Web Browser on HMI device

User Manual

Version v83

Disclaimer

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

Web Browser for HMI Devices

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

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

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

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

Installation from USB Flash Drives

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

To install the web browser application follow this procedure:

1. Copy the application file to an empty USB Flash Drive
2. On the device select [Startup sequence], then [Install]
3. Double click on “mnt” to open the folder
4. Then double click on “usbmemory”
5. Select the web browser package
6. The runtime installation begins

Note: Supported file systems are FAT16/32 and Linux Ext2, Ext3 and Ext4.

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

Settings

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

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

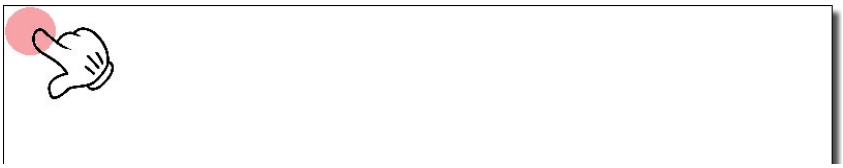
At first start up the browser will show System Settings as home page.

Logon is required to access System Settings. User name and password are same as for the HMI device (default admin, admin); they can be changed from System Settings.

For security reasons, it is highly recommended to change default password at first logon.

System Settings can be recalled using the settings button in the address bar

When the web browser is configured not to show the address bar, Systems Settings can be recalled keeping pressed the top left edge of the display for few seconds.



Web Browser

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

Property	Description
On Startup	Defines what the device should display when started.
Homepage	URL of the home page to load.
Fallback page	Secondary home page that is loaded when failed to load the primary home page. URL must include the protocol.
Enable toolbar	Show/hide the toolbar.
Allow downloading files	Enable/Disable 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.
Certificates	Open the web browser certificates manager. (Available only on local settings).
Certificate preferences	Clear all white listed sites . The action can be done in chromium from the toolbar (see: "Re-enable warnings" on page 6).
Use system virtual keyboard	When disabled, the system virtual keyboard is not shown. Keys can be entered from a physical keyboard or from virtual keyboards define on the active web page.
Enable form autofill	If enabled, the data previously entered are proposed when entering data.
Enable password management	When enabled, the browser will ask to save the entered passwords to repropose them the next time that you will try to log in to the same site.  **The option will be activated the next time the panel is restarted.**

For the complete list of available properties, refer to "System options" on page 7

The Toolbar

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

Available commands are:

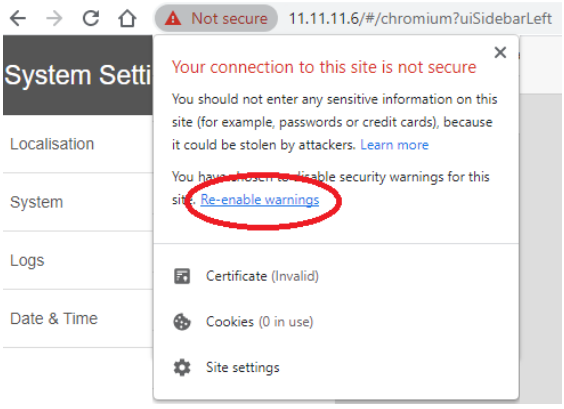
- Page Reload
- History Buttons
- Bookmark List
- URL Address
- Add Bookmark
- Open System Settings

Re-enable warnings

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

Note:

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



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

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

System options

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

Using command line arguments

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

Using settings file

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

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

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

Available System Options

Option	Description
--homepage=<uri>	Override homepage setting.
--enable-exit-button	Enables the "Exit" button in the options page and the "X" icon on the toolbar when enabled. Closes the web browser.
--enable-restart-button	Enables the "Exit" button in the options page and the "X" icon on the toolbar when enabled. Restart the web browser.
--enable-window-exit-button	Like above but only closes the window. In this case when starting again the web browser it will open a new window, which is faster. Command line flags given the first time can not be modified later as it is required a full restart for this. A different URL may be specified instead.
--enable-toolbar	Enables the toolbar. The setting is saved so it will be enabled the next time even without this option.
--enable-toolbar-navigation	Show the history navigation buttons in the toolbar
--enable-toolbar-on-error	Toolbar will be displayed only if there is an error loading the page. The setting is saved so it will be enabled the next time even without this option.
--fixed-toolbar	Toolbar will be fixed and will not be collapsed.
--disable-toolbar	Disables toolbar. The setting is saved so it will be enabled the next time even without this option.
--disable-toolbar-url	Removes URL text area from the toolbar. When used, the toolbar will no longer occupy the whole width of the screen and will be centered instead.
--enable-toolbar-bookmarks	Enables bookmark list and "Add bookmark" buttons on the toolbar when enabled. The "Add bookmark" button will still be hidden if --disable-toolbar-url is used. It won't enable the toolbar if disabled.
--disable-toolbar-options	Removes the options button from the toolbar. It will not enable the toolbar if

Option	Description
	disabled.
--disable-options	Like above but also disables the long press so that it is no longer possible to access the options page. On loading error the browser will continue to retry and also in this case the options page is never opened.
--disable-toolbar-reload	Removes the reload button from the toolbar
--loadingPage=<URL>	Specified to show a custom page that will load at boot while the actual page is being loaded. This will also hide default error page if the server is not 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. http://, 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. http://, file://)
- customUserAgent=<userAgent>
- showToolbarOnError=<true|false>
- showWiFiStatus=<true|false>
- showHistoryButton=<true|false>
- showLoadingBarAndStopButton=<true|false>
- onStartup=<settings|homepage|lastVisistedPage>
- enableToolbar=<true|false>
- holdTimer=<ms>
  Timeout in ms for long press, minimum 2000 (2s)
- fallbackToDefaultPageLink=<url>
  URL must include the protocol (i.e. http://, file://)
- disableFallbackReload=true

Example for file browser.ini

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

System Configuration

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

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.

Administrator username with full access right is "admin" with default password "admin". Generic username is “user” with default password “user”

WARNING: For security reasons, change the default passwords for both usernames (passwords can be modified from the “System Settings -> Authentication” command)

Accessing at the system settings from the HMI device do not require to enter a password until the default "admin" password is not changed.

Enter in System Settings

There are several ways to access the System Settings page.

You can enter

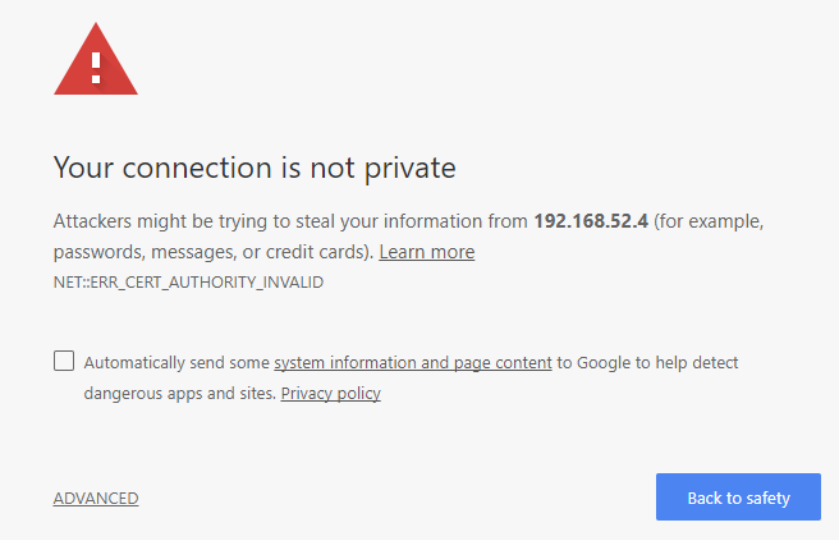
- From a web browser
- From the HMI device when no runtime is load
- From the HMI device using the tap-tap procedure

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.



Default security protocols proposed by the HTTPS server in the Linux HMI device are:

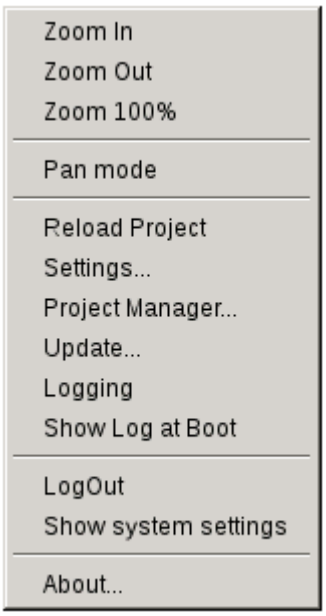
- SSLv3 256 bits ECDHE-RSA-AES256-SHA
- TLSv1 256 bits ECDHE-RSA-AES256-SHA

WARNING: We discourage usage of CBC cyber suites in the context of SSL3 or TLSv1.0 connections since potentially affected by some vulnerabilities.

System Settings access from HMI device

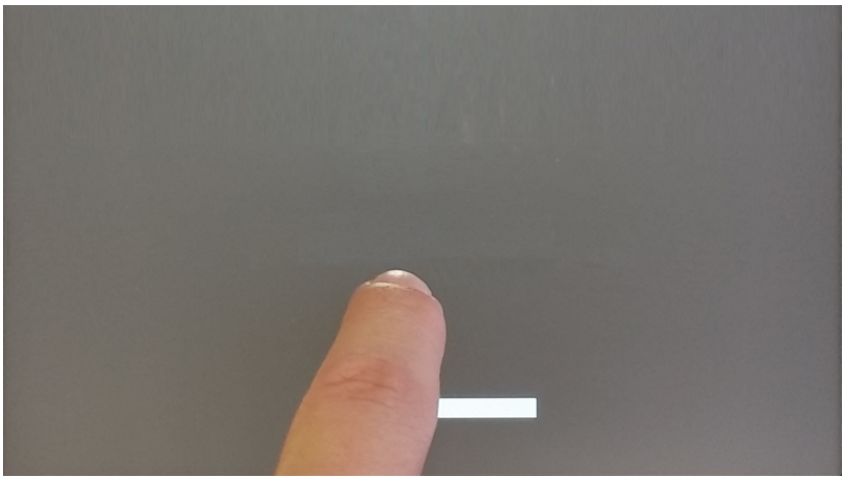
When Runtime is not installed, the System Settings is accessible from the Runtime Loader screen,

When Runtime is installed the System Settings is accessible selecting “Show System Settings” option of Context Menu,



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

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)
PlugIn	Hardware plugins information

Logs

Set the persistent log option if you want maintain the log files saved after a power reset.

Use save button to export a copy of the log files.

The log files manager cyclically fill 3 files of 4Mb

Date & Time

Device date and time.

Parameter	Description
Current Timezone	Timezone region
Current Date **Local Time**	Date and Time can set manually only when the Automatic Update is disabled.
Automatic Update (NTP)	Enable to keep date and time synchronized from a remote server • NTP Server Specify the Internet NTP Server address  The NTP Client of the HMI Device is a complete implementation of the Network Time Protocol (NTP) version 4, but also retains compatibility with version 3, as defined by RFC-1305, and version 1 and 2, as defined by RFC-1059 and RFC-1119, respectively. The poll process sends NTP packets at intervals determined by the clock discipline algorithm. The process is designed to provide a sufficient update rate to maximize accuracy while minimizing network overhead. The process is designed to operate in a changeable mode between 8 sec and 36 hr.
Accept NTP requests	When enabled the device will accepts NTP requests from outside. When automatic update is not enabled the device will share the local RTC clock time.

Networks

Network parameters. Available parameter in edit mode:

Parameter	Description
General Settings	Device hostname Avahi Hostname (see "Avahi Daemon" on page 24)
Network Interface	Network parameters of the available interfaces • DHCP • IP Address • Net Mask • Gateway  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 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 • System This space is used from the services embedded in the device (e.g. the VNC Server) • HMI Runtime This space is used from the 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. • 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.

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

Services are available only when logged as admin.

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

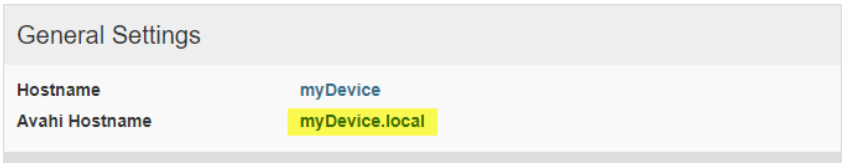
Autorun scripts from external storage

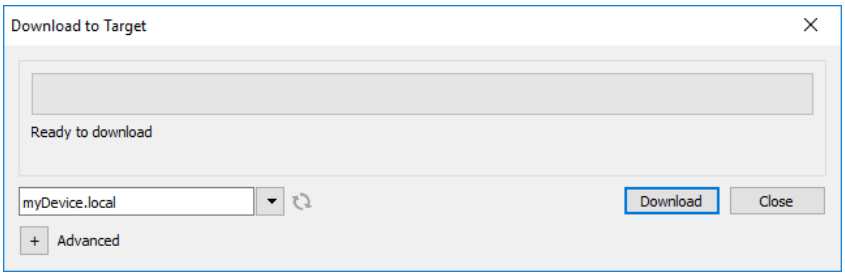
Enable/Disable the possibility to run the "autoexec.sh" script file when a USB key is plugged into the device. Disable this service if you want to prevent unauthorized access through the USB interface.

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).





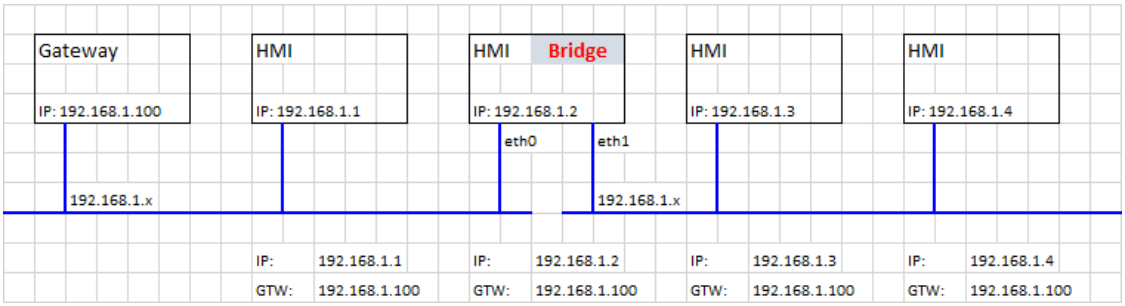
Avahi Daemon runs on UDP port 5353

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 38 for additional details.

DHCP Server

Provide the DHCP Server on the selected interfaces.

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

Enable device restore via TAP TAP option

When enabled, it gives the possibility to reset the operator panel in case the administrator password is forgotten. (See.: "Forgot password" on page 1)

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 1)

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).

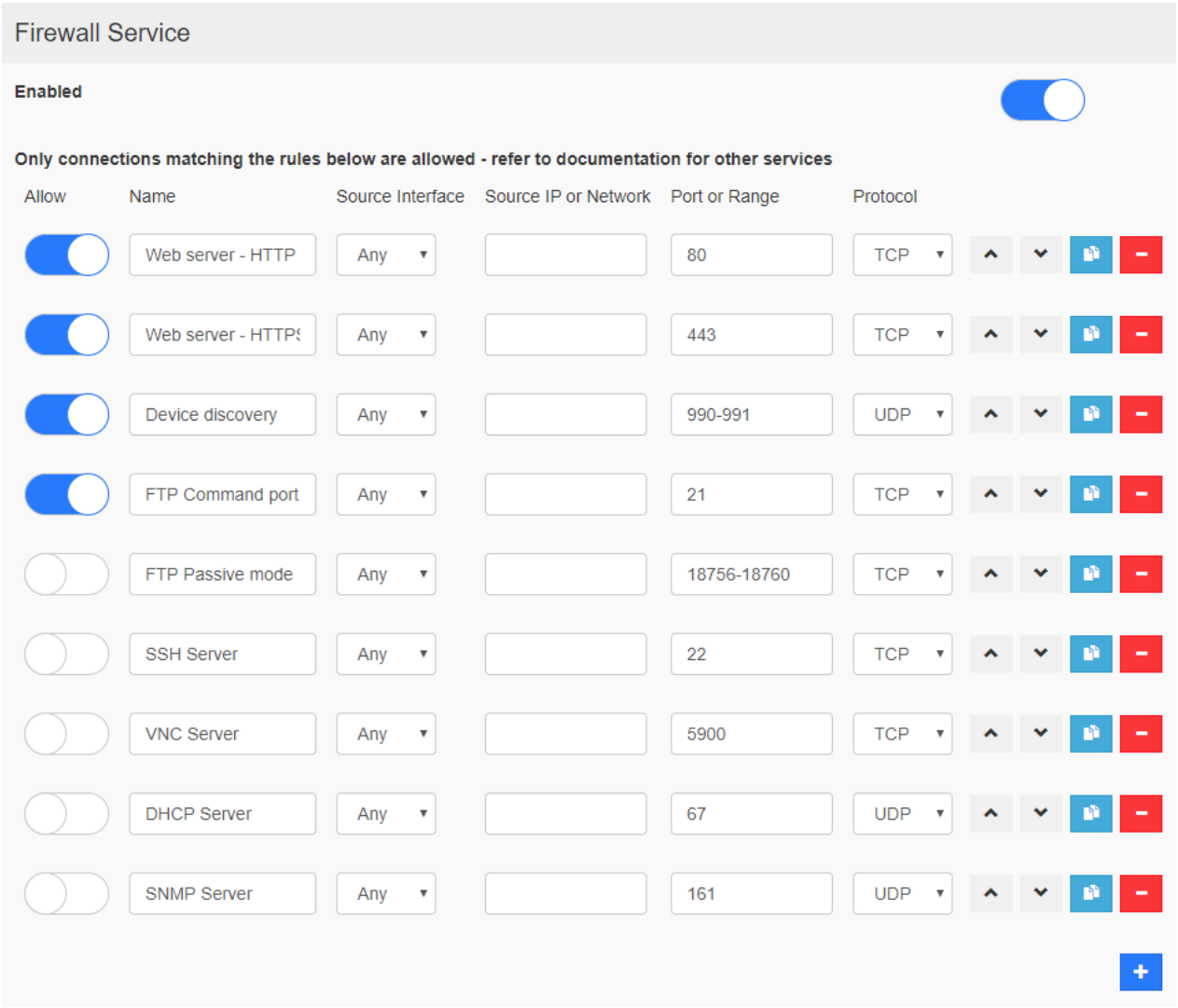
To obtain best performance, in addition of enabling the fast boot mode, it is recommended to:

- 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

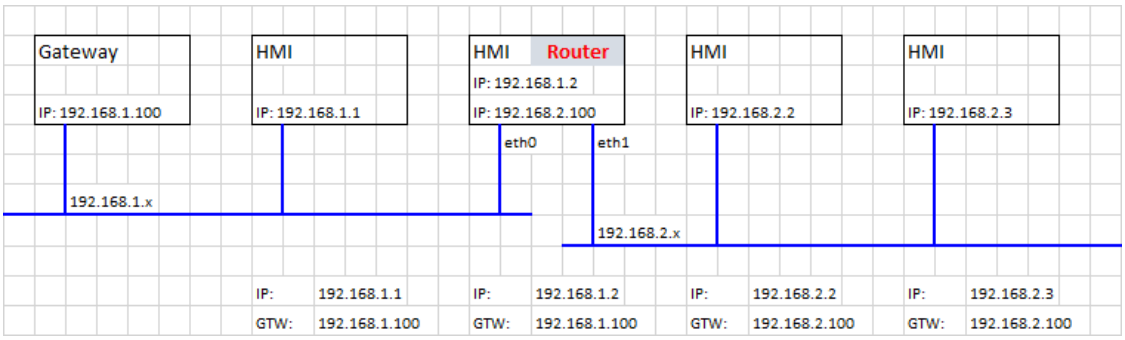
If this field is unspecified, access will be allowed from any source host. Otherwise, access can be restricted to a single IP address (e.g. 192.168.100.123) or a range of IP addresses in CIDR format (e.g. 192.168.100.0/24). For details on valid subnet specifications following such format, please refer 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 1).

Router Service

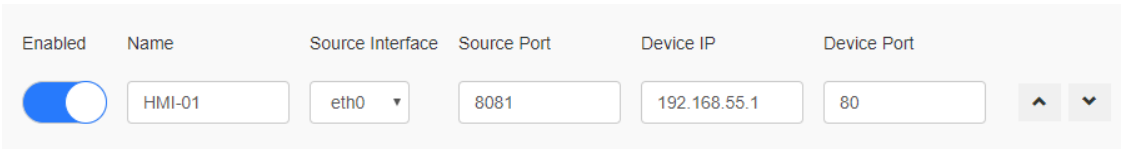
This service uses IP Forwarding and Network Address Translation to share the connection from WAN (eth0) towards LAN (eth1 or eth2): connected endpoints may reach the same networks reachable by the gateway (including Internet if available). With Cloud Service active, endpoints can be reached via the gateway's LAN port (please refer to "Cloud / VPN Service" on page 38 for more information)



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

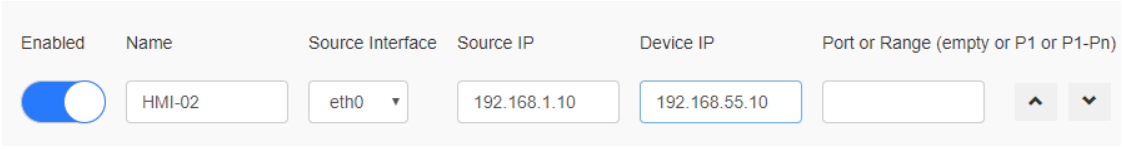


Available from BSP v1.0.507

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

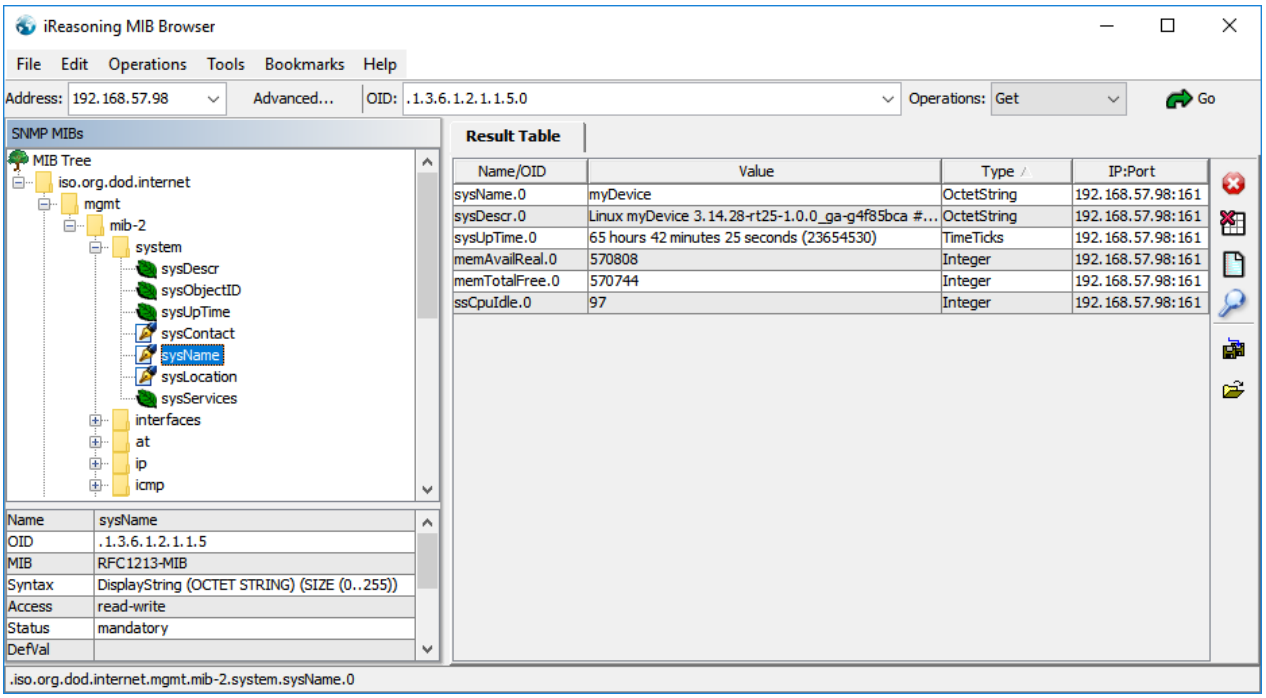
Show loading bar during boot

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

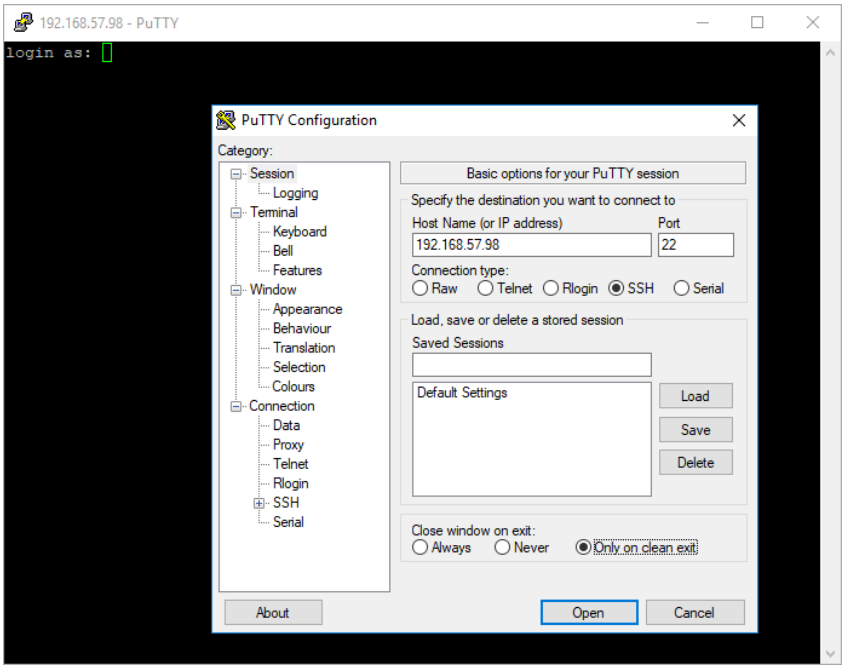
SNMP Server runs on UDP port 161

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

SSH Server

SSH service has been designed only for advanced users. It 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.

The default password for the username the admin is “admin”. See the "Authentication" on page 36 chapter to additional information.



SSH Server runs on TCP port 22

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.

VNC should be disabled after use and autostart is not recommended.

Parameter	Description
Enable	Enable the VNC server
Autostart	Keep the VNC server enabled when HMI device starts
Port	VNC Server listens for connections on TCP port 5900 (default)
Inactivity timeout (seconds)	“Inactivity timeout” occurs if no user interaction is detected (via keyboard, mouse, transfers or other RFB protocol interactions). The special value 0 indicates that idle timeout is disabled. Default value is 600 (10 minutes).
Multiple clients	Allow multiple sessions on the same port (if disabled, previously logged clients are disconnected upon a new incoming connection)
View only	Do not allow active user interactions (clients can only watch)
Encryption	Activate SSL encryption of connections **Custom certificate (Security/VNC KeyPair)** The HMI device certificate that is necessary to permit the remote VNC client to verify the authenticity of the HMI device. The certificate must contain both the private and the public keys and can be .pem format. **The encryption features are not widely supported, check your VNC client compatibility**
Authentication	Whether users are authenticated upon session creation. A custom VNC specific password can be set or system passwords can be used (this option is only available if also Encryption is enabled)

Example of how to generate a certificate using OpenSSL library:

```
@echo off set OpenSSL="C:\Program Files\OpenSSL-Win64\bin\openssl.exe" set
CertificateName=HMI-Certificate set DeviceIP=192.168.1.56 rem Create the certificate
keys %OpenSSL% req -x509 -newkey rsa -days 365 -nodes -keyout private.pem -out
public.pem -subj "/ST=NY/C=US/L=New
York/O=CompanyName/OU=Department/CN=%CertificateName%" -addext
"subjectAltName=IP:%DeviceIP%" rem Create .pem file copy private.pem + public.pem hmi-
certificate.pem echo. echo. pause
```

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)

Plugins

This page will show the parameters available to configure the optional plugins modules attached to the HMI device. See the description of the each plug-in module to additional information.

Management

Management is available only when logged as admin.

From the management area is possible "Update System Components" of the HMI device.

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.

Use the “Clear” command inside the “Data” section to remove HMI Runtime from the device

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

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

Users

There are two usernames:

- Administrator username with full access rights is **"admin"**
- Generic username with basic access rights is “**user**”

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

Required BSP v1.0.239 or greater

Restart

HMI device restart command

EXIT

Exit from the System Setting tool.

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 12).

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 Cloud server to use (available only when the selected server type is "Cloud Server")
Files	Allows you to upload VPN configuration files (available only when the selected server type is "OpenVPN")
Authentication	Select from the available authentication modes • Username/ password

Parameter	Description
	• Activation code (available only when the selected server type is "Cloud Server") • Certificate (available only when the selected server type is "OpenVPN") • Certificate + username/ password (available only when the selected server type is "OpenVPN") • None (available only when the selected server type is "OpenVPN")
Username	Enter the username of the remote server account
Password	Enter the password of the remote server account
Show Password	Displays the typed characters on the password

Cloud Server

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

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

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

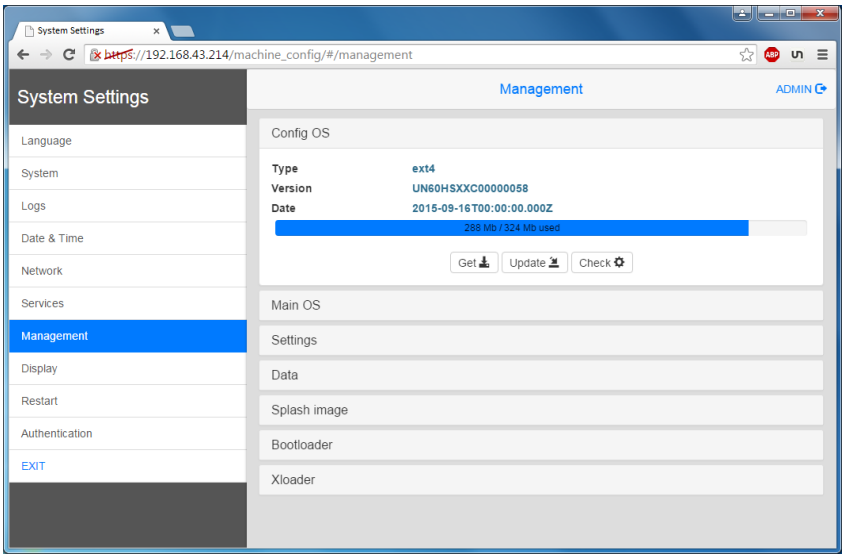
Please refer to OpenVPN documentation for further details.

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).

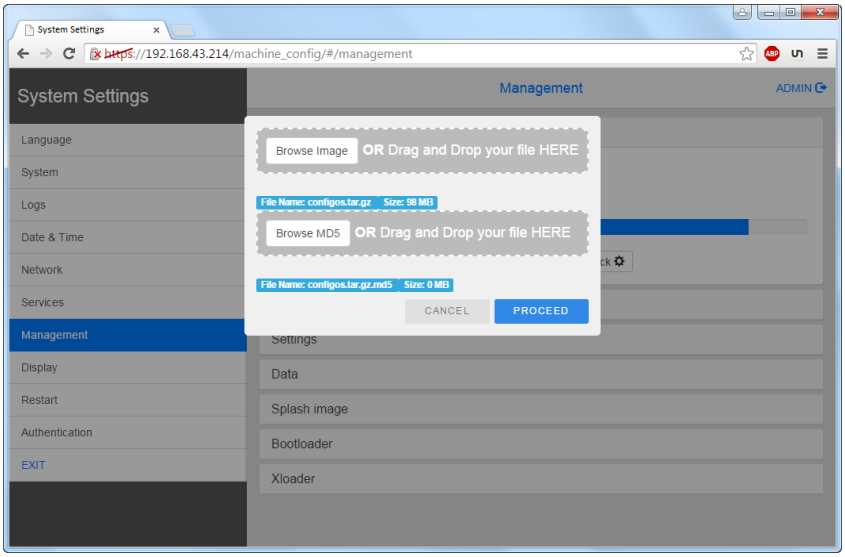
The system components of the Linux device can update locally using an USB memory key or remotely via web browser.

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]

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.



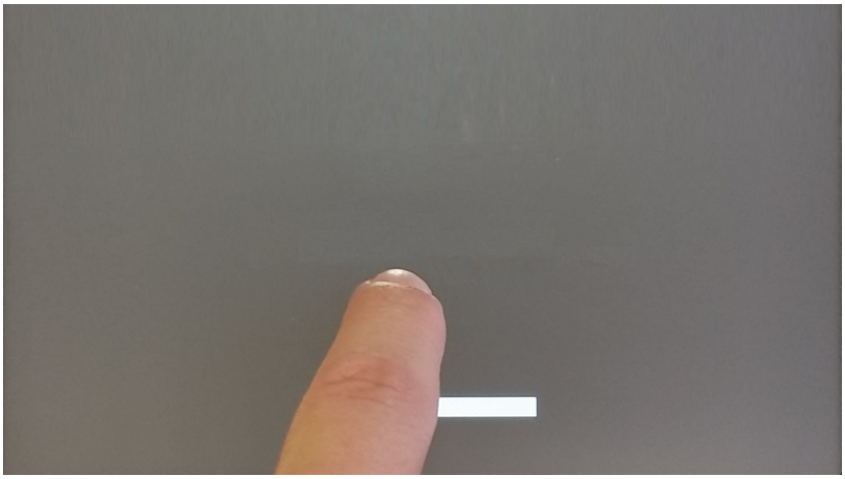
Important: Do not turn off the device while a system component is being upgraded.

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”

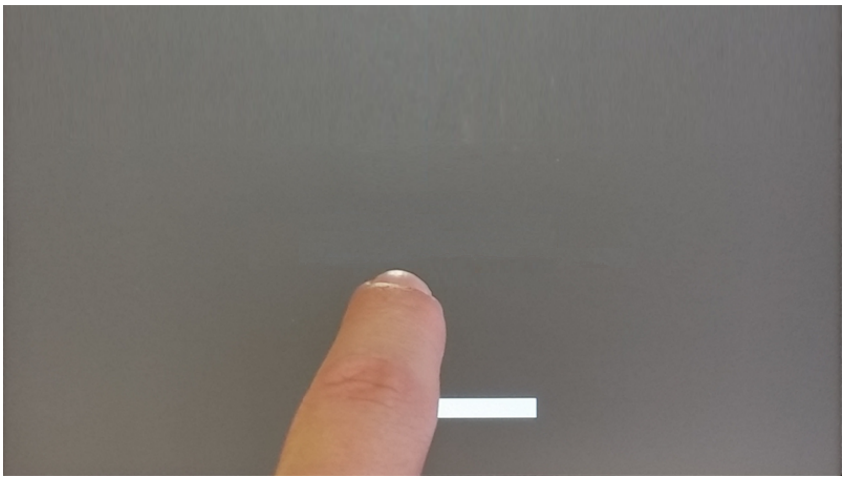
HMI will restart into System Settings in Config OS mode:


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

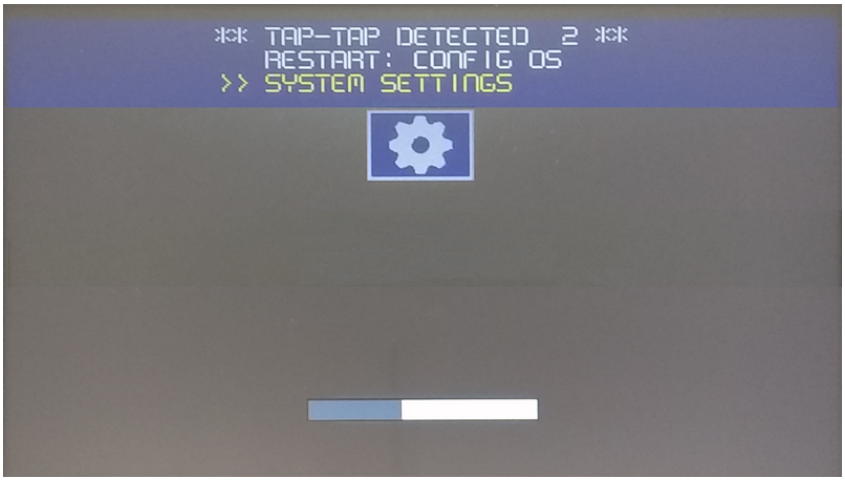
Touchscreen calibration

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

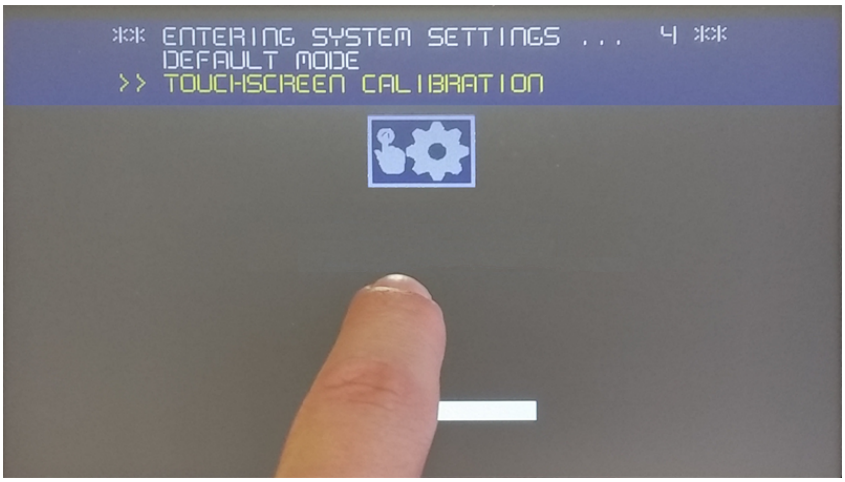
Tap-tap consists in a sequence of several touch activations by simple means of the finger tapping the touch screen performed during the power-up phase and started immediately after the HMI is powered on.



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.

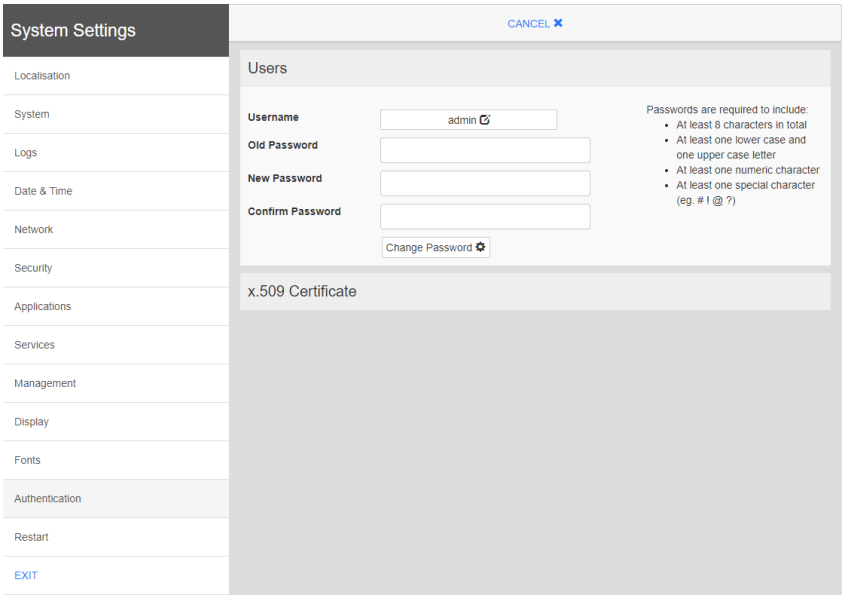
Password protection

Internal password of the HMI device.

From the Authentication tab, inside the "System Settings" on page 12, activate the edit mode and select the username to change the associated password.

There are two usernames:

- Administrator username with full access rights is "**admin**"
- Generic username with basic access rights is "**user**"



If you forgot the password, check the "Forgot password" on page 1

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 for both users (admin and user)

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. # ! @ ?)

Forgot password

If you have forgotten the admin password, you have the possibility to reset it to the "*admin*" value. Note this procedure will erase the entire memory of the HMI device and any previously downloaded project will be removed.

TAP TAP option

The procedure is available only if it has not been explicitly disabled through the "Enable device restore via TAP TAP option" available in the device system settings (Ref.: "Enable device restore via TAP TAP option" on page 25)

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.: "Password protection" on the previous page).
3. When "TAP TAP" is detected select "System Settings" on the first menu, "Default mode" on the second menu, and finally "**Device restore**" on the third menu.

USB option

The procedure is available only if it has not been explicitly disabled through the "Enable device restore via USB option" available in the device system settings (Ref.: "Enable device restore via USB" on page 26)

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.

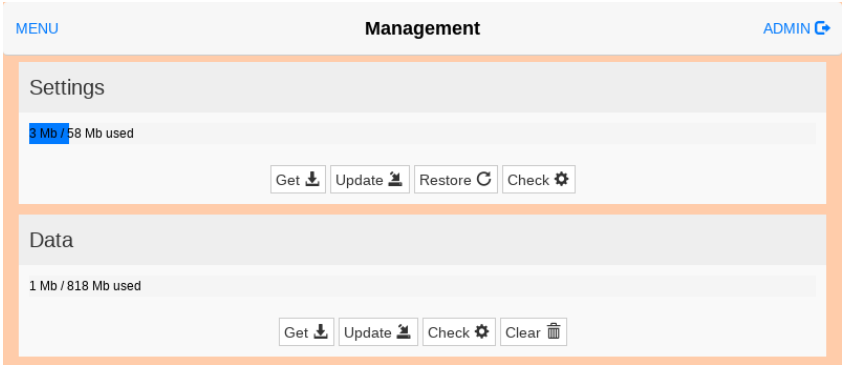
Backup and Restore

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 "Enter System Settings in Config OS mode via tap-tap procedure " on page 1

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.

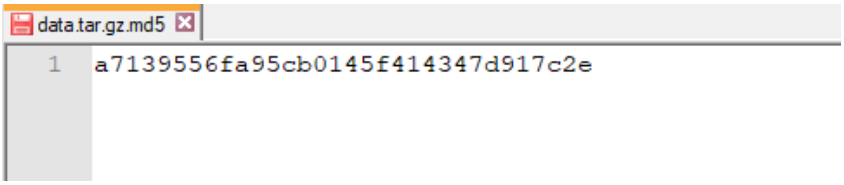
The MD5 checksum file must have the same name as the files that you want to load with the .md5 suffix as e.g.:

- 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.



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

Web Browser on HMI device
User Manual

v83
2023-02-10