Danfoss MCX15B2 Programmable Controller

# Danfoss MCX15B2 Programmable Controller User Guide



Contents



## Danfoss MCX15B2 Programmable Controller

**Table of new contents**

| Manual Version | Software Version | New or modified Contents |
|---|---|---|
| 1.00 | Site version: 2v30 | First release |

## Overview

- The MCX15/20B2 controller provides a Web Interface that can be accessed with mainstream internet browsers.

**The Web Interface has the following main functionalities:**

- Access to the local controller
- Gateway to access controllers connected with fieldbus (CANbus)
- Displays log data, real-time graphs, and alarms
- System configuration
- Firmware and application software update
- This user manual covers the features of the Web Interface and a few other aspects mainly related to connectivity.
- Some pictures in this manual may look a bit different in the actual version. This is because newer software versions may slightly change the layout.
- Pictures are only provided to support the explanation and may not represent the current implementation of the software.

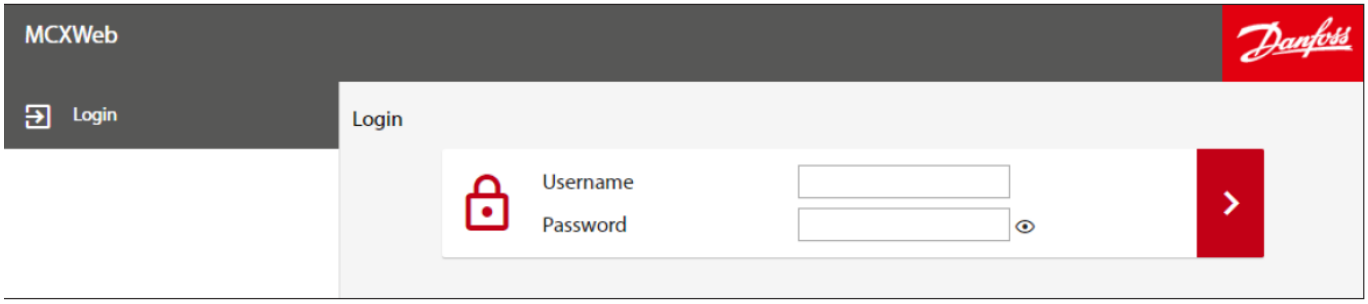
**Disclaimer**

- This user manual does not describe how the MCX15/20B2 is expected to work. It describes how to perform most of the operations that the product allows.
- This user manual provides no guarantee that the product is implemented and works as described in this manual.
- This product can be changed at any time, without previous notice, and this user manual may be outdated.
- Security cannot be guaranteed, as new ways to break into systems are found every day.
- This product uses the best security strategies to provide the required functionalities.
- Updating the product regularly is critical to keep the product secure.

## Login

To login navigate with an HTML5 browser (e.g. Chrome) to the IP address of the gateway.

**The screen will appear as follows:**




- Enter the username in the first box and the password in the second then press the right arrow.

**The default credentials to access all configuration settings are:**

- **Username** = admin
- **Password** = PASS
- Password change is requested at first login.
- **Note:** after each login attempt with wrong credentials a progressive delay is applied. See 3.5 Users' Configuration on how to create users.

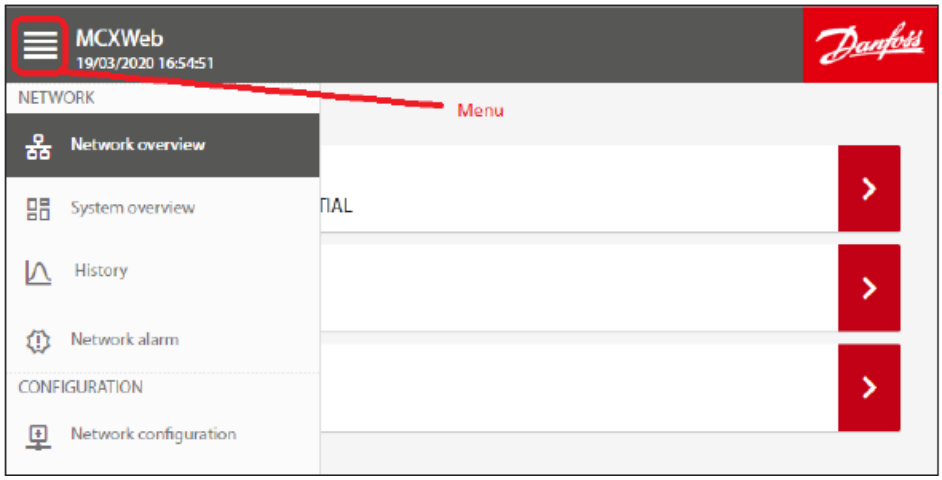
## Configuration

### First-time configuration

- The controller is provided with an HTML user interface that can be accessed with any browser.
- By default, the device is configured for dynamic IP address (DHCP):
- You can get the MCX15/20B2 IP address in several ways:
- Through USB. Within 10 minutes after powering up, the device writes a file with configuration settings into a USB flash drive, if present (see 3.9 Read current network configuration without web interface).
- Through the local display of MCX15/20B2 (in models where it is present). Press and release X+ENTER immediately after powering up to enter the BIOS menu. Then select GEN SETTINGS > TCP/IP.
- Through the software tool MCXWFinder, which you can download from the MCX website.

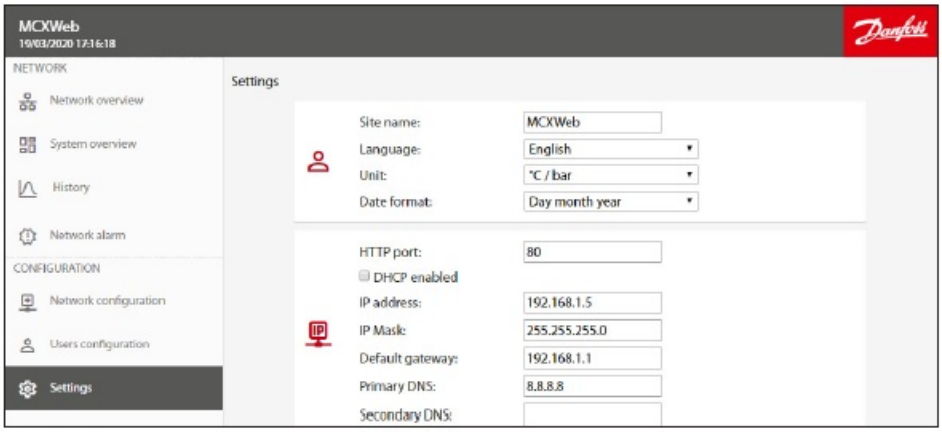
**Once connected for the first time, you can start to:**

- configure the Web Interface. See 3.2 Settings
- to configure the users. See 3.5 Users' Configuration
- configure the main device MCX15/20B2 and any network of devices connected to the main
- MCX15/20B2 through the Fieldbus (CANbus). See 3.3 Network Configuration
- **Note:** the main menu is available on the left side of any page or can be displayed by clicking on the menu symbol in the top left corner when it is not visible due to the page dimension:



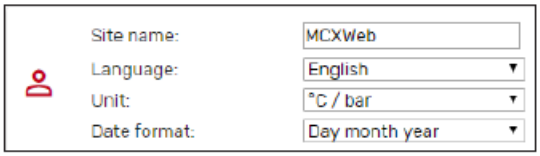

- To install updates, follow the instructions in 3.11 Install web page updates.

**Settings**




- The Settings menu is used to configure the Web Interface.
- The Settings menu is visible only with the appropriate access level (Admin).
- All the possible settings are described here below.

**Site name & localization settings**

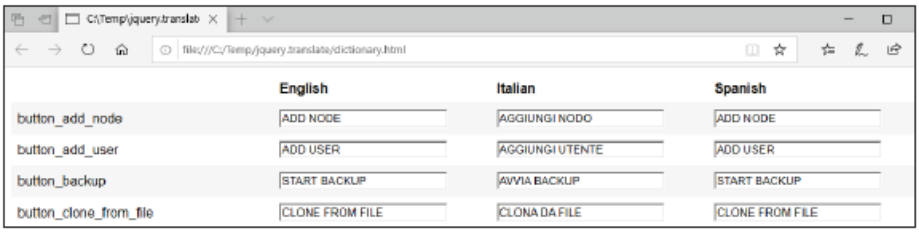



- Site name is used when alarms and warnings are notified with an email to the users (see 3.2.4 Email notifications).
- Language of the Web Interface: English/Italian.

**Further languages can be added following this procedure (for advanced users only):**

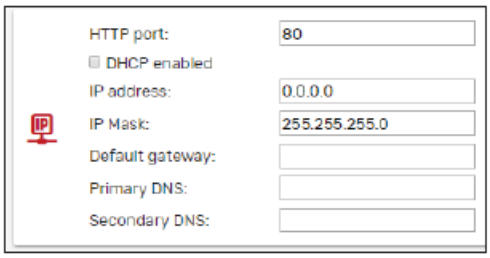
- Copy the folder http\js\jquery.translate from the MCX to your computer via FTP
- Edit the dictionary.js file and add your language in the “languages” section of the file.
- e. g. For Spanish, add the following two lines:


- **Note:** you must use the language code based on RFC 4646, which specifies a unique name for each culture (e.g. es-ES for Spanish) if you want to retrieve the correct translation of the application software data from the CDF file (see 3.3.3 Application and CDF).
- Using your browser, open the file **dictionary.htm**/ and you will see an additional column with the Spanish lanquage




- Translate all the strings and press SAVE at the end. Strings that might be too long are highlighted in red.
- Copy the newly generated file dictionary.js into the MCX, in the HTTP\js\jquery.translate folder overwriting the previous one.
- Units of measurement used by the Web Interface: °C/bar or °F/psi
- **Date format:** Day month year or Month day year

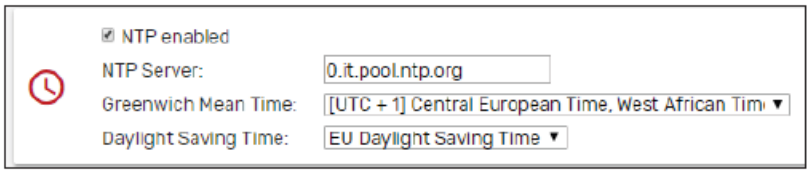
### Network Settings




- **HTTP** port: You can change the default listening port (80) to any other value.
- **DHCP:** if DHCP is enabled by ticking the DHCP enabled box, the network settings (IP address, IP mask, Default gateway, Primary DNS, and Secondary DNS) will be automatically assigned by the DHCP server.
- Otherwise, they must be manually configured.

### Date and Time acquisition mode

- The NTP protocol is used to automatically synchronize the time setting in the local controller. By ticking the NTP enabled box, the Network Time Protocol is enabled, and the Date/Time is automatically obtained from an NTP time server.



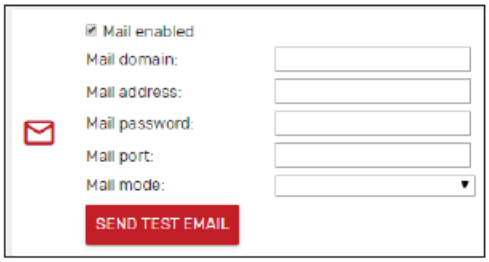

- Set the NTP server you wish to synchronize with. If you don't know the most convenient NTP server URL of your region, use pool.ntp.org.
- The MCX15/20B2 real-time clock will then be synchronized and set according to the defined time zone and eventual daylight saving time.

**Daylight Saving Time:**

- **OFF:** deactivated
- **ON:** activated
- **US:** Start=Last Sunday of March – End=Last Sunday of October
- **EU:** Start=2nd Sunday of March – End=1st Sunday of November
- If the NTP-enabled box is not ticked, you can set the date and time of the MCX15/20B2 manually.

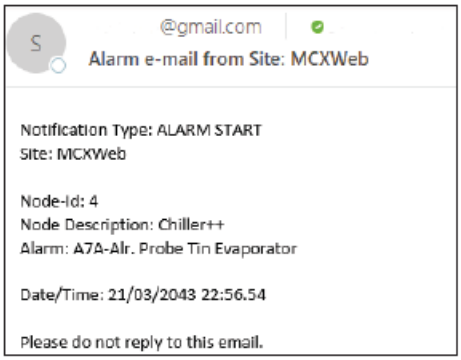

- **Warning:** the time synchronization of the MCX controllers connected via fieldbus (CANbus) to the MCXWeb is not automatic and must be implemented by the application software.

**Email notifications**




- The device can be configured to send a notification via email when the status of the application alarm changes.
- Tick on Mail enabled to allow MCX15/20B2 to send an email after every change of the alarm status.
- Mail domain is the name of the Simple Mail Transfer Protocol (SMTP) server that you want to use. The mail address is the email address of the sender.
- Mail password: password to authenticate with the SMTP server
- For the Mail port and Mail mode refer to the configuration of the SMPT Server. Both unauthenticated and SSL or TLS connections are managed.
- For each mode, the typical port is automatically proposed but you can manually change it afterward.

**Example of email sent by the device:**




- There are two types of notifications: ALARM START and ALARM STOP.
- Send Test Email is used to send an email as a test to the Mail address above. Save your settings before sending the test email.
- The email destination is set when configuring the users (see 3.5 Users' Configuration).

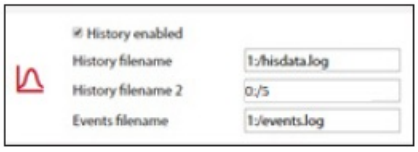
**In case of mailing problems, you will receive one of the following error codes:**

- **50** – FAIL LOADING CA ROOT CERTIFICATE
- **51** – FAIL LOADING CLIENT CERTIFICATE
- **52** – FAIL PARSING KEY
- **53** – FAIL CONNECTING SERVER
- **54** -> 57 – FAIL SSL
- **58** – FAIL HANDSHAKE
- **59** – FAIL GET HEADER FROM SERVER
- **60** – FAIL HELO
- **61** – FAIL START TLS
- **62** – FAIL AUTHENTICATION
- **63** – FAIL SENDING
- **64** – FAIL GENERIC
- **Note:** do not use private email accounts to send emails from the device as it has not been designed to be GDPR compliant.

**Gmail configuration**

- Gmail may require you to enable access to less secure apps to send emails from embedded systems.
- You can enable this feature here: **https://myaccount.google.com/lesssecureapps**.

**History**




- Specify the name and position of the datalog files as defined by the MCX application software.
- If the name starts with 0: the file is saved in the internal MCX15/20B2 memory. In the internal memory it is possible to have max. one datalog file for variables and the name must be 0:/5. If the name starts with 1: the file

is saved in the USB flash drive connected to the MCX15/20B2. In the external memory (USB flash drive), it is possible to have one file for logging variables (the name must be 1:/hisdata.log) and one for events like alarm start and stop (the name must be 1:/events.log)
- See 4.2 History for a description of how to view historical data.

**System Overview**

- Tick on System Overview enabled to create a page with the overview of the main system data including those coming from all devices connected to the main controller's FTP communication (see 5.1.2 Creation of a Customized System Overview page).

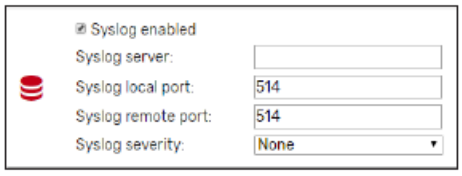
**FTP**

- Tick on FTP enabled to allow FTP communication. FTP communication is not secure, and it is not recommended that you enable it. It can be useful if you need to upgrade the web interface, however (see 3.11 Install web pages updates)

**Modbus TCP**

- Tick on Modbus TCP Slave enabled to enable Modbus TCP slave protocol, connecting over port 502.
- Note that the COM3 communication port must be managed by the application software on the MCX to have the Modbus TCP protocol working.
- In MCXDesign applications, the brick ModbusSlaveCOM3 must be used and in the InitDefines.c file in the App folder of your project, the instruction #define ENABLE_MODBUS_SLAVE_COM3 must be present in the right position (see the help of the brick).

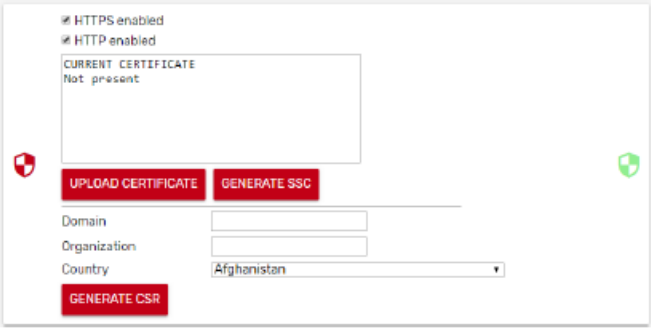
**Syslog**




- Tick on Syslog enabled to enable Syslog protocol. Syslog is a way for network devices to send event messages to a logging server for diagnostic and troubleshooting purposes.
- Specifies the IP address and port for connections to the server.
- Specifies the kind of messages, by severity level, to be sent to the syslog server.

**Security**

- See 6. Security for further information on MCX15/20B2 security.




**Certificates**

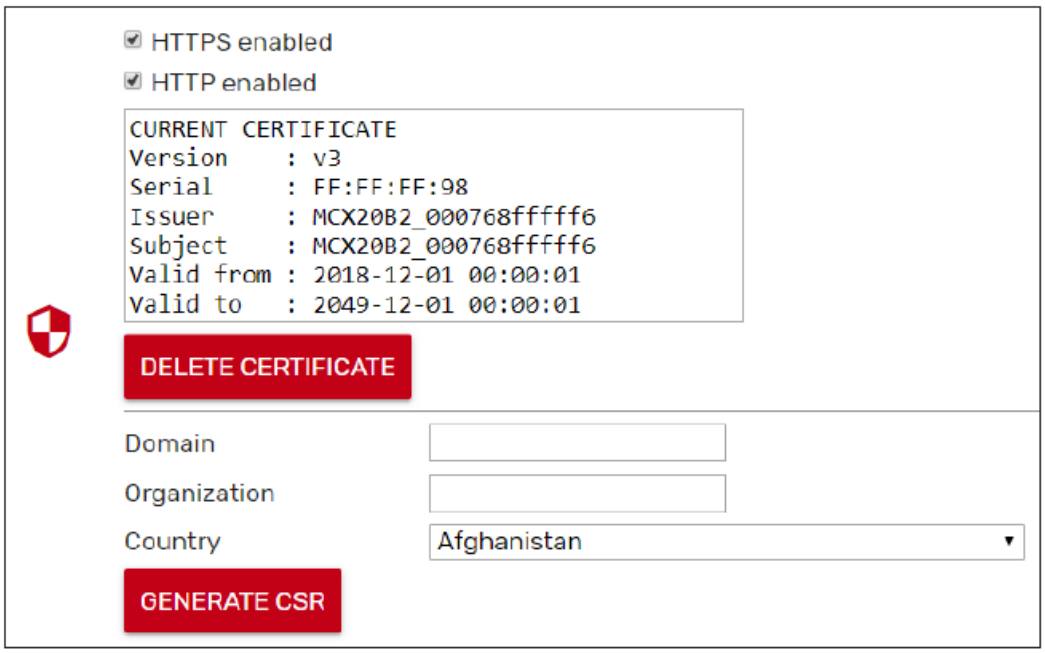
- Enable HTTPS with a personalized server certificate if the device is not in a secure environment.
- Enable HTTP if the device is in a secure LAN with authorized access available (also VPN).
- A dedicated certificate is needed to access the web server over HTTPS.
- The certificate management is the responsibility of the user. To generate a certificate, it is necessary to follow the steps below.

**Creating a self-signed certificate**

- Click GENERATE SSC to generate a self-signed certificate

**Creating and assigning a CA-signed certificate**

- Fill in the requested data about the Domain, Organization, and Country
- Click GENERATE CSR to generate a Private key and Public key pair and a Certificate Sign Request (CSR) in PEM and DER format
- The CSR can be downloaded and sent to the Certification Authority (CA), public or other, to be signed
- The signed certificate can be uploaded into the control by clicking the UPLOAD CERTIFICATE. Once completed the certificate information is shown in the text box, see the example below:

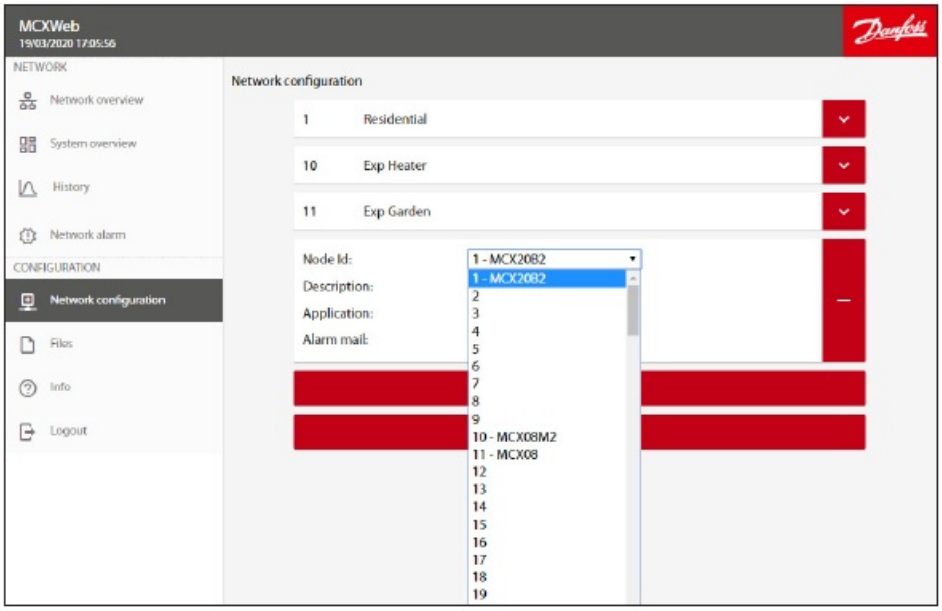



**Network Configuration**

- On this page, you configure which devices you want to access through the MCX Web interface.
- Press ADD NODE to configure each device on your network.
- Press SAVE to save the changes.
- After the configuration, the device is shown on the Network Overview page.

**Node ID**

- Select the ID (CANbus address) of the node that will be added.
- The devices that are physically connected to the network are automatically displayed in the dropdown list of Node Id.




- You can also add a device that is not connected yet, selecting the ID that it will have.

**Description**

- For each device in the list, you can specify a description (free text) that will be displayed on the Network overview page.

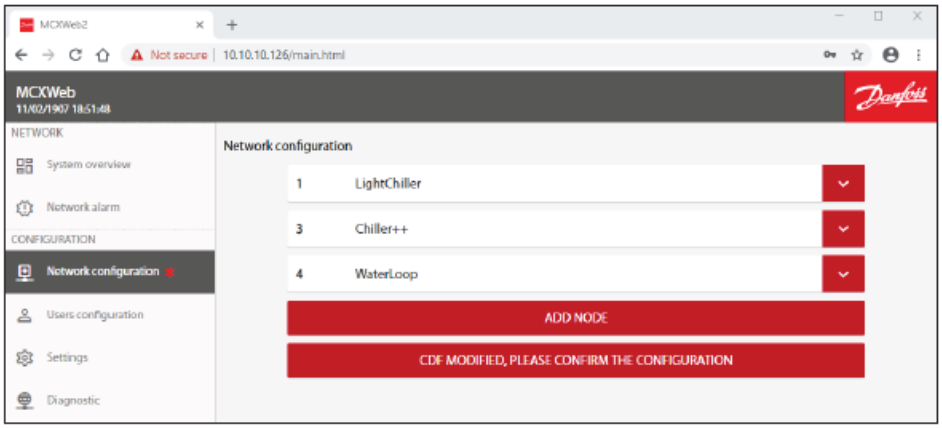
**Application and CDF**

- For each device in the list, you must specify the application description file (CDF).
- The application description file is a file with a CDF extension containing the description of variables and parameters of the software application running in the MCX device.
- CDF must be 1) created 2) loaded 3) associated.

1. **Create the CDF with MCXShape**
    - Before creating the CDF, use the MCXShape tool to configure the MCX software application according to your needs.
    - The CDF file of the MCX software application has the CDF extension and it is created during the Generate and Compile" procedure by MCXShape.
    - The CDF file is saved in the folder App\ADAP-KOOL\edf of the software application.
    - It is required MCXShape v4.02 or higher.

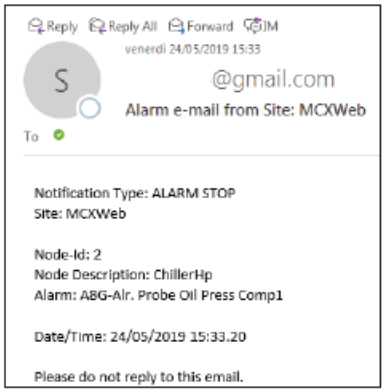
2. **Load the CDF**
    - Load the CDF in the MCX15/20B2 as described in 3.4 Files
3. **Associate the CDF**

- Finally, the CDF must be associated with the device through the combo menu in the Application field.
- This combo is populated with all the CDF files created with the MCXShape and loaded into the MCX15/20B2. **Note:** when you change a CDF file that was already associated with a device, a red star appears aside from the Network configuration menu and you get the following warning message on the Network configuration page: CDF MODIFIED, PLEASE CONFIRM THE CONFIGURATION. Press over it to confirm the change after checking the Network configuration.




**Alarm mail**

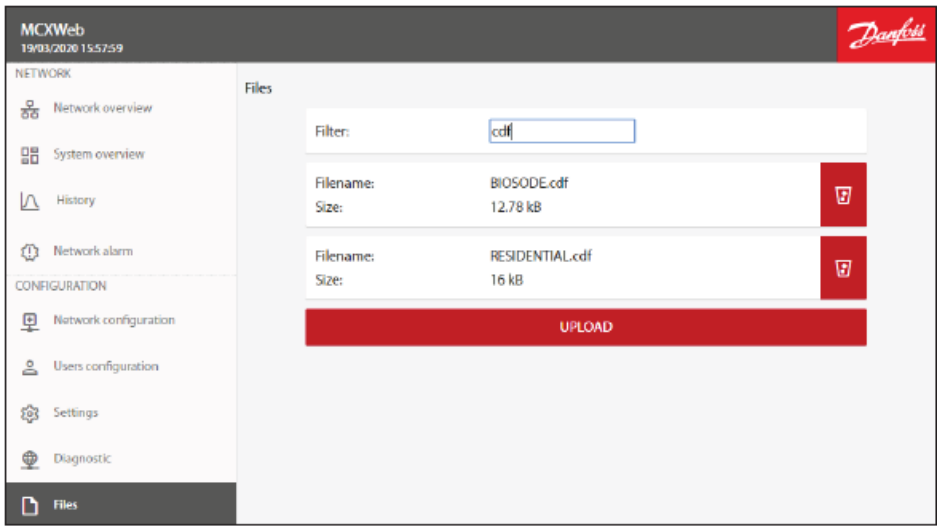
- Tick on Alarm mail to allow email notification from the device.
- The email target is set in Users' Configuration (see 3.5 Users' Configuration).
- The email account of the sender is set in Settings (see 3.2.4 Email notifications)
- Below is an example of an email sent by a device. The Date/Time of the alarm start or stop is when the web server recognizes that event: this may be different from when it occurred, for example after a power off, the Date/Time will be the power on time.




**Files**

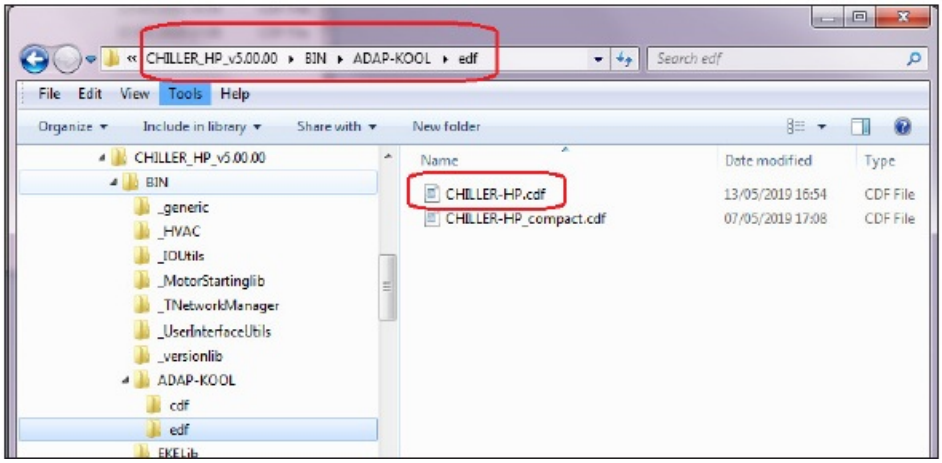
- This is the page used to load any file into the MCX15/20B2 related to the MCX15/20B2 itself and to the other MCX connected to it. Typical files are:
- Application software
- BIOS

- CDF
- Pictures for the overview pages




- Press UPLOAD and select the file that you want to load into the MCX15/20B2.

**Example of CDF file**



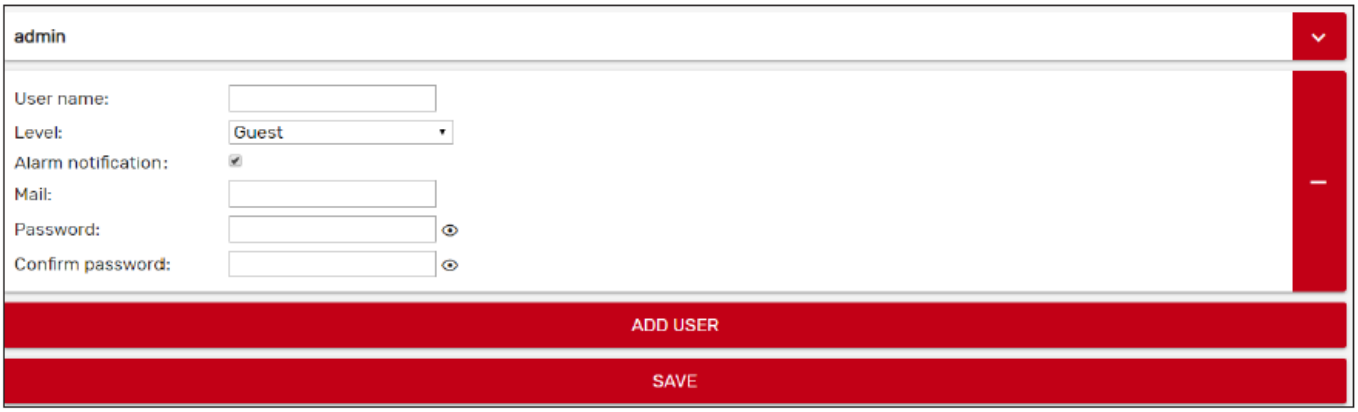

**Users' Configuration**

- This is the list of all the users that can access the Web interface. Click on ADD USER to add a new user or on "-"to delete it.
- There are 4 possible levels of access: guest (0), maintenance (1), service (2), and admin (3). These levels correspond to the levels assigned in the CDF by the MCXShape tool.

**Each level has associated specific permissions:**

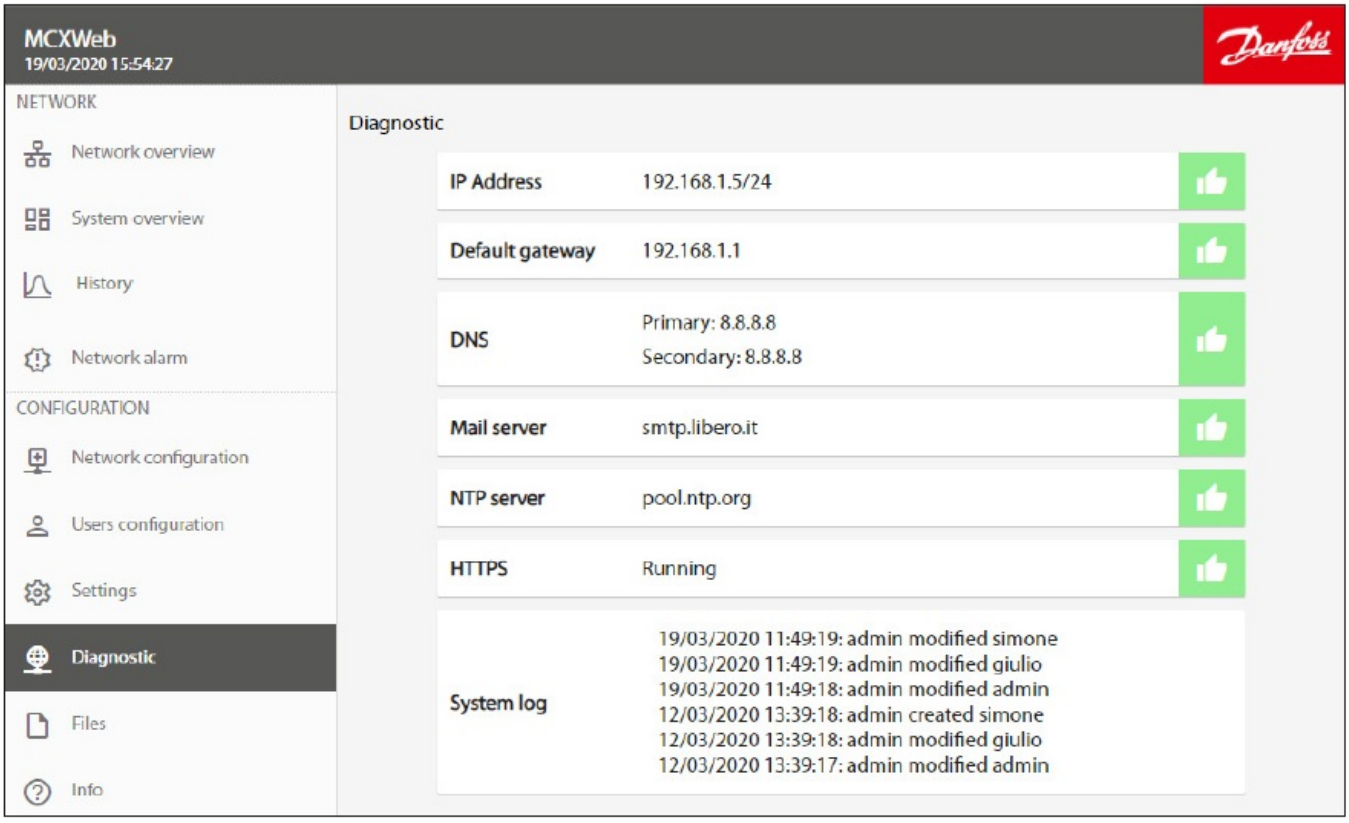
| Permissions | Admin (3) | Service (2) | Maintenance (1) | Guest (0) |
|---|---|---|---|---|
| Parameter settings | ✓ | ✓ | ✓ | ✓ |
| Modify overview page | ✓ | | | |
| Alarms | ✓ | ✓ | ✓ | ✓ |
| Runtime chart | ✓ | ✓ | ✓ | ✓ |
| Backup / Copy / Clone | ✓ | ✓ | | |
| Upgrade | ✓ | ✓ | | |
| Device info | ✓ | ✓ | ✓ | ✓ |
| Network overview | ✓ | ✓ | ✓ | ✓ |
| History | ✓ | ✓ | ✓ | ✓ |
| Network alarms | ✓ | ✓ | ✓ | ✓ |
| Network configuration | ✓ | ✓ | | |
| User configuration | ✓ | | | |
| Settings | ✓ | | | |
| Diagnostic | ✓ | | | |
| Files | ✓ | ✓ | | |
| Info | ✓ | ✓ | ✓ | ✓ |

**Note:** you can see only the users with the level equal or lower than the one you are logged in with.



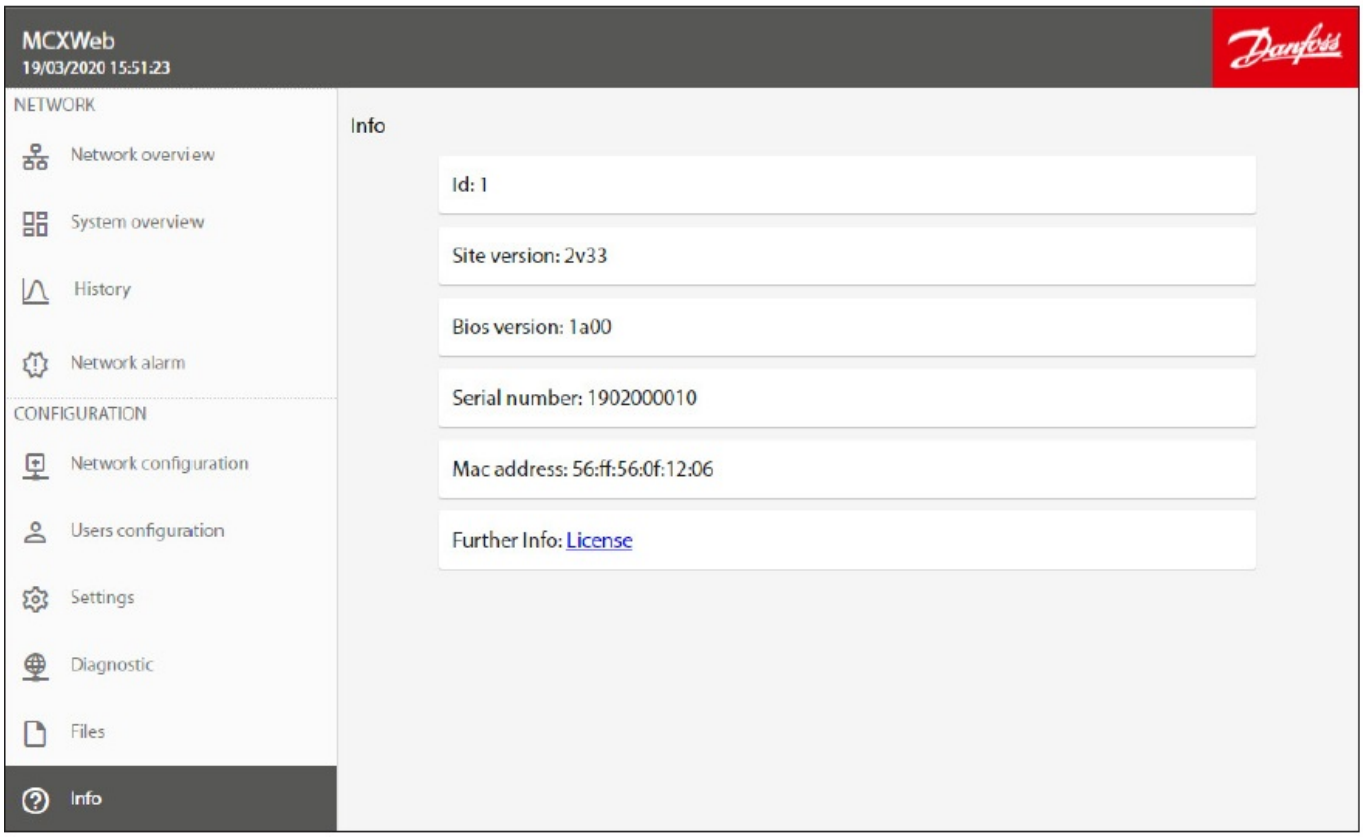

- Select the Alarm Notification check box to send notification emails to the user when alarms occur in any device in the CANbus network enabled to send email (see 3.3 Network Configuration).
- The target address for emails is defined in the Mail field of the user.
- See also 3.2.4 Email notifications, on how to set the SMTP mail server.
- The password must be at least 10 characters in length.

**Diagnostic**




- This section is useful for verifying your network configuration and seeing which protocols are active and whether the corresponding destinations are reachable, if relevant.
- In addition, a System log is displayed where events of major importance concerning security are recorded.

**Info**




- This page displays the following information relating to the current MCX15/20B2 device:
- **Id:** address in the CANbus network

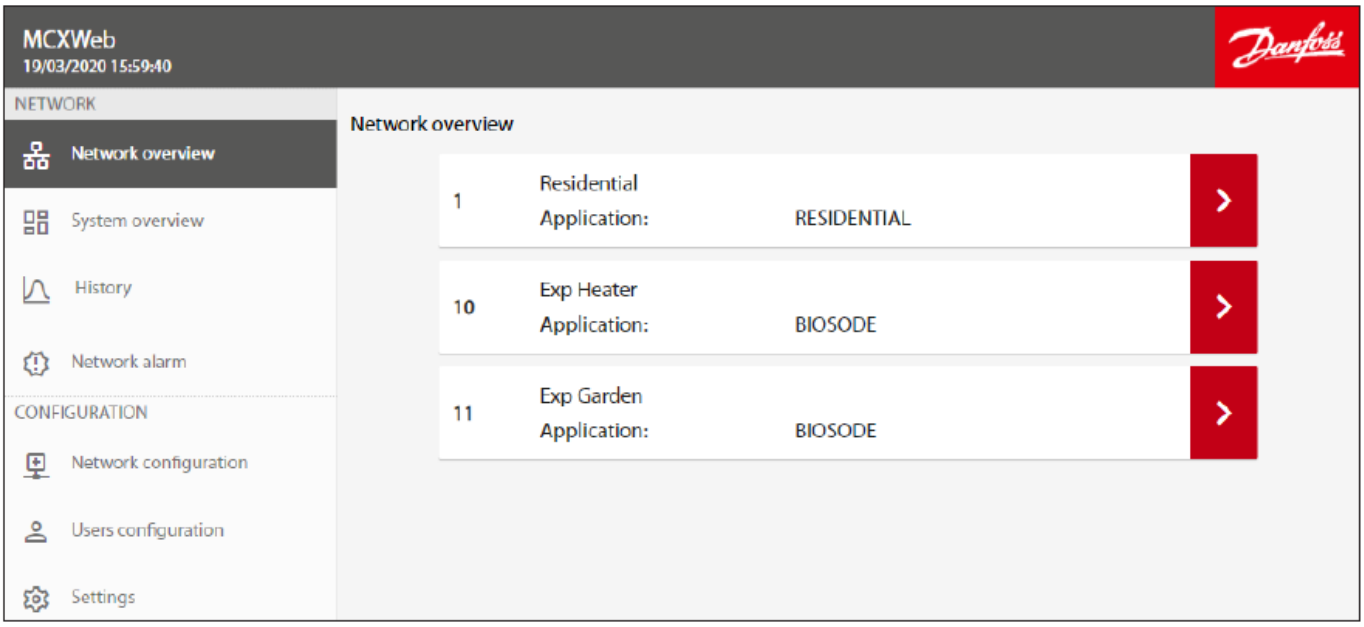
- **Site version:** version of the web interface
- **BIOS version:** version of the MCX15/20B2 firmware
- **Serial number** of MCX15/20B2
- **Mac address** of MCX15/20B2
- **Further Info:** license information

#### Logout

Select this to log out.

### Network

#### Network overview

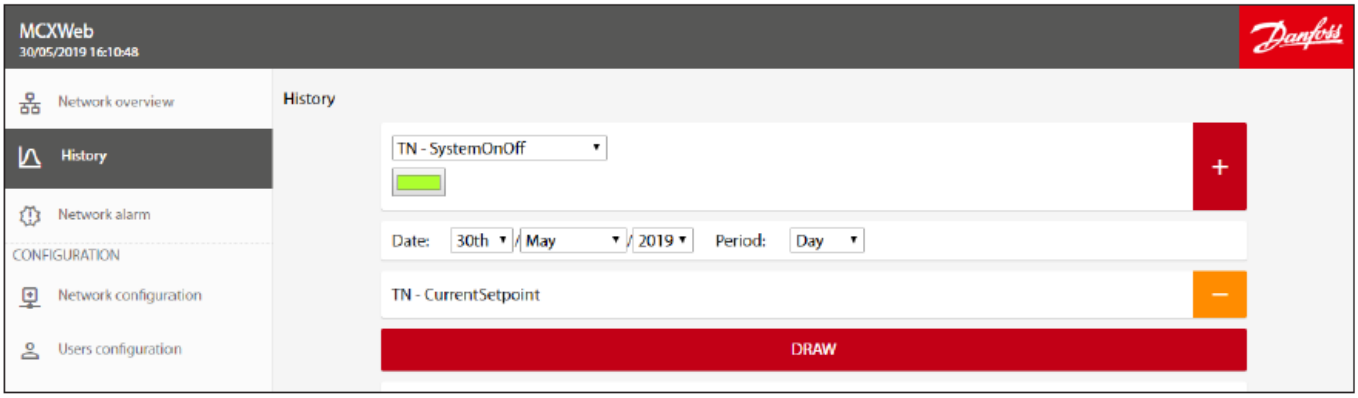



- The Network overview is used to list the main controller MCX15/20B2 and all the devices configured in the Network Configuration and connected to the main controller through Fieldbus (CANbus).
- For each configured MCX the following information is displayed:
- Node ID, which is the CANbus address of the device
- Device Name (e.g. Residential), which is the name of the device. This is defined in Network Configuration
- Application, this is the name of the application software running in the device (e.g. RESIDENTIAL).
- The application is defined in Network Configuration.
- Communication status. If the device is configured but not connected, a question mark is shown on the right side of the device line. If the device is active, a right arrow is displayed
- If you click over the right arrow of the line with the device you are interested in, you will enter the device-specific pages.

#### System overview

See 5.1.2 Creation of a Customized System Overview page.

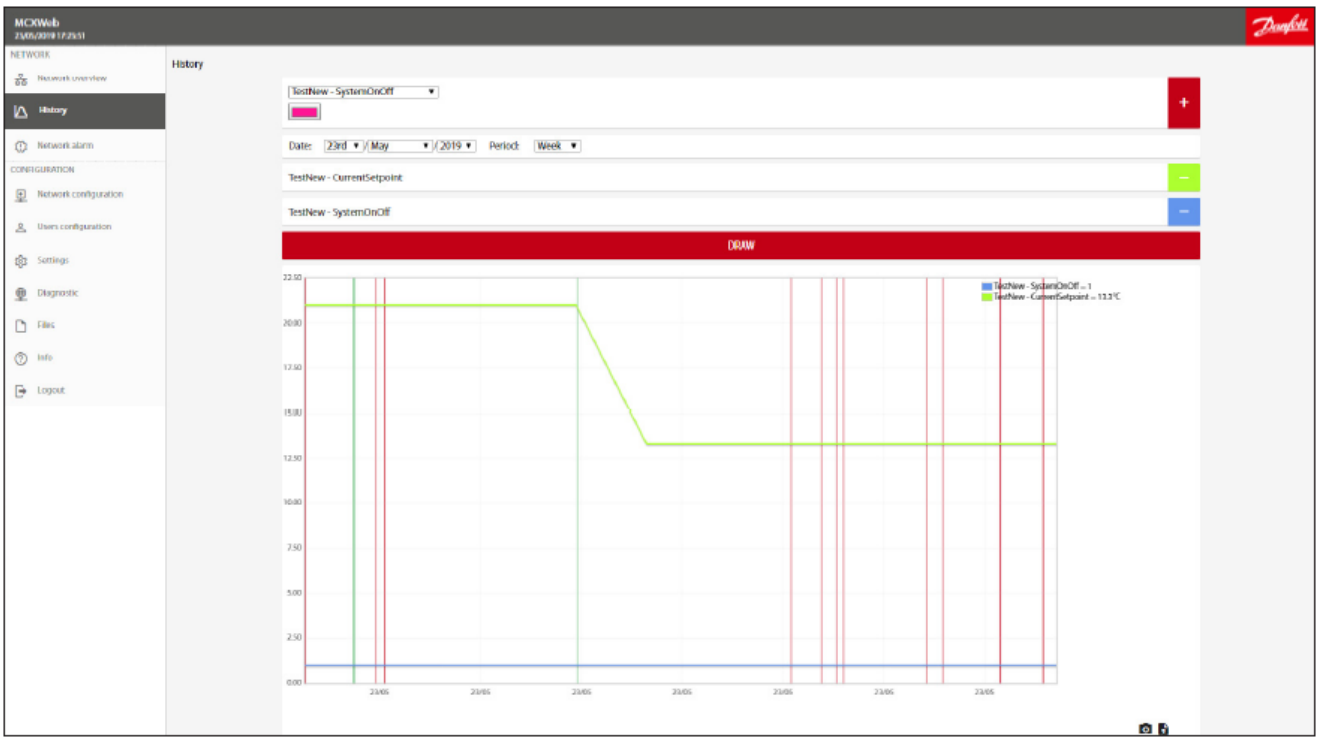
#### History




- The History page will show the historical data stored in the MCX15-20B2 if the application software on the MCX has been developed to store them.

**Note:**

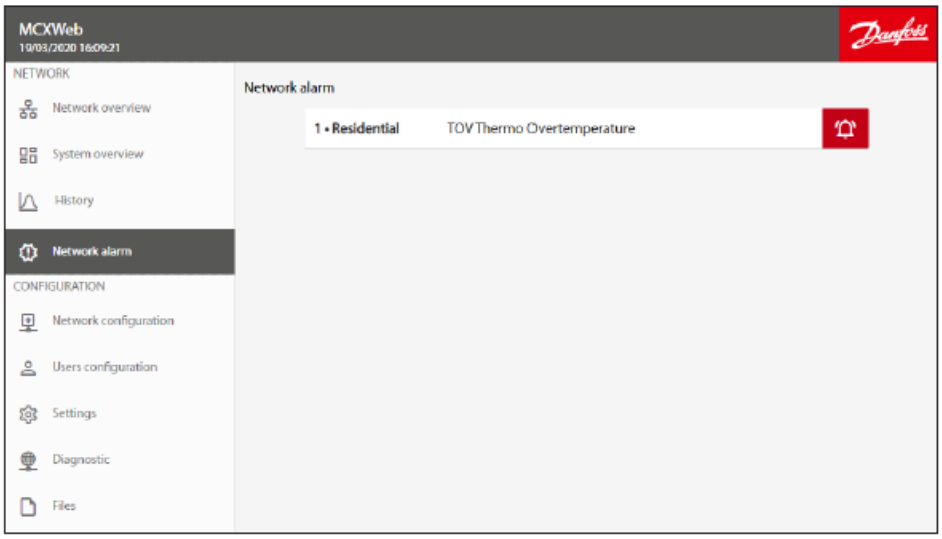
- Your application on the MCX must use the software library LogLibrary v1.04 and MCXDesign v4.02 or greater.
- History must be enabled in Settings (see 3.2.5 History).
- Each MCX software application defines the set of variables that are logged. The drop-down list only shows the available variables.
- If you can't see any variables, check that the name of the history file in Settings is correct and corresponds to the name used by the application software (see 3.2.5 History).
- Select the variable you want to view, the color of the line in the graph, and set the date/time interval.
- Press "+"to add the variable and "-" to remove it.
- Then press DRAW to view the data.

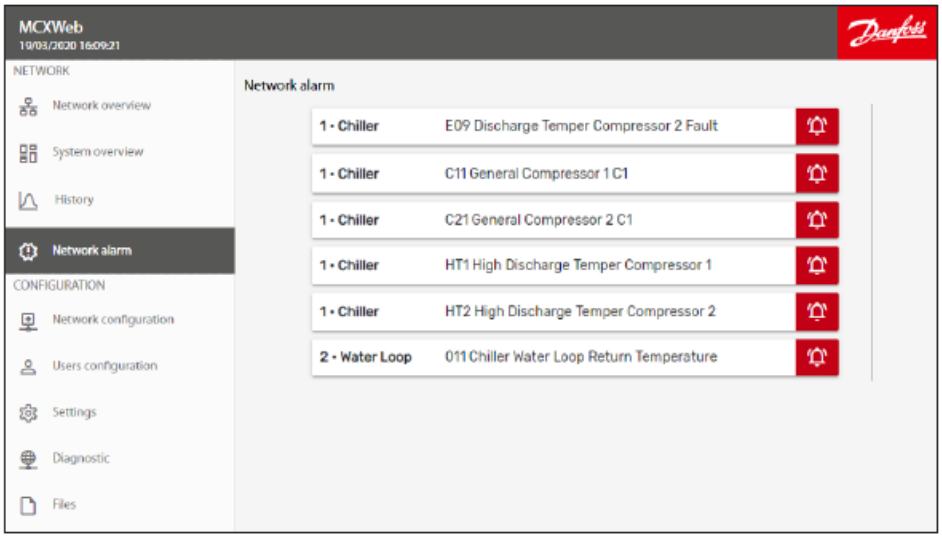



- Use your mouse to zoom in on your graph by using the click+drag option.
- This feature is not available on the mobile version of the pages.
- Press the camera icon to take a snapshot of the chart.
- Press the File icon to export displayed data in CSV format. In the first column, you have the time stamp of points in Unix Epoch time, which is the number of seconds that have elapsed since 00:00:00 Thursday, 1

January 1970.

- Note that you can use Excel formulas to convert the Unix time, e.g =((((LEFT(A2;10) & “,” & RIGHT(A2;3))/60)/60)/24)+DATE(1970;1;1) where A2 is the cell with the Unix time.
- The cell with the formula should then be formatted as gg/mm/aaaa hh:mm: ss or similar.
- **Network Alarm**

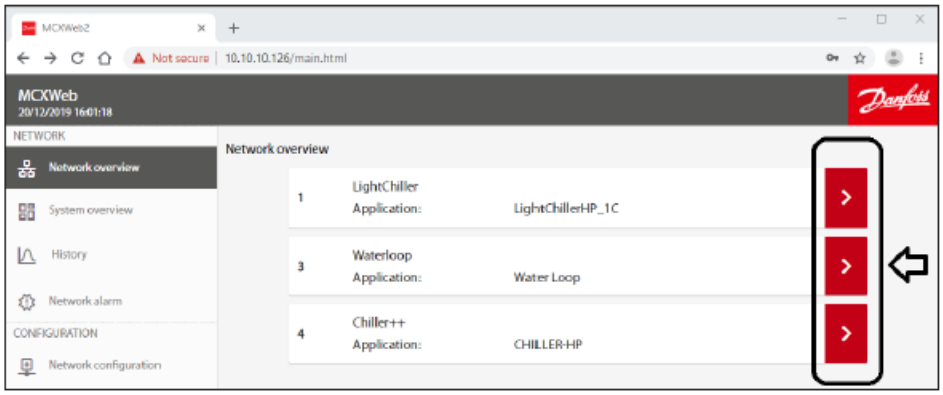


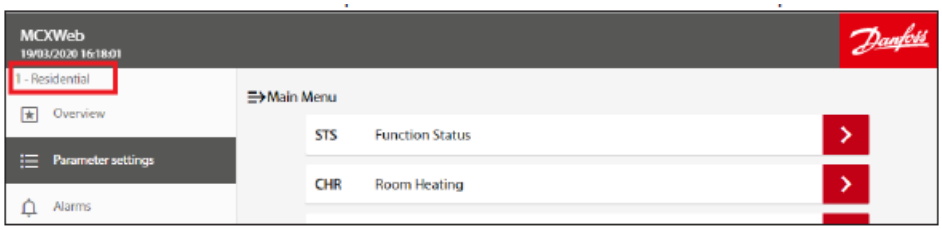

- This page shows the list of the alarms active for all the devices connected to the fieldbus (CANbus).
- Alarms for each device are also available on the device pages.

## Device Pages

From the Network overview page, if you click over the right arrow of a specific device you will enter the device-specific pages.

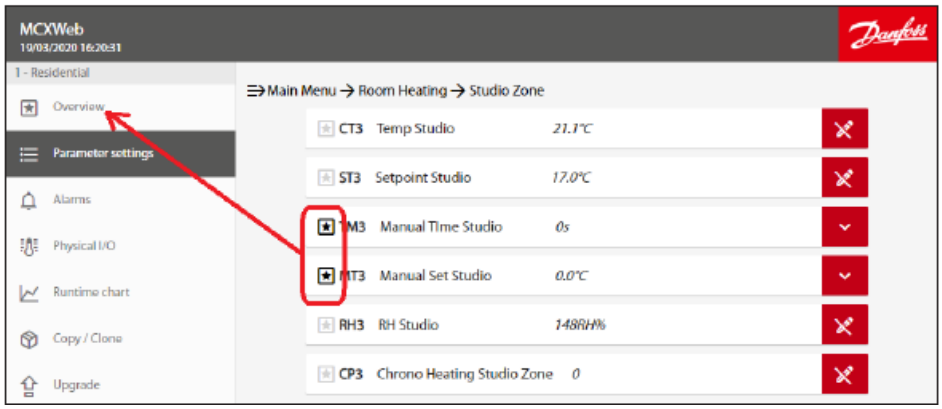


- The Fieldbus address and node description of the selected device are shown at the top of the menu:



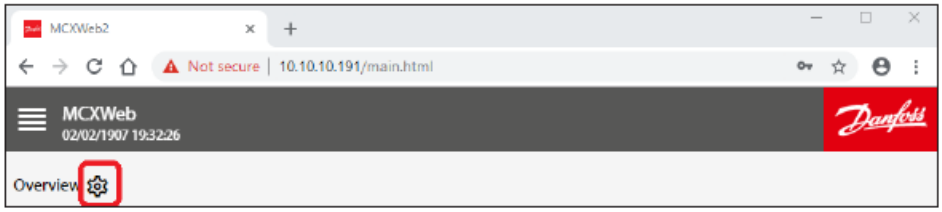

**Overview**

- The overview page is typically used to show the main application data.
- By pressing the Favorite icon on the left side of a variable, you make it automatically visible on the Overview page.

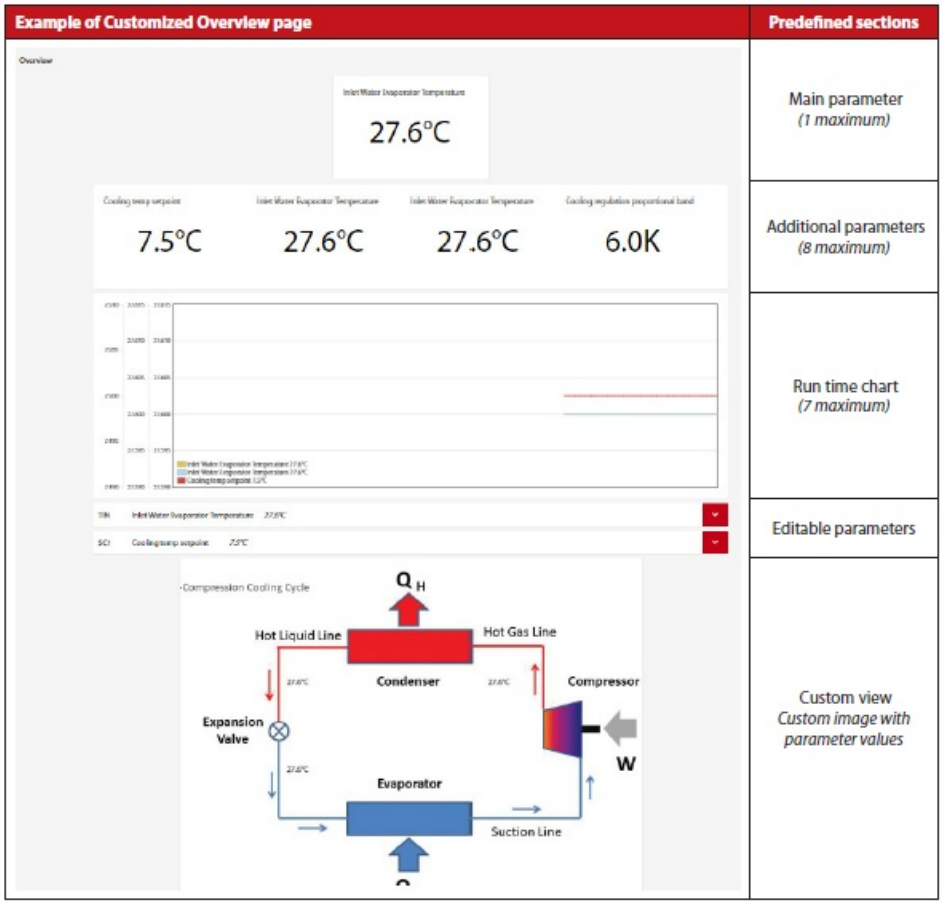



**Customization of the Overview page**

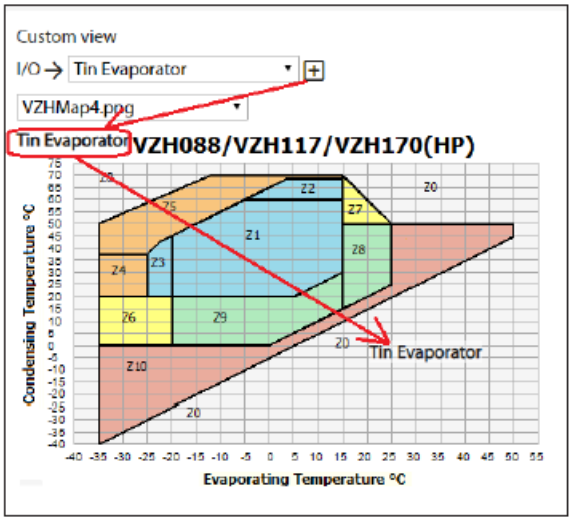
- Pressing the Gear icon on the Overview page, you can customize it further using a predefined format.




**The format is as follows:**




- The Editable Parameters are those selected by pressing the Favorite icon on the left side of a variable (see 5.1 Overview).
- You can add or remove new parameters to this list from this Overview configuration page.
- The Custom View is the section where you define which image you want to display in the Overview and what the data is for the values you want to show over the picture.




**To create a Custom view, follow these steps:**

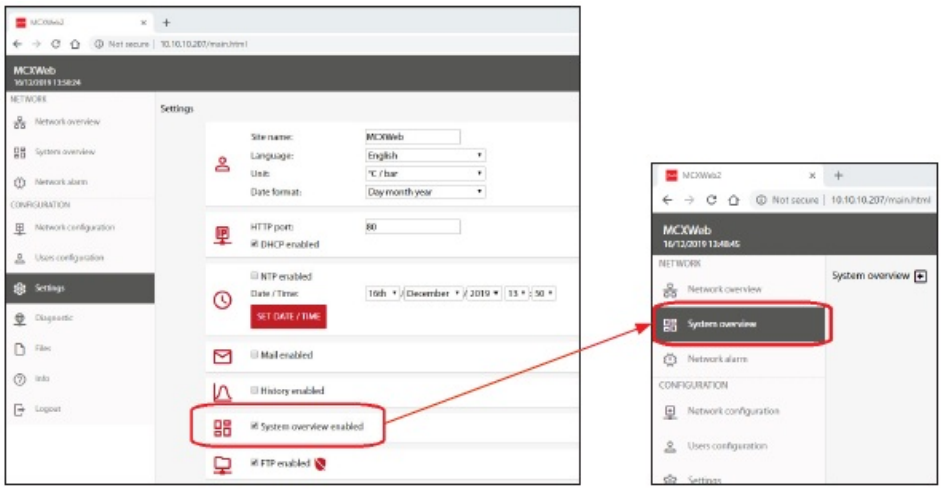
1. Load an image, e.g. VZHMap4.png in the figure above
2. Select a variable to display over the image, e.g. the input Tin Evaporator
3. Drag and drop the variable over the image in the desired position. Drag and drop it outside the page to remove it
4. Right-click over the variable to change the way it will be displayed. The following panel will appear:


**If you select the Type=On/Off Image:**


- The Image on and Image off fields can be used to associate different images to the ON and OFF values of a Boolean variable. A typical usage is to have different icons for the alarm ON and OFF states.
- The On/ Off images must have been loaded previously through the Files menu (see 3.4 Files).

**Creation of a Customized System Overview page**

- A System Overview page is a page that collects data from different devices in the network.
- If you follow the instructions below you can create a System Overview page and display data over a picture of the system.
- In Settings, tick on System Overview enabled to enable the System Overview page. In the Network section of the menu, the line System Overview will appear.

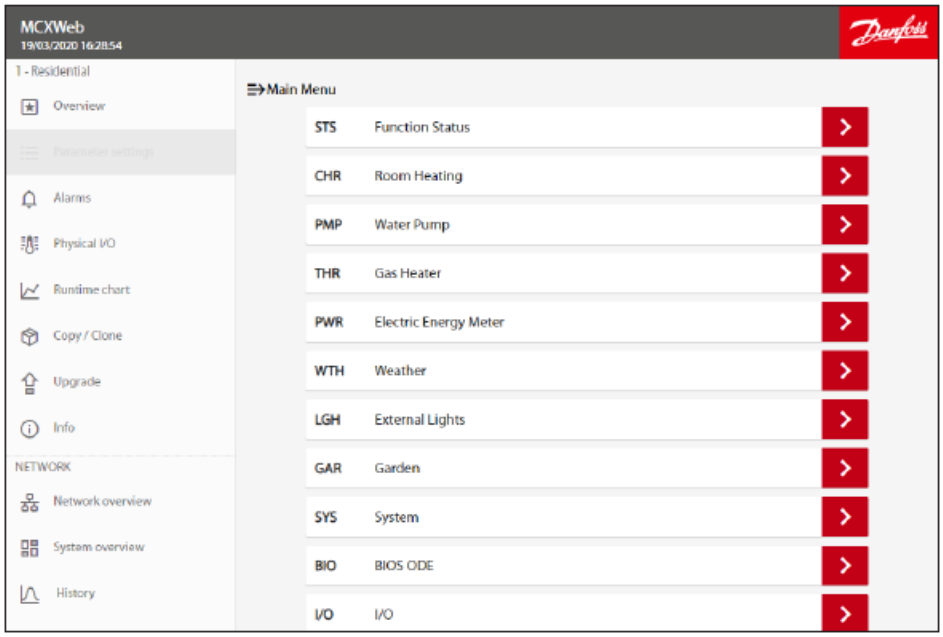



- Press the Gear icon on the System Overview page to customize it.
- Select the node in the network from which you want to select the data and then follow steps 1-4 described in 5.1.1 Customization of the Overview page.

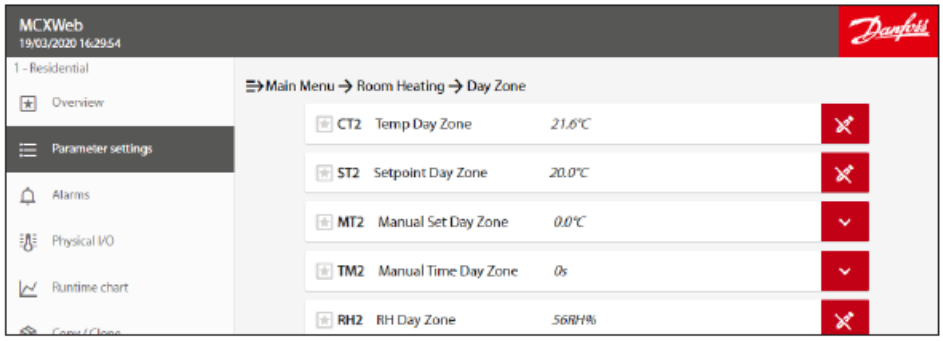
**Parameter settings**

- On this page, you have access to the different parameters, virtual input/output (I/O functions) values, and main commands by navigating the menu tree.

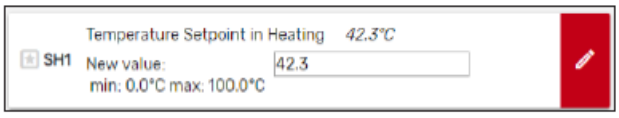
- The menu tree for the application is defined with MCXShape.



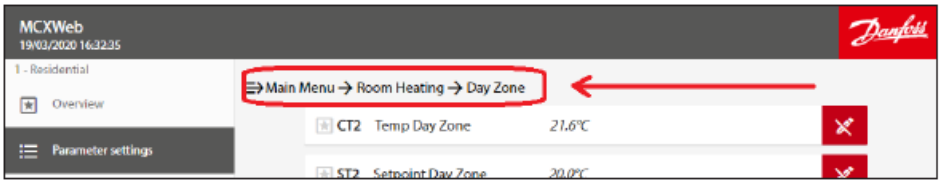

- When the parameters are displayed, you can check the current value and the unit of measurement for each of them.



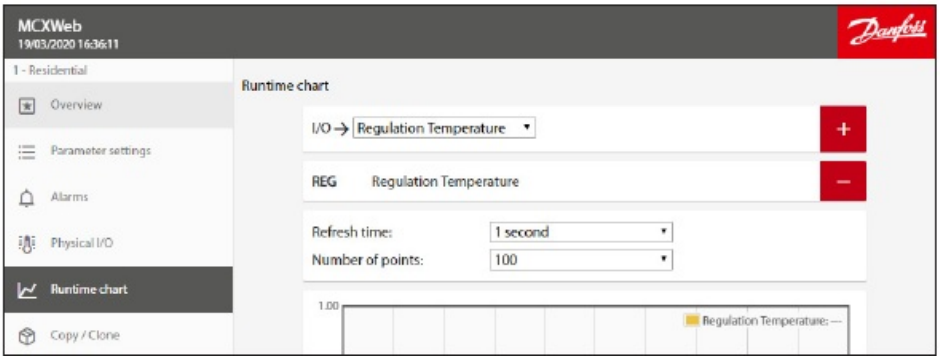

- To change the current value of a writable parameter, click on the down arrow.




- Edit the new value and click outside the text field to confirm.
- **Note:** Min. and max. value is monitored.
- To move through the parameter tree, you can click on the desired branch at the top of the page.




- **Alarms**
  - On this page are all the alarms active in the device.
- **Physical I/O**
  - On this page are all the physical inputs/outputs.
- **Runtime chart**
  - On this page, you can select the variables to populate the real-time graph.
  - Navigate the menu tree and select the variable you want to graph. Press “+” to add it and “-“ to delete it.




- The X-axis of the graph is the number of points or samples.
- The period to display in the graph window is defined by Refresh time x Number of points.


- Press the camera icon to take a snapshot of the chart.
- Press the File icon to export displayed data in CSV format. In the first column, you have the time stamp of points in Unix Epoch time, which is the number of seconds that have elapsed since 00:00:00 on Thursday, 1 January 1970.
- Note that you can use Excel formulas to convert the Unix time, e.g.
- =((((LEFT(A2;10) & "," & RIGHT(A2;3))/60)/60)/24)+DATE(1970;1;1) where A2is the cell with the Unix time.
- The cell with the formula should then be formatted as gg/mm/aaaa hh:mm: ss or similar.

**Copy/Clone**

- This page is used to save and restore the current value of parameters. It allows you to make a backup of your configuration and to replicate, if necessary, the same configuration or a subset of it in a different device when the same software application is running.
- The selection of parameters to be backed up and restored is made when you configure your MCX application through the MCXShape configuration tool. In MCXShape, when the Developer mode is enabled, there is a column "Copy Type" with three possible values:
  **Don't Copy:** identifies parameters that you do not want to save in the backup file (e.g. Read Only parameters)
- **Copy:** identifies parameters that you want to save in the backup file and that can be restored with the Copy and the Clone functionalities in the web interface (see 5.6.2 Copy from File)
- **Clone:** identifies parameters that you want to save in the backup file and that will be restored only with the Clone functionality in the web interface (see 5.6.3 Clone from file) and that will be skipped by the Copy functionality (e.g. Canbus ID, baud rate, etc).

**Backup**

- When you press on START BACKUP, all the parameters with the attributes Copy or Clone in the column Copy Type of MCXShape configuration tool will be saved into the file BACKUP_ID_Applicationname in your Download folder, where ID is the address in the CANbus network and the Application name is the name of the application running in the device.

**Copy from File**

- The Copy function allows you to copy some of the parameters (those marked with the attribute Copy in the column Copy Type of MCXShape configuration tool) from the backup file to the MCX controller.
- Parameters marked with Clone are excluded from this type of copy.

**Clone from file**

- The Clone function allows you to copy all the parameters (marked with the attribute Copy or Clone in the column Copy Type of MCXShape configuration tool) from the backup file to the MCX controller.

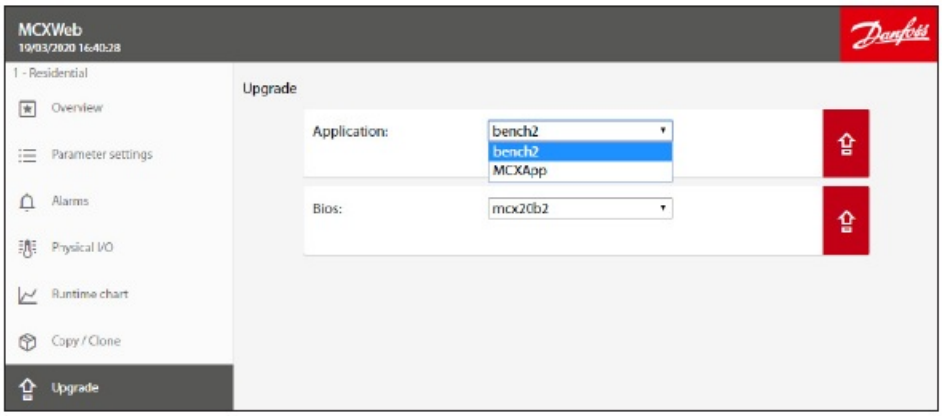
**Upgrade**

- This page is used to upgrade the applications (software) and BIOS (firmware) from the remote.
- The target controller can be both the MCX15-20B2 device or other controllers connected through the Fieldbus (CANbus), where the upgrade progress is shown in the upgrade tab.

**To proceed with the application and/or BIOS update, follow these steps:**

**Application Upgrade**

- Copy the software application file, created with the MCXShape with the pk extension, into the MCX15/20B2 as described in 3.4 Files.
- On the Upgrade page, select from the Application combo menu the application you wish to upgrade on the device from all the pk files you have loaded.
- Confirm the update by pressing the upgrade icon (up arrow).
- It is recommended that you power off the device after the upgrade




- After the application upgrade, also remember to upgrade the related CDF file (see 3.4 Files) and the
- Network configuration (see 3.3.3 Application and CDF).
- **Note:** applications can also be upgraded via USB, see 7.2.1 Install application upgrades from USB flash drive.

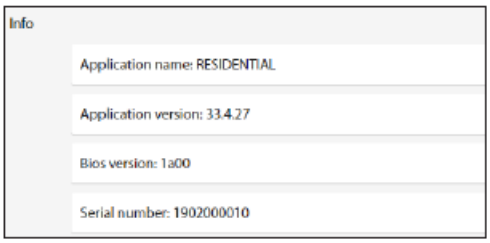
**BIOS Upgrade**

- Copy the BIOS file, with the bin extension, into the MCX15/20B2 as described in 3.4 Files.
- **Note:** do not change the file name of the BIOS or it will not be accepted by the device.
- On the Upgrade page, select from the Bios combo menu the BIOS you wish to upgrade on the device from all

the BIOS files you have loaded.

- Confirm the update by pressing the upgrade icon (up arrow).
- If you have selected the appropriated BIOS (bin file) for the current MCX model, then the BIOS update procedure will start.
- **Note:** if the BIOS of the MCX you are connected to the web interface with is upgraded, you will need to log into the web interface again once the device has completed the reboot.
- **Note:** The BIOS can also be upgraded via the USB, see 7.2.2 Install BIOS upgrades from USB flash drive.

**Device Info**



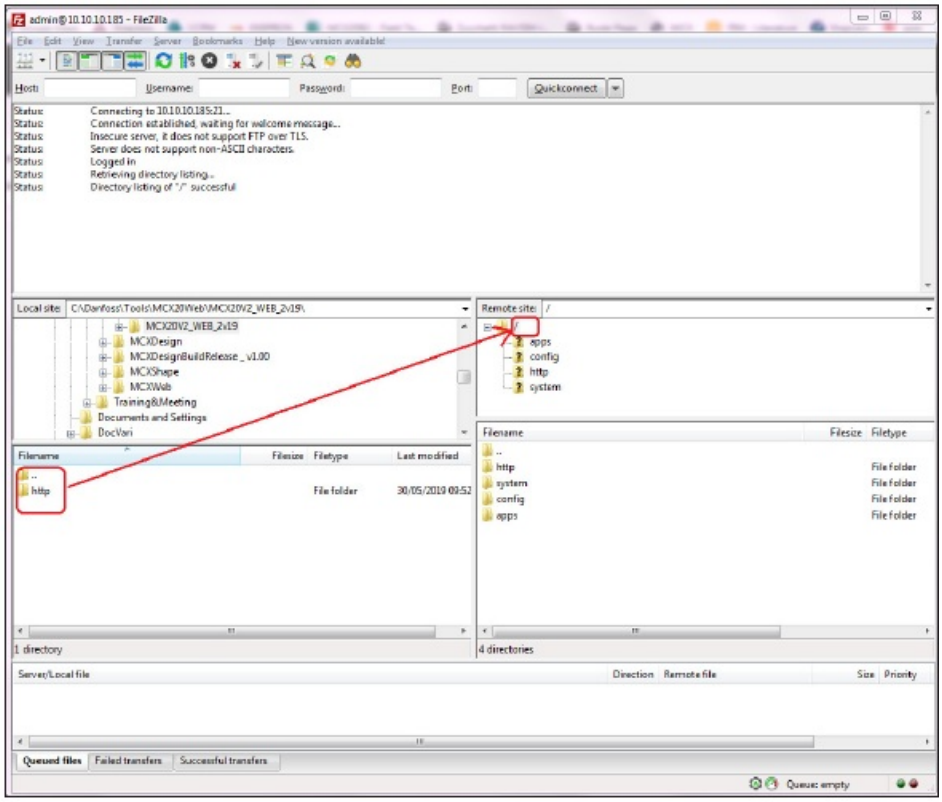

- On this page, the main information relating to the current device is displayed.

## Install web page updates

- New web pages can be updated via FTP if enabled (see 3.2.6 FTP):
- The web pages package is made of files grouped in four folders which must replace the ones in the MCX15/20B2.
- To update the pages, it is sufficient simply to overwrite the HTTP folder, as the others will be created automatically.

**Notes:**

- It is recommended that you stop running the application on MCX15/20B2 before starting the FTP communication. To do this, press and release X+ENTER immediately after powering up to enter the
- BIOS menu. At the end of the FTP communication, select APPLICATION from the BIOS menu to start the application again.
- After the upgrade of the web pages, it is mandatory to clean the cache of your browser (e.g. with CTRL+F5 for Google Chrome).




**USB Read current network configuration without web interface**

- If you can't access the web interface, you can still read the network configuration using a USB flash drive:
- Make sure the USB flash drive is formatted as FAT or FAT32.
- Within 10 minutes of MCX15/20B2 powering up, insert the USB flash drive into the USB connector of the device.
- Wait about 5 seconds.
- Remove the USB flash drive and insert it into a PC. The file mcx20b2.cmd will contain the basic information about the product.

**Here is an example of the content:**

```
[node_info]
ip=10.10.10.45/24
mac_address=00:07:68:ff:ff:f6
sw_descr=MCX20B2  0c41
node_id=1
CANBaud=50000
Key=bsFJt3VWi9SDoMgz
```

```
< - Current ip address
< - Mac address
< - Bios software description
< - CANbus Node ID
< - CANbus baudrate
< - Temporary key generated at file
creation
```

**BIOS and Application upgrade**

- A USB flash drive can be used to upgrade the BIOS and application of MCX15-20B2.
- Both can also be upgraded via web pages, see 5.8 Upgrade.

**Install application upgrades from the USB flash drive**

- To update the MCX15-20B2 application from a USB flash drive.

- Make sure the USB flash drive is formatted as FAT or FAT32.
- Save the firmware in a file named app. pk in the root folder of the USB flash drive.
- Insert the USB flash drive into the USB connector of the device; turn it off and on again and wait a few minutes for the update.
- **Note:** do not change the file name of the application (it must be app. pk) or it will not be accepted by the device.

**Install BIOS upgrades from USB flash drive**

- To update the MCX15-20B2 BIOS from a USB flash drive.
- Make sure the USB flash drive is formatted as FAT or FAT32.
- Save the BIOS in the root folder of the USB flash drive.
- Insert the USB flash drive into the USB connector of the device; turn it off and on again and wait a few minutes for the update.
- **Note:** do not change the file name of the BIOS or it will not be accepted by the device.

**Emergency actions through USB**

- It is possible to recover the unit in case of emergencies by providing some commands through the USB.
- These instructions are for expert users and assume familiarity with the INI file format.
- The available commands allow the user to perform the following operations:
- Reset the network settings to default
- Reset the user configuration to the default
- Format the partition that contains pages and configurations

**Procedure**

- Follow the instructions in 7.1 Read the current network configuration without the web interface to generate the file mcx20b2.cmd.
- Open the file with a text editor and add the following lines to perform special operations as described in the table below.

| **Command** | **Function** |
|---|---|
| ResetNetworkConfig=1 | Reset the network settings to default:<br>• DHCCP enabled<br>• FTP enabled<br>• HTTPS disabled |
| ResetUsers=1 | Reset the user configuration to default:<br>• User=admin<br>• Password=PASS |
| Format | Format the partition containing web pages and configurations |

Insert the USB flash drive back into the MCX15/20B2 to execute the commands

**Example:**

```
[node_info]
ip=10.10.10.45/24
mac_address=00:07:68:ff:ff:f6
sw_descr=MCX20B2  0c41
node_id=1
CANBaud=50000
Key=bsFJt3VWi9SDoMgz

ResetNetworkConfig=1
```

- This will reset the network settings.
- **Note:** the commands will not be re-executed if you remove and insert the USB flash drive again. The Key line in the node-info section is for doing this.
- To execute new commands, you must delete the mcx20b2.cmd file and re-generate it.

#### Data logging

A USB flash drive can be used to store historical data, see 4.2 History.

## Security

#### Security information

- MCX15/20B2 is a product with functions that support the security in the operation of machines, systems, and networks.
- Customers are responsible for preventing unauthorized access to their machines, systems, and networks. These must be connected to a corporate network only or the Internet if and to the extent that such connection is necessary and only when appropriate security measures are in place (e.g. firewall). Contact your IT department to ensure that the device is installed according to your company's security policies.
- MCX15/20B2 is continuously developed to make it safer, therefore is recommended that you apply product updates as they become available and use the latest product versions.
- Use of product versions that are no longer supported and failure to apply the latest updates may increase customers' exposure to cyber threats.

#### Security architecture

- MCX15/20B2 architecture for security is based on elements that can be grouped into three main building blocks.
- foundation
- core
- monitoring and threats

**Foundation**

- The foundation is part of hardware and basic low-level drivers that ensure access restriction at the HW level, that the device is operated with genuine Danfoss software, and includes the basic building blocks needed by the core components.

**Core**

- The core building blocks are the central part of the security infrastructure. It includes support for cipher suites, protocols, and user and authorization management.

**Authorization**

- User Management
- Access control to configuration
- Access control to application/machine parameters

**Policies**

- Strong password enforcement.
- A change of the default password is enforced on the first access. This is mandatory as it would be a major security leak.
- In addition, a strong password is enforced according to minimum requirements policy: at least 10 characters.
- Users are managed only by the administrator
- User passwords are stored with a cryptographic hash
- Private keys are never exposed

**Secure Update**

- The update manager software library verifies that the new firmware has a valid digital signature before starting the update process.
- Cryptographic Digital Signature
- Firmware roll-back guaranteed if not valid

**Factory Configuration**

- From the factory, the web interface will be accessible without security.
- HTTP, FTP
- 1st access administrator password selection with a strong password is required

**Certificates**

- A dedicated certificate is needed to access the web server over HTTPS.
- The certificate management including any updates is the responsibility of the customer.

**Reset Default Settings and Recovery**

- The Reset to default parameters are available through a special command with the USB port. Physical access to the device is considered to be an authorized access.
- As such the reset of network settings or reset of user passwords can be executed without further restrictions.

**Monitoring**

- Track, inform, and respond to security threats.

**Response**

- There are some response strategies implemented to mitigate the risk of brute force cyber-attacks.

**This kind of attack can work on different levels:**

- on the login API, thus trying continuously different credentials for access
- using different session tokens
- In the first instance, progressive delays are implemented to mitigate the risk, whilst for the second one a warning email is sent out and a log entry is written.

**Log and email**

- To keep track of and inform the user/IT about threats the following services are available:
- Log of security-related events
- Reporting of events (email to the administrator)

**Events relevant to security are:**

- Too many attempts to log in with the wrong credentials
- Too many requests with the wrong session ID
- Changes to account settings (password)
- Changes to security settings
- Danfoss can accept no responsibility for possible errors in catalogs, brochures, and other printed material. Danfoss reserves the right to alter its products without notice.
- This also applies to products already on order provided that such alterations can be made without subsequential changes being necessary in specifications already agreed.
- All trademarks in this material are the property of the respective companies.
- 
- **www.danfoss.com**

## Documents / Resources

| | |
|---|---|
|  | Danfoss MCX15B2 Programmable Controller [pdf] User Guide<br>MCX15B2 Programmable Controller, MCX15B2, Programmable Controller, Controller |
|  | Danfoss MCX15B2 Programmable Controller [pdf] User Guide<br>MCX15B2, MCX15B2 Programmable Controller, Programmable Controller, Controller |

## References

- User Manual