INSTALLATION AND OPERATING MANUAL

EN

Display and power supply interface

DIRIS Digiware D-50 & D-70 v2

socomec
Innovative Power Solutions

CONTENTS

1. DOCUMENTATION 4
2. HAZARDS AND WARNINGS 5
2.1. Risk of electrocution, burns or explosion 5
2.2. Risk of damaging the device 5
2.3. Liability 5
3. PRELIMINARY OPERATIONS 6
4. PREREQUISITES 6
5. CYBER SECURITY RECOMMENDATIONS & BEST PRACTICES* 7
6. INTRODUCTION 9
6.1. Range 9
6.2. Introduction to DIRIS Digiware D 9
6.2.1. Introduction to DIRIS Digiware D-50 9
6.2.2. Introduction to DIRIS Digiware D-70 10
6.3. Touchscreens 11
6.4. LED display 12
6.5. Navigation 12
6.6. Menu structure 13
6.7. Dimensions 14
7. MOUNTING 15
7.1. Recommendations and safety 15
7.2. Door mounting 15
7.3. DIN rail mounting 16
8. COMMUNICATION ARCHITECTURES 17
8.1. RS485 Master 17
8.2. RS485 Slave 17
9. CONFIGURATION 18
9.1. Display settings 19
9.1.1. Language 20
9.1.2. Date / time 20
9.1.3. RS485 communication 21
9.1.4. Ethernet communication 21
9.2. Automatic detection of slave devices 22
9.3. Configuring the DIRIS Digiware system from the D-50/D-70 display 27
9.3.1. Network configuration 29
9.3.2. Load configuration 29
9.3.2.1. Example of a load configuration 29
9.3.2.2. Changing the load settings 31
10. CONFIGURATION VIA EASY CONFIG SYSTEM 33
10.1. USB connection mode 33
10.2. Ethernet connection mode 34

11. WEBSERVER EMBEDDED IN THE D-50/D-70 DISPLAYS 36
11.1. User profiles 36
11.2. Admin profile 39
11.2.1. “Devices” menu 39
11.2.2. “Protocols” menu 42
11.3. Cyber security profile 46
11.3.1. Cyber security menu 46
11.3.2. “Security Policy” tab 47
11.3.3. “HTTPS” tab 48
11.3.4. CAs (FTPS/SMTPS) tab 48
11.3.5. “Firewall” tab 49
11.3.6. Upgrading the firmware of the D-50/D-70 display 49
11.4. WEBVIEW-M 51
12. ALARMS 52
13. USE 53
14. DIRIS DIGIWARE D-50/D-70 TECHNICAL CHARACTERISTICS 54
14.1. Mechanical characteristics 54
14.2. Communication characteristics 54
14.3. Electrical characteristics 54
14.4. Environmental characteristics 54
14.5. EMC characteristics 55

ANNEX I. SNMP COMWMUNICATION WITH THE DIRIS DIGIWARE D-50 / D-70 56
Annex I - 1. SNMP generalities 56
Annex I - 2. SNMP functions supported 56
Annex I - 3. SNMP versions supported 57
Annex I - 4. SNMP ports 57
Annex I - 5. Retrieving data using the DIRIS Digiware D-50 / D-70 MIB file 58
Annex I - 6. SNMP configuration via Easy Config System 60
ANNEX II. BACNET COMMUNICATION WITH THE DIRIS DIGIWARE D-50 / D-70 61
Annex II - 1. BACnet Generalities 61
Annex II - 2. BACnet Objects 61
Annex II - 3. BACnet Services 66
Annex II - 4. BACnet IP configuration via Easy Config System 66
Annex II - 5. BACnet configuration from the embedded webserver 67
ANNEX III. FTP CONFIGURATION 68
Annex III - 1. FTP file export protocol (only available with DIRIS Digiware D-70) 68
Annex III - 1.1. FTP server activation: 68
Annex III - 2. FTP planning configuration 70
Annex III - 3. Understanding the exported .csv file in EMS mode 71
ANNEX IV. FIND AND ADD A SERVER’S CA (CERTIFICATE AUTHORITY) TO A DIRIS DIGIWARE D-50/D-70 . 72

1. DOCUMENTATION

Socomec Resource Center

To download, brochures, catalogues and technical manuals

Related instruction manuals

Additional instruction manuals linked to the DIRIS Digiware system can be found on the Socomec website:

Instruction manual	Reference
DIRIS Digiware - Power Metering and Monitoring System and associated current sensors	542875
WEBVIEW-M - Energy Server embedded DIRIS Digiware M & D	551295
Easy Config System - Configuration Software	551765
Product Upgrade Tool - Software for firmware upgrade	545534

2. HAZARDS AND WARNINGS

The term "device" used in this document covers both DIRIS Digiware D-50 and D-70.

The assembly, use, servicing and maintenance of this equipment must only be carried out by trained, qualified professionals.

SOCOMEC shall not be held responsible for failure to comply with the instructions in this manual.

2.1. Risk of electrocution, burns or explosion

- This device must only be installed and serviced by qualified personnel who have in-depth knowledge of installing, commissioning and operating the device and who have had appropriate training. He or she should have read and understood the various safety measures and warnings stated in the instructions.
- Before carrying out any work on the device, switch off the power supply to the device.
- Always use an appropriate voltage detection device to confirm the absence of voltage.
- Replace all devices, doors and covers before turning on power to this equipment.
- Always power the device with the correct rated voltage.
- Install the device following the recommended installation instructions and in a suitable electrical cabinet.

Failure to take these precautions could cause death or serious injuries.

2.2. Risk of damaging the device

To ensure that the device operates correctly, make sure that:

- The device is correctly installed.
- The auxiliary power supply voltage indicated on the product is observed: 24 VDC ± 15%.
- Use 230 VAC / 24 VDC SOCOMEC power supply (P15 15W 4829 0120) or use a 1 A 24 VDC safety fuse.

Failure to respect these precautions could cause damage to the device.

2.3. Liability

- Assembly, connection and use must be carried out in accordance with the installation standards currently in force.
- The device must be installed in accordance with the rules given in this manual.
- Failure to observe the rules for installing this device may compromise the device's intrinsic protection.
- The device must be positioned within an installation which complies with the standards currently in force.
- Any cable which needs to be replaced may only be replaced with a cable having the correct rating.

3. PRELIMINARY OPERATIONS

To ensure the safety of personnel and the product, please carefully read the contents of these instructions before installation.

Check the following points as soon as you receive the package containing the device:

- The packaging is in good condition
- The device has not been damaged during transportation
- The device reference number conforms to your order
- The packaging includes the device fitted with removable terminal blocks and a Quick start guide.

4. PREREQUISITES

Before commissioning your DIRIS Digiware D-50/D-70 display, make sure it operates under the latest firmware versions.

The latest firmware versions are available on the Socomec website.

The firmware upgrade is done using the Product Upgrade Tool software, by connecting a laptop to the Micro USB port of your DIRIS Digiware D-50/D-70.

The firmware upgrade of the D-50/D-70 can also be done remotely directly from their embedded webserver.

5. CYBER SECURITY RECOMMENDATIONS & BEST PRACTICES*

The DIRIS Digiware D-50/D-70, as any device connected to a user's Ethernet network, must be protected against any risk of cyber-attack or data loss/destruction.

(*) Our D-50/D-70 displays provide certain cyber security features to prevent these attacks and to help users in their responsibility to implement and guarantee adequate IT protection. Some recommendations are listed in the following paragraphs. Make sure they are in line with your IT security policy:

- **Awareness of the security policy:** Users and administrators of DIRIS Digiware D-50/D-70 displays and WEBVIEW-M must be aware of and trained in proper IT security practice (information and compliance with corporate security policy, authentication procedure management and password safety, online session management, risks of fishing…).
- **Network security:** The IT system architecture must be able to safeguard resources, by segmenting the network according to their degree of sensitivity and using a variety of protective devices (firewall, demilitarised zone, VLAN, network anti-virus etc.).

How DIRIS Digiware D-50/D-70 displays can help:

By forcing the user to use secure versions of standard communication protocols:

- FTPS: secure export of data
- SMTPS: secure email notification in case of alarms
- SNMPv3: secure version of the SNMP communication protocol
- HTTPS: secure webserver navigation (WEBVIEW-M) by uploading TLS/SSL certificates

> Refer to paragraphs 11.3.3 & 11.3.4 for more information on how to upload digital certificates.

With their firewall, to monitor and control incoming/outgoing traffic: this protects the DIRIS Digiware D-50/D-70 displays in case of denial-of-service (flooding) attacks, in order to guarantee service continuity of the display.

> Refer to paragraph 11.3.5 for more information on how to configure the firewall protection.

- **Device security:** Device security depends on its network environment, but also user behaviour. In terms of the environment, elementary protective measures (filtering authorised stations by MAC address, opening service ports, selecting authorised applications etc.) are highly recommended. Greater precaution is required on managing removable media (external hard drive, USB flash drive, wireless communication provision etc.). Finally, in terms of a server like the DIRIS Digiware D-50/D-70, it should be protected by controlling and limiting physical access to the rooms and cabinets hosting the device.

How DIRIS Digiware D-50/D-70 displays can help:

DIRIS Digiware D-50/D-70 displays reduce the attack exposure by blocking or restraining the access to certain peripherals and services that are not essential to the customer use case.

> Refer to paragraph 11.3.2 for more information on how to configure your D-50/D-70 display's security policy.

Moreover, the firmware and webserver applications are signed with an asymmetrical key to make sure any firmware upgrade uses the correct matching signature to allow the device to be upgraded. This prevents the diversion of the device from its intended use by Socomec (by uploading a dummy firmware for instance) and guarantees that the firmware stays without virus over time.

- **Data security:** Data security covers several aspects, in particular the confidentiality, integrity, authenticity and availability of data. Special care is required with data security and archiving procedures on backup devices both inside and outside the company.

How DIRIS Digiware D-50/D-70 displays can help:

It is possible to export data such as energy indexes, load curves and historical measurement (Trends), both manually or automatically for back-up.

It is also possible to save the topology (mapping of slaves connected to the D-50/D-70 display) from the embedded webserver and configuration file from Easy Config software.

Confidentiality is addressed by providing 256-bit AES encryption (AES 256) for personal data such as passwords along with product. This means it would take 2256 combinations to break the encryption key.

- **Access and authentication management:** Managing access to resources and data is a crucial element of the IT system's security policy. Each user requires an account and access rights corresponding to their profile. Access to the IT system's resources is controlled by a user authentication process, based on a minimum of a high-security username and password. The password management procedure, specifying the systematic modification of default passwords and their validity period, is included in the IT security policy.

How DIRIS Digiware D-50/D-70 displays can help:

Multiple profiles are available to access the web application. The highest profile is "Cybersecurity", which allows you to manage users' access to the web application based on what is relevant for them.

Profiles are password protected. Certain measures are taken into account in Socomec D-50/D-70 displays to reduce the risk of password theft:

- Encryption of credentials
- Password must meet minimum security requirements (minimum 10 characters, including at least one upper case, one lower case, one number and a special character).
- Password must be changed at least once a year.
- After 3 failed log-in attempts, account is locked for 1 hour.
- Passphrase for password recovery in case password is lost.

> Refer to paragraph 11.1 for more information regarding the different profiles and their password protection.

6. INTRODUCTION

6.1. Range

 DIRIS Digiware D-50 **Multipoint display** Ref. 4829 0204	 **DIRIS Digiware D-70** **Multipoint display** Ref. 4829 0203
Ethernet output Modbus TCP BACnet IP SNMP v1, v2 & v3	Ethernet output Modbus TCP BACnet IP SNMP v1, v2 & v3
-	WEBVIEW-M embedded web server Power & Energy Monitoring

6.2. Introduction to DIRIS Digiware D

DIRIS Digiware D-50 and D-70 are system displays and act as the unique point of access to measurements from DIRIS Digiware modules.

They can also display measurements from other SOCOMEC meters and measuring devices: COUNTIS, DIRIS A, DIRIS B.
They centralise data from up to 32 devices (a maximum of 192 circuits).
These products may be connected by a Digiware bus and/or an RS485 bus.

Centralised products can be shown as well as configured by DIRIS Digiware D displays.

6.2.1. Introduction to DIRIS Digiware D-50

The DIRIS Digiware D-50 display is a master on the Digiware bus and acts as a gateway interface to communicate measurements over RS485 and Ethernet.

The RS485 port can be configured as a Master or Slave.

The Ethernet port is used to:

- Communicate via Modbus TCP (max. 32 simultaneous connections), measurements from meters and measuring devices connected to the Digiware and RS485 buses.
- Communicate via BACnet IP and SNMP, measurements from meters and measuring devices connected to the Digiware and RS485 buses.
- Automatically send alarm notifications via emails (SMTPS).
- Synchronize the date/time to an SNTP server.
- Automatically and cyclically export historical measurements via FTPS.

6.2.2. Introduction to DIRIS Digiware D-70

The DIRIS Digiware D-70 display embeds a web-based software (WEBVIEW-M) which allows a remote visualisation of real-time and historical measurements.

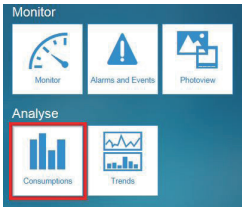
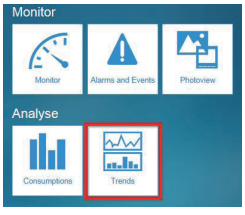
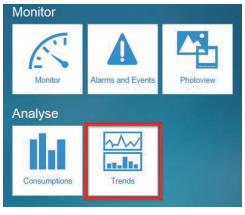
The DIRIS Digiware D-70 display is a master on the Digiware bus and acts as a gateway interface to communicate measurements over RS485 and Ethernet.

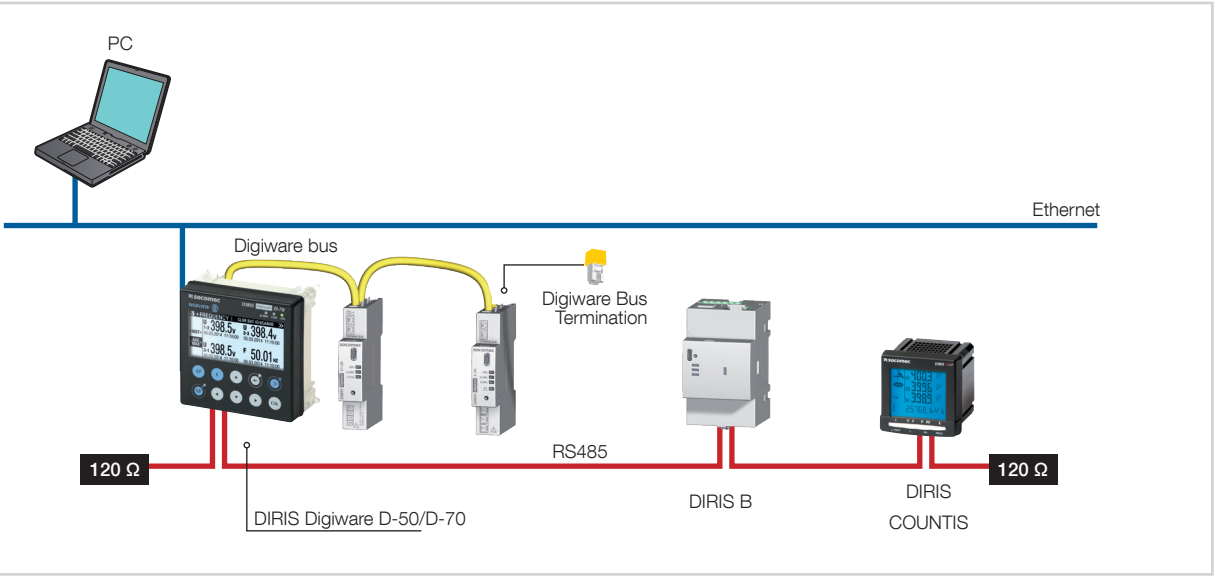
The RS485 port can be configured as a Master or Slave.

The Ethernet port is used to:

- Communicate via Modbus TCP (max. 32 simultaneous connections), measurements from meters and measuring devices connected to the Digiware and RS485 buses.
- Communicate via BACnet IP and SNMP, measurements from meters and measuring devices connected to the Digiware and RS485 buses.
- Automatically send alarm notifications via emails (SMTPS).
- Synchronize the date/time to an SNTP server.
- Automatically and cyclically export historical measurements via FTPS.

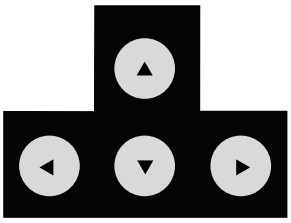
Data logging capabilities of the DIRIS Digiware D-70 are explained in the table below:

<table>
<tr><th></th><th>Consumption curves</th><th>Load curves</th><th>Trends</th></tr>
<tr><td>Logged data</td><td>Energy: kWh, kvarh, kVAh</td><td>Power: kW, kvar, kVA</td><td>Average measurements: U, V, I, P, Q, S, PF, Temperature...</td></tr>
<tr><td>Compatible products</td><td>COUNTIS Exx (all)
DIRIS Axx (all)
DIRIS Bxx (all)
DIRIS Digiware XXX (all)</td><td>Countis Eci, Countis E3x
DIRIS A-30 + MEM / A60
DIRIS B-30
DIRIS Digiware I-31 / I-61 /I-35 / I-45 / I-35dc / S-135 / S-Datacenter
DIRIS A-40</td><td>DIRIS B-30
DIRIS Digiware I-35 / I-45 / U-30 / U-31dc / U-32dc / S-135 / S-Datacenter
DIRIS A-40</td></tr>
<tr><td>Integration period</td><td>configurable from Easy Config System, 10 min to 60 min</td><td colspan="2">configurable from Easy Config System, 1 min to 60 min</td></tr>
<tr><td>Data logging duration</td><td colspan="3">1 year with a 60-min integration period.
Proportional for different values:
For example: 3 months with a 15-min integration period.
This applies no matter how many devices (1 to 32) are connected to the D-70. The level of detail of the log is not linked to the number of devices connected:</td></tr>
<tr><td>Operation</td><td>Readings taken every 10 min / 60 min in the meter/PMD.</td><td colspan="2">The data is recorded in a cache memory on the meter and then downloaded by the D-70. If communication is interrupted, the missing data is recovered by the D-70 once the connection is restored so that recording continues.</td></tr>
<tr><td>Data backup (in the event of a loss of communication between the D-70 and the meter)</td><td>NO</td><td colspan="2">YES (in the meter's cache memory)</td></tr>
<tr><td>Export to FTP server</td><td>YES</td><td>YES</td><td>YES</td></tr>
<tr><td>Webview link</td><td> 
</td><td> 
</td><td> 
</td></tr>
<tr><td>Specific configuration</td><td>Nothing to configure (data is recorded automatically).</td><td>Load curves must be activated on the meters (via Easy Config System). Load curves are then automatically downloaded from the meter's cache memory to the D-70.</td><td>Trends must be activated on the meters (via Easy Config System). The logs are then automatically downloaded from the meter's cache memory to the D-70.</td></tr>
</table>



6.3. Touchscreens

The display consists of a screen and 10 shortcut keys:

	Shortcut keys for load measurements: current, active power, reactive power, apparent power, power factor, cos phi
	Shortcut keys for electrical network measurements: line to neutral voltages, to line-line voltages, frequency
	Shortcut keys for active, reactive, apparent energy meters (total and partial readings)
	Arrow keys for navigation
	Use this to go back to a previous navigation menu
	Use this to go to the previous/next product (to scroll through all your meters and centralised measuring devices)
	Use this to confirm your navigation or entry selection

6.4. LED display

ALARM* (red)

- Off: no active alarm
- Stable: at least one alarm (measurement, logical, protection) is active on the display or a connected device
- Flashing: at least one system alarm is active on the display or a connected device

**Go to the EVENTS menu for details on active alarms*

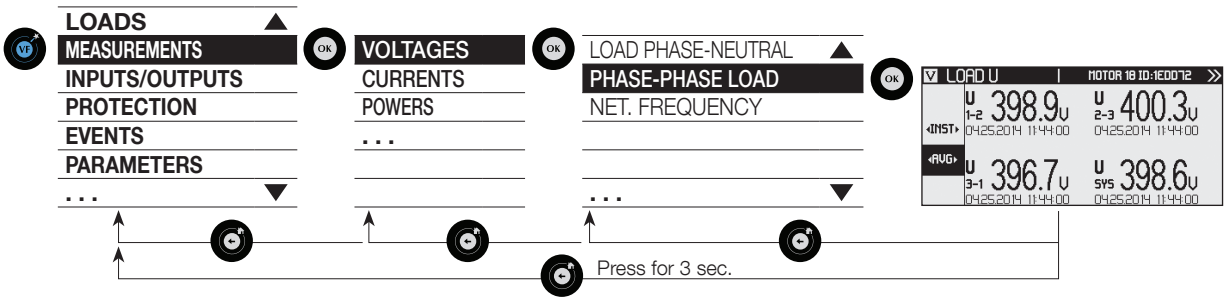
COM (orange)

- Off: display is not communicating with downstream devices
- Stable: address conflicts during auto-discovery process
- Flashing: communication in progress with a downstream device (RS485 or Digiware)

ON (green)

- Off: display is not powered
- Stable: device is powered

6.5. Navigation



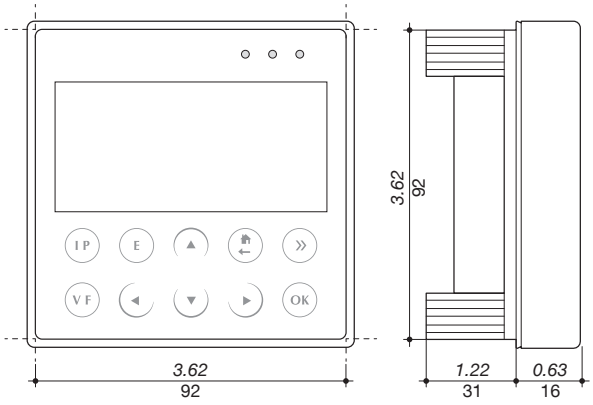
6.6. Menu structure

Loads		
Measures	Voltages	Load Line-Neutral
		Load Line-Line
		Net. Frequency
		Net. Line-Neutral
		Net. Line-Neutral Unbalance
		Net. Line-Neutral Harmonics
		Net. Line-Neutral Crest Factor
		Net. Line-Line
		Net. Line-Line Unbalance
		Net. Line-Line Harmonics
		Net. Line-Line Crest Factor
	Currents	Currents
		Current System
		Currents Unbalance
		Currents THD
		Currents K Factor
		Currents Harmonics
		Currents Crest Factor
	Powers	Active Powers
		Reactive Powers
		Apparent Powers
		Predicitve Powers
		Power Factors
		Cos Phi
		Tan Phi
	Energies	Positive Active Energies
		Negative Active Energies
		Positive Reactive Energies
		Negative Reactive Energies
		Positive/Negative Reactive Lead/Lag Energies
		Apparent Energies
		Hour Meters
	Pulse Meters	
	Reset All Min/Max Values	
Input/Output	Digital Input	
	Digital Ouput	
	Analogue Input	
Protection		
Events	In Progress	
	History	Alarms
		Quality
Parameters	Display Settings	Language
		Date / Time (synchronisation method, time zone, date format and separator)
		RS485 communication: Mode (master/slave), Baudrate, Stop, Parity, Address
		Ethernet communication: DHCP, IP Address, Mask, Gateway
		Change Password
	Autodetect Serial Devices	Status
		Found/Conflict
		Addressing range: Start address, End address, Conflict resolution (Autoset or Push button)
		Method: Fast or Full
	Add Device Manually	Type: RS485 / Digiware, D-xx/M-xx or Other Ethernet device
		IP Address
		Modbus Address
	Device Actions	Choose device from device list
		Soft Version
		Operating Hours
		Configure, Remove, Restore to factory settings or Reboot slave devices
Diagnosis	Ethernet	IP Address
		Host Name
	Serial Com	RS485 comm status
		Digiware comm status
		Devices comm OK
		Devices comm NOK
		Restart serial comm analysis
	Network Time	SNTP
		Current Date/Time
		Last activity
	Email	SMTP
		Last activity
	FTP Client	FTP
		Last activity
	Datalogger	Consumptions
		Trends
		Alarms
About	IP address	
	MAC address	
	Serial number	
	Software version	
	Reboot	

Note: the menus available depend on the slave device connected.

6.7. Dimensions

Dimensions *in*/mm



Dimensions *in*/mm

Door cut-out must be 92x92mm.

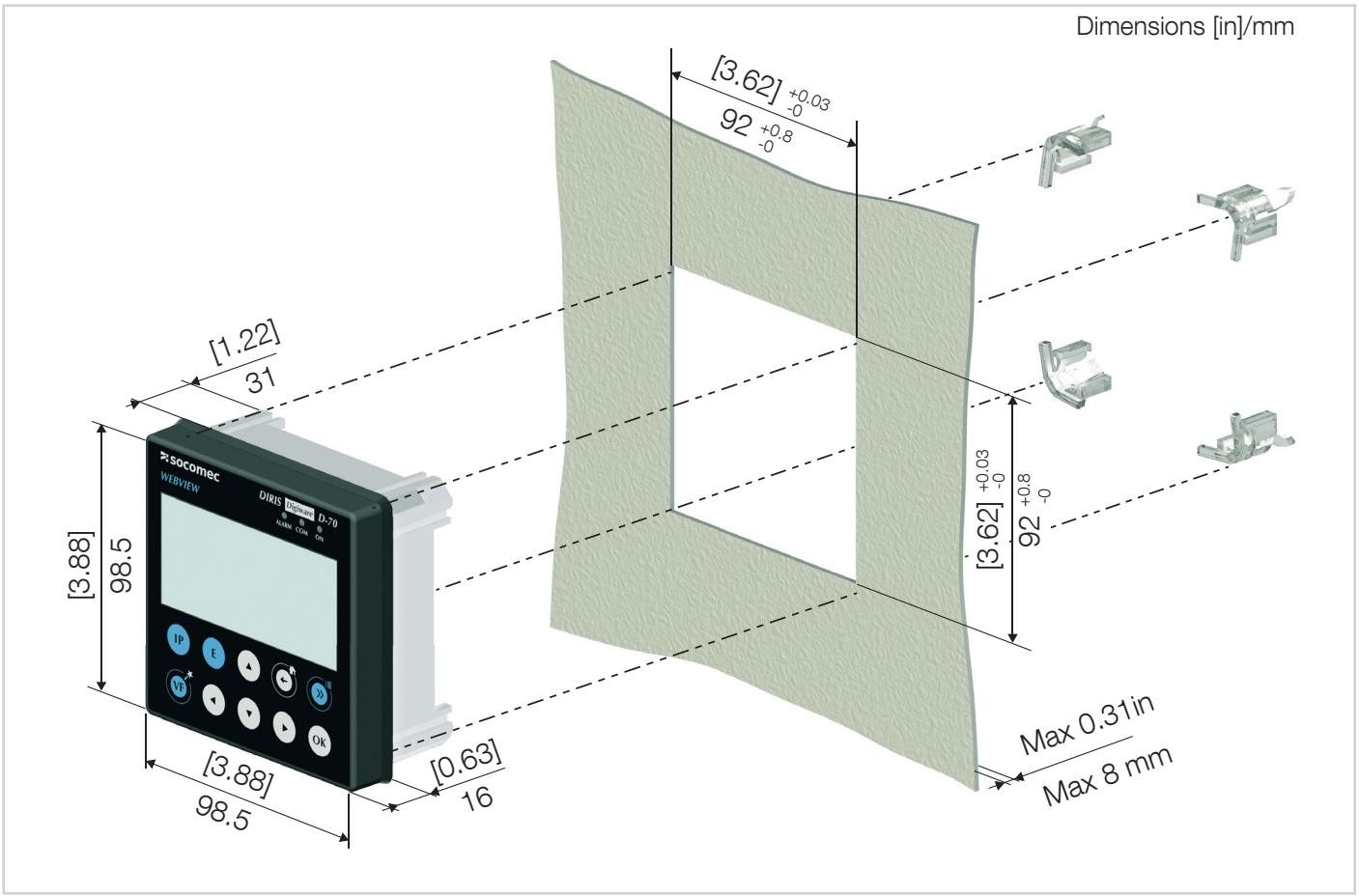
7. MOUNTING

7.1. Recommendations and safety

Refer to the safety instructions (section "2. Hazards and warnings", page 5)

7.2. Door mounting

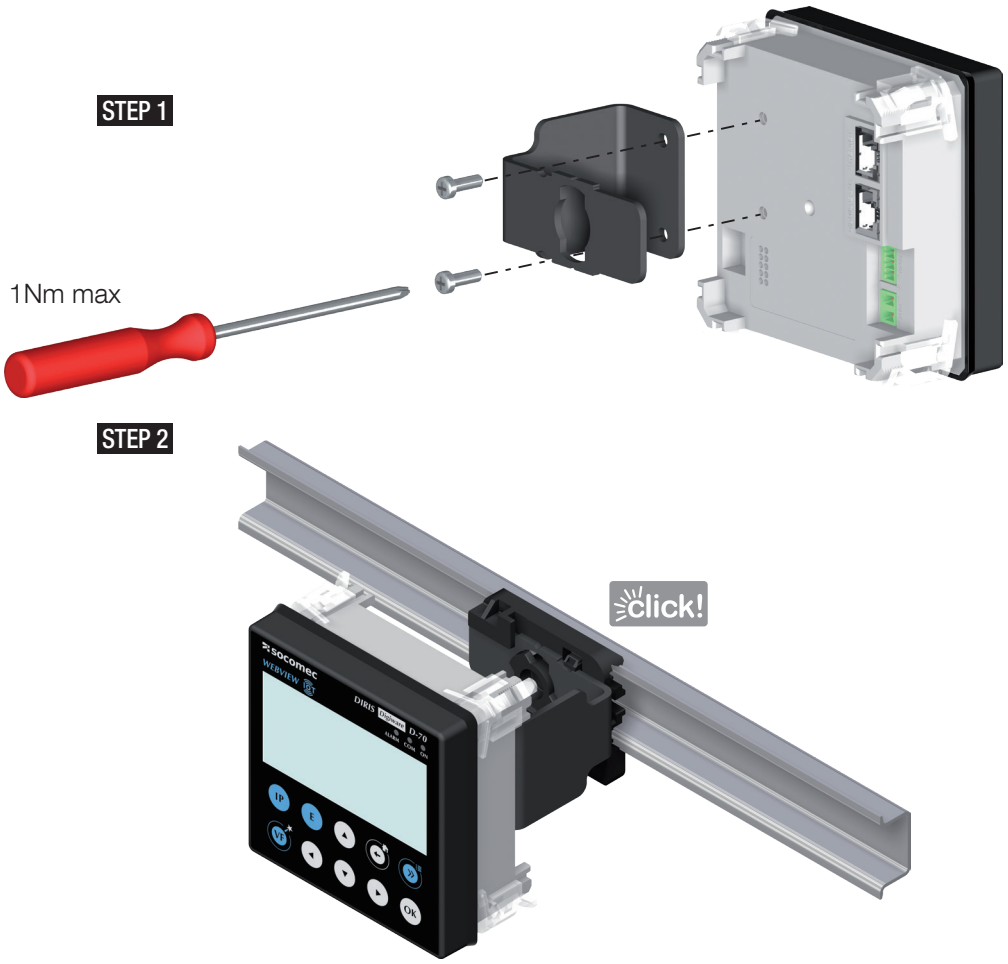
DIRIS Digiware D-50 and D-70 are panel-mounted (cut-out: 92x92mm). The display is secured with clips.



7.3. DIN rail mounting

DIRIS Digiware D-50 and D-70 can also be mounted on a DIN rail using a dedicated accessory (4829 0230) sold separately.

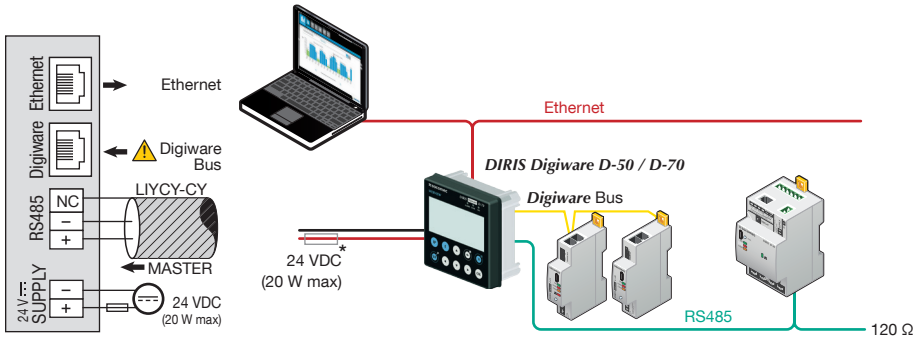
DIN rail mouting kit (separate part number: 4829 0230)



8. COMMUNICATION ARCHITECTURES

The DIRIS Digiware D-50 and D-70 display can be configured as a Slave or a Master for the RS485 bus.

8.1. RS485 Master

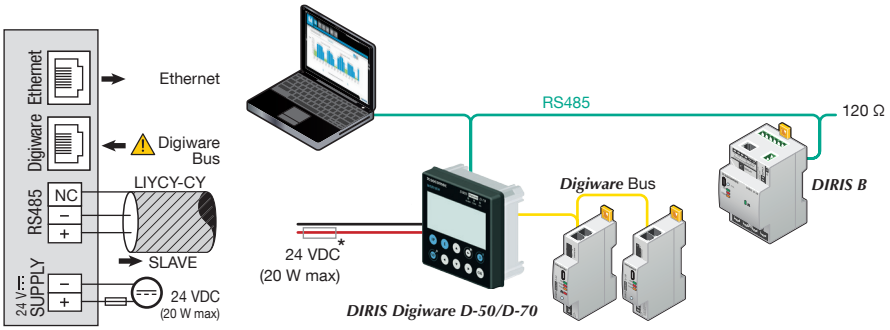


(*) The use of a 1A / 24 VDC fuse protection is recommended if the 24 VDC power supply is not provided by Socomec. For North America, the use of recognized fuses is mandatory.

All inputs/outputs are considered as SELV (Safety Extra-Low Voltage).

When configured as RS485 Master, the D-50/D-70 acts as a gateway (Digiware to Ethernet and RS485 to Ethernet).

8.2. RS485 Slave



(*) The use of a 1A / 24 VDC fuse protection is recommended if the 24 VDC power supply is not provided by Socomec. For North America, the use of recognized fuses is mandatory.

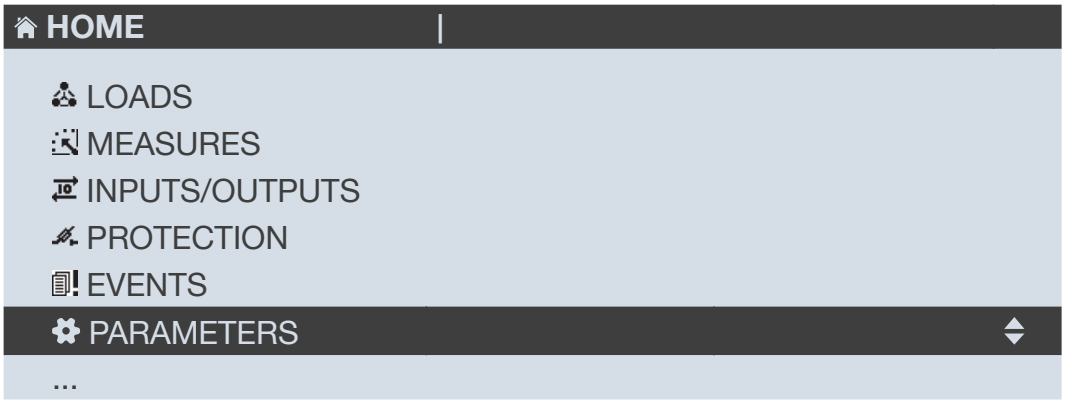
All inputs/outputs are considered as SELV (Safety Extra-Low Voltage).

When configured as RS485 Slave, the D-50/D-70 communicates measurements from DIRIS Digiware modules over RS485.

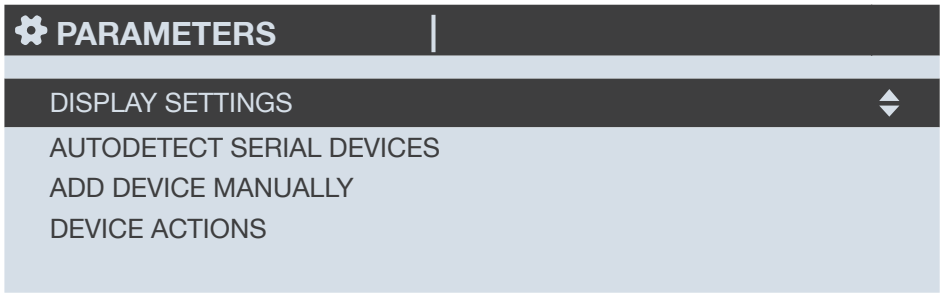
9. CONFIGURATION

From the Socomec start-up sreen, press “OK” to enter the navigation menu:

Select the "PARAMETERS" menu by using the navigation key "DOWN ARROW" 3x and confirm with "OK”:

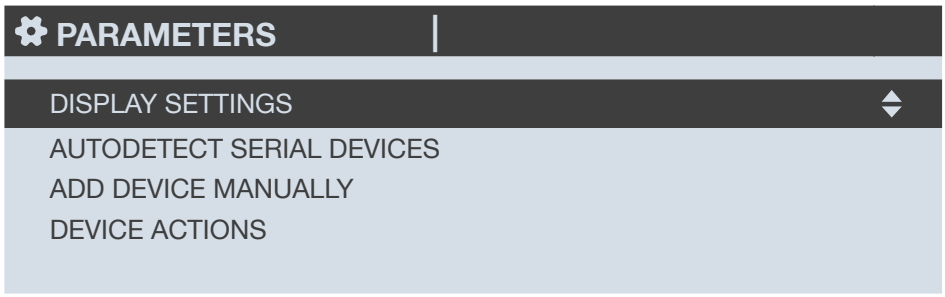


Do not power off the display before saving the configuration or changes will be lost

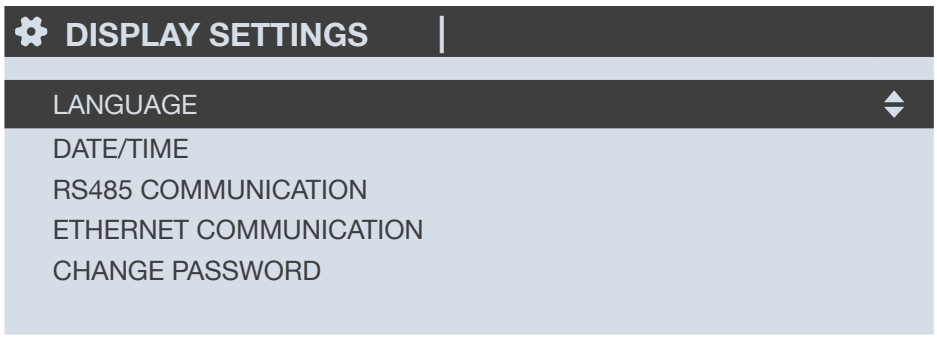


- DISPLAY SETTINGS: to access settings that are specific to the display.
- AUTODETECT SERIAL DEVICES: to launch an automatic detection and addressing of meters and power monitoring devices connected to the D-50/D-70 display.
- ADD DEVICE MANUALLY: to add a new power monitoring device to the topology of the D-50/D-70 display. The device can be connected to the D-50/D-70 via Digiware, RS485 or Ethernet.
- DEVICE ACTIONS: to access the list of devices in the topology and perform associated actions (configuring, removing, rebooting, restoring factory settings, etc.)

9.1. Display settings



Click on "DISPLAY SETTINGS". Default Password is 0100.



- LANGUAGE: to set the display's navigation language (english by default)
- DATE / TIME: to change Date/Time settings (synchronisation method, format etc.)
- RS485 COMMUNICATION: to configure the RS485 communication settings
- ETHERNET COMMUNICATION: to configure the IP configuration of the D-50/D-70
- CHANGE PASSWORD: to change the password to access the settings menu (default: "0100")

9.1.1. Language

You can change the display's navigation language here.
Choose from: English, French, German, Italian, Spanish, Flemish, Polish, Turkish, Russian, Slovenian and Chinese.

Select your language with the arrow pad and confirm with "OK".

PARAMETERS	
ENGLISH	
FRANCAIS	
DEUTSCH	
ITALIANO	
POLSKI	
…	

9.1.2. Date / time

You can configure the date and time on the DIRIS Digiware D-50/D-70 display:

- Manually by entering the year, month, day, hour, minute, second
- Automatically (like a computer) by SNTP server

If the DIRIS Digiware D-50/D-70 is synchronised by SNTP, it will broadcast and synchronise the date and time of all downstream devices.

You can also choose the display's date format, including the separator between the day, month and year.

DATE/TIME	
METHOD	◀ MANUAL ▶
DATE	12.20.21
TIME	10:56
TIME ZONE	GMT +0:00
DATE FORMAT	MM/DD/YYYY
DATE SEPARATOR	.

To configure the SNTP server, you will need to enter the following fields:

- SNTP server IP address
- SNTP server port

DATE/TIME	
METHOD	◀ SNTP ▶
SERVER IP ADDRESS	000.000.000.000
SERVER PORT	00123
TIME ZONE	GMT +0:00
DATE FORMAT	MM/DD/YYYY
DATE SEPARATOR	.

9.1.3. RS485 communication

Configure the display's Modbus address.

Configure the baudrate, stop bits, parity of the RS485 and Digiware bus.

By default, DIRIS Digiware D-50 / D-70 are master devices on Digiware and RS485 buses (baudrate, parity, stop bits). RS485 mode can be changed to Slave.

RS485 COMMUNICATION	
MODE	◀ MASTER ▶
BAUDRATE	38400
STOP	1BIT
PARITY	NONE
ADDRESS	001
APPLY SETTINGS	

9.1.4. Ethernet communication

You can configure the Ethernet settings of DIRIS Digiware D-50 / D-70 displays:

- DHCP (IP address dynamically assigned by the Ethernet network) ENABLED/DISABLED
- IP address
- Subnet mask
- LAN gateway

ETHERNET	
DHCP	◀ ENABLED ▶
IP ADDRESS	010.067.096.167
MASK	255.255.248.000
GATEWAY	010.067.103.254

9.2. Automatic detection of slave devices

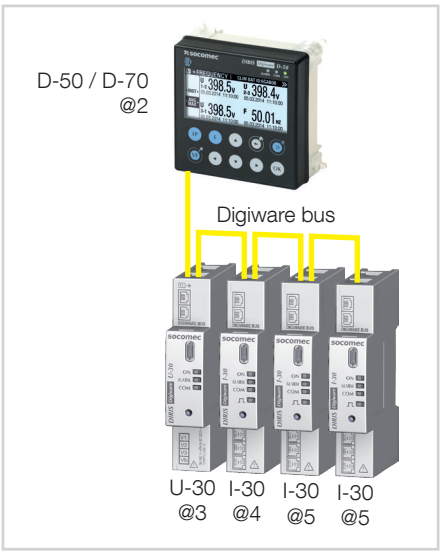
The auto-discovery function scans and discovers slave devices connected to the Digiware and RS485 buses and automatically assigns a unique Modbus address to each device.

The auto-discovery function is compatible with DIRIS Digiware modules, DIRIS B and DIRIS A-40 power meters.

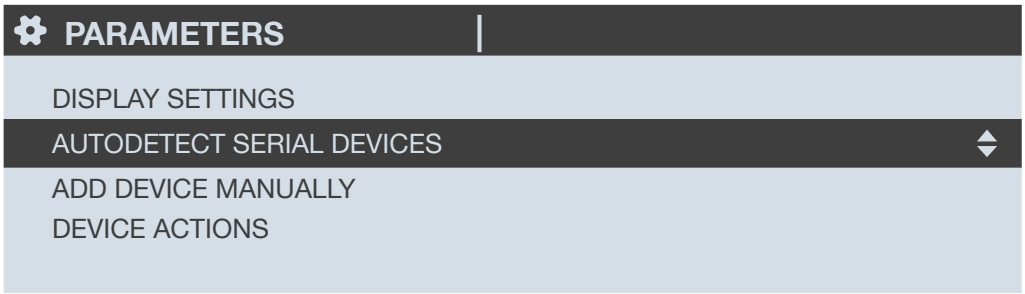
For other devices such as COUNTIS energy meters and DIRIS A-10/A-20/A-30/A-60 power meters, you must change their Modbus address manually.

Example of auto-discovery on a D-50/D-70 display.

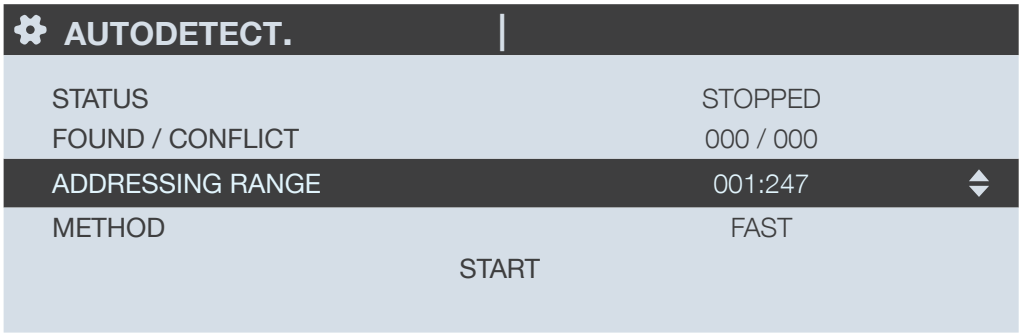
Four slave devices are connected to the D-50 / D-70. Two are addressed correctly, the other two have the same Modbus Address.



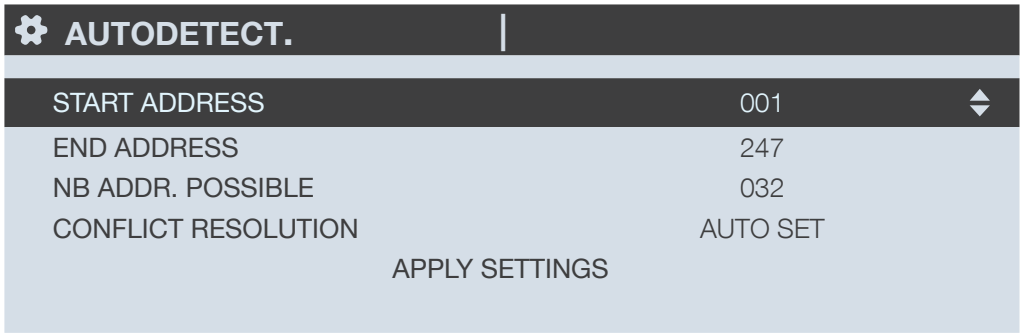
Go to “PARAMETERS” / “AUTODETECT SERIAL DEVICES” (password is 0100) :



Click on “DIGIWARE ADDRESSING RANGE”:



This allows you to allocate Modbus addresses to the connected devices within a specific range:



Choose the conflict resolution method:

- "PUSH BUTTON": you must press the push button on each module to resolve address conflicts. The order you will use to press the push buttons on the modules will also determine the order for the Modbus addressing of those modules.
- "AUTO SET": connected devices are automatically allocated individual Modbus addresses within the specified range.

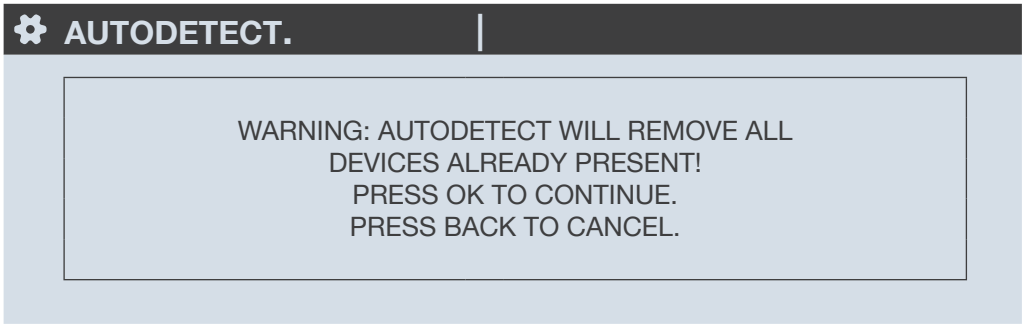
Click on "APPLY SETTINGS" to apply your modifications.

Choose the auto-discovery "METHOD":

- FAST (default mode): this mode will only detect DIRIS Digiware modules on the Digiware bus and RS485 bus, DIRIS B and DIRIS A-40 on the RS485 bus.
- FULL: this mode will also detect other Socomec PMDs (DIRIS A) and meters (COUNTIS E) connected on the RS485 bus.

Click on "START" then "OK" to start the auto-discovery process (this can take up to 5 minutes).

Please be aware that this removes all previously found devices (if they are still there they will be found again).



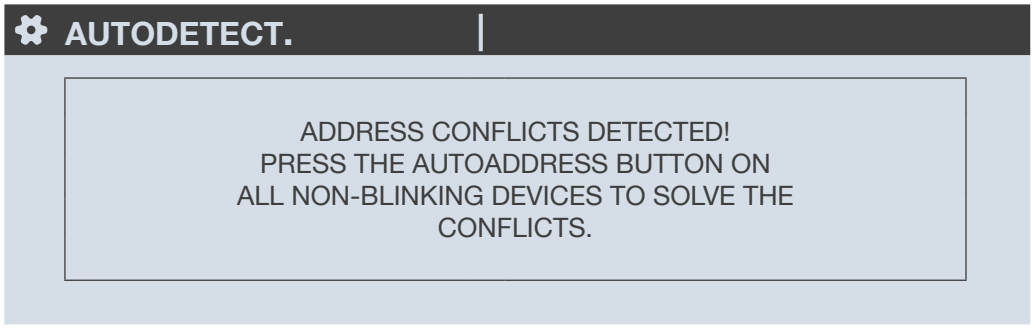
After pressing "OK", the steps below will automatically follow:

- ADDRESS DETECTION

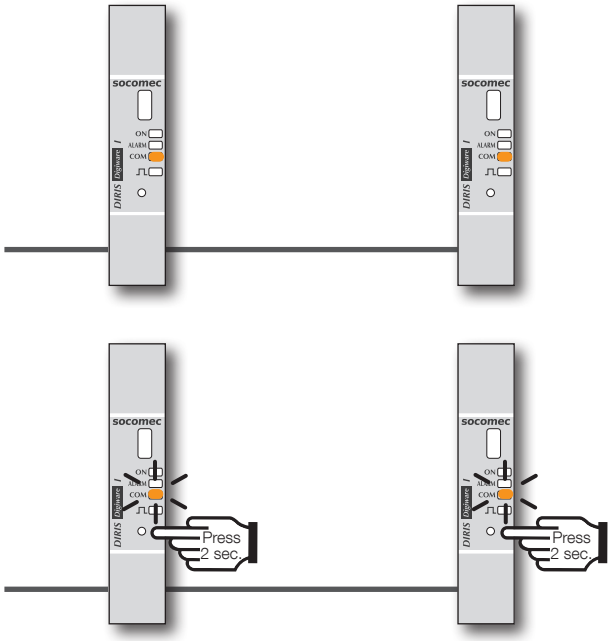
- ADDRESS SCANNING

If you have chosen an automatic address conflict resolution ("AUTOSET"), the STATUS automatically goes to "STOPPED" once the auto-discovery process is finished.

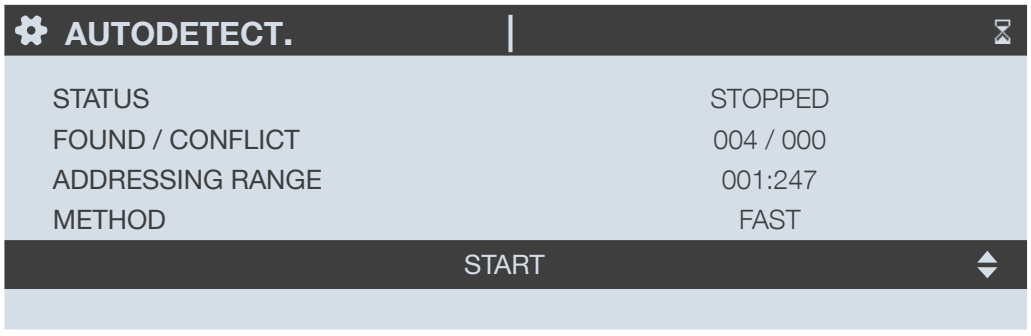
If you have chosen a manual address conflict resolution ("PUSH BUTTON"), there will be one or several conflicts if multiple devices have the same Modbus address.
A pop-up message will be displayed on the HMI:



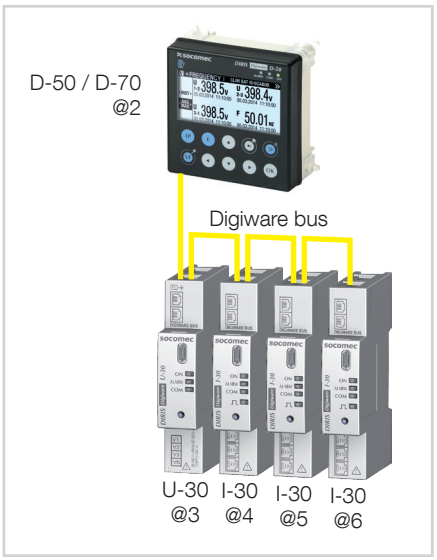
To manually resolve address conflicts, locate the devices which have a lit and stable "COM" LED. Press and hold down the addr. button on the front face of the module for 2 seconds until the COM LED flashes:



COM LED ON AND STABLE = address conflict
COM LED FLASHING = product address identified correctly.



The number of detected devices increases and the number of conflicts decreases to reach zero once all products have a unique address.



You can then check the list of detected products along with their Modbus addresses in the “PRODUCT LIST” menu, available from the Home screen.

Example:

LIST PROD.	LOAD1
U-30@3 ID:546434	@003
I-30@4 ID:F0C1D2	@004
I-30@5 ID:F0C1D3	@005
I-30@6 ID:F0C1D4	@006

You can find the IDs on the marking on the products (546434 on the U-30 and F0C1D2 on one of the I-30s) as shown in the picture below:

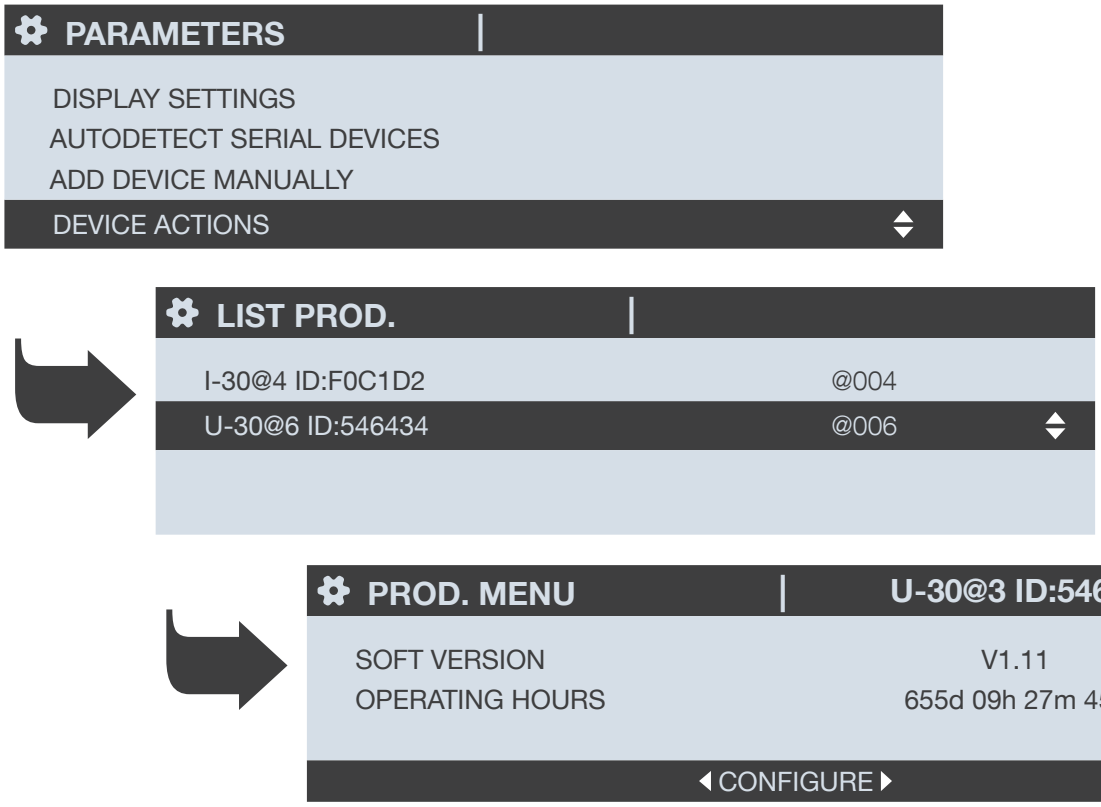
You can now perform the configuration of the system. Each product must be configured individually.

9.3. Configuring the DIRIS Digiware system from the D-50/D-70 display

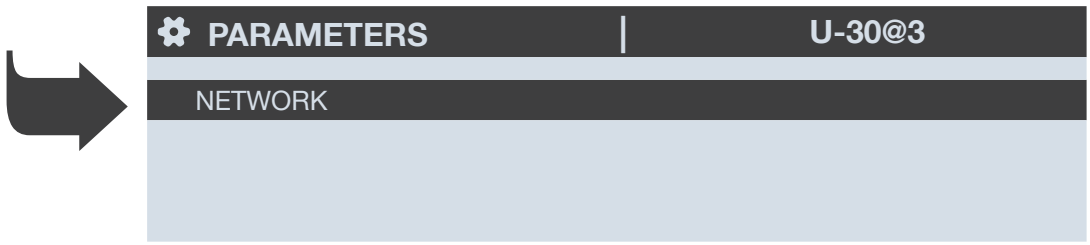
There are 2 steps to configure the DIRIS Digiware system:

- **Network:** setting the type of voltage network: single-phase (1P+N), two-phase (2P), three-phase without neutral (3P), three-phase with neutral (3P+N).
- **Load:** configuring the loads/circuits measured. You can, for example, measure three-phase and single-phase loads connected to a three-phase electrical network.

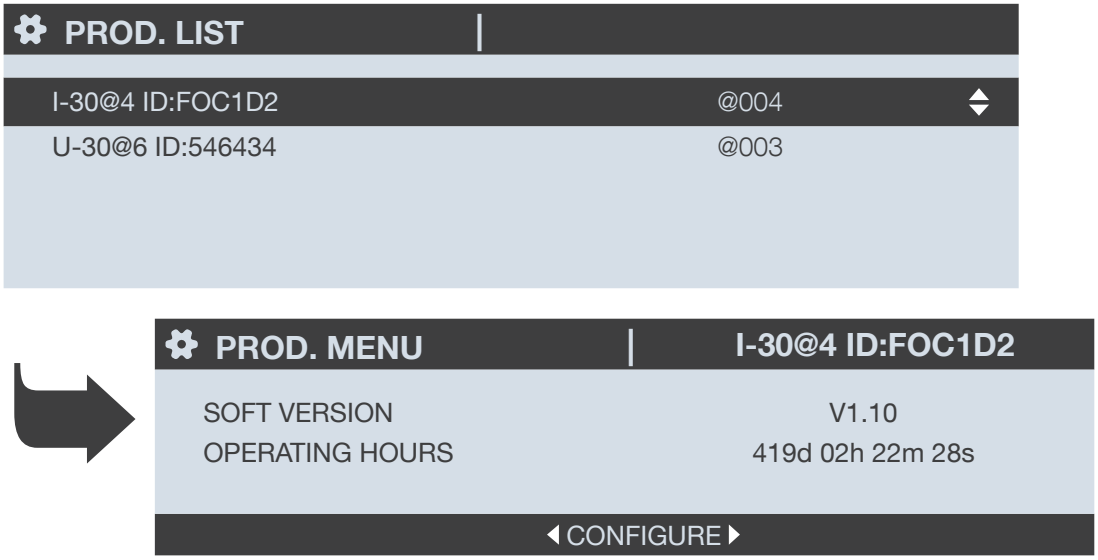
Electrical network settings are configured from the DIRIS Digiware U-xx module.
Go to "PARAMETERS" > "DEVICE ACTIONS", then select the DIRIS Digiware U-xx module:



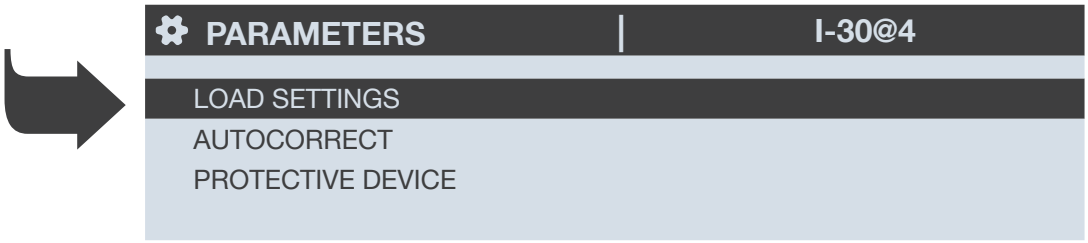
Select "CONFIGURE" and press "OK":



Loads are configured from DIRIS Digiware I-xx modules



Select "CONFIGURE" and press "OK":



With DIRIS B power monitoring devices, network and loads settings are accessible from the DIRIS B altogether.

9.3.1. Network configuration

You can configure the various network voltage parameters:

- Network type: single-phase (1P+N), two-phase (2P), three-phase without neutral (3P), three-phase+neutral (3P+N)
- Nominal voltage:
  This is the phase-phase voltage (usually 400 V) for three-phase networks
  This is the phase-neutral voltage (usually 230 V) for single-phase networks
- Nominal frequency: 50 or 60 Hz depending on the country
- Phase rotation: V1-V2-V3 (Direct) or V1-V3-V2 (reverse).

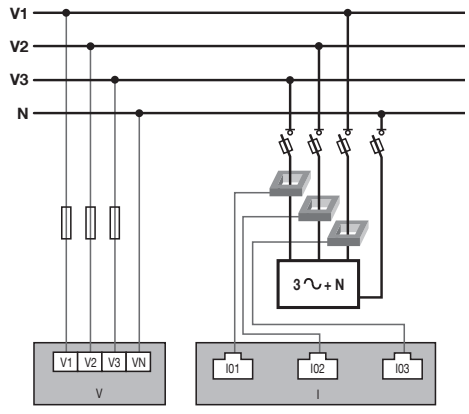
NET. SETTINGS	U-30@3 ID:546434
NETWORK TYPE	3P + N
NOMINAL VOLTAGE (V)	00400
NOMINAL FREQUENCY	50 Hz
PHASE ROTATION	V1-V2-V3
PRESS OK TO ENTER SETTINGS	

9.3.2. Load configuration

Multiple loads (single-phase, two-phase or three-phase) can be measured on a DIRIS B or DIRIS Digiware I module.

9.3.2.1. Example of a load configuration

This example shows a DIRIS Digiware I-30 module measuring a three-phase + neutral load using 3 current sensors.



LOAD	I-30@4 ID:FOC1D2			
INPUT	I01	I02	I03	
CT	250 A	250 A	250 A	
WAY	+/DIRECT	+/DIRECT	+/DIRECT	
V LINE	V3	V2	V1	
LOAD	L1	L1	L1	
TYPE	3P+N_3CT	3P+N_3CT	3P+N_3CT	
PRESS OK TO ENTER SETTINGS				

The current sensor connected to the current 1 input measures the current of phase 3 (V3).
The current sensor connected to the current 2 input measures the current of phase 2 (V2).
The current sensor connected to the current 3 input measures the current of phase 1 (V1).

LOAD	I-30@4 ID:FOC1D2			
INPUT	I01	I02	I03	
CT	250 A	250 A	250 A	
WAY	+/DIRECT	+/DIRECT	+/DIRECT	
V LINE	V3	V2	V1	
LOAD	L1	L1	L1	
TYPE	3P+N_3CT	3P+N_3CT	3P+N_3CT	
PRESS OK TO ENTER SETTINGS				

The 3 current inputs I01, I02, I03 are assigned to the same three-phase load no. 1 (L1).

LOAD	I-30@4 ID:FOC1D2			
INPUT	I01	I02	I03	
CT	250 A	250 A	250 A	
WAY	+/DIRECT	+/DIRECT	+/DIRECT	
V LINE	V3	V2	V1	
LOAD	L1	L1	L1	
TYPE	3P+N_3CT	3P+N_3CT	3P+N_3CT	
PRESS OK TO ENTER SETTINGS				

The “CT” field indicates the current rating of the sensor connected and the “WAY” field indicates if it was mounted in the correct orientation (+/DIRECT = P1 --> P2) or backwards (-/INV = P2 --> P1).

LOAD	I-30@4 ID:FOC1D2			
INPUT	I01	I02	I03	
CT	250 A	250 A	250 A	
WAY	+/DIRECT	+/DIRECT	+/DIRECT	
V LINE	V3	V2	V1	
LOAD	L1	L1	L1	
TYPE	3P+N_3CT	3P+N_3CT	3P+N_3CT	
PRESS OK TO ENTER SETTINGS				

9.3.2.2. Changing the load settings

Following the example above, press "OK" to change the settings and select "MANUAL CONFIG OF LOADS".

LOAD	I-30@4 ID:FOC1D2			
INPUT	**I01**	**I02**	**I03**	
CT	250 A	250 A	250 A	
WAY	+/DIRECT	+/DIRECT	+/DIRECT	
V LINE	V3	V2	V1	
LOAD	L1	L1	L1	
TYPE	3P+N_3CT	3P+N_3CT	3P+N_3CT	
PRESS OK TO ENTER SETTINGS				

You can change each parameter to configure each of the loads (the values in bold are shown on the screen in the example below)

- LOAD -> configure load 1: **L1** - load 2: L2 - load 3: L3
- NAME -> name of the load: **LOAD 1** (edit with max. 16 characters)
- TYPE -> type of load: single-phase (1P+N), two-phase (2P), three-phase (3P), **three-phase+neutral (3P+N)**
- NOMINAL I (A) -> set the nominal current of the load: **20A** (caution: the nominal current of the load may differ from the rating of the current sensor (CT1) used: a 63A current sensor can be used to monitor a 20A circuit breaker.
- CT SETTINGS -> to perform the configuration of current sensors.

LOAD	I-30@4 ID:FOC1D2
LOAD	◀ L1 ▶
NAME	LOAD 1
TYPE	3P+N_3CT
NOMINAL I (A)	00020
CT SETTINGS	I1
SEND SETTINGS	

Go to "CT SETTINGS" and select inputs I01 - I03 to perform the configuration of current sensors:

CT SETTINGS	I-30@4 ID:FOC1D2
CURRENT INPUT	◀ I01 ▶
WAY	-/INV
V LINE	V1
CT	0250
DETECT	
OK	

Configure:

- CURRENT INPUT -> choose the current input associated to this current sensor (here I01).
- WAY -> Direction of the current sensor +/DIRECT, -/INV.
- V LINE -> V1, V2, V3 (position of the current sensor on phase 1, phase 2 or phase 3).
- CT -> Indicates the rating of the current sensor used. Click on “DETECT” to automatically detect the rating. After 2 seconds, the rating is displayed.

Complete the process by selecting "OK".

If a load is configured as three-phase or three-phase+neutral, for example, you would have to configure multiple current sensors (e.g. 3 current sensors for one three-phase load):

LOAD	I-30@4 ID:FOC1D2
LOAD	L1
NAME	LOAD 1
TYPE	3P+N_3CT
NOMINAL I (A)	00020
CT SETTINGS	◀ I2 ▶
SEND SETTINGS	

When you have finished configuring the entire load (L1) (type of load, name, nominal current, current sensors), scroll right from the “LOAD” line to configure loads 2 and 3 (L2, L3):

LOAD	I-30@4 ID:FOC1D2
LOAD	◀ L1 ▶
NAME	LOAD 1
TYPE	3P+N_3CT
NOMINAL I (A)	00020
CT SETTINGS	I1
SEND SETTINGS	

For example, a DIRIS Digiware I-30 with 3 current inputs is best for measuring:

- 1 three-phase load (1 three-phase load L1 using the current inputs I01, I02, I03)
- 3 single-phase loads (1 single-phase load L1 with a current sensor connected to the I01 current input, 1 single-phase load L2 with a current sensor connected to the I02 current input, and 1 single-phase load L3 with a current sensor connected to the I03 current input).

Numerous other load combinations are possible.

When all the loads are configured (maximum 3 on one DIRIS Digiware I-30), apply your settings by selecting "SEND SETTINGS" and press "OK".

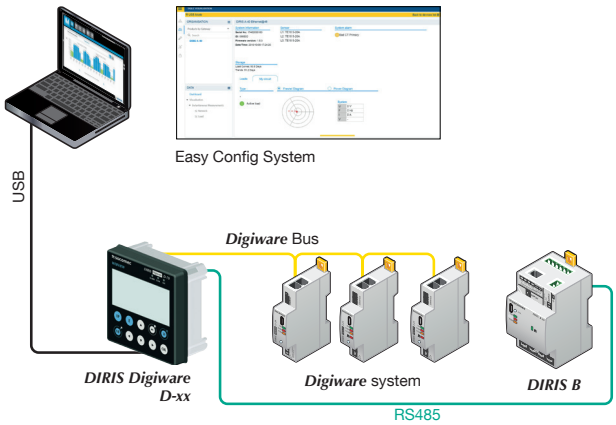
LOAD	I-30@4 ID:FOC1D2
LOAD	L1
NAME	LOAD 1
TYPE	3P+N_3CT
NOMINAL I (A)	00020
CT SETTINGS	I1
SEND SETTINGS	

10. CONFIGURATION VIA EASY CONFIG SYSTEM

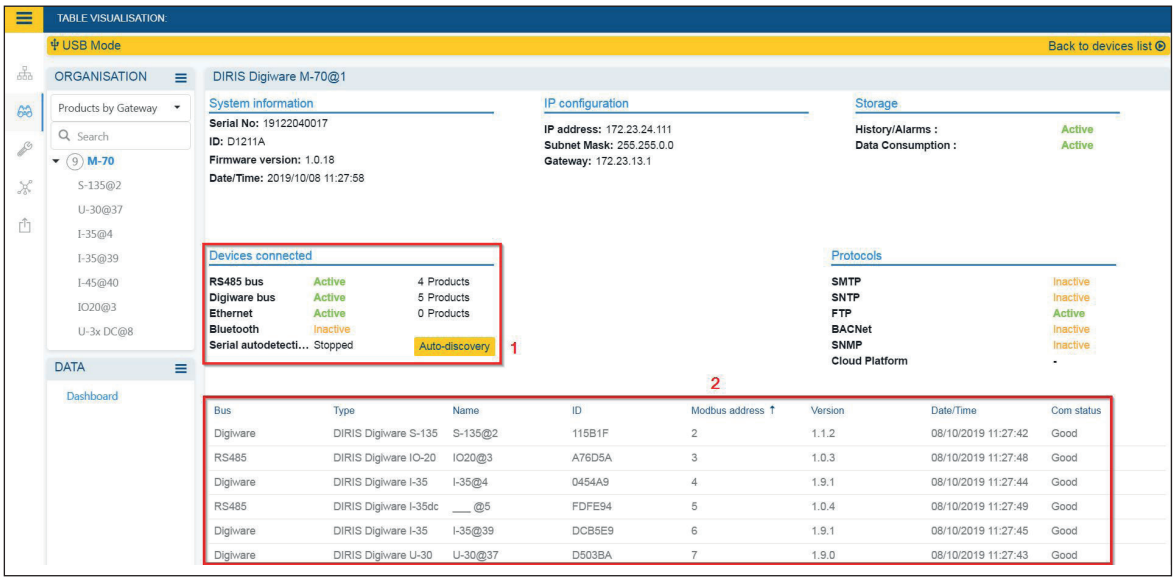
The Easy Config System software can be downloaded from the Socomec website at the following link:
www.socomec.com/easy-config-system_en.html

The Configuration of the DIRIS Digiware D-50/D-70 display and downstream Socomec devices can be done from the Easy Config System software, by connecting a computer to the D-50/D-70 display either via USB or via Ethernet.

10.1. USB connection mode

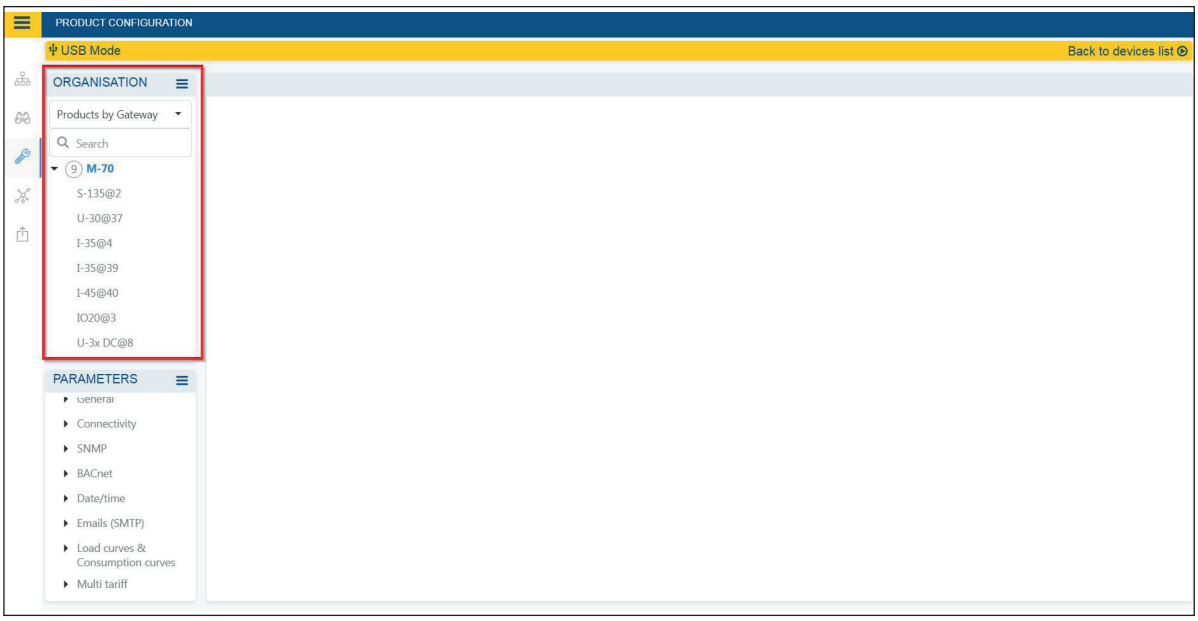


- Open Easy Config System.
- Connect a USB cable between the DIRIS Digiware D-50/D-70 display and a computer.
- Log in as User or Admin. Admin default password is “Admin”.
- Click on “New Configuration”, enter a name and icon.
- Click on the newly created configuration.
- Click on “USB mode” on the right top corner to connect to the D-50/D-70 display and access configuration menus.
- Click on the “Binocular” icon on the left side bar.
- Under the “Organisation” part, select the D-70/D-50 display.
- Click on “Dashboard” to visualise general information about the display.
- Click on “Auto-discovery” (1):

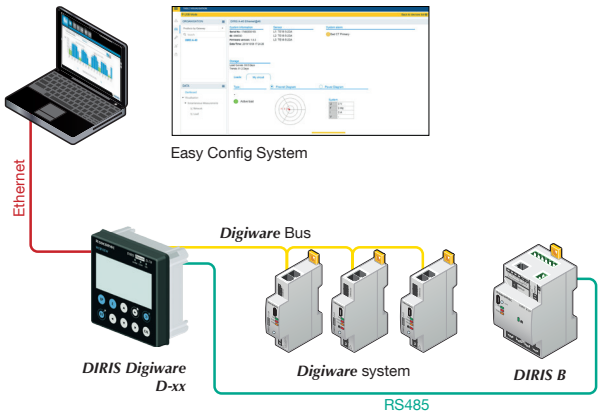


- Once the slave auto-discovery process is finished, slave devices will be displayed in the lower part of the dashboard (2). The number of devices accessible downstream the D-50/D-70 display is also displayed in the “Organisation” part, next to the D-50/D-70 display.

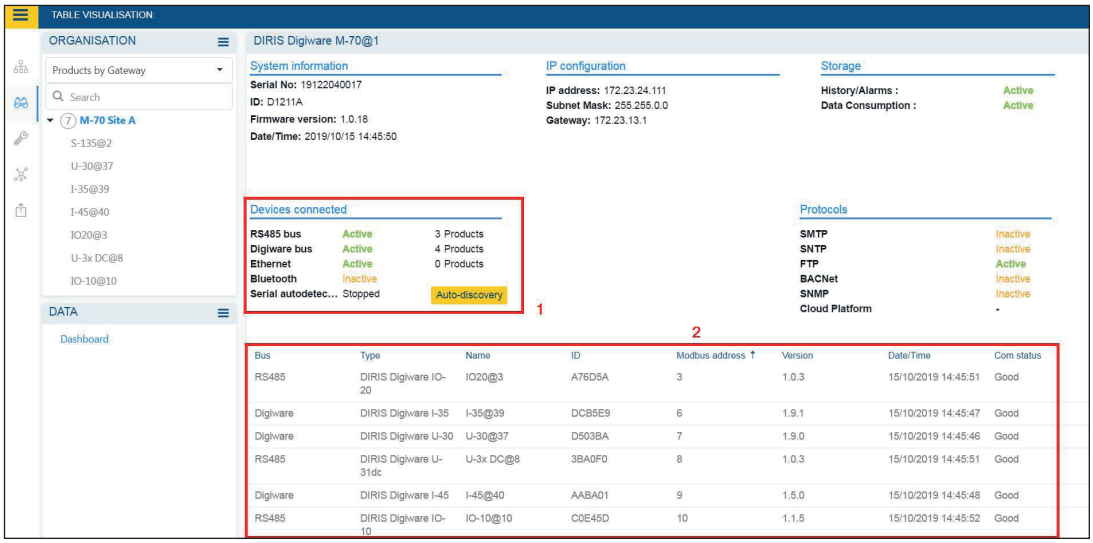
- Configuration of slave devices can be done directly without unplugging the USB cable, by clicking on the Wrench icon on the left side bar:



10.2. Ethernet connection mode



- Open Easy Config System.
- Log in as User or Admin. Admin default password is “Admin”.
- Click on “New configuration”, enter a name and icon.
- Click on the newly created configuration.
- Click on the “+” icon to manually add the D-50/D-70 display to the topology, by selecting the product, entering the IP address, Modbus address. To be able to communicate with the D-50/D-70 display, your computer must be in the same network as the D-50/D-70
- Click on the “Binocular” icon on the left side bar.
- In the “Organisation” part, select the D-70/D-50 display.
- In the “Data” part, click on “Dashboard” to visualise general information about the display.
- Click on “Auto-discovery” (1).



- Once the slave auto-discovery process is finished, slave devices will be displayed in the lower part of the dashboard menu (2). The number of devices accessible downstream the D-50/D-70 display is also displayed in the “Organisation” part, next to the D-50/D-70 display.
- Configuration of slave devices can be done directly by clicking on the Wrench icon on the left side bar and selecting the right device:

11. WEBSERVER EMBEDDED IN THE D-50/D-70 DISPLAYS

A webserver is embedded for the configuration of network parameters (WEB-CONFIG, D-50/D-70) and the remote visualisation of measurement data (WEBVIEW-M, D-70 only).

To connect to the D-50/D-70 display's webserver, enter its IP address in the address bar of your web browser.

Default Ethernet parameters of the DIRIS Digiware D-50/D-70 displays are as follows:

- IP address: 192.168.0.4
- Mask: 255.255.255.0
- Gateway: 192.168.0.1

11.1. User profiles

Several profiles are available:

- User (default)
- Advanced User
- Totem User
- Admin
- Cyber security

The Advanced User, Administrator and Cyber security profiles are authorised to modify settings.

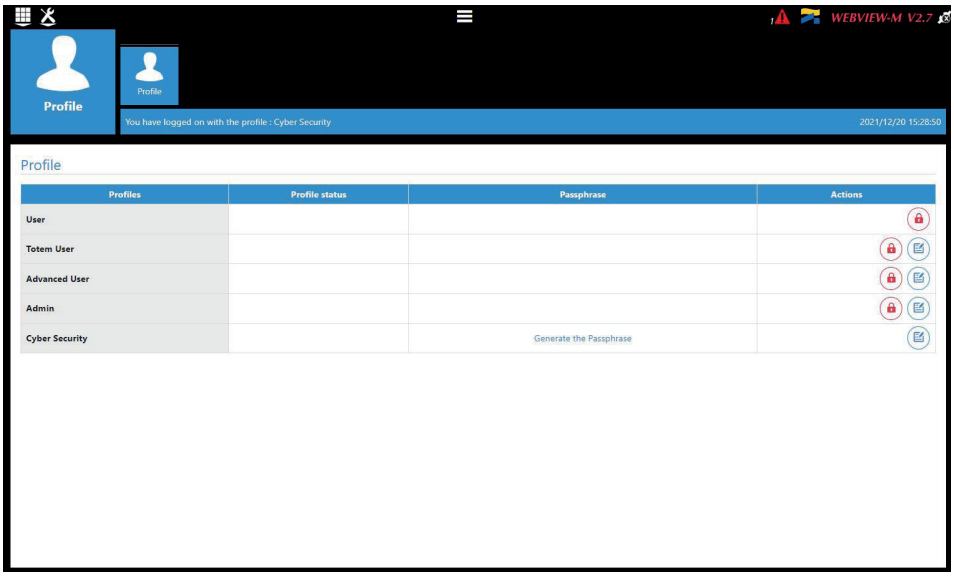
Profile	Access	Default password
User	- Visualisation of measurement data - Access to diagnostics	None
Advanced User	- Visualisation of measurement data - Access to diagnostics + Password management of the Advanced User profile + Reset of counters	Advanced
Totem User	- Visualisation of measurement data - Access to diagnostics + Password management of the Totem User profile + Reset of counters + No disconnection	Totem
Admin	- Visualisation of measurement data - Access to diagnostics + Password management of the Admin profile + Access to configuration menu	Admin
Cyber security	- Visualisation of measurement data - Access to diagnostics - Password management of all profiles - Access to configuration menu + Cyber Security configuration menu + Firmware upgrade via web server	Cyber

When connecting to the Admin, Advanced User or Cyber security profiles for the first time, it is mandatory to change default passwords. If these passwords are not changed, the "Password alert" alarm will remain active.

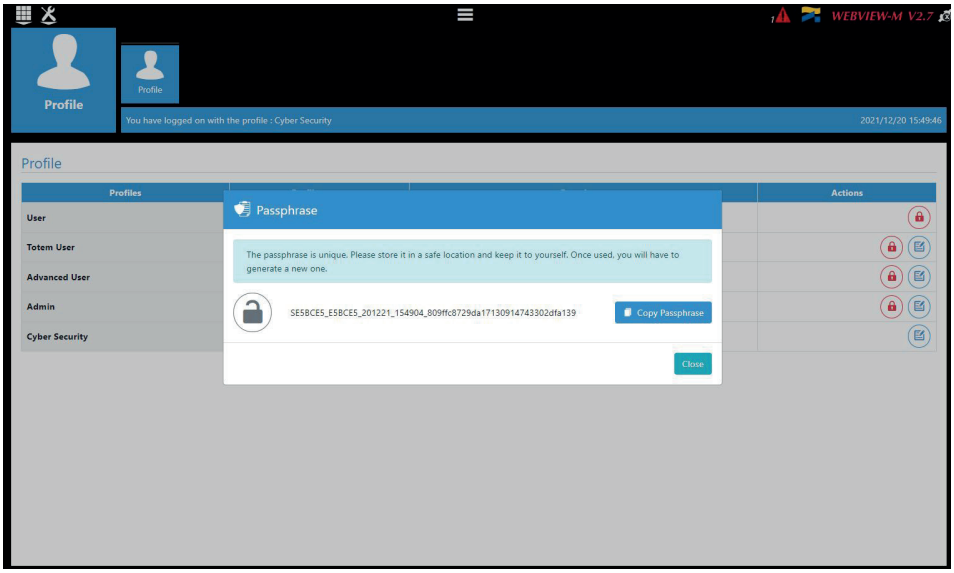
Totem User profile is locked by default. If the use of the Totem User profile is needed, you must connect with the Cyber Security profile, go to the "Profile" menu and unlock the Totem User profile.

It is highly recommended to change all default passwords right away, especially the password of the Cyber security profile which has the highest privileges including changing passwords for other accounts.

Once passwords have been changed, connect to the Cyber security profile, go to the “Profile” menu and click on “Generate the passphrase”:



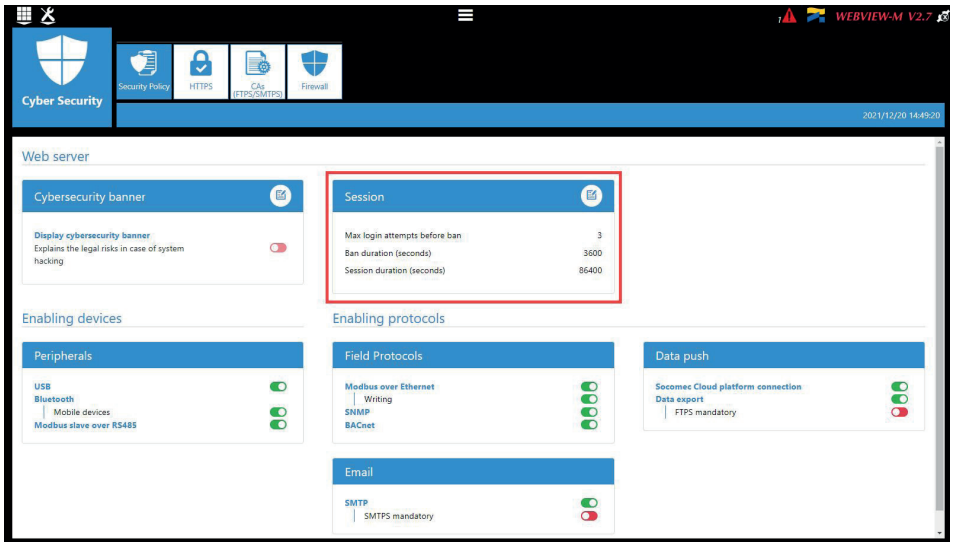
Copy the passphrase using the “Copy passphrase” button on the right side of the key, paste it somewhere and keep it safe. This will allow you to recover your password for the Cyber security account, should you lose it.



If you have forgotten to save the passphrase, the only option left is to reset the D-50/D-70 to factory default settings

Default profile lockout policy: 3 unsuccessful login attempts to the Admin, Advanced User or Cyber security profile will lock it for 1 hour. If you do not wish to wait 1 hour, you can reboot the D-50/D-70 display.

The lockout policy can be modified in the "Cyber Security" menu, in the "Security Policy" tab:



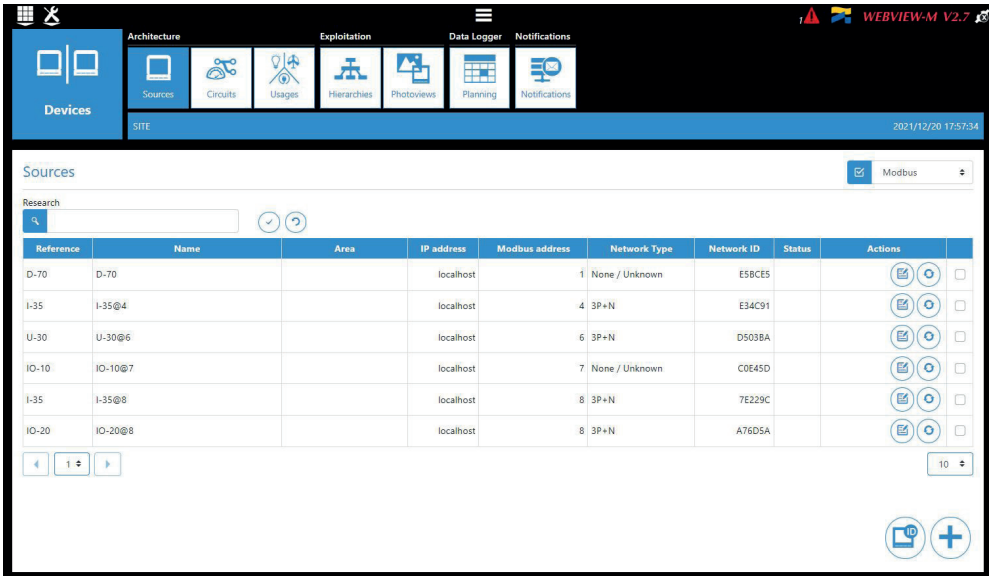
11.2. Admin profile

When connected as Admin, you can access the configuration page by clicking on the “wrench/screwdriver” icon on the top left corner:

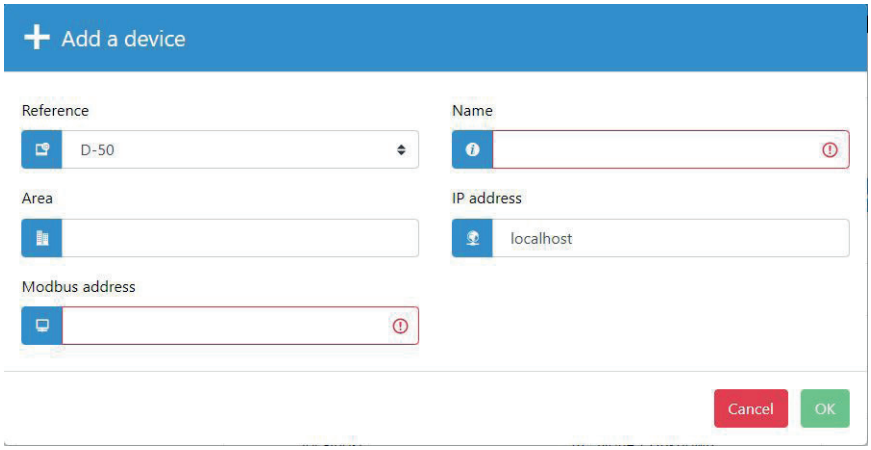
11.2.1. “Devices” menu

- Go to the “Devices” menu:

- After a few seconds, the devices present in the D-50/D-70 display's topology are displayed:



- Click on the "+" icon at the right bottom corner for manually adding products one at a time. Adding an M-xx gateway or D-xx display will add the entire topology under that gateway or display.



• The various SOCOMEC devices that are supported by WEBVIEW-M are given in the following list:

Gateways
- D-50
- D-50v2
- D-70
- G-30/G-40
- G-50/G-60
- M-50
- M-70

DIRIS B
- B-10
- B-30 RF
- B-30 RS485

DIRIS Digiware
- D-40
- I-30
- I-30 dc
- I-31
- I-33
- I-35
- I-35 dc
- I-43
- I-45
- I-60
- I-61
- IO-10
- IO-20
- S-130
- S-135
- S-Datacenter
- U-10
- U-20
- U-30
- U-31 dc
- U-32 dc
- R-60

COUNTIS
- Ci
- E03
- E04
- E13
- E14
- E17
- E18
- E23
- E24
- E27
- E28
- E33
- E34
- E43
- E44
- E44R
- E47
- E48
- E53
- ECI32
- ECI3

DIRIS A
- A-10
- A-20
- A-30
- A-40
- A-40 Ethernet
- A-40 Profibus
- A14
- A17
- A17 2In
- A17 THD
- A17 THD In
- A60
- A80

Switches
- ATyS p M
- C55
- C65
- C66

Old DIRIS A
- A10
- A20
- A20v2
- A40v2
- A40v3

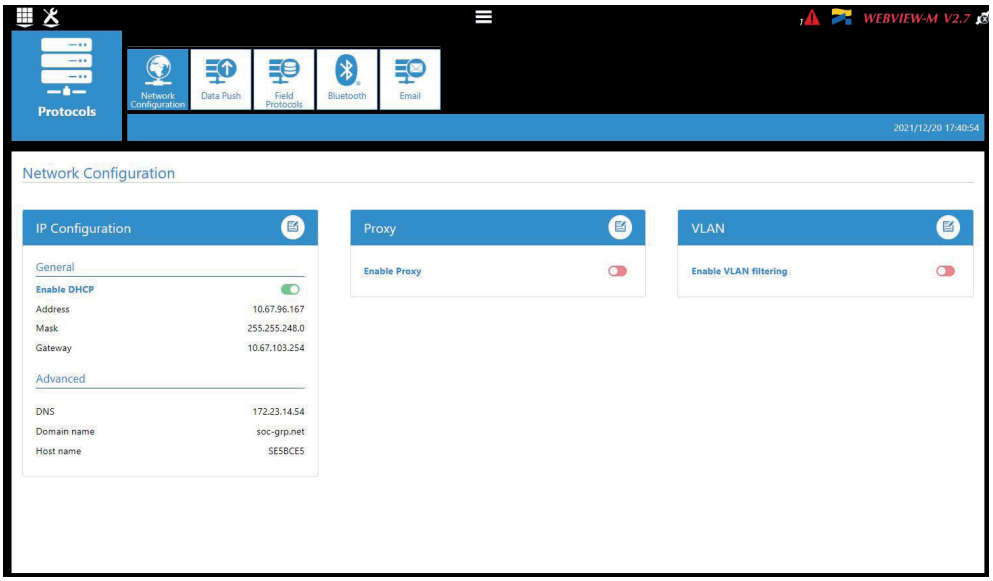
Other tabs such as “Hierarchy” and “Photoview” can be configured as well. They offer additional modes for the visualisation and analysis of measurements and consumption.

11.2.2. “Protocols” menu

Once the system is fully configured to visualise measurements and consumption on WEBVIEW-M, the communication protocols which will be used by the D-50/D-70 display to exchange data with an external supervisor (SCADA, Energy Management System, etc.) can be configured from the “Protocols” menu:

- **Network Configuration**

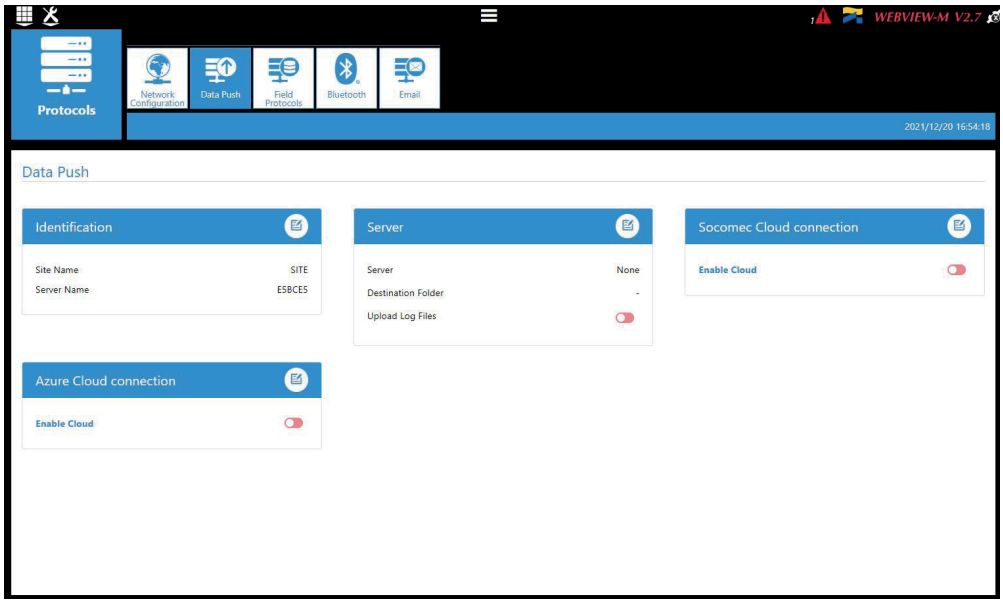
This tab allows you to modify the D-50/D-70 display’s IP configuration:



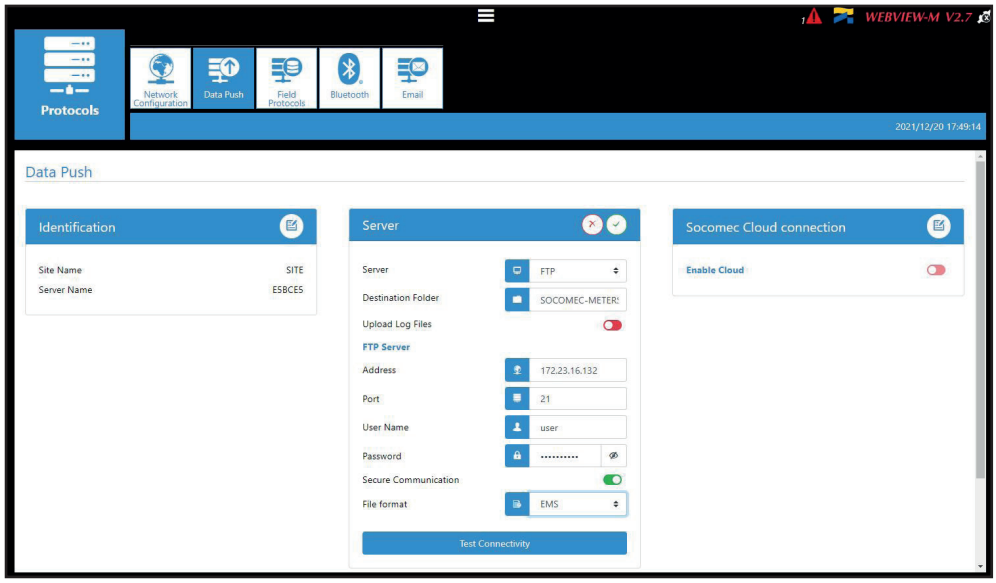
After modifying those parameters, a reboot of the D-50/D-70 display is necessary.

• **Data Push**

- Identification
  - Site name: This setting is essential to connect the D-50/D-70 display to a physical location within the project structure. Default Site name is “SITE” and must be changed (in EMS export mode only) or a system alarm will be triggered.
  - Server name: Unique identifier of the display. The default server name is the ID shown in the bottom right corner of the home screen of the D-50/D-70 display.

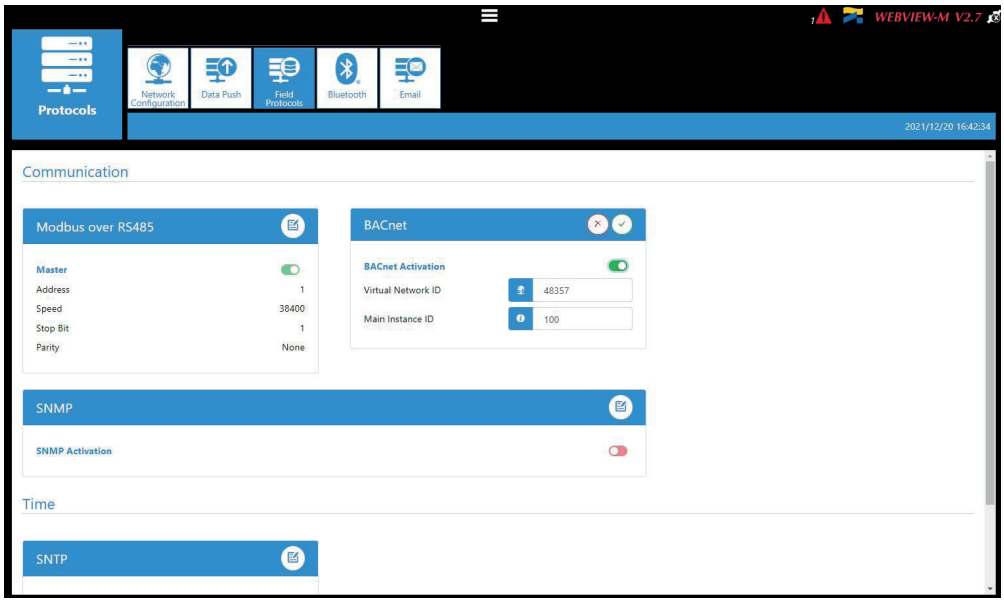


- Server
  - Server: To send data files to a remote server, the Administrator selects the FTP(S) server
  - Destination folder: Enter the remote server directory for receiving the files
  - Upload log files: Select if you want the display to also send the log file to the remote server
  - Address: Enter the IP address of the remote server
  - Port: Enter the software port (usually 20 or 21 for FTP and 990 for FTPS)
  - User name: enter the user name the access the remote server. It must be consistent with the User name configured on the FTP server.
  - Password: enter the password to access the remote server. It must be consistent with the password configured on the FTP server.
  - Secure communication: open a secure session between the display and the remote server
  - File format: data can be exported in different file formats (CSV and EMS – see appendices 1 and 2). The CSV format is easier to use while EMS is better for importing data into an external energy management software.
  - Test connectivity: Test the FTP export function



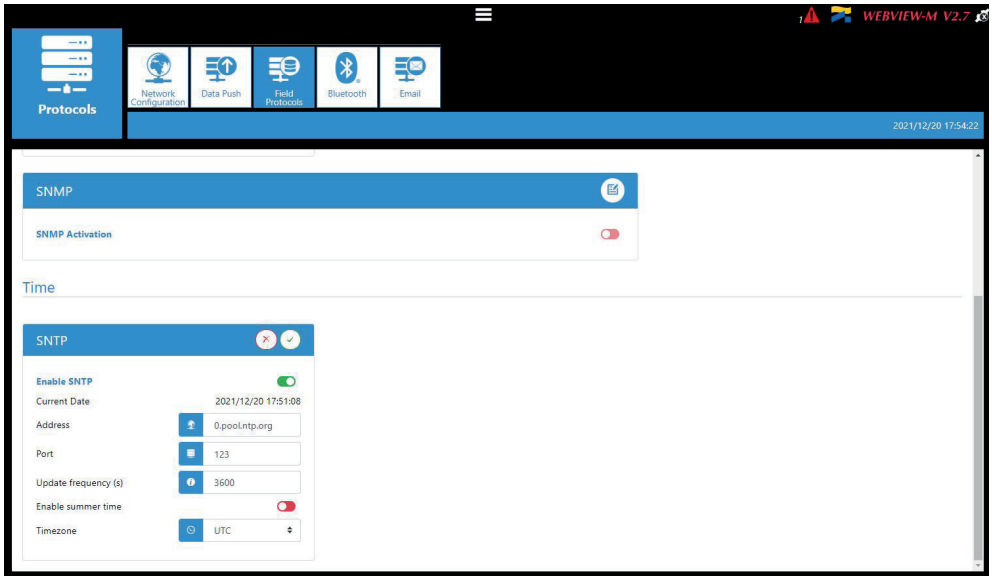
• **Field protocols**

- Communication: allows you to configure the different protocols that the D-50/D-70 display can use to communicate to external energy management systems.



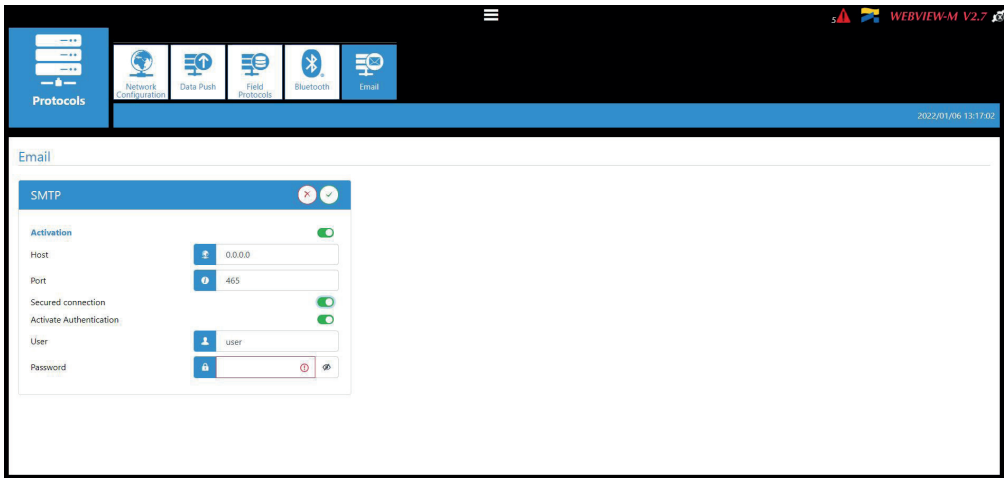
Refer to Annex. I and II for more information on SNMP and BACnet communication protocols with the D-50/D-70 display.

- Time: allows you to configure an SNTP server to automatically synchronise the clock of the D-50/D-70 display to an external computer.



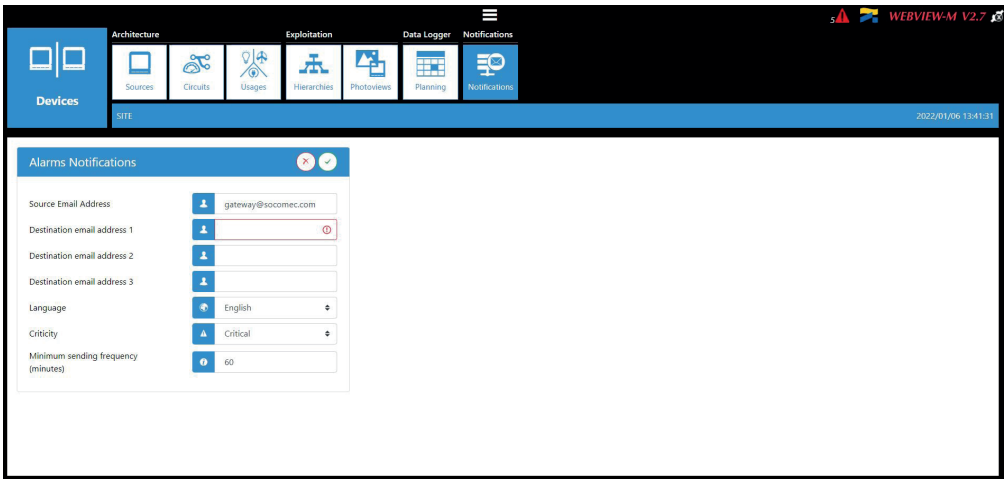
- **Email**

This tab allows you to activate and configure email notifications in case of alarms:



- Activation: enable/disable the SMTP email export function
- Host: enter the IP address or Host name of the SMTP server
- Port: enter the SMTP port
- Secured connection: enable or disable the secured connection (SMTPS)
- Activate Authentication: enable or disable the SMTP authentication. It is possible to activate the authentication, even if the secured connection is disabled.
- User: enter the user name for the authentication
- Password: enter the password for the authentication

Once the SMTP server has been configured, go to the "Devices" menu, "Notifications" tab to configure the email notification settings (source and recipient email address, notification frequency etc.):



- Source email address: email address used by the D-50/D-70 display to send emails
- Destination email address 1: email address #1 to which email notifications will be sent
- Destination email address 2: email address #2 to which email notifications will be sent
- Destination email address 3: email address #3 to which email notifications will be sent
- Language: language in which emails are sent
- Criticality of alarms to send: choose to send “information” or “Non critical” or “Critical” alarms
- Maximum waiting time: Time to wait to receive the email notification after the alarm is triggered on a device. This allows to limit the number of emails sent by the D-50/D-70 display, especially when the alarm repeatedly changes state.

11.3. Cyber security profile

In addition to the rights of the Admin profile, the Cyber security profile allows you to:

- Manage all profiles and change their passwords. The Cyber security profile also allows to generate the passphrase for password recovery.
- Implement a custom Cyber Security policy from a dedicated menu:

11.3.1. Cyber security menu

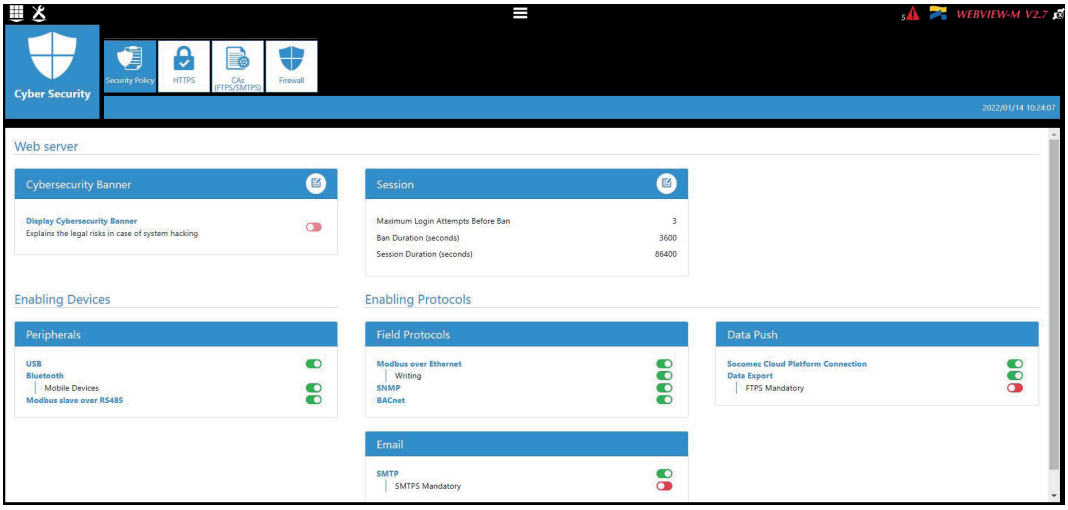
The Cyber Security menu allows you to:

- Define a custom security policy.
- Secure the client-server communication (HTTPS, FTPS, SMTPS).
- Prevent denial-of-service attacks by implementing a firewall in the D-50/D-70 display.

The configuration of Cyber security functions is explained in paragraphs 11.3.2 through 11.3.4.

11.3.2. “Security Policy” tab

DIRIS Digiware D-50/D-70 displays can reduce the attack exposure by disabling certain peripherals or services that are not essential to the customer’s use case.



Cybersecurity Banner

Choose if you want to display the cybersecurity banner which explains the legal risks in case of system hacking. The message will be displayed on login page.

Session

You can customise the session policy (maximum login attempts before profile lockout, lockout duration and session duration).

Peripherals

- USB: disable the USB port of the D-50/D-70 display.
- Bluetooth Low Energy: disable the Bluetooth Low Energy of the D-50/D-70 display.
- Modbus slave over RS485: authorise or disable Modbus communication on the RS485 port of the D-50/D-70 display.

Email

- Make the secure version of SMTP mandatory for email notifications in case of alarm on a connected device.

Field protocols

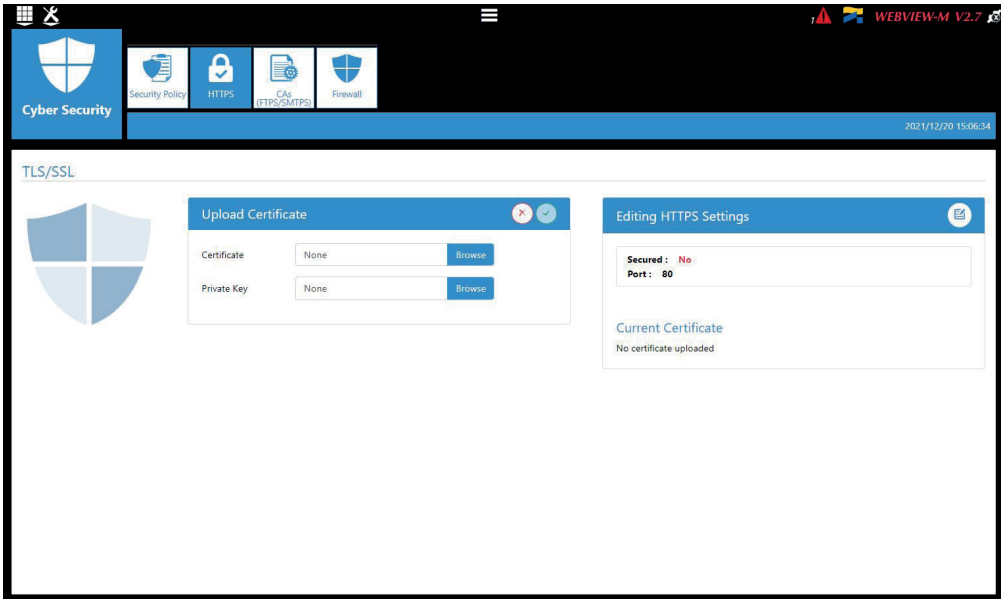
- Modbus Write function: authorise or disable to prevent people from changing settings over Modbus.
- SNMP: allow or disable the use of the SNMP protocol.
- BACnet: allow or disable the use of the BACnet protocol.

Data push

- Socomec cloud platform: authorise or block the export of data to the Socomec platform.
- Data export, FTPS mandatory: force the data export to an FTP server with a secure connection.

11.3.3. “HTTPS” tab

The HTTPS tab allows you to upload a digital certificate to secure the web navigation:



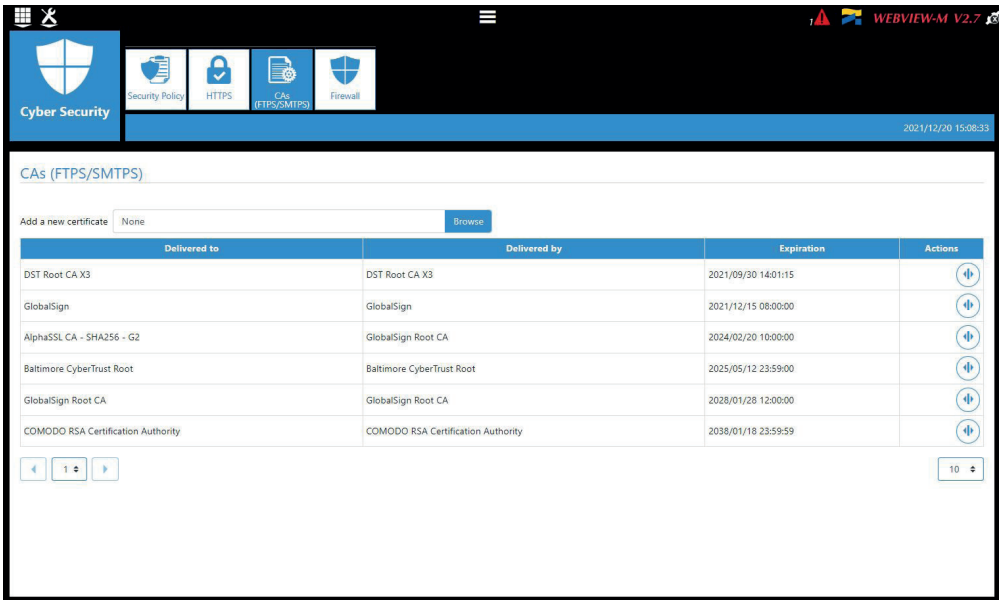
The D-50/D-70 displays will accept a digital certificate under the .pem format. Once a digital certificate and private key has been uploaded, you can edit HTTPS settings to secure the web navigation.

- The D-50/D-70 displays are compatible with RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) digital certificates. The use of ECDSA digital certificates is recommended to optimise the speed of the web navigation.
- The private key size must not exceed 2048 Bits.

11.3.4. CAs (FTPS/SMTPS) tab

This tab allows you to secure the client (D-50/D-70) to server (FTPS, SMTPS) communication by adding the relevant Certificate Authorities (CA) on the Client side.

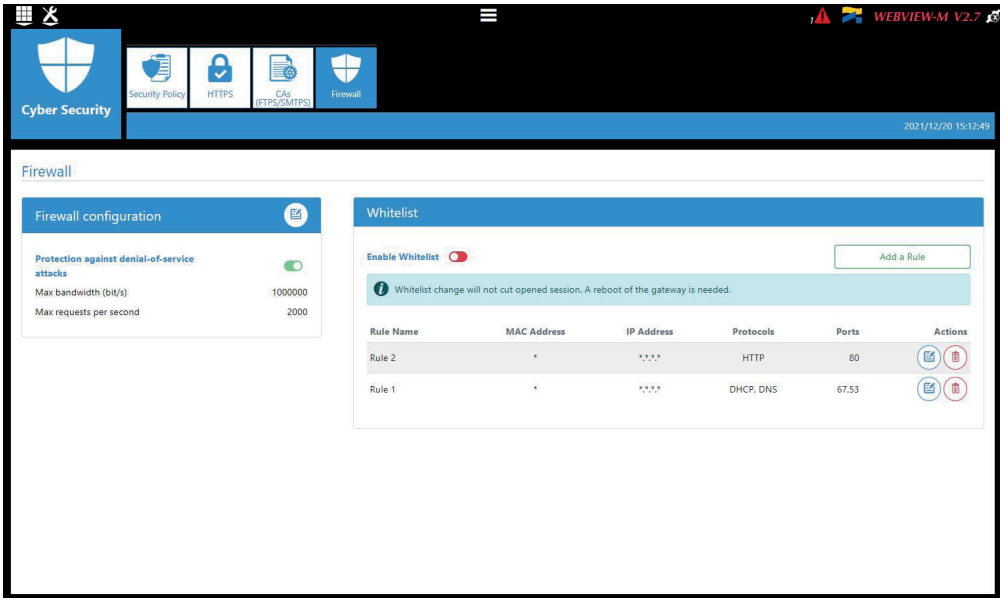
Several common Certificate Authorities are already included to the D-50/D-70 display, but the user can add others if necessary.



Refer to Annex. IV for more information on how to find and upload a server’s CA to a DIRIS Digiware D-50/D-70.

11.3.5. “Firewall” tab

This tab allows you to implement a firewall to protect against Denial-Of-Service attacks also called Flooding attacks by entering a max bandwidth in kbit/s and a max number of requests per second:



A client exceeding one of the above parameters while communicating to the DIRIS Digiware D-50/D-70 display will be blocked for 30 seconds.

The Whitelist part allows to add rules to filter the communication between hosts and the D-50/D-70 display on MAC Addresses / IP Addresses / Protocols / Ports.

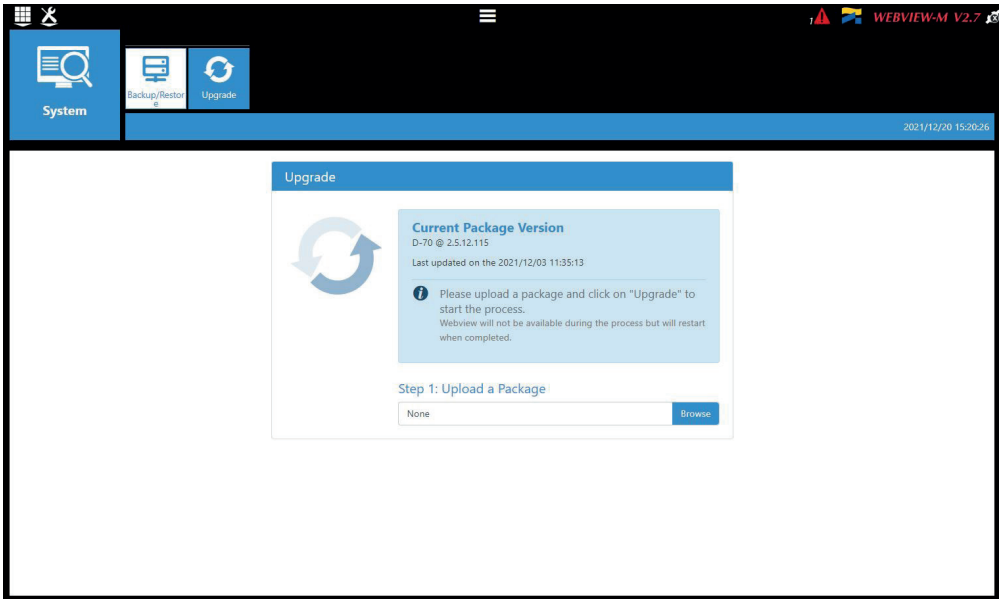
Up to 10 rules can be set.

- "*" in the MAC address column allows all MAC addresses.
- 192.168.*.* allows all IP addresses starting with 192.168.

11.3.6. Upgrading the firmware of the D-50/D-70 display

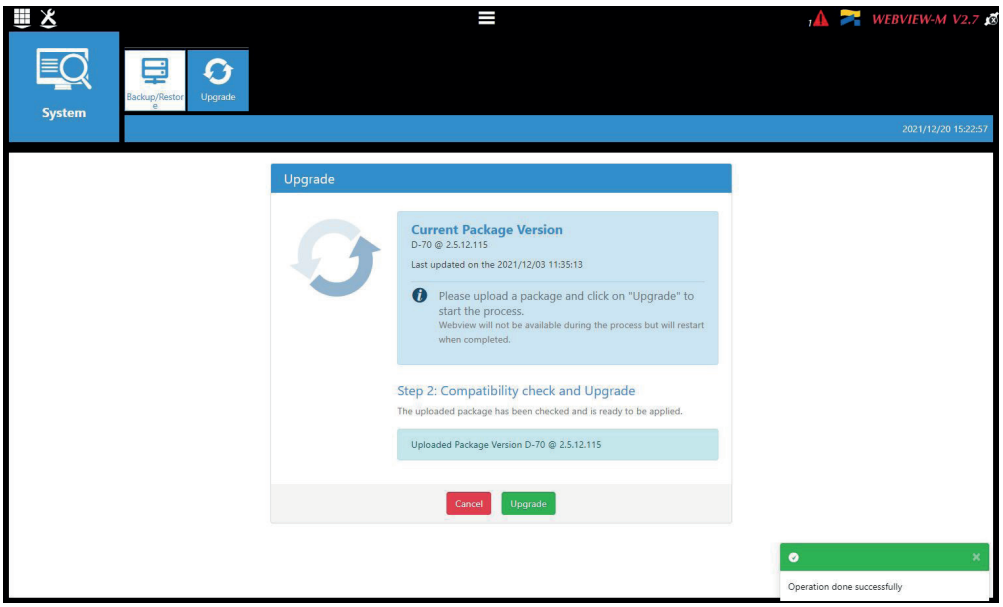
To upgrade the firmware of the DIRIS Digiware D-50/D-70 display, go to the “System” menu:

Go to the “Upgrade” tab:

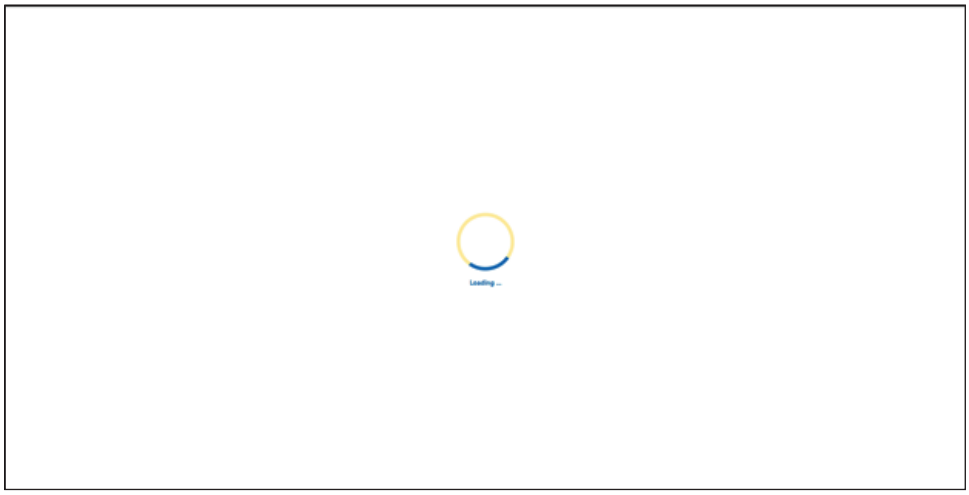


Upload the desired firmware package (.dfu file) by clicking on the “Browse” button.

Wait until the package is loaded, and once package consistency check is finished, click on “Upgrade”:



Once the upgrade is finished, the web page will reload automatically:



11.4. WEBVIEW-M

For more information on the visualisation of measurement data, please refer to the WEBVIEW-M instruction manual, available on the Socomec website at the following link:
https://www.socomec.com/range-software-solutions_en.html?product=/webview_en.html

12. ALARMS

DIRIS Digiware D-50 and D-70 displays collect alarms from downstream devices connected on the Digiware or RS485 bus.

DIRIS Digiware D-50 and D-70 displays also support 8 System alarms. The types of system alarms and the possible causes are listed in the table below:

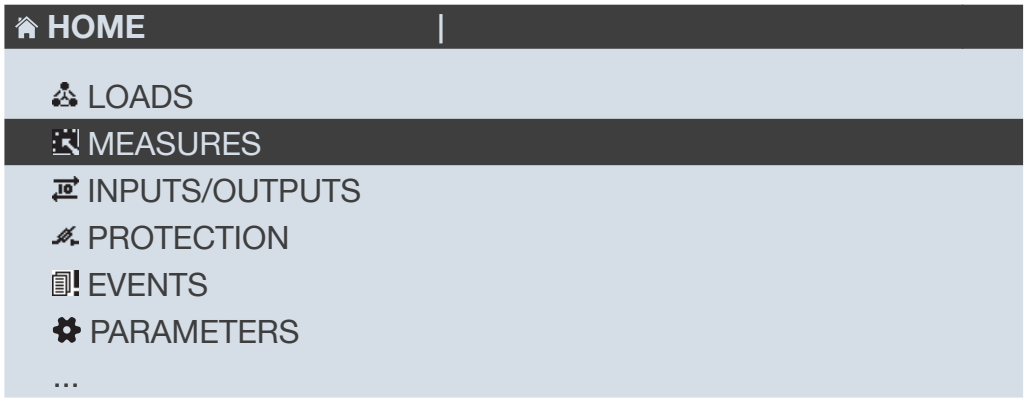
System alarm #	Alarm type	Description	Possible causes
System alarm 1	Email transmission error	Triggered if the D-50/D-70 display could not send the notification email in case of an alarm.	- Inconsistent password or user name between server and client - Incorrect server information - Server is not available
System alarm 2	SNTP Synchronisation error	Triggered if the D-50/D-70 display could not synchronise its internal clock to the SNTP server.	- Incorrect server information (address, port etc.) - Server is not available
System alarm 3	Modbus slave timeout error	Triggered if the D-50/D-70 display could not communicate with a Modbus slave on the Digiware or RS485 bus.	- Bad RS485 or Digiware connection. - Communication speed on the Digiware bus is too low (38400 by default) - Product is incorrectly requested (wrong Modbus register, …)
System alarm 4	Modbus address conflict	Triggered if the D-50/D-70 display has detected an address conflict among slaves.	A slave's Modbus address must be unique within Digiware and RS485 buses altogether; this alarm will be triggered if 2 slaves have the same Modbus address.
System alarm 5	Product damaged	Triggered if the product is flagged as damaged. Please return the device to Socomec.	- Product has a wrong Network ID, Serial Number or MAC Address - A newer version is available for a slave product
System alarm 6	FTP export error	Triggered if the D-50/D-70 display could not export data to the remote FTP server.	- Inconsistent password or user name between server and client - D-50/D-70 does not have permission to write files on FTP server - FTP server unavailable - Site Name is not configured
System alarm 7	Cyber Security alert	Triggered if the D-50/D-70 display detects a cyber security threat.	- Denial-of-service attack caught (client banned) - Expiration of a digital certificate
System alarm 8	Password alert	Triggered if there is an issue with the password of the Admin, Advanced User or Cyber security profile.	- Alarm is active by default until passwords are changed - Alarm is triggered once a year, 15 days before the expiration of one of the passwords and will remain active until they are changed - Alarm is also triggered if a user has been locked out after too many unsuccessful login attempts

When one or more System alarms are active, the ALARM LED on the front face of the D-50/D-70 display starts blinking.

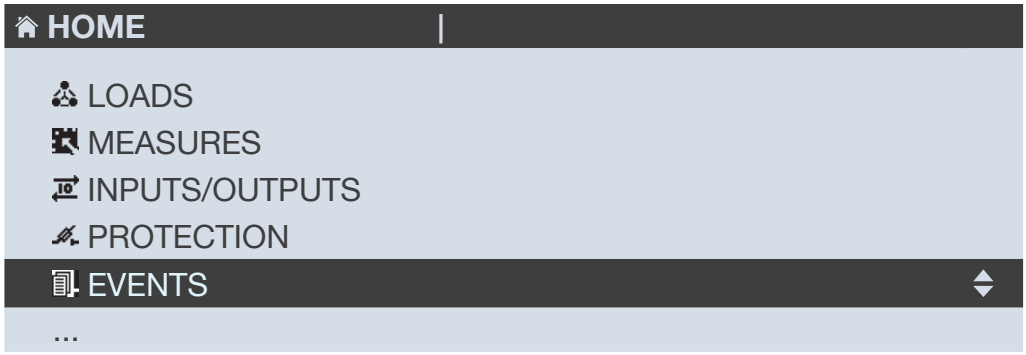
Alarms are displayed on WEBVIEW-M (for D-70 display only) and a notification will be sent by email if the SMTP(S) feature is enabled.

13. USE

Once the devices are configured, you can visualise the measurements of each load from the "MEASURES" menu.
You can view active and finished alarms from the "EVENTS" menu.



If the "ALARM" LED of the D-50/D-70 display is lit, stable or flashing, it means there is at least one active alarm. Go to the "EVENTS" menu to see which alarms are active.



The "Password Alert" alarm remains active (and the ALARM LED of the D-50/D-70 display blinks) until you change the default passwords of the Admin, Advanced and Cybersecurity profiles on the webserver.
The "Password alert" alarm can also be disabled from the Easy Config System software in the "Alarms" menu of the D-50/D-70.

14. DIRIS DIGIWARE D-50/D-70 TECHNICAL CHARACTERISTICS

14.1. Mechanical characteristics

Type of screen	Capacitive touch-screen technology, 10 keys
Screen resolution	350 x 160 pixels
Front panel protection index	IP65* (IEC 60529)
Weight DIRIS Digiware D-50 / D-70	210 g

* Front face only. The use of a silicone seal may be required to ensure sufficient sealing of the junction between D-50/D-70 display and panel door.

14.2. Communication characteristics

Type of screen	Multipoint remote screen
Ethernet RJ45 10/100 Mbs	Gateway function: - Modbus TCP (max. 32 simultaneous connections) - WEBVIEW-M embedded web server (D-70 only) - BACnet IP - SNMP v1, v2 & v3
SNTP protocol	Updates the D-50/D-70 from an SNTP server. The D-50/D-70 updates the connected devices.
SMTP(S) protocol	Email notifications in case of an alarm.
FTP(S) protocol	Automatically exports data via FTP standard or secure server (consumption curves, load curves, measurement logs).
RJ45 Digiware	Control and power supply interface function.
RS485 2-3 wires	1 port, configured as Input (Master) or Output (slave).
USB	Firmware upgrade and configuration via type B micro USB connector

14.3. Electrical characteristics

Power supply	24 VDC ±10% - Class 2 power supply unit according to UL1310 - 20 W max.
Power consumption	2.5 VA
Battery life	10 years with the following typical battery profile over its lifetime: - Product storage: 1 year of full time battery back-up (based on an average storage temperature of 25°C). - Product life: 10 days / year of battery back-up over 9 years
Battery type	3V Lithium cell battery, 48mAh rated capacity

14.4. Environmental characteristics

Use	Indoor
Storage temperature	-40°C … +70°C (IEC 60068-2-1 / IEC 60068-2-2)
Operating temperature	-10°C … +55°C (IEC 60068-2-1 / EN/IEC 60068-2-2)
Humidity	40°C / 95% RH (IEC 60068-2-30)
Pollution degree	2
PEP ecopassport - ISO 14025	DIRIS Digiware D: SOCO-00043-V01.01-EN

14.5. EMC characteristics

Characteristic	Test standard	Performance criteria	Level
Electrostatic discharges (Contact)	IEC 61000-4-2	B	III
Electrostatic discharges (Air)	IEC 61000-4-2	B	III
Radiated radio-frequency field immunity	IEC 61000-4-3	A	III
Burst immunity	IEC 61000-4-4	B	III
Surge immunity (Common mode)	IEC 61000-4-5	B	III
Surge immunity (Differential mode)	IEC 61000-4-5	NA	NA
Conducted RF immunity	IEC 61000-4-6	A	III
Power magnetic field immunity	IEC 61000-4-8	A	IV / 400 A/m
Dips immunity	IEC 61000-4-11	NA	NA
Conducted emissions	CISPR11	NA	NA
Radiated emissions	CISPR11	Passed	Gr:1 – Class B

ANNEX I. SNMP COMWMUNICATION WITH THE DIRIS DIGIWARE D-50 / D-70

Annex I - 1. SNMP generalities

SNMP stands for Simple Network Management Protocol and is widely used by administrators for an easy network monitoring of devices on IP networks. It works in a client-server communication mode on an Ethernet physical layer.

Once enabled from the Easy Config configuration software, the DIRIS Digiware D-70 display supports SNMP v1, v2 and v3.The D-50 / D-70 is an agent SNMP v1, v2, v3 which responds to queries from managers (also called management stations or supervisors).

The D-50 / D-70 allows access through SNMP of measurement data from SOCOMEC slaves connected via the RS485 bus or the Digiware bus.

Data from the slaves can be reached through a file called “MIB” (“Management Information Base”) under a hierarchical and pre-defined structure. The MIB file of the D-50 / D-70 is named ”socomec-diris-products-mib” and is available from www.socomec.com
The file must be uploaded in the Management station managing your metering system.

The Tree structure of the MIB contains multiple OIDs (Object Identifiers). An OID uniquely identifies and labels a managed object (=parameter from metering devices) in the MIB.

For example, the electrical parameter “Current Inst I1” is identified by one OID. “Current Inst I2” is identified by another one.

Common SNMP terms	Consumption curves
Agent	Corresponds to the DIRIS Digiware D-50 / D-70: Interface between the PMDs and the manager
Managed device	The PMDs connected downstream the D-50 / D-70 (ex: I-35, DIRIS B, DIRIS A…)
MIB	Management information base where the OIDs are organized in a hierarchical tree
OID	An object identifier that uniquely identifies and labels a managed object in the MIB hierarchy
Community strings	A text that enables the authentication between an agent and the manager
Traps	Notifications sent by the agent and received by the manager

Annex I - 2. SNMP functions supported

There are 4 types of SNMP requests supported by the DIRIS Digiware D-50 / D-70:

- **GetRequest:** to retrieve the variable of an OID (I1 Inst for example)
- **GetNextRequest:** to retrieve the variable of the next OID (I2 Inst in this case)
- **GetBulk:** to retrieve multiple variables gathered together
- **SetRequest:** to change the value of one variable such as the state of a Digital output.
- **Traps:** Unlike the above commands which are initiated by the SNMP manager, Traps are initiated by the Agents with no solicitation from the Manager. Traps are notifications to the Manager by the Agent of the occurrence of an event and/or alarm..

Traps are sent by the agent in case one of the following alarms occurs:

- Alarm on a measurement
- Logical alarm (change of status of a Digital input)
- Combination alarms
- PQ events (inrush, voltage swells, voltage sags/dips, voltage interruptions)
- System alarms (Phase Rotation, CT disconnect, VI association)

Traps are sent automatically when the alarm occurs. They will be sent again once the “Trap report frequency” time (entered in Easy Config) is elapsed.

The alarm must be activated in the product (using the configuration software Easy Config) in order for the Traps to be sent. Traps can either be configured for specific hosts or “broadcast” to the whole network. Up to two server IP addresses can be entered in Easy Config for SNMP trap notification of specific hosts.

Annex I - 3. SNMP versions supported

The DIRIS Digiware D-50 / D-70 can use all three versions of SNMP: SNMPv1, v2 and v3.

- **SNMPv1 and v2:**

The identification is based on Read-only and Read-Write Community passwords. They are non-encrypted and are passed over the network in plaintext.

Both passwords have to be entered in the Agent (DIRIS Digiware D-50 / D-70) and the Manager and must be identical.

A matching Read Community allows the Get functions to be executed on the agent.

A matching Read-Write Community also allows the Set function to be executed on the agent.

- The default Read Community V1 password is “public” and the default Read-Write Community V1 password is “Private”.

- The default Read Community V2 password is “publicv2” and the Read-Write Community V2 is “privatev2”.

- **SNMPv3:**

SNMPv3 uses the USM (User-based Security Module) for controlling access to information available via SNMP. This version offers more security using three important features to prevent the interception and deciphering of data:

- A username (called security username)

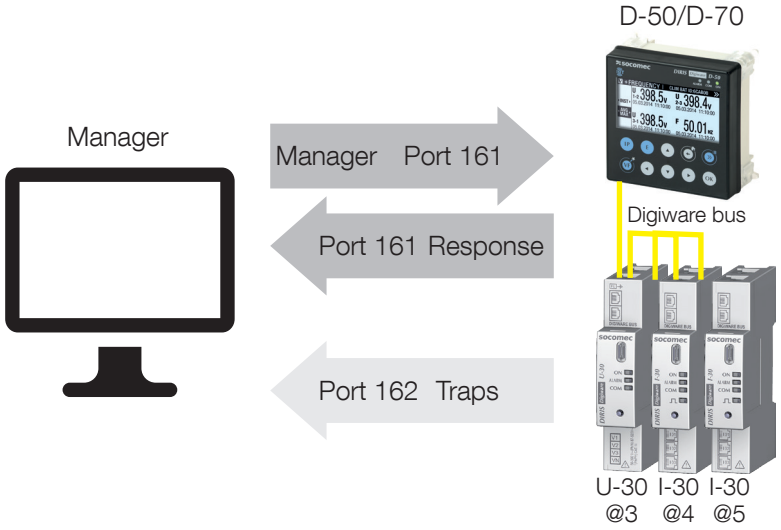
- MD5 and SHA1 authentication protocols to hash the passwords

- DES and AES Privacy protocols to encrypt the data

Annex I - 4. SNMP ports

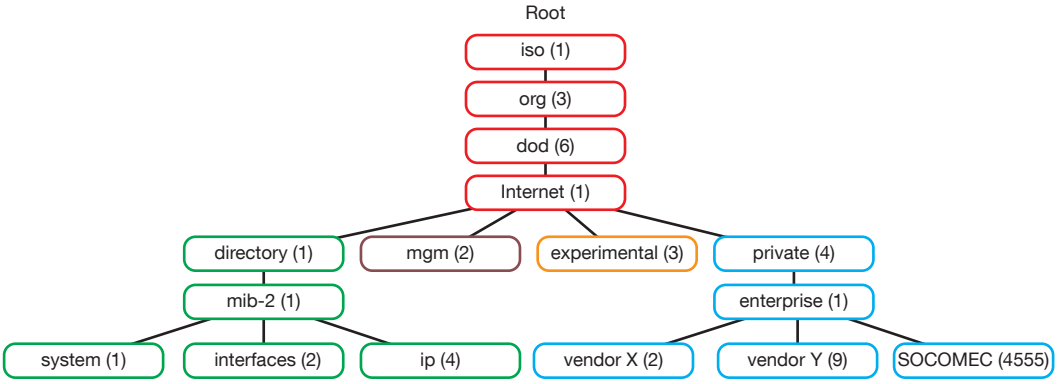
The DIRIS Digiware D-50 / D-70 is configured with standard SNMP ports to receive requests and send notifications:

Port	Description
161	Used to send and receive requests from the manager.
162	Used by the manager to receive notifications from the agent



Annex I - 5. Retrieving data using the DIRIS Digiware D-50 / D-70 MIB file

The DIRIS Digiware D-50 / D-70 is compliant with MIB-II defined by the MIB standard RFC 1213 which defines the following structure:



OID Tree Example

The standard branches are under the same parent branch structure: 1.3.6.1.4.1

The “Private (4)” group enables vendors to define private branches including the MIB OIDs of their own products. Data related to SOCOMEC metering devices is located under the SOCOMEC enterprise category identified by OID 1.3.6.1.4.1.4555. This implies that all queries from a manager to SOCOMEC agents will start by the base path 1.3.6.1.4.1.4555.

Because the DIRIS Digiware is a multi-circuit system, the DIRIS Digiware D-50 / D-70 creates a dynamic table which depends on the products connected downstream compatible with the DIRIS Digiware D-50 / D-70 and the loads configured on each product.
After adding/deleting a downstream device or a load, make sure to update the topology of the D-70 display. This can be done either directly from the display or from Webview:

- Add or delete a device
- Refresh the loads

Example: The OID for “Current Inst I1” will return a value for all I-xx, B-xx, DIRIS A etc.. On the contrary, the OID for “THD Inst I1” will return “0” for an I-30 or an I-31 module.

This implies that each OID can be associated with several products and several loads.

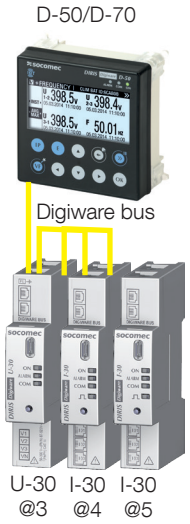
For example the OID for instCurrentI1 is represented by the sequence 1.3.6.1.4.1.**4555.10.20.20.1.10000**.

OID sequence	Description
4555	“SOCOMEC” enterprise branch
10	“SocomecProducts” table
20	“ProductMetrology” table
20	“InstantaneousTable”
1	Entry (always = 1)
10000	Service ID

This OID is associated with the multiple devices connected downstream the DIRIS Digiware D-50 / D-70.

To identify those multiple devices, the Modbus address and the load number are added to the end of the OID.

Example: Let us consider the following architecture:



Product	I-30	I-30
Modbus address	4	5
Load type	Load 1: 3P + N - 3CT	Load 1: 1P + N - 1CT Load 2: 1P + N - 1CT Load 3: 1P + N - 1CT

The final OID to get the instantaneous current I1 for the I-30 module @ Modbus address 4 for load 1 is:
1.3.6.1.4.1.4555.10.20.20.1.10000.4.1

For the I-30 module @ address 5, there are multiple loads configured. This implies that the Modbus address must be followed by the Load number in the OID.

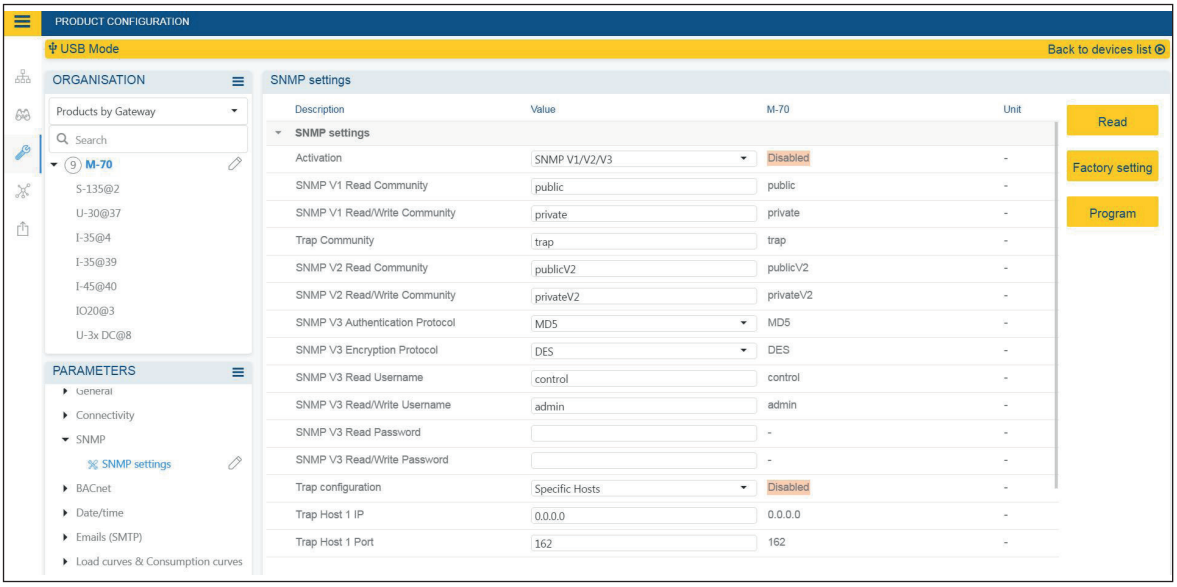
Therefore, the final OID used to request I1 Inst for load 1 of the I-30 @ address 5 is:
1.3.6.1.4.1.4555.10.20.20.1.10000.5.1
The final OID to request I1 Inst for load 2 of the I-30 @ address 5 is **1.3.6.1.4.1.4555.10.20.20.1.10000.5.2**
The final OID to request I1 Inst for load 3 of the I-30 @ address 5 is **1.3.6.1.4.1.4555.10.20.20.1.10000.5.3**

OID sequence	Description
4555	“SOCOMEC” enterprise branch
10	“SocomecProducts” table
20	“ProductMetrology” table
20	“InstantaneousTable”
1	Entry (always = 1)
10000	Service ID
5	Modbus Address
3	Load number

Note: a request to OID 1.3.6.1.4.1.4555.10.20. 20.1.10001.5 will return “0” because the service ID 10001 corresponds to I2 inst whereas only single-phase loads are configured in the I-30 module @ address 5, which means currents I2 and I3 parameters aren’t used.

Annex I - 6. SNMP configuration via Easy Config System

After logging in to Easy Config System on the DIRIS Digiware D-50 / D-70, you can find the SNMP settings in the SNMP menu, under SNMP settings:



- **Community configuration SNMP V1 & V2:**
  - **SNMP V1 Read Community:** Read-only community string for SNMP v1. Default community string is “public”. It allows a manager to retrieve read-only data from a device connected to the DIRIS Digiware D-50 / D-70.
  - **SNMP V1 Read/Write Community:** Read-Write community string for SNMP v1. Default Read/Write community string is “private”. It allows a manager to write (ex: position of a Digital output) to a device connected to the DIRIS Digiware D-50 / D-70.
  - **Trap Community:** The Trap community string allows the manager to receive notifications in case of an event and/or alarm.
  - **SNMP V2 Read Community:** Read-only community string for SNMP v2. Default community string is “publicV2”. It allows a manager to retrieve read-only data from a device connected to the DIRIS Digiware D-50 / D-70.
  - **SNMP V2 Read/Write Community:** Read-Write community string for SNMP v2. Default Read/Write community string is “privateV2”. It allows a manager to change a setting (ex: position of a Digital output) in a device connected to the DIRIS Digiware D-50 / D-70.

- **SNMP V3 configuration:**
  - **SNMP V3 Authentication Protocol:** If SNPM v3 is activated, you can choose an authentication protocol (MD5 or SHA) to hash your password. For no authentication, select “None”.
  - **SNMP V3 Encryption Protocol:** Choose between DES or AES privacy protocols for the encryption of data messages. For no encryption, select “None”.
  - **SNMP V3 Read Username:** Username enabling authentication for read-only functions.
  - **SNMP V3 Read/Write Username:** Username enabling authentication for read and write functions.
  - **SNMP V3 Read Password:** Password (also passphrase) accompanying the authentication and privacy protocols, and allowing read-only functions. The length of the Read-only authentication & privacy password must be between 8 and 16 characters.
  - **SNMP V3 Read/Write password:** Password (also called passphrase) accompanying the authentication and privacy protocols and allowing read and write functions. The length of the Read-Write authentication & privacy password must be between 8 and 16 characters.
  - **Trap configuration:** Choose to deactivate or activate the traps. If activated, you can choose to broadcast trap notifications to all supervisers on the network or to notify only specific host stations (up to 2).
  - **Trap Host 1 IP:** Enter the IP address of the 1st host station which will receive trap notifications.
  - **Trap Host 1 port:** Enter the port used to send traps for the 1st host station.
  - **Trap Host 2 IP:** Address: enter the IP address of the 2nd host station which will receive trap notifications.
  - **Trap Host 2 port:** Enter the port used to send traps for the 2nd host station.
  - **Trap notification cycle:** Enter the time after which a trap reminder will be sent for active alarms. By default, it is set to 60min.

ANNEX II. BACNET COMMUNICATION WITH THE DIRIS DIGIWARE D-50 / D-70

The DIRIS Digiware D-50 / D-70 supports the BACnet IP protocol.
It acts as a BACnet IP gateway to all devices compatible and connected downstream via RS485 or the Digiware Bus.

The PICS (Protocol Implementation Conformance Statement) of the DIRIS Digiware D-50 / D-70 is available on the Socomec website at www.socomec.com.

Annex II - 1. BACnet Generalities

BACnet provides a method for computer-based control equipment from different manufacturers to be interoperable. BACnet is designed to handle many types of building controls, including HVAC, lighting, security, fire, access control, maintenance, waste management and so forth.

Common terms used in BACnet communication:

Object: Represents a device and its data. Multiple objects type can be available for each device *analog input, binary input…). Each object has a number of properties which fully describe the BACnet object to the network.

Object identifier: Uniquely identifies an object within a BACnet device.

Property: A property describes a BACnet object to the network.

Present value: It is one of the properties of the Analog_Input Object. It represents the current value of an analog input object.

Service: Message type between one BACnet device to another.

BACnet uses a client/server communication mode between devices. Devices communicate between each other using services describing the type of exchange.
A BACnet client is a device that requests a service, and a BACnet server is a device that executes a service.
Data inside a BACnet device is organized as a series of objects, each composed of multiple properties.

Ex: the analog_input object defines a property for present_value, a property for average_value etc…

A BACnet client initiates a request to a BACnet server using a service (ex: read_property) to a specific property (ex: present_value) contained in a BACnet object (ex: analog_input).

Annex II - 2. BACnet Objects

BACnet defines a standard set of “Objects”, each of which has a standard set of “Properties” describing the object and its current status to other devices on the BACnet internetwork. The properties allow for the object to be controlled by other BACnet devices.

BACnet defines 54 objects. Each element of the building control system is represented by one or more objects.
The DIRIS Digiware M-50 / M-70 supports the below Objects:

Object type	Exemple of use
Device	To describe the device to the BACnet network.
Analog input	Instantaneous current for phase 1 (I1) measured by a DIRIS Digiware I-xx current module with associated current sensor
Binary input	Status (ON/OFF) of an auxiliary contact
Binary output	Change of status of the output of a DIRIS Digiware IO-10

A list of properties defines each BACnet Object. Properties can be:

- Required by the BACnet specification.
- Optional. In this case, vendors can choose whether to implement them for their devices.
- Proprietary. Vendors can add their own created properties.

Device Object:

Every BACnet device compatible with the DIRIS Digiware D-50 / D-70 must have the Device Object and its associated required properties that fully describe the BACnet device to the network.

Example for the Device Object of the DIRIS Digiware D-50 / D-70:

Property	BACnet
Object_Identifier (OID)	Required
Object_Name	Required
Object_Type	Required
System_Status	Required
Vendor_Name	Required
Vendor_Identifier	Required
Model_Name	Required
Firmware_Revision	Required
Application_Software_Version	Required
Protocol_Version	Required
Protocol_Conformance_Class	Required
Protocol_Services_Supported	Required
Protocol_Object_Types_Supported	Required
Object_List	Required
Max_APDU_Length_Supported	Required
Segmentation_Supported	Required
APDU_Timeout	Required
Location	Optional
Description	Optional
Local_Time	Optional
Utc_Offset	Optional
Local_Date	Optional
Daylight_Saving_Status	Optional
Active_COV_Subscriptions	Optional
Serial_Number	Optional
Property_List	Optional
Version_Build_Date	Proprietary
Operating_Hour_Counter	Proprietary

The way the OID is assigned to a device (instance number) is the following:

OID = Main OID (= default 100) + ModbusAddress:

- Device with Main OID (100) is the DIRIS Digiware D-50 / D-70 display itself.
- The device with OID (1xx) is the device with the Modbus address xx.

Analog Input Object:

The DIRIS Digiware D-50 / D-70 acts as a BACnet gateway. It provides a number of Analog Input objects which may be available from the devices compatible and connected to the DIRIS Digiware D-50 / D-70.
Whether a device supports an AI object depends on its measurement functionalities.

Ex: The OID for THD_I1 will return 0 for a DIRIS Digiware I-30 module because this parameter is not handled.

The AI object defines 25 properties. The devices compatible and connected downstream the DIRIS Digiware D-50 / D-70 support the following properties:

Property	BACnet
Object_Identifier	Required
Object_Name	Required
Object_Type	Required
Present_Value	Required
Status_Flags	Required
Event_State	Required
Out_Of_Service	Required
Units	Required
Description	Optional
Reliability	Optional
Min_Pres_Value	Optional
Minimum_Value_Timestamp	Optional
Max_Pres_Value	Optional
Maximum_Value_Timestamp	Optional
Average_Value	Optional
Instantaneous_Timestamp	Proprietary
Average_Timestamp	Proprietary
Max_Average_Value	Proprietary
Max_Average_Timestamp	Proprietary
Min_Average_Value	Proprietary
Min_Average_Timestamp	Proprietary
Harmonics_Row_02	Proprietary
Harmonics_Row_03	Proprietary
Harmonics_Row_04	Proprietary

Property	BACnet
Harmonics_Row_05	Proprietary
Harmonics_Row_06	Proprietary
Harmonics_Row_07	Proprietary
Harmonics_Row_08	Proprietary
Harmonics_Row_09	Proprietary
Harmonics_Row_10	Proprietary
Energy_Total_Residual	Proprietary
Energy_Total_Hourmeter	Proprietary
Energy_Partial	Proprietary
Energy_Partial_Residual	Proprietary
Energy_Partial_Hourmeter	Proprietary
Energy_Total_Lagging	Proprietary
Energy_Total_Lagging_Res	Proprietary
Energy_Total_Leading	Proprietary
Energy_Total_Leading_Res	Proprietary
Energy_Last_Partial	Proprietary
Energy_Last_Partial_Res	Proprietary
Energy_Last_Partial_Timestamp	Proprietary
Multifluid_Partial	Proprietary
Multifluid_Weight	Proprietary
Instant_Min_Max_Reset	Proprietary
Average_Min_Max_Reset	Proprietary

The way the OID is assigned to an Analog Input Object (instance number) is the following:
OID = LLMM

- with LL = Load # of the device (starting at 1).
- with MM = Index of the measurement type (see Analog Input Measurement List).

For example, Analog Input with OID 204 reflects Phasis/Neutral Voltage V1 of Load 2 of corresponding device.

The table with indexes of the analog input measurement list is given below:

Index	Object Namew	Object Description	Unit	Type	Present + Timestamp	Present Min/Max + Timestamp	Average + Timestamp	Average Min/Max + Timestamp	Harmonics 2 -> 10	Energies Total + Partial + LastPartial	Energies Total Lagging/Leading	Multifluid	Reset Min/Max
0	VystPhN	System Ph-N Voltage	V	Unsigned	•								•
1	VystPhPh	System Ph-Ph Voltage	V	Unsigned	•								•
2	CurrentSyst	System Current	A	Unsigned	•								•
3	Frequency	System Frequency	Hz	Unsigned	•	•	•	•					•
4	VoltPhNV1	Ph-N Voltage V1	V	Unsigned	•	•	•	•					•
5	VoltPhNV2	Ph-N Voltage V2	V	Unsigned	•	•	•	•					•
6	VoltPhNV3	Ph-N Voltage V3	V	Unsigned	•	•	•	•					•
7	VoltPhNVn	Ph-N Voltage Vn	V	Unsigned	•	•	•	•					•
8	VoltPhPhU12	Ph-Ph Voltage U12	V	Unsigned	•	•	•	•					•
9	VoltPhPhU23	Ph-Ph Voltage U23	V	Unsigned	•	•	•	•					•
10	VoltPhPhU31	Ph-Ph Voltage U31	V	Unsigned	•	•	•	•					•
11	CurrentI1	Current I1	A	Unsigned	•	•	•	•					•
12	CurrentI2	Current I2	A	Unsigned	•	•	•	•					•
13	CurrentI3	Current I3	A	Unsigned	•	•	•	•					•
14	CurrentIn	Current In	A	Unsigned	•	•	•	•					•
15	CurrentInba	Current Inba	%	Unsigned	•								•
16	CurrentIdir	Current Idir	A	Unsigned	•								•
17	CurrentIinv	Current Iinv	A	Unsigned	•								•
18	CurrentIhom	Current Ihom	A	Unsigned	•								•
19	CurrentInb	Current Inb	%	Unsigned	•								•
20	PowerApparentNom	Nominal Apparent Power	VA	Unsigned	•								•
21	TotalPowerActive	Total Active Power	W	Signed	•	•	•	•					•
22	TotalPowerRActive	Total Reactive Power	VAr	Signed	•	•	•	•					•
23	TotalPowerApparent	Total Apparent Power	VA	Unsigned	•	•	•	•					•
24	TotalPowerFactor	Total Power Factor	-	Signed	•	•	•	•					•
25	TotalPowerFactorType	Total Power Factor Type	-	Unsigned	•	•	•	•					•
26	PowerActiveP1	P1 Active Power	W	Signed	•	•	•	•					•
27	PowerActiveP2	P2 Active Power	W	Signed	•	•	•	•					•
28	PowerActiveP3	P3 Active Power	W	Signed	•	•	•	•					•
29	PowerRActiveQ1	Q1 Reactive Power	VAr	Signed	•	•	•	•					•
30	PowerRActiveQ2	Q2 Reactive Power	VAr	Signed	•	•	•	•					•
31	PowerRActiveQ3	Q3 Reactive Power	VAr	Signed	•	•	•	•					•
32	PowerApparentS1	S1 Apparent Power	VA	Unsigned	•	•	•	•					•
33	PowerApparentS2	S2 Apparent Power	VA	Unsigned	•	•	•	•					•
34	PowerApparentS3	S3 Apparent Power	VA	Unsigned	•	•	•	•					•
35	PowerFactorPF1	PF1 Power Factor	-	Signed	•	•	•	•					•

Index	Object Namew	Object Description	Unit	Type	Present + Timestamp	Present Min/Max + Timestamp	Average + Timestamp	Average Min/Max + Timestamp	Harmonics 2 -> 10	Energies Total + Partial + LastPartial	Energies Total Lagging/Leading	Multifluid	Reset Min/Max
36	PowerFactorTypeSPF1	sPF1 Power Factor Type	-	Unsigned	•	•	•	•					•
37	PowerFactorPF2	PF2 Power Factor	-	Signed	•	•	•	•					•
38	PowerFactorTypeSPF2	sPF1 Power Factor Type	-	Unsigned	•	•	•	•					•
39	PowerFactorPF3	PF3 Power Factor	-	Signed	•	•	•	•					•
40	PowerFactorTypeSPF3	sPF1 Power Factor Type	-	Unsigned	•	•	•	•					•
41	LoadCurve_ P+	Load Curve Positive Active Power	W	Unsigned	•								•
42	LoadCurve_P-	Load Curve Negative Active Power	W	Unsigned	•								•
43	LoadCurve_ Q+	Load Curve Positive Reactive Power	VAr	Unsigned	•								•
44	LoadCurve_Q-	Load Curve Negative Reactive Power	VAr	Unsigned	•								•
45	LoadCurve_S	Load Curve Apparent Power	VA	Unsigned	•								•
46	THD_I1	THD I1	%	Unsigned	•	•			•				•
47	THD_I2	THD I2	%	Unsigned	•	•			•				•
48	THD_I3	THD I3	%	Unsigned	•	•			•				•
49	THD_In	THD In	%	Unsigned	•	•			•				•
50	THD_V1	THD V1	%	Unsigned	•	•			•				•
51	THD_V2	THD V2	%	Unsigned	•	•			•				•
52	THD_V3	THD V3	%	Unsigned	•	•			•				•
53	THD_U12	THD U12	%	Unsigned	•	•			•				•
54	THD_U23	THD U23	%	Unsigned	•	•			•				•
55	THD_U31	THD U31	%	Unsigned	•	•			•				•
56	A+	Positive Active Energy	Wh	Unsigned	•					•			•
57	A-	Negative Active Energy	Wh	Unsigned	•					•			•
58	ER+	Positive Reactive Energy	VArh	Unsigned	•					•	•		•
59	ER-	Negative Reactive Energy	VArh	Unsigned	•					•	•		•
60	ES	Apparent Energy	VAh	Unsigned	•					•			•
61	Mff	Multifluid feeder	-	Signed	•							•	•

Annex II - 3. BACnet Services

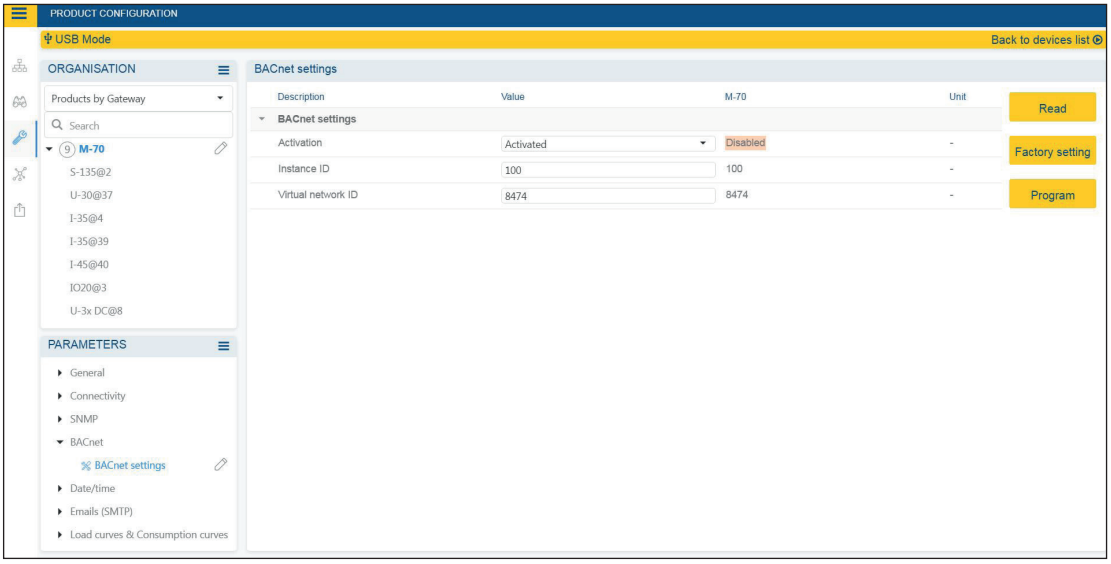
The services define methods for BACnet devices to communicate and exchange data with one another.
The D-50 / D-70 supports the following services:

Service list	Description
readProperty	Used by a BACnet device (the client) to ask another BACnet device (the server) to provide the value of one of its object properties
readPropertyMultiple	Used by a BACnet device (the client) to ask another BACnet device (the server) to provide the values of multiple object properties
writeProperty	Used by a BACnet device (the client) to ask another BACnet device (the server) to change the value of one of its object properties
timeSynchronization	Used to broadcast the current time to one or more BACnet servers
who_Has	Asks which BACnet devices contain a particular Object
who_Is	Used by a BACnet client to ask the presence of BACnet servers

Annex II - 4. BACnet IP configuration via Easy Config System

The PICS file (Protocol Implementation Conformance Statement) is available at www.socomec.com

After logging in to Easy Config System on the DIRIS Digiware D-50 / D-70, you can find the BACnet IP settings in the BACnet menu under BACnet settings:



Activation: Enable or disable the BACnet IP function

Main instance ID: 100 by default. It must be unique within the BACnet network.

Virtual network ID: Set the virtual network ID. It must be unique within the BACnet network.

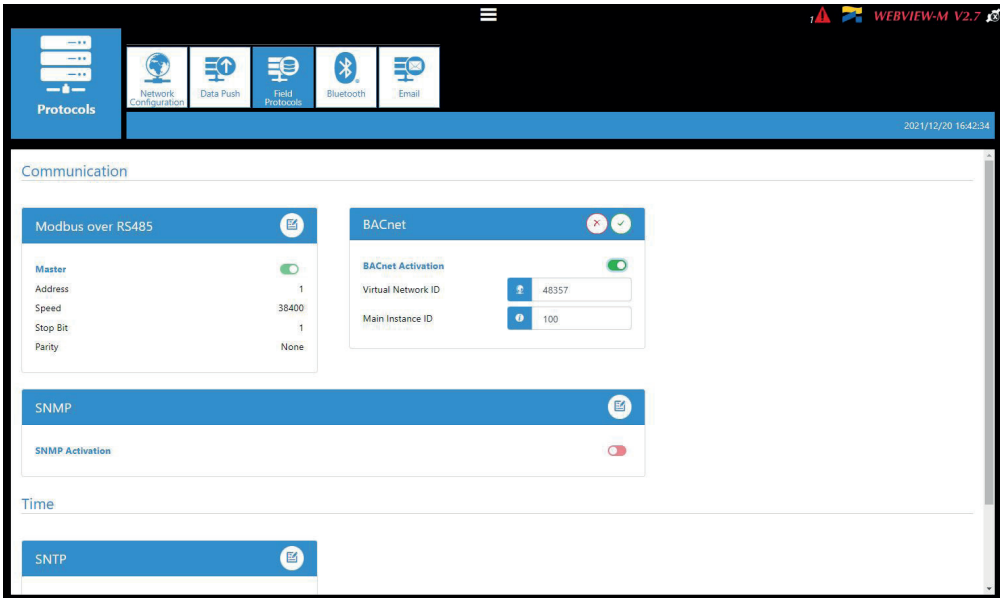
The port used by the DIRIS Digiware D-50 / D-70 for BACnet IP communication is set to 47808 (BAC0 in hexadecimal) and cannot be changed.

Annex II - 5. BACnet configuration from the embedded webserver

Click on the “Wrench” icon on the top left corner and click on “Protocols”:

Click on the “Field protocols” tab:

- **BACnet activation:** activate or disable BACnet IP communication from the D-50/D-70 display.
- **Virtual Network ID:** set the virtual Network ID of the D-50/D-70 display. It must be unique within the BACnet network.
- **Main instance ID:** set the main Instance ID (100 by default) for the D-50/D-70 display. It must be unique within the BACnet network.



ANNEX III. FTP CONFIGURATION

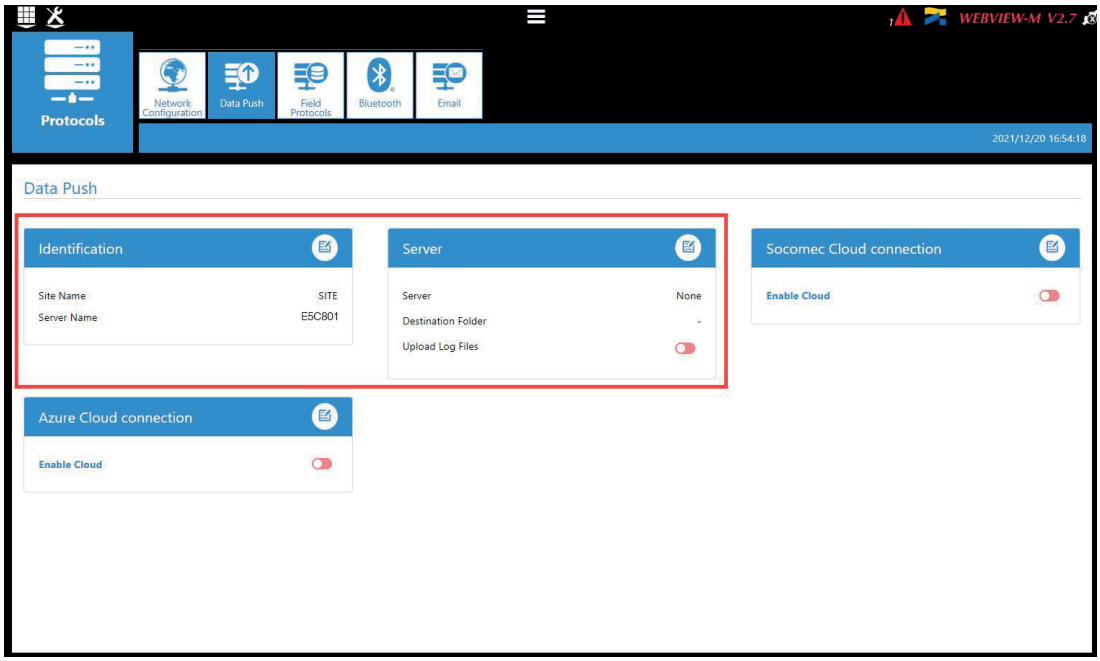
Annex III - 1. FTP file export protocol (only available with DIRIS Digiware D-70)

Measurement logs ("6.2.2. Introduction to DIRIS Digiware D-70", page 10) can be automatically exported via FTP(S).

Annex III - 1.1. FTP server activation:

Click on the “Wrench” icon on the top left corner and click on “Protocols”:

Click on “Data Push”.

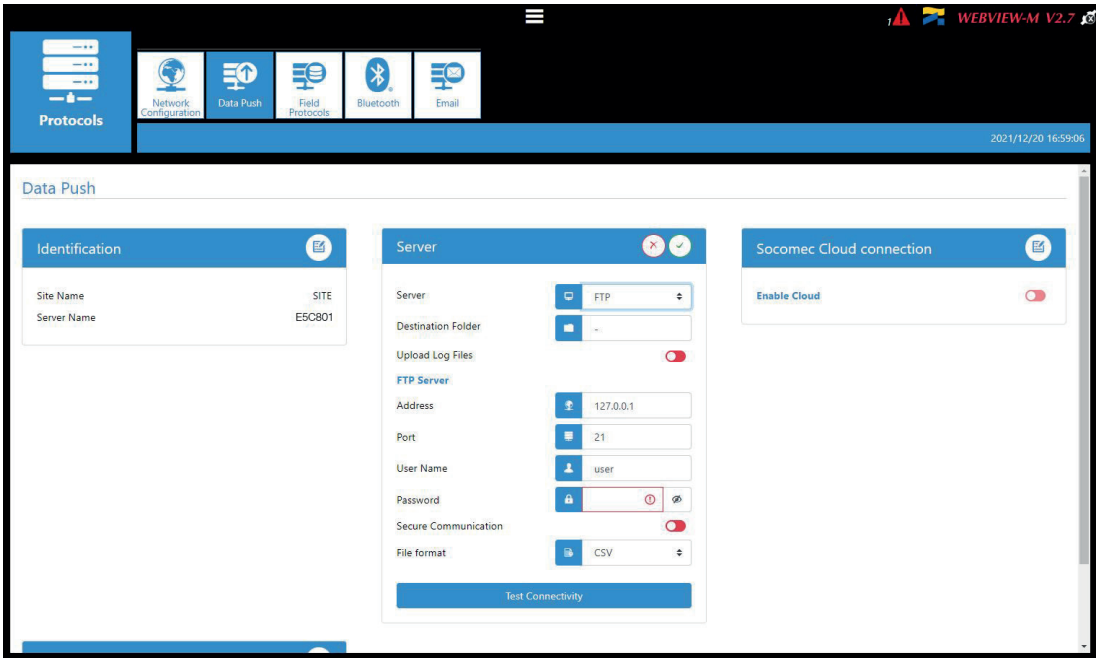


Identification part:

Site Name & Server Name: used to identify from which DIRIS Digiware D-50/D-70 the files are being exported.

The default site name is “SITE” (must be modified if the export mode is set to EMS) and the default server name corresponds to the ID shown in the bottom right corner of the home screen of the D-50/D-70 display.

Server part:



Server: activate the FTP server to enable the automatic export of data to a remote FTP server.

Destination folder: tree view of the FTP server folder in which you want to export the files.

Upload Log files: activate this to have additional information for troubleshooting in case of an export issue.

FTP Server: This contains the login details of the FTP server (standard or secure).

Address: enter the IP address of your FTP server

Port: enter the secured or non-secured port to use for the FTP export

User Name: enter the user name the access the remote server. It must be consistent with the User name configured on the FTP server.

Password: enter the password to access the remote server. It must be consistent with the passwordconfigured on the FTP server.

Secure Communication: activate or deactivate the secured export (FTPS)

File format: there are two different types of data file

- **CSV:** file in which data is in a user-friendly layout
- **EMS:** file in .csv format whose layout is more practical to integrate into an energy management software.

In EMS mode, the exported files are named according to the following:

Site name_Server name_Device name_Data type_date_time.csv

Example: if an export file is named “***socomec_E5C801_I35_LoadCurve_2017-08-15_20-00-00.csv***”, then the file was exported on August 15th, 2017 at 20:00 (8:00pm), it contains Load curves (Demand Power) from a device named I35 from a gateway whose Server name is E5C801 and Site name is socomec.

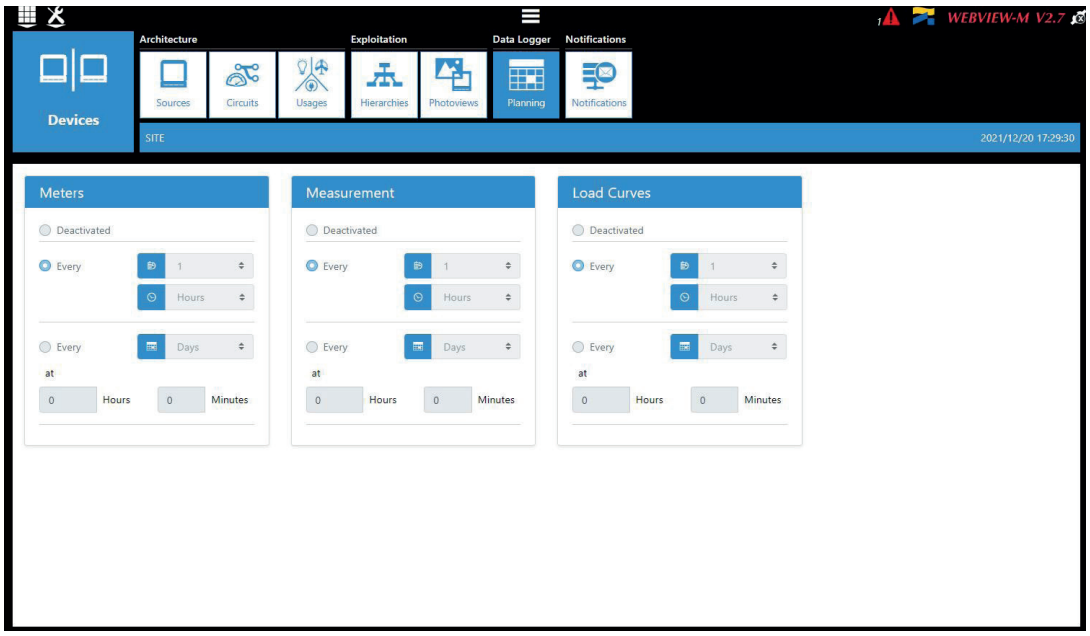
In EMS mode, the Site Name must be different from default name (“SITE”), or the “FTP error” system alarm will be triggered.

Test Connectivity: once the configuration is done, you can test the connectivity by manually exporting a test file.

Annex III - 2. FTP planning configuration

Click on “Devices”:

Click on “Planning”



Activate the type of data you want to export automatically. The DIRIS Digiware D-70 can log and export 3 types of data:

Energies Index: Ea, Er, Es etc. (Meters)

Measurement logs/trends: archived parameters U, I, F, PF etc. (Measurements)

Load curves / demand: P, Q, S etc. (Load curves)

For each data type, specify the export frequency (once an hour, once a day etc.) and at which time.

Annex III - 3. Understanding the exported .csv file in EMS mode

socomec_E5C801_I-35@4_Avg_2019-01-18_15-15-10.csv

	A	B	C	D	E	F	G	H	I	J	K	L
1	Data Type	TimeZone	Datation	Transfer Cycle (sec)	Pooling Ti	Version	Site name	Server name				
2	Avg	UTC	Local	600	N/A	1	socomec	E5C801				
3												
4	Index Key	Key	Type	Name	Fluid	Use	Coef	Unit	Path	Device Id	Index	Data Id
5	0	socomec|E5C801|14|1|ANA|100006	ANA	THD I1 of PC 1-2-3 of I-35@4	ELEC	Use2	100	%	/	14	1	100006
6	1	socomec|E5C801|14|1|ANA|100007	ANA	THD I2 of PC 1-2-3 of I-35@4	ELEC	Use2	100	%	/	14	1	100007
7	2	socomec|E5C801|14|1|ANA|100008	ANA	THD I3 of PC 1-2-3 of I-35@4	ELEC	Use2	100	%	/	14	1	100008
8	3	socomec|E5C801|14|1|ANA|10023	ANA	I1 AVG of PC 1-2-3 of I-35@4	ELEC	Use2	1000	A	/	14	1	10023
9	4	socomec|E5C801|14|1|ANA|10024	ANA	I2 AVG of PC 1-2-3 of I-35@4	ELEC	Use2	1000	A	/	14	1	10024
10	5	socomec|E5C801|14|1|ANA|10025	ANA	I3 AVG of PC 1-2-3 of I-35@4	ELEC	Use2	1000	A	/	14	1	10025
11												
12	Index Key	Date	Value	Quality								
13	0	2019-01-18T15:14:00	234	192								
14	0	2019-01-18T15:13:00	237	192								
15	0	2019-01-18T15:12:00	190	192								
16	0	2019-01-18T15:11:00	201	192								
17	0	2019-01-18T15:10:00	200	192								
18	0	2019-01-18T15:09:00	198	192								
19	0	2019-01-18T15:08:00	210	192								
20	0	2019-01-18T15:07:00	231	192								
21	0	2019-01-18T15:06:00	211	192								
22	0	2019-01-18T15:05:00	199	192								
23	1	2019-01-18T15:14:00	20001	192								
24	1	2019-01-18T15:13:00	21605	192								
25	1	2019-01-18T15:12:00	19804	192								
26	1	2019-01-18T15:11:00	20901	192								

1

2

The csv file is split into two parts:

- The part (1) in red corresponds to the header. It contains a unique key, created out of multiple parameters such as the the site and server name, the data type, the data ID, the device ID to uniquely identify each parameter that is exported.
- The part (2) in green contains the logged and time stamped measurements. Each line is identified via the simplified index key, which refers to a unique key in cells B5 through B10.

The final value for cells C13 through C26 is obtained considering the right coefficient in cells G5 through G10 along with the right unit in cells H5 through H10.

Example for line 13:

The final value for THD I1 of circuit PC1-2-3 on module I-35@4 is equal to 2.34 % on January 18th, 2019 at 15:14:00.

When integrating data into a third-party energy management or monitoring software, always refer to the unique Key in column “B”, part (1) as a unique import code and do not only use the simplified index key in column “A”, part (2).

If multiple DIRIS Digiware D-70 displays are exporting to the same folder, the simplified index key cannot differentiate them.

ANNEX IV. FIND AND ADD A SERVER'S CA (CERTIFICATE AUTHORITY) TO A DIRIS DIGIWARE D-50/D-70

Requirements:

1. An unfiltered internet connection
2. OpenSSL software installed

Instructions

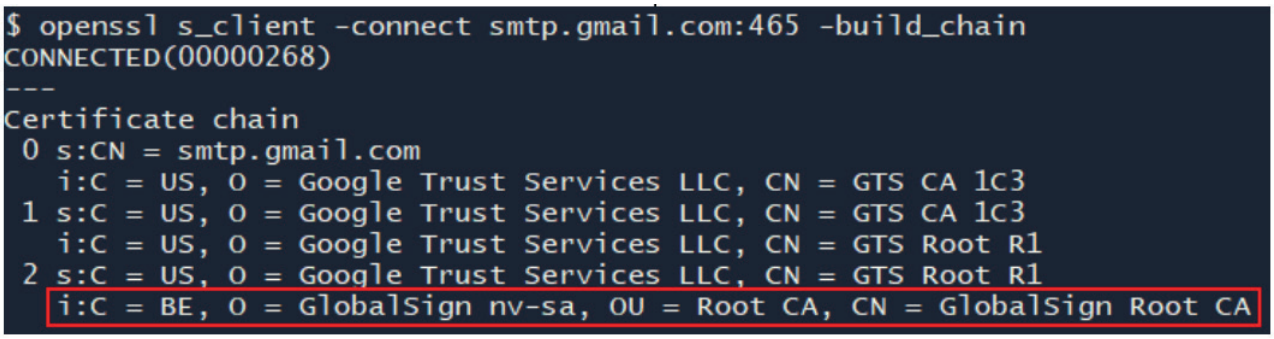
> Use the following command:

```
openssl s_client -connect <server>:<port> -build_chain
```

> Example for Gmail (SMTP):

```
openssl s_client -connect smtp.gmail.com:465 -build_chain
```

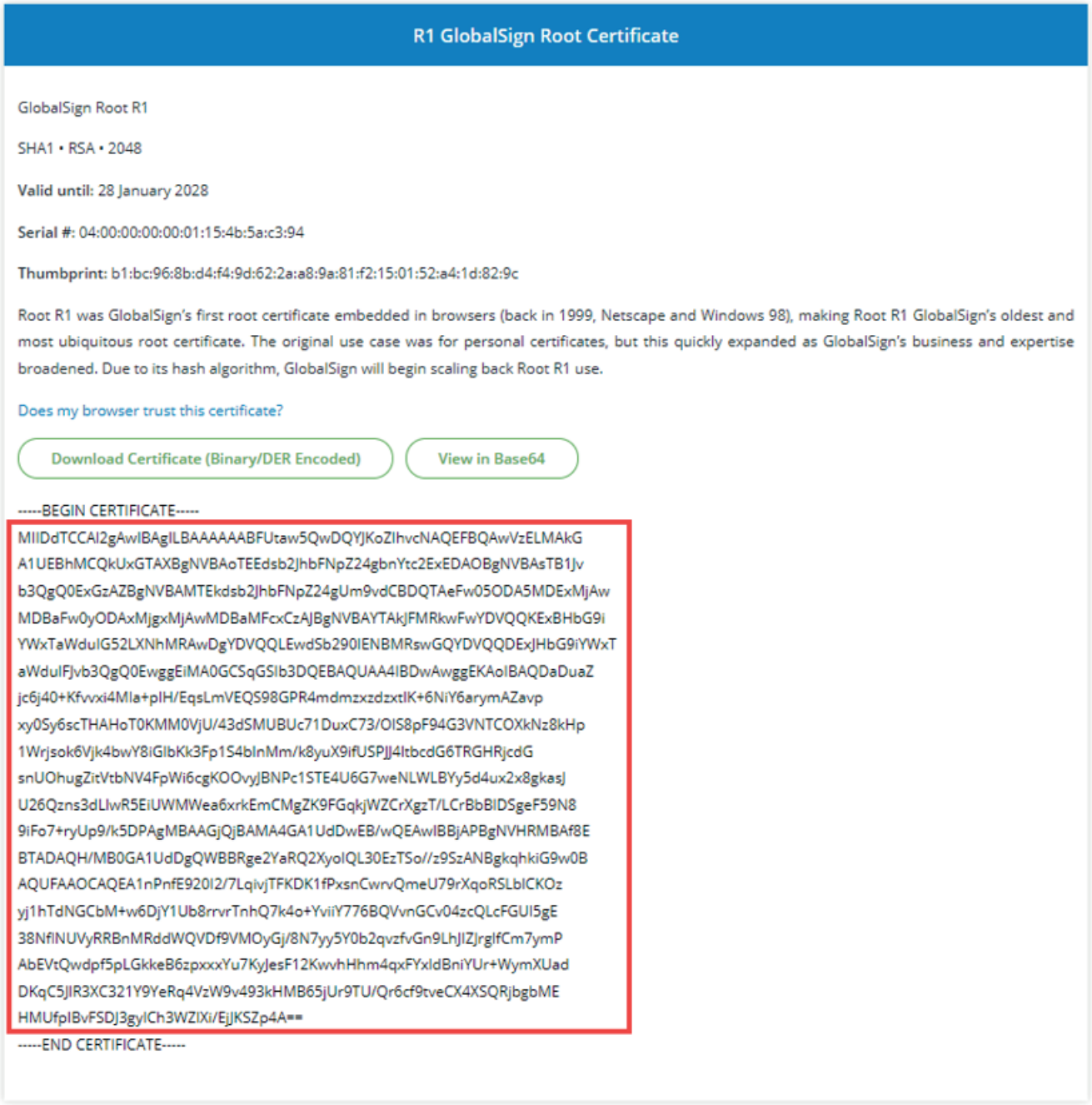
> Check the last line of the certificate chain in the command output:



> Go the corresponding company's website and find the page where you can download the root certificates.
For Gmail, GlobalSign Root CA: https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates

> Download the PEM (or Base64) certificate.

If the certificate is given as text, copy the text in between `BEGIN CERTIFICATE` and `END CERTIFICATE` into a text file and save it with a `.pem` extension, as shown in the example below:



R1 GlobalSign Root Certificate

GlobalSign Root R1

SHA1 • RSA • 2048

Valid until: 28 January 2028

Serial #: 04:00:00:00:00:01:15:4b:5a:c3:94

Thumbprint: b1:bc:96:8b:d4:f4:9d:62:2a:a8:9a:81:f2:15:01:52:a4:1d:82:9c

Root R1 was GlobalSign's first root certificate embedded in browsers (back in 1999, Netscape and Windows 98), making Root R1 GlobalSign's oldest and most ubiquitous root certificate. The original use case was for personal certificates, but this quickly expanded as GlobalSign's business and expertise broadened. Due to its hash algorithm, GlobalSign will begin scaling back Root R1 use.

Does my browser trust this certificate?

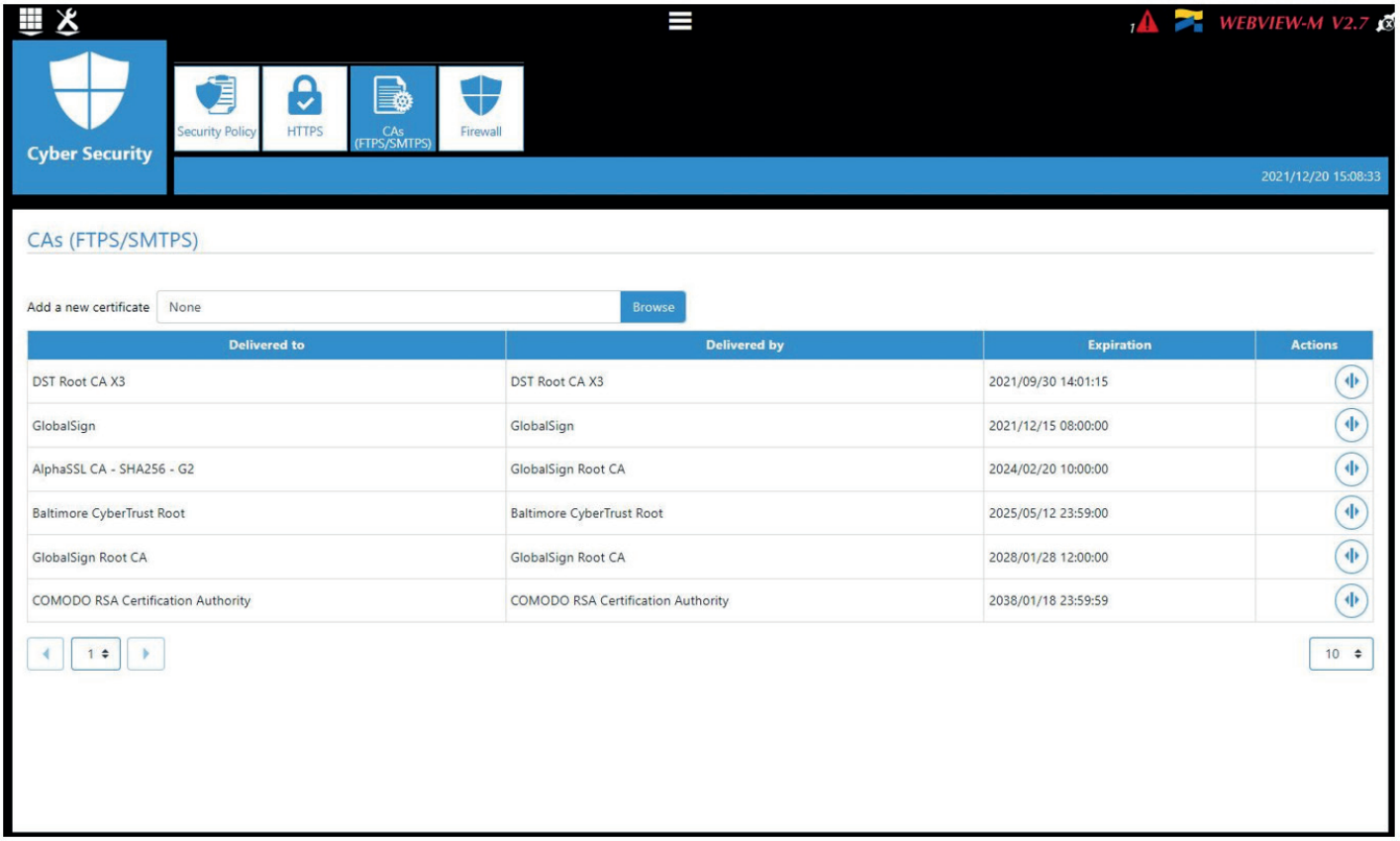
Download Certificate (Binary/DER Encoded) View in Base64

-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----

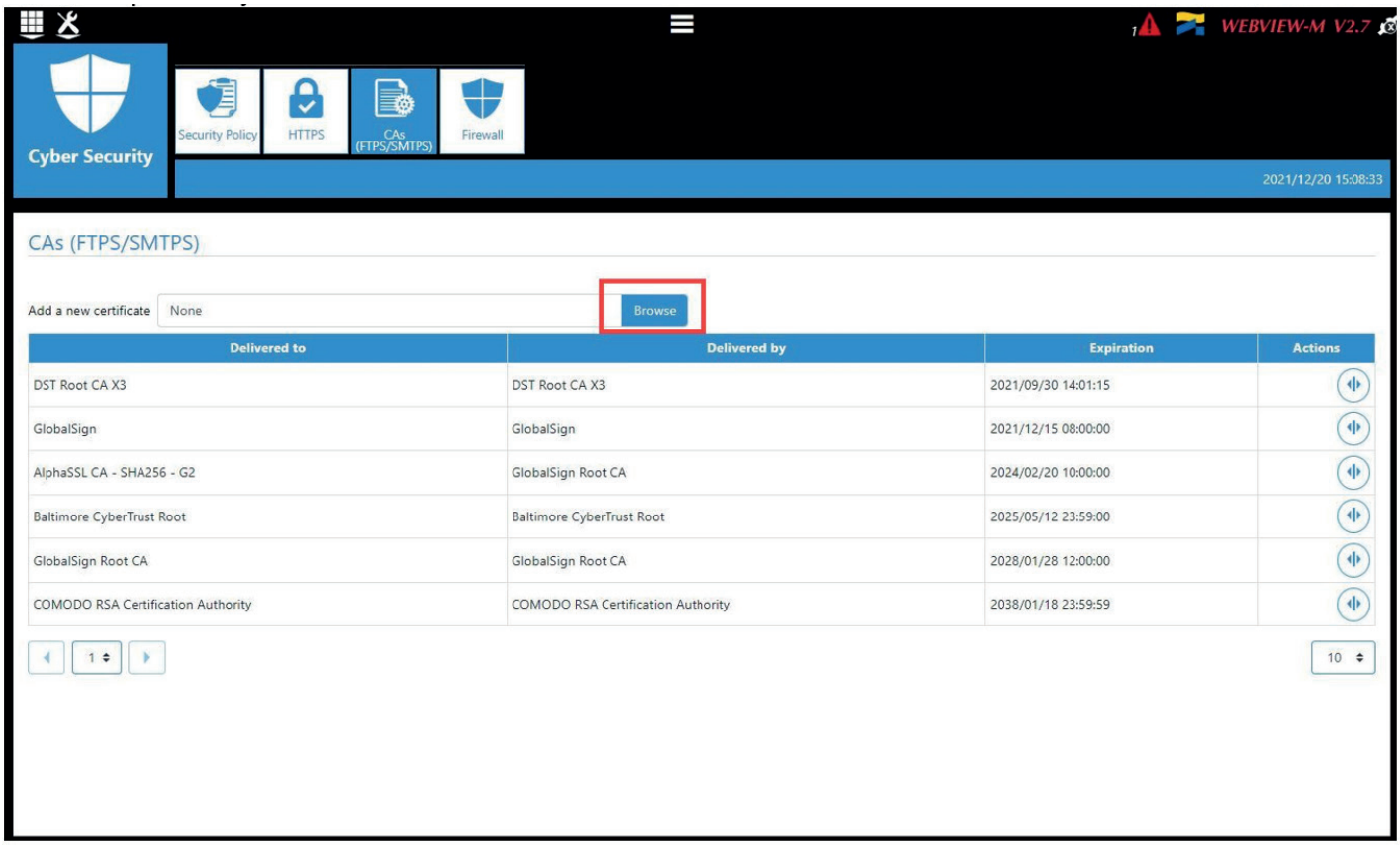
> Connect to the webserver (WEBVIEW for D-70 and WEB-CONFIG for D-50) under the Cyber Security profile.

> Go to the Cyber Security menu:

> Click on the “CAs (FTPS/SMTPS)” tab:



> Add the previously downloaded PEM file :



CORPORATE HQ CONTACT:
SOCOMEC SAS
1-4 RUE DE WESTHOUSE
67235 BENFELD, FRANCE

www.socomec.com

Non contractual document. © 2024, Socomec SAS. All rights reserved.

548088D

socomec
Innovative Power Solutions