

## boss Family– Frequently Asked Questions (FAQ)

<b>1. System administration</b> .....	<b>2</b>
1.1. Supported browsers for the usage of the System Administration interface .....	2
1.2. Supported printers .....	2
1.3. Wi-Fi network passphrase.....	4
1.4. System administration user passwords.....	4
1.5. Supported memory devices .....	4
1.6. Backup and restore.....	4
1.7. Supported 2G/3G modem for sending SMS messages .....	6
1.8. Supported Touch Screens .....	6
1.9. Set custom resolution for optimized display via monitor (function available only in boss mini advanced) .....	7
<b>2. Software functions</b> .....	<b>9</b>
2.1. Registration of the unit .....	9
2.2. Registration of plugins .....	9
2.3. Telegram channel configuration for notifications .....	10
2.4. Import/export site configuration.....	11
2.5. Internal relay management .....	13
2.6. "Remember me" option: how to keep a user session always active .....	15
2.7. How to show groups of devices for specific user profiles .....	16
2.8. Meaning of acknowledge, cancel and inhibition of alarms.....	16
2.9. Information on the Modbus TCP/IP communication as a client.....	17
2.10. Datalogging Frequency/Depth table .....	18
2.11. Update of c.pCO software through the supervisor .....	19
<b>3. Connectivity</b> .....	<b>21</b>

**CST** Technical support |  FAQ

3.1.	Access through the integrated Wi-Fi.....	21
3.2.	Access through the temporary IP Address (available only for boss mini).....	22
3.3.	Internet access .....	23
3.4.	File transfer via FTP (only for boss not boss mini).....	24

It is premised that in this document with the term **supervisor (s)**, we will refer to **both boss** and **boss mini**. The specific names will be used only if differentiations are necessary.

## 1. System administration

### 1.1. Supported browsers for the usage of the System Administration interface

The web interface of the System Administration is compatible with the following browsers: Chrome, Firefox both on the desktop and mobile versions. Instead Internet Explorer and Edge are not supported.

#### [Back to index](#)

### 1.2. Supported printers

The supervisor is compatible with all printers supporting PostScript protocol (also in emulation mode). The printers can be connected to the supervisor both via USB and the network.

#### **USB Printers**

For USB connections, the printer is automatically recognised by the system and the supervisor automatically uses a generic driver.

#### **Network Printers**

##### **a) boss Machines with SW rev $\geq$ 1.2.0 and boss mini (all the SW rev.)**

The boss machines with SW rev  $\geq$  1.2.0 and boss mini (all the SW rev.), support all the PostScript printers (also in emulation mode) with network protocol LPD. It is not necessary to use a print server. The configuration mask is reported below:

CST Technical support | ? FAQ

Local printer   Windows printer   **Network printer**

Local printer name

Printer name or IP Address

Queue name

**boss Machines with SW rev < 1.2.0**

For boss machines with SW rev < 1.2.0, the network printers management needs the usage of a print server. The print server is required because it contains the drivers needed to print.

The configuration screen is shown below, please note that all the fields are required:

boss Add printer

SUPERVISORY APPLICATION  
 boss supervisory application

GENERAL  
 Backup & Restore  
 Dashboard  
 Language  
 Passwords  
 System update

SOFTWARE  
 Security services

SYSTEM  
 Date & time  
 Diagnostics  
 Keyboard  
 Network config  
 Power  
 Printers  
 Add printer  
 Jobs

Local printer   **Network printer**

Local printer name

Workgroup

Server

Printer

Username

Password

## Technical support | FAQ

For any printing issues contact [sw.support@carel.com](mailto:sw.support@carel.com) for further info.

### [Back to index](#)

#### 1.3. Wi-Fi network passphrase

When first powering on the unit, the passphrase is empty but during the first start-up procedure this will be set by the administrator to a string with 8 chars minimum length.

### [Back to index](#)

#### 1.4. System administration user passwords

The passwords of System Administration users are set by the *administrator* user during the first start-up procedure. Therefore there are no default passwords. The passwords can be changed from the System administration web interface in the *General/Passwords* session.

The *administrator* user can change their own password as well as those of the *maintainer* and *user*.

The *maintainer* user can change their own password as well as that of the *user*.

The *user* can only change their own password.

#### 1.5. Supported memory devices

The following memory devices are managed by boss for import and export operations:

- microSD to be inserted into the dedicated slot for boss
- SD for boss mini
- USB devices formatted to vfat, ext3, ext2, ext4, squashfs, iso9660, udf, fuseblk, fat12, fat16, fat32 (not: exFAT, NTFS)
- 

### [Back to index](#)

#### 1.6. Backup and restore

In System administration it is possible to create, restore and schedule backups.

Users can find all the backup and restore functions in the **GENERAL\ Backup & Restore** section.

Three tabs are available:

## CST Technical support | FAQ

- **Backup**

The user can choose whether to export the backup:

- to a USB/SD device directly connected to the supervisor (even if the backup is created remotely).

- Only for boss: to the internal **ftp** folder (see paragraph 3.2 for further info on boss ftp server). The folder ftp is not present in boss mini.

The following types of backups are available:

- *Full backup*: contains all the configurations (lines, rules configured in the Activity section, users), models, logged data, alarms/events, reports archive, maps and custom device detail pages, site images, any registered plugins (to be registered again on the new unit after importing).
- *Configuration backup*: contains all the configurations (lines, rules configured in the Activity section, users), models, maps and customised device detail pages, site images, any registered plugins (to be registered again on the new unit after importing); no logged data are included.
- *Service backup (only for boss)*: backup for analysis purposes which can be useful for Carel assistance (not available in boss mini).

- **Restore**

*Full backups* and *Configuration backups* can be restored with this procedure.

The user can choose whether to restore the backup from a USB/SD device connected directly to the supervisor or in case of boss from the internal **ftp** folder (not present in boss mini). For boss machines with SW rev.  $\geq 1.1.0$  and boss mini (all SW rev) when accessing remotely it's also possible by the button **UPLOAD** to upload and import a Full Backup saved into the remote PC's file system.

- **Schedule**

From here users can enable and schedule backups, specifying the destination (SD, USB memory, ftp for boss), date and time.

Compatibility: there is no compatibility between Full Backup/Configuration Backup exported from boss to boss mini and vice versa.

For SW rev inferior than 1.4.0: Full Backup or Configuration backup can be imported only on units having exactly the same software version of the backup.

Starting from SW rev 1.4.0: Full Backups from machines with SW rev  $\geq 1.3.0$  can be imported on units with SW rev  $\geq$  of the backup. However, the restriction of the same version remains for the import of Configuration Backup.

Examples:

- 1.4.0  $\leftarrow$  1.3.0 (full backups of version 1.3.0 can be imported, NO of prevision versions)
- 1.5.x  $\leftarrow$  1.4.x / 1.3.0 (full backups of versions 1.4.x and 1.3.x can be imported)
- 1.6.x  $\leftarrow$  1.5.x / 1.4.x / 1.3.0 (full backups of the 1.4.x, 1.5.x and 1.3.0 versions can be imported)

## Technical support | FAQ

For further information on the procedure, please see the Video FAQ **System Administration backup.mp4**.

The supervisor also gives users the possibility to backup the Supervisor application. See "[2.4 – Import/export site configuration](#)" for further information.

[Back to index](#)

### 1.7. Supported 2G/3G modem for sending SMS messages

SMS delivery management is available in boss starting from SW revision 1.1.0 and in all the SW rev of boss mini.

The supported modem is USB model "**MULTITECH MTC-H5-B03-KIT**" with Carel Code **BMHSTMDA00**. All the documentation is available at the following link: <https://www.multitech.com/models/92506950LF>.

[Back to index](#)

### 1.8. Supported Touch Screens

boss **with SW rev** >= **1.2.0** and **boss mini** >= **1.0.3**:

- support of the 17" touch screen with Carel code **BMHSTMNA00** (available in boss from SW rev 1.1.0; documentation available at the link: <https://www.lg.com/it/supporto/supporto-prodotto/lg-17MB15T#manuals>).
- full support of 'single touch' touchscreens with eGalaX chip; to verify the chip used by the monitors, you can consult any reference sites as [http://touch-base.com/touch\\_device\\_list.asp](http://touch-base.com/touch_device_list.asp) (available in boss from SW rev 1.2.0)
- support of the touchscreen multitouch '**iiyama prolite t1731sr**' (available in boss from SW rev 1.2.0 and boss mini from SW rev 1.0.3; documentation available at the link: [https://iiyama.com/it\\_it/products/prolite-t1731sr-b1/](https://iiyama.com/it_it/products/prolite-t1731sr-b1/)).
- Generally increased the support with the 'multitouch' touchscreens with eGalax chip, nevertheless the compatibility with all models based on this chip is not guaranteed. In case you decide to use another model, a connection test between the touch and the supervisor has to be performed by the user. In case of failure it is not possible to install any driver or change the supervisor to make it compatible

## Technical support | FAQ

with the tested monitor model (available in boss from SW rev 1.2.0 and boss mini from SW rev 1.0.3).

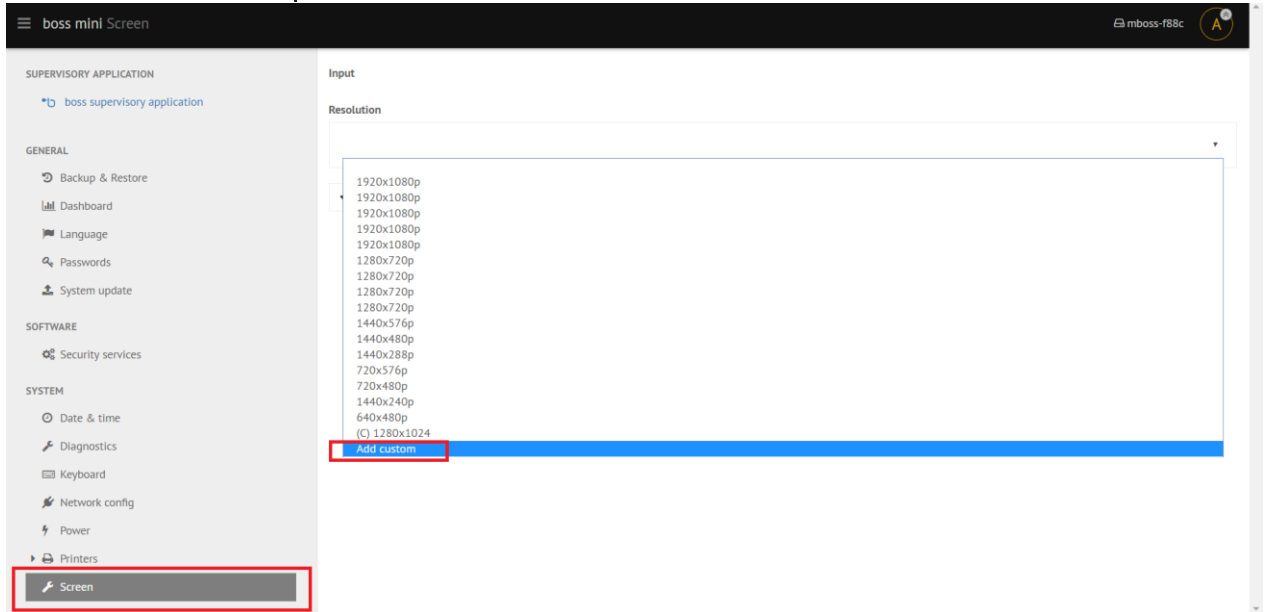
[Back to index](#)

### 1.9. Set custom resolution for optimized display via monitor (function available only in boss mini advanced)

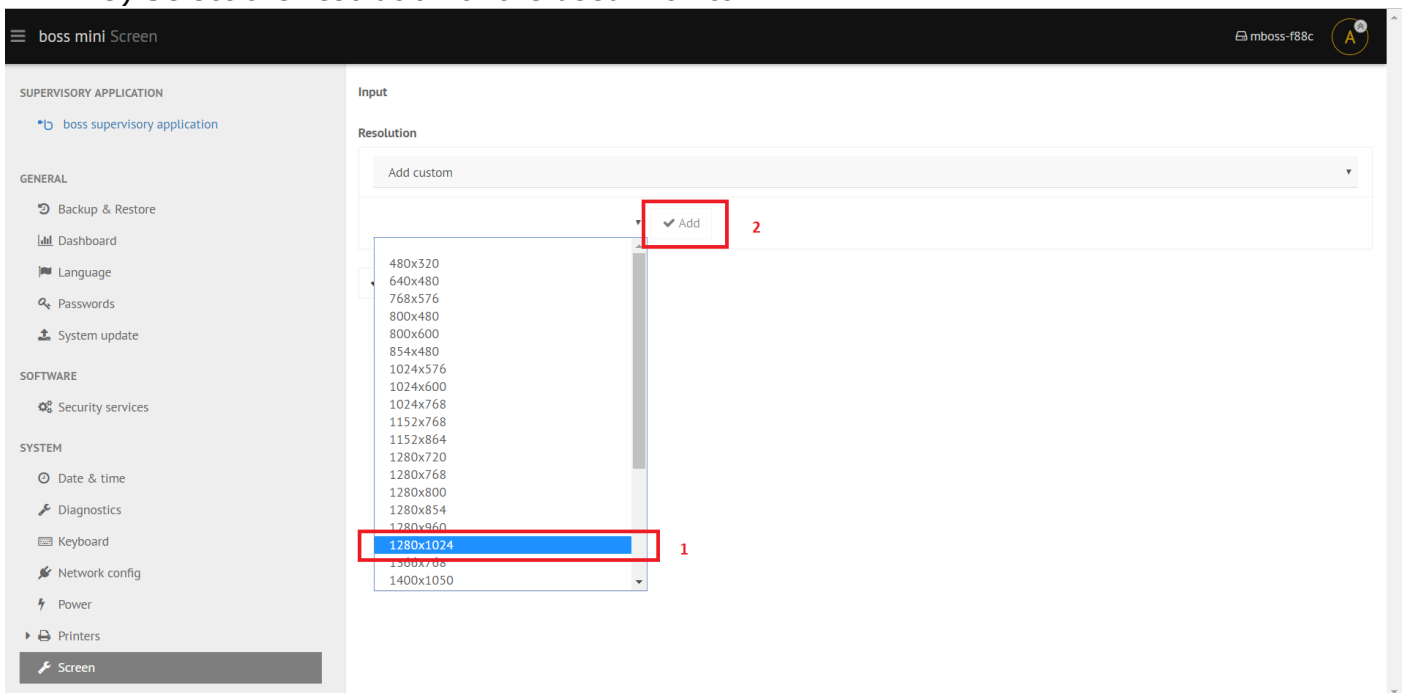
In case of non-optimal display or no video signal via the connected monitor, it is recommended to try to set in boss mini the custom resolution suitable for the screen in use. If it is not possible locally, through the monitor itself, the procedure can be performed via Wi-Fi or network.

Here are the necessary instructions:

- 1) identify the resolution in the monitor's technical specifications. For example, the resolution of the BMHSTMNA00 monitor (paragraph 1.8) is 1280 x 1024.
- 2) Access the boss mini **System Administration** interface, select the **Screen** item and then click **Add custom** resolution:



### 3) Select the resolution of the used monitor:



[Back to index](#)



## 2. Software functions

### 2.1. Registration of the unit

boss does not need to be registered.

For boss mini when first starting up, it is necessary to insert the activation code shown on the label on the right side of the machine. However, no registration is required on the Carel.com website.

### 2.2. Registration of plugins

Each plugin is worth one credit, and credits can be purchased individually or three or five at a time, allowing the corresponding number of functions to be activated. The three packages of credits for activating the system optimisation functions in **boss** are as follows:

<b>P/N</b>	<b>Description</b>
BMHST01P00	CREDIT FOR 1 PLUG-IN FOR BOSS HIGH-END
BMHST03P00	CREDIT FOR 3 PLUG-INS FOR BOSS HIGH-END
BMHST05P00	CREDIT FOR 5 PLUG-INS FOR BOSS HIGH-END

The packages of credits for activating the system optimisation functions in **boss mini** are as follows:

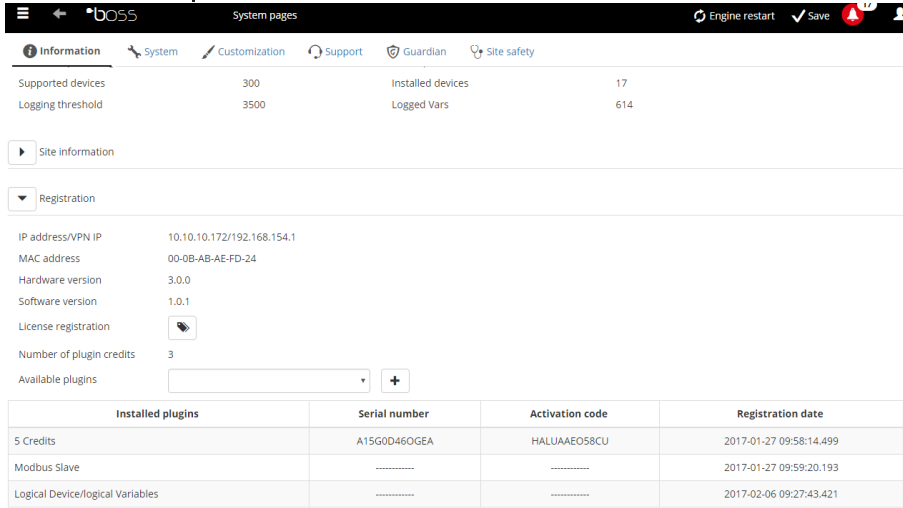
<b>Codice articolo</b>	<b>Descrizione</b>
BMEST01P00	CREDITO PER 1 PLUG-IN PER BOSS MINI
BMEST03P00	CREDITO PER 3 PLUG-IN PER BOSS MINI

Once the order has been sent you will receive the serial number by email (in two/three working days).


In order to obtain the Activation code, it is necessary to register the Serial Number and Mac Address of the boss unit at our website: <http://www.carel.com/activations>.

Then the credits can be registered on the supervisor web interface under the **Configuration/System pages/Information, Registration** session:

## CST Technical support | FAQ



The screenshot shows the BOSS system configuration interface. The top navigation bar includes 'Information', 'System', 'Customization', 'Support', 'Guardian', and 'Site safety'. The 'Information' section displays system statistics: Supported devices (300), Logging threshold (3500), Installed devices (17), and Logged Vars (614). Below this, there are sections for 'Site information' and 'Registration'. The 'Registration' section shows the following details:

- IP address/VPN IP: 10.10.10.172/192.168.154.1
- MAC address: 00-0B-AB-AE-FD-24
- Hardware version: 3.0.0
- Software version: 1.0.1
- License registration: 
- Number of plugin credits: 3
- Available plugins:  +

At the bottom, there is a table of installed plugins:

Installed plugins	Serial number	Activation code	Registration date
5 Credits	A15G0D460GEGA	HALUAAE058CU	2017-01-27 09:58:14.499
Modbus Slave	-----	-----	2017-01-27 09:59:20.193
Logical Device/logical Variables	-----	-----	2017-02-06 09:27:43.421

Once the credits have been registered, each plugin can be selected according to the number of credits.

In boss it is possible to activate up to 20 plugins while in boss mini up to 3 plugins.

[Back to index](#)

### 2.3. Telegram channel configuration for notifications

Below is the procedure to properly configure the Telegram channel for instant messaging notifications:

1. Install Telegram client on a Smartphone or Desktop (or both).
2. Create a new BOT using "BotFather" in Telegram. To do this, simply type BotFather in the Telegram search bar and select the Botfather found. Click "start" and follow the instructions shown:
  - /newbot to create the bot
  - choose the name
  - choose the username (this must end with "bot").
3. The new BOT has an unique ID. Copy that **token** and paste it on the **Configuration/IO Configuration/IM** page in the **BOT token** field. Click "Save".
4. Use the Telegram client to add the newly created Bot to your Contacts: Click on the newly-created BOT and click "Start".
- 4a. Every contact (client) that can receive Telegram messages has to repeat point 4 in his/her Telegram client.

## CST Technical support | FAQ

5. Open the **Configuration/ IO Configuration/IM** page, click “refresh” and check whether your users are in the Contacts. If so, run a Test. You should receive a test PDF in your Telegram client, whose sender is the BOT.
6. Repeat the test for all desired recipients.
7. Configure in **Alarms and Events management** the IM action in the same way as for emails or other notification channels.
8. OPTIONAL: if you wish to create a Groupchat, proceed as follows:
  - 8a. Create a group using your Telegram app.
  - 8b. Add the BOT as if it were a normal human contact, and then add the other users in the same way (search by username).
  - 8c. Go to the **Configuration/IO Configuration/IM** page: click “refresh” and now the Contacts should also contain the name of the Group you have created. You can now use the Group as a recipient. All Group members will see the messages.

[Back to index](#)





### 2.4. Import/export site configuration

It is possible to import and/or export the site configuration from the software application interface.

A site export contains all the “Supervisory application” settings: line configuration, device configuration, all the rules configured in the Activity section (Plant Calendar, Alarms and events management and Activities Scheduler), models (standard and custom), device detail images/customised detail page, maps, site images and any registered plugins (to be registered again on the new unit after importing the site).

This function is available in the Configuration / System pages/ System/ Import/Export site configuration section:

▼ Import/export site configuration

Export configuration	<input checked="" type="checkbox"/> Include historized data	
Configuration restore	<input type="text"/>	
Download configuration	<input type="text"/>	
Upload configuration	<input type="text"/>	

## Technical support | FAQ

The available operations are:

- **Export configuration:** export the configuration of the supervisor, choosing whether or not to include logged data.  
In boss the configuration is exported in the internal memory.  
Instead in boss mini the configuration is exported to:
  - a SD/USB memory plugged to the machine if the operation is done locally
  - in the PC's file system if the operation is done remotely.
- **Configuration restore:** restore a configuration that has been previously exported.
- **Download configuration (only for boss):** download a previously exported configuration and store it externally to boss. For local management, the backup can be saved to the ftp folder or any connected USB/microSD device, while for remote management it will be downloaded to the file system on the computer/mobile device used.
- **Upload configuration (only for boss):** upload a configuration stored externally to boss

Compatibility: there is no compatibility between "site configuration" exported from boss to boss mini and viceversa.

For SW rev less than 1.4.0: "Site configuration" can be imported only on units having exactly the same software version of the "site configuration".

Starting from SW rev 1.4.0: "Site configuration" from machines with SW rev  $\geq$  1.3.0 can be imported on units with SW rev  $\geq$  of the configuration.

Examples:

- 1.4.0  $\leftarrow$  1.3.0 ("site configuration" of version 1.3.0 can be imported, NO of prevision version)
- 1.5.x  $\leftarrow$  1.4.x / 1.3.0 ("site configuration" of versions 1.4.x and 1.3.x can be imported)
- 1.6.x  $\leftarrow$  1.5.x / 1.4.x / 1.3.0 ("site configuration" of the 1.4.x, 1.5.x and 1.3.0 versions can be imported)

Compatibility: there is not compatibility between configurations exported from boss to boss mini and vice versa. Furthermore a "site configuration" can only be imported to units with the exact same software version as the backup.

The supervisor also gives users the possibility to perform, restore and schedule backups from System administration.

See "[1.5 Backup and restore](#)" for further information and the Video FAQ **System Administration backup.mp4** for the procedure.

[Back to index](#)

## 2.5. Internal relay management

### boss

Three internal relays are available on boss for alarm management and/or safety actions.

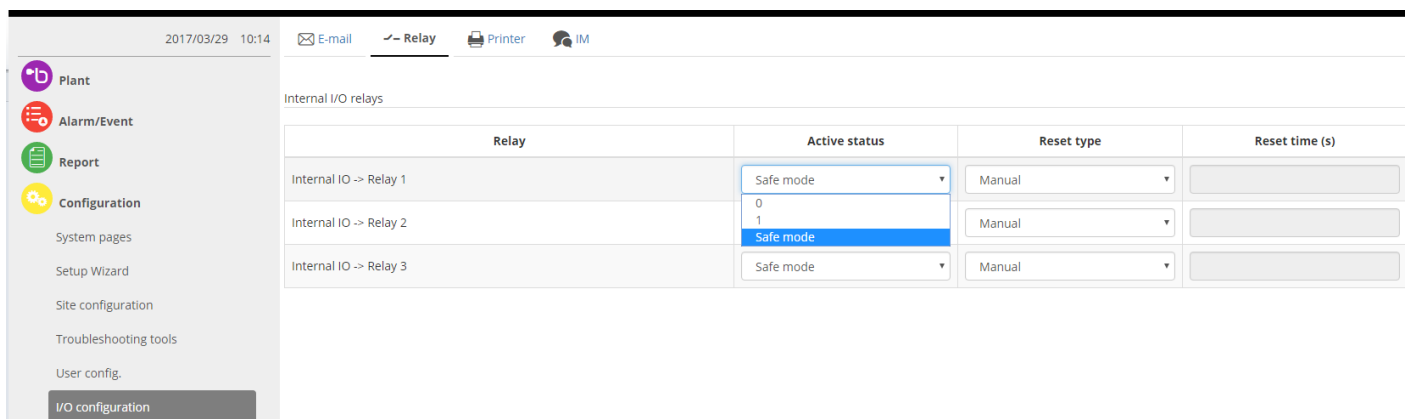
### boss mini

boss mini does not have directly integrated relays but is able to drive three external relays via 24Vdc outputs. It is possible to use the special external I / O module with three relays, P/N BMESTRLA00. As an alternative it is possible to connect relays with a 24 Vdc max 20 mA coil, using the cable supplied with boss mini. Other 24 Vdc devices as buzzers or lamps can also be connected, for signalling.

### Software Management of the relays/digital outputs

The supervisor can be configured to automatically control the relays/outputs by setting them to a digital value identified in the supervisor as **Status**.

Users can configure the **Active status** on the **Configuration/System pages/IO Configuration/Relay** page:



Relay	Active status	Reset type	Reset time (s)
Internal IO -> Relay 1	Safe mode	Manual	
Internal IO -> Relay 2	0 1 Safe mode	Manual	
Internal IO -> Relay 3	Safe mode	Manual	

**Active status** represents the logical status taken by the relay when the action activates it:

**1:** means that the relay is considered active when in logical state 1. Consequently, when the action activates it, the relay will be energized.

**0:** means that the relay is considered active when in logical state 0. Consequently, when the action activates it, the relay de-energized.

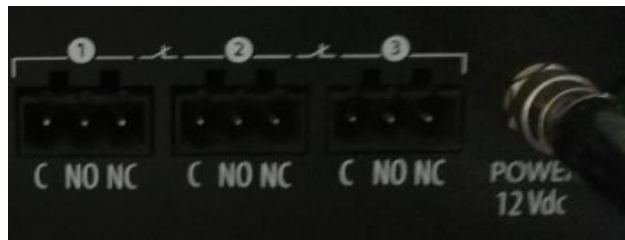
## CST Technical support | FAQ

**Safe mode:** same as 0 status however with safer behaviour. This means that the relay also manages emergency situations not only alarms, being set to 0 when boss is NOT actively supervising, therefore in the following cases:

1. Restart of the engine (until the engine is active again)
2. Stop of the engine
3. System reboot (until the engine is active again)
4. System shutdown
5. Power failure

Safe Mode does not however prevent the relays from being controlled by actions defined by the user (manual and scheduled).

Referring to the serigraphy on boss:



for the internal relays, Status 0, 1 and Safe mode correspond to:

Status	C-NC contact	C-NO contact	Led (boss)
0	Closed	Open	OFF
1	Open	Closed	ON
Safe mode	Closed	Open	OFF

### Starting status of the relays

**a) boss machines with native SW rev  $\geq$  1.2.0**

The starting status of the relays at the power on of the machine is 1 (led on).

**b) boss mini (all SW rev.) and boss Machines with native SW rev  $<$  1.2.0 (even if updated by Service pack)**

The default starting status of internal relays is 0 (led off in boss). Therefore to have an effective functioning of the Safety Mode, the designed relay/s should be set manually to 1: this starting value will be maintained on the next reboots/power on. In this way in case of "Safety" issues, the relay/s will pass from 1 to 0, otherwise the status will not be modified, but set from 0 to 0.

## 2.6. “Remember me” option: how to keep a user session always active

This function has been introduced to allow a guest user with very limited rights to always display the map or the device page.

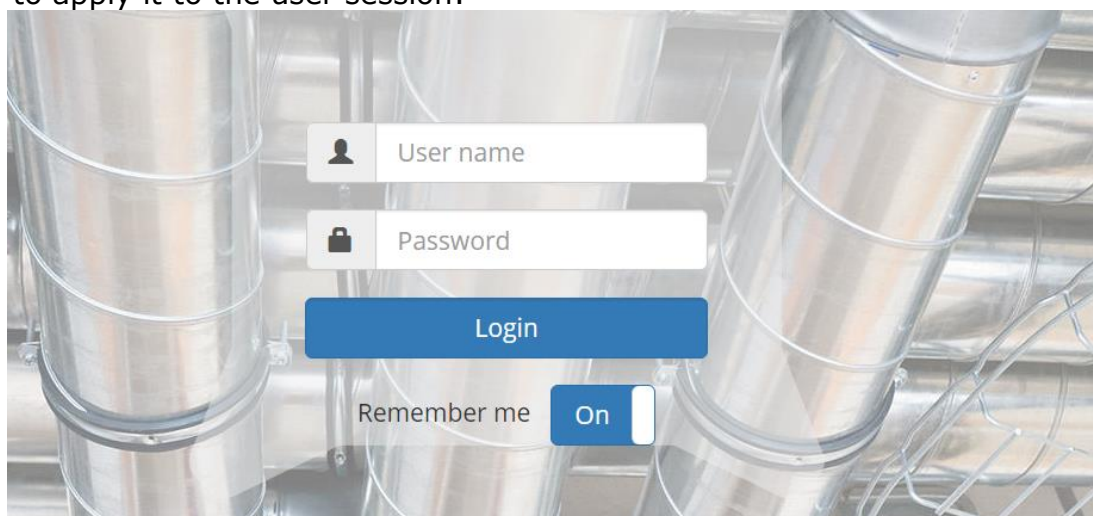
In fact, by enabling the **Remember me** option, the current user session will be kept open even in the event of inactivity longer than the configured session timeout. Once the session timeout has elapsed, the user will not be automatically logged out and the device or map page (depending on the home page set) will be displayed.

Only a manual logout will close the user session. It should be stressed that for security reasons it is recommended to only allow the remember me option for user profiles with read-only rights (not configuration or parameter setting).

To Show the 'Remember me' option in the Login page go to *Configuration/System pages/System* and set the corresponding item as shown in the image below:

Set session time timeout (minutes)	<input type="text" value="30"/>
Show the 'Remember me' option in the Login page	<input checked="" type="checkbox"/> On

On the next logout, the option will be displayed again on the login page: before logging in, set this to ON to apply it to the user session:



## 2.7. How to show groups of devices for specific user profiles

It is possible to show a group of devices for specific user profiles, by creating and properly configuring logical groups according to what needs to be shown for every user profile.

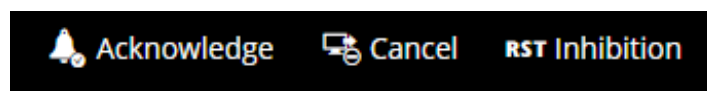
- 1) Click **Configuration/Logical Devices Creation**: here the groups of devices can be created according to needs.
- 2) Click **Configuration/User config./Profiles**: access to modify the desired profile/profiles, go to the bottom of the configuration page and enable/disable the possibility to display the previously created groups of devices:

Enabled	Group
<input checked="" type="checkbox"/>	Refr
<input checked="" type="checkbox"/>	Cond

[Back to index](#)

## 2.8. Meaning of acknowledge, cancel and inhibition of alarms

The following actions can be performed on active alarms:



**Acknowledge:** if the *Active alarms verification* option is enabled in GuardianPRO, the acknowledge action affects the behaviour of GuardianPRO only regarding that particular alarm event: GuardianPRO will not perform any kind of action to signal or manage the alarm even if it lasts longer than the safety time (configured on the Configuration/Site Configuration/Alarms Safety page).

This means that the acknowledge action does not affect the Alarms and Events management but only GuardianPRO.

**Cancel:** this affects the behaviour of *Alarms and Events management* in the case of rules for managing the alarm (present in the Alarm condition for the rule). If a delay has been set for



## Technical support | FAQ

execution of the rule and the alarm is cancelled before this delay, the action will not be performed even if the alarm is still active.

**Inhibition:** the alarm will be deleted from the Active alarms list and added to the Reset alarms list. The alarm will be considered by the supervisor again only when it has physically ended and started again (new occurrence) or when the engine is restarted.

[Back to index](#)

### 2.9. Information on the Modbus TCP/IP communication as a client

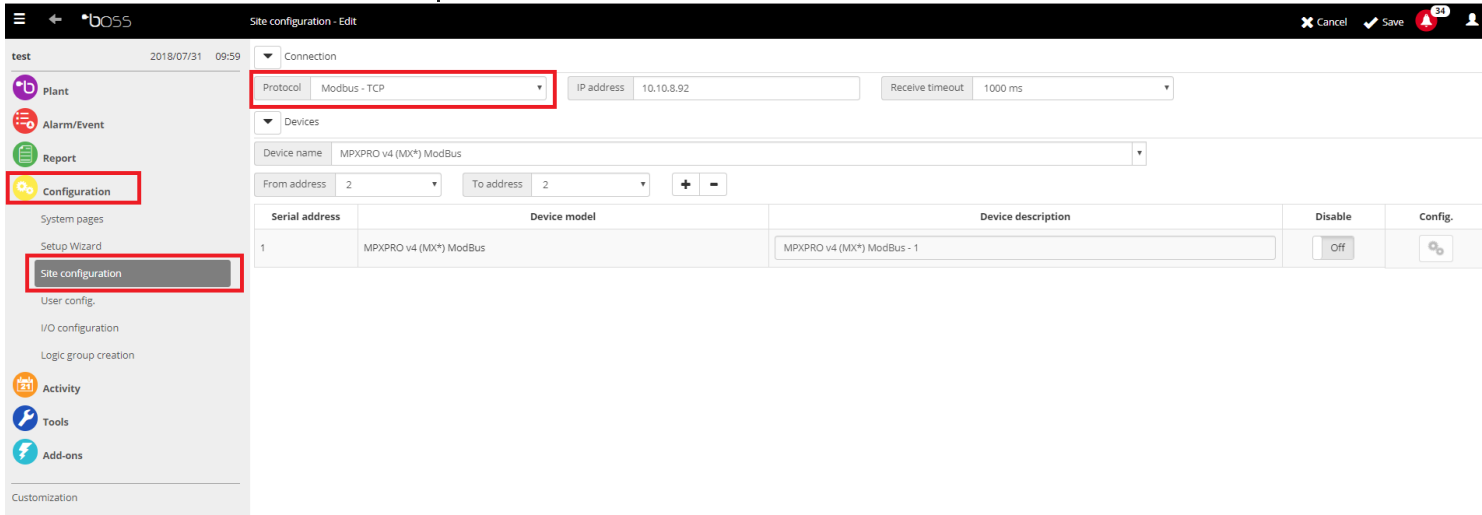
The supervisor can communicate as a client via Modbus TCP/IP protocol with slave devices that support this type of communication.

The physical channel to be used is the **FIELD** Ethernet port, dedicated just for the communication with the field devices. The LAN network interface can't instead be used for this purpose, since it is for the standard network activity (access via https, email, telegram ..).

From the software point of view these devices are considered as all the other devices connected as slaves to the supervisor and therefore their number is included in the count of the total maximum number of devices:

- 1) 100 for part numbers BMH\*S0
- 2) 300 for part numbers BMH\*E0
- 3) 30 for part numbers BME\*S0
- 4) 50 for part numbers BME\*E0

To add and configure a Modbus TCP/IP line, select **Configuration/Site Configuration/Site/Add:**



Select *Protocol Modbus – TCP*, insert the IP Address of the slave device or of the Modbus TCP/IP gateway and set the *Receive Timeout* (timeout for the offline management of the device).

Add the device/s with the corresponding address/es. In the modbus TCP/IP communication this address represents the *unit identifier* used to communicate via devices such as bridges, routers and gateways that use a single IP address to support multiple independent MODBUS units.

In case of custom devices it is necessary to create the corresponding xml model to communicate with the instrument.

## 2.10. Datalogging Frequency/Depth table

Below the table reporting the sample frequency and the admitted depths.

Depth/ Frequency	7 giorni	30 days	60 days	180 days	360 days	540 days	720 days
60 min.	X	X	X	X	X	X	X
30 min.	X	X	X	X	X	X	X

## CST Technical support | FAQ

15 min.	X	X	X	X	X	X	
5 min.	X	X	X	X	X	X	
2 min.	X	X	X	X			
1 min.	X	X	X	X			
30 sec.	X	X	X				
15 sec.	X*						
10 sec.	X*						
5 sec.	X*						

\*: available only for boss not for boss mini.

### 2.11. Update of c.pCO software through the supervisor

Through the supervisor it is possible to update the software of the connected c.pCO devices.

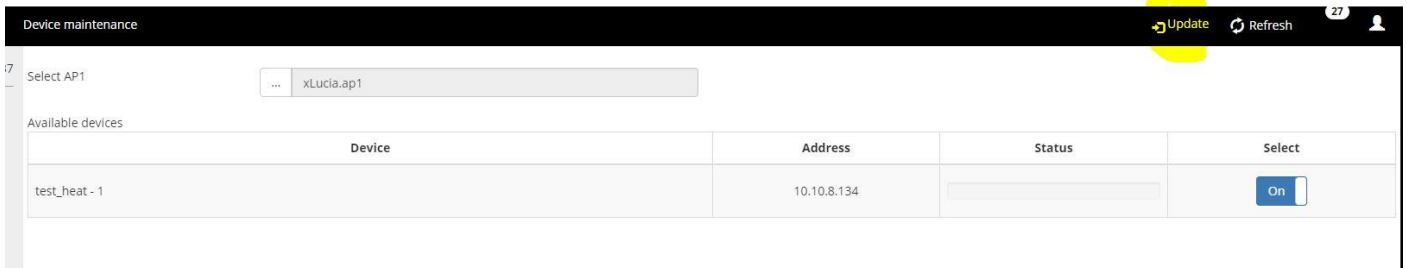
To perform the update it is necessary that:

- the supervisor and the c.pCOs are in the same local network (recommended to use the FIELD port, dedicated just to the FIELD communication).
- The c.pCOs are configured in the supervisor communication lines as Modbus TCP devices.
- In the c.pCOs the http protocol is enabled (in fact the file transfer will be via http).
- In the c.pCOs the port 80 is configured for http protocol.
- In c.pCOs the access via http is NOT protected by "htaccess" file.

To access the function, select from the menu the page **Tools/Device maintenance** where all the c.pCOs instantiated in the Modbus TCP lines will be visible. It is therefore possible to

## CST Technical support | FAQ

select the .ap1 file to be transferred to the c.pCOs for updating.



The screenshot shows a web interface titled "Device maintenance". At the top right, there are buttons for "Update" (highlighted in yellow), "Refresh", and a user profile icon. Below the header, there is a "Select AP1" dropdown menu with "xLucia.ap1" selected. Underneath, a table lists "Available devices".

Device	Address	Status	Select
test_heat - 1	10.10.8.134	<input type="text"/>	<input type="button" value="On"/>

Press Update to update the selected c.pCOs.

[Back to index](#)

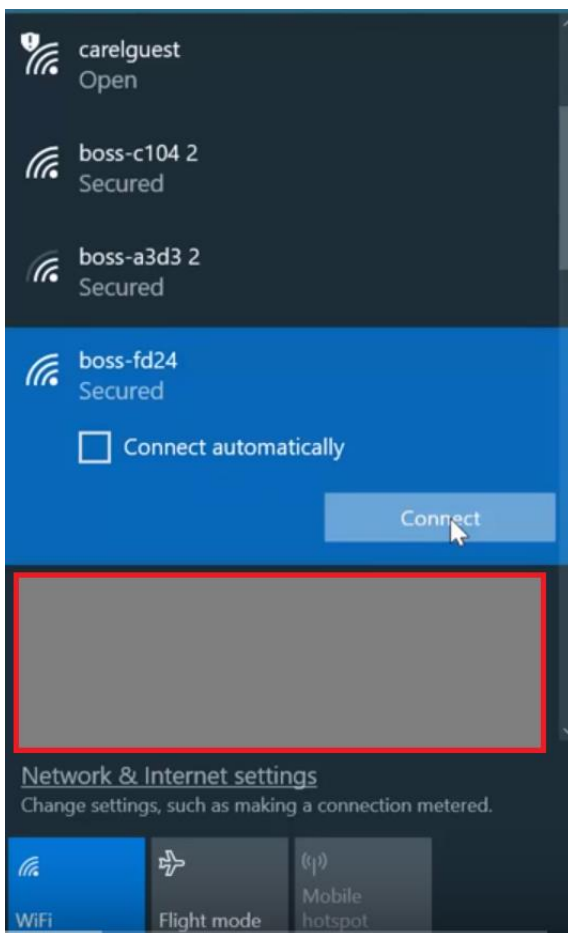
## 3. Connectivity

### 3.1. Access through the integrated Wi-Fi

It is possible to access to the supervisor by the integrated Wi-Fi interface.

Below the procedure:

- from your device (PC, smartphone or tablet), simply identify the supervisor Wi-Fi network among the available ones. This is identified by the supervisor name (boss-xxxx for boss, mboss-xxx for boss mini). Then connect to it:



## Technical support | FAQ

The first time you will connect you have to insert the Wi-Fi password which is empty at the first power on of the machine but that will be set by the administrator user at the end of first startup procedure.

- once the Wi-Fi connection between your device (PC, smartphone or tablet) and the supervisor will be established, it will be possible to access to the Supervisory Application interface by typing in the address bar of the browser the following address: **https://name** (where name represents the name of boss or boss mini reported on the product label).

If the access by name is not possible (for example due to problems of name/IP address mapping in the PC/smartphone), it is possible to access through the IP address of the supervisor within the Wi-Fi connection: **192.168.42.1**. To access then type in the address bar of the browser the following address: <https://192.168.42.1>.

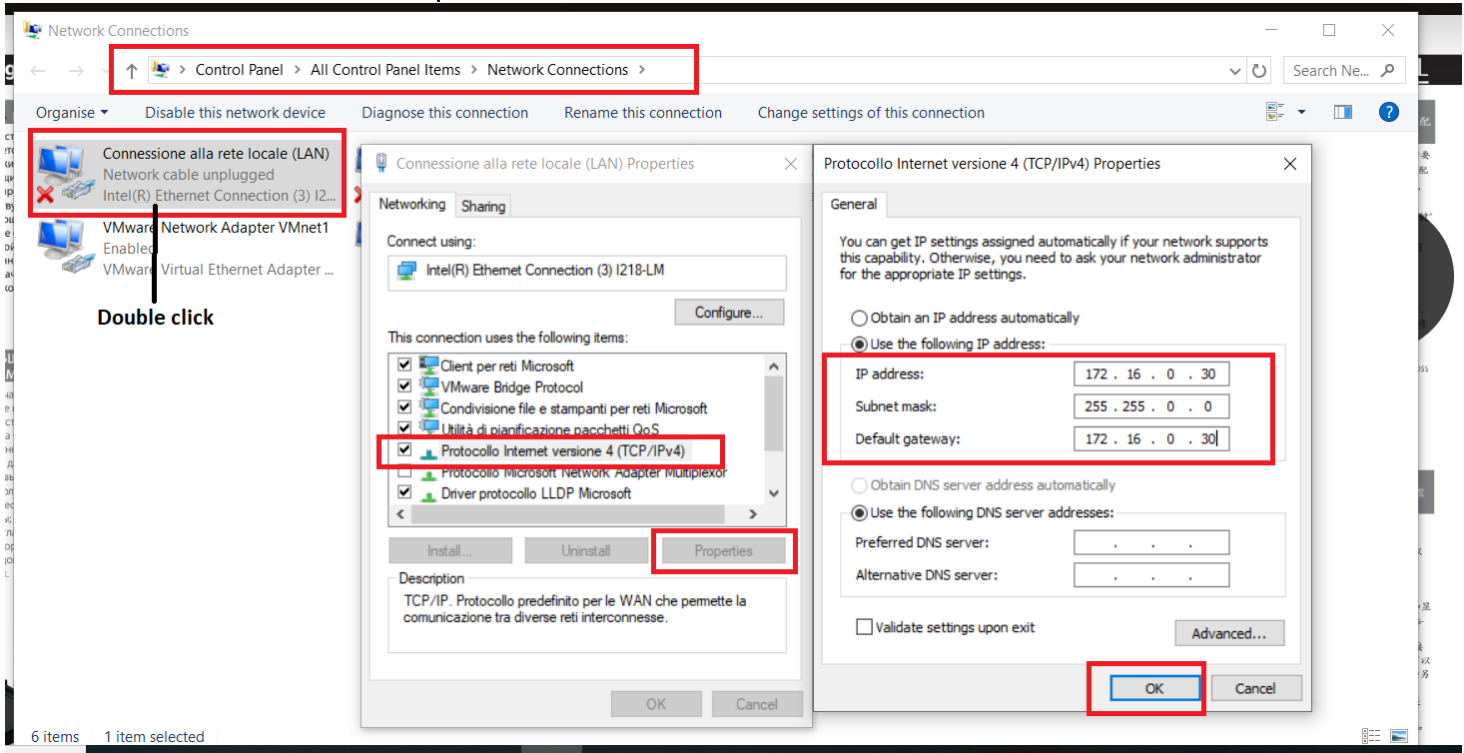
[Back to index](#)

### 3.2. Access through the temporary IP Address (available only for boss mini)

It is possible to assign a temporary fixed IP address to boss mini to allow the access via the LAN port (not FIELD) in case the IP Address set in the machine is not known. For details on the procedure for enabling the function by using the dedicated button, please refer to the technical leaflet of the product.

The temporary IP address, assigned for about an hour, is **172.16.0.33** with subnet mask **255.255.0.0**.

To access to boss mini by this IP, the used PC must be in the same IP addresses network. To do this, set the parameters of the ethernet network appropriately, for example as follows (taking care to insert IP Address and subnet mask compatible with those of boss mini):



Once the network of your PC has been properly configured, it will be possible to access the boss mini pages by typing in the address bar: <https://mboss-xxxx> (boss mini name indicated on the product side label) or <https://172.16.0.33>.

[Back to index](#)

### 3.3. Internet access

Being a web application, if the supervisor is correctly connected to an ADSL router it can provide access to all the functions both of the supervisory application (software functions) and system administration via Internet using a public IP.

The supervisor must be connected to the router or the local network via the Ethernet port (not USB port).

For **direct internet** web access the following communication ports are used:

- port **443** for the Supervisory application

## CST Technical support | FAQ

- port **8443** for the System administration

If firewalls are active on the router and/or inside the local network, then HTTPS forwarding for ports 443 and 8443 to the machine local IP must be correctly configured using the necessary exception rules.

To access the **supervisory application**, simply enter in the browser's address bar: <https://PublicIPAddress>.

To access the System administration, simply click the *System administration* button present on the supervisory application Login page.

For **access via the integrated VPN**, please refer to the document [How to configure a VPN on boss.pdf](#).

The port used for VPN connection is 1100. If firewalls are active on the router and/or inside the local network, then forwarding for port 1100 (UDP protocol) to the supervisor local IP must be correctly configured using the necessary exception rule.

### [Back to index](#)

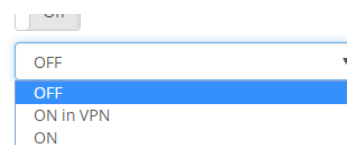
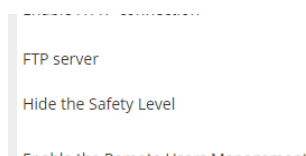
### 3.4. File transfer via FTP (only for boss not boss mini)

In boss it is possible to enable an FTP server for file transfer from/to boss.

The local folder for file exchange is called **ftp** and is the same used locally for importing / exporting/saving files inside the machine. For example the scheduled Backups automatically created by the System Administration by default are saved to **ftp** folder.

For security reasons, the FTP server is disabled by default and can be started from the page *Configuration / System / System Pages* of the Supervisory Application.

*Procedure for supervisors with SW rev  $\geq 1.4.0$*



Select **ON in VPN** to use the FTP server within the built-in VPN.



## CST Technical support | FAQ

Select **ON** to use the FTP server within the local network or Internet directly, without passing through the built-in VPN. In this case boss firewall settings will be changed as well.

The FTP server will be ON until the next manual stop, by selecting **OFF**.

*Procedure for supervisors with SW rev < 1.4.0*

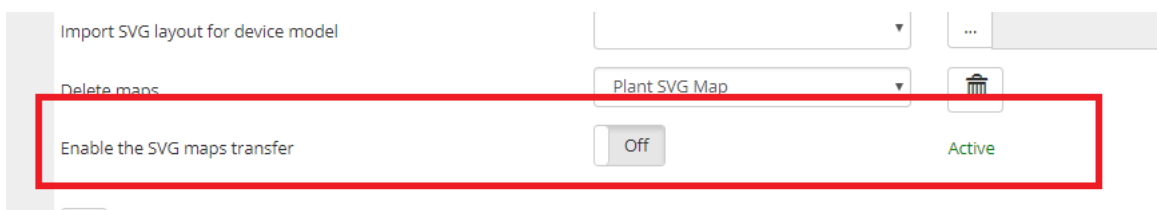
Bring the FTP Server to **ON**:



The FTP server remains active until a manual stop from the same page or a complete reboot of the machine are performed.

In case of access via the integrated VPN, the FTP transfer is possible without further configuration.

In case of direct access via the Internet or local network (without going through the internal VPN), it is necessary to temporarily change the boss firewall settings, through the Supervisory Application, on page *Configuration / System Pages / Customization, Enable the SVG map transfer*:



This option can be activated only if the FTP server is already started in the machine. Once the file transfer has been done, it is recommended to disable this option in order to return the firewall to the initial security settings.

For information on login credentials via FTP, submit request to [sw.support@carel.com](mailto:sw.support@carel.com).

[Back to index](#)