



SITEMANAGER

USER MANUAL

EN



Table of Contents

Welcome	7
SITEMANAGER 7 – Scope of Function	8
power connection	9
integration into the network	9
Initial Configuration: The Configuration Mode 10.10.10.10	10
Preparation on SITEMANAGER 7	10
Preparations on the PC	10
The DHCP Mode	11
Information required for DHCP mode	11
Netfinder: Search for IP addresses	12
Operating Modes of the SITEMANAGER 7	13
The Configuration Mode	13
The regular operating mode	13
The Manual Mode	13
The DHCP Mode	13
The rescue mode	13
Before you start	14
Installation Examples	14
Pipe Through	15
Technical feature SITEMANAGER 7	15
Complex structures	16
Please note during installation	16
Required ports	16
First login: Predefined users	17
The Setup Wizard	17
General	18
Network	18
Date & Time	18
UPS setup	18
Review	18
Basic setting in configuration mode	18
Wired LAN and Wi-Fi	18
Special feature Initial configuration in DHCP mode	19
WLAN – The Wi-Fi interface	19
Additional basic settings	20
System contacts and location data	20
Select region and unit of measurement	20
Difference Fahrenheit / Celsius	20
Services	21
Web Server	22
SNMP	22
Modbus	22
BACnet Server	22
Serial Trace	23
UNMS & RCCMD Trap Service	23
Remote Syslog Client	23
BACS Viewer	23
Date and time	23
NTP Services and time control	23

Advanced User Management.....	24
User Roles	24
Available Users	24
The Administrator	24
The Technician.....	24
The Customer.....	24
The Guest Account.....	24
Anonymous Guest.....	25
User management under RADIUS.....	25
System Overview: The About Page.....	26
System and the Firmware version	26
Reboot and cold start	27
Cold Start	27
Warm start - Reboot The reboot button	27
Configuring system notifications.....	27
Email settings.....	27
Mail Server	28
SMTP port	28
Connection Security	28
Sender Email Address.....	28
Use email authentication, user and password.....	28
Advanced Options	28
Format.....	28
Log.....	28
Automatically send an email.....	28
Testing the mail settings.....	29
Connection refused - The most common error message:.....	29
Email Traps.....	29
Modbus	29
Modbus in devices.....	30
Modbus as a single-master protocol	30
Modbus over RS232 and Modbus over IP	30
Modbus function codes.....	30
Modbus error codes	30
Configuration of Modbus	31
Enable Modbus Slave.....	31
TCP port 502.....	31
Slave Address	31
Baud Rate	32
Parity.....	32
Stop Bit.....	32
Apply / Cancel	32
Additional documents and Modbus lists	33
SNMP Agent	33
SNMP v2 and SNMP v3	33
Setting up SNMP V2:	34
IP address	34
permission.....	34
Setting up SNMP traps	34
Trap Receivers on SITEMANAGER 7.....	35
Testing the Trap Receivers.....	35
Setting up SNMP v3.....	35
User Definition.....	36
Authentication.....	36
Setting up TRAP recipients under SNMP v3.....	36
Testing the trap settings	36

General interface settings of the COM ports	37
COM 1	37
COM 2 – Sensor	37
COM 3	37
USB port	37
Setting up the UPS	37
Settings overview	38
Model	39
power (VA)	39
load (VA)	39
holding time (min)	39
battery charging time	39
baud rate	39
cable type	39
battery installation date	39
Battery expires after	39
System Shutdown Time	40
UPS ID	40
Apply / Cancel	40
Connecting the UPS to the SITEMANAGER 7	40
Special feature: The RFC1628 UPS interface	40
Setting up the target card under SNMP v2	41
Model	41
SNMP version	41
SNMP Community	41
Apply/Cancel	41
Setting up the target card under SNMP v3	41
UPS Monitor: Checking the Settings	42
The UPS functions	42
UPS functions -working principles	42
Custom Test	43
Battery Test	43
Full Test	43
self-test	43
UPS Control settings	43
Switchable Outputs	43
System event Setup	44
Definition of a job for an event	44
Job Definition	45
Manage jobs	45
Symbols with a clear function	45
Symbols with dual function:	45
Setting up a job	46
Available Jobs	46
Special features of the UPS Shutdown job	47
Definition of a UPS Shutdown	47
Time to turn off in seconds	47
Time to turn on in seconds	47
Type	47
Using the UPS Shutdown job	47
Search and display jobs	47
Event: contains	47
Jobs	47
Job Definition: Selectable time windows:	48
Time management of jobs in relation to the UPS	48
Add Multiple Jobs	49
Deleting jobs	50
Assign jobs to counter events	50

Custom Thresholds.....	51
Difference between Warning and Alarm Levels	51
Example configuration: UPS Temperature.....	51
Setting the alarm levels	52
Example excerpt: Custom Thresholds	53
Example scenario: Custom Thresholds	54
RCCMD	54
What is RCCMD.....	54
Configuring RCCMD.....	55
Setting up an RCCMD job	55
Setting the IP address for RCCMD	56
broadcast	56
Limiting to IP addresses	56
Port	56
Define time for RCCMD	56
The RCCMD commands	57
The RCCMD Shutdown	57
The RCCMD Message.....	57
Configuring an RCCMD Execute	57
The RCCMD Traps.....	58
SITEMANAGER 7 - specific devices and sensors	59
The cable comb.....	59
Sensors And Devices	59
SITEMANAGER 7 Sensor Setup	60
connection of the sensors.....	60
Using the analog and digital connections	61
Analog sensors	61
definition of alarm thresholds	61
sensor area	61
pre-alarm and alarm	62
The digital inputs	62
name	63
NC Contact.....	63
Active	63
SITEMANAGER 7 Outputs	63
name	63
switching on.....	63
delay	63
Advanced Monitoring.....	63
Digital Output	63
Analog Alarms.....	63
The system status LEDs.....	64
Special feature: Power LED.....	64
SITEMANAGER 7: Assign an event to sensors	64
Assigning system events to analog inputs	64
Assigning system events to digital inputs.....	65
Special feature of JOB AUX:	65
scheduler	66
web server	67
Enabling / Disabling the Web Interface.....	67

Web access configuration	67
Overview of the basic settings	67
HTTP port.....	68
HTTPs port.....	68
Force HTTPs	68
HTTP refresh time	68
Use simple monitor.....	68
Automatic logout.....	69
Certificate management / https – access	69
Diagnosis: Status bar and LEDs	69
log files	70
The Eventlog Files.....	70
The Datalog.....	72
Datalog Chart – Graphical representation.....	73
Overview	73
calendar function	73
zoom function.....	74
Toolbox.....	74
reboot / cold start.....	74
Tracer	74
COM 1/ UPS.....	74
COM 2 / GSM modem	74
COM 3 / AUX.....	75
network scan.....	75
Network scan: evaluation of the data.....	76
Deleting log files.....	76
Corporate Identity – Replacing the OEM Logo.....	77
Quick Guide: Replace Logo.....	77
Data backup and firmware updates	78
Step 1: Back up the data	78
Step 2: Restore data	78
firmware updates.....	78
Reset to factory settings	79
Reset network to factory settings	79
Changing the OEM firmware	79
The current firmware	79
When nothing else works – The Rescue System	80
Start the rescue system.....	81
FAQ – Frequently Asked Questions.....	82
Appendix: Hardware Layout and Connections CS141 / SITEMANAGER 7	84
Copyright Statement on Intellectual Property and Handling of Confidential Information	91

Welcome

We thank you for your trust in the extensive CS141 WEBMANAGER product family – the reliable solution in critical resource management.

The CS141 was developed specifically for use in critical resource management. Since CS141 was developed as a fully-fledged and independent manager, its task is not limited to collecting and forwarding information, but also fulfills numerous tasks in measurement, control and regulation technology in the area of critical resource management. Another core function is message management:

The CS141 can not only answer requests from higher-level systems, but also independently inform responsible personnel in an emergency and initiate emergency measures based on predetermined parameters. The CS141 can independently activate emergency systems, shut down servers and workstations and restart them under predetermined conditions. In addition to standard technologies such as SNMP and Modbus, the CS141 exclusively uses the powerful RCCMD software solution, which can even implement the emergency behavior of complex, fully virtualized server landscapes.

Even more flexibility thanks to RFC1628

Thanks to the new RFC1628 compliant UPS interface, you can use the CS141 to query any UPS that supports this standard via the existing LAN and display the current status natively. If you are using a UPS whose interfaces are unexpectedly not compatible with the CS141, you can use this function to establish compatibility with little effort and cost and thus use the powerful and reliable GENEREX products such as the RCCMD developed by GENEREX.

Note:

Since the CS141 web manager can act as an independent manager, it can be used flexibly in many areas, even outside of the functionality described in this manual. This manual therefore describes the basic functionality implemented in connection with UPS systems. The enormous flexibility and the ability to communicate with higher- and lower-level systems in real time.

As individual as your network

SITEMANAGER 7 adapts flexibly to your specific network requirements. This manual describes all the menus you may encounter when configuring the following devices:

- SITEMANAGER 7

Please note that although there is a lot of overlap, for technical reasons not all accessories are fully cross-compatible, even if the external connector configuration would fit.

These include, for example:

- Additional sensors and devices

This includes, for example, the GSM modem, analog sensors and the Sensor Manager II or the Relay Board CON_R_AUX / 4 or the BACS version GX_R_AUX

- AUX devices and BACS upgradeability

In addition to switchable outputs, SITEMANAGER 7 offers analog and digital inputs, either via the terminal block or the analog sensor inputs, as well as full BACS functionality

The heart of SITEMANAGER 7 is the powerful CS141 used:

Unlike the CS141, COM port 1 is the interface to the UPS and cannot be used for sensors. The menus differ from the CS141 standard interface, and some functionalities are different.

If your device does not offer a hardware layout, the corresponding menus will not be available within the software.

SITEMANAGER 7 – Scope of Function*Hardware:*

The SITEMANAGER 7 is specially designed for use in standard server racks. Accessories can be attached nearby as required, for example using standardized DIN rails. SITEMANAGER 7 offers the option of communicating with the UPS as an SNMP adapter directly with an RS-232 interface or via the RFC1628 smart UPS interface via LAN and acting as a full-fledged web manager.

This includes:

-SNMP and SNMP traps:

SNMP (Simple Network Management Protocol) is an Internet standard protocol for monitoring systems over IP networks. The protocol is defined and standardized in RFC specifications. UPS systems generally use the RFC 1628 specification as the MIB, which defines UPS-specific devices. Therefore, it is usually not necessary to insert a separate MIB into the SNMP software.

The SITEMANAGER 7 is designed for numerous tasks. For example, the power supply and battery status of a UPS can be monitored by an SNMP management station, door contacts or access controls can be activated, etc. The current switching states can be switched both time-controlled and reactively in the form of switching chains including feedback. A specially defined message can be sent automatically for each switching state.

-Remote control of UPS systems:

This function can be used, for example, to switch the UPS to bypass (manufacturer dependent); this is triggered by a corresponding command via the Network Management Station or by the UPS management software for the web that belongs to the UPS.

-Multiple shutdowns via RCCMD:

A SITEMANAGER 7 can initiate a network shutdown with all RCCMD modules of the UPS management software. A TCP/IP-based RCCMD transmission signal is sent to all configured RCCMD clients. This can also trigger a shutdown on an unlimited number of computers, regardless of their operating system. RCCMD is an optional component of the UPS management software. UPS management software and RCCMD licenses are available from your UPS specialist dealer.

-Time-accurate log file:

A SITEMANAGER 7 provides a unique set of log files to accurately record events and alarms. This log file is accessible via UNMS, UPSMAN, Web GUI and FTP. Exporting as a CSV file allows easy archiving for later diagnosis

-Communication via email:

The CS141 models come with a standard Simple Mail Transfer Protocol (SMTP) compatible email client that can automatically send emails when events occur.

-Integration into Network Management Systems

The SNMP adapter is compatible with all common network management systems. All SNMP systems that allow the compilation of a MIB - or already contain the Management Information Base (MIB) / Request for Comment 1628 (RFC) for UPS systems - can be operated with the adapter. Potential-free contacts can also be used to interact with higher- and lower-level monitoring and management systems.

-Modern web technology for easy configuration:

The models in the CS141 product family have a web server that displays all the information about the device. UPSView can be used to display a graphical representation of the data. The web interface can be accessed using a standard web browser.

-Modbus support

The SITEMANAGER 7 offers a connection to existing Modbus infrastructures with Modbus over IP as standard.

-RS-232 / Pipe-through:

The SNMP adapter type CS141 can output the UPS protocol, which is read via COM1, directly to COM2. This makes it possible to connect additional software/hardware to the UPS without using additional distribution hardware (RS-232 multiplexer).

- UPSTCP:

The most common way to communicate with the CS141 adapter is TCP. The CS141 includes UPSTCP, which provides you with a complete API interface to integrate your adapter into the network. This interface is supplied to software manufacturers on request to enable their own integration. All other users use TCP for access via a web interface (UPSVIEW, UPSMON, UNMS) or SNMP or MODBUS over IP.

power connection



The SITEMANAGER 7 provides flexibility in connecting to any power grid:

As a standard, it is supplied with a 24V/1.5A power supply. The connection terminal is coded to prevent polarity reversal.

Under certain conditions it may be necessary or advisable to use an alternative power source.



For this reason, the connector is designed to be modular. The SITEMANAGER 7 adapts dynamically to the input voltage:

Minimum: 18 VDC

Maximum: 75 VDC

When connecting your own power sources, please ensure the polarity is correct to avoid damage to the device.

integration into the network

All models of the CS141 family are configured exclusively via the adapter's specially developed web interface. To facilitate initial configuration or quick on-site intervention, the CS141 family's web manager is preset to the IP address 10.10.10.10 on the hardware side:



You can recognize this preset when the slide switch on the front is in the middle position. The only exception here is the CS141 MINI, which uses dip switches on the circuit board due to its more compact design. The middle position or both dip switches on off activates the so-called configuration mode. In this mode, some functions such as entering the IP address data can be configured, but are only available once you switch to the regular operating mode.

The following table shows the possibilities of the regular operating modes in standard operation:

<p>Switch button to center position: On startup, the device boots into configuration mode. The hard-coded default IP address 10.10.10.10 is active.</p>	
<p>Switch button to right position: Exclusive IP addressing via DHCP is set. All IP-Settings are blocked by hardware setting. Check the MAC address of your device to identify the IP address in the DHCP server table.</p>	
<p>Switch button to left position: Full Control by Menu Setup settings. Choose between Manual IP Setup and DHCP mode. All configuration can be set and changed by an administrator without reboot.</p>	

[Initial Configuration: The Configuration Mode 10.10.10.10](#)

[Preparation on SITEMANAGER 7](#)

Before commissioning, move the slide switch on the back to the middle position. After the boot process, the manager is in configuration mode and can be reached at the hardware-preset IP address 10.10.10.10.

Note:

Changing the mode using the hardware switches requires a reboot. You can perform the reboot in two ways:

- By briefly removing the power supply (hardware reset)
- Using the restart function in the Tools menu (Software Reset)

This process does not apply to the connected UPS – this continues to run independently of the web manager.

[Preparations on the PC](#)

After the system starts in configuration mode, the web manager can be found physically in the following network:

IP address 10.10.10.10
Subnet mask: 255.255.255.0

The recommended network settings for the client PC to set up are:

IP address 10.10.10.11
subnet mask 255.255.255.0
Gateway 10.10.10.11(will then be automatically hidden)
DNS empty

Check the settings of your service computer by opening a console and entering the command `PING 10.10.10.10` if the settings are correct, the CS141 will respond accordingly:

```
C:\Users\Gunnar>ping 10.10.10.10

Ping wird ausgeführt für 10.10.10.10 mit 32 Bytes Daten:
Antwort von 10.10.10.10: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 10.10.10.10:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    <0% Verlust>,
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

C:\Users\Gunnar>
```

You can then open a web browser and access the SITEMANAGER 7 web interface directly via the request <http://10.10.10.10> and start the configuration.

Add a route

Within larger installations with clearly defined domain joins, it can be helpful to temporarily use a route.

In this case, it must be ensured that the SITEMANAGER 7 is in the same network segment and can therefore be accessed directly.

Example: Add a route on a Windows PC:

1. Open the command console "cmd" as administrator
This step is important because Windows requires a user with local administrative rights to add a route.
2. Enter the following command: `route add 10.10.10.10 <your IP address>`
In this case, Windows responds with OK

```
C:\Windows\system32>route add 10.10.10.10 192.168.200.17
OK!
```

To check the newly created route, enter the route print command:

```
IPv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel   Netzwerkmaske   Gateway         Schnittstelle   Metrik
  0.0.0.0        0.0.0.0         192.168.200.1  192.168.200.17  20
  10.10.10.10    255.255.255.255 Auf Verbindung  192.168.200.17  21
  127.0.0.0      255.0.0.0       Auf Verbindung  127.0.0.1       306
  127.0.0.1      255.255.255.255 Auf Verbindung  127.0.0.1       306
  127.255.255.255 255.255.255.255 Auf Verbindung  127.0.0.1       306
  192.168.200.0   255.255.255.0   Auf Verbindung  192.168.200.17  276
```

You can find the entry 10.10.10.10 under Active Routes. As an additional test, you can use the command `ping 10.10.10.10` to check whether the web manager is responding as expected.

Note:

In configuration mode, you can only operate one CS141 with the preset IP address 10.10.10.10. If you want to connect several devices at the same time, there will be a network conflict in configuration mode.

The DHCP Mode

Since the models of the CS141 family can fulfil a large number of functions due to their flexibility, it is a completely realistic scenario that you will have to operate several devices simultaneously within an installation and that a fixed IP address cannot be assigned for the time being.

To activate DHCP mode, slide the slide switch to the right, towards the outer edge of the CS141. For the CS141 Mini, leave dip switch 1 OFF and move dip switch 2 to ON. The next time you restart, the web manager will boot in DHCP mode according to the hardware configuration and obtain an IP address from your network.

Information required for DHCP mode

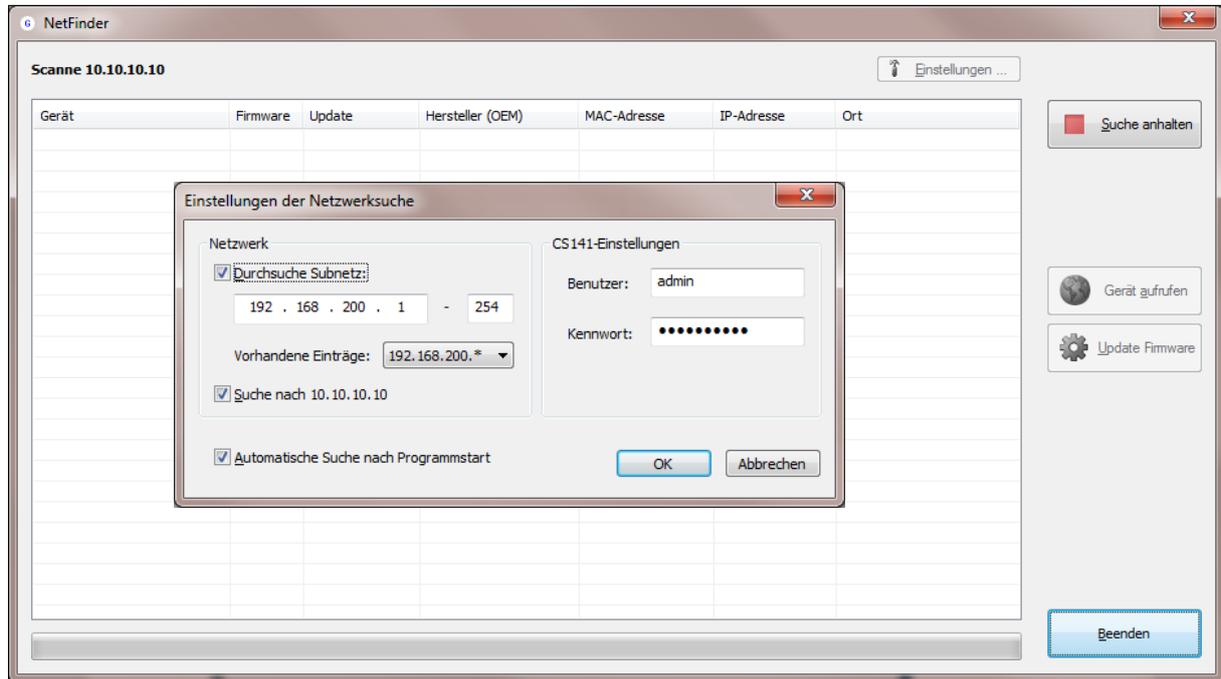
To be able to clearly identify the devices after the hardware installation, make a note of the MAC address and the installation location before installation, which can be found on a sticker on every web manager of the CS141 family:



Make sure that a suitable DHCP server is available for this operating mode, otherwise the automatic retrieval of the IP address data is not possible.

Netfinder: Search for IP addresses

To read the IP addresses, use the Netfinder tool, which is available on the support CD and for download at www.generex.de. The Netfinder is a useful software tool that can display all CS141 and SITEMANAGER 7 devices accessible in a network.



The default search always refers to the network segment in which the service computer is located. To scan other networks and subnets of CS121 or CS141 installations, specify the corresponding IP address ranges.

Gerät	Firmware	Update	Hersteller (OEM)	MAC-Adresse	IP-Adresse	Ort
CS141L	1.61	Nicht nötig	ABB (36)	00-30-d6-16-1d-e7	192.168.222.106	
CS141BSC	1.60	Nicht nötig	Online (4)	00-30-d6-13-3d-eb	192.168.222.104	
CS141R_2	1.60	Nicht nötig	Piller (3)	00-30-d6-12-6e-c7	192.168.222.107	
CS141L	1.56	Verfügbar (1.58)	ABB (36)	00-30-d6-12-60-70	192.168.222.108	
CS141LM	1.60	Nicht nötig	AMG Accent Monitorin...	00-30-d6-12-0f-2b	192.168.222.110	
CS141SC	1.60	Nicht nötig	Salicru (82)	00-30-d6-16-bb-f3	192.168.222.112	
BACSKIT_B4	1.60	Nicht nötig	Generex (12)	00-30-d6-12-60-61	192.168.222.114	
BACS II Webmanager BUDGET	5.62	Nicht nötig	UPS LTD (84)	00-03-05-18-77-6A	192.168.222.113	
BACS II Webmanager BUDGET	5.62	Nicht nötig	Hoppecke (91)	00-03-05-18-59-7A	192.168.222.103	
CS131 16MB	5.62	Nicht nötig	ALTERNAC (92)	00-03-05-18-6A-A4	192.168.222.111	GENEREX Hamburg Garage
CS141BSC	1.60	Nicht nötig	CET (81)	00-30-d6-12-6f-9d	192.168.222.119	
CS131 16MB	5.34	Verfügbar (5.62)	Generex (12)	00-03-05-18-96-A2	192.168.222.123	

The Netfinder gives you a detailed overview of all devices in the network and allows quick and easy access to the web console of the corresponding manager.

Note:

In DHCP mode, the IP address can change sporadically depending on the network configuration. Web managers that are to be monitored by a higher-level system such as the UNMS II should therefore be given a fixed IP address. If this is not the case, you can use Netfinder to find all devices again.

Operating Modes of the SITEMANAGER 7

Difference between configuration, rescue and operating mode

All models in the CS141 family are configured exclusively via an intuitive web interface. The web managers offer five valid operating states that differ fundamentally from one another.

The Configuration Mode

In this case the slide switch is in the middle position.



The configuration mode is the mode in which the manager is delivered by default. In this mode, the web manager can be reached via a hardware-preset IP address 10.10.10.10 and allows all system-relevant settings.

Since the manager generally uses the preset IP address in configuration mode, you can also import data backups here and adjust them after the restart.

The regular operating mode

The slide switch is in the left or right position depending on the setting. Depending on the setting, the CS141 is in DHCP mode or manual mode.

The Manual Mode



In manual mode, you specify the IP address data: Please note that incorrect settings may lead to address conflicts in the network, or the settings made may not work. The data required for manual mode can be obtained from the local administrator.

Note:

In manual mode, the data is entered "by hand" and thus permanently assigned: The SITEMANAGER 7 will use this data to make itself known in the network. If an IP address conflict occurs because the IP address was assigned twice, you can switch back to configuration mode at any time and reach the web manager under the preset IP address 10.10.10.10

The DHCP Mode



In DHCP mode, the SITEMANAGER 7 automatically adopts settings assigned by a server and uses these for the IP address settings. The web server manages the IP address data. After the start-up process, the web manager can be found using the Netfinder tool.

Note:

As a rule, IP addresses assigned via DHCP are only assigned for specific time windows. DHCP clients therefore ask after 50% of this time window whether the IP address is still valid or whether another one has been assigned. How statically the DHCP server assigns IP addresses is a decision made by the system administrator. It can therefore happen that a different IP address is assigned just by restarting.

When choosing the operating mode, the function of the SITEMANAGER 7 within the network should be considered:

If the web manager is to be an active element within shutdown solutions or in connection with higher-level monitoring structures, a manually assigned IP address is useful, as an authenticated IP address must be configured. Another advantage is that the web manager can start autonomously in an emergency, even without an existing DHCP server, thanks to preconfigured IP addresses.

The rescue mode

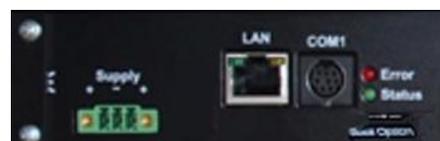
In this mode, an additional jumper is set, and the slide switch is in the middle position:

Each web manager has two ROMs that can be booted from. The current firmware and the last state before the firmware update, including the configuration file, are stored here. If the web manager is put into rescue mode, the logic starts from the last known status and is initially fully operational again but shows a note in the general system information that the web manager is in rescue mode.

The rescue mode represents an emergency operation and is intended, for example, to repeat a faulty flash process.

To activate emergency mode:

1. Open the device and look for the small circuit board with the network interface – since the circuit board itself does not need to be removed, you can use the back of the web manager as a guide:



- On the small, screwed circuit board you will find a ribbon data cable and directly below it there is an open jumper. Close this jumper and reconnect the power adapter:



The web manager will automatically start in rescue mode. For more information about the Rescue Mode, refer to the chapter:

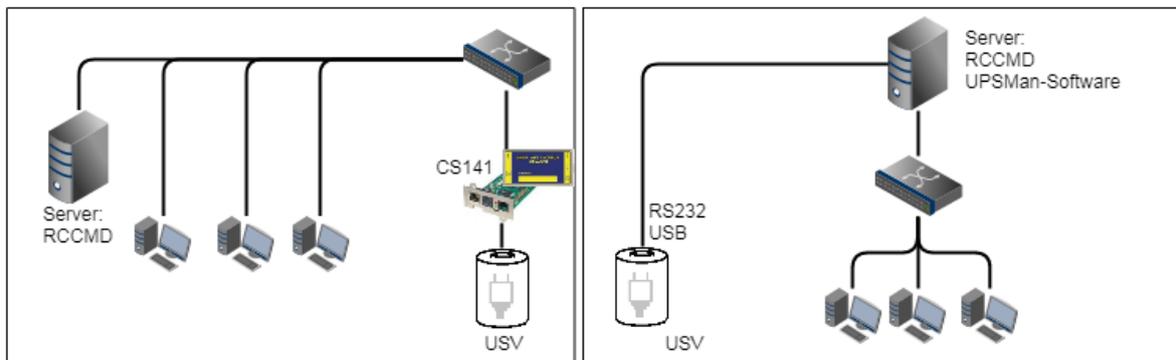
[When nothing else works – the rescue system](#)

Before you start ...

[Installation Examples](#)

The CS141 was specifically designed as a web manager to give you maximum freedom of action during installation in order to meet the ever-increasing demands and the resulting central role of modern UPS systems within the general power supply:

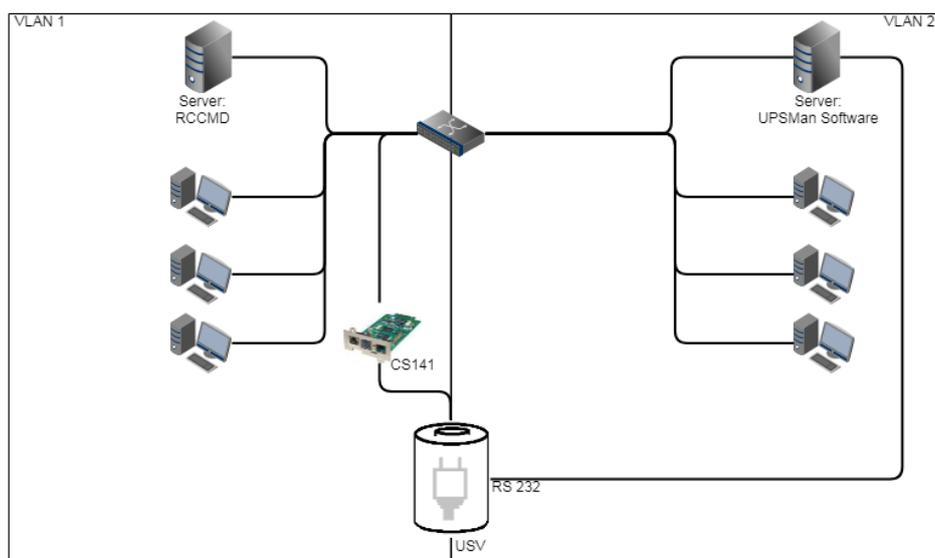
The simple case:



The UPS should protect the server until it has been shut down. The complete shutdown routine is controlled by the CS141, as this is a fully-fledged manager that can act independently. As an alternative to the CS141, the shutdown routine can also be initiated using the UPSMan software. Additional stations and servers only require another RCCMD license.

Two separate networks

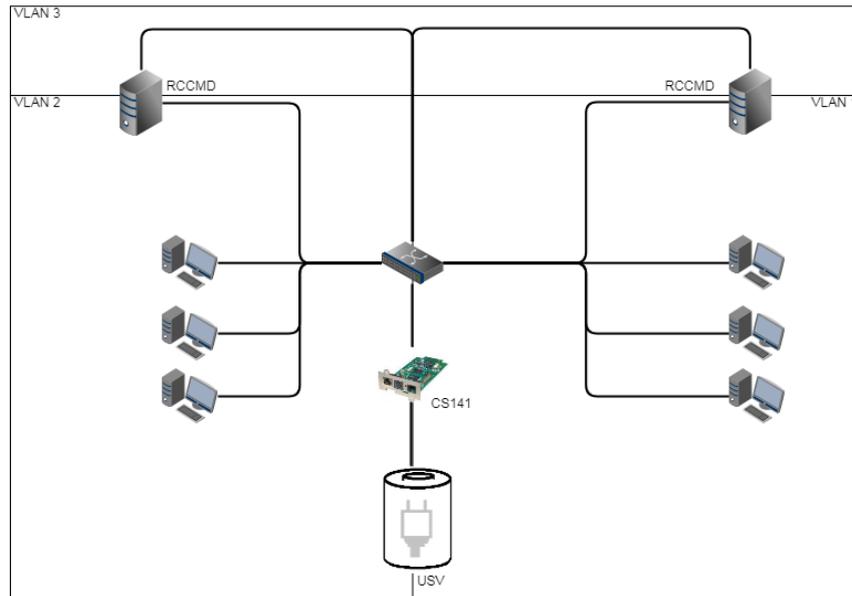
Things become more difficult when two servers are to be connected via separate networks that are protected by the same UPS:



The UPS is a central component of vital importance. Since the VLANs are physically separated, only the server in a LAN can be supplied via the CS141. The UPSMan software provides a simple solution here, as it can communicate with the UPS via the

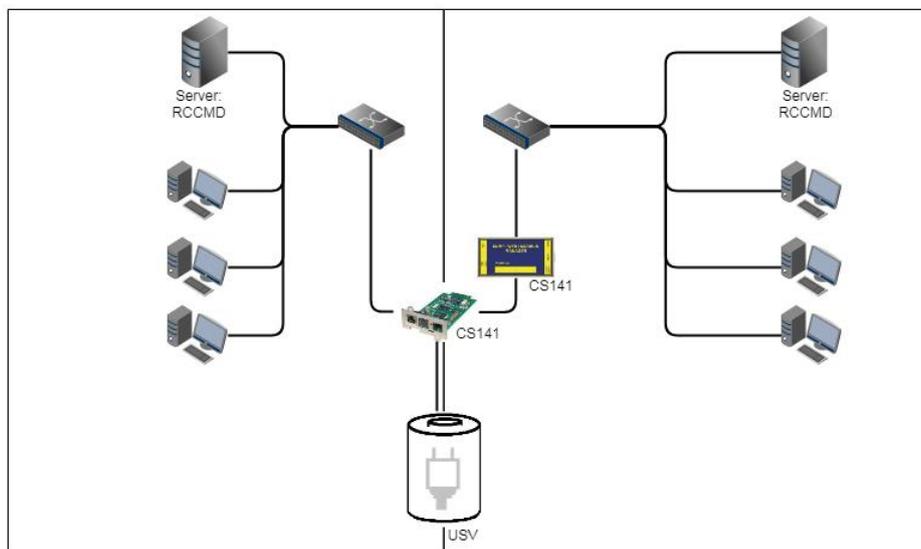
server's COM port and offers the same functionality as the CS141 and also supports RCCMD. VLAN 2 represents a "software only" solution that does not require a CS141 as additional hardware.

If this RS232 connection is not available, you only need servers with 2 network cards each:



If you have a free RS232 interface, this solution allows you to use the interface for the next independent network, provided that the UPS supports parallel operation of slot and RS232.

Pipe Through



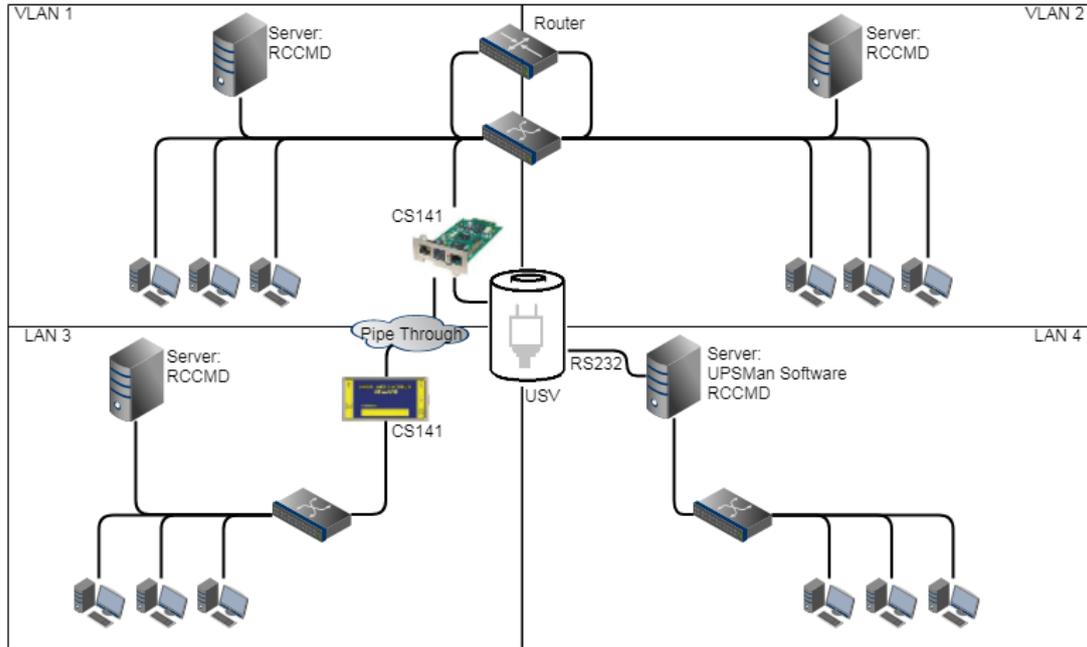
In some companies, physical separation of the networks is unavoidable, but the UPS does not offer the option of operating RS232 and slot in parallel. In this case, the signal can be looped through 1:1 using the pipe-through function, so that two CS141s can perform the same function together. The different CS141 versions can be combined as desired. The combination CS141/UPSMan software is also possible.

Technical feature SITEMANAGER 7

The SITEMANAGER 7 uses a mini-DIN connector as the UPS connection COM1. This means that the pipe-through function is generally supported, but for technical reasons the SITEMANAGER 7 can only be used as the last device in the pipe-through chain.



Complex structures



In this example, VLAN 1 and VLAN 2 were logically linked with a router so that a CS141 can pass RCCMD commands to the servers in both VLAN 1 and VLAN 2. The Pipe Through function simultaneously enables the same signal to be sent to an independent LAN 3, in which another CS141 as manager receives the same information about the UPS status. LAN 4 is connected to the UPSMan software via the RS232 interface. In this example, you get two connected and two physically isolated networks that share a central power supply and are informed about the exact status of the UPS at all times.

Note:

The UPSMan software also supports communication via USB – if your UPS supports pair-allelic operation, you can also connect individual servers with the UPSMan software installed to the UPS via USB.

Please note during installation

For technical reasons, SITEMANAGER 7 is subject to limitations when it comes to nested network structures:

In an installation that requires pipe through, they can only be integrated as a second device, since the COM port required to loop through UPS signals is already there.

One way to circumvent this would be to specifically use the RFC 1628 – UPS interface in conjunction with defined routing.

Required ports

The CS141 requires a number of ports that must be open or available. Some ports are standard ports within your computer, others must be opened or made available exclusively for the CS141. Please check on site whether the following ports are available or open:

Service	Port	Style	Service	Port	Style
ECHO	7	TCP	SNMP	161	UDP
ECHO	7	UDP	SNMP trap	162	UDP
WOL	9	UDP	Time (rfc868)	37	TCP
FTP data	20	TCP	Time (NTP)	123	TCP
FTP	21	TCP	RCCMD	6003	TCP
telnet	23	TCP	RCCMD Broadcast	6003	UDP
SMTP	25	TCP	UPSMon	5769	TCP
HTTP	80	TCP	Modbus / IP	502	TCP
HTTPs	43	TCP			

Note:

This user manual covers all menus that you may encounter when configuring a CS141. The basis of this documentation is firmware 2.22 and subsequent versions. If you cannot find a menu, there may be several reasons:

The CS141 you are using does not offer this function
 The firmware version you are using is older and the feature is therefore not yet available
 The menu is present, but has shifted due to the ongoing development process

First login: Predefined users

After you have entered the IP address, the CS141 will display its web interface and ask you to enter a password:

User: admin	Password: cs141-snmp	...System Administrator, full menu
User: engineer	Password: engineer	...Technician, administrative menus locked
User: customer	Password: customer	... customer, access limited to log files and screens
User: guest	Password: guest	... guest access, only status displays visible

Important: During the initial setup, only the user “admin” is activated! Additional users must be authorized or set up exclusively.

To begin the initial configuration, log in with the user admin and the default password cs141-snmp:

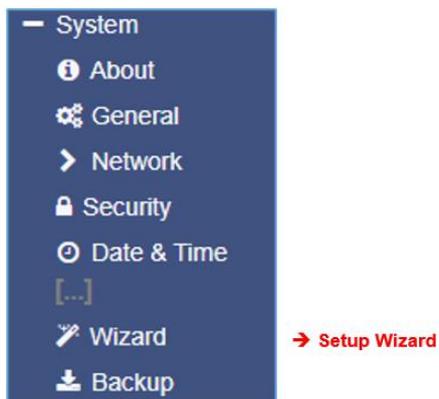
Note:

Modern web browsers are designed to display websites as quickly as possible. Among other things, techniques are used to load images, pages and query forms into a cache so that they can be displayed again later. This can sometimes lead to a display or presentation error, or certain menus no longer appear to work:

If these phenomena occur, refresh the browser display with CTRL + F5 or clear the cache of the web browser you are using and deactivate additionally installed tools and add-ons that could hinder the display.

[The Setup Wizard](#)

For this configuration step you need the following menu:



When login to any CS141-based product for the first time, the welcome screen with the wizard starts automatically:

The following basic settings can be made:

General

Provide basic information about location, contact person, point of contact, system language and temperature scale.

Network

Specify the network configuration – The necessary data can be obtained from the local administrator.

Date & Time

Provide basic information about the date, time and time server.

UPS setup

Specify the UPS to which the CS141 is to be connected and operated.

Review

Check all data again before you click Finish to end the configuration process and the CS141 takes over the configuration.

Note:

The Setup Wizard simply summarizes basic settings and offers a quick and convenient solution for making or changing basic settings for quick commissioning of the CS141. If you want to carry out the configuration completely manually, press Cancel here - you can restart the Setup Wizard in the configuration menu at any time.

Basic setting in configuration mode

For this configuration step, you need the following menu:



Wired LAN and Wi-Fi

Most settings can be made in configuration mode, but tests and forwarding functions are often not possible because the web manager is set to the IP address 10.10.10.10 on the hardware side. It is therefore recommended that you make the basic settings in configuration mode and then switch to manual operating mode. To integrate the web manager into your network, open the Network menu:

Configure	Active
IP-Adresse: 192.168.0.100	IP-Adresse: 10.10.10.10
Subnetzmaske: 255.255.255.0	Subnetzmaske: 255.255.255.0
Standard Gateway: 192.168.0.1	Standard Gateway: 0.0.0.0
DNS Server: 192.168.0.1	DNS Server:

The left side is the configuration you enter; the right side shows the currently active configuration.

You can make the following settings:

MAC: 00-30-d6-13-87-20	→	The MAC address of the system
Hostname: cs141	→	hostname
IPv4		
Local Address: 10.10.10.10	→	Local IP address
Subnet Mask: 255.255.255.0	→	subnet mask
Default Gateway: 10.10.10.1	→	Gateway
DNS Server: 10.10.10.1	→	DNS server

Please contact the network administrator responsible for the required settings. Click Apply to save the settings. When you use the device for the first time, the hardware default values are shown here.

Note:

At this point, the web browser will try to redirect you to a different IP address. Since the CS141 is still in configuration mode, you will then receive an error message from your web browser. In this case, press CTRL F5 to refresh the web display.

If you are doing complete reconfiguration, the Network menu is the only setting you currently need to make in configuration mode. You can also make all the other settings in regular operating mode.

Special feature Initial configuration in DHCP mode

When you start the CS141 in DHCP mode, an IP address is assigned by a DHCP server. You can display this address using the free Netfinder tool. If you are using several web managers, the device is easy to identify using the MAC address and the address label.

CS141L	1.61	Nicht nötig	Generex (12)	d0-39-72-3b-df-f8	192.168.200.142	
BACSKIT_B4	1.60	Nicht nötig	Generex (12)	00-30-d6-16-b3-4b	192.168.200.148	
CS141BL	1.61	Nicht nötig	ALTEVAC (92)	00-30-d6-12-6f-56	192.168.200.224	
BACSKIT_B4	1.61	Nicht nötig	Generex (12)	00-30-d6-12-60-42	192.168.200.225	
CS131	5.58	Verfügbar (5.62)	Generex (12)	00-03-05-0E-2F-49	192.168.200.227	FB Office



The Access Device function opens a web browser with the correct IP address. You can now make your IP address settings under Network and then switch to manual mode:

In DHCP mode, these settings are completely ignored and only the address assigned by the server is used:



The advantage is that you can easily connect as many CS141s as you want to the network at the same time and they can be reached immediately. The disadvantage is that in DHCP mode the IP addresses can change dynamically, which means that higher-level or docked shutdown solutions may no longer be effective or may produce errors.

WLAN – The Wi-Fi interface

Independent of the LAN settings, SITEMANAGER 7 and SITEMONITOR 7 have a pre-installed Wi-Fi module that can be connected to any WLAN:

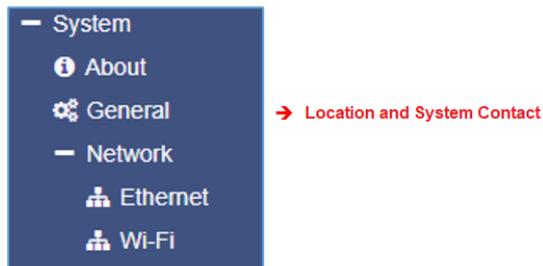
Configured	
IP Configuration	disabled
Network Name	Trikorder
Password	Password
Security	WPA2

- Einschalten / Ausschalten des Wi-Fi – Moduls
- Definition der SSID
- WLAN-Passwort
- Verschlüsselungsart

Additional basic settings

System contacts and location data

For this configuration step you need the following menu:



Location data can be read by software that supports this option. If you monitor many locations with multiple installations, you can use this feature to make it easier to assign installed devices.

Location	General Pump Station 3	→ Enter the location of the device
System Contact	Jane Dow	→ Enter the name of responsible operator
Customer Signature		
Check Firmware Update	<input checked="" type="checkbox"/>	→ If checked, the device will check for firmware updates

Click Apply to accept the current settings and display them accordingly in the About menu.

The freeware tool Netfinder will provide you with the location data, making it easier to search for a specific device:

CS141L	1.61	Nicht nötig	Generex (12)	d0-39-72-3b-df-f8	192.168.200.142	General Pump Station 3	
BACSKIT_B4	1.60	Nicht nötig	Generex (12)	00-30-d6-16-b3-4b	192.168.200.204		
CS141BL	1.61	Nicht nötig	ALTERVAC (92)	00-30-d6-12-6f-56	192.168.200.224		
BACSKIT_B4	1.61	Nicht nötig	Generex (12)	00-30-d6-12-60-42	192.168.200.225		
CS141L	1.61	Nicht nötig	Generex (12)	00-30-d6-12-70-36	192.168.200.231		
CS141L	1.60	Nicht nötig	Generex (12)	00-30-d6-14-21-3c	192.168.200.232		

Select region and unit of measurement

Language	English	→ Choose the language
Temperature	<input checked="" type="radio"/> Celsius <input type="radio"/> Fahrenheit	→ Select unit of measurement

Under Language, select your preferred system language. The following languages are supported:

German, English, Chinese (Simple), French, Spanish, Polish, Portuguese

Under Temperatures, select the unit of measurement in which the temperatures should be displayed.

Difference Fahrenheit / Celsius

Although initially defined by the freezing point of water (and later melting point of ice), the Celsius scale is officially derived from the Kelvin scale.

Zero on the Celsius scale (0 °C) corresponds to 273.15 K, with a temperature difference of 1 °C equivalent to a difference of 1 K, so the size of the unit is the same in each scale. This means that 100 °C, previously defined as the boiling temperature of water, now corresponds to 373.15 K.

The Celsius scale is an interval system, not a ratio system, which means that it follows a relative, not an absolute scale. This can be seen because the temperature interval between 20 °C and 30 °C is the same as between 30 °C and 40 °C, but 40 °C does not have twice the air heat energy as 20 °C.

The temperature difference of 1 °C corresponds to a temperature difference of 1.8 °F.

Since both scales are used worldwide, it is important to know which scale to use before configuring.

Note:

A SITEMANAGER 7 recalculates the values when the scale is changed and adjusts the settings automatically - however, a higher-level system that is configured to Fahrenheit will inevitably receive incorrect information from a web manager that is set to Celsius.

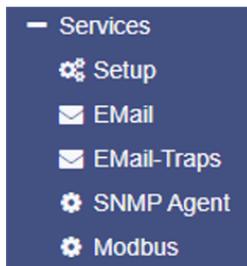
This small problem can have big consequences, especially when working in an international team:

For example, on December 11, 1998, the Mars Climate Orbiter entered the planet's orbit as programmed, but 170 kilometers lower than planned. The reason was that two different groups at NASA carried out the trajectory calculations - one in inches and one in meters:

"The 'root cause' was the failed translation of English units into metric units in a segment of ground-based, navigation-related mission software ..."

Services

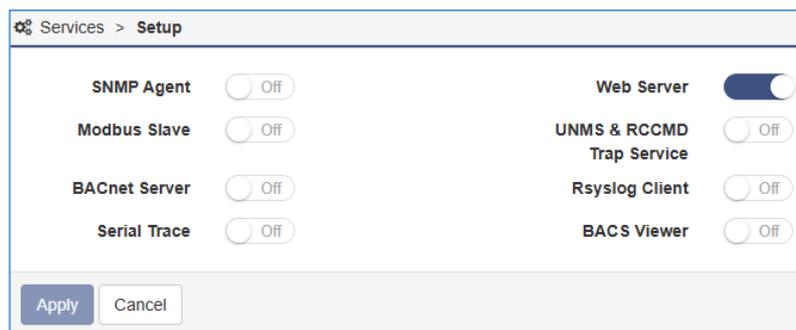
For this setting you need the following menu:



→ General Setup: Enable / Disable Services

Please note: The services and their setup, including all necessary tables (e.g. for setting up Modbus) are discussed in detail in the CS141 user documentation. The complete CS141 documentation can be found at www.generex.de in the download area.

By default, all but the web server are disabled for security reasons and must be enabled individually if required.



A SITEMANAGER 7 uses various, independent system services for communication. This allows functions to be activated and deactivated without the devices having to be completely restarted.

Note: Doctrine change with firmware 2.14 – Cybersecurity Enhanced!

According to best practice, the default settings were chosen so that a quick and uncomplicated integration into existing systems that rely on standards was possible. With a view to cybersecurity, this has now been changed. All services that are not required for the initial setup will in future be set to "OFF" by default in the factory settings - administrators will in future have to manually and consciously activate functions such as SNMP or Remote Syslog before they can be used.

Web Server

The web server service is the local web interface of the CS14. A connection is established via port 80 using a web browser, via which the CS141 can be configured.

In some high-security areas, it may be necessary to permanently prohibit this access to the web interface after configuration, without restricting the configured functionality.

Since web access is completely blocked, this option cannot be reversed - this requires booting via the rescue system and restoring the delivery state. A data backup is possible, as this must be done as the last step before deactivating the web interface.



Note:

The rescue system on the CS141 not only has the latest firmware saved, but also the last configuration before your update. If you have accidentally or intentionally deactivated this function and want to activate it later, we recommend that you perform a firmware update before activating it.

This ensures that you can still access the system later without losing the general configuration.

SNMP

The Simple Network Management Protocol (SNMP) is a network protocol developed by the IETF to monitor and control network elements from a central station.

The protocol regulates communication between the monitored devices and the monitoring station. SNMP describes both the structure of the data packets that can be sent and the communication process.

It was designed in such a way that any network-capable device can be included in the monitoring. The network management tasks that are possible with SNMP include:

- monitoring of network components,
- Remote control and remote configuration of network components,
- Error detection and error notification.

Due to its simplicity, modularity and versatility, SNMP has become the standard supported by most management programs as well as end devices.

If you want to use SNMP in your network, leave this feature checked.

Modbus

Fieldbuses are bus systems via which individual devices such as sensors or actuators can be connected to one another and enable orderly communication with a corresponding fully automated management system.

If several communication partners send their information over the same line, fixed rules must be established for communication

- who (identifier)
- what (measure, command) and
- when (initiative)

may send. Standardized protocols are used for this purpose.

Modbus is not new here:

The Modbus protocol was introduced in 1979 by Gould-Modicon for communication with its programmable logic controllers and has become an unofficial standard for industrial use due to its open protocol standard.

Since 1999, fieldbuses have been standardized worldwide in the IEC 61158 standard (Digital data communication for measurement and control technology - Fieldbus for use in industrial control systems). The second generation of fieldbus technology is based on real-time Ethernet.

For more information about the options, see the "Modbus" chapter in this manual; the necessary Modbus lists can be found in the appendix.

BACnet Server

BACnet (Building Automation and Control Networks) is a network protocol that has been standardized by ASHRAE, ANSI and ISO 16484-5 for building automation. You can find out more about the options and configuration in the "BACnet" chapter in this manual.

Serial Trace

The CS141 offers a system tracer under Tools, with which you can observe and record communication between the CS141 and the UPS. This communication takes place via port 4000. With this slider you can specifically open (on) or close (off) port 4000.

UNMS & RCCMD Trap Service

The UNMS & RCCMD Trap Service was specially developed for communication with the universal network management software from GENEREX. The powerful successor UNMS 2 communicates with the CS141 via UPSTCP on port 5769. The UPS server service enables or disables availability via this port.

Remote Syslog Client

Remote Syslog is a popular method for sending locally stored log files in a standardized format to a central network node, a so-called Syslog receiver, regardless of the device or manufacturer.

BACS Viewer

If you operate a BACS system, you can use the BACS Viewer software to download the data from the batteries you are managing. This function opens the necessary SFTP port and activates the agent through which the BACS Viewer can connect to the CS141 / BACS WEBMANAGER.

Date and time

For this configuration step you need the following menu:



For some system-critical settings such as event logs or recurring tasks, an exact time specification is necessary. For this reason, the CS141 has its own system clock and the option of querying external NTP servers.

In addition, if supported by the UPS, the UPS's internal clock can be set and read again in an emergency in the event that there is no external means of checking the time itself.

NTP Services and time control

Aktuelle Systemzeit	02.01.2000, 00:37		
Zeit-Server Adresse 1	<input type="text" value="0.pool.ntp.org"/>	SNTp	Test
Zeit-Server Adresse 2	<input type="text" value="1.pool.ntp.org"/>	SNTp	Test
Zeit-Server Adresse 3	<input type="text"/>	SNTp	Test
Timezone	<input type="text" value="(UTC) Coordinated Universal Time"/>		
	<input type="button" value="Synchronize CS141 with Timeserver"/>		
<input type="button" value="Übernehmen"/> <input type="button" value="Abbrechen"/>			

- The current system time
- Entering the first NTP server
- Entering the second NTP server
- Entering the third time server
- Select time zone
- Synchronize system with time server
- Accept input

If the network settings are set correctly and there is an Internet connection, you can use the preset servers. You can use the test function to test availability. If you use your own local time server in your network, you can also enter the IP address of your internal time server here.

Note:

A time server outputs a preformatted time, which also contains the time zone used. The CS141 calculates the real system time itself from the time zone setting. If you operate your own time server, this time zone must be adjusted accordingly.

By clicking Apply, the settings are applied, and the time server service is restarted and an initial time synchronization is performed.

Advanced User Management

For this configuration step you need the following menu:



User Roles

User roles have a major influence on the availability of menus. Only users with the user role "Administrator" have full access to all functions. Other user roles have menus displayed dynamically based on their function.

- Lock the Engineer Role
- Lock the Customer Role
- Lock the Guest Role

To be able to use the respective user role, remove the corresponding check mark and click Apply. The user role will then become available and the corresponding user can be used. Exceptions to this are the user role "Administrator" and the "Super User" admin.

Available Users

The default setting is 4 users.

The Administrator

User admin
Default password: cs141-snmp

Due to his role, the administrator has the full range of configuration options available. The administrator manages network and mail settings and is the only user with the right to change the landscape of the connected devices. This user cannot be deleted or deactivated. The user "admin" also has full access to user management and can manage any user he has created with the user role "administrator". The user "admin" is the only user who can be used in configuration mode (sliding switch in the middle).

The Technician

User engineer
Default password: engineer

The technician has a user account restricted to his area of responsibility. He has access to the functions that relate to technical activities. He can adapt and configure the available devices and make the necessary adjustments. This user can be freely edited and deleted, and the user role is deactivated.

The Customer

User customer
Default password: customer

The customer is a further level below the technician. He has access to system and status monitors and their functions and can also download all log files. This user can be freely edited and deleted, and the user role is deactivated.

The Transporter

Frank Martin (Jason Statham) is a highly skilled driver who transports packages for shady customers, no questions asked. However, when he opens a delivery, he discovers a woman tied up and breaks his own rules. From now on he not only has to fight his clients but also protect the woman while he gets caught up in a dangerous whirlpool of violence and corruption. But this another story and therefore not part of the SITEMANAGER 7 configuration ...

The Guest Account

User guest
Default password: guest

Guest access allows you to simply view the system monitors without being able to trigger any other functions. This user is essential for sub-functions and can be deactivated but not renamed or deleted.

Anonymous Guest

The Anonymous Guest is an additional function of the regular guest access, and is directly linked to it:

With the Anonymous Guest it is possible to access or view the status screens on a session basis without repeatedly entering a password and is only available if the user "guest" is not blocked.

Please note that the Anonymous Guest does not use its own password but uses the user password for regular guest access.

Create additional administrators

Every user with the user role "Administrator" can create users in free text under "local users" and assign a corresponding user role. The menu will dynamically display the available menus according to the user role. The only exception is access to the user "admin".

User management under RADIUS

The prerequisite is that a RADIUS server has been successfully set up and tested.

The setting partially overwrites the local user database:

1. user / release level

RADIUS Servers		
	Priority	IP Address
<input checked="" type="checkbox"/>	Primary	127.0.0.1
<input checked="" type="checkbox"/>	Secondary	127.0.0.1

Local Authentication Only
 RADIUS, then Local Authentication
 RADIUS Only

The RADIUS user and its shares are used to display the respective menu.

Exceptions:

- The user role is locked locally.
- The device is in configuration mode, in which case access is restricted to the superuser "admin".

The RADIUS setup offers the following options:

Local only: the RADIUS server is ignored and only the specifications of the local user database apply

RADIUS, then Local: An attempt is first made to reach the RADIUS server. If this is not available, a comparison is made with the local user database. Important: If the RADIUS server is reachable but does not respond, login is not possible.

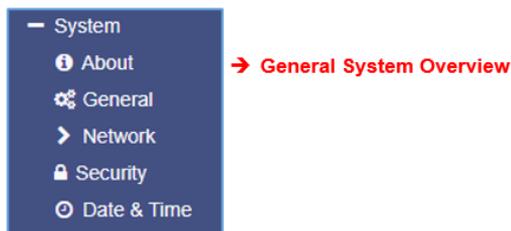
RADIUS only: Restrictive operating mode – The specifications of the RADIUS server apply exclusively. If this cannot be achieved, access is not possible.

Note:

A complete and detailed configuration guide for the RADIUS server can be found in the official CS141 user documentation in the download area at www.generex.de

System Overview: The About Page

For the system overview, click on the following menu item:



Once you have completed all the basic settings, you can access the general system information under About and display it in an overall overview:

System and the Firmware version

The following list contains the most important information about your SITEMANAGER 7

Name CS141LM	➔ The WEBMANAGER in USE
Version 2.23.12.250220	➔ Current firmware
License Pro Edition	➔ UPS license key
Manufacturer Generex	➔ Vendor OEM
UPS Model No UPS model defined	➔ Configured UPS model
Location	➔ Device location
System Contact	➔ Contact data of responsible staff
Time 2025-02-20 16:18:10 (UTC+01:00, DST) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	➔ System time and time zone
Uptime 0 days, 1 hours, 11 minutes, 33 seconds	➔ Operating time since last reboot
Serial No. 1016909336	➔ Serial Number of the CS141 device
Features hw161	➔ Hardware revision of the device
MAC Address 00-30-d6-38-4d-a4	➔ MAC address of the device
Hostname cs141	➔ Configured host name
Domain localdomain	➔ Domain setup
Timeserver Address 1 0.pool.ntp.org	➔ Defined Timeserver (NTP services)
Timeserver Address 2 1.pool.ntp.org	➔ IP address mode (DHCP / static IP)
Network Configuration Mode Static IP address	➔ Current IP address
IPV4 Address 10.10.10.10	➔ Subnet Mask
IPV4 Subnet Mask 255.255.255.0	➔ Default gateway
IPV4 Gateway 10.10.10.1	➔ DNS (Domain Name Server) Settings
IPV4 DNS Server 1 10.10.10.1	

If you require technical support, our technical support will require at least the following information from you:

- firmware version
- The UPS model used
- operating time since last start
- serial number of the device
- The hardware revision shown under Features

Reboot and cold start

For some reasons, it may be necessary to restart SITEMANAGER 7. Depending on the application scenario, there are two different options:

Cold Start

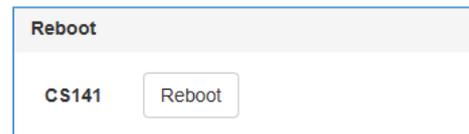
Briefly interrupt the power supply by pulling the power plug or removing the card from the slot. The device will then boot into the corresponding operating state with the new hardware setting.

Warm start - Reboot The reboot button

For this process you need the following menu:



When prompted for a password, enter the default user admin and the password for your administrator access. If you have not assigned a password, the default password applies cs141-snmp



You can then use the Restart function to restart the CS141 boot into operating mode with a software-controlled restart. Whichever boot method you choose, in both cases the UPS is not restarted, only the CS141 is affected - your power supply is always guaranteed.

Configuring system notifications

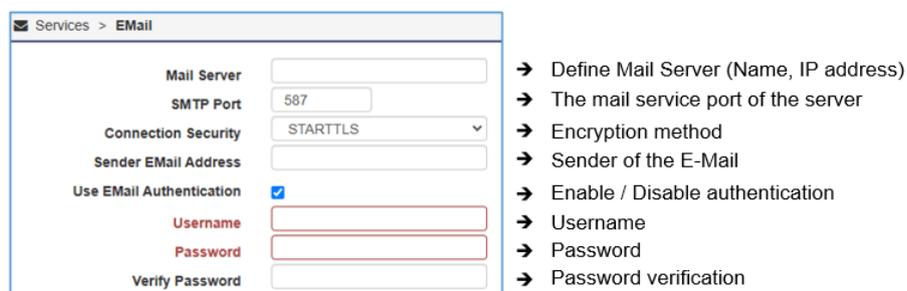
Email settings

For this configuration step you need the following menu:



A SITEMANAGER 7 has different options for interacting with the environment, connected devices and networks. One of the basic functions is automatic notification via email and email traps.

However, a valid email account must be stored for this functionality:



Mail Server

Enter the mail server to be used here. You can enter both a mail server and the corresponding IP address. You can use your own internal mail server or an external service provider via an Internet connection.

Note:

The fact that SITEMANAGER 7 has a connection to the Internet to access external accounts of large email providers does not mean that the external provider allows service emails as such or that it will block such emails at a later date without giving reasons. If in doubt, contact your service provider.

SMTP port

Defines the port through which a mail client communicates with the mail server. The ports are generally standardized, but it is always possible to use your own ports for communication. The necessary access data must therefore be obtained from the local administrator.

Connection Security

Select the encryption type with which the CS141 should transfer the emails to the mail server:

None	No encryption
STARTTLS	If available
TLS / SSL	Force Encryption

Sender Email Address

Enter the email address you want to use to send an email. This will then be displayed in the "From" field of the respective recipient.

Use email authentication, user and password

Depending on the configuration, email servers use either the email address or their own user ID and password as the username to receive emails for sending.

For valid access data, please contact the relevant network administrator on site.

Advanced Options

The screenshot shows the 'Advanced' configuration window with the following options:

- Format:** Database interface Format
- Log:** (dropdown menu)
- Automatically send an EMail:**
 - For the most important events
 - On scheduled Jobs

- ➔ Custom Database converted E-Mail format
- ➔ Logging behavior for E-Mail Jobs
- ➔ Automatic mailing function for events/jobs

Format

If emails are automatically recorded in a database, the format of the email can be pre-formatted accordingly.

Log

Defines the conditions under which sending an email is recorded in the event log.

The following options are available:

Errors only	Emails indicating malfunctions are recorded in the event log.
Always	Each email is recorded as "sent" in the event log.
Never	Emails are sent but not recorded in the event log.

Automatically send an email

Based on the RCCMD traps entered in the event management. If selected, the SITEMANAGER 7 sends an email regardless of the other configuration

<input checked="" type="checkbox"/> For the most important events	A predefined set of system events – the exact list depends on the range of functions, expansion level and connected UPS.
<input checked="" type="checkbox"/> On scheduled Jobs	For all tasks scheduled via the scheduler.

Note:

Depending on the configuration, this global setting can send a second email for many system events. If you specifically define your own emails in event management, it may be useful to deactivate this function.

The same applies to the Log function:

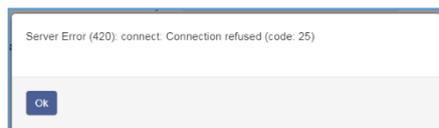
Too many entries in the event log quickly leads to confusing data sets as soon as you search for specific entries within a time window.

Click Apply to apply the settings to the configuration and restart the email sending service.

Testing the mail settings

Please note that this function is only available after you have clicked on Apply and the data has been transferred to the SITEMANAGER 7 configuration.

Using this function, you can send a message to an email address of your choice to check the functionality.

Connection refused - The most common error message:

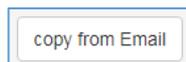
This error means that no connection to the mail server could be established.

The reasons for this can be varied, ranging from an incorrect or inactive port to the fact that an external mail provider prevents this type of mail transmission.

Email Traps

Mail traps are status and information messages automatically generated by industrial systems, which can be picked up and evaluated by a corresponding recipient. The difference to an email is that you cannot enter any text or define a different recipient.

For further information, see the chapter UPS configuration

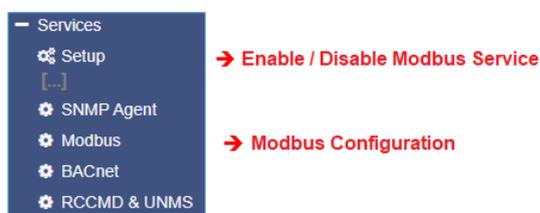


If you want to use the same account that you set up under Email, you can copy the data directly using copy from Email:

The copy from Email function copies the data you have already entered. You only have to confirm the password again under Verify Password. If you use a different email account or mail server, enter the corresponding access data.

Modbus

For this configuration step you need the following menu:



Fieldbuses are bus systems that connect field devices such as sensors and actuators in a system for communication with an automation device. If several communication participants send their information over the same line, then it must be determined who (identifier) can and may transmit what (measured value, command) and when (initiative). There are standardized protocols to ensure this communication.

The Modbus protocol was launched in 1979 by Gould-Modicon for communication with its programmable logic controllers and has since become an unofficial standard in the industry because it is an open protocol.

Since 1999, fieldbuses have been standardized worldwide in the IEC 61158 standard (Digital data communication for measurement and control - Fieldbus for use in industrial control systems). The second generation of fieldbus technology is based on real-time Ethernet.

Note:

For further information please refer to the Modbus manual, which is available in the download area of our website at www.generex.de.

[Modbus in devices](#)

Modbus is a protocol for serial communication. Data is transmitted in the form of 16-bit registers (integers) or data byte status information. MODBUS has many advantages:

- The basic structure of MODBUS has never really changed for compatibility reasons. The set of uniform devices enables a stable basis for integration and maintenance and configuration.
- This open protocol has established itself as a quasi-standard for many industrial machines worldwide. As soon as a device supports Modbus, it can usually be integrated into an existing network.

[Modbus as a single-master protocol](#)

The master controls the entire transmission and monitors any timeouts that may occur. The connected devices may only send telegrams if the master requests them.

For remote control and monitoring of devices, the Modbus interface in each CS141 can read measured values, events, status and other information within the master-slave protocol.

Note:

If you are missing certain measured values, this is not necessarily an error - especially when it comes to special functions, it may be that the UPS informs the CS141 via SNMP, but the manufacturer does not have a Modbus address assigned to it. In this case, the CS141 would react to a function such as low battery in the web interface and send messages, RCCMD commands, etc. according to the configuration, but this status cannot be queried via Modbus.

[Modbus over RS232 and Modbus over IP](#)

As already mentioned, all devices in the CS141 family can handle MODBUS - the difference is in the details. While the CS141 Modbus adapter can be integrated into a bus with the RS485 interface, SITEMANAGER and SITEMONITOR use a point-to-point connection with Modbus over RS232 and Modbus over IP. The RS232 Modbus connection is usually used when you want to transfer Modbus data from the UPS to another system or special monitoring software.

Both devices adhere to the RFC1628 standard. If required, the MIB can be downloaded from the download area at www.generex.de.

[Modbus function codes](#)

The devices of the CS141 product family support the following function codes:

01H	-	Read Coils
02H	-	Read Discrete Inputs
03H	-	Read Holding Registers
04H	-	Read Input Registers
05H	-	Write Single Coil

Please note that the function codes actually available depend on the UPS connected, as the UPS must support commands of this type. As a rule, functions 03H and 04H are available for standard UPS systems, although the CS141 does not differentiate between these two functions. Since the CS141 supports query speeds of up to 38400 baud, the CS141 can be flexibly integrated into an existing system.

[Modbus error codes](#)

With the exception of broadcast messages, where the master device sends a request to the slave device, the master expects a clear and valid response from the slave. If the response does not meet the requirements, the packet is discarded with an appropriate error.

The following possible events can occur when a master device requests a request:

1. The slave responds accordingly with a suitable data packet.
The master will react accordingly.
2. The slave unit does not receive the request from the master

This event occurs, for example, in the event of a communication error. As a consequence, from the master's perspective, the request was not answered, it reacts with a corresponding timeout.

3. Master or slave send invalid messages

Such a phenomenon can occur if, for example, the terminating resistors have not been set. Data is sent, but there are clear errors in the parity, LRC or CRC within the data packet. Since invalid packets are discarded, the slave will usually not respond to such a request. The master generally reacts to an incorrect response with a corresponding timeout message.

4. The slave receives a valid request that cannot be answered

If the slave unit receives a request without a communication error, but reading is not possible due to, for example, a non-existent register, the slave unit responds with a specific exception message, informing the master unit about the reason for the error.

The following error codes are possible with the CS141:

- 02H Illegal Data Address

The data address received with the valid request is not a valid address that the slave can serve

- 03H Illegal Data Value

A value that was included in the request is not a valid value for the slave.

- 06H Slave device busy

The slave has received a valid request, but is currently busy with a time-intensive or time-critical process, which means that it cannot currently serve the master. In this case, the master will not respond with a timeout, but will repeat the request at a later time.

Configuration of Modbus

Since Modbus relies on standards, the basic configuration is relatively simple. To do this, open the Modbus tab under Services to open the menu for the corresponding settings:

TCP Port	502	→	Port 502: Standard Modbus address
Max Connections	10	→	Maximum simultaneous device accesses
Slave Address	1	→	Modbus ID of the device
COM2 (RS232 / RS485)			
Baud Rate	38400	→	transfer rate
Parity	n	→	parity bit
Stop Bit	1	→	stop bit
Übernehmen	Abbrechen	→	Save / Cancel

Enable Modbus Slave

This function activates the Modbus query directly from this menu. Please note that other, higher-level menus can also contain this function - if you deactivate Modbus there, this check mark will automatically be removed from the system.

TCP port 502

TCP port 502 is a general setting within the Modbus standard that cannot be changed or adjusted. The CS141 generally answers all Modbus requests on exactly this port.

Slave Address

The Modbus slave is the ID under which a device feels addressed and will actually respond. This ID can be freely assigned, but can only exist once in the network.

Note:

If you assign a Modbus slave address twice, this does not lead to a so-called network short circuit - in this case both addressed devices would respond, which would cause the Modbus master to display misleading data.

In this case, check the uniqueness of the slave address and, if necessary, assign a free address.

Baud Rate

The baud rate defines the transmission rate - the speed at which Modbus queries can be received and answered. In this context, note that the query speed by the master must be identical to the setting in the slave, otherwise communication cannot be established.

Parity

When data is transmitted in the form of a bit stream, the parity bit forms a security instance with which error detection can be carried out. The value of the parity bit is calculated by the sender and communicated to the receiver. The receiver can then use the same mathematical algorithm to check whether the data is corrupted.

The parity calculation can be designed for even or odd.

Sender and receiver must therefore agree in advance whether to perform an even or odd parity calculation.

Example: Even parity

If an agreement is reached to calculate an even parity, the number of all 1-bits in the data to be secured is counted. The task of the parity bit is to extend the result to an odd number if necessary.

Therefore, if the number of bits to be checked is even, the parity bit must be transmitted as 0, otherwise the total value will be incorrect.

The CS141 offers the following options in this context:

N	No parity control
O	Odd parity control
e	Straight parity control

By default, the CS141 is delivered with the value n for no parity check.

Stop Bit

The stop bit defines the end of a data word within a data stream and is used in asynchronous data transmission:

Usually, a corresponding start bit is sent before the beginning of a data word so that the receiving device can recognize the beginning of the character string. In principle, this is also a high signal, but the level is different from that of the following data word.

At the end, depending on the configuration, one or two stop bits are added, which explicitly define the end of the data word. As a consequence, no valid data word can be present between the stop bits and the next start bit and is therefore discarded.

If data is lost or incomplete due to problems during data transmission, this predefined chain can be used to distinguish between start and stop, making resynchronization possible.

Note:

If several Modbus devices are on the same ID, these devices will send out their data stream accordingly when a corresponding request is made. Among other things, the start and stop bits within the network overlap, which leads to problems in assigning valid and invalid data packets.

With the Stop Bit function you define whether the SITEMANAGER or SITEMONITOR should send one or two corresponding stop bits.

Apply / Cancel

This function saves the entered data and restarts the corresponding services if necessary. A complete reboot of the CS411 is not necessary.

Take over -Saves the entered data and restarts the services

Cancel -Discards the entered data and cancels the configuration dialog without making any changes.

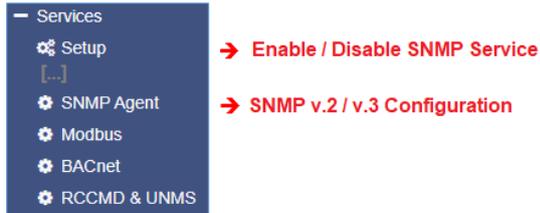
Please note that some clients such as MODBUS Poll use "MODBUS addresses" like the CS1451 with a valid range of 0-65535. If you use another client whose "MODBUS register" works with a valid range of 1-65536, it is necessary to add a 1 to the address

[Additional documents and Modbus lists](#)

Further system documentation and all available Modbus lists can be found in the official CS141 user documentation in the download area at www.generex.de

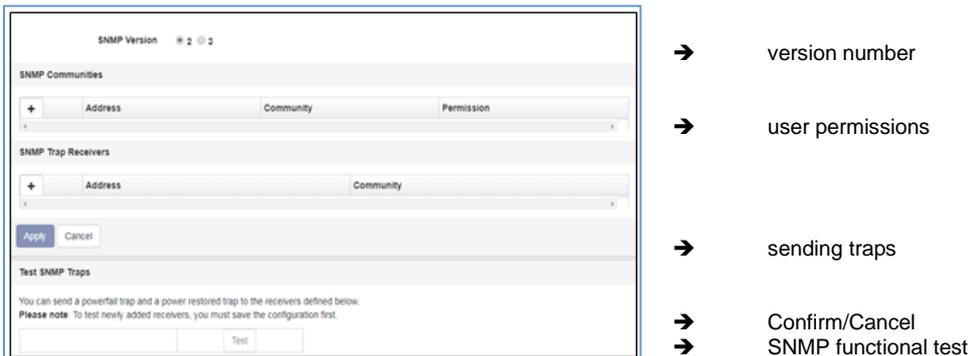
SNMP Agent

For this configuration step you need the following menu:



The Simple Network Management Protocol is a network protocol developed by the IETF to monitor and control network elements from a central station. The protocol regulates communication between the monitored devices and the monitoring station. SNMP describes the structure of the data packets that can be sent and the communication process.

The SITEMANAGER 7 can be fully integrated into a network with SNMP monitoring. The SNMP agent takes on the task of receiving and sending corresponding requests.



Note:

SNMP V1.0 is not officially supported by SITEMANAGER 7. We recommend using only version 2.0 or higher. However, since V1.0 is included in large parts of V2.0, SITEMANAGER 7 will respond to SNMP V1 requests, but the use of V1.0 is outside of official support.

[SNMP v2 and SNMP v3](#)

The difference is that SNMP v2 works on the basis of the authorized IP address while SNMP v3 works on the basis of direct user authorizations with name and password.



First activate the SNMP agent to access the menu. Under SNMP version, select the desired version.

Setting up SNMP V2:

The overview shows all user groups created so far

SNMP Communities			
	Address	Community	Permission
←			

To configure a new permission, click on the +

Add Community

IP Address
IP address required

Community

Permission

- The authorized IP address
- The eligible community
- data access permissions

- Save / Cancel Configuration

IP address

Under IP Address, enter the IP address of the authorized computer that is allowed to access the CS141 via SNMP v2. The community defines the authorization group.

permission

This setting defines the direct authorization with which a device can access the CS141:

- Read only** Devices in this authorization group have read-only rights
- Read/Write** Devices in this authorization group have read and write permissions.

Setting up SNMP traps

What are SNMP traps for?

Basically, an agent that monitors a system can send a so-called trap packet to its management station without being asked to do so, should this be necessary. This includes, among other things, the status of the monitored device. The agent can then receive and process requests from its manager.

Two ports are required by default:

- Port 161** Required by the agent on the device to receive requests
- Port 162** Required by the management station to receive messages

If these ports are blocked in the firewall or on switches, communication will not work.

Trap Receivers on SITEMANAGER 7

The advantage of trap messages is that SITEMANAGER 7 can automatically inform you about changes in the UPS. However, the system must be informed where the messages should be sent:

Click on the + to create a new trap receiver.

Since trap messages are only sent and inform about status changes, the input field for the write/read operations is omitted.

Enter the recipient's IP address and the valid community.

When you click Save, SITEMANAGER 7 applies the settings and restarts the SNMP agent. SITEMANAGER 7 does not need to be completely rebooted.

Testing the Trap Receivers

The newly configured Trap recipients can then be tested by pressing the test button. The corresponding test message is sent and should be displayed directly in your program.

Note:

Trap messages are automatically generated messages that do not require confirmation - a device that sends trap messages generally does not know whether the messages have arrived. Consequently, no information about receipt can be logged.

Setting up SNMP v3

The overview shows all currently configured users:

Since SNMP v3 works on a user basis, you cannot create user groups here. Click on the + to configure a new user:

- Define a username
- access authorization
- access protection
- Save / Cancel

User Definition:

By default, every user has read and write permissions. If you want to specifically deny a user the right to write, activate the Read only option.

Authentication

Define the security level with which a user can access:

No security	No password required.
authentication	A password is requested.
Authentication and Privacy	The connection is additionally encrypted, and two passwords are required.

Note:

Please note that in addition to the correct access data, the encryption type must also be identical, otherwise no connection will be established.

Setting up TRAP recipients under SNMP v3

To set up a trap receiver under SNMP v3, you must first create a suitable user. You can then select this user as a trap receiver in SNMP v3.

Add Trap Receiver

IP Address
IP address required

User

Testing the trap settings

You can then use the test function to test the SNMP v3 trap receiver:

Test SNMP Traps

Select a device and a corresponding trap to send to the receiver(s) defined above.
A TrapAlarmEntryAdded and a TrapAlarmEntryRemoved will be sent.
Please note: To test newly added receivers, you must save the configuration first.

Device

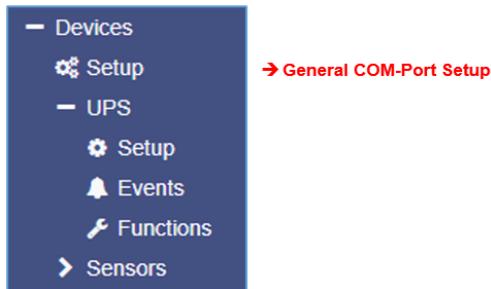
Trap

Oid 1.3.6.1.2.1.33.1.6.3.1

From the drop-down menus, select the device and the trap you like to test. Click on "Test" to trigger a test alarm. The trap receiver should show the incoming trap accordingly.

General interface settings of the COM ports

For this configuration step you need the following menu:



Depending on the design and model, the devices of the CS141 family have up to three hardware COM ports, which can fulfill different functions.

Both the SITEMANAGER and the SITEMONITOR are technically largely preconfigured here:

COM 1

This port is reserved for connecting the UPS

COM 2 – Sensor

Type: SITEMANAGER

A SITEMANAGER 7 has internal relays and the option to manage analog sensors and digital inputs. The integrated CS141 communicates internally with the pre-installed hardware.

COM 3

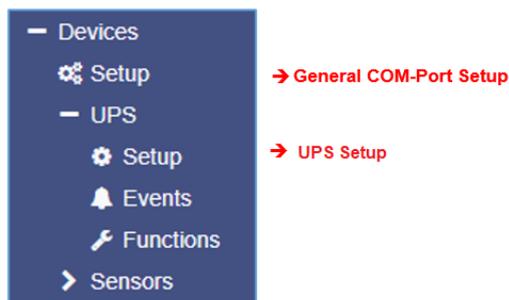
A SITEMANAGER 7 uses the COM interface to communicate with the BACS system.

USB port

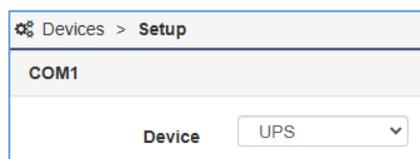
A SITEMANAGER 7 communicates with the WLAN module via the internal USB port

Setting up the UPS

For this configuration step you need the following menus:



First check the general COM port settings:



By default, the UPS device is selected for COM1. If this is not the case, open the selection menu and select UPS.

Click Apply to save the new setting and the CS141 starts the relevant services that are necessary to be able to access a UPS. When you activate this function, a general dummy is first set, which gives you access to the relevant menus.

You can clearly see the successful activation in the top bar

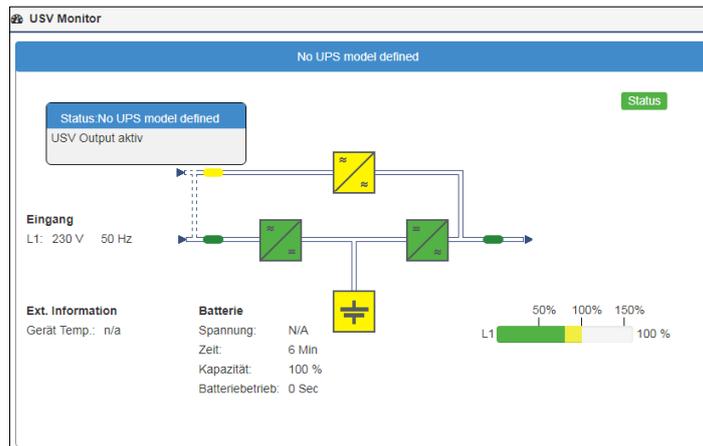


→ The system starts the UPS function



→ The dummy and the UPS menu are ready for use

Please note that at this point only a dummy has been started without any function, even though a UPS appears to be connected and in operation:



Note: If you do not want to use a UPS or do not have one connected, you can set COM 1 to none. In this case, the relevant services are deactivated, and the additional configuration menus are automatically hidden.

After you have provided COM1 for the UPS, go to the UPS submenu and then to Configuration

- Selecting the UPS model
- The power provided by the UPS
- Maximum load that can be connected to the UPS
- Maximum time the UPS will last at maximum load
- Time until the batteries are recharged.
- speed of data transfer
- Cable to be used
- UPS ID
- Date when the batteries were installed
- Indication of when the batteries should be replaced
- Duration after which the UPS switches itself off
- Save / Cancel

[Settings overview](#)

These values become interesting when the UPS protocol does not provide the relevant data. In this case, the CS141 can calculate the corresponding running time in battery mode independently based on the data available. As a rule, these settings do not need to be changed if you can select a UPS model - the optimal configuration for the model has already been stored.

If you want to set a configuration different from the standard model or a model where this data is not provided by the UPS via the protocol, contact the UPS manufacturer to find out the correct values.

Note:

The OEM ID 12 is set for GENEREX SYSTEMS by default. If you want to use a UPS from another manufacturer, it is worth taking a look at the download area at www.generex.de - select the firmware for your UPS and install it as a regular firmware update.

The corresponding UPS models are then available to you.

The following information can be customized:

Model

Defines the presetting of the UPS with the corresponding stored protocol. If your UPS is listed and communication has been established, the UPS telemetry usually provides all the necessary data that the CS141 needs to calculate and display the real autonomy times.

Please note that when changing the UPS model, the UPS event configuration will also be reset. The SITEMANAGER 7 therefore offers the option of creating a backup of the event configuration beforehand.

Don't save
Save
Cancel

Continue without backup
Create backup
Do not make any changes to the system

power (VA)

Defines the power in VA that a UPS can provide. If this value is exceeded, the UPS can be permanently damaged or even destroyed.

load (VA)

Defines the maximum load that should actually be connected. This value should never be higher than the value under Power. Please note that the maximum load can be equal to the Power value.

holding time (min)

This value is given in minutes and defines the maximum running time at 100% connected load.

battery charging time

The estimated time required for a full charge cycle.

Note:

Behind the values of power (VA), load (VA), holding time and battery charging time there is a mathematical formula that the CS141 can use to independently calculate how long the UPS batteries would have to last in the event of autonomy and to trigger the corresponding system events. These values only come into play if the UPS protocol cannot provide any values - for example, if a UPS communicates exclusively via switchable contacts and only basic operating states can be recorded.

baud rate

Different protocols support different data transfer speeds. The baud rate defines the speed at which data can be sent and received. An incorrect baud rate can lead to communication problems between the CS141 and the UPS.

cable type

UPS manufacturers sometimes use specially prepared cables for their models. In addition to these special in-house developments, there are also standardized cable types whose wiring can be used to represent different functions and switching states.

battery installation date

Batteries in a UPS have a limited lifespan - replacing the batteries is therefore part of regular maintenance work. To keep track of larger installations, you can enter the date when you put the batteries into operation or last replaced them.

Battery expires after

The CS141 can automatically provide information about when the regular operating period for the installed batteries has expired. By default, the CS141 will provide system information after 48 months. You can extend or shorten the period in months

System Shutdown Time

The system shutdown time defines the last emergency shutdown of the network, which can be found under Devices/Systems>UPS>Events. In principle, this value can be used to define the last emergency shutdown of the entire network.

UPS ID

Large UPS systems can contain more than one UPS module, which are queried using a unique ID. The 0 is a form of broadcast, where the CS141 can recognize and manage the number of UPS modules itself, which is normally the optimal setting. If you change this value, you will only see the exact module with this specific ID.

Apply / Cancel

This function allows saving and restarting the UPS service on the CS141.

Connecting the UPS to the SITEMANAGER 7

On the back of the device, next to the network connection, there is a MINI-DIN connection labeled COM 1:

Connect the adapter cable MINIDIN / RS232 included in delivery and then connect the standard data cable included in delivery of your UPS to the adapter cable:



To ensure correct hold, place the screw nuts included in delivery between the two small locking devices.

After a short synchronization phase, the SITEMANAGER or SITEMONITOR displays the UPS data in the UPS monitor:

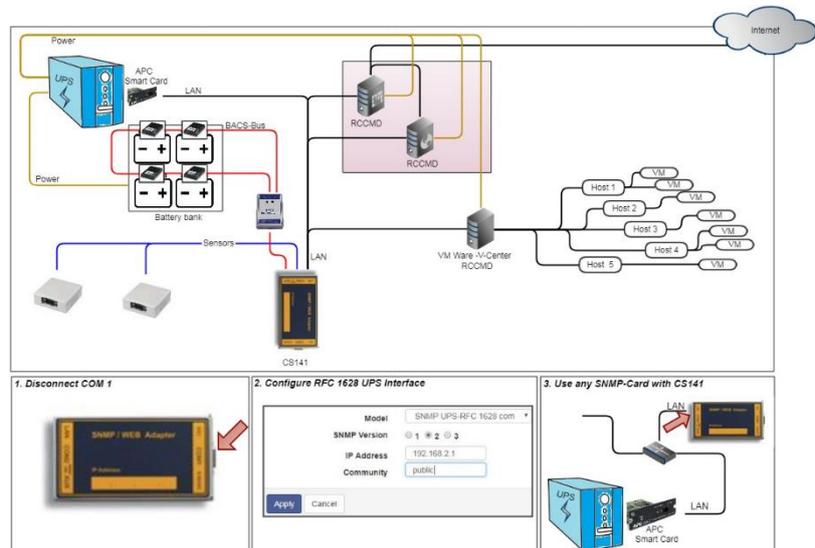
The status LED flashes green slowly and evenly

Special feature: The RFC1628 UPS interface

In some cases, UPS manufacturers deliver systems with which the CS141 cannot communicate directly - often this is due to the problem that the card does not fit into the slot, for example, or that the data sent by the UPS is not compatible.

In this case, UPS manufacturers have installed their own SNMP card, which offers similar functions, but may not be compatible with your GENEREX software landscape. To ensure compatibility, the CS141 Web Manager offers the option of connecting to any card using SNMP. The only condition here is that the RFC 1628 MIB is supported by the target card.

To use this function, you must first configure a corresponding SNMP release on the target card. You can then enter the access data in the CS141 and establish a connection to the target card.



Setting up the target card under SNMP v2

Modell	SNMP UPS-RFC 1628 com	→	UPS model selection
SNMP Version	<input type="radio"/> 1 <input checked="" type="radio"/> 2 <input type="radio"/> 3	→	SNMP version
IP Address	192.168.222.116	→	IP address of the target system
SNMP Community	public	→	SNMP Community
<input type="button" value="Übernehmen"/> <input type="button" value="Abbrechen"/>		→	Save/Cancel

Model

Select the model SNMP UPS-RFC 128 com here

SNMP version

Depending on the configuration of the target card, set SNMP version v1 or v2 here.

SNMP Community

Specify the SNMP community under which the target card can be reached.

Apply/Cancel

Click Apply to accept the configuration and the CS141 establishes a connection to the other SNMP card. When communication is established, you can see a green marker at UPS in the upper area.

Note:

What is the difference between the RF1628 UPS interface and the APC Smart Network?

In principle, the APC card can also handle the RFC1628 standard - you will be able to query basic information about the UPS. However, the APC card uses its own OIDs in many places, which are specific to APC and therefore not compatible with the RFC1628 standard.

To ensure the full range of functions, it is therefore recommended not to use the RFC1628 interface for APC UPS systems in this application, but to use the APC-specific setting APC Smart Network.

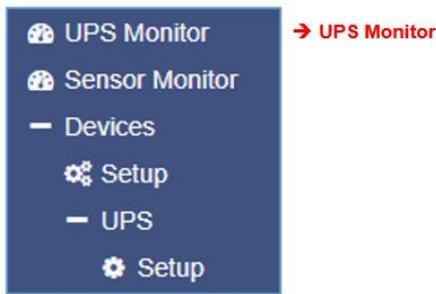
Setting up the target card under SNMP v3

Model	SNMP UPS-RFC 1628 compliant	→	Selecting the UPS model
Battery Installation Date (BID)	DD.MM.YYYY	→	Battery Installation Date
Battery too old after	48 months	→	
SNMP Version	<input type="radio"/> 1 <input type="radio"/> 2 <input checked="" type="radio"/> 3	→	Determine the SNMP version
IP or Host address	192.168.222.116	→	IP address of the target system
User	cs141	→	SNMP User
Security Level	Authentication and Privacy	→	Authentication type
Auth Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA	→	
Auth Password	*****	→	password entry MD5/SHA
Privacy Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES	→	
Privacy Password	*****	→	password entry DES/AES
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		→	Apply/Cancel

In this operating mode, the CS141 supports SNMP version v1, v2 and v3. Enter the access data for the target card according to your configuration and click Apply.

UPS Monitor: Checking the Settings

To check the settings, click the following menu:

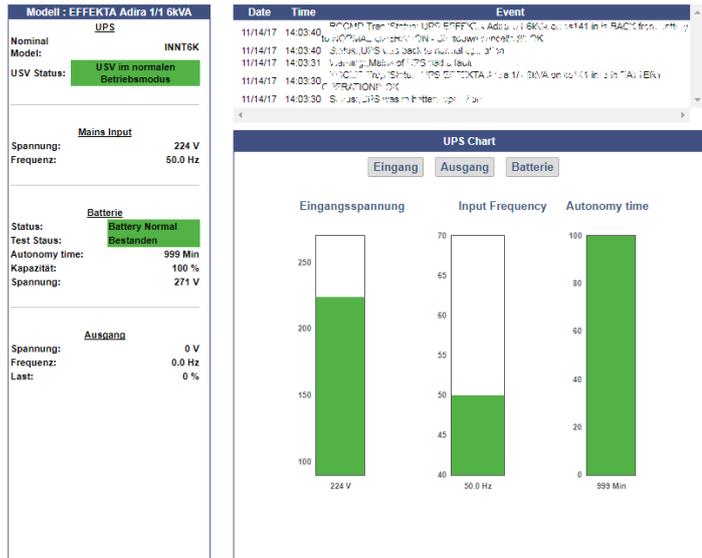


If all settings are entered correctly
 You can use the UPS monitor to view the
 Check the status of the UPS in real time.
 Although the representation varies depending on
 the manufacturer and model can vary greatly,
 some data such as the selected model always
 displayed.

It is clearly visible:

- Model
- Manufacturer
- performance data

The exact scope and presentation
 vary depending on manufacturer and model.



The UPS functions

For this configuration click on the following menu:



UPS functions -working principles

The UPS functions menu contains options for carrying out UPS tests and control scenarios such as battery tests, etc. The masks displayed for this menu can therefore be very different. They are tailored to the UPS model used to be able to display its range of functions. Some UPSs only allow the on/off state, others offer more functions.

Typical test functions would be, for example:

UPS Test	
Start Custom Test	Custom Test Duration[Min] 3
Start Battery Test	Battery Test
Start Full Test	Full Test
Start Self Test	Self Test
Start Cancel Test	Cancel Test

- ➔ UPS test with self-defined runtime
- ➔ battery test
- ➔ full test
- ➔ self-test
- ➔ Termination of ongoing tests

Custom Test

The custom test is a functional test over a self-defined time in minutes.

Battery Test

The battery test checks whether the batteries are taking over and working properly. This test usually takes about 15 seconds.

Full Test

The full test checks the batteries until they are exhausted. This test can take a very long time depending on the power and load. The CS141 also precisely measures and determines the running time under load. Please note that UPS systems require a connected load of at least 25% for a full test.

self-test

With this test, the UPS checks its own functionality as a whole

Note:

In some cases, it may happen that a UPS command is apparently not carried out or an error message appears. The reason for this is that the UPS receives and confirms the command, but decides for itself whether and when this command can or will be carried out - depending on the UPS model, it may well happen that, for example, a minimum charge must be present for a certain battery test, otherwise the UPS returns an error message as a result. This is then logged accordingly as an "error".

In the opposite case, it may also be the case that the UPS sends positive feedback despite an error, but displays an error on the front panel itself.

UPS Control settings

Depending on the design and model, some UPS systems support additional functions that can be used to check the operating behavior of the UPS. The exact range of functions and configurations varies greatly and depends heavily on both the manufacturer and the model used.

Example: Typical UPS control functions:

The screenshot shows a control panel titled "UPS Control". It contains several buttons and input fields:

- A "Shutdown Restore" button.
- Input fields for "Shutdown[Sec]" (value: 60) and "Restore[Sec]" (value: 120).
- A "Shutdown with Duration" button.
- An input field for "Shutdown[Sec]" (value: 60).
- A "Switch off UPS" button.
- A "Cancel Shutdown" button.
- A "Toggle Buzzer" button.

Switchable Outputs

Depending on the design, some UPS systems support switching the outputs on and off.

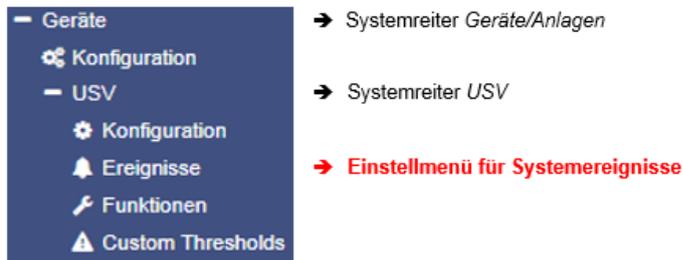
The screenshot shows a control panel titled "Toggle the outlets". It contains two green buttons labeled "1" and "2".

Note:

The UPS systems are equipped differently depending on the performance class, manufacturer and model. Both the layout and the range of functions vary.

System event Setup

For this configuration step you need the following menu:



There are always incidents that require the operation of a UPS or affect the UPS and the connected equipment behind the UPS - for example, the failure of the main power supply, the restoration of the main power supply, a defect in the UPS that prevents switching to autonomous battery mode, etc.

Compared to other so-called systems, the CS141 is a full-fledged manager that can react to these incidents with a system event, inform and independently manage complete event chains: It offers the possibility of implementing a complete shutdown solution for a complex network with mutual dependencies.

Definition of a job for an event

System events are highly dependent on the UPS model used and vary both in terms of their name and the range of options available. One of the biggest problems here is the interaction between events and counter-events:

An event is assigned an action - a so-called job - which is only carried out when the event occurs. The jobs differ in their function and type:

- *information*

These jobs can be executed as often as you like and only serve the purpose of providing information. Depending on the configuration, the content can be repeated once or cyclically if an event is pending - the type of event is basically irrelevant. If the situation changes and the event no longer applies, this job is simply no longer executed.

- *action*

These jobs are designed to switch, trigger, initiate, etc. These jobs are triggered as soon as an event occurs. The difference is that they must be terminated with a corresponding counter job or instructions must be withdrawn.

Note:

Why is it important to understand this difference?

As long as there is a power outage, an email should be written every 5 minutes that sends log files. As soon as the power outage is resolved, no more emails are written. A job that closes a potential-free contact as soon as a power outage is detected is executed once and is then finished. Even if the power outage has been resolved, the contact remains closed. If a warning light is switched on via the contact, it would light up until this contact is deliberately opened again.

The reason for this becomes clear in the following example:

If a temperature sensor causes the CS141 to send an email with a warning and close the contact for an air conditioning system when the temperature reaches a certain temperature, this is done according to the configuration. As soon as the temperature drops below the critical value, no further emails are sent with a warning about critical temperatures - but the air conditioning system must continue to run until the temperature has completely normalized. This would not work if the contact opened automatically at that moment because the event for excessive temperatures no longer exists. An active job is required to specifically switch off the air conditioning system as soon as the temperature falls below a certain value.

It becomes problematic when two UPS systems that run on separate circuits have to issue a shutdown command due to a power failure: As soon as both systems have ordered a valid shutdown, the server shuts down immediately - even if both UPS systems reported a power failure at different times and did not withdraw the shutdown command after their respective individual problems had been resolved.

Job Definition

The jobs can be configured at any time. However, they can only be tested under two conditions:

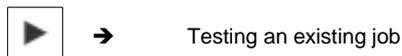
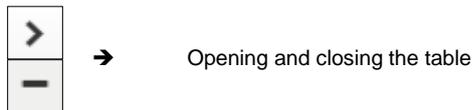
1. Jobs associated with an email account require valid login details
2. Jobs based on TCP/IP settings require valid network configuration

Before proceeding to the next configuration step, check that all access data has been entered, the network settings are correct and the CS141 is in regular operating mode in your network.

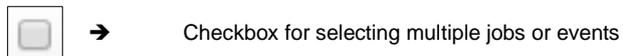
Manage jobs

In the UPS submenu, click Events to view the available system events. Please note that both the number and name of the events may vary between different UPS models.

Symbols with a clear function:



Symbols with dual function:

**Note:**

Symbols with dual functions have two different meanings. Depending on where they are used, they refer to ALL events or to a specific event or set event. This dual functionality allows a specific event to be added to certain or all system events without having to enter it individually each time.

Setting up a job

Managing jobs for a system event always follows the same rules - for this example, the following system events were selected:

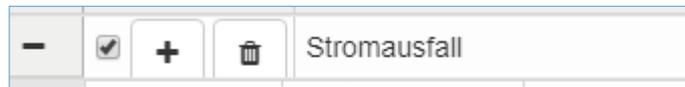
>	<input type="checkbox"/>	+	🗑️	Stromausfall	3	1	0	1	0
>	<input type="checkbox"/>	+	🗑️	Power restored	3	1	0	1	0

Click > to get a general overview of existing jobs:

-	<input type="checkbox"/>	+	🗑️	Stromausfall	3	1	0	1	0	0
				Job Typ	Wann	Parameter				
	✎	🗑️	▶	Log	Periodisch alle 100s, sofort	{"text":"Powerfail"}				
	✎	🗑️	▶	RCCMD Trap	Einmal, sofort	{"text":"Powerfail on #MODEL . Autonomietime #AUTONOMTIME min."}				
	✎	🗑️	▶	E-Mail Trap	Einmal, sofort	{}				

A total of 3 jobs are already configured for the power failure event. These jobs were loaded as a recommended standard configuration when the UPS was selected. If you want to change or remove them, click on the corresponding icon.

If you want to delete all jobs within a system event, activate the checkbox in the line for power failure and press the delete symbol. In this case, all jobs associated with this one event will be deleted from the list. This option is very useful if there are a lot of jobs.

**Note:**

Deleted jobs cannot be retrieved; they must be created again or restored from a backup. To prevent accidental deletion, this entry must be confirmed again via security prompt.

To add a job to the power failure event, press the + in the event line. This function starts the configuration menu for setting up jobs.

Available Jobs:

Job	Description
log	An entry is made in the event log.
E-mail	An email is sent
Email Trap	A trap message is sent to an E-Mail recipient.
RCCMD Shutdown	A shutdown signal is sent to one or more RCCMD clients.
RCCMD Message	An RCCMD message is sent to one or more RCCMD clients.
RCCMD Execute	A command is sent via RCCMD, causing an RCCMD client to execute a file
UPS Shutdown**	Turning off the UPS
AUX*	Turns external relays on or off.
buzzer*	If an alarm device is connected, it can be activated with this command.
RCCMD Trap	An RCCMD trap message is sent
Send WOL	Wake On LAN – a so-called magic packet – is transmitted to a network device.
Remote Command*	Control a CON_R_AUX4, or a GSM modem on another device
Send SMS*	If a GSM modem is connected, an SMS can be sent*
* Additional equipment and accessories may be required to use these features or may not be supported by your device	
** This function is only available to a limited extent: Some UPS systems support the functionality, but react very differently to this job	

Special features of the UPS Shutdown job

A UPS performs a UPS shutdown to protect the batteries from deep discharge. The UPS is physically shut down and switched off. The point in time at which a UPS performs this function varies between models within a manufacturer - in addition, each manufacturer also uses its own definitions for protecting the batteries.

Since the UPS is switched off, it is difficult to configure counter events in the process.

Definition of a UPS Shutdown

Job	UPS Shutdown	→	Selection of the job
Parameter			
Shutdown Time	<input type="text"/>	→	Time to turn off in seconds
Restore Time	<input type="text"/>	→	Time to turn on in seconds
Type	1	→	power off mode

Time to turn off in seconds

Define how long the UPS should maintain operation before shutting itself down.

Time to turn on in seconds

When the main power is restored, the UPS will wait the preset number of seconds before booting up again.

Type

This setting defines what exactly the UPS should switch off or on. There are two different settings:

- 1 The UPS switches off the output but remains operating autonomously.
- 2 The UPS switches off completely and waits until the main power is restored

Using the UPS Shutdown job

This job cannot map both settings in one; depending on the desired goal, at least two jobs are necessary. For example, you can implement the following sequence using two different jobs:

- Turn off outputs after 3 minutes
- Shut down UPS after 4 minutes
- Turn on the UPS 2 minutes after the main power supply is restored
- 15 minutes later, unlock the exits

Please note that the shutdown time and the restore time must be correctly displayed for both jobs, nested accordingly. In this case, enter either a 1 or a 2, depending on the desired event.

Search and display jobs

>	<input type="checkbox"/>	+	Ereignis	Jobs	Log	E-Mail	E-Mail Trap	RCCMD Shutdown	RCCMD Nachricht	R
			contains...	<input type="text"/>						

The search function is a quick and easy way to find configured jobs within the events. You have two basic options:

Event: contains...

If you are looking for a specific event, you can use this bar to display all matching events by entering a word or word fragment.

Jobs

Enter the number of configured jobs here and all events with this number of jobs will be listed. During setup, some parameters change depending on which job is selected.

The selection of the job defines which parameters are displayed:

Example 1: Log files- which text should appear in the event log?

Example 2: RCCMD- Which IP address should receive the message, and which port should be listened to?

The parameters differ depending on which job was selected.

[Job Definition: Selectable time windows:](#)

The CS141 offers many system events to which a job can be assigned. Some system events can be assigned clear conditions, each using different time calculations:

Immediately, one-time execution:

After XXX seconds:

Repeat every XXX seconds:

After XXX seconds on battery:

With XXX seconds remaining:

Once the event occurs, this job is executed exactly once.

As soon as the event occurs, the job waits for the set time in seconds before executing. If the event ends before then, the job will not be executed.

The job is repeated cyclically until the event no longer exists.

The event must occur, and the UPS must be running in autonomous mode for a preset time. For example, if 300 seconds is set, this job will only run if the UPS has been in autonomous mode for at least 300 seconds.

The job is executed when the remaining runtime of the UPS is reached or exceeded based on the actual attached load.

[Time management of jobs in relation to the UPS](#)

Time management for jobs to be carried out is difficult because you must conceptually distinguish between two different perspectives. The example of a power outage makes this difference clear:

In the event of a power failure, the UPS takes over the power supply and ensures the operation of the servers until one of two events occurs:

1. The batteries are exhausted
2. The main power supply has been restored.

When the UPS switches to the so-called autonomous mode, two different times run:

A linear forward-running clock in seconds starting at 0.

If a job is to be executed after 45 seconds, it will only be executed if the event has been pending for at least 45 seconds. If the event ends earlier, the job will not be triggered.

A relative clock that counts down depending on the connected load.

This time measurement is based on a relative value that considers the connected load. For example, if the UPS allows 7 minutes of autonomous operation at 100% load, it will last 50% longer at 50%, i.e. 10.5 minutes:

Therefore, following the logic, if devices are switched off after 3 minutes and the load drops to 50%, the clock would jump from 4 minutes to 7.5 minutes.

Both counting methods have their specific advantages and disadvantages:

One counter gives a clear indication of a time sequence and ignores the actual remaining running time. If there are several small power outages in succession, a server shutdown after exactly 7 minutes would not take effect if there were only enough power available for 6 minutes.

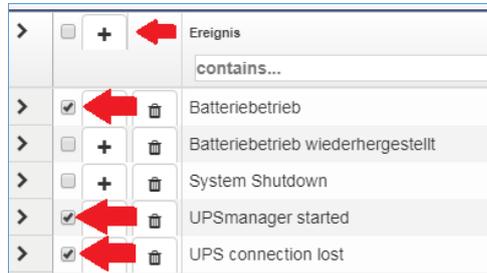
The other counter is difficult to calculate and there is a time offset between the tasks being carried out. 5 minutes of remaining running time cannot be achieved even over a longer period of time if the framework conditions increase the remaining running time, or a predetermined sequence of events can be disrupted as soon as the circumstances correct this time downwards.

Note:

In principle, the shutdown over the remaining running time makes sense, as the actual battery charge can be included in the calculation. However, if other jobs have to be carried out in a specific order, it makes sense to use the linearly forward-running clock for scheduling.

Add Multiple Jobs

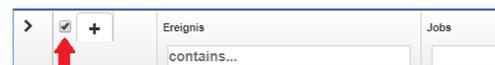
In some circumstances, a configuration may require that the same job be assigned to several events. To assign these jobs to an event, it is possible to select each event individually and define a job.



The faster way is to select the events that should receive the same job and then click on the remote upper **+**.

In this case, the same job is created for each selected event.

Activate the check box in the top row if an event should be assigned to all events - all events will be selected. To assign a job, press the **+** in exactly this line.



Deleting jobs

If certain system events are no longer relevant for the configuration, it is possible to remove these jobs from the system configuration:

- Delete a job

Fold with > the desired tab:

Batteriebetrieb			
	Job Typ	Wann	
	Log	Einmal, sofort	
	RCCMD Trap	Einmal, sofort	

Select the desired job and click the small trash can icon to immediately and permanently remove it from the configuration.

- Delete all jobs within an event

Batteriebetrieb			
	Job Typ	Wann	
<input checked="" type="checkbox"/>	Log	Einmal, sofort	
<input checked="" type="checkbox"/>	RCCMD Trap	Einmal, sofort	

Select the checkbox for the event to delete all jobs within this event together.

Note:

You can delete, create or edit any job within an event. The event itself is specified by the system and cannot be deleted.

Assign jobs to counter events

Some jobs must be explicitly canceled as soon as an opposing event occurs:

- Information from those responsible / "all clear"
- Further actions
- Initiated server shutdowns
- ...

Configuring a counter job follows the same pattern as creating a job. The time management described above is important in this context, since the UPS was in autonomous mode and needed a certain amount of time to charge the batteries.

Example scenario:

The UPS has switched to autonomous mode due to a power failure and can keep all connected devices running for 60 minutes at 100% load. With 30 minutes remaining, many computers are automatically shut down, reducing the load to 20%. The remaining runtime is adjusted upwards accordingly. Since all systems are only shut down when there are 5 minutes remaining, but the power failure was eliminated after 6 minutes, normality is restored.

In this case, the CS141 can restart all computers that have been shut down to protect the remaining runtime via Wake on LAN (WOL) – a fact that is desirable.

If in this scenario all connected computers were to be restarted automatically, this would mathematically mean that the UPS could last for 6 minutes with 20% load during the next power outage - but would have to deliver 100% load. Since this cannot work, the WOL packet must be sent with a time delay to give the UPS the opportunity to carry out a minimum charge of the batteries.

Note:

Up to 50 jobs can be created per system event. Please note that individual jobs may contradict each other and desired jobs may be reversed with counter jobs.

Custom Thresholds

For this configuration step you need the following menu:



Some UPS models allow you to individually set the limits for some UPS-specific events.

The CS141 supports these functions if the UPS provides this option. If this is not the case, you will be informed via a corresponding system message. The configuration is done via two different menus:

- In the Custom Thresholds you define which measured values are read out and
- Under UPS > Events, assign jobs to the events accordingly

Warning Levels			
		Min	Max
<input type="checkbox"/> Battery Voltage	out of range	0 V	0 V
<input type="checkbox"/> Input voltage P-N	out of range	0 V	0 V
<input type="checkbox"/> UPS Temperature	out of range	0 °C	0 °C
<input type="checkbox"/> UPS Autonomy	less than	0 m	
<input type="checkbox"/> Battery Charge	less than	0 %	
<input type="checkbox"/> Output Load	less than	0 %	
<input type="checkbox"/> Seconds on Battery	greater than	0 s	

Difference between Warning and Alarm Levels

The Custom Thresholds are identical for Warning and Alarm Levels – however, they are listed separately in the UPS events and can contain different values and are listed in the log files as Warning or Alarm.

This is necessary in order to be able to configure both the warning and alarm behavior differently.

The following conditions can be met:

- out of range** The event – regardless of whether it is an alarm or warning – is triggered when the measured value falls below or exceeds the entered values.
- less than** The event – regardless of whether it is an alarm or warning – is triggered when the measured value falls below the entered value.
- greater than** The event – regardless of whether it is an alarm or warning – is triggered when the measured value exceeds the entered value.

Example configuration: UPS Temperature:

All electrical devices have a minimum and a maximum temperature within which they can be operated safely. If these temperatures are exceeded or not met, anything can happen, from simple defects to an acute fire hazard. To be able to intervene in time, a specified temperature must be compared with the measured temperatures:

For example, if the manufacturer specifies the “safe operating temperature” as being between +5°C and +39°C, a warning could be issued at both +5°C and +39°C:

The out-of-range condition first defines what lies outside this range.

The configuration takes place in two separate menus:

- Custom Thresholds:

The first setting is made under Custom Thresholds, where the corresponding values are specified.

Warning Levels			
		Min	Max
<input type="checkbox"/> Battery Voltage	out of range	0 V	0 V
<input type="checkbox"/> Input voltage P-N	out of range	0 V	0 V
<input checked="" type="checkbox"/> UPS Temperature	out of range	10 °C	34 °C
<input type="checkbox"/> UPS Autonomy	less than	0 m	

Click the check box to include this entry in the UPS events. For the argument out of range, enter the lowest permissible temperature for Min and the highest permissible temperature for Max.

Note:

Since this is the warning, it should be issued before the critical values are reached, which in this case are +5°C and +39°C respectively. Therefore, the values must be corrected accordingly. In this example, the warning with +10°C and +34°C was corrected by 5°C each.

Click Apply to save the configuration.

- UPS events

Look for the necessary entries in the UPS events. Unlike in the Custom Thresholds menu, the individual thresholds are displayed like regular system events in order to be able to map all states:

>	<input type="checkbox"/>	+		UPS Temperature Threshold Warning Low On	1	1	0	0	0
>	<input type="checkbox"/>	+		UPS Temperature Threshold Warning Low Off	1	1	0	0	0
>	<input type="checkbox"/>	+		UPS Temperature Threshold Warning High On	1	1	0	0	0
>	<input type="checkbox"/>	+		UPS Temperature Threshold Warning High Off	1	1	0	0	0

Since the custom thresholds can be configured like regular UPS events, all jobs are available.

[Setting the alarm levels](#)

Alarm Levels			
		Min	Max
<input type="checkbox"/>	Battery Voltage	out of range	0 V
<input type="checkbox"/>	Input voltage P-N	out of range	0 V
<input checked="" type="checkbox"/>	UPS Temperature	out of range	6 °C
<input type="checkbox"/>	UPS Autonomy		0 m

The alarm levels form the escalation level of the warning levels and are displayed separately in the UPS events with all 4 possible statuses:

>	<input type="checkbox"/>	+		UPS Temperature Threshold Alarm Low On	1	1	0	0	0
>	<input type="checkbox"/>	+		UPS Temperature Threshold Alarm Low Off	1	1	0	0	0
>	<input type="checkbox"/>	+		UPS Temperature Threshold Alarm High On	1	1	0	0	0
>	<input type="checkbox"/>	+		UPS Temperature Threshold Alarm High Off	1	1	0	0	0

Since the alarm levels represent an escalation level and are intended to trigger emergency measures if necessary, the values must be adjusted accordingly. Since the condition for an alarm is met in addition to the warning, poorly configured jobs can be executed in parallel, overlap or even contradict or cancel each other out.

Example excerpt: Custom Thresholds

This list is an example; depending on the UPS model and manufacturer, this list can vary in both name and range of functions. The example list is provided by an Alerex Kronos UPS:

		Min	Max	Logic	OnBattery	OnBypass	Overload	OverTemp
<input type="checkbox"/> Battery voltage	out of range	0 V	0 V	Or	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Battery Temperature	out of range	0 °C	0 °C	Or	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> UPS Temperature	out of range	0 °C	0 °C	Or	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[...]								
<input type="checkbox"/> Output load L2	greater than	0 %		Or	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Output load L3	greater than	2 %		And	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Seconds on Battery	less than	50 s		And	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Battery Autonomy	less than	50 m		And	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Battery charge	less than	50 %		Or	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Battery symmetry pos./neg. String	greater than	0 V		Or	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Battery Voltage *out of range* XX V – XX V

Batteries are sensitive to voltages; excessive voltages and deep discharges can cause permanent damage. This value can be used to provide timely warnings of such events as soon as they entered range in volts is exceeded.

Input voltage PN *out of range* XX V – XX V

Some UPS systems provide the measurement data of the input voltage on request. This value can be used to set up an alarm in the event of voltage drops or overvoltage in the power grid.

UPS Temperature *out of range* XX°C – XX °C

Some UPS systems have internal temperature sensors. This value can be used to define an additional alarm behavior based on the temperature values that the UPS delivers in that case.

UPS Autonomy *less than* XX m

In some cases, it may be useful to define an additional alarm behavior based on the time a UPS has available in autonomous mode in minutes - for example, if jobs are provided with a forward-running time delay and there is not enough time available due to several short power outages in a row: An emergency behavior could be defined, for example an alarm shutdown.

Battery Charge *less than* XX%

After a UPS has been in autonomous operation, the batteries are automatically recharged. For example, if there have been several short power outages in a row, this value can be used to define additional early warning behavior.

Output Load *less than* XX%

Some UPS systems offer a measurement value that shows the actual load applied in real time. If non-relevant systems are shut down in the event of autonomy, this value could be used to implement confirmation or warning behavior.

Battery Symmetry Pos./Neg. *greater than*

Some UPS systems use both the positive and negative half-wave of AC power. This setting defines the alarm behavior when the positive battery string and the negative battery string are not charged evenly.

Seconds on Battery *greater than* XX s

In some cases, only a voltage drop is recorded, for example when large industrial plants are put into operation. In this case, a UPS may switch to autonomous mode. This value in seconds could be used to implement an additional warning that „real case of autonomy“ verified.

Note:

Pay close attention to the arguments associated with the thresholds:

Greater than, less than, in range, out of range – since arguments are taken literally as conditions, the warning and alarm behavior is interpreted accordingly. For example, with Output Load less than 67% a warning will be issued if the value falls to 43%, while at 68% no warning will be issued.

Example scenario: Custom Thresholds

The problem:

SITEMANAGER 7 recognizes the UPS correctly, but contactors are to be controlled via potential-free contacts, which switch off external devices as soon as the battery charge falls below a certain percentage.

This configuration is possible, but only indirectly:

Since A SITEMANAGER 7 provides internal relays, this configuration can be carried out without any additional hardware. Things get difficult when the according UPS does not provide required events by default:

As a result, these will not be displayed under Devices/Systems>UPS>Events. The custom thresholds can be used for this task - once enabled, a freely definable job will be added to the UPS event list.

If you set Warning Levels to 71% and Alarm Levels to 61%, you can then assign a corresponding behavior to the UPS events:

- In this case, when the battery charge drops to 70%, the first devices will be switched off.
- When the battery charge drops to 60%, the next devices will be turned off.

The counter events are then set to Warning OFF or Alarm Off accordingly.

Since the batteries are being charged, the devices are started using the Battery Charge value:

- ➔ From 61% the devices are switched on again,
- ➔ From 71% the second devices are switched on again

Since there is no AND connection to the power fail, these events are repeated until the set percentage value is reached, or are executed once, depending on the setting. If devices are switched off at 70% and switched on at 61%, there could be conflicts between the events, so the devices should be consistently configured to one value.

If another power failure occurs between 0% and 71%, the devices would either remain off or be switched off again a short time later.

Additional devices could then be triggered independently as a job over the remaining runtime via the Power Fail and Power Restored events:

Since the remaining running time adapts dynamically to the load, these devices would only be switched off once it has actually reached the value X in minutes. When power is restored, the corresponding counter event is then configured.

RCCMD

What is RCCMD

RCCMD (Remote Console Command) is the world's most successful shutdown client for heterogeneous networks and is the safest way to send a variety of messages and To initiate shutdown sequences from the UPS. The RCCMD clients listen on port 6003 for an RCCMD server, which is generally part of a UPSMAN software, a CS141 or RCCMD-licensed UPS manager

An RCCMD server controls the RCCMD clients in the network in the event of a UPS alarm. The range of functions extends from notices and notifications to an orderly shutdown of a multiple server environment, where mutual dependencies must be taken into account.

Note:

The RCCMD client is not freeware, a separate license is required, which you can purchase worldwide from licensed resellers, OEM partners or via the web shop at www.generex.de. The license itself is valid indefinitely, and the service includes 2 years of free updates from the date of purchase.

The screenshot shows the configuration interface for Warning Levels and Alarm Levels. The 'Warning Levels' section has the following settings:

Parameter	Condition	Min	Max	Logic
Battery voltage	out of range	0 V	0 V	Or
Battery Temperature	out of range	0 °C	0 °C	Or
UPS Temperature	out of range	0 °C	0 °C	Or
Seconds on Battery	less than	50 s		And
Battery Autonomy	less than	50 m		And
Battery charge	less than	50 %		Or
Battery symmetry pos./neg. String	greater than	0 V		Or

The 'Alarm Levels' section has the following settings:

Parameter	Condition	Min	Max	Logic
Battery voltage	out of range	0 V	0 V	Or
Battery Temperature	out of range	0 °C	0 °C	Or
UPS Temperature	out of range	0 °C	0 °C	Or
Seconds on Battery	greater than	0 s		Or
Battery Autonomy	less than	0 m		Or
Battery charge	less than	0 %		Or
Battery symmetry pos./neg. String	greater than	0 V		Or

Configuring RCCMD

On the RCCMD server, RCCMD commands are defined as jobs via the system events. There are three different job categories available:

RCCMD Shutdown

The RCCMD – Shutdown sends a signal to an RCCMD client that causes the client to shut down the computer in an orderly manner according to its configuration.

RCCMD Message

An RCCMD message is a notification text that can be sent to an RCCMD recipient and displayed on the screen via a message box.

RCCMD Execute

If scripts need to be executed prior to a shutdown, they can be executed using an Execute command. In addition to ready-made commands, RCCMD also offers the option of starting your own scripts.

RCCMD Trap

Trap messages are purely informational messages that can be sent to an RCCMD client. The client receives these text messages and displays them in a message box.

Note:

Once an RCCMD shutdown has been initiated, it cannot be undone. However, you can define redundancies within the RCCMD client and restrict IP addresses that are authorized to send an RCCMD shutdown.

Setting up an RCCMD job

RCCMD works based on IP addresses to control devices within a network or network segment. While some parameters are valid for all RCCMD jobs, there are some differences in the parameters depending on the job.

→ Drop-Down Menu for Job selection

- Send RCCMD Signals as broadcast (UDP)
- Target IP Address
- Port of the RCCMD Listener

→ Customizable Job conditions for sending a job

Setting the IP address for RCCMD

broadcast

If you activate this checkbox, a so-called broadcast is sent to your network segment. Every RCCMD client installed in this network segment is addressed and responds by shutting down and turning off the computer. No distinction is made between host, virtual machine, individual server or workstation.

Limiting to IP addresses

If you want to address a specific machine within your network, enter the direct IP address here. Only the addressed computer - whether physical or as a virtual machine - will be addressed. You can create a single job for each RCCMD client or combine several IP addresses into one job:

... one job per IP address ...

... multiple IP addresses with one collective job

If you have multiple IP addresses, please pay close attention to the syntax: 192.168.3.1,192.168.3.18 ...

There must be no spaces between the individual entries and the comma, otherwise you will receive an error message.

Note:

Broadcast and individual IP addresses or collective addresses are mutually exclusive. If you want to shut down devices and device groups first and then send a broadcast, create another job with an appropriate delay.

Keep in mind: The RCCMD Client is a unique software that needs local configuration on site! For more information, documentation and download resources about RCCMD, visit www.generex.de.

Port

The standard port for RCCMD commands is port 6003 - the RCCMD client listens for an RCCMD command on this port. If your RCCMD client was assigned a different port during installation and configuration, please adjust the data so that the sender and receiver are on the same port.

Define time for RCCMD

Under Time, specify the timing of the job. You can choose from:

- *Immediate, one-time execution*

The job is executed immediately when the event occurs.

- *After XXX seconds*

The CS141 waits a preset time before executing the job. If the circumstances change and the job becomes obsolete, it will no longer be executed

- *After XXX seconds, repeat every XXX seconds*

The job is started after a preset time and then repeated cyclically until the event is no longer pending or the circumstances make it impossible to execute - for example, if the UPS batteries are exhausted and the UPS has switched itself off to prevent deep discharge.

- *After XXX seconds on battery*

The job will only run if the UPS runs on battery for a preset value in seconds in autonomous mode.

- *With XXX seconds remaining*

The CS141 only carries out this job when the overall remaining running time has reached a certain value in seconds. Since the value can shift with the actual load attached, it is possible that this condition can be reached multiple times. This happens, for example, when the overall load drops due to a machine being shut down and the remaining running time is again above the set value.

The RCCMD commands

The RCCMD Shutdown

Parameter	
IP	<input type="checkbox"/> Broadcast 192.168.3.1
Port	6003

The RCCMD shutdown is predefined and causes the addressed RCCMD client to shut down the operating system and turn off the device.

The RCCMD Message

Parameter	
Text	Am Brunnen, vor dem Tore, da steht ein...
IP	<input type="checkbox"/> Broadcast 192.168.3.15
Port	6003

The RCCMD message is a text message that you can define freely. The text field automatically moves with the text entered as soon as you reach the right edge. This message will then appear as a notice in an alarm box on a computer with the RCCMD client installed. RCCMD also displays a box with a warning message on the taskbar.

Configuring an RCCMD Execute

Parameter	
IP	<input type="checkbox"/> Broadcast 192.168.3.1
Port	6003
Command	hallowelt.bat

A comprehensive function within RCCMD is that you can directly run your own executable files and batch files on a target device. This function is useful if, for example, scripts still need to be run before a shutdown. To do this, place the file to be executed in the client in the RCCMD directory. You can then name the file to be executed directly as RCCMD Execute.

Note:

In the screenshot you can see that hallowelt.bat was entered under Command. In this case, the RCCMD client on the PC with the IP address 192.168.3.1 would try to start the file hallowelt.bat directly.

The RCCMD Traps

RCCMD traps are pure messages intended to inform about the current status of the UPS. A special data packet is generated which can be received, read and interpreted by the corresponding program.

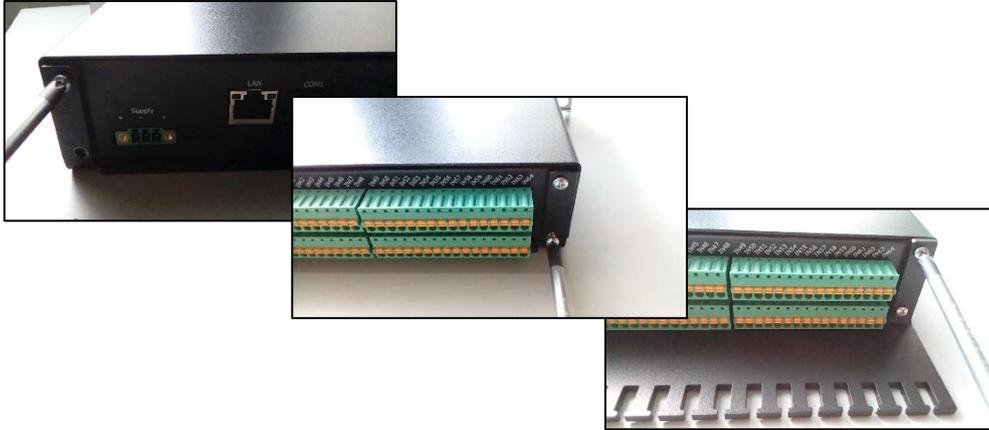
The following list contains possible variables that you can use to define RCCMD traps:

Trap Code	Description
#AGENTSOFTRVCS141	Firmware Version
#AUTONOMTIME	Autonomy time in minutes
#BATT2OLD()	Time in months until the event "Please check batteries"
#BATT2OLD_YEARS	Battery age years
#BATTCAP	Battery capacity in %
#BATTINSTDATE	Battery installation date
#BATTTESTDATE	Date of last battery test
#BATTVOLT	Battery voltage in V
#CHARGECURR	Current charging current
#CNT_BL	Counter for battery low events
#CNT_PF	Counter for power fails
#CNT_SA	Counter Active Shutdowns
#CNT_SD	Counter Shutdowns
#CNT_TF	Counter test error
#DATE	Current date
#EVENTSTATE	OBS status (idle, error, progress, success)
#FULLTESTDATE	Date of the last full test
#GETLASTRESULT()	Results from the last test performed
#HOLDTIME	Runtime at 100 percent load
#IDENT_NAME	Name of the SNMP adapter
#INCURRO/1/2	Input current in V
#INFREQ0/1/2	Input frequency in Hz
#INPHASES	Number of input phases
#INPUTCURRENT0/1/2	Current input current in V
#INVOLT0/1/2	Input voltage in V
#LASTERR	Last error
#LOAD	Current load
#LOCATION	Location
#MANUFACTURER	manufacturer of the UPS
#MODEL	UPS model
#OUTFREQ0/1/2	Output frequency in Hz
#OUTPHASES	number of output phases
#OUTPOWER0/1/2	Load in percent
#OUTPUT_VOLT0/1/2	Output Power in V
#OUTPUTCURRENT0/1/2	Output Current in Ampere
#OVERLOAD	Overload
#PHASES	Available UPS phases
#POWER	Performance
#RECHARGETIME	Time to full charge
#RESTORETIME	recovery time
#RUNTIME	Running time since last commissioning / Maintenance
#SECONBAT()	Seconds on battery power
#SELFTESTDATE	Date of the last self-test
#SERVER	IP of the SNMP adapter
#STATUS	System status
#SYSDATE()	system date
#SYSTEMTIME()	system time
#TEMPDEG	Temperature in °Celsius
#TIMEZONE	Current time zone
#VOLTAVAI	UPS related, // UPS has a way to query the input voltage

SITEMANAGER 7 - specific devices and sensors

The cable comb

There are 4 screws on the back of the device – these hold the cable comb in the delivery position:



Note:

If you have not activated the Hold function and confirm a current alarm with ACK, this alarm behavior is also triggered, and the state is held accordingly

The difference is that without the hold function the alarm can be optionally confirmed, whereas the alarm with the hold function active must be confirmed.

Sensors And Devices

The SITEMANAGER 7 has 8 analog and 8 digital inputs, which can be operated either via regular plugs or via the terminal block.

Please note that you either use pre-assembled cables with the corresponding analog sensors or use the connections via the terminal block:



The following should be noted:

AN 1 and AN 2	Sensor Input 1
AN 3 and AN 4	Sensor Input 2
AN 5 and AN 6	Sensor Input 3
AN 7 and AN 8	Sensor Input 4

So, you can connect an analog standalone sensor to Sensor Input 1 via the cable and attach another sensor to AN 2 via the terminal block. If you connect two sensors to Sensor Input 1, the two connections AN1 and AN2 are assigned accordingly.

In addition, there are up to 8 digital inputs that can be connected via the terminal block:

The lower terminal block provides a 12 V power supply via the plus and minus poles, which are operated in a similar way to the SITEMONITOR:

If you want to use the digital input directly with an external switch or relay, select the negative pole as the reference source in order to provoke a corresponding high signal at the input. If you also equip external sensors or switching devices with a power supply, you can tap the necessary power supply via the lower terminal block and then place the digital contact on the corresponding digital input.

Although the SITEMANAGER offers fewer digital inputs than the SITEMONITOR, it can manage 8 analog sensors and has 8 pre-integrated relays to activate outputs.

SITEMANAGER 7 Sensor Setup

For this configuration step you need the following menu:



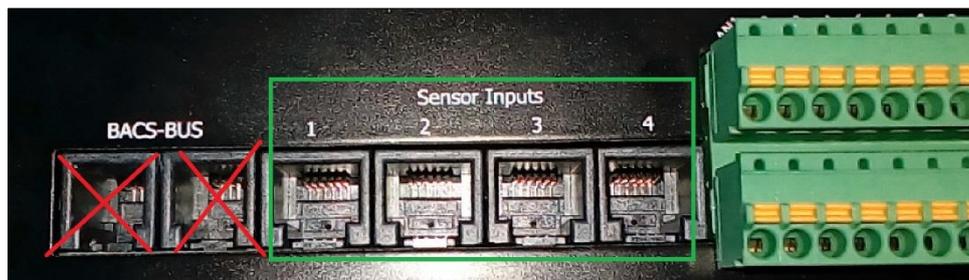
The SITEMANAGER 7 offers a significant difference to the CS141 with its optional modules. Due to the connection, the UPS interface COM1 is a MINI-DIN connection, the serial 9-pin SUB-D connection is used internally for other purposes to map the additional functionality.

Sensors are important for a SITEMANAGER 7, because they provide a wealth of information about the environment that can be relevant for the operation of systems. This includes humidity, air pressure, temperatures, etc. If systems are operated outside of their regular operating environments, they can be damaged or, in the worst case, destroyed.

One of the special features of the SITEMANAGER 7 is the ability to manage up to 8 sensors, analog and digital inputs and assign specific system events to them. Furthermore, the SITEMANAGER 7 is the only device in the CS141 family to offer 4 output relays for switching external systems or defining switching states for target devices.

connection of the sensors

The sensors are connected in a similar way to the GENEREX sensor manager - on the back of the SITEMANAGER II/V6 you will find the corresponding connections to the left of the terminal block with the analog and digital inputs.



When connecting the sensors, do not confuse the sensor inputs with the input sockets of the BACS-BUS – the plugs of the sensor cables are assembled differently and can therefore mechanically damage the BACS bus sockets

In total, up to 8 sensors can be connected - each sensor input is assigned to 2 channels. Basically, you can distinguish between two different sensors:

- The Single Sensor

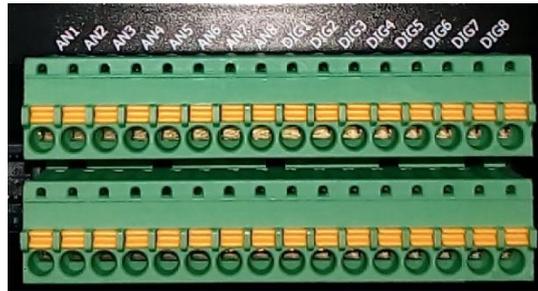
This sensor offers the possibility to connect a second sensor in series.

- The combination sensor

This sensor consists of two different sensors which are housed together in one housing. In this case, both channels are assigned to one sensor input for the sensor.

When connecting, please make sure that you connect the correct sensors in series, otherwise you may be missing a sensor in the configuration.

Using the analog and digital connections



If you want to connect your own sensors directly, the SITEMANAGER II/V6 offers you the option of using a terminal block. The following key is used:

- AN1 / AN2 Sensor Input 1
- AN3 / AN4 Sensor Input 2
- AN5 / AN6 Sensor Input 3
- AN7 AN8 Sensor Input 4

The corresponding operating voltage or reference points can be obtained from the second terminal block below.

The configuration screen in SITEMANAGER is divided into 3 parts

Analog sensors

Sensor Inputs	Name	Sensortype	Unit	Low Alarm	Low PreAlarm	High PreAlarm	High Alarm	Sensor Range	Offset
1	1 Temperature Testlab 1	SM_T_H	°C	5 <input type="checkbox"/>	2 <input checked="" type="checkbox"/>	29 <input checked="" type="checkbox"/>	34 <input checked="" type="checkbox"/>	0 - 100	
	2 Humidity Testlab 1	SM_T_H	% rel H	1 <input checked="" type="checkbox"/>	2 <input type="checkbox"/>	81 <input checked="" type="checkbox"/>	90 <input checked="" type="checkbox"/>	0 - 100	
2	3 Temperature Testlab 2	SM_T_H	°C	1 <input type="checkbox"/>	2 <input type="checkbox"/>	28 <input checked="" type="checkbox"/>	34 <input checked="" type="checkbox"/>	0 - 100	
	4 Humidity Testlab 2	SM_T_H	% rel H	1 <input type="checkbox"/>	2 <input type="checkbox"/>	81 <input type="checkbox"/>	91 <input checked="" type="checkbox"/>	0 - 100	
3	5 - H2 Gas Concentration	Custom 0-10V	%	1 <input type="checkbox"/>	2 <input checked="" type="checkbox"/>	35 <input checked="" type="checkbox"/>	45 <input checked="" type="checkbox"/>	0 - 100	
	6 - Dieseltank Generator	Custom 0-10V	Liter	2 <input checked="" type="checkbox"/>	3 <input type="checkbox"/>	95 <input type="checkbox"/>	99 <input checked="" type="checkbox"/>	0 - 100	
4	Channel 7 not connected	Custom 0-10V		1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 10	
	Channel 8 not connected	Custom 0-10V		1 <input type="checkbox"/>	2 <input type="checkbox"/>	8 <input type="checkbox"/>	9 <input type="checkbox"/>	0 - 10	
Hysteresis				3					

After you have connected a sensor, define the type of sensor at "Sensor type". Please note that the individual channels are routed out in pairs.

Sensors 1 and 2 form a channel pair, sensors 3 and 4 form one, etc.

When you set a combination sensor on a channel, the corresponding twin is automatically adjusted. The corresponding unit is automatically preset.

definition of alarm thresholds

The sensors offer several possibilities to be adapted to the operating environment. As an example, in this case a temperature sensor is adapted.

Low Alarm	Low PreAlarm	High PreAlarm	High Alarm	Sensor Range
5 <input type="checkbox"/>	2 <input checked="" type="checkbox"/>	29 <input checked="" type="checkbox"/>	34 <input checked="" type="checkbox"/>	0 - 100

sensor area

The sensor range defines the area that is measured. The 0 defines 0°C and the 100°C - if you are operating a deep-freeze room, you would have to adjust the value downwards accordingly, whereas in a generator room in the desert temperatures of up to 80°C could be a realistic value. In this example, a room is to be monitored whose systems can be operated between 5°C and 45°C.

To adjust the scale to the realistic value, you would design the scale from 0°C to 60°C. That should be enough.

pre-alarm and alarm

The pre-alarm is the alarm instance where increased vigilance is required. There are no problems in this area yet, but the temperature is worrying. Alarm is the instance where an immediate reaction should be made, otherwise the systems could be damaged.

In this example, the lower limit for operation is 5°C – this raises two interesting questions:

1. What is the average temperature during operation
2. How should temperature fluctuations due to operation and environmental influences be evaluated?

A poorly ventilated or heated room can easily reach 50°C in summer, while in winter temperatures can be below freezing. If the general temperature is on average 15°-20°C, the lower and upper values can be defined very well:

The pre-alarm should therefore be triggered BEFORE the actual alarm. So at around 10°C - sending emails can be stored as a job as an event later on. The alarm, however, is triggered at 6°C. Here, for example, the shutdown of the system can be defined in connection with alarm and notification emails.

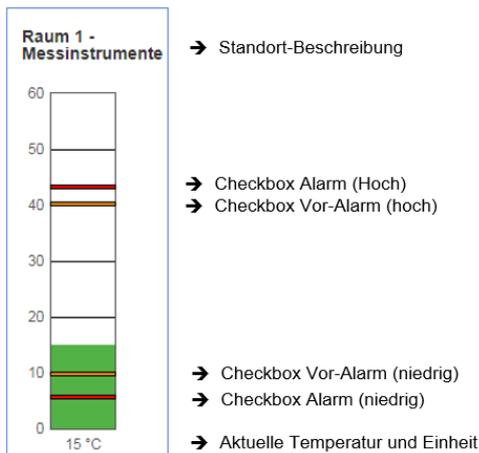
The upper range is defined similarly: The VOR alarm is set at 40°C, while the alarm itself is triggered at 43°C and initiates appropriate emergency measures. The

Adjusted, the temperature line would look like this:

Sensor Inputs	Name	Sensortype	Unit	Low Alarm	Low PreAlarm	High PreAlarm	High Alarm	Sensor Range	Offset						
1	1 Temperature Testlab 1	SM_T_H	°C	5	<input checked="" type="checkbox"/>	2	<input checked="" type="checkbox"/>	29	<input checked="" type="checkbox"/>	34	<input checked="" type="checkbox"/>	0	-	100	
	2 Humidity Testlab 1	SM_T_H	% rel H	1	<input checked="" type="checkbox"/>	2	<input type="checkbox"/>	81	<input checked="" type="checkbox"/>	90	<input checked="" type="checkbox"/>	0	-	100	

The checkbox defines whether this value is activated or should be ignored.

You can then see the result in the Sensor Monitor:



The digital inputs

SiteManager Inputs							
Eingang	Name	NC-Kontakt	Aktiv	Eingang	Name	NC-Kontakt	Aktiv
1	Input 1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	5	Input 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Input 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	6	Input 6	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Input 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7	Input 7	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	Input 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	8	Input 8	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Übernehmen

The digital inputs are configured similarly to the sensors.

The following settings are possible:

name

Enter a clear name for the entrance in the free text. Since the associated systems may be located in other parts of the building, make sure the name is clear.

NC Contact

This setting defines whether a contact should normally be closed or open. Different sensors or systems handle this very differently. Since the digital input can only detect high/low signals, it is important to know which value represents the normal state.

Active

This checkbox activates or deactivates the contact according to your specification.

SITEMANAGER 7 Outputs

The outputs offer the option of actively switching a relay contact. These are later displayed in the sensor monitor and on the front of your SITEMANAGER 7 in the LED group Digital Outputs. In some cases, it is necessary that relay contacts are switched automatically at start-up.

In other cases, the relay contacts must be switched with a time delay or are used via explicit jobs.

SiteManager Outputs							
Ausgang	Name	Anschalten	Delay	Ausgang	Name	Anschalten	Delay
1	<input type="text" value="Output 1"/>	<input type="checkbox"/>	<input type="text" value="0"/>	5	<input type="text" value="Output 5"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text" value="Output 2"/>	<input type="checkbox"/>	<input type="text" value="0"/>	6	<input type="text" value="Output 6"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text" value="Output 3"/>	<input type="checkbox"/>	<input type="text" value="0"/>	7	<input type="text" value="Output 7"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text" value="Output 4"/>	<input type="checkbox"/>	<input type="text" value="0"/>	8	<input type="text" value="Output 8"/>	<input type="checkbox"/>	<input type="text" value="0"/>

name

Give the output a unique name. This will later be displayed in the Event Log and Sensor Monitor.

switching on

Define whether the SITEMANAGER should automatically switch these outputs when restarting.

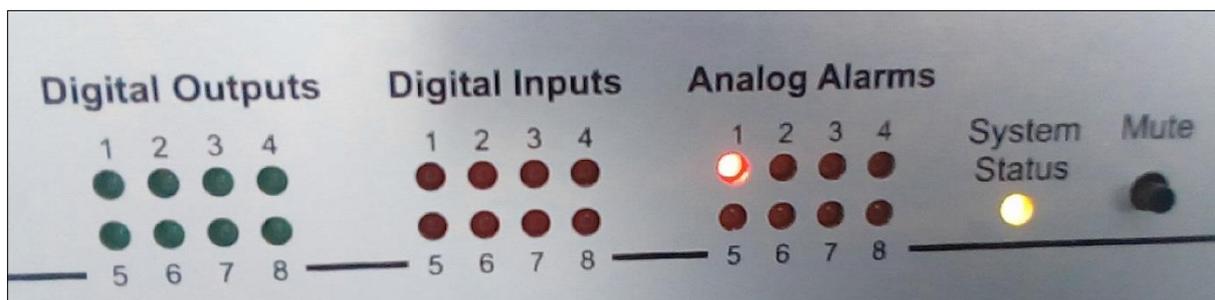
delay

Defines the time delay when switching in seconds.

Advanced Monitoring

SITEMANAGER 7 communicates via 2 ways to report problems:

On the front panel there are status LEDs logically assigned to all possible connections:



Digital Output

LED color: green

These LEDs light up when you have switched a digital output

Digital Input

LED color: red

These LEDs flash when a problem is detected

The flashing becomes a static light as soon as the error has been confirmed in SITEMANAGER II/V6

Analog Alarms

LED color: red
 These LEDs flash when a problem is detected.
 The flashing becomes a static light as soon as the error is confirmed by the SITEMANAGER 7

The system status LEDs

This LED is assigned to the BACS system, for which there is a separate manual.

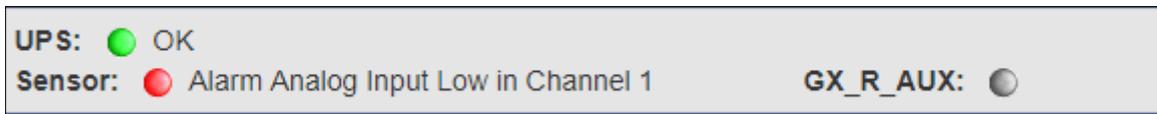
Special feature: Power LED

LED color: green
 The power LED indicates different system states:

The LED...

- Lights up statically green when the system is properly connected internally and is functioning.
- Flashes green when the BOOT process has been initiated or there is no connection to the CS141.

In addition to the LEDs, you can use the Sensor Monitor screen to obtain more detailed information about the switching states. After logging in, the upper status bar provides quick information:



As soon as you confirm in the Sensor Monitor, the LED will behave accordingly:



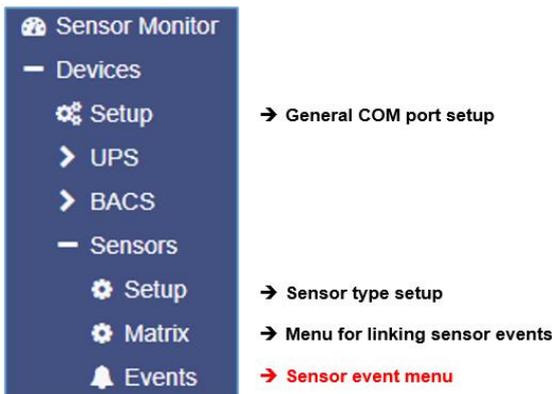
The sensor monitor will initially assume that this state is somehow intended:



However, the LED on the front panel will continue to glow static red to indicate a corresponding error during the next maintenance.

SITEMANAGER 7: Assign an event to sensors

For this configuration step you need the following menus:



The definition of events is important for emergency measures. Please note that these events refer to the alarm behavior, but not to the pre-alarms that appear in the monitoring.

Assigning system events to analog inputs

The event: Alarm Analog Input 1:

>	+	-	Alarm Analog Input 1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
---	---	---	----------------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Jobs associated with this event determine what should happen when an alarm condition is reached.

The counter event: Alarm Analog Input 1 off

>	+	Alarm Analog Input 1 off	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
---	---	--------------------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Jobs assigned to this event determine what should happen when the alarm state is exited.

Click > to get a general overview of existing jobs > Open the list of configured events to see the corresponding preconfigured jobs.

-	+	Alarm Analog Input 1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
		Job Typ	Wann		Parameter												
		Log	Einmal, sofort		{"text":"Alarm Analog Input 1"}												

With +, open the configuration dialog for the job definition.

Note:

The executable jobs are the same as those that can be triggered by UPS events. This allows environmental control sensors to be fully integrated into warning and alarm behavior. Please note that other sensors may provide different setting options depending on their function.

Assigning system events to digital inputs

Search for Alarm Digital Input

-	+	Alarm Digital Input 1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
		Job Typ	Wann		Parameter												
		Log	Einmal, sofort		{"text":"Alarm Digital Input 1"}												

With +, open the configuration dialog for the job definition.

You can assign as many jobs as you like to the event – the SITEMANAGER II/V6 will trigger them according to the configuration.

Setting up the counter event:

Depending on the configuration of the event, jobs are executed as long as an event is pending or are initiated and remain active until a corresponding counter event is triggered.

A typical example would be an RCCMD shutdown with redundancy behavior. The RCCMD client receives the command from the SITEMANAGER to trigger a shutdown but is still waiting for a CS141 that did not trigger the command. In this case, the RCCMD shutdown must be revoked by the SITEMANAGER as a corresponding counter event, otherwise the RCCMD client believes that the shutdown instruction is still active.

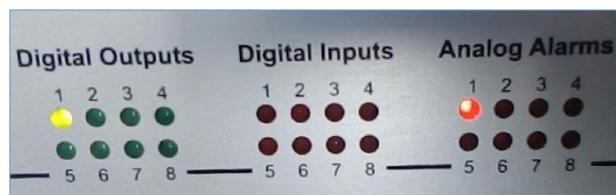
As soon as an event is no longer pending, corresponding A

-	+	Digital Input 1 off	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
		Job Typ	Wann		Parameter												
		Log	Einmal, sofort		{"text":"Digital Input 1 off"}												

Special feature of JOB AUX:

If operating the CS141 with a CON_R_AUX4, switching outlets is possible. The SITEMANAGER 7 already has this function integrated.

Select AUX as the job. The Site Manager Outlets Port 1 - 8 are then available under Parameters, which you can freely switch. Switched outputs are displayed accordingly on the front panel under Digital Outputs.



You can conveniently display the status in the Sensor Monitor and change it in real time: Note that the label of the button represents the state that the output will take:

Ausgänge			
	Name	Status	Anschalten
1	Output 1	●	Switch Off
2	Output 2	●	Switch On

Switch on / Switch Off is displayed accordingly for the outputs on the front of SITEMANAGER 7. If switching the output off, both displays are switched off. In this context, please note the caching problem of the web browsers:

If the front LED on the device turns off but is still on in the web interface, refresh the browser cache.

Setting up a job

Note:

The executable jobs are the same as those that can be triggered by UPS events. This allows environmental control sensors to be fully integrated into the warning and alarm behavior. Please note that other sensors may provide different setting options depending on their function.

The icons used in this menu are described in detail in the Setting System Events chapter.

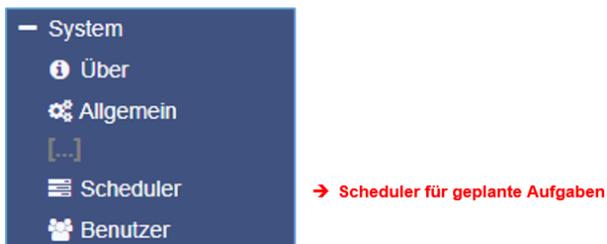
Click  to get a general overview of existing jobs

-							
			SM_T_H_COM Temperature High	1	1	0	0
		Job Typ	Wann	Parameter			
			Log	Einmal, sofort	{"text": "SM_T_H_COM Temperature High"}		

A job is therefore already configured for the event of a temperature being too high.

Scheduler

For this configuration step you need the following menu



Regardless of all system events, all models in the CS141 product family offer the option of running jobs at freely definable times. These so-called scheduled jobs can be assigned to all connected devices. These jobs can be used, for example, to control higher- or lower-level systems, restart computers, etc.

The configuration menu

In the basic configuration, no job is defined as a factory setting in the scheduler – these must be defined exclusively if required.

To define a job, click +:

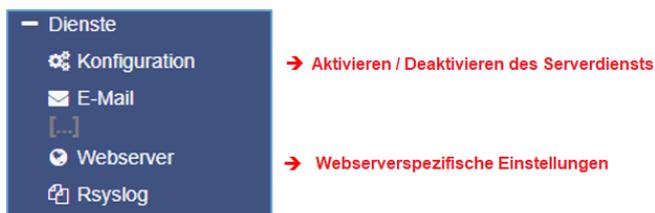
The familiar mask opens, which contains all jobs that are currently selectable.

Note:

Some jobs can be configured differently depending on the configuration of the connected devices. For example, if you have defined a CON_AUX4 in the general port settings, the jobs only offer the option of controlling a CON_AUX4. The extended functionality of the CON_R_AUX4 is hidden.

web server

For this configuration step you need the following menus:



For security reasons, console access has been completely blocked. All models of the CS141 product family are configured exclusively via the web interface via http or https.

Enabling / Disabling the Web Interface

The integrated web server is deactivated under Services using the slider. Important: This turns off the integrated web server in regular operating mode, no access for configuration is possible. Before you set this slide to OFF, make sure that a current system backup (System>Update) has been made.

Web access configuration

Overview of the basic settings

- Einstellen des HTTP-Ports
- Einstellen des HTTPS – Ports
- Deaktiviert Zugriff über http
- Zeit in Sekunden zur Webseitenaktualisierung
- Begrüßungsseite nach dem Anmelden
 - Umschalten zu einfachem USV-Monitor
- Tooltips
- Zeit bis zum automatischen Logout

HTTP port

The international standard for websites of any kind is port 80 - normally this port does not need to be changed. If you have other ports in your IT infrastructure for the web manager, you can enter a different port here. Please note that under these conditions you must also specify the port for the web query in your web browser: 192.168.3.1:85

In this case, the web manager would be accessible on IP 192.168.3.1 on port 85. On port 80, however, you would receive an error message from your web browser.

HTTPs ports

If you use HTTPs, port 443 is used by default. If necessary, you can adapt this port to your network.

Note:

Once you have enabled force https, you must use https:// as syntax in your web browser. Otherwise, you have two options for how a web browser responds to this request:

Connection Timeout

Since CS141 only responds to HTTPs, the web browser does not receive any communication.

redirect (browser-specific)

If you operate several devices from the CS141 product family in your network, it may happen that there is an alternative valid entry in your web browser - in this case a CS141 will be displayed automatically.

Force HTTPs

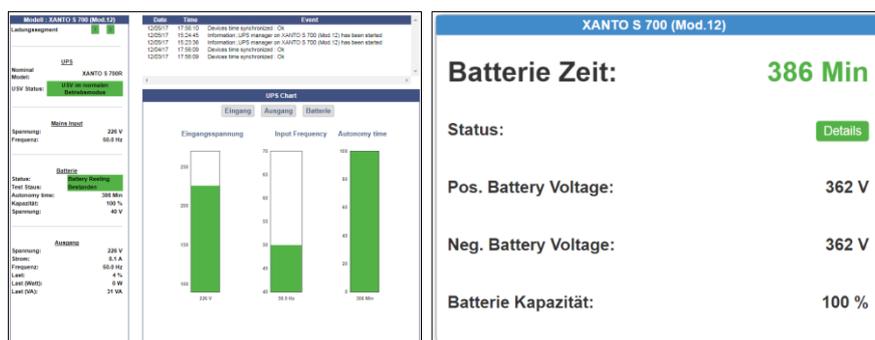
A standard HTTP connection on the Internet can easily be intercepted by unauthorized people. To avoid this and to ensure secure data transmission, an HTTPs connection is used. On the one hand, the Transmission is encrypted and on the other hand the server is authenticated. The advantage is the increased security, the disadvantage is the increased response time, since the data is transmitted encrypted. Force HTTPs prevents regular HTTP traffic and forces the use of HTTPs

HTTP refresh time

The CS141 automatically delivers an updated page cyclically, which shows the status of UPS systems or other status monitors, among other things. This value defines how often an automatic page update is carried out. By default, the CS141 updates these displays every 10 seconds.

Using simple monitor functions

The CS141 offers two different displays in the UPS monitor, which differ greatly in both layout and content:



The simple monitor (pictured right) contains significantly less information but is easier to read.

Enable HTTP tooltips

Tooltips are context-sensitive hint windows that appear automatically when you move the mouse over a setting option. Tooltips are enabled by default but can be permanently disabled using this option.

Automatic logout

The time window between two configuration entries. It is not enough to move the mouse, a menu must be opened within the time window or a configuration entry must be confirmed - Entering a value in an input field is not enough, in this case a write/read process must also be explicitly triggered by clicking Apply. If you do not want an automatic logout when inactive, activate the checkbox for "No auto-logout".

Certificate management / https – access

When commissioned, the SITEMANAGER 7 offers a factory-installed HTTPS certificate to ensure the encryption of the connection.

To replace the certificate with your own certificate, drag and drop the new certificate as a "PEM file" into the corresponding box and click Upload.

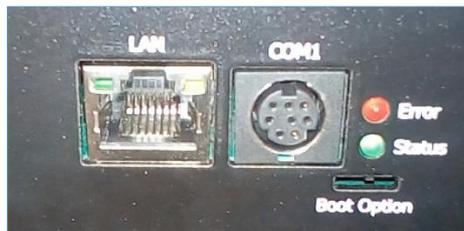
Note:

For the test run, temporarily deactivate the "Force https" function, as an incorrect/wrong certificate prevents access via https. In this case, you can still access the web interface via http and upload a new certificate.



Diagnosis: Status bar and LEDs

The SITEMANAGER 7 offers several options for visual inspection. This allows a quick preliminary check to see whether any action is required. For example, the SITEMANAGER 6 has general control LEDs right next to the COM1 connection on the back.



Green LED	Red LED	adapter
OUT OF	OUT OF	No power supply
OUT OF	TO	boot process
OUT OF	FLASHES SLOWLY	update process
OUT OF	FLASHES FAST	update process faulty
TO	TO	Connection to UPS or external device lost
FLASHES SLOWLY	OUT OF	Normal operation, connection active

More detailed information about the current status can be found directly in the upper status bar after logging in:

In addition to the physical LED status, there is also the status bar. Here the different states and more detailed information about the current status are displayed:

UPS: ● Ready

A green marker means that communication is taking place and there are no problems. If you have not selected a UPS, the LED will also light up green.

UPS: ● Initializing

A yellow marker is displayed when:

- The device is currently initializing, and communication is being established
- There is a warning behavior that may require appropriate intervention soon.

UPS: ● Temperature Bad

If the marker lights up red, there is an alarm or critical condition:

- The CS141 has lost communication with a connected device
- There is a system-critical condition that requires timely intervention.

All types of alarms are displayed here in detail. Loss of communication is also displayed here.

UPS:  Communications Lost

A blue marker means that the device has probably been configured correctly, but communication has not yet taken place.

Sensor:  Disabled

A gray marker with the note disabled means that a device has been completely deactivated and therefore cannot provide any data.

Note:

There is a separate status display on the front panel that shows the internal SITEMANAGER 7 system state. If the status display flashes, there is an internal communication problem with the connections.

Since the UPS management and all jobs are managed exclusively by the CS141 in the device, UPS management and correspondingly configured system services such as an RCCMD shutdown will continue to be executed provided the available data is sufficient.

Log files

In the event of a malfunction, the log files provide a wealth of information that can provide valuable clues about the chain of events and the course of the fault during subsequent investigation into the cause.

The Eventlog Files

Depending on your system configuration, the following files may arise:

- Logfile	
📄 EventLog	→ SITEMANAGER 7 UPS Events
- UPS	
📄 DataLog	
📊 DataLog Chart	
- Sensor	
📄 SensorLog	→ Sensor Events
📊 SensorLog Chart	
- BACS	
📄 BACSLog	→ BACS Events
📊 BacsLog Chart	

In addition to the system events, all actions that affect the CS141 and the UPS are recorded in the event log. The entry is made in the event menu of the UPS settings. You can create individual log files with the "Log" job or leave the preset configuration.

Logtime	Logtext
<input type="text" value="Logtime search"/>	<input type="text" value="Logtext search ..."/>
12/07/2017,09:38:01	time synchronization job : OK
12/07/2017,09:38:01	Restart NTP service: OK
12/07/2017,09:33:45	UPSMAN on No UPS model defined has started
12/07/2017,09:33:25	CS141L V1.63 - OEM 32

Download als CSV Datei

The first entry after a reboot is always the CS141 itself with its unique OEM ID:

12/07/2017,09:33:25	CS141L V1.63 - OEM 32
---------------------	-----------------------

The oldest entry is always at the bottom and the newest entry at the top of the list. Downloading as a CSV file creates a CSV file from this event log and saves it locally on your hard drive:

DataLog	04.10.2017 13:45	MICROSOFT EXCEL-C...	400 KB
eventlog	07.12.2017 10:45	Microsoft Excel-C...	1 KB

You can open this file for later analysis in a program of your choice:

	A	B
1	12/07/2017,09:33:25, CS141L V1.63 - OEM 32	
2	12/07/2017,09:33:45, UPSMAN on No UPS model defined has started	
3	12/07/2017,09:38:01, Restart NTP service: OK	
4	12/07/2017,09:38:01, time synchronization job : OK	
5		
6		

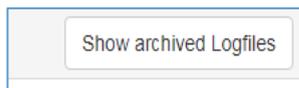
When the continuous storage for event logs is exhausted, its contents are moved to an archive file that is stored on the CS141 and available for display and download.

Note:

Depending on the configuration, the system events are retained in the event log for up to three months. As soon as the continuous storage for the current event log file is exhausted, the files are saved alternately in 2 archive files. This generally provides a monitored period of up to 9 months from initial commissioning.

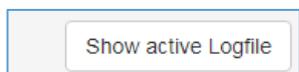
Navigate between log files

By default, the current event log is displayed.



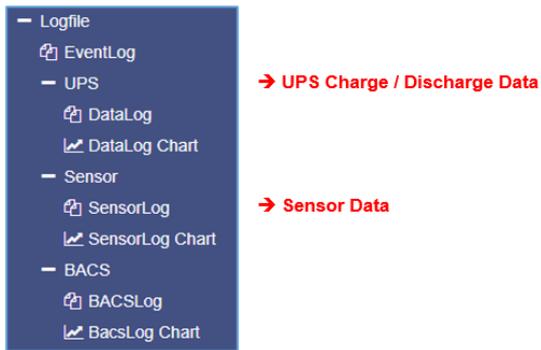
You can switch between the two logs by clicking the "Show archived log files" button in the upper right corner.

Note that the button label changes:



To return to the active log file, press the button

"Show active log file"

The Datalog

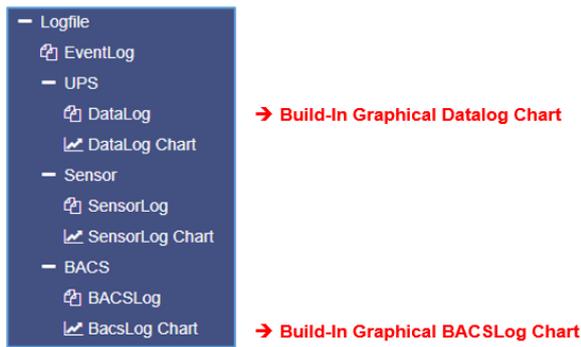
Logfile > DataLog																
Date,Time	InVolt1	InVolt2	InVolt3	InFreq	Load1	Load2	Load3	BattVolt	UPSTemp	BattCap	OutVolt1	OutVolt2	OutVolt3	OutFreq	AutonomTime	
01/01/2000,00:04:51	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:07:59	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:11:06	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:14:16	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:17:23	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:20:31	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0
01/01/2000,00:23:39	230.0	230.0	230.0	50.0	100.0	n/a	n/a	n/a	n/a	100.0	n/a	n/a	n/a	n/a	n/a	6.0

Existing measurement data is recorded in the data log. Since this is provided with a time stamp, it can be used together with the event log to create event chains with additional data. Like the event log, this data can be exported as a CSV file for later analysis.

The data log saves the entries every 3 minutes and keeps the entries as a current data log file for 8 weeks. The data is then moved to an archive file and a new data log is opened for the current data. In addition to the current file, 2 archive files can be created - so up to 24 archived weeks are available in addition to the current period. After the time has elapsed, the oldest archive file is replaced.

As with the event log, the data log can be switched between archived files and the current log file using the Show archived log files and show active log files functions, and the files can be downloaded in CSV format using the link at the bottom of the data log.

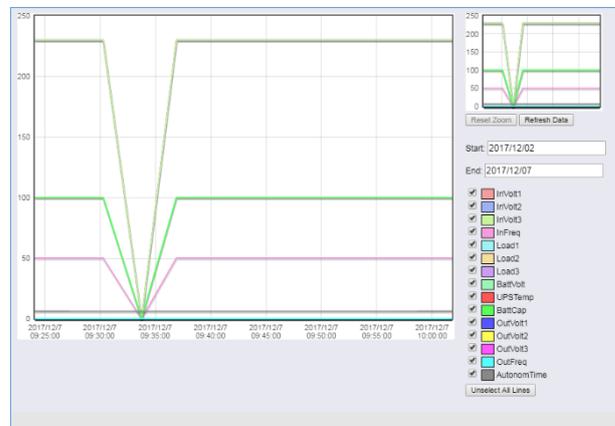
Datalog Chart – Graphical representation



Overview

The Datalog Chart is a graphical representation of the Datalog:

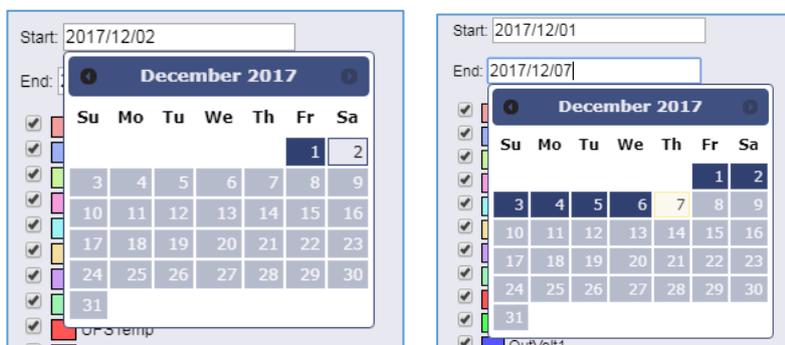
All entries within the data log can be specifically selected or deselected using the checkboxes.



In addition to the current values, you have the option of selecting specific values from current data sets. By default, all checkboxes are checked when you call up the function. You can remove these and check the relevant boxes using the Unselect All Lines function.

Calendar function

The calendar function provides a quick overview of available time periods that you can select. To do this, click in the date field to

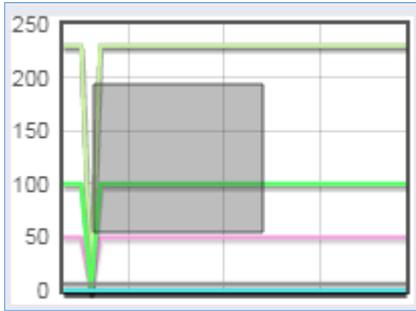


open the calendar:

The data of the corresponding period is automatically loaded and displayed in the main window.

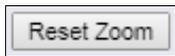
zoom function

The SITENANAGER 7 provides to zoom into the collected data and thus obtain a detailed view within the displayed measurement data.



To refine the display, drag a frame into the small window. A detailed view with an adjusted timeline is automatically displayed in the main window:

The zoom function allows the timeline to be enlarged to up to 2 minutes.



→ Returns the zoom depth to the original value



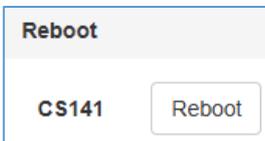
→ Updates the current data and sets the focus on it.

Toolbox

- ⚙ Scheduler
- ⚙ Webserver
- ⚙ Users
- ⚙ Tools
- ⚙ Backup
- ⚙ Update

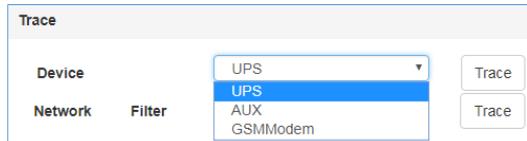
→ **Toolbox: Additional Tools for diagnostic**

Reboot / cold start



Since the CS141 writes the configurations in real time and restarts the corresponding system services, a complete restart is only necessary in exceptional situations. Even if the restart only affects the CS141 and the UPS continues to run normally during this time, monitoring will be temporarily unavailable. To prevent accidental restarts, this function has been deliberately placed under Tools.

Tracer



The Tracer is a comprehensive diagnostic tool for checking communication both between the CS141 and the connected end devices and for identifying network problems when communication problems between the CS141 and a server are not working properly.

Under Device, communication information between the end device and the CS141 is queried. The COM ports with which problems occur can be selected. To select a device, open the context menu and select the device you want to monitor:

COM 1 / UPS

This tracer actively monitors the UPS communication that runs via the serial RS232 port. Faults or faulty communication are displayed and can be saved for later evaluation.

COM 2 / GSM modem

The tracer queries the communication between the CS141 and the GSM modem and displays it in real time. Errors and communication problems can be easily collected and saved for later analysis.

COM 3 / AUX

A CON_AUX4 or CON_R_AUX4 can be connected via the AUX port. The tracer can query the communication with the device in real time.

Note:

The tracer adapts itself to the selection you have made under Devices/Systems in the general port settings. If you have a GSM modem instead of a Sensormanager2, the tracer will only display sensor displayed.

Click the Trace button to start the process, which opens a new tab in your web browser showing the communication between the device and the CS141:



When you close this window, the trace will be terminated automatically and any unsaved data will be lost. To save the data, select it with the left mouse button and copy the content with CTRL + C, and paste the information into a document of your choice with CTRL + V.

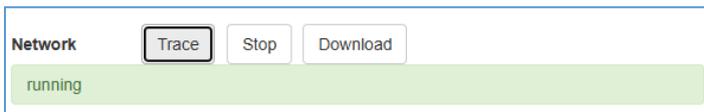
network scan

A special feature of the CS141 is the ability to use an integrated network scanner to examine the LAN for sources of error. The network scan provides extensive information for evaluation about the network card and the data traffic it contains in your LAN. All data packets are collected in a log file and can be downloaded for later evaluation.

Privacy Policy:

Since the network scan records all data traffic in this network segment, an evaluation with an appropriate network tool can not only provide deep insights into network traffic but can also be used, for example, to log user behavior. Technicians should inform the relevant responsible persons before using the tool.

To perform a network scan, press the Trace button:



The tracer confirms that it has been started with a short display.

The tracer logs all packet data within the LAN segment and saves it locally on the CS141. The data collected is saved in real time - if the CS141 crashes, the data up to the crash is available afterwards and can be saved to the local hard drive using the Download button. The tracer is terminated when two conditions are met:

1. A fresh start
2. Pressing the stop function

After completion, the data will be downloaded in the form of a compressed archive for later evaluation.



Note:

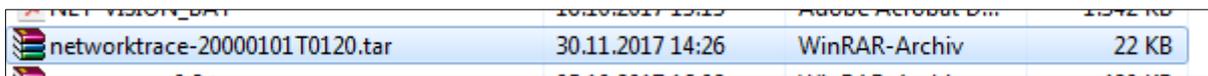
The network tracer is usually only needed very rarely, for example when GENEREX technical support needs specific information to solve a problem. In this case, it is recommended to start the tracer without a special filter.

This feature can do even more: It turns your CS141 into a network diagnostic tool with numerous features that allow you to examine your local LAN:

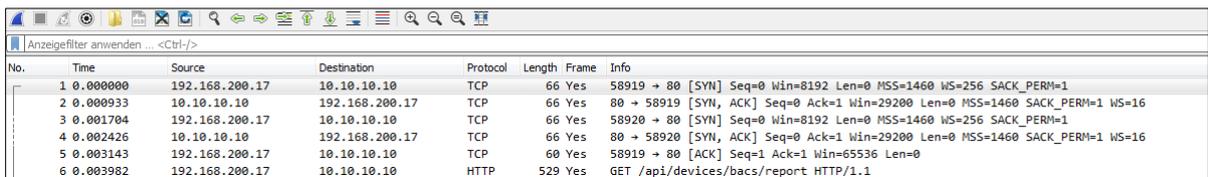
Visit www.tcpdump.org to find extensive tutorials on how to define filters to utilize the full potential of the CS141 as a network diagnostic system.

Network scan: evaluation of the data

The collected data can be read and analyzed using special diagnostic tools such as Wireshark*:

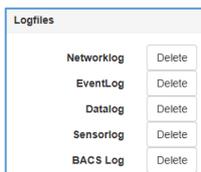


Unzip the file and import the dataset into Wireshark:



*The tool "Wireshark" is not a GENEREX product. You can get it from www.wireshark.org

Deleting log files



The CS141 collects and logs large amounts of data and stores them permanently in its own memory. This data can then be retrieved via a web browser and evaluated using diagnostic tools. Since the log files contain very sensitive information about a network, they can be completely and permanently deleted if necessary.

Networklog*	Deletes all records collected by the network tracer
EventLog*	Deletes all records of system events in the log file
Datalog*	Deletes all UPS data records
Sensorlog*	Deletes all sensor data records
BACS Log*	Deletes all BACS sensors / measuring data

**) Only data stored on the SITEMANAGER 7 are deleted, 3rd party storage resources are not harmed*

Corporate Identity – Replacing the OEM Logo

It can happen that the original logo is ultimately not desired within a company, organization or corporation. Therefore, a SITEMANAGER 7 offers the option of replacing the existing logo with your own logo.

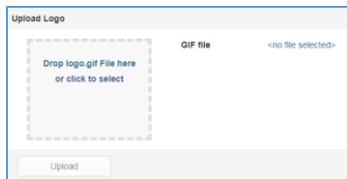
Quick Guide: Replace Logo

1. Open an available graphics program
2. First, create a new image. Make sure the maximum size is 200x54 pixels



3. Edit the image and adjust the content as you wish.
4. Save the image as logo.gif – otherwise it will not be accepted by CS141.
5. Open the tools in CS141.

Under Tools you will find the following option:

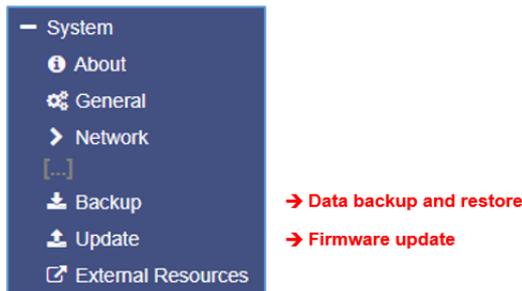


Use drag and drop to place the new logo into the designated window.

6. The new logo will be adopted upon upload:



Data backup and firmware updates



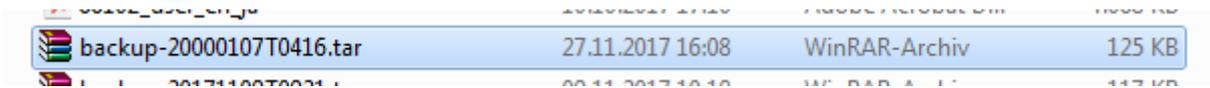
Data backup offers the possibility to completely save the current system configuration in order to be able to restore it quickly in an emergency.

The backup and recovery took place in two steps:

Step 1: Back up the data



If you click Backup under Save Configuration in the Backup menu, a compressed file will be saved locally on your PC in the download directory. Since the backup function is system-critical, you will be explicitly asked for the valid administrator password again.



You can then use this data backup on any CS141 with the same or a higher firmware version. Please note that if you change the file name, the backup file will no longer be valid and an error message will appear.

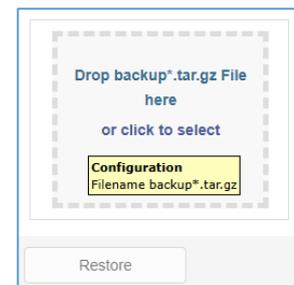
Step 2: Restore data

Restoring a backup is done in the same menu:

Drag and drop the compressed file into the box or left-click on the box to open a file browser and double-click the desired backup file.

With Restore you start the restore process, which unpacks the file and automatically adopts it as the existing configuration. After the process is complete, you will be automatically logged out and must log in again using the login data from the backup. Please note that backups from a CS141 are compatible with any CS141 with the same or newer firmware. If you use the backup on a CS141 with an older firmware, problems may arise.

The reason is that a new firmware version adds general improvements as well as new features whose configuration files may not work properly on older firmware versions.



firmware updates



The updates can be found in the download area at www.generex.de.

System updates are regularly provided for all devices in the CS141 product family. In addition to general product improvements such as increased stability and improvements in operational and reliability, these updates also regularly offer new features that integrate seamlessly into the existing system.

By default, the OEM ID 12 / GENEREX is pre-installed upon delivery. Deviations arise if you have purchased the web manager as part of a UPS from a manufacturer for whom an OEM contract exists.

Note:

Since SITEMANAGER 7 is not technically locked, you can always install the OEM version of another manufacturer if your UPS changes.

Under Firmware, select the version you want and download it to your computer. It is not necessary to unzip the file.

After downloading, open the web interface and go to Update under System:

The screenshot shows a web interface for firmware updates. On the left, there is a dashed rectangular box containing the text "Drop firmware file here or click to select". To the right of this box, the text "Firmware file <no file selected>" is displayed. Below this text are two checkboxes: "Reset to factory settings" and "Reset network to factory settings". At the bottom of the interface is a blue button labeled "Start".

Drag the downloaded, zipped file into the window provided. Click Start to begin the update process. Before you start the update by clicking Start, you can select the following additional options:

[Reset to factory settings](#)

This option deletes all configurations during the update and resets the device to its factory defaults.

[Reset network to factory settings](#)

This option also resets the network and IP settings to factory defaults.

Note:

These two options are independent of each other, as an update via remote access would otherwise cause the CS141 to lose its IP settings. If you have problems, you can use this function at any time to reset the device to its factory settings without changing the IP address.

The update routine runs automatically, you do not have to stay on the page. If you return to the web interface too early, the CS141 will automatically reject the connection. In this context, please pay attention to the cache behavior of your browser: Since some of the content of the web interface is already in the browser's internal memory, this can lead to apparent error messages if the boot process is not yet fully completed.

[Changing the OEM firmware](#)

The CS141 Web Manager comes in two different firmware versions:

- GENEREX – ID 12
- OEM version of your UPS manufacturer

If you cannot find your UPS in the list of selectable UPS systems, it may be necessary to install a different firmware.

To do this, it is necessary to understand how to identify the currently installed firmware and the required firmware:

[The current firmware](#)

You can recognize the current firmware by the logo in the top left corner:



Depending on the manufacturer, you will find the corresponding entry here.

The firmware version

In the general system information provides, among other things, this entry:

Hardware	BACSKIT_B4
Firmware	CS141-SNMP V1.64.12 171213
Serial	1004211625 - 0030D6160377

The firmware displays the OEM key:

V1.64 the current firmware
 .12 the currently installed OEM version
 171213 the creation date read backwards

If you want to operate the CS141 in a UPS from another manufacturer, you can find the necessary firmware on www.generex.de in the download area



You can use the Show Version info link to check whether an updated firmware is available for download. Please note that - unlike an update within the same OEM firmware - changing the OEM firmware requires a reset to factory settings, as the functions, among other things, also change.

When nothing else works – The Rescue System

The SITEMANAGER 7 has an integrated protection function to automatically re-initialize itself in case of problems. If this does not happen, the CS141 has two possible options with which administrators can restart the web manager.

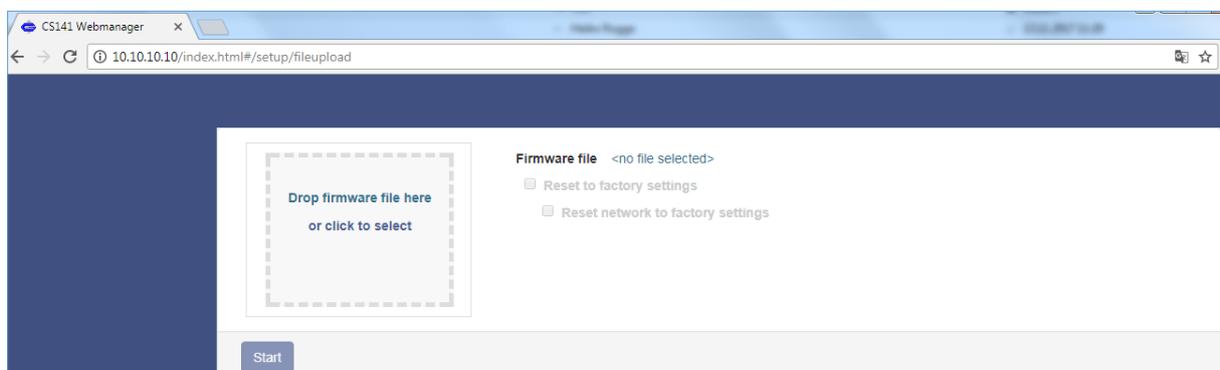
If the CS141 does not allow login or the interface displays an incorrect display but is still normally accessible, you can try the following:

`http://<IP address>/reboot`

This option allows you to restart the CS141 without having to log in completely. Since the restart is a system-critical process, you will be explicitly asked for the administrator password.

`http://<IP address>/update`

This option allows administrators to distribute quick system updates by opening the update screen directly.



Now you can select the desired firmware package by dragging and dropping it or by clicking the button. If necessary, you can use the Reset to factory defaults function to reset the CS141 to factory settings. This will delete all configurations and set the device to the start-up configuration.

Now enter the password for the administrator. The process starts and after successful transfer the login screen appears.

Note:

Network settings and system settings are separated from each other. This allows a flash update including deletion of the configuration without deleting the IP address settings.

[Start the rescue system](#)

If this function is not possible, for example because the update went wrong and the CS141 no longer boots, there is another way to save the device:

During each update process, the CS141 saves a complete backup copy of all log files and configurations of the last known working version. This version can be activated by setting a jumper:



When the jumper is set and the adapter boots, you can identify the rescue system by the firmware version in the About screen - behind the firmware version you will find the word (RESCUE).

Appendix

FAQ – Frequently Asked Questions

What does error 500 / 503 mean?

This error occurs when the CS141 web server is not running correctly. If the problem persists after restarting the adapter, the firmware must be updated / reinstalled. This is recommended in conjunction with a reset to factory settings.

What does error 422 means?

This error occurs when attempting to change the configuration of certain values in older firmware. Update to the latest version.

What does error 400 / 420/ 522 mean?

This problem can occur if the firmware has been updated but the browser still has old data stored in the cache. Press CTRL + F5 or clear the cache. Restart the adapter.

The UPS status is (temporarily) set to "Paused".

When accessing the UPS Alert History via the adapter, the normal connection must be suspended. Switch to the page and press F5 to restore the display status (if this does not happen automatically).

What does error -1 mean?

This error occurs when no connection is established to the adapter (e.g. after a restart), but the user still has the adapter's configuration page open. Wait until the adapter is back in normal operating mode and then call up the adapter's IP again.

I forgot my password.

Please refer to the "Rescue System" section to learn how to reset your password.

Why am I logged out when I disable the http tooltips under Services?

Because the tooltips are related to the http service and changing these values will redirect the user to the newly configured page / correct port.

The CON_R_AUX does not get a stable connection!

This device is not supported by the CS141. Use the CON_R_AUX4 here.

I keep getting entries in the log file called "UPSMAN started".

This entry is generated when changes are made to the event configuration. Because the changes are applied immediately, the service must be restarted.

When I access the alert history, I only get an error message!

The function is not supported by the selected UPS.

I got the error "Backend busy" when trying to log in!

Wait a moment and try again with a different browser if necessary. If the problem persists after 5 minutes, use the /reboot function.

Does the CS141 support SNMP queries in version 1

The CS141 has never officially supported SNMP polling v1.0 - which doesn't mean it can't do it. If your polling system forces you to do a v1 poll, it will work - but there will be no official bug fix if you have problems.

I have questions that are not explained in the manual

No problem, we are always striving to improve our documentation. If you have something that is not explained or is explained insufficiently, write us a short message at support@generex.de - we are happy to help.

I want to manually set a different time, but it always returns to the original value

In 99% of all applications, the time should be set correctly. The CS141 solves the problem by first querying time servers - in exactly the order in which they were entered. Both your own IP addresses and external time servers can be used. If the CS141 does not find the specified server, it takes the next entry. If there is no entry, it first tries to reach the UPS clock. Only then does it resort to the internal clock.

Here lies the problem:

If the UPS supports setting and reading via the CS141, the UPS system clock will not be overwritten when the time is entered manually - however, the CS141 can correct its own clock using the UPS system clock. If you want to set this clock manually, you must also adjust the UPS clock to the settings via the UPS menu, as the CS141 synchronizes with the UPS's internal clock.

Why can't I include the CS141 in the NAGIOS process?

One thing that might be worth mentioning: after saving the file in /usr/share/snmp/mibs, the file should be renamed from RFC1628-cs1x1.mib to UPS-MIB.txt so that Centos will recognize it and be able to interact with it. Please note that depending on your Linux distribution, the directories and access rights may differ.

The manual always shows a block diagram, but I only get a bar view, can this be changed?

The view varies depending on the manufacturer and cannot be changed as it is specified by the manufacturer. However, you can choose between a simple and a complex display of the UPS screen in the Web server selection menu.

The links provided in the manual are correct in terms of content, but the position has shifted

Unfortunately, this happens every now and then, especially when a last-minute change is made to the so-called "release candidate", which ultimately results in a multitude of changes. Unfortunately, these overlaps cannot be completely ruled out.

Why can't I downgrade to 1.66.XX firmware?

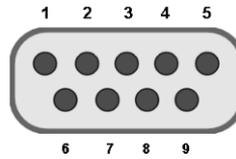
As of 2018, there is a new hardware revision of the CS141 boards. In the "About box" under System, the hardware revision is displayed under Features:

bch16 uses an older chip that was installed before 2018. This chip is fully upward and downward compatible.

bch8 uses a newer chip, which is installed from 2018 onwards. This chip starts with firmware 1.66.XX and is not compatible with older firmware

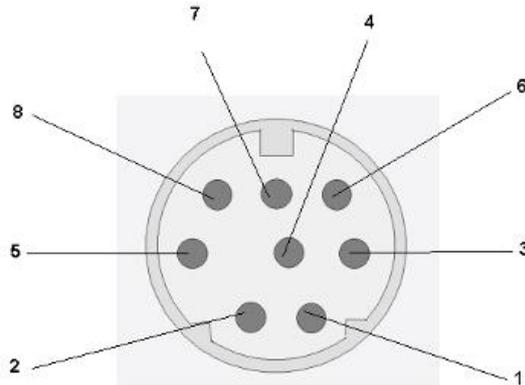
Since the CS141 is only delivered with the latest firmware that is current at the time, it is possible that firmware older than 1.66.XX will not run for this reason.

For further questions please contact our support at support@generex.de !

Appendix: Hardware Layout and Connections CS141 / SITEMANAGER 7interface description

External D-SUB 9-pin male

Pin1: DCD	Pin6: DSR
Pin2: RxD	Pin7: RTS
Pin3: TxD	Pin8: CTS
Pin4: DTR	Pin9: RI
Pin5: GND	

Pin COM2 Mini-DIN 8 pin

Mini DIN 8 socket RS-232:

Pin1:	-> DCD
Pin2:	-> RxD
Pin3:	-> TxD
Pin4:	-> DTR
Pin5:	-> DSR
Pin6:	-> RTS
Pin7:	-> CTS
Pin8:	-> RI
screen	-> GND

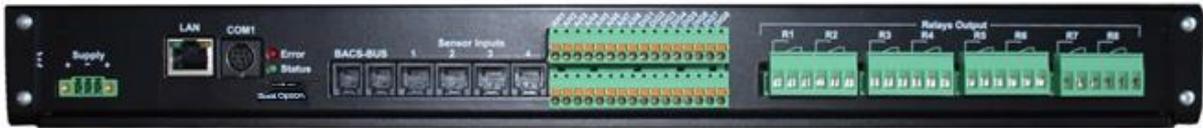
RS-485 (optional):

Pin1	→GND
Pin2	-> RS485/A
Pin3	-> RS485/B (-)

Connection options on the SITEMANAGER 6

The figure shows a typical installation of the Site Manager with a UPS connected. It is possible to connect numerous types of sensors to the Site Manager and manage circuits by switching the relay contacts.

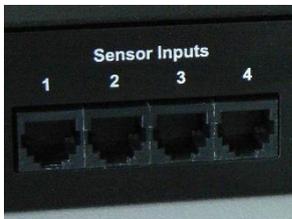
connection sockets and terminal blocks
 The back of the site manager is equipped with the following connectors:



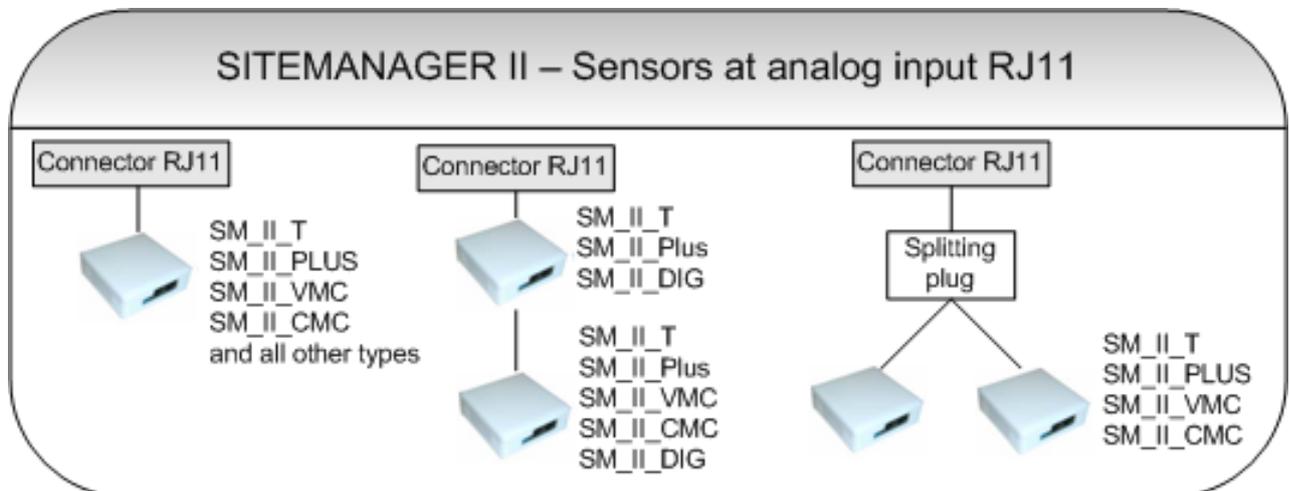
Back of SITEMANAGER II/v6

- Power supply: Connect the included external power supply (DC, 24V).
- Fast switching between operating modes thanks to Sliding Switch
- COM Port 1: RS232 connection for UPS, Sensor Manager or other RS232 devices.
- LAN socket: Connect the SITEMANAGER II/v6 to the network using an RJ45 cable.
- 2 RJ10 connectors for connecting a BACS bus system
- 4 RJ12 ports, connection for 8 analog measuring units.
- Terminal blocks for 8 analog and 8 digital signals.
- 8 switchable relay contacts (NO and NC).

Analog inputs via RJ12 connectors



Each of the 4 RJ12 connection sockets can read 2 analog input signals (0-10V or 0/4-20mA), making it possible to connect 8 analog sensors. The following illustration shows how the various sensors can be connected to the RJ12 connection sockets. For the PIN assignment, please see the relevant appendix at the end of this document.



Sensors connection options on the analog RJ12 input

1.1.1 Analog inputs via terminal blocks

The 8 analog inputs are also connected to the upper terminal block A01-A08. Customer-specific sensors/transducers that provide an output signal of 0-10VDC can be connected there. The connection is made via open cable ends (min.0.14mm² / max.1.5mm²) to the respective spring-loaded connection on the terminal block.

Please make sure that channels are not used twice via the RJ11 socket and terminal block!

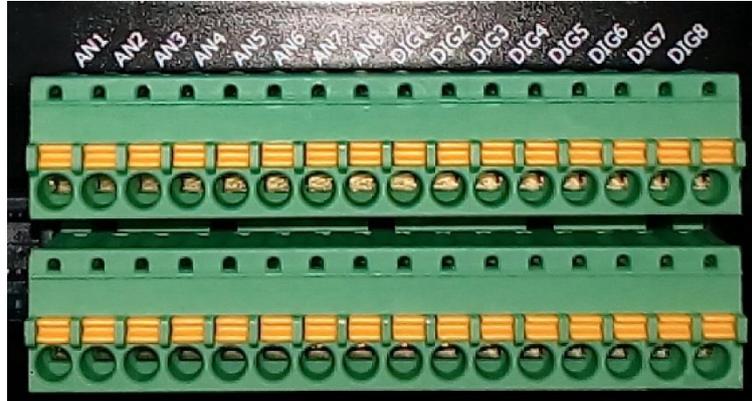
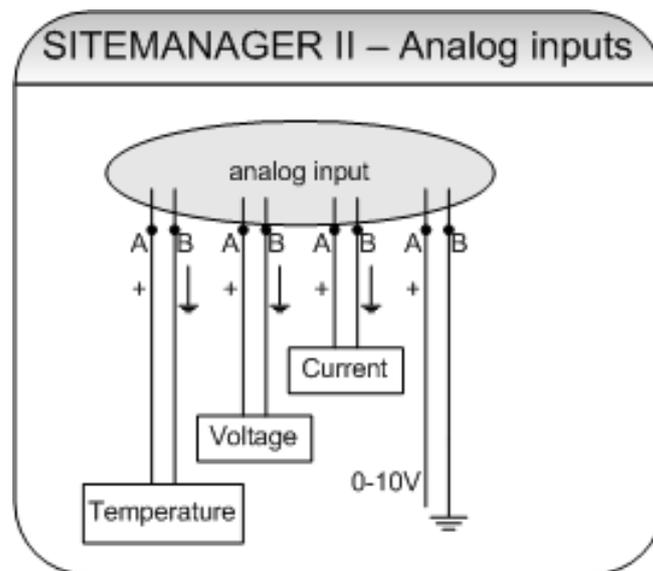


Figure: On the terminal block, the analog inputs are clearly marked with AN. recognize

The following figure shows the terminal block pin assignment for the analog inputs. Note that the input signal is in the range of 0-10V DC.



Terminal block connection assignment for analog inputs

Configuration of the SITEMANAGER 7 analog inputs

Each of the 8 analog inputs of the SITEMANAGER II/v6 offers the possibility to receive analog measured values either from **0-10V (delivery state is set to 0-20mA or 4-20mA)** to read.

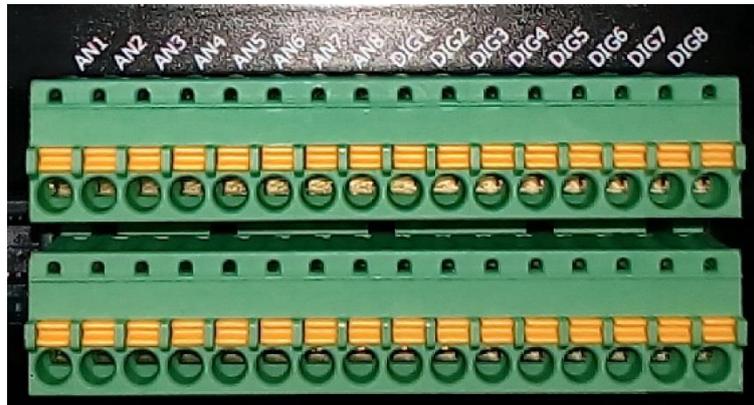
To do this, the jumpers for the respective analog input on the main board must be set to the correct position.

To change the delivery state, please proceed as follows:

- Activating the S (unplug the power supply)
- Disconnect all connection cables from the device (16/6-pin Phoenix connectors can be completely removed from the device if necessary).
- removal of the device
- Open the device by loosening the 4 side screws and removing the housing cover
- Set jumpers in the desired configuration (see Fig.1/Fig.2)
- Reassembly/put the device back into operation in reverse order

Digital inputs via terminal blocks

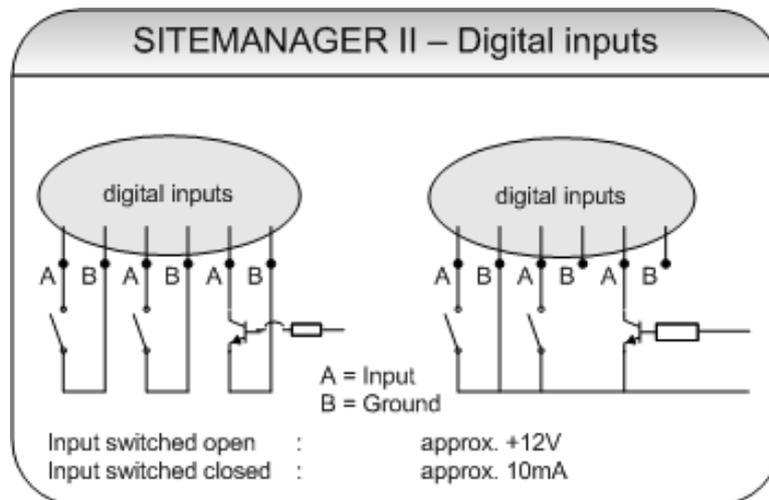
Below the analog input connection sockets is the terminal block for the 8 digital inputs.



Analog input terminal block (A01-A08) and digital input terminal block (D01-D08)

The following figure shows the connection assignment of the terminal block for the digital inputs.

Connection assignment of the terminal block digital inputs



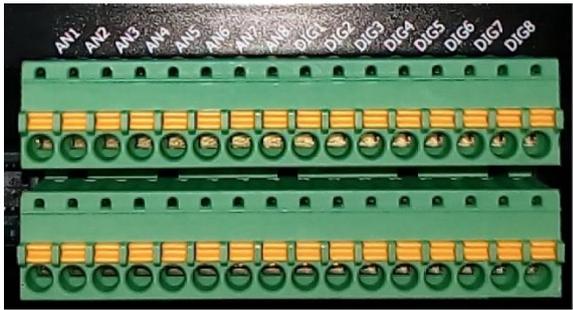


Fig.: Digital/analog inputs SITEMANAGER II/v6

Terminal designation:	Connection:
X1 / 12V +	operating voltage +12VDC
X1 / -	GND -
X2/A01	Analog Input 1
X2/A02	Analog Input 2
X2/A03	Analog Input 3
X2/A04	Analog Input 4
X2/A05	Analog Input 5
X2/A06	Analog Input 6
X2/A07	Analog Input 7
X2/A08	Analog Input 8
X2/D01	Digital Input 1
X2/D02	Digital Input 2
X2/D03	Digital Input 3
X2/D04	Digital Input 4
X2/D05	Digital Input 5
X2/D06	Digital Input 6
X2/D07	Digital Input 7
X2/D08	Digital Input 8

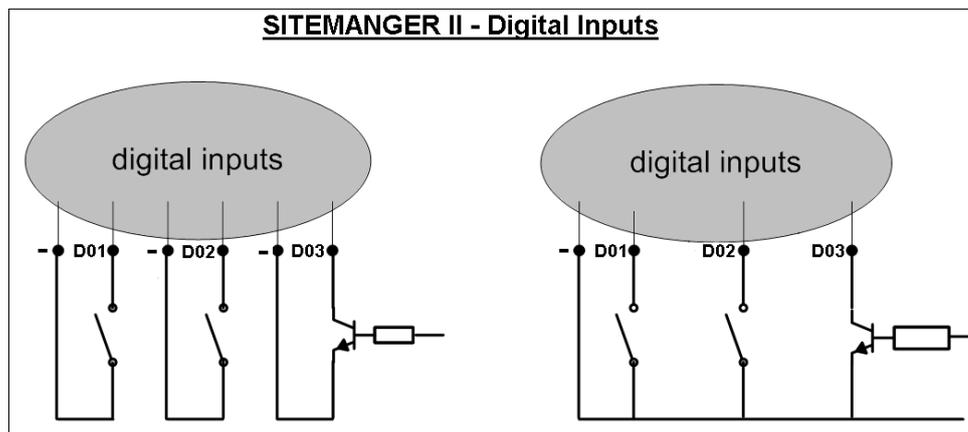
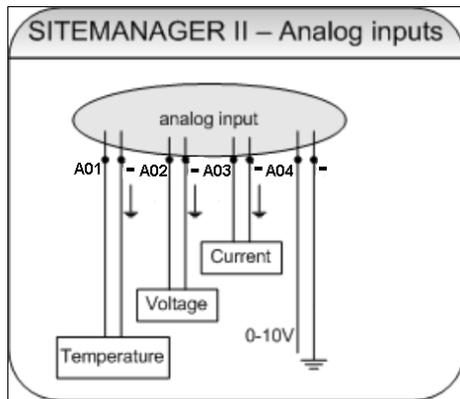
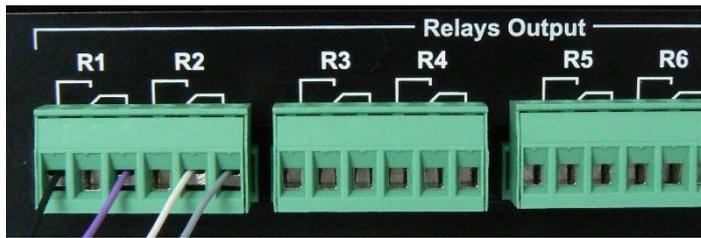
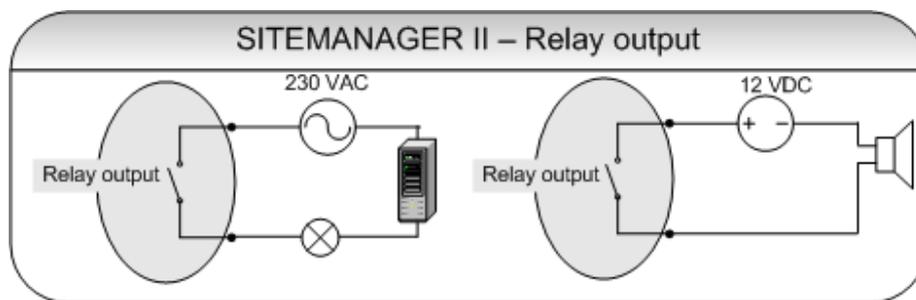


Fig.: Circuit diagram of analog inputs

relay contacts via screw terminals*Switchable relay contacts*

The SITEMANAGER II/v6 has 8 switchable relay contacts that can be used to switch circuits of up to 250V/4A. Each relay has one normally closed contact (NC) and one normally open contact (NO). Please see the following illustration for connection examples.

*Circuit diagram: Relay contact*

Copyright Statement on Intellectual Property and Handling of Confidential Information

The information in this user manual is not intended to be a guarantee of accuracy and is subject to change without notice. Although GENEREX has attempted to provide accurate information in this document, GENEREX assumes no responsibility for the accuracy of this information.

GENEREX shall not be liable for any indirect, special, consequential or incidental damages, including, without limitation, lost profits or revenues, cost of replacement goods, loss or corruption of data arising out of the use of this document or the product described herein.

GENEREX, as the manufacturer of the products mentioned, assumes no obligation with this information. The products described in this manual have been given solely as information for business partners to gain a better understanding of the GENEREX products.

GENEREX authorizes its business partners to transmit the information contained in this document to third parties, as well as to personnel in their company or their own customers, electronically, manually, in the form of photocopies or similar. GENEREX states that the content may not be modified or adapted without the written permission of GENEREX.

All right, title and interest in the GENEREX trademark BACS or logo (registered or unregistered) or the goodwill and/or intellectual property of GENEREX, copyright and product patents are owned exclusively and without restriction by GENEREX.

GENEREX will promptly resolve any complaint regarding the content of this document. Comments or complaints regarding this document should be addressed to GENEREX Systems Vertriebsgesellschaft mbH.

The copyright law of the European Union applies (Copyright EU).
Copyright (c) 1995-2020 GENEREX GmbH, Hamburg, Germany.

All rights reserved.

