# HMI System Settings

## User Manual

Version

© 2010-2024 Exor International S.p.A.

# Disclaimer

© 2010-2024 Exor International S.p.A.

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 Exor International S.p.A.
- 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.

---

*This products/software contains software licensed under the GNU General Public License, Version 2.0 (GPL V2.0), software licensed under the GNU LESSER General Public License, Version 2.1 (LGPL V2.1), and/or open source software other than the software licensed under the GPL V2.0 and/or LGPL V2.1. The software open source included is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.*

*For more details or for a copy of sources where required by license , as well as the respective copyright notice, please ref to device settings menu or https://www.exorint.com or contact us at support.it@exorint.com*

# Contents

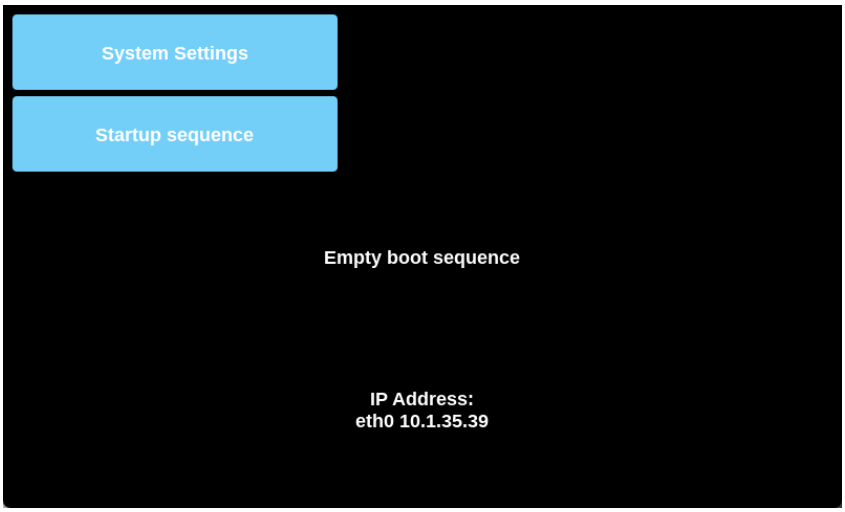
# HMI device configuration

Linux products offer a powerful integrated tool called System Settings that allows management and upgrade of system components. Operations can be done directly on HMI or remotely using web browser.

***CAUTION: Working with the System Settings tool is a critical operation and, when not performed correctly, may cause product damages requiring service of the product. Contact technical support for assistance.***

# Runtime Installation

If the HMI device is delivered from the factory without Runtime, at first power up HMI shows the “Runtime Loader” screen.




Runtime can be installed:

- Automatically, via Ethernet on first project download with JMobile Studio
- Manually via USB Memory, creating an “Update Package”.

## Install Runtime via Ethernet

To install Runtime via Ethernet follow the "Download to HMI device" procedure.

**WARNING: Runtime installation via Ethernet download requires the HMI to have a valid IP address.**

The IP address can be assigned in three ways:

- *Automatically via DHCP server.* This option is enabled by default. If a DHCP server is available on the network IP address will be assigned automatically by the server.
- *Automatically via Auto-IP feature.* If DHCP assignment is enabled but no DHCP server is available on the network the HMI assigns itself an IP Address into range 169.254.x.x with subnet mask 255.255.0.0
- *Manually via System Settings.* From System Settings menu, in Network section the IP address can be manually assigned, disabling the DHCP server assignment feature.

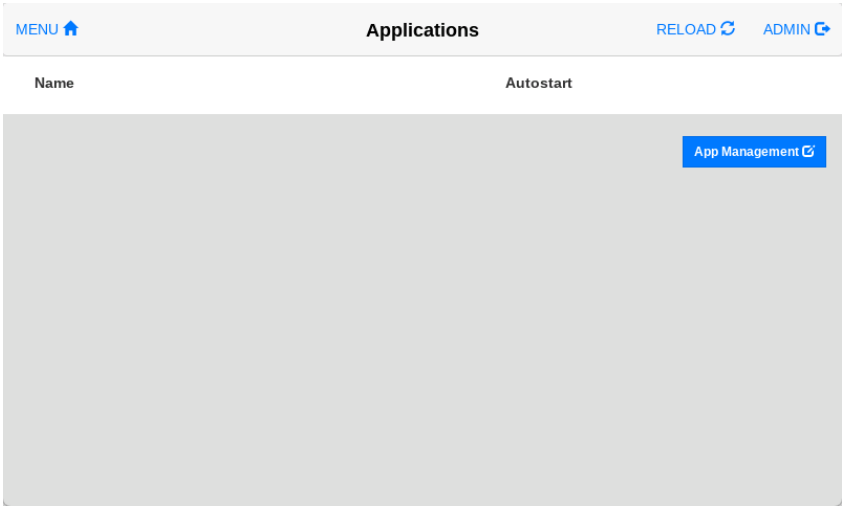
## Install Runtime via USB Memory

To install Runtime, UpdatePackage or Backup Package via USB device follow this procedure:

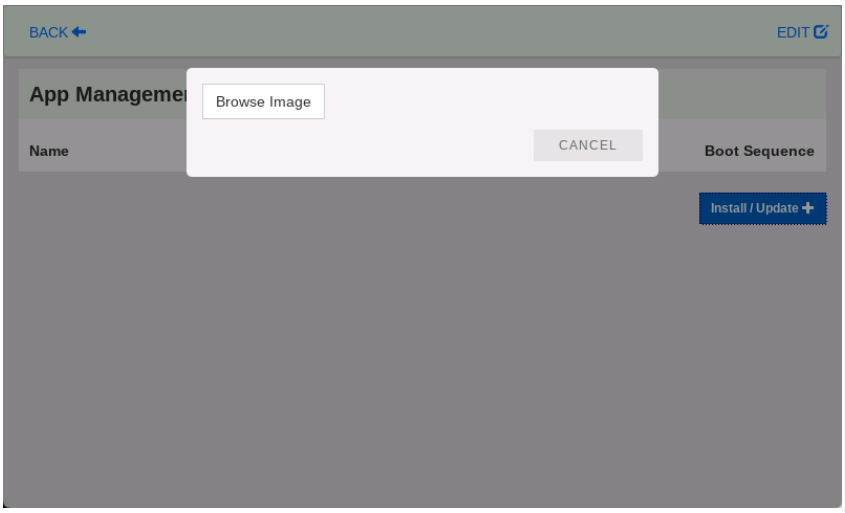
1. Create an Update Package from JMobile Studio and copy into an empty USB memory stick

Note: File systems supported are FAT16/32 and Linux Ext2, Ext3 and Ext4.

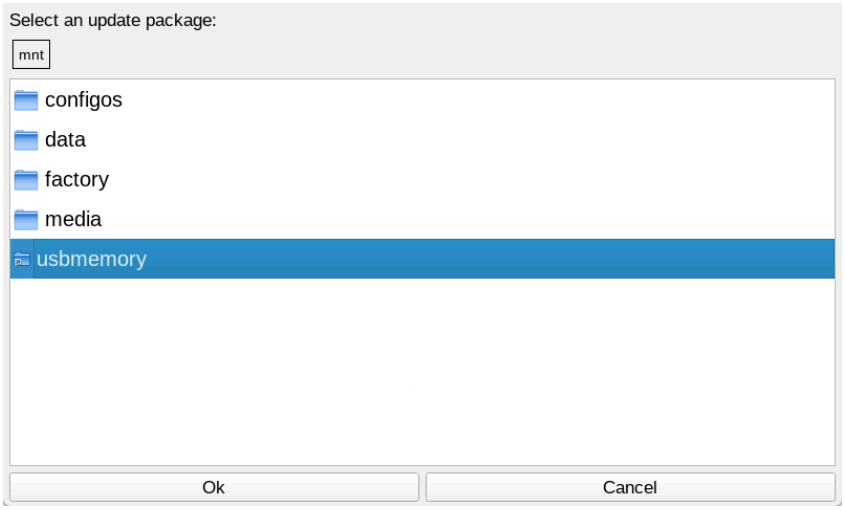
2. On HMI select the [Startup sequence], then enter the password of the HMI Device. The below page will appear.



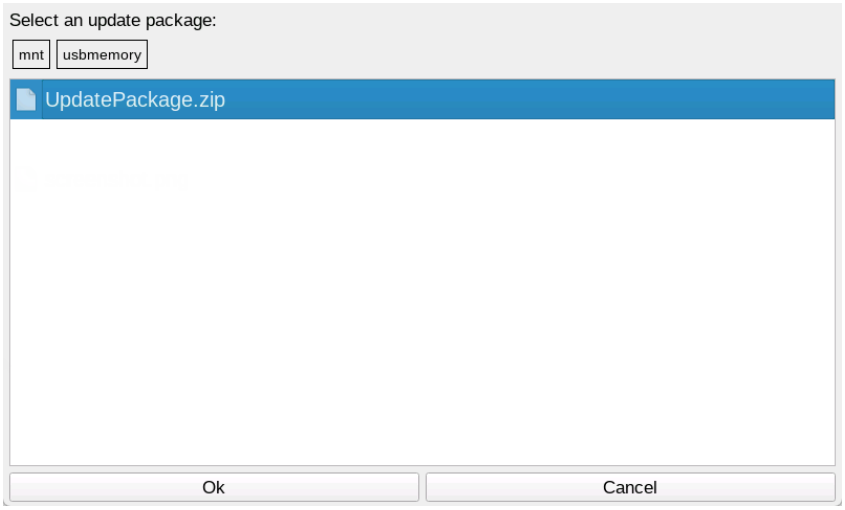

3. Click on the [App Management] button and then the [Install/Update] button to get the below page.



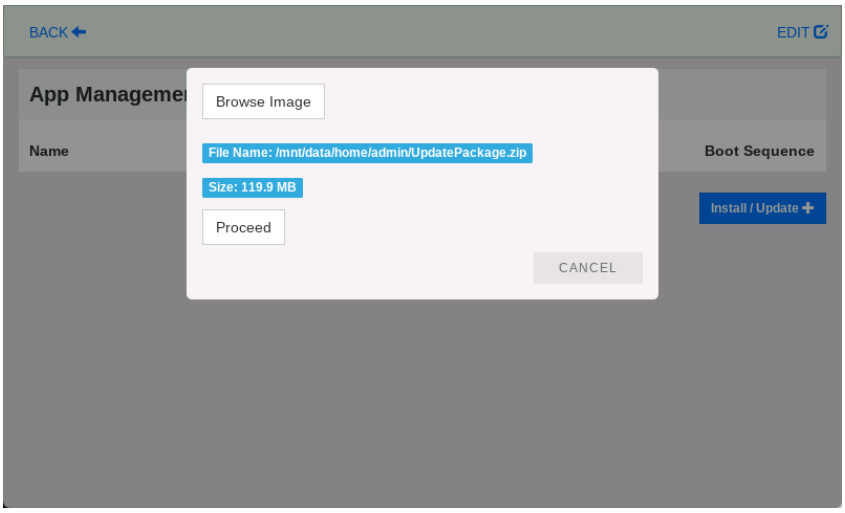

4. Click on the [Browse Image] button to open the browse folder dialog.



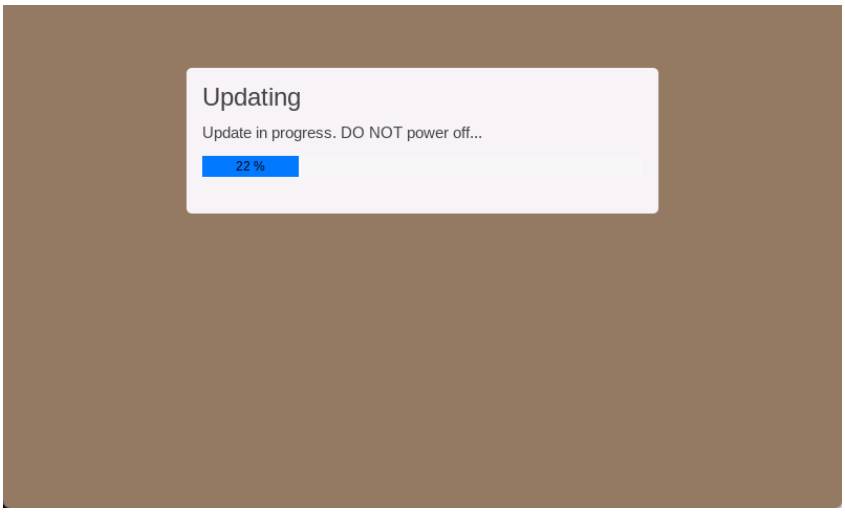

5. Click on the [usbmemory] folder and then on the file to install (generally the UpdatePackage.zip)



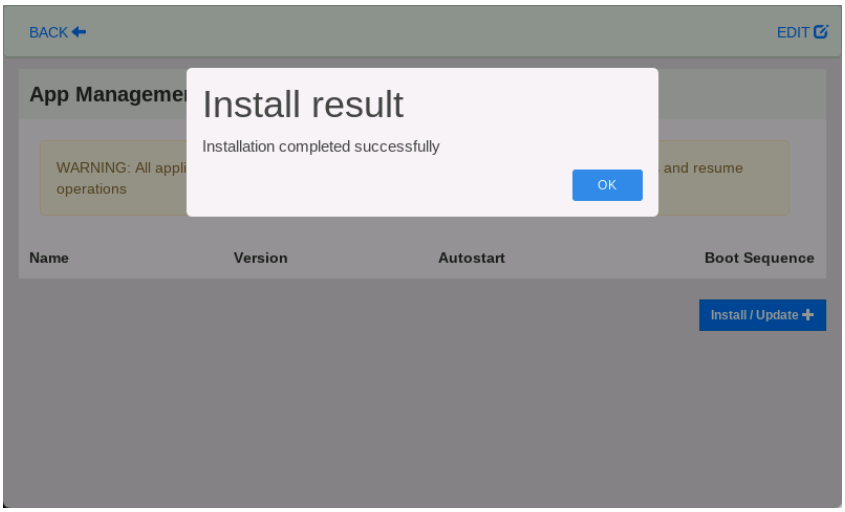

6. Select “UpdatePackage.zip” and confirm with [Ok]




7.Finally, press [Proceed] and the runtime installation begin




8. Once complete, the HMI device restarts, and the application is loaded.

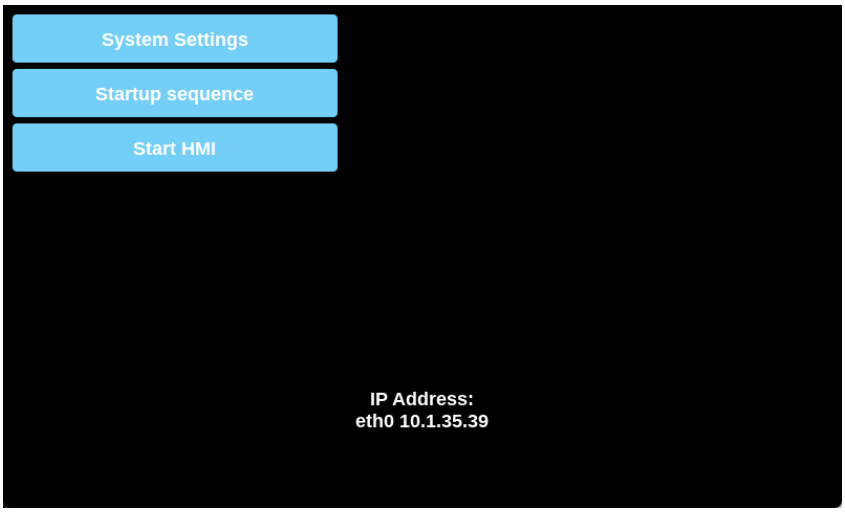



## Runtime Uninstall

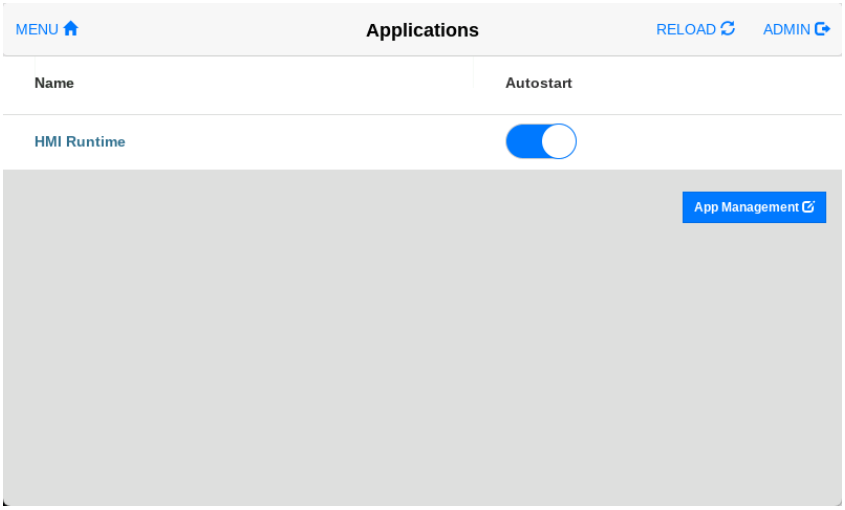
System Settings in Default mode allows to uninstall HMI Runtime or change Startup sequence, this mode is available via tap-tap sequence and can be accessed also when HMI is facing a software failure.

See "System Settings access via TAP TAP procedure " on page 9

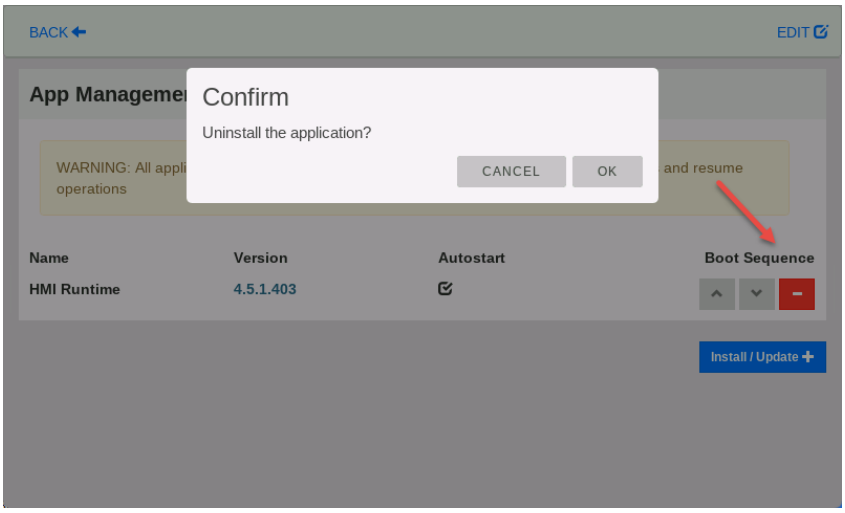
1. To uninstall the Runtime from HMI in Default Mode screen select [Startup Sequence], then enter the password of the HMI Device:



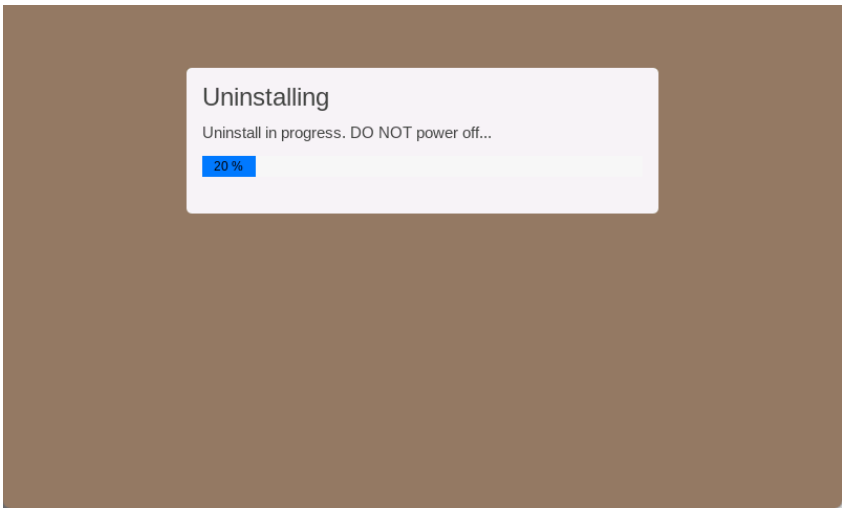

2. From the installed applications view, click on the [App Management] button.



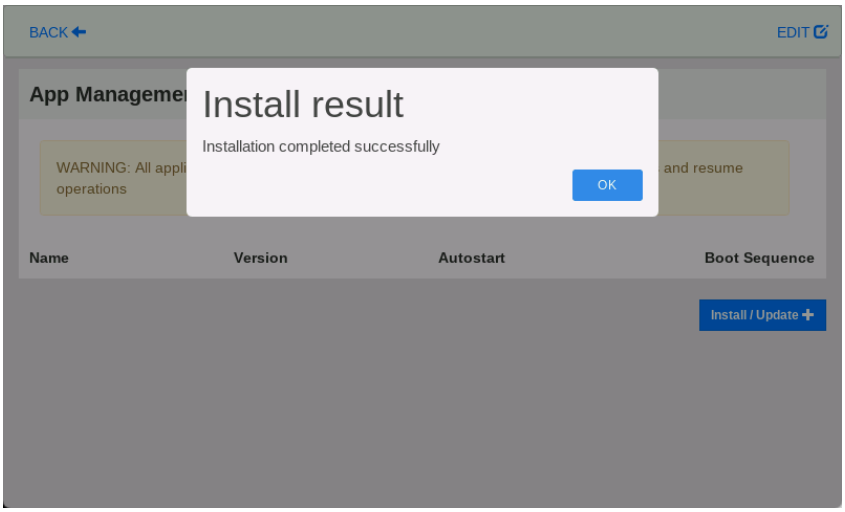

3. Click on the uninstall button [ - ] and then press the [OK] button to confirm in the pop up dialog.




4. Runtime uninstall process will be performed:




5. When finished, press the [OK] button and the HMI device will restart.


BACK
EDIT
App Manageme
Install result
Installation completed successfully
OK
WARNING: All appli
operations
and resume
Name
Version
Autostart
Boot Sequence
Install / Update

# 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

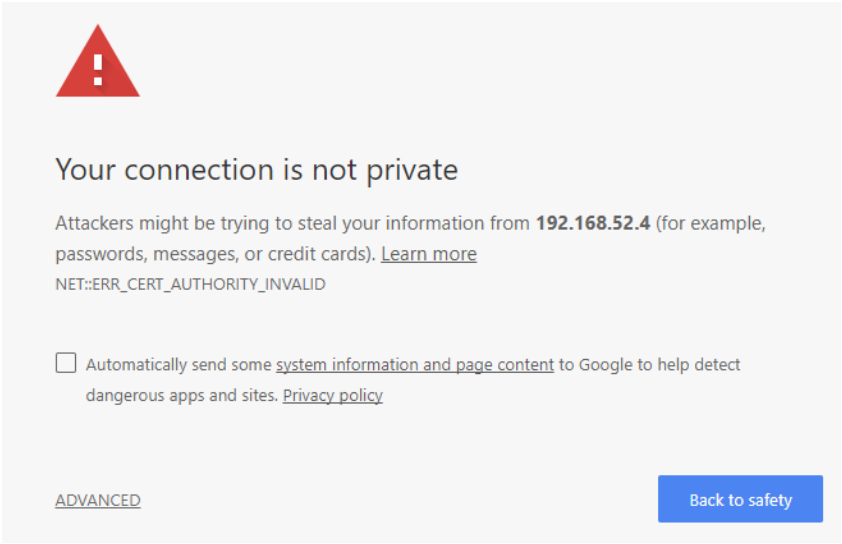
- From a remote web browser (remote access may be disabled and may be unavailable)
- From the HMI device when no runtime is load
- From the HMI device using the tap-tap procedure

### 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.

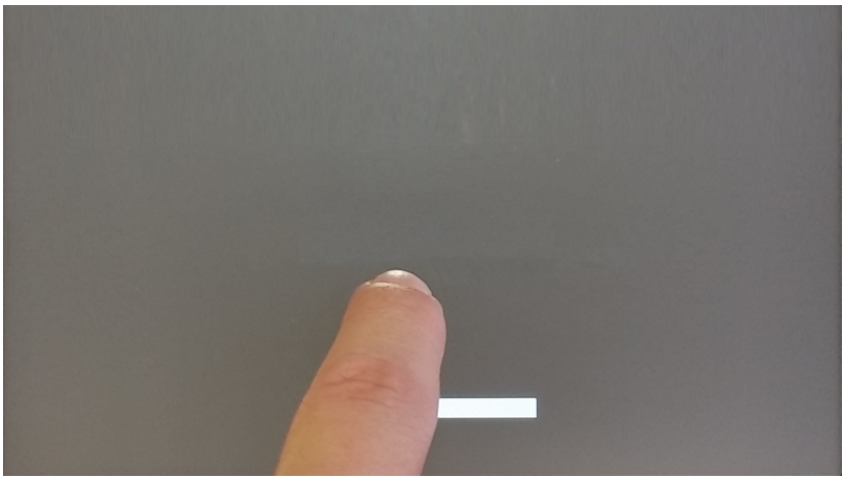



### System Settings access from HMI device

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


### System Settings access via TAP TAP procedure

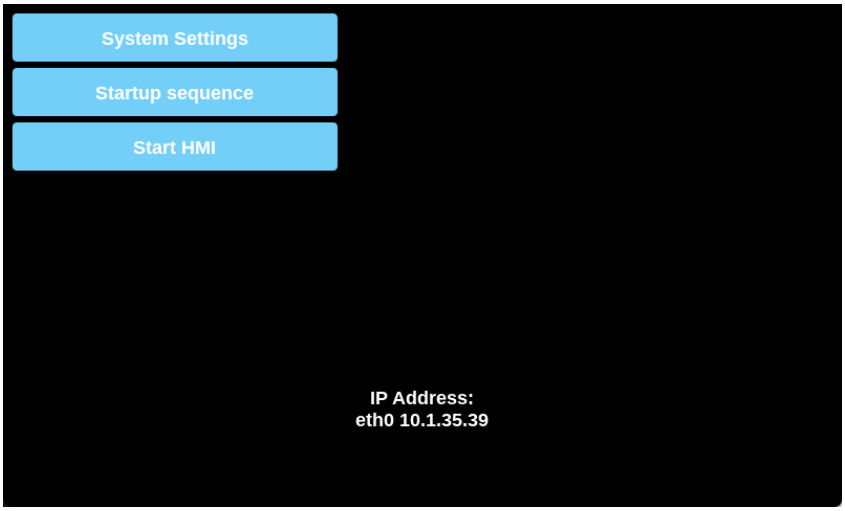
Tap-tap consists in a sequence of several touch activations by simple means of the finger tapping the touch screen performed during the power-up phase and started immediately after the HMI is powered on.



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.)<br>  Sensors are not available on all models. |
| **PlugIn** | Hardware plugin information |
| **Legal** | Legal information regarding components licensed under GPL/LGPL |

# Logs

System logs contain two types of information:

- **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.
- **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.

| 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.

The information gathered in the 'audit' file complies with the requirements of CR 2.8 (Auditable events) of the IEC-62443 standard. Internally, the 'RFC5424' format (Syslog Protocol) is used.

# Date & Time

Device date and time.

| Parameter | Description |
|---|---|
| **Current Timezone** | Timezone region |
| **Current Date**<br>**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<br>• NTP Server<br>Specify the Internet NTP Server address<br>  <br>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.<br><br>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.<br>• Disabled<br>The NTP can apply a signification correction to correct date & time error<br>• Enabled<br>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<br>Avahi Hostname (see "System Settings" on page 8) |
| **Network Interface** | Network parameters of the available interfaces<br>• DHCP<br>• IP Address<br>• Net Mask<br>• Gateway<br>• 801.2x Protocol<br>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-autoip service is used to set an IP address in the range 169.256.x.x. |
| **DNS** | DNS Servers<br>Generally provided from the DHCP servers, but can be modified in edit mode<br>Search Domains<br>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:<br>• General<br>This space is available for third party applications<br>• System<br>This space is used from the services embedded in the device (e.g. the VNC Server)<br>• HMI Runtime<br>This space is used from the JMobile HMI Runtime application |
| **Secret ID** | Name used to identify each secret information included in the selected domain. |
| **Type** | Type of information to be stored.<br>• Text |

| Parameter | Description |
|---|---|
| | • Password<br>• Certificate<br>• File |
| **Secret Info** | The secret information to keep stored..<br>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.

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

# 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 page 17chapter.

# 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 34 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

| Parameter | Description |
|---|---|
| **Brightness** | Brightness level of the display |
| **Back light timeout** | Backlight inactivity timeout |
| **Orientation** | Display orientation |

# 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 25for 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.

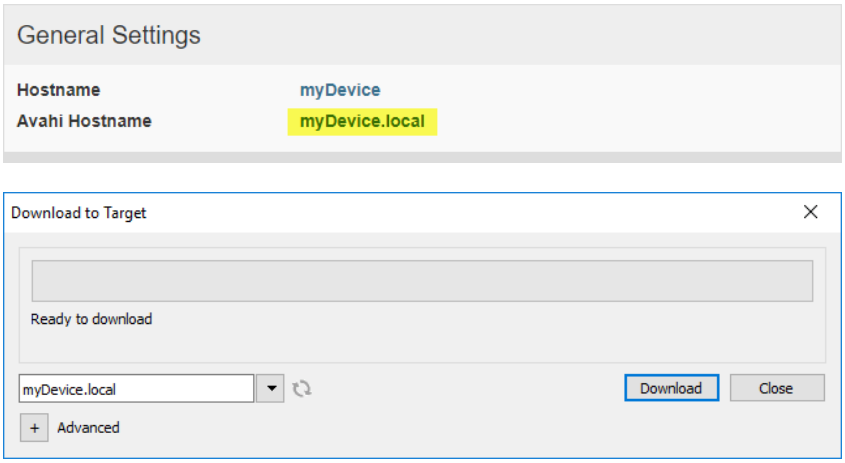
## Autorun scripts from external storage

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.

**Required BSP v1.0.212 or greater**

## 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).



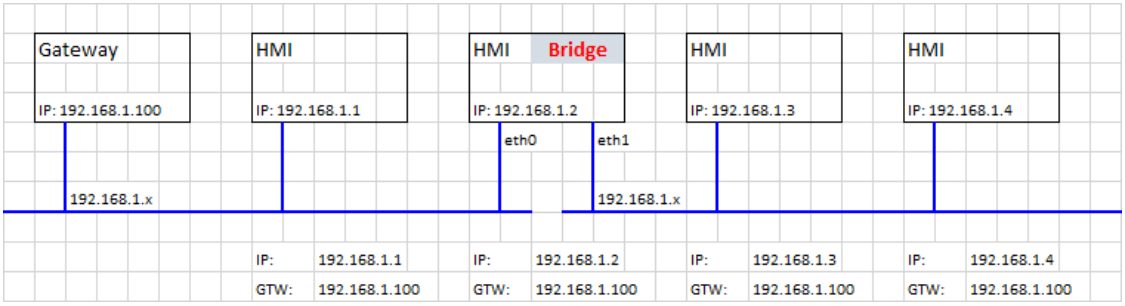

Avahi Daemon runs on UDP port 5353

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 30 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**<br>**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)<br>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 28)

**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 28)

**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**

# 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).

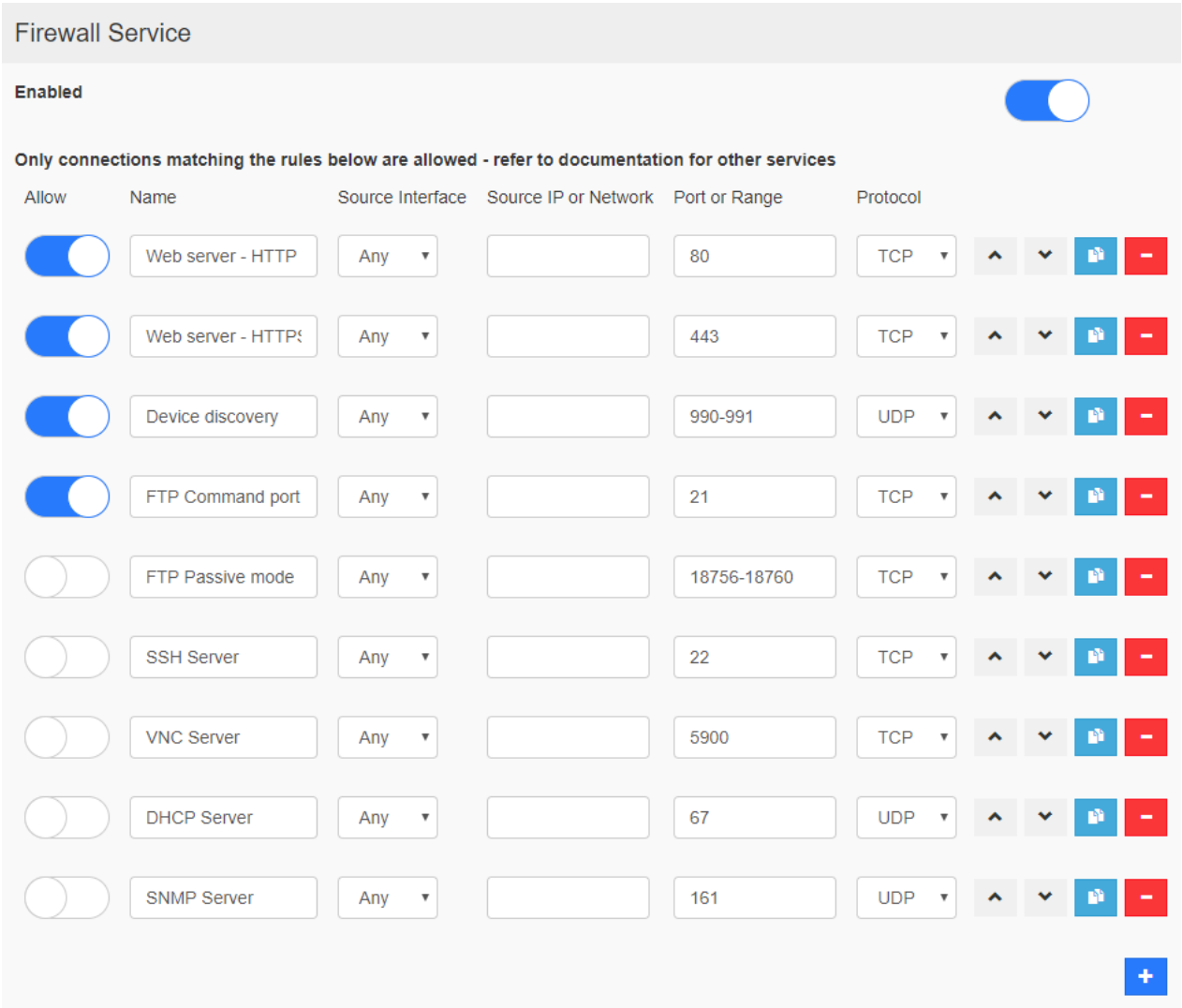
To obtain best performance, in addition of enabling the fast boot mode, it is recommended to:

- 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 JMobile 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 instead, JMobile 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 34).**

### 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.

# 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.

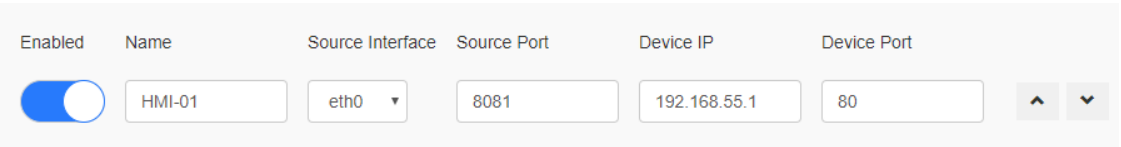
# Reserved CPU cores for applications

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

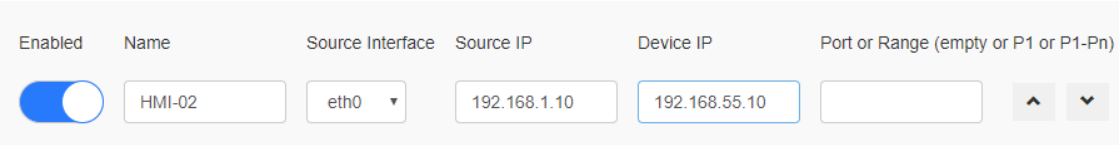



**Available from BSP v1.0.507**

### 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**

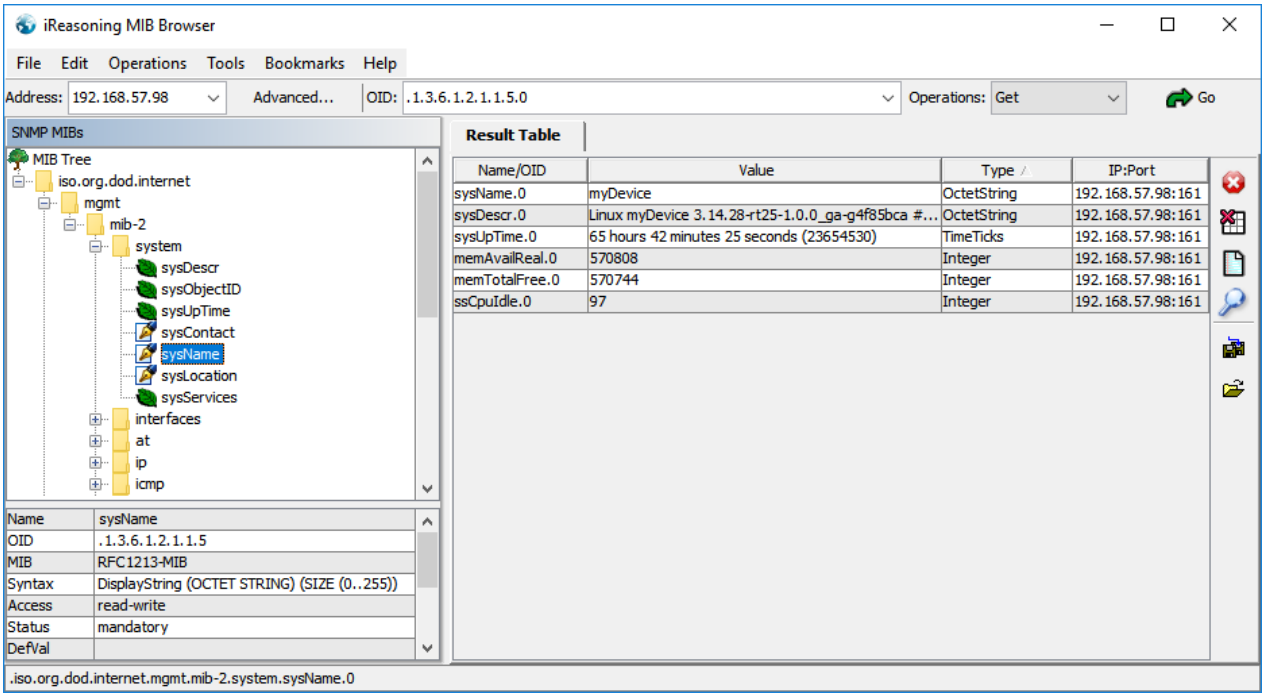
# Show loading bar during boot

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 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.**

# 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 |
| **Port** | VNC Server listens for connections on TCP port 5900 (default) |
| **Authentication** | When authentication is required, a password must be set to access the service |

**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.

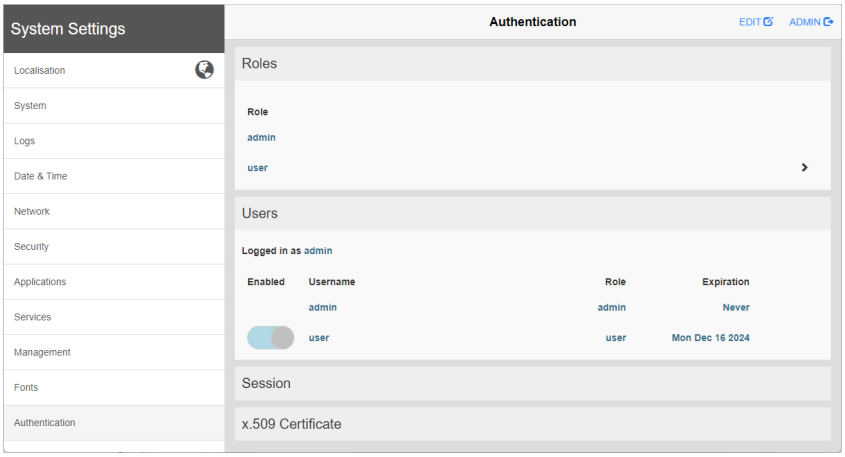
Note that passwords must include:

- 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. # ! @ ?)

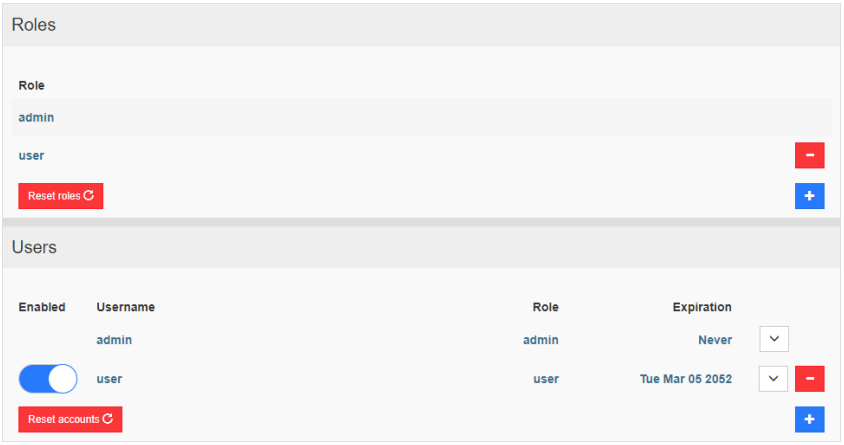
## Users and Roles

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.



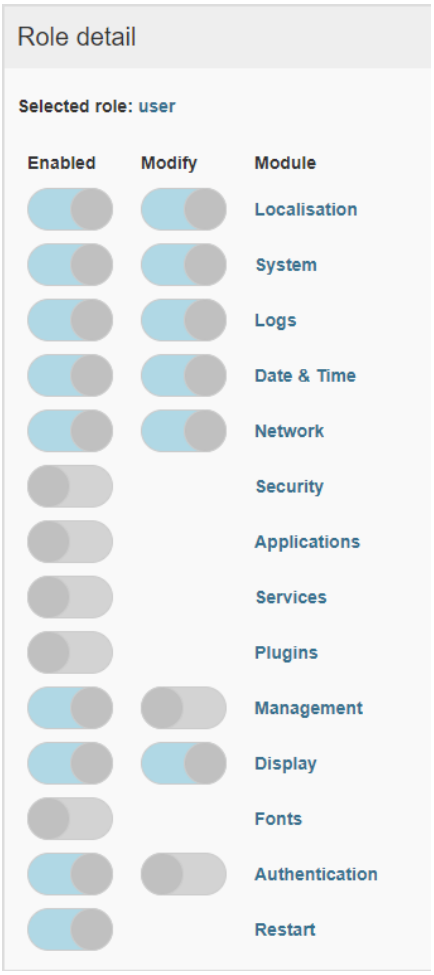

Clicking 'Reset Roles' will delete all existing roles. Please ensure that no roles are currently assigned to any users.

Clicking 'Reset Accounts' will delete all existing accounts.

### Roles

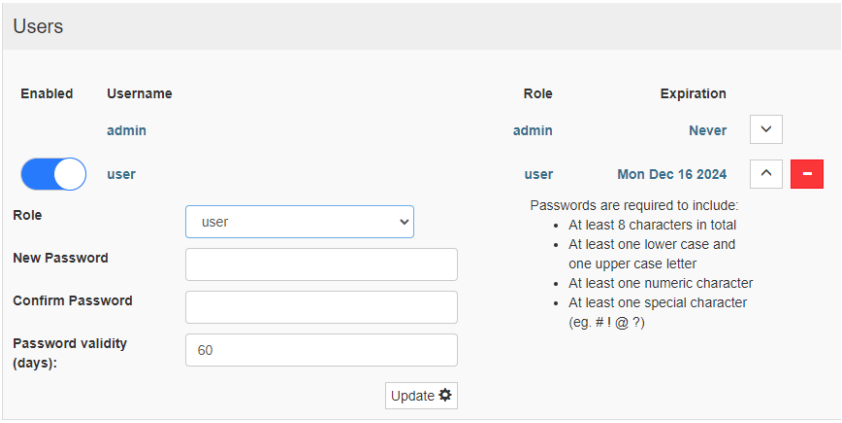
Click the "EDIT" button to add or remove a role, or click the role (">") to open the role definition.

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. |

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

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 (Ref.: "System Settings" on page 8)

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 9)."System Settings access via TAP TAP procedure " on page 9
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.: "System Settings" on page 8)

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.

# 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 8).

**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<br>• Username/ password<br>• Activation code (available only when the selected server type is "Cloud Server") |

| Parameter | Description |
|---|---|
| | • Certificate (available only when the selected server type is "OpenVPN")<br>• Certificate + username/ password (available only when the selected server type is "OpenVPN")<br>• 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.

## 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**

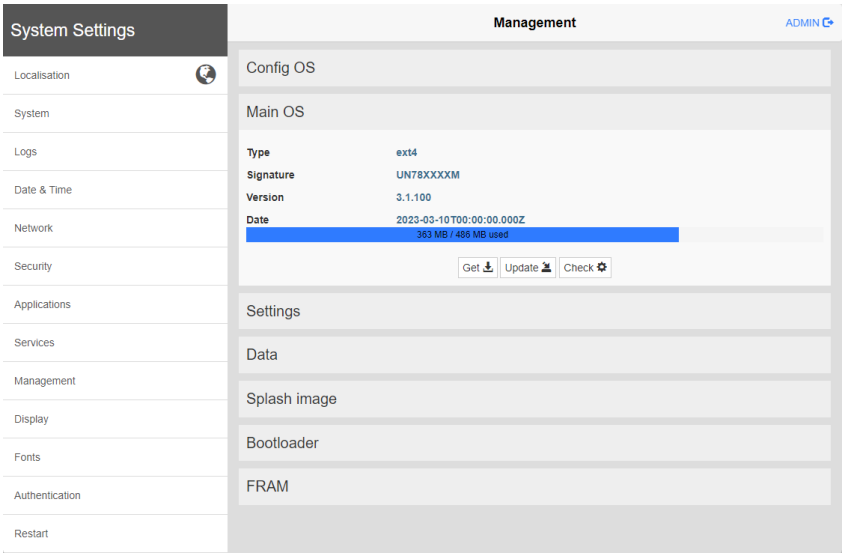
Please refer to openvpn.net for further details.

# 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).***

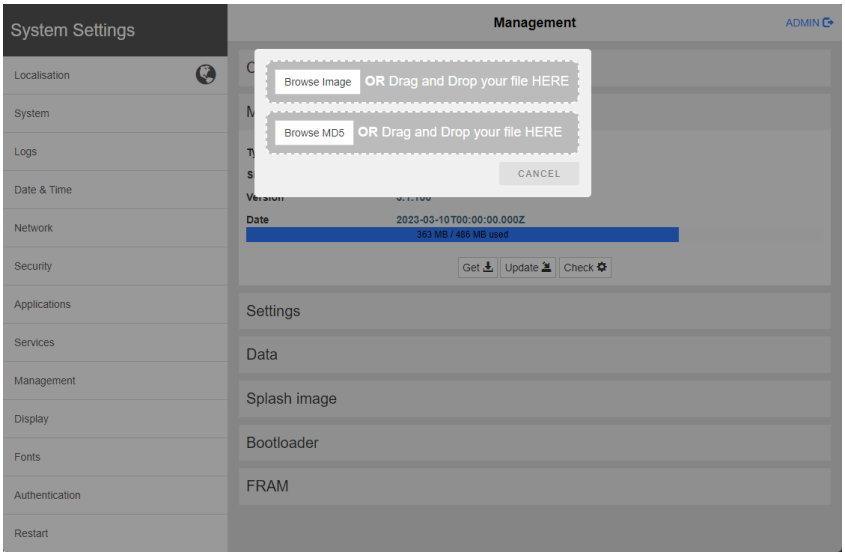
The system components of the Linux device can update locally using an USB memory key or remotely via web browser.

To update system components enter System Settings in Config OS mode 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]

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**

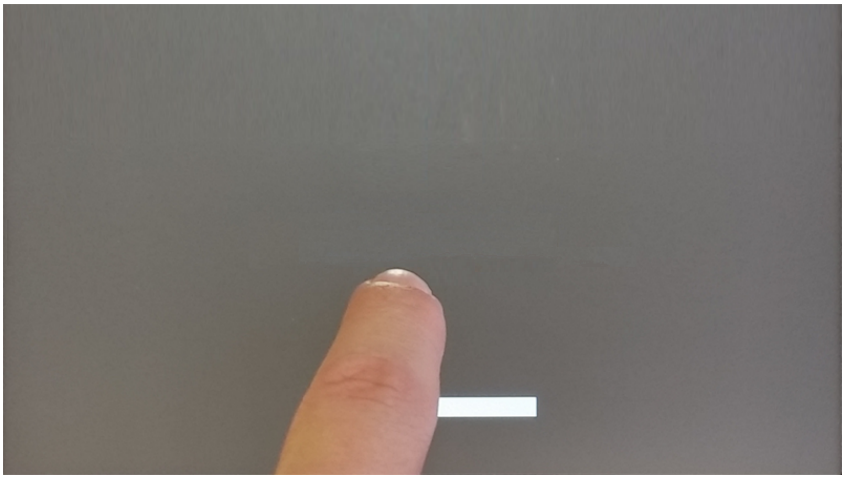
When available on the HMI device, you can "Get" or "Update" the FRAM data. To transfer FRAM data, the HMI device must be in OS Config mode, otherwise, the transfer will not take place.

**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 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”

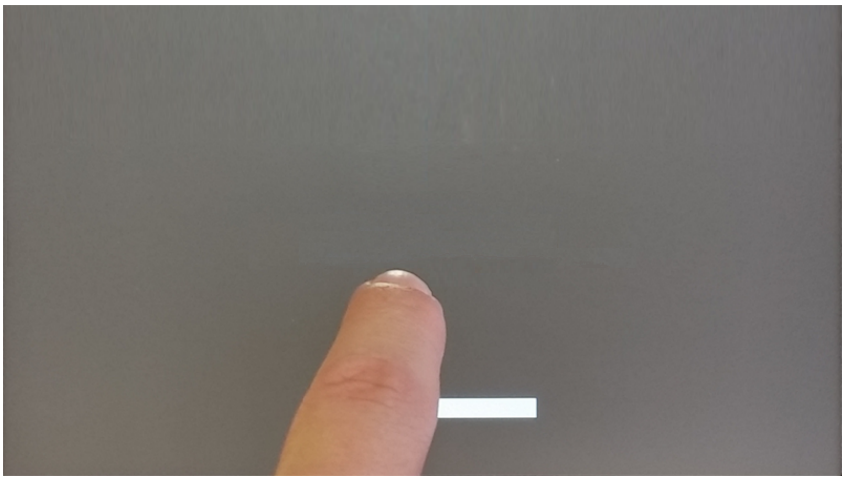

HMI will restart into System Settings in Config OS mode:


** TAP-TAP DETECTED 0 **
RESTARTING: CONFIG OS ...

# Touchscreen calibration

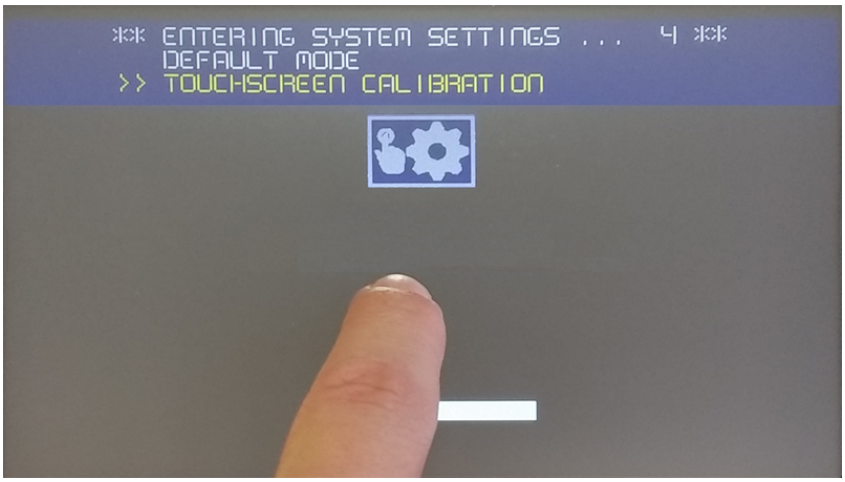
System Setting Calibration allows to calibrate Touchscreen device, can be accessed by tap-tap procedure (available only for resistive type displays).

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.

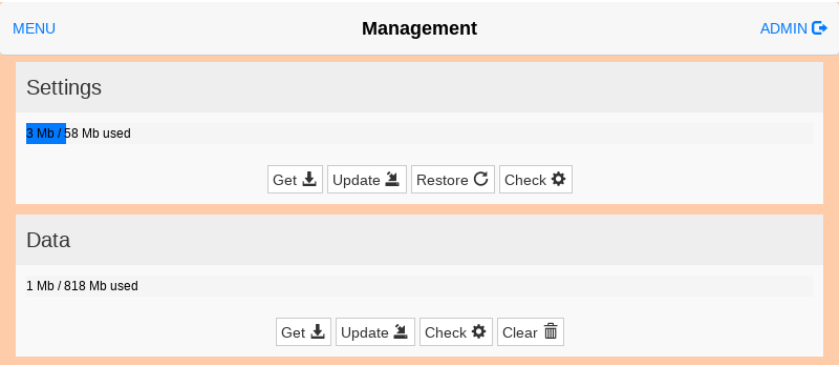
# Backup and Restore

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 9

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.

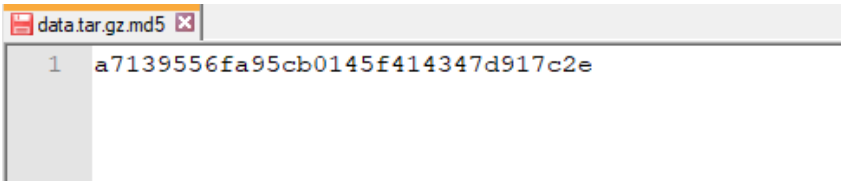
The MD5 checksum file must have the same name as the files that you want to load with the .md5 suffix as e.g.:

- 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

In the case that it is not even possible to boot the device, there is a special procedure to recovery the device by booting it in a special mode called configuration mode. From this mode you can open the device management dialog from where you can delete user data, restore system setting or update the firmware of the device.

To boot the device in configuration 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 time 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.

**Exor International S.p.A.**
Via Monte Fiorino, 9
37057 San Giovanni Lupatoto (Verona)
Italy

info@exorint.com
**phone**: +39 045 8750404
**fax**: +39 045 8779023

**HMI System Settings**
User Manual

2024-10-21

Copyright © 2010-2024