are started, and system components are loaded and initialized to enable the device's normal operations (Operating mode). During this phase, unless expressly disabled, the TAP TAP feature is available on the touchscreen to activate the device in Recovery Mode.

- **Operating Mode (mainOS)**

  In operating mode, the device is controlled by the loaded application (the user-level application that implements the functionality required by the end customer). If an application isn't present, or if its startup is disabled, the HMI device's "Launcher Screen" will be displayed. From this interface, you can install an application to run or configure system parameters.

- **Recovery Mode (configOS)**

  This operational state is dedicated to system recovery and machine configuration tasks. In this state, a system configuration with parameters adapted to the specific recovery functionality is loaded. Any changes to the system parameters will be temporary and will be lost on the next device reboot.

Unboxing

At the first attempt to access the device's System Settings, you will be asked to define a password that will be associated with the "admin" user. If you try to access it remotely via a web browser, you'll need to authenticate as the "admin" user with the password "admin" to access the password definition. Next, once you've defined the password for the "admin" user, all BSP parameters will be accessible.

> It is assumed that the initial development and configuration stages will take place in a secure environment. Ensure the device is properly configured before moving it to its operational environment.

Device security-related parameters

By default, the main security functions are enabled, but the default configuration is primarily designed to facilitate the development and commissioning of the HMI device. The following lists the security features available on the device, so you can review and configure them based on your requirements.

> It is the responsibility of the system integrator and the application developer to verify the correct device configuration in order to achieve the desired level of security. This guide is intended to provide support for a quick configuration of the available security feature

Some features are mandatory and cannot be disabled, while others are optional and can be disabled or configured differently.

A security feature can be disabled because it is not needed (e.g., the firewall is not needed if the device is not connected to the network) or to allow the management of devices that do not support the highest security standards (e.g., enable the possibility to use the HTTP or FTP protocols instead to force using HTTPs and FTPs). The disabling of security-related functions, when possible, is the responsibility of the developer of the application, who must take care to make up for it with alternative measures.

Often some features related to security are disabled during the development phase of the application to be able to access the device resources more easily. It is a good practice to remember to perform a check before releasing the developed application in order not to risk leaving unnecessary services active which could compromise the safety of the device.

It's recommended to read the detailed description of each security-related parameter in the manual before modifying it.

Logs

- To reduce the risk of data saved in log files being lost, you can also configure and send all data to a remote server (SysLog).

Date & Time

- The device's date must be set correctly. If the device is connected to the internet, you can enable automatic date updates through an NTP server.

Network

- The 802.1X authentication protocol can be configured to get access protected networks that require this type of authentication.

Security

- It's possible to configure the device so that it does not use unknown external memory cards.

Disable external USB devices	
Default state	FALSE
Suggested state to maximize security	TRUE

Disable SD card automount	
Default state	TRUE
Suggested state to maximize security	TRUE

- It is possible to increase security by encrypting the data partition to render the data illegible in case the storage medium is removed, and by repeating the authenticity check of the software modules at every device power up.

Enable encryption of user data	
Default state	TRUE
Suggested state to maximize security	TRUE

Enable application signature verification at startup	
Default state	TRUE
Suggested state to maximize security	TRUE

> These options are not available in BSPs with the 'MainOS\ConfigOS' architecture.

- It's possible to configure the device so that all software module updates are only accepted if they are digitally signed.

Allow installation of unsigned modules (insecure mode)	
Default state	TRUE
Suggested state to maximize security	FALSE

> This option is not available in BSPs with the 'A/B MainOS' architecture because the authenticity check of the software modules cannot be disabled in these devices.

Applications

- It's possible to configure the device so that all applications run in restricted user mode.

Execute all applications as root	
Default state	FALSE
Suggested state to maximize security	FALSE

Services

There are several services supported by HMI devices that can be enabled or disabled to meet the needs of different work environments.

It is recommended to disable any services that are not strictly necessary in order to reduce the attack surface and minimize opportunities for a potential attacker.

Autorun scripts from external storage

- It is possible to disable the automatic execution of scripts from external storage devices (USB and SD card).

Enabled Autorun scripts from external storage	
Default state	FALSE
Suggested state to maximize security	FALSE

- Through the "Allow only user-certified scripts" parameter, you can configure the device to execute only the scripts that have been validated by the HMI device administrator..

Allow only user-certified scripts	
Default state	FALSE
Suggested state to maximize security	TRUE

Avahi Daemon

- It's possible to prevent the device from being identified on the network by its name by disabling the Avahi Daemon.

Enabled Avahi Daemon	
Default state	FALSE
Suggested state to maximize security	FALSE

Cloud / VPN Service

- Through Cloud/VPN services, it is possible to access the panel from the outside.

Enabled Cloud / VPN Service	
Default state	FALSE
Suggested state to maximize security	FALSE

Device Discovery

- It's possible to prevent the device from being identified on the network via the Device Discovery message.

Enabled Device Discovery	
Default state	TRUE
Suggested state to maximize security	FALSE

Enable device restore via TAP TAP option

- It's possible to disable the ability to perform a factory restore of the device through the “TAP TAP”.

Enable device restore via TAP TAP option	
Default state	TRUE
Suggested state to maximize security	FALSE

If the ability to restore the device is disabled both via the TAP TAP option and through a USB drive then, in the event the administrator password is lost, the device can only be recovered by returning it to the manufacturer.

Enable device restore via USB

- It is possible to disable the ability to perform a factory restore of the device by reading the special file from the USB device.

Enable device restore via USB	
Default state	TRUE
Suggested state to maximize security	FALSE

If the ability to restore the device is disabled both via the TAP TAP option and through a USB drive then, in the event the administrator password is lost, the device can only be recovered by returning it to the manufacturer.

Enable TAP TAP menu via touchscreen or mouse

- It's possible to disable access to the device configuration via the TAP TAP on touchscreen or mouse (keyboard access, via the CANC key on a USB keyboard, will remain unaffected by this setting)..

Enable TAP TAP menu via touchscreen or mouse	
Default state	TRUE
Suggested state to maximize security	FALSE

Firewall Service

- The device is equipped with a firewall that allows you to define which connections will be accepted while excluding all remaining undefined connections.

Enable Firewall Service	
Default state	FALSE
Suggested state to maximize security	TRUE

Network Rate Limiter

- Rate limiting controls the amount of network traffic by setting limits on the number of requests allowed within a specific time frame. This prevents system overload and protects against Denial-of-Service (DoS) attacks. It lets you create rules to limit the maximum number of packets transmitted on network interfaces.

Enable Network Rate Limiter	
Default state	FALSE
Suggested state to maximize security	TRUE

Router / NAT / Port forwarding

- This service allows network devices to be accessed from the outside through the HMI device.

Enable Router / NAT / Port forwarding	
Default state	FALSE
Suggested state to maximize security	FALSE

SNMP Server

- When the SNMP service is enabled, an SNMP client can retrieve various information from the device using the SNMP protocol.

Enable SNMP Server	
Default state	FALSE
Suggested state to maximize security	FALSE

SSH Server

- Through this service, you can access any resource on the HMI device. The service was designed to be used only by expert users during application development.

Enable SNMP Server	
Default state	FALSE
Suggested state to maximize security	FALSE

VNC Service

- VNC is a service that allows remote access to the HMI device's display.

Enable VNC Service	
Default state	FALSE
Suggested state to maximize security	FALSE

> If enabled, the service provides several security-related parameters (authentication, encryption, certificates, session timeout, etc.) that must be configured to suit your specific needs.

Web Server

- For backward compatibility, by disabling the "Allow only Secure HTTPS connections" parameter, access to the HMI device parameters is also accepted from insecure web connections.

Allow only Secure HTTPs connections	
Default state	TRUE
Suggested state to maximize security	TRUE

- Using the CORS (Cross-Origin Resource Sharing) parameter, you can enable access to the HMI device's system parameters from websites on a different domain. If enabled, make sure the CORS domains filter" parameter contains the list of external domains that will be accepted because, if left empty, any domain will be accepted.

CORS domains enabled	
Default state	FALSE
Suggested state to maximize security	FALSE

Management

- It does not contain parameters related to security. However, from this page, you can back up and restore the entire HMI device. A policy for regular backups is useful for maximizing the security of the HMI device.

Authentication

- The "Session" panel contains parameters that are useful for strengthening the defense against potential cyber threats, such as brute-force attacks aimed at guessing account passwords. These parameters should be adjusted on a case-by-case basis, depending on the work environment that will host the HMI device. The default values are designed to suit the most common work environments.
- By default, a “Password security policy” is already in place, which should be sufficient for most cases. If needed, you can redefine it to better suit your specific requirements.

Safe disposal

When the HMI device is decommissioned and needs to be disposed of, it's important to remember that it may contain confidential information. This data must be erased to ensure it is not left on the device after disposal.

All information can be deleted by performing a factory reset. You should also check that any removable storage (USB or SD card) is not left inside the device.

> You can find the information for performing the "Factory Reset" in the "HMI System Settings" manual. (Ref.: "Factory Reset" on page 52)

Security Disclosure Policy

For general information or inquiries related to cyber security, please contact our Technical Support team through the standard communication channels.

We are committed to investigating all reports and taking appropriate action to ensure the security and integrity of our solutions.