



Getting started

Lenze v4x0

Content

About this documentation	5
Getting started	6
Web Browser for HMI Devices	7
Installation from USB Flash Drives	8
Installation from Remote	11
Settings.....	12
Web Browser.....	13
The Toolbar	15
Re-enable warnings	15
System options.....	16
Initial configuration	19
System Configuration	20
Installation of certified software modules.....	20
Signed File	21
User's Certificate	21
Signature of USB tools	22
Manufacturer's certificate	23
Guideline	23
Allow installation of unsigned modules (Compatible Mode)	24
System Settings	25
Enter in System Settings.....	25
Localization	28
System.....	29
Logs	30
Date & Time	31
Networks.....	32
Security	33
Applications	35
Services	35
Management.....	35
Display.....	37
Fonts.....	37
Authentication	38

Restart.....	38
Exit	38
Services	39
Autorun scripts from external storage.....	39
Avahi Daemon.....	39
DHCP Server	40
Enable device restore via TAP TAP option.....	40
Enable device restore via USB	40
Fast Boot	40
Firewall Service	41
Network Rate Limiter	42
Router / NAT / Port Forwarding	43
Show loading bar during boot	44
SNMP Server	44
SSH Server	45
Web Server.....	46
Authentication	47
Users and Roles.....	47
Session	49
x.509 Certificate	50
Forgot password	52
Update System Components	53
Backup and Restore	55
Cybersecurity Guide.....	56
Operational States	56
Unboxing	57
Device security-related parameters.....	57
Logs	58
Date & Time	58
Security	58
Applications	58
Services	58
Management.....	62
Authentication	62

Safe disposal	63
Security Disclosure Policy	63

About this documentation

Version	Date
1.0	2025-03-05



Current sets of documentation and software updates about Lenze products can be found in the Download area at: www.lenze.com

Target group

This documentation is intended exclusively for qualified technical personnel.

Getting started

Lenze v4x0 have a system settings interface to allow configuration of system options. The user interface of System Settings is based on HTML pages accessible from the HMI screen or remotely using a Web browser Chrome v44 or higher using port 443. To connect enter the address https://IP/machine_config where IP is the IP address of the HMI device. Default username is “admin”, default password is “admin”. Use the navigation menu on the left side of the screen to browse through the available options.

System Settings		Language		ADMIN 
Language	☒	English		
System		Italiano		
Logs		Deutsch		
Date & Time		中文		
Network				
Services				
Management				
Display				
Restart				
Authentication				

Web Browser for HMI Devices

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

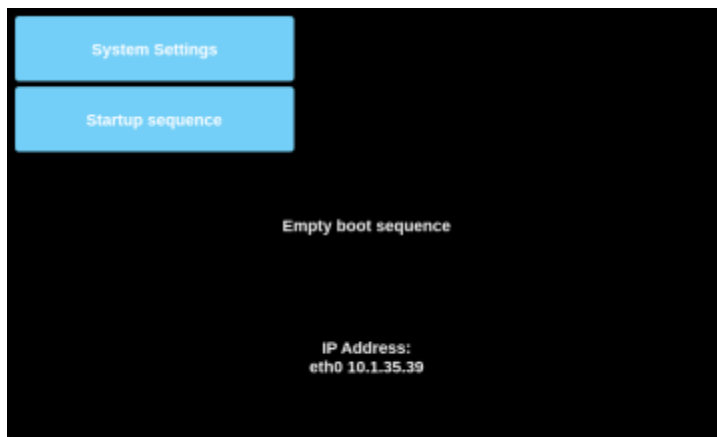
Web Browser is the ideal solution to transform an embedded HMI device into a browser device with HTML5 compatibility for state-of-the-art browsing applications for the industry. With the choice of the appropriate HMI device, the browsing application can be easily installed in the most challenging industrial 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.

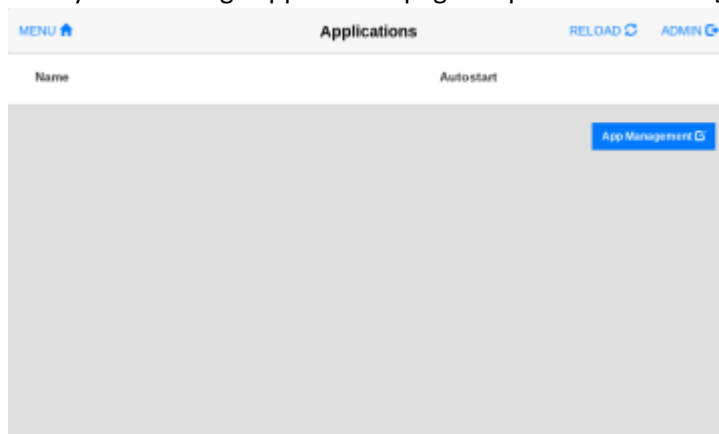
Installation from USB Flash Drives

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](#)".



To install the web browser application, follow this procedure:

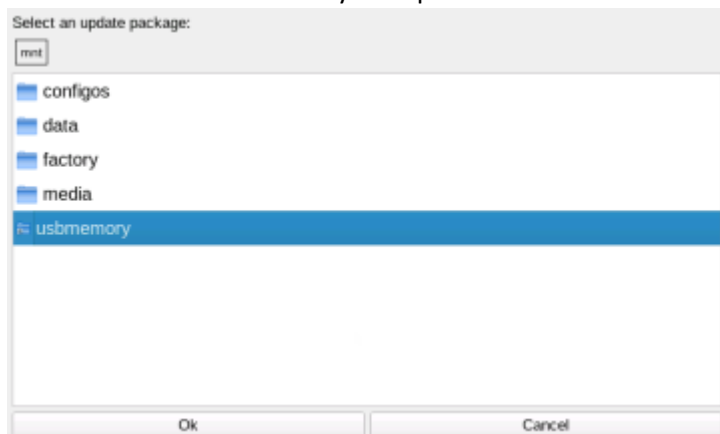
1. Copy the application file to an empty USB stick and insert the key into the operator panel (The supported file systems are FAT16/32 and Linux Ext2, Ext3 and Ext4).
2. On the device select [Startup sequence]
3. Authentication with "admin" credentials is required.
4. The System Settings Applications page is open. Click on the [App Management] button.



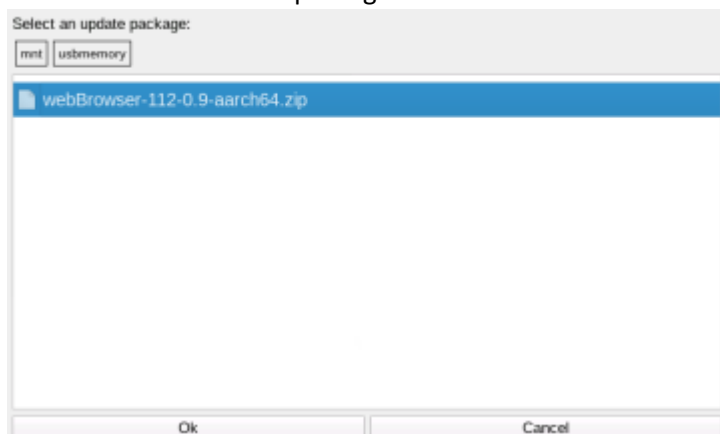
5. In the App Management dialog, click on [Install/Update] button.
6. Then click [Browse Image] to open the file system dialog where you can select the package to install



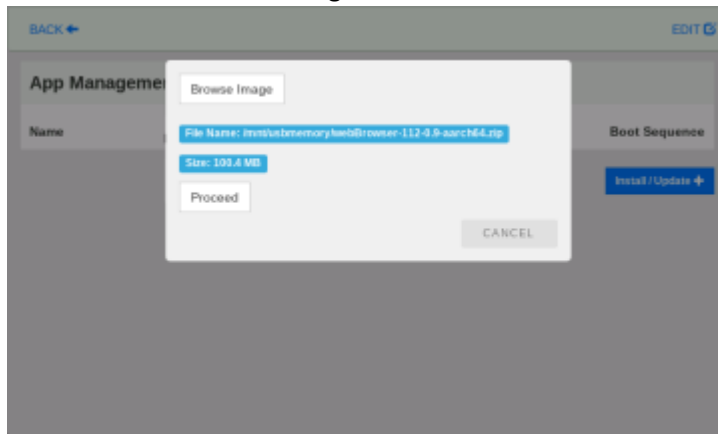
7. Double click on “usbmemory” to open the folder



8. Select the web browser package



9. The runtime installation begins



At the end of the installation, the 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 Web Browser package.

Settings

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

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

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

To access System Settings, you must log in. The username 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).

Username

Password

Back

Proceed

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](#)".
- From a remote browser, see: "[Enter in System Settings](#)" (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 the top left edge of the display pressed 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.
Alternative homepage	URL of an alternative home page (see below).
Fallback page	Secondary home page that is loaded when failed to load the primary home page (the URL must include the protocol).
Enable toolbar	Show/hide the toolbar. (Available only in Advanced view mode)
- 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.
Default page zoom	Set default zoom factor from the loaded page.
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. • 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 in local settings)
Certificate preferences	Clear all white listed sites. The action can be done in chromium from the toolbar (see: " Re-enable warnings ").
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.

Property	Description
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](#)”.

The Toolbar

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



Available commands are:

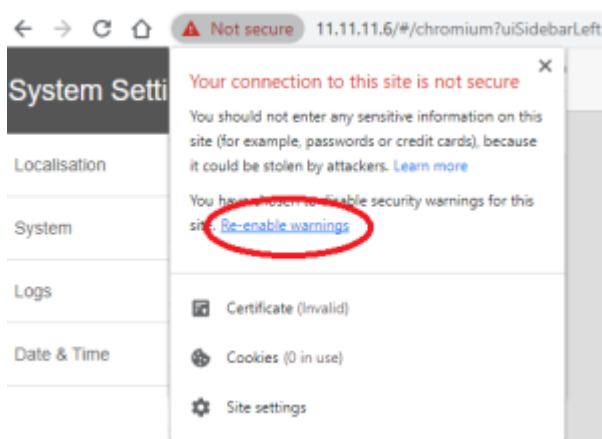
- Page Reload
- Bookmark List
- History Buttons
- URL Address
- Add Bookmark
- Open System Settings

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 on the options page and the "X" icon on the toolbar when enabled. Closes the web browser.
--enable-restart-button	Enables the "Exit" button on 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 the web browser starts again it will open a new window, which is faster. Command line flags given the first time cannot 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 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 next time even without this option.
--fixed-toolbar	The toolbar will be fixed and will not be collapsed.
--disable-toolbar	Enable the ability to download files. The files will be stored in the folder: /mnt/data/storage/chromium/home/Downloads
--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.

Option	Description
--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	Overrides the default browser user agent.
--disable-options	Like the 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 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

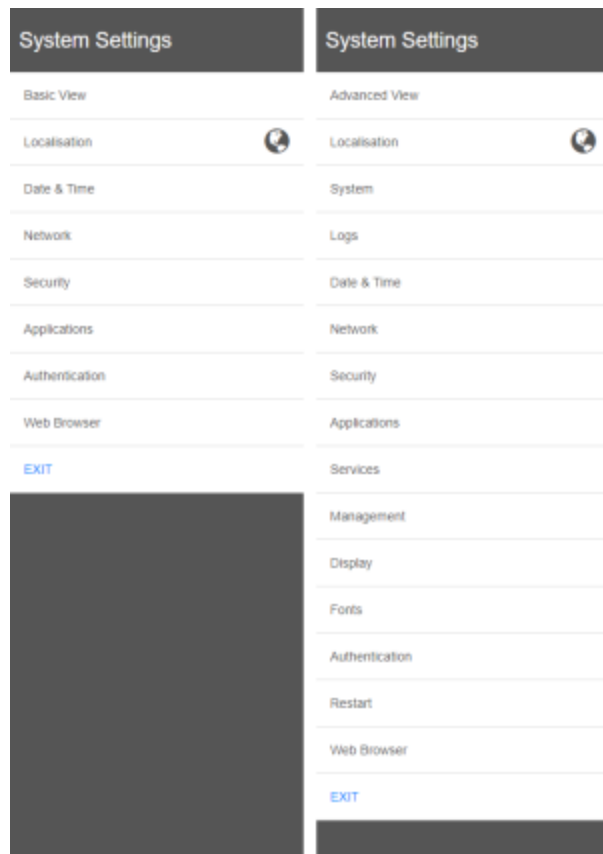
- homepageLink=<url>
URL must include the protocol (i.e. https://, file://)
- customUserAgent=<userAgent>
- showToolBarOnError=<true|false>
- showWiFiStatus=<true|false>
- showHistoryButton=<true|false>
- showLoadingBarAndStopButton=<true|false>
- onStartup=<settings|homepage|lastVisistedPage>
- enableToolBar=<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.com
```

System Configuration

System Settings is available in the HMI devices as a tool for the configuration of the system properties of the device. For your convenience, there are a Basic view and an Advanced view where the base view list only the main properties while the advanced view lists all the available properties.



To switch between Basic Mode and Advanced Mode press the first item in the System Settings menu list.

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).

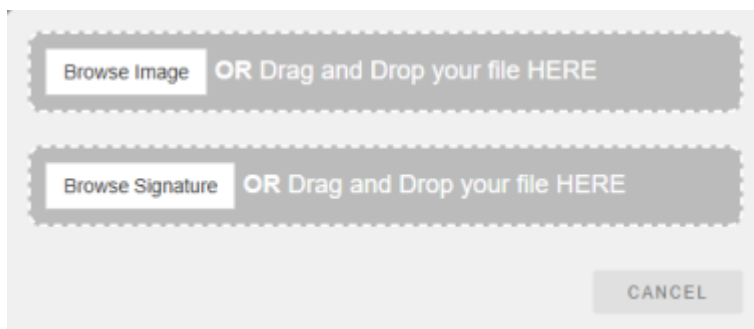
Since European directive RED-DA-18031 requires verification of software module authenticity for all devices equipped with radio equipment, when WiFi is enabled (for devices that support it), it's recommended to also enable signature control.

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.

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.



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 23).

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

The certificate used to validate BSP updates is located in the /usr/share/platform-keys folder on the HMI device and is distributed/updated along with firmware updates. To validate its integrity, you need to verify its fingerprint (contained within the certificate) by comparing it with the fingerprint published by Lenze v4x0 web panel.

Date	Fingerprint	Status
18.06.2025	11dffefde555a9d02a3bee70ba29c973b9f07241	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.

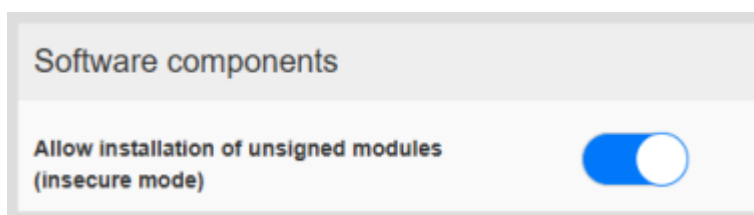
Step by Step procedure

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



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).

Enter in System Settings

There are several ways to access the System Settings page.

You can enter

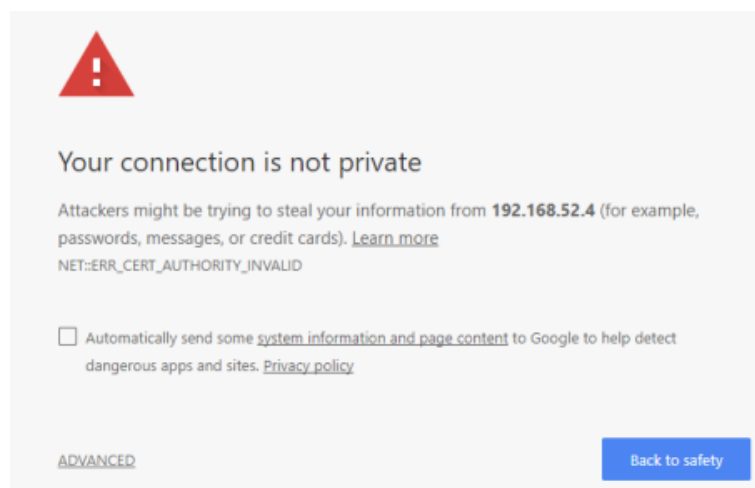
- From a remote web browser (remote access may be disabled and may be unavailable)
- From the HMI device when no runtime is load
- From the HMI device using the tap-tap procedure

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:

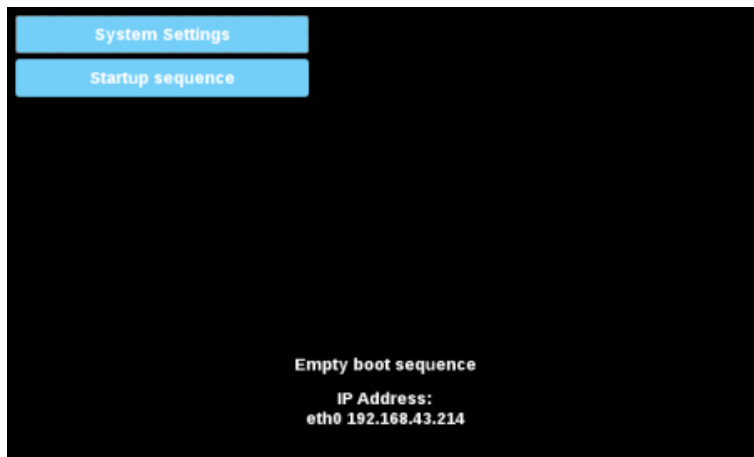
https://IP/machine_config

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.



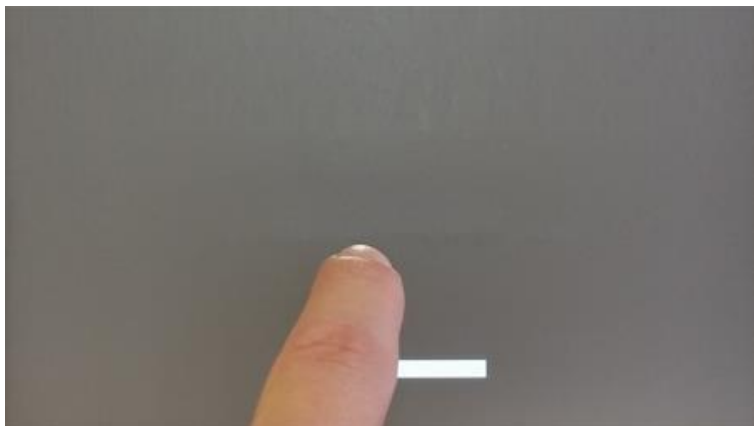
System Settings access from HMI device

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.

Localization

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

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)
Sensors	Device sensors (Temperature, Humidity, Working voltage, Absorbed current)
Legal	License overview used software-components and libraries

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

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
Current Date Local Time	Date and time can set manually only if 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 seconds and 36 hours.
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 - 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 in edit mode:

Parameter	Description
General Settings	Device hostname Avahi Hostname (see " Avahi Daemon ")
Network Interface	Network parameters of the available interfaces • DHCP • IP Address • Net Mask • Gateway • 801.2x Protocol By default, the network interface is set with DHCP turned on to retrieve network parameters from the DHCP server. If the DHCP server is not found, the avahi-autoipd service is used to set an IP address in the range 169.254.x.x. 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.
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 Generally provided from the DHCP servers, but can be modified in edit mode 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
Secret ID	Name used to identify each secret information included in the selected domain.
Type	Type of information to be stored. • 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.

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.

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 checksum 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 directly available 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. Please refer to the chapter "[Services](#)" for more details.

Management

From the management page, you can update the system components of the HMI device. Please refer to the chapter "[Update System Components](#)" 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”](#) for 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.

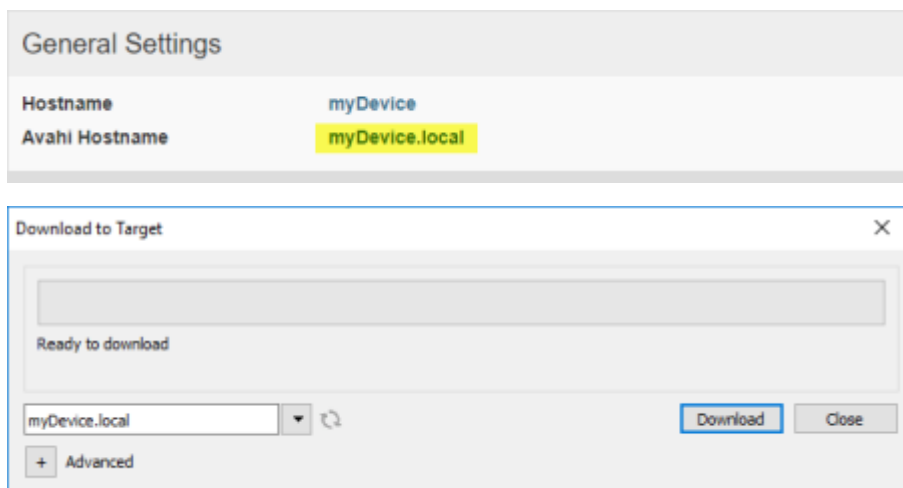
Autorun scripts from external storage

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)

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.).

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”](#))

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).

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”](#))

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).

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

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.

Firewall Service

Enabled



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

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

+

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., 192.168.5.123) or a range of IP addresses in CIDR format (e.g., 192.168.5.0/24). For details on valid subnet specifications following such format, please refer to:

https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

If you 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](#)").

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)

Parameter	Description
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)
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 • IPV\$, TCP, UDP or ICMP using Data Type = IP

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

Enabled	Name	Source Interface	Source Port	Device IP	Device Port	
☒	HMI-01	eth0	8081	192.168.55.1	80	Up Down

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

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

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.

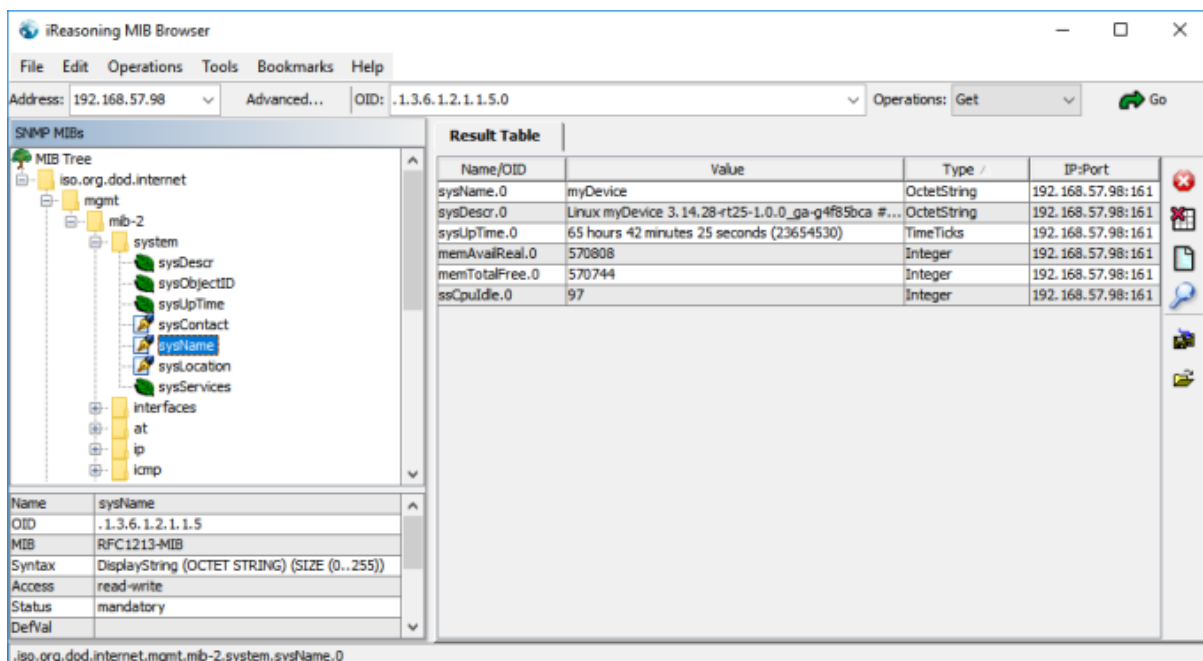
Show loading bar during boot

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 VNC server
Autostart	Keep the VNC 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.

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 to external domains is not allowed. When enabled, access to 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

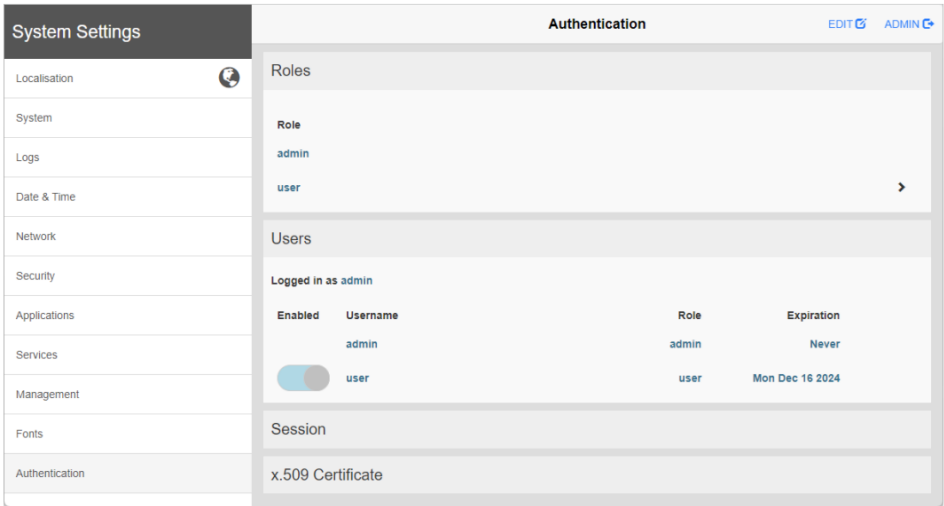
It is possible to define a custom policy for the required password format.

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.

Roles

Role

admin

user

Reset roles

Users

Enabled

admin

user

Username

admin

user

Role

admin

user

Expiration

Never

Tue Mar 05 2052

Reset 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).

Role detail

Selected role: user

Enabled

Modify

Module

Localisation

System

Logs

Date & Time

Network

Security

Applications

Services

Plugins

Management

Display

Fonts

Authentication

Restart

Users

Click the "EDIT" button to manage users.

Users

Enabled

admin

user

Role

user

New Password

Confirm Password

Password validity (days):

60

Update

Role

admin

Expiration

Never

user

Mon Dec 16 2024

Passwords are required to include:

At least 8 characters in total

At least one lower case and one upper case letter

At least one numeric character

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

Parameter	Description
Enabled	Button to keep user account enabled or disabled.
Role	Specify the user’s permission level.
New Password	Set a temporary password that the user will be forced to change in their first login.
Password validity	Duration in days for which the password remains valid, after which the user is required to change it.

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.

49

Parameter	Description
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

Enter in edit mode to change the authentication passwords or to personalize the x.509 certificate of the HMI device.

x.509 Certificate

HMI Device use a self-certificate to encrypt the Internet communication through 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

Parameter	Description
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

In the event that all administrators have forgotten their passwords, access to the device configuration will be irrevocably lost. To restore functionality, a factory reset must be performed. This process will result in the complete erasure of the device's memory, including any prior project downloads. Upon completion of the factory reset, the administrator password will be automatically reset to its original default value of "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 (Please refer to the chapter "[System Settings](#)" for more details).

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 (Please refer to the chapter "[System Settings access via TAP TAP procedure](#)" for more details.).
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 (Please refer to the chapter "[System Settings](#)" for more details).

Steps to reset the admin password:

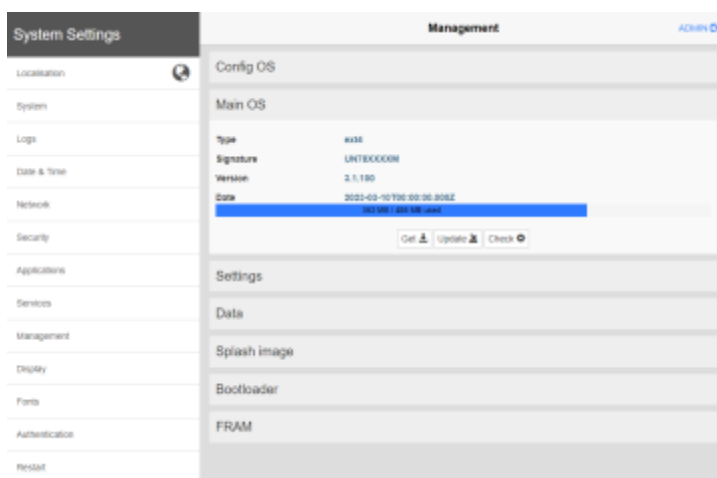
1. Placing a file named "device-factory-restore" into a USB stick and plugging it into the device.
2. The device restore process starts automatically. The buzzer is played once at the beginning and 3 times at the end if the operation is successful.
3. The "device-factory-restore" is deleted from the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

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 be provided from tech support).

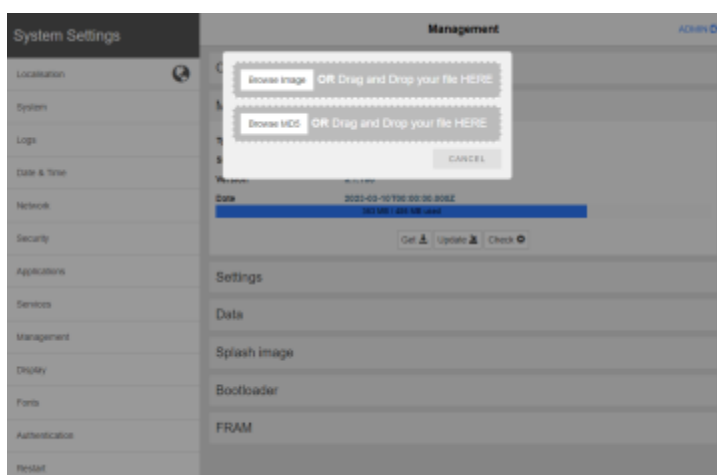
The system components of the Linux device can be updated locally using a USB memory key or remotely via web browser (remote access may be disabled and may be unavailable).

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



Expand the component to update and select [Update]

On the opened dialog, click [Browse Image], then select the “xxx-mainos-xxx.tar.gz” file. Click then on [Browse MD5] and select the “xxx-mainos-xxx.tar.gz.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.

Enter System Settings in Config OS mode via tap-tap procedure

System Setting in Config OS 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”



HMI will restart into System Settings in Config OS mode:



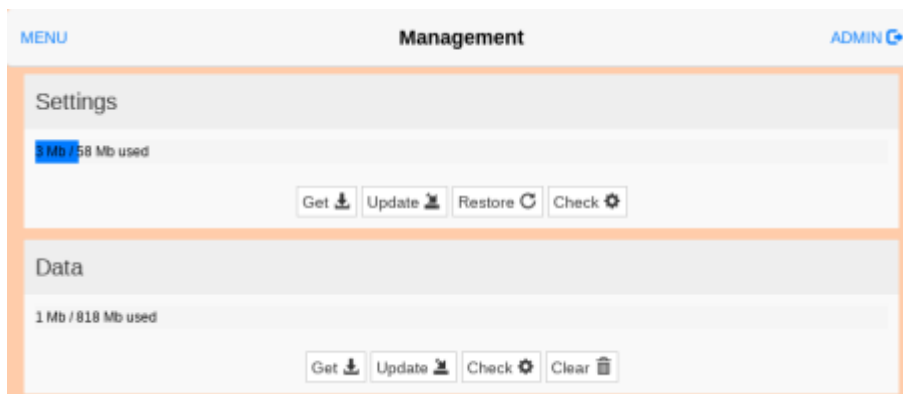
Backup and Restore

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](#)"

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.

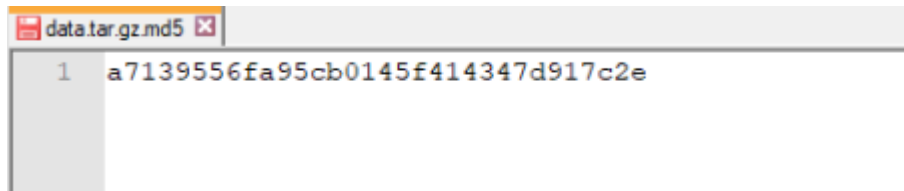
The MD5 checksum file must have the same name as the files that you want to load with the .md5 suffix as e.g.:

- 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 checksum generates a file with multiple lines, the additional lines must be deleted.



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 version has been installed on the HMI devices and that they are updated whenever a new version is made available on the manufacturer's website.

The HMI device is designed for use in typical industrial and naval automation operating environments, which usually involves communication with programmable logic controllers (PLCs). The overall system is assumed to operate at Security Level 2. Consequently, the products are designed to meet the security requirements for this level.

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.

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

- 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	FALSE
Suggested state to maximize security	TRUE

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).

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

Enabled 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.

Enabled Autorun scripts from external storage

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 SSH Server

Default state	FALSE
Suggested state to maximize security	FALSE

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) is not left inside the device.

Security Disclosure Policy

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

If you have identified a potential security vulnerability affecting our products or devices, we kindly ask you to report it by sending a detailed disclosure to: security@lenze.com.

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