

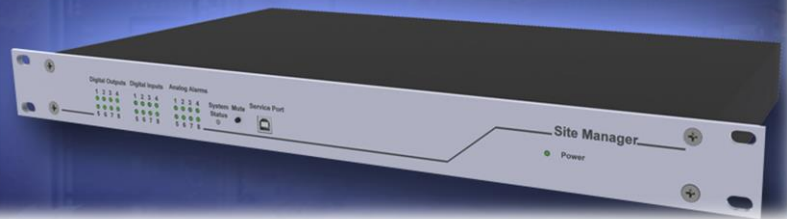
CS141 User Manual English

SITEMANAGER 6

SITEMONITOR 6

SITEMANAGER 6

- Powerful IT management functions
- Intelligent building management with escalation levels
- Open interfaces for any type of sensor
- Power switches above 2 amperes



SITEMONITOR 6

- Optimized for 19" installation frames in server cabinets
- 64 digital inputs to connect contact detectors
- Intelligent sensor matrix for batch notifications and escalation management
- Can be adapted to fit to nearly any IT infrastructure



Copyright Statement for Intellectual Property and Confidential Information

The information contained in this manual is non-conditional and may be changed without due notice. Although Generex has attempted to provide accurate information within this document, Generex assumes no responsibility for the accuracy of this information.

Generex shall not be liable for any indirect, special, consequential, or accidental damage including, without limitations, lost profits or revenues, costs of replacement goods, loss or damage to data arising out of the use of this document.

Generex the manufacturer of the BACS products undertakes no obligations with this information. The products that are described in this brochure are given on the sole basis of information to its channel partners for them to have a better understanding of the Generex products.

Generex allows its channel partners to transfer information contained in this document to third persons, either staff within their own Company or their own customers, either electronically or mechanically, or by photocopies or similar means. Generex states that the content must not be altered or adapted in any way without written permission from Generex.

It is agreed that all rights, title and interest in the Generex's trademarks or trade names (whether or not registered) or goodwill from time to time of Generex or in any intellectual property right including without limitation any copyright, patents relating to the Products, shall remain the exclusive property of Generex.

Generex will undertake to deal promptly with any complaints about the content of this document. Comments or complaints about the document should be addressed to Generex Systems GmbH.

Copyright of the European Union is effective (Copyright EU).

Copyright (c) 1995-2020 GENEREX GmbH, Hamburg, Germany. All rights reserved.

Table of Content

[Welcome](#)

General Information

[Scope of function](#)

[Power Connector](#)

Configuration: SITEMONITOR 6/ SITEMANAGER 6

[Operation modes: Sliding Switch](#)

Initial Configuration via 10.10.10.10

[Preparation: Setting up the computer](#)

[Adding a route within a Windows Operating System](#)

[DHCP-Mode](#)

[How to find the MAC address](#)

[The Netfinder tool](#)

[The different operation modes](#)

[Installation examples](#)

[Technical differences with the: SITEMANAGER 6](#)

[Limitations caused by convoluted network structures](#)

[Required Ports](#)

[Standard passwords](#)

[The Setup-Wizard](#)

[IP address and host name](#)

[Things to note for Initial configuration in DHCP mode](#)

[Location settings, contact details, required services](#)

[Time server, time zone and internal system time](#)

[Setting up a network time service \(NTP\)](#)

[Setting up system time manually](#)

[User management](#)

[System overview](#)

[Changing operation mode to regular](#)

[Rebooting the system](#)

Setup: Mail, SNMP and Modbus

[Email settings](#)

[Advanced Mail Options](#)

[Testing mail function](#)

[Most common error messages](#)

[Email-Traps](#)

[Modbus](#)

[Configuration: Modbus](#)

[SNMP Agent](#)

[Setting up SNMP v2](#)

[Setting up trap receiver v2](#)

[Testing trap receiver v2](#)

[Setting up SNMP v3](#)

[Setting up trap receiver v3](#)

[Testing trap receiver v3](#)

UPS configuration

[General COM-Port Setup](#)

[Setting up a UPS](#)

[Using the RFC1628 smart UPS interface](#)

[UPS Monitor – UPS configuration test](#)

[UPS functions menu](#)

[Using system events](#)

[Job – definition – setting up tasks to an event](#)

[General symbol overview](#)

[Setting up Jobs](#)

[List of available jobs](#)

[Time management of Jobs](#)

[Setting up multiple jobs](#)

Custom Thresholds

[Differences between Warning and Alarm Levels](#)

[Custom Threshold Example: UPS Temperature](#)

[Sample excerpt of the Custom Thresholds](#)

[Example: How to use Custom Thresholds](#)

RCCMD

[What is RCCMD](#)

[Configuration of RCCMD](#)

[Setting up RCCMD-Jobs](#)

[Defining the IP address for RCCMD jobs](#)

[How to define the timing for RCCMD](#)

[RCCMD Commands](#)

[UPS variables for RCCMD Traps](#)

SITEMONITOR 6: specific sensors and devices

[Strain relief and cable harness](#)

[Removing the terminal strips](#)

[Naming contacts](#)

[How to use NC \(normally close\) contacts](#)

[The „hold function“](#)

[Configuration of a job for alarm behaviour](#)

[The SITEMONITOR 6 AUX Ports](#)

[Configuring the outputs](#)

SITEMANAGER 6: Sensor setup

[Sensors and devices for the SITEMANAGER 6](#)

[SITEMANAGER 6 Configuration](#)

[Differences SITEMANAGER / SITEMONITOR](#)

[Using the direct connectors](#)

[Definition of the alarm thresholds](#)

[Sensor range, Pre-Alarm and Alarm](#)

[Digital Inputs](#)

[Extended System Monitoring](#)

[SITEMANAGER 6 – Job definition:](#)

Scheduler

[How it works](#)

[Setting up Scheduled Jobs](#)

Webserver

[Safety instructions](#)

[HTTP-setup](#)

[How to use a server.pem - file](#)

Diagnosis

[System status LED's](#)

Log files

[Event log](#)

[Datalog](#)

[Datalog Chart](#)

[Premium function: The UPS alert history](#)

Tools

[Reboot](#)

[Tracer](#)

[Network Scan](#)

[Data protection notice for the Network Scan](#)

[Data evaluation](#)

[Delete data](#)

[Change the displayed logo / use your own logo](#)

Backup and Update

[Creating a backup file](#)

[Restore system configuration from a backup](#)

[Running a firmware update](#)

[Changing the OEM firmware](#)

[Known update problems](#)

If nothing works ...

[How to reboot](#)

[Running a firmware update directly / Factory default](#)

[The rescue mode](#)

Appendix

[Diagrams](#)

... The SITEMONITOR 6 / SITEMANAGER 6 supports all software features of a CS141 and include special adaptations. For more information about

- ***tutorials,***
- ***configuration examples,***
- ***MODBUS-Lists,***
- ***Syslog-tutorial,***
- ***SNMP Configuration guide,***
- ***Radius-Support,***
- ***BACS***
- ***Sensor Matrix configuration and tutorials***
- ***And many more,***

please refer to the official CS141 documentation, available at www.generex.de

Welcome

We thank you for your confidence in the extensive product family of the CS141 Webmanager - the reliable solution in critical resource management.

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

The CS141 can not only answer queries from higher-level systems, but also independently inform responsible personnel in an emergency and initiate emergency measures as far as configured by an administrator. The CS141 can independently activate emergency systems, shut down servers and workstations and restart them under predefined conditions. In addition to standard technologies such as BACnet, SNMP and Modbus, the CS141 makes exclusive use of the powerful RCCMD software solution, with which even the emergency behaviour of complex, fully virtualized server landscapes can be realized.

It is no coincidence that the CS141 is the heart of the new SITEMANAGER 6 and SITEMONITOR 6.

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. So, if you have a UPS in use whose interfaces are, contrary to expectations, not compatible with the CS141, you can use this function to establish compatibility with little effort and cost and thus fall back on the powerful and reliable GENEREX products such as the RCCMD developed by GENEREX.

Note:

As the CS141 Webmanager can act as a stand-alone manager, it can be used flexibly with nearly any task, even outside the functionality described in this manual. This manual therefore describes the basic implemented functionality in connection with UPS systems. The enormous flexibility and the possibility to communicate with higher and lower-level systems in real time.

As individual as your network

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

- SITEMANAGER 6
- SITEMONITOR 6

Please note that - although there are many overlaps - for technical reasons not all accessories are fully cross-compatible, even if the external connector configuration would fit.

This includes for example:

- *Additional sensors and devices*

This includes, as an example, the GSM modem, analogue sensors as well as the SENSORMANAEGR 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, the SITEMANAGER offers analogue and digital inputs, optionally via the terminal strip or the analogue sensor inputs, as well as the complete BACS functionality

The SITEMONITOR offers two AUX ports, via which specially developed relay boards can be addressed, and 64 inputs, which can be configured exclusively via the terminal strip.

In both units, the powerful CS141 is used as the heart:

Unlike the CS141, COM port 1 here is the interface to the UPS and cannot be used for sensors. The menus here differ from the CS141 standard interface, and some functionalities are different. If your unit does not offer a hardware layout, you will not be offered the corresponding menus within the software.

Scope of functions

The SITEMANAGER and SITEMONITOR are specially designed for use in standard server racks. Accessories can be mounted nearby as required, for example, using standardized DIN-RAILS. The SITEMANAGER and the SITEMONITOR offer the option of communicating with the UPS directly via an RS-232 interface as an SNMP adapter or via the RFC1628 smart UPS interface via LAN and of acting as a fully-fledged web manager.

Standardized included functions are:

-SNMP und SNMP Traps:

The SNMP (Simple Network Management Protocol) is an Internet standard protocol for monitoring installations via IP networks. The protocol is defined and standardized via RFC specifications. UPS systems generally use the RFC 1628 specification as MIB, which defines UPS-specific devices. Therefore, it is usually not necessary to insert an own MIB into the SNMP software. SITEMANAGER and SITEMONITOR can fulfil 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 switched to active, etc. The current switching states can be both time-controlled and switched reactively in the form of switching chains, including feedback. A specially defined message can be sent automatically for each switching status.

-Remote control of UPS functions

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 is part of the UPS.

-Multiple Server Shutdown via RCCMD:

With RCCMD, all models of the CS141 product family can initiate a network shutdown. A TCP/IP-based RCCMD signal is sent to all configured RCCMD clients. This also allows shutdowns to be initiated 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 licences are available from your UPS dealer.

-Time critical log files:

Both, SITEMONITOR and SITEMANAGER have their own set of log files to accurately log events and alarms. This log file is accessible via UNMS, UPSMAN, GUI and FTP. The export as CSV file allows easy archiving for later diagnosis.

-Advanced mail communication features:

Each model of the CS141 family provides a Simple Mail Transfer Protocol (SMTP) compatible email client that can automatically send emails in case of a system events it is configured to.

-Integration of 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. Furthermore, it is possible to interact with higher- and lower-level monitoring and management systems via pole-free contacts.

-Modern and light-weight web-based technologies for intuitive configuration:

Each model of the CS141 product family provides his own a web interface that displays all information of the unit. By doing so, all system-critical information is available and displayed graphically. And, of course, the web interface is accessible with a common web browser.

- *Modbus, BACnet and Syslog*

Both, the SITEMANAGER and the SITEMONITOR provide a connection to existing network monitoring concepts, e.g., Modbus, BACnet and remote syslog for transparent and individual adaption to any existing building maintenance and monitoring concepts. If the existing system only provides dry contacts, even this is supported.

RS-232 / Pipe-through:

The SNMP adapter type CS141 can output the UPS protocol, which is read via COM1, directly on COM2. This makes it possible to connect further software / hardware to the UPS without using additional distribution hardware (RS-232 multiplexer) - Just activate Pipe Through and connect your SITEMANAGER or SITEMONITOR with an existing CS141 WEBMANAGER.

- *UPSTCP:*

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

- *and many more...*

In combination, all products of the CS141 product family can be used to fulfill nearly infinite tasks even for the most complex networks and combine all existing systems to a unique and holistic maintenance concept

Main Power



The SITEMANAGER and SITEMONITOR 6 offer you flexibility in connecting to the mains:

Both units are supplied with a 24V /1.5A power supply unit as standard. The connection terminal is coded to prevent polarity reversal. Under certain conditions, it may be necessary or useful to use an alternative power source.



For this reason, the connector plug has a modular design. The Sitemanager 6 dynamically adjusts to the input voltage:

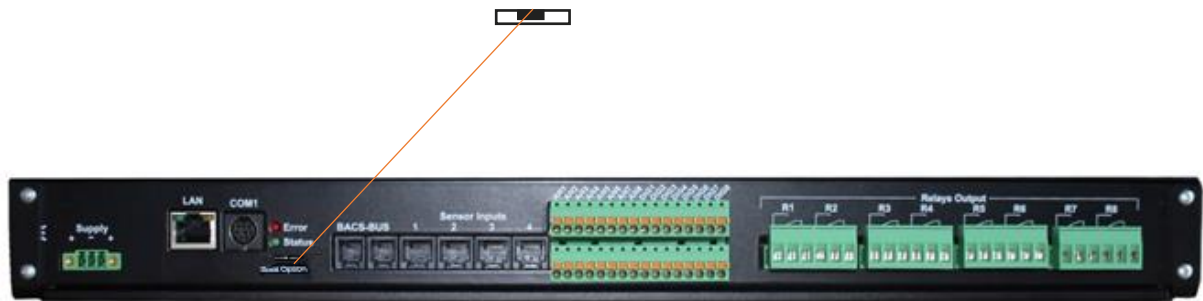
Minimum: 18 VDC

Maximum: 75 VDC

To avoid damages to the device, please respect the correct wiring ...

Network integration of the CS141

All models of the CS141 family are configured exclusively through the specially designed web interface. In order to facilitate the initial configuration or a quick on-site intervention, the CS141 family Web Manager's present is the hard-coded IP address 10.10.10.10:



You will recognize this pre-setting that the slide switch is in the middle position on the front side. Due to its more compact design, the CS141 MINI brakes the standard and uses on-board dip switches instead of a sliding switch.

You will recognize this pre-setting that the slide switch is in the middle position on the front side. Due to its more compact design, the CS141 MINI brakes the standard and uses on-board dip switches instead of a sliding switch. The centre position or alternatively both dip-switches set to off position activates the configuration mode: In this mode, some functions such as IP address data are configurable, but available only as soon as CS141 is switched to regular operating mode.

The following table lists regular operating modes:

<p>Sliding switch to centre position:</p> <p>Enables configuration mode. After reboot the hard-coded IP address 10.10.10.10 is active.</p>	
<p>Sliding switch to the right</p> <p>Automatic IP addressing: DHCP is activated and an IP address is set automatically. Check the MAC address of your CS141 to identify the IP address in the DHCP server table.</p>	
<p>Sliding switch to he left</p> <p>Use of the IP address values manually configured. If DHCP is used, the IP address needs to be blocked for single usage.</p>	

First configuration 10.10.10.10Preparation: SITEMANAGER / SITEMONITOR

On the very first start, the sliding switch is in left position but the IP address 10.10.10.10 is active. Once you have entered a valid IP address or activated the DHCP mode (both is possible), the device will restart and take over the new settings. In any other case, you need to set the sliding switch on the back to centre position and reboot the device.

On restart, the device will automatically fall back to the hard coded IP address 10.10.10.10

Preparing the Workstation

After starting, the CS141 Web Manager can be found using the following network address:

IP address 10.10.10.10
Subnet Mask: 255.255.255.0

Depending on the type of connection you choose, the service computer can be connected directly to a crossover cable or via the local network segment.

This is recommended network settings for the computer:

IP address 10.10.10.11
subnet mask of 255.255.255.0
Gateway 10.10.10.11
DNS: none

Obey whether the settings of your service computer work by opening a console in order to enter the command

"PING 10.10.10.10."

```
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
Antwort von 10.10.10.10: Bytes=32 Zeit<1ms TTL=64
Antwort von 10.10.10.10: Bytes=32 Zeit<1ms TTL=64
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>
```

If the settings are correct, the CS141 will respond accordingly. As soon as the CS141 answers correctly, open a web browser. The CS141 web interface will be accessible by tipping <http://10.10.10.10>

Adding a route

Within larger installations with well-defined domain services, it may be helpful temporarily editing the routing table.

In case of using a route, ensure the CS141 is located within the same network segment and is therefore directly accessible

Example: Adding a route into a Windows-driven Computer:

1. Run the command console cmd as *administrator*
This is important due to the fact; Windows requires a user with local administration rights to add a route.
2. Enter the following command: `route add 10.10.10.10 <IP address of your system>`
Windows will accept the command and return *OK*

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

In order to check the new rout, enter the command *route print*

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

Under active routes, 10.10.10.10 should be seen. As an additional test, use the command ping 10.10.10.10 to verify the CS141 web manager is responding as expected.

Note:

In configuration mode, only one CS141 with the default IP address of 10.10.10.10 can be operated. If you connect several devices at the same time this way, a network conflict is unavoidable.

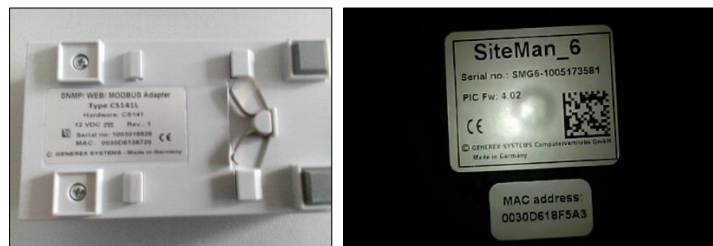
The DHCP mode

Since the models of the CS141 family can fulfil many functions due to their flexibility, it is a quite realistic scenario that you have to operate several units simultaneously within an installation and that no fixed IP address can be assigned for the time being.

To activate the DHCP mode, slide the slide switch to the right, i.e., to the outer edge of the CS141. At the next restart, the web manager will boot in DHCP mode according to the hardware configuration and obtain an IP address from your network.

Useful information for the DHCP mode

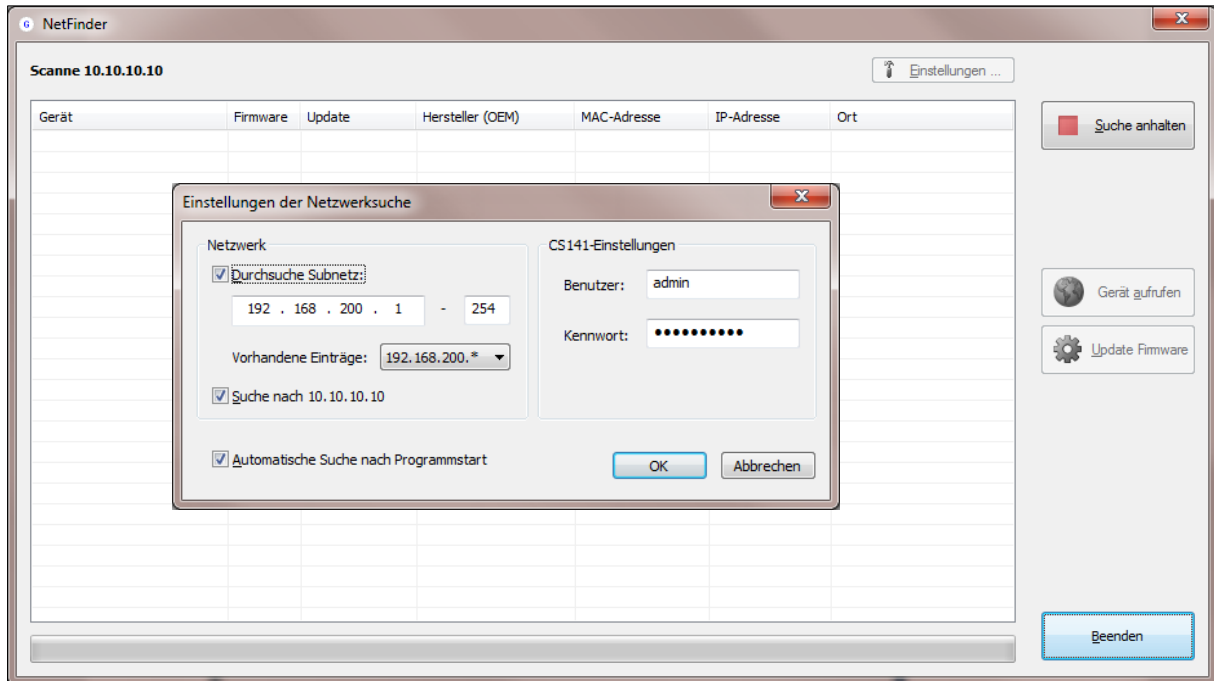
In order to be able to clearly assign the units after the hardware installation, copy the MAC address and the installation location before installing the device. The information can be found on each web manager of the CS141 family as a sticker:



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

Netfinder: Finding your IP address

To read out the IP addresses, use the Netfinder tool, which is available on the support CD coming with the SITEMANAGER / SITEMONITOR. However, it can be also be downloaded from www.generex.de. Netfinder is a useful software tool that can display all CS121 and CS141 devices that are reachable within a network node.



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

Netzwerk von 192.168.222.1 bis 192.168.222.254 - scanne 192.168.222.168						
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	ALTERVAC (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 standard search always refers to the network segment in which the service computer is located. To scan other networks and subnets CS121 or CS141 installations, specify the corresponding IP address range. Please note: Technically, if you configured your computer to use the IP address 10.10.10.11, it may not work. You need a valid IP address.

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, one can find all devices again with the Netfinder

Operation mode of the web manager

The difference between configuration mode, rescue mode and operation mode

All models of the CS141 family can be configured exclusively via an intuitive web interface. The web managers offer 4 valid hardware operating states, which are fundamentally different from each other:

1. The configuration mode

The sliding switch is in centre position.



Configuration mode is the mode in which the manager is delivered by default. In this mode, the web manager is accessible via a hardware-preset IP address 10.10.10.10 and allows all system-relevant settings. Since the manager generally uses the pre-set IP address in configuration mode, you can also import data backups here and adjust them after restarting.

2. Der regular operation 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.

Der manual mode



In manual mode, you define the IP address data as a software feature: 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. As a special feature, within the manual mode, you may choose between DHCP / manual IP address for both, IPv4 and IPv6 independent to each other.

Note:

In manual mode, the data is entered by technicians and thus permanently assigned. The CS141 will use this data to make itself known in the network. assigning an address twice will cause a network conflict. In this case, switching back to configuration mode at any time is possible to reach the Web Manager at the default IP address 10.10.10.10.

Der DHCP Modus



In DHCP mode, the CS141 automatically inherits settings assigned by a server and uses them for the IP address settings. The web server takes over the administration of the IP address data. After the start-up process, the web manager can be found using the tool Netfinder.

Tipp:

As a rule, DHCP-assigned IP addresses via automatic mode are reserved for specific time. DHCP clients therefore ask after 50% of this time window whether the IP address is still valid or will be assigned to another client. How statically the DHCP server allocates IP addresses is a decision the system administrators make.

Due to this fact another IP address can be re-assigned after booting or a CS141 seems to be lost during regular operation.

When selecting the operating mode, the function of the CS141 within the network should be considered:

If the Web Manager runs as an active element within shutdown solutions or in conjunction with higher-level monitoring structures, a manually assigned IP address makes sense, since an authenticated and fixed IP address must be configured. As another advantage the CS141 starts faster with preconfigured IP addresses if the DHCP server is not available.

3. The rescue mode

In this mode, an additional jumper is set and the slide switch centre position.

The webmanager can access two ROMs for booting. Therefore, this failsafe design is able to contain the current firmware as well as the last state before the firmware update including the configuration file.

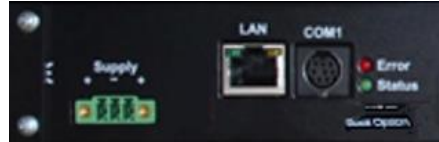
When the web manager is set to rescue mode, the logic starts from the last known state and is initially fully operational again but indicates in the general system information that the web manager is in rescue mode.

The rescue mode represents a manually chosen emergency operation state and is intended to repeat a faulty flash process

Preparing the rescue mode

1. Open the device and search for the small board containing the network interface - as the board itself does not have to be removed, you can orient yourself at the back of the web manager.
2. On the screwed small board, you will find a flat ribbon data cable. Directly below, there is an open jumper. Close this jumper and reconnect the power adapter:

The web manager will automatically start in rescue mode.

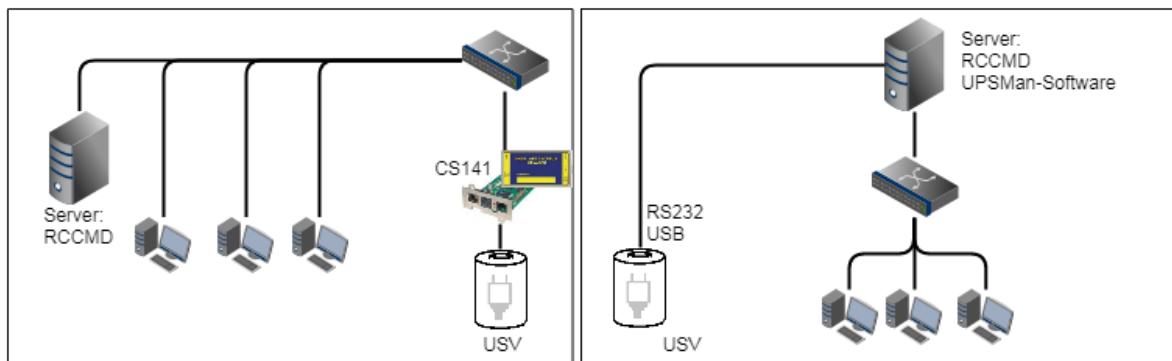


Before you start

Installation examples

The CS141 was designed to provide a maximum of flexibility and freedom during the installation - as a result the CS141 match the tasks of modern UPS systems as well as expectations coming with it. The installation examples will show general scenarios and how they could be solved – depending on your device, the wiring method may differ, but in principle, all models of the CS141 family can be used that way:

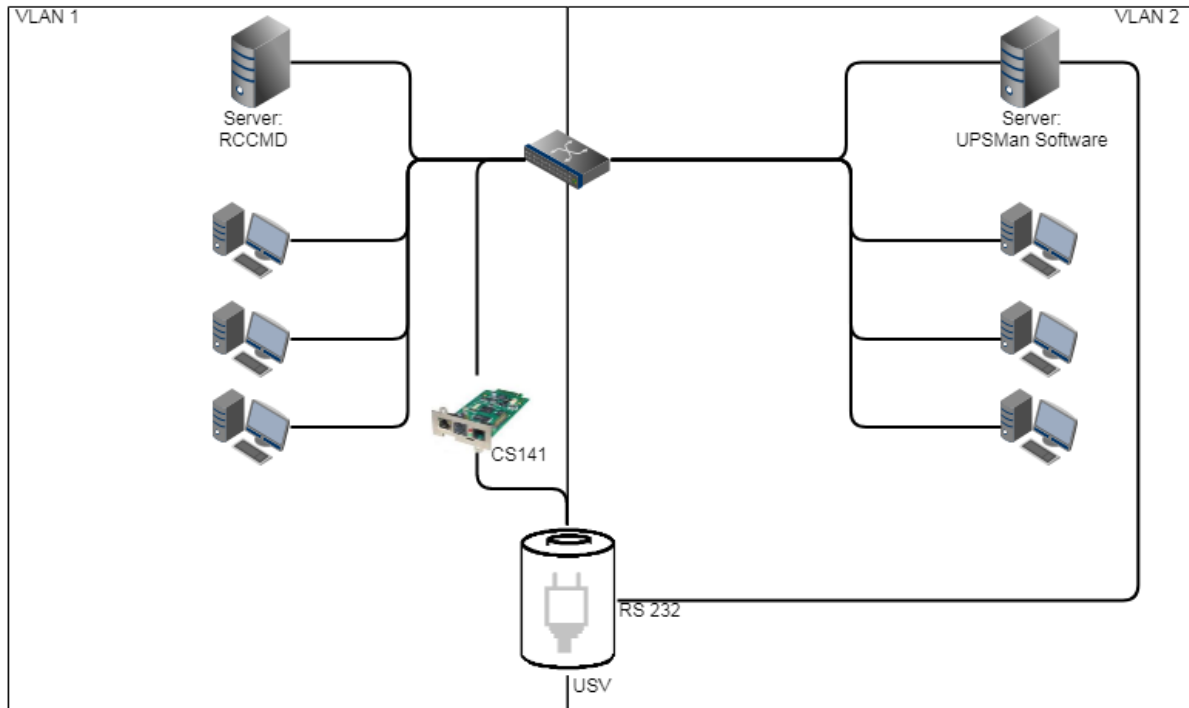
Case one:



The central part of the UPS is to ensure emergency power until the server shut down securely during main power loss. The complete shutdown routine is controlled by the CS141, as this is a full-fledged manager that can act independently. As an alternative to the CS141, the shutdown routine can also be initiated via the UPSMan software. Further servers need only one more RCCMD license.

Two separate networks

It becomes more difficult as soon as emergency power coming one UPS has to ensure the shutdown of two servers inside separate networks without linking possibilities:

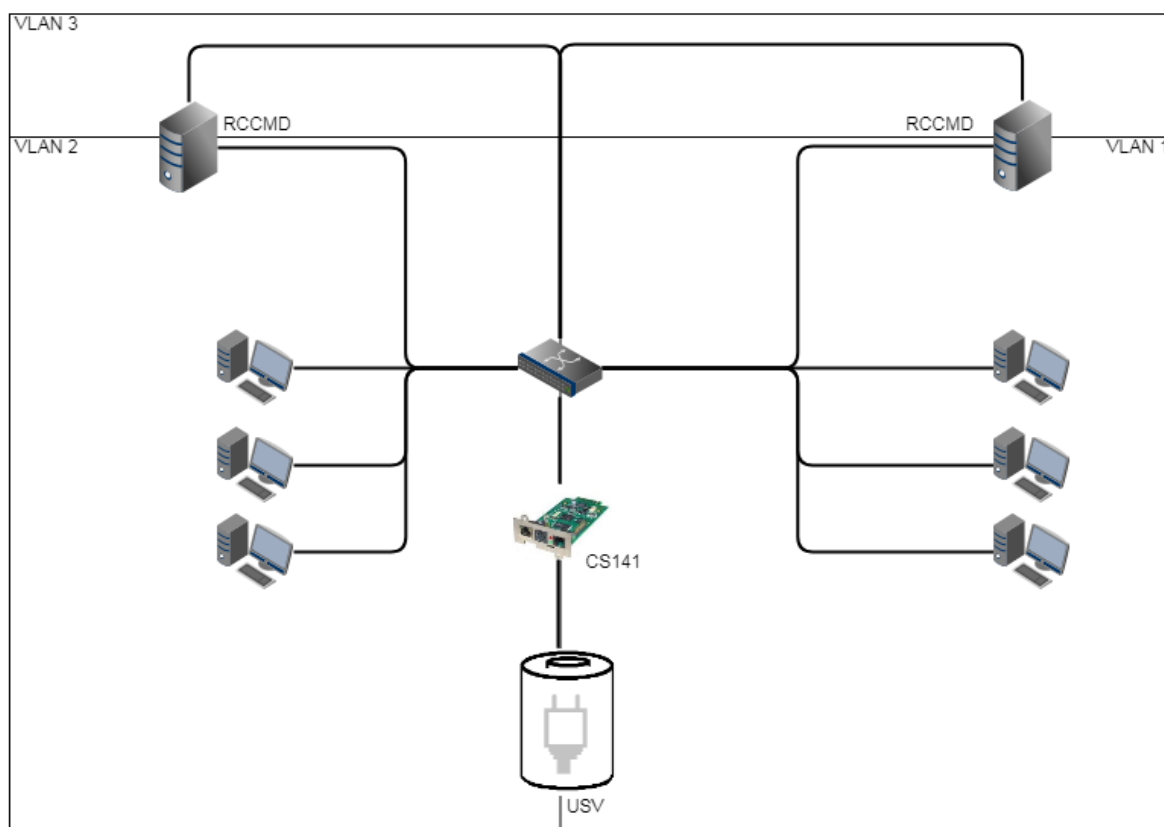


In this case, the UPS becomes a central role inside the network's emergency power security.

Since the VLANs represent physically separated own network segments, only one server can be secured by the CS141. The UPSMan software will secure the second server:

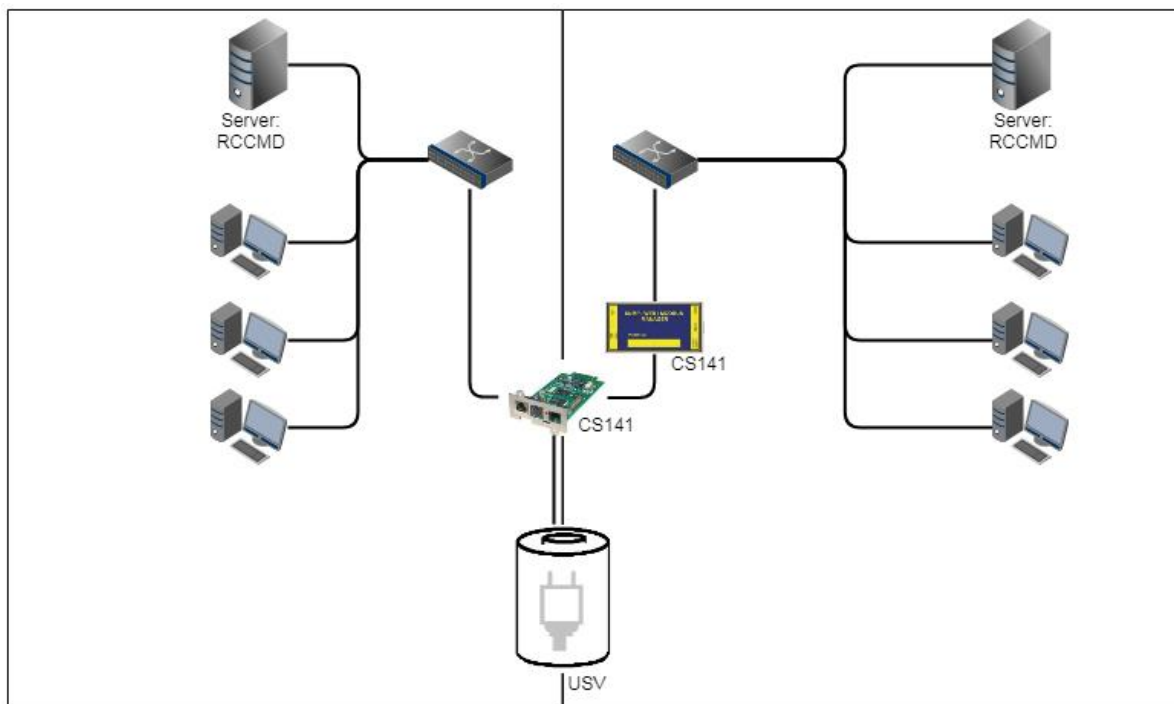
Once Installed directly on the server, it communicates with the UPS via the COM port of the server and offers the same functionality as the CS141 including a full support of RCCMD. Therefore VLAN 2 represents a "software only" solution that does not require a CS141 as additional hardware.

The required RS232 connection is not available or the installation of software is not possible?
Just use servers providing 2 network cards:



If you have chosen a solution with two network cards and the UPS provides a usable RS232 interface, this solution allows future installations - even complete closed up networks are possible.

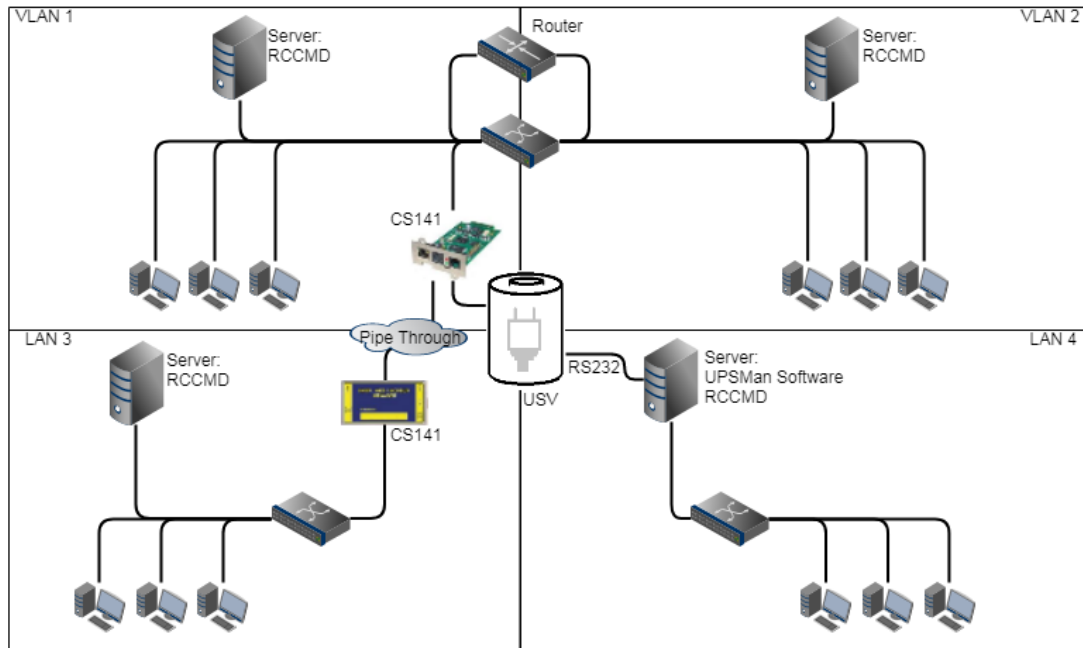
Pipe Through



In some companies, physical separation of the networks is essential, but the UPS does not offer the option of operating RS232 and slot parallelly. In this case, the signal can be looped by the pipe-through function: This feature allows two CS141 jointly perform the same function inside of complete separated networks. Furthermore, different CS141 versions can be combined as desired - Even the combination CS141 / UPSMan software is possible for a maximum of flexibility.

Technical feature SITEMANAGER 6 / SITEMONITOR 6:

The SITEMANAGER 6 uses a Mini-Din connection as UPS connection COM1. As a result, the pipe-through function is generally supported, but for technical reasons SITEMANAGER 6 can only be used as the last device in the pipe-through chain.

Complex network structures

In this example, VLAN 1 and VLAN 2 were logically linked by a router to allow one CS141 sending RCCMD commands to all servers inside of VLAN 1 and VLAN2. At the same time, the Pipe Through function allows the same signal coming from the UPS to a third CS141 physically installed inside LAN3. Due to this fact, the CS141 can completely control LAN3 and ensure a shutdown routine using RCCMD. LAN 4 is connected to the UPSMan software via the RS232 interface and the server itself can act like a CS141 including full RCCMD functionality. This example demonstrates a complex system:

- two complete separated networks
- two logical linked networks
- on central UPS solution to provide auxiliary power in case of main power is down.

Each CS141 or UPSMan is completely informed about the current UPS alarm state. Furthermore, each network can be managed for its own without harming others.

Note.

The UPSMAN software also handles communication via USB - If your UPS supports parallel operation, it is possible to combine USB, Slot and RS232.

The examples shown above illustrate how flexible the CS141 can be adapted to nearly any network structure. Please note that both devices- the SITEMANAGER and the SITEMONITOR - require an RS232 interface for native UPS operation. If this is not possible, there are options to avoid running without a UPS state:

the RFC 1628 UPS interface in companion with well-defined routing:

It is possible to query a UPS over the LAN in parallel to a CS141 and set configurations accordingly - the behaviour is similar to that of a direct connection to the UPS.

Port list

Required Ports

For optimal functionality, the CS141 requires a various number of ports open or available. Some ports are standard ports within your computer, others need to be opened in order to use all functions. Please check on-site whether the following ports are available for usage:

Echo	7/tcp
echo	7/udp
WOL	9/udp
ftp-data	20/tcp
ftp	21/tcp
telnet	23/tcp
smtp	25/tcp
http	80/tcp
snmp	161/udp
snmptrap	162/udp
time (rfc868)	37/tcp
time (snmp)	123/tcp
rccmd	6003
Upsmon	5769
Modbus over IP	502/tcp

This user guide covers all the menus that you can encounter when configuring a CS141. Basically it is written for firmware version 1.62 and subsequent versions with a special eye on SITEMANAGER 6 and SITEMONITOR 6. Many menus will be available for all products of the CS141 family and the configuration method is similar. Once you understood the concept, you will be able configure any device of the CS141 family intuitively.

If you can not find a menu, there are several reasons:

- The CS141 you are using does not offer this feature
- The firmware version you are using is older so the feature this manual describes is not available
- The configuration menu is present, but has been delayed by the ongoing development process

Basic settings

After you enter the IP address, the CS141 responds with its web interface and prompts for a password

There are three users with different system rights to choose from. The users are predefined, the passwords can be freely defined:

User: admin	Password: cs141-snmp	... System administrator, complete menu tree accessible
User: engineer	Password: engineer	... Technician, administrative restricted system access
User: guest	Password: guest	... guest account, only status indicators visible

To start initial configuration, log in with user admin and default password cs141-snmp

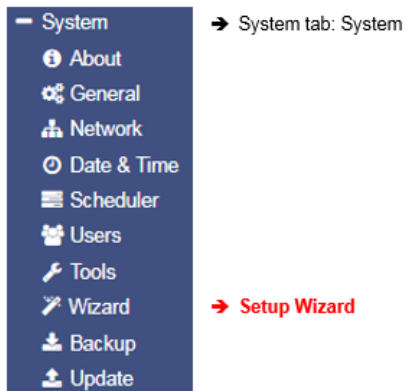
Note

Modern web browsers are designed to display websites as fast as possible. Among other things, special techniques are used to pre-load images, pages and query masks are loaded into a buffer for a faster review. In some cases, this web browser behaviour may result in screen errors.

If these phenomena occur, update the browser by pressing CTRL + F5 or clear the cache of the web browser and deactivate additionally installed tools and addons, which could obstruct the presentation.

Der Setup Wizard

For this configuration step, navigate to the following menu:



When you use the CS141 for the first time, the welcome screen will automatically start with the wizard. Please note that you cannot switch through the masks directly, you need to follow by pressing *next*.

The screenshot shows the 'System Setup Wizard' window with the 'General' tab selected. The tabs are: General, Network, Date & Time, UPS Setup, and Review. The form contains the following fields and options:

- Location:** Text input field.
- System Contact:** Text input field.
- Check Firmware Update:** Checkmark icon (checked).
- Region:** Section header.
- Language:** Dropdown menu showing 'English'.
- Temperature:** Radio buttons for 'Celsius' (selected) and 'Fahrenheit'.

At the bottom, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

The Setup Wizard helps to set up a basic configuration:

General

Provides basic information about the location to be installed, system language, responsibilities and temperature scale.

Network

Enter 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

Enter information about the UPS the CS141 shall be connected to

Review

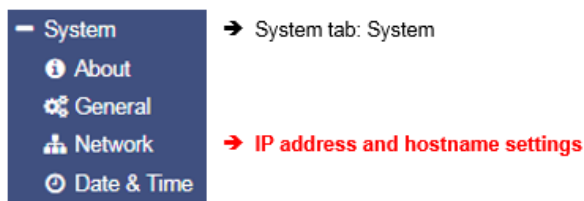
Check data before you finish the configuration process before finishing.

Note:

The Setup Wizard simply summarizes basic settings and provides a quick and convenient solution that can be used to make or change basic settings. If you want to perform the configuration completely manually, click here [Cancel](#) - You can always restart the Setup Wizard in the configuration menu. *But be careful:* Some entries such as UPS configuration have dependencies to advanced configuration entries the Wizard does not include.

Configuration mode: Basic settings

For this configuration step, navigate to the following menu



Most settings can be done as long as the CS141 is in configuration mode. Depending on your network settings there could be a problem when performing tests and forwarding functions - they are often not possible on hardware pre-set 10.10.10.10. Due to this fact it is a good choice to configure all basic settings inside configuration mode and switch to normal mode before starting advanced UPS configuration.

To configure system's network configuration, open *Network*:

IPv4	
Configure	Active
IP Address 10.10.10.10 Subnet Mask 255.255.255.0 Default Gateway 10.10.10.1 DNS Server 10.10.10.1	IP Address 10.10.10.10 Subnet Mask 255.255.255.0 Default Gateway 0.0.0.0 DNS Server

Under Configure, enter the IP address data the system shall use. Active shows the current IP address settings used by the system.

It is possible to change the following settings

MAC 00-30-d5-13-87-20	➔ Hostname: location data, system name, serial number
Hostname cs141	
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 service of the network
DNS Server 10.10.10.1	➔ DNS-Server

On first start-up, the CS141 will get hard-coded information. The required IP address information to enter the operational mode correctly can be obtained by contacting the responsible network administrator. Press Apply to save your settings.

Note:

At this point, the web browser redirects you to the new IP address. Since the CS141 is still in configuration mode, you will receive an error message from your web browser. In this case, ensure to work with the IP 10.10.10.10 and press CTRL F5 to refresh the web browser.

For a first configuration, the Network menu is the only setting you currently need to make in Configuration mode.

It is possible to carry out all other settings in regular operating mode.

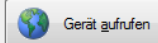
Exception: Initial configuration in case of DHCP mode

DHCP mode during initial configuration

While booting in DHCP mode, an according server assigns an IP address to the CS141 device. This IP address can be found comfortable by using the freeware tool Netfinder.

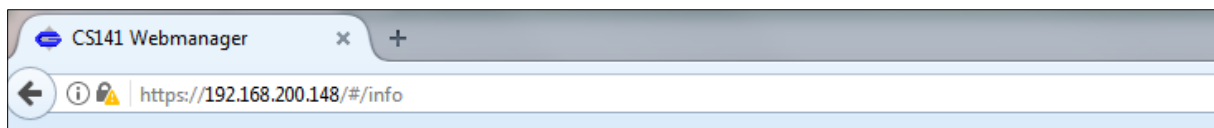
Therefore, it is easy to identify the device by the MAC address shown by Netfinder and the address label glued on the CS141 device:

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	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	
CS131	5.58	Verfügbar (5.62)	Generex (12)	00-03-05-0E-2F-49	192.168.200.227	FB Office



The function open device opens a separate web browser and inserts the IP address automatically.

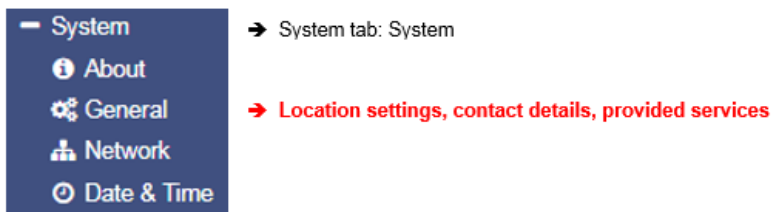
After login, it is possible to access network settings and change the IP address. after rebooting the device with manual mode setting, new IP address setting is active. By switching back to DHCP mode, these settings are completely ignored and the CS141 falls back to server-assigned address.



The advantage is as many CS141 into the network at the same time without much effort, which are immediately accessible without the possibility of an address conflict. The disadvantage is the fact that in DHCP mode the IP addresses can change dynamically, which means that higher-level or docked shutdown solutions may no longer be able to access or output errors.

Advanced basic settings

For this configuration step, navigate to the following menu:



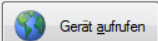
Location description

Location data can be read by software that supports this option. If you monitor many sites with multiple installations, you can use this function to facilitate the mapping of installed devices.

Location	<input type="text" value="your location name"/>	→ Enter a physical location the device runs
System Contact	<input type="text" value="administrator, numbers, ..."/>	→ Enter responsible staff or department to be called
Customer Signature	<input type="text"/>	
Check Firmware Update	<input checked="" type="checkbox"/>	→ If checked, the CS141 reports firmware updates

Apply will save the settings and restart according services to activate the new settings instantly. Netfinder will find the new name next to the IP address:

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	192.168.200.204	Allgemeine Anlage 3
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	



Regional settings

→ Select the language for configuration menus

→ Select temperature measurement scale

Under Language, select your preferred system language. Supported languages are German, English, Chinese (Simple), French, Spanish, Polish, Portuguese

Under Temperatures, select the unit of measure in which to display the temperatures.

The Difference between Fahrenheit / Celsius

Although initially defined by the freezing point of water (and later melting point of ice), the Celsius scale is officially derived among Kelvin scale: Zero on the Celsius scale (0 ° C) corresponds to 273.15 K, with a temperature difference of 1 ° C which is equivalent to a difference of 1° K - the size of the unit in each scale is the similar. Therefore 100 ° C, the previously defined boiling point of water, equates to 373.15K. Due to the fact the Celsius scale is an interval system, but not a ratio system, means it follows a relative and not an absolute scale.

This is indicated by the fact that a temperature interval between 20 ° C and 30 ° C is the same as between 30 ° C and 40 ° C, but essentially 40 ° C does not have twice the air heat energy like 20 ° C. A temperature difference of 1 ° C therefore corresponds to a temperature difference of 1.8 ° F.

There both scales are used worldwide, it is important to know in advance which measurement scale to use for configuration.

Note

The CS141 recalculates the values when rescaling the scale and adjusts the settings automatically - but a higher-level system configured to Fahrenheit will inevitably receive incorrect information from a web manager set to Celsius.

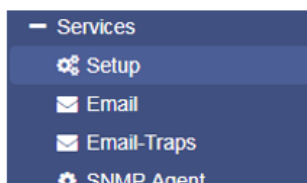
This small problem may lead into a big impact, especially if teams are placed inside an international co-operation.

As an example, on December 12, 1998, the Mars Climate Orbiter has entered as programmed the mars orbit, but 170 kilometres lower than planned. Investigations found the reason for this incident: There was a communication issue between two different groups of NASA scientists who performed the trajectory calculations - one used inches and the other meters. They simply forgot to communicate this small fact...

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

Provide services

For this configuration step, navigate to the following menu:



→ CS141 services overview

→ **Basic settings: Service configuration**

The CS141 uses separate system services for communication, which can be started and stopped independently to each other:

This allows activating and deactivating the functions without having to restart the CS141 completely.

While Modbus and SNMP are used as the industry standard inside almost all higher-level monitoring systems, the UNMS server is only necessary if you use the monitoring software UNMS 2 from GENEREX.

Webserver

to increase security, the configuration by using SSH console is no longer allowed, the integrated web server is the only communication option for configuring the CS141.

Disabling HTTP will restart the device without starting the web interface. By disabling, no further configuration is possible. The CS141 therefore issues a direct alert before disabling this option. Ensure your configuration is done perfectly - Disabling the HTTP Server cannot be withdrawn without physical access to the device.



Why it is possible to deactivate this server?

In some cases, it is necessary to ensure a minimum of possible interactions. The CS141 takes care even in this seldom cases:

Depending on its configuration only additional sftp-access is possible in order to download data logs. Therefore, the admin password can be known without consequences of network security.

Note:

The rescue system on the CS141 has not only saved the last firmware, but also the last configuration before your update. If you intend to deactivate the http functionality, it is recommended to perform a firmware update before this last configuration step:

By doing it, you will be able to access the system by its build-in rescue mode.

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 controls the communication between the monitored devices and the monitoring station. Thereby SNMP describes the structure of the data packets that can be sent as well as the entire communication process.

It was designed to ensure any network-capable device can be implemented into monitoring systems.

Possible tasks of network management using SNMP include:

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

With its simplicity, modularity and versatility, SNMP has become the standard supported by most management programs as well as endpoints.

If you want to use SNMP in your network, leave the check mark active for this function.

Modbus

Fieldbuses are bus systems that connect field devices like sensors or actuators inside a complex operating scenario to allow communication to an according full-automated managing system.

If several communication partners send their information over the same line, it is necessary to ensure communication about fixed rules:

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

To ensure this communication, there are standardized protocols to be used.

Some historical facts about Modbus:

The Modbus protocol was launched in 1979 by Gould-Modicon for communicating with its programmable logic controllers and has become an unofficial standard for industrial usage 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 - Fieldbus for use in industrial control systems). The second generation of fieldbus technology is based on real-time Ethernet.

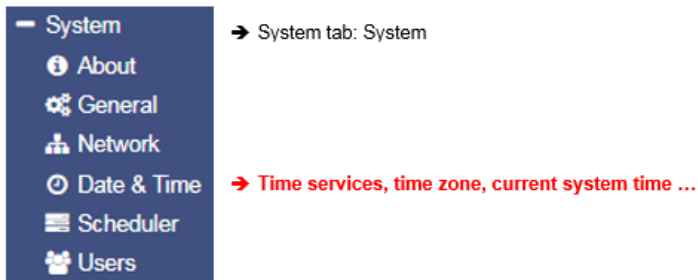
UNMS Server

The UNMS server was specially developed to communicate with the universal network management software from GENEREX. The powerful successor UNMS 2 communicates via UPSTCP on port 5769. The UPS server service enables or disables availability through this port.

When using an UNMS / UNMS2 – Software product, this function should be left enabled.

Date and Time

For this configuration step, navigate to the following menu:

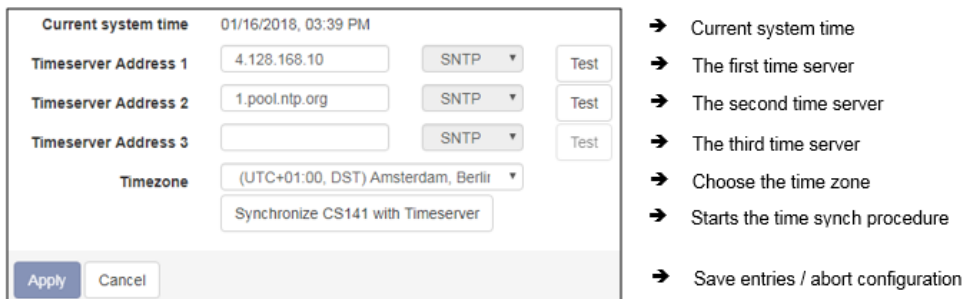


Surprisingly some system critical duties like logging or running recurring tasks require a reliable Realtime-clock. For this reason, the CS141 provides an own system clock but also offers the ability to query external NTP servers. For maximizing failure security, the CS141 can even set and read the internal clock of the UPS if supported.

Automatic clock correction

Surprisingly some system critical duties like logging or running recurring tasks require a reliable Realtime-clock. For this reason, the CS141 provides an own system clock but also offers the ability to query external NTP servers. For maximizing failure security, the CS141 can even set and read the internal clock of the UPS if supported.

Automatic time adjustment



If the network settings are set correctly and CS141 gets an internet connection, you can use the default server settings. In case of a local time server inside a closed-up network segment, the CS141 provides to use an IP address instead of name services. If internal time services used, we recommend the option to enter an IP address although a DNS-Service is available:

If DNS lookup fails, the NTP synchronization will not run.

Note:

A time server normally provides preformatted time containing information about used time zones. 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.

Pressing Apply will save the settings and restarts the time server service inside the CS141 without rebooting. As soon as the time service accepted the new settings, the first-time synchronization follows.

How to set up a custom time server

In order to use a custom time server, a PC needs an NTP service.

Important:

Please note in case of using a Microsoft Windows operating system:

From professional Edition, Windows operating systems offer an integrated NTP service. Unfortunately, this internal NTP service provided by Microsoft Windows is not compatible for using with CS141.

Numerous freeware tools located on the Web, which can provide this service, too - therefore it is not necessary to use Microsoft's internal NTP service. These individual providers differ in the points

- User guidance
- Installation
- Pricing for additional features
- Supported Operating Systems
- ..

A well-made little tool is NTP for Windows, we exemplify in this manual. Due to the fact this is a freeware tool, the download source may differ after writing this manual.

Step 1: Download the tool from the Internet:
Possible download sources would be

The download area of the news service heise.de

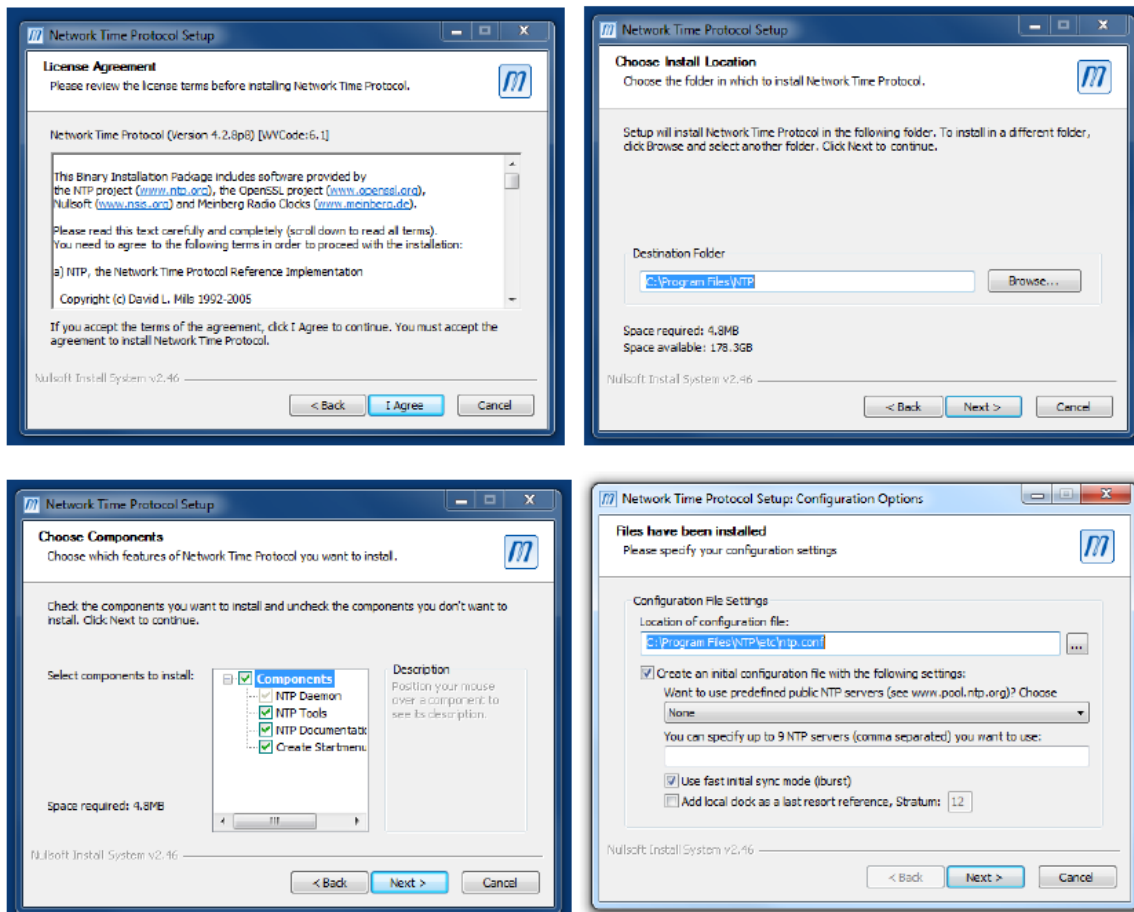
<https://www.heise.de/download/product/ntp-fuer-windows-49605/download>

Meinberg, provider of this tool:

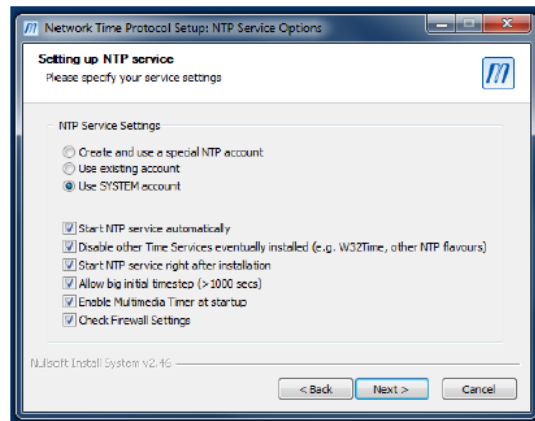
<https://www.meinberg.de/german/sw/ntp.htm>

Please note, download links may differ and even change after writing this manual.
After download, the tool can be easily installed.

Step 2: Start the installation routine. The installer guides you through the complete installation:



Please note that the features selected and working this example may not match your network. If you are not sure if these settings are correct or have trouble after installing, refer local system administrator team.



NTP Tool needs an account to provide time services – Normally you can use this option:

- Use SYSTEM Account

The tool asks to create a configuration file during installation. This is necessary for operation therefore you need to allow it - the tool will create and configure this file for you.

Note:

After installation, you should restart NTP for Windows using the option *Start as administrator*. Otherwise, it could cause problems during operation. If you are not authorized to use this option, please contact your local system administrator.

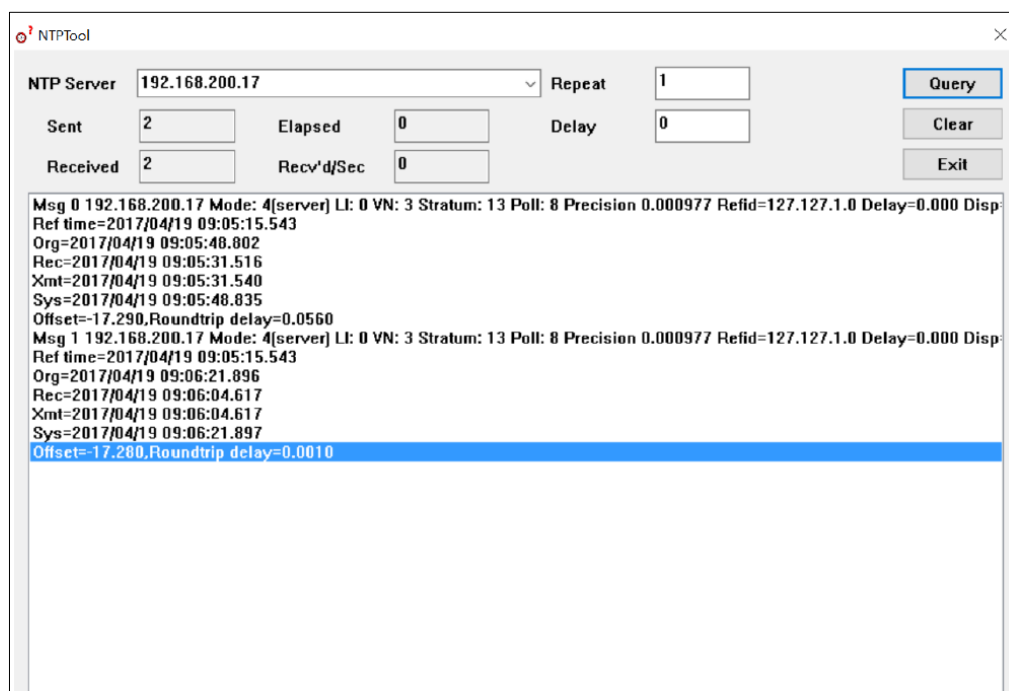
Testing the NTP server tool

If the NTP server has been started, you can check the functions with an NTP server testing tool. Download another freeware tool from the following website:

<http://www.ntp-time-server.com/ntp-server-tool.html>

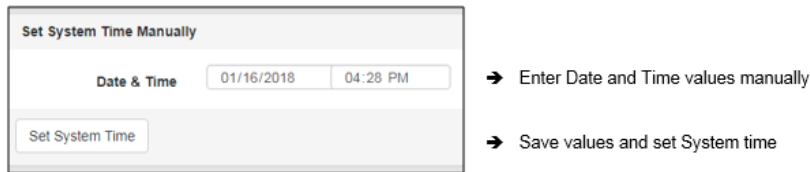
Please note that this tool only returns correct values if the following 2 conditions are completed:

1. The computer with the NTP time server is in the same network segment like the computer containing the NTP testing tool.
2. You use a second computer for testing



The NTP server in this example is installed on a Windows machine dealing with the IP 192.168.200.17, subnet mask 255.255.255.0. Both the test PC and the CS141 must therefore be located within the corresponding IP address space. Otherwise, the NTP server service will not work.

Set up time manually



In some case it may be required to enter time manually. with pressing *Set System Time*, the CS141 will accept the new values and overwrite the current system time. The result can be seen instantly under *Current System Time*. To prevent automatic time correction, delete NTP Server. Please ensure the UPS does not correct it, too.

Note:

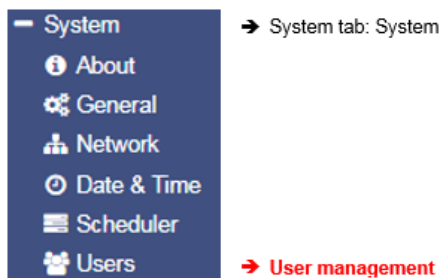
The synchronization with a time server is performed automatically by the operating system inside of the CS141 device. Therefore, you will not find it in event log files. "Device time synchronized" refers to a special function of the UPS and indicates the internal clock of the UPS has been readjusted by the CS141.

Exception:

You have changed the settings and restarted the NTP service using the Synchronize with Timeserver function. in this case, the according user interface subsystem recognizes a manually triggered execution and will insert a log entry.

User management

For this configuration step, navigate to the following menu:



The CS141 provides a pre-set for 3 user profiles to assign different system privileges:

Settings that do not correspond to the corresponding user profile are hidden as soon as the corresponding user logs on. The user names as well as the privileges coming with the users are hard-coded by the CS141. Administrators are only allowed to change passwords:

The administrator

User *admin*
Default-password: *cs141-snmp*

Due to its function, the administrator gets the full range of configuration options. The administrator manages network and mail settings. Furthermore, he is the only user with permission to change the landscape of connected devices.

The technician

User *engineer*
Default password: *engineer*

The technician's user account is restricted to his area of responsibilities - he may access to the functions that relate to technical action. He has the ability to customize and configure available devices and performs the necessary adjustments.

Guest access

User: guest
 Default Password: guest

The guest access is designed to view system monitors without triggering additional functions. Due to this fact, a special feature comes with this user: If necessary, password queries can be deactivated by administrators.

- ➔ Enable/disable password query
- ➔ Enter a new password
- ➔ Verify password

To use guest access without password query, set the mark for Anonymous Access. Otherwise, the CS141 will ask for a valid password.

Note:

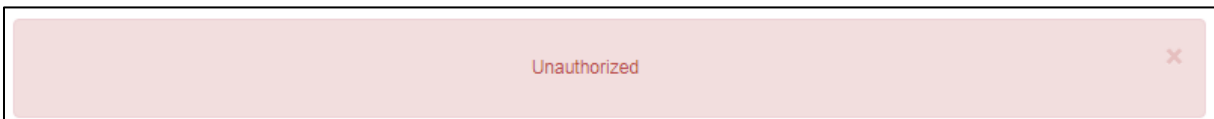
The user *admin* is allowed to manage COM interfaces, but not the user engineer. This is necessary due to the fact, attached monitoring systems may need to be prepared for a change inside the hardware landscape before local hardware or components will be disabled for local maintenance duties.

If a technician already "starts" before administrators stop according monitoring services, wrong alarm states may cause trouble.

How to use guest /anonymous login

The guest access can be used for

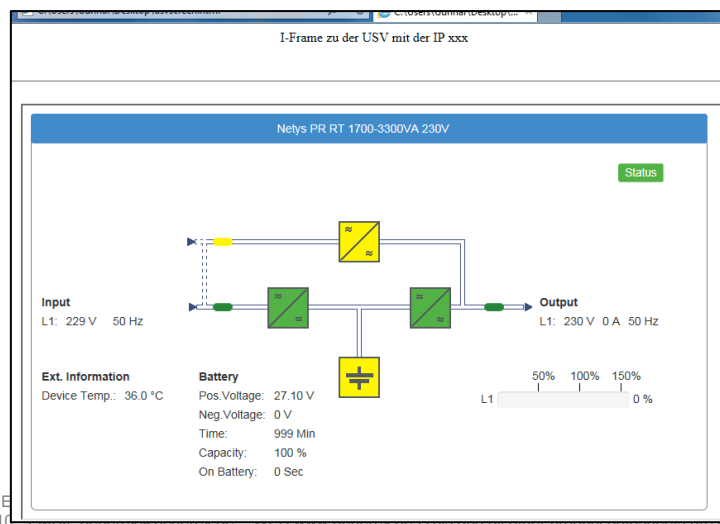
Normally, the CS141 only provides information via its web interface if a user successfully logs in - a deep link to view the UPS monitor directly is treated accordingly:



After activating Anonymous authentication, it is possible to view the monitoring screens directly – it is even possible to create a small html page and set up an i-frame to show it inside larger websites or content management systems. This html code may help you to create the html web site:

```
<html><head></head>
<body>
<center>
<p>I-Frame zu der USV mit der IP xxx </p>
<br><hr><br>
<iframe src="http://<Ihre IP>/www/devices/ups/page" width="500" height="600" name="iFrame" title="iFrame to my UPS"></iframe>
</center>
</body></html>
```

As a result, the UPS monitoring screen will appear inside your html document:



Possible deep links:

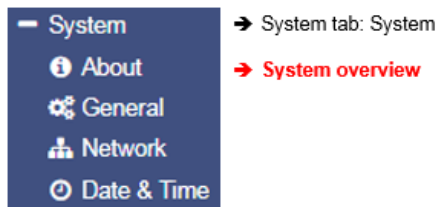
http://10.10.10.10/www/devices/ups/page	Opens the UPS monitoring screen
http://10.10.10.10/www/devices/sensor/page	Opens the Sensor monitoring screen
http://10.10.10.10/www/devices/bacs/page	Opens the BACS monitoring screen.

Note

By using the web query directly, you will notice the URL inside your web browser will change. This is because you start a page request, but the web server on the CS141 responds with a different page and will redirect you automatically: Since the page behaviour is dynamically, the response page may change accordingly. However, the HTML request is standardized with this three deep links and deep links will be served as long as the Anonymous login is active.

System and Setup Overview

For this configuration step, navigate to the following menu:



After completing all basic settings, the advanced system overview will list available information about your CS14. The system overview is divided into several sections:

System overview

Name	CS141SC	→ CS 141 Webmanager version
Version	CS141-SNMP V1.68.12 180319	→ Current firmware
License	Pro Edition	→ Used license key
Manufacturer	Generex	→ OEM-manufacturer
UPS Model	No UPS model defined	→ Configured UPS
Location		→ Location of the device
Time	2000-01-01 01:44:44 (UTC) Coordinated Universal Time	→ Current system time and used time zone
Uptime	0 days, 0 hours, 6 minutes, 55 seconds	→ Uptime since last reboot

If there are questions or some issues during installation, our technical support will help as fast as possible. Please note, our support needs at least following information:

- Firmware
- UPS model and type
- Uptime since last reboot

Hardware

Serial No. 1003600455	→ System serial number
Features bch16	→ Hardware revision

Since 2018, there are two CS141 hardware revisions available on the market. They differ in some aspects inside: All CS141 that are built in 2018 uses a new flash kit. Due to this fact there are some registrations to firmware versions:

Earlier versions of CS141 are fully update compatible, but the newer version is designed to run from firmware 1.66.xx onwards. In support cases it is essentially required to know your hardware release:

- bch16 can run earlier firmware version than 1.66.XX
- bch 8 runs with minimum firmware 1.66.XX

Ensure to use the correct firmware, if you are using *bhh 8* – feature, old firmware will not run.

Network settings

Network	
MAC Address	00-30-d6-14-21-3c
IP Address	192.168.200.113
Subnet Mask	255.255.255.0
Gateway	192.168.200.1
DNS Server	192.168.200.3

→ MAC-Address of yourCS141

→ Configured IP Address

→ Configured Subnet Mask

→ Configured Gateway

→ Configured DNS-Server

The network settings show the current configuration:

MAC address:	The Media Access Control is a worldwide unique address to identify a network device. This address is given by the manufacturer and cannot be changed.
IP-Address:	Shows current IP address assigned to this device. In configuration mode, the default IP 10.10.10.10 is set, even if the IP address configured by administrators differs.
Gateway:	Defines the network device that is allowed to accept and serve requests to the Internet. By default, the configuration mode uses IP 10.10.10.1
DNS	The DNS server provides the translation of names and IP addresses into reachable destinations within networks. In configuration mode, it is the IP 10.10.10.1

Connectivity

Connectivity	
Devices	UPS
Services	Webserver, UNMS Server, SNMP Agent, Modbus Slave, Pipe Through

→ Devices according to COM 1

→ Services this CS141 device provides

Connectivity allows a general overview of the options the CS141 currently provides.

Devices thereby merely indicates a UPS can be connected hardwarely to the CS141, but not the kind of model. Services define the software-related services installed and started on the CS141 to communicate with additional devices as well as software.


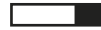

Switch to operating mode

After completing basic configurations, move the slider to the desired position or set the DIP switches accordingly

to enable regular operating mode. After reboot, the device will run in desired mode. if necessary, the device can fall back to configuration mode by setting DIP Switches or sliding switch into configuration mode.

Note that the current switch position will generally take effect after rebooting CS141.

The table below shows the regular operation modes available to the CS141 family.

<p>Sliding switch to centre position:</p> <p>Enables configuration mode. After reboot the hard-coded IP address 10.10.10.10 is active.</p> <p>Sliding switch to the right</p> <p>Automatic IP addressing: DHCP is activated and an IP address is set automatically. Check the MAC address of your CS141 to identify the IP address in the DHCP server table.</p> <p>Sliding switch to the left</p> <p>Use of the IP address values manually configured. If DHCP is used, the IP address needs to be blocked for single usage.</p>	  
--	---

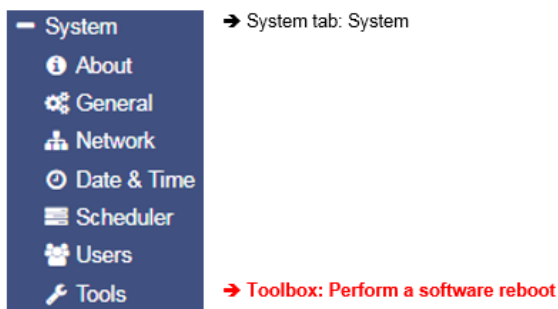
In general, there are two different options to restart the device:

Option 1 – the cold boot

Briefly disconnect power by pulling the power plug or removing the card from the slot. The device will then boot to the appropriate operating state with the new hardware setting.

Option 2 - Reboot by software

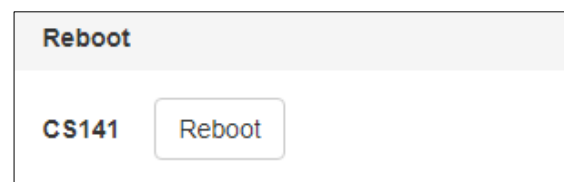
For this step, please switch to the following menu:



The toolbox is restricted for administration usage only.

After login as hard-coded user admin using default password cs141-snmpp, you will be allowed to use the toolbox with extended support features. Please note: The default password is only active in case of no other password was set.

Afterwards it is possible to use the CS141 reboot option.

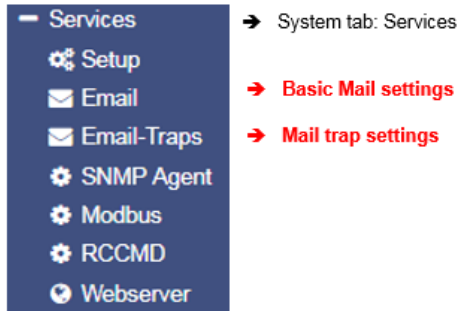


In both cases the UPS will not be restarted, but it only affects the CS141 - your power supply is ensured.

System notifications

Setting up email services

For this configuration step, navigate to the following menu:



The CS141 provides a variety of options to interact with the environment, external devices, and the network itself.

For this, the necessary services must be configured.

One basic feature is the automatic notification via email and email traps. Due to the fact the CS141 does not provide a complete mail server, a valid email account must be configured.

Mail server

Enter the mail server to be used.

To ensure a maximum of flexibility, the CS141 allows an appropriate IP address as well as an URL of external mail provider. Administrators can choose between additional external provider or use own mail servers.

Note:

The fact, your CS141 has a connection to the Internet to access external accounts of large mail providers does not mean an external provider will allow a usage for free. Sometimes they start to block service mails without stating reasons or failure message. It just stops working. In this case, it may be necessary to switch to another provider.

SMTP Port

Defines the port used by a mail client to communicate with the mail server. Basically, the ports are standardized. In some cases, administrators need to choose own ports configurations to ensure communication; The necessary access data must be obtained from the local administrator.

Connection Security

Select the encryption type used by the CS141 for sending the emails:

None	no encryption required
If available	STARTTLS
Force encryption	SSL / TLS

Sender Email Address

Enter the mail address to be shown as sender

Email authentication – user and password

Depending on its configuration, email servers either use the e-mail address as their username or their own user ID and password to receive e-mails.

For the valid access data, please contact the local network supervisor.

Advanced Options

The CS141 offers the possibility to send mail traffic as a blind carbon copy, too.

For some cases, this facilitates the analysis for example, if the sequence of an event has to be examined. With this menu, administrators may specify:

- What else should be sent
- The format to be used
- When it should be sent

- ➔ Define data to be appended
- ➔ Database compliant mail format
- ➔ Condition to appendix data
- ➔ Automated blind carbon copy
- ➔ Mail address of the receiver

Attachments

In addition to a normal message mail, administrators may attach event log and / or the data log.

Format

In some cases, mails will be stored by using database systems. This option enables sending mails compatible formatted.

Log

This setting toggles the conditions whether a sent mail will be registered by event log. Administrators can choose:

- | | |
|--------------------|--|
| Errors only | Mails that indicate errors are recorded in the event log |
| Always | Each mail is recorded as "sent" in the event log |
| Never | The mails are sent but not recorded in the event log. |

Note:

Under circumstances, automatically sending a copy for all emails may cause a flood of messages - each message will be sent as a copy again.

The same applies to Logging option:

Too many entries in the event log quickly may lead into confusing data as soon as you search for special entries within a time window.

With Apply, the settings are transferred to the configuration and the service for sending mails is restarted.

Testing mail settings

This function will be available after successful saving mail configuration. It allows to send a test mail to any valid mail address to test the connectivity:

- ➔ Open/Close Test Email Settings
- ➔ Receiver der Mail
- ➔ Subject
- ➔ Text body of the mail.

Mail error message

Connection refused

This error indicates CS141 cannot establish a connection to the mail server it is configured to.

The reasons for this behaviour can vary. some reasons may be:

- wrong encryption type
- wrong or closed ports
- DNS / Gateway settings are wrong

... or the fact, a mail provider does not allow this kind of mail traffic.

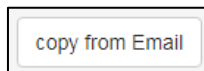
Email-Traps

Mail trap messages are automatically generated by industrial systems for information and status reports. Retrieved and evaluated by a corresponding recipient they are very useful inside semi- or full-automated infrastructures. The difference to a normal email is that there is no option to enter custom text or define a different recipient.

A valid mail account must be deposited to send mail traps.

For details, please refer the Chapter *Configuring UPS*

In some cases, administrators need to use different mail accounts - if they choose to one Email account, CS141 offers to copy registration data directly from standard mail configuration:



By pressing copy from Email, the CS141 fetches the data already entered without passwords:
The password of the mail account needs to be verified by entering manually.

Modbus

Field buses are bus systems that connect field devices like sensors or actuators to communicate with a parent automation device.

If several communication participants send their information through the same line, it is necessary to determine who (identifier) will send what (measure, command) at a specified time (initiative). To ensure this communication, standardized protocols will be used.

The Modbus protocol was launched in 1979 by Gould-Modicon for communicating with their own programmable logic controllers, and has become an unofficial standard in the industry due to the fact 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, downloadable from our website at www.generex.de.

Modbus providing devices

Modbus is a protocol for serial communication. The data is transmitted using 16-bit registers (integer) or data byte status information.

Using Modbus has many advantages:

- The basic structure of Modbus has never really changed to ensure best compatibility over the years. The number of unified devices provides a stable platform for integration, maintenance and configuration.
- This open protocol has been established as an unofficial standard in many industrial machines worldwide. As soon as a device supports Modbus, it can usually be integrated into an existing Modbus network

Modbus can be used as single-master protocol

The master controls the entire transmission and monitors accidental occurring timeouts. The connected slave devices may only send telegrams if requested by the master. For remote control and monitoring of equipment, the Modbus interface in each CS141 can read measuring, events, status information and other things within the master-slave protocol.

Note:

If you do not find readings you are looking for, do not assume this could be an error. As an example, if you are looking for rare or custom UPS functions, it is possible that the according UPS communicates this to the CS141 via SNMP, but the manufacturer does not store a Modbus address for these readings.

As a consequence, the CS141 will show it with its own web interface, but cannot serve your Modbus query.

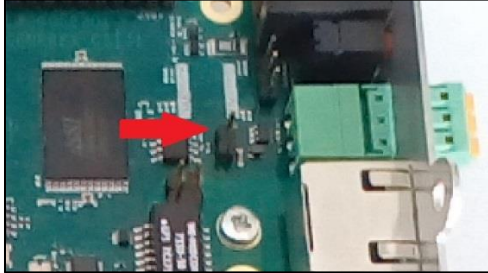
Modbus via RS232 and Modbus over IP

As mentioned, all devices of the CS141 family can handle MODBUS -

there are some differences how to handle Modbus queries:

While the CS141 Modbus adapter can be integrated into a bus with the RS485 interface, Modbus over IP uses a point-to-point connection via RS232. The RS232 Modbus port is commonly used when transferring Modbus data from the UPS to another system or monitoring software. When using Modbus over IP, no terminating resistors are necessary.

Accordingly, the hardware layout of the boards differs



CS141 Modbus



CS141 Professional

In direct comparison, the visual inspection of the CS141 Modbus can be differentiated from the CS141 professional or budget.

Both, the CS141 Modbus and the CS141 Professional, comply with RFC1628 standards. If required, the MIB can be downloaded from www.generex.de in the download area.

Modbus function codes

The CS141 supports 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 a UPS must support this type of commands - the currently available function codes depend on the connected UPS. In general, standard UPS systems provide the functions 03H and 04H. The CS141 is designed not to distinct between these two functions.

Furthermore, the CS141 supports a query speed up to 38400 baud to allow a flexible integration into existing IT environments.

Modbus error codes

Excepted broadcast messages, where the master device sends requests to the slave device, the master expects a clear and valid response from the slave he queried. If the answer does not match with expected specifications, the packet will be discarded with a corresponding error message.

There are several possible events that may occur when a slave answers to a master's request:

1. The slave responds accordingly with a data packet that is both, correct and valid.

The master will handle it accordingly.

2. The slave unit does not receive the request the master device sends.

This event occurs, for example, in case of a communication error. from the point of view of the master the request was not answered. As a consequence, the master will assume an appropriate timeout incident.

3. Master or slave will send invalid queries / answers

Such a phenomenon can occur if the termination resistors are not set up correctly: Although data is being sent, there are clear parity, LRC, or CRC errors within the data packet. Since invalid packets are discarded, the slave will usually ignore an invalid request without answering. However, the master's reaction will differ: In general, he will handle a faulty slave response with a corresponding timeout message.

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

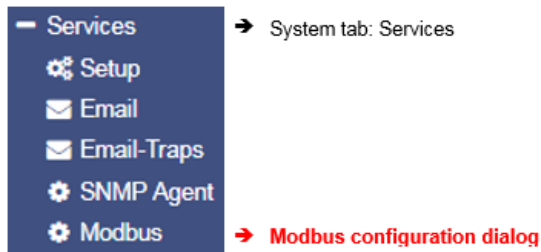
This occurs if a requested register does not exist. If the slave unit receives a valid request, but the requested readings are not available, the slave unit will respond a specific exception message in order to inform the master about the reason for this error.

The CS141 provides these error codes:

- 02H - Illegal Data Address
The address data obtained with the valid request is not a valid address servable by the slave.
- 03H - Illegal Data Value
A contained value inside a valid request is not an allowed for this slave.
- 06H - Slave device busy
The slave has received a valid request, but is currently busy with a time-consuming or time-critical process. As a result, he cannot serve the master for now. For the master, there is no reason to assume a timeout- he will repeat the request sometime later.

How to configure Modbus

For this configuration step, navigate to the following menu:



Since Modbus is standardized, the basic configuration is intuitive to handle. To configure the Modbus agent, go to services and open Modbus.

The image shows the 'Modbus' configuration dialog box. It has a title bar 'Services > Modbus'. The dialog is divided into two sections: 'TCP' and 'COM2 (RS232 / RS485)'.
 In the 'TCP' section, there are three fields: 'TCP Port' (502), 'Max Connections' (10), and 'Slave Address' (1).
 In the 'COM2 (RS232 / RS485)' section, there are three fields: 'Baud Rate' (38400), 'Parity' (n), and 'Stop Bit' (1).
 At the bottom, there are 'Apply' and 'Cancel' buttons.
 Annotations on the right side of the dialog:
 - An arrow points to 'Port 502: Standardized Modbus address'
 - An arrow points to 'Maximum concurrent device access'
 - An arrow points to 'Modbus-ID of this device'
 - An arrow points to 'Data transfer speed'
 - An arrow points to 'Parity-Bit'
 - An arrow points to 'Stop-Bit'
 - An arrow points to 'Save / Abort' (referring to the Apply button).

TCP Port 502

The TCP port 502 is a static port setting within the Modbus standard that cannot be changed or customized without leaving standards - This port value is hardcoded inside the CS141 source code.

Slave Address

The Modbus slave is the ID that make a Modbus device addressable. The Slave ID mentioned by a master's query will cause this device to answer This ID may be customized, but only exist once inside a Modbus network.

Note:

Doubling a Modbus Slave Address will not result in a complete network short-circuit - if the ID is requested by a Modbus master, both addressed slave devices will respond. This will cause the Modbus Master to display misleading data accordingly or assumes a timeout due to the fact the data packets are not valid.

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

Baud Rate

The baud rate defines the data transmission speed for Modbus queries and answers. Please note that the polling speed through the master must be identical to the answering speed configured at the slave to avoid communication lost issues.

Parity

When transmitting data in the form of a bit stream, the parity bit will ensure an error detection can be performed.

The value of the parity bit is calculated by the transmitter and communicated to the receiver accordingly. The receiver of the data stream uses the same Modbus mathematical algorithm to verify valid data and find corrupt data packets. Thereby Sender and receiver must therefore agree beforehand on how to perform the parity calculation:

The parity calculation can be interpreted as even or odd.

Example: even parity

If devices agree to calculate with even parity, the number of all "1 bits" will be counted within the data word. The task of the parity bit is to set the result to an even number:

Therefore, if the number of bits to be checked within a data packet is even, the parity bit must be transferred as 0, otherwise the total count will be not an even value. Differently configured devices would therefore declare an odd or an even value valid and discard other data packets accordingly as invalid.

Der CS141 offers three options:

n	No parity control
o	Odd parity control
e	Even parity control

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

Stop Bit

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

Usually, a corresponding start bit is sent before a data word transmission starts. Start/Stop bits allow a receiving device to recognize the beginning as well as the end of a data word inside a data stream. In principle, it is also a high signal, but the level of the signal differs from the subsequent data word.

At the end, depending on the configuration, one or two stop bits are set to determine the explicit end of this data word. As a consequence, no valid data word can be present between stop bits and the next start bit:

The receiving device will recognize these data as discardable and ignores them accordingly.

If data transfer issues cause a synchronisation lost, the device will look for predefined bit chains for re-synchronization.

Note:

If more than one Modbus device is on the same ID, they will all start sending data to serve the master's query.

Amongst other things, the start and stop bits within the network will begin cross talking, causing problems with the assignment of valid and invalid data packets.

The Stop Bit function defines whether the CS141 should send one or two corresponding stop bits

Apply/Cancel

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

- Apply: Save changes and restart the service as required
- Cancel: Withdraw settings and return to current state.
-

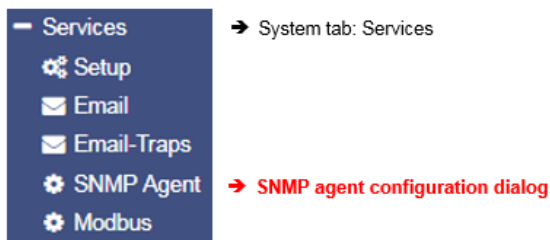
Note:

The standard UPS Modbus addresses can be found in the appendix of this manual starting on page XXX.

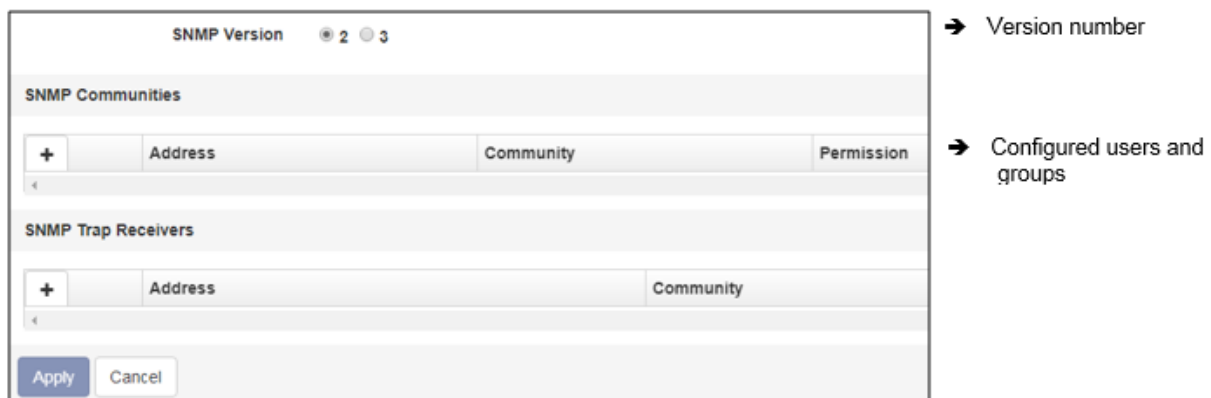
The CS141 uses a valid Modbus reading range from 0-65535. Some Programs like "Modbus Poll" use the same range. Other Modbus polling clients may use 1 - 65536 - in this case, you need to correct this by adding 1 to the original value.

SNMP Agent

For this configuration step, navigate to the following menu:



Developed by the IETF the Simple Network Management Protocol is designed for monitoring and controlling network elements from a central station. The protocol controls the communication traffic between monitored devices and monitoring stations: SNMP describes the structure of the data packets that can be sent as well as the entire communication process. The CS141 can fully be integrated into a network with SNMP monitoring. The build-in SNMP agent regulates both - receiving and sending corresponding requests

**Note:**

SNMP V1.0 is not officially supported by the CS141. We recommend the use version 2.0 upward. However, since V1.0 is largely included in V2.0, the CS141 will respond to SNMP-V1 requests, but using V1.0 will be out of official supporter's guidance.

The CS141 supports SNMP v2 as well as SNMP v3

The difference that SNMP v2 and v3:



SNMP v2 works on behalf of legitimating an IP address inside user communities, SNMP v3 is based on direct user permissions with name and password.

Configuring SNMP V2:

The overview shows all configured communities:

SNMP Communities			
+	Address	Community	Permission

To configure new SNMP permissions, click **+**

Add Community

IP Address:

IP address required

Community

Permission

Read only

Save

Cancel

- ➔ IP address of the authorized device
- ➔ Community name for access authorization
- ➔ Access authorization type

- ➔ Save changes / Abort configuration

IP address

Under IP Address, enter the IP address of the authorized computer to allow access to the CS141 device via SNMP v2. Thereby the name of the community defines the authorization group.

Permission

Defines permissions during access:

- Read only** Devices dealing inside this permission group have read-only permissions
- Read/Write** Devices dealing inside this authorization group can read and write /delete data packets.

Set up trap receivers v2

Set up trap receivers

What are SNMP traps for?

In principle, an agent monitoring a system can unsolicited send a so-called trap packet to its management station should this be required. Among other things, the status of the monitored device is communicated. On the other hand, the agent can receive and service requests from his manager. There are two ports required by default:


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

If these ports are blocked, the communication will not work.

Configuring trap receivers on the CS141

The advantage of the trap messages is that the CS141 can automatically inform about changes in the UPS.

SNMP Trap Receivers		
	Address	Community
<div> <div>Apply</div> <div>Cancel</div> </div>		

To add a new trap receiver, click ,

Since trap messages are sent exclusively to inform about status changes, no read / write operations permissions are required.

Enter the recipient's IP address as well as a valid community.

With Save button, CS141 takes over the settings and the SNMP agent will be restarted. The CS141 will not need to be rebooted.

Add Trap Receiver	
IP Address:	<input type="text" value="10.10.10.10"/> <small>IP address required</small>
Community	<input type="text" value="public"/>
<div> <div>Save</div> <div>Cancel</div> </div>	

Trap receiver test

Test SNMP Traps		
<p>You can send a powerfail trap and a power restored trap to the receivers defined below.</p> <p>Please note: To test newly added receivers, you must save the configuration first.</p>		
192.168.200.17	public	<div>Test</div>

The Trap receiver can be subsequently tested by pressing the test button. The corresponding test message should be displayed directly in your management program.

Note:

Trap messages are automatically generated messages that do not request confirmation - therefore an agent does never know if his trap message have arrived. Du to this fact, a reception logging is not possible.

Configuring SNMP v3

The overview shows all configured users:

SNMP User		
+	User	Access
◀		

Since SNMPv3 is user-based, you need to configure single users instead of communities. Click **+** to configure a new user:

Add User	
User:	<input type="text" value="My_User"/>
Permission	<input type="text" value="Read only"/>
Security Level	<input type="text" value="No Security"/>
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

- ➔ Add user name
- ➔ Toggle Read/write permission
- ➔ Access control to CS141
- ➔ Save changes / Abort configuration

User

SNMP v3 dispenses with the possibility of setting up authorized IP addresses and user groups. Administrators need to add a local user inside the CS141 device.

Read-only / Read Write

As a standard, any user gets the permission for both - reading and writing. In some cases, this may be not allowed by administrators. To prevent SNMP users from writing data, activate the option *Read only*

Authentication

Defines security level and password control to access the CS141 device using SNMP v3:

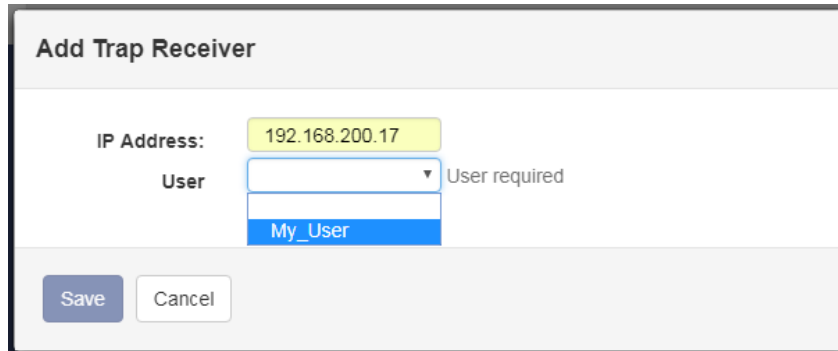
No security	no passwords or encryption is required
Authenticities	Single password request.
Authentication and Privacy	The connection is additionally encrypted and two passwords are required.

Note:

In addition to access data, the encryption type must be identical. Otherwise, no connection will be established.

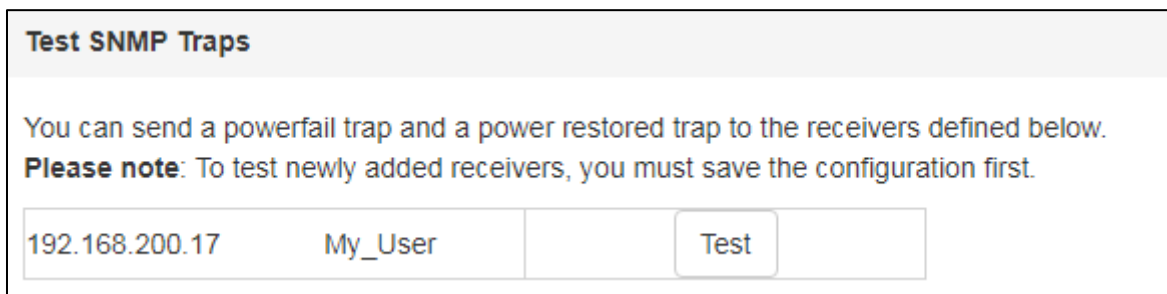
Configure TRAP receiver dealing with SNMP v3

To set up a trap receiver dealing with SNMP v3, you need to create a suitable user. This user can then be selected as the trap recipient in SNMP v3.



The 'Add Trap Receiver' dialog box contains the following fields and controls:

- IP Address:** A text field containing '192.168.200.17'.
- User:** A dropdown menu with 'My_User' selected. To the right of the dropdown is the text 'User required'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

Trap receiver test


The 'Test SNMP Traps' dialog box contains the following elements:

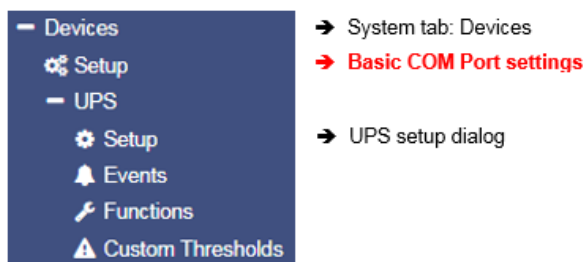
- Title:** 'Test SNMP Traps'.
- Text:** 'You can send a powerfail trap and a power restored trap to the receivers defined below. **Please note:** To test newly added receivers, you must save the configuration first.'
- Fields:** Two input fields containing '192.168.200.17' and 'My_User'.
- Button:** A 'Test' button.

The Trap receiver can be subsequently tested by pressing the test button. The corresponding test message should be displayed directly in your management program.

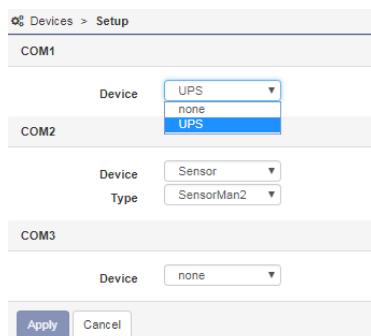
UPS Setup

This configuration step requires 2 menus.

First, open the system tab Devices and click on Setup:



Depending on the design and model, the CS141 provides up to three additional COM ports fulfilling different functions. Please note in some cases submenus will appear to specify functions of devices connected to CS141. To start configuration, go to Devices and press Setup.



The 'UPS Setup' dialog box shows the following configuration for three COM ports:

- COM1:** Device dropdown menu with 'UPS' selected.
- COM2:** Device dropdown menu with 'UPS' selected. Below it, 'Sensor' and 'SensorMan2' are listed as options.
- COM3:** Device dropdown menu with 'none' selected.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

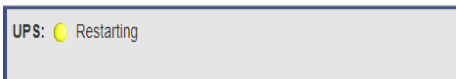
Ensure UPS is selected at COM 1:

As a standard, COM1 the setting UPS should be selected. If not, open the drop-down menu and select UPS.

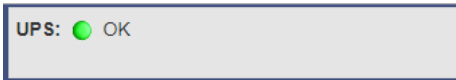
By pressing Apply this selection will be saved and the CS141 will start required services to communicate with the UPS:

Keep in mind by activating this function, a dummy is set first - this is necessary to allow a general access to the corresponding submenus.

The CS141 will display the current starting phase as well as the success of the activation at the upper task bar.

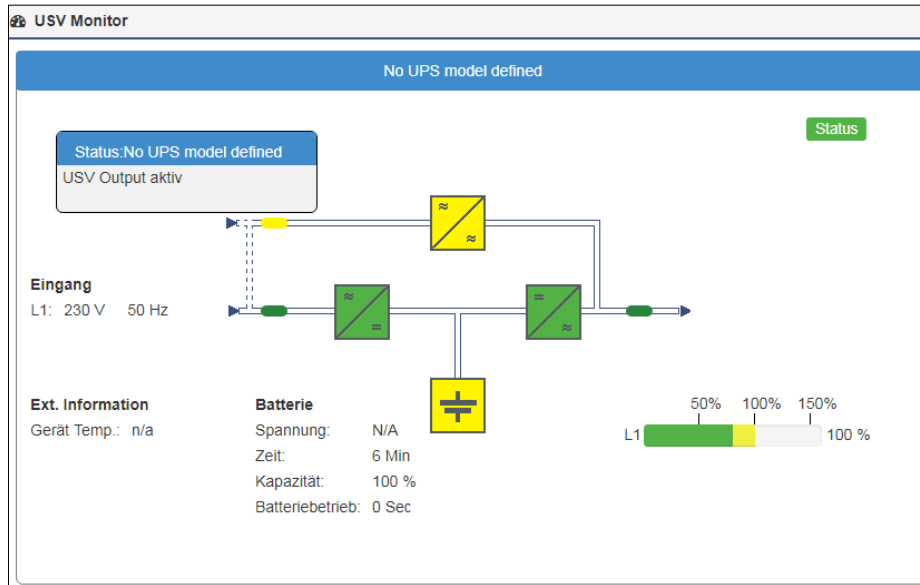


→ UPS service start-up routine in progress



→ UPS feature finished booting, the UPS menu accessible

Please note that only a dummy without a function has been started at this point, even if a UPS is apparently connected and in operation:



Piping Through UPS signals

The COM port 2 is flexible and provides to connect various devices to fulfil different functionalities:

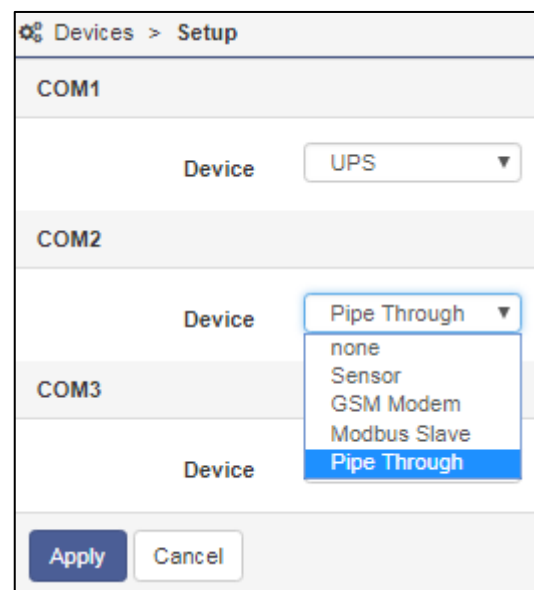
- Sensors
- Modbus
- External modems
- UPS Signal piping

In companion to UPS configuration, the Pipe-Through functionality of the CS141 offers an advantage in UPS signal usage:

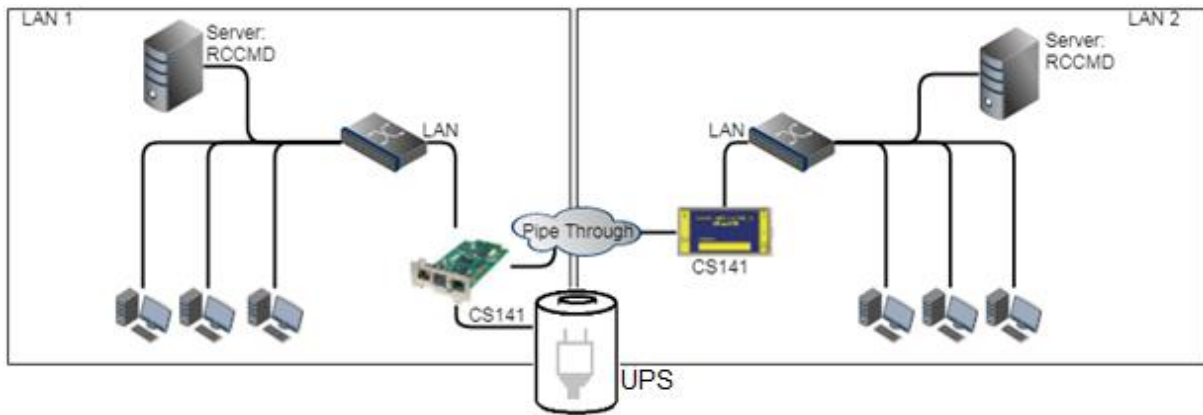
The signal received from the UPS can be piped through the CS141 and will be available 1:1 at COM port 2.

Due to this fact administrators can harmonize emergency shutdown solutions even if they need to use two different and physically separated networks:

Physically separated network resources can be managed for their own and use simultaneously the same UPS solution.



The configuration of Pipe Through is done on the Web Manager connected to the UPS. The second Web Manager is configured as described on COM 1 but is connected to the COM2 port of the first Web Manager instead of the UPS.

**Note:**

When using the pipe-through function, be sure to set the correct COM2 port to Pipe Through. Furthermore, set the same UPS with identical values on both CS141s. All other settings may differ.

When using SITEMANAGER 6 or SITEMONITOR 6:

In general, these devices support the Pipe-Through function, but the connection possibilities are limited. Both, SITEMANAGER 6 and SITEMONITOR 6 need to be installed as second device.

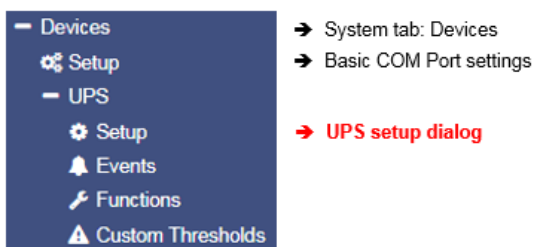
Attention:

In some cases, SITEMANAGER 6 and SITEMONITOR 6 may offer options to change the pre-sets of COM 2 and COM 3. Due to the pre-set fact internal wiring to a second main board is used, changing these values will not work:

Although the CS141 may work in general, all other functions coming with the SITEMANAGER and SITEMONITOR will not be available:

Even the SITEMANAGER 6 and SITEMONITOR 6 will not be damaged by changing these values, the devices are not fully operational.

Proceed to submenu UPS and click on Setup to enter the basic UPS configuration dialog.



This configuration dialog allows to choose the UPS your CS141 is installed to – recommended values will be entered automatically by selecting a UPS:

- Choose UPS model
- Maximum output provided by the UPS
- Maximum load provided by the UPS
- Time window the UPS ensure emergency
- Time needed for a complete charge cycle
- Data transmission speed
- Cable to be used
- If necessary, define a UPS ID
- Installation date of the batteries.
- Battery change notification
- Remaining time the UPS shall shut down itself.
- Save settings / Abort configuration process

In some cases, the UPS protocol does not provide the appropriate data. The CS141 will, based on the data situation, independently calculate the corresponding battery life runtime. In general, these settings do not need to be changed if you can select a UPS model directly from the list - optimized configuration settings will be displayed after selecting the UPS.

if your UPS operates with a system configuration that differs to the basic model, it is possible that you need to adjust these default values: In this case, please refer to your local UPS dealer or the UPS manufacturer of the UPS to get the correct values.

Entering wrong values may cause heavy system failures

Note:

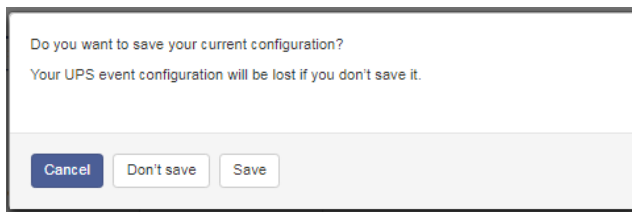
By default, OEM ID 12 / GENEREX SYSTEMS is set. If you want to use a UPS from a manufacturer that is not listed, take a look at the download area of www.generex.de - Search for the firmware for your UPS and install it as a regular firmware update.

Afterwards the corresponding UPS models are available.

Adjustable information about the installed UPS

Model

Defines listed default setting of a UPS including the corresponding communication protocol. When your UPS is listed and communication has been established, telemetry of the UPS typically provides all the necessary data that the CS141 needs to calculate and display autonomy times.



Please note that changing the UPS model will also reset the configuration of the UPS events. The CS141 therefore offers the possibility to create a corresponding backup of the event configuration beforehand:

Cancel:	Do not make any changes to the system
Do not save:	Continue without backup
Save:	Create a Backup of the event handling

Power (VA)

Defines the maximum power in VA the selected UPS in can provide. Exceeding the maximum may cause the UPS getting damaged or even destroyed

Load (VA)

This value defines the maximum load connected to the UPS. Even the possibility is given, exceeding the power VA value can damage or destroy the UPS as well as the installed batteries.

The maximum possible value is less or equal to the value entered at Power (VA).

Hold Time (min)

If main power fails, the batteries of a UPS will ensure this operating time if 100% load is used. The real-life uptime is determined dynamically by the percent of usage: of you use 50% the hold time will raise accordingly.

Note:

Behind the values of power (VA), load (VA), holding time and battery charging time, a mathematical formula is stored - this will allow the CS141 to calculate independently battery operating time and trigger corresponding system events. Thus, allow to use the CS141 even if the UPS protocol cannot provide real-time data - as an example, if a UPS only communicates via switchable contacts or only basic operating states can be detected.

Baud Rate

Different protocols provide different speeds of data transmission. The baud rate defines the speed at which data can be sent and received. An incorrect baud rate can cause communication problems between the CS141 and the UPS.

Cable Type

UPS manufacturers sometimes use specially designed cables for their models. In addition to these in-house developments, there are standardized cable types. This cable types can be used to map different functions and switching states.

UPS-ID

If large UPS systems use more than This one UPS module, these modules can be queried directly via a unique ID. „0“ is hereby a something like a broadcast to allow the CS141 search and manage capability to figure out the number of UPS modules. If you change this value, you only get the exact module with this special ID. Otherwise the CS141 will manage all available modules and display them at the monitoring screen.

Battery installation date

The lifespan of batteries running inside a UPS is limited - regular battery maintenance also requires replacement. In order to keep track of larger installations, you may enter the date when the batteries start into operation.

Battery too old after

If entered, the CS141 automatically indicates regular operating period for the installed batteries will expire. By default, the CS141 logs in with appropriate system notes after 48 months. Editing this value will extend or shorten the default time period until the CS141 will start sending maintenance notifications.

System shutdown time

In principle, the system shutdown time is the last emergency shutdown event that will be executed just before the UPS itself will shut down itself to prevent battery damage. This value can be used to trigger the according system event. Please note that this value is an emergency shutdown – it is not suitable to ensure a regular system shutdown.

Apply / Cancel

Apply allows you to save and restart the UPS service on the CS141. Cancel will abort the configuration process and withdraw all settings – they need to be entered again.

Battery Health Level feature**Battery Health Level(%)**

20 ▼

The battery health level will be automatically provided by CS141 inside the UPS configuration menu if the UPS connected to the CS141 principally carries out battery testing but does not return a reporting value for "Battery test passed / faulty". Thus, the result needs to be determined by comparing two measurements:

Before battery test starts, the battery voltage will be recorded. This value will be compared with the battery voltage to be found after finishing the battery test. The Battery Health Level (%) setting defines the maximum percentage deviation these two values may differ. On exceeding this value, a battery failure will be displayed.

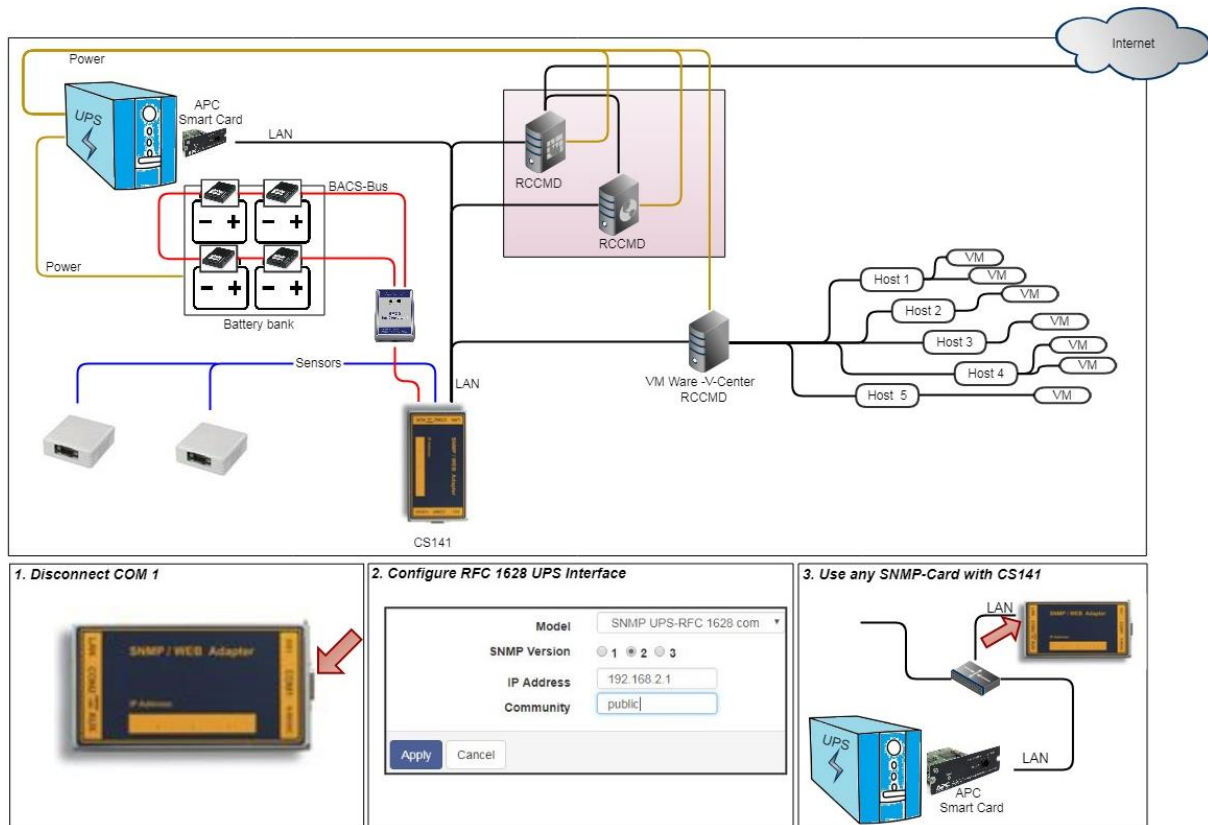
The default setting for this test is 10% deviation - but can be specified with a custom value between 5% and 30%.

Premium feature: The RFC1628 UPS interface

In some cases, UPS manufacturers supply systems that the CS141 cannot communicate to. As an example, known problems are the card does not fit to the slot, or that the data stream sent by the UPS is not compatible formatted:

UPS manufacturers have installed their own SNMP card, which offers similar functions but may not be compatible to your flexible and powerful GENEREX software environment. To ensure compatibility, the CS141 Web Manager offers the option to connect to any card via SNMP. The condition is that the RFC 1628 MIB is supported by the target card. In order to use this function, it is first necessary to configure a corresponding SNMP Agent at the destined UPS.

After that enter the access data in the CS141 UPS menu. The CS141 will restart required services and establish a connection to the destination card.



Setting up the target SNMP card with SNMP v2 at CS141

- Choose UPS model
- Select SNMP Version
- IP-Adresse of the destination
- Select SNMP Community
- Save settings / abort configuration dialog

Model

Choose SNMP UPS-RFC 128 compliant as UPS model

SNMP-Version

Depending on the configuration of your destined SNMP card, choose SNMP version 1 or 2

SNMP Community

Enter the SNMP Community configured at destined SNMP card

Save/Abort

Abort will withdraw all settings, save will restart required services. After restarting the services CS141 will automatically establish a communication to destined SNMP card.

Note:

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

In principle, the APC card can handle the RFC1628 standard - you will be able to query basic information about the UPS. However, the APC cards often use their own OIDs. These OIDs are specific to AP and not conform to the RFC1628 standards.

Therefore, it is recommended to use the APC Smart network setting instead of RFC1628 interface.

Setting up the destination card using SNMP v3 at CS141

Devices > UPS > Setup	
Model	SNMP UPS-RFC 1628 compliant
SNMP Version	<input type="radio"/> 1 <input checked="" type="radio"/> 2 <input type="radio"/> 3
IP Address	192.168.222.116
User	cs141
Security Level	Authentication and Privacy
Auth Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Auth Password	
Privacy Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Privacy Password	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

→ Choose UPS model

→ Choose / change SNMP Version

→ IP address of the target system

→ SNMP User

→ Encryption method

→ MD5/SHA password

→ ES/AES password

→ Apply / abort

All devices of the CS141 family support SNMP v1, v2, and v3.

Enter the access data for the destination card according to your configuration and click *Apply*

Wiring UPS with SITEMANAGER 6 / SITEMONITOR 6

On the back of the device, next to the network connector, is a MINI DIN connector labelled COM 1:

Connect the supplied adapter cable MINIDIN / RS232 and then connect the standard data cable that came with your UPS to the adapter cable.



To ensure proper grip, place the included nuts between the small two latches. The SITEMANAGER or SITEMONITOR displays the data of the UPS in the UPS monitor after a short synchronization phase:

The status LED next to the MINI DIN connector flashes slowly and evenly green.

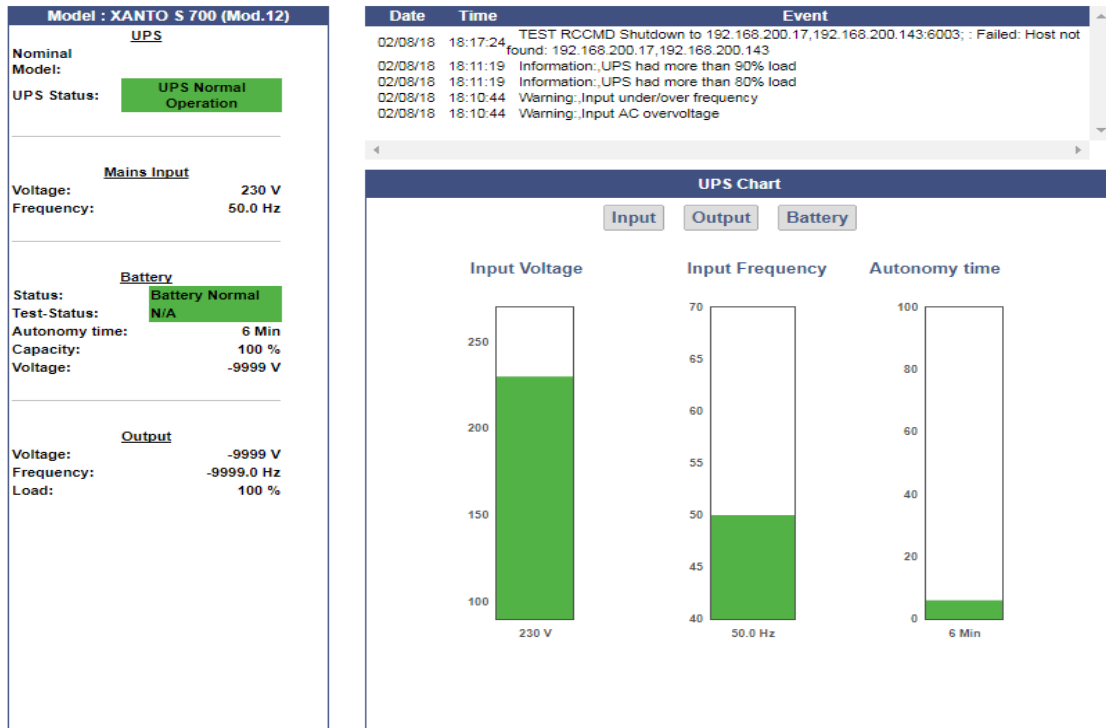
Note

Please note that just connecting the UPS is not enough: As long as you have selected the dummy, the LED will flash green even if no UPS model has been set up – By activating COM 1 without further configuration, the CS141 will select a placeholder to ensure all menus are available.

UPS-Monitor: Checking UPS Settings








 UPS Monitor	➔ Realtime UPS monitoring screen
 Sensor Monitor	➔ Realtime sensor monitoring screen

In case of all settings have been entered correctly, administrators can check the UPS's current status in real time by using the UPS monitor. Although the representation may differ depending on the manufacturer and model, some data such as the selected model will be shown:



UPS functions

For this configuration step, navigate to the following menu:

 Devices	➔ System Tab: Devices
 Setup	
 UPS	➔ System Tab: UPS Menu
 Setup	
 Events	
 Functions	➔ Advanced UPS functions
 Custom Thresholds	

The UPS Functions menu contains options to perform tests sequences or to configure build-in special functions a UPS may provide. They are tailored to the UPS model used to represent its functionality. As a consequence, the functions displayed for this menu item can vary - some UPSs only allow the on / off state as well as a single test-button, others provide more functionality.

The following functions represent typical menu entries:

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 a custom defined runtime
- ➔ Standard battery test
- ➔ Full test until batteries are depleted
- ➔ Starts a self-test of the UPS
- ➔ If possible, abort a triggered test

Custom Test

The Custom Test is an on-battery function test using a self-defined time in minutes.

Battery Test

The battery test checks whether the UPS works properly and the batteries take over. This test usually takes about 15 seconds. This test will not show how long the batteries will be able to take over.

Full Test

The Full Test will test the batteries until they are depleted. This test can take a long time depending on power and load. The CS141 also accurately measures and determines the runtime under load. Please note UPS systems require stable load of at least 25% to perform a full test.

Self test

With this test, the UPS checks its own electrical functionality

Note:

In some cases, a UPS command may seem to fail or an error message may appear. This behaviour is based on the fact a UPS receives and confirms a command, but without doing it until pre-conditions are fulfilled. As an example, there must be a minimum charge for a particular battery test - otherwise the UPS returns an error message as a result. This result will be logged accordingly as "error". In reverse cases, it is possible the UPS sends a positive feedback despite errors but indicates an error on the front display itself.

Due to these facts in sometimes the behaviour of a UPS system is unique and for some cases unfortunately not predictable.

UPS Control settings

Depending on design and model, some UPS systems support additional functions to be used for verifying the performance of the UPS. The scope of functionality and configuration possibilities varies considerably and depends on both the manufacturer as well as the model to be used.

Typical functions a UPS may provide:

The screenshot shows a 'UPS Control' panel with the following elements:

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

Switchable output

Depending on the design, some UPS systems support switchable output ports.

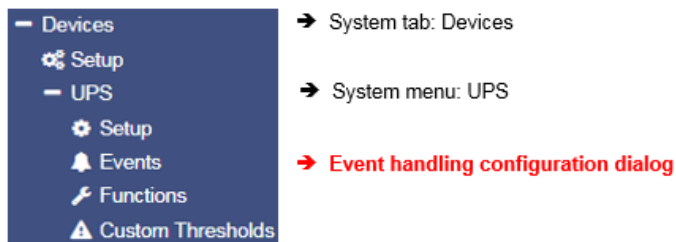
The screenshot shows a 'Toggle the outlets' panel with two green buttons labeled '1' and '2'.

Note:

Depending on the performance class, UPS systems are equipped differently. Due to this fact, the scope of functions varies.

Event handling

For this configuration step, navigate to the following menu:



There are many incidents that may require the operation of a UPS. In other cases, devices connected to the UPS may be harmed by different events.

These events could be as an example

- the failure of the main power supply,
- the restoration of the main power supply,
- a defect from inside the UPS prevents taking over to autonomous battery mode
- batteries are depleted and main power is still missing

As a full-fledged manager, the CS141 has the ability to respond to incidents independently, inform responsible personal and even manage event chains to provide a complete shutdown solution inside complex interdependent networks.

Defining jobs for an event

System events are highly dependent on the UPS model to be used and vary in both - designation as well as abundance of possibilities. Furthermore, administrators will find interesting conceptual issues according to the interplay of events and counter-events:

An event receives an action, a job. This job will be executed when the event occurs. These jobs differ in central role as well as its direct function:

- *Information*

These jobs can be executed as often as desired and only fulfil the purpose of the information. Depending on the configuration, information can be sent once or cyclically as long as an event is pending - the nature of the event does not matter. If the situation changes and the event does not come to fruition, an according job will not continue.

- *Action*

These jobs are designed to switch, trigger, start emergency routines, etc. These jobs are triggered as soon as an event occurs. They differ from information jobs due to the fact administrators have to terminate these jobs by using corresponding counter-rotating jobs. In some cases, there are counter-events to be used, others need to be configured manually.

Note:*It is important to understand the difference*

As long as a power failure occurs, a mail with log files appendixes to should be sent every 5 minutes. Once the power failure is eliminated, no more email is written. On the other hand, a job to close potential-free contact as soon as a power failure is detected is executed. This cannot be reverted - even if the main power comes back, the contact remains in closed position. If a warning light is switched via this contact, it would light up until this contact is deliberately opened. A counter-job is needed in case of main power returns.

The following example shows why it is important to understand the difference:

If the temperature sensor measures critical temperatures, the CS141 will send e-mails and simultaneously close the contact of an air conditioner. As soon as the temperature drops below the critical level, CS141 stops sending e-mails - but the air conditioner needs to run until the temperature has returned to normal condition. This will not work if the contact automatically opens in case of critical temperature is no longer given:

You need to use an active job to switch off the air conditioning system as soon as a certain temperature has been reached.

It becomes problematic if a power failure causes two UPS systems running on separated power input circuits to send a server shutdown command:

As soon as both systems send a valid shutdown command, the server shuts down immediately - even if both UPS systems report a power failure time-separated. If they do not cancel the shutdown command after their respective individual problems were resolved, the server will shut down due the fact, both UPS systems seems to report problems.

Event handling: Defining a job

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

1. e-mail - based jobs require a valid mail account to send a mail.
2. jobs based on TCP/IP settings require a valid network configuration.

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

Managing jobs

Under Devices, open the UPS submenu and go to Events.

Please note that both the functions as well as designation will differ by usage of different UPS systems.

These are the icons the CS141 provides:



→ Open /close tables



→ Edit an existing job



→ Test an existing job

Symbols providing two functions:



→ delete



→ Checkbox to select multiple jobs or events



→ Add a job

Note:

Dual function symbols have two different meanings:

Depending on where you serve them, they refer to ALL events or to a specific event or job. This dual functionality allows you to add a specific event to specific or all system events without the need of entering each job individually.

Setting up a job

Managing jobs for a system event always follows the same rules - as an example, the following system events are selected:

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

Select > to open the job table:

-	<input type="checkbox"/>	+		Powerfail	3	1	0	1	0	0
				Job Type	When	Parameter				
				Log	Periodic all 100s, immediately	{ "text": "Powerfail" }				
				RCCMD Trap	Once, immediately	{ "text": "Powerfail on #MODEL . Autonomietime #AUTONOMTIME min." }				
				Email Trap	Once, immediately	{ }				

For the event Power failure, a total of 3 jobs are already configured. These jobs were loaded as a recommended default configuration when selecting a UPS. To change or remove, just click on the corresponding icon..

The CS141 allows to delete all jobs within a system event:

By doing so, activate the checkbox in the line for power failure and press the symbol for deleting events. After pressing all jobs associated with this one event will be deleted from the list.



Note:

Deleted jobs can not be retrieved, they must be recreated or restored by using a backup. To prevent accidental deletion, administrators will be prompted to confirm their decision to delete all entries inside an event...

To add a job to the power failure event, press + at the event line. This will trigger the configuration dialog who will guide you through configuration process.

The following jobs are currently available:

Log	Inserts a free definable message into the event log.
Email*	CS141 will send an email.
Email Trap*	CS141 will send Trap Mails
RCCMD Shutdown*	CS141 will transmit a shutdown signal to one or more RCCMD clients.
RCCMD Message*	CS141 will send an RCCMD message to one or more RCCMD clients.
RCCMD Execute*	CS141 will send a command to execute a custom file.
UPS Shutdown***	Turn off UPS
AUX**	CS141 will trigger external relays.
Buzzer**	If a buzzer is connected, CS141 can activate it by using this job.
RCCMD Trap*	CS141 will send an RCCMD trap message.
Send WOL	Wake On LAN - The CS141 will send so-called magic packet to a network device.
Send SMS**	If a GSM modem is connected, CS141 will be able to send SMS.
AUX: Switch Outlets***	As an example, the UPS can be instructed to disconnect the live outlets after a full discharge of the batteries and run a time-delayed release to guarantee a minimum charge of the batteries..
WAKEUP	If two UPS are running in redundancy mode, this custom RCCMD command can be used to withdraw an RCCMD shutdown command

* Additional software may be necessary.

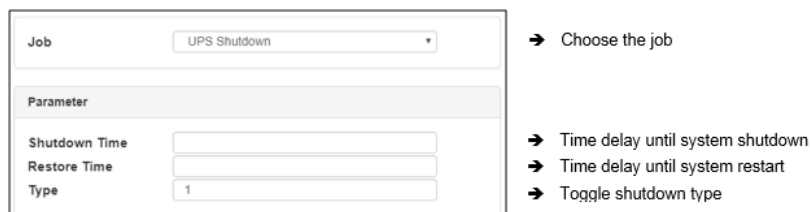
** This feature may require additional equipment and accessories.

*** This function is only available to a limited extent: although some UPS systems fundamentally support the functionality, they respond very differently to this job:

Some UPS systems accept and confirm this job, but ultimately decide themselves about execution and timing.

UPS Shutdown definitionWhy is the job UPS shutdown a little bit tricky?

A UPS performs a UPS shutdown to protect the batteries from a deep discharge. The UPS is physically shut down and turned off. The time when a UPS performs this action or how it reacts to a triggered action by scheduler or via UPS functions already varies even between the models within a manufacturer - in addition, each manufacturer uses its own definitions for to protect batteries. But due to the fact the UPS has been physically turned off, counter events cannot be configured.

Configuring UPS Shutdown

Shutdown time in seconds

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

Restore time in seconds

When the main power supply is restored, the UPS waits for the pre-set value in seconds until it starts up again.

Type

With this setting the UPS will be turned off or turn on. Two different settings are possible:

- 1 The UPS switches off the outputs but remains in operation mode.
- 2 The UPS shuts down and turns off completely until the main power is restored.

How to use the job UPS Shutdown

This job cannot map both settings together.

Depending on the desired operation modes, at least two jobs are required.

As an example, it is possible to use different jobs to complete the following sequence:

- Switch off outputs after 3 minutes
- Shutdown the UPS after 4 minutes
- Turn on the UPS 2 minutes after the main power supply is restored
- Activate the outputs 15 minutes later

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

Search and display jobs

Event	Jobs	Log	Email	Email Trap	RCCMD Shutdown	RCCMD Message	RCCMD
contains...							

The Search function is a quick method to find jobs configured within events.
The CS141 provides two basic options:

Event contains...

Search for a UPS event. By typing a part of an event all events according to the text fragment are listed.

Jobs

Lists events containing a number of jobs defined by this value. As an example, if you want to know how many events contain 3 jobs, enter 3. All events containing this number of jobs will be listed.

Configuring a Job

Press **+** at an event to open the job configuration dialog.

Job

Log

Different jobs provide different parameters to be configured

Example 1: Log – Enter the text CS141 shows at Event Log?

Parameter	
Text	

Example 2: RCCMD execute – Due to the fact RCCMD needs IP adress data, the parameters will change.

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

Timing

The CS141 provides many system events a job can be assigned to. Some jobs allow to configure advanced timing:

The image shows a 'Timing' configuration window with five radio button options, each followed by a text label and a text input field. The first option, 'Immediately, once', has its radio button selected. The other options are 'After [] seconds', 'After [] seconds, repeat all [] seconds', 'After [] seconds on Battery', and 'At [] seconds remaining time'.

Immediately, once	As soon as an event happens, this job is executed at once and not repeated.
After XXX seconds:	The CS141 will wait a pre-defined time in seconds and then execute the job. If the event is no longer active before time is up, the job will not be executed.
Repeat all XXX seconds:	The job is repeated cyclically until the event is no longer active.
After XXX seconds on battery:	The event forces the UPS to switch to autonomous mode. The job will be executed if the UPS remains a pre-defined time in this state. For example, if 300 seconds are set, this job will only be executed if the UPS operates in autonomous reaches 300 seconds.
At XXX seconds remaining time:	The job is executed when the remaining UPS operating time is reached or undershot. Note based on the current load this time value becomes flexible.

Time management of jobs

The time management of jobs to be performed is difficult since one has to distinguish conceptually between two different points of view. The following example according to the event power failure illustrates the differences:

In case of a power outage, the UPS will take over power and protect the servers until ...

1. The batteries are depleted
2. Main power is available again

As soon as the UPS runs into autonomous mode, it will start two different timers:

A linearly advancing time in seconds starting at 0.

If a job is to be executed after 45 seconds, it will only be executed if the event is pending for at least 45 seconds. If the event is terminated before consequently the job is not executed..

A relative clock that counts backwards depending on the connected load currently used.

This becomes tricky if the UPS will operate with a load of 100%

If some of the machines connected to the UPS will be shut down after 3 minutes and cause the load to drop to 50%, it will take effect this way: Because of dropping load, the clock would jump from 4 minutes to 7.5 minutes.

Both methods to count come with specific advantages and disadvantages:

The first counter gives a clear time window to sequent jobs but ignores the actual remaining time of the UPS:

If there are several small power failures in a row, a server shutdown would not work with a time delay of 5 minutes if battery power is left to ensure power a maximum of 4 minutes.

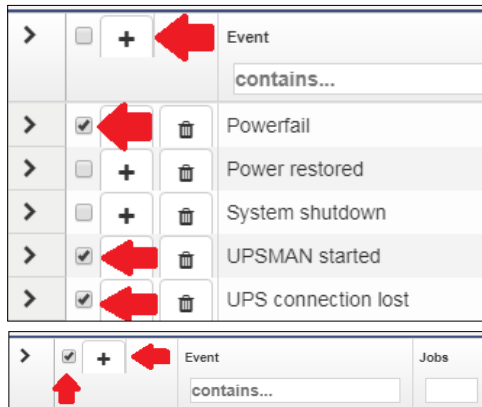
The second counter is difficult to calculate and varies depending to the current load. As a consequence there may be a time lag to execute configured tasks: 5 minutes remaining time cannot be achieved over a longer period of time, if the circumstances increase the remaining time - for example some systems will be shut down at 7 minutes remaining time. On the other hand, a predetermined Sequence of events can get mixed up as soon as the circumstances correct UPS uptime down and cause normally sequentially configured jobs simultaneously getting triggered.

Note:

Basically a shutdown using remaining time is useful, since the actually existing battery charge can be included. If a special order must be observed for jobs, it makes sense to use the linearly forwarding clock for scheduling.

Adding jobs to several events

Under circumstances, a configuration require multiple events be assigned the same job. To assign these jobs to more than one event, it is possible to select each event individually and to define this job.



To speed up the process select the events that should receive the same job. Then click on the upper **+**.

By doing so, the same job is created inside the selected events. In diesem Fall wird der selbe Job bei jedem angewählten Ereignis angelegt.

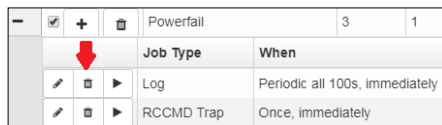
Activating the checkbox at the top row will advise the CS141 to add a job is to all events. To start the job configuration dialog, click **+**.

Deleting a jobs

If system events are no longer used inside a configuration, administrators should remove these jobs to prevent unexpected incidents.:

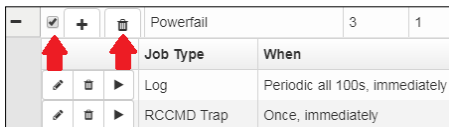
- Delete a job

Open event tab by clicking **>**



Choose the job you want to do delete and press the small trash icon. The job will be deleted immediately..

- Delete all jobs within an event



To delete all jobs inside an event, choose the checkbox of the desired event tab. Than press the small trash icon. By doing so, all jobs listed inside this event will be deleted immediately. accidentally deleted jobs need to be configured again.

Note:

The CS141 allows to add, edit and delete any job. The event list itself is hard-coded and depends to the UPS you are using. Events cannot be deleted or edited by any user.

Assigning jobs to conter events

Some jobs must be explicitly withdrawn when an adverse event occurs:

- Information of responsible persons / "all-clears"
- Further actions
- Advised server shut downs
- ...

The configuration of a counter job follows the same pattern as the creation of a job. According to this context, for some jobs time management becomes a significant role:

Since the UPS comes back from autonomous mode to normal mode, it will take amount of time to recharge the batteries in order to run all jobs as configured.

Example scenario:

Due to a power failure the UPS has switched to autonomous mode and will hold all connected devices for 60 minutes at 100% load.

With 30 minutes remaining, many computers automatically shut down, reducing the load to 20%.

The remaining time will be corrected upwards accordingly.

Since all systems are shut down only after 5 minutes of remaining time, but the power failure at 6 minutes has been eliminated, normality returns.

In this case, the CS141 can restart all computers shut down to protect the remaining time via Wake on LAN (WOL) - this absolutely useful for automated restart of networks after power failure.

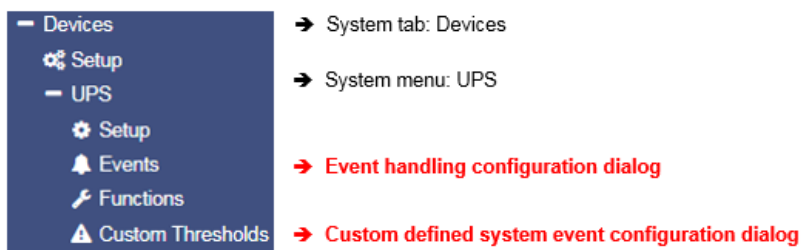
In this scenario, if all connected computers were to be restarted automatically, this means that the UPS could withstand 20% load for 6 minutes at the next power failure - but 100% load must be delivered. Since this cannot work, the WOL packet must be delayed in time to give the UPS the ability to charge a minimum of batteries.

Note:

It is possible to create up to 50 jobs per event. In some cases, individual jobs may contradict each other or undo desired jobs accidentally by using counter jobs.

Custom Thresholds

For this configuration step, proceed to the following two menus:



In some cases, UPS models allow you to customize the limits for some UPS-specific events.

The CS141 supports these features if the UPS provides such an option. Otherwise, you will be informed by a corresponding system message.

The configuration is done via two menus:

- *Custom Thresholds* to define and customize settings
- *event menu* to assign jobs

Differences between Warning and Alarm Levels

The Custom Thresholds are identical for Warning and Alarm Levels - but they are listed separately in the UPS event menu. Furthermore, they will be listed inside log files as a Warning or Alarm.

This will allow to configure warning and alarm behaviour containing different values.

These conditions can be set up:

- out of range** the event – regardless of alarm or warning - is triggered if the measured value falls below or exceeds entered values.
- less than** the event - regardless of alarm or warning - is triggered if the measured value falls below configured values.
- greater than** the event - regardless of alarm or warning - is triggered if measured value exceeds configured values.

Example: How to configure UPS temperature Custom Thresholds

Electrical devices operate safely between a minimum and a maximum temperature grade. Running a device exceeding these conditions may cause issues. These issues may vary starting from simple defects up to acute fire hazards.

In order to be able to intervene in time, therefore, a predetermined temperature value must be compared with the measured temperatures.

As an example, the manufacturer of a device specifies the "safe operating temperature" between + 5 ° C and + 39 ° C:

The CS141 can configured to warn if these values will be exceeded - the condition out of range first defines the safe temperature range.

As mentioned, two menus are required to configure Custom Thresholds:

- Custom Thresholds:

The first setting is made under Custom Thresholds where the appropriate values are set.

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

Enabling the checkbox UPS Temperature will include measuring values according to the UPS. For the argument out of range you need to specify both - the lowest temperature value and the highest temperature value.

Note:

Since this is the warning, it should be sent before reaching critical values.

Due to the fact the minimum of + 5 ° C and a maximum of + 39 ° C is predefined by manufacturer, the values for warning levels must be corrected accordingly. In this example the decision is made to use 5°C:

Min: 10°C
Max: 34°C

Save your entries and move to the next menu:

- USP events

Search for temperature threshold entries to be found at UPS events. Unlike the Custom Thresholds menu, each Threshold is displayed as regular system events and shows all possible 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 Custom Thresholds can be configured like regular UPS events, all jobs are available. If necessary, counter jobs can be defined according to temperature.

Setting up Alarm Levels

The alarm levels represent an escalation level and, if necessary, should trigger emergency measures, the values must be adjusted accordingly to warning levels.

>	<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

Please note, since the condition for an alarm is fulfilled in addition to existing warning levels, configured jobs can be executed in parallel, overlap or even contradict or cancel each other out.

Exemplary excerpt: Custom Thresholds

This excerpt is an example. Depending on UPS model and manufacturer, this list will vary in naming as well as functionality differs. The sample list shown below shows the custom threshold list of a XANTO 2000R from the manufacturer Online:

		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"/> Battery Symmetry Pos./Neg.	greater than	0	V		
<input type="checkbox"/> Seconds on Battery	greater than	0	s		

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

Batteries are sensitive to voltages, high voltages and deep discharges can permanently damage them. This value can be used to warn in good time as the entered range is left.

Input voltage P-N *out of range* XX V – XX V

on request some UPS systems offer on measurement data of the input voltage. This value can be used to implement an alarm response to voltage dips or overvoltage on main power input

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

Some UPS systems provide internal temperature sensors to measure device temperature values. This value can be used to define an additional alarm behaviour based on the temperature values that the UPS supplies.

UPS Autonomy *less than* XX m

in some cases, it may be useful to define additional alarm behaviour about the remaining time a UPS ensure emergency power in autonomous mode - as an example if defined jobs depend on a configured time delay and due to several short power outages in a row Time is available: An emergency behaviour scenario could be an alarm shutdown of systems.

Battery Charge *less than* XX %

If a UPS comes back from autonomous operation to normal mode, it will automatically start to recharge the batteries. This may last some time. In case of several short power failures in sequence, an additional early warning behaviour can be defined using this value.

Output Load *less than* XX %

Some UPS systems provide real-time measurements of the current load. In case of the UPS switches to autonomy mode, normally non-vital systems will be shut down as soon as possible. Due to the fact the output load differs if systems will be shut down, this value can be useful for confirmation or advisory behaviour.

Battery Symmetry Pos./Neg. *greater than*

Some UPS systems use the positive and the negative half wave of AC to charge batteries. This setting defines the alarm behaviour if the positive battery string and the negative battery string are not loaded evenly.

Seconds on Battery *greater than* XX s

in some cases, a voltage drop is recorded, for example in case of large industrial plants are put into operation. In some cases, it may happen that a UPS switches to autonomous mode for one or several seconds. With this value an additional warning could be realized to verify a "genuine autonomy case".

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 a condition, the warning and alarm behaviour will be done according to the configuration:

As an example, if the output load warning is less than 67%, it will also issue a warning if it drops to 43%. On the other hand, 67% will not warn due to the fact the value has to be below 67%

Tutorial: Custom Thresholds

Problem description

Although the CS141 recognizes the UPS correctly, contactors are to be activated via potential-free contacts. This shall switch off external devices as soon as the charge of the batteries drops below a configured value.

This configuration can be realized indirectly:

If a CON_R_AUX4 is connected to CS141, the potential-free outputs can be used to control the contactors - it is possible to switch through (ON) and block (OFF). This will allow to implement the control of the contactors without tricky issues.

It will be difficult if the UPS does not offer suitable events:

As a consequence, these events are not displayed inside the UPS event menu. Using Custom Thresholds will allow this configuration:

The key to this configuration is the fact this function depicts a user definable job as a UPS event:

Setting 71% for Warning Levels and 61% for Alarm Levels, you can subsequently assign appropriate behaviour in the UPS events:

- if the battery charge drops to 70%, the first devices are switched off.
- If the battery charge drops to 60%, the next devices are turned off. The counter events are set to Warning OFF or Alarm Off.

As the batteries are charging, the devices should start after battery charge reaches similar values for shutdown.

- From 61% the first device list will be switched on
- From 71% the second device list will be switched on.

Since there is no AND connection to the Power Fail, there are basically two possibilities to run these jobs:

1. Once
2. Repeat as long as the event is active

Note you have a difference of 1% between ON and OFF. Due to the fact the value needs to drop below the values, it is technically not possible to switch exactly ON and OFF at 70% or 60%. A decision is needed whether you wish to switch ON the devices at 60/70% or off

You need to define your jobs exactly:

Turning off the same devices 70% and to on position at 61% could cause conflicts between events and jobs, devices should therefore be consistently configured separately

What will happen between 0% – 71%

Depending on the configuration, independent to any power fail the devices will stay off, shutdown or restart between 0% and 71% battery charge. Above 71% the devices will run as long as no power fail will cause the battery charge to drop at 70%. Since the current load has no influence on the percentage of battery load, the flexible remaining time does not affect this setting. The percentages of the current battery charge are basically used.

Note:

A detailed description of the CON_R_AUX4 can be found at chapter *Sensors*

The screenshot displays two configuration panels: 'Warning Levels' and 'Alarm Levels'. Both panels have a list of parameters on the left and their corresponding Min and Max values on the right. In both panels, the 'Battery Charge' parameter is checked and highlighted with a red box, showing a 'less than' condition with a value of 0%. Other parameters include Battery Voltage, Input voltage P-N, UPS Temperature, UPS Autonomy, Output Load, Battery Symmetry, and Seconds on Battery, each with its own set of Min/Max values and units.

RCCMD

Ever heard something about RCCMD?

RCCMD (Remote Console Command) is the world's most successful shutdown solution for heterogeneous networks and is the best method to ensure initiating multiple messages and shutdown sequences. The solution integrates even the UPS to set up an all-in-one monitoring and messaging solution:

The RCCMD clients listen on port 6003 for incoming messages of RCCMD server module. This module is a general part of

- UPSMAN software
- CS121
- CS141
- RCCMD licensed UPS manager.

An RCCMD server controls the RCCMD clients inside networks. The functional scope ranges from monitoring, notifications up to a structured shutdown of a multiple server environment. RCCMD even considers mutual dependencies.

Note:

The RCCMD client is not freeware

A separate license is available and can be obtained worldwide from licensed resellers, OEM partners or directly ordered at www.generex.de.

The license itself is unlimited valid, the service scope includes 2 years of free updates from the date of purchase.

Available RCCMD commands for the CS141

As mentioned, CS141 provides an RCCMD server.

The RCCMD commands are defined as jobs via the system events. There are four different categories available:

→ RCCMD Shutdown

The RCCMD shutdown sends a signal to an RCCMD client. The RCCMD client advises the server to initiate the shutdown sequence.

→ RCCMD Message

An RCCMD message is a notification text that can be sent to an RCCMD receiver. This text will be displayed on the screen using a separate message box.

→ RCCMD Execute

If scripts have to be executed in advance for a shutdown, they can be triggered by using the execute command. RCCMD offers not only ready-made commands but also the possibility to start own scripts.

→ RCCMD Trap

Trap messages are pure informational messages that can be sent to RCCMD clients. The client receives these text messages and displays them inside a pop-up message box.

Note:

An initiated RCCMD shutdown cannot be withdrawn. However, within the RCCMD client, you can also define so-called redundancies and limit IP addresses that are authorized to send an RCCMD signals. By doing so, as an example, two UPSs need to advise a server shutdown. In this case the RCCMD execute *wakeup* will withdraw a server shutdown command.

Configure an RCCMD-Job

RCCMD uses IP addressing to communicate within a network as well as a single network segment.

the following parameters can be adjusted:

Set up IP address for RCCMDBroadcast messages

Activating this checkbox will trigger an RCCMD broadcast job will be sent. Each RCCMD client installed in this network segment is addressed and responds by shutting down and turning off the computer. There is no distinction between host, virtual machine, single server or workstation.

Limiting IP addressing

A broadcast message is not always the best method for shutting down networks...

To address a particular machine within your network, enter the IP address of the device. In fact, only addressed computer - physically or virtual devices - will receive the RCCMD message.

The CS141 provides both:

creating a single job for each RCCMD client as well as combining several IP addresses to create a device group job.

... One job, one IP address ...

... several IP-addresses to configure a group job.

For several IP addresses, please ensure the correct syntax:

192.168.3.1,192.168.3.18, ...

The IP addresses will be written without space between the individual entries. Otherwise, you will receive a corresponding error message.

Note:
Broadcast messages and individual IP addressed or collective addressed messages are mutually exclusive: You can configure the RCCMD client to accept commands by single IP addresses. But the client cannot be configured to differ between a broadcast message and a single message. If you want to shut down devices and device groups first and then send a broadcast, you need to create several jobs with a corresponding time delay.

Port selection

As a default port, RCCMD uses port 6003. The RCCMD client is listening on this port for a valid RCCMD command.

If your RCCMD client has been assigned a different port during installation and configuration, ensure sender and receiver are using the same ports.

Parameter

IP

☐ Broadcast

192.168.3.1

Port

6003

RCCMD Job Timing

The CS141 provides many system events a job can be assigned to. Some jobs allow to configure advanced timing:

Timing

☒ Immediately, once

☐ After seconds

☐ After seconds, repeat all seconds

☐ After seconds on Battery

☐ At seconds remaining time

- Immediately, once

As soon as an event happens, this job is executed at once and not repeated.
- After XXX seconds:

The CS141 will wait a pre-defined time in seconds and than exucte the jobIf the event is no longer active before time is up, the job will not be executed.
- Repeat all XXX seconds:

The job is repeated cyclically until the event no longer is no longer active.
- After XXX seconds on battery:

The event forces the UPS will to switch to autonomous mode.The job will be executed if the UPS remains a pre-defined time in this state. For example, if 300 seconds are set, this job will only be executed if the UPS operates in autonomous reaches 300 seconds.
- At XXX seconds remaining time:

The job is executed when the remaining UPS operating time is reached or undershot. Note based on the current load this time value becomes flexible

RCCMD command

Der RCCMD Shutdown

Parameter

IP

☐ Broadcast

192.168.3.1

Port

6003

The RCCMD shutdown is predefined and advices the addressed RCCMD client to shut down the operating system and turn off the device. Adjustable options include broadcast, sending to individual IP addresses and the port used for RCCMD.

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 can be defined freely. The text box automatically shifts with the entered text as soon as you reach the right margin. This message will then appear as an alert on a computer the RCCMD client is installed to. RCCMD also displays a warning box on the taskbar.

RCCMD Executes

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

An extensive feature within RCCMD is the possibility to run own executables and batch files on a target computer.

This function is useful if scripts have to be executed right before a shutdown is triggered. It is necessary to move the file to be executed to the installation directory of the RCCMD client. Afterwards, the CS141 provides to execute this script directly.

Note:

The screenshot shows the command helloworld.bat has been entered. In this case, the RCCMD client on the PC with the IP address 192.168.3.1 would try to start the file helloworld.bat directly. If you want to use other directories, you need to specify them accordingly:

C:\skript\helloworld.bat

Please note, it is tricky to run a script on a PC that shall trigger scripts on a third device.

RCCMD Traps

RCCMD traps are data packets designed to inform about the current state of the UPS:

A data package is generated, which can be received, read out and interpreted by a corresponding software or device.

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

#AGENTSOFTREV	CS141 firmware version
#AUTONOMTIME	autonomy time in minutes
#BATT2OLD()	Time in months until the event "Please check batteries"
#BATT2OLD_YEARS	Battery age in years
#BATTCAP	battery capacity in%
#BATTINSTDATE	Installation date of the battery
#BATTTESTDATE	Date from the last battery test
#BATTVOLT	battery voltage in V
#CHARGECURR	charging current
#CNT_BL	Counter Battery Low
#CNT_PF	Counter Power fail
#CNT_SA	Counter Active Shutdowns
#CNT_SD	Counter Shutdowns
#CNT_TF	Counter test failure
#DATE	current date
#EVENTSTATE	status (idle, error, progress, success)
#FULLTESTDATE	date of the last full test
#GETLASTRESULT()	Results from the last test performed
#HOLDTIME	UPS hold time at 100 percent load
#IDENT_NAME	name of the SNMP webmanager
#INCURR0/1/2	Input current in A
#INFREQ0/1/2	Input frequency in Hz
#INPHASES	Number of input phases
#INPUTCURRENT0/1/2	Continuously measured current in A

#INVOLT0/1/2	input voltage in V
#LASTERR	last error occurred
#LOAD	current load
#LOCATION	location description of the device
#MANUFACTURER	manufacturer of the UPS the device is installed to
#MODEL	UPS model
#OUTFREQ0/1/2	output frequency in Hz
#OUTPHASES	Number of output phases
#OUTPOWER0/1/2	Load in %
#OUTPUT_VOLT0/1/2	output volt in V
#OUTPUTCURRENT0/1/2	current output in A
#OVERLOAD	Overload
#PHASES	phases
#POWER	UPS Power
#RECHARGETIME	Time to fulfil recharge cycle
#RESTORETIME	Time to restore UPS after usage
#RUNTIME	Runtime since last start-up
#SECONBAT()	Seconds on battery
#SELFTESTDATE	Date of the last self-test
#SERVER	IP address of the SNMP adapter
#STATUS	System status
#SYSDATE()	System date
#SYSTIME()	System time
#TEMPDEG	Temperature in °Celsius
#TIMEZONE	Time zone
#VOLTAVAI	UPS related - The UPS provides input voltage queries

Sensors and devices

SITEMONITOR 6 specific information

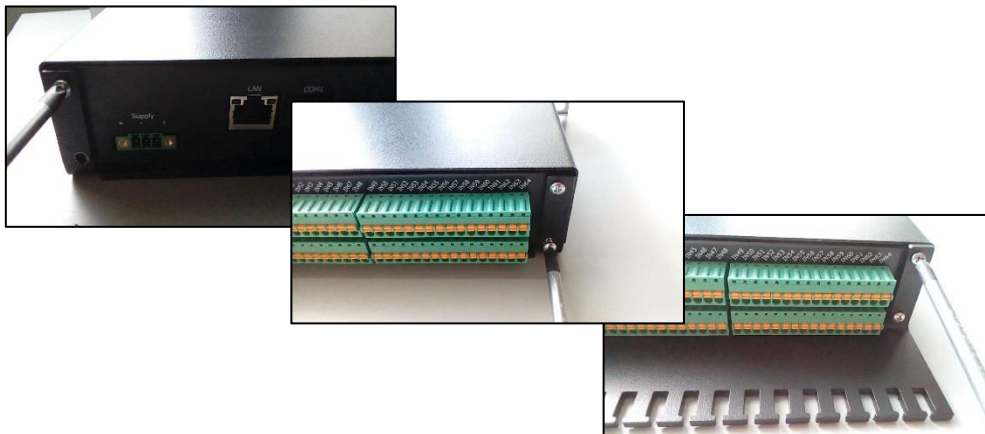
SITEMONITOR 6

The SITEMONITOR has 64 digital inputs and, via 2 special AUX ports, offers the possibility of connecting a relay board specially developed for the SITEMONITOR for up to 8 outputs in addition to analogue sensors. In total, the SITEMONITOR provides 12 volts of operating voltage for external sensors if required and 1 ampere of current distributed over the entire number of connected devices. Both active and passive devices can be connected.

The cable tree

With 64 digital inputs, installations with up to 100 cables are a realistic scenario. For this reason, the SITEMONITOR 6 offers the option of an optional cable comb:

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



Remove the screws and bring the strain relief into position. Then fasten the strain relief again with the screws. To avoid damage to the unit, please use only the screws provided for this purpose.

Removing the terminal strips

Take a suitable tool and detach the green terminal strip from the base. Afterwards, the strip can simply be removed from the back of the unit. The green terminal strips are pre-coded, so inadvertently inserting them incorrectly is basically impossible.

You can either use the plug-in contacts or the terminal strip for your installation.

Connecting devices

Please note that the upper and lower row of connections are assigned differently:

The upper connections are marked IN 1 - IN 64 and are the digital inputs. The lower row is marked + and - and are optionally the reference point as well as an internal power source should external sensors require an operating voltage.

The connections are assigned as follows:

IN 1 is opposite the positive pole on the other side.
IN 2 is opposite the negative pole on the other side.
[...]
IN 54 sits on the other side opposite a negative pole
IN 55 is opposite a positive pole on the other side.



When connecting contacts or devices, please note:

- A relay with its own power supply is placed from the negative pole to the digital input.

Which negative pole you ultimately use for the connection is irrelevant- only the digital input must be able to detect an open or closed contact. The digital input just needs a negative pole to be connected to and will be configured within the configuration interface.

- A sensor or switching unit with power supply with an operating voltage of up to 12:

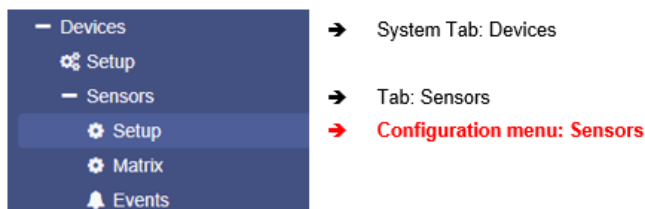
In this case, you can tap the required power supply from the lower bar from the plus and minus poles via plugs or terminals. The digital output of the sensor or the switching unit is then connected to the corresponding digital input on the SITEMONITOR.

Note:

The upper connection bar offers 64 digital inputs that can be freely assigned. The lower bar offers 32 plus and 32 minus poles, which can deliver a total power of 12 V / 1A. When counting, the odd designation of the digital input is always opposite the positive pole and the even designation of the digital input is opposite the negative pole.

Configuration: Specific devices for the SITEMONITOR 6

For this configuration step, open the following menu:



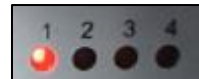
How to name the contacts

To change the name of the inputs, open the Sensor Configuration menu and enter a new name:

Input	Name	NC Contact	Active
1	Emergency Power Route active	<input type="checkbox"/>	<input type="checkbox"/>
2	Warp Drive Offline	<input type="checkbox"/>	<input type="checkbox"/>
3	Air Condition Online	<input type="checkbox"/>	<input type="checkbox"/>
4	Doors Locked	<input type="checkbox"/>	<input type="checkbox"/>

Port

The port number is fixed and is used to uniquely identify the port both in the sensor monitor and on the front of the unit. Triggered contacts can thus be quickly assigned to a unique port. can be quickly assigned.

Name

This field is freely definable and allows a more detailed description of the connected system:

Port	Name	NC-Kontakt	Aktiv	Hold
1	Türkontrolle Eingang	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	Klimakontrolle	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	Pumpensystem	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

After adapting the name to fit to the according system, press Apply to save the settings. You will then find the exact name in the sensor monitor:

01 02 03 04	09 10 11 12	17 18 19 20	25 26 27 28
05 06 07 08	13 14 15 16	21 22 23 24	29 30 31 32
<div> <div>1</div> <div>Türkontrolle Eingang</div> </div> <div> <div>2</div> <div>Klimakontrolle</div> </div> <div> <div>3</div> <div>Pumpensystem</div> </div>			

NC-Contact

This function defines whether the contact should normally be closed or open. Depending on the configuration, there are automatic normally closed or normally open contacts, which means that an adjustment must be made in the SITEMONITOR so that the alarm behaviour is synchronized with the actual function of the connected system:

For example, while a door access control normally has a closed contact, a switch coupled to an emergency shutdown device may open automatically because the system has been switched off.

Possible functionality

1. NC contact control hook not set:

The contact must be closed during normal operation. If the contact is opened, an alarm is triggered.

2. NC contact control hook is marked:

The contact is open in normal operation and closes automatically should the condition for this be fulfilled. In this case, the alarm is triggered because the contact has been closed.

Active

Defines whether a connected contact is to be checked. The SITEMONITOR will only check the contacts on mark.

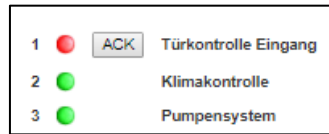
Hold

Defines the type of alarm. Normally, an alarm is triggered on actuation and as soon as the control state has been restored:

For example, if a door access control is checked, an alarm is normally triggered because the NC contact was also opened by opening the door. If the door is closed, this normally also closes the NC contact. In the alarm behaviour, you would accordingly only be able to see the alarm as long as the contact was triggered.

Hold is a game changer for this behaviour:

When the door contact is opened, the alarm is triggered:

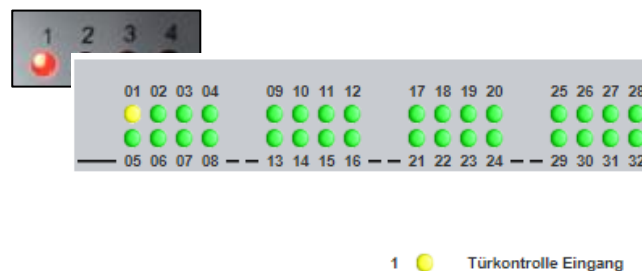


In addition, the corresponding LED on the front of the unit flashes slowly in red. Due to the hold function, however, this alarm remains even if the door contact has been closed again in the meantime - it must be confirmed manually with ACK - button in the sensor monitor.

With the confirmation, the current status is checked and one of the following options is displayed

1. The event is still present:

In that case, the system will respond by changing the control LED on the front of the unit from a flashing red (unconfirmed alarm) to a static red glow (confirmed alarm). In addition, the corresponding alarm marker in the sensor monitor will change to the colour yellow.



After the cause has been eliminated, the SITEMONITOR will automatically return to its normal operating state:

- The front LED will be switched off
- The alarm marker will fall back to green.
- Jobs that are configured to the fallback behaviour will be executed.

2. The event is no longer present.

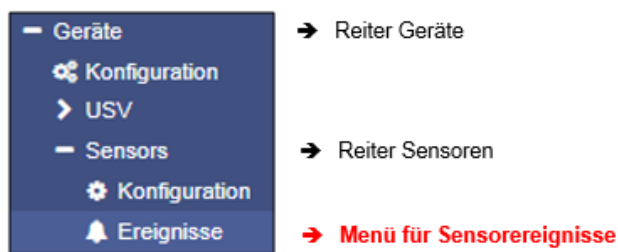
The LED on the front of the SITEMONITOR will be switched off and the yellow marker will fall back to green. They will return executed jobs that are configured to the fall back and switch back to normal system state.

Note

If you have not activated the hold function and acknowledge a current alarm with ACK, this alarm behaviour is also triggered to hold the system state is accordingly. The difference is, that without the hold function, the alarm can be optionally acknowledged, whereas with the hold function enabled, the alarm must be acknowledged.

Configuration of a job for alarm behaviour

For this configuration step, these menus are required:



In this case, an alarm is an event, related to the according digital input. Jobs assigned to an event determine what should happen when the alarm state is active or has been left.

Click ➤, to open the job list overview:

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

Click **+** to open the job configuration dialogue that inserts a new job to this list.

Note:

The jobs that can be executed are the same as those that can be triggered for the UPS events. This allows full integration of the environmental control sensors into the warning and alarm behaviour. Please note that other sensors may provide different setting options depending on their function.

The registered jobs are executed independently to the hold function:

As soon as the alarm is triggered, these jobs are triggered according to their time configuration. There is no job that is explicitly triggered by pressing "ACK".

Setting up a job to the counter event:

In principle, there are 3 known system states available:

1. The normal state when the system starts up
2. The alarm state (alarm is active)
3. The fallback o the normal system state (Alarm is no longer present)

The start-up system state

At the start-up system state, a general basic system state is initially assumed according to the configuration, which is cyclically checked via the sensors - you will therefore not receive any "alarm-off" messages at system start-up.

The alarm status

If the conditions for the alarm are met, a corresponding alarm condition is triggered and all configured jobs assigned to this event are initiated.

The fall back to normal system state

Depending on the configuration, a corresponding job is necessary to display an appropriate counter event when normal operation is restored. Typical jobs are, for example, email notifications that the normal state has been restored or the opening/closing of outlets to inform neighbouring systems about this event or to provide feedback about triggered event chains, etc.

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

Alarm event and counter alarm event are defined as follows:

Alarm Input [Port Number]

Alarm Input 1 definiert den Port 1 als Alarmereignis. Sobald nach Konfiguration ein Alarm vorliegt, werden die hier definierten Jobs ausgelöst.

Reset Alarm Input [Port Nummer]

Mit Reset Alarm Input 1 werden die Jobs angesteuert, die dem Aufheben eines Alarms zugeordnet sind. Anders als der Alarm-Input hängt die Ausführung der Jobs indirekt sowohl von der Hold-Funktion als auch von der Betätigung des ACK-Buttons im Sensor Monitor ab:

Die „Hold“- Funktion friert den Alarmzustand ein, bis er mit ACK bestätigt und das Problem beseitigt wurde.

Der „ACK“- Button ohne „Hold“-Funktion gedrückt friert den aktuellen Alarmzustand optional ein, bis das Problem entsteht wurde.

The SITEMONITOR 6 AUX Ports

Please note:
The AUX ports for SITEMONITOR 6 are specially build for the SITEMONITOR relay board. Even though the name implies this, no BACS Bus Converter can be connected

The SITEMONITOR 6 can manage up to 8 outputs via the optionally available relay board. Outputs 1-4 are assigned to AUX port 1 and outputs 5-8 to AUX port 2.



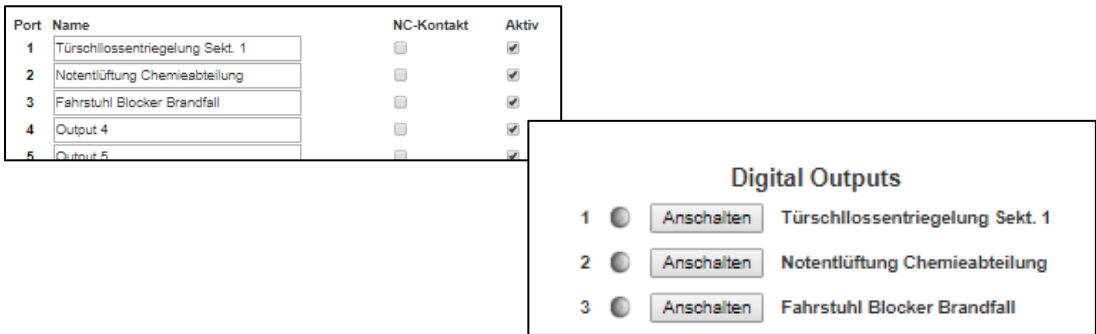
Due to this fact, the SITEMONITOR 6 has up to 8 switchable outputs that you can switch separately.

Port

The port number defines the output that is to be switched. This number is assigned hard-coded and cannot be changed.

Name

The name is freely editable and can be used, for example, to describe its function in more detail. The name entered here will be displayed later in the sensor monitor:



With apply, the text will be saved and displayed. If there are web-proxy in use, please refresh the browser or proxy cache.

NC Contact

This function defines whether the contact should normally be closed or opened.

Depending on the configuration, there are automatic NC or NO contacts, which means that an adjustment must be made with the SITEMONITOR configuration so that the switching behaviour is synchronous with the actual function of the connected system:

If, for example, emergency lighting is to be explicitly switched on, then the contact must normally be open, and closed in an emergency. A lift, on the other hand, can be switched exactly the other way round - because there is an emergency, it is switched off or only travels to the ground floor and remains there.

The following functions are possible

1. NC-Contact is marked, NC active

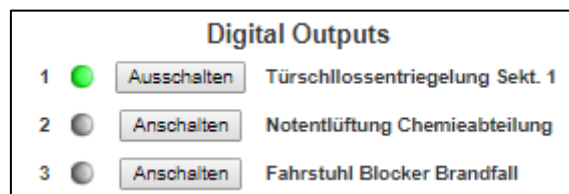
During standard operation, the contact is set to be closed. In case of an incident the SITEMONITOR is configured to, the contact will open.

2. NC-Contact is unmarked, NC disabled

During standard operation, the contact is open. When triggered, a switch will close the contact.

Configuring the outputs

The outputs are switched by setting up a corresponding job. In this case, there is no separate system event for switched outputs. The current status is clearly displayed in the sensor monitor:



Please note that markers and labels change according to the current state:

- Port 1 is ON
 - o The marker is green.
 - o The button shows „switch off“
- Port 2 OFF
 - o The alarm marker is grey
 - o The button shows „Switch on“

Switching outputs via a system event

Switching of outputs are assigned as a job to a system event of your choice - it does not matter whether you use an input or - if available - a UPS event to switch an output:

1. As Job, select the Job AUX.
2. With port number, select the Output.
3. With Command, define whether the output signal shall be set to ON (High) or OFF (Low)

Please note that these are digital outputs which are converted accordingly by a relay board or a digital input of another device.

Job timing

Please note that these are digital outputs which are converted accordingly by a relay board or a digital input of another device.

Job Timing

Based on the event the job AUX is configured to, the correct trigger timing may be useful. Please note that wrong timing may harm other aspects within your IT infrastructure and the warning behaviour. With job timing options, the SITEMONITOR provides a unique

Add Job to Event Powerfail

Job
AUX

Parameter

Port Number
SiteManager Outlet 1

Command
Set High (On)

Timing

☒ Immediately, once

☐ After seconds

☐ After seconds, repeat all seconds

☐ After seconds on Battery

☐ At seconds remaining time

Save
Cancel

function to automate time-controlled output switching behaviour.

Sensors and devices for the SITEMANAGER 6

Differences to the SITEMONITOR 6

As with the SITEMONITOR, remove the clamping and screw strips carefully. The difference can be found in detail:

Whereas the SITEMONITOR can manage 64 digital inputs and operate outputs via a special relay board, the SITEMANAGER has 8 analogue and 8 digital inputs that can be operated either via regular plugs or via the terminal strip.

Furthermore, the SITEMANAGER 6 provides a fully featured native BACS support.

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



To avoid damaging the SITEMANAGER or the system connected to it, please the Daleks and obey the hardware setup as followed:

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

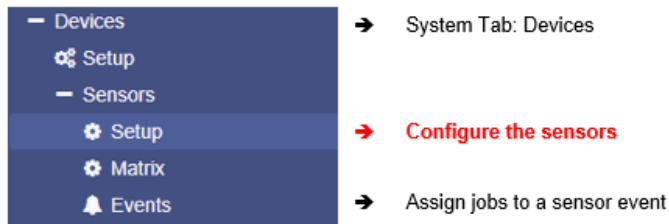
It is possible to use one channel via the sensor input 1 and at the same time address the second channel via the terminal strip via AN2. In case of using a combined sensor with the Sensor Input 1, Sensor Input 1 and 2 / AN 1 and AN2 are in use simultaneously.

With the „DIG “– Inputs, up to 8 digital inputs are provided. They can be used to connect digital devices to the SITEMANAGER 6. The lower terminal strip provides a 12 V power supply via the plus and minus poles, which can be operated in a similar way to the SITEMONITOR:

if there is the need of using 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 want to equip external sensors or switching devices with a power supply, you can tap the necessary power supply via the lower terminal strip and then connect the digital contact to the corresponding digital input.

SITEMANAGER 6 Configuration

For this configuration step, open the following menu:

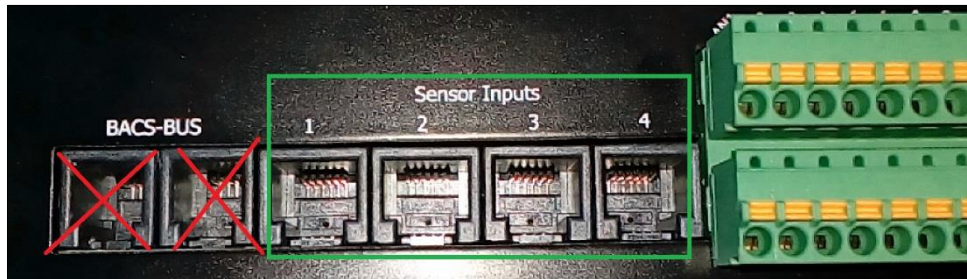


The SITEMANAGER 6 offers a significant difference to the CS141 with its optional modules. Due to the connection, the UPS interface COM1 is a MINI-DIN connection, the serial 9-pin SUB-D connection is used internally elsewhere to map the additional functionality.

Sensors are important for SITEMANAGER 6 because they provide a lot of information about the environment, which can be relevant for the operation of systems. This includes, among other things, humidity, air pressure, temperatures, etc: If electrical devices are operated outside the regular operating environments, they can be damaged or, in the worst case, destroyed. With sensors, the SITEMANAGER 6 is capable to trigger countermeasures before these devices are harmed by environmental conditions. To do this task, one of the special features of the SITEMANAGER 6 is the possibility to manage up to 8 sensors, analogue and digital inputs and to assign specific system events to them. Furthermore, the SITEMANAGER 6 is the only device in the CS141 family that offers 4 output relays for switching external systems or defining switching states for target devices.

Connecting a sensor

Connecting a sensor is similar to the GENEREX sensor manager - on the back of the SITEMANAGER, you will find the corresponding connection ports to the left of the terminal strip.



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, you can connect up to 8 sensors - 2 channels are assigned to each sensor input. Basically, you can distinguish between two different sensors:

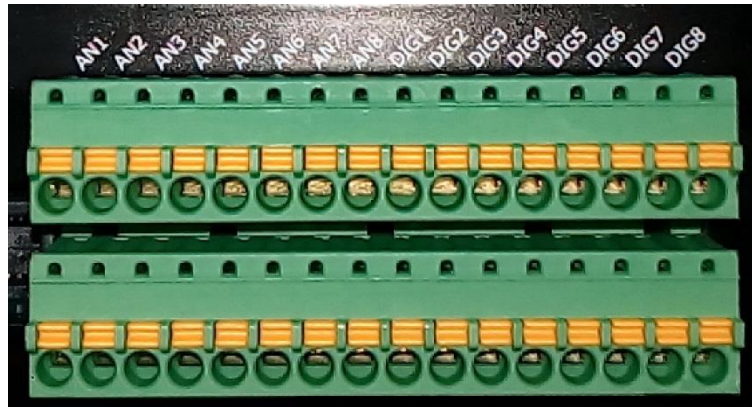
- The Single Sensor

This sensor provides a second port to connect a second sensor.

- Der Combined sensor

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

When connecting, please ensure that the sensors are connected correctly in series to avoid running into a "missing sensor" - issue during configuration.

Using the direct connectors

If there is a need to connect of sensors directly, the SITEMANAGER 6 offers an optional terminal strip. The following key is used for this:

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 the reference points can be obtained from the second terminal strip below.

The configuration screen in the SITEMANAGER is divided into 3 parts

Analogue Sensors

Sensor Inputs	Name	Sensortype	Unit	Low PreAlarm	Low Alarm	High PreAlarm	High Alarm	Sensor Range	Offset
1	Channel 1	Custom 0-10V		2	1	8	9	0 - 10	
	Channel 2	Custom 0-10V		2	1	8	9	0 - 10	
2	SM_DIG	SM_II_DIG	°C	12	10	32	35	-25 - 100	
	Channel 4	Custom 0-10V		2	1	8	9	0 - 10	
3	Temperatur	SM_T_H	°C	12	10	32	35	0 - 100	
	Luftfeuchte	SM_T_H	% rel H	15	10	50	60	0 - 100	
4	Channel 7	Custom 0-10V		2	1	8	9	0 - 10	
	Channel 8	Custom 0-10V		2	1	8	9	0 - 10	
Hysteresis		3							

After connecting the sensors, open the system menu "sensor type" and define which sensor is connected. Please note that the individual channels are routed to the outside in pairs: Sensors 1 and 2 form a channel pair, sensors 3 and 4 form one, and so on. If you set a combination sensor that uses 2 channels, the corresponding sensor twin is automatically assigned to the channels.

Definition of the alarm thresholds

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

Alarm (niedrig)	Vor-Alarm (niedrig)	Vor-Alarm (hoch)	Alarm (hoch)	Sensor Bereich
1	2	8	9	0 - 100

Sensor range

The sensor range defines the range that is measured.

Depending on the sensor, the Thresholds may vary, in this case it is a temperature sensor with the measuring range of 0-100°C: 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 higher than 80°C could well be a realistic value.

Let us do an example configuration: In this example configuration, let's say a room will be monitored whose equipment is allowed to operate between 5°C and 45°C. To adapt the scale to the realistic value, one would therefore design the scale from 0°C to 60°C approximately. That should be should fit to the equipment.

Pre-Alarm and Alarm

The pre-alarm is the alarm instance where increased vigilance is required. - Although problems do not yet occur in this area, the temperature is remarkably high. Alarm is the instance where an immediate response should be made, otherwise the equipment may be damaged.

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

1. What is the average temperature if the technical equipment is in use?
2. How temperature fluctuations due to operation and environmental influences are to be assessed.

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

The pre-alarm should be triggered BEFORE the actual alarm. This means at about 10°C - the sending of emails, for example, can be stored there later as a job event. The alarm, on the other hand, is triggered at 6°C. Here, for example, the shutdown of the system can be defined in companion with alarm and notification emails.

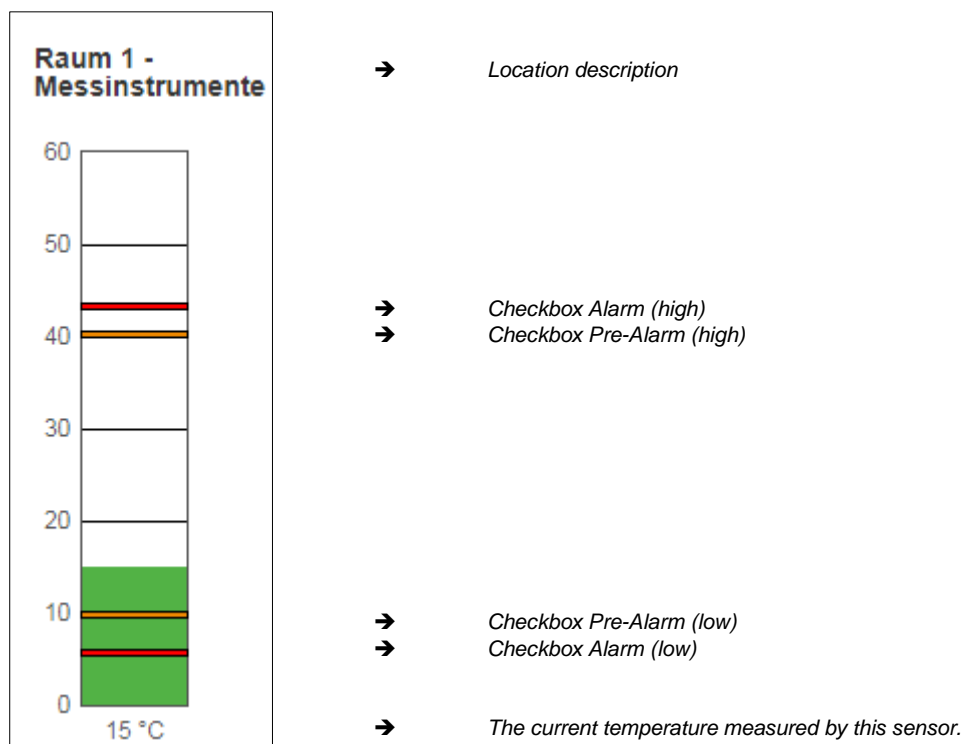
The upper range is defined similarly: The VOR alarm is set at 40°C, while the alarm itself is triggered at 43°C and initiates appropriate emergency measures.

The complete configuration line will look like this line:

Sensor	Standort	Sensortype	Einheit	Alarm (niedrig)	Vor-Alarm (niedrig)	Vor-Alarm (hoch)	Alarm (hoch)	Sensor Bereich
1	Raum 1 - Messinstrumente	SM_T_H	°C	6 <input checked="" type="checkbox"/>	10 <input checked="" type="checkbox"/>	40 <input checked="" type="checkbox"/>	43 <input checked="" type="checkbox"/>	0 - 60

The checkbox defines whether this value is activated or ignored.

After pressing Apply, the results can be seen in within the sensor monitor:



Digital Inputs

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

The digital inputs are configured similarly to the sensors. The following settings are possible:

Name

Assign a unique name for the input in the free text. Since the associated sensor or system can be located somewhere inside a building, make sure that the name is clear.

NC contact

This setting defines whether a contact should normally be closed or open. 3rd party sensors or systems handle this very differently. Since the digital input can only detect high/low signals, it is important to know which value ultimately represents the normal state.

Active

This checkbox enables / disables the output

The outputs offer the possibility to actively switch a relay contact. The switching state will be shown in the sensor monitor and on the front of the SITEMANAGER 6 (the LED group 'Digital Outputs'). In some cases, it is necessary that relay contacts are automatically switched on SITEMANAGER system start.

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"/>

Enable

Define whether the SITEMANAGER should automatically switch these outputs on when restart is in progress

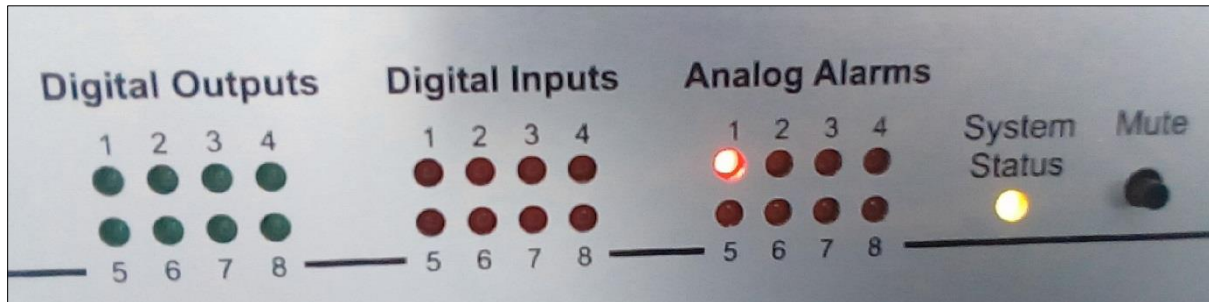
Delay

The SITEMANAGER will wait this time in seconds until an output is switched.

Extended System Monitoring

The SITEMANAGER 6 provides different methods to communicate a problem:

There are status LEDs on the front that are logically assigned to all possible connections:



Digital Outputs

LED colour: green

These LEDs light up in case of a switched a digital output

Digital Input

LED colour: red

These LEDs flash when a problem has been detected.

The flashing becomes a static light as soon as the error has been confirmed within the SITEMANAGER 6.

Analog Alarms

LED colour: red

These LEDs flash when a problem has been detected.

The flashing becomes a static light as soon as the error has been confirmed within the SITEMANAGER 6.

Die System Status LED's

This LED is assigned to the BACS system, please refer to the BACS manual.

Special feature: Power LED

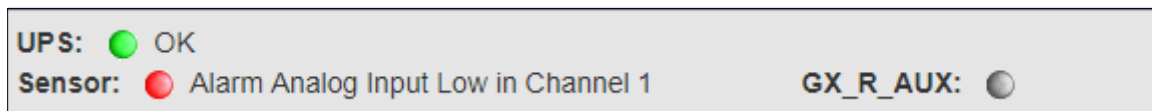
LED colour: green

The power LED provides information about different system states:

Die LED...

- Lights up static green when the system has been 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. The upper status bar provides quick information after logging in:



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



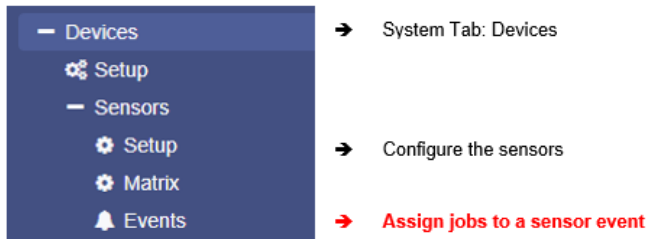
The sensor monitor will initially assume that this state is wanted in some way:



However, the LED on the front bar will continue to glow red statically to indicate a corresponding fault during the next maintenance.

SITEMANAGER 6 – Job definition:

For this configuration step, open the following menu:



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

Search for the following events:

Event: Alarm Analog Input 1:

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

Jobs assigned to 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
---	---	--------------------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Jobs assigned to this event determine what should happen when the alarm state has been left.

Click ➤, to unfold the tab and get an overview of all configured jobs coming with this event:

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

Click + to open the Job configuration dialogue.

Note:

The jobs that can be executed are the same as those that can be triggered for the UPS events. This allows full integration of the environmental control sensors into the warning and alarm behaviour. Please note that other sensors may provide different setting options depending on their function. For more information, please refer to the CS141 user manual, available for download at www.generex.de

Digital Inputs – Assign a Job to an Event

Suchen Sie nach Alarm Digital Input

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

Click **+** to open the configuration dialogue to define a job.

Feel free to assign as many jobs as you like to the event - SITEMANAGER 6 will trigger them according to the configuration.

The counter event:

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

A typical example would be an RCCMD shutdown with redundancy behaviour. The RCCMD client receives a command from the SITEMANAGER to trigger a shutdown, but is still waiting for a CS141 that has not triggered the command.

In this case, the RCCMD shutdown must be withdrawn by the SITEMANAGER. This counter job will be configured accordingly as a corresponding. Otherwise, the RCCMD client assumes that the command for shutdown is still active until RCCMD is restarted manually by a user.

Depending on the type of event, there will be a specific canter event or an event pair like "Digital Contact 1 ON / Digital Contact 1 OFF" - If necessary, please remember to configure an according job.

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

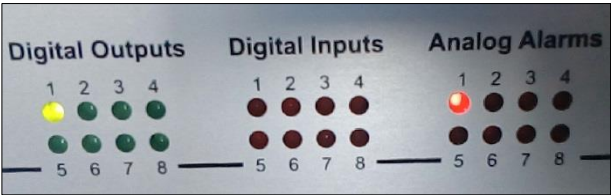
Exception coming with the Job "AUX":

Special feature of the JOB AUX:

For the CS141, a CON_R_AUX4 is an optional part to provide fully featured outlets and inputs.

The SITEMANAGER 6 has this function already integrated.

As job, select AUX. The parameters will switch to provide configuration options for outlets Port 1 - 8. Switched outputs are displayed accordingly on the front side under Digital Outputs.



Ausgänge			
	Name	Status	Anschalten
1	Output 1		<div>Switch Off</div>
2	Output 2		<div>Switch On</div>

Switch ON / Switch Off is displayed accordingly at the outputs on the front of the SITEMANAGER 6. If you switch the output to off, both displays are switched off. Please note the caching problem of web browsers in this context:

If the front LED on the unit is switched off but is still on in the web interface, update the browser cache.

Creating a job

Note:

The jobs that can be executed are the same as those that can be triggered for the UPS events. By doing so, the SITEMANAGER 6 allows full integration and to combine environmental control sensors with a UPS based warning and alarm behaviour.

Please note that other sensors may provide different setting options depending on their function.

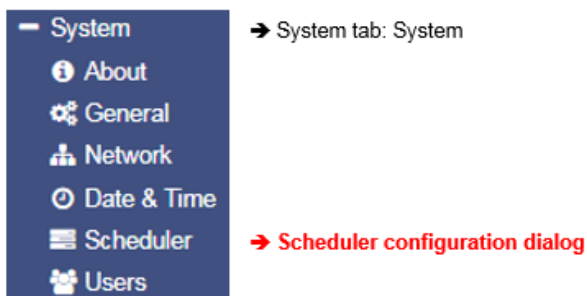
Click ➤ to open the Job overview for the according event:

–	□	+	🗑	SM_T_H_COM Temperature High	1	1	0	0
				Job Typ	Wann	Parameter		
				Log	Einmal, sofort	{ "text": "SM_T_H_COM Temperature High" }		

Für das Ereignis einer zu hohen Temperatur ist demnach bereits ein Job konfiguriert.

Scheduler

For this configuration step, navigate to the following menu:



Regardless of all system events, the models of the CS141 series offer the possibility to run jobs at freely definable times.

These so-called scheduled jobs can be used, for example, to control subordinate systems, to restart computers, to perform battery tests, etc.

Configuration menu for scheduled jobs

As factory default configuration, no job is defined. They need to be defined by administrators or engineers

Press +: to start scheduled task configuration dialog

The job configuration dialog is similar to UPS event job configuration dialog. Timing configuration differs due to the fact these jobs have to be triggered independently to UPS alarm states:

Start: enter date and time the job will be executed the first time.

Repeat toggles the job repeating behaviour

These values are valid:

One time: only one execution

Daily:

Every day depending on system time

Weekly:

Once a Week depending on system time

Monthly:

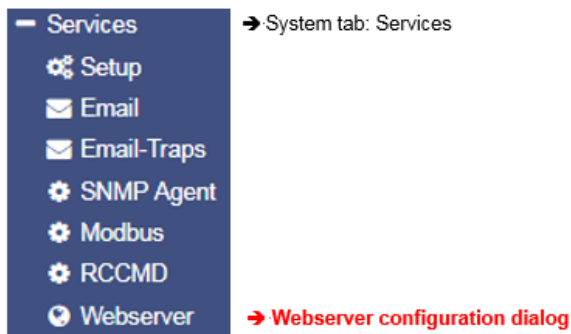
Once a month depending on system time

Note:

In some cases, jobs can be set up according to the configuration of connected devices.

Webserver

For this configuration step, navigate to the following menu

**Warning:**

In normal mode we do not recommend disabling the http Server.

The checkbox Enable HTTP Server should be active at least inside rescue mode! In some high-security networks, it may be desirable for the CS141 not to be accessible via the web interface. Disabling this feature will accomplish this condition - be careful with your decision: The web interface will be completely disabled and cannot be started again. In this case you can only access the CS141 via the rescue system - if you deactivate this function inside normal mode and rescue mode, the device must be sent to the manufacturer for a complete hardware reset.

For security reasons, the console access was completely locked up. The CS141 is configured exclusively via the web interface via http or https.

- HTTP Port to reach the web interface
- HTTPS Port to reach the web interface
- If marked, only https will be served
- Time until the web page refreshes
- Select start up page after login
 - Simple monitor: Usefull for small screens
 - If marked, tooltips will be shown
- Auto Logout if no click is done for this time

Enable HTTP Server

This feature controls the accessibility of the internal web server of your CS141 web manager. If this checkbox is deselected, the CS141 works as part of its functions, but refuses to respond http requests.

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 specified different ports for your Web Manager or inside your IT infrastructure, you can enter an according port number. Please note these conditions require to specify the port for the web query inside your web browser:

192.168.3.1:85

In this case, the web manager would be reachable on the IP 192.168.3.1 at port 85. Port 80, on the other hand, the web browser will prompt an error message.

HTTPS Port

As a standard HTTPS port 443 will be used. If necessary, you can adapt this port to your network.

Force HTTPS

A standard HTTP connection on the Internet can be easily tapped by unauthorized persons. In order to avoid this and thus ensure a secure data transfer, an HTTPS connection is used. This will allow encrypted data transmissions as well as authenticated server devices.

As advantage the security level increases. As disadvantage reaction time will drop since the data are transmitted encrypted.

Force HTTPS stops regular HTTP traffic and forces the use of HTTPS

Note:

Once force https is enabled, the syntax https:// must be used. Otherwise, there are two basic options for the web browser:

Connection timeout

Since CS141 only responds to HTTPS, the web browser will not receive data.

Forwarding (browser-specific)

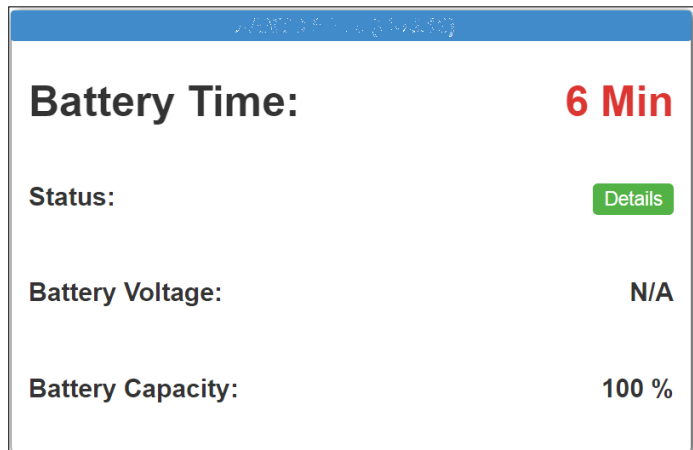
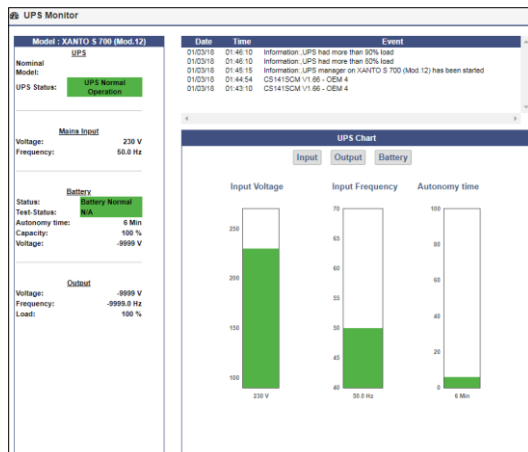
If multiple CS141s works inside a network, it may happen that there is an alternative valid entry in your web browser - you will be re-routed to another CS141.

HTTP Refresh time

The CS141 will automatically return an updated page showing, among other things, the status of UPS systems or other available status monitors. This value defines how often an automatic page refresh is performed. By default, the CS141 updates these displays every 10 seconds.

Use simple monitor

The CS141 provides two different monitoring screens for UPS data. This function is useful in case of a small monitor is used.



information but better readability

The simple monitor (pictured on the right) contains significantly less

Enable HTTP Tooltips

Tooltips are contextual hint windows that pop up automatically when you hover settings. By default, the tooltips are enabled but can be permanently disabled.

Tutorial: How to create a server.pem-file

There are many ways to create a key and a certificate.

A comfortable freeware tool is X Certificate and Key Management.

This tool offers not only the possibility to create valid certificates but also the option to include necessary keys. After creating, these files can be exported to be used with the CS141.

In addition, this tool comes with a small database to manage all keys as well as certificates easily. This tool is not the only one of its kind, but highly recommended:

- Easy to use
- Fast key and certificate creation (administration)
- This tool is available for Windows, Apple and Linux.

Create certificate and key

Step 1. Download and Installation

The tool is available through several download sources, a good and clear download link is presented here:

<https://hohnstaedt.de/xca/>

Please note that download links may change over time and need to be adjusted accordingly. The setup file includes an installer that guides through the installation process.

Step 2 Create database (example: Windows version, Linux and Apple may vary slightly)

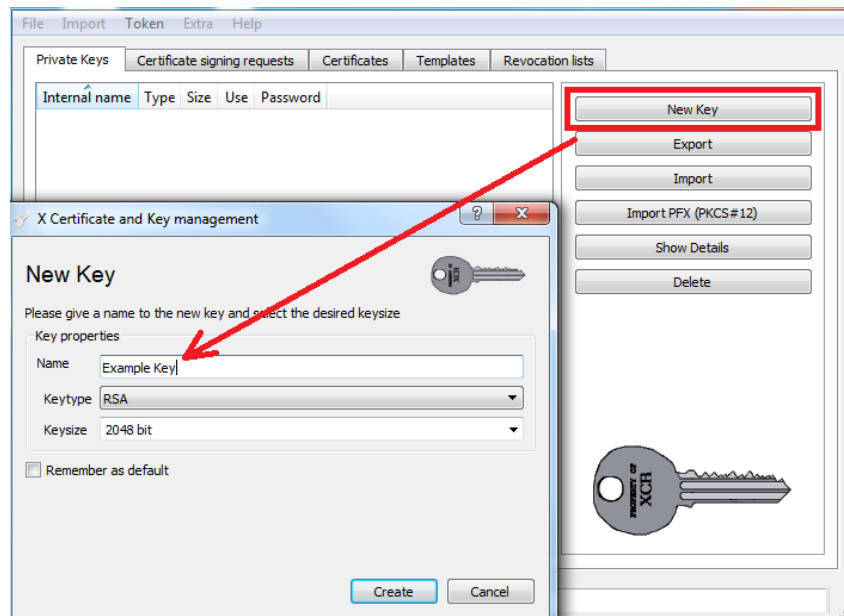
After installation, click on File and create a new database. It is not necessary to enter a password to protect the database

WOLZ	13.02.2018 12:40	Dateiordner	
Beispieldatenbank	09.07.2018 16:28	XCA database	1 KB
	09.07.2018 16:28	XCA database	1 KB

This database can be stored and re-opened for later usage.

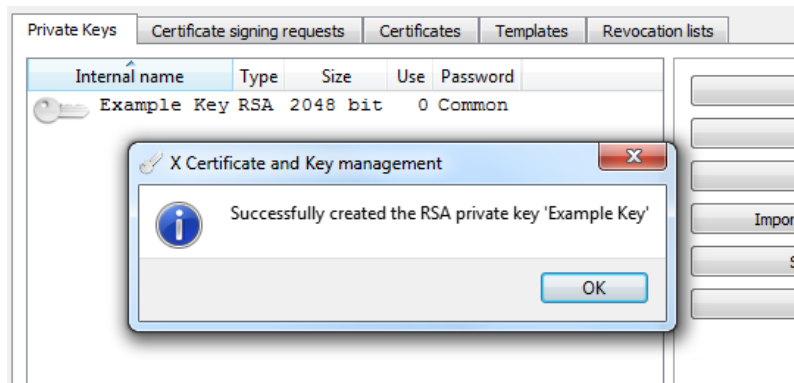
Step 3: Create and export a private key

Go to private Keys and press the button New Key:

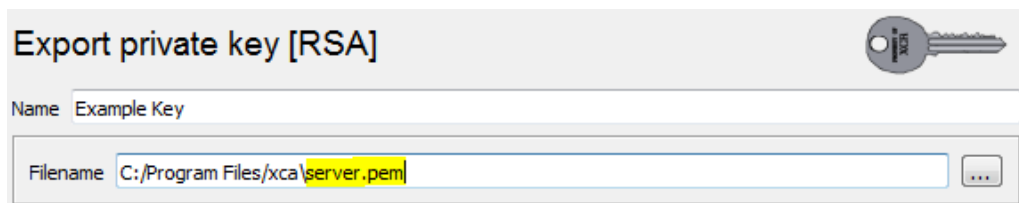


Click Create to complete this process. The key will be provided in the database containing a corresponding message.

This key is the first of two required parts to create a valid PEM file.



After creating, export this key. Remember to rename the export file name to server.pem:



There is no need for special editing tools required - Edit this file with a regular text editor and attach the certificate.

Step 4: Creating / exporting the certificate

The second part of the PEM file contains the necessary certificate to operate the CS141 with force HTTPS mode. To create the certificate, open Certificate signing request click on "New request" This will begin the certificate configuration dialog:

Most Important are information about holder, extensions and key usage.

Distinguished name			
Internal Name	Beispielzertifikat	organizationName	GENEREX
countryName	HH	organizationalUnitName	GENEREX-IT
stateOrProvinceName	HH	commonName	GENEREX
localityName	GENEREX_Demo	emailAddress	support@generex.de

Enter the owner's data for this certificate here. Adjust the data according to your usage. Click Add to transfer your entry to the tool's database.

Extensions

Unter Erweiterungen können Sie die Gültigkeit des Zertifikats einstellen:

Validity		Time range	
Not before	2018-08-20 11:11 GMT	10	Years
Not after	2028-08-20 11:11 GMT	<input type="checkbox"/> Midnight <input type="checkbox"/> Local time <input type="checkbox"/> No well-defined expiration	
		<input type="button" value="Apply"/>	

Passen Sie diese Daten an, um die Dauer des Zertifikats zu bestimmen. Mit übernehmen Schließen Sie diesen Vorgang ab. Schlüsselverwendung.

Check both check boxes and mark all modules you wish to include in your new certificate:

X509v3 Key Usage

☒ Critical

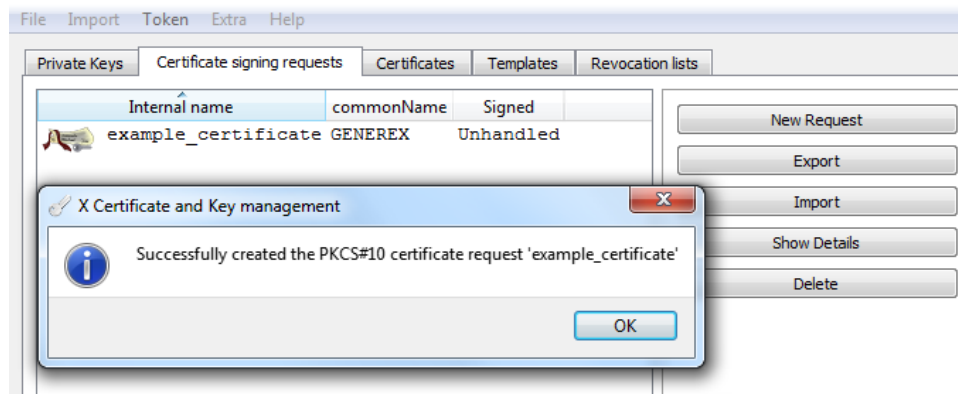
- ☐ Digital Signature
- ☐ Non Repudiation
- ☐ Key Encipherment
- ☐ Data Encipherment
- ☐ Key Agreement
- ☐ Certificate Sign
- ☐ CRL Sign

X509v3 Extended Key Usage

☒ Critical

- ☐ TLS Web Server Authentication
- ☐ TLS Web Client Authentication
- ☐ Code Signing
- ☐ E-mail Protection
- ☐ Time Stamping
- ☐ Microsoft Individual Code Signing
- ☐ Microsoft Commercial Code Signing

If you are not sure of the exact purpose for which you want to use the certificate, in case of doubt, activate all the options offered to you. This will allow the certificate to maximum functionality. After you have entered all data, click OK at the lower right corner



Export the certificate to a .crt file.

Stitch together...

From now, you should have two different data:



Open the certificate with an editor and copy the content. The content looks something like this:

```
-----BEGIN CERTIFICATE-----
MIIEoDCCA4igAwIBAgIBATANBgkqhkiG9w0BAQsFADCBjTElMAkGA1UEBhMCSEgx[...]
hQ9t4jtt2VSTnv4rlrHoT8j5/yEFpRKg6D/5zmaVscI94gUp
-----END CERTIFICATE-----
```

It is important that you completely copy the entire file including BEGIN CERTIFICATE and END CERTIFICATE! Otherwise, it will not work.

open the file server.pem and copy the certificate under the key:

```
24 HbASwwKBgQCsZfpDOEsNZis3h6khXXWIj3/A1NKmWB4Hsq9EgVKMZasKK8mGLIqD
25 RmkXwyQQgoTJuknaDLAFXFQV4XBpEC6N5/zvNj1LKYGEEKik4ibwlyF52CqhPtiI
26 DOPUGYKLeDfEAXNK5mKq349qC5C177YFDFrAtiZDysh2KgRR0kCg==
27 -----END RSA PRIVATE KEY-----
28
29 -----BEGIN CERTIFICATE-----
30 MIIEoDCCA4igAwIBAgIBATANBgkqhkiG9w0BAQsFADCBjTElMAkGA1UEBhMCSEgx
31 CzAJBgNVBAGTAkhIMRUwEwYDVQQHDAxHRU5FUKVYX0R1bW8xEDA0BgNVBAoTB0dF
32 TkVSRVgxZzARBgNVBA5TCkdFTkVSRVgtSVQxEDA0BgNVBAMTB0dFTkVSRVgxITAf
33 BekahkiG9w0BCOEWEnN1cHBvcnRAZ22VuZlZlZC5kZTAeFw0xODA3MDkxND0zMDBa
```

Save this file without changing the file name, the file extension or file type.

CS141: Inserting the server.pem file

Open CS141 and navigate to the certificate web server:

Upload TLS Certificate for Webserver

Drop server.pem File here
or click to select

PEM file <no file selected>

The order of the items in server.pem is important!

```
-----BEGIN RSA PRIVATE KEY-----  
[server private key]  
-----END RSA PRIVATE KEY-----  
  
-----BEGIN CERTIFICATE-----  
[server certificate]  
-----END CERTIFICATE-----
```

use drag'n'drop to copy server.pem into the field provided by CS141. Upload will start the upload and import process. Once upload is finished, you can test the certificate by typing:

http: // <your IP address>

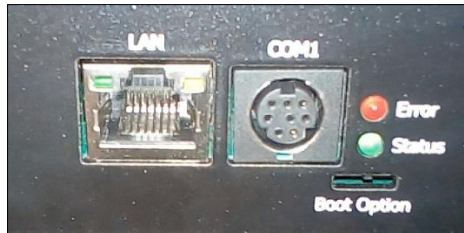
https: // <your IP address>

If both inputs respond as desired, you can use Force https to enable explicit encryption.

Diagnostic: Status LED's

The CS141 offers several options for diagnosis. The fastest method is a quick visual inspection of the LEDs

To perform a quick inspection, just take a look at the two LEDs next to the COM 1 interface:



Green LED	Red LED	Adapter
OFF	OFF	No Power
OFF	AN	Boot in progress
OFF	SLOW BLINKING	Update in progress
AUS	FAST BLINKING	Update failure
ON	ON	Communication lost: UPS or external device
SLOW BLINKING	OFF	Everything is OK with the world

After logging in, the CS141 will display a more detailed overview of the current system state:

UPS: Ready

A green marker indicates communication without problems.

Please note the setting no UPS device selected will show a dummy screen and the LED will also be green.

UPS: Initializing

A yellow marker is displayed if:

- The device will initialize and the communication is being established
- there is a warning behaviour. It might be required appropriate intervention in the near future.

UPS: Temperature Bad

If the LED is red, an alarm or critical condition is currently detected:

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

The type of the alarm is displayed in detail.

UPS: Communications Lost

A blue marker indicates that the device was probably configured correctly, but no initial communication has been established.

Sensor: Disabled

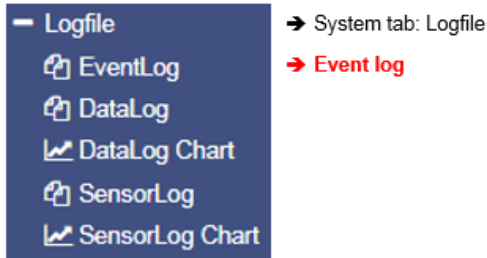
A grey marker and the description disabled means that a device has been completely deactivated and cannot provide any data.

Logfiles

In the event of a malfunction, the log files offer a great deal of information that can provide valuable clues about the chain of events and the course of the malfunction in the subsequent search for the cause.

Event log

Since this is not a configuration step, just navigate to the following menu:



The event log contains all actions concerning the CS141 and the UPS are recorded. The event history will be written by any event containing a log job. The most significant jobs are included by default settings. Administrators may create, edit and delete default settings as well as creating custom log entries.

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	

After reboot the first entry is a message by CS141 with its OEM ID:

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

Please note the latest entry is always on top of the list. Download as CSV file creates a CSV file from this event log and stores it locally on your hard disk:

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

Any program that can deal with CSV files can be used to open the event log.

A12		
	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		

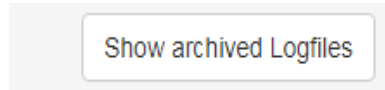
In case of current memory to store event, logs are exhausted, the CS141 will open an archive file and move the current event log. This archive file will be provided for both: downloading as well as instant view.

Note:

Depending on the configuration, the system events in the event log are kept for up to three months. As soon as the running memory for the current event log file is exhausted, the files are stored alternately in up to two archive files. This generally provides a monitored period of up to 9 months from initial start-up.

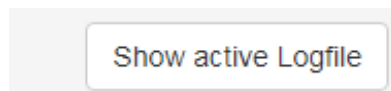
Navigate between logfiles

By default, the current event log is displayed



Administrators are able to toggle between the two logs by clicking the button "Show archived Logfiles" in the upper right corner.

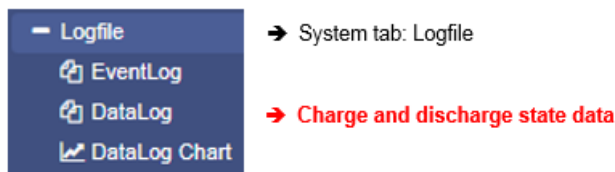
By doing so, the label of this button will change:



To return to the active log file, press the button labeled "Show active log file"

Data Log

Since this is not a configuration step, just navigate to the following menu:



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,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,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,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,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,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,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,6.0

The data log recognizes measurement data of the UPS. Due to the fact these are provided with a time stamp, they can be combined with the event log:

Analysts can build event chains with additional UPS data.

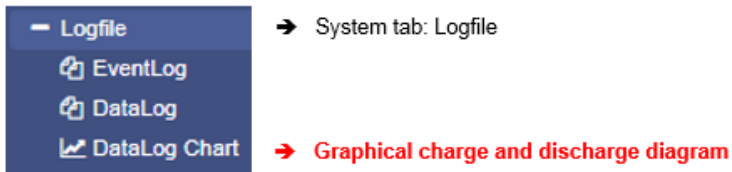
Like the event log, data log can be exported as CSV file as data backup. The data log stores the entries every 3 minutes and keeps the entries 8 weeks as the current data log file. After that the actual data log will be moved to an archive file and a new data log for the current data is opened.

The CS141 provides storing up to 2 independent archive files:

In addition to the current period, there are up to 24 weeks available. After expiry of the time, the oldest archive file is replaced. As with the event log, administrators can toggle between active log and achieved logfiles.

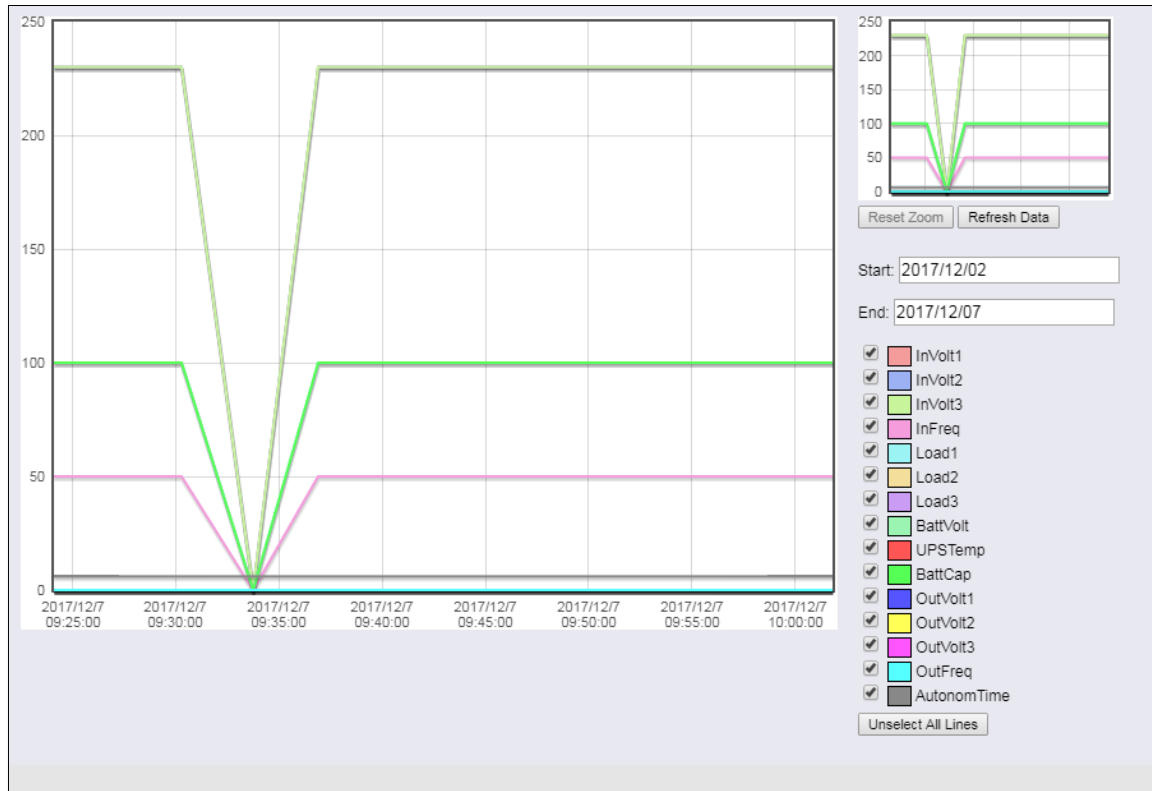
Data log Chart

Since this is not a configuration step, just navigate to the following menu:



With data log Chart CS141 provides a graphical presentation of the battery history:

This feature allows to examine all entries within the data log exclusively. Single entries can be selected by using checkboxes:



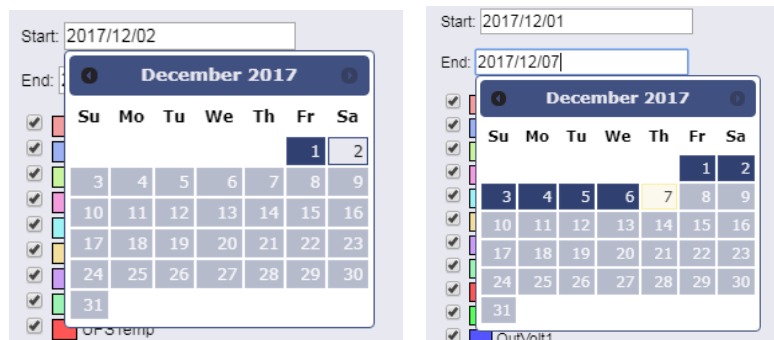
In addition to the current values, the CS141 provides selecting specific values from current databases.

As a default, all check marks are set when called. You can use the Unselect All Lines function to remove them and set the relevant checkmarks.

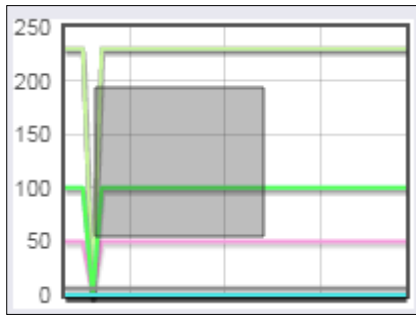
How to use the calendar

The calendar feature provides a quick overview of existing time periods that are selectable. Click the date field to bring up the calendar:

The dates of the corresponding period are automatically loaded and displayed inside the main window.

Zoom the Chart

The CS141 provides zooming the data and thus obtain a detailed view within the displayed measurement data.



To refine display, drag a frame inside the small window. The main window will automatically show a detailed view and provide a customized timeline.

Reset Zoom

The zoom function allows an enlargement of the timeline up to 2 minutes.

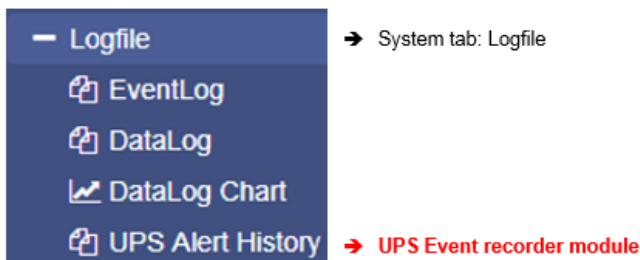
This function resets the zoom back to the original scope.

Refresh Data

This function updates the current data shown and refocusses the timeline.

Premium function: The UPS alert history

This menu is only available if your UPS will support the functionality
Since this is not a configuration step, just navigate to the following menu:

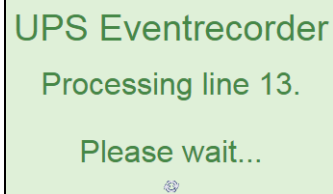


Not only the CS141 logs events - many UPS systems provide their own internal non-volatile memory to log events as well as internals. This information can provide very useful insights if irregularities occur after a configuration.

Note

The CS141 adapts itself to functions a UPS provides - The UPS Alert History is only available if your UPS supports this function.

Reading internal event logs of the UPS



Each time the UPS Alert History button is pressed, the event memory of the UPS read out and displayed accordingly.

Please note that displayed status messages as well as the scope and information value may vary:

Some UPS models provide more useful information than others.

After reading, UPS data are displayed inside a chronologically arranged history. At the top of the list, you will find the oldest UPS log entries. At the bottom of the list, the latest entries will be shown.

```
2018/05/30 14:42:28.780 Event #298: ABM testing
2018/06/05 14:02:54.000 Event #290: Clock set
2018/06/11 10:06:07.610 Event #139: Inverter off
2018/06/11 10:06:07.610 Event #294: UPS off
2018/06/11 10:48:57.130 Event #139: Inverter on
2018/06/11 10:48:57.130 Event #298: ABM discharging
2018/06/11 10:48:57.170 Event #237: UPS on normal
End
```

End determines the last entry of the logfile.

Exporting UPS data log

If needed for later analysis for statistical and diagnostic purposes, the CS141 provides to export and save the log as CSV file and save it locally to your hard disk

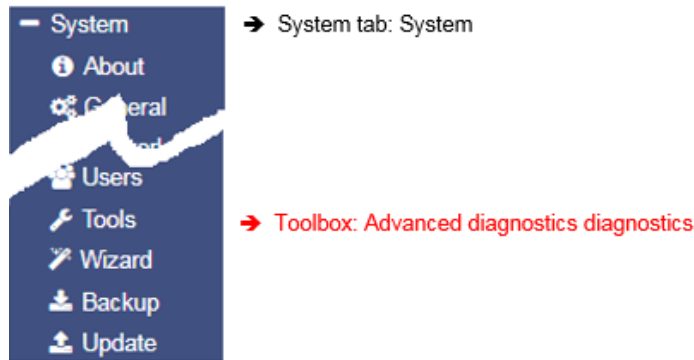
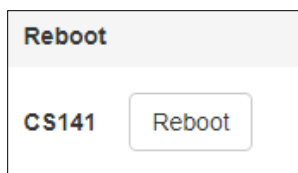
[Export to CSV](#)

Note:

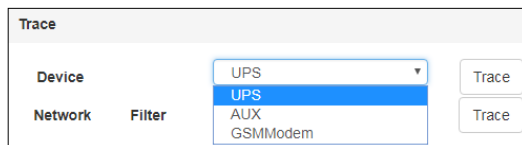
The UPS Event Recorder polls the current list from the UPS with each call - These log data will not be cached or saved by CS141.

Tools

For this configuration step, navigate to the following menu:

**Reboot**

Due to the fact the CS141 accept changes inside the configuration and start or restarts the corresponding system services in real time, a complete restart is an exceptional situation. In case of a restart of the CS141, UPS continues its normal mode: A reboot of CS141 does not affect the UPS. To prevent an accidental triggered reboot, this feature was deliberately placed inside *Tools*.

Tracer

The Tracer is a comprehensive diagnostic tool for verifying communication between the CS141 and the connected devices as well as for identifying network problems.

Under Device communication information about external devices connected to CS141 can be queried. To track a device, open the

context menu and select the device you want to monitor. As the screenshot illustrates, the CS141 provides COM 1 / UPS, COM 2 / GSM modem and COM 3 / AUX-Port:

COM 1/ UPS

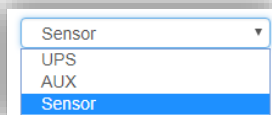
The tracer will screen the current communication running at the serial RS232 port. Faults or faulty communication are displayed in real time and can be saved for later evaluation

COM 2 / GSM-Modem

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

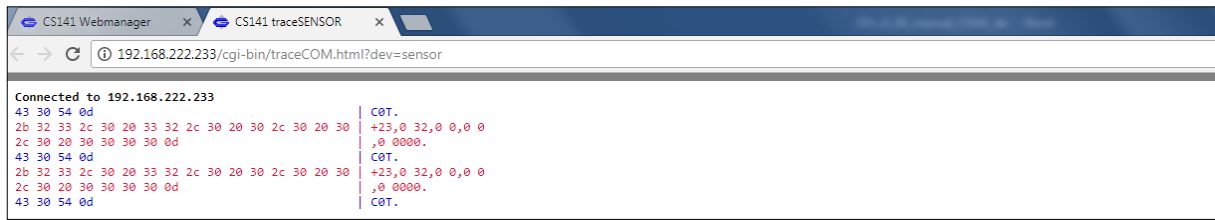
COM 3 / AUX

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

Note:

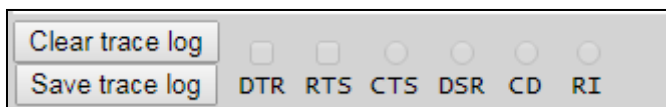
The Tracer adapts itself to the choice met under Devices in the configured in general port settings. If sensors or a Sensor manager 2 is configured instead of a GSM modem, the tracer will show these devices.

The button labeled Trace starts the process. Depending on your browser's configuration a new tab will be opened to show the data stream of the communication between the device and the CS141:



The trace ends automatically by closing this tab. Please note that the data will be discarded. To save the data, mark it with the left mouse button and copy the content with CTRL + C, and insert the information with CTRL + V to a text file.

Available Tracing tool control options



- Clear trace log

Clear trace log deletes the current display - the information cannot be recovered afterwards.

- Save trace log

This function will transfer the current browser content into a standardized text file.

Note

This log file contains the complete time-stamped communication between the CS141 and UPS connected to it: The CS141 asks and the UPS responds accordingly. Since these entries are time stamped, this communication may be compared to external events - this valuable information may help finding the cause of an incident.

The telemetry data file is placed in real time inside the memory of the web browser. By closing this window, the trace data file is automatically terminated and lost. Ensure saving data before closing the window of the web browser.

Trace file evaluation

Open the saved text file. Please note the extended text formatting - Ensure to use a text editor mastering extended text formatting. As an example, typical applications would be editors like sublime or the editor write by Microsoft Windows.

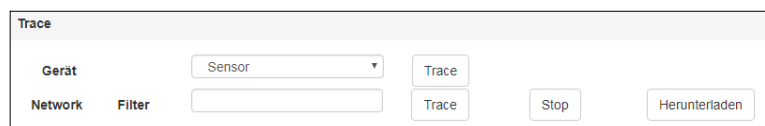
For a detailed analysis, the official protocol description of the UPS is necessary.

For further details, please refer to the manufacturer of your UPS.

Network-Scan

As special feature the CS141 provides an integrated network scanner to examine the LAN for issues and errors. The network scan provides extensive information for evaluation about the network the CS141 is connected to. All data packets are collected in a log file.

After network scan, the network log can be downloaded for evaluation.



Privacy Policy:

Since the network scan records all traffic in this network segment the CS141 is connected to, an evaluation with a corresponding network tool can be used to find error. Furthermore, deep insights into the network traffic are available, e.g., to log the user behaviour. Technicians should inform the respective responsible person before use.

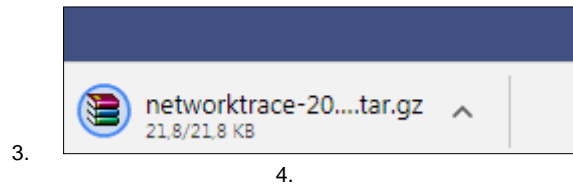
To perform a network scan, click on the Trace button in the Network line. The tracer will confirm tracing activity with a short fade in.

Device	UPS	Trace
Network	Filter	Trace
running		
Stop		
Download		

The Tracer logs packet data within the LAN segment in real-time and stores it locally on the CS141. The tracer will quit if there are two conditions:

1. A reboot (expected / unexpected)
2. By pressing the Stop button

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



Note:
The network tracer is usually very rarely needed. In seldom cases GENEREX technical support needs specific additional information to locate a problem. In this case, it is recommended to start the tracer without using filtering options. Furthermore, it turns your CS141 into a powerful network diagnostic tool that lets you examine your local LAN: Refer www.tcpdump.org to find extensive tutorials how to define filters in order to use the full potential of the CS141 as a network diagnostic system.

Data evaluation

The data analysed via diagnostic tools such as Wireshark *:

networktrace-20000101T0120.tar	30.11.2017 14:26	WinRAR-Archiv	22 KB
--------------------------------	------------------	---------------	-------

Downloaded data can be read and analysed by special diagnostic tools such as Wireshark *:

No.	Time	Source	Destination	Protocol	Length	Frame	Info
1	0.000000	192.168.200.17	10.10.10.10	TCP	66	Yes	58919 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000933	10.10.10.10	192.168.200.17	TCP	66	Yes	80 → 58919 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=16
3	0.001704	192.168.200.17	10.10.10.10	TCP	66	Yes	58920 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.002426	10.10.10.10	192.168.200.17	TCP	66	Yes	80 → 58920 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=16
5	0.003143	192.168.200.17	10.10.10.10	TCP	60	Yes	58919 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.003982	192.168.200.17	10.10.10.10	HTTP	529	Yes	GET /api/devices/bacs/report HTTP/1.1

*Wireshark is not a GENEREX product. It is available at www.wireshark.org

Delete log files

The CS141 collects and logs many data and uses non-volatile memory to store it permanently:

These data can then be retrieved via a web browser or evaluated by diagnostic tools. Since the log files may contain very sensitive information about a network state, it is recommended to delete all data before re-using the CS141 Webmanager.

Logfiles	
Networklog	Delete
Eventlog	Delete
Datalog	Delete

Network log

Deletes any network trace data

Event log

Deletes all logged data according to events

Data log

Deletes additional data of UPS measurements.

Note

Once deleted, the logfiles are gone with the wind! Normally, the CS141 provides enough space to store the data a complete lifetime cycle. If in doubt, ensure a backup of the data files is available. Please note, there is no option to recover data on the device itself.

Tutorial: Complete data delete routine

As a web manager, the CS141 provides a large amount of data about installed devices to ensure deep analysis in case of incidents:

- Battery data
- Sensor data
- Event Logs
- Transmit / receive confirmations
- [...]

The exact data collected by the CS141 webmanager depends on the hardware connected to it as well as the state of configuration. However, as these data may contain both, very sensitive information about the security concept of an IT infrastructure and clearly reconstructable chain of events, a complete data deletion is recommended in case of a reorientation to new tasks.:

As an example, if the CS141 shall be sold, all user traces should be removed completely.

Where are log files stored?

In principle, these log files can be found in two places:

1. The regular operating mode

The current log files are created in real time and managed accordingly. If you intentionally delete these files via the toolbox, they are lost - data recovery is not possible

2. The Rescue Mode

As soon as you perform a system update in any form, the existing data and configurations are parked in the Rescue Mode as "last known good". The regular operating mode is set back to 0 and starts after a successful flashing with a new set of log files. Due to this fact, the CS141 provides even an emergency data rescue option:
After an accidental flash, the rescue mode will allow to access log files as well as the last existing configuration since the previous planned firmware flash.

Complete removal of all user traces

To completely erase all data, first set the slide switch to centre position to enable the configuration mode and its hard-coded IP address 10.10.10.10 and the subnet mask 255.255.255.0. Make sure that you have assigned a suitable IP address to your computer or enter a corresponding route to access the CS141. Carry out two flash updates in a row. Ensure both cases the checkboxes are selected: Factory default and network reset.

The first flash update transfers data and configuration from the regular operating mode to the Rescue mode and deletes all data during the subsequent flash process. The second flash update transfers the completely empty configuration from the configuration mode to the rescue mode.

Note

Type `http://10.10.10.10/update` in the browser and run the flash update after entering the current administrator password. On the second pass, the default password `cs141-snmp` is active

Changing logo

Some companies do not want foreign logos inside their IT Infrastructure. Therefore, it is possible to change the logo shown on the upper left side.

How to change the logo

1. Open the graphic program of your choice
2. Create a new picture, maximum size is 200 X 54 PX

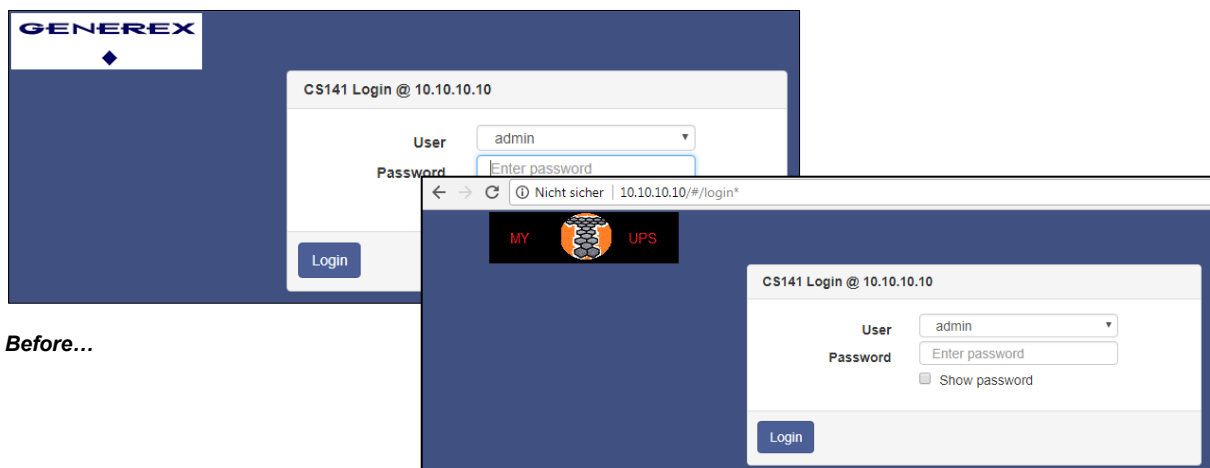


3. Edit the logo as your wish
4. When finished, save the logo with filename logo.gif – otherwise it will not work.
5. Open CS141 Toolbox:

Under Tools, you will find the configuration screen:

Use drag and drop to insert the new logo or click to select from a list.

6. Press Upload to insert the new logo.

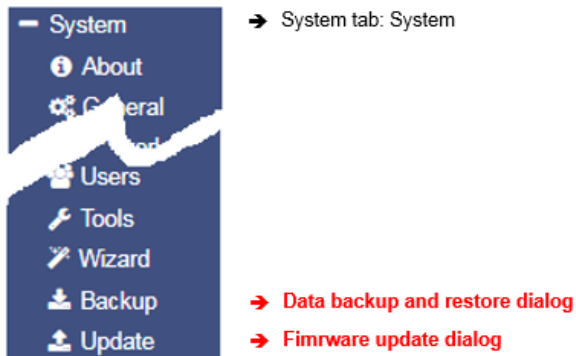


Before...

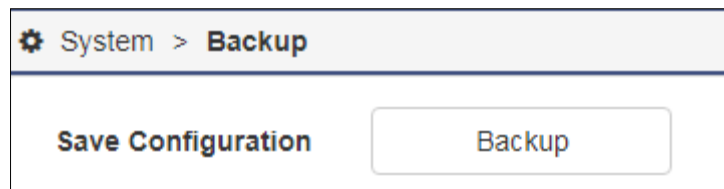
... and after

Data backup /Data restore and system updates

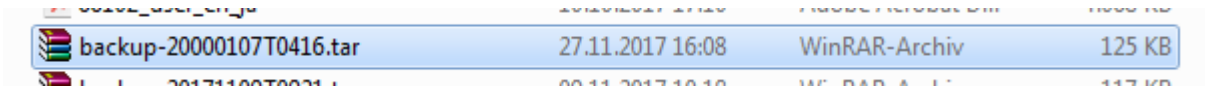
For this configuration step, navigate to the following menus



Data backup offers the option of completely backing up the current system configuration in order to quickly perform a recovery if required. The backup and restore will be done in two steps:

Step 1: Perform a backup

Open *Backup*. Under *Save Configuration*, click *Backup* to locally save a backup file to your download directory. Since the backup function is system-critical, CS141 asks for the valid administrator password.



This data backup can be run with any CS141 using a similar or higher OEM firmware version. Please note changing the file name will cause the backup file to lose its validity. As a consequence, CS141 will show an error message.

Step 2: Restoring data

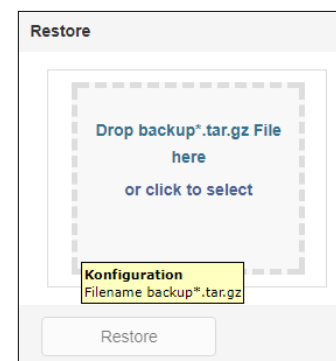
Importing a backup will use the same menu:

Use drag'n'drop to place the packed file into the box or left click on the box to open a file browser and double-click on the desired backup file. With *Restore*, the recovery process will be triggered. During recovery process, CS141 unpacks the file and automatically takes over as a current configuration. After completing the process, you will automatically be logged out and have to re-login with credentials according to the backup.

Restoring network data

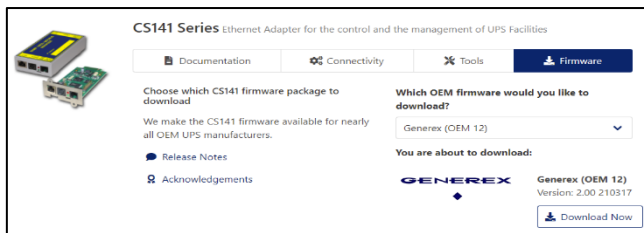
☒ **Restore network settings**

If you back up multiple identically configured web managers, you can exclude IP address settings from recovery. By doing so, previously configured IP address entries will persist while restoring all other configurations.



Please note that backups from a CS141 are compatible with any CS141 of the same or later firmware: If you use the backup on a CS141 with an older firmware, problems may arise. This behaviour is reasoned by general improvements as well as new features older firmware versions cannot work properly with. In some cases, it is possible the backup does not work.

Firmware updates



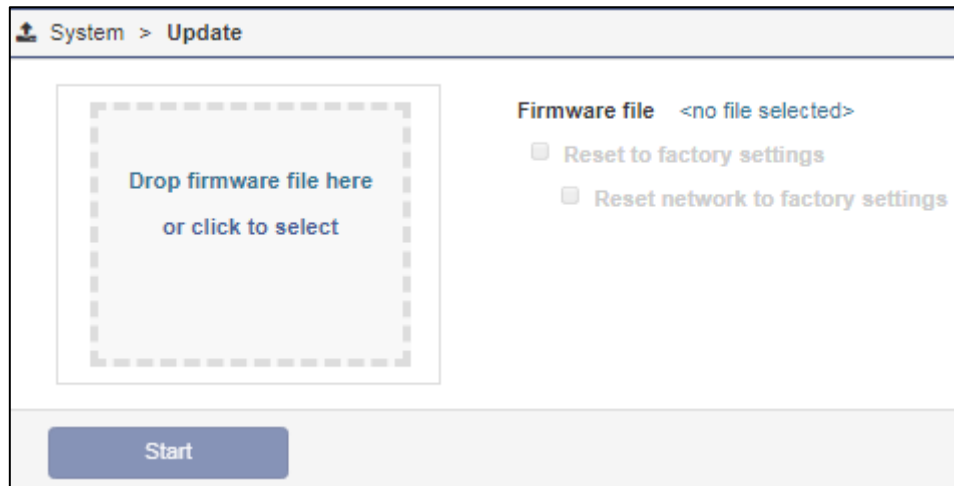
Firmware updates can be found at www.generex.de by following the download area. These System updates are regularly provided for the CS141. In addition to general product enhancements such as increased stability and improvements in operational and reliability, these updates also regularly provide new features that integrate seamlessly to existing configurations.

By default, the OEM ID 12 / GENEREX is preinstalled on delivery. Deviations will result if you have purchased the Web Manager as part of a UPS from a manufacturer that comes with OEM agreements.

Note:

Due to the fact CS141 is not technically locked, you can install the OEM version of another manufacturer at any time. In case of another UPS is used, just install an according OEM firmware version.

Under Firmware, select the version you need to use and download it to your computer. Unpacking the file is not necessary.



After downloading, open the web interface of the CS141 and open *Update*:

Drag the downloaded, packed file directly to the provided window. With Start will trigger the update process. Before triggering the update with Start button, you can select the following additional options:

Reset to factory settings

This option deletes all configurations during the update and returns the device to the delivery state.

Reset the network to factory settings

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

Note:

These two options are independent to each other to ensure not losing the IP settings. Due to this fact a factory reset using a remote access to the CS141 is possible. Please note Reset network to factory settings needs to be de-selected if CS141 has to hold its IP settings

Since the update is interactive, please remain on the page until you are prompted to restart the device. Under system, open about menu to check the success of the update.

Changing OEM Firmware

The CS141 WEBMANAGER comes in two different firmware versions:

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

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

For this, it is necessary to understand how you can detect the currently installed firmware and the required firmware:

The current firmware

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



Depending on the manufacturer, you will find the corresponding logo.

Checking firmware version

In the general system information, you will find this entry

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

The firmware version shows the OEM key:

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

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



Use the Show Version Info to check if an updated firmware is available for download. Please note that unlike updating within the same OEM firmware, changing the OEM firmware requires triggering a factory default setting since features and functions may vary among UPS manufacturers.

Most common problems while configuration and updating

This list contains typical errors that can occur when dealing with firmware updates:

Dip-switches / slide switch in wrong position

As a result, the CS141 uses either at the configuration mode IP address or an IP address assigned via DHCP. In this case you can no longer reach the CS141. Since the configuration mode on the hardware side has the 10.10.10.10 as a pre-set, it may also cause a network error, since this IP address will be used by any CS141 as a default.

Forgot manual IP address assignment or IP address set to factory default

The CS141 boots up and tries to get an IP address. If this is not possible, it starts with the default IP 10.10.10.10.

Forgotten Reboot

Since the CS141 offers the possibility to change the sliding switch on the fly and to carries out the function via software reboot, an update can evidently trigger the change of the IP address and the CS141 is no longer accessible.

The reason for this is that the CS141 starts regularly with 10.10.10.10 and points the route to it on the local PC:

if you boot the CS141 the first time, set the sliding switch to manual mode, enter IP address data and then perform an update, only the IP settings you entered will be used. As a consequence, it seems CS141 cannot be accessed at the hardcoded IP address 10.10.10.10.

Web Browser caching caused issues

Modern web browsers use technologies designed to speed up content viewing and improving multimedia experiences:

- Speech recognition
- Auto-complete names and address data
- Automatic login into websites
- Personalized commercials
- Pre-caching files from websites
- Holding website files for faster revisit
- and many more ...

These media files are loaded into a separate browser cache to ensure the fastest and most comfortable possible web experience. The CS141 uses build-in web-based technology. If you use more than one CS141, web browsers sometimes show pre-cashed data:

Mixing identical content from different devices can cause strange or illogical error messages.

Note:

This is caused by web browsers' behaviour. In this case, the browser cache must be deleted.

Force https is active

Depending on patch level and web browser used for displaying web-based content, some web browsers tend to detect this condition and automatically add the https. However, others ignore the wrong http query and return a device is not available message or react in a very strange way:

https was sometimes automatically enabled, but the https-query will be redirected to another device. In this case, browser logged your surf behaviour and assumed that you meant another device that is known to use https. As a result, you enter the IP address http://192.168.3.15 and https://192.168.3.56 will be shown. At https://192.168.3.15, however, it would have been the correct CS141 been displayed.

Again, the behaviour of the web browser is involved to cause some confusion. Deleting the browser cache will fix it.

If nothing works...

The CS141 comes with two possible options if a problem needs to reinitialize the firmware or resetting the device to factory defaults.

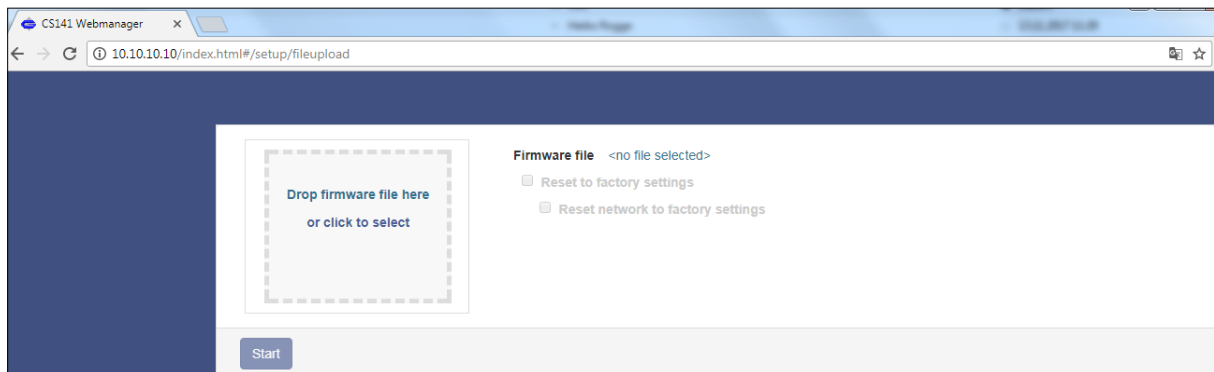
If the CS141 does not allow a login or the interface shows a faulty display, but still can be reached regularly, administrators may try the following:

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

This option allows you to force a restart of the CS141 directly.

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

This option takes administrators directly to the update screen without the need for logging in



From now you can select the desired firmware package by drag & drop or by clicking the button. If necessary, you can use the Reset to factory defaults function to reset the CS141 to factory settings. All configurations are deleted and the device is set to start-up configuration.

Enter the password for the administrator account, if you are not in configuration mode.

The process starts and after successful flashing the standard login screen will be shown.

Note:

If you have lost the administrator password, move the DIP switch to centre position. After cold boot, it is possible to flash the device directly. Enter the following line in your web browser:

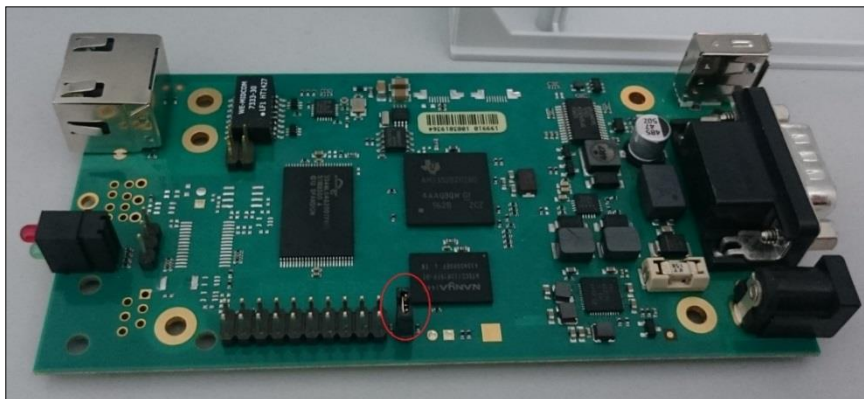
`http://10.10.10.10/update`

As a consequence, the administrative password will be set to default setting.

Starting the rescue system

If this feature is not available, the CS141 offers second option: During flashing, the CS141 saves a complete backup including the configuration of the "last known: good".

This version can be activated by setting the following jumper:

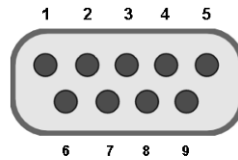


If the jumper is set and the adapter boots, CS141 will run this version as a rescue system based on the last firmware version: Inside the About menu, the firmware version will add the word RESCUE to show its current operational mode.

Appendix – useful information and diagrams

Hardware layout und and connectors of the CS141

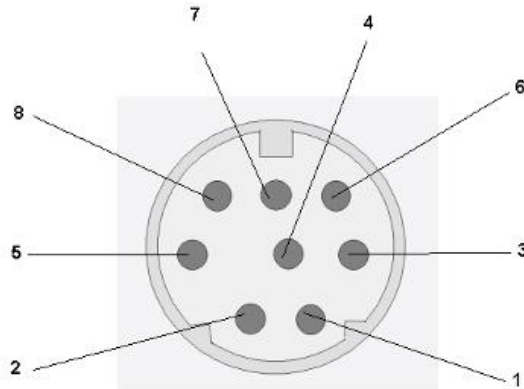
Interface description



External D-SUB 9-polig male

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

Pin COM2 Mini-DIN 8 pol



Mini DIN 8 socket RS-232:

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

RS-485 (optional):

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

Connection options for the SITEMANAGER 6

The illustration shows a typical installation of the Sitemanager without a UPS connected. It is possible to connect many types of sensors to the Sitemanager and manage circuits by switching the relay contacts.

Connection sockets and terminal strips

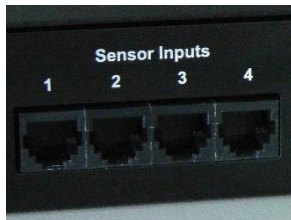
The rear of the Sitemanager is equipped with the following connection plugs:



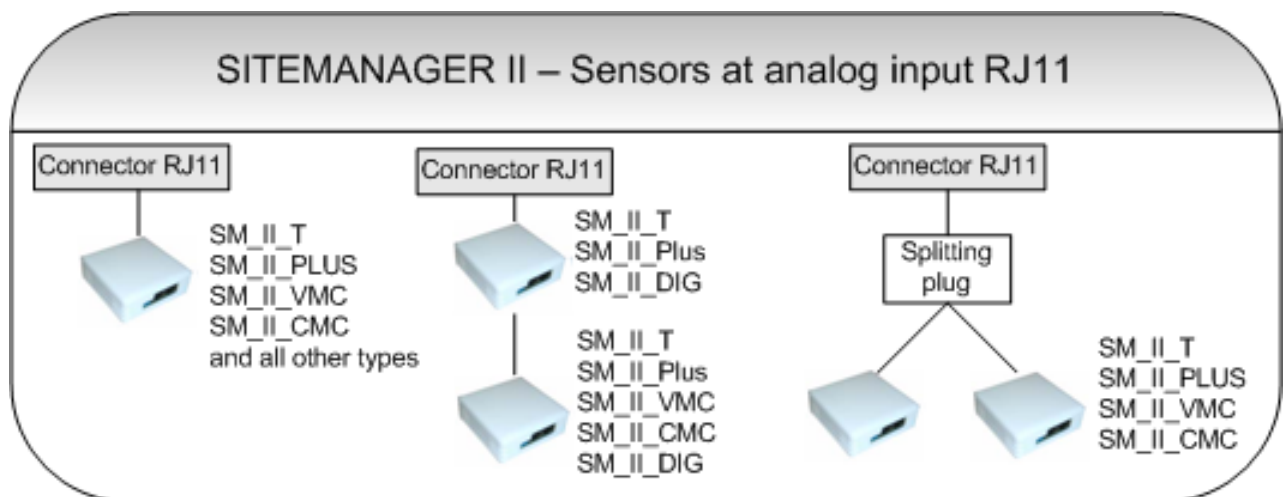
Back plate of the SITEMANAGER 6

- Power supply: Connect the external power supply unit supplied (DC, 24V).
- Sliding switch for fast and intuitive operation mode selection
- COM Port 1: RS232-Connector for Sensor Manager and other RS232-Geräte.
- LAN-Port: Connect the SITEMANAGER 6 to your network infrastructure
- 2 RJ10-BACS Bus Ports
- 4 RJ12-Connectors- each connector provides 2 analogue channels for up to 8 external sensors
- Terminal strips for 8 analogue and 8 digital signals.
- 8 Terminal stripped switchable Relay contacts (NO und NC).

Analog Inputs via RJ12-Ports



Jede der 4 RJ12-Anschlussbuchsen kann 2 analoge Eingangssignale (0-10V o. 0/4-20mA) einlesen, damit ist es möglich 8 analoge Sensoren anzuschließen. Die folgende Abbildung zeigt wie die verschiedenen Sensoren an die RJ12-Anschlussbuchsen angeschlossen werden können. Für die PIN-Belegung schauen Sie bitte in den entsprechenden Anhang am Ende dieses Dokumentes.



Sensoren Anschlussmöglichkeiten am analogen RJ12 Input

Analogue Inputs via terminal strip

Die 8 analogen Eingänge sind zusätzlich noch auf die obere Klemmleiste A01-A08 geführt. Dort können kundenspezifische Sensoren / Messwandler angeschlossen werden die ein Ausgangssignal von 0-10VDC liefern. Der Anschluss erfolgt über offene Leitungsenden (min.0,14mm² / max.1,5mm²) an den jeweiligen Federkraftanschluss der Klemmleiste.

Bitte darauf achten, dass Kanäle nicht doppelt über die RJ11-Buchse und Klemmleiste belegt werden!

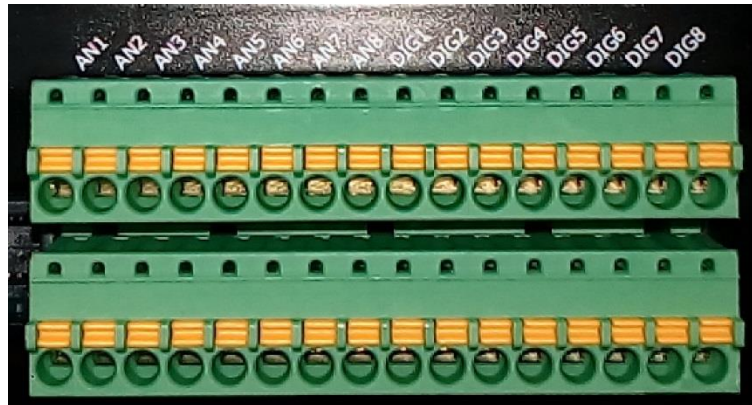
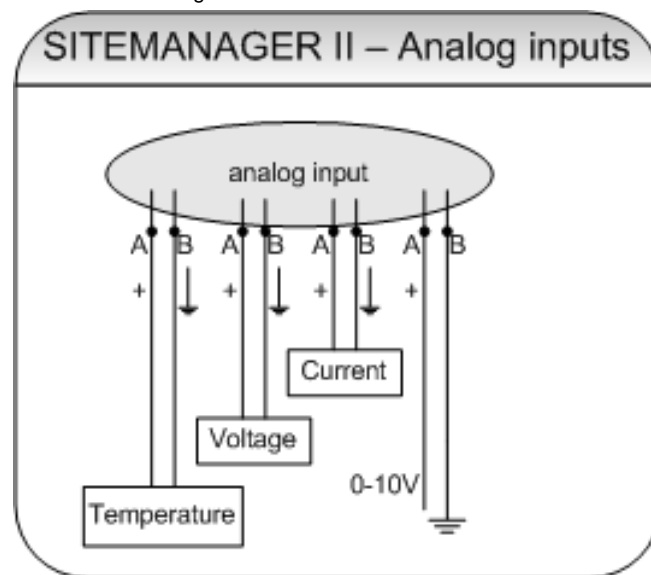


Abbildung: Auf der Klemmleiste sind die analogen Eingänge mit AN deutlich zu *erkennen*

Die folgende Abbildung zeigt die Anschlussbelegung der Klemmleiste für die Analogeingänge. Beachten Sie, dass das Eingangssignal in dem Bereich von 0-10V DC liegt.



Anschlussbelegung der Klemmleiste Analogeingänge

Konfiguration der SITEMANAGER II/v6 Analogeingänge

Jeder der 8 Analogeingänge des SITEMANAGER II/v6 bietet die Möglichkeit analoge Messwerte entweder von **0-10V (Auslieferungszustand)** oder **0-20mA bzw. 4-20mA** einzulesen.

Hierzu müssen auf der Hauptplatine die Jumper des jeweiligen Analogeinganges in der richtigen Position gesetzt sein.

Zum Ändern des Auslieferungszustandes bitte wie folgt vorgehen:

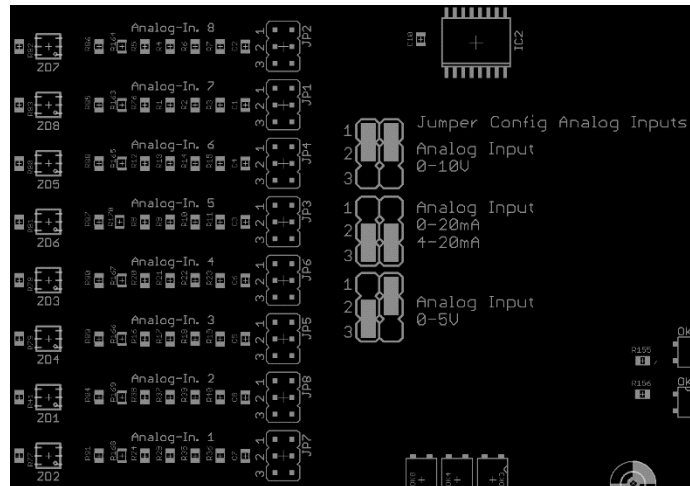
- Freischalten des SiteManagers II/v6 (Steckernetzteil ziehen)
- sämtliche Anschlussleitungen vom Gerät trennen (16/6-polige Phoenixstecker können bei Bedarf komplett vom Gerät abgezogen werden).
- Ausbau des Gerätes
- Gerät durch Lösen der 4 seitlichen Schrauben und Abziehen des Gehäusedeckels öffnen
- Jumper in der gewünschten Konfiguration setzen (siehe *Abb. 1/Abb.2*)
- In umgekehrter Reihenfolge Gerät wieder zusammenbauen/in Betrieb nehmen

Auslieferungszustand (Analog Inputs 0-10V)

Beide Jumper der Analog Inputs 1-8 (Channel 1-8) sind auf **PIN 1+2** gesetzt (Abb. 1)

In diesen Jumperstellungen dürfen nur folgende Sensoren an die Analog Inputs angeschlossen und innerhalb der Konfiguration der Sensor Type“ in der SITEMANAGER II/v6 ausgewählt werden:

- Custom 0-10V
- SM_II_T
- SM_II_T_H
- SM_II_T_Plus
- SM_II_VMC
- SM_II_CMC

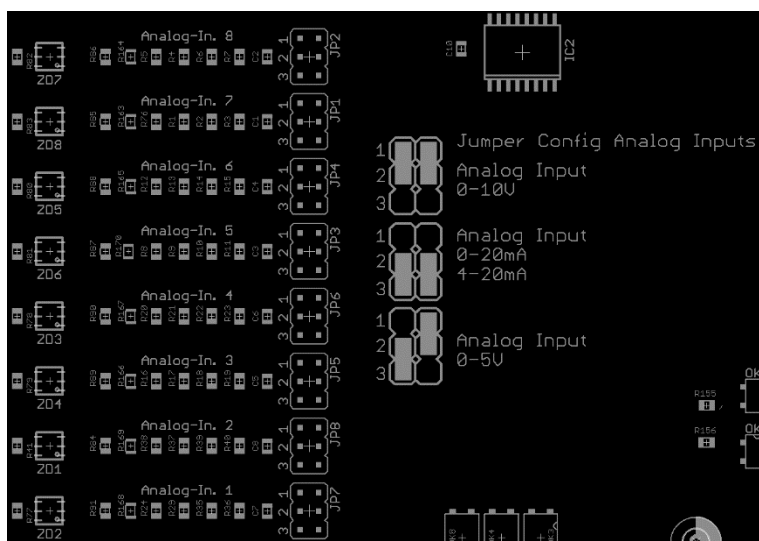


Jumperstellungen der Analog Eingänge 0-20mA bzw. 4-20mA

Beide Jumper der Analog Inputs 1-8 (Channel 1-8) sind auf **PIN 2+3** gesetzt (Abb.2)

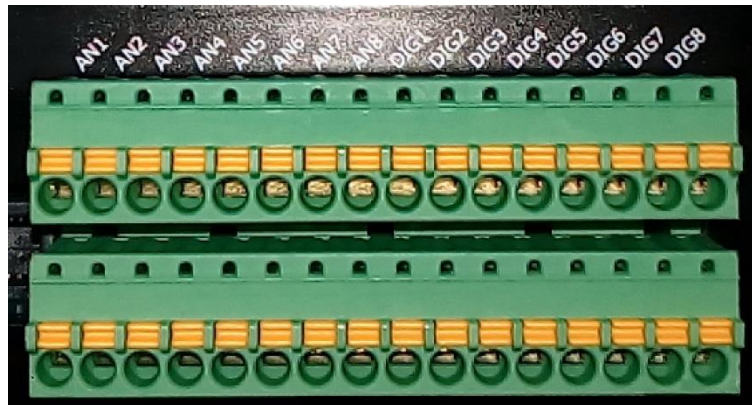
In diesen Jumperstellungen dürfen nur folgende Sensoren an die Analog Inputs angeschlossen und bei der Konfiguration des Sensor Type“ in der SITEMANAGER II/v6 Configuration ausgewählt werden:

- Custom 0-20mA
- Custom 4-20mA



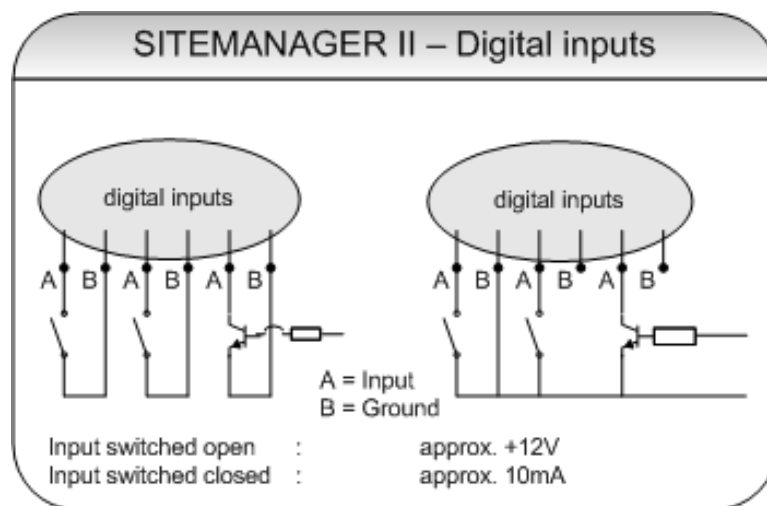
Digitale Eingänge über Klemmleisten

Unterhalb des analogen Inputs Anschlussbuchsen befindet sich die Klemmleiste für die 8 digitalen Eingänge.



Analogeingangsklemmleiste (A01-A08) und Digitaleingangsklemmleiste (D01-D08)

Die folgende Abbildung zeigt die Anschlussbelegung der Klemmleiste für die Digitaleingänge.



Anschlussbelegung der Klemmleiste Digitaleingänge

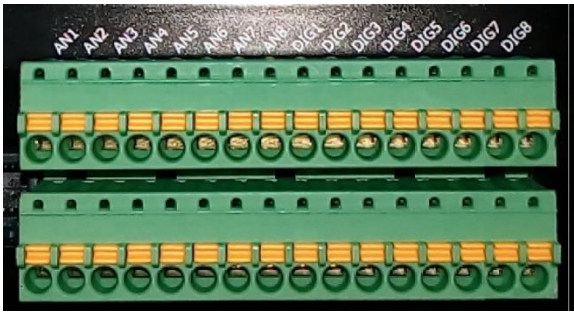
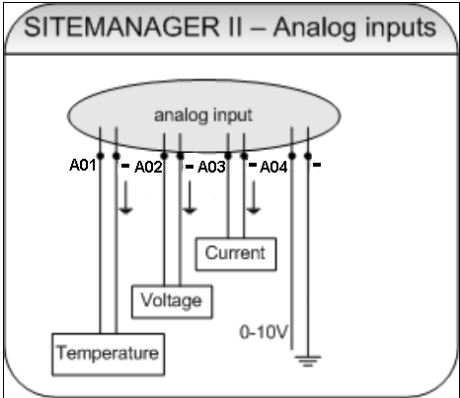


Abb.: Digital-/Analogeingänge SITEMANAGER II/v6



Klemmenbezeichnung:	Anschluss:
X1 / 12V +	Betriebsspannung +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

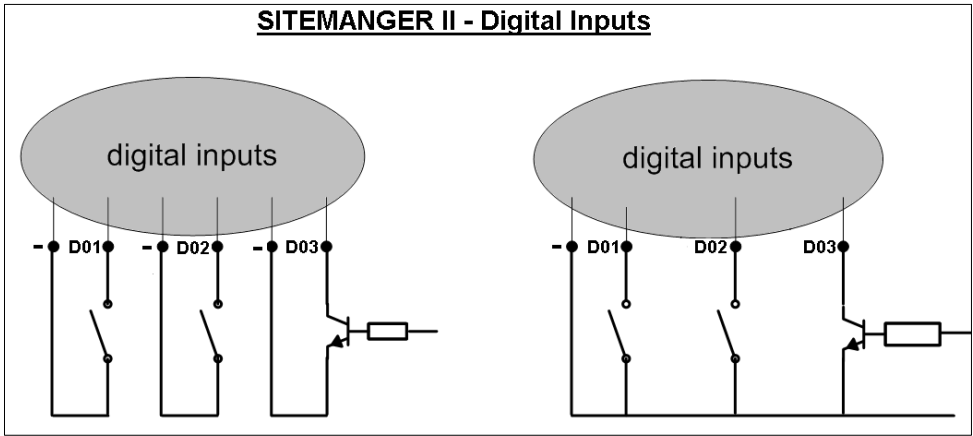
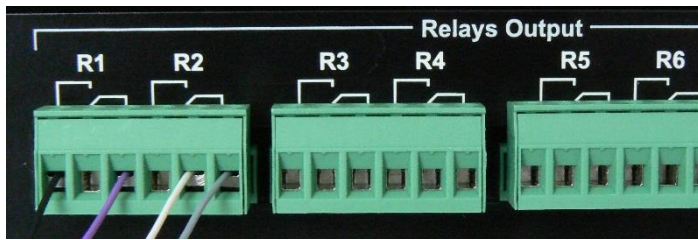
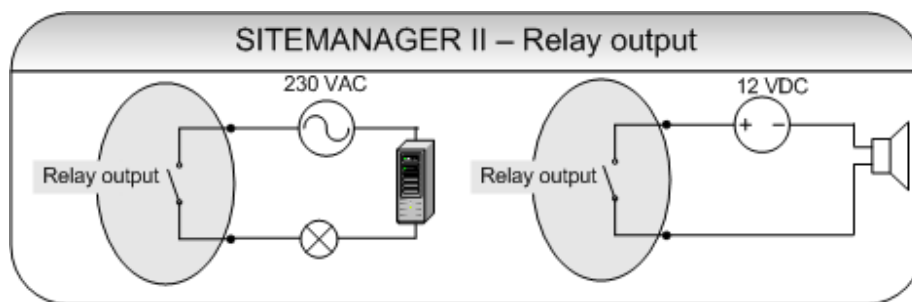


Abb.: Schaltbild Analogeingänge

Relaiskontakte über Schraubklemmen*Umschaltbare Relaiskontakte*

Der SITEMANAGER II/v6 verfügt über 8 schaltbare Relaiskontakte, mit denen man Stromkreise von bis zu 250V/4A schalten kann. Jedes Relais verfügt je über einen Öffnerkontakt (NC) und einen Schließer kontakt (NO). Für Anschlussbeispiele bitte folgende Abbildung beachten.

*Schaltbild: Relaiskontakt*

SITEMONITOR 6

Klemmenbezeichnung:	Anschluss:
X1 / 15V +	Betriebsspannung +15VDC
X1 / -	GND -
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
X2/D09	Digital Input 9
X2/D10	Digital Input 10
X2/D11	Digital Input 11
X2/D12	Digital Input 12
X2/D13	Digital Input 13
X2/D14	Digital Input 14
X2/D15	Digital Input 15
X2/D16	Digital Input 16
X2/D17 → D64	Digital Input 17 → 64

